IBM i

バージョン 7.2

セキュリティー
ディジタル証明書マネージャー

IBM i

バージョン 7.2

セキュリティー
ディジタル証明書マネージャー

ご注意

本書および本書で紹介する製品をご使用になる前に、 105 ページの『特記事項』に記載されている情報をお読みください。

本製品およびオプションに付属の電源コードは、他の電気機器で使用しないでください。

本書にはライセンス内部コードについての参照が含まれている場合があります。ライセンス内部コードは機械コードであり、IBM 機械コードのご使用条件に基づいて使用権を許諾するものです。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM i
Version 7.2
Security
Digital Certificate Manager

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2014.4

目次

ディジタル証明書マネージャー 1
IBM i 7.2 の新機能 1
DCM の PDF ファイル 2
DCM の概念 2
証明書の拡張 3
証明書の更新 3
識別名 4
ディジタル署名 4
公開鍵と秘密鍵のペア 6
証明書アルゴリズム 6
認証局 7
証明書取り消しリストの位置 8
証明書ストア 9
暗号 10
IBM i 用 IBM 暗号化コプロセッサー 11
アプリケーション定義 11
妥当性検査 13
シナリオ: DCM 14
シナリオ : 証明書を使用して外部の認証を行う 14
計画ワークシートを完成させる 18
サーバーまたはクライアント証明書要求を作成する 19
SSL を使用するようにアプリケーションを構成する 20
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 20
アプリケーションを SSL モードで開始する 21
(オプション): アプリケーションに必要な CA 信頼リストを定義する 21
シナリオ : 証明書を使用して内部の認証を行う 22
計画ワークシートを完成させる 25
SSL を使用するように人事 HTTP Server を構成する 27
ローカル CA の作成および運用 28
人事 Web サーバー用のクライアント認証を構成する 29
人事 Web サーバーを SSL モードで開始する 30
ブラウザーでのローカル CA 証明書のコピーのインストール 30
ローカル CA からの証明書を要求する . . . 31
シナリオ: ディジタル証明書マネージャーを使用して認証局をセットアップする 31
ディジタル証明書マネージャーの計画ワークシートの作成 32
システム A でのIBM HTTP Server for i の開始 33
システム A を認証局として構成する 34
システム B 用のディジタル証明書の作成 . . 36
システム B における .KDB ファイルおよび .RDB ファイルの名前変更 36
システム B における証明書ストアのパスワードの変更 37
システム B の IBM i VPN 鍵マネージャーに対する CA 信頼の定義 38
DCM の計画 38
DCM のセットアップ要件 38
DCM データのバックアップおよび回復に関する考慮事項 38
ディジタル証明書のタイプ 39
公開証明書と秘密証明書 41
SSL セキュア通信のためのディジタル証明書 . . 43
ユーザー認証のディジタル証明書 44
ディジタル証明書とエンタープライズ識別マッピング 46
VPN 接続のディジタル証明書 47
オブジェクトに署名するためのディジタル証明書 48
オブジェクトの署名検査のためのディジタル証明書 49
DCM の構成 50
ディジタル証明書マネージャーの開始 51
証明書のはじめてのセットアップ 51
ローカル CA の作成および運用 52
ユーザー証明書の管理 55
API を使用して証明書を IBM i ユーザー以外のユーザーへプログラマチックに発行する 60
秘密 CA 証明書のコピーの取得 61
公開インターネット CA からの証明書の管理 62
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 63
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 65
オブジェクトの署名検査のための証明書の管理 67
既存の証明書の更新 69
ローカル CA から証明書を更新する 69
インターネット CA から証明書を更新する . . 70
インターネット CA から直接取得した証明書のインポートおよび更新 70
証明書の新規の公開鍵と秘密鍵のペアおよび CSR を作成することによって、証明書を更新する 70
証明書のインポート 71
DCM の管理 71
ローカル CA を使用して他の IBM i モデルの証明書を発行 71
SSL セッションのための秘密証明書の使用 . . 73
*SYSTEM 証明書ストアが存在しない場合 73
*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 . . 75

ターゲット・システムでのオブジェクト署名のための秘密証明書の使用 78
*OBJECTSIGNING 証明書ストアが存在しない場合 78
*OBJECTSIGNING 証明書ストアが存在する場合 80
DCM によるアプリケーションの管理 81
アプリケーション定義の作成 82
アプリケーションに対する証明書割り当ての管理 83
アプリケーションの CA 信頼リストの定義 . . 84
有効期限による証明書の管理 85
証明書およびアプリケーションの妥当性検査 . . 86
アプリケーションへの証明書の割り当て 87
CRL 位置の管理 88
IBM 暗号化コプロセッサー上での証明書鍵の保管 89
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 90
PKIX CA の要求場所の管理 91
ユーザー証明書の LDAP 位置の管理 91
オブジェクトへの署名 93
オブジェクトの署名検査 95
DCM のトラブルシューティング 97
パスワードおよび一般的な問題のトラブルシューティング 97
証明書ストアおよび鍵データベースの問題のトラブルシューティング 99
ブラウザーの問題のトラブルシューティング . . 100
HTTP Server for IBM i の問題のトラブルシューティング 101
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 103
DCM の関連情報 104

特記事項 105

プログラミング・インターフェース情報 107
商標 107
使用条件 107

ディジタル証明書マネージャー

ディジタル証明書マネージャー (DCM) を使用すると、ネットワークのディジタル証明書を管理したり、Secure Sockets Layer (SSL) を使用して、さまざまなアプリケーションでセキュアな通信を実行したりすることができます。

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、SSL を構成して使用するためには、ディジタル証明書が不可欠です。 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。多くの IBM® i プラットフォームおよびアプリケーション (FTP、Telnet、HTTP Server など) では、データのプライバシーを確保するために、SSL をサポートしています。

IBM i 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 と仮想プライベート・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。

無料の機能であるディジタル証明書マネージャーを使用すると、証明書の IBM i 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秘密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。

関連情報:

Secure Sockets Layer (SSL)

オブジェクト署名および署名検査

IBM i 7.2 の新機能

ディジタル証明書マネージャー (DCM) に関する新情報や大幅に変更された情報についてお読みください。

- ローカル 認証局、*SYSTEM、およびその他の鍵ストアの楕円曲線ディジタル署名アルゴリズム (ECDSA) のサポートが追加されました。詳細については、 6 ページの『証明書アルゴリズム』を参照してください。
- ローカル認証局によって使用されるメッセージ・ダイジェスト・アルゴリズムの選択のサポートが追加されました。詳細については、 6 ページの『証明書アルゴリズム』を参照してください。
- 複数のローカル認証局の作成のサポートが追加されました。詳細については、 9 ページの『証明書ストア』のトピックの『ローカル認証局』を参照してください。

- *SYSTEM 証明書ストアでの、 11 ページの『アプリケーション定義』に対する最大 4 つの証明書の割り当てのサポートが追加されました。
- いくつかのシステム SSL 属性に対する DCM アプリケーション定義の新しいサポートが追加されました。
- すべてのアプリケーション定義がクライアント認証をサポートするため、アプリケーション定義の 「**クライアント認証のサポート (Client authentication supported)**」フィールドがなくなりました。このため、アプリケーションに CA 信頼リストを定義しているときに、「**クライアント認証のサポート (Client authentication supported)**」フィールドを「はい」に設定する必要はなくなりました。

新機能および変更点の確認法

技術的な変更が行われた箇所を確認するには、以下を利用してください。
- 新機能または変更された情報の開始点を示すマーク »
- 新機能および変更された情報の終了点を示すマーク «

本リリースのその他の新規または変更された情報を探すには、ユーザーへのメモ (Memo to Users) を参照してください。

DCM の PDF ファイル

この情報の PDF ファイルを表示および印刷することができます。

この文書の PDF 版を表示またはダウンロードするには、「ディジタル証明書マネージャー」 を選択します。

PDF ファイルの保存

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. ご使用のブラウザーで PDF のリンクを右クリックする。
2. ローカルに PDF を保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Reader がシステムにインストールされている必要があります。Adobe Reader は、Adobe の Web サイト (www.adobe.com/products/acrobat/readstep.html) から無償でダウンロードすることができます。

DCM の概念

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。ディジタル証明書が提供する識別情報は、サブジェクト識別名 (subject distinguished name) として知られています。認証局 (CA) と呼ばれるトラステッド・パーティーが、ユーザーまたは組織に対して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。

また、ディジタル証明書には、公開鍵と秘密鍵のペアの一部となる公開鍵があります。さまざまなセキュリティー機能は、ディジタル証明書とそれに関連付けられた鍵のペアを使用することで実現します。ディジタル証明書を使用すると、Secure Sockets Layer (SSL) セッションを構成して、ユーザーとサーバー・アプリケーションとの間で、非公開のセキュア通信セッションを確立できます。 SSL が使用可能なアプリケーションをいくつも構成することでこのセキュリティーを拡張し、よりセキュアにユーザー認証を行うため、ユーザー名とパスワードの代わりに証明書を要求するようにすることができます。

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。

証明書の拡張

証明書の拡張は、証明書に関する追加情報を提供する情報フィールドです。

証明書の拡張は、基本となる X.509 証明書の情報標準を拡張する手段を提供します。拡張に関する情報には、証明書の識別情報を拡張するための情報や、証明書の暗号化機能に関する情報があります。

すべての証明書が拡張フィールドを使用して、識別名およびその他の情報を拡張するわけではありません。証明書が使用する拡張フィールドの数およびタイプは、証明書を発行する認証局 (CA) エンティティーによって異なります。

たとえば、ディジタル証明書マネージャー (DCM) が備えるローカル CA では、サブジェクト代替名の証明書拡張のみを使用できます。これらの拡張により、証明書を、特定の IP アドレス、完全修飾ドメイン名、または電子メール・アドレスに関連付けることができます。証明書を使用して、IBM i 仮想プライベート・ネットワーク (VPN) 接続のエンドポイントを識別しようとする場合、これらの拡張に関する情報を提供する必要があります。

関連概念:

4 ページの『識別名』
識別名 (DN) とは、証明書の識別情報を示す用語で、証明書本体の一部です。証明書には、(サブジェクト DN と呼ばれる) 証明書の所有者または要求者と、証明書を発行した CA (発行元 DN と呼ばれる) の両方に関する DN 情報が含まれています。 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。

証明書の更新

ディジタル証明書マネージャー (DCM) が使用する証明書の更新プロセスは、証明書を発行する認証局 (CA) のタイプによって異なります。

ローカル CA を使用して、更新された証明書に署名する場合、DCM は、新しい証明書を作成するためにユーザーが現行の証明書ストアに提供した情報を使用し、以前の証明書は保存します。

既知のインターネット CA を使用して証明書を発行する場合、 2 つある方法のうちの 1 つを使用して、証明書を更新することができます。1 つ目の方法は、署名する認証局から受け取るファイルから更新した証明書をインポートするやり方、 2 つ目の方法は、DCM を使用して、認証用の新しい公開鍵と秘密鍵のペアを作成するやり方です。証明書を発行した CA で直接、証明書を更新したい場合、DCM で 1 つ目のオプションを行います。

新しい鍵のペアを作成する場合、DCM は、証明書の作成を行ったときと同じ方法で更新を行います。DCM は、更新された証明書用に新しい公開鍵と秘密鍵のペアを作成し、証明書署名要求 (CSR) を生成します。CSR は、公開鍵と、新しい証明書用に指定したその他の情報で構成されています。ユーザーは、CSR を使用して、VeriSign またはその他の任意の公開 CA が発行する新しい証明書を要求できます。署名

のある証明書を CA から受け取ると、DCM を使用して、適切な証明書ストアに証明書をインポートできます。その後、証明書ストアは、オリジナルと新しく発行した更新済みの証明書両方の証明書のコピーを保管します。

DCM で新しい鍵のペアを生成することを選択しなかった場合、 DCM のガイドに従って、CA から受け取った署名付きの更新済み証明書を既存のファイルから証明書ストアにインポートする処理を行うことになります。その後、インポートされた更新済み証明書は、以前の証明書と置き換わります。

識別名

識別名 (DN) とは、証明書の識別情報を示す用語で、証明書本体の一部です。証明書には、(サブジェクト DN と呼ばれる) 証明書の所有者または要求者と、証明書を発行した CA (発行元 DN と呼ばれる) の両方に関する DN 情報が含まれています。 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。

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、使用する場合は、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。

ディジタル証明書マネージャー (DCM) を使用すると、秘密認証局を運用して、秘密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 情報と鍵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
- 市区町村
- 都道府県
- 国または地域

DCM を使用して秘密証明書を発行する場合は、証明書の拡張を使用して、次のような証明書に関する追加の DN 情報を提供できます。

- 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

関連概念:

3 ページの『証明書の拡張』
証明書の拡張は、証明書に関する追加情報を提供する情報フィールドです。

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、署名生成操作でその証明書に関連付けられた秘密鍵を使用して、オブジェクトに「署名」します。 オブジェクトの受信側では、署名の検証操作で証明書内に組み込まれた公開鍵を使用して署名を検証し、次に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、署名生成操作で認証局の秘密鍵を使用して作成されるバイナリー・データ・ストリングです。その後で、任意のユーザーが、署名の検証操作で認証局の公開鍵を使用して、証明書の署名を検証できます。

ディジタル署名は、署名の生成操作で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署名です。オブジェクト上のディジタル署名により、署名者 (署名する鍵の所有者) 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 IBM i 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、既知の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。

関連概念:

7 ページの『認証局』
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。

10 ページの『暗号』
共用鍵と公開鍵は、2 つの異なるタイプの暗号機能です。ディジタル証明書でセキュリティーを確保するために使用されます。

6 ページの『公開鍵と秘密鍵のペア』
すべてのディジタル証明書には公開鍵が含まれています。公開鍵と、それに関連付けられた秘密鍵 (証明書の一部ではない) から、鍵ペアが構成されます。これらは同時に生成され、数学的にリンクしています。作成する各証明書には、鍵ペアがあります。

公開鍵と秘密鍵のペア

すべてのディジタル証明書には公開鍵が含まれています。公開鍵と、それに関連付けられた秘密鍵 (証明書の一部ではない) から、鍵ペアが構成されます。これらは同時に生成され、数学的にリンクしています。作成する各証明書には、鍵ペアがあります。

注: 署名検査証明書は、この規則の例外です。これらは公開鍵を含んでいますが、関連する秘密鍵を持っていません。

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、鍵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、鍵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、これらの鍵を使用することにより、鍵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」することができます。署名されたオブジェクトの受信者は、署名者の証明書に含まれている公開鍵を用いて、署名を検証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。

関連概念:

4 ページの『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。

7 ページの『認証局』
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。

証明書アルゴリズム

証明書アルゴリズムは、鍵ペアの作成と、ディジタル署名の操作を実行するときに使用される、数学的な手順を記述する暗号アルゴリズムです。

楕円曲線暗号 (ECC) アルゴリズムと RSA アルゴリズムは、DCM によってサポートされる公開鍵アルゴリズムで、公開鍵と秘密鍵のペアを生成するためにいずれかを選択できます。証明書には、どの鍵アルゴリズムが使用されるかを指定する情報が含まれています。 RSA 公開鍵を含む証明書は、RSA 証明書と呼ばれることがあります。 ECC 公開鍵を含む証明書は、ECDSA (楕円曲線ディジタル署名アルゴリズム) 証明書と呼ばれます。DCM は、証明書が作成されるときに使用する公開鍵アルゴリズムを選択するオプションを提供します。

注: ECC アルゴリズムは、*SIGNING ストア内の証明書、またはユーザー証明書に対して適用されることはありません。これらは常に RSA 鍵ペアです。

公開鍵アルゴリズムとメッセージ・ダイジェスト・アルゴリズムは、ディジタル署名の生成と検証のための数学的手順を説明するものです。証明書には、公開鍵のアルゴリズムと、その証明書の署名の作成に使用されるメッセージ・ダイジェスト・アルゴリズムを指定する情報も含まれています。DCM は、署名の生成と検証で使用されるメッセージ・ダイジェスト・アルゴリズムとして SHA1、SHA224、SHA256、SHA384、および SHA512 をサポートします。また、DCM は、署名の検証でのみ、MD2 および MD5 のダイジェスト・アルゴリズムをサポートします。DCM は、証明書に署名するためにローカル CA によって公開鍵アルゴリズムと共に使用されるメッセージ・ダイジェスト・アルゴリズムを選択するオプションを提供します。このオプションは、ローカル CA 証明書が作成されたときに表示されます。

認証局

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ためには、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 のような公開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秘密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) を使用すると、公開 CA の証明書も秘密 CA の証明書も管理できます。

また、独自の秘密ローカル CA を運用して、システムやユーザーに秘密証明書を発行する場合にも、DCM は使用できます。ローカル 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 IBM i ユーザー・プロファイルまたはその他のユーザー ID に自動的に関連付けます。 DCM が証明書を、ユーザーのプロファイルに関連付けるのか、別のユーザー ID に関連付けるのかは、 DCM をエンタープライズ識別マッピング (EIM) と連携するように DCM を構成しているかによります。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、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用してローカル認証局 (CA) を作成する場合、ローカル CA のポリシー・データを指定できます。ローカル CA のポリシー・データには、その 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。

- ローカル 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
- ローカル CA で発行される証明書の有効期間

関連概念:

4 ページの『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。

6 ページの『公開鍵と秘密鍵のペア』
すべてのディジタル証明書には公開鍵が含まれています。公開鍵と、それに関連付けられた秘密鍵 (証明書の一部ではない) から、鍵ペアが構成されます。これらは同時に生成され、数学的にリンクしています。作成する各証明書には、鍵ペアがあります。

証明書取り消しリストの位置

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。

LDAP サーバーへの接続時には、LDAP サーバーに匿名でバインドすることを避けるために、DN およびパスワードを提供する必要があります。サーバーに匿名でバインドすると、「重要」属性 (CRL など) へのアクセスに必要な権限レベルが提供されません。そのような場合、DCM は CRL から正しい状況が入手できないので、取り消し状況において DCM は証明書を妥当性検査する可能性があります。LDAP サーバーに匿名でアクセスする場合は、Directory Server Web Administration Tool を使用し、「スキーマの管理」タスクを選択して **certificateRevocationList** 属性および **authorityRevocationList** 属性のセキュリティー・クラス (「アクセス・クラス」とも呼ばれる) を「重要」から「標準」に変更する必要があります。

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、仮想プライベート・ネットワーク (VPN) 接続、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。

