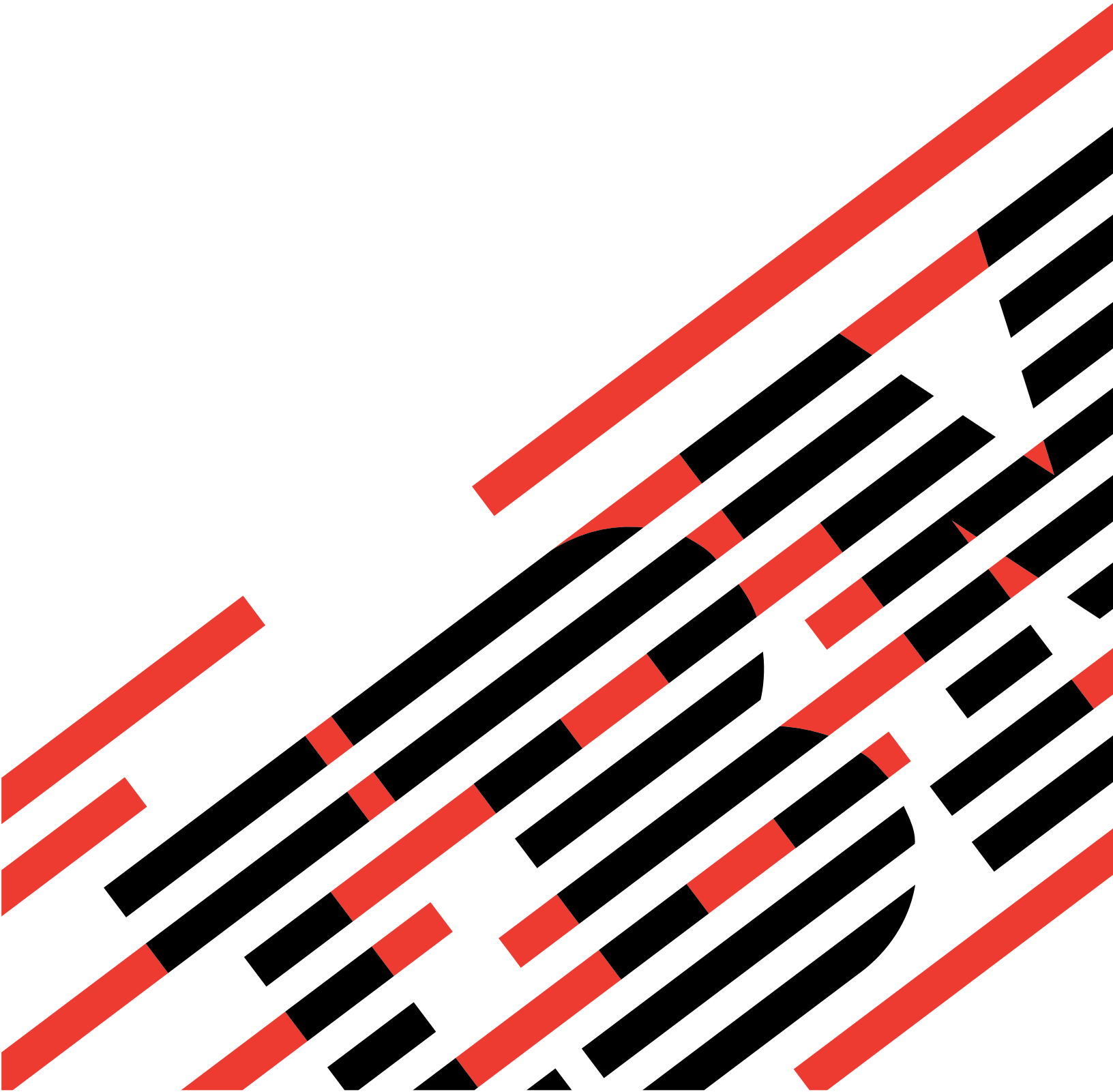
IBM

eserver

iSeries

ディジタル証明書マネージャー



IBM

@server

iSeries

ディジタル証明書マネージャー

目次

第 1 部 ディジタル証明書マネージャー

ディジタル証明書は電子信任状で、これを使用することにより、電子取引で本人であることが証明できます。ネットワーク・セキュリティーを強化するために、ディジタル証明書が使用されることがますます増えています。たとえば、ディジタル証明書は、Secure Sockets Layer (SSL) の使用と構成には、欠くことのできないものです。SSL を使用すると、インターネットのような非トラステッド・ネットワークで、ユーザーとサーバー・アプリケーションの間にセキュア接続が確立できます。SSL は、インターネット上の機密データ (ユーザー名やパスワードなど) のプライバシー保護には、最も優れた方法の 1 つです。iSeries™ の多くのサービスおよびアプリケーション (FTP、Telnet、HTTP Server for iSeries など多数) は、 SSL をサポートしてデータのプライバシーを確保しています。

iSeries は、広範囲にわたるディジタル証明書をサポートし、ユーザーが、多様なセキュリティー・アプリケーションで、信任状としてディジタル証明書を使用できるようにします。証明書は SSL を構成する際に使用するだけでなく、SSL と仮想私設ネットワーク (VPN) の両方のトランザクションで、クライアント認証の信任状として使用することができます。また、ディジタル証明書およびそれらに関連したセキュリティー・キーを使用して、オブジェクトに署名することもできます。オブジェクトに署名すると、オブジェクト上の署名を確認することにより、オブジェクトの内容に対して加えられた変更や改ざんを検出し、オブジェクトの保全性を確保することができます。

iSeries が無料で提供する機能であるディジタル証明書マネージャー (DCM) を使用すれば、iSeries による証明書のサポートが簡単に利用でき、アプリケーションの証明書を集中的に管理できます。DCM を使うと、任意の認証局 (CA) から取得した証明書を管理することができます。また、独自のローカル CA を作成、運用して、組織内のアプリケーションやユーザーに専用証明書を発行する場合にも、DCM は使用できます。

証明書を効果的に利用して、そのセキュリティー上の利点を生かすには、適切な計画と評価が重要です。本書の各トピックをよく読んで、証明書の機能と、DCM を使用して証明書および証明書を使用するアプリケーションを管理する方法について、知識を深めてください。

V5R2 の新機能
今回のリリースでディジタル証明書マネージャー・フィーチャーに対して行われた変更、および情報トピックに対して行われた変更については、この情報を参照してください。

トピックの印刷
トピック全体を PDF ファイルとして印刷する方法については、このページを参照してください。

以前のリリースからの DCM のマイグレーション
既存のバージョンの DCM から現行リリースのバージョンにマイグレーションする場合に行う必要のある作業、および理解しておく必要のあるその他の考慮事項については、この情報を参照してください。

DCM シナリオ
この情報を使用して、証明書を実装する典型的な方式を説明した 2 つのシナリオについて検討し、iSeries セキュリティー・ポリシーの一部としてのユーザー独自の証明書の実装を計画するうえで役立ててください。各シナリオでは、記載されているシナリオを利用するために行う必要のある、すべての構成作業も示されています。

ディジタル証明書の概念
ディジタル証明書とはどのようなもので、どのような働きをするのかを知るには、このトピックと参照情報を参照してください。さまざまなタイプの証明書について知り、それらをセキュリティー・ポリシーの一部として使用する方法を学習してください。

DCM の計画
この情報は、どのような場合にどのような方法でディジタル証明書を使用すれば、セキュリティー上の目的に見合うのかを判断する際に役立ちます。 DCM をインストールするために必要な前提条件、および DCM を使用する前に考慮する必要のあるその他の要件を知るには、この情報を参照してください。

DCM の構成
ユーザーの証明書とそのキーを管理するために DCM を使用できるようにするうえで必要なすべての事項を構成する方法については、この情報を参照してください。

DCM の管理
DCM を使用して、証明書と、その証明書を使用するアプリケーションを管理する方法を理解するには、この情報を利用してください。また、オブジェクトにディジタル署名をする方法や、独自の認証局を作成および運用する方法についても、ここで知ることができます。

DCM に関するトラブルシューティング
DCM を使用していて比較的よく発生するいくつかのエラーについて、その解決方法が知りたい場合は、この情報を利用してください。

DCM の関連情報
このトピックには、ディジタル証明書、PKI (Public Key Infrastructure)、ディジタル証明書マネージャー、およびその他の関連情報について説明した他の情報源へのリンクが記載されています。

第 1 章 V5R2 の新機能

V5R2 では、以下のようなディジタル証明書マネージャー (DCM) および iSeries ディジタル証明書の機能が強化されています。

- **証明書の割り当て機能**
  この新規 DCM タスクを使用すると、1 つまたは複数のアプリケーションに、より迅速かつ簡単に証明書を割り当てることができます。このタスクには、「**証明書の管理 (Manage Certificates)**」タスク・リストからアクセスすることも、高速パス・ページの「**サーバーおよび証明書の処理 (Work with server and certificates)**」および「**オブジェクト署名証明書の処理 (Work with object signing certificates)**」からアクセスすることもできます。この機能は、*SYSTEM および *OBJECTSIGNING 証明書ストアでのみ使用可能です。
- **コマンド (*CMD) オブジェクトへの署名**
  DCM を使用してコマンド (*CMD) オブジェクト上にディジタル署名を作成することにより、保全性を検査する手段を提供できるようになりました。また、*CMD オブジェクトの署名の有効範囲、つまり、*CMD オブジェクト全体に署名するのか、 *CMD オブジェクトのコア・コンポーネントのみに署名するのかを選択することができます。 DCM を使用して *CMD オブジェクトの署名を表示すると、 DCM により、署名の有効範囲に関する情報が示されます。
- **DCM を使用しないでローカル CA によって署名されたユーザー証明書を作成するための API**
  ローカル認証局 (CA) によって署名された証明書を非 iSeries ユーザーに対してプログラマチックに発行するために使用できる、2 つの新しい API が追加されました。これらの API を使用することにより、 iSeries ユーザー・プロファイルを持たないユーザーに対して、DCM を使用してクライアント認証のための証明書を個別に獲得させることなく、証明書を発行できるようになりました。

このトピックに関する新規情報または追加された情報には、以下のものが含まれます。

- セキュリティーの目標を満たすための証明書の最善の利用法を決定するうえで役立てることのできる、2 つの新しいシナリオ。
- DCM を使用するために必要な情報を、簡単かつ迅速に検索できるように再編成された情報。

今回のリリースで追加または変更された機能に関するその他の情報については、

「プログラム資料説明書」  を参照してください。

第 2 章 トピックの印刷

PDF 版をダウンロードし、表示するには、『ディジタル証明書マネージャー』

 (約 1383 KB、126 ページ) を選択します。

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「**ファイル**」をクリックする。
3. 「**名前を付けて保存**」をクリックする。
4. PDF を保存したいディレクトリーに進む。
5. 「**保存**」をクリックする。

PDF を表示または印刷するために Adobe Acrobat Reader が必要な場合には、

Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html)  からコピーをダウンロードすることができます。

第 3 章 以前のリリースからの DCM のマイグレーション

V4R3 のバージョンのディジタル証明書マネージャー (DCM) から V5R2 へマイグレーションすると、DCM は、ローカル認証局 (CA) とシステム証明書キー・リング・ファイルを自動的に更新します。DCM は、default.kyr という名前が付けられたこれらのファイルを、default.kdb という名前の付いた対応する証明書ストア・ファイルにアップグレードします。DCM は、Hypertext Transfer Protocol (HTTP) サーバーおよび Lightweight Directory Access Protocol (LDAP) サーバーに関連付けられたキー・リング・ファイル内の有効な証明書をすべてマイグレーションします。DCM は、有効な証明書を *SYSTEM 証明書ストア (default.kdb) にマイグレーションします。

注: DCM の V4R4、V4R5、または V5R1 バージョンからマイグレーションする場合、これらのバージョンの証明書ファイルは、V5R2 バージョンの DCM と互換性があるので、マイグレーション作業を実行する必要はありません。

証明書ストアのマイグレーションに対するキー・リング - V4R3 マイグレーション

V5R2 DCM インストール時に、システムは以下のキー・リング・ファイルをマイグレーションします。
- DCM のデフォルト・キー・リング・ファイル
- HTTP Server の構成ファイルが使用するキー・リング
- LDAP サーバーの構成ファイルが使用するキー・リング

DCM により自動的にアップグレードされなかった .kyr ファイルを使用すると、DCM は、初めて処理する際にこのファイルを kyr.kdb ファイルに変換します。たとえば、初めて DCM ユーザー・インターフェースで secure.kyr ファイルを指定するときに、DCM は、このファイルを secure.kyr.kdb というファイル名の新規証明書ストアに変換します。

注: キー・リングは、証明書ストアとは異なるので、DCM により自動的にアップグレードされなかったキー・リング・ファイルを、DCM ユーザー・インターフェースを使用して変換する必要があります。ファイル名拡張子を手動で .kdb に変更すると、次に DCM ユーザー・インターフェースによりファイルを処理しようとしたときにエラーになります。

DCM の使用時に secure.kyr ファイルを削除しようとすると、DCM は実際にはそれを保存して、secure.kyr.kdb ファイルを削除します。

デフォルトの証明書ストアのパスワード

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR というファイルが存在する場合、システムはこのキー・リング・ファイル、およびその他のすべての適格なキー・リング・ファイルを *SYSTEM 証明書ストアにマイグレーションします。/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR ファイルに関連した元のパスワードが、 *SYSTEM 証明書ストアのパスワードとして使用されます。

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR ファイルは存在しないが、マイグレーションするのに適格な他のキー・リング・ファイルが存在する場合 (たとえば、HTTP Server 構成ファイルが使用するキー・リング・ファイル)、システムは、*SYSTEM 証明書ストアを DEFAULT (すべて大文字) というパスワードを指定して作成し、マイグレーションを完了します。

ファイルのマイグレーション作業時に発生する可能性のあるエラーおよびその解決方法については、『マイグレーション・エラーおよび回復方法』を参照してください。

第 4 章 DCM シナリオ

ディジタル証明書マネージャーおよび iSeries が提供するディジタル証明書サポートにより、証明書を使用して、ユーザーのセキュリティー・ポリシーをさまざまな方法で強化できるようになります。どのような証明書の使用法を選択するのかは、ユーザーのビジネス目標とセキュリティーの必要性の両方に応じて異なります。

ディジタル証明書を使用すると、さまざまな方法でセキュリティーを改良することができます。ディジタル証明書を使うと、Secure Sockets Layer (SSL) を使用して、Web サイトやその他のインターネット・サービスへ安全にアクセスできます。また、ディジタル証明書を使用して、仮想私設ネットワーク (VPN) 接続を構成することもできます。さらに、証明書のキーを使用すれば、オブジェクトにディジタル署名をしたり、ディジタル署名の検証を行ってオブジェクトの認証性を確認することもできます。このようなディジタル署名により、オブジェクトの発行元の信頼性が保証され、そのオブジェクトの保全性が保護されます。

ディジタル証明書 (ユーザー名とパスワードの代わりに) を使って、サーバーとユーザー間のセッションを認証し、許可すると、システム・セキュリティーをさらに増強できます。また、DCM を使用して、ユーザーの証明書を、そのユーザーの iSeries ユーザー・プロファイルと関連付けることもできます。そうすることで、証明書の権限と許可は、関連付けられたプロファイルと同じものになります。

したがって、証明書の使用法の選択は、複雑となり、また、多くの要因によって異なる可能性があります。このトピックで提供するシナリオでは、典型的なビジネスのコンテキストにおける、より一般的なディジタル証明書のセキュリティーの目的をいくつか説明します。また、各シナリオでは、そのシナリオを実施するために必要なすべてのシステムおよびソフトウェアの前提条件、および必要なすべての構成作業も示されています。これらのシナリオを検討して、ユーザーのニーズに最も合うようにセキュリティーを向上させるには、証明書をどのように使用するのがよいのかを決定するうえで役立ててください。

シナリオ: 証明書を使用して共通アプリケーションおよび資源へのアクセスを保護する
このシナリオでは、一般ユーザーによる共通またはエクストラネットの資源およびアプリケーションへのアクセスを保護および制限するために、いつ、どのように証明書を使用すべきかを説明します。

シナリオ: 証明書を使用して内部アプリケーションおよび資源へのアクセスを保護する
このシナリオでは、内部のサーバーで、内部ユーザーがアクセスすることのできる資源およびアプリケーションを保護および制限するために、いつ、どのように証明書を使用すべきかを説明します。

シナリオ: 証明書を使用して共通アプリケーションおよび資源へのアクセスを保護する

状況

ユーザーが保険会社 (MyCo., Inc) に勤務しており、会社のイントラネット・サイトおよびエクストラネット・サイトで、各種アプリケーションの保守を担当しているとします。担当しているアプリケーションの 1 つが、料率計算のアプリケーションであり、これを使用して、数百の独立した代理店が顧客に見積もりを作成できるとします。このアプリケーションが提供する情報には、ある程度の機密性があるため、登録された代理店のみがこのアプリケーションを使用できるようにする必要があります。さらに、最終的には、現在使用しているユーザー名とパスワードによる方式よりも安全な方法による、アプリケーションへのユーザー・アクセスの方法を提供するものとします。このアプリケーションによって提供される情報が、信頼の置けないネットワークを介して伝送される際に、許可されていないユーザーによって取り込まれることが懸念されます。また、さまざまな代理店が、許可を得ずに、この情報を相互に共用し合う可能性もあります。

研究を重ねた結果、ディジタル証明書を使用することで、必要なセキュリティーが得られるという結論に達しました。証明書を使用すると、Secure Sockets Layer (SSL) を使用して料率データの伝送を保護することができます。最終的にはすべての代理店に、アプリケーションにアクセスするために証明書を使用してもらいたいものの、その目標を実現するためには、会社および代理店がある程度の時間が必要であることが判明しています。現時点では、伝送中の機密データのプライバシーが SSL によって保護されるため、現行のユーザー名とパスワードによる認証方式を引き続き使用することにします。

アプリケーションおよびそのユーザーのタイプ、およびユーザーを証明書によって認証するという将来の目標に基づいて、一般に知られている認証局 (CA) から得た公開証明書を使用して、アプリケーションに合わせて SSL を構成することに決定しました。

このシナリオの利点

このシナリオには、以下の利点があります。

- ディジタル証明書を使用して料率計算アプリケーションへの SSL アクセスを構成すると、サーバーとクライアントの間で伝送される情報が確実に保護され、秘密を保つことができます。
- クライアント認証において、可能な限りディジタル証明書を使用すると、より確実に許可ユーザーを識別する方法が提供されます。ディジタル証明書の使用が不可能な場合にも、ユーザー名とパスワードによるクライアント認証は SSL セッションによって保護され、機密が保たれるため、こうした機密データの交換がより安全に行えるようになります。
- *公開* ディジタル証明書を使って、アプリケーションおよびデータへのアクセスの許可や制限を行う方法は、次のような条件下では実用的な選択です。
  - データとアプリケーションにさまざまなレベルのセキュリティーが必要な場合。
  - トラステッド・ユーザー間のターンオーバーの割合が高い場合。

- アプリケーションとデータ (インターネット Web サイトなど)、あるいはエクストラネット・アプリケーションへの公衆アクセスを提供している場合。
- アプリケーションおよび資源にアクセスするユーザーの数が多いため、あるいはその他の管理上の理由により、独自の認証局 (CA) を運用したくない場合。

• このシナリオに従って、公開証明書を使用して SSL 用に料率計算アプリケーションを構成すると、アプリケーションにアクセスするためにユーザーが行わなければならない構成作業の量が少なくなります。ほとんどのクライアント・ソフトウェアには、有名な CA の大部分に対応する CA 証明書が含まれています。

目的

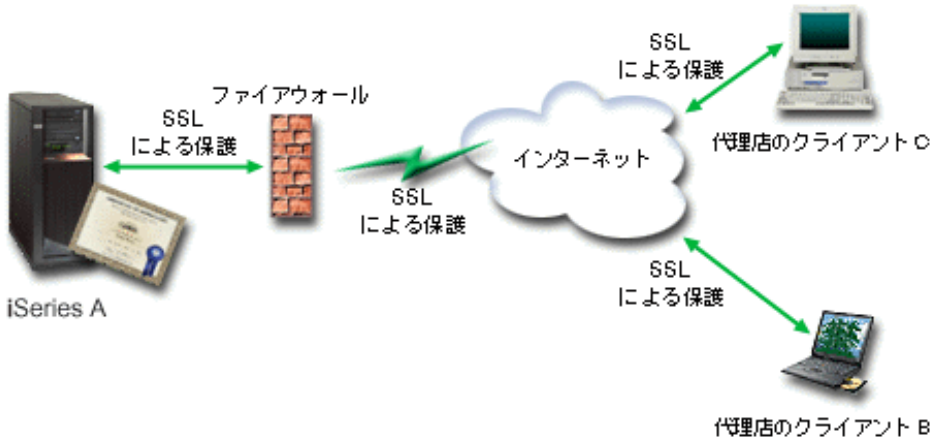
このシナリオでは、MyCo., Inc. は、自社のアプリケーションが、許可された一般ユーザーに提供する料率計算情報を保護するために、ディジタル証明書を使用したいと考えています。同社はまた、このアプリケーションにアクセスできるユーザーの認証における、より安全な方法も求めています。

このシナリオの目的は以下のとおりです。

• 同社の共通料率計算アプリケーションでは、SSL を使用して、ユーザーに提供するデータのプライバシーを保護する必要があります。
• SSL 構成は、一般的に知られている一般のインターネット認証局 (CA) から提供される公開証明書を使用して行われる必要があります。
• 許可ユーザーは、SSL モードでアプリケーションにアクセスするために、有効なユーザー名およびパスワードを入力する必要があります。最終的には、許可ユーザーは、アプリケーションへのアクセス権を得るために、2 つのいずれかの方式のセキュア認証を使用できるようにする必要があります。代理店は、一般的に知られている認証局 (CA) から提供される公開ディジタル証明書、または有効なユーザー名およびパスワードを提示する必要があります。

詳細

次の図は、このシナリオのネットワーク構成状態を示したものです。



この図は、このシナリオの状況に関する、以下の情報を表しています。

会社の公開サーバー - iSeries A

• iSeries A は、この会社の料率計算アプリケーションをホストするサーバーです。

- iSeries A は OS/400® バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries A には、Cryptographic Access Provider (5722-AC3) がインストールされています。
- iSeries A には、ディジタル証明書マネージャー (OS/400 オプション 34) および IBM® HTTP Server for iSeries (5722-DG1) がインストールされ、構成されています。
- iSeries A は料率計算アプリケーションを実行します。このアプリケーションは、次のように構成されています。
  - SSL モードを必要とする。
  - 一般的に知られている認証局 (CA) が発行した公開証明書を使用して SSL 構成を行う。
  - ユーザー名およびパスワードによるユーザー認証を必要とする。
- iSeries A は、クライアント B および C がアプリケーションにアクセスする際に、その証明書を提示して SSL セッションを開始します。
- SSL セッションを初期化した後で、iSeries A は、料率計算アプリケーションへのアクセスを許可する前に、クライアント B および C に対して有効なユーザー名とパスワードの提示を要求します。

代理店のクライアント・システム - クライアント B およびクライアント C

- クライアント B および C は、料率計算アプリケーションにアクセスする独立の代理店です。
- クライアント B および C のクライアント・ソフトウェアには、アプリケーション証明書を発行した、一般的に知られている CA の証明書のコピーがインストールされています。
- クライアント B および C は iSeries A にある料率計算アプリケーションにアクセスします。 iSeries A は、その ID を検証して SSL セッションを開始するために、クライアント・ソフトウェアにその証明書を提示します。
- クライアント B および C のクライアント・ソフトウェアは、iSeries A からの証明書を受け入れて、SSL セッションを開始するよう構成されています。
- SSL セッションが開始された後で、クライアント B および C は有効なユーザー名とパスワードを提示しなければなりません。その後で、iSeries A がアプリケーションへのアクセスを許可します。

前提条件および前提事項

このシナリオは、以下の前提条件および前提事項に依存します。

1. iSeries A にある料率計算アプリケーションは、SSL を使用するように構成することのできる汎用アプリケーションです。多くの iSeries アプリケーションを含め、ほとんどのアプリケーションは SSL をサポートします。 SSL 構成のステップは、アプリケーションによって大幅に異なります。したがって、このシナリオでは、SSL を使用するように料率計算アプリケーションを構成するための具体的な手順は示しません。このシナリオでは、あらゆるアプリケーションが SSL を使用するために必要な証明書を構成および管理するための手順を示します。
2. オプションで、料率計算アプリケーションは、クライアント認証のために証明書を要求する機能を提供することができます。このシナリオでは、このサポートを提供するアプリケーション用に証明書の信頼を構成するための、ディジタル証明書マネージャー (DCM) の使用法を示します。クライアント認証の構成ステップ

はアプリケーションによって大幅に異なるため、このシナリオでは、料率計算アプリケーション用に、証明書によるクライアント認証を構成するための具体的な手順は示しません。
3. iSeries A は、ディジタル証明書マネージャー (DCM) をインストールし、使用するための要件を満たしています。
4. これまで誰も、iSeries A で DCM を構成または使用したことはありません。
5. DCM を使用してこのシナリオのタスクを実施する人には、ユーザー・プロファイルで特殊権限 *SECADM および *ALLOBJ が割り当てられていなければなりません。
6. iSeries A には IBM 4758-023 PCI 暗号化コプロセッサーはインストールされていません。

タスク・ステップ

このシナリオを実施するには、iSeries A で以下のタスクを行う必要があります。

1. 必要なすべての iSeries 製品をインストールし、構成するための前提条件となるステップをすべて行う。
2. ディジタル証明書マネージャー (DCM) を使用して、サーバー証明書要求を作成する。
3. Secure Sockets Layer (SSL) を使用するようにアプリケーションを構成する。
4. DCM を使用して、ユーザーのアプリケーションのアプリケーション ID への、署名されたサーバーまたはクライアント証明書のインポートおよび割り当てを行う。
5. 必要であれば、アプリケーションを SSL モードで開始する。
6. オプショナル・タスク: DCM を使用して、このサポートを提供するアプリケーションの証明書に基づいてクライアント認証を使用可能にするよう、CA 信頼リストを定義する。

注: このシナリオで述べる状況では、料率計算アプリケーションがクライアント認証のために証明書を使用する必要はありません。多くのアプリケーションは、証明書によるクライアント認証サポートを提供しています。このサポートの構成方法は、アプリケーションによって大幅に異なります。このオプショナル・タスクは、アプリケーションの証明書によるクライアント認証のサポートを構成するための基礎として、クライアント認証用の証明書の信頼を DCM によって使用可能にする方法の理解を支援するために提供するものです。

構成の詳細

このシナリオで説明する、アプリケーションおよび資源への保護された共通アクセスを、証明書を使用して構成するには、以下のタスク・ステップに従ってください。

ステップ 1: 必要なすべての iSeries 製品をインストールするための前提条件となるタスクを行う

このシナリオを実施するための特定の構成タスクを実行する前に、必要なすべての iSeries 製品をインストールおよび構成するための前提条件となるタスクをすべて行う必要があります。

ステップ 2: サーバーまたはクライアント証明書要求を作成する

このシナリオで述べる、Secure Sockets Layer (SSL) を使用してアプリケーションのデータ通信を保護するプロセスを開始するためには、まず最初に、公開証明書 (CA) からディジタル証明書を取得する必要があります。ディジタル証明書マネージャー (DCM) を使用して、証明書を発行するために公開 CA が必要とする情報を作成してください。

証明書取得プロセスを開始するには、以下のステップに従ってください。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、「**新規証明書ストアの作成 (Create New Certificate Store)**」を選択して、ガイド・タスクを開始し、一連のフォームを完了します。これらのフォームは、証明書ストアおよびアプリケーションで SSL セッション確立のために使用できる証明書の作成プロセスをガイドするものです。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
3. 作成する証明書ストアとして ***SYSTEM** を選択して、「**続行 (Continue)**」をクリックします。
4. 「**はい (Yes)**」を選択して、*SYSTEM 証明書ストア作成の一環として証明書を作成し、「**続行 (Continue)**」をクリックします。
5. 新規証明書の署名者として「**VeriSign または他のインターネット認証局 (CA) (VeriSign or other Internet Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックすると、新規証明書の識別情報を指定できるフォームが表示されます。
6. フォームに入力して、「**続行 (Continue)**」をクリックすると、確認用ページが表示されます。この確認用ページには、証明書を発行する公開認証局 (CA) に提供する必要がある証明書要求データが表示されます。証明書署名要求 (CSR) データは、新規証明書に指定した公開鍵およびその他の情報から構成されています。
7. 証明書を要求する際に公開 CA が必要とする CSR データを、証明書申請フォームまたは別個のファイルに、注意深くコピー・アンド・ペーストします。「開始 (Begin)」行と「新規証明書要求の終わり (End New Certificate Request)」行の両方を含む、すべての CSR データを使用しなければなりません。このページを終了すると、データは失われ、そのデータを回復することはできません。
8. 選択した CA に申請フォームまたはファイルを送信して、証明書を発行したり、証明書に署名したりします。
9. CA から、署名されて完成した証明書が戻されるまで待機してから、このシナリオの次のタスク・ステップに進みます

CA から、署名されて完成した証明書が戻されると、SSL を使用するようにアプリケーションを構成し、*SYSTEM 証明書ストアに証明書をインポートし、その証明書をアプリケーションに割り当てて SSL 用に使用させることができます。

ステップ 3: SSL を使用するようにアプリケーションを構成する

公開証明書 (CA) から署名された証明書を受け取ると、公開アプリケーションでの Secure Sockets Layer (SSL) 通信を使用可能にするプロセスを続行できるようになります。署名された証明書での作業を行う前に、SSL を使用するようにアプリケーションを構成する必要があります。アプリケーションによっては、HTTP Server for iSeries のように、アプリケーションで SSL を使用するように構成すると、固有のアプリケーション ID を生成し、その ID をディジタル証明書マネージャー (DCM) に登録するものがあります。その場合、DCM を使用して、署名された証明書をこのアプリケーション ID に割り当て、SSL 構成プロセスを完了させるには、このアプリケーション ID を知らなければなりません。

SSL を使用するようにアプリケーションを構成するための方法は、アプリケーションによって異なります。このシナリオでは、述べられている料率計算アプリケーションのための特定のソースを想定していません。MyCo., Inc. がこのアプリケーションを代理店に提供する方法は、何通りも考えられるためです。

SSL を使用するようにアプリケーションを構成するには、アプリケーションのドキュメントに記載された手順に従ってください。また、多くの一般的な IBM アプリケーションで、SSL を使用するように構成する詳しい方法については、Information Center のトピック『SSL によるアプリケーションの保護』を参照してください。

ステップ 4: 署名された公開証明書のインポートおよび割り当てを行う

SSL を使用するようにアプリケーションを構成した後で、ディジタル証明書マネージャー (DCM) を使用して署名済みの証明書をインポートし、それをアプリケーションに割り当てることができます。

証明書をインポートしてそれをアプリケーションに割り当て、SSL 構成プロセスを完了させるには、以下のステップに従ってください。

1. DCM を開始します。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
5. タスク・リストから「**証明書のインポート (Import certificates)**」を選択して、署名済みの証明書を *SYSTEM 証明書ストアにインポートするプロセスを開始します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
6. 次に、「**証明書の管理 (Manage Certificates)**」タスク・リストから「**証明書の割り当て (Assign certificate)**」を選択し、現行の証明書ストアの証明書のリストを表示します。

7. リストから証明書を選択して、「**アプリケーションへの割り当て (Assign to Applications)**」をクリックし、現行の証明書ストアに関するアプリケーション定義のリストを表示します。
8. このリストからアプリケーションを選択して、「**続行 (Continue)**」をクリックします。割り当ての選択に関する確認メッセージ、あるいは、(問題が生じた場合には) エラー・メッセージを示すページが表示されます。

これらのタスクが完了すると、アプリケーションを SSL モードで開始し、そのアプリケーションで提供されるデータのプライバシーの保護を開始することができます。

ステップ 5: アプリケーションを SSL モードで開始する

アプリケーションへの証明書のインポートと割り当てのプロセスが完了した後で、アプリケーションを終了してから、SSL モードで再始動する必要のある場合があります。これが必要となるのは、一部のケースにおいて、アプリケーションの実行中に証明書割り当てが行われたことを、アプリケーションが判別できない可能性があるためです。ご使用になっているアプリケーションを再始動する必要があるかどうか、また、アプリケーションを SSL モードで再始動するための具体的な情報については、該当するアプリケーションの資料を参照してください。

オプションのステップ 6: クライアント認証用の証明書を必要とするアプリケーションのための CA 信頼リストを定義する

Secure Sockets Layer (SSL) セッションでクライアント認証に証明書の使用をサポートしているアプリケーションは、有効な ID 証明として、証明書を受け入れるかどうか決定しなければなりません。アプリケーションが証明書を認証する場合に使用する基準の 1 つは、証明書を発行した認証局 (CA) をアプリケーションが承認するかどうかです。

このシナリオで述べる状況では、料率計算アプリケーションがクライアント認証のために証明書を使用する必要はありません。多くのアプリケーションは、証明書によるクライアント認証のサポートを提供しています。このサポートの構成方法は、アプリケーションによって大幅に異なります。このオプショナル・タスクは、アプリケーションで証明書を使用してクライアント認証を行うように構成するための基礎として、クライアント認証用の証明書の信頼を DCM によって使用可能にする方法の理解を支援するために提供するものです。

アプリケーションの CA 信頼リストを定義できるようにするには、いくつかの条件を満たしていなければなりません。

- アプリケーションは、クライアント認証に証明書の使用をサポートしていなければならない。
- アプリケーションの DCM 定義で、アプリケーションが CA 信頼リストを使用するように指定しなければならない。

アプリケーションの定義で、アプリケーションが CA 信頼リストを使用するように指定する場合、アプリケーションが証明書のクライアント認証を正常に実行できるようにするには、このリストを定義しておかなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性

検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

DCM を使用してアプリケーションの CA 信頼リストを定義するには、以下のステップを完了します。

1. DCM を開始します。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
5. タスク・リストから「**CA 状況の設定 (Set CA status)**」を選択し、CA 証明書のリストを表示します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
6. アプリケーションが承認する必要のある CA 証明書をリストから選択し、「**使用可能 (Enable)**」をクリックして、CA 信頼リストを使用するアプリケーションのリストを表示してください。
7. このリストから、選択された CA をその信頼リストに追加する必要のあるアプリケーションを選択し、「**OK**」をクリックします。ページの先頭にメッセージが表示され、選択されたアプリケーションが、その CA、およびその CA が発行した証明書を承認することが示されます。

