

VPN クライアント導入/設定 (Windows)

2024/5/30



国立大学法人

滋賀医科大学

SHIGA UNIVERSITY OF MEDICAL SCIENCE

はじめに

- 滋賀医科大学のネットワークに学外から接続する時にはFortiClientというVPNクライアントを使用します。なお、CA証明書の導入も必要です。
- 本マニュアルは **Windows PC** のVPNクライアントの導入方法、設定方法を記述します。
- VPN接続後は、学内と同じ方法で通常通り滋賀医科大学のホームページにアクセスするなど実施下さい。

1. FortiClient VPN導入
2. FortiClient VPN設定
3. CA証明書の導入
 - Firefox以外のブラウザ( や )を使用する場合
 - Firefox()を使用する場合
4. VPNの接続
5. VPNの切断

1. FortiClient ダウンロードと導入

以下のサイトから「FortiClient VPN」を選択し、導入するOSを選択しダウンロードしてください。

<https://www.fortinet.com/support/product-downloads#vpn>

FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.

Remote Access

- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA

Windows
Download VPN for Windows
DOWNLOAD

MacOS
Download VPN for MacOS
DOWNLOAD

Linux
Download VPN for Linux
DOWNLOAD .rpm

iOS
Download VPN for iOS
DOWNLOAD

Android
Download VPN for Android
DOWNLOAD

Linux
Download VPN for Linux
DOWNLOAD

注意
「DOWNLOAD」をクリック後、下記画面に切り替わりますが、何もせず画面右上にある ↓ (ダウンロード) をクリックし、**FortiClientVPNOnlineInstaller.exe** があることを確認してください

FortiClient Products Solutions Support Store FORTIGUARD LABS THREAT INTELLIGENCE

Your zero trust journey starts here

Learn More

ZTNA Resources

- ZTNA Resources and the benefits of a zero trust architecture
- How to Harden VPN with ZTNA
- Technical documentation to design, demo, and deploy ZTNA with FortiClient

First Name * Last Name *

Email Address *

Do you work in IT/Operations? Yes No

I consent to receive promotional communications (which may include phone, email, and social) from Fortinet. I understand I may proactively opt out of communications with Fortinet at anytime.

