FENICS II ユニバーサルコネクト アドバンス
メディカル VPN 接続サービス
デバイス証明書タイプ

Windows
利用者マニュアル

第 1.4 版

2023 年 3 月

富士通株式会社

改版履歴

版数	更新月	更新内容
1.0	2020/12	初版
1.1	2021/03	図 1.1-1、表 1.4-1 を更新
1.2	2022/07	第 3 章に注意事項（※）を追記、3.1.3 章を追加
1.3	2022/11	4.4 アンインストール手順 の一部内容を修正
1.4	2023/03	図 1.1 1 FENICS II ユニバーサルコネクト アドバンス メディカル VPN 接続サービス 概要 を更新 1.3 設定に必要な情報について で、ユーザ ID に関する情報を変更 1.4 動作環境、および、表 1.1-1 を更新 2.2 証明書の取り込み を更新 2.3.1 VPN 接続ツールのダウンロード ③ の補足内容を更新 3.1.2 接続手順 ② ③ の補足内容を更新 Windows 8.1 のサポート終了に伴い関連する記載を削除

はじめに

このたびは「FENICS II ユニバーサルコネクト アドバンス メディカル VPN 接続サービス(以下、本サービス)」をご契約いただき、ありがとうございます。この「FENICS II ユニバーサルコネクト アドバンス メディカル VPN 接続サービス Windows 利用者マニュアル(以下、本書)」は、本サービスをご利用になる上で必要な設定手順および使用手順を説明しています。

ご使用の前に本書をお読みいただき、正しくお使いください。お読みになった後は、いつでも見られるように大切にお手元に保管してください。

本書で記載する設定画面などは例であり、お客様がご利用の端末の画面とは異なる場合がありますのでご了承ください。

弊社では、工場出荷状態から基本ソフトウェアのバージョンアップを行った Windows 端末において、接続確認を実施しております。

【注意事項】
Windows 端末本体、接続されている周辺機器、使用するアプリケーションなど、お客様のご利用環境下での接続を保証するものではありません。
お客様のご利用環境下によっては、正常に接続できない(動作しない)場合があります。
弊社ではお客様の特定環境下に依存した問題については対応いたしかねますので、あらかじめご了承ください。

本書は、今後、サービス仕様の変更にあわせて、予告なく変更する場合があります。

目次

第1章 ご利用になる前に

1.1 FENICS II ユニバーサルコネクト メディカル VPN 接続サービスとは

「FENICS II ユニバーサルコネクト アドバンスメディカル VPN 接続サービス」とは、オンライン資格確認等サービス、オンライン請求システムに接続するためのインターネット VPN サービスです。VPN 接続のため VPN 接続用クライアントソフトウェア、機体を特定するデバイス証明書を予めインストールして利用します。

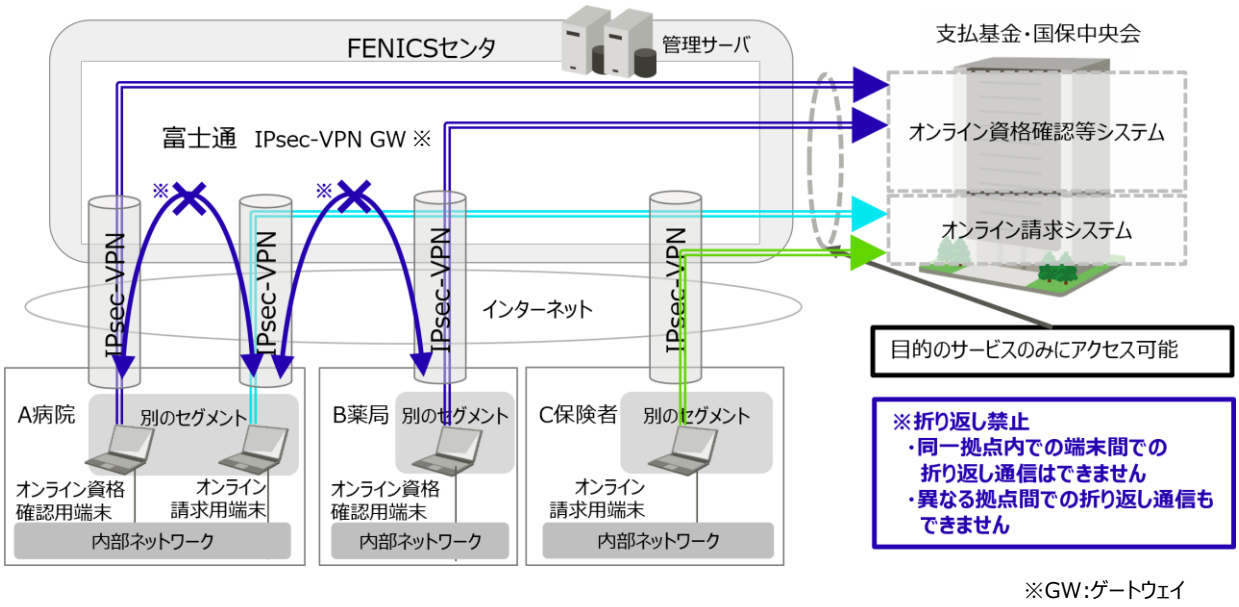

図 1.1-1 FENICS II ユニバーサルコネクト アドバンス メディカル VPN 接続サービス 概要

1.2 サポートデスクについて

本サービス専用のサポートデスクを用意しています。問題発生時に、お問い合わせください。

※ お客様で購入された Windows 端末については、購入時にご契約された窓口などへお問い合わせください。

1.3 設定に必要な情報について

本サービスを利用するには以下の情報が必要です。これらの情報は、開通通知書にてご案内いたします。開通通知書は大切保管してください。

- ユーザポータル URL (デバイス証明書と VPN 接続ツールをダウンロードする URL)
- ユーザ ID：xxxxxxxx@yyy.fenics2 (ユーザポータルにログインするための ID)
- パスワード：AbC1d2E3 (ランダムな文字列) (初期パスワード)
  ※ ユーザポータルにログインしてパスワードを変更してください。変更後のパスワードは大切に保管してください。ユーザポータルにログインする際に使用します。
- 証明書 ID、ダウンロード期限 (デバイス証明書の ID とダウンロードの期限)
- 解凍パスワー ド (ダウンロードした VPN 接続ツールを解凍するためのパスワード)

1.4 動作環境

本サービスのサポート端末は以下の通りです。尚、本項目の記載にかかわらず、OS ベンダのサポートが終了したバージョン OS 搭載の端末は、本サービスにおけるサポートの対象外となります。

表 1.4-1

用途	オンライン資格確認等システム/オンライン請求システム
サポート端末	Windows 10 IoT enterprise 2019 LTSC (64bit)
	Windows 10 Enterprise 2019 LTSC (64bit)
	Windows 10 (64bit)
	Windows 11 (64bit)

※ 搭載 OS の最新バージョンについては、弊社検証が完了後にサポートを開始いたします。

※ オンライン資格確認等システムでのご利用の場合は、厚生労働省 HP の「資格確認端末における満たすべき要件」をご確認ください。

第2章 準備

本サービスを Windows 端末でご利用いただくには、各種設定が必要です。本章では、設定の手順を説明します。本章の手順にて Windows 端末に設定される各種証明書および VPN 接続ツールは以下の通りです。

- 認証局デジタル証明書 (以下、認証局証明書)
- FENICS 認証局が発行するクライアント用デジタル証明 (以下、デバイス証明書)
  ※ 認証局証明書とデバイス証明書をあわせて「証明書」と言います。
- 接続に必要なソフトウェア (以下、VPN クライアントソフト)
- VPN クライアントソフトの動作に必要な設定ファイル(以下、VPN クライアントソフト用設定ファイル)
  ※ VPN クライアントソフトと VPN クライアントソフト用設定ファイルを合わせて「VPN 接続ツール」と呼びます。

2.1 ユーザポータルでのログインとログアウト

本項では、ユーザポータルでのログインとログアウトについて説明します。

2.1.1 初回ログイン

サービスご利用開始の際は、以下の手順で新たにパスワードを設定します。
※ 変更後のパスワードは、お客様にて大切に保管してください。

【初回ログイン時に必要な情報】

- サービスご利用開始の場合
  開通通知書に記載のある以下の情報が必要です。
  - ユーザポータル URL
  - ユーザ ID
  - パスワード

① ブラウザのアドレス入力欄にユーザポータルの URL を入力、「Enter」キーを押下しログイン画面を開きます。
ログイン画面で「ユーザ名」に開通通知書に記載のある「ユーザ ID」を、「パスワード」に開通通知書に記載のある「パスワード」を入力、「ログイン」ボタンをクリックし、「パスワード変更」画面を開きます。

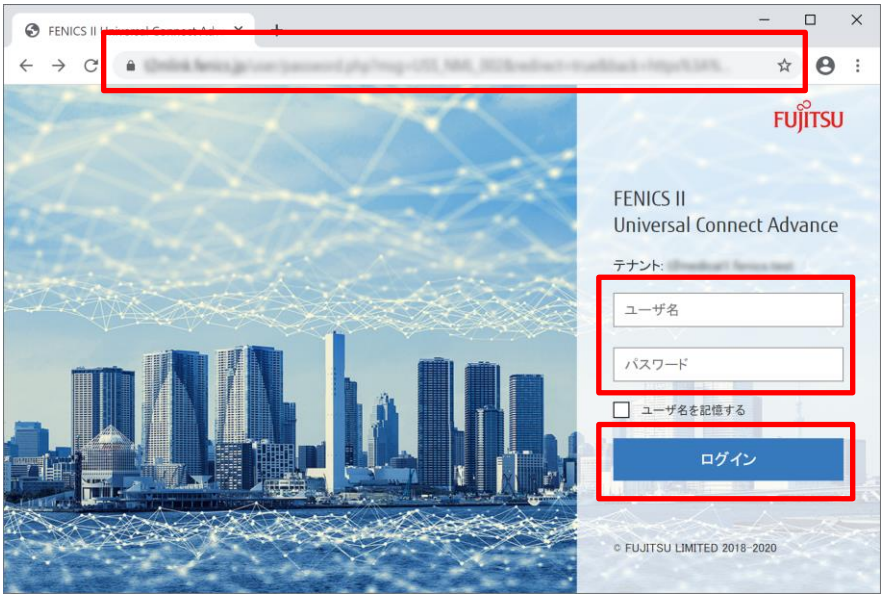

図 2.1-1

② 「パスワード変更」画面で、「新しいパスワードを入力」と「新しいパスワードを再度入力」に任意の新しいパスワード(同じパスワード)を入力し、「更新」ボタンをクリックします。

※ 新しく設定したパスワードはお客様にて大切に保管してください。

※ 更新ができない場合、「新しいパスワードを入力」と「新しいパスワードを再度入力」に入力したパスワードが異なっている可能性があります。再度お試しください。

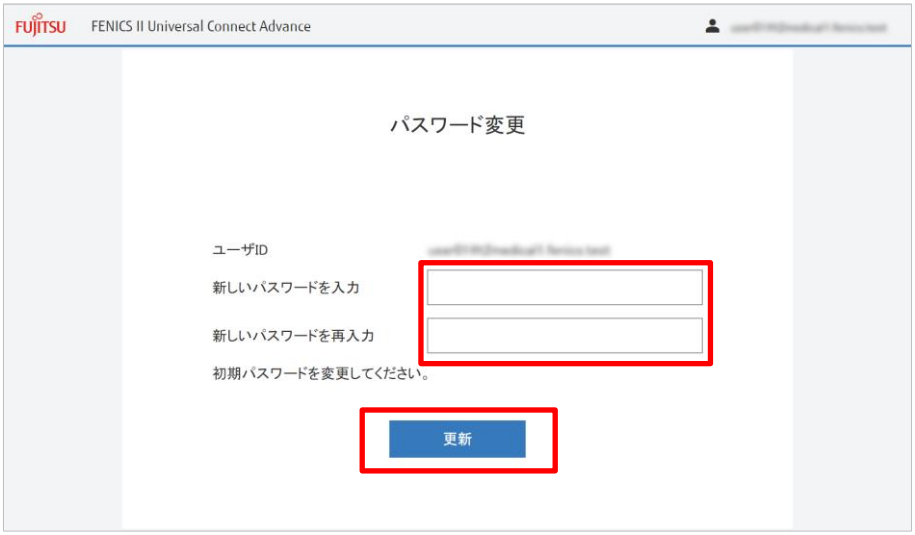

図 2.1-2

③ ユーザポータルへのログイン画面が再度表示されるので、「ユーザ名」に開通通知書に記載のある「ユーザ ID」を、「パスワード」に一つ前の手順で設定した新しいパスワードを入力、「ログイン」ボタンをクリックし、ユーザポータルの画面を開きます。

