Arcot WebFort®
インストールおよび展開ガイド
（Unix プラットフォーム用）
バージョン 6.2

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort インストールおよび展開ガイド
バージョン 6.2
2010 年 5 月
部品番号：WF-0062-0IGC-10

商標

特許

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

サードパーティ ソフトウェア

WebFort によって使用されるすべてのサードパーティ ソフトウェア、および関連するコンポーネントは、付録 「サードパーティ製ソフトウェアのライセンス」にリストされています。

目次

序文

本「Arcot WebFort 6.2 インストールおよび展開ガイド」では、さまざまなソリューションの要件に応じた WebFort の計画および展開について解説します。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。

本書の目的

ここでは、本書の対象読者、本書の内容、関連文献、および本書で使用されている表記規則について説明します。

対象読者

本書は、アーキテクト、システム管理者、データベース管理者、システム インテグレータ、Web 開発者、および Arcot WebFort のインストール、展開、保守の担当者を読者として想定しています。

本書の内容

本書の構成は以下のとおりです。

- 第 1 章の「WebFort VAS® の基本の理解」では、WebFort の概要、主要概念、現在のバージョンの新機能について説明します。
- 第 2 章の「展開の計画」では、さまざまな展開オプションを紹介し、各展開モデルのアーキテクチャについて詳説します。
- 第 3 章の「インストールの準備」では、WebFort のインストール要件について説明します。また、設定と計画に関する情報も紹介します。
- 第 4 章の「単一システム上の WebFort の展開」では、単一システムへの展開時のインストール作業およびインストール後の作業を紹介します。

- 第 5 章の「分散システムでの WebFort の展開」では、分散システムへの展開時または高可用性を重視した展開時のインストール作業およびインストール後の作業を紹介します。
- 第 6 章の「Java SDK および Web サービスの設定」では、WebFort で提供されている API と Web サービスの設定手順について説明します。
- 第 7 章の「WebFort のアンインストール」では、WebFort コンポーネントのアンインストール手順について説明します。
- 付録 A の「WebFort ファイル システム構造」では、WebFort インストーラでインストールされる全ファイルの保存場所を示します。
- 付録 B の「設定ファイルおよびオプション」では、WebFort で使用する設定ファイルと、これらのファイル中で設定する必要があるパラメータについて説明します。
- 付録 C の「データベース リファレンス」では、WebFort のテーブルについて説明し、テーブルの縮小に関する推奨事項を紹介します。
- 付録 D の「デフォルトのポート番号および URL」では、WebFort で使用するデフォルトのポート番号と URL を表にまとめています。
- 付録 E の「アプリケーション サーバの設定」では、接続プーリング利用時のアプリケーション サーバの設定手順について説明します。
- 付録 F の「SSL 用の設定」では、WebFort サーバとクライアント間の SSL 通信の設定方法について説明します。
- 付録 G の「サードパーティ製ソフトウェアのライセンス」では、WebFort で使用するサードパーティ製ソフトウェア パッケージのライセンス情報を列挙しています。
- 付録 H の「用語集」は、WebFort の関連用語集です。

関連するドキュメント

その他の関連するドキュメントは以下のとおりです。

Arcot WebFort 6.2 クイック インストール ガイド	WebFort のインストール時に実行する必要がある作業について概説しています。
Arcot WebFort 6.2 管理ガイド	WebFort の管理および設定に関する情報が記載されています。
Arcot WebFort 6.2 Java 開発者ガイド	WebFort で提供される Java API と、その使用法について解説しています。
ArcotID Client 6.0.2 リファレンス ガイド	ArcotID Client のタイプ、各クライアントで提供される API について解説しています。

本書の表記規則

ここでは、本書の表記規則、定型見出し、およびサポート窓口について説明します。

表記規則

本書は、次の表記規則に従っています。

斜体	強調、ガイド名
太字	ユーザによる入力内容、GUI 画面のテキスト
固定幅フォント	ファイル名およびディレクトリ名、拡張、コマンド プロンプト、CLI テキスト、コード
固定幅フォント **太字**	パス内のターゲット ファイル名またはターゲット ディレクトリ名
固定幅フォント *斜体*	ユーザごとに異なる可能性があるファイル名またはディレクトリ名
リンク	本書内の参照先へのリンク、URL リンク

形式

本書では、次の定型見出しを付けて注意事項を記載しています。

注： 重要な情報や特別に注意を喚起する必要がある情報を示します。

ヒント： 時間またはリソースの節約手法を紹介します。

警告： この見出しが付いた注記を無視すると、機器の誤作動や破損につながる危険があります。

重要： 操作の実行前に確認しておくべき情報を示します。

	**注意 :** 重大な問題発生の危険性について注意を促します。

	**関連文書 :** 他の参照文献を紹介します。

サポートへのお問い合わせ

ヘルプが必要な場合は、次の Arcot サポート窓口にお問い合わせください。

電子メール	*support@arcot.com*
Web サイト	*http://www.arcot.com/support/index.html*

第 1 章
WebFort VAS® の基本の理解

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のみに頼る認証方式では万全ではなくなってきました。エンド ユーザを守るため、また政府当局によるセキュリティ規制、社内ポリシー、またはベスト プラクティスを遵守するため、より強固な認証方式が求められています。しかし、強力な認証方式の導入に際しては、往々にしてコンプライアンス要件を重視するあまりユーザの利便性が損なわれがちです。つまり、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し、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。

Arcot WebFort Versatile Authentication System®（VAS）は、アプリケーションでエンド ユーザの身元を確認し、保護するための実績ある強力な認証サービスで、次のような特長があります。

- ネットワーク上でパスワードを（クリア テキスト パスワードと暗号化したパスワードのいずれも）転送しない。
- セキュリティや利便性に対する各種ユーザの要件に最適な認証方式を選択できる。
- ArcotID® および ArcotOTP 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、キーを総当たり攻撃対策となる長さのパスワード 1 つのみで暗号化する方法は取りません。実際にキーを正しく復号化できるパスワードは 1 つのみですが、複数のパスワードでキーを復号化して有効なキーを入手できるように見せかけて攻撃者を欺きます。そのため、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中で実現します。

WebFort の最大の利点は、認証に ArcotID を利用することで、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、単純なユーザ名 / パスワード認証のセキュリティを強化できる点にあります。

この章では、WebFort Versatile Authentication Server、そのコンポーネントのアーキテクチャ（WebFort のアーキテクチャ）について説明し、本リリース（このリリースの新機能）で導入された新機能や拡張機能を紹介します。

WebFort Versatile Authentication Server

WebFort 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、汎用認証サーバ（VAS、Versatile Authentication Server）といえます。また、PKI（Public Key Infrastructure）やワンタイム パスワード（OTP）を利用した認証をサポートするだけでなく、必要に応じて既存の認証メカニズムを組み込めるため、従来の業務環境への支障なく重大なシステムやパートナー アプリケーションに対する変更を処理できます。

こうした WebFort の VAS 機能のおかげで、組織内のエンド ユーザの要件に最適な認証メカニズムを柔軟に選択できます。次の手法を選択できます。

- 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。
- ワンタイム パスワード（OTP）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、ArcotID などの新しい認証メカニズムを追加する。
- プラグインまたはコールアウトにより WebFort VAS を拡張し、独自の認証メカニズムを導入する。

WebFort への組み込み

WebFort では、以下の認証メカニズムをすぐに導入できます。

- ArcotID
- ユーザ名 / パスワード
- ワンタイム パスワード
- OATH 準拠のワンタイム パスワード
- 質問と回答（Q&A）
- ArcotOTP
- LDAP ユーザ名 / パスワード

上記以外のメカニズムを実装する必要がある場合も、コールアウトやプラグインを記述するか、カスタム API を使用する形で柔軟に WebFort に組み込むことができます。

コールアウト

コールアウトは、WebFort の標準機能を変更または補強するカスタム コンポーネントで、任意のプログラミング言語で記述できます。コールアウトは外部プロセスです。そのため、WebFort サーバ コンテキストの外部に常駐し、HTTPS ベースの別個のサーバ上でホストされます。

コールアウトは外部プロセスであるため、登録する必要はありません。ただし、所定のイベントの発生時に呼び出されるように、発行される一連のイベントに対して（Administration Console を使用して）コールアウトを設定する必要があります。

1 つの組織で複数のコールアウトを設定できます。また、複数の組織に同一のコールアウトを設定できます。

プラグイン

コールアウトと同様、プラグインもカスタムのサーバサイド コンポーネント（C または C++ で記述）で、WebFort VAS の機能を拡張できます。ただし、外部プロセスであるコールアウトとは異なり、プラグインはサーバサイド プロセスであり、WebFort サーバのコンテキスト内のカスタム イベント ハンドラ ライブラリとして実装されます。

コールアウトと異なり、所定のイベントの発生時に呼び出されるように、発行される一連のイベントに対して（Administration Console を使用して）プラグインを登録する必要があります。

1 つの組織で複数のプラグインを設定できます。また、複数の組織に同一のプラグインを設定できます。

カスタム API

WebFort では、デフォルトでサポートされているもの以外の認証方式を実装できます。たとえば、トークンを使用したハードウェアベースの認証や、証明書ベースの認証です。WebFort には、こうしたクレデンシャルを作成および管理し、認証するための API（`CustomIssuance` と `CustomAuth`）があります。

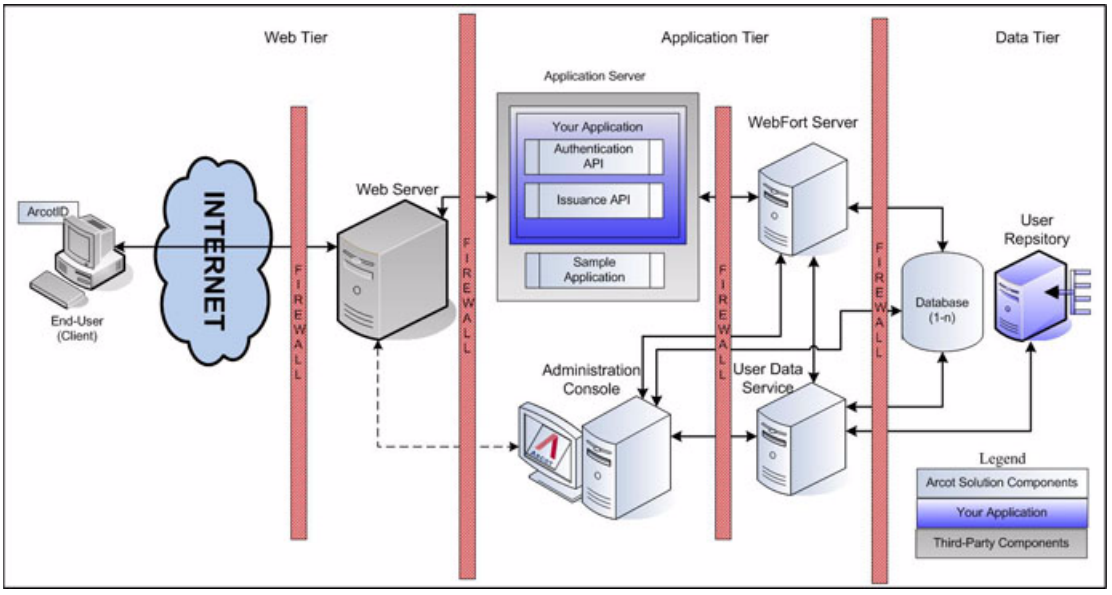
WebFort のアーキテクチャ

単一のシステム上に WebFort をインストールするか、複数のシステムにコンポーネントを分散できます。ただし、トランザクションのセキュリティを最大限確保できるように、以下の 3 層から形成されるアーキテクチャ（図 1-1 を参照）を推奨します。

- Web 層

- アプリケーション層
- データ層

図 1-1 WebFort のアーキテクチャ図



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

Web 層

この層は静的な（HTML）コンテンツで形成され、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。

この層がエンド ユーザのブラウザに ArcotID Client （Java、Flash、または Native）を提供します。ArcotID Client が WebFort サーバと対話し、ユーザ認証を行います。また、ArcotID 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 WebFort サーバに送信して WebFort サーバによる検証を受けます。

	関連文書： ArcotID Client の詳細については、「*ArcotID Client 6.0.2 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、WebFort サーバ、WebFort SDK を使用するアプリケーション、Administration Console とユーザ データ サービス（UDS）が常駐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。

- **WebFort 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 WebFort SDK を利用して処理するサーバ コンポーネント。

- **Administration Console**

  サーバ インスタンス、WebFort コンポーネント間の通信モード、および認証ポリシーの設定、クレデンシャルの管理、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**

  リレーショナル データベース（RDBMS）およびディレクトリ サーバ（LDAP）などの各種のユーザ リポジトリのユーザ関連データや組織関連データへのアクセスを実現する抽象層。

- **認証 SDK**

  認証リクエストを WebFort サーバに転送するためにアプリケーションが呼び出す API。

- **発行 SDK**

  発行リクエストを WebFort サーバに転送してユーザを登録し、WebFort でユーザのクレデンシャルを作成および管理するためにアプリケーションが呼び出す API。

- **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、WebFort Java API の使用法と、アプリケーションと WebFort の統合方法の具体例を示します。また、WebFort が正常にインストールされたどうかや、発行操作と認証操作を実行できるかどうかを確認するためにも使用できます。

データ層

この層には、他のユーザ リポジトリが設定されていない場合に、WebFort で設定、クレデンシャル、ユーザ データの格納に使用する RDBMS（リレーショナル データベース管理システム）があります。

このリリースの新機能

WebFort 6.2 リリースの主な機能や拡張機能は以下のとおりです。

- **部分パスワード検証のサポート**

  ユーザのパスワード全体の検証に加えて、ユーザ パスワードの一部の文字を検証するのみでユーザを認証できるようになりました。この機能を有効にした場合、ユーザはパスワード中のさまざまな文字位置の文字を入力するよう求められます。たとえば、パスワードが「casablanca!」である場合に、1、3、および 8 の位置の文字の入力を求められます。この場合は、「csn」となります。

  部分パスワードの検証を行うと、ユーザが認証時にパスワード全体を入力しないため、キーロガーによる攻撃阻止に役立ちます。

  この機能を実現するため、Administration Console が以下の点で拡張されました。

  - ユーザ名 / パスワード発行プロファイルで部分パスワード機能を有効に設定できます。
  - ユーザ名 / パスワード認証ポリシーで、入力文字位置のオプションを設定できます。

- **同一ユーザに対する複数のパスワード クレデンシャルのサポート**

  WebFort では、同じユーザに対して用途別に複数のパスワード クレデンシャルをサポートできます。Administration Console の機能が強化され、1 人のユーザに複数のパスワード クレデンシャルを発行するための設定を作成し、管理できるようになりました。

  この機能を実現するため、Administration Console が以下の点で拡張されました。

  - ユーザ名 / パスワード発行プロファイルで、パスワードの用途を指定できます。
  - ユーザ名 / パスワード発行プロファイルで、WebFort サーバによってパスワードを生成する必要があるか、またはユーザがパスワードを入力する必要があるかを指定できます。
  - ユーザ名 / パスワード発行プロファイルで、1 人のユーザに対して用途にかかわらず一意のパスワードを使用するように強制設定できます。

- ユーザ名 / パスワード認証ポリシーで、特定の用途のパスワードを検証するか、同一ユーザに対して用途にかかわらず 1 つのパスワードを検証するかを設定できます。

- **ユーザ名 / パスワード クレデンシャルの使用回数のサポート**

  WebFort では、ユーザ名 / パスワード クレデンシャルを使用できる回数を設定できるようになりました。パスワードを無制限で使用できるように設定するか、使用可能回数を指定できます。

  この機能を実現するため、Administration Console が以下の点で拡張されました。

  - ユーザ名 / パスワード発行プロファイルで、パスワードの使用回数を指定できます。

- **質問と回答クレデンシャルの呼び出し元検証のサポート**

  この機能は、テクニカル サポート担当者（CSR）、または同様の機関によって行われる Q&A 検証をサポートします。検証の結果は、WebFort サーバに送信されます。この機能をサポートするために `QnAAuth` インターフェースが機能強化されています。詳細については、「Arcot WebFort 6.2 Java 開発者ガイド」を参照してください。

  この機能を実現するため、Administration Console が以下の点で拡張されました。

  - 質問と回答発行プロファイルで呼び出し元検証を有効に設定できます。

- **事前定義の質問のサポート**

  WebFort では、質問と回答クレデンシャル用の質問一式をあらかじめ設定しておくことができます。組織用に設定されている質問の数に応じて、ユーザは、質問と回答クレデンシャルの発行の際に、設定済みの質問一式の中から質問を選択できます。

  この機能を実現するため、Administration Console が以下の点で拡張されました。

  - 質問と回答発行プロファイルで、質問を設定できます。

- **異なる質問選出オプションのサポート**

  Q&A 認証では、提示される質問の選択方法を選択できます。WebFort は 2 つのモード、Random および Alternate をサポートします。Random オプションを選択した場合は、ユーザに対して設定済みの質問の中からランダムに質問が選出されます。Alternate オプションを選択すると、WebFort では質問セットが選択されます。これは、前回の質問用に選択されたセットとは異なります。

  WebFort での質問セットの変更は、認証の度に行うことも、認証が成功したときにのみ行うことも可能です。WebFort が新しい質問セットを選択するように設定されている場合、Q&A 認証が試行されるたびに、新しい質問セットがユーザに提供されます。

認証が正常に終了した場合に限り新しい質問一式に入れ替えるように WebFort が設定されている場合は、GetQuestions （または同等の）リクエストが行われるたびに、認証が正常に終了しない限り同じ質問一式が提示されます。

この機能を実現するため、Administration Console が以下の点で拡張されました。

- Q&A 認証ポリシーで質問の選択モードを指定できます。
- Q&A 認証ポリシーで質問一式の変更オプションを指定できます。

- **ArcotOTP クレデンシャルのサポート**

  WebFort では、ArcotOTP と呼ばれる新しいクレデンシャルを利用できるようになりました。これは、OATH 標準に準拠したワンタイム パスワードです。ユーザが PIN を入力する際に、クライアント デバイス（たとえば携帯電話）上で ArcotOTP が生成されます。生成された ArcotOTP は、セキュリティで保護されたアプリケーションに対する認証に使用されます。WebFort では、カウンタ同期方式（HOTP）と時刻同期方式（TOTP）の両方の ArcotOTP をサポートしています。

- **OATH ベースのトークンのサポート**

  WebFort で OATH ベースのトークン クレデンシャルがサポートされるようになりました。WebFort サーバにトークンの詳細情報をバッチ処理でアップロードし、これらのトークンをユーザと関連付けることができます。他の WebFort クレデンシャルと同様、これらのトークンも Administration Console で管理されます。WebFort ではカウンタ同期方式（TOTP）と時刻同期方式（HOTP）の両トークンをサポートしています。

- **クレデンシャル管理の機能強化**

  WebFort では、ユーザ クレデンシャル管理用に以下の機能が Administration Console に追加されています。

  - 複数のパスワードを管理する機能。
  - 各クレデンシャルのカスタム属性を追加、更新、削除する機能。
  - OATH クレデンシャルを管理し、OATH トークン ID をユーザに割り当てる機能。
  - ArcotOTP クレデンシャルを管理する機能。
  - 一定期間クレデンシャルを無効にする機能。たとえば、現在の日付から 3 か月間 ArcotID を無効にしたり、特定の日付から 3 か月間無効にしたりすることができます。
  - 単一のボタンを使用してユーザのクレデンシャルをすべて有効または無効にする機能。

- **Plug-In SDK の機能強化**

  Plug-In SDK で、以下の機能がサポートされるようになりました。

  - プラグインが必要とする WebFort プロファイルへの読み取りアクセス。
  - プラグインが必要とする WebFort ポリシーへの読み取りアクセス。
  - ユーザ名 / パスワード プロファイルでパスワードの自動生成機能が設定されている場合に、この機能を無効にする機能。
  - エンコードされた値を対応するプレーン値と照合する機能。たとえば、暗号化されたパスワードを、プレーン テキスト パスワードと照合し、パスワードの独自性を検証できます。
  - プラグインで WebFort 応答コードがサポートされ、呼び出し元アプリケーションにこれらのコードが返されるようになりました。

- **ArcotID エイリアスのサポート**

  ArcotID の発行中に、アプリケーションごとに複数のエイリアスを指定できます。これらのエイリアスはすべて ArcotID 認証に使用できます。

  たとえば、ArcotID が `USERNAME=USER1` およびエイリアス `ALIAS1` と `ALIAS2` で作成されている場合、認証中にユーザは同じ ArcotID の `USERNAME` として `USER1`、`ALIAS1`、または `ALIAS2` を提供できます。