SUBMIT

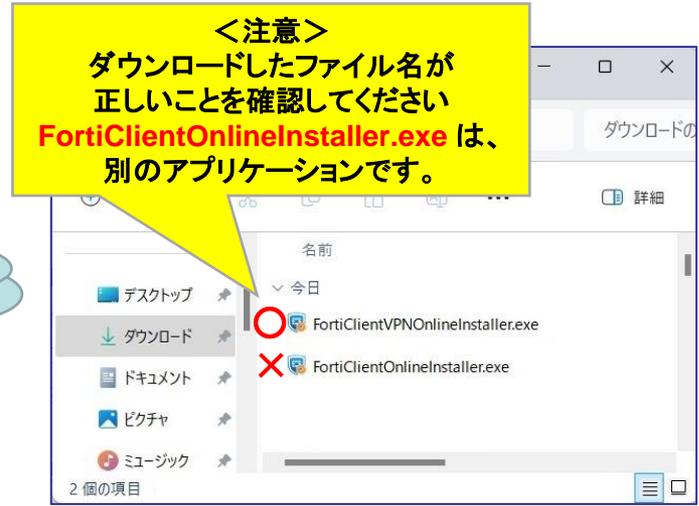
↓ **Downloaded...**

Install Now

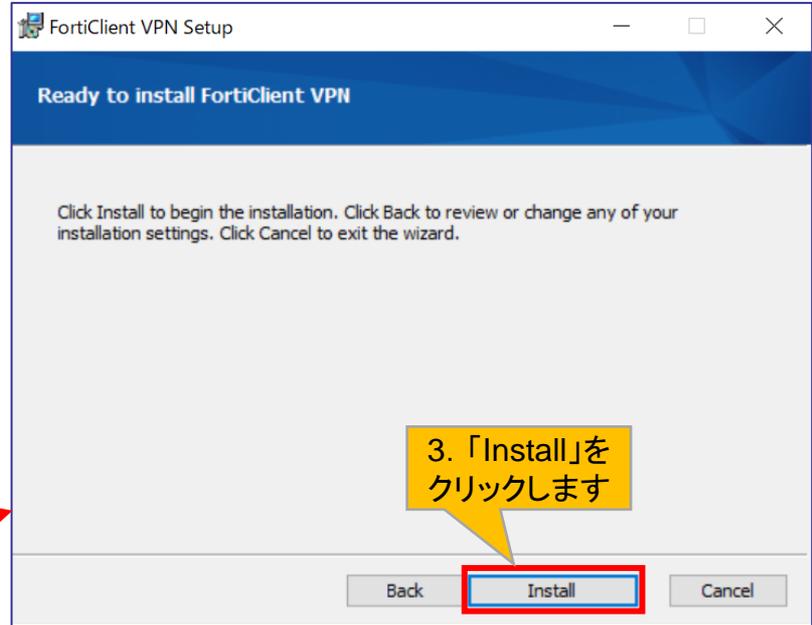
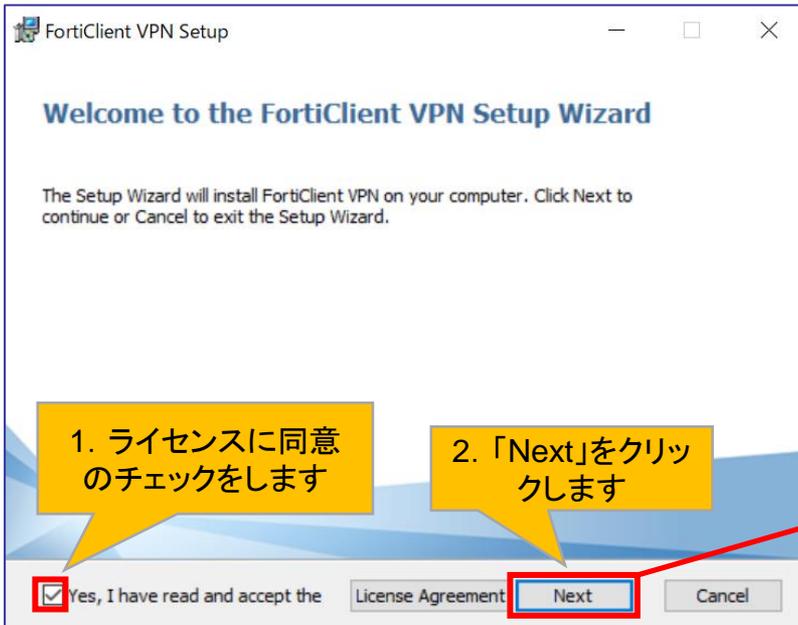
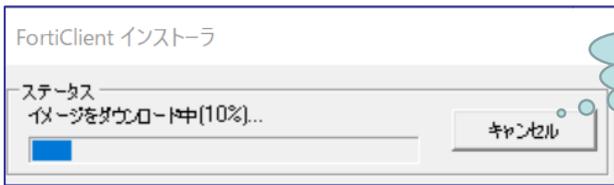
1-1. FortiClient VPN導入