これで、クライアント認証用に証明書を要求するようにアプリケーションを構成できます。ご使用のアプリケーションの資料に記載された手順に従ってください。

シナリオ: 証明書を使用して内部アプリケーションおよび資源へのアクセスを保護する

状況

ユーザーは、ある会社 (MyCo., Inc.) のネットワーク管理者であり、この会社の人事部門は、法律的な問題や記録のプライバシー保護などの問題を扱っているとします。会社の従業員から、自分たちの個人的な諸手当や保険関係の情報にオンラインでアクセスできるようにしてほしいという要求が出されています。会社はこの要求に対する答えとして、従業員にこうした情報を提供するための社内 Web サイトを作成することにしました。ユーザーはこの社内 Web サイトの管理を任されています。

従業員は地理的に離れた 2 個所のオフィスに勤務しており、また、頻繁に出張する従業員もいることから、この情報がインターネット経由で伝送される際における機

密の保持について懸念しています。また、従来より、会社のデータへのアクセスを制限するために、ユーザー名とパスワードによる認証が使用されています。このデータは機密性が高く、またプライバシーに関係しているため、パスワードに基づくアクセス制限では十分とはいえないことが分かっています。パスワードでは、共用されたり、忘れてしまったり、また、時には盗まれたりすることさえあります。

研究を重ねた結果、ディジタル証明書を使用することで、必要なセキュリティーが得られるという結論に達しました。証明書を使用すると、Secure Sockets Layer (SSL) を使用してデータの伝送を保護することができます。また、パスワードの代わりに証明書を使用すると、より確実にユーザーを認証して、ユーザーがアクセスできる人事情報を制限することができます。

そこで、専用ローカル認証局 CA を設定し、すべての社員に証明書を発行して、社員にその証明書と iSeries のユーザー・プロファイルとを関連付けさせることを決定したとします。このタイプの専用証明書を発行すると、機密データへのアクセスを厳しく管理できるだけでなく、SSL を使用してそのデータのプライバシーを管理することもできます。結果的に、証明書を自身で発行することにより、データが安全に保たれ、特定のユーザーだけがそのデータにアクセスできる可能性が高くなります。

このシナリオの利点

このシナリオには、以下の利点があります。

- ディジタル証明書を使用して人事 Web サーバーへの SSL アクセスを構成すると、サーバーとクライアントの間で伝送される情報が確実に保護され、秘密にすることができます。
- クライアント認証のためにディジタル証明書を使用することで、より確実に許可ユーザーを識別する方法が提供されます。
- *専用* ディジタル証明書を使って、アプリケーションおよびデータへのアクセスの許可や制限を行う方法は、次のような条件下では実用的な選択です。
  - 特にユーザーの認証に関して、高いレベルのセキュリティーを必要とする場合。
  - 証明書を発行する対象のユーザーが信用できる場合。
  - ユーザーが、アプリケーションおよびデータへのアクセスを制御する、iSeries のユーザー・プロファイルをすでに持っている場合。
  - 独自の認証局 (CA) を運用したい場合。
- クライアント認証に専用証明書を使用すると、証明書と許可ユーザーの iSeries ユーザー・プロファイルをより簡単に関連付けることができます。このような証明書とユーザー・プロファイルの関連付けにより、認証時に HTTP Server が証明書所有者のユーザー・プロファイルを判別できるようになります。これにより、HTTP Server は、ユーザー・プロファイルにスワップして、そのユーザー・プロファイルに基づいて実行したり、ユーザー・プロファイル内の情報に基づいて該当ユーザーに関するアクションを実行したりすることができます。

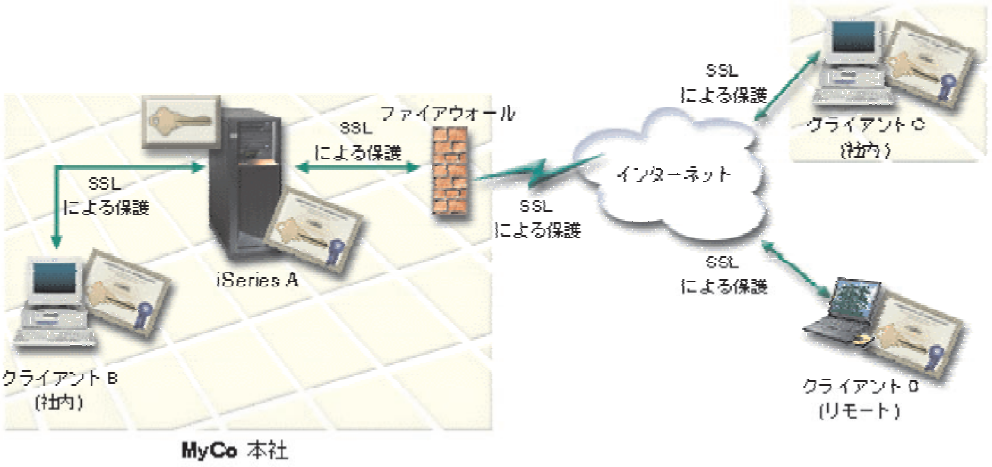
目的

このシナリオでは、MyCo., Inc. は、社内の人事 Web サイトが従業員に提供する機密の個人情報を保護するために、ディジタル証明書を使用します。同社はまた、この Web サイトにアクセスできるユーザーを認証するための、より確実な方法も求めています。

このシナリオの目的は以下のとおりです。
- 同社の人事用内部 Web サイトでは、ユーザーに提供するデータのプライバシーを保護するために、SSL を使用する必要があります。
- SSL 構成は、社内のローカル認証局 (CA) から提供される専用証明書を使用して行われる必要があります。
- 許可ユーザーは、SSL モードでこの人事 Web サイトにアクセスするために、有効な証明書を提示する必要があります。

詳細

次の図は、このシナリオのネットワーク構成状態を示したものです。



この図は、このシナリオの状況に関する、以下の情報を表しています。

会社の人事 Web サーバー - iSeries A
- iSeries A は、会社の Web ベースの人事アプリケーションをホストするサーバーです。
- iSeries A は OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries A には、Cryptographic Access Provider (5722-AC3) がインストールされています。
- iSeries A には、ディジタル証明書マネージャー (OS/400 オプション 34) および IBM HTTP Server for iSeries (5722-DG1) がインストールされ、構成されています。
- iSeries A は人事アプリケーションを実行します。このアプリケーションは、次のように構成されています。
  - SSL モードを必要とする。
  - ローカル認証局 (CA) が発行した専用証明書を使用して SSL 構成を行う。
  - クライアント認証のために証明書を必要とする。
- iSeries A は、クライアント B、C、および D がアプリケーションにアクセスする際に、その証明書を提示して SSL セッションを開始します。

- SSL セッションを初期化した後で、iSeries A は、人事アプリケーションへのアクセスを許可する前に、クライアント B、C、および D に対して有効な証明書の提示を要求します。この証明書の交換は、クライアント B、C、および D のユーザーに意識されることなく行われます。

従業員のクライアント・システム - クライアント B、クライアント C、およびクライアント D

- クライアント B は、iSeries A が置かれている MyCo の本社に勤務する従業員です。
- クライアント C は、本社から地理的に離れた場所にある MyCo の 2 番目のオフィスに勤務する従業員です。
- クライアント D は、遠隔地に勤務し、社用で頻繁に出張する従業員です。この従業員は、どこにいる場合でも人事 Web サイトへ安全にアクセスできなければなりません。
- クライアント B、C、および D は、人事アプリケーションにアクセスする従業員です。
- クライアント B、C、および D のクライアント・ソフトウェアには、アプリケーション証明書を発行したローカル CA 証明書のコピーがインストールされています。
- クライアント B、C、および D は iSeries A にある人事アプリケーションにアクセスします。iSeries A は、その ID を検証して SSL セッションを開始するために、クライアント・ソフトウェアにその証明書を提示します。
- クライアント B、C、および D のクライアント・ソフトウェアは、iSeries A からの証明書を受け入れるように構成されており、SSL セッションが開始されます。
- SSL セッションが開始された後で、クライアント B、C、および D は有効な証明書を提示しなければなりません。その後で、iSeries A がアプリケーションおよびその資源へのアクセスを許可します。

前提条件および前提事項

このシナリオは、以下の前提条件および前提事項に依存します。

1. IBM HTTP Server for iSeries は iSeries A で人事アプリケーションを実行します。HTTP Server for iSeries には 2 つのタイプ (オリジナルおよび Apache で拡張されたもの) があり、この情報の発表後に、大幅に改訂されたバージョンの HTTP Server が使用可能になる予定です。したがって、このシナリオでは、SSL を使用するように HTTP Server を構成するための*具体的な* 手順は示しません。このシナリオでは、あらゆるアプリケーションが SSL を使用するために必要な証明書を構成および管理するための手順を示します。
2. HTTP Server は、クライアント認証のために証明書を要求する機能を備えています。このシナリオでは、このシナリオでの証明書管理要件を構成するための、ディジタル証明書マネージャー (DCM) の使用手順を示します。ただし、このシナリオでは、HTTP Server における、証明書によるクライアント認証を構成するための*具体的な* 構成ステップは示しません。
3. iSeries A にある人事用の HTTP Server では、すでにパスワード保護が使用されています。
4. iSeries A は、ディジタル証明書マネージャー (DCM) をインストールし、使用するための要件を満たしています。

5. これまで誰も、iSeries A で DCM を構成または使用したことはありません。
6. DCM を使用してこのシナリオのタスクを実施する人には、ユーザー・プロファイルで特殊権限 *SECADM および *ALLOBJ が割り当てられていなければなりません。
7. iSeries A には IBM 4758-023 PCI 暗号化コプロセッサーはインストールされていません。

タスク・ステップ

このシナリオを実施するには、2 つのタスク・セットを完了する必要があります。そのうちの 1 つのタスク・セットでは、iSeries A にある人事アプリケーションを、SSL を使用し、ユーザー認証のために証明書を要求するように設定することができます。もう 1 つのタスク・セットでは、クライアント B、C、および D のユーザーに、人事アプリケーションとの SSL セッションに参加して、ユーザー認証のための証明書を取得させることができます。

人事 Web サーバー・アプリケーションのタスク・ステップ

このシナリオを実施するには、iSeries A で以下のタスクを行う必要があります。

1. 必要なすべての iSeries 製品をインストールし、構成するための前提条件となるステップをすべて行う。
2. SSL を使用し、サーバー・インスタンスのアプリケーション ID の記録を取るように、人事 HTTP Server を構成する。
3. ディジタル証明書マネージャー (DCM) を使用して、ローカル CA の作成および運用を行い、それを使用して人事 HTTP Server 用の証明書を発行する。また、このタスクを行うと、Web サーバー・アプリケーションに証明書が割り当てられて、そのアプリケーションが信頼する CA のリストにその CA が追加されます。
4. クライアント認証用に証明書を要求するように人事 Web サーバーを構成する。
5. 人事 HTTP Server を SSL モードで開始する。

クライアント構成のタスク・ステップ

このシナリオを実施するには、iSeries A にある人事 Web サーバーにアクセスする各ユーザー (クライアント B、C、および D) が、以下のタスクを行う必要があります。

6. 各自のブラウザー・ソフトウェアにローカル CA 証明書のコピーをインストールする。
7. ローカル CA からの証明書を要求する。

構成の詳細

このシナリオで説明するように、社内のアプリケーションおよび資源への保護されたアクセスを、証明書を使用して構成するには、以下のタスク・ステップに従ってください。

ステップ 1: 必要なすべての iSeries 製品をインストールするための前提条件となるタスクを行う

このシナリオを実施するための特定の構成タスクを実行する前に、必要なすべての iSeries 製品をインストールおよび構成するための前提条件となるタスクをすべて行う必要があります。

ステップ 2: SSL を使用するように人事 HTTP Server を構成する

iSeries A 上の人事用 HTTP Server の Secure Sockets Layer (SSL) 構成ステップは、オリジナル・バージョンの HTTP Server を使用するか、Apache で拡張されたバージョンの HTTP Server を使用するかによって異なります。

SSL を使用するように HTTP Server (オリジナル) を構成するための具体的な情報については、『HTTP Server でセキュア・サーバーを構成する』を参照してください。

SSL を使用するように HTTP Server (Apache 拡張バージョン) を構成するための具体的な情報については、『シナリオ: JKL により HTTP Server (Apache 拡張バージョン) で Secure Sockets Layer (SSL) 保護を使用可能にする』を参照してください。このシナリオでは、仮想ホストを作成し、SSL を使用するようにそのホストを構成するための、すべてのタスク・ステップを示します。 SSL を構成するための具体的なステップについては、『仮想ホストで SSL を使用可能にする』という見出しの項目を参照してください。

現行および将来の両方のバージョンの HTTP Server for iSeries (オリジナルまたは Apache 拡張バージョン) を構成するための追加情報については、『Web サービス提供』というトピックを参照してください。

ステップ 3: ローカル CA を作成し、運用する

Secure Sockets Layer (SSL) を使用するように人事 HTTP Server を構成した後で、SSL を開始するためにサーバーが使用する証明書を構成する必要があります。ユーザーはすでに、このシナリオの目的に基づいて、サーバーに対して証明書を発行するローカル認証局 (CA) を作成し、運用することを選択しています。

ディジタル証明書マネージャー (DCM) を使用してローカル CA を作成する際には、アプリケーションで SSL を使用可能にするうえで必要なすべての構成を確実に行うための、一連の手順が提供されます。これには、ローカル CA が Web サーバー・アプリケーションに対して発行する証明書の割り当てなどが含まれます。また、ローカル CA を Web サーバー・アプリケーションの CA 信頼リストに追加します。アプリケーションの信頼リストにローカル CA を含めると、そのアプリケーションは、そのローカル CA が発行する証明書を提示するユーザーを認識し、認証できるようになります。

ディジタル証明書マネージャー (DCM) を使用してローカル CA の作成および運用を行い、人事サーバー・アプリケーションに対して証明書を発行するには、以下のステップに従ってください。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、「**認証局 (CA) の作成 (Create a Certificate Authority (CA))**」を選択すると、一連のフォームが表示されます。これらのフォームが、ローカル CA の作成プロセスならびに、SSL、オブジェク

ト署名、および署名検査を実行するためのディジタル証明書を使用するために必要となる他のタスクを完了させるプロセスをガイドします。

注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) ボタンを選択してください。オンライン・ヘルプが表示されます。

3. このガイド・タスクのフォームを完成させます。これらのフォームを使用して、作業するローカル認証局 (CA) のセットアップに必要なすべてのタスクを実行するには、以下のようにします。
   a. ローカル CA についての識別情報を提供します。
   b. PC またはブラウザーにローカル CA 証明書をインストールして、ユーザー側のソフトウェアでローカル CA を認識し、そのローカル CA が発行する証明書の妥当性検査ができるようにします。
   c. ローカル CA についてのポリシー・データを選択します。

      注: 必ず、ローカル CA がユーザー証明書を発行できるように選択してください。
   d. 新規ローカル CA を使用して、アプリケーションが SSL 接続に使用できるサーバーまたはクライアント証明書を発行します。
   e. SSL 接続のためのサーバーまたはクライアント証明書を使用できるアプリケーションを選択します。

      注: 人事 HTTP Server 用のアプリケーション ID を必ず選択してください。
   f. 新規ローカル CA を使用して、アプリケーションがオブジェクトにディジタル署名するために使用できるオブジェクト署名証明書を発行します。このサブタスクは *OBJECTSIGNING 証明書ストアを作成します。これは、オブジェクト署名証明書を管理するために使用する証明書ストアです。

      注: このシナリオではオブジェクト署名証明書を使用しませんが、このステップは必ず行ってください。タスクのこの時点で取り消しを行うと、タスクが終了してしまうため、SSL 証明書の構成を完了するためにいくつかの別のタスクを行わなければなりません。
   g. ローカル CA 証明書を承認するアプリケーションを選択します。

      注: 人事 HTTP Server 用のアプリケーション ID を、このローカル CA を信頼するアプリケーションの 1 つとして必ず選択してください。

これにより Web サーバー・アプリケーションが SSL を使用するために必要な証明書の構成が完了し、この Web サーバー・アプリケーションを、ユーザー認証のために証明書を要求するように構成することができるようになりました。

ステップ 4: クライアント認証用に証明書を要求するように人事 Web サーバーを構成する

iSeries A 上の人事用 HTTP Server のクライアント認証用に証明書を要求するように Secure Sockets Layer (SSL) を構成するステップは、オリジナル・バージョンのアプリケーションを使用するか、Apache で拡張されたバージョンのアプリケーションを使用するかによって異なります。

クライアント認証用に証明書を要求するように HTTP Server (オリジナル) を構成するための具体的な情報については、『HTTP Server (オリジナル) での保護設定項目の作成』を参照してください。

クライアント認証に証明書を使用するように HTTP Server (Apache 拡張バージョン) を構成するための具体的な情報については、『Scenario: JKL enables Secure Sockets Layer (SSL) protection on their HTTP Server (powered by Apache)』を参照してください。この HTTP Server シナリオでは、仮想ホストを作成し、SSL およびクライアント認証用の証明書を使用するようにそのホストを構成するための、すべてのタスク・ステップを示します。 SSL およびクライアント認証用の証明書を構成するための具体的なステップについては、 『Enable SSL for a virtual host』という見出しの項目を参照してください。

現行および将来の両方のバージョンの HTTP Server for iSeries (オリジナルまたは Apache 拡張バージョン) を構成するための追加情報については、『Web サービス提供』というトピックを参照してください。

ステップ 5: 人事 Web サーバーを SSL モードで開始する

HTTP Server が、証明書割り当てが行われたことを判別し、それを使用して SSL セッションを開始できるようにするために、 HTTP Server を停止してから再始動しなければならないことがあります。

HTTP Server (オリジナル) を停止してから再始動するためには、「構成および管理 (Configuration and Administration)」フォームを使用して、以下のステップに従ってください。

1. 「**管理 (Administration)**」をクリックします。
2. 「**HTTP Server の管理 (Manage HTTP servers)**」をクリックします。
3. サーバーを選択します。
4. フォームで提供されるフィールドに、オプションの始動パラメーターを入力します。
5. 「**開始 (Start)**」をクリックします。

   注: 証明書の割り当てを行った際にこのサーバーが実行中であった場合には、サーバーを停止してから開始してください。「**再始動 (Restart)**」をクリックしたのでは、サーバーは、実行中に行われた証明書の変更を必ずしも判別できないことがあります。

HTTP Server (Apache 拡張バージョン) を停止してから再始動するためには、「構成および管理 (Configuration and Administration)」フォームを使用して、以下のステップに従ってください。

1. 「**管理 (Administration)**」をクリックします。
2. 左側のメニューで「**一般的なサーバー管理 (General Server Administration)**」の下の「**HTTP Server の管理 (Manage HTTP Servers)**」をクリックします。
3. 使用するサーバーを選択し、「**開始 (Start)**」または「**停止 (Stop)**」をクリックします。始動パラメーターの詳細については、オンライン・ヘルプを参照してください。

現行および将来のバージョンの HTTP Server for iSeries (オリジナルまたは Apache 強化バージョン) を管理するための追加情報については、『Web サービス提供』というトピックを参照してください。

これらのタスクが完了すると、人事アプリケーションを SSL モードで開始し、そのアプリケーションで提供されるデータのプライバシーの保護を開始することができます。

ステップ 6: ユーザーに、各自のブラウザー・ソフトウェアへローカル CA 証明書のコピーをインストールさせる

ユーザーが Secure Sockets Layer (SSL) 接続を提供しているサーバーにアクセスすると、サーバーは、ID の証明として、証明書をそのユーザーのクライアント・ソフトウェアに提示します。クライアント・ソフトウェアは、サーバーがセッションを確立する前に、サーバーの証明書を妥当性検査しなければなりません。サーバー証明書を妥当性検査するには、クライアント・ソフトウェアは、サーバー証明書を発行した認証局 (CA) の証明書のローカル保管コピーにアクセスできなければなりません。サーバーが公開インターネット CA の発行した証明書を提示する場合は、ユーザーのブラウザー、または他のクライアント・ソフトウェアは既に、その CA 証明書のコピーを所有していなければなりません。このシナリオのように、サーバーが専用ローカル CA の発行した証明書を提示する場合は、各ユーザーは、ディジタル証明書マネージャー (DCM) を使用して、そのローカル CA 証明書のコピーをインストールする必要があります。

各ユーザー (クライアント B、C、および D) は、下記のステップに従ってローカル CA 証明書のコピーを入手する必要があります。

1. DCM を開始します。
2. ナビゲーション・フレームの中で、「**ローカル CA 証明書の PC へのインストール (Install Local CA Certificate on Your PC)**」を選択して、ローカル CA 証明書をブラウザーにダウンロードしたり、ローカル CA 証明書をシステム上のファイルに保管したりするためのページを表示します。
3. 証明書をインストールするオプションを選択します。このオプションは、ローカル CA 証明書をトラステッド・ルートとして、ブラウザーにダウンロードします。これを行うと、ブラウザーが、この CA の発行した証明書を使用している Web サーバーとセキュア通信セッションを確立できるようになります。ブラウザーは、一連のウィンドウを表示して、インストール・プロセスの進行を支援します。
4. ディジタル証明書マネージャーのホーム・ページに戻るには、「**OK**」をクリックします。

ステップ 7: 各ユーザーに、ローカル CA へ証明書を要求させる

これまでのステップで、クライアント認証用に証明書を要求するように人事 Web サーバーを構成しました。ここで、ユーザーは、この Web サーバーへのアクセスの許可を得るためには、ローカル CA の発行した有効な証明書を提示しなければなりません。各ユーザーは、ディジタル証明書マネージャー (DCM) を使用し、「**証明書の作成 (Create Certificate)**」タスクを使用して証明書を取得しなければなりません。ローカル CA から証明書を取得するには、ローカル CA ポリシーが CA にユーザー証明書の発行を許可していることが必要です。

各ユーザー (クライアント B、C、および D) は、下記のステップに従って証明書を入手する必要があります。

1. DCM を開始します。
2. ナビゲーション・フレームの中で、「**証明書の作成 (Create Certificate)**」を選択します。
3. 作成する証明書のタイプとして、「**ユーザー証明書 (User certificate)**」を選択します。証明書に対する識別情報を入力するためのフォームが表示されます。
4. フォームに入力して、「**続行 (Continue)**」をクリックします。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
5. この時点で、DCM はユーザーのブラウザーで作業して秘密鍵および公開鍵を証明書に対して作成します。ブラウザーによって、このプロセスを進めるためのウィンドウが自動的に表示されます。これらのタスクについてのブラウザーの命令に従います。ブラウザーがこれらのキーを生成した後、確認ページが表示され、DCM が証明書を作成したことを示します。
6. 新規証明書をユーザーのブラウザー・ソフトウェアにインストールします。ブラウザーによって、このプロセスを進めるためのウィンドウが自動的に表示されます。ブラウザーが表示する指示に従って、このタスクを完了します。
7. 「**OK**」をクリックしてタスクを終了します。

処理時には、ディジタル証明書マネージャーによって、証明書と iSeries ユーザー・プロファイルが自動的に関連付けられます。

第 5 章 ディジタル証明書の概念

システムおよびネットワークのセキュリティー・ポリシーを高めるためにディジタル証明書を使う前に、ディジタル証明書とは何か、またディジタル証明書によるセキュリティー上のメリットとは何かについて、理解しておく必要があります。

ディジタル証明書とは、証明書の所有者を識別する妥当性検査をするディジタル信任状のことで、パスポートのようなものです。認証局 (CA) と呼ばれるトラステッド・パーティーが、ユーザーとサーバーまたはクライアント・アプリケーションに、ディジタル証明書を発行します。証明書が有効な信任状として信頼されるためには、CA に信用があることが前提となります。

ディジタル証明書の概念についての詳細は、以下のトピックを参照してください。

識別名
ディジタル証明書の識別特性の詳細について知るには、この情報をお読みください。

ディジタル署名
ディジタル署名の説明、および、これによってオブジェクトの保全性がどのように確保されるのかについて知るには、この情報をお読みください。

公開鍵と秘密鍵のペア
ディジタル証明書に関連付けられているセキュリティー・キーの詳細について知るには、この情報をお読みください。

認証局 (CA)
CA、すなわちディジタル証明書を発行するエンティティーの詳細については、この情報をお読みください。

CRL 位置
証明書取り消しリスト (CRL) とは何か、および、証明書の妥当性検査および認証のプロセスでそのリストをどう使うかを知りたい場合は、この情報をお読みください。

証明書ストア
証明書ストアとは何か、および、ディジタル証明書マネージャー (DCM) を使用して、証明書ストアおよびそこに含まれる証明書を処理する方法について知りたい場合は、この情報をお読みください。

暗号
暗号とは何か、および、ディジタル証明書の暗号機能を使用してセキュリティーを提供する方法を知りたい場合は、この情報をお読みください。

Secure Sockets Layer (SSL)
SSL の簡単な説明については、この情報をお読みください。

識別名

各 CA には、CA が証明書を発行するために必要とする識別情報を判断するポリシーが存在します。公開インターネット認証局の中には、名前や電子メール・アドレスなどのわずかな情報しか必要としないものもあります。他の公開 CA には、もっと多くの情報を必要とし、証明書の発行前にその識別情報のより厳密な証明を要求するものもあります。たとえば、Public Key Infrastructure Exchange (PKIX) 規格を

サポートする CA では、要求元が、証明書の発行前に登録機関 (RA) を通じて識別情報を検証する必要があります。したがって、証明書を信任状として受け入れ、使用するつもりなら、CA の識別要件を調べて、その要件がセキュリティー上の必要性に合うかどうかを判断しなければなりません。

識別名 (DN) とは、証明書の所有者の識別情報を示す用語で、証明書本体の一部です。証明書を発行する CA の識別ポリシーに応じて、DN にはさまざまな情報が含まれます。ディジタル証明書マネージャー (DCM) を使用すると、専用認証局を運用して、専用証明書を発行することができます。また、公開インターネット CA が組織用に発行する証明書のための、DN 情報とキーのペアを生成することもできます。どちらのタイプの証明書にも含まれる DN 情報には、次のようなものがあります。

- 証明書所有者の一般名
- 組織
- 組織内の団体
- 市
- 州
- 国

DCM を使用して専用証明書を発行する場合は、その証明書用に、たとえば次のような追加の DN 情報が提供される場合もあります。

- バージョン 4 の IP アドレス
- 完全修飾ドメイン・ネーム
- 電子メール・アドレス

証明書を使用して仮想私設ネットワーク (VPN) 接続を構成する予定の場合は、この追加情報が役立ちます。

ディジタル署名

電子文書またはその他のオブジェクトのディジタル署名は、暗号形式で作成され、書面文書での署名に相当します。ディジタル署名により、オブジェクトの発信元の証明が提供され、また、そのオブジェクトの保全性を検証する手段が提供されます。ディジタル証明書の所有者は、その証明書の秘密鍵を使用してオブジェクトに「署名」します。オブジェクトの受信側では、対応する公開鍵を使って署名を復号し、署名済みオブジェクトの保全性を検証し、送信側をソースとして検証します。

認証局 (CA) では、発行する証明書に署名します。この署名は、認証局の秘密鍵で暗号化されたデータ・ストリングで構成されています。したがって、認証局の公開鍵を使って署名を復号すると、すべてのユーザーが証明書の署名を検証できます。

ディジタル署名は、ユーザーまたはアプリケーションがディジタル証明書の秘密鍵を使用してオブジェクト上に作成する、電子的な署名のことです。オブジェクト上のディジタル署名により、署名者 (署名キーの所有者) の ID と、オブジェクトの発信元との、固有の電子的な結び付けが行われます。ディジタル署名を含んでいるオブジェクトにアクセスする際には、オブジェクトの署名を検証することにより、そのオブジェクトの送信元が正当であることを確かめることができます (たとえば、ダウンロードしようとしているアプリケーションが、IBM などのような許可された

送信元から実際に送られているかどうかなどを確認できます)。この検証プロセスにより、署名後にオブジェクトに対して未許可の変更が行われたかどうかを判別することもできます。

ディジタル署名の働きを示す例

あるソフトウェア開発者が iSeries アプリケーションを作成しました。この開発者は、このアプリケーションを配布するにあたり、顧客のために便利でコスト効果の高い手段として、インターネット経由での配布を行いたいと考えています。しかし彼は、顧客がインターネット経由でのプログラムのダウンロードに懸念を抱いていることを知っています。適正なプログラムであることを装いながら、実はウィルスなどの有害なプログラムを含んでいるオブジェクトの問題が増えていることを考えると、このような心配は無理もないことです。

したがって、彼の会社がアプリケーションの適正な送信元であることを顧客が確認できるように、アプリケーションにディジタル式の署名を行うことにしました。彼は、一般的に知られている公開認証局から入手したディジタル証明書の秘密鍵を使用して、アプリケーションに署名を行います。そのうえで、そのアプリケーションを顧客がダウンロードできるようにします。ダウンロード・パッケージの一部として、オブジェクトへの署名に使用したディジタル証明書のコピーを含めます。顧客は、アプリケーション・パッケージをダウンロードするときに、証明書の公開鍵を使用してアプリケーションの署名を検証することができます。このプロセスにより、顧客はアプリケーションの識別および検証を行うことができ、また、アプリケーション・オブジェクトの内容が署名後に変更されていないことを確認することができます。

公開鍵と秘密鍵のペア

ディジタル証明書にはそれぞれ、互いに関連した暗号鍵のペアがあります。このキーのペアは、秘密鍵と公開鍵で構成されています。 (署名検査証明書は例外で、関連した公開鍵しか持っていません。)

公開鍵は所有者のディジタル証明書の一部であり、すべてのユーザーが使用できます。しかし、秘密鍵は、キーの所有者が保護しており、その所有者しか使用できません。この制限されたアクセスにより、キーを使用する通信の安全性が保たれます。

証明書の所有者は、これらのキーを使用することにより、キーが提供する暗号セキュリティー機能を利用できます。たとえば、証明書の所有者は、証明書の秘密鍵を使って、ユーザーとサーバーとの間で送信されるデータ (メッセージ、文書、およびコード・オブジェクトなど) に「署名」したり、データを暗号化したりすることができます。署名付きオブジェクトの受信側は、署名者の証明書に含まれている公開鍵を使用して署名を復号することができます。このようなディジタル署名により、オブジェクトの送信元の信頼性が保証され、そのオブジェクトの保全性を検査する手段が提供されます。

認証局 (CA)

認証局 (CA) とは、ユーザーとサーバーにディジタル証明書を発行できる、承認された中央管理エンティティーのことです。証明書が有効な信任状として信頼されるには、CA に信用があることが前提となります。CA は、その秘密鍵を使って、証明書の発行元の妥当性検査をするために発行する証明書に、ディジタル署名を作成します。受信側は CA 証明書の公開鍵を使用して、CA が発行し、署名した証明書の認証性を検証することができます。

CA は、VeriSign のような公衆の商用エンティティーである場合と、組織が内部用に運用する専用エンティティーである場合があります。いくつかの企業が、インターネット・ユーザーのために商用の認証局サービスを提供しています。ディジタル証明書マネージャー (DCM) を使うと、公開 CA の証明書も専用 CA の証明書も管理できます。

また、独自の専用 CA を運用して、システムやユーザーに専用証明書を発行する場合にも、DCM は使用できます。CA でユーザー証明書が発行されると、DCM ではその証明書を、そのユーザーの iSeries システム・ユーザー・プロファイルに自動的に関連付けます。これにより、証明書のアクセス権と許可が、所有者のユーザー・プロファイルのアクセス権と許可と同じになります。

トラステッド・ルート状況

トラステッド・ルートとは、認証局の証明書に特別に与えられる呼称です。トラステッド・ルートの指定があると、ブラウザーまたは他のアプリケーションは、認証局 (CA) が発行する証明書を認証し、受け入れることができます。

認証局の証明書をブラウザーにダウンロードすると、ブラウザーを使用して、その認証局をトラステッド・ルートに指定することができます。証明書の使用をサポートするその他のアプリケーションも、CA を承認するように構成してからでなければ、特定の CA が発行する証明書を認証し、承認することはできません。

DCM を使用すると、証明書ストアの認証局 (CA) 証明書の承認状況を、使用可能にしたり使用不可にしたりすることができます。CA 証明書を使用可能にした場合、アプリケーションがそれを使用して、CA が発行する証明書の認証および受け入れを行えるように指定することができます。CA 証明書を使用不可にすると、アプリケーションがそれを使用して、CA が発行する証明書の認証および受け入れを行えるように指定することはできません。

認証局のポリシー・データ

ディジタル証明書マネージャーを使って認証局 (CA) を作成すると、CA のポリシー・データを指定できます。CA のポリシー・データには、CA の署名特権が記述されています。ポリシー・データによって次のことが決まります。

- CA でユーザー証明書を発行し、それに署名できるかどうか
- CA で発行される証明書の有効期限

証明書取り消しリスト (CRL) の位置

証明書取り消しリスト (CRL) は、特定の認証局 (CA) の、無効な証明書および取り消された証明書をすべてリスト表示したファイルです。CA は定期的にその CRL を更新し、利用者はそれを Lightweight Directory Access Protocol (LDAP) ディレクトリーで公表できます。フィンランドの SSH など少数の CA では、ユーザーが直接アクセスできる LDAP ディレクトリーで、CRL そのものを公表しています。CA がその CRL を公表する場合、証明書には、CRL 配布ポイントの拡張を Uniform Resource ID (URI) 形式で組み込んで、このことが明記されます。

ディジタル証明書マネージャー (DCM) を使用すると、CRL 位置情報を定義および管理して、ユーザーが使用する証明書や外部から受け入れる証明書の認証を、より厳密に行うことができます。CRL の位置定義には、CRL を保管する Lightweight Directory Access Protocol (LDAP) サーバーの、位置とアクセス情報が示されています。

証明書の認証を実行するアプリケーションは、特定の CA の CRL 位置が定義されていればそこにアクセスして、その CA が特定の証明書を取り消していないことを確認します。DCM を使用すると、アプリケーションが証明書の認証中に CRL 処理を実行するのに必要とする、CRL 位置情報を定義および管理することができます。証明書の認証のために CRL 処理を実行するアプリケーションやプロセスの例としては、仮想私設ネットワーク (VPN) の Internet Key Exchange (IKE) サーバー、Secure Sockets Layer (SSL) 対応アプリケーション、オブジェクト署名プロセスなどがあります。また、CRL 位置を定義し、それを CA 証明書と関連付ける場合、DCM は、指定された CA が発行する証明書の妥当性検査プロセスの一部として、CRL 処理を実行します。

