



お客様各位

2023年 9月 吉日
シスメックス株式会社

Windows 向け PrismGuide NET のセットアップ方法について

PrismGuide NET をご利用いただくためには、パソコンにクライアント証明書及びサーバー証明書を登録していただく必要がございます。クライアント証明書及びサーバー証明書を登録するための手順を以下にまとめました。ご参考の上、登録をお願いいたします。

※注意

クライアント証明書を登録する際、パソコンの管理者権限が必要です。
管理者権限がない、もしくは管理者権限があるか不明な場合は、システム管理部門にお問い合わせください。本手順書に記載に従い PrismGuide NET にアクセスしてください。第三者からの情報による偽サイトへの誘導にご注意ください。

以上

問い合わせ先： シスメックス株式会社

専用窓口：0120-056-034

目次

はじめに.....	3
ネットワークについて.....	3
インターネット接続の場合.....	3
MSEdge、Chrome 共通.....	3
VPN 接続の場合.....	13
MSEdge、Chrome 共通.....	13

はじめに

PrismGuideNET は大きく 2 つの機能で構成されています。①ポータル機能：検査依頼を登録頂き、検査結果レポートを受け取る機能です。②エキスパートパネル支援機能：検査結果レポートや患者の属性情報を他病院と共有しエキスパートパネルを支援する機能です。

本ドキュメントではこの 2 つの機能を使うためのセットアップ方法を説明します。なお、PrismGuideNET は Windows10 にて動作を確認しており、対応しているブラウザは MS Edge(バージョン 83 以上)と Google Chrome(バージョン 83 以上)になります。

ネットワークについて

PrismGuideNET を利用するにあたって、ネットワークの種類を 2 種類用意しております。一つは通常のインターネットアクセスになりますが、この場合セキュリティを考慮し 3 省 2 ガイドラインに対応するためクライアント証明書をインストールする方式を採用しております。

次にどうしてもインターネット接続に制限がある場合、ご相談頂き VPN での接続も可能となっております。この場合、接続先サーバーのサーバー証明書を登録頂く必要がありますので、後述します。

インターネット接続の場合

このインストール作業は、インターネット接続を選択した場合に必要です。

MSEdge、Chrome 共通

<登録手順>

1. クライアント証明書の保存

メールにて配布されたクライアント証明書を任意のフォルダに保存します。

本手順書は例として次のフォルダに保存したものととして以後の説明を行います。

例) C:\¥証明書¥client_<病院コード>.pfx (クライアント証明書)

