IBM

System i

セキュリティー
Secure Sockets Layer (SSL)

バージョン 6 リリース 1

System i

セキュリティー
Secure Sockets Layer (SSL)

バージョン 6 リリース 1

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、 25 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。

本書は、i5/OS (5761–SS1) バージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

http://www.ibm.com/jp/manuals/

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

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： System i
Security
Secure Sockets Layer
Version 6 Release 1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

Secure Sockets Layer (SSL)

このトピックでは、ご使用のサーバーで Secure Sockets Layer (SSL) を使用する方法について説明します。

Secure Sockets Layer (SSL) は、非保護ネットワーク (インターネットなど) を介して、アプリケーションでセキュアな通信セッションを行えるようにするための業界標準になっています。

V6R1 の新機能

Secure Sockets Layer (SSL) のトピック・コレクションの新規または重要な変更情報についてお読みください。

新規情報: システム SSL

システム SSL は、SSL/TLS プロトコルを使用して TCP/IP 通信を保護するために、i5/OS® Licensed Internal Code (LIC) で提供される一般的なサービスのセットです。システム SSL はオペレーティング・システム、および追加のパフォーマンスおよびセキュリティーを特別に供給するソケット・コードと密結合しています。

以下のトピックはシステム SSL を説明するために追加されました。

- 18 ページの『システム SSL』
- 18 ページの『システム SSL プロパティー』

システム SSL の新規システム値

以下のシステム値が追加されました。

- SSL システム値: QSSLPCL
- SSL システム値: QSSLCSLCTL
- SSL システム値: QSSLCSL

新規箇所または変更箇所を見つける方法

技術上の変更点を見つけるには、次の記号を使用します。

- » 記号は、新規の情報または変更された情報の開始点を示します。
- « 記号は、新規の情報または変更された情報の終了を示します。

PDF ファイルでは、新規および変更された情報の左マージンに、リビジョン・バー (|) が表示されることがあります。

このリリースの新機能または変更に関する他の情報を見つけるには、『プログラム資料説明書』を参照してください。

SSL 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、「Secure Sockets Layer (SSL)」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。

シナリオ: SSL

SSL シナリオは、System i™ プラットフォームで SSL を使用可能にすることによって得られる利点を、最大限に活用することを目的としています。

SSL 使用の実現可能な例を提供する SSL シナリオを読むことで、i5/OS での SSL の実行に関する理解を深めることができます。

関連情報

シナリオ: SSL を使用した Telnet の保護

シナリオ: 暗号化ハードウェアを使用した秘密鍵の保護

シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護

このシナリオは、SSL を使用して、リモート・クライアントと System i モデルとの接続を保護する方法を説明しています。このモデルは、System i ナビゲーター のマネージメント・セントラル・サーバーを使用して、セントラル・システムとして機能しています。

状況:

ある企業が、数台の i5/OS システムを組み込んだローカル・エリア・ネットワーク (LAN) をオフィスに構築しています。この企業のシステム管理者であるボブは、この i5/OS システムの 1 つを LAN のセントラル・システム (今後、システム A と呼びます) に指定しました。ボブは、システム A でマネージメント・セントラル・サーバーを使用して、LAN 上にある他のエンドポイントをすべてを管理しています。

ボブは、システム A のマネージメント・セントラル・サーバーに、社内 LAN の外部のネットワークから接続されることを心配しています。ボブは出張が多いため、外出している間、マネージメント・セントラル・サーバーへのセキュアな接続が必要です。彼はオフィスにいない場合、自分の PC とマネージメント・セントラル・サーバーの間の接続を確実にセキュアにしたいと思っています。ボブは、自分の PC と

システム A のマネージメント・セントラル・サーバーで、SSL を使用可能にすることを決めました。このように SSL を使用可能にすると、出張時にマネージメント・セントラル・サーバーへの接続を確実にセキュアにすることができます。

目的:

ボブは、自分の PC とマネージメント・セントラル・サーバーの間の接続を確実にセキュアにしたいと思っています。ボブは、システム A 上のマネージメント・セントラル・サーバーと LAN 上のエンドポイントの間の接続に、セキュリティーを追加する必要は感じていません。この企業のオフィスで働いている他の従業員たちも、マネージメント・セントラル・サーバーへの接続に関して、追加のセキュリティーを必要としていません。ボブの計画は、接続でサーバー認証を使用するように、自分の PC とシステム A のマネージメント・セントラル・サーバーを構成することです。他の PC または LAN 上の i5/OS システムからマネージメント・セントラル・サーバーへの接続は、SSL により保護されていません。

詳細:

次の表は、PC クライアント上で SSL が使用可能であるか使用不可であるかに基づいて、使用される認証のタイプを説明したものです。

表 1. SSL によるクライアントとマネージメント・セントラル・サーバー間の接続の保護に必要な要素

ボブの PC での SSL の状況	システム A のマネージメント・セントラル・サーバーに指定された認証レベル	SSL 接続が使用可能か
SSL 設定はオフ	任意	いいえ
SSL 設定はオン	任意	はい (サーバー認証)

サーバー認証は、ボブの PC でマネージメント・セントラル・サーバーの証明書を認証することを意味します。マネージメント・セントラル・サーバーに接続する場合は、ボブの PC は SSL クライアントとして機能します。マネージメント・セントラル・サーバーは、SSL サーバーとして機能し、ID を証明しなければなりません。マネージメント・セントラル・サーバーは、ボブの PC が信頼する認証局 (CA) により発行された証明書を提供することによって、ID を証明します。

前提条件および前提事項

ボブは、自分の PC とシステム A のマネージメント・セントラル・サーバーの間の接続を保護するため、以下の管理タスクおよび構成タスクを行わなければなりません。

1. システム A を SSL の前提条件に合わせます。
2. システム A は i5/OS V5R3 以降で稼働します。
3. PC クライアントは System i Access for Windows® V5R3 以降の System i ナビゲーター で稼働します。
4. i5/OS システムの認証局 (CA) を取得します。
5. システム A 用に CA によって署名された証明書を作成します。
6. CA および証明書をシステム A に送信し、それらを鍵データベースにインポートします。
7. マネージメント・セントラル・サーバー ID およびすべての i5/OS システムのアプリケーション ID を証明書に割り当てます。 TCP セントラル・サーバー、データベース・サーバー、データ待ち行列サーバー、ファイル・サーバー、ネットワーク・プリント・サーバー、リモート・コマンド・サーバーおよびサインオン・サーバーは、すべて i5/OS システムです。
   a. システム A で、IBM® ディジタル証明書マネージャーを始動します。ボブが証明書の取得または作成を行います。もしくは、ここで認証システムのセットアップまたは変更を行います。

b. 「**証明書ストアの選択**」を選択します。
c. 「***SYSTEM**」を選択し、「**続行**」をクリックします。
d. 「*証明書ストア・パスワード*」に *SYSTEM を入力し、「**続行**」をクリックします。メニューが再ロードされたら、「**アプリケーションの管理**」を展開します。
e. 「**証明書割り当ての更新**」をクリックします。
f. 「**サーバー**」を選択し、「**続行**」をクリックします。
g. 「**マネージメント・セントラル・サーバー**」を選択し、「**証明書割り当ての更新**」をクリックします。これにより、証明書が使用するマネージメント・セントラル・サーバーに割り当てられます。
h. 「**新規証明書の割り当て**」をクリックします。DCM は、「証明書割り当ての更新」ページを再ロードして、確認メッセージを表示します。
i. 「**完了**」をクリックします。
j. すべてのクライアント・アクセス・サーバーに証明書を割り当てます。

8. CA を PC のクライアントにダウンロードします。

ボブがマネージメント・セントラル・サーバーで SSL を使用可能にする前に、SSL 前提条件のプログラムをインストールし、システムにディジタル証明書をセットアップする必要があります。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーで SSL を使用可能にできます。

