CA Risk Authentication

CA Risk Authentication 管理ガイド

8.0

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。 本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。 いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。 また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに

このトピックでは、CA Risk Authentication を正常にインストールし、コンソールを展開し、ブートストラップした後に、*マスタ管理者*として CA Advanced Authentication にログインして基本情報を設定するための手順について説明します。

注: CA Risk Authentication のインストール、CA Advanced Authentication の展開、およびそのブートストラップの詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」を参照してください。

このトピックでは、以下の項目について説明します。

管理コンソールへのアクセス

デフォルトの MA （マスタ管理者）アカウントは、初めて CA Advanced Authentication にログインするために使用します。 以下の認証情報を使用してコンソールにログインします。

- **ユーザ名：** masteradmin
- **パスワード：** <*ブートストラップ時に設定されたパスワード*>

次の手順に従ってください:

1. Web ブラウザ ウィンドウを開きます。
2. CA Advanced Authentication にアクセスするための URL を入力します。 CA Advanced Authentication デフォルトのアドレスは以下のとおりです。

   http://<hostname>:CA Portal/arcotadmin/masteradminlogin.htm

   上記の URL で、以下を実行します。

   - *hostname* および *port* を、それぞれ、CA Advanced Authentication を展開したシステムのホスト名または IP アドレス、コンソールがリスンしているポートに置き換えます。
   - デフォルトのアプリケーション コンテキスト（arcotadmin）を変更した場合、これを新しい値に置換する必要があります。

   マスタ管理者のログイン ページが表示されます。
3. ［**パスワード**］フィールドに、ブートストラップ時に設定したパスワードを入力し、［**ログイン**］をクリックします。

   CA Advanced Authentication のランディング ページが表示されます。

CA Advanced Authentication 使用時のセキュリティに関する推奨事項

CA Advanced Authentication を使用している間、ブラウザ セッションを介した悪意のある攻撃から CA Risk Authentication を保護するために、次のことを確認してください。

- 他のアプリケーションとブラウザ セッションを共有しない。
- コンソールを操作しながら他のサイトを開かない。
- CA Advanced Authentication のために厳しいパスワード制限を実施する。
- CA Advanced Authentication の使用後は必ずログアウトする。
- セッションの終了後にブラウザ ウィンドウを閉じる。

- 実行する必要のあるタスクに応じて、管理者に適切なロールを割り当てる。

パスワードとプロファイル情報の変更

マスタ管理者パスワードを定期的に変更し、高いセキュリティを維持することを推奨します。これにより、権限のないユーザが MA 認証情報を使用して CA Advanced Authentication にアクセスするのを防ぐことができます。

［マイ プロファイル］ページを使用して、現在のパスワードと、今後実行する管理者関連およびユーザ関連のすべてのタスクがデフォルトで反映されている基本設定を変更します。

次の手順に従ってください:

1. MA としてログインしていることを確認します。
2. 管理コンソールのヘッダにある［マスタ管理者］リンクをクリックします。

   ［マイ プロファイル］ページが表示されます。
3. ［パスワードの変更］セクションで、以下を指定します。
   a. 現在のパスワード
   b. 新規パスワード
   c. ［パスワードの確認］フィールドに、新しいパスワードを再入力します。
4. ［管理者基本設定］セクションで、以下を指定します。
   a. 優先組織を有効にするかどうか。

      この組織は、今後実行するすべての管理者関連およびユーザ関連のタスクの［組織］フィールドで、デフォルトで選択されます。たとえば管理者を検索する場合、デフォルトでは、優先組織内で管理者が検索されます。
   b. 今後［組織］フィールドでデフォルトで選択される優先組織。
   c. 優先される日付/時刻形式。

      この［日付/時刻形式］は、今後すべての日付関連フィールドに表示されます。ただし、日付を入力する必要があるレポート条件ページ、ユーザ無効化ダイアログ ボックス、および管理者認証情報ロック セクションは除きます。
   d. CA Advanced Authentication のログインで優先されるロケール。

ロケールを設定する方法の詳細については、「カスタム ロケールの設定」を参照してください。デフォルト ロケールは英語（米国）です。

e. 優先されるタイム ゾーン。

このタイム ゾーンは、今後 CA Advanced Authentication のすべての日付関連のフィールドで表示されます。

タイム ゾーンのデフォルトは［GMT］です。

5. ［保存］をクリックします。

CA Risk Authentication の設定

CA Risk Authentication 固有の設定を構成する前に、CA Advanced Authentication のグローバル設定を行うことをお勧めします。 これには、以下の項目が含まれます。

- UDS の設定の更新 (P. 20)
- キャッシュのリフレッシュ (P. 25)
- キャッシュ リフレッシュ リクエストのステータスの表示 (P. 28)
- 属性の暗号化の設定 (P. 30)
- カスタム ロケールの設定 (P. 32)
- デフォルトの組織の設定 (P. 35)
- アカウント タイプの設定 (P. 36)
- 電子メールと電話のタイプの設定 (P. 39)
- 基本認証ポリシー設定の指定 (P. 41)
- マスタ管理者認証ポリシーの設定 (P. 44)
- Web サービス認証および許可の設定 (P. 46)

以下のトピックでは、これらのグローバル設定を構成するための手順について説明します。

UDS の設定の更新

ユーザ データ サービス (*UDS*) は、組織によってすでに展開されているサードパーティのデータ リポジトリ（LDAP ディレクトリ サーバなど）へのアクセスを可能にするためのユーザ仮想化レイヤです。 CA Risk Authentication サーバおよび CA Advanced Authentication は、UDS を使用して既存のデータにシームレスにアクセスしたり、エンド ユーザの情報を活用したりすることができます。標準の CA Risk Authentication SQL データベース テーブルにデータを複製する必要はありません。

CA Risk Authentication はリレーショナル データベース（RDBMS）から、または LDAP サーバから直接ユーザ データにアクセスできます。

- **リレーショナル データベースを使用する場合**は、インストール後の設定の一環として CA Risk Authentication スキーマをデータベースにシードする必要があります。
- **LDAP ディレクトリ サーバを使用していて**、このサーバに CA Risk Authentication サーバと CA Advanced Authentication からシームレスにアクセスしたい場合は、インストール後の設定の一環としてユーザ データ サービスを展開する必要があります。

UDS 接続設定の更新

デフォルトの UDS 接続設定を更新するには、［UDS 接続設定］ページを使用する必要があります。

次の手順に従ってください:

1. 必ず MA としてログインしてください。
2. **［サービスおよびサーバの設定］**タブをアクティブにします。
3. タブのサブメニューで［**CA Advanced Authentication**］オプションをクリックします。
4. サイドバー メニューの［**システム設定**］セクションで、［**UDS 接続設定**］リンクをクリックして、対応するページを表示します。
5. このページで、以下の表で説明するパラメータを指定します。 このページの有効パラメータはすべて必須です。

パラメータ	デフォルト値	Description
プロトコル	TCP	CA Advanced Authentication を使用して UDS サービスに接続するプロトコル。 使用可能なオプションは、以下のとおりです。 ■ **TCP**： UDS と CA Advanced Authentication、CA Risk Authentication サーバ、および CA Risk Authentication データベースの間で暗号化されていない情報交換を実装する場合。 ■ **一方向 SSL**: UDS と CA Risk Authentication コンポーネントの間の SSL 通信を実装し、UDS にアクセスする際に CA Risk Authentication コンポーネントがその証明書を示す必要がある場合。 ■ **双方向 SSL**: UDS と CA Risk Authentication コンポーネント間の SSL 通信を実装し、UDS および CA Risk Authentication コンポーネントの両方が情報交換中にその証明書を示す必要がある場合。
ホスト	localhost	UDS サービスを使用可能なホストの IP アドレスまたはホスト名。
ポート	8080	UDS サービスが使用可能なポート。
アプリケーション コンテキスト ルート	arcotuds	アプリケーション サーバに UDS を展開するときに指定したアプリケーション コンテキスト。

パラメータ	デフォルト値	Description
接続タイムアウト（ミリ秒）	30000	UDS サービスが到達不能になるまでのミリ秒単位の最大時間。
読み取りタイムアウト（ミリ秒）	10000	UDS からのレスポンスを待機する最大時間（ミリ秒）。
アイドル タイムアウト（ミリ秒）	30000	リクエストに応答しないアイドル接続が閉じる前の時間（ミリ秒）。
サーバ ルート証明書		UDS サーバの認証機関（CA）証明書ファイルへのパス。このファイルは PEM 形式である必要があります。 **注**: ［プロトコル］フィールドで［**TCP**］オプションを選択した場合、このフィールドは有効になりません。
クライアント証明書		CA Advanced Authentication の CA 証明書ファイルのパス。このファイルは PEM 形式である必要があります。 **注**: ［プロトコル］フィールドで［**TCP**］または［**一方向 SSL**］オプションを選択した場合、このフィールドは有効になりません。
クライアント秘密キー		CA の秘密キーが含まれるファイルの場所。 パスは絶対パス、または ARCOT_HOME への相対パスのいずれにもできます。 **注**: ［プロトコル］フィールドで［**TCP**］または［**一方向 SSL**］オプションを選択した場合、このフィールドは有効になりません。
最小接続数	4	CA Risk Authentication サーバと UDS サーバ間で作成される接続の最小数。
最大接続数	32	CA Risk Authentication サーバと UDS サーバ間で作成できる接続の最大数。

1. ［**保存**］をクリックして、加えた変更を保存します。
2. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

UDS パラメータの更新

UDS パラメータを更新する必要がある場合は、［UDS 構成］ページを使用する必要があります。

UDS パラメータを更新する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. タブのサブメニューで［**CA Advanced Authentication**］オプションをクリックします。
4. サイドバー メニューの［**UDS 設定**］セクションで、［**UDS 設定**］リンクをクリックして、対応するページを表示します。
5. このページで、以下の表で説明するパラメータを指定します。

パラメータ	**デフォルト値**	Description
検索設定		
検索結果の最大数	500	CA Advanced Authentication 内でのすべての**検索**操作に対して返されるレコードの最大数。
LDAP Configuration **注**: これらのフィールドは CA Advanced Authentication を使用して編集できません。 これらのパラメータの設定については、「*CA CA Risk Authentication インストールおよび展開ガイド*」を参照してください。		
LDAP 接続プールの初期サイズ	NA	プール内に作成される UDS と LDAP 間の接続の初期数。
LDAP 接続プールの最大サイズ	NA	UDS と LDAP 間で許可される接続の最大数。
LDAP 接続プールの推奨サイズ	NA	UDS と LDAP 間の推奨される接続数。
LDAP 接続プールのタイムアウト （ミリ秒）	NA	新しい接続がリクエストされたとき、UDS が LDAP からのレスポンスを待機する時間。
認証および認可トークンの有効期間の設定		
パージ間隔（秒）	3600	トークンが失効した*後に*、認証トークンがデータベースから消去される前の最大間隔。

パラメータ	デフォルト値	Description
有効期間（秒）	86400	発行済み認証トークンが失効する前の最大期間（デフォルトは 1 日）。

6. ［保存］をクリックして、加えた変更を保存します。
7. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

キャッシュのリフレッシュ

CA Advanced Authentication は特定のデータをキャッシュします。これにより、頻繁にアクセスされるコンソール ページおよび UDS データを高速に処理します。 通常、組織およびロールはキャッシュされます。 CA Risk Authentication はシステム レベルおよび組織レベルでキャッシュされるデータを保持します。

システム レベルでキャッシュされるデータ

以下のデータがシステム レベルでキャッシュされます。

- すべてのシステム レベル設定
  - UDS 設定および UDS 接続
  - LDAP 接続プールの詳細
  - 組織のリスト
  - グローバル キー ラベル
  - アカウント タイプの詳細
  - カスタム ロール
- グローバル データ
  - 暗号化セット
  - ローカライゼーションの設定
  - 電子メールと電話のタイプ
  - 認証および許可の設定
- すべての組織に適用可能なリソース

  すべての組織に適用可能なグローバル アカウント タイプ

組織レベルでキャッシュされるデータ

以下のデータが組織レベルでキャッシュされます。

- 個別の組織に適用可能なデータ

  暗号化セット、ローカライゼーション設定、および電子メールと電話のタイプなどのグローバル データを参照しない設定
- 組織のセットに適用可能なリソース

  組織に固有のアカウント タイプ

- ルール

重要: システム レベルと組織レベルの両方での変更が関係するデータの設定を変更するときには、先にシステム キャッシュがリフレッシュされ、次に組織のキャッシュがリフレッシュされます。 変更時にこの順序でキャッシュのリフレッシュが行われることにより、整合性のない動作が生じる場合があります。

キャッシュのリフレッシュ順序に関する例

アカウント タイプの詳細およびグローバル アカウント タイプはシステム レベルでキャッシュされます。 新しいアカウント タイプを作成する場合は、それがグローバルか組織に固有かどうかに関係なく、常にシステム キャッシュをリフレッシュする必要があります。 また、アカウント タイプが組織固有の場合は、スコープに関係するすべての組織のキャッシュをリフレッシュする必要があります。アカウント タイプの詳細については、「アカウント タイプの設定」を参照してください。

キャッシュのリフレッシュ

設定を変更した場合は、変更を有効にするために、影響を受けるサーバ インスタンスのキャッシュをリフレッシュする必要があります。 CA Risk Authentication には、管理者が CA Advanced Authentication からすべてのサーバ インスタンスのキャッシュをリフレッシュできる*統合キャッシュ リフレッシュ*機能があります。

注: MA （マスタ管理者）と GA （グローバル管理者）は、CA Advanced Authentication のキャッシュおよび CA Risk Authentication サーバとケース管理キュー サーバのすべてのインスタンスをリフレッシュできます。 MA、GA、および OA （組織管理者）は、そのスコープ内の組織のキャッシュをリフレッシュできます。

キャッシュをリフレッシュする方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［システム設定］セクションで、［キャッシュのリフレッシュ］リンクをクリックして、対応するページを表示します。
5. 以下のいずれか、または両方を選択します。
   - CA Advanced Authentication、ユーザ データ サービス、およびすべての CA Risk Authentication サーバとケース管理キュー サーバ インスタンスのキャッシュ設定をリフレッシュするには、［システム設定をリフレッシュ］を選択します。
   - ［組織キャッシュのリフレッシュ］を選択し、権限の範囲内のすべての組織のキャッシュ設定をリフレッシュします。
6. ［OK］をクリックします。
7. 表示される確認ダイアログ ボックスで［OK］をクリックします。

   現在のキャッシュ リフレッシュ リクエストのリクエスト ID を示すメッセージが表示されます。

キャッシュ リフレッシュ リクエストのステータスの表示

キャッシュ リフレッシュ リクエストのステータスを表示する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［システム設定］セクションで、［キャッシュ リフレッシュ ステータスの確認］リンクをクリックして、対応するページを表示します。
5. リクエスト ID を入力するか、または［ステータス］を選択し、［検索］をクリックしてキャッシュ リフレッシュ リクエストのステータスを確認します。

   キャッシュ リフレッシュの詳細が表示されます。 別のサーバ インスタンスのキャッシュ リフレッシュ操作のステータスを確認することができます。

   検索結果には以下の項目が一覧表示されます。

   - キャッシュ リフレッシュ リクエストの一意の識別子
   - キャッシュ リフレッシュ リクエストによって影響を受けた組織
   - リクエストを受信した時間
   - イベント タイプ
   - キャッシュ リフレッシュ リクエストによって影響を受けた CA Risk Authentication サーバ インスタンス（以下の表を参照）

パラメータ	Description
Resource	リフレッシュされた CA Risk Authentication リソース。 以下の値が使用可能です。 ■ **CA Advanced Authentication** CA Advanced Authentication とユーザ データ サービスの場合 ■ **CA Risk Authentication** CA Risk Authentication サーバの場合

パラメータ	Description
サーバ インスタンス ID	リフレッシュされたサーバ インスタンスの一意の識別子を指定します。 ■ CA Advanced Authentication とユーザ データ サーバの場合は、この値は arcotcommon.ini ファイルに設定された InstanceID パラメータから取得されます。 ■ CA Risk Authentication サーバの場合は、CA Risk Authentication サーバのインスタンス名です。 デフォルトでは、ホスト名と一意の識別子の組み合わせです。
サーバ インスタンス名	リフレッシュされた CA Risk Authentication コンポーネントのインスタンス名を指定します。 以下の値が使用可能です。 ■ CA Advanced Authentication ■ ユーザ データ サービス ■ CA Risk Authentication サーバ インスタンスの名前。
ホスト名	リフレッシュされたコンポーネントがインストールされているシステムの名前を指定します。
ステータス	キャッシュ リフレッシュ リクエストのステータスを指定します。

属性の暗号化の設定

デフォルトでは、CA Risk Authentication は、インストール時にシードしたデータベース テーブルにプレーンな形式でユーザ関連データを格納します。 このデータを暗号化するには、［属性暗号化設定］ページを使用して、暗号化するユーザ属性を選択する必要があります。 暗号化された形式で格納できる属性のリストについては、付録「マルチバイト文字および暗号化されるパラメータ」を参照してください。

属性暗号化およびデータ マスキングを設定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［システム設定］セクションで、［属性暗号化設定］リンクをクリックして、対応するページを表示します。

   注: ユーザ識別子属性を暗号化することを選択する場合は、一意にユーザを識別する際に使用する以下の属性もすべて暗号化されます。
   - ユーザ ID
   ¥xE2¥x80¥x93 アカウント ID
   - アカウント ID 属性
5. ［暗号化する属性の選択］セクションで、［暗号化用に利用可能な属性］から暗号化する属性を選択し、［暗号化用に選択した属性］に指定します。

   ［>］または［<］ボタンをクリックして、選択した属性を目的のリストに移動します。 ［>>］または［<<］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。
6. ［データ マスキング設定］セクションで、以下の表に示すパラメータを指定します。

   注: データ マスキングは、実際のデータ文字列内の特定の要素を非表示にするプロセスです。 これは、機密データを実際のデータ以外のいくつかのデータと置き換えます。

パラメータ	Description
Type	ドロップダウン リストから、暗号化を設定した属性をマスクするかマスク解除するオプションを選択します。

パラメータ	Description
開始位置からの文字数	実際のデータ文字列の開始位置からのマスクまたはマスク解除する文字の数。
終了位置からの文字数	実際のデータ文字列の終了位置からのマスクまたはマスク解除する文字の数。
マスキング文字	実際のデータをマスクする（非表示にする）ために使用する文字。

7. ［**保存**］をクリックして変更内容を保存します。
8. 展開された CA Risk Authentication サーバインスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

マスキングとマスキング解除の例

暗号化するように設定されたユーザ名をマスクする場合、［**開始位置からの文字数**］、［**終了位置からの文字数**］、［**マスキング文字**］を 2、2、x に指定すると、ユーザ名「mparker」が「xxarkxx」とマスクされます。

暗号化するように設定されたユーザ名をマスク解除する場合、［**開始位置からの文字数**］、［**終了位置からの文字数**］、［**マスキング文字**］を 2、2、x に指定すると、ユーザ名「mparker」が「mpxxxer」とマスク解除されます。

カスタム ロケールの設定

CA Risk Authentication は*ローカライゼーション*をサポートしています。ローカライゼーションとは、ロケール固有のコンポーネントを追加し、テキストを翻訳することで、選択した地域または言語の国際化されたソフトウェアを適応するプロセスです。 CA Risk Authentication がサポートするロケールを設定するには、CA Advanced Authentication の［ローカライズ設定］ページを使用します。

利用可能なロケールを設定する前に、ロケールを［利用可能］リストで選択できるように追加することができます。「*CA CA Risk Authentication インストールおよび展開ガイド*」の「ローカライゼーションの準備」を参照してください。

カスタム ロケールを設定し、デフォルト ロケールおよび日付/時刻形式を設定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［システム設定］セクションで、［ローカライズ設定］リンクをクリックして、対応するページを表示します。
5. ［サポートされるロケールの設定］セクションで、追加するロケールを［利用可能］リストから選択し、［>］または［<］ボタンを使用して［選択済み］リストに移動させます。

   ［>>］または［<<］ボタンをクリックして、すべてのロケールを目的のリストに移動することもできます。
6. ［デフォルト ロケールの設定］セクションで、ドロップダウン リストからデフォルト ロケールを選択します。
7. ［デフォルトの日付/時刻形式の設定］セクションで、使用する日付/時刻形式を指定します。

   疑問符アイコン上にカーソルを移動して、使用する日付/時刻形式を確定します。

   注: 管理者は、組織レベルで、［マイ プロファイル］ページを使用してロケールおよび日付/時刻形式を変更できます。
8. ［保存］をクリックして変更内容を保存します。

9. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

第 2 章: デフォルトの組織の設定

CA Advanced Authentication を展開すると、デフォルトで、MA アカウントと共に組織が作成されます。 このデフォルトの組織は*デフォルトの組織*（DEFAULTORG）と呼ばれます。

新しい組織を作成する必要がないため、単一の組織システムとして、「デフォルトの組織」は有用です。 「デフォルトの組織」の設定を構成し、「表示名」を変更し、管理目的で続けて使用できます。 ただし、複数組織システムの場合には、「デフォルトの組織」の「表示名」を変更し、設定を構成し、これを既定として続けて使用できます。また、新しい組織を作成し、「デフォルトの組織」に設定できます。

注: 通常、組織を指定*せずに*管理者を作成するか、ユーザを登録する場合、これらは「デフォルトの組織」内で作成されます。

デフォルトの組織を指定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイドバー メニューの［UDS 構成］セクションで、［デフォルト組織の設定］リンクをクリックして、対応するページを表示します。
5. ［デフォルトの組織］で、［組織名］リストからデフォルトの組織として設定する組織を選択します。
6. ［保存］をクリックして、このページに対して行った変更を保存します。
7. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

アカウント タイプの設定

システムで CA Risk Authentication ユーザはすべて一意のユーザ名によって識別されます。 CA Risk Authentication は、*アカウント*または*アカウント ID* の概念をサポートしています。これは、ユーザを識別するためのユーザ名とは別の ID です。 ユーザは 1 つ以上のアカウントまたはアカウント ID を持つことができます。またアカウントまたはアカウント ID を持たないことも可能です。

たとえば、顧客であるロバート ローリーを識別するために CIF（顧客情報ファイル）の ID を使用する金融機関について考えてみます。また、ロバートは、定期預金の取引を銀行と行うためのアカウント番号と、オンライン バンキング用の別のアカウント ID を使用します。 したがって、ロバートは以下のアカウント ID を持っています。

- ユーザ名： BNG02132457678
- 定期預金用のアカウント ID： 000203876544
- オンライン バンキング用のアカウント ID： rlaurie

*アカウント タイプ*は、アカウント ID を修飾し、アカウント ID を別のコンテキストで使用できるようにする属性です。 アカウント ID は、特定のアカウント タイプのユーザを一意に識別します。

たとえば、000203876544 というアカウント ID に対して FIXED_DEPOSITS というアカウント タイプを作成し、rlaurie というアカウント ID に対して ONLINE_BANKING というアカウント タイプを作成できます。

これで、ロバートがシステムにログインできるようになり、以下のいずれかを使用して識別できます。

- BNG02132457678
- FIXED_DEPOSITS/000203876544
- ONLINE_BANKING/rlaurie

CA Advanced Authentication でアカウント タイプを作成してからアカウント ID を作成する必要があります。 今後作成される組織を含め、特定の組織のみ、またはすべての組織で利用できるアカウント タイプを設定できます。 組織レベルでは、各組織はアカウント タイプのセットをサポートすることを選択できます。

注: 特定の組織で 2 人のユーザが 1 つのアカウント タイプに対して同じアカウント ID を持つことはできません。 以下の組み合わせは常に一意です。
– 組織名、アカウントタイプ、およびアカウント ID
- 組織名、ユーザ名

新しいアカウント タイプの作成

新しいアカウント タイプを作成する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイドバー メニューの［UDS 構成］セクションで、［アカウント タイプの設定］リンクをクリックして、対応するページを表示します。
5. （これが初めて追加するアカウント タイプである場合）［新規アカウント タイプの追加］セクションで以下の操作を行います。
   a. アカウント タイプの名前を入力します。
   b. アカウント タイプの表示名を入力します。
   c. 必要に応じて、［+］記号をクリックして［カスタム属性］セクションを展開し、このアカウント タイプに対して追加するカスタム属性の名前と値を指定します。
6. 割当先組織のセクションで、以下を実行します。
   - このアカウント タイプを、既存のすべての組織および今後作成されるすべての組織に対して使用する場合は、すべてに適用することを選択します。

     注: このようなアカウントは、組織レベルで［アカウント タイプの設定］ページの［グローバル アカウント］の下に表示されます。

     または

   - アカウント タイプを割り当てる組織を［利用可能］リストから選択して［選択済み］リストに移動させます。

     注: 特定の組織に割り当てられたアカウントは、組織レベルの［アカウント タイプの設定］ページで**組織固有アカウント**として表示されます。

［>］または［<］ボタンをクリックして、選択した組織を目的のリストに移動します。［>>］または［<<］ボタンをクリックして、すべての組織を目的のリストに移動することもできます。

7. ［作成］ボタンをクリックしてアカウント タイプを作成します。
8. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

アカウント タイプの更新

既存のアカウント タイプを更新する方法

1. ［アカウント タイプの選択］ドロップダウン リストからアカウント タイプを選択します。
2. 必要なフィールドを変更し、［更新］をクリックします。

   注: いったんアカウント タイプを作成すると、アカウント タイプの名前を変更することはできません。
3. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

アカウント タイプの削除

既存のアカウント タイプを削除する方法

1. ［アカウント タイプの選択］ドロップダウン リストからアカウント タイプを選択します。
2. ［Delete］をクリックします。

   重要: アカウント タイプに対してユーザ アカウントを作成した場合、そのアカウント タイプを削除することはできません。
3. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

電子メールと電話のタイプの設定

CA Risk Authentication では、ユーザと管理者を作成する際に、複数の電子メール アドレスと電話番号を指定することができます。MA はグローバル レベルで複数の電子メールと電話のタイプを設定でき、これは自動的にすべての組織で利用できるようになります。また MA は、特定の電子メールと電話のタイプを必須として、その他のものをオプションとして指定することができます。 組織内にユーザと管理者を作成するときには、MA が設定した電子メールと電話のタイプに値を入力するように促されます。 組織を作成する際には、別の電子メールと電話のタイプを設定して、グローバル設定を無効にすることもできます。

注: 組織レベルで設定された電子メールおよび電話タイプの属性は、グローバル レベルで設定された値より優先されます。

電子メールと電話のタイプの例

MA が、すべての組織で使用する必要があるとして以下の電子メールと電話のタイプを設定したと仮定します。

- （必須）電子メール タイプ： Work Email
- （オプション）電子メール タイプ： Personal Email
- （必須）電話タイプ： Work Phone
- （オプション）電話タイプ： Home Phone

GA がグローバル設定を使用する組織 *Org1* の管理者を作成するとき、GA は Work Email および Work Phone に対して値を指定する*必要があります*。必要に応じて、GA はその他の電子メールと電話のタイプを追加できますが、電子メールと電話のタイプに対するグローバル設定を削除することはできません。

電子メールと電話のタイプの属性を設定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［UDS 構成］セクションで、［電子メール/電話タイプ設定］リンクをクリックして、対応するページを表示します。
5. ［電子メール タイプの設定］セクションで、以下のように指定します。

- 複数の電子メール タイプが設定されている場合、電子メール タイプの優先度。 上向きまたは下向きのアイコンを使用して優先度を変更します。 優先度は、複数の電子メール タイプが設定されているときに、電子メール タイプが画面に表示される順序を定義します。
- 設定する電子メールのタイプ。たとえば、業務用、個人用など。
- 電子メール タイプの表示名。
- 電子メール タイプが必須かどうか。

たとえば、業務用電子メールが最初に表示されるように、業務用電子メールの優先度が個人用電子メールより高くなるように設定できます。

6. ［電話タイプの設定］セクションで、以下のように指定します。
   - 複数の電話タイプが設定されている場合、電話タイプの優先度。上向きまたは下向きのアイコンを使用して優先度を変更します。 優先度は、複数の電話タイプが設定されているときに、電話タイプが画面に表示される順序を定義します。
   - 設定する電話番号のタイプ。たとえば、自宅、業務用など。
   - 電話タイプの表示名。
   - 電話タイプが必須かどうか。

   注: ［**+**］アイコンをクリックすると、複数の電子メールおよび電話タイプを追加できます。
7. ［保存］をクリックして変更内容を保存します。
8. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

基本認証ポリシー設定の指定

基本認証ポリシー、LDAP 認証ポリシー、または WebFort ユーザ パスワード メカニズムを使用して、CA Advanced Authentication にログインする管理者を認証することができます。使用されるメカニズムは、以下のように、組織の作成時に選択したオプションによって決定されます。

- 組織の作成時に［**基本ユーザ パスワード**］オプションを選択した場合は、「基本認証パスワード ポリシーの設定」で説明しているデフォルトの認証ポリシーを使用できます（グローバル レベル）。
- ［**LDAP ユーザ パスワード**］オプションを選択した場合は、LDAP に格納されたパスワードを管理者がログインに使用します。認証ポリシーは LDAP システムで定義します。
- **ユーザ パスワード** オプションを選択した場合は、Strong Authentication が展開され、アクセス可能であることを確認します。

注: ご使用の環境に Strong Authentication をインストールおよび設定する場合の詳細については、「*CA Strong Authentication インストールおよび展開ガイド*」および「*CA Strong Authentication 管理ガイド*」を参照してください。

基本認証ポリシーの設定

*基本認証方法*では、その名前が意味するように、管理者がユーザ ID と対応するパスワードを使用して管理コンソールにログインします。

［基本認証ポリシー］ページを使用して、パスワード長、使用可能な特殊文字の数、アカウントをロックする前に許可されたログインの失敗回数などの制限を実施することでパスワード ポリシーを強化することができます。

基本認証ポリシーを設定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイド バー メニューの［認証］セクションで、［基本認証ポリシー］リンクをクリックして、対応するページを表示します。
5. ［パスワード ポリシー設定］セクションで、以下の表に示すパラメータを指定します。 このページのパラメータはすべて必須です。

パラメータ	デフォルト値	Description
パスワードの最小文字数	6	パスワードで使用する必要がある最小文字数。 値は 6 ～ 32 文字で設定できます。
パスワード最大長	25	パスワードに含めることのできる最大文字数。 値は 6 ～ 32 文字で設定できます。
失敗の最大試行回数	5	管理者がパスワードを不正確に指定しても良い連続回数。この回数を超えると認証情報がロックされます。 3 ～ 10 の値を設定できます。
数字の最小文字数	1	パスワードに含める必要のある数字(0 ～ 9)の最小数。値は 0 ～ 32 文字で設定できます。
パスワード履歴数	3	再使用できない以前のパスワードの最大数。
有効期間	180 日	パスワードが有効な最大日数。
マルチバイト文字を許可 このチェック ボックスをオンにした場合、以下のオプションは無効です。		パスワード内のマルチバイト文字を許可する場合は、このオプションを選択します。

パラメータ	デフォルト値	Description
アルファベット文字の最小文字数	4	パスワードに含める必要のあるアルファベット文字（a-z および A-Z）の最小数。 値は 0 ～ 32 文字で設定できます。
特殊文字の最小文字数	1	パスワードに含める必要のある使用可能な特殊文字の最小文字数。 値は 0 ～ 32 文字で設定できます。
使用できる特殊文字（オプション）	!@#$%^&*()_+	パスワードに含めることができる特殊文字のリスト。

6. ［**保存**］をクリックして、このページに対して行った変更を保存します。
7. 展開された CA Risk Authentication サーバインスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

マスタ管理者認証ポリシーの設定

デフォルトでは、マスタ管理者は、ユーザ ID と対応するパスワードを使用して管理コンソールにログインできる*基本認証*方式を使用します。

［マスタ管理者認証ポリシー］ページを使用して、パスワード長、使用可能な特殊文字の数、アカウントをロックする前に許可されたログインの失敗回数などの制限を実施することで MA のパスワード ポリシーを強化することができます。

マスタ管理者認証ポリシーを設定する方法

1. 必ず MA としてログインしてください。
2. **［サービスおよびサーバの設定］**タブをアクティブにします。
3. タブのサブメニューで［**CA Advanced Authentication**］オプションをクリックします。
4. サイド バー メニューの［**認証**］セクションで、［**マスタ管理者認証ポリシー**］リンクをクリックして、対応するページを表示します。
5. ［**パスワード ポリシー設定**］セクションで、以下の表に示すパラメータを指定します。 このページのパラメータはすべて必須です。

パラメータ	**デフォルト値**	Description
パスワードの最小文字数	6	パスワードで使用する必要がある最小文字数。 値は 6 ～ 32 文字で設定できます。
パスワード最大長	25	パスワードに含めることのできる最大文字数。 値は 6 ～ 32 文字で設定できます。
失敗の最大試行回数	5	管理者がパスワードを不正確に指定しても良い連続回数。 この回数を超えると認証情報がロックされます。 3 ～ 10 の値を設定できます。
数字の最小文字数	1	パスワードに含める必要のある数字（0 ～ 9）の最小数。 値は 0 ～ 32 文字で設定できます。
パスワード履歴数	3	再使用できない以前のパスワードの最大数。
有効期間	180 日	パスワードが有効な最大日数。
マルチバイト文字を許可 このチェック ボックスをオンにした場合、以下のオプションは無効です。		パスワード内のマルチバイト文字を許可する場合は、このオプションを選択します。

パラメータ	デフォルト値	Description
アルファベット文字の最小文字数	4	パスワードに含める必要のあるアルファベット文字（a-z および A-Z）の最小数。 値は 0 ～ 32 文字で設定できます。
特殊文字の最小文字数	1	パスワードに含める必要のある使用可能な特殊文字の最小文字数。 値は 0 ～ 32 文字で設定できます。
使用できる特殊文字（オプション）	!@#$%^&*()_+	パスワードに含めることができる特殊文字のリスト。

6. ［**保存**］をクリックして、このページに対して行った変更を保存します。

Web サービス認証および許可の設定

CA Risk Authentication は、CA Advanced Authentication によってサポートされている操作をプログラムによって実行する Web サービスを提供します。認証および許可を有効にすることで、これらの Web サービスの呼び出しを安全に保護できます。CA Advanced Authentication を使用して、認証と許可を有効にする Web サービスを選択できます。

注: Web サービスの認証と許可がどのように動作するかの詳細については、「*CA CA Risk Authentication Web サービス開発者ガイド*」の「Web サービス セキュリティの管理」を参照してください。

Web サービスの認証および許可を設定する方法

1. 必ず MA としてログインしてください。
2. ［サービスおよびサーバの設定］タブをアクティブにします。
3. タブのサブメニューで［CA Advanced Authentication］オプションをクリックします。
4. サイドバー メニューの［Web サービス］セクションで、［認証と許可］リンクをクリックして、対応するページを表示します。
5. ［Web サービス］セクションで、Web サービスを［無効］リストから選択して［有効］リストに移動させます。

   ［>］または［<］ボタンをクリックして、選択した Web サービスを目的のリストに移動します。［>>］または［<<］ボタンをクリックして、すべての Web サービスを目的のリストに移動することもできます。
6. ［保存］をクリックして変更内容を保存します。
7. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

第 3 章: カスタム ロールの操作

重要: このトピックで説明されているロール管理タスクは、**マスタ管理者**のみが実行できます。

CA Risk Authentication には、事前定義された権限に関連付けられたビルトイン ロールが付属しています。このトピックの詳細については、「サポートされるロール」を参照してください。 ただし、CA Risk Authentication では、これらの事前定義されたロールを以下のような場合に操作できる機能も提供しています。

- デフォルトのロールが組織の要件を満たしていない場合。
- CA Risk Authentication によって提供されるものとは異なるロール情報を管理する必要がある場合。

このトピックでは、重要な利点である、CA Risk Authentication でカスタム ロールを作成して適用する機能について説明します。 ここでは、以下について説明します。

カスタム ロールについて

MA は、以下のいずれかの事前定義された親ロール（「CA Advanced Authentication の概要」で説明）からの権限のサブセットを継承する*新しい管理ロール*を作成できます。

- GA （グローバル管理者）
- OA （組織の管理者）
- UA （ユーザ管理者）

これらのロールはカスタム ロールと呼ばれ、親ロールに関連付けられているデフォルト権限のいくつかを**無効にする**ことによって作成されます。たとえば、GA の組織を作成する権限を無効にする必要がある場合、この権限を無効にし、同じものを GA に割り当てることにより、カスタム ロールを作成できます。

カスタム ロールを作成すると、管理者を作成または更新する際にロール オプションとして利用可能になります。 カスタム ロールは、作成するだけではなく更新および削除も行えます。

カスタム ロールについて知っておくべきこと

- MA *のみ*がカスタム ロールを作成できます。
- カスタム ロールは、単一のロールの権限のサブセットのみを継承できます。 言い換えれば、カスタム ロールは、2 つの異なるロールから権限を継承することはできません。

  たとえば、ユーザの管理（UA 権限）および組織の作成（OA 権限）を行う権限を持つカスタム UA ロールは作成できません。
- 親ロールに割り当てられていない権限は、カスタム ロールにも割り当てることはできません。

  たとえば、事前定義された OA ロールに組織の作成権限がない場合は、この OA ロールに基づいたカスタム ロールもその権限を持つことができません。
- カスタム ロールを作成するときには、1 つ以上の権限に相当するタスクは、それらの権限の少なくとも 1 つがまだ利用可能な場合に限り、継続して表示されます。

  たとえば、アクティブ化、非アクティブ化、および削除の権限が無効な場合でも、更新の権限がまだ利用できる場合、［**組織の検索**］リンクが表示されます。
- 新たに作成したカスタム ロールは、CA Advanced Authentication サーバのキャッシュをリフレッシュした*後にのみ*、CA Advanced Authentication のほかのインスタンスで利用できます。

事前定義済みカスタム ロール

作成できるカスタム ロールのほかに、CA Risk Authentication にはケース管理に必要な 3 つの事前定義済みカスタム ロールが付属しています。 これらのロールには次のものが含まれます。

- **QM：** キュー マネージャ ロールには、ケースの監督に必要な権限があります。 このロールはデフォルトの組織管理者ロールから派生しています。
- **CSR：** テクニカル サポート担当者ロールには、ケースでの作業およびエンド ユーザの呼び出しの処理に必要な権限があります。このロールはデフォルトのユーザ管理者ロールから派生しています。
- **FA：** 不正行為アナリスト ロールには、隠れた傾向およびパターンを検索するケースの分析に必要な権限があります。 このロールもデフォルトのユーザ管理者ロールから派生しています。

ケース管理およびキュー マネージャ、テクニカル サポート担当者、および不正行為アナリスト ロールに関する詳細については、「ケースの管理」を参照してください。

［カスタム ロールの更新］ページでこれらの既定のカスタム ロールを参照できます。

カスタム ロールの作成

カスタム ロールを作成する方法

1. 必ず MA としてログインしてください。
2. ［ユーザと管理者］タブをアクティブにします。
3. タブのサブメニューで［ロールの管理］リンクをクリックします。
4. ［ロールの管理］セクションで、［カスタム ロールの作成］リンクをクリックします。 ［カスタム ロールの作成］ページが表示されます。
5. ［ロール詳細］セクションで、以下の情報を指定します。
   - ［ロール名］： 新規ロールを識別する一意の名前です。 この名前は、この新規ロールを認証して認可するために CA Risk Authentication によって内部で使用されます。
   - ロール表示名： CA Advanced Authentication のほかのすべてのページおよびレポートに表示されるロールの説明的な名前です。
   - ［ロールの説明］： 以降での参照に役立つ、ロールに関連する情報です。
   - ［ロール元］: このカスタム ロールの派生元の既存のロールです。
6. ［権限の設定］で、新規ロールには利用できないロールを指定します。
   a. ［利用可能な権限］リストで、カスタム ロールに関して無効にすることが必要なすべての権限を選択します。

      このリストには、［ロール元］フィールドで選択した管理ロールで利用可能なすべての権限が表示されます。

   b. ［>］ボタンをクリックすると、選択した権限が［利用不可の権限］リストに移動されます。
7. ［作成］をクリックすると、カスタム ロールが作成されます。
8. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

カスタム ロール情報の更新

既存のカスタム ロールの定義を更新する方法

1. 必ず MA としてログインしてください。
2. ［ユーザと管理者］タブをアクティブにします。
3. タブのサブメニューで［ロールの管理］リンクをクリックします。
4. ［ロールの管理］セクションで、［カスタム ロールの更新］リンクをクリックします。

   ［カスタム ロールの更新］ページが表示されます。
5. 更新するロール名を選択します。
6. ［ロール詳細］セクションで、必要に応じて［ロール表示名］および［ロールの説明］を変更します。
7. ［権限の設定］で、必要に応じてロールに利用できない権限のリストを指定します。
   a. ［利用可能な権限］リストで、新規ロールに対して無効にする必要のある権限をすべて選択します。

      このリストには、［ロール元］フィールドで選択した管理ロールで利用可能なすべての権限が表示されます。
   b. ［>］ボタンをクリックすると、選択した権限が［利用不可の権限］リストに移動されます。
8. ［権限の設定］で、必要に応じてロールに利用できる権限のリストを指定します。
   a. ［利用不可の権限］リストで、新規ロールのために有効にする権限を選択します。

      このリストには、［ロール元］フィールドで選択した管理ロールで利用できないすべての権限が表示されます。
   b. ［>］ボタンをクリックして、選択した権限を［利用可能な権限］リストに移動します。
9. ［更新］をクリックすると、カスタム ロールの定義が更新されます。
10. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

カスタム ロールの削除

重要: 現在管理者に割り当てられているカスタム ロールを削除する必要がある場合は、［管理者の更新］ページを使用して、まずこのロールを割り当てられているすべての管理者のロールを変更する必要があります。その後で、このトピックの手順に従います。

既存のカスタム ロールを削除する方法

1. 必ず MA としてログインしてください。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. タブのサブメニューで［**ロールの管理**］リンクをクリックします。
4. ［**ロールの管理**］セクションで、［**カスタム ロールの削除**］リンクをクリックします。

   ［カスタム ロールの削除］ページが表示されます。
5. ［**ロール詳細**］セクションで、削除する必要のあるカスタム ロールを［**ロール名**］リストから選択します。
6. ［**削除**］をクリックすると、選択したカスタム ロールが削除されます。
7. 展開したすべての RiskMinder サーバ インスタンスをリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

管理権限の要約

以下の表に、カスタム ロールの作成に使用するサポートされている 3 つのレベルの管理者が使用できる権限を要約して示します。

表で使用されている列名の頭字語は次のとおりです。

- グローバル管理者 -> **GA**
- 組織の管理者 -> **OA**
- ユーザ管理者 -> **UA**

注: + 記号は、指定されたレベルの管理者が利用できるアクション（または権限）を示します。

権限	GA	OA	UA
組織を管理する権限 これらの権限に関係するタスクの詳細については、「組織の管理」を参照してください。			
組織の作成	+	*	*
組織の更新	+	+	*
組織ステータスの更新	+	+	*
組織の一覧表示	+	+	+
デフォルト組織の取得	+	+	+
組織の削除	+	+	*
アカウント タイプを管理する権限 これらの権限に関係するタスクの詳細については、「アカウント タイプの設定」を参照してください。			
アカウント タイプの作成	+	*	*
アカウント タイプの更新	+	+	*
アカウント タイプの削除	+	*	*
管理者を管理する権限 これらの権限に関係するタスクの詳細については、「管理者の管理」を参照してください。			
管理者の作成	+	+	*
管理者の更新	+	+	+
管理者の削除	+	+	*

権限	GA	OA	UA
ユーザを管理する権限 これらの権限に関係するタスクの詳細については、「ユーザの管理」を参照してください。			
Create User	+	+	+
ユーザの更新	+	+	+
ユーザ ステータスの更新	+	+	+
ユーザの一覧表示	+	+	+
アカウントのユーザの一覧表示	+	+	+
ユーザ ステータスの取得	+	+	+
ユーザ カスタム属性の設定	+	+	+
ユーザの検索	+	+	+
ユーザ詳細の取得	+	+	+
PAM の取得	+	+	+
PAM の設定	+	+	+
ユーザの削除	+	+	+
ユーザ アカウントを管理する権限			
ユーザ アカウントの作成	+	+	+
ユーザ アカウントの更新	+	+	+
ユーザ アカウントの一覧表示	+	+	+
ユーザ アカウントの取得	+	+	+
ユーザ アカウントの削除	+	+	+
キャッシュを管理する権限 これらの権限に関係するタスクの詳細については、「キャッシュのリフレッシュ」を参照してください。			
システム キャッシュのリフレッシュ		*	*
組織キャッシュのリフレッシュ			*
グローバル キャッシュ リフレッシュ リクエストの表示		*	*

権限	GA	OA	UA
組織キャッシュ リフレッシュ リクエストの表示			*
電子メールと電話のタイプの権限 これらの権限に関係するタスクの詳細については、「電子メールと電話のタイプの設定」を参照してください。			
電子メール/電話のタイプの追加			*
電子メール/電話のタイプの更新			*
電子メール タイプの一覧表示			
電話タイプの一覧表示			
基本認証の権限 これらの権限に関係するタスクの詳細については、「基本認証ポリシー設定の指定」を参照してください。			
グローバル基本認証ポリシーの更新		*	*
組織の基本認証ポリシーの更新			*
暗号化の権限 これらの権限に関係するタスクの詳細については、「属性の暗号化の設定」を参照してください。			
選択した暗号化セットの設定			*
暗号化用に設定された属性の一覧表示			*
ケースを管理する権限 これらの権限に関係するタスクの詳細については、「ケースの管理 (P. 341)」を参照してください。			
キューの管理			*
キューの再構築			*
キュー ステータスの表示			*
ケースでの作業			

権限	GA	OA	UA
着信コールの管理			
トランザクションの分析			
CA Risk Authentication 設定 これらの権限に関係するタスクの詳細については、「グローバル設定の管理 (P. 157)」および「組織固有の CA Risk Authentication の設定の管理」を参照してください。			
ルール セットの作成	+	+	*
ルール セットの割り当て	+	+	*
チャネルの割り当ておよびデフォルト アカウント タイプの設定	+	*	*
その他の設定の管理（グローバル レベル）	+	*	*
その他の設定の管理（組織レベル）	+	+	*
モデル設定（グローバル レベル）	+	*	*
モデル設定（組織レベル）	+	*	*
CA Risk Authentication コールアウトの設定	+	+	*
運用環境への移行	+	+	*
ルールを管理する権限 これらの権限に関係するタスクの詳細については、「グローバル設定の管理 (P. 157)」を参照してください。			
リスクの評価	+	+	+
ユーザとデバイスの関連付けの一覧表示	+	+	+
ユーザとデバイスの関連付けの削除	+	+	+
リスト データおよびカテゴリ マッピングの管理	+	+	*
ルールおよびスコアリング管理	+	+	*
評価後	+	+	+
その他の権限			
Q&A 属性の取得	+	+	+
Q&A 値の取得	+	+	+
Arcot 属性の一覧表示	+	+	*

権限	GA	OA	UA
リポジトリ属性の一覧表示	+	+	*
Q&A 検証の実行	+	+	+
バルク アップロード	+	+	*
バルク アップロード リクエストの表示	+	+	*
レポートの権限 これらの権限に関係するタスクの詳細については、「ケース管理レポートの生成 (P. 380)」および「レポートの管理」を参照してください。			
マイ アクティビティ レポートの表示	+	+	+
ユーザ アクティビティ レポートの表示	+	+	+
ユーザ作成レポートの表示	+	+	+
組織レポートの表示	+	+	*
管理者アクティビティ レポートの表示	+	+	+
リスク詳細アクティビティ レポート	+	+	+
アドバイス サマリ レポートの表示	+	+	+
例外ユーザ レポートの表示	+	+	+
ルール設定レポートの表示	+	+	*
ルール データ レポートおよびカテゴリ マッピングの表示	+	+	*
ケース アクティビティ レポート	+	+	*
平均ケース期間レポート	+	+	*
誤検知レポート	+	+	+
不正行為統計レポートの表示	+	+	+
ルール有効性レポート	+	+	+
レポート サマリ	+	+	+

第 4 章: CA Risk Authentication サーバ インスタンスの管理

重要: このトピックで説明されるすべての設定およびタスクは、**マスタ管理者**のみが実行できます。

マスタ管理者は、CA Risk Authentication インスタンスをローカルで管理する必要があります。 ただし、サーバ インスタンスを管理するには、インスタンスに接続するための接続パラメータを設定する必要があります 詳細については、「サーバ接続の設定」を参照してください。

接続パラメータを設定してからのみ、CA Risk Authentication サーバ インスタンスを管理できます。 インスタンスを管理するためのタスクには、以下があります。

- サーバ接続の設定 (P. 60)
- 信頼ストアの作成 (P. 67)
- 通信プロトコルの設定 (P. 68)
- CA Risk Authentication 予測モデルの設定 (P. 74)
- サーバ インスタンスのリフレッシュ (P. 75)
- サーバ インスタンス設定の更新 (P. 78)
- サーバ インスタンスのシャットダウン (P. 81)
- サーバ インスタンスの再起動 (P. 82)

注: 「**サーバ インスタンスのシャットダウン**」は、「システム管理者用のツール」で説明されているシステム ツールを使用して実行することもできます。

サーバ接続の設定

CA Risk Authentication には以下の 2 つのサーバ コンポーネントが含まれています。

- **CA Risk Authentication サーバ**。このサーバはリスク評価のコア エンジンです。
- **ケース管理キュー サーバ**。このサーバはキューの定義に応じてケースの構築、優先順位付け、管理者への送信を行います。

以下の表に、［CA Risk Authentication 接続］ページの 4 つのセクションを示し、各セクションを使用して接続できるコンポーネントについて説明します。

設定セクション	Description
サーバ管理接続	CA Risk Authentication サーバ管理ポートに接続するために CA Advanced Authentication によって使用されます。たとえば、CA Risk Authentication サーバへのキャッシュ リフレッシュおよびシャットダウン リクエストです。
ケース管理キュー サーバ接続	ケース管理キュー サーバ管理ポートに接続するために CA Advanced Authentication によって使用されます。 たとえば、CA Risk Authentication サーバへのキャッシュ リフレッシュおよびシャットダウン リクエストです。
管理接続	CA Risk Authentication サーバ管理 Web サービス ポートに接続するために CA Advanced Authentication によって使用されます。 たとえば、［ルールおよびスコアリング管理］画面、［モデル設定］画面です。
ケース管理キュー サーバ接続	ケース管理キュー サーバ インスタンスに接続するために CA Advanced Authentication によって使用されます。たとえば、キュー再構築リクエストの発行、キュー内の次のケースの取得です。

CA Risk Authentication サーバ管理接続

CA Risk Authentication サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続設定を行うには、［CA Risk Authentication サーバ管理接続］セクションを使用する必要があります。

CA Risk Authentication サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続パラメータを指定する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. タブのサブメニューで［**CA Risk Authentication**］リンクをクリックします。
4. 対応するページがまだ表示されていない場合は、タスク ペインの［**CA Risk Authentication 接続**］リンクをクリックすると表示されます。
5. 以下の表の情報を使用して、CA Risk Authentication 接続パラメータを設定します。

フィールド	Description
サーバ	必要な CA Risk Authentication サーバ管理インスタンスをインストールしたシステムの IP アドレスまたはホスト名を入力します。 **注**: CA Risk Authentication サーバがインストールされているシステムが、そのホスト名を使ってネットワーク アクセスできることを確認してください。
サーバ管理ポート	リスク評価サービスが公開されているポートを入力します。
Transport	CA Risk Authentication サーバ管理インスタンスに接続するために、以下のコンポーネントのトランスポート モード（**TCP** または **SSL**）を指定します。 ■ Server Management Web Services ■ Administration Web Services ■ Transaction Web Services ■ Authentication Native
サーバ CA ルート証明書	サーバの CA ルート証明書を参照してアップロードします。 **注**: このサーバ証明書は PEM 形式である必要があります。
PKCS#12 内のクライアント証明書 - キーのペア	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。

フィールド	Description
クライアント PKCS#12 パスワード	クライアントの PKCS#12 ストアのパスワードを入力します。

1. ［**保存**］をクリックすると、設定した設定が保存されます。

ケース管理キュー サーバ管理

ケース管理キュー サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続設定を行うには、［ケース管理キュー サーバ接続］セクションを使用する必要があります。

ケース管理キュー サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続パラメータを指定する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. タブのサブメニューで［**CA Risk Authentication**］リンクをクリックします。
4. 対応するページがまだ表示されていない場合は、タスク ペインの［**CA Risk Authentication 接続**］リンクをクリックすると表示されます。
5. 以下の表の情報を使用して、CA Risk Authentication 接続パラメータを設定します。

フィールド	Description
サーバ	必要なケース管理キュー サーバ管理インスタンスをインストールしたシステムの IP アドレスまたはホスト名を入力します。
サーバ管理ポート	ケース管理サービスが公開されているポートを入力します。
Transport	ケース管理キュー サーバ管理インスタンスに接続するために、以下の対応するコンポーネントのトランスポート モード（**TCP** または **SSL**）を指定します。 ■ Server Management Web Services ■ Administration Web Services ■ Transaction Web Services ■ Authentication Native

フィールド	Description
サーバ CA ルート証明書	サーバの CA ルート証明書を参照してアップロードします。 **注**: このサーバ証明書は PEM 形式である必要があります。
PKCS#12 内のクライアント証明書 - キーのペア	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。
クライアント PKCS#12 パスワード	クライアントの PKCS#12 ストアのパスワードを入力します。

1. ［**保存**］をクリックすると、設定した設定が保存されます。

CA Risk Authentication 管理接続

CA Risk Authentication サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続設定を行うには、［CA Risk Authentication 管理接続］セクションを使用する必要があります。

CA Risk Authentication サーバ管理インスタンスに接続するために CA Advanced Authentication によって使用される接続パラメータを指定する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. タブのサブメニューで［**CA Risk Authentication**］リンクをクリックします。
4. 対応するページがまだ表示されていない場合は、タスク ペインの［**CA Risk Authentication 接続**］リンクをクリックすると表示されます。
5. 以下の表の情報を使用して、CA Risk Authentication 接続パラメータを設定します。

フィールド	Description
サーバ	必要な CA Risk Authentication サーバ管理インスタンスをインストールしたシステムの IP アドレスまたはホスト名を入力します。 **注**: CA Risk Authentication サーバがインストールされているシステムが、そのホスト名を使ってネットワーク アクセスできることを確認してください。

フィールド	Description
サーバ管理ポート	リスク評価サービスが公開されているポートを入力します。
Transport	CA Risk Authentication サーバ管理インスタンスに接続するために、以下のコンポーネントのトランスポート モード(**TCP** または **SSL**)を指定します。 ■ Server Management Web Services ■ Administration Web Services ■ Transaction Web Services ■ Authentication Native
サーバ CA ルート証明書	サーバの CA ルート証明書を参照してアップロードします。 **注**: このサーバ証明書は PEM 形式である必要があります。
PKCS#12 内のクライアント証明書 - キーのペア	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。
クライアント PKCS#12 パスワード	クライアントの PKCS#12 ストアのパスワードを入力します。

1. ［**保存**］をクリックすると、設定した設定が保存されます。

ケース管理キュー サーバ接続

ケース管理キュー サーバ インスタンスに接続するために CA Advanced Authentication によって使用される接続設定を行うには、［ケース管理キュー サーバ接続］セクションを使用する必要があります。

ケース管理キュー サーバ インスタンスに接続するために CA Advanced Authentication によって使用される接続パラメータを指定する方法

1. 必ず MA としてログインしてください。
2. **［サービスおよびサーバの設定］**タブをアクティブにします。
3. タブのサブメニューで［**CA Risk Authentication**］リンクをクリックします。
4. 対応するページがまだ表示されていない場合は、タスク ペインの［**CA Risk Authentication 接続**］リンクをクリックすると表示されます。
5. 以下の表の情報を使用して、CA Risk Authentication 接続パラメータを設定します。

フィールド	Description
ホスト	キュー サーバ インスタンスをインストールしたシステムの IP アドレスまたはホスト名を入力します。 **注**: キュー サーバがインストールされているシステムが、そのホスト名を使ってネットワーク アクセスできることを確認してください。
バックアップ ホスト	バックアップの Queuing Server インスタンスが使用可能なシステムの IP アドレスを入力します（インストールされている場合）。 **重要**: ケース管理キュー サーバのバックアップを開始する*前*に、この［**バックアップ ホスト**］パラメータを設定する必要があります。
ポート	ケース管理サービスが公開されているポートを入力します。
Transport	ケース管理インスタンスに接続するために、以下の対応するコンポーネントのトランスポート モード（**TCP** または **SSL**）を指定します。 ■ Server Management Web Services ■ Administration Web Services ■ Transaction Web Services ■ Authentication Native

フィールド	Description
サーバ CA ルート証明書	サーバの CA ルート証明書を参照してアップロードします。 **注**: このサーバ証明書は PEM 形式である必要があります。
PKCS#12 内のクライアント証明書 - キーのペア	クライアント証明書および秘密キーを含む PKCS#12 ストアを参照してアップロードします。
クライアント PKCS#12 パスワード	クライアントの PKCS#12 ストアのパスワードを入力します。

1. ［**保存**］をクリックすると、設定した設定が保存されます。

信頼ストアの作成

トラスト ストアを作成して、SSL ベースの通信の実行中に、CA Risk Authentication サーバ インスタンスに対して CA Risk Authentication コンポーネント（CA Advanced Authentication や Java SDK を含む）またはその他のクライアントを認証することができます。*トラスト ストア*には、CA Risk Authentication サーバおよびケース管理キュー サーバ インスタンスが信頼している CA ルート証明書のセットが含まれます。

［トラステッド認証機関］ページを使用することにより、信頼ストアを作成し、新しいルート証明書を信頼ストアに追加できます。

CA Risk Authentication サーバまたはケース管理キュー サーバ インスタンス用のトラスト ストアを作成する方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにし、サブメニューの［**CA Risk Authentication**］タブがアクティブになっていることを確認します。
3. ［**システム設定**］セクションで、［**トラステッド認証機関**］リンクをクリックして、［トラステッド認証機関］ページを表示します。
4. ［**名前**］フィールドに、作成する新しいトラスト ストアの名前を入力します。
5. 対応する［**参照**］ボタンをクリックし、信頼された CA の 1 つ以上のルート証明書をアップロードします。 ［**さらに追加**］をクリックすると、証明書をアップロードするための他のフィールドが表示されます。
6. 証明書がすべてアップロードされたら、［**保存**］をクリックします。

通信プロトコルの設定

［プロトコル設定］ページでは、CA Risk Authentication サーバ インスタンスまたはケース管理キュー サーバ インスタンスのプロトコルを設定できます。

ドロップダウン リストから CA Risk Authentication サーバ インスタンスを選択することによって、認証と管理を行うために、CA Advanced Authentication、SDK、および Web サービスが CA Risk Authentication サーバ インスタンスと通信するために使用するプロトコルを設定できます。サーバがこれらの有効な各コンポーネントをリスンするポートに加えて、トランスポートのセキュリティ メカニズム（TCP または SSL）も指定できます。また、メカニズムとして SSL を指定した場合、有効で信頼できるクライアント コンポーネントの証明書と秘密キーを指定する必要があります。これらは安全な接続を確立するために必要です。

以下の表では、CA Risk Authentication サーバ インスタンスの［**プロトコル リスト**］テーブルに表示されるプロトコルについて説明し、そのデフォルト ポート番号のリストを示します。

プロトコル	**デフォルト ポート番号**	Description
ネイティブ（TCP）	7680	このプロトコルは、CA Risk Authentication サーバ インスタンスと CA Risk Authentication Java SDK （リスク評価と発行（廃止）を含む）の間の通信を可能にします。 **注**: Web サービス インターフェースは、ユーザ管理 Web サービス定義言語（WSDL）の一部として発行に使用できます。
管理 Web サービス	7777	これは、CA Risk Authentication サーバと管理 Web サービスの間の通信用プロトコルです。 CA Risk Authentication サーバは管理 Web サービス コールをこのポートで待ち受けます。 **注**: これらのコールに CA Risk Authentication 発行（廃止）またはリスク管理コールは*含まれません*。

プロトコル	デフォルト ポート番号	Description
トランザクション Web サービス	7778	このプロトコルは、CA Risk Authentication サーバ インスタンスに接続するために、リスク評価および発行（廃止）Web サービスによって使用されます。このプロトコルは、認証および発行 Web サービスによって送信される Web サービス リクエストを受信します。 **注**: これらのコールに管理サービス コールは*含まれません*。
ネイティブ（SSL）	7681	このバイナリ プロトコルは、CA Risk Authentication サーバ インスタンスと CA Risk Authentication Java SDK （リスク評価と発行（廃止）を含む）の間の SSL ベースの通信を可能にします。
サーバ管理	7980	arrfclient ツールは、サーバ管理アクティビティ（正常なシャットダウンとサーバ キャッシュ リフレッシュ）で、このプロトコルを使用して CA Risk Authentication サーバ インスタンスと通信します。 この CA Advanced Authentication ツールの詳細については、「arrfclient : サーバ リフレッシュとシャットダウン ツール」を参照してください。

同様に、ドロップダウン リストからケース管理キュー サーバ インスタンスを選択して、認証と管理を行うために、CA Advanced Authentication とケース管理キュー サーバが CA Risk Authentication サーバ インスタンスと通信するために使用するプロトコルを設定できます。 サーバがこれらの有効な各コンポーネントをリスンするポートに加えて、トランスポートのセキュリティ メカニズム（TCP または SSL）も指定できます。 また、メカニズムとして SSL を指定した場合、有効で信頼できるクライアント コンポーネントの証明書と秘密キーを指定する必要があります。これらは安全な接続を確立するために必要です。

以下の表では、ケース管理キュー サーバ インスタンスの［**プロトコルのリスト**］テーブルに表示されるプロトコルについて説明し、そのデフォルト ポート番号のリストを示します。

プロトコル	**デフォルト ポート番号**	Description
ケース管理キュー サーバ	7779	このプロトコルは、指定のポートでケース管理リクエスト（サーバ側）を待ち受けるために、キュー サーバ モジュールによって使用されます。
ケース管理のキュー管理	7780	これは CA Risk Authentication サーバとケース管理キュー サーバの間の通信用プロトコルです。 CA Risk Authentication サーバは、このポートでケース管理 Web サービス コールを待ち受けます。

CA Risk Authentication サーバおよびケース管理キュー サーバのネットワーク プロトコルを設定する方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにし、サブメニューの［**CA Risk Authentication**］タブが表示されていることを確認します。
3. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
4. ドロップダウン リストから CA Risk Authentication サーバ インスタンスまたはケース管理キュー サーバ インスタンスを選択します。

   ［**プロトコルのリスト**］が表示されます。
5. ［**プロトコルのリスト**］テーブルで、設定するプロトコルに対応するリンクをクリックします。

   対応するプロトコルのページが表示されます。
6. 必要に応じて、ページ上でフィールドを編集します。以下の表に、これらのフィールドの説明を示します。

列	アクションの説明
プロトコル ステータスの変更	［**アクション**］ドロップダウン リストを有効にし、プロトコルのステータスを変更するには、このチェック ボックスをオンにします。
アクション	必要なプロトコルを有効にするには、［**有効化**］を選択します。 サポートされているプロトコルの詳細については、前の 2 つの表を参照してください。
ポート	対応するサービスが使用可能なポート番号を入力します。 CA Risk Authentication プロトコルのデフォルト ポート番号を以下に示します。 ■ **CA Risk Authentication ネイティブ（TCP）** ： 7680 ■ **CA Risk Authentication ネイティブ（SSL）** ： 7681 ■ **管理 Web サービス** ： 7777 ■ **トランザクション Web サービス** ： 7778 ■ **キュー サーバ** ： 7779 ■ **キュー管理** ： 7780 ■ **サーバ管理** ： 7980
最小スレッド数	ポート上で処理されるスレッドの最小数。

列	アクションの説明
最大スレッド数	ポート上で処理されるスレッドの最大数。
Transport	サポートされている以下のいずれかのデータ転送モードを指定します。 ■ **TCP**： TCP （Transmission Control Protocol）モードは、両方の CA Risk Authentication プロトコルによってサポートされているデフォルトのモードです。 データをクリア テキストで送信します。 ■ **SSL**： SSL （Secure Sockets Layer）はトランザクションに高度なセキュリティを提供します。これは、データを暗号化して転送し、受信後復号化するためです。
HSM 内のキー	SSL 通信用の秘密キーが HSM デバイスにある必要がある場合は、このチェック ボックスを有効にします。この場合、CA Risk Authentication サーバおよびケース管理キュー サーバは、提供された証明書チェーンに基づいて秘密キーを検索します。 このチェック ボックスは［トランスポート］で［**SSL**］を選択した場合にのみ有効です。
サーバ証明書チェーン	トランスポートのセキュリティ モードが SSL の場合に使用される証明書チェーンを指定します。 **サーバ証明書チェーン**をアップロードするには、**参照**ボタンを使用します。 **重要**: ここでアップロードしたチェーン内の証明書は、リーフ証明書 --> 中間 CA 証明書 --> ルート証明書の階層に従います。証明書とキーは PEM 形式である必要があります。
サーバ秘密キー	**サーバ秘密キー**をアップロードするには、**参照**ボタンを使用します。 **注**: このフィールドは［**HSM 内のキー**］チェック ボックスをオンにしなかった場合にのみ有効になります。
クライアント ストアの選択	信頼された CA のルート証明書が含まれる信頼ストアを選択します。 トラスト ストアの設定の詳細については、「信頼されるストアの作成」を参照してください。

1. ページ上で設定を完了したら、［**保存**］をクリックします。

（オプション）SSL 通信の設定

デフォルトでは、CA Advanced Authentication は Transmission Control Protocol （TCP）を使用して CA Risk Authentication サーバと通信します。 ただし、TCP はスプーフィングおよび man-in-the-middle 攻撃に対して脆弱です。 CA Advanced Authentication を使用して、CA Risk Authentication のさまざまなコンポーネント間の安全な通信を保証するように SSL を設定できます。

注: CA Risk Authentication のさまざまなコンポーネント間の SSL ベースの通信の段階的な設定については、「SSL の設定」を参照してください。

安全な通信を行うために SSL を設定している場合は、スタートアップ ログ ファイルで対応するエントリを参照できます。 以下の表に、SSL が CA Risk Authentication サーバおよびケース管理キュー サーバのプロトコルに対して設定される場合のログ ファイル エントリを示します。

プロトコル	ログ ファイルのエントリ
CA Risk Authentication	
サーバ管理	Started listener for [Server Management] [7980] [SSL] [srvmgrwsprotocol]
トランザクション Web サービス	Started listener for [RiskFort Trans WS] [7778] [SSL] [transwsprotocol]
管理 Web サービス	Started listener for [RiskFort Admin WS] [7777] [SSL] [aradminwsprotocol]
ネイティブ（SSL）	Started listener for [RiskFort Native (SSL)] [7681] [SSL] [RiskFort]
ケース管理キュー サーバ	
ケース管理キュー管理	Started listener for [Case Management Admin] [7780] [SSL] [srvmgrwsprotocol]
ケース管理キュー サーバ	Started listener for [Case Management Server] [7779] [SSL] [RiskFortCaseManagement]

CA Risk Authentication 予測モデルの設定

CA Advanced Authentication を使用して、CA Risk Authentication 予測モデルの URL とタイムアウトのパラメータを設定できます。

CA Risk Authentication 予測モデルを設定する方法

1. MA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. ［**CA Risk Authentication**］タブをアクティブにします。
4. サイドバー メニューの［**モデル設定**］で、［**モデル設定**］リンクをクリックします。

   ［モデル設定］ページが表示されます。
5. ［**候補値**］列で、以下の表に示すパラメータを指定します。

パラメータ	Description
予測モデル URL （プライマリ）	CA Risk Authentication 予測モデルのプライマリ URL。
予測モデル URL （バックアップ）	CA Risk Authentication 予測モデルのバックアップ URL。
接続タイムアウト（ミリ秒）	CA Risk Authentication サーバと予測モデルの間の接続が期限切れになるまでの時間。
読み取りタイムアウト（ミリ秒）	CA Risk Authentication サーバが予測する予測モデルからレスポンスが戻るまでの時間。
最小接続数	モデル サーバに接続する接続プール内の接続の最小数。
最大接続数	モデル サーバに接続する接続プール内の接続の最大数。

6. ［**モデル設定のアップロード**］をクリックして、変更を保存します。
7. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

サーバ インスタンスのリフレッシュ

CA Advanced Authentication または arrfclient ツールを使用して、CA Risk Authentication サーバおよびケース管理キュー サーバ インスタンスをリフレッシュできます。

CA Advanced Authentication を使用したサーバ インスタンスのリフレッシュ

［インスタンス管理］ページでインスタンスを選択して、特定の CA Risk Authentication サーバおよびケース管理キュー サーバ インスタンスをリフレッシュできます。

サーバ インスタンスをリフレッシュする方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにし、サブメニューの［**CA Risk Authentication**］タブが表示されていることを確認します。
3. ［**インスタンス設定**］セクションで、［**インスタンス管理**］リンクをクリックして、対応するページを表示します。

   以下の表に、［インスタンス管理］ページの列を示します。

列	Description
［Instance Name］	CA Risk Authentication サーバまたはケース管理キュー サーバ インスタンスの名前。
最終スタートアップ時刻	インスタンスが最後に起動された時刻。
最終シャットダウン時刻	インスタンスが最後にシャット ダウンされた時刻。
前回のリフレッシュ時刻	インスタンスが最後にリフレッシュされた時刻。
稼働時間	インスタンスが実行されている期間。
ステータス	インスタンスのステータス。
リフレッシュする組織リスト	リフレッシュする組織のリスト。 ■ リフレッシュする組織を選択するには、ドロップダウン リスト内の［**選択**］を選択します。 または ■ 組織をすべてリフレッシュするには、ドロップダウン リスト内の［**すべて**］を選択します。

列	Description
システム キャッシュ リフレッシュ	システム キャッシュをリフレッシュする場合は、このチェックボックスをオンにします。

1. ［**CA Risk Authentication インスタンス**］セクションで、以下の操作を実行します。
   a. リフレッシュする CA Risk Authentication サーバのインスタンスを選択します。
   b. ［**リフレッシュする組織リスト**］ドロップダウン リストからリフレッシュする組織を選択します。
   c. システム キャッシュ設定をリフレッシュする場合は、［**システム キャッシュ リフレッシュ**］を選択します。
   d. ［**リフレッシュ**］をクリックします。
2. ［**ケース管理インスタンス**］セクションで、以下の操作を実行します。
   a. リフレッシュするケース管理キュー サーバのインスタンスを選択します。
   b. ［**リフレッシュする組織リスト**］ドロップダウン リストからリフレッシュする組織を選択します。
   c. システム キャッシュ設定をリフレッシュする場合は、［**システム キャッシュ リフレッシュ**］を選択します。
   d. ［**リフレッシュ**］をクリックします。

arrfclient ツールを使用したサーバ インスタンスのリフレッシュ

CA Risk Authentication サーバとケース管理キュー サーバ インスタンスの両方をリフレッシュするには、arrfclient ツールを使用できます。

重要: 以下のサブセクションで説明するように、CA Risk Authentication サーバの arrfclient ツールを実行する前に、riskfortadminclient.ini. の Host と Port の値を設定します。 詳細については、「arrfserver : CA Risk Authentication サーバ ツール」を参照してください。

ツールの詳細については、「arrfclient : サーバ リフレッシュとシャットダウン ツール」を参照してください。

Windows の場合

以下のように arrfclient ツールを実行して、CA Risk Authentication サーバのキャッシュをリフレッシュします。

1. コマンド プロンプト ウィンドウを開きます。
2. 以下のディレクトリに移動します。
   `<install_location>¥Arcot Systems¥bin¥`
3. 以下のコマンドを実行してリフレッシュします。
   - **CA Risk Authentication サーバ インスタンスの場合**
     `arrfclient -cr`
   - **ケース管理キュー サーバ インスタンスの場合**
     `arrfclient <host_name> CA Portal -cr`

UNIX ベースのプラットフォームの場合

以下のように arrfclient ツールを実行して、CA Risk Authentication サーバのキャッシュをリフレッシュします。

1. ターミナル ウィンドウを開きます。
2. 以下のディレクトリに移動します。
   `<install_location>/arcot/bin/`
3. 以下のコマンドを実行してリフレッシュします。
   - **CA Risk Authentication サーバ インスタンスの場合**
     `arrfclient -cr`
   - **ケース管理キュー サーバ インスタンスの場合**
     `arrfclient <host_name> CA Portal -cr`

サーバ インスタンス設定の更新

CA Risk Authentication サーバおよびケース管理キュー サーバ インスタンスのインスタンス属性、ログ設定、およびデータベース設定を更新できます。

インスタンスに固有の設定を更新する方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにし、サブメニューの［**CA Risk Authentication**］タブがアクティブになっていることを確認します。
3. ［**インスタンス設定**］セクションで、［**インスタンス管理**］リンクをクリックして、対応するページを表示します。
4. 設定を更新するインスタンスに対応するリンクをクリックします。

   インスタンスに固有の設定を更新するページが表示されます。
5. ［**インスタンス属性**］セクションで、以下の操作を実行します。
   a. CA Risk Authentication サーバまたはケース管理キュー サーバ インスタンスの［**インスタンス名の変更**］チェック ボックスをオンにします。
   b. ［**新規インスタンス名**］フィールドでインスタンスの名前を指定します。
6. ［**ロギング構成**］セクションで、以下の表に記載されている値を指定します。

フィールド	Description
トランザクション ログ ディレクトリ	トランザクション ログ ファイルを格納するディレクトリ。 パスは絶対パス、または ARCOT_HOME への相対パスのいずれにもできます。
ロールオーバー開始サイズ（バイト単位）	ログ ファイルが記録できる最大バイト数。 ログ ファイルがこのサイズに達すると、指定した名前で新規ファイルが作成され、古いファイルがバックアップ ディレクトリに移動されます。
トランザクション ログ バックアップ ディレクトリ	古いトランザクション ログ ファイルを格納するバックアップ ディレクトリ。 パスは絶対パス、または ARCOT_HOME への相対パスのいずれにもできます。

フィールド	Description
［Log Level］	ログに記録されたエントリの重大度レベル。 Fatal、WARNING、INFO、および DETAIL は、サポートされている重大度レベルを降順で示したものです。 詳細については、付録「サポートされる重大度レベル」を参照してください。
GMT でのタイム スタンプのログ記録	GMT を使用してログ記録された情報にタイム スタンプを設定する場合は、このオプションを選択します。 CA Risk Authentication では、ローカル タイム ゾーンまたは GMT を使用してログ記録された情報にタイム スタンプを設定できます。
トレース ログの有効化	処理中に呼び出された各機能の開始および終了ログをログ記録する追加のログ フラグ。 デフォルトでは、このフラグは無効になっています。 このフラグを有効にすると、デバッグ用に大量のデータがログに記録されます。CA サポートより指示がない限り、運用環境でこのフラグを有効にしないでください。

7. ［**データベース構成**］セクションで、以下の表に記載されている値を指定します。

フィールド	Description
最小接続数	CA Risk Authentication サーバとデータベースの間で作成される接続の最小数。
最大接続数	CA Risk Authentication サーバとデータベースの間で作成できる接続の最大数。
接続数の増分	プール内のデータベース接続がすべて既存のスレッドによって使い果たされた場合、およびスレッドのどれかが新しいデータベース接続をリクエストした場合の接続のインクリメント値。
モニタ スレッド スリープ時間（秒）	データベースがアクティブで機能しているかどうかを確認するためにデータベース モニタ スレッドがデータベースをポーリングする時間間隔。
障害がある場合のモニタ スレッド スリープ時間（秒）	［モニタ スレッド スリープ時間］と同じ。ただし、この値はデータベース モニタ スレッドが障害を検出したときに限り使用されます。障害が発生した場合に頻繁な間隔でポーリングを実行する必要があるので、この値は［モニタ スレッド スリープ時間］未満である*必要があります*。