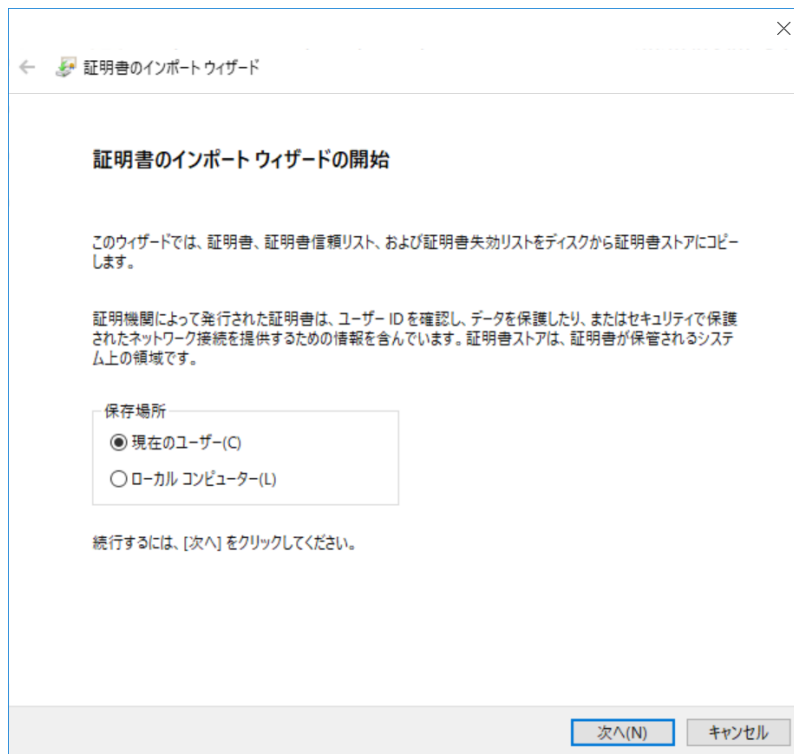
※<病院コード>は 3 ケタの数字となります。

配布されたクライアント証明書は安全に管理する必要があります。

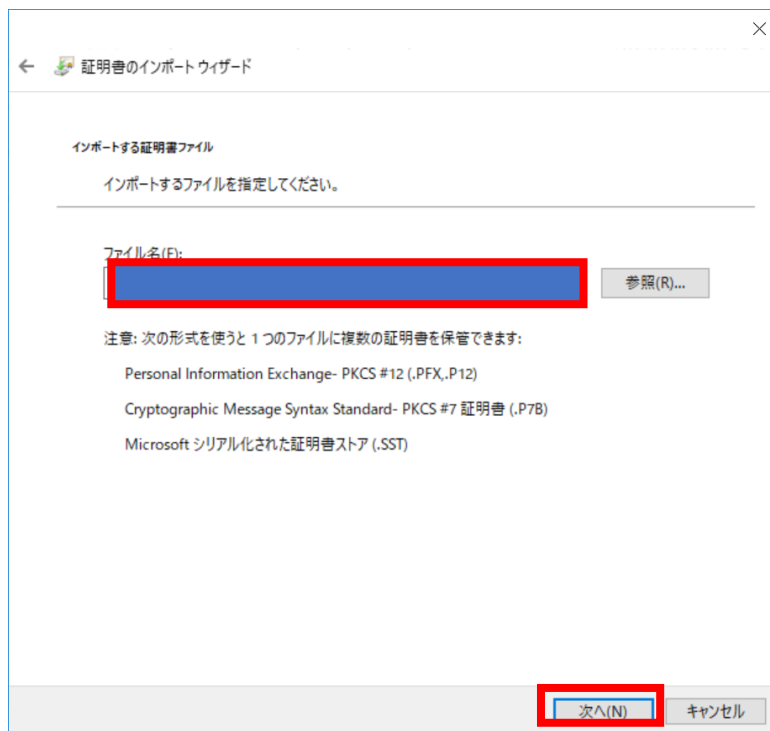
2. クライアント証明書の登録

① 保存したクライアント証明書をダブルクリックします。

証明書のインポートウィザード画面が表示されます。「保存場所」に「現在のユーザ」を選択して、「次へ(N)>」 ボタンをクリックします。



- ② 「証明書のインポート ウィザード」画面の「インポートする証明書ファイル」が表示されます。項目「ファイル名」に配布されたクライアント証明書が既に選択されていますので、「次へ(N)」ボタンをクリックします。



「証明書のインポート ウィザード」画面の「パスワード」が表示されます。
項目「パスワード」に「クライアント証明書と一緒にメールでお伝えしたパスワード」を入力します。

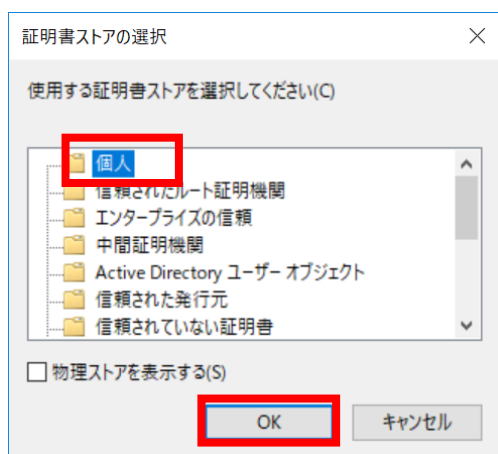
「すべての拡張プロパティを含める(A)」のみ選択状態にし、「次へ(N)>」ボタンをクリックします。

The screenshot shows the 'Certificate Import Wizard' dialog box, specifically the 'Secret Key Protection' (秘密キーの保護) step. The title bar reads '証明書インポートウィザード'. The main text states: 'セキュリティを維持するために、秘密キーはパスワードで保護されています。' (To maintain security, secret keys are protected with a password.) Below this, it says '秘密キーのパスワードを入力してください。' (Please enter the password for the secret key.) There is a text box for the password, currently containing six dots, which is highlighted with a red rectangle. Below the text box is a checkbox labeled 'パスワードの表示(D)' (Show password). Underneath is the 'Import Options' (インポートオプション) section. It contains three checkboxes: '秘密キーの保護を強力にする(E)' (Strengthen secret key protection), 'このキーをエクスポート可能にする(M)' (Exportable key), and '仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)' (Protect secret key with virtualization-based security). The fourth checkbox, 'すべての拡張プロパティを含める(A)' (Include all extended properties), is checked and highlighted with a red rectangle. At the bottom right, there are two buttons: '次へ(N)' (Next) and 'キャンセル' (Cancel), with the '次へ(N)' button highlighted by a red rectangle.

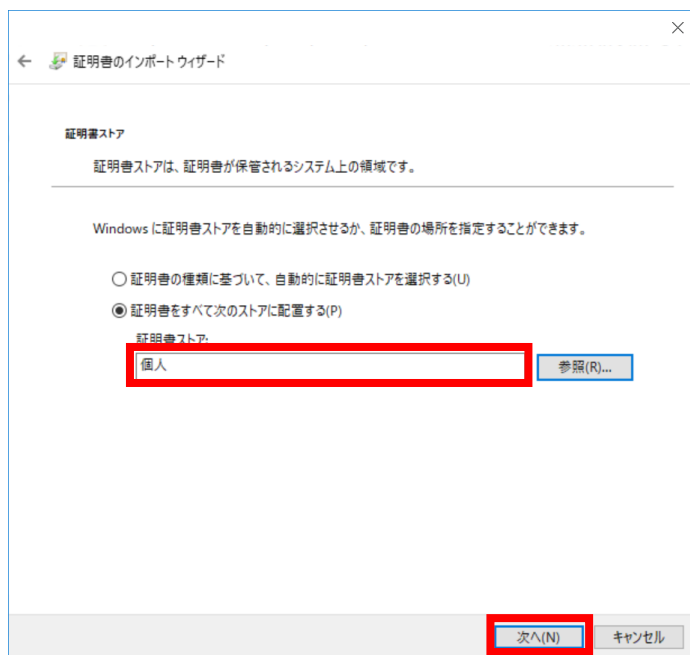
- ③ 「証明書のインポート ウィザード」画面の「証明書ストア」が表示されます。「証明書をすべて次のストアに配置する(P)」を選択し、「参照(R)」ボタンをクリックします。

The screenshot shows the 'Certificate Import Wizard' dialog box, specifically the 'Certificate Store' (証明書ストア) step. The title bar reads '証明書インポートウィザード'. The main text states: '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。' (Certificate stores are areas on the system where certificates are stored.) Below this, it says: '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。' (You can either let Windows automatically select a certificate store or specify the location of the certificate.) There are two radio button options: '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)' (Automatically select certificate store based on certificate type) and '証明書をすべて次のストアに配置する(P)' (Place all certificates in the following store). The second option is selected and highlighted with a red rectangle. Below the radio buttons is a text box for the certificate store name, which is currently empty. To the right of the text box is a button labeled '参照(R)...' (Browse...), which is highlighted with a red rectangle. At the bottom right, there are two buttons: '次へ(N)' (Next) and 'キャンセル' (Cancel), with the '次へ(N)' button highlighted by a red rectangle.

