

VPN クライアント導入/設定 (Windows)

2025/2/6






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接続できない時は...
6. 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>

The screenshot shows the FortiClient VPN download page. On the left, under 'Remote Access', there are two options: 'SSL VPN with MFA' and 'IPSEC VPN with MFA', both marked with a green checkmark. The main content area displays download links for various operating systems: Windows, macOS, Linux, iOS, and Android. The 'Windows' link is highlighted with a red box. A yellow callout box with a speech bubble points to the 'DOWNLOAD' button for Windows, containing the following text:

＜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

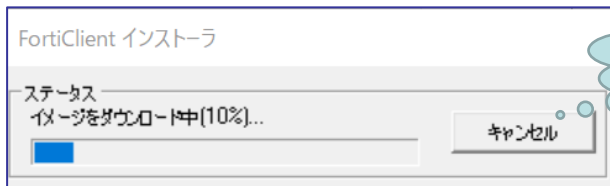
An inset image shows the next step in the process, where the user is prompted to download the installer. It features a 'Downloaded...' status with a green checkmark and a button labeled 'Install Now'. Below this, there is a 'Learn More' section with a 'SUBMIT' button.

1-1. FortiClient VPN導入

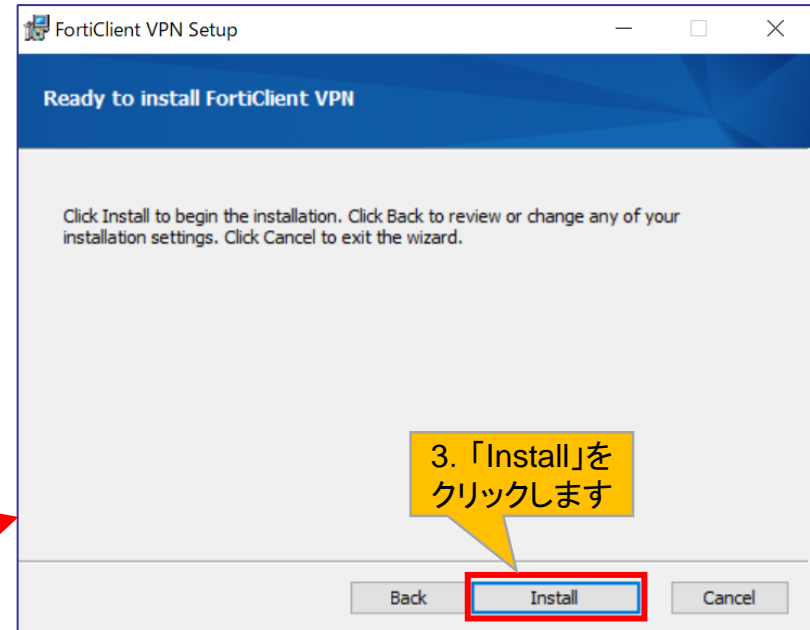
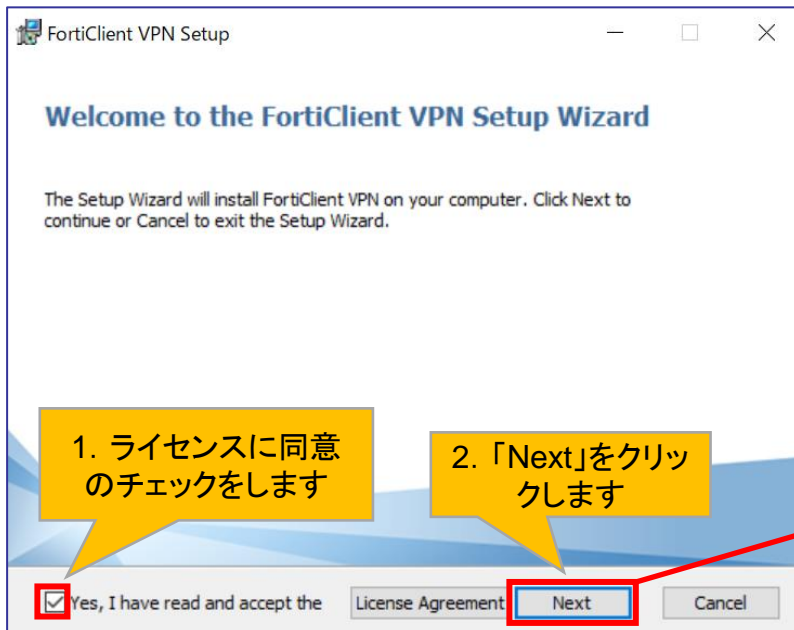
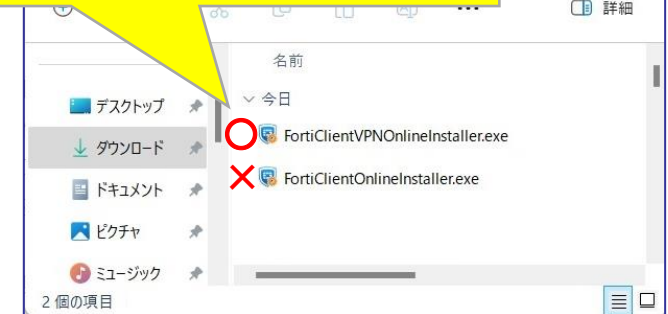
ダウンロードされた以下のファイルを
ダブルクリックしてください。

