

IBM i World 2024

IBM i コンテンツ (2024年4月版)

5250セッションの通信を暗号化して、
在宅勤務で使ってみよう！

日本アイ・ビー・エム株式会社
テクノロジー事業本部
IBM Powerテクニカルセールス



5250セッションの通信を暗号化して、在宅勤務で使ってみよう

在宅勤務にて5250セッションを使用するときには、VPNが有効ですが、さらに安全性を強化するために、5250の通信データ自体を暗号化することをお勧めします。

5250セッションだけでなく、Navigator for iのWebブラウザの通信データも暗号化する方法をご紹介します。

目次

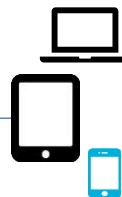
1. 通信の暗号化利用例
2. TLSによる暗号化通信のしくみ
3. 5250クライアントをTLSでセキュアにする方法
4. Navigator for iのWebブラウザをTLS通信でセキュアにする方法
5. 補足情報

1. 通信の暗号化の利用例

オフィス内でご使用いただいている、ACS (5250 エミュレータ) で、在宅で仕事をする場合は、多くの場合はインターネットVPN経由での接続です。その際に通信データを暗号化すればより安心です。IBM iは、OSの標準機能で、ブラウザーや、5250 通信セッションを、TLSで暗号化することが可能です (IBM i 7.3以上であれば、最新のTLS通信プロトコル1.3が利用できます)。



ACS(5250)
又は
ブラウザー



在宅勤務

5250



ブラウザー (下記はNavigator for i)画面



解説：

- TLSとは
Transport Layer Security (TLS) と、その前身である Secure Sockets Layer (SSL) (現在は非推奨) は、コンピューター・ネットワークを介した通信セキュリティを提供するために設計された暗号プロトコルです
- TLSによる暗号化は、Webアプリケーションをデータ漏えいやその他の攻撃から保護するのに役立ちます。現在では、TLSで保護されたHTTPSがWebサイトの標準的な慣行となっています。IBM iではWebブラウザだけでなく、ACSによる5250 通信もTLSで保護することが可能です。
- TLS プロトコルは、通信セッションの一方または両方のエンドポイントの認証を提供するクライアントアプリケーションとサーバーアプリケーション間のセキュア接続を確立します。また、TLS は、クライアントアプリケーションとサーバーアプリケーションが交換するデータのプライバシーと安全性も提供します。
- TLS v1.3 は、最新で最もセキュアな TLS プロトコルです。IBM iではv7.3からサポートされています。

IBM iのTLSについては下記のマニュアルに詳しく記述されています。

https://www.ibm.com/docs/ja/ssw_ibm_i_75/pdf/rzainpdf.pdf

2. TLSによる暗号化通信のしくみ

クライアントとサーバーの通信のやり取りの概要は下記のようになります。

- ①クライアントはサーバーから暗号化されたセッションを要求するように構成されている
- ②クライアントはサーバーに接続し、セッションの暗号化に使用できる暗号のリスト（暗号アルゴリズム）をサーバーに提供する
- ③サーバーは、どの暗号アルゴリズムを使用するか決定し、デジタル証明書+公開鍵を送付する
- ④クライアントはサーバーのデジタル証明書を検証します
- ⑤クライアントはセッションキーを生成し、デジタル証明書の公開鍵で暗号化して、サーバーへ送信する。
- ⑥クライアントとサーバーは同じ元データを使用し、共通鍵を生成します
以降、実際のデータのTLS暗号化通信が開始されます。



解説：

- TLSによる暗号化は、このような流れに基づいて実施されます。
- このフローに登場するデジタル証明書の利用により、TLSは暗号化に加え、電子証明書により通信相手の本人性を証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。
- IBM iのTLSの設定のほぼすべての作業は、このデジタル証明書の設定と管理になります。
- IBM iのデジタル証明書の概要
 - IBM iによる証明書のサポートは、標準機能である「Digital Certificate Manager(DCM)」を使用して、アプリケーションの証明書を一元的に管理することができます。DCMを使うと、任意の認証局(CA)から取得した証明書を管理することができます。
 - また、独自のローカルCAを作成、運用して、組織内のアプリケーションやユーザーに秘密証明書を発行することもできます。(当資料の3章では、このローカルCAを利用しています)
- IBM i 7.5でのデジタル証明書新規機能
 - 以前のデジタル証明書マネージャー・ユーティリティーに代わって、IBM Digital Certificate Manager for iという名前の更新されたグラフィカル・ユーザー・インターフェースが提供されます。
 - 最新のインターフェースでは、パフォーマンス、ユーザビリティ、および機能性が向上しています。

3. 5250クライアントをTLSでセキュアにする方法

この章では、ACSによる5250通信をTLSで暗号化する設定を実施していきます。実際の作業は、下記の1から5のステップになります。

ステップ 1: ポート制限を除去

ステップ 2: ローカル認証局を作成および操作する

ステップ 3: クライアント認証の証明書を要求するように Telnet サーバーを構成

ステップ 4: Telnet サーバーでの TLS の有効化および開始

ステップ 5: ACSクライアントでのTLS接続設定

各ステップでの作業詳細は、下記のマニュアルに記述がありますが、当資料では、実画面を表示して、設定方法をご紹介します。

https://www.ibm.com/docs/ja/i/7.5?topic=tls-configuration-details-securing-telnet#rzaiwscenariosldetails_removeport

解説：

- ・ デジタル証明書作業の前提として、IBM i の標準機能である、**IBM Digital Certificate Manager for i (DCM)**を利用します。

DCMの前提要件として、下記がIBM i にインストールさせている必要があります。

5770-SS1 オプション 34: デジタル Certificate Manager

5770-DG1のインストール: IBM® HTTP Server for i

5770-JV1のインストール: IBM Developer Kit for Java™

5770-JV1のインストール: オプション 17: Java SE 8 64 ビット

- ・ この資料では、IBM i 7.5の最新のGUIインターフェイスを使用する前提です。

ステップ1：ポート制限を除去

TCP/IPのポート制限を定義している場合は、TLSを使用するために、そのポート制限を除去する必要があります。Navigator for iで、ポート制限タブを開き、制限がある場合は除去します。

- ✓ TLS通信は、デフォルトでは、ポート 992 での TLS セッションおよびポート 23 での非 TLS セッションを開始する設定となっています。ACS等で5250セッションを暗号化する場合は、その他の多数のポートを公開する必要があります。それらのポート制限があれば除去します。
- ・「Navigator for iにログイン」→「TCP/IP構成」→「TCP/IPプロパティ」をクリック
下記の様に、上記のポート制限がないか、確認する。（あれば解除します）



The image shows two screenshots from the Navigator for i interface. The left screenshot displays the 'TCP/IP 構成' (TCP/IP Configuration) menu with 'TCP/IP 構成プロパティ' (TCP/IP Configuration Properties) highlighted by a red box. The right screenshot shows the 'TCP/IP 構成プロパティ' (TCP/IP Configuration Properties) window, specifically the 'ポートの制限' (Port Restrictions) tab. The table below shows no records, and the '合計行数: 0' (Total rows: 0) is displayed.

