Arcot RiskFort™
インストールおよび展開ガイド
（Unix プラットフォーム用）
バージョン 2.2.6

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot RiskFort インストールおよび展開ガイド
バージョン 2.2.6
2010 年 10 月
部品番号：RF-0226-0IGU-10

商標

特許

Arcot Systems, Inc., 455 West Maude Avenue, Sunnyvale, CA 94085

サードパーティ ソフトウェア

RiskFort によって使用されるサードパーティ ソフトウェア、および関連するコンポーネントはすべて、付録 「サードパーティ ソフトウェア ライセンス」に記載されています。

目次

はじめに

本書「Arcot RiskFort インストールおよび展開ガイド」は、Solaris （SPARC）10 および Red Hat Enterprise Linux 4.0 プラットフォームに関する以下のトピックについて説明します。

- Arcot RiskFort の概要
- RiskFort のインストール手順
- RiskFort SDK および Web サービスの設定
- RiskFort のアンインストール手順
- RiskFort のテーブルの肥大化とデータベース サイズの変更に関する推奨事項
- RiskFort 設定ファイル

対象読者

このガイドは、管理者、システム オペレータ、および Arcot RiskFort のインストールと展開を担当するユーザを対象としています。

注： このガイドの一部のトピックは、ユーザやグループの作成、グループへのユーザの追加、オペレーティング システム パッチのインストールなどのシステム管理操作に慣れたユーザを対象としています。これらのタスクに精通していない場合は、経験を積んだシステム オペレータやデータベース管理者に実行を依頼するよう強くお勧めします。

本書の内容

このガイドは、以下のパートで構成されています。

- 第 1 章の「RiskFort の基本について」: RiskFort の機能とアーキテクチャについて説明します。
- 第 2 章の「展開の計画」: RiskFort で展開できる各種モデルの概要を説明します。

- 第 3 章の「インストールの準備」: Solaris および Linux 上に RiskFort をインストールするための要件について説明します。また、設定と計画に関する情報も提供します。
- 第 4 章の「単一システムへの RiskFort の展開」: 単一のシステム環境に RiskFort をインストールする手順について説明します。
- 第 5 章の「分散システムへの RiskFort の展開」: 分散システム環境に RiskFort をインストールする手順について説明します。
- 第 6 章の「RiskFort SDK と Web サービスの設定」: Solaris および Linux プラットフォームで RiskFort が提供する API と Web サービスを設定する手順について説明します。
- 第 7 章の「RiskFort のアンインストール」: Solaris および Linux プラットフォームで RiskFort および関連コンポーネントをアンインストールする手順について説明します。
- 付録 A の 「RiskFort のディレクトリ構造」: RiskFort インストーラによってインストールされるファイルの場所に関する情報を提供します。
- 付録 B の 「設定ファイルおよびオプション」: RiskFort が使用する設定ファイル、およびこれらのファイルで設定する必要のあるパラメータについて説明します。また、これらのデフォルト設定ファイルのサンプルが記載されています。
- 付録 C の 「データベース リファレンス」: RiskFort におけるテーブルの肥大化、および調整に関する推奨事項について説明します。
- 付録 D の 「デフォルト ポート番号および URL」: RiskFort が使用するデフォルトのポート番号と URL のリストです。
- 付録 E の 「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」: 接続プーリングに必要なアプリケーション サーバの設定について説明します。
- 付録 F の 「SSL の設定」: RiskFort サーバとコンポーネント間の SSL 通信をセットアップする方法について説明します。
- 「サードパーティ ソフトウェア ライセンス」: RiskFort が使用するサードパーティのソフトウェア パッケージのリストを提供します。
- 「用語集」: RiskFort に関する重要な用語のリストです。

関連出版物

上記以外の関連出版物は以下のとおりです。

Arcot RiskFort 2.2.6 管理ガイド	このガイドには、RiskFort の管理と設定を行うための情報が記載されています。
Arcot RiskFort 2.2.6 Java 開発者ガイド	このガイドでは、RiskFort が提供する Java API とその使用方法について説明します。
Arcot RiskFort 2.2.6 クイック インストール ガイド	このガイドは、RiskFort のインストールに必要なタスクのサマリです。

本書の表記規則

このマニュアルで使用する規則、形式、および範囲は、以下のパラグラフのとおりです。

表記法

このマニュアルでは以下の表記法を使用します。

斜体	強調、ガイド名
太字	ユーザ入力、GUI 画面のテキスト
固定	ファイル名とディレクトリ名、拡張、コマンド プロンプト、CLI テキスト、本文内のコード
固定太字	パス内のターゲット ファイル名またはディレクトリ名
固定	コマンド プロンプト、CLI テキスト、コード
固定斜体	ユーザごとに異なる可能性のあるファイル名またはディレクトリ名
リンク	ガイド内のリンク、URL リンク

形式

このマニュアルでは、特別なメッセージを強調するために以下の形式を使用します。

注： 重要な情報、または特に注意が必要な情報を強調します。

	**ヒント :** 時間またはリソースの節約につながる方法を強調します。

	**警告 :** このタイプの注意を無視すると、誤動作または機器への損傷が発生するおそれがあります。

	**重要 :** 操作を実行する前に知っておくべき情報

	**注意 :** 考えられる危険に対して注意を促します。

	**関連文書 :** ほかのガイドへの参照を提供します。

サポートへのお問い合わせ

サポートが必要な場合は、以下の Arcot サポートにお問い合わせください。

E-MAIL （電子メール）	*support@arcot.com*
Web サイト	*http://www.arcot.com/support/index.html*

第 1 章
RiskFort の基本について

Arcot RiskFort （以下、RiskFort）は順応性の高い認証ソリューションです。広範囲に収集されたデータを標準装備のルールで検査することによって、オンライン トランザクション（ショッピング、バンキング、または企業アクセス）1 つ 1 つをリアル タイムで評価します。評価後、各トランザクションにはリスク スコアとアドバイスが割り当てられます。リスク スコアが高いほど、不正行為である可能性が高くなります。このリスク スコアとアドバイスをアプリケーションで利用し、自社のビジネス ポリシーに基づいて、トランザクションを承認または拒否したり、追加の認証を要求したり、テクニカル サポート担当者にアラートを発行したりすることができます。

RiskFort は設定の自由度が高く、ポリシーやリスク緩和要件との整合性を保ちながら、任意のリスク評価ルールの設定パラメータを柔軟に変更することができます。また、個々のルールでデフォルトのリスク スコア、スコアリング設定、およびスコアリング優先度を変更したり、1 つ以上のルールに対して実行の有効化と無効化を選択的に指定したりすることもできます。

事前設定済みのすぐに使えるルールに加えて、RiskFort は作業環境でプログラムが可能なアドオン ルール機能を備えており、業界特有のルールを選択的に展開できます。

この章では、RiskFort の基本概念とアーキテクチャについて説明し、本リリースで導入された機能と拡張機能を紹介します。

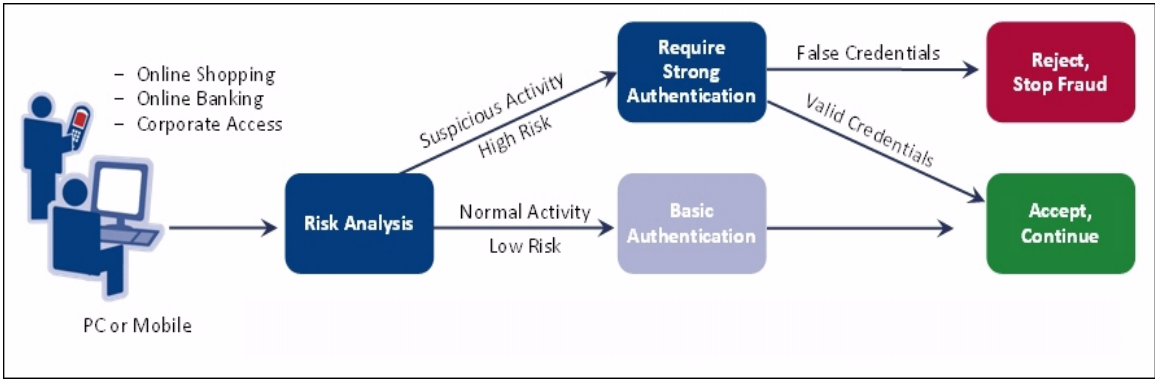
RiskFort の概要

RiskFort は、リスク評価のためのさまざまなデータを収集します（「リスク評価に使用されるデータ」で詳述）。収集したデータは、あらかじめ設定されたルールによって評価されます（「ルールおよびリスク処理」を参照）。各ルールの結果は、RiskFort 管理者によって設定された優先度の順序で評価され、最初に一致したルールに応じてスコアとアドバイスが生成されます（「リスク スコアとアドバイス」）。その後、RiskFort によって RiskFort データベースにユーザとデバイスの関連付けが作成されます（「ユーザとデバイスの関連付け」）。

RiskFort の動作のしくみ

図 1-1 は、RiskFort の広範囲に及ぶリスク評価と、各トランザクションにおける不正行為の検出のしくみを示しています。

図 1-1 ログイン前のリスク評価と不正行為検出



RiskFort のリスク分析機能は、ユーザがオンライン アプリケーションにログインする*前*、または正常にログインした*後*のどちらにも実装することができます。以降のサブセクションで詳細を説明します。

ログイン前のリスク評価と不正行為検出

ユーザがオンライン アプリケーションにアクセスしたとき、ログイン前であっても潜在的リスクについてユーザを評価できます。

ユーザがオンライン アプリケーションにログインする前に RiskFort のリスク分析機能が呼び出された場合、リスク評価のワークフローは以下のように行われます。

1. ユーザがオンライン アプリケーションにアクセスします。
2. アプリケーションが RiskFort を呼び出し、トランザクションに伴うリスクを分析します。
3. RiskFort が、受信入力と設定済みルールを使用して、リスクを評価します。「リスク評価に使用されるデータ」で説明されているデータがこのために使用されます。
4. ルールの実行結果と、評価した情報の一致 / 不一致に基づき、リスク スコアとアドバイスが RiskFort によって生成されます。
5. アプリケーションは以下のようにユーザを検証します。

- リスクが低い場合、ユーザはオンライン アプリケーションへのアクセスを許可されます。
- リスクが高い場合、ユーザはシステムへのアクセスを拒否されます。
- トランザクションが不審であるとタグ付けされた場合、アプリケーションはユーザに、アイデンティティを証明するための追加の（2 次）認証を要求します。

ログイン後のリスク評価と不正行為検出

ユーザがオンライン アプリケーションにアクセスしたら、まずログインさせておいて、事前定義のアクション（電子取引など）をユーザが実行しようとしたときに、そのユーザの潜在的リスクを包括的に評価することができます。

ユーザがオンライン アプリケーションで認証された後に RiskFort のリスク分析機能が呼び出された場合、リスク評価のワークフローは以下のように行われます。

1. ユーザがオンライン アプリケーションにログインします。
2. 指定しておいたアクションをユーザが実行しようとします。
3. アプリケーションが RiskFort を呼び出し、トランザクションに伴うリスクを分析します。
4. RiskFort が、受信入力と設定済みルールを使用して、リスクを評価します。「リスク評価に使用されるデータ」で説明されているデータがこのために使用されます。
5. ルールの実行結果と、評価した情報の一致 / 不一致に基づき、リスク スコアとアドバイスが RiskFort によって生成されます。
6. アプリケーションは以下のように、ユーザにトランザクションの続行を許可します。
   - リスクが低い場合、ユーザは続行を許可されます。
   - リスクが高い場合、ユーザはトランザクションを拒否されます。
   - トランザクションが不審であるとタグ付けされた場合、アプリケーションはユーザに、アイデンティティを証明するための追加の（2 次）認証を要求します。

リスク評価に使用されるデータ

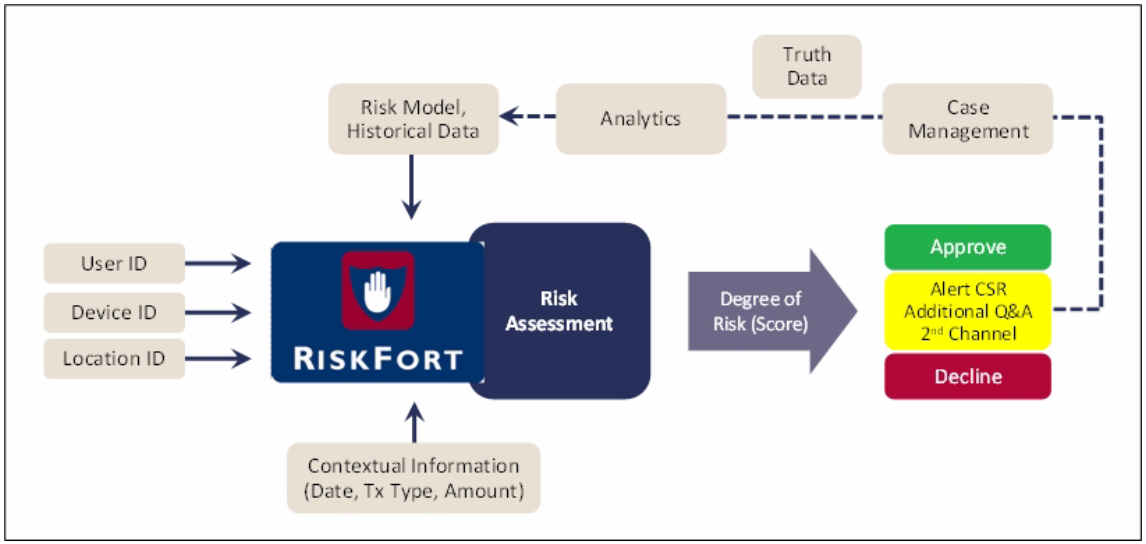
RiskFort のリスク分析の結果は、受信される以下の情報（利用できる場合）と、ユーザの履歴データとの比較に基づいています。

- 不正行為モデル
- デバイス DNA
- デバイス ID

- 場所情報
- ユーザおよびトランザクション情報

図 1-2 は、これらのデータが RiskFort でどのように使用されるかを示しています。以降のサブセクションで、各データ カテゴリの概要について説明します。

図 1-2 RiskFort で使用されるデータ



不正行為モデル

RiskFort 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 RiskFort 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。このスコアの範囲は通常、0 ～ 100 です。数字が大きくなるほど、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、RiskFort 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、詳細ルールを設定する際、システム パラメータの一部（ModelScore）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。

デバイス DNA

デバイス DNA （業界用語ではデバイス フィンガープリンティングまたは PC フィンガープリンティングとも言います）は、タグを用いないデバイス識別とアナリティクスの技術です。この技術によって、ユーザのシステム情報（ブラウザ、オペレーティング システム、インストールされているソフトウェア、表示画面設定、マルチメディア コンポーネント、その他の属性）が収集および分析され、デバイスのリスク プロファイルがリアル タイムで生成されます。

RiskFort がユーザのデバイスから収集する MFP 属性には、以下のものがあります。

- オペレーティング システムの名前とバージョン
- ブラウザ情報（名前、メジャー バージョン、マイナー バージョン、JavaScript のバージョン、HTTP ヘッダなど）
- 画面設定（高さ、幅、色深度など）
- システム情報（タイム ゾーン、言語、システム ロケールなど）

RiskFort は、エンド ユーザによるすべてのトランザクションの受信情報を、データベース内に格納された対応する MFP と照合します。この一致率（%）が Administration Console の［Other Configuration］画面で指定された値以上の場合、トランザクションは「安全である」と見なされます。

デバイス ID

デバイス ID は、RiskFort によって生成され、エンド ユーザのシステム上に設定される cookie です。これを使用して、オンライン アプリケーションへのログインとトランザクションの実行に使用されるデバイスを識別して追跡します。この情報は暗号化されています。

RiskFort デバイス ID は以下のように保存されます。

- **Flash オブジェクト：** `.sol` または `.ssl` （通信に SSL が使用されている場合）の拡張子で保存される Flash Shared Object （FSO）。ユーザ プロファイルの Flash Player ディレクトリに格納されます。このタイプの cookie は、すべてのブラウザで共通です。
- **ブラウザ cookie**：HTTP cookie。拡張子と保存場所はエンド ユーザが使用するブラウザに依存します。このタイプの cookie は、ブラウザ固有です。

注： 初めてデバイスを評価する際、RiskFort ではデバイス ID を*利用できません*。このデータは、2 回目以降の評価で使用されます。

ユーザを初めて評価する際、RiskFort は一意のデバイス情報（デバイス ID）を cookie 形式で生成し、ユーザのシステムに設定します。その後ユーザを評価する際に毎回、ユーザのシステム上のデバイス ID が RiskFort データベースに格納されたデバイス ID と一致するかどうかが検証されます。2 つのデバイス ID が一致すれば、受信された情報は「安全である」と見なされます。

場所情報

この情報には、ロケール、ISP、タイム ゾーン、関連する地理情報など、エンド ユーザのシステム IP アドレスから得られる地理的な場所についての情報が含まれます。RiskFort では、これらの情報を取得するために Quova® 社と提携しており、IP アドレスと地域とのマッピングという形で、各 IP アドレスの詳細な地理情報の提供を受けています。

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

RiskFort は、エンド ユーザによるすべてのトランザクションにおいて、受信 IP アドレスおよびその IP アドレスから得られる情報を、RiskFort データベースに格納された関連情報と照合します。この情報は、その後、［Negative IP］アドレス リスト、［Negative Country］リスト、および［Zone Hopping］のルールへの入力に使用されます。

ユーザおよびトランザクション情報

システム内では通常、ユーザのログイン ID によってユーザが一意に識別されます。RiskFort では、ユーザを一意に識別する属性の 1 つとしてこの情報が使用されます。

また、設定されている場合は、トランザクションに伴うリスクの分析に、コンテキスト情報やトランザクション情報（トランザクション量、トランザクション タイプ、日付など）も使用できます。ただし、RiskFort でこのコンテキスト情報の評価を有効にするには、カスタムのアドオン ルールを使用する必要があります。

関連文書： アドオン ルールの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

ルールおよびリスク処理

必要なデータが収集されると、それらのデータはルール エンジン（RiskFort サーバのモジュールの 1 つ）に転送されます。ルール エンジンは設定済みルールのセットで、これらのデータを受信される情報と履歴データ（利用できる場合）に基づいて評価します。

ルールは、1 つの条件または条件のセットで、ルールを呼び出すためには条件が真である必要があります。デフォルトでは、各ルールに優先度が割り当てられており、優先度レベルの順に評価されます。このルール スコアリングの優先度は、自社のビジネス要件に合わせて変更できます。

RiskFort が提供する標準装備ルールについては、表 1-1 を参照してください。

表 1-1. RiskFort の標準装備ルール

ルール名	説明
Trusted IP	「トラステッド」IP アドレスから組織に送信されたトランザクションには、低いスコアが割り当てられます。アドバイスはデフォルトで［Allow］に設定されます。
Trusted Aggregator	多くの企業で、オンラインの販路を拡大するためにアカウントとデータの集計サービス プロバイダのサービスを使用しています。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。 「トラステッド」アグリゲータから組織に送信されたトランザクションには、低いスコアが割り当てられます。アドバイスはデフォルトで［Allow］に設定されます。
Negative IP	このリストは、アノニマイザ プロキシの IP アドレスや、過去に不正なトランザクションか悪意のあるトランザクションの送信元だったことがわかっている IP アドレスで構成されます。 設定済みの拒否 IP アドレスから送信されたトランザクションには、高いスコアが割り当てられます。アドバイスは［Deny］に設定されます。
Negative Country	このリストは、過去に大量の不正行為の送信元だったことがわかっている国で構成されます。 RiskFort は、入力 IP アドレスに基づいて国情報を取得し、これらのデータを使用して、「拒否する」国から送信されたオンライン トランザクションに高いリスク スコアを割り当てます。
User Velocity	同一ユーザ ID の使用頻度の高さは、危険な動作を示している可能性があります。たとえば、不正行為の実行者は、複数のデバイスから同じユーザ ID とパスワードを使用して、ターゲット アカウントの特定のアクティビティを監視する場合があります。 短い間隔（設定可能）で同一ユーザから送信される過剰なトランザクションには、高いスコアが割り当てられます。アドバイスは［Deny］に設定されます。

表 1-1. RiskFort の標準装備ルール

ルール名	説明
Device Velocity	同一デバイスの使用頻度の高さも、危険な動作を示している可能性があります。たとえば、不正行為の実行者は、同一デバイスを使用してユーザ ID とパスワードの複数の組み合わせをテストする場合があります。管理者は、この動作を追跡するよう RiskFort を設定できます。 短い間隔（設定可能）で同一ユーザ デバイスから送信される大量のトランザクションは、高いスコアが割り当てられます。アドバイスは［Deny］に設定されます。
Zone Hopping	ユーザが同一ユーザ ID を使用して短時間に距離の離れた 2 か所からログインしている場合、不正行為である可能性が高いと考えられます。 また、ユーザ ID は共有も可能なので、このような場合、RiskFort では同一ユーザ ID を共有する 2 人のユーザが地理的に異なる場所にいる可能性があると判断し、適切なレスポンスで応答します。 短い間隔（設定可能）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には、高いスコアが割り当てられます。アドバイスは［Deny］に設定されます。
Unknown User	*既知のユーザ*とは、RiskFort データベースに登録されているユーザを指します。ユーザが RiskFort に対して不明な場合、デフォルトでは［Alert］が返されます。 これを受けて、CSR はアドバイスに基づき、ユーザをさらに認証することを選択できます。
Exception User	組織は、特定の期間、リスク評価からユーザを除外するよう選択できます。たとえば、ユーザが RiskFort 内で拒否に設定されている国へ旅行する場合、指定した期間、このユーザのステータスを［*Exception User*］に変更できます。 RiskFort は、例外ユーザから送信されたトランザクションに対し、低いリスク スコアを返します。アドバイスは通常［Allow］です。
DeviceID	デバイス ID は、RiskFort によって生成され、エンド ユーザのシステム上に設定されるデバイス識別子文字列です。これを使用して、ユーザがオンライン アプリケーションへのログインとトランザクションの実行に使用したデバイスが識別され、追跡されます。 RiskFort は、既知のデバイスから送信されたトランザクションに対し、低いリスク スコアを返します。アドバイスは通常［Allow］です。
User Associated with Device and Device-MFP Matched	トランザクションを送信したデバイスが一致する MFP を持つ既知のデバイスで、ユーザがそのデバイスに関連付けられている場合、トランザクションには低いスコアが割り当てられます。アドバイスは［Allow］に設定されます。

表 1-1. RiskFort の標準装備ルール

ルール名	説明
Device-MFP Matched but User Not Associated with Device	既知のユーザに関連付けられてない既知のデバイスからトランザクションが送信されている場合、トランザクションには中程度のスコアが割り当てられます。アドバイスには［IncreaseAuth］が設定されます。
User Associated with Device but Device-MFP Does Not Match	トランザクションを送信したデバイスが一致する MFP のない既知のデバイスである場合、トランザクションには低いスコアが割り当てられます。アドバイスは［IncreaseAuth］に設定されます。
User Not Associated with Device and Device-MFP Does Not Match	トランザクションが既知のユーザに関連付けられてない不明のデバイスから送信されている場合、トランザクションには高いスコアが割り当てられます。アドバイスには［Deny］が設定されます。

ルール エンジンは優先順位に従って、これらのルールを実行します。評価結果は、「スコアリング エンジン」と呼ばれる RiskFort サーバの別のモジュールに転送されます。

リスク スコアとアドバイス

スコアリング エンジンは、ルール エンジンによって提供される各ルールの実行結果に基づいて、優先度（管理者が設定）の順に各ルールを評価し、最初に一致したルールに対応するスコアを返します。

たとえば、以下の順序で 3 つのルールが設定されているとします。

1. Negative IP （スコアを 85 とします）
2. User Velocity （スコアを 70 とします）
3. Device Velocity （スコアを 65 とします）

注： 通常、クリティカルなルールほど高いスコアが割り当てられます。

トランザクションが拒否 IP アドレスから送信されていると RiskFort が判断した場合、最初に一致する設定済みルールに基づき、スコアとして「85」（否認）が返されます。別のトランザクションが設定済みの［Device Velocity］を上回っている場合、RiskFort はスコアとして「65」を返します。

スコアリング エンジンによって生成されるリスク スコアは **0** ～ **100** （表 1-2）までの整数です。RiskFort は、このリスク スコアを使用して、対応するアドバイスを生成し、アプリケーションにアドバイスを返します。

表 1-2 は、リスク スコアと対応するアドバイスのマトリックスの例を示しています。

表 1-2. リスク スコアとアドバイスのマトリックス

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
0	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、ユーザ名が現時点で不明な場合、アラートが発行されたら、テクニカル サポート担当者（CSR）にリダイレクトするか、RiskFort で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。

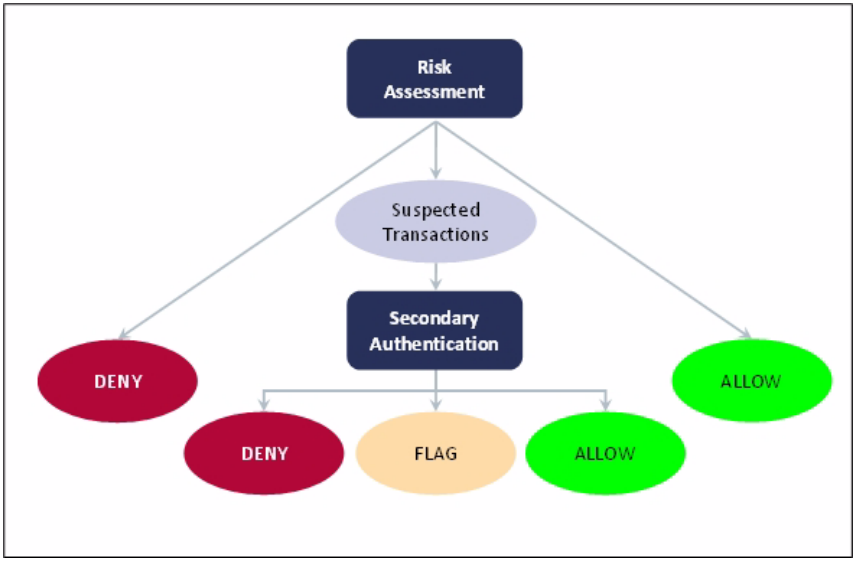
アドバイスは、RiskFort が受信したデータに応じて、以下のいずれかになります。

- **ALLOW**：トランザクションに関連付けられたリスク スコアが低い場合、RiskFort は［ALLOW］を返します。
- **ALERT**：RiskFort に登録されていないユーザがログインしようとした場合、［ALERT］を返します。
- **INCREASE AUTHENTICATION**：RiskFort では不審なトランザクションを検出すると、トランザクションに［INCREASE AUTHENTICATION］というフラグを設定し、アプリケーションに対して追加の認証をユーザに強制するようアドバイスします。

  たとえば、RiskFort に登録されているユーザが RiskFort に認識されていないデバイスからトランザクションを試みた場合、ユーザはアプリケーションで 2 次認証（OTP や Q&A など）を受ける必要があります。
- **DENY**：トランザクションに関連付けられたリスク スコアが高い場合、RiskFort は［DENY］を返します。

図 1-3 は、RiskFort によって返されるアドバイスの例を示しています。

図 1-3 リスク アドバイス



ユーザとデバイスの関連付け

RiskFort では、将来の評価のために、ユーザがアプリケーションへのアクセスに使用するデバイスとユーザを自動的に関連付ける（バインドする）ことによって、ユーザを有効なユーザとして一意に識別します。RiskFort の用語では、これを関連付け（またはデバイス バインディング）と呼びます。バインドされていないユーザが認証を受けようとすると、アドバイスとして［Increase Authentication］が返される可能性が高くなります。

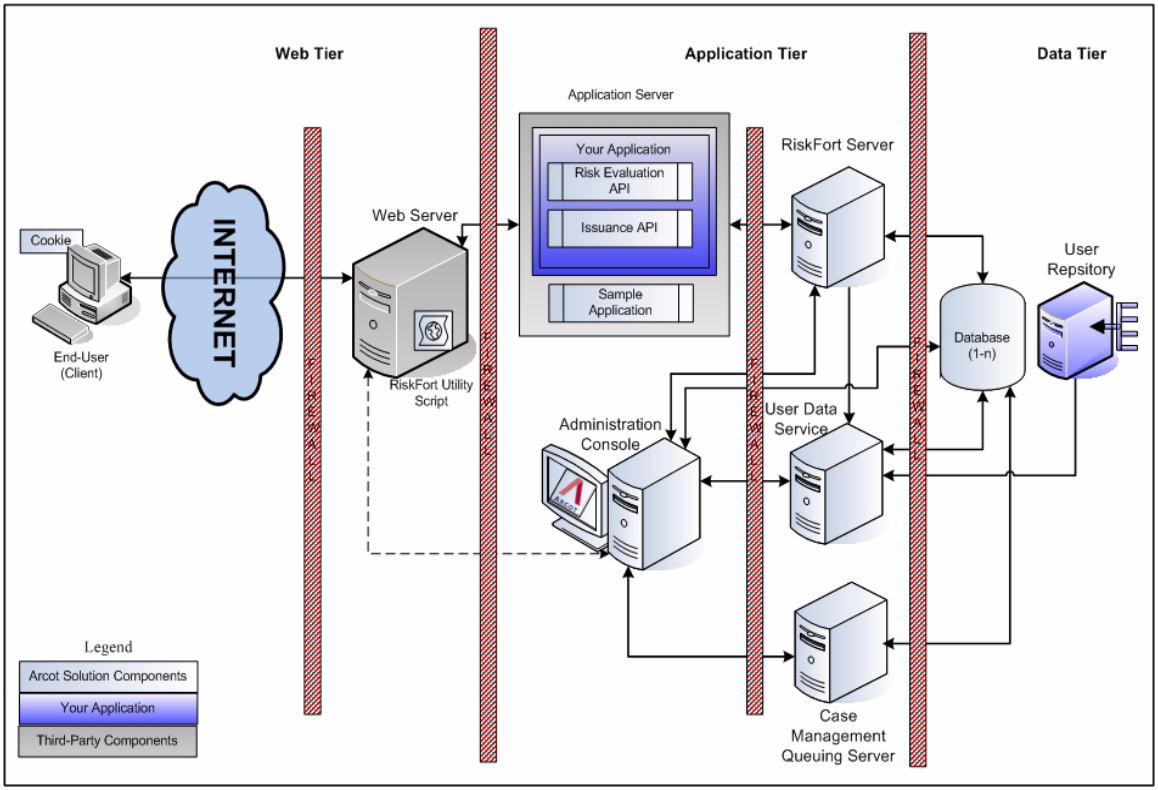
また、RiskFort では、ユーザを複数のデバイスにバインドできます。たとえば、ユーザは仕事用コンピュータと自宅のコンピュータを使用してアプリケーションにアクセスできます。同様に、単一のデバイスを複数のユーザにバインドできます。たとえば、家族全員が 1 台のコンピュータを使用してアプリケーションにアクセスできます。

RiskFort アーキテクチャ

RiskFort は単一のシステムにインストールすることも、複数のシステムにコンポーネントを分散することもできます（詳細は、このガイドの後の章で説明します）。ただし、データとトランザクションのセキュリティと整合性を最大限に高めるために、Arcot では図 1-4 に示すような、以下の 3 層を持つアーキテクチャを推奨します。

- Web 層
- アプリケーション層
- データ層

図 1-4 3 層構造の推奨 RiskFort アーキテクチャ



以下のサブセクションで、これらの層のコンポーネントについて説明します。

Web 層

この層は HTML コンテンツで構成され、ネットワークまたはインターネットを介してユーザと直接対話します。

RiskFort ユーティリティ スクリプト（`json.js`）は、アプリケーション内に含める必要のあるクライアント側 JavaScript で、この層に位置する Web サーバを通じてエンド ユーザのブラウザに提供されます。このスクリプトによって以下のことが可能です。

- エンド ユーザのシステムへのデバイス ID （cookie 形式）の設定

- デバイス DNA （MFP）情報とデバイス ID 情報の収集

関連文書： MFP、デバイス ID、およびユーティリティ スクリプトの使用方法の詳細については、「Arcot RiskFort 2.2.6 Java 開発者ガイド」の 第 5 章「デバイス ID とマシン FingerPrint の収集」を参照してください。

アプリケーション層

この層は、システム内にあるすべてのアプリケーション サーバ コンポーネントで構成されます。これには RiskFort サーバ、UDS、Administration Console、および RiskFort SDK が含まれます。

注： この層のすべてのコンポーネントは、1 つのシステムにインストールすることも、複数のシステムに分散することもできます（詳細は、2 章、3 章、および 4 章で説明します）。

- **RiskFort サーバ**

  RiskFort SDK を介したアプリケーションからのリスク評価リクエストを処理するサーバ コンポーネント

- **Case Management Queuing サーバ**

  ケースをスケジュールしてテクニカル サポート担当者（CSR）に送信し、その後これらのケースのライフサイクルを管理するサーバ コンポーネント

- **Administration Console**

  サーバ インスタンス、RiskFort コンポーネント間の通信モード、およびビジネス ルールとその対応データを設定したり、組織、管理者、およびユーザを管理したりするための Web ベースのコンソール

- **ユーザ データ サービス**

  リレーショナル データベース（RDBMS）やディレクトリ サーバ（LDAP）など、各種ユーザ リポジトリからユーザと組織に関するデータへのアクセスを提供する抽象化層

- **リスク評価 SDK**

  RiskFort サーバにリスク分析リクエストを転送する API。アプリケーションから呼び出すことができます。

- **発行 SDK**

  RiskFort にユーザを登録したり、ユーザの詳細を管理したりするために RiskFort サーバに発行リクエストを転送する API。アプリケーションから呼び出すことができます。

- **サンプル アプリケーション**

  サンプル アプリケーションは、RiskFort Java API の使用方法およびアプリケーションと RiskFort の統合方法の例を示します。また、RiskFort が正常にインストールされているかどうかや、リスク評価操作と発行操作を実行できるかどうかを確認する際にもサンプル アプリケーションを使用できます。

データ層

この層は、各トランザクションを分析するために RiskFort で使用される設定、ユーザ、および履歴データを格納するリレーショナル データベースのインスタンスで構成されます。また、この層には、ユーザの詳細の格納用に設定したディレクトリ サーバ（LDAP）も含まれます。

このリリースの新機能

RiskFort 2.2.6 リリースの主な機能と拡張機能は、以下のとおりです。

- 複数のチャネルをサポートするためのインフラストラクチャ
- 評価後の予測モデルへのフィードバックの提供
- ケース管理モジュールの拡張機能
- RiskFort コンポーネントとデータベース間の SSL ベース通信のサポート
- 以前 WAR ファイルとして公開された管理 Web サービスの RiskFort サーバへの移動
- 以前 WAR ファイルとして公開された管理 Web サービスの RiskFort サーバへの移動
- 容量チェック ルール タイプ設定の強化

複数のチャネルをサポートするためのインフラストラクチャ

RiskFort では、デフォルトで 2 つのチャネル（デフォルトおよび 3D セキュア）がサポートされています。一方、本リリースでは、インフラストラクチャが強化され、必要なチャネルをすべてサポートします。

新しいチャネルが必要な場合、新規チャネルに関連するデータのタイプに基づいて、新しいオンデマンド スキーマが提供されます。

評価後の予測モデルへのフィードバックの提供

本リリースから、評価後段階にフィードバック情報を予測モデルに送信できるようになりました。

ケース管理モジュールの拡張機能

前のリリース（2.1）では、ログイン、ワイヤ転送、またはユーザ アプリケーションによってリスク評価されているトランザクションなど、すべてのユーザ トランザクションを潜在的な事例と見なしていました。しかしこのリリースでは、**事例が生成されるのは以下の場合です**。

- トランザクションのリスク評価アドバイスが［**Increase Authentication**］と［**否認**］のいずれかである。

注： オープンしているケースがこのユーザにすでにある場合は、このトランザクションは既存のケースに追加されます。

- 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ケースに追加されます。

- 不正行為分析者がトランザクションのいくつかを不正行為の疑いがあると判断し（通常、以前に検出されたパターンに基づく）、詳しい調査が必要であるとマークした。

注： このようなトランザクションは、すでにオープンしているケースが対象ユーザにあれば、既存のケースに追加されます。

異なる 3 つのロールが、ケース管理でサポートされるようになりました。

- **キュー マネージャ**：ケース キュー設定を指定し、CSR をキューに割り当て、ケース キュー内のケースをオペレータがどの順序で処理する必要があるかを決定します。また、管理対象のケースや保留中のケースに関する統計を QM に表示できます。

注： 本リリースでは、システム内の組織ごとに、1 つのキューのみ（デフォルト キュー）がサポートされます。

- **テクニカル サポート担当者（CSR）：**以下を担当します。
  - カスタマ コールの対応。たとえば、顧客はあるトランザクションについて訴えるために電話をかけてくる場合があります。そのような場合、CSR は顧客からの入力を記録し、しかるべき処置を講じます。この記録された情報は、その後不正行為分析者が RiskFort を調整して分析を行うために使用できます。

    このケースに対してさらに処置を講じる必要がある場合、CSR は次にユーザに連絡する時間を指定することもできます。

    CSR はユーザ入力に基づいて、指定した期間、例外ユーザ リストにユーザを追加することもできます。
  - 疑わしいトランザクションの信頼性を確認するための顧客への連絡。CSR はエンド ユーザ入力に基づいて、指定した期間、例外ユーザ リストにユーザを追加することもできます。