証明書ストア

証明書ストアは特殊なキー・データベース・ファイルで、ディジタル証明書マネージャー (DCM) はこれを使用して、ディジタル証明書を保管します。証明書ストアには、ユーザーがキーの保管に 4758 暗号化コプロセッサーを使用することを選択した場合を除き、証明書の秘密鍵も含まれます。 DCM では、いくつかのタイプの証明書ストアを作成および管理することができます。 DCM は、証明書ストアを構成する IFS ディレクトリーおよび IFS ファイルへのアクセス制御とパスワードとを組み合わせて、証明書ストアへのアクセスを制御します。

証明書ストアは、そこに含まれる証明書のタイプに基づいて分類されます。それぞれの証明書ストアで実行できる管理タスクは、その証明書ストアに含まれる証明書のタイプによって異なります。DCM では、ユーザーが作成し、管理することのできる、以下の事前定義された証明書ストアが提供されています。

ローカル認証局 (CA)
ローカル CA が作成されると、DCM はこの証明書ストアを使用して、ローカル CA 証明書とその秘密鍵を保管します。この証明書ストアの証明書を使用すると、ローカル CA を使用して発行される証明書に署名することができます。ローカル CA が証明書を発行すると、DCM は、CA 証明書のコピー (秘密鍵のないもの) を適切な証明書ストア (たとえば *SYSTEM) に入れ、認証に使用します。アプリケーションは CA 証明書を使用して、証明書の発信元を検証し、SSL ネゴシエーションの一部としてその妥当性を検査して、資源への権限を認可します。

***SYSTEM**
DCM のこの証明書ストアは、アプリケーションが Secure Sockets Layer (SSL) 通信セッションに参加するために使用する、サーバーまたはクライアント証明書を管理するために提供されます。IBM iSeries アプリケーション (および他の数多くのソフトウェア開発者によるアプリケーション) は、*SYSTEM 証明書ストアの証明書のみを使用するように作成されています。ユーザーが DCM を使用してローカル CA を作成する際、DCM がそのプロセスの一環としてこの証明書ストアを作成します。サーバーまたはクライアント・アプリケーションで使用する証明書を VeriSign などの公開 CA から入手することを選択した場合、この証明書ストアはユーザーが作成しなければなりません。

***OBJECTSIGNING**
DCM が提供するこの証明書ストアは、オブジェクトにディジタル署名をする際に使用される証明書を管理するためのものです。また、この証明書ストア内のタスクにより、オブジェクト上にディジタル署名を作成したり、オブジェクト上のディジタル署名を表示および検証したりすることもできます。ユーザーが DCM を使用してローカル CA を作成する際、DCM がそのプロセスの一環としてこの証明書ストアを作成します。オブジェクトに署名するために使用する証明書を VeriSign などの公開 CA から入手することを選択した場合、この証明書ストアはユーザーが作成しなければなりません。

***SIGNATUREVERIFICATION**
DCM が提供するこの証明書ストアは、オブジェクトのディジタル署名の認証性を検証する際に使用される証明書を管理するためのものです。ディジタル署名を検証できるように、この証明書ストアには、オブジェクトに署名した証明書のコピーが含まれていなければなりません。証明書ストアには、オブジェクト署名証明書を発行した CA の CA 証明書のコピーも含まれていなければなりません。これらの証明書は、現行システムにあるオブジェクト署名証明書をストアにエクスポートすることによって入手することも、オブジェクト署名者から受け取った証明書をインポートすることによって入手することもできます。

その他のシステム証明書ストア
この証明書ストアは、SSL セッションに使用されるサーバーまたはクライアント証明書の代替保管場所となります。「他のシステム証明書ストア (Other System Certificate Store)」は、SSL 証明書を保管する、ユーザー定義の 2 次的な証明書ストアです。「その他のシステム証明書ストア (Other System Certificate Store)」オプションを選択すると、証明書に SSL_Init API を使用してプログラマチックなアクセスを行い、証明書を使用して SSL セッションを確立する、ユーザー作成のアプリケーション用の証明書を管理することができます。この API を使用すると、アプリケーションは、ユーザーが特に指定した証明書ではなく、証明書ストアのデフォルト証明書を使用することができます。通常、この証明書ストアは、DCM の以前のリリースから証明書をマイグレーションする場合、あるいは SSL で使用するために証明書の特別なサブセットを作成する場合に、使用されます。

注: iSeries サーバーに IBM 4758 PCI 暗号化コプロセッサーがインストールされている場合は、証明書 (オブジェクト署名証明書は除きます) 用に、別の秘密鍵保管オプションを選ぶこともできます。コプロセッサー自体に秘密鍵を保管することも、コプロセッサーを使用して秘密鍵を暗号化し、それを証明書ストアではなく特別のキー・ファイルに保管することもできます。

DCM は、パスワードを使用して証明書ストアへのアクセスを制御します。また、統合ファイル・システム・ディレクトリーと、証明書ストアを構成するファイルの、アクセス制御を保守します。ローカル認証局 (CA)、*SYSTEM、*OBJECTSIGNING、*SIGNATUREVERIFICATION の各証明書ストアは、統合ファ

イル・システム内の特定のパスになければなりませんが、その他のシステム証明書ストアは、統合ファイル・システム内の任意の場所に置くことができます。

暗号

暗号は、データを安全に保つ技術です。暗号により、情報を保管したり他のユーザーと通信したりすることができるほかに、関係のないユーザーに保管された情報や通信の内容を知られないようにすることができます。暗号化とは、理解可能なテキストを理解不可能なデータ (暗号テキスト) に変換することです。復号とは、理解不可能なデータから理解可能なテキストに戻すことです。この 2 つのプロセスには、数学上の公式またはアルゴリズム、そしてデータの秘密の順序 (キー) が関係します。

暗号には次の 2 種類があります。

- **共用 / 秘密鍵 (対称)** 暗号方式では、1 つのキーを発信側と受信側が他のユーザーに知られないように共有します。暗号化と復号の両方で、同じキーを使用します。
- **公開鍵 (非対称)** 暗号方式では、暗号化と復号で、別々のキーを使用します。情報を送受信するユーザーは、公開鍵と秘密鍵からなるキーのペアを持ちます。公開鍵は、通常はディジタル証明書内で自由に配布されていますが、秘密鍵は、所有者が安全に保管しています。2 つのキーは数学上関係がありますが、公開鍵から秘密鍵を引き出すことは実質的には不可能です。特定のユーザーの公開鍵で暗号化されたオブジェクト (メッセージなど) は、関連する秘密鍵でのみ復号することができます。反対に、サーバーまたはユーザーが、秘密鍵を使用してオブジェクトに「署名」して、受信者がそれに対応する公開鍵を使用してディジタル署名を復号し、そのオブジェクトの送信元と保全性を検証することもできます。

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) は、Netscape によって作成されたもので、クライアントとサーバー間のセッション暗号化の業界標準です。SSL は、非対称キー、すなわち公開鍵の暗号を使用して、サーバーとクライアント間のセッションを暗号化します。クライアントとサーバー・アプリケーションでは、ディジタル証明書の交換時に、このセッション・キーをネゴシエーションします。キーは 24 時間後に自動的に期限が切れ、SSL プロセスでは、サーバー接続とクライアントごとに別々のキーが作成されます。その結果、非許可ユーザーがセッション・キーを代行受信し復号したとしても、その後のセッションでそのキーを使って盗聴することはできません。

第 6 章 DCM の計画

ディジタル証明書マネージャー (DCM) を使用して会社のディジタル証明書を効果的に管理するためには、セキュリティー・ポリシーの一部としてディジタル証明書をどのように使用するのかについて、全体的な計画を立てておく必要があります。

DCM を使用する計画の立て方、およびディジタル証明書がユーザーのセキュリティー・ポリシーにどう適合するかについての詳細は、以下のトピックを参照してください。

DCM の使用に関する要件
インストールが必要なソフトウェアおよび DCM を使用するようにシステムをセットアップする際に必要なその他の情報については、これをお読みください。

ディジタル証明書のタイプ
DCM を使用して管理することのできるさまざまな証明書のタイプについて知るには、この情報を参照してください。

公開証明書と専用証明書
証明書によって提供されるより高度なセキュリティーを利用するために、証明書をどのように使用するかを決めた後、自分のビジネス上の必要性に最も適合する証明書のタイプを決定する方法を知りたい場合は、この情報を使用してください。ユーザーは、公開 CA から取得した証明書を使用することも、専用 CA を作成、運用して証明書を発行することもできます。どちらの方法で証明書を取得するかは、証明書をどのように使うかによって決まります。

Secure Sockets Layer (SSL) 通信のためのディジタル証明書
アプリケーションがセキュア通信セッションを確立できるように、証明書を使用する方法が知りたい場合は、この情報を利用してください。

ユーザー認証のディジタル証明書
証明書を使用して、iSeries サーバー資源にアクセスするユーザーをさらに厳密に認証する方法を知りたい場合は、この情報を利用してください。

仮想プライベート・ネットワーク (VPN) 接続を認証するためのディジタル証明書
証明書を VPN 接続構成の一部として使用する方法を知りたい場合は、この情報を利用してください。

オブジェクトに署名するためのディジタル証明書
証明書を使用して、オブジェクトの保全性を確実にする方法や、オブジェクトのディジタル署名を検査してその認証性を確認する方法を知りたい場合は、この情報を利用してください。

オブジェクトの署名検査のためのディジタル証明書
証明書を使用して、オブジェクトのディジタル署名を検査してその認証性を確認する方法を知りたい場合は、この情報を利用してください。

DCM のセットアップ要件

ディジタル証明書マネージャー (DCM) は、アプリケーションのディジタル証明書を集中的に管理するために使用できる、無料の iSeries フィーチャーです。 DCM を正常に使用するには、以下の項目を必ず実行してください。

- Cryptographic Access Provider ライセンス・プログラム (5722-AC3) をインストールします。この暗号プロダクトにより、エクスポートおよびインポート規則に基づいて、暗号アルゴリズムに認められる最大キー長が決まります。証明書を作成するには、この製品をインストールする必要があります。
- OS/400 のオプション 34 をインストールします。これはブラウザー・ベースの DCM フィーチャーです。
- IBM HTTP Server for iSeries (5722-DG1) をインストールして、*ADMIN サーバー・インスタンスを開始します。
- Web ブラウザーおよび HTTP Server *ADMIN インスタンスを使用して DCM フィーチャーにアクセスできるように、システムに TCP を構成してください。

注: 必要な製品がすべてインストールされないと、証明書を作成できません。必要な製品がインストールされていないと、DCM から、足りない構成要素をインストールするようエラー・メッセージが表示されます。

ディジタル証明書のタイプ

ディジタル証明書はいくつかの種類に分類されます。分類は、証明書の使用方法に基づいています。ディジタル証明書マネージャー (DCM) を使用すると、以下のタイプの証明書を管理することができます。

認証局 (CA) の証明書

認証局の証明書は、証明書を所有する認証局 (CA) の識別の妥当性検査をするディジタル信任状です。認証局の証明書には、認証局についての識別情報が含まれているのに加えて、公開鍵も含まれています。受信側は CA 証明書の公開鍵を使用して、CA が発行し、署名した証明書の認証性を検証することができます。認証局の証明書は、VeriSign などの別の CA によって署名されることもありますが、独立エンティティーである場合は自己署名することもあります。ディジタル証明書マネージャーで作成する CA は独立エンティティーになります。受信側は CA 証明書の公開鍵を使用して、CA が発行し、署名した証明書の認証性を検証することができます。 SSL、オブジェクトへの署名、またはオブジェクト署名の検証のために証明書を使用するには、その証明書を発行した CA の CA 証明書のコピーも必要になります。

サーバーまたはクライアントの証明書

サーバーまたはクライアントの証明書は、セキュア通信のために証明書を使用するサーバーまたはクライアント・アプリケーションを識別する、ディジタル信任状です。サーバーまたはクライアントの証明書には、アプリケーションを所有する組織に関する識別情報 (たとえばシステムの識別名) も含まれています。また、証明書にはシステムの公開鍵が含まれています。サーバーがセキュア通信のために Secure Sockets Layer (SSL) を使用するときには、ディジタル証明書が必要です。ディジタル証明書をサポートするアプリケーションでは、クライアントがサーバーにアクセスするときに、サーバーの識別を検証するためにサーバーの証明書を検査できます。次に、アプリケーションは、クライアントとサーバー間の SSL 暗号化セッションを開始する際の基礎として、証明書の認証を使用できます。これらのタイプの証明書の管理は、*SYSTEM 証明書ストアからのみ行うことができます。

オブジェクト署名の証明書
オブジェクト署名の証明書は、オブジェクトにディジタル「署名」をして、使用される証明書です。オブジェクトに署名することにより、オブジェクトの保全性と、オブジェクトの送信元または所有権の両方を検証する手段を提供することができます。この証明書を使用して、Integrated File System (IFS) 内のほとんどのオブジェクトや *CMD オブジェクトなどを含むさまざまなオブジェクトに署名することができます。署名可能なすべてのオブジェクトを含むリストが、『オブジェクト署名および署名の検査』のトピックに掲載されています。オブジェクト署名の証明書の秘密鍵を用いてオブジェクトに署名すると、そのオブジェクトの受信者がオブジェクト署名を正しく認証するためには、その受信者に、それに対応する署名検査証明書へのアクセス権がなければなりません。これらのタイプの証明書の管理は、*OBJECTSIGNING 証明書ストアからのみ行うことができます。

署名検査証明書
署名検査証明書は、オブジェクト署名証明書のコピーですが、これにはその証明書の秘密鍵は含まれていません。署名検査証明書の公開鍵を使用すると、オブジェクト署名証明書で作成したディジタル署名を認証することができます。署名を検査することにより、オブジェクトの発信元を判別することができ、また、そのオブジェクトが署名後に変更されていないかどうかを判別することができます。これらのタイプの証明書の管理は、*SIGNATUREVERIFICATION 証明書ストアからのみ行うことができます。

ユーザー証明書
ユーザー証明書とは、証明書を所有するクライアントまたはユーザーの識別の妥当性検査をするディジタル信任状です。今では、多くのアプリケーションが、ユーザー名やパスワードではなく証明書を使用して、資源に対してユーザーの認証を行う機能をサポートしています。ディジタル証明書マネージャー (DCM) は、専用 CA が発行するユーザーの証明書を、そのユーザーの iSeries ユーザー・プロファイルと自動的に関連付けます。また、DCM を使用すると、他の認証局で発行されるユーザー証明書を、そのユーザーの iSeries ユーザー・プロファイルと関連付けることもできます。

ディジタル証明書マネージャー (DCM) を使用して証明書を管理する場合、DCM は、以上のような分類に従って証明書を編成し、証明書とそれに関連した秘密鍵を証明書ストアに入れます。

注: iSeries サーバーに IBM 4758 PCI 暗号化コプロセッサーがインストールされている場合は、証明書 (オブジェクト署名証明書は除きます) 用に、別の秘密鍵保管オプションを選ぶこともできます。コプロセッサー自体に秘密鍵を保管することもできます。あるいは、コプロセッサーを使用して秘密鍵を暗号化し、それを証明書ストアではなく特別のキー・ファイルに保管することもできます。ただし、ユーザー証明書とその秘密鍵は、ユーザーのシステム上の、ブラウザー・ソフトウェアか、他のクライアント・ソフトウェア・パッケージが使用するファイルのいずれかに保管されます。

公開証明書と専用証明書

証明書を使用することに決定したら、セキュリティーの必要性に応じて、最適な証明書のタイプを選択する必要があります。証明書を取得するには、次の方法のいずれかを選択します。
- 公開インターネット認証局 (CA) から証明書を購入する。
- ユーザーおよびアプリケーション用の専用証明書を発行する独自の CA を運用する。

- 公開インターネット CA と独自の CA から入手した証明書を組み合わせて使用する。

この 3 つの方法のどれを選択するかは、いろいろな要因によって決まりますが、最も重要な要因の 1 つが、証明書が使用される環境です。ビジネスおよびセキュリティー上の必要性に適した選択肢を決めるのに役立つ情報を、いくつか挙げておきます。

公開証明書の使用

公開インターネット CA では、必要な料金を支払うユーザーに証明書を発行します。しかし、インターネット CA から証明書を発行するには、まず、本人であることの証明が必要です。しかし、このレベルの証明は、CA の識別ポリシーによってさまざまです。CA から証明書を取得しようと、あるいは CA が発行する証明書を承認しようと決める前に、CA の厳重な識別ポリシーがセキュリティー上の必要性に適しているかどうかを検討する必要があります。 Public Key Infrastructure for X.509 (PKIX) 規格の変化に伴い、比較的新しい公開 CA の中には、証明書の発行に、これまでよりはるかに厳格な識別規格を設けているものがあります。このような PKIX CA から証明書を取得するプロセスはかなり複雑ですが、その CA が発行する証明書を使用すれば、特定ユーザーによるアプリケーションへのアクセスの保護が、より確実に保証されることになります。ディジタル証明書マネージャー (DCM) を使うと、これらの新しい証明書規格を使用する PKIX CA が発行する証明書を使用および管理できます。

また、公開 CA を使って証明書を発行するのに要するコストについても考慮する必要があります。証明書を発行する必要があるサーバーまたはクライアント・アプリケーション、およびユーザーの数が限られている場合は、コストは重大な要素ではないかもしれません。しかし、クライアント認証用に公開証明書を必要とする*専用*ユーザーを、多数抱えている場合は、コストが特に重要になってきます。この場合は、公開 CA が発行する証明書の特定のサブセットだけを受け入れるようにサーバー・アプリケーションを構成するのに必要な、管理作業やプログラミング作業も考慮に入れなければなりません。

公開 CA からの証明書を使用すると、時間や資源を節約できます。これは、多くのサーバーやクライアント、ユーザー・アプリケーションが、一般的に知られている公開 CA であればほとんどを認識するように構成されているためです。また、他の企業やユーザーも、専用 CA が発行する証明書より、一般的に知られている公開の CA が発行する証明書の方を、認識し、承認すると考えられます。

専用証明書の使用

独自のローカル CA を作成すると、企業や組織などの、範囲を限定したシステムとユーザーに証明書を発行できます。 独自の CA の作成および保守を行うことにより、グループ内の承認されたユーザーにのみ証明書を発行できます。これにより、証明書の所有者、つまり資源へのアクセス権所有者をより厳重に管理することができるため、セキュリティーが強化されます。独自のローカル CA を維持することの潜在的なデメリットは、時間と資源を費やす必要があるという点です。しかし、ディジタル証明書マネージャー (DCM) を使用することにより、このプロセスは容易になります。

ローカル CA を使用してクライアント認証用の証明書をユーザーに対して発行する場合、そのユーザーの証明書を iSeries のユーザー・プロファイルと関連付けるかどうかを決定する必要があります。ユーザーの証明書を iSeries のユーザー・プロファイルと関連付けたい場合には、そのユーザーにローカル CA から DCM を介して証明書を入手させることができます。また、V5R2 以降では、API を使用して証明書を非 iSeries ユーザーへプログラマチックに発行することにより、それらのユーザーが iSeries のユーザー・プロファイルを持たなくても、クライアント認証用の専用証明書を使用できるようにすることができます。

注: いずれの CA を使用して証明書を発行する場合でも、システム上のアプリケーションでどの CA を承認するかは、システム管理者が決めます。一般的に知られている CA の証明書のコピーがブラウザー内に見つかった場合、その CA により発行されたサーバー証明書を承認するように、ブラウザーを設定することができます。ただし、その CA 証明書が *SYSTEM 証明書ストアになければ、サーバーは、その CA が発行したユーザーまたはクライアント証明書を承認できません。CA の発行するユーザー証明書を承認するには、CA から CA 証明書のコピーを取得する必要があります。これは正しいファイル形式である必要があり、ユーザーは、その証明書を DCM 証明書ストアに追加しなければなりません。

公開証明書と専用証明書のどちらを使用するのがビジネス上、およびセキュリティー上の必要性に最も適しているのかを決める際には、一般的な証明書の使用方法のシナリオを参照することが役立ちます。

関連タスク

証明書の使用方法と使用する証明書のタイプを決定した後、ディジタル証明書マネージャーを使用して計画を実行する方法について、次のトピックを参照してください。

- 『専用 CA の作成および運用』では、専用証明書を発行する CA を運用する場合に実行しなければならないタスクについて説明しています。
- 『公開インターネット CA からの証明書の管理』では、一般的に知られている公開 CA (PKIX CA など) からの証明書を使用する場合に、実行しなければならないタスクについて説明しています。
- 『ローカル CA を使用して他の iSeries システムの証明書を発行』では、専用 CA の発行した証明書を複数のシステムで使用する場合に、実行しなければならないタスクについて説明しています。

SSL セキュア通信のためのディジタル証明書

ディジタル証明書を使用すると、アプリケーションを構成して Secure Sockets Layer (SSL) を使用し、セキュア通信セッションを確立することができます。SSL セッションを確立する場合、サーバーは必ず、接続を要求するクライアントが妥当性検査を行えるように、証明書のコピーを提供します。SSL 接続を使用すると、次のことが行われます。

- クライアントまたはエンド・ユーザーに、そのサイトが認証されていることを保証する。

- 通信セッションを暗号化して、その接続を介してやり取りされるデータのプライバシーが保たれることを保証する。

サーバーおよびクライアント・アプリケーションは、以下のように、共同してデータのセキュリティーを確保します。

1. サーバー・アプリケーションは、クライアント (ユーザー) アプリケーションに対し、サーバー識別の証明として証明書を提示する。
2. クライアント・アプリケーションは、発行された認証局証明書に対して、サーバーの識別を検査する。 (クライアント・アプリケーションには、ローカルに保管された該当する CA (認証局) 証明書に対するアクセス権が必要です。)
3. サーバーおよびクライアント・アプリケーションは暗号化のための対称キーを承認し、その対称キーを使用して通信セッションを暗号化する。
4. (オプション) ここでサーバーは、クライアントが要求した資源へのアクセスを許可する前に、クライアントに識別の証明を提供するよう要求することができる。識別の証明として証明書を使用するには、通信しているアプリケーションが、ユーザー認証のための証明書の使用を、サポートしていなければなりません。

SSL は、SSL ハンドシェーク処理の間、非対称キー (公開鍵) アルゴリズムを使用して、対称キーのネゴシエーションを行います。この対称キーは、続いてアプリケーションのデータを、その特定の SSL セッション用に暗号化および復号するのに使用されます。つまり、サーバーとクライアントは異なるセッション・キーを使用し、これらのキーは、接続ごとに、一定時間が過ぎると自動的に有効期限が切れます。誰かが特定のセッション・キーを代行受信して復号するようなことが万一あっても、そのセッション・キーを使ってそれ以後に使用されるキーを推測することはできません。

ユーザー認証のディジタル証明書

従来から、ユーザーはユーザー名とパスワードに基づいて、アプリケーションまたはシステムから資源へのアクセス権を許可されています。ディジタル証明書 (ユーザー名とパスワードの代わりに) を使って、多くのサーバー・アプリケーションとユーザー間のセッションを認証および許可するようにすると、システム・セキュリティーをさらに増強できます。また、ディジタル証明書マネージャー (DCM) を使用すると、ユーザーの証明書をそのユーザーの iSeries ユーザー・プロファイルと関連付けることもできます。これを行うことで、証明書の権限と許可は、関連付けられたプロファイルと同じものになります。 V5R2 以降では、API を利用し、ローカル認証局をプログラマチックに使用して非 iSeries ユーザーに証明書を発行することができます。これらの API を使用することにより、iSeries のユーザー・プロファイルを割り当てたくない場合でも、それらのユーザーに対して専用証明書を発行できるようになります。

ディジタル証明書は電子認証として機能し、証明書を提示するユーザーが本人であるかどうかを検証します。この点では、証明書はパスポートと同様の役割を果たします。どちらもユーザーの識別を確立し、識別のための固有の数値を含み、その信任状を本物だと確認する認識可能な発行権限を持っています。証明書の場合は、認証局 (CA) が証明書を発行し、それを本物の証明書と確認する信頼のおける第三者機関として機能します。

認証のために、証明書では公開鍵とそれに関連した秘密鍵が利用されます。証明書を発行する CA は、これらのキーと、証明書の所有者に関するその他の情報を、識別情報としてその証明書自体にバインドします。

SSL セッション中のクライアント認証のために証明書の使用をサポートするアプリケーションは、今ではますます増えています。現時点では、以下の iSeries アプリケーションがクライアント認証用の証明書のサポートを提供しています。

- Telnet サーバー
- IBM HTTP Server (オリジナルのものと Apache で強化したもの)
- ディレクトリー・サービス (LDAP) サーバー
- マネージメント・セントラル
- Client Access Express (iSeries ナビゲーターを含む)
- FTP サーバー

今後、クライアント認証用の証明書のサポートを提供するアプリケーションが追加される可能性があります。特定のアプリケーションがこのサポートを提供しているかどうかを判別するには、当該アプリケーションの資料を参照してください。

証明書は、次のようないくつかの理由で、ユーザー認証の強力な手段となります。

- ユーザーはパスワードを忘れる可能性があります。そこで、ユーザーはユーザー名とパスワードを暗記するか記録して、それを忘れないようにしなければなりません。その結果、非許可ユーザーが、許可ユーザーからユーザー名とパスワードを入手することが容易になります。証明書はファイルまたはその他の電子的な場所に保管されているので、認証のための証明書へのアクセスとその提示は、クライアント・アプリケーション (ユーザーではなく) によって行われます。このため、ユーザーが非許可ユーザーと証明書を共用する可能性は、非許可ユーザーがユーザーのシステムにアクセスできない限り、少なくなります。また、スマート・カードを不正な使用から保護する方法として、スマート・カードに証明書をインストールすることもできます。
- 証明書には秘密鍵が含まれていますが、識別のためにこれを証明書と共に送信することはありません。このキーは、システムが暗号化処理および復号処理を行うときに使用されます。証明書にはこれに対応する公開鍵があり、受信側はこれを使用して、秘密鍵で署名されているオブジェクトの送信側を識別します。
- 多くのシステムには 8 文字以下のパスワードが必要ですが、その程度のパスワードでは、推測によってパスワードを盗まれる危険があります。証明書の暗号鍵の長さは数百文字に達します。この長さとそのランダムな性質により、暗号鍵はパスワードよりはるかに解読が難しくなっています。
- ディジタル証明書のキーには、データの保全性やプライバシーなど、パスワードでは実現できない機能がいくつかあります。証明書とそれに関連したキーを使用すると、次のようなことが実現できます。
  - データの変更を検出することにより、データ保全性を保証する。
  - 特定のアクションが確実に実行されたことを証明する。これは否認防止と呼ばれます。
  - Secure Sockets Layer (SSL) を使用して通信セッションを暗号化し、データ転送のプライバシーを保証する。

SSL セッション時にクライアント認証のための証明書を使用する iSeries サーバー・アプリケーションの構成について詳しく知りたい場合は、『SSL によるアプリケーションの保護』を参照してください。

VPN 接続のディジタル証明書

iSeries の仮想私設ネットワーク (VPN) 接続を確立する方法の 1 つとして、ディジタル証明書が使用できるようになりました。動的な VPN 接続のどちらのエンドポイントでも、もう一方のエンドポイントを認証してから接続を開始しなければなりません。エンドポイントの認証は、両端の Internet Key Exchange (IKE) サーバーがそれぞれ行います。認証が正常に行われれば、次に IKE サーバーは、VPN 接続の保護に使用される暗号化の方法とアルゴリズムについてネゴシエーションします。

V5R1 より古いバージョンでは、IKE サーバーが互いに認証できる方法は、事前共用キーを使用するというものだけでした。事前共用キーを使用する方法は、このキーを、VPN のもう一方のエンドポイントの管理者に手動で送る必要があるため、それほど安全とは言えません。キーを送るプロセスで、そのキーが他者の目に触れる可能性があるためです。

事前共用キーを使用せず、ディジタル証明書を使用してエンドポイントを認証することで、このリスクを回避できます。IKE サーバーは、相手側サーバーの証明書を認証して接続を確立し、接続保護のためにサーバーが使用する暗号化の方法とアルゴリズムについてネゴシエーションします。

ディジタル証明書マネージャー (DCM) を使用すると、IKE サーバーが動的 VPN 接続の確立に使用する証明書を管理することができます。それにはまず、IKE サーバー用に、公開証明書を使用するか、専用証明書を発行するかを決めなければなりません。

VPN インプリメンテーションには、証明書に、標準の識別名情報だけでなく、それに代わるサブジェクト名情報 (たとえば、ドメイン・ネームや電子メール・アドレスなど) が含まれている必要があります。DCM ユーティリティーの専用 CA を使用して証明書を発行する場合、その証明書の代替サブジェクト情報を指定することができます。この情報を指定することにより、iSeries の VPN 接続の認証のためにその情報を必要とする他の VPN インプリメンテーションとの互換性が保証されます。

VPN 接続用の証明書を管理する方法についてもっと詳しく知りたい場合は、以下の情報源を参照してください。

- 以前に DCM を使用して証明書を管理した経験がない場合は、入門用として次のトピックが役に立ちます。
  - 『ローカル、専用 CA の作成および運用』では、DCM を使用してアプリケーション用の専用証明書を発行する方法について説明しています。
  - 『公開インターネット CA からの証明書の管理』では、DCM を使用して公開 CA からの証明書を処理する方法について説明しています。
- 現在、DCM を使用して他のアプリケーションの証明書を管理している場合は、アプリケーションが既存の証明書を使用するように指定したり、そのアプリケーションが受け入れ、認証することのできる証明書を指定する方法について以下のトピックを参照してください。
  - 『アプリケーションに対する証明書割り当ての管理』では、DCM を使用して既存の証明書をアプリケーション (IKE サーバーなど) に割り当てる方法について説明しています。

– 『アプリケーションの CA 信頼リストの定義』では、アプリケーションがクライアント (または VPN) 認証を受け入れる際に、そのアプリケーションが承認できる CA を指定する方法について説明しています。

オブジェクトに署名するためのディジタル証明書

OS/400 では、V5R1 から、オブジェクトにディジタル「署名」をするための、証明書の使用をサポートしています。オブジェクトへのディジタル署名を利用することにより、オブジェクトの内容の保全性とその発信元の両方を検査する方法が提供されます。オブジェクト署名のサポートは、オブジェクトを変更できる人を制御する、これまでの iSeries システム・ツールを補うものです。従来の制御機能では、オブジェクトがインターネットまたは他の非トラステッド・ネットワーク経由で転送されている間や、iSeries 以外のシステムに保管されている間は、非許可ユーザーによる不正操作からオブジェクトを保護することができません。また、従来の方法による制御では、オブジェクトに対して未許可の変更または改ざんが行われたかどうかを、必ずしも判別することができません。オブジェクトでディジタル署名を使用すると、署名済みオブジェクトに対して行われた変更を確実に検出する方法が提供されます。

オブジェクトにディジタル署名を入れるということは、証明書の秘密鍵を使用して、オブジェクト内のデータの数学的要約を暗号化して追加するということです。この署名により、データが勝手に変更されるのを防ぐことができます。オブジェクトとその内容は暗号化されず、ディジタル署名によって秘密にされます。しかし、要約自体は、勝手に変更されるのを防ぐために暗号化されます。オブジェクトが転送中に変更されていないこと、そのオブジェクトが正当な送信元からのものであることを確認したい場合は、署名のある証明書の公開鍵を使って、元のディジタル署名を検査することができます。署名が一致しない場合は、データが変更された可能性があります。その場合、受信側はそのオブジェクトを使用せず、代わりに署名者に連絡して、署名済みオブジェクトのコピーを改めて入手することができます。

ディジタル署名の使用がセキュリティー上の必要性やポリシーに適合すると判断した場合は、公開証明書と専用証明書の発行のどちらを使用すべきかを検討してください。オブジェクトを一般ユーザーに配布したい場合には、一般的に知られている公開証明書 (CA) から得られた証明書を使用してオブジェクトの署名を行うことを検討してください。公開証明書を使用すると、配布されるオブジェクトの署名を、誰でも簡単かつ低コストで確認することができます。しかし、オブジェクトを組織内のみで配布する予定の場合には、ディジタル証明書マネージャー (DCM) を使用して独自のローカル CA を運用し、オブジェクトに署名するための証明書を自分で発行することもできます。ローカル CA から得られた専用証明書を使用してオブジェクトに署名するほうが、一般的に知られている公開 CA から証明書を購入するよりも費用が少なくて済みます。

オブジェクトの署名は、そのオブジェクトに署名したシステムを表すものであって、そのシステムの特定のユーザーを表すわけではありません (ただしそのユーザーには、オブジェクトに署名するための証明書を使用する正当な権限がなくてはなりません)。オブジェクトに署名したり、オブジェクトの署名を検証したりするために使用する証明書を管理するには、ディジタル証明書マネージャー (DCM) を使用してください。 DCM を使用してオブジェクトに署名したり、オブジェクトの署名を検査したりすることもできます。

オブジェクトの署名検査のためのディジタル証明書

iSeries では、V5R1 から、オブジェクトのディジタル署名を検証するための、証明書の使用をサポートしています。署名済みオブジェクトが転送中に変更されていないこと、およびそのオブジェクトが、一般に認められている正当な送信元からのものであることを確認したい場合は、誰でも、署名を行った証明書の公開鍵を使って、元のディジタル署名を検査することができます。署名が一致しない場合は、データが変更された可能性があります。その場合、受信側はそのオブジェクトを使用せず、代わりに署名者に連絡して、署名済みオブジェクトのコピーを改めて入手することができます。

オブジェクトの署名は、そのオブジェクトに署名したシステムを表すものであって、そのシステムの特定のユーザーを表すわけではありません。ディジタル署名を検証するプロセスの一環として、ユーザーは、ユーザーが承認する認証局と、オブジェクトへの署名を承認する証明書を決定する必要があります。ある CA を承認することに決めたとしても、そのトラステッド CA が発行した証明書を使用して作成される署名を承認するかどうかは、改めて選択することができます。CA を承認しないことに決めたら、その CA が発行する証明書や、その証明書を使用して作成される署名も、承認しないと決めたことになります。

オブジェクトの復元検査 (QVFYOBJRST) のシステム値

署名の検証を実行することにした場合、まず決めなければならない重要なことの 1 つが、システムに復元されるオブジェクトにとって、署名がどれほど重要であるかを決定することです。これは、QVFYOBJRST と呼ばれるシステム値で制御されます。このシステム値をデフォルトに設定しておくと、署名のないオブジェクトは復元できますが、署名のあるオブジェクトは、その署名が有効なものである場合だけ復元可能になります。システムがオブジェクトを署名済みと定義するのは、そのオブジェクトの署名をシステムが承認している場合だけです。システムは、オブジェクトのそれ以外の「承認されていない」署名は無視し、そのオブジェクトを署名がないものと同様に扱います。

