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

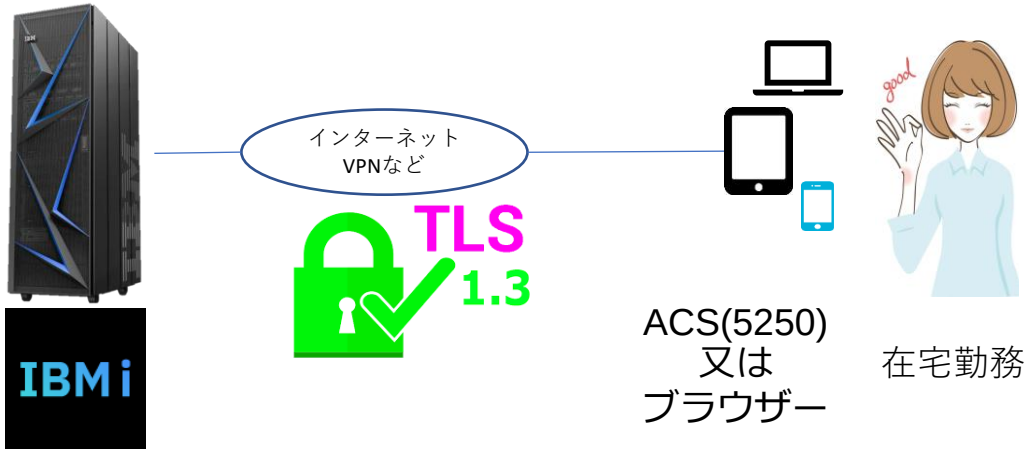
5250セッションの通信を暗号化して、在宅勤務で使ってみよう

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ブラウザーの通信データも暗号化する方法をご紹介します。

目次

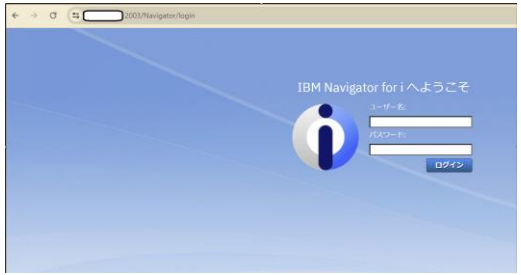
1. 通信の暗号化の利用例

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)。



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ー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ブラウザーだけでなく、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保全性も提供します。

・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、ユーザビリティー、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ています。
https://www.ibm.com/docs/ja/i/7.5?topic=tls-configuration-details-securing-telnet#rzaiwscenariossldetails__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

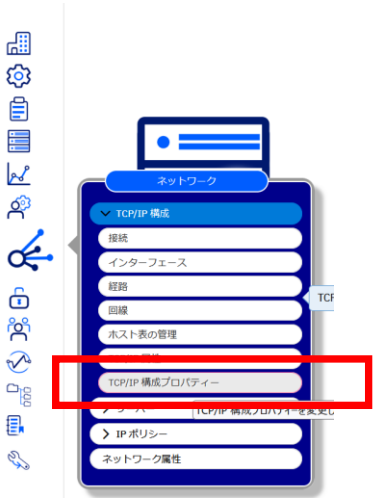
・この資料では、IBM i 7.5の最新のGUIインターフェイスを使用する前提です。

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プロパティー」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）



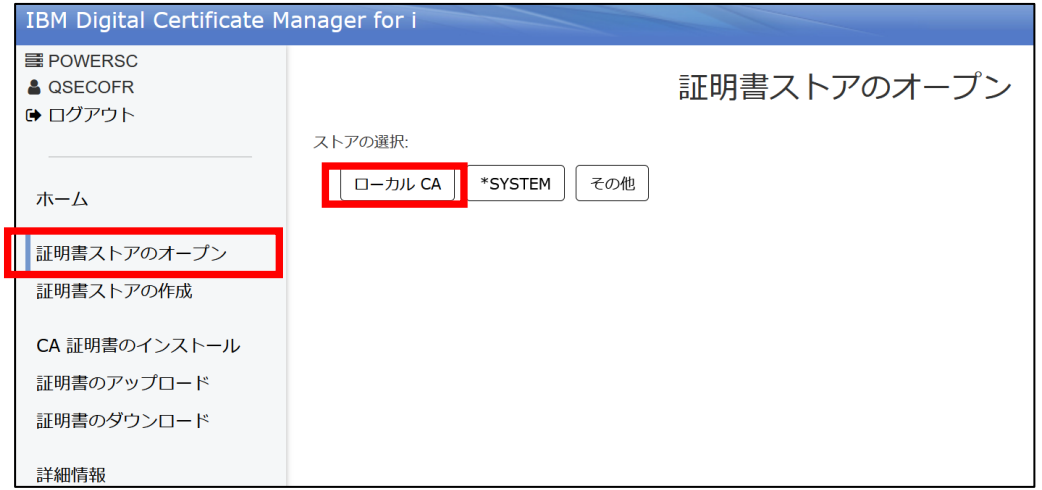
ステップ２：ローカル認証局を作成および操作する（１）

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。

①IBM ディ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。

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

②「証明書ストアのオープン」→「ローカルCA」を選択します。



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、ディ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。ディ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。

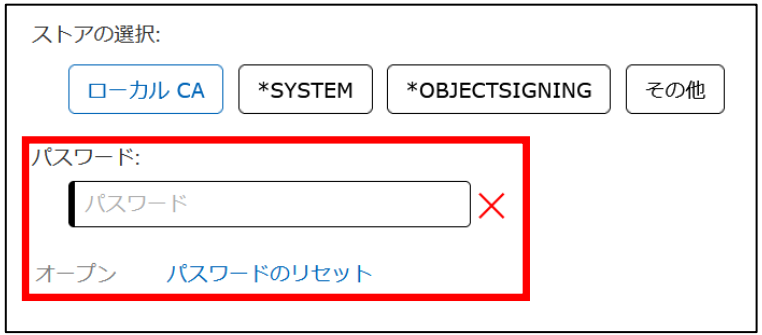
・独自のローカルCAを運用して、組織内のサーバーやクライアントにデジタル証明書を発行する場合にも、DCM を使用できます。

☆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。

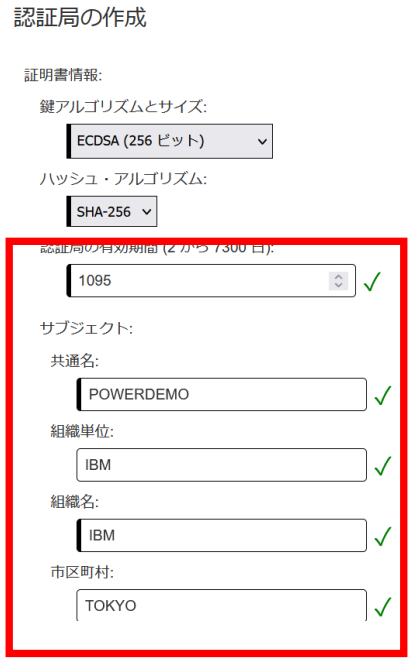


④「作成」を選択します。

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。



・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

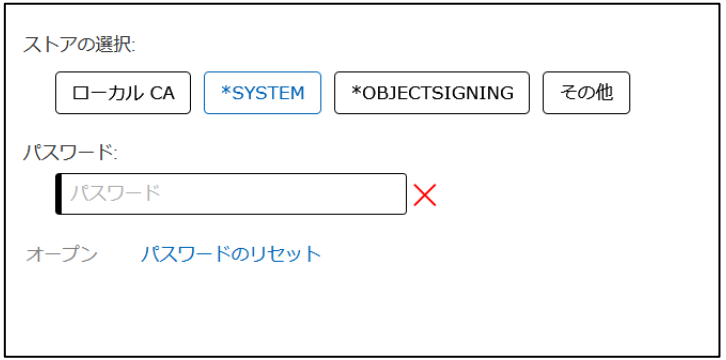
ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（1）