関連概念:

86 ページの『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。

関連タスク:

88 ページの『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。

証明書ストア

証明書ストアは特殊な鍵データベース・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、ユーザーが鍵の保管に IBM 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、証明書の秘密鍵が含まれます。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統合ファイルシステム・ディレクトリー、およびその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)

DCM はこの証明書ストアを使用して、ローカル CA 証明書および関連付けられた秘密鍵を保管します。この証明書ストアのローカル CA 証明書を使用して、自分が作成する他の証明書に署名したり、他の証明書を発行したり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。複数のローカル CA を作成できます。ほかの証明書ストアのいずれかで証明書を作成する場合、その証明書に署名する CA を選択します。複数の CA を作成すると役に立つ場合があります。例えば、ECDSA 証明書を使用するようアップグレードするが、ECDSA をまだサポートしていないクライアントのために RSA 証明書も引き続き発行する必要がある場合などです。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 i アプリケーション (およびその他のさまざまなソフトウェア・デベロッパーが作成したアプリケーション) 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。DCM を使用してローカル CA を作成すると、DCM は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。 DCM を使用してローカル CA を作成すると、DCM は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。

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。「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、ユーザーまたは他の人が作成した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。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: システムに IBM 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鍵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。

関連概念:

39 ページの『ディジタル証明書のタイプ』
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、証明書ストアにある証明書と関連する秘密鍵とを、証明書のタイプを基に分類して管理します。

暗号

共用鍵と公開鍵は、2 つの異なるタイプの暗号機能です。ディジタル証明書でセキュリティーを確保するために使用されます。

暗号は、データを安全に保つ技術です。暗号を使用すると、情報を保管したり他のユーザーと通信したりする際に、保管された情報や通信の内容を無関係なユーザーに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 (鍵) 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 つの鍵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、同じ鍵を使用します。
- **公開鍵 (非対称)** 暗号方式では、暗号として相互に逆の鍵がペアで生成されます。一方の鍵は署名に使用され、もう一方は検証に使用されます。RSA の場合、一方の鍵が暗号化に使用され、データはもう一方の鍵を使用した場合にのみ回復されます。情報を送受信するユーザーは、公開鍵と秘密鍵からなる鍵のペアを持ちます。公開鍵は、通常はディジタル証明書にあり自由に配布されていますが、秘密鍵は、所有者がセキュアに保管しています。2 つの鍵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 RSA 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 RSA 秘密鍵でのみ復号することができます。また、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、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検証し、それによりオブジェクトの送信元と保全性を検証することも可能です。

関連概念:

4 ページの『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。

IBM i 用 IBM 暗号化コプロセッサー

暗号化コプロセッサーは、実績のある暗号化サービスを提供し、セキュアな e- ビジネス・アプリケーションの開発のため、プライバシーと保全性を確保します。

IBM i の IBM 暗号化コプロセッサーを使用すると、非常にセキュアな暗号処理機能がシステムに追加されます。ご使用のシステムに、暗号化コプロセッサーがインストールおよびオンに変更されている場合、暗号化コプロセッサーを使用して、証明書の秘密鍵用によりセキュアな鍵の保管場所を提供できます。

注: 暗号化コプロセッサーは、ECDSA 証明書の生成に使用できません。

また、暗号化コプロセッサーを使用して、サーバーまたはクライアント証明書、およびローカル認証局 (CA) 証明書の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、暗号化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。

証明書の秘密鍵を直接、暗号化コプロセッサーに保管することができますが、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、それを特別な鍵ファイルに保管することもできます。 これらの鍵保管オプションは、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。

暗号化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、保管場所の選択のためのオプションを提供しません。

関連概念:

89 ページの『IBM 暗号化コプロセッサー上での証明書鍵の保管』
IBM 暗号化コプロセッサーがシステムにインストールされていれば、そのコプロセッサーを使用して証明書の秘密鍵をよりセキュアに保管することができます。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。

アプリケーション定義

ディジタル証明書マネージャー (DCM) では、SSL 構成およびオブジェクト署名を使用するアプリケーション定義を管理できます。

DCM で管理できるアプリケーション定義のタイプには、以下の 2 つがあります。

- Secure Sockets Layer (SSL) 通信セッションを使用する、クライアントまたはサーバーのアプリケーション定義。

- オブジェクトの保全性を確保するためオブジェクトに署名する、オブジェクト署名のアプリケーション定義。

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 i 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。

1 つのクライアントまたはサーバー・アプリケーション ID に対して、最大 4 つの証明書を割り当てることができます。複数の証明書を割り当てると、SSL セッションの確立中にどの証明書を使用するかをシステムが判断します。証明書の選択は、ピアを使用してネゴシエーションが行われたプロトコル情報に基づきます。アプリケーションに割り当てられた複数の証明書をシステムが処理する方法について詳しくは、『複数の証明書の選択』を参照してください。

アプリケーションには、SSL プロトコル、SSL 暗号化仕様のオプション、Extended Renegotiation Critical Mode、Serve Name Indication (SNI)、SSL 署名アルゴリズムなど、SSL セッションが確立されたときにシステムで利用できる設定がいくつかあります。これらの設定の詳細については、『DCM アプリケーション定義』を参照してください。

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 アプリケーション定義と異なり、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す場合があります。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。

別のアプリケーション設定である「CA 信頼リストの定義 (Define the CA trust list)」を使用して、アプリケーションがトラステッド CA のリストを参照するか、またはアプリケーションが *SYSTEM 証明書ストア内の使用可能な状況であるすべての CA を信頼するかを決定できます。

この設定が「はい」になっている場合は、アプリケーションで *SYSTEM 証明書ストアの使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込むことができます。この値を選択した場合、アプリケーションの CA 信頼リストが定義されるまで、アプリケーションはすべての CA 証明書を信頼します。つまり、CA 信頼リストが空である場合は、この設定に「いいえ」を選択した場合と同じように動作します。

この設定が「いいえ」の場合、アプリケーションは、*SYSTEM 証明書ストアで使用可能になっている CA 証明書をすべて信頼します。

関連概念:

81 ページの『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) を使用することで、アプリケーション定義を作成したり、アプリケーションの証明書の割り当てを管理したりすることができます。また、クライアント認証用の証明書を受け入れる基礎としてアプリケーションが使用する、CA 信頼リストを定義することもできます。

関連タスク:

82 ページの『アプリケーション定義の作成』
ディジタル証明書マネージャー (DCM) では、2 つのタイプのアプリケーション定義を作成して、使用することができます。1 つは SSL を使用するサーバー・アプリケーションまたはクライアント・アプリケーション定義、もう 1 つはオブジェクトへの署名に使用するアプリケーション定義です。

妥当性検査

ディジタル証明書マネージャー (DCM) は、証明書の妥当性検査、またはアプリケーションの妥当性検査を行うタスクを備えており、証明書やアプリケーションが持つ必要があるさまざまなプロパティーの妥当性を検査できます。

証明書の妥当性検査

証明書の妥当性検査を行う際、ディジタル証明書マネージャー (DCM) は、その証明書に関連する多くの項目を検査し、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。

CRL を使用するように Lightweight Directory Access Protocol (LDAP) マッピングを構成すると、証明書が CRL にリストされていないことを確認するための証明書の妥当性検査時に、DCM が CRL を検査します。しかし、妥当性検査プロセスで CRL が正確に検査されるようにするためには、LDAP マッピング用に構成されたディレクトリー・サーバー (LDAP サーバー) に該当の CRL が入っている必要があります。そうでない場合は、証明書は正しく妥当性検査されません。取り消し状況において、証明書の妥当性検査を回避するためには、バインディング DN およびパスワードを提供する必要があります。また、LDAP マッピングの構成時に DN およびパスワードを指定しないと、LDAP サーバーに匿名でバインドされることになります。LDAP サーバーへの匿名のバインドでは、「重要」属性へのアクセスに必要な権限レベルは提供されず、CRL は「重要」属性です。そのような場合、DCM は CRL から正しい状況が入手できないので、取り消し状況において DCM は証明書を妥当性検査する可能性があります。LDAP サーバーに匿名でアクセスする場合は、Directory Server Web Administration Tool を使用し、「スキーマの管理」タスクを選択して **certificateRevocationList** 属性および **authorityRevocationList** 属性のセキュリティー・クラス (「アクセス・クラス」とも呼ばれる) を「重要」から「標準」に変更する必要があります。

また、DCM は、発行元 CA の CA 証明書が現行の証明書ストアにあり、その CA 証明書にトラステッドのマークが付いているかを確認します。証明書の秘密鍵がある場合 (たとえば、サーバーとクライアント、またはオブジェクト署名の証明書)、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。つまり、DCM は、データの公開鍵の操作を実行し、そのデータが秘密鍵の操作を使って回復できることを確認します。

アプリケーションの妥当性検査

アプリケーションの妥当性検査を行う際、ディジタル証明書マネージャー (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ことを確認します。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。

アプリケーションの妥当性検査は、アプリケーションが証明書を必要とする機能を実行する際に発生する可能性のある問題に対してユーザーの注意を促します。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加わったり、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。

関連概念:

86 ページの『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。

シナリオ: DCM

これらのシナリオでは、標準的な証明書実装方式について説明します。これは、IBM i セキュリティー・ポリシーの一環として、ユーザー独自の証明書実装を計画する際に役立ちます。シナリオを実行するために行わなければならない構成作業についても、各シナリオですべて紹介しています。

ディジタル証明書マネージャー (DCM) を使うと、証明書を使用して、さまざまな方法でセキュリティー・ポリシーを強化することができます。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、仮想プライベート・ネットワーク (VPN) 接続を構成することもできます。さらに、証明書の鍵を使用すれば、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 の構成方法により、DCM を使用して、ユーザー証明書と、 IBM i ユーザー・プロファイルまたはエンタープライズ識別マッピング (EIM) ID とを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、関連付けられたユーザー・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場面でセキュアな通信を実現するため、より一般的なディジタル証明書のセキュリティー目的を説明しています。また、各シナリオでは、そのシナリオを実行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説明しています。

関連情報:

オブジェクト署名のシナリオ

シナリオ : 証明書を使用して外部の認証を行う

このシナリオでは、公開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に対して一般ユーザーアクセスする際に、そのアクセスを保護および制限する認証メカニズムとして証明書を使用するタイミングとその使用方法について説明します。

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セキュアな手法で、アプリケーションへのユーザー認証の方法を提供するものとします。 非トラステッド・ネットワークを介して伝送される場合は、この情報が、認証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、権限を得ずに、この情報を相互に共用し合う可能性も考慮しました。

調査の結果、ディジタル証明書を使用すれば、アプリケーションへ入力またはアプリケーションから検索する機密情報の保護に必要なセキュリティーを実現でき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。伝送中の機密データのプライバシーが SSL によって保護されているため、証明書クライアント認証の使用に加え、現行のユーザー名およびパスワードによる認証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、およびすべての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、既知の認証局 (CA) から得た公開証明書を使用して、アプリケーションに 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認証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セキュアに行えるようになります。
- このシナリオで説明しているような、*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に対するユーザー認証を行う方法は、次のような、または同様の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開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外部ユーザーの数が多いなど、管理上の理由から、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セキュア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、既知の CA の CA 証明書が含まれています。

目的

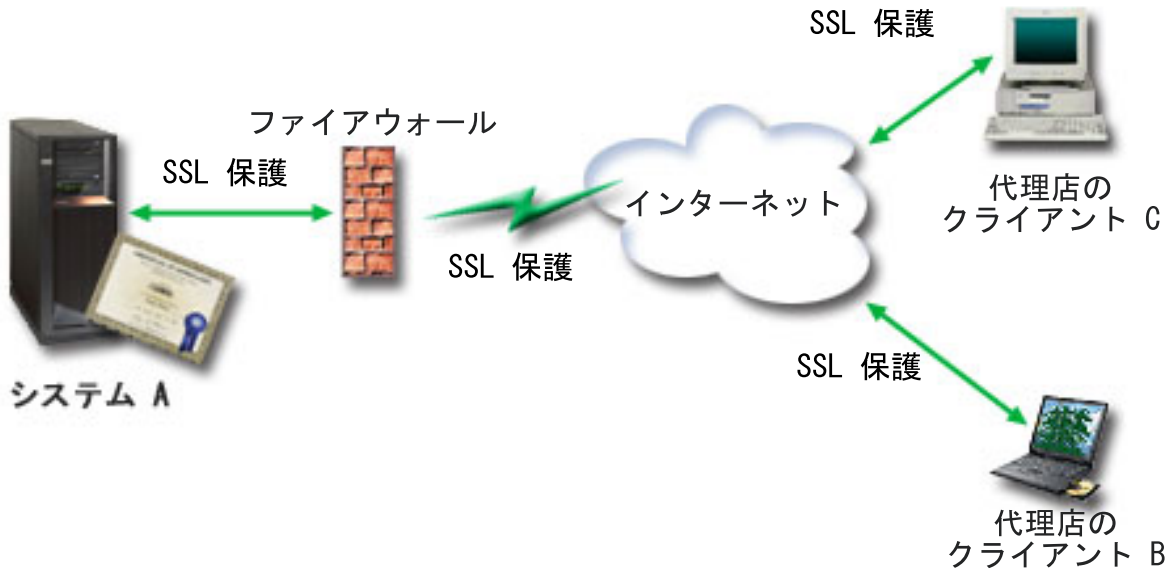
このシナリオでは、MyCo, Inc. は、自社のアプリケーションが、許可された公開ユーザーに提供する料率計算情報を保護するために、ディジタル証明書を使用したいと考えています。同社はまた、可能なときにはいつでも、このアプリケーションにアクセスできるユーザーの認証について、よりセキュアな方法も求めています。

このシナリオの目的は以下のとおりです。

- 同社の公開の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、またユーザーから受け取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、既知の公開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、証明書が使用できない場合は、既知の認証局 (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 - システム A

- システム 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。
- システム A は、IBM i バージョン 5 リリース 4 (V5R4) 以降を実行します。
- システム A には、ディジタル証明書マネージャーおよび IBM HTTP Server for i がインストールされており、構成済みになっています。

- システム 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。
  - 既知の認証局 (CA) が発行した公開証明書を使用して、認証を行い、SSL セッションを初期化する。
  - 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。
- システム A は、クライアント B および C が料率計算アプリケーションにアクセスする際に、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、システム 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、既知の 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、システム A にある料率計算アプリケーションにアクセスします。システム A は、クライアント・ソフトウェアに証明書を提示し、ID を認証して SSL セッションを開始します。
- 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、システム 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に構成されています。
- SSL セッションの開始後に、システム A がアプリケーションにアクセス権限を付与するには、まずクライアント B および C が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。

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。

- システム A の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IBM i 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。
- 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。
- システム 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 38 ページの『DCM のセットアップ要件』を満たしています。
- システム A で DCM の構成または使用が行われたことはありません。
- 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。
- システム A に IBM 暗号化コプロセッサーはインストールされていません。

構成タスク

関連タスク:

51 ページの『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) の機能を使用するには、まずシステムで DCM を開始する必要があります。

計画ワークシートを完成させる

以下の計画ワークシートには、このシナリオで説明している、収集する必要のある情報、およびディジタル証明書のインプリメンテーションを準備する際に必要な決定事項が記載されています。インプリメンテーションを確実に成功させるには、構成タスクを実行する前に、すべての前提条件項目が、はいとなるようにし、必要な情報をすべて収集しておく必要があります。

表 1. 証明書のインプリメンテーションの前提条件に関する計画ワークシート

前提条件ワークシート	**答え**
システムで実行されているのは IBM i V5R4 以降ですか。	はい
ディジタル証明書マネージャーは、システムにインストールされていますか。	はい
IBM HTTP Server for i がシステムにインストールされて、管理サーバー・インスタンスが開始されていますか。	はい
Web ブラウザーおよび HTTP Server 管理サーバー・インスタンスを使用して DCM にアクセスできるように、TCP がシステムに構成されていますか。	はい
*SECADM および *ALLOBJ 特殊権限がありますか。	はい

必要な構成タスクを実行しインプリメンテーションを完了するには、ディジタル証明書のインプリメンテーションに関する以下の情報を収集する必要があります。

表 2. 証明書のインプリメンテーションを構成するための計画ワークシート

システム A の計画ワークシート	**答え**
独自のローカル CA を運用しますか、あるいは、公開 CA からアプリケーションの証明書を取得しますか。	公開 CA から証明書を入手する
システム A は、SSL を有効にする予定のアプリケーションをホストしますか。	はい

表 2. 証明書のインプリメンテーションを構成するための計画ワークシート (続き)

システム A の計画ワークシート	答え
DCM で作成する証明書署名要求 (CSR) に使用する、識別名情報は何ですか。 • **鍵のサイズ** : 証明書の暗号鍵の強度を決定します。 • **鍵アルゴリズム (Key algorithm)**: 証明書の公開鍵と秘密鍵の生成に使用する鍵アルゴリズムを選択します。 • **証明書ラベル**: 固有の文字ストリングで証明書を識別します。 • **共通名**: 証明書のサブジェクト DN の一部である、個人、エンティティー、またはアプリケーションなど、証明書の所有者を識別します。 • **組織内の団体** : この証明書を使用するアプリケーションを使用する、組織のセクションまたはエリアを識別します。 • **組織名** : この証明書を使用するアプリケーションを使用する、企業または部門のセクションを識別します。 • **市区町村**: 所属する組織の、市区町村を識別します。 • **都道府県**: この証明書を使用する都道府県を識別します。 • **国または地域**: この証明書を使用する国または地域を 2 文字で識別します。	**鍵のサイズ**: 2048**鍵アルゴリズム (Key algorithm)**: RSA または ECDSA**証明書ラベル**: Myco_public_cert**共通名**: myco_rate_server@myco.com**組織内の団体**: Rate dept**組織名**: myco**市区町村**: Any_city**都道府県**: Any**国または地域**: ZZ
SSL を使用するように構成するアプリケーションの DCM アプリケーション ID は何ですか。	mcyo_agent_rate_app
SSL が使用可能なアプリケーションを構成して、クライアント認証の証明書を使用するようにしますか。使用する場合、どの CA を、アプリケーションの CA 信頼リストに追加しますか。	いいえ

サーバーまたはクライアント証明書要求を作成する

1. DCM を開始します。『DCM の開始』を参照してください。
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、一連のフォームに入力します。 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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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**」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、公開鍵、識別名、およびその他の新規証明書に指定した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。

   注: 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. 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。
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。