図 2.1-3

④ 各項目のタイルが表示されたユーザポータルの画面が表示され、ログインが完了です。

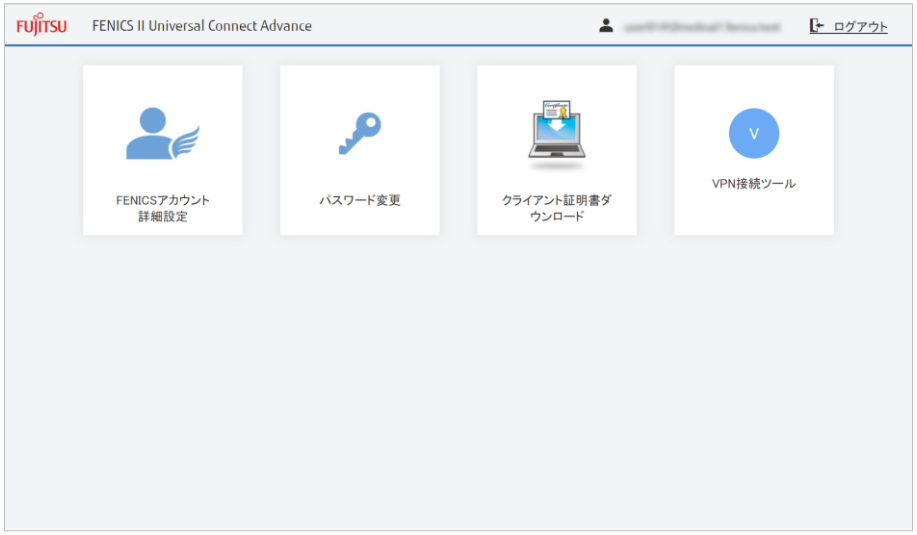

図 2.1-4

以上で、初回ログインは完了です。

2.1.2 ログイン

ユーザポータルにログインする手順は以下の通りです。

【通常のログイン時に必要な情報】

- 開通通知書に記載のある情報
  - ユーザポータル URL
  - ユーザ ID
- お客様にて保管している情報
  - 初回ログイン時に新しく設定したパスワード

① ブラウザのアドレス入力欄にユーザポータルの URL を入力、「Enter」キーを押下しログイン画面を開きます。ログイン画面の「ユーザ名」に開通通知書に記載のある「ユーザ ID」を、「パスワード」に初回ログイン時に新しく設定したパスワードを入力、「ログイン」ボタンをクリックします。

② 各項目のタイルが表示されたユーザポータルの画面が表示され、ログインが完了です。

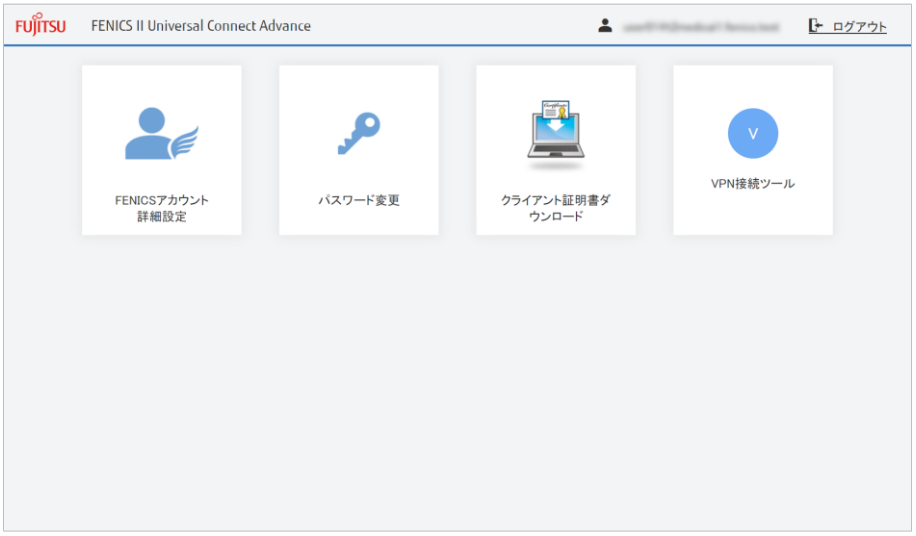

図 2.1-5

以上で、初回ログインは完了です。

2.1.3 ログアウト

ユーザポータルからログアウトする手順は以下の通りです。

① 「FENICS アカウント詳細設定」画面や、「デバイス証明書」画面を表示している際は、「閉じる」ボタンをクリクし、画面を閉じます。
② 各項目のタイルが表示されたユーザポータルの画面にて、「ログアウト」のボタンをクリックします。

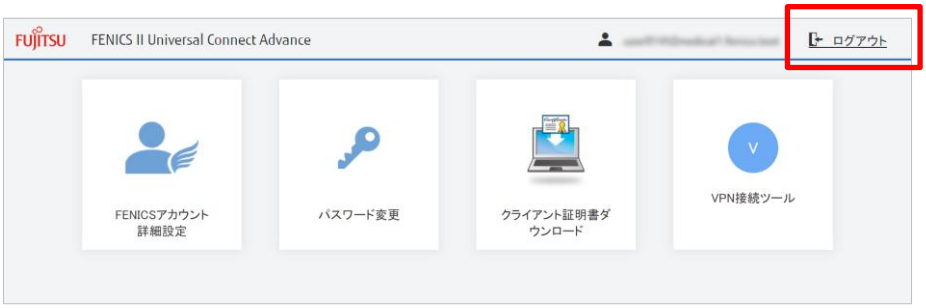

図 2.1-6

③ 「ログアウトしました。」と画面に表示されると、ログアウトの完了です。

図 2.1-7

以上で、ログアウトは完了です。

2.2 証明書の取り込み

本項では、デバイス証明書の Windows 端末への取り込み方法として、ユーザポータル画面からの証明書のダウンロードおよびインポートについて説明しています。

【留意事項】

- Windows10 IoT enterprise 2019 LTSC モデルをご使用の場合
  証明書の取り込みを実施する前に、UWF(統合書き込みフィルター)機能による C ドライブの保護が解除されていることをご確認ください。
  本サービスは C ドライブを保護した状態でご利用になれます。証明書、および、VPN 接続ツールの取り込みを実施後、VPN 接続が正常に実施できることをご確認いただき、C ドライブを保護した状態に設定してください。

2.2.1 証明書のダウンロード

① ブラウザにユーザポータルの URL を指定、ログイン画面で「ユーザ名」と「パスワード」を入力して「ログイン」ボタンをクリックし、ユーザポータル画面を表示します。

図 2.2-1

② ユーザポータル画面にて、「クライアント証明書ダウンロード」タイルをクリックし、「証明書ダウンロード」画面を表示します。

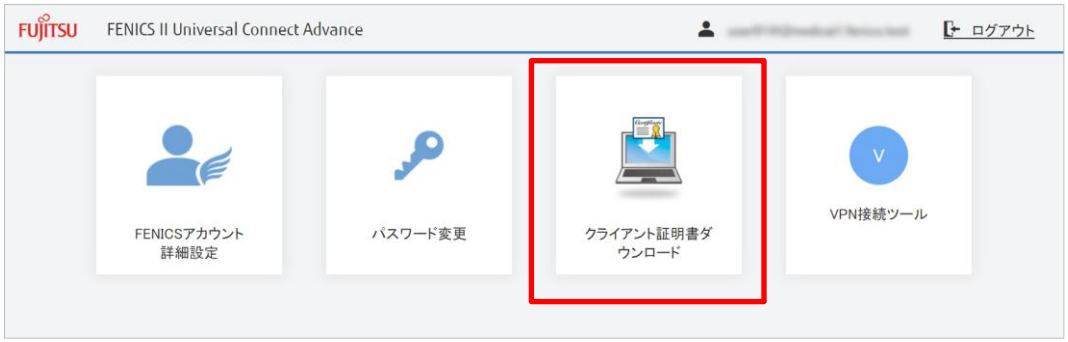

図 2.2-2

③ 「証明書ダウンロード」画面にて、開通通知書に記載のある証明書 ID であるか確認し、ダウンロード(DL にある▼)をクリックします。

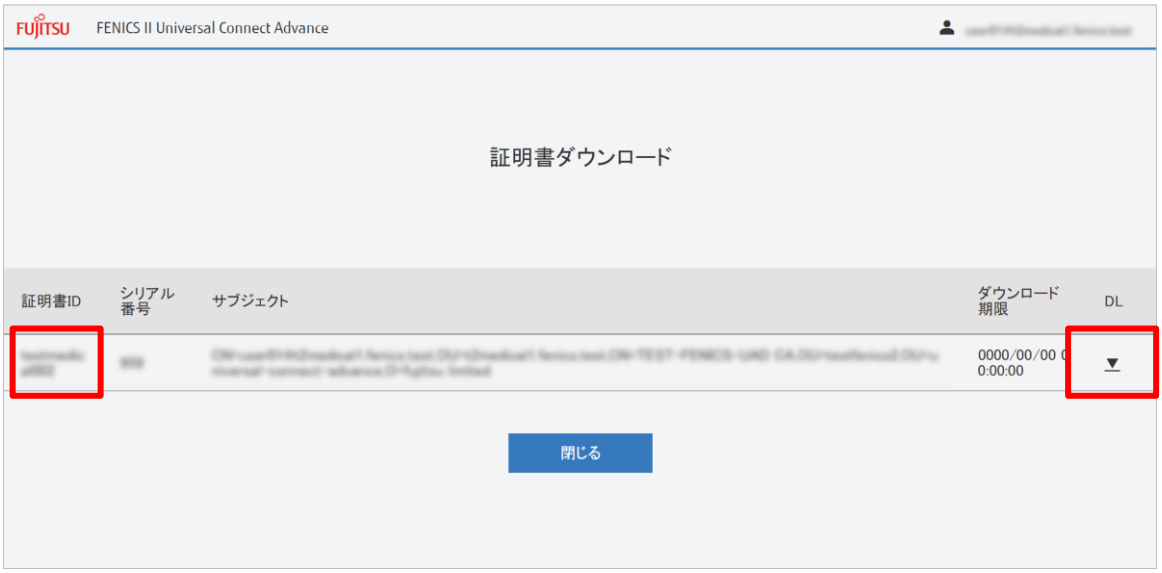

図 2.2-3

④ インポートパスワードが表示された「OK」ボタンをクリックします。

※ ここで表示されているパスワード(例)の「tiDeuGHBvIWd」は後ほど利用しますので、大文字小文字を区別して控えておいてください。

図 2.2-4

⑤ 証明書の保存を確認するダイアログが表示されるので「保存」ボタンをクリックします。

図 2.2-5

⑥ ダウンロード完了後、以下のダイアログが表示されるので「フォルダを開く」をクリックします。

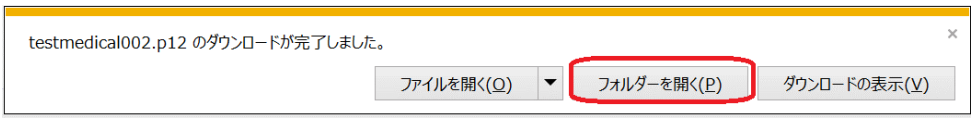

図 2.2-6

⑦ 端末のダウンロードフォルダーに証明書(ここでは testmedical002.p12)ファイルが格納されていることが確認できます。

図 2.2-7

以上で、証明書のダウンロードは完了です。つづけて 0 証明書のインポート の手順を実施ください。

2.2.2 証明書のインポート

① 2.2.1 証明書のダウンロード ⑦ でダウンロードを確認したデバイス証明書(ここではtestmedical002.p12)をダブルクリックし、「証明書のインポートウィザード」ウィンドウを表示します。

図 2.2-8

② 「証明書のインポートウィザードの開始」画面で「保存場所」を「現在のユーザー」に指定していること(黒い●で選択されていること)を確認し、「次へ」ボタンをクリックします。