ユーザー名	開始ポート	終了ポート	プロトコル
レコードが見つかりません			
合計行数: 0			

Additional fields visible in the screenshot include:

- ユーザー名:
- 開始ポート:
- 終了ポート:
- プロトコル:
- Buttons: 追加 (Add), 除去 (Remove)

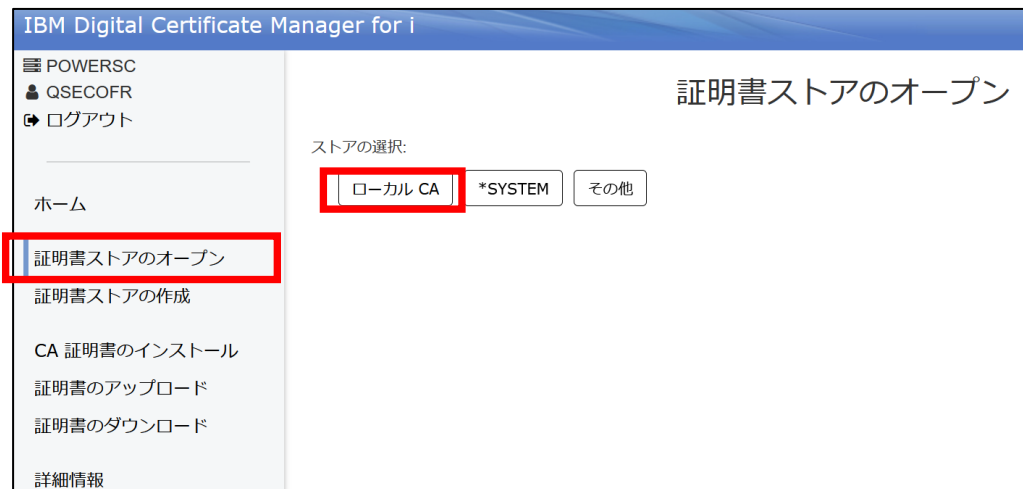
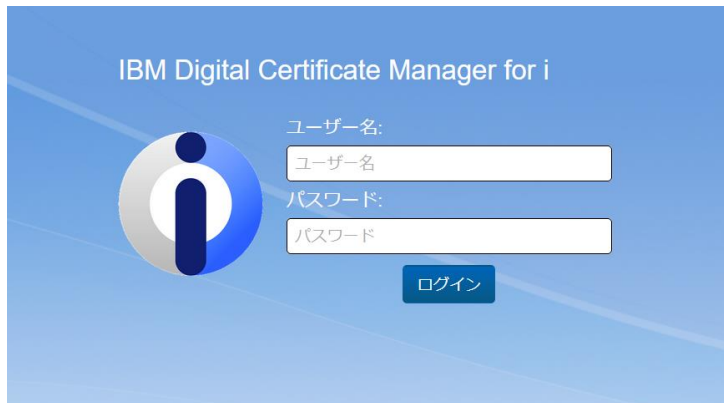
ステップ2：ローカル認証局を作成および操作する（1）

デジタル証明書マネージャー (DCM) を使用してIBM iシステム上に、ローカル認証局を作成します。

- ① IBM デジタル証明書マネージャー(DCM)を開始します
QSECOFRまたは、QSECOFR同等権限のユーザープロファイルでログインします。

- ② 「証明書ストアのオープン」 → 「ローカルCA」を選択します。

<http://XXX.XXX.XXX.XXX:2006/dcm/login>
(XXX.XXX.XXX.XXXは、IBM iのIPアドレス)



解説：

- ・ 認証局とは

認証局 (Certificate Authorities) とは、ユーザーとサーバーにデジタル証明書を発行できる、承認された組織のことです。

- デジタル証明書が有効な信任状として信頼されるためには、認証局に信用があることが前提となります。認証局は、秘密鍵を使って、証明書の発行元の妥当性検査をするために発行する証明書に、デジタル署名を作成します。受信側は認証局のデジタル証明書の公開鍵を使用して、認証局が発行し、署名したデジタル証明書の認証性を検証することができます。

- 認証局には、第三者機関が運営するパブリック認証局と、自社で独自に構築するプライベート認証局（ローカルCA）の2種類があります。社内に安全なインターネット環境を構築したり、社内アプリケーションを利用したりする場合は、プライベート認証局を立ち上げる方法もあります。デジタル証明書マネージャー (DCM) を使用すると、パブリック認証局の証明書もプライベート認証局の証明書も管理できます。

- ・ 独自のローカルCAを運用して、組織内のサーバーやクライアントにデジタル証明書を発行する場合にも、DCM を使用できます。

☆当資料では、ローカルCAの発行するデジタル証明書を用いて、社内に安全なインターネット環境を作成していきます。

ステップ 2：ローカル認証局を作成および操作する（2）

デジタル証明書マネージャー (DCM) を使用して IBM i システム上に、ローカル認証局を作成します。

- ③ パスワードを入力します。
忘れた場合はリセットします。

- ④ 「作成」を選択します。

ストアの選択:

[ローカル CA](#) [*SYSTEM](#) [*OBJECTSIGNING](#) [その他](#)

パスワード:

✖

[オープン](#) [パスワードのリセット](#)

ローカル CA

[最新表示](#) [ポリシー・データの変更](#) [パスワードの変更](#) [削除](#)

認証局 (CA) 証明書

[作成](#) [複数の証明書の処理](#)

ステップ2：ローカル認証局を作成および操作する（3）

デジタル証明書マネージャー (DCM) を使用してIBM iシステム上に、ローカル認証局を作成します。

- ⑤認証局を作成します。サブジェクト共通名、その他必要項目入力し、最下部の「作成」をクリックします。

認証局の作成

証明書情報:

鍵アルゴリズムとサイズ:

ECDSA (256 ビット) ▼

ハッシュ・アルゴリズム:

SHA-256 ▼

認証局の有効期間 (2 から 7300 日):

1095 ✓

サブジェクト:

共通名:

POWERDEMO ✓

組織単位:

IBM ✓

組織名:

IBM ✓

市区町村:

TOKYO ✓

- ここでは、サブジェクトを下記のように設定しました。
(これはサンプルです。貴社の固有情報を入力してください)

共通名：POWERDEMO

組織単位：IBM 組織名:IBM

市区町村：TOKYO 都道府県：TOKYO

郵便番号：1038510 国または地域：JP

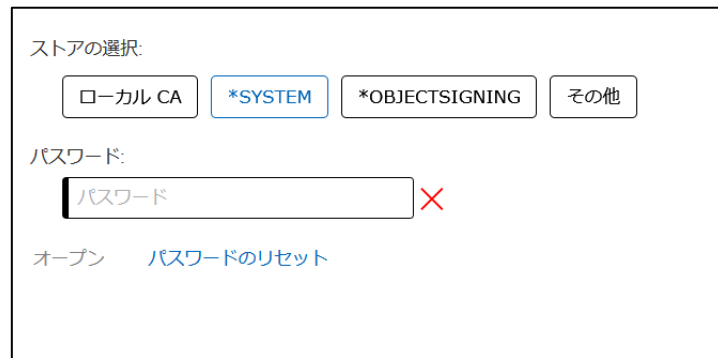
ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（1）

DCMは、システムがすべての 5250 通信セッションに TLS クライアント認証を必要とするかどうかを示す機能を備えています。TLS が有効であり、システムがクライアント認証を必要とする場合、有効なクライアント証明書が存在することは、クライアントが信頼されることを意味します。

ここでは、クライアント認証の証明書を要求するように Telnet サーバーを構成します。

- ① 「証明書ストアのオープン」
→ 「*SYSTEM」を選択します。

- ② パスワードを入力します。
忘れた場合はリセットします。



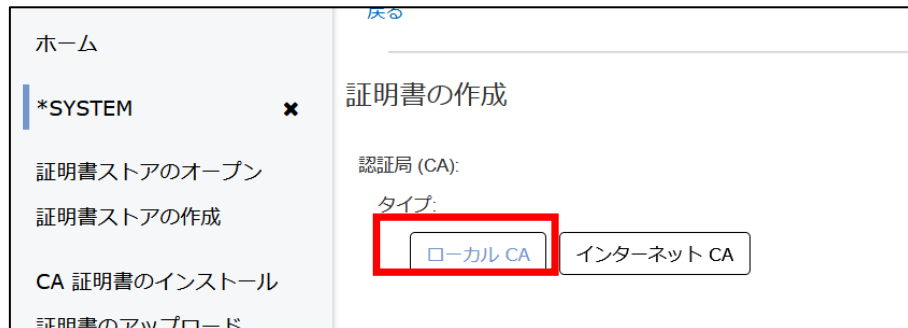
ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（2）