QVFYOBJRST システム値で使用できる値は、すべての署名を無視するものから、システムが復元するすべてのオブジェクトに有効な署名を必要とするものまで、いくつかの種類があります。このシステム値は復元される予定の実行可能オブジェクトにだけ影響を与えるもので、保管ファイルや IFS ファイルには影響を与えません。このシステム値およびその他のシステム値の使用についての詳細は、Information Center の『システム値ファインダー』を参照してください。

証明書や CA の承認を決定するためばかりでなく、オブジェクトの署名を検証するために使用する証明書を管理するためにも、ディジタル証明書マネージャー (DCM) を使用してください。 DCM を使用してオブジェクトに署名したり、オブジェクトの署名を検査したりすることもできます。

第 7 章 DCM の構成

ディジタル証明書マネージャー (DCM) は、アプリケーションおよびユーザーのディジタル証明書を管理するために使用できる、ブラウザー・ベースのユーザー・インターフェースを提供します。ユーザー・インターフェースは、ナビゲーション・フレームとタスク・フレームという 2 つの主なフレームに分かれています。

証明書またはそれらを使用するアプリケーションを管理するタスクを選択するには、ナビゲーション・フレームを使用します。メイン・ナビゲーション・フレームに個別タスクが直接表示される場合もありますが、ナビゲーション・フレームのほとんどのタスクは、カテゴリー別に編成されます。たとえば、「**証明書の管理 (Manage Certificates)**」は、「証明書の表示 (View certificate)」、「証明書の更新 (Renew certificate)」、「証明書のインポート (Import certificates)」など、各種の個別ガイド・タスクを含んだタスク・カテゴリーです。ナビゲーション・フレームの 1 つの項目が複数のタスクから成るカテゴリーになっている場合は、その左側に矢印が表示されます。矢印は、カテゴリー・リンクを選択したときに、タスクの拡張リストが表示されて実行するタスクを選択できることを示しています。

「**高速パス (Fast Path)**」カテゴリーを除き、ナビゲーション・パスのタスクはそれぞれ、一連のステップを実行してタスクを迅速および簡単に完了させる、ガイド・タスクです。「高速パス (Fast Path)」カテゴリーは、経験のある DCM ユーザーが、中心となる一連のページから各種関連タスクに迅速にアクセスすることを可能にする、一連の証明書およびアプリケーション管理機能を提供します。

ナビゲーション・フレームで使用可能なタスクの種類は、作業している証明書ストアによって異なります。ナビゲーション・フレームに表示されるタスクのカテゴリーおよびその数についても、iSeries ユーザー・プロファイルが保有している権限によって異なります。CA の操作タスク、ユーザーが使用する証明書を管理するすべてのタスク、およびその他のシステム・レベルのタスクは、iSeries のセキュリティー担当者か管理者だけが使用できます。セキュリティー担当者か管理者がこれらのタスクを表示して使用するには、*SECADM および *ALLOBJ の特殊権限が必要です。このような特殊権限を持たないユーザーは、ユーザー証明書機能だけにアクセスできます。

DCM を構成し、これを使用して証明書の管理を開始する方法については、以下のトピックを参照してください。

DCM の開始
iSeries のディジタル証明書マネージャー・フィーチャーを利用する方法については、これを参照してください。

ディジタル証明書のはじめてのセットアップ
証明書を使用するために必要となるものをすべてセットアップするために、はじめにどのように DCM を使用すればよいのかを、ここで説明しています。公開インターネット認証局 (CA) から証明書の管理を開始する方法または、専用ローカル CA を作成および運用して証明書を発行する方法について学習します。

システムおよびネットワーク・セキュリティーを強化するため、インターネット環境でのディジタル証明書の詳細については、VeriSign Web サイトが役立ちます。VeriSign Web サイトは、他のインターネット・セキュリティー問題と同様に、ディジタル証明書のトピックに関する幅広いライブラリーを提供しています。これらのライブラリーは、「VeriSign Help Desk」  にあります。

ディジタル証明書マネージャーの開始

ディジタル証明書マネージャー (DCM) の機能を使用できるようにするには、DCM を開始する必要があります。DCM を正常に開始するには、以下のタスクを実行してください。

1. 5722 SS1 オプション 34 をインストールします。これは、ディジタル証明書マネージャー (DCM) です。

   5722 DG1 をインストールします。これは IBM HTTP Server for iSeries です。

   5722 AC3 をインストールします。これは、証明書の公開鍵と秘密鍵のペアを生成したり、エクスポートされた証明書ファイルを暗号化したり、インポートされた証明書ファイルを復号化したりするために、V5R2 DCM が使用する暗号プロダクトです。
2. 以下のように iSeries ナビゲーションを使用して、HTTP Server *ADMIN インスタンスを開始します。
   a. **iSeries ナビゲーター**を開始します。
   b. メイン・ツリー・ビューの iSeries サーバーをダブルクリックします。
   c. 「**ネットワーク (Network)**」をダブルクリックします。
   d. 「**サーバー (Servers)**」をダブルクリックします。
   e. 「**TCP/IP**」をダブルクリックします。
   f. 「**HTTP 管理 (HTTP Administration)**」を右クリックします。
   g. 「**開始 (Start)**」をクリックします。
3. Web ブラウザーを開始します。
4. ブラウザーを使用して、システムの http://*your_system_name*:2001 にある「iSeries タスク (iSeries Tasks)」ページに移動します。
5. DCM フィーチャーを利用するには、「iSeries タスク (iSeries Tasks)」ページのプロダクト・リストから「**ディジタル証明書マネージャー (Digital Certificate Manager)**」を選択します。

以前のバージョンの DCM からマイグレーションする場合には、このページに、システムのアップグレードに必要な詳細が表示されます。

ディジタル証明書のはじめてのセットアップ

ディジタル証明書マネージャー (DCM) の左側のフレームは、タスク・ナビゲーション・フレームです。このフレームを使用して、証明書およびそれらを使用するアプリケーションを管理するための、多岐にわたる種類のタスクを選択することができます。使用可能なタスクの種類は、(ある場合) オープンしている証明書ストアの種類およびユーザー・プロファイル権限によって決まります。ほとんどのタスクは、*ALLOBJ および *SECADM 特殊権限がある場合しか使用できません。

ディジタル証明書マネージャー (DCM) をはじめて使用するときは、(前のバージョンの DCM からマイグレーションしたのでない限り) 証明書ストアが存在しません。そのために、ナビゲーション・フレームには、必要な権限がある場合に、以下のタスクしか表示されません。

- ユーザー証明書の管理。
- 新規証明書ストアの作成。
- 認証局 (CA) の作成。(注: このタスクを使用して専用 CA を作成すると、このタスクはリストに表示されなくなります。)
- CRL 位置の管理。
- PKIX 要求場所の管理。

証明書ストアがシステム上にすでに存在する場合にも (たとえば、以前のバージョンの DCM からマイグレーションする場合)、DCM は、左側のナビゲーション・フレームに、限られた数のタスクまたはタスク・カテゴリーのみを表示します。ほとんどの証明書およびアプリケーション管理タスクの処理を開始できるようにするには、まず適切な証明書ストアにアクセスしなければなりません。特定の証明書ストアをオープンするには、ナビゲーション・フレームの「**証明書ストアの選択 (Select a Certificate Store)**」をクリックします。

DCM のナビゲーション・フレームには、「**セキュア接続 (Secure Connection)**」ボタンもあります。このボタンを使用して、2 番目のブラウザー・ウィンドウを立ち上げ、Secure Sockets Layer (SSL) を使用して、セキュア接続を初期化することができます。この機能を正常に使用するには、まず、SSL を使用してセキュア・モードで作動するように、IBM HTTP Server for iSeries を構成しなければなりません。次に、セキュア・モードで HTTP Server を始動します。SSL 操作が可能となるように HTTP Server を構成して始動していない場合は、エラー・メッセージが表示され、ブラウザーはセキュア・セッションを開始しません。

はじめに

証明書を使用して、セキュリティー関連の目標をいくつも達成したい場合があるかもしれませんが、最初に実行することは、証明書を取得する計画の仕方によって決まります。公開証明書を使用するか、専用証明書を発行するかによって、初めて DCM を使用するときに取ることができる 2 つの主な方法があります。

ローカル CA の作成および運用を行い、アプリケーションに対して証明書を発行する。

公開インターネット CA からの証明書を管理して、アプリケーションで使用する。

ローカル CA の作成および運用

セキュリティー上の必要性とポリシーを慎重に検討した結果、ローカル認証局 (CA) を運用して、アプリケーションに専用証明書を発行することに決定しました。ディジタル証明書マネージャー (DCM) を使用して、独自のローカル CA の作成および運用を行うことができます。DCM は、CA の作成プロセスと、これを使用してアプリケーションに証明書を発行する方法をユーザーに示すガイド・タスク・パスを提供しています。ガイド・タスク・パスを使用すると、ディジタル証明書を使用し

て、SSL を使用するようにアプリケーションを構成したり、オブジェクトに署名したり、オブジェクトの署名を検査したりするのに必要なすべての条件が確実にそろいます。

注: IBM HTTP Server for iSeries で証明書を使用する場合は、DCM を実行して、処理する前に、Web サーバーを作成して構成しておく必要があります。Web サーバーを構成して SSL を使用すると、そのサーバーにアプリケーション ID が生成されます。このアプリケーション ID はメモに控えておき、DCM を使用してこのアプリケーションが SSL に使用する証明書を指定できるようにします。

DCM を使用してサーバーに証明書を割り当てるまでは、サーバーを終了して再始動しないでください。証明書を割り当てる前に、Web サーバーの *ADMIN インスタンスを終了して再始動すると、サーバーは始動せず、DCM を使用してサーバーに証明書を割り当てることはできません。

DCM を使用して、ローカル CA を作成し、運用するには、以下のステップに従ってください。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、「**認証局 (CA) の作成 (Create a Certificate Authority (CA))**」を選択すると、一連のフォームが表示されます。これらのフォームが、ローカル CA の作成プロセスならびに、SSL、オブジェクト署名、および署名検査を実行するためのディジタル証明書を使用するために必要となる他のタスクを完了させるプロセスをガイドします。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) ボタンを選択してください。オンライン・ヘルプが表示されます。
3. このガイド・タスクのすべてのフォームを完成させます。これらのフォームを使用して、作業するローカル認証局 (CA) のセットアップに必要なすべてのタスクを実行するには、以下のようにします。
   a. ローカル CA 証明書の秘密鍵の保管方法を選択します。(このステップが組み込まれるのは、iSeries に IBM 4758-023 PCI 暗号化コプロセッサーがインストールされている場合のみです。システムに暗号化コプロセッサーがない場合、DCM は、ローカル認証局 (CA) 証明書ストアに証明書とその秘密鍵を保管します)。
   b. ローカル CA についての識別情報を提供します。
   c. PC またはブラウザーにローカル CA 証明書をインストールして、ユーザー側のソフトウェアでローカル CA を認識し、その CA が発行する証明書の妥当性検査ができるようにします。
   d. ローカル CA についてのポリシー・データを選択します。
   e. 新規ローカル CA を使用して、アプリケーションが SSL 接続に使用できるサーバーまたはクライアント証明書を発行します。(iSeries に IBM 4758-023 PCI 暗号化コプロセッサーがインストールされている場合、このステップにより、サーバーまたはクライアント証明書の秘密鍵の保管方法を選択することができます。システムにコプロセッサーがない場合、DCM は、*SYSTEM 証明書ストアに証明書とその秘密鍵を自動的に保管します。DCM は、このサブタスクの一環として *SYSTEM 証明書ストアを作成します。)
   f. SSL 接続のためのサーバーまたはクライアント証明書を使用できるアプリケーションを選択します。

注: 公開インターネット CA からの SSL の証明書を管理するために、これまで DCM を使用して、*SYSTEM 証明書ストアを作成していた場合は、このステップも直前のステップも実行しないでください。

g. 新規ローカル CA を使用して、アプリケーションがオブジェクトにディジタル署名するために使用できるオブジェクト署名証明書を発行します。このサブタスクは *OBJECTSIGNING 証明書ストアを作成します。これは、オブジェクト署名証明書を管理するために使用する証明書ストアです。
h. オブジェクトにディジタル署名するオブジェクト署名証明書を使用できるアプリケーションを選択します。

注: 公開インターネット CA からのオブジェクト署名証明書を管理するために、これまで DCM を使用して、*OBJECTSIGNING 証明書ストアを作成していたのであれば、このステップも直前のステップも実行しないでください。

i. ローカル CA 証明書を承認するアプリケーションを選択します。

ガイド・タスクを完了すると、SSL を使用してセキュア通信を行うようにアプリケーションを構成するために必要な条件がすべてそろいます。

アプリケーションの構成後、SSL 接続を介してアプリケーションにアクセスするユーザーは、DCM を使用してローカル CA 証明書のコピーを入手しなければなりません。ユーザーごとに証明書のコピーを持ち、ユーザーのクライアント・ソフトウェアがこれを使用して、SSL 折衝プロセスの一環として、サーバー識別を認証できるようにします。ユーザーは、DCM を使用して、ローカル CA 証明書をファイルにコピーしたり、証明書をブラウザーにダウンロードしたりすることができます。ユーザーによるローカル CA 証明書の保管方法は、アプリケーションへの SSL 接続を確立するために使用する、クライアント・ソフトウェアによって決まります。

このローカル CA を使用して、ユーザー・ネットワーク内の他の iSeries システムのアプリケーションへ証明書を発行することもできます。

DCM を使用してユーザー証明書を管理する方法、およびローカル CA が発行する証明書を認証するためのローカル CA 証明書のコピーの入手方法については、以下のトピックを参照してください。

ユーザー証明書の管理
ユーザーが DCM を使用して、証明書を取得したり、既存の証明書に iSeries ユーザー・プロファイルを関連付けたりする方法を学べます。

API を使用して証明書を非 iSeries ユーザーへプログラマチックに発行する
証明書を iSeries ユーザー・プロファイルと関連付けずに、ローカル CA を使用して専用証明書をユーザーに発行する方法を学べます。

専用 CA 証明書のコピーの取得
専用 CA 証明書のコピーを取得して、自己の PC にインストールし、CA が発行するサーバー証明書を認証できるようにする方法を学べます。

ユーザー証明書の管理

ユーザーとエンド・ユーザーは、ディジタル証明書マネージャー (DCM) を使用して、エンド・ユーザーが Secure Sockets Layer (SSL) セッションに参加する際に必要な証明書を管理できます。

ユーザーが SSL 接続を介して公開サーバーまたは内部サーバーにアクセスする場合、ユーザーは、サーバーの証明書を発行した認証局 (CA) 証明書のコピーを持っていなければなりません。ユーザーが CA 証明書を持っていなければならないのは、ユーザーのクライアント・ソフトウェアがサーバー証明書の認証性を妥当性検査して接続を確立するのに必要だからです。サーバーが公開 CA からの証明書を使用している場合は、エンド・ユーザーのソフトウェアは、既にその CA 証明書を持っていなければなりません。その結果、DCM アドミニストレーターとしてのユーザーも、エンド・ユーザーも、SSL セッションに参加する前に、何のアクションも取る必要がありません。しかし、サーバーが専用ローカル CA からの証明書を使用している場合は、エンド・ユーザーは、サーバーと SSL セッションを確立する前に、ローカル CA 証明書のコピーを取得していなければなりません。

さらに、サーバー・アプリケーションが証明書を介したクライアント認証をサポートしており、それを要求する場合は、ユーザーは、サーバーが提供する資源にアクセスするために、受け入れ可能なユーザー証明書を提示しなければなりません。セキュリティー・ニーズに基づいて、ユーザーは、公開インターネット CA からの証明書を提示するか、またはユーザーが操作しているローカル CA から取得した証明書を提示できます。サーバー・アプリケーションが、現在、iSeries ユーザー・プロファイルを持っている内部ユーザーに資源へのアクセスを提供する場合、ユーザーは、DCM を使用してユーザーの証明書をユーザー・プロファイルに追加できます。この関連付けによって、ユーザーが証明書を提示したときに、そのユーザー・プロファイルが認可または拒否するとおりに、資源へのアクセス権または制限が行われるようになります。

ディジタル証明書マネージャー (DCM) を使用すると、iSeries ユーザー・プロファイルに割り当てられる証明書を管理できます。*SECADM および *ALLOBJ の特殊権限を備えたユーザー・プロファイルを持っている場合、自分自身または他のユーザーに対するユーザー・プロファイル証明書割り当てを管理できます。証明書ストアがオープンしていない場合、またはローカル認証局 (CA) 証明書ストアがオープンしている場合は、ナビゲーション・フレームの中の「**ユーザー証明書の管理 (Manage User Certificates)**」を選択して適切なタスクにアクセスできます。異なる証明書ストアがオープンしている場合、ユーザー証明書タスクは、「**証明書の管理 (Manage Certificates)**」下のタスクに統合されます。

*SECADM および *ALLOBJ ユーザー・プロファイル特殊権限を持たないユーザーは、自分の証明書の割り当てのみを管理できます。これらのユーザーは、「**ユーザー証明書の管理 (Manage User Certificates)**」を選択して、自分のユーザー・プロファイルに関連付けられた証明書の表示、自分のユーザー・プロファイルからの証明書の除去、または自分のユーザー・プロファイルへの、別の CA からの証明書の割り当てが可能なタスクにアクセスできます。ユーザーは、自分のユーザー・プロファイルの特殊権限を所持しているかどうかにかかわらず、メイン・ナビゲーション・フレームから「**証明書の作成 (Create Certificate)**」タスクを選択することにより、ローカル CA からユーザー証明書を入手することができます。

DCM を使用してユーザー証明書を管理および作成する方法の詳細については、以下のトピックを参照してください。

ユーザー証明書の作成
この情報では、ユーザーがローカル CA を使ってクライアント認証のために証明書を発行する方法を学べます。

ユーザー証明書の割り当て
この情報では、所有している証明書と自分のユーザー・プロファイルとを関連付ける方法を学べます。証明書は、別のシステム上の専用ローカル CA から得られたものでも、一般的に知られているインターネット CA から得られたものでも、どちらでも利用できます。証明書を自分のユーザー・プロファイルに割り当てる前に、発行 CA はサーバーによってトラステッドにされている必要があり、証明書がそのシステム上のユーザー・プロファイルに既に関連付けされているものであってはなりません。

ユーザー証明書の作成: ユーザー認証のためにディジタル証明書を使用する場合は、ユーザーが証明書を持っている必要があります。ディジタル証明書マネージャー (DCM) を使用して専用ローカル認証局 (CA) を運用する場合は、ローカル CA を使って証明書を各ユーザーに発行できます。各ユーザーは、DCM にアクセスし、「**証明書の作成 (Create Certificate)**」タスクを使用して証明書を取得しなければなりません。ローカル CA から証明書を取得するには、CA ポリシーが CA にユーザー証明書の発行を許可していることが必要です。

ローカル CA から証明書を取得するには、以下のステップを完了します。
1. DCM を開始します。
2. ナビゲーション・フレームの中で、「**証明書の作成 (Create Certificate)**」を選択します。
3. 作成する証明書のタイプとして、「**ユーザー証明書 (User certificate)**」を選択します。証明書に対する識別情報を入力するためのフォームが表示されます。
4. フォームに入力して、「**続行 (Continue)**」をクリックします。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
5. この時点で、DCM はユーザーのブラウザーで作業して秘密鍵および公開鍵を証明書に対して作成します。ブラウザーによって、このプロセスを進めるためのウィンドウが自動的に表示されます。これらのタスクについてのブラウザーの命令に従います。ブラウザーがこれらのキーを生成した後、確認ページが表示され、DCM が証明書を作成したことを示します。
6. 新規証明書をユーザーのブラウザー・ソフトウェアにインストールします。ブラウザーによって、このプロセスを進めるためのウィンドウが自動的に表示されます。ブラウザーが表示する指示に従って、このタスクを完了します。
7. 「**OK**」をクリックしてタスクを終了します。

処理時には、ディジタル証明書マネージャーによって、証明書と iSeries ユーザー・プロファイルが自動的に関連付けられます。

ユーザーがクライアント認証の際に提示する、別の CA からの証明書に、ユーザー・プロファイルと同じ権限を持たせたい場合、ユーザーは DCM を使用して、自己のユーザー・プロファイルに証明書を割り当てることができます。

ユーザー証明書の割り当て: ユーザー認証のためにディジタル証明書を使用する場合は、ユーザーが証明書を持っている必要があります。エンド・ユーザーが証明書

を公開インターネット認証局 (CA) から提示しなければならない場合、ディジタル証明書マネージャー (DCM) を使用して、これらの証明書を自己のユーザー・プロファイルに割り当てることができます。これにより、ユーザーとエンド・ユーザーは DCM を使用して、これらの証明書を管理できます。

「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを使用するには、ディジタル証明書マネージャー (DCM) へのアクセスに使用している HTTP Server にセキュア・セッションが必要です。セキュア・セッションがあるかどうかは、DCM へのアクセスに使用した URL のポート番号によって決まります。DCM へのアクセスのデフォルト・ポートである、ポート 2001 を使用した場合は、セキュア・セッションはありません。また、セキュア・セッションに切り替える前に、HTTP Server を SSL を使用するように構成する必要があります。

このタスクを選択すると、新規ブラウザー・ウィンドウが表示されます。セキュア・セッションがない場合は、セキュア・セッションを開始するために、「**ユーザー証明書の割り当て (Assign a User Certificate)**」をクリックするよう、DCM がプロンプトを出します。その後、DCM は、ブラウザーと Secure Sockets Layer (SSL) 折衝を開始します。

これらの折衝の一環として、ブラウザーは、HTTP Server を識別する証明書を発行した認証局 (CA) を信頼するかどうかについてプロンプトを出すことがあります。また、ブラウザーは、サーバー証明書そのものを受け入れるかどうかについてプロンプトを出すこともあります。

ブラウザーに、CA の信頼とサーバー証明書の受け入れを許可した後、サーバーは、証明書をクライアント認証のために提示するようユーザーに要求することがあります。ブラウザーの構成設定に基づいて、ブラウザーは、認証のために提示する証明書の選択についてプロンプトを出すことがあります。システムがトラステッドとして受け入れている CA から、ブラウザーが証明書を提示する場合、DCM は証明書情報を別のウィンドウに表示します。受け入れ可能な証明書が提示されなかった場合、サーバーは、アクセスを許可する前に、証明書の代わりとして、認証のためのユーザー名とパスワードを入力するようにプロンプトを出します。

セキュア・セッションを確立すると、DCM はユーザー・プロファイルと関連付けるために、ブラウザーから適切な証明書を検索しようとします。 DCM が 1 つまたは複数の証明書を正常に検索した場合は、証明書情報が表示され、証明書をユーザー・プロファイルと関連付けることができます。

DCM によって証明書からの情報が表示されない場合は、DCM がユーザー・プロファイルに割り当てるはずだった証明書をユーザーが提示できなかったということです。ユーザー証明書の諸問題の 1 つが原因となっている可能性があります。たとえば、ブラウザーに含まれている証明書が既にユーザー・プロファイルと関連付けられている可能性があります。

ローカル CA を使用して証明書をエンド・ユーザーに発行したい場合は、エンド・ユーザーはユーザー証明書の作成を行う必要があります。

API を使用して証明書を非 iSeries ユーザーへプログラマチックに発行する

V5R2 からは、証明書を非 iSeries ユーザーへプログラマチックに発行するために使用できる、2 つの新しい API が利用可能となりました。これまでのリリースでは、ローカル認証局 (CA) を使用してユーザーに対して証明書を発行するときには、これらの証明書は自動的に iSeries ユーザー・プロファイルに関連付けられるようになっていました。したがって、ローカル CA を使用してクライアント認証用の証明書をユーザーに対して発行するときには、そのユーザーに iSeries ユーザー・プロファイルを提供する必要がありました。また、ユーザーがクライアント認証のための証明書をローカル CA から入手する必要があるときには、各ユーザーはディジタル証明書マネージャー (DCM) を使用して必要な証明書を作成する必要がありました。したがって、各ユーザーは、DCM をホストする iSeries サーバーにユーザー・プロファイルを所有している必要があり、また、その iSeries サーバーに正しくサインオンできる必要がありました。

証明書をユーザー・プロファイルに関連付けておくことには、特に社内ユーザーの場合には、それなりの利点があります。しかし、そのような制限および要件が課されることにより、多数のユーザーのユーザー証明書を発行するために ローカル CA を使用するのは (特に、それらのユーザーに iSeries ユーザー・プロファイルを割り当てたくない場合には)、あまり実用的ではないものとなっていました。これらのユーザーにユーザー・プロファイルを提供しないためには、アプリケーションを使用するためのユーザー認証に証明書を必要とする場合に、ユーザーに、一般的に知られている CA から証明書を有料で購入してもらう必要があります。

新しい 2 つの API が提供するサポートにより、任意のユーザー名で使用できる、ローカル CA 証明書によって署名されたユーザー証明書を作成するための、インターフェースを用意できるようになります。この証明書はユーザー・プロファイルとは関連付けられません。ユーザーは、DCM をホストする iSeries サーバー上に存在している必要がなく、また、証明書を作成するために DCM を使用する必要もありません。

広く使用されているブラウザー・プログラムごとに 1 つずつ、合わせて 2 つの API が提供されており、Net.Data® を使用して、証明書をユーザーに発行するためのプログラムを作成する際に起動することができます。ユーザーが作成するアプリケーションは、ユーザー証明書を作成するため、また、ローカル CA を使用して証明書に署名する目的でいずれかの適切な API を呼び出すために必要な、グラフィカル・ユーザー・インターフェース (GUI) コードを備えていなければなりません。

これらの API の詳しい使用方法については、以下のページを参照してください。
- 『ユーザー証明書要求生成 / 署名 (QYCUGSUC) API』
- 『ユーザー証明書要求署名 (QYCUSUC) API』

専用 CA 証明書のコピーの取得

Secure Sockets Layer (SSL) 接続を使用しているサーバーにアクセスすると、サーバーは、ID の証明として、証明書をクライアント・ソフトウェアに提示します。クライアント・ソフトウェアは、サーバーがセッションを確立する前に、サーバーの証明書を妥当性検査しなければなりません。サーバー証明書を妥当性検査するには、クライアント・ソフトウェアは、サーバー証明書を発行した認証局 (CA) の証明書のローカル保管コピーにアクセスできなければなりません。サーバーが証明書を公

開インターネット CA から提示する場合は、ブラウザー、または他のクライアント・ソフトウェアは既に、その CA 証明書のコピーを持っていなければなりません。しかし、サーバーが証明書を専用ローカル CA から提示する場合は、ディジタル証明書マネージャー (DCM) を使用してそのローカル CA 証明書のコピーを取得する必要があります。

DCM を使用してローカル CA 証明書を直接ブラウザーにダウンロードすることも、あるいはローカル CA 証明書をファイルにコピーして、他のクライアント・ソフトウェアがそのコピーにアクセスして使用できるようにすることもできます。セキュア通信用にブラウザーと他のアプリケーションを両方とも使用する場合は、両方の方法を使用してローカル CA 証明書をインストールする必要があります。両方の方法を使用する場合は、証明書をブラウザーにインストールしてから、その証明書をコピーしてファイルに貼り付けます。

証明書をローカル CA から提示して自分自身を認証するように、サーバー・アプリケーションが要求する場合は、ローカル CA 証明書を自己のブラウザーにダウンロードした後で、ローカル CA からユーザー証明書の要求を行う必要があります。

DCM を使用してローカル CA 証明書のコピーを取得するには、以下のステップを完了します。

1. DCM を開始します。
2. ナビゲーション・フレームの中で、「**ローカル CA 証明書の PC へのインストール (Install Local CA Certificate on Your PC)**」を選択して、ローカル CA 証明書をブラウザーにダウンロードしたり、ローカル CA 証明書をシステム上のファイルに保管したりするためのページを表示します。
3. ローカル CA 証明書を取得する方法を選択します。
   a. 「**証明書のインストール (Install certificate)**」を選択して、ローカル CA 証明書をトラステッド・ルートとして、ブラウザーにダウンロードします。これを行うと、ブラウザーが、この CA からの証明書を使用しているサーバーとセキュア通信セッションを確立できるようになります。ブラウザーは、一連のウィンドウを表示してインストール・プロセスを進行させます。
   b. 「**証明書のコピーと貼り付け (Copy and paste certificate)**」を選択して、ローカル CA 証明書の特別にコード化されたコピーを含むページを表示します。このページに表示されたテキスト・オブジェクトをクリップボードにコピーします。後程、この情報をファイルに貼り付ける必要があります。このファイルは、PC 上のクライアント・プログラムが使用する証明書を格納するために、PC ユーティリティー・プログラム (MKKF または IKEYMAN など) によって使用されます。クライアント・アプリケーションがローカル CA 証明書を認識して認証のために使用するようになるには、アプリケーションがその証明書をトラステッド・ルートとして認識するように構成しなければなりません。ファイルを使用するにあたっては、これらのアプリケーションの指示に従ってください。
4. ディジタル証明書マネージャーのホーム・ページに戻るには、「**OK**」をクリックします。

公開インターネット CA からの証明書の管理

セキュリティー上の必要性とポリシーを慎重に検討した結果、VeriSign などの公開インターネット認証局 (CA) の証明書を使用することに決定しました。たとえば、公開 Web サイトを運営しており、セキュアな通信セッションのために Secure

Sockets Layer (SSL) を使用して、特定の情報トランザクションのプライバシーを保護するとします。この Web サイトは一般に公開されて利用されているので、ほとんどの Web ブラウザーで容易に認識できる証明書の使用が必要になります。

あるいは、外部顧客用のアプリケーションを開発して、公開証明書を使用して、アプリケーション・パッケージにディジタル署名することもできます。アプリケーション・パッケージに署名すると、このパッケージがユーザーの会社のものであり、転送中に許可されていないパーティーによりコードが変更されていないことが顧客に保証されます。公開証明書を使用すれば、顧客が簡単かつ安価にパッケージのディジタル署名を検査できます。また、この証明書を使用して、署名を検査してから顧客にパッケージを送信することもできます。

ディジタル証明書マネージャー (DCM) のガイド・タスクを使用して、これらの公開証明書、およびその証明書を使用して SSL 接続の確立、オブジェクトへの署名、あるいはオブジェクトのディジタル証明書の認証性の検査を行うアプリケーションを集中的に管理することができます。

公開証明書の管理

DCM を使用して公開インターネット CA の証明書を管理する場合は、まず証明書ストアを作成しなければなりません。証明書ストアは、DCM がディジタル証明書およびそれに関連した秘密鍵を保管するために使用する、特殊キー・データベース・ファイルです。DCM を使用して、含まれる証明書のタイプに基づいて、いくつかのタイプの証明書ストアを作成および管理することができます。

作成する証明書ストアのタイプ、ならびに証明書およびその証明書を使用するアプリケーションを管理するために実行しなければならないその後のタスクは、証明書の使用計画の立て方によって決まります。DCM を使用して、適切な証明書ストアを作成し、アプリケーション用の公開インターネット証明書を管理する方法については、以下のトピックを参照してください。

- SSL 通信セッションのための公開インターネット証明書の管理
- オブジェクトに署名するための公開インターネット証明書の管理
- オブジェクトの署名検査のための証明書の管理

DCM を使用すると、Public Key Infrastructure for X.509 (PKIX) 認証局から取得した証明書を管理することができます。

SSL 通信セッションのための公開インターネット証明書の管理

ディジタル証明書マネージャー (DCM) を使用して、Secure Sockets Layer (SSL) を使ったセキュアな通信セッションを確立するために、アプリケーションで使用する公開インターネット証明書を管理することができます。DCM を使用して独自のローカル認証局 (CA) を運用している場合以外は、まず、SSL で使用する公開証明書を管理するための適切な証明書ストアを作成しなければなりません。これが *SYSTEM 証明書ストアです。証明書ストアを作成すると、DCM により、証明書を取得するために公開 CA に提供しなければならない証明書要求情報を作成するプロセスを実行できます。

DCM を使用して、アプリケーションで SSL セッションを確立できるように公開インターネット証明書を管理および使用するには、以下のステップに従ってください。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、「**新規証明書ストアの作成 (Create New Certificate Store)**」を選択して、ガイド・タスクを開始し、一連のフォームを完了します。これらのフォームは、証明書ストアおよびアプリケーションで SSL セッション確立のために使用できる証明書の作成プロセスをガイドするものです。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
3. 作成する証明書ストアとして ***SYSTEM** を選択して、「**続行 (Continue)**」をクリックします。
4. 「**はい (Yes)**」を選択して、*SYSTEM 証明書ストア作成の一環として証明書を作成し、「**続行 (Continue)**」をクリックします。
5. 新規証明書の署名者として「**VeriSign または他のインターネット認証局 (CA) (VeriSign or other Internet Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックすると、新規証明書の識別情報を指定できるフォームが表示されます。

   注: ユーザーの iSeries に IBM 4758-023 PCI 暗号化コプロセッサーがインストールされている場合、DCM により、次のタスクとして証明書の秘密鍵の保管方法を選択することができます。システムにコプロセッサーがない場合、DCM は、*SYSTEM 証明書ストアにその秘密鍵を自動的に保管します。秘密鍵の保管方法の選択についてヘルプが必要な場合は、DCM のオンライン・ヘルプを参照してください。
6. フォームに入力して、「**続行 (Continue)**」をクリックすると、確認用ページが表示されます。この確認用ページには、証明書を発行する公開認証局 (CA) に提供する必要がある証明書要求データが表示されます。証明書署名要求 (CSR) データは、新規証明書に指定した公開鍵およびその他の情報から構成されています。
7. 証明書を要求する際に公開 CA が必要とする CSR データを、証明書申請フォームまたは別個のファイルに、注意深くコピー・アンド・ペーストします。「開始 (Begin)」行と「新規証明書要求の終わり (End New Certificate Request)」行の両方を含む、すべての CSR データを使用しなければなりません。このページを終了すると、データは失われ、そのデータを回復することはできません。選択した CA に申請フォームまたはファイルを送信して、証明書を発行したり、証明書に署名したりします。

   注: この手順を終了するのは、CA から、署名されて完成した証明書が戻されるまで待たなければなりません。

   注: HTTP Server for iSeries で証明書を使用する場合は、DCM を実行して、署名されて完了した証明書を処理する前に、Web サーバーを作成して構成しておく必要があります。 Web サーバーを構成して SSL を使用すると、そのサーバーにアプリケーション ID が生成されます。このアプリケーション ID はメモに控えておき、DCM を使用してこのアプリケーションが SSL に使用する証明書を指定できるようにします。