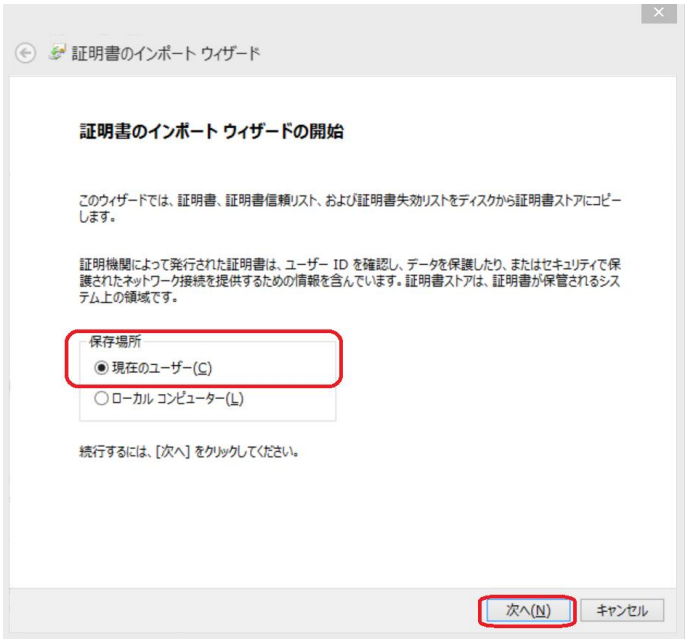

図 2.2-9

③ 「インポートする証明書ファイル」画面で「次へ」ボタンをクリックします。

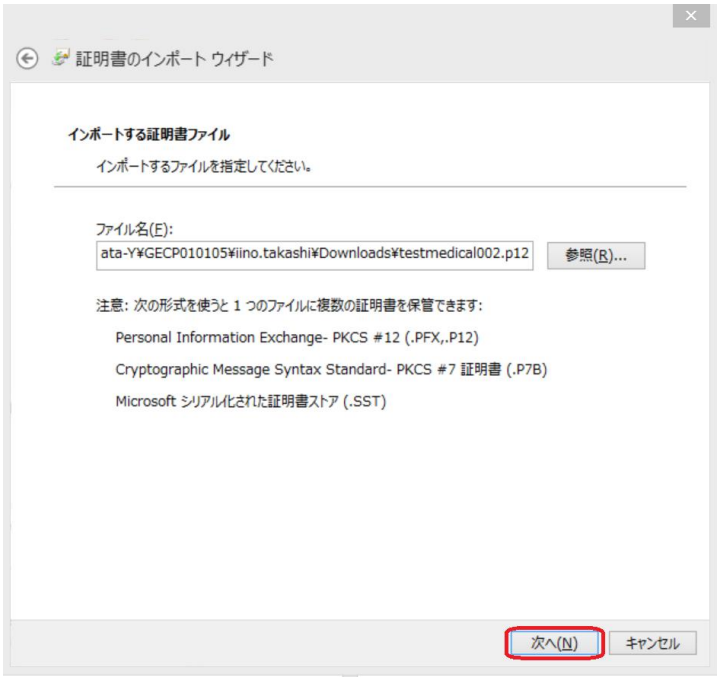

図 2.2-10

④ 「秘密キー保護」画面のパスワード欄に、2.2.1 証明書のダウンロード 0 で控えたインポートパスワードを入力し「次へ」ボタンをクリックします。
※ ここでは、「パスワードの表示」を選択して、パスワードを表示しております。

図 2.2-11

⑤ 「証明書ストア」画面で、「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」を指定していること(黒い●で選択されていること)を確認し、「次へ」ボタンをクリックします。

図 2.2-12

⑥ 「証明書のインポートウィザードの完了」画面で「完了」ボタンをクリックします。

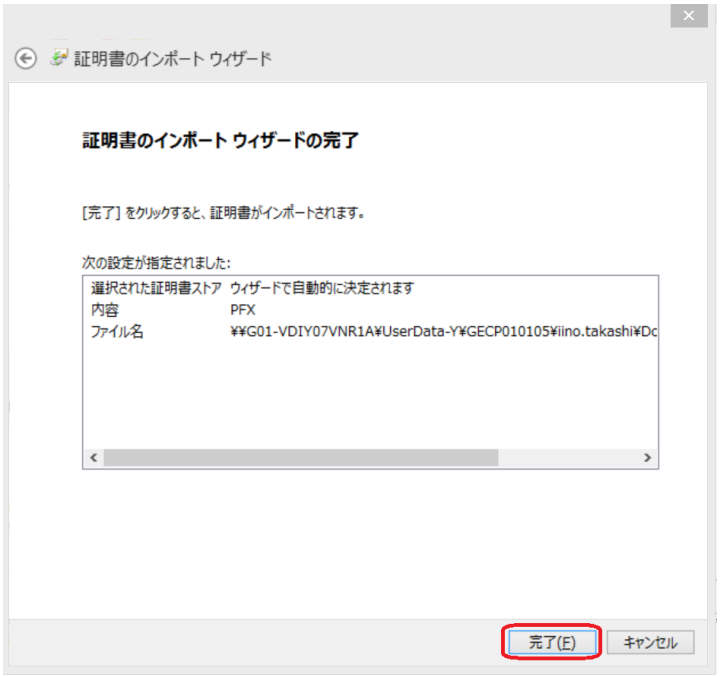

図 2.2-13

⑦ 「セキュリティ警告」画面で「はい」ボタンをクリックします。

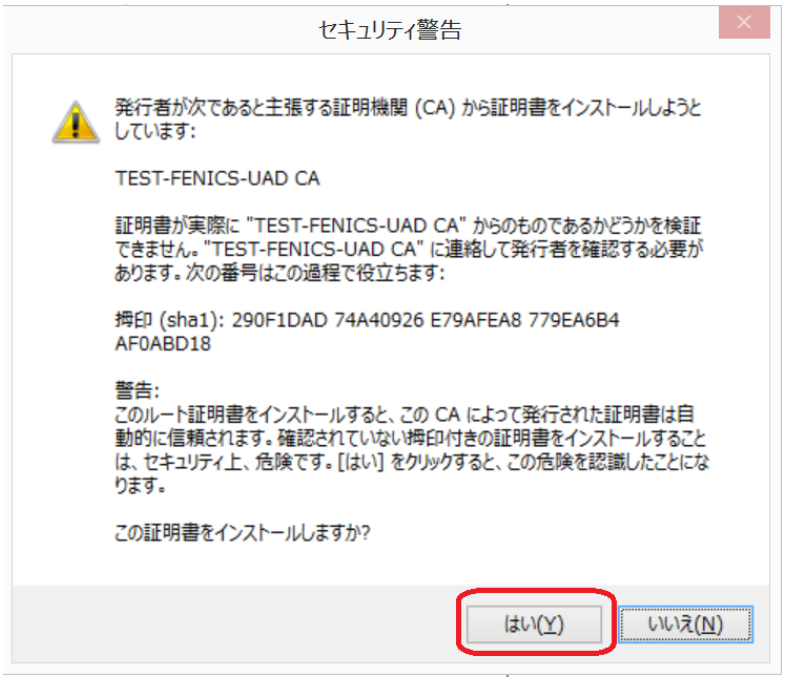

図 2.2-14

⑧ インポートが正しく完了した旨を表示するウィンドウで「はい」ボタンをクリックし、ウィンドウを閉じます。

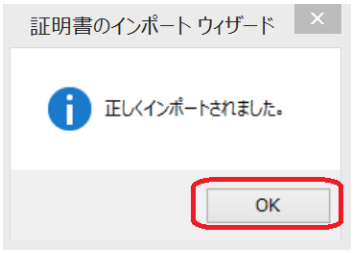

図 2.2-15

以上で、証明書のインポートは完了です。

2.3 VPN 接続ツールの取り込み

本項では、VPN 接続ツールの Windows 端末への取り込み方法として、ユーザポータル画面からの VPN 接続ツールのダウンロード、VPN クライアントソフトのインストールならびに VPN クライアントソフト用設定ファイルの配置について説明しています。

※ VPN 接続ツールとは、接続に必要なソフトウェア(VPN クライアントソフトと呼ぶ)と、VPN クライアントソフトの動作に必要な設定ファイル(VPN クライアントソフト用設定ファイルと呼ぶ)の二つからなります。

※ VPN 接続ツールのファイル名は「VPN_cli.zip」です。このファイルはパスワード保護されており、開通通知書にパスワード(解凍パスワード)が記載されています。

※ 本項の手順では、Chrome での操作画面を例としています。

【留意事項】

- 他社の VPN クライアントソフトウェアとの競合
  お客様の環境によっては、他社製の VPN クライアントソフトウェアがインストールされている場合があります。トラブルの原因になりますので、あらかじめ削除してください。
- ウイルス対策ソフト
  ウイルス対策ソフトの挙動により、VPN 接続がうまく出来ない場合があります。
- Windows10 IoT enterprise 2019 LTSC モデルをご使用の場合
  VPN 接続ツールの取り込みを実施する前に、UWF(統合書き込みフィルター)機能による C ドライブの保護が解除されていることをご確認ください。
  本サービスは C ドライブを保護した状態でご利用になれます。証明書、および、VPN 接続ツールの取り込みを実施後、VPN 接続が正常に実施できることをご確認いただき、C ドライブを保護した状態に設定してください。

2.3.1 VPN 接続ツールのダウンロード

① ブラウザにユーザポータルの URL を指定、ログイン画面で「ユーザ名」と「パスワード」を入力して「ログイン」ボタンをクリックし、ユーザポータル画面を表示します。すでに、デバイス証明書のダウンロードのため、ログインをしている場合は、次の画面をご覧ください。

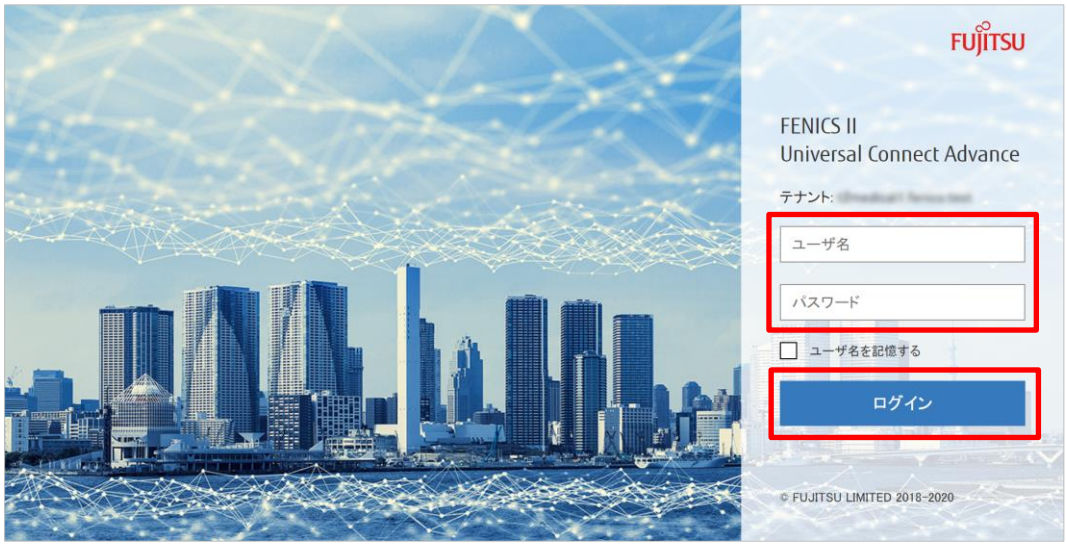

図 2.3-1

② ユーザポータル画面にて「VPN 接続ツール」ボタンをクリックします。

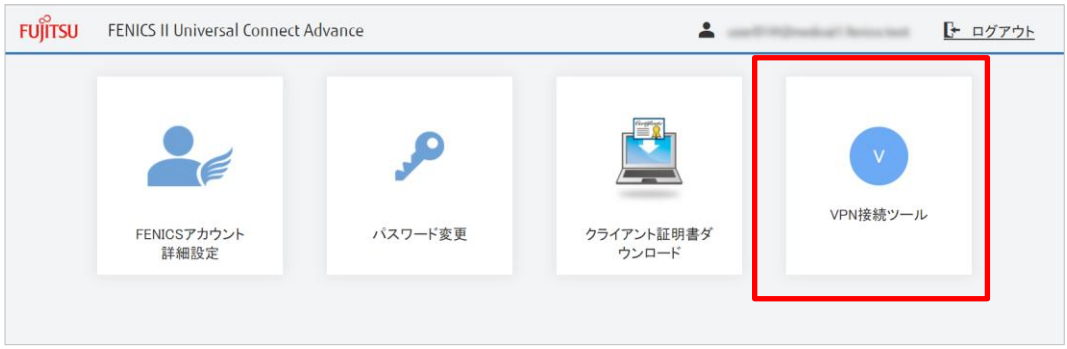

図 2.3-2

③ ダウンロード完了後、ファイルが「VPN_cli.zip」(VPN 接続ツール)であることを確認し、「ダウンロード」フォルダを開きます。

※ 「VPN_cli.zip」は、「VPNx_cli.zi(x は数字等)」となる場合があります(以下「「VPN_cli.zip」と称する)。

※ 「VPN_cli.zip」ファイルの保存先は、ご使用のブラウザや設定により異なります。本書では、「ダウンロード」フォルダを保存先の例としております。

※ ダウンロードの操作画面は、ご利用のブラウザによって異なります。ご利用のブラウザの画面遷移に従って操作してください。

④ 「ダウンロード」フォルダに「VPN_cli.zip」ファイルが格納されていることを確認し、ファイルをダブルクリックします。表示された「展開」タブの「すべて展開」をクリックします。