ここでは、クライアント認証の証明書を要求するように Telnet サーバーを構成します。

③ 証明書の「作成」を選択します。



④ ローカルCAを選択



ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（3）

ここでは、クライアント認証の証明書を要求するように Telnet サーバーを構成します。

- ⑤ラベル名、共通名（任意）、サブジェクト代替名（IPv4アドレスに IPアドレスを入力する）、ローカル CA（自分が作成した認証局になっていることを）などの必須項目入力後、最下部の「作成」を選択します。

ローカル CA | インターネット CA

ローカル CA:

LOCAL_CERTIFICATE_AUTHORITY_78051B03E(1) : ECDSA (256 ビット) : SHA256 with ECDSA

証明書情報:

ラベル: POWER_DEMO ✓

鍵アルゴリズムとサイズ: ECDSA (256 ビット)

サブジェクト:

共通名: POWER_DEMO ✓

組織単位: IBM ✓

組織名: IBM ✓

市区町村: TOKYO ✓

ここでは、サブジェクトを下記のように設定（これはサンプルです。貴社の固有情報を入力してください）

共通名: POWER_DEMO

組織単位: IBM

組織名: IBM

市区町村: TOKYO

都道府県: TOKYO

郵便番号: 1038510

国または地域: JP

- ⑥証明書が作成されたのを確認し、下記のように、右下の[+]を選択する

*SYSTEM

デフォルト証明書:
POWER_DEMO

最新表示 | アプリケーション定義の管理 | デフォルト証明書の削除 | パスワードの変更

証明書

作成 | インポート | CA の取り込み

▼ × サーバー/クライアント証明書

1/2 証明書を表示中

POWER_DEMO
POWER_DEMO

364 日後に有効期限が切れます
ECDSA (256 ビット)
ソフトウェアに保管されている
サーバー/クライアント証明書
デフォルト

表示

+

ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（4）

ここでは、クライアント認証の証明書を要求するように Telnet サーバーを構成します。

⑦下記画面で、「割り当て」を選択



⑧証明書の割り当て画面にて、「すべて選択」を選択する



ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（5）

ここでは、クライアント認証の証明書を要求するように Telnet サーバーを構成します。

⑨一番下の「追加」を選択

⑩この証明書を「デフォルトに設定」を選択する

<input checked="" type="checkbox"/>	QIBM_QTMM_POP_SERVER IBM I TCP/IP POPサーバー サーバー 証明書が割り当てられていません		
<input checked="" type="checkbox"/>	QIBM_QHASM_WEB サーバー 証明書が割り当てられていません		
<input checked="" type="checkbox"/>	SERVER サーバー 証明書が割り当てられていません		
置換	追加	すべて選択	すべて選択解除

*SYSTEM

[戻る](#)

証明書を表示

[更新](#) [エクスポート](#) [削除](#) [妥当性検査](#) [割り当](#) [デフォルトに設定](#)

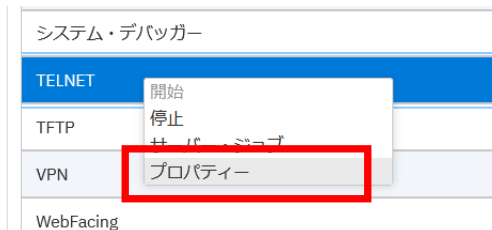
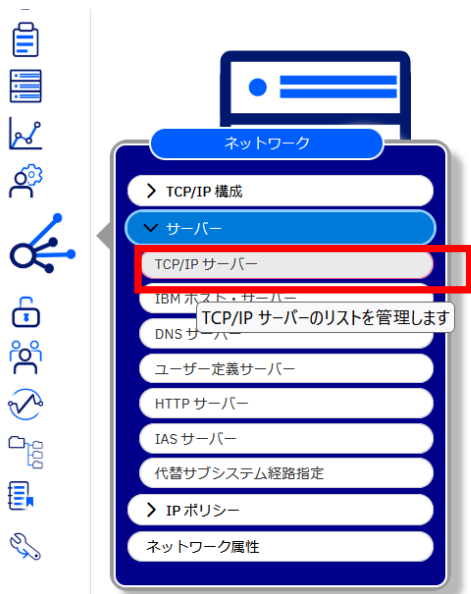
POWER_DEMO
POWER_DEMO

364 日後に有効期限が切れます
ECDSA (256 ビット)
ソフトウェアに保管されている
サーバー/クライアント証明書

ステップ4： Telnet サーバーでの TLS の有効化および開始 （1）

5250 セッションで TLS通信 を使用可能にするには、IBM Navigator for i または Telnet 属性変更 (CHGTELNA) コマンドを使用して、以下のステップを実行します。

- ① Navigator for i の [ネットワーク] → 「サーバー」 → [TCP/IPサーバー] を選択
- ② 「TELNET」 → 「プロパティ」 を選択する



ステップ4： Telnet サーバーでの TLS の有効化および開始 （2）

- ③下記の「一般」タブの下部にある、サーバーで開始されるソケット・レイヤー・サポート欄で、[セキュアと非セキュアの両方] を選択。

Telnet プロパティ

一般 TCP/IP の開始時に開始

マッピング 開始するサーバー・ジョブの数 (1 から 200)

システム・サインオン 計算

タイムアウト セッション・キープアラブ・タイムアウト (0 から 2419199 秒)

デバイス・エラー・アクション 計算されたデフォルト (600 秒)

リモート・サインオン デフォルトのネットワーク仮想端末

VT100

サーバーで開始されるソケット・レイヤー・サポート

セキュアのみ

非セキュアのみ

セキュアと非セキュアの両方

- ④ TELNETサーバーを再始動する。
- コンソールから下記を実施
(この作業は他に誰も使っていないことを確認して実施してください。)

- 一度TELNETサーバーを終了
ENDTCPSVR SERVER(*TELNET)
- 再度TELNETサーバーを起動
STRTCPSVR SERVER(*TELNET)

ステップ5：ACSクライアントでのTLS接続設定（1）

ACSクライアントが、TLS通信を確立するためにIBM iのTelnetサーバーが提示する証明書を認識し、受け入れることができなければなりません。Access Client Solutions (ACS) は、ユーザーにCAの受け入れを求めるプロンプトを出し、ACSが使用する鍵ストアに自動的に追加します。

ここからはACS側のTLS通信の設定方法をご紹介します。

- ① IBM i Access Client Solution (ACS)のメインメニューを起動します。管理の中の「システム構成」をクリックします。



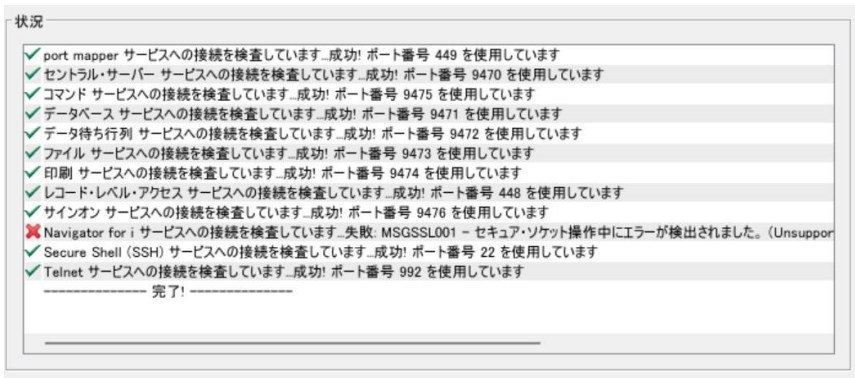
- ② 「新規」を選択して作成します。「システム名」フィールドにシステム名またはシステムIPアドレスを入力します。「一般」タブで、「接続にSSLを使用する」のチェックボックスをオンにします