構成ステップ

ボブは、SSL によって、自分の PC からシステム A のマネージメント・セントラル・サーバーへの接続を保護するために、次のステップを完了する必要があります。

1. 5 ページの『ステップ 1: System i ナビゲーター クライアントについて SSL を非アクティブにする』
2. 5 ページの『ステップ 2: マネージメント・セントラル・サーバーの認証レベルを設定する』
3. 5 ページの『ステップ 3: セントラル・システム上のマネージメント・セントラル・システムを再始動する』
4. 5 ページの『ステップ 4: System i ナビゲーター クライアントについて SSL をアクティブにする』
5. 6 ページの『オプショナル・ステップ: System i ナビゲーター クライアントについて SSL を非アクティブにする』

関連概念

21 ページの『SSL の前提条件』
このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

関連情報

DCM の構成

ディジタル証明書マネージャーの開始

構成の詳細: SSL によるマネージメント・セントラル・システムへのクライアント接続の保護

このトピックでは、SSL を使用してマネージメント・セントラル・サーバーへのクライアント接続を保護する拡張された構成ステップについて説明しています。

次の情報は、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護』に目を通していることを前提としています。

このシナリオでは、System i モデルは、企業のローカル・エリア・ネットワーク (LAN) のセントラル・システムに指定されています。 ボブは、セントラル・システム (ここではシステム A と呼びます) 上のマネージメント・セントラル・サーバーを使用して、企業のネットワークのエンドポイントを管理しています。次の情報で、マネージメント・セントラル・サーバーに対する外部のクライアント接続を保護するために必要なステップを行う方法を説明します。ボブがシナリオの構成ステップを完了するのを追っていきます。

関連概念

21 ページの『SSL の前提条件』
このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

6 ページの『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』
このシナリオは、SSL を使用して、System i モデルとのすべての接続を保護する方法を説明しています。このモデルは、System i ナビゲーターのマネージメント・セントラル・システムを使用して、セントラル・システムとして機能しています。

関連情報

証明書のはじめてのセットアップ

ステップ 1: System i ナビゲーター クライアントについて SSL を非アクティブにする:
このステップは、System i ナビゲーター クライアントで SSL を使用可能にしてある場合のみ必要です。

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. システム A を右クリックし、「**プロパティー**」を選択します。
3. 「**セキュア・ソケット**」タブをクリックし、「**SSL (Secure Sockets Layer) を接続に使用**」を選択解除します。
4. System i ナビゲーターを終了し、再始動します。

パッドロックが、System i ナビゲーター のマネージメント・セントラル・コンテナーから見えなくなります。これは、接続が非セキュアであるということを示しています。このことは、ボブが、クライアントと企業のセントラル・システムの間に SSL で保護された接続を保持していないことを示しています。

ステップ 2: マネージメント・セントラル・サーバーの認証レベルを設定する:

1. System i ナビゲーター で、「**マネージメント・セントラル**」を右クリックし、「**プロパティー**」を選択します。
2. 「**セキュリティー**」タブをクリックし、「**Secure Sockets Layer (SSL) を使用**」を選択します。
3. 認証レベルで**いずれか**を選択します。(System i Access for Windows で使用可能です)
4. 「**OK**」をクリックして、この値をセントラル・システムに設定します。

ステップ 3: セントラル・システム上のマネージメント・セントラル・システムを再始動する:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. システム A で、「**ネットワーク**」**-->**「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
3. 「**マネージメント・セントラル**」を右クリックし、「**停止**」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
4. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。

ステップ 4: System i ナビゲーター クライアントについて SSL をアクティブにする:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. システム A を右クリックし、「**プロパティー**」を選択します。

3. 「**セキュア・ソケット**」タブをクリックし、「**SSL (Secure Sockets Layer) を接続に使用**」を選択します。
4. System i ナビゲーターを終了し、再始動します。

パッドロックは、System i ナビゲーター のマネージメント・セントラル・サーバーの横に表示されます。これは、SSL で接続がセキュアになっていることを示します。このことは、ボブが、彼のクライアントと彼の企業のセントラル・システムの間の SSL でのセキュアな接続をアクティブにするのに成功したということを示しています。

注: この手順は、1 つの PC とマネージメント・セントラル・システムの間の接続のみをセキュアにします。マネージメント・セントラル・サーバーへの他のクライアント接続や、エンドポイントからマネージメント・セントラル・サーバーへの接続は、セキュアになりません。他のクライアントをセキュアにするためには、前提条件を満たしていることを確認してから、5 ページの『ステップ 4: System i ナビゲーター クライアントについて SSL をアクティブにする』を繰り返し行ってください。マネージメント・セントラル・サーバーとの他の接続を保護するには、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』を参照してください。

オプショナル・ステップ: System i ナビゲーター クライアントについて SSL を非アクティブにする:
ボブがオフィスで仕事をしていて、SSL 接続によって彼の PC のパフォーマンスに影響を与えたくない場合は、次のステップを実行することで簡単に SSL を非アクティブにすることができます。

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. システム A を右クリックし、「**プロパティー**」を選択します。
3. 「**セキュア・ソケット**」タブをクリックし、「**SSL (Secure Sockets Layer) を接続に使用**」を選択解除します。
4. System i ナビゲーターを終了し、再始動します。

シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護

このシナリオは、SSL を使用して、System i モデルとのすべての接続を保護する方法を説明しています。このモデルは、System i ナビゲーターのマネージメント・セントラル・システムを使用して、セントラル・システムとして機能しています。

状況:

ある企業が最近、複数の System i モデルをリモート・ロケーション (エンドポイント) に置く広域ネットワーク (WAN) をセットアップしました。エンドポイントは、メイン・オフィスにある 1 台のシステム (セントラル・システム) によって中央管理されています。トムは、この企業のセキュリティー・スペシャリストです。トムは、企業のセントラル・システムのマネージメント・セントラル・サーバーと、すべての i5/OS システムおよびクライアントとの間の接続を、すべてセキュアにするために、Secure Sockets Layer (SSL) を使用したいと思っています。

詳細:

トムは、SSL を使用することにより、マネージメント・セントラル・サーバーへのすべての接続を、**セキュアに**管理することができます。マネージメント・セントラル・サーバーで SSL を使用するには、トムは、セントラル・システムへのアクセスに使用する PC で、System i ナビゲーターを保護する必要があります。

トムは、マネージメント・セントラル・サーバー用に以下の 2 つの認証レベルを選択します。

サーバー認証

サーバー証明書の認証を行います。クライアントは、クライアントが PC 上の System i ナビゲーター にあるか、セントラル・システム上のマネージメント・セントラル・サーバーにあるかを検証する必要があります。System i ナビゲーターがセントラル・システムに接続しているとき、PC は SSL クライアントであり、セントラル・システムで実行しているマネージメント・セントラル・サーバーは SSL サーバーです。エンドポイント・システムに接続する場合は、セントラル・システムは SSL クライアントとして機能します。エンドポイント・システムは SSL サーバーとして機能し、サーバーは、クライアントが信頼する認証局によって発行された証明書を提供することによって、クライアントに ID を証明しなければなりません。すべての SSL サーバーには、トラステッド CA から有効な証明書が発行される必要があります。