  この機能は、ユーザが同じセットアップ中の異なるアプリケーションに対して別々のログイン ID を割り当てられている場合に便利です。

- **WebFort とデータベース間の一方向 SSL のサポート**

  WebFort では、以下の一方向 SSL がサポートされるようになりました。

  - WebFort サーバとデータベース間
  - Administration Console とデータベース間
  - ユーザ データ サービスとデータベース間

注： WebFort では、現在 Oracle データベースに*限り*この機能をサポートしています。

- **サンプル アプリケーションの機能強化**

  サンプル アプリケーションは、新しいクレデンシャルやその操作をサポートするために提供されている新しい Java API や、既存のクレデンシャル用の新機能の使用法の具体例を示します。以下を実証するサンプル アプリケーションが付属しています。

  - OATH OTP の発行および認証。
  - ArcotOTP の発行および認証。
  - 完全パスワードと部分パスワードによる認証。
  - Q&A クレデンシャル用のサーバ検証および呼び出し元検証。
  - Java SDK を使用して実行できるすべてのクレデンシャル操作のサポート。
  - 新しく機能強化されたユーザ インターフェース。

- **ドキュメントの変更**

  このリリースには、新規テンプレートに基づく各種ガイドが付属しています。新しいテンプレートは以下の点で改善されています。

  - ページ レイアウトの刷新（ドキュメント サイズが縮小されました）。
  - 特別なメッセージ（注、重要、参照文献、ヒント、警告など）を示す画像アイコンの採用。
  - 業界標準フォントの使用。
  - 画像解像度の改善（図が鮮明に表示されるようになりました）。

第 2 章
展開の計画

この章では、以下の展開関連のトピックが説明されています。

- 展開の概要
- 展開モデルの選択

展開の概要

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

1. ビジネス ニーズに適する展開モデルを選択します。「展開モデルの選択」を参照してください。
2. 前提条件となるソフトウェアをすべてインストールします。前提条件となるソフトウェアの詳細については、「システム要件」を参照してください。
3. WebFort コンポーネントをインストールします。以下のセクションを参照してください。
   - 「単一システム上の WebFort の展開」（完全インストール用）。
   - 「分散システムでの WebFort の展開」（カスタム インストール用）。
4. データベースで SQL スクリプトを実行し、Arcot スキーマを作成して、初期設定値を設定します。以下を参照してください。
   - 「データベース スクリプトの実行」（単一システム展開用）。
   - 「2 つ目のシステムへのインストール」（分散システム展開用）。
5. Web ベースのアプリケーションを展開します。以下を参照してください。
   - 「Web アプリケーションの展開」（単一システム展開用）。
   - 「Web アプリケーションの展開」（分散システム展開用）。
6. Administration Console にログインし、システムをブートストラップします。以下を参照してください。
   - 「システムのブートストラップ」（単一システム展開用）。

- 「システムのブートストラップ」（分散システム展開用）。

展開モデルの選択

このセクションは、展開モデルを選択し、各システムにインストールする必要のある WebFort コンポーネントおよび前提条件ソフトウェアを判断するうえで役立ちます。

WebFort サーバは、インストール用のプライマリ コンポーネントです。WebFort サーバとは別に、アプリケーションと統合させるための Java SDK および Web サービスが提供されます。

WebFort には、サーバ設定データ、ユーザ固有の基本設定、および監査ログ データを格納するための SQL データベースが必要です。

この章で説明されているコンポーネント図は Java SDK 向けです。Web サービスの展開も同様の方法で実行します。認証および発行 Web サービス用の WSDL を使用し、お好みのソフトウェアを使用してクライアントを生成します。

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。

以下の展開モデルが、この章で説明されています。

- 単一システムへの展開
- 分散システムへの展開

単一システムへの展開

単一システムへの展開では、WebFort 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、WebFort 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。

単一システムの展開で Java SDK および Web サービスの両方を使用できます。これらのコンポーネントの前提条件となるソフトウェアについては、「ソフトウェア要件」を参照してください。

単一システムに WebFort を展開するには、WebFort 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。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、第 4 章の「単一システム上の WebFort の展開」を参照してください。

コンポーネント図

コンポーネント図には、前提条件ソフトウェアおよび WebFort コンポーネントの可能な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。WebFort 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。

単一システムの展開を実行する場合、以下の選択を行う必要があります。

選択肢

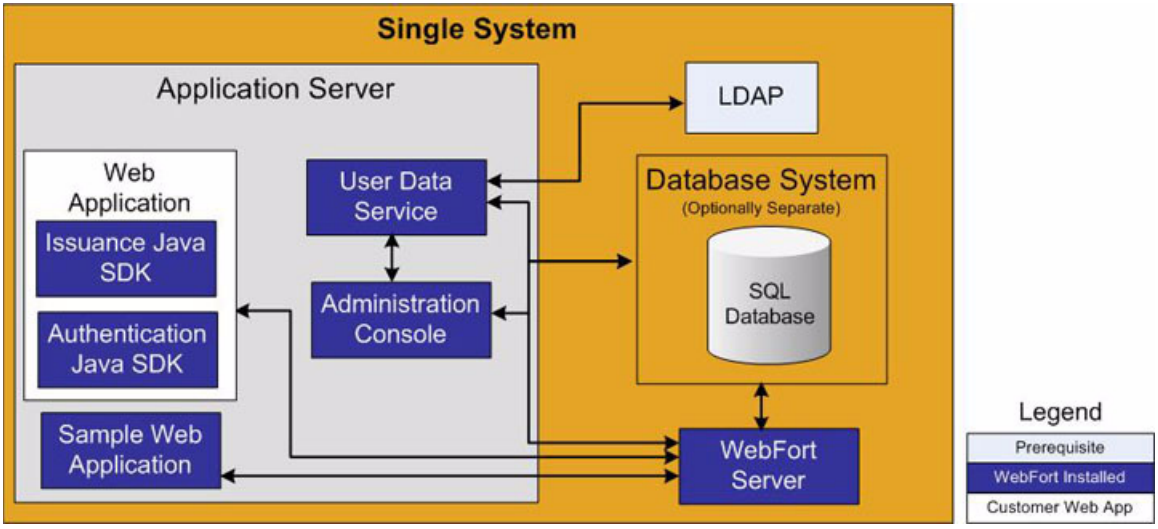
WebFort サーバがあるシステム上にデータベース サーバをインストールするか、または別のシステム上の既存のデータベースを使用します。

選択肢

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。

図 2-1 には、単一システムへの WebFort サーバおよび Java SDK の展開が示されています。

図 2-1 単一システムへの WebFort コンポーネントの展開



分散システムへの展開

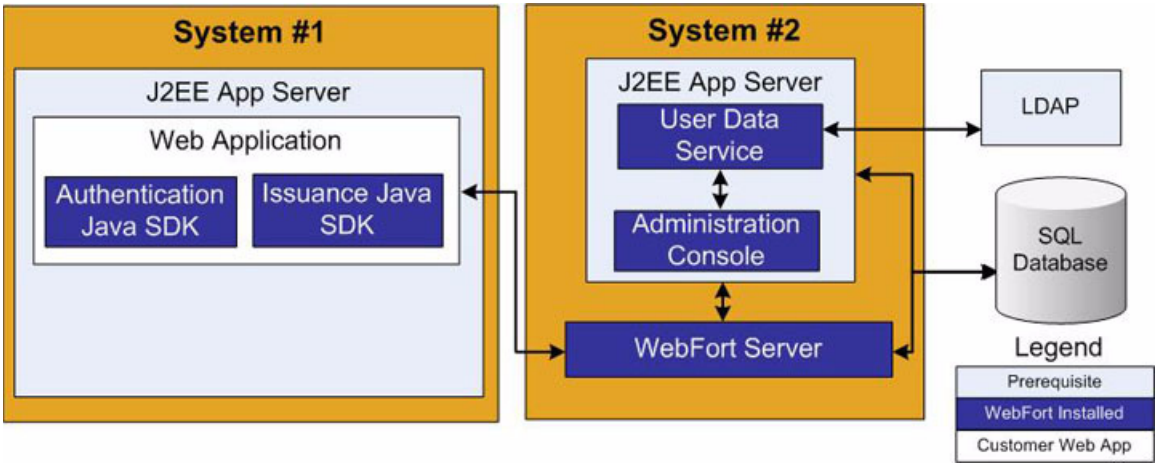
分散システムへの展開では、WebFort コンポーネントは異なるシステム上にインストールされます。このタイプの展開は、セキュリティおよびパフォーマンスを向上させます。このモデルは通常、運用環境の展開またはステージングの環境で使用されます。

最も一般的な展開では、単一システム上に WebFort サーバをインストールし、追加システム上に 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 WebFort を展開するには、WebFort 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、第 5 章の「分散システムでの WebFort の展開」を参照してください。

単一アプリケーションへの Java SDK の展開

図 2-2 には、Java SDK を使用した、単一アプリケーションへの WebFort の展開が示されています。高可用性展開では、このアプローチを使用して複数システム上に展開し、稼働の継続性を確保できます。

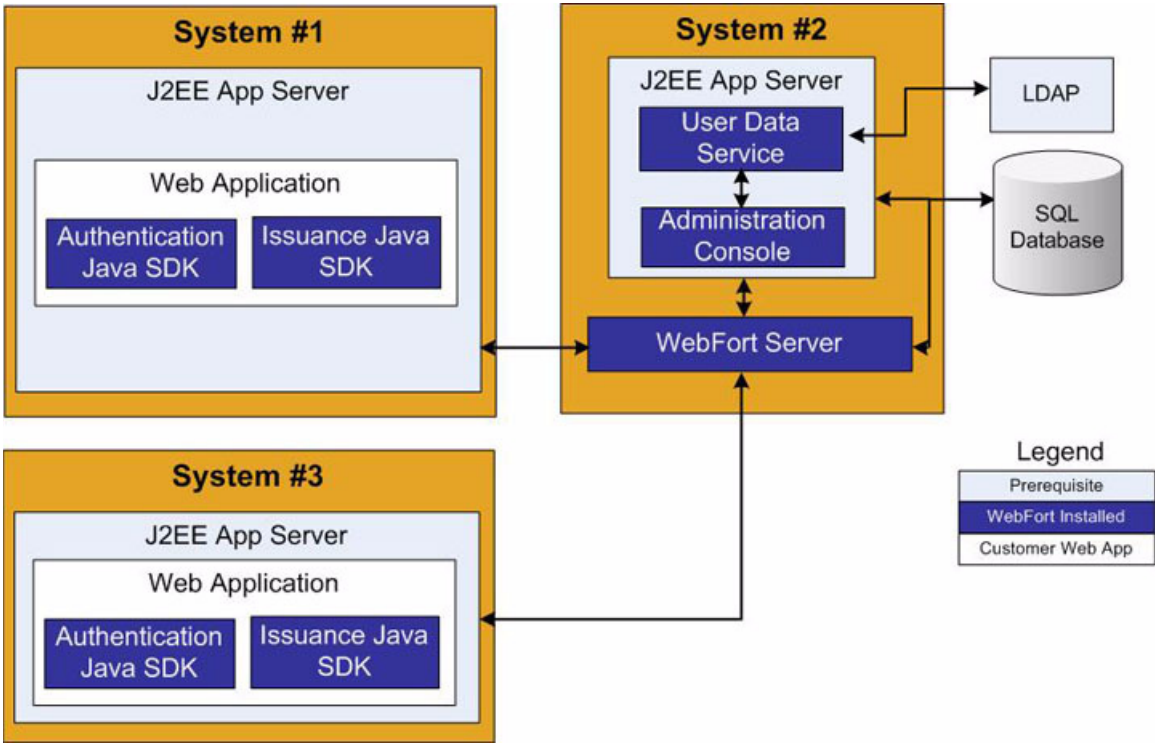
図 2-2 単一システムへの Java SDK の展開



複数アプリケーションへの Java SDK の展開

図 2-3 には、Java SDK を使用した、複数アプリケーションへの WebFort の展開が示されています。

図 2-3 複数システムへの Java SDK の展開



第 3 章
インストールの準備

WebFort をインストールする前に、コンピュータがこの章に記載された要件を満たしていることを確認してください。この章では、WebFort のインストール前に収集する必要があるデータベース情報にも言及します。本章は以下の節によって構成されています。

- システム要件
- インストールのチェックリスト

システム要件

ここでは、WebFort のインストールに際して必要な、ソフトウェアとハードウェアの最小要件について説明します。

- ハードウェア要件
- ソフトウェア要件

ハードウェア要件

ここに記載されているハードウェア要件は、WebFort のみを対象としています。データベースやアプリケーション サーバなど他の必須ソフトウェアに必要となるハードウェアについては記載されていません。

- RAM：1 GB
- ハード ドライブ容量：10 GB

ソフトウェア要件

注： 以下の表に記載されたサードパーティ製ソフトウェアについては、記載されたサポート バージョン以降のバージョンとの間に互換性があるものとみなします。

表 3-1 に、Solaris SPARC 上に WebFort をインストールする際に必要なサポート対象ソフトウェアを示します。

表 3-1. WebFort のインストールに必要なサポート対象ソフトウェア

ソフトウェア タイプ	バージョン
オペレーティング システム	以下のバージョンの Solaris オペレーティング システムがサポートされています。 • Solaris 10（SPARC） • Solaris 10 x-86
データベース	• Oracle 10g • Oracle 11g
ディレクトリ サーバ	• SunOne Directory Server 5.2 • SunOne Directory Server 6.1
アプリケーション サーバ	以下のアプリケーション サーバがサポートされています。 • Apache Tomcat 5.5.23 （*http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/*） • IBM WebSphere 6.1 • BEA WebLogic 10 • Oracle WebLogic 11g（WebLogic Server 10.3）
JDK	アプリケーション サーバと互換性のある JDK バージョン

表 3-2 に、Red Hat Enterprise Linux 上に WebFort をインストールする際に必要なサポート対象ソフトウェアを示します。

表 3-2. WebFort のインストールに必要なサポート対象ソフトウェア

ソフトウェア タイプ	バージョン
オペレーティング システム	• Red Hat Enterprise Linux 4.0（x86） • Red Hat Enterprise Linux 5.0（x86）
データベース	• Oracle 10g • Oracle 11g • IBM DB2 9.5
ディレクトリ サーバ	• SunOne Directory Server 5.2 • SunOne Directory Server 6.1

表 3-2. WebFort のインストールに必要なサポート対象ソフトウェア

ソフトウェア タイプ	バージョン
アプリケーション サーバ	以下のアプリケーション サーバがサポートされています。 • Apache Tomcat 5.5.23 （*http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.23/bin/*） • WebSphere 6.1 • WebLogic 10 • Oracle WebLogic 11g（WebLogic Server 10.3）
JDK	アプリケーション サーバと互換性のある JDK バージョン

インストールのチェックリスト

インストール前のチェックリスト

WebFort のインストールおよびセットアップを進める前に、以下のチェックリストに必要事項を書き留めておくことを推奨します。

表 3-3. インストール前のチェックリスト

情報	入力例	記入欄
ハードウェア		
プロセッサ	SPARC	
RAM	2 GB	
ディスク容量	20 GB	
ソフトウェア		
オペレーティング システム	Sun Solaris 10	
サービス パック（パッチ）	最新	
データベース		
タイプ	Oracle	
DSN 名	webfort	
ホスト名（またはサーバ）	webfort	
ポート（Oracle データベースのみ）	1521	
サービス ID （Oracle データベースのみ）	ocsdb1	
ユーザ名	dbadmin	

表 3-3. インストール前のチェックリスト（続き）

情報	入力例	記入欄
パスワード	データベース パスワード	
設定済みの権限：		
CREATE TABLE		
CREATE INDEX		
CREATE PROCEDURE		
REFERENCES		
DML 権限		
CREATE TABLESPACE（Oracle データベースのみ）		
UNLIMITED TABLESPACE（Oracle データベースのみ）		
DROP TABLESPACE（Oracle データベースのみ）		
アプリケーション サーバ		
タイプ	Apache Tomcat 5.5	
ホスト名	localhost	
ポート	8080	
JDK	1.5.0_10	
ディレクトリ サービス		
ホスト名	ds.myldap.com	
ポート	389	
スキーマ名	inetorgperson または user	
ベース識別名	dc=myldap,dc=com	
ユーザ名	cn=admin,cn=Administrators,cn=dscc	
パスワード	ディレクトリ サービス パスワード	
Web サーバ（オプション）		
タイプ	Apache HTTP Server	

表 3-3. インストール前のチェックリスト（続き）

情報	入力例	記入欄
ホスト名	mywebserver.com	
ポート	443	

インストール後のチェックリスト

WebFort のインストールおよびセットアップに関する情報を以下のチェックリストに書き留めておくことを推奨します。これらの情報は、後から実行する各種の管理業務に必要となります。

表 3-4. インストールのチェックリスト

情報	入力例	記入欄
ARCOT_HOME	opt/arcot	
システム情報		
ホスト名	my-bank	
ユーザ名	administrator	
パスワード	システム パスワード	
設定済みのコンポーネント	WebFort サーバ Administration Console および ユーザ データ サービス	
WebFort サーバ情報		
インスタンス名	server name-unique number	
Administration Console 情報		
ホスト名	localhost	
ポート	8080	
Master Administrator パスワード	Master Administrator パスワード	
ユーザ データ サービス情報		
ホスト名	localhost	

表 3-4. インストールのチェックリスト（続き）

情報	入力例	記入欄
ポート	8080	
アプリケーション コンテキスト ルート	arcotuds	

第 4 章
単一システム上の WebFort の展開

この章では、単一のシステムに展開する場合の WebFort のインストールと設定について説明します。

大まかな作業の流れは以下のとおりです。

- WebFort インストーラを実行し、ファイル システムに WebFort コンポーネントを追加して、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、「WebFort のインストール」を参照してください。
- データベース スクリプトを実行してスキーマとデータベース テーブルを作成します。詳細については、「データベース スクリプトの実行」を参照してください。
- アプリケーション サーバに Web ベース アプリケーションを展開します。詳細については、「Web アプリケーションの展開」を参照してください。
- Master Administrator として Administration Console にログインし、システムのブートストラップを行います。詳細については、「Administration Console へのログイン方法」を参照してください。
- インストールを検証します。詳細については、「インストールの確認」を参照してください。

WebFort インストーラでは、以下のインストール方法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]* インストールを実行する必要があります。

1. **[Complete]**：単一のシステム上に WebFort コンポーネントをすべてインストールします。
2. **[Custom]**：選択した WebFort コンポーネントをインストールします。

WebFort のインストール

ここでは、単一のシステムに展開する場合の WebFort のインストール手順について説明します。インストール時に使用する予定のアカウントが Administrators グループに属していることを確認してください。そうでないと、インストール自体はエラーが発生することなく終了しますが、WebFort サービスの作成といった重要な手順が正常に実行されません。

WebFort をインストールする前に、第 3 章の「インストールの準備」に記載の手順に従って、必須のソフトウェアがすべてインストールされ、データベースがセットアップされていることを確認してください。

注： WebFort インストーラの実行前に、PATH 環境変数に <*Java ホーム*>/bin が設定されていることを確認します。設定されていないと、arcotadmin.war ファイルを生成できない場合があります。

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

1. WebFort インストーラ Arcot-WebFort-6.2-<*プラットフォーム名*>-Installer.bin ファイルを探します。
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。

```
prompt> sh Arcot-WebFort-6.2-<プラットフォーム名>-Installer.bin
```

   インストーラがインストールの準備を開始します。

3. root ログインでインストーラを実行している場合は、「root としてインストールしています」という内容の警告メッセージが表示されます。インストールを続行するには「**Y**」、インストールを終了するには「**N**」を入力します。必要な選択肢を指定した後で、**Enter** キーを押して続行します。

   ［Welcome］画面が表示されます。

4. **Enter** キーをクリックしてインストールを続行します。

   WebFort の使用許諾契約書が表示されます。

5. 使用許諾契約書がすべて表示されるまで **Enter** キーを押します。

   使用許諾契約書が最後まで表示されたら、契約書の内容に同意するように求められます。

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

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

7. インストール先のフォルダの絶対パスを入力します。または、**Enter** キーを押して、表示されたデフォルト パスをそのまま使用します。

注： インストール先フォルダ名には、スペースが含まれていない名前を指定してください。スペースが含まれている場合、WebFort スクリプトやツールが想定どおりに機能しないためです。

8. インストール先のシステムに既存の Arcot 製品がある場合は、以下のオプションが表示されます。
   a. 1：新しい場所を入力する。
   b. 2：手順 7 で選択したフォルダへのインストールを続行する。
   c. 3：既存の Arcot 製品がインストールされている場所を使用する。
9. 上記のオプションのいずれかを選択し、**Enter** キーを押してインストールを続行します。

