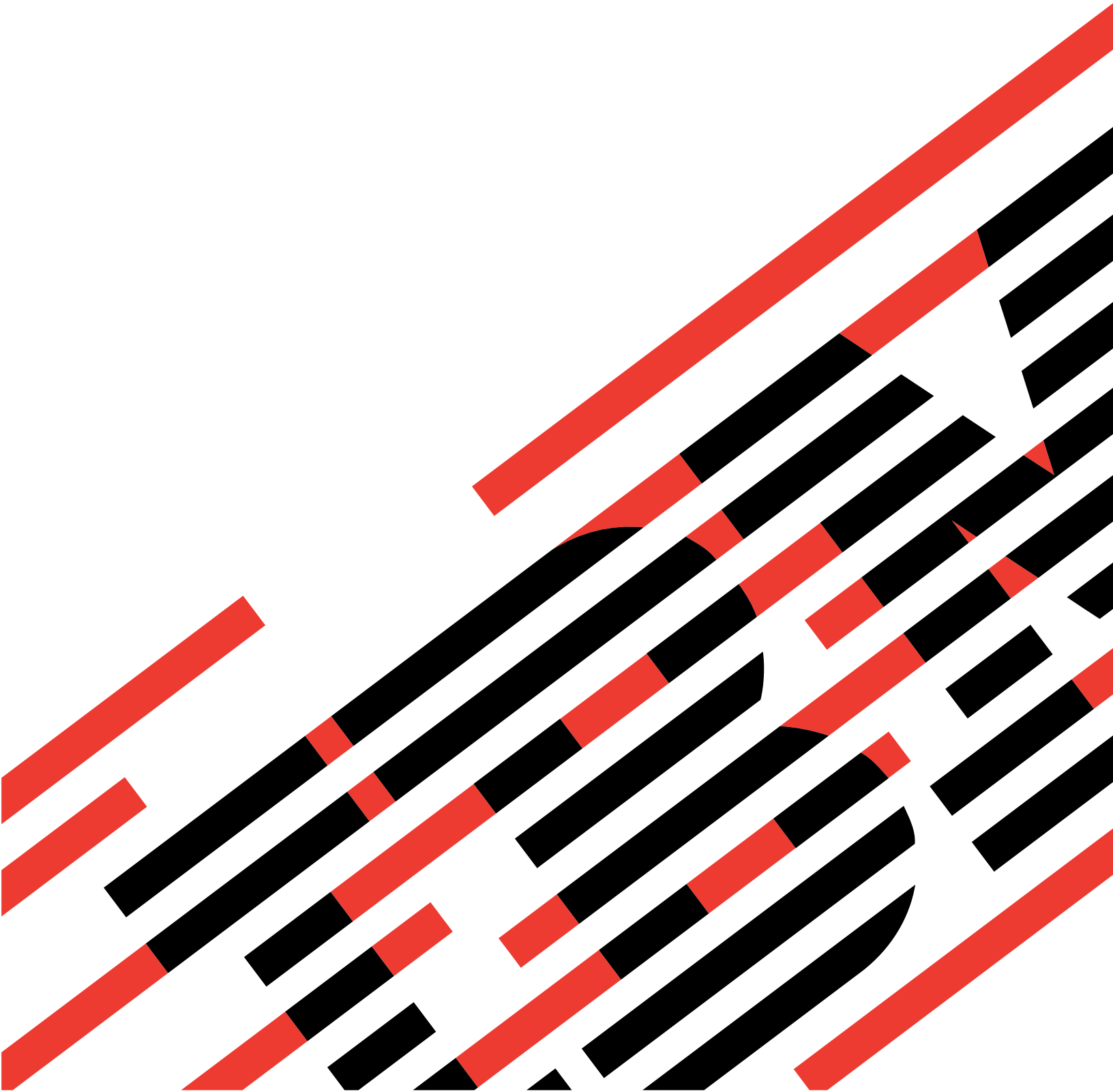
IBM

eserver

iSeries

Secure Sockets Layer (SSL)



IBM

@server

iSeries

Secure Sockets Layer (SSL)