フィールド	Description
クエリ詳細のログ	有効にした場合、サーバによって実行されたすべての Oracle、MS SQL、MySQL データベース クエリがログに記録されます。 デフォルトでは、このオプションは無効で、［トレース ログの有効化］の場合と同様にデバッグが必要なときに*限り*有効にする必要があります。
データベース接続のモニタ	このオプションが有効な場合、サーバはデータベース モニタ スレッドを作成します。 そうでない場合、データベース モニタリングは無効です。
プライマリに自動的に戻す	プライマリ データベースへの接続が失敗すると、サーバはバックアップ データベースを選択します。 このオプションが有効な場合、プライマリ データベースが稼働していると、サーバは自動的にプライマリ データベースに戻ります。

8. ［**保存**］をクリックして変更内容を保存します。
9. 更新したパラメータに応じて、サーバ インスタンスをリフレッシュするか再起動します。

   この方法の詳細については、「サーバ インスタンスのリフレッシュ」および「サーバ インスタンスの再起動」を参照してください。

サーバ インスタンスのシャットダウン

CA Risk Authentication サーバまたはケース管理キュー サーバ インスタンスをシャットダウンする方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにし、サブメニューの［CA Risk Authentication］タブが表示されていることを確認します。
3. ［**インスタンス設定**］セクションで、［**インスタンス管理**］リンクをクリックして、対応するページを表示します。
4. シャットダウンする CA Risk Authentication サーバ インスタンスまたはケース管理キュー サーバ インスタンスを選択します。
5. ［**シャットダウン**］をクリックして、選択したサーバ インスタンスをシャットダウンします。

注: シャットダウン リクエストが CA Risk Authentication サーバによって受信されると、進行中のトランザクションがすべて処理されてから、シャットダウン リクエストが処理されます。

サーバ インスタンスの再起動

以下のセクションでは、CA Risk Authentication サーバおよびケース管理キュー サーバ インスタンスを再起動するための手順について説明します。

Windows の場合

Windows 上のサーバ インスタンスを開始する方法

1. インスタンスが停止されているコンピュータにログインします。
2. デスクトップの［**スタート**］ボタンをクリックします。
3. ［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。
4. 以下を再起動します。
   - **CA Risk Authentication サーバ インスタンス**：リスト表示されたサービスから［**CA Risk Authentication Service**］をダブルクリックします。
   - **ケース管理キュー サーバ インスタンス**：リスト表示されたサービスから［**Case Management Queuing Service**］をダブルクリックします。
5. ［**開始**］をクリックすると、サービスが開始されます。

UNIX ベースのプラットフォームの場合

UNIX ベースのプラットフォーム上のサーバ インスタンスを開始する方法

1. インスタンスを開始する必要があるコンピュータにログインします。
2. 以下のディレクトリに移動します。
   `<install_location>/arcot/bin/`
3. 再起動するには、以下のコマンドを実行します。
   - **CA Risk Authentication サーバ インスタンスの場合**
     `./riskfortserver start`
   - **ケース管理キュー サーバ インスタンスの場合**
     `./casemanagementserver start`

第 5 章: SSL の環境設定

デフォルトでは、CA Risk Authentication コンポーネントは、コンポーネント同士での通信に TCP （Transmission Control Protocol）を使用します。 CA Advanced Authentication と CA Risk Authentication サーバ間および SDK と CA Risk Authentication サーバ間での安全な通信を確保するには、SSL （Secure Socket Layer）をサポートするように CA Risk Authentication ネイティブおよびサーバ管理プロトコルを設定します。SSL は、安全性の低いメディア上でアプリケーションどうしが安全に通信することを可能にします。

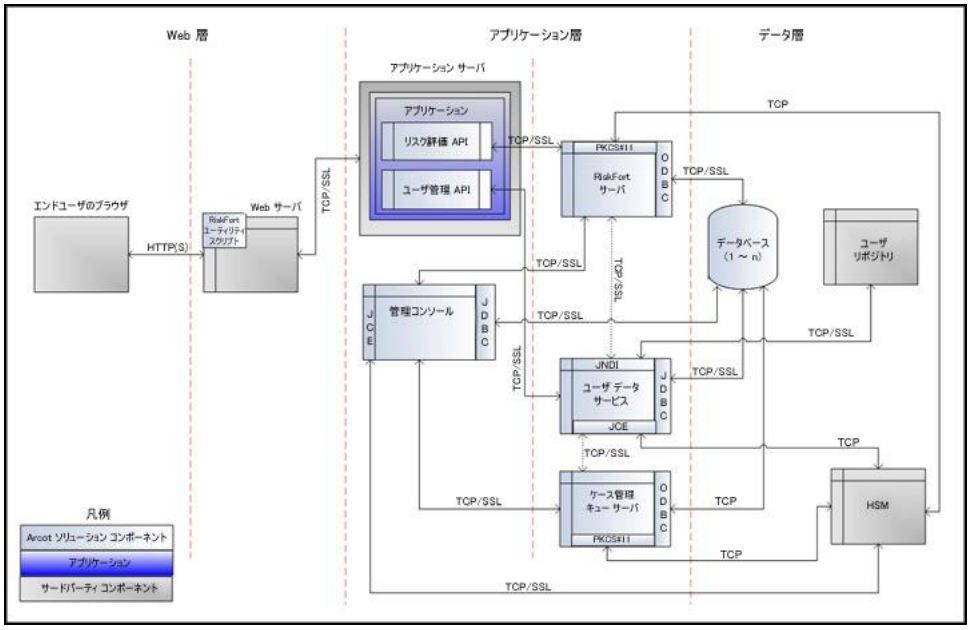
CA Risk Authentication のさまざまなコンポーネント間で SSL を設定するには、以下のような手順があります。

注: この順序に従って SSL を正常に設定する*必要があります*。 各手順を完了したら、接続が正常に設定されたかどうかテストします。

1. SSL 通信の準備
2. CA Risk Authentication サーバとユーザ データ サービスの間で SSL を有効にする
3. ケース管理キュー サーバとユーザ データ サービスの間で SSL を有効にする
4. CA Advanced Authentication と CA Risk Authentication サーバの間で SSL を有効にする
5. CA Advanced Authentication とケース管理キュー サーバの間で SSL を有効にする
6. Java SDK と CA Risk Authentication サーバの間で SSL を有効にする
7. リスク評価 Web サービスと CA Risk Authentication サーバの間で SSL 通信を有効にする
8. 管理 Web サービスと CA Risk Authentication サーバの間で SSL 通信を有効にする
9. CA Risk Authentication コンポーネントとデータベースの間の一方向 SSL を有効にする

CA Risk Authentication コンポーネントおよびその通信モード

以下の図は、CA Risk Authentication とそのコンポーネントの間でサポートされている通信モードを示しています。



この図に示されるように、コンポーネント間の通信のデフォルト モードは TCP で、トランザクション中に交換されるデータの整合性および機密性を確保するために、CA Risk Authentication サーバは以下のコンポーネントとの SSL 通信（双方向および一方向）をサポートします。

- ケース管理キュー サーバ
- CA Risk Authentication データベース
- ユーザ データ サービス
- CA Risk Authentication SDK （リスク評価）
- サンプル アプリケーション
- 評価コールアウト
- スコアリング コールアウト

RiskMinder は、コンポーネント間の一方向 SSL および双方向 SSL をサポートします。

SSL 通信の準備

CA Risk Authentication コンポーネント間の SSL 通信を有効にするには、まずサーバとクライアントの証明書を取得する必要があります。 これらの証明書は、以下のいずれかの方法を使用して取得できます。

- 認証機関（CA）からの証明書の直接取得（P. 86）
- ユーティリティを使用した証明書リクエストの生成（P. 101）

CA がユーザ用の証明書を生成すると（「認証機関（CA）からの証明書の直接取得」を参照）、その証明書と関連付けられた秘密キーも生成されます。 その結果、秘密キーはユーザ側で生成されるときほど安全ではない場合があります。 キーを「オフサイト」で生成しないようにするには、「ユーティリティを使用した証明書リクエストの生成」の手順に従う必要があります。

認証機関(CA)からの証明書の直接取得

このセクションで説明される手順は **Microsoft CA 2008** に固有です。 その他の CA を使用して証明書と秘密キーを生成する場合は、ベンダーのドキュメントを参照する必要があります。

CA によって発行される証明書を生成する方法

1. 任意の CA へのリンクにアクセスします。 Microsoft CA の場合は、以下のとおりです。

   http://<IP_Address_of_the_CA>/certsrv/

2. 証明書リクエストを作成し、サブミットするためのリンクに移動します。

   たとえば、**MSCA** を使用する場合、［**タスクの選択**］セクションで、［**証明書の要求**］オプション、［**証明書の要求の詳細設定**］オプション、［**この CA への要求を作成し送信する**］オプションの順にクリックします。

3. 表示される証明書リクエスト フォームで詳細を指定します。

   - 以下の表に示す証明書の識別情報。

証明書属性	**必要な情報**
共通名 （名前）	サーバの完全修飾ドメイン名（FQDN）。 **重要**: 共通名の入力を促すメッセージが表示されたら、SSL によって保護されるサーバの完全修飾ドメイン名（FQDN）を指定する*必要があります*。 たとえば、login.my-bank.com に対して発行された SSL 証明書は、online.my-partner.com に対して有効に*なりません*。SSL に対して使用される URL が login.my-bank.com である場合は、CSR でサブミットされた共通名が login.my-bank.com であることを確認します。
［Email Address］	組織内の担当者の電子メール ID。 **注**: 通常、これは、証明書管理者または IT 部門の管理者の電子メール アドレスです。

証明書属性	必要な情報
組織 （会社）	組織の名前。 **重要**: このエントリが短縮されていないことを確認します。 また、Inc.、Corp.、LLC などのサフィックスを指定していないことも確認する必要があります。
組織単位 （部門）	証明書を処理する組織の部門（たとえば IT）。
市区町村 （市区町村）	組織単位がある市区町村（たとえば、ブリズベーン）。
都道府県	組織単位がある都道府県（たとえば、クィーンズランド）。 **重要**: このエントリが短縮されていないことを確認します。
国 （地域）	組織の本部がある国の ISO コード（たとえば、AU）。

- 証明書の詳細。 これらの証明書の詳細を指定する際には、以下の表で指定されている詳細を考慮する必要があります。

証明書属性	必要な情報
証明書のタイプ	**サーバ認証証明書**： サーバ証明書を生成する場合 **クライアント認証証明書**： クライアント証明書を生成する場合
CSP	任意の CSP
キーの使用方法	交換
キー サイズ	バイト単位のキー サイズ。
キーのエクスポート可能性	■ キーをエクスポート可能としてマーク ■ キーをファイルにエクスポート ■ フル パス名（*.pvk）
リクエストの形式	PKCS#12 ファイル

1. ［**送信**］をクリックして証明書をリクエストします。
2. ［**この証明書のインストール**］をクリックしてブラウザ ストアに証明書をインストールします。

証明書のダウンロード

Microsoft CA 2008 を介してリクエストした証明書はブラウザ ストアにインストールされます。そのブラウザ ストアから証明書をダウンロードする必要があります。 証明書をダウンロードする必要がある形式は、暗号化モードによって異なります。

- ソフトウェア暗号化が使用される場合、証明書は PKCS#12 形式である必要があります。
- ハードウェア暗号化が使用される場合、証明書は PEM 形式である必要があります。

PKCS#12 形式の場合

Microsoft CA 2008 を使用して PKCS#12 ファイルに証明書と秘密キーをダウンロードする方法

1. Internet Explorer ウィンドウを開きます。
2. ［**ツール**］-［**インターネット オプション**］に移動します。

   ［インターネット オプション］ダイアログ ボックスが表示されます。
3. ［**コンテンツ**］タブをアクティブにし、［証明書］セクションで［**証明書**］をクリックします。

   ［証明書］ダイアログ ボックスが表示されます。
4. ダウンロードする証明書を選択し、［**エクスポート**］をクリックします。

   ［証明書のエクスポート］ウィザードが表示されます。
5. ウィザードの開始画面で［**次へ**］をクリックします。
6. ［**はい、秘密キーをエクスポートします**］オプションを選択し、［**次へ**］をクリックします。
7. ［**Personal Information Exchange - PKCS # 12 (.PFX)**］オプションが選択されていることを確認します。
8. ［**強力な保護を有効にする**］オプションを選択し、［**次へ**］をクリックします。
9. ［**パスワード**］フィールドと［**パスワードの確認入力**］フィールドに PKCS#12 （.PFX）ファイルのパスワードを入力し、［**次へ**］をクリックします。

10. ［**ファイル名**］に PKCS#12 （.PFX）ファイルのダウンロードに使用するファイル名を入力し、［**次へ**］をクリックします。
11. ［**完了**］をクリックして、ウィザードを終了します。

    これで証明書と秘密キーは指定された場所のシステムで利用できます。

PEM 形式の場合

ブラウザ証明書ストアから直接 .PEM 形式の証明書をエクスポートすることはできません。 したがって、まず .DER 形式で証明書をダウンロードし（Microsoft CA 2008 を使用）、以下のように .PEM 形式に変換する必要があります。

1. Internet Explorer ウィンドウを開きます。
2. ［**ツール**］-［**インターネット オプション**］に移動します。

   ［インターネット オプション］ダイアログ ボックスが表示されます。
3. ［**コンテンツ**］タブをアクティブにし、［証明書］セクションで［**証明書**］をクリックします。

   ［証明書］ダイアログ ボックスが表示されます。
4. ダウンロードする証明書を選択し、［**エクスポート**］をクリックします。

   ［証明書のエクスポート］ウィザードが表示されます。
5. ウィザードの開始画面で［**次へ**］をクリックします。
6. ［**いいえ、秘密キーをエクスポートしません**］オプションを選択し、［**次へ**］をクリックします。
7. ［**DER encoded binary X.509 (.CER)**］オプションが選択されていることを確認します。
8. ［**次へ**］をクリックします。
9. ［**ファイル名**］に証明書のダウンロードに使用するファイル名を入力し、［**次へ**］をクリックします。
10. ［**完了**］をクリックして、ウィザードを終了します。

    これで証明書は指定された場所のシステムで利用できます。
11. DER 形式を PEM 形式に変換します。

    証明書を DER 形式から PEM 形式に変換する場合、OpenSSL などのオープン ソース ツールを使用できます。OpenSSL ツールを使用して変換するには、以下のコマンドを使用します。

```
openssl x509 -inform der -in <certificate>.cer -out
<certificate>.pem
```

CA Advanced Authentication とケース管理キュー サーバの間で SSL を有効にする

このセクションでは、CA Advanced Authentication とケース管理キュー サーバの間の SSL 設定の手順について説明します。

- サーバ リフレッシュおよび再起動アクティビティの場合 (P. 90)
- ケース取得の場合 (P. 95)

サーバ リフレッシュおよび再起動アクティビティの場合

ケース管理キュー サーバは、ケース管理のキュー管理ポート（7780）を使用して CA Advanced Authentication からのサーバ管理アクティビティ（正常なシャットダウン、サーバ キャッシュ リフレッシュなど）を待ち受けます。

サーバ管理アクティビティ用に CA Advanced Authentication とケース管理キュー サーバの間で SSL を設定するには、SSL 用のサーバ管理ポート（7780）を設定し、［CA Risk Authentication 接続］ページで対応するサーバ ルート CA 証明書を提供する必要があります。 また、双方向 SSL が必要な場合、［CA Risk Authentication 接続］ページで **PKCS#12 内のクライアント証明書キー ペア** ファイルをアップロードし、このポートの［プロトコル設定］ページ上で適切なトラスト ストアを選択する必要があります。

以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL (P. 91)
- 双方向 SSL (P. 93)

一方向 SSL

サーバ管理アクティビティ用に CA Advanced Authentication とケース管理キュー サーバ間の一方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］サブタブがアクティブになっていることを確認します。
5. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
6. SSL 通信を設定する**サーバ インスタンス**を選択します。
7. ［**プロトコルのリスト**］セクションで、［**ケース管理のキュー管理**］リンクをクリックします。

   ケース管理のキュー管理プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、ケース管理キュー サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、ケース管理キュー サーバ秘密キーを選択します。
9. ［**保存**］ボタンをクリックします。
10. ケース管理キュー サーバを再起動します。

- **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

11. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
12. ［**ケース管理キュー サーバ接続**］セクションで、以下の操作を実行します。
    - ケース管理サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］がサーバ管理リクエストに対して開いているケース管理サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、ケース管理サーバ ルート証明書を選択します。
13. ［**保存**］ボタンをクリックします。
14. ケース管理キュー サーバを再起動します。
    - **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。
15. CA Advanced Authentication を再起動します。

双方向 SSL

サーバ管理アクティビティ用に CA Advanced Authentication とケース管理キュー サーバ間の双方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. **［サービスおよびサーバの設定］**タブをアクティブにします。
4. ［**CA Risk Authentication**］タブがアクティブであることを確認します。
5. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
6. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
7. **［保存］**ボタンをクリックします。
8. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
9. SSL 通信を設定する**サーバ インスタンス**を選択します。
10. ［**プロトコルのリスト**］セクションで、［**ケース管理のキュー管理**］リンクをクリックします。

    ケース管理のキュー管理プロトコルを設定するページが表示されます。
11. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。

- ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、ケース管理サーバ ルート証明書を選択します。
- （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、ケース管理サーバ秘密キーを選択します。
- 手順 6 で作成した**クライアント ストアを選択します**。

12. ［**保存**］ボタンをクリックします。
13. ケース管理キュー サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。
14. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
15. ［CA Risk Authentication 接続］ページで、以下の操作を実行します。
    - ケース管理サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］がサーバ管理リクエストに対して開いているケース管理サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、ケース管理サーバ ルート証明書を選択します。
    - ［**PKCS#12 内のクライアント証明書 - キーのペア**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
    - ［**クライアント PKCS#12 パスワード**］フィールドに PKCS#12 ファイルのパスワードを入力します。
16. ［**保存**］ボタンをクリックします。
17. ケース管理キュー サーバを再起動します。

- **Windows の場合：** ［スタート］ボタンをクリックし、［設定］-［コントロール パネル］-［管理ツール］-［サービス］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

18. CA Advanced Authentication を再起動します。
19. 以下の手順に従って、ケース管理サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotriskfortcasemgmtserverstartup.log ファイルを開きます。
    c. 以下の行を確認します。
    ```
    Started listener for [Case Management Admin] [7780] [SSL] [srvmgrwsprotocol]
    ```
    この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

ケース取得の場合

ケース管理キュー サーバは、ケース管理キュー サーバ ポート（7779）を使用して CA Advanced Authentication からの次のケースを取得するリクエストを待ち受けます。

CA Advanced Authentication とケース管理キュー サーバの間で SSL を設定するには、SSL 用のケース管理キュー サーバ ポート（7779）を設定し、［CA Risk Authentication 接続］ページで対応するサーバ ルート CA 証明書を提供する必要があります。 また、双方向 SSL が必要な場合、［CA Risk Authentication 接続］ページで **PKCS#12 内のクライアント証明書キー ペア** ファイルをアップロードし、このポートの［プロトコル設定］ページ上で適切なトラスト ストアを選択する必要があります。

以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL（P. 96）
- 双方向 SSL（P. 98）

一方向 SSL

キュー内の次のケースを表示するために CA Advanced Authentication とケース管理キュー サーバ間の一方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］サブタブがアクティブになっていることを確認します。
5. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
6. SSL 通信を設定する**サーバ インスタンス**を選択します。
7. ［**プロトコルのリスト**］セクションで、［**ケース管理キュー サーバ**］リンクをクリックします。

   ケース管理キュー サーバ プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
9. ［**保存**］ボタンをクリックします。
10. ケース管理キュー サーバを再起動します。

- **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

11. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
12. ［**ケース管理キュー サーバ接続**］セクションまでスクロールします。
13. ［**ケース管理キュー サーバ接続**］セクションで、以下の操作を実行します。
    - ケース管理サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］がコンソール リクエストに対して開いているケース管理サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、CA Risk Authentication ルート証明書を選択します。
14. ［**保存**］ボタンをクリックします。
15. ケース管理キュー サーバを再起動します。
    - **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。
16. CA Advanced Authentication を再起動します。

双方向 SSL

ケース アクティビティ用に CA Advanced Authentication とケース管理サーバ間の双方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］タブがアクティブであることを確認します。
5. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
6. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
7. ［**保存**］ボタンをクリックします。
8. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
9. SSL 通信を設定する**サーバ インスタンス**を選択します。
10. ［**プロトコルのリスト**］セクションで、［**ケース管理キュー サーバ**］リンクをクリックします。

    ケース管理キュー サーバ プロトコルを設定するページが表示されます。
11. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。

- ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
- （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
- 手順 6 で作成した**クライアント ストアを選択します**。

12. ［**保存**］ボタンをクリックします。
13. ケース管理キュー サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。
14. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
15. ［CA Risk Authentication 接続］ページの［**ケース管理キュー サーバ接続**］セクションで、以下の操作を実行します。
    - ケース管理サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**ポート**］がケース リクエストに対して開いているケース管理サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、ケース管理サーバ ルート証明書を選択します。
    - ［**PKCS#12 内のクライアント証明書 - キーのペア**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
    - ［**クライアント PKCS#12 パスワード**］フィールドに PKCS#12 ファイルのパスワードを入力します。
16. ［**保存**］ボタンをクリックします。
17. ケース管理キュー サーバを再起動します。

- **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**Arcot Case Management Queuing Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

18. CA Advanced Authentication を再起動します。
19. 以下の手順に従って、ケース管理サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。
    c. 以下の行を確認します。
    ```
    Started listener for [Case Management Server] [7779] [SSL]
    [RiskFortCaseManagement]
    ```
    この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

ユーティリティを使用した証明書リクエストの生成

ユーティリティまたはツールを使用して証明書を生成することもできます。 keytool ユーティリティ（JDK で使用可能）は以下の操作に使用されています。

1. キーストアを生成します。

   keytool は、*キーストア*と呼ばれるファイルにキーと証明書を格納します。キーストアは、クライアントまたはサーバの識別に使用される証明書のリポジトリです。 通常、キーストアは 1 つのクライアントまたは 1 つのサーバに固有です。デフォルト キーストア実装は、ファイルとしてキーストアを実装します。 これはパスワードを使用して秘密キーを保護します。キーストアは、keytool を実行するディレクトリで作成されます。

   以下のコマンドを使用して、キーストアを生成します。

   ```
   $%JAVA_HOME%/¥bin/¥keytool -genkey -keyalg RSA -alias
   <server/or/client> -keystore <keystore_name>.jks -storetype JKS
   -storepass <password> -keysize 1024 -validity
   <validity_period_in_days>
   ```

2. 証明書署名リクエスト（CSR）を生成します。

   CSR は、暗号化された識別テキスト（「認証機関（CA）からの証明書の直接取得」の 1 つ目の表を参照）で、証明書が使用されるシステム上で生成する必要があります。 秘密キーは通常 CSR を作成するのと同時に作成されます。

   以下のコマンドを使用して、CSR を生成します。

   ```
   $%JAVA_HOME%/¥bin/¥keytool -certreq -v -alias <server/or/client>
   -keystore <keystore_name>.jks -storepass <password> -file
   <server/or/client>certreq.csr
   ```

3. 前の手順で生成された CSR を CA にサブミットして証明書を生成します。

   a. 任意の CA へのリンクにアクセスします。

      たとえば、**MSCA** を使用する場合、リンクは以下のようになります。

      http://<IP_Address_of_the_CA>/certsrv/

   b. 証明書リクエストを作成し、サブミットするためのリンクに移動します。

たとえば、**MSCA** を使用する場合、［**タスクの選択**］セクションで、［**証明書の要求**］オプション、［**証明書の要求の詳細設定**］オプション、［**Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信する**］オプションの順にクリックします（または、証明書を更新する場合、base-64-encoded PKCS #7 ファイルを使用して更新リクエストをサブミットします）。 最後に、<*server/or/client*>clientcertreq.csr の内容をコピーして **Base-64-encoded certificate request** フィールドに貼り付け、［**提出**］をクリックします。

c. Base-64 エンコード形式で以下のファイルをダウンロードします。

- clientcert.cer としての署名された証明書
- clientcertchain.p7b としての完全な証明書チェーン
- clientcacert.cer としての CA 証明書

4. キーストアに証明書チェーンをインポートします。

以下のコマンドを使用します。

```
$%JAVA_HOME%/¥bin/¥keytool -import -keystore
<server/or/client>keystore.jks -storepass <password> -file
<server/or/client>certchain.p7b -alias <server/or/client>
```

5. 証明書またはキーストアを必要な形式に変換します。

- DER 形式からの場合
  - DER 形式を PEM 形式に変換するには、以下のコマンドを使用します。

```
openssl x509 -inform der -in <server/or/client>cert.cer -out
<server/or/client>cert.pem
```

  - DER 形式を PKCS#12 に変換するには、まず上記のコマンドを使用して DER を PEM に変換し、次に以下のコマンドを使用して PEM を PKCS#12 に変換します。

```
openssl pkcs12 -export -out <server/or/client>cert.pfx -inkey
privateKey.key -in <server/or/client>cert.cer -certfile
<server/or/client>cacert.cer
```

- P7B 形式からの場合
  - P7B 形式を PEM 形式に変換するには、以下のコマンドを使用します。

```
openssl pkcs7 -print_certs -in <server/or/client>cert.p7b -out
<server/or/client>cert.cer
```

  - P7B 形式を PKCS#12 に変換するには、まず上記のコマンドを使用して P7B を PEM に変換し、次に以下のコマンドを使用して PEM を PKCS#12 に変換します。

```
openssl pkcs12 -export -in <server/or/client>cert.cer -inkey
privateKey.key -out <server/or/client>cert.pfx -certfile
<server/or/client>cacert.cer
```

CA Risk Authentication サーバとユーザ データ サービスの間で SSL を有効にする

CA Risk Authentication サーバとユーザ データ サービス (UDS) の間で SSL を設定するには、CA Advanced Authentication の［**ユーザ データ サービス接続設定**］ページを使用して SSL 通信に必要な UDS サーバ証明書をアップロードする必要があります。 双方向 SSL の場合は、［**ユーザ データ サービス接続設定**］ページを使用して CA Risk Authentication サーバのクライアント証明書もアップロードする必要があります。 以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL (P. 104)
- 双方向 SSL (P. 105)

一方向 SSL

CA Risk Authentication サーバと UDS 間の一方向 SSL 通信を有効にする方法

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
3. MA （マスタ管理者）として CA Advanced Authentication にログインします。
4. ［**サービスおよびサーバの設定**］タブをアクティブにします。
5. ［**CA Advanced Authentication**］サブタブをアクティブにして［ユーザ データ サービス接続設定］ページを表示します。
6. ［**プロトコル**］リストから［**一方向 SSL**］を選択します。
7. ［**ポート**］の値をデフォルトの SSL ポートに設定します。
8. ［**サーバ ルート証明書**］フィールドの隣の**参照**ボタンをクリックし、UDS ルート証明書に移動して選択します。
9. ［**保存**］をクリックします。
10. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで *<install_location>*/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

双方向 SSL

CA Risk Authentication サーバとユーザ データ サービス（UDS）間の双方向 SSL を設定する方法

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
3. MA として CA Advanced Authentication にログインします。
4. ［**サービスおよびサーバの設定**］タブをアクティブにします。
5. ［**CA Advanced Authentication**］サブタブをアクティブにして［ユーザ データ サービス接続設定］ページを表示します。
6. ［**プロトコル**］リストから［**双方向 SSL**］を選択します。
7. ［**ポート**］の値をデフォルトの SSL ポートに設定します。
8. ［**サーバ ルート証明書**］フィールドの隣の**参照**ボタンをクリックし、UDS ルート証明書に移動して選択します。
9. ［**クライアント証明書**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication ルート証明書に移動して選択します。
10. ［**クライアント秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
11. ［**保存**］をクリックします。
12. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

ケース管理キューとユーザ データ サービスの間で SSL を有効にする

ケース管理キュー サーバとユーザ データ サービス（UDS）の間で SSL を設定するには、CA Advanced Authentication の［**ユーザ データ サービス接続設定**］ページを使用して SSL 通信に必要な UDS サーバ証明書をアップロードする必要があります。 双方向 SSL の場合は、［**ユーザ データ サービス接続設定**］ページを使用してケース管理キュー サーバのクライアント証明書もアップロードする必要があります。 以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL（P. 107）
- 双方向 SSL（P. 108）

一方向 SSL

ケース管理キュー サーバと UDS 間の一方向 SSL 通信を有効にする方法

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
3. MA （マスタ管理者）として CA Advanced Authentication にログインします。
4. ［**サービスおよびサーバの設定**］タブをアクティブにします。
5. ［**CA Advanced Authentication**］サブタブをアクティブにして［ユーザ データ サービス接続設定］ページを表示します。
6. ［**プロトコル**］リストから［**一方向 SSL**］を選択します。
7. ［**ポート**］の値をデフォルトの SSL ポートに設定します。
8. ［**サーバ ルート証明書**］フィールドの隣の**参照**ボタンをクリックし、UDS ルート証明書に移動して選択します。
9. ［**保存**］をクリックします。
10. ケース管理キュー サーバ インスタンスを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。表示されるサービスのリストから［**CA Risk Authentication Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

双方向 SSL

ケース管理キュー サーバとユーザ データ サービス（UDS）間の双方向 SSL を設定する方法

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
3. MA として CA Advanced Authentication にログインします。
4. ［**サービスおよびサーバの設定**］タブをアクティブにします。
5. ［**CA Advanced Authentication**］サブタブをアクティブにして［ユーザ データ サービス接続設定］ページを表示します。
6. ［**プロトコル**］リストから［**双方向 SSL**］を選択します。
7. ［**ポート**］の値をデフォルトの SSL ポートに設定します。
8. ［**サーバ ルート証明書**］フィールドの隣の**参照**ボタンをクリックし、UDS ルート証明書に移動して選択します。
9. ［**クライアント証明書**］フィールドの隣の**参照**ボタンをクリックし、ケース管理キュー サーバ ルート証明書に移動して選択します。
10. ［**クライアント秘密キー**］フィールドの隣の**参照**ボタンをクリックし、ケース管理キュー サーバ秘密キーを選択します。
11. ［**保存**］をクリックします。
12. ケース管理キュー サーバ インスタンスを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。表示されるサービスのリストから［**CA Risk Authentication Case Management Queuing Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./casemanagementserver start コマンドを指定します。

CA Advanced Authentication と CA Risk Authentication サーバの間で SSL を有効にする

このセクションでは、CA Advanced Authentication と CA Risk Authentication サーバの間の SSL 設定の手順について説明します。

- サーバ リフレッシュ、再起動、インスタンス管理、プロトコル管理アクティビティの場合（P. 109）
- ルール設定アクティビティの場合（P. 115）

サーバ リフレッシュ、再起動、インスタンス管理、プロトコル管理アクティビティの場合

CA Risk Authentication サーバは、正常なシャットダウン、サーバ キャッシュ リフレッシュ、インスタンス管理など、サーバ管理ポート（7980）を使用して CA Advanced Authentication からのサーバ管理アクティビティを待ち受けます。

サーバ管理アクティビティ用に CA Advanced Authentication と CA Risk Authentication サーバの間で SSL を設定するには、SSL 用のサーバ管理ポート（7980）を設定し、［CA Risk Authentication 接続］ページで対応するサーバ ルート CA 証明書を提供する必要があります。 また、双方向 SSL が必要な場合、［CA Risk Authentication 接続］ページで **PKCS#12 内のクライアント証明書キー ペア** ファイルをアップロードし、このポートの［プロトコル設定］ページ上で適切なトラスト ストアを選択する必要があります。

以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL（P. 110）
- 双方向 SSL（P. 112）

一方向 SSL

サーバ管理アクティビティ用に CA Advanced Authentication と CA Risk Authentication サーバ間の一方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］サブタブがアクティブになっていることを確認します。
5. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
6. SSL 通信を設定する**サーバ インスタンス**を選択します。
7. ［**プロトコルのリスト**］セクションで、［**サーバ管理**］リンクをクリックします。

   サーバ管理プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
9. ［**保存**］ボタンをクリックします。
10. CA Risk Authentication サーバを再起動します。

- **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

11. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
12. ［**CA Risk Authentication サーバ管理接続**］セクションで、以下の操作を実行します。
    - CA Risk Authentication サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］がサーバ管理リクエストに対して開いている CA Risk Authentication サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、CA Risk Authentication ルート証明書を選択します。
13. ［**保存**］ボタンをクリックします。
14. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。表示されるサービスのリストから［**Arcot CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
15. CA Advanced Authentication を再起動します。

双方向 SSL

サーバ管理アクティビティ用に CA Advanced Authentication と CA Risk Authentication サーバ間の双方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］タブがアクティブであることを確認します。
5. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
6. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
7. ［**保存**］ボタンをクリックします。
8. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
9. SSL 通信を設定する**サーバ インスタンス**を選択します。
10. ［**プロトコルのリスト**］セクションで、［**サーバ管理**］リンクをクリックします。

    サーバ管理プロトコルを設定するページが表示されます。
11. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。

- ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
- （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
- 手順 6 で作成した**クライアント ストアを選択します**。

12. ［**保存**］ボタンをクリックします。
13. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
14. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
15. ［CA Risk Authentication 接続］ページで、以下の操作を実行します。
    - CA Risk Authentication サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］がサーバ管理リクエストに対して開いている CA Risk Authentication サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、CA Risk Authentication ルート証明書を選択します。
    - ［**PKCS#12 内のクライアント証明書 - キーのペア**］フィールドの隣の**参照**ボタンをクリックし、CA Advanced Authentication が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
    - ［**クライアント PKCS#12 パスワード**］フィールドに PKCS#12 ファイルのパスワードを入力します。
16. ［**保存**］ボタンをクリックします。
17. CA Risk Authentication サーバを再起動します。

- **Windows の場合：** ［スタート］ボタンをクリックし、［設定］-［コントロール パネル］-［管理ツール］-［サービス］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

18. CA Advanced Authentication を再起動します。
19. 以下の手順に従って、CA Risk Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。
    c. 以下の行を確認します。
    ```
    Started listener for [Server Management] [7980] [SSL]
    [srvmgrwsprotocol]
    ```
    この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

ルール設定アクティビティの場合

CA Risk Authentication サーバは、管理 Web サービス ポート（7777）を使用して CA Advanced Authentication からのルール設定リクエスト（例外ユーザ リストへのユーザの追加、例外ユーザ リストからのユーザの削除、ユーザ プロファイルや接続情報の表示など）を待ち受けます。

ルール設定アクティビティ用に CA Advanced Authentication と CA Risk Authentication サーバの間で SSL を設定するには、SSL 用の管理 Web サービス ポート（7777）を設定し、［CA Risk Authentication 接続］ページで対応するサーバ ルート CA 証明書を提供する必要があります。また、双方向 SSL が必要な場合、［CA Risk Authentication 接続］ページで **PKCS#12 内のクライアント証明書キー ペア** ファイルをアップロードし、このポートの［プロトコル設定］ページ上で適切なトラスト ストアを選択する必要があります。

以下のサブセクションでは、以下のものを設定するための詳細な手順について説明します。

- 一方向 SSL（P. 116）
- 双方向 SSL

一方向 SSL

管理アクティビティ用に CA Advanced Authentication と CA Risk Authentication サーバ間の一方向 SSL 通信を設定する方法

1. Web ブラウザ ウィンドウで CA Advanced Authentication にアクセスします。
2. MA として CA Advanced Authentication にログインします。
3. ［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］サブタブがアクティブになっていることを確認します。
5. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
6. SSL 通信を設定する**サーバ インスタンス**を選択します。
7. ［**プロトコルのリスト**］セクションで、［**管理 Web サービス**］リンクをクリックします。

   管理 Web サービス プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
9. ［**保存**］ボタンをクリックします。
10. CA Risk Authentication サーバを再起動します。

- **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

11. ［**システム設定**］で、［**CA Risk Authentication 接続**］リンクをクリックして、［CA Risk Authentication 接続］ページを表示します。
12. ［**CA Risk Authentication 管理接続**］セクションまでスクロールします。
13. ［**CA Risk Authentication 管理接続**］セクションで、以下の操作を実行します。
    - CA Risk Authentication サーバの IP アドレスまたはホスト名が［**サーバ**］フィールドで正しく設定されていることを確認します。
    - ［**サーバ管理ポート**］が管理 Web サービス リクエストに対して開いている CA Risk Authentication サーバ ポートを指すように設定されていることも確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - ［**サーバ CA ルート証明書**］フィールドの隣の**参照**ボタンをクリックして、CA Risk Authentication ルート証明書を選択します。
14. ［**保存**］ボタンをクリックします。
15. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
16. CA Advanced Authentication を再起動します。

双方向 SSL

リスク評価 SDK と CA Risk Authentication サーバの間で双方向 SSL を設定するには、まず CA Risk Authentication によって信頼された CA のルート証明書をアップロードし、次に CA Advanced Authentication を使用して CA Risk Authentication **ネイティブ（SSL）**プロトコルを設定し、最後に riskfort.risk-evaluation.properties ファイルを設定する必要があります。

Java SDK と CA Risk Authentication サーバ間の双方向 SSL を設定する方法

1. SSL 通信用に Java SDK が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. マスタ管理者アカウントを使用して、CA Advanced Authentication にログインします。
3. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにします。
4. ［**CA Risk Authentication**］タブがアクティブであることを確認します。
5. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
6. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
7. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、Java SDK が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
8. ［**保存**］ボタンをクリックします。
9. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
10. SSL を設定する**サーバ インスタンス**を選択します。
11. ［**プロトコルのリスト**］セクションで、［**ネイティブ（SSL）**］プロトコル リンクをクリックして、プロトコルを設定するページを表示します。

12. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
    - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
    - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
    - 手順 7 で作成した**クライアント ストア**を選択します。
13. ［**保存**］ボタンをクリックします。
14. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
15. 以下の場所に移動します。
    - Windows の場合：
      `<install_location>¥Arcot Systems¥sdk¥java¥properties¥`
    - UNIX ベースのプラットフォームの場合
      `<install_location>/arcot/sdk/java/properties/`
16. 任意のエディタ ウィンドウで riskfort.risk-evaluation.properties ファイルを開きます。

    注: riskfort.risk-evaluation.properties ファイルの詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の付録「設定ファイルおよびオプション」を参照してください。

a. 以下のパラメータを設定します。

- TRANSPORT_TYPE= SSL（デフォルトで、このパラメータは TCP に設定されます）。
- CA_CERT_FILE= <*absolute_path_to_Server_root_certificate_in_PEM_format*>

たとえば、以下のいずれかのように指定できます。

- CA_CERT_FILE=<*install_location*>/certs/<ca_cert>.pem
- CA_CERT_FILE=<*install_location*>¥¥certs¥¥<ca_cert>.pem

たとえば、次のように指定できます： CA_CERT_FILE= <*install_location*>/certs/<ca_cert>.pem.

重要: 絶対パスを指定する際、必ず ¥ の代わりに ¥¥ または / を使用してください。 これは、Windows でパスの指定に使用される従来の ¥ を使用すると変更が機能しない場合があるからです。

b. 変更を保存して、ファイルを閉じます。

17. Java SDK が展開されているアプリケーション サーバを再起動します。
18. 以下の手順に従って、CA Risk Authentication サーバで SSL 通信が有効になっていることを確認します。

a. 以下の場所に移動します。

b. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。

c. 以下の行を確認します。

```
Started listener for [RiskFort Native (SSL)] [7681] [SSL]
[RiskFort]
```

この行があれば、双方向 SSL は正常に設定されています。

d. ファイルを閉じます。

Java SDK と CA Risk Authentication サーバの間で SSL を有効にする

SSL 通信用の CA Risk Authentication Java SDK を有効にするには、SSL 通信用の SDK にアクセスするクライアントをまず設定し、次に CA Advanced Authentication を使用して**ネイティブ（SSL）**プロトコルを設定する必要があります。

- 一方向 SSL（P. 122）
- 双方向 SSL

一方向 SSL

リスク評価 SDK と CA Risk Authentication サーバの間で一方向 SSL を設定するには、まず CA Advanced Authentication を使用して CA Risk Authentication **ネイティブ（SSL）**プロトコルを設定し、次に、riskfort.risk-evaluation.properties ファイルを設定する必要があります。

Java SDK と CA Risk Authentication サーバ間の一方向 SSL を設定する方法

1. 必ず MA としてログインしてください。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにします。
3. ［**CA Risk Authentication**］タブがアクティブであることを確認します。
4. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
5. SSL を設定する**サーバ インスタンス**を選択します。
6. ［**プロトコルのリスト**］セクションで、［**ネイティブ（SSL）**］プロトコル リンクをクリックして、プロトコルを設定するページを表示します。
7. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
8. ［**保存**］ボタンをクリックします。
9. CA Risk Authentication サーバを再起動します。

- **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

10. 以下の場所に移動します。
    - Windows の場合：
      <*install_location*>¥Arcot Systems¥sdk¥java¥**properties**¥
    - UNIX ベースのプラットフォームの場合
      <*install_location*>/arcot/sdk/java/**properties**/
11. 任意のエディタ ウィンドウで riskfort.risk-evaluation.properties ファイルを開きます。

    注: riskfort.risk-evaluation.properties ファイルの詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の付録「設定ファイルおよびオプション」を参照してください。

    a. 以下のパラメータを設定します。
       - TRANSPORT_TYPE= SSL（デフォルトで、このパラメータは TCP に設定されます）。
       - CA_CERT_FILE= <*absolute_path_to_Server_root_certificate_in_PEM_format*>

       たとえば、以下のいずれかのように指定できます。
       - CA_CERT_FILE=<*install_location*>/certs/<ca_cert>.pem
       - CA_CERT_FILE=<*install_location*>¥¥certs¥¥<ca_cert>.pem

       たとえば、次のように指定できます： CA_CERT_FILE= <*install_location*>/certs/<ca_cert>.pem.

       重要: 絶対パスを指定する際、必ず ¥ の代わりに ¥¥ または / を使用してください。 これは、Windows でパスの指定に使用される従来の ¥ を使用すると変更が機能しない場合があるからです。

    b. 変更を保存して、ファイルを閉じます。
12. Java SDK が展開されているアプリケーション サーバを再起動します。

双方向 SSL

リスク評価 SDK と RiskMinder サーバの間で双方向 SSL を設定するには、まず Risk Authentication によって信頼された CA のルート証明書をアップロードし、次に管理コンソールを使用して Risk Authentication ネイティブ（SSL）プロトコルを設定し、最後に riskfort.risk-evaluation.properties ファイルを設定する必要があります。

Java SDK と CA Risk Authentication サーバ間の双方向 SSL を設定する方法

1. SSL 通信用に Java SDK が展開されているアプリケーション サーバを有効にします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. マスタ管理者アカウントを使用して、CA Advanced Authentication にログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをアクティブにします。
4. ［リスク ベース認証］タブがアクティブであることを確認します。
5. ［インスタンス設定］セクションで、［プロトコル設定］リンクをクリックして、［プロトコル設定］ページを表示します。
6. ［システム設定］で、［トラステッド認証機関］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
7. このページで以下の情報を設定します。
   - ［名前］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［ルート CA］フィールドの隣の参照ボタンをクリックし、Java SDK が展開されているアプリケーション サーバのルート証明書に移動し、選択します。
   - ［保存］ボタンをクリックします。
8. ［インスタンス設定］セクションで、［プロトコル設定］リンクをクリックして、［プロトコル設定］ページを表示します。
9. SSL を設定するサーバ インスタンスを選択します。
10. ［プロトコルのリスト］セクションで、［ネイティブ（SSL）］プロトコル リンクをクリックして、プロトコルを設定するページを表示します。

11. 以下のフィールドを設定します。
    a. ［プロトコル ステータス］が［有効］であることを確認します。
    b. そうでない場合は、［プロトコル ステータスの変更］オプションを選択し、［アクション］リストから［有効化］を選択します。
    c. ［ポート］が正しい SSL ポート値に設定されていることを確認します。
    d. ［トランスポート］リストから［SSL］を選択します。
    e. HSM に SSL キーを格納する場合は、［HSM 内のキー］オプションを選択します。
    f. ［サーバ証明書チェーン］フィールドの隣の参照ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
    g. （［HSM 内のキー］オプションを選択しなかった場合のみ）［サーバ秘密キー］フィールドの隣の参照ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
12. 手順 7 で作成したクライアント ストアを選択します。
13. ［保存］ボタンをクリックします。
14. CA Risk Authentication サーバを再起動します。

    Windows の場合： ［スタート］ボタンをクリックし、［設定］-［コントロール パネル］-［管理ツール］-［サービス］に移動します。 表示されるサービスのリストから［Risk Authentication Service］をダブルクリックします。

    UNIX プラットフォームの場合： コンソール ウィンドウで <install_location>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
15. 以下の場所に移動します。

    Windows の場合：

    <install_location>¥Arcot Systems¥sdk¥java¥properties¥

    UNIX ベースのプラットフォームの場合

    <install_location>/arcot/sdk/java/properties/
16. 任意のエディタ ウィンドウで Risk Authentication.risk-evaluation.properties ファイルを開きます。

    注: riskfort.risk-evaluation.properties ファイルの詳細については、「CA Risk Authentication インストールおよび展開ガイド」の付録「設定ファイルおよびオプション」を参照してください。

17. 以下のパラメータを設定します。
    - TRANSPORT_TYPE= SSL （デフォルトで、このパラメータは TCP に設定されます）。
    - CA_CERT_FILE= <absolute_path_to_Server_root_certificate_in_PEM_format>

      たとえば、以下のいずれかのように指定できます。
    - CA_CERT_FILE=<install_location>/certs/<ca_cert>.pem
    - CA_CERT_FILE=<install_location>¥¥certs¥¥<ca_cert>.pem

      たとえば、次のように指定できます： CA_CERT_FILE= <install_location>/certs/<ca_cert>.pem.

      重要: 絶対パスを指定する際、必ず ¥ の代わりに ¥¥ または / を使用してください。 これは、Windows でパスの指定に使用される従来の ¥ を使用すると変更が機能しない場合があるからです。
18. 変更を保存して、ファイルを閉じます。
19. Java SDK が展開されているアプリケーション サーバを再起動します。
20. 以下の手順に従って、CA Risk Authentication サーバで SSL 通信が有効になっていることを確認します。
21. 以下の場所に移動します。
    a. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。
    b. 以下の行を確認します。

       Started listener for [Risk Authentication Native (SSL)] [7681] [SSL] [Risk Authentication]
    c. この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

新規トピック（255）

SSL 通信用の CA Risk Authentication Web サービスを有効にするには、SSL 通信用の Web サービスにアクセスするクライアントをまず設定し、次に CA Advanced Authentication を使用してトランザクション Web サービス プロトコルを設定する必要があります。

- 一方向 SSL（P. 128）
- 双方向 SSL（P. 130）

一方向 SSL

リスク評価 Web サービスと CA Risk Authentication サーバ間の一方向 SSL を設定する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サブメニュー内の［**CA Risk Authentication**］タブがアクティブであることを確認します。
4. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
5. SSL 通信を設定する**サーバ インスタンス**を選択します。
6. ［**プロトコルのリスト**］セクションで、［**トランザクション Web サービス**］リンクをクリックします。

   トランザクション Web サービス プロトコルを設定するページが表示されます。
7. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - (［**HSM 内のキー**］オプションを選択しなかった場合のみ) ［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
8. ［**保存**］ボタンをクリックします。
9. CA Risk Authentication サーバを再起動します。

- **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

双方向 SSL

リスク評価 Web サービスと CA Risk Authentication サーバ間の双方向 SSL 通信モードを有効にする方法

1. MA として CA Advanced Authentication にログインします。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サブメニュー内の［**CA Risk Authentication**］タブがアクティブであることを確認します。
4. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
5. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、Web サービス クライアントが展開されているアプリケーション サーバのルート証明書に移動し、選択します。
6. ［**保存**］ボタンをクリックします。
7. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
8. SSL 通信を設定する**サーバ インスタンス**を選択します。
9. ［**プロトコルのリスト**］セクションで、［**トランザクション Web サービス**］リンクをクリックします。

   トランザクション Web サービス プロトコルを設定するページが表示されます。
10. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。

- ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
- （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
- 手順 5 で作成した**クライアント ストア**を選択します。

11. ［**保存**］ボタンをクリックします。
12. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで *<install_location>*/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
13. 以下の手順に従って、CA Risk Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。
    c. 以下の行を確認します。
    ```
    Started listener for [RiskFort Trans WS] [7778] [SSL]
    [transwsprotocol]
    ```
    この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

リスク評価 Web サービスと CA Risk Authentication サーバ間の双方向 SSL 通信モードを有効にする方法

SSL 通信用の管理 Web サービスを有効にするには、SSL 通信用の Web サービスにアクセスするクライアントをまず設定し、次に CA Advanced Authentication を使用して Administration Web Service プロトコルを設定する必要があります。

- 一方向 SSL（P. 132）
- 双方向 SSL（P. 134）

一方向 SSL

管理 Web サービスと CA Risk Authentication サーバ間の一方向 SSL を設定する方法

1. 必ず MA としてログインしてください。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サブメニュー内の［CA Risk Authentication］タブがアクティブであることを確認します。
4. ［**インスタンス設定**］セクションで、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
5. SSL 通信を設定する**サーバ インスタンス**を選択します。
6. ［**プロトコルのリスト**］セクションで、［**管理 Web サービス**］リンクをクリックします。

   管理 Web サービス プロトコルを設定するページが表示されます。
7. 以下のフィールドを設定します。
   - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

     そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
   - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
   - ［**トランスポート**］リストから［**SSL**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。
   - ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
   - （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
8. ［**保存**］ボタンをクリックします。
9. CA Risk Authentication サーバを再起動します。
   - **Windows の場合：**［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。

- **UNIX プラットフォームの場合：** コンソール ウィンドウで <*install_location*>/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。

双方向 SSL

管理 Web サービスと CA Risk Authentication サーバ間の双方向 SSL 通信モードを有効にする方法

1. MA として CA Advanced Authentication にログインします。
2. メイン メニューの［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サブメニュー内の［**CA Risk Authentication**］タブがアクティブであることを確認します。
4. ［**システム設定**］で、［**トラステッド認証機関**］リンクをクリックして、［CA Risk Authentication サーバ トラステッド認証機関］ページを表示します。
5. このページで以下の情報を設定します。
   - ［**名前**］フィールドに、SSL トラスト ストアの名前を入力します。
   - 最初の［**ルート CA**］フィールドの隣の**参照**ボタンをクリックし、Web サービス クライアントが展開されているアプリケーション サーバのルート証明書に移動し、選択します。
6. ［**保存**］ボタンをクリックします。
7. ［**インスタンス設定**］で、［**プロトコル設定**］リンクをクリックして、［プロトコル設定］ページを表示します。
8. SSL 通信を設定する**サーバ インスタンス**を選択します。
9. ［**プロトコルのリスト**］セクションで、［**管理 Web サービス**］リンクをクリックします。

   管理 Web サービス プロトコルを設定するページが表示されます。
10. 以下のフィールドを設定します。
    - ［**プロトコル ステータス**］が［**有効**］であることを確認します。

      そうでない場合は、［**プロトコル ステータスの変更**］オプションを選択し、［**アクション**］リストから［**有効化**］を選択します。
    - ［**ポート**］が正しい SSL ポート値に設定されていることを確認します。
    - ［**トランスポート**］リストから［**SSL**］を選択します。
    - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］オプションを選択します。

- ［**サーバ証明書チェーン**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ ルート証明書を選択します。
- （［**HSM 内のキー**］オプションを選択しなかった場合のみ）［**サーバ秘密キー**］フィールドの隣の**参照**ボタンをクリックし、CA Risk Authentication サーバ秘密キーを選択します。
- 手順 5 で作成した**クライアント ストア**を選択します。

11. ［**保存**］ボタンをクリックします。
12. CA Risk Authentication サーバを再起動します。
    - **Windows の場合：** ［**スタート**］ボタンをクリックし、［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。 表示されるサービスのリストから［**CA Risk Authentication Service**］をダブルクリックします。
    - **UNIX プラットフォームの場合：** コンソール ウィンドウで *<install_location>*/arcot/bin/ に移動し、./riskfortserver start コマンドを指定します。
13. 以下の手順に従って、CA Risk Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotriskfortstartup.log ファイルを開きます。
    c. 以下の行を確認します。
    ```
    Started listener for [RiskFort Admin WS] [7777] [SSL]
    [aradminwsprotocol]
    ```
    この行があれば、双方向 SSL は正常に設定されています。
    d. ファイルを閉じます。

CA Risk Authentication コンポーネントとデータベースの間の一方向 SSL を有効にする

このセクションでは、CA Risk Authentication コンポーネントと CA Risk Authentication データベースの間の一方向 SSL 通信を設定する手順について説明します。 このセクションは以下のトピックで構成されます。

- CA Risk Authentication サーバとデータベース間（P. 136）
- CA Advanced Authentication とデータベース間（P. 138）
- UDS とデータベース間（P. 138）

CA Risk Authentication サーバとデータベース間

CA Risk Authentication は、DataDirect ドライバを使用してデータベースに接続します。 このセクションでは、CA Risk Authentication サーバ インスタンスと Oracle データベースの間の一方向および双方向の SSL を設定する手順について説明します。

- Windows の場合
- UNIX ベースのプラットフォームの場合

Windows の場合

CA Risk Authentication サーバと Oracle データベースの間の一方向 SSL を有効にする方法

1. CA Risk Authentication サーバをインストールしたシステムで、［**コントロール パネル**］を開き、［**管理ツール**］-［**データ ソース（ODBC）**］-［**システム DSN**］に移動します。
2. CA Risk Authentication のインストール中に指定したデータ ソースを選択し、［**構成**］をクリックします。

   ［ODBC Oracle Wire Protocol Driver Setup］ダイアログ ボックスが表示されます。
3. ［**Encryption**］セクションで、［**Encryption Method**］リストから［**1-SSL Auto**］を選択します。
4. ［**Truststore**］を CA Risk Authentication によって信頼される有効な認証機関（CA）のリストが含まれるトラスト ストア ファイルの場所に設定します。
5. ［**Truststore Password**］フィールドでトラスト ストアのパスワードを指定します。
6. ［**Host Name in Certificate**］フィールドをデータベース サーバがインストールされているシステムのホスト名に設定します。

   このパラメータについては、データベース ベンダーのドキュメントを参照してください。
7. ［**OK**］をクリックして設定を保存します。

UNIX ベースのプラットフォームの場合

UNIX プラットフォーム上で CA Risk Authentication とデータベースの間の SSL を有効にするには、必要な DataDirect ドライバ情報で odbc.ini ファイルを更新する必要があります。 この odbc.ini ファイルを設定する方法

1. 以下の場所に移動します。
   `<install_location>/arcot/odbc32v60wf`
2. 任意のファイル エディタで odbc.ini ファイルを開きます。
3. 使用しているデータベースに対応する［*<Database_name>* Wire Protocol］セクションで、以下の表に示す SSL 接続に必要なパラメータを編集します。

パラメータ	Description
EncryptionMethod	ドライバが、ドライバとデータベース サーバ間で送信されるデータを暗号化するために使用する方法を指定します。 このパラメータを 1 に設定すると、SSL を使用してデータが暗号化されます。
Truststore	トラスト ストア ファイルの場所を指定します。この場所には、SSL サーバ認証用にクライアント マシンによって信頼されている有効な認証機関（CA）のリストが含まれています。
TrustStorePassword	トラスト ストア ストアへのアクセスに必要なパスワードを指定します。
ValidateServerCertificate	サーバのセキュリティ証明書を SSL 認証ハンドシェイクの一部として検証します。 このパラメータを 1 に設定すると、 データベース サーバによって送信される証明書が検証されます。

4. odbc.ini ファイルを保存して閉じます。

CA Advanced Authentication とデータベース間

CA Advanced Authentication は、Java Database Connectivity （JDBC）を使用して、データベースに接続します。 CA Advanced Authentication とデータベース間の SSL を有効にする方法

1. CA Advanced Authentication が SSL 用に展開されているアプリケーション サーバを設定します。
2. arcotcommon.ini ファイル内の TrustStorePath.*N* および HostNameInCertificate.*N* パラメータを設定します。

   注: arcotcommon.ini パラメータの詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の「設定ファイルおよびオプション」を参照してください。

UDS とデータベース間

UDS はデータベースに接続するために JDBC も使用します。 UDS とデータベース間の SSL を有効にする方法

1. UDS が SSL 用に展開されているアプリケーション サーバを設定します。
2. arcotcommon.ini ファイル内の TrustStorePath.*N* および HostNameInCertificate.*N* パラメータを設定します。

   注: arcotcommon.ini パラメータの詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の「設定ファイルおよびオプション」を参照してください。

第 6 章: CA Risk Authentication ルールの基礎知識

重要: このセクションで説明する概念に関連するほとんどのタスクを実行できるのは、**グローバル管理者**および**組織管理者**のみですが、このセクションは、CA Risk Authentication が使用するルールの基本事項を理解したい人に役立ちます。

CA Risk Authentication では、ルールを使用して各トランザクションに関連付けられたリスクを評価します。 これらのルールは、以下のカテゴリに大きく分類することができます。

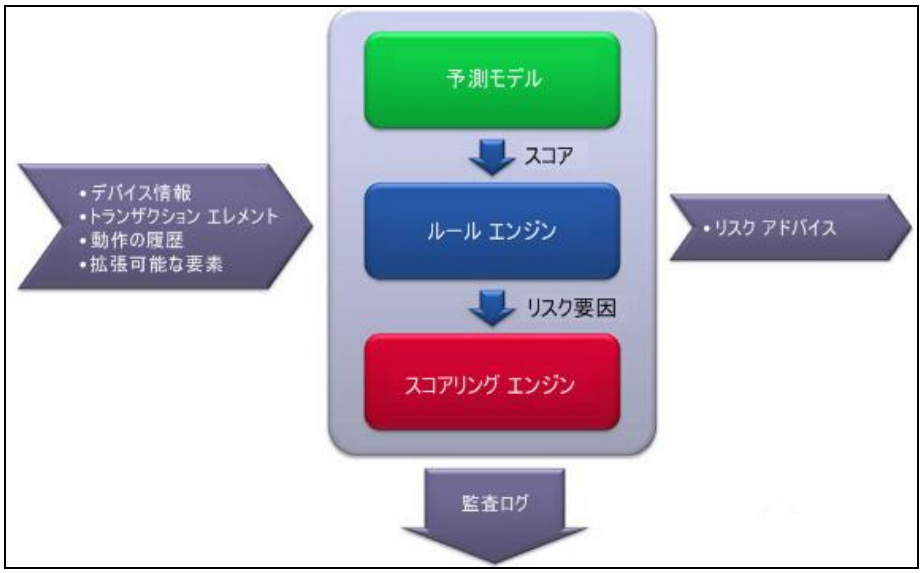
- 評価ルール
- スコアリング エンジン

ルールが属するカテゴリに関係なく、CA Risk Authentication のすべてのルールには以下の 3 つの特性があり、ルールがどのように処理されるかを制御しています。

- ルール セット： 各ルールはルール セットに属する*必要があります*。ルール セットを選択すると、ルールで使用可能なオプションが決まります。 ルール セットの操作の詳細については、「ルール セットの作成」を参照してください。
- ルール実装（グローバル レベルまたは組織レベル）： これは、ルールがグローバル レベル（テンプレートとして組織で利用可能）、または個別の組織のレベルで適用可能かどうかを指定します。

  グローバル レベルおよび組織レベルでのルールの実装については、「グローバル設定の管理」および「組織固有の CA Risk Authentication の設定の管理」を参照してください。
- ルール タイプ: これは、ルールの機能およびスコープを指定し、「ルール ビルダを使用して追加された新規ルール」と密接に関連しています。

以下の図は、CA Risk Authentication ルールとそのスコアリングの順序の概略を示しています。



ルールは以下の段階で実行されます。

実行段階

CA Risk Authentication サーバは、アクティブなルール セット内のすべてのルールの最初の解析を実行します。 この段階で、サーバは以下を実行します。

1. 実行優先度の順序でリスト内のルールをすべて実行します。

   この実行優先度は内部用で、サーバによって定義されます。

2. 実行する各ルールの個別のリスク スコアおよびアドバイスを生成します。

スコアリング段階

CA Risk Authentication サーバはルールの 2 番目の解析を実行します。 この段階で、サーバは以下を実行します。

1. 最初の解析の各ルールの結果を使用し、スコアリング優先度に基づいてルール セット内のルールを解析します。

   スコアリング優先度は、GA （グローバル管理者）が CA Advanced Authentication を使用して設定します。

2. 最初に一致したルールでスコアリングを停止します。
3. 最終結果として一致したルールのスコアおよびアドバイスを返します。

注: 最初のルールが一致したタイミングによっては、2 番目の解析が完全に実行されない場合があります。

評価ルール

評価ルールとはそれぞれ事前設定済みのロジックであり、ブール値を返します。 アプリケーションからリスク評価のリクエストがあった場合、このロジックはリクエストの入力トランザクション データに適用されます。ルールが一致した場合、ルールはそれぞれ TRUE を返し、一致しなかった場合は FALSE を返します。

重要: スコアリングの際、評価ルールは一致が検出されるまで優先度に従ってスコアリングされます。

CA Risk Authentication では以下のタイプの評価ルールを提供しています。

- 既定のルール
- ルール ビルダを使用して追加された新規ルール
- 評価コールアウト

既定ルール

これは*終端ルール*です。 つまり、スコアリングの際に任意の評価ルールに一致した（TRUE が返された）場合、リスク エンジンはこのカテゴリの以降のルールに対するスコアリングを中止し、一致したルールに対応するリスク スコアを生成します。

既定のルールは以下のように分類できます。

- 設定可能なルール
- 設定不能なルール

設定可能なルール

以下の表に、CA Risk Authentication をインストールするとデフォルトでインストールおよび展開される既定のルールを示します。

ルール名 （表示名）	Rule Mnemonic （短縮名）	Rule Description
Exception User Check	EXCEPTION	組織では、指定された期間にリスク評価から一時的にユーザを除外することを選択する場合があります。 たとえば、あるユーザが拒否国に移動する必要があったとします。 このようなユーザは*例外ユーザ リスト*に追加され、*例外ユーザ*として参照されます。 例外ユーザ リストで見つかった場合、デフォルトでは、CA Risk Authentication は例外ユーザから発生したトランザクションに対して低いスコアと ALLOW アドバイスを返します。
Untrusted IP Check	UNTRUSTEDIP	詳細については、「信頼できない IP アドレスの設定 (P. 223)」を参照してください。
Negative Country Check	NEGATIVECOUNTRY	詳細については、「拒否国リストの設定 (P. 221)」を参照してください。
Trusted IP/Aggregator Check	TRUSTEDIP	詳細については、「トラステッド IP アドレスの設定 (P. 225)」および「トラステッド アグリゲータの設定 (P. 228)」を参照してください。
Device MFP Not Match	MFPMISMATCH	入力された署名と対応する格納済み署名の一致率が指定された[シグネチャ一致しきい値]と[逆引きしきい値]に対して LESSER_OR_EQUAL であるかどうかを確認します。
User Velocity Check	USERVELOCITY	詳細については、「ユーザ頻度の設定 (P. 212)」を参照してください。
Device Velocity Check	DEVICEVELOCITY	詳細については、「デバイス頻度の設定 (P. 214)」を参照してください。
ゾーン ホッピング チェック	ZONEHOPPING	詳細については、「ゾーン ホッピングの設定 (P. 216)」を参照してください。

設定不能なルール

前述の設定可能なルールに加えて、CA Risk Authentication は以下の設定不能なルールも提供します。

- **Unknown User（UNKNOWNUSER）**：ユーザが CA Risk Authentication データベースに存在しない場合、CA Risk Authentication は ALERT を返します。アプリケーションでは、CA Risk Authentication API を呼び出して CA Risk Authentication にユーザを作成するか、または適切なアクションを取ることができます。
- **Unknown DeviceID （UNKNOWNDEVICEID）** ：（トランザクションが評価されている）デバイスが CA Risk Authentication データベースに存在するかどうかを確認します。 この情報はマシンのフィンガープリントとの照合に使用されます。
- **User Not Associated with DeviceID （USERDEVICENOTASSOCIATED）** ：対応するユーザとデバイスの関連付けが存在するかどうかを確認します。

ルール ビルダを使用して追加された新規ルール

CA Risk Authentication の既定ルールは汎用的であり、すべてに適用可能なルールに基づいてリスクを評価するために設定されます。 CA Risk Authentication がデフォルトで提供しているルールと大きく異なるカスタム ルール、または業界固有のルールが必要な場合は、*ルール ビルダ*を使用して独自のルールを展開する必要があります。

既定のルールとは異なり、これらのルールはインストールはされていますが、自動的に展開されません。

ルール ビルダ ウィザードを使用した新規ルールの追加の詳細については、「新規ルールの追加 (P. 176)」を参照してください。

評価コールアウト

ビジネス要件に基づいて、独自のカスタム評価ルールを作成することもできます。このルールは、CA Risk Authentication サーバの外部のアプリケーション側で実行されます。

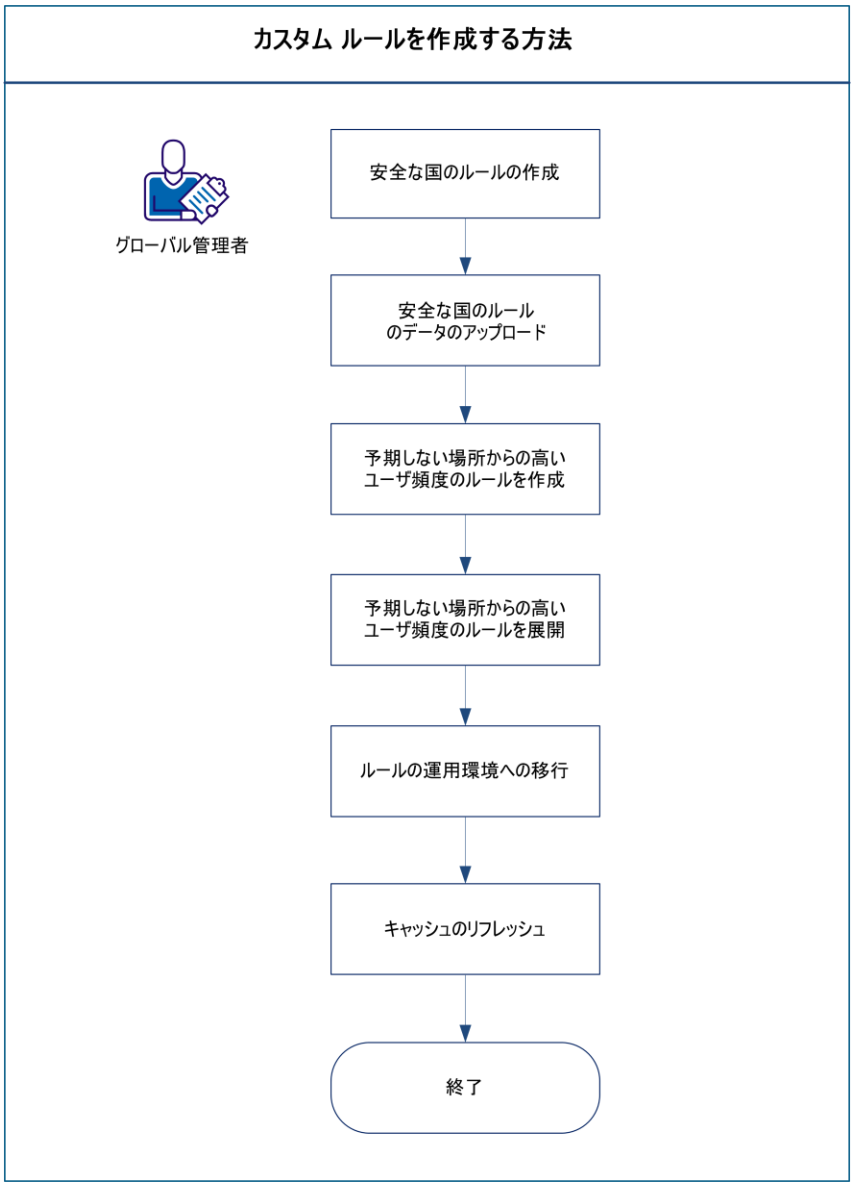
既定のルールおよびユーザの新しいルールがすべて実行された*後*、CA Risk Authentication はこのルールを実行します。 このコールアウトは、以前のすべてのルールの結果と追加入力を入力として受け入れ、レスポンス（SUCCESS/FAILURE）、*修飾文字列*（スコアリング コールアウトによって使用される追加情報）、および*注釈文字列*（コールアウトの実装モジュールによって CA Risk Authentication サーバに返された理由または説明）を返します。

評価コールアウトの操作の詳細については、「コールアウトの設定」を参照してください。

第 7 章: カスタム ルールを構築する方法

このシナリオは、グローバル管理者が通常以外の場所からのユーザ頻度が高速のトランザクションを見つけるために新しいルールを構築する方法の例を示します。 このルールはさらに、安全でないと考えられる国からのトランザクションを見つけるために使用される別のカスタム ルールに依存します。 高速のユーザ頻度とは、短い（設定可能）間隔内の同じユーザによる複数のトランザクションを示します。

以下の図では、RiskMinder でカスタム ルールを作成し、展開するために必要な手順を概説します。



新しいルールを構築するには、以下の手順に従います。

- Safe Countries ルールの作成 (P. 150)
- Safe Countries ルールのデータのアップロード (P. 152)
- High User Velocity from Unexpected Locations ルールの作成 (P. 153)
- High User Velocity from Unexpected Locations ルールの展開 (P. 154)
- ルールの運用環境への移行 (P. 155)
- キャッシュのリフレッシュ (P. 156)

Safe Countries ルールの作成

Safe Countries ルールを作成する方法

1. GA としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. サイド バー メニューの［ルール管理］セクションで、［ルールおよびスコアリング管理］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［選択ルールセット］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［新しいルールの追加］をクリックします。

   ［RiskMinder ルール ビルダ］ページが表示されます。
6. ルールについて、以下の基本情報を入力します。
   - 名前： Safe Countries
   - 短縮名： SAFECOUNTRIES
   - 説明： 送信元が安全であると考えられる国のリストを含むルール
7. デフォルト チャネルおよびすべてのアクションを選択します。

   注: ルールはそれぞれ 1 つ以上のチャネルおよびアクションと関連付ける必要があります。デフォルトでは、ルールはすべてのチャネルおよびすべてのアクションと関連付けられています。
8. 以下のようにルール フラグメントを構築します。
   a. ［データ エレメントの選択］リストから、地理的位置エレメントの COUNTRY を選択します。
   b. 作成しているルールを編集するには、［演算子の選択］リストから IN_LIST 演算子を選択します。
   c. リストの識別子（SAFE_COUNTRY_LIST など）を指定します。
   d. ［追加］をクリックして作成中のルールにフラグメントを追加します。
9. ［作成］をクリックします。

   Safe Countries ルールが作成されます。

Safe Countries ルールのデータのアップロード

展開する Safe Countries ルールは、リストの形式で追加データを必要とします。 このリストには、送信元が安全であると考えられる国の名前が含まれている必要があります。

Safe Countries ルールのデータをアップロードする方法

1. グローバル管理者としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. サイド バー メニューの［ルール管理］セクションで、［リスト データおよびカテゴリ マッピングの管理］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
4. ［既存のルール セットの選択］リストから、この設定が適用可能なルール セットを選択します。
5. ［リスト データを管理］オプションを選択します。
6. ［リスク タイプの選択］リストから、［その他のリスト］を選択します。
7. ［リストの選択］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。 この場合、リスト識別子は SAFE_COUNTRY_LIST です。

   更新されたページが表示されます。
8. ［ファイルをアップロード、またはデータを入力します］セクションで、データを書き込む際の適切なモードを選択します。
   - 追加

     このオプションは、アップロードするデータをリストまたはデータセットに追加します。
   - 置換

     このオプションは、指定されたリストまたはデータ セットの既存のデータを上書きします。
9. 以下の手順のいずれかを実行します。
   - ［参照］をクリックし、改行文字によって区切られたエントリのリストを含むデータ ファイルに移動します。

- データ ファイルが存在しない場合は、［データを入力］フィールドにエントリを入力します。

10. ［アップロード］をクリックしてタスクを完了します。

    安全な国のリストが SAFE_COUNTRY_LIST にアップロードされます。

High User Velocity from Unexpected Locations ルールの作成

High User Velocity from Unexpected Locations ルールを作成する方法

1. GA としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. サイド バー メニューの［ルール管理］セクションで、［ルールおよびスコアリング管理］リンクをクリックします。

    ［ルールおよびスコアリング管理］ページが表示されます。
4. ［選択ルールセット］リストから、この設定が適用可能なルール セットを選択します。

    指定されたルール セットの設定情報が表示されます。
5. ［新しいルールの追加］をクリックします。

    ［RiskMinder ルール ビルダ］ページが表示されます。
6. ルールについて、以下の基本情報を入力します。
    - 名前： High User Velocity from Unexpected Locations
    - 短縮名： HIGH_USER_VEL_UNSAFE
    - 説明： 予期しない場所からの高速のユーザ頻度のトランザクションを判断するルール
7. このルールが適用可能なデフォルト チャネルおよびすべてのチャネルを選択します。
8. ［保存済みルール］リストから、既定の USERVELOCITY ルール、および作成したカスタム SAFECOUNTRIES ルールを選択し、以下のようにルールを構築します。

    ```
    USERVELOCITY AND NOT SAFE_COUNTRIES
    ```
9. ［作成］をクリックします。

    High User Velocity from Unexpected Locations ルールが作成されます。

High User Velocity from Unexpected Locations ルールの展開

作成した High User Velocity from Unexpected Locations カスタム ルールを展開する方法

1. グローバル管理者としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. サイド バー メニューの［ルール管理］セクションで、［ルールおよびスコアリング管理］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［選択ルールセット］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［ルールおよびスコアリング管理］ページの［有効化］オプションを選択して、展開した High User Velocity from Unexpected Locations ルールと Safe Countries ルールを有効にします。
6. ［保存］をクリックして変更内容を保存します。

   展開した新しいルールはまだアクティブでなく、エンド ユーザに利用可能ではありません。 新しいルールをアクティブにするには、それらを運用環境に移行します。

ルールの運用環境への移行

任意の時点で、RiskMinder サーバはアクティブ データの設定のみを使用して動作するようになります。RiskMinder の設定データに対する変更を追跡するため、アクティブ データではバージョン管理が行われます。提示データが運用環境に移行されるたびに、新しいアクティブ設定データ セットに一意のデータ バージョンが作成されます。

新しいルールをアクティブにするには、それらを運用環境に移行します。

変更を移行するには、以下の手順に従います。

1. グローバル管理者としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブを選択します。
3. サイド バー メニューの［実稼働にマイグレート］セクションの下で、［実稼働にマイグレート］リンクをクリックします。

   ［実稼働にマイグレート］ページが開きます。
4. ［選択ルールセット］リストから、新しいルールが含まれるルール セットを選択します。
5. ［マイグレート］をクリックします。

