CA Strong Authentication

インストール ガイド（Microsoft Windows 用）

8.0

CA への連絡先

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

目次

第 1 章: はじめに

過去数年でインターネット詐欺の件数は急増し、ユーザ名とパスワードに頼る認証方式では万全ではなくなってきました。 組織は、複雑な工程は排除しながらも組織内の認証処理のセキュリティを強化することを望んでいます。 また、顧客やパートナーがアプリケーションやデータにアクセスする機会を増やしながらも財務損失やブランドへの悪影響といったリスクを回避する必要があります。

Strong Authentication は、エンド ユーザの身元を確認し、保護するための実績あるサービスで、以下のような特長があります。

- ネットワーク上でパスワード（クリア テキスト形式または暗号化形式のいずれも）を保護する。
- 各ユーザのセキュリティや利便性に対する最適な認証方式を選択できる。
- CA Auth ID および CA Auth ID OTP を使用する（両者とも特許取得のキー隠蔽技術 **Cryptographic Camouflage** に基づく）。

  Cryptographic Camouflage では、有効に見える一連のキーが攻撃者を欺くために生成されます。 この方法では、スマート カードと同様に辞書攻撃や MITM （Man-in-the-Middle、中間者）攻撃から秘密キーを保護できますが、これを完全にソフトウェア形式で実現します。

  詳細については、「Cryptographic Camouflage の仕組み」を参照してください。

このガイドでは、さまざまなソリューション要件に基づく Strong Authentication の展開の計画について説明します。 各ソリューションは複数のコンポーネントで構成され、これらのコンポーネントが相互に、および企業内の他のシステムや複数のネットワークで形成されるシステムと通信します。

Strong Authentication は、ユーザによるログイン操作や重要なビジネス プロセスを変更する必要なく、CA Auth ID を利用した認証にアップグレードできます。 また、Strong Authentication は、独自認証メカニズムとオープン認証メカニズムの実装を幅広くサポートしている点で、*VAS*（*Versatile Authentication Server*：汎用認証サーバ）といえます。また、PKI（Public Key Infrastructure）や OTP/Activation Code （ワンタイム パスワード）を利用した認証をサポートするだけでなく、既存の認証方式を組み込むことができるよう設計されています。

VAS 機能によって、エンド ユーザのニーズに最適な認証方式を選択できます。 以下を選択できます。

- 各種の標準的な認証インターフェースと統合する。
- 標準ベースのハードウェアまたはソフトウェア認証メカニズムを実装する。
- OTP/Activation Code トークンなどの従来の技術を引き続きサポートする一方で、CA Auth ID などの新しい認証方式を追加する。
- プラグインによって Strong Authentication VAS を拡張し、独自の認証方式を実行する。

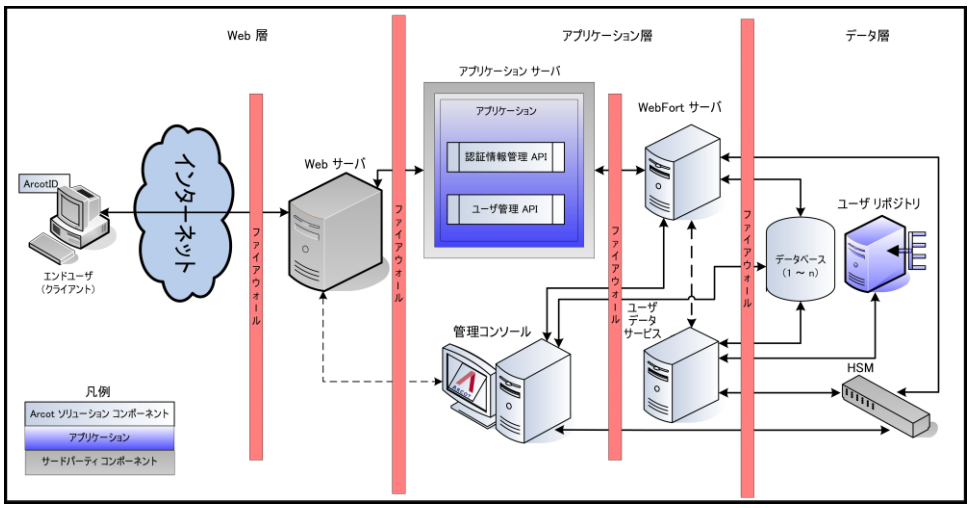
重要: このドキュメントでは、コード オブジェクトやその他の製品の一部に Arcot、WebFort、RiskFort、WebFort、RiskMinder、AuthMinder という用語が使用されています。 ArcotID は、現在、CA Auth ID と呼ばれています。また、このガイドには標準的なフォーマットのガイドラインに従っていないトピックが一部あります。

このセクションには、以下のトピックが含まれています。

システム アーキテクチャ

Strong Authentication は、単一のシステムにインストールするか、そのコンポーネントを複数のシステムに分散してインストールできます。 トランザクションのセキュリティを最大限に高めるために、以下の図に示されているアーキテクチャを実装します。

- Web 層
- アプリケーション層
- データ層



以降では、上記の各層における Strong Authentication コンポーネントについて説明します。

Web 層

Web 層は静的な（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。

Web 層によって、エンドユーザのブラウザに CA Auth ID クライアント（Java、Flash、またはネイティブ）が提供されます。 CA Auth ID クライアントは、Strong Authentication サーバと対話してユーザ認証を行います。また、CA Auth ID パスワードを収集し、チャレンジに署名し、署名済みのチャレンジを Strong Authentication サーバに送信して検証します。

注: CA Auth ID クライアントについては、「CA CA Auth ID クライアント リファレンス ガイド」を参照してください。

アプリケーション層

この層は、Strong Authentication サーバ、Strong Authentication SDK を使用するアプリケーション、Administrative UI とユーザ データ サービス（UDS）が存在するアプリケーション サーバで構成されます。

注: この層のコンポーネントをすべて単一のシステムにインストールするか、または複数のシステムに分散できます。

- **Strong Authentication サーバ**

  アプリケーションからの発行リクエストと認証リクエストを Strong Authentication SDK を利用して処理するサーバ コンポーネント。

- **CA Advanced Authentication**

  サーバ インスタンス、Strong Authentication コンポーネント間の通信モード、認証ポリシー、認証情報プロファイル、および認証情報の管理を設定し、組織、管理者、およびユーザの管理を行うための Web ベースのコンソール。

- **ユーザ データ サービス**

  RDBMS（リレーショナル データベース管理システム）やディレクトリ サーバ（LDAP）などの各種ユーザ リポジトリのユーザ関連データおよび組織関連データへのアクセスを提供する抽象層。

- **認証 API**

  認証リクエストを Strong Authentication サーバに転送するためにアプリケーションから呼び出される Java API。

- **認証情報管理 API**

  Strong Authentication でユーザ認証情報を作成および管理するために Strong Authentication サーバに発行リクエストを転送する Java API。アプリケーションから呼び出されます。

- **ユーザ管理 API**

  Strong Authentication でユーザを作成および管理するために UDS に発行リクエストを転送する Web サービス クライアント。アプリケーションから呼び出されます。

- **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、Strong Authentication Java API の使用方法およびアプリケーションと Strong Authentication の統合方法の例を示します。また、Strong Authentication が正常にインストールされているかどうかの確認、および発行操作と認証操作を実行できるかどうかの確認を行うためにも使用できます。

データ層

データ層には、ほかのユーザ リポジトリが設定されていない場合に、設定、認証情報、およびユーザ データを格納するために Strong Authentication が使用する RDBMS があります。

HSM （ハードウェア セキュリティ モジュール）は、ユーザの機密データを暗号化するために使用される場合、この層の一部になります。

プラグイン

Strong Authentication には、以下の既定の認証方式が用意されています。

- **CA Auth ID**

  CA Auth ID は、2 要素認証を提供する CA 独自のセキュア ソフトウェア認証情報です。 CA Auth ID は小さなデータ ファイルであり、それ自体を Web や VPN （仮想プライベート ネットワーク）などのさまざまなクライアントに対する強力な認証に使用できます。

  CA Auth ID の詳細については、「CA Auth ID の主要概念」を参照してください。

- **Password**

  ユーザには、システムにログインするためにユーザ名およびパスワードが発行されます。

- **ワンタイム パスワード認証 OTP/Activation Code**

  ワンタイム パスワードは、Strong Authentication サーバによって生成されるもう 1 つの認証情報です。 OTP/Activation Code は、数字の文字列または英数字の文字列です。 使用される回数を設定できます。

- **OATH 準拠のワンタイム パスワード**

  OATH（オープン認証）標準に準拠したワンタイム パスワード。Strong Authentication では、カウンタベースの OATH OTP Token （HOTP）と時間ベースの OATH OTP Token （TOTP）の両方がサポートされています。

- **質問と回答**

  質問と回答（*Q&A*）は、チャレンジ/レスポンス認証メカニズムです。ユーザは、尋ねられた質問に対して正しい回答を行うことで Strong Authentication サーバに認証されます。 これらの質問と回答は、登録時にユーザ自身が設定します。

- **CA MobileOTP**

  CA Auth ID は、OATH、EMV （Europay、MasterCard、VISA）標準に準拠しています。 お使いのアプリケーションが CA Auth ID OTP に統合されると、ユーザのパスワードを入力として受け入れ、ユーザのデバイス上でパスワード（*パスコード*とも呼ばれる）を生成します。 ユーザはこのパスコードをサブミットして、Web アプリケーションを認証します。 ユーザは、認証結果に基づき、保護されているアプリケーションへのアクセス権を付与されるか、またはアクセスを拒否されます。

パスコードの生成はオフライン プロセスです。つまり、パスコードを生成するためにアプリケーションを Strong Authentication に接続する必要はありません。

- **LDAP Username-Password**

  Strong Authentication は LDAP 認証をサポートしています。この認証では、ディレクトリ サービス内のユーザ認証情報を使用してユーザが認証されます。

1 つ以上の認証情報をユーザに対して発行できます。同じタイプの認証情報を複数発行することもできます。

デフォルトの認証メカニズムを拡張するには、プラグインを記述します。

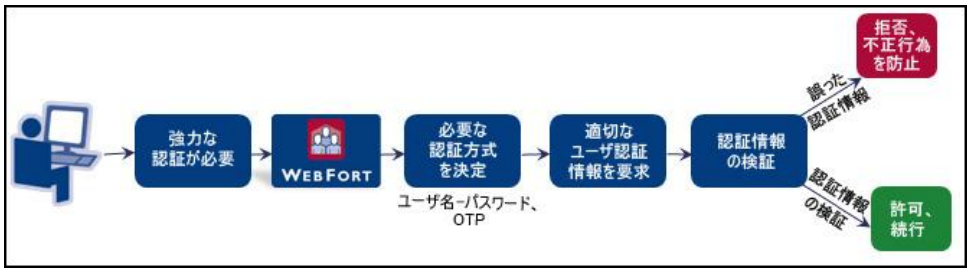
ユーザ認証

Strong Authentication で保護されている Web アプリケーションにアクセスを試みるユーザは、Strong Authentication でサポートされている既定の認証情報のいずれかを使用して認証できます。

すべての認証メカニズムで、認証が成功するたびにクライアントに認証トークンが提供されます。 トークンはクライアントがサーバに認証されていることを証明し、一定の期間のみ有効です。その期間後は、再度認証が必要です。

すべてのパスワード タイプの認証情報（パスワード、OTP/Activation Code、CA Auth ID OTP、および OATH OTP Token）は、シングル ステップ認証モデルに基づいています。 認証情報はクライアントによってユーザに渡され、サーバがユーザ認証情報を確認します。

以下の図は、典型的な認証ワークフローを示しています。



ただし、CA Auth ID および Q&A はチャレンジ/レスポンス認証モデルに基づいています。 これらの認証メカニズムには、ユーザを認証する複数の手順が含まれています。

Challenge-Response 認証ワークフロー

CA Auth ID を使用する認証は、PKI ベースのチャレンジ/レスポンス メカニズムです。クライアントはユーザの秘密キーを提供することで、認証トークンを取得します。 認証中のクライアントとサーバ間の対話は以下のとおりです。

1. **ユーザ認証情報の取得**

   Strong Authentication で保護されているアプリケーションまたはリソースがユーザ認証情報を取得します。たとえば、ユーザの CA Auth ID がシステムに存在しない場合などです。

2. **適切なチャレンジの取得**

   アプリケーションがチャレンジをリクエストします。

   Strong Authentication サーバが一意のチャレンジを作成して、ユーザの認証のためにアプリケーションに送信します。

3. **署名の生成**

   ユーザは、CA Auth ID を発見するために正しい CA Auth ID パスワードを入力します。 クライアントが、発見の結果利用可能になったユーザの秘密キーを使用してこのチャレンジに署名します。 チャレンジは、クライアント マシンに事前にロードするか、またはサーバからダウンロードすることができます。

4. **署名済みチャレンジの検証**

   署名済みチャレンジが、検証のために Strong Authentication サーバに送信されます。 署名が正常に検証されると、ユーザはログインしたり、保護されているリソースにアクセスしたりできます。 また、Strong Authentication は、トランザクションが成功するたびにユーザの認証トークンを返します。

以下の図は、CA Auth ID の認証フローを示しています。

CA Auth ID の主要概念

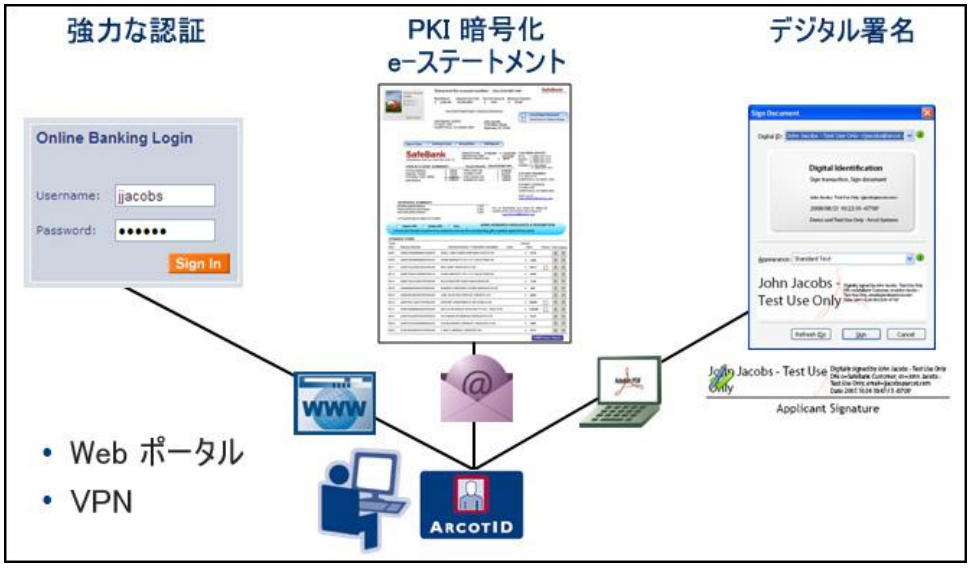
このセクションでは、Strong Authentication がサポートする第 1 の認証情報である CA Auth ID の主要概念について説明します。

- CA Auth ID の概要
- CA Auth ID のファイル構造
- Cryptographic Camouflage の仕組み
- ローミング ダウンロードのサポート
- セキュア コンテナ（Key Authority）としての CA Auth ID
- CA Auth ID クライアント

CA Auth ID の概要

CA Auth ID は、エンド ユーザのハードウェアを使用せずに、PKI 対応アプリケーションの認証、デジタル署名、暗号化、および復号化に、スマートカードと同じ機能を提供します。Web アプリケーションが PKI ベースの認証をサポートしていない場合でも、CA Auth ID は Web アプリケーションに対して認証を行います。

以下の図は、CA Auth ID のユース ケースを示しています。



CA Auth ID はデータ ファイルであり、セキュリティ保護されたオンデマンド認証のために、エンド ユーザのコンピュータや USB ドライブに保存されるか、またはリモートでダウンロードされます。CA Auth ID は、パスワードの総当たり攻撃、中間者攻撃などのフィッシング攻撃に対して脆弱では*ありません*。

CA Auth ID は、Web や VPN （仮想プライベート ネットワーク）など、さまざまなアプリケーションの強力な認証に使用されます。

CA Auth ID は、シンプルであるが安全ではないユーザ名/パスワード認証と、高価で展開が難しいが非常に安全なスマート カードおよび USB トークン ソリューションの間のギャップを埋める、設定可能なソリューションです。

CA Auth ID は、業界標準および CA の特許取得済みの Cryptographic Camouflage 技術に基づいており、総当たり攻撃に対して保護されている強力な認証をソフトウェアのみで提供します。

CA Auth ID はパスワードで保護されており、強力な認証を提供するために以下の機能をサポートしています。

- CA Auth ID にアクセスできるのは正しい CA Auth ID パスワードのみです。
- 入力されるすべての CA Auth ID パスワードに対して、それが正しくない場合でも、偽装したレスポンスが生成されます。CA Auth ID パスワードのオフラインでの識別が妨げられます。
- CA Auth ID 認証はチャレンジ/レスポンス認証プロトコルであり、ユーザのパスワードはローカルでのみ使用され、転送されたり、サーバ側で検証されたりすることはありません。
- 正しくない CA Auth ID パスワードが繰り返し入力されると、設定されている最大の認証試行数に応じて CA Auth ID がロックアウトされます。
- CA Auth ID を発行したドメインでのみ有効です。
- CA Auth ID はオンラインでのみ使用されます。ユーザが自分の CA Auth ID パスワードを検証するためには、Strong Authentication サーバに接続する*必要があります*。

CA Auth ID のファイル構造

CA Auth ID には、以下のコンポーネントが含まれています。

1. 標準の X.509v3 デジタル証明書（CA 固有の拡張あり）。
2. Strong Authentication サーバに対する認証のために生成される、公開キーと秘密キーの 2 番目のペア。 これは、一般的な署名や暗号化には使用されません。

   公開キーは暗号化された形式で格納されます。公開キーは、CA Auth ID の作成および認証に使用される *ドメイン キー*を使用して暗号化されます。 ドメイン キーは、グローバル レベルまたは組織レベルで設定できます。 組織に固有のドメイン キーを使用して発行された CA Auth ID は、組織を越えて使用することは *できません*。

   秘密キーは、CA Auth ID パスワードを使用して暗号的に隠蔽されます。
3. 署名、暗号化、および復号化を行うためのユーザのオープン PKI キーおよび証明書を格納するセクション。詳細については、「セキュア コンテナ（Key Authority）としての CA Auth ID」を参照してください。

Cryptographic Camouflage の仕組み

Web ブラウザでの公開キー暗号化のサポートにより、公開キー暗号化署名および認証プロトコルの使用は以前より一般的になっています。 ただし、秘密キーのセキュリティは課題として残っています。 最も基本的な脅威は、ディスクに保存されている秘密キーの盗難です。 通常、秘密キーはソフトウェア キー コンテナ、ファイルに格納されていて、キーはパスワードを使用して暗号化されています。 コンテナを盗む攻撃者は、辞書攻撃を使用して、パスワードを推測しようとします。

このような問題を打開するために、Strong Authentication は、Cryptographic Camouflage を使用して、ソフトウェア内に秘密キーの安全なストレージを確保する方式を提供しています。 キー コンテナへの攻撃は本質的に監視されます。 キー コンテナでは、偽装の秘密キーの中にユーザの秘密キーを埋め込みます。 キー コンテナのクラッキングを試みる攻撃者は、多くの偽装の秘密キーを復元化します。 攻撃者は、そのキーを使用してチャレンジに署名して、Strong Authentication サーバに送信するまで、正しい秘密キーと偽装キーを区別することはできません。 Strong Authentication サーバは複数の認証の失敗を検知して、ユーザのアクセスを一時的に停止します。

ローミング ダウンロード

CA Auth ID は、移動中に任意のデバイスを使用してダウンロードできます。この機能は*ローミング*と呼ばれています。Strong Authentication サーバは、ユーザが CA Auth ID を安全にダウンロードして任意のシステムから認証することができるローミング機能を提供します。ローミング機能は、データを不正なアクセスから保護しながら、必要な場合はいつでも、クリティカルなデータおよびサービスへの即時アクセスを提供します。