目次

第 1 部 Secure Sockets Layer (SSL)

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。 SSL および iSeries™ サーバー・アプリケーションに関する詳細は、以下のリンクを参照してください。

- **V5R2 の新機能**
  SSL に関する新機能または利用できる新しい情報について説明します。
- **SSL シナリオ**
  SSL の情報に新しく追加されたものであり、SSL で実現可能な例を挙げることで、iSeries サーバーでの SSL の実行に関する理解を深める目的があります。
- **SSL の概念**
  Secure Sockets Layer プロトコルの基礎について説明する補助的情報が記載されています。
- **SSL を使用可能にする計画**
  iSeries サーバーで SSL を使用可能にするための前提条件、および役に立つヒントが記載されています。
- **SSL によるアプリケーションの保護**
  iSeries サーバーで 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が記載されています。
- **SSL のトラブルシューティング**
  iSeries サーバーで行う SSL のトラブルシューティングの処置を開始する方法の基本的な手引きです。
- **関連情報**
  追加の情報源へのリンクが記載されてます。

第 1 章 V5R2 の新機能

V5R2M0 では、2058 PCI 暗号化アクセラレーターがオプションとして使用できます。この暗号化ハードウェアのオプションは、iSeries サーバーでの SSL のパフォーマンスを改善するように設計されています。このオプションに関する詳細は、『暗号化ハードウェア』を参照してください。

新規のグローバル・セキュア・ツールキット (GSKit) アプリケーション・プログラミング・インターフェース (API)

新規の OS/400® グローバル・セキュア・ツールキット (GSKit) API である `gsk_secure_soc_startInit()` が使用可能になりました。詳細は、『グローバル・セキュア・ツールキット (GSKit)』を参照してください。

今回のリリースでの新規の機能や変更された機能に関する詳細は、「iSeries プログラム資料説明書」  を参照してください。

新規箇所または変更箇所を見つける方法

技術に関する変更箇所を見つけるには、以下の情報を使用します。

- » 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点を示します。

第 2 章 トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。PDF 版をダウンロードし、表示するには、『SSL によるアプリケーションの保護』(約 425 KB、36 ページ) を選択します。

その他の情報

このトピックについての関連情報も表示したり、印刷することができます。

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. ブラウザーで PDF を右クリックする。
2. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) 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 Acrobat 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 Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、ダウンロードできます。

第 3 章 SSL シナリオ

以下のシナリオは、iSeries サーバーで SSL を使用可能にすることの利点を、最大限に活用することを目的としています。

- シナリオ: SSL によるマネージメント・セントラルの保護
- シナリオ: SSL による FTP の保護
- シナリオ: SSL による Telnet の保護
- シナリオ: iSeries での SSL のパフォーマンスの改善
- シナリオ: 暗号化ハードウェアによる秘密鍵の保護

シナリオ: SSL によるマネージメント・セントラルの保護

状況

ある企業が最近、iSeries サーバーをリモート・ロケーション (エンドポイント・システム) に置く広域ネットワークをセットアップしました。これらのサーバーは、本社にある 1 台の iSeries サーバーによって中央管理されます。この企業のセキュリティーの専門家である Tom は、iSeries ナビゲーター・クライアントのマネージメント・セントラル・テクノロジーを使用して、本社の iSeries サーバー (セントラル・システム) に接続しています。Tom は、セントラル・システムとすべてのエンドポイント・サーバーの間の接続を SSL を使用してセキュアにすることを考えています。

詳細

iSeries ナビゲーターのマネージメント・セントラルのテクノロジーを使用すると、Tom は単一のセントラル・システムを通じて複数のシステムを管理することができます。マネージメント・セントラルで SSL を使用することにより、Tom はこれらのシステムを**セキュアに**管理することができます。マネージメント・セントラルで SSL を使用するには、Tom は iSeries Access for Windows® およびマネージメント・セントラルを実行する PC で iSeries ナビゲーターをセキュアにする必要があります。