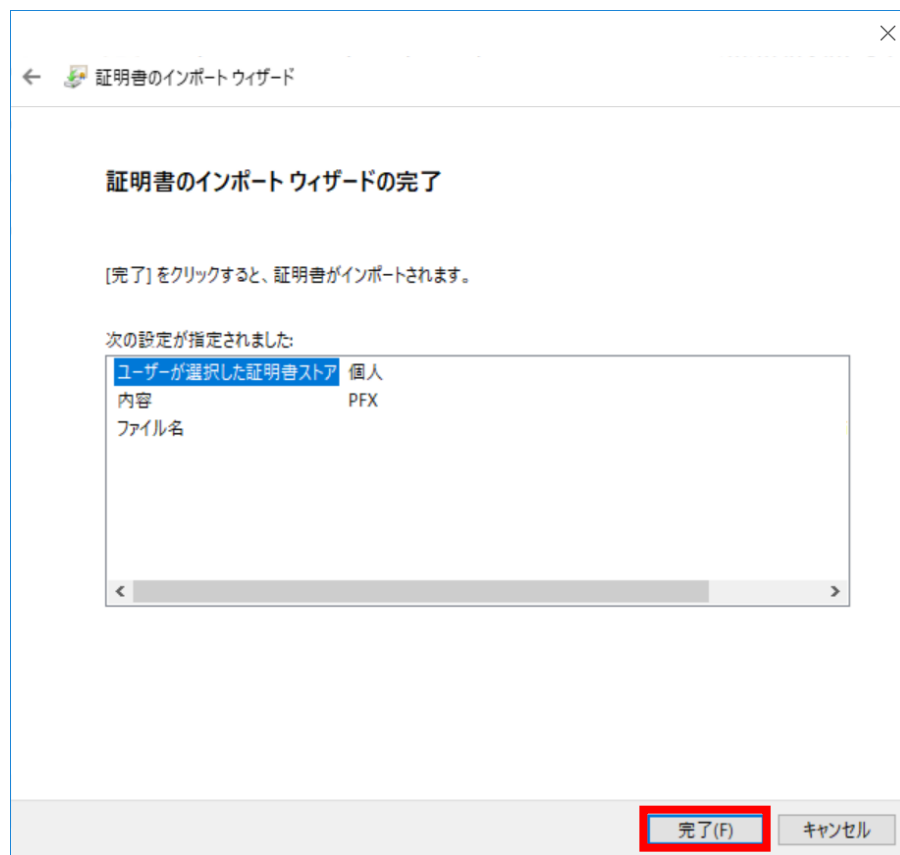
- ④ 「証明書ストアの選択」画面が表示されます。「個人」を選択し、「OK」ボタンをクリックします。



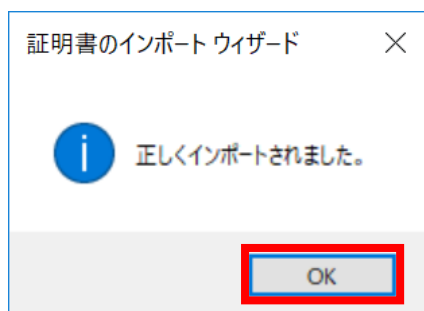
- ⑤ 「証明書のインポート ウィザード」画面の「証明書ストア」の項目「証明書ストア」に「個人」と表示されていることを確認し、「次へ(N) >」をクリックします。



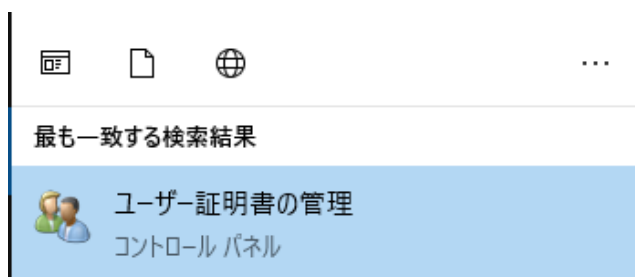
- ⑥ 「証明書のインポート ウィザード」画面の「証明書のインポート ウィザードの完了」が表示されます。「完了」ボタンをクリックします。