ローミング ユーザは、Q&A、OTP を使用して、またはカスタマイズしたサードパーティのソリューションを使用して認証できます。

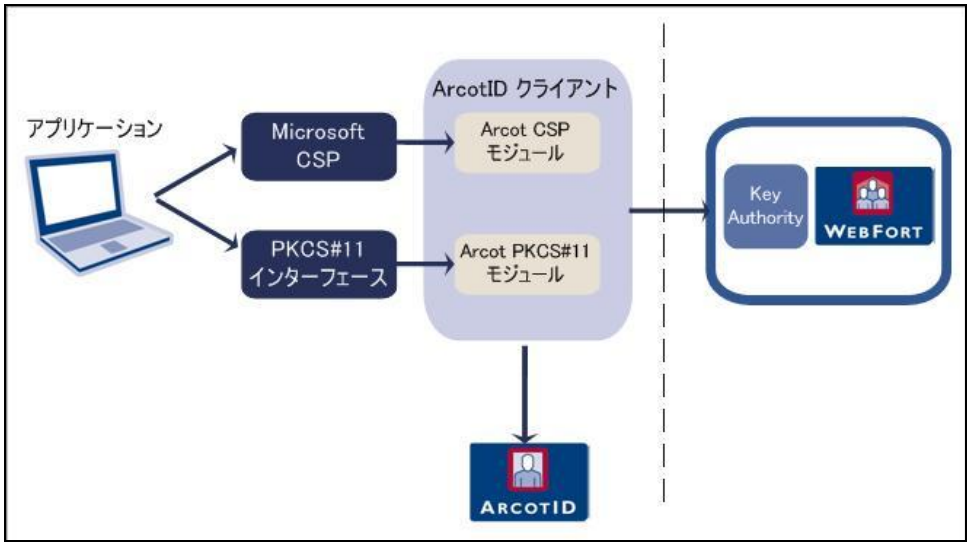
セキュア コンテナ（Key Authority）としての CA Auth ID

CA Auth ID は、電子メール署名（S/MIME）、ドキュメント署名、証明書ベースの認証（オープン PKI）など、さまざまなアプリケーションや操作に使用できるデジタル証明書および秘密キーを格納するためのセキュア コンテナとしても使用できます。CA Auth ID 内の秘密キー ストレージを管理するプロセスは、KA （*Key Authority*）によって実行されます。

*キー バッグ*または*キー ボールト*と呼ばれる無署名属性が、これらの認証情報を格納するために CA Auth ID に作成されます。デジタル証明書は暗号化されていない形式でキー バッグに格納されます。 秘密キーは、Strong Authentication データベースに格納されている *Key Authority* キーと呼ばれるキーを使用して暗号化されます。

キー バッグに格納されている秘密キーを使用するために、CA Auth ID クライアント（「CA Auth ID クライアント」を参照）は、ユーザの秘密キーを使用してリクエストに署名して、Strong Authentication サーバに KA キーをリクエストします。 Strong Authentication サーバは受信リクエストを認証して、クライアントに KA キーを送信します。クライアントは、キー バッグを開き、秘密キーにアクセスします。

以下の図は、オープン PKI コンテナとして CA Auth ID を使用する方法を示しています。



CA Auth ID クライアント

CA Auth ID クライアント ソフトウェアは Strong Authentication サーバと一緒に使用されます。CA Auth ID クライアントでは、エンド ユーザは Web ブラウザで CA Auth ID を使用して、Web サイト、VPN、またはその他のオンライン リソースへの認証を行うことができます。

さまざまなアプリケーション環境（オペレーティング システム、ブラウザ、JVM）をサポートするために、CA Auth ID クライアントは以下のようなさまざまなもので利用できます。

- ネイティブ クライアント
- Flash クライアント
- Java 署名済みアプレット
- Java 未署名アプレット
- JavaScript クライアント

注: これらのクライアント タイプの詳細については、「CA CA Auth ID クライアント リファレンス 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、展開モデルの選択と、各システムにインストールする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。

注: このガイドでは、*システム*は物理デバイスを指し、*サーバ*はシステム上で実行されるソフトウェアを指します。

この章は以下のトピックで構成されます。

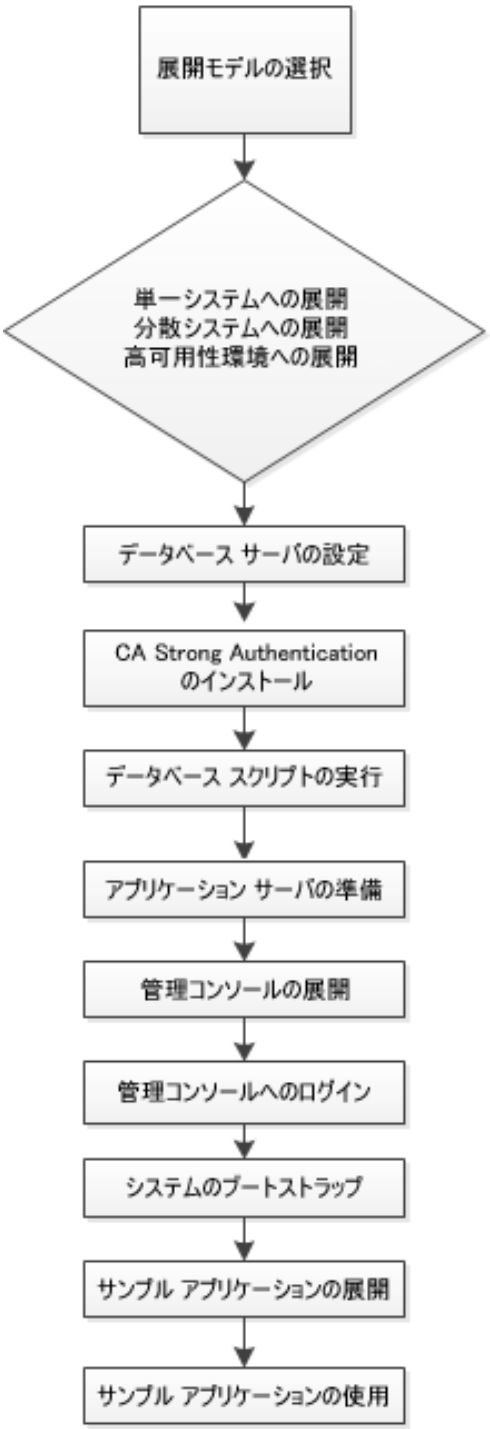
- 新規インストールの展開の概要
- 展開モデルの選択

新規インストールの展開の概要

このセクションでは、Strong Authentication を展開するための手順を簡潔に説明します。

Strong Authentication の展開には、以下の図に示されている手順が含まれます。

CA Strong Authentication の新規インストールの展開の概要



1. ビジネス ニーズに適した展開モデルを選択します。 Strong Authentication は、単一のシステムにインストールするか、複数のシステムに分散してインストールできます。

   詳細については、「展開モデル」を参照してください。

2. Strong Authentication スキーマをシードするデータベース サーバを設定します。

   - MS SQL Server データベースの設定の詳細については、「Microsoft SQL Server の設定」を参照してください。
   - Oracle データベースの設定の詳細については、「Oracle データベースの設定」を参照してください。
   - IBM DB2 データベースの設定の詳細については、「IBM DB2 ユニバーサル データベースの設定」を参照してください。
   - MySQL データベースの設定の詳細については、「MySQL の設定」を参照してください。

3. Strong Authentication をインストールします。

   - 単一システムへの展開については、「単一システムへの Strong Authentication の展開」を参照してください。
   - 分散システムへの展開については、「分散システムに Strong Authentication を展開する方法」を参照してください。

4. データベースで SQL スクリプトを実行し、Strong Authentication スキーマを作成して、初期設定値を設定します。

   - 単一システムの展開については、「データベース スクリプトの実行」を参照してください。
   - 分散システムの展開については、「データベース スクリプトの実行」を参照してください。

5. アプリケーション サーバ上の必要なファイルと JAR をコピーします。CA Advanced Authentication およびユーザ データ サービスは、正常に機能するためにこれらのファイルを使用します。

   - 単一システム展開でのファイルのコピーの詳細については、「アプリケーション サーバの準備」を参照してください。
   - 分散展開でのファイルのコピーの詳細については、「アプリケーション サーバの準備」を参照してください。

6. CA Advanced Authentication を展開します。

- 単一システム展開への CA Advanced Authentication の展開の詳細については、「CA Advanced Authentication の展開」を参照してください。
- 分散システム展開への CA Advanced Authentication の展開の詳細については、「CA Advanced Authentication の展開」を参照してください。

7. マスタ管理者として CA Advanced Authentication にログインし、Strong Authentication を初期化します。
   - 単一システム展開での CA Advanced Authentication の初期化の詳細については、「CA Advanced Authentication へのログイン」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。
   - 分散システム展開での CA Advanced Authentication の初期化の詳細については、「CA Advanced Authentication へのログイン」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。
8. Strong Authentication サーバを起動し、サービスが正常に開始されていることを確認します。
   - 単一システム展開での Strong Authentication サーバの起動の詳細については、「Strong Authentication サーバの起動」および「インストールの確認」を参照してください。
   - 分散システム展開での Strong Authentication サーバの起動の詳細については、「Strong Authentication サーバの起動」および「インストールの確認」を参照してください。
9. サンプル アプリケーションを展開および実行して、Strong Authentication のインストールをテストします。
   - 単一システム展開でのこの実行方法の詳細については、「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。
   - 分散展開でのこの実行方法の詳細については、「サンプル アプリケーションの展開」、「サンプル アプリケーションの通信サーバの設定」、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。
10. **（オプション）**ユーザ リポジトリとしてディレクトリ サービスを使用する*場合のみ*、ユーザ データ サービス（UDS）を展開します。
    - 単一システム展開での UDS の展開および起動の詳細については、「ユーザ データ サービスの展開」を参照してください。

- 分散展開での UDS の展開および起動の詳細については、「ユーザ データ サービスの展開」を参照してください。

展開モデル

Strong Authentication サーバは、展開時にユーザを認証するためにインストールする主要コンポーネントです。 Strong Authentication サーバ上のアプリケーションは、付属の Java SDK または Web サービスを使用して Strong Authentication サーバに統合できます。

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 データベースが必要です。

通常、開発および単純なテストが目的の場合は、Strong Authentication のすべてのコンポーネントを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は、Strong Authentication サーバを専用のシステムにインストールすることをお勧めします。 付属の SDK または Web サービスは、別のシステムまた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システムにインストールします。

Strong Authentication には、Strong Authentication が正しくインストールされているかどうか、およびユーザ認証を実行できるかどうかを確認するためのサンプル アプリケーションも付属しています。 また、Strong Authentication を既存のアプリケーションと統合するためのサンプル コードとしても役立ちます。

Strong Authentication でサポートされてい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

  詳細については、「単一システムへの展開」を参照してください。
- **分散システム展開** - 運用環境またはステージング環境用

  詳細については、「分散システムへの展開」を参照してください。
- **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

  詳細については、「高可用性環境での展開」を参照してください。

単一システムへの展開

単一システムへの展開では、Strong Authentication および Web アプリケーションのすべてのコンポーネントが、単一システム上にインストールされます。 データベースは、Strong Authentication がインストールされているのと同じシステム上、または異なるシステム上のどちらにあってもかまいません。 この展開モデルは通常、開発、概念実証、または初期テストで使用されます。

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。

単一システムに Strong Authentication を展開するには、Strong Authentication のインストール時に［*Complete*］オプションを選択する必要があります。

コンポーネント図

コンポーネント図には、事前インストール ソフトウェアおよび Strong Authentication コンポーネントの展開オプションがいくつか示されています。 Complete インストールを実行すると、Java SDK および Web サービスの両方がシステムにインストールされます。 Strong Authentication と Web アプリケーションの統合には、これらのいずれの方法も使用できます。

- Java SDK の展開
- Web サービスの展開

決定のポイント

単一システムへの展開を実行する場合は、以下の選択を行います。

- Strong Authentication 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お勧めします。

- Java SDK または Web サービスを使用して、ご使用の Web アプリケーションと統合します。

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

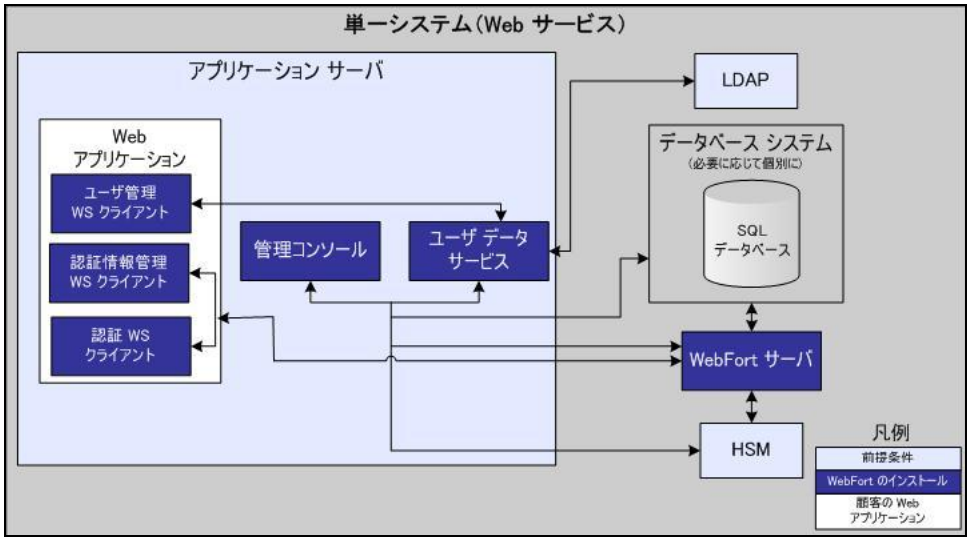
以下の図は、単一システムへの Strong Authentication サーバおよび Java SDK の展開を示しています。

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、Strong Authentication 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に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、以下の図は、単一システムの Strong Authentication 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 Strong Authentication サーバ モジュール自体に組み込まれているので、Strong Authentication 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済みます。 追加設定は必要ありません。



分散システムへの展開

分散システムへの展開では、セキュリティおよびパフォーマンスを向上させるために Strong Authentication コンポーネントは異なるシステム上にインストールされます。 このモデルは通常、運用環境の展開またはステージングの環境で使用されます。

最も一般的な展開では、1 つのシステムに Strong Authentication サーバをインストールし、追加のシステムに 1 つ以上の Web アプリケーションをインストールします。 分散システム上に Strong Authentication を展開するには、Strong Authentication インストール時に［*Custom*］オプションを選択する必要があります。 インストールおよびインストール後の手順の詳細については、「分散システムに Strong Authentication を展開する方法」の章を参照してください。

コンポーネント図

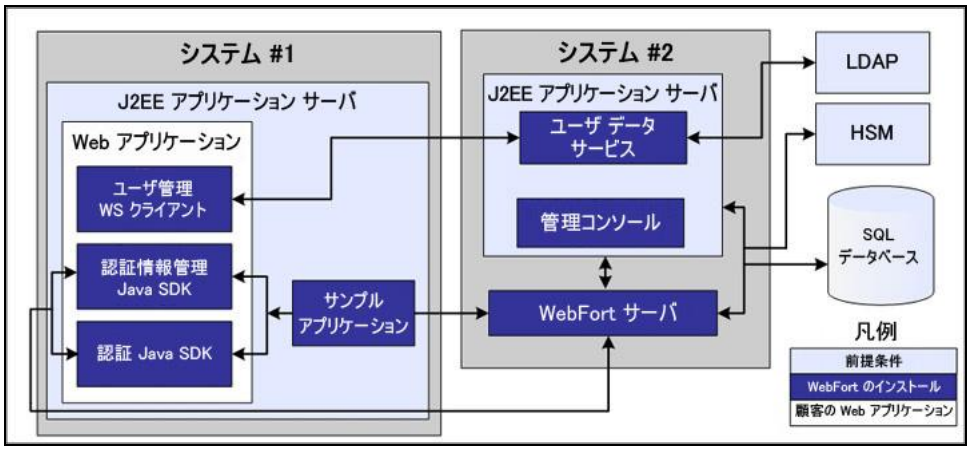
このセクションの図は、事前インストール ソフトウェアと Strong Authentication コンポーネントを複数のシステムにインストールする場合のオプションを示しています。

- 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

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。

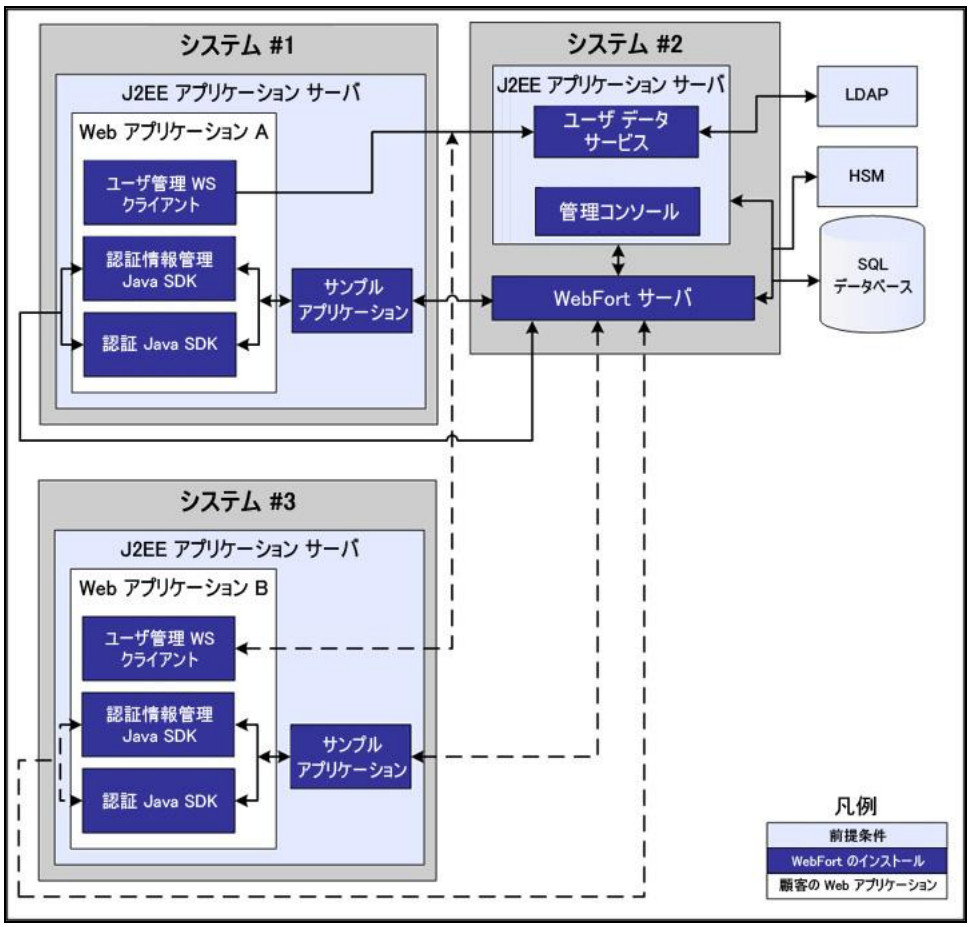
Java SDK を使用した単一アプリケーションの展開

以下の図は、Java SDK を使用した単一アプリケーションへの Strong Authentication の展開を示しています。



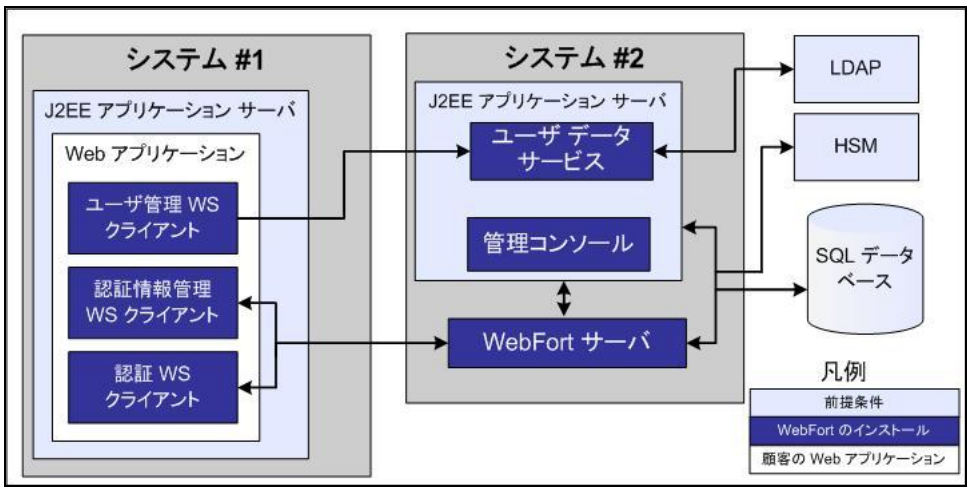
Java SDK を使用した複数アプリケーションの展開

以下の図は、Java SDK を使用した複数アプリケーションへの Strong Authentication の展開を示しています。



Web サービスを使用した単一アプリケーションの展開

以下の図は、Web サービスを使用した単一アプリケーションへの Strong Authentication の展開を示しています。



高可用性展開

高可用性展開では、高可用性と拡張性を実現するために、Strong Authentication 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。