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。

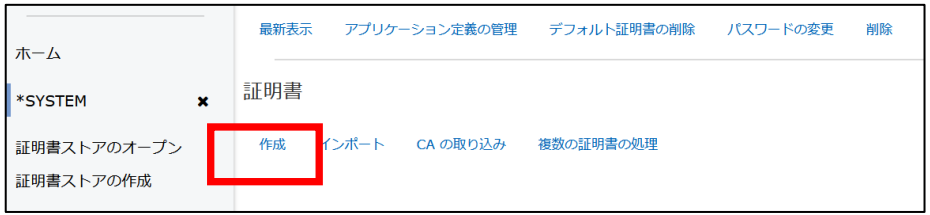
②パスワードを入力します。
忘れた場合はリセットします。



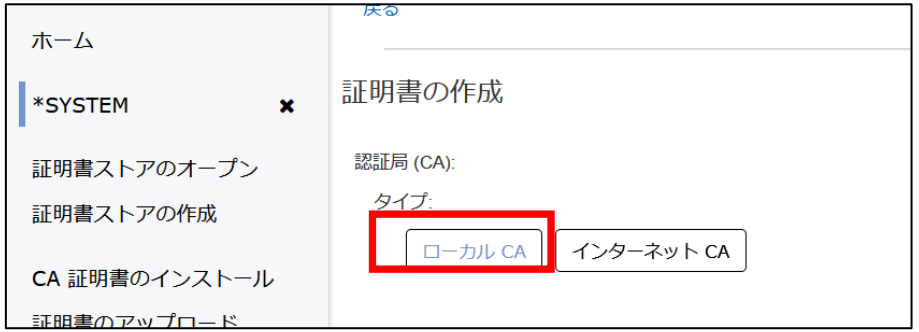
ステップ3：クライアント認証の証明書を要求するように Telnet サーバーを構成（２）

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。



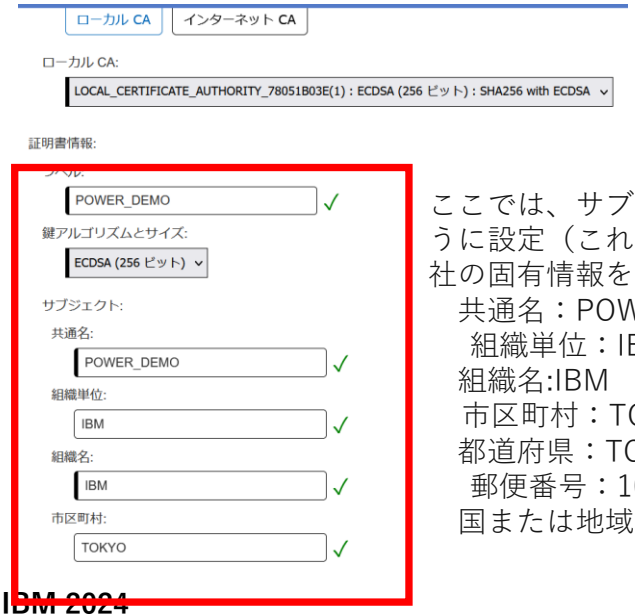
④ローカルCAを選択



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。



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

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。

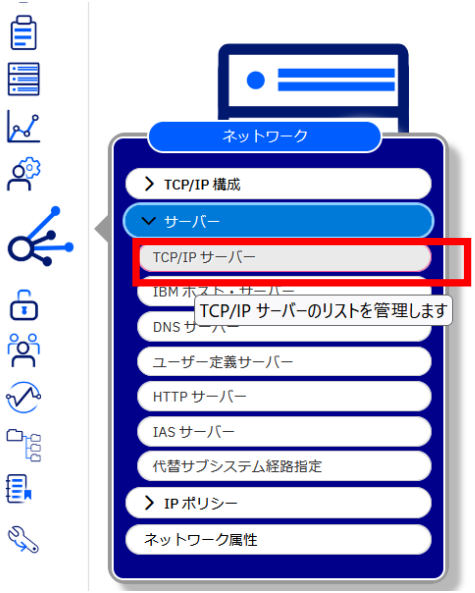
⑨一番下の「追加」を選択

⑩この証明書を「デフォルトに設定」を選択する

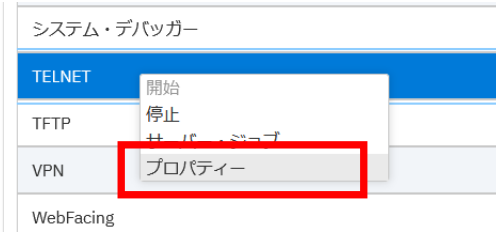
ステップ4： Telnet サーバーでの TLS の有効化および開始 （１）

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。

①Navigator for iの[ネットワーク」→「サーバー」
→[TCP/IPサーバー」を選択

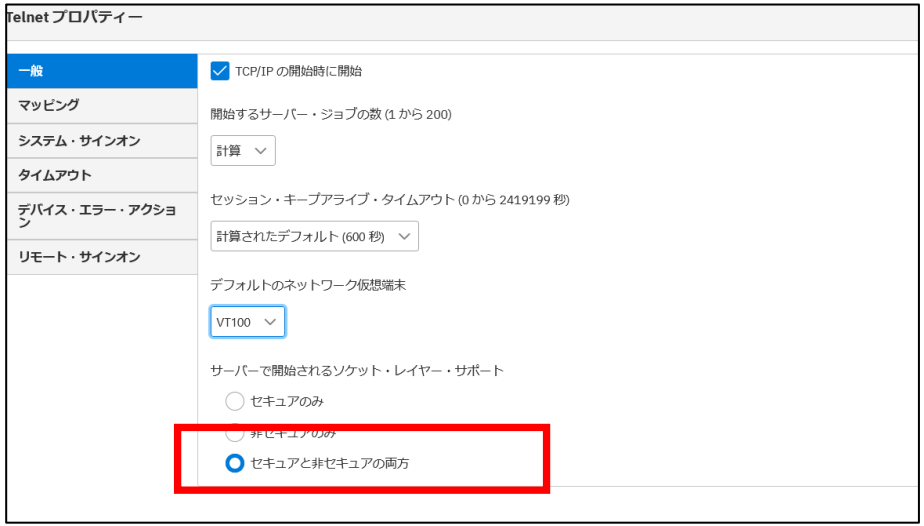


②「TELNET」→「プロパティ」を選択する



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、[セキュアーと非セキュアーの両方」を選択。



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。)

