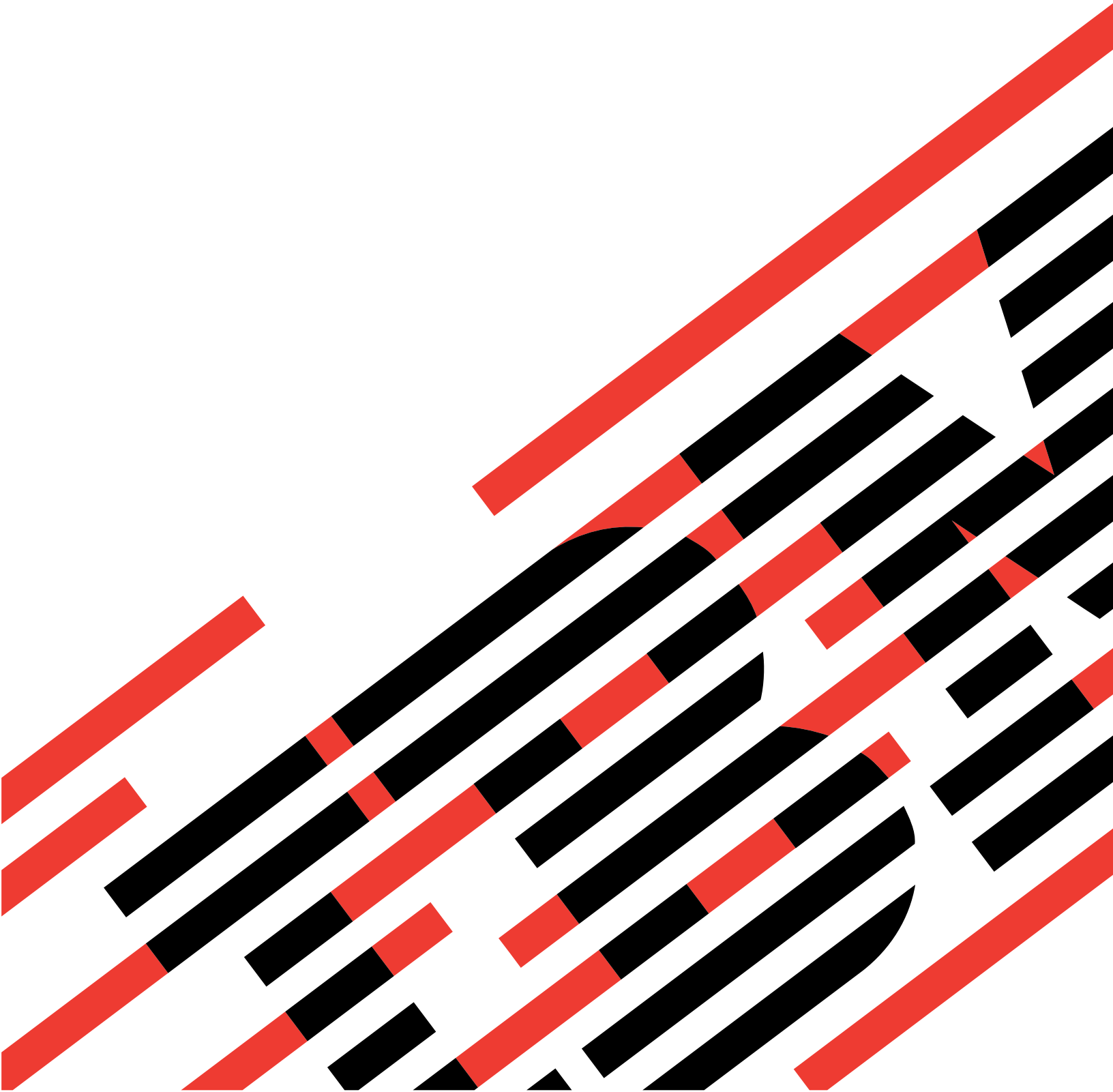
IBM

eserver

iSeries

オブジェクト署名と署名検査



IBM

@server

iSeries

オブジェクト署名と署名検査

目次

オブジェクト署名と署名検査

オブジェクト署名と署名検査は、さまざまな iSeries™ オブジェクトの整合性を検査するために採用できるセキュリティー機能です。ディジタル証明書の秘密鍵を使用してオブジェクトに署名し、証明書 (対応する公開鍵を含む) を使用してそのディジタル署名を検査します。ディジタル署名により、サインするオブジェクトの時刻および内容の正確さが保証されます。署名は、認証と権限の両方に関する否定できない証拠となります。これは、発信元の証拠を示したり、改ざんされたことを検出するときに使用できます。オブジェクトに署名することにより、そのオブジェクトの出所を示し、そのオブジェクトに対する変更を検出するために役立てます。オブジェクトの署名を確認すると、オブジェクトの署名後に、そのオブジェクトの内容に変更が加えられているかどうかを判別できます。さらに、署名のソースを確認して、オブジェクトの発信元の信頼性を確認することもできます。

以下を使用して、iSeries オブジェクト署名および署名検査をインプリメントできます。

- プログラム的にオブジェクトに署名しその署名を検査する API。
- オブジェクトに署名し、オブジェクト署名を表示または検査するディジタル証明書マネージャー。
- 他のシステムで使用するための配布パッケージの一部としてオブジェクトに署名する iSeries ナビゲーター・マネージメント・セントラル機能。
- 署名を検査するオブジェクト整合性の検査 (CHKOBJITG) などの CL コマンド。

これらのオブジェクトに署名するための方法の詳細や、オブジェクトへの署名によって現在のセキュリティー・ポリシーが拡張される仕組みを学習するには、以下のトピックを参照してください。

V5R2 の新機能
この情報を利用して、新しい iSeries オブジェクト署名および署名検査機能を学習します。さらに、このリリースでの資料の変更点も掲載されています。

トピックの印刷
この情報を利用して、PDF ファイルとしてトピック全体を印刷します。

オブジェクト署名のシナリオ
この情報を利用して、iSeries オブジェクト署名および署名検査機能を使用するときの、いくつかの一般的な状況を示したシナリオを検討します。各シナリオには、説明されているシナリオをインプリメントするときに実行しなければならない構成作業も示されています。

オブジェクト署名の概念
この概念と参照情報を利用して、ディジタル署名や、オブジェクト署名および署名検査の処理作業について詳しく学習します。

オブジェクト署名と署名検査の前提条件
この情報を利用して、構成の前提条件について学習します。さらに、オブジェクトに署名して署名を検査するときの、他の計画上の考慮事項も掲載されています。

署名付きオブジェクトの管理
この情報を利用して、署名付きオブジェクトを処理するときに使用できる iSeries コマンドおよびシステム値や、署名付きオブジェクトがバックアップおよびリカバリー処理に影響する仕組みについて学習します。

オブジェクト署名と署名検査のトラブルシューティング
この情報を利用して、オブジェクトに署名し署名を検査するときに生じる可能性のある問題やエラーの解決方法を学習します。

オブジェクト署名と署名検査の関連情報
この情報を利用して、オブジェクトへの署名やオブジェクト署名の検査を学習するための他のリソースへのリンクを見つけます。

V5R2 の新機能

iSeries のオブジェクト署名および署名検査機能は、 V5R1 で初めて登場しました。 V5R2 では更に新しい機能および強化された機能がいくつか利用できるようになっています。

新しいまたは強化されたオブジェクト署名および署名検査機能としては、以下のものがあります。

- **iSeries ナビゲーター・マネージメント・セントラル機能のオブジェクト署名機能。**
  マネージメント・セントラルの「製品の定義」ウィザードを使用して、 iSeries エンドポイント・システムへ配布するためにパッケージするオブジェクトに署名できるようになりました。
- **コマンド (*CMD) オブジェクトへの署名。**
  コマンド (*CMD) オブジェクトへ署名できるようになりました。 *CMD オブジェクト全体に署名するか、*CMD オブジェクトのコア・コンポーネントだけに署名するか選択できます。
- **新しい署名および検査用の API。**
  OS/400® 署名および検査機能に対する拡張機能をプログラム的に利用するため、 3 つの新しい API を使用することができます。
  - バッファーの署名 (QYDOSGNB、QydoSignBuffer) API。
    この API を使用すると、ローカル・システムは、信頼できることを示すために、バッファーにディジタル署名できます。バッファーに署名したら、システムはそのディジタル署名を API の呼び出し側に戻します。たとえば、この API を使用して、XML ファイルの一部に署名し、その署名を XML ファイルの別の部分に保管することができます。あるいは、データベース・ファイル・レコードをバッファーに読み込み、 API を使用してそれらに署名することも可能です。
  - バッファーの検査 (QYDOVFYB、QydoVerifyBuffer)。
    この API を使用すると、ローカル・システムは、以前に署名したバッファー上のディジタル署名を検査することができます。
  - 証明書の追加 (QYDOADDV、QydoAddVerifier) API。
    この API では、システムの *SIGNATUREVERIFICATION 証明書ストアに証明書を追加します。システムは、追加した証明書を使用して、証明書が作成したオブジェクトの署名を検査できます。署名を検査することにより、システムは、署名付きオブジェクトの整合性を検査して、オブジェクトが署名後に変更されていないことを確認できます。証明書ストアが存在しない場合、この API は証明書を追加するときに証明書ストアを作成します。

    注: セキュリティー上の理由により、この API では、認証局 (CA) 証明書を *SIGNATUREVERIFICATION 証明書ストアに挿入できません。 CA 証明書を証明書ストアに追加すると、システムは CA を証明書の信頼されたソースであると見なし、システムは、CA が発行した証明書を信頼されたソースからのものとして扱います。したがって、この API を使用して、CA 証明書を証明書ストアに挿入するためのインストール出口プログラムを作成することはできません。 CA 証明書を証明書ストアに追加し、システムに信頼される CA を個別かつ手動で制御するためには、ディジタル証明書マネージャーを使用する必要があります。こうすることで、管理者がわざと信頼できるものとして指定しなかったソースから、システムが証明書をインポートしてしまう可能性を防ぐことができます。

だれかがこの API を無許可で使用して、 *SIGNATUREVERIFICATION 証明書ストアに検査証明書を追加するのを防ぐには、システムでこの API を使用不可に設定することを検討してください。これは、システム・サービス・ツール (SST) を使用して、 セキュリティー関連のシステム値に対する変更を禁止することによって実現できます。

これまで、 iSeries のオブジェクト署名と署名検査の機能についての情報は、 Information Center の Digital Certificate Management トピックの一部として利用できました。このリリースからは、更にオブジェクト署名や署名検査に関する情報が追加されています。この新しい Information Center のトピックでは、オブジェクト署名および署名検査機能を使用するときの情報がまとめられていて、このような情報を活用して、より簡単にこれらの機能を使用できるようになっています。トピックには、シナリオのような、強化されたより複雑な情報が収められていて、これらの機能を使用してセキュリティー・ポリシーを補足する時と方法を決定するときに役立てられます。

このトピックでの新しいまたは強化された情報は、以下のものがあります。

- シナリオ。セキュリティー・ポリシーを補足するものとして、オブジェクト署名と署名検査を採用する最善の方法を決定できます。
- システムで署名付きオブジェクトを管理するときに使用できるコマンドとシステム値を説明した新しい節。
- オブジェクト署名と署名検査についての計画などの概念情報を説明した新しい節。

新機能やこのリリースでの変更点についての他の情報については、 プログラム資料説明書  を参照してください。

トピックの印刷

PDF 版をダウンロードし、表示するには、オブジェクト署名と署名検査  (約 884 KB、58 ページ) を選択します。

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

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

PDF の表示または印刷のために Adobe Acrobat Reader が必要であれば、 Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html)  からコピーをダウンロードできます。

オブジェクト署名のシナリオ

iSeries サーバーには、オブジェクトに署名し、オブジェクトの署名を検査するためのいくつかの方法が備えられています。オブジェクトに署名する方法と署名付きオブジェクトを処理する方法は、ビジネス上およびセキュリティー上の必要性と目的によって異なります。場合によっては、システムのオブジェクト署名を検査し、オブジェクトの整合性が損なわれていないことを確認するだけのときもあります。または、他者へ配布するオブジェクトに署名することもあります。オブジェクトに署名することで、他者は、オブジェクトの発信元を識別でき、オブジェクトの整合性を検査できます。

使用する方法の選択は、さまざまな要因によって異なります。このトピックで提供されているシナリオでは、一般的なビジネス情況での、一般的なオブジェクト署名と署名検査の目的をいくつか説明します。さらに各シナリオでは、前提条件や、シナリオを説明のとおりにインプリメントするために実行しなければならないタスクも説明します。これらのシナリオを検討し、それぞれのビジネス上およびセキュリティー上のニーズに最適な方法で iSeries オブジェクト署名機能を使用する方法を決定してください。

シナリオ: ディジタル証明書マネージャーを使用してオブジェクトに署名し署名を検査する
このシナリオでは、それぞれの公開 Web サーバーで、攻撃されやすいアプリケーション・オブジェクトに署名する会社があると想定します。これらのオブジェクトに対して許可されていない変更があるかどうかを、もっと簡単に判別できることを目指しています。その会社のビジネス上のニーズとセキュリティー上の目標に基づき、このシナリオでは、オブジェクト署名と署名検査の最初の方法として、ディジタル証明書マネージャー (DCM) を使用する方法を説明します。

シナリオ: API を使用してオブジェクトに署名し署名を検査する
このシナリオでは、販売するアプリケーションにプログラム的に署名することを検討しているアプリケーション開発会社があると想定します。アプリケーションがその会社で開発されたものであることを顧客が確認し、インストール時にアプリケーションに対して許可されていない変更が加えられていないかどうかを検査できることを目指しています。会社のビジネス上のニーズとセキュリティー上の目標に基づき、このシナリオでは、オブジェクトの署名 API と証明書の追加 API を使用して、オブジェクト署名と、署名検査を実現する方法を説明します。

シナリオ: マネージメント・セントラルを使用してオブジェクトに署名する
このシナリオでは、パッケージして複数の iSeries サーバーに配布するオブジェクトに署名することを目指す会社があると想定します。その会社のビジネス上のニーズとセキュリティー上の目標に基づき、このシナリオでは、 iSeries ナビゲーターのマネージメント・セントラルを使用して、他の iSeries サーバーに配布するオブジェクトをパッケージし、署名する方法を説明します。

シナリオ: DCM を使用してオブジェクトに署名し署名を検査する

状況

MyCo., Inc. の iSeries 管理者として、所有する 2 台の iSeries サーバーの管理を担当しています。この iSeries サーバーの 1 つでは、会社の公開 Web サイトを提供しています。会社の内部実動 iSeries サーバーは、この公開 Web サイトのコンテンツを開発し、ファイルとプログラム・オブジェクトをテストした後に公開 Web サイトに転送するときに使用します。

会社の公開 Web サーバーでは、一般的な会社情報 Web サイトを提供しています。この Web サイトには、商品を登録したり商品情報を要求するために顧客が記入するさまざまなフォーム、商品更新の通知、商品配布場所、などがあります。ここで、このようなフォームを実現する cgi-bin プログラムは攻撃されやすいことを認知しているあなたは、内容が変更されることを危惧しています。したがって、このようなプログラム・オブジェクトの整合性を検査し、いつ許可されていない変更が加えられたかを確認できることを目指します。それで、このセキュリティー上の目標を実現するために、このようなオブジェクトにディジタル署名することを決めました。

OS/400 オブジェクト署名機能をリサーチし、オブジェクトに署名してオブジェクト署名を検査するために使用できる方法がいくつか存在することが分かりました。少数の iSeries サーバーの管理を担当していて、それほど頻繁にオブジェクトに署名する必要性を感じないため、このようなタスクを実行するために、ディジタル証明書マネージャー (DCM) を使用することに決定しました。また、ローカル認証局 (CA) を作成し、専用証明書を使用して、オブジェクトに署名することも決定しました。オブジェクト署名のためにロー

カル認証局 (CA) によって発行された専用証明書を使用すると、よく知られた公開 CA から証明書を購入しなくても済むため、コストを抑えることができます。

この例は、少数の iSeries サーバーのオブジェクトに署名する場合に必要な、セットアップやオブジェクト署名の使用に関係する手順の紹介になります。

シナリオの利点

このシナリオには、以下のような利点があります。

- オブジェクトに署名することで、攻撃を受けやすいオブジェクトの整合性を検査でき、オブジェクトの署名後に変更が加えられたかどうかをより容易に判別できるようになります。これにより、アプリケーションやシステムの問題にかかわるトラブルシューティングをいくらか減らせます。
- DCM のグラフィカル・ユーザー・インターフェース (GUI) を使用してオブジェクトに署名し、オブジェクト署名を検査することにより、社内のユーザーはこれらのタスクを早く簡単に行えるようになります。
- DCM を使用してオブジェクトに署名し、オブジェクト署名を検査することで、セキュリティー戦略の一部としてオブジェクト署名を理解し使用するために費やす時間を減らせます。
- ローカル認証局 (CA) によって発行された証明書を使用してオブジェクトに署名することにより、オブジェクトの署名をより少ないコストで実現できるようになります。