注： CSR はログインしたり、次のケースに移動したりすると、自動的にケースに割り当てられます。

- **不正行為分析者**：ほかのオペレータや利用可能なフィルタによって収集された真実性に関するデータを使用して、トランザクションの傾向を分析します。トランザクション セットが大きい場合、分析者はデータをオフラインにエクスポートしてから、分析できます。分析者はその分析に基づいて、RiskFort の微調整に関するアドバイスをシステム管理者に提供できます。

  不正行為分析者がトランザクションを不審であると判断した場合、オペレータに対してリクエストを発行し、エンド ユーザに連絡を取ってもらい、システムでトランザクションが不審と見なされていない場合でも、疑わしいトランザクションに関する詳細をさらに調査するよう依頼できます。

本リリースは、不正行為分析者がトランザクション データの分析に使用できるフィルタを多数提供しています。これらのフィルタには、以下を表示する機能が含まれています。

- 指定された時間帯のトランザクション
- 過去 30 分や 1 時間などのトランザクション
- 指定されたリスク アドバイスが割り当てられたトランザクション
- 特定のルールが起動したトランザクション
- 2 次認証ステータスが、[Successful]、[Failed]、または [Unknown] のトランザクション
- 同一のデバイス、業者、IP アドレス、またはユーザからのトランザクション
- （3D セキュア固有）業者名が指定パターンから始まるか終わるトランザクション、または指定した単語が含まれるトランザクション

RiskFort コンポーネントとデータベース間の SSL ベース通信のサポート

RiskFort データベースと通信するすべてのコンポーネントで、双方向 SSL 通信がサポートされるようになりました。これらのユーザおよびグループは、以下のとおりです。

- RiskFort サーバ
- Administration Console
- ユーザ データ サービス
- Case Management Queuing サーバ

以前 WAR ファイルとして公開された管理 Web サービスの RiskFort サーバへの移動

以前は WAR ファイルとして公開されていた以下の管理 Web サービスは、本リリースでは RiskFort サーバに組み込まれています。

- `addUserToExceptionList`
- `deleteUserFromExceptionList`
- `getUserProfile`
- `getLocationAndConnectionInfo`

	**重要 :** ネームスペースは変更されています。そのため、これらの組み込み Web サービスを使用する場合、スタブを再構築する必要があります。ただし、コードの変更は必要ありません。

ARCOT_HOME 内の wsdls/**admin**/ ディレクトリに、付属の WSDL（ArcotRiskFortAdminWebService.wsdl）があります。これを使用して、RiskFort Web サービスと通信するための Web サービス クライアント コードを生成できます。

容量チェック ルール タイプ設定の強化

容量チェック アドオン ルール タイプを設定する際、設定用の比較演算子をドロップダウン方式で利用できるようになりました。サポートされている演算子は以下のとおりです。

- 等しい
- 等しくない
- 以上
- 以下
- より大きい
- より小さい

	**関連文書 :** この変更の詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

第 2 章
展開の計画

この章では、RiskFort の展開モデルの選択と、各システムにインストールする RiskFort コンポーネントと事前インストール ソフトウェアの決定に役立つ情報を提供します。展開計画がしやすくなるように、各展開モデルのアーキテクチャ図も示します。

注 : このガイドで、「システム」とは物理デバイスを意味します。また、「サーバ」とはシステム上で実行されるソフトウェアを意味します。

この章は以下のトピックで構成されます。

展開の概要

このセクションでは、RiskFort を展開する手順の簡単な概要と、要件に基づく展開モデルを選択するためのアドバイスを提供します。

1. 展開モデルを選択します。RiskFort は、単一のシステムにインストールするか、複数のシステムにまたがってインストールできます。

   詳細については、「展開モデルの選択」を参照してください。

2. RiskFort とそのコンポーネントのインストール先となるシステムが、すべてのハードウェア要件を満たしていることを確認します。

   詳細については、3-33 ページの「ハードウェア要件」を参照してください。

3. 事前にインストールが必要なソフトウェアをインストールします。

   詳細については、3-34 ページの「ソフトウェア要件」を参照してください。

4. SQL データベースでデータベース ユーザを作成します。

   詳細については、3-37 ページの「データベース サーバの設定」を参照してください。

5. RiskFort をインストールします。

   - 単一システム環境へのインストールの詳細については、4-47 ページの「Complete インストールの実行」を参照してください。
   - 分散環境へのインストールの詳細については、5-75 ページの「1 つ目のシステムへのインストール」を参照してください。

6. データベースの SQL スクリプトを実行して Arcot スキーマを作成し、基本の初期設定を行います。

   - 単一システム展開での SQL スクリプト実行の詳細については、4-52 ページの「データベース スクリプトの実行」を参照してください。
   - 分散展開での SQL スクリプト実行の詳細については、5-83 ページの「データベース スクリプトの実行」を参照してください。

7. ユーザ データ サービス（UDS）と Administration Console を展開します。

   - 単一システム展開での UDS と Administration Console の展開および起動の詳細については、4-53 ページの「Web アプリケーションの展開」を参照してください。
   - 分散展開での UDS と Administration Console の展開および起動の詳細については、5-84 ページの「Web アプリケーションの展開」を参照してください。

8. Master Administrator として Administration Console にログインし、コンソールを初期化します。

   - 単一システム展開での Administration Console 初期化の詳細については、4-59 ページの「Administration Console へのログイン方法」および 4-60 ページの「システムのブートストラップ」を参照してください。
   - 分散環境での Administration Console 初期化の詳細については、5-90 ページの「Administration Console へのログイン方法」および 5-91 ページの「システムのブートストラップ」を参照してください。

9. RiskFort サーバと Case Management Queuing Server を起動し、サービスが正常に動作していることを確認します。

   - 単一システム展開での Administration Console 初期化の詳細については、4-66 ページの「RiskFort サーバの起動」、4-66 ページの「Case Management Queuing サーバの開始」、および 4-67 ページの「インストールの確認」を参照してください。

- 分散環境での Administration Console 初期化の詳細については、5-97 ページの「RiskFort サーバの起動」、5-97 ページの「Case Management Queuing サーバの開始」、および 5-98 ページの「インストールの確認」を参照してください。

10. （**分散インストールの場合のみ**）残りのシステムに RiskFort をインストールします。
    - 詳細については、5-99 ページの「2 つ目のシステムへのインストール」を参照してください。
11. サンプル アプリケーションを展開、実行して、RiskFort のインストールをテストします。
    - 単一システム環境でのテスト方法の詳細については、4-68 ページの「サンプル アプリケーションの展開」および 4-69 ページの「サンプル アプリケーションの使用」を参照してください。
    - 分散環境でのテスト方法の詳細については、5-100 ページの「サンプル アプリケーションの展開」、5-101 ページの「RiskFort サーバとの通信用サンプル アプリケーションの設定」、および 5-102 ページの「サンプル アプリケーションの使用」を参照してください。

展開モデルの選択

RiskFort 展開の一部として、RiskFort サーバはインストールする必要のある主要コンポーネントです。トランザクションリスク評価などのリスク評価サービスは、RiskFort サーバによって提供されるからです。RiskFort サーバを使用する必要のあるアプリケーションは、付属の Java SDK または Web サービスを使って RiskFort サーバに統合できます。

RiskFort には、サーバ設定データ、ユーザ固有の基本設定、および使用データを格納するための SQL データベースも必要です。

通常、開発および単純なテストが目的の場合、すべての RiskFort コンポーネントは単一のシステムにインストールします。ただし、運用展開およびステージング環境の場合、RiskFort サーバは専用のシステムにインストールする必要があります。付属の SDK または Web サービスは、ユーザがログインするアプリケーションが配置された別のシステムにインストールします。

RiskFort にはサンプル アプリケーションも付属しています。これらのアプリケーションは、RiskFort が正しくインストールされているかどうかや、リスク評価を実行できるかどうかを確認するために使用できます。また、RiskFort を既存のアプリケーションに統合するためのコード サンプルとしても役立ちます。

RiskFort によってサポートされる高レベルの展開タイプは以下のとおりです。

- **単一システム展開** - 開発またはテスト用
- **分散システム展開** - 運用環境またはステージング環境用
- **高可用性展開** - 可用性および拡張性の高い、運用環境またはステージング環境用

単一システムでの展開

単一システム展開では、RiskFort のすべてのコンポーネントとユーザがログインするアプリケーションを、単一のシステムにインストールします。データベースは、RiskFort がインストールされているシステムまたは別のシステムに配置されます。

この展開モデルは一般に、開発、概念実証、または初期テストに使用されます。

単一システム展開では Java SDK と Web サービスの両方を使用することができます。これらのコンポーネントの事前インストール ソフトウェアは同じです。

単一システム展開を実行する最も単純な方法は、RiskFort インストーラの実行中に**完全インストール** オプション（詳細については、4-47 ページの「Complete インストールの実行」を参照）を選択することです。

コンポーネント図

このセクションで紹介する図は、事前インストール ソフトウェアと RiskFort コンポーネントについての展開オプション候補を示しています。**完全インストール**を実行する場合は、Java SDK と Web サービスの両方がシステム上に配置されます。この場合、いずれか 1 つまたは両方の統合方法を選択できます。

- Java SDK の展開
- Web サービスの展開

単一システム展開を計画している場合は、以下の決定をする必要があります。

決定のポイント

- RiskFort サーバが配置されているシステムにデータベース サーバをインストールするか、別のシステム上にある既存のデータベースを使用する。
- サンプル アプリケーションを使用するか、独自の Web アプリケーションを作成する。

重要 : サンプル アプリケーションを運用展開で使用*しないでください*。サンプル アプリケーションのコードを参考にして、独自の Web アプリケーションを作成することを強くお勧めします。

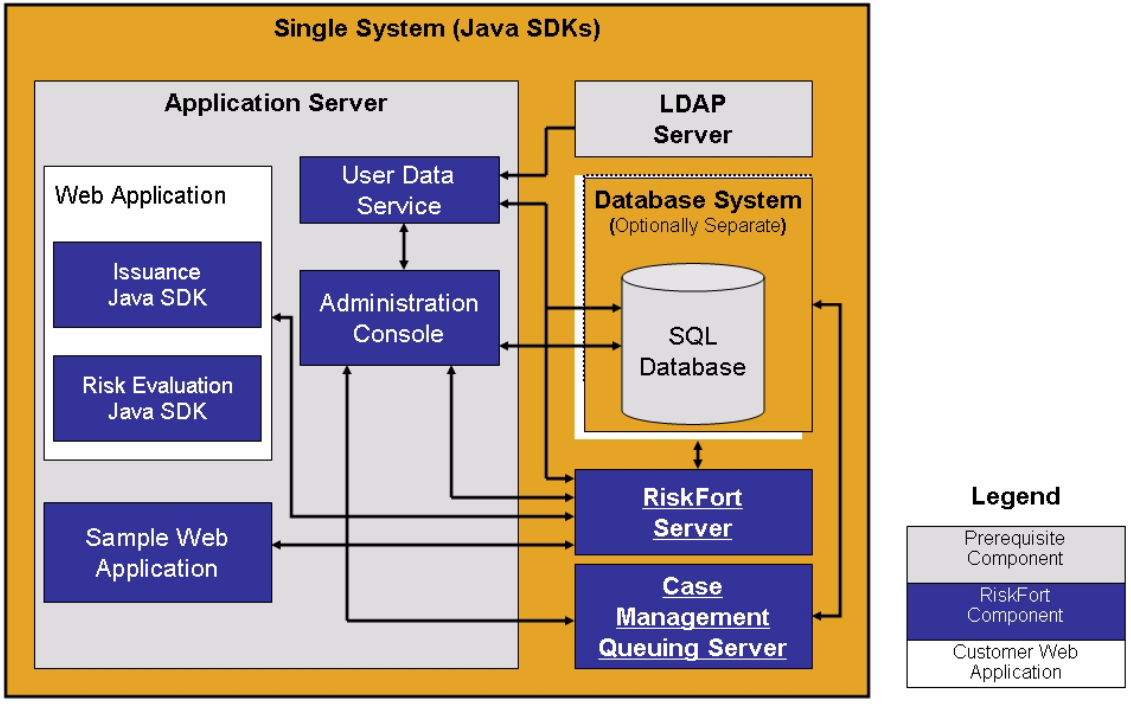
- 独自の Web アプリケーションの統合に、Java SDK または Web サービスを使用する。

以降の各セクションでは、展開の決定に役立つ情報を提供します。

Java SDK の展開

図 2-1 は、単一のシステムに展開された RiskFort サーバと Java SDK を示しています。

図 2-1 単一システム上の RiskFort（Java SDK）



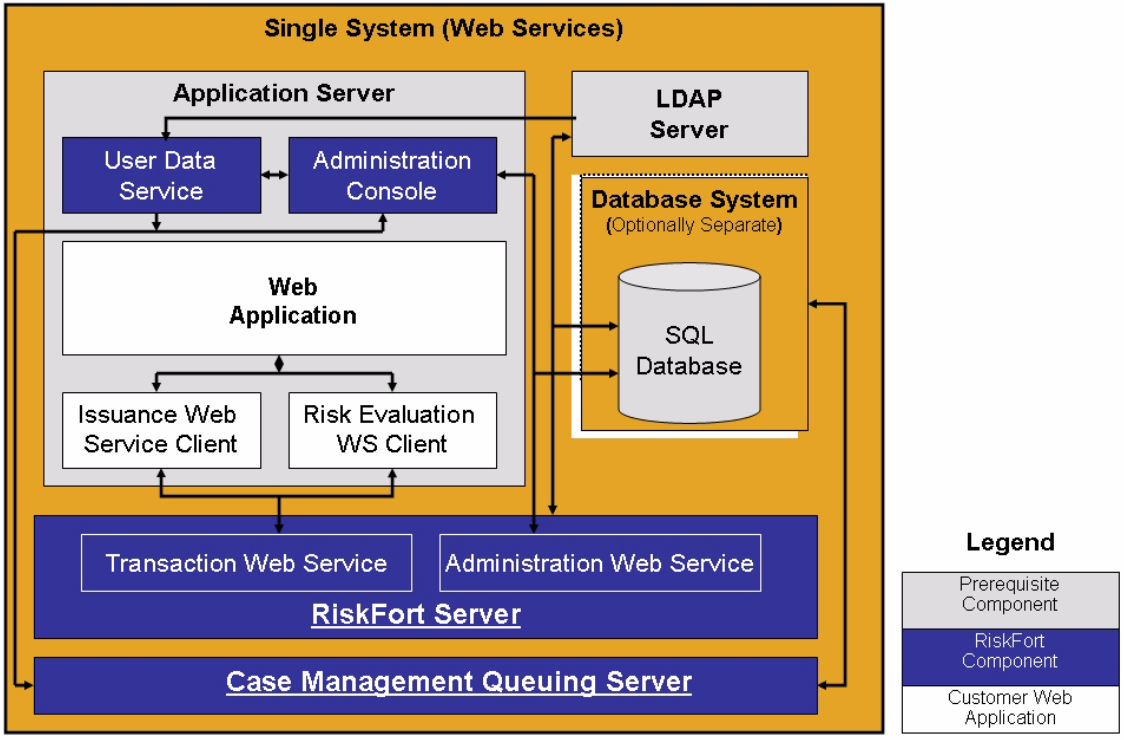
注： アプリケーション サーバの HTML ページを配信するための Web サーバの使用はオプションであり、RiskFort に対して透過的です。運用展開では、アプリケーション サーバのパフォーマンスとセキュリティを高めるため、通常はこの方法が使用されます。詳細については、アプリケーション サーバのドキュメントを参照してください。

Web サービスの展開

Web サービスを展開する場合について、図 2-2 は、単一のシステムに展開された RiskFort サーバと Web サービスを示しています。

	注： 現在すべての Web サービスは RiskFort サーバ モジュール自体に組み込まれているので、RiskFort サーバをターゲット システムにインストールし、必要なクライアント スタブを生成するだけです。追加設定は必要ありません。

図 2-2 単一システム上の RiskFort（Web サービス）



分散システムでの展開

分散システム展開では、RiskFort コンポーネントをさまざまなサーバにインストールします。その目的は、セキュリティとパフォーマンスを高めることと、複数のアプリケーションがリスク評価機能を使用できるようにすることです。

この展開モデルは通常、運用展開またはステージング環境に使用されます。

たとえば、最も一般的な展開では、1 台のシステムに RiskFort サーバをインストールし、追加システムに 1 つ以上の Web アプリケーションをインストールします。この展開は複数のシステムにまたがるため、どのシステムが相互に通信可能である必要があるかを示すアーキテクチャ図が追加されます。

分散システム展開を実行するには、RiskFort インストーラで［**Custom**］インストールオプション（詳細については、5-75 ページの「1 つ目のシステムへのインストール」を参照）を選択する必要があります。

このセクションでは、高可用性展開のコンポーネント図とアーキテクチャ図について説明します。

- コンポーネント図
- アーキテクチャ図

コンポーネント図

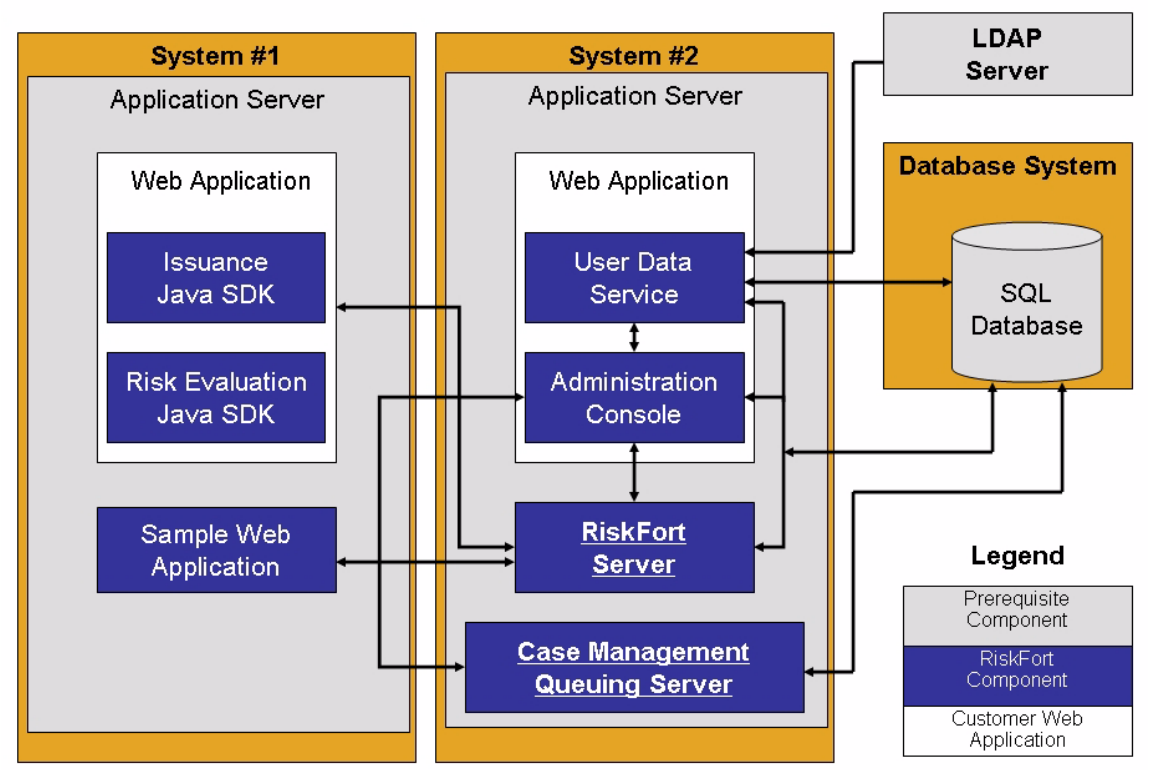
このセクションで紹介する図は、事前インストール コンポーネントと RiskFort コンポーネントを複数のシステムにインストールする場合の、いくつかのオプション候補を示しています。

- Java SDK を使用した単一アプリケーションの展開
- Java SDK を使用した複数アプリケーションの展開
- Web サービスを使用した単一アプリケーションの展開

Java SDK を使用した単一アプリケーションの展開

図 2-3 は、単一のアプリケーションに Java SDK を使用する RiskFort 展開を示しています。

図 2-3 分散システム上の RiskFort（単一アプリケーションとしての Java SDK）

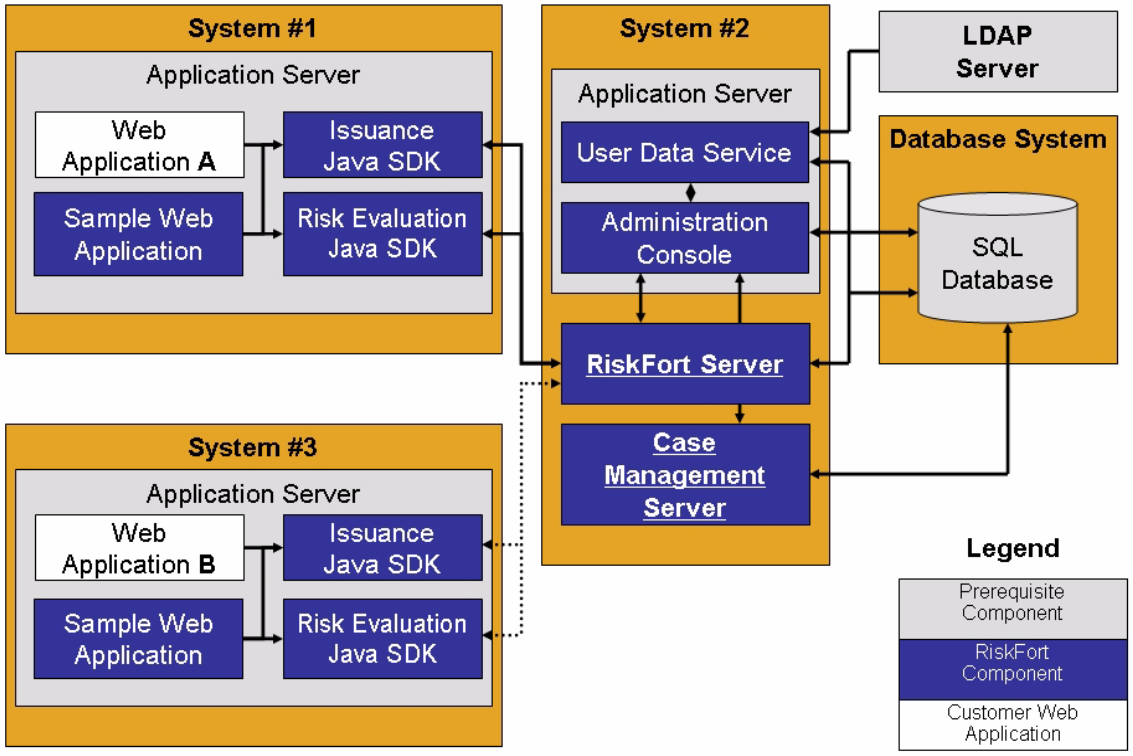


注： Administration Console は、任意の個別のシステム、すべてのシステム、または図に示されていないシステムにインストールできます。

Java SDK を使用した複数アプリケーションの展開

図 2-4 は、複数のアプリケーションに Java SDK を使用する RiskFort 展開を示しています。

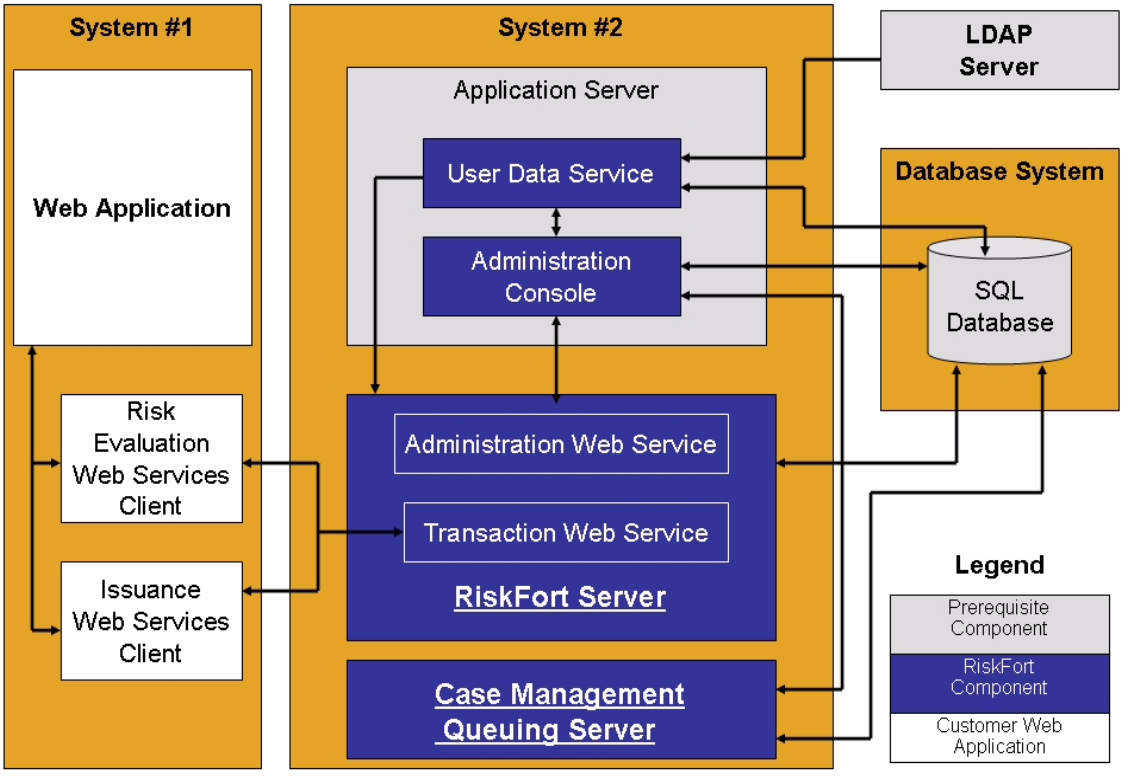
図 2-4 分散システム上の RiskFort（複数アプリケーションとしての Java SDK）



Web サービスを使用した単一アプリケーションの展開

図 2-5 は、単一アプリケーションに Web サービスを使用する RiskFort 展開を示しています。

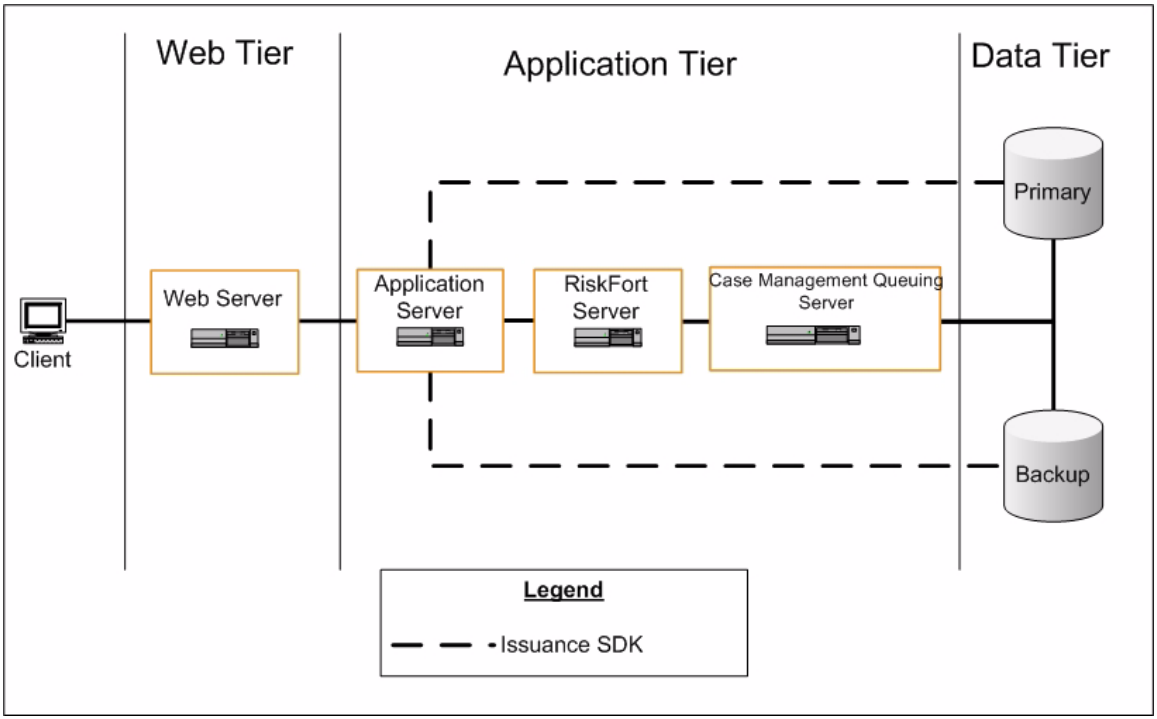
図 2-5 分散システム上の RiskFort（単一アプリケーションとしての Web サービス）



アーキテクチャ図

図 2-6 は、分散システム展開のアーキテクチャ図を示しています。

図 2-6 分散アーキテクチャ図



注： ネットワーク アーキテクチャに基づいて、必要に応じてロード バランサを使用できます。

決定：

どの RiskFort コンポーネントを各システムにインストールするのか。

高可用性環境での展開

高可用性展開では、高可用性と拡張性を実現するため、RiskFort コンポーネントを 2 台以上のサーバにインストールします。

このセクションでは、高可用性環境における展開のコンポーネント図とアーキテクチャ図について説明します。

- コンポーネント図
- 高可用性アーキテクチャ図

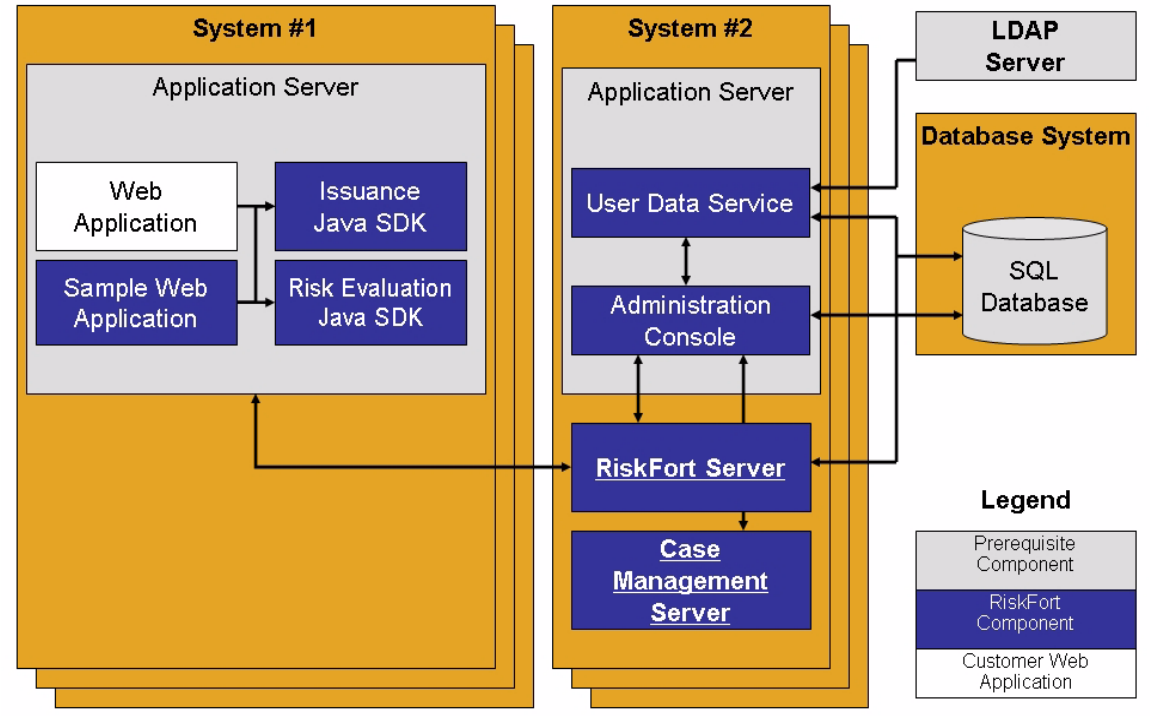
コンポーネント図

このセクションで紹介する図は、事前インストール コンポーネントと RiskFort コンポーネントを高可用性展開用の複数のシステムにインストールする場合の、いくつかのオプション候補を示しています。

Java SDK を使用した高可用性展開

図 2-7 は、Java SDK を使用した、RiskFort の複数インスタンス展開を示しています。

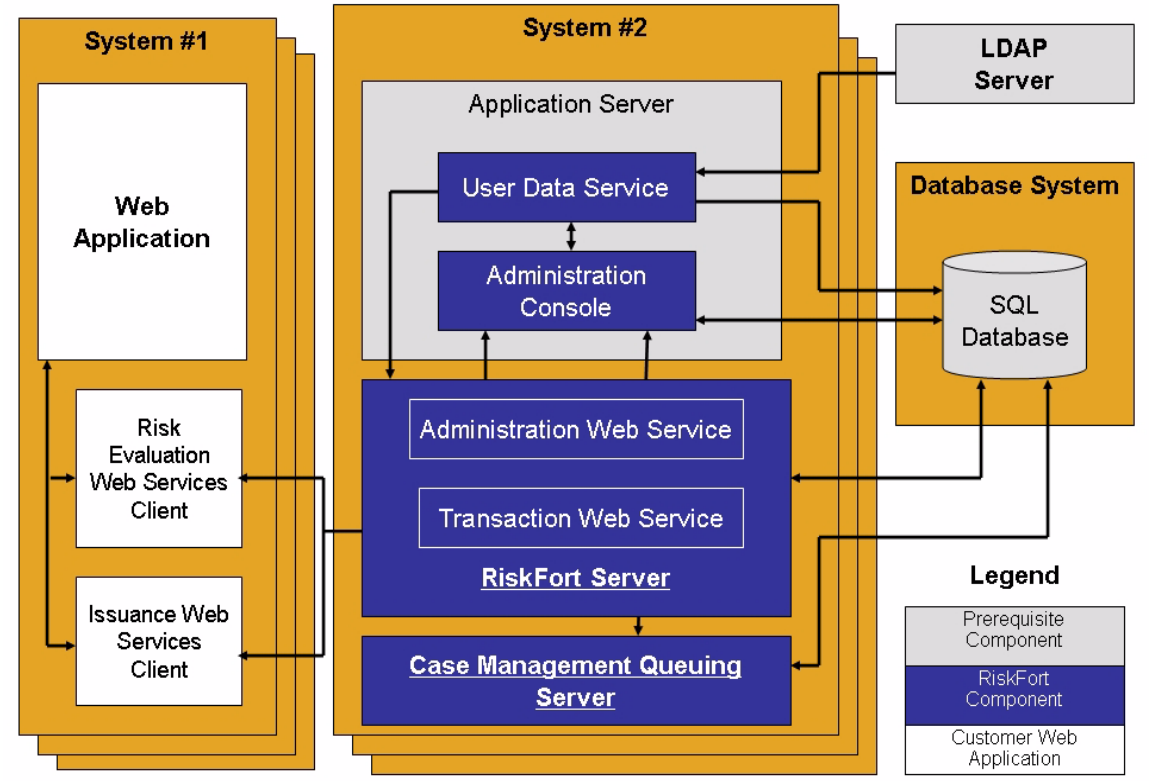
図 2-7 高可用性環境における RiskFort（Java SDK）



Web サービスを使用した高可用性展開

図 2-8 は、Web サービスを使用した、RiskFort の複数インスタンス展開を示しています。

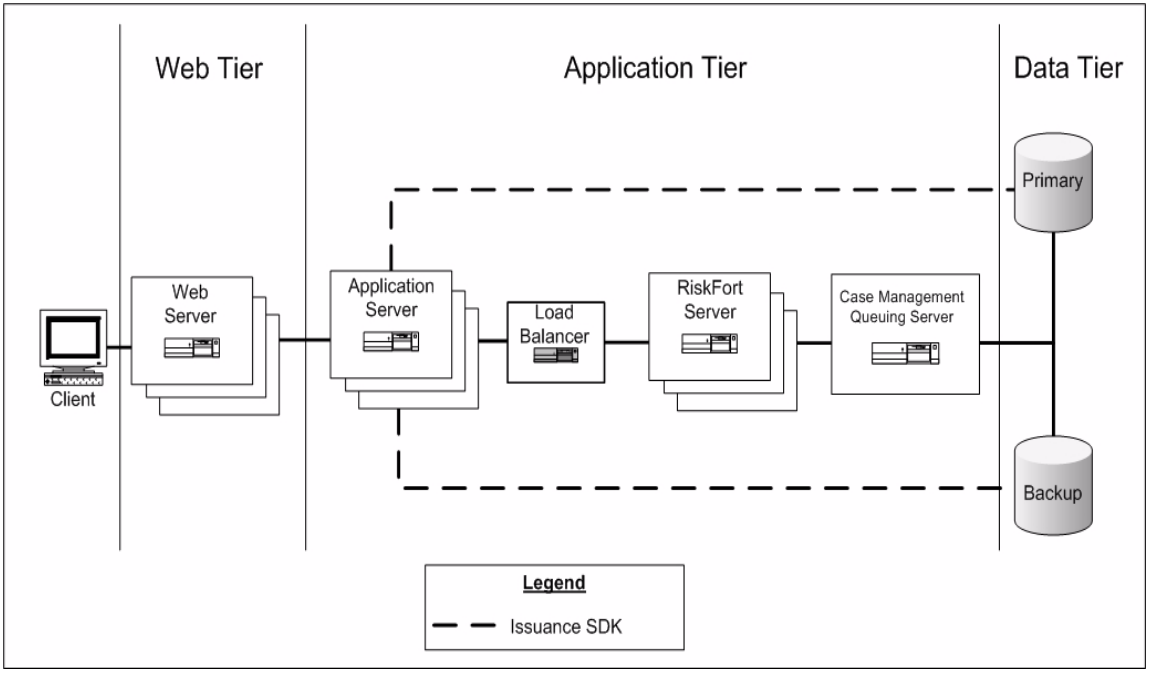
図 2-8 高可用性環境における RiskFort（Web サービス）



高可用性アーキテクチャ図

図 2-9 は、複数インスタンス展開のアーキテクチャ図を示しています。

図 2-9 高可用性アーキテクチャ図



第 3 章
インストールの準備

RiskFort サーバとそのコンポーネントをインストールする前に、使用しているコンピュータがこの章で説明されている要件を満たしていることを確認してください。この章では設定と計画に関連する情報も提供します。