コンポーネント図

このセクションの図は、事前インストール ソフトウェアと Strong Authentication 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オプションを示しています。

決定のポイント

- 新しいサーバ インスタンスをいつ追加するか。

  通常、トランザクション レートが許容されるしきい値（組織のポリシーによって決定）を超えた場合、新しいサーバ インスタンスを追加する必要があります。

- Strong Authentication サーバ、CA Advanced Authentication、UDS、および SDK インスタンスはそれぞれいくつ必要か。

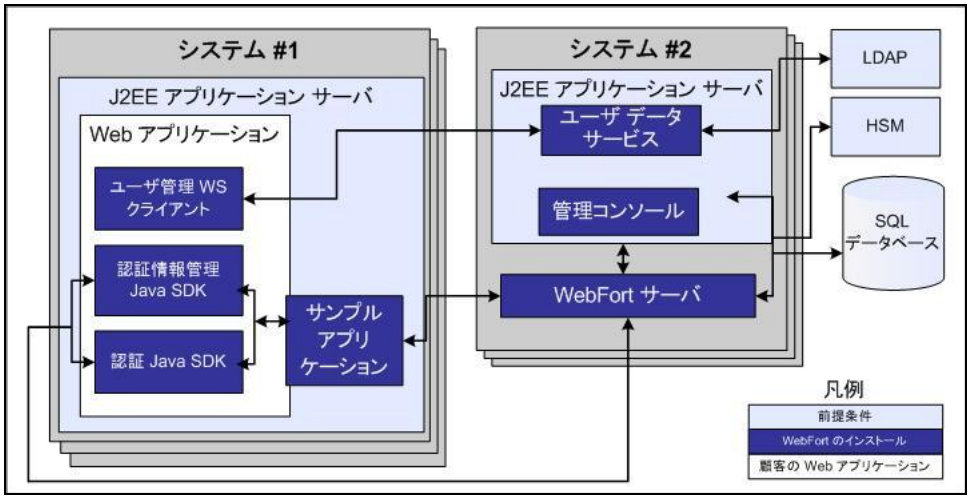
  - **Strong Authentication サーバ：** 複数インスタンスがサポートされています。 数は、目標のトランザクション レートによって異なります。
  - **CA Advanced Authentication：** 複数インスタンスがサポートされています。 数は、管理コンソールに同時にログインするシステム内の管理者の数によって異なります。
  - **UDS サーバ：** 現在、1 つのみサポートされています。複数の UDS インスタンスが必要な場合は、ロード バランサの背後に配置する必要があります。 ただし、UDS フェイルオーバはサポートされていません。
  - **SDK：** 複数インスタンスがサポートされています。 数は、サポートするアプリケーション インスタンスの数によって異なります。

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 を使用した高可用性展開
- Web サービスを使用した高可用性展開

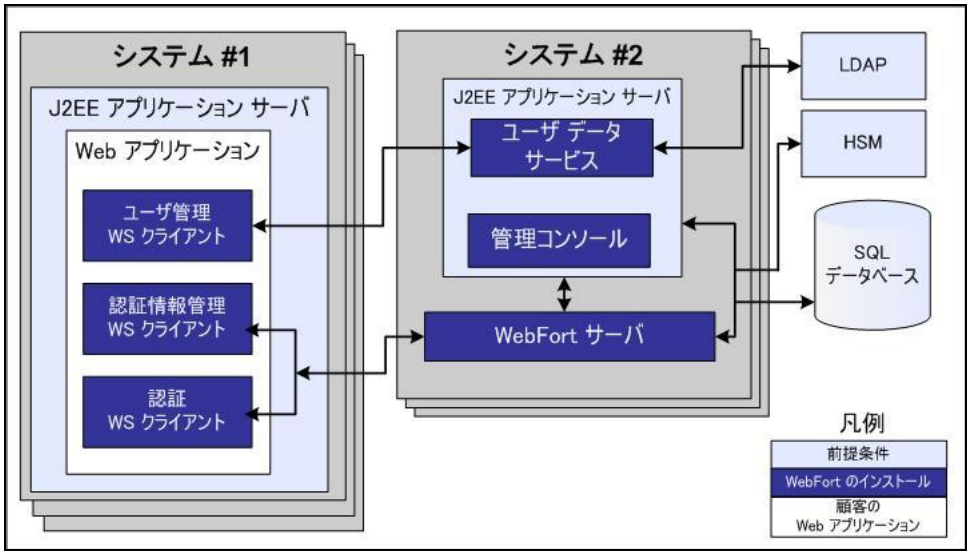
Java SDK を使用した高可用性展開

以下の図は、Java SDK を使用した Strong Authentication の複数インスタンス展開を示しています。



Web サービスを使用した高可用性展開

以下の図は、Web サービスを使用した Strong Authentication の複数インスタンス展開を示しています。



第 3 章: データベース サーバを設定する方法

Strong Authentication 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します。

Strong Authentication では、プライマリ データベースと、高可用性展開でのフェールオーバ時とフェールバック時に使用できるバックアップ データベースを使用できます。 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。

- インストール時に、ユーザが入力したデータベース情報を使用して、インストーラが arcotcommon.ini ファイルを編集するときに自動的に設定されます。
- 以下の方法で、手動で設定します。
  - DSN （データ ソース名）を作成します。
  - arcotcommon.ini ファイルを編集します。
  - dbutil ツールを使用して、securestore.enc を更新します。

サポートされているデータベースごとに固有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。

注: JBoss アプリケーション サーバでは、バックアップ データベースの設定時に以下の手順を実行します。

a. <JBOSS_HOME>¥modules¥system¥layers¥base¥sun¥jdk¥main フォルダ内の module.xml ファイルを編集して、以下のステートメントを記述します。

```
<path name="com/sun/rowset"/>
<path name="com/sun/rowset/internal"/>
<path name="com/sun/rowset/providers"/>
```

アプリケーション サーバを再起動します。

重要: データベースを保護するために、データベース サーバをファイアウォールまたはその他のアクセス制御メカニズムで保護し、関連するすべての製品と同じタイム ゾーンに設定することをお勧めします。

- Microsoft SQL Server の設定
- Oracle データベースの設定
- IBM DB2 Universal Database の設定
- MySQL の設定

SQL Server の設定

このセクションでは、Microsoft SQL Server 用の以下の設定情報を示します。

重要: Microsoft SQL Server が「**SQL Server 認証**」認証方式を使用するように設定されていることを確認します。

注: このセクションに示すタスクの実行の詳細については、Microsoft SQL Server のドキュメントを参照してください。

以下の条件に従ってデータベースを設定します。

1. 推奨される名前は arcotdb です。
2. データベース サイズは自動的に拡大するように設定する必要があります。
3. データベース ユーザの作成

データベース ユーザの作成

データベース ユーザを作成するには、以下の手順に従います。

次の手順に従ってください:

1. SQL Server Management Studio で、*<SQL_Server_Name>* に移動し、［**セキュリティ**］フォルダを展開して、［**ログイン**］をクリックします。

   注: *<SQL_Server_Name>* は、データベースを作成した SQL Server のホスト名または IP アドレスを指します。

2. ［**ログイン**］フォルダを右クリックし、［**新しいログイン**］をクリックします。
3. ログイン名を入力します。 推奨される名前は arcotuser です。
4. 以下のパラメータを設定します。
   a. **SQL Server 認証**に対する認証。
   b. ログインの［**パスワード**］および［**パスワードの確認入力**］を指定します。

      組織のパスワード ポリシーに従い、このページのその他のパスワード設定を指定してください。

   c. 作成したデータベース（arcotdb）に対する［**既定のデータベース**］。
   d. ログイン（［**このログインにマップされたユーザー**］セクション内）用の［**ユーザー マッピング**］。
   e. db_owner （［**<db_name> のデータベース ロール メンバシップ**］セクション）に対するデフォルト データベース用の［**ユーザー マッピング**］（SQL 2005）。

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 Strong Authentication 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。

Oracle を使用して Strong Authentication 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、デフォルト 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、別のテーブルスペースを使用することをお勧めします。

スクリプト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、データベース設定スクリプト（arcot-db-config-for-common-8.0.sql）によってレポート テーブルスペースが自動的に作成されます。ユーザに必要な権限がない場合、DBA は手動でレポート テーブルスペースを作成し、テーブルスペースを作成するこのスクリプト内のセクションを削除できます。

同じ名前のテーブルスペースがすでに存在する場合は、削除され再作成されます。

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-8.0.sql データベース スクリプト内のパラメータは、DBA の希望に応じて変更できます。ただし、テーブルスペース名が ARReports であることを確認します。

データベースの作成

UTF-8 文字セットで情報を格納するデータベースを作成します。 この文字セットにより、Strong Authentication で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。

次の手順に従ってください:

1. SYS または SYSTEM として Oracle データベース サーバにログインします。
2. 以下のコマンドを実行します。
   ```
   Update sys.props$ set value$='UTF8' where
   name='NLS_NCHAR_CHARACTERSET' Or name = 'NLS_CHARACTERSET';
   ```
3. データベースを再起動し、文字セットが UTF-8 に設定されているかどうかを確認します。
4. 新しいデータベース arcotdb にユーザを作成します（推奨される名前は arcotuser）。
5. 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: 本稼働、ステージング、またはその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「データベース リファレンス」を参照してください。
6. ユーザに以下の権限を付与します。

   ```
   CREATE TABLE
   CREATE INDEX
   CREATE SEQUENCE
   CREATE PROCEDURE
   CREATE SESSION
   DML PRIVILEGES
    RESOURCE PRIVILEGES
   CONNECT PRIVILEGES
   ALTER TABLE
   ```

   - アップグレード専用の追加権限

   ```
    ALTER EXTENT PARAMETERS
    CREATE TABLESPACE
   ```

   - レポートを使用するための追加権限

UNLIMITED TABLESPACE

（オプション） DROP TABLESPACE

IBM DB2 Universal Database の設定

このセクションでは、IBM DB2 Universal Database （UDB）用の以下の設定情報を示します。

UTF-8 文字セットで情報を格納する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、Strong Authentication で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。

1. IBM DB2 UDB データベース サーバにログインします。
2. 以下のコマンドを実行して、UTF-8 サポートを有効にします。
   `create db <DB-NAME> using codeset utf-8 territory us;`
3. テーブルスペースのページ サイズを **16K** に設定します。デフォルトは 4K です。

   テーブルスペースのページ サイズの変更の詳細については、ベンダーのドキュメントを参照してください。
4. データ量が多い場合、トランザクション ログ ファイルのデフォルト サイズでは不十分な場合があります。 そのため、ログ ファイル サイズを増やすことをお勧めします。

   ログ ファイル サイズの変更の詳細については、ベンダーのドキュメントを参照してください。
5. 設定変更が適用されたことを確認します。

   代替スキーマを使用する場合の詳細については、付録「IBM DB2 Universal Database の代替スキーマの設定」を参照してください。
6. 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）。
7. ユーザに以下の権限を付与します。

   ```
   CREATE TABLE
   CREATE INDEX
   CREATE SEQUENCE
   CREATE PROCEDURE
   CREATE SESSION
   DML PRIVILEGES
   CONNECT PRIVILEGES
   ALTER TABLE
   ```

   - アップグレード専用の追加権限

CREATE TABLESPACE （AUTORESIZE = yes を指定）

- レポートを使用するための追加権限

DROP TABLESPACE

MySQL データベースの設定

このセクションでは、MySQL データベース用の以下の設定情報を示します。

Strong Authentication は、MySQL の InnoDB ストレージ エンジンを使用します。 このストレージ エンジンが MySQL のインストールでサポートされているかどうかを確認するには、SHOW ENGINES コマンドを使用します。 このコマンドの出力に InnoDB がサポートされていないことが示されている場合は、InnoDB のサポートを有効にします。

注: InnoDB のサポートを有効にする手順については、MySQL のドキュメントを参照してください。

1. MySQL コマンド ウィンドウを開きます。
2. 以下のコマンドを実行して、データベース スキーマを作成します。
   `CREATE SCHEMA '<schema-name>' DEFAULT CHARACTER SET utf8;`
3. 以下のコマンドを実行して、データベース ユーザを作成します。
   `CREATE USER '<user-name>' identified by '<user-password>';`
4. 新しいデータベース arcotdb にユーザを作成します（推奨される名前は arcotuser）。
5. ユーザに以下の権限を付与します。

   オブジェクト権限

   `SELECT`

   `INSERT`

   `UPDATE`

   `DELETE`

   `EXECUTE`

   DDL 権限

   `CREATE`

   `ALTER`

   `CREATE ROUTINE`

   `ALTER ROUTINE`

   `DROP`

   その他の権限

   `GRANT OPTION`

第 4 章: インストール前のチェックリスト

Strong Authentication のインストールと設定に進む前に、以下のチェックリストを確認することをお勧めします。

注: 以下のチェックリストの項目および値はサンプルです。インストールを開始する前に、動作環境の要件を満たすように、このチェックリストを変更してください。

情報	入力例	記入欄
ハードウェア		
プロセッサ	Intel Xeon X5450 3 GHz	
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	Windows Server 2003	
ディストリビューション	Enterprise Edition	
サービス パック（パッチ）	SP3	
データベース		
Type	Oracle	
データベース名（*MS SQL および DB2 のみ*）	arcotdb	
DSN 名	arcotdsn	
ホスト名（またはサーバ IP アドレス）	51.100.25.24	
ポート	1521	
サービス ID（Oracle データベースのみ）	oradb1	
データベース ユーザ	arcotuser	
データベース ログイン パスワード	password1234!	
設定済みの権限： **注**: CREATE 権限の場合はすべて、対応する DROP 権限があります。		

情報	入力例	記入欄
Oracle データベース		
CREATE TABLE		
CREATE INDEX		
CREATE SEQUENCE		
CREATE PROCEDURE		
CREATE SESSION		
DML PRIVILEGES		
RESOURCE PRIVILEGES		
CONNECT PRIVILEGES		
ALTER TABLE *(アップグレードの場合のみ)*		
ALTER EXTENT PARAMETERS		
CREATE TABLESPACE *(レポートの場合)*		
UNLIMITED TABLESPACE *(レポートの場合、オプション)*		
DROP TABLESPACE		
MS SQL Server **注**: これらのアクションを実行するユーザは、ddladmin ロールに属している必要があります。		
CREATE TABLE		
CREATE INDEX		
CREATE PROCEDURE		
REFERENCES		
DML PRIVILEGES		
CONNECT PRIVILEGES		
ALTER *(アップグレードの場合のみ)*		

情報	入力例	記入欄
DB2 データベース		
CREATE TABLE		
CREATE INDEX		
CREATE SEQUENCE		
CREATE PROCEDURE		
CREATE SESSION		
DML PRIVILEGES		
CONNECT PRIVILEGES		
ALTER TABLE *(アップグレードの場合のみ)*		
CREATE TABLESPACE （AUTORESIZE = yes を指定） *(レポートの場合)*		
DROP TABLESPACE		
MySQL		
SELECT		
INSERT		
UPDATE		
DELETE		
EXECUTE		
CREATE		
ALTER		
CREATE ROUTINE		
ALTER ROUTINE		
DROP		
GRANT OPTION		
アプリケーション サーバ		
Type	Apache Tomcat 5.5	
ホスト名	localhost	

情報	入力例	記入欄
ポート	8080	
JDK	1.5.0_10	
ディレクトリ サービス（オプション）		
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	
User Name	cn=admin,cn=Administrators,cn=dscc	
Password	mypassword1234!	
Web サーバ（オプション）		
Type	IIS 6	
ホスト名	mywebserver.com	
ポート	443	

第 5 章: 単一システムへの Strong Authentication の展開

Strong Authentication コンポーネントのインストールは、Strong Authentication 8.0 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 Strong Authentication 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*］オプションを使用します。

大まかな作業の流れは以下のとおりです。

1. Strong Authentication インストーラを実行してファイル システムに Strong Authentication コンポーネントを追加し、SQL データベースにアクセスできるように設定します。

   インストール手順については、「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、スキーマおよびデータベース テーブルを作成します。データベースが正常にセットアップ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 セットアップの確認」を参照してください。

3. アプリケーション サーバを準備して、CA Web コンポーネントが使用するファイルをコピーします。

   詳細については、「アプリケーション サーバの準備」を参照してください。

4. アプリケーション サーバに CA Advanced Authentication を展開して、展開を確認します。

   詳細については、「CA Advanced Authentication の展開」および「CA Advanced Authentication の確認」を参照してください。

5. マスタ管理者として CA Advanced Authentication にログインし、Strong Authentication を初期化します。

   詳細については、「CA Advanced Authentication へのログイン」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。

6. Strong Authentication サーバを起動し、サービスが正常に開始されていることを確認します。

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

7. アプリケーション サーバにユーザ データ サービスを展開して、展開を確認します。

   詳細については、「ユーザ データ サービスの展開」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、これを使用して Strong Authentication 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。

9. （オプション）Strong Authentication 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、「Strong Authentication 管理ガイド」の付録「SSL の設定」を参照してください。

10. 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 Strong Authentication をインストールする際は、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）。

- 現時点では、インストーラを使用して Strong Authentication 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 Systems¥ およびそのサブディレクトリは手動でクリーンアップします。
- 既存の %ARCOT_HOME% のインスタンスがすでに含まれているシステム上でインストーラを実行する場合。
  - インストール ディレクトリを要求され*ません*。
  - データベースのセットアップを要求され*ません*。 インストーラは既存のデータベースを使用します。
  - また、暗号化のセットアップを要求され*ません*。

Strong Authentication インストーラは、以下のインストール タイプをサポートしています。単一のシステムへの展開時には、*Complete* インストールを使用します。

1. **Complete** - 単一のシステムにすべての Strong Authentication コンポーネントをインストールします。
2. **Custom** - 選択した Strong Authentication コンポーネントをインストールします。

Complete インストールの実行

Strong Authentication をインストールするには、インストールに使用するユーザ アカウントが Administrators グループに属している*必要があります*。

Strong Authentication コンポーネントを単一システムにインストールするには、［*Complete*］オプションを使用する必要があります。 *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。これは、上級ユーザが実行することをお勧めします。

次の手順に従ってください:

1. インストール パッケージにある Strong Authentication インストーラ Strong Authentication-Windows-Installer.exe ファイルを見つけます。
2. インストーラ ファイルをダブルクリックし、［Next］をクリックします。
3. 使用許諾契約書の条件に同意して［Next］をクリックします。

   インストーラによって、ほかの CA 製品がコンピュータにインストールされているかどうかが確認されます。

   インストールされた既存の CA 製品が見つからなければ、インストール ディレクトリの入力を求めるプロンプトが表示されます。 この場合、［Installation Location］画面が表示されます。

   インストールされている既存の CA 製品が検出された場合、インストール ディレクトリの入力を求めるプロンプトは表示されません。既存の ARCOT_HOME がコンピュータ上にある場合は、以下の画面が表示されます。
4. インストーラによって指定されたデフォルト ディレクトリをそのまま使用して、Strong Authentication をインストールします。 または、［Choose］をクリックし、別のディレクトリに移動して、そこを指定することもできます。
5. ［Next］をクリックし、指定したディレクトリへのインストールを実行します。
6. すべてのコンポーネントをインストールする場合は［*Complete*］オプションを選択し、［Next］をクリックします。

   ［Database Type］画面が表示されます。

7. データベース タイプを選択し、［Next］をクリックします。

   対応する［Database Details］画面が表示されます。

   注: Strong Authentication では、Oracle Real Application Clusters （Oracle RAC）がサポートされています。 Strong Authentication インストール環境で Oracle RAC を使用するには、この手順で Oracle データベースを選択し、「Oracle RAC 用の CA Strong Authentication の設定」の手順を実行します。