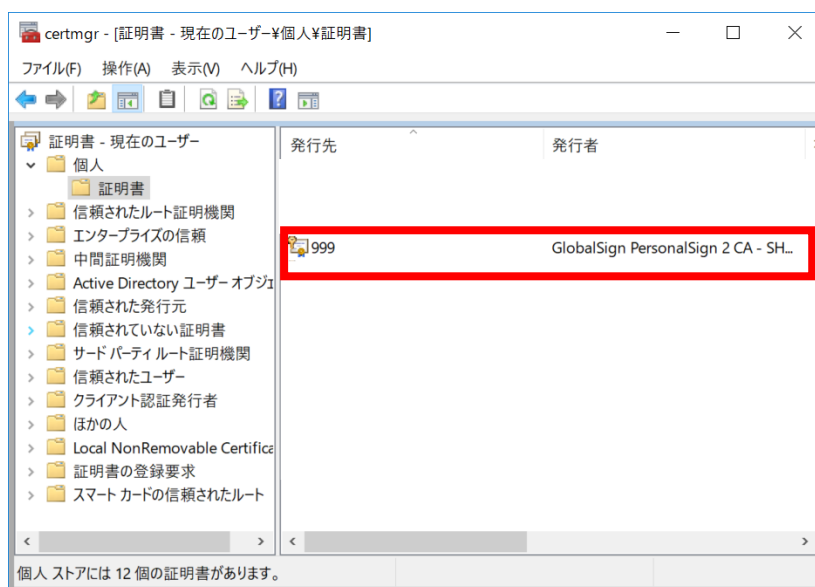
- ⑦ 「証明書のインポート ウィザード」画面にて「正しくインポートされました。」と表示されます。「OK」ボタンをクリックします。