目的

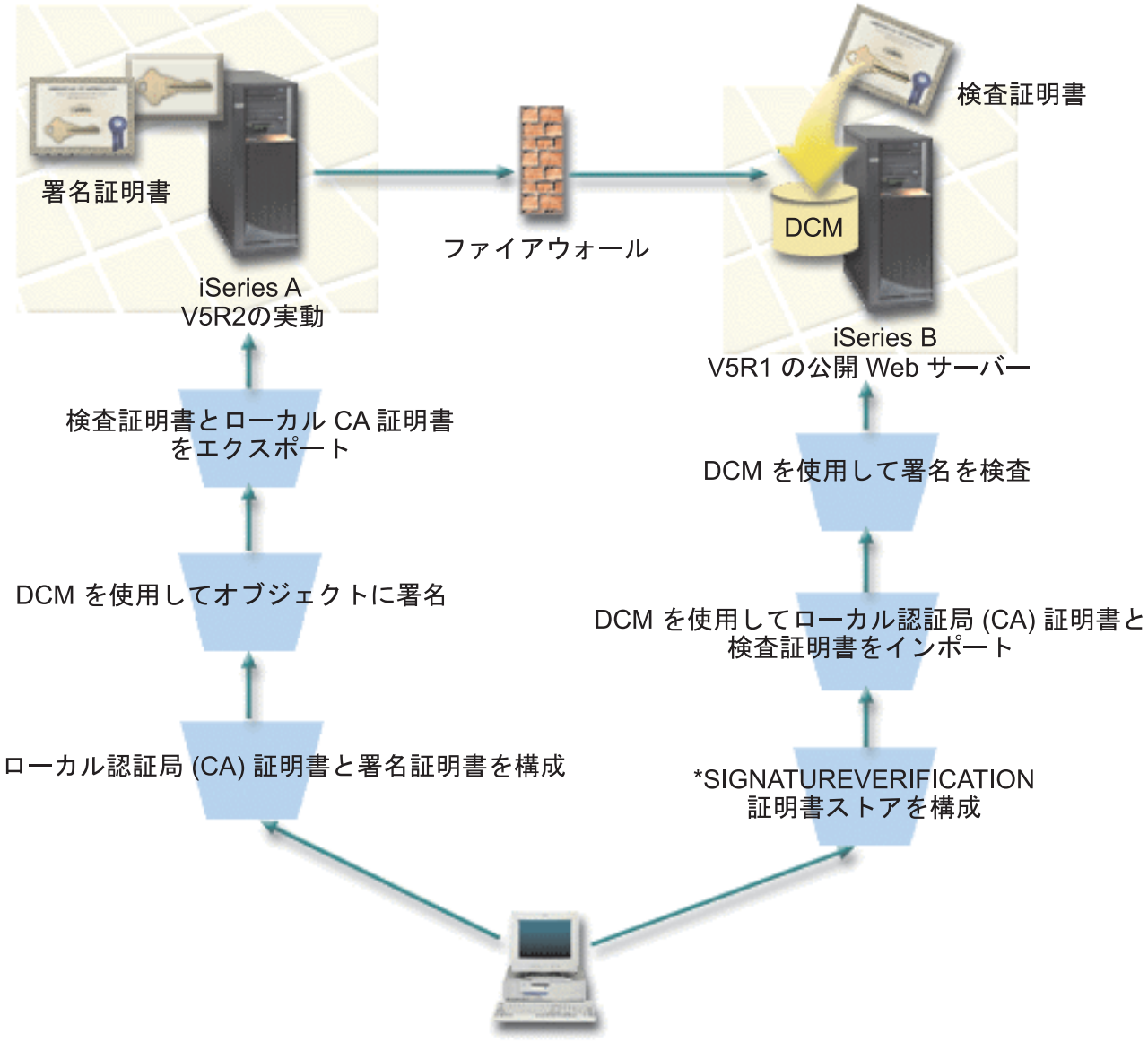
このシナリオでは、会社の公開 iSeries サーバーで、フォームを生成する cgi-bin プログラムのような攻撃を受けやすいオブジェクトにディジタル署名することを目指します。 MyCo, Inc. のシステム管理者は、ディジタル証明書マネージャー (DCM) を使用して、これらのオブジェクトに署名し、オブジェクトの署名を検査します。

このシナリオの目的は、以下のとおりです。

- 公開 Web サーバー (iSeries B) 上にある会社のアプリケーション、および他の攻撃を受けやすいオブジェクトに、ローカル認証局 (CA) からの証明書を使用して署名し、アプリケーションへの署名のコストを抑えます。
- システム管理者や他の指定ユーザーが、 iSeries サーバー上のディジタル署名を検査して、会社の署名付きオブジェクトのソースと認証を容易に確認できるようにします。このことを実現するために、各 iSeries サーバーには、会社の署名検査証明書と、各サーバーの *SIGNATUREVERIFICATION 証明書ストアにあるローカル認証局 (CA) 証明書の両方のコピーが必要です。
- 会社のアプリケーションなどのオブジェクトの署名を検査することにより、 iSeries 管理者や他のユーザーは、オブジェクトに署名された後にその内容が変更されていないかどうかを確認できます。
- システム管理者が、DCM を使用してオブジェクトに署名し、システム管理者や他のユーザーが、 DCM を使用してオブジェクト署名を検査することになります。

詳細

次の図は、このシナリオを実現するための、オブジェクト署名と署名検査のプロセスを示しています。



この図には、このシナリオに関する以下の点が示されています。

iSeries A

- iSeries A は、 OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries A は、会社の内部実動サーバーで、公開 iSeries Web サーバー (iSeries B) の開発プラットフォームです。
- iSeries A には、 Cryptographic Access Provider 128-bit for iSeries (5722-AC3) がインストールされています。
- iSeries A では、ディジタル証明書マネージャー (OS/400 オプション 34) と、 IBM® HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries A は、ローカル認証局 (CA) として稼働し、またオブジェクト署名証明書もこのシステム上に保管されています。

- iSeries A は、 DCM を使用してオブジェクトに署名する、会社の公開アプリケーションなどのオブジェクトの主なオブジェクト署名システムです。
- iSeries A は、署名検査を行えるように構成されています。

iSeries B

- iSeries B は、 OS/400 バージョン 5 リリース 1 (V5R1) を実行しています。
- iSeries B は、会社の外部公開 Web サーバーで、会社のファイアウォールの外側にあります。
- iSeries B には、 Cryptographic Access Provider 128-bit (5722-AC3) がインストールされています。
- iSeries B では、ディジタル証明書マネージャー (OS/400 オプション 34) と、 IBM HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries B では、ローカル認証局 (CA) も iSeries B オブジェクト署名も運用されていません。
- iSeries B は、 DCM を使用して *SIGNATUREVERIFICATION 証明書ストアを作成し、必要な検査証明書とローカル認証局 (CA) 証明書をインポートすることにより、署名検査を行えるように構成されています。
- DCM は、オブジェクトの署名を検査するときに使用されます。

前提条件

このシナリオは、次の前提条件に依存しています。

1. すべてのiSeries サーバーが、ディジタル証明書マネージャー (DCM) をインストールし、使用するための要件を満たしていること。
2. 使用する iSeries の DCM において、いかなる操作または構成が実施されていないこと。
3. すべての iSeries サーバーに、最高レベルの Cryptographic Access Provider 128-bit ライセンス・プログラム (5722-AC3) がインストールされていること。
4. すべてのシナリオの iSeries サーバーにおける (QVFYOBJRST) システム値の復元中の検査オブジェクト署名のデフォルト設定は 3 で、この設定から変更されていないこと。デフォルト設定により、署名されたオブジェクトを復元する際に、サーバーが確実にオブジェクト署名を検査できること。
5. オブジェクトに署名するために、 iSeries A のシステム管理者が *ALLOBJ 特殊権限を持っているか、システム管理者のユーザー・プロファイルがオブジェクト署名アプリケーションに対して許可されていること。
6. システム管理者や、DCM で証明書ストアを作成するユーザーが、 *SECADM および *ALLOBJ 特殊権限を持っていること。
7. 他のすべての iSeries サーバー上のシステム管理者や他のユーザーが、オブジェクト署名を検査するための *AUDIT 特殊権限を持っていること。

タスク手順

このシナリオを実現するために完了しなければならないタスク・セットは 2 つあります。 1 つ目のタスク・セットでは、 iSeries A をローカル認証局 (CA) として構成し、オブジェクトに署名して署名を検査します。 2 番目のタスク・セットでは、 iSeries A が作成するオブジェクト署名を iSeries B が検査できるように構成します。

iSeries A のタスク手順

iSeries A でこれらのタスクすべてを完了することで、専用ローカル認証局 (CA) を作成し、このシナリオで説明されているように、オブジェクトに署名してオブジェクト署名を検査が可能になります。

1. すべての前提条件ステップを完了させ、必要なすべての iSeries 製品をインストールして構成します。
2. ディジタル証明書マネージャー (DCM) を使用して、ローカル認証局 (CA) を作成し、オブジェクト署名証明書を発行します。
3. DCM を使用して、 アプリケーション定義を作成します。
4. DCM を使用して、オブジェクト署名アプリケーション定義に証明書を割り当てます。
5. DCM を使用して、 cgi-bin プログラム・オブジェクトに署名します。
6. DCM を使用して、オブジェクト署名を検査するために他のシステムで使用する必要のある証明書をエクスポートします。ローカル認証局 (CA) 証明書のコピーと、オブジェクト署名証明書のコピーの両方を、署名検査証明書としてファイルにエクスポートする必要があります。
7. iSeries A が作成する署名を検査できるように、会社の公開 iSeries サーバー (iSeries B) に対し、 証明書ファイルを転送します。

iSeries B のタスク手順

このシナリオの公開 Web サーバー (iSeries B) に転送する署名付きオブジェクトを復元する場合、その署名付きオブジェクトを転送する前に、 iSeries B でこれらの署名検査構成タスクを完了させなければなりません。公開 Web サーバー上に署名付きオブジェクトを復元する際、署名を検査する前に署名検査構成を完了させる必要があります。

iSeries B では、以下のタスクを完了することで、このシナリオで説明されているように、オブジェクトに対する署名を検査することが可能になります。

8. ディジタル証明書マネージャー (DCM) を使用して、 *SIGNATUREVERIFICATION 証明書ストアを作成します。
9. DCM を使用して、 ローカル認証局 (CA) 証明書と署名検査証明書をインポートします。
10. DCM を使用して、転送されたオブジェクトの署名を検査します。

構成の詳細

以下のタスク手順を完了させ、ディジタル証明書マネージャーを構成して使用することにより、このシナリオで説明されているように、オブジェクトに署名します。

ステップ 1: すべての前提条件ステップを完了する

このシナリオを実現するための構成タスクを実行する前に、インストールするため前提条件タスクを完了しておく必要があります。

ステップ 2: ローカル認証局 (CA) を作成して専用オブジェクト署名証明書を発行する

ディジタル証明書マネージャー (DCM) を使用して専用認証局 (CA) を作成する場合、そのプロセスでは一連のフォームを完了することが必要です。これらのフォームが、CA の作成プロセスと、 Secure Socket Layer (SSL)、オブジェクト署名、および署名検査を実行するためのディジタル証明書を使用するために必要となる他のタスクを完了させるプロセスをガイドします。このシナリオでは SSL の証明書を構成する必要はありませんが、タスク中のすべてのフォームを完了し、オブジェクトに署名するためにシステムを構成する必要があります。

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

1. DCM を開始します。

2. DCM のナビゲーション・フレームで、**「認証局 (CA) の作成 (Create a Certificate Authority (CA))」**を選択すると、一連のフォームが表示されます。

   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れば、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。このタスクを実行する場合、以下のことを行う必要があります。
   a. ローカル認証局 (CA) についての識別情報を提供します。
   b. ブラウザーにローカル認証局 (CA) 証明書をインストールして、ユーザー側のソフトウェアでローカル認証局 (CA) を認識し、そのローカル認証局 (CA) が発行する証明書の妥当性検査ができるようにします。
   c. ローカル認証局 (CA) についてのポリシー・データを指定します。
   d. 新規ローカル認証局 (CA) を使用して、アプリケーションが SSL 接続に使用できるサーバーまたはクライアント証明書を発行します。

      注: このシナリオでは使用しませんが、必要なオブジェクト署名証明書を発行するためにローカル認証局 (CA) を使用するには、この証明書を作成する必要があります。この証明書を作成しないでタスクを取り消すと、オブジェクト署名証明書と、その証明書が個別に保管される *OBJECTSIGNING 証明書を作成する必要が生じます。
   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: このシナリオの目的に合わせるため、どのアプリケーションも選択せずに**「Continue (続行)」**をクリックして、次のフォームを表示してください。
   f. 新規ローカル認証局 (CA) を使用して、アプリケーションがオブジェクトにディジタル署名するために使用できるオブジェクト署名証明書を発行します。このサブタスクは *OBJECTSIGNING 証明書ストアを作成します。これは、オブジェクト署名証明書を管理するために使用する証明書ストアです。
   g. ローカル認証局 (CA) を信頼する必要があるアプリケーションを選択します。

      注: このシナリオの目的に合わせるため、どのアプリケーションも選択せずに**「続行 (Continue)」**をクリックして、タスクを終了してください。

これでローカル認証局 (CA) とオブジェクト署名証明書を作成したので、次に、オブジェクトに署名できるように、証明書を使用するオブジェクト署名アプリケーションを定義します。

ステップ 3: オブジェクト署名アプリケーション定義を作成する

オブジェクト署名証明書の作成後、ディジタル証明書マネージャー (DCM) を使用して、オブジェクトに署名するのに使用するオブジェクト署名アプリケーションを定義します。アプリケーション定義は、実際のアプリケーションを参照する必要はありません。作成するアプリケーション定義は、署名対象オブジェクトのタイプまたはグループを表します。証明書と関連付けて、署名プロセスを可能にするためのアプリケーション ID を持つには、定義が必要です。

DCM を使用してオブジェクト署名を作成するには、以下のステップに従ってください。

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)」** をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。

2. 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。
3. 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。
4. 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。
5. フォームを完成させて、**「追加 (Add)」** をクリックします。

次に、オブジェクト署名証明書を、作成したアプリケーションに割り当てます。

ステップ 4: 証明書をオブジェクト署名アプリケーション定義に割り当てる

証明書をオブジェクト署名アプリケーションに割り当てる手順は、次のとおりです。

1. DCM 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。
2. 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。
3. リストから証明書を選択して、**「アプリケーションへの割り当て (Assign to Applications)」** をクリックし、現行の証明書ストアのアプリケーション定義のリストを表示します。
4. リストから 1 つ以上のアプリケーションを選択し、**「続行 (Continue)」**をクリックします。メッセージ・ページが表示され、証明書の割り当てを確認するか、問題が発生した場合エラー情報を提供します。

このタスクを完了したら、DCM を使用して、会社の公開 Web サーバー (iSeries B) で使用するプログラム・オブジェクトにすぐに署名できます。

ステップ 5: プログラム・オブジェクトに署名する

DCM を使用して、会社の公開 Web サーバー (iSeries B) で使用するプログラム・オブジェクトに署名する手順は、次のとおりです。

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)」** をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
2. *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。
3. ナビゲーション・フレームが最新表示されたら、**「署名可能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。
4. 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。
5. 前のステップで定義したアプリケーションを選択し、**「オブジェクトに署名 (Sign an Object)」**をクリックします。フォームが表示されるので、そこで署名対象のオブジェクトの位置を指定できます。
6. 表示されたフィールドに、署名対象のオブジェクトの完全修飾パスとファイル名、つまりオブジェクトのディレクトリーを入力して、**「続行 (Continue)」** をクリックします。あるいは、ディレクトリー位置を入力して、**「ブラウズ (Browse)」** をクリックし、ディレクトリーの内容を表示して、署名対象のオブジェクトを選択します。

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

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

7. 選択した 1 つまたは複数のオブジェクト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 (ジョブの処理日付を示す) です。

8. オブジェクト署名操作のジョブ結果を保管するために使用する完全修飾パスおよびファイル名を指定し、**「続行 (Continue)」** をクリックします。あるいは、ディレクトリー位置を入力して、**「ブラウズ (Browse)」** をクリックし、ディレクトリーの内容を表示して、ジョブ結果を保管するファイルを選択します。オブジェクトに署名するジョブが実行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。

署名を検査できるようにするには、必要な証明書をファイルにエクスポートし、その証明書ファイルを iSeries B に転送する必要があります。さらに、署名付きプログラム・オブジェクトを iSeries B に転送する前に、 iSeries B ですべての署名検査構成タスクを完了させる必要もあります。 iSeries B で署名付きオブジェクトを復元するときには、署名を検査する前に、署名検査構成を完了させなければなりません。

ステップ 6: iSeries B で署名検査できるように証明書をエクスポートする

内容の整合性を保護するためのオブジェクト署名には、署名の認証性を検査する手段がなければなりません。オブジェクトに署名する同じシステム (iSeries A) でオブジェクト署名を検査するには、 DCM を使用して、*SIGNATUREVERIFICATION 証明書ストアを作成しなければなりません。この証明書ストアには、オブジェクト署名証明書、および署名証明書を発行した CA 証明書のコピーの両方が入っていなければなりません。

他の人も署名を検査できるようにするには、オブジェクトに署名した証明書のコピーを提供することが必要です。ローカル認証局 (CA) を使用して証明書を発行する場合、ローカル認証局 (CA) 証明書のコピーも提供する必要があります。

オブジェクトに署名したのと同じシステム (このシナリオでは iSeries A) で署名を検査できるように DCM を使用する手順は、次のとおりです。

1. ナビゲーション・フレームで**「証明書ストアの選択 (Select New Certificate Store)」**を選択して、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
2. **「はい (Yes)」**を選択して、既存の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します。

3. 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。これで、DCM を使用して、オブジェクトに署名するのに使用するのと同じシステムでオブジェクト署名を検査できます。

他のシステム (iSeries B) のオブジェクト署名を検査できるようにするため、 DCM を使用して、ローカル認証局 (CA) 証明書のコピーとオブジェクト署名証明書のコピーを署名検査証明書としてエクスポートする手順は、次のとおりです。

1. ナビゲーション・フレームで、**「証明書の管理 (Manage Certificates)」** を選択してから、**「証明書のエクスポート (Export certificate)」** タスクを選択します。
2. **「認証局 (CA) (Certificate Authority (CA))」** を選択して、**「続行 (Continue)」** をクリックすると、エクスポートできる CA 証明書のリストが表示されます。
3. リストから以前に作成したローカル認証局 (CA) 証明書を選択して、**「エクスポート (Export)」**をクリックします。
4. **「ファイル (File)」**をエクスポートの宛先として指定して、**「続行 (Continue)」**をクリックします。
5. エクスポートされるローカル認証局 (CA) 証明書の完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックし、証明書をエクスポートします。
6. **「OK」**をクリックして「エクスポート (Export)」確認ページを終了します。これで、オブジェクト署名証明書のコピーをエクスポートできます。
7. **「証明書のエクスポート (Export certificate)」**タスクを再度選択します。
8. **「オブジェクト署名 (Object signing)」**を選択し、エクスポートできるオブジェクト署名証明書のリストを表示します。
9. リストから適切なオブジェクト署名証明書を選択して、**「エクスポート (Export)」**をクリックします。
10. 宛先として**「署名検査証明書としてのファイル (File, as a signature verification certificate)」**を選択して、**「続行 (Continue)」**をクリックします。
11. エクスポートされる署名検査証明書の完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックし、証明書をエクスポートします。