クライアントおよびサーバー認証

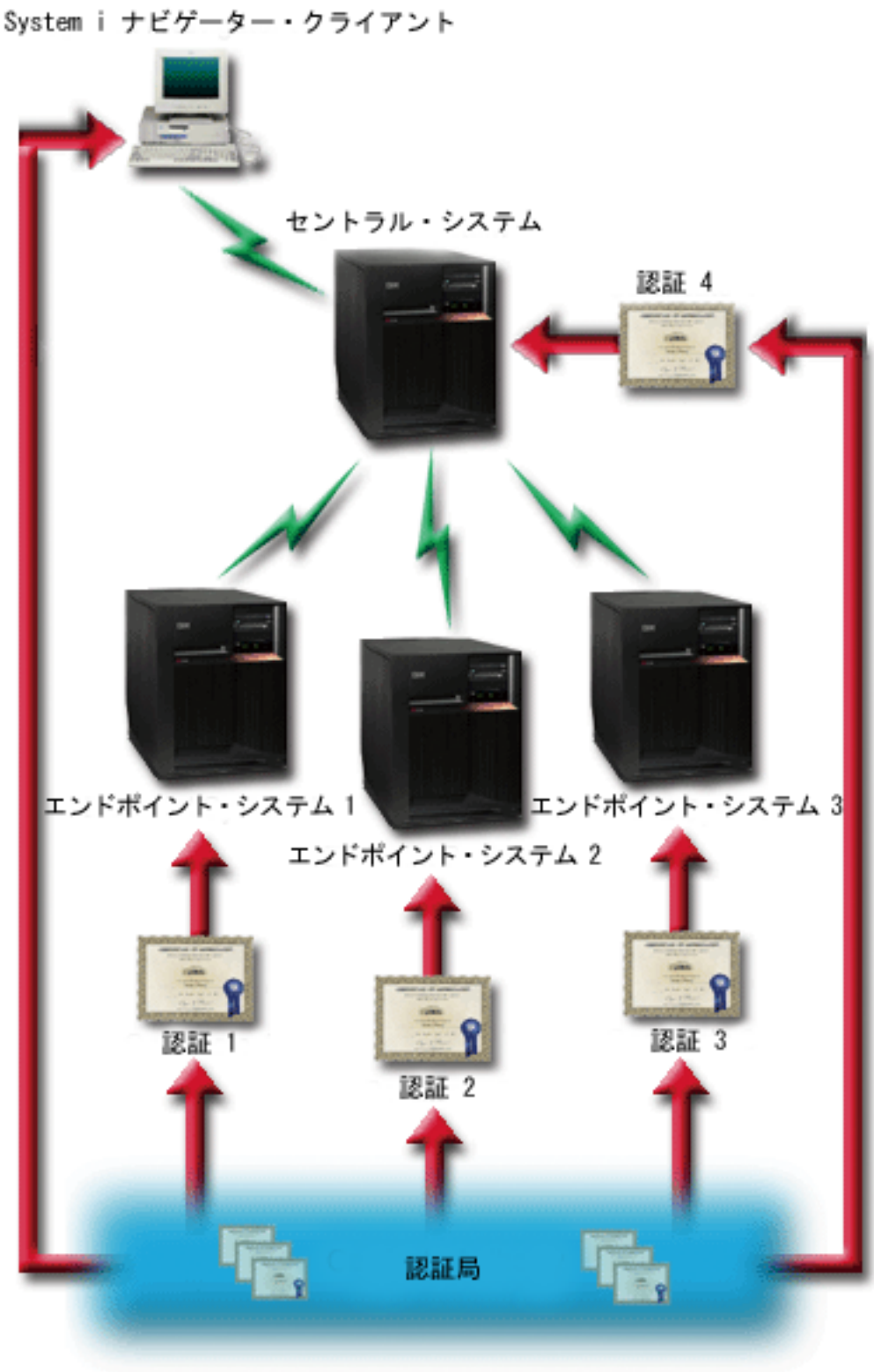
セントラル・システム証明書とエンドポイント・システム証明書の両方の認証を行います。この認証は、サーバー認証レベルよりも高いセキュリティー・レベルです。他のアプリケーションでは、この認証はクライアント認証と呼ばれています。その場合、クライアントは有効な信頼できる証明書を提供する必要があります。セントラル・システム (SSL クライアント) がエンドポイント・システム (SSL サーバー) との接続を確立しようとすると、セントラル・システムとエンドポイント・システムは、互いの証明書の CA 認証性を認証します。

注: クライアントおよびサーバー認証は、2 つの System i モデル間でのみ行われます。クライアントが PC の場合、クライアント認証はサーバーによって実行されません。

他のアプリケーションと異なり、マネージメント・セントラルは、トラステッド・グループ妥当性検査リストと呼ばれる妥当性検査リストを通して認証を提供します。一般に、妥当性検査リストには、ユーザーを識別する情報 (たとえば、ユーザー ID) と認証情報 (たとえば、パスワード、個人識別番号、ディジタル証明書) が保管されています。この認証情報は暗号化されています。

大半のアプリケーションでは通常、サーバー認証とクライアント認証の両方を使用可能にすることを指定しません。これは、サーバー認証が、ほとんど常に SSL セッションが使用可能になっている間に発生するためです。多くのアプリケーションには、クライアント認証の構成のオプションがあります。セントラル・システムがネットワークで果たす役割は 2 つあるので、マネージメント・セントラルでは、クライアント認証ではなく、「サーバーおよびクライアント認証」という用語を使用しています。PC ユーザーがセントラル・システムに接続している場合は、セントラル・システムはサーバーとして機能します。しかし、セントラル・システムがエンドポイント・システムに接続する場合、セントラル・システムはクライアントとして機能します。次の図は、セントラル・システムがネットワークでサーバーおよびクライアントとして機能する様子を示したものです。

注: この図では、認証局に関連付けられた証明書は、セントラル・システム、およびすべてのエンドポイント・システム上の鍵データベースに保管する必要があります。認証局は、PC、セントラル・システム、すべてのエンドポイントにある必要があります。



前提条件および前提事項

トムは、マネージメント・セントラル・サーバーへのすべての接続を保護するために、以下の管理タスクおよび構成タスクを行う必要があります。

1. システム A を SSL の前提条件に合わせます。
2. セントラル・システムおよびすべてのエンドポイント・システムは、OS/400® V5R2、または i5/OS V5R3 以降で稼働します。

   注: OS/400 V5R1 システムへの i5/OS V5R4 以降の接続は、許可されません。
3. PC クライアントは System i Access for Windows V5R3 以降の System i ナビゲーター で稼働します。
4. System i モデルの認証局 (CA) を取得します。
5. システム A 用に CA によって署名された証明書を作成します。
6. CA および証明書をシステム A に送信し、それらを鍵データベースにインポートします。
7. マネージメント・セントラル・アプリケーション ID およびすべての i5/OS システムのアプリケーション ID を証明書に割り当てます。 TCP セントラル・サーバー、データベース・サーバー、データ待ち行列サーバー、ファイル・サーバー、ネットワーク・プリント・サーバー、リモート・コマンド・サーバーおよびサインオン・サーバーは、すべて i5/OS システムです。
   a. マネージメント・セントラル・サーバーで IBM ディジタル証明書マネージャーを開始します。トムが証明書を取得または作成する必要がある場合、あるいは証明書システムをセットアップまたは変更する必要がある場合には、それをこの時点で行います。
   b. 「**証明書ストアの選択**」を選択します。
   c. 「***SYSTEM**」を選択し、「**続行**」をクリックします。
   d. 「**証明書ストア・パスワード**」に *SYSTEM を入力し、「**続行**」をクリックします。メニューが再ロードされたら、「**アプリケーションの管理**」を展開します。
   e. 「**証明書割り当ての更新**」をクリックします。
   f. 「**サーバー**」を選択し、「**続行**」をクリックします。
   g. 「**マネージメント・セントラル・サーバー**」を選択し、「**証明書割り当ての更新**」をクリックします。これにより、使用するマネージメント・セントラル・システムに証明書が割り当てられます。
   h. アプリケーションに割り当てる証明書を選択し、「**新規証明書の割り当て**」をクリックします。DCM は、「**証明書割り当ての更新**」ページを再ロードして、確認メッセージを表示します。
   i. 「**キャンセル**」をクリックし、アプリケーションのリストに戻ります。
   j. すべての i5/OS システムについて、この手順を繰り返します。
8. CA を System i ナビゲーターの PC クライアントにダウンロードします。