ダウンロードされた以下のファイルを
ダブルクリックしてください。

FortiClientVPNOnlineInstaller.exe

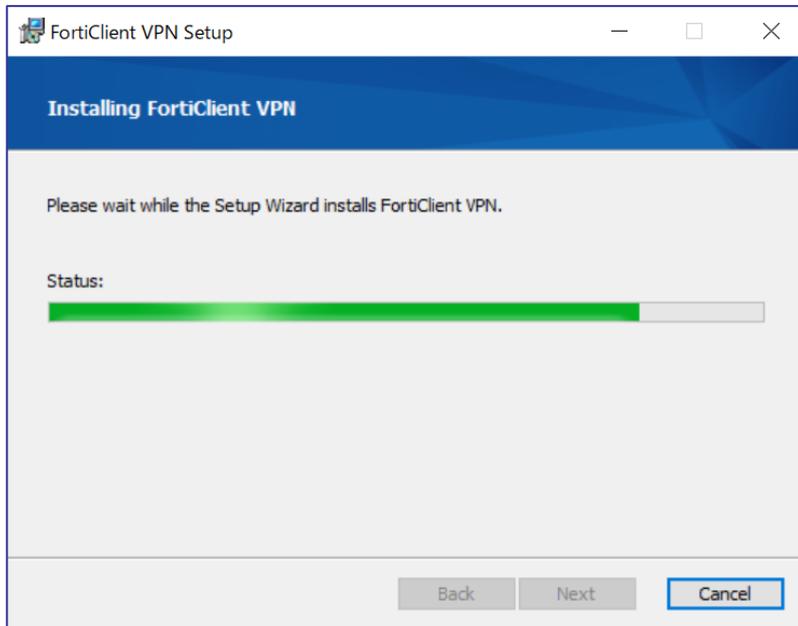


ダウンロードに時間
がかかります

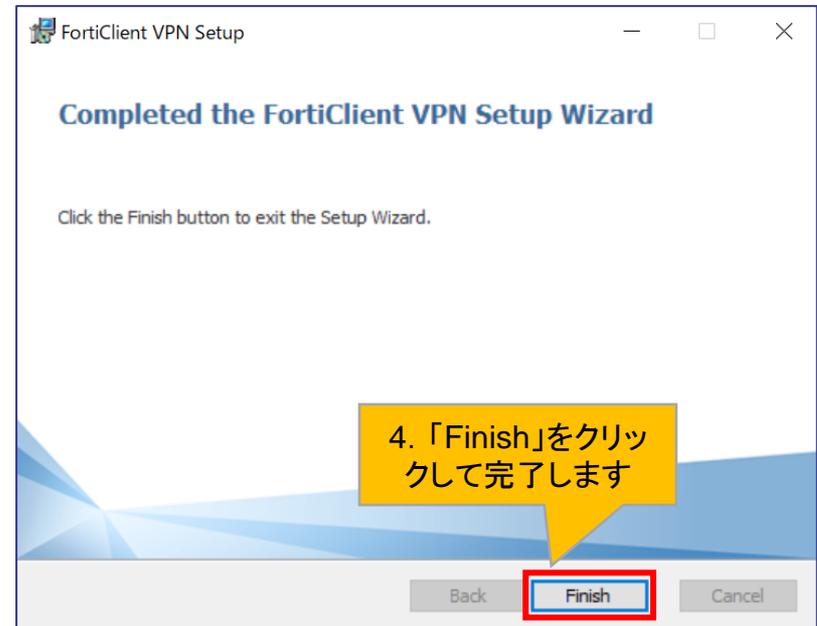


1-2. FortiClient VPN導入

導入中

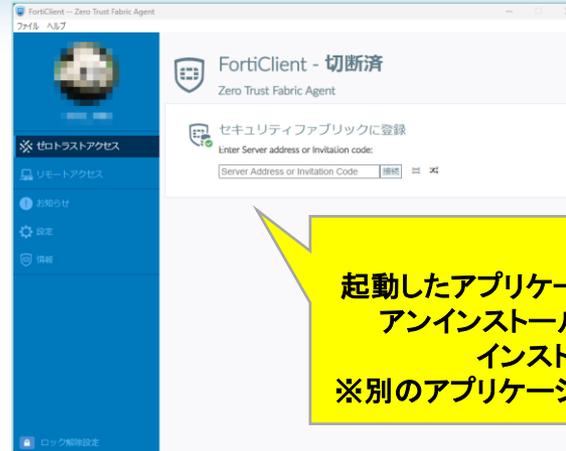


導入完了



2-1 VPNの初期設定

FortiClient VPNを起動します



<注意>
起動したアプリケーションがこの画面の場合は、
アンインストールして、**FortiClient VPN** を
インストールしてください。
※別のアプリケーションをインストールしています