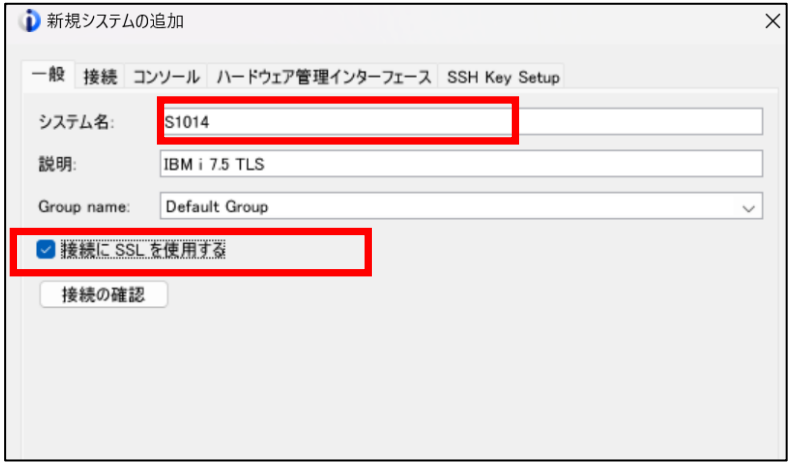
・一度TELNETサーバーを終了
　ENDTCPSVR SERVER(*TELNET)
・再度TELNETサーバーを起動
　STRTCPSVR SERVER(*TELNET)

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。

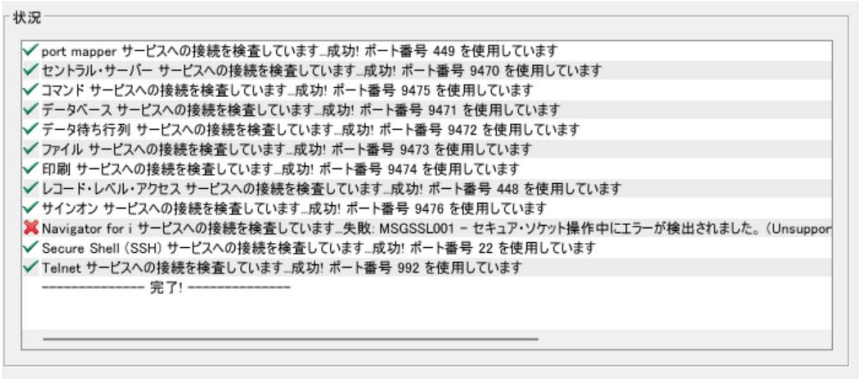
② 「新規」を選択して作成します。「システム名」フィールドにシステム名またはシステムIPアドレスを入力します。
「一般」タブで、「接続にSSLを使用する」のチェックボックスをオンにします