この章は以下のセクションで構成されます。

ハードウェア要件

RiskFort をインストールするための最小ハードウェア要件は以下のとおりです。

- RiskFort とデータベースを単一のシステムに配置する場合の要件
  - **RAM**：2 GB
  - **ハード ドライブ領域**：10 GB
  - **プロセッサ**：2.4 GHz
- RiskFort とデータベースを別々のシステムに配置する場合の要件
  - **RAM**：1 GB
  - **ハード ドライブ領域**：300 MB
  - **プロセッサ**：2.4 GHz

注： リソースの要件は、アプリケーションの種類や使い方のパターンに応じて大きく変わります。インストールに必要な最適メモリ量を決定するには、サイトの負荷テストを実施することを強くお勧めします。負荷テスト中、メモリを監視するための一部のオペレーティング システム ユーティリティでは、メモリ使用量が実際より多く報告される場合があることに留意してください（共有メモリも含まれることが理由の 1 つにあります）。メモリ要件を決定するために推奨される方法は、負荷テストで RAM/ 物理メモリを追加した後にパフォーマンスの向上を監視することです。テスト目的でメモリおよびプロセッサ リソースを構成する方法については、プラットフォーム ベンダーのドキュメントを参照してください。

ソフトウェア要件

このセクションで示すソフトウェア要件の情報は以下のとおりです。

- 最小ソフトウェア要件
- RiskFort コンポーネント別の事前インストール ソフトウェア

最小ソフトウェア要件

このセクションでは、以下のバージョンの Solaris および Linux でサポートされるソフトウェアを示します。このセクションで示すソフトウェア要件の情報は以下のとおりです。

- Solaris SPARC
- Red Hat Enterprise Linux

Solaris SPARC

表 3-1 に、RiskFort をインストールするために最低限必要なソフトウェアを示します。

注： 表 3-1 に示すすべてのサードパーティ ソフトウェアについて、サポートされている指定のバージョンと、それより高いバージョンとは、互換性のあることが前提となっています。

表 3-1. Solaris SPARC の最小ソフトウェア要件

ソフトウェアのタイプ	バージョン
オペレーティング システム	Solaris 10（SPARC）
パッチ	最新のパッチ *http://sunsolve.sun.com* にアクセスし、［**Patches and Updates**］リンク、［**Patch Cluster & Patch Bundle Downloads**］リンクの順にクリックします。［**Solaris Patch Clusters**］で［**Recommended Patch Clusters**］を展開して、Solaris 10 SPARC 05/08 Patch Bundle のエントリを表示します。
データベース サーバ	• **サーバ**：Oracle 10*g* 以上 • **クライアント**：Oracle 10*g* 以上
ディレクトリ サーバ	以下のディレクトリ サーバがサポートされています。 • SunOne Directory Server 5.2 • SunOne Directory Server 6.1
アプリケーション サーバ	以下のアプリケーション サーバがサポートされています。 • Apache Tomcat 5.5.23 以上（*http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/*） • IBM WebSphere 6.1 以上 • BEA WebLogic 10 以上
JDK	使用しているアプリケーション サーバと最も互換性のある JDK バージョン。 **注：** JDK を新規インストールする場合は、`JAVA_HOME` 環境変数に新しいパスを追加する必要があります。パスを追加しなかった場合、Administration Console および他の JDK 依存コンポーネントが起動しない可能性があります。

Red Hat Enterprise Linux

表 3-2 に、RiskFort をインストールするために最低限必要なソフトウェアを示します。

注： 表 3-2 に示すすべてのサードパーティ ソフトウェアについて、サポートされている指定のバージョンと、それより高いバージョンとは、互換性のあることが前提となっています。

表 3-2. RHEL の最小ソフトウェア要件

ソフトウェアのタイプ	バージョン
オペレーティング システム	Red Hat Enterprise Linux 4.0（x86） Red Hat Enterprise Linux 5.0（x86）
更新	Update 1 以上
パッチ	最新のパッチ *http://www.redhat.com* にアクセスし、自分のアカウントにログインします。必要に応じて、最新の更新とパッチをダウンロードし、適用します。
データベース サーバ	• **サーバ**：Oracle 10*g* 以上 • **クライアント**：Oracle 10*g* 以上
ディレクトリ サーバ	以下のディレクトリ サーバがサポートされています。 • SunOne Directory Server 5.2 • SunOne Directory Server 6.1
アプリケーション サーバ	以下のアプリケーション サーバがサポートされています。 • Apache Tomcat 5.5.23 以上（*http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/*） • IBM WebSphere 6.1 以上 • BEA WebLogic 10 以上
JDK	使用しているアプリケーション サーバと最も互換性のある JDK バージョン。 **注：** JDK を新規インストールする場合は、`JAVA_HOME` 環境変数に新しいパスを追加する必要があります。パスを追加しなかった場合、Administration Console および他の JDK 依存コンポーネントが起動しない可能性があります。

RiskFort コンポーネント別の事前インストール ソフトウェア

事前インストール ソフトウェアは、システムにインストールする RiskFort コンポーネントによって異なります。展開のタイプ別にどの RiskFort コンポーネントをインストールするべきかを判断するには、第 2 章の「展開の計画」を参照してください。

表 3-3 に、各 RiskFort コンポーネントで必要とされる事前インストール ソフトウェアを示します。

表 3-3. RiskFort コンポーネントの事前インストール ソフトウェア

コンポーネント	事前インストール ソフトウェア		
	データベース クライアント	JDK	アプリケーション サーバ
RiskFort サーバ	✓		
Case Management Queuing サーバ	✓		
Administration Console		✓*	✓
リスク評価 Java SDK		✓*	✓
発行 Java SDK		✓*	✓
管理 Web サービス		✓*	✓
トランザクション Web サービス		✓*	✓
サンプル アプリケーション		✓*	✓

データベース サーバの設定

RiskFort をインストールする前に、ユーザ情報、サーバ設定データ、監査ログ データ、およびその他の情報を格納するためのデータベースを設定する必要があります。

RiskFort では、プライマリ データベースと共に、高可用性展開でのフェイルオーバ時とフェイルバック時に使用できるバックアップ データベースも使用できます。データベース接続は以下のいずれかの方法で設定できます。

- RiskFort のインストール中に設定する
- arcotcommon.ini ファイルを手動で編集して設定する

サポートされるデータベース（Oracle）ごとに、特定の設定要件があります。データベース サーバを自分で設定する場合は、以下の情報を使用してください。あるいは、データベース アカウントを要求するとき、データベース管理者（DBA）に以下の情報を提供してください。

重要 : データベースを保護するため、データベース サーバについて、ファイアウォールまたは他のアクセス制御メカニズムで保護することと、すべての Arcot 製品と同じタイム ゾーンに設定することを強くお勧めします。

- Oracle データベースの設定

Oracle データベースの設定

このセクションでは、Oracle データベースおよび RiskFort サーバ用の設定情報を示します。

注 : 以下のセクションに示すタスクの実行の詳細については、Oracle データベースのドキュメントを参照してください。

必要なテーブルスペース

Oracle に対して RiskFort を実行するには 2 つのテーブルスペースが必要です。

- 1 つ目のテーブルスペースは、設定データ、監査ログ、およびユーザ情報の格納に使用されます。このテーブルスペースは、Arcot データベース内でデフォルトのユーザ テーブルスペースにすることができます。

  データベースの作成については、「新規データベースの作成」を参照してください。
- 2 つ目のテーブルスペースはレポートの実行に使用されます。パフォーマンスを高めるため、このテーブルスペースを 1 つ目とは別個のテーブルスペースにすることをお勧めします。

Arcot データベース設定スクリプト

Arcot データベース設定スクリプト arcot-db-config-for-common-1.0.sql は、これを実行するデータベース ユーザがテーブルスペースを作成するための十分な権限を持っている場合、レポートのテーブルスペースを自動的に作成します。必要な権限がユーザにない場合、DBA はこのテーブルスペースを手動で作成し、レポートのテーブルスペースを作成するセクションをスクリプトから削除する必要があります。

重要 : レポートのテーブルスペースを作成するための arcot-db-config-for-common-1.0.sql データベース スクリプト内のパラメータは、DBA の希望どおりに変更できます。ただし、レポートを正常に生成するには、テーブルスペース名を ARRFReports にする必要があります。

Oracle データベースを設定するには、以下の手順に従います。

1. 新規データベースの作成
2. データベース ユーザの作成

新規データベースの作成

UTF-8 文字セットで情報を格納する新しいデータベースを作成します（推奨される名前は arcotdb）。この文字セットにより、RiskFort では、ダブルバイト言語を含む国際的な文字を使用できるようになります。

データベース ユーザの作成

以下の条件に従ってユーザを作成します。

1. 新しいデータベース arcotdb のスキーマを使用して、ユーザを作成します（推奨される名前は arcotuser）。
2. 開発またはテスト用の展開では、ユーザのクォータを少なくとも 5 ～ 10 GB に設定します（主に監査ログに使用されます）。

注 : 運用、ステージング、または他の負荷の高いテスト用の展開の場合、ユーザに必要なクォータを決定する方法については、付録 C の 「データベース リファレンス」を参照してください。

3. ユーザに CONNECT 権限と RESOURCE 権限を付与します。
4. ユーザに CREATE TABLESPACE 権限を付与します。

5. ユーザに CREATE TABLE 権限を付与します。
6. ユーザに ALTER EXTENT PARAMETERS 権限を付与します。
7. ユーザに LOB 列の拡張記憶域を変更する権限を付与します。

インストールの準備

RiskFort のインストールに入る前に、RiskFort データ ストア（データベース クライアント）を設定し、後でインストール中に必要になるデータベース情報を収集する必要があります。また、RiskFort コンポーネントによって必要とされる、前提条件となる JDK バージョンとアプリケーション サーバがインストールされていることを確認する必要もあります。

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。

- RiskFort のインストールに必要なデータベース情報
- Java 依存コンポーネントの要件

RiskFort のインストールに必要なデータベース情報

このセクションで説明するタスクを、RiskFort のインストール先となるシステムまたは RiskFort コンポーネントを使用するシステムで実行します。

Oracle データベース

DBA から以下のデータベース情報を入手します。この情報は RiskFort のインストール時に必要になります。

1. **サービス ID**（Oracle データベースのインスタンス識別子）
2. **ホスト名**
3. **ポート番号**
4. **ユーザ名**
5. **パスワード**

これらのパラメータの詳細については、手順 11（4-49 ページ）を参照してください。

Java 依存コンポーネントの要件

Administration Console、RiskFort Java SDK、および Web サービスによって必要とされる以下のコンポーネントをインストールします。

- **JDK**

注： JDK を新規インストールする場合は、JAVA_HOME 環境変数を設定する*必要があります*。path 変数は $JAVA_HOME/**bin**/ を参照している必要があります。パスを追加しなかった場合、Administration Console および他の JDK 依存コンポーネントが起動しない可能性があります。

- アプリケーション サーバ

重要： Oracle データベース サーバと RiskFort コンポーネントを同じシステムにインストールする単一システム展開を実行する場合は、Apache Tomcat のデフォルト ポート（8080）を変更します。この変更により、ポート 8080 上での Oracle データベース サーバとの競合が回避されます。

インストール前チェックリスト

RiskFort のインストールと設定に入る前に、以下のチェックリストを確認することをお勧めします。

表 3-4. インストール前チェックリスト

ユーザ情報	入力例	ユーザ欄
ハードウェア		
プロセッサ	SPARC	
RAM	2 GB	
ディスク容量	20 GB	
ソフトウェア		
オペレーティング システム	Solaris 10	
ディストリビューション	Enterprise Edition	
Service Pack（またはパッチ）	SP3	

表 3-4. インストール前チェックリスト

ユーザ情報	入力例	ユーザ欄
データベース		
タイプ	Oracle	
DSN 名	arcotdsn	
ホスト名（またはサーバ）	arcotdsn	
ポート（Oracle データベースのみ）	1521	
サービス ID（Oracle データベースのみ）	oradb1	
ユーザ名	rfdbadmin	
パスワード	password1234!	
設定されている権限：		
CREATE TABLE	，	
CREATE INDEX	，	
CREATE PROCEDURE	，	
REFERENCES	，	
DML 権限	，	
RESOURCE 権限（Oracle データベースのみ）	，	
CONNECT 権限（Oracle データベースのみ）	，	
ALTER EXTENT PARAMETERS（Oracle データベースのみ）	，	
CREATE TABLESPACE（Oracle データベースのみ）	，	
UNLIMITED TABLESPACE（Oracle データベースのみ）	，	
DROP TABLESPACE（Oracle データベースのみ）	，	
アプリケーション サーバ		
タイプ	Apache Tomcat 5.5	
ホスト名	localhost	
ポート	8080	

表 3-4. インストール前チェックリスト

ユーザ情報	入力例	ユーザ欄
JDK	1.5.0_10	
ディレクトリ サービス		
ホスト名	ds.myldap.com	
ポート	389	
スキーマ名	inetorgperson または user	
ベース識別名	dc=myldap,dc=com	
ユーザ名	cn=admin,cn=Administrators,cn=dscc	
パスワード	mypassword1234!	
WEB サーバ（オプション）		
タイプ	IIS 6	
ホスト名	mywebserver.com	
ポート	443	

第 4 章
単一システムへの RiskFort の展開

RiskFort コンポーネントのインストールは、**Arcot RiskFort** 2.2.6 **InstallAnywhere ウィザード**を使用して実行します。このウィザードでは *Complete* と *Custom* のインストールタイプをサポートしています。ただし、単一のコンピュータ上に RiskFort をインストールして設定する場合、インストーラを実行する際に **Complete** オプションを使用する必要があります。

以下の手順は、プロセスの概要です。

1. RiskFort インストーラを実行し、RiskFort コンポーネントをインストールして、SQL データベースにアクセスするようコンポーネントを設定します。

   インストールの手順については、「Complete インストールの実行」を参照してください。

2. データベース スクリプトを実行し、RiskFort スキーマおよびデータベース テーブルを作成します。また、データベースが正常に設定されていることを確認します。

   詳細については、「データベース スクリプトの実行」、および「データベースの設定の確認」を参照してください。

3. アプリケーション サーバに Web アプリケーション（UDS および Administration Console）を展開し、展開を確認します。

   詳細については、「Web アプリケーションの展開」を参照してください。

4. Master Administrator クレデンシャルで Administration Console にログインし、RiskFort を初期化します。

   詳細については、「Administration Console へのログイン方法」および「システムのブートストラップ」を参照してください。

5. RiskFort サーバおよび Case Management Queuing サーバを起動し、サービスが正常に開始するかどうかを確認します。

   詳細については、「RiskFort サーバの起動」、「Case Management Queuing サーバの開始」、および「インストールの確認」を参照してください。

6. （オプション）RiskFort コンポーネント間の安全な通信を確保するために、SSL（Secure Socket Layer）トランスポート モードをサポートするよう設定できます。

   詳細については、付録 F の 「SSL の設定」を参照してください。

7. サンプル アプリケーションを展開し、これを使用して RiskFort 設定をテストします。

注： サンプル アプリケーションは、Complete 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。

詳細については、「サンプル アプリケーションの展開」および「サンプル アプリケーションの使用」を参照してください。

8. インストール チェックリストを完了します。

詳細については、「インストール後のチェックリスト」を参照してください。

インストールに関する重要な注意事項

単一のシステムまたは分散環境に RiskFort をインストールする際、以下の点に注意してください。

- *<install_location>* には特殊文字が含まれないようにしてください（~ !@ # $ % ^ & * ( ) _ + = { }[ ] ' " など）。
- RiskFort 2.2.6 は、旧バージョン（1.7 以前）からのアップグレードをサポートしていません。また、以前にインストールしたバージョンの上に RiskFort 2.2.6 をインストールすることはできません。
- 現時点では、インストーラを使用して RiskFort コンポーネントを変更または修復することはできません。必ずコンポーネントをアンインストールしてから、再インストールしてください。
- インストールの実行中は、インストーラ ウィンドウを閉じないでください。インストール中（特に最後の段階）に［**Cancel**］ボタンをクリックしてインストールを中止した場合、それまでに作成されたディレクトリはすべてが削除されるとは限りません。インストール ディレクトリ、*<install_location>*/arcot/、およびそのサブディレクトリを手動でクリーンアップする必要があります。

Complete インストールの実行

Complete インストールでは、RiskFort パッケージのコンポーネントをすべてインストールできます。これらのコンポーネントには、RiskFort サーバ、および RiskFort 用に使用するデータベースの設定に必要なスクリプトが含まれます。

注： インストールを実行する前に、第 3 章の「インストールの準備」の説明に従って、前提条件となるソフトウェア コンポーネントがすべてインストールされ、データベースが設定されていることを確認してください。

RiskFort コンポーネントをインストールするには、以下の手順に従います。

1. ログインし、インストーラを解凍したディレクトリに移動します。
2. 以下のようにインストーラを実行します。
   - **Solaris の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Solaris-Installer.bin
     ```

   - **Linux の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Linux-Installer.bin
     ```

   `root` ログインでインストーラを実行すると、警告メッセージが表示されます。続行する場合は「**Y**」を入力し、インストールを終了する場合は「**N**」を入力します。

   インストーラ画面を終了した場合は、再度インストーラを実行する必要があります。
3. **Enter** キーを押して続行します。

   セットアップ画面が表示されます。
4. **Enter** キーを押してインストールを続行します。

   ［License Agreement for RiskFort］が表示されます。
5. ［License Agreement］画面で以下を実行します。
   a. テキストをよく読み、**Enter** キーを押してライセンス テキストの次の画面を表示します。使用許諾契約書のすべてのテキストが表示されるまで、**Enter** キーを複数回押す必要がある場合があります。

      使用許諾契約書の最後で、使用許諾契約書の条項への同意を求めるプロンプトが表示されます（**DO YOU ACCEPT THE TERMS OF LICENSE AGREEMENT?**）。

b. 使用許諾契約書に同意する場合は、「**Y**」を入力してインストールを続行します。

> **注 :** 「**N**」を入力すると、警告メッセージが表示され、インストールが中止されます。

［Choose Installation Location］画面が表示されます。

6. 画面の指示に従って、以下のいずれかを実行します。
   - RiskFort をインストールするディレクトリの絶対パスを入力し、**Enter** キーを押して続行します。

     > **注 :** 指定するインストール ディレクトリ名にはスペースを含めないでください。スペースを含めると、RiskFort スクリプトとツールの一部が想定どおりに機能しない場合があります。

     または
   - **Enter** キーを押して、インストーラによって表示されたデフォルトのディレクトリを受け入れます。

   RiskFort でサポートされるインストール オプションが表示されます。
7. インストールを実行しているコンピュータに既存の Arcot 製品がすでにインストールされている場合、インストーラに以下のオプションが表示されます。
   - **1** - 新しい場所を入力する。
   - **2** - 手順 6 で選択したディレクトリへのインストールを続行する。
   - **3** - 既存の Arcot 製品がインストールされている場所を使用する。
8. 必要なオプションを選択し、**Enter** キーを押してインストールを続行します。

   > **注 :** オプション **1** または **2** を選択した場合、指定された場所に `arcot` という新しいディレクトリが作成されます。

［Installation Type］画面が表示されます。この画面には、RiskFort でサポートされているインストールのタイプ（**Complete** または **Custom**）が表示されます。
9. デフォルトの（**Complete**）オプションを選択して RiskFort のすべてのコンポーネントをインストールする場合は「**1**」を入力し、**Enter** キーを押して続行します。

［Database Type］画面が表示されます。この画面には、RiskFort でサポートされているデータベースの種類がリスト表示されます。

10. 選択するデータベースに対応する数字を入力し、**Enter** キーを押して続行します。

    ［Primary Database Access Configuration］画面が表示されます。

11. ［Primary Database Access Configuration］画面で、表 4-1 のリストに記載された情報を指定します。

表 4-1. プライマリ DSN パラメータ

パラメータ	説明
Primary ODBC DSN	インストーラによって、RiskFort がデータベースへの接続に使用する ODBC 接続が作成されます。 推奨される入力値は `arcotdsn` です。
User Name	RiskFort がデータベースにアクセスする際のデータベース ユーザ名。この名前は、データベース管理者によって指定されます。 **注：** ユーザ名はプライマリ DSN とバックアップ用 DSN とで *異なっている必要があります。*
Password	上記のフィールドで指定した**ユーザ名**に関連付けられたパスワード。RiskFort がデータベースにアクセスする際に使用されます。このパスワードは、データベース管理者によって指定されます。
Service ID	サーバ上で実行される Oracle データベースのインスタンスを表す Oracle システム識別子（SID）
Port No	データベースが受信リクエストをリスンするポート。 **注：** デフォルトのポートをそのまま使用する場合は、**Enter** キーを押します。
Host Name	RiskFort データストアのホスト名または IP アドレス **構文**：*<server_name>* **例**：`demodatabase`

［Backup Database Access Configuration］画面が表示されます。

12. ［Backup Database Access Configuration］画面で以下を実行します。

    - 入力を求められたら、「**N**」を入力してセカンダリ DSN の設定をスキップし、**Enter** キーを押して次の画面に進みます。

      または

- 入力を求められたら、「**Y**」を入力してセカンダリ DSN を設定し、**Enter** キーを押して続行します。

  実行するタスクの詳細については、表 4-1 を参照してください。

［Pre-Installation Summary］画面が表示されます。この画面には、製品の詳細、インストール ディレクトリ、インストールの種類、インストールされるコンポーネント、およびディスク領域に関する情報がリスト表示されます。

13. 表示された製品の詳細をよく確認し、**Enter** キーを押してインストールを続行します。ここまでの画面のいずれかで設定を変更する場合は、その画面に戻るまで「**back**」と入力し、必要な変更を加え、**Enter** キーを押して次の画面に進みます。

    ［Installing］画面が表示されます。これには数分かかる場合があります。その間、インストーラによって以下が実行されます。

    - すべてのコンポーネントおよび関連するバイナリがインストール ディレクトリに配置されます。
    - データベース設定が arcotcommon.ini ファイルに格納され、パスワードが `securestore.enc` ファイルに格納されます。
    - 必要な INI ファイルに書き込みが行われます。
    - 発行と Administration Console の `JNI_LIBRARY_PATH` や、`ODBC_HOME`、`ODBCINI`、`ORACLE_HOME`、`ORACLE_LIB_PATH` などの環境変数を `arctenv` ファイル内に設定します。
    - 前の画面で指定したとおり、`odbc.ini` ファイル内の選択された ODBC ドライバを使用して、プライマリ DSN およびバックアップ用 DSN （選択され設定されている場合）を作成または上書きします。

    上記のタスクが正常に完了すると、［Installation *Complete*］画面が表示されます。

14. **Enter** を押してインストーラを終了します。

    プロンプトが再度表示されるまで（インストーラが一時ファイルをクリーンアップするまで)、数分かかる場合があります。

15. インストール ログ ファイルを確認します。ファイルは *`<install_location>`*`/`**`arcot`**`/` ディレクトリにあります。

注： インストールが完了したら、「インストール後のタスクの実行」の説明に従ってインストール後のタスクを実行してください。

インストール ログ

インストール後、以下のディレクトリでインストール ログ ファイル（Arcot_RiskFort_InstallLog.log）にアクセスできます。

```
<install_location>/arcot/logs/
```

何らかの理由でインストールが失敗した場合、インストールを実行したのと同じ場所にエラー ログが生成されます。

インストール後のタスクの実行

このセクションでは、RiskFort のインストール後に実行する必要があるインストール後のタスクについて説明します。これらの手順は RiskFort を正常に設定するために必要で、以下の順序で実行する必要があります。

1. データベース スクリプトの実行
2. データベースの設定の確認
3. Web アプリケーションの展開
4. Administration Console へのログイン方法
5. システムのブートストラップ
6. RiskFort サーバの起動
7. Case Management Queuing サーバの開始
8. インストールの確認
9. サンプル アプリケーションの展開
10. サンプル アプリケーションの使用

注： これらのインストール後のタスクを完了した後に、第 6 章の「RiskFort SDK と Web サービスの設定」の説明に従って、SDK および Web サービス設定タスクを実行してください。

データベース スクリプトの実行

重要 : このセクションで説明されるスクリプトを実行する前に、第 3 章の「データベース サーバの設定」セクションで作成したときと同じデータベース ユーザとしてログインしていることを確認してください。

RiskFort には、RiskFort データベースに必要なテーブルを作成する際に必要なスクリプトが付属されています。必要なデータベース スクリプトを実行するには、以下の手順に従います。

1. 以下のディレクトリに移動します。

   <install_location>/arcot/**dbscripts**/

2. 使用しているデータベースに応じて、に移動します。

   - **Oracle の場合 :**

   <install_location>/arcot/dbscripts/**oracle**/

3. 以下の順序でスクリプトを実行します。

   - arcot-db-config-for-common-1.0.sql
   - arcot-db-config-for-riskfort-2.2.6.sql

データベースの設定の確認

必要なデータベース スクリプトの実行後、RiskFort スキーマが正常にシードされたかどうかを確認する必要があります。以下の手順に従ってください。

1. SYSDBA 特権を持つユーザとして RiskFort データベースにログインします。
2. 以下のクエリを実行します。

```
SELECT SERVERNAME, VERSION FROM ARRFSERVERS;
```

   上記のクエリの結果、以下の出力が表示されます。

```
SERVERNAME                    VERSION
-------------------------  ----------------
RiskFort                      2.2.6
RiskFortCaseManagement        2.2.6
```

3. データベース コンソールからログアウトします。

Web アプリケーションの展開

RiskFort の 2 つのコンポーネント、ユーザ データ サービス（UDS）および Administration Console は Web ベースのコンポーネントで、以下のサポート対象アプリケーション サーバのいずれにも展開できます。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

選択したアプリケーション サーバにこれらの Web アプリケーションの WAR ファイルを展開する前に、UDS および Administration Console に必要な Arcot 独自仕様のファイルをアプリケーション サーバ上の適切な場所にコピーする必要があります。このセクションでは、アプリケーション サーバに必要な暗号化ファイルをコピーし、以下の Web アプリケーションの WAR ファイルを展開する手順について説明します。

1. アプリケーション サーバの準備
2. （オプション）エンタープライズ アーカイブ ファイルの作成
3. ユーザ データ サービス（UDS）の展開
4. UDS 展開の確認
5. Administration Console の展開
6. Administration Console の展開の確認

アプリケーション サーバの準備

UDS および Administration Console では、RiskFort データベースに安全にアクセスするために以下のファイルを使用します。

- `arcot-crypto-util.jar`。以下の場所にあります。
  `<install_location>/arcot/java/ext/`
- `ArcotAccessKeyProvider.so`。以下の場所にあります。
  `<install_location>/arcot/java/ext/win/<32\or\64\bit>/`

このため、RiskFort コンポーネントを展開したアプリケーション サーバ上の適切な場所にこれらのファイルをコピーする必要があります。以下のサブセクションで、次のサーバ用ファイルのコピーについて説明します。

- Apache Tomcat
- IBM WebSphere

- BEA WebLogic

Apache Tomcat

Arcot 独自仕様のファイルをコピーする方法

1. `arcot-crypto-util.jar` を次の場所にコピーします：`$JAVA_HOME/jre/lib/ext/`
2. `ArcotAccessKeyProvider.so` を次の場所にコピーします：:
   - **Solaris の場合：**`$JAVA_HOME/jre/sparc/`
   - **RHEL の場合：**`$JAVA_HOME/jre/bin/`
3. アプリケーション サーバを再起動します。

IBM WebSphere

Arcot 独自仕様のファイルをコピーする方法

1. WebSphere Administration Console にログインします。
2. ［**Environment**］をクリックして、［**Shared Libraries**］をクリックします。
   a. ［**Scope**］ドロップダウンから、有効な表示範囲を選択します。この範囲には、アプリケーションが展開されているターゲット サーバまたはノードが含まれる必要があります。
   b. ［**New**］をクリックします。
   c. ［**Name**］に「*ArcotJNI*」などの名前を入力します。
   d. ［**Classpath**］を指定します。

      このパスは、`arcot-crypto-util.jar` ファイルが存在する場所を指し、ファイル名も含まれている必要があります。例：
      `/opt/arcot/ext/arcot-crypto-util.jar`
   e. JNI ライブラリ パスを入力します。

      このパスは、`ArcotAccessKeyProvider.so` ファイルが存在する場所を指している必要があります。
3. ［**Apply**］をクリックして、変更を保存します。
4. サーバ レベルのクラス ローダを設定します。
   a. ［**Servers**］をクリックして、［**Application Servers**］をクリックします。
   b. ［**Application Servers**］で、設定対象のサーバの設定ページにアクセスします。

c. ［**Java and Process Management**］をクリックし、［**Class Loader**］をクリックします。

d. ［**New**］をクリックします。

e. デフォルトの［**Classes loaded with parent class loader first**］を選択し、［**OK**］をクリックします。

f. 自動生成された**クラス ローダ ID** をクリックします。

g. クラス ローダの［**Configuration**］ページで、［**Shared Library References**］をクリックします。

h. ［**Add**］をクリックし、［**ArcotJNI**］を選択して、［**Apply**］をクリックします。

i. 変更を保存します。

5. `ArcotAccessKeyProvider.so` を次の場所にコピーします：:

   - **Solaris の場合：** *<WebSphere_JAVA_HOME>*`/jre/`**`sparc`**`/`
   - **RHEL の場合：** *<WebSphere_JAVA_HOME>*`/jre/`**`bin`**`/`

6. WebSphere を再起動します。

BEA WebLogic

Arcot 独自仕様のファイルをコピーする方法

1. `ArcotAccessKeyProvider.so` を WebLogic の次の場所にコピーします：:

   - **Solaris の場合：** *<WebLogic_JAVA_HOME>*`/jre/`**`sparc`**`/`
   - **RHEL の場合：** *<WebLogic_JAVA_HOME>*`/jre/`**`bin`**`/`

2. `arcot-crypto-util.jar` を WebLogic の次の場所にコピーします：
   `<WebLogic_JAVA_HOME>/jre/lib/ext/`

注： 使用している *<JAVA_HOME>* が WebLogic で使用されている適切なものであるをことを確認してください。

3. WebLogic Administration Console にログインします。
4. ［**Deployments**］に移動します。
5. ［**Lock and Edit**］オプションを有効にします。

6. ［**Install**］をクリックし、arcot-crypto-util.jar ファイルが含まれるディレクトリに移動します。
7. ［**Next**］をクリックし、アプリケーション インストール アシスタントを開きます。
8. ［**Next**］をクリックし、［Summary］ページを表示します。
9. ［**Finish**］をクリックします。
10. 変更をアクティブ化します。
11. サーバを再起動します。

（オプション）エンタープライズ アーカイブ ファイルの作成

デフォルトで、UDS と Administration Console を展開するための Web ARchive （WAR）ファイルが提供されます。ただし、必要に応じて、これらのファイルの形式をエンタープライズ アーカイブ（EAR）に変更し、EAR ファイルを展開できます。

以下のサブセクションの説明に従って、UDS と Administration Console の両方の EAR ファイルを個別に生成できます。または、両方の Web アーカイブを含む単一の EAR ファイルを生成することもできます。

個別の EAR ファイルの生成

UDS と Administration Console 用の EAR ファイルを個別に作成する方法

1. コマンド プロンプト ウィンドウを開きます。
2. *<install_location>*/arcot/tools/**bundlemanager**/ ディレクトリに移動します。
3. 以下のコマンドを実行して EAR ファイルを作成します。

   ```
   java -jar bundle-manager.jar -ear <filename.ear> -warList
   <filename.war>
   ```

   上記のコマンドによって、以下の場所に個別の EAR ファイルが生成されます。

   <install_location>/arcot/**java**/**webapps**/

単一の EAR ファイルの生成

UDS と Administration Console の Web アーカイブを含んだ単一の EAR ファイルを作成する方法

1. コマンド プロンプト ウィンドウを開きます。
2. *<install_location>*/arcot/tools/**bundlemanager**/ ディレクトリに移動します。
3. 以下のコマンドを実行して EAR ファイルを作成します。

```
java -jar bundle-manager.jar -ear <filename.ear> -warList
arcotadmin.war arcotuds.war
```

上記のコマンドによって、以下の場所に単一の EAR ファイルが生成されます。

<install_location>/arcot/**java**/**webapps**/

ユーザ データ サービス（UDS）の展開

ユーザ データ サービス（UDS）によって、組織が展開した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）へのアクセスが可能になります。これによって、RiskFort サーバと Administration Console は、シームレスに既存のデータにアクセスできます。LDAP ディレクトリ サーバが設定されていない場合は、RiskFort データベースにアクセスして、ユーザ情報を読み取ります （UDS をほかの RiskFort コンポーネントに接続するために設定が必要なパラメータの詳細については、4-64 ページの手順 3 でブートストラップの手順を参照してください）。

ユーザ データ サービス（UDS）を展開するには、arcotuds.war ファイルが必要です。このファイルを使用して UDS を展開するには、以下の手順に従います。

1. アプリケーション サーバに arcotuds.war を展開します。このファイルは、以下の場所にあります。

注： 展開の手順は、使用しているアプリケーション サーバによって異なります。手順の詳細については、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。
たとえば、Apache Tomcat の場合は、*<APP_SERVER_HOME>***webapps**\ に WAR ファイルを展開する必要があります。

<install_location>/arcot/**java**/**webapps**/

2. （**WebSphere の場合のみ**）アプリケーション ファイルが更新されたときに UDS クラスが再ロードされるよう設定します。
   a. ［**Application**］-［**Enterprise Applications**］に移動し、UDS 設定ページにアクセスします。
   b. ［**Class loader order**］で［**Classes loaded with local class loader first (parent last)**］オプションを選択します。
   c. ［**WAR class loader policy**］で、［**Single class loader for application**］を選択します。
   d. ［**Apply**］をクリックして、変更を保存します。
3. アプリケーション サーバを再起動します。

UDS 展開の確認

UDS 関連情報のログ記録には arcotuds.log ファイルが使用されます。UDS が正しく開始したかどうか確認するには、以下の手順に従います。

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで arcotuds.log ファイルを開き、以下の行を見つけます。
   - `Initializing Arcot User Data Service (Version: 1.0.9)`
   - `Arcot User Data Service initialized successfully.`

   これらの行は、UDS が正常に展開されたことを示しています。

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

Administration Console の展開

Administration Console は、サーバ設定のカスタマイズや展開したシステムの管理を実行できる RiskFort へのブラウザ ベース インターフェースです。

注： Administration Console を使用して RiskFort を管理するには、RiskFort サーバがホスト名でインストールされているシステムに Administration Console がアクセスできるようにする必要があります。

RiskFort Administration Console を展開するには arcotadmin.war ファイルが必要です。このファイルは、以下の場所にあります。

<install_location>/arcot/java/**webapps**/

アプリケーション サーバに Administration Console WAR ファイルを展開する方法

1. アプリケーション サーバの適切なディレクトリに arcotadmin.war を展開します。

注： 展開の手順は、使用しているアプリケーション サーバによって異なります。手順の詳細については、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。
たとえば、Apache Tomcat の場合は、*<APP_SERVER_HOME>***webapps**\ に WAR ファイルを展開する必要があります。

2. アプリケーション サーバを再起動します。

Administration Console の展開の確認

Administration Console 情報のログ記録には `arcotadmin.log` ファイルが使用されます。

Administration Console が正常に展開されているかどうかを確認する方法

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで `arcotadmin.log` ファイルを開き、以下の行を見つけます。
   - `Arcot Administration Console v1.0.9`
   - `Arcot Administration Console Configured Successfully.`

   これらの行は、Administration Console が正常に展開されたことを示しています。

注： また、ログ ファイルに「`FATAL`」と「`WARNING`」のメッセージが含まれていないことを確認することもお勧めします。

Administration Console へのログイン方法

初めて Administration Console にログインする際は、展開時にデータベースに自動的に設定される **Master Administrator** （MA）クレデンシャルを使用する必要があります。

MA として Administration Console にログインする方法

1. Web ブラウザ ウィンドウで Administration Console を開きます。Administration Console のデフォルト URL は以下のとおりです。

   http://<host>:<port>/arcotadmin/masteradminlogin.htm

注： 上記の URl で指定するホストとポートの情報は、Administration Console を展開したアプリケーション サーバのものである必要があります。

2. デフォルトの Master Administrator アカウント クレデンシャルを使用してログインします。クレデンシャルは以下のとおりです。
   - **ユーザ名：masteradmin**
   - **パスワード：master1234!**

	**重要 :** 最初のログイン後、Master Administrator パスワードを変更するよう強くお勧めします。 管理者パスワードの変更の詳細については、「Arcot RiskFort 管理ガイド」を参照してください。

システムのブートストラップ

Administration Console を使用して RiskFort の管理を始めるには、まず以下の必須の手順を実行して、システムを初期化する必要があります。