SSL を使用するようにアプリケーションを構成する

公開認証局 (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。署名された証明書を処理する前に、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。一部のアプリケーション (IBM HTTP Server for i など) では、SSL を使用するように構成することで、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) に登録します。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。アプリケーションで SSL の構成を完了すると、アプリケーション用の署名された公開証明書を構成して、SSL セッションを開始できます。

関連情報:

SSL を使用したアプリケーション・セキュリティー

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。『DCM の開始』を参照してください。
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 ***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 certificate)**」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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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、「**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。
8. このリストからアプリケーションを選択して、「**続行**」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。

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。アプリケーションを再始動する必要があるかどうかについてなど、アプリケーションを SSL モードで開始するための詳しい情報については、該当するアプリケーションの資料を参照してください。

クライアントの認証に証明書を使用し、アプリケーションで *SYSTEM 証明書ストアの使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込むようにする場合に、CA 信頼リストを定義して、*SYSTEM ストアから信頼する CA を選択できるようになりました。

(オプション): アプリケーションに必要な 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が、有効な場合は、アプリケーションが認証用に証明書を受け入れることができる必要があります。多くのアプリケーションは、クライアント認証証明書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。このオプションは、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 信頼リストを使用して信頼する CA 証明書のリストを制限するように指定されている場合、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 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。『DCM の開始』を参照してください。
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 ***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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
6. アプリケーションが承認する CA 証明書をリストから 1 つ以上選択し、「**使用可能**」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 を信頼リストに追加す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の認証を行う

このシナリオでは、内部ユーザーが、内部サーバーでアクセスできるリソースおよびアプリケーションを保護および制限するための認証メカニズムとして、どのように証明書を使用すべきかを説明します。

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などの問題に関心があるとします。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 サイトの管理担当者となり、そのサイトは、IBM HTTP Server for i (powered by Apache) で運営します。

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、これまでは、ユーザー名とパスワードを使用して認証を行い、会社のデータへのアクセスを制限していました。このデータは非常に重要で、またプライバシーに関するものであるため、パスワード認証に基づくアク

セス制限では十分とはいえない場合がある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。

調査を重ねた結果、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、秘密ローカル認証局 (CA) をセットアップし、すべての社員に証明書を発行して、その証明書と社員の IBM i ユーザー・プロファイルとを関連付けさせることに決定しました。このタイプの秘密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。
- *秘密* ディジタル証明書を使用して、アプリケーションおよびデータへアクセスするユーザーの認証を行う方法は、次のような、または同様の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、IBM i 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秘密証明書を使用すると、証明書と許可ユーザーの IBM i 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

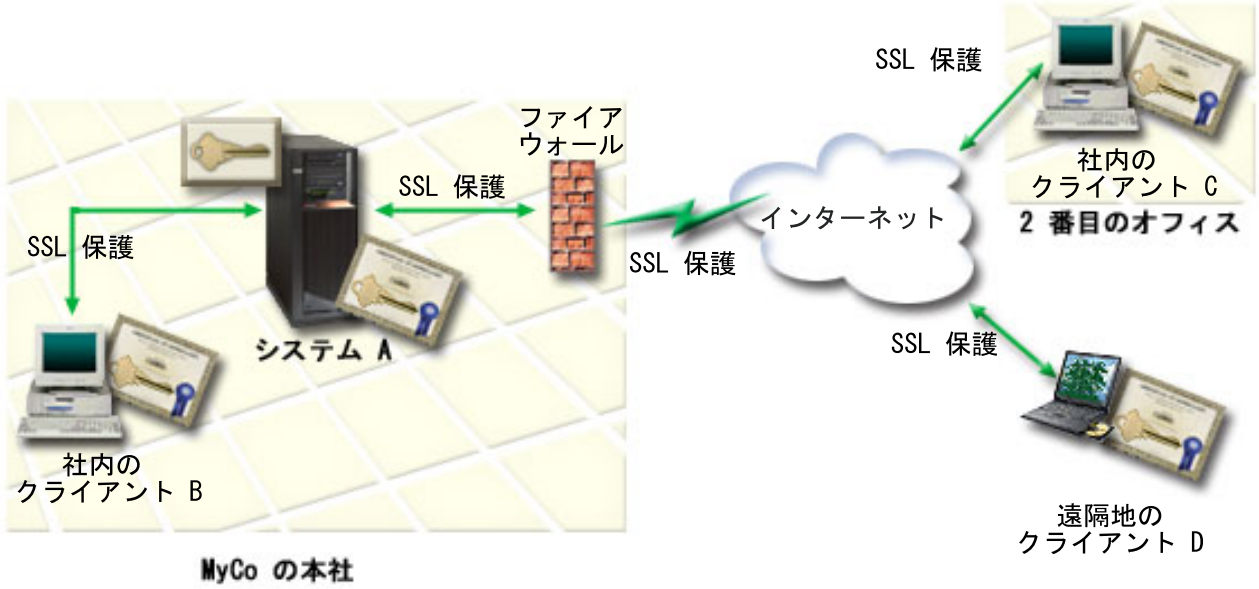
このシナリオでは、MyCo, Inc. は、社内の人事 Web サイトが従業員に提供する機密の個人情報を保護するために、ディジタル証明書を使用します。同社はまた、この Web サイトにアクセスできるユーザーを認証するための、よりセキュアな方法も求めています。

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) から提供される秘密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。

会社の公開サーバー - システム A

- システム 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。
- システム A は、IBM i バージョン 5 リリース 4 (V5R4) 以降を実行します。
- システム A には、ディジタル証明書マネージャーおよび IBM HTTP Server for i がインストールされており、構成済みになっています。
- システム 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。
  - 既知の認証局 (CA) が発行した公開証明書を使用して、認証を行い、SSL セッションを初期化する。
  - 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。
- システム A は、クライアント B および C が料率計算アプリケーションにアクセスする際に、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、システム 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、既知の 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、システム A にある料率計算アプリケーションにアクセスします。システム A は、クライアント・ソフトウェアに証明書を提示し、ID を認証して SSL セッションを開始します。

- 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、システム 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に構成されています。
- SSL セッションの開始後に、システム A がアプリケーションにアクセス権限を付与するには、まずクライアント B および C が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。

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。

- IBM HTTP Server for i (powered by Apache) は、システム A で人事用アプリケーションを実行します。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紹介しません。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。
- 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、DCM の使用手順について説明します。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。
- システム A にある人事用の HTTP Server では、既にパスワード認証を使用しています。
- システム A は、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。
- システム A で DCM の構成または使用が行われたことはありません。
- 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。
- システム A に IBM 暗号化コプロセッサーはインストールされていません。

構成タスク

計画ワークシートを完成させる

以下の計画ワークシートには、このシナリオで説明している、収集する必要のある情報、およびディジタル証明書のインプリメンテーションを準備する際に必要な決定事項が記載されています。インプリメンテーションを確実に成功させるには、構成タスクを実行する前に、すべての前提条件項目が、はいとなるようにし、必要な情報をすべて収集しておく必要があります。

表 3. 証明書のインプリメンテーションの前提条件に関する計画ワークシート

前提条件ワークシート	答え
システムで実行されているのは IBM i V5R4 以降ですか。	はい
ディジタル証明書マネージャーは、システムにインストールされていますか。	はい
システムに IBM HTTP Server for i がインストールされて、管理サーバー・インスタンスが開始されていますか。	はい
Web ブラウザーおよび HTTP Server 管理サーバー・インスタンスを使用して DCM にアクセスできるように、TCP がシステムに構成されていますか。	はい
*SECADM および *ALLOBJ 特殊権限がありますか。	はい

必要な構成タスクを実行しインプリメンテーションを完了するには、ディジタル証明書のインプリメンテーションに関する以下の情報を収集する必要があります。

表 4. 証明書のインプリメンテーションを構成するための計画ワークシート

システム A の計画ワークシート	答え
独自のローカル CA を運用しますか、あるいは、公開 CA からアプリケーションの証明書を取得しますか。	証明書を発行するローカル CA を作成する
システム A は、SSL を有効にする予定のアプリケーションをホストしますか。	はい
ローカル CA 用に使用する識別名情報は何ですか。 • **鍵のサイズ** : 証明書の暗号鍵の強度を決定します。 • **鍵アルゴリズム (Key algorithm)**: 証明書の公開鍵と秘密鍵の生成に使用する鍵アルゴリズム (RSA または ECDSA) を選択します。 • **認証局 (CA) の名前** : CA を識別し、 CA 証明書の一般名、および CA が発行する証明書の発行元 DN になります。 • **組織内の団体** : この証明書を使用するアプリケーションを使用する、組織のセクションまたはエリアを識別します。 • **組織名** : この証明書を使用するアプリケーションを使用する、企業または部門のセクションを識別します。 • **市区町村**: 所属する組織の、市区町村を識別します。 • **都道府県**: この証明書を使用する都道府県を識別します。 • **国または地域**: この証明書を使用する国または地域を 2 文字で識別します。 • **認証局の有効期間**: 認証局の証明書が有効である日数を明示します。	**鍵のサイズ**: 2048 **鍵アルゴリズム (Key algorithm)**: RSA **認証局 (CA) 名**: Myco_CA@myco.com **組織内の団体**: Rate dept **組織名**: myco **市区町村**: Any_city **都道府県**: Any **国または地域**: ZZ **認証局の有効期間**: 1095
クライアント認証用にユーザー証明書を発行するよう、ローカル CA のポリシー・データを設定しますか。	はい

表 4. 証明書のインプリメンテーションを構成するための計画ワークシート (続き)

システム A の計画ワークシート	答え
ローカル CA が発行するサーバー認証用に使用する識別名情報は何ですか。 • **鍵のサイズ** : 証明書の暗号鍵の強度を決定します。 • **鍵アルゴリズム (Key algorithm)**: 証明書の公開鍵と秘密鍵の生成に使用する鍵アルゴリズム (RSA または ECDSA) を選択します。 • **証明書ラベル**: 固有の文字ストリングで証明書を識別します。 • **共通名**: 証明書のサブジェクト DN の一部である、個人、エンティティー、またはアプリケーションなど、証明書の所有者を識別します。 • **組織内の団体** : この証明書を使用するアプリケーションを使用する、組織のセクションまたはエリアを識別します。 • **組織名** : この証明書を使用するアプリケーションを使用する、企業または部門のセクションを識別します。 • **市区町村**: 所属する組織の、市区町村を識別します。 • **都道府県**: この証明書を使用する都道府県を識別します。 • **国または地域**: この証明書を使用する国または地域を 2 文字で識別します。	**鍵のサイズ**: 1024 **鍵アルゴリズム (Key algorithm)**: RSA **証明書ラベル**: Myco_public_cert **共通名**: myco_rate_server@myco.com **組織内の団体**: Rate dept **組織名**: myco **市区町村**: Any_city **都道府県**: Any **国または地域**: ZZ
SSL を使用するように構成するアプリケーションの DCM アプリケーション ID は何ですか。	mcyo_agent_rate_app
SSL が使用可能なアプリケーションを構成して、クライアント認証の証明書を使用するようにしますか。使用する場合、どの CA を、アプリケーションの CA 信頼リストに追加しますか。	はい Myco_CA@myco.com

SSL を使用するように人事 HTTP Server を構成する

システム A 上の人事用 HTTP Server (powered by Apache) の Secure Sockets Layer (SSL) 構成には、サーバーの現在の構成方法に従って、異なるタスクが複数組み込まれます。

SSL を使用するようにサーバーを構成するには、以下のステップに従います。

1. HTTP Server 管理インターフェースを開始します。
2. 特定の HTTP サーバーを操作するには、ページ・タブ「**管理 (Manage)**」 > 「**すべてのサーバー (All Servers)**」 > 「**すべての HTTP サーバー (All HTTP Servers)**」を選択して、構成済みのすべての HTTP サーバーのリストを表示します。
3. リストから該当するサーバーを選択し、「**詳細の管理 (Manage Details)**」をクリックします。
4. ナビゲーション・フレームで、「**セキュリティー**」を選択します。
5. フォームにある「**SSL で証明書認証 (SSL with Certificate Authentication)**」タブを選択します。
6. 「**SSL**」フィールドで、「**使用可能**」を選択します。
7. 「**サーバー証明書アプリケーション名 (Server certificate application name)**」フィールドで、このサーバー・インスタンスを認識できるアプリケーション ID を指定します。リストから 1 つ選択すること

もできます。このアプリケーション ID は、 QIBM_HTTP_SERVER_[server_name] という形式で、たとえば、QIBM_HTTP_SERVER_MYCOTEST のようになります。**注 :** このアプリケーション ID を忘れないようにしてください。 DCM で再度この ID を選択する必要があります。

HTTP Server の構成を完了して SSL が使用できるようになれば、DCM を使用して、SSL およびクライアント認証に必要な証明書サポートを構成できます。

関連情報:

IBM HTTP Server for i5/OS

ローカル CA の作成および運用

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 を有効にする上で必要なすべての構成を確実に行うための、一連の手順が示されます。これには、*SYSTEM ストアに作成されたばかりのローカル CA 証明書のコピーの追加、およびローカル CA が発行した証明書の Web サーバー・アプリケーションへの割り当てが含まれます。アプリケーションが CA 信頼リストを使用して、*SYSTEM 証明書の使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込んでいる場合は、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。『DCM の開始』を参照してください。
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。 これらのフォームのガイドに従って、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、および署名検査用のディジタル証明書を使用するために必要となるタスクを完了させるプロセスを実行します。

   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、稼働させるローカル認証局 (CA) のセットアップに必要なすべてのタスクを実行させるには、以下の手順を実行します。
   a. ローカル CA の識別情報を指定します。
   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、ソフトウェアがそのローカル CA を認識し、その CA が発行する証明書の妥当性検査を実行できるようにします。
   c. ローカル CA 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、SSL 接続用にアプリケーションが使用可能なサーバー証明書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、オブジェクトにディジタル署名するためにアプリケーションが使用可能な、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別のタスクを行わなければなりません。

g. CA 信頼リストを使用し、ローカル CA を信頼しようとしているアプリケーションを選択します。アプリケーションの CA 信頼リストが空の場合は、*SYSTEM ストアのすべての CA がデフォルトで信頼されます。

注: CA 信頼リストの使用を計画している場合を除き、QIBM_HTTP_SERVER_MYCOTEST など、人事 HTTP Server 用のアプリケーション ID を選択しないでください。

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すれば、ユーザー認証のための証明書を要求するように、 Web サーバーを構成できます。

人事 Web サーバー用のクライアント認証を構成する

HTTP Server が認証のための証明書を要求するように指定する場合に、一般的な認証の設定を HTTP Server に対して構成する必要があります。これらの設定は、Secure Sockets Layer (SSL) を使用するようサーバーを構成するために使用したものと同じセキュリティー・フォームで構成します。

クライアント認証のための証明書を要求するようにサーバーを構成するには、以下のステップに従います。

1. HTTP Server 管理インターフェースを開始します。
2. Web ブラウザーを開いて http://your_system_name:2001 と入力し、IBM Navigator for i のウェルカム・ページをロードします。
3. ウェルカム・ページから「**IBM i タスク・ページ**」リンクをクリックします。
4. 「**IBMWeb Administration for i**」を選択します。
5. 特定の HTTP サーバーを操作するには、ページ・タブ「**管理 (Manage)**」 > 「**すべてのサーバー (All Servers)**」 > 「**すべての HTTP サーバー (All HTTP Servers)**」を選択して、構成済みのすべての HTTP サーバーのリストを表示します。
6. リストから該当するサーバーを選択し、「**詳細の管理 (Manage Details)**」をクリックします。
7. ナビゲーション・フレームで、「**セキュリティー**」を選択します。
8. フォームにある「**認証**」タブを選択します。
9. 「**クライアントの IBM プロファイルを使用 (Use IBM i profile of client)**」を選択します。
10. 「**認証の名前またはレルム (Authentication name or realm)**」フィールドで、権限レルムの名前を指定します。
11. 「**クライアントの権限を使用して要求を処理する (Process requests using client's authority)**」フィールドで「使用可能」を選択し、「**適用**」をクリックします。
12. フォームにある「**アクセスの制御 (Control Access)**」タブを選択します。
13. 「**すべての認証されたユーザー (有効なユーザー名およびパスワード) (All authenticated users (valid user name and password))**」を選択し、「**適用**」をクリックします。
14. フォームにある「**SSL で証明書認証 (SSL with Certificate Authentication)**」タブを選択します。
15. 「**SSL**」フィールドで、「使用可能」が選択された値であることを確認してください。
16. 「**サーバー証明書アプリケーション名 (Server certificate application name)**」フィールドで、QIBM_HTTP_SERVER_MYCOTEST などのように、正しい値が指定されているか、確認します。

17. 「**接続を確立する前に、使用可能な場合はクライアント証明書を受け入れる (Accept client certificate if available before making connection)**」を選択します。「**OK**」をクリックします。

クライアント認証の構成を完了すると、HTTP サーバーを SSL モードで再始動し、人事アプリケーションのデータのプライバシー保護を開始できます。

関連情報:

IBM HTTP Server for i5/OS

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 (powered by Apache) を停止してから始動するには、以下のステップに従ってください。

1. System i® ナビゲーターで、「**システム (system)**」 > 「**ネットワーク**」 > 「**サーバー**」 > 「**TCP/IP**」 > 「**HTTP 管理 (HTTP Administration)**」と展開します。
2. 「**開始**」をクリックして、 HTTP Server 管理インターフェースを開始します。
3. 「**管理 (Manage)**」タブをクリックして、構成済みのすべての HTTP サーバーのリストを表示します。
4. リストから該当するサーバーを選択し、サーバーが稼働中の場合は、「**停止**」をクリックします。
5. 「**開始**」をクリックして、サーバーを再始動します。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。

ユーザーが人事 Web アプリケーションにアクセスするには、ローカル CA 証明書のコピーを、各自のブラウザー・ソフトウェアにあらかじめインストールしておく必要があります。

関連情報:

HTTP Server Information Center の概要 (HTTP Server Information Center Overview)

ブラウザーでのローカル CA 証明書のコピーのインストール

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、秘密ローカル CA の発行した証明書をサーバーが提示する場合、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 証明書のコピーを取得する必要があります。

1. DCM を開始します。『DCM の開始』を参照してください。
2. ナビゲーション・フレームにある「**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、ブラウザーへのローカル CA 証明書のダウンロードや、システム上のファイルへの保管を行う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 からの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・プロセスを進行させます。