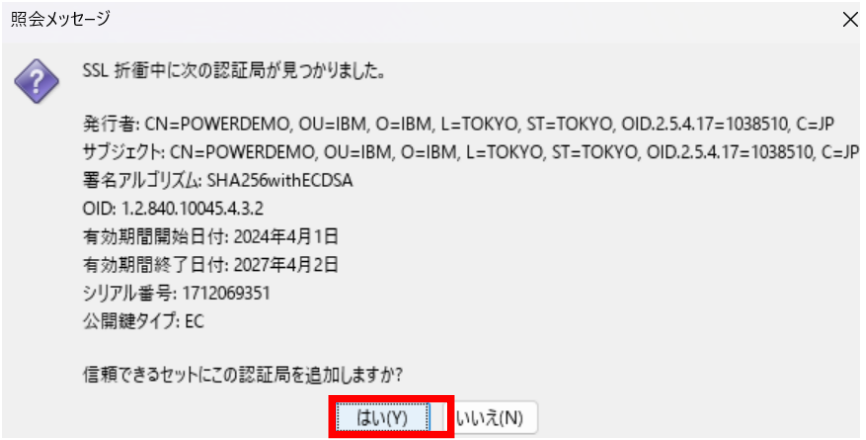
ステップ5： ACSクライアントでのTLS接続設定 （２）

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）

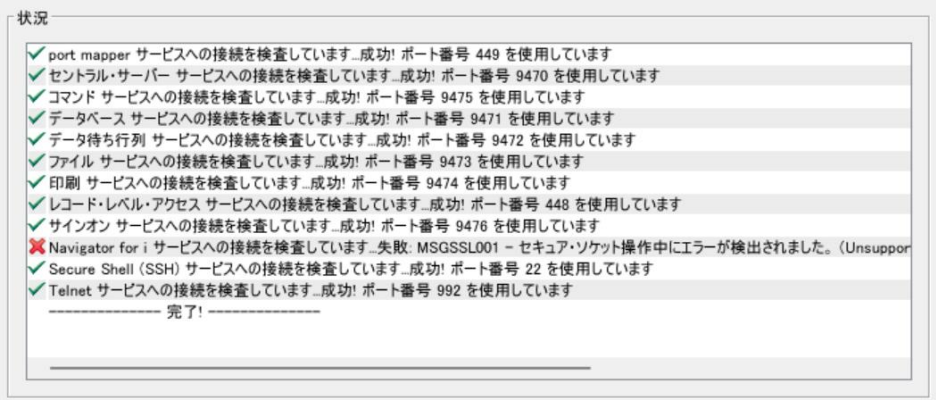


ステップ5： ACSクライアントでのTLS接続設定 （３）

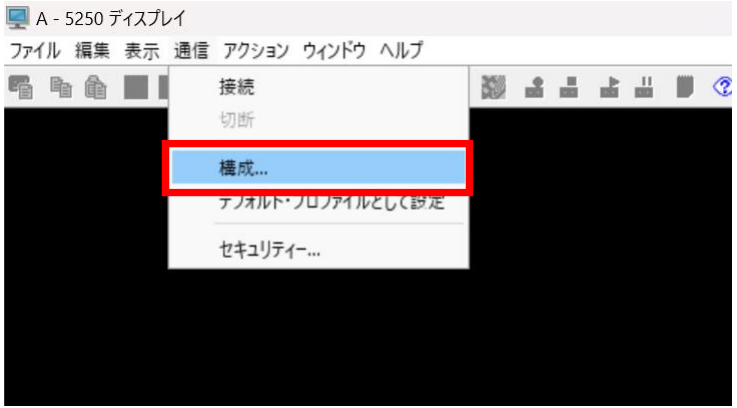
⑤成功すると、接続の確認の結果は次のように表示されます

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。

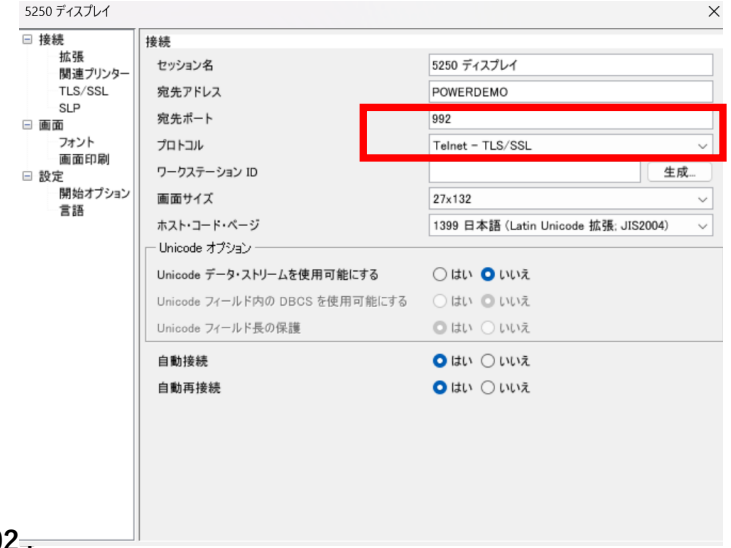


⑥ ACSの5250エミュレーターをオープンし、
「通信」→「構成」タブ開く



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。



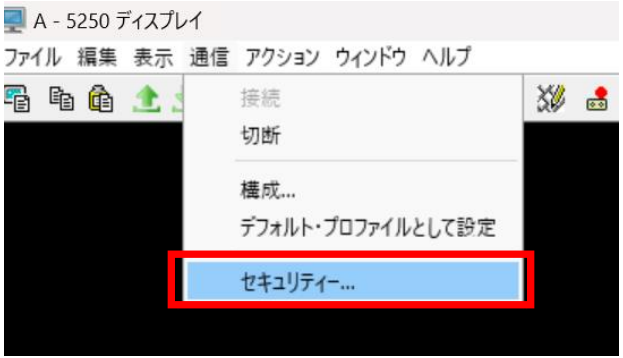
⑧この状態でサーバーへ接続すると
5250画面の右下にロックマークが表示される

→これで5250セッションはTLS通信で暗号化されています

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ブラウザーをTLS通信でセキュアーにする方法

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ブラウザーでの通信を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ています。
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。

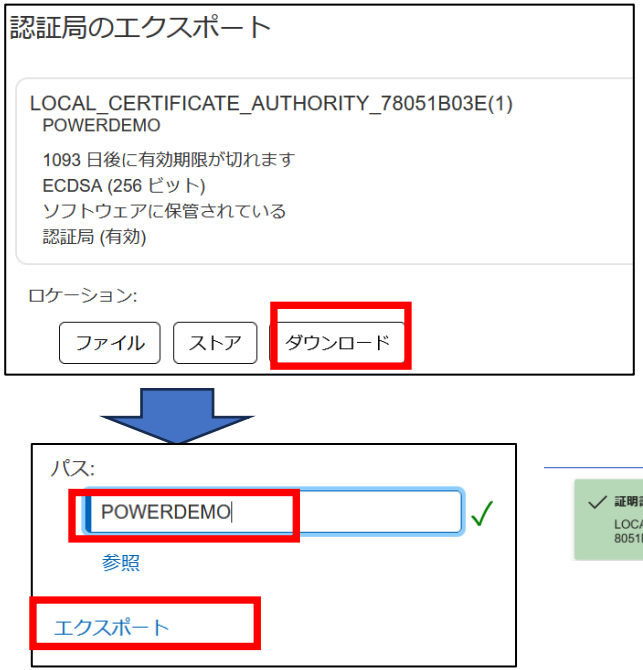
①下記のようにして、DCMにアクセスする。
http://xxx.xxx.xxx.xxx:2006/dcm/login

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

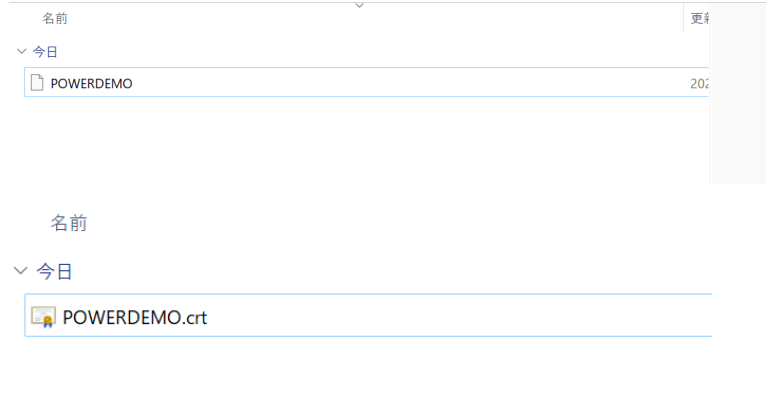
④認証局をローカルPCへダウンロードするため、
ロケーションを「ダウンロード」をクリック、
パス（任意の認証局ファイル名）を入力後、
「エクスポート」をクリック



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

⑥PC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。

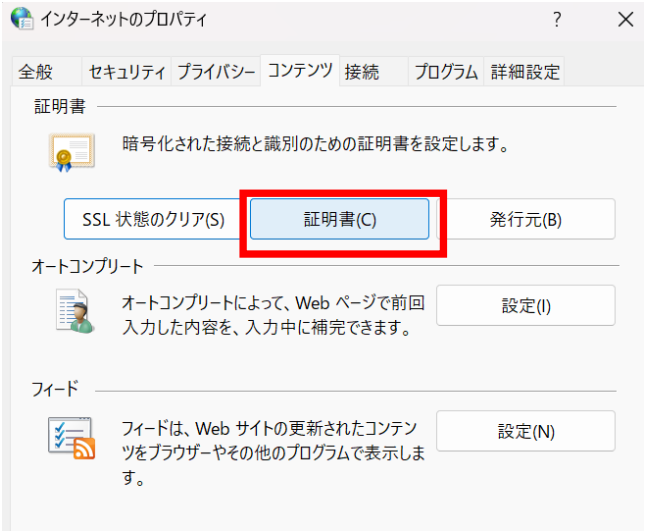


ステップ2：PCにローカル認証局の証明書をインポートする（１）

次に、ダウンロードした、証明書をWindows PCへ取り込みます。

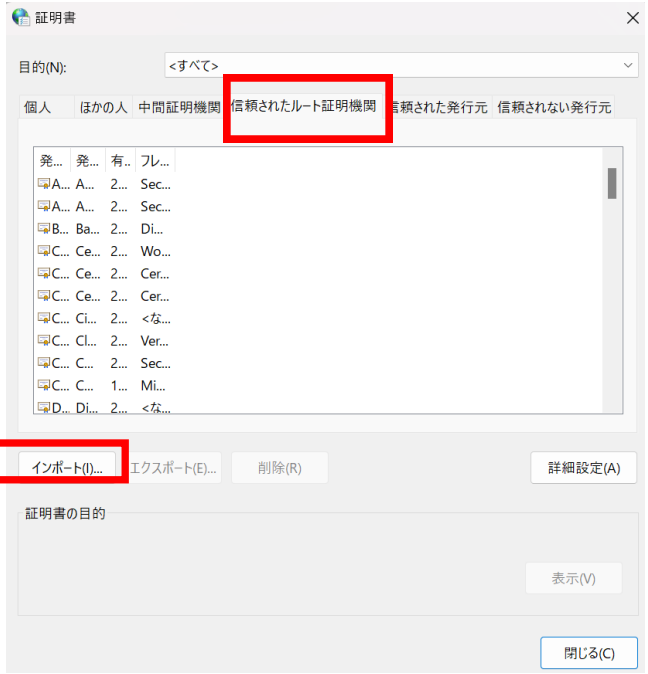
①Windowsの「ネットワークとインターネット」の中にある、インターネットオプションを選択