DCM を使用して、署名して完了した証明書をサーバーに割り当てるまでは、サーバーを終了して再始動しないでください。証明書を割り当てる前に、Web サーバーの *ADMIN インスタンスを終了して再始動すると、サーバーは始動せず、DCM を使用してサーバーに証明書を割り当てることはできません。

8. 公開 CA が署名済み証明書を戻してから、DCM を開始します。
9. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
10. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
11. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
12. タスク・リストから「**証明書のインポート (Import certificates)**」を選択して、署名済みの証明書を *SYSTEM 証明書ストアにインポートするプロセスを開始します。証明書のインポートが終了したら、SSL 通信に証明書を使用するアプリケーションを指定することができます。
13. ナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
14. タスク・リストから、「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、証明書を割り当てることができる、SSL 対応アプリケーションのリストを表示します。
15. このリストからアプリケーションを選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。
16. インポートした証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。DCM は、そのアプリケーションに対する証明書の選択について確認するためのメッセージを表示します。

    注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。これをサポートしているアプリケーションで証明書を認証できるようにしてから、資源にアクセスするようにしたい場合は、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

ガイド・タスクを完了すると、SSL を使用してセキュア通信を行うようにアプリケーションを構成するために必要な条件がすべてそろいます。ユーザーが、SSL セッション経由でこれらのアプリケーションにアクセスできるようにするには、サーバー証明書を発行した CA の CA 証明書のコピーが必要です。証明書が一般的に知られているインターネット CA のものである場合は、ユーザーのクライアント・ソフトウェアに、必要な CA 証明書のコピーが既に存在している場合があります。ユー

ザーは、CA 証明書を取得する必要がある場合は、CA の Web サイトにアクセスして、そのサイトの指示に従う必要があります。

オブジェクトに署名するための公開インターネット証明書の管理

ディジタル証明書マネージャー (DCM) を使用して、オブジェクトにディジタル署名を行うための公開インターネット証明書を管理することができます。 DCM を使用して独自のローカル認証局 (CA) を運用している場合以外は、まず、オブジェクトに署名するために使用する公開証明書を管理するための適切な証明書ストアを作成しなければなりません。これが *OBJECTSIGNING 証明書ストアです。証明書ストアを作成すると、DCM により、証明書を取得するために公開インターネット CA に提供しなければならない証明書要求情報を作成するプロセスが開始されます。

証明書を使用してオブジェクトに署名するには、アプリケーション ID も定義しなければなりません。このアプリケーション ID は、特定の証明書を使用してオブジェクトに署名するために必要な権限のレベルを制御し、DCM が提供するレベルより上の別のアクセス制御を提供します。アプリケーションで証明書を使用してオブジェクトに署名するには、デフォルトのアプリケーション定義に、ユーザーに *ALLOBJ 特殊権限があることが条件として定義されている必要があります。 (ただし、iSeries ナビゲーターを使用して、アプリケーション ID が必要とする権限を変更することができます。)

DCM を使用して、オブジェクトに署名するように公開インターネット証明書を管理および使用するには、以下のタスクを完了してください。

1. DCM を開始します。
2. DCM の左端のナビゲーション・フレームで、「**新規証明書ストアの作成 (Create New Certificate Store)**」を選択して、ガイド・タスクを開始し、一連のフォームを完了します。これらのフォームは、証明書ストアおよびオブジェクトに署名するために使用できる証明書の作成プロセスをガイドするものです。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) ボタンを選択してください。オンライン・ヘルプが表示されます。
3. 作成する証明書ストアとして ***OBJECTSIGNING** を選択して、「**続行 (Continue)**」をクリックします。
4. 「**はい (Yes)**」を選択して、この証明書ストア作成の一環として証明書を作成し、「**続行 (Continue)**」をクリックします。
5. 新規証明書の署名者として「**VeriSign または他のインターネット認証局 (CA) (VeriSign or other Internet Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックします。これにより、新規証明書の識別情報を指定できるフォームが表示されます。
6. フォームに入力して、「**続行 (Continue)**」をクリックすると、確認用ページが表示されます。この確認用ページには、証明書を発行する公開認証局 (CA) に提供する必要がある証明書要求データが表示されます。証明書署名要求 (CSR) データは、新規証明書に指定した公開鍵およびその他の情報から構成されています。
7. 証明書を要求する際に公開 CA が必要とする CSR データを、証明書申請フォームまたは別個のファイルに、注意深くコピー・アンド・ペーストします。

「開始 (Begin)」行と「新規証明書要求の終わり (End New Certificate Request)」行の両方を含む、すべての CSR データを使用しなければなりません。このページを終了すると、データは失われ、そのデータを回復することはできません。選択した CA に申請フォームまたはファイルを送信して、証明書を発行したり、証明書に署名したりします。

注: この手順を終了するのは、CA から、署名されて完成した証明書が戻されるまで待たなければなりません。

8. 公開 CA が署名済み証明書を戻してから、DCM を開始します。
9. 左端のナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
10. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
11. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
12. タスク・リストから「**証明書のインポート (Import certificates)**」を選択して、署名済みの証明書を *OBJECTSIGNING 証明書ストアにインポートするプロセスを開始します。証明書のインポートが終了したら、証明書を使用してオブジェクトに署名するようにアプリケーション定義を作成することができます。
13. 左端のナビゲーション・フレームが最新表示されたら、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
14. タスク・リストから「**アプリケーションの追加 (Add Application)**」を選択して、証明書を使用してオブジェクトに署名するための、オブジェクト署名アプリケーション定義を作成するプロセスを開始します。
15. オブジェクト署名アプリケーションを定義するフォームを完成させて、「**追加 (Add)**」をクリックします。このアプリケーション定義は、実際のアプリケーションを示しているのではなく、特定の証明書を使って署名することになっているオブジェクトのタイプを示しています。このフォームの入力方法については、オンライン・ヘルプを参照してください。
16. 「**OK**」をクリックして、アプリケーション定義確認メッセージを確認し、「アプリケーションの管理 (Manage Applications)」のタスク・リストを表示します。
17. タスク・リストから「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、「**続行 (Continue)**」をクリックし、証明書を割り当てることができるオブジェクト署名アプリケーション ID のリストを表示します。
18. このリストからアプリケーション ID を選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。
19. インポートした証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。

これらのタスクを完了すると、 オブジェクトへの署名を開始して、その保全性を保証するために必要な、すべての条件が整います。

署名済みオブジェクトを配布した際、このオブジェクトの受信側は、V5R1 またはそれ以降のバージョンの DCM を使用して、オブジェクトの署名の妥当性検査を行い、データが未変更であることを確認し、送信側の識別検査を行わなければなりません。署名の妥当性検査を行うには、受信側に署名検査証明書のコピーがなければなりません。署名済みオブジェクトのパッケージの一部として、この証明書のコピーを提示する必要があります。

受信側には、オブジェクトに署名するために使用した証明書を発行した CA の CA 証明書のコピーも必要です。一般的に知られているインターネット CA の証明書を使用してオブジェクトに署名した場合は、受信側のバージョンの DCM に、必要な CA 証明書のコピーが既に存在している必要があります。したがって、受信側にまだコピーが存在しないと思われる場合は、署名済みオブジェクトと一緒に CA 証明書のコピーを提供する必要があります。たとえば、専用ローカル CA の証明書を使用してオブジェクトに署名した場合は、ローカル CA 証明書のコピーを提供する必要があります。セキュリティー上の理由から、別のパッケージで CA 証明書を提供するか、証明書を必要とするユーザーからの要求があった時点で、公的に CA 証明書を入手できるようにする必要があります。

オブジェクトの署名検査のための証明書の管理

ディジタル証明書マネージャー (DCM) を使用して、オブジェクトのディジタル署名の妥当性検査を行うために使用する署名検査証明書を管理することができます。オブジェクトに署名するには、証明書の秘密鍵を使用して署名を作成します。署名済みオブジェクトを他に送信する場合は、オブジェクトに署名した証明書のコピーを含める必要があります。これを実行するには、DCM を使用して、オブジェクト署名証明書を (証明書の秘密鍵を指定しないで) 署名検査証明書としてエクスポートします。署名検査証明書は、他に配布することができるファイルにエクスポートできます。あるいは、作成した署名を検査したい場合は、署名検査証明書を *SIGNATUREVERIFICATION 証明書ストアにエクスポートできます。

オブジェクトの署名の妥当性検査を行うには、オブジェクトに署名した証明書のコピーを持っていなければなりません。署名証明書に含まれる公開鍵を使用して、対応する秘密鍵で作成された署名を検査することができます。したがって、オブジェクトの署名を検査できるようにするには、署名済みオブジェクトの提供先から署名証明書のコピーを取得しなければなりません。

オブジェクトに署名した証明書を発行した認証局 (CA) の CA 証明書のコピーも持っていなければなりません。CA 証明書を使用して、オブジェクトに署名した証明書の認証性を検査します。DCM は、一般的に知られている CA からの CA 証明書のコピーを提供しています。ただし、オブジェクトが別の公開 CA または専用ローカル CA の証明書で署名されている場合、オブジェクトの署名を検査できるようにするには、CA 証明書のコピーを取得しなければなりません。

DCM を使用してオブジェクトの署名を検査するには、まず、必要な署名検査証明書を管理するための適切な証明書ストアを作成しなければなりません。これが *SIGNATUREVERIFICATION 証明書ストアです。この証明書ストアを作成する際に、DCM は、証明書ストアを一般的に知られている公開 CA 証明書のコピーと一緒に配置します。

注: 独自のオブジェクト署名証明書で作成した署名を検査できるようにしたい場合は、*SIGNATUREVERIFICATION 証明書ストアを作成して、そこに

*OBJECTSIGNING 証明書ストアの証明書をコピーしなければなりません。*OBJECTSIGNING 証明書ストア内から署名検査を実行する予定がある場合でも、これは当てはまります。

DCM を使用して、署名検査証明書を管理するには、以下のタスクを実行します。

1. DCM を開始します。
2. DCM の左端のナビゲーション・フレームで、「**新規証明書ストアの作成 (Create New Certificate Store)**」を選択して、ガイド・タスクを開始し、一連のフォームを完了します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) ボタンを選択してください。オンライン・ヘルプが表示されます。
3. 作成する証明書ストアとして ***SIGNATUREVERIFICATION** を選択して、「**続行 (Continue)**」をクリックします。

   注: *OBJECTSIGNING 証明書ストアが存在する場合は、この時点で、DCM から、オブジェクト署名証明書を署名検査証明書として新規証明書ストアにコピーするかどうかを指定するようにプロンプトが出されます。既存のオブジェクト署名証明書を使用して署名を検査したい場合は、「**はい (Yes)**」を選択して、「**続行 (Continue)**」をクリックします。*OBJECTSIGNING 証明書ストアの証明書をコピーするには、そのパスワードを知っていなければなりません。
4. 新規証明書ストアにパスワードを指定して、「**続行 (Continue)**」をクリックして証明書ストアを作成します。確認用ページが表示され、証明書ストアが正常に作成されたことを示すメッセージが表示されます。これで、このストアを使用して、オブジェクトの署名を検査するための証明書を管理し、使用することができます。

   注: このストアを、署名したオブジェクトの署名を検査できるように作成している場合は、ここで作業を停止することができます。新規オブジェクト署名証明書を作成する際に、これらの証明書を *OBJECTSIGNING 証明書ストアからこの証明書ストアにエクスポートする必要があります。これらの証明書をエクスポートしない場合は、これらの証明書で作成した署名を検査できなくなります。

   注: この証明書ストアを他のソースから受信したオブジェクトの署名を検査できるように作成している場合は、この手順を続行して、証明書ストアに必要な証明書をインポートできるようにする必要があります。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。

8. タスク・リストから、「**証明書のインポート (Import certificates)**」を選択します。このガイド・タスクにより、受信したオブジェクトの署名を検査できるように、証明書ストアに必要な証明書をインポートするプロセスを実行することができます。
9. インポートする証明書のタイプを選択します。「**署名の検査 (Signature verification)**」を選択して、署名済みオブジェクトと一緒に受信した証明書をインポートし、インポート・タスクを完了します。

   注: 証明書ストアに、署名検査証明書を発行した CA の CA 証明書のコピーがない場合は、まず CA 証明書をインポートしなければなりません。CA 証明書をインポートする前に署名検査証明書をインポートしていない場合、署名検査証明書をインポートする際にエラーを受信する可能性があります。

これで、これらの証明書を使用して、オブジェクトの署名を検査することができます。

第 8 章 DCM の管理

ディジタル証明書マネージャー (DCM) を構成した後で、いくつかの証明書管理タスクを実施する必要があります。 DCM を使用してディジタル証明書を管理する方法については、以下のトピックを参照してください。

ローカル CA を使用して他の iSeries システムの証明書を発行
あるシステムの専用ローカル CA を使用して、他の iSeries システムで使用する証明書を発行する方法について説明します。

DCM によるアプリケーションの管理
DCM を使用して SSL 対応アプリケーションまたはオブジェクト署名アプリケーションに関するアプリケーション定義を行う方法について説明します。このトピックでは、アプリケーション定義の作成およびアプリケーションに対する証明書割り当ての管理方法について説明します。クライアント認証のための証明書の受け入れに関してアプリケーションが使用する、CA 信頼リストの定義について学習することができます。

証明書およびアプリケーションの妥当性検査
アプリケーションが特定の証明書を使用したり受け入れたりする前に、その証明書の認証性を検査するための方法について説明します。

証明書の割り当て
セキュア機能で使用する証明書を 1 つまたは複数のアプリケーションに迅速に割り当てる方法について説明します。

CRL 位置の管理
アプリケーションが、受け入れる証明書の有効性を検査するために使用できる、証明書取り消しリスト (CRL) の位置を定義および使用する方法について説明します。

IBM 4758 暗号化コプロセッサー上での証明書キーの保管
インストールされたコプロセッサーを使用して、証明書の秘密鍵をより安全に保管する方法について説明します。

PKIX CA の要求場所の管理
Public Key Infrastructure for X.509 (PKIX) 規格に基づいて証明書を発行する公開インターネット CA から取得した証明書を、DCM を使用して管理する方法について説明します。

オブジェクトへの署名
オブジェクトの整合性を確保するために、オブジェクトへのディジタル署名に使用する証明書を、DCM を使用して管理する方法について説明します。

オブジェクトの署名検査
DCM を使用してオブジェクトのディジタル署名の認証性を検査する方法について説明します

ローカル CA を使用して他の iSeries システムの証明書を発行

ネットワーク内の iSeries システムで、すでに専用ローカル認証局 (CA) を使用している場合があります。このローカル CA の使用範囲をネットワーク内の別の iSeries まで広げたいとします。たとえば、現行ローカル CA を別の iSeries システムのアプリケーションに対して SSL 通信セッションを使用するために、サーバーまたはクライアント証明書を発行するようにしたい場合があります。あるいは、あるシステ

ムのローカル CA の証明書を使用して、別の iSeries サーバーに保管されているオブジェクトに署名したい場合があります。

この要件は、ディジタル証明書マネージャー (DCM) を使用することで達成できます。ローカル CA を運用している iSeries でいくつかのタスクを実行し、証明書の発行先となるアプリケーションをホスト処理する 2 次 iSeries でその他のタスクを実行します。この 2 次システムは、ターゲット・システムと呼ばれます。ターゲット・システムで実行すべきタスクは、システムのリリース・レベルによって決まります。

注: 問題が発生する可能性があるのは、ローカル CA を運用している iSeries が、ターゲット・システムよりも強度の暗号化機能を提供するプロバイダー製品で暗号を使用する場合です。 (V5R2 で使用できる暗号アクセス・プロバイダーは 5722-AC3 のみです。これは、現在使用可能な、最も強力な製品です。ただし、以前のリリースでは、これよりも機能が弱く、提供される暗号機能のレベルが低い、他の暗号アクセス・プロバイダー製品 (5722-AC1 または 5722-AC2) がインストールされている可能性があります。) (秘密鍵を持つ) 証明書をエクスポートする場合、システムは、ファイルを暗号化してその内容を保護します。システムでターゲット・システムよりも強度の暗号化製品を使用すると、ターゲット・システムはインポート・プロセスでファイルを復号できません。その結果、インポートが失敗したり、SSL セッションの確立に証明書が使用できなかったりする場合があります。このことは、新規証明書において、ターゲット・システムの暗号製品での使用に適したキー・サイズを使用している場合にも当てはまります。

ローカル CA を使用して証明書を他のシステム発行することができます。そうすると、この証明書でオブジェクトに署名をしたり、アプリケーションで SSL セッションを確立する際にこの証明書を使用したりできます。ローカル CA を使用して、別の iSeries システムで使用する証明書を作成する場合、DCM が作成するファイルには、ローカル CA 証明書のコピーだけでなく、数多くの公開インターネット CA のための証明書のコピーも含まれています。

DCM で実行しなければならないタスクは、ローカル CA が発行する証明書のタイプとターゲット・システムにおけるリリース・レベルおよび条件によって少し異なります。

別の V5R2 または V5R1 iSeries システムで使用する専用証明書の発行

ローカル CA を使用して、別の V5R2 または V5R1 iSeries システムで使用する証明書を発行するには、ローカル CA をホスト処理するシステムで、以下のステップを実行します。

1. DCM を開始します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
2. ナビゲーション・フレームで、「**証明書の作成 (Create Certificate)**」を選択して、ローカル CA を使用して作成できる証明書タイプのリストを表示します。

このタスクを完了するために、証明書ストアをオープンする必要はありません。これらの手順は、特定の証明書ストア内で作業していないこと、あるいは、ローカル認証局 (CA) 証明書ストア内で作業していることを前提としています。これらのタスクを実行できるようにするには、ローカル CA がこのシステムに存在していなければなりません。

3. ローカル CA で発行したい証明書のタイプを選択して、「**続行 (Continue)**」をクリックし、ガイド・タスクを開始して、一連のフォームを完了します。「**別の iSeries のためのサーバーまたはクライアント証明書 (server or client certificate for another iSeries)**」(SSL セッションの場合)、または「**別の iSeries のためのオブジェクト署名証明書 (object signing certificate for another iSeries)**」(別のシステムで使用する場合) のどちらを作成するか選択します。

   注: 別のシステムで使用するオブジェクト署名証明書を作成する場合、そのシステムは、証明書を使用するために V5R1 以降のバージョンの OS/400 を稼働していなければなりません。ターゲット・システムが V5R1 以降でなければならないため、ホスト・システムの DCM から、新規オブジェクト署名証明書のターゲット・リリース形式を選択するようにプロンプトが出されることはありません。

4. サーバーまたはクライアント証明書を作成する場合は、この証明書を作成する対象の iSeries のリリース・レベルを選択します。「**続行 (Continue)**」をクリックすると、新規証明書の識別情報を指定できるフォームが表示されます。

   注: 選択するリリース・レベルによって、新規証明書を作成するために DCM が使用する形式が決まります。フォーム上の識別情報の量およびタイプは、選択したリリース・レベルによって異なります。これにより、証明書ファイルと、その証明書を使用する iSeries システムとの互換性を確保できるようになります。

5. フォームに入力して、「**続行 (Continue)**」をクリックすると、確認用ページが表示されます。

   注: ターゲット・システムに既存の *OBJECTSIGNING または *SYSTEM 証明書ストアが存在する場合は、証明書に固有の証明書レベルおよび固有のファイル名を必ず指定してください。固有の証明書レベルおよびファイル名を指定すると、ターゲット・システムの既存の証明書ストアに証明書を簡単にインポートすることができます。

   この確認ページには、DCM がターゲット・システムへの転送用に作成したファイルの名前が表示されます。DCM は、指定したターゲット・システムのリリース・レベルに基づいてこれらのファイルを作成します。DCM は、ローカル CA 証明書のコピーをこれらのファイルへ自動的に書き込みます。

   注: DCM は、独自の証明書ストアに新規証明書を作成して、転送する 2 つのファイル、証明書ストア・ファイル (拡張子 .KDB) および要求ファイル (.RDB 拡張子) を生成しています。

6. バイナリーのファイル転送プロトコル (FTP) または別の方法を使用して、ファイルをターゲット・システムに転送します。

別の V4R4 または V4R5 iSeries システムで使用する専用証明書の発行

ローカル CA を使用して、V4R4 または V4R5 iSeries システムで使用する証明書を発行するには、V5R2 ローカル CA をホストするシステムで、以下のステップを実行してください。

1. DCM を開始します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。

2. ナビゲーション・フレームで、「**証明書の作成 (Create Certificate)**」を選択して、ローカル CA を使用して作成できる証明書タイプのリストを表示します。

   このタスクを完了するために、証明書ストアをオープンする必要はありません。これらの手順は、特定の証明書ストア内で作業していないこと、あるいは、ローカル認証局 (CA) 証明書ストア内で作業していることを前提としています。これらのタスクを実行できるようにするには、ローカル CA がこのシステムに存在していなければなりません。

3. ローカル CA で発行したい証明書のタイプを選択して、「**続行 (Continue)**」をクリックし、ガイド・タスクを開始して、一連のフォームを完了します。

   注: V4R4 または V4R5 iSeries システムで使用する目的でこの証明書を作成しているため、「**別の iSeries のためのサーバーまたはクライアント証明書 (server or client certificate for another iSeries)**」を選択していなければなりません。V5R1 よりも以前のリリース・レベルのターゲット・システムでは、オブジェクト署名証明書は使用できません。

4. この証明書を作成する対象の iSeries のリリース・レベルを選択します。「**続行 (Continue)**」をクリックすると、新規証明書の識別情報を指定できるフォームが表示されます。

   注: 選択するリリース・レベルによって、新規証明書を作成するために DCM が使用する形式が決まります。フォーム上の識別情報の量およびタイプは、選択したリリース・レベルによって異なります。これにより、証明書ファイルと、その証明書を使用する iSeries システムとの互換性を確保できるようになります。

5. フォームに入力して、「**続行 (Continue)**」をクリックすると、確認用ページが表示されます。

   注: ターゲット・システムに既存の *SYSTEM 証明書ストアが存在する場合は、証明書に固有の証明書レベルおよび固有のファイル名を必ず指定してください。固有の証明書レベルおよびファイル名を指定すると、ターゲット・システムの既存の証明書ストアに証明書を簡単にインポートすることができます。

   この確認ページには、DCM がターゲット・システムへの転送用に作成したファイルの名前が表示されます。DCM は、指定したターゲット・システムのリリース・レベルに基づいてこれらのファイルを作成します。DCM は、ローカル CA 証明書のコピーをこれらのファイルへ自動的に書き込みます。

   注: DCM は、独自の証明書ストアに新規証明書を作成して、転送する 2 つのファイル、証明書ストア・ファイル (拡張子 .KDB) および要求ファイル (拡張子 .RDB) を生成しています。

注: V4R4 または V4R5 ターゲット・システムの既存の *SYSTEM 証明書ストアにあるこれらのファイルの証明書を使用する予定である場合、ローカル CA 証明書を .KDB および .RDB ファイルから直接インポートすることはできません。これは、CA 証明書が、DCM インポート機能で認識および使用できる形式ではないためです。代わりに、ホスト・システムを使用してローカル CA 証明書のコピーを別ファイルにエクスポートし、CA 証明書が以前のリリースのインポート機能を処理する形式になっているようにしなければなりません。

6. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
7. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、ホスト・システムで証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
8. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
9. タスク・リストから、「**証明書のエクスポート (Export certificate)**」を選択します。
10. エクスポートする証明書のタイプとして「**認証局 (CA) (Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックすると、 CA 証明書のリストが表示されます。
11. 証明書のリストからローカル CA 証明書 (たとえば、LOCAL_CERTIFICATE_AUTHORITY) を選択します。「**エクスポート (Export)**」をクリックすると、 CA 証明書の宛先を選択できるフォームが表示されます。
12. 「**ファイル (File)**」を選択して、「**続行 (Continue)**」をクリックします。
13. エクスポート・ファイルの完全修飾パスおよびファイル名を指定して、「**続行 (Continue)**」をクリックします。確認用ページが表示され、DCM によりファイルが正常にエクスポートされたことが示されます。

    注: ファイルには、固有の名前と拡張子を必ず指定してください。たとえば、ファイルに mycafile.exp という名前を付けることができます。ファイルに名前を付けるときに、ファイル拡張子、.TXT、.KDB、.RDB または .KYR はいずれも使用しないでください。これらのいずれかの拡張子タイプを使用すると、ファイルをターゲット・システムへインポートする際に問題が生じる可能性があります。
14. バイナリーのファイル転送プロトコル (FTP) または別の方法を使用して、作成した証明書ストア・ファイル (.KDB および .RDB) を V4R4 または V4R5 ターゲット・システムに転送します。エクスポートされたローカル CA 証明書を含むファイルを転送する場合には、ASCII FTP モードを使用してください。

転送されたファイルをターゲット・システムで使用する

ファイルを転送した後、ターゲット・システムで DCM を使用して、転送証明書ファイルを処理します。実行しなければならない DCM タスクは、ターゲット・システムのリリース・レベルおよびターゲット・システムに存在する証明書ストアの種類によって異なります。ホスト・システムに作成した証明書のタイプも、ターゲット・システムで実行しなければならないタスクに影響を与えます。ターゲット・システムで DCM を使用して、転送証明書ファイルを処理する方法については、以下のトピックを参照してください。

- V5R2 ターゲット・システムでの SSL セッションのための専用証明書の使用。
- V5R1 ターゲット・システムでの SSL セッションのための専用証明書の使用。
- V5R2 または V5R1 ターゲット・システムでのオブジェクト署名のための専用証明書の使用。
- V4R5 または V4R4 ターゲット・システムでの SSL セッションのための専用証明書の使用。

V5R2 ターゲット・システムでの SSL セッションのための専用証明書の使用

アプリケーションが SSL セッションのために使用する証明書は、ディジタル証明書マネージャー (DCM) の *SYSTEM 証明書ストアから管理します。V5R2 ターゲット・システムで DCM を使用して SSL のための証明書をこれまでに管理したことがない場合、この証明書ストアはターゲット・システムには存在していません。ローカル認証局 (CA) ホスト・システムで作成した転送証明書ストア・ファイルを使用するために必要なタスクは、*SYSTEM 証明書ストアが存在しているかどうかによって異なります。 *SYSTEM 証明書ストアが存在しない場合は、転送された証明書ファイルを使用して *SYSTEM 証明書ストアを作成することができます。
*SYSTEM 証明書が V5R2 ターゲット・システムに存在する場合には、転送された証明書ファイルを次の 2 つのうちのいずれかの方法で使用することができます。
- 転送されたファイルを「他のシステム証明書ストア (Other System Certificate Store)」として使用する。
- 転送されたファイルを既存の *SYSTEM 証明書ストアにインポートする。

*SYSTEM 証明書ストアが存在しない場合

*SYSTEM 証明書ストアが、転送証明書ストア・ファイルを使用しようとする V5R2 システムに存在しない場合は、転送証明書ストア・ファイルを *SYSTEM 証明書ストアとして使用することができます。 *SYSTEM 証明書ストアを作成し、証明書ファイルを V5R2 ターゲット・システムで使用するには、以下のステップに従ってください。

1. ローカル CA をホスト処理するシステムで作成した証明書ストア・ファイル (拡張子 .KDB を持つファイルと拡張子 .RDB を持つファイルの 2 ファイル) が、/QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにあることを確認してください。
2. 転送された証明書ファイルが /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに配置された後で、これらのファイルの名前を DEFAULT.KDB および DEFAULT.RDB に変更します。当該ディレクトリー内でこれらのファイル名を変更することによって、ターゲット・システムの *SYSTEM 証明書ストアを構成する構成要素が作成されます。証明書ストア・ファイルには、既に数多くの公開インターネット CA の証明書のコピーが含まれています。DCM は、これらのコピーおよびローカル CA 証明書のコピーを、作成時に証明書ストア・ファイルに追加しています。

   重要: ターゲット・システムの /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにすでに DEFAULT.KDB および DEFAULT.RDB ファイルが存在する場合、*SYSTEM 証明書ストアはこのターゲット・システムにすでに存在しています。したがって、転送ファイルの名前を指示どおり変更する必要はありません。デフォルト・ファイルを上書きすると、DCM、転送証

明書ストア、およびその内容を使用する際に問題が生じます。これを行う代わりに、転送ファイルに固有の名前を付け、転送証明書ストアを「**他のシステム証明書ストア (Other System Certificate Store)**」として使用する必要があります。ファイルを「他のシステム証明書ストア (Other System Certificate Store)」として使用すると、DCM を使用して、証明書を使用する必要があるアプリケーションを指定することはできません。

3. DCM を開始します。ここで、転送されたファイルを名前変更して作成した *SYSTEM 証明書ストアのパスワードを変更しなければなりません。パスワードを変更することにより、DCM によって新規パスワードが保管されるため、この証明書ストアですべての DCM 証明書管理機能を使用することができます。
4. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
5. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されてから、V5R2 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
6. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、SSL セッションに証明書を使用するアプリケーションを指定できます。
7. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
8. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、新規パスワードを指定して、「**続行 (Continue)**」をクリックします。
9. ナビゲーション・フレームが最新表示されたら、ナビゲーション・フレームの「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
10. タスク・リストから「**証明書の割り当て (Assign certificate)**」を選択し、現行の証明書ストア内にある証明書のリストを表示します。
11. ホスト・システムで作成した証明書を選択し、「**アプリケーションへの割り当て (Assign to Applications)**」をクリックして、証明書の割り当て対象とすることができる SSL 対応アプリケーションのリストを表示します。
12. SSL セッションのためにその証明書を使用する必要があるアプリケーションを選択し、「**続行 (Continue)**」をクリックします。DCM は、そのアプリケーションに対する証明書選択についての確認メッセージを表示します。

注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。これをサポートしているアプリケーションでは、資源にアクセスする前に証明書を認証できるようにしなければなりません。したがって、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになり

ます。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

これらのタスクが完了した後、ターゲット・システムのアプリケーションは、別の iSeries のローカル CA により発行された証明書を使用することができます。ただし、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを取得しなければなりません。ローカル CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

*SYSTEM 証明書ストアが存在する場合 -「他のシステム証明書ストア (Other System Certificate Store)」としてファイルを使用

V5R2 ターゲット・システムに既に *SYSTEM 証明書ストアがある場合は、証明書ファイルの処理方法を決定しなければなりません。転送証明書ファイルを「**他のシステム証明書ストア (Other System Certificate Store)**」として使用することが選択できます。あるいは、専用証明書およびそれに対応するローカル CA 証明書を既存の *SYSTEM 証明書ストアにインポートすることが選択できます。

「他のシステム証明書ストア (Other System Certificate Store)」は、SSL 証明書を保管する、ユーザー定義の 2 次的な証明書ストアです。これらを作成して使用すると、DCM フィーチャーにアプリケーション ID を登録する際に DCM API を使用しない、ユーザー作成の SSL 対応アプリケーションに証明書を提供できます。「他のシステム証明書ストア (Other System Certificate Store)」オプションを選択すると、証明書に SSL_Init API を使用してプログラマチックにアクセスを行い、その証明書を使用して SSL セッションを確立する、ユーザー作成のアプリケーションの証明書を管理することができます。この API を使用すると、アプリケーションは、ユーザーが特に指定した証明書ではなく、証明書ストアのデフォルト証明書を使用することができます。

IBM iSeries アプリケーション (および他の数多くのソフトウェア開発者によるアプリケーション) は、*SYSTEM 証明書ストアの証明書のみを使用するように作成されています。転送ファイルを「他のシステム証明書ストア (Other System Certificate Store)」として使用するようにすると、DCM を使用して、SSL セッションの証明書を使用する必要があるアプリケーションを指定することはできません。したがって、この証明書を使用するように、標準 iSeries SSL 対応アプリケーションを構成することはできません。iSeries アプリケーションで証明書を使用したい場合は、転送証明書ストア・ファイルの証明書を *SYSTEM 証明書ストアにインポートしなければなりません。

転送証明書ファイルを「他のシステム証明書ストア (Other System Certificate Store)」として利用して処理するには、以下のステップに従ってください。

1. DCM を開始します。

2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、ホスト・システムから転送した証明書ストア・ファイル (拡張子 .KDB を持つファイル) の完全修飾パスおよびファイル名を指定します。また、V5R2 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、このストアの証明書をデフォルト証明書として使用するように指定できます。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指定し、新規パスワードを入力して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されたら、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**デフォルト証明書の設定 (Set default certificate)**」を選択します。

「他のシステム証明書ストア (Other System Certificate store)」が作成され、構成されたため、SSL_Init API を使用するすべてのアプリケーションは、その証明書ストア内の証明書を使用して SSL セッションを確立することができます。

*SYSTEM 証明書ストアが存在する場合 - 既存の *SYSTEM 証明書ストアの証明書を使用

V5R2 システムの既存の *SYSTEM 証明書ストアの転送証明書ストア・ファイルの証明書を使用することができます。これを行うには、証明書ストアの証明書を既存の *SYSTEM 証明書ストアにインポートしなければなりません。ただし、.KDB および .RDB ファイルから証明書を直接インポートすることはできません。これは、これらの証明書が、DCM インポート機能で認識および使用できる形式ではないためです。転送された証明書を既存の *SYSTEM 証明書ストアで使用するには、それらのファイルを「他のシステム証明書ストア (Other System Certificate store)」として開き、*SYSTEM 証明書ストアにエクスポートする必要があります。

証明書ストア・ファイルから *SYSTEM 証明書ストアにファイルをエクスポートするには、V5R2 ターゲット・システムで以下のステップを行ってください。
1. DCM を開始します。

2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を指定します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、ホスト・システムから転送した証明書ストア・ファイル (.KDB 拡張子を持つファイル) の完全修飾パスおよびファイル名を指定します。また、V5R2 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。パスワードを変更しないで「自動ログイン (Automatic login)」オプションを選択すると、このストアから *SYSTEM 証明書ストアに証明書をエクスポートする際にエラーが発生する可能性があります。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指定し、新規パスワードを入力して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されてから、ナビゲーション・フレームの「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示し、「**証明書のエクスポート (Export certificate)**」を選択します。
8. エクスポートする証明書のタイプとして「**認証局 (CA) (Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックします。

   注: サーバーまたはクライアント証明書を証明書ストアにエクスポートする前に、ローカル CA 証明書を証明書ストアにエクスポートする必要があります。最初にサーバーまたはクライアント証明書をエクスポートしてしまうと、ローカル CA 証明書が証明書ストアに存在しないという理由で、エラーになる可能性があります。
9. エクスポートするローカル CA 証明書を選択して、「**エクスポート (Export)**」をクリックします。
10. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
11. 対象の証明書ストアとして *SYSTEM と入力し、*SYSTEM 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。証明書が正常にエクスポートされたことを示すメッセージ、あるいは、(エクスポート・プロセスが失敗した場合には) エラー情報を示すメッセージが表示されます。