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。

ユーザーは、SSL モードで人事 Web サーバーにアクセスできるようになったため、ユーザーは、認証のために適切な証明書をサーバーに対して提出できる必要があります。したがって、ユーザーは、ローカル CA からユーザー証明書を取得する必要があります。

ローカル CA からの証明書を要求する

これまでのステップで、ユーザー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、この Web サーバーへのアクセスの許可をユーザーが得るためには、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、CA によるユーザー証明書の発行が、ローカル CA のポリシーによって許可されている必要があります。

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証明書を入手する必要があります。

1. DCM を開始します。『DCM の開始』を参照してください。
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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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鍵を生成した後、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IBM i ユーザー・プロファイルが自動的に関連付けられます。

これらのタスクを完了すると、有効な証明書を持つ許可ユーザーだけが人事 Web サーバーのデータにアクセスできるようになり、また、そのデータは、伝送中 SSL によって保護されます。

シナリオ: ディジタル証明書マネージャーを使用して認証局をセットアップする

営業所の管理者は、認証局 (CA) をセットアップする前に、さまざまな計画作業を完了させておく必要があります。以下の作業を実行する前に、このシナリオのすべての前提条件が満たされているようにしてください。

ディジタル証明書マネージャーの計画ワークシートの作成

MyCo, Inc. では、ビジネス・パートナーに発行するディジタル証明書のセットアップを行えるように、計画ワークシートを作成します。

表 5. ディジタル証明書マネージャー (DCM) を使用して認証局 (CA) を作成するための計画ワークシート

質問	答え
証明書の公開鍵および秘密鍵を生成するために、どのくらいの鍵サイズを使用する予定ですか。	2048
証明書の公開鍵および秘密鍵を生成するために、どの鍵アルゴリズム (RSA または ECDSA) を使用する予定ですか。	RSA
証明書ストアのパスワードは何ですか。	secret **重要:** このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
認証局の名前は何ですか。	mycoca
組織の名前は何ですか。	myco
認証局の有効日数は何日ですか。	1095 (3 年)
使用するブラウザーは何ですか。	Windows Internet Explorer バージョン 6.0
ネットワーク上のユーザーに証明書を発行しますか。	いいえ

表 6. システム A 用のディジタル証明書の計画ワークシート

質問	答え
証明書の公開鍵および秘密鍵を生成するために、どのくらいの鍵サイズを使用する予定ですか。	521
証明書の公開鍵および秘密鍵を生成するために、どの鍵アルゴリズム (RSA または ECDSA) を使用する予定ですか。	ECDSA
証明書ストアのパスワードは何ですか。	secret **重要:** このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
証明書ラベルの名前は何ですか。	mycocert
証明書の共通名は何ですか。	mycocert
組織の名前は何ですか。	MyCo, Inc

表 6. システム A 用のディジタル証明書の計画ワークシート (続き)

質問	答え
システムの IP アドレスは何ですか。	192.168.1.2 (IPv6 の場合は 2001:DB8::2) **重要:** このシナリオで使用する IP アドレスは、あくまでも一例です。 IP アドレスの指定方式に従ったものではないため、実際の構成では使用しないでください。これらの作業を実行する際には、実際の IP アドレスを使用してください。
システムの完全修飾ホスト名は何ですか。	systema.myco.min.com

表 7. システム B 用のディジタル証明書の計画ワークシート

質問	答え
証明書の公開鍵および秘密鍵を生成するために、どのくらいの鍵サイズを使用する予定ですか。	2048
証明書の公開鍵および秘密鍵を生成するために、どの鍵アルゴリズム (RSA または ECDSA) を使用する予定ですか。	RSA
証明書ラベルの名前は何ですか。	corporatecert
証明書の共通名は何ですか。	corporatecert
証明書ストアのパスおよびファイル名は何ですか。	/tmp/systemb.kdb
証明書ストアのパスワードは何ですか。	secret2 **重要:** このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
ディジタル証明書の共通名は何ですか。	corporatecert
この証明書を所有する組織の名前は何ですか。	MyCo, Inc
システムの IP アドレスは何ですか。	172.16.1.3 (IPv6 の場合は 2002:DD8::3) **重要:** このシナリオで使用する IP アドレスは、あくまでも一例です。 IP アドレスの指定方式に従ったものではないため、実際の構成では使用しないでください。これらの作業を実行する際には、実際の IP アドレスを使用してください。
システムの完全修飾ホスト名は何ですか。	systemb.myco.wis.com

システム A でのIBM HTTP Server for i の開始

システム A で IBM HTTP Server for i を開始するには、以下の手順に従います。

ディジタル証明書マネージャー (DCM) のインターフェースにアクセスするには、以下のタスクを実行して、HTTP Server の管理インスタンスを開始してください。

1. システム A から文字ベース・インターフェースにサインオンします。
2. コマンド・プロンプトで、`strtcpsvr server(*HTTP) httpsvr(*admin)` と入力します。これにより、HTTP Server の管理システムが始動します。

システム A を認証局として構成する

システム A を認証局 (CA) として構成するには、以下の手順に従います。

1. Web ブラウザーを開いて http://your_system_name:2001 と入力し、IBM Navigator for i のウェルカム・ページをロードします。
2. システム A のユーザー・プロファイル名およびパスワードを使用して、ログオンします。
3. ウェルカム・ページから「**IBM i タスク・ページ**」リンクをクリックします。
4. 「**ディジタル証明書マネージャー**」を選択します。
5. 左側のナビゲーション・ペインから、「**認証局 (CA) の作成 (Create a Certificate Authority (CA))**」を選択します。
6. DCM 計画ワークシートの情報を基に、「認証局 (CA) の作成 (Create a Certificate Authority (CA))」ページの以下の必須フィールドに入力を行います。
   - **鍵のサイズ:** 1024
   - **証明書ストアのパスワード (Certificate store password):** secret
   - **確認パスワード (Confirm password):** secret

     重要: このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
   - **認証局名 (Certificate Authority name):** mycoca
   - **組織名:** MyCo, Inc
   - **都道府県:** min
   - **国または地域:** us
   - **認証局の有効期間 (2 から 7300) (Validity period of Certificate Authority (2-7300)):** 1095
7. 「**続行 (Continue)**」をクリックします。
8. 「**ローカル CA 証明書のインストール (Install Local CA certificate)**」ページで「**続行 (Continue)**」をクリックします。
9. 「**認証局 (CA) のポリシー・データ (Certificate Authority (CA) Policy Data)**」ページで、以下のオプションを選択します。
   - **ユーザー証明書の作成の許可 (Allow creation of user certificates):** はい (Yes)
   - **認証局が発行した証明書の有効期間 (1 から 2000) (Validity period of certificates that are issued by this Certificate Authority (1-2000)):** 365
10. 「ポリシー・データの受け入れ (Policy Data Accepted)」ページで表示されたメッセージを読み、「**続行 (Continue)**」をクリックして、デフォルトのサーバー証明書ストア (*SYSTEM)、および CA によって署名されたサーバー証明書を作成します。確認メッセージを読み、「**続行 (Continue)**」をクリックします。
11. 「サーバーまたはクライアント証明書の作成 (Create a Server or Client Certificate)」ページで、以下の情報を入力します。
    - **鍵のサイズ:** 2048

- **鍵アルゴリズム (Key algorithm):** RSA または ECDSA
- **証明書ラベル:** mycocert
- **証明書ストアのパスワード (Certificate store password):** secret
- **確認パスワード (Confirm password):** secret

  重要: このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
- **共通名:** mycocert
- **組織名:** myco
- **都道府県:** min
- **国または地域:** us
- **IP バージョン 4 のアドレス (IP version 4 address):** 192.168.1.2

  注: このシナリオで使用する IP アドレスは、あくまでも一例です。 IP アドレスの指定方式に従ったものではないため、実際の構成では使用しないでください。これらの作業を実行する際には、実際の IP アドレスを使用してください。
-
- **完全修飾ドメイン・ネーム:** systema.myco.min.com
- **電子メール・アドレス:** administrator@myco.min.com

12. 「**続行 (Continue)**」をクリックします。
13. 「アプリケーションの選択 (Select Application)」ページで「**続行 (Continue)**」をクリックします。

    ヒント: 「VPN 新規接続 (VPN New Connection)」ウィザードによって、作成した証明書が IBM i VPN 鍵マネージャー・アプリケーションに自動的に割り当てられます。この証明書を使用する可能性があるアプリケーションが他にある場合は、このページで選択することができます。このシナリオでは VPN 接続だけに証明書を使用するため、追加のアプリケーションを選択する必要はありません。
14. 「アプリケーションの状況 (Application Status)」ページで表示されたメッセージを読み、「**キャンセル**」をクリックします。これで、行った変更が受け入れられます。

    注: 証明書ストアを作成して、オブジェクトに署名するために使用する証明書を組み込む場合は、「**続行 (Continue)**」を選択します。
15. DCM インターフェースが最新表示されたら、「**証明書ストアの選択 (Select a Certificate Store)**」を選択します。
16. 「証明書ストアの選択 (Select a Certificate Store)」ページで、「***SYSTEM**」を選択します。「**続行 (Continue)**」をクリックします。
17. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページに、`secret` と入力します。「**続行 (Continue)**」をクリックします。
18. 左側のナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択します。
19. 「アプリケーションの管理 (Manage Applications)」ページで、「**CA 信頼リストの定義 (Define CA trust list)**」を選択します。「**続行 (Continue)**」をクリックします。
20. 「CA 信頼リストの定義 (Define CA Trust List)」ページで、「**サーバー (Server)**」を選択します。「**続行 (Continue)**」をクリックします。
21. 「**IBM i VPN Key Manager**」を選択します。「**CA 信頼リストの定義 (Define CA Trust List)**」をクリックします。

22. 「CA 信頼リストの定義 (Define CA Trust List)」ページで、「**LOCAL_CERTIFICATE_AUTHORITY**」を選択します。「**OK**」をクリックします。

システム B 用のディジタル証明書の作成

システム B 用のディジタル証明書を作成するには、次の手順に従います。

1. 左側のナビゲーション・ペインで、「**証明書の作成 (Create Certificate)**」をクリックして、「**IBM i を実行する別のシステム用のサーバーまたはクライアント証明書 (Server or client certificate for another system running IBM i)**」を選択します。
2. 「**続行 (Continue)**」をクリックします。
3. 「IBM i を実行する別のシステム用のサーバーまたはクライアント証明書の作成 (Create a Server or Client Certificate for Another System Running IBM i)」ページで、以下の情報を入力します。
   - **鍵のサイズ:** 2048
   - **証明書ラベル:** corporatecert
   - **証明書ストアのパスおよびファイル名 (Certificate store path and filename):** /tmp/systemb.kdb
   - **証明書ストアのパスワード (Certificate store password):** secret2
   - **確認パスワード (Confirm password):** secret2

     注: このシナリオで使用するパスワードは、すべて一例です。実際の構成では、これらのパスワードを使用しないようにしてください。
   - **共通名:** corporatecert
   - **組織名:** MyCo, Inc
   - **都道府県:** wis
   - **国または地域:** us
   - **IP バージョン 4 のアドレス (IP version 4 address):** 172.16.1.3
   - このシナリオで使用する IP アドレスは、あくまでも一例です。 IP アドレスの指定方式に従ったものではないため、実際の構成では使用しないでください。これらの作業を実行する際には、実際の IP アドレスを使用してください。
   - **完全修飾ホスト名 (Fully qualified host name):** systemb.myco.wis.com
   - **電子メール・アドレス:** administrator@myco.wis.com
4. 「**続行 (Continue)**」をクリックします。システム A でシステム B 用のサーバー証明書が作成されたことを確認する、確認メッセージが表示されます。ユーザーは、営業所のネットワーク管理者として、企業オフィスの管理者に対して、これらのファイルを暗号化された電子メールで送信します。企業オフィスの管理者は、証明書ストア (.KDB) ファイルおよび要求 (.RDB) ファイルをシステム B に移動して、名前変更を行う必要があります。企業オフィスの管理者は、統合ファイル・システムの /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに、これらのファイルを移動する (バイナリー FTP を使用) 必要があります。この作業が完了したら、管理者は適切なディレクトリーで、これらのファイルを名前変更しなければなりません。

システム B における .KDB ファイルおよび .RDB ファイルの名前変更

システム B で .KDB ファイルおよび .RDB ファイルを名前変更するには、以下の手順に従います。

システム B には *SYSTEM 証明書ストアが存在しないため、企業ネットワークの管理者は、これらの転送されたファイルをシステム B の *SYSTEM 証明書ストアとして使用することで、systemb.kdb ファイルおよび systemb.RDB ファイルを、DEFAULT.KDB および DEFAULT.RDB に名前変更する必要があります。

1. System i ナビゲーターで、「**システム B (System B)**」 > 「**ファイル・システム (File Systems)**」 > 「**統合ファイル・システム**」 > 「**Qibm**」 > 「**UserData**」 > 「**ICSS**」 > 「**Cert**」 > 「**サーバー (Server)**」と展開し、systemb.kdb ファイルおよび systemb.RDB ファイルが、このディレクトリーにリストされているか確認します。
2. コマンド行で、`wrklnk ('/qibm/userdata/icss/cert/server')` と入力します。
3. 「リンク・オブジェクトの使用 (Work with Link Objects)」ページで 7 (「名前変更 (Rename)」) を選択し、systemb.kdb ファイルを名前変更します。 Enter キーを押します。
4. 「オブジェクトの名前変更 (Rename Object)」ページの「**新規オブジェクト (New Object)**」フィールドに、`DEFAULT.KDB` と入力します。 Enter キーを押します。
5. ステップ 3 およびステップ 4 を繰り返して、systemb.RDB ファイルを DEFAULT.RDB に名前変更します。
6. System i ナビゲーターを最新表示して、「**システム *B (System B)***」 > 「**ファイル・システム (File Systems)**」 > 「**統合ファイル・システム**」 > 「**Qibm**」 > 「**UserData**」 > 「**ICSS**」 > 「**Cert**」 > 「**サーバー (Server)**」と展開し、これらのファイルが変更されているか確認します。 DEFAULT.KDB ファイルおよび DEFAULT.RDB ファイルが、このディレクトリーにリストされます。

システム B における証明書ストアのパスワードの変更

システム B で証明書ストアのパスワードを変更するには、以下の手順に従います。

企業オフィスのネットワーク管理者は、DEFAULT.KDB ファイルおよび DEFAULT.RDB ファイルの作成時に作成された、新規の *SYSTEM 証明書ストアのパスワードを変更する必要があります。

注: *SYSTEM 証明書ストアのパスワードを変更する必要があります。パスワードが変更されると、アプリケーションがそのパスワードを自動的に回復して証明書ストアを開き、証明書にアクセスできるように、パスワードが保管されます。

1. Web ブラウザーを開いて http://your_system_name:2001 と入力し、IBM Navigator for i のウェルカム・ページをロードします。
2. ウェルカム・ページから「**IBM i タスク・ページ**」リンクをクリックします。
3. 「**ディジタル証明書マネージャー**」を選択します。
4. 左側のナビゲーション・ペインにある「**証明書ストアの選択 (Select a Certificate Store)**」をクリックします。
5. 「***SYSTEM 証明書ストア (*SYSTEM Certificate Store)**」を選択し、パスワードとして `secret2` を入力します。このパスワードは、システム B のサーバー証明書の作成時に営業所の管理者が指定したものです。「**続行 (Continue)**」をクリックします。
6. 左側のナビゲーション・フレームで、「**証明書ストアの管理 (Manage Certificate Store)**」、「**パスワードの変更 (Change Password)**」と選択し、「**続行 (Continue)**」をクリックします。
7. 「証明書ストアのパスワードの変更 (Change Certificate Store Password)」ページの「**新規パスワード (New password)**」フィールドおよび「**確認パスワード (Confirm password)**」フィールドに、`corporatepwd` と入力します。
8. 有効期限ポリシーでは、「**パスワードの有効期限なし (Password does not expire)**」を選択します。「**続行 (Continue)**」をクリックします。確認ページがロードされます。「**OK**」をクリックします。
9. 「証明書ストアのパスワードの変更 (Change Certificate Store Password)」確認ページに表示されたメッセージを読み、「**OK**」をクリックします。

10. 再ロードされた「証明書ストアおよびパスワード (Certificate Store and Password)」ページにある「**証明書ストアのパスワード (Certificate Store Password)**」フィールドに、coporatepwd と入力します。「**続行 (Continue)**」をクリックします。

システム B の IBM i VPN 鍵マネージャーに対する CA 信頼の定義

システム B の VPN 鍵マネージャーに対する CA 信頼を定義するには、以下の手順に従います。

1. 左側のナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択します。
2. 「アプリケーションの管理 (Manage Applications)」ページで、「**CA 信頼リストの定義 (Define CA trust list)**」を選択します。「**続行 (Continue)**」をクリックします。
3. 「CA 信頼リストの定義 (Define CA Trust List)」ページで、「**サーバー (Server)**」を選択します。「**続行 (Continue)**」をクリックします。
4. 「**IBM i VPN Key Manager**」を選択します。「**CA 信頼リストの定義 (Define CA Trust List)**」をクリックします。
5. 「CA 信頼リストの定義 (Define CA Trust List)」ページで、「**LOCAL_CERTIFICATE_AUTHORITY**」を選択します。「**OK**」をクリックします。

これで、営業所の管理者および企業オフィスの管理者は、VPN 構成を開始することができます。

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 のセットアップ要件

ディジタル証明書マネージャー (DCM) が正常に機能するためには、特定製品のインストールとアプリケーションの構成が必要になります。

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 IBM i 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。

- ディジタル証明書マネージャー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 i をインストールして、管理サーバー・インスタンスを開始します。
- 必ず、Web ブラウザーおよび HTTP Server 管理サーバー・インスタンスを使用して DCM 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。

DCM データのバックアップおよび回復に関する考慮事項

ディジタル証明書マネージャー (DCM) の証明書ストアにアクセスする際に使用する、暗号化された鍵データベースのパスワードは、システムの特別なセキュリティー・ファイルに保管、つまり隠されています。

DCM を使用してシステムに証明書ストアを作成すると、DCM は、自動的にユーザー用のパスワードを知られないように隠しておきます。ただし、状況によっては、DCM が証明書ストアのパスワードを隠しておくように手動で処理する必要があります。