構成ステップ:

トムがマネージメント・セントラル・サーバーで SSL を使用可能にするためには、まずその前に前提条件のプログラムをインストールし、セントラル・システムにディジタル証明書をセットアップする必要があります。続行する前に、このシナリオの前提条件と前提事項を参照してください。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーですべての接続を保護できます。

注: SSL が System i ナビゲーター で使用可能になっている場合、トムは SSL をマネージメント・セントラル・サーバーで使用可能にする前に、SSL を使用不可にする必要があります。 SSL が System i ナビゲーターで使用可能であり、マネージメント・セントラル・サーバーでは使用可能でない場合は、System i ナビゲーターがセントラル・システムと接続しようとしても、失敗します。

1. 11 ページの『ステップ 1: サーバー認証用にセントラル・システムを構成する』
2. 11 ページの『ステップ 2: サーバー認証用にエンドポイント・システムを構成する』

3. 12 ページの『ステップ 3: セントラル・システム上のマネージメント・セントラル・システムを再始動する』
4. 12 ページの『ステップ 4: すべてのエンドポイント・システム上のマネージメント・セントラル・システムを再始動する』
5. 12 ページの『ステップ 5: System i ナビゲーター クライアントについて SSL をアクティブにする』
6. 13 ページの『ステップ 6: クライアント認証用にセントラル・システムを構成する』
7. 13 ページの『ステップ 7: クライアント認証用にエンドポイント・システムを構成する』
8. 14 ページの『ステップ 8: 妥当性検査リストをエンドポイント・システムにコピーする』
9. 14 ページの『ステップ 9: セントラル・システム上のマネージメント・セントラル・システムを再始動する』
10. 15 ページの『ステップ 10: すべてのエンドポイント・システム上のマネージメント・セントラル・システムを再始動する』

関連概念

21 ページの『SSL の前提条件』
このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

22 ページの『SSL によるアプリケーション・セキュリティー』
以下の System i プラットフォームで SSL を使用してセキュアにできるアプリケーションのリストを参照して検討してください。

関連タスク

4 ページの『構成の詳細: SSL によるマネージメント・セントラル・システムへのクライアント接続の保護』
このトピックでは、SSL を使用してマネージメント・セントラル・サーバーへのクライアント接続を保護する拡張された構成ステップについて説明しています。

『構成の詳細: SSL を使用したマネージメント・セントラル・システムへのすべての接続の保護』
このトピックでは、SSL を使用したマネージメント・セントラル・サーバーへのすべての接続の保護に関する詳細について説明しています。

関連情報

DCM の構成

証明書のはじめてのセットアップ

構成の詳細: SSL を使用したマネージメント・セントラル・システムへのすべての接続の保護

このトピックでは、SSL を使用したマネージメント・セントラル・サーバーへのすべての接続の保護に関する詳細について説明しています。

次の情報は、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべてのクライアント接続の保護』に目を通していることを前提としています。

ここで、マネージメント・セントラル・サーバーに対するすべての接続をセキュアにするのに必要なステップを実行する方法を理解します。トムがシナリオを完了するのを追っていきます。

トムがマネージメント・セントラル・システムで SSL を使用可能にするためには、まずその前に前提条件のプログラムをインストールし、System i モデルにディジタル証明書をセットアップする必要があります。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーですべての接続を保護できます。

注: SSL が System i ナビゲーター で使用可能になっている場合、トムは SSL をマネージメント・セントラル・サーバーで使用可能にする前に、SSL を使用不可にする必要があります。 SSL が System i ナビゲーター で使用可能であり、マネージメント・セントラル・サーバーでは使用可能でない場合は、System i ナビゲーター がセントラル・システムと接続しようとしても、失敗します。

トムは SSL を使用することで、セントラル・システムとエンドポイント・システムの間の伝送、および System i ナビゲーター クライアントとセントラル・システムの間の伝送をセキュアにすることができます。SSL では、証明書の移送と認証、およびデータの暗号化を行うことができます。SSL 接続が可能なのは、SSL が使用可能なセントラル・システムと SSL が使用可能なエンドポイント・システムの間だけです。トムは、クライアントの認証を構成する前に、サーバーの認証を構成する必要があります。

関連概念

21 ページの『SSL の前提条件』
このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

6 ページの『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』
このシナリオは、SSL を使用して、System i モデルとのすべての接続を保護する方法を説明しています。このモデルは、System i ナビゲーターのマネージメント・セントラル・システムを使用して、セントラル・システムとして機能しています。

関連情報

証明書のはじめてのセットアップ

ステップ 1: サーバー認証用にセントラル・システムを構成する:

1. System i ナビゲーター で、「**マネージメント・セントラル**」を右クリックし、「**プロパティー**」を選択します。
2. 「**セキュリティー**」タブをクリックし、「**Secure Sockets Layer (SSL) を使用**」を選択します。
3. 認証レベルとして「**サーバー**」を選択します。
4. 「**OK**」をクリックして、この値をセントラル・システムに設定します。

   注: 指示があるまで、マネージメント・セントラル・サーバーを再始動**しないでください**。ここでサーバーを再始動した場合、エンドポイント・サーバーに接続できません。SSL を活動化してサーバーを再始動する前に、さらに構成タスクを完了する必要があります。最初に、比較および更新タスクで、エンドポイント・システムへ SSL 構成を伝搬する必要があります。

ステップ 2: サーバー認証用にエンドポイント・システムを構成する:
トムは、セントラル・システムでサーバー認証を構成した後に、すべてのエンドポイント・システムにサーバー認証を構成する必要があります。次のタスクを実行します。

1. 「**マネージメント・セントラル**」を展開します。
2. エンドポイント・システムのシステム値を比較および更新します。
   a. 「**エンドポイント・システム**」において、「セントラル・システム」を右クリックし、「**インベントリー**」 → 「**収集**」の順に選択します。

b. セントラル・システムで使用しているシステム値のインベントリーを収集するために、「収集」ダイアログ・ボックスで「**システム値**」オプションをチェックします。他のオプションを選択解除します。「OK」をクリックし、インベントリー・タスクが完了するまで待機します。

c. 「**システム・グループ**」 → 「**新規システム・グループ**」の順に右クリックします。

d. SSL を使用して、接続するすべてのエンドポイント・システムを含む新規のシステム・グループを定義します。この新規システム・グループに「トラステッド・グループ」という名を付けます。

e. 新規グループ「トラステッド・グループ」を表示するには、システム・グループのリストを展開します。

f. 収集が完了した後に、新規のシステム・グループを右クリックして、「**システム値**」 → 「**比較および更新**」と選択します。

g. 「**モデル・システム**」フィールドにセントラル・システムが表示されていることを確認します。

h. 「**カテゴリー**」フィールドで、「**マネージメント・セントラル**」を選択します。

i. 「**Secure Sockets Layer (SSL) を使用**」が「**はい**」に設定されているかを確認し、「**更新**」を選択して、この値を「トラステッド・グループ」に伝搬します。

j. 「**SSL 認証レベル**」が「**サーバー**」に設定されているかを確認して、「**更新**」を選択し、この値を「トラステッド・グループ」に伝搬します。

注: これらの値を設定していない場合は、『ステップ 1: サーバー認証用にセントラル・システムを構成する』を完了してください。

k. 「**OK**」をクリックします。「**比較および更新**」で処理が完了するまで待機してから、次のステップに進んでください。

ステップ 3: セントラル・システム上のマネージメント・セントラル・システムを再始動する:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. セントラル・システムを展開します。
3. 「**ネットワーク**」 → 「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
4. 「**マネージメント・セントラル**」を右クリックし、「**停止**」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
5. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。