- ⑧ [🔍] 検索機能で「証明書」を検索し「ユーザ証明書の管理」をクリックします。



- ⑨ 「ユーザ証明書の管理」画面の「個人」の「証明書」を選択し、インポートした証明書の情報が一覧に表示されていることを確認してください。



以上

<アクセス方法>

● MSEdge の場合

① ブラウザを起動します。

次の URL を入力し、エンターキーを押下します。

URL : <https://www.prismguidenet.com/>

② 「PrismGuideNET のログイン画面へ」をクリックします。

PrismGuide™NET INFORMATION

Windows用インストール手順 Mac用インストール手順

お知らせ 運営からのお知らせやメンテナンス・障害情報など

2023.09.01 システム稼働開始連絡 PrismGuideNETが稼働開始致しました。

バックナンバー 過去の掲載情報はこちらをご覧ください。

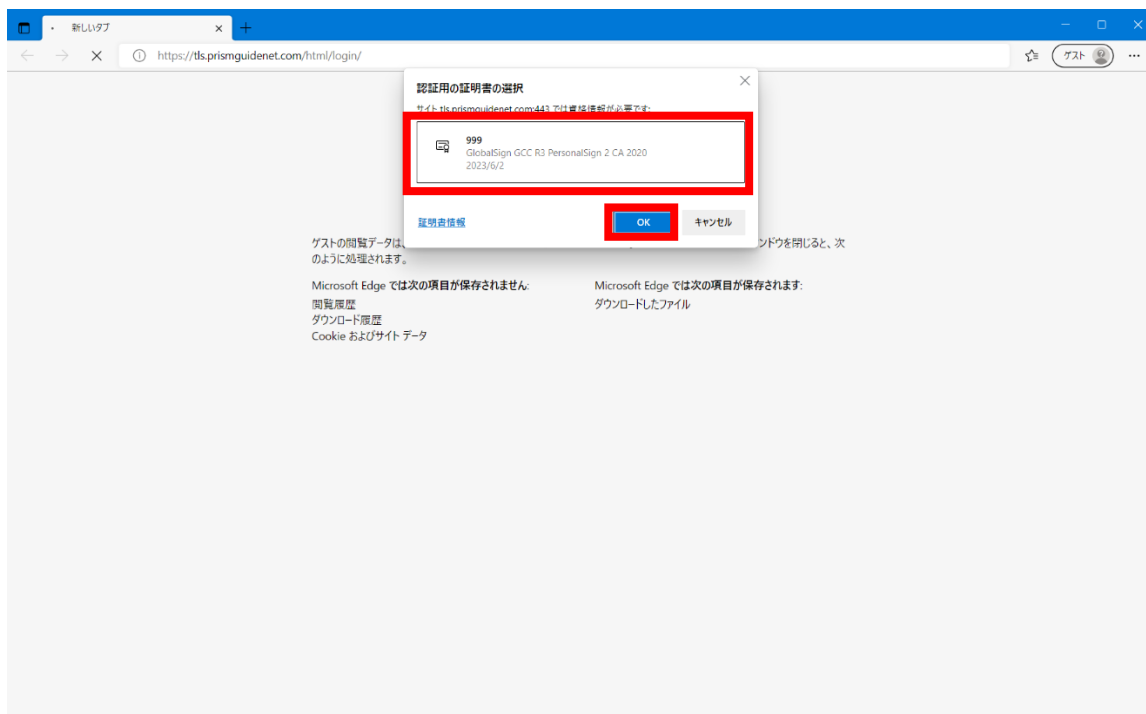
使用しているソフトウェアについて OSSの掲載情報はこちらをご覧ください。

ご利用申し込み頂き、アカウントをお持ちの方は下記よりシステムのログイン画面からログインをお願いします。

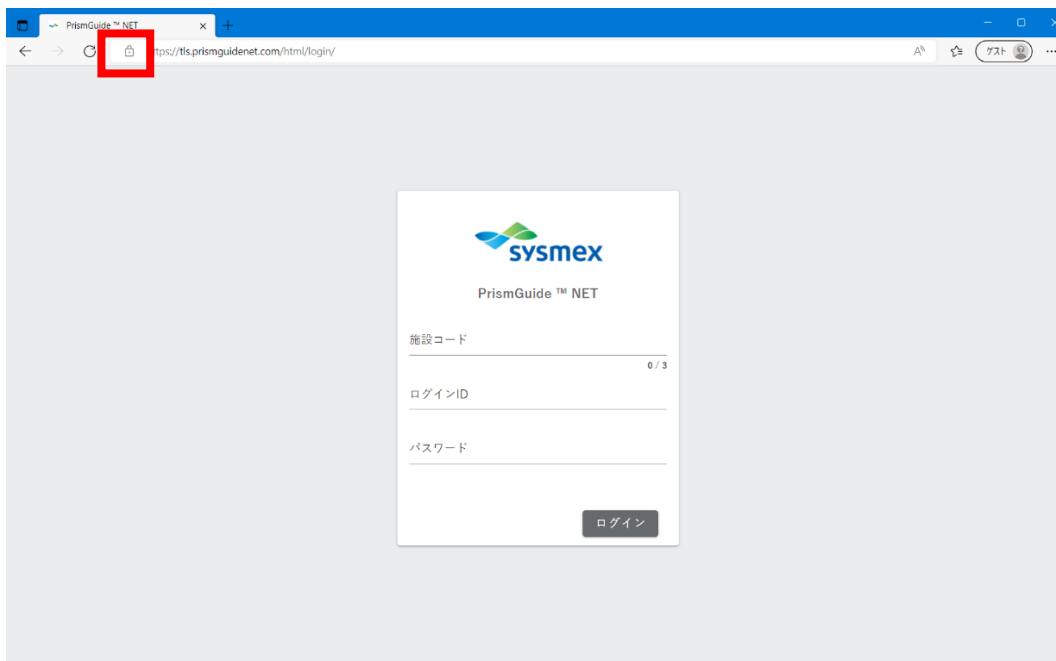
PrismGuide™NETポータル機能のログイン画面へ

PrismGuide™NETエキバネ機能のログイン画面へ

- ③ 「Windows セキュリティ」画面の「証明書の確認」が表示されます。
これはクライアント証明書を選択する画面になります。
先ほど登録したクライアント証明書を選択し、「OK」ボタンをクリックします。