これで、これらのファイルを、証明書を使って作成した書名を検査する iSeries エンドポイント・システムに転送することができます。

ステップ 7: 証明書ファイルを会社の公開サーバー iSeries B に転送する

署名付きオブジェクトを検査するために、 iSeries A で作成した証明書ファイルを構成する前に、それらの証明書ファイルを iSeries B (このシナリオでは、会社の公開 Web サーバー) へ転送しなければなりません。証明書ファイルの転送にはいくつかの方法があります。たとえば、ファイル転送プロトコル (FTP) またはマネージメント・セントラルのパッケージ配布機能を使ってファイルを転送できます。

ステップ 8: 署名検査タスク: *SIGNATUREVERIFICATION 証明書ストアを作成する

iSeries B (会社の公開 Web サーバー) でオブジェクト署名を検査するには、 iSeries B の *SIGNATUREVERIFICATION 証明書ストアに、対応する署名検査証明書のコピーがなければなりません。ローカル認証局 (CA) に発行された証明書を使用してオブジェクトに署名していたため、この証明書ストアにはローカル認証局 (CA) 証明書のコピーも含まれているはずです。

*SIGNATUREVERIFICATION 証明書ストアを作成する手順は、次のとおりです。

1. DCM を開始します。
2. ディジタル証明書マネージャー (DCM) ナビゲーション・フレームで**「証明書ストアの選択 (Select New Certificate Store)」**を選択して、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れば、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. 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。これで、証明書をストアにインポートしてから、オブジェクト署名の検査に使うことができます。

ステップ 9: 署名検査タスク: 証明書をインポートする

オブジェクトの証明書を検査するためには、 *SIGNATUREVERIFICATION ストアに署名検査証明書のコピーがなければなりません。署名証明書が専用である場合、この証明書ストアには、署名証明書を発行したローカル認証局 (CA) 証明書のコピーを持っていなければなりません。このシナリオでは、両方の証明書がファイルにエクスポートされ、そのファイルが各 iSeries エンドポイント・システムに転送されています。

これらの証明書を *SIGNATUREVERIFICATION 証明書ストアにインポートする手順は、次のとおりです。

1. DCM 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。
2. 「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。
3. 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。
4. タスク・リストから、**「証明書のインポート (Import certificates)」**を選択します。
5. 証明書タイプとして**「認証局 (CA) (Certificate Authority (CA))」** を選択し、**「続行 (Continue)」**をクリックします。

   注: 専用署名検査証明書をインポートする前にローカル認証局 (CA) 証明書をインポートする必要があります。そうしないと、署名検査証明書のインポート処理に失敗します。
6. CA 証明書ファイルの完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックします。インポート処理が正常に実行されたことを確認するメッセージか、処理に失敗した場合はエラー情報を提供するメッセージが表示されます。
7. **「証明書のインポート (Import certificate)」**タスクを再度選択します。
8. **「署名検査 (Signature verification)」**を証明書タイプとして選択し、**「続行 (Continue)」**をクリックします。
9. 署名検査証明書ファイルの完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」** をクリックします。インポート処理が正常に実行されたことを確認するメッセージか、処理に失敗した場合はエラー情報を提供するメッセージが表示されます。

これで、 iSeries B で DCM を使用することにより、 iSeries A の対応する署名証明書を使用して作成したオブジェクトの署名を検査できるようになりました。

ステップ 10: 署名検査タスク: プログラム・オブジェクトの署名を検査する

DCM を使用して、転送されたプログラム・オブジェクトの署名を検査する手順は、次のとおりです。

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)」**をクリックして、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
2. *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。
3. ナビゲーション・フレームが最新表示されたら、**「署名可能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。
4. 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。
5. 表示されたフィールドに、署名検査対象のオブジェクトの完全修飾パスとファイル名、つまりオブジェクトのディレクトリーを入力して、**「続行 (Continue)」**をクリックします。あるいは、ディレクトリー位置を入力して、**「ブラウズ (Browse)」**をクリックし、ディレクトリーの内容を表示して、署名検査対象のオブジェクトを選択します。

   注: 特定のワイルドカード文字を使用して、検査したいディレクトリーの一部を表現することもできます。このようなワイルドカード文字には、「任意の数の文字」を示すアスタリスク (*****) と、「任意の単一文字」を示す疑問符 (**?**) があります。たとえば、特定のディレクトリーのすべてのオブジェクトに署名する場合は、`/mydirectory/*` と入力し、特定のライブラリー内のすべてのプログラムに署名する場合は、`/QSYS.LIB/QGPL.LIB/*.PGM` と入力することができます。これらのワイルドカードが使用できるのは、パス名の最後の部分だけです。たとえば、`/mydirectory*/filename` と指定するとエラー・メッセージが戻されることになります。ブラウズ機能を使用して、ライブラリーまたはディレクトリーの内容のリストを表示したい場合は、パス名の一部としてワイルドカードを入力してから、**「ブラウズ (Browse)」**をクリックする必要があります。
6. 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 (ジョブの処理日付を示す) です。
7. 署名検査操作のジョブ結果を保管するために使用する完全修飾パスおよびファイル名を指定し、**「続行 (Continue)」** をクリックします。あるいは、ディレクトリー位置を入力して、**「ブラウズ (Browse)」**をクリックし、ディレクトリーの内容を表示して、ジョブ結果を保管するファイルを選択します。オブジェクトの署名を検査するジョブが実行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。

シナリオ: API を使用してオブジェクトに署名しオブジェクト署名を検査する

状況

MyCo, Inc. という会社は、 iSeries ビジネス・パートナーで、顧客のためにアプリケーションを開発しています。会社のソフトウェア開発者は、顧客に配布するためにアプリケーションをパッケージする仕事を担当しています。現在、アプリケーションをパッケージするプログラムを使用しています。顧客はコンパクト・ディスク (CD-ROM) を注文することもできますし、会社の Web サイトにアクセスしてアプリケーションをダウンロードすることもできます。

担当者は、業界の最新ニュース、特にセキュリティー関連ニュースに通じています。そのため、顧客がプログラムのソースや内容に関心を持つのも当然だと思っています。顧客は信頼できるソースから製品を受け取る (ダウンロードする) と思っているのに、実際は本当の製品のソースから受け取っているのではないことが判明する場合もあります。このような混乱は、顧客が考えていた製品とは別の製品をインストールするために生じる場合もあります。また、インストールされた製品が、悪意のあるプログラムであることが判明するか、変更されてシステムに損傷を与えるような場合もあります。

この種の問題は、 iSeries の顧客によく起きるわけではありませんが、顧客が受け取るアプリケーションは、本当にその会社からのものであることを保証したいと思います。さらに、顧客がアプリケーションをインストールする前に、アプリケーションが変更されていないかどうかを判別できるように、アプリケーションの整合性を検査する方法を顧客に知らせたいとも思います。

リサーチを基に、 OS/400 オブジェクト署名機能を使用して、このセキュリティー上の目標を実現できると判断しました。アプリケーションにディジタル署名することにより、顧客は、その会社がアプリケーションの本物のソースであることを確認できるようになります。現在はアプリケーションをプログラム的にパッケージしているため、 API を使用することにより、既存のパッケージ・プロセスに対してオブジェクト署名を簡単に追加できると判断しました。また、顧客が製品をインストールするときに、顧客に対して署名検査プロセスをはっきりと提示できるように、オブジェクトに署名するときには公開証明書を使用することを決定しました。

アプリケーション・パッケージの一部として、オブジェクトに署名するのに使用したディジタル証明書のコピーも含めます。顧客がアプリケーション・パッケージを入手すると、顧客はその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査できます。このプロセスを使用すると、顧客はアプリケーションのソースを識別して検査できると同時に、署名されてからアプリケーション・オブジェクトの内容が変更されていないことを確認できます。

この例は、他のユーザーが使用できるように開発してパッケージしたアプリケーションのオブジェクトに、プログラム的に署名する場合の手順を紹介しています。

シナリオの利点

このシナリオには、以下のような利点があります。

- API を使用して、プログラム的にオブジェクトをパッケージして署名すると、このセキュリティーをインプリメントするのに費やす総時間を節約できます。
- オブジェクトをパッケージするときに、API を使用してオブジェクトに署名すると、オブジェクトに署名するときに実行しなければならないステップを減らせます。これは、署名プロセスがパッケージ・プロセスの一部となるためです。
- オブジェクトのパッケージに署名することにより、オブジェクトの署名後に変更が加えられたかどうかをより容易に判別できるようになります。これにより、顧客のアプリケーション問題にかかわるトラブルシューティングをいくらか減らせます。
- 一般的に良く知られている認証局 (CA) からの証明書を使用して、オブジェクトに署名することにより、製品インストール・プログラムの出口プログラムの一部として、証明書の追加 API を使用できるよ

うになります。この API を使用すると、アプリケーションに署名するときに使用した公開証明書を、顧客のシステムへ自動的に追加できるようになります。これにより、署名検査は顧客にもはっきりと分かるものになります。

目的

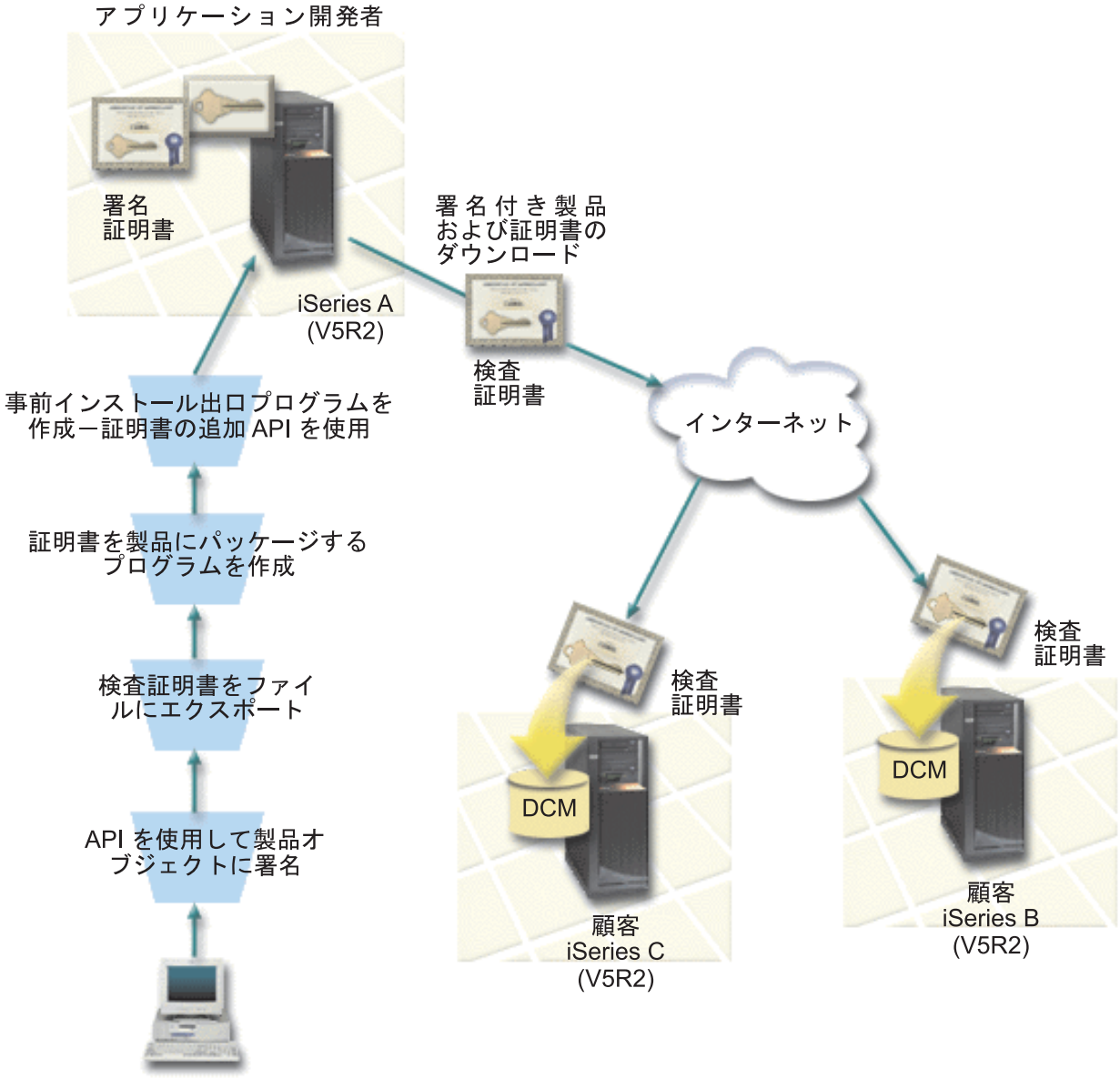
このシナリオでは、MyCo, Inc. は、パッケージして顧客に配布するアプリケーションにプログラム的に署名することを目指しています。 MyCo, Inc. のアプリケーション製品開発者は、会社のアプリケーションを顧客へ配布するためにプログラム的にパッケージしています。そのため、 iSeries API を使用してアプリケーションに署名することを目指すと共に、製品のインストール時に、顧客の iSeries でプログラム的に署名を検査することを目指しています。

このシナリオの目的は、以下のとおりです。

- 会社の製品開発者は、既存のプログラム的なアプリケーション・パッケージ・プロセスの一部として、オブジェクトの署名 API を使用することにより、オブジェクトに署名できなければなりません。
- 会社のアプリケーションは、公開証明書を使用して署名し、アプリケーション製品のインストール・プロセス時に、署名検査プロセスが顧客にはっきりと分かるようにしなければなりません。
- 会社は、 iSeries API を使用して、必要な署名検査証明書を顧客の iSeries サーバー *SIGNATUREVERIFICATION 証明書ストアにプログラム的に追加できなければなりません。会社は、製品のインストール・プロセスの一部として、顧客の iSeries サーバー上に、この証明書ストアをプログラム的に作成できなければなりません。ただし、これは証明書ストアが存在しない場合に限ります。
- 顧客は、製品のインストール後に、会社のアプリケーションのディジタル署名を簡単に検査できなければなりません。顧客が署名アプリケーションのソースと認証性が確実であることを確信できると同時に、署名後にアプリケーションに変更が加えられているかどうかを判別できるように、顧客はその署名を検査できなければなりません。

詳細

次の図は、このシナリオを実現するための、オブジェクト署名と署名検査のプロセスを示しています。



この図には、このシナリオに関する以下の点が示されています。

セントラル・システム (iSeries A)

- iSeries A は、 OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries A は、アプリケーション開発者の製品パッケージ・プログラムを実行しています。
- iSeries A には、 Cryptographic Access Provider 128-bit for iSeries (5722-AC3) がインストールされています。
- iSeries A では、ディジタル証明書マネージャー (OS/400 オプション 34) と、 IBM HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries A は、会社のアプリケーション製品用の主要なオブジェクト署名システムです。カスタマー配布用の製品オブジェクト署名は、以下のタスクを実行することにより、 iSeries A で達成されます。

  1. API を使用して、会社のアプリケーション製品に署名します。

2. 顧客が署名付きオブジェクトを検査できるように、 DCM を使用して、署名検査証明書をファイルにエクスポートします。
3. 検査証明書を署名アプリケーション製品に追加するプログラムを作成します。
4. 証明書の追加 API を使用する製品の事前インストール出口プログラムを作成します。この API を使用すると、製品のインストール・プロセスでは、顧客の iSeries サーバー (iSeries B、 C) の *SIGNATUREVERIFICATION 証明書ストアに対し、検査証明書をプログラム的に追加できるようになります。

顧客の iSeries サーバー B、C

- iSeries B は、 OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries C は、 OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries B、C では、ディジタル証明書マネージャー (オプション 34) と、 IBM HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries B、C は、 (iSeries A を所有する) アプリケーション開発会社の Web サイトからアプリケーションを購入してダウンロードします。
- MyCo のアプリケーション・インストール・プロセスが顧客それぞれの iSeries サーバーに *SIGNATUREVERIFICATION 証明書ストアを作成する場合に、 iSeries B、C には、 MyCo の署名検査証明書のコピーが含まれます。

前提条件

このシナリオは、次の前提条件に依存しています。

1. すべてのiSeries サーバーが、ディジタル証明書マネージャー (DCM) をインストールし、使用するための要件を満たしていること。

   注: DCM をインストールして使用するための前提条件を満たすことは、顧客 (このシナリオでは、iSeries B、C) にとっては必須ではありません。証明書の追加 API は、製品のインストール・プロセスの一部として *SIGNATUREVERIFICATION 証明書ストアを作成し、必要であれば、それをデフォルトのパスワードで作成します。顧客がデフォルトのパスワードを変更して許可されていないアクセスからこの証明書ストアを保護するには、 DCM を使用する必要があります。
2. 使用する iSeries の DCM において、いかなる操作または構成が実施されていないこと。
3. すべての iSeries サーバーに、最高レベルの Cryptographic Access Provider 128-bit ライセンス・プログラム (5722-AC3) がインストールされていること。
4. すべてのシナリオの iSeries サーバーにおける (QVFYOBJRST) システム値の復元中の検査オブジェクト署名のデフォルト設定は 3 で、この設定から変更されていないこと。デフォルト設定により、署名されたオブジェクトを復元する際に、サーバーが確実にオブジェクト署名を検査できること。
5. iSeries A のネットワーク管理者が *ALLOBJ ユーザー・プロファイル特殊権限を持っているか、またはユーザー・プロファイルがオブジェクト署名アプリケーションに対して許可されていること。
6. システム管理者や、DCM で証明書ストアを作成するユーザー (プログラムを含む) が、 *SECADM および *ALLOBJ ユーザー・プロファイル特殊権限を持っていること。
7. 他のすべての iSeries サーバーで、システム管理者または他の人物が、オブジェクト署名を検査するための *AUDIT ユーザー・プロファイルを持っていること。