2-2. VPNの初期設定

3. 「SSL-VPN」を選択します

4. 右図のように設定します (接続名/説明は任意)

5. 「保存」をクリックして終了します

<注意>
リモートGWの入力間違いがよくあります。
ご注意ください。

sumsvpn.shiga-med.ac.jp

VPN接続できない場合は、リモートGWを
下記に変更してください。
202.19.144.126

設定確認・編集方法

VPN名称 SUMS

接続

新規接続の追加
接続の編集
接続の削除

| 項目 | 設定 |
|------------------------------|-------------------------|
| 接続名 | 例: SUMS |
| 説明 | 例: SUMS VPN |
| リモートGW | sumsvpn.shiga-med.ac.jp |
| ポートの編集 | チェックを入れる: 443 |
| VPNトンネルのシングルサインイン (SSO) を有効可 | チェックを入れる |
| クライアント証明書 | なし |

初期設定完了

VPN名称 SUMS

SAMLログイン

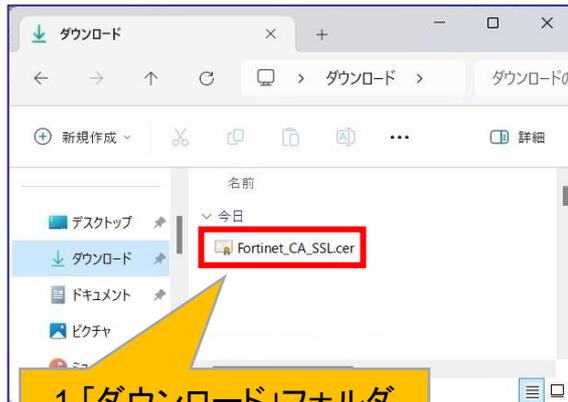
引き続き、ご利用のブラウザ環境に合わせて、
次ページからの証明書導入を行ってください

3-1-1 CA証明書の導入

Firefox以外のブラウザ( や )を使用する場合

CA証明書を以下のURLからダウンロードください。(Fortinet_CA_SSL.cer)

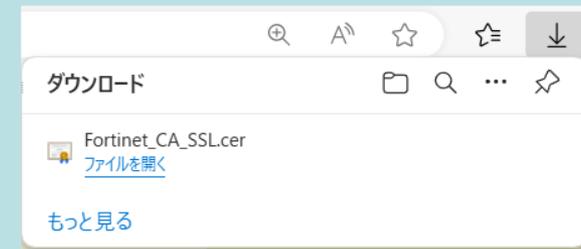
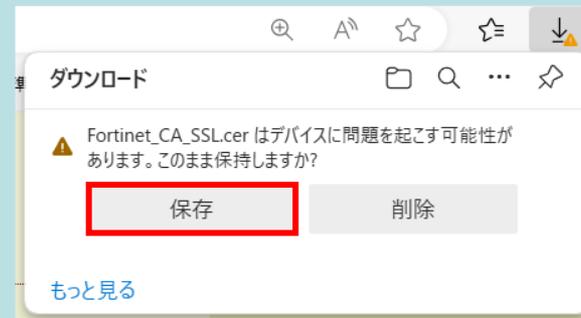
https://www.shiga-med.ac.jp/mmc/service/vpn/Fortinet_CA_SSL.cer