ステップ 4: すべてのエンドポイント・システム上のマネージメント・セントラル・システムを再始動する:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. 再始動するエンドポイント・システムを展開します。
3. 「**ネットワーク**」 → 「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
4. 「**マネージメント・セントラル**」を右クリックし、「**停止**」を選択します。
5. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。
6. それぞれのエンドポイント・システムについて、この手順を繰り返します。

ステップ 5: System i ナビゲーター クライアントについて SSL をアクティブにする:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. セントラル・システムを右クリックし、「**プロパティー**」を選択します。

3. 「**セキュア・ソケット**」タブをクリックし、「**SSL (Secure Sockets Layer) を接続に使用**」を選択します。
4. System i ナビゲーターを終了し、再始動します。

注: これらのステップを完了した後、サーバー認証がセントラル・システムおよびエンドポイント・システムで構成されます。同様に、クライアント認証のセントラル・システムおよびエンドポイント・システムをオプションで構成することができます。セントラル・システムおよびエンドポイント・システムでクライアント認証を使用可能にする場合は、ステップ 6 から 10 までを完了してください。

ステップ 6: クライアント認証用にセントラル・システムを構成する:

これで、トムはサーバー認証用の構成を終了したので、以下のオプションのクライアント認証手順の実行を選択できます。クライアント認証では、エンドポイント・システムとセントラル・システムの両方について、認証局とトラステッド・グループの妥当性検査を行います。セントラル・システム (SSL クライアント) が SSL を使用してエンドポイント・システム (SSL サーバー) に接続しようとした場合、セントラル・システムとエンドポイント・システムは、サーバー認証とクライアント認証により互いの証明書を認証します。また、これは、認証局 (CA) とトラステッド・グループの認証と呼ばれます。

注: サーバーの認証を構成するまで、クライアントの認証の構成は完了できません。サーバー認証を構成していない場合は、前に戻って構成してください。

1. System i ナビゲーター で、「**マネージメント・セントラル**」を右クリックし、「**プロパティー**」を選択します。
2. 「**セキュリティー**」タブをクリックし、「**Secure Sockets Layer (SSL) を使用**」を選択します。
3. 認証レベルの「**クライアントおよびサーバー**」を選択します。
4. 「**OK**」をクリックして、この値をセントラル・システムに設定します。

   注: 指示があるまで、マネージメント・セントラル・サーバーを再始動**しないでください**。ここでサーバーを再始動した場合、エンドポイント・サーバーに接続できません。SSL を活動化してサーバーを再始動する前に、さらに構成タスクを完了する必要があります。最初に、比較および更新タスクで、エンドポイント・システムへ SSL 構成を伝搬する必要があります。

ステップ 7: クライアント認証用にエンドポイント・システムを構成する:
エンドポイント・システムのシステム値を比較および更新します。

1. 「**マネージメント・セントラル**」を展開します。
2. エンドポイント・システムのシステム値を比較および更新します。
   a. 「**エンドポイント・システム**」において、「セントラル・システム」を右クリックし、「**インベントリー**」 → 「**収集**」の順に選択します。
   b. セントラル・システムで使用しているシステム値のインベントリーを収集するために、「収集」ダイアログ・ボックスで「**システム値**」オプションをチェックします。他のオプションを選択解除します。「OK」をクリックし、インベントリー・タスクが完了するまで待機します。
   c. 収集が完了した後に、「トラステッド・グループ」を右クリックして、「**システム値**」 → 「**比較および更新**」と選択します。
   d. 「**モデル・システム**」フィールドにセントラル・システムが表示されていることを確認します。
   e. 「**カテゴリー**」フィールドで、「**マネージメント・セントラル**」を選択します。
   f. 「**Secure Sockets Layer (SSL) を使用**」が「**はい**」に設定されているかを確認し、「**更新**」を選択して、この値を「トラステッド・グループ」に伝搬します。

g. 「**SSL 認証レベル**」が「**クライアントおよびサーバー**」に設定されているかを確認して、「**更新**」を選択し、この値を「トラステッド・グループ」に伝搬します。

注: これらの値を設定していない場合は、『ステップ 6: クライアント認証用にセントラル・システムを構成する』を完了してください。

h. 「**OK**」をクリックします。「**比較および更新**」で処理が完了するまで待機してから、次のステップに進んでください。

ステップ 8: 妥当性検査リストをエンドポイント・システムにコピーする:

| このタスクは、ご使用のセントラル・システムがi5/OS V5R3 以上であることを前提しています。i5/OS
| V5R3 よりも前のシステムでは、QYPSVLDL.VLDL は QMGTC2.LIB ではなく、QUSRSYS.LIB にありま
| す。したがって、ご使用のシステムが V5R3 よりも前の場合、妥当性検査リストをそのシステムに送信し
| て、QMGTC2.LIB ではなく QUSRSYS.LIB にセットする必要があります。V5R3 以上のシステムの場合、
| 以下のステップを続行してください。

1. System i ナビゲーターで、「**マネージメント・セントラル**」 → 「**定義**」の順に展開します。
2. 「**パッケージ**」を右クリックし、「**新規定義**」を選択します。
3. 「**新規定義**」ウィンドウで、以下のものについての作業を行います。
   a. **名前:** 定義名を入力する。
   b. **ソース・システム:** セントラル・システム名を選択する。
   c. **選択されているファイルとフォルダー:** フィールド内をクリックし、`/QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL` と入力する。
4. 「**オプション**」タブをクリックし、「**既存のファイルを送信中のファイルで置き換える**」を選択します。
5. 「**拡張**」をクリックします。
6. 「**拡張オプション**」ウィンドウで、「**はい**」を指定して、復元時にオブジェクトの違いが許されるようにし、「**ターゲット・リリース**」をエンドポイントの最初のリリースに変更します。
7. 「**OK**」をクリックして、定義のリストを最新表示し、新規のパッケージを表示します。
8. 新規パッケージを右クリックし、「**送信**」を選択します。
9. 「**送信**」ダイアログ・ボックスで、「**使用可能なシステムおよびグループ**」リストから、「**システム・グループ**」->「**トラステッド・グループ**」を展開します。このグループは、 11 ページの『ステップ 2: サーバー認証用にエンドポイント・システムを構成する』で定義されたものです。

   注: セントラル・システムは常にソース・システムであるため、「**送信**」タスクは、セントラル・システムでは常に失敗します。「**送信**」タスクは、すべてのエンドポイント・システムで正常に完了するはずです。

| 10. 「**トラステッド・グループ**」に、i5/OS V5R3 よりも前のシステムがある場合、手動でそれらのシステ
| ムに進み、`QYPSVLDL.VLDL` オブジェクトを `QMGTC2.LIB` から `QUSRSYS.LIB` に移動します。
| `QUSRSYS.LIB` にすでに `QYPSVLDL.VLDL` のバージョンがある場合、それを削除し、`QMGTC2.LIB` の新規の
| バージョンと置き換えます。

ステップ 9: セントラル・システム上のマネージメント・セントラル・システムを再始動する:

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. セントラル・システムを展開します。
3. 「**ネットワーク**」 → 「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。

4. 「**マネージメント・セントラル**」を右クリックし、「**停止**」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
5. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。

ステップ 10: すべてのエンドポイント・システム上のマネージメント・セントラル・システムを再始動する:

注: それぞれのエンドポイント・システムについて、この手順を繰り返します。

1. System i ナビゲーターで、「**ユーザー接続**」を展開します。
2. 再始動するエンドポイント・システムを展開します。
3. 「**ネットワーク**」 → 「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
4. 「**マネージメント・セントラル**」を右クリックし、「**停止**」を選択します。
5. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。