マネージメント・セントラル環境では、Tom には以下の 2 つの認証レベルが必要になります。

サーバー認証
: エンドポイント・システム・サーバー証明書の認証を行います。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、セントラル・システム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、識別を証明しなければなりません。すべてのエンドポイント・システムには、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。

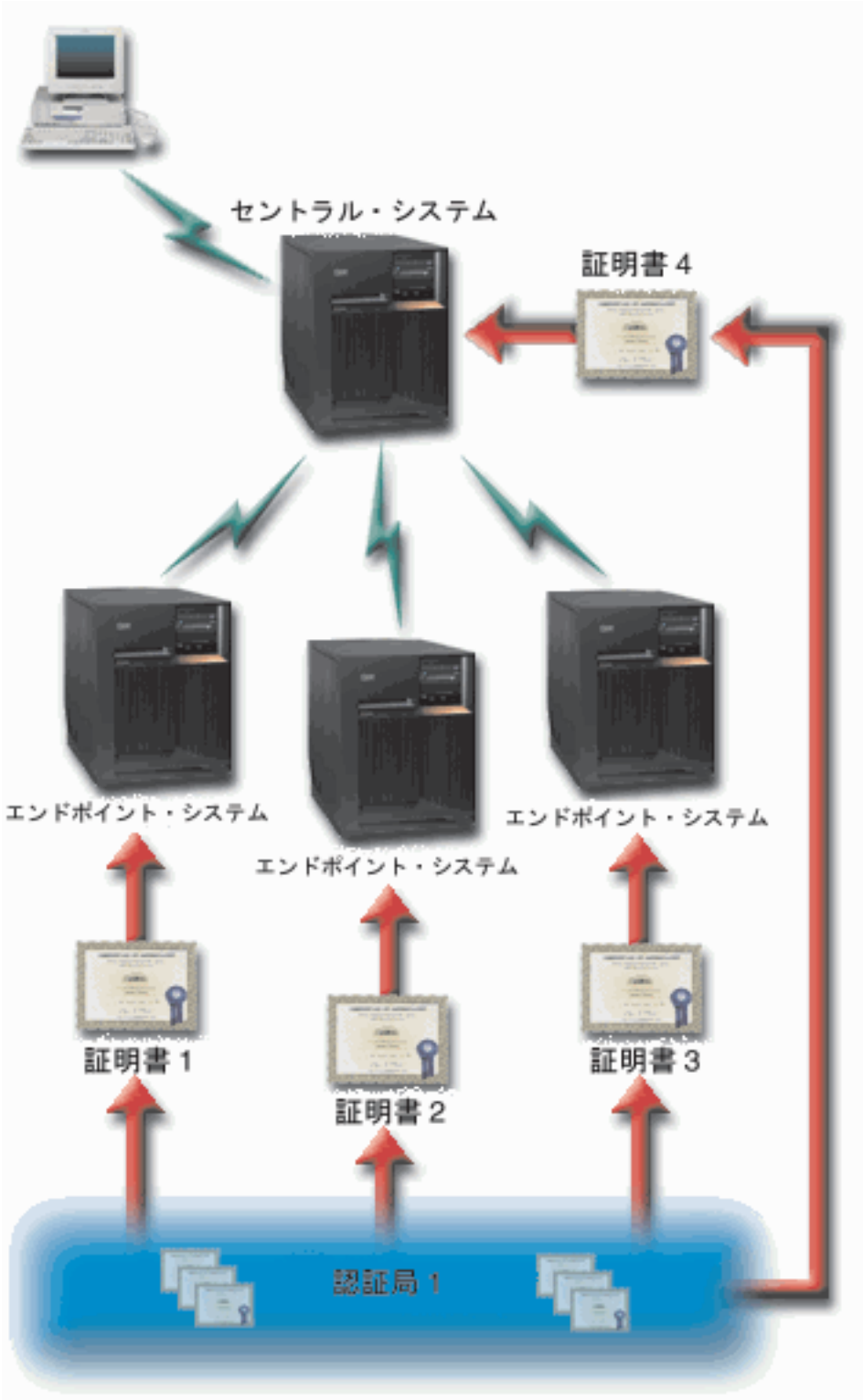
クライアントおよびサーバー認証

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・レベルであると考えられています。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。