   アクションを確認するページが表示されます。
6. 確認ページで［確認］をクリックし、移行処理を開始します。

   注: 運用環境に移行するデータ量によっては、移行処理に数分かかる場合があります。

   移行が完了すると、成功したことを示すメッセージが表示されます。

ここで RiskMinder サーバのキャッシュをリフレッシュします。 この作業については、以下のトピックで説明します。

キャッシュのリフレッシュ

設定を変更した場合は、変更を有効にするために、影響を受けるサーバ インスタンスのキャッシュをリフレッシュします。RiskMinder には、管理者が管理コンソールからすべてのサーバ インスタンスのキャッシュをリフレッシュできる*統合キャッシュ リフレッシュ*機能があります。

キャッシュをリフレッシュする方法

1. グローバル管理者としてログインしていることを確認します。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. タブのサブメニューで［管理コンソール］オプションをクリックします。
4. サイド バー メニューの［システム設定］セクションで、［キャッシュのリフレッシュ］リンクをクリックして、対応するページを表示します。
5. 以下のいずれかまたは両方のオプションを選択します。
   - 管理コンソール、ユーザ データ サービス、およびすべての RiskMinder サーバとケース管理キュー サーバ インスタンスのキャッシュ設定をリフレッシュするには、［システム設定をリフレッシュ］を選択します。
   - 自分の権限の範囲内のすべての組織のキャッシュ設定をリフレッシュするには、［リフレッシュする組織を選択］を選択します。
6. ［OK］をクリックします。
7. 表示される確認ダイアログ ボックスで［OK］をクリックします。

   現在のキャッシュ リフレッシュ リクエストのリクエスト ID を示すメッセージが表示されます。

これで新しいルールを使用できます。

第 8 章: グローバル設定の管理

重要: このセクションで説明される設定およびタスクはすべて、**グローバル管理者**のみが実行できます。

グローバル レベルで作成される RiskMinder 設定には以下の 2 つのタイプがあります。

- **システム レベル設定**: この設定は［**サービスおよびサーバの設定**］タブで行います。［**組織**］タブで同じ設定を行うことにより特定の組織に対して無効にされない限り、この設定はすべての組織に適用可能です。［**サービスおよびサーバの設定**］タブで行なわれた変更は、すべての組織で利用可能です。
- **すべての組織で使用できるが、すべての組織で自動的に利用可能にならない設定**: このタイプの設定の一例はグローバル レベルで作成されたルール セット テンプレートです。 このルール セットは、オプションで組織のルール セットを作成するときの開始点として使用できます。

このセクションでは、以下について説明します。

- GA が実行できる組織固有の RiskMinder 設定
  - チャネルとアカウントの関連付けの設定 (P. 160)
  - RiskMinder プロパティの設定 (P. 163)
  - RiskMinder モデルの有効化 (P. 167)
- GA がシステムのすべての現在と今後の組織に「テンプレート」として設定できる RiskMinder ルール
  - グローバル ルール設定の管理 (P. 168)

グローバル管理者としてのログイン

最初の GA アカウントは、MA が作成する*必要があります*。GA としてログインし、引き続き設定を続行するには、MA からアカウント詳細を取得する必要があります。

ログインする前に、最初のアカウントへのログインに必要な ID とパスワードを受け取ったことを確認します。 何らかの理由でこのパスワードを紛失してしまった場合は、管理者に再度送信してもらうように連絡する必要があります。

基本認証情報（ユーザ名/パスワード）を使用して GA として CA Advanced Authentication にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. CA Advanced Authentication にアクセスするための URL を入力します。CA Advanced Authentication のデフォルトの URL は以下のとおりです。

   http://<hostname>:CA Portal/arcotadmin/adminlogin.htm

   上記の URL の *hostname* と *port* をそれぞれ、CA Advanced Authentication を展開したシステムのホスト名または管理コンソールがリスンするポートの IP アドレスと置き換えます。

   注: CA Advanced Authentication にアクセスするために、この URL をお気に入りに登録することをお勧めします。いずれの GA、OA、または UA も、ユーザ名とパスワードを使用して CA Advanced Authentication にログインするためにこの URL を使用できます。

   ［管理者ログイン］ページが表示されます。
3. ログインする組織名を入力します。

   重要: 組織の表示名を入力*しないでください*。（組織名によって定義される）組織の一意の ID を入力する必要があります。たとえば、デフォルトの組織（その表示名は Arcot Systems）にログインする場合、この組織の（デフォルト）一意の ID である「defaultorg」を入力する必要があります。 ここで Arcot Systems を指定しないでください。
4. ［ログイン］をクリックします。

   ［ログイン］ページが表示されます。
5. ［ユーザ名］フィールドで管理者 ID を指定し、受け取った対応するパスワードを［パスワード］フィールドに入力して、［ログイン］をクリックします。

初めてログインする場合は、パスワードを変更するように求められます。

6. ［新規パスワード］、［パスワードの確認］を指定し、次に［ログイン］をクリックします。

   ログイン ページにリダイレクトされます。

7. 再度パスワードを指定し、［ログイン］をクリックします。

   CA Advanced Authentication のランディング ページが表示されます。

CA Advanced Authentication からのログアウト

CA Advanced Authentication からログアウトするには、管理コンソールのヘッダ領域の右上隅にある［**ログアウト**］リンクをクリックします。

CA Advanced Authentication 使用時のセキュリティに関する推奨事項

CA Advanced Authentication にアクセスするときには、以下のベスト プラクティスに従ってください。

- ほかのアプリケーションとブラウザ セッションを共有しない。
- コンソールを操作しながら他のサイトを開かない。
- ブラウザの別のタブでほかのサイトを開かない。
- CA Advanced Authentication のために厳しいパスワード制限を実施する。
- CA Advanced Authentication の使用後は必ずログアウトする。
- セッションの終了後にブラウザ ウィンドウを閉じる。
- ユーザが実行する必要のあるタスクに従って適切な役割をユーザに割り当てる。

チャネルとアカウントの関連付けの設定

CA Risk Authentication は、複数のチャネルから送信されるリスク評価リクエストをサポートします。 CA Risk Authentication は、さまざまなチャネルからのトランザクションを評価し、いくつかの要因に基づいてリスク スコアを生成します。 たとえば、アメリカからのホーム バンキング ログイン、およびインドからの 3D セキュア トランザクションが立て続けに実行された場合、不正行為の可能性を示します。 以下の表に、CA Risk Authentication に既定で用意されているチャネルを示します。

チャネル	Description
DEFAULT	Web ブラウザを使用して開始されるトランザクション。これは、コンピュータ、スマートフォン、タブレット、またはセットトップ ボックスのいずれかです。 デフォルト チャネルは Web チャネルです。
3D セキュア	クレジット カードまたはデビット カードを使用して開始されたオンライン トランザクション。

チャネルを割り当てて各チャネルのアカウント タイプを設定する方法

注: チャネルの設定は 1 回限りの設定であるとみなされます。実稼働環境でこれらの設定を変更する場合は、影響を見極めるために CA サポートにお問い合わせください。 チャネルを既存の展開に追加できますが、チャネルまたはアカウント タイプのサポートの削除およびデフォルト チャネルまたはデフォルト アカウント タイプの変更を行う場合は細心の注意を払う必要があります。

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。
7. ［**一般 CA Risk Authentication 設定**］セクションで、［**チャネルの割り当ておよびデフォルト アカウント タイプの設定**］リンクをクリックします。

   ［チャネルの割り当ておよびデフォルト アカウント タイプの設定］ページが表示されます。
8. ［**関連付けるチャネルの選択**］チェック ボックスを選択することによって、組織によってサポートされているチャネルを選択します。
9. 各チャネルのデフォルト アカウント タイプを選択します。
   - 特定のチャネル上の呼び出し元のアプリケーションからのリクエストがリスク評価 API でユーザ名を送信する場合は、［**ユーザ名**］を［**デフォルトのアカウント タイプ**］として選択します。
   - 呼び出し元アプリケーションからのリクエストでユーザ名フィールドにアカウント ID が含まれる場合は、そのチャネルに関連する**デフォルトのアカウント タイプ**を選択します。
10. ［**デフォルト チャネルの選択**］でオプションを選択して、チャネルをリスク評価目的に使用されるデフォルト チャネルにします。

11. ［**保存**］をクリックして変更内容を保存します。

CA Risk Authentication プロパティの設定

CA Risk Authentication プロパティを設定する方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。
7. ［**一般 CA Risk Authentication 設定**］セクションで、［**その他の設定**］リンクをクリックします。 ［その他の設定］ページが表示されます。
8. ［**チャネルの選択**］リストから、これらのパラメータを設定するチャネルを選択します。
9. 以下の表に示されているように、パラメータの値を指定します。

パラメータ	**デフォルト値**	Description
ユーザ登録モード	暗黙的	ユーザが CA Risk Authentication データベースに作成されるモード。 暗黙的： ［**暗黙的**］を選択した場合、CA Risk Authentication でユーザを作成するために createUser() Web サービスを呼び出す必要はありません。 この場合、トランザクションに対して evaluateRisk() API を呼び出すと、CA Risk Authentication は自動的に CA Risk Authentication 内にユーザを作成します（まだ存在しない場合）。 明示的: ［**明示的**］を選択した場合、（evaluateRisk() API を呼び出して）ユーザのトランザクションのリスク評価を実行する前に、createUser() Web サービスを明示的に呼び出して CA Risk Authentication 内にユーザを作成する必要があります。

パラメータ	デフォルト値	Description
基準通貨コード	USD	組織が取引する通貨コード。 このパラメータは、金額ベースのルール用およびケース管理での表示用に使用されます。
デバイス識別で逆引き検索を有効化	いいえ	デバイスを識別する逆引き検索を有効にします。このパラメータがチャネルに適用可能でない場合は（たとえば ATM）、［**いいえ**］を選択します。
逆引き検索で IP アドレスを使用	いいえ	デバイス識別の逆引き検索方法に IP アドレスを使用します。
ケースが自動的にクローズされるまでの非アクティブ状態の期間（時間単位）	48	ケースが自動的にクローズされるまでそのケースが非アクティブなままである期間。
ケースでの作業時に表示するケース ノートの数	1	CSR が［ケース管理］画面上にケースを表示するときに表示されるケース ノートの数。
"追加" をクリックしたときに表示される追加のケース ノート数	3	CSR が［ケース ノート」の下で［**追加**］リンクをクリックしたときに表示されるケース ノートの数。
ケース マネジメント画面を使用してユーザが例外リストに追加されるデフォルトの日数	10	ユーザが［ケース管理］画面を介して例外リストに追加される日数。
デフォルト トランザクション表示期間（日単位）	30	トランザクションがデフォルトで［ケース管理］画面に CSR に対して表示される期間。
ケースが再割り当て可能になるまで、独占的に CSR に割り当てられる最大期間（秒単位）	3600	コンソールでケースを表示する CSR に独占的に割り当てられたままのケースの最大期間。
トランザクションの分析画面の各ページに表示するレコード数	10	ケース管理の［トランザクションの分析］画面の各ページに表示されるレコードの数。

パラメータ	デフォルト値	Description
アドバイス用のケースの生成	DENY ALERT	ケースが生成される CA Risk Authentication アドバイス。 以下の値を指定できます。 ■ NONE ■ DENY ■ ALERT ■ INCREASEAUTH ■ ALLOW

1. ［**更新**］をクリックして、変更内容を保存します。
2. 変更を有効にするために、組織キャッシュをリフレッシュします。

   この方法の詳細については、「組織キャッシュのリフレッシュ」を参照してください。

システム レベルの CA Risk Authentication プロパティの設定

「CA Risk Authentication プロパティの設定 (P. 163)」で説明されている組織固有の CA Risk Authentication 設定に加えて、GA はシステム レベルで特定のパラメータを設定できます。

システム レベルで CA Risk Authentication プロパティを設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. タブのサブメニューで［**CA Risk Authentication**］オプションをクリックします。
4. サイドバー メニューの［**一般 CA Risk Authentication 設定**］セクションで、［**その他の設定**］リンクをクリックして、対応するページを表示します。
5. 以下の表に従って、GA がシステム レベルで設定できるパラメータを指定します。

パラメータ	デフォルト値	Description
ケースをキュー再構築に含める次回アクションまでの期間（秒単位）	1800	ケースがキュー再構築に追加されるまでの期間。

パラメータ	デフォルト値	Description
トランザクションの分析レポートのエクスポート時に、データベースから一括で取得するレコード数（これはアプリケーション サーバで利用可能な最大ヒープメモリに応じて設定してください。）	5000	エクスポートするレコードの数が非常に多い場合、CA Risk Authentication アプリケーションは、アプリケーション サーバがメモリを使い果たさないようにするために小さなサイズのチャンクでデータ セットを取得します。アプリケーション サーバに使用可能なヒープ メモリが十分にある場合、CA Risk Authentication アプリケーションがデータベースへのクエリの数を減らすように、この値を増加させることができます。これにより、パフォーマンスが向上します。
トランザクションの分析画面での検索の最大期間（日単位）	180	［トランザクションの分析］画面で検索が許可される最大時間。
自動キュー再構築スケジュールの頻度（秒単位）	1800	ケース スケジューラが自動的にキューを再構築する頻度。

注: その他のパラメータについては前のトピックで説明されています。

6. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

CA Risk Authentication モデルの有効化

組織の CA Risk Authentication モデルを有効にする方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。
7. ［**ルール管理**］セクションで、［**モデル設定**］リンクをクリックします。
8. ［**ルール セットの選択**］リストから、この設定が適用可能なルールセットを選択します。

   ［モデル設定］情報が表示されます。
9. ［**モデルの有効化**］を選択してモデルを有効にします。
10. ［**保存**］をクリックして変更内容を保存します。
11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。
12. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

グローバル ルール設定の管理

グローバル ルール設定の管理は、CA Risk Authentication 管理および最適化の重要な部分であり、GA の重要な責任です。

注: グローバル レベルまたは組織レベルでの設定の変更は、自動的に適用*されません*。 これらの設定変更を適用するためにサーバ インスタンスをすべてリフレッシュする必要があります。

以下の 2 つのレベルで CA Risk Authentication ルール設定を管理できます。

- グローバル レベル（すべての組織で利用可能）

  注: これらのルールはすべての組織で利用可能ですが、組織レベルでそのまま使用することはできません。 たとえば、グローバル管理者がグローバル レベルに Untrusted IP Check ルールを設定しても、個々の組織は、グローバル ルールからコピーすることによってこのルールを設定する必要があります。

- 組織レベル（個別の組織で利用可能）

  これらの設定は、特定の設定対象の組織*にのみ*適用されます。

  注: システム内の各組織のデフォルトのルール設定を個別に変更することもできますが、ほとんどの組織は繰り返して同じ設定を使用している可能性があります。また、個々の組織にルール設定を行うことは、設定された組織が多数ある場合、厄介なタスクになります。この場合、ルールにグローバル設定を設定すると、組織管理者（OA）は毎回同じ設定を指定する必要がなくなります。

このセクションでは、システム内の現在と将来の*すべての*組織のために「テンプレート」として GA が設定できる設定について説明します。 これらの設定には次のものが含まれます。

- ルール セットの設定（P. 169）
- CA Risk Authentication 予測モデルの設定（P. 173）
- 既定のルールの設定（P. 175）
- 新規ルールの追加（P. 176）
- 新規ルールの展開（P. 200）
- 新規デバイス ベース ルールの展開（P. 204）
- ルール ビルダを使用したルール定義の編集（P. 209）

注: これらの設定は、それを設定する GA の権限の範囲内のすべての組織に適用可能です。個別の組織を設定するには、GA（グローバル管理者）、または対象組織の OA（組織管理者）としてログインする必要があります。

詳細については、「組織固有の CA Risk Authentication の設定の管理」を参照してください。

これらのタスクに加えて、GA は以下も行うことができます。

- システム レベルおよび組織レベルのキャッシュ設定のリフレッシュ（実行方法の詳細については、「キャッシュのリフレッシュ」を参照）。
- 権限の範囲内の組織のアカウント タイプの設定（実行方法の詳細については、「アカウント タイプの設定」を参照）。
- 基本認証ポリシーの設定（実行方法の詳細については、「基本認証ポリシー設定の指定」を参照）。
- プロファイル情報の変更（実行方法の詳細については、「パスワードとプロファイル情報の変更」を参照）。

ルール セットの設定

このセクションでは、以下のトピックについて説明します。

- ルール セットについて (P. 170)
- ルール セットの作成 (P. 171)

ルール セットについて

*ルール セット*は、設定した 1 つ以上の CA Risk Authentication ルール（「評価ルール」および「スコアリング エンジン」）の集合体で、実行順序およびスコアリングの優先度も含まれます。 ルール セットはそれぞれが以下の観点から異なる場合があります。

- 設定されたルールのセット
- セット内の各ルールのスコアおよび優先度
- セット内のルールの有効化または無効化
- 各ルールの設定されたパラメータおよびデータ

グローバル管理者は、すべての組織で利用可能な複数のグローバル ルール セットを設定することができます。 これらのルール セットを組織の他の GA または OA が使用し、既存のルール セットから「コピー」するだけで新しいルール セットを作成することができます。 さらに、ルール セット内の「コピーされた」ルールは編集することもできます。 これは、組織のために個別にルールを再度設定するために必要な時間および労力を大幅に節約するだけでなく、エラーの数も削減されます。

重要: CA Risk Authentication には **DEFAULT** と呼ばれるすぐに使えるグローバル ルール セットが付属しています。

ルール セットの作成

重要: GA がグローバル ルール セットを作成した後、個々の組織の OA はそれぞれの組織にこれらのルール セットを割り当てる必要があります。

詳しい方法については、「ルール セットの割り当て」を参照してください。

ルール セットの作成方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. ［**CA Risk Authentication**］タブをアクティブにします。
4. サイド バー メニューの［**ルール セット管理**］で、［**ルール セットの作成**］リンクをクリックします。

   ［ルール セットの作成］ページが表示されます。
5. ［**名前**］フィールドにルール セットの名前を指定します。
6. ［**詳細オプション**］で、必要に応じて以下の手順に従います。
   a. 既存のルール セットからルール設定をコピーする場合は、［**既存のルール セットからコピー**］オプションを選択します。
   b. 対応するリストから設定をコピーするルール セットの名前を選択します。

   注: 既存のルール セットからコピーしない場合、新しいルール セットがデフォルト設定で作成されます。
7. ［**作成**］をクリックして新しいルール セットを作成して保存します。

   ルール セットはまだアクティブでなく、エンド ユーザに利用可能ではありません。
8. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

CA Risk Authentication のスコアリングについて

アプリケーションからリスク評価リクエストが発生すると、CA Risk Authentication は評価ルールを実行して *リスク スコア*（または*スコア*）を生成します。通常、このスコアは **0** ～ **100** までの値であり、推奨される *リスク アドバイス*（または*アドバイス*）にマップされます。その後で CA Risk Authentication はスコアリング エンジンを使用して、最終的なスコアおよび対応するアドバイスを生成します。

以下の表では、事前定義済みスコアの値範囲と対応するアドバイスのマッピングについて説明します。

注: 0 のスコアは、実行する必要はあるが、スコアリングには使用されないルールに割り当てられます。スコアを 0 に設定した場合、生成されるアドバイスは SILENT です。

スコア値（最小値）	スコア値（最大値）	アドバイス	デフォルトの推奨アクション
1	30	**ALLOW**	トランザクションの続行を許可します。
31	50	**ALERT**	適切なアクションを実行します。 たとえば、現在ユーザ名が不明である場合、アラートを取得したらすぐに CSR にリダイレクトするか、CA Risk Authentication にユーザを作成することができます。
51	70	**INCREASEAUTH**	続行する前に追加の認証を実行します。
71	100	**DENY**	トランザクションを拒否します。

［ルールおよびスコアリング管理］ページを使用して、ユーザのビジネス要件に合わせて CA Risk Authentication スコアリングを設定できます。詳細については、「既定のルールの設定 (P. 175)」を参照してください。

CA Risk Authentication 予測モデルの設定

注: CA Risk Authentication 予測モデルはオプション コンポーネントです。予測モデルの使用に関心がある場合は、担当営業にお問い合わせのうえ、作業明細書をご確認ください。

CA Risk Authentication は、高度な不正行為モデリング機能を備えています。このモデリング機能により、履歴データに基づいて CA Risk Authentication 内にモデルを構築および作成できます。 モデルは、利用可能なトランザクション データとシステム データを使用して、トランザクションの真正性に対する疑わしさを示すスコアを生成します。 通常、このスコアの範囲は 0 ～ 100 までであり、数値が大きいほど不正行為の可能性が高くなります。 アプリケーションの呼び出しに対し、CA Risk Authentication がこのモデル スコアに応じて異なるレスポンスを返すように設定できます。

モデル スコアは、既定のルールを設定する際、システム パラメータの一部（スコア）として表示されます。 このスコアは、リスク アドバイスで提供されるほかのデータ要素と組み合わせて使用できます。

CA Advanced Authentication を使用して、CA Risk Authentication 予測モデルの URL とタイムアウトのパラメータを設定できます。

CA Risk Authentication 予測モデルを設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. ［**CA Risk Authentication**］タブをアクティブにします。
4. サイド バー メニューの［**モデル設定**］で、［**モデル設定**］リンクをクリックします。

   ［モデル設定］ページが表示されます。
5. ［**候補値**］列で、以下の表に示すパラメータを指定します。

パラメータ	Description
予測モデル URL （プライマリ）	CA Risk Authentication 予測モデルのプライマリ URL。
予測モデル URL （バックアップ）	CA Risk Authentication 予測モデルのバックアップ URL。
接続タイムアウト（ミリ秒）	CA Risk Authentication サーバと予測モデルの間の接続が期限切れになるまでの時間。
読み取りタイムアウト（ミリ秒）	CA Risk Authentication サーバが予測する予測モデルからレスポンスが戻るまでの時間。

パラメータ	Description
最小接続数	モデル サーバに接続する接続プール内の接続の最小数。
最大接続数	モデル サーバに接続する接続プール内の接続の最大数。

6. ［**モデル設定のアップロード**］をクリックして、変更を保存します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

7. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

既定のルールの設定

［ルール設定］ページを使用して以下を実行します。

- 既定のルールの有効化または無効化
- リスク スコアおよび既定のルールの優先度の設定

ルールを有効または無効にする方法、およびリスク スコアと既定のルールの優先度を設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. ［**CA Risk Authentication**］タブをアクティブにします。
4. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
5. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
6. 表示された表の［**候補**］列で、各ルールに対して以下の操作を行います。

   a. ［**有効化**］オプションをオン（ルールを有効）またはオフ（ルールを無効）にします。

   b. 必要な**リスク スコア**を指定します。

   c. ［**優先度**］リストからルールの優先度を選択します。
7. ［**デフォルト スコア**］（このページの 2 番目の表）の［**候補**］列に、必要なリスク スコアを指定します。

   注: CA Risk Authentication では、前の表に一致するルールがない場合に、この値を使用して最終的なリスク スコアとアドバイスを生成します。デフォルト スコアに対して設定できる最小値は 1 です。
8. ［**保存**］をクリックして、この画面で行った変更を保存します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
9. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

10. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

新規ルールの追加

CA Risk Authentication の既定の評価ルールは汎用的であり、一般的なトランザクションのリスクを評価するために設定されます。 デフォルト ルールのスコアや優先度を調整したり、ホワイト リストやブラック リストを作成して結果を改善することができますが、すべてのケースで十分ではない可能性があります。 このような場合、CA Risk Authentication がデフォルトで提供しているルールとは大きく異なる新しいルールを追加できます。

ルール ビルダを使用して、既定のルール（頻度ルールなど）またはアップロードされたリストを、トランザクション、デバイス、および地理的位置のエレメント、数学演算子、ブール関数と組み合わせて不正なトランザクションを識別できます。

新規ルールの作成に使用するデータ エレメントと演算子

新規ルールを作成するには、以下のエレメントが必要です。

- データ エレメント
- 演算子

データ エレメント

作成するルールに応じて、以下のデータ エレメントから選択できます。

- **トランザクション エレメント**: すべてのチャネル上の不審なトランザクション パターンを識別するルールを作成できます。
- **デバイス エレメント**: 特定のデバイスに関連付けられたリスクを識別するルールを作成できます。
- **地理的位置エレメント**: トランザクションが実行されたユーザの地理的位置データを分析するルールを作成できます。
- **モデル エレメント**: モデル スコアに基づいてトランザクションを分析するルールを作成できます。
- **カスタム エレメント**: あらかじめ設定されたデータ エレメントのリストにない独自のデータ エレメントを作成できます。 カスタム エレメントに使用できるエレメント名のリストについては、「CA Risk Authentication ルール タグ」を参照してください。

演算子

ルールを作成するために使用する演算子は、以下のカテゴリに分類できます。

- **式**: これらの演算子は、ルールを構築するルール フラグメントを組み合わせるために使用されます。
  使用可能な演算子には、AND、OR、NOT、(、) 演算子が含まれます。
- **一致タイプ**: これらの演算子は、IN_CATEGORY および IN_LIST 演算子によって使用されます。 使用可能な演算子には以下が含まれます。
  - EXACT: リスト値が入力値に完全に一致する場合、ルールがトリガされます。
  - PARTIAL: リスト内の値のいずれかが入力値の部分的なサブセットである場合、ルールがトリガされます
- **検索タイプ**: 使用可能な演算子には IN_LIST、IN_TRUSTED_LIST、および IN_NEGATIVE_LIST が含まれます。

- **演算子：** これらの演算子は、データ エレメントの数値の比較に使用されます。
  使用可能な演算子には、EQUAL_TO （=）、NOT_EQUAL_TO （!=）、GREATER_OR_EQUAL（>=）、LESS_OR_EQUAL（<=）、GREATER_THAN（>）、および LESS_THAN （<）が含まれます。

以下の表では、トランザクション エレメントおよび対応する演算子について説明します。

データ エレメント	使用する場合	演算子の説明
ACTION	1 つ以上の事前定義済みアクションがリスト内にあるか、特定の期間中に実行されたかをルールが追跡する必要がある場合。	■ IN_LIST : 実行されたアクションが単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ VELOCITY : 指定されたアクション セットのトランザクションの頻度が事前定義済みのしきい値に達するか超えているかを確認し、この条件が満たされる場合 True を返します。このルールは、以前のパスワードの変更が現在のトランザクションを危険にする状況を検出するのに役立ちます。 たとえば、過去 24 時間に送金の前にパスワードのリセットが行われていないかどうかを確認するには、［**対象アクション セット**］リストの FORGOT_PWD アクションに対して［**次の値以上**］が 1、［**期間**］が 24 時間のルールを設定する必要があります。 ■ IN_CATEGORY : マッピング データ セットのテーブル内の実行されたアクションをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
USERNAME	ルールで、トランザクションが特定のユーザによって実行されたかどうかを確認する必要がある場合。	■ IN_LIST: ユーザが単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ VELOCITY： 特定のユーザのトランザクションの数が指定された期間および頻度によって設定された制限を超えているかどうかを確認します。 ■ ZONE_HOP： 短い間隔で同一ユーザによって複数の遠く離れた場所から送信されるトランザクションを確認します。 ■ UNKNOWN： ユーザが CA Risk Authentication データベースにすでに登録されているかどうかを確認します。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のユーザをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
CURRENTTIME	ルールで、トランザクションが実行された時刻に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ 以下の演算子を使用して、トランザクションが実行された **CURRENTTIME** を指定された**時刻**と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST： **CURRENTTIME** が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **CURRENTTIME** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 注: **CURRENTTIME** の形式は HHMM です。

データ エレメント	使用する場合	演算子の説明
DATE	ルールで、トランザクションが実行された日付に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： **DATE** が単純なルックアップ リストにあるかどうかを確認します。 完全一致のみが許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ 以下の演算子を使用して、トランザクションの **DATE** を指定された日付と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY： マッピング データ セットのテーブル内の **DATE** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: **DATE** の形式は YYYYMMDD です。

データ エレメント	使用する場合	演算子の説明
DAYOFMONTH	ルールで、トランザクションが実行された月内の日付に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： **DAYOFMONTH** が単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ 以下の演算子を使用して、トランザクションが実行された **DAYOFMONTH** を選択された**月内の日付**と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY： マッピング データ セットのテーブル内の **DAYOFMONTH** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: **DAYOFMONTH** は、01 = 1 月、02 = 2 月というような 2 桁の数です。
DAYOFWEEK	ルールで、トランザクションが実行された曜日に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： **DAYOFWEEK** が単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **DAYOFWEEK** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: **DAYOFWEEK** に使用できる値は、SUNDAY、MONDAY、TUESDAY、WEDNESDAY、THURSDAY、FRIDAY、および SATURDAY です。

データ エレメント	使用する場合	演算子の説明
MONTH	ルールで、トランザクションが実行された月に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： トランザクションの **MONTH** が単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ 以下の演算子を使用して、トランザクションの **MONTH** を指定された月と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY： マッピング データ セットのテーブル内の **MONTH** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: **MONTH** の形式は MM です。

データ エレメント	使用する場合	演算子の説明
YEAR	ルールで、トランザクションが実行された年に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： トランザクションの **YEAR** が単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ 以下の演算子を使用して、トランザクションの **YEAR** を指定された年と比較します。 – EQUAL_TO – NOT_EQUAL_TO ¥xE2¥x80¥x93 GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_CATEGORY： マッピング データ セットのテーブル内の **YEAR** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: **YEAR** の形式は YYYY です。

以下の表では、3D セキュア チャネルに固有のトランザクション エレメントについて説明します。

データ エレメント	使用する場合	演算子の説明
ACQ_BIN	ルールで、トランザクションが実行された業者のアクワイアラ BIN を確認する必要がある場合。	■ IN_LIST： アクワイアラ BIN が単純なルックアップリストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のアクワイアラ BIN をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
AMOUNT	ルールで、指定された通貨のしきい値の金額と比較してトランザクションを追跡する必要がある場合。 自動通貨換算をサポートするルールを設定できます。 これが有効な場合、基準通貨でしきい値の金額のみを指定する必要があります。 自動換算を使用しない追加の通貨でしきい値を指定することができます。 通貨換算テーブルの詳細については、付録「通貨換算 (P. 463)」を参照してください。	■ 以下の演算子を使用して、トランザクションの **AMOUNT** を指定された金額と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST： **AMOUNT** が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **AMOUNT** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。
CURRCODE	ルールで、トランザクションに使用された 3 桁の数値コードを確認する必要がある場合。	■ IN_LIST: 通貨コードが単純なルックアップ リストにあるかどうかを確認します。完全一致のみが許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の通貨コードをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
MERCHANT_ID	ルールで、トランザクションに関与する業者の一意の識別子に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： 業者 ID が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の業者の ID をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。
MERCHANT_NAME	ルールで、トランザクションに関与する業者の名前に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST: 業者名が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の業者名をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。
MERCHANT_URL	ルールで、トランザクションに関与する業者の URL に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST： 業者の URL が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の業者の URL をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
MERCH_CAT	ルールで、トランザクションに関与する業者のカテゴリに基づいて不審なトランザクション パターンを識別する必要がある場合。	■ IN_LIST: 業者のカテゴリが単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の業者のカテゴリをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。
MERCH_COUN	ルールで、購入が行われた業者の国コードに基づいて不審なトランザクション パターンを識別する必要がある場合。 MERCH_COUN は 3 桁の ISO 国コードです。	■ IN_LIST: 業者の国が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の業者の国をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。

データ エレメント	使用する場合	演算子の説明
PREVTXNDATA	ルールで、前のトランザクションが指定された時間数内の選択されたアクションのいずれかと一致するかどうかを確認する場合。 前のトランザクション タイプが指定された時間フレーム内のこのユーザの選択されたタイプと同じだった場合、ルールは True を返します。	CHECK：特定のユーザの指定された期間内に実行された前のトランザクションのタイプが、選択されたアクションの 1 つ以上と一致するかどうかを確認します。 トランザクション タイプは以下のとおりです。 ■ **REGULAR**： 標準的な購入トランザクション。 ■ **ATTEMPTS**： 試行トランザクション（ユーザは登録されず、銀行はユーザの認証を試行したことを業者に通知できます）。 ■ **AE_WITH_PWD**： すべてのカード所有者が有効なパスワードを持つ自動登録。 ■ **AE_WITHOUT_PWD**： 一部のカード所有者が空のパスワードを持つ自動登録。 ■ **FORGOT_PWD**： パスワードを忘れたトランザクション。 ■ **SEC_CH**：セカンダリ カード所有者の追加（追加のカード所有者（ユーザ名/パスワード）が既存のカード番号に追加されます）。 ■ **FORGOT_PWD_MULTI_CH**：複数のカード所有者シナリオ内のパスワードを忘れたトランザクション。 ■ **FORGOT_PWD_SINGLE_CH**：単一のカード所有者シナリオ内のパスワードを忘れたトランザクション（これは **FORGOT_PWD** と同じです）。 ■ **ABRIDGED_ADS**： 一時パスワードで買い物をする間の有効化。 ■ **SEC_CH_ABRIDGED**：簡易登録によるセカンダリ カード所有者。 ■ **UNKNOWN**： 不明なトランザクション タイプ（これは例外的な状況です）。

以下の表では、デバイス エレメントおよび対応する演算子について説明します。

データ エレメント	使用する場合	演算子の説明
BROWSER	ルールで、トランザクションが発生したブラウザを確認する必要がある場合。	■ IN_LIST: ブラウザ名が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のブラウザ名をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: サポートされているブラウザは、Mobile Safari、Android Webkit、Microsoft Internet Explorer、Firefox、Epiphany、K-Meleon、Konqueror、Minimo、Mozilla、SeaMonkey、Netscape、NetPositive、Novarra、OmniWeb、Opera、Safari、Camino、Shiira、Lynx、w3m、Chrome、CrMo、CriOS、Avant Browser、PSP、ELinks、Links、および OffByOne です。

データ エレメント	使用する場合	演算子の説明
DEVICEID	ルールで、トランザクションに関与するデバイスの ID に基づいて不審なトランザクション パターンを識別する必要がある場合。	■ VELOCITY： 特定のデバイスからの 1 人以上のユーザによって実行されたトランザクションの数が期間と頻度によって設定された制限を超えるかどうかを確認します。 ■ UNKNOWN： デバイスが認識されたデバイスかどうかを確認します。 ■ IN_LIST： デバイス ID が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のデバイス ID をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 ■ VELOCITY_DISTINCT_USER： 特定のデバイスから設定された期間内にトランザクションを実行した *n* 名の個別ユーザの数をカウントします。 詳細については、「Device User Velocity ルールの作成 (P. 205)」を参照してください。

データ エレメント	使用する場合	演算子の説明
DEVICETYPE	ルールで、トランザクションに関与するデバイスのタイプをチェックする必要がある場合。	■ IN_LIST： デバイス タイプが単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のデバイス タイプをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 **注**: サポートされているデバイス タイプは、PC、Mac、iPad、iPhone、Kindle、Android、Linux、BlackBerry、Nokia、iPod、PlayBook、Web OS、HP Tablet、Sony PlayStation、および任天堂 Wii です。
MFPMATCHPERCENT	ルールで、マシン フィンガープリントの一致をチェックする必要がある場合。	入力デバイスのシグネチャと対応する格納済みデバイス シグネチャの一致率が、以下のしきい値に対して **LESSER_OR_EQUAL** であるかどうかを確認します。 ■ シグネチャ一致しきい値: トランザクションに有効なデバイス ID があり、入力シグネチャが前のトランザクションのシグネチャと照合される場合にチェックされる一致率に対するしきい値。 ■ 逆引きしきい値: 入力デバイス シグネチャをユーザに正常に関連付けられたデバイス シグネチャと照合することによりデバイス ID が取得される場合にチェックされる一致率に対するしきい値。

データ エレメント	使用する場合	演算子の説明
OS	ルールで、トランザクションに関与するデバイスによって使用されるオペレーティング システムをチェックする必要がある場合。	■ IN_LIST： オペレーティング システムが単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のオペレーティング システム値をチェックし、リスト データ セット内の入力の関連する派生値を比較します。 完全一致および部分一致が許可されます。 **注**: サポートされている OS は、Windows 98、Windows 95、Windows NT 4.0、Windows NT 3.51、Windows NT、Windows CE、Windows、PPC Mac OS X Mach-O、PPC Mac OS X、Intel Mac OS X、PPC Mac OS、Intel Mac OS、Mac OS、Macintosh、Linux、FreeBSD、NetBSD、OpenBSD、Debian、Gentoo、Red Hat Linux、SUSE、CentOS、Fedora、Mandriva、PCLinuxOS、Ubuntu、OS/2、SunOS、PalmOS、Symbian、Darwin、J2ME/MIDP、PSP、iOS、および Android です。

以下の表では、地理的位置エレメントおよび対応する演算子について説明します。

データ エレメント	使用する場合	演算子の説明
CITY	ルールで、トランザクションが発生した市区町村をチェックする必要がある場合。	■ IN_LIST : 発生元の市区町村が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の発生元の市区町村をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、データ リストにデータをアップロードし、カテゴリ マッピングを管理できます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。

データ エレメント	使用する場合	演算子の説明
CLIENTIPADDRESS	ルールで、トランザクションの実行に使用されるクライアント IP アドレスをチェックする必要がある場合。	■ IN_TRUSTED_LIST： クライアントの IP アドレスがトラステッド IP アドレスの事前定義済みリストにあるかどうかを確認します。 ■ IN_LIST: IP アドレスが単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ VELOCITY: この IP アドレスからのトランザクションの数が期間と頻度によって設定された制限を超えているかどうかを確認します。 ■ IN_NEGATIVE_LIST： 匿名プロキシをチェックします。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の IP アドレスをチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。
CONNECTIONTYPE	ルールで、トランザクションの実行に使用された接続のタイプを確認する必要がある場合。 **CONNECTIONTYPE** は、インターネット プロバイダへの接続のタイプを示します。	■ IN_LIST: **CONNECTIONTYPE** が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **CONNECTIONTYPE** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 可能な値のリストについては、「接続タイプ (P. 451)」を参照してください。

データ エレメント	使用する場合	演算子の説明
CONTINENT	ルールで、トランザクションが発生した大陸をチェックする必要がある場合。	■ IN_LIST： トランザクションが発生した大陸が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 CA Risk Authentication では、入力 IP アドレスに基づいて国情報を導き出します。 ■ IN_CATEGORY： マッピング データ セットのテーブル内のトランザクションが発生した大陸をチェックし、リスト データ セット内の入力の関連する派生値を比較します。 完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、データ リストにデータをアップロードし、カテゴリ マッピングを管理できます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 大陸のリストについては、「大陸 (P. 453)」を参照してください。
COUNTRY	ルールで、トランザクションが発生した国をチェックする必要がある場合。	■ IN_NEGATIVE_LIST： 発生元の国が「拒否」国の事前定義済みリストにあるかどうかを確認します。 ■ IN_LIST: 発生元の国が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 CA Risk Authentication では、入力 IP アドレスに基づいて国情報を導き出します。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の発生元の国をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、データ リストにデータをアップロードし、カテゴリ マッピングを管理できます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。

データ エレメント	使用する場合	演算子の説明
IP_ROUTINGTYPE	ルールで、トランザクションの実行に使用された接続の IP ルーティング タイプをチェックする必要がある場合。 **IP_ROUTINGTYPE** は、場所の正確性の評価を支援する IP アドレスの属性です。	■ IN_LIST： **IP_ROUTINGTYPE** が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **IP_ROUTINGTYPE** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 可能な値のリストについては、付録「IP ルーティング タイプ (P. 450)」を参照してください。
LINESPEED	ルールで、トランザクションを実行するために使用されるユーザのインターネット接続の速度をチェックする必要がある場合。	■ IN_LIST： **LINESPEED** が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の **LINESPEED** をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 可能な値のリストについては、「回線速度 (P. 452)」を参照してください。

データ エレメント	使用する場合	演算子の説明
REGION	ルールで、トランザクションが発生した都道府県をチェックする必要がある場合。	■ IN_LIST: 発生元の都道府県が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の発生元の都道府県をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、データ リストにデータをアップロードし、カテゴリ マッピングを管理できます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 可能な値のリストについては、「地域 (P. 453)」を参照してください。
STATE	ルールで、トランザクションが発生した都道府県をチェックする必要がある場合。	■ IN_LIST: 発生元の都道府県が単純なルックアップ リストにあるかどうかを確認します。完全一致および部分一致が許可されます。［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY： マッピング データ セットのテーブル内の発生元の都道府県をチェックし、リスト データ セット内の入力の関連する派生値を比較します。完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、データ リストにデータをアップロードし、カテゴリ マッピングを管理できます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。

以下の表では、モデル エレメントおよび対応する演算子について説明します。

データ エレメント	使用する場合	演算子の説明
MODEL_SCORE	ルールで、モデル評価の結果のスコアをチェックする必要がある場合	■ 以下の演算子を使用して、モデル スコアを指定された値と比較します。 – EQUAL_TO – NOT_EQUAL_TO – GREATER_THAN – LESS_THAN – GREATER_OR_EQUAL – LESS_OR_EQUAL ■ IN_LIST : モデル スコアが単純なルックアップ リストにあるかどうかを確認します。 完全一致および部分一致が許可されます。 ［リスト データおよびカテゴリ マッピングの管理］ページで、リストを表示し、このリストにデータをアップロードできます。 詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください。 ■ IN_CATEGORY : マッピング データ セットのテーブル内のモデル スコアをチェックし、リスト データ セット内の入力の関連する派生値を比較します。 完全一致および部分一致が許可されます。

新規ルールの使用例

以下のサブセクションでは、デフォルトの CA Risk Authentication ルールと作成したルールを組み合わせて、複合的な要因と条件を使用してカスタムの組み合わせルールを定義する方法について説明します。

- 高額チェック
- 予期しない場所からの高速のユーザ頻度
- 予期しない場所からの高速のデバイス頻度
- 予期しない場所からの電子送金

注: 以下の例にあるルール（SAFE_COUNTRIES など）は、安全な送金元と見なされる国のリストを使用する単純なリスト ルールを表すものです。

高額チェック

トランザクション金額が 500 ドルを超えるかどうかをチェックする必要がある AMOUNT_CHECK ルールの以下の詳細について検討します。

- **ルールの短縮名：** HIGHAMTCHK
- **ルールの表示名：** High Amount Check
- **説明：** このルールは 500 ドルを超える高額のトランザクション金額をチェックします。
- **金額：** 500

この例のルールは、以下の内容を実行します。

1. Amount という名前のタグによって evaluateRisk() API 呼び出しで渡される AdditionalInput の文字列（Amount=750）を解析し、このタグの変数 ActualAmount の値を抽出します。

   注: AdditionalInput エレメントの解析の詳細については、Javadoc を参照してください。

2. ルールのパラメータ値（500）を抽出し、それを ParameterAmount という変数に保存します。
3. この場合、ActualAmount（750）が ParameterAmount（500）より大きいため、Matched が返されます。

予期しない場所からの高速のユーザ頻度

SAFE_COUNTRIES が単純なリスト ルール（US、CA、UK、DE などのエレメントを含む）を参照している場合を考えます。この場合、以下のように新しいルールを定義して、通常以外の場所からのユーザ頻度が高速のトランザクションを見つけることができます。

```
USERVELOCITY AND NOT SAFE_COUNTRIES
```

予期しない場所からの高速のデバイス頻度

「予期しない場所からの高速のユーザ頻度」と同様に、以下のように新しいルールを定義して、通常以外の場所からのデバイス頻度が高速のトランザクションを見つけることができます。

```
DEVICEVELOCITY AND NOT SAFE_COUNTRIES
```

予期しない場所からの電子送金

HIGHAMTCHK と呼ばれるルールを作成した場合を考えます（「高額チェック」で説明）。また、SAFE_COUNTRIES ルールで送金元が安全であると考えられる国のリストを使用すると、以下のようなルールを定義して、通常ではない場所からの小額または高額の電子送金を追跡できます。

```
(HIGHAMTCHK OR Amount < 20) AND NOT SAFE_COUNTRIES
```

新規ルールの展開

新規ルールを展開する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイドバー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［選択ルールセット］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**新しいルールの追加**］をクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. 以下の表の説明に従ってルールの基本情報を入力します。

フィールド	Description
Name	作成するルールの表示名。
ニーモニック	ログの記録と API で使用するルールの短縮名。 短縮名の最大文字数は 15 文字です。スペースは使用できません。
Description	作成するルールの簡単な説明。

7. このルールが適用可能な**チャネル**および**アクション**を選択します。

   すべてのチャネルおよびすべてのアクションを選択する場合は、［**すべてのチャネル**］および［**すべてのアクション**］チェック ボックスを選択します。

   注: ルールはそれぞれ 1 つ以上のチャネルおよびアクションと関連付ける必要があります。デフォルトでは、ルールは**すべてのチャネル**および**すべてのアクション**と関連付けられています。

8. 以下のようにルール フラグメントを構築します。

   a. ［**データ エレメントの選択**］リストから、以下のエレメントを選択します。

      - トランザクション
      - デバイス
      - 地理的位置
      - モデル
      - カスタム

      エレメントの詳細については、「データ エレメント」を参照してください。

   b. ［**演算子の選択**］リストから演算子を選択し、作成しているルールを編集します。

      演算子の詳細については、「演算子」を参照してください。

   c. ［**追加**］をクリックして、［**ルールを作成中です**］領域にルール フラグメントを追加します。

9. 利用可能な論理演算子、ルール フラグメント、および［**保存済みルール**］リストのルールを使用することにより、完全なルールを構築します。

10. ［**作成**］をクリックしてルールを作成します。

11. ［ルールおよびスコアリング管理］ページの［**有効化**］を選択して、展開した新しいルールを有効にします。

    ここで展開した新しいルールはまだアクティブではなく、エンド ユーザに利用可能ではありません。

12. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

13. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

スコアリングなしの新規ルールの展開

ルールがどのように実行されるかのみを確認し、最終アドバイスにルールスコアを含めたくない場合があります。 CA Risk Authentication のこのリリースでは、新しいルールを定義し、スコアリングを有効にせずにどのように実行されるかを確認することができます。 スコアリングなしで新規ルールを展開する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［選択ルールセット］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**新しいルールの追加**］をクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. 以下の表の説明に従ってルールの基本情報を入力します。

フィールド	Description
Name	作成するルールの表示名。
ニーモニック	ログの記録と API で使用するルールの短縮名。 短縮名の最大文字数は 15 文字です。スペースは使用できません。
Description	作成するルールの簡単な説明。

7. このルールが適用可能な**チャネル**および**アクション**を選択します。

   すべてのチャネルおよびすべてのアクションを選択する場合は、［**すべてのチャネル**］および［**すべてのアクション**］チェック ボックスを選択します。

   注: ルールはそれぞれ 1 つ以上のチャネルおよびアクションと関連付ける必要があります。デフォルトでは、ルールは**すべてのチャネル**および**すべてのアクション**と関連付けられています。

8. 以下のようにルール フラグメントを構築します。

   a. ［**データ エレメントの選択**］リストから、以下のエレメントを選択します。

      - トランザクション
      - デバイス
      - 地理的位置
      - モデル
      - カスタム

      エレメントの詳細については、「データ エレメント」を参照してください。

   b. ［**演算子の選択**］リストから演算子を選択し、作成しているルールを編集します。

      演算子の詳細については、「演算子」を参照してください。

   c. ［**追加**］をクリックして、［**ルールを作成中です**］領域にルール フラグメントを追加します。

9. 利用可能な論理演算子、ルール フラグメント、および［**保存済みルール**］リストのルールを使用することにより、完全なルールを構築します。

10. ［**作成**］をクリックしてルールを作成します。

11. ［ルールおよびスコアリング管理］ページの［**有効化**］を選択して、展開した新しいルールを有効にします。

    ここで展開した新しいルールはまだアクティブではなく、エンド ユーザに利用可能ではありません。

12. ［**リスク スコア**］を 0 に指定します。

    リスク スコアを 0 に設定すると、このルールがリスク スコアリングに対して考慮されないようになります。

13. ［**優先度**］リストから、このルールの優先度を 1 に設定します。

    ルールの優先度を 1 に設定すると、このルールが最初に実行されるようになります。

14. ［保存］をクリックして変更内容を保存します。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

15. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

16. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

新規デバイス ベース ルールの展開

CA Risk Authentication のこのリリースでは、デバイスとユーザの関連付けに基づいて以下の新しいルールを作成できます。

- Device User Velocity
- Device User Maturity

Device User Velocity ルールの作成

既存の Device Velocity Check ルールは、特定のデバイスから 1 名以上のユーザによる頻繁なトランザクションが定義された頻度を超えているかどうかを確認します。 これは、単一のデバイスが複数のユーザによって共有されている場合、不正確な結果をもたらすことがあります。 新しい *Device User Velocity* ルールでは、設定された期間で *n* 名の異なるユーザがデバイスを使用できます。設定された期間内にデバイスが *n* 名を超える個別ユーザによって使用された場合、不正行為であることを示します。

ルールは以下のパラメータに基づきます。

- **デバイスごとに許可する個別ユーザの数**

  リスク評価の結果が成功または失敗であるかに関係なく、指定されたデバイスを使用してトランザクションを実行する個別ユーザの数を示します。

  このパラメータのデフォルト値は **5** です。

- **Time Interval**

  トランザクションの数を追跡する期間を示します。

  このパラメータのデフォルト値は **60** です。

- **時間間隔の単位**

  測定される期間の単位を示します。

  このパラメータのデフォルト値は**分**です。

たとえば、60 分でデバイスあたり 5 つのトランザクションの設定を考えてみます。 User1 が Device1 から 1 時間あたり 5 つのトランザクションを実行するとき、このルールはトリガされません。しかし、1 時間で Device1 を使用する 5 名のユーザからの複数のトランザクションがある場合、このルールはトリガされます。

Device User Velocity ルールを作成する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイドバー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。

4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。

5. ［**新しいルールの追加**］をクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。

6. 作成するルールの［**名前**］、［**ニーモニック**］、および［**説明**］を入力します。

7. このルールが適用可能な**チャネル**および**アクション**を選択します。

8. 以下のようにルール フラグメントを構築します。

   a. デバイス エレメント リストから、［**DEVICEID**］を選択します。

   b. ［**演算子の選択**］リストから［**VELOCITY_DISTINCT_USER**］を選択します。

   c. ［**次の値より大きい**］フィールド内のデバイスからトランザクションを実行する個別ユーザの数を指定します。

   d. 時間間隔を指定します。

      この値は、*n* 名の個別ユーザのデバイスにとって安全であると考えられる（指定された時間間隔内の）トランザクションの最大数を示します。 指定された時間内のトランザクションの実数がこの数を超えると、CA Risk Authentication はトランザクションをリスクとして追跡し、結果として Device User Velocity ルールと一致させます。

   e. ドロップダウン リストから時間間隔の単位を選択します。

   f. ［**追加**］をクリックしてルール フラグメントを構築します。

9. ［ルール ビルダ］ページの下部にある［**作成**］をクリックして、ルールを作成します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

11. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

Device User Maturity ルールの作成

User Not Associated with DeviceID ルールは、関連付けが作成された時間に関係なく、ユーザとデバイスの関連付けを確認することにより、トランザクションを評価します。 ユーザとデバイスの関連付けが存在する場合、トランザクションには低いリスク スコアが割り当てられます。 不正行為の実行者がユーザのパスワードをリセットし、自分自身とデバイスを関連付ける場合があります。 そのような場合、ユーザとデバイスの関連付けにのみ基づいたトランザクションの評価は、不正行為を除外するのに十分ではない場合があります。

Device User Maturity ルールでは、デバイスの信頼レベルを設定できます。たとえば、1 か月間存在しているユーザとデバイスの関連付けは、そのユーザまたはデバイスに対して不正行為がなかったことが確認されていると仮定した場合、最近確立されたユーザとデバイスの関連付けより信頼レベルが高くなります。

ルールは以下のパラメータに基づきます。

- **ユーザとデバイスの関連付けに対して成功したトランザクションの数**

  指定されたユーザとデバイスの関連付けに対して CA Risk Authentication によって識別された成功したトランザクションの数を示します。

- **最初の成功したトランザクション**

  最初の成功したトランザクションが識別されるまでの期間（日数）を示します。

これらのパラメータは、ユーザとデバイスの関連付けの強さを決定します。ユーザがデバイスを少なくとも指定された日数の間使用しており、成功したトランザクションの数が設定された値以上である場合、Device User Maturity ルールは True を返します。

Device User Maturity ルールを作成する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。

4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。

5. ［**新しいルールの追加**］をクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。

6. 作成するルールの［**名前**］、［**ニーモニック**］、および［**説明**］を入力します。

7. このルールが適用可能な**チャネル**および**アクション**を選択します。

8. 以下のようにルール フラグメントを構築します。

   a. トランザクション エレメント リストから、［**USERNAME**］を選択します。

   b. デバイス エレメント リストから **Ctrl** キーを押しながら［**DEVICEID**］を選択します。

   c. ［**演算子の選択**］リストから［**MATURITY**］を選択します。

   d. 成功したトランザクションの数を指定します。

   e. 最初の成功したトランザクションが発生するまでの日数を指定します。

   f. ［**追加**］をクリックしてルール フラグメントを構築します。

9. ［ルール ビルダ］ページの下部にある［**作成**］をクリックして、ルールを作成します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

10. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

11. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

ルール ビルダを使用したルール定義の編集

このセクションでは、以下のルール定義に変更を加えるためのルール ビルダの使用方法について説明します。

- Untrusted IP Check
- User Velocity Check
- Device Velocity Check
- Zone Hopping Check
- Device MFP Not Match

信頼できない IP タイプの設定

CA Risk Authentication では、入力パラメータの 1 つとしてユーザのコンピュータの IP アドレスを使用して各トランザクションのリスクを評価します。 CA Risk Authentication は受信トランザクションを評価して、*信頼できない*としてマークが付けられている IP アドレスからの発信であるかどうかを確認します。そのようなトランザクションは通常拒否されます。信頼できない IP タイプのカテゴリは以下のとおりです。

- **拒否**

  これが指定されている IP アドレスは、過去に不正トランザクションの発信元となっていました。

  重要: 「信頼できない IP アドレスの設定 (P. 223)」で説明されているように、IP アドレスを拒否として手動で設定した場合は、このオプションを使用します。

- **アクティブ**

  これが指定されている IP アドレスは、不正トランザクションの発信元となったことがあり、過去 6 か月間アクティブであった匿名プロキシの疑いがあります。

- **要注意**

  これが指定されている IP アドレスは、過去 2 年にわたってアクティブであったが、過去 6 か月はアクティブではなかった匿名プロキシの疑いがあります。

- **ブライベート**

  これが指定されている IP アドレスは、公にアクセス可能でない匿名プロキシの疑いがあります。 これらのアドレスは、一般的に公に匿名サービスを販売する商業的企業に属しています。

- **非アクティブ**

  これが指定されている IP アドレスは、不正トランザクションの発信元となった疑いがあり、過去 2 年間は非アクティブであったことがわかっています。

- **Unknown**

  これが指定されている IP アドレスは、匿名プロキシの疑いがあり、現在それを否定する結果が得られていません。

  注: アクティブ、要注意、プライベート、非アクティブ、および不明の拒否タイプのカテゴリは、Quova データから派生しています。

組織に適用可能な信頼できない IP アドレスのタイプを設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**ルール名**］列で、［**Untrusted IP Check**］リンクをクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. ［**拒否 IP タイプ設定**］セクションで、拒否 IP アドレス カテゴリの適用可能なタイプを選択し、［**更新**］をクリックします。
7. ［ルール ビルダ］ページの下部にある［**更新**］をクリックして、変更を保存します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
8. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。
9. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

ユーザ頻度の設定

*User Velocity Check ルール*では、指定された期間のユーザからのトランザクション数のチェックを行います。 ルールは以下のパラメータに基づきます。

- ユーザごとのリスク評価の数

  アドバイスまたはリスク スコアに関係なく指定されたユーザのための CA Risk Authentication によって実行されたトランザクション（**N**）の数を示します。

  このパラメータのデフォルト値は **5** です。

- Time Interval

  トランザクションの数を追跡する期間（**T**）を示します。

  このパラメータのデフォルト値は **60** です。

- 時間間隔の単位

  測定される期間（**T**）の単位を示します。

  このパラメータのデフォルト値は**分**です。

User Velocity Check ルールを設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**ルール名**］列で、［**User Velocity Check**］リンクをクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. ［**次の値より大きい**］フィールド内のユーザあたりのリスク評価の数の値を指定します。
7. 時間間隔を指定します。

この値は、ユーザにとって安全であると考えられる（指定された時間内の）トランザクションの最大数を示します。 指定された時間内のトランザクションの実数がこの数を超えると、CA Risk Authentication はリスクとして追跡し、結果として User Velocity ルールと一致させます。

8. ドロップダウン リストから時間間隔の単位を選択します。
9. ［**更新**］をクリックしてルール フラグメントを構築します。
10. ［ルール ビルダ］ページの下部にある［**更新**］をクリックして、変更を保存します。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。
12. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

デバイス頻度の設定

*Device Velocity Check ルール*では、指定された期間のデバイスからのトランザクション数のチェックを行います。 ルールは以下のパラメータに基づきます。

- **デバイスごとのリスク評価の数**

  リスク評価の結果が成功または失敗であるかに関係なく、指定されたデバイスの CA Risk Authentication によって実行されたトランザクション（**M**）の数を示します。

  このパラメータのデフォルト値は **10** です。

- **Time Interval**

  トランザクションの数を追跡する期間（**T**）を示します。

  このパラメータのデフォルト値は **60** です。

- **時間間隔の単位**

  測定される期間（**T**）の単位を示します。

  このパラメータのデフォルト値は**分**です。

Device Velocity Check ルールを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイドバー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**ルール名**］列で、［**Device Velocity Check**］リンクをクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. ［**次の値より大きい**］フィールド内のデバイスあたりのリスク評価の数を指定します。
7. 時間間隔を指定します。

この値は、デバイスにとって安全であると考えられる（指定された時間内の）トランザクションの最大数を示します。 指定された時間内のトランザクションの実数がこの数を超えると、CA Risk Authentication はトランザクションをリスクとして追跡し、結果として Device Velocity ルールと一致させます。

8. ドロップダウン リストから時間間隔の単位を選択します。
9. ［**更新**］をクリックしてルール フラグメントを構築します。
10. ［ルール ビルダ］ページの下部にある［**更新**］をクリックして、変更を保存します。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。
12. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

ゾーン ホッピングの設定

ゾーン ホッピングは、短い時間の間に別々の離れた場所（かなりの距離で）で合理的に可能ではない速度で発生する、同じユーザからの連続のトランザクションを追跡します。たとえば、ボブが午前 9 時（GMT）にニューヨークからログインし、再度午前 10 時（GMT）にロンドンからログインした場合、Zone Hopping Check ルールは後者のトランザクションを危険として追跡します。

Zone Hopping Check ルールは、以下のパラメータに基づきます。

- **ユーザが移動できる最高速度**

  ユーザが飛行機、自動車、列車のような通常の交通手段を使用して、物理的に移動できる最高速度（**S**、時速マイル）を示します。

  （連続する 2 つのトランザクション間に）ユーザが移動したとみられる速度がこのあらかじめ設定されたしきい値速度（S）を超えた場合、CA Risk Authentication はそれを、ゾーン ホッピングとみなします。

  デフォルトでは、この値は 500 マイルですが、［CA Risk Authentication ルール ビルダ］ページの［**ユーザが移動できる最高速度**］フィールドの値を設定することにより設定できます。

- **同じユーザ ID を共有するユーザの最大数**

  複数のユーザ（たとえば夫婦）が、別々のゾーンに居るため、同じユーザ名を使用することがあります。 そのような場合、CA Risk Authentication がこれをゾーン ホッピングと見なさないようにする必要があります。 たとえば、夫が午前 10 時（GMT）にニューヨークからログインし、妻が午前 11 時（GMT）にロンドンからログインした場合、CA Risk Authentication はこれらのトランザクションを危険としてマークしません。

  デフォルトではこの値は **1** ですが、［CA Risk Authentication ルール ビルダ］ページの［同じユーザ ID を共有するユーザの最大数］フィールドを編集することにより、値を 2 に設定できます。

- **IP アドレスのロケーション間で許容される最大距離**

  ISP が提供する IP アドレスの場所にはばらつきがあるため、公の IP アドレスを使用してユーザの物理的な場所（地理緯度と経度）を厳密に特定することはできません。 これを解決するために、CA Risk Authentication では、不確実性の補正（**U**、マイル単位）を使用して、トランザクションの発信元である IP アドレスの物理的な場所におけるばらつきを調整します。

デフォルトでは、この値は 50 マイルですが、［CA Risk Authentication ルール ビルダ］ページの［**IP アドレスの場所の最大許容距離**］フィールドの値を設定することにより設定できます。

Zone Hopping Check ルールを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**ルール名**］列で、［**Zone Hopping Check**］リンクをクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. ［**ユーザが移動できる最大スピード**］パラメータの値を指定します。
7. ［**同じユーザ ID を共有するユーザの最大数**］パラメータの値を指定します。
8. ［**IP アドレスのロケーション間で許容される最大距離**］パラメータの値を指定します。
9. ［**更新**］をクリックします。
10. ［ルール ビルダ］ページの下部にある［**更新**］をクリックして、変更を保存します。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
11. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。
12. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

マシン フィンガープリント(MFP)一致率の設定

Device MFP Not Match ルールは、入力デバイスのシグネチャと対応する格納済みデバイス シグネチャの一致率が、指定された［シグネチャ一致しきい値］と［逆引きしきい値］以下であるかどうかを確認します。

Device MFP Not Match ルールを設定する方法

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイドバー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
4. ［**ルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
5. ［**ルール名**］列で、［**Device MFP Not Match**］リンクをクリックします。

   ［CA Risk Authentication ルール ビルダ］ページが表示されます。
6. ［**シグネチャ一致しきい値**］および［**逆引きしきい値**］の値を入力し、［**更新**］をクリックします。
7. ［ルール ビルダ］ページの下部にある［**更新**］をクリックして、変更を保存します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
8. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

ルールの削除

重要: 作成し展開した新規ルールのみを削除できます。 CA Risk Authentication に付属している既定のルールは削除できません。

展開したルールを削除するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. このページの［**検索**］ボタンをクリックして、組織のリストを表示します。
4. ［**変更する組織の選択**］の下で、ルールを削除する組織名のリンクをクリックします。
5. ［**CA Risk Authentication 設定**］タブをクリックします。
6. サイドバー メニューの［**ルール管理**］セクションで、［**ルールおよびスコアリング管理**］リンクをクリックします。

   ［ルールおよびスコアリング管理］ページが表示されます。
7. ［**ルール セットの選択**］リストから、この設定が適用可能なルールセットを選択します。

   ［ルールおよびスコアリング管理］ページが表示されます。
8. ［+］記号をクリックして削除するルールを展開します。
9. ［**このルールの削除**］をクリックします。

   メッセージが表示されます
10. ［**OK**］をクリックしてタスクを完了します。

    確認メッセージが表示されます。
11. ［**OK**］をクリックします。

    ルールが削除されたことを示すメッセージが候補設定領域に表示されます。 ただし、ルールは運用環境でまだアクティブであるため、引き続き［**アクティブ**］列にリスト表示されます。
12. 運用環境からルールを削除するには、設定の変更を運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。
13. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

ルールが削除されます。

この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

ルール リスト データのアップロード

重要: このセクションで説明するすべての設定およびタスクは、主に組織管理者が実行する必要があります。 組織固有の設定を行うためにタスクページにアクセスする場合の詳細については、「組織固有の CA Risk Authentication 設定へのアクセス」を参照してください。
必要に応じて、グローバル管理者もこれらの手順を実行できます。 ただし、［組織］タブを使用して組織レベルで実行する必要があります。

展開したルールにリスト形式の追加データが必要な場合、このセクションのタスクを実行する必要があります。CA Advanced Authentication で［リスト データおよびカテゴリ マッピングの管理］ページを使用することにより、リスト データを追加、変更、削除できます。 このセクションでは、以下のリストのデータを管理する方法について説明します。

- 拒否国リスト
- アントラステッド IP リスト
- トラステッド IP リスト
- トラステッド アグリゲータ リスト
- データ リスト
- カテゴリ マッピング リスト

拒否対象国リストの設定

拒否対象国リストは、不正または悪意のあるトランザクションが過去に発信されたと知られている国をすべて含みます。 企業は、その国の規制に沿ってこのリストを保持することもできます。

CA Risk Authentication では、入力 IP アドレスに基づいて国情報を導き出します。 その後、このデータを使用して、そのような国から発信されたオンライン トランザクションの不正の可能性をスコアリングします。 このため、CA Risk Authentication では Quova と統合し、各 IP アドレスの詳細な地理情報を領域にマッピングすることによって提供して、分析を強化します。

Quova とそのサービスの詳細については、以下のサイトを参照してください。

http://www.quova.com

CA Risk Authentication では受信トランザクションを評価し、これらのトランザクションが拒否対象としてマークが付けられた国に属している IP アドレスから発信されているかどうかを確認します。 そのようなトランザクションは通常拒否されます。

［リスト データおよびカテゴリ マッピングの管理］ページを使用して、国を拒否国リストに追加するかまたはリストから削除します。

拒否国リストを更新する方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］で、［**組織の検索**］リンクをクリックします。
4. ［組織の検索］ページの［**検索**］ボタンをクリックして、組織のリストを表示します。
5. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
6. ［**CA Risk Authentication 設定**］タブをクリックします。
7. サイドバー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。

8. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。
9. ［**リスト データを管理**］オプションを選択します。
10. ［**リスク タイプの選択**］リストから、［**拒否対象国リスト**］を選択します。
11. ［**リストの選択**］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。
12. リストに追加する**拒否国を選択します**。
13. ［>］または［<］ボタンをクリックして、選択した国を目的のリストに移動します。

    また、すべての国を対象のリストに移動するには、**>>** または **<<** ボタンをクリックします。
14. ［**保存**］をクリックすると、変更内容が保存されます。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
15. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

信頼できない IP アドレスの設定

*アントラステッド IP リスト*は、過去に既知のアノニマイザ プロキシまたは不正行為や悪意のあるトランザクションの発信元となった IP アドレスの集合体です。 このリストは、「信頼できない IP タイプの設定 (P. 210)」で説明されている拒否カテゴリのソースです。

［リスト データおよびカテゴリ マッピングの管理］ページを使用して、組織の信頼できない IP アドレス範囲を設定します。

IP アドレス範囲の追加または削除

組織の信頼できない IP アドレスおよび範囲を追加または削除する方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］で、［**組織の検索**］リンクをクリックします。
4. ［組織の検索］ページの［**検索**］ボタンをクリックして、組織のリストを表示します。
5. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
6. ［**CA Risk Authentication 設定**］タブをクリックします。
7. サイドバー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
8. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   ルール セット設定情報が表示されます。
9. ［**リスト データを管理**］オプションを選択します。
10. ［**リスク タイプの選択**］リストから、［**アントラステッド IP リスト**］を選択します。
11. ［**リストの選択**］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。
12. ［**信頼されていない IP 範囲のアップロード**］セクションで、データを書き込む際の適切なモードを選択します。

- **追加**： このオプションは、アップロードするデータをリストまたはデータセットに追加します。

  注: リストが存在しない場合は、このオプションを選択する必要があります。

- ［**置換**］: このオプションは、指定されたリストまたはデータ セットの既存のデータを上書きします。

13. **参照**ボタンをクリックし、エントリのリストを含むデータ ファイルに移動します。
14. ［**アップロード**］をクリックしてタスクを完了します。
15. ［**信頼されていない IP 範囲の追加/削除**］セクションで、以下の操作を実行します。
    a. ［**IP アドレス**］フィールドに開始 IP アドレスを入力します。
    b. 以下のいずれかのオプションを選択します。
       - **サブネット マスク**： サブネット マスクに基づいてアントラステッド IP リストに追加される IP アドレスの範囲を指定する場合。
       - **終了 IP アドレス**： アントラステッド IP リストに追加される IP アドレスの単純な範囲を指定する場合。
    c. 信頼できない IP アドレス範囲の**情報ソース**（またはベンダー）を指定します。
16. 必要に応じて、以下のいずれかのボタンをクリックします。
    - ［**範囲を追加**］： 指定された IP アドレスまたは範囲をデータベースに追加する場合。
    - ［**範囲を削除**］： データベースから指定された IP アドレスまたは範囲を削除する場合。

    対応するメッセージが表示されます。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
17. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド IP アドレスの設定

CA Risk Authentication では、*トラステッド IP アドレス リスト*に属している IP アドレスまたは範囲から発信されるか、これらを経由するトランザクションは低リスクと考えます。 その結果、CA Risk Authentication は、これらのトランザクションのリスク評価を省略し、低いスコアと ALLOW アドバイスを割り当てます。

［リスト データおよびカテゴリ マッピングの管理］ページを使用して、トラステッド IP アドレスおよび範囲と関係する以下のタスクを実行します。

- トラステッド IP アドレス範囲の追加
- トラステッド IP アドレス範囲の追加
- トラステッド IP アドレス範囲の追加

トラステッド IP アドレス範囲の追加

トラステッド IP アドレスまたは範囲を追加するには、以下のタスクを実行します。

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］で、［**組織の検索**］リンクをクリックします。
4. ［組織の検索］ページの［**検索**］ボタンをクリックして、組織のリストを表示します。
5. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
6. ［**CA Risk Authentication 設定**］タブをクリックします。
7. サイド バー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
8. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   ルール セット設定情報が表示されます。
9. ［**リスト データを管理**］オプションを選択します。

10. ［**リスク タイプの選択**］リストから、［**トラステッド IP リスト**］を選択します。
11. ［**リストの選択**］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。
12. ［トラステッド IP リスト］に追加される必要な［**IP Address**］を指定します。
13. 以下のいずれかを指定します。
    - **サブネット マスク**：サブネット マスクに基づいて［トラステッド IP リスト］に追加される IP アドレスの範囲を指定する場合。
    - **終了 IP アドレス**：トラステッド IP リストに追加される IP アドレスの単純な範囲を指定する場合。
14. ［**範囲を追加**］をクリックして、IP アドレスまたは範囲を［トラステッド IP リスト］に追加します。

    追加した範囲の［トラステッド IP リスト］テーブルが、ページの最後に表示されます。
15. ［**更新**］をクリックすると、変更が保存されます。

    変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
16. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド IP アドレス範囲の追加

トラステッド IP アドレスまたは範囲を更新する方法

1. 「トラステッド IP アドレス範囲の追加」の手順 1 ～ 11 のタスクを実行して、［**トラステッド IP リスト**］テーブルを表示します。
2. ［**トラステッド IP リスト**］テーブルで必要な変更を加えます。
3. ［**トラステッド IP リスト**］テーブルで影響を受けた IP アドレスの範囲をすべて選択します。
4. ［**更新**］をクリックして加えた変更を更新します。

   変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。
5. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド IP アドレス範囲の追加

トラステッド IP アドレスまたは範囲を追加するには、以下のタスクを実行します。

1. 「トラステッド IP アドレス範囲の追加」の手順 1 ～ 11 のタスクを実行して、［**トラステッド IP リスト**］テーブルを表示します。
2. ［**トラステッド IP リスト**］テーブルで、削除が必要な IP アドレス範囲を選択します。
3. ［**削除**］をクリックして選択した範囲を削除します。
4. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド アグリゲータの設定

アグリゲータは、複数の企業にわたってユーザのログイン情報を照合することによりアカウント集約サービスを提供するサードパーティ ベンダーです。保護されたポータルからユーザがログインした場合と、アグリゲータ経由でアクセスした場合とでは、送信元 IP アドレスが異なります。 多くの企業が、これらのアカウントとデータの集約サービス プロバイダのサービスを使用し、オンライン サービスの範囲を拡大しています。

組織に「信頼されている」アグリゲータが発信元である（または経由している）トランザクションは低リスクであると考えられます。 このため、CA Risk Authentication では、これらのアグリゲータのリストを設定する機能を提供し、アグリゲータの IP アドレスが発信元となっているすべてのトランザクションに低いスコアおよび ALLOW アドバイスを割り当てるようにします。

CA Risk Authentication は、IP アドレス範囲と一意のアグリゲータ ID を組み合わせることにより、一意にアグリゲータを識別します。このアグリゲータ ID もトランザクションと共に CA Risk Authentication に送信される必要があります。

また CA Risk Authentication では、各アグリゲータにつき *3* つまでの一意の ID をいつでも指定できます。 これにより、セキュリティを強化する目的で ID を定期的にローテーションすることができます。 このローテーション中に、CA Risk Authentication は、アグリゲータで後で更新できるように、新しい ID に加えて前の ID を引き続き認識します。

［リスト データおよびカテゴリ マッピングの管理］ページを使用して、トラステッド アグリゲータと関係する以下のタスクを実行します。

- トラステッド アグリゲータの追加
- トラステッド アグリゲータの更新
- トラステッド アグリゲータの削除

トラステッド アグリゲータの追加

トラステッド アグリゲータを追加するには、以下のタスクを実行します。

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］で、［**組織の検索**］リンクをクリックします。

4. ［組織の検索］ページの［**検索**］ボタンをクリックして、組織のリストを表示します。
5. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
6. ［**CA Risk Authentication 設定**］タブをクリックします。
7. サイドバー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
8. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   ルール セット設定情報が表示されます。
9. ［**リスト データを管理**］オプションを選択します。
10. ［**リスク タイプの選択**］リストから、［**トラステッド アグリゲータ リスト**］を選択します。
11. ［**リストの選択**］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。
12. ［**新規アグリゲータの追加**］フィールドで新しいアグリゲータの名前を指定し、［**作成**］をクリックします。

    更新された［トラステッド アグリゲータ設定］ページが表示されます。
13. 設定する［**アグリゲータ**］をドロップダウン リストから選択します。
14. ［**IP アドレス**］フィールドに開始 IP アドレスを入力します。
15. 以下のいずれかのオプションを選択します。
    - **サブネット マスク**：サブネット マスクに基づいて［トラステッド アグリゲータ リスト］に追加される IP アドレスの範囲を指定する場合。
    - **終了 IP アドレス**: トラステッド アグリゲータ リストに追加される IP アドレスの単純な範囲を指定する場合。
16. ［**範囲を追加**］をクリックしてこの IP アドレスまたは範囲をデータベースに追加します。

    アグリゲータに追加した範囲の［トラステッド IP リスト］テーブルが、ページの最後に表示されます。

変更はまだアクティブではなく、エンドユーザに利用可能ではありません。

17. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

    詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド アグリゲータの更新

CA Risk Authentication ではアグリゲータ ID を更新できます。 これらの ID の定期的な更新は、アグリゲータ ID のローテーションと呼ばれています。

重要: セキュリティ目的にアグリゲータ ID の定期的なローテーションまたは変更が推奨されます。 このローテーション期間はビジネス ルールに応じて決定できます。

ID が更新された後、最新のアグレゲータ ID がアグリゲータに伝えられていることを確認する必要があります。 アグリゲータ ID の伝達には遅延が生じる場合があります。 この期間、CA Risk Authentication は、新しいアグリゲータ ID と同様に古い ID も IP アドレスに関連付けられていることを認識します。

注: アグリゲータ側から始まるトランザクションには、CA Risk Authentication API によって指定された形式でこのアグリゲータ ID が含まれている必要があります。

アグリゲータ ID を更新する方法

1. 「トラステッド アグリゲータの追加」の手順 1 ～ 11 を完了して、トラステッド アグリゲータの設定情報を表示します。
2. ［**アグリゲータ**］リストから既存のアグリゲータを選択します。

   トラステッド アグリゲータの設定情報に、選択されたアグリゲータのアグリゲータ ID が表示されます。
3. ［**アグリゲータ ID の更新**］をクリックして新しい Aggregator ID を生成します。

   アグリゲータの更新されたアグリゲータ ID が表示され、次の空のアグリゲータ ID が表示されます。
4. ［**トラステッド IP リスト**］テーブルで、更新するアグリゲータ IP アドレスまたは範囲を選択します。
5. 必要な変更を加え、［**更新**］をクリックします。