- デフォルトの Master Administrator パスワードの変更
- UDS 接続パラメータの設定
- デフォルトの組織用の認証メカニズムの指定

ブートストラップとは、これらの設定タスクを順を追って実行するウィザード形式のプロセスです。ほかの管理リンクは、これらのタスクを実行した後で有効になります。

「ブートストラップ タスクの実行」に進む前に、「デフォルトの組織」に関する概念を理解しておく必要があります。

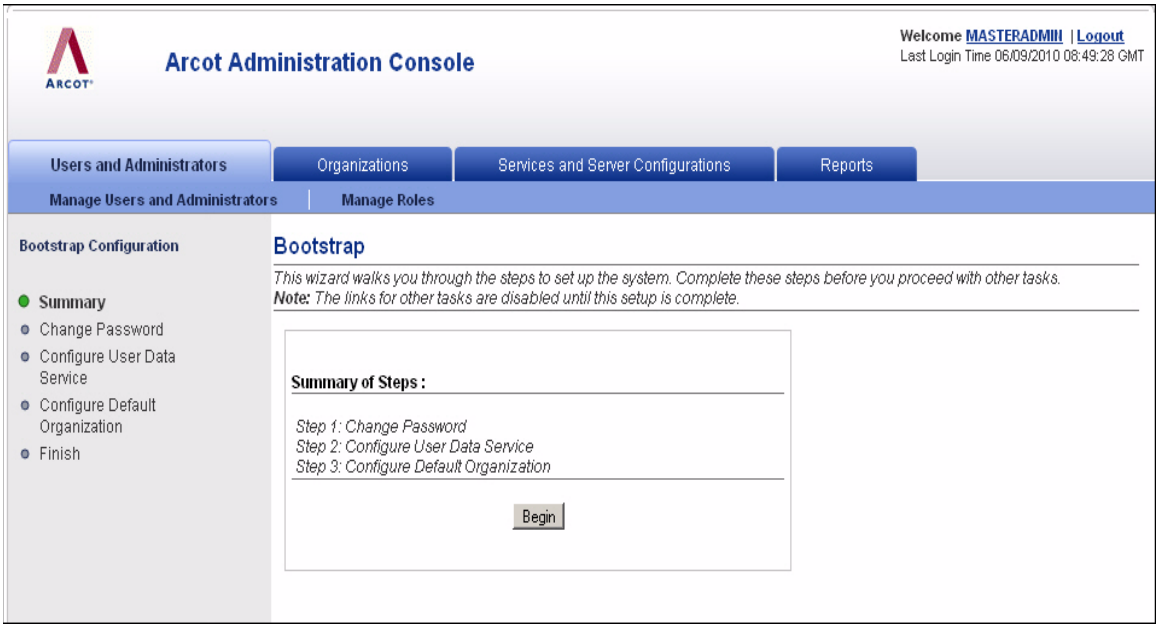
デフォルトの組織

Administration Console を展開すると、組織が 1 つ自動的に作成されます。この組織を、デフォルトの組織（DEFAULTORG）と呼びます。デフォルトの組織はそれだけで単一組織システムとして、ほかに新しい組織を作らずに使用できます。

ブートストラップ タスクの実行

初めて Master Administrator （MA）として Administration Console にログインすると、ブートストラップ ウィザード画面（図 4-1）の［Summary］画面が表示されます。

図 4-1 ブートストラップ ウィザード：［Summary］画面

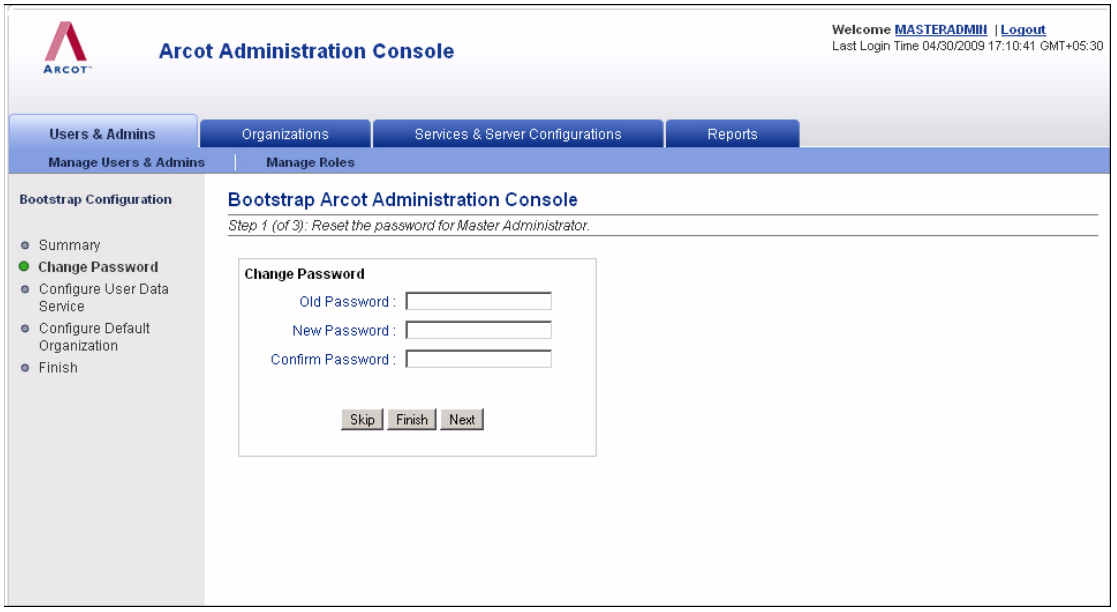


ウィザードを使用してシステムをブートストラップする方法

1. ［**Begin**］をクリックして、プロセスを開始します。

   図 4-2 のような［Change Password］画面が表示されます。

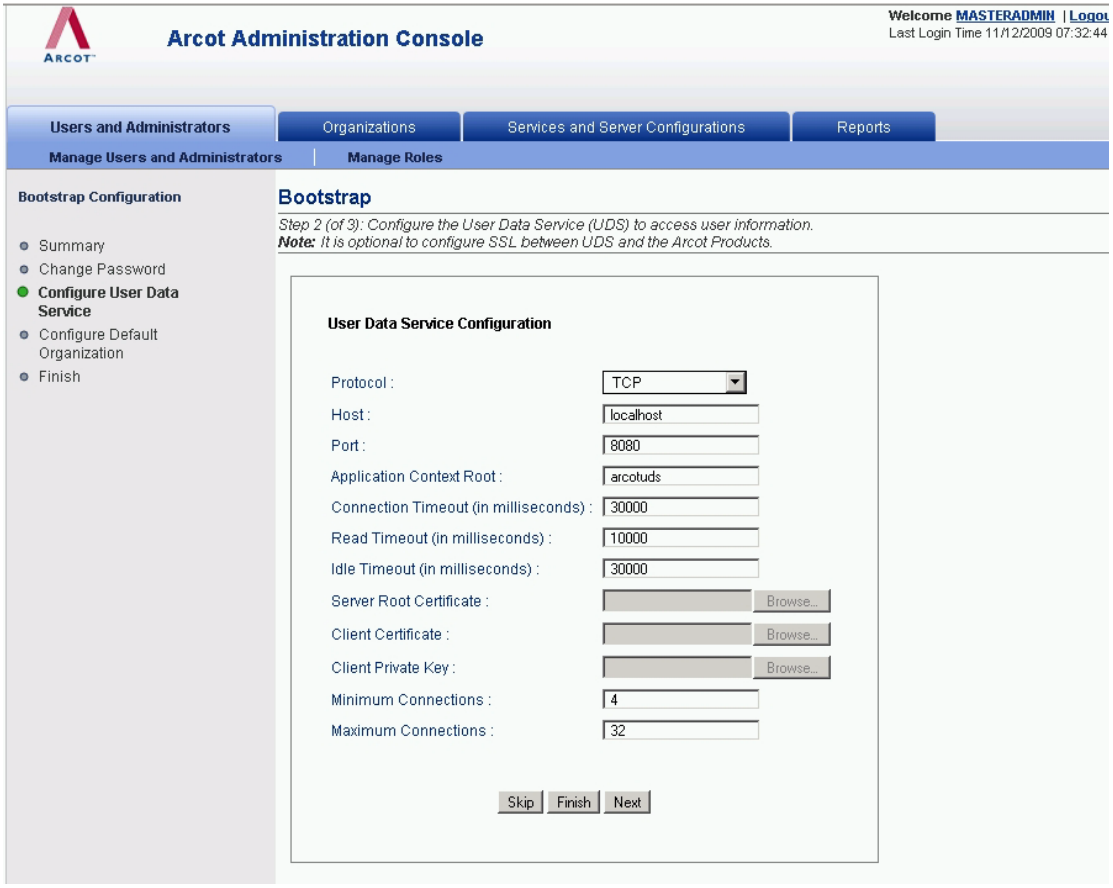
図 4-2 ブートストラップ ウィザード：［Change Password］画面



2. ［**Old Password**］、［**New Password**］、［**Confirm Password**］を指定し、［**Next**］をクリックします。

   図 4-3 のような［Configure User Data Service］画面が表示されます。

図 4-3 ブートストラップ ウィザード：［Configure User Data Service］の設定



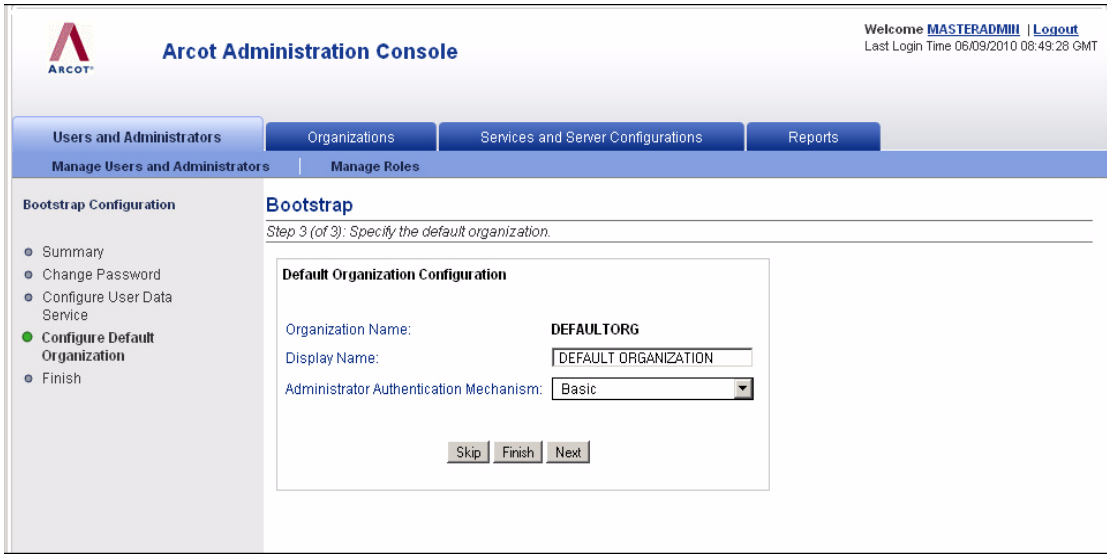
3. 表 4-2 のリスト内のパラメータを指定して、UDS を設定します。

表 4-2. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Protocol	TCP	Administration Console を使用して UDS に接続するためのプロトコル。使用可能なオプションは、以下のとおりです。 • TCP • 一方向 SSL • 双方向 SSL
Host	localhost	UDS が展開されているアプリケーション サーバのホスト名または IP アドレス
Port	8080	アプリケーション サーバを利用できるポート
Application Context Root	arcotuds	アプリケーション サーバに UDS を定義するために使用されるタグ。 たとえば、*http://<host>:<port>/arcotuds/services* という URL のコンテキスト ルートは arcotuds です。
Connection Timeout（ミリ秒）	30000	UDS サービスが到達不可と見なされるまでの最大時間（**ミリ秒単位**）
Read Timeout（ミリ秒）	10000	UDS からのレスポンスを待機する最大時間（**ミリ秒単位**）
Idle Timeout（ミリ秒）	30000	アイドル接続が終了されるまでの最大時間（**ミリ秒単位**）
Server Root Certificate	デフォルトなし	UDS サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式である必要があります。
Client Root Certificate	デフォルトなし	RiskFort サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式である必要があります。
Client Private Key	デフォルトなし	CA の秘密キーが含まれるファイルの場所
Minimum Connections	4	RiskFort サーバと UDS 間で作成される接続の最小数
Maximum Connections	32	RiskFort サーバと UDS 間で作成できる接続の最大数

図 4-4 のような［Configure Default Organization］画面が表示されます。

図 4-4 ブートストラップ ウィザード：［Configure Default Organization］画面



4. デフォルトの組織用に以下のパラメータを指定します。
   - **表示名**：組織の説明的な名前。この名前が、ほかのすべての Administration Console ページとレポートに表示されます。
   - **認証メカニズム**：デフォルトの組織に所属する管理者を認証するために使用されるメカニズム。Administration Console では、管理者がログインするための認証方式を 2 種類サポートしています。
     - **基本ユーザ パスワード**

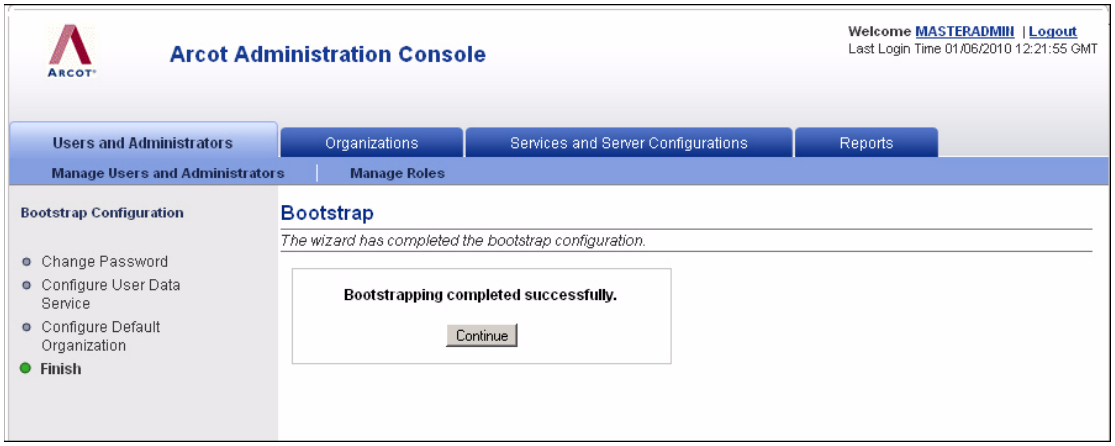
       このオプションを選択すると、Administration Console で提供される組み込みの認証方式が管理者の認証に使用されます。
     - **WebFort ユーザ パスワード**

       ここで［**WebFort User Password**］オプションを選択すると、クレデンシャルが発行され 、WebFort サーバによって認証されます。この場合、Arcot WebFort サーバがインストールされている必要があります。

	関連文書： WebFort のインストールと設定の詳細については、「Arcot WebFort 6.0 インストールおよび展開ガイド」を参照してください。

［Finish］画面（図 4-5）で示されているように、Administration Console の初期化が完了します。

図 4-5 ブートストラップ ウィザード：［Finish］画面



5. ［**Continue**］をクリックし、Administration Console を使用してほかの設定を続行します。

RiskFort サーバの起動

RiskFort サーバを起動する方法

1. 以下のディレクトリに移動します。

<*install_location*>/arcot/**bin**/

2. `./riskfortserver start` コマンドを実行します。

> **注：** RiskFort サーバを停止する場合は、`bin` ディレクトリに移動し、`./riskfortserver stop` コマンドを入力します。

Case Management Queuing サーバの開始

Case Management サーバを**開始**する方法

1. 以下のディレクトリに移動します。

<*install_location*>/arcot/**bin**/

2. `./casemanagementserver start` コマンドを実行します。

注： Case 管理サーバを停止する場合は、`bin` ディレクトリに移動し、`./casemanagementserver stop` コマンドを入力します。

Case 管理サービスが正常に開始されているかどうかを**確認**する方法

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで `arcotriskfortcasemgmtserver.log` ファイルを開き、以下の行を見つけます。
   - `STARTING Arcot RiskFort Case Management 2.2.6_s`
   - `STARTING Arcot RiskFort Case Management 2.2.6_l`
   - `Arcot RiskFort Case Management Service READY`

注： また、ログ ファイルに「`FATAL`」と「`WARNING`」のメッセージが含まれていないことを確認することもお勧めします。

インストールの確認

データベース スキーマをシードし、UDS と Administration Console を展開して、システムをブートストラップし、サーバを開始したら、これらのコンポーネントがすべて正常に開始されていることを確認する必要があります。このために確認する必要のあるログ ファイルは、`arcotriskfort.log` です。

サーバが正常に開始したかどうかを確認する方法

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで `arcotriskfort.log` ファイルを開き、以下の行を見つけます。
   - **Solaris の場合：**`Arcot RiskFort 2.2.6_s を開始しています`
   - **RHEL の場合：**`Arcot RiskFort 2.2.6_l を開始しています`
   - `Arcot RiskFort サービスの準備が整いました`

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

サンプル アプリケーションの展開

重要： リスク評価 SDK および発行 SDK がインストールされているのと同じアプリケーション サーバ上にサンプル アプリケーションを展開する必要があります。

サンプル アプリケーションを使用して、RiskFort が正常にインストールされ、設定されているかどうかを確認できます。また、サンプル アプリケーションは以下についての例を提供します。

- 一般的な RiskFort ワークフロー
- RiskFort API の基本操作（呼び出しと後処理）
- RiskFort と自社アプリケーションの統合

サンプル アプリケーションは、RiskFort 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。サンプル アプリケーションを展開する方法

1. アプリケーション サーバ サービスを停止します。
2. 以下の場所から riskfort-2.2.6-sample-application.war ファイルを展開します。

   <install_location>/arcot/**samples**/**java**/

   注： また、パッケージ内に riskfort-2.2.6-sample-application.war がある場合は、上記の場所からサンプル アプリケーションファイルを展開することをお勧めします。

3. アプリケーション サーバを再起動します。

サンプル アプリケーションの使用

このサブセクションでは、サンプル アプリケーションを使用して実行できるリスク評価操作について説明します。サンプル アプリケーションでの各操作は RiskFort が完全にインストールされ、機能していれば、エラーなく実行されるように設計されています。

サンプル アプリケーションでは、RiskFort 発行および RiskFort サーバが実行できる以下の操作について、その例を示します。

- 初めてのユーザのリスク評価および後評価の実行
- ユーザの作成
- 既知のユーザのリスク評価および後評価の実行
- デフォルト プロファイルの編集およびリスク評価の実行

初めてのユーザのリスク評価および後評価の実行

ユーザのデフォルト プロファイルでリスク評価を実行する方法

1. サンプル アプリケーションが（Web ブラウザ ウィンドウで）開いていることを確認します。サンプル アプリケーションのデフォルト URL は以下のとおりです。

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

2. ［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
3. このページの［**User Name**］フィールドにユーザ（評価対象）の名前を指定します。
4. ユーザが所属する組織の名前を［**User Organization**］フィールドに指定します。
5. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。

   このページには、リスク スコアおよび関連付けられているリスク アドバイスが表示され、指定した組織用に設定されたルールがリスト表示されます。初めてのユーザの場合、結果は **ALERT** になります。

6. ［**Next Step**］をクリックし、［Post Evaluation］ページを開いて、指定したユーザ プロファイルに対してポスト評価を実行します。

   アプリケーションは後評価を通じて、現在のユーザやユーザが使用しているデバイスに関するフィードバックを RiskFort サーバに提供します。RiskFort では、このフィードバックに基づいて、ユーザ属性やデバイス属性、ユーザとデバイスの関連付けを更新し、その後ユーザのトランザクションに伴うリスクを適宜評価します。

7. ［**Result of Secondary Authentication**］リストから適切なオプションを選択して、2 次認証の結果を指定します。

8. ユーザ名とデバイスの関連付けの名前を［**Association Name**］に指定します。
9. ［**Post Evaluate**］をクリックし、後評価プロセスを完了すると、［Post Evaluation Results］セクションに同じ後評価プロセスの結果が表示されます。

ユーザの作成

ユーザの作成方法

1. Web ブラウザ ウィンドウでサンプル アプリケーションを開きます。サンプル アプリケーションのデフォルト URL は以下のとおりです。

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

   ［RiskFort Sample Application］ページが表示されます。
2. ［**Create User**］をクリックして、［Create User］ページを開きます。
3. ［**User Name**］フィールドおよび［**Organization Name**］フィールドに一意のユーザ名とその組織名をそれぞれ入力し、［**Create User**］をクリックします。［**Organization Name**］を指定しない場合、ユーザは `defaultorg` 内に作成されます。

   指定したユーザがデータベースに正常に追加されると、「The User is created successfully」というメッセージが表示されます。
4. ［**Main Page**］をクリックして、［RiskFort Sample Application］ページに戻ります。

既知のユーザのリスク評価および後評価の実行

1. サンプル アプリケーションの［Main Page］で［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
2. ［**User Name**］フィールドで、作成済みのユーザの名前を指定します。
3. ユーザの組織を［**User Organization**］フィールドに指定します。
4. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。

   リスク アドバイスは通常 **INCREASEAUTH** です。
5. ［**Next Step**］をクリックして、後評価を実行します。
   - リストから［**Result of Secondary Authentication**］を指定します。
   - 必要に応じて［**Association Name**］を編集します。
6. ［**Post Evaluate**］をクリックして、最終的なアドバイスを表示します。

   手順 1 ～手順 4 を繰り返せば、［Risk Evaluation Results］ページの**リスク アドバイス**は **ALLOW** に変わります。

デフォルト プロファイルの編集およびリスク評価の実行

サンプル アプリケーションを使用して、使用しているコンピュータの DeviceDNA、IP アドレス、およびデバイス ID を変更して、さまざまな状況をシミュレートできます。ユーザのデフォルト プロファイルを編集するには、以下の手順に従います。

1. サンプル アプリケーションの［Main Page］で［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
2. ［**User Name**］フィールドで、プロファイルを編集するユーザ名を指定します。
3. ユーザの組織を［**User Organization**］フィールドに指定します。
4. ［**Edit Inputs**］をクリックし、［Edit Risk-Evaluation Inputs］ページを開きます。
5. このページでは、すべてのフィールドがあらかじめ入力されています。1 つ以上の必要なフィールドの値を変更します。
   - **My User Name**
   - **My Org**
   - **Machine Finger Print of My Device**
   - **IP Address of My Machine**
   - **Device ID of My Machine**
6. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。
7. ［**Next Step**］をクリックし、［Post Evaluation］ページを開いて、指定したユーザ プロファイルに対してポスト評価を実行します。
8. ［**Result of Secondary Authentication**］リストから適切なオプションを選択して、2 次認証の結果を指定します。
9. ［**Post Evaluate**］をクリックし、後評価プロセスを完了すると、同じ後評価プロセスの結果が表示されます。

注： RiskFort コンポーネント間の安全な通信を確保するために、SSL （Secure Socket Layer）トランスポート モードをサポートするよう設定できます。詳細については、付録 F の 「SSL の設定」を参照してください。

インストール後のチェックリスト

RiskFort のインストールと設定の情報でこのチェックリスト（表 4-3）を記入することをお勧めします。後に実行する各種管理タスクでこれらの情報が必要になります。

表 4-3. インストール時のチェックリスト

情報	エントリ例	実際のエントリ
ARCOT_HOME	/var/opt/arcot/	
システム情報		
ホスト名	my-bank	
ユーザ名	管理者	
パスワード	password1234!	
設定済みコンポーネント	RiskFort サーバ Administration Console ユーザ データ サービス	
Administration Console 情報		
ホスト名	ローカルホスト	
ポート	8080	
Master Administrator パスワード	mypassword1234!	
ユーザ データ サービス情報		
ホスト名	ローカルホスト	
ポート	8080	
アプリケーションのコンテキストルート	arcotuds	

第 5 章
分散システムへの RiskFort の展開

RiskFort コンポーネントのインストールは、**Arcot RiskFort 2.2.6 InstallAnywhere ウィザード**を使用して実行します。このウィザードでは *Complete* と *Custom* のインストールタイプをサポートしています。ただし、分散環境に RiskFort をインストールして設定する場合、インストーラを実行する際に **Custom** オプションを使用する必要があります。

以下の手順は、プロセスの概要です。

1. RiskFort インストーラを実行し、RiskFort サーバと Administration Console をインストールして、SQL データベースにアクセスするよう設定します。また、同じシステム上に Web サービスをインストールすることも選択できます。

   インストールの手順については、「1 つ目のシステムへのインストール」を参照してください。

2. データベース スクリプトを実行し、RiskFort スキーマおよびデータベース テーブルを作成します。また、データベースが正常に設定されていることを確認します。

   詳細については、「データベース スクリプトの実行」、および「データベースの設定の確認」を参照してください。

3. アプリケーション サーバに Web アプリケーション（UDS および Administration Console）を展開し、展開を確認します。

   詳細については、「Web アプリケーションの展開」を参照してください。

4. Master Administrator クレデンシャルで Administration Console にログインし、RiskFort を初期化します。

   詳細については、「Administration Console へのログイン方法」および「システムのブートストラップ」を参照してください。

5. RiskFort サーバおよび Case Management Queuing サーバを起動し、サーバが正常に開始するかどうかを確認します。

   詳細については、「RiskFort サーバの起動」、「Case Management Queuing サーバの開始」、および「インストールの確認」を参照してください。

6. （オプション）RiskFort コンポーネント間の安全な通信を確保するために、SSL（Secure Socket Layer）トランスポート モードをサポートするよう設定できます。

   詳細については、付録 F の 「SSL の設定」を参照してください。

7. 1 つ以上のシステムに Java SDK および Web サービスをインストールします。

   詳細については、「2 つ目のシステムへのインストール」を参照してください。

8. サンプル アプリケーションを展開して設定し、これを使用して RiskFort 設定をテストします。

注 : サンプル アプリケーションのみをインストールするには、[**SDKs and Sample Application**] オプションのみが選択されていることを確認して、インストールを続行する必要があります。

   詳細については、「サンプル アプリケーションの展開」、「RiskFort サーバとの通信用サンプル アプリケーションの設定」、および「サンプル アプリケーションの使用」を参照してください。

9. インストール チェックリストを完了します。

   詳細については、「インストール後のチェックリスト」を参照してください。

インストールに関する重要な注意事項

単一のシステムまたは分散環境に RiskFort をインストールする際、以下の点に注意してください。

- *<install_location>* には特殊文字が含まれないようにしてください（~ ! @ # $ % ^ & * ( ) _ + = { } [ ] ' " など）。
- RiskFort 2.2.6 は、旧バージョン（1.7 以前）からのアップグレードをサポートしていません。また、以前にインストールしたバージョンの上に RiskFort 2.2.6 をインストールすることはできません。
- 現時点では、インストーラを使用して RiskFort コンポーネントを変更または修復することはできません。必ずコンポーネントをアンインストールしてから、再インストールしてください。
- インストールの実行中は、インストーラ ウィンドウを閉じないでください。インストール中（特に最後の段階）に [**Cancel**] ボタンをクリックしてインストールを中止した場合、それまでに作成されたディレクトリはすべてが削除されるとは限りません。インストール ディレクトリ、*<install_location>*/**arcot**/、およびそのサブディレクトリを手動でクリーンアップする必要があります。

  a. を選択します。

1 つ目のシステムへのインストール

分散環境では、RiskFort、Administration Console、Java SDK、および Web サービスを展開するシステムの数にもよりますが、通常は 1 つ目のシステム上に RiskFort サーバをインストールします。*Custom* インストールでは、選択したコンポーネントのみをパッケージからインストールできます。このオプションは上級ユーザが実行することをお勧めします。

インストールを実行する前に、第 3 章の「インストールの準備」の説明に従って、前提条件となるソフトウェア コンポーネントがすべてインストールされ、データベースが設定されていることを確認してください。

RiskFort コンポーネントをインストールする方法

1. ログインし、インストーラを解凍したディレクトリに移動します。
2. 以下のようにインストーラを実行します。
   - **Solaris の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Solaris-Installer.bin
     ```

   - **Linux の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Linux-Installer.bin
     ```

   `root` ログインでインストーラを実行すると、警告メッセージが表示されます。続行する場合は「**Y**」を入力し、インストールを終了する場合は「**N**」を入力します。

   インストーラ画面を終了した場合は、再度インストーラを実行する必要があります。
3. **Enter** キーを押して続行します。

   セットアップ画面が表示されます。
4. **Enter** キーを押してインストールを続行します。

   ［License Agreement for RiskFort］が表示されます。
5. ［License Agreement］画面で以下を実行します。
   a. テキストをよく読み、**Enter** キーを押してライセンス テキストの次の画面を表示します。使用許諾契約書のすべてのテキストが表示されるまで、**Enter** キーを複数回押す必要がある場合があります。

      使用許諾契約書の最後で、使用許諾契約書の条項への同意を求めるプロンプトが表示されます（**DO YOU ACCEPT THE TERMS OF LICENSE AGREEMENT?**）。

b. 使用許諾契約書に同意する場合は、「**Y**」を入力してインストールを続行します。

注 : 「**N**」を入力すると、警告メッセージが表示され、インストールが中止されます。

［Choose Installation Location］画面が表示されます。

6. 画面の指示に従って、以下のいずれかを実行します。
   - RiskFort をインストールするディレクトリの絶対パスを入力し、**Enter** キーを押して続行します。

注 : 指定するインストール ディレクトリ名にはスペースを*含めないでください*。スペースを含めると、RiskFort スクリプトとツールの一部が想定どおりに機能しない場合があります。

   または

   - **Enter** キーを押して、インストーラによって表示されたデフォルトのディレクトリを受け入れます。

   RiskFort でサポートされるインストール オプションが表示されます。
7. インストールを実行しているコンピュータに既存の Arcot 製品がすでにインストールされている場合、インストーラに以下のオプションが表示されます。
   - **1** - 新しい場所を入力する。
   - **2** - 手順 6 で選択したディレクトリへのインストールを続行する。
   - **3** - 既存の Arcot 製品がインストールされている場所を使用する。
8. 必要なオプションを選択し、**Enter** キーを押してインストールを続行します。

注 : オプション 1 または 2 を選択した場合、指定された場所に `arcot` という新しいディレクトリが作成されます。

［Installation Type］画面が表示されます。この画面には、RiskFort でサポートされているインストールのタイプ（**Complete** または **Custom**）が表示されます。

9. **Custom** インストール オプションを受け入れてインストールを続行する場合は、「**2**」を入力して **Enter** キーを押します。

［Choose Product Features］画面が表示されます。この画面で、システムにインストールするコンポーネントを個別に選択できます。

10. インストールする RiskFort コンポーネントを表す番号をカンマ区切りリスト（カンマと番号の間にスペースを入れない）で指定し、**Enter** キーを押して続行します。

注： サンプル アプリケーションのみをインストールするには、［**Risk Evaluation SDK**］オプションと［**Issuance SDK**］オプションのみが選択されていることを確認して、インストールを続行する必要があります。

表 5-1 は、RiskFort インストーラによってインストールされるすべてのコンポーネントについて説明しています。

表 5-1. RiskFort によってインストールされるコンポーネント

コンポーネント番号	コンポーネント	説明
1	**サーバ**	このオプションでは、Administration Console から以下のリクエストを提供するコア処理エンジン（**RiskFort サーバ**）がインストールされます。 • リスク評価 • 発行 • 設定 また、このコンポーネントでは、サーバに組み込まれている以下の Web サービスもインストールされます。 • **リスク評価 Web サービス** - RiskFort サーバによるリスク評価用の Web ベース プログラミング インターフェースを提供します。 • **発行 Web サービス** - ユーザの作成と管理用の Web ベース プログラミング インターフェースを提供します。 • **管理 Web サービス** - RiskFort Administration Console で使用される Web ベース プログラミング インターフェースを提供します。
2	**Case Management Queuing サーバ**	このオプションでは、Case に対応するテクニカル サポート担当者（CSR）に Case を割り当てるコア キュー エンジン（Case Management Queuing サーバ）をインストールします。 **注：** Administration Console のすべてのインスタンスは、ある一時点では、Case Management Queuing サーバの単一のインスタンスにのみ接続できます。

表 5-1. RiskFort によってインストールされるコンポーネント

コンポーネント番号	コンポーネント	説明
3	**Administration Console and User Data Service**	このオプションでは、サーバ設定用、およびルールとユーザの管理用の Web ベース インターフェースを提供します。このパッケージは、以下のサブコンポーネントで構成されます。 • **Administration Console** - RiskFort サーバおよびリスク評価に関する設定を管理するための Web ベース インターフェースを提供します。 • **ユーザ データ サービス（UDS）** - リレーショナル データベース（RDBMS）やディレクトリ サーバ（LDAP）など、各種ユーザ リポジトリにアクセスするための抽象化層として機能します。
4	**SDKs and Sample Application**	このオプションでは、RiskFort サーバにリスク分析リクエストとユーザ発行リクエストを転送するためにアプリケーションが呼び出せるプログラミング インターフェースを（API および Web サービスの形式で）提供します。このパッケージは、以下のサブコンポーネントで構成されます。 • **RiskFort SDK** - RiskFort サーバによるリスク評価用の Java プログラミング インターフェースを提供します。 • **発行 SDK** - ユーザの作成と管理用の Java プログラミング インターフェースを提供します。 • **サンプル アプリケーション** - RiskFort Java API の使用方法の例を示します。また、RiskFort が正常にインストールされているかどうかや、リスク評価リクエストと発行リクエストを実行できるかどうかを確認する目的でも使用できます。 これらのコンポーネントの設定の詳細については、第 6 章の「RiskFort SDK と Web サービスの設定」を参照してください。

たとえば、現在のシステムに RiskFort サーバ、Case Management Queuing サーバ、および Administration Console を（SDK およびサンプル アプリケーション*なし*で）インストールする場合は、以下の操作を実行する必要があります。

- ［**Server**］オプションを選択します。
- ［**Case Management Queuing Server**］オプションを選択します。
- ［**Administration Console and User Data Service**］オプションを選択します。

- ［**SDKs and Sample Application**］オプションを選択解除します。

注： この画面で**サーバ** コンポーネントがインストール用に選択されていない場合、画面では手順 11 ～手順 14 が表示されません。

［Database Type］画面が表示されます。この画面には、RiskFort でサポートされているデータベースの種類がリスト表示されます。

11. 選択するデータベースに対応する番号を入力し、**Enter** キーを押して続行します。

［Primary Database Access Configuration］画面が表示されます。

12. 表 5-2［Primary Database Access Configuration］画面で、のリストに記載された情報を指定します。

表 5-2. プライマリ DSN パラメータ

パラメータ	説明
Primary ODBC DSN	インストーラによって、RiskFort がデータベースへの接続に使用する ODBC 接続が作成されます。 推奨される入力値は `arcotdsn` です。
User Name	RiskFort がデータベースにアクセスする際のデータベース ユーザ名。この名前は、データベース管理者によって指定されます。 **注：** ユーザ名はプライマリ DSN とバックアップ用 DSN とで*異なっている必要があります。*
Password	上記のフィールドで指定した**ユーザ名**に関連付けられたパスワード。RiskFort がデータベースにアクセスする際に使用されます。このパスワードは、データベース管理者によって指定されます。
Service ID	サーバ上で実行される Oracle データベースのインスタンスを表す Oracle システム識別子（SID）
Port No	データベースが受信リクエストをリスンするポート。 **注：** デフォルトのポートをそのまま使用する場合は、**Enter** キーを押します。
Host Name	RiskFort データストアのホスト名または IP アドレス **構文**：*<server_name>* **例**：`demodatabase`

［Backup Database Access Configuration］画面が表示されます。

13. ［Backup Database Access Configuration］画面で以下を実行します。
    - 入力を求められたら、「**N**」を入力してセカンダリ DSN の設定をスキップし、**Enter** キーを押して次の画面に進みます。

      または

    - 入力を求められたら、「**Y**」を入力してセカンダリ DSN を設定し、**Enter** キーを押して続行します。

      実行するタスクの詳細については、表 5-2 を参照してください。

    ［Pre-Installation Summary］画面が表示されます。この画面には、製品の詳細、インストール ディレクトリ、インストールの種類、インストールされるコンポーネント、およびディスク領域に関する情報がリスト表示されます。
14. 表示された製品の詳細をよく確認し、**Enter** キーを押してインストールを続行します。ここまでの画面のいずれかで設定を変更する場合は、その画面に戻るまで「**back**」と入力し、必要な変更を加え、**Enter** キーを押して次の画面に進みます。

    ［Installing］画面が表示されます。これには数分かかる場合があります。その間、インストーラによって以下が実行されます。
    - すべてのコンポーネントおよび関連するバイナリがインストール ディレクトリに配置されます。
    - データベース設定が arcotcommon.ini ファイルに格納され、パスワードが `securestore.enc` ファイルに格納されます。
    - 必要な INI ファイルに書き込みが行われます。
    - 発行と Administration Console の `JNI_LIBRARY_PATH` や、`ODBC_HOME`、`ODBCINI`、`ORACLE_HOME`、`ORACLE_LIB_PATH` などの環境変数を `arctenv` ファイル内に設定します。
    - 前の画面で指定したとおり、`odbc.ini` ファイル内の選択済み ODBC ドライバを使用して、プライマリ DSN およびバックアップ用 DSN （選択され設定されている場合）を作成または上書きします。