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。ほとんどの場合、サーバー認証は SSL セッションを使用可能にするときに行われるからです。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、SSL が使用可能になっている場合は、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。



前提条件および前提事項

Tom は、SSL が使用可能になっているマネージメント・セントラルが正常に動作するように、以下の管理タスクおよび構成タスク (SSL によってセキュアになっているマネージメント・セントラルの広域ネットワーク (WAN) の図を参照) を行う必要があります。

1. マネージメント・セントラルを使用する iSeries サーバーが、SSL の前提条件 (SSL の前提条件を参照) を満たす。
2. セントラル・システムおよびすべてのエンドポイントの iSeries サーバーが OS/400 の V5R2 を実行する。OS/400 が V5R1 である場合、以下の OS/400 (5722-SS1) 用のフィックス (PTF) をインストールします。
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. iSeries ナビゲーター PC クライアントが iSeries Access for Windows の V5R2 を実行する。クライアントが V5R1 である場合、サービス・パック PTF SI01907 (以降) を V5R1 の iSeries Access for Windows (5722-XE1) にインストールします。詳細は、V5R1 Information Center の『マネージメント・セントラルの保護』ページを参照してください。
4. iSeries サーバーの認証局 (CA) を取得する。
5. SSL が使用可能になっているマネージメント・セントラル・サーバーが管理する iSeries サーバーごとに、証明書を作成し、CA に署名してもらう。
6. CA および証明書をそれぞれの iSeries サーバーに送信し、それらを鍵データベースにインポートする。
7. マネージメント・セントラルのアプリケーション ID および iSeries ナビゲーターが使用するすべてのエンドポイント・サーバーのアプリケーション ID が記載されている証明書を割り当てる。
   a. 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。Tom 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 (証明書システムのセットアップの詳細は、『ディジタル証明書マネージャーの使用』を参照)。
   b. 「**証明書ストアの選択 (Select a Certificate Store)**」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 (Certificate Store password)**」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 (Manage Applications)**」を展開します。
   e. 「**証明書割り当ての更新 (Update certificate assignment)**」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 (Management Central Server)**」を選択し、「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。これによって、iSeries Access for Windows クライアントに対してサーバーの識別の確立に使用する証明書を、マネージメント・セントラル・サーバーに割り当てます。

h. 「**新しい証明書の割り当て (Assign New Certificate)**」をクリックします。DCM は、「**証明書割り当ての更新 (Update certificate assignment)**」ページを再ロードして、確認メッセージを表示します。

i. 「**終了 (Done)**」をクリックします。

j. iSeries ナビゲーターが使用するすべてのエンドポイント・サーバーについて、この手順を繰り返します。

8. iSeries ナビゲーターをセットアップする。

a. iSeries ナビゲーターの SSL コンポーネントを、選択してインストールします。

b. CA を作成したシステムから CA をダウンロードします。

注: Tom が iSeries Access for Windows クライアントの鍵データベースにない CA 証明書を持つ CA からの証明書を選択した場合、SSL を使用するためにその証明書をデータベースに追加する必要があります。

構成のステップ

Tom がマネージメント・セントラルで 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、iSeries サーバー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 (続ける前に、このシナリオに関して『前提条件および前提事項』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・セントラルで SSL を使用可能にできます。

注: iSeries ナビゲーターで SSL が使用可能になった場合、Tom はマネージメント・セントラルで SSL を使用可能にするために、iSeries ナビゲーターで SSL を使用不可にする必要があります。SSL が iSeries ナビゲーターで使用可能になり、マネージメント・セントラルでは使用可能にならない場合は、iSeries ナビゲーターがマネージメント・セントラル・セントラル・システムと接続しようとしても、失敗します。

サーバー認証の場合 (必須)

1. サーバー認証用にセントラル・システムを構成する
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

クライアント認証の場合 (オプション)

注: クライアント認証の構成は、サーバー認証が構成されるまで、完了することができません。

1. クライアント認証用にセントラル・システムを構成する
2. 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