注： オプション 1 または 2 を選択した場合は、指定した場所に新しい `arcot` というフォルダが作成されます。

［Installation Type］画面が表示されます。

10. この画面には、WebFort で実行できるインストール タイプが表示されます。「**1**」を入力して、選択した WebFort コンポーネントをすべてインストールします。**Enter** キーを押して続行します。

［Database Type］画面が表示されます。

11. この画面にはデータベースの種類が表示されます。データベースの種類の番号を入力し、**Enter** キーを押して続行します。

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

12. プライマリ DSN の情報を入力します。表 4-1 に、必要となるデータベース詳細情報をまとめます。

表 4-1. プライマリ Oracle データベースのパラメータ

フィールド	説明
[Primary ODBC DSN]	インストーラによって、WebFort が Arcot 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。入力推奨値は「*arcotdsn*」です。
[User Name]	WebFort がデータベースへのアクセス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り指定されています。
[Password]	WebFort がデータベースへのアクセスに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り指定されています。
[Service ID]	Oracle 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 システム識別子。
[Port No]	データベース サーバが着信リクエストをリスニングするポート。
[Host Name]	Oracle サーバが稼働している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

13. バックアップ DSN の設定を求められます。バックアップ DSN を設定する場合は「**Y**」、バックアップ データベース設定をスキップする場合は「**N**」を入力して続行します。

14. 必要に応じて、バックアップ DSN の情報を入力します。表 4-2 に、必要となるデータベース詳細情報をまとめます。

表 4-2. バックアップ Oracle データベースのパラメータ

フィールド	説明
[Backup ODBC DSN]	インストーラによって、WebFort が Arcot 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。入力推奨値は「*arcotdsnbkp*」です。 **注：** プライマリ DSN とバックアップ DSN の DSN 名は異なる値にする必要があります。
[User Name]	WebFort がデータベースへのアクセス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り指定されています。 **注：** プライマリ DSN とバックアップ DSN の［User Name］は異なる値にする必要があります。
[Password]	WebFort がデータベースへのアクセスに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り指定されています。

表 4-2. バックアップ Oracle データベースのパラメータ

フィールド	説明
[Service ID]	Oracle 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 システム識別子。
[Port No]	データベース サーバが着信リクエストをリスニングするポート。
[Host Name]	Oracle サーバが稼働している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

[Pre-Installation Summary] 画面が表示されます。この画面には、製品名、インストール先フォルダ、インストールのタイプ、選択されているコンポーネント、ディスク空き容量情報が表示されます。

15. インストール設定のいずれかを変更する場合は、「**back**」を入力します。または **Enter** キーを押してインストールを続行します。

    [Ready to Install] 画面が表示されます。

16. **Enter** キーを押してインストール処理を開始します。

    [Installing] 画面が表示されます。数分かかる場合があります。

    インストールが正常に終了すると、[Installation Complete] 画面が表示されます。

17. **Enter** キーを押してインストーラを終了します。

注： インストール処理の内容を確認するには、< *インストール先ディレクトリ* >/arcot/logs のログ ファイル Arcot_WebFort_InstallLog.log を参照してください。

インストール後の作業

ここでは、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. Web アプリケーションの展開
3. Administration Console へのログイン方法
4. システムのブートストラップ
5. WebFort サーバの起動

6. インストールの確認
7. サンプル アプリケーションの展開

注： これらのインストール後の作業を完了した後で、第 6 章の「Java SDK および Web サービスの設定」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

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

WebFort で使用するデータベースを設定する方法

1. データベースの種類に対応するスクリプトが保存されているフォルダを探します。デフォルトの場所は以下のとおりです。

   （Oracle の場合）< *インストール先ディレクトリ* >/arcot/dbscripts/oracle

   （DB2 の場合）< *インストール先ディレクトリ* >/arcot/dbscripts/db2

2. データベース ベンダーのツールを使用して、*スクリプトを以下の順序で*実行します。

   a. arcot-db-config-for-common-1.0.sql

   b. arcot-db-config-for-webfort-6.2.sql

注： スクリプトの実行時にエラーが発生した場合は、必要な権限が割り当てられているかどうかデータベース管理者に確認してください。

Web アプリケーションの展開

ここでは、ユーザ データ サービスおよび Administration Console で必要となるファイルをコピーし、これらのアプリケーションの WAR ファイルを展開する手順について説明します。

- アプリケーション サーバの準備

- （オプション）エンタープライズ アーカイブ ファイルの作成
- ユーザ データ サービスの展開
- Administration Console の展開

アプリケーション サーバの準備

ここでは、以下のアプリケーション サーバ別に Arcot ファイル `libArcotAccessKeyProvider.so` および `arcot-crypto-util.jar` のコピー手順を説明します。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

`libArcotAccessKeyProvider.so` ライブラリ ファイルは以下の場所にあります。

< インストール先ディレクトリ >`/arcot/java/ext/`*< プラットフォーム名 >*`/32bit/`

`arcot-crypto-util.jar` ファイルは以下の場所にあります。

< インストール先ディレクトリ >`/arcot/java/ext/`

Apache Tomcat

Arcot ファイルをコピーするには、以下の手順に従います。

1. `libArcotAccessKeyProvider.so` ファイルを以下のディレクトリにコピーします。

Solaris の場合：

<Java ホーム >`/jre/lib/sparc`

RHEL の場合：

<Java ホーム >`/jre/bin`

2. `arcot-crypto-util.jar` ファイルを *<Java ホーム >*`/jre/lib/ext` ディレクトリにコピーします。
3. `LD_LIBRARY_PATH` を、`libArcotAccessKeyProvider.so` ファイルのコピー先ディレクトリに設定およびエクスポートします。
4. Tomcat を再起動します。

IBM WebSphere

WebSphere 6.1 上で Arcot ファイルをコピーするには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［**Environment**］をクリックし、［**Shared Libraries**］をクリックします。
   a. ［**Scope**］ドロップダウン リストから、有効な可視範囲を選択します。有効範囲には、アプリケーションの展開先サーバ / ノードが含まれている必要があります。
   b. ［**New**］をクリックします。
   c. ［**Name**］に、たとえば「**ArcotJNI**」と入力します。
   d. ［**Classpath**］を指定します。`arcot-crypto-util.jar` ファイルが存在する場所のパスを指定する必要があります。また、必ずファイル名を含めます。たとえば、< *インストール先ディレクトリ* >`/arcot/java/ext/arcot-crypto-util.jar` と指定します。
   e. JNI ライブラリのパスを入力します。`libArcotAccessKeyProvider.so` ファイルが存在する場所のパスを指定する必要があります。
   f. ［**Apply**］をクリックして、変更内容を保存します。
3. サーバ レベルのクラス ローダを設定します。
   a. ［**Servers**］をクリックし、［**Application Servers**］をクリックします。
   b. ［**Application Servers**］で、設定を行うサーバの設定ページを開きます。
   c. ［**Java and Process Management**］をクリックし、［**Class Loader**］をクリックします。
   d. ［**New**］をクリックします。［**Classes loaded with parent class loader first**］を選択し、［**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、ArcotJNI を選択して［**Apply**］をクリックします。
   h. 変更内容を保存します。
4. `libArcotAccessKeyProvider.so` ファイルを以下のディレクトリにコピーします。

Solaris の場合：

`<Java ホーム>/jre/lib/sparc`

RHEL の場合：

`<Java ホーム>/jre/bin`

5. WebSphere を再起動します。

BEA WebLogic

Arcot ファイルをコピーするには、以下の手順に従います。

1. `libArcotAccessKeyProvider.so` ファイルを以下の WebLogic ディレクトリにコピーします。

Solaris の場合：

`<Java ホーム>/jre/lib/sparc`

RHEL の場合：

`<Java ホーム>/jre/bin`

2. `arcot-crypto-util.jar` を WebLogic の *<WebLogic インスタンスで使用する Java ホーム>*`\jre\lib\ext` にコピーします。

注： WebLogic で使用されている適切な *<Java ホーム>* を使用してください。

3. WebLogic Admin Console にログインします。
4. **［Deployments］**に移動します。
5. **［Lock and Edit］**オプションを有効にします。
6. **［Install］**をクリックし、`arcot-crypto-util.jar` ファイルが保存されているディレクトリに移動します。
7. **［Next］**をクリックします。

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

   ［Summary］ページが表示されます。

9. ［**Finish**］をクリックします。
10. 変更をアクティブ化します。
11. WebLogic サーバを起動します。

（オプション）エンタープライズ アーカイブ ファイルの作成

デフォルトでは、WebFort は Administration Console およびユーザ データ サービス（UDS）の展開用として Web アーカイブ（WAR）ファイルを提供します。これらのファイルの形式をエンタープライズ アーカイブ（EAR）に変更し、その EAR ファイルを展開できます。

個別の EAR ファイルの生成

Administration Console またはユーザ データ サービス用の EAR ファイルを作成するには、以下の手順に従います。

1. *<インストール先ディレクトリ>*/arcot/tools/bundlemanager ディレクトリに移動します。
2. bundlemanager ツールを実行し、以下のコマンドを使用して EAR ファイルを作成します。

   ユーザ データ サービス用

   ```
   java -jar bundle-manager.jar  -ear <ファイル名 .ear> -warList
   arcotuds.war
   ```

   Administration Console 用

   ```
   java -jar bundle-manager.jar  -ear <ファイル名 .ear> -warList
   arcotadmin.war
   ```

   上記のコマンドを実行すると、EAR ファイルが *<インストール先ディレクトリ>* /arcot/java/webapps に生成されます。

単一の EAR ファイルの生成

Administration Console と UDS の Web アーカイブを含む単一の EAR ファイルを作成するには、以下の手順に従います。

1. < *インストール先ディレクトリ* >/arcot/tools/bundlemanager ディレクトリに移動します。
2. bundlemanager ツールを実行し、以下のコマンドを使用して EAR ファイルを作成します。

```
java -jar bundle-manager.jar  -ear < ファイル名 .ear> -warList
arcotuds.war arcotadmin.war
```

上記のコマンドを実行すると、EAR ファイルが < *インストール先ディレクトリ* >/arcot/java/webapps に生成されます。

ユーザ データ サービスの展開

ユーザ データ サービス（UDS）を展開するには、arcotuds.war ファイルが必要です。

ユーザ データ サービスを展開する方法

1. 作業ディレクトリを以下のディレクトリに変更します。

   < *インストール先ディレクトリ* >/arcot/sbin
2. 「../arctenv」と入力して **Enter** キーを押し、Arcot 環境変数を設定します。
3. アプリケーション サーバ上の < *インストール先ディレクトリ* >/arcot/java/webapps にある 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 ベンダーが提供するドキュメントを参照してください。

4. （**WebSphere のみ**）アプリケーション ファイルの更新時に UDS を再ロードするように設定します。
   a. ［**Application**］の［**Enterprise Applications**］に移動し、UDS の設定ページを表示します。
   b. ［**Class loader order**］で［**Classes loaded with local class loader first (parent last)**］オプションを選択します。
   c. ［**WAR class loader policy**］で［**Single class loader for application**］を選択します。
   d. ［**Apply**］をクリックして、変更内容を保存します。
5. UDS 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。

a. 次のディレクトリに移動します。

< インストール先ディレクトリ >/arcot/logs

b. 任意のエディタで arcotuds.log ファイルを開き、以下の行を探します。

- UDS Initialized successfully
- Starting Arcot User Data Service (Version: 1.0.8)

注 : また、ログ ファイルに FATAL と WARNING のメッセージが記録されていない点も確認してください。

Administration Console の展開

WebFort Administration Console を展開するには、arcotadmin.war ファイルが必要です。

注 : Administration Console を使用して WebFort サーバを管理するには、WebFort サーバがインストールされているシステムに Administration Console からホスト名を指定してアクセスできることが必要です。

Administration Console を展開する方法

1. アプリケーション サーバ上の *< インストール先ディレクトリ >*/arcot/java/webapps にある arcotadmin.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 ベンダーが提供するドキュメントを参照してください。

2. Administration Console 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。

a. 次のディレクトリに移動します。

< インストール先ディレクトリ >/arcot/logs

b. 任意のエディタで arcotadmin.log ファイルを開き、以下の行を探します。

```
Arcot Administration Console v1.0.8

Arcot Administration Console Configured Successfully
```

注： また、ログ ファイルに FATAL と WARNING のメッセージが記録されていない点も確認してください。

Administration Console へのログイン方法

Administration Console への初回ログイン時には、インストール中にデータベースに自動作成された Master Administrator のクレデンシャルを使用する*必要があります*。

Administration Console にログインする方法

1. 以下の URL にアクセスし、Web ブラウザ ウィンドウで Administration Console を起動します。

   http://< ホスト >:< ポート >/arcotadmin/masteradminlogin.htm

   注： 上記の URL 中のホストとポートの情報には、Administration Console の展開先アプリケーション サーバの情報を指定する必要があります。

2. デフォルトの Master Administrator アカウント クレデンシャルを使用して Master Administrator として Administration Console にログインします。以下のクレデンシャルを使用します。
   - **ユーザ名** *: masteradmin*
   - **パスワード** *: master1234!*

システムのブートストラップ

Administration Console を使用して WebFort の管理を始める前に、以下の必須手順を実行してシステムを初期化する必要があります。

- デフォルトの Master Administrator パスワードを変更する
- UDS 接続パラメータを設定する
- デフォルトの組織の認証メカニズムを指定する

ブートストラップとは、これらの設定作業をウィザードに従って行うプロセスを指します。これらの作業の実行後、他の管理業務用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、以下の関連概念について理解しておく必要があります。

- ユーザ データ サービス（UDS）
- デフォルトの組織

ユーザ データ サービス（UDS）

ユーザ データ サービス（UDS）により、組織が展開したサードパーティ製データ リポジトリ（LDAP ディレクトリ サーバ）へのアクセスが可能になります。その結果、WebFort サーバおよび Administration Console から既存のデータにシームレスにアクセスできるようになります。LDAP ディレクトリ サーバが設定されていない場合は、WebFort データベースにアクセスしてユーザ情報を読み取ります。UDS から他の WebFort コンポーネントに接続する場合に設定する必要があるパラメータについては、ブートストラップ手順の手順 3 を参照してください。

デフォルトの組織

Administration Console を展開すると、組織が 1 つデフォルトで作成されます。この組織は「デフォルトの組織」（DEFAULTORG）として参照されます。デフォルトの組織自体を単一組織のシステムとして、新しい組織を作成せずに使用できます。

ブートストラップ タスクの実行

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

図 4-1 ブートストラップ ウィザード：［Summary］画面

ウィザードを使用してシステムのブートストラップを行う方法

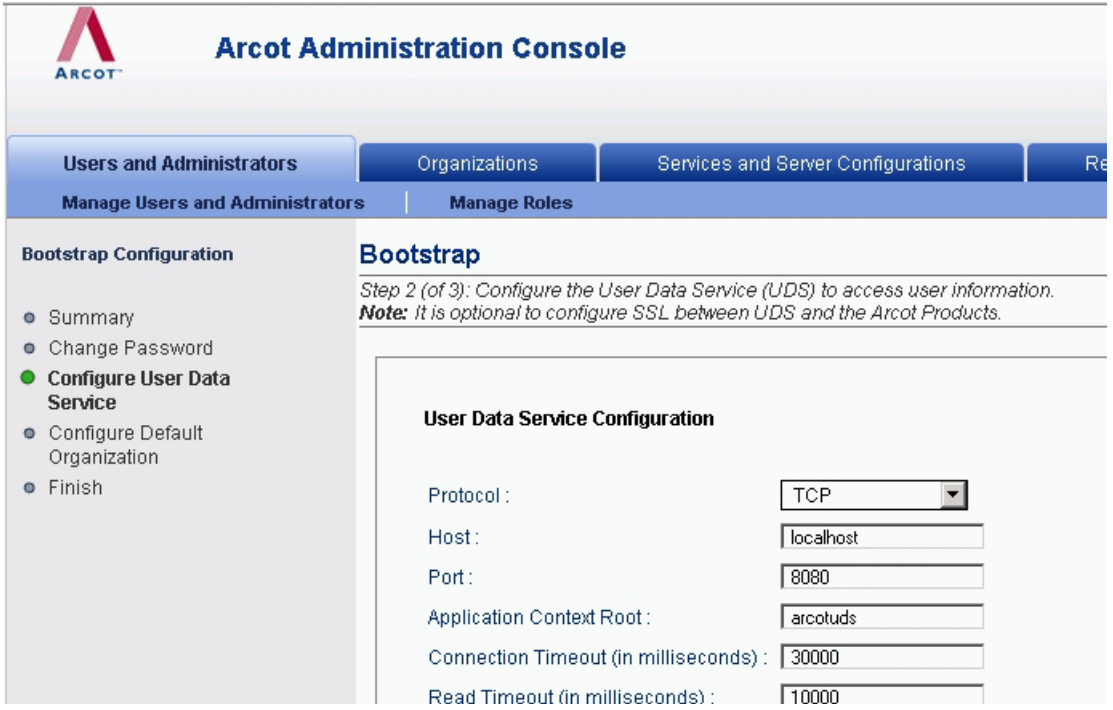
1. ［**Begin**］をクリックすると、プロセスが開始します。
   ［Change Password］画面（図 4-2）が表示されます。

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

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

   ［Configure User Data Service］画面（図 4-3）が表示されます。

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



3. 表 4-3 に記載のパラメータを指定して、UDS を設定します。

表 4-3. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Protocol	TCP	Administration Console を使用して UDS に接続するためのプロトコル。選択肢は以下のとおりです。 • TCP • One way SSL • Two way SSL
Host	localhost	UDS が展開されているアプリケーション サーバのホスト名または IP アドレス。
Port	8080	アプリケーション サーバが利用可能なポート。
App Context Root	arcotuds	アプリケーション サーバで UDS を定義するために使用されるタグ。たとえば、*http://< ホスト >:< ポート >/arcotuds/services* URL のコンテキスト ルートは `arcotuds` です。
Connection Timeout	30000	ここで指定した最長時間（ミリ秒単位）が経過すると、UDS サービスが到達不能と判断されます。
Read Timeout	10000	ここで指定した最長時間（ミリ秒単位）が経過するまでの間、UDS からの応答を待機します。
Idle Timeout	30000	ここで指定した最長時間（ミリ秒単位）が経過すると、アイドル状態の接続が閉じられます。
Server Root Certificate	デフォルト値なし	UDS サーバの CA 証明書ファイルをアップロードします。このファイルは PEM 形式です。
Client Root Certificate	デフォルト値なし	WebFort サーバの CA 証明書ファイルをアップロードします。このファイルは PEM 形式です。
Client Private Key	デフォルト値なし	CA の秘密キーが含まれるファイルの場所。
Minimum Connections	4	WebFort サーバと UDS 間で作成される接続の最小数。
Maximum Connections	32	WebFort サーバと UDS 間で作成される接続の最大数。

［Configure Default Organization］画面（図 4-4）が表示されます。

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

4. デフォルトの組織について以下のパラメータを指定します。
   - ［**Display Name**］：組織をわかりやすく示す名前。この名前が Administration Console の他のすべてのページやレポートに表示されます。
   - ［**Authentication Mechanism**］：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。Administration Console では、管理者のログイン時の認証方式として以下の 2 種類がサポートされています。
     - **Basic User Password**

       このオプションを選択した場合は、Administration Console に組み込みの認証方式を使用して管理者が認証されます。
     - **WebFort User Password**

       ここで［**WebFort User Password**］オプションを選択した場合は、WebFort サーバによってクレデンシャルが発行され、認証されます。具体的な方法の詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

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

図 4-5 ブートストラップ ウィザード：［Finish］画面

5. Administration Console を使用して他の設定を続ける場合は、［**Continue**］をクリックします。

WebFort サーバの起動

WebFort サーバを起動するには、以下の手順に従います。

1. 以下のディレクトリに移動します。

   < インストール先ディレクトリ >/arcot/bin/

2. 以下のコマンドを実行します。

```
./webfortserver start
```

注： サーバを停止する場合は、./webfortserver stop コマンドを実行します。

インストールの確認

以下の方法で WebFort サーバおよび Web アプリケーションが正常に起動したかどうかを確認できます。

- ログ ファイルの使用

ログ ファイルの使用

WebFort 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. 次のディレクトリに移動します。

   < インストール先ディレクトリ >/arcot/logs

2. 任意のエディタで arcotwebfortstartup.log ファイルを開き、以下の行を探します。

```
INSTANCE_VER.................................: [6.2]
Arcot WebFort Authentication Service READY
```