1.「ダウンロード」フォルダの「Fortinet_CA_SSL.cer」をダブルクリックします

Edge  をお使いの場合

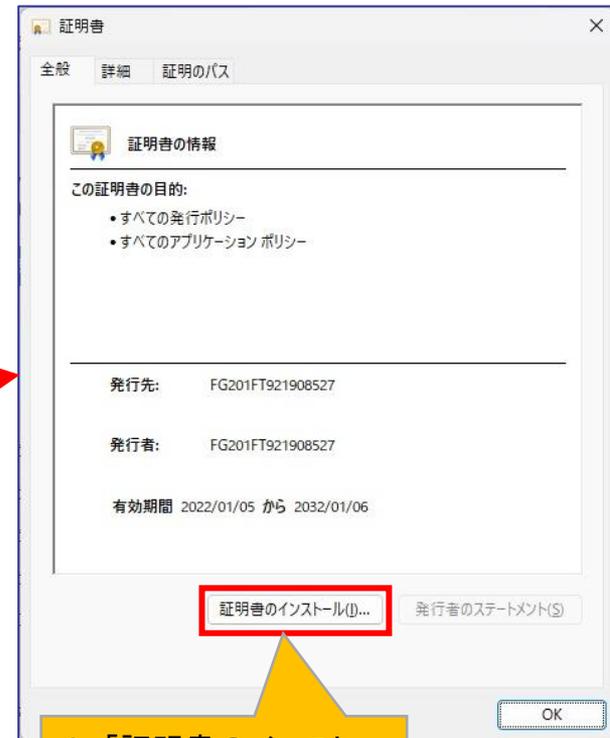
下記の表示が出た場合は、「保存」をクリックしてください。



3-1-1 CA証明書の導入

Firefox以外のブラウザ( や )を使用する場合

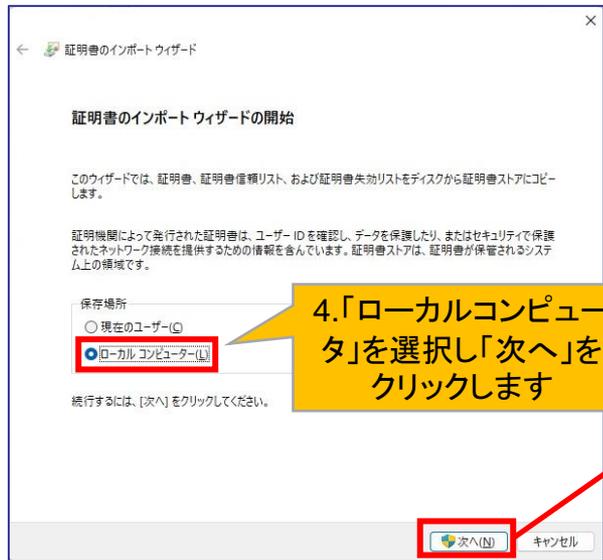
2. 「このファイルを開きますか?」で「開く」をクリックします



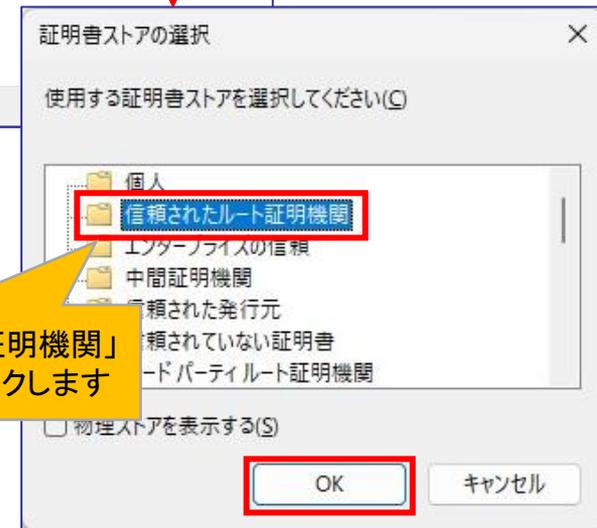
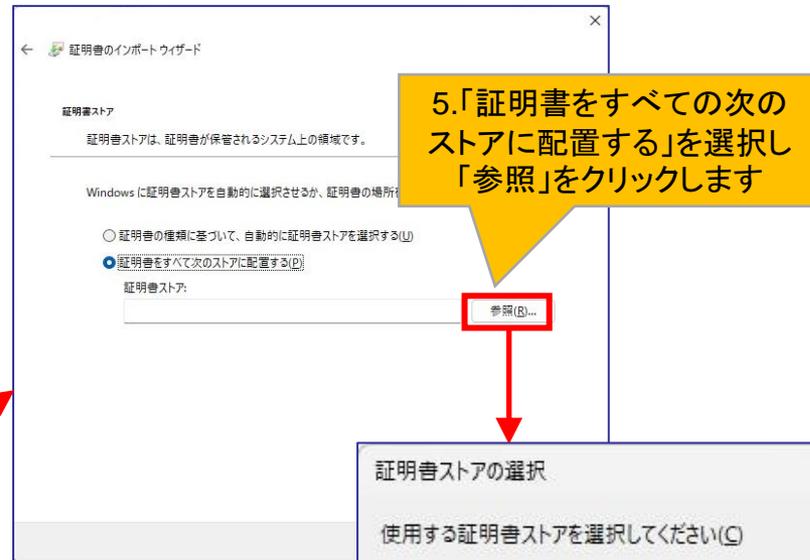
3. 「証明書のインストール」をクリックします