SSL 概念

SSL 概念は補足情報であり、Secure Sockets Layer (SSL) プロトコルを構成する基本的な構築ブロックについて説明します。

SSL プロトコルを使用することによって、クライアントとサーバー・アプリケーション間でセキュアな接続を確立して、通信セッションの一方のエンドポイントまたは両方のエンドポイントを認証できるようになります。SSL は、クライアントとサーバー・アプリケーション間でやり取りするデータのプライバシーと保全性も維持します。

SSL の機能

SSL は、実際は 2 つのプロトコルからなっています。つまり、レコード・プロトコルとハンドシェーク・プロトコルです。レコード・プロトコルは、SSL セッションの 2 つのエンドポイント間のデータの流れを制御します。

ハンドシェーク・プロトコルは、SSL セッションの一方のエンドポイントまたは両方のエンドポイントを認証し、その SSL セッション用データの暗号化や暗号化解除に使用する鍵のセットを生成する固有な対称鍵を 1 つ設定します。SSL は、非対称暗号、ディジタル証明書、および SSL ハンドシェーク・フローを使用して、SSL セッションの一方のエンドポイントまたは両方のエンドポイントを認証します。通常 SSL はサーバーを認証しますが、オプションでクライアントを認証します。認証局によって発行されるディジタル証明書は、各エンドポイントに割り当てることも、または接続の各エンドポイントで SSL を使用するアプリケーションに割り当てることもできます。

ディジタル証明書は、公開鍵と、トラステッド認証局 (CA) がディジタル署名した識別情報からなっています。各公開鍵には、秘密鍵が 1 つずつ関連付けられています。秘密鍵は、証明書と一緒に、またはその一部として保管されることはありません。サーバー認証の場合もクライアント認証の場合も、認証されるエンドポイントは、ディジタル証明書に含まれている公開鍵に関連付けられた秘密鍵にアクセスできることを証明しなければなりません。

SSL ハンドシェークは、公開鍵と秘密鍵を使用する暗号操作のために、パフォーマンス集約型の操作になってしまいます。2 つのエンドポイント間で最初に SSL セッションが確立されたときに、これらの 2 つのエンドポイントとアプリケーションに関する SSL セッション情報をセキュアなメモリーにキャッシュすることで、後続の SSL セッションを迅速に使用可能にすることができます。SSL セッションが再開される

と、2 つのエンドポイントはハンドシェーク・フローを簡略化して、それぞれのエンドポイントが固有の情報に対するアクセス権を持っていることを、公開鍵や秘密鍵を使用することなく認証します。両方のエンドポイントがこの固有の情報にアクセスできることを証明できた場合は、次に、新しい対称鍵が設定され、SSL セッションが「再開」されます。TLS バージョン 1.0 と SSL バージョン 3.0 のセッションでは、キャッシュに入れられた情報が、24 時間を超えてセキュア・メモリーに残っていることはありません。OS/400 V5R2 以降のリリースまたは i5/OS の場合は、暗号化ハードウェアを使用してメイン CPU に対する SSL ハンドシェークのパフォーマンスの影響を最小限にすることができます。

関連情報

ディジタル証明書の概念

暗号化ハードウェア

サポートされている SSL および Transport Layer Security プロトコル

このトピックでは、i5/OS インプリメンテーションがサポートする Secure Sockets Layer (SSL) および Transport Layer Security (TLS) プロトコルのバージョンについて説明しています。

いくつかのバージョンの SSL プロトコルが定義されています。最新バージョンである Transport Layer Security (TLS) プロトコルは、SSL 3.0 に基づいており、Internet Engineering Task Force (IETF) が作成したものです。i5/OS インプリメンテーションは、以下のバージョンの SSL プロトコルおよび TLS プロトコルをサポートします。

- TLS バージョン 1.0
- TLS バージョン 1.0 (SSL バージョン 3.0 との互換性を持つもの)

注:

1. TLS バージョン 1.0 (SSL バージョン 3.0 との互換性を持つもの) では、まず、可能な場合は TLS が折衝され、この折衝が可能でない場合には次に、SSL バージョン 3.0 が折衝されます。SSL バージョン 3.0 が折衝できないと、SSL ハンドシェークは失敗します。
2. System i は、SSL バージョン 3.0 と SSL バージョン 2.0 間の互換性を持つ TLS バージョン 1.0 もサポートします。これを指定するには、プロトコル値を「**すべて**」にします。つまり、可能な場合は TLS が折衝され、この折衝が可能でない場合には次に SSL バージョン 3.0 が折衝されます。SSL バージョン 3.0 が折衝できない場合は、SSL バージョン 2.0 が折衝されます。SSL バージョン 2.0 が折衝できないと、SSL ハンドシェークは失敗します。SSL バージョン 2.0 は使用不可に設定されて出荷されていますが、システム値 QSSLPCL を変更することで再度使用可能にできます。QSSLPCL システム値は、任意のプロトコルを使用不可または使用可能に設定するために使用できます。

- SSL バージョン 3.0
- SSL バージョン 2.0
- SSL バージョン 3.0 (SSL バージョン 2.0 との互換性を持つもの)

SSL バージョン 3.0 と SSL バージョン 2.0

SSL バージョン 3.0 は、SSL バージョン 2.0 とは大きく異なるプロトコルです。この両者の大きな違いは、以下のとおりです。

- SSL バージョン 3.0 のハンドシェーク・プロトコル・フローは、SSL バージョン 2.0 のフローと異なっています。
- SSL バージョン 3.0 は、RSA Data Security, Incorporated. 社の BSAFE 3.0 インプリメンテーションを使用しています。BSAFE 3.0 には、いくつかのタイミングのアタックの修正と SHA-1 ハッシュ・アル

ゴリズムが組み込まれています。SHA-1 ハッシュ・アルゴリズムは、MD5 ハッシュ・アルゴリズムよりもセキュアであると考えられます。SHA-1 によって、MD5 の代わりに SHA-1 を使用する追加の暗号スイートを SSL バージョン 3.0 がサポートできるようになります。

- SSL バージョン 3.0 プロトコルは、SSL ハンドシェーク処理中に man-in-the-middle (MITM) (中継) アタックの発生を抑えます。SSL バージョン 2.0 では、まれに MITM アタックにより暗号化仕様が弱められる可能性がありました。暗号化が弱まると、無許可の人に SSL セッション鍵を壊す機会を与える可能性があります。

TLS バージョン 1.0 と SSL バージョン 3.0 の対比

SSL バージョン 3.0 を基にした Transport Layer Security (TLS) バージョン 1.0 は、最新の業界標準 SSL プロトコルです。その仕様は、Internet Engineering Task Force (IETF) により RFC 2246、『*The TLS Protocol*』に定義されています。

TLS の主要な目標は、SSL をよりセキュアにし、このプロトコルの仕様をより正確かつ完全にすることです。TLS は、SSL バージョン 3.0 に対して以下のような拡張を行っています。

- よりセキュアな MAC アルゴリズム
- より細分化されたアラート
- 「グレー・エリア」仕様のより明確な定義

SSL が使用可能になっている System i アプリケーションは、SSL バージョン 3.0 または SSL バージョン 2.0 のみを使用するよう別途要求しない限り、自動的に TLS によってサポートされます。