タスク手順

このシナリオが説明しているように、 iSeries A でこれらの各タスクを完了し、オブジェクトに署名する必要があります。

1. すべての前提条件ステップを完了させ、必要なすべての iSeries 製品をインストールして構成します。
2. よく知られた公開認証局 (CA) からオブジェクト署名証明書を入手するため、 DCM を使用して、証明書要求を作成します。
3. DCM を使用して、 オブジェクト署名アプリケーション定義を作成します。
4. DCM を使用して、 署名付きオブジェクトの署名証明書をインポートし、それをオブジェクト署名アプリケーション定義に割り当てます。
5. DCM を使用して、署名検査証明書としてオブジェクト署名証明書をエクスポートし、顧客がそれを使用してアプリケーション・オブジェクトの署名を検査できるようにします。
6. アプリケーション・パッケージ・プログラムを再作成し、署名検査証明書ファイルを製品の一部として組み込み、顧客へ配布するためにパッケージするときに、 オブジェクトの署名 API を使用してアプリケーションに署名するようにします。
7. アプリケーション・パッケージ・プロセスの一部として、 証明書の追加 API を使用する事前インストール出口プログラムを作成します。この出口プログラムを使用すると、*SIGNATUREVERIFICATION 証明書ストアを作成し、製品のインストール時に、必要な署名検査証明書を顧客の iSeries サーバーへ追加できるようになります。
8. 顧客に DCM を使用してもらい、 iSeries サーバー上にある *SIGNATUREVERIFICATION 証明書ストアのデフォルト・パスワードをリセットします。

構成の詳細

以下のタスク・ステップを完了させ、このシナリオで説明されているように、 OS/400 API を使用してオブジェクトに署名します。

ステップ 1: すべての前提条件ステップを完了する

必要なすべての iSeries 製品をインストールして構成するには、このシナリオを実現するための構成タスクを実行する前に、すべての前提条件タスクを完了させる必要があります。

ステップ 2: DCM を使用してよく知られている公開 CA から証明書を入手する

このシナリオでは、以前にディジタル証明書マネージャー (DCM) を使用して証明書を作成し管理していなかった場合を想定しています。そのため、オブジェクト署名証明書を作成するプロセスの一部として、*OBJECTSIGNING 証明書ストアを作成する必要があります。この作成される証明書ストアによって、オブジェクト署名証明書の作成や管理するタスクが実現できます。よく知られている公開認証局 (CA) から証明書を入手するには、 DCM を使用して識別情報と証明書の公開鍵と秘密鍵のペアを作成します。そして、この情報を CA に登録して証明書を入手します。

オブジェクト署名証明書を入手できるように、よく知られた公開 CA に提供する必要がある証明書要求情報を作成する手順は、次のとおりです。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、**「新規証明書ストアの作成 (Create New Certificate Store)」**を選択して、ガイド・タスクを開始し、一連のフォームを完了します。これらのフォームは、証明書ストアおよび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れば、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。

3. 作成する証明書ストアとして ***OBJECTSIGNING** を選択して、**「続行」**をクリックします。
4. **「はい (Yes)」**を選択して、 *OBJECTSIGNING 証明書ストア作成の一環として証明書を作成し、**「続行」**をクリックします。
5. 新規証明書の署名者として**「VeriSign または他のインターネット認証局 (CA) (VeriSign or other Internet Certificate Authority (CA))」**を選択して、**「続行 (Continue)」**をクリックすると、新規証明書の識別情報を指定できるフォームが表示されます。
6. フォームを完成させて、**「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、証明書を発行する認証局 (CA) に提供する必要がある認証要求データが表示されます。認証署名要求 (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 CA が必要とする CSR データを、証明書アプリケーション・フォームまたは個別ファイルに、注意しながらコピー・アンド・ペーストします。「開始 (Begin)」行と「新規認証要求の終わり (End New Certificate Request)」行の両方を含む、すべての CSR データを使用しなければなりません。このページを終了すると、データは失われ、そのデータを回復することはできません。
8. 選択した CA にアプリケーション・フォームまたはファイルを送信して、証明書を発行したり、証明書に署名したりします。
9. シナリオの次のタスク手順に進む前に、 CA が署名して完了した証明書を戻すのを待ちます。

ステップ 3: オブジェクト署名アプリケーション定義を作成する

証明書要求を良く知られた公開 CA に送信した後、DCM を使用して、オブジェクトの署名に使用できるオブジェクト署名アプリケーションを定義します。アプリケーション定義は、実際のアプリケーションを参照する必要はありません。作成するアプリケーション定義は、署名対象オブジェクトのタイプまたはグループを表します。証明書と関連付けて、署名プロセスを可能にするためのアプリケーション ID を持つには、定義が必要です。

DCM を使用してオブジェクト署名を作成するには、以下のステップに従ってください。

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)」**をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
2. 「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。
3. 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。
4. 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。
5. フォームを完成させて、**「追加 (Add)」**をクリックします。

CA から戻された署名証明書を受け取ったら、作成したアプリケーションにその証明書を割り当てることができます。

ステップ 4: 署名公開証明書をインポートしてオブジェクト署名アプリケーションに割り当てる

証明書をインポートしてアプリケーションに割り当て、オブジェクト署名できるようにする手順は、次のとおりです。

1. DCM を開始します。
2. ナビゲーション・フレームで**「証明書ストアの選択 (Select a Certificate Store)」**をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
3. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページが表示されたら、証明書ストアの作成時に証明書ストアに指定したパスワードを指定して、**「続行 (Continue)」**をクリックします。
4. ナビゲーション・フレームが最新表示されたら、**「証明書の管理 (Manage Certificates)」**を選択して、タスクのリストを表示します。
5. タスク・リストから**「証明書のインポート (Import certificates)」**を選択して、署名済みの証明書を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れば、ページの上部にある疑問符 **(?)** を選択してください。オンライン・ヘルプが表示されます。
6. **「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、現在の証明書ストアの証明書のリストを表示します。
7. リストから証明書を選択して、**「アプリケーションへの割り当て (Assign to Applications)」**をクリックし、現行の証明書ストアの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。割り当て選択の確認メッセージが示されたページか、問題が発生した場合には、エラー・メッセージが示されたページが表示されます。

このタスクを完了したら、 OS/400 API を使用して、アプリケーションなどのオブジェクトに署名できます。しかし、ユーザーと他のユーザーが署名を検査できるようにするために、必要な証明書をファイルにエクスポートして、署名アプリケーションをインストールする任意の iSeries サーバーに転送する必要があります。顧客の iSeries サーバーでは、アプリケーションのインストール時に、証明書を使用してアプリケーションの署名を検査できなければなりません。証明書の追加 API をアプリケーション・インストール・プログラムの一部として使用し、顧客のために必要な署名検査構成を実行できます。たとえば、証明書の追加 API を呼び出す事前インストール出口プログラムを作成して、顧客の iSeries サーバーを構成することが可能です。

ステップ 5: 他の iSeries サーバーで署名検査できるように証明書をエクスポートする

オブジェクトに署名する場合には、その署名の認証性を検査してその署名を使用することにより、署名付きオブジェクトに変更が加えられていないかどうかを判別する手段が必要になります。オブジェクトに署名する同じシステム上のオブジェクト署名を検査するには、 DCM を使って *SIGNATUREVERIFICATION 証明書ストアを作成することが必要です。この証明書ストアには、オブジェクト署名証明書、および署名証明書を発行した CA 証明書のコピーの両方が入っていなければなりません。

他の人も署名を検査できるようにするには、オブジェクトに署名した証明書のコピーを提供することが必要です。ローカル認証局 (CA) を使用して証明書を発行する場合、ローカル認証局 (CA) 証明書のコピーも提供する必要があります。

オブジェクトに署名したのと同じシステム (このシナリオでは iSeries A) で署名を検査できるように DCM を使用する手順は、次のとおりです。

1. ナビゲーション・フレームで**「証明書ストアの選択 (Select New Certificate Store)」**を選択して、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
2. **「はい (Yes)」**を選択して、既存の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します。

3. 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。これで、DCM を使用して、オブジェクトに署名するのに使用するのと同じシステムでオブジェクト署名を検査できます。

他のユーザーがオブジェクト署名を検査できるように、DCM を使用して、オブジェクト署名証明書のコピーを署名検査証明書としてエクスポートする手順は、次のとおりです。

1. ナビゲーション・フレームで、**「証明書の管理 (Manage Certificates)」**を選択してから、**「証明書のエクスポート (Export certificate)」**タスクを選択します。
2. **「オブジェクト署名 (Object signing)」**を選択し、エクスポートできるオブジェクト署名証明書のリストを表示します。
3. リストから適切なオブジェクト署名証明書を選択して、**「エクスポート (Export)」**をクリックします。
4. 宛先として**「署名検査証明書としてのファイル (File, as a signature verification certificate)」**を選択して、**「続行 (Continue)」**をクリックします。
5. エクスポートされる署名検査証明書の完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックし、証明書をエクスポートします。

これで、製品用に作成するアプリケーション・インストール・パッケージにこのファイルを追加できるようになりました。証明書の追加 API をインストール・プログラムの一部として使用することにより、この証明書を顧客の *SIGNATUREVERIFICATION 証明書ストアに追加できます。この API は、まだ存在していなければ、この証明書ストアも作成します。その後、製品のインストール・プログラムは、顧客の iSeries サーバーで、アプリケーション・オブジェクトを復元するときに、そのオブジェクトの署名を検査できます。

ステップ 6: アプリケーションの署名に iSeries API を使用するアプリケーション・パッケージ・プログラムを更新する

アプリケーション・パッケージに追加する署名検査証明書ファイルが完成したので、顧客に配布するために製品ライブラリーをパッケージするときには、オブジェクトの署名 API を使用して、製品ライブラリーに署名するアプリケーションを作成したり、既存のアプリケーションを編集したりすることができます。

オブジェクトの署名 API をアプリケーション・パッケージ・プログラムの一部として使用する方法をよりよく理解するために、以下のサンプル・プログラムを検討します。 C で作成されたこのサンプル・コードは、完全な署名およびパッケージ・プログラムではありません。むしろ、オブジェクトの署名 API を呼び出すそのようなプログラムの該当部分を例として取り出したものです。このサンプル・プログラムを使用するのであれば、それぞれの固有の必要に適した形に変更してください。セキュリティー上の理由から、IBM では、提供されているデフォルト値を使用するのではなく、サンプル・プログラムをそれぞれの事情に合わせるようにお勧めしています。

注: IBM は、お客様に、すべてのサンプル・プログラミング・コードを使用することができる非独占的な著作権ライセンスを許諾します。お客様は、このサンプル・プログラミング・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。すべてのサンプル・コードは、例として示す目的でのみ、IBM により提供されます。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。したがって 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。ここに含まれるすべてのプログラムは、現存するままの状態で提供され、いかなる保証もありません。著作権の非侵害性、商品性、特定目的適合性に関する黙示の保証の適用も一切ありません。

オブジェクトの署名 API をアプリケーション製品のパッケージ・プログラムの一部として使用するときのそれぞれのニーズに合わせ、このコード断片を変更してください。このプログラムには、2 つのパラメーターを渡す必要があります。すなわち、署名するライブラリーの名前と、オブジェクト署名アプリケーション ID の名前です。このアプリケーション ID は大文字小文字を区別しますが、ライブラリー名は区別しません。署名する製品の一部として複数のライブラリーが使用される場合に、作成するプログラムではこの断片を複数回呼び出すことができます。

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Use Sign Object API to sign one or more libraries                */
/*                                                                  */
/* The API will digitally sign all objects in a specified library   */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* This material contains programming source code for your          */
/* consideration.  This example has not been thoroughly             */
/* tested under all conditions.  IBM, therefore, cannot             */
/* guarantee or imply reliability, serviceability, or function      */
/* of these programs.  All programs contained herein are            */
/* provided to you "AS IS".  THE IMPLIED WARRANTIES OF              */
/* MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE         */
/* ARE EXPRESSLY DISCLAIMED.  IBM provides no program services for  */
/* these programs and files.                                        */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* The parameters are:                                              */
/*                                                                  */
/*  char *   name of the library to sign                            */
/*  char *   name of the application ID                             */
/*                                                                  */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* parameters:

       char * library to sign objects in,
       char * application identifier to sign with

     */

    int         lib_length, applid_length, path_length, multiobj_length;
    Qus_EC_t    error_code;
    char        libname[11];
    char        path_name[256];

    Qydo_Multi_Objects_T * multi_objects = NULL;
    multiobj_length = 0;
    error_code.Bytes_Provided = 0;     /* return exceptions for any errors  */


    /* ------------------------------------ */
    /* construct path name given library name */
    /* ------------------------------------ */
    memset(libname, '¥00', 11); /* initialize library name */
    for(lib_length = 0;
```

```
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '¥00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* fill in library name */

    /* build path name parm for API call */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* ---------------------------- */
    /* find length of application id */
    /* ---------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '¥00'));
        applid_length++);

    /* ------------------------------- */
    /* sign all objects in this library */
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* path name to object         */
               &path_length,          /* length of path name         */
               "OBJN0100",            /* format name                 */
               argv[2],               /* application identifier (ID) */
               &applid_length,        /* length of  application ID   */
               "1",                   /* replace duplicate signature */
               multi_objects,         /* how to handle multiple
                                         objects                   */
               &multiobj_length,      /* length of multiple objects
                                         structure to use
                                      (0=no mult.object structure)*/
               &error_code);          /* error code                  */



    return 0;

}
```

ステップ 7: 証明書の追加 API を使用する事前インストール出口プログラムを作成する

アプリケーションに署名するためのプログラム的なプロセスが実現したので、証明書の追加 API をインストール・プログラムの一部として使用して、配布する最終的な製品を作成できます。たとえば、証明書の追加 API を事前インストール出口プログラムの一部として使用して、署名アプリケーション・オブジェクトを復元する前に、証明書を証明書ストアに追加するようにします。このようにすると、インストール・プログラムでは、顧客の iSeries サーバーで、アプリケーション・オブジェクトを復元するときに、そのオブジェクトの署名を検査できます。

注: セキュリティー上の理由により、この API では、認証局 (CA) 証明書を *SIGNATUREVERIFICATION 証明書ストアに挿入できません。 CA 証明書を証明書ストアに追加すると、システムは CA を証明書の信頼されたソースであると見なします。したがって、システムは、CA が発行した証明書を信頼されたソースからのものとして扱います。それで、この API を使用して、 CA 証明書を証明書ストアに挿入するためのインストール出口プログラムを作成することはできません。 CA 証明書を証明書ストアに追加し、システムに信頼される CA を個別かつ手動で制御するようにするには、ディジタル証明書マネージャーを使用する必要があります。そのようにすることで、管理者がわざと信頼できるものとして指定しなかったソースから、システムが証明書をインポートしてしまう可能性を防ぐことができます。

だれかがこの API を無許可で使用して、 *SIGNATUREVERIFICATION 証明書ストアに検査証明書を追加することを防ぐには、システムでこの API の使用を使用不可にすることを考慮する必要があります。これは、システム・サービス・ツール (SST) を使用してセキュリティー関連のシステム値への変更の許可を解除することによって行えます。

証明書の追加 API をアプリケーション・インストール・プログラムの一部として使用する方法をよりよく理解するために、以下の事前インストール出口プログラムのサンプル・プログラムを検討します。 C で作成されたこのサンプル・コードは、完全な事前インストール出口プログラムではありません。むしろ、証明書の追加 API を呼び出すプログラムの該当部分を例として取り出したものです。このサンプル・プログラムを使用するのであれば、それぞれの固有の必要に適した形に変更してください。セキュリティー上の理由から、 IBM では、提供されているデフォルト値を使用するのではなく、サンプル・プログラムをそれぞれの事情に合わせるようにお勧めしています。

注: IBM は、お客様に、すべてのサンプル・プログラミング・コードを使用することができる非独占的な著作権ライセンスを許諾します。お客様は、このサンプル・プログラミング・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。すべてのサンプル・コードは、例として示す目的でのみ、IBM により提供されます。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。ここに含まれるすべてのプログラムは、現存するままの状態で提供され、いかなる保証もありません。著作権の非侵害性、商品性、特定目的適合性に関する黙示の保証の適用も一切ありません。

製品のインストール時に、証明書の追加 API を事前インストール出口プログラムの一部として使用して、必要な署名検査証明書を顧客の iSeries サーバーに追加するときのそれぞれのニーズに合わせ、このコード断片を変更してください。

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2002                                  */
/*                                                               */
/* Use Add Verifier API to add a certificate in the specified    */
/* IFS file to the *SIGNATUREVERIFICATION certificate store.     */
/*                                                               */
/* The API will create the certificate store if it does not exist.  */
/* If the certificate store is created it will be given a default   */
/* password that should be changed using DCM as soon as possible.   */
/* This warning needs to be given to the owners of the system that  */
/* use this program.                                             */
/*                                                               */
/*                                                               */
/*                                                               */
/* This material contains programming source code for your       */
/* consideration.  This example has not been thoroughly          */
/* tested under all conditions.  IBM, therefore, cannot          */
/* guarantee or imply reliability, serviceability, or function   */
/* of these programs.  All programs contained herein are         */
/* provided to you "AS IS".  THE IMPLIED WARRANTIES OF           */
/* MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE      */
/* ARE EXPRESSLY DISCLAIMED.  IBM provides no program services for  */
/* these programs and files.                                     */
/*                                                               */
/*                                                               */
/*                                                               */
/* The parameters are:                                           */
/*                                                               */
/*  char *   path name to IFS file that holds the certificate    */
/*  char *   certificate label to give certificate               */
/*                                                               */
/*                                                               */
```

```
/*                                                                  */
/* ---------------------------------------------------------------- */

#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

    int         pathname_length, cert_label_length;
    Qus_EC_t    error_code;
    char      * pathname = argv[1];
    char      * certlabel = argv[2];

    /* find length of path name */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '¥00'));
        pathname_length++);

    /* find length of certificate label */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '¥00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* return exceptions for any errors  */

    QydoAddVerifier (pathname,         /* path name to file with certificate*/
                     &pathname_length, /* length of path name               */
                     "OBJN0100",       /* format name                       */
                     certlabel,        /* certificate label                 */
                     &cert_label_length, /* length of certificate label     */
                     &error_code);     /* error code                        */

    return 0;
}
```