   使用しているデータベースに関する以下の詳細を入力します。

- MS SQL データベース アクセス

   a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
Primary ODBC DSN	インストーラによって、Strong Authentication 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。
サーバ	データベース サーバのホスト名または IP アドレス。SQL サーバが名前付きインスタンス モードで展開する場合は、さらに円記号「¥」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスする（SQL Server ではこれを*ログイン*といいます）ために、Strong Authentication が使用するユーザ名。 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	データベースにアクセスするために Strong Authentication が使用するパスワード。 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。
データベース	Strong Authentication がアクセスするデータベースの名前。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。

b. ［Test Data Source］をクリックして、正常にデータベースに接続されているかどうかをテストします。

c. ［次へ］をクリックします。

d. 手順 8 に進みます。

- IBM DB2 （UDB）データベースの詳細情報

a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
Primary ODBC DSN	インストーラによって、Strong Authentication 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。
サーバ	データベース サーバのホスト名または IP アドレス。 データベースを名前付きインスタンス モードで展開する場合は、さらに円記号「¥」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスするために Strong Authentication が使用するユーザ名。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	データベースにアクセスするために Strong Authentication が使用するパスワード。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。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。
データベース	Strong Authentication がアクセスするデータベースの名前。

a. ［次へ］ボタンをクリックして続行します。

b. 手順 8 に進みます。

- Oracle データベースの詳細情報

  a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
Primary ODBC DSN	インストーラによって、Strong Authentication 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	データベースにアクセスするために Strong Authentication が使用するユーザ名。 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	データベースにアクセスするために Strong Authentication が使用するパスワード。 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	Oracle の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参照する Oracle システムの識別子。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。
ホスト名	Oracle サーバが利用可能なコンピュータのホスト名または IP アドレス。 **構文**： <*サーバ名*> **例**： demodatabase

  b. ［Test Data Source］をクリックして、正常にデータベースに接続されているかどうかをテストします。

  c. テストが完了したら、［Next］をクリックして次に進みます。

- MySQL データベースの詳細情報

  a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
Primary ODBC DSN	インストーラによって、Strong Authentication 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。

フィールド	Description
サーバ	データベース サーバのホスト名または IP アドレス。SQL サーバが名前付きインスタンス モードで展開する場合は、さらに円記号「¥」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスする（SQL Server ではこれを*ログイン*といいます）ために、Strong Authentication が使用するユーザ名。 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	データベースにアクセスするために Strong Authentication が使用するパスワード。 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。
データベース	Strong Authentication がアクセスするデータベースの名前。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。

b. ［Test Data Source］をクリックして、正常にデータベースに接続されているかどうかをテストします。

c. テストが完了したら、［Next］をクリックして次に進みます。

d. 手順 8 に進みます。

［Encryption Configuration］画面が表示されます。この画面を使用して、暗号化モードを選択し、暗号化に使用される情報を設定します。

1. この画面で以下の情報を入力します。

   - **Master Key**： データベースに格納されたデータを暗号化するために使用されるマスタ キーを入力します。 デフォルトでは、マスタ キーの値は MasterKey に設定されます。 このキーは、*<install_location>*¥Arcot Systems¥conf にある securestore.enc ファイルに格納されます。

     インストール後にマスタ キーの値を変更する場合は、新しいマスタ キーの値を使用して securestore.enc ファイルを再生成します。詳細については、「CA Strong Authentication 管理ガイド」を参照してください。

   - **Configure HSM**： このオプションは、機密データを暗号化するためにハードウェア セキュリティ モジュール（HSM）を使用する場合のみ選択します。 選択しない場合、デフォルトでは、ソフトウェア モードがデータの暗号化に使用されます。

     注: 以下のオプションは、［Configure HSM］を選択した場合のみ有効になります。

   - **PIN**： HSM に接続するために使用されるパスワードを入力します。

   - **Choose Hardware Module**： 使用する予定の HSM を選択します。Strong Authentication がサポートする HSM は以下のとおりです。

     - Luna HSM
     - nCipher netHSM

   - **HSM Parameters**： 以下の HSM 情報を設定します。

     - **Shared Library**： HSM に対応する PKCS#11 共有ライブラリへの絶対パス。

       Luna （cryptoki.dll）および nCipher netHSM （cknfast.dll）の場合は、ファイルの絶対パスと名前を指定します。

     - **Storage Slot Number**： データの暗号化に使用される 3DES キーが存在する HSM スロット。 Luna のデフォルト値は 0 です。また、nCipher netHSM のデフォルト値は 1 です。

   注: ここで指定する HSM パラメータ値は、*<install_location>*¥Arcot Systems¥conf にある arcotcommon.ini ファイルに記録されます。インストール後にこれらの値を変更する場合は、付録「設定ファイルおよびオプション」の説明に従い、arcotcommon.ini ファイルを編集する必要があります。

2. ［次へ］をクリックして続行します。
3. ［インストール］をクリックします。

   ［Microsoft Visual C++ 2010 x86 Redistributable Setup］画面が表示されます。この画面は、Strong Authentication をインストールしている現在のシステムに Microsoft Visual C++ 2010 x86 がインストールされていない場合にのみ表示されます。
4. ［I have read and accept the license terms］オプションを選択して、［Install］をクリックします。

   ［Installation Progress］画面が表示されます。数秒間表示される場合があります。 しばらくすると、［Installation Is Complete］画面が表示されます。
5. ［Finish］をクリックして［Microsoft Visual C++ 2010 x86 Redistributable Setup］ダイアログ ボックスを閉じ、Strong Authentication のインストールを続けます。

   ［Installing Strong Authentication］画面が表示されます。 数分かかる場合があります。 しばらくすると、［Installation Complete］画面が表示されます。
6. ［Done］をクリックしてインストール ウィザードを終了します。

インストール後の作業

このセクションでは、Strong Authentication 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 Strong Authentication 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 セットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. CA Advanced Authentication へのログイン
7. システムのブートストラップ
8. Strong Authentication サーバの起動
9. インストールの確認
10. ユーザ データ サービスの展開
11. サンプル アプリケーションの展開
12. 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ら、「Strong Authentication Java SDK および Web サービスの設定」の章の説明に従って、Java SDK および Web サービスの設定を行います。

データベース スクリプトの実行

Strong Authentication には、Strong Authentication データベースでスキーマを作成して初期設定値を設定するデータベース スクリプトが付属しています。

次の手順に従ってください:

1. データベース タイプに対応するスクリプトが格納されたフォルダを見つけます。 デフォルトの場所は以下のとおりです。

   （Microsoft SQL Server の場合） <*install_location*>/arcot/dbscripts/mssql

   （Oracle データベースの場合）<*install_location*>/arcot/dbscripts/oracle

   （IBM DB2 UDB の場合） <*install_location*>/arcot/dbscripts/db2

   （MySQL の場合） <*install_location*>/arcot/dbscripts/mysql

2. データベース ベンダー ツールを使用して、*以下の順でスクリプト*を実行します。

   a. arcot-db-config-for-common-8.0.sql

      重要: Risk Authentication 8.0 をインストール済みの場合は、Risk Authentication 8.0 のインストール時にすでに実行しているため、arcot-db-config-for-common-8.0.sql を実行しないでください。

   b. arcot-db-config-for-webfort-8.0.sql

注: スクリプトの実行中にエラーが発生した場合は、必要な権限が付与されているかどうかをデータベース管理者に確認します。

データベースのセットアップの確認

データベース スクリプトを実行した後、arwfutil ツールを使用して、スキーマが正しくシードされていることを確認します。

次の手順に従ってください:

1. コマンド プロンプト ウィンドウを開きます。
2. 以下の場所に移動します。
   `<install_location>/arcot/sbin`
3. コマンド プロンプトで、以下のコマンドを入力します。
   `./arwfutil vdb`

   このコマンドにより、*<install_location>*/arcot/logs ディレクトリに arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルが作成されます。
4. テキスト エディタで arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルを開き、以下のタイプのエントリを確認します。
   `ARWF*  FOUND`

   これらの行は、データベース が正常にセットアップされたことを示します。
5. arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルを閉じます。

アプリケーション サーバを準備する方法

Strong Authentication のコンポーネントであるユーザ データ サービス（UDS）および CA Advanced Authentication は、Web ベースのコンポーネントであり、以下のアプリケーション サーバをサポートしています。

- Apache Tomcat
- IBM WebSphere アプリケーション サーバ
- Oracle WebLogic Server
- JBoss アプリケーション サーバ

UDS および CA Advanced Authentication WAR ファイルをアプリケーション サーバに展開する前に、Strong Authentication ファイルと JDBC JAR ファイルを、お使いのアプリケーション サーバ上の適切な場所にコピーします。

- 手順 1： Java ホームの設定
- 手順 2： アプリケーション サーバへのファイルのコピー
- 手順 3： アプリケーション サーバへの JDBC JAR のコピー
- 手順 4： （Oracle WebLogic 10.1 に必須） Enterprise Archive ファイルの作成

手順 1: Java ホームの設定

アプリケーション サーバに UDS および CA Advanced Authentication を展開する前に、JAVA_HOME 環境変数が設定されていることを確認します。Apache Tomcat の場合、JAVA_HOME を、使用している JDK に対応する Java ホーム ディレクトリに設定します。

また、PATH 環境変数に $JAVA_HOME/bin を含めます。含めなかった場合、CA Advanced Authentication およびその他の JDK 依存コンポーネントが起動しない可能性があります。

手順 2: アプリケーション サーバへのデータベース アクセス ファイルのコピー

UDS および CA Advanced Authentication では、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。

- libArcotAccessKeyProvider.so。以下の場所にあります。
  <install_location>/arcot/native/*<platform name>*/*<32bit-or-64bit>*/
- arcot-crypto-util.jar。以下の場所にあります。
  <install_location>/arcot/java/lib/
- これらのファイルを、Strong Authentication を展開したアプリケーション サーバにコピーする必要があります。

Apache Tomcat へのデータベース アクセス ファイルのコピー

次の手順に従ってください：

1. 以下のディレクトリに libArcotAccessKeyProvider.so ファイルをコピーします。
   - **RHEL の場合**： *<Apache Tomcat で使用する JAVA_HOME>*/jre/bin
2. arcot-crypto-util.jar ファイルを以下のディレクトリにコピーします。
   <Apache Tomcat で使用する JAVA_HOME>/jre/lib/ext
3. libArcotAccessKeyProvider.so ファイルがコピーされるディレクトリに LD_LIBRARY_PATH を設定しエクスポートします。
4. アプリケーション サーバを再起動します。

   注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

IBM WebSphere へのデータベース アクセス ファイルのコピー

次の手順に従ってください：

1. IBM WebSphere Administration Console にログインします。
2. ［**Environment**］をクリックしてから、［**Shared Libraries**］をクリックします。
   a. ［**Scope**］ドロップダウンから、有効な可視性範囲を選択します。スコープには、アプリケーションを展開するターゲット サーバ/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. **名前**を入力します（たとえば、**ArcotJNI**）。
   d. **クラスパス**を指定します。 このパスは、arcot-crypto-util.jar ファイルが存在し、ファイル名も含まれる場所を指している必要があります。 たとえば、<*install_location*>/arcot/java/lib/arcot-crypto-util.jar などです。
   e. JNI のライブラリ パスを入力します。 このパスは、libArcotAccessKeyProvider.so ファイルがある場所を指している必要があります。 たとえば、<*install_location*>/arcot/java/native/linux/<*32bit-or-64bit*> などです。
   f. ［**Apply**］をクリックします。

3. サーバ レベルのクラス ローダを設定します。

   a. ［Servers］-［Server Types］-［WebSphere Application Servers］に移動します。

   b. ［**Application Servers**］で、設定が行われたサーバの設定ページにアクセスします。

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

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

   e. 自動生成された**クラス ローダ ID** をクリックします。

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

   g. ［**Add**］をクリックし、この手順の前半で作成した共有ライブラリ（たとえば、ArcotJNI）を選択して、［**Apply**］をクリックします。

   h. 変更を保存します。

4. 以下のディレクトリに libArcotAccessKeyProvider.so ファイルをコピーします。

   - **RHEL の場合**： <*IBM WebSphere で使用する JAVA_HOME*>/jre/bin

5. アプリケーション サーバを再起動します。

   注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

Oracle WebLogic へのデータベース アクセス ファイルのコピー

次の手順に従ってください：

1. 以下のディレクトリに libArcotAccessKeyProvider.so をコピーします。
   - **RHEL の場合**： <*Oracle WebLogic インスタンスで使用する JAVA_HOME*>/jre/bin
2. libArcotAccessKeyProvider.so ファイルがコピーされるディレクトリに LD_LIBRARY_PATH を設定しエクスポートします。
3. arcot-crypto-util.jar を <*Oracle WebLogic インスタンスで使用する JAVA_HOME*>/jre/lib/ext ディレクトリにコピーします。
4. WebLogic Administration Console にログインします。
5. ［**Deployments**］に移動します。
6. ［**Lock and Edit**］オプションを有効にします。
7. ［**Install**］をクリックして、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。
8. ［**次へ**］をクリックします。

   ［Application Installation Assistant］画面が表示されます。
9. ［**次へ**］をクリックします。

   ［Summary］ページが表示されます。
10. ［**完了**］をクリックします。
11. 変更を有効にします。
12. アプリケーション サーバを再起動します。

    注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

JBoss へのデータベース アクセス ファイルのコピー

次の手順に従ってください:

1. 以下に対して libArcotAccessKeyProvider.so をコピーします。
   - RHEL の場合： *JBoss_JAVA_HOME*/jre/bin/

   ここで、*JBoss_JAVA_HOME* は、JBoss アプリケーション サーバ インスタンスによって使用される JAVA_HOME を表します。
2. *<JBOSS_HOME>¥modules¥advauth-admin-libs¥main¥* というフォルダ構造を作成し、<ARCOT_HOME>¥java¥lib から以下の JAR をこのフォルダにコピーします。
   - arcot-crypto-util.jar
   - bcprov-jdk15-146.jar
3. 同じフォルダ（<JBOSS_HOME>¥modules¥advauth-admin-libs¥main¥）内に *module.xml* という名前で、以下のコードを持つファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="advauth-admin-libs">
<resources>
<resource-root path="arcot-crypto-util.jar"/>
<resource-root path="bcprov-jdk15-146.jar"/>
</resources>
    <dependencies>
        <module name="javax.api"/>
    </dependencies>
                </module>
```

4. アプリケーション サーバを再起動します。

手順 3: アプリケーション サーバへの JDBC JAR のコピー

CA Advanced Authentication、UDS、およびサンプル アプリケーションは、Java 依存コンポーネントであり、データベースに接続するために JDBC JAR ファイルを使用します。 これらのファイルはアプリケーション サーバにコピーする必要があります。

注: 以下のセクションで説明されている手順に進む前に、JDBC JAR ファイルをダウンロード済みであることを確認します。サポートされる JDBC JAR ファイルの詳細については、「インストールの準備」を参照してください。

Apache Tomcat への JDBC JAR のコピー

次の手順に従ってください:

1. JDBC JAR ファイルをダウンロードした場所に移動します。
2. JDBC JAR ファイルをコピーして、以下のディレクトリに貼り付けます。
   - **Apace Tomcat 5.5.x の場合**： *<TOMCAT-HOME>*¥common¥lib
   - **Apace Tomcat 6.x および 7.x の場合**： *<TOMCAT-HOME>*¥lib

   または、JDBC JAR ファイルが含まれるパスを **Classpath** 環境変数に追加します。
3. Apache Tomcat を再起動します。

IBM WebSphere への JDBC JAR のコピー

次の手順に従ってください:

1. IBM WebSphere Administration Console にログインします。
2. ［**Environment**］をクリックしてから、［**Shared Libraries**］をクリックします。
   a. ［**Scope**］ドロップダウンから、有効な可視性範囲を選択します。スコープには、アプリケーションを展開するターゲット サーバ/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. **名前**を入力します（たとえば、**JDBCJAR**）。
   d. **クラスパス**を指定します。 このパスは、JDBC JAR ファイルが存在する場所で、ファイル名も含まれている必要があります。
   e. ［**Apply**］をクリックします。
3. サーバ レベルのクラス ローダを設定します。

   注: クラス ローダを作成するか、または「手順 2： アプリケーション サーバへのデータベース アクセス ファイルのコピー」の実行時に作成したクラス ローダを使用できます。
   a. ［Servers］-［Server Types］-［WebSphere Application Servers］に移動します。
   b. ［**Application Servers**］で、設定を行うサーバの設定ページにアクセスします。
   c. ［**Java and Process Management**］をクリックしてから、［**Class Loader**］をクリックします。
   d. ［**New**］をクリックします。 デフォルトの［**Classes loaded with parent class loader first**］を選択して、［**OK**］をクリックします。
   e. 自動生成された**クラス ローダ ID** をクリックします。
   f. クラス ローダの［**Configuration**］ページで、［**Shared Library References**］をクリックします。
   g. ［**Add**］をクリックし、［**JDBCJAR**］を選択して、［**Apply**］をクリックします。
   h. 変更を保存します。
4. IBM WebSphere を再起動します。

Oracle WebLogic への JDBC JAR のコピー

次の手順に従ってください:

注: Oracle データベースを使用している場合、Oracle WebLogic Server はデフォルトで Oracle データベースをサポートしているため、このセクションで説明されている手順を実行する必要はありません。

1. JDBC JAR ファイルを以下のディレクトリにコピーします。

   <*Oracle WebLogic インスタンスで使用する JAVA_HOME*>/jre/lib/ext

2. WebLogic Administration Console にログインします。
3. ［**Deployments**］に移動します。
4. ［**Lock and Edit**］オプションを有効にします。
5. ［**Install**］をクリックして、JDBC JAR ファイルが含まれるディレクトリに移動します。
6. ［**次へ**］をクリックします。

   ［Application Installation Assistant］画面が表示されます。
7. ［**次へ**］をクリックします。

   ［Summary］ページが表示されます。
8. ［**完了**］をクリックします。
9. 変更を有効にします。
10. Oracle WebLogic Server を再起動します。

JBoss への JDBC JAR のコピー

次の手順に従ってください:

1. 任意のソースから必要な JAR をダウンロードし、ダウンロードした場所に移動します。
2. このフォルダに *<JBOSS_HOME>¥modules¥advauth-jdbc-driver¥main¥* というフォルダ構造を作成し、そのフォルダに *JDBC Jar* ファイルをコピーします。
3. 同じフォルダ（*<JBOSS_HOME>¥modules¥advauth-jdbc-driver¥main¥*）内に *module.xml* という名前で、以下のコードを持つファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="advauth-jdbc-driver">
<resources>
<resource-root path="<JDBC Jar Name>"/>
</resources>
    <dependencies>
        <module name="javax.api"/>
<module name="javax.transaction.api"/>
    </dependencies>
</module>
```

   注: JDBC Jar ファイル名を指定しているタグで「<JDBC Jar Name>」を編集します。

   例： sqljdbc.jar

4. アプリケーション サーバを再起動します。

手順 4: Enterprise Archive ファイルの作成

Weblogic 10.1 で有効

Strong Authentication には、CA Advanced Authentication およびユーザ データ サービスを展開するための WAR ファイルが付属しています。これらのファイルの形式を EAR に変更して、その EAR ファイルを展開することができます。

以下の手順に従います。

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/common/bundlemanager ディレクトリに移動します。
3. 以下のコマンドを使用して bundlemanager ツールを実行し、EAR ファイルを作成します。

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

   注: 上記のコマンドの *<war_file_name>* は、CA Advanced Authentication の EAR ファイルを生成する場合は arcotadmin.war、UDS の EAR ファイルを生成する場合は arcotuds.war に置き換えます。

   このコマンドは <*install_location*>/arcot/Java/webapps に EAR ファイルを生成します。

CA Advanced Authentication の展開

注: WebSphere 7.0、8.0、および 8.5 に CA Advanced Authentication を展開する場合は、付録「*IBM WebSphere での CA Advanced Authentication の展開*」に記載されている手順を参照してください。

Strong Authentication CA Advanced Authentication 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から入手できます。
`<install_location>/arcot/java/webapps/`

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

次の手順に従ってください:

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。 詳細な手順については、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. アプリケーションが再起動されたことを確認します。

CA Advanced Authentication へのログイン

初めて CA Advanced Authentication にログインするときは、インストール時にデータベースで自動的に作成されたマスタ管理者の認証情報を使用します。

次の手順に従ってください:

1. 以下の URL を使用して、Web ブラウザ ウィンドウで CA Advanced Authentication を起動します。

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

   注: 上記の URL で指定するホストおよびポートの情報は、CA Advanced Authentication が展開されるアプリケーション サーバのものである必要があります。

2. デフォルトのマスタ管理者アカウントの認証情報を使用して、マスタ管理者として CA Advanced Authentication にログインします。認証情報は以下のとおりです。