    上記のタスクが正常に完了すると、［Installation Complete］画面が表示されます。
15. **Enter** を押してインストーラを終了します。

    プロンプトが再度表示されるまで（インストーラが一時ファイルをクリーンアップするまで)、数分かかる場合があります。

16. インストール ログ ファイルを確認します。ファイルは *<install_location>*/arcot/ ディレクトリにあります。

注： インストールが完了したら、以降のセクションの説明に従ってインストール後のタスクを実行してください。

インストール ログ

インストール後、以下のディレクトリでインストール ログ ファイル（Arcot_RiskFort_InstallLog.log）にアクセスできます。

<install_location>/arcot/**logs**/

何らかの理由でインストールが失敗した場合、インストールを実行したのと同じ場所にエラー ログが生成されます。

1 つ目のシステムでのインストール後のタスクの実行

このセクションでは、1 つ目のシステムへの RiskFort のインストール後に実行する必要があるインストール後のタスクについて説明します。これらの手順は RiskFort を正常に設定するために必要で、以下の順序で実行する必要があります。

1. データベース スクリプトの実行
2. データベースの設定の確認
3. Web アプリケーションの展開
4. Administration Console へのログイン方法
5. システムのブートストラップ
6. RiskFort サーバの起動
7. Case Management Queuing サーバの開始
8. インストールの確認

注： これらのインストール後のタスクを完了した後に、第 6 章の「RiskFort SDK と Web サービスの設定」の説明に従って、SDK および Web サービス設定タスクを実行してください。

データベース スクリプトの実行

重要 : このセクションで説明されるスクリプトを実行する前に、第 3 章の「データベース サーバの設定」セクションで作成したときと同じデータベース ユーザとしてログインしていることを確認してください。

RiskFort には、RiskFort データベースに必要なテーブルを作成する際に必要なスクリプトが付属されています。必要なデータベース スクリプトを実行するには、以下の手順に従います。

1. 以下のディレクトリに移動します。

   `<install_location>/arcot/dbscripts/`

2. 使用しているデータベースに応じて、に移動します。

   - **Oracle の場合 :**

     `<install_location>/arcot/dbscripts/oracle/`

3. 以下の順序でスクリプトを実行します。

   - `arcot-db-config-for common-1.0.sql`
   - `arcot-db-config-for-riskfort-2.2.6.sql`

データベースの設定の確認

必要なデータベース スクリプトの実行後、RiskFort スキーマが正常にシードされたかどうかを確認する必要があります。以下の手順に従ってください。

1. SYSDBA 特権を持つユーザとして RiskFort データベースにログインします。
2. 以下のクエリを実行します。

   ```
   SELECT SERVERNAME, VERSION FROM ARRFSERVERS;
   ```

   上記のクエリの結果、以下の出力が表示されます。

   ```
   SERVERNAME                    VERSION
   ------------------------  ----------------
   RiskFort                        2.2.6
   RiskFortCaseManagement          2.2.6
   ```

3. データベース コンソールからログアウトします。

Web アプリケーションの展開

RiskFort の 2 つのコンポーネント、ユーザ データ サービス（UDS）および Administration Console は Web ベースのコンポーネントで、以下のサポート対象アプリケーション サーバのいずれにも展開できます。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

選択したアプリケーション サーバにこれらの Web アプリケーションの WAR ファイルを展開する前に、UDS および Administration Console に必要な Arcot 独自仕様のファイルをアプリケーション サーバ上の適切な場所にコピーする必要があります。このセクションでは、アプリケーション サーバに必要な暗号化ファイルをコピーし、以下の Web アプリケーションの WAR ファイルを展開する手順について説明します。

1. アプリケーション サーバの準備
2. （オプション）エンタープライズ アーカイブ ファイルの作成
3. ユーザ データ サービス（UDS）の展開
4. UDS 展開の確認
5. Administration Console の展開
6. Administration Console の展開の確認

アプリケーション サーバの準備

UDS および Administration Console では、RiskFort データベースに安全にアクセスするために以下のファイルを使用します。

- `arcot-crypto-util.jar`。以下の場所にあります。
  `<install_location>/arcot/java/ext/`
- `ArcotAccessKeyProvider.so`。以下の場所にあります。
  `<install_location>/arcot/java/ext/win/<32\or\64\bit>/`

このため、RiskFort コンポーネントを展開したアプリケーション サーバ上の適切な場所にこれらのファイルをコピーする必要があります。以下のサブセクションで、次のサーバ用ファイルのコピーについて説明します。

- Apache Tomcat
- IBM WebSphere

- BEA WebLogic

Apache Tomcat

Arcot 独自仕様のファイルをコピーする方法

1. `arcot-crypto-util.jar` を次の場所にコピーします：*`$JAVA_HOME`*`/jre/lib/`**`ext`**`/`
2. `ArcotAccessKeyProvider.so` を次の場所にコピーします：
   - **Solaris の場合：**`$JAVA_HOME/jre/`**`sparc`**`/`
   - **RHEL の場合：**`$JAVA_HOME/jre/`**`bin`**`/`
3. アプリケーション サーバを再起動します。

IBM WebSphere

Arcot 独自仕様のファイルをコピーする方法

1. WebSphere Administration Console にログインします。
2. ［**Environment**］をクリックして、［**Shared Libraries**］をクリックします。
   a. ［**Scope**］ドロップダウンから、有効な表示範囲を選択します。この範囲には、アプリケーションが展開されているターゲット サーバまたはノードが含まれる必要があります。
   b. ［**New**］をクリックします。
   c. ［**Name**］に「*`ArcotJNI`*」などの名前を入力します。
   d. ［**Classpath**］を指定します。

      このパスは、`arcot-crypto-util.jar` ファイルが存在する場所を指し、ファイル名も含まれている必要があります。例：
      `/opt/arcot/ext/`**`arcot-crypto-util.jar`**
   e. JNI ライブラリ パスを入力します。

      このパスは、`ArcotAccessKeyProvider.so` ファイルが存在する場所を指している必要があります。
3. ［**Apply**］をクリックして、変更を保存します。
4. サーバ レベルのクラス ローダを設定します。
   a. ［**Servers**］をクリックして、［**Application Servers**］をクリックします。
   b. ［**Application Servers**］で、設定対象のサーバの設定ページにアクセスします。

c. ［**Java and Process Management**］をクリックし、［**Class Loader**］をクリックします。

d. ［**New**］をクリックします。

e. デフォルトの［**Classes loaded with parent class loader first**］を選択し、［**OK**］をクリックします。

f. 自動生成された**クラス ローダ ID** をクリックします。

g. クラス ローダの［**Configuration**］ページで、［**Shared Library References**］をクリックします。

h. ［**Add**］をクリックし、［**ArcotJNI**］を選択して、［**Apply**］をクリックします。

i. 変更を保存します。

5. `ArcotAccessKeyProvider.so` を次の場所にコピーします：
   - **Solaris の場合：** `<WebSphere_JAVA_HOME>/jre/`**`sparc`**`/`
   - **RHEL の場合：** `<WebSphere_JAVA_HOME>/jre/`**`bin`**`/`
6. WebSphere を再起動します。

BEA WebLogic

Arcot 独自仕様のファイルをコピーする方法

1. `ArcotAccessKeyProvider.so` を WebLogic の次の場所にコピーします：
   - **Solaris の場合：** `<WebLogic_JAVA_HOME>/jre/`**`sparc`**`/`
   - **RHEL の場合：** `<WebLogic_JAVA_HOME>/jre/`**`bin`**`/`
2. `arcot-crypto-util.jar` を WebLogic の次の場所にコピーします：
   `<WebLogic_JAVA_HOME>/jre/lib/`**`ext`**`/`

注： 使用している `<JAVA_HOME>` が WebLogic で使用されている適切なものであるをことを確認してください。

3. WebLogic Administration Console にログインします。
4. ［**Deployments**］に移動します。
5. ［**Lock and Edit**］オプションを有効にします。

6. ［**Install**］をクリックし、arcot-crypto-util.jar ファイルが含まれるディレクトリに移動します。
7. ［**Next**］をクリックし、アプリケーション インストール アシスタントを開きます。
8. ［**Next**］をクリックし、［Summary］ページを表示します。
9. ［**Finish**］をクリックします。
10. 変更をアクティブ化します。
11. サーバを再起動します。

（オプション）エンタープライズ アーカイブ ファイルの作成

デフォルトで、UDS と Administration Console を展開するための Web ARchive （WAR）ファイルが提供されます。ただし、必要に応じて、これらのファイルの形式をエンタープライズ アーカイブ（EAR）に変更し、EAR ファイルを展開できます。

以下のサブセクションの説明に従って、UDS と Administration Console の両方の EAR ファイルを個別に生成できます。または、両方の Web アーカイブを含む単一の EAR ファイルを生成することもできます。

個別の EAR ファイルの生成

UDS と Administration Console 用の EAR ファイルを個別に作成する方法

1. コマンド プロンプト ウィンドウを開きます。
2. *<install_location>*/arcot/tools/**bundlemanager**/ ディレクトリに移動します。
3. 以下のコマンドを実行して EAR ファイルを作成します。

   ```
   java -jar bundle-manager.jar -ear <filename.ear> -warList
   <filename.war>
   ```

   上記のコマンドによって、以下の場所に個別の EAR ファイルが生成されます。

   <install_location>/arcot/**java**/**webapps**/

単一の EAR ファイルの生成

UDS と Administration Console の Web アーカイブを含んだ単一の EAR ファイルを作成する方法

1. コマンド プロンプト ウィンドウを開きます。
2. *<install_location>*/arcot/tools/**bundlemanager**/ ディレクトリに移動します。
3. 以下のコマンドを実行して EAR ファイルを作成します。

```
java -jar bundle-manager.jar -ear <filename.ear> -warList
arcotadmin.war arcotuds.war
```

上記のコマンドによって、以下の場所に単一の EAR ファイルが生成されます。

<install_location>/arcot/**java**/**webapps**/

ユーザ データ サービス（UDS）の展開

ユーザ データ サービス（UDS）によって、組織が展開した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）へのアクセスが可能になります。これによって、RiskFort サーバと Administration Console は、シームレスに既存のデータにアクセスできます。LDAP ディレクトリ サーバが設定されていない場合は、RiskFort データベースにアクセスして、ユーザ情報を読み取ります （UDS をほかの RiskFort コンポーネントに接続するために設定が必要なパラメータの詳細については、5-94 ページの手順 3 でブートストラップの手順を参照してください）。

ユーザ データ サービス（UDS）を展開するには、`arcotuds.war` ファイルが必要です。このファイルを使用して UDS を展開するには、以下の手順に従います。

1. アプリケーション サーバに `arcotuds.war` を展開します。このファイルは、以下の場所にあります。

   注： 展開の手順は、使用しているアプリケーション サーバによって異なります。手順の詳細については、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。
   たとえば、Apache Tomcat の場合は、*<APP_SERVER_HOME>***webapps**\ に WAR ファイルを展開する必要があります。

   <install_location>/arcot/**java**/**webapps**/

2. （**WebSphere の場合のみ**）アプリケーション ファイルが更新されたときに UDS クラスが再ロードされるよう設定します。
   a. ［**Application**］-［**Enterprise Applications**］に移動し、UDS 設定ページにアクセスします。
   b. ［**Class loader order**］で［**Classes loaded with local class loader first (parent last)**］オプションを選択します。
   c. ［**WAR class loader policy**］で、［**Single class loader for application**］を選択します。
   d. ［**Apply**］をクリックして、変更を保存します。
3. アプリケーション サーバを再起動します。

UDS 展開の確認

UDS 関連情報のログ記録には arcotuds.log ファイルが使用されます。UDS が正しく開始したかどうか確認するには、以下の手順に従います。

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで arcotuds.log ファイルを開き、以下の行を見つけます。
   - `Initializing Arcot User Data Service (Version: 1.0.9)`
   - `Arcot User Data Service initialized successfully.`

   これらの行は、UDS が正常に展開されたことを示しています。

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

Administration Console の展開

Administration Console は、サーバ設定のカスタマイズや展開したシステムの管理を実行できる RiskFort へのブラウザ ベース インターフェースです。

注： Administration Console を使用して RiskFort を管理するには、RiskFort サーバがホスト名でインストールされているシステムに Administration Console がアクセスできるようにする必要があります。

RiskFort Administration Console を展開するには arcotadmin.war ファイルが必要です。このファイルは、以下の場所にあります。

<install_location>/arcot/java/**webapps**/

アプリケーション サーバに Administration Console WAR ファイルを展開する方法

1. アプリケーション サーバの適切なディレクトリに arcotadmin.war を展開します。

注： 展開の手順は、使用しているアプリケーション サーバによって異なります。手順の詳細については、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。
たとえば、Apache Tomcat の場合は、*<APP_SERVER_HOME>***webapps**\ に WAR ファイルを展開する必要があります。

2. アプリケーション サーバを再起動します。

Administration Console の展開の確認

Administration Console 情報のログ記録には arcotadmin.log ファイルが使用されます。

Administration Console が正常に展開されているかどうかを確認する方法

1. 次のディレクトリに移動します。

   <install_location>/arcot/**logs**/

2. 任意のエディタで arcotadmin.log ファイルを開き、以下の行を見つけます。
   - `Arcot Administration Console v1.0.9`
   - `Arcot Administration Console Configured Successfully.`

   これらの行は、Administration Console が正常に展開されたことを示しています。

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

Administration Console へのログイン方法

初めて Administration Console にログインする際は、展開時にデータベースに自動的に設定される **Master Administrator** （MA）クレデンシャルを使用する必要があります。

MA として Administration Console にログインする方法

1. Web ブラウザ ウィンドウで Administration Console を開きます。Administration Console のデフォルト URL は以下のとおりです。

   http://<host>:<port>/arcotadmin/masteradminlogin.htm

注： 上記の URl で指定するホストとポートの情報は、Administration Console を展開したアプリケーション サーバのものである必要があります。

2. デフォルトの Master Administrator アカウント クレデンシャルを使用してログインします。クレデンシャルは以下のとおりです。
   - **ユーザ名：masteradmin**
   - **パスワード：master1234!**

	重要 : 最初のログイン後、Master Administrator パスワードを変更するよう強くお勧めします。 管理者パスワードの変更の詳細については、「Arcot RiskFort 管理ガイド」を参照してください。

システムのブートストラップ

Administration Console を使用して RiskFort の管理を始めるには、まず以下の必須の手順を実行して、システムを初期化する必要があります。

- デフォルトの Master Administrator パスワードの変更
- UDS 接続パラメータの設定
- デフォルトの組織用の認証メカニズムの指定

ブートストラップとは、これらの設定タスクを順を追って実行するウィザード形式のプロセスです。ほかの管理リンクは、これらのタスクを実行した後で有効になります。

「ブートストラップ タスクの実行」に進む前に、「デフォルトの組織」に関する概念を理解しておく必要があります。

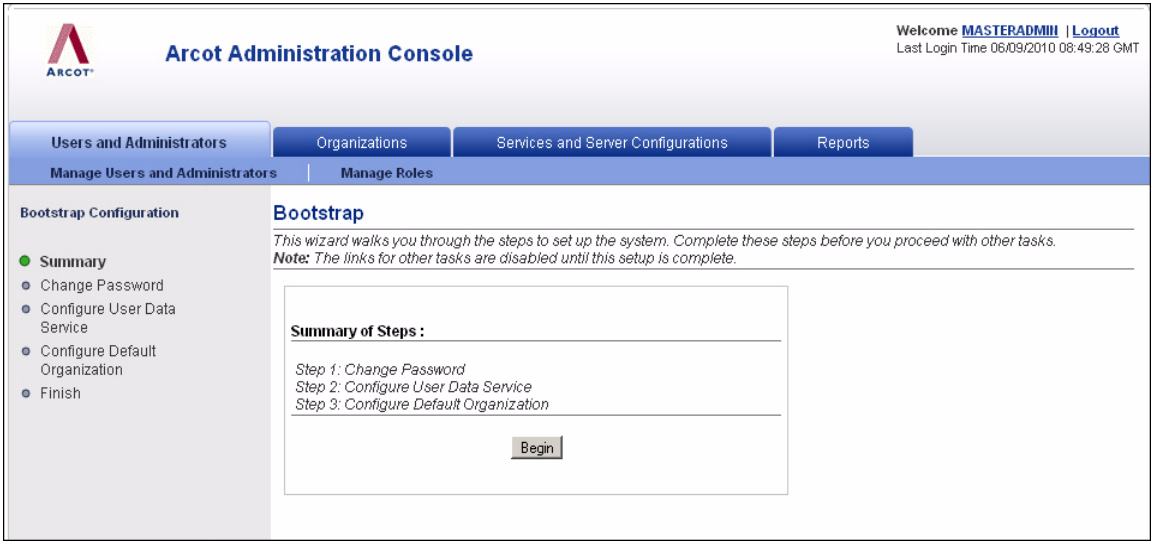
デフォルトの組織

Administration Console を展開すると、組織が 1 つ自動的に作成されます。この組織を、デフォルトの組織（DEFAULTORG）と呼びます。デフォルトの組織はそれだけで単一組織システムとして、ほかに新しい組織を作らずに使用できます。

ブートストラップ タスクの実行

初めて Master Administrator （MA）として Administration Console にログインすると、ブートストラップ ウィザード画面（図 5-1）の［Summary］画面が表示されます。

図 5-1 ブートストラップ ウィザード：［Summary］画面

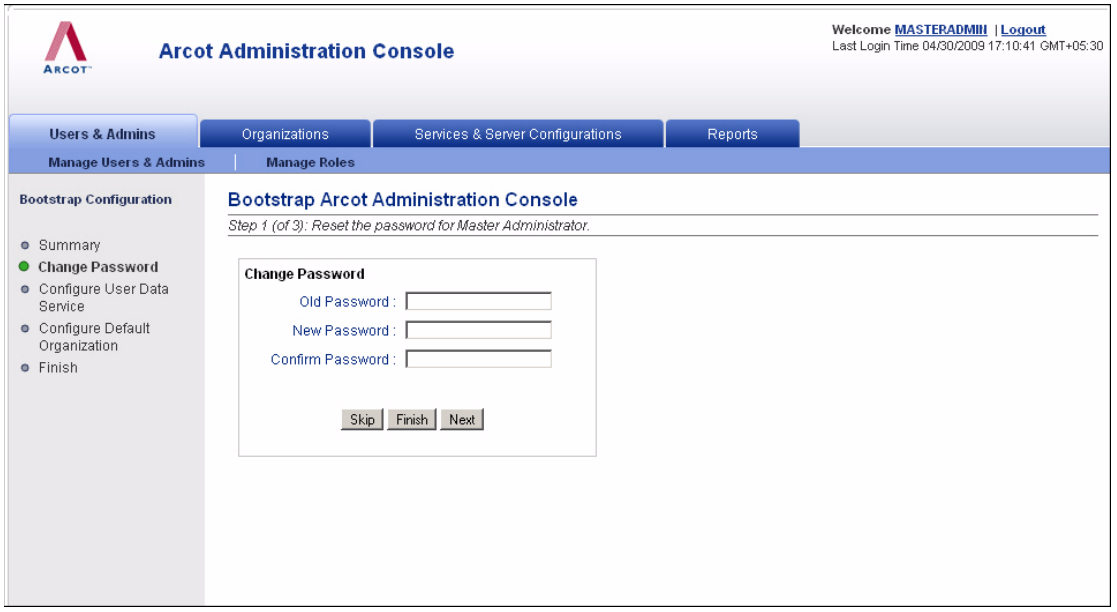


ウィザードを使用してシステムをブートストラップする方法

1. ［**Begin**］をクリックして、プロセスを開始します。

   図 5-2 のような［Change Password］画面が表示されます。

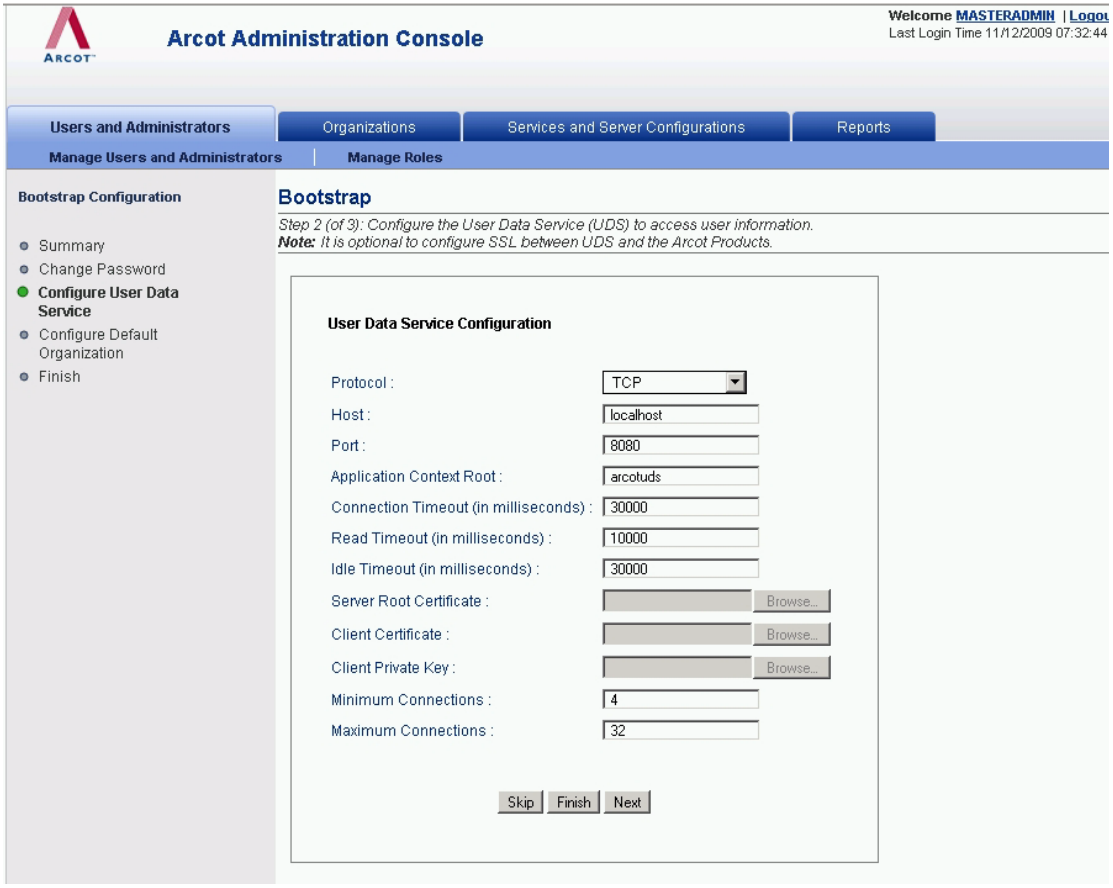
図 5-2 ブートストラップ ウィザード：［Change Password］画面



2. ［**Old Password**］、［**New Password**］、［**Confirm Password**］を指定し、［**Next**］をクリックします。

   図 5-3 のような［Configure User Data Service］画面が表示されます。

図 5-3 ブートストラップ ウィザード：［Configure User Data Service］画面



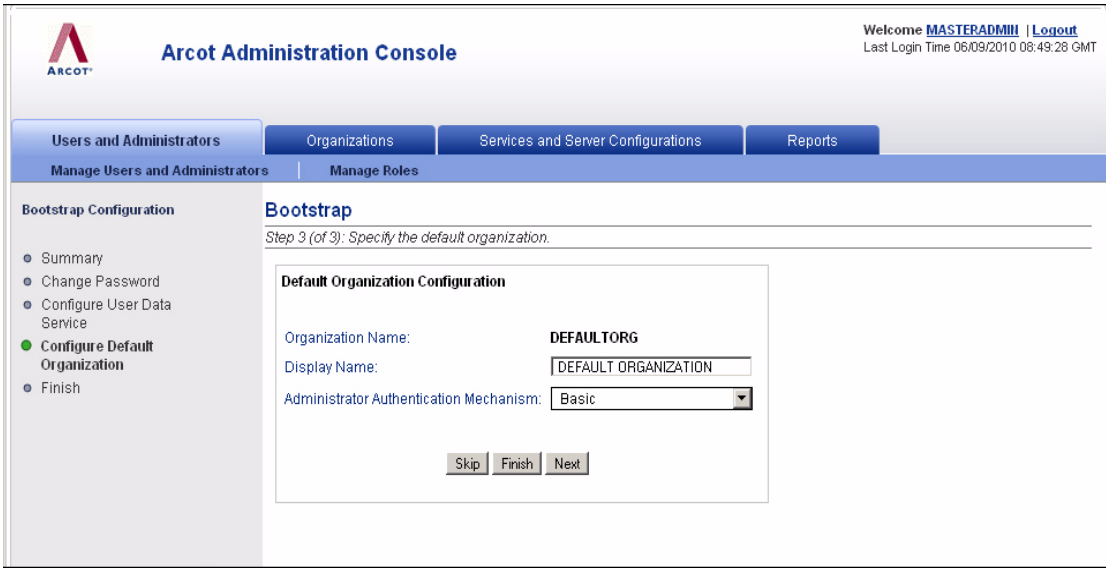
3. 表 5-3 のリスト内のパラメータを指定して、UDS を設定します。

表 5-3. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Protocol	TCP	Administration Console を使用して UDS に接続するためのプロトコル。使用可能なオプションは、以下のとおりです。 • TCP • 一方向 SSL • 双方向 SSL
Host	localhost	UDS が展開されているアプリケーション サーバのホスト名または IP アドレス
ポート	8080	アプリケーション サーバを利用できるポート
Application Context Root	arcotuds	アプリケーション サーバに UDS を定義するために使用されるタグ。 たとえば、*http://<host>:<port>/arcotuds/services* という URL のコンテキスト ルートは arcotuds です。
Connection Timeout（ミリ秒）	30000	UDS サービスが到達不可と見なされるまでの最大時間（**ミリ秒単位**）
Read Timeout（ミリ秒）	10000	UDS からのレスポンスを待機する最大時間（**ミリ秒単位**）
Idle Timeout（ミリ秒）	30000	アイドル接続が終了されるまでの最大時間（**ミリ秒単位**）
Server Root Certificate	デフォルトなし	UDS サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式である必要があります。
Client Root Certificate	デフォルトなし	RiskFort サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式である必要があります。
Client Private Key	デフォルトなし	CA の秘密キーが含まれるファイルの場所
Minimum Connections	4	RiskFort サーバと UDS 間で作成される接続の最小数
Maximum Connections	32	RiskFort サーバと UDS 間で作成できる接続の最大数

図 5-4 のような［Configure Default Organization］画面が表示されます。

図 5-4 ブートストラップ ウィザード：［Configure Default Organization］画面



4. デフォルトの組織用に以下のパラメータを指定します。
   - **表示名**：組織の説明的な名前。この名前が、ほかのすべての Administration Console ページとレポートに表示されます。
   - **認証メカニズム**：デフォルトの組織に所属する管理者を認証するために使用されるメカニズム。Administration Console では、管理者がログインするための認証方式を 2 種類サポートしています。
     - **基本ユーザ パスワード**

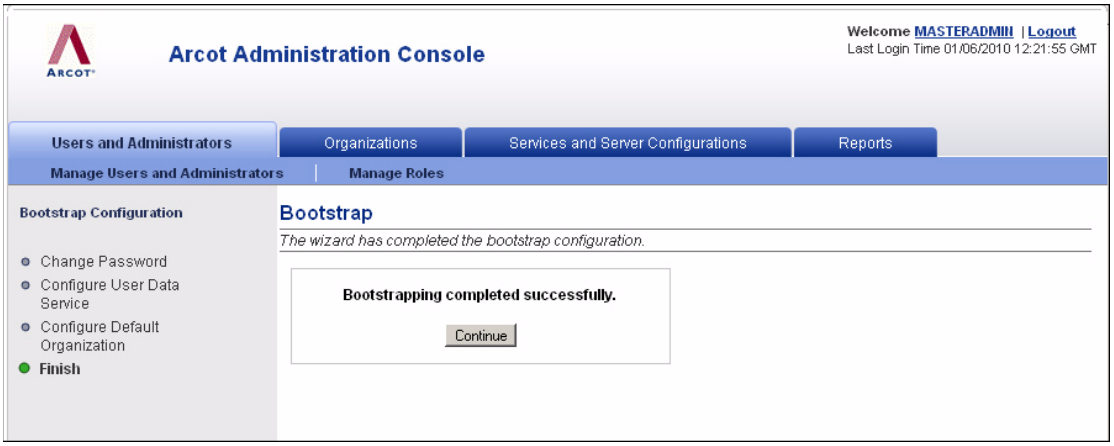
       このオプションを選択すると、Administration Console で提供される組み込みの認証方式が管理者の認証に使用されます。
     - **WebFort ユーザ パスワード**

       ここで［**WebFort User Password**］オプションを選択すると、クレデンシャルが発行され 、WebFort サーバによって認証されます。この場合、Arcot WebFort サーバがインストールされている必要があります。

	関連文書： WebFort のインストールと設定の詳細については、「Arcot WebFort 6.0 インストールおよび展開ガイド」を参照してください。

［Finish］画面（図 5-5）で示されているように、Administration Console の初期化が完了します。

図 5-5 ブートストラップ ウィザード：［Finish］画面



5. ［**Continue**］をクリックし、Administration Console を使用してほかの設定を続行します。

RiskFort サーバの起動

RiskFort サーバを起動する方法

1. 以下のディレクトリに移動します。

   `<install_location>/arcot/bin/`

2. `./riskfortserver start` コマンドを実行します。

> **注：** RiskFort サーバを停止する場合は、`bin` ディレクトリに移動し、`./riskfortserver stop` コマンドを入力します。

Case Management Queuing サーバの開始

Case Management サーバを**開始**する方法

1. 以下のディレクトリに移動します。

   `<install_location>/arcot/bin/`

2. ./casemanagementserver start コマンドを実行します。

注： Case 管理サーバを停止する場合は、bin ディレクトリに移動し、./casemanagementserver stop コマンドを入力します。

Case 管理サービスが正常に開始されているかどうかを**確認**する方法

1. 次のディレクトリに移動します。

   <*install_location*>/arcot/**logs**/

2. 任意のエディタで arcotriskfortcasemgmtserver.log ファイルを開き、以下の行を見つけます。
   - STARTING Arcot RiskFort Case Management 2.2.6_s
   - STARTING Arcot RiskFort Case Management 2.2.6_l
   - Arcot RiskFort Case Management Service READY

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

インストールの確認

サーバが正常に開始したかどうかを確認する方法

1. 次のディレクトリに移動します。

   <*install_location*>/arcot/**logs**/

2. 任意のエディタで arcotriskfort.log ファイルを開き、以下の行を見つけます。
   - **Solaris の場合：** Arcot RiskFort 2.2.6_s を開始しています
   - **RHEL の場合：** Arcot RiskFort 2.2.6_l を開始しています
   - Arcot RiskFort サービスの準備が整いました

注： また、ログ ファイルに「FATAL」と「WARNING」のメッセージが含まれていないことを確認することもお勧めします。

2 つ目のシステムへのインストール

RiskFort サーバと Administration Console のインストール後、この分散環境内の 2 つ目のシステムに残りのコンポーネントをインストールする必要があります。インストールする個々のコンポーネントは、第 2 章の「展開の計画」で計画を立てたときに決定されている必要があります。

インストールを実行する前に、第 3 章の「インストールの準備」の説明に従って、前提条件となるソフトウェア コンポーネントがすべてこのシステムにインストールされていることを確認してください。

2 つ目以降のシステムに RiskFort コンポーネントをインストールする方法

1. インストーラ ファイルをターゲット（2 つ目の）システムにコピーします。
   - **Solaris の場合：**

     ```
     Arcot-RiskFort-2.2.6-Solaris.tar.gz
     ```
   - **Linux の場合：**

     ```
     Arcot-RiskFort-2.2.6-Linux.tar.gz
     ```
2. 以下のようにインストーラを実行します。
   - **Solaris の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Solaris-Installer.bin
     ```
   - **Linux の場合：**

     ```
     prompt> sh Arcot-RiskFort-2.2.6-Linux-Installer.bin
     ```
3. ［**Choose Install Set**］画面が表示されるまで、手順 6 以降のインストーラ手順に従います。
4. インストールするコンポーネントを選択します。

   通常は、リスク評価と発行用の Java SDK をインストールします。
5. コンポーネントをすべて選択したら、手順 11 から手順 16 の指示に従って、インストールを完了します。

2 つ目のシステムでのインストール後のタスクの実行

Java SDK および Web サービスをインストール済みの 2 つ目のシステム上で、以下のインストール後タスクを実行します。

1. サンプル アプリケーションの展開
2. RiskFort サーバとの通信用サンプル アプリケーションの設定
3. サンプル アプリケーションの使用

注： これらの設定を完了したら、第 6 章の「RiskFort SDK と Web サービスの設定」の説明に従って、RiskFort SDK （および Web サービス）を設定する必要があります。

サンプル アプリケーションの展開

サンプル アプリケーションを使用して、RiskFort が正常にインストールされ、設定されているかどうかを確認できます。また、サンプル アプリケーションは以下についての例を提供します。

- 一般的な RiskFort ワークフロー
- RiskFort API の基本操作（呼び出しと後処理）
- RiskFort と自社アプリケーションの統合

重要： リスク評価 SDK および発行 SDK がインストールされているのと同じアプリケーション サーバ上にサンプル アプリケーションを展開する必要があります。

注： サンプル アプリケーションを製品インストール時にインストールしなかった場合は、インストーラを再度実行し、[**SDKs and Sample Application**] オプションを選択してインストールを続行すれば、サンプル アプリケーションのみをインストールできます。

サンプル アプリケーションを展開する方法

1. アプリケーション サーバ サービスを停止します。
2. 以下の場所から `riskfort-2.2.6-sample-application.war` ファイルを展開します。

<*install_location*>/arcot/**samples**/**java**/

注： また、パッケージ内に riskfort-2.2.6-sample-application.war がある場合は、上記の場所からサンプル アプリケーションファイルを展開することをお勧めします。

3. アプリケーション サーバを再起動します。

RiskFort サーバとの通信用サンプル アプリケーションの設定

riskfort.risk-evaluation.properties ファイルには、RiskFort サーバ情報を読み取るための Java SDK とサンプル アプリケーションのパラメータが含まれています。サンプル アプリケーションの展開後、RiskFort サーバと通信できるようファイルを設定する必要があります。このファイルは、RiskFort サンプル アプリケーション WAR ファイル（riskfort-2.2.6-sample-application.war）を展開した後でのみ利用できます。

riskfort.risk-evaluation.properties ファイルを設定する方法

1. アプリケーション サーバの riskfort.risk-evaluation.properties ファイルに移動します。

   Apache Tomcat の場合、このファイルは以下の場所にあります。

   <*App_Home*/**riskfort--sample-application**>/WEB-INF/classes/**properties**/2.2.6

   ここで、<*App_Home*/**riskfort-2.2.6-sample-application**/> は、RiskFort アプリケーション WAR ファイルが展開されているディレクトリ パスを表しています。

2. エディタ ウィンドウで riskfort.risk-evaluation.properties ファイルを開き、以下のパラメータの値を設定します。

   - HOST.1
   - PORT.1

   ファイル内の残りのパラメータには、デフォルト値が指定されています。必要に応じて、これらの値を変更できます。設定パラメータの詳細については、付録 B の「riskfort.risk-evaluation.properties」を参照してください。

3. （**オプション：**付録 F の 「SSL の設定」で SSL ベースの通信を設定した場合のみ、この手順を実行してください）

   以下のパラメータを設定します。

   - TRANSPORT_TYPE=SSL （デフォルトでは、このパラメータは「TCP」に設定されています）

- CA_CERT_FILE=<*absolute_path_of_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**

4. 変更を保存して、ファイルを閉じます。
5. これらの変更を反映するためにアプリケーション サーバを再起動します。

サンプル アプリケーションの使用

このサブセクションでは、サンプル アプリケーションを使用して実行できるリスク評価操作について説明します。サンプル アプリケーションでの各操作は RiskFort が完全にインストールされ、機能していれば、エラーなく実行されるように設計されています。

サンプル アプリケーションでは、RiskFort 発行および RiskFort サーバが実行できる以下の操作について、その例を示します。

- 初めてのユーザのリスク評価および後評価の実行
- ユーザの作成
- 既知のユーザのリスク評価および後評価の実行
- デフォルト プロファイルの編集およびリスク評価の実行

初めてのユーザのリスク評価および後評価の実行

ユーザのデフォルト プロファイルでリスク評価を実行する方法

1. サンプル アプリケーションが（Web ブラウザ ウィンドウで）開いていることを確認します。サンプル アプリケーションのデフォルト URL は以下のとおりです。

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

2. ［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
3. このページの［**User Name**］フィールドにユーザ（評価対象）の名前を指定します。
4. ユーザが所属する組織の名前を［**User Organization**］フィールドに指定します。
5. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。

   このページには、リスク スコアおよび関連付けられているリスク アドバイスが表示され、指定した組織用に設定されたルールがリスト表示されます。初めてのユーザの場合、結果は **ALERT** になります。

6. ［**Next Step**］をクリックし、［Post Evaluation］ページを開いて、指定したユーザ プロファイルに対して後評価を実行します。

   アプリケーションは後評価を通じて、現在のユーザやユーザが使用しているデバイスに関するフィードバックを RiskFort サーバに提供します。RiskFort では、このフィードバックに基づいて、ユーザ属性やデバイス属性、ユーザとデバイスの関連付けを更新し、その後ユーザのトランザクションに伴うリスクを適宜評価します。