これらのタスクが完了したら、アプリケーションをパッケージし、顧客に配布できます。顧客がアプリケーションをインストールするときに、インストール・プロセスの一部として、署名アプリケーション・オブジェクトが検査されます。後で、顧客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・オブジェクトの署名を検査できます。これにより、顧客は、アプリケーションのソースが信頼できるものかどうか、アプリケーションに署名してから変更が加えられていないかどうかを判別できます。

注: インストール・プログラムでは、顧客のデフォルト・パスワードを使用して、*SIGNATUREVERIFICATION 証明書ストアが作成された可能性があります。許可されていないアクセスから保護するために、顧客に対し、 DCM を使用して証明書ストアのパスワードをできるだけ早くリセットするようアドバイスする必要があります。

ステップ 8: 顧客に *SIGNATUREVERIFICATION 証明書ストアのデフォルト・パスワードをリセットしてもらう

証明書の追加 API は、顧客の iSeries サーバーで、製品のインストール・プロセスの一部として *SIGNATUREVERIFICATION 証明書ストアを作成した可能性があります。この API で証明書ストアを作成した場合、デフォルト・パスワードも作成されています。そのため、証明書ストアを無許可アクセスから保護するために、 DCM を使用してこのパスワードをリセットするよう顧客にアドバイスする必要があります。

*SIGNATUREVERIFICATION 証明書ストアのパスワードをリセットするには、顧客に以下のステップを実行してもらってください。

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 ***SIGNATUREVERIFICATION** 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、**「パスワードのリセット (Reset Password)」**をクリックして、「証明書ストア・パスワードのリセット (Reset Certificate Store Password)」ページを表示します。

   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れば、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
4. ストアの新しいパスワードを指定し、確認のために再入力し、証明書ストアのパスワード有効期限ポリシーを選択し、**「続行」**をクリックします。

シナリオ: マネージメント・セントラルを使用してオブジェクトに署名する

状況

MyCo, Inc. という会社では、社内の複数の場所に存在する複数の iSeries サーバーに配布するアプリケーションを開発しています。ネットワーク管理者は、これらのアプリケーションが会社のすべての iSeries サーバーにインストールされて更新されたことを確認する仕事を担当しています。現在は、iSeries ナビゲーターのマネージメント・セントラルを使用することにより、これらのアプリケーションをより容易にパッケージして配布し、担当する他の管理用タスクを実行しています。しかし、オブジェクトに対して許可されていない変更が加えられているため、これらのアプリケーションを追跡して問題を訂正することに思ったより時間がかかっています。そのため、このようなオブジェクトにディジタル署名することによって、オブジェクトの整合性をより安全に保護したいと考えています。

OS/400 オブジェクト署名機能についてリサーチして学習した結果、 V5R2 よりマネージメント・セントラルを使用して、オブジェクトをパッケージして配布するときに、そのオブジェクトに署名できることが分かりました。マネージメント・セントラルを使用することにより、会社でのセキュリティー上の目標を効果的かつ比較的簡単に満たすことができます。また、ローカル認証局 (CA) を作成し、それを使用してオブジェクトに署名するための証明書を発行することも決定しました。オブジェクト署名のためにローカル認証局 (CA) によって発行された証明書を使用すると、よく知られた公開 CA から証明書を購入しなくても済むため、コストを抑えることができます。

この例は、会社にある複数の iSeries サーバーに配布するアプリケーションのためにオブジェクト署名を構成して使用する場合の手順として紹介しています。

シナリオの利点

このシナリオには、以下のような利点があります。

- マネージメント・セントラルを使用して、オブジェクトをパッケージして署名すると、署名付きオブジェクトを会社の iSeries サーバーに配布するのに費やす総時間を節約できます。
- マネージメント・セントラルを使用してパッケージ内のオブジェクトに署名すると、オブジェクトに署名するときに実行しなければならないステップを減らせます。これは、署名プロセスがパッケージ・プロセスの一部となるためです。

- オブジェクトのパッケージに署名することにより、オブジェクトの署名後に変更が加えられたかどうかをより容易に判別できるようになります。これにより、アプリケーション問題にかかわるトラブルシューティングをいくらか減らせます。
- ローカル認証局 (CA) によって発行された証明書を使用してオブジェクトに署名することにより、オブジェクトの署名をより少ないコストで実現できるようになります。

目的

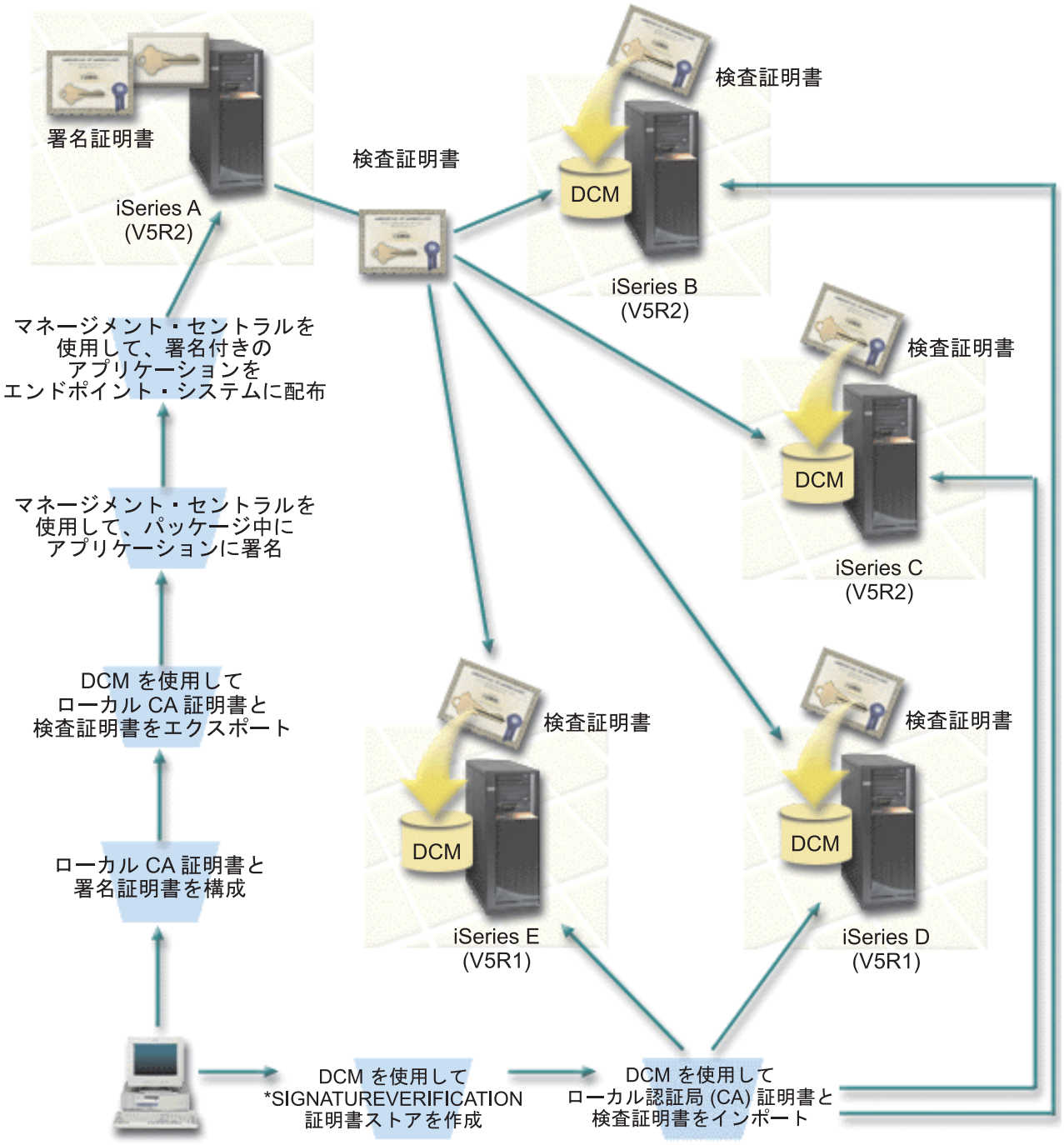
このシナリオでは、MyCo, Inc. は、社内の複数の iSeries サーバーに配布するアプリケーションに、ディジタル署名を付けることを望んでいます。 MyCo, Inc. のネットワーク管理者は、多数の iSeries 管理用タスクで、すでにマネージメント・セントラルを使用しています。それで、他の iSeries サーバーに配布する会社のアプリケーションに署名するために、マネージメント・セントラルの現在の使用方法を拡張することを目指します。

このシナリオの目的は、以下のとおりです。

- 会社のアプリケーションに、ローカル認証局 (CA) が発行した証明書を使用して署名し、アプリケーションへの署名のコストを節約します。
- システム管理者や他の指定ユーザーが、すべての iSeries サーバー上のディジタル署名を検査して、会社の署名付きオブジェクトのソースと認証性を容易に確認できるようにします。このことを実現するために、各 iSeries サーバーには、会社の署名検査証明書と、各サーバーの *SIGNATUREVERIFICATION 証明書ストアにあるローカル認証局 (CA) 証明書の両方のコピーが必要です。
- 会社のアプリケーションの署名を検査することにより、 iSeries 管理者や他のユーザーは、オブジェクトに署名された後にその内容が変更されていないかどうかを確認できます。
- 管理者は、マネージメント・セントラルを使用して、アプリケーションをパッケージし、署名し、それぞれの iSeries サーバーに配布できなければなりません。

詳細

次の図は、このシナリオを実現するための、オブジェクト署名と署名検査のプロセスを示しています。



この図には、このシナリオに関する以下の点が示されています。

セントラル・システム (iSeries A)

- iSeries A は、 OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。
- iSeries A は、企業のアプリケーションのパッケージおよび配布を含めた、マネージメント・セントラル機能の実行元のセントラル・システムとしての役割を果たします。
- iSeries A には、 Cryptographic Access Provider 128-bit for iSeries (5722-AC3) がインストールされています。

- iSeries A では、ディジタル証明書マネージャー (OS/400 オプション 34) と、 IBM HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries A は、ローカル認証局 (CA) として稼働し、またオブジェクト署名証明書もこのシステム上に保管されています。
- iSeries A は、アプリケーションにオブジェクト署名する主となるシステムです。顧客配布用の製品オブジェクト署名は、以下のタスクを実行することにより、 iSeries A で達成されます。
  1. DCM を使用してローカル認証局 (CA) を作成し、ローカル認証局 (CA) を使用してオブジェクト署名証明書を作成します。
  2. DCM を使用してローカル認証局 (CA) 証明書と署名検査証明書のコピーをファイルにエクスポートし、エンドポイント・システム (iSeries B、C、D、E) が署名付きオブジェクトを検査できるようにします。
  3. マネージメント・セントラルを使用して、アプリケーション・オブジェクトに署名し、それらのオブジェクトを検査証明書ファイルでパッケージします。
  4. マネージメント・セントラルを使って、署名付きのアプリケーションと証明書ファイルをエンドポイント・システムに配布します。

エンドポイント・システム (iSeries サーバー B、C、D、E)

- iSeries B、C は、 OS/400 バージョン5 リリース 2 (V5R2) を実行しています。
- iSeries D、E は、 OS/400 バージョン 5 リリース 1 (V5R1) を実行しています。
- iSeries B、C、D、E では、ディジタル証明書マネージャー (オプション 34) と、 IBM HTTP Server (5722-DG1) がインストールされて構成されています。
- iSeries B、C、D、E は、システムが署名されたアプリケーションを受け取る際に、企業の署名検査証明書およびセントラル・システム (iSeries A) からのローカル認証局 (CA) の両方のコピーを受け取ります。
- DCM は、*SIGNATUREVERIFICATION 証明書ストアを作成し、この証明書ストアにローカル認証局 (CA) と検査証明書をインポートするために使用されます。

前提条件

このシナリオは、次の前提条件に依存しています。

1. すべてのiSeries サーバーが、ディジタル証明書マネージャー (DCM) をインストールし、使用するための要件を満たしていること。
2. 使用する iSeries の DCM において、いかなる操作または構成が実施されていないこと。
3. iSeries A が、 iSeries ナビゲーターおよびマネージメント・セントラルをインストールし、使用するための要件を満たしていること。
4. マネージメント・セントラル・サーバーが、すべての iSeries エンドポイント・システムで稼働していること。
5. すべての iSeries サーバーに、最高レベルの Cryptographic Access Provider 128-bit ライセンス・プログラム (5722-AC3) がインストールされていること。
6. すべてのシナリオの iSeries サーバーにおける (QVFYOBJRST) システム値の復元中の検査オブジェクト署名のデフォルト設定は 3 で、この設定から変更されていないこと。デフォルト設定により、署名されたオブジェクトを復元する際に、サーバーが確実にオブジェクト署名を検査できること。
7. iSeries A のネットワーク管理者が *ALLOBJ ユーザー・プロファイル特殊権限を持っているか、またはユーザー・プロファイルがオブジェクト署名アプリケーションに対して許可されていること。

8. ネットワーク管理者または DCM に証明書ストアを作成する他の人物が、 *SECADM および *ALLOBJ ユーザー・プロファイルを持っていること。
9. 他のすべての iSeries サーバーで、システム管理者または他の人物が、オブジェクト署名を検査するための *AUDIT ユーザー・プロファイルを持っていること。

タスク手順

このシナリオを実現するために完了すべきタスクのセットは 2 つあります。 1 つ目のタスク・セットでは、 iSeries A をセットアップし、マネージメント・セントラルを使用して、アプリケーションの署名および配布を行います。もう 1 つのタスク・セットでは、システム管理者や他の人物が、他のすべての iSeries サーバー上でアプリケーションの署名を検査します。

オブジェクト署名のタスク手順

このシナリオが説明しているように、オブジェクトに署名するためには、以下のタスクを完了する必要があります。

1. すべての前提条件となるステップを完了し、必要な iSeries 製品をすべてインストールして構成します。
2. ディジタル証明書マネージャー (DCM) を使用して、ローカル認証局 (CA) を作成し、専用オブジェクト署名証明書を発行します。
3. DCM を使って、 アプリケーション定義を作成します。
4. DCM を使って、オブジェクト署名アプリケーション定義に対して証明書を割り当てます。
5. DCM を使って、他のシステムがオブジェクト署名の検査に使用する必要のある証明書をエクスポートします。ローカル認証局 (CA) 証明書のコピーと、オブジェクト署名証明書のコピーの両方を、署名検査証明書としてファイルにエクスポートすることが必要です。
6. 署名を検査する予定の各 iSeries エンドポイント・システムに、 証明書ファイルを転送します。
7. マネージメント・セントラルを使って、 アプリケーション・オブジェクトに署名します。

署名検査のタスク手順

マネージメント・セントラルを使って、署名付きのアプリケーション・オブジェクトを転送する前に、各 iSeries エンドポイント・システムで、以下の署名検査構成タスクを完了することが必要です。エンドポイント・システム上で署名付きオブジェクトを復元する際に、正常に署名の検査を行うには、署名検査構成を完了しておかなければなりません。

各 iSeries エンドポイント・システムで、次のタスクを完了し、このシナリオが説明するとおりオブジェクト署名を検査することが必要です。

8. ディジタル証明書マネージャー (DCM) を使用して、*SIGNATUREVERIFICATION 証明書ストアを作成します。
9. DCM を使用して、ローカル認証局 (CA) 証明書および署名検査証明書をインポートします。

構成の詳細

次のタスク手順にしたがってマネージメント・セントラルを構成し、このシナリオの説明どおりオブジェクトに署名します。

ステップ 1: すべての前提条件を完了する

すべての前提条件タスクを完了し、必要な iSeries 製品すべてを構成してから、このシナリオを実現する特定の構成タスクを実行できます。

ステップ 2: ローカル認証局 (CA) を作成して専用オブジェクト署名証明書を発行する

ディジタル証明書マネージャー (DCM) を使用してローカル認証局 (CA) を作成する場合、そのプロセスでは一連のフォームを完了することが必要です。これらのフォームが、CA の作成プロセスと、 Secure Socket Layer (SSL)、オブジェクト署名、および署名検査を実行するためのディジタル証明書を使用するために必要となる他のタスクを完了させるプロセスをガイドします。このシナリオでは SSL の証明書を構成する必要はありませんが、タスク中のすべてのフォームを完了し、オブジェクトに署名するためにシステムを構成する必要があります。

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

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、**「認証局 (CA) の作成 (Create a Certificate Authority (CA))」**を選択すると、一連のフォームが表示されます。

   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れば、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。このタスクを実行する場合、以下のことを行う必要があります。
   a. ローカル認証局 (CA) についての識別情報を提供します。
   b. ブラウザーにローカル認証局 (CA) 証明書をインストールして、ユーザー側のソフトウェアでローカル認証局 (CA) を認識し、そのローカル認証局 (CA) が発行する証明書の妥当性検査ができるようにします。
   c. ローカル認証局 (CA) についてのポリシー・データを指定します。
   d. 新規ローカル認証局 (CA) を使用して、アプリケーションが SSL 接続に使用できるサーバーまたはクライアント証明書を発行します。

      注: このシナリオでは使用しませんが、必要なオブジェクト署名証明書を発行するためにローカル認証局 (CA) を使用するには、この証明書を作成する必要があります。この証明書を作成しないでタスクを取り消すと、オブジェクト署名証明書と、その証明書が個別に保管される *OBJECTSIGNING 証明書を作成する必要が生じます。
   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: このシナリオの目的に合わせるため、どのアプリケーションも選択せずに**「Continue (続行)」**をクリックして、次のフォームを表示してください。
   f. 新規ローカル認証局 (CA) を使用して、アプリケーションがオブジェクトにディジタル署名するために使用できるオブジェクト署名証明書を発行します。このサブタスクは *OBJECTSIGNING 証明書ストアを作成します。これは、オブジェクト署名証明書を管理するために使用する証明書ストアです。
   g. ローカル認証局 (CA) を信頼する必要があるアプリケーションを選択します。