ステップ5：ACSクライアントでのTLS接続設定（2）

ここからはACS側のTLS通信設定をご紹介します。

- ③ 「接続の確認」 ボタンを選択して、このシステム名へのTLS/SSL接続をテストします。
- ④ SSL をイネーブルにしてこのシステムに接続する最初の試行の場合、ACS は認証局を受け入れて信頼できるセットに追加するように要求します。認証局を受け入れて信頼するには、「はい」を選択する必要があります。ACS は、「はい」を選択して、認証局をキー管理データベースに追加します。（下記の認証局はサンプルです）

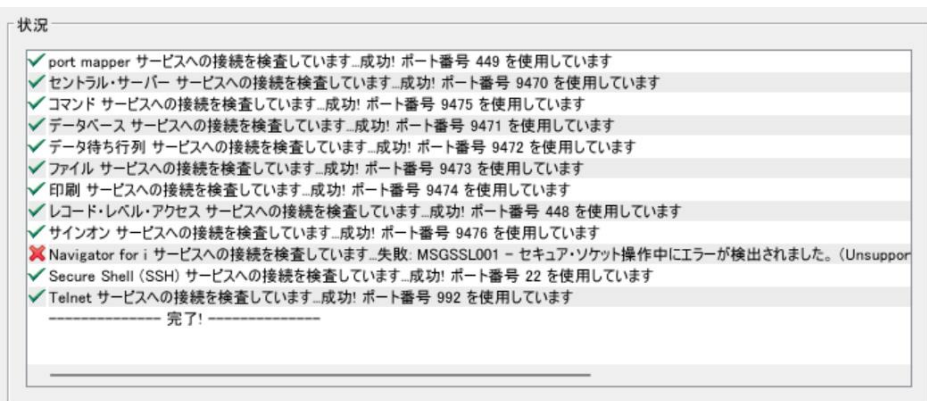


ステップ5：ACSクライアントでのTLS接続設定（3）

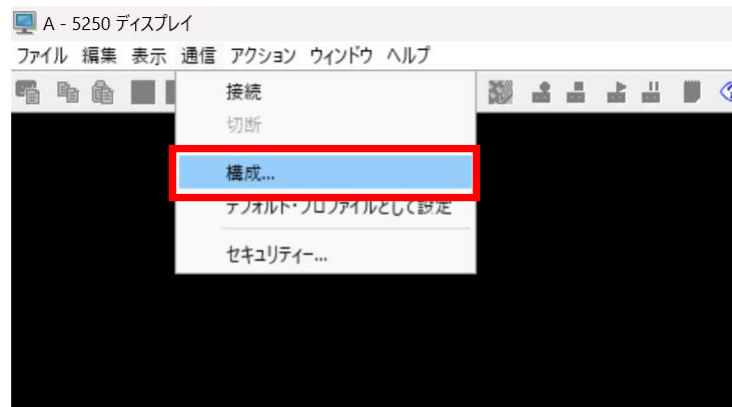
⑤成功すると、接続の確認の結果は次のように表示されます

Navigator for iはこの時点では、エラーになりますが、次章でNavigator for iでの設定方法をご紹介します。

その他のACSのサービスが、接続に成功していることを確認します。



⑥ ACSの5250エミュレーターをオープンし、「通信」→「構成」タブ開く



ステップ5：ACSクライアントでのTLS接続設定（4）

- ⑦5250ディスプレイメニューが開き、「接続」設定が表示されます。5250セッションでTLS/SSLを個別に使用するように設定するには、「プロトコル」設定を「Telnet - TLS/SSL」に変更します。この設定を変更すると、宛先ポートが23から992 (Telnetで使用されるTLSポート)に変更されます。OKをクリックします。

- ⑧この状態でサーバーへ接続すると5250画面の右下にロックマークが表示される

→これで5250セッションはTLS通信で暗号化されています

5250 ディスプレイ

接続

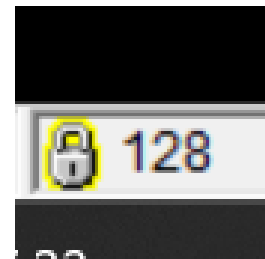
セッション名	5250 ディスプレイ
宛先アドレス	POWERDEMO
宛先ポート	992
プロトコル	Telnet - TLS/SSL
ワークステーション ID	<input type="text"/> 生成...
画面サイズ	27x132
ホスト・コード・ページ	1399 日本語 (Latin Unicode 拡張; JIS2004)

Unicode オプション

Unicode データストリームを使用可能にする	<input type="radio"/> はい <input checked="" type="radio"/> いいえ
Unicode フィールド内の DBCS を使用可能にする	<input type="radio"/> はい <input checked="" type="radio"/> いいえ
Unicode フィールド長の保護	<input checked="" type="radio"/> はい <input type="radio"/> いいえ

自動接続 はい いいえ

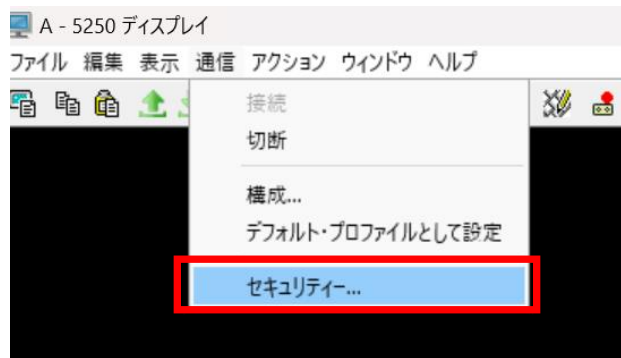
自動再接続 はい いいえ



ステップ5： ACSクライアントでのTLS接続設定（5）

- ⑨5250画面で、「通信」→セキュリティをクリックすると、セキュリティ情報の確認が可能

下記はサンプルです。



以上でACSによる5250通信のTLS設定は完了です。

ACS側のTLS設定の詳細な参考資料は下記になります。

<https://www.ibm.com/support/pages/how-configure-ibm-i-access-client-solutions-client-use-tlsssl>

4. Navigator for iのWebブラウザをTLS通信でセキュアにする方法

次に、IBM iの運用で最近利用することが多くなった、Navigator for iのWebブラウザでの通信をTLSで暗号化する設定を実施してみましょう。

設定は、下記の1から3のステップになります。

ステップ 1: ローカル認証局の証明書をPCにダウンロードする

ステップ 2: PCにローカル認証局の証明書をインポートする

ステップ 3: IBM Web Administration for iにてNavigator for iのTLS設定

各ステップでの作業詳細は、下記のマニュアルに記述ありますが、当資料では、実画面を表示して、設定方法をご紹介します。

<https://www.ibm.com/support/pages/enabling-tls-ibm-navigator-i>


ステップ1：ローカル認証局の証明書をダウンロードする（1）

まずは、ローカル認証局にアクセスして、証明書をPCへダウンロードします。

- ① 下記のようにして、DCMにアクセスする。
<http://xxx.xxx.xxx.xxx:2006/dcm/login>



- ② 「証明書のストアオープン」 → 「ローカルCA」
→ パスワード入力で、
作成済のローカルCAの「表示」をクリック



ステップ1：ローカル認証局の証明書をダウンロードする（2）

③認証局の表示で「エクスポート」を選択

認証局の表示

更新 **エクスポート** 削除

LOCAL_CERTIFICATE_AUTHORITY_78051B03E(1)
POWERDEMO

1093 日後に有効期限が切れます
ECDSA (256 ビット)
ソフトウェアに保管されている
認証局 (有効)