12. これで、*SYSTEM 証明書ストアにサーバーまたはクライアント証明書をエクスポートすることができます。「**証明書のエクスポート (Export certificate)**」タスクを再度選択します。
13. エクスポートする証明書のタイプとして**サーバーまたはクライアント**を選択して、「**続行 (Continue)**」をクリックします。
14. エクスポートする当該サーバー証明書またはクライアント証明書を選択して、「**エクスポート (Export)**」をクリックします。
15. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
16. 対象の証明書ストアとして *SYSTEM と入力し、*SYSTEM 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。証明書が正常にエクスポートされたことを示すメッセージ、あるいは、(エクスポート・プロセスが失敗した場合には) エラー情報を示すメッセージが表示されます。
17. これで、SSL で使用する証明書をアプリケーションに割り当てることができます。ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
18. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、*SYSTEM 証明書ストアのためのパスワードを入力して、「**続行 (Continue)**」をクリックします。
19. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
20. タスク・リストから「**証明書の割り当て (Assign certificate)**」を選択し、現行の証明書ストア内にある証明書のリストを表示します。
21. ホスト・システムで作成した証明書を選択し、「**アプリケーションへの割り当て (Assign to Applications)**」をクリックして、証明書の割り当て対象とすることができる SSL 対応アプリケーションのリストを表示します。
22. SSL セッションのためにその証明書を使用する必要があるアプリケーションを選択し、「**続行 (Continue)**」をクリックします。DCM は、そのアプリケーションに対する証明書の選択についての確認メッセージを表示します。

    注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。これをサポートしているアプリケーションでは、資源にアクセスする前に証明書を認証できるようにしなければなりません。したがって、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

これらのタスクが完了した後、ターゲット・システムのアプリケーションは、別の iSeries のローカル CA により発行された証明書を使用することができます。ただし、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを

取得しなければなりません。ローカル CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

V5R1 ターゲット・システムでの SSL セッションのための専用証明書の使用

アプリケーションが SSL セッションのために使用する証明書は、ディジタル証明書マネージャー (DCM) の *SYSTEM 証明書ストアから管理します。V5R1 ターゲット・システムで DCM を使用して SSL のための証明書をこれまでに管理したことがない場合、この証明書ストアはターゲット・システムには存在していません。ローカル認証局 (CA) ホスト・システムで作成した転送証明書ストア・ファイルを使用するために必要なタスクは、*SYSTEM 証明書ストアが存在しているかどうかによって異なります。 *SYSTEM 証明書ストアが存在しない場合は、転送された証明書ファイルを使用して *SYSTEM 証明書ストアを作成することができます。
*SYSTEM 証明書が V5R1 ターゲット・システムに存在する場合には、転送された証明書ファイルを次の 2 つのうちのいずれかの方法で使用することができます。

- 転送されたファイルを他のシステム証明書ストアとして使用する。
- 転送されたファイルを既存の *SYSTEM 証明書ストアにインポートする。

*SYSTEM 証明書ストアが存在しない場合

*SYSTEM 証明書ストアが、転送証明書ストア・ファイルを使用しようとする V5R1 システムに存在しない場合は、転送証明書ストア・ファイルを *SYSTEM 証明書ストアとして使用することができます。証明書ファイルを V5R1 ターゲット・システムで使用するには、以下のステップに従ってください。

1. ローカル CA をホスト処理するシステムで作成した証明書ストア・ファイル (拡張子 .KDB を持つファイルと拡張子 .RDB を持つファイルの 2 ファイル) が、 /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにあることを確認してください。
2. 転送された証明書ファイルが /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに配置されてから、これらのファイルの名前を DEFAULT.KDB および DEFAULT.RDB に変更します。当該ディレクトリー内でこれらのファイル名を変更することによって、ターゲット・システムの *SYSTEM 証明書ストアを構成する構成要素が作成されます。証明書ストア・ファイルには、既に数多くの公開インターネット CA の証明書のコピーが含まれています。DCM は、これらのコピーおよびローカル CA 証明書のコピーを、作成時に証明書ストア・ファイルに追加しています。

   重要: ターゲット・システムの /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにすでに DEFAULT.KDB および DEFAULT.RDB ファイルが存在する場合、*SYSTEM 証明書ストアはこのターゲット・システムにすでに存在しています。したがって、転送ファイルの名前を指示どおり変更する必要はありません。デフォルト・ファイルを上書きすると、DCM、転送証明書ストア、およびその内容を使用する際に問題が生じます。これを行う代わりに、転送ファイルに固有の名前を付け、転送証明書ストアを「**他のシステム証明書ストア (Other System Certificate Store)**」として使用する必要があります。ファイルを「他のシステム証明書ストア

(Other System Certificate Store)」として使用すると、DCM を使用して、証明書を使用する必要があるアプリケーションを指定することはできません。

3. DCM を開始します。ここで、転送されたファイルを名前変更して作成した *SYSTEM 証明書ストアのパスワードを変更しなければなりません。パスワードを変更することにより、DCM によって新規パスワードが保管されるため、この証明書ストアですべての DCM 証明書管理機能を使用することができます。
4. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
5. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されてから、V5R1 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
6. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、SSL セッションに証明書を使用するアプリケーションを指定できます。
7. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
8. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、新規パスワードを指定して、「**続行 (Continue)**」をクリックします。
9. ナビゲーション・フレームが最新表示されたら、ナビゲーション・フレームの「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
10. タスク・リストから、「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、証明書を割り当てることができる、SSL 対応アプリケーションのリストを表示します。
11. このリストからアプリケーションを選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。
12. ホスト・システムのローカル CA が発行した証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。 DCM は、そのアプリケーションに対する証明書選択について確認するためのメッセージを表示します。

注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。これをサポートしているアプリケーションでは、資源にアクセスする前に証明書を認証できるようにしなければなりません。したがって、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リス

トにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

これらのタスクが完了した後、ターゲット・システムのアプリケーションは、別の iSeries のローカル CA により発行された証明書を使用することができます。ただし、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを取得しなければなりません。CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

*SYSTEM 証明書ストアが存在する場合 -「他のシステム証明書ストア (Other System Certificate Store)」としてファイルを使用

V5R1 ターゲット・システムに既に *SYSTEM 証明書ストアがある場合は、証明書ファイルの処理方法を決定しなければなりません。転送証明書ファイルを「**他のシステム証明書ストア (Other System Certificate Store)**」として使用することが選択できます。あるいは、専用証明書およびそれに対応するローカル CA 証明書を既存の *SYSTEM 証明書ストアにインポートすることが選択できます。

「他のシステム証明書ストア (Other System Certificate Store)」は、 SSL 証明書を保管する、ユーザー定義の 2 次的な証明書ストアです。これらを作成して使用し、DCM ユーティリティーでアプリケーション ID を登録する際に DCM API を使用しない、ユーザー作成の SSL 対応アプリケーションに証明書を提供できます。「他のシステム証明書ストア (Other System Certificate Store)」オプションを選択すると、証明書に SSL_Init API を使用してプログラマチックなアクセスを行い、その証明書を使用して SSL セッションを確立する、ユーザー作成のアプリケーションの証明書を管理することができます。この API を使用すると、アプリケーションは、ユーザーが特に指定した証明書ではなく、証明書ストアのデフォルト証明書を使用することができます。

IBM iSeries アプリケーション (および他の数多くのソフトウェア開発者によるアプリケーション) は、*SYSTEM 証明書ストアの証明書のみを使用するように作成されています。転送ファイルを「他のシステム証明書ストア (Other System Certificate Store)」として使用するようにすると、DCM を使用して、SSL セッションの証明書を使用する必要があるアプリケーションを指定することはできません。したがって、この証明書を使用するように、標準 iSeries SSL 対応アプリケーションを構成することはできません。iSeries アプリケーションで証明書を使用したい場合は、証明書を転送された証明書ストア・ファイルから *SYSTEM 証明書ストアにインポートしなければなりません。

転送された証明書ファイルを「他のシステム証明書ストア (Other System Certificate Store)」として利用して処理するには、以下のステップに従ってください。

1. DCM を開始します。

2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」が表示されたら、ホスト・システムから転送した証明書ストア・ファイル (拡張子 .KDB を持つファイル) の完全修飾パスおよびファイル名を指定します。また、V5R1 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、このストアの証明書をデフォルト証明書として使用するように指定できます。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指定し、新規パスワードを入力して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されたら、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**デフォルト証明書の設定 (Set default certificate)**」を選択します。

「他のシステム証明書ストア (Other System Certificate store)」が作成され、構成されましたので、SSL_Init API を使用する任意のアプリケーションは、その証明書ストア内の証明書を使用して SSL セッションを確立することができます。

*SYSTEM 証明書ストアが存在する場合 - 既存の *SYSTEM 証明書ストアの証明書を使用

V5R1 システムの既存の *SYSTEM 証明書ストアの転送証明書ストア・ファイルの証明書を使用することができます。これを行うには、証明書ストアの証明書を既存の *SYSTEM 証明書ストアにインポートしなければなりません。ただし、.KDB および .RDB ファイルから証明書を直接インポートすることはできません。これは、これらの証明書が、DCM インポート機能で認識および使用できる形式ではないためです。転送された証明書を既存の *SYSTEM 証明書ストアで使用するには、それらのファイルを「他のシステム証明書ストア (Other System Certificate store)」として開き、*SYSTEM 証明書ストアにエクスポートする必要があります。

注: この手順は、ターゲット・システムで「他のシステム証明書ストア (Other System Certificate store)」を使用して、元の証明書ストア・ファイルから *SYSTEM 証明書ストアに証明書をエクスポートする方法を説明しています。この方法を使用して証明書を *SYSTEM 証明書ストアに追加すると、ターゲッ

ト・システムがホスト・システムよりもセキュリティー・レベルの低い暗号アクセス・プロバイダー製品 (5722-AC2 など) を使用している場合に発生する可能性がある問題を回避するうえで役立ちます。

証明書ストア・ファイルから *SYSTEM 証明書ストアに証明書をエクスポートするには、V5R1 ターゲット・システムで以下のステップを行ってください。

1. DCM を開始します。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を指定します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、ホスト・システムから転送した証明書ストア・ファイル (拡張子 .KDB を持つファイル) の完全修飾パスおよびファイル名を指定します。また、V5R1 ターゲット・システム用の証明書の作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。パスワードを変更しないで「自動ログイン (Automatic login)」オプションを選択すると、このストアから *SYSTEM 証明書ストアに証明書をエクスポートする際にエラーが発生する可能性があります。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指定し、新規パスワードを入力して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されてから、ナビゲーション・フレームの「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示し、「**証明書のエクスポート (Export certificate)**」を選択します。
8. エクスポートする証明書のタイプとして「**認証局 (CA) (Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックします。

   注: サーバーまたはクライアント証明書を証明書ストアにエクスポートする前に、ローカル CA 証明書を証明書ストアにエクスポートする必要があります。最初にサーバーまたはクライアント証明書をエクスポートしてしまうと、ローカル CA 証明書が証明書ストアに存在しないという理由で、エラーになる可能性があります。
9. エクスポートするローカル CA 証明書を選択して、「**エクスポート (Export)**」をクリックします。

10. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
11. 対象の証明書ストアとして *SYSTEM と入力し、*SYSTEM 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。
12. これで、*SYSTEM 証明書ストアにサーバーまたはクライアント証明書をエクスポートすることができます。「**証明書のエクスポート (Export certificate)**」タスクを再度選択します。
13. エクスポートする証明書のタイプとして**サーバーまたはクライアント**を選択して、「**続行 (Continue)**」をクリックします。
14. エクスポートする当該サーバー証明書またはクライアント証明書を選択して、「**エクスポート (Export)**」をクリックします。
15. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
16. 対象の証明書ストアとして *SYSTEM と入力し、*SYSTEM 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。証明書が正常にエクスポートされたことを示すメッセージ、あるいは、(エクスポート・プロセスが失敗した場合には) エラー情報を示すメッセージが表示されます。
17. これで、SSL で使用する証明書をアプリケーションに割り当てることができます。ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SYSTEM** を選択します。
18. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、*SYSTEM 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。
19. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
20. タスク・リストから、「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、証明書を割り当てることができる、SSL 対応アプリケーションのリストを表示します。
21. このリストからアプリケーションを選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。
22. ホスト・システムのローカル CA が発行した証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。 DCM は、そのアプリケーションに対する証明書選択について確認するためのメッセージを表示します。

    注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。これをサポートしているアプリケーションでは、資源にアクセスする前に証明書を認証できるようにしなければなりません。したがって、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

これらのタスクが完了した後、ターゲット・システムのアプリケーションは、別の iSeries のローカル CA により発行された証明書を使用することができます。ただ

し、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを取得しなければなりません。CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

V5R2 または V5R1 ターゲット・システムでのオブジェクト署名のための専用証明書の使用

ディジタル証明書マネージャー (DCM) で、*OBJECTSIGNING 証明書ストアのオブジェクトの署名に使用する証明書を管理します。ターゲット・システムで DCM を使用して、オブジェクト署名証明書を管理したことがない場合、この証明書ストアはターゲット・システムには存在していません。ローカル CA ホスト・システムで作成した転送証明書ストア・ファイルを使用するために実行しなければならないタスクは、*OBJECTSIGNING 証明書ストアが存在しているかどうかによって異なります。 *OBJECTSIGNING 証明書ストアが存在しない場合は、転送された証明書ストア・ファイルを使用して *OBJECTSIGNING 証明書ストアを作成することができます。 *OBJECTSIGNING 証明書ストアがターゲット・システムに存在する場合には、転送された証明書をその証明書ストアにインポートしなければなりません。

*OBJECTSIGNING 証明書ストアが存在しない場合

ローカル CA ホスト・システムで作成した証明書ストア・ファイルを使用するために実行するタスクは、ターゲット・システムで DCM を使用して、オブジェクト署名証明書を管理したことがあるかどうかによって異なります。

*OBJECTSIGNING 証明書ストアが、転送証明書ストア・ファイルのある V5R2 または V5R1 ターゲット・システムに存在しない場合、以下のステップに従ってください。

1. ローカル CA をホスト処理するシステムで作成した証明書ストア・ファイル (拡張子 .KDB を持つファイルと拡張子 .RDB を持つファイルの 2 ファイル) が、 /QIBM/USERDATA/ICSS/CERT/SIGNING ディレクトリーにあることを確認してください。
2. 転送された証明書ファイルが /QIBM/USERDATA/ICSS/CERT/SIGNING ディレクトリーに配置された後で、必要に応じて、証明書ファイルの名前を SGNOBJ.KDB、および SGNOBJ.RDB に変更します。これらのファイル名を変更することによって、ターゲット・システムの *OBJECTSIGNING 証明書ストアを構成する構成要素が作成されます。証明書ストア・ファイルには、既に数多くの公開インターネット CA の証明書のコピーが含まれています。DCM は、これらのコピーおよびローカル CA 証明書のコピーを、作成時に証明書ストア・ファイルに追加しています。

   重要: すでにターゲット・システムの /QIBM/USERDATA/ICSS/CERT/SIGNING ディレクトリーに SGNOBJ.KDB および SGNOBJ.RDB ファイルがある場合、*OBJECTSIGNING 証明書ストアは現在このターゲット・システムに存在しています。したがって、転送ファイルの名前を指示どおり変更する必

要はありません。デフォルト・オブジェクトを上書きすると、DCM、転送証明書ストア、およびその内容を使用する際に問題が生じます。2 通りの方法のいずれかで、これらのファイルから証明書を取得して、既存の *OBJECTSIGNING 証明書ストアに配置します。このファイルの証明書を一連のフラット・ファイルにエクスポートして、ここから証明書を既存の *OBJECTSIGNING 証明書ストアにインポートできます。あるいは、後述するように、転送ファイルを「他のシステム証明書ストア (Other System Certificate Store)」としてオープンして、証明書を *OBJECTSIGNING 証明書ストアに直接エクスポートできます。いずれの場合も、この手順で説明しているように、証明書を使用するアプリケーションを管理できるようにしたい場合は、*OBJECTSIGNING 証明書ストアに証明書を入れなければなりません。

3. DCM を開始します。ここで、*OBJECTSIGNING 証明書ストアのパスワードを変更しなければなりません。パスワードを変更すると DCM によって新規パスワードが保管されるため、証明書ストアですべての DCM 証明書管理機能を使用することができます。
4. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
5. パスワード・ページが表示されたら、ホスト・システムで証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
6. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、証明書を使用してオブジェクトに署名するようにアプリケーション定義を作成することができます。
7. 証明書ストアを再オープンした後、ナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
8. タスク・リストから「**アプリケーションの追加 (Add Application)**」を選択して、証明書を使用してオブジェクトに署名するための、オブジェクト署名アプリケーション定義を作成するプロセスを開始します。
9. オブジェクト署名アプリケーションを定義するフォームを完成させて、「**追加 (Add)**」をクリックします。このアプリケーション定義は、実際のアプリケーションを示しているのではなく、特定の証明書を使って署名することになっているオブジェクトのタイプを示しています。このフォームの入力方法については、オンライン・ヘルプを参照してください。
10. 「**OK**」をクリックして、アプリケーション定義確認メッセージを確認し、「**アプリケーションの管理 (Manage Applications)**」のタスク・リストを表示します。
11. タスク・リストから、「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、証明書を割り当てることができる、オブジェクト署名アプリケーション ID のリストを表示します。
12. このリストからアプリケーション ID を選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。

13. ホスト・システムのローカル CA が作成した証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。

これらのタスクを完了すると、整合性を保証するためにオブジェクトへの署名を開始するうえで必要なすべての条件が整います。

署名済みオブジェクトを配布すると、このオブジェクトの受信側は、V5R2 または V5R1 バージョンの DCM を使用して、オブジェクトの署名の検査を行い、データが未変更であることを確認し、送信側の識別検査を行います。署名の妥当性検査を行うには、受信側に署名検査証明書のコピーがなければなりません。署名済みオブジェクトのパッケージの一部として、この証明書のコピーを提示する必要があります。

受信側には、オブジェクトに署名するために使用した証明書を発行した CA の CA 証明書のコピーも必要です。一般的に知られているインターネット CA の証明書を使用してオブジェクトに署名した場合は、受信側のバージョンの DCM に、必要な CA 証明書のコピーが既に存在している必要があります。ただし、必要に応じて、署名済みオブジェクトと共に CA 証明書のコピーを別パッケージで提供する必要があります。たとえば、ローカル CA の証明書を使用してオブジェクトに署名した場合は、ローカル CA 証明書のコピーを提供する必要があります。セキュリティー上の理由から、別のパッケージで CA 証明書を提供するか、証明書を必要とするユーザーからの要求があった時点で、公的に CA 証明書を入手できるようにする必要があります。

*OBJECTSIGNING 証明書ストアが存在する場合

V5R2 または V5R1 システムの既存の *OBJECTSIGNING 証明書ストアで転送証明書ストア・ファイルの証明書を使用することができます。そうするには、証明書ストア・ファイルの証明書を既存の *OBJECTSIGNING 証明書ストアにインポートしなければなりません。ただし、.KDB および .RDB ファイルから証明書を直接インポートすることはできません。これは、これらの証明書が、DCM インポート機能で認識および使用できる形式ではないためです。V5R2 または V5R1 ターゲット・システムの「他のシステム証明書ストア (Other System Certificate Store)」として転送ファイルをオープンすることによって、既存の *OBJECTSIGNING 証明書ストアに証明書を追加することができます。そうすれば、この証明書を *OBJECTSIGNING 証明書ストアに直接エクスポートすることができます。転送されたファイルからオブジェクト署名証明書自体とローカル CA 証明書の両方のコピーをエクスポートしなければなりません。

証明書ストア・ファイルから証明書をエクスポートして、それを *OBJECTSIGNING 証明書ストアに直接インポートするには、V5R2 または V5R1 ターゲット・システムで以下のステップを完了してください。

1. DCM を開始します。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を指定します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指

定します。また、証明書ストアの作成時にホスト・システムで証明書ストア用に指定したパスワードを入力して、「**続行 (Continue)**」をクリックします。

4. ナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」を選択して、タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。パスワードを変更しないで「自動ログイン (Automatic login)」オプションを選択すると、このストアから *OBJECTSIGNING 証明書ストアに証明書をエクスポートする際にエラーが発生する可能性があります。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。
5. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして「**他のシステム証明書ストア (Other System Certificate Store)**」を選択します。
6. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示された後で、証明書ストア・ファイルの完全修飾パスおよびファイル名を指定し、新規パスワードを入力して、「**続行 (Continue)**」をクリックします。
7. ナビゲーション・フレームが最新表示されてから、ナビゲーション・フレームの「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示し、「**証明書のエクスポート (Export certificate)**」を選択します。
8. エクスポートする証明書のタイプとして「**認証局 (CA) (Certificate Authority (CA))**」を選択して、「**続行 (Continue)**」をクリックします。

   注: このタスクの説明では、「他のシステム証明書ストア (Other System Certificate Store)」に対する操作であること、サーバーまたはクライアントの証明書を処理していることが前提になっています。これは、このタイプの証明書ストアを *SYSTEM 証明書ストアに対する 2 次ストアとして使用するように設計しているためです。しかし、この証明書ストアのエクスポート・タスクを使用することが、転送ファイルの証明書を既存の *OBJECTSIGNING 証明書ストアに追加する最も簡単な方法です。
9. エクスポートするローカル CA 証明書を選択して、「**エクスポート (Export)**」をクリックします。

   注: オブジェクト署名証明書を証明書ストアにエクスポートする前に、ローカル CA 証明書を証明書ストアにエクスポートする必要があります。最初にオブジェクト署名証明書をエクスポートしてしまうと、ローカル CA 証明書が証明書ストアに存在しないという理由で、エラーになる可能性があります。
10. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
11. 対象の証明書ストアとして *OBJECTSIGNING と入力し、証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。

12. これで、オブジェクト署名証明書を *OBJECTSIGNING 証明書ストアにエクスポートすることができます。「**証明書のエクスポート (Export certificate)**」タスクを再度選択します。
13. エクスポートする証明書のタイプとして**サーバーまたはクライアント**を選択して、「**続行 (Continue)**」をクリックします。
14. エクスポートする証明書を選択して、「**エクスポート (Export)**」をクリックします。
15. エクスポートされる証明書の宛先に「**証明書ストア (Certificate store)**」を選択して、「**続行 (Continue)**」をクリックします。
16. 対象の証明書ストアとして *OBJECTSIGNING と入力し、*OBJECTSIGNING 証明書ストアのパスワードを入力して、「**続行 (Continue)**」をクリックします。証明書が正常にエクスポートされたことを示すメッセージ、あるいは、(エクスポート・プロセスが失敗した場合には) エラー情報を示すメッセージが表示されます。

    注: この証明書を使用してオブジェクトに署名するには、ここで、オブジェクト署名アプリケーションに証明書を割り当てておかなければなりません。

V4R5 または V4R4 ターゲット・システムでの SSL セッションのための専用証明書の使用

アプリケーションが SSL セッションのために使用する、*SYSTEM 証明書ストアから取得した証明書は、ディジタル証明書マネージャー (DCM) で管理します。V4R5 または V4R4 ターゲット・システムで DCM を使用して SSL のための証明書を管理したことがない場合、この証明書ストアはターゲット・システムには存在していません。ローカル CA ホスト・システムで作成され、転送された証明書ストア・ファイルには、2 つの証明書が含まれています。すなわち、ユーザー側で作成したサーバーまたはクライアント証明書と、それに署名するために使用した専用ローカル CA 証明書です。

転送証明書ストア・ファイルを使用するために実行しなければならないタスクは、*SYSTEM 証明書ストアが存在しているかどうかによって異なります。 *SYSTEM 証明書ストアが存在しない場合は、転送された証明書ストア・ファイルを使用して *SYSTEM 証明書ストアを作成することができます。 *SYSTEM 証明書がターゲット・システムに存在する場合には、転送された証明書ファイルを、次の 2 つのうちのいずれかの方法で使用することができます。

- 転送されたファイルを他のシステム証明書ストアとして使用する。
- 転送されたファイルを既存の *SYSTEM 証明書ストアにインポートする。

*SYSTEM 証明書ストアが存在しない場合

*SYSTEM 証明書ストアが、転送証明書ストア・ファイルを使用しようとしている V4R5 または V4R4 システムに存在しない場合は、以下のステップに従ってください。

1. ローカル CA をホスト処理するシステムで作成した証明書ストア・ファイル (.KDB 拡張子を持つファイルと .RDB 拡張子を持つファイルの 2 ファイル) が、 /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにあることを確認してください。

2. 転送された証明書ファイルが /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに配置されてから、これらのファイルの名前を DEFAULT.KDB および DEFAULT.RDB に変更します。当該ディレクトリー内でこれらのファイル名を変更することによって、ターゲット・システムの *SYSTEM 証明書ストアを構成する構成要素が作成されます。証明書ストア・ファイルには、既に数多くの公開インターネット CA の証明書のコピーが含まれています。DCM は、これらのコピーおよびローカル CA 証明書のコピーを、作成時に証明書ストア・ファイルに追加しています。

   重要: ターゲット・システムの /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーにすでに DEFAULT.KDB および DEFAULT.RDB ファイルがある場合、*SYSTEM 証明書ストアは現在このターゲット・システムに存在しています。したがって、転送ファイルの名前を指示どおり変更する必要はありません。デフォルト・ファイルを上書きすると、DCM、転送証明書ストア、およびその内容を使用する際に問題が生じます。これを行う代わりに、転送ファイルに固有の名前を付け、転送証明書ストア・ファイルを**他の**証明書ストアとして使用する必要があります。ファイルを他の証明書ストアとして使用する場合、DCM を使用して、証明書を使用する必要があるアプリケーションを指定することはできません。
3. DCM を開始します。ここで、*SYSTEM 証明書ストアのパスワードを変更しなければなりません。パスワードを変更することにより DCM によって新規パスワードが保管されるため、この証明書ストアですべての DCM 証明書管理機能を使用することができます。
4. ナビゲーション・フレームでドロップダウン・リスト・ボックスに証明書ストアとして *SYSTEM が表示されていることを確認し、「**システム証明書 (System Certificates)**」を選択して、使用可能なタスクのリストを表示します。「**証明書ストアおよびパスワード (Certificate Store and Password)**」ウィンドウが表示されます。
5. 所要のフィールドに、オープンする証明書ストアとして *SYSTEM と入力し、ホスト・システムでローカル CA を使用してファイルを作成した際に使用したパスワードを入力してください。ここで、証明書ストアのパスワードを変更することができます。
6. ナビゲーション・フレームのタスク・リストで、「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。
7. *SYSTEM 証明書ストアを再オープンした後、タスク・リストから「**セキュア・アプリケーションの処理 (Work with secure applications)**」を選択して、特定のアプリケーションに関連付けられた証明書を管理できるページを表示します。
8. アプリケーションのリストから、SSL セッションのために転送専用証明書を使用する必要があるアプリケーションを選択します。
9. 「**システム証明書の処理 (Work with system certificate)**」をクリックして、ホスト・システムのローカル CA が発行した証明書を選択します。
10. 「**新規証明書の割り当て (Assign new certificate)**」をクリックして、指定されたアプリケーションで選択した証明書を使用するようにします。

    注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。クライアント認証に証明書を使用すると、

アプリケーションは、有効な証明書を受け取ってから、制御する資源へのアクセスが許可されることになります。これをサポートしているアプリケーションが特定の CA が発行した資源を認証できるようにするには、CA を承認するように設定されていなければなりません。「**認証局の処理 (Work with Certificate Authorities)**」ページを使用して、証明書ストア内で CA 証明書がトラステッド状況になるようにしてください。そのうえで、「**保護アプリケーションの処理 (Work with Secure Applications)**」ページを使用して、証明書を使用するアプリケーションが、証明書を発行したローカル用 CA を信頼するようにします。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、トラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

これらのタスクが完了した後、 V4R5 または V4R4 ターゲット・システムのアプリケーションは、別の iSeries の V5R2 ローカル CA により発行された証明書を使用することができます。ただし、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを取得しなければなりません。CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

*SYSTEM 証明書ストアが存在する場合 -「他のシステム証明書ストア (Other system certificate Store)」としてファイルを使用

V4R5 または V4R4 ターゲット・システムに既に *SYSTEM 証明書ストアがある場合は、証明書ファイルの処理方法を決定しなければなりません。転送証明書ストア・ファイルには、ユーザー側で作成したサーバーまたはクライアント証明書と、これに署名するのに使用した専用ローカル CA 証明書という 2 つ証明書が含まれています。転送証明書ファイルを**他の**システム証明書ストアとして使用することができます。あるいは、専用証明書およびそれに対応する CA 証明書を既存の *SYSTEM 証明書ストアにインポートすることが選択できます。

転送ファイルを**他の**システム証明書ストアとして使用することにした場合、DCM を使用して、SSL セッションの証明書を使用する必要があるアプリケーションを指定することはできません。ただし、この証明書ストアの証明書を証明書ストアのデフォルト証明書として指定することができます。「他のシステム証明書ストア (Other System Certificate Store)」オプションを使用すると、証明書に SSL_Init API を使用して方針に基づいたアクセスを行い、その証明書を使用して SSL セッションを確立する、ユーザー作成のアプリケーションの証明書を管理できるようになります。この API を使用すると、アプリケーションは、特定の証明書ではなく、デフォルトの証明書を、証明書ストアに使用することができます。

*SYSTEM 証明書ストアが、転送証明書ストア・ファイルを使用しようとしている V4R5 または V4R4 システムに存在する場合は、以下のステップに従ってください。

1. DCM を開始します。ここで、転送証明書ストアのパスワードを変更しなければなりません。パスワードを変更することにより、DCM によって新規パスワードが保管されるため、この証明書ストアですべての DCM 証明書管理機能を使用することができます。
2. ナビゲーション・フレームでドロップダウン・リスト・ボックスに証明書ストアとして OTHER が表示されていることを確認し、「**システム証明書 (System Certificates)**」を選択して、使用可能なタスクのリストを表示します。「**証明書ストアおよびパスワード (Certificate Store and Password)**」ウィンドウが表示されます。
3. 所定のフィールドに、ローカル CA ホスト・システムから転送した証明書ストア (.KDB 拡張子) の完全修飾パスおよびファイル名を入力します。ホスト・システムでファイルを作成した際に使用したパスワードを入力してください。ここで、証明書ストアのパスワードを変更することができます。
4. ナビゲーション・フレームで、「システム証明書 (System Certificate)」タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。次に、このストアの証明書をデフォルト証明書として使用するように指定できます。
5. ナビゲーション・フレームで「**証明書の処理 (Work with certificates)**」を選択して、数多くの証明書管理タスクを実行できるページを表示します。
6. 証明書のリストから、現行ストアのデフォルト証明書として使用したい証明書を選択して、「**デフォルトの設定 (Set default)**」をクリックします。

「他のシステム証明書ストア (Other system certificate store)」を作成し、構成したので、SSL_Init API を使用するアプリケーションはいずれも、その証明書ストア内の証明書を使用して、SSL セッションを確立することができます。

*SYSTEM 証明書ストアが存在する場合 - このファイルを既存の *SYSTEM 証明書ストアにインポート

V4R5 または V4R4 ターゲット・システムの *SYSTEM に証明書をインポートできるようにするには、まず、作成した証明書ストアの証明書を別のファイル・フォーマットにエクスポートしなければなりません。これで、新規ファイルから *SYSTEM 証明書ストアに証明書をインポートできます。転送証明書ストア・ファイルには、ユーザー側で作成したサーバーまたはクライアント証明書と、これに署名するのに使用した専用ローカル CA 証明書という 2 つ証明書が含まれています。ユーザー側で作成したサーバーまたはクライアント証明書と、専用ローカル CA 証明書の両方を *SYSTEM 証明書ストアにインポートしなければなりません。

注: V4R5 および V4R4 の場合、DCM で使用可能なエクスポート機能は、V5R2 の場合ほど機能的に優れていないため、ターゲット・システムを使用して、専

用ローカル CA 証明書をエクスポートする場合に問題が発生する可能性があります。したがって、ローカル CA 証明書の*追加* コピーを別ファイルにエクスポートするには、V4R4 または V4R5 ターゲット・システムを使用するのではなく、V5R2 ホスト・システムを使用してエクスポートする必要があります。V5R2 ホスト・システムでローカル CA 証明書をエクスポートした後、V4R4 または V4R5 ターゲット・システムにローカル CA 証明書エクスポート・ファイルを手動で転送し、この手順で詳しく説明されているステップに従って、ローカル CA 証明書を *SYSTEM 証明書ストアにインポートすることができます。ローカル CA 証明書で作成した専用証明書をインポートする*前*に、ローカル CA 証明書をインポートしなければなりません。最初に専用証明書をインポートしてしまうと、ローカル CA 証明書が証明書ストアに存在しないという理由で、エラーになる可能性があります。

証明書ストア・ファイルから証明書をエクスポートするには、 V4R4 または V4R5 ターゲット・システムで以下のステップを完了してください。

1. DCM を開始します。
2. ナビゲーション・フレームでドロップダウン・リスト・ボックスに証明書ストアとして OTHER が表示されていることを確認し、「**システム証明書 (System Certificates)**」を選択して、使用可能なタスクのリストを表示します。「**証明書ストアおよびパスワード (Certificate Store and Password)**」ウィンドウが表示されます。
3. 転送証明書ストア・ファイルの完全修飾パスおよびファイル名を指定して、ホスト・システムでシステム証明書ストア・ファイルの作成時に使用したパスワードを指定して、「**OK**」をクリックします。ここで、証明書ストアのパスワードを変更することができます。
4. ナビゲーション・フレームで、「システム証明書 (System Certificate)」タスクのリストから「**パスワードの変更 (Change password)**」を選択します。証明書ストアのパスワードを変更するフォームを完成させます。

   注: 証明書ストアのパスワードを変更する場合は、必ず「**自動ログイン (Automatic login)**」オプションを選択してください。このオプションを使用すると、DCM で新規パスワードが保管されるようになるため、新規ストアですべての DCM 証明書管理機能を使用することができます。パスワードを変更しないで「自動ログイン (Automatic login)」オプションを選択すると、このストアから証明書をエクスポートする際にエラーが発生する可能性があります。

   パスワードの変更後に証明書ストアの証明書を使用できるようにするには、証明書ストアを再オープンしなければなりません。
5. ナビゲーション・フレームで「**証明書の処理 (Work with certificates)**」を選択して、証明書のリストを表示します。
6. リストから専用証明書を選択して、「**エクスポート (Export)**」をクリックして、「証明書のエクスポート (Export Certificate)」ページを表示します。
7. 「証明書のエクスポート (Export Certificate)」フォームを完成させます。