      注: このシナリオの目的に合わせるため、どのアプリケーションも選択せずに**「続行 (Continue)」**をクリックして、タスクを終了してください。

これでローカル認証局 (CA) とオブジェクト署名証明書を作成したので、次に、オブジェクトに署名できるように、証明書を使用するオブジェクト署名アプリケーションを定義します。

ステップ 3: オブジェクト署名アプリケーション定義を作成する

オブジェクト署名証明書の作成後、ディジタル証明書マネージャー (DCM) を使用して、オブジェクトに署名するのに使用するオブジェクト署名アプリケーションを定義します。アプリケーション定義は、実際のアプリケーションを参照する必要はありません。作成するアプリケーション定義は、署名対象オブジェクトのタイプまたはグループを表します。証明書と関連付けて、署名プロセスを可能にするためのアプリケーション ID を持つには、定義が必要です。

DCM を使用してオブジェクト署名を作成するには、以下のステップに従ってください。

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)」**をクリックして、オープンする証明書ストアとして ***OBJECTSIGNING** を選択します。
2. 「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。
3. 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。
4. 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。
5. フォームを完成させて、**「追加 (Add)」**をクリックします。

次に、オブジェクト署名証明書を、作成したアプリケーションに割り当てます。

ステップ 4: 証明書をオブジェクト署名アプリケーション定義に割り当てる

証明書をオブジェクト署名アプリケーションに割り当てる手順は、次のとおりです。

1. DCM 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。
2. 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。
3. リストから証明書を選択して、**「アプリケーションへの割り当て (Assign to Applications)」**をクリックし、現行の証明書ストアのアプリケーション定義のリストを表示します。
4. リストから 1 つ以上のアプリケーションを選択し、**「続行 (Continue)」**をクリックします。メッセージ・ページが表示され、証明書の割り当てを確認するか、問題が発生した場合エラー情報を提供します。

このタスクを完了すると、マネージメント・セントラルのパッケージおよび配布時に、マネージメント・セントラルを使用してオブジェクトに署名する準備ができたことになります。しかし、だれかが必ず署名を検査できるようにするには、必要な証明書をファイルにエクスポートし、証明書をすべての iSeries エンドポイント・システムに転送します。マネージメント・セントラルを使って、署名付きのアプリケーション・オブジェクトを転送する前に、各 iSeries エンドポイント・システムで、すべての署名検査構成タスクを完了することも必要です。エンドポイント・システム上で署名付きオブジェクトを復元する際に、正常に署名の検査を行うには、署名検査構成を完了しておかなければなりません。

ステップ 5: 他の iSeries システムでの署名検査を可能にするために証明書をエクスポートする

内容の整合性を保護するためのオブジェクトへの署名には、署名の認証性を検査する手段がなければなりません。オブジェクトに署名する同じシステム上のオブジェクト署名を検査するには、 DCM を使って *SIGNATUREVERIFICATION 証明書ストアを作成することが必要です。この証明書ストアには、オブジェクト署名証明書、および署名証明書を発行した CA 証明書のコピーの両方が入っていなければなりません。

他の人も署名を検査できるようにするには、オブジェクトに署名した証明書のコピーを提供することが必要です。ローカル認証局 (CA) を使用して証明書を発行する場合、ローカル認証局 (CA) 証明書のコピーも提供する必要があります。

オブジェクトに署名したのと同じシステム (このシナリオでは iSeries A) で署名を検査できるように DCM を使用する手順は、次のとおりです。

1. ナビゲーション・フレームで**「証明書ストアの選択 (Select New Certificate Store)」**を選択して、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。
2. **「はい (Yes)」**を選択して、既存の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します。
3. 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。これで、DCM を使用して、オブジェクトに署名するのに使用するのと同じシステムでオブジェクト署名を検査できます。

DCM を使ってローカル認証局 (CA) 証明書のコピーとオブジェクト署名証明書のコピーを署名検査証明書としてエクスポートし、他のシステムでオブジェクト署名を検査できるようにする手順は、次のとおりです。

1. ナビゲーション・フレームで、**「証明書の管理 (Manage Certificates)」**を選択してから、**「証明書のエクスポート (Export certificate)」**タスクを選択します。
2. **「認証局 (CA) (Certificate Authority (CA))」**を選択して、**「続行 (Continue)」**をクリックすると、エクスポートできる CA 証明書のリストが表示されます。
3. リストから以前に作成したローカル認証局 (CA) 証明書を選択して、**「エクスポート (Export)」**をクリックします。
4. **「ファイル (File)」**をエクスポートの宛先として指定して、**「続行 (Continue)」**をクリックします。
5. エクスポートされるローカル認証局 (CA) 証明書の完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックし、証明書をエクスポートします。
6. **「OK」**をクリックして「エクスポート (Export)」確認ページを終了します。これで、オブジェクト署名証明書のコピーをエクスポートできます。
7. **「証明書のエクスポート (Export certificate)」**タスクを再度選択します。
8. **「オブジェクト署名 (Object signing)」**を選択し、エクスポートできるオブジェクト署名証明書のリストを表示します。
9. リストから適切なオブジェクト署名証明書を選択して、**「エクスポート (Export)」**をクリックします。
10. 宛先として**「署名検査証明書としてのファイル (File, as a signature verification certificate)」**を選択して、**「続行 (Continue)」**をクリックします。
11. エクスポートされる署名検査証明書の完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックし、証明書をエクスポートします。

これで、これらのファイルを、証明書を使って作成した書名を検査する iSeries エンドポイント・システムに転送することができます。

ステップ 6: 証明書ファイルを iSeries エンドポイント・システムに転送する

署名付きオブジェクトの検査のために、 iSeries A で作成した証明書ファイルを構成する前に、このシナリオの iSeries エンドポイント・システムに証明書ファイルを転送することが必要です。証明書ファイルの転送にはいくつかの方法があります。たとえば、ファイル転送プロトコル (FTP) またはマネージメント・セントラルのパッケージ配布機能を使ってファイルを転送できます。

ステップ 7: マネージメント・セントラルを使ってオブジェクトに署名する

マネージメント・セントラルのオブジェクト署名のプロセスは、ソフトウェア・パッケージ配布プロセスの一部です。マネージメント・セントラルを使って、署名付きのアプリケーション・オブジェクトを転送する前に、各 iSeries エンドポイント・システムで、すべての署名検査構成タスクを完了することが必要です。エンドポイント・システム上で署名付きオブジェクトを復元する際に、正常に署名の検査を行うには、署名検査構成を完了しておかなければなりません。

このシナリオの iSeries エンドポイント・システムに配布するアプリケーションに署名する手順は、次のとおりです。

1. マネージメント・セントラルを使って、ソフトウェア製品をパッケージおよび配布します。
2. **「製品の定義 (Product Definition)」**ウィザードで**「識別 (Identification)」**パネルが表示されたら、**「拡張 (Advanced)」**をクリックして**「拡張識別 (Advanced Identification)」**パネルを表示します。
3. **「ディジタル署名 (Digital signing)」**フィールドに、 以前作成したオブジェクト署名アプリケーションのアプリケーション ID を入力し、**「OK」**をクリックします。
4. ウィザードを完了し、マネージメント・セントラルを使って、 ソフトウェア製品をパッケージおよび配布するプロセスを続行します。

ステップ 8: 署名検査タスク: iSeries エンドポイント・システムで *SIGNATUREVERIFICATION 証明書ストアを作成する

このシナリオの iSeries エンドポイント・システムでオブジェクト署名を検査するためには、各システムの *SIGNATUREVERIFICATION 証明書ストアに、それぞれの署名に対応する署名検査証明書がなければなりません。専用証明書がオブジェクトに署名した場合、この証明書ストアにローカル認証局 (CA) 証明書のコピーも入っていなければなりません。

*SIGNATUREVERIFICATION 証明書ストアを作成する手順は、次のとおりです。

1. DCM を開始します。
2. ディジタル証明書マネージャー (DCM) ナビゲーション・フレームで**「証明書ストアの選択 (Select New Certificate Store)」**を選択して、オープンする証明書ストアとして ***SIGNATUREVERIFICATION** を選択します。

   注: 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れば、ページの上部にある疑問符 (**?**) を選択してください。オンライン・ヘルプが表示されます。
3. 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。これで、証明書をストアにインポートしてから、オブジェクト署名の検査に使うことができます。

ステップ 9: 署名検査タスク: 証明書をインポートする

オブジェクトの証明書を検査するためには、 *SIGNATUREVERIFICATION ストアに署名検査証明書のコピーがなければなりません。署名証明書が専用である場合、この証明書ストアには、署名証明書を発行したローカル認証局 (CA) 証明書のコピーを持っていなければなりません。このシナリオでは、両方の証明書がファイルにエクスポートされ、そのファイルが各 iSeries エンドポイント・システムに転送されました。

これらの証明書を *SIGNATUREVERIFICATION 証明書ストアにインポートする手順は、次のとおりです。

1. DCM 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。
2. 「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。
3. 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。
4. 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。
5. 証明書タイプとして**「認証局 (CA) (Certificate Authority (CA))」** を選択し、**「続行 (Continue)」**をクリックします。

   注: 専用署名検査証明書をインポートする前にローカル認証局 (CA) 証明書をインポートする必要があります。そうしないと、署名検査証明書のインポート処理に失敗します。
6. CA 証明書ファイルの完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックします。インポート処理が正常に実行されたことを確認するメッセージか、処理に失敗した場合はエラー情報を提供するメッセージが表示されます。
7. **「証明書のインポート (Import certificate)」**タスクを再度選択します。
8. **「署名検査 (Signature verification)」**を証明書タイプとして選択し、**「続行 (Continue)」**をクリックします。
9. 署名検査証明書ファイルの完全修飾パスおよびファイル名を指定して、**「続行 (Continue)」**をクリックします。インポート処理が正常に実行されたことを確認するメッセージか、処理に失敗した場合はエラー情報を提供するメッセージが表示されます。

これで、 iSeries システムは、署名付きオブジェクトの復元時に、対応する署名証明書で作成されたオブジェクトの署名を検査できます。

オブジェクト署名の概念

iSeries のオブジェクト署名と署名検査機能の使用を開始する前に、これらの概念をいくらか復習するとよいでしょう。

ディジタル署名
ディジタル署名とは何か、またディジタル署名が提供する保護について学びます。

署名可能オブジェクト
署名可能な iSeries オブジェクトと、コマンド (*CMD) オブジェクト署名オプションについて学びます。

オブジェクト署名の処理
オブジェクト署名の処理のしくみや、その処理に設定できるパラメーターについて学びます。

署名検査の処理
オブジェクト署名検査の処理のしくみや、その処理に設定できるパラメーターについて学びます。

ディジタル署名

OS/400 は、ディジタル方式でオブジェクトに「署名」するためのディジタル署名の使用をサポートしています。オブジェクトのディジタル署名は、一般の文書の署名に相当するもので、暗号形式で作成されます。ディジタル署名は、オブジェクトの発信元を証明し、そのオブジェクトの保全性を検査する手段になります。ディジタル証明書の所有者は、その証明書の秘密鍵を使用してオブジェクトに「署名」します。オブジェクトの受信側では、対応する公開鍵を使って署名を復号し、署名済みオブジェクトの保全性を検証し、送信側をソースとして検証します。

オブジェクト署名のサポートは、オブジェクトを変更できる人を制御する、これまでの iSeries サーバー・ツールを補うものです。従来の制御機能では、オブジェクトがインターネットまたは他の非トラステッド・ネットワーク経由で転送されている間や、iSeries 以外のシステムに保管されている間は、非許可ユーザーによる不正操作からオブジェクトを保護することができません。署名の後にオブジェクトの内容が変更されているかどうかを検査できるので、そのようなオブジェクトが信用できるかどうかを容易に判断できます。

ディジタル署名とは、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ことです。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、署名付きオブジェクトを改めて入手します。

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)。

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ら、 公開証明書とローカル証明書の発行のどちらの手段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するつもりなら、既知の公開認証局 (CA) の証明書を使用してオブジェクトに署名することを考えるべきです。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、だれでも簡単に安く確認することができます。しかし、オブジェクトを組織内だけで配布するつもりなら、 ディジタル証明書マネージャー (DCM) を使用して、独自のローカル認証局 (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こともできます。ローカル認証局 (CA) からの専用証明書を使用してオブジェクトに署名すれば、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。

ディジタル署名のタイプ

V5R2 以降、コマンド (*CMD) オブジェクトに署名できるようになりました。また、*CMD オブジェクトでは、 2 つのタイプの署名、つまり、コア・オブジェクト署名と全体オブジェクト署名のどちらかを選択できます。

- **全体オブジェクト署名**
  このタイプの署名は、オブジェクトのバイトをすべてカバーします (ただし、ごく一部の非基本バイトを除きます)。
- **コア・オブジェクト署名**
  このタイプの署名は、*CMD オブジェクトの基本バイトだけをカバーします。より頻繁に変更されるバイトはカバーしません。このタイプの署名を使用すると、署名を無効にすることなく、コマンドに変更を加えることができます。コア・オブジェクト署名がカバーしないバイトは、それぞれの *CMD オブジ

ェクトによって異なりますが、基本的に、*CMD オブジェクトのパラメーター・デフォルトはカバーしません。コマンドに変更を加えても、コア・オブジェクト署名が無効にならないケースとしては、次のような場合があります。

– コマンド・デフォルトを変更した場合。
– 妥当性検査プログラムを持たないコマンドに妥当性検査プログラムを追加した場合。
– 実行が許可されている場所に関するパラメーターを変更した場合。
– 制限ユーザーの許可に関するパラメーターを変更した場合。

署名可能な iSeries オブジェクト、およびコア・オブジェクト署名がカバーする *CMD オブジェクトのバイトについては、 署名可能オブジェクトを参照してください。

署名可能オブジェクト

署名に使用する方法に関係なく、さまざまなタイプの OS/400 オブジェクトにディジタル方式で署名できます。システムの統合ファイル・システムに保管されているオブジェクト (*STMF) は、ライブラリーに保管されているオブジェクトを除いてすべて署名できます。オブジェクトに Java™ プログラムが接続されている場合は、そのプログラムにも署名が付くことになります。 QSYS.LIB ファイル・システムで署名できるオブジェクトは、プログラム (*PGM)、サービス・プログラム (*SRVPGM)、モジュール (*MODULE)、SQL パッケージ (*SQLPKG)、 *FILE (保管ファイルのみ)、コマンド (*CMD) だけになります。

オブジェクトに署名するには、そのオブジェクトがローカル・システムになければなりません。たとえば、統合 xSeries サーバー (iSeries 用) で Windows® 2000 サーバーを運用する場合、統合ファイル・システムの中に QNTC ファイル・システムがあります。このファイル・システムのディレクトリーは、ローカルとは見なされません。これらのディレクトリーに、 Windows 2000 オペレーティング・システムが所有するファイルが入っているためです。また、空のオブジェクトや、 V5R1 より前のリリース用にコンパイルされたオブジェクトに署名することもできません。

コマンド (*CMD) オブジェクトの署名

*CMD オブジェクトの署名時、2 つの署名のタイプ から 1 つを選んで、*CMD オブジェクトに適用できます。つまり、オブジェクト全体に署名するか、オブジェクトのコア部分のみに署名するかを選択になります。オブジェクト全体に署名する場合は、オブジェクトのごく一部の非基本バイトを除いてすべてのバイトに署名が適用されます。全体オブジェクト署名は、コア・オブジェクト署名に入っている項目をカバーします。

コア・オブジェクトだけに署名する場合は、基本バイトだけが署名によって保護されることになり、頻繁に変更されるバイトには署名が付きません。署名されないバイトは、それぞれの *CMD オブジェクトによって異なりますが、基本的には、オブジェクトが有効になっているモードを判別するバイトや、オブジェクトの実行が許可されている場所を判別するバイトなどがそれに当たります。たとえば、 *CMD オブジェクトのパラメーター・デフォルトは、コア署名でカバーされません。このタイプの署名を使用すると、その署名を無効にすることなく、コマンドに変更を加えることができます。コマンドに変更を加えても、この種の署名が無効にならないケースとしては、次のような場合があります。

- コマンドのデフォルト値を変更した場合。
- 妥当性検査プログラムを持たないコマンドに妥当性検査プログラムを追加した場合。
- 実行が許可されている場所に関するパラメーターを変更した場合。
- 制限ユーザーの許可に関するパラメーターを変更した場合。

次の表は、コア・オブジェクト署名の一部として含められる、 *CMD オブジェクトのバイトを詳細にまとめたものです。

***CMD オブジェクトのコア・オブジェクト署名の構成**

オブジェクトの一部	コア・オブジェクト署名との関係
CHGCMDDFT が変更するコマンド・デフォルト	コア・オブジェクト署名の一部でない
コマンドとライブラリーを処理するプログラム	常にコア・オブジェクト署名の一部として含められる
REXX ソース・ファイルとライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
REXX ソース・メンバー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
REXX コマンド環境とライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
REXX 出口プログラム名、ライブラリー、終了コード	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
妥当性検査プログラムとライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
有効になっているモード	コア・オブジェクト署名の一部でない
実行が許可されている場所	コア・オブジェクト署名の一部でない
制限ユーザーの許可	コア・オブジェクト署名の一部でない
ヘルプ・ブックシェルフ	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
ヘルプ・パネル・グループとライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
ヘルプ ID	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
ヘルプ検索索引とライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
現行ライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
製品ライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
プロンプト指定変更プログラムとライブラリー	署名時にコマンドに指定される場合はコア・オブジェクト署名に含められ、そうでない場合は含められない
テキスト (説明)	オブジェクトに保管されていないため、コア・オブジェクト署名の一部でも全体オブジェクト署名の一部でもない
グラフィカル・ユーザー・インターフェース (GUI) の使用可能化	コア・オブジェクト署名の一部でない