④認証局をローカルPCへダウンロードするため、ロケーションを「ダウンロード」をクリック、パス（任意の認証局ファイル名）を入力後、「エクスポート」をクリック

認証局のエクスポート

LOCAL_CERTIFICATE_AUTHORITY_78051B03E(1)
POWERDEMO

1093 日後に有効期限が切れます
ECDSA (256 ビット)
ソフトウェアに保管されている
認証局 (有効)

ロケーション:

ファイル ストア **ダウンロード**

パス:

POWERDEMO| ✓

参照

エクスポート

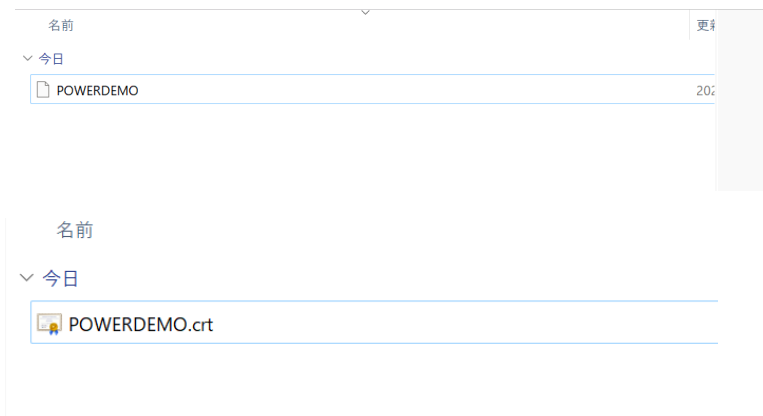
✓ 証明書が正常にエクスポートされました ×
LOCAL_CERTIFICATE_AUTHORITY_78051B03E(1)

ステップ1：ローカル認証局の証明書をダウンロードする（3）

- ⑤ 「証明書のダウンロード」を選択し、
証明書の「ダウンロード」を選択



- ⑥ PCに、証明書がダウンロードされます。
拡張子にcrtを付けて保管しておきます。



ステップ2：PCにローカル認証局の証明書をインポートする（1）

次に、ダウンロードした、証明書をWindows PCへ取り込みます。

①Windowsの「ネットワークとインターネット」の中にある、インターネットオプションを選択

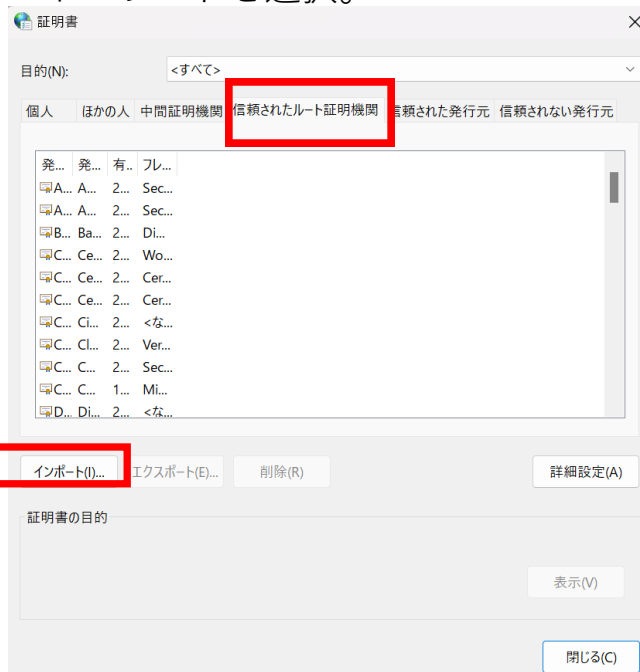


②下記の「インターネットのプロパティ」の「コンテンツ」タブの「証明書」を選択します。

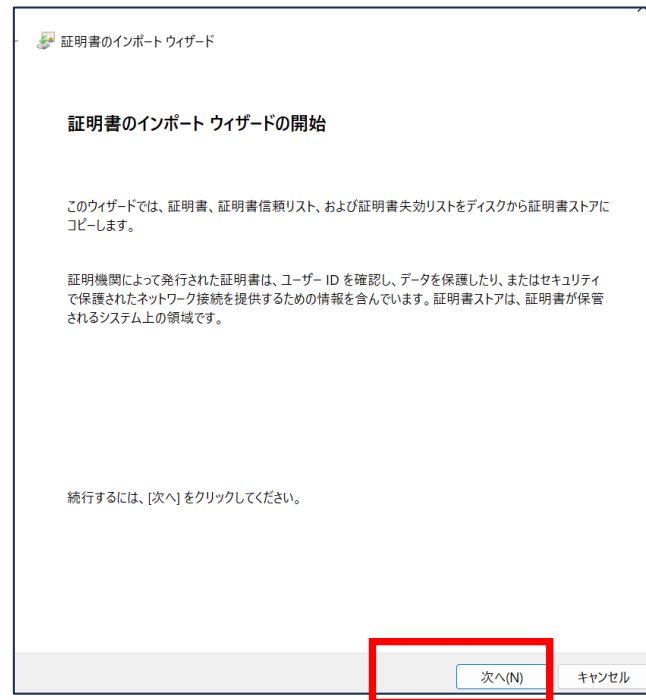


ステップ2：PCにローカル認証局の証明書をインポートする（2）

- ③「信頼されたルート証明機関」で、インポートを選択。

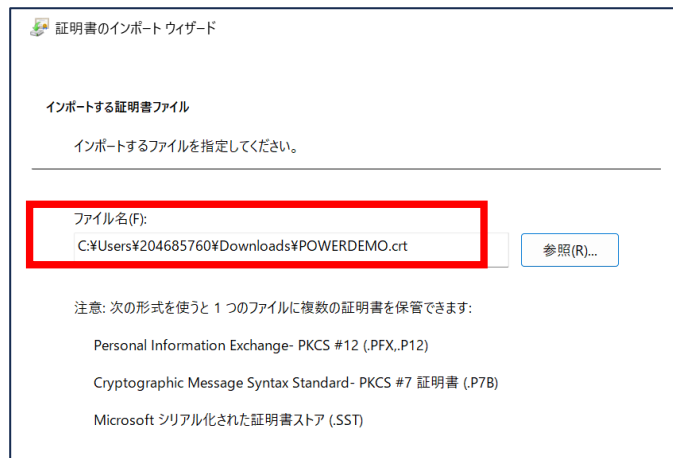


- ④証明書のインポートウィザードが起動するので次へをクリック



ステップ2：PCにローカル認証局の証明書をインポートする（3）

- ⑤ファイル名に、ダウンロードしたファイルを入力して、次へを選択



証明書のインポート ウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

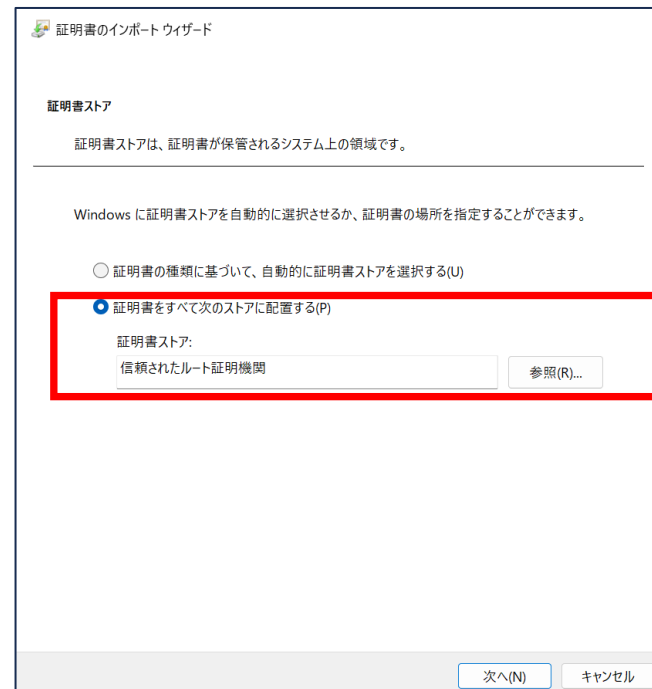
ファイル名(F):
C:\Users\204685760\Downloads\POWERDEMO.crt