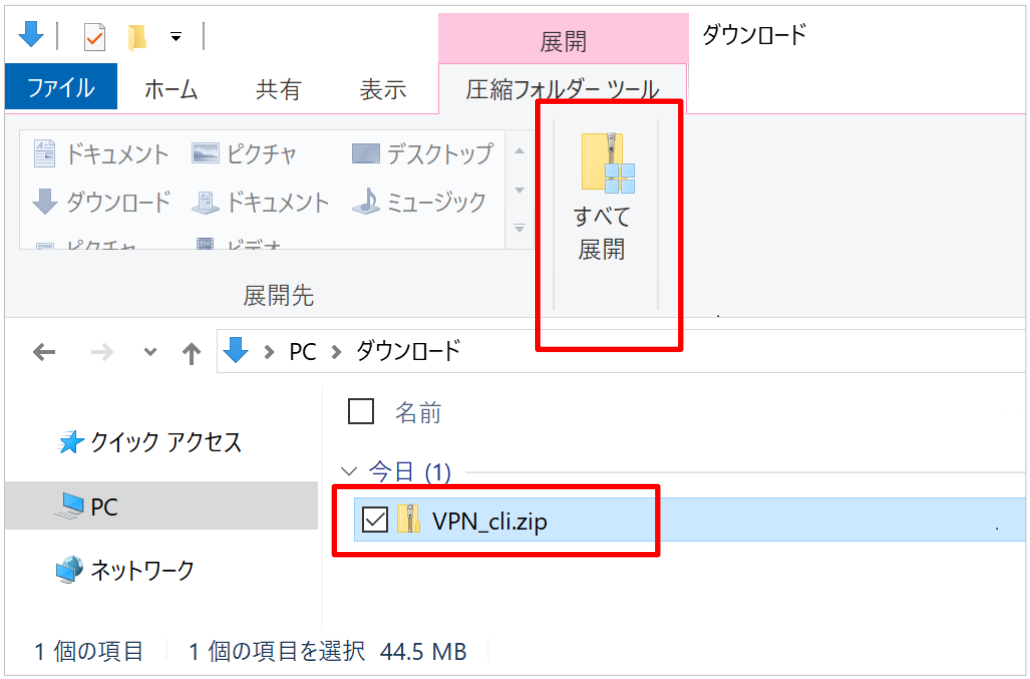

図 2.3-3

⑤ 表示された「圧縮(ZIP 形式)フォルダーの展開」画面で「展開」ボタンをクリックします。

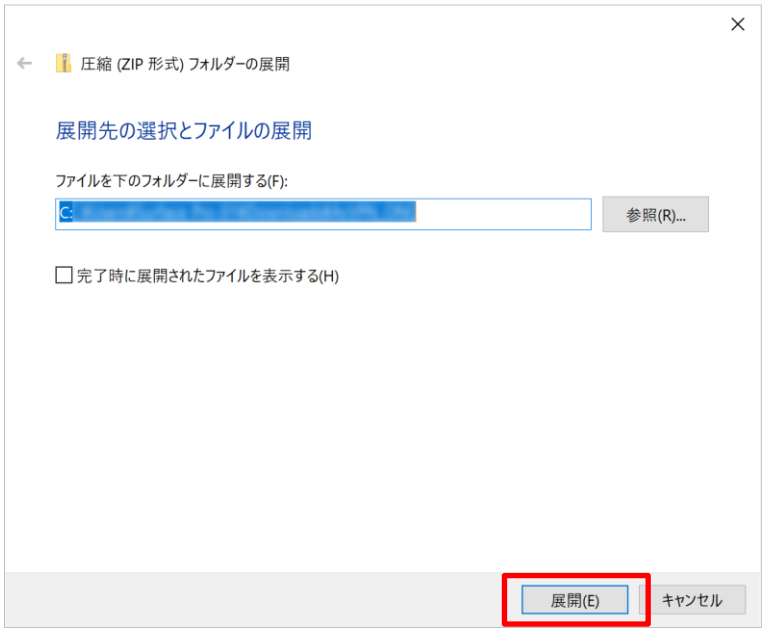

図 2.3-4

⑥ 表示された「パスワードの入力」画面でパスワード欄に開通通知書に記載のある解凍用パスワードを入力し、「OK」ボタンをクリックします。

※ アップデート等に対応するために VPN 接続ツールの再インストールを実施する際、①～⑤の手順により VPN 接続ツールをダウンロードすると、パスワードの入力無しで「VPN_cli.zip」ファイルが展開されることがあります。

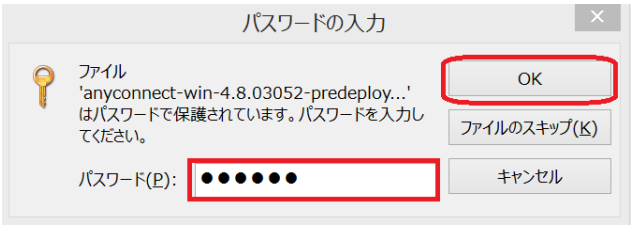

図 2.3-5

⑦ 端末の「ダウンロード」フォルダに「VPN_cli.zip」ファイルと並んで「VPN_cli」フォルダが格納されていることを確認します。

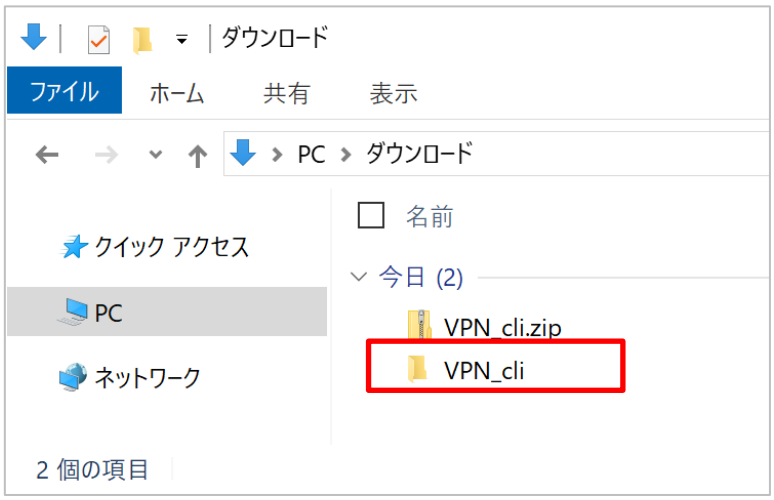

図 2.3-6

以上で、VPN 接続ツールのダウンロードは完了です。つづいて 2.3.2VPN クライアントソフトのインストール の手順を実施ください。

2.3.2 VPN クライアントソフトのインストール

① 2.3.1VPN 接続ツールのダウンロード ⑦で開いたフォルダの「VPN_cli」フォルダをクリックします。

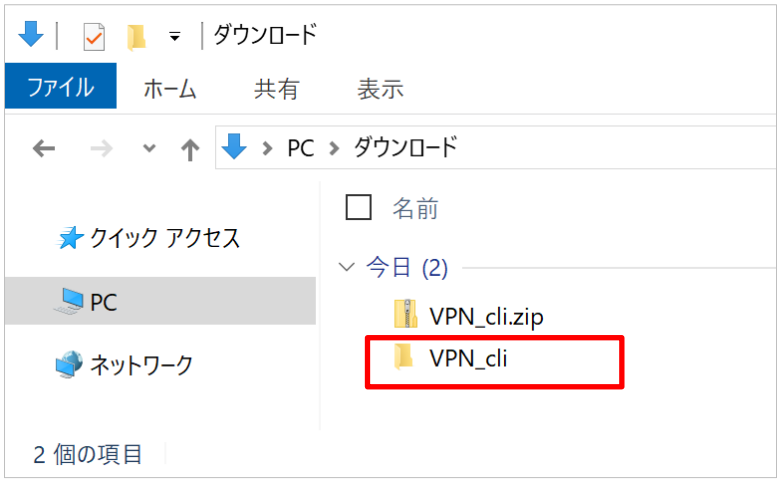

図 2.3-7

② フォルダ(下図例：「anyconnect-win-4.8.03052-predeploy-k9」)をクリックして開きます。

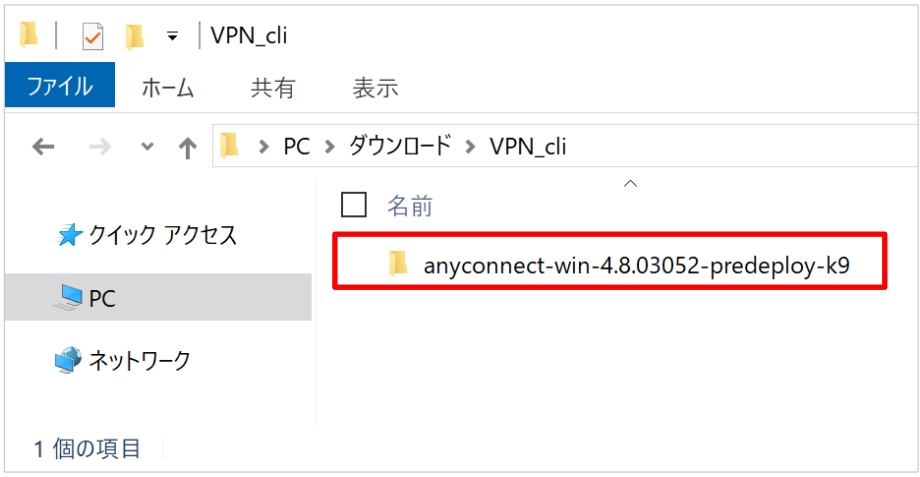

図 2.3-8

③ Setup.exe をダブルクリックで実行します。

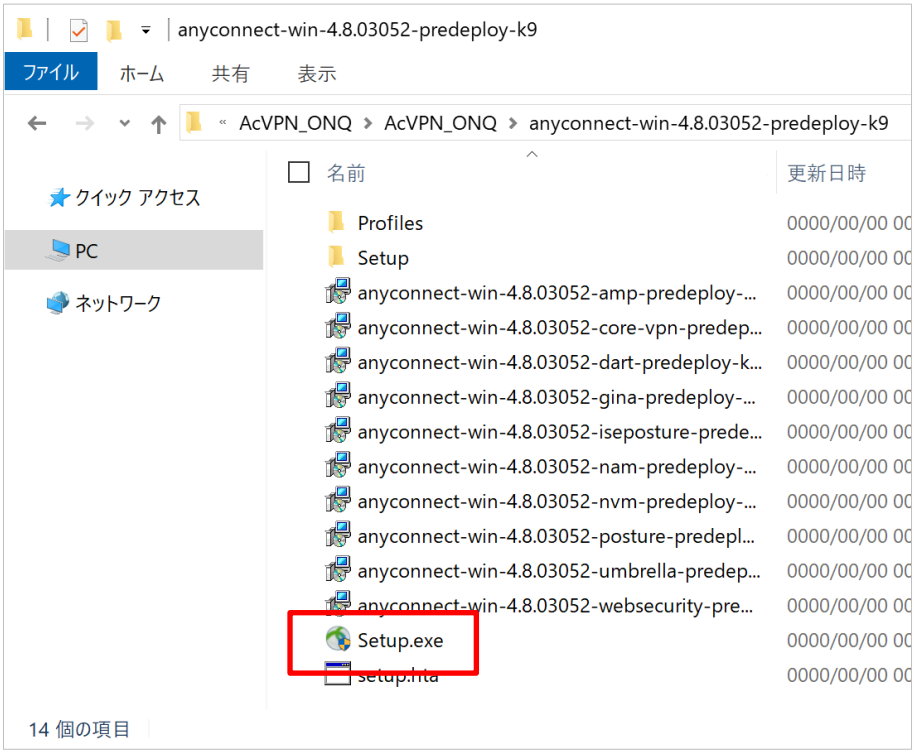

図 2.3-9

④ 「ユーザー アカウント制御」のダイアログ画面が表示される場合は、「はい」をクリックします。

図 2.3-10

⑤ 「Cisco AnyConnect Secure Mobility Client Setup A」のウィンドウにて、「Core & VPN」を選択し、「Install Sellected」ボタンをクリックします。