サーバー認証用にセントラル・システムを構成する

Tom 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 iSeries 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 接続が実現するのは、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。Tom がクライアント認証を行うためには、まずその前にサーバー認証をセットアップする必要があります。

1. iSeries 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) を使用する (Use Secure Sockets Layer (SSL))**」を選択します。
3. 認証レベルとして「**サーバー (Server)**」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: エンドポイント・システムのサーバー認証用の構成が完了するまで、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。
5. サーバー認証用にエンドポイント・システムを構成します。

サーバー認証用にエンドポイント・システムを構成する

Tom は、セントラル・システムでサーバー認証を行うために SSL を使用可能にした後に、すべてのエンドポイント・システムについてサーバー認証を行うために、SSL を使用可能にする必要があります。SSL とサーバー認証を使用するようにエンドポイント・システムを構成するには、以下のタスクを行います。

1. 「**マネージメント・セントラル**」ビューを展開する。
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する。**
   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。他のオプションのチェックを外します。
   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。
   e. 新規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. 「**マネージメント・セントラル**」カテゴリーを選択して以下の値を確認し、それぞれの隣にあるボックスをチェックします。
      - 「Secure Sockets Layer を使用する (Use Secure Sockets Layer)」が「**はい**」に設定されている。
      - 「SSL 認証レベル (SSL authentication level)」が「**サーバー**」に設定されている。

      これらの値は、サーバー認証用にセントラル・システムを構成する手順の間に、セントラル・システムに設定されます。
   i. 「**OK**」をクリックして、これらの値を新規のシステム・グループのエンドポイント・システムに設定します。
   j. 「**比較および更新**」が完了するのを待ってから、マネージメント・セントラル・サーバーを再始動します。これには、数分を要することがあります。
3. **セントラル・システム上のマネージメント・セントラル・サーバーを再始動する。**
   a. iSeries ナビゲーターで、「**ユーザー接続**」を展開します。
   b. 「セントラル・システム (central system)」ビューを展開します。
   c. 「**ネットワーク**」->「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
   d. 「**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、サーバーにはもう接続されていないことを示すメッセージが表示されます。

e. 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。

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・サーバーを再始動する。**
   a. 再始動するエンドポイント・システムを展開します。
   b. 「**ネットワーク**」->「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
   c. 「**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。
   d. 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。
   e. 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。
5. **iSeries 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。**
   a. iSeries ナビゲーターで、「**ユーザー接続**」を展開します。
   b. 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。
   c. 「**セキュア・ソケット (Secure Sockets)**」タブをクリックし、「**接続に Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL) for connection)**」を選択します。
   d. iSeries ナビゲーターを終了し、再始動します。

これで、Tom 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を実行することができます。

- クライアント認証用にセントラル・システムを構成する
- 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

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。

クライアント認証用にセントラル・システムを構成する

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、クライアント認証 (マネージメント・セントラルでは、認証局およびトラステッド・グループ認証と呼ばれる) により互いの証明書を認証します。

1. iSeries 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 (Security)**」タブをクリックし、「**Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL))**」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 (Client and server)**」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: すべてのエンドポイント・システムでクライアント認証およびサーバー認証に SSL を使用するように構成し終えるまで、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。
5. クライアント認証用にエンドポイント・システムを構成します。

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

1. **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する。**

   注: このタスクは、V4R5 を実行しているエンドポイントの iSeries サーバーでは正常に動作しません。

   V4R4 のレッドブック、「Management Central: A Smart Way to Manage AS/400® Systems」  を参照してください。

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。他のオプションのチェックを外します。

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。

e. 新規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. 「**マネージメント・セントラル**」カテゴリーを選択して以下の値を確認します。

- 「Secure Sockets Layer を使用する (Use Secure Sockets Layer)」が「**はい**」に設定されている。
- 「SSL 認証レベル (SSL authentication level)」が「**クライアントおよびサーバー (Client and Server)**」に設定されている。