参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

- ⑥下記のように証明書ストアに、信頼されたルート証明機関であることを確認して、次へを選択



証明書のインポート ウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

証明書をすべて次のストアに配置する(P)

証明書ストア:
信頼されたルート証明機関

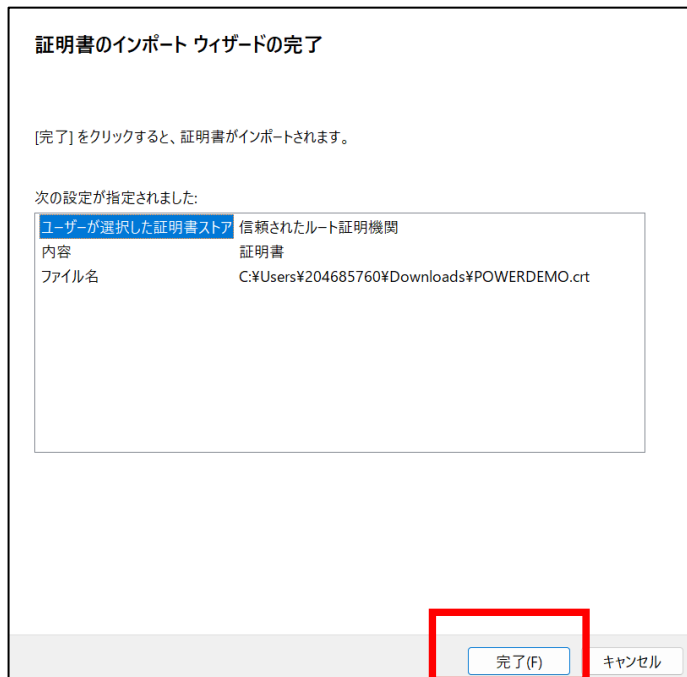
参照(R)...

次へ(N) キャンセル

ステップ2：PCにローカル認証局の証明書をインポートする（4）

⑦下記で完了を選択

以上で、PCへの証明書の取り込みは完了です。



ステップ3： IBM Web Administration for i にて Navigator for i の TLS 設定 (1)

次に、 Navigator for i を TLS 通信で起動するための設定を実施します。

- ① 下記のようにして、
IBM Web Administration for i にログインする
`http:// XXX.XXX.XXX.XXX:2001/HTTPAdimn`
(XXX.XXX.XXX.XXXはIBM i のIPアドレス)

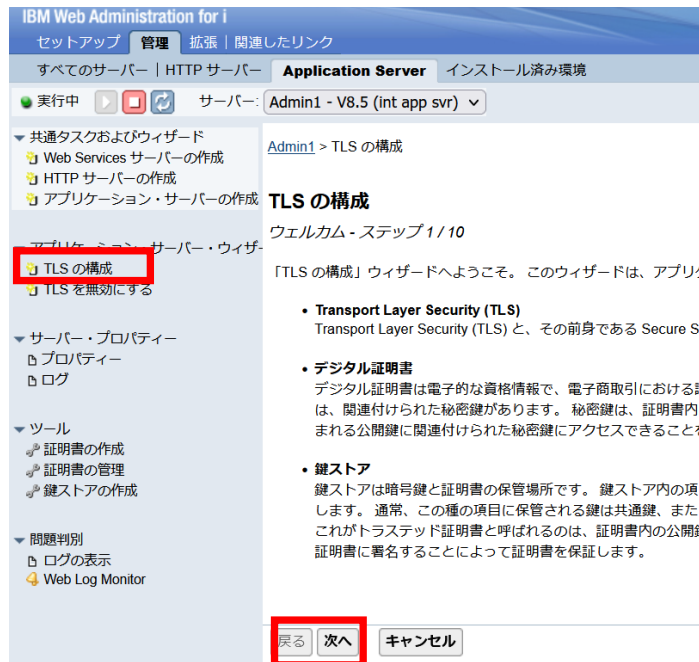


- ② 「管理」 タブのサーバー：Admin1を選択して
「詳細の管理」を選択
※Admin1はNavigator for i のサーバーです

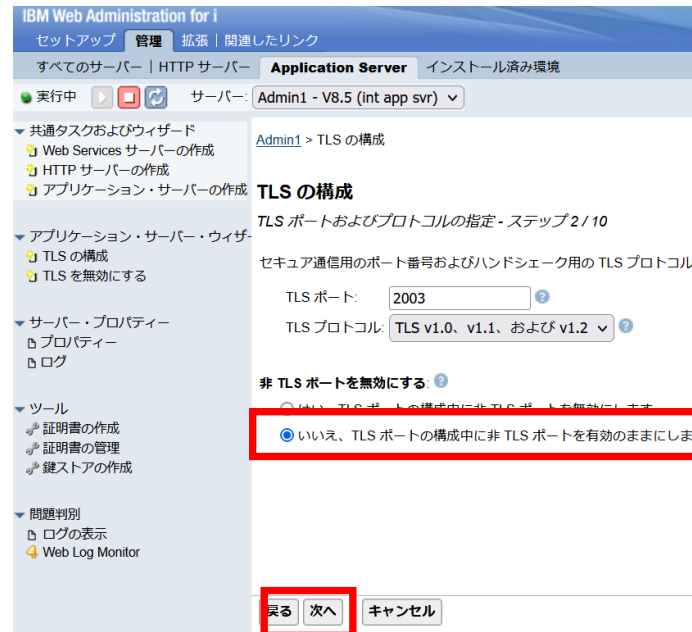


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（2）

- ③ 「TLSの構成」をクリック、
TLS構成の設定エリアで「次へ」をクリック



- ④ 非TLSサポートを無効にする の項目で、
「いいえ」にチェックを入れ、「次へ」をクリック
*http接続が全くできなくなってしまうため
「いいえ」で設定すること



ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（3）

- ⑤ 「鍵ストア情報の指定」の項目で、
「デジタル証明書マネージャ(DCM)システムストアの使用」
にチェックを入れ、「次へ」をクリック

IBM Web Administration for i
セットアップ 管理 拡張 関連したリンク
すべてのサーバー | HTTP サーバー Application Server インストール済み環境
実行中 サーバー: Admin1 - V8.5 (int app svr)