   注: ファイルには、固有の名前と拡張子を必ず指定してください。たとえば、ファイルに `myfile.exp` という名前を付けることができます。ファイルに名前を付ける際には、ファイル拡張子、`.TXT`、`.KDB`、`.RDB`、または `.KYR` は、いずれも使用しないでください。これらの拡張子を使用すると、ファイルから証明書をインポートする際にエラーが発生する可能性があります。この証明

書を使用するターゲット・システムの、適切なリリース・レベルを選択してください。選択するリリース・レベルは、エクスポートされる証明書の形式に影響を与えます。

8. 「**OK**」をクリックします。指定したファイルに DCM により証明書がエクスポートされたというメッセージが、ページの一番上に表示されます。

この時点で、元の V5R2 ホスト・システムで DCM を使用して、ローカル CA 証明書の追加コピーをエクスポートし、これを V4R4 または V5R5 ターゲット・システムに手動で転送していなければなりません。また、このターゲット・システムの DCM を使用して、専用サーバーまたはクライアントの証明書をファイルにエクスポートしていなければなりません。これで、これらの証明書を *SYSTEM 証明書ストアにインポートできる状態になりました。ローカル CA 証明書で作成した専用証明書をインポートする*前*に、ローカル CA 証明書をインポートしなければなりません。最初に専用証明書をインポートしてしまうと、ローカル CA 証明書が証明書ストアに存在しないという理由で、エラーになる可能性があります。

これらのエクスポート・ファイルから証明書をインポートして、これらを SSL 対応アプリケーションが使用するように指定するには、V4R4 または V5R5 ターゲット・システムで以下のステップを完了してください。

1. DCM を開始します。
2. ナビゲーション・フレームでドロップダウン・リスト・ボックスに証明書ストアとして *SYSTEM が表示されていることを確認し、「**システム証明書 (System Certificates)**」を選択して、使用可能なタスクのリストを表示します。「**証明書ストアおよびパスワード (Certificate Store and Password)**」ウィンドウが表示されます。
3. オープンする証明書ストアとして *SYSTEM を指定して、パスワードを入力し、「**続行 (Continue)**」をクリックします。
4. ここで、V5R2 ホスト・システムで作成したエクスポート・ファイルからローカル CA 証明書をインポートしなければなりません。ナビゲーション・フレームで、「**CA 証明書の受信 (Receive a CA certificate)**」を選択して、フォームを表示します。
5. このフォームに入力して、「**OK**」をクリックして「証明書を正常に受信 (Receive Certificate Successful)」ページを表示します。 *SYSTEM 証明書ストアで作業する場合、インポートされた CA 証明書を承認するように設定できるアプリケーションのリストがこのページに表示されます。

   注: SSL 対応アプリケーションには、証明書に基づくクライアント認証をサポートしているものもあります。クライアント認証に証明書を使用すると、アプリケーションは、有効な証明書を受け取ってから、制御する資源へのアクセスが許可されることになります。これをサポートしているアプリケーションが特定の CA が発行した資源を認証できるようにするには、CA を承認するように設定されていなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、トラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。
6. CA 証明書を承認するアプリケーションを選択して、「**OK**」をクリックします。選択したアプリケーションが、新しい証明書を承認するように設定された

ことを確認する、「セキュア・アプリケーション・ステータス (Secure Applications Status)」ページが表示されます。
7. これで、サーバー証明書をインポートできます。ナビゲーション・フレームで「**証明書の処理 (Work with certificates)**」を選択して、証明書のリストを表示します。
8. 「**インポート (Import)**」をクリックして、「証明書のインポート (Import Certificate)」ページを表示します。
9. 「証明書のインポート (Import Certificate)」フォームに入力して、「**OK**」をクリックし、「証明書の処理 (Work with Certificates)」ページに戻ります。エクスポートされたサーバーまたはクライアント証明書の入っているファイルの名前を必ず指定し、また、前に証明書をエクスポートしたときに指定したものと一致するターゲット・リリースを必ず指定してください。 DCM により証明書が現行の証明書ストアに追加されたというメッセージが、ページの一番上に表示されます。インポートした証明書も同様に、証明書のリストに表示されます。
10. ここで、SSL にインポートされた専用証明書を使用する必要があるアプリケーションを指定しなければなりません。ナビゲーション・フレームで「**セキュア・アプリケーションの処理 (Work with secure applications)**」を選択して、特定のアプリケーションに関連付けられた証明書を管理できるページを表示します。
11. リストからアプリケーションを選択して、「**システム証明書の処理 (Work with system certificate)**」を選択して、SSL セッション確立のために選択したアプリケーションで使用するように指定できる証明書のリストを表示します。
12. リストから証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックし、選択した証明書を指定されたアプリケーションに割り当てます。証明書の選択を示す確認メッセージが、ページの一番上に表示されます。

これらのタスクが完了した後、 V4R4 または V4R5 ターゲット・システムのアプリケーションは、別の iSeries のローカル CA により発行された証明書を使用することができます。ただし、これらのアプリケーションで SSL の使用を開始するには、SSL を使用するようにアプリケーションを構成しなければなりません。

選択したアプリケーションに SSL 接続経由でアクセスできるようにするには、ユーザーは、DCM を使用して、ホスト・システムからローカル CA 証明書のコピーを取得しなければなりません。 CA 証明書はユーザーの PC のファイルにコピーするか、ユーザーのブラウザーにダウンロードする必要があります。これは SSL 使用可能アプリケーションの要件により異なります。

DCM によるアプリケーションの管理

ディジタル証明書マネージャー (DCM) を使用して、SSL 対応アプリケーションおよびオブジェクト署名アプリケーションのための各種管理タスクを実行することができます。たとえば、Secure Sockets Layer (SSL) 通信セッションでアプリケーションが使用する証明書の種類を管理することができます。実行可能なアプリケーション管理タスクは、アプリケーションのタイプおよび使用しているで証明書ストアによって異なります。*SYSTEM または *OBJECTSIGNING 証明書ストアのアプリケーションのみ管理することができます。

DCM から提供されている、ほとんどのアプリケーション管理タスクは、理解しやすいものばかりですが、これらのタスクの中には、分かりにくいものも少しだけあります。このようなタスクについて、詳しくは、以下のトピックを参照してください。

『**アプリケーション定義の作成**』では、ユーザーが定義して使用することのできるアプリケーションのタイプについて説明します。

『**アプリケーションに対する証明書割り当ての管理**』では、SSL セッションを確立したり、オブジェクトに署名したりするために、アプリケーションで使用する証明書の割り当ておよび変更方法を説明します。

『**アプリケーションの CA 信頼リストの定義**』では、証明書の妥当性検査および受け入れのためにアプリケーションが承認可能な認証局を、いつ定義できるか、および、いつ定義する必要があるかを説明します。

その他の DCM タスクについては、オンライン・ヘルプを参照してください。

アプリケーション定義の作成

DCM で処理できるアプリケーション定義のタイプには、SSL を使用するサーバーまたはクライアント・アプリケーションの場合のアプリケーション定義、およびオブジェクトの署名に使用するアプリケーション定義の 2 つがあります。

DCM を使用して、SSL アプリケーション定義およびその証明書を処理するには、アプリケーションはまず、固有のアプリケーション定義 ID を持つように、アプリケーション定義として DCM に登録しなければなりません。アプリケーション開発者は、API (QSYRGAP、QsyRegisterAppForCertUse) を使用して、アプリケーション ID を DCM に自動的に作成し、SSL 対応アプリケーションを登録します。 IBM iSeries のすべての SSL 対応アプリケーションが DCM に登録されます。その結果、ユーザーは、アプリケーションが SSL セッションを確立できるように、DCM 使用して、これらのアプリケーションに証明書を簡単に割り当てることができます。作成または購入したアプリケーションの場合も、ユーザーは、アプリケーション定義を定義して、DCM 内にそのアプリケーションのアプリケーション ID を作成できます。クライアント・アプリケーションまたはサーバー・アプリケーションのいずれかのために SSL アプリケーション定義を作成するには、*SYSTEM 証明書ストア内で作業しなければなりません。

証明書を使用してオブジェクトに署名するには、まず、証明書で使用するアプリケーションを定義しなければなりません。SSL アプリケーションと異なり、オブジェクト署名アプリケーションは、実際のアプリケーションを表しているわけではありません。そうではなく、作成するアプリケーション定義は、署名対象オブジェクトのタイプまたはグループを表します。オブジェクト署名アプリケーション定義を作成するには、*OBJECTSIGNING 証明書ストア内で作業しなければなりません。

アプリケーション定義を作成するには、以下のステップに従ってください。

1. DCM を開始します。
2. 「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、所要の証明書ストアを選択します。 (これは、*SYSTEM 証明書ストアまたは *OBJECTSIGNING 証明書ストアのいずれかで、作成するアプリケーション定義のタイプによって決まります。)

注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが利用できます。

3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
5. タスク・リストから「**アプリケーションの追加 (Add Application)**」を選択して、アプリケーションを定義するフォームを表示します。

   注: *SYSTEM 証明書ストアで作業している場合は、サーバー・アプリケーション定義かクライアント・アプリケーション定義のどちらを追加するのか選択するように、 DCM からプロンプト表示が出されます。
6. フォームに入力して、「**追加 (Add)**」をクリックします。アプリケーション定義に指定できる情報は、定義するアプリケーションのタイプによって異なります。サーバー・アプリケーションを定義する場合、アプリケーションでクライアント認証に証明書が使用できるかどうか、そして、クライアント認証を必要とするかどうかも指定することができます。アプリケーションが CA 信頼リストを使用して、証明書を認証しなければならないように指定することもできます。

アプリケーションに対する証明書割り当ての管理

アプリケーションが、Secure Sockets Layer (SSL) の確立またはオブジェクトへの署名などのセキュア機能を実行できるようにするには、ディジタル証明書マネージャー (DCM) を使用して、アプリケーションに証明書を割り当てなければなりません。アプリケーションに証明書を割り当てたり、アプリケーションに対する証明書割り当てを変更したりするには、以下のステップに従ってください。

1. DCM を開始します。
2. 「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、所要の証明書ストアを選択します。 (これは、*SYSTEM 証明書ストアまたは *OBJECTSIGNING 証明書ストアのいずれかで、証明書を割り当てようとするアプリケーション定義のタイプによって決まります。)

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが利用できます。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
5. *SYSTEM 証明書ストアで作業を行っている場合には、管理対象アプリケーションのタイプを選択してください。 (状況に応じて「**サーバー (Server)**」または「**クライアント (Client)**」アプリケーションを選択してください。)
6. タスク・リストから、「**証明書割り当ての更新 (Update certificate assignment)**」を選択して、証明書を割り当てることができるアプリケーションのリストを表示します。

7. リストからアプリケーションを選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックして、アプリケーションに割り当て可能な証明書のリストを表示します。
8. リストから証明書を選択して、「**新規証明書の割り当て (Assign new certificate)**」をクリックします。 DCM は、そのアプリケーションに対する証明書選択について確認するためのメッセージを表示します。

   注: クライアント認証に証明書の使用をサポートしている、SSL 対応アプリケーションに証明書を割り当てる場合、アプリケーションに CA 信頼リストを定義しなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

アプリケーションの証明書を変更または除去する際、証明書割り当ての変更を行った時点で、アプリケーションが実行中である場合、アプリケーションは変更を認識できる場合とそうでない場合があります。たとえば、Client Access Express サーバーは、ユーザーが作成するすべての証明書の変更を自動的に適用します。しかし、Telnet サーバー、IBM HTTP Server for iSeries、またはその他のアプリケーションの場合、これらのアプリケーションが証明書を適用できるようにするには、これらを停止してから開始しなくてはなりません。

V5R2 以降では、一度に複数のアプリケーションに証明書を割り当てる際に、「証明書の割り当て (Assign certificate)」タスクを使用できるようになりました。

アプリケーションの CA 信頼リストの定義

Secure Sockets Layer (SSL) セッションでクライアント認証に証明書の使用をサポートしているアプリケーションは、有効な ID 証明として、証明書を受け入れるかどうか決定しなければなりません。アプリケーションが証明書を認証する場合に使用する基準の 1 つは、証明書を発行した認証局 (CA) をアプリケーションが承認するかどうかです。

ディジタル証明書マネージャー (DCM) を使用すると、証明書のクライアント認証を行う際に、アプリケーションが承認できる CA を定義することができます。CA 信頼リストによってアプリケーションが承認する CA を管理します。

アプリケーションの CA 信頼リストを定義できるようにするには、いくつかの条件を満たしていなければなりません。
- アプリケーションは、クライアント認証に証明書の使用をサポートしていなければならない。
- アプリケーションの定義で、アプリケーションが CA 信頼リストを使用するように指定しなければならない。

アプリケーションの定義で、アプリケーションが CA 信頼リストを使用するように指定する場合、アプリケーションが証明書のクライアント認証を正常に実行できるようにするには、このリストを定義しておかなければなりません。これにより、アプリケーションは、トラステッドとして指定されている CA の証明書のみを妥当性

検査することができるようになります。ユーザーまたはクライアント・アプリケーションから、CA 信頼リストにおいてトラステッドであると指定されていない CA の証明書が提供された場合、アプリケーションは、その証明書を有効な認証の基礎としては受け入れません。

アプリケーションの信頼リストに CA を追加する際、CA も使用可能な状態にしておかなければなりません。

アプリケーションの CA 信頼リストを定義するには、以下のステップに従ってください。

1. DCM を開始します。
2. 「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして *SYSTEM を選択します。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが利用できます。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択して、タスクのリストを表示します。
5. タスク・リストから、「**CA 信頼リストの定義 (Define CA trust list)**」を選択します。
6. リストを定義したいアプリケーション (サーバーまたはクライアント) のタイプを選択して、「**続行 (Continue)**」をクリックします。
7. リストからアプリケーションを選択して、「**続行 (Continue)**」をクリックして、信頼リストの定義に使用する CA 証明書のリストを表示します。
8. アプリケーションが承認する必要がある CA を選択して、「**OK**」をクリックします。 DCM は、信頼リスト選択について確認するためのメッセージを表示します。

   注: リストから個別の CA を選択することも、アプリケーションでリスト内の CA をすべて承認するように、あるいは全く承認しないように指定することもできます。信頼リストに追加する前に、CA 証明書を表示したり、妥当性検査することもできます。

証明書およびアプリケーションの妥当性検査

ディジタル証明書マネージャー (DCM) を使用して、個別の証明書またはその証明書を使用するアプリケーションの妥当性検査を行うことができます。 DCM が検査する項目のリストは、証明書の妥当性検査を行うのか、アプリケーションの妥当性検査を行うのかによって少し異なります。

アプリケーションの妥当性検査

DCM を使用してアプリケーション定義を妥当性検査すると、証明書を必要とする機能を実行しているときに、アプリケーションの証明書に関する問題を防ぐ手助けに

なります。このような問題があると、アプリケーションが Secure Sockets Layer (SSL) セッションに正常に関係したり、オブジェクトに正常に署名したりすることができなくなる可能性があります。

アプリケーションの妥当性検査を行う際、DCM は、そのアプリケーションに対する証明書割り当てがあるかどうか検査し、割り当てられた証明書が有効であるかを確認します。さらに、DCM は、アプリケーションが認証局 (CA) の信頼リストを使用するように構成されているか、そして、信頼リストに少なくとも 1 つの CA 証明書が含まれているかを確認します。次に DCM は、アプリケーション CA 信頼リストの CA 証明書が有効であるかを検査します。アプリケーション定義で、証明書取り消しリスト (CRL) の処理を実行するように指定があり、CA に対して CRL 位置が定義されている場合は、DCM は、CRL も検査プロセスの一環として検査します。

証明書の妥当性検査

証明書の妥当性検査を行う際、DCM は、その証明書に関連する複数の項目を検査し、証明書の認証性および妥当性を確認します。証明書の妥当性検査を行うと、セキュア通信またはオブジェクトへの署名のために証明書を使用するアプリケーションが証明書を使用する際に、問題が発生する可能性が低くなります。

検査プロセスの一環として、DCM は選択した証明書の有効期限が切れていないことを確認します。DCM は、証明書を発行した CA に対して CRL 位置が存在している場合に、その証明書が、証明書取り消しリストに取り消し対象としてリストされていないことも確認します。さらに、DCM は、発行 CA の CA 証明書が現行の証明書ストアにあり、その CA 証明書が使用可能であるかどうかにより、トラステッドであるかどうかを確認します。証明書の秘密鍵がある場合 (たとえば、サーバー、クライアント、およびオブジェクト署名の証明書) は、DCM は、公開鍵と秘密鍵のペアの妥当性検査も行い、公開鍵と秘密鍵のペアが一致していることを確認します。言い換えれば、DCM は公開鍵でデータを暗号化してから、そのデータが秘密鍵を使って復号できることを確認します。

アプリケーションへの証明書の割り当て

V5R2 より、あらたにディジタル証明書マネージャー (DCM) が機能強化され、複数のアプリケーションに証明書を迅速かつ簡単に割り当てることができるようになりました。 *SYSTEM または *OBJECTSIGNING 証明書ストア内でのみ、証明書を複数のアプリケーションに割り当てることができます。

1 つまたは複数のアプリケーションに証明書を割り当てるには、以下のステップに従ってください。

1. DCM を開始します。

   注: DCM を使用する際に特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択して、オンライン・ヘルプを利用してください。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** または ***SYSTEM** を選択します。

3. 証明書ストアにパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
5. タスクのリストから「**証明書の割り当て (Assign certificate)**」を選択し、現行の証明書ストアに関する証明書のリストを表示します。
6. リストから証明書を選択し、「**アプリケーションへの割り当て (Assign to Applications)**」をクリックして、現行の証明書ストアに関するアプリケーション定義のリストを表示します。
7. このリストから 1 つまたは複数のアプリケーションを選択して、「**続行 (Continue)**」をクリックします。割り当ての選択に関する確認メッセージを示すページ、あるいは、(問題が生じた場合には) エラー・メッセージを示すページが表示されます。

CRL 位置の管理

ディジタル証明書マネージャー (DCM) を使用して、証明書妥当性検査プロセスの一環として使用する特定の認証局 (CA) に関する証明書取り消しリスト (CRL) 位置情報を定義および管理することができます。DCM、または CRL 処理を必要とするアプリケーションは、CRL を使用して、特定の証明書を発行した CA がその証明書を取り消していないかどうか判断することができます。特定の CA の CRL 位置を定義するときに、クライアント認証に証明書の使用をサポートしているアプリケーションは、CRL にアクセスすることができます。

クライアント認証に証明書の使用をサポートしているアプリケーションは、CRL 処理を実行して、証明書を有効な ID 証明として受け入れるかどうかを確認するための、より厳正な認証を行うことができます。アプリケーションが、証明書検査プロセスの一環として、定義された CRL を使用できるようにするには、DCM のアプリケーション定義で、アプリケーションが CRL 処理を実行するように指定されていなければなりません。

CRL 処理の内容

DCM を使用して、証明書またはアプリケーションの妥当性検査を行う際、デフォルトの DCM では、検査プロセスの一環として CRL 処理を実行します。妥当性検査を行っている証明書を発行した CA に CRL 位置が定義されていない場合、DCM は CRL 検査を実行できません。ただし、DCM は、特定の証明書の CA 署名が有効であるかどうか、あるいはそれを発行した CA がトラステッドであるかどうかなどの、証明書に関する他の重要な情報の妥当性検査を試みることができます。

CRL 位置の定義

特定の CA の CRL 位置を定義するには、以下のステップに従ってください。

1. DCM を開始します。
2. ナビゲーション・フレームで、「**CRL 位置の管理 (Manage CRL Locations)**」を選択して、タスクのリストを表示します。
3. タスク・リストから「**CRL 位置の追加 (Add CRL location)**」を選択して、CRL 位置および DCM またはアプリケーションがその位置にアクセスする方法を指定するためのフォームを表示します。

4. このフォームに入力して、「**OK**」ボタンをクリックします。CRL 位置に固有の名前を付け、CRL をホスト処理する LDAP サーバーを特定し、LDAP サーバーへのアクセス方法を記述した接続情報を提供しなければなりません。

   注: このガイド・タスクでの特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。

   ここで、CRL 位置定義と特定の CA を関連付ける必要があります。
5. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択して、タスクのリストを表示します。
6. タスク・リストから「**CRL 位置割り当ての更新 (Update CRL location Assignment)**」を選択し、CA 証明書のリストを表示します。
7. このリストから、作成した CRL 位置定義を割り当てる CA 証明書を選択し、「**CRL 位置割り当ての更新 (Update CRL Location Assignment)**」をクリックします。 CRL 位置のリストが表示されます。
8. CA と関連付ける CRL 位置をリストから選択し、「**割り当ての更新 (Update Assignment)**」をクリックします。ページの先頭にメッセージが表示され、その CRL 位置が認証局 (CA) 証明書に割り当てられたことが示されます。

特定の CA の CRL 位置を定義していると、DCM またはその他のアプリケーションが CRL 処理の実行時にこれを使用できます。ただし、CRL 処理が機能できるようにするには、Directory Services サーバーに適切な CRL が含まれていなければなりません。また、Directory Services サーバーとクライアント・アプリケーションの両方で SSL を使用するように構成し、 DCM のアプリケーションに証明書を割り当てなければなりません。

iSeries Directory Services (LDAP) サーバーの構成および使用について、詳しくは、以下の Information Center トピックを参照してください。

- ディレクトリー・サービス (LDAP)
  このトピックでは、iSeries Directory Services (LDAP) サーバーの構成および使用に関する必要事項をすべて説明しています。
- LDAP ディレクトリー・サーバーでの Secure Sockets Layer (SSL) セキュリティーの使用
  このトピックでは、セキュア通信として SSL を使用するように LDAP サーバーを構成する際に実行する必要のある事項について説明しています。

IBM 4758 暗号化コプロセッサー上での証明書キーの保管

iSeries 上に IBM 4758-023 PCI 暗号化コプロセッサーをインストール済みの場合は、そのコプロセッサーを使用して証明書の秘密鍵にさらにセキュアなストレージを提供できます。このコプロセッサーを使用してサーバー証明書、クライアント証明書、またはローカル認証局 (CA) 証明書に対する秘密鍵を保管できます。ただし、ユーザー証明書の秘密鍵は、ユーザーのシステム上に保管しなければならないので、コプロセッサーを使用してこの秘密鍵を保管することはできません。また、この時点では、コプロセッサーを使用してオブジェクト署名証明書に対する秘密鍵を保管することもできません。

コプロセッサーを使用して証明書秘密鍵を保管するには、次の 2 つの方法のいずれかを行います。

- 証明書秘密鍵を直接コプロセッサー上に保管する。
- 特殊キー・ファイルに保管するために、 コプロセッサー・マスター・キーを使用して証明書秘密鍵を暗号化する。

このキー保管オプションは、証明書の作成または更新のプロセスの一環として選択できます。また、コプロセッサーを使用して証明書の秘密鍵を保管する場合は、その秘密鍵に対するコプロセッサー装置割り当ても変更できます。

コプロセッサーを秘密鍵の保管のために使用する場合は、ディジタル証明書マネージャー (DCM) を使用する前に、コプロセッサーがオンに変更されていることを確認する必要があります。オンに変更されていない場合は、DCM は、証明書の作成または更新プロセスの一環として、保管オプションの選択のためのページを提供しません。

サーバー証明書またはクライアント証明書を作成、または更新する場合は、現行証明書に署名する CA のタイプを選択した後、秘密鍵保管オプションを選択します。ローカル CA を作成、または更新する場合は、プロセスの第 1 ステップとして秘密鍵保管オプションを選択します。

証明書秘密鍵のコプロセッサーへの直接保管

証明書の秘密鍵へのアクセスおよび使用をさらに強固に保護するために、秘密鍵を IBM 4758-023 PCI 暗号化コプロセッサー上に直接保管することができます。このキー保管オプションは、ディジタル証明書マネージャー (DCM) で証明書を作成または更新する際に選択できます。

「**キー保管場所の選択 (Select a Key Storage Location)**」ページで以下のステップに従い、証明書の秘密鍵をコプロセッサー上に直接保管します。

1. 「**ハードウェア (Hardware)**」を保管オプションとして選択します。
2. 「**続行 (Continue)**」をクリックします。「**暗号装置記述の選択 (Select a Cryptographic Device Description)**」ページが表示されます。
3. 装置のリストから、証明書の秘密鍵の保管に使用したい装置を選択します。
4. 「**続行 (Continue)**」をクリックします。 DCM は、ユーザーが作成または更新している証明書に対する識別情報など、ユーザーが完了しようとしている作業のためのページを引き続き表示します。

コプロセッサー・マスター・キーの使用による証明書秘密鍵の暗号化

証明書の秘密鍵へのアクセスおよび使用をさらに強固に保護するために、IBM 4758-023 PCI 暗号化コプロセッサーのマスター・キーを使用して秘密鍵を暗号化し、特殊キー・ファイルに保管することができます。このキー保管オプションは、ディジタル証明書マネージャー (DCM) で証明書を作成または更新する際に選択できます。

このオプションを正常に使用するには、事前に IBM 4758-023 PCI 暗号化コプロセッサーの構成 Web インターフェースを使用して、適切な鍵ストア・ファイルを作成しなければなりません。また、コプロセッサー構成 Web インターフェースを使

用して、鍵ストア・ファイルを、使用したいコプロセッサー装置記述と関連付けることも必要です。コプロセッサー構成 Web インターフェースには、iSeries タスク・ページからアクセスできます。

複数のコプロセッサー装置がシステムにインストールされ、オンにされている場合は、証明書の秘密鍵を複数の装置間で共用することもできます。装置記述が秘密鍵を共用するには、すべての装置が同じマスター・キーを持っていなければなりません。同じマスター・キーを複数の装置に配布する処理は、*複製* と呼ばれます。キーを装置間で共用すると、Secure Sockets Layer (SSL) ロード・バランシングの使用が可能となり、セキュア・セッションのパフォーマンスが改善されます。

「**キー保管場所の選択 (Select a Key Storage Location)**」ページで以下のステップに従い、コプロセッサー・マスター・キーを使用して証明書の秘密鍵を暗号化し、特殊鍵ストア・ファイルに保管します。

1. 「**暗号化されたハードウェア (Hardware encrypted)**」を保管オプションとして選択します。
2. 「**続行 (Continue)**」をクリックします。「**暗号装置記述の選択 (Select a Cryptographic Device Description)**」ページが表示されます。
3. 装置のリストから、証明書の秘密鍵の暗号化に使用したい装置を選択します。
4. 「**続行 (Continue)**」をクリックします。複数のコプロセッサー装置がインストールされ、オンにされている場合は、「**追加暗号装置記述の選択 (Select Additional Cryptographic Device Descriptions)**」ページが表示されます。

   注: 複数のコプロセッサー装置がない場合は、DCM は、ユーザーが作成または更新している証明書に対する識別情報など、ユーザーが完了しようとしている作業のためのページを引き続き表示します。
5. 装置のリストから、証明書の秘密鍵を共用させたい 1 つまたは複数の装置記述の名前を選択します。

   注: 選択する装置記述は、前のページで選択した装置と同じマスター・キーを持っていなければなりません。装置上のマスター・キーが同じであることを検査するには、4758 暗号化コプロセッサー構成 Web インターフェースの「マスター・キー検査 (Master Key Verification)」タスクを使用します。コプロセッサー構成 Web インターフェースには、iSeries タスク・ページからアクセスできます。
6. 「**続行 (Continue)**」をクリックします。 DCM は、ユーザーが作成または更新している証明書に対する識別情報など、ユーザーが完了しようとしている作業のためのページを引き続き表示します。

PKIX CA の要求場所の管理

Public Key Infrastructure for X.509 (PKIX) 認証局 (CA) は、PKI (Public Key Infrastructure) をインプリメントする最新のインターネット x.509 規格に基づいて証明書を発行する CA です。 PKIX 規格は、Request For Comments (RFC) 2560 に概説されています。

PKIX CA は、証明書を発行する前に、さらに厳格な識別を要求します。通常は、登録機関 (RA) による識別証明の提供を申請者に要求します。RA は、必要な識別証明を申請者が提示してから、申請者の識別を認証します。CA の確立したプロシージャーに合わせて、RA または申請者のいずれかが、認証済みのアプリケーション

を関連した CA に提出します。これらの標準が広く採用されるにつれ、PKIX 準拠の CA はさらに広く使用されるようになってきています。SSL で使用できるアプリケーションによってユーザーに提供される資源に、セキュリティー・ニーズ上、厳重なアクセス制御が必要な場合には、PKIX 準拠の CA を使用して検査しなければなりません。たとえば、ロータス® ドミノ™ は、共通使用に対して PKIX CA を提供します。

PKIX CA に、アプリケーションで使用する証明書を発行させるようにした場合は、ディジタル証明書マネージャー (DCM) を使用してこれらの証明書を管理することができます。DCM を使用して PKIX CA の URL を構成します。このようにすると、署名済み証明書を取得するオプションの 1 つとして PKIX CA を提供するように、ディジタル証明書マネージャー (DCM) を構成することになります。

DCM を使用して PKIX CA からの証明書を管理するには、以下のステップに従って、CA 用の場所を確保するように DCM を構成しなければなりません。

1. DCM を開始します。
2. ナビゲーション・フレームの中で、「**PKIX 要求場所の管理 (Manage PKIX Request Location)**」を選択して、PKIX CA またはその関連した RA に対する URL の指定を行うためのフォームを表示します。
3. 証明書の要求に使用したい PKIX CA に対する完全修飾 URL、たとえば、`http://www.thawte.com` を入力し、「**追加 (Add)**」をクリックします。URL を追加すると、DCM を構成する際、署名済み証明書を取得するオプションの 1 つとして、PKIX CA が追加されます。

PKIX CA 要求場所を追加した後、DCM は、「**証明書の作成 (Create Certificate)**」タスクの使用時に、証明書の発行のために選択できる CA タイプを指定するオプションの 1 つとして PKIX CA を追加します。

オブジェクトへの署名

オブジェクトに署名する方法は 3 つあります。 Sign Object API を呼び出すプログラムを作成します。 ディジタル証明書マネージャー (DCM) を使用してオブジェクトに署名することができます。また、V5R2 より、他の iSeries システムに配布するためにパッケージする時点で、iSeries ナビゲーターのマネージメント・セントラル・フィーチャーを使用してオブジェクトに署名することも可能となりました。

ライブラリーに保管されているオブジェクトを除く DCM 管理の証明書を使用して、システムの統合ファイル・システムに保管している任意のオブジェクトに署名することができます。署名できるのは、QSYS.LIB ファイル・システムに保管されている、*PGM、*SRVPGM、*MODULE、*SQLPKG および *FILE (保管ファイルのみ) などのオブジェクトのみです。 V5R2 より、コマンド (*CMD) オブジェクトにも署名することが可能となりました。他の iSeries サーバーに保管されているオブジェクトに署名することはできません。

公開インターネット認証局 (CA) で購入する証明書、または DCM で専用、ローカル CA を使用して作成する証明書を使って、オブジェクトに署名することができます。証明書の署名のプロセスは、公開証明書または専用証明書のいずれを使用していても同じです。

オブジェクト署名の前提条件

DCM (または Sign Object API) を使用してオブジェクトに署名できるようにするには、以下のような一定の前提条件が満たされていなければなりません。

- ローカル CA の作成プロセスの一部、または公開インターネット CA のオブジェクト署名証明書の管理プロセスの一部として、*OBJECTSIGNING 証明書ストアを作成していなければなりません。
- *OBJECTSIGNING 証明書ストアには、少なくとも 1 つの証明書 (ローカル CA を使用して作成したものか、公開インターネット CA から取得したもののいずれか) が含まれていなければなりません。
- オブジェクトへの署名に使用するためには、オブジェクト署名アプリケーション定義を作成しておかなければなりません。
- オブジェクトに署名するために使用する予定のオブジェクト署名アプリケーションには、証明書を割り当てておかなければなりません。

DCM を使用してオブジェクトに署名

DCM を使用してオブジェクト (複数可) に署名するには、以下のステップに従ってください。

1. DCM を開始します。

   注: DCM を使用する際に特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択して、オンライン・ヘルプを利用してください。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
3. *OBJECTSIGNING 証明書ストアにパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**署名可能なオブジェクトの管理 (Manage Signable Objects)**」を選択して、タスクのリストを表示します。
5. タスクのリストから「**オブジェクトに署名 (Sign an object)**」を選択して、オブジェクトに署名するために使用できるアプリケーション定義のリストを表示します。
6. アプリケーションを選択して、「**オブジェクトに署名 (Sign an object)**」をクリックし、署名したいオブジェクトの位置を指定するフォームを表示します。

   注: 選択するアプリケーションに証明書が割り当てられていない場合は、それを使用してオブジェクトに署名することはできません。アプリケーション定義に証明書を割り当てるには、「**アプリケーションの管理 (Manage Applications)**」の下にある、「**証明書割り当ての更新 (Update certificate assignment)**」タスクを最初に使用しなければなりません。
7. 表示されたフィールドに、署名対象のオブジェクトの完全修飾パスとファイル名、つまりオブジェクトのディレクトリーを入力して、「**続行 (Continue)**」をクリックします。あるいは、ディレクトリー位置を入力して、「**ブラウズ (Browse)**」をクリックし、ディレクトリーの内容を表示して、署名対象のオブジェクトを選択します。

   注: オブジェクト名は、スラッシュで始めなければなりません。そうしないと、エラーになる場合があります。特定のワイルドカード文字を使用して、署名したいディレクトリーの一部を表現することもできます。このようなワイル

ドカード文字には、「任意の数の文字列」を示すアスタリスク (*)、および「任意の単一文字」を示す疑問符 (?) があります。たとえば、特定のディレクトリーのすべてのオブジェクトに署名する場合は、/mydirectory/* と入力し、特定のライブラリー内のすべてのプログラムに署名する場合は、/QSYS.LIB/QGPL.LIB/*.PGM と入力することができます。これらのワイルドカードが使用できるのは、パス名の最後の部分だけです。たとえば、/mydirectory*/filename と指定するとエラー・メッセージが戻されることになります。ブラウズ機能を使用して、ライブラリーまたはディレクトリーの内容のリストを表示したい場合は、パス名の一部としてワイルドカードを入力してから、「**ブラウズ (Browse)**」をクリックする必要があります。