TLS では、以下のようなセキュリティーの改善を行っています。

- **Key-Hashing for Message Authentication** TLS は、Key-Hashing for Message Authentication Code (HMAC (メッセージ確認コード用キー・ハッシュ)) を使用します。この機能は、レコードがインターネットのようなオープン・ネットワークを通過しているときに変更されないようにします。SSL バージョン 3.0 も鍵付きメッセージ認証を提供しますが、SSL バージョン 3.0 が使用する MAC (Message Authentication Code (メッセージ確認コード)) よりも、HMAC の方がよりセキュアです。
- **Enhanced Pseudorandom Function (PRF)** PRF は、鍵データを生成します。TLS では、PRF は HMAC で定義されます。PRF は、そのセキュリティーを保証する 2 つのハッシュ・アルゴリズムを使用します。いずれかのアルゴリズムが露出した場合は、2 番目のアルゴリズムが露出しない限り、そのデータがセキュアな状態を持続します。
- **終了メッセージ検査の改善** TLS バージョン 1.0 と SSL バージョン 3.0 はどちらも、交換されたメッセージが変更されなかったことを認証する終了メッセージを両方のエンドポイントに提供します。ただし、TLS の場合は、この終了メッセージは PRF 値および HMAC 値に基づいて作成されるので、SSL バージョン 3.0 よりもセキュアです。
- **一貫性のある証明書処理** SSL バージョン 3.0 と異なり、TLS は、TLS インプリメンテーション間で交換する必要のある証明書のタイプを指定します。
- **特定のアラート・メッセージ** TLS は、より具体的な内容の追加のアラートを提供して、いずれかのセッション・エンドポイントで検出された問題を指摘します。TLS は、特定のアラートをいつ送信するかについても文書化します。

関連情報


TLS プロトコル (TLS Protocol)

システム SSL

システム SSL は、SSL/TLS プロトコルを使用して TCP/IP 通信を保護するために、i5/OS Licensed Internal Code (LIC) で提供される一般的なサービスのセットです。システム SSL はオペレーティング・システム、および追加のパフォーマンスおよびセキュリティーを特別に供給するソケット・コードと密結合しています。

アプリケーション開発者は、以下のプログラミング・インターフェースおよび JSSE インプリメンテーションからシステム SSL にアクセスすることができます。

- Global Secure Toolkit (GSKit) API
  - これらの ILE C API は他の ILE 言語からアクセス可能です
- 統合 i5/OS SSL_API
  - これらの ILE C API は他の ILE 言語からアクセス可能です
  - この API セットの使用は推奨されていません。推奨されている C インターフェースは GSKit です。
- 統合 i5/OS JSSE インプリメンテーション
  - JDK 1.4 のデフォルト JSSE インプリメンテーション
  - i5/OS JSSE インプリメンテーションは、JDK 1.5 および JDK 1.6 で使用可能ですが、デフォルトのインプリメンテーションではありません。

IBM、IBM ビジネス・パートナー、独立系ソフトウェア・ベンダー (ISV)、または上記にリストされた 3 つのシステム SSL インターフェースの 1 つを使用するお客様によって作成される SSL アプリケーションは、システム SSL を使用します。例えば、FTP および Telnet は、システム SSL を使用する IBM アプリケーションです。すべての SSL がシステム SSL 使用の System i 上でのアプリケーションの実行を可能にしたわけではありません。

システム SSL プロパティー

システム SSL プロパティーによって、デフォルトの動作が要求されるときのデフォルトでサポートされる SSL 機能、およびデフォルトで使用される SSL 機能を決定します。

各アプリケーションは、デフォルトの機能を使用するか、またはアプリケーションでなされたコーディングの選択によってオーバーライドするかを決定します。多くのアプリケーションでは、コード変更を実装することなく新規のシステム SSL の機能を利用できるシステム SSL のデフォルトを使用します。

i5/OS V6R1 以降では、システム SSL はシステム管理者に、お使いのシステム上でシステム SSL によってサポートされる SSL プロトコルおよび暗号スイートを正確に制御するメカニズムを提供します。システム SSL には、それを使用する前に理解しておく必要がある 2 つの主な概念があります。最初の概念はサポート値です。サポート値はシステム SSL が機能としてサポートしているものです。システムはその全体の機能が使用可能に設定されたサブセットで出荷されます。2 番目の概念はデフォルト値です。デフォルト値はサポート値のサブセットでなければなりません。デフォルト値は、アプリケーションがデフォルトのサポートを要求するときに使用されます。システム SSL のデフォルトを使用する IBM アプリケーションが、低レベルのセキュリティーをサポートするように強制されるのを防ぐため、管理者のデフォルト値に対する制御は制限されています。機能として、システムの出荷時のデフォルト以外にデフォルトのサポートに追加することはできません。管理者は提供されたフィーチャーのサポートを完全に使用不可に設定することによって、デフォルトでサポートされているものをさらに制限することができます。

SSL プロトコル

システム SSL には、以下のプロトコルをサポートするインフラストラクチャーがあります。

- Secure Sockets Layer バージョン 2.0 プロトコル (SSLv2)
- Secure Sockets Layer バージョン 3.0 プロトコル (SSLv3)
- Transport Layer Security バージョン 1.0 プロトコル (TLSv1)

出荷時の SSL サポート・プロトコル

システム SSL は以下のサポート・プロトコルで出荷されます。

- Secure Sockets Layer バージョン 3.0 プロトコル (SSLv3)
- Transport Layer Security バージョン 1.0 プロトコル (TLSv1)

注: Secure Sockets Layer バージョン 2.0 プロトコル (SSLv2) はシステム SSL では使用不可に設定されて出荷されます。SSLv2 はシステム値 QSSLPCL を変更することで再度使用可能にできます。QSSLPCL システム値は、任意のプロトコルを使用不可または使用可能に設定するために使用できます。

出荷時の SSL デフォルト・プロトコル

以下のデフォルト・プロトコルは、アプリケーションによって要求されたときシステム SSL によって使用されます。

- Secure Sockets Layer バージョン 3.0 プロトコル (SSLv3)
- Transport Layer Security バージョン 1.0 プロトコル (TLSv1)

注: SSLv2 が管理者によってサポート・プロトコル・リストに戻された場合、デフォルト・プロトコルには追加されません。サポート・プロトコル・リストからデフォルト・プロトコルを除去した場合、デフォルト・プロトコル・リストからも除去されます。

SSL 暗号スイート

システム SSL には、13 の暗号スイートをサポートするインフラストラクチャーがあります。各プログラミング・インターフェースには、異なる方法で暗号スイートが指定されます。システム値の命名規則は以下に表示されています。

以下の暗号スイートはシステム SSL によるサポートが可能です。

- *RSA_NULL_MD5
- *RSA_NULL_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_RC4_128_MD5
- *RSA_RC4_128_SHA
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_DES_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_AES_256_CBC_SHA
- *RSA_RC2_CBC_128_MD5
- *RSA_DES_CBC_MD5

| • *RSA_3DES_EDE_CBC_MD5

出荷時の SSL サポート暗号化仕様リスト

| 暗号化仕様リストは暗号スイートのリストを含みます。システム SSL は 10 の暗号スイートがサポートされた状態で出荷されます。管理者はシステム値 QSSLCSL および QSSLCSLCTL を使用して、システム SSL によってサポートされる暗号を制御できます。暗号スイートは、必要とする SSL プロトコルがサポートされていなければ、サポートされません。

| 以下の暗号スイートはシステム SSL によってサポートされた状態で出荷されています。

| • *RSA_AES_256_CBC_SHA
| • *RSA_AES_128_CBC_SHA
| • *RSA_RC4_128_SHA
| • *RSA_RC4_128_MD5
| • *RSA_3DES_EDE_CBC_SHA
| • *RSA_DES_CBC_SHA
| • *RSA_EXPORT_RC4_40_MD5
| • *RSA_EXPORT_RC2_CBC_40_MD5
| • *RSA_NULL_SHA
| • *RSA_NULL_MD5

| サポートされている暗号化仕様リストは、システムよってサポートされる SSL プロトコル、およびシステム値 QSSLCSL になされた変更によって影響を受けます。QSSLCSL の値を表示して、お使いのシステムの暗号化仕様リストを確認することができます。