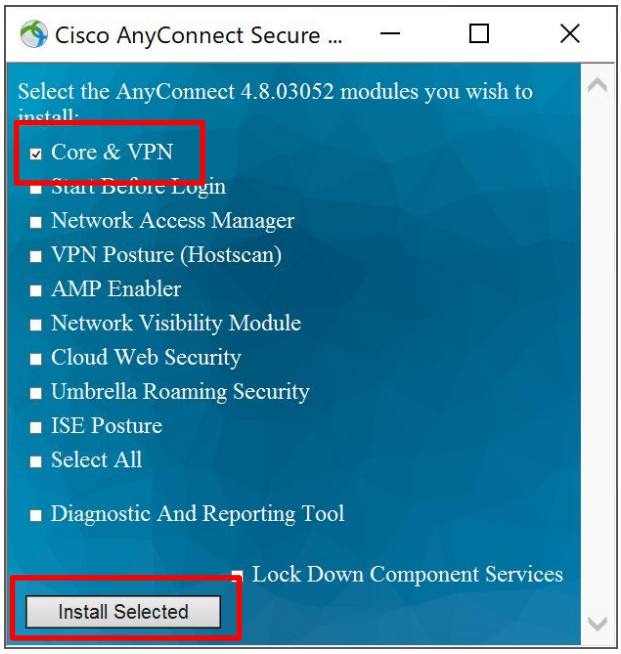

図 2.3-11

⑥ インストールの実行を確認する画面で「OK」をクリックします。

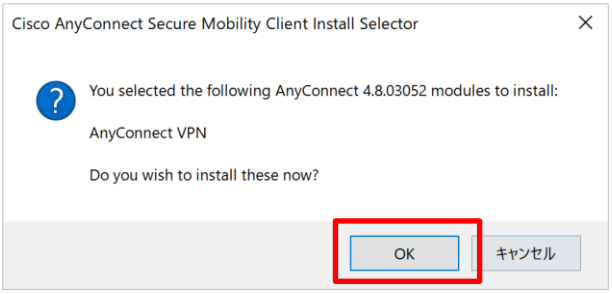

図 2.3-12

⑦ 「使用許諾」画面で「Accept」ボタンをクリックし、インストールを開始します。

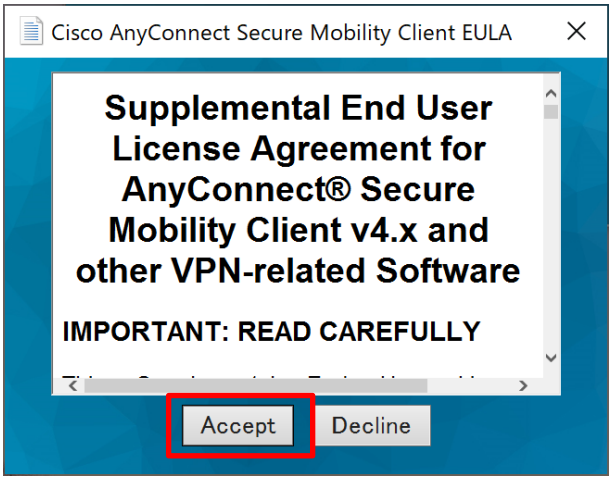

図 2.3-13

⑧ 「Installation Complete」と表示されると、インストールは完了です。「OK」ボタンをクリックし、ポップアップ画面を閉じます。

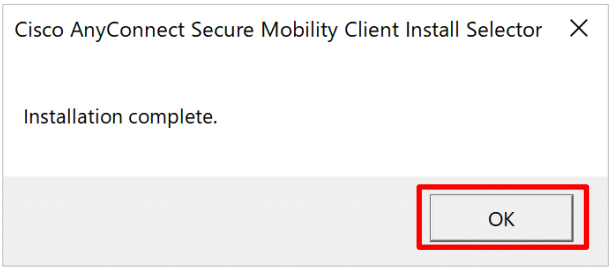

図 2.3-14

以上で、VPN クライアントソフトのインストールは完了です。

第3章 接続・切断(Disconnect)・再接続・終了(Quit)

本章では、接続・切断・再接続・終了について説明します。
以下の手順は、第 2 章に記載されている本サービスご利用に必要な設定をすべて終えていることを前提としています。

※ 本章は本サービスの接続・切断・再接続・終了について記載しています。接続後に、支払基金・国保中央会より提示された手順にてオンライン資格確認等システムのご利用となります。
※ 第 2 章での設定を一部のみ実施した場合、追加の設定を実施した場合は、本章での接続方法では接続できない場合があります。ご注意ください。

3.1 接続

3.1.1 Windows の事前設定の確認

通信が有効になっている(通信が行われている)ことを確認します。
確認方法、および、設定方法は、ご利用端末の取り扱い説明書をご確認ください。

3.1.2 接続手順

① 画面左下の Windows スタートボタンをクリックし、表示されるアプリケーション一覧から「Cisco」フォルダ->「Cisco AnyConnect Secure Moility Client」をクリックします。

図 3.1-1

② 「Cisco AnyConnect Secure Moility Client」ウィンドウのプルダウンで「medical_onq」が選択されていることを確認し、「Connect」ボタンをクリックします。
※ 「medical_onq」は、「medx_onq(x は数字等)」となる場合があります(以下「medical_onq」と称する)。

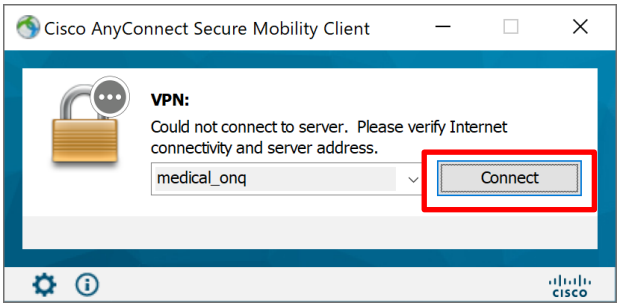

図 3.1-2

③ 新たに表示されたウィンドウで「Username」および「Password」を入力し、「OK」ボタンをクリックします。

- Username：ユーザ ID@yyy.fenics2 (開通通知書のユーザ ID に@～を追加)
- Password：パスワード (パスワード変更後のパスワード)

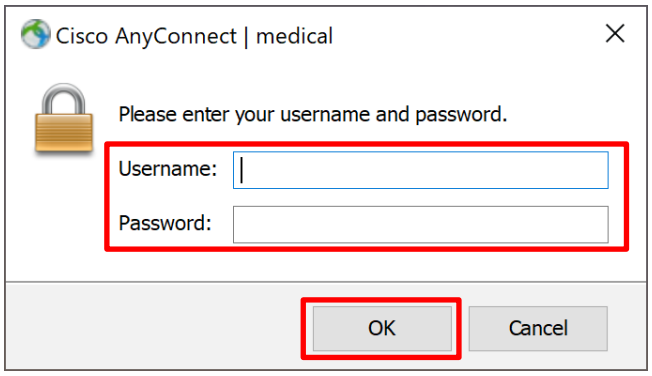

図 3.1-3

④ 正常に接続されると、その旨が接続通知として画面に表示されます(デフォルト設定)。

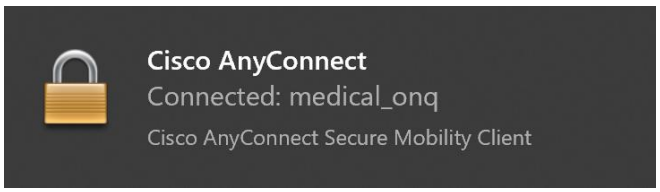

図 3.1-4

※ 本サービスのクライアントインストール後初めて接続する際、または、クライアントを終了(Quit)後再度接続する際は、Username および Password を入力するウィンドウがクライアントのウィンドウと同時に立ち上がります。

以上で、本サービスの接続は完了です。

3.1.3 オンライン資格確認等システムへの接続について

本サービスの接続後に、支払基金・国保中央会より提示された手順にてオンライン資格確認等システムをご利用ください。

3.2 切断 (Disconnect)

3.2.1 クライアントウィンドウからの切断手順

① 通知領域の「隠れているインジケーターを表示します」矢印をクリックし、本サービスのインジケーター(下図参照)をクリックし、「Cisco AnyConnect Secure Moility Client」ウィンドウを開きます。

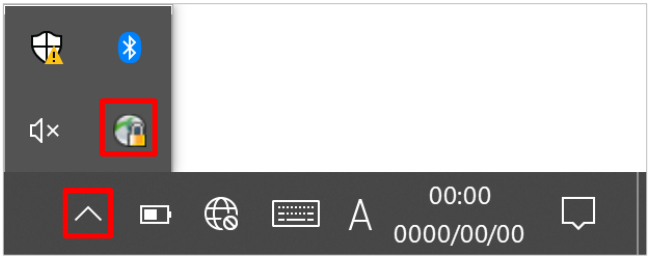

図 3.2-1

② 「Cisco AnyConnect Secure Moility Client」ウィンドウで「Disconnect」ボタンをクリックし、VPN 接続を切断します。

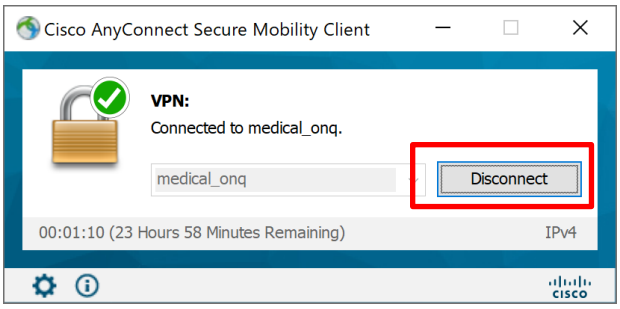

図 3.2-2

③ 右上の閉じる(X)ボタンをクリックし、ウィンドウを閉じます。

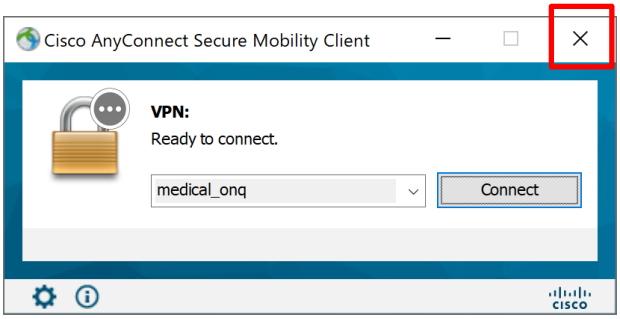

図 3.2-3

以上で、クライアントウィンドウからの切断手順は完了です。

3.2.2 通知領域のインジケーターからの切断手順

① 通知領域の「隠れているインジケーターを表示します」矢印をクリックします。

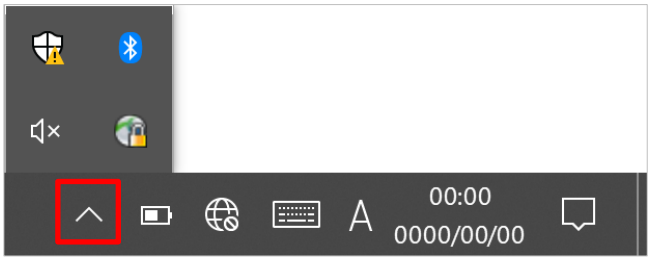

図 3.2-4

② 本サービスのインジケーター(下図参照)を右クリック、「VPN」の「Disconnect」をクリックし、VPN 接続を切断します。

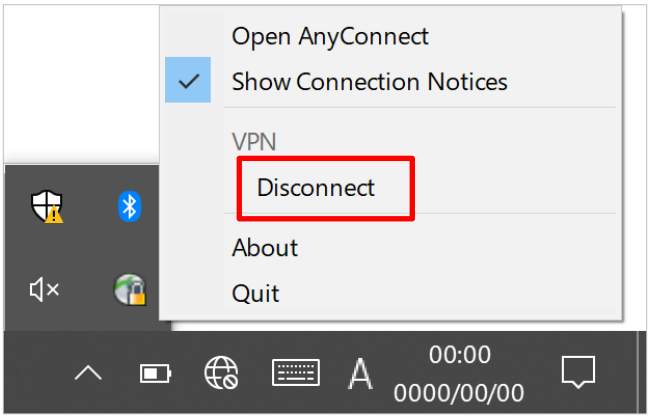

図 3.2-5

以上で、通知領域のインジケーターからの切断手順は完了です。

3.3 再接続

3.3.1 前提条件

VPN 接続を切断(Disconnect)後、再接続する際にご利用になれます。
本サービスのクライアントインストール後初めて接続する際、または、クライアントを終了(Quit)後再度接続する際は、通知領域に本サービスのインジケーターは表示されません。