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）

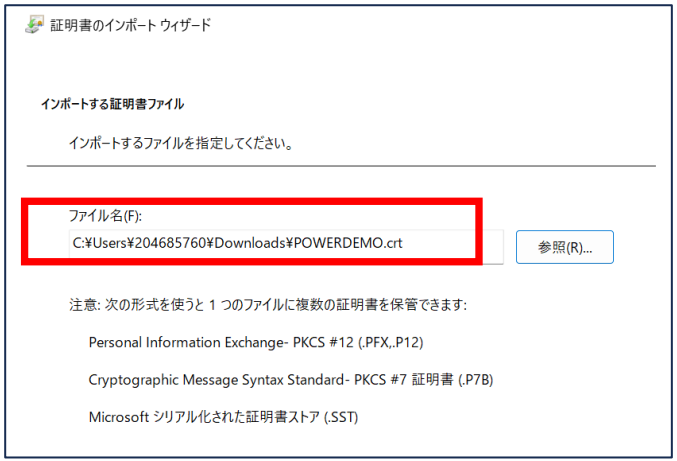
③「信頼されたルート証明機関」で、
インポートを選択。



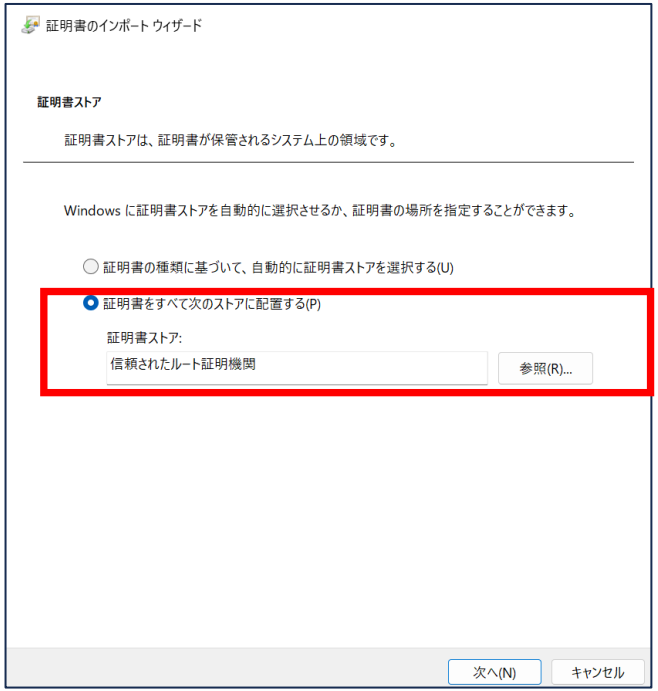
④証明書のインポートウィザードが起動するので
次へをクリック

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

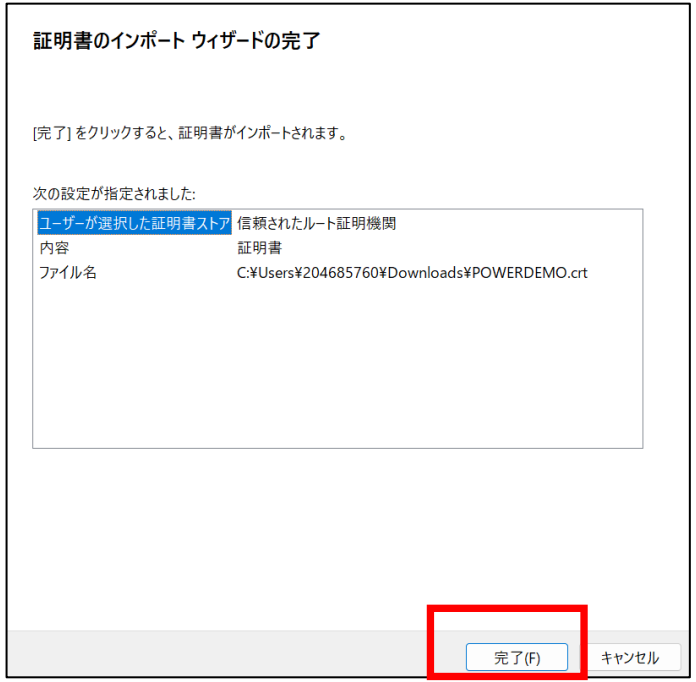


⑥下記のように証明書ストアに、信頼されたルート証明機関であることを確認して、次へを選択



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）

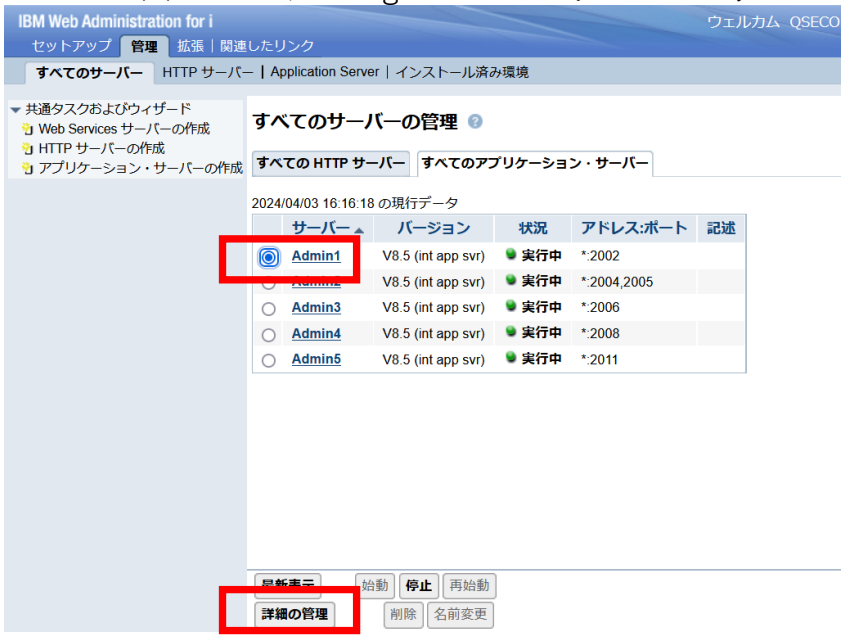
次に、Navigator for iをTLS通信で起動するための設定を実施します。