- ④ エキスパートパネルのログイン画面が表示されます。
URL 右の「🔒 (鍵マーク)」が表示されることを確認してください。



- ⑤ 割り当てられたログイン情報を入力し、「ログインボタン」をクリックしてください。

- Chrome の場合

① ブラウザを起動します。

次の URL を入力し、エンターキーを押下します。

URL : <https://www.prismguidenet.com/>

② 「PrismGuideNET のログイン画面へ」をクリックします。

PrismGuide™NET INFORMATION

Windows用インストール手順 Mac用インストール手順

お知らせ 運営からのお知らせやメンテナンス・障害情報など

2023.09.01 システム稼働開始連絡 PrismGuideNETが稼働開始致しました。

バックナンバー 過去の掲載情報はこちらをご覧ください。

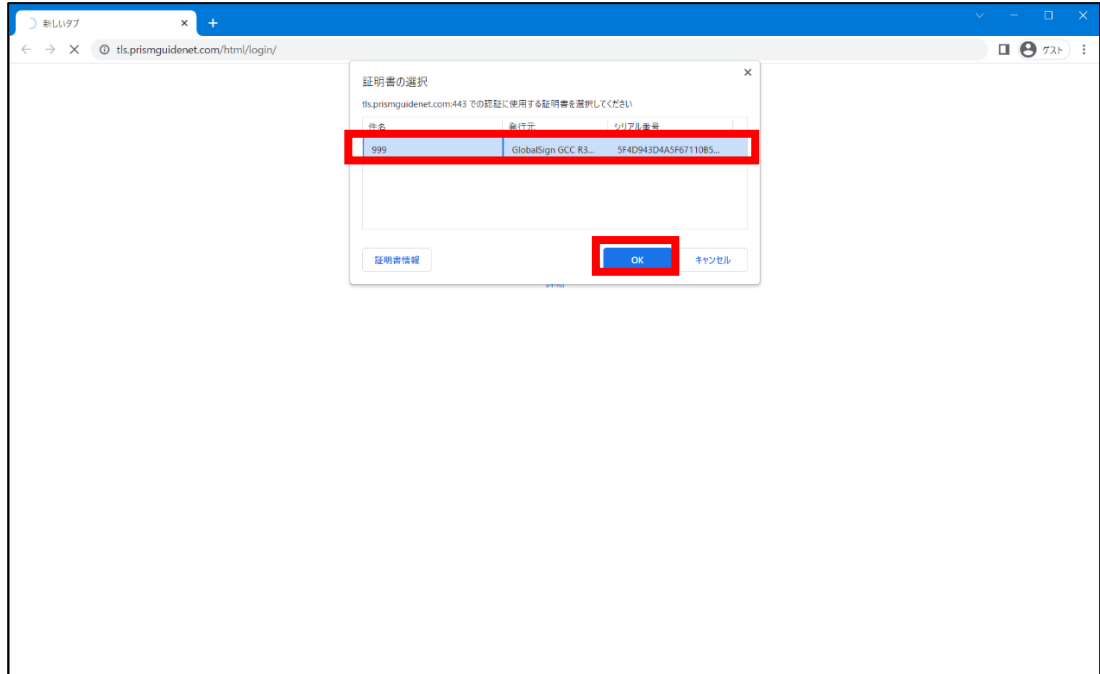
使用しているソフトウェアについて OSSの掲載情報はこちらをご覧ください。

ご利用申し込み頂き、アカウントをお持ちの方は下記よりシステムのログイン画面からログインをお願いします。

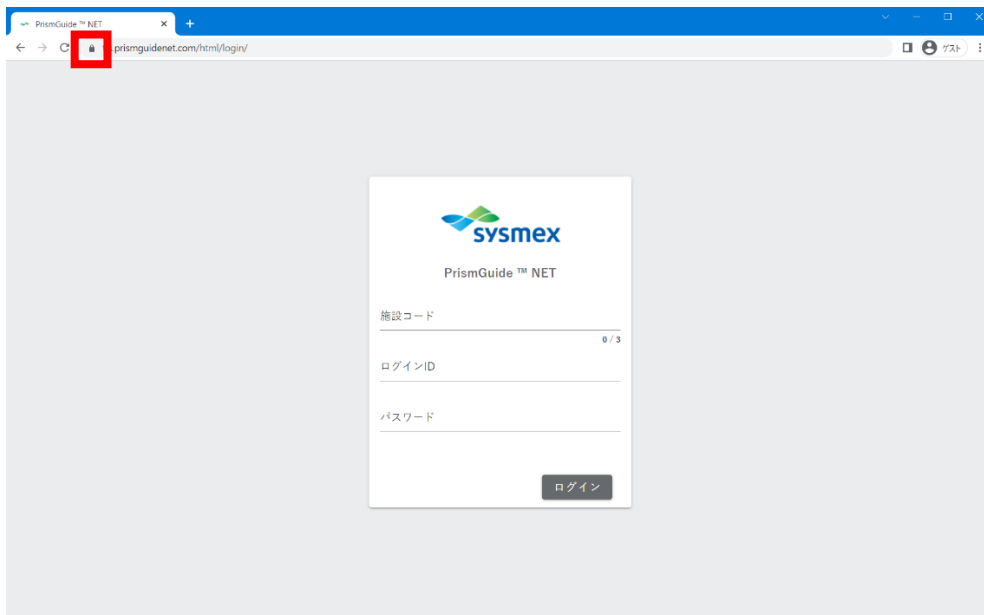
PrismGuide™NETポータル機能のログイン画面へ

PrismGuide™NETエキバネ機能のログイン画面へ

- ③ 「Windows セキュリティ」画面の「証明書の確認」が表示されます。
これはクライアント証明書を選択する画面になります。
先ほど登録したクライアント証明書を選択し、「OK」ボタンをクリックします。



- ④ エキスパートパネルのログイン画面が表示されます。
URL 右の「🔒 (鍵マーク)」が表示されることを確認してください。



- ⑤ 割り当てられたログイン情報を入力し、「ログインボタン」をクリックしてください。

VPN 接続の場合

このインストール作業は、VPN 接続を選択した場合に必要です。

MSEdge、Chrome 共通

1. サーバー証明書の保存

メールにて配布されたサーバー証明書を任意のフォルダに保存します。

本手順書は例として次のフォルダに保存したものとして以後の説明を行います。

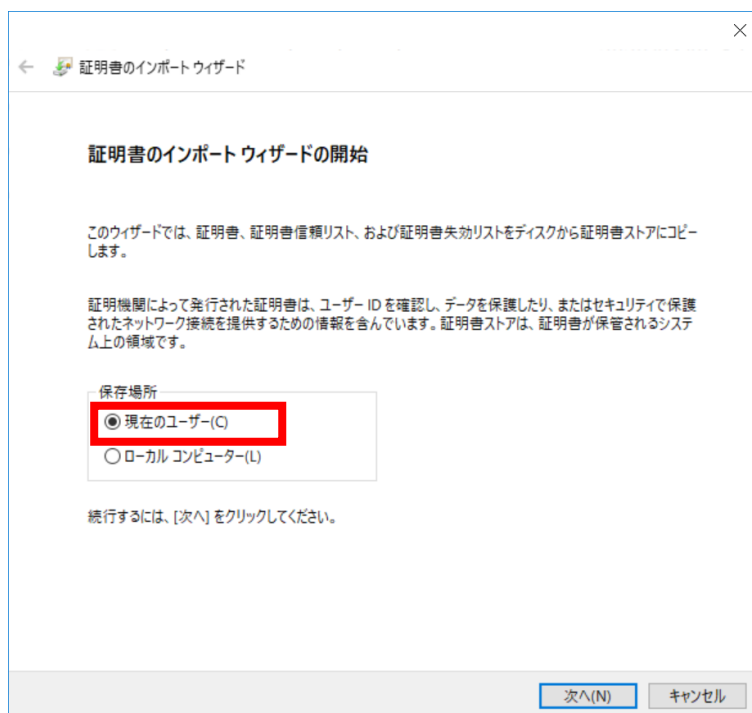
例) デスクトップ/証明書/app-prismguidenet-com-ca (サーバー証明書)

※配布されたサーバー証明書は安全に管理する必要があります。

2. サーバー証明書の登録

① 保存したサーバー証明書をダブルクリックします。

証明書のインポートウィザード画面が表示されます。「保存場所」に「現在のユーザ」を選択して、「次へ(N)>」 ボタンをクリックします。



- ② 「証明書のインポート ウィザード」画面の「インポートする証明書ファイル」が表示されます。項目「ファイル名」に配布されたクライアント証明書が既に選択されていますので、「次へ(N)>」ボタンをクリックします。