3.3.2 再接続手順

① 通知領域の「隠れているインジケーターを表示します」矢印をクリックします。

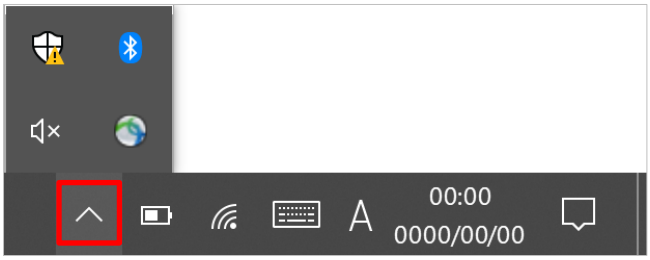

図 3.3-1

② 本サービスのインジケーター(下図参照)をクリックし、「Cisco AnyConnect Secure Moility Client」ウィンドウを開きます。

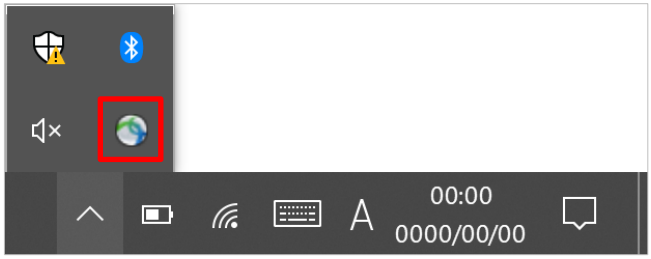

図 3.3-2

または、インジケーターを右クリックし、「VPN」の「Connect」をクリックします。

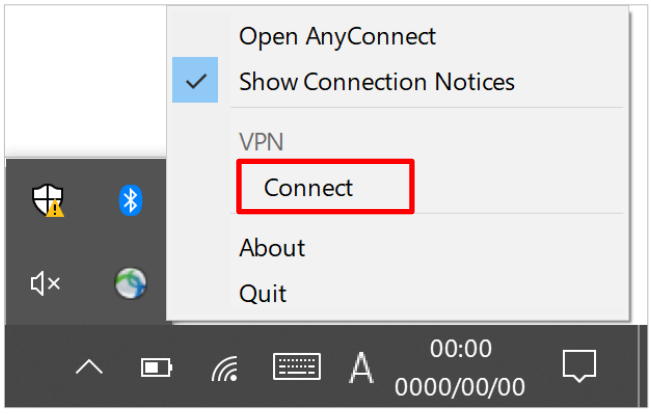

図 3.3-3

③ 「Cisco Anyconnect | medical_onq」ウィンドウで、「Password」を入力し、「OK」ボタンをクリックします。

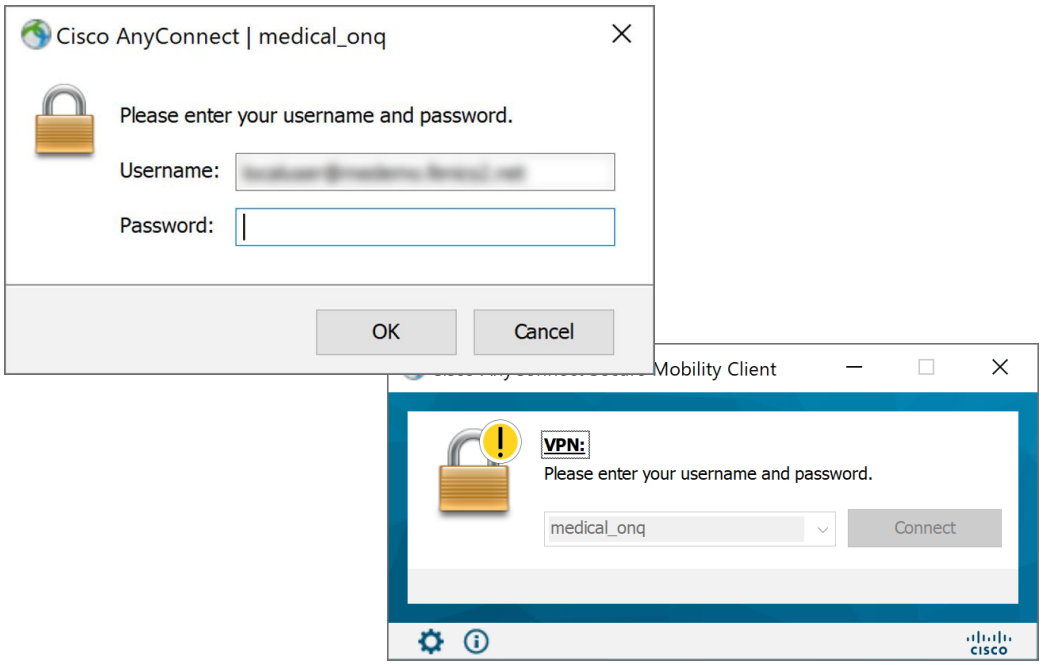

図 3.3-4

④ 正常に接続されると、その旨が接続通知として画面に表示されます(デフォルト設定)。

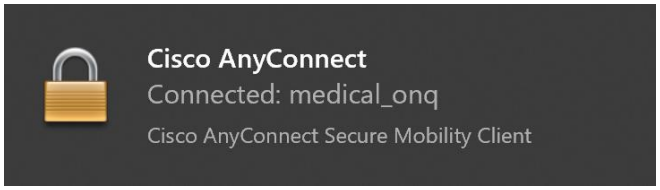

図 3.3-5

以上で、再接続手順は完了です。

3.4 終了 (Quit)

3.4.1 終了手順

※ 本項の操作を実施すると、通知領域から本サービスのインジケーターの表示が消えます。
※ インジケーターは本サービスの VPN 接続を実行すると再度表示されます。

① 通知領域の「隠れているインジケーターを表示します」矢印をクリックします。

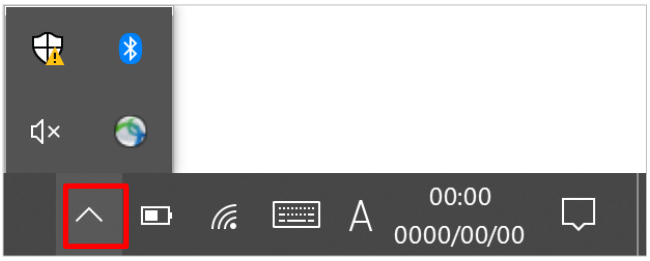

図 3.4-1

② 本サービスのインジケーター(下図参照)を右クリック、「Quit」をクリックし、本サービスのクライアントを終了します。

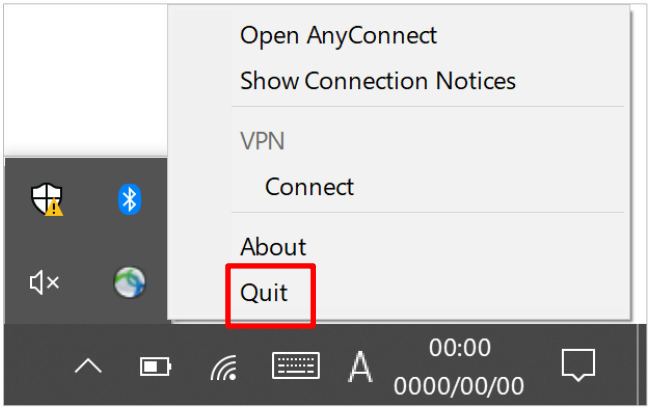

図 3.4-2

以上で終了手順は完了です。

第4章 その他

4.1 シリアル番号の確認

① ご使用の Windows 端末でコントロールパネルを開き、「ネットワークとインターネット」をクリックします。

図 4.1-1

② 「インターネットオプション」をクリックし「インターネットのプロパティ」ウィンドウを開きます。

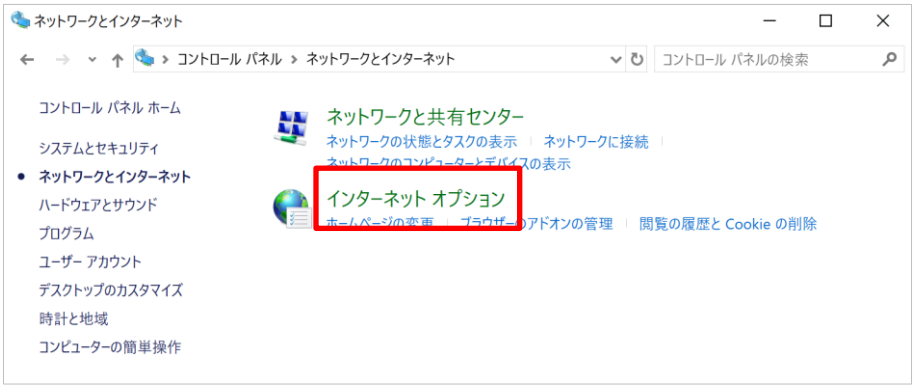

図 4.1-2

③ 「コンテンツ」タブの「証明書」ボタンをクリックします。

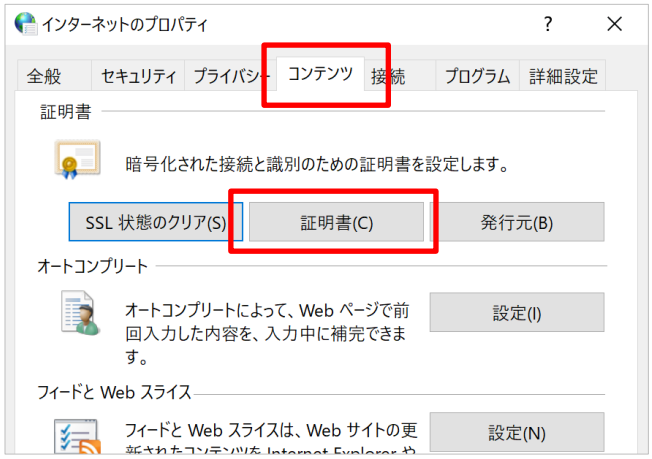

図 4.1-3

④ 「個人」タブに表示される一覧より該当の証明書をクリックします。

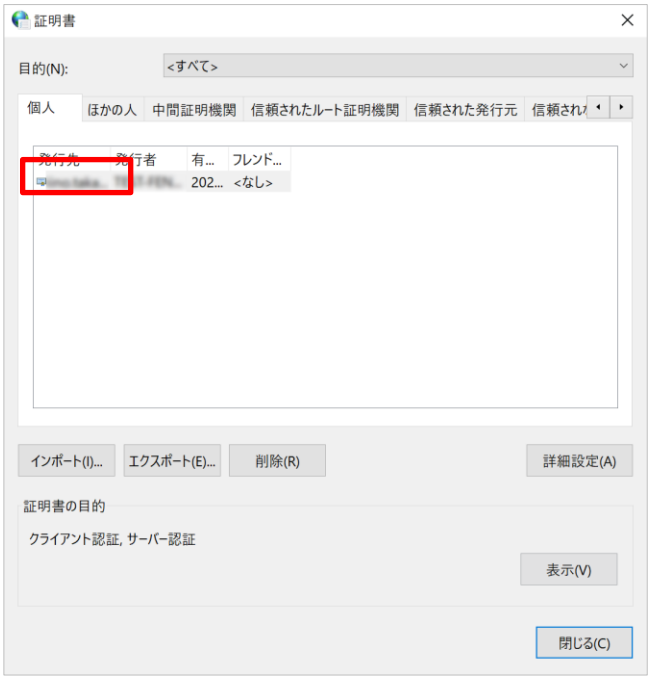

図 4.1-4

⑤ 表示される「証明書」ウィンドウの「詳細」タブをクリックし、シリアル番号を表示します。右下の「OK」ボタン、もしくは、右上の閉じるボタン(X)をクリックしてウィンドウを閉じます。