3-1-2 CA証明書の導入

Firefox以外のブラウザを( や ) 使用する場合



※ユーザーアカウント制御画面が表示されたら、「はい」をクリックします。



3-1-2 CA証明書の導入

Firefox以外のブラウザを( や ) 使用する場合

7.「次へ」をクリックします

8.「完了」をクリックします

9.「OK」をクリックします

10.「OK」をクリックして完了します

3-2-1 CA証明書の導入 Firefox()を使用する場合

CA証明書を以下のURLからダウンロードください。(Fortinet_CA_SSL.cer)

https://www.shiga-med.ac.jp/mmc/service/vpn/Fortinet_CA_SSL.cer



The image shows a screenshot of the Firefox browser interface with three numbered steps for navigating to the security settings:

- 1. ☰ をクリックします** (Click the menu icon): A red box highlights the menu icon (three horizontal lines) in the top right corner of the browser window.
- 2. 「設定」をクリックします** (Click "Settings"): A red box highlights the "設定" (Settings) option at the bottom of the menu.
- 3. 「プライバシーとセキュリティ」をクリックします** (Click "Privacy & Security"): A red box highlights the "プライバシーとセキュリティ" (Privacy & Security) option in the settings menu.

The settings menu on the right shows the following options:

- 一般 (General)
- ホーム (Home)
- 検索 (Search)
- プライバシーとセキュリティ (Privacy & Security)**
- 同期 (Sync)
- Mozilla カスタマイズ (Customize)
- 拡張機能とテーマ (Extensions and Themes)
- Firefox サポート (Support)

Additional settings visible include "起動" (Startup) with options for opening windows and tabs, and "新しいウィンドウではなく新しいタブ" (Open new windows in tabs instead of new windows) which is checked.

3-2-2 CA証明書の導入 Firefox()を使用する場合

Firefoxの「プライバシーとセキュリティ」設定画面のスクリーンショット。左側のメニューで「プライバシーとセキュリティ」が選択されている。右側の設定項目で「証明書」が赤い点線で囲まれている。その下に「OCSP レスポンスサーバーに問い合わせさせて証明書の現在の正当性を確認する」がチェックされている。さらに「証明書を表示...(C)」というボタンが赤い枠で囲まれている。右側の黄色い吹き出しには「4.「証明書を表示」をクリックします」とある。

「証明書マネージャー」ダイアログボックスのスクリーンショット。タブで「認証局証明書」が選択されている。下部のリストには「Fortinet」の証明書が赤い枠で囲まれている。その証明書名は「FG201FT921908527」であり、セキュリティデバイスは「Software Security Device」である。下部には「表示...(V)」、「信頼性を設定...(E)」、「インポート...(M)」、「エクスポート...(X)」、「削除または信頼しない...(D)」のボタンがある。右下には「OK」ボタンがある。