注 : また、ログ ファイルに FATAL と WARNING のメッセージが記録されていない点も確認してください。

webfortserver の使用

webfortserver ツールを使用して、インストールした WebFort のバージョンを確認できます。このツールの詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

WebFort のバージョンを確認するには、以下の手順に従います。

1. 次のディレクトリに移動します。

   < インストール先ディレクトリ >/arcot/bin

2. 以下のオプションを指定して webfortserver を実行し、ツールを対話モードで実行します。

```
webfortserver -i
```

3. プロンプトに「version」と入力します。

   webfort-ver-<dd>-<mmm>-<yy>.txt ファイルが *< インストール先ディレクトリ >*/arcot/logs フォルダに作成されます。

4. このファイルを開き、ライブラリ ファイルのバージョンが 6.2 かどうかを確認します。

ポートの確認

WebFort サーバがデフォルト ポート上の各種プロトコルをリスニング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. 次のディレクトリに移動します。

   < インストール先ディレクトリ >/arcot/logs

2. 任意のエディタで arcotwebfortstartup.log ファイルを開き、以下の行を探します。

```
PROTOCOLNAME : [Administration-WS]
PORTNO : 9745
PROTOCOLID : [ASSP-WS]
PORTNO : 9741
PROTOCOLID : [Authentication-Native]
PORTNO : 9742
PROTOCOLID : [Authentication-RADIUS]
PORTNO : 1812
PROTOCOLID : [ServerManagement-WS]
PORTNO : 9743
PROTOCOLID : [Transaction-HTTP]
PORTNO : 9746
PROTOCOLID : [Transaction-WS]
PORTNO : 9744
```

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

サンプル アプリケーションの展開

WebFort のテスト時に、または ArcotID および他の認証方式を既存の Web アプリケーションに統合する場合のコード例として、サンプル アプリケーションを使用できます。

サンプル アプリケーションを展開する方法

1. 以下の場所から `webfort-6.2-sample-application.war` ファイルを展開します。

   < インストール先ディレクトリ >`/arcot/samples/java`

2. 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://< ホスト >:< ポート >/webfort-6.2-sample-application/

第 5 章
分散システムでの WebFort の展開

この章では、分散システム環境または高可用性環境での WebFort のインストールおよび設定について説明します。

次の一覧にプロセスの概要を示します。

- WebFort 6.2 インストーラを実行して、ファイル システムに WebFort サーバおよび Administration Console を追加し、SQL データベースにアクセスするよう設定します。インストール手順については、「最初のシステムへのインストール」を参照してください。
- データベース スクリプトを実行して、スキーマとデータベース テーブルを作成します。「データベース スクリプトの実行」を参照してください。
- アプリケーション サーバに Web ベースのアプリケーションを展開します。「Web アプリケーションの展開」を参照してください。
- Master Administrator として Administration Console にログインして、システムをブートストラップします。詳細については、「WebFort サーバの起動」を参照してください。
- 1 つ以上のシステムに Java SDK 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。
- サンプル アプリケーションを展開します。詳細については、「サンプル アプリケーションの展開」を参照してください。

WebFort 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。分散システム環境では、*カスタム*のインストール タイプを使用する必要があります。

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

最初のシステムへのインストール

このセクションでは、分散システム環境または高可用性環境での WebFort のインストールについて説明します。インストールでは、必ず Administrators グループに属するアカウントを使用してください。それ以外のアカウントを使用した場合、インストールがエラーなしで完了した場合でも、WebFort によるサービスの作成など、インストールにおける一部の重要な手順が正常に行われません。

WebFort をインストールする前に、第 3 章の「インストールの準備」の説明に従って、すべての必須ソフトウェアをインストールしてデータベースを設定するようにしてください。

注： WebFort インストーラを実行する前に、必ず `PATH` 環境変数に `<JAVA_HOME>/bin` を設定してください。設定しない場合、`arcotadmin.war` ファイルの生成に失敗することがあります。

WebFort および関連するコンポーネントをインストールするには、以下の手順に従います。

1. WebFort インストーラの `Arcot-WebFort-6.2-<`*プラットフォーム名*`>-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。

   ```
   prompt> sh Arcot-WebFort-6.2-<プラットフォーム名>-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. `root` としてログインし、インストーラを実行している場合は、「You are installing as root」という警告メッセージが表示されます。インストールを続行するには「**Y**」を、インストールを中止するには「**N**」を入力します。必要な情報を指定したら、**Enter** キーを押して次に進みます。

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

   WebFort の使用許諾契約が表示されます。
5. **Enter** キーを押して、使用許諾契約を最後まで表示します。

   使用許諾契約の最後で、契約に同意するかどうかを確認するプロンプトが表示されます。
6. 使用許諾契約に同意する場合は、「**Y**」を入力してインストールを続行します。

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

7. インストールを実行するフォルダの絶対パスを入力します。または、**Enter** キーを押して、表示されたデフォルト パスを使用します。

注： 指定するインストール フォルダ名にはスペースを使用できません。スペースを使用すると、意図したとおりに WebFort スクリプトおよびツールが機能しないからです。

8. インストールするシステムにすでに Arcot 製品がある場合、インストーラは以下のオプションを表示します。
   a. 1 - 新しい場所を入力する。
   b. 2 - 手順 7 で選択したフォルダ内にインストールを続行する。
   c. 3 - 既存の Arcot 製品がインストールされている場所を使用する。
9. 上記のオプションのいずれかを選択し、**Enter** キーを押してインストールを続行します。

注： オプション 1 または 2 を選択したら、新規フォルダ `arcot` が指定された場所に作成されます。

［Installation Type］画面が表示されます。

10. この画面には、WebFort によって提供されるインストール タイプが表示されます。「**2**」を入力して、WebFort の選択したコンポーネントをインストールします。

［Choose Product Features］画面が表示されます。

11. この画面には、すべての WebFort の機能が表示されます。インストールする機能に対応する番号を入力します。

通常、最初のシステムでは、WebFort サーバ、Administration Console およびユーザ データ サービスをインストールします。**Enter** キーを押して続行します。

［Database Type］画面が表示されます。

12. この画面にはデータベースのタイプが表示されます。データベース タイプの番号を入力し、**Enter** キーを押して次に進みます。

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

13. この画面にはデータベースのタイプが表示されます。データベース タイプの番号を入力し、**Enter** キーを押して次に進みます。

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

14. プライマリ DSN の情報を入力します。表 5-1 では必要なデータベースの詳細情報について説明します。

表 5-1. プライマリ Oracle データベースのパラメータ

フィールド	説明
［Primary ODBC DSN］	インストーラにより、WebFort が Arcot データベースに接続するために使用する 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 WebFort 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。
［Password］	データベースにアクセスするために WebFort 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 No］	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。
［Host Name］	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

15. インストーラから、バックアップ DSN を設定するようリクエストされます。バックアップ DSN を設定する場合は「**Y**」を、バックアップ データベースの設定をスキップする場合は「**N**」を入力して、次に進みます。

16. 必要に応じて、バックアップ DSN の情報を入力します。表 5-2 では必要なデータベースの詳細情報について説明します。

表 5-2. バックアップ Oracle データベースのパラメータ

フィールド	説明
［Backup ODBC DSN］	インストーラにより、WebFort が Arcot データベースに接続するために使用する ODBC 接続が作成されます。推奨される入力値は *arcotdsnbkp* です。 **注：** プライマリ DSN とバックアップ DSN の DSN 名は異なる必要があります。
［User Name］	データベースにアクセスするために WebFort 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：** プライマリ DSN とバックアップ DSN のユーザ名は異なる必要があります。
［Password］	データベースにアクセスするために WebFort 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 No］	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。
［Host Name］	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

［Pre-Installation Summary］画面が表示されます。この画面には製品名、インストール フォルダ、インストールのタイプ、選択したコンポーネント、およびディスク容量についての情報が表示されます。

17. インストール設定を変更する場合は、「**back**」と入力します。変更の必要がない場合は、**Enter** キーを押してインストールを進めます。

    ［Ready to Install］画面が表示されます。

18. **Enter** キーを押して、インストール プロセスを開始します。

    ［Installing］画面が表示されます。数分かかる場合があります。

    インストールが正常に行われたら、インストールの完了を示す画面が表示されます。

19. **Enter** キーを押してインストーラを終了します。

    プロンプトが再度表示されるまで、（インストーラがテンポラリ ファイルをクリーンアップするため）数分間待機する必要がある場合があります。

注： インストール アクティビティを表示するには、< *インストール場所* >/arcot/logs/ でログ ファイル Arcot_WebFort_InstallLog.log を参照してください。

最初のシステムにおける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. Web アプリケーションの展開
3. Administration Console へのログイン方法
4. システムのブートストラップ
5. WebFort サーバの起動
6. インストールの確認

注： これらのインストール後のタスクを完了した後に、第 6 章の「Java SDK および Web サービスの設定」で説明されている Java SDK および Web サービス設定を実行します。

データベース スクリプトの実行

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

WebFort で使用されるデータベースの設定方法

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

   （Oracle の場合）< *インストール場所* >/arcot/dbscripts/oracle

   （DB2 の場合）< *インストール場所* >/arcot/dbscripts/db2

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-1.0.sql

b. `arcot-db-config-for-webfort-6.2.sql`

注： スクリプトの実行中にエラーが発生する場合は、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。

Web アプリケーションの展開

このセクションでは、ユーザ データ サービスおよび Administration Console で必要なファイルをコピーし、これらのアプリケーションの WAR ファイルを展開する手順について説明します。

- アプリケーション サーバの準備
- （オプション）Enterprise Archive ファイルの作成
- ユーザ データ サービスの展開
- Administration Console の展開

アプリケーション サーバの準備

このサブセクションでは、以下のアプリケーション サーバに Arcot ファイル `libArcotAccessKeyProvider.so` および `arcot-crypto-util.jar` ファイルをコピーする手順を示します。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

`libArcotAccessKeyProvider.so` ライブラリ ファイルは以下の場所にあります。

`<` *インストール場所* `>/arcot/Java/ext/<` *プラットフォーム名* `>/32bit/`

`arcot-crypto-util.jar` ファイルは以下の場所にあります。

`<` *インストール場所* `>/arcot/java/ext/`

Apache Tomcat

Arcot ファイルをコピーするには、以下の手順に従います。

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

Solaris の場合：

`<JAVA_HOME>/jre/lib/sparc`

RHEL の場合：

`<JAVA_HOME>/jre/bin`

2. `arcot-crypto-util.jar` ファイルを `<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. Tomcat を再起動します。

IBM WebSphere

WebSphere 6.1 に Arcot ファイルをコピーするには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［**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、有効な可視性スコープを選択します。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、*< インストール場所 >*`/arcot/java/ext/arcot-crypto-util.jar`。
   e. JNI のライブラリ パスを入力します。このパスは、`libArcotAccessKeyProvider.so` ファイルが存在する場所を指している必要があります。
   f. ［**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。
   a. ［**Servers**］をクリックしてから、［**Application Servers**］をクリックします。
   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［**Class Loader 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**］をクリックして、［ArcotJNI］を選択してから、［**Apply**］をクリックします。

h. 変更内容を保存します。

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

Solaris の場合：

`<JAVA_HOME>/jre/lib/sparc`

RHEL の場合：

`<JAVA_HOME>/jre/bin`

5. WebSphere を再起動します。

BEA WebLogic

Arcot ファイルをコピーするには、以下の手順に従います。

1. 以下の WebLogic ディレクトリに `libArcotAccessKeyProvider.so` をコピーします。

Solaris の場合：

`<JAVA_HOME>/jre/lib/sparc`

RHEL の場合：

`<JAVA_HOME>/jre/bin`

2. `arcot-crypto-util.jar` を WebLogic の *<WebLogic のインスタンスで使用する JAVA_HOME>*`\jre\lib\ext` にコピーします。

注： WebLogic で使用する適切な *<JAVA_HOME>* を使用するようにしてください。

3. WebLogic 管理者コンソールにログインします。
4. ［**Deployments**］に移動します。
5. ［**Lock and Edit**］オプションを有効にします。
6. ［**Install**］をクリックして、`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。
7. ［**Next**］をクリックします。

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

   ［Summary］ページが表示されます。
9. ［**Finish**］をクリックします。
10. 変更内容を有効化します。
11. WebLogic サーバを再起動します。

（オプション）Enterprise Archive ファイルの作成

WebFort には、Administration Console およびユーザ データ サービス（UDS）を展開するための Web ARchive （WAR）ファイルがデフォルトで付属しています。また、これらのファイルの形式を Enterprise ARchive （EAR）に変更し、EAR ファイルを展開できます。

個別の EAR ファイルの生成

Administration Console 用またはユーザ データ サービス用の EAR ファイルを作成するには、以下の手順に従います。

1. *<インストール場所>*`/arcot/tools/bundlemanager` ディレクトリに移動します。
2. 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。

   ユーザ データ サービスの場合

```
java -jar bundle-manager.jar  -ear <ファイル名 .ear> -warList
arcotuds.war
```

Administration Console の場合

```
java -jar bundle-manager.jar  -ear <ファイル名 .ear> -warList
arcotadmin.war
```

上記のコマンドで EAR ファイルが生成されます。ファイルは <*インストール場所*> /arcot/java/webapps に配置されます。

単一の EAR ファイルの生成

Administration Console および UDS Web アーカイブが含まれる単一の EAR ファイルを作成するには、以下の手順に従います。

1. <*インストール場所*>/arcot/tools/bundlemanager ディレクトリに移動します。
2. 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 <ファイル名 .ear> -warList
arcotuds.war arcotadmin.war
```

上記のコマンドで EAR ファイルが生成されます。ファイルは <*インストール場所*> /arcot/java/webapps に配置されます。

ユーザ データ サービスの展開

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。

ユーザ データ サービスの展開方法

1. 作業ディレクトリを、次のディレクトリに変更します。

   <*インストール場所*>/arcot/sbin
2. 「../arctenv」と入力し、**Enter** キーを押して Arcot 環境変数を設定します。
3. <*インストール場所*>/arcot/java/webapps にある arcotuds.war をアプリケーション サーバに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 サーバにより異なります。アプリケーション サーバのベンダーのマニュアルで詳細手順を参照してください。

4. （**WebSphere のみ**）アプリケーション ファイルが更新されるときに UDS クラスを再ロードするよう設定します。
   a. ［**Application**］-［**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**］をクリックして、変更を保存します。
5. 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. 次のディレクトリに移動します。

      < *インストール場所* >/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。
      - `UDS Initialized successfully`
      - `Starting Arcot User Data Service (Version: 1.0.8)`

注： ログ ファイルに致命的エラーと警告のメッセージが含まれないように確認することもお勧めします。

Administration Console の展開

WebFort Administration Console を展開するには、ファイル arcotadmin.war が必要です。

注： Administration Console を使用して WebFort サーバを管理するには、WebFort サーバがインストールされたシステムに、Administration Console 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。

Administration Console の展開方法

1. *<インストール場所>*/arcot/java/webapps にある arcotadmin.war をアプリケーション サーバに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 サーバにより異なります。アプリケーション サーバのベンダーのマニュアルで詳細手順を参照してください。

2. Administration Console が正しく開始されたかどうかを確認するには、以下の手順に従います。

   a. 次のディレクトリに移動します。

      <インストール場所>/arcot/logs

   b. 任意のエディタで arcotadmin.log ファイルを開き、以下の行を見つけます。

```
Arcot Administration Console v1.0.8
Arcot Administration Console Configured Successfully
```

注： ログ ファイルに致命的エラーと警告のメッセージが含まれないように確認することもお勧めします。

Administration Console へのログイン方法

初めて Administration Console にログインするときは、インストール時にデータベースで自動的に作成される Master Administrator のクレデンシャルを使用する*必要があります*。

Administration Console にログインする方法

1. 以下の URL を使用して、Web ブラウザ ウィンドウで Administration Console を開始します。

   http://< ホスト >:< ポート >/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、Administration Console が展開す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 Master Administrator のアカウント クレデンシャルを持つ Master Administrator として Administration Console にログインします。クレデンシャルは以下のとおりです。
   - **ユーザ名** *: masteradmin*
   - **パスワード** *: master1234!*

システムのブートストラップ

Administration Console を使用して WebFort を管理できるようにするには、最初にシステムを初期化する以下の手順を実行する必要があります。

- デフォルトの Master Administrator パスワードを変更する
- UDS の接続性パラメータを設定する
- 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、以下の関連概念について理解しておく必要があります。

- ユーザ データ サービス（UDS）
- デフォルトの組織

ユーザ データ サービス（UDS）

ユーザ データ サービス（UDS）により、組織によって展開されたサードパーティのデータ リポジトリ（LDAP ディレクトリ サーバ）へのアクセスが有効になります。その結果、WebFort サーバおよび Administration Console は、シームレスにユーザの既存のデータにアクセスできるようになります。LDAP ディレクトリ サーバが設定されていない場合は、ユーザ情報を読み取るため WebFort データベースにアクセスします。UDS をほかの WebFort コンポーネントに接続するように設定されるパラメータについては、手順 3 のブートストラップの手順を参照してください。

デフォルトの組織

Administration Console 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、新しい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

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

図 5-1 ブートストラップ ウィザード：［Summary］画面

ウィザードを使用して、システムをブートストラップする方法

1. ［**Begin**］クリックすると、プロセスが起動します。

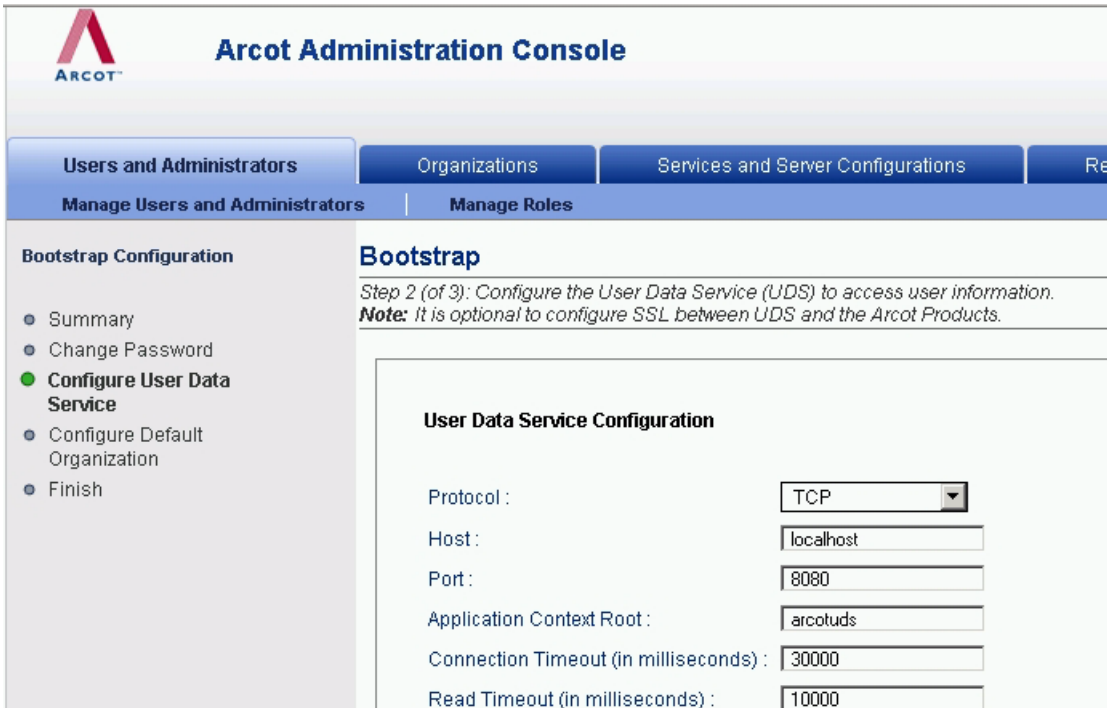
   図 5-2 に示されたとおりに、［Change Password］画面が表示されます。

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

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

   図 5-3 に示されたとおりに、［Configure User Data Service］画面が表示されます。

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



3. 表 5-3 にリスト表示されたパラメータを指定して、UDS を設定します。

表 5-3. UDS 設定パラメータ

パラメータ	デフォルト値	説明
プロトコル	TCP	Administration Console を使用して、UDS に接続するプロトコル。使用可能なオプションは、以下のとおりです。 • TCP • One way SSL • Two way SSL
ホスト	localhost	UDS が展開されているアプリケーション サーバのホスト名または IP アドレス。
ポート	8080	アプリケーション サーバが利用可能なポート。