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）

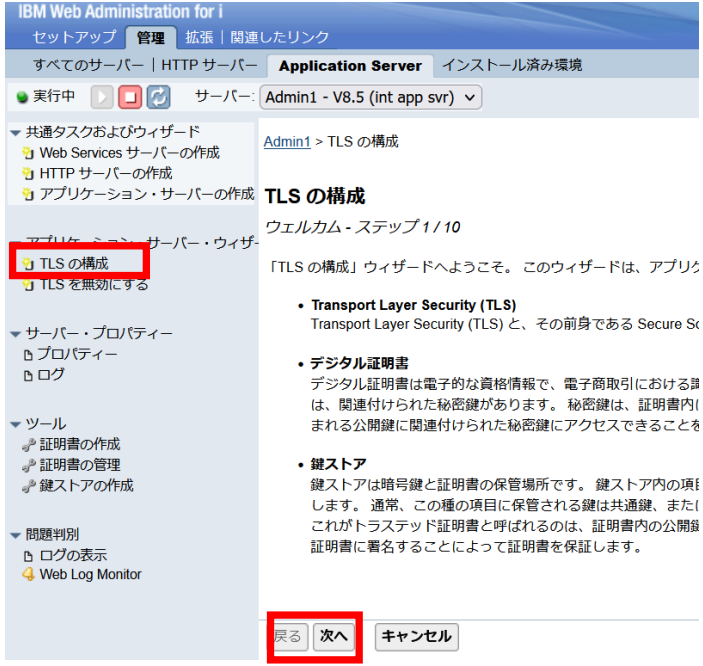
②「管理」タブのサーバー：Admin1を選択して
「詳細の管理」を選択

※Admin1はNavigator for i のサーバーです

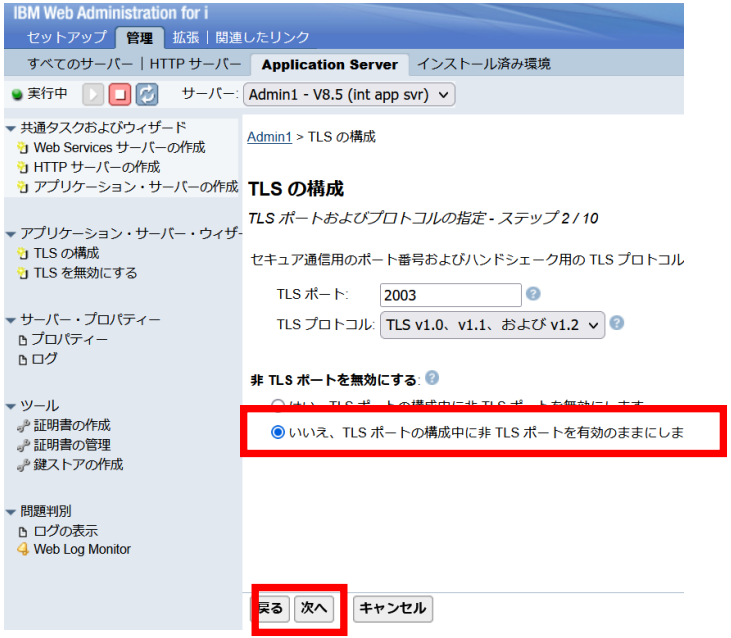


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（２）

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

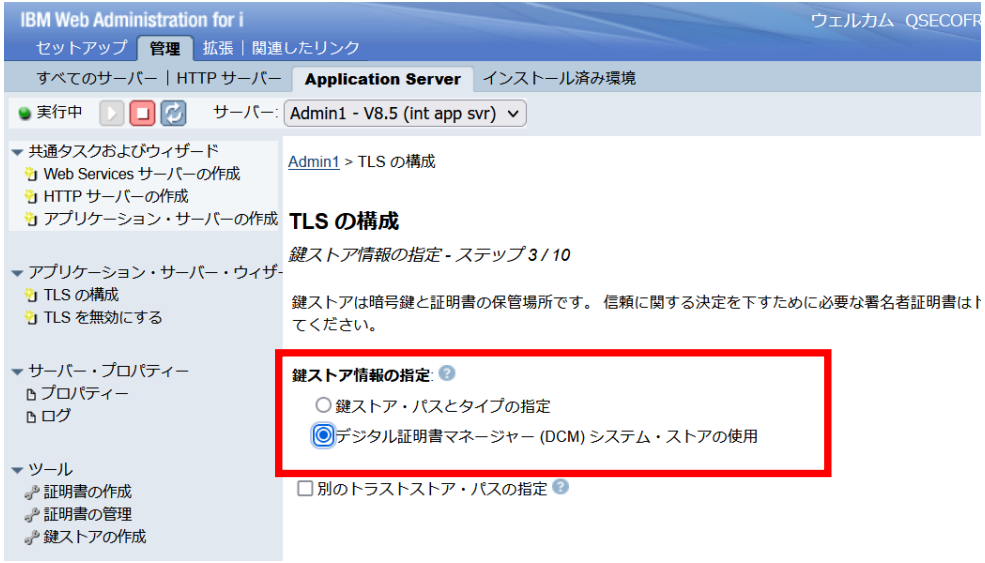


④非TLSサポートを無効にする　の項目で、
「いいえ」にチェックを入れ、「次へ」をクリッ
*http接続が全くできなくなってしまうため
「いいえ」で設定すること

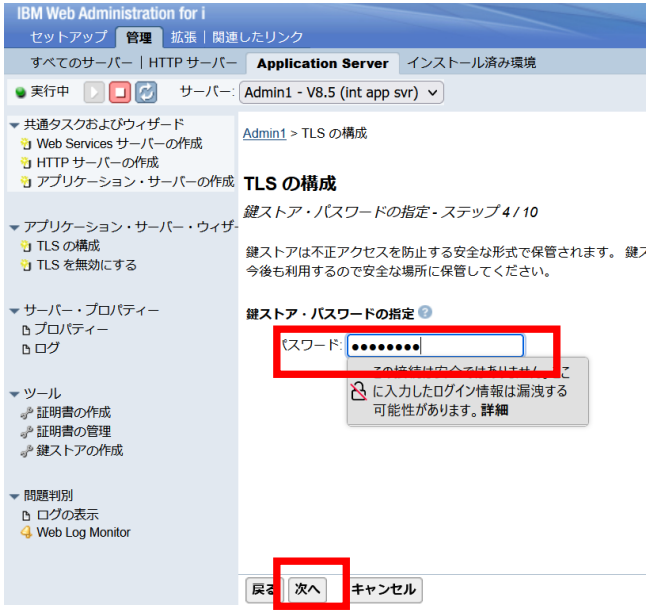


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（３）

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

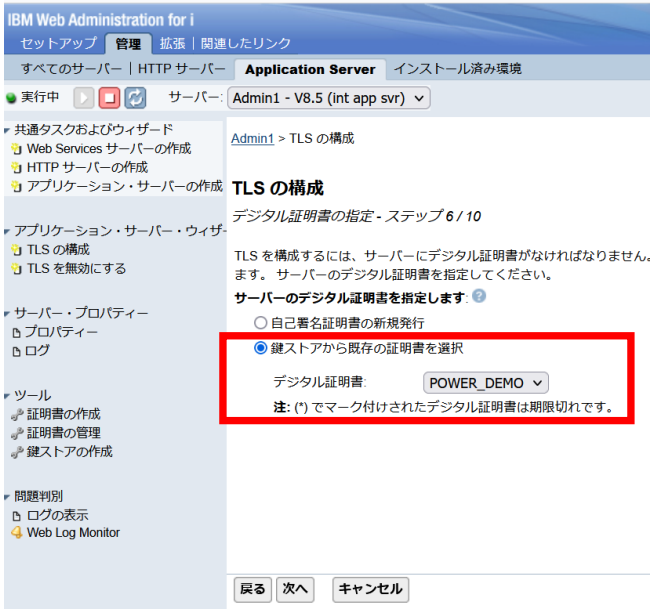


⑥ *SYSTEMストアのパスワードを入力し、
「次へ」をクリック

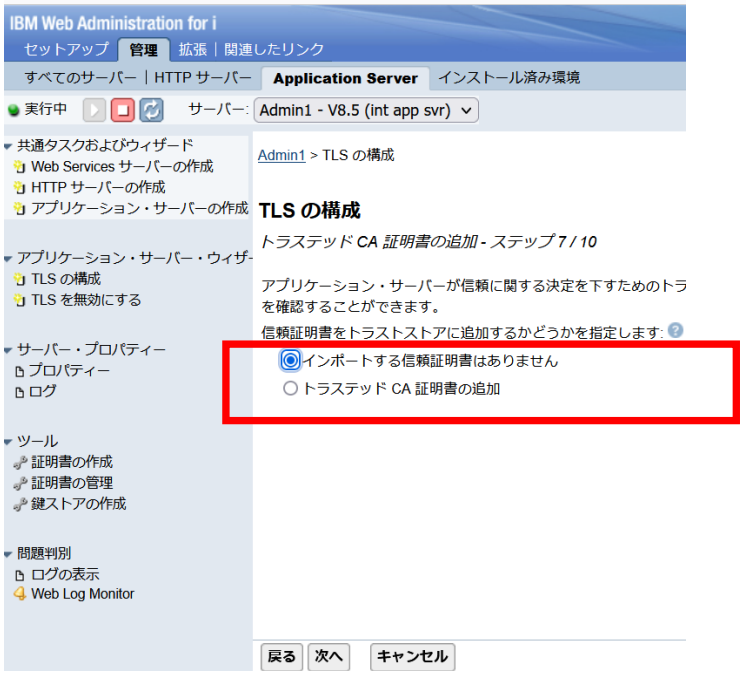