たとえば、DCM を使用して別の IBM i モデルの証明書を作成し、ターゲット・システムにある証明書ファイルを使用して、新しい証明書ストアを作成する場合などです。このような場合には、新しく作成された証明書ストアを開き、「**パスワードの変更 (Change password)**」タスクを使って、ターゲット・システムの証明書ストアのパスワードを変更し、DCM に新しいパスワードを確実に隠しておくようにする必要があります。証明書ストアが「別システム証明書ストア (Other System Certificate Store)」である場合も、パスワードを変更する際に、「**自動ログイン (Auto login)**」オプションを使用するように指定する必要があります。

さらに、「別のシステム証明書ストア」のパスワードを変更またはリセットする場合は、必ず「**自動ログイン (Auto login)**」オプションを指定する必要があります。

DCM の重要なデータを確実にバックアップするには、以下に従ってください。

- 保管 (SAV) コマンドを使用して、すべての `.KDB` および `.RDB` ファイルを保存します。各 DCM 証明書ストアは 2 つのファイルで構成され、それぞれ `.KDB` 拡張子と `.RDB` 拡張子が付いています。
- システム保管 (SAVSYS) コマンドとセキュリティー・データ保管 (SAVSECDTA) コマンドを使用して、証明書ストアへのアクセスに必要な鍵データベースのパスワードがある特別なセキュリティー・ファイルを保管します。 DCM パスワードのセキュリティー・ファイルを復元するには、ユーザー・プロファイルの復元 (RSTUSRPRF) コマンドを使用し、ユーザー・プロファイル (USRPRF) オプションで `*ALL` を指定します。

このほかの回復に関する考慮事項としては、SAVSECDTA 操作の使用により、現行の証明書ストアのパスワードが、保管されている DCM パスワード・セキュリティー・ファイルにあるパスワードと同期しなくなる可能性の問題があります。 SAVSECDTA 操作の後、その操作からデータを復元する前に、証明書ストアのパスワードを変更した場合、現行の証明書ストアのパスワードは、復元されたファイルにあるものと同期していません。

この問題を避けるには、SAVSECDTA 操作からデータを復元した後、DCM で「**パスワードの変更 (Change password)**」タスク (ナビゲーション・フレームの「**証明書ストアの管理 (Manage Certificate Store)**」の下) を使用して、証明書ストアのパスワードを変更し、パスワードを同期させる必要があります。ただし、この場合に、証明書ストアのオープンを選択したとき表示される「**パスワードのリセット (Reset Password)**」ボタンを使用しないでください。パスワードをリセットしようとすると、DCM は隠されているパスワードを取り戻そうとします。隠されているパスワードが現行のパスワードと同期していない場合、リセットの操作は失敗します。証明書ストアのパスワードを変更することがあまり多くない場合は、パスワードを変更するたびに、SAVSECDTA を実行し、このデータの復元が必要になる場合に備えて、常に隠されている最新バージョンのパスワードが保管されるようにしてください。

関連タスク:

71 ページの『ローカル CA を使用して他の IBM i モデルの証明書を発行』
ディジタル証明書マネージャー (DCM) を使用すると、あるシステム上に秘密ローカル CA を構成して、他の IBM i プラットフォームで使用する証明書を発行することができます。

ディジタル証明書のタイプ

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、証明書ストアにある証明書と関連する秘密鍵とを、証明書のタイプを基に分類して管理します。

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して操作するローカル CA は、独立エンティティーです。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、発行元である CAs の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 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、秘密 CA が発行するユーザーの証明書を、そのユーザーの IBM i 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 IBM i ユーザー・プロファイルと関連付けることもできます。

注: システムに IBM 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。暗号化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、暗号化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鍵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。

関連概念:

9 ページの『証明書ストア』
証明書ストアは特殊な鍵データベース・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。

公開証明書と秘密証明書

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、秘密 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。

証明書を発行する CA のタイプを決めた後、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のインプリメンテーション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。
- 独自のローカル CA を運用して、ユーザーおよびアプリケーション用の秘密証明書を発行する。
- 公開インターネット CA と独自のローカル 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 から証明書を取得することにするのか、あるいは CA が発行する証明書を承認することにするかを決定する前に、 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、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。証明書が必要な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秘密ユーザーを、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、既知の公開 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においても、無名なローカル CA が発行する証明書よりも、有名な公開 CA が発行する証明書の方を、承認して信頼すると考えられます。

秘密証明書の使用

独自のローカル CA を作成すると、会社内または組織内のように、より限られた範囲にあるシステムとユーザーに証明書を発行できます。独自のローカル 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メンバー・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 を維持する際のデメリットとして、時間と資源を投入しなくてはならない、ということが考えられます。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、ユーザー証明書の保管場所を決定する必要があります。ユーザーが DCM を使用してローカル CA から証明書を取得する場合、それらの証明書はデフォルトでユーザー・プロファイルに保管されます。ただし、エンタープライズ識別マッピング (EIM) と連携するように DCM を構成して、ユーザーの証明書が Lightweight Directory Access Protocol (LDAP) 位置に保管されるようにすることもできます。ユーザー証明書とユーザー・プロファイルの関連付けや、ユーザー・プロファイルへの保管を行いたくない場合は、API を使用することで、IBM i ユーザー以外のユーザーに対してプログラマチックに証明書を発行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定します。 既知の 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。管理者は、既知の公開 CA 証明書のコピーがある適切な DCM 証明書ストアで、CA 証明書に対する承認を設定します。ただし、CA 証明書が証明書ストアにない場合、ユーザーが CA 証明書のコピーを取得しインポートしない限り、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 証明書が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。

公開証明書と秘密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。

- 『ローカル CA の作成および運用』では、ローカル CA を運用して秘密証明書を発行する場合に実行する必要がある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、既知の公開 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。
- 『他の IBM i モデルでのローカル CA の使用』では、秘密ローカル CA が発行した証明書を複数のシステムで使用する場合に、実行する必要があるタスクについて説明しています。

関連概念:

62 ページの『公開インターネット CA からの証明書の管理』
ディジタル証明書マネージャー (DCM) を使用して、公開インターネット CA から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、特殊鍵データベース・ファイルです。

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

51 ページの『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。

48 ページの『オブジェクトに署名するためのディジタル証明書』
IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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。

関連タスク:

46 ページの『ディジタル証明書とエンタープライズ識別マッピング』
エンタープライズ識別マッピング (EIM) およびディジタル証明書マネージャー (DCM) を一緒に使用すると、EIM マッピングのルックアップ操作のソースとして証明書を適用し、証明書から同じ EIM ID と関連付けられているターゲット・ユーザー ID へとマップします。

56 ページの『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) を使用して秘密ローカル認証局 (CA) を運用する場合は、そのローカル CA を使用して証明書を各ユーザーに発行できます。

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

71 ページの『ローカル CA を使用して他の IBM i モデルの証明書を発行』
ディジタル証明書マネージャー (DCM) を使用すると、あるシステム上に秘密ローカル CA を構成して、他の IBM i プラットフォームで使用する証明書を発行することができます。

関連資料:

60 ページの『API を使用して証明書を IBM i ユーザー以外のユーザーへプログラマチックに発行する』
ローカル CA では、証明書と IBM i ユーザー・プロファイルを関連付けずに、ユーザーに秘密証明書を発行することができます。

SSL セキュア通信のためのディジタル証明書

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、クライアントまたはエンド・ユーザーに対して、接続先のサイトが信頼できるサイトであると保証できます。また、通信セッションが暗号化されるため、こ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ます。

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、発行元認証局 (CA) 証明書のコピーに対して、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鍵を承認し、その対称鍵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 開始処理の間、非対称鍵 (公開鍵) アルゴリズムを使用して対称鍵のネゴシエーションを行います。この対称鍵を引き続き使用して、その特定の SSL セッションでアプリケーションのデータの暗号化および複合を行います。 つまり、サーバーとクライアントは異なるセッション鍵を使用し、これらの鍵は、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鍵を代行受信して復号するようなことが万一あっても、そのセッション鍵を使ってそれ以後に使用される鍵を推測することはできません。

関連概念:

『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。

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。

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同じユーザーの IBM i ユーザー・プロファイルや別のユーザー ID と関連付けることができます。この場合、証明書の権限と許可は、関連付けられたユーザー ID またはユーザー・プロファイルと同じものになります。別の方法として、API を使用して、秘密ローカル認証局 (CA) をプログラマチックに使用し、IBM i ユーザー以外のユーザーに証明書を発行することもできます。これらの API を使用することにより、IBM i ユーザー・プロファイルまたは他の内部ユーザー ID を割り当てたくないユーザーに対して、秘密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、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するのは CA です。

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、これらの鍵と、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 IBM i アプリケーションが、クライアント認証用の証明書をサポートしています。

- Telnet サーバー
- IBM HTTP Server for i (powered by Apache)
- IBM Tivoli® Directory Server for IBM i
- IBM i Access for Windows (System i 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。この鍵は、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鍵には、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鍵を使用すると、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。

関連概念:

43 ページの『SSL セキュア通信のためのディジタル証明書』
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。

関連資料:

60 ページの『API を使用して証明書を IBM i ユーザー以外のユーザーへプログラマチックに発行する』
ローカル CA では、証明書と IBM i ユーザー・プロファイルを関連付けずに、ユーザーに秘密証明書を発行することができます。

ディジタル証明書とエンタープライズ識別マッピング

エンタープライズ識別マッピング (EIM) およびディジタル証明書マネージャー (DCM) を一緒に使用すると、EIM マッピングのルックアップ操作のソースとして証明書を適用し、証明書から同じ EIM ID と関連付けられているターゲット・ユーザー ID へとマップします。

EIM では、ユーザー・プロファイルやユーザー証明書など、企業内のユーザー ID を管理することができます。ユーザー名およびパスワードは、ユーザー ID の最も一般的な形式ですが、証明書も別の形式のユーザー ID です。アプリケーションの中には、ユーザー名やパスワードではなく、ユーザー証明書によってユーザーの認証を行うように構成できるものもあります。

EIM を使用すれば、ユーザー ID 間にマッピングを作成して、必要なユーザー ID を提供しなくても、ユーザーが 1 つのユーザー ID によって認証を受け、別のユーザー ID の資源にアクセスできるようになります。 EIM でこれを実現するためには、ユーザー ID 間にアソシエーションを定義する必要があります。ユーザー ID にはさまざまな形式があり、ユーザー証明書もその 1 つです。また、EIM ID と、その EIM ID が表すユーザーに属するさまざまなユーザー ID との間に、それぞれアソシエーションを作成することもできます。また、ポリシーのアソシエーションを作成して、ユーザー ID のグループを、1 つのターゲット・ユーザー ID にマップさせることもできます。ユーザー ID にはさまざまな形式があり、ユーザー証明書もその 1 つです。これらのアソシエーションを作成すると、ユーザー証明書は、適切な EIM ID へとマップされるので、証明書を使用した認証が容易になります。

この EIM フィーチャーを利用してユーザー証明書を管理するには、DCM 構成タスクを実行する前に、以下の EIM 構成タスクを実行する必要があります。

1. **System i ナビゲーター** の「**EIM 構成**」ウィザードを使用して、EIM を構成します。
2. EIM に加えたいユーザーそれぞれについて、EIM ID を作成します。
3. EIM ID と、ローカルの IBM i ユーザー・レジストリーにあるそのユーザーのユーザー・プロファイルごとに、ターゲット・アソシエーションを作成し、DCM によってユーザーが割り当てた、または DCM で作成したユーザー証明書が、ユーザー・プロファイルにマップされるようにします。 「**EIM 構成**」ウィザードで指定したローカルの **IBM i** ユーザー・レジストリーに対して、EIM レジストリー定義名を使用します。

必要な EIM 構成タスクが完了したら、「**LDAP 位置の管理 (Manage LDAP Location)**」タスクを使用して、ディジタル証明書マネージャー (DCM) を構成し、ユーザー証明書をユーザー・プロファイル付きではなく、Lightweight Directory Access Protocol (LDAP) 位置に保管します。 EIM と DCM が連携するように構成すると、ユーザー証明書の「**証明書の作成 (Create Certificate)**」タスクと、「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクは、証明書をユーザー・プロファイルに割り当てる代わりに、EIM 使用のために証明書を処理します。 DCM は、構成された LDAP ディレクトリーに証明書を保管し、証明書の識別名 (DN) 情報を使用して、適切な EIM ID に対してソースとなるアソシエーションを作成します。これにより、オペレーティング・システムおよびアプリケーションは、 EIM マッピングのルックアップ操作のソースとして証明書を使用し、証明書から同じ EIM ID で関連付けられているターゲット・ユーザー ID へとマップします。

さらに、EIM と DCM が連携するように構成を行う場合、 DCM を使用して、システム・レベルだけではなくエンタープライズ・レベルでも、有効期限によるユーザー証明書を確認できます。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

関連タスク:

58 ページの『有効期限によるユーザー証明書の管理』
ディジタル証明書マネージャー (DCM) では、証明書の有効期限の管理がサポートされています。これによって管理者は、ローカル IBM i モデルにあるユーザー証明書の有効期限を確認できます。DCM の持つユーザー証明書の有効期限の管理サポートと、エンタープライズ識別マッピング (EIM) を組み合わせて使用することで、管理者は DCM を使用して、ユーザー証明書の有効期限をエンタープライズ・レベルで確認できます。

91 ページの『ユーザー証明書の LDAP 位置の管理』
ディジタル証明書マネージャー (DCM) を使用すると、Lightweight Directory Access Protocol (LDAP) サーバーのディレクトリー位置に、ユーザー証明書を保管することができます。これによって、エンタープライズ識別マッピングを拡張して、ユーザー証明書を処理できるようになります。

関連情報:

EIM Information Center のトピック

VPN 接続のディジタル証明書

IBM i 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。

IKE サーバーが、互いを認証するために使用する方法の 1 つとして、事前共用鍵があります。ただし、事前共用鍵を使用する方法は、この鍵を、VPN のもう一方のエンドポイントにいる管理者に手動で送る必要があるため、それほどセキュアとは言えません。鍵を送るプロセスで、その鍵が他者の目に触れる可能性があるためです。

事前共用鍵を使用せず、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、秘密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 のローカル 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名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、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。

関連概念:

62 ページの『公開インターネット CA からの証明書の管理』
ディジタル証明書マネージャー (DCM) を使用して、公開インターネット CA から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、特殊鍵データベース・ファイルです。

関連タスク:

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

84 ページの『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。

関連情報:

VPN を構成する

オブジェクトに署名するためのディジタル証明書

IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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 IBM i モデルのツールを強化したものです。従来の制御機能では、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オブジェクトが転送されている間や、IBM i プラットフォーム以外のシステムにオブジェクトが保管されている間に、無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、公開証明書と秘密証明書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、既知の公開認証局 (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発行する、という方法も考えられます。ローカル CA から取得した秘密証明書を使用してオブジェクトに署名する方が、既知の公開 CA から証明書を購入するよりも、コストを抑えることができます。

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 (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、DCM を使用してください。また、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証したりすることができます。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

『オブジェクトの署名検査のためのディジタル証明書』
IBM i は、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送信元からのものであることを確認する場合は、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。

関連タスク:

95 ページの『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。

65 ページの『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。

67 ページの『オブジェクトの署名検査のための証明書の管理』
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。

オブジェクトの署名検査のためのディジタル証明書

IBM i は、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送信元からのものであることを確認する場合は、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。ある認証局 (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、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。

復元時のオブジェクト署名の検証 (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、復元時のオブジェクト署名の検証 (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、いろいろな種類があります。このシステム値は、復元中の実行可能オブジェクトにだけ影響を与えるもので、保管ファイルや統合ファイルシステムの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、 IBM i 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。 また、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証したりすることができます。

関連概念:

48 ページの『オブジェクトに署名するためのディジタル証明書』
IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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。

関連情報:

システム値ファインダー

QVFYOBJRST システム値

DCM の構成

ディジタル証明書マネージャー (DCM) には、ブラウザー・ベースのユーザー・インターフェースが備わっており、アプリケーションおよびユーザーのディジタル証明書の管理および構成に使用できます。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**」は、「証明書の表示」、「証明書の更新」、「証明書のインポート」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・フレーム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、IBM i 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、IBM i 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。

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ディジタル証明書を使用する場合の詳細については、VeriSign の 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。VeriSign ヘルプ・デスク (VeriSign Help Desk) で、このライブラリーにアクセスすることができます。

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) の機能を使用するには、まずシステムで 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. ディジタル証明書マネージャーをインストールします。
2. IBM HTTP Server for i をインストールします。
3. 以下のように System i ナビゲーターナビゲーターを使用して、HTTP Server 管理サーバーを開始します。
   a. System i ナビゲーターで、「**システム (system)**」 > 「**ネットワーク**」 > 「**サーバー**」 > 「**TCP/IP**」と展開します。
   b. 「**HTTP 管理 (HTTP Administration)**」を右クリックします。
   c. 「**開始**」を選択します。
4. Web ブラウザーを開いて http://your_system_name:2001 と入力し、IBM Navigator for i Web コンソールをロードします。
5. ウェルカム・ページから「**IBM i タスク・ページ**」リンクをクリックします。
6. 「IBM i タスク (Tasks)」ページにある製品リストから、「**ディジタル証明書マネージャー**」を選択して、DCM ユーザー・インターフェースにアクセスします。

関連概念:

14 ページの『シナリオ : 証明書を使用して外部の認証を行う』
このシナリオでは、公開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に対して一般ユーザーアクセスする際に、そのアクセスを保護および制限する認証メカニズムとして証明書を使用するタイミングとその使用方法について説明します。

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、処理する証明書ストアの種類 (ある場合) と、ユーザー・プロファイルの特殊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。 DCM を使用してオブジェクトの署名を検証するには、ユーザー・プロファイルに *AUDIT 特殊権限が必要です。

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、証明書ストアが存在しません。そのため、最初に DCM にアクセスしたとき、必要な特殊権限がある場合には、ナビゲーション画面に以下のタスクだけが表示されます。

- 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秘密ローカル 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。
- LDAP 位置の管理 (Manage LDAP Location)。
- PKIX 要求場所の管理。
- 「IBM i タスク (IBM i Tasks)」ページへの戻り。

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。DCM が表示するタスクまたはカテゴリーは、オープンしている証明書ストアおよびユーザー・プロファイルの特殊権限によって異なります。

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・ウィンドウを表示させ、Secure Sockets Layer (SSL) 使用によるセキュア接続を開始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 i 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、秘密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。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

ローカル CA の作成および運用

ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

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 i で証明書を使用する場合は、DCM で作業する前に、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。 DCM を使用してこのアプリケーションが SSL 用に使用する証明書を指定できるように、このアプリケーション ID をメモに控えておく必要があります。