   - ユーザ名 : **masteradmin**
   - パスワード : *master1234!*

システムをブートストラップする方法

CA Advanced Authentication を使用して Strong Authentication を管理できるようにするには、以下の手順を実行してシステムを初期化します。

- デフォルトのマスタ管理者パスワードの変更
- グローバル キー ラベルを指定する
- デフォルトの組織の認証メカニズムを指定する

*ブートストラップ*は、これらのセットアップ タスクについて説明するウィザード主導のプロセスです。 これらのタスクを実行したら、ほかの管理リンクが有効になります。

「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

CA Advanced Authentication を展開すると、デフォルトで組織が作成されます。 この組織は*デフォルトの組織*（**DEFAULTORG**）と呼ばれます。 単一の組織システムとして、デフォルトの組織は、何らかの組織を作成せずにそれ自身で使用できます。

ブートストラップ タスクの実行

MA（マスタ管理者）として初めて CA Advanced Authentication にログインすると、［ブートストラップ］ウィザード画面の［サマリ］画面が表示されます。

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. ［**開始**］をクリックします。

   ［パスワードの変更］画面が表示されます。

2. ［**古いパスワード**］、［**新規パスワード**］、［**パスワードの確認**］を指定し、［**次へ**］をクリックします。

   ［グローバル キー ラベルの設定］画面が表示されます。

3. **グローバル キー ラベル**を指定して、［**次へ**］をクリックします。

   Strong Authentication では、機密データに対してハードウェア ベースまたはソフトウェア ベースの暗号化を使用できます。ハードウェアの暗号化かソフトウェアの暗号化かに関係なく、ユーザおよび組織データの暗号化に*グローバル キー ラベル*が使用されます。

   ハードウェアの暗号化を使用している場合、このラベルは、HSM デバイスに格納されている実際の 3DES キーへの参照（ポインタ）としてのみ機能します。そのため、キー ラベルは HSM キー ラベルと一致する*必要があります*。 ただし、ソフトウェア ベースの暗号化の場合には、このラベルが、データベース内の実際のソフトウェア キーへの参照として機能します。

   重要: *ブートストラップ プロセスの完了後に、このキー ラベルを更新することはできません。*

   ［**暗号化ストレージ タイプ**］フィールドには、暗号化キーがデータベース（**ソフトウェア**）に格納されているか、または HSM（**ハードウェア**）に格納されているかが示されます。

   ［デフォルト組織の設定］画面が表示されます。

4. ［**デフォルト組織設定**］セクションで、デフォルトの組織の以下のパラメータを指定します。

   - **表示名**： 組織の名称。 この名前は、CA Advanced Authentication のほかのすべてのページおよびレポート上に表示されます。

- **管理者認証メカニズム**： デフォルトの組織に属する管理者の認証に使用されるメカニズム。 CA Advanced Authentication は、管理者がログインするための以下の 3 種類の認証方式をサポートしています。
  - **基本**

    このオプションを選択すると、CA Advanced Authentication 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。
  - **LDAP ユーザ パスワード**

    このオプションを選択すると、管理者はディレクトリ サービスに格納されているそれぞれの認証情報を使用して認証されます。

  注: このメカニズムを管理者の認証に使用する場合、「ユーザ データ サービスの展開」の説明に従い、UDS を展開する必要があります。
  - **Strong Authentication ユーザ パスワード**

    ユーザがここで［**Strong Authentication ユーザ パスワード**］オプションを選択すると、Strong Authentication サーバによって認証情報が発行されて認証されます。

  注: この実行方法の詳細については、「CA Strong Authentication 管理ガイド」を参照してください。

5. ［デフォルト組織の設定］画面の［**キー ラベル設定**］セクションで、以下を指定します。
   - **グローバル キーの使用**： デフォルトでは、このオプションが選択されています。上記の手順で指定したグローバル キー ラベルを無効にして、新たに暗号化ラベルを指定する場合は、このオプションを選択解除します。
   - **キー ラベル**： ［**グローバル キーの使用**］オプションを選択解除した場合は、デフォルトの組織に使用する新しいキー ラベルを指定します。
   - **暗号化ストレージ タイプ**： このフィールドには、暗号化キーがデータベース（**ソフトウェア**）に格納されているか、または HSM（**ハードウェア**）に格納されているかが示されます。
6. ［**終了**］をクリックして、ブートストラップ プロセスを完了します。

   ［終了］画面に示されるとおりに、CA Advanced Authentication の初期化が完了します。

7. ［**続行**］をクリックして、CA Advanced Authentication を使用するほかの設定に進みます。

Strong Authentication の起動

Strong Authentication サーバを起動するには、以下の手順に従います。

1. タスク バーで、［**スタート**］をクリックします。
2. ［**設定**］をクリックして、［**コントロール パネル**］-［**管理ツール**］-［**サービス**］の順にポイントします。
3. ［**Strong Authentication Service**］を選択します。
4. ［**開始**］をクリックします。

インストールの確認

以下の手順を実行することで、Strong Authentication サーバおよび Web アプリケーションが正常に起動していることを確認できます。

- ログ ファイルの使用
- arwfserver ユーティリティの使用
- ポートの確認

ログ ファイルの使用

Strong Authentication サーバが正常に起動したかどうかを確認するには、以下の手順に従います。

1. 以下の場所に移動します。
   `<install_location>¥Arcot Systems¥logs`
2. 任意のエディタで arcotwebfortstartup.log ファイルを開き、以下の行を見つけます。
   ```
   INSTANCE_VER.................................: [8.0]
   Strong Authentication Service READY
   ```
   これらの行は、Strong Authentication サーバが正常にインストールされていることを示しています。

注: ログ ファイルに FATAL および WARNING のメッセージが含まれていないことを確認します。

arwfserver ユーティリティの使用

arwfserver ツールを使用して、インストールした Strong Authentication のリリースを確認できます。 このツールの詳細については、「Strong Authentication 管理ガイド」を参照してください。

以下の手順に従います。

1. 以下の場所に移動します。
   `<install_location>¥Arcot Systems¥bin`
2. 以下のオプションを指定して arwfserver.exe を実行し、対話モードでツールを開始します。
   `arwfserver -i`
3. プロンプトで「version」と入力します。

   webfort-ver-<dd>-<mmm>-<yy>.txt ファイルが <*install_location*>¥Arcot Systems¥logs フォルダに作成されます。
4. このファイルを開き、以下の項目をチェックして、最新のリリースを使用していることを確認します。
   - bin セクションの Strong Authentication ライブラリ ファイルのバージョンが 8.0 である。
   - bin セクションの UDS ライブラリ ファイル（arwfuds.dll）のバージョンが 2.0.3 である。
5. ファイルを閉じます。

ポートの確認

Strong Authentication サーバがデフォルト ポートで各プロトコルをリスンしているかどうかを確認するには、以下の手順に従います。

1. 以下の場所に移動します。
   <install_location>¥Arcot Systems¥logs
2. 任意のエディタで arcotwebfortstartup.log ファイルを開いてプロトコル名を検索し、以下のスニペットに示されているように、それらが正しいポートをリスンしているかどうかを確認します。

```
PROTOCOLNAME : [Administration-WS]
PORTNO : 9745
PROTOCOLID : [Transaction-Native]
PORTNO : 9742
PROTOCOLID : [ServerManagement-WS]
PORTNO : 9743
PROTOCOLID : [Transaction-WS]
PORTNO : 9744
```

デフォルトのポートおよびプロトコルの詳細については、付録「デフォルトのポート番号および URL」を参照してください。

ユーザ データ サービスの展開

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

ユーザ データ サービス（UDS）を展開するには、ファイル arcotuds.war が必要です。 このファイルは以下から入手できます。
`<install_location>/arcot/java/webapps/`

次の手順に従ってください:

1. アプリケーション サーバの適切なディレクトリに arcotuds.war をインストールします。

   注: 展開手順は、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。 詳細な手順については、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. （**WebSphere のみ**）アプリケーション ファイルが更新されると、UDS クラスを再ロードするように設定します。

   a. ［Applications］-［Application Types］-［WebSphere Enterprise Applications］に移動し、［UDS settings］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**］をクリックします。

3. アプリケーション サーバを再起動します。

4. UDS が正しく開始したかどうかを確認するには、以下の手順に従います。

   a. 以下の場所に移動します。
   `<install_location>/arcot/logs`

   b. 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。
   `User Data Service (Version: 2.0.3) initialized successfully.`

   この行は、UDS が正常に展開されたことを示しています。

注: FATAL および ERROR メッセージがある場合は確認して解決します。予期しない状態に関する WARNING メッセージはすべて確認します。

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、Strong Authentication が正常にインストールおよび設定されていることを確認できます。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 Strong Authentication の ワークフロー
- Strong Authentication Java API を使用して実行できるタスク
- Strong Authentication とアプリケーションの統合

重要: サンプル アプリケーションを運用環境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お勧めします。

次の手順に従ってください:

1. 以下の場所からサンプル アプリケーションの war ファイルを展開します。
   `<install_location>/arcot/samples/java`
2. サンプル アプリケーションを開始します。
3. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/sample-application/

第 6 章: 分散システムに Strong Authentication を展開する方法

InstallAnywhere ウィザードを使用して、Strong Authentication コンポーネントをインストールします。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 Strong Authentication をインストールして設定する場合は、インストーラを実行する際に［*Custom*］オプションを使用してください。

以下の手順は、プロセスの概要です。

1. Strong Authentication インストーラを実行し、Strong Authentication サーバと CA Advanced Authentication 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、Web サービスも同じシステムにインストールできます。

   インストール手順については、「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ます。データベースが正常にセットアップ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 セットアップの確認」を参照してください。

3. アプリケーション サーバを準備して、CA Web コンポーネントが使用するファイルをコピーします。

   詳細については、「アプリケーション サーバの準備」を参照してください。

4. アプリケーション サーバに CA Advanced Authentication を展開して、展開を確認します。

   詳細については、「CA Advanced Authentication の展開」および「CA Advanced Authentication の確認」を参照してください。

5. マスタ管理者の認証情報を使用して CA Advanced Authentication にログインし、Strong Authentication を初期化します。

   詳細については、「CA Advanced Authentication へのログイン」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。

6. Strong Authentication サーバを起動し、サービスが正常に開始されていることを確認します。

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

7. アプリケーション サーバにユーザ データ サービスを展開して、展開を確認します。

   詳細については、「ユーザ データ サービスの展開」を参照してください。

8. 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。

9. 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 Strong Authentication 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**］オプションのみを選択して、インストールを続行します。

   詳細については、「サンプル アプリケーションの展開」、「サンプル アプリケーションの通信サーバの設定」、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。

10. （オプション）Strong Authentication 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します。

    詳細については、「Strong Authentication 管理ガイド」の付録「SSL の設定」を参照してください。

11. 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。

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）。
- インストーラを使用して Strong Authentication 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 Systems¥ およびそのサブディレクトリは手動でクリーンアップします。
- 既存の %ARCOT_HOME% のインスタンスがすでに含まれているシステム上でインストーラを実行する場合。
  - インストール ディレクトリを要求*されません*。
  - データベースのセットアップを要求*されません*。 インストーラは既存のデータベースを使用します。
  - 暗号化をセットアップするように要求*されません*。

1 つ目のシステムへのインストール

Strong Authentication をインストールするには、インストールに使用するユーザ アカウントが Administrators グループに属している*必要があります*。

分散シナリオでは、Strong Authentication サーバを 1 つ目のシステムに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。

次の手順に従ってください:

1. インストーラの Strong Authentication-<version_number>-Windows-Installer.exe をダブルクリックします。
2. ［**Next**］ボタンをクリックして次に進みます。

   ［License Agreement］画面が表示されます。

3. 使用許諾契約書に同意し、［**Next**］をクリックします。

   インストーラによって、ほかの CA 製品がコンピュータにインストールされているかどうかが確認されます。

   インストールされている既存の CA 製品が見つからなければ、インストール ディレクトリの入力を求めるプロンプトが表示されます。この場合、［Installation Location］画面が表示されます。

   インストールされている既存の CA 製品が検出された場合、インストール ディレクトリの入力を求めるプロンプトは表示されません。［Installation Location］画面： 既存の ARCOT_HOME がコンピュータ上にある場合は、［Previous Installation Detected］画面が表示されます。

4. インストーラによって指定されたデフォルト ディレクトリをそのまま使用するか、［**Choose**］をクリックして別のディレクトリに移動して指定します。

   ［**Next**］をクリックし、指定したディレクトリへのインストールを実行します。

   ［Installation Type］画面が表示されます。

5. コンポーネントを選択してインストールするために［*カスタム*］オプションを選択して、［**Next**］をクリックします。

   ［Component Selection］画面が表示されます。

6. 必要でないコンポーネントを選択解除します。デフォルトでは、すべてのコンポーネントがインストール用に選択されています。

   以下の表に、使用できるすべてのコンポーネントを示します。

[Component]	Description
Strong Authentication サーバ	このオプションは、SDK、CA Advanced Authentication、および Web サービスからの以下のリクエストを処理するコア処理エンジン（**Strong Authentication サーバ**）をインストールします。 ■ 認証情報発行の設定 ■ 認証情報認証の設定 ■ サーバの設定 また、このコンポーネントでは、以下の Web サービスにアクセスできます。 ■ **認証と許可 Web サービス** - ユーザを認証および許可するためのプログラミング インターフェースを提供します。 ■ **発行 SDK および Web サービス** - Strong Authentication データベース内のユーザ認証情報を作成、読み取り、更新するためのプログラミング インターフェースを提供します。 ■ **認証 Web サービス** - ユーザを認証するためのプログラミング インターフェースを提供します。 ■ **認証情報管理 Web サービス** - ユーザ認証情報の作成および管理用のプログラミング インターフェースを提供します。 ■ **管理 Web サービス** - Strong Authentication 管理コンソールで使用されるプログラミング インターフェースを提供します。 ■ **バルク操作 Web サービス**： OATH トークンをアップロードおよび取得するためのプログラミング インターフェースを提供します。

［Component］	Description
Java SDK および WS	このオプションは、Strong Authentication サーバに認証およびユーザ認証情報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（API および Web サービスの形式）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。 ■ **認証 Java SDK および Web サービス** - Strong Authentication サーバを使用して認証するためのプログラミング インターフェースを提供します。 ■ **認証情報管理 Java SDK および Web サービス** - ユーザ認証情報の作成および管理用のプログラミング インターフェースを提供します。 ■ **管理 Web サービス** - 設定を作成するためのプログラミング インターフェースを提供します。 ■ **バルク操作 Web サービス**： OATH トークンをアップロードおよび取得するためのプログラミング インターフェースを提供します。 これらのコンポーネントの設定の詳細については、「Strong Authentication Java SDK および Web サービスの設定」の章を参照してください。
サンプル アプリケーション	このオプションは、Java API の使用方法を示すための Web ベースのインターフェースを提供します。また、認証情報管理リクエストと認証リクエストを実行できます。
CA Advanced Authentication	このオプションは、Strong Authentication サーバおよび認証関連の設定を管理するための Web ベースのインターフェースを提供します。
ユーザ データ サービス	このオプションは、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する UDS をインストールします。

1. インストールするコンポーネントをすべて選択したら、［**Next**］をクリックします。

   ［Database Type］画面が表示されます。

2. データベース タイプを選択し、［**Next**］をクリックして次に進みます。

   選択したデータベースに応じて、対応する［*Database Details*］画面が表示されます。

   注: Strong Authentication では、Oracle Real Application Clusters （Oracle RAC）がサポートされています。 Oracle RAC を使用するには、この手順で Oracle データベースを選択し、「Oracle RAC 用の CA Strong Authentication の設定」の手順を実行します。

   選択したデータベースに応じて、以下のいずれかの手順を実行します。

- Microsoft SQL Server データベースの詳細情報

  a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
ODBC DSN	Strong Authentication サーバは、ODBC DSN を使用してデータベースに接続します。 推奨される入力値は *arcotdsn* です。インストーラはこの値を使用して DSN を作成します。
サーバ	データベース サーバのホスト名または IP アドレス。 SQL サーバが**名前付きインスタンス** モードで展開する場合は、さらに円記号「**¥**」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスする（SQL Server ではこれを *ログイン*といいます）ために使用するユーザ名。 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	ユーザ アカウントに関連付けられたパスワード。 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。
データベース	データベースの名前。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。

b. ［**Test Data Source**］をクリックして、正常にデータベースに接続されているかどうかをテストします。

c. テストが完了したら、［**Next**］をクリックして次に進みます。

d. 手順 10 に進みます。

- IBM DB2 （UDB）データベースの詳細情報

a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
ODBC DSN	Strong Authentication サーバは、ODBC DSN を使用してデータベースに接続します。 推奨される入力値は *arcotdsn* です。インストーラはこの値を使用して DSN を作成します。
サーバ	データベース サーバのホスト名または IP アドレス。データベースを**名前付きインスタンス** モードで展開する場合は、さらに円記号「¥」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスする（SQL Server ではこれを *ログイン*といいます）ために使用するユーザ名。 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	ユーザ アカウントに関連付けられたパスワード。 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。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。
データベース	Strong Authentication がアクセスするデータベースの名前。

b. ［**次へ**］をクリックして続行します。

c. 手順 10 に進みます。

- Oracle データベースの詳細情報

a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
ODBC DSN	Strong Authentication サーバは、ODBC DSN を使用して Strong Authentication データベースに接続します。推奨される入力値は *arcotdsn* です。インストーラはこの値を使用して DSN を作成します。
User Name	データベースにアクセスするために Strong Authentication が使用するユーザ名。 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	データベースにアクセスするために Strong Authentication が使用するパスワード。 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	Oracle の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参照する Oracle システムの識別子。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。
ホスト名	Oracle サーバが利用可能なコンピュータのホスト名または IP アドレス。 **構文**： <*ホスト名または IP アドレス*> **例**： demodatabase

b. ［**Test Data Source**］をクリックして、正常にデータベースに接続されているかどうかをテストします。

c. テストが完了したら、［**Next**］をクリックして次に進みます。

- MySQL データベースの詳細情報

a. 以下の表に記載されている必要な情報を入力します。

フィールド	Description
ODBC DSN	Strong Authentication サーバは、ODBC DSN を使用して Strong Authentication データベースに接続します。推奨される入力値は *arcotdsn* です。インストーラはこの値を使用して DSN を作成します。

フィールド	Description
サーバ	データベース サーバのホスト名または IP アドレス。 SQL サーバが**名前付きインスタンス** モードで展開する場合は、さらに円記号「¥」に続けてインスタンス名を入力する必要もあります。詳細については、ベンダーのマニュアルを参照してください。 デフォルト インスタンス **構文**： <*サーバ名*> **例**： demodatabase 名前付きインスタンス **構文**： <*サーバ名*>¥<*インスタンス名*> **例**： demodatabase¥instance1
User Name	データベースにアクセスする（SQL Server ではこれを*ログイン*といいます）ために、Strong Authentication が使用するユーザ名。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	データベースにアクセスするために Strong Authentication が使用するパスワード。 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。
データベース	Strong Authentication がアクセスするデータベースの名前。
Port Number	データベース サーバが受信リクエストを待ち受けるポート。

b. ［**Test Data Source**］をクリックして、正常にデータベースに接続されているかどうかをテストします。

c. テストが完了したら、［**Next**］をクリックして次に進みます。

d. 手順 10 に進みます。

［Encryption Configuration］画面が表示されます。この画面を使用して、暗号化モードを選択し、暗号化に使用される情報を設定します。

1. この画面で以下の情報を入力します。

   - **Master Key**： データベースに格納されたデータを暗号化するために使用されるマスタ キーを入力します。 デフォルトでは、マスタ キーの値は MasterKey に設定されます。 このキーは、*<install_location>*¥Arcot Systems¥conf にある securestore.enc ファイルに格納されます。

     インストール後にマスタ キーの値を変更する場合は、新しいマスタ キーの値を使用して securestore.enc ファイルを再生成する必要があります。詳細については、「Strong Authentication 管理ガイド」を参照してください。

   - **Configure HSM**： このオプションは、機密データを暗号化するためにハードウェア セキュリティ モジュール（HSM）を使用する場合のみ選択します。 選択しない場合、デフォルトのソフトウェア モードがデータの暗号化に使用されます。

     注: 以下のオプションは、［**Configure HSM**］を選択した場合のみ有効になります。

   - **PIN**： HSM に接続するために使用されるパスワードを入力します。

   - **Choose Hardware Module**： 使用する予定の HSM を選択します。 Strong Authentication がサポートする HSM は以下のとおりです。