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（４）

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

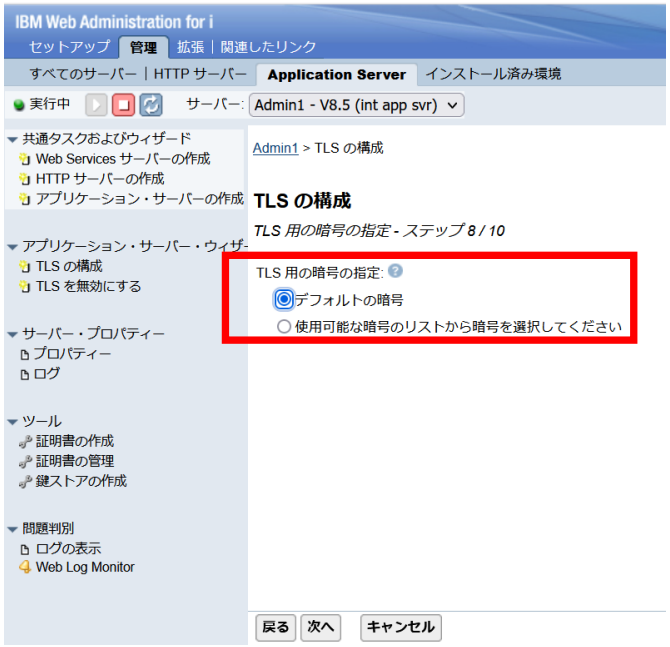


⑧「インポートする証明書はありません」に
チェックを入れ、「次へ」をクリック

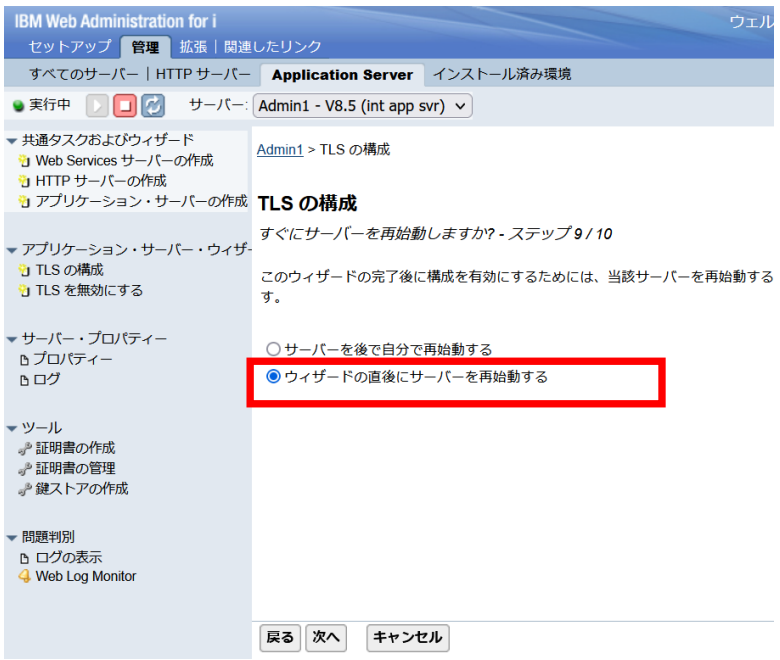


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（５）

⑨「デフォルトの暗号」にチェックを入れ、
「次へ」をクリック

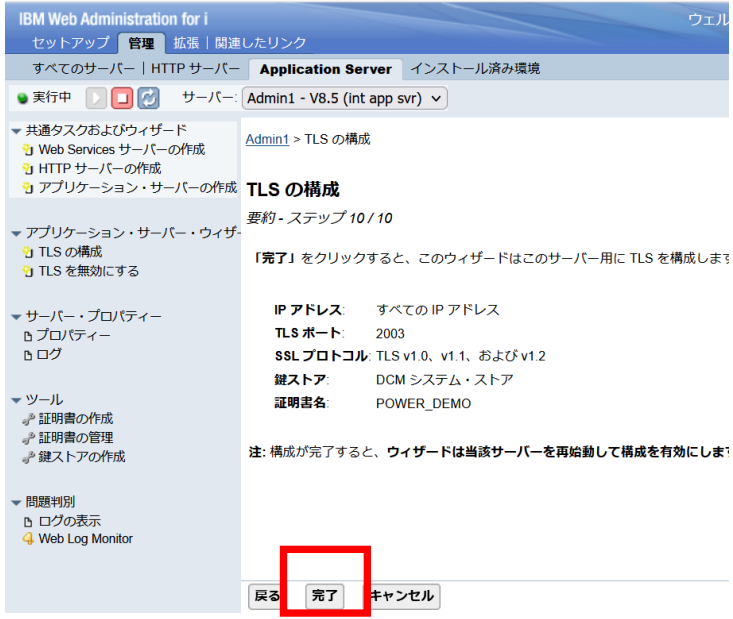


⑩「ウィザードの直後にサーバーを再始動する」に
チェックを入れ、「次へ」をクリック



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

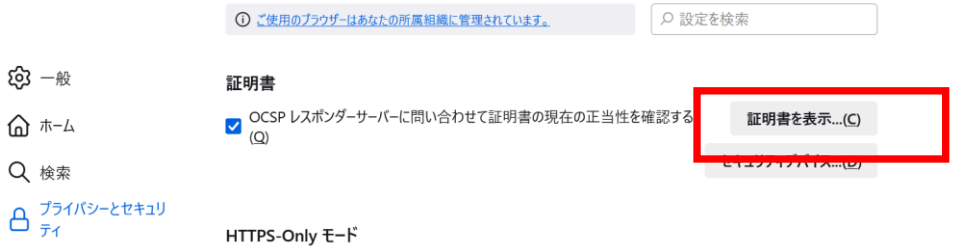
⑪下記の要約画面で「完了」をクリック
サーバーが実行中になるのを待つ



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。

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

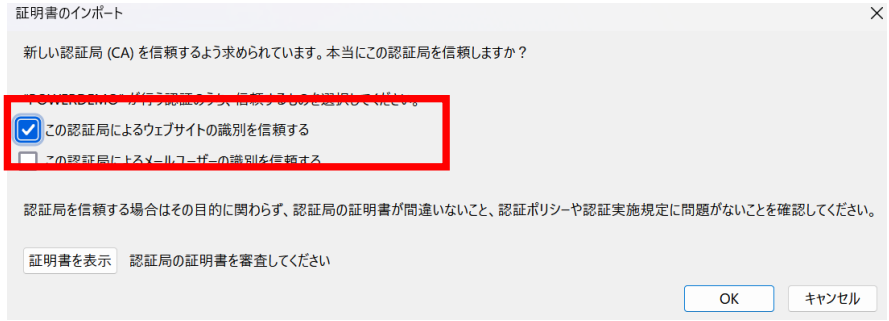
⑬「プライバシーとセキュリティ」を選択して、
「証明書を表示」を選択