変更はまだアクティブではなく、エンドユーザに利用可能ではありません。

6. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

トラステッド アグリゲータの削除

トラステッドアグリゲータを追加するには、以下のタスクを実行します。

1. 「トラステッドアグリゲータの追加」の手順 1 ～ 11 を完了して、トラステッドアグリゲータの設定情報を表示します。
2. ［**アグリゲータ**］リストから既存のアグリゲータを選択します。

   トラステッドアグリゲータの設定情報が表示されます。
3. ［**トラステッド IP リスト**］テーブルで、削除するアグリゲータ IP アドレスまたは範囲を選択します。
4. ［**削除**］をクリックして、選択した情報を削除します。

   変更はまだアクティブではなく、エンドユーザに利用可能ではありません。
5. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

   詳細については、「運用環境への移行 (P. 236)」を参照してください。

リスト データのアップロード

IN_LIST 演算子を使用するルールのデータをアップロードする方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］で、［**組織の検索**］リンクをクリックします。
4. ［組織の検索］ページの［**検索**］ボタンをクリックして、組織のリストを表示します。
5. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
6. ［**CA Risk Authentication 設定**］タブをクリックします。
7. サイドバー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
8. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。
9. ［**リスト データを管理**］オプションを選択します。
10. ［**リスク タイプの選択**］リストから、［**その他のリスト**］を選択します。
11. ［**リストの選択**］ドロップダウン リストから、対応するリストの作成中に指定したリスト識別子を選択します。

    更新されたページが表示されます。
12. ［**ファイルをアップロード、またはデータを入力します**］セクションで、データを書き込む際の適切なモードを選択します。
    - **追加**： このオプションは、アップロードするデータをリストまたはデータセットに追加します。

      注: リストが存在しない場合は、このオプションを選択する必要があります。
    - ［**置換**］: このオプションは、指定されたリストまたはデータ セットの既存のデータを上書きします。
13. 以下の*いずれか*の操作を行います。
    - ［**参照**］をクリックし、改行文字によって区切られたエントリのリストを含むデータ ファイルに移動します。

または

- データ ファイルが存在しない場合は、［**データを入力**］フィールドにエントリを入力します。

  重要: エントリが改行文字（ENTER）で区切られていることを確認します。

14. ［**アップロード**］をクリックしてタスクを完了します。

カテゴリ マッピング データのアップロード

IN_CATEGORY 演算子を使用するルールのデータをアップロードする方法

1. GA としてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. このページの［**検索**］ボタンをクリックして、組織のリストを表示します。
4. ［**変更する組織の選択**］の下で、ルールを適用する組織名のリンクをクリックします。
5. ［**CA Risk Authentication 設定**］タブをクリックします。
6. サイド バー メニューの［**ルール管理**］セクションで、［**リスト データおよびカテゴリ マッピングの管理**］リンクをクリックします。

   ［リスト データおよびカテゴリ マッピングの管理］ページが表示されます。
7. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   指定されたルール セットの設定情報が表示されます。
8. ［**カテゴリ マッピングの管理**］オプションを選択します。
9. ［**カテゴリ マッピングを選択**］リストから、対応するリストの作成中に指定したマッピング セット識別子を選択します。

   更新されたページが表示されます。
10. ［**ファイルをアップロードするか、分類データを入力します**］セクションで、データを書き込む際の適切なモードを選択します。
    - **追加**： このオプションは、アップロードするデータをリストまたはデータセットに追加します。

      注: リストが存在しない場合は、このオプションを選択する必要があります。
    - ［**置換**］: このオプションは、指定されたリストまたはデータ セットの既存のデータを上書きします。
11. 以下のいずれかを実行します。
    - ［**参照**］をクリックし、改行文字によって区切られたエントリのリストを含むデータ ファイルに移動します。

      または

- データ ファイルが存在しない場合は、［**データを入力**］フィールドにエントリを入力します。

  重要: エントリが改行文字（ENTER）で区切られていることを確認します。

12. ［**アップロード**］をクリックしてタスクを完了します。

運用環境への移行

CA Risk Authentication には、以下のルールおよび設定の**デフォルトの**設定が付属しています。

- トラステッド IP アドレスおよびアグリゲータ
- 信頼できない IP アドレス
- 拒否国リスト
- Exception User
- Unknown User
- Device MFP Not Match
- User Velocity
- Unknown DeviceID
- User Not Associated with DeviceID
- Device Velocity
- Zone Hopping
- その他のルール設定
- スコアリング

さらに、以下を設定することもできます。

- 新規ルール
- コールアウト

前のリストに関連するデータを設定する場合、そのデータは*提示データ*と呼ばれます。 このデータは、ある期間において、複数の管理セッションで作成できます。 このデータを設定している場合、このデータは**提示設定**領域に保存され、対応する設定ページの［**候補**］列に反映されます。 その結果、［**候補**］列に加えられた変更がこのデータに反映されます。

ユーザの要件に従ってすべてのデータを設定したら、そのデータを運用環境に移行し、CA Risk Authentication サーバ キャッシュをリフレッシュすることで、提示データを*アクティブ データ*（対応する設定ページの［**アクティブ**］列）に変換できます。 詳細については、「arrfclient： サーバ リフレッシュとシャットダウン ツール」を参照してください。

注: 任意の時点で、CA Risk Authentication サーバはアクティブ データの設定*のみ*を使用して動作するようになります。

提示データがアクティブ データに移行された後に再度データを設定すると、提示設定領域にアクティブ データのコピーが作成されます。 設定を運用環境に移行する準備ができるまで、さらに提示データの追加および削除を実行できます。 すべての変更は提示データのみに反映されます。 ただし、レポートはアクティブな設定または提示設定として表示することができます。

注: CA Risk Authentication の設定データに対する変更を記録するため、アクティブ データではバージョン管理が行われます。 提示データが運用環境に移行されるたびに、新しいアクティブ設定データ セットに一意のデータ バージョンが作成されます。

提示設定領域からアクティブ データ領域に変更を移行する方法

1. GA または OA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイド バー メニューの［**実稼働にマイグレート**］セクションの下で、［**実稼働にマイグレート**］リンクをクリックします。

   ［実稼働にマイグレート］ページが表示されます。
4. このページで、以下のいずれかを実行します。
   - すべての設定済みのルール セットに対して行ったすべての変更を移行する場合は、［**すべてのルール セットの選択**］オプションをオンにします。

     または
   - 現在のルール セットに対して行った変更を移行する場合は、［**ルール セットの選択**］リストから特定のルール セットを選択します。
5. ［**マイグレート**］をクリックします。

   アクションを確認するページが表示されます。
6. 確認ページで［**確認**］をクリックし、*移行処理*を開始します。

   注: 運用環境に移行するデータ量によっては、移行処理に数分かかる場合があります。

   移行が完了すると、「提案されたデータは、実稼働に正常にマイグレートされました。」というメッセージが表示されます。
7. CA Risk Authentication サーバのキャッシュをリフレッシュします。 この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

第 9 章: コールアウトの設定

重要: このセクションで説明されているすべての設定およびタスクは、**グローバル管理者**がルールを全体的に適用したり、**組織管理者**が組織にルールを適用する場合に実行できます。

組織に固有の設定を実行するためのタスク ページにアクセスする方法の詳細については、「組織固有の CA Risk Authentication の設定の管理」を参照してください。

*コールアウト*は、CA Risk Authentication の標準的な機能を変更または拡張するためのカスタム コンポーネント（任意のプログラミング言語で記述可能）です。 コールアウトは通常、外部プロセスです。 つまり、コールアウトは CA Risk Authentication サーバ コンテキストの「外部」に存在し、別の HTTPS ベースのサーバでホストされます。 外部プロセスであるため、コールアウトは CA Advanced Authentication を使用して設定する必要があります。設定することにより、必要に応じて起動できるようになります。

このセクションでは、CA Risk Authentication がサポートするコールアウトのタイプ、およびビジネス要件を満たすコールアウトを設定する方法について説明します。 さらに、CA Risk Authentication パッケージに同梱されているサンプル コールアウトの展開、設定、および使用方法についても説明します。

- コールアウトについて (P. 240)
- コールアウトの設定 (P. 245)
- サンプル コールアウトでの作業 (P. 250)

注: 設定関連のアクティビティを実行する管理者にこれらの操作を実行するために必要な権限があることを確認します。 各レベルの管理者が使用可能な権限の詳細については、「管理権限の要約」を参照してください。

コールアウトを設定した後、変更はすぐに**アクティブ**（エンド ユーザに利用可能）にはなりません。**提示された**設定変更を運用環境データベースにすべて「移動」するには、CA Advanced Authentication のサイド バー メニューの［**実稼働にマイグレート**］リンクを使用する*必要があります*。運用環境に移行する手順については、「運用環境への移行」を参照してください。

コールアウトについて

ビジネス要件に基づいて、独自のカスタム評価ロジックおよびスコアリング ロジックを作成することができます。実装した場合、CA Risk Authentication サーバとは関係なく、アプリケーション側で実行されます。これらのカスタム評価またはスコアリング プログラムは、アプリケーションのバックエンド システムとの対話用に実装できる**コールアウト**としても知られています。

注: CA Risk Authentication には、簡易評価コールアウトおよびスコアリング コールアウトを作成して実装する方法を示す基本的なサンプル コールアウト WAR ファイル（riskfort-8.0-sample-callouts.war）が同梱されています。このファイルを展開して設定する方法の詳細については、「サンプル コールアウトでの作業」を参照してください。

たとえば金融機関では、各トランザクションの発信元の追跡に加えて、トランザクションの金額に基づいた通常の銀行取引と電信送金のリスクの評価も希望します。 銀行はトランザクションが普通取引であるか電信送金であるかに関係なく、30,000 ドル以上のトランザクションすべてのリスクを評価します。 この場合、CA Risk Authentication の拒否国、信頼できない IP、ゾーン ホッピング、および頻度チェックの使用に加えて、金融機関は評価コールアウト（アプリケーションの範囲内で）を作成することでこの動作を追跡することができます。

注: コールアウトが展開されたら、［コールアウト設定］ページを使用してコールアウトを有効にする*必要があります*。

コールアウトの実装

注: コールアウトの実装はオプションです。

コールアウトを実装した場合、CA Risk Authentication サーバはデータベースからコールアウトに関連する設定をすべて読み取り、スタートアップ時に情報をキャッシュします。 トランザクションの間、以下の操作が行われます。

1. CA Risk Authentication サーバは、事前定義済みルールと新規ルール（評価コールアウトの場合）または標準的なスコアリング エンジン（スコアリング コールアウトの場合）をすべて実行した*後に*コールアウト フレームワークを呼び出します。

   注: コールアウト フレームワークは CA Risk Authentication サーバの一部で、その他の CA Risk Authentication 評価ルールと同様に、サーバのスタートアップ中にロードされます。これは .dll または .so ファイルとして実装されます。

2. フレームワークは、コールアウトのタイプ（**評価**または**スコアリング**）に応じて CA Risk Authentication サーバから必要なデータをすべて収集し、HTTP または HTTPS データを準備します。

   注: CA Risk Authentication では、HTTPS データの場合に CA Risk Authentication サーバとコールアウトの間で一方向および双方向の両方の SSL ベース接続をサポートしています。

3. その後、このデータはコールアウトの（設定されている） URL に投稿されます（HTTP または HTTPS）。

   これで、コールアウト フレームワークはコールアウトからのレスポンスを待ちます。

   評価コールアウトからのレスポンスが指定されたタイムアウト期間内に受信された場合、フレームワークはレスポンスを解析し、CA Risk Authentication サーバに結果を送信します。

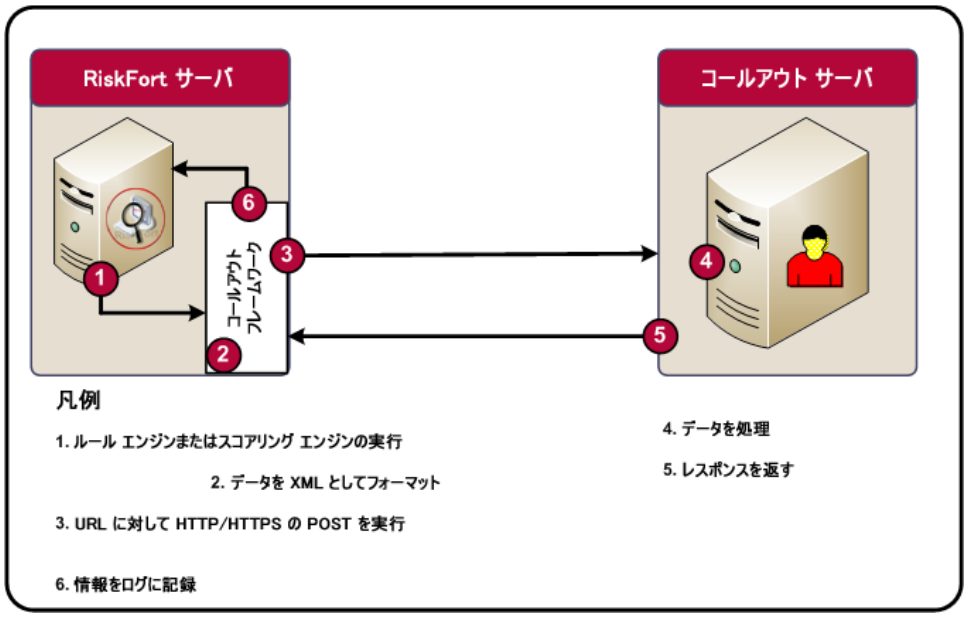
   レスポンスが指定されたタイムアウト期間内に受信されなかった場合、フレームワークは、ルールの結果として FAILURE を返し、修飾子と注釈には空の文字列（""）を返します。

   注: タイムアウト期間は CA Advanced Authentication を使用することによって設定できます。

4. コールアウトではカスタム ロジックを使用してデータを処理します。

5. その後、コールアウトはコールアウト フレームワークに適切なレスポンスを返し、コールアウト フレームワークは CA Risk Authentication サーバに同じレスポンスを転送します。
6. CA Risk Authentication サーバは、レポートおよび監査目的のためにフレームワークによって返された情報をすべてログに記録します。

以下の図は、CA Risk Authentication サーバ、コールアウト フレームワーク、およびユーザのコールアウトの間の対話を示します。



注: スコアリング コールアウトと同様に評価コールアウトも実装している場合は、それらを同じサーバ、または別々のサーバに実装することができます。

コールアウトのタイプ

CA Risk Authentication では、以下のタイプのコールアウトをサポートしています。

- 評価コールアウト
- スコアリング コールアウト

評価コールアウト

評価コールアウトはリスク評価の一部として実行されます。 評価コールアウトが実装された場合

1. CA Risk Authentication はスタンドアロンおよび組み合わせルールをすべて実行し、コールアウト フレームワークを呼び出します。
2. CA Risk Authentication コールアウト フレームワークは、XML 形式でデータをフォーマットします。
3. CA Risk Authentication コールアウト フレームワークは、評価コールアウトに以下の情報の HTTP または HTTPS POST を実行します。
   - 各 CA Risk Authentication 評価ルールに渡される**コンテキスト情報**（ユーザ名、IP アドレスおよびデバイス ID など）。
   - 実行された各評価ルールの**ルール結果**。
   - CA Risk Authentication SDK から CA Risk Authentication サーバに入力データとして提供された**追加の入力**（ある場合）。
4. コールアウトでは、カスタム ロジックを処理するために CA Risk Authentication によって渡されたデータを使用します。
5. その後、コールアウトは CA Risk Authentication に以下の情報を返します。
   - Y （SUCCESS）または N （FAILURE）の形式による**ルール結果**。
   - スコアリング コールアウト（実装されている場合）によって使用される追加の情報（ある場合）を持つ**修飾子文字列**。

   注: CA Risk Authentication サーバは修飾子文字列を一切処理しません。スコアリング コールアウトも実装されている場合、CA Risk Authentication サーバはこのデータをスコアリング コールアウトに投稿します。
   - CA Risk Authentication サーバに送り返された理由または説明が含まれている**注釈文字列**。

   注: この情報は、ログ（データベースで）、レポート、および監査目的に使用されます。
6. CA Risk Authentication サーバは、コールアウトによって返された情報をログに記録します。

スコアリング コールアウト

*スコアリング コールアウト*は標準的な CA Risk Authentication スコアリング ロジックが実行された*後*で実行されます。 スコアリング コールアウトが実装された場合

1. CA Risk Authentication サーバは標準的なスコアリング プログラムを実行し、コールアウト フレームワークを呼び出します。
2. CA Risk Authentication コールアウト フレームワークは、XML 形式でデータをフォーマットします。
3. CA Risk Authentication コールアウト フレームワークは、スコアリング コールアウトに以下の情報の HTTP または HTTPS POST を実行します。
   - 標準的な CA Risk Authentication ビルトイン スコアリング エンジンによって計算された**全体のスコア**。
   - 実行された各評価ルールの**ルール結果**。
   - evaluateRisk() API 呼び出しの一部として呼び出し元アプリケーションによって提供された**追加の入力**（ある場合）。
   - 評価コールアウトによって最初に返された**修飾子文字列**。
4. コールアウトでは、カスタム ロジックを処理するために CA Risk Authentication によって渡されたデータを使用します。
5. その後、コールアウトは CA Risk Authentication に以下の情報を返します。
   - ［0 ～100］の範囲で整数の形式による**最終スコア**。

   注: スコアリング コールアウトによって返されたスコアは、CA Risk Authentication スコアリング エンジンによって計算されたスコアを常に上書きします。 CA Risk Authentication の標準的なスコアリング エンジンによって計算されたスコアを保持する場合は、レスポンスの戻り値と同じスコアを渡す必要があります。
   - CA Risk Authentication サーバに送り返された理由または説明が含まれている**注釈文字列**。 たとえば、注釈フィールドにスコアを変更する理由を入力することができます。

   注: この情報は、ログ（データベースで）、レポート、および監査目的に使用されます。
6. CA Risk Authentication サーバは、コールアウトによって返された情報をログに記録します。

コールアウトの設定

［コールアウト設定］ページを使用して以下を実行します。

- 評価コールアウトの設定
- スコアリング コールアウトの設定

注: CA Risk Authentication には、評価コールアウトおよびスコアリング コールアウトを作成して実装する方法を示す基本的なサンプル コールアウト WAR ファイルが同梱されています。 このファイルを展開して設定する方法の詳細については、「サンプル コールアウトでの作業」を参照してください。

評価コールアウトの設定

評価コールアウトを設定するには、以下の手順に従います。

1. GA としてログインしていることを確認します。
2. ［**サービスおよびサーバの設定**］タブをアクティブにします。
3. サイドバー メニューの［**ルール管理**］で、［**コールアウト設定**］リンクをクリックします。

   ［コールアウト設定］ページが表示されます。
4. ［**評価コールアウト**］オプションが選択されていることを確認し、［**次へ**］をクリックします。

   ［評価コールアウト設定］ページが表示されます。
5. ［**既存のルール セットの選択**］リストから、この設定が適用可能なルール セットを選択します。

   更新された［評価コールアウト設定］ページが表示されます。
6. 表の［**候補**］列で、以下の手順を実行します。
   a. ［**サーバ認証 SSL**］で適切な SSL オプションを選択します。

      重要: CA Risk Authentication サーバとコールアウトの間に SSL ベースの通信を設定する場合は、［**はい**］を選択する必要があります。
   b. ［**クライアント認証 SSL**］で適切な SSL オプションを選択します。

      注: このクライアントはユーザのコールアウトです。

      - CA Risk Authentication サーバとコールアウトの間に双方向 SSL 接続を設定する場合は［**はい**］を選択し、**サーバ認証 SSL** も［**はい**］に設定します。
      - CA Risk Authentication サーバとコールアウトの間に一方向 SSL 接続を設定する場合は、［**いいえ**］を選択します。この場合、**サーバ認証 SSL** が［**はい**］に設定されていることを確認してください。
      - SSL ベースの接続を設定しない場合は［**いいえ**］を選択する必要があります。この場合、**サーバ認証 SSL** も［**いいえ**］に設定しておく必要があります。

   c. ［**コールアウト URL**］に、コールアウトの URL を指定します。

      - **サーバ認証 SSL** が［**はい**］に設定されているか、または**クライアント認証 SSL** が［**はい**］に設定されている場合、評価コールアウトの URL は *https://*から始まる必要があります。

- **サーバ認証 SSL** が［**いいえ**］に設定されていて、かつ**クライアント認証 SSL** も［**いいえ**］に設定されている場合、評価コールアウトの URL は *http://*から始まる必要があります。

d. ［**接続タイムアウト**］の値をミリ秒単位で指定します。

［*接続タイムアウト*］は、CA Risk Authentication サーバとユーザのコールアウトの間の接続が期限切れになるまでの時間を示します。

e. ［**読み取りタイムアウト**］の値をミリ秒単位で指定します。

［*読み取りタイムアウト*］は、CA Risk Authentication サーバがユーザのコールアウトからのレスポンスが戻るまでの予測時間を示します。

f. ［**参照**］をクリックして**コールアウト サーバのルート証明書**が配置されている場所へ移動します。

注: 以下の点に注意してください。
- ［**サーバ認証 SSL**］が［はい］に設定されているか、**クライアント認証 SSL** が［はい］に設定されている場合は、**コールアウト サーバ ルート証明書**を指定する*必要があります*。

- **コールアウト サーバ ルート証明書**は PEM （Base64 にエンコードされた）形式である*必要があります*。

g. ［**参照**］をクリックして **CA Risk Authentication サーバ証明書および秘密キー**が配置されている場所に移動します。

注: 以下の点に注意してください。
- ［**クライアント認証 SSL**］が［はい］に設定されている場合、**コールアウト サーバ ルート証明書**および **CA Risk Authentication サーバ証明書および秘密キー**を指定する*必要があります*。

- **CA Risk Authentication サーバ証明書および秘密キー**は PEM （Base64 にエンコードされた）形式である*必要があります*。

h. ［**コールアウトの説明**］に、コールアウトに関する有用な詳細を指定します。

7. ［**保存**］をクリックして変更を保存します。

変更はまだアクティブではなく、エンド ユーザに利用可能ではありません。

8. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

詳細については、「運用環境への移行 (P. 236)」を参照してください。

9. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

スコアリング コールアウト

*スコアリング コールアウト*は標準的な CA Risk Authentication スコアリング ロジックが実行された*後*で実行されます。 スコアリング コールアウトが実装された場合

1. CA Risk Authentication サーバは標準的なスコアリング プログラムを実行し、コールアウト フレームワークを呼び出します。
2. CA Risk Authentication コールアウト フレームワークは、XML 形式でデータをフォーマットします。
3. CA Risk Authentication コールアウト フレームワークは、スコアリング コールアウトに以下の情報の HTTP または HTTPS POST を実行します。
   - 標準的な CA Risk Authentication ビルトイン スコアリング エンジンによって計算された**全体のスコア**。
   - 実行された各評価ルールの**ルール結果**。
   - evaluateRisk() API 呼び出しの一部として呼び出し元アプリケーションによって提供された**追加の入力**（ある場合）。
   - 評価コールアウトによって最初に返された**修飾子文字列**。
4. コールアウトでは、カスタム ロジックを処理するために CA Risk Authentication によって渡されたデータを使用します。
5. その後、コールアウトは CA Risk Authentication に以下の情報を返します。
   - ［0 ～100］の範囲で整数の形式による**最終スコア**。

   注: スコアリング コールアウトによって返されたスコアは、CA Risk Authentication スコアリング エンジンによって計算されたスコアを常に上書きします。 CA Risk Authentication の標準的なスコアリング エンジンによって計算されたスコアを保持する場合は、レスポンスの戻り値と同じスコアを渡す必要があります。
   - CA Risk Authentication サーバに送り返された理由または説明が含まれている**注釈文字列**。 たとえば、注釈フィールドにスコアを変更する理由を入力することができます。

   注: この情報は、ログ（データベースで）、レポート、および監査目的に使用されます。
6. CA Risk Authentication サーバは、コールアウトによって返された情報をログに記録します。

サンプル コールアウトでの作業

CA Risk Authentication 8.0 には、非 GUI のサンプル コールアウト WAR ファイル（CA Risk Authentication-3.1.01-sample-callouts.war）が同梱されています。これは以下に対するサンプルを提供します。

- カスタム プログラムからの CA Risk Authentication サーバの基本的な操作（呼び出しと後処理）。
- コールアウトの CA Risk Authentication との統合。

このサンプル コールアウト WAR ファイルは、CA Risk Authentication の**完全**インストールの一部として自動的にインストールされます。 **カスタム** インストールの一部として、この WAR ファイルにアクセスするには **CA Risk Authentication サーバ** コンポーネントを選択する必要があります。

重要: サンプル コールアウトは CA Risk Authentication サーバがインストールされている同じアプリケーション サーバ上で展開する*必要があります*。

このセクションでは、次の項目について説明します。

- サンプル コールアウトの展開
- サンプル コールアウトと通信するための CA Risk Authentication サーバの設定

サンプル コールアウトの展開

このセクションでは、サンプル コールアウトを展開するための手順について説明します。

- Windows の場合
- UNIX ベースのプラットフォームの場合

Windows の場合

CA Risk Authentication に同梱されているサンプル コールアウトをアプリケーション サーバに展開する方法

1. ［設定］-［コントロール パネル］-［管理ツール］-［サービス］に移動します。
2. アプリケーション サーバ サービスを停止します。
3. riskfort-3.1.01-sample-callouts.war ファイルを以下の場所から展開します。
   `<install_location>¥Arcot Systems¥samples¥java¥`

   注: riskfort-3.1.01-sample-callouts.war はパッケージにも表示されますが、サンプル アプリケーション WAR ファイルは上記の場所から展開することをお勧めします。
4. ［設定］-［コントロール パネル］-［管理ツール］-［サービス］に移動します。
5. アプリケーション サーバのサービスを再開します。

UNIX ベースのプラットフォームの場合

CA Risk Authentication に同梱されているサンプル コールアウトをアプリケーション サーバに展開する方法

1. アプリケーション サーバ サービスを停止します。
2. riskfort-3.1.01-sample-callout.war ファイルを以下の場所から展開します。
   `<install_location>/arcot/samples/java/`
3. アプリケーション サーバのサービスを再開します。

サンプル コールアウトと通信するための CA Risk Authentication サーバの設定

注: リクエストおよびレスポンス XML の XSD は、*<install_location>*¥Arcot Systems¥docs¥riskfort¥Arcot-Riskfort-3.1.01-CallOutInterface-xsds.zip ファイルにあります。

サンプル コールアウトを設定するには、以下の手順に従います。

1. 「評価コールアウトの設定」の手順 1 ～ 5 を実行して［**評価コールアウト設定**］ページを表示します。
2. 表の［**候補**］列で
   a. ［**サーバ認証 SSL**］に［**いいえ**］を選択します。
   b. ［**クライアント認証 SSL**］に［**いいえ**］を選択します。

      注: このクライアントはサンプル コールアウトです。
   c. ［**コールアウト URL**］オプションに対して以下を指定します。

      http://<host>:CA Portal/riskfort-3.1.01-sample-callouts/SampleEvalCalloutServlet

      <host> はコールアウト WAR が展開されたサーバのホスト名または IP アドレスを示し、*CA Portal* はこのサーバが利用可能なポートを示します。
   d. ［**接続タイムアウト**］の値をミリ秒単位で指定します。 デフォルト値は 30000 ミリ秒です。
   e. ［**読み取りタイムアウト**］の値をミリ秒単位で指定します。デフォルト値は 30000 ミリ秒です。
   f. ［**コールアウトの説明**］に、コールアウトに関する有用な詳細を指定します。
   g. ［**保存**］をクリックして変更を保存します。
3. 「スコアリング コールアウトの設定」の手順 1 ～ 5 を実行して［**スコアリング コールアウトの設定**］テーブルを表示します。
4. 表の［**候補**］列で
   a. ［**サーバ認証 SSL**］に［**いいえ**］を選択します。
   b. ［クライアント認証 SSL］に［いいえ］を選択します。

      注: このクライアントはサンプル コールアウトです。
   c. ［**コールアウト URL**］オプションに対して以下を指定します。

http://<host>:CA Portal/riskfort-3.1.01-sample-callouts/SampleScoringCalloutServlet

<host> はコールアウト WAR が展開されたサーバのホスト名または IP アドレスを示し、*CA Portal* はこのサーバが利用可能なポートを示します。

d. ［**接続タイムアウト**］の値をミリ秒単位で指定します。 デフォルト値は 30000 ミリ秒です。

e. ［**読み取りタイムアウト**］の値をミリ秒単位で指定します。デフォルト値は 30000 ミリ秒です。

f. ［**コールアウトの説明**］に、コールアウトに関する有用な詳細を指定します。

g. ［**保存**］をクリックして変更を保存します。

今まで加えたすべての変更はまだアクティブではなく、エンドユーザに利用可能ではありません。

5. 変更をアクティブにするには、それらを運用環境に移行する必要があります。

詳細については、「運用環境への移行 (P. 236)」を参照してください。

第 10 章: 組織の管理

注: このセクションのほとんどのタスクは、GA（グローバル管理者）または OA （組織管理者）によって実行できます（その管理者が組織に対して必要なスコープを持っている場合）。

CA Advanced Authentication では、1 つの*組織*を企業（または会社）全体、または企業内の特定の部門、部署、その他のエンティティにマップできます。CA Advanced Authentication に用意されている組織構造はフラットです。つまり、組織階層（親組織と子組織の形式）はサポートされておらず、すべての組織はデフォルトの組織と同じレベルで作成されます デフォルトの組織の詳細については、「デフォルトの組織の設定」を参照してください。

企業の規模が大きくなるほど、その組織構成は複雑になります。 その結果、組織の管理は管理の中でも特に重要な部分になっています。 CA Risk Authentication でサポートされている組織管理操作には、以下のものが含まれます。

- 組織の作成とアクティブ化 (P. 256)
- 組織の検索 (P. 270)
- 組織情報の更新 (P. 271)
- ユーザとユーザ アカウントの一括でのアップロード (P. 275)
- バルク データ アップロード リクエストのステータスの表示 (P. 280)
- 組織キャッシュのリフレッシュ (P. 282)
- 組織の非アクティブ化 (P. 283)
- 組織のアクティブ化 (P. 284)
- 初期状態の組織のアクティブ化 (P. 285)
- 組織の削除 (P. 286)

注: 組織管理に関連する前述のタスク リストに加えて、OA は組織固有の設定も管理できます。詳細については、「組織固有の CA Risk Authentication の設定の管理」を参照してください。

組織の作成とアクティブ化

CA Risk Authentication リポジトリまたは既存の LDAP ベースのディレクトリ サーバ実装（Microsoft Active Directory、SunOne Directory Server、CA Directory Server など）で組織を作成できます。

注: 小規模な展開の場合には、新しい組織を作る代わりに、デフォルトの組織の名前を変更できます。

このセクションでは、実際の実装に基づいて、以下の手順について説明します。

- CA Risk Authentication リポジトリでの組織の作成
- LDAP リポジトリでの組織の作成

必要な権限

組織を作成してアクティブにするには、そのための適切な権限を持っていることを確認する必要があります。 MA および GA のみが、すべての組織を作成し、アクティブにすることができます。

CA Risk Authentication リポジトリでの組織の作成

CA Risk Authentication リポジトリに組織を作成する方法

1. 組織の作成に必要な権限でログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の作成**］リンクをクリックして［組織の作成］ページを表示します。
4. 以下の表の説明に従って組織の詳細を入力します。

フィールド	Description
組織情報	
［Organization Name］	作成する組織に対する一意の ID を入力します。 **注**: この組織にログインするには、組織の表示名 *ではなく*、この値を指定する必要があります。
表示名	組織のわかりやすい一意の名前を入力します。 **注**: この名前はほかのすべての CA Advanced Authentication ページやレポートに表示されます。

フィールド	Description
Description	この組織を管理する管理者に関する説明を入力します。 **注**: このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。
管理者認証メカニズム	この組織に属する管理者を認証するために使用されるメカニズムを選択します。 CA Advanced Authentication では、以下の種類の認証メカニズムがサポートされています。 ■ **基本ユーザ パスワード** これは、CA Advanced Authentication によって提供される組み込みの認証メカニズムです。 このオプションを選択した場合、管理者は自分のユーザ ID とパスワードを指定してコンソールにログインできます。 ■ **LDAP ユーザ パスワード** このメカニズムは LDAP 組織にのみ適用されます。 認証ポリシーは LDAP ディレクトリ サービスで定義されています。このオプションを選択した場合、管理者は LDAP に格納されている認証情報を使用して管理コンソールにログインする必要があります。 **AuthMinder ユーザ パスワード** これは、Strong Authentication のユーザ名-パスワード認証方式です。このオプションを選択した場合、管理者の認証情報は Strong Authentication サーバによって発行され、認証されます。 このメカニズムを使用するには、CA Strong Authentication がインストールされ、設定されている必要があります。 詳細については、「*CA Strong Authentication インストールおよび展開ガイド*」を参照してください。

フィールド	Description
キー ラベル設定 CA Risk Authentication では、ハードウェアまたはソフトウェア ベースの機密データの暗号化を使用できます。 暗号化モードは arcotcommon.ini 設定ファイルを使用して選択できます。 詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の「HSM 暗号化設定」を参照してください。 ハードウェアの暗号化かソフトウェアの暗号化かに関係なく、Strong Authentication と CA Risk Authentication はユーザおよび組織データの暗号化にグローバル キー ラベルを使用します。 ハードウェアの暗号化を使用している場合、このラベルは、HSM デバイスに格納されている実際の 3DES キーへの参照（ポインタ）としてのみ機能します。 この場合、指定するキー ラベルは HSM キー ラベルと一致する必要があります。ただし、ソフトウェア ベースの暗号化の場合、このラベルはキーとして機能します。	
グローバル キーの使用	デフォルトでは、このオプションが選択されています。 ブートストラップ プロセスで指定したグローバル キー ラベルを上書きする場合はこのオプションを選択解除し、組織に固有のデータの暗号化に使用される新しいキー ラベルを指定します。
キー ラベル	［**グローバル キーの使用**］オプションを選択解除した場合は、組織に対して使用する新しいキー ラベルを指定します。
暗号化ストレージ タイプ	このオプションは、暗号化キーがデータベース（**ソフトウェア**）に格納されるか HSM （**ハードウェア**）に格納されるかを示します。
ローカライズ設定	
グローバル設定の使用	グローバル レベルで設定されたローカライゼーション パラメータを使用するには、このオプションを選択します。
日付/時刻形式	［**グローバル設定の使用**］オプションを選択解除した場合は、この組織に対して使用する日付/時刻形式を指定します。
優先ロケール	［**グローバル設定の使用**］オプションを選択解除した場合は、この組織の優先ロケールを選択します。
ユーザ データの場所	
リポジトリ タイプ	［**Arcot データベース**］を選択します。 このオプションを指定すると、新しい組織のユーザや管理者の詳細が CA Risk Authentication でサポートされている RDBMS リポジトリに保存されます。
カスタム属性 このセクションを使用して、作成している組織に固有の情報を追加します。	
Name	カスタム属性の名前です。

フィールド	Description
値	カスタム属性の値です。

1. ［**Next**］をクリックします。
2. ［暗号化する属性の選択］ページが表示されます。
3. ［**暗号化する属性の選択**］セクションで、以下のいずれかを実行します。
   a. グローバル設定を属性の暗号化セットの設定に使用する場合は、［**グローバル設定の使用**］を選択します。

      または

   b. 暗号化する属性を［**暗号化用に利用可能な属性**］リストから選択し、それを［**暗号化用に選択した属性**］に移動します。

      ［>］または［<］ボタンをクリックして、選択した属性を目的のリストに移動します。［>>］または［<<］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。
4. ［**次へ**］をクリックします。

   ［管理者の追加］ページが表示されます。

   注: システムに現在存在するすべての管理者がすべての組織を管理するためのスコープを持っている場合、このページは表示*されません*。
5. ［**利用可能な管理者**］リストから組織を管理する管理者を選択し、**>** ボタンをクリックして管理者を［**管理している管理者**］リストに追加します。

   ［**利用可能な管理者**］リストには、新しい組織を管理できるすべての管理者が表示されます。

   注: 一部の管理者がシステム内のすべての組織を管理するためのスコープを持っている場合、このリストにはそれらの管理者に対応するエントリは表示されません。

   ［**管理している管理者**］リストには、この組織を管理するために選択した管理者が表示されます。
6. ［**次へ**］をクリックして、先に進みます。

   ［アカウント タイプの設定］ページが表示されます。

   注: 以下の点に注意してください。
   - アカウント タイプを作成していない場合、このページは表示されません。
   - デフォルトでは、グローバル アカウント タイプが選択されています。

7. ［**アカウント タイプの割り当て**］セクションで、［**利用可能**］リストからアカウント タイプを選択し、［**>**］ボタンをクリックしてそれらを［**選択済み**］リストに移動させます。
8. ［**次へ**］をクリックして、先に進みます。

   ［アカウント カスタム属性の設定］ページが表示されます。

   注: 前のページでアカウント タイプを選択しなかった場合、このページは表示されません。
9. ［**アカウント タイプ**］の［**カスタム属性**］を指定し、［**次へ**］をクリックします。

   ［電子メール/電話のタイプの設定］ページが表示されます。
10. ユーザが用意する必要がある必須およびオプションの電子メール アドレスと電話番号を指定します。
11. ［**スキップ**］をクリックしてシステム レベルで設定された電子メールおよび電話タイプを使用して次のページに移動するか、または［**保存**］をクリックして変更内容を保存します。

    ［組織のアクティブ化］ページが表示されます。
12. ［**有効化**］ボタンをクリックして新しい組織をアクティブにします。メッセージ ボックスが表示されます。
13. ［**OK**］をクリックして処理を完了します。

    注: 組織をアクティブにすることを選択しない場合、組織は初期状態で作成されます。この組織を後からアクティブにすることができます。この手順については、「初期状態の組織のアクティブ化」を参照してください。
14. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

    注意: 組織を作成する際に、属性の暗号化セット、アカウント タイプ、および電子メールと電話のタイプを設定している場合は、システム設定と組織のキャッシュの*両方*をリフレッシュします。 組織レベルのキャッシュをリフレッシュしないと、システムは回復不可能な状態になります。

LDAP リポジトリでの組織の作成

LDAP ユーザ ディレクトリをサポートするには、LDAP リポジトリに組織を作成してから、CA Risk Authentication データベースの属性を LDAP の属性にマップする必要があります。 以下の手順を実行します。

1. 組織の作成に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の作成**］リンクをクリックして［組織の作成］ページを表示します。
4. 以下の表の説明に従って組織の詳細を入力します。

フィールド	Description
組織情報	
［Organization Name］	作成する組織に対する一意の ID を入力します。 **注**: CA Advanced Authentication を使用してこの組織にログインするには、組織の表示名 *ではなく*、この値を指定します。
表示名	組織のわかりやすい一意の名前を入力します。 **注**: この名前はほかのすべての CA Advanced Authentication ページやレポートに表示されます。
Description	この組織を管理する管理者に関する説明を入力します。 **注**: このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。

フィールド	Description
管理者認証メカニズム	この組織に属する管理者を認証するために使用されるメカニズムを選択します。 CA Advanced Authentication では、以下の 2 種類の認証メカニズムがサポートされています。 ■ **基本ユーザ パスワード** これは、CA Advanced Authentication によって提供される組み込みの認証メカニズムです。 このオプションを選択した場合、管理者は自分の ID とプレーン テキスト パスワードを指定してコンソールにログインできます。 ■ **LDAP ユーザ パスワード** このメカニズムは LDAP 組織にのみ適用されます。 認証ポリシーは LDAP ディレクトリ サービスで定義されています。このオプションを選択した場合、管理者は LDAP に格納されている認証情報を使用して管理コンソールにログインする必要があります。 ■ **AuthMinder ユーザ パスワード** これは、Strong Authentication のユーザ名-パスワード認証方式です。このオプションを選択した場合、管理者の認証情報は Strong Authentication サーバによって発行され、認証されます。 このメカニズムを使用するには、Strong Authentication がインストールされ、設定されている必要があります。 Strong Authentication の展開の詳細については、「*CA Strong Authentication インストールおよび展開ガイド*」を参照してください。
キー ラベル設定	
グローバル キーの使用	デフォルトでは、このオプションが選択されています。 ブートストラップ プロセスで指定したグローバル キー ラベルを無効にして、新たに組織固有のデータの暗号化用のラベルを指定する場合は、このオプションを選択解除します。
キー ラベル	［**グローバル キーの使用**］オプションを選択解除した場合は、組織に対して使用する新しいキー ラベルを指定します。
暗号化ストレージ タイプ	このオプションは、暗号化キーがデータベース（**ソフトウェア**）に格納されるか HSM （**ハードウェア**）に格納されるかを示します。
ローカライズ設定	
グローバル設定の使用	グローバル レベルで設定されたローカライゼーション パラメータを使用するには、このオプションを選択します。

フィールド	Description
日付/時刻形式	［**グローバル設定の使用**］オプションを選択解除した場合は、この組織に対して使用する日付/時刻形式を指定します。
優先ロケール	［**グローバル設定の使用**］オプションを選択解除した場合は、この組織の優先ロケールを選択します。
ユーザ データの場所	
リポジトリ タイプ	［**エンタープライズ LDAP**］を選択します。このオプションを指定すると、新しい組織のユーザの詳細が次のページで指定する LDAP リポジトリに保存されます。
カスタム属性	
Name	カスタム属性の名前です。
値	カスタム属性の値です。

1. ［**Next**］をクリックします。

   LDAP リポジトリの詳細を収集するための［組織の作成］ページが表示されます。

2. 以下の表に従って、LDAP リポジトリに接続するための詳細を入力します。

フィールド	Description
ホスト名	LDAP リポジトリを使用できるシステムのホスト名を入力します。
Port Number	LDAP リポジトリ サービスがリスニングしているポート番号を入力します。
スキーマ名	LDAP リポジトリで使用される LDAP スキーマを指定します。 このスキーマには、LDAP リポジトリに含めることができるオブジェクトのタイプと、各オブジェクト タイプの必須属性および任意属性が指定されます。 通常、Active Directory のスキーマ名は user であり、SunOne Directory および CA Directory Server のスキーマ名は inetorgperson です。
ベース識別名	LDAP リポジトリのベース識別名を入力します。 この値は、LDAP リポジトリ内を検索する際の LDAP 階層の開始ノードを示します。 たとえば、cn=rob laurie, ou=sunnyvale, o=arcot, c=us という DN を持つユーザを検索するには、ベース DN を以下のように指定する必要があります。 ou=sunnyvale, o=arcot, c=us **注**: 通常、このフィールドでは大文字と小文字が区別され、このフィールドに指定されたベース DN のサブノードがすべて検索されます。

フィールド	Description
リダイレクト スキーマ名	「*member*」属性を定義するスキーマの名前を指定します。 組織に対して定義されたベース DN を使用して、LDAP リポジトリでユーザを検索できます。 ただし、この検索では、特定の OU （組織単位）に属するユーザしか返されません。LDAP 管理者は、グループ全体へのアクセスを制御するために、さまざまな組織単位に属するユーザのグループを作成し、さまざまなグループからユーザを検索したいと思われます。管理者がグループを作成すると、ユーザ ノード DN はグループ ノードの「member」属性に格納されます。デフォルトでは、UDS では属性値に基づいた検索や DN の解決が許可されていません。 リダイレクトを使用すると、特定のノードに対する特定の属性値に基づいて、LDAP 内のさまざまなグループに属するユーザを検索できます。 通常、リダイレクト スキーマ名は以下のとおりです。 ■ Active Directory： group ■ SunOne Directory： groupofuniquenames ■ CA Directory Server： groupOfUniqueNames
接続タイプ	CA Advanced Authentication と LDAP リポジトリの間で使用する接続のタイプを選択します。 サポートされているタイプは以下のとおりです。 ■ TCP ■ 一方向 SSL ■ 双方向 SSL
ログイン名	リポジトリ サーバにログインし、ベース識別名を管理する権限を持つ LDAP リポジトリ ユーザの完全識別名を入力します。 例を以下に示します。 uid=gt,dc=arcot,dc=com
ログイン パスワード	［ログイン名］で指定したユーザのパスワードを入力します。
サーバ トラステッド ルート証明書	［**一方向 SSL**］または［**双方向 SSL**］オプションが選択されている場合は、**参照**ボタンを使用して **LDAP** サーバに SSL 証明書を発行した信頼済みルート証明書のパスを入力します。
クライアント キーストア	［**双方向 SSL**］オプションが選択されている場合は、**参照**ボタンを使用してクライアント証明書と対応するキーを含むキー ストアのパスを入力します。 **注**: PKCS#12 または JKS のいずれかのキーストア タイプをアップロードする必要があります。

フィールド	Description
クライアント キー ストア パスワード	［**双方向 SSL**］オプションが選択されている場合は、クライアント キー ストアのパスワードを入力します。

1. ［**次へ**］をクリックして続行します。

   リポジトリの属性をマップするページが表示されます。

2. このページで、以下を実行します。

   a. ［**Arcot データベース属性**］リストから属性を選択し、CA Risk Authentication データベースの属性とマップする必要がある適切な属性を［**エンタープライズ LDAP 属性**］リストから選択して［**マップ**］ボタンをクリックします。

      重要: UserName 属性は必ずマップする必要があります。 一意にユーザを識別する LDAP 属性に UserName 属性をマップします。 Active Directory を使用している場合は、*UserName* を sAMAccountName にマップします。 SunOne Directory Server を使用している場合は、*UserName* を uid にマップします。 CA Directory Server を使用している場合は、*UserName* を cn にマップします。

      Active DIrectory の場合は、STATUS を userAccountControl にマップする必要があります。

   b. 必要なすべての属性のマップが完了するまで、属性をマップする作業を繰り返します。

      注: ［**Arcot データベース属性**］リスト内の属性をすべてマップする必要はありません。 マップする必要があるのは、使用する属性のみです。

      マップされた属性は［**Mapped Attributes**］リストに移動されます。

      必要な場合は、属性のマッピングを解消できます。 一度に 1 つの属性のマッピングを解消する場合は、属性を選択して［**Unmap**］ボタンをクリックします。 ただし、［**Mapped Attribute**］リストをクリアする場合は、［**Reset**］ボタンをクリックすると、マップされたすべての属性のマッピングが解消されます。 組織をアクティブにした後、UserName 属性のマッピングを解消することはできません。

   c. 前のページで［**リダイレクト スキーマ名**］を指定した場合は、［**リダイレクト検索属性**］リストから検索属性を選択する必要があります。

      通常、属性は以下のとおりです。

      - Active Directory： member
      - SunOne Directory： uniquemember
      - CA Directory Server： uniqueMember

3. ［**次へ**］をクリックして続行します。

   ［暗号化する属性の選択］ページが表示されます。

4. ［**暗号化する属性の選択**］セクションで、以下のいずれかを実行します。

   a. グローバル設定を属性の暗号化セットの設定に使用する場合は、［**グローバル設定の使用**］を選択します。

      または

   b. 暗号化する属性を［**暗号化用に利用可能な属性**］リストから選択し、それを［**暗号化用に選択した属性**］に移動します。

      ［>］または［<］ボタンをクリックして、選択した属性を目的のリストに移動します。［>>］または［<<］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。

5. ［**次へ**］をクリックします。

   ［管理者の追加］ページが表示されます。

   注: システムに現在存在するすべての管理者がすべての組織を管理するためのスコープを持っている場合、このページは表示*されません*。

6. ［**利用可能な管理者**］リストから組織を管理する管理者を選択し、**>** ボタンをクリックして管理者を［**管理している管理者**］リストに追加します。

   注: 管理者への組織の割り当ては、既存の管理者のスコープを更新するか、または組織を管理する新しい管理者を作成することによっていつでも実行できます。

   ［**利用可能な管理者**］リストには、新しい組織を管理できるすべての管理者が表示されます。

   注: 一部の管理者がシステム内のすべての組織を管理するためのスコープを持っている場合、このリストにはそれらの管理者に対応するエントリは表示されません。

   ［**管理している管理者**］リストには、この組織を管理するために選択した管理者が表示されます。

7. ［**次へ**］をクリックして続行します。

   ［アカウント タイプの設定］ページが表示されます。

   注: アカウント タイプを作成していない場合、このページは表示されません。

8. ［**アカウント タイプの割り当て**］セクションで、［**利用可能**］リストからアカウント タイプを選択し、［**>**］ボタンをクリックしてそれらを［**選択済み**］リストに移動させます。
9. ［**次へ**］をクリックして、先に進みます。

   ［アカウント カスタム属性の設定］ページが表示されます。

   注: 前のページでアカウント タイプを選択しなかった場合、このページは表示されません。
10. ［**アカウント タイプ**］の［**カスタム属性**］を指定し、［**次へ**］をクリックします。

    ［組織のアクティブ化］ページが表示されます。

    注: 組織がアクティブになると、UserName マッピングを変更したり、更新したり できなくなります。
11. ［**有効化**］ボタンをクリックして新しい組織をアクティブにします。

    警告メッセージが表示されます。
12. ［**OK**］をクリックして処理を完了します。
13. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

    この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

    注意: 組織を作成する際に、属性の暗号化セット、アカウント タイプ、および電子メールと電話のタイプを設定している場合は、システム設定と組織のキャッシュの*両方*をリフレッシュします。 組織レベルのキャッシュをリフレッシュしないと、システムは回復不可能な状態になります。

組織の検索

組織を更新、アクティブ化、または非アクティブ化する必要がない限り、検索する権限は必要ありません。 ただし、検索する組織がスコープに含まれている*必要があります*。 たとえば、対象となる組織が OA の権限の範囲内に*あれば*、OA はその組織を検索できます。

組織の検索

組織の検索には、表示名とステータスを使用できます。 1 つ以上の組織を検索するには、以下の手順に従います。

1. 組織の作成に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 必要な組織の情報の一部または全部を入力します。 以下のオプションを選択して、検索の範囲を広げることができます。

   注: ［**組織**］フィールドには、実際の組織名 *では*なく、組織の表示名の一部または全部を入力する必要があります。

   - **初期**（作成されたが、まだアクティブ化されていない組織を表示する場合）
   - **アクティブ**（作成され、アクティブ化された組織を表示する場合）
   - **非アクティブ**（非アクティブ化された組織を表示する場合）
   - **削除済み**（削除された組織を表示する場合）
5. ［**検索**］ボタンをクリックすると、指定した条件に一致するすべての組織がページに表示されます。

組織情報の更新

CA Advanced Authentication を使用して、組織の以下の情報を更新できます。

- 組織の表示名、説明、ステータス、組織を管理する管理者、組織に割り当てられたアカウント タイプ、設定された電子メール/電話のタイプ、および属性暗号化セットを含む**組織情報**（基本組織情報の更新）
- 認証情報プロファイル、認証ポリシー、拡張可能な設定、および割り当てられたデフォルト設定を含む組織の **CA Risk Authentication 固有の設定**（CA Risk Authentication 固有の設定の更新）

必要な権限

組織を更新するには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての組織を更新できます。 GA と OA は、自分のスコープに含まれるすべての組織の情報を更新できます。

基本組織情報の更新

基本的な組織情報を更新する方法

1. 組織を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**組織詳細**］セクションで、必要なフィールド（［**表示名**］と［**説明**］）を編集します。
7. 必要に応じて、［**管理者認証メカニズム**］を編集します。

   管理者がこの組織に存在しない場合にのみ、認証メカニズムを編集できます。
8. ［**ローカライズ設定**］セクションで、以下の操作を実行できます。

   a. ［**グローバル設定の使用**］を選択する。

   または

   b. ［**日付/時刻形式**］および［**優先ロケール**］を編集する。
9. ［**カスタム属性**］セクションで、必要に応じて［**名前**］フィールドと［**値**］フィールドを編集します。
10. ［**次へ**］をクリックして追加の設定に進みます。

    - 組織が **Arcot リポジトリ**に作成された場合は、以下の手順に従います。

      1. ［暗号化する属性の選択］ページで、属性の暗号化セット設定にグローバル設定を使用する場合は［**グローバル設定の使用**］を選択し、そうでない場合は［**暗号化用に利用可能な属性**］リストから暗号化する属性を選択して［**暗号化用に選択した属性**］リストに追加して、［**次へ**］をクリックします。

組織でユーザがすでに作成されている場合は、属性を更新できません。

2. ［管理者の更新］ページで、組織を管理する管理者を更新し、［**次へ**］をクリックします。
3. ［アカウント タイプの設定］ページで、アカウント タイプを［**利用可能**］リストから選択して［**選択済み**］リストに移動させて［**次へ**］をクリックします。

グローバル アカウント タイプは選択解除できません。

4. ［アカウント カスタム属性の設定］ページで、アカウントのカスタム属性を追加し、［**次へ**］をクリックします。
5. ［電子メール/電話のタイプの設定］ページで、ユーザ用の必須およびオプションの電子メール アドレスおよび電話のタイプを設定し、［**保存**］をクリックして処理を完了します。

- 組織が **LDAP リポジトリに**作成された場合は、組織の編集ページが表示されます。 組織の詳細を更新する方法

a. 必要に応じて「**LDAP リポジトリでの組織の作成**」の情報を使ってフィールドを更新し、［次へ］をクリックして［リポジトリ属性マッピング］を編集するページを表示します。

b. UserName マッピングを除くその他のマッピングを編集できます。［**次へ**］をクリックして、［暗号化する属性の選択］ページを表示します。

c. ［暗号化する属性の選択］ページで、属性の暗号化セット設定にグローバル設定を使用する場合は［**グローバル設定の使用**］を選択し、そうでない場合は［**暗号化用に利用可能な属性**］リストから暗号化する属性を選択して［**暗号化用に選択した属性**］リストに追加して、［**次へ**］をクリックします。

d. 組織でユーザがすでに作成されている場合は、属性を更新できません。LDAP の場合には、LDAP リポジトリ内のユーザに対する単純な検索操作でも、データベースにユーザを登録します。 したがって、LDAP リポジトリのユーザを検索した場合は、属性を更新できません。

e. ［管理者の更新］ページで、組織を管理する管理者を更新し、［**次へ**］をクリックします。

f. ［アカウント タイプの設定］ページで、アカウント タイプを［**利用可能**］リストから選択して［**選択済み**］リストに移動させることにより、アカウント タイプを設定し、［**更新**］をクリックして変更を保存し、プロセスを完了します。

グローバル アカウント タイプは選択解除できません。

11. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

CA Risk Authentication 固有の設定の更新

組織の CA Risk Authentication 設定を更新する方法

1. 組織を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報を一部または全部入力し、［**検索**］ボタンをクリックして、検索条件に一致する組織のリストを表示します。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックし、［組織情報］ページを表示します。
6. ［**CA Risk Authentication 設定**］タブをアクティブにして、タスク パネルの CA Risk Authentication 設定のリンクを表示します。

これらの設定の詳細については、「組織固有の CA Risk Authentication の設定の管理」を参照してください。

ユーザとユーザ アカウントの一括でのアップロード

CA Risk Authentication では、CA Advanced Authentication を使用してユーザとユーザ アカウントを一括してアップロードできるようになりました。複数のユーザおよびユーザ アカウントの情報をアップロードするには、CSV （カンマ区切り値）形式の入力ファイルが必要です。

ユーザの一括でのアップロード

ユーザをアップロードする CSV 形式の入力ファイル内の最初の行は、以下のようにする必要があります。

```
#UserID,fName,mName,lName,status,pam,pamURL,EmailAddr,telephoneNumber,INFOLIST#
```

注意： この最初の（テンプレート）行は*常に*必要です。 この行が指定されていないと、ユーザの一括アップロード操作は失敗します。

ユーザをアップロードするための CSV 形式の入力ファイルを作成するときは、以下に注意してください。

- CSV ファイルには、# で開始および終了するヘッダを 1 つ含める必要があります。 ほかのすべてのフィールド名はこれらの # 記号の間で指定する必要があります。
- 必須のエントリは UserID だけです。その他のエントリはオプションです。
- アップロードしようとしているユーザがすでに存在する場合、ユーザの詳細が更新されます。
- 最大で 5 つの電子メール アドレスと 5 つの電話番号を指定できます。この場合は、以下のようにヘッダを指定する必要があります。

  ```
  #UserID,fName,mName,lName,status,pam,pamURL,EmailAddr,EMAIL.2,EMAIL.3,EMAIL.4,EMAIL.5,telephoneNumber,PHONE.2,PHONE.3,PHONE.4,PHONE.5,INFOLIST#
  ```

ファイルのエントリについて、以下の表で説明します。

エントリ	Description
UserID	ユーザの一意の ID。
fName	ユーザの名。
mName	ユーザのミドル ネーム。
lName	ユーザの姓。

エントリ	Description
status	ユーザのステータス。 以下の値が使用可能です。 ■ INITIAL ■ ACTIVE
pam	個人の認証メッセージ。
pamURL	ユーザの個人の認証メッセージのイメージがある場所の URL。
EmailAddr	ユーザの連絡用電子メールの ID。
telephoneNumber	国際コードを伴うユーザの完全な電話番号。 たとえば、米国の電話番号は 1 で始まります。
INFOLIST	ユーザに関する追加情報。値はセミコロンで区切る必要があります。例 : age=25;favsport=cricket

たとえばファイルの例として、以下のエントリを含めることができます。

```
#UserID,fName,lName,status,EmailAddr,telephoneNumber,PHONE.2,INFOLIST#
mparker,martin,parker,ACTIVE,mparker@ca.com,12345,9999,age=29;favsport=cricket
jhume,john,hume,ACTIVE,jhume@ca.com,3939292,203939393,age=32;favbook=fiction
fantony,francis,antony,ACTIVE,fantony@ca.com,130203,29888,age=25;favfood=pizza#
```

ユーザ アカウントの一括でのアップロード

ユーザ アカウントをアップロードする CSV 形式の入力ファイル内の最初の行は、以下のようにする必要があります。

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountID
Attribute2,accountIDAttribute3,customAttr1,customAttr2,customAttr3
,customAttr4,customAttr5,customAttr6,customAttr7,customAttr8,custo
mAttr9,customAttr10#
```

注意： この最初の（テンプレート）行は*常に*必要です。 この行が指定されていないと、ユーザ アカウントの一括アップロード操作は失敗します。

ユーザ アカウントをアップロードするための CSV 形式の入力ファイルを作成するときは、以下に注意してください。

- 必須のエントリは、UserID、accountType、および accountID だけです。その他のエントリはオプションです。
- システムでユーザが作成済みである必要があります。
- アカウント タイプを作成して、組織にそれを割り当て済みである必要があります。
- アカウント タイプのカスタム属性を作成している必要があります。
- 1 つのアカウント タイプに対して最大 10 までのカスタム属性を指定できます。

ファイルのエントリについて、以下の表で説明します。

エントリ	Description
UserID	ユーザの一意の ID。
accountType	accountID に関連付けられたアカウント タイプ。
accountID	ユーザの代替 ID。
status	アカウント ID のステータス。 以下の値が使用可能です。 ■ ［0-9］ : INITIAL ■ ［10-19］ : ACTIVE ■ ［20-29］ : INACTIVE

エントリ	Description
accountIDAttribute1	accountID の属性。 最大 3 つのアカウント ID 属性を指定できます。
customAttr1	ユーザ アカウントのカスタム属性。

たとえばファイルの例として、以下のエントリを含めることができます。

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,accountIDAttribute3,customAttr1,customAttr2#
prush,ONLINE_BANKING,OB_ID1,10,login,password,image,chicago,music
jhume,SAVINGS,SA_ID1,10,interest,deposit,check,florida,soccer
```

CA Risk Authentication データベースに複数のユーザおよびユーザ アカウントを作成する方法

1. 組織を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ユーザとユーザ アカウントを一括してアップロードする組織を選択します。
6. ［**基本組織情報**］セクションで、［**バルク アップロード**］リンクをクリックし、［バルク データ アップロード］ページを表示します。
7. ［**バルク アップロード**］セクションで、以下の操作を実行します。
   a. ［**バルク アップロード操作**］ドロップダウン リストから、［**ユーザ アカウントのアップロード**］または［**ユーザのアップロード**］を選択します。
   b. **参照**ボタンをクリックして、ユーザ アカウントまたはユーザのエントリが含まれる CSV ファイルを指定します。
   c. 操作の［**説明**］を入力します。
8. ［**アップロード**］をクリックして、ユーザ アカウントまたはユーザを一括してアップロードします。
9. 操作が完了すると、メッセージにリクエスト ID が表示されます。
10. （**重要**）このリクエスト ID をメモしておいてください。

    バルク データ アップロード操作のステータスを表示するために必要になります。

バルク データ アップロード リクエストのステータスの表示

バルク データ アップロード リクエストのステータスを表示する方法

1. この操作に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. バルク アップロード リクエストのステータスを表示する組織を選択します。
6. ［**基本組織情報**］セクションで、［**バルク リクエストの表示**］リンクをクリックし、［バルク リクエストの検索］ページを表示します。
7. ［バルク リクエストの検索］ページで、以下の操作を実行します。
   a. 先にメモしておいたリクエスト ID を入力します（「ユーザとユーザ アカウントの一括でのアップロード」の手順 10）。

      または
   b. 表示したいバルク リクエストの［**ステータス**］を選択します。

      または
   c. ［**ユーザのアップロード**］リクエストを表示するか、または［**ユーザ アカウントのアップロード**］リクエストを表示するかに応じて、［**操作**］を選択します。
8. ［**検索**］をクリックしてテーブルを表示します。
9. 失敗の場合は、［**要求 ID**］リンクをクリックしてバルク リクエストの詳細情報を表示します。
10. ［**失敗した操作の数**］リンクをクリックすると、操作が失敗した理由が表示されます。

リクエストの操作が失敗した場合は、［**エクスポート失敗**］ボタンが有効になります。 ［**エクスポート失敗**］をクリックして、失敗したすべての操作を CSV ファイルにエクスポートします。 その後、エクスポートされたファイルでエラーを修正し、バルク アップロードのためにファイルを再サブミットできます。

組織キャッシュのリフレッシュ

属性暗号化セット、ローカライゼーション設定、および電子メールと電話のタイプなどのグローバル設定を参照しない組織設定は、組織レベルでキャッシュされます。 組織レベルでこれらの設定に変更を加えた場合は、変更を有効にするために組織のキャッシュをリフレッシュする必要があります。

注: MA は、すべての組織のキャッシュをリフレッシュできます。GA と OA は、そのスコープ内のすべての組織のキャッシュをリフレッシュできます。

組織キャッシュをリフレッシュする方法

1. 組織のキャッシュのリフレッシュに必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. キャッシュをリフレッシュする組織を選択します。
6. ［**キャッシュのリフレッシュ**］をクリックします。
7. キャッシュ リフレッシュ リクエストを確認するダイアログ ボックスで［**OK**］をクリックします。

   現在のキャッシュ リフレッシュ リクエストのリクエスト ID を示すメッセージが表示されます。 ［**キャッシュ リフレッシュ ステータスの確認**］リンクをクリックし、この**リクエスト ID** を選択すると、キャッシュ リフレッシュ リクエストのステータスを確認できます。

注: ある組織のキャッシュをリフレッシュしても、その他の組織に対してその時間に実行されているトランザクションの応答時間には影響しません。

組織の非アクティブ化

組織のすべての管理者に対して CA Risk Authentication のメカニズムを使った CA Advanced Authentication へのログインを禁止し、組織のエンドユーザに対して CA Risk Authentication のメカニズムを使ったアプリケーションへの認証を禁止する場合は、組織を非アクティブ化します。

必要な権限

組織を非アクティブにするには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての組織を非アクティブにできます。GA と OA は、自分のスコープに含まれるすべての組織を非アクティブにできます。

組織の非アクティブ化

1 つ以上の組織を非アクティブにする方法

1. 組織の非アクティブ化に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. 非アクティブにする組織を 1 つ以上選択します。
6. ［**非アクティブ化**］ボタンをクリックすると、選択した組織が無効になります。

   メッセージ ボックスが表示されます。
7. ［**OK**］ボタンをクリックして非アクティブ化を確定します。
8. 展開された CA Risk Authentication サーバインスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

組織のアクティブ化

非アクティブになっている組織を再度アクティブにする必要がある場合があります。 その場合は、［組織の検索］ページで検索条件を指定する際に、［**非アクティブ**］オプションを選択する必要があります。

必要な権限

組織をアクティブにするには、適切な権限およびスコープがあることを確認する必要があります。MA はすべての組織をアクティブ化できます。GA と OA は、自分のスコープに含まれるすべての組織をアクティブ化できます。

組織のアクティブ化

非アクティブになっている組織をアクティブにする方法

1. 組織のアクティブ化に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. 再度アクティブにする組織を 1 つ以上選択します。
6. ［**アクティブ化**］ボタンをクリックすると、選択した組織がアクティブになります。

   メッセージが表示されます。
7. ［**OK**］ボタンをクリックしてアクティブ化を確定します。
8. 展開された CA Risk Authentication サーバインスタンスをすべてリフレッシュします。

   この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

初期段階の組織のアクティブ化

場合によっては、組織を作成し始めても、組織をアクティブにしないことがあります。 たとえば、［組織の作成］ページで［**組織情報**］や［**ユーザ データの場所**］を指定しても、LDAP リポジトリの詳細や組織を管理する管理者を指定しない場合があります。 このような場合、組織は作成されますが、アクティブではなく、通常は検索時に表示されません（［**初期**］オプションを選択して検索しない限り）。

このような組織は、アクティブにしない限り、システム内では初期状態のままです。 後で初期状態の組織と同じ詳細情報を使って新しい組織を作成しようとしても、その組織が存在するため、作成できません。

必要な権限

初期状態の組織をアクティブにするには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての組織をアクティブ化できます。GA と OA は、自分のスコープに含まれるすべての組織をアクティブ化できます。

初期状態の組織のアクティブ化

初期状態の組織をアクティブ化する方法

1. 組織の作成に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 必要な組織の情報の一部または全部を入力し、［**初期**］オプションを選択します。
5. ［**検索**］ボタンをクリックすると、指定した条件に一致するすべての組織がページに表示されます。
6. アクティブにする組織を選択します。
7. ［**アクティブ化**］ボタンをクリックすると、選択した組織が有効になります。 メッセージが表示されます。
8. ［**OK**］ボタンをクリックしてアクティブ化を確定します。
9. 展開された CA Risk Authentication サーバ インスタンスをすべてリフレッシュします。

この方法の詳細については、「キャッシュのリフレッシュ」を参照してください。

組織の削除

組織を削除すると、その組織に関連付けられた管理者は CA Advanced Authentication を使用してログインできなくなり、その組織に属するエンドユーザは認証できなくなります。 ただし、組織に関連する情報はシステム内に保持され続けます。 削除された組織がスコープに含まれている管理者は、その組織の詳細を読み取ることができます。

必要な権限

組織を削除するには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての組織を削除できます。 GA と OA は、自分のスコープに含まれるすべての組織を削除できます。

組織の削除

組織を削除する方法

1. 組織の削除に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. 削除する 1 つ以上の組織を選択し、［**削除**］をクリックします。

   メッセージが表示されます。
6. ［**OK**］をクリックし、削除を確定します。

第 11 章: 組織固有の CA Risk Authentication の設定の管理

注: 組織の設定を管理するには、ユーザ（**組織管理者**）が適切な権限およびスコープを持っていることを確認する必要があります。

マスタ管理者は組織に固有の設定を管理 *できません*。 GA と OA は、自分のスコープに含まれるすべての組織の設定を管理できます。

「グローバル設定の管理」で説明したように、GA （グローバル管理者）によって設定された「テンプレート化された」ルール設定のコピーを作成できますが、自分の権限の範囲内で組織の特定のビジネス要件を満たすためには、このルール設定を上書きしても良いでしょう。

組織レベルでルール設定を行うと、変更は設定した特定の組織に限定されます。 また、設定に対して行われた変更内容は自動的には適用されません。 これらの設定変更を適用するためにサーバ インスタンスをすべてリフレッシュする必要があります。

指定された組織にスコープがある場合は、OA として以下のタスクを実行できます。

- 組織固有の CA Risk Authentication 設定へのアクセス（P. 288）
- ルール セットの作成（P. 289）
- ルール セットの割り当て（P. 290）
- グローバル ルール設定の使用（P. 292）
- 組織のための CA Risk Authentication の設定（P. 292）

組織固有の CA Risk Authentication 設定へのアクセス

組織固有の設定はグローバル設定に似ていますが、それぞれのタスク ページへのナビゲーション パスは異なります。 組織固有の設定を行うためのタスク ページにアクセスするには、以下の手順に従います。

1. 組織を更新するために必要な権限およびスコープを持つユーザとしてログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。

   タスク ペインに組織固有の設定のリンクが表示されます。
7. 必要なルール セットおよびリスク評価ルールを設定します。

   注: 必要なルールを設定して、必要に応じて割り当てる方法の詳細については、「グローバル設定の管理」を参照してください。 「**グローバル設定の管理**」で説明している操作は、グローバル レベルですが、ここで説明されている設定は組織レベルです。 設定内容はどちらも同じですが、このセクションの冒頭で説明したように、タスク ページにアクセスする方法のみが異なります。

ルール セットの作成

「ルール セットについて」で説明しているように、ルール セットとは、GA（グローバル管理者）または OA（組織管理者）によって設定される一連のルールです。

重要: GA によって作成された場合、ルール セットは*個々の組織用にコピーすることだけが可能です*。そのため、OA はグローバル ルール セットをコピーして新しいルール セットを作成するか、組織レベルで再度ルール セットを作成する必要があります。

ルール セットの作成方法の詳細については、「ルール セットの作成」を参照してください。

重要: ルール セットを作成したら、それを運用環境に移行してアクティブ化に使用できるようにする*必要があります*。

ルールの割り当て

OA が自分の組織のルールセットを作成し、それを運用環境に移行したら、スコープ内で組織のルール セットをアクティブ化して、そのルール セットを有効にする必要があります。 現在の組織に既存のルール セットを割り当てるには、以下の手順に従います。

1. ルール セットの割り当てに必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。
7. ［**ルール セット**］セクションで、［**ルール セットの割り当て**］リンクをクリックします。

   ［ルール セットの割り当て］ページが表示されます。
8. ［**割り当て対象ルールセットの選択**］リストから、アクティブにするルール セットを選択します。
9. ［**保存**］をクリックして、現在の組織で指定されたルール セットをアクティブにします。

ルール セットの削除

CA Risk Authentication のこのリリースでは、組織に現在割り当てられていないルール セットを削除することができます。 ルール セットを削除する方法

1. ルール セットの削除に必要な権限とスコープでログインしていることを確認します。
2. ［**組織**］タブをアクティブにします。
3. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
4. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
5. ［**組織**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   ［組織情報］ページが表示されます。
6. ［**CA Risk Authentication 設定**］タブをアクティブにします。
7. ［**ルール セット**］セクションで、［**ルール セットの削除**］リンクをクリックします。

   ［ルール セットの削除］ページが表示されます。
8. 削除する**ルール セットを選択します**。
9. ［**削除**］をクリックします。
10. 確認メッセージ ボックスで［**OK**］をクリックしてタスクを完了します。

    ルール セットが削除されます。

グローバル ルール設定の使用

スコープ内の各組織のルール設定を個別に変更することもできますが、ほとんどの組織は繰り返して同じ設定を使用している可能性があります。また、個々の組織にルール設定を行うことは、設定された組織が多数ある場合、厄介なタスクになります。 このような場合、同じ設定を毎回指定する必要がなくなるように、GA が設定したグローバル設定をカスタマイズすると良いでしょう。

組織をスコープとする GA がグローバル レベルでルール設定を行うと、すべての組織がこれらの設定を継承します。 *コピーを作成することにより*、これらの設定を使用できます。

［ルール セットの作成］ページに表示される［**詳細オプション**］セクションを使用します。 このセクションは折りたたまれているため、［**+**］記号をクリックしてセクションを展開し、使用可能なオプションを表示します。

既存のルール セットから設定をコピーするオプションがあります。

［**既存のルール セットからコピー**］オプションを選択し、コピーする設定を持つルール セットの名前をドロップダウン リストから選択します。

組織のための CA Risk Authentication の設定

ルール セットの作成と割り当てのほかに、OA（組織管理者）は、「グローバル設定の管理」で説明したほとんどのタスクを実行できます。 これには以下が含まれます。

- スコープ内の組織の既定ルールの設定。

  詳細な手順については、「既定のルールの設定」を参照してください。
- スコープ内の組織の新規ルールの展開。

  詳細な手順については、「新規ルールの追加」を参照してください。
- スコープ内の組織のコールアウトの設定。

  詳細な手順については、「コールアウトの設定」を参照してください。
- スコープ内の組織の運用環境への設定の移行。

  詳細な手順については、「運用環境への移行」を参照してください。

第 12 章: 管理者の管理

管理者のタイプ、および管理者のロールと責任は、展開の規模に依存します。 小規模な単独組織への展開では、マスタ管理者（MA）1 人のみと、エンドユーザのために組織を管理するグローバル管理者（GA）を配置する場合があります。 一方、大規模な複数組織への展開では、展開の複雑さとエンドユーザの数に基づいて複数の GA を配置する必要がある場合があります。GA は、組織とユーザの管理作業をさらに複数の組織管理者（OA）およびユーザ管理者（UA）に委任できます。

サポートされている管理ロールの詳細については、「サポートされるロール」を参照してください。 このセクションでは、以下の管理者管理操作について説明します。

注: マスタ管理者は、このセクションで説明する操作に加えて、「カスタム ロール」を作成する権限を持っています。これは CA Risk Authentication でサポートされている既存のデフォルト ロールから派生するロールです。

管理者の作成

管理者は、管理階層の同じまたは低いレベルに属し、かつ同じまたは小さいスコープを持っている他の管理者を作成できます。 例：

- MA は、ほかのすべてのタイプの管理者を作成できます。
- GA は自分のスコープ*内*に以下を作成できます。
  - 他の GA
  - OA
  - UA
- OA は自分のスコープ内に以下を作成できます。
  - 他の OA
  - UA

基本ユーザ名-パスワード認証情報のために設定される組織で管理者を作成する方法

1. 管理ユーザの作成に必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで、［**管理者の作成**］リンクをクリックし、［管理者の作成］ページを表示します。
4. ［**管理者詳細**］セクションで、管理者の詳細を入力します。 以下の表に、このページのフィールドの説明を示します。

入力	Description
User Name	管理者の一意のユーザ名。
組織	管理者が属する組織の表示名。 **注**: これはこの管理者が管理する組織では*ありません*。
［First Name］	管理者の名。
［Middle Name］（オプション）	管理者のミドル ネーム（ある場合）。
［Last Name］	管理者の姓。

5. ［**電子メール アドレス**］セクションで、組織に対して設定された電子メール タイプに管理者の電子メール アドレスを入力します。
6. ［**電話番号**］セクションで、管理者に問い合わせるための電話番号を入力します。

   複数の電話タイプが設定されている場合は、必須のすべての電話タイプに値を入力する*必要があります*。
7. ［**カスタム属性**］セクションで、勤務場所のように、追加したい任意の属性の**名前**と**値**を入力します。
8. ［**次へ**］をクリックして続行します。

   次のページが表示されます。
9. このページで、以下を実行します。
   - ［**ロール**］ドロップダウン リストから新しい管理者のロールを指定します。
   - ［**パスワードの設定**］セクションで、管理者にパスワードを設定して確認します。
   - ［**管理する**］セクションで、管理者がスコープを持っている組織を選択し、以下のいずれかを実行します。
     - この管理者にシステム内の現在および将来の組織をすべて管理させる場合は、［**全組織**］オプションを選択します。

       または
     - ［**利用可能な組織**］リストから必要な組織を選択し、［**>**］ボタンをクリックしてそれらの組織を［**選択された組織**］リストに追加します。