これらの値は、クライアント認証用にセントラル・システムを構成する手順の間に、セントラル・システムに設定されます。それぞれの値の隣にある「**更新**」ボックスをチェックします。

i. 「**OK**」をクリックして、これらの値を新規のシステム・グループのエンドポイント・システムに設定します。

2. **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**

a. iSeries 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。

b. 「**パッケージ**」を右クリックし、「**新規定義 (New Definition)**」を選択します。

c. 「**新規定義 (New Definition)**」ウィンドウで、以下のものについての作業を行います。

- **名前:** 定義名を入力する。
- **ソース・システム:** セントラル・システム名を選択する。
- **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/QUSRSYS.LIB/QYPSVLDL.VLDL` と入力する。

d. 「**オプション**」タブをクリックし、「**既存のファイルを送信されるファイルに置き換える (Replace existing file with the file being sent)**」を選択します。

e. 「**拡張 (Advanced)**」をクリックします。

f. 「**拡張オプション (Advanced Options)**」ウィンドウで、「**はい**」を指定して、復元操作時にオブジェクトの違いが許されるようにします。

g. 「**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。

h. 新規パッケージを右クリックし、「**送信**」を選択します。

i. 「**送信**」ダイアログで、トラステッド・グループを追加してその他のグループを除去し、「**OK**」をクリックします。トラステッド・グループは、この手順のステップ 1 で定義したシステム・グループです。

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。

3. **セントラル・システム上のマネージメント・セントラル・サーバーを再始動する。**

a. iSeries ナビゲーターで、「**ユーザー接続**」を展開します。

b. セントラル・システムを展開します。
c. 「**ネットワーク**」->「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
d. 「**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、サーバーにはもう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。
e. 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。

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・サーバーを再始動する。**

   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。

   a. 再始動されるエンドポイント・システムを展開します。
   b. 「**ネットワーク**」->「**サーバー**」の順に展開し、「**TCP/IP**」を選択します。
   c. 「**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。
   d. 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。

第 4 章 SSL の概念

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。

以下の概念に関する情報は、SSL と iSeries サーバーとの間の関係をより良く理解するのに役立ちます。

- SSL の歴史
- SSL の機能
- サポートされている SSL および Transport Layer Security (TLS) プロトコル
- サーバー認証
- クライアント認証

SSL の歴史

Secure Sockets Layer (SSL) プロトコルは、インターネットのセキュリティーについて関心が高まったことを受けて、1994 年に Netscape が開発しました。SSL は、当初は Web ブラウザーやサーバー通信をセキュアにするために開発されましたが、その仕様は TELNET や FTP などの他のアプリケーションも SSL を使用できるように作成されました。SSL および関連するプロトコルの詳細は、『サポートされている SSL および Transport Layer Security (TLS) プロトコル』を参照してください。

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。通常は、サーバーが認証され、オプションでクライアントが認証されます。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。V5R2M0 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。

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

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。OS/400 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. SSL バージョン 3.0 および SSL バージョン 2.0 との互換性を持つ TLS バージョン 1.0 もサポートされます。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、最終的に、SSL ハンドシェークは失敗することになります。

- 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, Inc. 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 アタックが暗号化仕様を弱めてしまう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 iSeries サーバー・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あると考えられています。
- **Enhanced Pseudorandom Function (PRF)**
  PRF は、鍵データを生成するために使用します。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。

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、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 iSeries サーバーは、クライアント認証をサポートします。

- IBM HTTP Server (オリジナル)
- IBM HTTP Server (powered by Apache)
- 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
- ディレクトリー・サービス (LDAP)

第 5 章 SSL を使用可能にする計画

iSeries サーバーで SSL を使用可能にすることを計画するときには、以下のことを考慮します。

- SSL の前提条件
- ディジタル証明書のタイプおよび取得場所

SSL の前提条件

- IBM ディジタル証明書マネージャー (DCM)、OS/400 のオプション 34 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-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™ (5722-JV1) をインストール済みであるか、または HTTP 管理サーバーが始動しないことを確認します。
- IBM Cryptographic Access Provider プロダクト (5722-AC3) (128 ビット)。このプロダクトのビット・サイズは、暗号操作で使用できる対称鍵内の秘密部分の最大サイズです。対称鍵に許されるサイズは、それぞれの国の輸出入関係法律によって規制されています。ビット・サイズが大きいと、よりセキュアな接続になります。
- 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。V5R2M0 リリースでは、以下の暗号化ハードウェアのオプションを iSeries サーバーで使用することができます。
  - 2058 PCI 暗号化アクセラレーター (ハードウェア機構コード 4805)
  - 4758 暗号化コプロセッサー (ハードウェア機構コード 4801 または 4802)