出荷時の SSL デフォルト暗号化仕様リスト

| 以下にはデフォルト暗号化仕様リストの出荷時の順序が表示されています。

| • *RSA_AES_128_CBC_SHA
| • *RSA_RC4_128_SHA
| • *RSA_RC4_128_MD5
| • *RSA_AES_256_CBC_SHA
| • *RSA_3DES_EDE_CBC_SHA

| 出荷時のデフォルト暗号化仕様リストは、QSSLCSL システム値を変更することによって削減および再配列することができます。暗号スイートをリストに追加することはできません。

| **関連情報**

| SSL システム値: QSSLPCL

| SSL システム値: QSSLCSLCTL

| SSL システム値: QSSLCSL

サーバー認証

サーバー認証の場合、クライアントは、サーバー証明書が有効であり、このクライアントが信頼する認証局 (CA) によってそれが署名されていることを確認します。

SSL は、非対称暗号およびハンドシェーク・プロトコル・フローを使用して、この固有な SSL セッションだけに使用する対称鍵を生成します。対称鍵は、SSL セッションを流れるデータの暗号化と暗号化解除に使用する鍵のセットを生成するために使用します。次に、SSL ハンドシェークが完了すると、通信リンクの一方のエンドポイントまたは両方のエンドポイントが認証されます。そして、データの暗号化と暗号化解除に使用する固有な鍵が生成されます。ハンドシェークが完了すると、暗号化されたアプリケーション層データがその SSL セッションを流れます。

クライアント認証

多くのアプリケーションは、クライアント認証を使用可能にするオプションを備えています。クライアント認証の場合、サーバーは、クライアント証明書が有効で、かつサーバーが信頼する認証局によって署名されていることを確認します。

以下の System i アプリケーションは、クライアント認証をサポートします。

- IBM HTTP Server for i5/OS
- FTP サーバー
- Telnet サーバー
- マネージメント・セントラル・エンドポイント・システム
- IBM Tivoli® Directory Server for i5/OS

関連情報

ディレクトリー・サーバーでの Secure Sockets Layer (SSL) および Transport Layer Security (TLS)

Transport Layer Security または Secure Sockets Layer を使用した FTP クライアントの保護

SSL を使用した Telnet の保護

HTTP Server の管理 (ADMIN) サーバー用の SSL のセットアップ

SSL の前提条件

このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

SSL を使用する前に、以下のオプションがインストールされていることを確認します。

- IBM デジタル証明書マネージャー (DCM) (5761-SS1 オプション 34)

  注: IBM Java™ Secure Socket Extension (JSSE) および OpenSSL は DCM を必要としません。
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
- IBM HTTP Server for i5/OS (5761-DG1)
- HTTP サーバーを使用して DCM を使用としている場合には、IBM Developer Kit for Java (5761–JV1) をインストール済みであるかを確認します。そうでない場合、HTTP 管理サーバーは開始しません。
- 暗号化ハードウェアをインストールし、SSL で使用するように構成して、SSL ハンドシェーク処理の速度を高めることもできます。暗号化ハードウェアをインストールする場合は、暗号サービス・プロバイダーもインストールする必要があります。

注: 5722 は V6R1 より前の i5/OS オプションおよび製品の製品コードです。

関連概念

23 ページの『SSL のトラブルシューティング』
このきわめて基本的なトラブルシューティング情報は、SSL の使用中に System i プラットフォームが直面する可能性のある一連の問題を軽減することを目的としています。

関連情報

暗号化ハードウェア

公開証明書と秘密証明書

DCM の構成

SSL によるアプリケーション・セキュリティー

以下の System i プラットフォームで SSL を使用してセキュアにできるアプリケーションのリストを参照して検討してください。

以下の System i アプリケーションは、SSL を使用することでセキュアにすることができます。

- エンタープライズ識別マッピング (EIM)
- FTP サーバー
- IBM HTTP Server for i5/OS
- System i Access for Windows
- IBM Tivoli Directory Server for i5/OS
- 分散リレーショナル・データベース・アーキテクチャー (DRDA®) および分散データ管理 (DDM) サーバー
- マネージメント・セントラル
- Telnet サーバー
- Websphere Application Server — Express
- System i Access for Windows の API (Application Programming Interface) セットに記述されているアプリケーション。
- System i プラットフォームでサポートされるセキュア・ソケットのアプリケーション・プログラミング・インターフェース (API) を使用して開発されるアプリケーション。サポートされる API は、グローバル・セキュア・ツールキット (GSKit) および SSL_System i の API です。

関連概念

6 ページの『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』
このシナリオは、SSL を使用して、System i モデルとのすべての接続を保護する方法を説明しています。このモデルは、System i ナビゲーターのマネージメント・セントラル・システムを使用して、セントラル・システムとして機能しています。

関連情報

エンタープライズ識別マッピング

SSL を使用した FTP サーバーの保護

HTTP サーバー

Secure Sockets Layer の管理 (iSeries Access for Windows のトピック)

Telnet シナリオ: SSL で保護された Telnet

Secure Sockets API

SSL のトラブルシューティング

このきわめて基本的なトラブルシューティング情報は、SSL の使用中に System i プラットフォームが直面する可能性のある一連の問題を軽減することを目的としています。

ただし、トラブルシューティングに関する包括的な情報源ではなく、共通の問題解決に役立つ手引きである点にご注意ください。

以下の内容に当てはまることを確認します。

- System i プラットフォーム上での SSL の前提条件を満たしている。
- 使用している認証局および証明書は有効であり、有効期限が切れていない。

前述の内容がご使用のシステムに当てはまることを確認しても、依然として SSL 関連の問題がある場合は、オプションで以下を試行してください。

- エラーに関する詳細については、サーバーのジョブ・ログにある SSL のエラー・コードをエラー・テーブルで相互参照することができます。たとえば、このテーブルではサーバーのジョブ・ログに示された -93 は、定数 SSL_ERROR_SSL_NOT_AVAILABLE にマップされます。
  - 負の戻りコード (コード番号の前にあるダッシュで表される) は、SSL_ API を使用していることを表します。
  - 正の戻りコードは、GSKit API を使用していることを表します。プログラマーは、プログラム内で gsk_strerror() API または SSL_Strerror() API をコーディングして、エラーの戻りコードの要旨を取得することができます。一部のアプリケーションはこの API を使用し、メッセージをこのセンテンスを含むジョブ・ログへ出力します。

  詳細な情報が必要な場合は、テーブルに提供されているメッセージ ID を System i モデル上に表示して、このエラーについての考えられる原因および回復方法を示すことができます。これらのエラー・コードに関するその他の説明は、エラーを戻した個々のセキュア・ソケット API 内で見つかる場合もあります。
- 以下の 2 つのヘッダー・ファイルには、テーブルに存在するものと同じシステム SSL の戻りコードの定数名が存在しますが、相互参照のためのメッセージ ID は存在しません。
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.QSOSSL

  システム SSL の戻りコードの名前はこれらの 2 つのファイル内では変化しませんが、それぞれの戻りコードには複数の固有のエラーが関連する場合があります。

関連概念

21 ページの『SSL の前提条件』
このトピックでは、System i プラットフォームでシステム SSL の前提条件、および役に立つヒントを示しています。

関連情報

セキュア・ソケット API のエラー・コード・メッセージ

SSL の関連情報

この情報を使用して、Secure Sockets Layer (SSL) の使用に関連する他のリソースおよび情報を学習します。

Web サイト

- RFC 2246: TLS プロトコル・バージョン 1.0 (The TLS Protocol Version 1.0) (ftp://ftp.isi.edu/in-notes/rfc2246.txt)

  TLS プロトコルについて詳細に説明しています。

- RFC2818: TLS を介した HTTP (HTTP Over TLS) (ftp://ftp.isi.edu/in-notes/rfc2818.txt)

  TLS を使用してインターネットで HTTP 接続をセキュアにする方法について説明しています。

その他の情報

- SSL および Java セキュア・ソケット拡張機能
- IBM Toolbox for Java

付録. 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。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

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、IBM 機械コードのご使用条件、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。

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_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

DRDA
i5/OS
IBM
OS/400
System i
Tivoli

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

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。

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