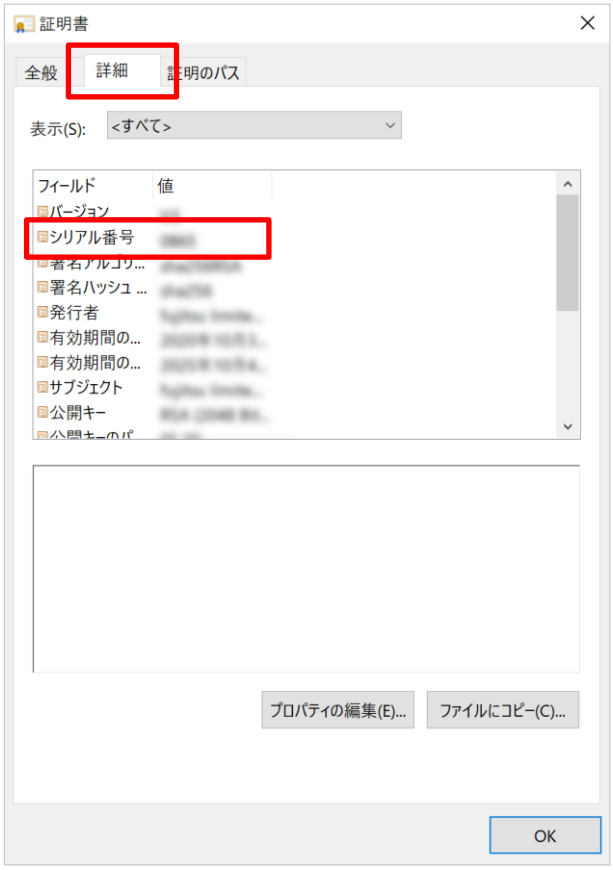

図 4.1-5

以上で、シリアル番号の確認の手順は完了です。

4.2 デバイス証明書の確認

インストール済みのデバイス証明書について確認します。

① ご使用の Windows 端末でコントロールパネルを開き、「ネットワークとインターネット」をクリックします。

図 4.2-1

② 次に表示される画面で「インターネットオプション」をクリックします。

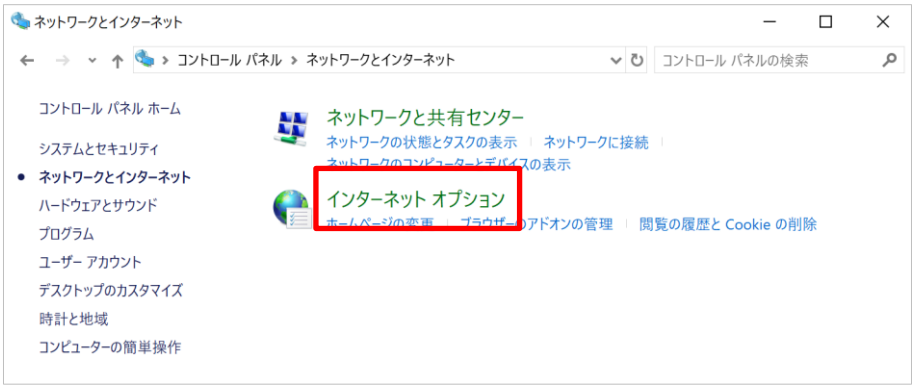

図 4.2-2

③ 表示される「インターネットのプロパティ」画面で「コンテンツ」タブの「証明書」をクリックします。

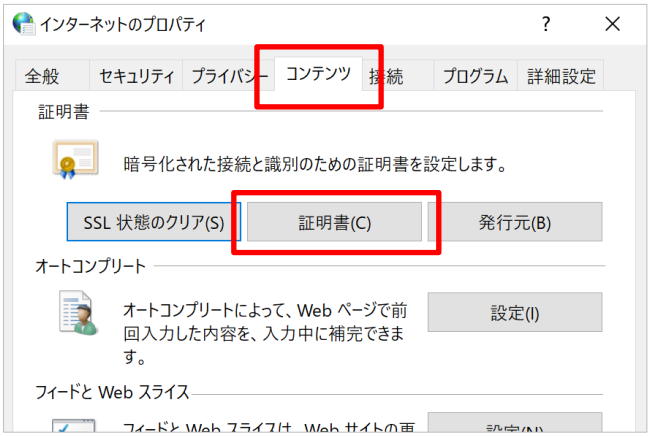

図 4.2-3

④ 証明書画面の「個人」タブにてインストール済みのデバイス証明書が確認できます。
詳細を確認するには、記載している証明書のうち、発行先に開通通知書に記載のあるユーザ名が記載されている証明書をダブルクリックします。

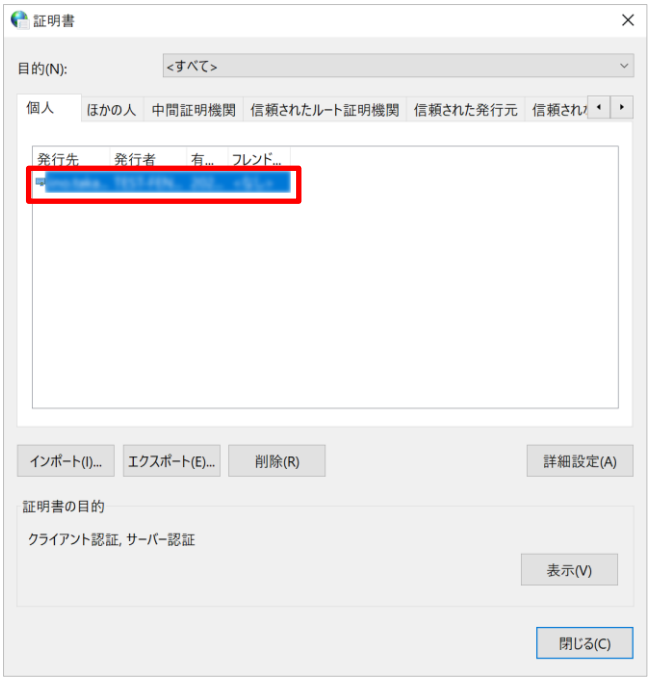

図 4.2-4

⑤ 「証明書」画面の「全般」タブ、「詳細」タブにて証明書の内容が確認できます。

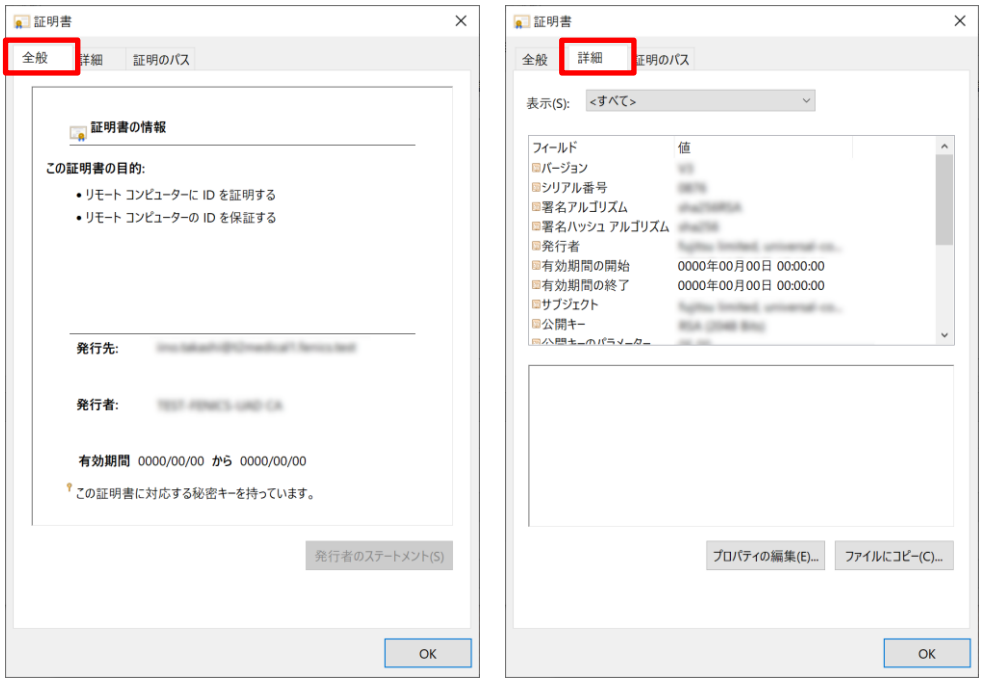

図 4.2-5

以上で、デバイス証明書の確認は完了です。

4.3 デバイス証明書の削除

デバイス証明書の有効期限がきれている、本サービスを解約する、など証明書が不要となった場合に、証明書を削除してください(別サービスでご利用中の証明書を削除しないよう、削除対象の証明書をご確認の上、削除してください)。

【留意事項】

- Windows10 IoT enterprise 2019 LTSC モデルをご使用の場合
  デバイス証明書の削除を実施する前に、UWF(統合書き込みフィルター)機能による C ドライブの保護が解除されていることをご確認ください。

① ご使用の Windows 端末でコントロールパネルを開き、「ネットワークとインターネット」をクリックします。

図 4.3-1

② 次に表示される画面で「インターネットオプション」をクリックします。

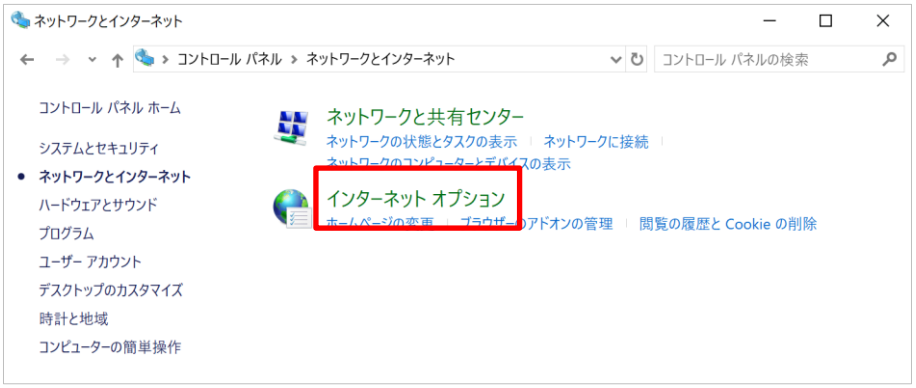

図 4.3-2

③ 表示される「インターネットのプロパティ」画面で「コンテンツ」タブの「証明書」をクリックします。

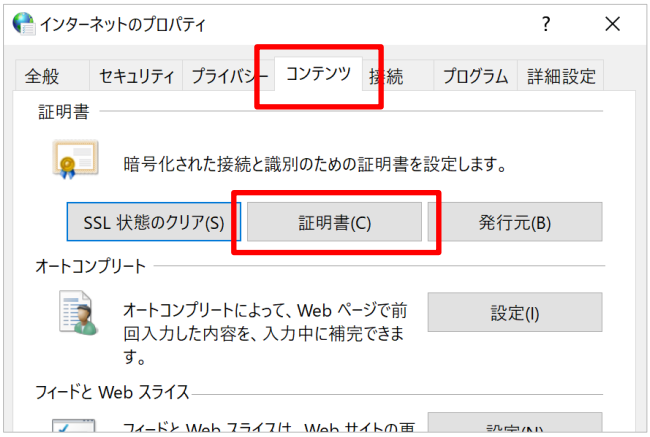

図 4.3-3

④ 証明書画面の「個人タブ」に記載している証明書のうち、発行先に開通通知書に記載のあるユーザ名が記載されている証明書をクリックし、「削除」ボタンをクリックします。

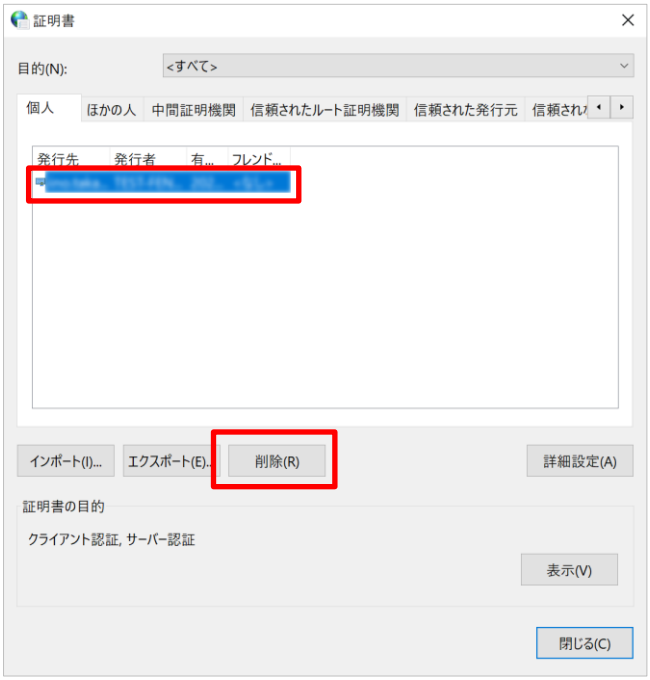

図 4.3-4

⑤ 表示される証明書削除の確認画面で「はい」ボタンをクリックします。

図 4.3-5

⑥ 「証明書」画面で「閉じる」ボタンをクリックします。

図 4.3-6

⑦ 「インターネットのプロパティ」画面で「OK」ボタンをクリックします。

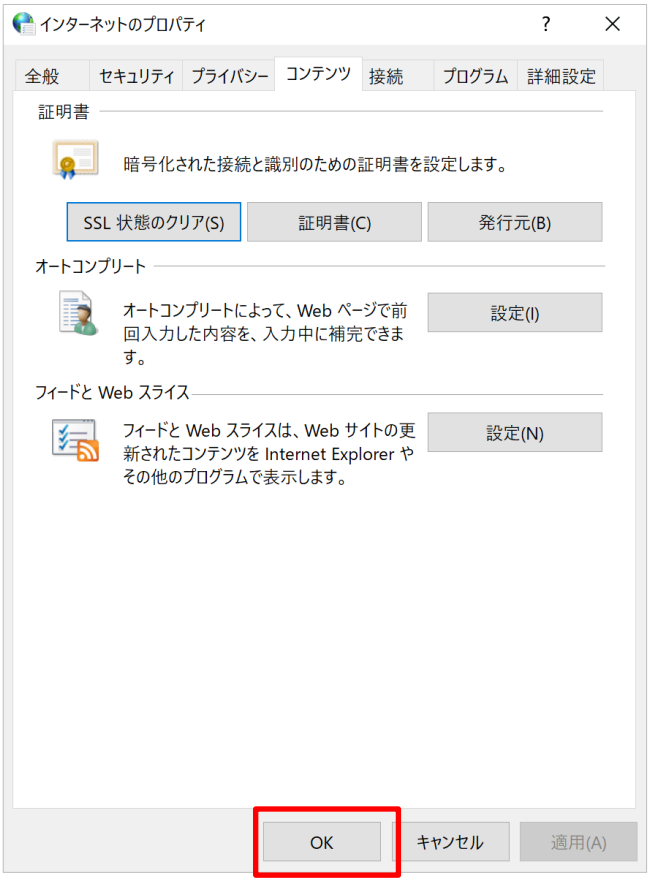

図 4.3-7

以上で、デバイス証明書の削除は完了です。

4.4 アンインストール手順

「Cisco AnyConnect Secure Mobility Client」のアンインストール手順は以下の通りです。手順は、インストールをした際に使用したブラウザを問いません。