表 5-3. UDS 設定パラメータ

パラメータ	デフォルト値	説明
App コンテキスト ルート	arcotuds	アプリケーション サーバで UDS を定義するために使用されるタグ。たとえば、URL *http://< ホスト >:< ポート >/arcotuds/services* のコンテキスト ルートは `arcotuds` です。
接続タイムアウト	30000	UDS サービスが到達不能になるまでのミリ秒単位の最大時間。
Read Timeout	10000	UDS からのレスポンスを待機する最大時間（ミリ秒単位）。
アイドル タイムアウト	30000	アイドル接続が閉じられるまでのミリ秒単位の最大時間。
Server Root Certificate	デフォルト値なし	UDS サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式です。
Client Root Certificate	デフォルト値なし	WebFort サーバの CA 証明書ファイルをアップロードします。ファイルは PEM 形式です。
Client Private Key	デフォルト値なし	CA の秘密キーが含まれるファイルの場所。
Minimum Connections	4	WebFort サーバと UDS の間で作成される接続の最小数。
Maximum Connections	32	WebFort サーバと UDS の間で作成できる接続の最大数。

図 5-4 に示されたとおりに、［Configure Default Organization］画面が表示されます。

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

4. デフォルトの組織についての以下のパラメータを指定します。

   - **Display Name**：組織の記述名。この名前がほかのすべての Administration Console ページおよびレポート上に表示されます。
   - **Authentication Mechanism**：デフォルトの組織に属する管理者を認証するために使用されるメカニズム。Administration Console は、管理者がログインするために以下の 2 つのタイプの認証方式をサポートしています。
     - **Basic User Password**

       このオプションを選択すると、Administration Console によって提供される inbuilt 認証方式が管理者を認証するために使用されます。
     - **WebFort User Password**

       ユーザがここで［**WebFort User Password**］オプションを選択すると、WebFort サーバによってクレデンシャルが発行されて認証されます。これを実行する方法の詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

   ［Finish］画面（図 5-5）示されるとおりに、Administration Console の初期化が完了します。

図 5-5 ブートストラップ ウィザード：［Finish］画面

5. ［**Continue**］をクリックして、Administration Console を使用するほかの設定に進みます。

WebFort サーバの起動

WebFort サーバを起動するには、以下の手順に従います。

1. 以下のディレクトリに移動します。

   <インストール場所>/arcot/bin/

2. 以下のコマンドを実行します。

```
./webfortserver start
```

注： サーバを停止する場合は、`./webfortserver stop` コマンドを実行します。

インストールの確認

以下により、WebFort サーバおよび Web アプリケーションが正常に開始したかどうかを確認できます。

- ログ ファイルの使用

- webfortserver の使用
- ポートの確認

ログ ファイルの使用

WebFort サーバ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。

1. 次のディレクトリに移動します。

   <インストール場所>/arcot/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.................................: [6.2]
Arcot WebFort Authentication Service READY
```

注： ログ ファイルに致命的エラーと警告のメッセージが含まれないように確認することもお勧めします。

webfortserver の使用

webfortserver ツールを使用して、インストールした WebFort のバージョンをチェックできます。このツールの詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

WebFort のバージョンを確認するには、以下の手順に従います。

1. 次のディレクトリに移動します。

   <インストール場所>/arcot/bin

2. 以下のオプションを指定して webfortserver を実行し、対話モードでツールを開始します。

```
webfortserver -i
```

3. プロンプトで「version」と入力します。

   webfort-ver-<dd>-<mmm>-<yy>.txt ファイルは、*<インストール場所>*/arcot/logs フォルダに作成されます。

4. このファイルを開き、ライブラリ ファイルのバージョンが 6.2 であるかどうかを確認します。

ポートの確認

WebFort サーバがデフォルト ポートの別のプロトコルを待ち受け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. 次のディレクトリに移動します。

   <インストール場所>/arcot/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。

```
PROTOCOLNAME : [Administration-WS]
PORTNO : 9745
PROTOCOLID : [ASSP-WS]
PORTNO : 9741
PROTOCOLID : [Authentication-Native]
PORTNO : 9742
PROTOCOLID : [Authentication-RADIUS]
PORTNO : 1812
PROTOCOLID : [ServerManagement-WS]
PORTNO : 9743
PROTOCOLID : [Transaction-HTTP]
PORTNO : 9746
PROTOCOLID : [Transaction-WS]
PORTNO : 9744
```

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

2 つ目のシステムへのインストール

WebFort サーバ、Administration Console およびユーザ データ サービスをインストールした後に、この分散システム環境の 2 つ目のシステム上にほかのコンポーネントをインストールする必要があります。第 2 章の「展開の計画」の計画を実行していれば、インストールするコンポーネントが決定されています。

インストールを開始する前に、第 3 章の「インストールの準備」に記載されているように、必須のソフトウェア コンポーネントがすべてこのシステムにインストールされていることを確認します。

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

1. WebFort インストーラの `Arcot-WebFort-6.2-<`*プラットフォーム名*`>-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。

   ```
   prompt> sh Arcot-WebFort-6.2-<プラットフォーム名>-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. 手順 3 から 手順 10 までのインストーラの手順に従います。
4. ［Choose Product Features］画面で、インストールするコンポーネントを選択します。通常、SDK およびサンプル アプリケーションをインストールします。
5. コンポーネントを選択したら、インストールを完了するために手順 12 から手順 19 までの手順に従います。

2 つ目のシステムにおけるインストール後のタスク

Java SDK、Web サービスおよびサンプル アプリケーションをインストールした 2 つ目のシステムで、以下のインストール後のタスクを実行します。

- サンプル アプリケーションの展開
- WebFort サーバ用のサンプル アプリケーションの設定

サンプル アプリケーションの展開

サンプル アプリケーションは、WebFort のテストに使用したり、ArcotID と既存の Web アプリケーションに対するほかの認証方式を統合するためのコード サンプルとして使用したりできます。

サンプル アプリケーションの展開方法

1. 以下の場所から `webfort-6.2-sample-application.war` ファイルを展開します。

   <インストール場所>`/arcot/samples/java`

2. 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。サンプル アプリケーションのデフォルト URL は次のとおりです。

   http://< ホスト >:< ポート >/webfort-6.2-sample-application/

WebFort サーバ用のサンプル アプリケーションの設定

サンプル アプリケーションが別のシステム上にインストールされる場合、WebFort サーバと通信するためにサンプル アプリケーションを設定する必要があります。これを行うには、以下の手順に従います。

1. 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。サンプル アプリケーションのデフォルト URL は次のとおりです。

   http://< ホスト >:< ポート >/webfort-6.2-sample-application/

   ［WebFort 6.2 Sample Application］ページが表示されます。

2. ［**Setup**］リンクをクリックします。
3. 表 5-4 にリスト表示されている接続パラメータに値を指定します。

注： これらのパラメータを使用して作成された設定は、現在のセッションに有効です。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する必要があります。

表 5-4. 接続パラメータ

フィールド	デフォルト値	説明
[Logger Configuration]		
[Log File Path]	./arcotwebfortsampleapp.log	サンプル アプリケーション ログ ファイルへの相対パス。このパスは通常アプリケーション サーバのメイン ディレクトリを指しています。
[Server Configuration]		
[IP Address]	localhost	WebFort 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。
[Port]	**Authentication Service:** 9742 **Issuance Service:** 9744	認証サービスまたは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。

4. ［**Set Up**］をクリックして、接続を保存します。

サンプル アプリケーションを設定して追加の WebFort サーバ インスタンスと通信する方法

1. ［**Additional Server Configuration**］の前にある［**+**］記号をクリックします。
2. ［**IP Address**］および［**Port**］接続パラメータを指定します。
3. ［**Set Up**］をクリックして、接続を設定します。

第 6 章
Java SDK および Web サービスの設定

この章では、WebFort で提供される Java SDK（Software Development Kit）および Web サービスの設定手順について説明します。

Java SDK の設定

ここでは、認証 Java SDK と発行 Java SDK を既存のアプリケーションと統合できるように設定する手順について説明します。

認証 Java SDK の設定

設定を進める前に、認証 Java SDK パッケージが WebFort のインストール中に正常にインストールされていることを確認してください。

J2EE アプリケーションで使用するために認証 SDK を設定する方法

1. 以下の JAR ファイルを
   <install_location>/arcot から
   <ApplicationHome>/WEB-INF/lib ディレクトリにコピーします。
   - sdk/java/lib/arcot/arcot-pool.jar
   - sdk/java/lib/arcot/arcot-webfort-authentication.jar
   - sdk/java/lib/arcot/arcot-webfort-common.jar
   - sdk/java/lib/external/bcprov-jdk14-139.jar
   - sdk/java/lib/external/commons-httpclient-3.1.jar
   - sdk/java/lib/external/commons-lang-2.4.jar
   - sdk/java/lib/external/commons-pool-1.4.jar
   - sdk/java/lib/external/log4j-1.2.9.jar

2. サーバ接続パラメータが指定されている webfort.authentication.properties 設定ファイルを *<install_location>*\Arcot Systems\sdk\java\properties*<install_location>*/arcot/sdk/java/properties から *<ApplicationHome>*/WEB-INF/classes/properties にコピーします。

注： API とそれらの初期化に関する詳細については、「*Arcot WebFort 6.2 Java 開発者ガイド*」および *<install_location>*/arcot/docs/webfort/Arcot-WebFort-6.2-authentication-sdk-javadocs.zip にある WebFort Javadoc を参照してください。

Web サービスの設定

Web サービスを使用している場合は、*<install_location>*/arcot/wsdls/webfort にある ArcotWebFortAuthSvc.wsdl ファイルを使用してクライアントを生成します。

発行 Java SDK の設定

設定を進める前に、発行 Java SDK パッケージが WebFort のインストール中に正常にインストールされていることを確認してください。

J2EE アプリケーションで使用するために発行 SDK を設定する方法

1. 以下の JAR ファイルを *<install_location>*\Arcot Systems*<install_location>*/arcot から *<ApplicationHome>*/WEB-INF/lib ディレクトリにコピーします。
   - sdk/java/lib/arcot/arcot-pool.jar
   - sdk/java/lib/arcot/arcot-webfort-common.jar
   - sdk/java/lib/arcot/arcot-webfort-issuance.jar
   - sdk/java/lib/external/activation-1.1.jar
   - sdk/java/lib/external/axiom-api-1.2.7.jar
   - sdk/java/lib/external/axiom-impl-1.2.7.jar
   - sdk/java/lib/external/axis2-adb-1.4.jar
   - sdk/java/lib/external/axis2-java2wsdl-1.4.jar
   - sdk/java/lib/external/axis2-kernel-1.4.jar
   - sdk/java/lib/external/backport-util-concurrent-2.2.jar
   - sdk/java/lib/external/bcprov-jdk14-139.jar
   - sdk/java/lib/external/commons-codec-1.3.jar

- sdk/java/lib/external/commons-collections-3.1.jar
- sdk/java/lib/external/commons-httpclient-3.1.jar
- sdk/java/lib/external/commons-lang-2.4.jar
- sdk/java/lib/external/commons-logging-1.1.jar
- sdk/java/lib/external/commons-pool-1.4.jar
- sdk/java/lib/external/geronimo-jms_1.1_spec-1.1.jar
- sdk/java/lib/external/log4j-1.2.9.jar
- sdk/java/lib/external/neethi-2.0.jar
- sdk/java/lib/external/stax-api-1.0.1.jar
- sdk/java/lib/external/wsdl4j-1.6.2.jar
- sdk/java/lib/external/wstx-asl-3.2.0.jar
- sdk/java/lib/external/XmlSchema-1.2.jar

2. サーバ接続パラメータが指定されている webfort.issuance.properties 設定ファイルを *<install_location>*/arcot/sdk/java/properties から *<ApplicationHome>*/WEB-INF/classes/properties にコピーします。

注： API とそれらの初期化に関する詳細については、「*Arcot WebFort 6.2 Java 開発者ガイド*」および *<install_location>*/arcot/docs/webfort/Arcot-WebFort-6.2-issuance-sdk-javadocs.zip にある発行 Javadoc を参照してください。

Web サービスの設定

Web サービスを使用している場合は、*<install_location>*/arcot/wsdls/webfort にある ArcotWebFortIssuanceSvc.wsdl ファイルを使用してクライアントを生成します。

SSL 通信の有効化

WebFort は、WebFort サーバおよび Java SDK 間の SSL（Secure Socket Layer）をサポートしています。付録 F の 「SSL 用の設定」では、転送モードを WebFort サーバとクライアント間の SSL に設定する方法を説明しています。

第 7 章
WebFort のアンインストール

この章では、WebFort および関連コンポーネントのアンインストール手順について説明します。この章の内容は以下のとおりです。

WebFort スキーマのアンインストール

データベースから WebFort スキーマをアンインストールする方法

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。

   Oracle の場合：< *インストール先ディレクトリ* >/arcot/dbscripts/oracle

   DB2 の場合：< *インストール先ディレクトリ* >/arcot/dbscripts/db2

2. スクリプトを*次に示す順序*で実行します。

   a. drop-webfort-6.2.sql

   b. drop-arcot-common-1.0.sql

      これでデータベース テーブルがすべて削除されます。

WebFort のアンインストール

WebFort をアンインストールするには、以下の手順に従います。

1. WebFort サーバを停止します。
2. WebFort のインストール中に作成された DSN エントリを削除します。

このエントリを削除するには、odbc.ini ファイルの保存先に移動してテキスト エディタでこのファイルを開き、対応するデータベース エントリを削除します。odbc.ini ファイルは、次の場所に保存されています。

< *インストール先ディレクトリ* >/arcot/odbc32v60wf/odbc.ini

3. 該当する INI ファイルが別のエディタで開いていないことを確認します。
4. 以下のディレクトリに移動します。

```
prompt> cd < インストール先ディレクトリ >/arcot/Uninstall_Arcot WebFort
```

5. 次のコマンドを使用してインストーラを実行します。

```
prompt> Uninstall_Arcot WebFort
```

［Uninstall Options］画面が表示されます。

6. アンインストール方法を選択します。
   - **［1-Completely remove all features and components］:** 現在のシステム上の WebFort のコンポーネントをすべてアンインストールする場合は、このオプションを選択します。
   - **［2-Choose specific features that were installed by InstallAnywhere］:** 現在のシステム上の選択した WebFort コンポーネントのみをアンインストールする場合は、このオプションを選択します。この場合、他のシステム上の残りのコンポーネントを別途アンインストールする必要があります。
7. **Enter** キーを押して続行します。

   すべてのコンポーネントをアンインストールするオプションを選択した場合は、手順 9 に進みます。

   選択したコンポーネントをアンインストールするオプションを選択した場合は、［Choose Product Features］画面が表示されます。

   ［Choose Product Features］画面が表示されます。
8. **（特定のコンポーネントのアンインストール時のみ）** この画面には、システム上にインストールされている WebFort コンポーネントが表示されます。コンポーネント番号を（カンマで区切って）入力し、**Enter** キーを押します。

   アンインストールが正常に終了すると、最後に *［Uninstall Complete］* 画面が表示されます。

9. **Enter** キーを押して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` 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`：Administration Console
   - `arcotuds`：ユーザ データ サービス
   - `webfort-6.2-sample-application`：サンプル アプリケーション

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。

付録 A
WebFort ファイル システム構造

この章は、WebFort インストーラによってインストールされるすべてのファイルの場所に関する情報が記載されています。

重要 : WebFort によってインストールされるファイルを削除しないでください。

- WebFort サーバ ファイル
- Administration Console のファイル
- ユーザ データ サービスのファイル
- 認証 Java SDK ファイル
- 発行 Java SDK ファイル
- WSDL ファイル
- Plug-In SDK

WebFort サーバ ファイル

表 A-1 には、WebFort サーバによって使用されるファイルのフォルダの場所がリストされています。

表 A-1. WebFort サーバ ファイル

フォルダ	ファイル説明
<*install_location*>/	arcotkey および wfkey ファイルが含まれています。これらのファイルは、インストーラによって使用され、過去にインストールした Arcot 製品を検出します。これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。このファイルは、パッチおよびアップグレードに影響を及ぼしません。
<*install_location*>/arcot/bin	sbin フォルダ内のサーバのバイナリを呼び出す webfortserver スクリプトが含まれています。
<*install_location*>/arcot/conf	以下の設定ファイルが含まれています。 • arcotcommon.ini • securestore.enc
<*install_location*>/arcot/dbscripts	WebFort スキーマを作成する SQL スクリプトが含まれています。データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<*install_location*>/arcot/logs	インストール ファイルおよび WebFort サーバ ログ ファイルが含まれています。
<*install_location*>/arcot/odbc32v60wf	WebFort によってサポートされるすべてのデータベース用の、ブランド製品の DataDirect ODBC ライブラリが含まれています。
<*install_location*>/arcot/sbin	管理者に必要なライブラリ ファイルおよび以下の実行可能ファイルが含まれています。 • arwfclient - WebFort サーバをシャットダウンし、リフレッシュするために使用されます。 • arwfserver.real - 設定を構成し、arwfclient バイナリを実行するスクリプトへのシンボリック リンク。 • dbutil - データベース処理に使用されるバイナリ。 • arwfwatchdog - このツールはサーバ健全性を監視し、また、停止したサーバを起動します。 • arwfenv - 環境変数を設定するために使用されるスクリプト。

表 A-1. WebFort サーバ ファイル

フォルダ	ファイル説明
<install_location>/arcot/Uninstall_Arcot WebFort	WebFort のアンインストールに必要な実行可能ファイルが含まれています。
<install_location>/arcot/xsd/webfort	WebFort にアップロードされる OATH トークン用の XML 形式を指定する ArcotWebFortTokenXchange.xsd ファイルが含まれています。

Administration Console のファイル

表 A-2 には、Administration Console によって使用されるファイルのフォルダの場所がリスト表示されています。

表 A-2. Administration Console のファイル

フォルダ	ファイル説明
<install_location>/	arcotkey および wfkey ファイルが含まれています。これらのファイルは、インストーラによって使用され、過去にインストールした Arcot 製品を検出します。これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。このファイルは、パッチおよびアップグレードに影響を及ぼしません。
bin	管理者に必要な以下の実行可能ファイルが含まれています。 • dbutil - このツールはデータベース関連の処理に使用されます。
<install_location>/arcot/conf	以下の設定ファイルが含まれています。 • arcotcommon.ini • adminserver.ini • securestore.enc
<install_location>/arcot/dbscripts	Administration Console のスキーマを作成する SQL スクリプトが含まれています。データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<install_location>/arcot/java/webapps	Administration Console の展開に必要な arcotadmin.war ファイルが含まれています。

表 A-2. Administration Console のファイル

フォルダ	ファイル説明
<*install_location*>/arcot/java/ext	securestore.enc ファイルの内容を読み取るために使用される arcot-crypto-util.jar および libArcotAccessKeyProvider.so ファイルが含まれています。
<*install_location*>/arcot/logs	Administration Console のログ ファイルが含まれています。
<*install_location*>/arcot/resourcepacks	以下の WebFort および Administration Console パッケージが含まれています。 • bundle_webfort.zip • bundler_adminconsole.zip
<*install_location*>/arcot/tools/bundlemanager	フォルダには、以下のファイルが含まれています。 • bundle-manager.jar • bundle_installer.xml

ユーザ データ サービスのファイル

表 A-3 には、ユーザ データ サービスによって使用されるファイルのフォルダの場所がリストされています。

表 A-3. ユーザ データ サービスのファイル

フォルダ	ファイル説明
<*install_location*>/	arcotkey および wfkey ファイルが含まれています。これらのファイルは、インストーラによって使用され、過去にインストールした Arcot 製品を検出します。これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。このファイルは、パッチおよびアップグレードに影響を及ぼしません。
bin	管理者に必要な以下の実行可能ファイルが含まれています。 • dbutil - このツールはデータベース関連の処理に使用されます。

表 A-3. ユーザ データ サービスのファイル

フォルダ	ファイル説明
<install_location>/arcot/conf	以下の設定ファイルが含まれています。 • arcotcommon.ini • udsserver.ini • securestore.enc
<install_location>/arcot/dbscripts	Administration Console のスキーマを作成する SQL スクリプトが含まれています。データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<install_location>/arcot/java/webapps	展開に必要な arcotuds.war ファイルおよびユーザ データ サービスが含まれています。
<install_location>/arcot/java/ext	securestore.enc ファイルの内容を読み取るために使用される arcot-crypto-util.jar および libArcotAccessKeyProvider.so ファイルが含まれています。
<install_location>/arcot/logs	UDS ログ ファイルが含まれています。