     - Luna HSM
     - nCipher netHSM

   - **HSM Parameters**： 以下の HSM 情報を設定します。

     - **Shared Library**： HSM に対応する PKCS#11 共有ライブラリへの絶対パス。

       Luna （cryptoki.dll）および nCipher netHSM （cknfast.dll）の場合は、ファイルの絶対パスと名前を指定します。

- **Storage Slot Number**： データの暗号化に使用される 3DES キーが存在する HSM スロット。Luna のデフォルト値は 0 です。また、nCipher netHSM のデフォルト値は 1 です。

［**Next**］をクリックして続行します。

［Pre-Installation Summary］画面が表示されます。

2. インストール設定を変更する場合は、［**Previous**］ボタンをクリックします。変更の必要がない場合は、［**Install**］ボタンをクリックしてインストールを進めます。

   ［Microsoft Visual C++ 2010 x86 Redistributable Setup］画面が表示されます。 この画面は、Strong Authentication をインストールしている現在のシステムに Microsoft Visual C++ 2010 x86 がインストールされていない場合にのみ表示されます。

3. ［**I have read and accept the license terms**］オプションを選択して、［**Install**］をクリックします。

   ［Installation Progress］画面が表示されます。数秒間表示される場合があります。 しばらくすると、［Installation Is Complete］画面が表示されます。

4. ［完了］をクリックします。

5. ［**Done**］をクリックしてインストール ウィザードを終了します。

1 つ目のシステムでのインストール後のタスク

このセクションでは、以下のインストール後の手順について説明します。

1. データベース スクリプトの実行
2. データベース セットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. CA Advanced Authentication へのログイン
7. システムのブートストラップ
8. Strong Authentication サーバの起動
9. インストールの確認
10. ユーザ データ サービスの展開

注: これらのインストール後のタスクを完了したら、「Strong Authentication Java SDK および Web サービスの設定」の章の説明に従って、Java SDK および Web サービスの設定を行います。

データベース スキーマの作成

Strong Authentication には、Strong Authentication データベースでスキーマを作成して初期設定値を設定する SQL スクリプトが付属しています。

次の手順に従ってください:

1. データベース タイプに対応するスクリプトが格納されたフォルダを見つけます。 デフォルトの場所は以下のとおりです。

   （Microsoft SQL Server の場合） <*install_location*>/arcot/dbscripts/mssql

   （Oracle データベースの場合）<*install_location*>/arcot/dbscripts/oracle

   （IBM DB2 UDB の場合） <*install_location*>/arcot/dbscripts/db2

   （MySQL の場合） <*install_location*>/arcot/dbscripts/mysql

2. データベース ベンダー ツールを使用して、*以下の順でスクリプト*を実行します。

   a. arcot-db-config-for-common-8.0.sql

      重要: Risk Authentication 8.0 をインストール済みの場合は、Risk Authentication 8.0 のインストール時にすでに実行しているため、arcot-db-config-for-common-8.0.sql を実行しないでください。

   b. arcot-db-config-for-webfort-8.0.sql

注: スクリプトの実行中にエラーが発生した場合は、必要な権限を持っているかどうかを確認します。

データベースのセットアップの確認

必要なデータベース スクリプトを実行した後、arwfutil ツールを使用して、スキーマが正しくシードされていることを確認します

次の手順に従ってください:

1. コマンド プロンプト ウィンドウを開きます。
2. 以下の場所に移動します。
   `<install_location>/arcot/sbin`
3. コマンド プロンプトで、以下のコマンドを入力します。
   `./arwfutil vdb`

   このコマンドにより、*<install_location>*/arcot/logs ディレクトリに arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルが作成されます。
4. テキスト エディタで arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルを開き、以下のタイプのエントリを確認します。
   `ARWF*  FOUND`

   これらの行は、データベース が正常にセットアップされたことを示します。
5. arcotwebfort-vdb-*<dd>*-*<mmm>*-*<yy>*.txt ファイルを閉じます。

アプリケーション サーバを準備する方法

ユーザ データ サービス（UDS）および CA Advanced Authentication は、Web ベースのアプリケーションであり、以下のアプリケーション サーバをサポートしています。

- Apache Tomcat
- IBM WebSphere アプリケーション サーバ
- Oracle WebLogic Server
- JBoss アプリケーション サーバ

UDS および CA Advanced Authentication WAR ファイルをアプリケーション サーバに展開する前に、Strong Authentication ファイルと JDBC JAR ファイルを、お使いのアプリケーション サーバ上の適切な場所にコピーします。

- 手順 1： Java ホームの設定
- 手順 2： アプリケーション サーバへのデータベース アクセス ファイルのコピー
- 手順 3： アプリケーション サーバへの JDBC JAR のコピー
- 手順 4： （Oracle WebLogic 10.1 に必須） Enterprise Archive ファイルの作成

Java ホームの設定

選択したアプリケーション サーバに UDS および CA Advanced Authentication の WAR ファイルを展開する前に、JAVA_HOME 環境変数を設定していることを確認します。 Apache Tomcat の場合、JAVA_HOME を、使用している JDK に対応する Java ホーム ディレクトリに設定します。

また、PATH 環境変数に $JAVA_HOME/bin を含めます。含めなかった場合、CA Advanced Authentication およびその他の 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 サーバへのデータベース アクセス ファイルのコピー

UDS および CA Advanced Authentication では、データベースにアクセスするために以下のファイルを使用します。

- libArcotAccessKeyProvider.so。以下の場所にあります。
  <install_location>/arcot/native/*<platform name>*/*<32bit-or-64bit>*/
- arcot-crypto-util.jar。以下の場所にあります。
  <install_location>/arcot/java/lib/

これらのファイルを、Strong Authentication を展開したアプリケーション サーバ上の適切な場所にコピーする必要があります。

Tomcat

次の手順に従ってください:

1. 以下のディレクトリに libArcotAccessKeyProvider.so ファイルをコピーします。
   - **RHEL の場合**： *<Apache Tomcat で使用する JAVA_HOME>*/jre/bin
2. arcot-crypto-util.jar ファイルを *<Apache Tomcat で使用する JAVA_HOME>*/jre/lib/ext ディレクトリにコピーします。
3. libArcotAccessKeyProvider.so ファイルがコピーされるディレクトリに LD_LIBRARY_PATH を設定しエクスポートします。
4. アプリケーション サーバを再起動します。

   注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

IBM WebSphere

次の手順に従ってください:

1. WebSphere Administration Console にログインします。
2. ［Environment］をクリックしてから、［Shared Libraries］をクリックします。
   a. ［Scope］ドロップダウンから、有効な可視性範囲を選択します。スコープには、アプリケーションを展開するターゲット サーバ/ノードが含まれる必要があります。
   b. ［新規］をクリックします。
   c. 名前を入力します（たとえば、ArcotJNI）。
   d. クラスパスを指定します。 このパスは、arcot-crypto-util.jar ファイルが存在し、ファイル名も含まれる場所を指している必要があります。 たとえば、<install_location>/arcot/java/lib/arcot-crypto-util.jar などです。
   e. JNI のライブラリ パスを入力します。 このパスは、libArcotAccessKeyProvider.so ファイルがある場所を指している必要があります。 たとえば、*<install_location>*/arcot/java/native/linux/*<32bit-or-64bit>* ディレクトリなどです。
   f. ［適用］をクリックします。

3. サーバ レベルのクラス ローダを設定します。
   a. ［Servers］-［Server Types］-［WebSphere Application Servers］をクリックします。
   b. ［Application Servers］で、設定が行われたサーバの設定ページにアクセスします。
   c. ［Java and Process Management］をクリックしてから、［Class Loader］をクリックします。
   d. ［新規］をクリックします。 デフォルトの［Classes loaded with parent class loader first］を選択して、［OK］をクリックします。
   e. 自動生成されたクラス ローダ ID をクリックします。
   f. クラス ローダの［Configuration］ページで、［Shared Library References］をクリックします。
   g. ［Add］をクリックし、この手順の前半で作成した共有ライブラリ（たとえば、ArcotJNI）を選択して、［Apply］をクリックします。
   h. 変更を保存します。
4. 以下のディレクトリに libArcotAccessKeyProvider.so ファイルをコピーします。
   - **RHEL の場合**： *<IBM WebSphere で使用する JAVA_HOME>*/jre/bin
5. アプリケーション サーバを再起動します。

   注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

WebLogic

次の手順に従ってください:

1. 以下のディレクトリに libArcotAccessKeyProvider.so をコピーします。
   - **RHEL の場合**： <*Oracle WebLogic インスタンスで使用する JAVA_HOME*>/jre/bin
2. libArcotAccessKeyProvider.so ファイルがコピーされるディレクトリに LD_LIBRARY_PATH を設定しエクスポートします。
3. arcot-crypto-util.jar を <*Oracle WebLogic インスタンスで使用する JAVA_HOME*>/jre/lib/ext ディレクトリにコピーします。
4. WebLogic Administration Console にログインします。
5. ［**Deployments**］に移動します。
6. ［**Lock and Edit**］オプションを有効にします。
7. ［**Install**］をクリックして、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。
8. ［**次へ**］をクリックします。

   ［Application Installation Assistant］画面が表示されます。
9. ［**次へ**］をクリックします。

   ［Summary］ページが表示されます。
10. ［**完了**］をクリックします。
11. 変更を有効にします。
12. アプリケーション サーバを再起動します。

    注: 残りのインストール タスクの一環としてアプリケーション サーバの再起動が必要になります。アプリケーション サーバを再起動する回数を最小限に抑えるには、再起動を必要とする最後のタスクを実行した後に 1 回再起動します。

JBoss アプリケーション サーバ

次の手順に従ってください:

1. 以下に対して libArcotAccessKeyProvider.so をコピーします。
   - RHEL の場合： *JBoss_JAVA_HOME*/jre/bin/

   ここで、*JBoss_JAVA_HOME* は、JBoss アプリケーション サーバ インスタンスによって使用される JAVA_HOME を表します。
2. *<JBOSS_HOME>¥modules¥advauth-admin-libs¥main¥* というフォルダ構造を作成し、<ARCOT_HOME>¥java¥lib から以下の JAR をこのフォルダにコピーします。
   - arcot-crypto-util.jar
   - bcprov-jdk15-146.jar
3. 同じフォルダ（<JBOSS_HOME>¥modules¥advauth-admin-libs¥main¥）内に *module.xml* という名前で、以下のコードを持つファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="advauth-admin-libs">
<resources>
<resource-root path="arcot-crypto-util.jar"/>
<resource-root path="bcprov-jdk15-146.jar"/>
</resources>
    <dependencies>
        <module name="javax.api"/>
    </dependencies>
                </module>
```

アプリケーション サーバを再起動します。

アプリケーション サーバへの JDBC JAR のコピー

CA Advanced Authentication、UDS、サンプル アプリケーションは、Strong Authentication の Java 依存コンポーネントであり、データベースに接続するために JDBC JAR ファイルを必要とします。 これらのファイルはアプリケーション サーバにコピーします。

注: 以下のサブセクションで示されている手順を実行する前に、JDBC JAR をダウンロードしていることを確認してください。サポートされている JDBC JAR の詳細については、「インストールの準備」を参照してください。

以下のセクションでは、データベースに必要な JDBC JAR を以下のいずれかのアプリケーション サーバにコピーするための手順について説明します。

- Apache Tomcat
- IBM WebSphere
- Oracle WebLogic
- JBoss アプリケーション サーバ

Apache Tomcat

Apache Tomcat インストール ディレクトリに JDBC JAR ファイルをコピーする方法

1. JDBC JAR ファイルをダウンロードした場所に移動します。
2. JDBC JAR ファイルをコピーして、以下のディレクトリに貼り付けます。
   - **Apace Tomcat 5.5.x の場合**： *<TOMCAT-HOME>*¥common¥lib
   - **Apace Tomcat 6.x および 7.x の場合**： *<TOMCAT-HOME>*¥lib

   または、JDBC JAR ファイルが含まれるパスを **Classpath** 環境変数に追加します。
3. Apache Tomcat を再起動します。

IBM WebSphere

IBM WebSphere に JDBC JAR 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**］をクリックしてから、［**Shared Libraries**］をクリックします。

a. ［**Scope**］ドロップダウンから、有効な可視性範囲を選択します。スコープには、アプリケーションを展開するターゲット サーバ/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. **名前**を入力します（たとえば、**JDBCJAR**）。

d. **クラスパス**を指定します。 このパスは、JDBC JAR ファイルが存在する場所で、ファイル名も含まれている必要があります。

e. ［**Apply**］をクリックして、変更を保存します。

3. サーバ レベルのクラス ローダを設定します。

注: クラス ローダを作成するか、または「手順 2： アプリケーション サーバへのデータベース アクセス ファイルのコピー (P. 105)」の実行時に作成したものを使用できます。

a. ［Servers］-［Server Types］-［WebSphere Application Servers］に移動します。

b. ［**Application Servers**］で、設定を行うサーバの設定ページにアクセスします。

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

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

e. 自動生成された**クラス ローダ ID** をクリックします。

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

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

h. 変更を保存します。

4. IBM WebSphere を再起動します。

Oracle WebLogic

Oracle WebLogic Server に JDBC JAR ファイルをコピーする方法

注: Oracle データベースを使用している場合、Oracle WebLogic Server はデフォルトで Oracle データベースをサポートしているので、このセクションで説明されている設定を行う必要はありません。

1. JDBC JAR ファイルを以下のディレクトリにコピーします。
   <Oracle WebLogic インスタンスで使用する JAVA_HOME>/jre/lib/ext ディレクトリ。
2. WebLogic Administration Console にログインします。
3. ［**Deployments**］に移動します。
4. ［**Lock and Edit**］オプションを有効にします。
5. ［**Install**］をクリックして、JDBC JAR ファイルが含まれるディレクトリに移動します。
6. ［次へ］をクリックします。

   ［Application Installation Assistant］画面が表示されます。
7. ［次へ］をクリックします。

   ［Summary］ページが表示されます。
8. ［完了］をクリックします。
9. 変更を有効にします。
10. Oracle WebLogic Server を再起動します。

JBoss アプリケーション サーバ

次の手順に従ってください:

1. 任意のソースから必要な JAR をダウンロードし、ダウンロードした場所に移動します。
2. このフォルダに *<JBOSS_HOME>¥modules¥advauth-jdbc-driver¥main¥* というフォルダ構造を作成し、そのフォルダに *JDBC Jar* ファイルをコピーします。
3. 同じフォルダ（*<JBOSS_HOME>¥modules¥advauth-jdbc-driver¥main¥*）内に *module.xml* という名前で、以下のコードを持つファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="advauth-jdbc-driver">
<resources>
<resource-root path="<JDBC Jar Name>"/>
</resources>
    <dependencies>
        <module name="javax.api"/>
<module name="javax.transaction.api"/>
    </dependencies>
</module>
```

注: JDBC Jar ファイル名を指定しているタグで「<JDBC Jar Name>」を編集します。

例： sqljdbc.jar

アプリケーション サーバを再起動します。

手順 4: Enterprise Archive ファイルの作成

Weblogic 10.1 で有効

Strong Authentication には、CA Advanced Authentication およびユーザ データ サービスを展開するための WAR ファイルが付属しています。これらのファイルの形式を EAR に変更して、その EAR ファイルを展開することができます。

以下の手順に従います。

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/common/bundlemanager ディレクトリに移動します。
3. 以下のコマンドを使用して bundlemanager ツールを実行し、EAR ファイルを作成します。

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

   注: 上記のコマンドの *<war_file_name>* は、CA Advanced Authentication の EAR ファイルを生成する場合は arcotadmin.war、UDS の EAR ファイルを生成する場合は arcotuds.war に置き換えます。

   このコマンドは <*install_location*>/arcot/Java/webapps に EAR ファイルを生成します。

ユーザ データ サービスの展開

Strong Authentication は、リレーショナル データベースから、または LDAP サーバから直接ユーザ データにアクセスします。

ユーザ データ サービス（UDS）を使用するには、arcotuds.war ファイルを展開する必要があります。 このファイルは以下から入手できます。
`<install_location>/arcot/java/webapps/`

次の手順に従ってください:

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

   注: 展開手順は、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。 詳細な手順については、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 ファイルを展開します。

2. （**WebSphere のみ**）アプリケーション ファイルが更新されると、UDS クラスを再ロードするように設定します。

   a. ［Applications］-［Application Types］-［WebSphere Enterprise Applications］に移動し、［UDS Settings］画面にアクセスします。

   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**］をクリックします。

3. アプリケーション サーバを再起動します。

4. UDS が正しく開始したかどうかを確認するには、以下の手順に従います。

   a. 以下の場所に移動します。
   `<install_location>/arcot/logs`

   b. 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。
   `User Data Service (Version: 2.0.3) initialized successfully.`

   この行は、UDS が正常に展開されたことを示しています。

注: FATAL および ERROR メッセージがある場合は確認して解決します。予期しない状態に関する WARNING メッセージはすべて確認します。

追加のサーバに Strong Authentication を展開する方法

Strong Authentication サーバおよび CA Advanced Authentication をインストールした後に、分散システム展開での追加のシステムにその他のコンポーネントをインストールします。

1. Strong Authentication インストーラである Installer.bin ファイルを見つけます。
2. 以下のコマンドを使用して、インストーラを実行します。
   `sh Strong Authentication-version_number-<platform name>-Installer.bin`

   インストーラによりインストールの準備が開始されます。
3. ［Choose Product Features］画面が表示されるまで、「1 つ目のシステムへのインストール」で説明されている手順を実行します。
4. インストールするコンポーネントを選択します。
5. 手順 12 から手順 19 に従って、インストールを完了します。

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、Strong Authentication のインストールが成功していることを確認できます。 また、サンプル アプリケーションは以下の機能の例を示します。

- 一般的なワークフロー
- Java API を使用して実行できるタスク
- Strong Authentication とアプリケーションの統合

以下の手順に従います。

1. 以下の場所から Strong Authentication *version_number*-sample-application.war ファイルを展開します。
   `<install_location>/arcot/samples/java`
2. サンプル アプリケーションを開始します。
3. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/Strong Authentication-version_number-sample-application/

サンプル アプリケーションの通信サーバの設定

サンプル アプリケーションと Strong Authentication サーバを異なるシステムにインストールした場合は、通信設定を行う必要があります。

以下の手順に従います。

Web ブラウザ ウィンドウのサンプル アプリケーションにアクセスします。

1. ナビゲーション ウィンドウで、［**Setup**］-［**Server Connectivity**］をクリックして、［Strong Authentication Server Connectivity］ページを開きます。
2. 以下の表に示す接続パラメータの値を指定します。

   注: これらのパラメータを使用して作成した設定は、現在のセッションに対して有効です。 サンプル アプリケーションまたはアプリケーション サーバを再起動した場合は、再度これらの値を設定します。

フィールド	デフォルト値	Description
IP アドレス	localhost	Strong Authentication サーバが利用可能なシステムのホスト名または IP アドレス。

フィールド	デフォルト値	Description
ポート	9742	認証および発行サービスが利用可能なポート。
Maximum Active Connections	64	サンプル アプリケーションによってメンテナンスされたデータベース接続の最大数。

3. ［**Set Up**］をクリックして、接続を保存します。

第 7 章: サイレント モード インストールを実行する方法

Strong Authentication をインストールした後に、サイレント インストール方式を使用して、コンポーネントを再度インストールできます。 サイレント インストールでは、ユーザによる操作なしでインストールが完了します。

以下を入力します。

1. サイレント インストールのガイドラインを確認します。
2. Strong Authentication ホスト システムから Strong Authentication プロパティ ファイルをコピーします。
3. Strong Authentication のインストール メディアをプロパティ ファイルと同じ場所にコピーします。
4. Strong Authentication インストーラのプロパティ ファイルを変更します。
5. Strong Authentication インストーラを実行します。

サイレント モード インストールのガイドライン

サイレント インストールを開始する前に、以下のガイドラインを確認します。

- デフォルト プロパティ ファイルを変更する前に、バックアップします。
- パラメータ名、等号 (=) およびパラメータの値の間に、決して余分なスペースを追加しないでください。
- 変更後に、ファイルを保存します。

重要: サイレント インストールで使用される応答ファイルを生成するために、「-r」オプションを使用してインストーラの実行可能ファイルを実行しないでください。 最初のインストール時に作成されるデフォルト プロパティ ファイルのみを使用する必要があります。