8. 選択した 1 つまたは複数のオブジェクトに署名するために使用する処理オプションを選択して、「**続行 (Continue)**」をクリックします。

   注: ジョブ結果を待つように選択すると、結果ファイルがブラウザーに直接表示されます。現行ジョブの結果は、結果ファイルの最後に追加されます。したがって、このファイルには、現行ジョブの結果だけでなく、これまでのすべてのジョブの結果が含まれている可能性があります。ファイルの日付フィールドを使用して、現行ジョブには、ファイル内の何行目が割り当てられているのか判別することができます。日付フィールドは YYYYMMDD 書式で表されます。ファイルの最初のフィールドは、メッセージ ID (オブジェクトの処理中にエラーが発生した場合) または日付フィールド (ジョブの処理された日付を示す) のいずれかです。

9. オブジェクト署名操作のジョブ結果を保管するために使用する完全修飾パスおよびファイル名を指定し、「**続行 (Continue)**」をクリックします。あるいは、ディレクトリー位置を入力して、「**ブラウズ (Browse)**」をクリックし、ディレクトリーの内容を表示して、ジョブ結果を保管するファイルを選択します。オブジェクトに署名するジョブがサブミットされたことを示すメッセージが表示されます。ジョブ結果を表示するには、ジョブ・ログの **QOBJSGNBAT** ジョブを参照してください。

オブジェクトの署名検査

ディジタル証明書マネージャー (DCM) を使用すると、オブジェクトのディジタル署名の認証性を検査することができます。署名を検査することで、オブジェクト所有者がオブジェクトに署名して以降、オブジェクト内のデータが変更されていないことを確認できます。

署名検査の前提条件

DCM を使用してオブジェクトの署名を検査できるようにするには、以下のような一定の前提条件が満たされていなければなりません。

- 署名検査証明書を管理するには、*SIGNATUREVERIFICATION 証明書ストアを作成しておかなければなりません。

  注: 同じシステムで署名されたオブジェクトの署名を検査する場合、*OBJECTSIGNING 証明書ストア内での処理中に署名検査を実行することができます。DCM で署名の検査を実行するステップは、証明書ストアの場合と同じです。ただし、*OBJECTSIGNING 証明書ストア内での処理中に署名検査を

実行する場合でも、*SIGNATUREVERIFICATION 証明書ストアが存在し、オブジェクトに署名した証明書のコピーを含んでいなければなりません。

- *SIGNATUREVERIFICATION 証明書ストアには、オブジェクトに署名した証明書のコピーが含まれていなければなりません。
- *SIGNATUREVERIFICATION 証明書ストアには、オブジェクトに署名した証明書を発行した CA 証明書のコピーが含まれていなければなりません。

DCM を使用してオブジェクトの署名を検査

DCM を使用してオブジェクトの署名を検査するには、以下のステップに従ってください。

1. DCM を開始します。

   注: DCM を使用する際に特定のフォームの入力方法について不明な点がある場合は、ページの上部にある疑問符 (**?**) を選択して、オンライン・ヘルプを利用してください。
2. ナビゲーション・フレームで「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
3. *SIGNATUREVERIFICATION 証明書ストアにパスワードを入力して、「**続行 (Continue)**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**署名可能なオブジェクトの管理 (Manage Signable Objects)**」を選択して、タスクのリストを表示します。
5. タスクのリストから、「**オブジェクトの署名検査 (Verify object signature)**」を選択して、署名検査対象のオブジェクトの位置を指定します。
6. 表示されたフィールドに、署名検査対象のオブジェクトの完全修飾パスとファイル名、つまりオブジェクトのディレクトリーを入力して、「**続行 (Continue)**」をクリックします。あるいは、ディレクトリー位置を入力して、「**ブラウズ (Browse)**」をクリックし、ディレクトリーの内容を表示して、署名検査対象のオブジェクトを選択します。

   注: 特定のワイルドカード文字を使用して、検査したいディレクトリーの一部を表現することもできます。このようなワイルドカード文字には、「任意の数の文字列」を示すアスタリスク (*****)、および「任意の単一文字」を示す疑問符 (**?**) があります。たとえば、特定のディレクトリーのすべてのオブジェクトに署名する場合は、`/mydirectory/*` と入力し、特定のライブラリー内のすべてのプログラムに署名する場合は、`/QSYS.LIB/QGPL.LIB/*.PGM` と入力することができます。これらのワイルドカードが使用できるのは、パス名の最後の部分だけです。たとえば、`/mydirectory*/filename` と指定するとエラー・メッセージが戻されることになります。ブラウズ機能を使用して、ライブラリーまたはディレクトリーの内容のリストを表示したい場合は、パス名の一部としてワイルドカードを入力してから、「**ブラウズ (Browse)**」をクリックする必要があります。
7. 選択した 1 つまたは複数のオブジェクトの署名を検査するために使用する処理オプションを選択して、「**続行 (Continue)**」をクリックします。

   注: ジョブ結果を待つように選択すると、結果ファイルがブラウザーに直接表示されます。現行ジョブの結果は、結果ファイルの最後に追加されます。したがって、このファイルには、現行ジョブの結果だけでなく、これまでのすべ

てのジョブの結果が含まれている可能性があります。ファイルの日付フィールドを使用して、現行ジョブには、ファイル内の何行目が割り当てられているのか判別することができます。日付フィールドは YYYYMMDD 書式で表されます。ファイルの最初のフィールドは、メッセージ ID (オブジェクトの処理中にエラーが発生した場合) または日付フィールド (ジョブの処理された日付を示す) のいずれかです。

8. 署名検査操作のジョブ結果を保管するために使用する完全修飾パスおよびファイル名を指定し、「**続行 (Continue)**」をクリックします。あるいは、ディレクトリー位置を入力して、「**ブラウズ (Browse)**」をクリックし、ディレクトリーの内容を表示して、ジョブ結果を保管するファイルを選択します。オブジェクトの署名を検査するジョブがサブミットされたことを示すメッセージが表示されます。ジョブ結果を表示するには、ジョブ・ログの **QOBJSGNBAT** ジョブを参照してください。

DCM を使用して、オブジェクトに署名した証明書に関する情報を表示することもできます。これにより、オブジェクトを処理する前に、オブジェクトが信頼できるソースからのものであるかどうかを判断することができます。

第 9 章 DCM に関するトラブルシューティング

以下のページには、ディジタル証明書マネージャー (DCM) での作業時に発生する可能性のある、共通的な問題の一部に関するトラブルシューティングに役立つ情報が記載されています。

問題に関する情報および考えられる解決策については、以下のページを参照してください。

パスワードおよび汎用的な問題のトラブルシューティング
このトピックでは、発生する可能性のある一般的な DCM ユーザー・インターフェースの問題、およびそれらの訂正方法について学ぶことができます。

証明書ストアおよびキー・データベースの問題のトラブルシューティング
このトピックでは、発生する可能性のある一般的な証明書ストアおよびキー・データベースの問題、およびそれらの訂正方法について学ぶことができます。

ブラウザーの問題のトラブルシューティング
このトピックでは、ブラウザーを使用して DCM にアクセスする際に発生する可能性のある一般的な問題、およびそれらの訂正方法について学ぶことができます。

HTTP Server for iSeries の問題のトラブルシューティング
このトピックでは、発生する可能性のある一般的な HTTP Server の問題、およびそれらの訂正方法について学ぶことができます。

マイグレーション・エラーおよび回復方法
このトピックでは、DCM を前のリリースからマイグレーションする際に発生する可能性のある一般的な問題、およびそれらの訂正方法について学ぶことができます。

ユーザー証明書の割り当てに関するトラブルシューティング
このトピックでは、DCM を使用してユーザー証明書を登録する際に発生する可能性のある一般的な問題、およびそれらの訂正方法について学ぶことができます。

パスワードおよび汎用的な問題のトラブルシューティング

ディジタル証明書マネージャー (DCM) での作業時に共通して発生する、パスワードその他の一般的な問題のいくつかをトラブルシューティングする際に役立つ情報については、以下の表を参照してください。

問題	可能な解決方法
DCM の追加ヘルプが見つからない。	DCM の "**?**" ヘルプ・アイコンをクリックします。Information Center およびインターネット上の外部のサイトを検索することもできます。
証明書ストアをオープンしようとすると、NET.DATA エラーを受け取る。	「**証明書ストアの選択 (Select a Certificate Store)**」を行うとき、キーボード上の**実行**キーを使用しないで、マウスを使って「**続行 (Continue)**」ボタンを選択します。
ローカル認証局 (CA) に対するパスワードおよび *SYSTEM 証明書ストアが機能しない。	パスワードは大文字小文字を区別します。大文字小文字の区別が、パスワードの割り当て時と同じ状態であることを確認してください。

問題	可能な解決方法
「証明書ストアの選択 (Select a Certificate Store)」タスクで使用したパスワードのリセットに失敗した。	リセット機能は、DCM がパスワードを保管した場合にのみ機能します。証明書ストアを作成すると、DCM はパスワードを自動的に保管します。ただし、「他のシステム証明書ストア (Other System Certificate Store)」のパスワードを変更 (リセット) した場合には、DCM で引き続きそのパスワードを隠しておくために、「**自動ログイン (Automatic login)**」オプションを選択する必要があります。
	また、あるシステムから別のシステムに証明書ストアを移動した場合には、新しいシステムで証明書ストア用のパスワードを変更して、DCM にそのパスワードを自動的に隠すようにさせる必要があります。パスワードを変更するためには、新規システムで証明書ストアを開く際に、その証明書ストア用の元のパスワードを入力する必要があります。元のパスワードを使用してストアを開き、パスワードを変更してそれを隠すようにするまでは、パスワード・リセット・オプションを使用することはできません。パスワードが変更されずに隠されている場合、DCM および SSL は、さまざまな機能でパスワードが必要なときに、パスワードを自動的に回復することができません。「他のシステム証明書ストア (Other System Certificate Store)」として使用する予定の証明書ストアを移動させる場合には、パスワードを変更する際に「**自動ログイン (Automatic login)**」オプションを選択して、DCM がこのタイプの証明書ストア用の新規パスワードを隠しておくようにしなければなりません。
	システム・サービス・ツール (SST) の「システム・セキュリティーの処理 (Work with system security)」オプションの下で「新規ディジタル証明書の許可 (Allow new digital certificates)」属性に割り当てられている値を調べてください。この属性の値が 2 (いいえ) に設定されている場合、証明書ストアのパスワードをリセットすることはできません。この属性の値は、STRSST コマンドを使用し、サービス・ツールのユーザー ID とパスワードを入力することにより、表示または変更できます。そのうえで、「システム・セキュリティーの処理 (Work with system security)」オプションを選択してください。サービス・ツールのユーザー ID は、おそらく QSECOFR のユーザー ID です。
iSeries システムで受信する CA 証明書のソースが見つからない。	CA の中には、CA 証明書を安易に提供しないところもあります。CA から CA 証明書が受け取れない場合は、VAR に問い合わせてください。VAR が CA に特別な、または金銭上の調整を加えている場合があります。
*SYSTEM 証明書ストアが見つからない。	*SYSTEM 証明書のファイルの位置は、`/qibm/userdata/icss/cert/server/default.kdb` でなければなりません。証明書ストアが存在しない場合は、DCM を使用してこれを作成する必要があります。「**新規証明書ストアの作成 (Create New Certificate Store)**」タスクを使用します。
DCM からエラーを受け取り、エラーの修正後もエラーが表示される。	ブラウザーのキャッシュをクリアします。キャッシュ・サイズを 0 に設定して、ブラウザーを終了、再始動します。

問題	可能な解決方法
証明書の割り当て後に、セキュア・アプリケーションに関する情報が表示される際に、証明書割り当てが表示されないなど、LDAP サーバーの問題が発生する。この問題は、iSeries ナビゲーターを使用して Netscape Communications 社のブラウザーを使用するとよく起こります。ブラウザー・キャッシュの設定で、キャッシュ内の文書をネットワーク上の文書と「セッションごとに 1 回ずつ (Once per session)」比較するようになっています。	デフォルト設定を、毎回キャッシュをチェックするよう変更します。
DCM を使用して、Entrust などの外部 CA が署名した証明書をインポートすると、「有効期限外または発行者の有効期限外 (The validity period does not contain today or does not fall within its issuer's validity period)」というエラー・メッセージを受け取る。	システムは、有効期限に汎用の時刻形式を使用しています。一日おいて、再度試行します。また、iSeries UTC オフセット値 (`dspsysval qutcoffset`) が正しいことを確認します。夏時間の場合、オフセットの設定が正しくない場合があります。
Entrust の証明書のインポート時に、ベース 64 エラーが発生する。	証明書が、PEM 形式など特定の形式としてリストされています。ブラウザーのコピー機能が正しく機能せず、証明書とは関係のない特殊なマテリアル (各行先頭のブランク・スペースなど) がコピーされてしまうと、証明書は iSeries で使用する際に正しい形式になりません。Web ページの設計によっては、このような問題が発生します。この問題を避けるよう設計されている Web ページもあります。オリジナルの証明書と、貼り付けた結果を比較して、貼り付けた情報が同様の表示となるように確認してください。
V4R3 バージョンの DCM から V5R2 バージョンにマイグレーションする際に、有効期限切れのシステム証明書が受け入れられない。	有効期限が切れたシステム証明書が問題となっており、*SYSTEM 証明書ストアには入れられません。マイグレーションする前に、V4R3 以前のキー・リンク・ファイルを削除または名前を変更するか、マイグレーションが失敗したことを示すメッセージを無視するか、または再度マイグレーションを行ってください。
妥当性検査リストに追加する証明書のサンプル・コードが見つからない。	サンプル・コードは、まだ使用できません。

証明書ストアおよびキー・データベースの問題のトラブルシューティング

ディジタル証明書マネージャー (DCM) での作業時に共通して発生する、証明書ストアおよびキー・データベースの問題のいくつかをトラブルシューティングする際に役立つ情報については、以下の表を参照してください。

問題	可能な解決方法
システムがキー・データベースを検出しない、またはキー・データベースが無効である。	パスワードおよびファイル名にタイプミスがないか確認してください。ファイル名には、先頭のスラッシュおよびパスが含まれていることを確認してください。
キー・データベースの作成が失敗する。	ファイル名に競合がないか確認してください。要求したファイルとは異なるファイルと競合している場合があります。

問題	可能な解決方法
他のシステムからバイナリー・モードで転送された CA テキスト・ファイルを、システムが受け入れない。ASCII 形式で転送したファイルは受け入れる。	キー・リングおよびキー・データベースはバイナリーであるため、CA テキスト・ファイルとは異なります。CA テキスト・ファイルについては、ファイル転送プロトコル (FTP) を ASCII モードで使用し、.kdb、.kyr、.sth、.rdb などのバイナリー・ファイルには FTP をバイナリー・モードで使用します。
キー・データベースのパスワードが変更できない。キー・データベースの証明書が無効である。	パスワードに誤りがないことを確認した後、証明書ストアから無効な証明書を見付けて削除し、パスワードを変更してみてください。証明書ストア内に有効期限が切れている証明書がある場合は、有効期限切れ証明書は無効となります。証明書が無効なので、証明書ストアのパスワード変更機能でパスワードが変更できず、暗号化プロセスでは、有効期限の切れた証明書の秘密鍵を暗号化できません。これによりパスワードの変更ができず、システムは理由の 1 つとして証明書ストアの破壊を報告する場合があります。無効な (有効期限が切れた) 証明書を証明書ストアから削除してください。
インターネット・ユーザーに対して証明書を使用するため妥当性検査リストを使用する必要があるが、DCM に妥当性検査リストの機能がない。	妥当性検査リストを使用するようアプリケーションを作成するビジネス・パートナーは、妥当性検査リストとそのアプリケーションを関連付けるコードを記述する必要があります。また、証明書が妥当性検査リストに追加されるよう、インターネット・ユーザーの識別をいつ検査するかを決定するコードを記述する必要もあります。 Information Center の QsyAddVldlCertificate API のトピックを参照してください。Web マスターの手引きの、妥当性検査リストを使用するためのセキュア・サーバー・インスタンスの構成のヘルプを参照してください。

ブラウザーの問題のトラブルシューティング

ディジタル証明書マネージャー (DCM) での作業時に発生する問題のうち、比較的一般的と思われるブラウザーに関連した問題のトラブルシューティングに役立つ情報については、以下の表を参照してください。

問題	可能な解決方法
Microsoft® Internet Explorer を使用した際、新規ブラウザー・セッションを開始しないと、別の証明書が選択できない。	Internet Explorer の新規ブラウザー・セッションを開始してください。
Internet Explorer で、ブラウザーの選択リストにすべての選択可能なクライアント / ユーザー証明書が表示されない。 Internet Explorer は、トラステッド CA が発行する、セキュア・サイトで使用可能な証明書のみを表示します。	CA は、キー・データベースにおいて、またセキュア・アプリケーションにより承認されている必要があります。Internet Explorer を使用する PC に、ブラウザーにユーザー証明書を配置したユーザー名と同じユーザー名でサインオンをしたか確認してください。アクセス先のシステムから、別のユーザー証明書を取得します。システム管理者は、証明書ストア (キー・データベース) が、ユーザーおよびシステム証明書に署名をした CA を承認していることを確認する必要があります。

問題	可能な解決方法
Internet Explorer 5 が CA 証明書を受信したが、ファイルをオープンできないか、証明書を保管したディスクを見付けることができない。	これは、Internet Explorer ブラウザーに承認されていない、証明書に対するこのブラウザーの新規機能です。PC 上の位置を選択することができます。
システム名とシステム証明書が一致しないことを示す警告が表示される。	システム名の大文字小文字の区別について、ブラウザーにより反応が異なります。システム証明書と同じ文字で URL を入力します。または、ほとんどのユーザーが使用すると思われる大文字小文字の区別によりシステム証明書を作成します。どうしたらよいか分からなければ、サーバー名またはシステム名はそのままにしておくのが得策です。また、ドメイン・ネーム・サーバーが正しく設定されていることを確認してください。
HTTP ではなく HTTPS で Internet Explorer を開始し、セキュアおよび非セキュア・セッションの混合を示す警告が表示される。	警告を受け入れ、無視します。 Internet Explorer の今後のリリースで、この問題は修正されます。
Windows® 版 Netscape Communicator 4.04 が、 16 進数値 A1 および B1 をポーランド語コード・ページの B2 および 9A に変換する。	これは NLS に影響を与えるブラウザーのバグです。別のブラウザーを使用するか、AIX® 版 Netscape 4.04 など異なるプラットフォームで同じバージョンのブラウザーを使用してください。
ユーザー・プロファイルで、Netscape Communicator 4.04 は大文字のユーザー証明書 NLS 文字は正しく表示するが、小文字を正しく表示しない。	各国語文字のなかには、1 文字として正しく入力されても、後でブラウザーに表示した場合に、同じ文字とならないものがあります。たとえば、Windows 版の Netscape Communicator 4.04 では、16 進数値 A1 および B1 はポーランド語コード・ページの B2 および 9A に変換され、異なる NLS 文字が表示されます。
ブラウザーがエンド・ユーザーに対し、CA が未承認であると表示する。	DCM を使用して、「**CA 状況 (CA status)**」を使用可能に設定し、CA にトラステッドのマークを付けてください。
Internet Explorer が、HTTPS 接続を拒否する。	これは、ブラウザー機能またはその構成の問題です。ブラウザーが、自己署名されたか、またはその他の理由で無効の可能性があるシステム証明書を使用するサイトには接続しないように設定されています。
Netscape Communicator ブラウザーおよびサーバー製品が、SSL 通信、特に認証の使用可能化フィーチャーとして、VeriSign などの会社からのルート証明書を採用している。すべてのルート証明書は、定期的に有効期限が切れます。Netscape ブラウザーおよびサーバー・ルート証明書のなかには、1999 年 12 月 25 日から 1999 年 12 月 31 日の間に有効期限が切れたものがあります。この問題を 1999 年 12 月 14 日以前に修正していない場合は、エラー・メッセージを受け取ります。	ブラウザーの以前のバージョン (Netscape Communicator 4.05 以前) は、有効期限が切れる証明書を持っています。ブラウザーを現行バージョンの Netscape Communicator にアップグレードする必要があります。ブラウザーのルート証明書に関する情報は、`http://home.netscape.com/security/` および `http://www.verisign.com/server/cus/rootcert /webmaster.html` を含め、多くのサイトで入手できます。ブラウザーの無料ダウンロードは、`http://www.netcenter.com` から行うことができます。

HTTP Server for iSeries の問題のトラブルシューティング

ディジタル証明書マネージャー (DCM) での作業時に共通して発生する、HTTP Server for iSeries の問題のいくつかをトラブルシューティングする際に役立つ情報については、以下の表を参照してください。

問題	可能な解決方法
Hypertext Transfer Protocol Secure (HTTPS) が機能しない。	HTTP Server が SSL を使用できるように正しく構成されていることを確認してください。V5R1 以降のバージョンでは、構成ファイルは、HTTP Server のグラフィカル・ユーザー・インターフェース (GUI) を使用して、**SSLAppName** を設定する必要があります。また、この構成では、SSL ポートを使用する仮想ホストを構成して、その仮想ホスト内部で **SSLEnable** に設定しておかなければなりません。さらに、SSL 用と非 SSL 用に 2 つの異なるポートを指定した、2 つの Listen ディレクティブも必要です。サーバー・インスタンスが作成されており、サーバー証明書が署名されていることを確認してください。
セキュア・アプリケーションとして HTTP Server インスタンスを登録する処理の説明が必要である。	iSeries システムで、HTTP Server の Web インターフェースに移動して、HTTP Server の構成を設定してください。最初に、SSL を使用可能にするために仮想ホストを定義しなければなりません。これは「コンテキスト管理 (Context Management)」画面で行います。仮想ホストは、すでに Listen ディレクティブで定義された SSL ポートを使用するように定義されていなければなりません。次に、「SSL 一般設定値 (SSL General Settings)」画面を使用して、すでに構成されている仮想ホストで SSL をオンにする必要があります。すべての変更内容を構成ファイルに適用しなければなりません。インスタンスを登録しても、そのインスタンスの使用する証明書が自動的に選択されるわけではない点に、注意してください。サーバー・インスタンスを終了して再始動する前に、DCM を使用して特定の証明書をアプリケーションに割り当てる必要があります。
妥当性検査リストおよびオプションのクライアント認証に HTTP Server を設定できない。	HTTP Server の Web マスターの手引きのインスタンスの設定オプションを参照してください。この情報は、Information Center の『Web サービス提供』というトピックにも記載されています。
Netscape Communicator が、HTTP Server コードの構成ディレクティブの有効期限が切れるのを待ってから別の証明書の選択を許可する。	証明書の値が大きいと、ブラウザーが最初の証明書を使用しているため、次の証明書の登録が困難になります。
ブラウザーが HTTP Server に X.509 証明書を提示するようにして、証明書を QsyAddVldlCertificate API への入力に使用しようとした。	HTTP Server が HTTPS_CLIENT_CERTIFICATE 環境変数をロードするようにするには、**SSLEnable** および **SSLClientAuth ON** を使用する必要があります。これらの API は、Information Center の『OS/400 API』トピックに記載されています。以下の妥当性検査リストまたは証明書関連の API も必要に応じて参照してください。 • QsyListVldlCertificates および QSYLSTVC • QsyRemoveVldlCertificate および QRMVVC • QsyCheckVldlCertificate および QSYCHKVC • QsyParseCertificate および QSYPARSC など

問題	可能な解決方法
HTTP Server のインストール時に作成された要求ファイルが見つからない。このファイルは、システムが、そのディレクトリー内の構成ファイルにある KEYFILE ディレクティブ上にある有効なキー・リング・ファイルを指示するために使用されます。	詳細については、『以前のリリースからの DCM のマイグレーション』を参照してください。 HTTP Server では、正しいファイルは、/qibm/userdata/httpsvr/keyring/keymreq.crt です。LDAP では、正しいファイルは、/qibm/userdata/os400/dirsrv/qdirsrv.crt です。
妥当性検査リストで証明書のリストを要求し、10,000 以上の項目がある場合、HTTP Server から戻るまでに時間がかかり過ぎるか、タイムアウトになる。	有効期限が切れた、または特定の CA の証明書すべてなど、特定の基準に一致する証明書を検出して削除するようバッチ・ジョブを作成してください。
V4R3 のリリース上に V5R2 をインストールした後、証明書ストアに問題が起こり、/qibm/userdata/httpsvr/keyring/keymreq.crt または /qibm/usedata/os400/dirsrv/qdirsrv.crt ファイルが存在する。システムが、キー・リングからキー・データベースへの自動マイグレーションを完了できない。	以前のキー・リング・ファイルを証明書ストアとして指定し、キー・リングから無効な証明書を見付けて削除してから、qicss/qyepmgrt を呼び出して再度マイグレーションを行ってください。または、マイグレーションにより重要な証明書がすべて移動されていれば、.crt ファイルを無視するか、削除してください。
SSLEnable が設定された状態で HTTP Server が正常に開始されず、ジョブ・ログにエラー・メッセージ HTP8351 が表示される。 *ADMIN サーバーのエラー・ログに、HTTP Server が失敗した際に SSL 初期化操作が戻りコード・エラー 107 で失敗した、というエラーが示される。	エラー 107 は、証明書の有効期限が切れたことを意味します。 サーバー・インスタンスが *ADMIN サーバーであれば、一時的に **SSLDisable** を設定して、*ADMIN サーバーで DCM を使用できるようにします。 DCM を使用して、別の証明書をアプリケーションに割り当てます。たとえば、サーバー・インスタンスが *ADMIN サーバーの場合、QIBM_HTTP_SERVER_ADMIN とします。

マイグレーション・エラーおよび回復方法

エラーとエラー回復

次の標識は、マイグレーション時に発生した可能性のあるエラーを通知するものです。

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
オプション 34 と 5722-DG1 を正常にインストールしたあとでこの標識が表示された場合は、5722-DG1 が実行しようとしたキー・リングのマイグレーションが正常に処理されなかったことを意味します。 *SYSTEM 証明書ストアにキー・リングのマイグレーションをする必要のある場合があります。

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
オプション 34 を正常にインストールしたあとでこの標識が表示された場合は、LDAP サーバーのためのキー・リングのマイグレーションが正常に行われなかったことを意味します。

表示されるエラーに加えて、システムが表示しない、マイグレーションが原因と考えられるエラーがあります。たとえば、システムが、*SYSTEM 証明書ストアにマイグレーションする必要があるキー・リングを見付けたときに、既存の統合ファイル・システムのユーザー・データ・ファイルとの競合も検出することがあります。そのようなインスタンスでは、インストールが正常に完了しても、システムがキー・リングのマイグレーションを完了しないことがあります。

まれに、キー・リングのマイグレーションの完了後、システム証明書の割り当てを行っている途中で、エラーによってマイグレーションの完了が妨げられることもあります。この結果、SSLMODE が ON である場合に IBM HTTP Server の *ADMIN インスタンスを開始すると、エラーとなることがあります。考えられる原因は次のとおりです。

- マイグレーションしたキー・リング・ファイルが、デフォルトとして不適切なシステム証明書セットを保持している。
- DCM が、クリティカル・ファイル名ですでに存在していたユーザー・データを保存してマイグレーションを終了した。
- マイグレーション・コードに予期しないエラーが発生した。

IBM HTTP Server は、SSLMODE が ON でなくても、*ADMIN インスタンスを開始する前に、一時的に *ADMIN インスタンスの SSLMODE を OFF にすることによって始動できます。これにより、DCM を使って証明書ストアを調査し、*ADMIN インスタンスを終了する前に問題を解決できます。*ADMIN インスタンスを終了したら、SSLMODE を ON に戻し、*ADMIN インスタンスを開始して、SSL を正しく初期設定します。

オプション 34 のマイグレーション後、証明書ストアを使用するという通常の DCM 要求時にエラーが発生することがあります。このようなエラーは、ブラウザー上で発生します。そのようなエラーには、以下のようなものがあります。

```
Database error
Database Read error
Database Write error
Database corruption
Database table corrupted
```

さらに、システム上で、default.kdb という名前の無効な証明書ストア・ファイルが /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR または /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR と同じディレクトリーに存在することがあります。この場合は、DCM を使って新しい証明書を作成する前に、次に示す手動マイグレーションを行う必要があります。

注: キー・リング・ファイルをマイグレーションしないで、新しい CA とシステム証明書を作成する場合は、次の手動によるマイグレーションの手順は無視してください。

- HTTP Server for iSeries (5722-DG1) をインストールする予定の場合は、先に進む前に、ここでインストールしてください。

  注:

  1. 5722-SS1 オプション 34 インストール・コードは、オプション 34 のインストールのあとでは、再度マイグレーションを実行することはありません。オプション 34 のみを再インストールしても、解決しません。
  2. 当該ファイルは、PUBLIC *EXCLUDE 権限で作成されたユーザー・データ・ディレクトリーにあります。それらに正しく許可を与えたことを確認してください。
- 次のファイルが存在するかどうかを確認してください。
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

存在する場合は、WRKLNK コマンドを使って、名前変更し、バックアップを作成します。

- *ALLOBJ 権限のあるユーザー・プロファイルから、次のようにコマンド行でプログラム QICSS/QYEPMGRT を呼び出してください。

  ```
  CALL QICSS/QYEPMGRT
  ```

  結果が正常である場合は、次のファイルがいずれもシステムに存在しないことを確認します。

  – /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  – /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

通常、DCM は、ファイル名が DCM が使用するファイル名と対立するファイルに保存するユーザー・データのバックアップ・コピーを保持します。次のファイルが存在しないとします。

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR

しかし、次のファイルは存在するとします。

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH

この場合は、システムが .OLD 拡張子を付けてファイルの名前を変更します。.OLD ファイルもすでに存在する場合は、システムはバックアップ・コピーを作成しません。代わりに、既存の .STH ファイルが上書きされます。

その他

CA とシステム証明書を作成しようとしても、ファイル名の競合が繰り返し起こる場合は、次のいずれかの状態になる可能性があります。

- **異なるファイル名の競合** - DCM では、ディレクトリー内に作成したユーザー・データを保護しようとします。ユーザー・データの入っているこれらのファイルが、DCM で必要とされるファイルを DCM で作成するのを妨げようとする場合であっても、このユーザー・データを保護しようとします。これは、すべての競合するファイルを別のディレクトリーにコピーすることによって解決し、可能であれば、DCM 機能を使って対応するファイルを削除します。DCM を使ってファイルの削除ができない場合は、DCM と競合していたファイルが収められていた統合ファイル・システムの元のディレクトリーから、ファイルを手動で削除します。どのファイルを移動し、どこに移動したかを正確に記録しておいてください。コピーしておくと、ファイルが必要になったときに、ファイルを復元することができます。次のファイルを移動した後で、新しい CA を作成する必要があります。

  ```
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
  ```

```
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
```

次のファイルを移動した後で、新しい *SYSTEM 証明書ストアとシステム証明書を作成する必要があります。

```
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP
```

- **前提条件の欠落** - 前提条件のライセンス・プログラム (LPP) を正しくインストールしたことを確認してください。
- **コード問題** - サービス技術員に問い合わせてください。

ユーザー証明書の割り当てに関するトラブルシューティング

「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを使用すると、ディジタル証明書マネージャー (DCM) によって、証明書を登録する前に確認する証明書情報が表示されます。DCM が証明書を表示できない場合は、次のいずれかの状態が原因で問題が発生している可能性があります。

1. ブラウザーが、サーバーに提示する証明書を選択するように要求しなかった。これは、ブラウザーが (別のサーバーにアクセスすることから) 直前の証明書をキャッシュしている場合に発生する可能性があります。ブラウザーのキャッシュをクリアし、タスクを再度試行してください。ブラウザーによって、証明書を選択するように表示されます。
2. 登録する証明書が、すでに DCM に登録されている。
3. 証明書を発行した認証局が、システム上でトラステッド・ルートとして指定されていない。したがって、提示する証明書は無効になります。システム管理者に問い合わせて、証明書を発行した CA が正しいかどうかを確認してください。CA が正しい場合は、システム管理者が、CA 証明書を *SYSTEM 証明書ストアに**インポート**する必要のある場合があります。あるいは、管理者が、「**CA 証明書の処理 (Work with CA certificates)**」タスクを使って、システム上で CA をトラステッド・ルートとして使用可能にし、問題を解決する必要のある場合があります。
4. 登録する証明書がない。これが問題であるかどうかを確認するため、ブラウザーでユーザー証明書をチェックできます。

5. 登録を試行している証明書の期限が切れているか、または不完全である。証明書を更新するか、または 証明書を発行した CA に問い合わせて、問題を解決する必要があります。
6. IBM HTTP Server for iSeries が、セキュア *ADMIN サーバー・インスタンスで SSL およびクライアント認証を使用して証明書登録を実行するように正しく設定されていない。上述のトラブルシューティングのヒントがいずれも該当しない場合は、システム管理者に問い合わせて、問題を報告してください。

「**ユーザー証明書の割り当て (Assign a user certificate)**」を行うには、SSL セッションを使って、ディジタル証明書マネージャー (DCM) に接続する必要があります。SSL を使用せずに「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを選択した場合、DCM によって、SSL を使用するように求めるメッセージが表示されます。このメッセージには、SSL を使って DCM に接続できるボタンが含まれています。メッセージにボタンが表示されない場合は、その問題をシステム管理者に報告してください。SSL 使用の構成ディレクティブを有効にするために、Web サーバーを再始動しなければならない場合があります。

第 10 章 DCM の関連情報

ディジタル証明書が広く使用されるようになるに従い、情報もさらに入手しやすくなりました。ディジタル証明書の詳細と、それらを使用して iSeries セキュリティー・ポリシーを強化する方法を学ぶために役立つその他のトピックのいくつかを以下に記載します。

- **VeriSign Help Desk Web サイト**
  VeriSign Web サイトは、他のインターネット・セキュリティー問題と同様に、ディジタル証明書のトピックに関する幅広いライブラリーを提供しています。
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  この IBM レッドブックは、V5R1 におけるネットワーク・セキュリティーの機能強化を中心に説明しています。このレッドブックは、iSeries のオブジェクト署名機能、ディジタル証明書マネージャー (DCM)、4758 Cryptographic Coprocessor support for SSL などの使用方法を含む、多くのトピックを扱っています。
- **AS/400® Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  このレッドブックは、iSeries サーバーでディジタル証明書を使用して行うことのできる内容について説明しています。また、証明書を使用するさまざまなサーバーやクライアントでのセットアップの方法について説明しています。さらに、OS/400 API を使用してディジタル証明書をユーザー・アプリケーションで管理および使用するための情報とサンプル・コードを提供しています。
- **RFC Index Search**
  この Web サイトは Request for Comments (RFC) の検索可能なリポジトリーを提供しています。 RFC は、ディジタル証明書の使用に関係のある、SSL、PKIX、およびその他のインターネット・プロトコルに関する規格を説明しています。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12