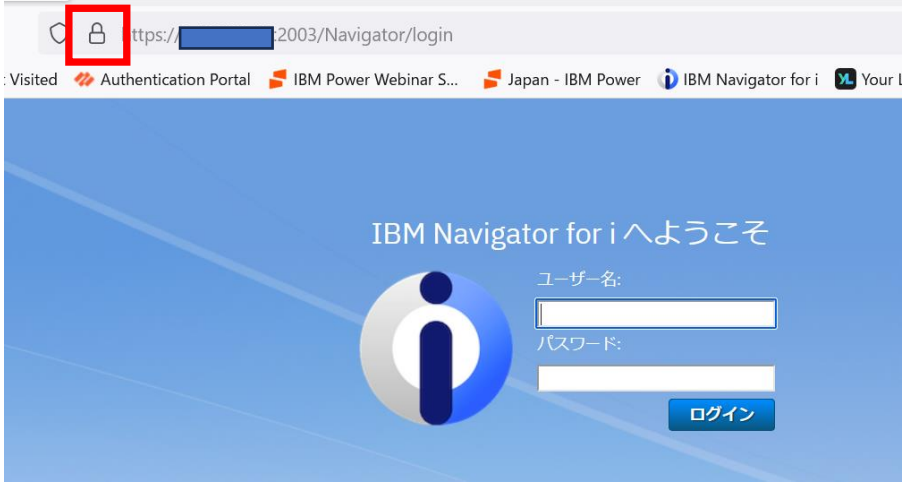
⑭下記の証明書マネジャーで、認証局証明書タブを選択してインポートをクリック

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

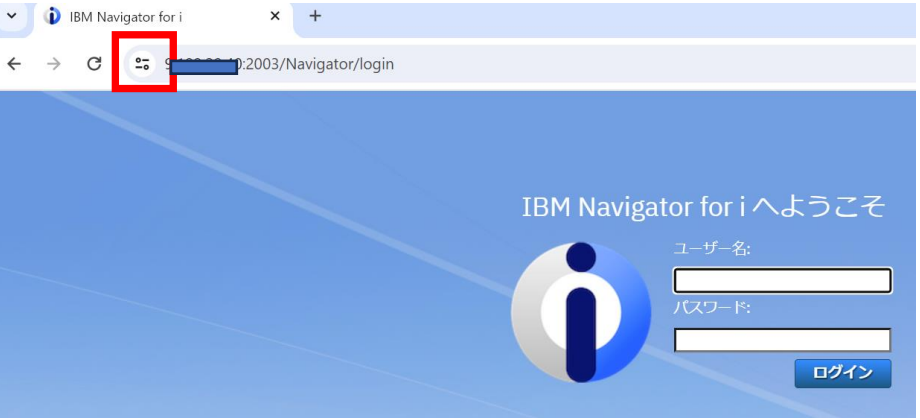


⑯以下にアクセスし、
　接続が保護されていることを確認する。
　https://XXX.XXX.XXX.XXX:2003/Navigator/login

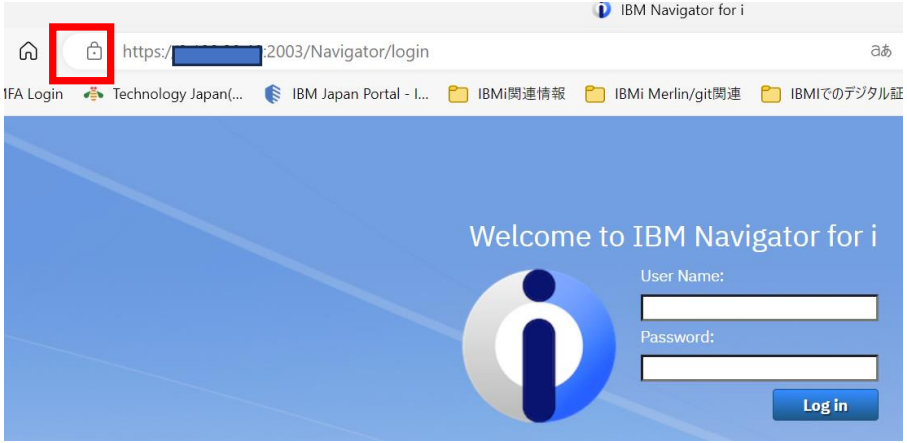


ステップ3： IBM Web Administration for i にてNavigator for i のTLS設定（９）

Chromeの場合は、ブラウザー側の設定なしで接続できました。



Edgeの場合も、ブラウザー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-lyer

2. IBM i 7.5マニュアル（ディ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-tlsssl

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-j

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/iseries.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/