7. ［**Result of Secondary Authentication**］リストから適切なオプションを選択して、2 次認証の結果を指定します。
8. ユーザ名とデバイスの関連付けの名前を［**Association Name**］に指定します。
9. ［**Post Evaluate**］をクリックし、後評価プロセスを完了すると、［Post Evaluation Results］セクションに同じ後評価プロセスの結果が表示されます。

ユーザの作成

ユーザの作成方法

1. Web ブラウザ ウィンドウでサンプル アプリケーションを開きます。サンプル アプリケーションのデフォルト URL は以下のとおりです。

   http://<host>:<port>/riskfort-2.2.6-sample-application/index.jsp

   ［RiskFort Sample Application］ページが表示されます。

2. ［**Create User**］をクリックして、［Create User］ページを開きます。
3. ［**User Name**］フィールドおよび［**Organization Name**］フィールドに一意のユーザ名とその組織名をそれぞれ入力し、［**Create User**］をクリックします。［**Organization Name**］を指定しない場合、ユーザは `defaultorg` 内に作成されます。

   指定したユーザがデータベースに正常に追加されると、「The User is created successfully」というメッセージが表示されます。

4. ［**Main Page**］をクリックして、［RiskFort Sample Application］ページに戻ります。

既知のユーザのリスク評価および後評価の実行

1. サンプル アプリケーションの［Main Page］で［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
2. ［**User Name**］フィールドで、作成済みのユーザの名前を指定します。
3. ユーザの組織を［**User Organization**］フィールドに指定します。
4. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。

リスク アドバイスは通常 **INCREASEAUTH** です。

5. ［**Next Step**］をクリックして、後評価を実行します。
   - リストから［**Result of Secondary Authentication**］を指定します。
   - 必要に応じて［**Association Name**］を編集します。
6. ［**Post Evaluate**］をクリックして、最終的なアドバイスを表示します。

   手順 1 ～手順 4 を繰り返せば、［Risk Evaluation Results］ページの**リスク アドバイス**は **ALLOW** に変わります。

デフォルト プロファイルの編集およびリスク評価の実行

サンプル アプリケーションを使用して、使用しているコンピュータの DeviceDNA、IP アドレス、およびデバイス ID を変更して、さまざまな状況をシミュレートできます。ユーザのデフォルト プロファイルを編集するには、以下の手順に従います。

1. サンプル アプリケーションの［Main Page］で［**Evaluate Risk**］をクリックし、［Risk Evaluation］ページを開きます。
2. ［**User Name**］フィールドで、プロファイルを編集するユーザ名を指定します。
3. ユーザの組織を［**User Organization**］フィールドに指定します。
4. ［**Edit Inputs**］をクリックし、［Edit Risk-Evaluation Inputs］ページを開きます。
5. このページでは、すべてのフィールドがあらかじめ入力されています。1 つ以上の必要なフィールドの値を変更します。
   - **My User Name**
   - **My Org**
   - **Machine Finger Print of My Device**
   - **IP Address of My Machine**
   - **Device ID of My Machine**
6. ［**Evaluate Risk**］をクリックし、［Risk Evaluation Results］ページを開きます。
7. ［**Next Step**］をクリックし、［Post Evaluation］ページを開いて、指定したユーザ プロファイルに対して後評価を実行します。
8. ［**Result of Secondary Authentication**］リストから適切なオプションを選択して、2 次認証の結果を指定します。

9. ［**Post Evaluate**］をクリックし、後評価プロセスを完了すると、同じ後評価プロセスの結果が表示されます。

注： RiskFort コンポーネント間の安全な通信を確保するために、SSL （Secure Socket Layer）トランスポート モードをサポートするよう設定できます。詳細については、付録 F の 「SSL の設定」を参照してください。

インストール後のチェックリスト

RiskFort のインストールと設定の情報でこのチェックリストを記入することをお勧めします。後に実行する各種管理タスクでこれらの情報が必要になります。

表 5-4. インストール時のチェックリスト

情報	エントリ例	実際のエントリ
ARCOT_HOME	/var/opt/arcot/	
システム情報		
ホスト名	my-bank	
ユーザ名	管理者	
パスワード	password1234!	
設定済みコンポーネント	RiskFort サーバ Administration Console ユーザ データ サービス	
Administration Console 情報		
ホスト名	ローカルホスト	
ポート	8080	
Master Administrator パスワード	mypassword1234!	
ユーザ データ サービス情報		
ホスト名	ローカルホスト	
ポート	8080	
アプリケーションのコンテキスト ルート	arcotuds	

第 6 章
RiskFort SDK と Web サービスの設定

この章では、RiskFort が提供するアプリケーション プログラミング インターフェース（API）と Web サービスを設定する手順について説明します。

本章では、以下のトピックを扱います。

RiskFort API

RiskFort には、Java API のセットが Java SDK の形式で付属しており、以下の場所に保存されています。

< インストール場所 >/arcot/**sdk**/**java**/**lib**/**arcot**/

RiskFort に付属する API には、以下のものが含まれます。

リスク評価 API

RiskFort SDK （arcot-riskfort-evaluaterisk.jar）は、リスク評価のロジックが含まれた riskfortAPI パッケージで構成されています。

riskfortAPI パッケージによって、以下の操作を実行できます。

- リスクの評価
- アドバイスの生成
- ユーザとデバイスの関連付けの表示

- 関連付けの削除

発行 API

RiskFort SDK （arcot-riskfort-issuance.jar）には、ユーザのための初期クレデンシャルのプロビジョニングが可能な riskfortIssuanceAPI パッケージも含まれています。

発行 API によって、以下のユーザ管理操作を実行できます。

- ユーザの作成
- ユーザ情報の更新

Java API の設定

このセクションでは、RiskFort および発行 Java API を既存のアプリケーションと共に使用できるように設定する手順について説明します。本セクションには、さらに以下のセクションがあります。

- リスク評価 Java API の設定
- 発行 Java API の設定

リスク評価 Java API の設定

	**重要 :** 設定を実行する前に、RiskFort のインストール時に RiskFort Java API パッケージが正常にインストールされていることを確認してください。

J2EE アプリケーションと共に使用できるように RiskFort リスク評価 API を設定する方法

	**注 :** 以下の手順は Apache Tomcat サーバをベースとしています。設定プロセスは、使用しているアプリケーション サーバによって変わる可能性があります。これらの手順の詳細については、アプリケーション サーバのドキュメントを参照してください。

1. 次の場所から、以下のリストの JAR ファイルをコピーします。

   < インストール場所 >/**arcot**/

コピー先には、<*APP_SERVER_HOME*>ディレクトリ内の適切な場所を選択します。たとえば、Apache Tomcat の場合、コピー先は <Application_Home>/WEB-INF/**lib**/ です。

- /sdk/java/lib/arcot/**arcot_core.jar**
- /sdk/java/lib/arcot/**arcot-riskfort-evaluaterisk.jar**
- /sdk/java/lib/arcot/**arcot-riskfort-mfp.jar**
- /sdk/java/lib/arcot/**arcot-pool.jar**
- /sdk/java/lib/external/**bcprov-jdk14-139.jar**
- /sdk/java/lib/external/**commons-httpclient-3.1.jar**
- /sdk/java/lib/external/**commons-lang-2.0.jar**
- /sdk/java/lib/external/**commons-logging-1.0.4.jar**
- /sdk/java/lib/external/**commons-pool-1.4.jar**
- /sdk/java/lib/external/**json-lib-0.7.1.jar**
- /sdk/java/lib/external/**log4j-1.2.9.jar**
- /sdk/java/lib/external/**oro-2.0.8.jar**
- /sdk/java/lib/external/**xalan-2.7.0.jar**
- /sdk/java/lib/external/**xercesImpl-2.6.2.jar**
- /sdk/java/lib/external/**xml-apis-1.0.b2.jar**
- /sdk/java/lib/external/**xmlParserAPIs-2.6.2.jar**
- /sdk/java/lib/external/**xom-1.1.jar**
- /sdk/java/lib/external/**servlet-api-2.4.jar**

2. log4j.properties.risk-evaluation ファイルと riskfort.risk-evaluation.properties ファイルを設定します。
   - アプリケーションに設定済みの log4j.properties.risk-evaluation ファイルがすでにある場合は、以下のログ設定ファイルとマージします。

     <*インストール場所*>/arcot/sdk/java/properties/**log4j.properties.risk-evaluation**

     および

     <*インストール場所*>/arcot/sdk/java/properties/**riskfort.risk-evaluation.properties**
   - アプリケーションに設定済みの log4j.properties ファイルがない場合 :

i. log4j.properties.risk-evaluation の名前を log4j.properties に変更します。

ii. riskfort.risk-evaluation.properties を log4j.properties にマージします。

iii. log4j.properties ファイルを以下の場所にコピーします。

<*Application_Home*>/WEB-INF/classes/**properties**/

注 : API とその初期化の詳細については、<*install_location*>/arcot/docs/riskfort/**Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip** で RiskFort Javadoc を参照してください。

発行 Java API の設定

重要 : 設定を実行する前に、RiskFort のインストール時に発行 Java API パッケージが正常にインストールされていることを確認してください。

J2EE アプリケーションと共に使用できるように発行 API を設定する方法 :

注 : 以下の手順は Apache Tomcat サーバをベースとしています。設定プロセスは、使用しているアプリケーション サーバによって変わる可能性があります。これらの手順の詳細については、アプリケーション サーバのドキュメントを参照してください。

1. 以下の JAR ファイルを、次の場所から <*APP_SERVER_HOME*> ディレクトリ内の適切な場所にコピーします。

   <*インストール場所*>/**arcot**/

   たとえば、Apache Tomcat の場合、コピー先は <*Application_Home*>/WEB-INF/**lib**/ です。

   - /sdk/java/lib/arcot/**arcot_core.jar**
   - /sdk/java/lib/arcot/**arcot-riskfort-issuance.jar**
   - /sdk/java/lib/arcot/**arcot-pool.jar**
   - /sdk/java/lib/external/**bcprov-jdk14-139.jar**
   - /sdk/java/lib/external/**commons-beanutils-1.7.0.jar**

- /sdk/java/lib/external/**commons-collections-3.1.jar**
- /sdk/java/lib/external/**commons-lang-2.0.jar**
- /sdk/java/lib/external/**commons-logging-1.0.4.jar**
- /sdk/java/lib/external/**commons-pool-1.4.jar**
- /sdk/java/lib/external/**dom4j-1.6.1.jar**
- /sdk/java/lib/external/**jaxen-1.1-beta-8.jar**
- /sdk/java/lib/external/**jdom-1.0.jar**
- /sdk/java/lib/external/**log4j-1.2.9.jar**
- /sdk/java/lib/external/**oro-2.0.8.jar**
- /sdk/java/lib/external/**xalan-2.7.0.jar**
- /sdk/java/lib/external/**xercesImpl-2.6.2.jar**
- /sdk/java/lib/external/**xml-apis-1.0.b2.jar**
- /sdk/java/lib/external/**xmlParserAPIs-2.6.2.jar**
- /sdk/java/lib/external/**xom-1.1.jar**

2. log4j.properties.riskfort-issuance ファイルを設定します。
   - アプリケーションにすでに設定済みの log4j.properties ファイルがある場合は、以下のログ設定ファイルとマージします。

     < インストール場所 >/arcot/sdk/java/properties/**log4j.properties.riskfort-issuance**
   - アプリケーションに設定済みの log4j.properties ファイルがない場合 :
     i. log4j.properties.riskfort-issuance の名前を log4j.properties に変更します。
     ii. このファイルを以下の場所にコピーします。

     <APP_SERVER_ROOT>/WEB-INF/classes/**properties**/

注 : API とその初期化の詳細については、*< インストール場所 >*/arcot/docs/riskfort/**Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip** で発行 Javadoc を参照してください。

RiskFort Web サービスの使用方法

このセクションでは、以下を実行する手順について説明します。

- リスク評価クライアント コードの生成
- 発行クライアント コードの生成
- 管理クライアント コードの生成

重要 : クライアント コードの生成を実行する前に、以降のサブセクションで説明するとおり、RiskFort パッケージが正常にインストールされ、サーバが稼働中であることを*確認する必要があります*。

リスク評価クライアント コードの生成

インストール後、`ArcotRiskFortEvaluateRiskSvc.wsdl` ファイルを使用して、クライアント スタブを生成する必要があります。これによって、Web サービス クライアントは RiskFort サーバとの通信が可能になります。このファイルは、以下のディレクトリにあります。

< インストール場所 >/arcot/wsdls/**riskfort**/

クライアント スタブを生成するには、以下の手順に従います。

1. アプリケーション サーバを停止します。
2. 次のディレクトリに移動します。

   < インストール場所 >/arcot/wsdls/**riskfort**/

3. `ArcotRiskFortEvaluateRiskSvc.wsdl` ファイルを使用して、クライアント コードを生成します。
4. アプリケーション サーバを再起動します。
5. ブラウザ ウィンドウで、以下の URL にアクセスし、クライアントが Web サービスにアクセスできるかどうかを確認します。

   http://<RISKFORT_SERVER_IP>:<PORT>/services/RiskFortEvaluateRiskSvc

注： Web サービスの詳細については、*< インストール場所 >*/arcot/docs/riskfort/**Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip** で RiskFort WSDLdoc を参照してください。

発行クライアント コードの生成

インストール後、ArcotRiskFortIssuanceSvc.wsdl ファイルを使用して、クライアント スタブを生成する必要があります。これによって、RiskFort サーバと通信するための発行 Web サービス クライアント コードを生成できます。このファイルは、以下のディレクトリにあります。

< インストール場所 >/arcot/wsdls/**riskfort**/

クライアント スタブを生成するには、以下の手順に従います。

1. アプリケーション サーバを停止します。
2. 次のディレクトリに移動します。

   < インストール場所 >/arcot/wsdls/**riskfort**/
3. ArcotRiskFortIssuanceSvc.wsdl ファイルを使用して、クライアント コードを生成します。
4. アプリケーション サーバを再起動します。
5. ブラウザ ウィンドウで、以下の URL にアクセスし、クライアントが Web サービスにアクセスできるかどうかを確認します。

   http://<RISKFORT_SERVER_IP>:<PORT>/services/RiskFortIssuanceSvc

注： Web サービスの詳細については、*< インストール場所 >*/arcot/docs/riskfort/**Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip** で発行 WSDLdoc を参照してください。

管理クライアント コードの生成

ARCOT_HOME 内の wsdls/**admin**/ ディレクトリには、付属の WSDL（ArcotRiskFortAdminWebService.wsdl）も含まれています。これを使用して、RiskFort Web サービスと通信するための Web サービス クライアント コードを生成できます。

クライアント スタブを生成するには、以下の手順に従います。

1. アプリケーション サーバを停止します。
2. 次のディレクトリに移動します。

   <インストール場所>/arcot/wsdls/**admin**/
3. ArcotRiskFortAdminWebService.wsdl WSDL を使用して、クライアント コードを生成します。
4. アプリケーション サーバを再起動します。
5. ブラウザ ウィンドウで、以下の URL にアクセスし、クライアントが Web サービスにアクセスできるかどうかを確認します。

   http://<RISKFORT_SERVER_IP>:<PORT>/ArcotRiskFortAdminWebService/services/ArcotRiskFortAdminWebService

注： Web サービスの詳細については、*<インストール場所>*/arcot/docs/riskfort/**Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip** で管理 WSDLdoc を参照してください。

デバイス ID の設定

RiskFort では、トランザクションでユーザが使用するデバイスをデバイス ID を使用して登録し、識別します。デバイス ID は、ユーザのコンピュータ上に cookie として設定する必要があります。この cookie は HTTP cookie または Flash オブジェクトのいずれかになります。

このセクションでは、これらの cookie の設定について説明します。本セクションでは、以下のトピックを扱います。

- HTTP cookie の設定
- Flash オブジェクトの設定

HTTP cookie の設定

完全インストール（詳細については、4-47 ページの「Complete インストールの実行」を参照）を実行するか、［Choose Install Set］画面（詳細については、5-76 ページの手順 9を参照）で RiskFort 評価 SDK または Web サービスをインストールするよう選択すると、以下のファイルが自動的にインストールされます。

<インストール場所>/arcot/sdk/**javascript**/rfutil.js

このファイルによって、HTTP cookie を取得して設定するための JavaScript 関数が提供されます。

HTTP cookie の設定

HTTP cookie をエンド ユーザのコンピュータ上に設定するには、HTTP cookie を取得または設定するアプリケーション ページ（複数可）に `rfutil.js` を含める必要があります。

以下の手順に従ってください。

1. ページ（`rfutil.js` ファイルを含める先）がある場所に関連する適切な Web アプリケーション ディレクトリに、`rfutil.js` をコピーします。
2. アプリケーションの関連する Web ページに、以下の JavaScript コードを含めます。

```
<script type="text/javascript" src="location_to_rfutil.js"></script>
```

上のコード スニペットの *`location_to_rfutil.js`* は `rfutil.js` への相対パスに置き換えてください。

Flash オブジェクトの設定

完全インストール（詳細については 4-47 ページの「Complete インストールの実行」を参照）を実行するか、［Choose Install Set］画面（詳細については 5-76 ページの手順 9 を参照）で RiskFort 評価 SDK または Web サービスをインストールするよう選択すると、以下のファイルが自動的にインストールされます。

- rfutil.js
- rfdevice.swf
- crossdomain.txt

rfutil.js

このファイルは以下の場所にインストールされます。

< インストール場所 >/arcot/sdk/**javascript**/rfutil.js

このファイルによって、デバイス ID 用の Flash オブジェクトを取得して設定するための JavaScript 関数が提供されます。

重要 : このファイルは、Flash オブジェクトを取得または設定するアプリケーション ページ（複数可）に*含める必要があります。*

rfdevice.swf

このファイルは以下の場所にインストールされます。

< インストール場所 >/arcot/sdk/**flash**/rfdevice.swf

このファイルによって、Flash オブジェクトが管理され、cookie へのクロスドメイン アクセスがサポートされます。その結果、あるドメインのアプリケーション ページから別のドメインに設定されている cookie へのアクセスが可能になります。

重要 : すべてのアプリケーション ページで、rfdevice.swf が同一の完全な URL で*参照される必要があります。*

crossdomain.txt

このファイルは以下の場所にインストールされます。

< インストール場所 >/arcot/sdk/**flash**/crossdomain.txt

このファイルによって、Flash オブジェクトへのアクセスが許可されるドメインのリストが指定されます。デフォルトでは、Flash オブジェクトへのアクセスが許可されるのは、RiskFort Flash ムービーが提供されるドメインのサブドメインのみです。

crossdomain.txt 内のドメイン エントリの形式は以下のとおりです。

```
&domainName=<pipe-separated_domain_list>&
```

重要 : このファイルは rfdevice.swf と同じ場所に*存在する必要があります。*

Flash オブジェクト設定

Flash オブジェクトをエンド ユーザのコンピュータに設定するには、以下の手順に従います。

1. Flash オブジェクトを取得または設定するアプリケーション ページ（複数可）に rfutil.js を含めます。
   a. ページ（rfutil.js ファイルを含める先）がある場所に関連する適切な Web アプリケーション ディレクトリに、rfutil.js をコピーします。
   b. アプリケーションの関連する Web ページに、以下の JavaScript コードを含めます。

```
   <script type="text/javascript"
src="location_to_rfutil.js"></script>
```

   上のコード スニペットの *location_to_rfutil.js* は rfutil.js への相対パスに置き換えてください。

2. rfdevice.swf と crossdomain.txt を適切な Web アプリケーション ディレクトリにコピーします。

重要： crossdomain.txt ファイルは rfdevice.swf と同じ場所に*存在する必要があります。*

3. Flash オブジェクトが複数のドメインからアクセスされる場合、crossdomain.txt に以下の形式でドメインのリストを追加します。

```
&domainName=<pipe-separated_domain_list>&
```

   たとえば、自社のサイトとパートナー サイトからページを集計した Web サイトの場合、エントリは以下のようになります。

```
&domainName=*.my-bank.com|*.my-partner.com&
```

4. すべてのアプリケーション ページで、rfdevice.swf は同じ絶対 URL で参照される必要があります。

   たとえば、rfdevice.swf が login.my-bank.com から提供される場合、両方のサイト（login.my-bank.com および online.my-partner.com）に login.my-bank.com からの rfdevice.swf が含まれる必要があります。

SSL 通信の有効化

RiskFort では、RiskFort サーバとその Java SDK 間の Secure Socket Layer （SSL）通信がサポートされます。RiskFort サーバとクライアント間で SSL を転送モードとして設定する方法の詳細については、使用しているアプリケーション サーバに基づいて、付録 F の 「SSL の設定」を参照してください。

第 7 章
RiskFort のアンインストール

RiskFort をアンインストールするときは、最初に RiskFort スキーマを削除してから、アンインストール処理を行う必要があります。RiskFort をシステムから削除するには、アンインストーラ ファイル（`Uninstall Arcot RiskFort.bin`）を実行できます。アンインストールを完了したら、システムに残っている WAR ファイルや入力内容をクリーンアップするため、アンインストール後のタスクを実行する必要があります。

この章では、RiskFort とそのコンポーネントをアンインストールするための手順について説明します。この章は以下のセクションで構成されます。

1. RiskFort スキーマの削除
2. RiskFort サーバのアンインストール
3. インストール後のタスクの実行

RiskFort スキーマの削除

注： 何らかの理由でデータベースを保持する必要がある場合は、このセクションの指示には*従わないでください*。
この場合のアンインストール手順については、「RiskFort サーバのアンインストール」を参照してください。

RiskFort データベースをアンインストールする方法

1. 以下のディレクトリに移動します。

   < インストール場所 >/arcot/**dbscripts**/

2. 使用しているデータベースに基づき、に移動します。

   - **Oracle の場合：**

     < インストール場所 >/arcot/dbscripts/**oracle**/

3. RiskFort と関連コンポーネントのすべてのデータベース テーブルを削除するには、以下の順序でスクリプトを実行します。

   - `drop-riskfort-2.2.6.sql`

- drop-arcot-common-1.0.sql

RiskFort サーバのアンインストール

RiskFort サーバをアンインストールするには、RiskFort に付属のファイルを削除する必要があります。アンインストールでは、データベースのアンインストールに必要なスクリプトも削除されます。RiskFort データベースを削除する必要がある場合は、作業を続ける前に、「RiskFort スキーマの削除」を参照してください。

RiskFort サーバをアンインストールする方法

1. 以下のコンポーネントを正常にシャットダウンします。
   - RiskFort サーバ
   - 他の RiskFort コンポーネントが展開されているすべてのアプリケーション サーバ
2. Administration Console が開いている場合は閉じます。
3. INI ファイルおよび RiskFort 関連の他のファイルがすべて閉じられていることを確認します。
4. 以下のコマンドを実行して RiskFort のアンインストールを開始します。

   ```
   prompt>< インストール ディレクトリ >/arcot/"Uninstall_Arcot
   RiskFort"/Uninstall_Arcot RiskFort
   ```

   ［Uninstall Arcot RiskFort］画面が表示されます。
5. ウィザード ウィンドウで以下の操作を行います。
   - ［**1**］を指定すると、［**1-Completely remove all features and components.**］オプションが選択されます。このオプションでは、RiskFort のインストール済みコンポーネントをすべてアンインストールできます。
   - ［**2**］を指定すると、［**2-Choose specific features that were installed by InstallAnywhere.**］オプションが選択されます。このオプションでは、選択したコンポーネントだけを現在のシステムからアンインストールできます。
6. **Enter** キーを押して確認し、アンインストールを続けます。

- ［**1**］を指定した場合は、手順 8 に進みます。

注 : アンインストールが完了するまで数分かかる場合があります。

- ［**2**］を指定した場合は、手順 7 に進みます。

  ［**2**］を指定すると、［Choose Product Features］画面が表示されます。この画面には、現在のシステムにインストールされている RiskFort コンポーネントが表示されます。

7. （**特定のコンポーネントをアンインストールする場合のみ**）コンポーネント番号を入力し（カンマで区切って）、**Enter** キーを押します。

注 : アンインストールが完了するまで数分かかる場合があります。

  アンインストールが完了すると、［Uninstall Complete］画面が表示され、コマンド プロンプトに戻ります。

8. **Enter** キーを押してウィザードを終了し、アンインストールを完了します。

インストール後のタスクの実行

すべての RiskFort コンポーネントが削除されていることを確認するために実行する必要のあるアンインストール後の手順は以下のとおりです。

1. アンインストール後に必要なくなった場合は、*< インストール場所 >*/**arcot/** ディレクトリを削除します。

注 : 複数の Arcot 製品がインストールされているシステムで、アンインストールする最後の製品が RiskFort である*場合に限り*、このディレクトリを削除します。

2. *<APP-SERVER-HOME>* 内の適切なサブディレクトリから以下の WAR ファイルをアンインストールします。

注： ここで、*APP-SERVER-HOME* は、アプリケーション サーバ（Apache Tomcat など）がインストールされているディレクトリ パスを表します。

WAR ファイルのアンインストールの詳細については、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。

- `arcotadmin.war`：Administration Console
- `arcotuds.war`：ユーザ データ サービス
- `riskfort-2.2.6-sample-application.war`：サンプル アプリケーション
- `riskfort-2.2.6-sample-callouts.war`：サンプル コールアウト

注： 分散システム展開を行っている場合は、特定のアプリケーションを展開したシステム上でこれらのファイルを探します。

3. データベースの設定に Oracle データベースを使用した場合は、RiskFort データベースを実行するシステムから `tabspace_arreports_<`*データベースが作成された時刻*`>.dat` ファイルを削除します。
4. RiskFort のインストール中に作成された DSN エントリを削除します。

   このエントリを削除するには、`odbc.ini` ファイルに移動し、テキスト エディタでファイルを開き、対応するデータベース エントリを削除します。ODBC の設定に基づき、このファイルは以下のいずれかの場所にある可能性があります。

   - `/etc/odbc.ini`
   - `/usr/local/etc/odbc.ini`

付録 A
RiskFort のディレクトリ構造

この付録では、RiskFort 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。以下の内容が含まれます。

RiskFort のディレクトリ構造

表 A-1 に、RiskFort 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、このマニュアル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。

	**注：** この表で説明するファイルとディレクトリに加え、`arcot` ディレクトリには `arcotkey` 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 Arcot 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 Arcot 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ついて同じインストール先ディレクトリを確保できなくなり、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やアップグレードには影響しません。

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明
<インストール場所>/arcot/**bin**/ **関連文書：** これらのツールの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。	• RiskFort サーバ • Case Management Queuing サーバ	RiskFort 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。 • arrfadmin.bin（RiskFort 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） • arrfcasemgmtserver.bin（Case Management Queuing サーバ モジュール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.bin（サーバ管理ポートおよび他のサーバ関連操作を設定するためのツール） • arrfupload.bin（Quova データを RiskFort データベースにアップロードするためのツール） • arrfversion.bin（Arcot によって提供されるモジュールのバージョンを確認するためのツール） • DBUtil.bin（RiskFort データベースへの接続に必要な暗号化情報を格納する securestore.enc ファイルを編集するためのツール） RiskFort 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.so • aradminwsprotocol.so • arRiskEngine.so • NameValueXref.so • transwsprotocol.so

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明
	• ユーザ データ サービス（UDS） • Administration Console	• DBUtil.bin（RiskFort データベースへの接続に必要な暗号化情報を格納する securestore.enc ファイルを編集するためのツール）
<インストール場所>/arcot/**conf**/ 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、付録 B の「設定ファイルおよびオプション」を参照してください。	• Administration Console	Administration Console 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 • application.xmlÅiAdministration Console 用の EAR ファイルの作成に必要） • arcotcommon.ini
	• RiskFort サーバ	RiskFort サーバおよび他の RiskFort 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 • riskfortadminclient.ini • riskfortcasemgmtserver.ini • riskfortdataupload.ini • riskfortserver.ini • securestore.enc
	• UDS	UDS によって使用される以下の設定ファイルが含まれます。 • udsserver.ini • application.xml（UDS 用の EAR ファイルの作成に必要）
<インストール場所>/arcot/**dbscripts**/	• Administration Console • RiskFort サーバ • UDS	インストール中に指定したデータベース タイプ（**Oracle**）の RiskFort 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。

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明
<インストール場所>/arcot/docs/**riskfort**/	• RiskFort 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 と発行 SDK 用の Javadoc と WSDLdoc が含まれます。 • Arcot-RiskFort-2.2.6-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） • Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip • Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip • Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip • Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip
	• Administration Console	対応する Administration SDK 用の以下の圧縮された WSDLdoc が含まれます。 • Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip（Admin Web Service の展開に必要な WAR ファイル）
<インストール場所>/arcot/java/**ext**/	• Administration Console • UDS	**ext** サブディレクトリには、使用している OS プラットフォームの securestore.enc の内容の読み取りに使用される以下のファイルが含まれます（適切なサブディレクトリ内）。 • arcot-crypto-util.jar • ArcotAccessKeyProvider.so
<インストール場所>/arcot/java/**lib**/		**lib** サブディレクトリには、Administration Console フレームワークによって必要とされる WAR ファイルが含まれます。 • adminframework.war

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明
<インストール場所>/arcot/java/**webapps**/	• Administration Console	Administration Console 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（Administration Console の展開に必要な WAR ファイル）
	• UDS	UDS によって必要とされる WAR ファイルが含まれます。 • arcotuds.war（UDS の展開に必要な WAR ファイル）
<インストール場所>/arcot/**logs**/	• Administration Console • RiskFort サーバ • Case Management Queuing サーバ • UDS	Administration Console、RiskFort、および UDS によって使用される最新のインストール ファイルと他のログ ファイルが含まれます。 • Arcot_RiskFort_InstallLog.log • arcotadmin.log • arcotriskfort.log • arcotriskfortcasemgmtserver.log • arcotuds.log **backup** サブディレクトリには古いログが含まれます。 **関連文書：** 古いログ ファイルの詳細については、「*Arcot RiskFort 2.2.6 管理ガイド*」の付録 A 「RiskFort ロギング」を参照してください。
<インストール場所>/arcot/**odbc32v60wf**/	• RiskFort サーバ	RiskFort によってサポートされるすべてのデータベース用の、Arcot にブランド設定された DataDirect ODBC ライブラリが含まれます。

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明
<インストール場所>/arcot/**plugins**/**rules**/	• RiskFort サーバ	既定のすべての Riskfort ルールとスコアリングをサポートするすべての SO（ライブラリ バイナリ）ファイルが含まれます。 • **addon/** ディレクトリには、リリースに付属するアドオン ルールの SO ファイルが含まれます。 **重要：** 1 つ以上のカスタム ルールを展開している場合、addon/ ディレクトリには、SO ファイルも含まれている*必要があります*。
<インストール場所>/arcot/**resourcepacks**/	• Administration Console • UDS	Administration Console フレームワークと UDS によって必要とされる以下の Administration Console パック バンドルが含まれます。 • bundler_adminconsole.zip • bundle_riskfort.zip

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明

<インストール場所>/arcot/**samples**/**java**/	• RiskFort サーバ
	• RiskFort 発行 SDK
	• RiskFort リスク管理 SDK
		以下のサブディレクトリがあります。
		• **addonruletype** サブディレクトリには、カスタム ルール タイプとそのパラメータを定義するために使用できるサンプルの XML ファイルが含まれます。
		関連文書： アドオン ルールの詳細とその展開方法の詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
		• **java** サブディレクトリには、以下のための WAR ファイルが含まれます。
		  • riskfort-2.2.6-sample-application.war：RiskFort サンプル アプリケーションの展開に使用します。
		  • riskfort-2.2.6-sample-callouts.war：RiskFort サンプル コールアウトの展開に使用します。

<インストール場所>/arcot/**sdk**/	• RiskFort 発行 SDK • RiskFort リスク管理 SDK	RiskFort によってサポートされる SDK と依存ファイルの **c**、**flash**、および **java** 言語バージョンが含まれます。 **javascript** サブディレクトリには、これらの SDK と DeviceDNA モジュールによって使用される付属の JavaScript が含まれます。 このディレクトリ内容の詳しい説明については、この付録の後半に出てくる「RiskFort 発行 SDK のファイル」と「RiskFort リスク管理 SDK のファイル」を参照してください。
<インストール場所>/arcot/**tools**/**bundlemanager**/	• Administration Console	Administration Console リソースパックによって必要とされるファイルが含まれます。

表 A-1. インストール ディレクトリ構造

ディレクトリ	使用元	ファイル名と説明

<インストール場所>/arcot/**Uninstall_Arcot RiskFort**/	• RiskFort サーバ	RiskFort 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、RiskFort 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。

<インストール場所>/arcot/**wsdls**/	• RiskFort サーバ	Administration Console（**admin** サブディレクトリ）と RiskFort（**riskfort** 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。 このディレクトリ内容の詳しい説明については、この付録の後半に出てくる「RiskFort リスク管理 SDK のファイル」を参照してください。

RiskFort 発行 SDK のファイル

表 A-2 に、発行 SDK によって使用されるファイルのディレクトリの場所を示します。

表 A-2. 発行 SDK のファイル

ディレクトリ	ファイルの説明
<インストール場所>/**arcot**/docs/**riskfort**/	Arcot-RiskFort-2.2.6-issuance-sdk-javadocs.zip ファイルが含まれます。このファイルには発行 SDK 用の Javadoc が含まれます。
<インストール場所>/arcot/**samples**/**java**/	サンプル アプリケーションを展開するための riskfort-2.2.6-sample-application.war ファイルが含まれます。
<インストール場所>/arcot/**sdk**/	RiskFort 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。
<インストール場所>/arcot/**sdk**/**java**/	• **lib** サブディレクトリには、Arcot 提供の JAR ファイルとサードパーティの JAR ファイルが含まれます。 • **properties** ディレクトリには、RiskFort の設定に必要なプロパティ ファイルが含まれます。
<インストール場所>/arcot/**sdk**/**java**/**lib**/**arcot**/	発行 Java SDK によって使用される以下の Arcot JAR ファイルが含まれます。 • arcot_core.jar • arcot-pool.jar • arcot-riskfort-issuance.jar

表 A-2. 発行 SDK のファイル

ディレクトリ	ファイルの説明
<インストール場所>/arcot/sdk/**java**/**lib**/**external**/	RiskFort 発行 Java SDK によって必要とされるサードパーティ JAR ファイルが含まれます。 • bcprov-jdk14-139.jar • commons-beanutils-1.7.0.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-logging-1.0.4.jar • commons-pool-1.4.jar • dom4j-1.6.1.jar • jaxen-1.1-beta-8.jar • jdom-1.0.jar • log4j-1.2.9.jar • oro-2.0.8.jar • servlet-api-2.4.jar • xalan-2.7.0.jar • xercesImpl-2.6.2.jar • xml-apis-1.0.b2.jar • xmlParserAPIs-2.6.2.jar • xom-1.1.jar
<インストール場所>/arcot/**sdk**/**java**/**properties**/	以下のファイルが含まれます。 • log4j.properties.riskfort-issuance • riskfort.issuance.properties

RiskFort リスク管理 SDK のファイル

表 A-3 に、リスク評価 Java SDK によって使用されるファイルのディレクトリの場所を示します。

表 A-3. リスク管理 SDK のファイル

ディレクトリ	ファイルの説明
<インストール場所>/arcot/**docs**/**riskfort**/	Arcot-RiskFort-2.2.6-risk-evaluation-sdk-javadocs.zip ファイルが含まれます。このファイルには、リスク管理 SDK 用の Javadoc が含まれます。
<インストール場所>/arcot/**samples**/**java**/	以下のファイルが含まれます。 riskfort-2.2.6-sample-application.war：RiskFort サンプル アプリケーションの展開に使用します。 riskfort-2.2.6-sample-callouts.war：RiskFort サンプル コールアウト サーバの展開に使用します。
<インストール場所>/arcot/**sdk**/	RiskFort 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。
<インストール場所>/arcot/**sdk**/**flash**/	以下のファイルが含まれます。 • 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。 • rfdevice.swf：デバイス ID Flash オブジェクトを管理します。
<インストール場所>/arcot/**sdk**/**java**/	• **lib** サブディレクトリには、Arcot 提供の JAR ファイルとサードパーティの JAR ファイルが含まれます。 • **properties** ディレクトリには、RiskFort の設定に必要なプロパティ ファイルが含まれます。
<インストール場所>/arcot/sdk/**java**/**lib**/**arcot**/	発行 Java SDK によって使用される以下の Arcot JAR ファイルが含まれます。 • arcot_core.jar • arcot-pool.jar • arcot-riskfort-evaluaterisk.jar • arcot-riskfort-mfp.jar

表 A-3. リスク管理 SDK のファイル

ディレクトリ	ファイルの説明
<インストール場所>/arcot/**sdk**/**java**/**lib**/**external**/	RiskFort 発行 Java SDK によって必要とされるサードパーティ JAR ファイルが含まれます。 • bcprov-jdk14-139.jar • commons-beanutils-1.7.0.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.0.jar • commons-logging-1.0.4.jar • commons-pool-1.4.jar • dom4j-1.6.1.jar • jaxen-1.1-beta-8.jar • jdom-1.0.jar • log4j-1.2.9.jar • oro-2.0.8.jar • servlet-api-2.4.jar • xalan-2.7.0.jar • xercesImpl-2.6.2.jar • xml-apis-1.0.b2.jar • xmlParserAPIs-2.6.2.jar • xom-1.1.jar