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 の作成および運用を行うには、以下のステップに従ってください。

1. DCM を開始します。『DCM の開始』を参照してください。
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。これらのフォームのガイドに従って、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、および署名検査用のディジタル証明書を使用するために必要となるタスクを完了させるプロセスを実行します。

   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、稼働させるローカル認証局 (CA) のセットアップに必要なすべてのタスクを実行させるには、以下の手順を実行します。
   a. ローカル CA 証明書の秘密鍵の保管方法を選択します。 (このステップが該当するのは、IBM 暗号化コプロセッサーが、ご使用のシステムにインストールされ、装置記述がオンに変更されている場合のみです。オンに変更された暗号装置記述がない場合、DCM は証明書とその秘密鍵を、ローカル認証局 (CA) 証明書ストアに自動的に保管します。)
   b. ローカル CA の識別情報を指定します。
   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、ソフトウェアがそのローカル CA を認識し、その CA が発行する証明書の妥当性検査を実行できるようにします。
   d. ローカル CA 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、SSL 接続用にアプリケーションが使用可能なサーバー証明書またはクライアント証明書を発行します。 (システムに、IBM 暗号化コプロセッサーがインストールされ、オンに変更されている場合、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、オブジェクトにディジタル署名するためにアプリケーションが使用可能な、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 を信頼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 を使用したセキュア通信を行うアプリケーションを構成するために必要なものが、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、サーバーの ID 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されるクライアント・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、ネットワーク内の他の IBM i モデル上のアプリケーションに対して、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詳しくは、以下のトピックを参照してください。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

47 ページの『VPN 接続のディジタル証明書』
IBM i 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。

55 ページの『ユーザー証明書の管理』
ディジタル証明書マネージャー (DCM) を使用して、SSL を伴う証明書を取得したり、既存の証明書を IBM i ユーザー・プロファイルに関連付けることができます。

関連タスク:

71 ページの『ローカル CA を使用して他の IBM i モデルの証明書を発行』
ディジタル証明書マネージャー (DCM) を使用すると、あるシステム上に秘密ローカル CA を構成して、他の IBM i プラットフォームで使用する証明書を発行することができます。

61 ページの『秘密 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。

93 ページの『オブジェクトへの署名』
オブジェクトには、3 つの異なる方法で署名することができます。オブジェクト署名 API を呼び出すプログラムを作成する方法、ディジタル証明書マネージャー (DCM) を使用する方法、他のシステムに配布するパッケージに対して System i ナビゲーター のマネージメント・セントラル機能を使用する方法のいずれかを使って、オブジェクトに署名することができます。

関連資料:

60 ページの『API を使用して証明書を IBM i ユーザー以外のユーザーへプログラマチックに発行する』
ローカル CA では、証明書と IBM i ユーザー・プロファイルを関連付けずに、ユーザーに秘密証明書を発行することができます。

ユーザー証明書の管理:

ディジタル証明書マネージャー (DCM) を使用して、SSL を伴う証明書を取得したり、既存の証明書を IBM i ユーザー・プロファイルに関連付けることができます。

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、ユーザーのソフトウェアは、既にその CA 証明書のコピーを持っている可能性があります。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、サーバーが秘密ローカル CA からの証明書を使用している場合、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。ユーザーは、セキュリティー・ニーズに応じて、公開インターネット CA から取得した証明書を提示することもできますし、ユーザーが運用しているローカル CA から取得した証明書を提示することもできます。サーバー・アプリケーションが、現在、IBM i 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、IBM i 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・フレーム内の「**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することができます。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、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で、自身のユーザー・プロファイルの特殊権限とは無関係に、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。

関連タスク:

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

61 ページの『秘密 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。

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) を使用して秘密ローカル認証局 (CA) を運用する場合は、そのローカル CA を使用し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 によるユーザー証明書の発行が、CA ポリシーによって許可されている必要があります。

ローカル CA から証明書を取得するには、以下のステップを実行します。

1. DCM を開始します。『DCM の開始』を参照してください。
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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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鍵を生成した後、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IBM i 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、自分のユーザー・プロファイルに証明書を割り当てることができます。

関連概念:
41 ページの『公開証明書と秘密証明書』
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、秘密 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。

関連タスク:

『ユーザー証明書の割り当て』
IBM i ユーザー・プロファイルまたはその他のユーザー ID に、所有するユーザー証明書を割り当てることができます。証明書は、別のシステム上の秘密ローカル CA から得られたものでも、既知のインターネット CA から得られたものでも構いません。証明書をご使用のユーザー ID に割り当てる前に、発行元 CA はサーバーによって承認されている必要があり、証明書は、そのシステムにあるユーザー・プロファイルまたはその他のユーザー ID に、まだ関連付けられてはなりません。

61 ページの『秘密 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。

ユーザー証明書の割り当て:

IBM i ユーザー・プロファイルまたはその他のユーザー ID に、所有するユーザー証明書を割り当てることができます。証明書は、別のシステム上の秘密ローカル CA から得られたものでも、既知のインターネット CA から得られたものでも構いません。証明書をご使用のユーザー ID に割り当てる前に、発行元 CA はサーバーによって承認されている必要があり、証明書は、そのシステムにあるユーザー・プロファイルまたはその他のユーザー ID に、まだ関連付けられてはなりません。

ユーザーによっては、外部の認証局 (CA) や、異なる iSeries® システムにあるローカル CA が発行した証明書を所有していることがあります。管理者としては、それらの証明書をディジタル証明書マネージャー (DCM) で利用できるようにしたいと考えます。この場合、管理者とエンド・ユーザーは、DCM を使用してこれらの証明書を管理することができ、証明書はクライアント認証のために使用される場合がほとんどです。「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクは、外部の CA が発行した証明書について、ユーザーが DCM 割り当てを作成できるようにする機能です。

ユーザーが証明書を割り当てる場合、DCM では、割り当てられた証明書を処理する以下の 2 つの方法のうち 1 つを行います。

- ユーザーのユーザー・プロファイルがある IBM i に、ローカルで証明書を保管する方法。LDAP 位置が DCM に対して定義されていない場合、「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを使用して、外部の証明書を、IBM i ユーザー・プロファイルに割り当てることができます。証明書をユーザー・プロファイルに割り当てれば、クライアント認証に証明書を必要とするシステムのアプリケーションで、証明書が使用できるようになります。
- エンタープライズ識別マッピング (EIM) で使用するために、 Lightweight Directory Access Protocol (LDAP) 位置に証明書を保管する方法。定義済みの LDAP 位置があり、IBM i モデルが EIM に加えられるように構成されている場合は、「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを使用することで、指定された LDAP ディレクトリーに、ユーザーが外部の証明書のコピーを保管できます。また、DCM は、その証明書用に EIM にソースとなるアソシエーションを作成します。この方法で証明書を保管すれば、EIM 管理者は、EIM に加えられている有効なユーザー ID として、その証明書を認識できます。

  注: ユーザーが、EIM 構成にあるユーザー ID に証明書を割り当てる前に、EIM は、そのユーザーに対して正しく構成されている必要があります。この EIM 構成には、そのユーザーの EIM ID の作成、および EIM ID とユーザー・プロファイルの間のターゲット・アソシエーションの作成が含まれます。 これらが構成されていないと、DCM は、その証明書の EIM ID と対応するソース・アソシエーションを作成できません。

「**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、以下の要件を満たしている必要があります。

1. HTTP Server とのセキュア・セッションを介して DCM へアクセスできる。

   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に求めるプロンプトが、DCM から出されます。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、ブラウザーから、HTTP Server を識別する証明書を発行した認証局 (CA) を承認するかどうかについて、ブラウザーからプロンプトが出されることがあります。また、ブラウザーから、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が出されることもあります。
2. クライアント認証のために証明書を提供できる。

   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。
3. タスクを実行しているユーザーのユーザー ID とまだ関連付けられていない証明書がブラウザーにある。 (または、DCM が EIM と連携するように構成されている場合は、ユーザーは DCM の LDAP 位置にまだ保管されていない証明書を、ブラウザーに入れておく必要があります。)

   セキュア・セッションを確立すると、DCM はユーザー ID 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 ID 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 ID と関連付けられている可能性があります。

関連タスク:

56 ページの『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) を使用して秘密ローカル認証局 (CA) を運用する場合は、そのローカル CA を使用して証明書を各ユーザーに発行できます。

103 ページの『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』
ディジタル証明書マネージャー (DCM) を使用してユーザー証明書を割り当てる際に、発生する可能性がある問題をトラブルシューティングする際には、以下のステップが役に立ちます。

関連情報:

EIM Information Center の概要

有効期限によるユーザー証明書の管理:

ディジタル証明書マネージャー (DCM) では、証明書の有効期限の管理がサポートされています。これによって管理者は、ローカル IBM i モデルにあるユーザー証明書の有効期限を確認できます。DCM の持つユ

ーザー証明書の有効期限の管理サポートと、エンタープライズ識別マッピング (EIM) を組み合わせて使用することで、管理者は DCM を使用して、ユーザー証明書の有効期限をエンタープライズ・レベルで確認できます。

エンタープライズ・レベルで、ユーザー証明書の有効期限サポートを利用するためには、EIM がエンタープライズに構成される必要があり、また EIM に、ユーザー証明書に関する適切なマッピング情報が必要です。ユーザー自身のユーザー・プロファイルに関連付けられたもの以外のユーザー証明書の有効期限を確認するには、 *ALLOBJ および *SECADM 特殊権限が必要です。

DCM を使用して、有効期限に基づいて証明書を表示すると、期限切れが近づいている証明書をす早く容易に見分けることができ、期限内に証明書を更新することができます。

有効期限に基づいて、ユーザー証明書を表示したり管理したりするには、以下のステップに従ってください。

1. DCM を開始します。『DCM の開始』を参照してください。

   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、「**ユーザー証明書の管理 (Manage User Certificates)**」を選択して、タスクのリストを表示します。

   注: 証明書ストアで作業中の場合は、「**証明書の管理 (Manage Certificates)**」を選択してタスクのリストを表示し、「**有効期限の確認 (Check expiration)**」を選択してから、「**ユーザー**」を選択します。
3. ユーザー・プロファイルに *ALLOBJ および *SECADM 特殊権限がある場合は、有効期限に基づいて、表示したり管理したりするユーザー証明書の種類を選択することができます。 (ユーザー・プロファイルにこれらの特殊権限がない場合、次のステップにあるように、有効期限の期間を指定するように求めるプロンプトが DCM から出されます。) 以下から 1 つを選択してください。
   - 特定の IBM i ユーザー・プロファイルに割り当てられたユーザー証明書を表示および管理する「**ユーザー・プロファイル (User profile)**」。「**ユーザー・プロファイル名 (User profile name)**」を指定し、「**続行**」をクリックします。

     注: *ALLOBJ および *SECADM 特殊権限がある場合にのみ、ユーザー自身のユーザー・プロファイル以外のユーザー・プロファイルを指定できます。
   - すべてのユーザー ID のユーザー証明書を表示および管理する「**すべてのユーザー証明書 (All user certificates)**」。
4. 「**有効期限の日数 (1 から 365) (Expiration date range in days (1-365))**」フィールドで、有効期限に基づいて、ユーザー証明書を表示する日数を入力し、「**続行**」をクリックします。今日の日付から指定された日数の日付までの間に期限切れとなる、指定されたユーザー・プロファイルのユーザー証明書すべてが表示されます。また、DCM は今日までに期限切れとなっているユーザー証明書もすべて表示します。
5. 管理するユーザー証明書を選択します。証明書の詳細情報を表示させたり、関連するユーザー ID からその証明書を除去したりすることができます。
6. リストの証明書について処理を終えたら、「**キャンセル**」をクリックしてタスクを終了します。

関連タスク:

46 ページの『ディジタル証明書とエンタープライズ識別マッピング』
エンタープライズ識別マッピング (EIM) およびディジタル証明書マネージャー (DCM) を一緒に使用すると、EIM マッピングのルックアップ操作のソースとして証明書を適用し、証明書から同じ EIM ID と関連付けられているターゲット・ユーザー ID へとマップします。

85 ページの『有効期限による証明書の管理』
ディジタル証明書マネージャー (DCM) では、証明書の有効期限の管理がサポートされています。これによって管理者は、サーバーまたはクライアントの証明書、オブジェクト署名証明書、認証局証明書、およびユーザー証明書を、ローカル・システム上の有効期限によって管理できます。

関連情報:

EIM Information Center の概要

API を使用して証明書を IBM i ユーザー以外のユーザーへプログラマチックに発行する:

ローカル CA では、証明書と IBM i ユーザー・プロファイルを関連付けずに、ユーザーに秘密証明書を発行することができます。

ユーザー証明書要求生成/署名 (QYCUGSUC) API およびユーザー証明書要求署名 (QYCUSUC) API を使用すると、IBM i ユーザー以外のユーザーに証明書をプログラマチックに発行することができます。証明書を IBM i ユーザー・プロファイルに関連付けることで、特に社内ユーザーの場合にはメリットが生じます。しかし、こ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 IBM i ユーザー・プロファイルを割り当てたくない場合には)、あまり実用的ではありません。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ようにするには、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が必要な場合に、ユーザーに、既知の CA から証明書を購入してもらう必要があります。

これら 2 つの API が提供するサポートにより、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、任意のユーザー名に対して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 をホストするシステム上に存在する必要がなく、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、計 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呼び出すことができます。ユーザーが作成するアプリケーションでは、グラフィカル・ユーザー・インターフェース (GUI) コードを用意しておく必要があります。これは、ユーザー証明書を作成したり、ローカル CA を使用して証明書に署名するための適切な API を呼び出したりする際に、必要となります。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

44 ページの『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。

関連タスク:

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

関連情報:

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

秘密 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、ブラウザーまたはその他のクライアント・ソフトウェアは、既にその CA 証明書のコピーを取得している可能性があります。しかし、秘密ローカル CA からの証明書をサーバーが提示した場合には、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できますし、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・ソフトウェアからのアクセスと使用が可能になるようにすることもできます。ブラウザーとその他のアプリケーションを、セキュア通信用に両方とも使用する場合、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しなくてはならない場合があります。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。

サーバー・アプリケーションで、ローカル CA からの証明書を提示して自分自身を認証することが求められた場合、ローカル CA 証明書を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を要求する必要があります。

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。『DCM の開始』を参照してください。
2. ナビゲーション・フレームにある「**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、ブラウザーへのローカル CA 証明書のダウンロードや、システム上のファイルへの保管を行う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。システムのローカル CA ごとに、2 つのリンクがあります。
   a. 「**証明書のインストール (Install certificate)**」を選択して、そのローカル 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、そのローカル CA 証明書を特別にコード化したコピーが組み込まれた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、認証用に使用できるようにするには、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、アプリケーションを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。

関連概念:

55 ページの『ユーザー証明書の管理』
ディジタル証明書マネージャー (DCM) を使用して、SSL を伴う証明書を取得したり、既存の証明書を IBM i ユーザー・プロファイルに関連付けることができます。

関連タスク:

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

56 ページの『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) を使用して秘密ローカル認証局 (CA) を運用する場合は、そのローカル CA を使用して証明書を各ユーザーに発行できます。

公開インターネット CA からの証明書の管理

ディジタル証明書マネージャー (DCM) を使用して、公開インターネット CA から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、特殊鍵データベース・ファイルです。

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。

DCM のガイド・タスクを使用すると、これらの公開証明書、およびそれら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署名の認証性の検査を行うアプリケーションについて、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、特殊鍵データベース・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。

注: 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。
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。

関連概念:

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

47 ページの『VPN 接続のディジタル証明書』
IBM i 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。

関連タスク:

91 ページの『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。

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。『DCM の開始』を参照してください。
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、一連のフォームに入力します。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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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**」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: ユーザーのシステムに、IBM 暗号化コプロセッサーがインストールされてオンに変更されている場合、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。

   システムの HTTP Server 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。DCM を使用してこのアプリケーションが SSL 用に使用する証明書を指定できるように、このアプリケーション ID をメモに控えておきます。

   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 certificate)**」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、*SYSTEM 証明書ストアの使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込むようにする場合は、アプリケーションの

CA 信頼リストを定義して、*SYSTEM ストアから信頼する CA を選択する必要があります。この信頼リストにより、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。 CA 信頼リストが定義されていない場合は、*SYSTEM 証明書ストア内のすべての使用可能な CA 証明書が信頼されます。

ガイド・タスクを完了すると、SSL を使用したセキュア通信を行うアプリケーションを構成するために必要なものが、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。証明書が既知のインターネット 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、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、System i ナビゲーター 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。『DCM の開始』を参照してください。
2. DCM の左側にあるナビゲーション・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、一連のフォームに入力します。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. 左側のナビゲーション・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 certificate)**」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. 左側のナビゲーション・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が配布された場合、このオブジェクトの受信側は、OS/400® V5R1 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、データが変更されていないことの確認と、送信側の ID の検証を行う必要があります。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。既知のインターネット 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可能性があります。ただし、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こともできます。たとえば、秘密ローカル 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。

関連概念:

48 ページの『オブジェクトに署名するためのディジタル証明書』
IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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。

関連タスク:

95 ページの『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。

93 ページの『オブジェクトへの署名』
オブジェクトには、3 つの異なる方法で署名することができます。オブジェクト署名 API を呼び出すプログラムを作成する方法、ディジタル証明書マネージャー (DCM) を使用する方法、他のシステムに配布するパッケージに対して System i ナビゲーター のマネージメント・セントラル機能を使用する方法のいずれかを使って、オブジェクトに署名することができます。

オブジェクトの署名検査のための証明書の管理:

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、既知の

CA からの CA 証明書のコピーを提供しています。ただし、別の公開 CA または秘密ローカル CA の証明書によってオブジェクトが署名されている場合、オブジェクトの署名を検査するためには、あらかじめ CA 証明書のコピーを取得しておく必要があります。

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、証明書ストアを既知の公開 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。『DCM の開始』を参照してください。
2. DCM の左側にあるナビゲーション・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、一連のフォームに入力します。

   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**」を選択して、「**続行**」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。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 certificate)**」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。署名検査証明書をインポートする前に、CA 証明書をインポートしていない場合は、署名検査証明書のインポート時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。

関連概念:

48 ページの『オブジェクトに署名するためのディジタル証明書』
IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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。

関連タスク:

95 ページの『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。

既存の証明書の更新

ディジタル証明書マネージャー (DCM) が使用する証明書の更新プロセスは、証明書を発行する認証局 (CA) のタイプによって異なります。

ローカル CA またはインターネット CA を使用して証明書を更新できます。

ローカル CA から証明書を更新する

ローカル CA を使用して、更新された証明書に署名する場合、DCM は、新しい証明書を作成するためにユーザーが現行の証明書ストアに提供した情報を使用し、以前の証明書は保存します。

ローカル CA を使用して証明書を更新するには、以下のステップに従います。

1. 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、更新する証明書を保管する証明書ストアを選択します。
2. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択します。
3. ナビゲーション・フレームで、「**証明書の更新 (Renew certificate)**」を選択します。
4. 更新する証明書を選択して、「**更新**」をクリックします。
5. 「**ローカル認証局 (CA)**」を選択して、「**続行**」をクリックします。
6. 証明書識別フォームを完成します。「**新規証明書ラベル**」フィールドを変更する必要がありますが、その他のフィールドは、そのままで構いません。
7. 更新済み証明書が使用するアプリケーションを選択して、「**続行**」をクリックし、証明書の更新を終了します。

   注: 証明書を使用するアプリケーションを選択する必要はありません。

インターネット CA から証明書を更新する

既知のインターネット CA を使用して証明書を発行する場合、2 つの方法で証明書の更新を処理できます。

インターネット CA を使用して証明書を直接更新して、署名 CA から受信するファイルから更新済み証明書をインポートできます。証明書を更新するには、もう 1 つ方法があります。DCM を使用して、新規の公開鍵と秘密鍵のペアおよび証明書の証明書署名要求 (CSR) を作成した後に、この情報をインターネット CA に送信して、新規証明書を取得する、という方法です。この証明書を CA から受信すると、更新処理を完了できます。

インターネット CA から直接取得した証明書のインポートおよび更新:
インターネット CA から直接取得した証明書をインポートおよび更新するには、以下のステップに従います。

1. 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、更新する証明書を保管する証明書ストアを選択します。

   注: パネルについて不明な点がある場合は、パネルの「?」をクリックすると説明が表示されます。
2. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択します。
3. ナビゲーション・フレームで、「**証明書の更新 (Renew certificate)**」をクリックします。
4. 更新する証明書を選択して、「**更新**」をクリックします。
5. 「**VeriSign**」またはその他の「**インターネット認証局 (CA)**」を選択して、「**続行**」をクリックします。
6. 「**いいえ - 既存ファイルから更新された署名済み証明書をインポートしてください**」を選択します。
7. ガイド・タスクを完了して、証明書をインポートします。 発行側の CA により証明書を直接更新することを選択すると、その CA は更新済みの証明書をファイルで戻します。証明書のインポート時に証明書が保管されるサーバー上のファイルの正しい絶対パスを必ず指定してください。更新済みの証明書が入るファイルは、任意の統合ファイル・システム (IFS) ディレクトリーに保管できます。
8. 「**OK**」をクリックしてタスクを終了します。

証明書の新規の公開鍵と秘密鍵のペアおよび CSR を作成することによって、証明書を更新する:
証明書の新規の公開鍵と秘密鍵のペアおよび CSR を作成することによって、インターネット CA で証明書を更新するには、以下のステップに従います。

1. 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、更新する証明書を保管する証明書ストアを選択します。

   注: パネルについて不明な点がある場合は、パネルの「?」をクリックすると説明が表示されます。
2. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択します。
3. ナビゲーション・フレームで、「**証明書の更新 (Renew certificate)**」をクリックします。
4. 更新する証明書を選択して、「**更新**」をクリックします。
5. 「**VeriSign**」またはその他の「**インターネット認証局 (CA)**」を選択して、「**続行**」をクリックします。
6. 「**はい - この証明書の新規鍵ペアを作成してください**」をクリックし、「**続行**」をクリックします。
7. 証明書識別フォームを完成します。「新規証明書ラベル」フィールドを変更する必要がありますが、その他のフィールドは、そのままで構いません。注: タスクの完了について不明な点がある場合は、パネルの「?」をクリックすると、説明が表示されます。
8. 「**OK**」をクリックしてタスクを終了します。

証明書のインポート

ディジタル証明書マネージャー (DCM) を使用すると、システム上のファイル内にある証明書をインポートすることができます。また、現行のサーバーで証明書を再作成するのではなく、別のサーバーから証明書をインポートすることもできます。

たとえば、システム A でローカル CA を使用して、リテール Web アプリケーションの証明書を作成し、SSL 接続の開始に使用したとします。ここ最近の業務拡張に伴い、この非常にビジーなリテール・アプリケーションのインスタンスをより多くホストするために、新規の IBM i モデル (システム B) をインストールしました。リテール・アプリケーションのすべてのインスタンスで同一の証明書を使用し、これらを識別し、SSL 接続を開始させます。そこで、システム A のローカル CA を使用して、システム B 用に新たな証明書を作成して使用する代わりに、ローカル CA 証明書およびサーバー証明書の両方を、システム A からシステム B にインポートすることにしました。

以下のステップに従い、DCM を使用して、証明書をインポートします。

1. 左のナビゲーション・ペインで、「**証明書ストアの選択 (Select a Certificate Store)**」をクリックして、証明書をインポートする証明書ストアを選択します。 証明書をインポートする証明書ストアには、他のシステムでエクスポートした証明書と同じタイプの証明書が含まれている必要があります。例えば、サーバー証明書 (タイプ) をインポートしている場合、この証明書を、*SYSTEM などのサーバー証明書を格納する証明書ストア、またはその他のシステム証明書ストアにインポートします。
2. ナビゲーション・フレームで、「**証明書の管理 (Manage Certificates)**」を選択します。
3. ナビゲーション・フレームで、「**証明書のインポート (Import certificate)**」を選択します。
4. インポートする証明書のタイプを選択して、「**続行 (Continue)**」をクリックします。インポートしている証明書のタイプは、エクスポートした証明書のタイプと同じである必要があります。例えば、サーバー証明書をエクスポートした場合、サーバー証明書のインポートを選択します。

   注: DCM が、pkcs12 形式で証明書をエクスポートする場合、発行 CA は、エクスポートされた証明書のチェーンに含まれるため、DCM により証明書自体が証明書ストアにインポートされる場合に自動的にインポートされます。ただし、証明書が、pkcs12 形式でエクスポートされず、インポート先の証明書ストアに CA 証明書がない場合、証明書のインポート前に発行 CA 証明書をインポートする必要があります。
5. ガイド・タスクを完了して、証明書をインポートします。証明書をインポートする場合、サーバー上で証明書が保管されている正しい絶対パスを指定していることを確認してください。

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 IBM i モデルの証明書を発行

ディジタル証明書マネージャー (DCM) を使用すると、あるシステム上に秘密ローカル CA を構成して、他の IBM i プラットフォームで使用する証明書を発行することができます。

ネットワーク内のシステムで、すでに秘密ローカル認証局 (CA) を使用していると仮定します。このローカル CA の使用範囲を、ネットワーク内の別のシステムにまで広げることにします。たとえば、別のシステムのアプリケーションに対して、現行ローカル CA からサーバー証明書またはクライアント証明書を発

行し、SSL 通信セッションを使用可能にしたいという場合があります。あるいは、あるシステム上にあるローカル CA の証明書を使用して、別のサーバーに保管されているオブジェクトに署名したいという場合もあります。

このような目標は、DCM を使用することで実現できます。ローカル CA を運用しているシステムで、必要なタスクの一部を実行します。残りのタスクは、証明書の発行先となるアプリケーションをホストする 2 次システムで実行します。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。

ローカル CA を使用して、他のシステムに証明書を発行することができます。この証明書は、オブジェクトに署名する際や、アプリケーションで SSL セッションを確立する際に、使用することができます。ローカル CA を使用して、別の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 証明書のコピーに加えて、さまざまな公開インターネット CA の証明書が組み込まれます。

DCM で実行する必要があるタスクは、ローカル CA が発行する証明書のタイプと、ターゲット・システムのリリース・レベルおよび条件によって若干変化します。

別の IBM i モデルで使用する秘密証明書の発行

ローカル CA を使用して、別の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。『DCM の開始』を参照してください。
2. ナビゲーション・フレームにある「**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。

   注: 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するには、このシステムにローカル CA が存在していなければなりません。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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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、開始されたガイド・タスクで一連のフォームに入力します。
4. 「**別の IBM i 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 IBM i)**」(SSL セッションの場合)、または「**別の IBM i のためのオブジェクト署名証明書 (object signing certificate for another IBM i)**」(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。
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ラベルおよび固有のファイル名を必ず指定してください。固有の証明書ラ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。

   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。

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。

関連概念:

38 ページの『DCM データのバックアップおよび回復に関する考慮事項』
ディジタル証明書マネージャー (DCM) の証明書ストアにアクセスする際に使用する、暗号化された鍵データベースのパスワードは、システムの特別なセキュリティー・ファイルに保管、つまり隠されています。DCM を使用してシステムに証明書ストアを作成すると、DCM は、自動的にユーザー用のパスワードを知られないように隠しておきます。ただし、状況によっては、DCM が証明書ストアのパスワードを隠しておくように手動で処理する必要があります。

41 ページの『公開証明書と秘密証明書』
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、秘密 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。

関連タスク:

52 ページの『ローカル CA の作成および運用』
ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

SSL セッションのための秘密証明書の使用

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。 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 証明書ストアがターゲット・システムに存在する場合、 転送済み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、または転送済みファイルを既存の *SYSTEM 証明書ストアにインポートすることができます。

***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 つ) が、/QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリー内にあることを確認してください。
2. 転送証明書ファイルが /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、これらのコピーの作成時に、ローカル CA 証明書のコピーと共に、そのコピーを証明書ストア・ファイルに追加しています。

アテンション: すでにターゲット・システムの /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに 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、転送されたファイルの名前を指示どおりに変更しないでください。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、必ず、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)」ページが表示されたら、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**」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証明書を使用するアプリケーションを選択し、「**続行**」をクリックします。DCM は、そのアプリケーションに選択した証明書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は、*SYSTEM 証明書ストアの使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込むようにする場合があります。 この構成を行うには、アプリケーションに CA 信頼リストを定義 して、*SYSTEM ストアから信頼する使用可能な CA を選択する必要があります。 CA 信頼リストが定義されていない場合は、*SYSTEM 証明書ストア内のすべての使用可能な CA 証明書が信頼されます。

これらのタスクが完了すると、ターゲット・システムのアプリケーションは、別のシステムのローカル CA により発行された証明書を使用できるようになります。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 証明書をユーザーの 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か、いずれかを行う必要があります。どちらを行うかについては、SSL 対応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:**
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、ターゲット・システムに転送した証明書ファイルの処理方法を決定する必要があります。 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、既存の *SYSTEM 証明書ストアに秘密証明書およびそれに対応するローカル CA 証明書をインポートするように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)」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、ユーザーまたは他の人が作成した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 i アプリケーション (およびその他のさまざまなソフトウェア・デベロッパーが作成したアプリケーション) 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 IBM i SSL 対応アプリケーションを構成することはできません。IBM i 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する必要があります。

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、これにアクセスして処理するには、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 (.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、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:***
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・ファイルから証明書を既存の *SYSTEM 証明書ストアにインポートする必要があります。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、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、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。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。

   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。
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: サーバー証明書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には、まずローカル 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**」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証明書を使用するアプリケーションを選択し、「**続行**」をクリックします。 DCM は、そのアプリケーションに選択した証明書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は、*SYSTEM 証明書ストアの使用可能な CA 証明書のリストから、信頼する CA 証明書の定義を絞り込むようにする場合があります。 この構成を行うには、アプリケーションに CA 信頼リストを定義 して、*SYSTEM ストアから信頼する使用可能な CA を選択する必要があります。CA 信頼リストが定義されていない場合は、*SYSTEM 証明書ストア内のすべての使用可能な CA 証明書が信頼されます。

これらのタスクが完了すると、ターゲット・システムのアプリケーションは、別のシステムのローカル CA により発行された証明書を使用できるようになります。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 証明書をユーザーの 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か、いずれかを行う必要があります。どちらを行うかについては、SSL 対応アプリケーションの要件により異なります。

ターゲット・システムでのオブジェクト署名のための秘密証明書の使用

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済み証明書ストア・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する必要があります。

***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 つ) が、`/QIBM/USERDATA/ICSS/CERT/SIGNING` ディレクトリー内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、これらのコピーの作成時に、ローカル CA 証明書のコピーと共に、そのコピーを証明書ストア・ファイルに追加しています。

アテンション: 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、転送されたファイルの名前を指示どおりに変更しないでください。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。*OBJECTSIGNING 証明書ストアが存在する場合、別のプロセスを使用して、証明書を既存の証明書ストアに入れる必要があります。

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 ***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、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、DCM を使用して、オブジェクトの署名検査を行い、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う必要があります。 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。既知のインターネット 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:**
システムの既存の *OBJECTSIGNING 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。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。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。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、転送されたファイルからエクスポートする必要があります。

証明書ストア・ファイルから直接 *OBJECTSIGNING 証明書ストアにファイルをエクスポートするには、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、*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。
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。

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) を使用することで、アプリケーション定義を作成したり、アプリケーションの証明書の割り当てを管理したりすることができます。また、クライアント認証用の証明書を受け入れる基礎としてアプリケーションが使用する、CA 信頼リストを定義することもできます。

DCM を使用すると、Secure Sockets Layer (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、さまざまな管理タスクを実行することができます。たとえば、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。

関連概念:

11 ページの『アプリケーション定義』
ディジタル証明書マネージャー (DCM) では、SSL 構成およびオブジェクト署名を使用するアプリケーション定義を管理できます。

アプリケーション定義の作成

ディジタル証明書マネージャー (DCM) では、2 つのタイプのアプリケーション定義を作成して、使用することができます。1 つは SSL を使用するサーバー・アプリケーションまたはクライアント・アプリケーション定義、もう 1 つはオブジェクトへの署名に使用するアプリケーション定義です。

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 i のほとんどの 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容易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 アプリケーション定義と異なり、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す場合があります。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。『DCM の開始』を参照してください。
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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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、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は、アプリケーションがクライアント認証を必要としているかどうかを指定します。すべてのアプリケーション

で、アプリケーションが CA 信頼リストを使用して、証明書を認証するかどうかを指定します。 SSL アプリケーション定義が使用されている場合、オプションのシステム SSL 属性を構成できます。

関連概念:

11 ページの『アプリケーション定義』
ディジタル証明書マネージャー (DCM) では、SSL 構成およびオブジェクト署名を使用するアプリケーション定義を管理できます。

関連情報:

QSYRGAP、QsyRegisterAppForCertUse API

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) セッション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。『DCM の開始』を参照してください。
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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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. リストの 4 つの証明書から 1 つ選択して、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。 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。 *OBJECTSIGNING 証明書ストアは、1 つの証明書のみ割り当てることができます。

   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、 IBM i Access for Windows 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 i、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。

関連タスク:

88 ページの『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。

87 ページの『アプリケーションへの証明書の割り当て』
ディジタル証明書マネージャー (DCM) により、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ます。 *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。

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信頼できる 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。 CA 信頼リストにより、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・アプリケーションが、CA 信頼リストでトラステッドとして指定されていない CA からの証明書を提示した場合は、アプリケーションはそれを有効な認証のための基準として受け入れません。

CA 信頼リストは、*SYSTEM ストアの CA のサブセットがアプリケーション定義によって信頼されている場合にのみ必要です。デフォルトでは、CA 信頼リストはなく、*SYSTEM ストア内の使用可能なすべての CA が信頼されます。個別の CA をトラステッドであると指定するには、その前に、アプリケーションの定義で、そのアプリケーションに対して CA 信頼リストが定義されていることを指定する必要があります。CA 信頼リストが定義されているが、その CA 信頼リストには CA が含まれていないことを、アプリケーションの定義で示している場合、*SYSTEM ストア内の使用可能なすべての CA が信頼されます。

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。『DCM の開始』を参照してください。
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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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。

   注: アプリケーションがリストに表示されるには、アプリケーション定義で「**CA 信頼リストの定義 (Define the CA trust list)**」が「**はい**」に設定されている必要があります。
8. アプリケーションが承認する 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 を選択することができます。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。

関連概念:

47 ページの『VPN 接続のディジタル証明書』
IBM i 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。

有効期限による証明書の管理

ディジタル証明書マネージャー (DCM) では、証明書の有効期限の管理がサポートされています。これによって管理者は、サーバーまたはクライアントの証明書、オブジェクト署名証明書、認証局証明書、およびユーザー証明書を、ローカル・システム上の有効期限によって管理できます。

注: エンタープライズ識別マッピング (EIM) を使用するように DCM を構成すると、有効期限によるユーザー証明書の管理を企業全体で実行できます。
DCM を使用して、有効期限基づいて証明書を表示すると、期限切れが近づいている証明書をす早く容易に見分けることができ、期限内に証明書を更新することができます。

注: 期限切れの場合でも、オブジェクト署名を検査するための署名検査証明書は使用できるので、 DCM には、これらの証明書の有効期限を確認するサポートはありません。

有効期限に基づいて、サーバーおよびクライアント証明書、またはオブジェクト署名の証明書を表示したり管理したりするには、以下のステップに従ってください。

1. DCM を開始します。 DCM がまだ開始されていない場合は、『DCM の開始』を参照してください。
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。

   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。
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、「**有効期限の確認 (Check expiration)**」を選択します。
6. 確認する証明書のタイプを選択します。

注: サーバー証明書またはクライアント証明書の有効期限を確認するには、*SYSTEM 証明書ストアまたは他のシステム証明書ストアでの作業が必要になります。オブジェクト署名証明書の有効期限を確認するには、*OBJECTSIGNING 証明書ストアでの作業が必要になります。認証局証明書の有効期限は、すべての証明書ストア (ただし、ローカル認証局証明書ストアは除く) で確認することができます。ユーザー証明書の有効期限は、すべての証明書ストアで確認することができます。ローカル CA 証明書の有効期限を判別するには、単一のローカル CA 証明書を表示しなければなりません。

7. 「**有効期限の日数 (1 から 365) (Expiration date range in days (1-365))**」フィールドで、有効期限に基づいて証明書を表示する日数を入力し、「**続行**」をクリックします。今日の日付から指定した日数に相当する日付までの間に期限切れとなるすべての証明書が表示されます。今日までに期限切れとなっているユーザー証明書もすべて表示されます。
8. 管理を行う証明書を選択します。証明書の詳細情報の表示、証明書の削除、または更新を行うことができます。
9. リストの証明書について処理を終えたら、「**キャンセル**」をクリックして終了します。