オブジェクト署名の処理

オブジェクトに署名するときには、オブジェクト署名の処理に次のオプションを指定できます。

- **エラー処理**

  1 つ以上のオブジェクトで署名を作成する場合に、アプリケーションが使用するエラー処理のタイプを指定します。エラーの発生時に、アプリケーションがオブジェクトの署名を停止するか、それともプロセス中の他のオブジェクトの署名を続行するかを指定できます。

- **オブジェクト署名の重複**
  アプリケーションがオブジェクトに再署名する場合に、署名プロセスをどう扱うかを指定できます。元の署名をそのままにしておくか、元の署名を新しい署名で置き換えるかを選択できます。
- **サブディレクトリー内のオブジェクト**
  アプリケーションが、サブディレクトリー内のオブジェクトの署名をどう扱うかを指定できます。アプリケーションがサブディレクトリー内のオブジェクトに個別に署名するか、アプリケーションがすべてのサブディレクトリーを無視し、メイン・ディレクトリー内のオブジェクトにのみ署名するかを指定できます。
- **オブジェクト署名の有効範囲**
  *CMD オブジェクトの署名時、オブジェクト全体に署名するか、オブジェクトのコア部分だけに署名するかを指定できます。

署名検査の処理

署名検査の処理には、次のオプションを指定できます。

- **エラー処理**
  1 つ以上のオブジェクトの署名を検査する場合に、アプリケーションが使用するエラー処理のタイプを指定します。エラーの発生時に、アプリケーションが署名検査を停止するか、それともプロセス中の他のオブジェクトの署名検査を続行するかを指定できます。
- **サブディレクトリー内のオブジェクト**
  アプリケーションが、サブディレクトリー内のオブジェクトの署名検査をどう扱うかを指定できます。アプリケーションがサブディレクトリー内のオブジェクトの署名を個別に検査するか、アプリケーションがすべてのサブディレクトリーを無視し、メイン・ディレクトリー内のオブジェクトの署名だけを検査するかを指定できます。
- **コア署名検査と全体署名検査**
  検査プロセスで、システムがオブジェクトのコア署名と全体署名を扱う方法を判別するシステム規則があります。これらの規則は、次のとおりです。
  - オブジェクト上に署名がない場合、検査プロセスはオブジェクトが署名されていないことをレポートし、プロセス中の他のオブジェクトの検査を続行します。
  - オブジェクトがシステム・トラステッド・ソース (IBM) により署名された場合、署名は一致しなければならず、一致しないと検査プロセスは失敗します。署名が一致する場合、検査プロセスは続行します。署名とは、オブジェクト内のデータの数学的要約を暗号化することです。したがって、検査中のオブジェクトのデータが、署名時のオブジェクトのデータに一致する場合、その署名は一致すると見なされます。
  - オブジェクトに信頼できる (*SIGNATUREVERIFICATION 証明書ストアに含まれる証明書に基づく) 全体オブジェクト署名がある場合、これらの署名のうち最低 1 つが一致しなければ検査プロセスは失敗します。 1 つでも全体オブジェクト署名が一致する場合、検査プロセスは続行します。
  - オブジェクトに信頼できるコア・オブジェクト署名がある場合、これらの署名のうち最低 1 つが *SIGNATUREVERIFICATION 証明書ストアにある証明書に一致しなければ検査プロセスは失敗します。 1 つでもコア・オブジェクト署名が一致する場合、検査プロセスは続行します。

オブジェクト署名と署名検査の前提条件

OS/400 のオブジェクト署名と署名検査の機能は、 iSeries サーバー上のオブジェクトを制御するための強力な手段になります。これらの機能を利用するには、その使用に関する前提条件を満たす必要があります。

オブジェクト署名の前提条件

自分の業務やセキュリティーのニーズに合わせて、オブジェクト署名に使用できる方法がいくつかあります。

- ディジタル証明書マネージャー (DCM) を使用できます。
- オブジェクト署名 API を使用するプログラムを作成できます。
- iSeries ナビゲーターのマネージメント・セントラルを使って、 iSeries エンドポイント・システムに配布するためにパッケージする際にオブジェクトに署名できます。

オブジェクト署名のために選択する方法は、業務やセキュリティーのニーズによって異なります。オブジェクト署名に使用する方法に関係なく、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。

- ディジタル証明書マネージャー (DCM) のインストールと使用に関する前提条件を満たしている必要があります。
  - DCM を使って *OBJECTSIGNING 証明書ストアを作成する必要があります。 ローカル認証局 (CA) の作成プロセスの一部、または公開インターネット CA のオブジェクト署名証明書の管理プロセスの一部として、この証明書ストアを作成します。
  - *OBJECTSIGNING 証明書ストアには、少なくとも 1 つの証明書 (ローカル認証局 (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、 DCM を使ってオブジェクト署名アプリケーション定義を少なくとも 1 つ作成しなければなりません。
  - DCM を使って、オブジェクト署名アプリケーション定義に特定の証明書を割り当てておかなければなりません。
- オブジェクトに署名する iSeries ユーザー・プロファイルには、*ALLOBJ 特殊権限がなければなりません。 *SIGNATUREVERIFICATION 証明書ストアを作成する iSeries ユーザー・プロファイルには、*SECADM および *ALLOBJ 特殊権限が必要です。

署名検査の前提条件

オブジェクト署名を検査するための方法は、いくつかあります。

- ディジタル証明書マネージャー (DCM) を使用できます。
- オブジェクトの検査 (QYDOVFYO) API を使用するプログラムを作成できます。
- オブジェクト整合性の検査 (CHKOBJITG) コマンドなど、たくさんのコマンドのうちの 1 つを使用できます。

署名検査のために選択する方法は、業務やセキュリティーのニーズによって異なります。使用する方法に関係なく、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。

- ディジタル証明書マネージャー (DCM) のインストールと使用に関する前提条件を満たしている必要があります。
- *SIGNATUREVERIFICATION 証明書ストアを作成する必要があります。この証明書ストアの作成には、必要に合わせて 2 つの方法から 1 つを選べます。 1 つの方法として、ディジタル証明書マネージャー (DCM) を使用して、 署名検査証明書を管理できます。または、公開証明書を使ってオブジェクトに署名している場合、証明書の追加 (QYDOADDV) API を使用するプログラムを作成することにより、この証明書ストアを作成できます。

注: 証明書の追加 API は、デフォルト・パスワードで証明書ストアを作成します。証明書ストアに権限のない人がアクセスしないよう、 DCM を使って自分の選択の 1 つに対してこのデフォルト・パスワードをリセットすることが必要です。

- *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。この証明書を証明書ストアに追加するには、2 つの方法があります。署名システムで DCM を使用して、ファイルに証明書をエクスポートしてから、ターゲット検査システムで DCM を使用して *SIGNATUREVERIFICATION 証明書ストアに証明書をインポートできます。または、公開証明書を使ってオブジェクトに署名している場合、証明書の追加 API を使用するプログラムを作成することにより、ターゲット検査システムの証明書ストアに証明書を追加できます。
- *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。公開証明書を使ってオブジェクトに署名している場合、ターゲット検査システム上の証明書ストアには、必要な CA 証明書のコピーがなければなりません。しかし、ローカル認証局 (CA) が発行した証明書を使ってオブジェクトに署名している場合は、 DCM を使ってターゲット検査システム上の証明書ストアに、ローカル認証局 (CA) 証明書のコピーを追加する必要があります。

  注: セキュリティー上の理由から、証明書の追加 API は認証局 (CA) 証明書を *SIGNATUREVERIFICATION 証明書ストアに挿入することを許可しません。 CA 証明書を証明書ストアに追加すると、システムは CA を証明書のトラステッド・ソースと見なします。その結果、システムは CA が発行した証明書を、トラステッド・ソースに由来しているものとして扱います。それで、この API を使用して、 CA 証明書を証明書ストアに挿入するためのインストール出口プログラムを作成することはできません。 CA 証明書を証明書ストアに追加し、システムに信頼される CA を個別かつ手動で制御するようにするには、ディジタル証明書マネージャーを使用する必要があります。そのようにすると、管理者がわざと信頼できるものとして指定しなかったソースから、システムが証明書をインポートしてしまう可能性を防ぐことができます。

  ローカル認証局 (CA) が発行する証明書を使用してオブジェクトに署名している場合、ローカル認証局 (CA) ホスト iSeries サーバー上で DCM を使用して、ローカル認証局 (CA) 証明書のコピーをファイルにエクスポートする必要があります。その後、 iSeries サーバーを検査するターゲットで DCM を使用して、ローカル認証局 (CA) 証明書を *SIGNATUREVERIFICATION 証明書ストアにインポートできます。発生する可能性のあるエラーを防ぐには、証明書の追加 API を使って署名検査証明書を追加する前に、ローカル認証局 (CA) 証明書をこの証明書ストアにインポートすることが必要です。その結果、ローカル認証局 (CA) が発行する証明書を使用している場合、 DCM を使用して CA 証明書と検査証明書の両方を証明書ストアにインポートするのが容易になります。

  だれかがこの API を無許可で使用して、 *SIGNATUREVERIFICATION 証明書ストアに検査証明書を追加することを防ぐには、システムでこの API の使用を使用不可にすることを考慮する必要があります。これは、システム・サービス・ツール (SST) を使用してセキュリティー関連のシステム値への変更の許可を解除する ことによって行えます。
- 署名を検査する iSeries ユーザー・プロファイルには、*AUDIT 特殊権限がなければなりません。*SIGNATUREVERIFICATION 証明書ストアを作成するか、またはそのパスワードを変更する iSeries ユーザー・プロファイルには、 *SECADM および *ALLOBJ 特殊権限が必要です。

署名付きオブジェクトの管理

V5R1 以降、 IBM は、 IBM に由来するものとしてオペレーティング・システムに公式にマーキングする方法や、権限のない変更がシステム・オブジェクトに加えられた場合にそれを検出する方法として、OS/400 ライセンス・プログラムと PTF の署名を行います。また、ビジネス・パートナーや他のベンダーも、購入するアプリケーションに署名することがあります。それで、自分はオブジェクトに署名しない場合でも、署名付きオブジェクトの処理方法や、署名付きオブジェクトがルーチン・システム管理タスクに与える影響を理解しておく必要があります。

署名付きオブジェクトは、基本的に、バックアップとリカバリーのタスク、特にシステムにおけるオブジェクトの保管方法と復元方法に影響します。

署名付きオブジェクトに影響するシステム値とコマンド
署名付きオブジェクトの管理に使用できる (実行時に署名付きオブジェクトに影響を与える) システム値とコマンドについて説明します。

署名付きオブジェクトの保管と復元に関する考慮事項
署名付きオブジェクトが、システムにおける保管および復元タスクの実行にどのように影響するかを説明します。

署名の整合性を確認するコード・チェッカー・コマンド
オブジェクト署名を検査してオブジェクトの整合性を判別するコマンドの使用について詳しく説明します。

署名付きオブジェクトに影響するシステム値とコマンド

署名付きオブジェクトを効果的に管理するには、システム値とコマンドがどのように署名付きオブジェクトに影響するかを理解する必要があります。**復元中のオブジェクト署名の検査** (QVFYOBJRST) システム値は、特定の復元コマンドが署名付きオブジェクトに与える影響や、システムが復元操作中に署名付きオブジェクトを扱う方法を決定します。 iSeries システム上で署名付きオブジェクトを処理するための専用の CL コマンドはありません。しかし、署名付きオブジェクトを管理する (またはオブジェクト署名を可能にする下部構造オブジェクトを管理する) 共通の CL コマンドはたくさんあります。他のコマンドは、オブジェクトから署名を除去し、それによって署名が提供する保護を無効にすることにより、システム上の署名付きオブジェクトに悪い影響を与えます。

署名付きオブジェクトに影響するシステム値

復元中のオブジェクト署名の検査 (QVFYOBJRST) システム値は、 OS/400 システム値の復元カテゴリーのメンバーで、コマンドがシステム上の署名付きオブジェクトに与える影響を決定します。このシステム値は、 iSeries ナビゲーターから操作できるものであり、システムが復元操作中に署名検査を扱う方法を制御します。このシステム値で使用する設定は、他の 2 つのシステム値設定と一緒に使用すると、システムの復元操作に影響します。この値に選択する設定によっては、オブジェクトを署名状態に基づいて復元することが可能になったり不可能になったりします。 (たとえば、オブジェクトに署名が付かない、オブジェクトに無効な署名が付く、トラステッド・ソースによる署名が付く、などの影響があります。) このシステム値をデフォルトに設定しておくと、署名のないオブジェクトは復元できますが、署名のあるオブジェクトは、その署名が有効なものである場合だけ復元可能になります。システムがオブジェクトを署名済みと定義するのは、そのオブジェクトの署名をシステムが承認している場合だけです。システムは、オブジェクトのそれ以外の「承認されていない」署名は無視し、そのオブジェクトを署名がないものと同様に扱います。

QVFYOBJRST システム値で使用できる値は、すべての署名を無視するものから、システムが復元するすべてのオブジェクトに有効な署名を必要とするものまで、いくつかの種類があります。このシステム値は、プログラム (*PGM)、コマンド (*CMD)、サービス・プログラム (*SRVPGM)、SQL パッケージ (*SQLPKG)、モジュール (*MODULE) など、復元中の実行可能オブジェクトにのみ影響します。また、Java プログラムの作成 (CRTJVAPGM) コマンドが作成する、 Java プログラム・オブジェクトを関連付けたストリーム・ファイル (*STMF) オブジェクトにも適用されます。保管 (*SAV) ファイルや IFS ファイルには適用されません。

このシステム値や他のシステム値の使用について詳しく知りたい場合は、 Information Center の『システム値ファインダー』を参照してください。

署名付きオブジェクトに影響する CL コマンド

署名付きオブジェクトを処理したり、 iSeries サーバー上の署名付きオブジェクトに影響したりする CL コマンドは、いくつもあります。さまざまなコマンドを使用して、オブジェクトの署名情報を表示したり、オブジェクトの署名を検査したり、署名検査に必要なセキュリティー・オブジェクトを復元したりできます。さらに、実行時にオブジェクトからの署名を除去し、署名が提供するセキュリティーを無効にできる一群のコマンドもあります。

オブジェクトの署名情報を表示するコマンド

- オブジェクト記述の表示 (DSPOBJD) コマンド。
  このコマンドは、指定されたライブラリーまたはスレッドのライブラリー・リスト中のライブラリーで、指定されたオブジェクトの名前と属性を表示します。このコマンドを使って、オブジェクトが署名されるかどうかを決定し、署名に関する情報を表示できます。
- オブジェクト・リンクの表示 (DSPLNK) およびオブジェクト・リンクの処理 (WRKLNK) 統合ファイル・システム・コマンド。
  これらのコマンドのどちらかを使用すると、統合ファイル・システムのオブジェクトに関する署名情報を表示できます。

オブジェクト署名を検査するコマンド

- オブジェクト整合性の検査 (CHKOBJITG) コマンド。
  このコマンドを使用すると、システム上のオブジェクトに整合性違反があるかどうかを判別できます。このコマンドでは、ウィルスがシステム上のファイルなどのオブジェクトを破壊した場合に、ウィルス・チェッカーを使ってそれを判別するのとほとんど同じ方法で署名を検査できます。署名付きオブジェクトと署名可能オブジェクトでこのコマンドを使用するための詳細については、『署名の整合性を確認するコード・チェッカー・コマンド』を参照してください。
- 製品オプションの検査 (CHKPRDOPT) コマンド。
  このコマンドは、正しい構造と、ソフトウェア製品の実際の構造の違いをレポートします。たとえば、インストール済みの製品からオブジェクトが削除されると、そのエラーをレポートします。 CHKSIG パラメーターを使用して、コマンドが製品の署名問題を処理し、レポートする方法を指定できます。署名付きオブジェクトと署名可能オブジェクトでこのコマンドを使用するための詳細については、『署名の整合性を確認するコード・チェッカー・コマンド』を参照してください。
- ライセンス・プログラムの保管 (SAVLICPGM) コマンド。
  このコマンドは、ライセンス・プログラムを構成するオブジェクトのコピーを保管します。ライセンス・プログラムは、ライセンス・プログラムの復元 (RSTLICPGM) コマンドで復元できるような形式で保管されています。 CHKSIG パラメーターを使用して、コマンドが製品の署名問題を処理し、レポート

する方法を指定できます。署名付きオブジェクトと署名可能オブジェクトでこのコマンドを使用するための詳細については、『署名の整合性を確認するコード・チェッカー・コマンド』を参照してください。

- 復元 (RST) コマンド。
  このコマンドは、統合ファイル・システム (IFS) で使用できる 1 つ以上のオブジェクトのコピーを復元します。また、システム上の証明書ストアとその内容を復元することもできます。しかし、このコマンドを使って、 *SIGNATUREVERIFICATION 証明書ストアを復元することはできません。復元コマンドが署名付きオブジェクトと署名可能オブジェクトを処理する方法は、復元中のオブジェクト署名の検査 (QVFYOBJRST) システム値の設定によって決定されます。
- ライブラリーの復元 (RSTLIB) コマンド。
  このコマンドは、ライブラリーの保管 (SAVLIB) コマンドが保管したライブラリー、またはライブラリーのグループを復元します。 RSTLIB コマンドは、ライブラリー記述、オブジェクト記述、およびライブラリー中のオブジェクトの内容を含むライブラリー全体を復元します。このコマンドが署名付きオブジェクトと署名可能オブジェクトを処理する方法は、復元中のオブジェクト署名の検査 (QVFYOBJRST) システム値の設定によって決定されます。
- ライセンス・プログラムの復元 (RSTLICPGM) コマンド。
  このコマンドは、初期インストール用、または新リリース・インストール用のどちらかに、ライセンス・プログラムをロードまたは復元します。このコマンドが署名付きオブジェクトと署名可能オブジェクトを処理する方法は、復元中のオブジェクト署名の検査 (QVFYOBJRST) システム値の設定によって決定されます。
- オブジェクトの復元 (RSTOBJ) コマンド。
  このコマンドは、単一のコマンドを使ってディスケット、テープ、光学式ボリューム、または保管ファイルに保管された、 1 つ以上のオブジェクトを 1 つのライブラリーで復元します。このコマンドが署名付きオブジェクトと署名可能オブジェクトを処理する方法は、復元中のオブジェクト署名の検査 (QVFYOBJRST) システム値の設定によって決定されます。