表 A-3. リスク管理 SDK のファイル

ディレクトリ	ファイルの説明
<インストール場所>/arcot/**sdk/java/properties/**	以下のファイルが含まれます。 • log4j.properties.risk-evaluation • riskfort.risk-evaluation.properties
<インストール場所>/arcot/**sdk/javascript/**	以下のファイルが含まれます。 • ArcotDeviceDNA.js：デバイス DNA 情報を収集するためにクライアント側で必要になります。 • deployJava.js：エンドユーザ システムに展開された Java コンポーネントを検出するために必要になります。 • FlashDetect.js：エンドユーザ システムに展開された Adobe Flash バージョンを検出するために必要になります。 • json.js：デバイス DNA 情報を収集するためにクライアント側で必要になります。 • PluginDetect.js：エンドユーザ システムに展開されたプラグインを検出するために必要になります。 • rfutil.js：Flash オブジェクトを取得、設定し、flash ディレクトリ内の rfdevice.swf をロードするために必要になります。 • swfobject.js：エンドユーザ システムに展開された Flash コンテンツ（ブラウザからアクセス可能）を検出するために必要になります。

RiskFort の WSDL ファイル

表 A-4 に、リスク管理と発行の WSDL によって使用されるファイルのディレクトリの場所を示します。

表 A-4. RiskFort の WSDL ファイル

ディレクトリ	ファイルの説明
< インストール場所 >/arcot/**docs**/**riskfort**/	RiskFort リスク管理および発行用の圧縮された WSDLdoc が含まれます。 • Arcot-RiskFort-2.2.6-issuance-wsdldocs.zip • Arcot-RiskFort-2.2.6-risk-evaluation-wsdldocs.zip • Arcot-RiskFort-2.2.6-AdminWebService-wsdldocs.zip
< インストール場所 >/arcot/**wsdls**/**admin**/	Administration Console によって必要とされる ArcotRiskFortAdminWebService.wsdl ファイルが含まれます。 この WSDLdoc は、管理 Web サービスについて、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。
< インストール場所 >/arcot/**wsdls**/**riskfort**/	RiskFort によって必要とされる WSDL および XML Schema ファイルが含まれます。 • ArcotRiskFortEvaluateRiskSvc.wsdl（WSDLdoc は、リスク評価 Web サービスについて、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。） • ArcotRiskFortIssuanceSvc.wsdl（WSDLdoc は、発行 Web サービスについて、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。）

付録 B
設定ファイルおよびオプション

この付録では、RiskFort が使用する設定ファイルと、これらのファイル内で設定する必要のあるパラメータについて説明します。また、デフォルト設定ファイルのサンプルも紹介します。

RiskFort にとって重要な設定ファイルは以下のように分類できます。

- INI ファイル
- プロパティ ファイル

INI ファイル

RiskFort の設定用に使用されるプレーンテキストの INI ファイルには以下のものがあります。

- adminserver.ini
- arcotcommon.ini
- riskfortadminclient.ini
- riskfortcasemgmtserver.ini
- riskfortdataupload.ini
- riskfortserver.ini
- udsserver.ini

すべての RiskFort 設定ファイルは、以下のデフォルトの場所にあります。

< *インストール場所* >/arcot/**conf**/

adminserver.ini

adminserver.ini ファイルには、Administration Console のログ情報を設定するためのパラメータが含まれます。表 B-1 に、Administration Console によって使用されるログ ファイル情報を示します。

表 B-1. Administration Console 設定用のパラメータ

パラメータ	デフォルト値	説明
log4j.logger.com.arcot.DEFAULT	INFO、roothandle **重要：** roothandle は UDS ログ ハンドルの名前で、必ず指定する*必要があります。*	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
log4j.logger.com.arcot.admin	INFO、roothandle **重要：** roothandle は UDS ログ ハンドルの名前で、必ず指定する必要があります。	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* • *WARNING* • *INFO* • *DEBUG* **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

表 B-1. Administration Console 設定用のパラメータ

パラメータ	デフォルト値	説明
log4j.logger.com.arcot.admin.framework	INFO	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
log4j.logger.com.arcot.adminconsole	INFO、roothandle **重要：** roothandle は Administration Console ログ ハンドルの名前で、必ず指定する必要があります。	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

表 B-1. Administration Console 設定用のパラメータ

パラメータ	デフォルト値	説明
log4j.logger.com.arcot.database	INFO、roothandle **重要：** roothandle は、Administration Console によって使用されるデータベース用のログ ハンドルの名前で、必ず指定する必要があります。	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
log4j.logger.com.arcot.common.database	INFO、dbfohandle **重要：** dbfohandle はデータベース フェイルオーバ ログ ハンドルの名前で、必ず指定する必要があります。	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
log4j.appender.debuglog.File	${arcot.home}/logs/**arcotadmin.log**	Administration Console ログのファイル名と、ログが作成される場所。 Administration Console 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。 < *インストール場所*>/arcot/**logs**/

表 B-1. Administration Console 設定用のパラメータ

パラメータ	デフォルト値	説明
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。

arcotcommon.ini

arcotcommon.ini ファイルには、RiskFort Sever および RiskFort の他のコンポーネント（Administration Console とユーザ データ サービス）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。

- データベースの設定
- インスタンスの設定
- Watchdog の設定

データベースの設定

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、フェイ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、第 3 章の「インストールの準備」の「データベース サーバの設定」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（Oracle）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。表 B-2 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。

表 B-2. [arcot/db/dbconfig] セクションのデータベース設定パラメータ

パラメータ	デフォルト	説明
DbType	--	すべてのデータベース接続に適用可能なデータベースのタイプ。サポートされる値は以下のとおりです。 • oracle •
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：正しいドライバ名については、JDBC ベンダーのドキュメントで確認してください。以下に例を示します。 • **Oracle:** oracle.jdbc.driver.OracleDriver •
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	32	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	RiskFort 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	4	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。

表 B-2. ［arcot/db/dbconfig］セクションのデータベース設定パラメータ

パラメータ	デフォルト	説明
MaxWaitTimeFor Connection	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）。
AutoRevert	1	フェイ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、またはフェイルオーバ発生後にサーバがデータベースに接続するようにしたい場合は、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 メッセージのログを記録するかどうか。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	0	ブランド設定された ODBC ドライバを使用するかどうか。
BrandLicenseFile	IVWF.LIC	ブランド設定された ODBC ドライバを使用する場合のライセンス 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、RiskFort 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>`
- `Username.<N>`
- `URL.<N>`

表 B-3 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。

表 B-3. [arcot/db/primarydb] セクションのプライマリ データベース パラメータ

パラメータ	デフォルト値	説明
Datasource.<*N*>	デフォルト値なし	サーバ データをホストしているプライマリ データベースを参照する ODBC システム データ ソース名（DSN）。
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 名によるプールは収容側とな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、Arcot Web アプリケーションが接続プールを使用できるように、アプリケーションに十分なアクセス権限を付与する必要があります。 • 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。以下に例を示します。 • 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。以下に例を示します。 • AppServerConnectionPoolName.1=SampleDS 詳細については、付録 E の 「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:< サーバ >:< ポート >:<SID> •

表 B-3. [arcot/db/primarydb] セクションのプライマリ データベース パラメータ

パラメータ	デフォルト値	説明
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。
TrustStorePath	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。 **関連文書：** dbutil の詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

[arcot/db/backupdb]

このセクション [arcot/db/backupdb] では、フェイ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。複数のフェイルオーバ 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*>
- Username.<*N*>
- URL.<*N*>
- TrustStorePath

このセクションは、[arcot/db/primarydb] セクションと同じパラメータを使用します。このセクションのデータベース設定パラメータのリストについては、表 B-3 を参照してください。

インスタンスの設定

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。RiskFort 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。表 B-4 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。

表 B-4. [arcot/system] セクションのインスタンス パラメータ

パラメータ	デフォルト値	説明
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。サーバのすべてのインスタンスに一意の値を指定することをお勧めします。 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。

Watchdog の設定

このセクションでは、UNIX プラットフォーム上の RiskFort サーバ インスタンスを監視する Watchdog プロセスの設定を指定できます。表 B-5 に、[arcot/watchdog] セクションの Watchdog の設定パラメータを示します。

表 B-5. [arcot/watchdog] セクションのパラメータ

パラメータ	デフォルト値	説明
ServerStartsTimeout	25	サーバ起動からの経過時間（分単位）。ServerStartsTimeout の指定時間（25 分）内に Watchdog プロセスがサーバを 5 回再起動した場合、それ以降サーバは再起動されません。
ServerStartsCount	5	サーバを再起動する最大回数。この回数を過ぎると、それ以降サーバは再起動されません。
RestartSleepTime	5000	Watchdog がサーバの再起動を開始するまでのスリープ時間（ミリ秒単位）。

riskfortadminclient.ini

riskfortadminclient.ini ファイルは、**arrfadmin** システム管理ツール（RiskFort インストール後の ARCOT_HOME の bin ディレクトリ内）が、ツール自身と RiskFort の間で双方向 SSL 接続を確立する際に役立ちます。

riskfortadminclient.ini ファイルは以下の場所にあります。
< *インストール場所* >/arcot/**conf**/

表 B-6 に、このファイル内のパラメータを示します。

表 B-6. riskfortadminclient.ini ファイルのパラメータ

パラメータ	デフォルト値	説明
Host	localhost	RiskFort 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。
Port	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。以下の値を使用できます。 • TCP • SSL
SSLClientKey	デフォルト値なし	arrrfadmin ツールによって使用される base64 エンコードされた（PEM 形式）SSL キーの絶対パス（ツールと RiskFort サーバの間で双方向 SSL 通信が必要な場合）。
SSLClientCertChain	デフォルト値なし	arrrfadmin ツールによって使用される base64 エンコードされた（PEM 形式）SSL 証明書または証明書チェーンの絶対パス（ツールと RiskFort サーバの間で双方向 SSL 通信が必要な場合）。
SSLServerCACert	デフォルト値なし	arrrfadmin ツールと RiskFort サーバの間での SSL 通信時、ツールが信頼する必要のある base64 エンコードされた（PEM 形式）SSL CA 証明書の絶対パス。

riskfortcasemgmtserver.ini

riskfortcasemgmtserver.ini ファイルを使用すると、RiskFort の Case Management モジュールに対して以下の設定を行うことができます。

- ログ ファイルの設定
- Case Management Queuing Server の設定

ログ ファイルの設定

RiskFort Case Management Queuing Server モジュールは、Case Management 関連のすべてのアクションを arcotriskfortcasemgmtserver.log ファイルに記録します。このファイルのデフォルトの場所は以下のとおりです。

< インストール場所 >/arcot/**logs**/

サーバ ログ ファイルのログ ファイル名は INI ファイルで定義できます。プライマリ ログ ファイルの最大ファイル サイズを定義することもできます。プライマリ ログ ファイルが最大サイズに達すると、新しいアクションは新しいプライマリ ログ ファイル（arcotriskfortcasemgmtserver.log の新しいインスタンス）に記録されます。

ログ記録に関連するパラメータはすべて、arcotriskfortcasemgmtserver.ini ファイルの [arcot/riskfortcasemgmtserver/logger] セクションにあります。表 B-7 に、riskfortcasemgmtserver.ini ファイルのログ ファイル設定パラメータとその説明を示します。

表 B-7. riskfortcasemgmtserver.ini のログ ファイル パラメータ

パラメータ	デフォルト値	説明
LogFile	logs/arcotriskfortcasemgmtserver.log	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（*< インストール場所 >*/arcot/）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	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 ファイルが維持されるディレクトリの場所。 注：このパスは ARCOT_HOME（*< インストール場所 >*/arcot/）からの相対パスです。

表 B-7. riskfortcasemgmtserver.ini のログ ファイル パラメータ

パラメータ	デフォルト値	説明
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）。 以下の値を使用できます。 • 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。 以下の値を使用できます。 • 0 ローカル時間 • 1 GMT

Case Management Queuing Server の設定

表 B-8 に示す Case Management のスレッド設定は、riskfortcasemgmtserver.ini ファイルの [arcot/riskfortcasemgmtserver/server] セクションにあります。これらのエントリを削除またはコメント アウトした場合、Case Management Queuing Server は無限待機にデフォルト設定されます。

表 B-8. Case Management Queuing Server の構成設定パラメータ

パラメータ	デフォルト値	説明
MaxThreads	128	Case Management コールに常に対応するために、この Server モジュールが維持できるスレッドの最大数。 **注：** この値は、サーバが処理できる同時リクエスト数に直接影響します。
MinThreads	32	Case Management コールに常に対応するために、この Server モジュールが維持する必要のあるスレッドの最小数。
ReadTimeout	7200000	Case Management Queuing Server が接続を閉じる前にレスポンスを待機する最大時間（**ミリ秒**単位）。

riskfortdataupload.ini

RiskFort 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。

RiskFort には、Quova ファイルから RiskFort 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、Arcot RiskFort 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、Arcot RiskFort 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。

<インストール場所>/arcot/**conf**/

表 B-9 に、このファイルの設定パラメータを示します。

表 B-9. riskfortdataupload.ini の設定パラメータ

パラメータ	デフォルト値	説明
Tables	ロードしない	ユーザが操作できるテーブル。 以下の値を使用できます。 • 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。 以下の値を使用できます。 • 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。 以下の値を使用できます。 • 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。

riskfortserver.ini

riskfortserver.ini ファイルを使用すると、以下の設定を構成できます。

- ログ ファイルの設定（[arcot/riskfort/logger]）
- スレッドの設定（[arcot/riskfort/server]）
- その他のサーバ設定

ログ ファイルの設定（[arcot/riskfort/logger]）

RiskFort では、すべてのシステム アクションが arcotriskfort.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。

<インストール場所>/arcot/**logs**/

サーバ ログ ファイルのログ ファイル名は INI ファイルで定義できます。プライマリ ログ ファイルの最大ファイル サイズを定義することもできます。プライマリ ログ ファイルが最大サイズに達すると、新しいアクションは新しいプライマリ ログ ファイル（arcotriskfort.log の新しいインスタンス）に記録されます。

ログ記録に関連するパラメータはすべて、riskfortserver.ini ファイルの [arcot/riskfort/logger] セクションにあります。表 B-10 に、riskfortserver.ini ファイルのログ ファイル設定パラメータとその説明を示します。

表 B-10. riskfortserver.ini のログ ファイル パラメータ

パラメータ	デフォルト値	説明
LogFile	logs/arcotriskfort.log	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（*<インストール場所>*/arcot/）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。

表 B-10. riskfortserver.ini のログ ファイル パラメータ

パラメータ	デフォルト値	説明
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 ファイルが維持されるディレクトリの場所。 注：このパスは ARCOT_HOME（<インストール場所>/arcot/）からの相対パスです。
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）。 以下の値を使用できます。 • 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。 以下の値を使用できます。 • 0 ローカル時間 • 1 GMT

スレッドの設定（[arcot/riskfort/server]）

スレッドとは、プログラム内で発生する一連の制御フローのひとまとまりを指します。プロセス（またはプログラムの実行）に似ていますが、スレッドはリソース管理がそれほど必要でないので、プロセスより容易に作成、破棄できます。各スレッドにはそれ自身のリソースが必要です。マルチスレッド環境では、複数のスレッドを生成し、同時に動作させることができます。つまり、システムはすべてのスレッドについて 1 つの環境を共有できるので、個々のスレッドによるオーバーヘッドが低下します。

システムで使用できるスレッドの最大数と最小数を決定する際は、考慮すべき 3 つの要素があります。

1. 各スレッドは特定量のリソースを使用し、システムの全体的なパフォーマンスを低下させます。
2. スレッドの開閉処理には、開いている状態のスレッドの維持に必要なリソースの最大 3 倍のリソースが必要になります。

3. サーバの能力に基づき、サーバ パフォーマンスが許容レベルを下回る前の段階で同時に開くことのできるスレッドの数には上限があります。

推奨事項としては、システムの平均的な使用レベルに対応するために必要な最小限のスレッド数を設定することです。スレッドの最大数については、システムで発生する可能性のあるピーク負荷に常に対応できると同時に、許容レベルのサーバ パフォーマンスを維持するのに十分な高さに設定します。

RiskFort のスレッド設定は、`riskfortserver.ini` ファイルの `[arcot/riskfort/server]` セクションにあります。表 B-11 に、`ini` ファイルのスレッド設定パラメータとその説明を示します。

表 B-11. スレッド設定のパラメータ

パラメータ	デフォルト値	説明
`MaxThreads`	128	リスク評価および発行コールに常に対応するために、RiskFort サーバが維持できるスレッドの最大数。 **注：** この値は、サーバが処理できる同時リクエスト数に直接影響します。
`MinThreads`	32	リスク評価および発行コールに常に対応するために、RiskFort サーバが維持する必要のあるスレッドの最小数。
`MaxTransWSThreads`	128	発行およびリスク評価 Web サービスが維持できるスレッドの最大数。
`MinTransWSThreads`	32	発行およびリスク評価 Web サービスが常に維持する必要のあるスレッドの最小数。
`MaxAdminWSThreads`	32	管理 Web サービスが維持できるスレッドの最大数。
`MinAdminWSThreads`	16	管理 Web サービスが常に維持する必要のあるスレッドの最小数。

その他のサーバ設定

表 B-12 に示すその他のサーバ構成設定は、riskfortserver.ini ファイルの [arcot/riskfort/server] セクションにあります。これらのエントリを削除またはコメント アウトした場合、RiskFort サーバは無限待機にデフォルト設定されます。

表 B-12. サーバ構成設定のパラメータ

パラメータ	デフォルト値	説明
ReadTimeout	7200000	発行およびリスク評価 API が RiskFort サーバからのレスポンスを待機する最大時間（**ミリ秒**単位）。
ReadTimeoutTransWS	7200000	発行およびリスク評価 Web サービスが RiskFort サーバからのレスポンスを待機する最大時間（**ミリ秒**単位）。
ReadTimeoutAdminWS	7200000	管理 Web サービスが RiskFort サーバからのレスポンスを待機する最大時間（**ミリ秒**単位）。

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ます。表 B-13 に、RiskFort 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。

表 B-13. UDS およびデータベース フェイルオーバ設定用のパラメータ

パラメータ	デフォルト値	説明
log4j.logger.com.arcot.uds	INFO、debuglog **重要：** debuglog は UDS ログ ハンドルの名前で、必ず指定する*必要があります。*	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
log4j.logger.com.arcot.common.database	INFO、dbfohandle **重要：** dbfohandle はデータベース フェイルオーバ ログ ハンドルの名前で、必ず指定する*必要があります。*	

表 B-13. UDS およびデータベース フェイルオーバ設定用のパラメータ

パラメータ	デフォルト値	説明
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。 *< インストール場所 >*/arcot/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。

プロパティ ファイル

RiskFort は主に、以下のサブ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。

- riskfort.risk-evaluation.properties
- riskfort.issuance.properties
- log4j.properties.risk-evaluation
- log4j.properties.riskfort-issuance

これらのファイルは以下の場所にあります。

< インストール場所 >/arcot/sdk/java/**properties**/

riskfort.risk-evaluation.properties

riskfort.risk-evaluation.properties ファイルには、RiskFort リスク評価 Java SDK とサンプル アプリケーションが RiskFort サーバ情報を読み取るためのパラメータが含まれます。表 B-14 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。

表 B-14. リスク評価 Java SDK と RiskFort サーバ間の通信用のパラメータ

パラメータ	デフォルト値	説明
HOST.1	localhost	RiskFort サーバの IP アドレス。
PORT.1	7680	RiskFort サーバが受信リクエストを待ち受けるポート番号。
CONNECTION_TIMEOUT	30000	RiskFort 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	1	RiskFort サーバで許可される最大試行回数。
READ_TIMEOUT	30000	RiskFort 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）。
MAX_ACTIVE	128	RiskFort 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。正の値でない場合、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。
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）。 **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する必要があります（SDK と RiskFort 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）。

表 B-14. リスク評価 Java SDK と RiskFort サーバ間の通信用のパラメータ

パラメータ	デフォルト値	説明
WHEN_EXHAUSTED_ACTION	BLOCK	すべての接続が使い果たされた場合の動作。
TRANSPORT_TYPE	TCP	RiskFort サーバが起動するためのデフォルト値は TCP です。 RiskFort 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、Administration Console と RiskFort 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、RiskFort サーバを再起動する*必要があります。*
CA_CERT_FILE	*< サーバの CA 証明書（PEM 形式）のファイル パス >*	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： server.CACert=*< インストール場所 >*/certs/ca.pem または server.CACert=*< インストール場所 >*\\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。

riskfort.issuance.properties

riskfort.issuance.properties ファイルには、RiskFort 発行 Java SDK とサンプル アプリケーションが RiskFort サーバ情報を読み取るためのパラメータが含まれます。

注： このファイルに含まれる設定パラメータとデフォルト値は riskfort.risk-evaluation.properties と同じですが、指定する値が異なる可能性があります。発行関連の操作で発生するタイム ラグに対応するために異なる値を指定する必要のある場合があります。

このファイルの設定パラメータの詳細については、表 B-14 を参照してください。

log4j.properties.risk-evaluation

log4j.properties.risk-evaluation ファイルは、RiskFort 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。表 B-15 に、RiskFort リスク管理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。

表 B-15. log4j.properties.risk-evaluation **設定用のパラメータ**

パラメータ	デフォルト値	説明
log4j.logger.com.arcot	INFO	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 • WARNING • INFO • DEBUG **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
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 （RiskFort Java SDK の場合） • arriskfortws.log （RiskFort Web Service の場合）

表 B-15. `log4j.properties.risk-evaluation` **設定用のパラメータ**

パラメータ	デフォルト値	説明
`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。
`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。

log4j.properties.riskfort-issuance

`log4j.properties.riskfort-issuance` ファイルは、RiskFort とその発行コンポーネントのログ記録の動作を指定します。表 B-16 に、RiskFort 発行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提供します。

表 B-16. `log4j.properties.riskfort-issuance` **設定用のパラメータ**

パラメータ	デフォルト値	説明
`log4j.logger.com.arcot`	INFO	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` • `WARNING` • `INFO` • `DEBUG` **関連文書：** ログ レベルの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。
`log4j.logger.com.arcot .riskfortissuanceAPI`	DEBUG	
`log4j.appender.debuglog.File`	`arcot-riskfort-issuance.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。 • `arcotissuance.log` （発行 Java SDK の場合） • `arissuancews.log`（発行 Web サービスの場合）

表 B-16. `log4j.properties.riskfort-issuance` **設定用のパラメータ**

パラメータ	デフォルト値	説明
`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。
`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 C
データベース リファレンス

RiskFort 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、製品を多く使うほど拡大するものがあります。ユーザ数に比例して拡大するテーブルもあれば、製品の使用頻度に比例して拡大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、RiskFort 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する必要があります。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： 設定とデータ レポートの必要性に基づいて、SQL データベースに対して適切な調整を行うことをお勧めします。たとえば、大量のデータを削除すると、削除処理中のパフォーマンスに悪影響が生じます。ロールバック セグメントのサイズによっては、システムが停止してしまう可能性すらあります。古い記録はアーカイブし、完全に削除しないことを強くお勧めします。

この付録では、データベース テーブルの複製に関する推奨事項、RiskFort 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、RiskFort 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。

RiskFort データベースのテーブル

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。

- RiskFort によって使用されるデータベース テーブル
- Administration Console と UDS によって使用されるデータベース テーブル

RiskFort によって使用されるデータベース テーブル

表 C-1 に、すべての RiskFort データベース テーブルとその説明を示します。

表 C-1. RiskFort のテーブル

テーブル名	説明
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、RiskFort 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、RiskFort 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、RiskFort 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、RiskFort 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。
ARREPORTTABLES	他のテーブルのメタデータが含まれます。

表 C-1. RiskFort のテーブル

テーブル名	説明
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	展開したアドオン 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アドオン 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 Arcot サポート（*support@arcot.com*）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。これはリスト検索ルール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。このデータは派生するリスト検索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アドオン 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。
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。

表 C-1. RiskFort のテーブル

テーブル名	説明
ARRFCASECONFIG	Case Management モジュールの設定データが格納されます。
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。
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-RiskFort 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。
ARRFCONFIG	RiskFort のグローバル設定情報が格納されます。
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。
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。
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 RiskFort 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 Arcot サポート（*support@arcot.com*）にお問い合わせいただくことをお勧めします。

表 C-1. RiskFort のテーブル

テーブル名	説明
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。
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。
ARRFDISPLAYNAMES	Administration Console 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。
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。
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アドオン 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。
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。 **注：** 現在、組織あたり 1 つのデフォルト キュー*だけ*がサポートされています。

表 C-1. RiskFort のテーブル

テーブル名	説明
ARRFPROTOCOLREGISTRY	RiskFort 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。
ARRFSERVERS	使用可能な RiskFort 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-RiskFort 統合展開でのみ適用されます。
ARRFSYSAUDITLOG	リスク評価およびログに記録される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。
ARRFSYSPARAMSCONFIG	Administration Console を使って設定できるすべての RiskFort システム パラメータに関する詳細情報が含まれます。
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。
ARRFUNTRUSTEDIPLIST	すべての拒否 IP アドレスの詳細が格納されます。
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。

表 C-1. RiskFort のテーブル

テーブル名	説明
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。

Administration Console と UDS によって使用されるデータベース テーブル

表 C-2 に、すべての RiskFort データベース テーブルとその説明を示します。

表 C-2. Administration Console のテーブル

テーブル名	説明
Administration Console のテーブル	
ARADMINAUDITTRAIL	管理者のアクティビティ監査が含まれます。
ARADMINBASICAUTHUSER	管理者の基本認証クレデンシャルが含まれます。
ARADMINCACHEREFRESH	Administration Console でキャッシュをリフレッシュする必要があるかどうかを決めるキャッシュ リフレッシュ情報が含まれます。
ARADMINCONFIG	Administration Console の設定が含まれます。
ARADMINCUSTOMROLE	カスタム定義ロールの設定が含まれます。
ARADMINMANAGEROLE	ロールが管理できるロールのリストが含まれます。
ARADMINMAP	キーと値のペアとして入力される、RiskFort サーバ インスタンスの情報が含まれます。
ARADMINMAPDATATYPE	ARADMINMAP でサポートされているデータ型のリストが含まれます。
ARADMINPAFCONFIG	組織の管理者認証設定が含まれます。
ARADMINPREDEFINEDROLE	サポートされているすべての管理者のロール情報が含まれます。
ARADMINPWDPOLICY	すべての組織の管理者パスワード ポリシーが含まれます。
ARADMINROLEPRIVILEGE	Administration Console 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。

表 C-2. Administration Console のテーブル

テーブル名	説明
ARADMINSCOPE	管理者が管理権を持つ一連の組織の情報が含まれます。
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を持つすべての管理者のリストが含まれます。
ARADMINSUPPORTEDAUTHMECH	Administration Console 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含まれます。
ARADMINTURNEDOFFPRIVILEGE	特定のカスタム ロールで使用できない権限に関する情報が含まれます。
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含まれます。
ARADMINUITAB	使用可能なタブに関する情報と、それらのタブを Administration Console で使用できる順序に関する情報が含まれます。
ARADMINUITASK	使用可能なタスクに関する情報と、それらのタスクを Administration Console で使用できる順序に関する情報が含まれます。
ARADMINUITASKATTRIBUTES	Administration Console の第 1 レベル タブと第 2 レベル タブをクリックしたときに表示されるタスクの詳細が含まれます。このようなタスクは待ち受け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含まれます。タスク コンテナは、Administration Console 内の第 2 レベル 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、ロケールなど）が含まれます。
ARADMINWIZARDTASK	ブートストラップ ウィザードを使って実行されるすべてのタスクに関する情報が含まれます。
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 状態値が含まれます。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イルオーバー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。
UDS のテーブル	
ARUDSAUDITLOG	ユーザ データ ソース（UDS）の操作とそのリターン ステータスの監査ログ情報が含まれます。
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含まれます。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。
ARUDSCONFIG	UDS 設定パラメータとその値が含まれます。

表 C-2. Administration Console のテーブル

テーブル名	説明
ARUDSORGANIZATION	組織の定義、その属性、およびリポジトリ接続の詳細が含まれます。
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含まれます。
ARUDSUSER	組織に所属するすべてのユーザの詳細と属性が含まれます。
ARUDSUSERATTRIBUTE	すべてのユーザ属性定義が含まれます。このテーブルは、個々の製品によって新規ユーザ属性が追加される場合を除き、ほとんど変更されないことが想定されています。

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 RiskFort 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

計算のため以下の前提値が使用されています。

- 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。以下のトピックで構成されます。

- リアルタイム同期が必要なテーブル
- 定期的な同期が必要なテーブル
- 同期が必要ないテーブル

リアルタイム同期が必要なテーブル

表 C-3 に、プライマリ データベースとバックアップ データベースの間でのリアルタイム同期を必要とするデータベース テーブルを示します。このカテゴリに入るのは主に、ユーザ関連情報が含まれるテーブルです。ユーザ データは認証に必要とされるので、このようなテーブルにはリアルタイム同期を実行する必要があります。

表 C-3. リアルタイム同期が必要なテーブル

テーブル	説明
ARADMINAUDITTRAIL	RiskFort 管理アクティビティの監査ログ情報が含まれます。
ARADMINBASICAUTHUSER	管理者の基本認証クレデンシャルが含まれます。
ARADMINSCOPE	管理者が管理権を持つ一連の組織の情報が含まれます。
ARADMINSCOPEALL	既存の組織および将来作成される組織すべてに管理権を持つ管理者のリストが含まれます。
ARADMINUSER	管理者の情報が含まれます。
ARADMINTXID	トランザクション ID を生成するのに必要な情報が含まれます。
ARUDSORGANIZATION	組織の定義、その属性、およびリポジトリ接続の詳細が含まれます。
ARUDSUSER	組織に所属するユーザの詳細と属性が含まれます。また、すべてのユーザ タイプについて PAM があれば PAM も含まれます。
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含まれます。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。

表 C-3. リアルタイム同期が必要なテーブル

テーブル	説明
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。
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）。
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。これはリスト検索ルール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。このデータは派生するリスト検索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。
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。
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。
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 RiskFort 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。
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。

表 C-3. リアルタイム同期が必要なテーブル

テーブル	説明
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。
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。
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。
ARRFNEGATIVECOUNTRYLIST	すべての拒否国のリストが格納されます。
ARRFSYSPARAMSCONFIG	Administration Console を使って設定できるすべての RiskFort システム パラメータに関する詳細情報が含まれます。
ARUDSAUDITLOG	ユーザ データ ソース（UDS）の操作とそのリターン ステータスの監査ログ情報が含まれます。
ARRFSYSAUDITLOG	リスク評価およびログに記録される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。
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。
ARRFUNTRUSTEDIPLIST	すべての拒否 IP アドレスの詳細が格納されます。

表 C-3. リアルタイム同期が必要なテーブル

テーブル	説明
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。
ARSEQUENCETABLE	シーケンス値を追跡するための情報が含まれます。

定期的な同期が必要なテーブル

表 C-4 に、プライマリ データベースとバックアップ データベースの間での定期的な同期を必要とするデータベース テーブルを示します。このようなデータベース テーブルは、設定に変更が行われたときに同期されます。

表 C-4. 定期的な同期が必要なテーブル

テーブル	説明
ARADMINCONFIG	Administration Console の設定が含まれます。
ARADMINCUSTOMROLE	カスタム定義ロールの設定が含まれます。
ARADMINMAP	キーと値のペアとして入力される、RiskFort サーバ インスタンスの情報が含まれます。
ARADMINPAFCONFIG	組織の管理者認証設定が含まれます。
ARADMINPWDPOLICY	すべての組織の管理者パスワード ポリシーが含まれます。
ARADMINTURNEDOFFPRIVILEGE	カスタム ロールで使用できない権限に関する情報が含まれます。
ARADMINCACHEREFRESH	Administration Console でキャッシュをリフレッシュする必要があるかどうかを決めるキャッシュ リフレッシュ情報が含まれます。
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。
ARUDSCONFIG	UDS 設定パラメータとその値が含まれます。

表 C-4. 定期的な同期が必要なテーブル

ARUDSREPOSITORYTYPES	UDS によってサポートされるリポジトリの定義が含まれます。このテーブルは、新しいプラグインがシステムに追加されたときだけ変更されることが想定されています。
ARUDSUSERATTRIBUTE	ユーザ属性定義が含まれます。このテーブルは、個々の製品によって新規ユーザ属性が追加される場合を除き、ほとんど変更されないことが想定されています。
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、RiskFort 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、RiskFort 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、RiskFort 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、RiskFort 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。
ARRFADDONRULETYPE	システム内の各組織に対して実装されたアドオン ルールの詳細な設定情報が格納されます。

表 C-4. 定期的な同期が必要なテーブル

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。
ARRFCASEQUEUES	各ケース キューの定義が格納されます。
ARRFCONFIG	RiskFort のグローバル設定情報が格納されます。
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-RiskFort 統合展開でのみ適用されます。
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。
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。
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。
ARRFLIBRARYTOTYPEMAPPING	サポートされているすべてのアドオン 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。 このテーブルは将来使用されます。
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。 注：現在、組織あたり 1 つのデフォルト キュー*だけ*がサポートされています。
ARRFPROTOCOLREGISTRY	RiskFort 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。
ARRFSERVERS	使用可能な RiskFort サーバ インスタンスのマッピングが格納されます。

表 C-4. 定期的な同期が必要なテーブル

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-RiskFort 統合展開でのみ適用されます。
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。

同期が必要ないテーブル

表 C-5 に、プライマリ データベースとバックアップ データベースの間でのいかなる同期も必要としないデータベース テーブルを示します。

表 C-5. 同期が必要ないテーブル

テーブル	説明
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 状態値が含まれます。バックアップが設定されている場合、データベースをフェイルオーバーするべきかどうかを判断するために、この情報が使用されます。
ARADMINMANAGEROLE	ロールが管理できるロールのリストが含まれます。
ARADMINPREDEFINEDROLE	サポートされているすべての管理者のロール情報が含まれます。
ARADMINSUPPORTEDAUTHMECH	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含まれます。
ARADMINUITAB	Administration Console のタブに関する情報が含まれます。
ARADMINUITASK	Administration Console を使って実行されるタスクに関する情報が含まれます。
ARADMINUITASKATTRIBUTES	Administration Console の第 1 レベル タブと第 2 レベル タブをクリックしたときに表示されるタスクの詳細が含まれます。このようなタスクは待ち受けページと呼ばれます。
ARADMINUITASKCONTAINER	タスク コンテナに関連する情報が含まれます。タスク コンテナは、Administration Console 内の第 2 レベル タブ ID またはタスク グループのいずれかです。
ARADMINWIZARDTASK	Administration Console ブートストラップ ウィザードを使って実行されるタスクに関する情報が含まれます。

表 C-5. 同期が必要ないテーブル

テーブル	説明
ARREPORTTABLES	他のテーブルのメタデータが含まれます。
ARADMINMAPDATATYPE	ARADMINMAP でサポートされているデータ型のリストが含まれます。
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。
ARRFADDONEXPOSEDPARAMS	展開したアドオン 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アドオン 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 Arcot サポート（*support@arcot.com*）にお問い合わせいただくことをお勧めします。
ARRFCASECONFIG	Case Management モジュールの設定データが格納されます。
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。
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。
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 Arcot サポート（*support@arcot.com*）にお問い合わせいただくことをお勧めします。
ARRFDISPLAYNAMES	Administration Console 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。
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。

データベース テーブルのアーカイブに関する推奨事項

このセクションで説明するテーブルは、トランザクションごとに絶えず拡大しますが、リスク スコアリングには必要ありません。したがって、このようなテーブルは削除できます。削除できるテーブルを以下に示します。

- **ARRFSYSAUDITLOG**

  監査ログ情報が格納されます。RiskFort によるすべてのトランザクションのエントリがこのテーブルに含まれます。このテーブルからエントリを削除すると、使用できるレポート データの量は少なくなります。

- **ARADMINAUDITTRIAL**

  管理者によって実行されたすべてのアクションの履歴が含まれます。

ARUDSUSER

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強くお勧めします。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。

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。

注： このような最適化にご興味がある場合は、Arcot のプロフェッショナル サービス チームにご相談いただくことをお勧めします。

ユーザに関する ARUDSUSER テーブル内のエントリは、登録済みユーザを表します。ユーザの基本情報はこのテーブルに格納されます。ユーザ レコードは RiskFort 発行 API を通してこのテーブルに入力されます。

データベース接続調整パラメータ

RiskFort 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、arcotcommon.ini ファイルで設定します。

付録 D
デフォルト ポート番号および URL

この付録では、RiskFort 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。以下のセクションがあります。

- デフォルト ポート番号
- RiskFort コンポーネントの URL

デフォルト 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 RiskFort 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 Arcot 製品または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、Administration Console の［RiskFort Protocol Setup］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。

表 D-1 に、RiskFort によって使用されるデフォルト ポート番号を示します。

表 D-1. RiskFort のプロトコルとポート番号

プロトコル	デフォルト ポート番号	説明
RiskFort Native（TCP）	7680	Arcot 独自仕様のプロトコルで、RiskFort サーバ インスタンスと RiskFort Java SDK（リスク管理と発行を含む）の間の通信を可能にします。
Native（SSL）	7681	Arcot 独自仕様のプロトコルで、RiskFort サーバ インスタンスと RiskFort Java SDK（リスク管理と発行を含む）の間の SSL ベースの通信を可能にします。