← 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。

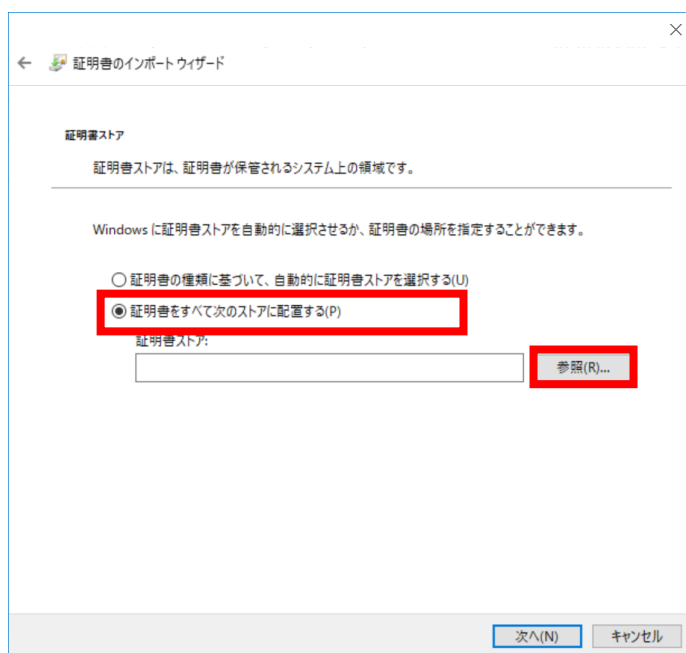
ファイル名(F):
[Redacted] 参照(R)...

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:

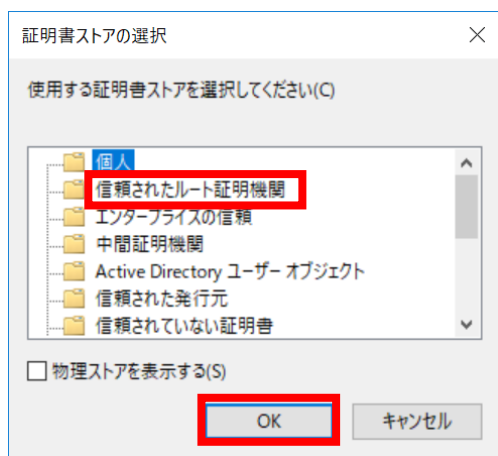
- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

次へ(N) キャンセル

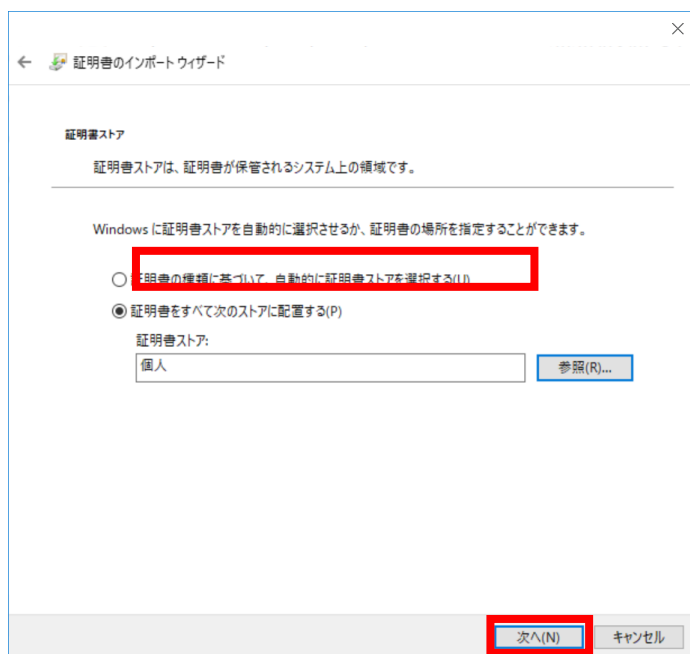
- ③ 「証明書のインポート ウィザード」画面の「証明書ストア」が表示されます。「証明書をすべて次のストアに配置する(P)」を選択し、「参照(R)」ボタンをクリックします。



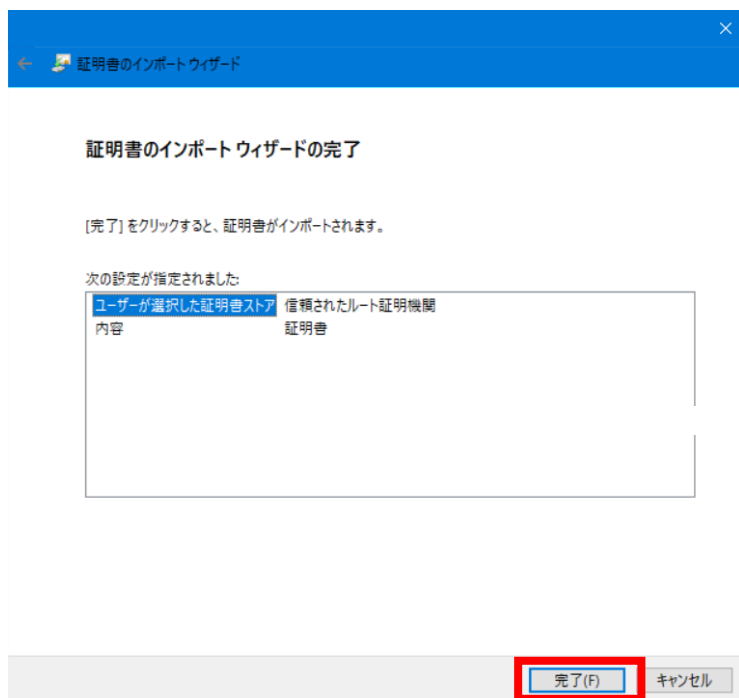
- ④ 「証明書ストアの選択」画面が表示されます。「信頼されたルート証明期間」を選択し、「OK」ボタンをクリックします。