Admin1 > TLS の構成

TLS の構成
鍵ストア・パスワードの指定 - ステップ 3 / 10

鍵ストアは暗号鍵と証明書の保管場所です。信頼に関する決定を下すために必要な署名者証明書はしてください。

鍵ストア情報の指定

鍵ストア・パスとタイプの指定
 デジタル証明書マネージャ (DCM) システム・ストアの使用
 別のトラストストア・パスの指定

- ⑥ *SYSTEMストアのパスワードを入力し、
「次へ」をクリック

IBM Web Administration for i
セットアップ 管理 拡張 関連したリンク
すべてのサーバー | HTTP サーバー Application Server インストール済み環境
実行中 サーバー: Admin1 - V8.5 (int app svr)

Admin1 > TLS の構成

TLS の構成
鍵ストア・パスワードの指定 - ステップ 4 / 10

鍵ストアは不正アクセスを防止する安全な形式で保管されます。鍵今後とも利用するので安全な場所に保管してください。

鍵ストア・パスワードの指定

パスワード: ●●●●●●

このパスワードは安全ではありません。このパスワードを入力したログイン情報は漏洩する可能性があります。詳細

戻る 次へ キャンセル

ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（4）

- ⑦ 「鍵ストアから既存の証明書を選択」にチェックを入れ、前章で作成したデジタル証明書を選択、「次へ」をクリック

IBM Web Administration for i
セットアップ 管理 拡張 関連したリンク
すべてのサーバー | HTTP サーバー Application Server インストール済み環境
実行中 停止 再起動 サーバー: Admin1 - V8.5 (int app svr)

共通タスクおよびウィザード
Web Services サーバーの作成
HTTP サーバーの作成
アプリケーション・サーバーの作成

アプリケーション・サーバー・ウィザード
TLS の構成
TLS を無効にする

サーバー・プロパティ
プロパティ
ログ

ツール
証明書の作成
証明書の管理
鍵ストアの作成

問題判別
ログの表示
Web Log Monitor

Admin1 > TLS の構成
デジタル証明書の指定 - ステップ 6 / 10
TLS を構成するには、サーバーにデジタル証明書がなければなりません。サーバーのデジタル証明書を指定してください。
サーバーのデジタル証明書を指定します: ⑦
 自己署名証明書の新規発行
 鍵ストアから既存の証明書を選択
 デジタル証明書: POWER_DEMO
 注: (*) でマーク付けされたデジタル証明書は期限切れです。

戻る 次へ キャンセル

- ⑧ 「インポートする証明書はありません」にチェックを入れ、「次へ」をクリック

IBM Web Administration for i
セットアップ 管理 拡張 関連したリンク
すべてのサーバー | HTTP サーバー Application Server インストール済み環境
実行中 停止 再起動 サーバー: Admin1 - V8.5 (int app svr)

共通タスクおよびウィザード
Web Services サーバーの作成
HTTP サーバーの作成
アプリケーション・サーバーの作成

アプリケーション・サーバー・ウィザード
TLS の構成
TLS を無効にする

サーバー・プロパティ
プロパティ
ログ

ツール
証明書の作成
証明書の管理
鍵ストアの作成

問題判別
ログの表示
Web Log Monitor

Admin1 > TLS の構成
トラステッド CA 証明書の追加 - ステップ 7 / 10
アプリケーション・サーバーが信頼に関する決定を下すためのトラを確認することができます。
信頼証明書をトラストストアに追加するかどうかを指定します: ⑧
 インポートする証明書はありません
 トラステッド CA 証明書の追加

戻る 次へ キャンセル

ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（5）

- ⑨ 「デフォルトの暗号」にチェックを入れ、「次へ」をクリック

IBM Web Administration for i
 セットアップ 管理 拡張 | 関連したリンク
 すべてのサーバー | HTTP サーバー Application Server インストール済み環境
 実行中 ▶ ⏸ ⏪ ⏩ サーバー: Admin1 - V8.5 (int app svr) ▼

Admin1 > TLS の構成

TLS の構成

TLS 用の暗号の指定 - ステップ 8 / 10

TLS 用の暗号の指定: デフォルトの暗号
 使用可能な暗号のリストから暗号を選択してください

戻る 次へ キャンセル

- ⑩ 「ウィザードの直後にサーバーを再始動する」にチェックを入れ、「次へ」をクリック

IBM Web Administration for i ウェル
 セットアップ 管理 拡張 | 関連したリンク
 すべてのサーバー | HTTP サーバー Application Server インストール済み環境
 実行中 ▶ ⏸ ⏪ ⏩ サーバー: Admin1 - V8.5 (int app svr) ▼

Admin1 > TLS の構成

TLS の構成

すぐにサーバーを再始動しますか? - ステップ 9 / 10

このウィザードの完了後に構成を有効にするためには、当該サーバーを再始動する。

サーバーを後で自分で再始動する
 ウィザードの直後にサーバーを再始動する

戻る 次へ キャンセル

ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（6）

- ⑪ 下記の要約画面で「完了」をクリック
サーバーが実行中になるのを待つ

IBM Web Administration for i

セットアップ 管理 拡張 関連したリンク

すべてのサーバー | HTTP サーバー Application Server インストール済み環境

実行中 実行 停止 刷新 サーバー Admin1 - V8.5 (int app svr)

Admin1 > TLS の構成

Web Services サーバーの作成
HTTP サーバーの作成
アプリケーション・サーバーの作成

アプリケーション・サーバー・ウィザード

TLS の構成
TLS を無効にする

サーバー・プロパティ
プロパティ
ログ

ツール
証明書の作成
証明書の管理
鍵ストアの作成

問題判別
ログの表示
Web Log Monitor

Admin1 > TLS の構成

要約 - ステップ 10 / 10

「完了」をクリックすると、このウィザードはこのサーバー用に TLS を構成します。

IP アドレス: すべての IP アドレス
TLS ポート: 2003
SSL プロトコル: TLS v1.0, v1.1, および v1.2
鍵ストア: DCM システム・ストア
証明書名: POWER_DEMO

注: 構成が完了すると、ウィザードは当該サーバーを再始動して構成を有効にします。

戻る 完了 キャンセル

- ⑫ ブラウザーが、Firefoxの場合は、右上のメニューから
「設定」を選択。

☆ 設定 拡張機能 検索 印刷

新しいタブ Ctrl+T
新しいウィンドウ Ctrl+N
新しいプライベートウィンドウ Ctrl+Shift+P

ブックマーク >
履歴 >
ダウンロード Ctrl+J
パスワード
アドオンとテーマ Ctrl+Shift+A

印刷... Ctrl+P
名前を付けてページを保存... Ctrl+S
ページ内を検索... Ctrl+F
ページを翻訳...