     ［**利用可能な組織**］リストには、この新規アカウントを作成する管理者のスコープ内で選択可能なすべての組織が表示されます。［**選択された組織**］には、管理者の管理対象として選択した組織のリストが表示されます。
10. ［**作成**］をクリックすると、変更が保存され、アカウントが作成されてアクティブになります。
11. 管理者に新しいパスワードを伝えます。

管理者のプロファイル情報の変更

アカウントのプロファイル情報には以下の項目が含まれます。

- 個人情報（姓、名、ミドル ネーム、および連絡先情報）
- アカウントのパスワード。
- 優先される組織（今後実行する可能性があるすべての管理者関連タスクの［組織］フィールドで、デフォルトで選択される**組織**）、日付/時刻形式、ロケール、およびタイム ゾーン情報などの管理者基本設定。

注: 管理者はいつでも各自のアカウントのプロファイル情報を変更できます。 その他の管理者アカウントの情報を変更する場合は、「管理者情報の更新」を参照してください。

基本ユーザ名-パスワード クレデンシャルを使って作成された自分のアカウントの管理者プロファイル情報を変更する方法

1. *自分のアカウント*にログインしていることを確認します。
2. **ヘッダ** フレームの <ADMINISTRATORNAME> リンクをクリックして、［マイ プロファイル］ページを表示します。
3. このページで、以下のように各セクション内の必要な設定を編集します。
   a. 必要に応じて、［個人情報］セクション内のフィールドを編集します。
   b. 現在のパスワードを変更する場合は、［**パスワードの変更**］セクションで［**現在のパスワード**］に入力し、［**新規パスワード**］フィールドと［**パスワードの確認**］フィールドに新しいパスワードを指定します。
   c. ［管理者基本設定］セクションで、以下を行います。
      - ［**優先組織の有効化**］オプションをオンにし、**優先組織**リストから組織を選択します。この組織は、今後実行するすべての管理者関連タスクで選択されます。
      - 優先される**日付/時刻形式**を指定します。
      - 使用する CA Advanced Authentication のインスタンスで優先される**ロケール**を選択します。
      - ［**タイム ゾーン**］リストから必要なオプションを選択します。
4. ［保存］ボタンをクリックすると、プロファイル情報が変更されます。

管理者の検索

注: 管理者アカウントを更新、アクティブ化、または非アクティブ化する必要がない限り、検索する権限は必要ありません。 ただし、管理者が属する組織がスコープに含まれている*必要があります*。 たとえば、対象となる組織が UA の権限の範囲内に*あれば*、UA はその組織の管理者を検索できます。

条件を指定して管理者を検索する方法

1. 必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 管理者のリストを表示するための検索条件を指定します。以下の操作を行うことができます。
   - このページの各フィールドに管理者の情報の一部または全部を指定して管理者を検索する。
   - 組織の表示名を指定して管理者を検索する。
   - 何も条件を指定せずに［**検索**］ボタンをクリックするだけで管理者を検索する。
   - ［**詳細検索**］リンクをクリックして［詳細検索］ページを表示し、管理者の［ステータス］または［ロール］を指定して必要な管理者を検索する。

   注: ［**ユーザ ステータス**］セクションで、ユーザ ステータス（［アクティブ］、［非アクティブ］、または［初期］）に基づいて［**現在のユーザ**］を検索できます。また、**削除されたユーザ**も検索できます。
5. またアカウント ID に基づいて管理者を検索する場合は、［**アカウント別検索の有効化**］を選択します。
6. 管理者の必要な詳細を指定し、［**検索**］ボタンをクリックします。

   検索条件に一致する管理者のリストが表示されます。

管理者情報の更新

注: 管理者情報を更新するには、適切な権限およびスコープがあることを確認する必要があります。MA はすべての管理者を更新できます。GA は、MA アカウントを*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を更新できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA を更新できます。一方、UA は自分のスコープに含まれる自分のピアのみを更新できます。

管理者の基本的な詳細（名、ミドル ネーム、姓、連絡先情報など）や管理者の管理ロール、パスワード、管理スコープを更新する方法

1. 管理ユーザの更新に必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、対応するページを表示します。
4. 前のセクションの説明に従ってアカウントを更新する管理者の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する管理者のリストが表示されます。
5. アカウントを編集する管理者の <*ユーザ名*> リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: 何らかのアカウント タイプが設定されている場合、このページには［**ユーザ アカウント情報**］（［**アカウント タイプ**］、［**アカウント ID**］、［**ステータス**］）も表示されます。
6. ［**編集**］をクリックし、このページで管理者情報を変更します。
7. ［**ユーザ詳細**］セクションで、必要なフィールド（［**名**］、［**ミドル ネーム**］、［**姓**］）を編集します。
8. ［**電子メール アドレス**］セクションで、組織に対して設定された電子メール タイプに電子メール アドレスを入力します。
9. ［**電話番号**］セクションで、組織に対して設定された電話タイプに電話番号を入力します。
10. ［**カスタム属性**］セクションで、カスタム属性の［**名**］および［**値**］を編集します。
11. ［**保存**］ボタンをクリックして変更を保存し、［基本ユーザ情報］ページに戻るか、または［**次へ**］ボタンをクリックして追加の設定に進みます。

注: ［**次へ**］ボタンが表示されない場合、アカウント タイプが組織に設定されていないことを意味します。 この場合は、［**管理者詳細の更新**］をクリックし、手順 14 に移動します。

［**次へ**］をクリックすると、［ユーザ アカウント］ページが表示されます。

12. ［**ユーザ アカウント**］セクションで、以下の操作を実行します。
    - ［**アカウント タイプ**］フィールドと［**ステータス**］フィールドを編集します。
    - ［**詳細属性**］を展開し、アカウント ID の **AccountID 属性**を追加します。

    注: これが作成する最初のアカウント ID である場合は、［**追加**］をクリックしてアカウント ID を追加してから更新します。 アカウント ID の追加の詳細については、「アカウントの作成」を参照してください。
    - アカウント タイプに対して設定する任意の［**カスタム属性**］の値を指定します。
13. ［**管理者詳細の更新**］をクリックします。

    ［**管理者の更新**］ページが表示されます。
14. このページの［**ロール**］セクションで、［**ロール**］ドロップダウン リストを使用して管理者のロールを変更します。
15. ［**パスワードの設定**］セクションで、以下の操作を実行します。
    - 管理者の［**パスワード**］と［**パスワードの確認**］を設定します。
    - ［**ロック**］を選択して、管理者の認証情報を［**認証情報ロック期間**］の期間ロックします。この期間は、［**開始**］フィールドと［**終了**］フィールドで指定できます。
16. ［**管理する**］セクションで、管理者が管理する組織を選択します。

    また、［**選択された組織**］から［**利用可能な組織**］に組織を移動させることにより、管理者のスコープから組織を削除できます。
17. ［**保存**］ボタンをクリックして更新を保存します。

管理者のロールをユーザへ変更

管理者のロールをユーザに変更することができます。たとえば、IT 部門の管理者がエンジニアリング部門に異動したとします。この場合、そのユーザの詳細は保持しますが、そのユーザの管理者権限は削除する必要があります。

管理者のロールをユーザに変更する方法

1. 前述の「管理者情報の更新」で説明されている手順 1 ～ 13 を実行します。

   ［管理者の更新］ページが表示されます。

2. ［管理者の更新］ページで、［**ロールをユーザに変更**］をクリックします。
3. 表示される確認ダイアログ ボックスで［**OK**］をクリックします。
4. 以下のメッセージが表示されます。

   管理者を正常に降格しました。

管理者用のアカウント ID の設定

アカウント ID は、ユーザを識別するためのユーザ名とは別の ID です。 組織で使用するアカウント タイプを設定した後、これらのアカウント タイプに対して、ユーザごとにアカウント ID を 1 つ関連付けることができます。 アカウント タイプの詳細については、「アカウント タイプの設定」を参照してください。

注: アカウント タイプに対してアカウント ID を設定するには、そのユーザ アカウントを更新するための適切な権限とスコープを持っていることを確認する必要があります。 MA は、すべてのユーザ アカウントを更新できます。GA は、スコープ内のすべてのユーザ アカウントを更新できます。OA と UA は、権限の範囲内でユーザ アカウントを更新できます。

アカウント ID の作成

アカウント ID を作成する方法

1. 管理者情報を更新するために必要な権限およびスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 前のセクションの説明に従ってアカウントを更新する管理者の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する管理者のリストが表示されます。
5. アカウントを編集する管理者の <*ユーザ名*> リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。
6. ［**編集**］をクリックして、［管理者の更新］ページを表示します。
7. ［**次へ**］をクリックして、［ユーザ アカウント］ページを表示します。
8. アカウント ID を追加する［**アカウント タイプ**］を選択します。
9. テキスト ボックスに一意の**アカウント ID** を指定します。

   このアカウント タイプとアカウント ID の組み合わせは、ユーザを識別するためにユーザ名に加えて使用されます。
10. ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
11. 必要に応じて、［**詳細属性**］セクションを展開し、以下の手順を実行します。
    - 作成するアカウント ID の属性を指定します。

    注: アカウント ID には最大 3 つのアカウント ID 属性を指定できます。
    - アカウント タイプに対して設定する任意の［**カスタム属性**］の値を指定します。
12. ［**追加**］をクリックして、アカウント ID を追加します。

アカウント ID の更新

注: アカウント ID を作成した後、それを変更することはできません。ユーザ アカウントのステータスを変更することと、アカウント ID 属性とカスタム属性を追加または削除することのみ可能です。

アカウント ID を更新する方法

1. 「アカウント ID の作成」の手順 1 ～ 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID 情報を更新する**アカウント タイプ**を選択します。
3. 必要に応じて、ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
4. 必要に応じて、［**詳細属性**］セクションを展開し、作成するアカウント ID の属性およびカスタム属性（ある場合）を指定します。
5. ［**更新**］をクリックして、変更内容を保存します。

アカウント ID の削除

アカウント ID を削除する方法

1. 「アカウント ID の作成」の手順 1 ～ 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID を削除する**アカウント タイプ**を選択します。
3. ［**削除**］をクリックして、アカウント ID を削除します。

管理者の非アクティブ化

セキュリティ上の理由で管理者が自分のアカウントにログインすることを禁止する場合は、アカウントを削除する代わりに、非アクティブ化することができます。 管理者を非アクティブにすると、管理者は自分のアカウントからロックアウトされ、アカウントを再度アクティブ化しない限りはログインできません。

注: 管理者を非アクティブにするには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての管理者を非アクティブ化できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を非アクティブ化できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA を非アクティブ化できます。一方、UA は自分のスコープに含まれる自分のピアのみを非アクティブ化できます。

管理者を非アクティブ化する方法

1. 管理者を非アクティブ化するために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. アカウントを非アクティブ化する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 非アクティブにする管理者を 1 人以上選択します。
6. ［**非アクティブ化**］ボタンをクリックして、選択した管理者を非アクティブにします。

管理者の一時的な非アクティブ化

管理者を*一時的に非アクティブ化*することは、管理者の*非アクティブ化*とは異なります（「管理者の非アクティブ化」を参照）。 一時的に管理者を非アクティブにした場合、ロック期間が終了すると、管理者は自動的にアクティブになります。 しかし、管理者を非アクティブにした場合、管理者がアクセスできるようにするには常に手動で再度アクティブ化する必要があります。

管理者を一時的に非アクティブにするには、管理者をロックする期間の**ロック開始日**と**ロック終了日**を指定する必要があります。 **ロック終了日**に到達すると、管理者は自動的にアクティブ化されます。

管理者を一時的に非アクティブ化する方法

1. 管理者を非アクティブ化するために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. アカウントを非アクティブ化する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 一時的に非アクティブにする管理者を 1 人以上選択します。
6. ［**一時的に非アクティブ化**］をクリックします。

   ［ユーザを一時的に非アクティブ化］ダイアログ ボックスが表示されます。
7. ［**開始日**］セクションで、ロックを開始する**日付**と**時間**を選択します。
8. ［**終了**］セクションで、ロックを終了する**日付**と**時間**を選択します。
9. ［**保存**］をクリックして変更内容を保存します。

   注: ［**開始日**］フィールドの値を指定しないと、アカウントは現在の時刻からロックされます。 ロック終了**日**を指定しないと、アカウントは永久的にロックされます。

管理者のアクティブ化

非アクティブになっている管理者をアクティブにする必要がある場合があります。 たとえば、管理者が長期休暇を取っているときには、管理者を非アクティブにしたい場合があります。 これによって、その管理者情報に対する不正アクセスを防止できます。

非アクティブ化されている管理者は、［ユーザと管理者の検索］ページで検索条件を指定して［**検索**］ボタンをクリックするだけでは直接検索できません。 このような管理者の場合には、［**詳細検索**］を実行し、［**現在のユーザ**］セクションで［**非アクティブ**］オプションを使用して検索*する必要があります。*

注: 管理者をアクティブにするには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべての管理者をアクティブ化できます。一方、GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）をアクティブ化できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA をアクティブ化できます。一方、UA は自分のスコープに含まれる自分のピアのみをアクティブ化できます。

非アクティブになっている管理者をアクティブにする方法

1. 管理者をアクティブにするために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. ［**詳細検索**］リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいて［**現在のユーザ**］を検索します。

   ［詳細検索］ページが表示されます。
5. ［**ユーザ詳細**］セクションに管理者の情報の一部または全部を入力します。
6. ［**ユーザ ステータス**］セクションで、［**現在のユーザ**］に対して［**非アクティブ**］オプションと［**初期**］オプションを選択し、すべての非アクティブまたは初期状態の管理者を検索します。
7. ［**検索**］ボタンをクリックすると、検索条件と一致するすべての管理者のリストが表示されます。
8. アクティブにする管理者を選択します。

9. ［**アクティブ化**］をクリックして、管理者をアクティブにします。

管理者の削除

CA Risk Authentication の管理者情報には、個人情報（名、ミドルネーム、姓、電子メール アドレス、電話番号）、認証情報、およびアカウントが含まれます。CA Advanced Authentication から管理者を削除する場合、認証情報とアカウント情報も個人情報と共に削除する必要があります。CA Risk Authentication は、管理者が削除されると管理者の認証情報、アカウント、およびリスク関連情報もすべて削除されるカスケード ユーザ削除機能をサポートしています。

以前に削除した管理者と同じ名前の管理者を新しく作成しても、新しい管理者が、以前に削除した管理者の権限を自動的に引き継ぐことは*ありません*。 削除した管理者を複製するには、すべての権限を手動で再作成する必要があります。

注: 管理者を削除するには、適切な権限およびスコープがあることを確認する必要があります。MA はすべての管理者を削除できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を削除できます。 OA は、自分の権限の範囲内にあるほかのすべての OA と UA を削除できます。

ただし、UA は、自分のスコープ内のピアを削除 *できません*。

管理者を削除する方法

1. 管理者を削除するために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 削除する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ステータス（アクティブ、非アクティブ、または初期）またはロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 削除する管理者を 1 人以上選択します。
6. ［**削除**］をクリックします。

注: 管理者を削除しても、そのアカウント情報はデータベースに引き続き保持されます。

第 13 章: ユーザの管理

CA Risk Authentication はユーザのアプリケーションと連携して動作し、管理者とエンドユーザのための強力な認証を管理します。 CA Risk Authentication では、CA Advanced Authentication を使用してユーザを直接作成できます。 ユーザ情報を管理することは、安全なシステムを維持するために非常に重要です。この目的のための CA Risk Authentication によってサポートされるエンドユーザ管理操作には、以下があります。

ユーザの作成

オンライン アプリケーション システムのすべてのエンド ユーザは、管理コンソール内でユーザと呼ばれます。GA（グローバル管理者）、OA（組織管理者）、および UA（ユーザ管理者）は、自分のスコープ内に組織のユーザを作成できます。

ユーザの作成方法

1. ユーザの作成に必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで、［**ユーザの作成**］リンクをクリックし、［ユーザの作成］ページを表示します。
4. ［**ユーザ詳細**］セクションで、ユーザの詳細を入力します。以下の表に、このページのフィールドの説明を示します。

フィールド	説明
ユーザ名	一意のユーザ名。
組織	ユーザが属する組織の表示名。
名（オプション）	ユーザの名。
ミドル ネーム（オプション）	ユーザのミドル ネーム（ある場合）。
姓（オプション）	ユーザの姓。

5. ［**電子メール アドレス**］セクションで、ユーザの電子メール アドレスを入力します。
6. ［**電話番号**］セクションで、ユーザに問い合わせるための電話番号を入力します。
7. ユーザを**初期**状態にするか、**アクティブ**にするかを選択します。
8. ［**カスタム属性**］セクションで、勤務場所のように、追加したい任意の属性の**名前**と**値**を入力します。
9. ［**ユーザの作成**］をクリックして、ユーザを作成します。

ユーザの検索

注: ユーザの作成、更新、アクティブ化、または非アクティブ化を行う必要がない場合は、検索の権限は必要ありません。ただし、ターゲット ユーザが属する組織に対するスコープを持つ*必要があります*。 たとえば、組織の GA は、他の組織が権限の範囲内である場合には、その組織のユーザを検索できます。

条件を指定してユーザを検索する方法

1. 適切なスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 検索するユーザの条件を指定します。以下の操作を行うことができます。
   - このページのフィールドでユーザの部分的または完全な情報を指定してユーザを検索します。

     注: フィールドに暗号化のためのマークがされて*いない*場合のみ、フィールドに部分的な情報を指定できます。 このページのいずれかのフィールドに暗号化のマークがされている場合、正しく機能するためには、検索する完全な値を正しく指定する*必要があります*。
   - 組織の表示名を指定してユーザを検索します。
   - 基準は何も指定せず、［**検索**］をクリックしてユーザを検索します。
   - ［**詳細検索**］リンクをクリックすると、［詳細検索］ページが表示されます。ステータスまたはロールを指定してユーザを検索します。
5. ユーザに関する必要な詳細情報を指定し、［**検索**］をクリックします。

   検索条件に一致したユーザのリストが表示されます。

ユーザ情報の更新

注: ユーザのアカウント設定を更新するには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべてのユーザの情報を更新できます。 GA は、自分のスコープに含まれるすべてのユーザを更新できます。 OA と UA は、権限の範囲内でユーザの情報を更新できます。

ユーザの基本的な詳細情報（名、ミドル ネーム、姓、連絡先情報など）を更新する方法

1. ユーザ情報を更新するために必要な権限およびスコープで、ログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. （前のセクションで説明されているように）アカウントを更新するユーザの部分的または完全な情報を入力し、［**検索**］をクリックします。

   検索条件に一致する管理者のリストが表示されます。
5. 編集するアカウントのユーザの *<user name>* リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: 何らかのアカウント タイプが設定されている場合、［基本ユーザ情報］ページには［**ユーザ アカウント情報**］（［**アカウント タイプ**］、［**アカウント ID**］、［**ステータス**］）も表示されます。
6. ［**編集**］をクリックし、このページのユーザ情報を変更します。
7. ［**ユーザ詳細**］セクションで、必要なフィールド（［**名**］、［**ミドル ネーム**］、［**姓**］）を編集します。
8. ［**電子メール アドレス**］セクションで、組織に対して設定された電子メール タイプに電子メール アドレスを入力します。
9. ［**電話番号**］セクションで、組織に対して設定された電話タイプに電話番号を入力します。
10. 必要に応じて、［**ユーザ ステータス**］を更新します。
11. 必要に応じて、［**カスタム属性**］の［**名前**］および［**値**］を編集します。

12. ［**保存**］ボタンをクリックして変更を保存し、［基本ユーザ情報］ページに戻るか、または［**次へ**］ボタンをクリックして追加の設定に進みます。

    注: ［**次へ**］ボタンは、組織のアカウントを設定している場合にのみ利用可能です。

    ［**次へ**］をクリックすると、［ユーザ アカウント］ページが表示されます。

13. ［**ユーザ アカウント**］セクションで、以下の操作を実行します。

    - 必要に応じて、［**ステータス**］を編集します。
    - ［**詳細属性**］を展開し、アカウント ID の［**AccountID 属性**］と［**カスタム属性**］を追加します。

    注: これが作成する最初のアカウント ID である場合は、［**追加**］をクリックしてアカウント ID を追加してから更新します。 アカウント ID の追加の詳細については、「アカウントの作成 (P. 316)」を参照してください。

14. ［**更新**］をクリックして、変更内容を保存します。

ユーザを管理者レベルに上げる

注: ユーザを管理者レベルに上げるには、適切な権限およびスコープがあることを確認する必要があります。 MA は、すべてのユーザのレベルを上げることができます。 GA は、管理権限の範囲内で、ユーザを組織の OA、UA、GA のレベルに上げることができます。OA は、管理権限の範囲内で、ユーザを組織の OA または UA のレベルに上げることができます。 UA は、ユーザを管理者レベルに上げることが *できません*。

ユーザの管理ロール、パスワード、および管理スコープを更新する方法

1. 管理者を作成しユーザ情報を更新するために必要な権限およびスコープで、ログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. （前のセクションで説明されているように）アカウントを更新するユーザの部分的または完全な情報を入力し、［**検索**］をクリックします。

   検索条件に一致したユーザのリストが表示されます。
5. 編集するアカウントのユーザの *<user name>* リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。
6. ［**編集**］をクリックして、［ユーザの更新］ページを表示します。
7. ユーザの［**名**］、［**姓**］、［**電子メール アドレス**］、［**電話番号**］が指定されていない場合は、これらを入力します。 これらの属性は管理者にとって必須です。
8. ［**次へ**］をクリックして、［ユーザ アカウント］ページを表示します。

   注: ユーザの組織に対してアカウント タイプが設定されていない場合は、［**ロールを管理者に変更**］ボタンが［ユーザの更新］ページに表示されます。
9. ［ユーザ アカウント］ページで、［**ロールを管理者に変更**］をクリックして、［管理者の作成］ページを表示します。
10. このページで、以下の作業を実行します。
    - ［**ロール**］ドロップダウン リストから新しい管理者のロールを指定します。

- ［**パスワード**］フィールドと［**パスワードの確認**］フィールドに管理者のパスワードを入力します。
- ［**管理する**］セクションで、管理者がスコープを持っている組織を選択し、以下を実行します。
  - この管理者にシステム内の現在および将来の組織をすべて管理させる場合は、［**全組織**］オプションを選択します。

    または
  - ［**利用可能な組織**］リストから必要な組織を選択し、［**>**］ボタンをクリックしてそれらの組織を［**選択された組織**］リストに追加します。

  ［**利用可能な組織**］には、ログインしている管理者のスコープで利用可能なすべての組織が表示されます。［**選択された組織**］には、管理者の管理対象として選択した組織のリストが表示されます。

11. ［**作成**］をクリックして、変更の保存、管理者の作成およびアクティブ化を行います。

ユーザのアカウント ID の設定

アカウント ID は、ユーザを識別するためのユーザ名とは別の ID です。組織で使用するアカウント タイプを設定した後、これらのアカウント タイプに対して、ユーザごとにアカウント ID を 1 つ関連付けることができます。アカウント タイプの詳細については、「アカウント タイプの設定」を参照してください。

注: アカウント タイプに対してアカウント ID を設定するには、ユーザを更新するための適切な権限とスコープを持っていることを確認する必要があります。MA は、すべてのユーザを更新できます。GA は、自分のスコープに含まれるすべてのユーザを更新できます。OA と UA は、権限の範囲内でユーザを更新できます。

アカウント ID の作成

アカウント ID を作成する方法

1. ユーザの更新に必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. アカウント ID を作成するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 編集するアカウントのユーザの *<user name>* リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: このページには、設定されているアカウント タイプの［**ユーザ アカウント情報**］（［**アカウント タイプ**］、［**アカウント ID**］、［**ステータス**］）も表示されます。
6. ［**編集**］をクリックして、［ユーザの更新］ページを表示します。
7. ［**次へ**］をクリックして、［ユーザ アカウント］ページを表示します。
8. アカウント ID を追加する［**アカウント タイプ**］を選択します。
9. テキスト ボックスに一意の**アカウント ID** を指定します。

   このアカウント タイプとアカウント ID の組み合わせは、ユーザを識別するためにユーザ名に加えて使用されます。アカウント タイプとアカウント ID の組み合わせが特定の組織にとって一意であることを確認する必要があります。
10. ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
11. 必要に応じて、［**詳細属性**］セクションを展開し、以下の手順を実行します。

    a. アカウント ID の［**AccountID 属性**］を指定します。

    注: アカウント ID には最大 3 つの属性を指定できます。

b. アカウント タイプに対して設定する任意の［**カスタム属性**］の値を指定します。

12. ［**追加**］をクリックして、アカウント ID を追加します。

アカウント ID の更新

注: アカウント ID を作成した後、それを変更することはできません。ユーザ アカウントのステータスを変更することと、アカウント ID 属性を追加することのみ可能です。

アカウント ID を更新する方法

1. 「アカウント ID の作成 (P. 316)」の手順 1 ～ 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID を更新する［**アカウント タイプ**］を選択します。
3. 必要に応じて、ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
4. 必要に応じて、［**詳細属性**］セクションを展開し、更新するアカウント ID の［**AccountID 属性**］と［**カスタム属性**］を指定します。
5. ［**更新**］をクリックして、変更内容を保存します。

アカウント ID の削除

アカウント ID を削除する方法

1. 「アカウント ID の作成 (P. 316)」の手順 1 ～ 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID を削除する**アカウント タイプ**を選択します。
3. ［**削除**］をクリックして、アカウント ID を削除します。

ユーザの非アクティブ化

セキュリティ上の理由でユーザがアカウントにログインすることを禁止する場合は、アカウントを削除する代わりに、非アクティブ化することができます。ユーザを非アクティブにすると、ユーザはアカウントからロックされ、再度アクティブ化するまでログインできなくなります。

注: ユーザを非アクティブにするには、適切な権限およびスコープがあることを確認する必要があります。MA はすべてのユーザを非アクティブ化できます。GA はスコープ内のほかの GA を含むすべてのユーザを非アクティブ化できます。 OA と UA は、権限の範囲内ですべてのユーザを非アクティブ化できます。

ユーザを非アクティブ化する方法

1. ユーザの非アクティブ化に必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. アカウントを無効にするユーザの部分的または完全な情報を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 非アクティブにするユーザを 1 人以上選択します。
6. ［**非アクティブ化**］ボタンをクリックして、選択したユーザを非アクティブにします。

ユーザの一時的な非アクティブ化

ユーザを*一時的に非アクティブ化*することは、ユーザの*非アクティブ化*と異なります（「ユーザの非アクティブ化 (P. 318)」を参照）。一時的にユーザを非アクティブにした場合、ロック期間が終了すると、ユーザは自動的にアクティブになります。しかし、ユーザを非アクティブにした場合、ユーザがアクセスできるようにするには常に手動で再度アクティブ化する必要があります。

ユーザを一時的に非アクティブにするには、ユーザをロックする**ロック開始日**と**ロック終了日**を指定する必要があります。**ロック終了日**に到達すると、ユーザは自動的にアクティブ化されます。

ユーザを一時的に非アクティブ化する方法

1. ユーザの非アクティブ化に必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 非アクティブ化するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 一時的に非アクティブにするユーザを 1 人以上選択します。
6. ［**一時的に非アクティブ化**］をクリックします。
7. ［ユーザを一時的に非アクティブ化］ページが表示されます。
8. ［**開始日**］セクションで、ロックを開始する**日付**と**時間**を選択します。
9. ［**終了**］セクションで、ロックを終了する**日付**と**時間**を選択します。
10. ［**保存**］をクリックして変更内容を保存します。

    注: ［**開始日**］フィールドの値を指定しないと、ユーザは現在の時刻からロックされます。ロック終了**日**を指定しないと、アカウントは永久的にロックされます。

ユーザのアクティブ化

非アクティブになっているユーザをアクティブにする必要がある場合があります。 たとえば、管理者が長期休暇を取っているときには、管理者を非アクティブにしたい場合があります。 これによって、その管理者の情報に対する不正アクセスを防止できます。

非アクティブ化されているユーザは、［ユーザと管理者の検索］ページで検索条件を指定して［**検索**］ボタンをクリックするだけでは直接検索できません。 このようなユーザの場合には、［**詳細検索**］を実行し、［**現在のユーザ**］セクションで［**非アクティブ**］オプションを使用して検索する必要があります。

注: ユーザをアクティブにするには、適切な権限およびスコープがあることを確認する必要があります。 MA はすべてのユーザをアクティブ化できます。GA はスコープ内のすべてのユーザをアクティブ化できます。 OA と UA は、権限の範囲内ですべてのユーザをアクティブ化できます。

ロックされているユーザをアクティブ化する方法

1. ユーザをアクティブにするために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. ［**詳細検索**］リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいて［**現在のユーザ**］を検索します。

   ［詳細検索］ページが表示されます。
5. ［**ユーザ詳細**］セクションにユーザの情報の一部または全部を入力します。
6. ［**ユーザ ステータス**］セクションで、［**現在のユーザ**］に対して［**非アクティブ**］オプションと［**初期**］オプションを選択し、すべての非アクティブまたは初期状態のユーザを検索します。
7. ［**検索**］をクリックすると、検索条件に一致するすべてのユーザのリストが表示されます。
8. アクティブにするユーザを選択します。
9. ［**アクティブ化**］をクリックして、ユーザをアクティブ化します。

ユーザの削除

RiskMinder のユーザ情報には、個人情報（名、ミドルネーム、姓、電子メール アドレス、電話番号）、認証情報、およびアカウントが含まれます。 管理コンソールからユーザを削除する場合、認証情報とアカウント情報も個人情報と共に削除する必要があります。 RiskMinder は、ユーザが削除されるとユーザの認証情報、アカウント、およびリスク関連情報もすべて削除されるカスケード ユーザ削除機能をサポートしています。

以前に削除したユーザと同じ名前のユーザを新しく作成しても、新しいユーザが、以前に削除したユーザの権限を自動的に引き継ぐことは*ありません*。 削除したユーザを複製するには、すべての権限を手動で再作成する必要があります。

注: ユーザを削除するには、適切な権限およびスコープがあることを確認する必要があります。MA はすべてのユーザを削除できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれるすべてのユーザ（ほかの GA を含む）を削除できます。OA と UA は、権限の範囲内ですべてのユーザを削除できます。

ユーザを削除する方法

1. ユーザを削除するために必要な権限でログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 削除するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブ、非アクティブ、または初期）またはロール（ユーザ）に基づいてユーザを検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 削除するユーザを 1 人以上選択します。
6. ［**削除**］をクリックします。

   注: ユーザを削除すると、ユーザ情報はデータベースから削除されます。 ただし、ユーザの履歴は課金の目的でアーカイブされます。

第 14 章: システム管理者用のツール

このセクションでは、RiskMinder が提供するツールについて説明します。これらのツールを使用して管理者はシステムを監視し管理することができます。 以下の表に、ツールとその場所を示します。

ツール	場所
DBUtil	**Windows の場合** <*install_location*>¥Arcot Systems¥tools¥win **UNIX プラットフォームの場合** <*install_location*>/arcot/tools/<*platform_name*>
arrfversion arrfclient arrfserver arrfupload	**Windows の場合** <*install_location*>¥Arcot Systems¥bin¥ **UNIX プラットフォームの場合** <*install_location*>/arcot/bin/

このセクションでは以下のツールについて説明します。

- DBUtil: RiskMinder データベース ツール (P. 324)
- arrfversion: RiskMinder モジュール バージョン表示ツール (P. 330)
- arrfclient： サーバ リフレッシュとシャットダウン ツール
- arrfserver: RiskMinder サーバ ツール (P. 334)
- arrfupload: Quova データ アップロード ツール (P. 336)

DBUtil: RiskMinder データベース ツール

RiskMinder のインストール時に、インストーラは、RiskMinder データベースに接続するための情報を収集します。 インストールが完了すると、この情報は securestore.enc と呼ばれるファイルに暗号化された形式で格納されます。 このファイルは、RiskMinder データベースに接続するのに必要な以下の暗号化された情報を格納します。

- データベース ユーザの名前とパスワード（RiskMinder サーバがデータベースに接続するために使用）
- マスタ キー（securestore.enc に格納されるデータベース ユーザの名前とパスワードを暗号化するために使用）

RiskMinder では、データを保護するためにソフトウェア モードとハードウェア モードの両方をサポートしています。 DBUtil ツールは、この両方のモードのデータベース操作を実行するために使用できます。

何らかの理由により、インストール*後*に新しいデータベース ユーザの名前、パスワード、または DSN を追加したり、マスタ キー値を変更したりする必要がある場合は、DBUtil を使用して以下を実行することができます。

このセクションでは、以下のトピックについて説明します。

- DBUtil オプションの使用法
- マスタ キーの更新

注: マスタ キーは機密情報の暗号化に使用するため、セキュリティ上の理由から、DBUtil ツールにはこのキーの値を表示するオプションが*ありません*。

DBUtil オプションの使用法

以下の表に、DBUtil のオプションを示します。この表では、*キーと値*のペアは DSN/パスワードまたはデータベース ユーザ名/パスワード ペアのいずれかを指します。CA Risk Authentication サーバは DSN/パスワードを使用しますが、CA Advanced Authentication およびユーザ データ サービスはユーザ名/パスワードを使用します。

重要: **注**: マスタ キーは機密情報の暗号化に使用されるため、セキュリティ上の理由から、DBUtil ツールにはこのキー値を表示するオプションが*ありません*。

オプション	Description
-h	ツールのヘルプを表示します。 構文 **dbutil -h**
-init	指定した新しいマスタ キーで新しい securestore.enc を作成します。「マスタ キーの更新」を参照してください。 構文 **dbutil -init key** 例： dbutil -init MasterKeyNew dbutil -init RiskFortDatabaseMKNew **重要**: このコマンドは conf ディレクトリに securestore.enc がない場合にのみ、成功します。

オプション	Description
-pi	追加のキーと値のペアを securestore.enc に挿入します。 構文 **dbutil -pi <key> <value> [-h HSMPin [-d HSMModule]]** **securestore.enc** が HSM 暗号化法によって保護される場合は、**-h HSMPin** が必要です。 **-d HSMModule** は **-h** を指定する場合のオプションです。 デフォルトは「nfast」 （NCipher です）。 例： dbutil -pi RiskFortBackupDSN dbapassword dbutil -pi Jack userpassword dbutil -pi Jack userpassword -h hsmpassword -d chrysalis **重要**: 各キーは 1 つの値のみを持つことができます。 すでにキーと値のペアを挿入している場合、同じキーに別の値を挿入することはできません。
-pu	securestore.enc にすでに存在するキーと値のペアの値を更新します。 この機能はデータベース パスワードを更新する必要がある場合に使用できます。 構文 **dbutil -pu <key> <value> [-h HSMPin [-d HSMModule]]** 例： dbutil -pu RiskFortDatabaseDSN newPassword dbutil -pu Jack userPassword dbutil -pu Jack userpassword -h hsmpassword -d chrysalis
-pd	指定したキーと値のペアを securestore.enc から削除します。 構文 **dbutil -pd <key> [-h HSMPin [-d HSMModule]]** 例： dbutil -pd RiskFortDatabaseDSNOld dbutil -pd Jack

オプション	Description
-i	securestore.enc ファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、指定するプライマリの名前と値のペアをこのファイルに挿入します。これは HSM 初期化情報を提供するためにサーバ スタートアップ時に使用されます。 構文 **dbutil -i <primeKey> <HSMPin>** *primeKey* には、HSM モジュールの名前を指定します。 例： dbutil -i chrysalis hsmpassword
-u	securestore.enc ファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、このファイルに指定されたプライマリの名前と値のペアを更新します。 構文 **dbutil -u <primeKey> <HSMPin>** *primeKey* には、HSM モジュールの名前を指定します。 例： dbutil -u chrysalis newhsmpassword
-d	securestore.enc ファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、このファイルに指定されたプライマリの名前と値のペアを削除します。 構文 **dbutil -d <primeKey>** *primeKey* には、HSM モジュールの名前を指定します。 例： dbutil -d chrysalis

マスタ キーの更新

インストール中に指定されたマスタ キーは *securestore.enc* ファイル内の値を暗号化するために使用されます。また、この製品によって使用され、CA Risk Authentication データベースに格納される暗号化キーもすべて暗号化します。

セキュリティ上の理由で、securestore.enc 内のマスタ キー値を変更する必要がある場合は、以下の操作を実行します。

1. 現在の securestore.enc ファイルをバックアップします。

   現在の securestore.enc は以下の場所にあります。

   - **Windows の場合**
     `<install_location>¥Arcot Systems¥conf`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/conf`

2. ARCOT_HOME¥conf 内の securestore.enc を削除します。
3. DBUtil がある以下の場所に移動します。

   - **Windows の場合**
     `<install_location>¥Arcot Systems¥tools¥win`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/tools/<platform_name>`

4. 以下のコマンドを実行します。
   （ソフトウェア モードの場合） `dbutil -init <master_key_name>`
   （ハードウェア モードの場合） `dbutil -init <HSM_Key_Label>`

   ツールは指定されたマスタ キー名を持った securestore.enc を再作成します。

   重要: マスタ キーの設定が失敗した場合は、CA サポートにお問い合わせください。

5. securestore.enc ファイル内のデータベース情報を更新します。

   CA Risk Authentication インストーラは、securestore.enc にデータベース ユーザ名/パスワードおよびデータベース DSN/パスワード情報を自動的に設定します。 ただし、新しい securestore.enc ファイルを作成した後は、この情報を手動で新しいファイルに挿入する必要があります。このためには dbutil -pi オプションを使用する必要があります。

   提供されたデータベースの値を securestore.enc に挿入するには、以下のコマンドを使用します。

- （ソフトウェア モードの場合） dbutil -pi <*dbUser*> <*dbPassword*>
- （ハードウェア モードの場合）dbutil -pi <*dbUser*> <*dbPassword*> *[*-h *HSMPin [*-d *HSMModule]]*

  上記のコマンドで、dbUser はデータベース ユーザ名、dbPassword は指定されたユーザ名に関連付けられたパスワードです。 例：

  dbutil -pi arcotuser welcome123

注: このコマンドで指定するユーザ名では大文字と小文字が区別されます。

- （ソフトウェア モードの場合） dbutil -pi <*dsn*> <*dbPassword*>
- （ハードウェア モードの場合） dbutil -pi <*dsn*> <*dbPassword*> *[*-h *HSMPin [*-d *HSMModule]]*

  上記のコマンドで、dsn はデータ ソース名です。また dbPassword はデータベースのパスワードです。 例：

  dbutil -pi arcotdsn welcome123

注: このコマンドで指定する DSN 名では大文字と小文字が区別されます。

6. CA Risk Authentication の分散展開を実行した場合は、新しい securestore.enc ファイルを CA Risk Authentication のコンポーネントがインストールされているすべてのシステムにコピーする必要があります。

arrfversion: RiskMinder モジュール バージョン表示ツール

arrfversion ツールを使用すると、RiskMinder ルールおよびプラグイン モジュール（Windows 上の .dll ファイルおよび UNIX ベース プラットフォーム上の .so）のバージョンをチェックして表示することができます。これらのモジュールは以下のディレクトリにあります（ARCOT_HOME からの相対パス）。

- **/bin/**
- /plugin/**rules/**
- /plugin/rules/**addon/**

展開および操作に関連する問題について CA サポートに問い合わせる場合は、展開したモジュールのバージョンを指定するようにしてください。これは問題をより早く識別して解決するのに役立ちます。

構文

このツールを使用するための構文は以下のとおりです。

```
arrfversion <library1_path> [<library2_path> ...]
```

上記の構文では、*<libraryN_path>* 文字列に以下のように個々のモジュールの名前を指定します。

- **Windows の場合は** aradminprotocol.dll
- **UNIX ベースのプラットフォームの場合は** libaradminprotocol.so

ライブラリ モジュールの絶対パスを指定しなかった場合、指定されたモジュールは標準的な環境変数によって指定されたフォルダ内で参照されます。 以下に例を示します。

- **Windows の場合は** %PATH%
- **UNIX ベースのプラットフォームの場合は** $LD_LIBRARY_PATH

例 :

- **Windows の場合：**

  ```
  arrfversion ScoreEngine.dll
  ```

- **UNIX ベースのプラットフォームの場合**

  ```
  arrfversion /opt/arcot/plugins/rules/libaradminprotocol.so
  ```

arrfversion : CA Risk Authentication モジュール バージョン表示ツール

arrfversion ツールを使用すると、CA Risk Authentication ルールおよびプラグイン モジュール（Windows 上の .dll ファイルおよび UNIX ベース プラットフォーム上の .so）のバージョンをチェックして表示することができます。これらのモジュールは以下のディレクトリにあります（ARCOT_HOME からの相対パス）。

- **/bin/**
- /plugin/**rules/**
- /plugin/rules/**addon/**

展開および操作に関連する問題について CA サポートに問い合わせる場合は、展開したモジュールのバージョンを指定するようにしてください。これは問題をより早く識別して解決するのに役立ちます。

構文

このツールを使用するための構文は以下のとおりです。

```
arrfversion <library1_path> [<library2_path> ...]
```

上記の構文では、<*libraryN_path*> 文字列に以下のように個々のモジュールの名前を指定します。

- **Windows の場合は** aradminprotocol.dll
- **UNIX ベースのプラットフォームの場合は** libaradminprotocol.so

ライブラリ モジュールの絶対パスを指定しなかった場合、指定されたモジュールは標準的な環境変数によって指定されたフォルダ内で参照されます。 例 :

- **Windows の場合は** %PATH%
- **UNIX ベースのプラットフォームの場合は** $LD_LIBRARY_PATH

例 :

- **Windows の場合 :**
  ```
  arrfversion ScoreEngine.dll
  ```
- **UNIX ベースのプラットフォームの場合**
  ```
  arrfversion /opt/arcot/plugins/rules/libaradminprotocol.so
  ```

ツールを使用する前に

ツールを使用する前に、riskfortadminclient.ini の設定を構成する必要があります。 このファイルは以下の場所にあります。

Windows の場合

<*install_location*>¥Arcot Systems¥conf¥

UNIX プラットフォームの場合

<*install_location*>/arcot/conf/

注: riskfortadminclient.ini の詳細については、「*CA CA Risk Authentication インストールおよび展開ガイド*」の「設定ファイルおよびオプション」を参照してください。

ツールが正しく動作するために最低限設定する必要があるこのファイル内のパラメータを、以下の表に示します。

パラメータ	デフォルト	Description
ホスト	localhost	CA Risk Authentication サーバが実行されているシステムのホスト名または IP アドレス。
ポート	7980	サーバがサーバ管理リクエストを待ち受けるポート番号。
Transport	tcp	サーバ管理リスナの転送モード。

これらの設定は、ツールと CA Risk Authentication サーバ間の典型的な TCP ベースの通信を保証します。

対話モードでのツールの実行

ツールを対話モードで実行するには、-i オプションを指定します。 このモードで実行すると、サーバは固有のコンソール プロンプト（#）を開始します。 対話モードで arrfclient ツールを実行する方法

1. ツールが利用可能な場所に移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/bin/`
2. 以下のコマンドを実行します。
   `arrfclient -i`
   ツールが対話モードで起動されます。
3. 以下の表に示すオプションを指定して、必要なタスクを実行します。

Options	Description
?	arrfclient によってサポートされているすべてのオプションのコマンドを表示します。
cr	サーバ インスタンスのキャッシュをリフレッシュします。インスタンス IP および サーバ管理ポート番号を入力する必要があります。 ■ インスタンス IP は、CA Risk Authentication サーバまたはケース管理キュー サーバが利用可能な IP アドレスまたはホスト名です。 ■ CA Risk Authentication サーバまたはケース管理キュー サーバが操作リクエストをリスンするポート番号。 **注**: デフォルトでは、CA Risk Authentication サーバはポート 7980 で利用可能です。 操作が正常に完了すると、メッセージ「Instance refreshed successfully」とトランザクション ID が返されます。
sd	CA Risk Authentication サーバ インスタンスをシャットダウンします。 インスタンス IP およびサーバ管理ポート番号を入力する必要があります。 操作が正常に完了すると、メッセージ「Successfully initiated shutdown operations」とトランザクション ID が返されます。
q	対話モードを終了します。

arrfserver: RiskMinder サーバ ツール

arrfserver ツールを使用すると、RiskMinder サーバ接続エラー（たとえば、動作していない場合）のトラブルシューティングを行い、対話モードでコマンド ラインから以下の設定を行うことができます。

- RiskMinder Web サービスのための認証と許可の設定。
- ほとんど使用されないか、または特定の展開シナリオ下でのみ必要な RiskMinder の設定。
- 管理コンソールでは表示されない RiskMinder の設定。

対話モードでのツールの実行

ツールを対話モードで実行するには、-i オプションを指定します。 このモードでは、リスナは起動されませんが、すべてのサーバ設定はサービス モードとほとんど同様の方法で実行されます。

このモードで実行すると、サーバは固有のコンソール プロンプト（#）を開始します。 arrfserver ツールを実行するには、以下の手順に従います。

1. ツールが利用可能な場所に移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/bin/`
2. 以下のコマンドを実行します。
   ```
   arrfserver -i
   ```
   ツールが対話モードで起動されます。
3. 以下の表に示すオプションを指定して、必要なタスクを実行します。

オプション	説明
?	arrfserver によってサポートされているすべてのオプションのコマンドを表示します。
??	指定したパターンに基づいてコマンドを検索します。 たとえば、「?? conf 」と入力すると、パターンに一致するすべてのツール オプションが表示されます。

オプション	説明
help	指定されたコマンドについてより詳細に説明します。 たとえば、「help setsaconf」と入力すると、コマンドの使用方法の簡単な説明が表示されます。
setsaconf	認証と許可を行うために RiskMinder サーバによって提供されている Web サービス API を設定します。 **注**: このオプションを使用 *しないでください*。このオプションは、認証と許可用に Web サービスを設定するために以前のリリースで使用されていました。認証と認可用の Web サービスの有効化の詳細については、「Web サービス認証および許可の設定」を参照してください。
q	対話モードを終了します。

arrfupload: Quova データ アップロード ツール

RiskMinder は、トランザクションの発生元であるシステムの IP アドレスを使用することによって、Quova データからユーザの地理的位置情報を特定します。 その後、このデータから、拒否国、拒否 IP、およびゾーン ホッピングのルールを評価します。

詳細については、「信頼できない IP タイプの設定 (P. 210)」、「リスト データのアップロード (P. 232)」、および「ゾーン ホッピングの設定 (P. 216)」を参照してください。 また、IP の地理的位置データが RiskMinder でどのように使用されるかについては、「地理的位置およびアノニマイザのデータ (P. 447)」を参照してください。

Quova とそのサービスの詳細については、以下のサイトを参照してください。

http://www.quova.com

注: Quova データは定期的にダウンロードする必要があります。 地理的位置に関する情報のデータ ファイルは毎週ダウンロードする必要がありますが、アノニマイザに関するデータ ファイルは毎月ダウンロードする必要があります。 ダウンロード手順の詳細については、CA サポートにお問い合わせください。

Arcot RiskMinder データ アップロード ツール（arrfupload）は、Quova ファイルから RiskMinder データベースに地理的位置データをアップロードできるコマンド ライン ユーティリティです。

ツールを使用する前に

riskfortdataupload.ini ファイルは、CA Risk Authentication データ アップロード ツールの動作を制御します。 これは以下の場所にあります。

Windows の場合

<*install_location*>¥Arcot Systems¥**conf**¥

UNIX プラットフォームの場合

<*install_location*>/arcot/**conf**/

ツールを使用するには、このファイルにパラメータを設定する必要があります（以下の表を参照）。

パラメータ	デフォルト	Description
Tables	ロードしない	ユーザが操作できるテーブル。 以下の値が使用可能です。 ■ GeoPoint ■ Anonymizer
Load	0	テーブルにデータをアップロードするかどうかのインジケータ。 以下の値が使用可能です。 ■ 0（ロードしない） ■ 1（ロードする）
Swap	0	GeoPoint または GeoAnonymizer のデータがアップロードされたばかりの表を使用して開始するように CA Risk Authentication 設定を切り替えるかどうかを示すインジケータ。 **重要**: CA Risk Authentication サーバ キャッシュはこの変更の後にリフレッシュする必要があります。 以下の値が使用可能です。 ■ 0（スワップしない） ■ 1（スワップする）
Filename	--	Quova データのロード元となるファイルの名前。 **重要**: ファイル名と共にファイルの絶対パスを指定する必要があります。

注: Load と Swap の両方を 1 に設定した場合、テーブルは最初にロードされてからスワップされます。

ツールの使用

このツールは以下の場所にあります。

Windows の場合

```
<install_location>¥Arcot Systems¥bin¥
```

UNIX プラットフォームの場合

```
<install_location>/arcot/bin/
```

このツールは、arcotcommon.ini ファイルのデータベース情報を使用して CA Risk Authentication データベースに接続し、securestore.enc ファイルに指定されているユーザ名とパスワードを使用してデータベースへの認証を行います。

構文

ツールを使用するには、以下のコマンドを実行します。

```
arrfupload <option>
```

重要: このツールを使用してアップロードした Quova 情報は、RiskMinder サーバ キャッシュをリフレッシュするまで使用することはできません。キャッシュをリフレッシュする手順については、「キャッシュのリフレッシュ」を参照してください。

以下の表に、ユーティリティでサポートされているオプションを示します。

Options	Description
-help	ツールでサポートしているオプションをすべて表示し、オプションの簡単な使用方法をその後に示します。

Options	Description
-config	このオプションを使用して riskfortdataupload.ini（ツールが使用する設定ファイル）から情報を読み取り、必要なアクションを実行します。 このオプションでは以下のフラグを使用します。 ■ Tables： ユーザが更新する表のセット。 指定可能な値は Geopoint または Anonymizer のいずれかです。 どちらも指定されない場合、データはアップロードされません。 このオプションにはデフォルト値はありません。 ■ Load：1 に設定されている場合はデータがアップロードされることを示し、0 に設定されている場合はデータがアップロードされないことを示します。 デフォルト値は 0 です。 **重要**: 1 に設定する場合は、Filename と Tables のフラグを設定する*必要があります*。 ■ Swap： 1 に設定されている場合は表が交換されることを示し、0 に設定されている場合は表が交換されないことを示します。 デフォルト値は 0 です。 **重要**: Tables フラグが正しく設定されている場合のみ、このフラグは有効です。また、新規の表を使用するには CA Risk Authentication サーバ キャッシュをリフレッシュする必要があります。 ■ Filename： アップロードされるデータが含まれている Quova ファイルの名前とパスを示します。 **重要**: Load フラグが 1 に設定される場合のみ、このフラグは有効です。
-tnames	このオプションを使用して、CA Risk Authentication データベースによって使用されている現在の ARQGeoPoint および ARQGeoAnonymizer の表を表示します。

Options	Description
-prompt	このオプションを使用して、ユーザが最新の Quova データを使用して更新する表（ARQGeoPoint または ARQAnonymizer）を選択できるようにする対話型コマンド ライン メニューを表示します。 ユーザによって指定された表に基づいて、以下のオプションを選択するサブメニューが表示されます。 ■ ［**Load Quova Data**］：メイン メニューから選択された表のセットに応じて、データを指定された表にロードすることができます。Quova データをロードする必要があるファイルの名前およびこのファイルのパスを指定する必要があります。 ■ ［**Swap Quova Tables**］：メイン メニューから選択された表のセットに応じて、ユーザは表を交換することができます。 ■ ［**Exit to the previous menu**］：ユーザはメイン メニューに移動することができます。 ■ ［**Exit the program**］：ユーザはツールを終了することができます。
-prompt <<*Table name*> <*Load*> <*Swap*> <*Absolute path of the file*>> [<*Table name*> <*Load*> <*Swap*> <*Absolute path of the file*>]	このオプションは、GeoAnonymizer および GeoPoint データの両方をアップロードするスケジュールされたタスクを設定するために使用されます。

第 15 章: ケース管理

ケース管理は、ユーザ管理者（UA）および不正行為アナリスト（FA）にケースに、関連データの単一の統一ビューを提供します。 これによってより効率的にデータを分析し、ケースの解決に向けてより速く、適切な情報に基づいて決定を行うことができます。 さらに、アナリストは、ケースのステータスおよび進捗状況を常時追跡し、ケースの完全な履歴を保持すると共に、すべての関連情報へ即座にアクセスできます。

重要: このセクションでは、テクニカル サポート担当者が実行できるタスク（「ケース管理の概要 (P. 342)」）、不正行為アナリストのみが実行できるタスク（「不正行為の分析 (P. 363)」）、およびキュー マネージャが実行できるタスク（「キューの新規作成 (P. 364)」）があります。ただし、組織管理者（OA）およびグローバル管理者（GA）には、範囲内にある組織でこれらのタスクを処理するためのすべての権限があります。

この機能を使用すると、以下の作業が可能です。

- 顧客サービスおよびサポートを効率的に管理する
- 多数のケースおよび調査を管理する
- 期限付きのアクションおよびタスクを作成する
- 期限付きのアクションを割り当てる
- ユーザに提供する調査メモおよび解決策を記録する
- ケースとタスクをより効率的に処理する
- ケースにおけるアクションの明瞭な追跡記録または履歴を保持する
- 傾向を分析する
- 不正行為に関連するレポートを生成する

このセクションには、以下のトピックが含まれています。

ケース管理の概要

ケース管理機能により、トランザクションを調査し、疑わしいとマークされたトランザクションを直観的および効率的に管理できます。 この機能により、明確で包括的なアクティビティの記録が作成され、調査の各局面を記録して文書化するという課題に容易に取り組むことができます。 また、この機能では、理由の詳細なリスト、推奨事項、地理的位置情報、接続詳細およびリスク評価の詳細など、検索結果のレポートが自動的に作成されるため、時間を節約できます。

このセクションでは、以下のセクションの情報を参考にして、管理対象のケース（以下「ケース」）に関連する重要なポイントについて説明します。

- ケースの基本（P. 343）
- ケース管理のコンポーネント（P. 344）

ケースの基本

CA Advanced Authentication で管理されるケースの要点を以下に示します。

- CA Advanced Authentication システムでアドバイスの結果が**拒否**または**アラート**となったユーザのすべてのトランザクション（ログイン、電子送金、またはアプリケーションが評価するすべてのトランザクション）は、ケースと見なされます。

  言いかえれば、1 つのケースに複数の疑わしいユーザ トランザクションが含まれる場合があります。

- すべてのケースは、ユーザ、トランザクション詳細、およびケース履歴に関連する情報を提供します。

  ユーザと開かれたケースは、厳密に 1 対 1 で対応します。 そのため、ユーザに対してケースがすでに開かれている場合、疑わしい新規トランザクションは既存のケースに追加されます。 ユーザにすでに開かれているケースがある場合、新しいケースは作成されません。

- いかなる時にも、1 人のユーザはシステム内に開かれたケースを 1 つだけ持つことができます。

- 管理コンソールからケースを表示する場合、管理者によって処理されておらず、したがって不正行為ステータスがまだ決定されていないケース内のすべてのトランザクションが常に表示されます。

- システム内でケースが作成されると、そのケースのすべてのトランザクションが処理（［Fraud］または［Not A Fraud］としてマーク付け）されない限り、閉じることはできません。

  テクニカル サポート担当者（CSR）がこれらのトランザクションをすべて処理した場合は、そのケースを明示的に閉じる必要があります。 その時初めてそのケースは閉じられたと見なされます。

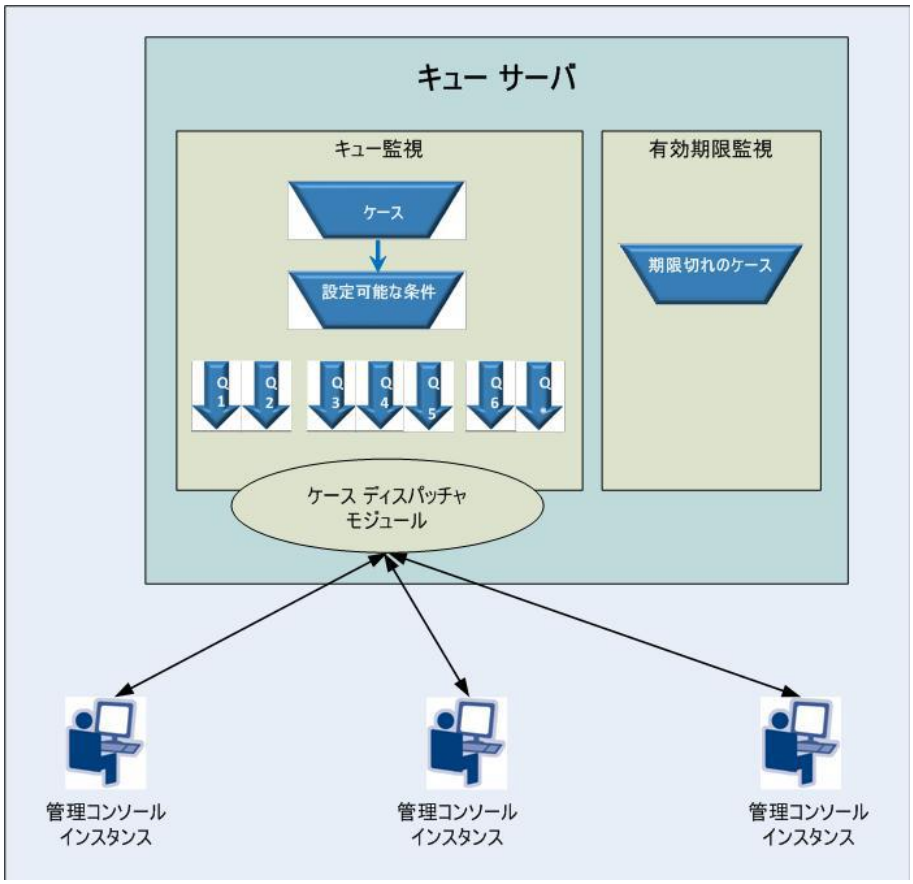
- ケースが閉じられた場合、指定されたユーザに新しい警告または疑わしいトランザクションが表示されると、システムに新しいケースが作成されます。 新規およびそれ以降のトランザクションはすべてこの新しいケースに割り当てられます。

ケース管理のコンポーネント

ケース管理モジュールのコンポーネントには次のものが含まれます。

- ケース キュー (P. 345)
- キュー サーバ (P. 346)
- キュー監視スレッド (P. 347)
- ケース ディスパッチャ モジュール (P. 349)
- 有効期限監視スレッド (P. 350)

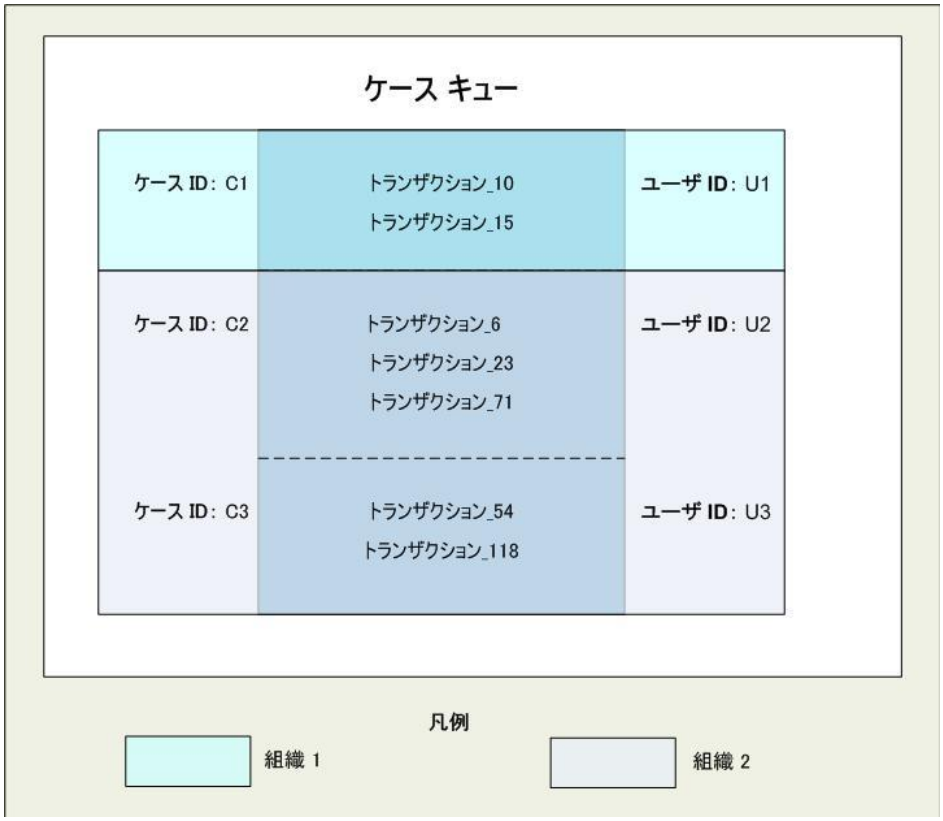
以下の図は、これらのコンポーネントがどのように連携するかを示します。



ケース キュー

ケース キュー（または単にキュー）は、**作成日時**、**更新日時**、**開かれているトランザクション数**、および**次のアクション日時**のような条件に基づいてグループ化されるケースのリストです。CA Advanced Authentication は、システムの各組織につき複数のキューをサポートします。

以下の図に、標準的なキューの例を示します。



キューはキュー マネージャ (P. 354)によって管理され、キュー名、キュー内のケース順序基準、およびケースの優先度に関連付けられています。 キュー マネージャは新しいキューを定義できます。 キューが再構築されると、生成された新しいケースはキューに追加されます。 デフォルトでは、キューの再構築は 30 分ごとに行われます。 GA は、［その他の設定］画面でこの頻度を設定できます。 組織のキュー マネージャは、管理コンソールからキュー再構築リクエストを発行することもできます。 どの個別のキューにも適合しないキューは、デフォルト キューに割り当てられます。

キュー マネージャは、テクニカル サポート担当者（CSR）のスキルまたはその他の組織ポリシーに応じて CSR を割り当てて各キューを処理することができます。

注: 1 つの組織の 1 つのキューを複数の CSR に割り当てることができます。また、CSR の権限の範囲内に複数の組織がある場合は、CSR を複数のキューに割り当てることができます。

キュー サーバ

キュー サーバは以下の処理に関与します。

- キュー監視スレッド (P. 347) を使用してケース キュー (P. 345) およびキューと管理者のマッピングをキャッシュする。
- ケース ディスパッチャ モジュール (P. 349) を使用して、ケース キュー (P. 345) 内のケースをアクティブな管理コンソール インスタンスに送信する。
- 有効期限監視スレッド (P. 350) を使用して、期限切れになったケースの更新済みリストを保持する。

キュー監視スレッド

キュー監視（スケジューラと呼ばれる）スレッドは、キュー サーバ (P. 346)側で実行され、ケース スケジュールの作成に関与し、ケース キュー (P. 345)にケースを投入し、ケース ディスパッチャ モジュール (P. 349)のためのキューを準備します。

このスレッドは以下のように動作します。

1. 事前に定義された間隔で起動し、以下に示すデータベースから最新のケースすべてのリストを取得します。
   - 少なくとも 1 つのトランザクションの［不正行為ステータス］が［**不明**］と表示されている。

   および

   - ケースが期限切れになっていない。
2. キューをケースと共にキャッシュします。
3. ケースの状態およびその他の基準（**トランザクション日付**、**トランザクション金額**、**次回アクション日付**など）に基づいて、このスレッドはケースをケース キュー (P. 345)に割り当てます。
4. ケースの状態の詳細については、「ケースの状態 (P. 356)」を参照してください。
5. ケースがキューに割り当てられる際に、キュー用のメモリ内リストが作成されます。
6. キューへのケース割り当てが完了すると、すべての割り当てられたケースの状態は［オープン］に変更されます。
7. テクニカル サポート担当者 (P. 351)（CSR）が［**保存して次のケースに移動**］または［**次のケースに移動**］をクリックすると、以下のようになります。
   a. キュー内の次のケースを取得するリクエストがキュー サーバ (P. 346)を介してキュー監視スレッド (P. 347)に送信されます。
   b. これに応えて、ケース ディスパッチャ モジュール (P. 349)はメモリキューからそのケースを選択し、リクエストが発信された管理コンソール インスタンスにそのケース ID を返します。
8. その後、そのケースの状態は［進行中］に変更され、CSR はそのケースの処理を実行できます。

9. Case ID を受信するとすぐに、管理コンソール インスタンスは、データベースからそのケースのトランザクションをすべて取得し、CSR に同じものを表示します。

   ケースの確認プロセスに基づいて、ケースの状態は変更する場合があります。詳細については、「ケースの状態 (P. 356)」を参照してください。

ケース ディスパッチャ モジュールの仕組み

ケース ディスパッチャ モジュール（またはディスパッチャ）は、キュー サーバ (P. 346)側で個々の CSR からのケース リクエストをリスンし、要求に応じてケース キュー (P. 345)から個々の管理コンソール インスタンスに、（キュー内の順序に従い）ケースを「プッシュ」します。

このモジュールは以下のように動作します。

1. CSR がログインすると、ディスパッチャは次のケースを取得するリクエストを受信します。
2. ディスパッチャはこの CSR に割り当てられたキューから次のケースを取得します。
3. ディスパッチャは CA Advanced Authentication データベース内の選択されたケースに対してロックを取得します。
4. ディスパッチャは、そのケースのステータスを［オープン］から［進行中］に変更します。
5. ディスパッチャは、管理コンソール インスタンスからリクエストを送信した CSR の名前を付けて、影響を受けたテーブルを更新します。
6. ディスパッチャは、管理コンソール インスタンスにケースの詳細を送り返します。管理コンソールは、そのケースに対するトランザクションを取得し、それらを CSR の画面に表示します。
7. また管理コンソール インスタンスは、表示されたケースの詳細に対してタイムアウトも設定します。

   これにより、CSR がケース ページを開いたまま、作業せずに事前定義された時間間隔が経過するのを防ぎます。 CSR への現在のケース割り当てがタイムアウトした場合、適切なメッセージが CSR に表示されます。 そのケースはその後タイムアウトして、そのステータスは［オープン］に変更されます。
8. 現在表示されているケースがタイムアウト*せずに*、CSR がキュー内の次のケースに移動した場合、ケース ステータスは［進行中］から［オープン］に変更されます。

   CSR は、画面上の［**次のケースに移動**］ボタンをクリックして次のケースを表示できます。

有効期限監視スレッドの仕組み

有効期限監視スレッドは、スレッドが最後に実行されてから期限切れになったすべてのケースにマークを付ける処理に関与します。 これは、キュー監視スレッド (P. 347)よりもかなり少ない頻度で起動します。

このスレッドは以下のように動作します。

1. 事前定義済みの間隔では、有効期限監視は以下に示したすべてのケースのリストを取得します。

   - ［OPEN］または［NEW］ステータスのケース。

   および

   - 設定された有効期間より後に更新されたケース。

   有効期限監視は、スレッドはまだ処理されていないケース、および新しいアラートが生成されていないケースを検索します。

2. 次に、スレッドは、前の手順で［有効期限切れ］と識別された CA Advanced Authentication データベース内のすべてのケースのステータスを更新します。
3. スレッドはスリープに戻ります。

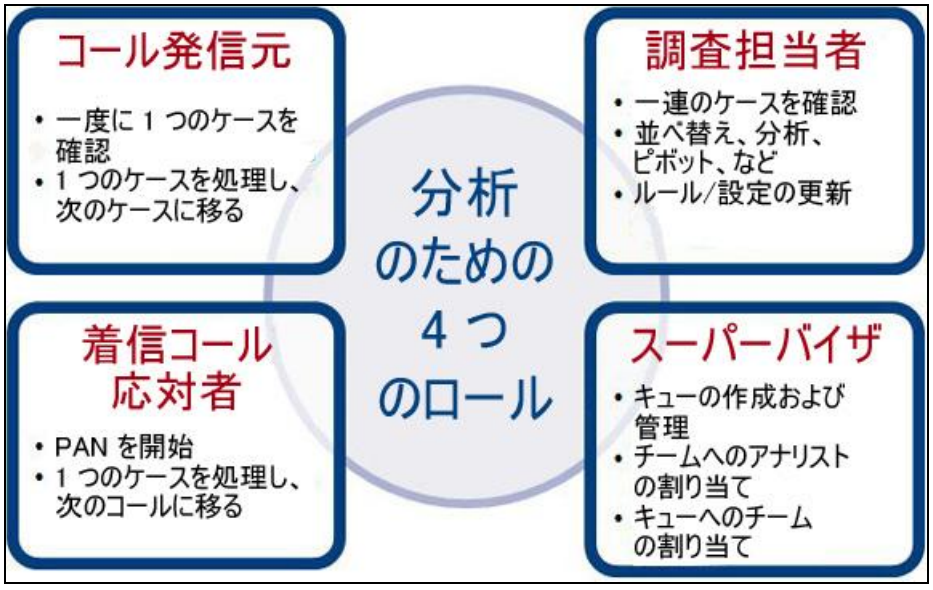
ケース ロール

ケース管理機能は以下の広範なカテゴリのロールをサポートします。

- テクニカル サポート担当者 (P. 351)
- キュー マネージャ (P. 354)
- 不正行為アナリスト (P. 355)

「ケース ロール権限サマリ (P. 356)」では、これらのロールに利用可能な権限の概要について説明します。

以下の図は、各ロールによって実行されるさまざまなケース ロールおよびタスクを示します。



テクニカル サポート担当者

名前が示すように、*テクニカル サポート担当者* (CSR) はエンド ユーザとの組織のインターフェースです。 以下の責任を担います。

- ケースのワークフロー (P. 352)
- カスタマ コール (P. 353)

ケースのワークフロー

通常、自動的に割り当てられるケースを確認して、それらのケースの処理を行います。ケースの処理を開始すると、そのケースはその CSR の名前でマークされます。その結果、そのケースは別の CSR の画面には表示されません。 ただし、キュー マネージャ (P. 354)はキューに別の CSR を割り当てることによって、ケースを別の CSR に再割り当てすることができます。

また、CSR はエンド ユーザに電話をかけて、疑わしいトランザクションの信頼性を確認します。CSR のメイン アクティビティには次のものが含まれます。

- 必要に応じて、エンド ユーザに電話をかけてトランザクションが不正かどうか確認する。
- ユーザ入力に基づいて、指定された期間ユーザを［**例外ユーザ リスト**］に追加する。

  デフォルト期間は 10 日ですが、必要に応じて変更できます。
- ケースを確認した後に、ケースを更新できる。その結果によって、ケース ステータスを［**進行中**］から以下のいずれかに変更できます。
  - 保留
  - クローズ
- また、調査の進捗状況をキャプチャするために、自由形式フィールドに適切なメモを取ることもできる。

カスタマ コール

CSR はエンド ユーザからの着信を処理することもあります つまり、彼らはカスタマ コールに対応します。 たとえば、顧客が実行しなかったトランザクションが表示されたため、コールセンターに電話をする場合があります。 そのような場合、指定されたユーザのケースがすでに存在すれば、オペレータはカスタマからの入力を記録します。 カスタマに対するケースが存在しない場合は、ケースは自動的に生成されます。

注: CSR によって収集された入力データは、不正行為アナリストによって分析に使用されます。

この場合、CSR は以下の処理を行います。

- ユーザ コールを処理する。
- ユーザからの情報を記録する。

  また、調査の進捗状況をキャプチャするために、自由形式フィールドに適切なメモを取ることができます。
- ユーザの最近のアクティビティを確認する。
- ユーザ入力に基づいて、指定された期間ユーザを［**例外ユーザ リスト**］に追加する。

  デフォルト期間は 10 日ですが、必要に応じて変更できます。
- 指定された期間のユーザによるトランザクションを検索する。

キュー マネージャ

キュー マネージャ（または単にスーパーバイザ）は、ケースがキューに割り当てられる順序を決定します。 次のことができます。

- 新しいキューを作成し、組織の複数のキューの 1 つにケースを割り当てる。

  キューを作成する方法の詳細については、「キューの新規作成 (P. 364)」を参照してください。

- スコープ内のすべての組織のキューを管理する。

  キューの詳細については、「ケース キュー (P. 345)」を参照してください。

- キューを再構築する。

  詳細については、「キューの再構築 (P. 373)」を参照してください。

- スコープ内のキューへの CSR の割り当て、および再割り当てを行います。

注: デフォルトでは、キュー マネージャは、不正行為アナリストのタスクを実行 *できません*。ただし、**カスタム ロール**を使用してキュー マネージャに基づいた新規ロールを作成し、このロールに FA 権限を割り当てることができます。

不正行為アナリスト

FA （*不正行為アナリスト*）は、トランザクションでの不正行為パターンを調査して分析し、不正行為対策の戦略を定義します。 また、ほかの CSR *および*利用可能なフィルタによって収集された以下に示すような真のデータを使用することにより、トランザクションの傾向を分析します。

- 指定された期間内の同じユーザによるトランザクション。
- 指定された期間内の同じユーザのデバイスからのトランザクション。
- 指定された期間内の同じ IP アドレスからのトランザクション。

これらの分析に基づいて、FA は CA Advanced Authentication の微調整についてシステム管理者に助言できます。 さらに、不審なトランザクションの疑いがある場合は、それまでシステムがそのトランザクションを疑ったことがない場合でも、エンド ユーザに電話してその疑わしいトランザクションに関連する詳細情報を見つけるように CSR にリクエストを要求することができます。

以下のリストでは、不正行為アナリストによって実行される主な機能について説明します。

- トランザクションのリストにログインして、リアル タイムで表示することができます。
- フィルタ条件の組み合わせを設定し、一定期間内に特定のリスク ステータスの値に一致するすべてのユーザのトランザクションを表示することができます。
- 調査の一部として、FA は、同様のトランザクションも検索できます。以下の条件に基づいて類似性を検出するようにフィルタを定義することができます。
  - 指定された期間内の同じユーザによるトランザクション。
  - 指定された期間内の同じユーザのデバイスからのトランザクション。
  - 指定された期間内の同じ IP アドレスからのトランザクション。
- トランザクションのセットが大きい場合は、データをオフラインでエクスポートし、それを分析することもできます。
- 疑わしいパターンが検索された場合は、CSR による詳細な調査が行われるように、それらのトランザクションに対してアラートを生成することができます。 「アラートが生成された」トランザクションは、問題になっているユーザのケースに自動的に追加されます。

注: 不正行為アナリストはケースを更新 できません。

ケース ロール権限サマリ

以下の表に、前のセクションで説明したケース ロールに使用可能な権限を要約します。

権限	CSR	キュー マネージャ	不正行為アナリスト
着信コールの管理	✓	X	X
ケースでの作業	✓	X	X
キューの管理	X	✓	X
キューの再構築	X	✓	X
キュー ステータスの表示	X	✓	X
トランザクションの分析	X	X	✓

ケースの状態

ケースはそのライフサイクルで、多くの状態を経て進行することができます。

このセクションは、以下のトピックから構成されます。

- New (P. 357)
- オープン (P. 341)
- 進行中 (P. 357)
- 保留 (P. 358)
- 有効期限切れ (P. 358)
- クローズ (P. 359)

New

ユーザのトランザクションが**アラート**または**拒否**アドバイスの結果となった場合、対応するケースがまだ存在しなければ、ユーザに対して新しいケースが作成されます。

CSR がそのケースを開くか、またはケースが期限切れになるまで、ケースは［**新規**］状態で残ります。

オープン

CSR がそれらに割り当てられた新しいケースを開くと、そのケースはアクティブになり、その状態は［**オープン**］に変わります。 ケースが［**オープン**］状態である場合は、新しいトランザクションまたはイベントをそのケースに追加できます。

ケースの状態が［**保留**］または［**クローズ**］のいずれかでない限り、すべてのケースは［**オープン**］状態で残ります。

進行中

CSR がケースで作業している間、ケースの状態は［**進行中**］のままです。すなわち、現在のケースで［**キャンセル**］をクリックするか、［**次のケースに移動**］をクリックしてそれらに割り当てられた次のケースに移動すると、現在開いているケースの状態は［**オープン**］に変わるか、または明示的にそのケースを変更した状態に変わります。