証明書ストアを保管および復元するコマンド

- 保管 (SAV) コマンド。
  このコマンドは、証明書ストアを含め、統合ファイル・システムで使用できる 1 つ以上のオブジェクトのコピーを復元します。しかし、このコマンドを使って *SIGNATUREVERIFICATION 証明書ストアを保管することはできません。
- セキュリティー・データの保管 (SAVSECDTA) コマンド。
  このコマンドを使用すると、システムを制限された状態にしなくても、すべてのセキュリティー情報を保管できます。また、*SIGNATUREVERIFICATION 証明書ストアとその中の証明書を保管できます。このコマンドは、他の証明書ストアは保管しません。
- システムの保管 (SAVSYS) コマンド。
  このコマンドによって、ライセンス内部コードと QSYS ライブラリーのコピーを、 iSeries サーバーのインストールと互換性のある形式で保管できます。他のライブラリーからのオブジェクトは保管しません。さらに、SAVSECDTA および SAVCFG コマンドでも保管できる、セキュリティーおよび構成オブジェクトを保管できます。また、*SIGNATUREVERIFICATION 証明書ストアとその中の証明書を保管できます。
- 復元 (RST) コマンド。
  このコマンドにより、システム上の証明書ストアとその内容を復元できます。しかし、このコマンドを使って、 *SIGNATUREVERIFICATION 証明書ストアを復元することはできません。
- ユーザー・プロファイルの復元 (RSTUSRPRF) コマンド。
  このコマンドにより、システムの保管 (SAVSYS) かセキュリティー・データの保管 (SAVSECDTA) コ

マンドで保管したユーザー・プロファイルの基本部分、またはユーザー・プロファイルのセットを復元できます。このコマンドを使用すると、*SIGNATUREVERIFICATION 証明書ストア、およびこの証明書ストアと他のすべての証明書ストアの隠されたパスワードを復元できます。 *DCM を SECDTA パラメーターの値に、*NONE を USRPRF パラメーターの値として指定することによって、ユーザー・プロファイル情報を復元せずに、 *SIGNATUREVERIFICATION 証明書ストアを復元できます。このコマンドを使用して、ユーザー・プロファイル情報および証明書ストアとそのパスワードを復元するには、USRPRF パラメーターに *ALL を指定します。

オブジェクトから署名を除去するコマンド

以下に示すコマンドを署名付きオブジェクトに使用すると、オブジェクトから署名を除去することになります。署名を除去すると、オブジェクトに影響を与え、問題が発生することがあります。最低でも、オブジェクトのソースをトラステッド・ソースとして検査できなくなり、オブジェクトへの変更を検出する署名検査もできなくなります。これらのコマンドは、作成した署名付きオブジェクトでのみ使用するべきです (IBM またはベンダーなどの他者から取得した署名付きオブジェクトでは使用しない)。コマンドがオブジェクトの署名を除去した不安がある場合は、オブジェクト記述の表示 (DSPOBJD) コマンドを使用して、署名がまだあるかどうかを確認し、必要なら再署名することができます。

注: 保管コマンドがオブジェクト署名を除去したかどうかを検査するには、保管元とは異なるライブラリー (たとえば QTEMP) にオブジェクトを復元する必要があります。その後、DSPOBJD コマンドを使用して、保管メディアのオブジェクトが署名を失ったかどうかを判別します。

- プログラムの変更 (CHGPGM) コマンド。
  このコマンドは、再コンパイルせずにプログラムの属性を変更します。また、指定されている属性が現行の属性と同じである場合でも、このコマンドを使用すればプログラムの再作成を強制できます。
- サービス・プログラムの変更 (CHGSRVPGM) コマンド。
  このコマンドは、再コンパイルせずにサービス・プログラムの属性を変更します。また、指定されている属性が現行の属性と同じである場合でも、このコマンドを使用すればサービス・プログラムの再作成を強制できます。
- 保管ファイルの消去 (CLRSAVF) コマンド。
  このコマンドは、保管ファイルの内容を消去します。保管ファイルからすべての既存レコードを消去し、ファイルが使用するストレージの量を削減します。
- 保管 (SAV) コマンド。
  このコマンドは、統合ファイル・システムで使用できる 1 つ以上のオブジェクトのコピーを保管します。− このコマンドの使用時、TGTRLS パラメーターに V5R2M0 より前の値を指定すると、保管メディア上のコマンド (*CMD) オブジェクトから署名が失われることがあります。署名の脱落は、 V5R2 より前のリリースではコマンド・オブジェクトに署名できないために発生します。
- ライブラリーの保管 (SAVLIB) コマンド。
  このコマンドにより、1 つ以上のライブラリーのコピーを保管できます。このコマンドの使用時、TGTRLS パラメーターに V5R2M0 より前の値を指定すると、保管メディア上のコマンド (*CMD) オブジェクトから署名が失われることがあります。署名の脱落は、 V5R2 より前のリリースではコマンド・オブジェクトに署名できないために発生します。
- オブジェクトの保管 (SAVOBJ) コマンド。
  このコマンドは、同一ライブラリーにあるオブジェクトまたはオブジェクトのグループのコピーを保管します。このコマンドの使用時、TGTRLS パラメーターに V5R2M0 より前の値を指定すると、保管メディア上のコマンド (*CMD) オブジェクトから署名が失われることがあります。署名の脱落は、 V5R2 より前のリリースではコマンド・オブジェクトに署名できないために発生します。

署名付きオブジェクトの保管と復元に関する考慮事項

iSeries サーバーの復元操作に影響を与える可能性のあるシステム値がいくつかあります。それらのシステム値のうち、**復元中のオブジェクト署名の検査 (QVFYOBJRST)** システム値のみが、復元時にシステムが署名付きオブジェクトを扱う方法を決定します。このシステム値に選択する設定により、復元操作時に、署名なしオブジェクト、または無効な署名を持つオブジェクトの検査を扱う方法を決定できます。

保管および復元コマンドによっては、保管および復元操作中に署名付きオブジェクトに影響するものや、署名付きオブジェクトや署名なしオブジェクトを扱う方法を決定するものがあります。システムをより良い方法で管理できるように、また発生する可能性のある潜在的な問題を避けるために、署名付きオブジェクトに対するこれらのコマンドの影響をよく理解しておくことが必要です。

以下のコマンドは、保管および復元操作中にオブジェクトの署名を検査できます。

- ライセンス・プログラムの保管 (SAVLICPGM) コマンド。
- 復元 (RST) コマンド。
- ライブラリーの復元 (RSTLIB) コマンド。
- ライセンス・プログラムの復元 (RSTLICPGM) コマンド。
- オブジェクトの復元 (RSTOBJ) コマンド。

以下のコマンドを使用すると、証明書ストアを保管し、復元することができます。証明書ストアは、オブジェクトに署名し、署名を検査するのに使用する証明書を含む、セキュリティー対応オブジェクトです。

- 保管 (SAV) コマンド。
- セキュリティー・データの保管 (SAVSECDTA) コマンド。
- システムの保管 (SAVSYS) コマンド。
- 復元 (RST) コマンド。
- ユーザー・プロファイルの復元 (RSTUSRPRF) コマンド。

使用するパラメーター値によっては、いくつかの保管コマンドが保管メディア上のオブジェクトから署名を脱落させ、それによって署名が提供するセキュリティーが無効になる場合があります。たとえば、V5R2M0 より前のターゲット・リリースを持つコマンド (*CMD) オブジェクトを参照するすべての 保管操作は、コマンドが署名なしで保管される原因になります。署名を除去すると、オブジェクトに影響を与え、問題が発生することがあります。最低でも、オブジェクトのソースをトラステッド・ソースとして検査できなくなり、オブジェクトへの変更を検出する署名検査もできなくなります。これらのコマンドは、作成した署名付きオブジェクトでのみ使用するべきです (IBM またはベンダーなどの他者から取得した署名付きオブジェクトでは使用しない)。

注: 保管コマンドがオブジェクト署名を除去したかどうかを検査するには、保管元とは異なるライブラリー (たとえば QTEMP) にオブジェクトを復元する必要があります。その後、DSPOBJD コマンドを使用して、保管メディアのオブジェクトが署名を失ったかどうかを判別します。

この問題に関して、一般の保管コマンドに加え、特に次の保管コマンドに注意してください。

- 保管 (SAV) コマンド。
- ライブラリーの保管 (SAVLIB) コマンド。
- オブジェクトの保管 (SAVOBJ) コマンド。

保管および復元操作中に、これらのコマンドが署名付きオブジェクトとオブジェクト署名に与える影響については、『署名付きオブジェクトに影響するシステム値とコマンド』を参照してください。

署名の整合性を確認するコード・チェッカー・コマンド

ディジタル証明書マネージャー (DCM) または API を使用して、オブジェクトの署名を検査できます。また、いくつかのコマンドを使って署名を検査することもできます。これらのコマンドでは、ウィルスがシステム上のファイルなどのオブジェクトを破壊した場合に、ウィルス・チェッカーを使ってそれを判別するのとほとんど同じ方法で署名を検査できます。ほとんどの署名は、たとえば RSTLIB コマンドを使って、オブジェクトがシステムに復元またはインストールされるのと同時に検査されます。

3 つのコマンドのうち 1 つを選択し、すでにシステム上にあるオブジェクトの署名を検査できます。その中で、オブジェクト整合性の検査 (CHKOBJITG) コマンドは、特にオブジェクト署名の検査用に設計されています。これらの各コマンドの署名検査は、 CHKSIG パラメーターによって制御されます。このパラメーターを使用すると、署名できるすべてのオブジェクト・タイプで署名を検査したり、すべての署名を無視したり、署名付きオブジェクトだけを検査したりすることができます。最後のオプションがパラメーターのデフォルト値です。

オブジェクト整合性の検査 (CHKOBJITG) コマンド

オブジェクト整合性の検査 (CHKOBJITG) コマンドを使用すると、システム上のオブジェクトに整合性違反があるかどうかを判別できます。このコマンドを使って、特定のユーザー・プロファイルが所有するオブジェクト、特定のパス名と一致するオブジェクト、またはシステム上のすべてのオブジェクトの整合性違反を検査できます。整合性違反ログ・エントリーは、以下のいずれかの条件が満たされると発生します。

- コマンド、プログラム、モジュール・オブジェクト、またはライブラリーの属性が変更されている場合。
- オブジェクトのディジタル署名が無効であると判断された場合。署名とは、オブジェクト内のデータの数学的要約を暗号化することです。したがって、検査中のオブジェクトのデータが、署名時のオブジェクトのデータに一致する場合、その署名は一致し、有効であると見なされます。無効な署名は、署名検査中にオブジェクトが署名され、数学的要約が暗号化された場合に作成される、暗号化された数学的要約の比較に基づいて判別されます。署名検査プロセスは、2 つの要約値を比較します。値が同じでない場合、オブジェクトの内容が署名後に変更されたということで、署名は無効と見なされます。
- オブジェクトのドメイン属性が、オブジェクト・タイプに合わない場合。

コマンドがオブジェクトの整合性違反を検出する場合、オブジェクト名、ライブラリー名 (またはパス名)、オブジェクト・タイプ、障害のタイプがデータベース・ログ・ファイルに追加されます。また、整合性違反ではないケースでログ・エントリーが作成されることもあります。たとえば、署名可能であるのにディジタル署名がないオブジェクト、検査できなかったオブジェクト、現行のシステム・インプリメンテーションで使用するため、変更 (IMPI から RISC への変換) が必要とされる形式のオブジェクトなどについて、ログ・エントリーが作成されます。

CHKSIG パラメーター値は、コマンドがオブジェクトのディジタル署名を扱う方法を制御します。このパラメーターには、次の 3 つの値のうち 1 つを指定できます。

- *SIGNED - この値を指定すると、コマンドはディジタル署名を持つオブジェクトを検査します。このコマンドは、無効な署名を持つオブジェクトについてログ・エントリーを作成します。これがデフォルト値です。
- *ALL - この値を指定すると、コマンドはすべての署名可能オブジェクトを検査し、署名があるかどうかを判別します。このコマンドは、署名がない署名可能オブジェクトと、無効な署名の付いたオブジェクトについてログ・エントリーを作成します。
- *NONE - この値を指定すると、コマンドはオブジェクトのディジタル署名を検査しません。

製品オプションの検査 (CHKPRDOPT) コマンド

製品オプションの検査 (CHKPRDOPT) コマンドは、正しい構造と、ソフトウェア製品の実際の構造の違いをレポートします。たとえば、インストール済みの製品からオブジェクトが削除されると、そのエラーをレポートします。

CHKSIG パラメーター値は、コマンドがオブジェクトのディジタル署名を扱う方法を制御します。このパラメーターには、次の 3 つの値のうち 1 つを指定できます。

- *SIGNED - この値を指定すると、コマンドはディジタル署名を持つオブジェクトを検査します。このコマンドは、署名付きオブジェクトの署名を検査します。このコマンドがオブジェクトの署名が無効であると判断した場合、ジョブ・ログにメッセージが送信され、製品はエラー状態であると識別されます。これがデフォルト値です。
- *ALL - この値を指定すると、コマンドはすべての署名可能オブジェクトを検査し、署名があるかどうかを判別し、署名可能オブジェクトの署名を検査します。このコマンドは、署名がない署名可能オブジェクトについてジョブ・ログにメッセージを送信します。しかし、製品がエラー状態であるとは見なされません。このコマンドがオブジェクトの署名が無効であると判断した場合、ジョブ・ログにメッセージが送信され、製品はエラー状態であると見なされます。
- *NONE - この値を指定すると、コマンドは製品オブジェクトのディジタル署名を検査しません。

ライセンス・プログラムの保管 (SAVLICPGM) コマンド

ライセンス・プログラムの保管 (SAVLICPGM) コマンドは、ライセンス・プログラムを構成するオブジェクトのコピーを保管します。ライセンス・プログラムは、ライセンス・プログラムの復元 (RSTLICPGM) コマンドで復元できるような形式で保管されています。

CHKSIG パラメーター値は、コマンドがオブジェクトのディジタル署名を扱う方法を制御します。このパラメーターには、次の 3 つの値のうち 1 つを指定できます。

- *SIGNED - この値を指定すると、コマンドはディジタル署名を持つオブジェクトを検査します。このコマンドは、署名付きオブジェクトの署名を検査しますが、署名なしオブジェクトは検査しません。このコマンドがオブジェクトの署名が無効であると判断した場合、ジョブ・ログにメッセージが送信されて、オブジェクトが無効と見なされ、保管は失敗します。これがデフォルト値です。
- *ALL - この値を指定すると、コマンドはすべての署名可能オブジェクトを検査し、署名があるかどうかを判別し、署名可能オブジェクトの署名を検査します。このコマンドは、署名がない署名可能オブジェクトについてジョブ・ログにメッセージを送信します。しかし、保管プロセスは終了しません。このコマンドがオブジェクトの署名が無効であると判断した場合、ジョブ・ログにメッセージが送信され、保管は失敗します。
- *NONE - この値を指定すると、コマンドは製品オブジェクトのディジタル署名を検査しません。

署名付きオブジェクトのトラブルシューティング

以下の表は、 iSeries のオブジェクト署名と署名検査の機能で発生する問題のうち、比較的一般的と思われる問題のトラブルシューティングに役立つ情報をまとめたものです。

オブジェクト署名の一般的な問題

問題	可能な解決方法
オブジェクトの署名 API を使用し、ターゲット・リリース V4R5 以前でオブジェクトに署名しようとすると、署名プロセスは失敗し、オブジェクトは署名されません (エラー・メッセージ CPFB721)。	iSeries は、V5R1 までオブジェクト署名をサポートしていませんでした。エラー・メッセージ CPFB721 を戻すオブジェクトに署名するには、ターゲット・リリース V5R1 以降を使用してプログラムを再作成する必要があります。

署名検査の一般的な問題

問題	可能な解決方法
署名のないオブジェクトの場合に復元プロセスが失敗します。	署名がないことが関係ない場合、 QVFYOBJRST システム値が 5 に設定されているかどうかを調べてください。値 5 は、署名なしオブジェクトを復元しないという設定です。値を 3 に変更して再度復元してみてください。
署名付きオブジェクトの場合に復元プロセスが失敗します。	これは、*SIGNATUREVERIFICATION 証明書ストアがシステムに転送され、そのパスワードを変更するのに DCM が使用されなかった場合に発生することがあります。このような場合、ストア中にある証明書を使用して、復元プロセス中にオブジェクトの署名を検査することはできません。 DCM を使用して証明書ストアのパスワードを変更してください。パスワードが分からない場合は、証明書ストアを削除する必要があります。証明書ストアを再作成してから DCM を使ってパスワードを変更してください。
製品の復元またはインストール時に、署名検査に失敗したためにエラーを受け取ります。	オブジェクト署名の検査に失敗した場合、その障害はオブジェクトが署名後に変更されていることを示している場合があります。オブジェクト整合性が問題である場合は、QVFYOBJRST システム値を変更したり、問題のあるオブジェクトを復元する可能性のある他のアクションを実行したりすべきではありません。そうすると、署名検査によるセキュリティーが機能しなくなり、システム上に有害なオブジェクトが存在することになります。それらのアクションを実行するのではなく、オブジェクト署名者と連絡と取り、適切なアクションを判断して問題を解決してください。

オブジェクト署名と署名検査の関連情報

オブジェクト署名と署名検査は、比較的新しいセキュリティー技術です。これらの技術とそれぞれのしくみに関する理解を深めるのに役立つ、その他のトピックのいくつかを以下に記載します。

- **VeriSign Help Desk Web サイト**
  VeriSign Web サイトは、他のインターネット・セキュリティー問題と同様に、オブジェクト署名などのディジタル証明書のトピックに関する幅広いライブラリーを提供しています。
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  この IBM レッド・ブックは、 V5R1 ネットワーク・セキュリティーの拡張機能に焦点を当てています。 iSeries のオブジェクト署名機能、ディジタル証明書マネージャー (DCM) などを含め、数多くのトピックを取り上げています。

Printed in Japan

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