① VPN 接続を実行している場合は切断し、クライアントもあわせて終了(Quit)します。
② コントロールパネルにて「Cisco AnyConnect Secure Mobility Client」を右クリックします。

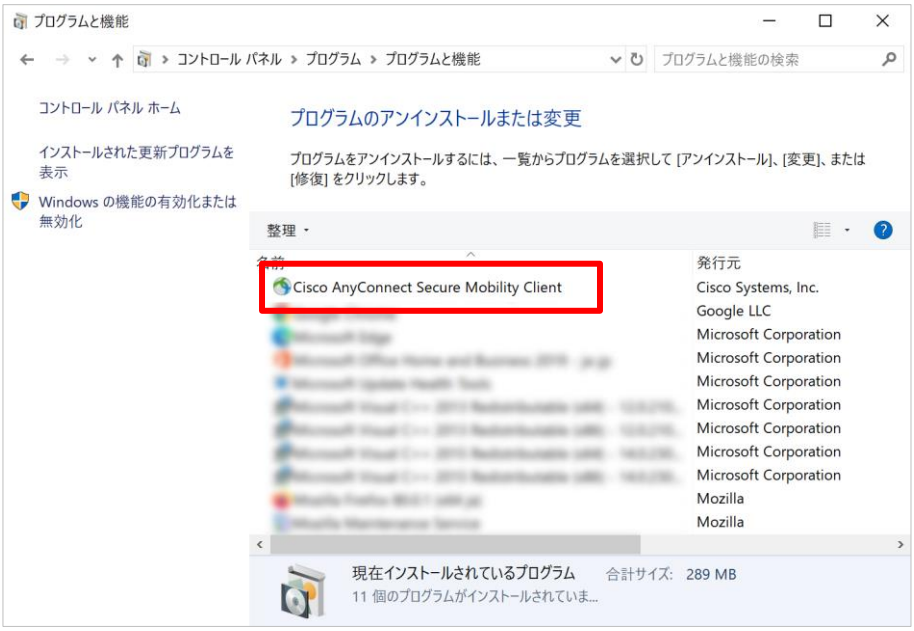

図 4.4-1

③ 表示される項目の「アンインストール」をクリックします。

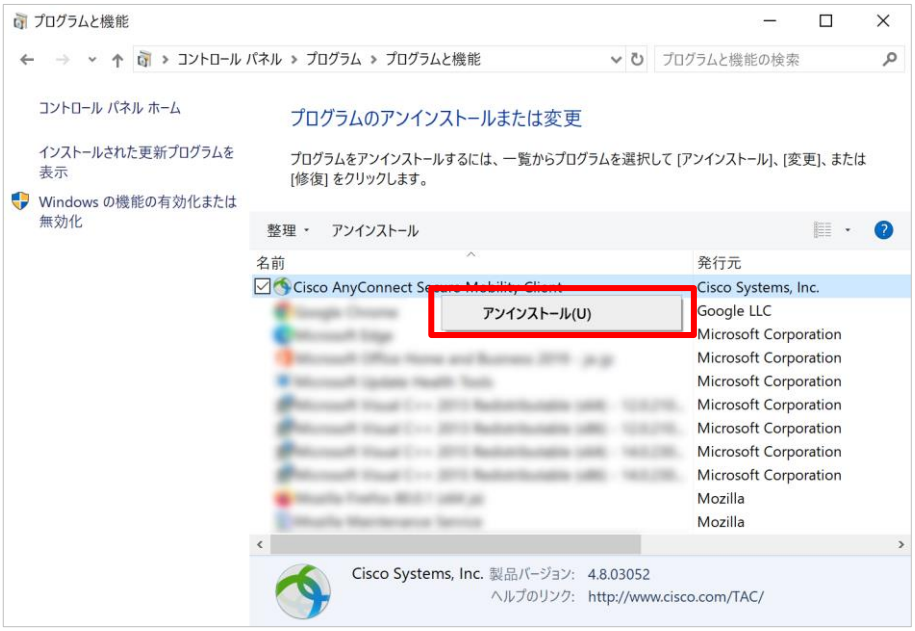

図 4.4-2

※ 「ユーザーアカウント制御」画面が表示される場合は、「はい」をクリックします。

図 4.4-3

④ アンインストールを確認する画面が表示される場合は、「はい」ボタンをクリックします。

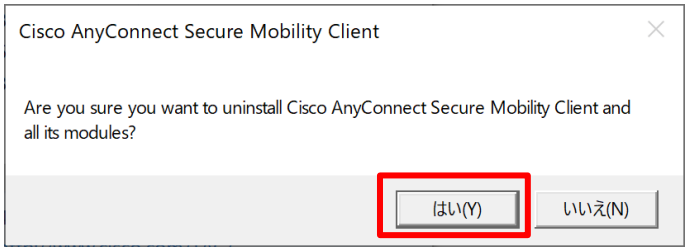

図 4.4-4

⑤　アンインストール処理が実行され、アンインストールのウィンドウが閉じれば終了です。

以上でアンインストール手順は完了です。

4.5 VPN クライアントソフト用設定ファイルの配置確認

① エクスプローラーを開き C ドライブを選択、「表示」タブの「表示/非表示」一覧にて「隠しファイル」にチェックを入れ、表示されるフォルダから「ProgramData」をクリックします。

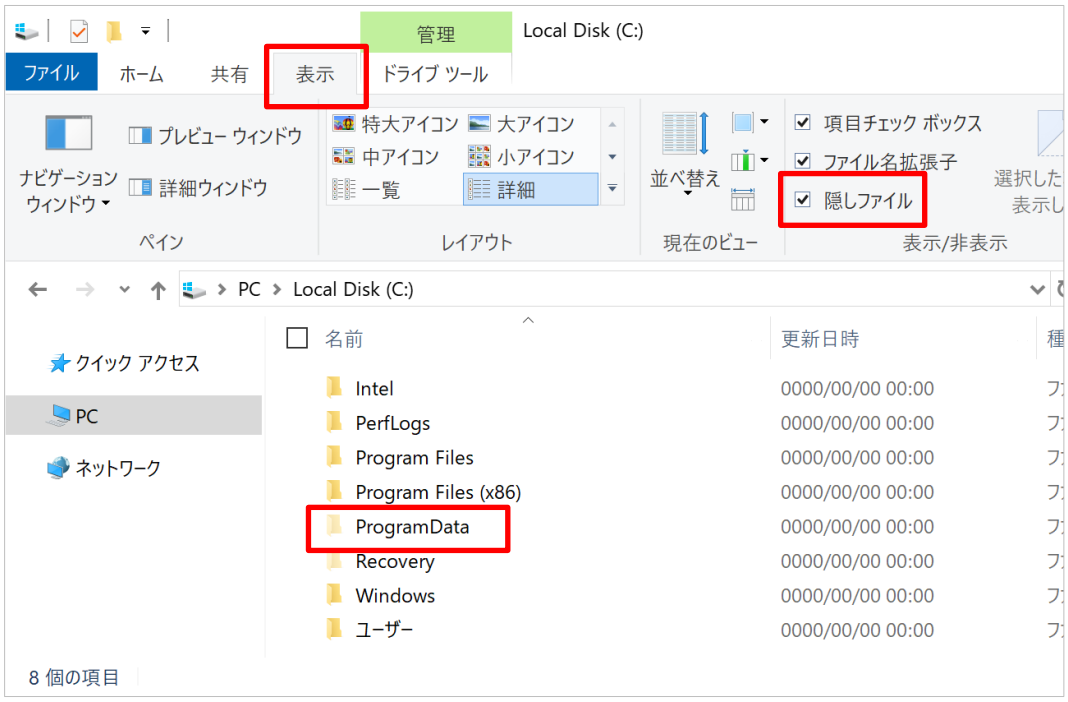

図 4.5-1

② 「Cisco」フォルダ→「Cisco AnyConnect Secure Mobility Client」フォルダ→「Profile」フォルダと順に開き、「Profile」フォルダ内に、「medical-vpn.xml」ファイル(VPN クライアントソフト用設定ファイル)が格納されていることを確認します。

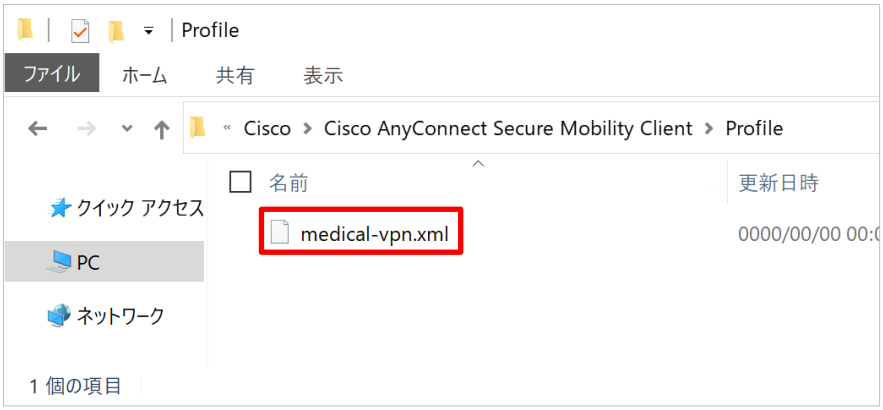

図 4.5-2

以上で、VPN クライアントソフト用設定ファイルの配置確認は完了です。

4.6 エラー

本項ではエラーについて説明します。

4.6.1 「Certificate Validation Failure」

VPN クライアント起動時に「Certificate Validation Failure」の画面が表示される場合、以下の手順でデバイス証明書が正しくインポートされているかご確認ください。

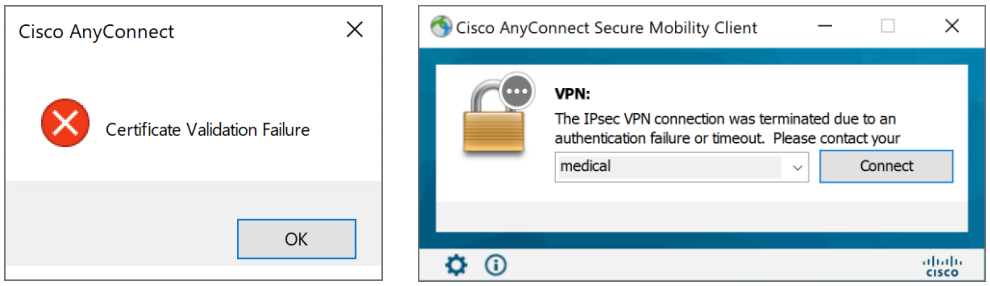

図 4.6-1 エラー画面

- デバイス証明書のインポート状況を確認する
  4.2 デバイス証明書の確認 ④ までの手順で、デバイス証明書のインポート状況を確認します。

  - デバイス証明書がインポートされていない場合
    2.2 証明書の取り込み の手順に従い、デバイス証明書をインポートします。

  - デバイス証明書がインポートされている場合
    4.2 デバイス証明書の確認 ⑤ までの手順を実施し、デバイス証明書の有効期限をご確認の上、「メディカル VPN 接続サービス サポートデスク」へご連絡ください。

以上

富士通株式会社
FENICS II ユニバーサルコネクト アドバンス
メディカル VPN 接続サービス Windows 利用者マニュアル