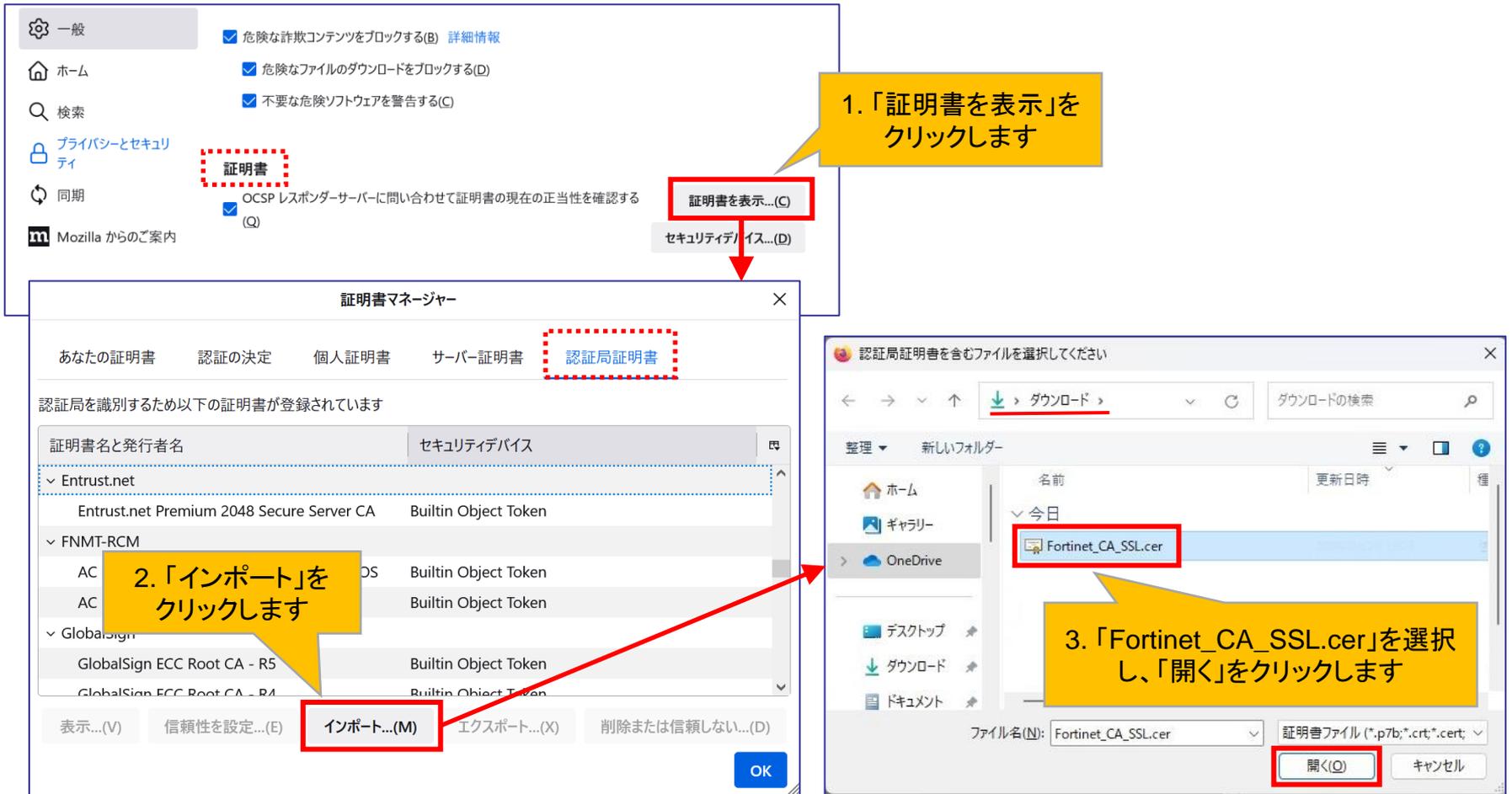
5.「認証局証明書」でFortinetの証明書が表示されていれば設定完了しています。

表示されている場合は、15ページの手順へ進んでください。

表示されていない場合は、次の手順へ進んでください。

3-2-3 CA証明書の導入 Firefox()を使用する場合

「認証局証明書」にFortinetの証明書がない場合の設定方法



The image shows a sequence of steps to import a Fortinet CA certificate into Firefox. It starts with the Firefox settings page, where the 'Certificates' option is selected. A callout box points to the 'Certificates' link, stating: "1. 「証明書を表示」をクリックします" (Click 'Show Certificates').