ズーム - 100% +

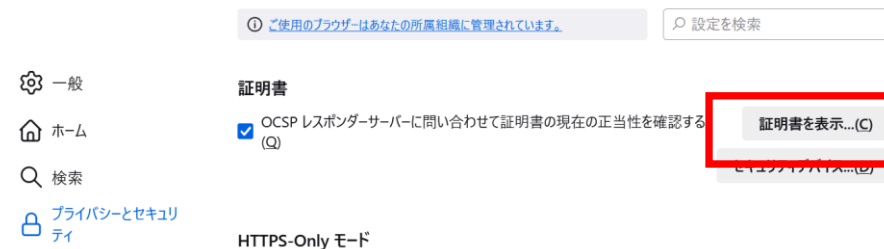
設定

その他のツール >
動作しないサイトを報告 >
ヘルプ >

終了 Ctrl+Shift+Q

ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（7）

- ⑬ 「プライバシーとセキュリティ」を選択して、「証明書を表示」を選択

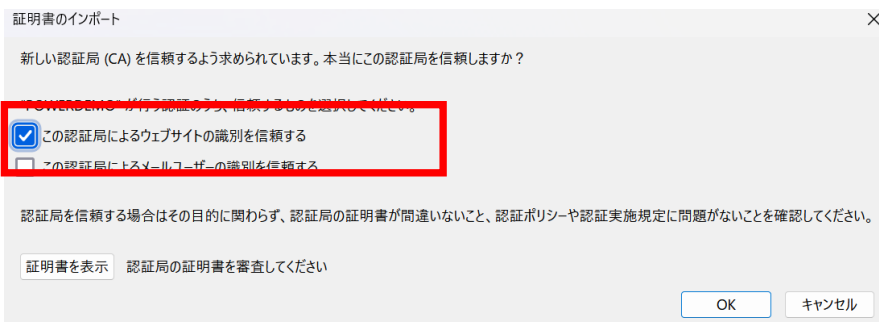


- ⑭ 下記の証明書マネージャーで、認証局証明書タブを選択してインポートをクリック



ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（8）

- ⑮ダウンロードしたPOWERDEMOを選択し、
下記のようにして、OKをクリック

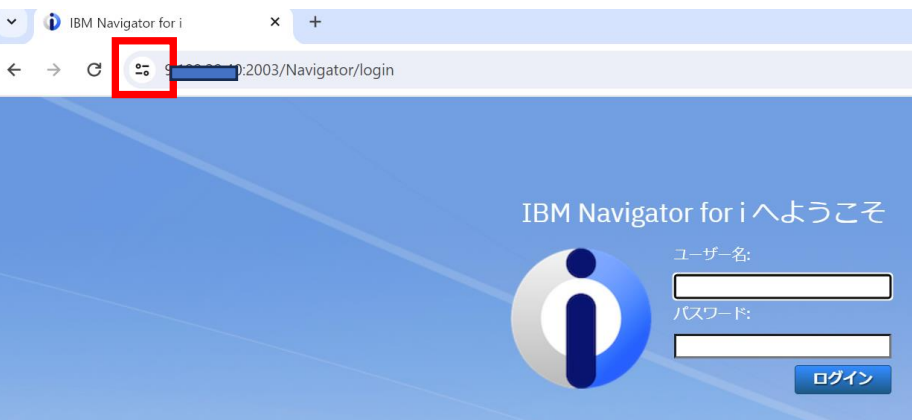


- ⑯以下にアクセスし、
接続が保護されていることを確認する。
<https://XXX.XXX.XXX.XXX:2003/Navigator/login>

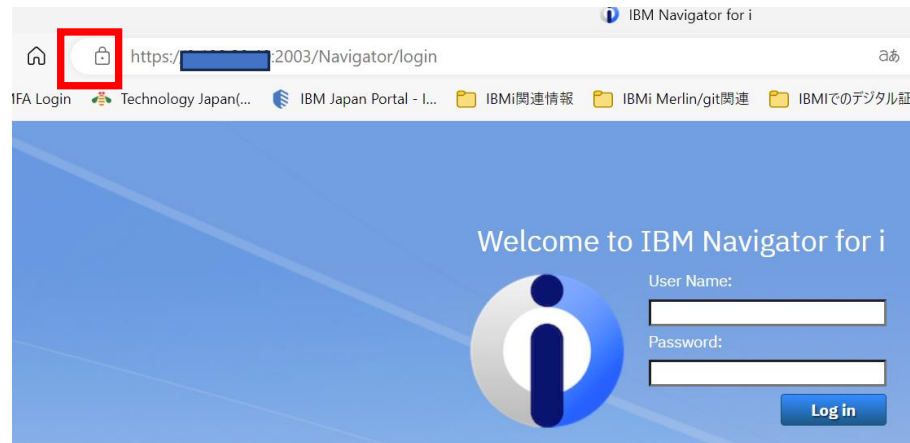


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（9）

Chromeの場合は、ブラウザ側の設定なしで接続できました。



Edgeの場合も、ブラウザ側の設定なしで接続できました。



5. 補足情報

1. IBM i 7.5 マニュアル (トランスポート層セキュリティー)
<https://www.ibm.com/docs/ja/i/7.5?topic=security-transport-layer>
2. IBM i 7.5 マニュアル (デジタル証明書マネージャー)
<https://www.ibm.com/docs/ja/i/7.5?topic=security-digital-certificate-manager>
3. Digital Certificate Manager (DCM) - Frequently Asked Questions and Common Tasks
<https://www.ibm.com/support/pages/digital-certificate-manager-dcm-frequently-asked-questions-and-common-tasks>
4. How to configure IBM i Access Client Solutions client to use TLS/SSL
<https://www.ibm.com/support/pages/how-configure-ibm-i-access-client-solutions-client-use-tlssl>
5. Configuring Your IBM i System Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Protocols and Cipher Suites
<https://www.ibm.com/support/pages/configuring-your-ibm-i-system-secure-sockets-layer-ssltransport-layer-security-tls-protocols-and-cipher-suites>
6. Configuring Telnet and Host Servers for Server Authentication with TLS for the First Time
<https://www.ibm.com/support/pages/configuring-telnet-and-host-servers-server-authentication-tls-first-time>

IBM i 関連情報

IBM i ポータル・サイト

<https://ibm.biz/ibmijapan>

i Magazine (IBM i 専門誌。春夏秋冬の年4回発刊)

<https://www.imagazine.co.jp/IBMi/>

IBM i World 2023 オンデマンド・セミナー

<https://ibm.biz/ibmiworld2023>

IBM i World 2022 オンデマンド・セミナー

<https://video.ibm.com/recorded/132423205>

月イチIBM Power情報セミナー「IBM Power Salon」

<https://ibm.biz/power-salon>

IBM i 関連セミナー・イベント

<https://ibm.biz/powerevents-i>

IBM i Club (日本のIBM i ユーザー様のコミュニティー)

<https://ibm.biz/ibmiclubjapan>

IBM i 研修サービス (i-ラーニング社提供)

<https://www.i-learning.jp/service/it/iseriess.html>

IBM Power Systems Virtual Server 情報

<https://ibm.biz/pvsjapan>

IBM i 情報サイト iWorld

<https://ibm.biz/iworldweb>

IBM i サポートロードマップ

<https://public.dhe.ibm.com/systems/support/planning/transfer/IBM.i.Support.Roadmap.pdf>

IBM i 7.5 技術資料

<https://www.ibm.com/docs/ja/i/7.5>

IBM Power ソフトウェアのダウンロードサイト (ESS)

<https://ibm.biz/powerdownload>

Fix Central (HW・SWのFix情報提供)

<https://www.ibm.com/support/fixcentral/>

IBM My Notifications (IBM IDの登録 [無償] が必要)

「IBM i」 「9009-41G」 などPTF情報の必要な製品を選択して登録できます。

<https://www.ibm.com/support/mynotifications>

IBM i 各バージョンのライフサイクル

<https://www.ibm.com/support/pages/release-life-cycle>

IBM i 以外のSWのライフサイクル (個別検索)

<https://www.ibm.com/support/pages/lifecycle/>



ワークショップ、セッション、および資料は、IBMによって準備され、IBM独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる読者に対しても法律的またはその他の指導や助言を意図したのではなく、またそのような結果を生むものでもありません。本資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。本資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引き出すことを意図したもので、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでなく、またそのような結果を生むものでもありません。

本資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本資料に含まれている内容は、読者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したもので、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

IBM、IBM ロゴ、ibm.com、Db2、Rational、Power、POWER8、POWER9、AIXは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。

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

現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、およびPentium は Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linuxは、Linus Torvaldsの米国およびその他の国における登録商標です。

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

ITILはAXELOS Limitedの登録商標です。

UNIXはThe Open Groupの米国およびその他の国における登録商標です。

JavaおよびすべてのJava関連の商標およびロゴは Oracleやその関連会社の米国およびその他の国における商標または登録商標です。