  暗号化ハードウェアをインストールする場合は、オプション 35、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。

iSeries Access for Windows または IBM Toolbox for Java コンポーネントで SSL を使用する場合は、iSeries Client Encryption プロダクト (5722-CE3) (128 ビット) もインストールする必要があります。iSeries Access for Windows では、セキュアな接続を確立するためにこのプロダクトが必要です。

注: パーソナル・コミュニケーションズ・プロダクトに同梱されている PC5250 エミュレーターを使用する場合は、Client Encryption プロダクトをインストールする必要はありません。パーソナル・コミュニケーションズには独自の暗号コードが組み込まれています。

ディジタル証明書

公衆ディジタル証明書と専用ディジタル証明書の違い、およびそれらを取得するためのオプションをより良く理解するには、『公衆証明書の使用と専用証明書の発行』を参照してください。

IBM ディジタル証明書マネージャー (DCM) は、ディジタル証明書管理のための iSeries サーバーのソリューションです。DCM の使用の詳細については、Information Center のトピック『ディジタル証明書マネージャーの使用』を参照してください。

第 6 章 SSL によるアプリケーションの保護

以下の iSeries サーバー・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。

- IBM HTTP Server for iSeries (オリジナル)
- IBM HTTP Server for iSeries (powered by Apache)
- FTP サーバー
- Telnet サーバー
- 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
- ディレクトリー・サービス・サーバー (LDAP)
- エンタープライズ識別マッピング (EIM)
- iSeries Access for Windows アプリケーション (iSeries ナビゲーターを含む)
- iSeries Access for Windows 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) に作成されたアプリケーション
- Java Developer Kit で開発されたプログラム、および IBM Toolbox for Java を使用するクライアント・アプリケーション
- iSeries サーバー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_iSeries のネイティブ API です。GSKit および SSL_API の詳細は、『Secure Sockets Layer (SSL) APIs』を参照してください。

第 7 章 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 iSeries サーバー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すべての情報源ではなく、単に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。

- iSeries サーバーで SSL の前提条件を満たしている (SSL の前提条件を参照)。
- V5R1 システムで iSeries ナビゲーターのマネージメント・セントラル・テクノロジーを使用している場合、以下の PTF をシステムにインストール済みである。
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- 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、iSeries サーバーで依然として 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。セキュア・ソケットのエラー・コード・メッセージの情報にアクセスするには、『セキュア・ソケット API エラー・コード・メッセージ』ページを参照してください。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、この文を含めたメッセージをジョブ・ログへ出力します。

  詳細な情報が必要な場合は、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ために、テーブルに提供されているメッセージ ID を iSeries サーバー上に表示することができます。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.SSL`

  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。

| iSeries サーバーに関連するトラブルシューティングの詳細は、『トラブルシューティングとサービス』ページを参照してください。
| 

第 8 章 関連情報

SSL の追加情報は、以下の情報源からも見つけることができます。

IBM の情報源

- 『SSL および Java Secure Socket Extension (JSSE)』ページには、JSSE およびその使用法についての要旨が記載されています。
- 『Java Secure Socket Layer (JSSL)』ページには、JSSL およびその使用法についての要旨が記載されています。
- 『IBM Toolbox for Java』ページには、使用できる Java クラスおよびその使用法についての要旨が記載されています。

Request For Comments (RFC)

- 『RFC 2246: The TLS Protocol Version 1.0』 では、TLS プロトコルについて詳細に説明しています。
- 『RFC2818: HTTP Over TLS』 では、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。

その他の情報源

- 『The SSL Protocol Version 3.0』文書 では、SSL プロトコル、バージョン 3.0 について詳細に説明しています。

Printed in Japan

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