認証 Java SDK ファイル

表 A-4 には、認証 Java SDK によって使用されるファイルのフォルダの場所がリストされています。

表 A-4. 認証 Java SDK ファイル

フォルダ	ファイル説明
<install_location>/arcot/docs/webfort	認証 SDK 用 Javadoc を含む Arcot-WebFort-6.2-authentication-sdk-javadocs.zip ファイルが含まれています。
<install_location>/arcot/samples/java	サンプル アプリケーションを展開する webfort-6.2-sample-application.war ファイルが含まれています。
<install_location>/arcot/sdk/java/lib/arcot	WebFort 認証 Java SDK 用の以下の JAR ファイルが含まれています。 • arcot-pool.jar • arcot-webfort-common.jar • arcot-webfort-authentication.jar

表 A-4. 認証 Java SDK ファイル

フォルダ	ファイル説明
<install_location>/arcot/sdk/java/lib/external	WebFort 認証 Java SDK に必要なサードパーティ JAR ファイルが含まれています。 • bcprov-jdk14-139.jar • commons-httpclient-3.1.jar • commons-lang-2.4.jar • commons-pool-1.4.jar • log4j-1.2.9.jar
<install_location>/arcot/sdk/java/lib/properties	サンプル プロパティ (webfort.authentication.properties) ファイルが含まれています。Java SDK の初期化にこのファイルのパラメータを使用することも、init() 関数を使用することもできます。

発行 Java SDK ファイル

表 A-5 には、発行 Java SDK によって使用されるファイルのフォルダの場所がリストされています。

表 A-5. 発行 Java SDK ファイル

フォルダ	ファイル説明
<install_location>/arcot/docs/webfort	発行 SDK 用 Javadoc を含む、Arcot-WebFort-6.2-issuance-sdk-javadocs.zip ファイルが含まれています。
<install_location>/arcot/samples/java	サンプル アプリケーションを展開する webfort-6.2-sample-application.war ファイルが含まれています。
<install_location>/arcot/sdk/java/lib/arcot	発行 Java SDK 用の以下の JAR ファイルが含まれています。 • arcot-pool.jar • arcot-webfort-common.jar • arcot-webfort-issuance.jar

表 A-5. 発行 Java SDK ファイル

フォルダ	ファイル説明
<install_location>/arcot/sdk/java/lib/external	WebFort 発行 Java SDK に必要なサードパーティ JAR ファイルが含まれています。 • activation-1.1.jar • axiom-api-1.2.7.jar • axiom-impl-1.2.7.jar • axis2-adb-1.4.jar • axis2-java2wsdl-1.4.jar • axis2-kernel-1.4.jar • backport-util-concurrent-2.2.jar • bcprov-jdk14-139.jar • commons-codec-1.3.jar • commons-collections-3.1.jar • commons-httpclient-3.1.jar • commons-lang-2.4.jar • commons-logging-1.1.jar • commons-pool-1.4.jar • geronimo-jms_1.1_spec-1.1.jar • log4j-1.2.9.jar • neethi-2.0.jar • stax-api-1.0.1.jar • XmlSchema-1.2.jar
<install_location>/arcot/sdk/java/lib/properties	サンプル プロパティ（webfort.issuance.properties）ファイルが含まれています。Java SDK の初期化にこのファイルのパラメータを使用することも、init() 関数を使用することもできます。

WSDL ファイル

表 A-6 には、認証および発行 WSDL によって使用されるファイルのフォルダの場所がリストされています。

表 A-6. WSDL ファイル

フォルダ	ファイル説明
<*install_location*>/arcot/docs/webfort	以下の WSDL ドキュメントが含まれています。 • Arcot-WebFort-6.2-authentication-wsdldocs.zip • Arcot-WebFort-6.2-issuance-wsdldocs.zip
<*install_location*>/arcot/wsdls/webfort	Web サービス クライアントがコードを生成するために使用する以下の WSDL ドキュメントが含まれています。 • ArcotWebFortAuthSvc.wsdl • ArcotWebFortIssuanceSvc.wsdl

Plug-In SDK

表 A-7 には、Plug-In SDK によって使用されるファイルのフォルダの場所がリストされています。

表 A-7. Plug-In SDK ファイル

フォルダ	ファイル説明
<*install_location*>/arcot/bin	プラグイン ライブラリを含む arwfpluginsdk.so が含まれています。
<*install_location*>/arcot/sdk/plugin/c/include	以下の SDK プラグイン ヘッダ ファイルが含まれています。 • wf-common-interface.h • wf-plugin-interface.h
<*install_location*>/arcot/sdk/plugin/c/lib	プラグイン ライブラリを含む arwfpluginsdk.so が含まれています。

付録 B
設定ファイルおよびオプション

この付録では、WebFort が使用する設定ファイル、およびこれらのファイル内の設定が必要なパラメータについて説明します。

以下の WebFort 設定ファイルは、ディレクトリ *<install_location>*/arcot/conf にあります。

- arcotcommon.ini
- adminserver.ini
- udsserver.ini

以下のプロパティ ファイルは、ディレクトリ *<install_location>*/arcot/sdk/java/properties/ にあります。

- webfort.authentication.properties
- webfort.issuance.properties

INI ファイル

arcotcommon.ini

arcotcommon.ini ファイルには、データベース用のパラメータ、WebFort サーバおよび WebFort のその他のコンポーネント（Administration Console およびユーザ データ サービス）用のインスタンス設定が含まれています。このセクションでは、arcotcommon.ini ファイルの以下のパラメータについて説明します。

- WebFort サーバによって使用されるパラメータ
- Administration Console およびユーザ データ サービスによって使用されるパラメータ

WebFort サーバによって使用されるパラメータ

表 B-1 には、WebFort サーバによって使用されるデータベース設定がリストされています。WebFort サーバ用のデータベースの追加設定は、Administration Console の［Instance Management］画面を使用して実行する必要があります。

表 B-1. WebFort サーバのパラメータ

セクション	パラメータ	デフォルト	説明
[arcot/db/dbconfig]	DbType	デフォルト値なし	すべてのデータベース接続に適用可能なデータベースのタイプ。サポートされている値は以下のとおりです。 • oracle • db2
	EnableBrandLicensing	0	ブランド設定された ODBC ドライバが使用されているかどうか。これは、DataDirect のブランド設定された ODBC ドライバを使用しているときに使用できます。
	BrandLicenseFile	デフォルト値なし	ブランド設定された ODBC ドライバを使用するときのライセンス ファイル名。
[arcot/db/primarydb]（*プライマリ データベース用*） または [arcot/db/backupdb]（*バックアップ データベース用*）	Datasource.<*N*>	デフォルト値なし	サーバ データをホストするプライマリ データベースを示す ODBC システム データ ソース名（DSN）の名前。
	Username.<*N*>	デフォルト値なし	データベースへのアクセス用に、サーバによって使用されるユーザ名。
[arcot/watchdog]	ServerStartsTimeout	25	サーバ起動からの期間。watchdog が ServerStartsTimeout （25 分）の指定された期間内に 5 回サーバを起動すると、サーバは再び再起動されなくなります。 時間は分単位です。
	ServerStartsCount	5	サーバを再起動する最大回数。この後には、サーバは再び再起動されません。
	RestartSleepTime	5000	watchdog がサーバを再起動する前のスリープ時間。スリープ時間はミリ秒単位です。

Administration Console およびユーザ データ サービスによって使用されるパラメータ

表 B-2 には、arcotcommon.ini ファイルのデータベース設定パラメータがリストされ、各パラメータの説明が記載されています。

表 B-2. Administration Console およびユーザ データ サービスのパラメータ

セクション	パラメータ	デフォルト	説明
[arcot/db/dbconfig]	DbType	デフォルト値なし	すべてのデータベース接続に適用可能なデータベースのタイプ。サポートされている値は以下のとおりです。 • oracle • db2
	Driver	デフォルト値なし	JDBC ドライバ ベンダーによって提供されるデータベース ドライバ クラスの完全修飾名。正しいドライバ名を知るには、JDBC ベンダーのマニュアルを参照してください。 • Oracle の場合 - oracle.jdbc.driver.OracleDriver • DB2 の場合 - jcom.ibm.db2.jcc.DB2Driver
	MaxConnections	32	WebFort コンポーネントとデータベース間に作成できる接続の最大数。
	MinConnections	4	WebFort コンポーネントとデータベース間に最初に作成する接続の最小数。
	IncConnections	2	WebFort コンポーネントとデータベース間に新しい接続が必要なときに作成される接続の数。
	MaxIdleConnections	4	サーバが管理できるアイドル データベース接続の最大数。
	MaxWaitTimeForConnection	30000	接続が、タイムアウトする前に、使用可能になるまで、サーバが待機する必要がある（使用可能な接続がない場合）最大時間（ミリ秒単位）。
	AutoRevert	1	フェイルオーバーの発生後に、システムがプライマリ データベースへの接続を試みるかどうかを指定します。 バックアップ データベースが設定されている場合、またはフェイルオーバーが発生した後にサーバがデータベース接続を試みる場合、AutoRevert=1 を設定します。

表 B-2. Administration Console およびユーザ データ サービスのパラメータ（続き）

セクション	パラメータ	デフォルト	説明
[arcot/db/dbconfig]	MaxTries	3	サーバが、接続を中止するまでデータベースへの接続を試みる回数。
	ConnRetrySleepTime	100	データベースへの接続の試行間の遅延時間（ミリ秒）。
	MonitorSleepTime	50	監視スレッドがすべてのデータベースのハートビート チェック間にスリープする時間（秒）。
	Profiling	0	データベース メッセージがログ記録されているかどうか。データベース メッセージのログを有効化する場合は、1 に設定します。
	EnableBrandLicensing	0	ブランド設定された ODBC ドライバが使用されているかどうか。これは、DataDirect のブランド設定された ODBC ドライバを使用しているときに使用できます。
	BrandLicenseFile	デフォルト値なし	ブランド設定された ODBC ドライバを使用するときのライセンス ファイル名。
	MaxTransactionRetries	3	同じデータベース インスタンスで、トランザクションが再試行される最大回数。
	TransactionRetrySleepTime	10	トランザクションの再試行間の時間差。この値はミリ秒単位です。
[arcot/db/primarydb]（*プライマリ データベース用*） または [arcot/db/backupdb]（*バックアップ データベース用*）	Datasource.<*N*>		サーバ データをホストするプライマリ データベースを示す ODBC システム データ ソース名（DSN）の名前。

表 B-2. Administration Console およびユーザ データ サービスのパラメータ（続き）

セクション	パラメータ	デフォルト	説明
[arcot/db/primarydb] （*プライマリ データベース用*） または [arcot/db/backupdb] （*バックアップ データベース用*）	AppServerConnectionPoolName.<*N*>	デフォルト値なし	アプリケーション サーバのデータベース接続プーリングが使用されている場合、接続プール オブジェクトを検索するために使用する JNDI 名を指定します。この JNDI 名によるプールは、含まれるアプリケーション サーバ内に作成する必要があります。また、Arcot Web アプリケーションに対して、接続プールを使用するために、十分なアクセス権限を与える必要があります。 JNDI 名が Tomcat で設定されている場合は、完全修飾 JNDI 名を使用します。たとえば、 AppServerConnectionPoolName.1=java:comp/env/SampleDS その他のアプリケーション サーバでは、JNDI 名のみを指定します。たとえば、 AppServerConnectionPoolName.1=SampleDS 詳細については、付録 E の 「アプリケーション サーバの設定」を参照してください。 アプリケーション サーバ接続プールが必要 *でない* 場合は、この設定を空白のままにします。
	URL.<*N*>	デフォルト値なし	JDBC データ ソースの名前。 • Oracle の場合 - jdbc:oracle:thin:<*server*>:<*port*>:<*sid*> • DB2 の場合 - jdbc:db2://<*server*>:<*port*>/<*database*>
	Username.<*N*>	デフォルト値なし	データベースへのアクセス用に、サーバによって使用されるユーザ名。
	TrustStorePath.<*N*>	デフォルト値なし	Datasource.<N> に対応する SSL 証明書 truststore パス。このパス（ファイル名を含む）は証明書 truststore ファイルを参照します。このファイルには、クライアントが信頼する証明書のリストが含まれています。 **注：** TrustStore パスに対応するパスワード。<*N*> は、DBUtil ツールを使用して、鍵に TrustStorePath.<*N*> の値が使用された securestore.enc に安全に保存する必要があります。このツールの詳細については、*「Arcot WebFort 6.2 管理ガイド」*を参照してください。

表 B-2. Administration Console およびユーザ データ サービスのパラメータ（続き）

セクション	パラメータ	デフォルト	説明
	HostNameInCertificate.<*N*>	デフォルト値なし	truststore の Datasource.<N> SSL 証明書のサブジェクト識別名（DN）の共通名（CN）の値。 **注：** このパラメータは、Microsoft SQL Server を使用している場合のみ必要です。
[arcot/system]	InstanceId	1	Administration Console またはユーザ データ サービス インスタンスを識別するために使用できるパラメータ。サーバのすべてのインスタンスに対して一意の値を指定することをお勧めします。 インスタンス ID はトランザクション レポートにも表示されます。 このパラメータには整数値を指定する必要があります。

adminserver.ini

adminserver.ini ファイルには、Administration Console のログ情報を設定するパラメータが含まれています。表 B-3 には、Administration Console のログ ファイル情報がリストされています。

表 B-3. ログ パラメータ

パラメータ	説明
• log4j.logger.com.arcot.admin • log4j.logger.com.arcot.database • log4j.logger.com.arcot.admin.framework • log4j.logger.com.arcot.adminconsole • log4j.logger.com.arcot.common.database	Administration Console のログを書き込むために使用する必要のあるログ レベルを指定します。サポートされるログ レベルは以下のとおりです。 • FATAL • WARNING • INFO • DEBUG **注：** ログ レベルの詳細については、*「Arcot WebFort 6.2 管理ガイド」*を参照してください。
log4j.appender.debuglog.File	ログ ファイル名、および Administration Console のログを書き込む必要のある場所を指定します。 デフォルトでは、Administration Console のログ ファイル名は arcotadmin.log で、<*install_location*>/arcot/ にあるログ フォルダ内に作成されます。

表 B-3. ログ パラメータ

パラメータ	説明
`log4j.appender.debuglog.MaxFileSize`	ログ ファイルのサイズを指定します。デフォルトでは、2 MB です。
`log4j.appender.debuglog.MaxBackupIndex`	作成できるバックアップ ファイルの数を指定します。バックアップ ファイルの数がこの数と等しいとき、アプリケーションは最初のログ ファイルから上書きを開始します。

udsserver.ini

`udsserver.ini` ファイルには、ユーザ データ サービス（UDS）のログ情報を設定するためのパラメータが含まれています。表 B-4 には、UDS のログ ファイル情報がリストされています。

表 B-4. ログ パラメータ

パラメータ	説明
• `log4j.logger.com.arcot.uds` • `log4j.logger.com.arcot.common.database`	UDS ログを書き込むために使用する必要のあるログ レベルを指定します。サポートされるログ レベルは以下のとおりです。 • `FATAL` • `WARNING` • `INFO` • `DEBUG` **注：** ログ レベルの詳細については、*「Arcot WebFort 6.2 管理ガイド」*を参照してください。
`log4j.appender.debuglog.File`	ログ ファイル名、および UDS ログを書き込む必要のある場所を指定します。 デフォルトでは、UDS ログ ファイル名は `arcotuds.log` で、*<install_location>*`/arcot/` にあるログ フォルダ内に作成されます。
`log4j.appender.debuglog.MaxFileSize`	ログ ファイルのサイズを指定します。デフォルトでは、2 MB です。
`log4j.appender.debuglog.MaxBackupIndex`	作成できるバックアップ ファイルの数を指定します。バックアップ ファイルの数がこの数と等しいとき、アプリケーションは最初のログ ファイルから上書きを開始します。

プロパティ ファイル

webfort.authentication.properties

webfort.authentication.properties ファイルは、認証 Java SDK が WebFort サーバ情報を読み取るためのパラメータを提供します。表 B-5 には、設定パラメータがリストされています。

表 B-5. 認証 Java SDK 用パラメータ

パラメータ	デフォルト	説明
authentication.host.1	localhost	WebFort サーバのホスト名または IP アドレス。
authentication.port.1	9742	Authentication Native プロトコル用に設定されたポート番号。
authentication.transport	TCP	WebFort 認証 SDK と WebFort サーバ間の SSL 通信を有効化するには、このパラメータを SSL に設定します。 注：トランスポート モードを SSL に変更した場合、WebFort サーバを再起動する必要があります。
authentication.connectionTimeout	10000	WebFort サーバが到達できないと考えられるまでの最大時間（ミリ秒）。
authentication.readTimeout	30000	WebFort サーバからのレスポンスに許容される最大時間（ミリ秒）。
pool.maxActive	32	SDK から WebFort サーバへの、プール内に許容される接続の最大数。
pool.maxIdle	8	SDK から WebFort サーバへの、プール内に許容されるアイドル接続の最大数。
pool.maxWaitTimeMillis	-1	リクエストが接続まで待機する最大時間（ミリ秒単位）。デフォルトの -1 は、スレッドが無限に待機することを示します。
pool.minEvictableIdleTimeMillis	30000	接続がアイドル接続エビクター（ある場合）によって削除されるまでの、プール内で接続がアイドルになる可能性のある最小時間。
pool.timeBetweenEvictionRunsMillis	300000	プールをチェックしてアイドル接続を削除するまでのスリープする時間（ミリ秒）。

表 B-5. 認証 Java SDK 用パラメータ（続き）

パラメータ	デフォルト	説明
authentication.serverCACertPEMPath	デフォルト値なし	サーバの CA 証明書ファイルのパスを提供します。このファイルは PEM 形式である*必要があります*。 ファイルの完全パスを入力します。 例： server.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
authentication.clientCertKeyP12Path	デフォルト値なし	p12 形式のクライアント証明書のパスを提供します。
authentication.clientCertKeyPassword	デフォルト値なし	p12 ファイルを開くためのクライアント鍵ペア パスワードを入力します。

webfort.authentication.properties ファイルには、認証 Java SDK 用のログ ファイル情報も含まれています。log4j.rootLogger および log4j.logger.com.arcot パラメータを必要なレベルに設定します。ログ レベルの詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

webfort.issuance.properties

webfort.issuance.properties ファイルは、発行 Java SDK が WebFort サーバ情報を読み取るためのパラメータを提供します。表 B-6 には、設定パラメータがリストされています。

表 B-6. 発行 Java SDK 用のパラメータ

パラメータ	デフォルト	説明
issuance.host.1	localhost	WebFort サーバのホスト名または IP アドレス。
issuance.port.1	9744	Transaction Web Service プロトコル用に設定されたポート番号。
issuance.transport	TCP	WebFort 発行 SDK と WebFort サーバ間の SSL 通信を有効化するには、このパラメータを SSL に設定します。 **注：** トランスポート モードを SSL に変更した場合、WebFort サーバを再起動する必要があります。

表 B-6. 発行 Java SDK 用のパラメータ（続き）

パラメータ	デフォルト	説明
issuance.connectionTimeout	10000	WebFort サーバが到達できないと考えられるまでの最大時間（ミリ秒）。
issuance.readTimeout	30000	WebFort サーバからのレスポンスに許容される最大時間（ミリ秒）。
pool.maxActive	32	SDK から WebFort サーバへの、プール内に許容される接続の最大数。
pool.maxIdle	8	SDK から WebFort サーバへの、プール内に許容されるアイドル接続の最大数。
pool.maxWaitTimeMillis	-1	リクエストが接続まで待機する最大時間（ミリ秒単位）。デフォルトの -1 は、スレッドが無限に待機することを示します。
pool.minEvictableIdleTimeMillis	30000	接続がアイドル接続エビクター（ある場合）によって削除されるまでの、プール内で接続がアイドルになる可能性のある最小時間。
pool.timeBetweenEvictionRunsMillis	300000	プールをチェックしてアイドル接続を削除するまでのスリープする時間（ミリ秒）。
issuance.serverCACertPEMPath	デフォルト値なし	サーバの CA 証明書ファイルのパスを提供します。このファイルは PEM 形式である*必要があります*。ファイルの完全パスを入力します。 例： server.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
issuance.clientCertKeyP12Path	デフォルト値なし	p12 形式のクライアント証明書のパスを提供します。
issuance.clientCertKeyPassword	デフォルト値なし	p12 ファイルを開くためのクライアント鍵ペア パスワードを入力します。

webfort.issuance.properties ファイルには、発行 Java SDK 用のログ ファイル情報が含まれています。log4j.rootLogger および log4j.logger.com.arcot パラメータを必要なレベルに設定します。ログ レベルの詳細については、「Arcot WebFort 6.2 管理ガイド」を参照してください。