表 D-1. RiskFort のプロトコルとポート番号

プロトコル	デフォルト ポート番号	説明
管理 Web サービス	7777	これは、RiskFort サーバと管理 Web サービスの間の通信用プロトコルです。 RiskFort 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 RiskFort 発行またはリスク管理コールは*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、RiskFort 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 Web サービスによって使用されます。 **注：** これらのコールに Administration Service コールは*含まれません*。
キュー サーバ	7779	このプロトコルは、指定のポートで Case Management 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。
キュー管理	7780	これは RiskFort サーバと Queuing Management の間の通信用プロトコルです。 RiskFort サーバは、このポートで Case Management Web Service コールを待ち受けます。
サーバ管理	7980	`arrfadmin` ツールは、サーバ管理アクティビティ（正常終了とサーバ キャッシュ リフレッシュ）で、このプロトコルを使用して RiskFort サーバ インスタンスと通信します。 **関連文書：** この Administration Console ツールの詳細については、「Arcot RiskFort 2.2.6 管理ガイド」を参照してください。

RiskFort コンポーネントの URL

製品のインストール後に RiskFort コンポーネントにアクセスするには、表 D-2 に示された 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。

表 D-2. デフォルト ポート番号

コンポーネントまたはサービス	URL
Administration Console（Master Administrator （MA）用）	*http://< ホスト名 >:< ポート >/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。
Administration Console（その他の管理者用）	*http://< ホスト名 >:< ポート >/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://< ホスト名 >:< ポート >/riskfort-2.2.6-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。
発行 Web サービス	*http://< ホスト名 >:< ポート >/services/RiskFortIssuanceSvc* **注：** ここで指定するデフォルト ポートは 7778 です。
リスク評価 Web サービス	*http://< ホスト名 >:< ポート >/services/RiskFortEvaluateRiskSvc* **注：** ここで指定するデフォルト ポートは 7778 です。

付録 E
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

この付録では、RiskFort コンポーネントを展開するアプリケーション サーバに、データベース接続プールをセットアップする手順について説明します。以下のアプリケーション サーバの設定手順について説明します。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

このセクションでは、Apache Tomcat で JNDI ベースのデータベース操作を行うための手順を説明します。Apache Tomcat で JNDI 接続を作成には、以下の手順に従います。

1. Apache Tomcat アプリケーション サーバをインストールし、以下の URL を使用してインストールをテストします。

   http://localhost:8080/

2. `<TOMCAT_HOME>/conf/` ディレクトリにある `server.xml` ファイルを開きます。
3. データ ソースを定義するために必要な以下の情報を収集します。

   - **JNDI 名**

     Arcot コンポーネントによって使用される JNDI 名。

     重要 : この名前は、arcotcommon.ini の AppServerConnection PoolName.<N> (`java:comp/env/` *を付けない*) と一致する*必要があります。*

   - **ユーザ ID**

     データベースのユーザ ID。

- **パスワード**

  データベースのパスワード。

- **JDBC ドライバ クラス**

  JDBC ドライバ クラス名。以下に例を示します。

  `oracle.jdbc.driver.OracleDriver`

- **JDBC URL**

  データベース サーバの JDBC URL。たとえば Oracle のドライバを使用している場合、URL は以下のようになります。

  `jdbc:oracle:thin:<server>:<port>:<sid>`

4. 次のエントリを追加して、`<GlobalNamingResources>` タグ内にデータ ソースを定義します。

```
<Resource name="SampleDS"
        auth="Container"
        type="javax.sql.DataSource"
factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"
        username="<userid>"
        password="<password>"
        driverClassName="<JDBC driver class>"
        url="<jdbc-url>"
        maxWait="30000"
        maxActive="32"
        maxIdle="8"
        initialSize="4"
        timeBetweenEvictionRunsMillis="300000"
        minEvictableIdleTimeMillis="30000"/>
```

5. *<TOMCAT_HOME>*/**conf**/ ディレクトリにある `context.xml` ファイルを開きます。

6. 次のエントリを追加して、<Context> タグ内にデータソースを定義します。

```
<ResourceLink global="SampleDS" name="SampleDS"
type="javax.sql.DataSource"/>
```

7. *<TOMCAT_HOME>*/common/**lib**/ ディレクトリに、以下のデータベース接続プール（DBCP）依存性をコピーします。
   - commons-dbcp-1.2.2.jar
   - ojdbc14-10.2.0.1.0.jar（Oracle データベースの場合）

IBM WebSphere

このセクションでは、IBM WebSphere で JNDI ベースのデータベース操作を行うための手順を説明します。RiskFort の Java 依存コンポーネントを展開するために IBM WebSphere インスタンスを設定するには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［**Resources**］を選択し、［**JDBC**］ノードを展開します。
3. ［**JDBC Providers**］を選択して［**New**］をクリックし、使用しているデータベースに基づいて適切な JDBC プロバイダを作成します。

注： 詳細については、以下を参照してください。
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html

4. 画面上の手順に従って、データベースの CLASSPATH 情報を入力します。
5. ［**Next**］をクリックし、サマリ ページを確認します。［**Finish**］をクリックして、JDBC プロバイダの設定を完了します。
6. ［**Save**］をクリックして変更内容を保存します。
7. ［**Resources**］に移動し、［**JDBC**］をクリックします。
8. ［**JDBC**］の下の［**Data Sources**］を開き、［**New**］をクリックして新しいデータ ソースを作成します。
   a. ［**Data Source Name**］を指定します。

b. ［**JNDI Name**］を指定します。

注： この名前は `arcotcommon.ini` の AppServerConnectionPoolName.<N> の値と一致する*必要があります*。

c. ［**Next**］をクリックし、手順 3 で作成した **JDBC プロバイダ**を選択します。

d. ［**Next**］をクリックし、［**JDBC URL**］を指定します。

e. データ ソースを選択し、［**Next**］をクリックしてから［**Finish**］をクリックします。

f. ［**Next**］をクリックしてサマリ ページを表示し、［**Finish**］をクリックします。

9. ［**Save**］をクリックして変更内容を保存します。
10. 前の手順で作成したデータ ソースを選択し、［**Related Items**］セクションをクリックします。
11. ［**New**］を選択して新しいクレデンシャルを作成します。
12. データベースの接続に使用するログイン クレデンシャルを入力し、クレデンシャルを保存します。
13. ［**Apply**］をクリックしてから［**Save**］をクリックし、変更内容を保存します。
14. ［**Data Sources**］を選択し、手順 7 で作成したデータ ソースを選択します。
15. ［**Component-managed authentication alias**］の下で、手順 12 で作成した JAAS クレデンシャルを選択し、［**Save**］をクリックします。
16. ［**Data Sources**］を選択し、手順 7 で作成したデータ ソースのチェック ボックスをオンにします。
17. ［**Test Connection**］をクリックして、接続が正しく指定されたことを確認します。

注： このテストは、データベース サーバへの接続のみをチェックします。データ ソースの定義が正しいかどうかは*確認されません*。

BEA WebLogic

このセクションでは、BEA WebLogic で JNDI ベースのデータベース操作を行うための手順を説明します。BEA WebLogic で RiskFort のデータ ソースを作成するには、以下の手順に従います。

1. WebLogic Administration Console にログインします。
2. まだ［Change Center］の［**Lock & Edit**］ボタンをクリックしていない場合は、このボタンをクリックします。
3. ［**Services**］-［**JDBC**］-［**Data Sources**］の順に移動します。
4. ［**JDBC**］の下の［**Data Sources**］を開き、［**New**］をクリックして JDBC データ ソースの新規作成ページを開きます。
5. 以下の JNDI およびデータベースの情報を設定します。
   a. ［**Name**］= `ArcotDB` に設定
   b. ［**JNDI Name**］= `ArcotDB` に設定
   c. 必要な［**Database Type**］を選択（Oracle など）。
   d. 必要な［**Database Driver**］を選択（Oracle Thin Driver など）。
6. ［**Next**］をクリックし、デフォルト値を保持したまま、再度［**Next**］をクリックします。
7. 表示される接続プロパティ ページで、データベース接続の詳細を設定します。たとえば、［**Oracle**］には次の値を使用できます。
   - ［**Database Name**］= データベース サーバの SID またはサービス名
   - ［**Host Name**］= データベースのホスト名または IP アドレス
   - ［**Port**］= 1521、またはデータベース サーバを実行している任意の他のポート
   - ［**Database User Name**］= データベース接続を作成できるデータベース アカウント ユーザ名
   - ［**Password**］/［**Confirm Password**］= 指定されたデータベース ユーザ名のパスワード
8. ［**Test Configuration**］をクリックして、指定したデータベース情報を確認します。
9. ［**Next**］をクリックし、WebLogic サーバ インスタンス用の優先データ ソースのターゲット サーバを設定します。

10.［**Finish**］をクリックしてデータ ソース リストのページに戻ります。

11.［Change Center］の［**Activate**］ボタンをクリックして、前の手順で設定したデータ ソースの設定を有効にします。

付録 F
SSL の設定

RiskFort コンポーネントはデフォルトで、TCP（Transmission Control Protocol）を使って相互に通信します。ただし、TCP はスプーフィング攻撃と man-in-the-middle 攻撃に対して脆弱です。Administration Console と RiskFort サーバ間および SDK と RiskFort 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 RiskFort Native 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より安全に通信することを可能にし、TCP 攻撃の可能性を低減します。

RiskFort 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： SSL を正常に設定するには、以下の順番に従う*必要があります*。すべての手順を完了したら、接続が正常に設定されているかどうかをテストします。

1. UDS で SSL を有効にする
2. Administration Console とユーザ データ サービスの間で SSL を有効にする
3. RiskFort 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. Administration Console と RiskFort サーバの間で SSL を有効にする
5. Java SDK と RiskFort サーバの間で SSL を有効にする
6. arrfadmin ツールと RiskFort サーバの間で SSL を有効にする

UDS で SSL を有効にする

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 サーバで SSL を有効にする必要があります。

注： 詳細については、使用しているアプリケーション サーバのベンダー各社のドキュメントを参照してください。

Administration Console とユーザ データ サービスの間で SSL を有効にする

Administration Console と UDS が別々のアプリケーション サーバ上に展開されている場合は、各アプリケーション サーバで SSL を有効にする必要があります。

注： SSL を設定する方法の詳細については、使用しているアプリケーション サーバのベンダー各社のドキュメントを参照してください。

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

RiskFort 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、SSL に必要な証明書をアップロードする必要があります。この作業は、システムのブートストラップ中か、後で Administration Console から、［**User Data Service Configuration**］ページを使って行います。

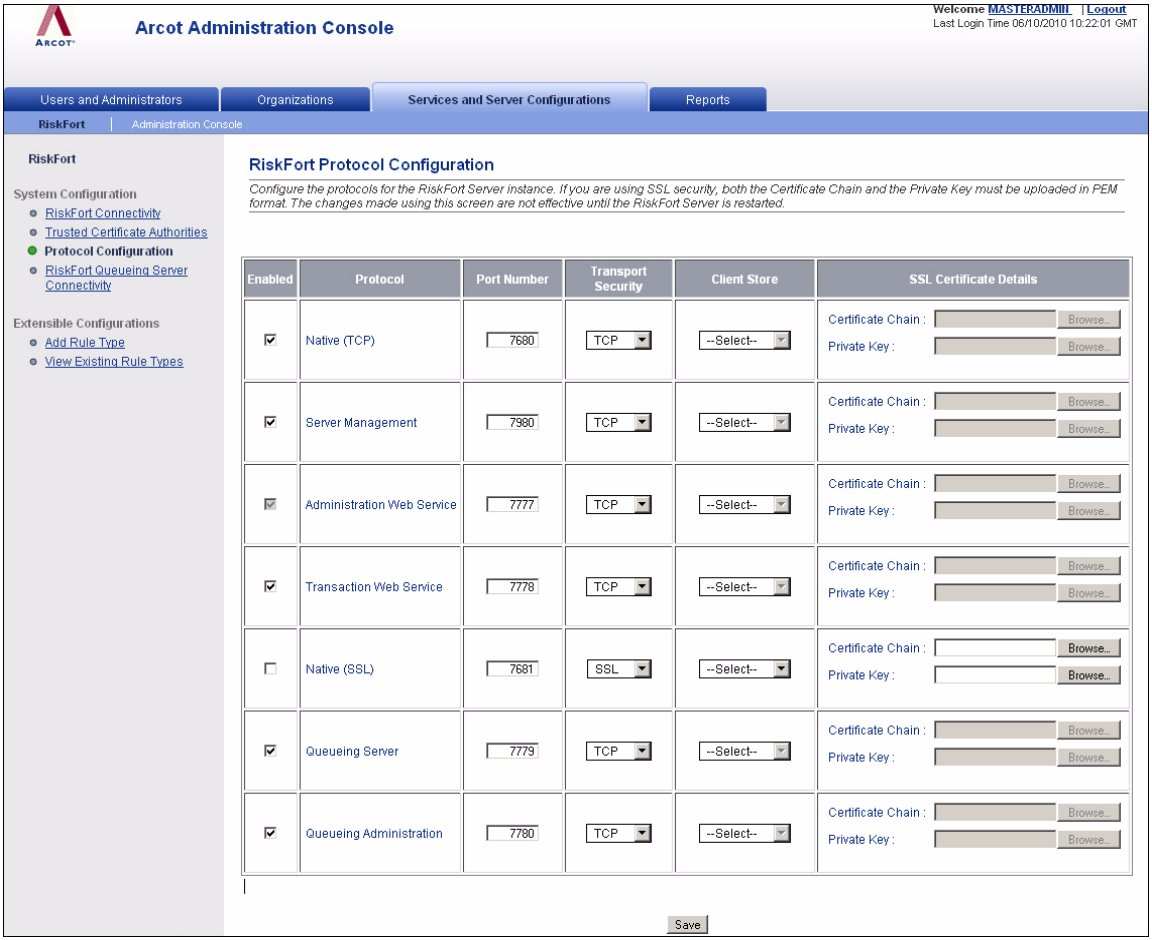
詳細については、「システムのブートストラップ」を参照してください。

Administration Console と RiskFort サーバの間で SSL を有効にする

RiskFort サーバと Administration Console の間で SSL ベースの通信を設定する方法

1. Web ブラウザで Administration Console を開きます。
2. Master Administrator （MA）クレデンシャルを使って Administration Console にログインします。
3. ［**Services and Server Configurations**］タブをアクティブにします。
4. タブのサブメニューで［**RiskFort**］オプションが選択されていることを確認します。
5. ［**System Configurations**］セクションで、［**Protocol Configuration**］リンクをクリックして［RiskFort Protocol Configuration］ページ（図 F-1）を表示します。

図 F-1［RiskFort Protocol Configuration］ページ



6. ［**Administration Web Service**］プロトコルを以下のように設定します。
   a. ［**Enabled**］列で、［**Administration Web Service**］に対応するボックスがオンになっていることを確認します。
   b. ［**Port Number**］列で、対応するフィールドに必要なポート番号を入力します。
   c. ［**Transport Security**］列で、ドロップダウン リストから［**SSL**］を選択します。
   d. ［**Client Store**］列で、信頼できる認証機関（CA）のルート証明書を含む、必要なトラスト ストアをドロップダウン リストから選択します。
   e. ［**SSL Certificate Details**］列で、以下の操作を行います。
      i. ［**Certificate Chain**］の［**Browse**］をクリックして適切な場所に移動し、サーバの CA 証明書チェーンをアップロードします。

重要 : 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をたどっている必要があります。

      ii. ［**Private Key**］の［**Browse**］をクリックして適切な場所に移動し、証明書チェーンの対応する秘密キーをアップロードします。

注 : 証明書チェーンと秘密キーはどちらも .PEM 形式である*必要があります*。また、関連する秘密キーの暗号化が解除されている必要があります。秘密キーが .PEM 形式で、かつ暗号化されている場合、Administration Console にはエラー メッセージが表示されます。

   f. ［**Save**］をクリックして変更内容を保存します。
7. 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［**RiskFort Connectivity**］をクリックすると表示されます。

8. ［RiskFort Connectivity］ページのフィールドを編集するには、表 F-1 の情報を使用します。

表 F-1. RiskFort の接続パラメータ

フィールド	説明
［Server］	必要な RiskFort サーバ インスタンスをインストールしたシステムの IP アドレスを入力します。 **注**：RiskFort サーバがインストールされているシステムに、その `hostname` 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。
［Port］	管理 Web サービスが公開されているポートを入力します。
［Transport］	Administration Console から指定の RiskFort サーバ インスタンスに接続するためのトランスポート モードに［**SSL**］を指定します。
［Server CA Root Certificate］	サーバ証明書が含まれる PKCS#12 ストア パスを参照し、証明書を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。
［Client Certificate-Key Pair in PKCS#12］	クライアント証明書と秘密キーが含まれる PKCS#12 ストア パスを参照し、証明書とキーをアップロードします。 **注**：このクライアント証明書は PEM 形式である必要があります。
［Client PKCS#12 Password］	クライアントの PKCS#12 ストアのパスワードを入力します。

9. ［**Save**］をクリックして、設定した構成を保存します。

注： 新しい RiskFort サーバ インスタンスを追加する場合は、インスタンス固有の設定に入る前に、このページの［**Save**］をクリックする必要があります。［Save］をクリックすることで、Administration Console からすべてのインスタンスの詳細を取得できると共に、インスタンス管理機能がすべてのインスタンスで円滑に動作することが保証されます。

10. RiskFort サーバを再起動します。
11. Administration Console を再起動します。

Java SDK と RiskFort サーバの間で SSL を有効にする

RiskFort サーバと Java SDK の間で SSL 通信を有効にするには、まず Administration Console で RiskFort ネイティブ プロトコルを有効にし、適切なプロパティ ファイルを設定する必要があります。

- *<インストール場所>*/arcot/sdk/java/properties/**riskfort.risk-evaluation.properties**
- *<インストール場所>*/arcot/sdk/java/properties/**riskfort.issuance.properties**

RiskFort サーバと Java SDK の間で SSL 通信モードを有効にする方法

1. MA としてログインしていることを確認します。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブ メニューの［**RiskFort**］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**］セクションで、［**Protocol Configuration**］リンクをクリックして［Protocol Configuration］ページ（図 F-1）を表示します。
5. ［**Native (SSL)**］プロトコルを以下のように設定します。
   a. ［**Enabled**］列で、［**RiskFort Native**］に対応するボックスがオンになっていることを確認します。
   b. ［**Port Number**］列で、対応するフィールドに必要なポート番号を入力します。
   c. ［**Transport Security**］列で、ドロップダウン リストから［**SSL**］を選択します。
   d. ［**Client Store**］列で、信頼できる認証機関（CA）のルート証明書を含む、必要なトラスト ストアをドロップダウン リストから選択します。
   e. ［**SSL Certificate Details**］列で、以下の操作を行います。
      i. ［**Certificate Chain**］の［**Browse**］をクリックして適切な場所に移動し、サーバの CA 証明書チェーンをアップロードします。

重要 : 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をたどっている必要があります。

      ii. ［**Private Key**］の［**Browse**］をクリックして適切な場所に移動し、証明書チェーンの対応する秘密キーをアップロードします。

注 : 証明書チェーンと秘密キーはどちらも .PEM 形式である*必要があります*。また、関連する秘密キーの暗号化が解除されている必要があります。秘密キーが .PEM 形式で、かつ暗号化されている場合、Administration Console にはエラー メッセージが表示されます。

f. ［**Save**］をクリックして変更内容を保存します。

6. RiskFort Java SDK が展開されているシステム上の以下の場所に移動します。

   < インストール場所 >/arcot/**sdk**/**java**/**properties**/

7. エディタ ウィンドウで riskfort.risk-evaluation.properties ファイルを開きます。

   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=<*PEM 形式のルート証明書の絶対パス*>

      たとえば、次のように指定できます：CA_CERT_FILE=< *インストール場所* >/certs/<*CA 証明書*>.pem。

      設定パラメータの詳細については、riskfort.risk-evaluation.properties を参照してください。

   b. 変更を保存して、ファイルを閉じます。

8. エディタ ウィンドウで riskfort.issuance.properties ファイルを開きます。

   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=<*PEM 形式のルート証明書の絶対パス*>

      たとえば、次のように指定できます：CA_CERT_FILE=< *インストール場所* >/certs/<*CA 証明書*>.pem。

      設定パラメータの詳細については、riskfort.issuance.properties を参照してください。

   b. 変更を保存して、ファイルを閉じます。

9. RiskFort サーバを再起動します。

10. RiskFort 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。

arrfadmin ツールと RiskFort サーバの間で SSL を有効にする

arrfadmin ツールと RiskFort サーバの間で SSL 通信を有効にするには、まず RiskFort サーバでサーバ管理プロトコルを有効にし、適切な INI ファイルを設定する必要があります。

- *<インストール場所>*/arcot/sdk/java/properties/

	**注：** arrfadmin ツールの詳細については、「Arcot RiskFort 管理ガイド」を参照してください。

riskfortadminclient.ini

RiskFort サーバと Java SDK の間で SSL 通信モードを有効にする方法

1. MA としてログインしていることを確認します。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブ メニューの［**RiskFort**］タブがアクティブであることを確認します。
4. ［**System Configurations**］セクションで、［**Protocol Configuration**］リンクをクリックして［Protocol Configuration］ページ（図 F-1）を表示します。
5. ［**Server Management**］プロトコルを以下のように設定します。
   a. ［**Enabled**］列で、［**Server Management**］に対応するボックスがオンになっていることを確認します。
   b. ［**Port Number**］列で、対応するフィールドに必要なポート番号を入力します。
   c. ［**Transport Security**］列で、ドロップダウン リストから［**SSL**］を選択します。
   d. ［**Client Store**］列で、信頼できる認証機関（CA）のルート証明書を含む、必要なトラスト ストアをドロップダウン リストから選択します。
   e. ［**SSL Certificate Details**］列で、以下の操作を行います。

i.［**Certificate Chain**］の［**Browse**］をクリックして適切な場所に移動し、サーバの CA 証明書チェーンをアップロードします。

	**重要 :** 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をたどっている必要があります。

ii.［**Private Key**］の［**Browse**］をクリックして適切な場所に移動し、証明書チェーンの対応する秘密キーをアップロードします。

	**注 :** 証明書チェーンと秘密キーはどちらも .PEM 形式である*必要があります*。また、関連する秘密キーの暗号化が解除されている必要があります。秘密キーが .PEM 形式で、かつ暗号化されている場合、Administration Console にはエラー メッセージが表示されます。

f. ［**Save**］をクリックして変更内容を保存します。

6. 以下の場所に移動します。

   < *インストール場所* >/arcot/**conf**/

7. （**双方向 SSL 通信が必要な場合**）エディタ ウィンドウで riskfortadminclient.ini ファイルを開きます。

   a. 以下のパラメータを設定します。

   - Host（デフォルトで、このパラメータは localhost に設定されます）。
   - Port（デフォルトで、このパラメータは 7980 に設定されます）。
   - Transport=SSL （デフォルトで、このパラメータは TCP に設定されます）。
   - SSLClientKey=<*PEM 形式のクライアント SSL キーの絶対パス* >
   - SSLClientCertChain=<*PEM 形式のクライアント SSL 証明書または証明書チェーンの絶対パス* >
   - SSLServerCACert=<*PEM 形式のサーバ ルート SSL 証明書の絶対パス* >

   たとえば、次のように指定できます :

   SSLServerCACert=< *インストール場所* >/certs/<*CA 証明書* >.pem。

   設定パラメータの詳細については、riskfortadminclient.ini を参照してください。

   b. 変更を保存して、ファイルを閉じます。

8. RiskFort サーバを再起動します。
9. アプリケーション サーバを再起動します。

付録 G
サードパーティ ソフトウェア ライセンス

この付録では、RiskFort によって使用されるサードパーティのソフトウェア パッケージを示します。以下のようなパッケージがあります。

アスペクト指向プログラミング（AOP）アライアンス

- `aopalliance-1.0.jar`

パブリック ドメインの下にライセンスされています（AOP アライアンス用）。（*http://aopalliance.sourceforge.net/*）

ANTLR 2

- `antlr-2.7.6.jar`
- `antlr-2.7.7.jar`

Copyright © 2003-2006, Terence Parr.（*http://www.antlr.org/license.html*）

パブリック ドメインの下にライセンスされています。（*https://olex.openlogic.com/licenses/4*）

Apache

Copyright © The Apache Software Foundation.**Apache License Version 1.1** の下にライセンスされています。（*http://www.apache.org/licenses/LICENSE-1.1.html*）

- `jakarta-oro-2.0.7.jar`

Copyright © The Apache Software Foundation.**Apache License Version 2.0** の下にライセンスされています。（*http://www.apache.org/licenses/*）

- `ant-1.7.0.jar`
- `axiom-impl-1.2.7.jar`
- `Axis2-1.4.jar`
- `cglib-2.1_3.jar`
- `commons-beanutils-1.7.0.jar`
- `commons-codec-1.3.jar`
- `commons-collections-3.1.jar`

- commons-dbcp-1.2.2.jar
- commons-digester-1.7.jar
- commons-fileupload-1.1.1.jar
- commons-fileupload-1.2.jar
- commons-httpclient-3.1.jar
- commons-io-1.2.jar
- commons-io-1.4.jar
- commons-lang-2.4.jar
- commons-logging-1.1.jar
- commons-logging-1.1.1.jar
- commons-pool-1.3.jar
- commons-pool-1.4.jar
- commons-validator-1.3.1.jar
- geronimo-activation-1.1.jar
- geronimo-annotation-1.0.jar
- geronimo-javamail-1.4.jar
- geronimo-jms.1.1.jar
- geronimo-stax-api-1.0.jar
- httpcore-4.0.jar
- iBATIS-2.3.4.726.jar
- jdom-1.0.jar
- jdom-1.1.jar
- jettison-1.0.1.jar
- jstl-api-1.1.2.jar
- jstl-standard-1.1.2.jar
- log4j.1.2.9.jar
- neethi-2.0.jar
- neethi-2.0.4.jar
- standard-1.1.2.jar
- stax-api-1.0.1.jar
- struts-1.2.8.jar

- velocity-1.5.jar
- woden-1.0.0.jar
- xbean-2.2.0.jar
- xbean-2.3.0.jar
- xercesImpl-2.8.1.jar
- xml.resolver-1.2.0.jar
- xml-commons-1.3.04.jar
- xml-xalan-2.7.0.jar
- xmlParserAPIs-2.6.0.jar
- XmlSchema-1.2.jar
- XmlSchema-1.4.2.jar

ASM

- asm-1.5.3.jar

Backport-Util-Concurrent

- backport-util-concurrent-2.2.jar

Bouncy Castle

- bcprov-jdk14-139.jar
- bcprov-jdk14-131.jar

Codehaus Annogen

- annogen-0.1.0.jar

Apache License Version 2.0 の下にライセンスされています。
（*http://www.apache.org/licenses/*）

- Java XPath Engine

  Copyright © 2003-2006 The Werken Company.All Rights Reserved.
  （*http://jaxen.org/license.html*）

  - `jaxen-1.1.jar`
  - `jaxen-1.1.1.jar`

Cryptix

Copyright © 1995-2005 The Cryptix Foundation Limited.All rights reserved.
（*http://www.cryptix.org/LICENSE.TXT*）

DOM4j

- `dom4j-1.6.1.jar`

Copyright 2001-2005 © MetaStuff, Ltd. All Rights Reserved.
（*http://www.dom4j.org/license.html*）

Apache Software License 1.1 BSD スタイル ライセンスの下にライセンスされています。
（*http://dom4j.sourceforge.net/dom4j-1.6.1/license.html*）

gSOAP 2.7.10

Copyright © 2000-2006 Robert A.van Engelen, Genivia, Inc. All Rights Reserved.

gSOAP Public License version 1.3b.（*http://www.cs.fsu.edu/~engelen/license.html*）

Hibernate Core 3.1

Copyright © 2006, Red Hat Middleware, LLC.All rights reserved.JBoss および Hibernate は、Red Hat, Inc. の登録商標およびサービスマークです。（*https://www.hibernate.org/*）

ICU License - ICU 1.8.1 以上

- `icu4j-2.6.1.jar`

Copyright © 1995-2010 International Business Machines Corporation and others
（*http://source.icu-project.org/repos/icu/icu/trunk/license.html*）

JavaScript Object Notation Lib（JSON-Lib）

- `json-lib-0.7.1.jar`

Copyright © 2002 JSON.org.（*http://www.json.org/license.html*）

Apache Software License 2.0 の下にライセンスされています。
（*http://www.apache.org/licenses/LICENSE-2.0.html*）

JiBX: Binding XML to Java Code

- `jibx-bind-1.1.5.jar`

© 2003-2010, Dennis M.Sosnoski（Sosnoski Software Associates Ltd）. 無料配布および使用を目的として JiBX Project にライセンスされています。
（*http://jibx.sourceforge.net/jibx-license.html*）

Open Source Initiative（OSI）

Common Development And Distribution License（CDDL）Version 1.0.
（*http://www.opensource.org/licenses/cddl1.txt*）

Java Architecture for XML Binding

- `jaxb-api-2.1.6.jar`

Java Mail

- `mail-1.4.jar`

JSTL

- `jstl 1.0.3.jar`

WSDL4J

Common Public License（CPL）Version 1.0.（*http://www.opensource.org/licenses/cpl1.0.php*）

- `wsdl4j-1.6.2.jar`

jQuery

Copyright © 2010 John Resig, http://jquery.com/.
（*http://github.com/jquery/jquery/blob/master/MIT-LICENSE.txt*）

- `jquery-1.4.2.js`

OpenSSL

Copyright © 1998-2007 The OpenSSL Project.All rights reserved.
（*http://www.openssl.org/source/license.html*）

Object-Graph Navigation Language（OGNL）

- `ognl-2.6.9.jar`

Copyright (c) 2001-2004 The OpenSymphony Group.All rights reserved.
（*http://www.opensymphony.com/ognl/license.action*）

OpenSSL

Copyright © 1998-2007 The OpenSSL Project.All rights reserved.
（*http://www.openssl.org/source/license.html*）

Oracle Database 10*g* JDBC Driver

Copyright © 1995-2007, Oracle.All rights reserved.（*http://www.oracle.com/*）

Spring Framework

Copyright © 2006-2008, SpringSource, All Rights Reserved.Spring Framework は Apache License Version 2.0 の条件の下にライセンスされています。
（*http://www.springsource.org/about*）

- `spring-2.5.2.jar`
- `spring-aop-2.5.2.jar`
- `spring-beans-2.5.2.jar`
- `spring-binding-1.0.5.jar`
- `spring-context-2.5.2.jar`
- `spring-context-support-2.5.2.jar`
- `spring-core-2.5.2.jar`
- `spring-dao-2.0.8.jar`
- `spring-ibatis-2.0.8.jar`
- `spring-jdbc-2.5.2.jar`
- `spring-jms-2.5.2.jar`
- `spring-orm-2.5.2.jar`
- `spring-test-2.5.2.jar`
- `spring-tx-2.5.2.jar`
- `spring-web-2.5.2.jar`
- `spring-webflow-1.0.5.jar`
- `spring-webmvc-2.5.2.jar`
- `spring-webmvc-portlet-2.5.2.jar`
- `spring-webmvc-struts-2.5.2.jar`
- `springmodules-validation-0.4.jar`

Sun Microsystems

- JavaBeans Activation Framework（JAF）
  - `activation-1.1.jar`
- Java Architecture for XML Binding（JAXB）
  - `jaxb-impl-2.1.6.jar`
- LDAP JNDI
  - `ldap-1.2.4.jar`
- JDBC
  - `jdbc-1.2.2828.jar`
- Java Servlet
  - `servlet-api-2.3.jar`
- JavaServer Pages Standard Tag Library（JSTL）
  - `jstl-1.0.3.jar`

Streaming API for XML（StAX）

- `stax-api-1.0.1.jar`

Woodstox XML Processor

- `woodstox-core-asl-3.2.0.jar`
- `woodstox-core-asl-3.2.4.jar`

XOM

- `xom-1.0.jar`

その他の商標

- Java™ および Java ベースの商標はすべて、米国およびその他の国における Oracle® の商標です。その他の会社名、製品名、およびサービス名は、各社の商標またはサービスマークである場合があります。
- WebSphere は、米国およびその他の国における IBM の商標です。
- BEA WebLogic Server® および Solaris SPARC は、米国およびその他の国における Oracle® の商標です。BEA WebLogic Server® は、米国およびその他の国における Oracle® の商標です。

付録 H
用語集

CSR（Customer Support Representatives、テクニカル サポート担当者）	セキュリティ システムのユーザに関連する日常業務を担当する管理者。 たとえば、管理者は、ユーザの登録支援、パスワードのリセット、登録レポートの生成を行うことができます。
Global Administrator	CSR（Customer Support Representatives、テクニカル サポート担当者）アカウントのセットアップおよびシステムの設定を担当する管理者。
Master Administrator	RiskFort 管理者の最高レベル。主な担当業務は、RiskFort を初期化し、Global Administrator アカウントを作成することです。
PKI（Public Key Infrastructure）	ネットワーク環境における公開キー暗号化法および証明書の使用を促進する標準およびサービス。
RiskFort	RiskFort には、指定されたトランザクションのリスクを評価するメカニズムが用意されています。
RiskFort ネイティブ プロトコル	RiskFort サーバ、そのコンポーネント、および Administration Console の間の通信用の Arcot 専用プロトコル。
SSL（Secure Sockets Layer）	公衆ネットワーク上でのメッセージ伝送のセキュリティを管理するためのプロトコル。
TCP（Transmission Control Protocol）	保証されたデータ伝送を行うためのインターネット プロトコル。暗号化されていないデータを送信します。
アグリゲータ	複数の企業にまたがってユーザ情報を照合することによって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。
アドオン ルール	RiskFort に付属する追加のリスク評価ルール。
クレデンシャル	ユーザ ID を証明するもの。デジタル クレデンシャルは、スマート カードまたは USB トークンなどのハードウェアまたはサーバ上に保存されている場合があります。そのクレデンシャルは認証時に検証されます。
コールアウト	外部（RiskFort の外）で実行するカスタム プログラム。

サーバ管理プロトコル	RiskFort サーバを起動およびシャットダウンするための Arcot 専用プロトコル。
スコアリング エンジン	個別の評価ルールからリスク スコアを収集し、スコアリングの優先順位順にそれらを処理する RiskFort サーバのコンポーネント。
スコアリング コールアウト	RiskFort のスコアリング エンジンによってスコアが付けられた後で動作し、最終リスク スコアを変更するカスタムのスコアリング ロジックを含むコールアウト。
スコアリング ルール	他のすべての設定済みルールの実行結果を受け取り、最終リスク スコアおよびリスク アドバイスを返す最後のルール。
ゾーン ホッピング	現実的な速度で移動可能な距離以上に隔たった場所からの、同一ユーザによる連続するトランザクション。
デジタル証明書	個人、コンピュータ システム、または組織の ID およびキーの所有権の証明となるデジタル ドキュメント。この認証方式は公開キー暗号化（PKI）法に基づいています。
デバイス頻度	指定された時間内に同一デバイスから発行されるトランザクションの数。
トラステッド IP アドレス	組織に信頼されているため今後のリスク評価から除外される IP アドレス。
トラステッド アグリゲータ	組織に信頼されているため今後のリスク評価から除外されるアグリゲータ。
ユーザ ID/ パスワード	登録時にユーザに発行されるクレデンシャルの 1 つ。
ユーザ頻度	指定された時間内に同一ユーザから発行されるトランザクションの数。
リスク アドバイス	トランザクションのリスクを評価した後に RiskFort によって呼び出し元のアプリケーションに示されるアクション（`ALLOW`、`ALERT`、`DENY`、`INCREASEAUTH`）。
リスク スコア	評価結果に応じて RiskFort から通知されるスコア。スコアは 0 ～ 100 です。数字が大きいほど、リスクも高くなります。
暗号化	内容を判読できないように情報にスクランブルをかける処理。
一方向 SSL	SSL セッションが確立される前に、クライアント アプリケーションが（サーバのデジタル証明書を受理することによって）サーバ アプリケーションの ID を検証します。

拡張可能エレメント	リスク評価のためにアドオン ルールによって使用されるトランザクションに関連する追加のエレメント。
拒否 IP アドレス	過去において、アノニマイザ プロキシ、不正なトランザクション、または悪意のあるトランザクションの要求元であったことがわかっている IP アドレス。
拒否国	過去において、不正なトランザクションまたは悪意のあるトランザクションの要求元であったことがわかっている国。
公開キー	PKI で使用される 1 対のキーの一方。このキーは自由に配布され、証明書の一部として発行されます。 通常、公開キーの所有者に送信されたデータを暗号化するために使用されます。その後、公開キーの所有者は、対応する秘密キーを使用して、データを復号化します。
終端ルール	単独で全体的なリスク スコアを決定するルール。
証明書	「デジタル証明書」を参照してください。
双方向 SSL	SSL セッションが確立される前に、クライアント アプリケーションとサーバ アプリケーションの両方が（それぞれのデジタル証明書を提示することによって）互いの ID を確認します。
追加認証	現在のトランザクションが安全でないと RiskFort によって判断される場合に、RiskFort から与えられるリスク アドバイス。たとえば、ユーザが初めて大量のトランザクションを実行する場合が挙げられます。そのような場合、ユーザは、より強力な認証方式を使用して認証サーバに再認証されることを求められます。
認証	エンティティのログイン情報が本人のものであることを証明するプロセス。
秘密キー	PKI で使用される 1 対のキーの一方。このキーは秘密に保持され、データの復号化または暗号化に使用できます。
非終端ルール	全体的なリスク スコアは、このルール単独では決定されません。他のルールも必要です。
評価コールアウト	すべての評価ルールの後で実行され、カスタムのリスク評価ロジックを含むコールアウト。
評価ルール	着信トランザクション データに適用される、事前に設定された RiskFort ロジック。
頻度チェック	「デバイス頻度」および「ユーザ頻度」を参照してください。
例外ユーザ	RiskFort に「登録」されており、指定された期間、リスク評価から除外されるユーザ。

索引