注: CSR とキュー マネージャは、ケースのステータスを［**保留**］から［**進行中**］に変更できます。

保留

CSR が［**進行中**］ケースに［**次回アクション日付**］を指定することにより、ケースの詳細調査を延期した場合は、ケースの状態は［**保留**］に変わります。

注:［**次回アクション日付**］の時間枠内に生成されたすべてのイベントはケースに追加されます。

指定された［**次回アクション日付**］に達すると、ケースの状態は自動的に［**オープン**］に変わります。

有効期限切れ

CSR が事前定義された日数内に［**新規**］ケースで作業しなかった場合、ケース状態は［**有効期限切れ**］に変わります。

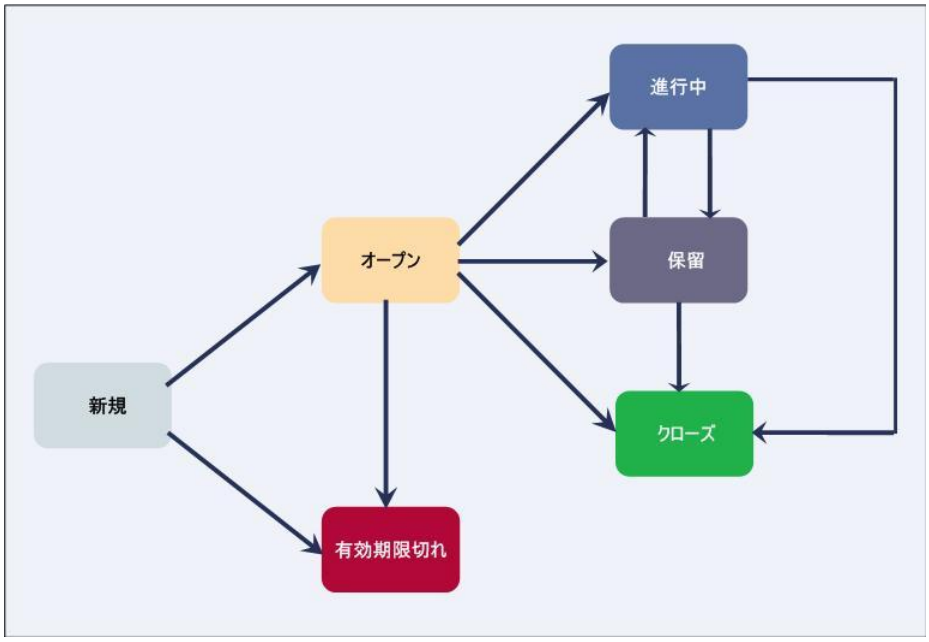
注: 最後のトランザクションがそのケースに追加された時間、または更新された時間がそのケースの*開始日*と見なされます。 ケースの有効期限は、開始日 + *N* 日として計算されます。ここで、*N* は設定可能な値です。 *N* のデフォルト値は **10** 日です。

新しいトランザクションは期限切れのケースに追加できません。 新しいケース（およびそのための新しいケース ID）が作成されて、新しいトランザクションまたはイベントはこの新しいケースに追加されます。

クローズ

CSR が**オープン**のケースを解決し、それに［**クローズ**］として明示的にマークを付けると、ケースの状態は［**クローズ**］に変わります。

以下の図は、ケースの状態がどのように変わるかを示しています。



ケース管理ワークフロー

このセクションは、以下のトピックから構成されます。

- ケースの生成 (P. 360)
- ケースのキュー
- ケースの割り当て (P. 361)
- ケースの処理 (P. 362)
- ケースの期限切れ (P. 363)
- 不正行為の分析 (P. 363)

ケースの生成

通常、ケースはシステムによって自動的に作成されます。 ただし、ケース オペレータがユーザの不審なトランザクションに対して手動でフラグを付けた場合、または不正行為アナリストがユーザのトランザクションで不審なパターンを検出した場合は、ケースに不審なトランザクションを追加できます。

ケースは以下の場合に生成されます。

- トランザクションのリスク評価に対するアドバイスが**アラート**または**拒否**のいずれかの場合。

  注: ユーザに対してすでにケースが開かれている場合、このトランザクションは既存のケースに追加されます。これは[その他の設定]ページで設定できます。

- あるトランザクションについてユーザからコールセンターに訴えがあった場合。

  この場合オペレータは、訴えのあったトランザクションをより詳細な調査に回すか、不正トランザクションとしてマークすることができます。 どちらの場合も、トランザクションは自動的に事例に追加されます。

- 不正行為アナリストは、いくつかのトランザクションを（通常、過去に検出されたパターンに基づいて）不正であると疑い、詳細な調査のためにそれらをマークします。

  注: その後、これらのトランザクションは既存のケースに追加されます。

ケースのキュー

ケースが作成され、トランザクションがそのケースに追加されると、組織が所有しているキューにそのケースを割り当てる必要があります。 さらに、これらのケースに取り組むことができる CSR も各キューに割り当てる必要があります。 キュー監視スレッド (P. 347)はこの場合、極めて重要な役割を担います。

このスレッドがケースをキューに登録する方法の詳細については、「キュー監視スレッド (P. 347)」を参照してください。

ケースの割り当て

ケースがキューに登録された後で、それを各 CSR の画面にディスパッチする必要があります。ケース ディスパッチャ モジュール (P. 349)はこの場合、極めて重要な役割を担います。

このスレッドがケースをディスパッチする方法の詳細については、「ケース ディスパッチャ モジュール (P. 349)」を参照してください。

ケースの割り当てに関する注意事項

このトピックで注意するべき点を以下に示します。

- 新しいケースはそのケースが属する組織から CSR に割り当てられます。
- ケースはケース キューの順序に基づいて割り当てられます。順序の基準には次のものを含めることができます。
  - 次の連絡/アクション日
  - ケースで開いているトランザクションの数
  - ケースの経過日数（作成された日付）
  - ケースが最後に更新された日時
- すべてのケースは、組織内の CSR によって最終的に処理されます。

ケースの処理

ケースは、CSR によって以下のように処理されます。

- 新しいトランザクションに FA によってフラグが付けられたり、トランザクションに［拒否］または［認証強化］アドバイスが生成されると、新しいケースが作成されます。キュー監視スレッド (P. 347)のスケジュールの*前*では、ケースのステータスは［**新規**］と予定されます。キュー監視スレッド (P. 347)はそのステータスを［**オープン**］に変更し、CSR がそのケースを表示したときに、ケースのステータスは［**進行中**］に変更されます。

  注: ケースが CSR によって処理される前に、フラグ付きのトランザクションがさらにそのケースに追加される場合があります。

- CSR には、作業するケースが自動的に割り当てられます。
- 電子メールを送信したり、指定された連絡先番号に電話をすることにより、オフラインのユーザに連絡します。
- 進行中の調査およびエンド ユーザとの連絡の結果に基づいて、CSR はケースを以下のように展開して更新することができます。
  - 特定の時間間隔に基づいてトランザクションを検索する。
  - ユーザとのやり取りの間で、以前疑われていなかったトランザクションをケースに追加する。
  - ケース内の 1 つ以上のトランザクションに対する解決策を選択する。
  - ケースに追跡のためのマークを付けて［**次回アクション日付**］を設定する。

    通常、そのような**ケースのステータス**は［**進行中**］または［**保留**］のいずれかに更新されます。また、ユーザには後で CSR から連絡があります。
  - ユーザの入力データに基づいて、ユーザを指定された期間［**例外ユーザ リスト**］に追加する。
  - ケースを解決し、［**ケース ステータス**］を［**クローズ**］に変更する。
- 必要に応じて、キュー マネージャ (P. 354)は期限切れのケースを再開できます。

ケースの期限切れ

トランザクションのすべてが規定された時間内に処理されない場合、または事前定義された期間のケースでアクティビティがない場合、ケースは期限切れになります。

注: デフォルトのケース有効期限は 48 時間です。

このスレッドが期限切れのケースを管理する方法の詳細については、「有効期限監視スレッド (P. 350)」を参照してください。

不正行為の分析

不正行為アナリスト (P. 355)によるトランザクションの不正行為分析ワークフローの要点を以下に示します。

- FA は、トランザクション日、2 次認証ステータス、トランザクションのタイプ、リスク アドバイス、およびケース ステータスなどの基準に基づいてトランザクションを検索できます。
  - すべてのトランザクションは最初に［トランザクション サマリ］ビューに表示されます。
  - すべてのトランザクションの最初のケース ステータスは［**新規**］です。
  - トランザクションのリストは、.csv ファイルにエクスポートして Microsoft Excel で処理することができます。
- FA は、ケースをクリックしてその詳細を表示することができます
- FA は、ケースに類似しているすべてのトランザクションを検索できます
- 分析中に疑わしいトランザクションおよび潜在的な不正行為のパターンが検索された場合、FA は CSR によって詳細な調査が行われるようにトランザクションをマークできます

キューの新規作成

重要: GA、OA、または QM （キュー マネージャ）のみがこのセクションのタスク（スコープ内にある組織で）を実行できます。 MA、UA、FA、および CSR はこれらのタスクを実行できません。

キュー マネージャは、キューの名前、説明、基準、および優先度を指定して新しいキューを作成できます。 また、キュー マネージャはキューに管理者を割り当てます。 管理者を複数のキューに割り当てることができます。また、複数の管理者を同じキューに割り当てることもできます。

新しいキューを作成する方法

1. GA、OA、または QM として管理コンソールにログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キューを管理**］リンクをクリックして［キューを管理］ページを表示します。
4. ［**組織の選択**］リストから、キューを作成する組織を指定します。
5. 更新されたページが表示されます。
6. ［**キューの新規作成**］をクリックします。

   更新されたページが表示されます。
7. ［**キュー名**］を指定します。
8. キューの［**表示名**］を指定します。
9. 必要に応じて、［**キューの説明**］を指定します。
10. ［**管理者の割り当て**］セクションで、以下の操作を実行します。
    a. ［**管理者**］リストから、キューに割り当てる必要な管理者を選択します。
    b. ［**選択された管理者**］リストに選択された管理者を移動するには、［**>**］ボタンをクリックします。

    注: ［**選択された管理者**］リストにすべての**管理者**を移動させる場合は、［**>>**］ボタンをクリックします。
11. ［**条件**］セクションで、以下の操作を実行します。
    a. キューに追加されるケースを決定するために基準（［**リスク アドバイス**］または［**一致するルール**］）を定義します。
    b. 対応するドロップダウン リストから演算子と値を選択します。

c. ［**追加**］をクリックして、式を式領域に追加します。

d. AND、OR、(、または) 演算子を使用してフラグメントを組み合わせ、最終の条件式を作成します。

この式に一致するケースは作成するキューに割り当てられます。

12. ［**並べ替え基準**］セクションで、以下の操作を実行します。

a. キューの並べ替えに使用する要素を指定します。 使用可能なオプションは、以下のとおりです。

- 次の連絡日付
- 作成日
- 更新日
- オープン トランザクション数
- リスク アドバイス
- リスク スコア

b. 対応する要素を並べ替える順序を指定します。 使用可能なオプションは、以下のとおりです。

- 昇順
- 降順

13. ［**保存**］をクリックして画面で行った更新を保存し、キューを作成します。

14. 変更を有効にするために、組織キャッシュをリフレッシュします。

ケース キュー管理

重要: OA、GA、または QM （キュー マネージャ）のみがこのセクションのタスク（スコープ内にある組織で）を実行できます。 MA、UA、FA、および CSR はこれらのタスクを実行 *できません*。

このセクションは、以下のトピックから構成されます。

キューのステータスの表示

［キュー ステータス］ページで、**デフォルト** キューに関連する最新の統計を表示できます。 表示できる統計は以下のとおりです。

- オープン ケース総数
- 合計記録済みケース数
- 進行中ケース数
- ケース総数
- 割り当て済み管理者数

また、［**過去 8 時間で取り扱われたケース**］の詳細も表示します。

キュー ステータスを表示する方法

1. キューを管理するために必要な権限で管理コンソールにログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キュー ステータスの表示**］リンクをクリックして［キュー ステータス］ページを表示します。
4. ［**組織の選択**］リストから、キュー ステータスを表示する組織を選択します。

   更新されたキューの詳細を示すページが表示されます。

注: ［**記録済みケース数（キュー外）**］は、［**受信ケース（進行中）**］と共に個別に表示されます。

キューのステータスの更新

以下のいずれかの方法を使用することにより、キューのステータスを更新できます。

- ［**キュー ステータスの表示**］リンクをクリックして対応するページを表示し、次に更新するキューに対応する［**キュー名**］列のリンクをクリックする。
- ［**キュー管理**］セクションの［**キューを管理**］リンクを使用する。

後のオプションを使用してキューのステータスを更新する方法

1. キューを管理するために必要な権限で管理コンソールにログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キューを管理**］リンクをクリックして［キューを管理］ページを表示します。
4. ［**組織の選択**］リストから、キュー ステータスを更新する組織を選択します。
5. ［**キュー名**］リストから、管理するキューの名前を選択します。

   更新されたページが表示されます。
6. 必要に応じて、［**キューの説明**］を指定します。
7. ［**管理者の割り当て**］セクションで、以下の操作を実行します。
   a. ［**管理者**］リストから、キューに割り当てる必要な管理者を選択します。

      注: 複数の管理者を選択するには、Shift キーを押しながら必要な管理者をクリックします。
   b. ［**選択された管理者**］リストに選択された管理者を移動するには、［**>**］ボタンをクリックします。

      注:［**選択された管理者**］リストにすべての**管理者**を移動させる場合は、［**>>**］ボタンをクリックします。
8. （デフォルト キュー以外のキューを選択した場合）［**条件**］セクションで、以下の操作を実行します。
   a. キューに追加されるケースを決定するために基準（［**リスク アドバイス**］または［**一致するルール**］）を定義します。

b. 基準を定義するために、対応するドロップダウン リストからデータ項目、演算子、および値を選択します。

9. ［**並べ替え基準**］セクションで、以下の操作を実行します。

a. キューの並べ替えに使用する要素を指定します。 使用可能なオプションは、以下のとおりです。

- 次の連絡日付
- 作成日
- 更新日
- オープン トランザクション数
- リスク アドバイス
- リスク スコア

b. 対応する要素を並べ替える順序（**昇順**または**降順**）を指定します。

10. ［**保存**］をクリックして画面で行った更新を保存します。

11. 変更を有効にするために、組織キャッシュをリフレッシュします。

キューの無効化

注: キューを無効にするには、無効にするための適切な権限とスコープを持っている必要があります。 GA、OA、および QM のみがキューを無効にすることができます。

キューを無効にする方法

1. GA、OA、または QM としてログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キューを管理**］リンクをクリックして［キューを管理］ページを表示します。
4. ［**組織の選択**］リストから、キュー ステータスを更新する組織を選択します。
5. ［**キュー名**］リストから、無効にするキューの名前を選択します。

   更新されたページが表示されます。
6. ［**このキューの無効化**］をクリックしてキューを無効にします。
7. 変更を有効にするために、組織キャッシュをリフレッシュします。

重要: デフォルト キューを無効にすることはできません。

キューの有効化

注: キューを有効にするには、適切な権限およびスコープがあることを確認する必要があります。 GA、OA、および QM のみがキューを有効にすることができます。

キューを有効にする方法

1. GA、OA、または QM としてログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キューを管理**］リンクをクリックして［キューを管理］ページを表示します。
4. ［**組織の選択**］リストから、キュー ステータスを更新する組織を選択します。
5. ［**キュー名**］リストから、有効にするキューの名前を選択します。

   更新されたページが表示されます。
6. ［**このキューの有効化**］をクリックしてキューを有効にします。
7. 変更を有効にするために、組織キャッシュをリフレッシュします。

キューの削除

注: キューを削除する前に、このキューにケースが存在しなくなるようにキュー定義を編集し、キャッシュのリフレッシュとキューの再構築を行ってからこのキューを削除することを強く推奨します。 これにより、このキュー内にあったケースが失われることはありません。

1. OA または QM としてログインします。
2. ［ケース管理］タブをアクティブにします。
3. ［キュー管理］セクションで、［キューを管理］リンクをクリックして［キューを管理］ページを表示します。
4. ［組織の選択］リストから、キュー ステータスを更新する組織を選択します。
5. ［キュー名］リストから、削除するキューの名前を選択します。

   更新されたページが表示されます。
6. ［このキューの削除］をクリックしてキューを削除します。
7. 変更を有効にするために、組織キャッシュをリフレッシュします。

重要: デフォルト キューを削除することはできません。

キューの再構築

ケース管理キュー サーバは、あらかじめ設定された間隔でキューを再構築します。 デフォルト値は 1800 秒です。 GA は、［その他の設定］ページの［**自動キュー再構築スケジュールの頻度（秒単位）**］パラメータを設定して、すべての組織に対してグローバル レベルでこの値を変更できます。

以下の場合、自動再構築時間の前にキューを再構築する必要がある場合があります。

- 新しいキューが定義された場合。
- 1 つ以上のキュー定義が変更された場合。
- キューが有効化、無効化、または削除された場合。

そのような場合、キュー マネージャは［キューを再構築］ページを使用して、キューを再構築できます。

キューを再構築する方法

1. GA、OA、または QM としてログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**キュー管理**］セクションで、［**キューを再構築**］リンクをクリックして［キューを再構築］ページを表示します。
4. 以下のいずれかを実行します。
   - QM に権限の範囲内のすべての組織のキューを再構築させる場合は、［**全組織**］を選択します。

     または
   - ［**利用可能な組織**］リストから必要な組織を選択し、［**>**］ボタンをクリックしてそれらの組織を［**選択された組織**］リストに追加します。

     ［**利用可能な組織**］には、ログインしている管理者のスコープで利用可能なすべての組織が表示されます。 ［**選択された組織**］には、管理者の管理対象として選択した組織のリストが表示されます。
5. ［**再構築**］をクリックして、選択された組織のキューを再構築します。

ケースの処理

重要: OA および CSR のみが、スコープ内にある組織に属しているケースを処理できます。 MA、GA、UA および FA はこれらのタスクを実行できません。

このセクションは、以下のトピックから構成されます。

- ケースでの作業 (P. 374) (CSR)
- 顧客からの着信電話の管理 (P. 374) (CSR)

ケースでの作業 (CSR)

CA Advanced Authentication がトランザクションを疑わしいとしてマークした場合、または FA が詳細な調査を行うようにトランザクションにマークした場合は、*自動的に* CSR のケース リストに表示されます。

リストのケースで作業する方法

1. CSR としてログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**ケース管理**］セクションで、［**ケースの作業**］リンクをクリックします。

   (ケースに割り当てられた優先度の順序で) 最初のケースが表示されます。

   ページのフィールドについては、以下の表に説明されています。

フィールド	Description
User Name	電話をしてきたユーザの名前。
次の連絡日付	ユーザに次に連絡する必要のある日付。
ケース履歴	前のコール応対者によって入力された最新のケース ノートおよび追加ノート。 このフィールドの前のメモをすべて確認する場合は、［**その他**］リンクをクリックします。
このケースのアラート	

フィールド	Description
選択対象を以下のものとしてマーク	トランザクションの不正ステータス。このフィールドに指定できる値は次のとおりです。 ■ 未確定 ■ 不正行為と確認 ■ 正規と確認 ■ 不正行為と推定 ■ 正規と推定 アラートが発生し、対応が必要なトランザクションが複数あり、かつユーザと対話した後でそれらの［不正行為ステータス］がすべて同じ（［不正行為と確認］または［正規と確認］など）であると判断した場合は、このドロップダウン リストを使用して 1 回のアクションで同じ設定を行うことができます。
不正行為ステータス	上記の［選択対象を以下のものとしてマーク］フィールドのエントリに基づいて、このフィールドには以下のいずれかのステータスを指定できます。 ■ 未確定 ■ 不正行為と確認 ■ 正規と確認 ■ 不正行為と推定 ■ 正規と推定
国	IP アドレスを基に判別した、トランザクションが実行された国。
IP アドレス	ユーザのトランザクションに使用したシステムまたはデバイスの IP アドレス。
販売者	トランザクションに関与する業者。
通貨	トランザクションで使用される通貨。
金額	トランザクションの合計金額。
一致するルール	一致し、CA Advanced Authentication がトランザクションにリスクがあるとしてフラグを付けたルール。
トランザクション日付	指定されたトランザクションが実行されたタイム スタンプ。

フィールド	Description
リスク アドバイス	指定されたトランザクションのリスク スコアを評価した後に CA Advanced Authentication によって提案されたアクション。 使用可能なアクションは、以下のとおりです。 ■ ALLOW ■ ALERT ■ DENY ■ 認証の強化
モデル スコア	トランザクションに対してモデルによって返されたリスク スコア。
セカンダリ認証ステータス	リスク アドバイスが認証の強化である場合、この列ではアプリケーションがフィードバックとして CA Advanced Authentication に返した追加の認証の結果を指定します。
トランザクション ステータス	トランザクションのステータス。
デバイス タイプ	トランザクションに関与するデバイスのタイプ。
トランザクション ID	ユーザ トランザクションに対する一意のシステム生成識別子。 **注**: 必要な場合は、［トランザクション ID］をクリックすると、詳細を表示できます。
OS	トランザクションを実行するために使用されたデバイス上のオペレーティング システム。
ブラウザ	トランザクションを実行するために使用されたブラウザ。
デバイス ID ステータス	デバイス ID のステータス。 ■ **読み取り**： デバイス ID がデバイスから読み取られました。 ■ **新規**： デバイス ID がデバイスに割り当てられました。 ■ **逆方向ルックアップ**： デバイス ID が、入力デバイス シグネチャをユーザに正常に関連付けられたデバイス シグネチャと照合することにより特定されました。

フィールド	Description
アクション	ユーザによって実行されたトランザクションのタイプ。以下の値にすることができます。 ■ ログイン ■ 電子送金 ■ アプリケーション経由で指定したその他の任意の値
チャネル	トランザクションが実行されたチャネル。
開始 終了	データをフィルタする事前定義された日付範囲。
トランザクションを表示	上記の［開始］および［終了］フィールドに基づいてアラートされたトランザクションを表示するボタン。
トランザクションを非表示	表示されているアラートが発生したトランザクションを非表示にするリンク。
ケース ステータス	ケースの現在のステータス。 以下の値を指定できます。 ■ 進行中 ■ 保留 ■ クローズ
キュー	このケースが割り当てられたキュー。
注	事前に特定された更新の理由。
追加ノート	ケース ステータスまたはフィールドのいずれかが変更された理由を説明する（上記の［ノート］に追加する）任意の追加情報。 **重要**: このフィールドには 250 文字以上入力することは できません。
次のアクション日付（GMT）	追加のフォローアップのため、次にユーザに連絡する必要がある日付。

フィールド	Description
例外リストへのユーザの追加	ユーザ入力に基づいて、指定された期間のリスク評価からユーザを一時的に除外することができます。 たとえば、ユーザが拒否国の 1 つに旅行している場合に、その国からのユーザのトランザクションを拒否したくないとします。この場合は、ユーザを例外ユーザ リストに追加できます。 ユーザが例外ユーザ リストに見つかれば、デフォルトでは、CA Advanced Authentication はこれらのユーザから発信されるトランザクションに低いスコアおよび ALLOW アドバイスを返します。
開始 終了	ユーザを CA Advanced Authentication リスク評価から免除されるようにする日付範囲。
理由	ユーザが例外ユーザ リストに追加されている理由。

1. 前の手順の表で説明されているフィールドを使用して、ユーザ入力をキャプチャするために必要なアクションを実行します。
2. 完了したら、ページ上で以下のいずれかのボタンをクリックします。
   - ［**保存**］をクリックして、ケースへの変更を更新します。
   - ［**保存して次のケースに移動**］をクリックして、ケースへの変更を更新して割り当てられた次のケースに移動します。
   - ［**次のケースに移動**］をクリックして、変更を保存せずに割り当てられた次のケースに移動します。
   - ［**キャンセル**］をクリックして、ページで加えたすべての変更をキャンセルします。

顧客からの着信電話の管理（CSR）

エンドユーザがトランザクションについて訴えるためにテクニカル サポート センターに電話した場合に、応対した CSR は、［着信コールの管理］ページを使用してユーザによって提供される情報をキャプチャし、この情報に基づいてケースに必要な変更を加える必要があります。

着信電話の管理ページを使用してケースに必要な変更を加える方法

1. CSR としてログインします。
2. ［**ケース管理**］タブをアクティブにします。
3. ［**ケース管理**］の下で、［**着信コールの管理**］リンクをクリックして、着信電話の管理ページを表示します。
4. ［**組織の選択**］リストから、必要な組織を選択します。

   更新された［着信コールの管理］ページが表示されます。
5. **ユーザ ID を入力**し、［**提出**］をクリックします。

   組織のアカウントを設定している場合、ユーザ識別子を入力するように促されます。 ドロップダウン リストのユーザ名またはアカウント タイプに基づいてフィルタできます。

   ［着信コールの管理］ページが指定されたユーザのケース情報でリフレッシュされます。

   ページのフィールドについては、「ケースのワークフロー (P. 352)」（CSR）の表で説明されています。
6. 「ケースのワークフロー（P. 352）」（CSR）の表で説明されているフィールドを使用して、ユーザ入力をキャプチャするために必要なアクションを実行します。
7. 完了したら、［**保存**］をクリックしてケースへの変更を更新します。

   加えた変更を保存しない場合は、［**キャンセル**］をクリックします。

ケース管理レポートの生成

ケース管理モジュールは、以下の表で説明されているレポートをサポートします。

Report	Description	レポートを生成できるケース ロール
ケース アクティビティ レポート (P. 381)	指定された期間にオープン、クローズ、または処理された（ケースに対して実行されたその他のアクティビティに対して）すべてのケースの累積数を表示します。 **注**: このレポートは、個々のケースが属するキュー、およびケースに対応した CSR で並べ替えられます。	■ グローバル管理者 ■ 組織管理者 ■ キュー マネージャ
平均ケース期間レポート (P. 382)	平均的なケースがシステム内に存在する期間に関する統計を表示します。 言いかえれば、ケース担当者が一般的なケースに対してどの程度のアクティビティを実行したかをまとめて表示します。 このレポートは、タイムアウトになったため自動的にクローズされたケースの数も表示します。	■ グローバル管理者 ■ 組織管理者 ■ キュー マネージャ

以下のサブセクションでは、これらのレポートのフィールドについて説明し、これらのレポートを生成する手順を示します。

- ケース アクティビティ レポート（P. 381）
- 平均ケース期間レポート（P. 382）
- ケース管理レポートの生成（P. 383）

ケース アクティビティ レポート

ケース アクティビティ レポートは、以下の表に説明されているように、システム内のケースに対するアクティビティ全体に関する情報を表示します。

フィールド	Description
ケース処理キュー	ケースが属するキューを指定します。 通常、これらのケースはケースのワークフロー (P. 352)を行うテクニカル サポート担当者 (P. 351)によって処理されます。
	［**着信コール数**］行内のエントリには、カスタマ コールの処理 (P. 353)を行うテクニカル サポート担当者 (P. 351)によって処理されたケースのアクティビティ詳細がまとめられています。
期間	レポートが生成された期間を示します。 このレポートは以下の期間について生成できます。 ■ 月単位 ■ 過去 7 日間 ■ 昨日 ■ 日付範囲別 **注**: ボタンをクリックすると、指定した期間の日々のアクティビティ詳細を参照できます。
オープンされたケース	指定された期間内にオープンされた新しいケースの総数を示します。
クローズされたケース	指定された期間内にクローズされた既存のケースの総数を示します。
ケース アクティビティ数	指定された期間内にケースに対して実行されたアクティビティの総数を示します。

平均ケース期間レポート

平均ケース期間レポートは、以下の表で説明されているように、システム内でケースをクローズするためにかかる平均時間に関する情報を表示します。 これらのケースは、（ケース担当者によって）手動でクローズされたか、時間経過のため自動的にクローズされたかに基づいてグループ化されます。

フィールド	Description
ケース処理キュー	ケースが属するキューを指定します。 通常、これらのケースは以下によってクローズされます。 ■ テクニカル サポート担当者 (P. 351) または ■ タイムアウトになったので、自動的に
	［**着信コール数**］行内のエントリには、カスタマ コールの処理 (P. 353) を行うテクニカル サポート担当者 (P. 351)によって処理されたケースのアクティビティ詳細がまとめられています。
期間	レポートが生成された期間を示します。 このレポートは以下の期間について生成できます。 ■ 月単位 ■ 過去 7 日間 ■ 日付範囲別
クローズされたケース	指定された期間内にクローズされた既存のケースの総数を示します。
ケース アクティビティ数	指定された期間内にケースに対して実行されたアクティビティの総数を示します。
ケースのクローズに必要な平均時間	システムでケースをクローズするためにかかった平均時間を示します。

ケース管理レポートの生成

重要: GA、OA、および FA （不正行為アナリスト）のみが、スコープ内にある組織でこのレポートを生成できます。 MA、UA、および CSR はこのレポートを生成 *できません*。

ケース管理レポートを生成する方法

1. 適切な認証情報でログインしていることを確認します。 対応するレポートを生成できるケース ロールの概要については、「ケース管理レポートの生成 (P. 380)」の表を参照してください。
2. メイン メニューで［**ケース管理**］タブをアクティブにします。
3. ［**ケース管理**］セクションで、必要なリンクをクリックします。
   - **ケース アクティビティ レポート**
   - **平均ケース期間レポート**
4. ［**組織名**］リストからこのレポートを生成する必要な組織を選択します。
5. レポートによっては、レポートを表示するために必要に応じてさらに以下の基準を指定する必要がある場合があります。
   - ドロップダウン リストから［**日付範囲**］

     または
   - ［**開始**］および［**終了**］フィールドで事前定義済み日付範囲
6. ［**レポートの表示**］をクリックして生成されたレポートを表示します。

   必要なレポートが表示されます。
7. ［**エクスポート**］をクリックしてレポートをファイルに保存するか、または［**新規レポート**］をクリックして別の基準を指定することにより新規レポートを生成します。

第 16 章: レポートの管理

レポートは、エンドユーザを管理し、高リスク イベントを調べるために必要なビジネス インテリジェンスを提供します。CA Risk Authentication のケース管理を使用する場合、レポートは不正行為エージェントおよびケース アクティビティの管理を支援します。 「管理者が使用可能なレポートのサマリ」では、さまざまな管理者が使用可能なすべてのレポートの一目でわかるサマリを表形式でリストしています。 「管理者が使用可能なレポートのサマリ」内の表の後のセクションでは、これらのレポートについて説明します。

- 管理者レポート (P. 389)
- CA Risk Authentication レポート (P. 396)
- ケース管理レポート (P. 420)

管理コンソールを通じて提供されるレポートは、指定したパラメータ（フィルタ）に基づいて生成されます。 つまり、レポートの実行時に指定する値によって、レポートの出力を制御できます。 データをフィルタするために、以下のフィルタが使用できます。

- 日付範囲
- ［Administrator Name］
- 組織
- User Name

「レポートの生成」では、管理者のためのアクティビティ レポートおよび CA Risk Authentication 固有のレポートを生成するための一般的なプロセスについて説明します。

作成済みレポートをすべてローカル ファイルにエクスポートすることもできます。 詳細については、「レポートのエクスポート」を参照してください。

管理者が使用可能なレポートのサマリ

以下の表に、すべての管理者がシステムで使用可能なすべてのカテゴリのレポート（管理者レポート、RiskMinder レポート、およびケース管理レポート）の概要を示します。 これらのレポートについては、以降のセクションで詳しく説明します。

管理者	レポートのカテゴリ		
	管理者レポート	RiskMinder レポート	ケース管理レポート
MA	マイ アクティビティ レポート	インスタンス管理レポート	
	管理者アクティビティ レポート		
	組織レポート		
グローバル管理者	マイ アクティビティ レポート	トランザクションの分析レポート	ケース アクティビティ レポート
	管理者アクティビティ レポート	リスク評価詳細アクティビティ レポート	平均ケース期間レポート
	ユーザ アクティビティ レポート	リスク アドバイス サマリ レポート	
	ユーザ作成レポート	不正行為統計レポート	
	組織レポート	ルール有効性レポート	
		誤検知レポート	
		デバイス サマリ レポート	
		例外ユーザ レポート	
		ルール設定レポート	
		ルール データ レポート	

管理者	レポートのカテゴリ		
	管理者レポート	RiskMinder レポート	ケース管理レポート
組織管理者	マイ アクティビティ レポート	トランザクションの分析レポート	ケース アクティビティ レポート
	管理者アクティビティ レポート	リスク評価詳細アクティビティ レポート	平均ケース期間レポート
	ユーザ アクティビティ レポート	リスク アドバイス サマリ レポート	
	ユーザ作成レポート	不正行為統計レポート	
	組織レポート	ルール有効性レポート	
		誤検知レポート	
		デバイス サマリ レポート	
		例外ユーザ レポート	
		ルール設定レポート	
		ルール データ レポート	
ユーザ管理者	マイ アクティビティ レポート	トランザクションの分析レポート	

<table>
<tr><td rowspan="9">管理者</td><td colspan="3">レポートのカテゴリ</td></tr>
<tr><td>管理者レポート</td><td>RiskMinder レポート</td><td>ケース管理レポート</td></tr>
<tr><td>管理者アクティビティ レポート</td><td>リスク評価詳細アクティビティ レポート</td><td rowspan="6"></td></tr>
<tr><td>ユーザ アクティビティ レポート</td><td>リスク アドバイス サマリ レポート</td></tr>
<tr><td rowspan="4">ユーザ作成レポート</td><td>不正行為統計レポート</td></tr>
<tr><td>ルール有効性レポート</td></tr>
<tr><td>誤検知レポート</td></tr>
<tr><td>例外ユーザ レポート</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="3">不正行為アナリスト</td><td rowspan="2">マイ アクティビティ レポート</td><td>不正行為統計レポート</td><td rowspan="3"></td></tr>
<tr><td rowspan="2">ルール有効性レポート</td></tr>
<tr><td rowspan="2">ユーザ作成レポート</td><td>誤検知レポート</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">テクニカル サポート担当者</td><td>マイ アクティビティ レポート</td><td rowspan="2">例外ユーザ レポート</td><td></td></tr>
<tr><td>ユーザ作成レポート</td><td></td></tr>
<tr><td colspan="4"></td></tr>
</table>

以下のセクションでは、これらのレポートについて詳しく説明します。

管理者レポート

CA Risk Authentication 用語で、*管理者*とは管理コンソールにログインできるユーザです。 管理者は、自分が実行するアクティビティおよび権限の範囲内の管理者が実行するアクティビティを監査するためにレポートを使用します。これらのレポートには、［**レポート**］メイン メニューの［**管理者レポート**］サブメニューからアクセスします。

注: 管理コンソールのレイアウトおよびこのメイン メニューとサブメニューにアクセスする方法については、「管理コンソールの要素」を参照してください。

このカテゴリの使用可能なすべての管理者レポートには、以下のものが含まれます。

- マイ アクティビティ レポート (P. 389)
- 管理者アクティビティ レポート (P. 391)
- ユーザ アクティビティ レポート (P. 392)
- ユーザ作成レポート (P. 393)
- 組織レポート (P. 394)

マイ アクティビティ レポート

このレポートは、現在の管理者によって実行されたすべての操作をリスト表示します。 定義されたデータ範囲に対して実行したアクションおよび操作をリスト表示するためにこのレポートを使用します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	イベントが実行された日時。
管理者 ID	レポートを生成している管理者の名前です。
管理者の組織	管理者として現在ログインしている組織の名前。

レポート フィールド	Description
トランザクション ID	CA Risk Authentication サーバにトランザクション（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）をサブミットするごとに作成される一意の数値識別子。 **注**: この ID を使用して、ログ ファイル内の特定のトランザクションに関する情報を特定できます。
［Event Type］	実行した管理者アクティビティのタイプ（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）。 可能なイベント タイプは以下のとおりです。 ■ ユーザの検索 ■ 組織の検索 ■ 管理者のログイン ■ AdminProfile の更新 ■ 優先ロケールの設定 ■ 組織の作成 ■ ルール セットの作成 ■ AccountType の作成 ■ AccountType 詳細の取得 ■ システムおよび組織キャッシュのリフレッシュ ■ 運用環境への移行 ■ レポートの表示： <*レポート名*> ■ トランザクション サマリのエクスポート ■ グローバル パスワード ポリシーの更新 ■ セッション期限切れ ■ キュー ステータスの表示
ステータス	トランザクションのステータス。 ■ **成功**： アクションは正常に完了しました。 ■ **失敗**： アクションは正常に終了しませんでした。
理由	トランザクションが失敗した理由。
ユーザ ID	トランザクションにユーザ属性の変更が含まれている場合、このフィールドは属性が更新または変更されたユーザの名前を指定します。

レポート フィールド	Description
ターゲット組織	アクティビティが実行された組織の名前。
［Component］	タスクを実行するために使用されたシステム リソース。列の値は以下のいずれかです。 ■ 管理コンソール ■ RiskMinder リソースパック
［Session ID］	管理コンソールにログインするごとに作成される一意の数値識別子。 ログアウトするまでこのセッションは続きます。
インスタンス ID	CA Risk Authentication サーバの複数のインスタンスが実行されている場合、このフィールドはログインしたインスタンスを一意に識別します。 **注**: このデータは問題を診断するために CA サポート担当者によって使用されます。

管理者アクティビティ レポート

このレポートは、指定された管理者、または指定された組織のすべての管理者によって実行されたすべてのアクティビティをリスト表示します。通常、グローバル管理者は、組織全体にわたってアクティビティを監視するためにこのレポートを使用します。一方、組織管理者は組織内のアクティビティを監視するためにこのレポートを使用します。

このレポートを使用すると、管理者は全体のアクティビティを表示したり、1 人の管理者にドリルダウンしたりすることができます。

このレポートは、組織管理者がその管理チームのアクティビティを管理する際に最も役立ちます。 管理者のログインおよびログアウトのタイム スタンプ、組織検索、管理者アカウントの更新、関連する詳細などの情報を表示します。

このレポートのフィールドはマイ アクティビティ レポートと同じです。フィールドの詳細については、「マイ アクティビティ レポート」の表を参照してください。

ユーザ アクティビティ レポート

CA Risk Authentication がエンタープライズ、e バンク、または e ポータル アプリケーションのリスク、または e コマースと 3D セキュア アプリケーションの場合のカード所有者のリスクを評価する場合、ユーザはエンドユーザを示す一般的な用語です。

ユーザ アクティビティ レポートは、ユーザ属性に対して実行されたアクティビティのレポート専用です。これには、ユーザの作成、ユーザの更新、PAM （Personal Assurance Message）設定、ユーザの削除、ユーザ ステータスの更新、ユーザの認証などが含まれます。

このレポートは、ユーザ名、ユーザのステータス、実行された操作のタイプ、ユーザ システムの IP アドレスなどの詳細を表示します。 そのため、ユーザが保護されているリソースへのアクセスが許可される前に管理者によって明示的に作成されるエンタープライズまたは e ポータル アプリケーションに最も適しています。通常ユーザが自動作成される e コマース アプリケーションにはそれほど適していません。 このレポートはアクティビティのタイプをレポートしますが、カード所有者からの初めてのトランザクションのレートについての情報を提供します。

このレポートを生成するには、以下の項目を指定する必要があります。

- **日付範囲**。
- （オプション）**ユーザ名**。
- 必要な**組織名**。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	イベントが実行された日時。
ユーザ ID	属性が更新または変更されたユーザの名前。
アカウント タイプ	ユーザが所属する組織と関連付けられたアカウント タイプ。
アカウント ID	ユーザのアカウント ID。
［Event Type］	実行した管理者アクティビティのタイプ（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）。
組織	ユーザが属する組織の名前です。

レポート フィールド	Description
ステータス	操作のステータスです。 ■ **成功**： 操作は正常に完了しました。 ■ **失敗**： 操作は正常に終了しませんでした。
トランザクション ID	CA Risk Authentication サーバにトランザクション（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）をサブミットするごとに作成される一意の数値識別子。 **注**: この ID を使用して、ログ ファイル内の特定のトランザクションに関する情報を特定できます。
理由	操作が失敗した理由を示します。
クライアント IP アドレス	エンド ユーザのシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって設定された一意の識別子です。 **注**: 呼び出し元のアプリケーションが値を設定しなかった場合、［コール元 ID］はブランクになることがあります。

ユーザ作成レポート

ユーザ作成レポートには、RiskMinder システムで作成されたユーザの詳細が表示されます。

このレポートを生成するには、以下の項目を指定する必要があります。

- **日付範囲**。
- （オプション）**ユーザ名**。
- 必要な**組織名**。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	説明
作成日	ユーザが作成された日時を示します。
ユーザ ID	作成されたユーザの名前です。
組織	ユーザが属する組織の名前です。

レポート フィールド	説明
ユーザ ステータス	ユーザのステータスです。以下の値になります。 ■ **アクティブ**： ユーザがアクティブなユーザである場合。 ■ **非アクティブ**： ユーザが非アクティブにされている場合。 ■ **初期**： ユーザが作成されているが、まだアクティブにされていない場合。
名	ユーザの名です。
ミドル ネーム	ユーザのミドル ネームです。
姓	ユーザの姓です。
電子メール アドレス	ユーザの電子メール アドレスです。
電話番号	ユーザの電話番号です。

組織レポート

このレポートは、指定した組織上で実行したすべての操作の詳細をリスト表示します。 このレポートには、ルールや設定に関係なく、管理者の権限の範囲内にある組織のアクティビティがすべて表示されます。

このレポートを生成するには、以下の項目を指定する必要があります。

- **日付範囲**。
- **組織名**。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	アクティビティが実行された日時。
管理者 ID	処理を実行した管理者の名前です。
管理者の組織	管理者が属する組織の名前です。
トランザクション ID	CA Risk Authentication サーバにトランザクション（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）をサブミットするごとに作成される一意の数値識別子。 **注**: この ID を使用して、ログ ファイル内の特定のトランザクションに関する情報を特定できます。

レポート フィールド	Description
［Event Type］	実行した管理者アクティビティのタイプ（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）。
ステータス	実行されたアクションのステータスです。 ■ **成功**： アクションは正常に完了しました。 ■ **失敗**： アクションは正常に終了しませんでした。
理由	操作が失敗した理由を示します。
ユーザ ID	トランザクションにユーザ属性の変更が含まれている場合、このフィールドは属性が更新または変更されたユーザの名前を指定します。
ターゲット組織	ユーザが属する組織です。
［Component］	タスクを実行するために使用されたリソースです。 列の値は以下のとおりです。 ■ Administration Console（Admin Console） ■ RiskFort （RiskFortResourcePack）
［Session ID］	管理コンソールにログインするごとに作成される一意の数値識別子。 ログアウトするまでこのセッションは続きます。
インスタンス ID	CA Risk Authentication サーバの複数のインスタンスが実行されている場合、このフィールドはログインしたインスタンスを一意に識別します。 **注**: このデータは問題を診断するために CA サポート担当者によって使用されます。

rauth> レポート

システムで使用可能な CA Risk Authentication 設定関連のすべてのレポートには、以下のレポートがあります。

- インスタンス管理レポート (P. 396)
- トランザクションの分析レポート (P. 397)
- リスク評価詳細アクティビティ レポート (P. 410)
- リスク アドバイス サマリ レポート (P. 413)
- 不正行為統計レポート (P. 414)
- ルール有効性レポート (P. 415)
- 誤検知レポート (P. 416)
- デバイス サマリ レポート (P. 417)
- 例外ユーザ レポート (P. 418)
- ルール設定レポート (P. 418)
- ルール データ レポート (P. 419)

インスタンス管理レポート

このレポートは MA のみが利用可能です。このレポートは、以下のいずれかまたはすべてのイベントのインスタンス管理アクティビティの詳細を表示します。

- システム キャッシュ リフレッシュ
- インスタンス設定の更新
- 起動
- キャッシュ リフレッシュ
- シャットダウン

以下の表に、インスタンス管理レポートに含まれる情報を示します。

フィールド	Description
［Instance Name］	CA Risk Authentication サーバまたはケース管理キュー サーバ インスタンスの名前。

フィールド	Description
サーバ タイプ	アクティビティが実行されたサーバ タイプ（CA Risk Authentication サーバまたはケース管理キュー サーバ）。
アクティビティ タイプ	実行されたアクティビティのタイプ。
アクティビティ時間	アクティビティが実行された時刻。
インスタンス設定	CA サポート担当者によってトラブルシューティングの目的で使用されます。
リフレッシュされた組織	キャッシュがリフレッシュされた組織。

トランザクションの分析レポート

重要: GA、OA、および FA （不正行為アナリスト）のみが、スコープ内にある組織のユーザ トランザクションを分析できます。MA、UA、および CSR はこのタスクを実行 *できません*。

トランザクションの分析レポートの表示には、以下のような複数の手順が含まれています。

- 手順 1： トランザクション サマリの表示
- 手順 2： ケース詳細の表示
- 手順 3： 類似トランザクションの表示
- 手順 4： トランザクションに詳細調査のマークを付ける（P. 409）

［トランザクション サマリ］ページに指定された基準に基づいてすべてのトランザクションを検索する際に、1 つ以上の疑わしいトランザクションが見つかった場合は、それらのトランザクションの詳細をさらに詳しく検索することができます（手順 2： ケース詳細の表示）。 類似したトランザクションを表示することにより（手順 3: 類似トランザクションの表示）、さらにパターンを検索することができます。 詳細を分析し、パターンを発見したら、疑わしいトランザクションに CSR による詳細な調査が行われるようにマークを付けることができます（手順 4： トランザクションに詳細調査のマークを付ける (P. 409)）。

手順 1: トランザクション サマリの表示

トランザクション サマリを表示するには、以下の手順に従います。

1. 適切な認証情報でログインしていることを確認します。
2. メイン メニューの［**レポート**］タブをアクティブにします。
3. ［**レポート**］サブメニューをクリックします。

   レポート タイプに対応するリンクが、左側のタスク パネルに表示されます。
4. ［**トランザクションの分析レポート**］リンクをクリックします。
5. ［**組織の選択**］リストから、レポートでデータをフィルタする組織を選択します。

   ［トランザクションを選択してください。］ページが表示されます。
6. ［**チャネルの選択**］ドロップダウン リストから、トランザクションを表示するチャネルを選択します。
7. トランザクションを表示するユーザの**ユーザ ID を入力します**。

   ユーザ名またはアカウント タイプのいずれかに基づいて検索できます。 組織に対してアカウントを設定していない場合、ユーザ名を入力するように促されます。

   注: ユーザの詳細を指定しない場合は、指定された**組織**のトランザクションがすべて表示されます。
8. 以下のいずれかの基準に基づいてトランザクションをフィルタする方法

   - トランザクション データをフィルタする［**トランザクション日付 - 開始**］および［**終了**］フィールドに基づいて、事前定義された日付範囲を選択します。

   または

   - ［**前回のトランザクション**］オプションを選択し、次に、実行された最新のトランザクションを参照する時間間隔（分単位）を選択します。
9. ［**リスク アドバイス**］リストから、データをフィルタするアドバイスに基づいて、アドバイスを選択します。
10. ［**セカンダリ認証ステータス**］リストから、データをフィルタするステータスに基づいて、ステータスを選択します。

11. ［**不正行為ステータス**］リストから、データをフィルタするステータスに基づいて、ステータスを選択します。
12. ［**ルール**］リストから、トランザクション データをフィルタするルールに基づいて、ルールを選択します。

    注: 一致したすべてのルールのトランザクションを参照する場合は、デフォルトの［**すべてのルール**］オプションが選択されていることを確認します。
13. **（3D セキュアの場合のみ）**［**販売者**］フィールドに業者名を入力し、トランザクション データをフィルタする基準（［**完全一致**］、［**指定の値で始まる**］、［**指定の値で終わる**］、［**指定の値を含む**］）を選択します。
14. トランザクション データをフィルタするデバイスの［**デバイス ID**］を入力します。
15. データをクリア テキストで表示する場合は、［**機密情報の復号化**］を選択します。
16. ［**提出**］をクリックして、［トランザクション サマリ］ページを生成します。

    ［**エクスポート**］をクリックすることにより情報を CSV ファイルに直接エクスポートできます。

    注:［**デフォルト**］または［**3D セキュア**］タブをクリックすると、チャネルに固有のトランザクションを表示できます。

    以下の表では、［トランザクション サマリ］ページに表示されるフィールドについて説明します。

フィールド	Description
詳細	トランザクションの詳細を調べるには、［**詳細**］リンクをクリックします。
User Name	トランザクションを実行するユーザの名前。
不正行為ステータス	ケースの不正ステータス。 このフィールドには、以下のいずれかのステータスを含めることができます。 ■ 不正行為と推定 ■ 正規と推定 ■ 不正行為と確認 ■ 正規と確認 ■ 未確定

フィールド	Description
国	IP アドレスを基に判別した、トランザクションが実行された国。
IP アドレス	購入トランザクションに使用したシステムまたはデバイスの IP アドレス。
一致するルール	一致し、CA Risk Authentication がトランザクションにリスクがあるとしてフラグを付けたルール。
トランザクション日付	トランザクションが実行されたタイム スタンプ。
リスク スコア	対応するトランザクションに対して CA Risk Authentication によって返された全体的なリスク スコア。 これは 0 ～ 100 の値です。
リスク アドバイス	トランザクションのリスク スコアを評価した後に CA Risk Authentication によって提案されたアクション。 使用可能なアクションは、以下のとおりです。 ■ ALLOW ■ ALERT ■ DENY ■ 認証の強化
デバイス ID	トランザクションに使用されたデバイスの ID。
モデル スコア	トランザクションに対してモデルによって返されたリスク スコア。これは 0 ～ 100 の値です。
セカンダリ認証ステータス	リスク アドバイスが**認証の強化**である場合、この列ではアプリケーションがフィードバックとして CA Risk Authentication に返した追加の認証の結果を指定します。
アカウント タイプ	トランザクションに関連付けられたアカウント タイプ。 組織のアカウント タイプを設定している場合にのみ、この列が表示されます。
すべてのルール結果	トランザクションのすべてのルールの結果。 結果は **Y** または **N** です。
アカウント ID	ユーザと関連付けられたアカウント ID がある場合、この列ではトランザクションを実行するために使用されたアカウント ID を指定します。
デバイス タイプ	トランザクションに関与するデバイスのタイプ。
トランザクション ID	各ユーザ トランザクションに生成された一意の ID。

フィールド	Description
OS	トランザクションを実行するために使用されたデバイス上のオペレーティング システム。
ブラウザ	トランザクションを実行するために使用されたブラウザ。
デバイス ID ステータス	デバイス ID のステータス。 ■ **読み取り**： デバイス ID がデバイスから読み取られました。 ■ **新規**： デバイス ID がデバイスに割り当てられました。 ■ **逆方向ルックアップ**： デバイス ID が、入力デバイス シグネチャをユーザに正常に関連付けられたデバイス シグネチャと照合することにより特定されました。
アクション	ユーザによって実行されたトランザクションのタイプ。以下の値にすることができます。 ■ ログイン ■ 電子送金 ■ アプリケーション経由で指定したその他の任意の値

手順 2: ケース詳細の表示

［トランザクション サマリ］ページを使用して、特定のトランザクションまたはケースの詳細を表示することもできます。 特定のケースの詳細を表示するには、以下の手順に従います。

1. ［トランザクション サマリ］ページで、対応する［**詳細**］列で該当する［**詳細**］リンクをクリックします。

   トランザクションの詳細がページに表示されます。 このページでは、選択されたトランザクションの詳細をリスト表示し、使用可能なパラメータに基づいてさらにトランザクションをフィルタすることもできます。

   以下の表では、［トランザクションの詳細］ページに表示されるフィールドについて説明します。

フィールド	Description
トランザクションの詳細（基本）	

フィールド	Description
トランザクション ID	トランザクションの一意の識別子。
トランザクション日付	トランザクションが実行されたタイム スタンプ。
アクション	ユーザによって実行されたトランザクションのタイプ。以下の値にすることができます。 ■ ログイン ■ 電子送金 ■ アプリケーション経由で指定したその他の任意の値
User Name	トランザクションを実行したユーザの名前。
不正行為ステータス	現在の不正ステータス。 以下の値が使用可能です。 ■ 未確定 ■ 不正行為と推定 ■ 正規と推定 ■ 不正行為と確認 ■ 正規と確認
デバイス ID	トランザクションに使用されたデバイスの ID。
リスク アドバイス	選択されたトランザクションのリスク スコアを評価した後にリスク評価モジュールによって提案されたアクション。 使用可能なアクションは、以下のとおりです。 ■ ALLOW ■ ALERT ■ DENY ■ INCREASEAUTH
一致するルール	一致し、CA Risk Authentication がトランザクションにリスクがあるとしてフラグを付けたルール。
セカンダリ認証ステータス	リスク アドバイスが**認証の強化**である場合、この列ではアプリケーションがフィードバックとして CA Risk Authentication に返した追加の認証の結果を指定します。 可能な値は［成功］と［失敗］です。
アカウント タイプ	トランザクションに関連付けられたアカウント タイプ。

フィールド	Description
アカウント ID	トランザクションを実行したユーザのアカウント ID。
モデル スコア	トランザクションに対してモデルによって返されたリスク スコア。
リスク スコア	対応するトランザクションに対して CA Risk Authentication によって返された全体的なリスク スコア。 これは 0 ～ 100 の値です。
場所の詳細	
IP アドレス	購入トランザクションに使用したシステムまたはデバイスの IP アドレス。
市区町村	トランザクションがユーザによって実行された都市。
都道府県	ユーザの所在地の都道府県。
国	ユーザの所在地の国。
接続タイプ	ユーザのデバイスとインターネット サービス プロバイダの間の接続のタイプ。 以下の値を指定できます。 ■ Satellite ■ OCX ■ Frame Relay ■ TX ■ Dialup ■ Cable ■ DSL ■ ISDN ■ Fixed Wireless ■ Mobile Wireless
回線速度	ユーザのインターネット接続の速度。 これは接続タイプに基づいています。

フィールド	Description
IP ルーティング タイプ	接続に使用した IP ルーティング メソッド。 以下の値を指定できます。 ■ Fixed： ケーブル、DSL、OCX ■ AOL： AOL ユーザ ■ POP： 地域 ISP までのダイアルアップ ■ Super POP： 多地域 ISP までのダイアルアップ ■ Cache Proxy： アクセラレータ プロキシ、コンテンツ配信サービス ■ Regional Proxy： 国内の多地域用プロキシ ■ Anonymizer： 匿名プロキシ ■ Satellite： 民生用衛星またはバックボーン衛星 ISP ■ International Proxy： 国際トラフィックを収束するプロキシ ■ Mobile Gateway： インターネットへのモバイル デバイス ゲートウェイ ■ 不明： 現在特定できません
アノニマイザ タイプ	アノニマイザのタイプ（ある場合）は、接続に使用されます。 以下の値を指定できます。 ■ **プライベート**： 公衆アクセスが可能でない匿名のプロキシ。 このタイプのアノニマイザは通常企業が所有しています。 ■ **アクティブ**： 過去 6 か月以内に陽性のテスト結果が出た匿名のプロキシ。 ■ **要注意**： 過去 6 か月以内にはなく、過去 2 年以内に陽性のテスト結果が出た、匿名のプロキシ。 ■ **非アクティブ**： 過去 2 年以内に陽性のテスト結果が出なかった匿名のプロキシ。 ■ **不明**： 陽性のテスト結果が現在まで得られていない匿名のプロキシ。
リスク評価の詳細	
MFP 一致 %	受信されたマシン フィンガープリント（MFP）と CA Risk Authentication データベースに格納されている値との一致率。 これは数値です。

フィールド	Description
Unknown User	Unknown User ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Exception User Check	Exception User Check ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Negative Country Check	Negative Country Check ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Device MFP Not Match	Device MFP Not Match ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Trusted IP/Aggregator Check	Trusted IP/Aggregator Check ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Untrusted IP Check	Untrusted IP Check ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。

フィールド	Description
User Velocity Check	ユーザ頻度チェック ルールが一致したかどうか。以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Unknown DeviceID	Unknown DeviceID ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
Device Velocity Check	デバイス頻度チェック ルールが一致したかどうか。以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
ゾーン ホッピング チェック	ゾーン ホッピングのチェック ルールが一致したかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
User Not Associated with DeviceID	ユーザとデバイスの関連付けが CA Risk Authentication データベース内で見つかったかどうか。 以下の値を指定できます。 ■ **Yes**： ルールが一致した場合。 ■ **No**： ルールが一致しなかった場合。 ■ **N/A**： リスク評価中に情報を得られなかった場合。
デバイスの詳細	
デバイス タイプ	トランザクションに関与するデバイスのタイプ。
OS	トランザクションを実行するために使用されたデバイス上のオペレーティング システム。
ブラウザ	トランザクションを実行するために使用されたブラウザ。

フィールド	Description
デバイス ID ステータス	デバイス ID のステータス。 ■ 読み取り： デバイス ID がデバイスから読み取られました。 ■ 新規： デバイス ID がデバイスに割り当てられました。 ■ 逆方向ルックアップ：デバイス ID が、入力デバイス シグネチャをユーザに正常に関連付けられたデバイス シグネチャと照合することにより特定されました。

手順 3: 類似トランザクションの表示

トランザクション詳細の最後にある小さなテーブルを使用することによって、データベースから類似したトランザクションについての詳細なデータを抽出するフィルタ条件を指定できます。

トランザクションを以下のパラメータに基づいてさらにフィルタすることができます。

- **同一ユーザ**： このオプションを選択すると、現在表示しているデータを所有するユーザに属するすべてのトランザクションを抽出できます。
- **同一デバイス**： このオプションを選択すると、現在詳細を表示しているトランザクションに使用されたのと同じデバイスを使用して実行されたトランザクションをすべて抽出できます。
- ［**同一 IP アドレス**］： このオプションを選択すると、現在詳細を表示しているトランザクションと同じ IP アドレスを持つトランザクションをすべて抽出できます。
- **トランザクション日付**： （［**開始**］フィールドと［**終了**］フィールドを使用して）日付範囲を指定することによって、指定された期間内に実行されたすべてのトランザクションをさらにフィルタすることができます。

  または

- ［**前回のトランザクション**］： 必要な時間間隔（分単位）を選択することによって、指定された間隔で実行された最新のすべてのトランザクションをさらにフィルタすることができます。

関連するトランザクションの表示

関連するトランザクションを表示する方法

1. ［トランザクションの詳細］ページで、以下のオプションのいずれかまたはすべてを選択します。
   - 同一ユーザ
   - 同一デバイス
   - 同一 IP アドレス
2. 以下のいずれかを行います。
   a. ［**トランザクション日付 - 開始**］フィールドおよび［**終了**］フィールドに日付の範囲を入力します。

   または

   b. ［**前回のトランザクション**］オプションを選択し、関連するトランザクションを参照する最新の時間間隔を選択します。
3. ［**表示**］をクリックします。

   ［トランザクション サマリ］ページが表示され、基準と一致したレコードが表示されます。

手順 4: トランザクションに詳細調査のマークを付ける

疑わしいトランザクションの詳細を分析するか、パターンを発見したら、疑わしいトランザクションに CSR による詳細な調査が行われるようにマークを付けることができます。 以下の手順を実行します。

1. 必要な権限でログインしていることを確認します。
2. 「手順 1: トランザクション サマリの表示」で説明されているように、［トランザクション サマリ］ページを表示します。
3. 指定した基準で表示されるトランザクションを確認します。

   「手順 2： ケース詳細の表示」を参照してください。
4. 類似するパターンを表示する場合は、「手順 3： 類似トランザクションの表示」の手順に従います。
5. スクロールしてトランザクション サマリ テーブルに戻ります。
6. テーブル内のトランザクションに対応するチェック ボックスをオンにすることにより、疑わしいトランザクションを選択します。
7. ［**調査対象としてマーク**］をクリックして、マークしたトランザクションのケースを生成します。

   これにより、これらのケースがリストに表示され、CSR はケースを処理できます。

リスク評価詳細アクティビティ レポート

このレポートは、CA Risk Authentication サーバによって実行されたすべてのトランザクションを表示します。

このレポートを生成するには、以下の項目を指定する必要があります。

- **組織名**。
- **チャネル**。
- **ユーザ ID**（必要な場合）。

  これはユーザ名またはアカウント タイプのいずれかに基づきます。
- **日付範囲**。

以下の表に、リスク評価詳細アクティビティに含まれる情報を示します。

フィールド	Description
ログ日付	ユーザのリスク評価が実行されたときのタイム スタンプ。
User Name	リスク評価アクティビティを実行したユーザの一意の ID。
［Organization Name］	ユーザが属する組織です。
トランザクション タイプ	CA Risk Authentication サーバによって実行されたリスク評価アクティビティのタイプ。 これには以下のアクティビティが含まれます。 ■ リスクの評価 ■ 属性の更新 ■ 関連付けの作成 ■ 関連付けの削除
ステータス	実行されたイベント アクションのステータス。以下のステータスを使用できます。 ■ **成功**： CA Risk Authentication はリスク評価アクティビティを正常に実行することができました。 ■ **失敗**： CA Risk Authentication はリスク評価アクティビティを正常に実行することができませんでした。
スコア	指定されたトランザクションのために生成されたスコア。

フィールド	Description
アドバイス ID	生成されたスコアに応じて CA Risk Authentication が生成したアドバイス。 アドバイスは以下のいずれかです。 ■ Allow ■ Deny ■ Alert ■ 認証強化
一致するルール	一致したルール。
セカンダリ認証結果	CA Risk Authentication によって生成された**リスク アドバイス**が「追加認証」だった場合、アプリケーションによって CA Risk Authentication に返されたセカンダリ認証の結果。
トランザクション ステータス	トランザクションのステータス。
設定名	ユーザが所属する組織用に設定されたルール セット。
アクション	現在のイベントで実行された対応するアクション（ログインなど）。
コール元 ID	呼び出し元のアプリケーションによって CA Risk Authentication API に渡された一意の識別子。 **注**: 呼び出し元のアプリケーションが値を設定しなかった場合は、［コール元 ID］が空白である可能性があります。
トランザクション ID	CA Risk Authentication サーバにトランザクション（管理者のログイン、レコードの表示、ユーザおよび組織情報の更新など）をサブミットするごとに作成される一意の数値識別子。 **注**: この ID を使用して、ログ ファイル内の特定のトランザクションに関する情報を特定できます。
［Session ID］	管理コンソールにログインするごとに作成される一意の数値識別子。 ログアウトするまでこのセッションは続きます。
インスタンス ID	CA Risk Authentication サーバの複数のインスタンスが実行されている場合、このフィールドはログインしたインスタンスを一意に識別します。 **注**: このデータは問題を診断するために CA サポート担当者によって使用されます。
国	トランザクションが発生した国。 **注**: これは［**クライアント IP アドレス**］の値から導出されます。

フィールド	Description
クライアント IP アドレス	エンド ユーザのシステムの IP アドレスです。
受信デバイス ID	受信デバイス ID 文字列。
送信デバイス ID	エンド ユーザのシステムからの初めてのトランザクションである場合、トランザクションの実行中に生成された対応するデバイス ID。
デバイス タイプ	トランザクションに関与するデバイスのタイプ。
デバイス ID ステータス	デバイス ID のステータス。 ■ 読み取り： デバイス ID がデバイスから読み取られました。 ■ 新規： デバイス ID がデバイスに割り当てられました。 ■ 逆方向ルックアップ： デバイス ID が、入力デバイス シグネチャをユーザに正常に関連付けられたデバイス シグネチャと照合することにより特定されました。
すべてのルール結果	適用されたすべてのルールの結果。 ルールが適用された場合、結果（［**はい**］または［**いいえ**］）は、ルールが一致を返したかどうかを示します。
アカウント タイプ	組織に対して設定されたアカウント タイプ。
アカウント ID	リスク評価アクティビティを実行したユーザのアカウント ID。

リスク アドバイス サマリ レポート

アドバイス サマリ レポートでは、指定された期間に Risk Authentication が返したアドバイスの全体のサマリを提供します。 また、別の表に、すべての 2 次認証結果の詳しい内容を示します。

注: Risk Authentication は、ユーザが試行したトランザクションごとにリスク アドバイスを返します。 Risk Authentication が送信したアドバイスに基づき、アプリケーションは、ユーザがトランザクションを完了することを許可したり、そのトランザクションを拒否したりすることができます。

このレポートを生成するには、以下の項目を指定する必要があります。

- 日付範囲。
- チャネル。
- 組織名（必要な場合）。

以下の表に、Risk Authentication アドバイス サマリ レポートに含まれる情報を示します。

フィールド	Description
チャネル	トランザクションが実行されたチャネル。
Allow	Risk Authentication が許可アドバイスを生成したトランザクションの総数。
認証強化	Risk Authentication が認証の強化アドバイスを生成し、アプリケーションがユーザに追加認証を要求したトランザクションの総数。
Alert	Risk Authentication がアラート アドバイスを生成したトランザクションの総数。
Deny	Risk Authentication が拒否アドバイスを生成したトランザクションの総数。
合計	生成されたリスク アドバイスの総数。

以下の表に、2 次認証結果サマリ レポートに含まれる情報を示します。

フィールド	Description
チャネル	■ トランザクションが実行されたチャネル。
Success	成功したすべての 2 次認証試行の合計回数。
［Failure］	ユーザによる、失敗したすべての 2 次認証試行の合計回数。
未確定	2 次認証の結果がアプリケーションから Risk Authentication に転送されなかった場合のすべてのインスタンスの総数。
合計	生成された結果に関係なく、実行された 2 次認証の総数。

不正行為統計レポート

以下の表で説明されているように、不正行為統計レポートは指定された期間内に CA Risk Authentication によって生成された各リスク アドバイスの統計を表示します。 ルール有効性レポートおよび誤検知レポートと共に、このレポートは不正行為アナリストが時間の機能としてそれらのルール セットのパフォーマンスを追跡するのを支援します。

パラメータ	Description
リスク アドバイス	各トランザクションのリスクを評価した後に CA Risk Authentication によって提案されたアクションを示します。 生成されたリスク アドバイスは以下のいずれかになります。 ■ Alert ■ 認証強化 ■ Allow ■ セカンダリ チャネル ■ Deny

パラメータ	Description
不正行為	CA Risk Authentication によって不正行為としてレポートされたすべてのトランザクションの総数およびパーセンテージを示します。
正規	CA Risk Authentication によって正当な行為と見なされたすべてのトランザクションの総数およびパーセンテージを示します。
未確定	CA Risk Authentication がリスク アドバイスを生成するための十分なデータを持っていなかったすべてのトランザクションの総数およびパーセンテージを示します。
合計	各「リスク アドバイス」に対するすべてのトランザクションの合計を示します。 また、全体的な**合計**も示します。

ルール有効性レポート

ルールの有効性は変化し、一般には時間の経過により低下します。 不正行為の実行者は、ルールを回避する新しい攻撃方法を見つけます。 ビジネスは進化し、以前は保護されていなかったアクセスや取引の新しい道が開かれます。 システムを変更すると、データの意味が変わり、わずかなダウンストリーム効果が発生します。 これらのすべての理由により、不正行為アナリストの担当業務の大部分が既存のルール セットの監視になります。 このレポートを使用すると、設定されたルールおよびそのスコアの有効性を評価することができます。

ルール有効性レポートは、以下の表で説明されているように、リスク評価に対して結果を確立したルールを表で示します。

パラメータ	Description
ルール名	システムで現在設定されているルールをリスト表示します。
アドバイス	各トランザクションのリスクを評価した後に CA Risk Authentication によって提案されたアクションを示します。生成されたリスク アドバイスは以下のいずれかになります。 ■ 認証強化 ■ Alert ■ Deny
トランザクション数（昨日）	過去 24 時間のレポート生成で対応するルール名がトリガされた合計回数を指定します。

パラメータ	Description
過去 7 日間 トランザクション数	過去 7 日間のレポート生成で対応するルール名がトリガされた合計回数を指定します。
過去 7 日間 日単位平均	過去 7 日間のレポート生成で対応するルール名がトリガされた平均回数を指定します。
トランザクション数（過去 30 日間）	過去 30 日間のレポート生成で対応するルール名がトリガされた合計回数を指定します。
過去 30 日間 日単位平均	過去 30 日間のレポート生成で対応するルール名がトリガされた平均回数を指定します。

誤検知レポート

誤検知レポートは、以下の表で説明されているように、リスク評価に対して結果を確立したルールを表で示します。

パラメータ	Description
ルール名	システムで現在設定されているルールをリスト表示します。
アドバイス	各トランザクションのリスクを評価した後に CA Risk Authentication によって提案されたアクションを示します。生成されたリスク アドバイスは以下のいずれかになります。 ■ 認証強化 ■ Alert ■ Deny
トランザクション数	指定された期間に対応するルール名がトリガされた合計回数を指定します。
不正行為	対応するルール名が不正なトランザクションに対して誤検知の結果を生成したすべてのトランザクションの総数を指定します。
正規	対応するルール名が正当なトランザクションに対して誤検知の結果を生成したすべてのトランザクションの総数を指定します。
未確定	対応するルール名がリスク アドバイスを生成するための十分なデータを持っていなかったすべてのトランザクションの総数を示します。

デバイス サマリ レポート

このレポートは、デバイス タイプごとのトランザクションの総数、およびデバイス ID を特定した方法を表示します。

このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な**組織名**。
- **チャネル**。
- **日付範囲**。

以下の表に、デバイス サマリ レポートに含まれる情報を示します。

フィールド	説明
デバイス タイプ	トランザクションの発生元であるデバイスのタイプ。
デバイス ID 読み取り	デバイス ID がトランザクションに関与するデバイスから読み取られたトランザクションの数。
新しいデバイス	デバイス ID がトランザクションに関与するデバイスに割り当てられたトランザクションの数。
逆方向ルックアップ	逆引き検索メカニズムを使用してデバイス ID が回復されたトランザクションの数。
合計	特定のデバイス タイプから生成されたトランザクションの総数。

例外ユーザ レポート

このレポートは、CA Risk Authentication システムに設定されているすべての例外ユーザのリストを表示します。

このレポートを生成するには、以下の項目を指定する必要があります。

- **日付範囲**。
- 必要な**組織名**。
- **ユーザ名**。

以下の表に、CA Risk Authentication 例外ユーザ レポートに含まれる情報を示します。

フィールド	Description
Start Date	ユーザがシステムで例外ユーザと見なされるようになった日時。
End Date	ユーザがシステムで例外ユーザではなくなる日時。
ユーザ	一意のユーザ名。
理由	システムでそのユーザを例外ユーザにした理由。
組織	管理者が属する組織。

ルール設定レポート

ルール設定レポートは、組織に対して展開されたすべてのルールの全体的なサマリを表示します。 このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- ターゲット情報の**ステータス**。

以下の表に、ルール設定レポートに含まれる情報を示します。

フィールド	説明
ルール名	ルールの名前。
有効	ルールが有効かどうかを示します。
優先度	ルールの優先度。

フィールド	説明
スコア	指定されたトランザクションのために生成されたスコア。
アドバイス	生成されたスコアに応じて RiskMinder が生成したアドバイス。アドバイスは以下のいずれかです。 ■ 許可 ■ 拒否 ■ アラート ■ 認証強化
ルール式	評価されるルール式。
チャネル	ルールが展開されるチャネル。
アクション	ルールに対して許可されるアクション。
ルールの短縮名	ルールの短縮名。
説明	ルールの説明。

ルール データ レポート

ルール データ レポートは、組織のためにアップロードされた、選択済みのリストの要約データを表示します （リスト データ、およびルールで使用するリストをアップロードする方法の詳細については、「ルール リスト データのアップロード (P. 220)」を参照してください）。

このレポートを生成するには、以下の項目を指定する必要があります。

- 必要な**組織名**。
- 必要な**ルール セット名**。
- **ルールリスト タイプ**。
- アップロードされた**リスト**名。
- ターゲット情報の**ステータス**。

ケース管理レポート

このカテゴリで利用可能なレポートの詳細については、「ケース管理レポートの生成」を参照してください。

レポートの生成

このセクションでは、次の項目について説明します。

- レポートを生成する際の注意事項 (P. 420)
- レポートの生成 (P. 421)

レポートを生成する際の注意事項

レポートの生成時には、以下の点に注意する必要があります。

- 管理者は、スコープを持つ組織のレポートのみを生成できます。
- 管理者は、下位または同レベルの管理者のレポートを生成できます。

  たとえば、組織管理者（OA）は、OA とユーザ管理者（UA）のレポートを生成できます。
- Oracle データベースを使用している場合は、UNLIMITED TABLESPACE 権限を有効にしていることを確認します。

レポートの生成

管理者固有または CA Risk Authentication 固有のレポートを生成する方法

1. 適切な認証情報（MA、GA、OA、または UA）でログインしていることを確認します。
2. メイン メニューの［**レポート**］タブをアクティブにします。
3. 生成するレポートに応じて、以下の手順に従います。
   - 管理者アクティビティ レポートを生成する場合は、［**管理者レポート**］サブメニューをクリックします。
   - CA Risk Authentication 固有のレポートを生成する場合は、［**レポート**］サブメニューをクリックします。

   レポート タイプに対応するリンクが、左側のタスク パネルに表示されます。
4. 生成するレポートに応じて、左側のサブメニューから必要なリンクをクリックします。

   注: CA Risk Authentication では、管理者レポートにクリア テキスト データまたは暗号化されたデータのどちらを表示するかを選択できます。すべての管理者レポートについて、レポートにクリア テキストでデータを表示する場合は、［**機密情報の復号化**］を選択します。
5. 選択に応じて以下の条件を 1 つ以上指定し、レポートを表示します。
   - ドロップダウン リストから［**日付範囲**］

     または
   - ［**開始**］および［**終了**］フィールドで事前定義済み日付範囲
6. レポートによっては、さらに以下の情報を指定する必要がある場合があります。
   - レポートに含めるデータを持つ、必要な組織の**組織名**。
   - **ユーザ名**または**管理者名**（生成するレポートに基づく）。
     - ユーザ名を入力します（ユーザ アクティビティ レポートの場合）。

     または
     - 管理者名を入力します（管理者アクティビティ レポートの場合）。

- レポートに含めるデータを持つ、必要なルール セットの**ルール セット名**。

7. ［**レポートの表示**］をクリックすると、指定した基準に基づいたレポートが生成されます。

レポートのエクスポート

CA Advanced Authentication には、レポートをファイルにエクスポートする機能が用意されています。レポートをエクスポートして、レポートのローカル コピーを保存できます。これを使用して傾向を追跡できます。また、保存したレポート データを別のアプリケーションで使用することもできます。

エクスポートされるレポートは、カンマ区切り値（CSV）形式で生成されるため、テキスト エディタや Microsoft Excel などのスプレッドシート アプリケーションで表示できます。 エクスポート オプションは、各レポートの右上に表示される［**エクスポート**］ボタンを介して利用できます。

レポートをローカル ファイルにエクスポートする方法

1. 必要なレポートを生成します。 詳細な説明については、「レポートの生成」を参照してください。 レポートが表示されます。
2. ［**エクスポート**］をクリックします。

   レポートを保存するか、開くかを問い合わせるプロンプトが表示されます。
3. レポートを開くか、またはファイルとして保存するかを選択します。レポートの保存を選択した場合は、ダウンロードする場所を指定する必要があります。

   このファイルは後ほど適切なアプリケーションを使用して表示できます。

arreporttool: レポートのダウンロード ツール

arreporttool では、Strong Authentication レポートまたは CA Risk Authentication レポートのデータを CSV ファイルにエクスポートできます。