デフォルト プロパティ ファイル

デフォルト プロパティ ファイル内のパラメータを変更するには、テキスト エディタを使用します。 デフォルト パラメータは、最初のインストール中に入力された情報を反映します。 デフォルト プロパティ ファイルには、機密情報と関連付けられているパラメータがあります。 たとえば、データベース パスワード、マスタ キー、および HSM の PIN に関連するパラメータなどです。 それらに適切な値を指定します。

Strong Authentication プロパティ ファイル

Strong Authentication プロパティ ファイルのデフォルトの名前および場所は以下のとおりです。

Name

installer.properties

場所

`strong_auth_home¥`

strong_auth_home

Strong Authentication の インストール パスを指定します。

Strong Authentication インストーラのプロパティ ファイルの変更

インストール変数を定義するには、Strong Authentication インストーラのプロパティ ファイルを変更します。

以下のデフォルト パラメータでは、Strong Authentication の最初のインストール時にユーザが入力した情報が指定されています。

CHOSEN_FEATURE_LIST

インストールされる機能のカンマ区切りリストを指定します。

有効な値は以下のとおりです。

WFSRV - Strong Authentication **サーバ**

Strong Authentication サーバ - 認証、プロビジョニング、設定およびサーバ インスタンスの管理、を行うサーバ

WFSDK - Strong Authentication Java SDK **および** WS

Strong Authentication サーバへの発行、認証、および設定のリクエストを有効にする Java SDK および Web サービス。

WFAPP - CA Strong Authentication **サンプル アプリケーション**

Java SDK の使用方法の例を示す Web ベースのアプリケーション。

ADMIN - **管理コンソール** - CA Advanced Authentication

サーバ設定を管理するための Web ベースのコンソール。

UDS - **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）などの、さまざまなタイプのユーザ リポジトリにアクセスするための抽象化層。

USER_INSTALL_DIR_SILENT

Strong Authentication のインストール場所を指定します。

ARCOT_DBTYPE_SILENT

設定されているデータベースのタイプを指定します。

有効な値： Oracle、Mssqlserver、db2、Mysql

プライマリ データベースの詳細

プライマリ データベースには、以下のデータベース関連の詳細があります。

ARCOT_CONFIG_PRIMARY_DB_SILENT

プライマリ データベースが設定されているかどうかを指定します。

有効な値： true、false

ARCOT_PRIMARY_DSN_NAME_SILENT

データベースのデータ ソース名を指定します。

ARCOT_PRIMARY_DATABASE_SILENT

データベース インスタンスの名前を指定します。

ARCOT_PRIMARY_SID_SILENT

Oracle データベースの SID を指定します。 その他のデータベース タイプでは、空白にままにします。

ARCOT_PRIMARY_TNS_SERVICE_NAME_SILENT

Oracle データベースの TNS サービス名を指定します。 その他のデータベース タイプでは、空白にままにします。

ARCOT_PRIMARY_HOST_NAME_SILENT

データベース サーバのホスト名を指定します。

ARCOT_PRIMARY_PORT_SILENT

指定したデータベース インスタンスのポート番号を指定します。

ARCOT_PRIMARY_USER_NAME_SILENT

データベース ユーザ名を指定します。

ARCOT_PRIMARY_PASSWORD_SILENT

指定したデータベース ユーザ名のパスワードを指定します。

ARCOT_CONFIG_BACKUP_DB_SILENT

バックアップ データベースが設定されているかどうかを指定します。

有効な値： true、false

バックアップ データベースの詳細

バックアップ データベースには、以下のデータベース関連の詳細があります。

ARCOT_BACKUP_DSN_NAME_SILENT

データベースのデータ ソース名を指定します。

ARCOT_BACKUP_DATABASE_SILENT

データベース インスタンスの名前を指定します。

ARCOT_BACKUP_SID_SILENT

Oracle データベースの SID を指定します。 その他のデータベース タイプでは、空白にままにします。

ARCOT_BACKUP_TNS_SERVICE_NAME_SILENT

Oracle データベースの TNS サービス名を指定します。 その他のデータベース タイプでは、空白にままにします。

ARCOT_BACKUP_HOST_NAME_SILENT

データベース サーバのホスト名を指定します。

ARCOT_BACKUP_PORT_SILENT

指定したデータベース インスタンスのポート番号を指定します。

ARCOT_BACKUP_USER_NAME_SILENT

データベース ユーザ名を指定します。

ARCOT_BACKUP_PASSWORD_SILENT

指定したデータベース ユーザ名のパスワードを指定します。

暗号化の詳細

データベースの暗号化の詳細を以下に示します。

暗号化方式： ソフトウェア/ハードウェア

ARCOT_ENC_TYPE_SILENT

暗号化の方式を指定します。

有効な値： software、nfast、chrysalis

ARCOT_ENC_DEVICE_NAME_SILENT

ハードウェア暗号化用のデバイス名を指定します。

ARCOT_KEY_LABEL_SILENT

マスタ キー ラベルを指定します。

ARCOT_HSM_PIN_SILENT

HSM のピン番号を指定します。

ARCOT_HSM_SHARED_LIBRARY_SILENT

HSM 共有ライブラリの完全パスを指定します。

ARCOT_HSM_STORAGE_SLOT_SILENT

HSM の「Storage Slot Number」を指定します。

サイレント インストールを実行する方法

無人インストールを実行し、ユーザによる操作なしで Strong Authentication をインストールします。

次の手順に従ってください：

1. 無人インストールのガイドラインを確認します。
2. Strong Authentication ホスト システムから Strong Authentication プロパティ ファイルをコピーします。
3. Strong Authentication のインストール メディアをプロパティ ファイルと同じ場所にコピーします。
4. Strong Authentication インストーラのプロパティ ファイルを変更します。
5. Strong Authentication インストーラを実行します。

   Strong Authentication のインストール実行可能ファイルおよびプロパティ ファイルをコピーしたディレクトリで、以下のコマンドを実行します。

   ```
   installation_media -f installer.properties -i silent
   ```

   Installation_media

   Strong Authentication のインストール実行可能ファイルを指定します。

   注: プロパティ ファイルがインストール メディアと同じディレクトリ内に存在しない場合は、その場所を指定します。 引数にスペースが含まれている場合は、二重引用符を使用します。

   -i silent

   インストーラがサイレントで実行されるように指定します。

   例：

   ```
   installation_media -f "C:¥Program Files¥CA¥Arcot Systems
   ¥installer.properties" -i silent
   ```

   インストールが始まります。 インストーラは、ユーザがプロパティ ファイルで指定したパラメータを使用して Strong Authentication をインストールします。
6. Strong Authentication のインストールを確認します。

第 8 章: Strong Authentication のアンインストール

この手順では、Strong Authentication および関連する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。

次の手順に従ってください:

1. 使用しているデータベース タイプに応じて、次のいずれかのフォルダに移動します。

   （MS SQL の場合） <*install_location*>¥Arcot Systems¥dbscripts¥mssql

   （Oracle の場合） <*install_location*>¥Arcot Systems¥dbscripts¥oracle

   （DB2 の場合） <*install_location*>¥Arcot Systems¥dbscripts¥db2

   （MySQL の場合） <*install_location*>¥Arcot Systems¥dbscripts¥mysql

2. スクリプトを*次に示す順序*で実行します。

   a. drop-webfort-8.0.sql

      注: （MySQL の場合） drop-webfort-8.0.sql の実行時には、「Safe Updates」が無効である必要があります。

   b. drop-arcot-common-8.0.sql

      これでデータベース テーブルがすべて削除されます。

3. Strong Authentication サーバを停止します。
4. 次の手順に従って DSN エントリを削除します。
   a. ［コントロール パネル］の［**管理ツール**］を開きます。
   b. ［**データ ソース (ODBC)**］を開きます。
   c. ［**システム DSN**］タブをクリックします。
   d. 目的の DSN を選択し、［**削除**］をクリックします。
5. sh <*install_directory*>/arcot/"Uninstall_CA Strong Authentication"/Uninstall CA Strong Authentication ディレクトリに移動します。
6. Uninstall Strong Authentication.exe ファイルをダブルクリックします。
7. 以下の*いずれか*のオプションを選択します。
   - コンポーネントをすべてアンインストールするには、［**Complete Uninstall**］を選択します。
   - 選択したコンポーネントをアンインストールするには、［**Uninstall Specific Features**］を選択し、［**Next**］をクリックして、［Choose Product Features］画面を表示します。
8. アンインストールするコンポーネントを選択し、［**Uninstall**］をクリックします。

   重要: **特定の機能をアンインストール**するには、インストール時に実行したのとは逆の順序で行う必要があります。 たとえば、Strong Authentication 認証サーバの後に CA Advanced Authentication をインストールした場合は、CA Advanced Authentication をアンインストールしてから認証サーバをアンインストールする必要があります。
9. アンインストールが正常に終了すると、最後に［Uninstallation Complete］画面が表示されます。［**Done**］をクリックしてインストール ウィザードを終了します。

アンインストール後の作業手順

アンインストール後には、以下の作業を実行します。

1. <install_location>¥Arcot Systems フォルダを削除します。
2. アプリケーション サーバから次の Web アプリケーションをアンインストールします。
   - arcotadmin - CA Advanced Authentication
   - arcotuds： ユーザ データ サービス
   - webfort-7.1.01-sample-application： サンプル アプリケーション
3. Zero G Registry フォルダが削除されていることを確認します。 この隠しフォルダはインストール時に %ARCOT_HOME% フォルダにコピーされます。

注: 分散システムに展開している場合は、該当するアプリケーションを展開したシステムでこれらのファイルを探してください。

第 9 章: クライアント システムの UTF-8 サポートの設定

データベースと通信する Strong Authentication コンポーネントをインストールするシステムで、UTF-8 サポートを有効にします。たとえば、Strong Authentication サーバ、CA Advanced Authentication、およびユーザ データ サービスなどです。このセクションでは、その手順について説明します。

UNIX プラットフォームで UTF-8 サポートを有効にするには、以下の環境変数を設定します。

- NLS_LANG=en_US.UTF-8
- LC_CTYPE=en_US.UTF-8

付録 A: HSM 設定の変更

この付録では、インストール時に指定したハードウェア セキュリティ モジュール（HSM）の設定を変更する場合に実行する必要がある手順を示します。

注: このセクションで説明されている設定を行う前に、HSM サーバおよびクライアントをセットアップしていて、HSM 内に 3DES キーを生成していることを確認します。 詳細については、「（オプション、HSM を使用している場合のみ） HSM の要件」を参照してください。

「ハードウェア セキュリティ モジュール（HSM）の要件」で説明されているように、Strong Authentication はデータを保護するためにハードウェア セキュリティ モジュール（HSM）をサポートするようになりました。 HSM を使用してデータを暗号化する場合、データベースに保存されているデータは HSM にあるキーを使用して暗号化されます。

Strong Authentication はハードウェアを使用したデータの暗号化のために、Luna および nCipher netHSM をサポートしています。 HSM の設定は arcotcommon.ini ファイルで行うことができます。 このファイルには、必要な HSM を設定するための個別のセクションがあります。現在のリリースでは以下のとおりです。

- Luna HSM （[crypto/pkcs11modules/chrysalis]）
- nCipher netHSM （[crypto/pkcs11modules/nfast]）

設定している HSM に基づいて、対応するセクションで sharedLibrary パラメータを指定します。 HSM 情報を指定したら、HSM キー ラベルを使用して securestore.enc ファイルを再作成し、HSM を初期化して、HSM キーを使用するように Strong Authentication を初期化します。

Strong Authentication が必要とする HSM 情報を変更する方法

1. 以下の場所に移動します。
   <*install_location*>¥Arcot System¥conf
2. securestore.enc のバックアップをとります。
3. <*install_location*>¥Arcot System¥conf から既存の securestore.enc ファイルを削除します。
4. Strong Authentication が必要とする HSM 情報を変更する方法
   a. 以下の場所に移動します。
      <*install_location*>¥Arcot System¥conf
   b. テキスト エディタで arcotcommon.ini を開きます。
   c. [arcot/crypto/device] セクションの HSMDevice パラメータが使用する HSM に設定されていることを確認します。
      - Luna HSM の場合は chrysalis。

      または

      - nCipher netHSM の場合は nfast。
   d. 設定する HSM に応じて、sharedLibrary パラメータを HSM ライブラリ ファイルがある場所に設定します。

      Luna （cryptoki.dll）および nCipher netHSM （cknfast.dll）の場合は、ファイルの絶対パスと名前を指定します。

      注: このセクションで使用可能なその他の HSM 設定パラメータの詳細については、「arcotcommon.ini」を参照してください。
   e. arcotcommon.ini ファイルを保存して閉じます。
5. DBUtil ツールがある以下の場所に移動します。
   <*install_location*>¥Arcot Systems¥tools¥win
6. 以下のコマンドを使用して DBUtil ツールを実行します。
   a. dbutil -init <*HSM_key_label*>

      注: <*HSM_key_label*> は、HSM に存在する 3DES キーに対応します。

      上記のコマンドは指定したキー ラベルで securestore.enc ファイルを作成します。 生成されたファイルは、<*install_location*>¥Arcot System¥conf に保存されます。
   b. dbutil -i <*HSM_module_name*> <*HSM_password*>

      注: <*HSM_module_name*> は、 Luna HSM の場合は chrysalis、nCipher netHSM の場合は nfast です。

上記のコマンドは HSM を初期化します。

c. dbutil -pi *<DSN_Name>* *<Database_password>* -h *<HSM_password>* -d *<HSM_module_name>*

注: *<DSN_NAME>* は、Strong Authentication データベースに接続するために Strong Authentication サーバが使用する ODBC DSN を指します。 *<Database_password>* は、データベースに接続するために使用されるパスワードを指します。

上記のコマンドは、HSM を使用して暗号化されるように Strong Authentication サーバ データを初期化します。

d. dbutil -pi *<Database_Username>* *<Database_password>* -h *<HSM_password>* -d *<HSM_module_name>*

注: *<Database_Username>* は、Strong Authentication データベースに接続するために使用されるユーザ名を指します。 データベースユーザ名は大文字と小文字が区別されるため、正しい値を入力する必要があります。 *<Database_password>* は、データベースに接続するために使用されるパスワードを指します。

上記のコマンドは、HSM を使用して暗号化されるように、CA Advanced Authentication およびユーザ データ サービス データを初期化します。

第 10 章: Java 依存コンポーネントの要件

CA Advanced Authentication、Strong Authentication 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 の新規インストールを実行する場合は、JAVA_HOME 環境変数を設定します。path 変数は $JAVA_HOME/**bin/** を参照している必要があります。 また、アプリケーション サーバが同じ JAVA_HOME を使用することを確認します。 そうなっていない場合、CA Advanced Authentication およびその他の JDK 依存コンポーネントが起動しない可能性があります。

- Application Server
- UDS

第 11 章: HSM の要件

HSM を使用して暗号化キーを格納する場合は、以下を設定してから先に進みます。

1. HSM Server
2. HSM クライアント
3. HSM の少なくとも 1 つの 3DES キー

   重要: データベース内の情報を暗号化する際に使用されるこれらの 3DES キーのラベルを書き留めておいてください。

HSM サーバおよびクライアント コンポーネントのインストールと設定、および必要なキーの生成方法の詳細については、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。

第 12 章: Oracle RAC 用の Strong Authentication の 設定

このセクションの手順は、Strong Authentication で Oracle RAC を使用する場合にのみ実行します。

データベース スクリプトの変更

データベース スクリプトは、Strong Authentication インストール手順のインストール後のタスクとして実行します。 このスクリプトを実行する前に、Oracle RAC に対して変更します。

以下の手順に従います。

1. Oracle RAC の共有データ ファイル パスを確認するには、データベースにログインし、以下のコマンドを実行します。

   ```
   SELECT file_name, tablespace_name FROM dba_data_files
   ```

   このコマンドのサンプル出力を以下に示します。

   ```
   +DATA/qadb/datafile/users.259.797224649      USERS
   +DATA/qadb/datafile/undotbs1.258.797224649   UNDOTBS1
   +DATA/qadb/datafile/sysaux.257.797224647     SYSAUX
   ```

2. arcot-db-config-for-common-8.0.sql ファイルを開きます。 このファイルは、install_location/arcot/dbscripts/oracle/ ディレクトリにあります。

3. ファイル内で以下の行を見つけます。

   ```
   filename varchar2(50) := 'tabspace_arreports_'|| to_char(current_timestamp,
   'YYYY-MM-DD-HH24-MI-SS') || '.dat';
   ```

4. その行を以下の行に置き換えます。

   ```
   filename varchar2(100) :=
   '+shared_location/service_name/datafile/tabspace_arreports_'||
   to_char(current_timestamp, 'YYYY-MM-DD-HH24-MI-SS') || '.dat';
   ```

   新しい行で以下を行います。

   - shared_location を、最初の手順で指定されたコマンドの実行により確認した共有データ ファイル パスに置き換えます。
   - service_name を、Oracle RAC インストールのサービス名に置き換えます。

   以下は変更後の行の例です。

   ```
   filename varchar2(100) := '+DATA/forwardinc/datafile/tabspace_arreports_'||
   to_char(current_timestamp, 'YYYY-MM-DD-HH24-MI-SS') || '.dat';
   ```

5. スクリプト ファイルを保存して閉じ、実行します。

JDBC URL の設定

arcotcommon.ini ファイルで、Oracle RAC でサポートされている形式で JDBC URL を指定します。

以下の手順に従います。

1. テキスト エディタで arcotcommon.ini ファイルを開きます。 このファイルは install_location/arcot/conf/ ディレクトリにあります。
2. URL パラメータの値を、INI ファイルの [arcot/db/primarydb] セクションに指定し、必要に応じて [arcot/db/backupdb] セクションにも指定します。 URL を以下の形式で入力します。

   ```
   URL.1=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host_name)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=service_name)(SERVER=DEDICATED)))
   ```

   例：

   ```
   URL.1=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=172.30.250.18)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=forwardinc)(SERVER=DEDICATED)))
   ```

   注: Oracle RAC が設定されたクライアントである場合は、すべてのノードをこの形式で含めます。
3. Strong Authentication インストーラの実行中に指定したデータベース ユーザが、Oracle RAC のデータベース ユーザと異なる場合は、以下の手順を実行します。
   a. arcotcommon.ini ファイル内のデータベース ユーザ認証情報を変更します。
   b. DBUtil を使用して、securestore.enc ファイル内のデータベース ユーザ認証情報を変更します。 DBUtil は、ARCOT_HOME/tools/<*platform_name*> ディレクトリにあります。 DBUtil の使用方法については、「securestore.enc ファイルの更新およびトラスト ストア パスワードの設定」を参照してください。
4. arcotcommon.ini ファイルを保存して閉じます。

odbc.ini ファイルの更新

odbc.ini ファイルには接続パラメータが含まれます。 Oracle RAC の場合、Oracle RAC インストールに関連する値を odbc.ini ファイルに指定する必要があります。

以下の手順に従います。

1. Strong Authentication をインストールしたシステムで *.ora ファイルを作成します。 たとえば、/var/opt/tns.ora です。
2. ファイルに以下の行を入力します。

```
section_name =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = host_name_or_IP_address)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = service_name)
    )
  )
```

例：

```
fwdincrac =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 172.30.250.18)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = forwardinc)
    )
  )
```

注: Oracle RAC が設定されたクライアントである場合は、すべてのノードをこの形式で含めます。

3. ファイルを保存します。
4. *ARCOT_HOME*/odbc32v60wf/odbc.ini ファイルをテキスト エディタで開きます。
5. 必要な DSN セクションについて、以下のパラメータが含まれる行をコメントアウトします。
   - HostName
   - PortNumber
   - SID

例：

```
#HostName=172.30.251.251
#PortNumber=1521
#SID=an
```

6. 以下のパラメータを追加します。

```
TNSNamesFile=ARCOT_HOME/ora_file_name
ServerName=section_name
```

例：

```
TNSNamesFile=/var/opt/tns.ora
ServerName=fwdincrac
```

7. ファイルを保存して閉じます。

付録 B: CA Adapter 2.2.7 用の追加設定

Strong Authentication を Adapter 2.2.7 インスタンスと統合するには、追加の設定を実行する必要があります。 このセクションの手順は、Strong Authentication コンポーネントがすべてインストールされ、正しく実行されていることを確認した後にのみ実行します。

このセクションには、以下のトピックが含まれています。

CA Adapter 2.2.7 インスタンスの更新

Strong Authentication には、Arcot-Adpater-2.2.7-Compatibility-Package.zip ファイルが含まれています。このファイルの内容を既存の Adapter インストール環境にコピーします。