付録 C
データベース リファレンス

WebFort データベースには多くのテーブルが含まれています。一部のテーブルは、製品の使用に伴って、サイズが大きくなります。ユーザ数に直接比例して肥大化するテーブルもあれば、製品の使用に直接比例して肥大化するテーブルもあります。この付録には、切り捨ててディスク容量を管理し、データベースのパフォーマンスを向上できるデータベース テーブルのリストが掲載されています。

注： Arcot では、設定およびデータのレポートの必要性に応じて、SQL データベースに適切な調整を行うことをお勧めします。たとえば、大量のデータの削除は、削除プロセス時のパフォーマンスに悪影響を与えます。ロールバック セグメントのサイズによっては、システムが機能しなくなる場合もあります。また、古いレコードをアーカイブし、これらを完全に削除しないことを強くお勧めします。

この付録では、WebFort 用のデータベースを設定するときに、データベース サイズを計算する方法について説明します。また、この付録には、WebFort によって使用されるすべてのテーブル、およびデータベース テーブルのレプリケーションに関する推奨事項がリストされています。この付録では、以下のトピックが説明されています。

- データベース テーブルおよびレプリケーションのアドバイス
- データベース サイズの計算
- データベース調整パラメータ

データベース テーブルおよびレプリケーションのアドバイス

このセクションには、WebFort によって提供されるデータベース テーブルのリストおよび説明が記載され、また、テーブルをプライマリ データベースとバックアップ データベース間で、どの程度の頻度でレプリケートする必要があるかに関するアドバイスが記載されています。このセクションでは、以下のトピックについて説明されています。

- リアルタイム同期が必要なテーブル
- 定期的な同期が必要なテーブル

- 同期が必要ないテーブル

リアルタイム同期が必要なテーブル

表 C-1 には、プライマリ データベースとバックアップ データベース間のリアルタイム同期が必要なデータベース テーブルがリストされています。このカテゴリには、主にユーザ関連情報が含まれるテーブルが含まれており、このデータは認証に必要です。そのため、これらのテーブルのリアルタイム同期を実行する必要があります。

表 C-1. リアルタイム同期テーブル

テーブル	説明
ARADMINBASICAUTHUSER	管理者の基本認証クレデンシャルが含まれています。
ARADMINSCOPE	管理者が管理する一連の組織の情報が含まれています。
ARADMINSCOPEALL	既存および今後作成される、すべての組織を管理する管理者のリストが含まれています。
ARADMINUSER	管理者の情報が含まれています。
ARADMINTXID	トランザクション ID の生成に必要な情報が含まれています。
ARUDSORGANIZATION	組織の定義、その属性、およびリポジトリの接続性の詳細が含まれています。
ARUDSUSER	ARUSER 組織に属するユーザのユーザ詳細および属性が含まれています。すべてのタイプのユーザの PAM も、ある場合は含まれます。
ARUDSAUTHSESSION	現在アクティブなセッションの認証セッション詳細が含まれています。このテーブルがレプリケートされないと、アクティブな認証セッションが失われる場合があります。
ARWFARCOTID	ユーザの ArcotID クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFARCOTOTP	ユーザの ArcotOTP クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFAUTHTOKENS	正常な認証の後に生成される認証トークンが含まれています。リクエストされたトークン タイプとは無関係に、それぞれの正常な認証に対し 1 つのエントリがこのテーブル内に作成されます。
ARWFINSTANCES	特定のデータベースと通信する WebFort サーバのすべてのインスタンスに関する情報が含まれています。
ARWFGENERICCRED	ユーザのその他のクレデンシャルに関する情報が含まれています。たとえば、カスタム API によってサポートされるクレデンシャルなどです。
ARWFOATH	ユーザの OATH ワンタイム パスワード（OTP）クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。

表 C-1. リアルタイム同期テーブル （続き）

テーブル	説明
ARWFOTP	ユーザのワンタイム パスワード（OTP）クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFQNA	ユーザの質問と回答（Q&A）クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFPASSWORD	ユーザのユーザ名 / パスワード クレデンシャルが含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFVERIFIEDCHALLENGES	ArcotID 署名が正常に検証されるチャレンジに関する情報が含まれています。チャレンジ用の `No Replay` がオンになった場合、正常な ArcotID 認証用にエントリが作成されます。デフォルトでは、このオプションはオフになっています。

定期的な同期が必要なテーブル

表 C-2 には、プライマリ データベースとバックアップ データベース間の定期的な同期が必要なデータベース テーブルがリストされています。設定に変更があった場合、これらのデータベース テーブルは同期化されます。

表 C-2. 定期的な同期テーブル

テーブル	説明
ARADMINCONFIG	Administration Console の設定が含まれています。
ARADMINCUSTOMROLE	カスタム定義されたロールの設定が含まれています。
ARADMINMAP	キー / 値のペアとして入力される、WebFort サーバ インスタンスの情報が含まれています。
ARADMINPAFCONFIG	組織の管理者認証設定が含まれています。
ARADMINPWDPOLICY	すべての組織の管理者パスワード ポリシーが含まれています。
ARADMINTURNEDOFFPRIVILEGE	カスタム ロールでは使用できない権限に関する情報が含まれています。
ARADMINCACHEREFRESH	Administration Console がキャッシュをリフレッシュする必要があるかどうか決定する、キャッシュ リフレッシュ情報が含まれています。
ARADMINAUDITTRAIL	管理者アクティビティ監査が含まれています。
ARUDSAUDITLOG	ユーザ データ ソース（UDS）の処理およびそれらのリターン ステータス用の監査ログ情報が含まれています。
ARUDSCONFIG	UDS 設定パラメータおよびその値が含まれています。

表 C-2. 定期的な同期テーブル （続き）

テーブル	説明
ARUDSREPOSITORYTYPES	UDS によってサポートされるリポジトリの定義が含まれています。新規プラグインがシステムに追加される場合のみ、このテーブルを変更することをお勧めします。
ARUDSUSERATTRIBUTE	ユーザ属性定義が含まれています。個々の製品によって、新規ユーザ属性が追加される場合のみ、このテーブルを変更することをお勧めします。
ARWFADMINAUDITLOG	WebFort 管理アクティビティの監査ログ情報が含まれています。
ARWFARCOTIDHISTORY	*再発行*状態のすべての ArcotID が含まれています。
ARWFAUTHAUDITLOG	認証アクティビティの監査ログ情報が含まれています。
ARWFCONFIG	WebFort 設定情報が含まれています。このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFCUSTOMCONFIG	WebFort プラグイン設定情報が含まれています。このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFGENERICCREDHISTORY	*再発行*状態のその他のすべての（サポートされている API など）クレデンシャルが含まれています。
ARWFISSUANCEAUDITLOG	クレデンシャル発行アクティビティの監査ログ情報が含まれています。
ARWFMODULEREGISTRY	WebFort サーバの内部モジュールおよびプラグインに関する情報が含まれています。
ARWFOATHHISTORY	*再発行*状態のすべての OATH OTP クレデンシャルが含まれています。
ARWFOATHTOKENREGISTRY	シード値、トークン ID、およびトークン タイプなどの OATH トークン詳細が含まれています。
ARWFORGACTIVECONFIG	現在アクティブな組織の設定マッピングが含まれています。このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFORGCONFIG	組織ごとの設定マッピングが含まれています。このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFOTPHISTORY	*再発行*状態のすべてのワンタイム パスワード クレデンシャルが含まれています。
ARWFPASSWORDHISTORY	*再発行*状態のすべての user-name パスワード クレデンシャルが含まれています。
ARWFPROTOCOLCONFIGURATION	WebFort サーバの各リスナ ポートの設定が含まれています。

表 C-2. 定期的な同期テーブル （続き）

テーブル	説明
ARWFQNAHISTORY	*再発行*状態のすべての質問と回答クレデンシャルが含まれています。
ARWFSEQUENCE	バージョン設定に使用されるシーケンスに関する情報が含まれています。
ARWFSSLTRUSTSTORE	WebFort サーバによって信頼される SSL ルート証明書が含まれています。
ARWFSVRMGMTAUDITLOG	サーバ管理アクティビティの監査ログ情報が含まれています。

同期が必要ないテーブル

表 C-3 には、プライマリ データベースとバックアップ データベース間の同期が必要ないデータベース テーブルがリストされています。

表 C-3. 同期が必要ないテーブル

テーブル	説明
ARCMNDBERRORCODES	ベンダー固有のデータベース エラー コード、およびデータベースが停止または応答しない状態であることを示す SQL 状態値が含まれています。この情報は、バックアップが設定されている場合に、データベースをフェイルオーバーすべきかどうか決定するために使用されます。
ARADMINMANAGEROLE	1 つのロールが管理できるロールのリストが含まれています。
ARADMINPREDEFINEROLE	すべてのサポートされている管理者のロール情報が含まれています。
ARADMINSUPPORTEDAUTHMECH	すべてのサポートされている認証メカニズムに関する情報が含まれています。
ARADMINUITAB	Administration Console のタブに関する情報が含まれています。
ARADMINUITASK	Administration Console を使用して実行されるタスクに関する情報が含まれています。
ARADMINUITASKATTRIBUTES	Administration Console の第 1 階層および第 2 階層のタブがクリックされると表示されるタスクの詳細が含まれています。これらのタスクはランディング ページと呼ばれます。
ARADMINUITASKCONTAINER	タスク コンテナに関連する情報が含まれています。タスク コンテナは、Administration Console の第 2 階層のタブ ID、またはタスク グループのいずれかにすることができます。
ARADMINWIZARDTASK	Administration Console ブートストラップ ウィザードを使用して実行されるタスクに関する情報が含まれています。
ARRFREPORTTABLES	その他のテーブルのメタデータが含まれています。

表 C-3. 同期が必要ないテーブル

テーブル	説明
ARADMINMAPDATATYPE	ARADMINMAP でサポートされているデータ型のリストが含まれています。
ARWFDBERRORCODES	通信失敗を示すデータベース エラー コードが含まれています。
ARWFDBQUERIES	WebFort サーバによって使用されるデータベース クエリのリストが含まれています。
ARWFDISPLAYNAMES	WebFort で使用されるさまざまな鍵の名前および値が含まれています。
ARWFLOCALE	WebFort によってサポートされるロケールのリストが含まれています。
ARWFMESSAGES	WebFort サーバによって送信されるメッセージが含まれています。

データベース サイズの計算

このセクションを使用して、データベース管理者は WebFort 用に設定する必要があるデータベースのおおよそのサイズを計算できます。

サンプル計算で使用される記号

以下の記号が計算で使用されます。

- ユーザ数 = *N*
- 1 日あたりのトランザクションの平均数 = *T*
- 処理時間枠（日単位）= *D*

前提値

計算用に以下の前提が定義されています。

- ユーザ数（**N**）= 1,000,000 （100 万）
- 1 日あたりのトランザクションの平均数（**T**）=24,000
- 処理時間枠（**D**）= 90 日

前提に基づいたサンプル計算

「前提値」で前提となる数字を考慮すると、最終的な要件は以下のようになる必要があります。

- **ユーザの総数**を基にした要件：データベース サイズ = （21 * *N*）KB

- 日常のアクティビティを基にした要件：データベース サイズ = (*T* * *D* * 5) KB

データベース調整パラメータ

表 C-4 には、WebFort サーバとデータベース間の接続を調整するために使用できる共通パラメータがリストされています。これらの設定は Administration Console の［Instance Management］画面を使用して定義されます。

表 C-4. WebFort サーバとデータベース間の接続パラメータ

フィールド	説明
［Minimum Connections］	WebFort サーバとデータベース間に最初に作成される接続の最小数。
［Maximum Connections］	WebFort サーバとデータベース間に作成できる接続の最大数。 **注：** この値は、`MaxConnections` パラメータより優先されるため、データベースがサポートする最大接続数に応じてこの値を設定する必要があります。詳細については、データベース ベンダーのマニュアルを参照してください。
［Increment Connections by］	必要性が生じた場合、既存の接続に追加される接続の数。接続の総数は、接続の最大数を超えることはできません。
［Monitor Thread Sleep Time (in Seconds)］	監視スレッドがすべてのデータベースのハートビート チェック間にスリープする時間。
［Query Timeout］	WebFort サーバによって送信されたクエリが有効な時間。クエリは、この期間内に応答されない場合、閉じられます。
［Connection Retry Sleep Time (in Seconds)］	データベースに接続する試行間の遅延時間。
［Log Query Details］	すべてのデータベース クエリのログ記録を有効化します。
［Auto-Revert to Primary］	プライマリ データベースが機能するようになったら、サーバのバックアップ データベースからプライマリ データベースへの切り替えを有効化します。

付録 D
デフォルトのポート番号および URL

この付録では、WebFort で使用するデフォルトのポート番号を表にまとめています。以下の内容について説明します。

- デフォルトのポート番号
- WebFort コンポーネントの URL

デフォルトのポート番号

WebFort は、異なるポートで設定される 4 つのプロトコルをサポートします。表 D-1 には、WebFort で使用するデフォルトのポート番号を記載しています。

表 D-1. WebFort プロトコル

プロトコル	デフォルトポート番号	デフォルトのステータス	説明
Server Management Web Services	9743	有効	このプロトコルは WebFort サーバの管理に使用されます。Administration Console および `arwfclient` クライアントは、このポートを使用して通信し、サーバ管理アクティビティを行います。
Transaction Web Services	9744	有効	このプロトコルは、認証 Web サービスおよび Issuance Web サービスのクライアントが WebFort サーバへの接続に使用します。
Authentication Native	9742	有効	これは、WebFort が認証目的で使用する専用のバイナリ プロトコルです。このポートは認証 SDK が使用します。
Administration Web Services	9745	有効	このプロトコルを使用して、プロファイル、ポリシー、SAML、ASSP などの設定が作成および管理されます。

表 D-1. WebFort プロトコル（続き）

プロトコル	デフォルト ポート番号	デフォルトのステータス	説明
RADIUS	1812	無効	RADIUS（Remote Authentication Dial In User Service）プロトコルをサポートするために使用されます。RADIUS プロトコルをサポートする設定になっている場合は、WebFort サーバは RADIUS サーバとして動作します。
ASSP	9741	無効	このプロトコルは、PDF 文書のサーバ サイドのデジタル署名を用いてユーザを認証する際に、Adobe® Reader および Adobe® Acrobat® と一緒に使用されます。
Transaction HTTP	9746	無効	このプロトコルは、HTTP クライアントから WebFort サーバに HTTP リクエスト パケットを転送するために使用されます。

他のサービスがすでにデフォルト ポート上で実行されている場合、該当プロトコル用に新しいポートを設定する必要があります。Server Management Web Services プロトコル用の新しいポート番号を設定するには、`webfortserver` ツールを使用します。詳細については、「Arcot WebFort 6.2 管理ガイド」の第 5 章「システム管理者用のツール」を参照してください。他のプロトコル用の新しいポート番号を設定する場合は、Administration Console の［Protocol Configuration］画面を使用します。詳細については、「Arcot WebFort 6.2 管理ガイド」の第 3 章「WebFort サーバ インスタンスの管理」を参照してください。

WebFort コンポーネントの URL

インストール後に WebFort コンポーネントにアクセスする際は、以下の表に記載の URL を使用します。

表 D-2. デフォルトのポート番号

コンポーネントまたはサービス	URL
Master Administrator 用の Administration Console の URL	*http://< アプリケーション ホスト >:< ポート > /arcotadmin/masteradminlogin.htm*
他の管理者用の Administration Console の URL	*http://< アプリケーション ホスト >:< ポート > /arcotadmin/adminlogin.htm*

表 D-2. デフォルトのポート番号

コンポーネントまたはサービス	URL
認証 Web サービス	*http://< アプリケーション ホスト >:< ポート > /WebFortAuthSvc*
Issuance Web サービス	*http://< アプリケーション ホスト >:< ポート > /WebFortIssuanceSvc*
サンプル アプリケーション	*http://< アプリケーション ホスト >:< ポート > /webfort-6.2-sample-application/*

付録 E
アプリケーション サーバの設定

この付録では、WebFort コンポーネントの展開先となるアプリケーション サーバ上でデータベース接続プーリングをセットアップするために実行する必要がある手順について概説します。以下のアプリケーション サーバ用の設定手順を網羅します。

- Apache Tomcat
- IBM WebSphere
- BEA WebLogic

Apache Tomcat

ここでは、JNDI ベースのデータベース操作用に Apache Tomcat を有効にする手順について説明します。

Apache Tomcat 内に JNDI 接続を作成するには、以下の手順に従います。

1. Apache Tomcat アプリケーション サーバをインストールし、以下の URL を使用してインストールをテストします。

   http://localhost:8080/

2. *<Tomcat ホーム>*/conf ディレクトリにある server.xml ファイルを開きます。
3. データ ソースの定義に必要な以下の情報を収集します。
   - JNDI 名

     arcot コンポーネントによって使用される JNDI 名。この名前は、arcotcommon.ini （java:comp/env/ プレフィックスなし）の AppServerConnectionPoolName.<N> と一致する必要があります。
   - ユーザ ID

     データベース ユーザ ID。
   - パスワード

     データベース パスワード。

- JDBC ドライバ クラス

  JDBC ドライバ クラス名。たとえば、`oracle.jdbc.driver.OracleDriver`。
- JDBC URL

  データベース サーバ用の JDBC URL。たとえば、Oracle ドライバを使用している場合、この URL は `jdbc:oracle:thin:<` *サーバ*`>:<` *ポート*`>:<`*sid*`>` となります。

4. `<`*GlobalNamingResources*`>` タグ内に以下のエントリを追加してデータ ソースを定義します。

```
<Resource name="SampleDS"
auth="Container"
type="javax.sql.DataSource"
factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"
username="<userid>"
password="<password>"
driverClassName="<JDBC driver class>"
url="<jdbc-url>"
maxWait="30000"
maxActive="32"
maxIdle="8"
initialSize="4"
timeBetweenEvictionRunsMillis="300000"
minEvictableIdleTimeMillis="30000"/>
```

5. `<`*Tomcat ホーム*`>/conf` ディレクトリにある `context.xml` ファイルを開きます。
6. `<`*Context*`>` タグ内に以下のエントリを追加してデータ ソースを定義します。

```
<ResourceLink global="SampleDS" name="SampleDS"
type="javax.sql.DataSource"/>
```

7. 以下のデータベース接続プーリング（DBCP）関係ファイルを `<`*Tomcat ホーム*`>/common/lib` ディレクトリにコピーします。

- commons-dbcp-1.2.2.jar
- ojdbc14-10.2.0.1.0.jar（Oracle データベースの場合）
- sqljdbc.jar（MS SQL Server 2005 用 Microsoft JDBC ドライバ バージョン 1.2.2828）

IBM WebSphere

ここでは、JNDI ベースのデータベース操作に対して IBM WebSphere を有効にする手順について説明します。

Arcot Adapter の Java 依存コンポーネントを展開するために IBM WebSphere を設定するには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［**Resources**］を選択し、［**JDBC**］ノードを展開します。
3. ［**JDBC Providers**］を選択し、［**New**］をクリックして、使用しているデータベースに応じて適切な JDBC プロバイダを作成します。

注： *http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html* を参照してください。

4. 画面上の手順に従って、［CLASSPATH］にデータベースのクラスパス情報を入力します。
5. ［**Next**］をクリックし、［Summary］ページで情報を確認します。［**Finish**］をクリックして、JDBC プロバイダの設定を完了します。
6. ［**Save**］をクリックして、変更内容を保存します。
7. ［**Resources**］に移動し、［**JDBC**］をクリックします。
8. ［**JDBC**］の［**Data Sources**］を開き、［**New**］をクリックして新しいデータ ソースを作成します。データ ソースを作成するには、以下の手順に従います。
   a. データ ソース名を指定します。
   b. JNDI 名を指定します。この名前は arcotcommon.ini の AppServerConnectionPoolName.<N> と一致する必要があります。
   c. ［**Next**］をクリックし、手順 3 で作成した JDBC プロバイダを選択します。

d. ［**Next**］をクリックし、JDBC URL を指定します。

e. データ ソースを選択し、［**Next**］、［**Finish**］の順にクリックします。

f. ［**Next**］をクリックして［Summary］画面を確認し、［**Finish**］をクリックします。

9. ［**Save**］をクリックして、変更内容を保存します。
10. 前の手順で作成したデータ ソースを選択し、［**Related Items**］セクションをクリックします。
11. ［**New**］をクリックして新しいクレデンシャルを作成します。
12. データベースへの接続に使用されるログイン クレデンシャルを入力し、クレデンシャルを保存します。
13. ［**Apply**］をクリックし、［**Save**］をクリックして変更内容を保存します。
14. ［**Data Sources**］を選択し、手順 7 で作成したデータ ソースを選択します。
15. ［**Component-managed authentication alias**］で、手順 12 で作成した JAAS クレデンシャルを選択し、［**Save**］をクリックします。
16. ［**Data Sources**］を選択し、手順 7 で作成したデータ ソースのチェック ボックスをオンにします。
17. ［**Test connection**］をクリックし、接続が正しく指定されているかどうかを検証します。