重要: report-id および report-url パラメータは、エクスポートしようとしているレポートに対して正しい必要があります。

その後、テキスト エディタや、Microsoft Excel などのスプレッドシート アプリケーションを使用して、これらのレポートを表示できます。

ツールの使用

arreporttool.jar ファイルは、以下の場所にあります。

Windows の場合

<*install_location*>¥Arcot Systems¥tools¥common¥arreporttool

UNIX プラットフォームの場合

<*install_location*>/arcot/tools/common/arreporttool

構文

ツールに関連するヘルプを表示するには、以下のコマンドを実行します。

```
java -jar arreporttool.jar --help
```

ツールを使用するには、以下のコマンドを実行します。

```
java -jar arreporttool.jar –-protocol <protocol> --host <host>
--port CA Portal --admin-orgid <admin-organization>
--admin-id <admin-user-id> --admin-password <password>
[--report-type hour | day | month [duration] | range]
--report-id <Report ID> --reporturl <Url of the report>
--is-filter-req <true | false> --data-type <Data Type>
--reportdata [Report Data] --start-date-time <date-and-time> [--end-date-time
<date-andtime>] [--logfile <logfile>]
[--log-level <loglevel>][log-file-max-size] <logfilesize>] [--organizations <target
orgNames>] [--userName <User/Admin Name>] [--output-file <output-file>.CSV]
[--is-url-encoded [true|false]]
```

以下の表に、このツールでサポートされているオプションの説明を示します。

オプション	説明
protocol	通信に使用されるプロトコル。指定可能な値は http と https です。デフォルト プロトコルは http です。
host	管理コンソールを展開したシステムのホスト名または IP アドレス。
port	管理コンソールがリスンするポート。
admin-orgid	管理者が属する組織。
admin-id	一意の管理者 ID。
admin-password	管理者パスワード。

オプション	説明
report-type	時間、日、月または範囲を指定します。 ■ 時間、日、月の後に数値を指定できます。たとえば、--report-type day 2 は、指定した start-date-time からの 2 日間の記録を示します。 ■ 範囲： range を指定した場合は、end-date-time を指定する必要があります。
report-id	取得するレポートの識別子。 使用できるレポート識別子のリストについては、「レポートの識別子のリスト (P. 426)」を参照してください。
reporturl	レポートの管理者の URL。 使用できるレポートの URL のリストについては、「レポートの URL のリスト (P. 427)」を参照してください。
is-filter-req	デフォルトでは true に設定されます。 たとえば、RiskMinder レポートなど、フィルタ ページがないレポートに対してはこの値を false に設定します。
data-type	これは RiskMinder レポートにのみ適用されます。 このオプションは、データ型が ACTIVE か STAGING かを指定します。
reportdata	開始日と終了日のほかに、レポートによってはさらにフィルタが必要になることがあります。これらの追加フィルタはレポート データとして指定します。 レポート データは「キー=値」の形式で指定する必要があります。 複数のキーと値のペアを区切るには、セミコロンを使用します。 レポートのデータに ; または = が含まれている場合は、URL エンコードする必要があります。 URL エンコードされた値を渡す場合には、is-url-encoded パラメータを true に設定します。
start-date-time	レポートの内容をこの後から取得する必要がある日付または時刻を指定します。 **形式** MM/dd/yyyy HH:mm:ss 時間（HH）および分（mm）はオプションで、時間単位でのレポートにのみ使用します。 日単位および月単位のレポート対しては、日付部分だけを使用します。 例： 03/21/2010 09:10:20
end-date-time	（オプション）レポートの内容をこの前まで選択する必要がある日付または時刻を指定します。

オプション	説明
logfile	（オプション）ログ ファイルの場所を指定します。 ログ ファイルが指定されていない場合、ファイルは現在のディレクトリに自動的に作成されます。
log-level	（オプション）ログのレベルを指定します。デフォルトのログ レベルは［情報］です。
log-file-max-size	（オプション）ログ ファイルの最大サイズを指定します。デフォルト値は 10 MB です。
organizations	（オプション）レポートの対象となる組織の名前をセミコロンで区切って指定します。 組織が必須パラメータであるレポートにはこの値を指定する*必要があります*。 組織名にセミコロン（;）が含まれる場合は、値を URL エンコードする必要があります。 URL エンコードされた値を渡す場合には、is-url-encoded パラメータを true に設定します。
userName	（オプション）ユーザまたは管理者の名前を指定します。
output-file	（オプション）レポートの内容を書き込む必要がある出力ファイルを指定します。 **<reporttype>-timestamp.CSV** を使用します。
is-url-encoded	（オプション）この値は、レポート データや組織に URL エンコードされた情報が含まれているかどうかによって true または false に設定します。デフォルト値は false です。

レポートの識別子のリスト

以下の表に、report-id 引数に使用できるレポート識別子を示します。

レポート	レポート ID
マイ アクティビティ レポート	AAC.ViewMyActivityReport
管理者アクティビティ レポート	AAC.ViewActivityReport
ユーザ アクティビティ レポート	AAC.ViewUserActivityReport
組織レポート	AAC.ViewOrgActivityReport
ユーザ作成レポート	AAC.ViewUserCreationReport

レポート URL のリスト

以下の表に、reporturl 引数に使用できるレポート URL を示します。

レポート	レポート URL
マイ アクティビティ レポート	/Ac_AdminMyActivity/view.htm
管理者アクティビティ レポート	/Ac_Adminreport/view.htm
ユーザ アクティビティ レポート	/Ac_AdminUserActivity/view.htm
組織レポート	/Ac_AdminOrgActivity/view.htm
ユーザ作成レポート	/Ac_AdminUserCreation/view.htm

ツールの使用例

ユーザ アクティビティ レポートをダウンロードする方法

```
java –jar arreporttool.jar --protocol http --host localhost --port 8080  arcot
--admin-id ga --admin-password ga123 --report-id AAC.ViewUserActivityReport
--report-url /Ac_AdminUserActivity/view.htm --startdate-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log ARCOT –-userName ua
```

組織レポートをダウンロードする方法

```
java -jar arreporttool.jar --protocol http --host localhost --port 8080  arcot
--admin-id ga --admin-password ga123 --report-id AAC.ViewOrgActivityReport
–report-url /Ac_AdminOrgActivity/view.htm --start-date-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log --organizations ARCOT;TEST
```

第 17 章: CA Risk Authentication のログ

CA Risk Authentication サーバとアプリケーションの間の通信を効率的に管理するには、サーバおよび他のコンポーネントのアクティビティとパフォーマンスに加えて発生した可能性のある問題に関する情報を取得することが必要です。

この付録では、CA Risk Authentication によってサポートされている各種ログ ファイル、これらのファイルに表示される重大度レベル、およびこれらのログ ファイルの形式について説明します。 この章では、以下の内容について説明します。

ログ ファイルについて

CA Risk Authentication のログ ファイルは以下のように分類できます。

- インストール ログ ファイル
- スタートアップ ログ ファイル
- トランザクション ログ ファイル
- CA Advanced Authentication ログ ファイル
- UDS ログ ファイル

これらのファイル内のログ記録を制御するパラメータは、UDS ログ ファイルと CA Advanced Authentication ログ ファイルの場合は関連する INI ファイルを使用することにより、CA Risk Authentication ログ ファイルとケース管理キュー サーバ ログ ファイルの場合は CA Advanced Authentication 自体を使用することにより設定できます。これらのファイル中で変更できる典型的なログ記録設定オプションには以下のものが含まれます。

- **Specifying the log file name and path**： CA Risk Authentication ではログ ファイルの書き込み先およびバックアップ ログ ファイルの保存先のディレクトリを指定できます。診断ログ記録ディレクトリを指定することにより、管理者はシステムとネットワークのリソースを管理できます。
- **Specifying the log file size**： ログ ファイルに保存できる最大バイト数を指定できます。ログ ファイルがこのサイズに達すると、指定した名前で新規ファイルが作成され、古いファイルがバックアップ ディレクトリに移動されます。
- **Using log file archiving**： CA Risk Authentication コンポーネントが診断メッセージを実行し生成すると共に、ログ ファイルのサイズは増加します。ログ ファイルのサイズが増加し続けるように許可する場合、管理者はログ ファイルを手動で監視しクリーンアップする必要があります。 CA Risk Authentication では、収集および保存されるログ ファイル データの量を制限する設定オプションを指定できます。 CA Risk Authentication では、診断ログ ファイルのサイズを制御する設定オプションを指定することができます。この設定により、ログ ファイルの最大サイズを指定できます。 最大サイズに達すると、古いログ情報がバックアップ ファイルに移動され、その後新しいログ情報が保存されます。

- **Setting logging levels：** CA Risk Authentication ではログ レベルも設定できます。ログ レベルを設定して、診断ログ ファイルに保存されるメッセージ数を削減できます。 たとえば、クリティカルなメッセージのみをレポートおよび保存するように、ログ レベルを設定できます。 サポートされているログ レベルの詳細については、「サポートされる重大度レベル」を参照してください。
- **Specifying time zone information**： CA Risk Authentication では、ログ記録された情報のタイム スタンプに、ローカル タイムゾーンまたは GMT を使用できます。

インストール ログ ファイル

CA Risk Authentication をインストールする際、インストーラは Arcot_RiskFort_Install<*timestamp*>.log ファイルに、インストール時に指定したすべての情報および Arcot ディレクトリ構造の作成、レジストリ エントリの作成などの実行されたアクションを記録します。 このファイルの情報は、CA Risk Authentication インストールが正常に完了しなかった場合、問題のソースを識別するのに非常に役立ちます。

このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合：

<install_location>¥*<log_file_name>*

UNIX ベースの場合

<install_location>/*<log_file_name>*

スタートアップ ログ ファイル

CA Risk Authentication は CA Risk Authentication サーバとケース管理キュー サーバの 2 つのサーバ モジュールで構成されているため、スタートアップ ログ ファイルには以下の 2 つがあります。

- CA Risk Authentication サーバ スタートアップ ログ ファイル
- ケース管理キュー サーバ スタートアップ ログ ファイル

これらのファイルのデフォルトの場所は以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

CA Risk Authentication サーバ スタートアップ ログ ファイル

CA Risk Authentication サーバを起動すると、スタートアップ（またはブート）操作がすべて arcotriskfortstartup.log ファイルに記録されます。CA Risk Authentication サービスが起動しない場合、問題の原因を特定するためにこのファイルの情報が役立ちます。

このファイルでは、[arcot/riskfort/logger] セクションで指定されたログ記録関連のパラメータはすべて管理コンソールによって制御されます。 これらのログ パラメータを設定するには、［**インスタンス管理**］ページで目的のインスタンスをクリックし、インスタンス固有の設定ページにアクセスする必要があります。

CA Risk Authentication スタートアップ ログ パラメータの変更

CA Risk Authentication サーバの起動時に表示されるログ パラメータを変更する方法

1. ARCOT_HOME 内の conf ディレクトリに移動します。
2. 任意のテキスト エディタで arcotcommon.ini を開きます。
3. 以下のセクションをファイルの最後に追加します。

```
[arcot/riskfort/startup]
LogDir=logs
LogFileSize=2097152
BackupLogFileDir=logs/backup
LogLevel=2
LogTimeGMT=0
LogTrace=0
```

以下の表に、これらのパラメータの詳細を示します。

パラメータ	デフォルト	Description
LogDir	logs	デフォルトのログ ディレクトリの場所。 **注**: このパスは ARCOT_HOME からの相対パスです（Windows： <*install_location*>¥Arcot Systems Linux： <*install_location*>/arcot/）。
LogFileSize	10485760	ログ ファイルが記録できる最大**バイト**数。 ログ ファイルがこのサイズに達すると、新しいファイルが作成され、古いファイルは BackupLogFileDir で指定した場所に移動されます。
BackupLogFileDir	logs/backup	現在のファイルが LogFileSize のバイト数を超えた後で、バックアップ ログ ファイルが保持されるディレクトリの場所。 **注**: このパスは ARCOT_HOME からの相対パスです（Windows： <*install_location*>¥Arcot Systems Linux： <*install_location*>/arcot/）。

パラメータ	デフォルト	Description
LogLevel	1	サーバのデフォルトのログ記録レベル（上書きが指定されていない場合）。 以下の値を指定できます。 ■ 0 FATAL ■ 1 WARNING ■ 2 INFO ■ 3 DETAIL
LogTimeGMT	0	ログ ファイル内のタイム スタンプのタイム ゾーンを示すパラメータ。 以下の値を指定できます。 ■ 0 ローカル時間 ■ 1 GMT

1. 変更するパラメータに必要な値を設定します。
2. ファイルを保存して閉じます。
3. CA Risk Authentication サーバを再起動します。

ケース管理キュー サーバ スタートアップ ログ パラメータ

ケース管理キュー サーバの起動時に表示されるログ パラメータを変更する方法

1. ARCOT_HOME 内の conf ディレクトリに移動します。
2. 任意のテキスト エディタで arcotcommon.ini を開きます。
3. 以下のセクションをファイルの最後に追加します。

```
[arcot/riskfortcasemgmtserver/startup]
LogDir=logs
LogFileSize=2097152
BackupLogFileDir=logs/backup
LogLevel=2
LogTimeGMT=0
LogTrace=0
```

   これらのパラメータの詳細については、「CA Risk Authentication サーバ スタートアップ ログ ファイル」の表を参照してください。

4. 変更するパラメータに必要な値を設定します。
5. ファイルを保存して閉じます。
6. ケース管理キュー サーバを再起動します。

トランザクション ログ ファイル

トランザクション ログは以下で構成されます。

- CA Risk Authentication サーバ ログ
- ケース管理サーバのログ ファイル

CA Risk Authentication サーバ ログ

CA Risk Authentication では、arcotriskfort.log ファイルにサーバによって処理されたすべてのリクエストおよび関連するアクションを記録します。このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

注: CA Risk Authentication ロガーを使用してアプリケーションのログを設定することはできません。 これらのログには、アプリケーションをホストしているサードパーティ アプリケーション サーバ（Apache Tomcat や IBM Websphere など）が使用するツールを使用することにより、アクセスできます。

ログ記録関連のパラメータはすべて管理コンソールを使用して設定できます。 設定するには、［**インスタンス管理**］ページで目的のインスタンスをクリックし、インスタンス固有の設定ページにアクセスする必要があります。

ログ ファイル パス、ログ ファイルの最大サイズ（バイト単位）、バックアップ ディレクトリ、ロギング レベル、およびタイム スタンプ情報に加えて、トレース ロギングを有効にするかどうかを制御できます。このファイルで使用されるデフォルト形式の詳細については、「CA Risk Authentication サーバおよびケース管理サーバのログ ファイルの形式」を参照してください。

ケース管理サーバのログ ファイル

ケース管理サーバ モジュールを展開して開始した場合、そのすべてのアクションおよび処理されたリクエストの詳細は arcotriskfortcasemgmtserver.log ファイルに記録されます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

ログ記録関連のパラメータ（[arcot/riskfortcasemgmtserver/logger] セクションで指定）はすべて、管理コンソールを使用して設定できます。 設定するには、[**インスタンス管理**] ページで目的のインスタンスをクリックし、インスタンス固有の設定ページにアクセスする必要があります。

ログ ファイル パス、ログ ファイルの最大サイズ（バイト単位）、バックアップ ディレクトリ、ロギング レベル、およびタイム スタンプ情報に加えて、トレース ロギングを有効にするかどうかを制御できます。このファイルで使用されるデフォルト形式の詳細については、「CA Risk Authentication サーバおよびケース管理サーバのログ ファイルの形式」を参照してください。

CA Advanced Authentication ログ ファイル

CA Advanced Authentication を展開して起動すると、そのすべてのアクションおよび処理されたリクエストの詳細が arcotadmin.log ファイルに記録されます。 この情報には、以下のものが含まれます。

- データベースの接続情報
- データベースの設定情報
- インスタンス情報、およびこのインスタンスによって実行されたアクション
- UDS 設定情報
- キャッシュ リフレッシュなど、マスタ管理者が指定した他の管理コンソール情報

このファイル内の情報は、管理コンソールが起動しない場合に問題の原因を特定するうえで役立ちます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

これらのファイルでのログ記録を制御するパラメータは、adminserver.ini ファイルを使用することによって設定できます。このファイルは、ARCOT_HOME の conf フォルダにあります。

ログ レベル、ログ ファイル名およびパス、ログ ファイルの最大サイズ (バイト単位) 、ならびにログ ファイルのアーカイブ情報に加えて、log4j.appender.debuglog.layout.ConversionPattern に対する適切な値を指定することにより、コンソールのログ記録パターンのレイアウトを制御できます。

このファイルで使用されるデフォルト形式の詳細については、「UDS および管理コンソールのログ ファイルの形式」を参照してください。

UDS ログ ファイル

重要: LDAP 接続を有効にするために arcotuds.war ファイルを展開した場合にのみ、このファイルが生成されます。

UDS (ユーザ データ サービス) 情報およびアクションはすべて arcotuds.log ファイルに記録されます。 この情報には、以下のものが含まれます。

- UDS データベースの接続情報
- UDS データベースの設定情報
- UDS インスタンス情報、およびこのインスタンスによって実行されたアクション

このファイル内の情報は、CA Advanced Authentication が UDS インスタンスに接続できなかった場合に問題の原因を特定するうえで役立ちます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

このファイルでのログ記録を制御するパラメータは、udsserver.ini ファイルを使用することによって設定できます。このファイルは、ARCOT_HOME の conf フォルダにあります。

ログ レベル、ログ ファイル名およびパス、ファイルの最大サイズ（バイト単位）、ならびにアーカイブ情報に加えて、log4j.appender.debuglog.layout.ConversionPattern に対する適切な値を指定することにより、UDS のログ記録パターンのレイアウトを制御できます。

このファイルで使用されるデフォルト形式の詳細については、「UDS および CA Advanced Authentication のログ ファイルの形式」を参照してください。

CA Risk Authentication サーバおよびケース管理サーバのログ ファイルの形式

以下の表では、「CA Risk Authentication サーバのログ」で説明されている CA Risk Authentication ログ ファイル（arcotriskfort.log）のエントリの形式について説明します。

列	Description
タイム スタンプ	エントリがログに記録された時刻は、指定されたタイムゾーンに変換されます。 この情報のログの形式は次のとおりです。 www mmm dd HH:MM:SS.mis yy z 前の形式で、 ■ www は曜日を表します。 ■ mis はミリ秒を表します。 ■ z は、arcotcommon.ini ファイルで指定したタイムゾーンを表します。
［Log Level］ （または重大度）	ログに記録されたエントリの重大度レベル。 詳細については、「サポートされる重大度レベル」を参照してください。
プロセス ID（pid）	エントリをログに記録したプロセスの ID。
スレッド ID （tid）	このエントリをログに記録したスレッドの ID。
トランザクション ID	このエントリをログに記録したトランザクションの ID。
メッセージ	フリーフロー形式でサーバによってログに記録されたメッセージ。 **注**: このメッセージの情報量は、arcotcommon.ini に設定したログ レベルによって異なります。

UDS および CA Advanced Authentication のログ ファイルの形式

以下の表に、以下のログ ファイルのエントリの形式を示します。

- arcotuds.log （UDS ログ ファイル）
- arcotadmin.log （CA Advanced Authentication ログ ファイル）

列	関連付けられたパターン（ログ ファイル内）	Description
タイム スタンプ	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	エントリがログ記録された時刻です。このエントリはアプリケーション サーバのタイム ゾーンを使用します。 この情報のログの形式は次のとおりです。 yyyy-MM-dd hh:mm:ss,mis z ここで、 ■ mis はミリ秒を表します。 ■ z はタイム ゾーンを表します。
スレッド ID	[%t] :	このエントリをログに記録したスレッドの ID。
［Log Level］（または重大度）	%-5p :	ログに記録されたエントリの重大度レベル。 詳細については、「サポートされる重大度レベル」を参照してください。
ロガー クラス	%-5c{3}(%L) :	ログ リクエストを作成したロガーの名前です。
メッセージ	%m%n :	自由形式でログ ファイルに記録されるメッセージ。 **注**: メッセージの情報量は、ログ ファイルに設定したログ レベルによって異なります。

UDS ログ ファイルおよび管理コンソール ログ ファイルの PatternLayout パラメータをカスタマイズするには、以下の URL を参照してください。

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

サポートされる重大度レベル

ログ レベル（*重大度レベル*）を使用して、CA Risk Authentication ログに保存される情報の詳細のレベルを指定できます。 また、この設定により、ログ ファイルが増大する速度を制御できます。

サーバ ログ ファイルの重大度レベル

以下の表に、サーバ ログ ファイルに出現するログ レベルを重大度の*降順*で示します。

[Log Level]		Description
0	FATAL	CA Risk Authentication サービスの突然の終了を引き起こす可能性がある、重大で回復不可能なエラーにはこのログ レベルを使用します。 FATAL レベルでは、致命的な問題を示す状況のみがログ記録されます。
1	注意	望まないランタイム例外、潜在的に有害な状況、および回復可能で FATAL（致命的）ではない問題にはこのログ レベルを使用します。
2	INFO	ランタイム イベントに関する情報を取得する場合にこのログ レベルを使用します。 言い換えれば、この情報は、アプリケーションの進捗状況を強調します。進捗状況には、次の変化が含まれます。 ■ 起動、停止、再起動などのサーバ状態。 ■ サーバのプロパティ。 ■ サービスの状態。 ■ サーバ上のプロセスの状態。 たとえば、リクエストが受信されており、処理されていることを示すために常に記録されるログがあります。 これらのログは INFO レベルで表示されます。
3	LOW DETAIL	デバッグ目的で詳細情報をログに記録する場合に、このログ レベルを使用します。 これには、プロセス追跡およびサーバ状態の変化が含まれる場合があります。

注: ログ レベルを指定すると、それよりも重要度が*高い*レベルのメッセージもレポートされます。 たとえば、LogLevel が 3 と指定されている場合、FATAL、WARNING、および INFO の各ログ レベルを持つメッセージも収集されます。

CA Advanced Authentication ログ ファイルおよび UDS ログ ファイルの重大度レベル

以下の表に、以下のログ ファイルのエントリの形式を示します。

- arcotuds.log （UDS ログ ファイル）
- arcotadmin.log （CA Advanced Authentication ログ ファイル）

列	関連付けられたパターン（ログ ファイル内）	Description
タイム スタンプ	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	エントリがログ記録された時刻です。このエントリはアプリケーション サーバのタイム ゾーンを使用します。 この情報のログの形式は次のとおりです。 yyyy-MM-dd hh:mm:ss,mis z ここで、 ■ mis はミリ秒を表します。 ■ z はタイム ゾーンを表します。
スレッド ID	[%t] :	このエントリをログに記録したスレッドの ID。
［Log Level］（または重大度）	%-5p :	ログに記録されたエントリの重大度レベル。 詳細については、「サポートされる重大度レベル」を参照してください。
ロガー クラス	%-5c{3}(%L) :	ログ リクエストを作成したロガーの名前です。
メッセージ	%m%n :	自由形式でログ ファイルに記録されるメッセージ。 **注**: メッセージの情報量は、ログ ファイルに設定したログ レベルによって異なります。

UDS ログ ファイルおよび管理コンソール ログ ファイルの PatternLayout パラメータをカスタマイズするには、以下の URL を参照してください。

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

各ログ レベルのサンプル エントリ

以下のサブセクションでは、**CA Risk Authentication ログ ファイル**内のサンプル エントリを（ログ レベルごとに）示します。

FATAL

```
May 27 18:31:01.585 2010 GMT FATAL: pid 4756 tid 5152: 0: 0: Cannot continue due to
ARRF_LIB_init failure, SHUTTING DOWN
```

注意

```
May 24 14:47:39.756 2010 GMT WARNING: pid 5232 tid 5576: 0: 110000: EVALHTTPCALLOUT :
Transport Exception : create: No Transports Available
```

INFO

```
May 24 14:41:43.758 2010 GMT INFO: pid 3492 tid 4904: 0: 109002: Error in
ArPFExtRuleSetEval::evaluate Could not get user context (two parallel requests)
```

```
May 25 10:01:28.131 2010 GMT WARNING: pid 1048 tid 3104: 8: 0: Error in
ArRFCaseStatus::startInit: No data found
```

DETAIL

```
May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering USERRISKEVALVELOCITY Rule Evaluation function

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE: VELOCITY_DURATION=[60], VELOCITY_DURATION_UNIT=[MINUTES],
VELOCITY_TRANSACTION_COUNT=[5]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Entering UserRiskEvalVelocityRule
durationToTimeConvertor

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting
ArUserRiskEvalVelocityDBO::decisionLogicForUserVelocity

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting UserRiskEvalVelocityRule
callUserEvalVelocityRule

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.RESULT=[0]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : USERRISKEVALVELOCITY.DETAIL=[RESULT=0;TCOUNT=2;
ACT=mection]

May 24 14:52:01.219 2010 GMT LOW: pid 2132 tid 1356: 0: 111004:
USERRISKEVALVELOCITYRULE : Exiting USERRISKEVALVELOCITY Rule Evaluation function
```

付録 A: 地理的位置およびアノニマイザのデータ

RiskMinder は、高リスクのアクティビティを防ぐために、地理的位置および IP チェックを併用します。 これらの機能は、以下の目的にエンドユーザの IP アドレスを使用します。

- エンドユーザがブラックリストに載せた国または地域からアクセスしていないことを確認する。
- エンドユーザが実際に可能な速度より速く移動していないことを確認する。
- エンドユーザが自分の場所を隠していないことを確認する。
- エンドユーザがブラックリストに載せた IP アドレスからアクセスしていないことを確認する。

選択する軽減アクションを決定できます。これには、不正行為またはセキュリティ チームにセキュリティ侵害の可能性を警告する、エンドユーザに追加認証を自動的に要求する、または単にアクセスを拒否するなどがあります。

この付録では、RiskMinder での IP 地理的位置データおよび拒否 IP チェックの使用について説明します。 これらの 2 つの機能は共に、RiskMinder の不正行為および高リスク アクセス検知の主要コンポーネントの 1 つを提供します。 これらは、RiskMinder の既定のルール設定の一部として提供される以下のチェックをサポートします。

- 地理的位置（拒否国リスト）
- エンドユーザのアクセス場所の変更（ゾーン ホッピング）
- アノニマイザ データ（拒否 IP タイプ）
- 管理者によって定義された拒否 IP （拒否 IP アドレス リスト）

この付録では、以下のトピックについて説明します。

地理的位置およびアノニマイザのデータについて

地理的位置情報を提供する業界トップ企業である Quova Inc. から RiskMinder の地理的位置およびアノニマイザ データが提供されています。Quova は、以下のタイプのデータを RiskMinder に提供しています。

- **地理的位置データ**。 このデータは緯度、経度、大陸、国、および市区町村によって各 IP を分類します。 デフォルトでは、このデータは Negative Country Check ルール、および Zone Hopping Check ルールの距離の計算で使用されます。また、このデータはルール ビルダの使用により作成されるルールにも使用できます。 国と市区町村のエレメントは両方ともアクセス ポイントでのチェックに役立ちます。
- **接続情報**。 IP はそれぞれルーティング タイプ、接続タイプ および回線速度により分類されます。この情報（特にルーティング タイプ）は、地理的位置情報の妥当性を評価するのに役立ちます。 たとえば、接続タイプが［Satellite］である場合、ユーザの場所は信頼できません。 実際には、地理的位置目的ではこの情報を無視できます。 ただし、［Cable］、［DSL］、および［OCX］などの固定接続タイプは、その場所がインターネット アカウントまでより容易に追跡されるので、不正行為の発生元になる可能性は低くなります。 不正行為を評価するためにこのデータを使用できます。
- **アノニマイザ データ**。 Quova は、場所情報が信頼できるかどうかを判断するために IP アドレスの厳格なテストを実行しています。このテストの一部として、Quova は一部の IP アドレスを「アノニマイザ」として識別します。 このステータスを持った IP アドレスは、エンド ユーザの本当の場所を隠すために使用される匿名プロキシとして陽性のテスト結果が出ています。 これは必ずしもその目的が不正であることを示しているわけではありませんが、明らかにユーザがその場所を隠していることを示しています。そのため高リスク アクセスの可能性があることを表します。

RiskMinder ルールでの地理的位置データの使用

このセクションでは、以下の内容について説明します。

- 以下の RiskMinder ルールで使用される地理的位置情報。
  - Negative Country Check (P. 449)
  - Zone Hopping Check (P. 450)
- Quova がルーティング可能な各 IP アドレスに対して提供する地理的位置データ。
  - IP ルーティング タイプ (P. 450)
  - 接続タイプ (P. 451)
  - 回線速度 (P. 452)
  - 地域 (P. 453)
  - 大陸 (P. 453)

拒否国チェック

管理コンソールの [リスト データおよびカテゴリ マッピングの管理] ページを使用して、高リスクであると見なす国を追加または削除して拒否国リストを設定できます。 通常、このリストは、アクセスが何らかの形式の認証の強化を使用して常に確認される国のリストとして定義できます。 また、拒否ルールとして使用し、拒否国リスト内の少数の国のセットのみをリストすることもできます。 金融取引の場合、Negative Country Check ルールを金額ベースのルールと組み合わせてケース数を削減できます。 一般的なアクセス制御については、ルールは、より厳格なログイン プロセスをトリガするために認証の強化リスク アドバイスとして定義されます。 これらの状況で、ケースは作成されません。

ゾーン ホッピング チェック

場所の緯度および経度は、Zone Hopping Check ルールで使用されます。 このルールは、ユーザがアクセスに使用した IP アドレスから連続するトランザクションを行うために必要な物理的な移動に必要な速度をチェックします。 ユーザの移動が速すぎる場合、2 人がアカウントにアクセスしていたか、またはユーザが故意にまたは誤って自分の本当の場所を隠すために何かしたと判断する必要があります。 CA では、Zone Hopping Check ルールの値を提供されているデフォルト値に設定することから開始することを推奨します。 パフォーマンスに基づいて、特定のユーザ ベースの要件を満たすためにこのルールの設定を調整することができます。 デフォルト設定では、このルールは時間の約 0.02% で適用されることになります。 このルールの誤検知の割合は 10:1 未満が適切です。

IP ルーティング タイプ

IP ルーティング タイプは、ユーザの場所が IP アドレスの場所と一致する可能性を決定する IP アドレスの属性です。 以下の表では、IP ルーティング タイプに使用可能な値について説明します。

IP ルーティング タイプ	説明
fixed	ユーザ IP はユーザと同じ場所にあります。
anonymizer	ユーザ IP は、アノニマイザ アクティビティに対して陽性の結果が出ているネットワーク ブロック内にあります。 これは、ユーザがすべてのユーザ トラフィックを意図的にプロキシするサービスを使用することにより本当の場所を隠している可能性があることを意味します。
aol： aol pop aol dialup aol proxy	ユーザは AOL サービスのメンバです。Quova はほとんどの場合ユーザの国を識別できます。国より詳細な地域情報は識別できません。 GeoPoint AOL IP では、単純な Y/N （はい/いいえ）によって示されることに注意してください。
pop	ユーザは地域 ISP へダイアルしており、IP の場所の近くにいる可能性があります。ユーザは地理的な境界を越えてダイアルしている可能性があります。
superpop	ユーザは複数の都道府県または複数の国の ISP へダイアルしており、IP の場所の近くにいない可能性があります。ユーザは地理的な境界を越えてダイアルしている可能性があります。

IP ルーティング タイプ	説明
satellite	民生用衛星によってインターネットに接続するユーザ、または地上接続に関する情報がないバックボーン衛星プロバイダでインターネットに接続するユーザ。いずれの場合も、ユーザは衛星のビーム パターン内の任意の場所にいます。これは通常大陸以上に及びます。
cache proxy	ユーザはインターネット アクセラレータまたはコンテンツ配信サービスのいずれかによってプロキシされます。ユーザは任意の場所にいる可能性があります。
international proxy	複数の国からのトラフィックが含まれるプロキシ。
regional proxy	1 つの国内の複数の地域からのトラフィックが含まれるプロキシ（アノニマイザではない）。
mobile gateway	パブリック インターネットへモバイル デバイスを接続するゲートウェイ。 たとえば、WAP は携帯電話プロバイダによって使用されるゲートウェイです。
unknown	ルーティング メソッドが不明、または上記の説明で識別できません。

接続タイプ

接続タイプは、デバイスまたはプライベート LAN とパブリック インターネット プロバイダの間のデータ接続を示します。 以下の表では、接続タイプに使用可能な値について説明します。

接続タイプ	説明
ocx	これは、主として大規模バックボーン キャリアによって使用される OC-3 回路、OC-48 回路などを表します。
tx	これには、多くの中小企業によってまだ使用されている T-3 回路および T-1 回路が含まれます。
satellite	これは、民生用衛星と静止または低軌道衛星の間の高速またはブロードバンド リンクを表します。
framerelay	フレーム リレー回路は低速のものから高速のものまでがあり、T-1 のバックアップまたは代替として使用されます。 ほとんどの場合、これらは高速リンクのため、GeoPoint ではそのように分類されます。
dsl	デジタル加入者線ブロードバンド回路。ADSL、IDSL、および SDSL が含まれます。 通常、速度は 256k ～ 20 MB/秒の範囲です。

接続タイプ	説明
cable	ケーブル テレビ会社によって提供されるケーブル モデム ブロードバンド回路。 速度は 128k ～ 36 MB/秒で、ケーブル モデム スイッチにかかる負荷によって変わります。
isdn	サービス総合デジタル網の高速銅線テクノロジで、128K/秒の速度をサポートし、1MB/秒以上の速度を提供する ISDN モデムおよびスイッチを使用します。
dialup	このカテゴリは、56k/秒で動作するコンシューマ ダイアルアップ モデム スペースを表します。 プロバイダには Earthlink、AOL、および Netzero が含まれます。
fixed wireless	受信者の場所が固定されている固定ワイヤレス接続を表します。 カテゴリには、Sprint Broadband Direct などの WDSL プロバイダおよび新興の WiMax プロバイダが含まれます。
mobile wireless	CDMA、EDGE、EV-DO テクノロジを採用した Cingular、Sprint、Verizon Wireless などのセルラー ネットワーク プロバイダを表します。 速度は 19.2k/秒から 3 MB/秒までさまざまです。
unknown	GeoPoint が接続タイプを取得できなかったか、または接続タイプが上記の説明で識別できません。

回線速度

デバイスまたはプライベート LAN とパブリック インターネット プロバイダの間の接続タイプ (P. 451)の速度。 以下の表では、各接続タイプの回線速度に使用可能な値について説明します。

回線速度	対応する接続タイプ
high	OCX、TX、および Framerelay。
medium	Satellite、DSL、Cable、Fixed Wireless、および ISDN。
low	Dialup および Mobile Wireless。
unknown	Quova は回線速度情報を取得できませんでした。

地域

便宜上、Quova は米国を 10 の地理的地域に分割しています。

- 北東
- 中部大西洋
- 南東
- 五大湖
- 中西
- 中南
- 山岳
- 北西
- 太平洋
- 南西

完全なリストは、Quova Extranet の **Download** セクションの Reference Data にあります。 最新情報についてはこれらのテキスト ファイルを参照してください。

大陸

Quova は 8 つの大陸を認識します。

- アフリカ
- 南極
- アジア
- オーストラリア
- ヨーロッパ
- 北米
- オセアニア（メラネシア、ミクロネシア、ポリネシア）
- 南米

アノニマイザ データの使用

IP アドレスもアノニマイザのステータスで分類できます。 ルールに含まれるアノニマイザ IP のタイプを制御できます。 拒否 IP タイプのカテゴリは次のとおりです。

- 拒否
- アクティブ
- 要注意
- プライベート
- 非アクティブ
- 不明

ルールを示されているデフォルトに設定するか、または要注意 IP をクリアすることをお勧めします。 アノニマイザの使用は、必ずしも犯罪を行う意図を示すわけではありませんが、ユーザが自分の場所を隠しているので非常に不審です。 たとえば、ユーザが許可されていない国からゲームにアクセスしたり、ライセンスを取得していない地域からビデオや音楽コンテンツにアクセスするなどの犯罪に関連するアクティビティに参加している場合があります。 このルールのヒット率は、エンド ユーザのポートフォリオによって影響を受けるので、カスタマによって大きく変動します。 ただし、アノニマイザに基づいたレビュー率は約 0.1% （1000 のトランザクションのうち 1 つ）です。 誤検知の割合は、米国および欧州のユーザの 20:1 から、途上地域の 100:1 まで大きく異なる傾向があります。

拒否 IP アドレス リストの使用

Negative IP Check ルールは、単一のルールで 2 つの機能を実行します。

- このルールは、既知のアノニマイザ プロキシのリストとエンド ユーザの IP アドレスを照合します。
- このルールは、IP がテーブル内で定義されている範囲の 1 つにあるかどうかを確認するために定義する拒否 IP アドレス リストを参照します。

管理コンソールの [リスト データおよびカテゴリ マッピングの管理] ページを使用して、IP アドレスを拒否 IP アドレス リストに追加できます。 ブラックリストに載った IP アドレス用のルールのパフォーマンスは、どのようにリストを管理するかに依存します。 通常、停止する必要がある不正または危険なアクセスが発生した場合は IP をリストに追加し、正当なユーザがアクセスを要求した場合はリストから IP を削除します。

注: トランザクション レポートを調べて、エンド ユーザがブロックまたは認証を要求された理由を確認できます。

付録 B: サーバ リフレッシュおよび再起動タスクのサマリ

設定変更を行うと、サーバを再起動しなければならない場合が多くあります。 たとえば、.ini ファイルを変更する場合はすべて、サーバを再起動する必要があります。 また、管理コンソールを使用して変更を行った場合にも、サーバを再起動またはリフレッシュする必要がある場合があります。そのような場合、管理コンソールが必要に応じてリフレッシュまたは再起動するようにユーザに通知します。

注: リフレッシュを選択した場合、サーバのダウン タイムは一切発生しません。 ほとんどの設定変更では、サーバの再起動は不要です。

以下の表に、設定変更を行った後にリフレッシュまたは再起動が必要になるサーバ タスクを示します。

タスク	リフレッシュ	再起動
UDS 接続の設定	✓	
UDS の設定	✓	
属性の暗号化の設定	✓	
カスタム ロケールの設定	✓	
デフォルト組織の設定	✓	
アカウント タイプの追加	✓	
アカウント タイプの更新	✓	
アカウント タイプの削除	✓	
アカウント タイプへのカスタム属性の追加	✓	
電子メール/電話のタイプの設定	✓	
基本認証ポリシーの設定	✓	
Web サービスの認証および許可の有効化	✓	

タスク	リフレッシュ	再起動
［インスタンス設定］ページでの以下の更新 ■ **ロギング構成： トランザクション ログ ディレクトリ、ロールオーバー開始サイズ（バイト単位）、トランザクション ログ バックアップ ディレクトリ、タイムスタンプを GMT でログ記録** ■ **データベース構成： 最小接続数、最大接続数、最大追加接続数**		✓
［インスタンス設定］ページでの以下の更新 ■ インスタンス属性 ■ **ロギング構成： ログ レベル、トレース ログの有効化** ■ **データベース構成（最小接続数、最大接続数、最大追加接続数** *を除く*）	✓	
RiskMinder 接続性	✓	
トラステッド認証機関	✓	
プロトコル設定		✓
チャネルの割り当ておよびデフォルト アカウント タイプの設定	✓	
ルール セットの作成	✓	
新規ルールの追加		
ルールの更新	✓	
ルールの削除	✓	
その他の設定	✓	
モデル設定	✓	
コールアウト設定	✓	
運用環境への移行	✓	
組織の作成	✓	
組織の更新	✓	
キューの新規作成	✓	
キューの更新	✓	
キューの削除	✓	

付録 C: マルチバイト文字および暗号化されるパラメータ

RiskMinder は UTF-8 をサポートしています。これは、ユニバーサル Unicode エンコーディング スキームの可変長 8 ビットのエンコード形式です。 可変長エンコーディングによって、さまざまなバイト数を使用して文字セットをエンコードできます。UTF-8 の設定については、「*CA RiskMinder インストールおよび展開ガイド*」の「インストールの準備」を参照してください。

RiskMinder では、ハードウェアまたはソフトウェア ベースの機密データの暗号化も使用できます。機密パラメータを暗号化することを選択でき、レポートにクリア テキスト データを表示するか、暗号化されたデータを表示するかを決定することもできます。 以下の表に、暗号化およびマルチバイト文字のエンコーディングに選択できるパラメータを示します。 また、パラメータに使用するキーや、キーを使用できるレベルについても示します。

パラメータ	暗号化	HSM サポート	キー レベル	キー タイプ	マルチバイト
ユーザ名	オプション	○	組織	OrgKey	○
ユーザ属性	オプション	○	組織	OrgKey	○
設定					
Action	×	×	なし	なし	×
OrgName	×	×	なし	なし	×
DeviceID	×	×	グローバル	固定 - 内部	○
Device Signature	×	×	なし	なし	○
CALLERID	×	×	なし	なし	○
CONFIGNAME	×	×	なし	なし	×
CHANNELNAME	×	×	なし	なし	×
CLIENTIPADDRESS	×	×	なし	なし	×
AGGREGATORNAME	×	×	なし	なし	×
ASSOCIATIONNAME	×	×	なし	なし	×

パラメータ	暗号化	HSM サポート	キー レベル	キー タイプ	マルチバイト
ACCOUNTTYPE	×	×	なし	なし	×
MATCHEDRULE	×	×	なし	なし	×
LINESPEED	×	×	なし	なし	×
CONNECTIONTYPE	×	×	なし	なし	×
ANONYMIZERTYPE	×	×	なし	なし	×
IP_ROUTINGTYPE	×	×	なし	なし	×
Rule Mnemonic	×	×	なし	なし	×
Rule Name	×	×	なし	なし	○
Rule Description	×	×	なし	なし	○
ACCOUNTID	×	×	なし	なし	○
PARENTUSERID	×	×	なし	なし	○
ERROR MESSAGE	×	×	なし	なし	○
QUEUE NAME	×	×	なし	なし	×
QUEUE DESCRIPTION	×	×	なし	なし	○
CASENOTE	×	×	なし	なし	○
3D セキュア エレメント					
ACQ_BIN	×	×	なし	なし	×
MERCHANT_NAME	×	×	なし	なし	○
MERCHANT_ID	×	×	なし	なし	×
MERCH_COUN	×	×	なし	なし	×
MERCHANT_URL	×	×	なし	なし	×
XID	×	×	なし	なし	×
PURCHASE_DESCRIPTION	×	×	なし	なし	○
PAN	×	×	なし	なし	×
EXPIRY	×	×	なし	なし	×
MERCH_CAT	×	×	なし	なし	×

パラメータ	暗号化	HSM サポート	キー レベル	キー タイプ	マルチバイト
TERM_URL	×	×	なし	なし	×
PREVTXNDATA	×	×	なし	なし	×

以下の表では、パラメータが大文字と小文字を区別しないか、およびレポートで表示されるかどうかを示します。

パラメータ	大文字と小文字が区別されない	レポートでの表示
ユーザ名	○	○
ユーザ属性	○	○
設定		
Action	×	○
OrgName	×	○
DeviceID	×	○
Device Signature	×	×
CALLERID	×	×
CONFIGNAME	×	○
CHANNELNAME	×	○
CLIENTIPADDRESS	×	○
AGGREGATORNAME	×	○
ASSOCIATIONNAME	×	
ACCOUNTTYPE	×	○
MATCHEDRULE	×	○
LINESPEED	×	
CONNECTIONTYPE	×	
ANONYMIZERTYPE	×	○
IP_ROUTINGTYPE	×	
Rule Mnemonic	×	○
Rule Name	×	○

パラメータ	大文字と小文字が区別されない	レポートでの表示
Rule Description	×	○
ACCOUNTID	×	○
ERROR MESSAGE	×	×
QUEUE NAME	×	○
QUEUE DESCRIPTION	×	○
CASENOTE	×	○
3D セキュア エレメント		
ACQ_BIN	×	○
MERCHANT_NAME	×	○
MERCHANT_ID	×	○
MERCH_COUN	×	○
MERCHANT_URL	×	○
XID	×	×
PURCHASE_DESCRIPTION	×	×
PAN	×	×
EXPIRY	×	×
MERCH_CAT	×	×
TERM_URL	×	×
PREVTXNDATA	×	×

付録 D: 通貨換算

この付録では、通貨換算の概要、および ARRFCURRCONVRATES テーブルのスキーマについて説明します。 以下のトピックについて説明します。

- 通貨換算について (P. 464)
- 通貨換算テーブル (P. 465)

通貨換算について

ルール ビルダを使用して、トランザクション金額をルールで指定されたしきい値金額と比較するルールを設定できます。 組織に対して設定された基準通貨でしきい値金額を指定できます。 トランザクションの通貨と基準通貨が異なる場合、トランザクション金額はトランザクションの通貨から組織の基準通貨に自動的に換算されます。

特定のチャネルで一部のルール演算子を使用すると、組織の基準通貨でしきい値金額を指定し、複数の通貨でしきい値金額を指定することができます。 そのようなルールが実行されると、トランザクションの通貨はしきい値金額が指定された通貨と比較されます。 一致する場合、トランザクション金額はその通貨のしきい値金額と直接比較されます。 この場合、通貨換算は必要ありません。 ただし、一致しない場合、トランザクション金額はまず基準通貨に換算されてから基準通貨で設定されたしきい値と比較されます。

重要: 基準通貨でしきい値金額の 1 つを設定することは必須です。

以下の例では、この機能がどのように動作するかを示します。

例 1

組織の基準通貨は USD ですが、しきい値金額が USD、JPY、および AUD であるルールを設定しました。以下のシナリオでは、各種のトランザクション中に通貨換算がどのように行われるかを説明します。

- **シナリオ 1**: トランザクションは USD で行われています。トランザクションの通貨が組織の基準通貨と同じであるため、指定されたしきい値が通貨換算の必要なしで使用されます。
- **シナリオ 2**: トランザクションは JPY で行われています。JPY はしきい値金額が指定された通貨の 1 つであるため、トランザクション金額は JPY のしきい値金額と直接比較されます。 通貨換算はこのシナリオでは必要ありません。
- **シナリオ 3**: トランザクションは EUR で行われています。 EUR はしきい値金額が指定された通貨の 1 つでは*ない*ため、トランザクション通貨はまず EUR から USD に換算されます。USD で指定されたしきい値が比較に使用されます。

例 2

組織の基準通貨は GBP ですが、しきい値金額が GBP、JPY、および AUD であるルールを設定しました。以下のシナリオでは、各種のトランザクション中に通貨換算がどのように行われるかを説明します。

- **シナリオ 1**：トランザクションは GBP で行われています。トランザクションの通貨が組織の基準通貨と同じであるため、指定されたしきい値が通貨換算の必要なしで使用されます。
- **シナリオ 2**：トランザクションは JPY で行われています。JPY はしきい値金額が指定された通貨の 1 つであるため、トランザクション金額は JPY のしきい値金額と直接比較されます。 通貨換算はこのシナリオでは必要ありません。
- **シナリオ 3**：トランザクションは EUR で行われています。 EUR はしきい値金額が指定された通貨の 1 つではないため、トランザクション通貨はまず EUR から USD に、その後 USD から GBP に換算されます。GBP で指定されたしきい値が比較に使用されます。

通貨換算テーブル

すべてのサポートされている通貨の換算データは、ARRFCURRCONVRATES テーブルに保存されます。 ARRFCURRCONVRATES テーブルには、トランザクション通貨および組織の基準通貨が異なるときに［金額］フィールドの値を比較するために使用される通貨換算データが含まれます。 以下の表では、ARRFCURRCONVRATES テーブルの列について説明します。

列	説明	形式
VERSION	レート バージョン	1 の値の整数。
CURR_FROM	金額が換算されるトランザクション通貨用の 3 桁の ISO 通貨コード。	0 ～ 1000 の値の整数。
CURR_FROM_STR	金額が換算されるトランザクション通貨用の 3 文字の ISO 通貨コード。	3 文字の文字列。
CURR_TO	金額が換算される通貨用の 3 桁の ISO 通貨コード。	0 ～ 1000 の値の整数。
CURR_TO_STR	金額が換算される通貨用の 3 文字の ISO 通貨コード。	最大 3 文字の文字列。
CONV_RATE	CURR_FROM と CURR_TO または CURR_FROM_STR と CURR_TO_STR の換算レート。	実数。

列	説明	形式
DTCREATED	CONV_RATE 値が作成された日時。	
CURR_NAME_AND_NOTES	その他特記事項	

ARRFCURRCONVRATES テーブルを使用するためのガイドライン

ARRFCURRCONVRATES テーブルを使用する際には以下のガイドラインを適用します。

- デフォルトでは、ARRFCURRCONVRATES テーブルにデータはありません。RiskMinder を展開した後に、値をこのテーブルに入力する必要があります。
- 通貨換算レートは、指定された CURR_FROM または CURR_FROM_STR と CURR_TO または CURR_TO_STR の 1 つの単位の換算値として指定する必要があります。
- ARRFCURRCONVRATES テーブル内の換算レートには USD のみで CURR_TO または CURR_TO_STR をロードする必要があります。
- 特定の通貨換算が必要な場合、たとえば EUR から JPY では、金額はまず EUR から USD への換算レートを使用して EUR から USD に換算され、次に USD から JPY への換算レートの逆を適用して JPY での金額を取得します。

付録 E: RiskMinder エラーのトラブルシューティング

この付録では、RiskMinder の使用時に発生する可能性があるエラーを解決するのに役立つトラブルシューティング手順について説明します。 トラブルシューティング トピックは、RiskMinder の各コンポーネントに基づき以下のように分類されます。

- 管理コンソールのエラー（P. 469）
- ユーザ データ サービスのエラー（P. 473）

トラブルシューティング タスクを実行する前に、RiskMinder ログ ファイルでエラーがあるかどうかを確認してください。 デフォルトでは、ログ ファイルはすべて以下のディレクトリに保存されます。

Windows の場合：

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX ベースの場合

```
<install_location>/arcot/logs/
```

以下の表に、RiskMinder コンポーネントのデフォルト ログ ファイル名を示します。

RiskMinder コンポーネント	ファイル名	説明
RiskMinder サーバ	arcotriskfortstartup.log	このファイルには、すべての起動（ブート）アクションが記録されます。 RiskMinder サービスが起動しない場合、問題の原因を特定するためにこのファイルの情報が役立ちます。 サーバで処理されたすべてのリクエスト。
	arcotriskfort.log	このファイルには、スタートアップの後にサーバで処理されたすべてのリクエストが記録されます。
管理コンソール	arcotadmin.log	このファイルには、管理コンソールの操作が記録されます。

RiskMinder コンポーネント	ファイル名	説明
ユーザ データ サービス	arcotuds.log	このファイルには、ユーザ データ サービス（UDS）の操作が記録されます。

注: RiskMinder のログ ファイルの詳細については、「RiskMinder のログ」を参照してください。

管理コンソールのエラー

問題

MA（マスタ管理者）として管理コンソールにログインできません。 以下のメッセージが表示されます。
「この管理者アカウントはロックされています。」

原因

誤ったパスワードを使用して、許可されている認証試行数を超えて認証しようとした可能性があります。

解決方法:

以下のスクリプトを使用して、認証の試行回数（または*失敗回数*）を 0 にリセットします。

- MS SQL Server の場合
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN';
  ```
  実行
- Oracle の場合：
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN'; commit;
  ```
- MySQL の場合
  ```
  update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
  USERID='MASTERADMIN';
  COMMIT;
  ```

問題

管理コンソールに MA としてログインしようとすると、以下のエラー メッセージが表示されます。
データベース クエリの処理中に内部サーバ エラーが発生しました。 データベース管理者に連絡してください。

原因

この問題の考えられる原因として、データベース プール内のアクティブなデータソースがすべて使い尽くされたことが考えられます。

解決方法:

この問題を解決するには、以下の手順に従います。

1. データベース サーバがアクセス可能であることを確認します。
2. データベースまたはデータベース リスナを再起動します
3. 管理コンソールと RiskMinder サーバが同じデータベースを使用している場合
   a. RiskMinder サービスを再起動します。
   b. ブラウザを再起動します。

問題

MA のパスワードを忘れてしまいました。パスワードをリセットするには、どうしたらいいですか。

解決方法:

1. データベース タイプのスクリプトが格納されたフォルダを見つけます。 デフォルトの場所は以下のとおりです。
   - **MS SQL の場合：**

     Windows の場合：
     `<install_location>¥Arcot Systems¥dbscripts¥mssql`

     UNIX ベースの場合
     `<install_location>/arcot/dbscripts/mssql`
   - **Oracle の場合：**

     Windows の場合：
     `<install_location>¥Arcot Systems¥dbscripts¥oracle`

     UNIX ベースの場合
     `<install_location>/arcot/dbscripts/oracle`
   - **MySQL の場合**

     Windows の場合：
     `<install_location>¥Arcot Systems¥dbscripts¥mysql`

     UNIX ベースの場合
     `<install_location>/arcot/dbscripts/mysql`

2. データベース ベンダーのツールを使用して、arcot-masteradmin-password-reset-2.0.sqll スクリプトを実行します。

   以上の操作で MA のパスワードがデフォルト パスワード（**master1234**）にリセットされます。

上記の手順でうまくいかない場合は、MA のパスワードをリセットするために CA テクニカル サポートにお問い合わせください。

問題

［**サービスおよびサーバの設定**］タブから RiskMinder のページにアクセスできません。 以下のエラー メッセージが表示されます。
現在サーバに接続できません。 後で再試行してください。

解決方法:

以下の点を確認します。

1. RiskMinder サーバが実行されている。
2. MA （マスタ管理者）としてログインしている。
3. RiskMinder サーバ接続の詳細が正しいことを確認します。
   a. ［**サービスおよびサーバの設定**］タブに移動します。
   b. ［**RiskFort**］サブタブをアクティブにします。
   c. ［**接続詳細**］リンクをクリックし、［**RiskMinder 管理接続**］の RiskMinder の［**ホスト**］と［**ポート**］の情報が正しく設定されているかどうかを確認します。

問題

管理コンソールにログインしようとすると、以下のメッセージが表示されます。
エラー コード `500`： 内部サーバ エラー。

原因

- ブラウザのキャッシュがいっぱいになっている可能性があります。
- アプリケーション サーバのタイムアウト設定をリセットする必要がある場合があります。

解決方法:

以下の手順を実行します。

1. 管理コンソールを開こうとしているブラウザのキャッシュを空にして、再度試してみてください。
2. 依然としてメッセージが表示される場合は、別のブラウザを使用して管理コンソールを開いてみてください。

3. アプリケーション サーバ コンテナのタイムアウト設定を確認します。
4. 問題がまだ解決されない場合は、arcotadmin.log ファイルを開き、「Administration Console configured successfully.」という文字列を検索してください。
5. 「Administration Console configured successfully.」という文字列が見つからない場合は、ファイル内の最後の（エラーの説明）エントリを検索し、適切な処理を実行します。

問題

管理コンソールの操作を実行する間、以下のエラーが頻繁に発生します。
内部通信エラーが発生しました。 システム管理者に問い合わせるか、後で再試行してください。

原因

管理コンソールの操作を妨げるブラウザ アドオンが 1 つ以上ある可能性があります。

解決方法:

ブラウザの不要なアドオンを無効にし、再度操作を実行します。

問題

UDS は起動していますが、管理コンソールが正しく展開されませんでした。java.lang.ClassNotFoundException 例外が arcotadmin.log ファイルに記録されています。

原因

この問題は、WAR または EAR が正しく展開されなかったか、破損した場合にのみ発生します。

解決方法:

この問題を解決するには、以下の手順に従います。

1. アプリケーション サーバの作業ディレクトリをクリーンアップします。

   たとえば、Apache Tomcat では、このディレクトリは work です。
2. 再度 WAR または EAR ファイルを展開します。

ユーザ データ サービスのエラー

問題

管理コンソールを使用して組織を作成し、アクティブにしましたが、RiskMinder の設定を行おうとすると、以下のエラーが表示されます。
組織が見つかりません

原因

考えられる原因は以下のとおりです。

- UDS を起動する*前*に、RiskMinder サーバ サービスを開始しました。
- 作成した新しい組織に対して操作を実行しようとしていますが、RiskMinder サーバのキャッシュがリフレッシュされていません。

解決方法:

以下の手順を実行します。

1. UDS の前に RiskMinder サーバを起動した場合、RiskMinder サーバのログにサーバが UDS と接続できなかったことが示されます。常にアプリケーション サーバ (UDS) を最初に起動し、次に RiskMinder サーバ サービスを開始します。
2. RiskMinder サーバのキャッシュをリフレッシュします。

   管理コンソールを使用して新しい組織を作成したときには、*必ず* RiskMinder サーバのキャッシュを再起動してください。

注: 詳細については、「組織の作成とアクティブ化」を参照してください。

問題

ユーザと管理者を検索しているときに、以下のエラー メッセージが表示されます。
ユーザ データ サービスとの通信中に内部サーバ エラーが発生しました。 管理者に連絡してください。

原因

検索対象のユーザの数が多すぎて、指定した組織で検索できない可能性があります。 その結果、操作が指定されたタイムアウト内で完了しませんでした。

解決方法:

以下の手順を実行します。

1. MA として管理コンソールにログインします。
2. ［**サービスおよびサーバの設定**］-［**管理コンソール**］-［**UDS 接続設定**］ページに移動します。
3. 接続設定ページで、以下の操作を実行します。
   a. ［**接続タイムアウト**］フィールドの値を大きくします。
   b. ［**読み取りタイムアウト**］フィールドの値を大きくします。
4. 上記の手順でうまくいかない場合は、検索結果を絞り込むために検索条件を変更します。

付録 F: アクセシビリティ機能

この付録では、CA Risk Authentication インストーラによってインストールされるすべてのファイルの場所について説明します。 以下の情報が含まれます。

- リスク評価 Java SDK ファイル（P. 475）
- CA Risk Authentication の WSDL ファイル（P. 486）

リスク評価 Java SDK ファイル

以下の表に、CA Risk Authentication インストーラによって作成されるメインディレクトリ、ファイル、および JAR を示します。 また、このガイドの中で言及している特定のサブディレクトリとファイルについても説明します。

この表で説明するファイルとディレクトリに加え、インストール ディレクトリには CA Risk Authenticationkey という名前の空のファイルもあります。 このファイルは、以前にインストールされた CA 製品を検出するためにインストーラによって使用されます。 このファイルを削除した場合、以前にインストールされた CA 製品が検出されず、新規インストールが任意の場所で実行されてしまいます。 その結果、複数の Arcot 製品およびコンポーネントに対して同じインストール先ディレクトリを確保できず、製品（またはコンポーネント）が想定どおりに動作しなくなる可能性があります。 このファイルは、パッチおよびアップグレードに影響を及ぼしません。

ディレクトリ	使用元	ファイル名と説明

ディレクトリ	使用元	ファイル名と説明
<*install_location*>¥Arcot Systems¥**bin**¥ **注**: これらのツールの詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。	■ CA Risk Authentication サーバ ■ ケース管理キュー サーバ	CA Risk Authentication サーバによって使用される以下の実行可能ファイルが含まれます。 ■ arrfcasemgmtserver.exe （ケース管理キュー サーバをリフレッシュおよび正常にシャットダウンするためのツール） ■ arrfclient.exe （CA Risk Authentication サーバをリフレッシュおよび正常にシャットダウンするためのツール） ■ arrfserver.exe（サーバ管理ポートおよびその他のサーバ関連操作を設定するためのツール） ■ arrfupload.exe （Quova データを CA Risk Authentication データベースにアップロードするためのツール） ■ arrfversion.exe（CA によって提供されるライブラリ ファイルのバージョンを確認するためのツール） CA Risk Authentication サーバによって使用される以下のライブラリ ファイルも含まれます。 ■ aradminprotocol.dll ■ aradminwsprotocol.dll ■ arrfuds.dll ■ arrfudswrapper.dll ■ arRiskEngine.dll ■ NameValueXref.dll ■ srvmgrwsprotocol.dll ■ transwsprotocol.dll

ディレクトリ	使用元	ファイル名と説明
<*install_location*>¥Arcot Systems¥**conf**¥ **注**: このディレクトリにある設定ファイルの詳細については、「*設定ファイルおよびオプション*」を参照してください。	■ 管理コンソール	管理コンソールによって使用される以下の設定ファイルが含まれます。 ■ adminserver.ini（管理コンソール ログ設定の読み取りに使用） ■ arcotcommon.ini （設定された場合、CA Risk Authentication データベース、CA Risk Authentication インスタンス、およびハードウェア セキュリティ モジュール（HSM）への接続に使用）
	■ CA Risk Authentication サーバ	CA Risk Authentication サーバおよびその他の CA Risk Authentication コンポーネントによって使用される以下の設定ファイルが含まれます。 ■ arcotcommon.ini （設定された場合、CA Risk Authentication データベース、CA Risk Authentication インスタンス、およびハードウェア セキュリティ モジュール（HSM）への接続に使用） ■ riskfortdataupload.ini（Quova データを CA Risk Authentication データベースにアップロードするために使用） ■ securestore.enc（CA Risk Authentication データベースへの接続に必要な暗号化された情報の格納に使用）
	■ UDS	UDS が UDS ログ設定の読み取りに使用する udsserver.ini ファイルが含まれます。
	■ UDS ■ 管理コンソール	resourcebundles ディレクトリには、管理コンソールおよび UDS によってスローされた共通のエラー用のプロパティ ファイルが含まれます。

ディレクトリ	使用元	ファイル名と説明
	■ ユーザ行動プロファイリング	■ arcotcommon.ini （設定された場合、CA Risk Authentication データベース、CA Risk Authentication インスタンス、およびハードウェア セキュリティ モジュール（HSM）への接続に使用） ■ ubp_logging.xml（UBP ログ設定の読み取りのために UBP が使用） ■ securestore.enc（CA Risk Authentication データベースへの接続に必要な暗号化された情報の格納に使用）
<*install_location*>¥Arcot Systems¥**dbscripts¥**	■ 管理コンソール ■ CA Risk Authentication サーバ ■ UDS ■ ユーザ行動プロファイリング	インストール中に指定したデータベース タイプの CA Risk Authentication スキーマを作成および削除するためのデータベース スクリプトが含まれます。
<*install_location*>¥Arcot Systems¥docs¥**riskfort¥**	■ 管理コンソール ■ CA Risk Authentication サーバ	以下の圧縮された WSDLdoc ドキュメントが含まれています。 ■ CA Risk Authentication-8.0-AdminWeb Service-wsdldocs.zip（管理 Web サービス用の WSDLDocs）

ディレクトリ	使用元	ファイル名と説明
	■ CA Risk Authentication サーバ	コールアウトを作成するための以下の圧縮ファイルと XSD、およびリスク管理 SDK 用の Javadoc と WSDLdoc が含まれます。 ■ CA Risk Authentication-8.0-CallOutInterface-xsds.zip （コールアウトの作成に必要な、評価とスコアリングのリクエスト ファイルとレスポンス ファイル） ■ CA Risk Authentication-8.0-risk-evaluation-sdk-javadocs.zip ■ CA Risk Authentication-8.0-risk-evaluation-wsdl docs.zip
<*install_location*>¥Arcot Systems¥docs¥**uds¥**	■ UDS	以下の圧縮された WSDLdoc ドキュメントが含まれています。 ■ arcot-uds-2_0-wsdl-docs.zip （UDS Web サービス用の WSDLDocs）
<*install_location*>¥Arcot Systems¥**java¥lib¥**	■ 管理コンソール	**sdk** という名前の空のディレクトリ、および管理コンソール フレームワークおよび UDS で必要な以下の WAR および JAR ファイルが含まれます。 ■ adminframework.jar ■ adminframework.war ■ arcot-common.jar ■ arcot-crypto-util.jar ■ arcot-euds.jar ■ bcprov-jdk15-146.jar ■ udsframework.war
<*install_location*>¥Arcot Systems¥**java¥webapps¥**	■ 管理コンソール	管理コンソールによって必要とされる以下の WAR ファイルが含まれます。 ■ arcotadmin.war（管理コンソールの展開に必要な WAR ファイル）

ディレクトリ	使用元	ファイル名と説明
	■ UDS	UDS の以下の展開に必要な arcotuds.war ファイルが含まれます。 ■ LDAP 接続 ■ UDS Web サービスへのアクセス ■ Web サービス用の認証および許可
	■ UBP	ユーザがユーザ行動プロファイリング機能にアクセスするために必要な ca-userprofiling-2.0-application.war ファイルが含まれます。
<*install_location*>¥Arcot Systems¥**logs**¥ **注**: これらのログ ファイルの詳細については、「*CA Risk Authentication 管理ガイド*」の「CA Risk Authentication のログ」を参照してください。		管理コンソール、ケース管理、CA Risk Authentication、および UDS によって使用されるログ ファイルが含まれます。 利用可能な場合、より古いログを格納するために **backup** サブディレクトリを使用できます。
	■ 管理コンソール	■ arcotadmin.log
	■ CA Risk Authentication サーバ	■ arcotriskfort.log ■ arcotriskfortstartup.log
	■ ケース管理キュー サーバ	■ arcotriskfortcasemgmtserver. ログ ■ arcotriskfortcasemgmtstartup.log
	■ UDS	■ arcotuds.log **注**: LDAP 接続用に UDS WAR ファイル（arcotuds.war）を展開した場合のみ、このログが表示されます。
	■ UBP	■ ubp_logfile.log **注**: UBP war ファイルを展開した後にのみ、このログが表示されます。

ディレクトリ	使用元	ファイル名と説明
<*install_location*>¥Arcot Systems¥**native**¥	■ 管理コンソール ■ UDS ■ UBP	32 ビットまたは 64 ビット OS プラットフォーム（RHEL、Solaris SPARC、または Microsoft Windows）用の securestore.enc の内容を読み取るために使用される ArcotAccessKeyProvider.dll（該当するサブディレクトリ内）が含まれます。
<*install_location*>¥Arcot Systems¥**odbc32v70wf**¥	■ CA Risk Authentication サーバ	CA Risk Authentication によってサポートされるすべてのデータベース用の、CA Risk Authentication にブランド設定された DataDirect ODBC ライブラリが含まれます。
<*install_location*>¥Arcot Systems¥**plugins¥rules**¥	■ CA Risk Authentication サーバ	既定のすべての CA Risk Authentication ルールとスコアリングをサポートするすべての DLL （ライブラリ バイナリ）ファイルが含まれます。
<*install_location*>¥Arcot Systems¥**resourcepacks**¥	■ 管理コンソール ■ UDS	必要な管理コンソールおよび製品パックバンドルが含まれます。 ■ bundle_adminconsole.zip ■ bundle_riskfort.zip また、**i18n** サブディレクトリが含まれています。これは、国際化に対して必要なファイルを格納する場所です。 **注**: CA Risk Authentication のローカライズの詳細については、「*ローカライゼーションの準備*」を参照してください。
<*install_location*>¥Arcot Systems¥**samples¥java**¥	■ CA Risk Authentication サーバ ■ CA Risk Authentication リスク管理 SDK	**java** サブディレクトリには、以下のためのサンプル WAR ファイルが含まれます。 ■ riskfort-3.1.01-sample-application.war：CA Risk Authentication サンプル アプリケーションの展開に使用します。 ■ riskfort-3.1.01-sample-callouts.war： CA Risk Authentication サンプル コールアウトの展開に使用します。

ディレクトリ	使用元	ファイル名と説明
<*install_location*>¥Arcot Systems¥**sdk**¥	■ CA Risk Authentication リスク管理 SDK	CA Risk Authentication によってサポートされる SDK と依存ファイルの **c**、**devicedna**、および **java** 言語バージョンが含まれます。 **devicedna** サブディレクトリには、これらの SDK および MFP と DeviceDNA のモジュールによって使用される付属の JavaScript および Flash ファイルが含まれます。
<*install_location*>¥Arcot Systems¥**tools**¥	■ 管理コンソール	**共通**のサブディレクトリには、以下のサブディレクトリが含まれます。 ■ **arreporttool** サブディレクトリには、レポートのエクスポート（またはダウンロード）を可能にするレポート コマンド ライン ユーティリティが含まれます。 ■ **bundlemanager** サブディレクトリには管理コンソール リソース パックに必要なファイルが含まれています。 ■ **uds-monitor** サブディレクトリには、UDS の状態を確認するスクリプトが含まれます。
<*install_location*>¥Arcot Systems¥**tools**¥**<platform>**¥ <*platform*> には、linux、solsparc、および win を指定できます。	■ 管理コンソール ■ ユーザ データ サービス（UDS）	OS プラットフォーム（RHEL、Solaris SPARC、または Microsoft Windows）用の DBUtil.exe ツールが含まれます。 このツールは、securestore.enc の編集に必要です。ここには、CA Risk Authentication データベースに接続するために CA Risk Authentication サーバで必要な暗号化された情報が格納されます。

ディレクトリ	使用元	ファイル名と説明
<*install_location*>¥Arcot Systems¥ **Uninstall_Arcot RiskFort¥**	■ CA Risk Authentication サーバ	CA Risk Authentication のアンインストールに必要なファイルが含まれます。 また、以下のファイルも含まれます。 ■ **jre** サブディレクトリには、Java Runtime Environment（JRE）のサポートに必要なすべてのファイルが含まれます。 – Java 仮想マシン – ランタイム クラス ライブラリ – Java アプリケーション ランチャ ■ **resource** ディレクトリには、CA Risk Authentication のアンインストールのためにインストーラによって必要とされるすべてのファイルが含まれます。
<*install_location*>¥Arcot Systems ¥**wsdls¥**	■ CA Risk Authentication サーバ	管理コンソール（**admin** サブディレクトリ）、CA Risk Authentication （**CA Risk Authentication** サブディレクトリ）、および UDS （uds サブディレクトリ）によって必要とされる WSDL ファイルが含まれます。

以下の表に、リスク評価 Java SDK で使用されるファイルのディレクトリの場所を示します。

ディレクトリ	ファイル説明
<*install_location*>¥Arcot Systems¥**docs¥riskfort¥**	CA Risk Authentication-8.0-risk-evaluation-sdk-javadocs.zip ファイル（リスク評価 SDK 用の Javadocs が含まれます）。

ディレクトリ	ファイル説明
<*install_location*>¥Arcot Systems¥**samples¥java¥**	以下のファイルが含まれます。 ■ CA Risk Authentication-8.0-sample-application.war （サンプル アプリケーションの展開用） ■ CA Risk Authentication-8.0-sample-callouts.war （製品に付属するサンプル コールアウト サーバの展開用） **注**: このサンプル コールアウトの展開および使用方法の詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。
<*install_location*>¥Arcot Systems¥**sdk¥**	CA Risk Authentication によってサポートされる SDK と依存ファイルが含まれます。
<*install_location*>¥Arcot Systems¥**sdk¥c¥**	C SDK に必要なライブラリとインクルード ファイルが含まれます。
<*install_location*>¥Arcot Systems¥**sdk¥devicedna¥**	以下のファイルが含まれます。 ■ riskminder-client.js : クライアント側で DeviceDNA 情報を収集するために必要になります。 ■ riskminder-client.swf : 以前のリリースから、このリリースがサポートするブラウザ（HTTP）Cookie ストアに Flash ベースの Cookie を移行するのに必要になります。
<*install_location*>¥Arcot Systems¥**sdk¥flash¥**	以下のファイルが含まれます。 ■ arcot-devicedna.swf : デバイス ID Flash オブジェクトを管理します。 ■ crossdomain.txt : Flash オブジェクトにアクセスできるドメインのリストを指定します。
<*install_location*>¥Arcot Systems¥**sdk¥java¥**	■ **lib** サブディレクトリには、製品で使用される、CA 提供の JAR ファイルとサードパーティ JAR ファイルが含まれます。 **注**: これらのサードパーティ JAR のライセンス情報については、パッケージでサードパーティ ソフトウェア ライセンス ドキュメントを参照してください。 ■ **properties** ディレクトリには、CA Risk Authentication の設定に必要なプロパティ ファイルが含まれます。

ディレクトリ	ファイル説明
<*install_location*>¥Arcot Systems¥**sdk¥java¥lib¥arcot¥**	リスク評価 Java SDK によって使用される以下の JAR ファイルが含まれます。 ■ arcot_core.jar ■ arcot-pool.jar ■ arcot-riskfort-evaluaterisk.jar ■ arcot-riskfort-issuance.jar ■ arcot-riskfort-mfp.jar **注**: 発行 API は、このリリースで廃止されました。 ただし、CA Risk Authentication-issuance.jar では、以前のリリースとの下位互換性が保証されています。
<*install_location*>¥Arcot Systems¥**sdk¥java¥lib¥external¥**	リスク評価 Java SDK に必要なサードパーティ JAR ファイルが含まれています。 ■ bcprov-jdk15-146.jar ■ commons-lang-2.0.jar ■ commons-pool-1.5.5.jar
<*install_location*>¥Arcot Systems¥**sdk¥java¥properties¥**	以下のファイルが含まれます。 ■ log4j.properties.risk-evaluation ■ riskfort.risk-evaluation.properties

CA Risk Authentication の WSDL ファイル

以下の表に、リスク評価 WSDL で使用されるファイルのディレクトリの場所を示します。

ディレクトリ	ファイル説明
<*install_location*>¥Arcot Systems¥**docs¥riskfort¥**	CA Risk Authentication リスク評価および管理コンソール用の圧縮された WSDLdoc が含まれます。 CA Risk Authentication-8.0-AdminWebService-wsdldocs.zip CA Risk Authentication-8.0-risk-evaluation-wsdldocs.zip

ディレクトリ	ファイル説明
<*install_location*>¥Arcot Systems¥**docs¥uds¥**	UDS で必要な arcot-uds-2_0-wsdl-docs.zip ファイルが含まれます。 この WSDL は、UDS Web サービス、およびこのサービスへのアクセス方法について説明しています。
<*install_location*>¥Arcot Systems¥**wsdls¥admin¥**	管理コンソールで必要な CA Risk AuthenticationAdminWebService.wsdl ファイルが含まれます。 この WSDL は、CA Risk Authentication 管理 Web サービス、およびこのサービスへのアクセス方法について説明しています。 また、例外ユーザを追加するときにも使用できます。
<*install_location*>¥Arcot Systems¥**wsdls¥riskfort¥**	CA Risk Authentication で必要な以下のファイルが含まれます。 ■ CA Risk AuthenticationEvaluateRiskService.wsdl WSDLdoc は、リスク評価 Web サービス、およびこのサービスへのアクセス方法について説明しています。
<*install_location*>¥Arcot Systems¥**wsdls¥uds¥**	UDS で必要な WSDL および XML スキーマ ファイルが含まれます。 この WSDL は、UDS Web サービス、およびこのサービスへのアクセス方法について説明しています。 ■ ArcotConfigManagementSvc.wsdl （ユーザ アカウント タイプの作成と管理のための WSDL） ■ ArcotOrganizationManagementSvc.wsdl（組織の作成と管理のための WSDL） ■ ArcotUserManagementSvc.wsdl （ユーザおよびユーザ アカウントの作成と管理のための WSDL） ■ ArcotUserSchema.xsd （UDS Web サービスで動作するためにコードで使用できる参考ライブラリとして機能する XML スキーマ定義）

付録 G: INI ファイルの詳細

CA Risk Authentication の設定用に使用されるプレーンテキストの INI ファイル。 以下のファイルが含まれます。

- adminserver.ini（P. 490）
- arcotcommon.ini（P. 493）
- riskfortdataupload.ini（P. 504）
- udsserver.ini（P. 506）