Next, the 'Certificates' dialog box is shown, with the 'Certificates' tab selected. A callout box points to the 'Show Certificates' button, stating: "1. 「証明書を表示」をクリックします".

The 'Certificates' dialog box shows a list of certificates. A callout box points to the 'Import...' button, stating: "2. 「インポート」をクリックします" (Click 'Import').

The 'Import...' dialog box is shown, with the file 'Fortinet_CA_SSL.cer' selected. A callout box points to the 'Open' button, stating: "3. 「Fortinet_CA_SSL.cer」を選択し、「開く」をクリックします" (Select 'Fortinet_CA_SSL.cer' and click 'Open').

3-2-4 CA証明書の導入 Firefox()を使用する場合

証明書のインポート

新しい認証局 (CA) を信頼するよう求められています。本当にこの認証局を信頼しますか？

"FG201FT921908527" が行う認証のうち、信頼するものを選択してください。

この認証局によるウェブサイトの識別を信頼する

この認証局によるメールユーザーの識別を信頼する

認証局を信頼する場合はその目的に関わらず、認証局の証明書が間違いないこと、認証ポリシーや認証実施規定に問題がないことを確認してください。

証明書を表示 認証局の証明書を審査してください

OK キャンセル

4. 信頼するものとして、2項目にチェックを入れ、「OK」をクリックします

5. 「認証局証明書」で Fortinet の証明書が表示されていれば設定OKです

証明書マネージャー

あなたの証明書 認証の決定 個人証明書 サーバー証明書 認証局証明書

認証局を識別するため以下の証明書が登録されています

| 証明書名と発行者名 | セキュリティデバイス |
|---|--------------------------|
| Entrust.net Premium 2048 Secure Server CA | Builtin Object Token |
| ▼ FNMT-RCM | |
| AC RAIZ FNMT-RCM SERVIDORES SEGUROS | Builtin Object Token |
| AC RAIZ FNMT-RCM | Builtin Object Token |
| ▼ Fortinet | |
| FG201FT921908527 | Software Security Device |
| ▼ GlobalSign | |
| GlobalSign Root CA - R6 | Builtin Object Token |

表示...(V) 信頼性を設定...(E) **インポート...(M)** エクスポート...(X) 削除または信頼しない...(D)

OK

4. VPN接続方法

FortiClient - ゼロトラストファブリックエージェント
ファイル ヘルプ

FortiClient VPN

製品版にアップグレードすると、追加機能の利用やテクニカルサポートを受けることができます。

VPN名称 SUMS

SAMLログイン

1.「SAMLログイン」をクリックします
「接続」になっている場合もあります

国立大学法人
滋賀医科大学
SHIGA UNIVERSITY OF MEDICAL SCIENCE

多要素認証システム / Multi-Factor Authentication System

ユーザ名

パスワード

ログインを記憶しません

送信する情報を再度表示して送信の可否を選択します。

ログイン

2.ユーザ名、パスワードを入力し「ログイン」をクリックします

国立大学法人
滋賀医科大学
SHIGA UNIVERSITY OF MEDICAL SCIENCE

多要素認証システム / Multi-Factor Authentication System

認証方式を選択してください

FIDO or イメージングマトリクス

ワンタイムパスワード(TOTP)

3.多要素認証の処理を行ってください

FortiClient - ゼロトラストファブリックエージェント
ファイル ヘルプ

FortiClient VPN

製品版にアップグレードすると、追加機能の利用

VPN接続済み

VPN名称 SUMS
IPアドレス 172.19.56.2
ユーザ名 sum159
期間 00:02:30
受信バイト 1.14 MB
送信バイト 216.72 KB

切断

4.VPN接続済みになれば、設定完了です
接続できない場合は、7ページの手順をご確認ください

5. VPNの切断