注 : このテストでは、データベース サーバへの接続のみが確認され、データ ソースの定義が正しいかどうかは必ずしも確認されません。

BEA WebLogic

ここでは、JNDI ベースのデータベース操作用に BEA WebLogic を有効にする手順について説明します。

BEA WebLogic にデータ ソースを作成するには、以下の手順に従います。

1. WebLogic Administration Console にログインします。
2. ロックと編集が終わっていない場合は、［**Lock & Edit**］ボタンをクリックします。
3. ［**Resources**］に移動し、［**JDBC**］をクリックします。

4. ［**JDBC**］の［**Data Sources**］を開き、［**New**］をクリックして新しいデータ ソースを作成します。データ ソースを作成するには、以下の手順に従います。
5. 以下の JNDI 情報とデータベース情報を設定します。
   a. ［**Name**］を「ArcotDB」に設定します。
   b. ［**JNDI Name**］を「ArcotDB」に設定します。
   c. ［**Database Type**］で適切な値（Oracle など）を選択します。
   d. ［**Database Driver**］で適切な値（Oracle Thin Driver など）を選択します。
6. ［**Next**］をクリックし、デフォルト値をそのまま使用して再度［**Next**］をクリックします。
7. ［Connection Properties］ページで、データベースの詳細情報を設定します。以下に示す値は Oracle データベースの値です。
   - ［**Database**］: DB サーバの SID またはサービス名
   - ［**Hostname**］: DB サーバの IP アドレスまたはホスト名
   - ［**Port**］: 1521 または DB サーバが動作している他の任意のポート
   - ［**Database User Name**］
   - ［**Database Password / Confirm Password**］
8. ［ **Test Configuration**］をクリックし、データベース パラメータが正しく指定されたかどうかを確認します。
9. ［**Next**］をクリックし、データ ソースの展開先として優先の WebLogic サーバ インスタンスを設定します。
10. ［**Finish**］をクリックして、データ ソースの一覧ページに戻ります。
11. ［**Activate**］をクリックして、データ ソース設定を有効にします。

付録 F
SSL 用の設定

デフォルトでは、WebFort コンポーネントは、コンポーネント同士での通信に TCP（Transmission Control Protocol）を使用します。ただし、TCP はスプーフィングおよび man-in-the-middle 攻撃に対して脆弱です。WebFort コンポーネント間の安全に通信を確保するために、これらを SSL （Secure Socket Layer）トランスポート モードに設定する必要があります。

以下の手順には、異なるコンポーネント間の SSL を設定する方法がリストされています。

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

Administration Console とユーザ データ サービス間

Administration Console および UDS が異なるアプリケーション サーバに展開された場合、アプリケーション サーバを SSL を有効にするように設定する必要があります。詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

WebFort サーバとユーザ データ サービス間

一方向 SSL

WebFort サーバとユーザ データ サービス（UDS）間の一方向 SSL を設定する方法

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。
2. Web ブラウザで Administration Console を開きます。
3. Master Administrator アカウントを使用して、Administration Console にログインします。
4. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
5. サブ メニューの［**Administration Console**］タブがアクティブであることを確認します。
6. ［**Administration Console**］で、［**UDS Configuration**］リンクをクリックし、該当するページを表示します。
7. ［**Protocol**］フィールドで、［**One-Way SSL**］を選択します。
8. ［**Port**］の値をデフォルトの SSL ポートに設定します。
9. ［**Server Root CA**］フィールド隣の［**Browse**］ボタンをクリックし、UDS ルート証明書を選択します。
10. ［**Next**］をクリックしてから［**Save**］をクリックします。

双方向 SSL

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

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバを有効にします。詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。
2. Web ブラウザで Administration Console を開きます。
3. Master Administrator アカウントを使用して、Administration Console にログインします。

4. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
5. サブ メニューの［**Administration Console**］タブがアクティブであることを確認します。
6. ［**Administration Console**］で、［**UDS Configuration**］リンクをクリックし、該当するページを表示します。
7. ［**Protocol**］フィールドで、［**Two-Way SSL**］を選択します。
8. ［**Port**］の値をデフォルトの SSL ポートに設定します。
9. ［**Server Root CA**］フィールド隣の［**Browse**］ボタンをクリックし、UDS ルート証明書を選択します。
10. ［**Client Certificate**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort ルート証明書を選択します。
11. ［**Client Private Key**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort 秘密キーを選択します。
12. ［**Next**］をクリックしてから［**Save**］をクリックします。

Administration Console と WebFort サーバ間

一方向 SSL

Administration Console と WebFort サーバ間の一方向 SSL を設定する方法

1. Web ブラウザで Administration Console を開きます。
2. Master Administrator アカウントを使用して、Administration Console にログインします。
3. メイン メニューの［**Services & Server Configurations**］タブを有効化します。
4. サブメニューの［**WebFort**］タブを有効化します。
5. ［**Instance Configurations**］で、［**Protocol Management**］リンクをクリックし、該当するページを表示します。

   ［Protocol Configuration］ページが表示されます。
6. プロトコルを設定する**サーバ インスタンス**を選択します。
7. ［**List of Protocols**］セクションで、***<Protocol Name>*** リンクをクリックします。

プロトコルを設定するページが表示されます。

8. 以下のフィールドを設定します。
   - ［**Protocol**］フィールドで、［**SSL**］を選択します。
   - ［**Server Certificate Chain**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort ルート証明書を選択します。
   - ［**Server Private Key**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort 秘密キーを選択します。
9. ［**Save**］ボタンをクリックします。
10. すべてのプロトコルに対して手順 7 から手順 9 を繰り返します。
11. WebFort サーバを再起動します。
12. Master Administrator アカウントを使用して、Administration Console にログインします。
13. メイン メニューの［**Services & Server Configurations**］タブを有効化します。
14. サブメニューの［**WebFort**］タブを有効化します。
15. ［**System Configuration**］で、［**WebFort Connectivity**］リンクをクリックして、該当ページを表示します。

    ［WebFort Connectivity］ページが表示されます。
16. SSL 用に有効にするプロトコルについて、以下を設定します。
    - ［**Transport**］フィールドで、［**SSL**］を選択します。
    - ［**Server CA Certificate in PEM**］フィールド隣の［**Browse**］ボタンをクリックして、WebFort ルート証明書を選択します。
17. ［**Save**］ボタンをクリックします。

双方向 SSL

Administration Console と WebFort サーバ間の双方向 SSL を設定する方法

1. Web ブラウザで Administration Console を開きます。
2. Master Administrator アカウントを使用して、Administration Console にログインします。
3. メイン メニューの［**Services & Server Configurations**］タブを有効化します。
4. サブメニューの［**WebFort**］タブを有効化します。

5. ［**Instance Configurations**］で、［**Protocol Management**］リンクをクリックし、該当するページを表示します。

   ［Protocol Configuration］ページが表示されます。
6. プロトコルを設定する**サーバ インスタンス**を選択します。
7. ［**List of Protocols**］セクションで、***<Protocol Name>*** リンクをクリックします。

   プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［**Protocol**］フィールドで、［**SSL**］を選択します。
   - ［**Server Certificate Chain**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort ルート証明書を選択します。
   - ［**Server Private Key**］フィールド隣の［**Browse**］ボタンをクリックし、WebFort 秘密キーを選択します。
9. ［**Save**］ボタンをクリックします。
10. すべてのプロトコルに対して手順 7 から手順 9 を繰り返します。
11. WebFort サーバを再起動します。
12. Master Administrator アカウントを使用して、Administration Console にログインします。
13. メイン メニューの［**Services & Server Configurations**］タブを有効化します。
14. サブメニューの［**WebFort**］タブを有効化します。
15. ［**System Configuration**］で、［**WebFort Connectivity**］リンクをクリックして、該当ページを表示します。

    ［WebFort Connectivity］ページが表示されます。
16. SSL 用に有効にするプロトコルについて、以下を設定します。
    - ［**Transport**］フィールドで、［**SSL**］を選択します。
    - ［**Server CA Certificate in PEM**］フィールド隣の［**Browse**］ボタンをクリックして、WebFort ルート証明書を選択します。
    - ［**Client Certificate-Key pair in PKCS#12**］フィールド隣の［**Browse**］ボタンをクリックして、PKCS#12 形式の Administration Console 証明書を選択します。
    - ［**Client PKCS#12 Password**］フィールドに PKCS#12 パスワードを入力します。
17. ［**Save**］ボタンをクリックします。

WebFort コンポーネントとデータベース間

このセクションでは、WebFort コンポーネントとデータベース間の SSL 通信を設定する方法について説明します。ここでは、以下のトピックについて説明します。

- WebFort サーバとデータベース間
- Administration Console とデータベース間
- ユーザ データ サービスとデータベース間

WebFort サーバとデータベース間

Unix プラットフォームでは、WebFort はデータベースへの接続に DataDirect ドライバを使用します。WebFort とデータベース間の SSL を有効にするには、`odbc.ini` ファイルを編集し、DataDirect ドライバを設定する必要があります。

`odbc.ini` ファイルを設定するには、以下の手順を実行します。

1. 次のディレクトリに移動します。

   `<install_location>/arcot/odbc32v60wf`

2. ファイル エディタで `odbc.ini` ファイルを開きます。
3. 使用しているデータベースに対応するセクションで、表 F-1 にリストされている

表 F-1. odbc.ini パラメータ

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

4. `odbc.ini` ファイルを保存して閉じます。

Administration Console とデータベース間

Administration Console は、Java Database Connectivity （JDBC）を使用して、データベースに接続します。Administration Console とデータベース間の SSL を有効にするには、以下の手順に従います。

1. SSL 用に Administration Console が展開されているアプリケーション サーバを設定します。
2. arcotcommon.ini で TrustStorePath.<N> および HostNameInCertificate.<N> パラメータを設定します。

ユーザ データ サービスとデータベース間

UDS は JDBC を使用して、データベースに接続します。ユーザ Administration Console とデータベース間の SSL を有効にするには、以下の手順に従います。

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

認証 SDK と WebFort サーバ間

WebFort サーバと認証 Java SDK 間の SSL を設定するには、次の場所にある `webfort.authentication.properties` ファイルを設定する必要があります。

`<install_location>/arcot/sdk/java/properties`

設定パラメータの詳細については、「webfort.authentication.properties」を参照してください。

発行 SDK と WebFort サーバ間

WebFort サーバと発行 Java SDK 間の SSL を設定するには、次の場所にある `webfort.issuance.properties` ファイルを設定する必要があります。

`<install_location>/arcot/sdk/java/properties`

設定パラメータの詳細については、「webfort.issuance.properties」を参照してください。

付録 G
サードパーティ製ソフトウェアのライセンス

この付録では、WebFort で使用されるサードパーティ製ソフトウェア パッケージを一覧で紹介します。以下のパッケージが該当します。

Annogen

- annogen-0.1.0.jar

  Copyright © 2003-2006 - The Codehaus. All rights reserved unless otherwise noted.（*http://annogen.codehaus.org//*）

AOP Alliance

- aopalliance-1.0.jar

Licensed under AOP Alliance.（*http://aopalliance.sourceforge.net/*）

Apache

Copyright © The Apache Software Foundation.Licensed under the Apache License, Version 2.0.（*http://www.apache.org/licenses/*）

- ant-1.7.0.jar
- axiom-impl-1.2.7.jar
- Axis2 1.4.jar
- commons-beanutils-1.7.0.jar
- commons-codec-1.3.jar
- commons-collections-3.1.jar
- commons-dbcp-1.2.2.jar
- commons-digester-1.7.jar
- commons-fileupload-1.1.1.jar
- commons-httpclient-3.1.jar
- commons-io-1.2.jar
- commons-lang-2.4.jar
- commons-logging-1.1.jar

- commons-pool-1.4.jar
- commons-validator-1.3.1.jar
- geronimo-activation-1.1.jar
- geronimo-annotation-1.0.jar
- geronimo-javamail-1.4.jar
- geronimo-jms.1.1.jar
- geronimo-stax-api-1.0.jar
- httpcore-4.0.jar
- iBATIS 2.3.4.726
- log4j.1.2.9.jar
- neethi-2.0.jar
- oro-2.0.7.jar
- standard-1.1.2.jar
- stax-api-1.0.1.jar
- struts-1.2.8.jar
- velocity-1.5.jar
- woden-1.0.0.jar
- wsdl4j-1.6.2.jar
- xbean-2.2.0.jar
- xbean-2.3.0.jar
- xercesImpl-2.8.1.jar
- xml.resolver-1.2.0.jar
- xml-commons-1.3.04.jar
- xml-xalan-2.7.0.jar
- xmlParserAPIs-2.6.0.jar
- XmlSchema-1.2.jar

ASM

- asm-1.5.3.jar

Backport-Util-Concurrent

- `backport-util-concurrent-2.2.jar`

Copyright © 2004-2007 Distributed Computing Laboratory, Emory University.
（*http://backport-jsr166.sourceforge.net/index.php*）

Bouncy Castle 1.3.9

Copyright © 2000 - 2006 The Legion Of The Bouncy Castle.（*http://www.bouncycastle.org/*）

cglib-2.1_3.jar

Licensed under Apache Software Foundation.（*http://www.apache.org/licenses/*）

db2jcc-9.5.jar

© Copyright IBM Corporation 1994, 2009.All rights reserved.
（*http://www-01.ibm.com/software/lotus/passportadvantage/licensing.html*）

ICU License - ICU 1.8.1 以降

- `icu4j`
- `icu4j-2.6.1.jar`

Copyright (c) 1995-2010 International Business Machines Corporation and others
（*http://source.icu-project.org/repos/icu/icu/trunk/license.html*）

Object-Graph Navigation Language（OGNL）

- `ognl-2.6.9.jar`

Copyright (c) 2001-2004 The OpenSymphony Group. All rights reserved.
（*http://www.opensymphony.com/ognl/*）

OpenSSL

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.
（*http://www.openssl.org/source/license.html*）

Oracle（*http://www.oracle.com/*）

- Oracle Database 10*g* JDBC Driver

  Copyright © 1995-2007, Oracle. All rights reserved.

- Sun Microsystems

  Copyright © 1995, 2010, Oracle and/or its affiliates. All rights reserved.

- Java Architecture for XML Binding
  - jaxb-api-2.1.6.jar
- Java Beans Activation Framework
  - activation-1.1.jar
- Java Mail
  - mail-1.4.jar
- Java Servlet
  - servlet-api-2.3.jar
- Java XPath Engine
  - jaxen-1.1.jar
  - jaxen-1.1.1.jar
- LDAP ライブラリ
  - ldap-1.2.4.jar
- JDBC
  - jdbc-1.2.2828.jar
- JSTL
  - jstl 1.0.3.jar

Spring Framework

Copyright © 2006-2008, SpringSource, All Rights Reserved.The Spring Framework is licensed under the terms of the Apache License, Version 2.0.（*http://www.springsource.org/*）

- spring-2.5.2.jar
- spring-aop-2.5.2.jar
- spring-beans-2.5.2.jar
- spring-binding-1.0.5.jar
- spring-context-2.5.2.jar
- spring-context-support-2.5.2.jar
- spring-core-2.5.2.jar
- spring-dao-2.0.8.jar
- spring-ibatis-2.0.8.jar

- `spring-jdbc-2.5.2.jar`
- `spring-jms-2.5.2.jar`
- `spring-orm-2.5.2.jar`
- `spring-test-2.5.2.jar`
- `spring-tx-2.5.2.jar`
- `spring-web-2.5.2.jar`
- `spring-webflow-1.0.5.jar`
- `spring-webmvc-2.5.2.jar`
- `spring-webmvc-portlet-2.5.2.jar`
- `spring-webmvc-struts-2.5.2.jar`
- `springmodules-validation-0.4.jar`

Woodstox

- `woodstox-core-asl-3.2.0.jar`

Copyright © 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA （*http://www.ohloh.net/p/woodstox*）

XOM License

- `xom-1.0.jar`
- `xom-1.1.jar`

その他の商標

- UNIX® は、米国およびその他の国における The Open Group の登録商標です。
- Linux® は、米国およびその他の国における Linus Torvalds の商標です。
- Java および Java をベースにしたすべての商標は、米国およびその他の国における Sun Microsystems, Inc. の商標です。その他の会社名、製品名、およびサービス名は、それぞれ各社の商標またはサービス マークです。
- DB2 および WebSphere は、米国およびその他の国における IBM の商標です。
- BEA WebLogic Server® および Solaris SPARC は、米国およびその他の国における Oracle® の商標です。

付録 H
用語集

ArcotID	ソフトウェアの形でのハードウェア レベルの認証を可能にするセキュアなソフトウェア クレデンシャル。
Digest-MD5	広く使用される暗号化ハッシュ関数。ハッシュ値は 128 ビットです。
FYP（Forgot Your Password、パスワードを忘れた場合）	ユーザが ArcotID のパスワードを忘れた場合、ユーザと WebFort の間で Q&A セッションが実施されます。ユーザは簡単な質問に答えた後で、新しい ArcotID パスワードの入力を求められ、新しい ArcotID が発行されます。
GA （Global Administrator、グローバル管理者）	CSR 管理者アカウントのセットアップおよびシステムの設定を担当する管理者。
PKCS	RSA によって考案され発行された公開キー暗号化標準のグループ。詳細については、「公開キー暗号化法」を参照してください。
PKCS#7	PKI に従ってメッセージを署名し暗号化するために使用。証明書の配布（たとえば PKCS#10 メッセージに対するレスポンスとして）にも使用されます。
PKI（Public Key Infrastructure）	ネットワーク環境における公開キー暗号化法および証明書の使用を促進する標準およびサービス。
SHA（Secure Hash Algorithm）	暗号化ハッシュ関数のセット。
SSL（Secure Socket Layer）	データの暗号化により、公衆ネットワーク間での通信のセキュリティ保護および認証を目的とするプロトコル。
UA （User Administrator、ユーザ管理者）	CSR は、セキュリティ システムのユーザに関連する日常業務を担当する管理者。たとえば、管理者は、ユーザの登録支援、ユーザ パスワードのリセット、およびさまざまな登録レポートの表示を行います。
WS-Security（Web Services Security）	Web サービスにセキュリティを適用するための手段となる通信プロトコル。

WSDL（Web Services Description Language）	ネットワーク サービスを、メッセージを交換できる通信エンドポイントの集合として記述する、W3C によって規定された標準的な XML フォーマット。操作とメッセージを抽象的に記述し、次に具体的なネットワーク プロトコルおよびメッセージ フォーマットにバインドしてエンドポイントを定義します。 WSDL ドキュメントでは Web サービスについて記述し、サービスが利用できる場所とメソッドを指定します。
エラー メッセージ	エラーが発生した場合に、その状況に関してユーザ エージェントに報告するためにアプリケーションによって返されるメッセージ。
クレデンシャル	ユーザ ID を証明するもの。デジタル クレデンシャルがスマート カードまたは USB トークンなどのハードウェアまたはサーバ上に保存される場合があります。そのクレデンシャルは認証時に検証されます。
暗号化	内容を判読できないように情報にスクランブルをかける処理。
暗号化ハッシュ関数	認証などのセキュリティ関連アプリケーションで使用される、セキュリティ プロパティが追加されたハッシュ関数。
公開キー	公開キー暗号化法で使用される 1 対のキーの一方。公開キーは自由に配布され、証明書の一部としてとして発行されます。通常、公開キーの所有者に送信されたデータを暗号化するために使用されます。その後、公開キーの所有者は、対応する秘密キーを使用して、データを復号化します。
公開キー暗号化法	秘密の共有について事前に合意しなくてもユーザが安全に通信することができる最新の暗号化形式。この方法では、対称暗号化法と異なり、全員が知っている公開キーと、公開キーと秘密キーのペアの所有者のみが知っている秘密キーという 2 つのキーを使用します。公開キー暗号化法は、非対称暗号化法とも呼ばれます。
失敗した試行	ユーザが特定のクレデンシャルで認証に失敗した回数。
認証	エンティティのログイン情報が本人のものであることを証明するプロセス。
認証トークン	トークンは、コンピュータ サービスの許可ユーザに与えられるオブジェクトで、認証の際に補助的に使用されます。
秘密キー	公開キー暗号化法で使用される 1 対のキーの一方。このキーは秘密に保持され、データの復号化または暗号化に使用できます。

索引

か

こ

さ

せ

そ

た

て

に

は

ふ