すべての CA Risk Authentication 設定ファイルは、以下のデフォルトの場所にあります。

`<install_location>¥Arcot Systems¥conf¥`

adminserver.ini

adminserver.ini ファイルには、管理コンソールのログ情報を設定するパラメータが含まれています。

ログ設定

以下の表に、管理コンソールによって使用されるログ ファイル情報を示します。 このファイルで設定できる共通のログ レベル値は次のとおりです。

- FATAL
- 注意
- INFO
- DEBUG

注: ログ レベルの詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

パラメータ	デフォルト値	Description
log4j.rootCategory	ERROR、roothandle **重要**: roothandle は管理コンソール ログ ハンドルの名前で、必ず指定する必要があります。	ロガー階層の一番上に存在するルート ロガー。 値が指定されていない場合、子ロガーはすべてこの値を継承します。
log4j.logger.com.arcot.euds	INFO	ユーザ データ ソース（UDS）情報を書き込むためのログ レベル。
log4j.logger.com.arcot.admin	INFO	管理コンソールのログを書き込むために使用する必要のあるログ レベル。
log4j.logger.com.arcot.admin.framework	INFO	管理コンソール フレームワークのログを書き込むために使用する必要のあるログ レベル。
log4j.logger.com.arcot.adminconsole	INFO	管理コンソールのログを書き込むために使用する必要のあるログ レベル。

パラメータ	デフォルト値	Description
log4j.logger.com.arcot.common.cache	INFO	キャッシュ関連情報を書き込むためのログ レベル。
log4j.logger.com.arcot.common.crypto	INFO	HSM に関連付けられた情報を書き込むためのログ レベル。
log4j.logger.com.arcot.crypto.impl.SecureStoreUtil	INFO	ハードウェア ベースまたはソフトウェア ベースの HSM を使用している場合に、ログを書き込むために使用する必要のあるログ レベル。
log4j.logger.com.arcot.common.database	INFO	データベース情報を書き込むために使用する必要があるログ レベル。
log4j.logger.com.arcot.common.ldap	INFO	LDAP 情報を書き込むために使用する必要があるログ レベル。
log4j.appender.roothandle	org.apache.log4j.RollingFileAppender	ロガー階層の一番上に存在するルート ロガー。 値が指定されていない場合、子ロガーはすべてこの値を継承します。
log4j.appender.roothandle.Encoding	UTF-8	ログ ファイルにエントリを書き込むときに使用するエンコーディング。
log4j.appender.roothandle.File	${arcot.home}/logs/**arcotadmin.log**	管理コンソール ログのファイル名と、ログが作成される場所。 管理コンソールのデフォルトのログ ファイル名は arcotadmin.log で、以下の場所に作成されます。 <*install_location*>¥Arcot Systems¥**logs¥**
log4j.appender.roothandle.MaxFileSize	10 MB	ログ ファイルについて許可される最大サイズ。

パラメータ	デフォルト値	Description
log4j.appender. roothandle. MaxBackupIndex	100	作成できるバックアップ ファイルの最大数。 バックアップ ファイルの数がこの値に達すると、アプリケーションは先頭のログ ファイルから上書きを開始します。
log4j.appender. roothandle.layout	org.apache.log4j. PatternLayout	ConversionPattern で指定されている出力形式。
log4j.appender. roothandle.layout. ConversionPattern	%d{yyyy-MM-dd HH:mm:ss,SSS z} : [%t] : %-5p : %-5c{3} : %m%n	管理コンソール ログ ファイル エントリが書き込まれる形式 ■ タイム スタンプ（%d{yyyy-MM-dd HH:mm:ss,SSS z} :） ■ スレッド ID （[%t] :） ■ ログ レベル（または重大度）（%-5p :） ■ ロガー クラス（%-5c{3} :） ■ メッセージ（%m%n） **注**: このパターンは C 言語の printf 関数に似ています。

arcotcommon.ini

arcotcommon.ini ファイルには、CA Risk Authentication サーバおよびその他のコンポーネント（管理コンソール、ユーザ データ サービス、およびユーザ行動プロファイリング）のデータベース設定用とインスタンス設定用のパラメータが含まれます。 通常は、このファイルの以下のセクションを編集する必要があります。

- データベース設定
- HSM 暗号化設定
- インスタンス設定

また、arcotcommon.ini を使用して、CA Risk Authentication サーバおよびケース管理キュー サーバに対するデフォルトのスタートアップ ログ設定を変更できます。 詳細については、「*サーバ起動ログ パラメータの変更*」を参照してください。

データベース設定

arcotcommon.ini のデータベース設定では、サーバの接続先となるデータベースと、フェールオーバに使用するバックアップ データベースを指定できます。 サーバとデータベース間で利用できるデータベース通信リソースを設定することもできます。

注: データベース設定に関する注意事項と推奨事項については、「*インストールの準備*」の章を参照してください。

arcotcommon.ini ファイルでは、データベース設定に関連する以下のセクションを編集する必要があります。

- [arcot/db/dbconfig]
- [arcot/db/primarydb]
- [arcot/db/backupdb]

[arcot/db/dbconfig]

このセクションでは、データベース タイプと、データベース タイプに関する一般情報を指定できます。 以下の表に、[arcot/db/dbconfig] セクションのデータベース設定パラメータを示します。

パラメータ	デフォルト	Description

パラメータ	デフォルト	Description
DbType	--	すべてのデータベース接続に利用可能なデータベースのタイプ。 サポートされている値は以下のとおりです。 ■ oracle ■ mssqlserver ■ mysql
Driver	--	JDBC ドライバ ベンダーによって提供されるデータベース ドライバ クラスの完全修飾名。 **注**: 正しいドライバ名を知るには、JDBC ベンダーのマニュアルを参照してください。 例： **– Oracle：** oracle.jdbc.driver.OracleDriver **– Microsoft SQL Server：** com.microsoft.sqlserver.jdbc.SQLServerDriver - **MySQL：** com.mysql.jdbc.Driver
MinConnections	4	サーバとデータベースの間で最初に作成する接続の最小数。
MaxConnections	64	サーバとデータベースの間で作成する接続の最大数。 **注**: データベースで許可される接続数には制限があり、その制限によって MaxConnections 数の接続を作成することが制限される場合があります。 受信接続数に対する制限の詳細については、データベース ドライバのドキュメントを参照してください。
IncConnections	2	CA Risk Authentication コンポーネントとデータベースの間で新しい接続が必要なときに作成される接続の数。
MaxIdleConnections	64	サーバが維持できるアイドル状態のデータベース接続の最大数。
MaxWaitTimeFor 接続	30000	接続が使用できるようになるまで（使用できる接続がないとき）サーバが待機する必要のあるタイムアウト前の最大時間（ミリ秒単位）。

パラメータ	デフォルト	Description
AutoRevert	1	フェールオーバが発生した後、システムがプライマリ データベースに接続を試みるかどうか。 バックアップ データベースを設定している場合、およびフェールオーバ発生後にサーバがプライマリ データベースに接続するようにする場合は、AutoRevert=1 を設定します。
MaxTries	3	サーバがデータベースへの接続を中止する前の接続試行回数。
ConnRetrySleep Time	100	データベースへの接続試行間の遅延時間（ミリ秒単位）。
MonitorSleepTime	50	すべてのデータベースに対するハートビート チェック間に監視スレッドがスリープする時間（秒単位）。
Profiling	0	データベース メッセージがログ記録されているかどうか。 データベース メッセージのログ記録を有効にする場合は、値を 1 に設定します。
EnableBrandLicensing	1	ブランド設定された ODBC ドライバが使用されているかどうか。
BrandLicenseFile	IVWF.LIC	ブランド設定された ODBC ドライバを使用するときのライセンス ファイル名。 EnableBrandLicensing の値が 1 の場合に、このパラメータが必要です。それ以外の場合は無視されます。 **重要**: この値が存在する場合は編集 *しないでください*。
MaxTransactionRetries	3	事前定義されたエラー状態についてデータベース インスタンスでトランザクションを再試行する最大回数。
TransactionRetrySleep Time	10	2 つの連続するトランザクション再試行間の間隔（ミリ秒単位）。

[arcot/db/primarydb]

このセクションでは、CA Risk Authentication サーバの接続先となるプライマリ データベースを指定できます。 プライマリ データベースを 2 つ以上設定する場合は、以下のパラメータで必要な数値 *N* を指定します。

- Datasource.*N*
- AppServerConnectionPoolName.*N*
- URL.*N*
- Username.*N*
- TrustStorePath.*N*
- KeyStorePath.*N*
- HostNameInCertificate.*N*

以下の表に、[arcot/db/primarydb] セクションのデータベース設定パラメータを示します。

パラメータ	デフォルト	Description
Datasource.*N*	デフォルト値なし	サーバ データをホストするプライマリ データベースを示す ODBC システム データ ソース名（DSN）の名前。

パラメータ	デフォルト	Description
AppServerConnectionPoolName.*N*	デフォルト値なし	アプリケーション サーバのデータベース接続プーリング機能を使用している場合、接続プール オブジェクトの検索に使用する JNDI 名。 この JNDI 名によるプールは、含まれるアプリケーション サーバ内に作成する必要があります。また、Web アプリケーションに対して、接続プールを使用するための十分なアクセス権限を与える必要があります。 JNDI 名を **Apache Tomcat** 内で設定する場合は、完全修飾 JNDI 名を使用します。 例： ■ AppServerConnectionPoolName.1=java:comp/env/SampleDS **Apache 以外のアプリケーション サーバ**については、JNDI 名だけ指定します。 例： ■ AppServerConnectionPoolName.1=SampleDS 詳細については、付録「データベース接続プールのためのアプリケーション サーバの設定」を参照してください。 アプリケーション サーバ接続プールが*必要でない*場合は、この設定を空のままにします。
URL.*N*	デフォルト値なし	JDBC データ ソースの名前。 以下に例を示します。 ■ **Oracle** -> jdbc:oracle:thin:<*server*>:<*database_port*>:<*sid*> ■ **Microsoft SQLServer** -> jdbc:sqlserver://<*server*>:<*database_port*>;databaseName=<*databasename*>;selectMethod=cursor ■ **MySQLServer** -> jdbc:mysql://<*server*>:<*database_port*>/<*database*>
Username.*N*	デフォルト値なし	データベース アクセスのためにサーバによって使用されるユーザ ID。

パラメータ	デフォルト	Description
TrustStorePath.*N* **注**: CA Risk Authentication とデータベースの間で SSL を設定する場合にのみ使用します。	デフォルト値なし	Datasource.*N* に対応する SSL 証明書トラスト ストア パス。 このパス（ファイル名を含む）は証明書のトラスト ストア ファイルを参照します。このファイルには、クライアントが信頼する証明書のリストが記述されています。 **重要**: TrustStorePath.*N* に対応するパスワードは、キーとしての TrustStorePath.*N* の値と共に securestore.enc 内に安全に格納する必要があります。 この操作は DBUtil ユーティリティを使って行います。 **注**: DBUtil の詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。
KeyStorePath.*N*		**注**: この属性は MySQL にのみ使用されます。 CA Risk Authentication と MySQL データベースの間で一方向 SSL を設定する場合、これは値を指定する必要があるパラメータの 1 つです。このパラメータは、Datasource.*N* に対応する SSL 証明書キーストア パスを保持します。 証明書キーストア ファイルを参照するパス（ファイル名を含む）になります。KeyStorePath.*N* に対応するパスワードは、キーとしての KeyStorePath.*N* の値と共に securestore.enc 内に安全に格納する必要があります。
HostNameInCertificate.*N* **注**: CA Risk Authentication とデータベースの間で SSL を設定する場合にのみ使用します。	デフォルト値なし	トラスト ストア内の Datasource.*N* SSL 証明書に含まれるサブジェクト識別名（DN）の共通名（CN）の値。

[arcot/db/backupdb]

このセクション [arcot/db/backupdb] では、フェールオーバに使用するバックアップ データベースを指定できます。 複数のフェールオーバ データベースを設定する場合は、以下のパラメータで必要な数値 *N* を指定します。

- Datasource.*N*
- AppServerConnectionPoolName.*N*
- URL.*N*
- Username.*N*
- TrustStorePath.*N*
- KeyStorePath.*N*
- HostNameInCertificate.*N*

HSM 暗号化設定

arcotcommon.ini ファイルを使用すると、ハードウェア セキュリティ モジュール（HSM）の設定を指定できます。 CA Risk Authentication に対して使用される秘密キーを暗号化形式で格納できます。 以下の HSM がサポートされています。

- Chrysalis-ITS Luna SA
- Thales nFast （nCipher netHSM）

以下の表に、[arcot/crypto/device] セクションで指定される、安全なストレージ用の共通設定を示します。

パラメータ	デフォルト	Description

パラメータ	デフォルト	Description
HSMDevice	S/W	データベースに格納されているキー、または HSM に格納されているキーの 1 つを使用して、CA Risk Authentication 情報を暗号化する必要があるかどうかを設定するモード。 サポートされている値は以下のとおりです。 ■ S/W： データベースに格納されているキー ラベルを使用してデータが暗号化されることを示します。 ■ chrysalis： データを暗号化するために Chrysalis （Luna） HSM が使用されることを示します。 ■ nfast： データを暗号化するために nFast （nCipher netHSM）が使用されることを示します。

以下の表に、[crypto/pkcs11modules/chrysalis] セクションで指定される、Chrysalis-ITS Luna SA 用の設定パラメータを示します。

パラメータ	デフォルト	Description
sharedLibrary	<*location/to/cryptoki*.dll>	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 Chrysalis （Luna）のデフォルト値は、以下のとおりです。 C:¥Program Files¥LunaSA¥cryptoki.dll
storageSlot	0	暗号化キー（非対称および対称）が存在する HSM スロット。
accelSlot	0	CA で内部的に使用されるスロット。
sessionCount	20	HSM デバイスで確立できるセッションの最大数。

以下の表に、[crypto/pkcs11modules/nfast] セクションで指定される、nCipher netHSM 用の設定パラメータを示します。

パラメータ	デフォルト	Description
sharedLibrary	<*location/to/ccknfast*.dll>	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 nFast（nCipher netHSM）のデフォルト値は、以下のとおりです。 C:¥nfast¥bin¥cknfast.dll
storageSlot	1	暗号化キー（非対称および対称）が存在する HSM スロット。
accelSlot	0	CA で内部的に使用されるスロット。
sessionCount	200	HSM デバイスで確立できるセッションの最大数。

インスタンス設定

サーバ ファームでは、サーバのすべてのインスタンスに一意の識別子を設定することをお勧めします。 CA Risk Authentication は、サーバのすべてのインスタンスを設定および識別するためのパラメータをサポートします。 このセクションでは、一意のインスタンスのためのシステム全体に関係する設定を行うことができます。以下の表に、[arcot/system] セクションのインスタンス設定パラメータを示します。

パラメータ	デフォルト	Description
InstanceId	1	任意のサーバ インスタンスの識別に使用できるパラメータ。 **重要**: サーバのすべてのインスタンスに対して一意の値を指定する必要があります。 サーバ インスタンスはトランザクション レポートにも表示されるので、サーバ インスタンスをトランザクションまでトレースすることが容易になります。

サーバ起動ログ パラメータの変更

CA Risk Authentication サーバまたはケース管理キュー サーバの起動時に表示されるログ パラメータを変更する場合は、次の手順に従ってください:。

1. ARCOT_HOME 内の conf ディレクトリに移動します。
2. テキスト エディタで arcotcommon.ini を開きます。
3. （*CA Risk Authentication サーバの場合*）以下のセクションをファイルの最後に追加します。

```
[arcot/riskfort/startup]
LogFile=
LogFileSize=10485760
BackupLogFileDir=
LogLevel=
LogTimeGMT=0
```

以下の表に、これらのパラメータの説明を示します。

パラメータ	デフォルト	Description
LogFile		ログ ファイルのデフォルト ディレクトリのファイル パスとログ ファイルの名前。 **注**: このパスは ARCOT_HOME （<*install_location*>¥Arcot Systems¥）からの相対パスです。
LogFileSize	10485760	ログ ファイルが記録できる最大**バイト**数。 ログ ファイルがこのサイズに達すると、新しいファイルが生成され、古いファイルは BackupLogFileDir で指定した場所に移動されます。
BackupLogFileDir		現在のファイルが LogFileSize のバイト数を超えた後で、バックアップ ログ ファイルが保持されるディレクトリの場所。 **注**: このパスは ARCOT_HOME （<*install_location*>¥Arcot Systems¥）からの相対パスです。

パラメータ	デフォルト	Description
LogLevel		サーバのデフォルトのログ記録レベル（上書きが指定されていない場合）。 以下の値を指定できます。 ■ 0： FATAL ■ 1： WARNING ■ 2： INFO ■ 3： DETAIL
LogTimeGMT	0	ログ ファイル内のタイム スタンプのタイム ゾーンを示すパラメータ。 以下の値を指定できます。 ■ 0： ローカル時間 ■ 1： GMT

1. （*ケース管理キュー サーバの場合*）以下のセクションをファイルの最後に追加します。

```
[arcot/riskfortcasemgmtserver/startup]
LogFile=
LogFileSize=10485760
BackupLogFileDir=
LogLevel=
LogTimeGMT=0
```

   注: これらのパラメータについては、前の手順の表で説明されています。

2. パラメータに必要な値を設定します。
3. ファイルを保存して閉じます。
4. CA Risk Authentication サーバを再起動します。

riskfortdataupload.ini

CA Risk Authentication は、トランザクションの発生元であるシステムの IP アドレスを使用することによって、Quova データからユーザの地理位置を特定します。その後、このデータから、拒否国、拒否 IP、およびゾーン ホッピングのルールを評価します。

CA Risk Authentication には、Quova ファイルから CA Risk Authentication データベースに地理位置データをアップロードできるようにするための、*CA Risk Authentication データ アップロード ツール*（arrfupload）が付属しています。 riskfortdataupload.ini ファイルは、CA Risk Authentication データ アップロード ツールの動作を制御します。このファイルは以下の場所にあります。

`<install_location>¥Arcot Systems¥conf¥`

以下の表に、このファイル内の設定パラメータを示します。

パラメータ	デフォルト	Description
Tables	ロードしない	ユーザが操作できるテーブル。 以下の値が使用可能です。 ■ GeoPoint ■ Anonymizer

パラメータ	デフォルト	Description
Load	0	テーブルにデータをアップロードするかどうかのインジケータ。 以下の値が使用可能です。 ■ 0：（ロードしない） ■ 1：（ロードする）
Swap	0	テーブルをスワップするかどうかのインジケータ。 以下の値が使用可能です。 ■ 0：（スワップしない） ■ 1：（スワップする）
Filename	--	Quova データのロード元となるファイルの名前。 **重要**: ファイル名と共にファイルへの絶対パスを指定します。

注: Load と Swap の両方を 1 に設定した場合、テーブルはロードされてからスワップされます。

udsserver.ini

udsserver.ini ファイルには、ユーザ データ サービス（UDS）のログ情報を設定するためのパラメータが含まれています。 以下の表に、CA Risk Authentication について設定する必要のあるパラメータに関する情報を示します。

このファイルで設定できる共通のログ レベル値は次のとおりです。

- FATAL
- 注意
- INFO
- DEBUG

注: ログ レベルの詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。

パラメータ	デフォルト値	Description
log4j.rootCategory	ERROR、debuglog	ロガー階層の一番上に存在するルート ロガー。 値が指定されていない場合、子ロガーはすべてこの値を継承します。
log4j.logger.com.arcot.euds	INFO	UDS 情報を書き込むために使用する必要があるログ レベル。
log4j.logger.com.arcot.crypto.impl. SecureStoreUtil	INFO	ハードウェア ベースまたはソフトウェア ベースの HSM を使用している場合に、ログを書き込むために使用する必要のあるログ レベル。
log4j.logger.com.arcot.common.database	INFO	データベース情報を書き込むために使用する必要があるログ レベル。
log4j.logger.com.arcot.common.cache	INFO	UDS キャッシュ情報を書き込むために使用する必要があるログ レベル。
log4j.appender.debuglog	org.apache.log4j.RollingFileAppender	ログ ファイルが開かれるモードおよび次の操作が開始する位置のオフセット ポインタを指定する UDS ログ ハンドルの名前。

パラメータ	デフォルト値	Description
log4j.appender.debuglog.File	${arcot.home} /logs/arcotuds.log	UDS ログのファイル名と、ログが作成される場所。 UDS のデフォルトのログ ファイル名は arcotuds.log で、以下の場所に作成されます。 <*install_location*>¥Arcot Systems¥logs¥
log4j.appender.debuglog.MaxFileSize	10 MB	ログ ファイルについて許可される最大サイズ。
log4j.appender.debuglog.MaxBackupIndex	100	作成できるバックアップ ファイルの最大数。 バックアップ ファイルの数がこの値に達すると、アプリケーションは先頭のログ ファイルから上書きを開始します。
log4j.appender.debuglog.layout	org.apache.log4j. PatternLayout	ConversionPattern パラメータによって指定された出力形式。
log4j.appender.debuglog.Encoding	UTF-8	ログ ファイルにエントリを書き込むときに使用するエンコーディング。
log4j.appender.debuglog.layout. ConversionPattern	%d{yyyy-MM-dd HH:mm:ss,SSS z} : [%t] : %-5p : %-5c{3} : %m%n	UDS ログ ファイル エントリが書き込まれる形式 ■ タイム スタンプ（%d{yyyy-MM-dd HH:mm:ss,SSS z} :） ■ スレッド ID （[%t] :） ■ ログ レベル（または重大度）（%-5p :） ■ ロガー クラス（%-5c{3} :） ■ メッセージ（%m%n） **注**: このパターンは C 言語の printf 関数に似ています。

付録 H: プロパティ ファイルの詳細

CA Risk Authentication は主に、以下のセクションで説明するプロパティ ファイルを使用します。

これらファイルは、以下の場所にあります。
<*install_location*>¥Arcot Systems¥sdk¥java¥**properties**¥

riskfort.risk-evaluation.properties

riskfort.risk-evaluation.properties ファイルには、CA Risk Authentication リスク評価 Java SDK とサンプル アプリケーションが CA Risk Authentication サーバ情報を読み取るためのパラメータが含まれます。 以下の表に、このファイルで使用される設定パラメータを示します。

パラメータ	デフォルト	Description
HOST.1	localhost	CA Risk Authentication サーバの IP アドレス。
PORT.1	7680	CA Risk Authentication サーバが受信リクエストを待ち受けるポート番号。
CONNECTION_TIMEOUT	10000	CA Risk Authentication サーバが接続不能と判断されるまでの時間（ミリ秒単位）。
CONNECTION_RETRIES	3	CA Risk Authentication サーバで許可される最大試行回数。
READ_TIMEOUT	30000	CA Risk Authentication サーバからのレスポンスに対して許可される最大時間（ミリ秒単位）。
USE_CONNECTION_POOLING	1	CA Risk Authentication サーバに対する接続プールを有効または無効にするパラメータ。 ■ 0： 無効 ■ 1： 有効
MAX_ACTIVE	128	CA Risk Authentication サーバで許可されるアクティブな接続（プールからの）の最大数。 プールから一度に借り出すことができる接続の最大数を制御します。負の値の場合、一度にアクティブになる可能性のあるオブジェクトの数に制限はありません。

パラメータ	デフォルト	Description
TIME_BETWEEN_CONNECTION_EVICTION	900000（15 分）	アイドル接続エビクター スレッドの連続実行間の間隔（ミリ秒単位）。 **注**: このパラメータを -1 に設定した場合、接続は削除されません。 **重要**: TIME_BETWEEN_CONNECTION_EVICTION の値と IDLE_TIME_OF_CONNECTION の値の合計が、ファイアウォールの接続タイムアウトの値より小さいことを確認します（SDK と CA Risk Authentication サーバの間）。これにより、アイドル時間が原因で接続がファイアウォールによって不意に削除されることがなくなり、システムの円滑な動作が保証されます。
IDLE_TIME_OF_CONNECTION	1800000（30 分）	接続が閉じられるまでのアイドル時間（ミリ秒単位）。 **注**: このパラメータを -1 に設定した場合、接続は削除されません。
WHEN_EXHAUSTED_ACTION	BLOCK	すべての接続が使い果たされた場合の SDK の動作。 ■ BLOCK： SDK は、接続が解放されるのを待機します。 これはデフォルトの動作です。 ■ FAIL： トランザクションは、失敗と解釈されます。 ■ GROW： SDK はプールを増加させることができます。

パラメータ	デフォルト	Description
TRANSPORT_TYPE	TCP	CA Risk Authentication サーバが起動するためのデフォルト値は TCP です。 CA Risk Authentication ネイティブ プロトコルが SSL に設定されている場合は、このパラメータを SSL に設定します。 つまり、管理コンソールと CA Risk Authentication サーバの間で SSL ベースの安全な通信を有効にしたい場合は、このパラメータを SSL に設定します。 **注**: この値を SSL に変更した場合は、CA Risk Authentication サーバを再起動します。
CA_CERT_FILE		サーバの CA 証明書ファイルのパス。このファイルは .PEM 形式である*必要があります*。 ファイルの完全パスを入力します。 例 : <*install_location*>/certs/ca.pem または <*install_location*>¥¥certs¥¥ca.pem **注**: – クライアントの PKCS#12 ファイル (クライアント キーと証明書のペアを含む) には、CLIENT_P12_FILE を使用します。 – 指定の PKCS#12 ファイルのパスワードには CLIENT_P12_PASSWORD を使用します。
LIFO	false	接続プールが後入れ先出し順でアイドル オブジェクトを返すかどうかを示します。 各接続がラウンド ロビン方式で使用され、アイドルではないようにするためには、false に設定します。 高負荷の展開の場合、推奨される値は false です。
NUM_PRE_CREATE	32	プールの初期化時に作成する必要がある接続の数。
NUM_CONNECT_FAILURES_TO_TRIGGER_FAILOVER	2	別のプールへのフェールオーバのトリガになる、連続して接続が失敗する数。

パラメータ	デフォルト	Description
MAX_IDLE	-1	SDK から、プールで許可される特定のサーバ インスタンスへのアイドル接続の最大数。
MAX_WAIT_TIME_MILLIS	3000	接続要求がプールからの接続を待機する最大時間（ミリ秒単位）。 **注**: このパラメータを -1 に設定した場合、要求は無期限に待機します。

log4j.properties.risk-evaluation

log4j.properties.risk-evaluation ファイルは、CA Risk Authentication とそのリスク管理コンポーネントのログ記録の動作を指定します。 以下の表に、リスク評価について変更が必要な可能性があるパラメータについて説明します。

パラメータ	デフォルト値	Description
log4j.rootLogger	INFO、debuglog	ログの書き込みに必要なログ レベルを指定します。サポートされるログ レベルは以下のとおりです。 ■ FATAL ■ 注意 ■ INFO ■ DEBUG **注**: ログ レベルの詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。
log4j.logger.com.arcot	INFO	
log4j.logger.com.arcot.riskfortAPI	DEBUG	
log4j.appender.debuglog.File	arcot-riskfort-evaluaterisk.log	ログ ファイルの名前。このパラメータに使用できる値は以下のとおりです。 ■ riskfortsdk.log （CA Risk Authentication Java SDK の場合） ■ arriskfortws.log （CA Risk Authentication Web サービスの場合）
log4j.appender.debuglog.MaxFileSize	1 MB	ログ ファイルについて許可される最大サイズ。

パラメータ	デフォルト値	Description
log4j.appender.debuglog.MaxBackupIndex	3	作成できるバックアップ ファイルの最大数。バックアップ ファイルの数がこの値に達すると、アプリケーションは先頭のログ ファイルから上書きを開始します。

付録 I: XML 設定ファイルの詳細

ユーザ行動プロファイリングは、XML ファイルをログ設定に使用します。

ubp_logging.xml ファイル

ubp_logging xml ファイルは、ユーザ行動プロファイリング モデルのログ設定を提供します。 パラメータについて以下の表で説明します。

タグ	デフォルト	Description
ubp_logging xml ファイル	ARCOT_HOME¥logs¥ubp_logfile.log	ログ ファイルの場所と名前を指定します。
MaxFileSize	5MB	ロールオーバーする必要があるファイル サイズを指定します。
レベル	ERROR	logger タグの「name」属性で指定されているパッケージ内のクラスで実行されるログ レベルを指定します。

CA Risk Authentication データベースには多くのテーブルが含まれます。 テーブルの中には、多く使うほど拡大するものがあります。 ユーザ数に直接比例して肥大化するテーブルもあれば、製品の使用に直接比例して肥大化するテーブルもあります。 また、ユーザがシステムに複数回アクセスすることによってもテーブルは拡大します。 ディスク容量には制限があるので、CA Risk Authentication の展開を管理しているデータベース管理者にとって、テーブルが無制限に拡大するのは望ましいことではありません。 この付録では、一部のテーブルを削除することで、ディスク容量を管理し、データベース パフォーマンスを向上させる方法について説明します。

削除するテーブルは、監査ログ情報など、トランザクションの詳細が含まれるテーブルに限定します。 ユーザ情報が含まれるテーブルは削除 *しないでください*。リスク評価の査定に必要です。

注: 設定およびデータのレポートの必要性に応じて、SQL データベースに適切な調整を行うことをお勧めします。 たとえば、大量のデータの削除は、削除プロセス時のパフォーマンスに悪影響を与えます。 ロールバック セグメントのサイズによっては、この削除でシステムが停止してしまう可能性すらあります。 また、古いレコードをアーカイブし、これらを完全に削除しないことを強くお勧めします。

このセクションでは、データベース テーブルの複製に関する推奨事項、CA Risk Authentication 用のデータベースの設定を計画する段階でデータベースのサイズを計算する方法、CA Risk Authentication によって使用されるすべてのテーブル、およびテーブルの削除に関する推奨事項について説明します。

- CA Risk Authentication データベース テーブル (P. 518)
- データベース サイズの計算 (P. 533)
- データベース テーブルの複製に関するアドバイス (P. 535)
- データベース テーブルのアーカイブに関する推奨事項 (P. 542)
- データベース接続調整パラメータ (P. 544)

CA Risk Authentication データベース テーブル

このセクションでは、すべてのデータベース テーブルについて簡単に説明します。 以下のファイルが含まれます。

CA Risk Authentication で使用

以下の表に、すべての CA Risk Authentication データベース テーブルとその説明を示します。

テーブル名	Description
ARQGEOANONYMIZER1	エンド ユーザの IP アドレスを伝達しないアノニマイザの既知の IP アドレスが格納されます。 これはプライマリ テーブルです。 **注**: このテーブルにデータを再ロードしている間、CA Risk Authentication サーバは ARQGeoAnonymizer2 を参照します。
ARQGEOANONYMIZER2	エンド ユーザの IP アドレスを伝達しないアノニマイザの既知の IP アドレスが格納されます。 これはセカンダリ テーブルです。 **注**: このテーブルにデータを再ロードしている間、CA Risk Authentication サーバは ARQGeoAnonymizer1 を参照します。
ARQGEOPOINT1	さまざまな範囲の IP アドレスの地理位置情報が格納されます。 この情報は Quova から取得されます。 **注**: このテーブルにデータを再ロードしている間、CA Risk Authentication サーバは ARQGEOPOINT2 を参照します。
ARQGEOPOINT2	さまざまな範囲の IP アドレスの地理位置情報が格納されます。 この情報は Quova から取得されます。 **注**: このテーブルにデータを再ロードしている間、CA Risk Authentication サーバは ARQGEOPOINT1 を参照します。
ARQUOVAVERSION	ARQ* テーブルにアップロードされた Quova のファイルを追跡します。

テーブル名	Description
ARRF_CASE_TXN	ケースとトランザクションの間のマッピングおよびデフォルト チャネルに関連する詳細が含まれます。 展開用に特定のチャネルを定義する場合は、別のデータベース テーブルが作成され、デフォルトのテーブル名にチャネル名を付加した名前が付けられます（ARRF_CASE_TXN_<*チャネル名*> など）。
ARRF_CMA	クレジットカード保有者 - 業者 - 金額（CMA）の同じ組み合わせの繰り返しトランザクションが含まれます。 **注**: このルールが使用されない場合、テーブルは空です。
ARRF_IMA	IP - 業者 - 金額の同じ組み合わせの繰り返しトランザクションが含まれます。 **注**: このルールが使用されない場合、テーブルは空です。
ARRFADDONEXPOSEDPARAMS	展開したカスタム ルールによって使用されるパラメータの詳細が格納されます。 このテーブルには、処理中に特定のパラメータをカスタム ルールで変更できるかどうかに関する情報も格納されます。 **注**: パラメータを変更するときは、事前に CA サポートにお問い合わせいただくことをお勧めします。
ARRFADDONRULELISTDATA	リスト データとそれに対応するデータセット バージョンが含まれます。 これは、IN_LIST および IN_CATEGORY 演算子を使用するルールまたはルール フラグメントによって使用されます。
ARRFADDONRULEMAPPINGDATA	要素と要素の所属先カテゴリの間のマッピングが含まれます。このデータは、IN_CATEGORY 演算子を使用してデータからカテゴリへのマッピングを格納するルールによって使用されます。 たとえば、3D セキュア展開の業者ルールがあります。
ARRFADDONRULETYPE	システム内の各組織に対して実装されたカスタム ルールの詳細な設定情報が格納されます。
ARRFADVICECODE	使用可能なリスク アドバイスのリストが格納されます。
ARRFADVICECONFIG	リスク スコア範囲とそれに対応するアドバイスの間のマッピングが格納されます。 **注**: 現在、このマッピングはすべての組織について同じです。

テーブル名	Description
ARRFBASECHANNELELEMENTS	チャネルにわたるすべての共通要素のマッピングおよびそれらの設定が格納されます。
ARRFBUCKETCONFIG	MFP と DeviceDNA によってシグネチャ一致に使用されるすべてのカテゴリの詳細が格納されます。 言いかえれば、このテーブルには、すべての分類のマスタリスト、および DeviceDNA アルゴリズムで使用される属性や相対的な重みなど、それらの詳細が含まれます。
ARRFBUCKETELEMENTCONFIG	DeviceDNA によってシグネチャ一致に使用されるすべてのカテゴリ内のすべての要素に関する設定詳細が格納されます。 また、このテーブルには、これらの要素の分類が含まれます。
ARRFCASEAUDITLOG	ケースの詳細およびログに記録されるケース関連の他のアクティビティが格納されます。
ARRFCASEQUEUES	各ケース キューの定義が格納されます。
ARRFCASES	システム内のすべてのオープン ケースの詳細が、ケースの所属先のキューに関係なく格納されます。
ARRFCHANNEL	システム内に存在するすべてのチャネルの基本的な定義（ケース トランザクション テーブル名や監査ログ テーブル名など）が格納されます。
ARRFCHANNELDETAILCATEGORY	各チャネルについて、GUI 表示要素が所属するさまざまなカテゴリの詳細が格納されます。
ARRFCHANNELELEMENTS	すべてのチャネル要素の詳細が格納されます。
ARRFCHANNELMSGPROPERTIES	チャネルの表示名やキーなど、チャネルに固有のローカライゼーション情報が格納されます。 **注**: ローカライゼーションは現在のリリースではサポートされていません。
ARRFCHANNELTXNTYPE	システム内で各チャネルに対してサポートされるすべてのトランザクションのマッピングの詳細が格納されます。
ARRFCHANNELTXNTYPEELEMENTS	リクエストの一部として受信する可能性がある、可能なすべての要素タイプのチャネルの詳細が格納されます。言いかえれば、このテーブルには、チャネル要素からアクションへのマッピングが格納されます。

テーブル名	Description
ARRFCLIENTCERTSANDKEYS	トークン化解除サービスとの通信に必要な SSL キーと証明書が格納されます。 **注**: 現在、このテーブルは TransFort-CA Risk Authentication 統合展開でのみ適用されます。
ARRFCLIENTSSLROOTCAS	双方向 SSL 認証用のクライアント トラスト ストアとそれに対応するルート CA 証明書が格納されます。
ARRFCONFIGURATION	グローバル レベルおよび組織レベルのその他の CA Risk Authentication 設定が格納されます。 これには、ケースの詳細およびログに記録されるケース関連のその他のアクティビティに関連する情報が含まれます。
ARRFCOUNTRY	すべての国とその ISO コードのリストが格納されます。
ARRFCOUNTRYLIST	Quova データに登録されているすべての国のリストが格納されます。
ARRFCURRCONVRATES	サポートされるすべての通貨および対応する換算レートのリストが格納されます。
ARRFCURRENCY	すべての通貨、その ISO コード、および各通貨指数の詳細が格納されます。
ARRFCURRENTCMSCHEDULE	ケース管理キュー サーバによって作成されたケース スケジュールが格納されます。
ARRFCURRENTORGCONFIG	システム内のすべての組織についての現在の設定が格納されます。
ARRFDATAVERSIONMAPPING	構成済みのすべての CA Risk Authentication 設定情報が格納されます。 このテーブルにはバージョン情報も含まれるので、設定ごとに複数のエントリが含まれる場合があります。
ARRFDBERRORCODES	通信障害の可能性を示すすべてのデータベース エラー コードが含まれます。 **注**: このテーブルを編集するときは、事前に CA サポートにお問い合わせいただくことをお勧めします。

テーブル名	Description
ARRFDEVICECONTEXT	ユーザ デバイスから受信した各トランザクションのコンテキスト情報（デバイス ステータス、トランザクションのタイム スタンプ、リクエストされたアクションなど）が格納されます。 **注**: この情報はデバイス頻度チェックに使用されます。
ARRFDEVICEINFO	ユーザ トランザクションに使用されるすべてのデバイスの詳細情報が格納されます。
ARRFDEVICEINFOHIST	システムに登録されているすべてのユーザ デバイスの履歴が格納されます。
ARRFDEVICETYPE	サポートされるすべてのデスクトップおよび携帯端末のマスタ リストが格納されます。
ARRFDEVUSERASSO	ユーザとデバイスの間のマッピングに関するすべての情報が格納されます。
ARRFDEVUSERASSO_ARCHIVE	ユーザとデバイスの間のマッピングに関するすべてのアーカイブ情報が格納されます。
ARRFDISPLAYNAMES	管理コンソールのラベル（ARRFMESSAGES）で使用されるすべての変数文字列（DISPLAYNAMEKEY 用）が格納されます。
ARRFELEMENTSSUPPORTEDVALUES	トランザクション詳細を表示するための Case Management のレイアウト詳細が格納されます。
ARRFELEMOPREGIONMAP	ルール ビルダを使用してカスタム ルールを作成するときに使用できる、要素から操作へのすべての詳細なマッピングが格納されます。 言いかえれば、このテーブルには、ルール ビルダ画面の構成に使用されるメタデータが格納されます。
ARRFEXCEPTIONUSER	例外ユーザとしてマークされたユーザのリストが格納されます。
ARRFEXCPUSERHIST	例外ユーザとしてマークされたすべてのユーザの履歴が格納されます。

テーブル名	Description
ARRFINSTANCEAUDITLOG	インスタンス上で実行されたすべてのアクティビティ（再起動、更新、リフレッシュ、シャットダウンなど）と共に、システムに設定されているすべてのインスタンスに関連するすべての詳細が格納されます。 言いかえれば、このテーブルには、システムの各インスタンスに対するすべての管理アクティビティの監査証跡が格納されます。
ARRFINSTANCES	システムに設定されているすべてのサーバ インスタンスの詳細が格納されます。これらのインスタンスは、CA Risk Authentication サーバ インスタンスまたはケース管理キュー サーバ インスタンスのいずれかです。
ARRFIPCONTEXT	IP 頻度ルールによって使用される IP コンテキストが格納されます。 **注**: このテーブルは将来使用されます。
ARRFLIBRARYTOTYPEMAPPING	サポートされているすべてのカスタム ルール タイプとそれに対応するライブラリ名の間のマッピングが格納されます。 **注**: このテーブルは将来使用されます。
ARRFLOCALE	サポートされているすべてのロケールに関連する情報が格納されます。
ARRFMESSAGES	応答コードと理由コードのメッセージが格納されます。
ARRFNEGATIVECOUNTRYLIST	すべての拒否国のリストが格納されます。
ARRFOPERATORS	CA Risk Authentication でサポートされているすべての演算子（ルール ビルダを使用してルールを作成する場合に使用）のリストが格納されます。
ARRFORGCHANNEL	各組織でサポートされているすべてのチャネルのリストが格納されます。
ARRFORGQUEUES	組織とチャネルに属するすべてのキューのリストと基本的な詳細が格納されます。

テーブル名	Description
ARRFOTHERELEMENTS	カスタム ルールの作成に使用できるすべての非チャネル要素（システム時間など）に関する詳細情報が格納されます。 言いかえれば、このテーブルには、トランザクション中には渡されないが、ルール ビルダ 画面で使用または表示される要素のリストが格納されます。
ARRFPROTOCOLREGISTRY	CA Risk Authentication サーバの各リスナ ポートの設定が格納されます。
ARRFQUEUEADMIN	キューと管理者の間のマッピングの詳細が格納されます。
ARRFRULEDEPENDENCY	ルールが依存するほかのルールの詳細が格納されます。
ARRFSERVERS	使用可能な CA Risk Authentication サーバ インスタンスのマッピングが格納されます。
ARRFSITES	各トークン化解除サービスのサイト詳細が格納されます。 **注**: 現在、このテーブルは TransFort-CA Risk Authentication 統合展開でのみ適用されます。 このテーブルはまもなく廃止されます。
ARRFSYSAUDITLOG	ログに記録されるすべてのトランザクション（リスク評価およびその他のアクティビティ）に関連するすべての詳細が格納されます。 展開用に追加のチャネルを設定する場合は、それに対応するテーブルが作成され、デフォルトのテーブル名にチャネル名を付加した名前が付けられます（ARRFSYSAUDITLOG_<*チャネル名*> など）。
ARRFSYSORGCONFIG	システム内のすべての組織で使用できる設定のすべてのバージョンが格納されます。 **注**: このテーブルには、履歴と、管理者によって行われた変更の両方が格納されます。
ARRFSYSPARAMSCONFIG	管理コンソールを使って設定できるすべての CA Risk Authentication システム パラメータに関する詳細情報が含まれます。 **注**: このテーブルには、履歴と、管理者によって行われた変更の両方が格納されます。

テーブル名	Description
ARRFSYSRULEEXECCONFIG	すべてのルールの設定情報が格納されます。 この情報には、各ルールのバージョンと設定が含まれます。 **注**: このテーブルには、履歴と、管理者によって行われた変更の両方が格納されます。
ARRFSYSTERMRULESCORECONFIG	各ルールとそれに対応する結果（リスク スコアに影響する）の設定情報が格納されます。
ARRFTRUSTEDIPLIST	すべてのトラステッド アグリゲータ、IP アドレス、および範囲の情報が格納されます。
ARRFTXNTYPE	システムでサポートされているすべてのトランザクション タイプのマスタ リストが格納されます。
ARRFUAOSLIST	すべてのユーザ エージェント OS 文字列から実際のオペレーティング システムおよびバージョンへのマッピングのマスタ リストが格納されます。 この情報は Windows の論理的なアップグレードに使用されます。
ARRFUNTRUSTEDIPLIST	すべての拒否 IP アドレスの詳細が格納されます。
ARRFUNTRUSTEDIPLIST_ ARCHIVE	ARRFUNTRUSTEDIPLIST テーブルのアーカイブ情報が格納されます。 言いかえれば、このテーブルは、削除されたすべての拒否 IP アドレスに関連する詳細のアーカイブとして機能します。
ARRFUNTRUSTEDIPTYPE	サポートされているすべての拒否 IP タイプのマッピングが格納されます。
ARRFUPLOADAUDITLOG	GeoPoint テーブルと GeoAnonymizer テーブルに対して実行される操作の詳細が格納されます。
ARRFUSERCONTEXT	ユーザから受信した各トランザクションのコンテキスト情報（ユーザ ステータス、トランザクションのタイム スタンプ、リクエストされたアクションなど）が格納されます。 **注**: この情報はユーザ頻度チェックに使用されます。
ARRFUSERCONTEXT_ARCHIVE	ARRFUSERCONTEXT テーブルのアーカイブ情報が格納されます。 言いかえれば、このテーブルは削除されたユーザに関するユーザ コンテキスト情報のアーカイブとして機能します。

管理コンソールによって使用されるデータベース テーブル

以下の表に、管理コンソールによって使用されるすべてのデータベース テーブルを示します。

テーブル名	Description
ARADMINAUDITTRAIL	管理者アクティビティ監査が格納されます。
ARADMINAUTHTOKEN	管理コンソールがプラグ可能な認証に使用するトークンが格納されます。 ユーザがパスワードを使用して管理コンソールにログインするたびに、パスワードが一致し、このテーブルに格納された後、トークンが内部的に生成されます。
ARADMINBASICAUTHPWDHISTORY	管理者用の基本認証を使用して管理コンソールにログインする、すべての組織のすべての管理者の最後の *n* 個のパスワードが格納されます。 この情報はパスワードの再利用を防ぐために格納されます。
ARADMINBASICAUTHUSER	管理者用の基本認証を使用して管理コンソールにログインする、すべての組織のすべての管理者の基本認証の認証情報が格納されます。
ARADMINCONFIG	管理コンソールの設定が格納されます。
ARADMINCUSTOMROLE	すべてのカスタム定義ロールの設定が格納されます。
ARADMINMANAGEROLE	指定したロールが管理できるロールのリストが格納されます。
ARADMINMAP	キーと値のペアとして入力される、CA Risk Authentication サーバ インスタンスの情報が格納されます。
ARADMINPAFCONFIG	システム内のすべての組織のすべての管理者の認証設定が格納されます。
ARADMINPREDEFINEDROLE	すべてのサポートされている管理者のロール情報が格納されます。
ARADMINPWDPOLICY	すべての組織のすべての管理者のパスワード ポリシーの詳細が格納されます。
ARADMINROLEPRIVILEGE	管理コンソールによってサポートされるすべての管理アクション（またはタスク）、各タスクのスコープ、およびタスクを実行できるロールの間のマッピングが格納されます。

テーブル名	Description
ARADMINSCOPE	各管理者が管理権（スコープ）を持つ組織のリストが格納されます。
ARADMINSCOPEALL	システム内にある既存のすべての組織に対して管理権（スコープ）を持つすべての管理者のリストが格納されます。
ARADMINSUPPORTEDAUTHMECH	管理コンソールにログインするためにサポートされているすべての認証メカニズムに関する情報が格納されます。
ARADMINSUPPORTEDTIMEZONE	CA Risk Authentication またはその他の依存製品をインストールした後、変更しないすべての使用可能なタイムゾーンのリストが格納されます。 **注**: これは内部テーブルです。
ARADMINTURNEDOFFPRIVILEGE	特定のカスタム ロールで使用できないすべての権限のリストが格納されます。
ARADMINTXID	各トランザクションの一意の ID を生成するために必要な情報が格納されます。
ARADMINUITAB	使用可能なタブに関する情報と、それらのタブを管理コンソールで使用できる順序に関する情報が格納されます。
ARADMINUITASK	使用可能なすべてのタスクに関する情報と、それらのタスクを管理コンソールで使用できる順序に関する情報が格納されます。
ARADMINUITASKATTRIBUTES	管理コンソールの第 1 階層および第 2 階層のタブがクリックされると表示されるタスクの詳細が格納されます。これらのタスクはランディング ページと呼ばれます。
ARADMINUITASKCONTAINER	使用可能な*タスク コンテナ*に関連する情報が格納されます。 タスク コンテナは、管理コンソール内の第 2 階層のタブ ID またはタスク グループのいずれかです。
ARADMINUSER	既存のすべての管理者に関する詳細情報（所属先の組織、現在のステータス、タイム ゾーン、ロケール、最終ログイン時間など）が格納されます。
ARADMINUSER_ARCHIVE	削除されたすべてのユーザに関する情報が格納されます。
ARADMINWIZARDTASK	ブートストラップ ウィザードを使用して実行可能なすべてのタスクに関する情報が格納されます。

テーブル名	Description
ARCMNBULKOPERATION	ユーザのアップロードやユーザ アカウントのアップロードを含む、サポートされているすべてのバルク操作に関する情報が格納されます。
ARCMNBULKOPERATIONATTRIBUTE	ARCMNBULKOPERATION テーブル内のすべてのバルク操作の属性が格納されます。
ARCMNBULKREQUEST	各バルク アップロード リクエストの詳細（組織名、リクエスト ID、リクエストのステータス、アップロードされたデータ、および操作など）が格納されます。
ARCMNBULKTASKPARAM	システムでサポートされている各タスクの各属性の名前と値が格納されます。
ARCMNBULKUPLOADTASK	すべてのバルク アップロード リクエストの各タスクのステータスが格納されます。
ARCMNCACHEREFRESH	管理コンソールをリフレッシュする必要があるかどうかを示すキャッシュ関連のハウスキーピング情報が格納されます。
ARCMNCONFIG	管理コンソールの共通の設定情報が格納されます。 ブートストラップが完了しているかどうか、キャッシュ リフレッシュは自動か手動か、属性の暗号化が有効になっているかどうか、バルク アップロード機能が有効になっているかどうかなどの設定情報が含まれます。
ARCMNDBERRORCODES	データベースがダウンしているか、応答していないことを示す、ベンダー固有のデータベース エラー コードおよび SQL 状態値が格納されます。 バックアップ データベースが設定されている場合、データベースをフェールオーバするべきかどうかを判断するために、この情報がシステムによって使用されます。
ARCMNMAPDATATYPE	コンソールのページを表示するために管理コンソールが使用する CA Risk Authentication 固有の情報、またはその以前製品の情報が格納されます。
ARPFCMNCACHEREFRESHEVENT	システム内のすべてのインスタンスのすべてのキャッシュ リフレッシュ イベントの詳細が格納されます。
ARPFCMNCACHEREFRESHSCOPE	サーバ キャッシュ リフレッシュ イベントが発生した場合に影響を受けるすべての組織に関する情報が格納されます。

テーブル名	Description
ARPFCMNCACHEREFRESHSTATUS	トリガされたすべてのインスタンスに対する各キャッシュ リフレッシュ イベントのステータスが格納されます。
ARPFCMNINSTANCE	システムに設定されているすべての CA Risk Authentication サーバ インスタンスの詳細情報が格納されます。 インスタンスが最後にリフレッシュされた時刻も含まれます。
ARPFCMNORGCONFIGDATA	各組織の設定の詳細が格納されます。 通常、組織レベルで優先可能なグローバル設定も含まれます。
ARPFCMNORGCONFIGSTATE	ARPFCMNORGCONFIGDATA テーブルの割り当て済みの各設定のステータスが格納されます。
ARPFCMNPRIVILEGEMAPPING	管理コンソールから使用可能な各権限の詳細が格納されます。
ARSEQUENCETABLE	このテーブルは、MS SQL Server によってのみ使用され、ストアド プロシージャを使用してシーケンスをシミュレートします。
ARREPORTTABLES	その他の管理コンソールおよび UDS テーブルのメタデータが含まれています。

ユーザ データ サービス(UDS)によって使用されるデータベース テーブル

以下の表に、UDS によって使用されるデータベース テーブルを示します。

テーブル名	Description
ARCMNKEY	グローバル レベルおよび組織レベルのすべてのキー ラベルが格納されます。
ARUDSACCOUNTTYPE	システムに設定されているすべてのアカウント タイプの詳細が格納されます。
ARUDSATTRMAP	各組織に固有のアカウントのカスタム属性のフィールド名を表す設定の詳細が格納されます。
ARUDSAUTHSESSION	現在アクティブなセッションの認証セッションの詳細が格納されます。このテーブルが複製されないと、アクティブな認証セッションは失われる可能性があります。
ARUDSCALLOUT	ユーザ固有のコールアウト設定が格納されます。 これらのコールアウトは、ユーザの作成や更新などの特定のイベントに対して呼び出されます（設定されている場合）。

テーブル名	Description
ARUDSCALLOUTINTERNAL	カスケード効果のある削除イベントがトリガまたは有効にされた場合のコールアウトに関する設定情報（呼び出される SDK メソッド）が格納されます。
ARUDSCALLOUTINTERNALPARAMS	内部コールアウトに固有のパラメータやタイプなどの詳細が格納されます。
ARUDSCALLOUTPARAM	外部コールアウトに固有のパラメータやタイプなどの詳細が格納されます。
ARUDSCONFIG	UDS 設定パラメータおよびその値が格納されます。
ARUDSCONFIGAUDITLOG	ユーザ データ ソース（UDS）の操作およびそのリターン ステータスの監査ログ情報が格納されます。
ARUDSCONTACTTYPE	組織またはグローバル レベルで設定可能な追加の連絡先情報（予備の電子メールや電話番号など）が格納されます。
ARUDSCUSTOMATTREXT	追加のユーザ アカウント カスタム属性が格納されます。 デフォルトでは、最大 10 個のユーザ アカウント カスタム属性が ARUDSUSERACCOUNT テーブルに格納されます。 最初の 10 個以降の追加の属性はこのテーブルに格納されます。
ARUDSCUSTOMATTREXT_ARCHIVE	ユーザ アカウントが削除されたときに、ユーザ アカウント カスタム属性に関するアーカイブ情報が格納されます。
ARUDSLDAPREPOSITORYCONFIG	LDAP ホストやポートの詳細など、LDAP リポジトリの設定が格納されます。
ARUDSORGANIZATION	組織の定義、その属性、およびリポジトリの接続性の詳細が格納されます。
ARUDSORGANIZATIONAUDITLOG	組織固有の UDS 監査ログ情報の詳細が格納されます。
ARUDSORGREPOATTRIBUTES	組織固有のリポジトリ マッピング情報が格納されます。 たとえば、ユーザ リポジトリとして LDAP を使用している場合、CA Risk Authentication 属性（たとえば、FNAME）が対応する LDAP 属性（たとえば、GIVENNAME）にマップされている場合があります。

テーブル名	Description
ARUDSORGSECUREATTRIBUTES	個人情報（PII）フィールドなど、暗号化する必要がある組織固有の属性が格納されます。 **注**: 管理コンソールを使用してこれらの属性を設定することもできます。
ARUDSREPOCLONESTATUS	外部リポジトリ（LDAP など）から ARUDSREPOSITORYUSER テーブルにユーザ情報の一時クローニングのステータスが格納されます。
ARUDSREPOSITORYTYPES	UDS によってサポートされるすべてのリポジトリの定義が格納されます。
ARUDSREPOSITORYUSER	パフォーマンスを向上させるために、外部リポジトリ（LDAP など）からのユーザ情報が一時的に格納されます。 これは通常、外部リポジトリから多数のユーザのユーザデータを取得する必要がある場合に行われます。
ARUDSRESOURCESCOPE	リソースと組織間のマッピングが格納されます。 つまり、このテーブルは、どのリソースがどの組織に適用可能かを指定します。 たとえば、特定のアカウント タイプは特定の組織にのみ適用可能な場合があります。
ARUDSRESOURCESCOPEALL	リソースと組織間のマッピングが格納されます。 ただし、すべての組織に適用可能なリソースを指定するので、ARUDSRESOURCESCOPE テーブルとは異なります。
ARUDSSECUREATTRIBUTES	暗号化する必要がある属性（PII を格納するフィールドなど）に関する情報が格納されます。 **注**: 管理コンソールを使用してこれらの属性を設定することもできます。
ARUDSUSER	組織に所属するすべてのユーザの詳細と属性が格納されます。
ARUDSUSER_ARCHIVE	システムから削除されたすべてのユーザ アカウントのユーザの詳細が格納されます。
ARUDSUSERACCOUNT	特定のユーザのユーザ アカウント情報が格納されます。
ARUDSUSERACCOUNT_ARCHIVE	システムから削除されたすべてのユーザ アカウントのユーザ アカウント情報が格納されます。

テーブル名	Description
ARUDSUSERATTRIBUTE	すべてのユーザ属性の定義が格納されます。 個々の製品によって、新規ユーザ属性が追加される場合のみ、このテーブルを変更することをお勧めします。
ARUDSUSERAUDITLOG	ユーザ操作固有の詳細な監査ログ情報が格納されます。
ARUDSUSERCONTACT	ユーザの予備の連絡先情報（電子メールや電話番号など）が格納されます。
ARUDSUSERCONTACT_ARCHIVE	システムから削除されたユーザ アカウントの予備の連絡先情報（電子メールや電話番号など）が格納されます。

ユーザ行動プロファイリング アプリケーションで使用

以下の情報は、データベース サイズの計算前に UBP によって使用されます。

テーブル名	Description
XUBPData	ユーザの行動パラメータを格納します。各ユーザのトランザクション データに基づいて更新されます。

データベース サイズの計算

このセクションでは、データベース管理者が CA Risk Authentication 用に設定する必要のあるデータベースの大体のサイズを計算するのに役立つ情報を提供します。

サンプル計算で使用される記号

サンプル計算では、以下の記号が使用されています。

- ユーザ数 = *N*
- 1 ユーザあたりのデバイスの平均数 = *O*
- ユーザとデバイスの関連付けの平均数 = *A*
- 1 日あたりのトランザクションの平均数 = *T*
- Quova データ フィード内のエントリ数 = *Q*
- 計算の対象期間（日単位）= *D*

前提値

計算用に以下の前提が定義されています。

- ユーザ数（**N**） = 1,000,000 （100 万）
- 1 ユーザあたりのデバイスの平均数（**O**）= 2
- ユーザとデバイスの関連付けの平均数（**A**）= 2
- 1 日あたりのトランザクションの平均数（**T**） = 24,000
- Quova データ フィード内のエントリ数（**Q**）= 10,000,000（1,000 万）
- 計算の対象期間（**D**）= 90 日

前提値に基づくサンプル計算

前のセクションで示した前提値を考慮すると、最終的な要件は以下のようになります。

- **ユーザの総数**に基づくデータベース サイズ = （10 * *N*） KB

  この計算で、1 ユーザあたりの値 10 KB は以下のように導き出されました。

  - **ARRFUSERCONTEXT**： 1 レコードあたり 3 KB
  - **ARUDSUSER**： 1 レコードあたり 3.5 KB

- **ARUDSAUDITLOG：** 1 レコードあたり 3 KB

- **デバイスの総数**に基づくデータベース サイズ = （6 * *O* * *N*） KB

  この計算で、1 ユーザあたりの値 6 KB は以下のように導き出されました。

  - **ARRFDEVICECONTEXT：** 1 レコードあたり 2 KB
  - **ARRFDEVICEINFO：** 1 レコードあたり 4 KB

  この計算では、前のセクションで示した以下の前提値を使用します。

  - **O**： 2

- **ユーザとデバイスの関連付けの総数**に基づくデータベース サイズ = （5 * *A* * *N*） KB

  この計算で、1 ユーザあたりの値 5 KB は以下のように導き出されました。

  - **DEVICEUSERASSOCIATION：** 1 レコードあたり 1 KB
  - **DEVICEINFO：** 1 レコードあたり 4 KB

  この計算では、前のセクションで示した以下の前提値を使用します。

  - **A**： 2

- **日常業務**に基づくデータベース サイズ = （*T* * *D* * 20） KB
- **Quova データ フィードのサイズ**に基づくデータベース サイズ = （*Q* * 2） KB

データベース テーブルの複製に関するアドバイス

このセクションでは、プライマリ データベースとバックアップ データベースの間でテーブルをどれくらいの頻度で複製する必要があるのかについて説明します。 このセクションでは、以下のトピックについて説明します。

リアルタイム同期が必要なテーブル

以下の表に、プライマリ データベースとバックアップ データベース間のリアルタイム同期が必要なデータベース テーブルを示します。 このカテゴリには、ユーザ関連情報をテーブルが主に含まれます。 このデータは認証に必要であるため、これらのテーブルのリアルタイム同期を実行する必要があります。

[Component]	テーブル
管理コンソール	ARADMINAUDITTRAIL
	ARADMINBASICAUTHUSER
	ARADMINSCOPE
	ARADMINSCOPEALL
	ARADMINUSER
	ARSEQUENCETABLE
	ARADMINTXID
	ARCMNKEY
	ARUDSORGANIZATION
	ARUDSORGREPOATTRIBUTES
	ARUDSORGSECUREATTRIBUTES
	ARUDSLDAPREPOSITORYCONFIG
	ARUDSACCOUNTTYPE
	ARUDSRESOURCESCOPE
	ARUDSRESOURCESCOPEALL
	ARUDSATTRMAP
	ARUDSCONTACTTYPE

[Component]	テーブル
UDS	ARUDSUSER
	ARUDSUSERACCOUNT
	ARUDSCUSTOMATTREXT
	ARUDSAUTHSESSION
	ARUDSUSERCONTACT
	ARUDSREPOSITORYUSER
	ARPFCMNINSTANCE
CA Risk Authentication	ARRF_CMA
	ARRF_IMA
	ARRF_CASE_TXN
	ARRFCURRENTCMSCHEDULE
	ARRFADDONRULELISTDATA
	ARRFADDONRULEMAPPINGDATA
	ARRFCASEAUDITLOG
	ARRFCLIENTSSLROOTCAS
	ARRFCURRENTORGCONFIG
	ARRFDATAVERSIONMAPPING
	ARRFDEVICECONTEXT
	ARRFDEVICEINFO
	ARRFDEVUSERASSO
	ARRFEXCEPTIONUSER
	ARRFINSTANCEAUDITLOG
	ARRFINSTANCES
	ARRFIPCONTEXT
	ARRFNEGATIVECOUNTRYLIST
	ARRFSYSPARAMSCONFIG
	ARUDSAUDITLOG

[Component]	テーブル
CA Risk Authentication	ARRFSYSAUDITLOG
	ARRFSYSORGCONFIG
	ARRFSYSRULEEXECCONFIG
	ARRFSYSTERMRULESCORECONFIG
	ARRFTRUSTEDIPLIST
	ARRFUNTRUSTEDIPLIST
	ARRFUSERCONTEXT
	ARRFORGQUEUES
	ARRFQUEUEADMIN
	ARRFUPLOADAUDITLOG
	ARRFCASEQUEUES

定期的な同期が必要なテーブル

以下の表に、プライマリ データベースとバックアップ データベース間の定期的な同期が必要なデータベース テーブルを示します。 設定に変更があった場合、これらのデータベース テーブルは同期化されます。

[Component]	テーブル
管理コンソール	ARADMINCONFIG
	ARADMINCUSTOMROLE
	ARADMINMAP
	ARADMINPAFCONFIG
	ARADMINPWDPOLICY
	ARADMINBASICAUTHPWDHISTORY
	ARADMINTURNEDOFFPRIVILEGE
	ARADMINCACHEREFRESH
	ARADMINAUDITTRAIL
	ARADMINUSER_ARCHIVE
	ARADMINMANAGEROLE
	ARADMINROLEPRIVILEGE

管理コンソール	ARPFCMNORGCONFIGDATA
	ARPFCMNORGCONFIGSTATE
	ARPFCMNCACHEREFRESHSTATUS
	ARPFCMNCACHEREFRESHEVENT
	ARPFCMNCACHEREFRESHSCOPE
UDS	ARUDSUSERAUDITLOG
	ARUDSORGANIZATIONAUDITLOG
	ARUDSCONFIGAUDITLOG
	ARUDSCONFIG
	ARUDSREPOSITORYTYPES
	ARUDSUSERATTRIBUTE
	ARUDSUSERACCOUNT_ARCHIVE
	ARUDSCUSTOMATTREXT_ARCHIVE
	ARUDSUSER_ARCHIVE
	ARUDSUSERCONTACT_ARCHIVE
	ARCMNCONFIG
	ARUDSREPOCLONESTATUS
	ARUDSCALLOUTINTERNAL
	ARUDSCALLOUTINTERNALPARAMS
	ARUDSCALLOUT
	ARUDSCALLOUTPARAM
	ARCMNBULKTASKPARAM
	ARCMNBULKUPLOADTASK
	ARCMNBULKREQUEST
	ARCMNBULKOPERATIONATTRIBUTE
	ARCMNBULKOPERATION
	ARRFCHANNEL

CA Risk Authentication	ARRFCHANNELDETAILCATEGORY
	ARRFCHANNELELEMENTS
	ARUDSUSERATTRIBUTE
	ARQGEOANONYMIZER1
	ARQGEOANONYMIZER2
	ARQGEOPOINT1
	ARQGEOPOINT2
	ARQUOVAVERSION
	ARRFADDONRULETYPE
	ARRFADVICECONFIG
	ARRFBASECHANNELELEMENTS
	ARRFBUCKETELEMENTCONFIG
	ARRFBUCKETCONFIG
	ARRFCONFIGURATION
	ARRFCOUNTRY
	ARRFCOUNTRYLIST
	ARRFCHANNELMSGPROPERTIES
	ARRFCHANNELTXNTYPE
	ARRFCHANNELTXNTYPEELEMENTS
	ARRFCLIENTCERTSANDKEYS
	ARRFCONFIGURATION
	ARRFCURRCONVRATES
	ARRFDEVICEINFOHIST
	ARRFELEMOPREGIONMAP
	ARRFELEMENTSSUPPORTEDVALUES
	ARRFEXCPUSERHIST
	ARRFLIBRARYTOTYPEMAPPING
	ARRFOPERATORS
	ARRFOTHERELEMENTS

	ARRFORGCHANNEL
	ARRFPROTOCOLREGISTRY
	ARRFSERVERS
	ARRFSITES
	ARRFTXNTYPE
	ARRFUNTRUSTEDIPTYPE
	ARRFUSERCONTEXT_ARCHIVE

同期が必要ないテーブル

以下の表に、プライマリ データベースとバックアップ データベース間の同期が必要ないデータベース テーブルを示します。

[Component]	テーブル
管理コンソール	ARADMINAUTHTOKEN
	ARCMNDBERRORCODES
	ARADMINPREDEFINEDROLE
	ARADMINSUPPORTEDAUTHMECH
管理コンソール	ARADMINUITAB
	ARADMINUITASK
	ARADMINUITASKATTRIBUTES
	ARADMINUITASKCONTAINER
	ARADMINWIZARDTASK
	ARREPORTTABLES
	ARCMNMAPDATATYPE
	ARCMNCACHEREFRESH
	ARCMNMAPDATATYPE
	ARPFCMNPRIVILEGEMAPPING
	ARADMINSUPPORTEDTIMEZONE
UDS	ARUDSSECUREATTRIBUTES

[Component]	テーブル
CA Risk Authentication	ARRFADVICECODE
	ARRFADDONEXPOSEDPARAMS
	ARRFCOUNTRYLIST
	ARRFCURRENCY
	ARRFDBERRORCODES
	ARRFDISPLAYNAMES
	ARRFLOCALE
	ARRFMESSAGES

データベース テーブルのアーカイブに関する推奨事項

このセクションでは、以下のテーブルの推奨事項について説明します。

重要: 削除するテーブルは、監査ログ情報など、トランザクションの詳細が含まれるテーブルに限定することをお勧めします。 ユーザ情報が含まれるテーブルは削除しないでください。リスク評価の査定に必要です。

急速に拡大するテーブル

以下のテーブル タイプは、すべてのトランザクションで急速に拡大し、組織のアーカイブのポリシーに従ってアーカイブまたはパージする必要があります。

- **監査データ**を格納するテーブル
  - ARADMINAUDITLOG
  - ARADMINAUDITTRAIL
  - ARRFINSTANCEAUDITLOG
  - ARRFUPLOADAUDITLOG
  - ARUDSAUDITLOG
- **トランザクション データ**を格納するテーブル
  - ARRFCASEAUDITLOG
  - ARRFSYSAUDITLOG
  - ARRFSYSAUDITLOG_<*channel*>
  - ARRF_CASE_TXN
  - ARRF_CASE_TXN_<*channel*>
  - ARRFUSERCONTEXT
- **レポート データ**および**デバイス データ**を格納するテーブル
  - ARREPORTS
  - ARRFDEVICECONTEXT
  - ARRFDEVICEINFO
  - ARRFDEVUSERASSO
  - ARRFUSERCONTEXT
  - ARRF_IMA
  - ARRF_CMA

- **設定データ**を格納するテーブル
  - ARRFCURRENTCMSCHEDULE
  - ARRFADVICECONFIG
  - ARRFCURRENTORGCONFIG
  - ARRFSYSORGCONFIG

これらのカテゴリの急速に拡大するテーブルのデータをアーカイブする場合、以下の手順が推奨されます。

1. バックアップ データベースからアーカイブします。

   このアクションは、トランザクションには影響せず、レポートのみに影響します。
2. バックアップ データベースをクリーンアップします。
3. バックアップ データベースを使用するには、サーバのフェールオーバを実行します。
4. プライマリ データベースをクリーンアップします。
5. プライマリ データベースに戻ります。

適度に拡大するテーブル

以下のテーブルは、ケース管理機能の使用方法に従って、適度に拡大します。したがって、これらのテーブルは、組織のアーカイブ ポリシーに従って、より低い頻度でアーカイブまたはパージできます。

- ARRFCASES
- ARUDSUSER

注: ARUDSUSER 内のエントリは登録済みユーザを表します。 ユーザ レコードは、ユーザ管理 Web サービスを通してこのテーブルに入力されます。 ただし、場合によっては、ARUDSUSER テーブル内のユーザ データをアーカイブすることもできます。 たとえば、ある一定の期間アプリケーションにアクセスしていないユーザの情報はアーカイブすることが推奨されます。 そのような場合、アプリケーションに再びアクセスするユーザを新規ユーザとして扱い、その分類に合ったリスク スコアを指定できます。
このような最適化にご興味がある場合は、CA サポート チームにご相談いただくことをお勧めします。

データベース接続調整パラメータ

CA Risk Authentication サーバとデータベースの間の接続を調整するためのパラメータは、管理コンソールの［インスタンス管理］ページを使用して設定します。このコンソール ページにアクセスするには、MA（マスタ管理者）としてログインする必要があります。 以下の表に、CA Risk Authentication サーバとデータベース間の接続を調整するために使用できる（共通）パラメータを示します。

フィールド	Description
最小接続数	CA Risk Authentication サーバとデータベース間に最初に作成される接続の最小数。
最大接続数	CA Risk Authentication サーバとデータベース間に作成できる接続の最大数。 **注**: この値は、MaxConnections パラメータより優先されるため、データベースがサポートする最大接続数に応じてこの値を設定する必要があります。 詳細については、データベース ベンダーのマニュアルを参照してください。
接続数の増分	必要性が生じた場合、既存の接続に追加される接続の数。接続の総数は、接続の最大数を超えることはできません。
モニタ スレッド スリープ時間（秒）	監視スレッドがすべてのデータベースのハートビート チェック間にスリープする時間。
障害がある場合のモニタ スレッド スリープ時間（秒）	データベース接続に障害が発生した場合に、データベース モニタ スレッドが接続プールの健全性をチェックする間隔。
クエリ詳細のログ	すべてのデータベース クエリのログ記録を有効化します。
データベース接続のモニタ	データベース モニタ スレッドでプールの事前チェックを有効にするオプション。
プライマリに自動的に戻す	プライマリ データベースが機能するようになったら、サーバのバックアップ データベースからプライマリ データベースへの切り替えを有効化します。

注:「CA Risk Authentication 管理ガイド」の「*CA Risk Authentication サーバ インスタンスの管理*」を参照してください。

第 18 章: デフォルトのポート番号および URL

この付録では、CA Risk Authentication が使用するデフォルト ポート番号および URL のリストを示します。 本章は以下の節によって構成されています。

デフォルトのポート番号

製品のインストール中、必要なデフォルト ポート番号が使用中であるかどうかがインストーラによって確認されます。 使用されていない場合は、そのポート番号が CA Risk Authentication コンポーネントに割り当てられます。ただし、デフォルト ポート番号が依存製品またはその他のアプリケーションによってすでに使用されている場合は、管理コンソールのプロトコル セットアップ画面を使ってポート番号を手動で指定する必要があります。

以下の表に、CA Risk Authentication で使用されるデフォルトのポート番号を示します。

プロトコル	デフォルト ポート番号	Description
CA Risk Authentication サーバ		
ネイティブ（TCP）	7680	これは、CA Risk Authentication がリスク評価の目的で使用する専用のプロトコルです。このポートは、CA Risk Authentication サーバ インスタンスと CA Risk Authentication Java SDK （リスク評価を含む）の間の通信に使用されます。
ネイティブ（SSL）	7681	CA Risk Authentication サーバ インスタンスと CA Risk Authentication Java SDK （リスク評価を含む）の間の SSL ベースの通信を可能にする独自仕様のプロトコルです。

プロトコル	デフォルト ポート番号	Description
管理 Web サービス	7777	このプロトコルは、CA Risk Authentication サーバと管理 Web サービスの間の通信に使用され、ルール設定の作成と管理に使用されます。 **注**: これらのコールには、リスク評価またはユーザおよび組織管理コールは含まれ*ません*。
トランザクション Web サービス	7778	このプロトコルは、CA Risk Authentication サーバインスタンスに接続するために、リスク評価 Web サービスによって使用されます。 **注**: これらのコールに管理サービス コールは*含まれません*。
サーバ管理	7980	管理コンソールは、このプロトコルを使用して CA Risk Authentication サーバ インスタンスと通信し、サーバ管理アクティビティ（正常なシャットダウン、サーバ キャッシュ リフレッシュ、インスタンス管理、およびプロトコル管理など）を行います。
ケース管理キュー サーバ **注**: ケース管理の詳細については、「*CA Risk Authentication 管理ガイド*」を参照してください。		
ケース管理キュー サーバ	7779	このプロトコルは、指定のポートでケース管理リクエスト（サーバ側）を待ち受けるために、ケース管理キュー サーバ モジュールによって使用されます。
ケース管理のキュー管理	7780	管理コンソールは、このプロトコルを使用してケース管理キュー サーバ インスタンスと通信し、サーバ管理アクティビティ（正常なシャットダウン、サーバ キャッシュ リフレッシュ、インスタンス管理、およびプロトコル管理など）を行います。

重要: ほかのサービスがすでに CA Risk Authentication が使用するデフォルト ポート上で実行されている場合、該当プロトコル用に新しいポートを設定する必要があります。
プロトコル用の新しいポート番号を設定するには、管理コンソールの［**プロトコル設定**］ページを使用します。「CA Risk Authentication 管理ガイド」の「CA Risk Authentication サーバ インスタンスの管理」を参照してください。

CA Risk Authentication コンポーネントの URL

インストール後に CA Risk Authentication コンポーネントにアクセスする際は、以下の表に記載されている URL を使用します。 表内の URL はデフォルト ポートを使用します。

コンポーネントまたはサービス	URL
管理コンソール （マスタ管理者（MA）用）	*http://<rf_hostname>:<rf_port>/arcotadmin/masteradminlogin.htm* **注**: ここで指定する必要があるポートは、アプリケーション サーバ ポートです。
管理コンソール （その他の管理者用）	*http://<rf_hostname>:<rf_port>/arcotadmin/adminlogin.htm* **注**: ここで指定する必要があるポートは、アプリケーション サーバ ポートです。
サンプル アプリケーション	*http://<rf_hostname>:<appserver_port>/ca-riskauth-8.0-sample-application/index.jsp* **注**: ここで指定する必要があるポートは、アプリケーション サーバ ポートです。
リスク評価 Web サービス	*http://<rf_hostname>:<rf_port>/services/RiskFortEvaluateRiskSvc* **注**: ここで指定するデフォルト ポートは **7778** です。
CA Risk Authentication 管理 Web サービス	*http://<rf_hostname>:<rf_port>/services/ArcotRiskFortAdminSvc* **注**: ここで指定するデフォルト ポートは **7777** です。

コンポーネントまたはサービス	URL
ユーザ管理 Web サービス	*http://<appserver_hostname>:<appserver_port>/arcotuds/services/ArcotUserRegistrySvc* **注**: ここで指定する必要があるポートは、UDS を展開したアプリケーション サーバ ポートです。
ユーザ行動プロファイリング アプリケーション	*http://<appserver_hostname>:<appserver_port>/ca-userprofiling-2.0-application/UBPServlet*
組織管理 Web サービス	*http://<appserver_hostname>:<appserver_port>/arcotuds/services/ArcotUserRegistryMgmtSvc* **注**: ここで指定する必要があるポートは、UDS を展開したアプリケーション サーバ ポートです。
構成レジストリ Web サービス	*http://<appserver_hostname>:<appserver_port>/arcotuds/services/ArcotConfigRegistrySvc* **注**: ここで指定する必要があるポートは、UDS を展開したアプリケーション サーバ ポートです。