関連タスク:

58 ページの『有効期限によるユーザー証明書の管理』
ディジタル証明書マネージャー (DCM) では、証明書の有効期限の管理がサポートされています。これによって管理者は、ローカル IBM i モデルにあるユーザー証明書の有効期限を確認できます。DCM の持つユーザー証明書の有効期限の管理サポートと、エンタープライズ識別マッピング (EIM) を組み合わせて使用することで、管理者は DCM を使用して、ユーザー証明書の有効期限をエンタープライズ・レベルで確認できます。

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加わったり、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。

関連概念:

8 ページの『証明書取り消しリストの位置』
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。

13 ページの『妥当性検査』
ディジタル証明書マネージャー (DCM) は、証明書の妥当性検査、またはアプリケーションの妥当性検査を行うタスクを備えており、証明書やアプリケーションが持つ必要があるさまざまなプロパティーの妥当性を検査できます。

アプリケーションへの証明書の割り当て

ディジタル証明書マネージャー (DCM) により、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ます。 *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。『DCM の開始』を参照してください。
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。

   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。
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. リストからアプリケーションを 1 つ以上選択します。現在の証明書の割り当てをこの証明書で置き換える場合は、「**置き換え**」をクリックします。現在証明書が割り当てられていない場合は、「**置き換え**」をクリックして、この証明書を割り当てます。この証明書を既に割り当て済みの証明書のリストに追加する場合は、「**追加 (Append)**」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。

関連タスク:

83 ページの『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) セッション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。

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。『DCM の開始』を参照してください。
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。

   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、ページ上部にある疑問符 (**?**) を選択し、オンライン・ヘルプにアクセスしてください。
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。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。

注: 匿名的に CRL 処理用の LDAP サーバーをバインドするには、ディレクトリー・サーバー Web 管理ツールを使用して、「スキーマの管理」タスクを選択し、certificateRevocationList および authorityRevocationList 属性のセキュリティー・クラス (「アクセス・クラス」とも呼ばれる) を「重要」から「標準」に変更し、「**ログイン識別名 (Login distinguished name)**」フィールドおよび「**パスワード (Password)**」フィールドを空白のままにしておく必要があります。

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、ディレクトリー・サーバー (LDAP) とクライアント・アプリケーションの両方において、SSL を使用するように構成し、DCM で証明書を割り当てる必要があります。

関連概念:

8 ページの『証明書取り消しリストの位置』
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。

関連タスク:

83 ページの『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) セッション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。

関連情報:

IBM Directory Server for iSeries (LDAP)

Directory Server での SSL の使用可能化

IBM 暗号化コプロセッサー上での証明書鍵の保管

IBM 暗号化コプロセッサーがシステムにインストールされていれば、そのコプロセッサーを使用して証明書の秘密鍵をよりセキュアに保管することができます。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。

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する必要があるため、コプロセッサーを使用した保管は行うことができません。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。
- 特殊鍵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。

この鍵保管オプションは、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。

関連概念:

11 ページの『IBM i 用 IBM 暗号化コプロセッサー』
暗号化コプロセッサーは、実績のある暗号化サービスを提供し、セキュアな e- ビジネス・アプリケーションの開発のため、プライバシーと保全性を確保します。

関連情報:

暗号化の概要

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 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、特殊鍵ファイルに保管することができます。 この鍵保管オプションは、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しく使用するには、あらかじめ IBM 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・ファイルを作成しておか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、IBM i 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。

「**鍵保管場所の選択 (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証するには、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・キー検証 (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、IBM Navigator for i Web コンソール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。

関連情報:

暗号化の概要

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 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 が使用可能なアプリケーションからユーザーに提供される資源に対して、セキュリティーのニーズ上、厳重なアクセス制御が必要な場合には、PKIX 準拠の CA の使用について調査してください。たとえば、Lotus® Domino® 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。『DCM の開始』を参照してください。
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。

注: PKIX 規格は、Request For Comments (RFC) 2560 に概説されています。

関連概念:

62 ページの『公開インターネット CA からの証明書の管理』

ディジタル証明書マネージャー (DCM) を使用して、公開インターネット CA から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、特殊鍵データベース・ファイルです。

ユーザー証明書の LDAP 位置の管理

ディジタル証明書マネージャー (DCM) を使用すると、Lightweight Directory Access Protocol (LDAP) サーバーのディレクトリー位置に、ユーザー証明書を保管することができます。これによって、エンタープライズ識別マッピングを拡張して、ユーザー証明書を処理できるようになります。

デフォルト時の DCM は、ローカル認証局 (CA) が発行したユーザー証明書を、IBM i ユーザー・プロファイルに保管します。ただし、ローカル認証局 (CA) がユーザー証明書を発行したときに、Lightweight Directory Access Protocol (LDAP) サーバーの特定のディレクトリー位置に、証明書の公開コピーが保管されるよう、ディジタル証明書マネージャー (DCM) をエンタープライズ識別マッピング (EIM) と組み合わせて構成することもできます。 EIM と DCM を連携するように構成することで、ユーザー証明書を LDAP ディレクトリー位置に保管し、別のアプリケーションが証明書を利用しやすいようにできます。また、この連携の構成では、EIM を使用して、企業全体でユーザー ID の 1 つのタイプとしてユーザー証明書を管理することもできます。

注: ユーザーが、別の CA が発行した証明書を LDAP 位置に保管するようにしたい場合、「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクを完了する必要があります。

EIM は、eServer™ テクノロジーの一種で、IBM i ユーザー・プロファイルやユーザー証明書などといったユーザー ID の企業内管理を可能にします。 EIM を使用してユーザー証明書を管理するには、DCM 構成タスクを実行する前に、以下の EIM 構成タスクを実行する必要があります。

1. System i ナビゲーター の「**EIM 構成**」ウィザードを使用して、EIM を構成します。
2. 証明書アソシエーションに使用する EIM ドメインに X.509 レジストリーを作成します。
3. EIM ドメイン内の「構成」フォルダーに対して「プロパティー」メニュー・オプションを選択し、X.509 レジストリー名を入力します。
4. EIM に加えたいユーザーそれぞれについて、EIM ID を作成します。
5. 各 EIM ID と、ローカルの IBM i ユーザー・レジストリーにあるそのユーザーのユーザー・プロファイルとの間に、ターゲット・アソシエーションを作成します。「**EIM 構成**」ウィザードで指定したローカルの IBM i ユーザー・レジストリーに対して、EIM レジストリー定義名を使用します。

必要な EIM 構成タスクを完了したら、以下のタスクを実行して、 EIM と DCM を連携して使用するための構成すべてを終了してください。

1. DCM において、「**LDAP 位置の管理 (Manage LDAP Location)**」タスクを使用して、ローカル CA が作成するユーザー証明書を保管するために DCM が使用する、LDAP ディレクトリーを指定します。LDAP 位置は、ローカル IBM i モデル上でなくてもかまいません。また、EIM が使用するものと同じ LDAP サーバー上である必要もありません。 DCM に LDAP 位置を構成する場合、DCM は指定された LDAP ディレクトリーを使用して、ローカル CA が発行するユーザー証明書をすべて保管します。また、DCM は、LDAP 位置を使用して、ユーザー・プロファイル付きの証明書を保管する代わりに、「**ユーザー証明書の割り当て (Assign a user certificate)**」タスクによって処理されたユーザー証明書を保管します。
2. 「**ユーザー証明書の変換 (Convert User Certificates)**」(CVTUSRCERT) コマンドを実行する。このコマンドは、既存のユーザー証明書を、適切な LDAP ディレクトリー位置にコピーするものです。ただし、このコマンドは、EIM ID とユーザー・プロファイルとの間にターゲット・アソシエーションを既に作成しているユーザーの証明書だけをコピーします。次にこのコマンドは、それぞれの証明書と関連付けられた EIM ID との間にソース・アソシエーションを作成します。このコマンドは、証明書のサブジェクト識別名 (DN)、発行元 DN、およびこれらの DN のハッシュ、さらに証明書の公開鍵を使用して、ソース・アソシエーションのユーザー ID 名を定義します。

注: 匿名的に CRL 処理用の LDAP サーバーをバインドするには、ディレクトリー・サーバー Web 管理ツールを使用して、「スキーマの管理」タスクを選択し、certificateRevocationList および authorityRevocationList 属性のセキュリティー・クラス (「アクセス・クラス」とも呼ばれる) を「重要」から「標準」に変更し、「**ログイン識別名 (Login distinguished name)**」フィールドおよび「**パスワード (Password)**」フィールドを空白のままにしておく必要があります。

関連タスク:

46 ページの『ディジタル証明書とエンタープライズ識別マッピング』
エンタープライズ識別マッピング (EIM) およびディジタル証明書マネージャー (DCM) を一緒に使用すると、EIM マッピングのルックアップ操作のソースとして証明書を適用し、証明書から同じ EIM ID と関連付けられているターゲット・ユーザー ID へとマップします。

関連情報:

ユーザー証明書の変換 (CVTUSRCERT) コマンド

エンタープライズ識別マッピング (EIM)

オブジェクトへの署名

オブジェクトには、3 つの異なる方法で署名することができます。オブジェクト署名 API を呼び出すプログラムを作成する方法、ディジタル証明書マネージャー (DCM) を使用する方法、他のシステムに配布するパッケージに対して System i ナビゲーター のマネージメント・セントラル機能を使用する方法のいずれかを使って、オブジェクトに署名することができます。

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。コマンド (*CMD) オブジェクトに署名することもできます。他のシステムに保管されているオブジェクトには、署名できません。

公開インターネット認証局 (CA) で購入した証明書、または DCM で秘密ローカル CA を使用して作成した証明書を使って、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、公開証明書または秘密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環、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環として、*OBJECTSIGNING 証明書ストアをあらかじめ作成しておく必要があります。
- *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。『DCM の開始』を参照してください。
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。

   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。

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、「**参照 (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/*` と入力でき、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ます。参照機能を使用して、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、「**参照 (Browse)**」をクリックしてください。
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、「**参照 (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。

関連タスク:

52 ページの『ローカル CA の作成および運用』

ディジタル証明書マネージャー (DCM) を使用すると、独自のローカル CA を作成して運用し、アプリケーション用の秘密証明書を発行することができます。

65 ページの『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。

関連情報:

署名オブジェクト API

シナリオ: System i ナビゲーターのマネージメント・セントラルを使用したオブジェクトへの署名

シナリオ: DCM を使用したオブジェクトへの署名および署名の検査

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ために、*SIGNATUREVERIFICATION 証明書ストアを作成する必要があります。

  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。『DCM の開始』を参照してください。
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。

   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。
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、「**参照 (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/* と入力でき、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ます。参照機能を使用して、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、「**参照 (Browse)**」をクリックしてください。
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、「**参照 (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。

関連概念:

48 ページの『オブジェクトに署名するためのディジタル証明書』
IBM i では、オブジェクトにディジタル「署名」するため、証明書を使用する方法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。

関連タスク:

65 ページの『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。

67 ページの『オブジェクトの署名検査のための証明書の管理』
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。

DCM のトラブルシューティング

以下のトラブルシューティング方法を使用すると、ディジタル証明書マネージャー (DCM) を構成または使用する際に発生する可能性がある基本的な問題について、解決できる場合があります。

DCM および証明書を操作する際にエラーが発生すると、タスクや目的を完了することができません。以下は、操作時に起こる可能性がある共通のエラーや問題を、いくつかのカテゴリーに分類したものです。

パスワードおよび一般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) の使用時に発生する可能性がある、パスワードに関する問題および他の一般的な問題のうち、頻繁に発生するものについてトラブルシューティングする際に、以下の表が役立つことがあります。

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。 IBM i Information Center およびインターネット上の外部の IBM Web サイトを検索することもできます。
ローカル認証局 (CA) および *SYSTEM 証明書ストアのパスワードが機能しない。	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。
証明書ストアを開こうとすると、パスワードの有効期限が切れているというエラー・メッセージを受け取ります。	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。「**OK**」ボタンをクリックして、パスワードを変更します。
「**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ない場合、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。

問題	可能な解決方法
	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確認してください。 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。
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。
証明書の割り当て直後に、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、Directory Server (LDAP) の問題が発生する。この問題は、System i ナビゲーター 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、ご使用のシステムの 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余分なマテリアル (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、証明書はシステム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、貼り付けた結果を必ず比較してください。貼り付けた情報は、オリジナルと同様に表示される必要があります。

証明書ストアおよび鍵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) の使用時に発生する可能性がある、証明書ストアおよび鍵データベースに関する主要な問題をトラブルシューティングする際に、以下の表が役に立つことがあります。

問題	可能な解決方法
システムが鍵データベースを検出しない、または鍵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。
鍵データベースの作成または「ローカル CA の作成 (Create a local CA)」に失敗する。	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。 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、ファイルを回復することができます。次のファイルを移動した後に、新しいローカル 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/LOCAL_CERTIFICATE*(*).TMT /QIBM/USERDATA/ICSS/CERT/CERTAUTH/LOCAL_CERTIFICATE*(*).TXT /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/LOCAL_CERTIFICATE*(*).CATMP /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/LOCAL_CERTIFICATE*(*).CACRT /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

問題	可能な解決方法
	DCM へのインストールが前提条件であるライセンス・プログラム (LPP) がない可能性があります。 38 ページの『DCM のセットアップ要件』のリストを参照して、すべてのライセンス・プログラムが正しくインストールされているか確認してください。
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。	鍵リングおよび鍵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 などの拡張子を持つバイナリー・ファイルには FTP をバイナリー・モードで使用します。
鍵データベースのパスワードが変更できない。鍵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。詳しくは、IBM i Information Center の QsyAddVldlCertificate API に関するトピックを参照してください。妥当性検査リストを使用するようにセキュア HTTP サーバー・インスタンスを構成する方法については、IBM HTTP Server for i5/OS™ の資料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、鍵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 (鍵データベース) 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。
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。

問題	可能な解決方法
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・サーバーが正しくセットアップ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 Communicator 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。
ブラウザーがユーザーに対し、CA を未承認であると表示し続ける。	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つけてください。
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 IBM i 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) の使用時に発生する可能性がある、HTTP Server の問題をトラブルシューティングする際に、以下の表が役立ちます。

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 管理インターフェースを使用して、**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、その仮想ホストで、「**SSL**」を「**使用可能**」に設定しておく必要があります。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。これらは「**一般設定 (General Settings)**」ページで設定されます。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。	システムで、HTTP Server 管理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 を使用可能にする仮想ホストを定義する必要があります。仮想ホストを定義した後、仮想ホストが、(「**一般設定 (General Settings)**」ページの) **Listen** ディレクティブで定義済みの SSL ポートを使用するように指定する必要があります。次に、「**セキュリティー**」の下の「**SSL で証明書認証 (SSL with Certificate Authentication)**」ページを使用して、構成済みの仮想ホストで SSL を使用可能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、そのインスタンスが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 の設定が困難である。	インスタンスをセットアップする際のオプションについては、 IBM HTTP Server for i5/OS の資料を参照してください。
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。IBM i Information Center の API ファインダーに関するトピックに、以下の API に関する情報が記載されています。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
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。

問題	可能な解決方法
「**SSL**」が「**使用可能**」に設定された状態で HTTP Server が正常に始動されず、ジョブ・ログにエラー・メッセージ HTP8351 が表示される。 HTTP Server 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、というエラーが表示されます。	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。 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 QIBM_HTTP_SERVER_MY_SERVER とします。開始に失敗したサーバー・インスタンスが *ADMIN サーバーであれば、一時的に「**SSL**」を「**使用不可**」に設定して、*ADMIN サーバーで DCM を使用できるようにします。次に、DCM を使用して、別の証明書を QIBM_HTTP_SERVER_ADMIN アプリケーションに割り当て、もう一度「**SSL**」を「**使用可能**」に設定してみてください。

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

ディジタル証明書マネージャー (DCM) を使用してユーザー証明書を割り当てる際に、発生する可能性がある問題をトラブルシューティングする際には、以下のステップが役に立ちます。

「**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承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。ブラウザーから、証明書を選択するよう求めるプロンプトが表示されます。
2. これはブラウザーの構成が、選択リストを表示しないように設定されていて、サーバーが承認している CA のリストにある認証局 (CA) の証明書が、ブラウザーに 1 つしかない場合にも発生する可能性がある。ブラウザーの構成の設定を確認し、必要な場合は変更してください。ブラウザーから、証明書を選択するプロンプトが表示されます。サーバーで承認するように設定されている CA の証明書を提出できない場合、証明書の割り当てはできません。 DCM 管理者に連絡してください。
3. 登録する証明書が、すでに DCM に登録されている。
4. 証明書を発行した認証局が、当該システムまたはアプリケーションでトラステッドに指定されていない。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 状況の設定 (Set CA status)**」タスクを使用して CA をトラステッドとして使用可能にし、問題を解決する必要が生じることがあります。
5. 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。
6. 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。
7. IBM HTTP Server for i が、セキュア管理サーバー・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セットアップされていない。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。

関連タスク:

57 ページの『ユーザー証明書の割り当て』
IBM i ユーザー・プロファイルまたはその他のユーザー ID に、所有するユーザー証明書を割り当てることができます。証明書は、別のシステム上の秘密ローカル CA から得られたものでも、既知のインターネット CA から得られたものでも構いません。証明書をご使用のユーザー ID に割り当てる前に、発行元 CA はサーバーによって承認されている必要があり、証明書は、そのシステムにあるユーザー・プロファイルまたはその他のユーザー ID に、まだ関連付けられてはなりません。

DCM の関連情報

IBM Redbooks® 資料および Web サイトには、ディジタル証明書マネージャー (DCM) の各種トピックに関連した情報が記載されています。以下の PDF ファイルのいずれも表示または印刷できます。

IBM Redbooks

- IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements
- AS/400 Internet Security: Developing a Digital Certificate Infrastructure

Web サイト

- **VeriSign Help Desk の Web サイト**: この Web サイトでは、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が公開されており、その他のインターネット・セキュリティー問題も数多く取り上げられています。
- **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。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。

© Copyright IBM Corp. _年を入れる_.

プログラミング・インターフェース情報

本書には、プログラムを作成するユーザーが IBM i のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、『www.ibm.com/legal/copytrade.shtml』 をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プログラム番号: 5770-SS1

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21