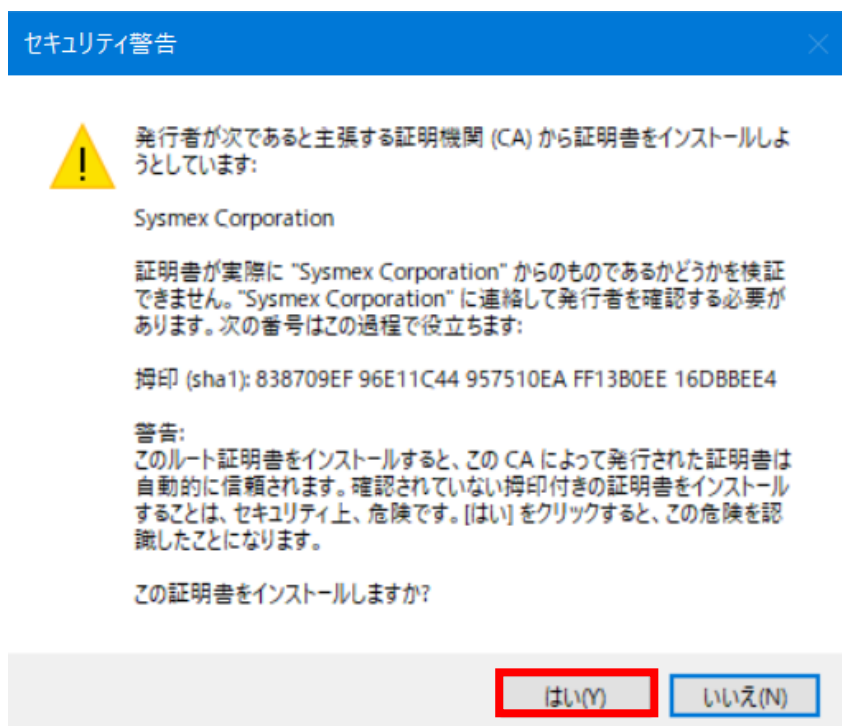
- ⑤ 「証明書のインポート ウィザード」画面の「証明書ストア」の項目「証明書ストア」に「個人」と表示されていることを確認し、「次へ(N) >」をクリックします。



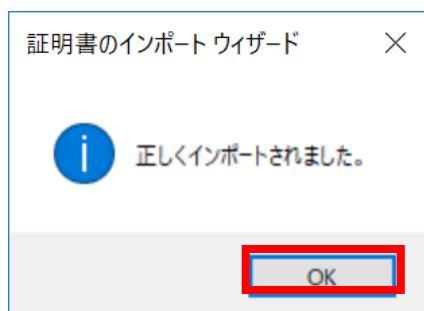
- ⑥ 「証明書のインポート ウィザード」画面の「証明書のインポート ウィザードの完了」が表示されます。「完了」ボタンをクリックします。



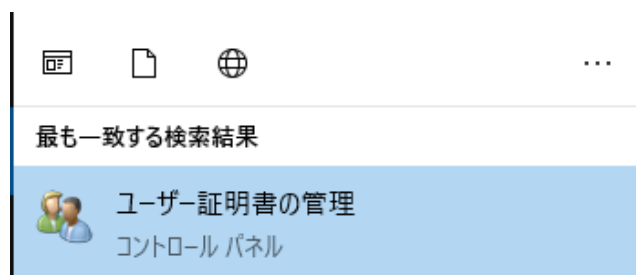
- ⑦ セキュリティ警告ダイアログにて「はい」をクリックします。



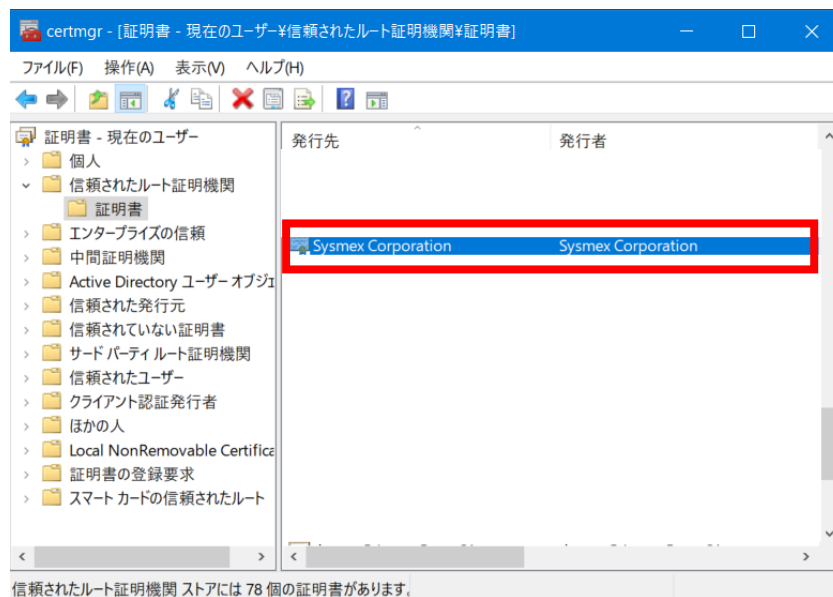
- ⑧ 「証明書のインポート ウィザード」画面にて「正しくインポートされました。」と表示されます。「OK」ボタンをクリックします。



- ⑨ [🔍] 検索機能で「証明書」を検索し「ユーザ証明書の管理」をクリックします。



- ⑩ 「ユーザ証明書の管理」画面の「信頼されたルート認証機関」の「証明書」を選択し、インポートした証明書の情報が一覧に表示されていることを確認してください。



以上