以下の手順に従います。

1. Strong Authentication-Adpater-2.2.7-Compatibility-Package.zip ファイルの内容を一時的な場所に抽出します。

   以下にそのファイル構造を示します。

```
arcotsm
    WEB-INF
        lib
            arcot-common.jar
            log4j-1.2.15.jar

arcotafm
    クライアント（client）
        arcotjsclient_jso.js
      vpn
             controller_vpn.jsp
WEB-INF
        クラス
            jspStrings_en.properties
dbscripts
    mssql
        arcot-db-config-for-adapter-statemanager.sql
        drop-adapter-statemanager.sql
    oracle
        arcot-db-config-for-adapter-statemanager.sql
        drop-adapter-statemanager.sql
```

2. State Manager を以下のように更新します。
   a. State Manager 2.2.7 を展開したアプリケーション サーバ上の場所に移動し、arcot-common-1.0.9.jar ファイルを削除します。

      たとえば、Apache Tomcat の場合、この場所は *TOMCAT_HOME*¥arcotsm¥WEB-INF¥lib です。

   b. 解凍されたファイル構造から、arcot-common.jar ファイルと log4j-1.2.15.jar ファイルをこの場所にコピーします。

   c. アプリケーション サーバを再起動します。
3. 以下のように Authentication Flow Manager を更新します。
   a. 解凍されたファイル構造から、arcotjsclient_jso.js ファイルを、Authentication Flow Manager 2.2.7 を展開したアプリケーション サーバ上の arcotafm¥client フォルダにコピーします。

      たとえば、Apache Tomcat の場合、この場所は *TOMCAT_HOME*/arcotafm/client です。

   b. 解凍されたファイル構造から、jspStrings_en.properties ファイルを、Authentication Flow Manager 2.2.7 を展開したアプリケーション サーバ上の arcotafm¥WEB-INF¥classes フォルダにコピーします。たとえば、Apache Tomcat の場合、この場所は *TOMCAT_HOME*/arcotafm/WEB-INF/classes です。
4. データベース スキーマで以下の手順に従います。
   a. State Manager と Strong Authentication のインスタンスが異なるデータベースを使用している場合は、State Manager によって使用されるデータベース内の ARCMNDBERRORCODES テーブルをドロップします。

   b. ARCMNDBERRORCODES テーブルを作成して行を挿入するスクリプトの一部を実行します。

LDAP プラグイン登録

このセクションの手順は、以下のシナリオの場合のみ実行します。

- Strong Authentication の新規インストールを実行し、Adapter 2.2.7 と共に使用する。
- バージョン 6.2.x から 7.x にアップグレードしたが、LDAP プラグインを登録せず、その後にアップグレードした。
- バージョン 6.2.x から 7.1.01 にアップグレードしたが、以前のリリースでは LDAP プラグインを登録していなかった。

CA Adapter 2.2.7 は、Strong Authentication を使用した LDAP 認証を有効にするためにプラグインを使用します。 Adapter 2.2.7 で使用される LDAP プラグインが Strong Authentication で動作するようにするには、LDAP プラグインを登録する必要があります。

LDAP プラグインの登録

CA Advanced Authentication を使用して、LDAP プラグインを登録します。

以下の手順に従います。

1. マスタ管理者として CA Advanced Authentication にログインします。
2. ［サービスおよびサーバの設定］タブをクリックします。
3. Strong Authentication サブタブをクリックし、左ペインで［拡張設定］の下の［プラグイン登録］を選択します。

   右ペインに［プラグインの登録］画面が表示されます。
4. 以下のフィールドに適切な値を指定します。
   - 名前： プラグインの名前。
   - ハンドラ パス： arwfldapauthplugin.dll
   - 設定テンプレート： ファイル システム内のファイル ldapauthplugin-config.xml へのパスを選択します。 通常、このファイルは *Install_Location*/arcot/samples/xml/webfort ディレクトリにあります。
   - UP_AUTH を［利用可能なイベント］リストから［サポート対象イベント］リストに移動させます。
5. ［登録］ボタンをクリックします。

組織用のプラグインの設定

登録済みのプラグインは、別の組織用に設定することができます。

以下の手順に従います。

1. グローバル管理者として CA Advanced Authentication にログインします。
2. ［組織］タブをクリックし、プラグインを使用する組織を検索します。

   注: ここで選択する組織は、AFM ウィザードで LDAP にマップする必要があります。

   組織の情報画面が表示されます。
3. Strong Authentication の設定サブタブをクリックし、左ペインで［拡張設定］の下の［プラグイン設定］を選択します。

   ［プラグインの設定］画面が表示されます。
4. ［名前］リストから、登録済みの LDAP 認証プラグインを選択します。
5. UP_AUTH を、［サポート対象イベント］リストから［選択したイベント］リストに移動させます。
6. ［サブミット］をクリックします。

   プラグインが正常に設定されたことを示すメッセージが表示されます。

付録 C: IBM WebSphere への管理コンソールの展開

IBM WebSphere 7.0、8.0、および 8.5 に CA Advanced Authentication を展開するには、以下の手順に従います。

1. 作業ディレクトリを、次のディレクトリに変更します。
   `<install_location>/arcot/sbin`
2. 「source arwfenv」と入力し、**Enter** キーを押して $ARCOT_HOME 環境変数を設定します。
3. 変更を有効にするために、アプリケーション サーバを再起動します。
4. CA Advanced Authentication の WAR ファイルがある以下の場所に移動します。
   `<install_location>/arcot/java/webapps`
5. arcotadmin.war ファイルを一時ディレクトリにコピーします。 たとえば、opt/arcot_temp などです。
6. arcotadmin.war ファイルの内容を抽出します。

   /opt/arcot_temp/WEB_INF/lib ディレクトリに抽出される JAR のうち、以下の JAR が IBM WebSphere で共有ライブラリを作成するために使用されます。

   - axiom-api-1.2.10.jar
   - axiom-impl-1.2.10.jar
   - axis2-java2wsdl-1.5.2.jar
   - backport-util-concurrent-3.1.jar
   - commons-httpclient-3.1.jar
   - commons-pool-1.5.5.jar
   - axiom-dom-1.2.10.jar

- axis2-adb-1.5.2.jar
- axis2-kernel-1.5.2.jar
- commons-codec-1.3.jar
- commons-logging-1.1.1.jar
- log4j-1.2.16.jar
- axis2-transport-http-1.5.2.jar
- axis2-transport-local-1.5.2.jar

7. IBM WebSphere Administration Console にログインします。
8. ［Environment］をクリックしてから、［Shared Libraries］をクリックします。
   a. ［Scope］ドロップダウンから、有効な可視性範囲を選択します。スコープには、アプリケーションを展開するターゲット サーバ/ノードが含まれる必要があります。
   b. ［新規］をクリックします。
   c. 名前を入力します（たとえば、ArcotAdminSharedLibrary）。
   d. クラスパスを指定します。 手順 3 で抽出したすべての JAR ファイルのパスとファイル名を入力します。

      例： /opt/arcot_temp/WEB_INF/lib/axiom-api-1.2.10.jar

   e. ［Apply］をクリックして、変更を保存します。
9. CA Advanced Authentication の WAR ファイルがある以下の場所に移動します。
   `<install_location>/arcot/java/webapps`
10. アプリケーション サーバに arcotadmin.war を展開します。

11. 以下の手順に従って、共有ライブラリを設定します。
    a. ［Applications］-［Application Types］-［WebSphere Enterprise Applications］をクリックします。
    b. ［arcotadmin_war］をクリックします。
    c. ［References］セクションで、［Shared library references］をクリックします。
    d. ［arcotadmin_war］を選択し、［Reference shared libraries］をクリックします。
    e. ［Available］リストから［ArcotAdminSharedLibrary］を選択し、［Selected］リストに移動させます。
    f. ［OK］をクリックして設定を保存します。
12. 以下の手順に従って、クラス ローダの順序およびポリシーを設定します。
    a. ［Applications］-［Application Types］-［WebSphere enterprise applications］をクリックします。
    b. ［arcotadmin_war］をクリックします。
    c. ［Class loading and update detection］リンクをクリックします。
    d. ［Class loader order］セクションで、［Classes loaded with local class loader first (parent last)］オプションを選択します。
    e. ［WAR class loader policy］セクションで、［Single class loader for application］オプションを選択します。
    f. ［OK］をクリックして設定を保存します。
13. アプリケーションが再起動されたことを確認します。

付録 D: Strong Authentication の問題のトラブルシューティング

この付録では、Strong Authentication の使用時に発生する可能性があるエラーを解決するのに役立つトラブルシューティング手順について説明します。 トラブルシューティング トピックは、Strong Authentication の各コンポーネントに基づき以下のように分類されます。

- インストール エラー
- Database-Related エラー
- Strong Authentication サーバ エラー

トラブルシューティング タスクを実行する前に、ログ ファイルでエラーがあるかどうかを確認してください。 デフォルトでは、ログ ファイルはすべて *<install_location>*¥Arcot Systems¥logs¥ ディレクトリに保存されます。以下の表に、コンポーネントのデフォルト ログ ファイル名を示します。

コンポーネント名	ファイル名	Description
Strong Authentication サーバ	arcotwebfortstartup.log	このファイルには、すべての起動 (ブート) アクションが記録されます。 Strong Authentication サービスが起動しない場合、問題の原因を特定するためにこのファイルの情報が役立ちます。
	arcotwebfort.log	このファイルには、サーバで処理されたすべてのリクエストが記録されます。
CA Advanced Authentication	arcotadmin.log	このファイルには、CA Advanced Authentication の操作が記録されます。
ユーザ データ サービス	arcotuds.log	このファイルには、ユーザ データ サービスの操作が記録されます。

インストール エラー

問題:

Strong Authentication がインストールされているサーバで IE ブラウザを使用して CA Auth ID をダウンロードすると、以下のエラーが表示されます。
`Your security settings have blocked an application signed with an expired or not-yet-valid certificate from running.`

解決方法:

コントロール パネルに移動し、［Java］をクリックして Java 設定を変更します。［セキュリティ］オプションを（［高］ではなく）［中］に指定します。デフォルト オプションは例外を指定する［高］です。その後、IE、Firefox、または Chrome で「Arcot アプレット クライアント」と「Arcot Flash クライアント」を使用して CA Auth ID をダウンロードします。

問題:

Strong Authentication がインストールされているサーバで Chrome ブラウザを使用して CA Auth ID をダウンロードすると、以下のエラーが表示されます。
`Permanent storage in the Flash player is disabled.`

解決方法:

「Arcot Flash クライアント」を使用してダウンロードするために HTTP ではなく HTTPS を有効にします。その後、IE、Firefox、または Chrome で CA Auth ID をダウンロードします。

問題:

<install_location>¥Arcot Systems¥java¥webapps ディレクトリに arcotadmin.war がありません。

原因

インストール時にファイルが作成されていない可能性があります。

解決方法:

arcotadmin.war ファイルを作成するには、以下の手順に従います。

1. コマンド ウィンドウを開きます。
2. ARCOT_HOME 環境変数が設定されていることを確認します。
3. *<install_location>*¥Arcot Systems¥tools¥common¥bundlemanger ディレクトリに移動します。
4. 以下のコマンドで bundlemanager を実行します。

   ```
   java -jar bundle-manager.jar
   ```

   上記のコマンドにより、*<install_location>*¥Arcot Systems¥java¥webapps ディレクトリに arcotadmin.war ファイルが生成されます。

問題:

Strong Authentication サーバ（Strong Authentication サービス）を起動できません。arcotwebfortstartup.log に以下のエラーが表示されます。

```
Failed to initialize DB Pool Manager
```

または
```
Data source name not found and no default driver specified
```

原因

この問題の考えられる原因は以下のとおりです。

- データベースの DSN がシステム DSN として作成されていない。
- 64 ビットのプラットフォームを使用している。 その結果、DSN が 64 ビットの ODBC Manager を使用して作成されている。

解決方法:

arcotcommon.ini ファイルで DSN 関連の問題を確認できます。 問題が DSN 関連の場合、以下の手順に従います。

1. 最初の原因を解決するには、DSN がシステム DSN であることを確認する必要があります。 以下の手順を実行します。
   a. ［コントロール パネル］を開き、［管理ツール］-［データ ソース（ODBC）］に移動します。
   b. ［システム DSN］タブをアクティブにし、該当 DSN が存在することを確認します。 存在しない場合は、以前と同じ名前で DSN を再作成する必要があります。
   c. サービスを再起動します。
2. 2 番目の原因（64 ビットのプラットフォームを使用している場合）を解決するには、ODBC Manager の 32 ビットのバージョンを使用します。 Windows の場合、C:¥Windows¥SysWOW64 に 32 ビットのバージョンがあります。

   注: arcotcommon.ini およびその他の設定ファイルの詳細については、「*Strong Authentication インストールおよび展開ガイド*」の付録「設定ファイルおよびオプション」を参照してください。

問題:

Strong Authentication サーバ（Strong Authentication サービス）を起動できません。 エラー メッセージは、サービスが起動し、自動的に停止していることを示しています。

原因

この問題の考えられる原因としては、インストール時にデータベースの詳細を指定したが、データ ソースが正常に作成されなかった可能性があります。

解決方法:

この問題を解決するには、以下の手順に従います。

1. DSN の対応するエントリが arcotcommon.ini にあるかどうかを確認します。
   - エントリがない場合は、手動で DSN を作成します。
2. エントリがある場合は、「データベース スクリプトの実行」の説明に従って、データベースをクリーンアップし（「Strong Authentication スキーマのアンインストール」を参照）、データベースを再シードします。
3. Strong Authentication サーバを再起動します。

問題:

マスタ管理者として CA Advanced Authentication を初めて起動した際（「ブートストラップ タスクの実行」を参照）に、以下のメッセージが表示されます。

```
The server encountered an internal error that prevented it from fulfilling this request.
```

arcotadmin.log ファイルに以下のエラーが記録されています。

```
adminLog: java.lang.UnsatisfiedLinkError: no ArcotAccessKeyProvider in java.library.path
```

原因

JAVA ライブラリに、以下のいずれかのファイルへのパスが含まれていません。

- ArcotAccessKeyProvider.dll
- arcot-crypto-util.jar

解決方法:

以下の手順を実行します。

1. PATH 変数に以下のファイルへの絶対パスが含まれていることを確認します。
   - ArcotAccessKeyProvider.dll
   - arcot-crypto-util.jar
2. アプリケーション サーバを再起動します。

問題:

ARCOT_HOME のログ ディレクトリにログ ファイル（arcotadmin.log、arcotuds.log、または webfortserver.log）がありません。

原因

この問題の考えられる原因は以下のとおりです。

- ARCOT_HOME がインストール時に正しく設定されていない。
- アプリケーション サーバの JAVA ホームが、JDK ホームではなく JRE を指していている。

解決方法:

これらの問題を解決するには、以下の手順に従います。

- ARCOT_HOME をリセットして、正しい場所を指すように設定されていることを確認します。通常は、*<installation_location>*¥Arcot Systems¥ を指します。

  この結果として、コマンド プロンプト ウィンドウで cd %ARCOT_HOME% コマンドを使用する際には、現在のディレクトリを *<installation_location>*¥Arcot Systems¥ に変更する必要があります。
- アプリケーション サーバの JAVA HOME の場所に ArcotAccessKeyProvider.dll ファイルおよび arcot-crypto-util.jar ファイルをコピーしたことを確認します。

問題:

UDS を展開しましたが、起動しません。

原因

考えられる原因の 1 つは、アプリケーション サーバの JAVA ホームが JDK ホームではなく JRE を指していているというものです。

解決方法:

アプリケーション サーバの JAVA ホームの場所に ArcotAccessKeyProvider.dll ファイルおよび arcot-crypto-util.jar ファイルをコピーしたことを確認します。

問題:

UDS に接続できません。 以下のエラー メッセージが表示されます。
`Unable to contact User Data Service`

原因

考えられる原因は以下のとおりです。

- UDS の **ホスト**、**ポート**、および**アプリケーション コンテキスト**情報を正しく指定していない可能性があります。
- UDS サービスが初期化されていない可能性があります。

解決方法:

この問題を解決するには、以下の手順に従います。

CA Advanced Authentication の［ユーザ データ サービス設定］ページで指定した UDS 情報が正しいかどうかを確認します。［**ホスト**］、［**ポート**］、および［**アプリケーション コンテキスト ルート**］フィールドの詳細は正確である必要があります。

1. UDS ログ ファイルを確認して、サービスが正常に初期化されたことを確認します。

Database-Related エラー

問題:

データベースへの接続に失敗し、サーバ ログ ファイルに以下のエントリが記録されます。

```
ReportError: SQL Error State:08001, Native Error Code: 30FD, ODBC Error: [DataDirect][ODBC Oracle driver][Oracle]ORA-12541: TNS:no listener
```

解決方法:

以下を確認します。

- データベース サーバのリスナ サービス。
- サーバがインストールされているシステムの TNSnames.ora ファイルの設定。

問題:

データベースへの接続に失敗し、サーバ ログ ファイルに以下のエントリが記録されます。

```
TNS:listener could not resolve SERVICE_NAME given in connect descriptor
```

解決方法:

以下を確認します。

- データベースが起動している。 起動していない場合、上記のメッセージが表示されます。
- データベースが起動している場合は、データベースがまだリスナに登録されていない可能性があります。 これは、データベースまたはリスナの起動直後に発生します。 通常、この問題は 1 分程度待てば解決します。
- 静的な登録を使用している場合は、接続文字列（TNSNAMES.ORA、NAMES、OID など）で使用される SERVICE_NAME エントリが、リスナが認識している有効なサービスと一致することを確認します。
- C:>tnsping SERVICE_NAME を使用して、ステータスを確認したり、C:>lsnrctl services を使用して、リスナが認識しているすべてのサービスを確認したりできます。

問題:

データベースへの接続に失敗し、サーバ ログ ファイルに以下のエントリが記録されます。
`Database password could not be obtained from securestore.enc`

原因

データベースの詳細が securestore.enc ファイルに含まれていない可能性があります。

解決方法:

DBUtil ツールを使用して、データベースの詳細を指定して securestore.enc ファイルを更新します。 DBUtil の使用方法の詳細については、「CA Strong Authentication 管理ガイド」を参照してください。

問題:

データベースへの接続に失敗し、サーバ ログ ファイルに以下のエントリが記録されます。
`RA-03113: end-of-file on communication channel`

原因

これは接続が失われたことを示す一般的なエラーです。 以下のようなさまざまな原因で発生します。

- ネットワークの問題
- サーバ セッションの強制切断
- Oracle データベースのクラッシュ
- データベース サーバのクラッシュ
- 中断を引き起こす Oracle の内部エラー(ORA-00600 や ORA-07445 など)
- Oracle クライアントまたは TNS レイヤで接続を処理できない

解決方法:

上記のリストにある考えられる原因を確認します。

Strong Authentication サーバ エラー

問題:

サーバを起動しようとしても、起動しません。 arcotwebfortstartup.log の最後の行に以下のエラーが表示されています。

```
WARN  STARTUP      -161388848 00WFMAIN - [11]: Protocol module
[SVRMGMT_WS] received portType error [bind: Address already in use]
```

原因

この問題の考えられる原因は、サーバ管理ポート（デフォルトのポート番号： 9743）が別のプロセスによってすでにホストで開かれているというものです。また、サーバが起動するためには、少なくともサーバ管理ポートが必要です。

解決方法:

以下の手順を実行します。

1. コマンド プロンプト ウィンドウを開きます。
2. %ARCOT_HOME%¥bin に移動します。
3. 以下のコマンドを実行します。

   arwfserver -i
4. 「setsvrmgmtport <*new_port_number*>」を入力します。

   サーバ管理ポートを設定すると、マスタ管理者は CA Advanced Authentication にログインして、別のポートを設定できます。

問題:

「Access-Reject」メッセージで RADIUS リクエストが失敗します。

原因

以下を確認します。

- 共有秘密キーが正しく設定されている。
- サーバ ログ内のエラー。

解決方法:

グローバル管理者または組織としてログインし、［RADIUS 設定］ページを使用して共有秘密キーを設定します。

問題:

CA Auth ID 認証が失敗し、サーバ ログ ファイルに以下のエントリが記録されます。

```
[Arcot Exception,No valid issuer certificate is available for this certificate: unknown or invalid certificate issuer in ArcotVerifier], Challenge verification failed -
```

原因

ドメイン キーが期限切れになっている可能性があります。

解決方法:

グローバル管理者または組織としてログインし、CA Advanced Authentication の［認証キー管理設定］ページを使用してドメイン キーを設定します。