FortiClientVPNOnlineInstaller.exe

＜注意＞
ダウンロードしたファイル名が
正しいことを確認してください
FortiClientOnlineInstaller.exe は、
別のアプリケーションです。

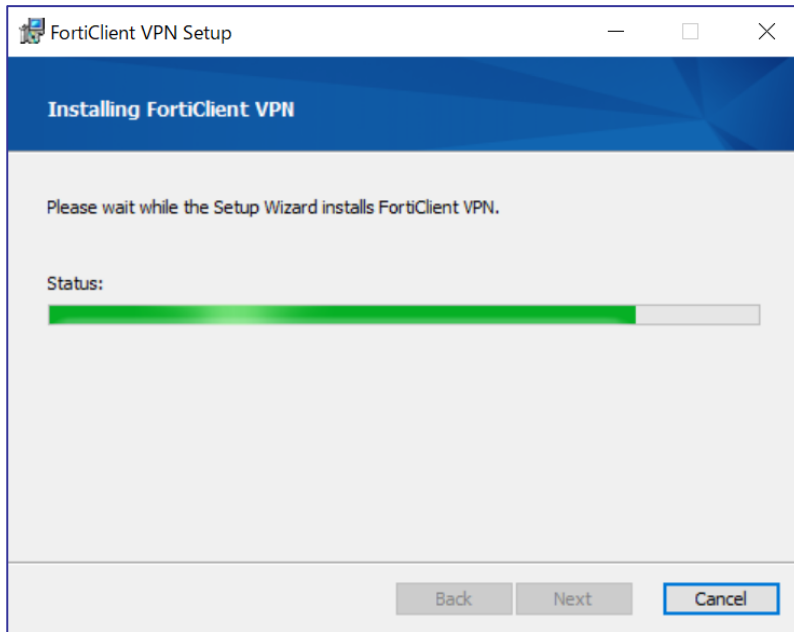


ダウンロードに時間
がかかります

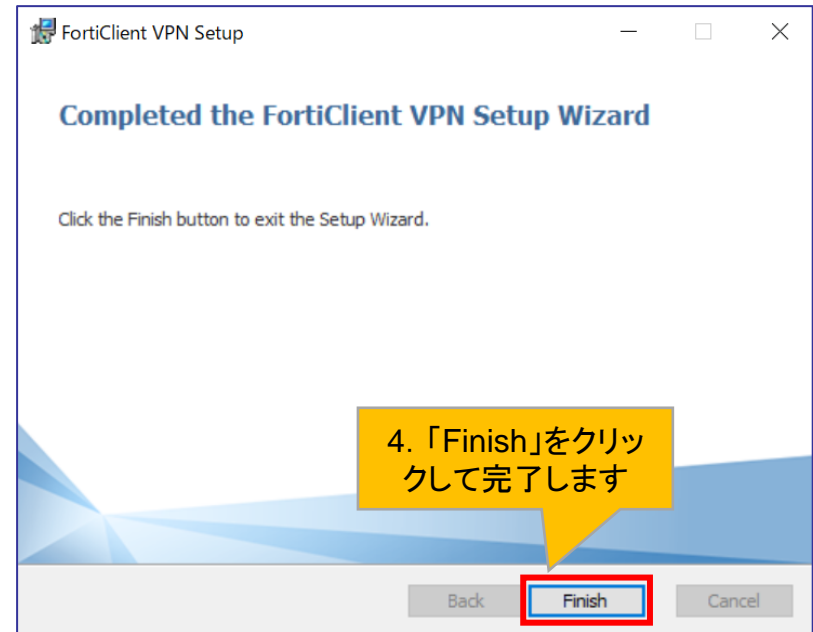


1-2. FortiClient VPN導入

導入中

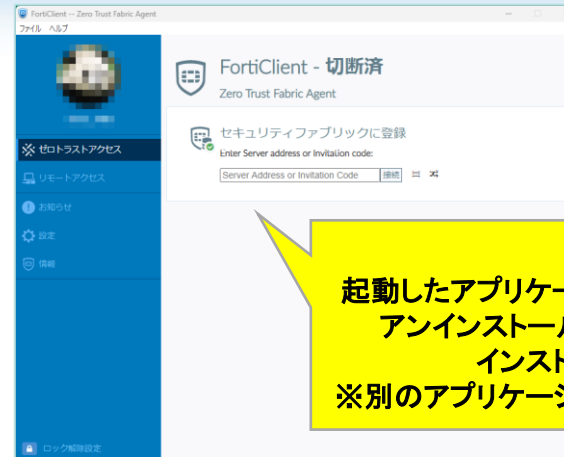


導入完了

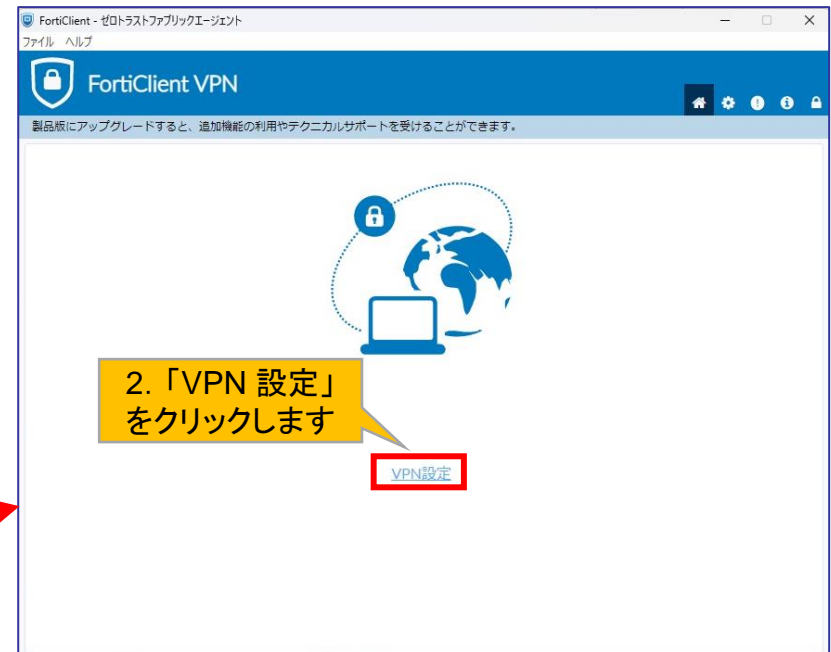


2-1 VPNの初期設定

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

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。

新規VPN接続

VPN

接続名

説明

リモートGW

ポートの編集

VPNトンネルのシングルサインイン (SSO) を有効化

クライアント証明書

キャンセル 保存

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

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

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

SAMLログイン

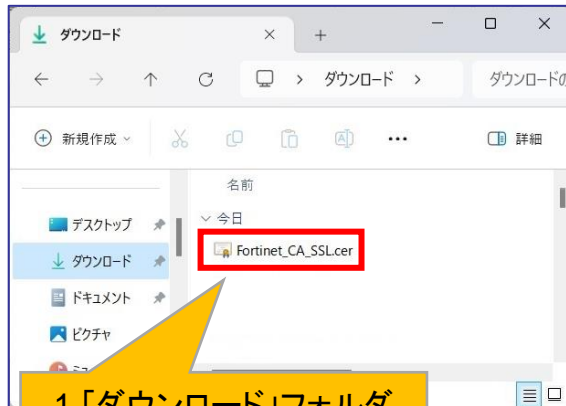
引き続き、ご利用のブラウザ環境に合わせて、次ページからの証明書導入を行ってください

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)

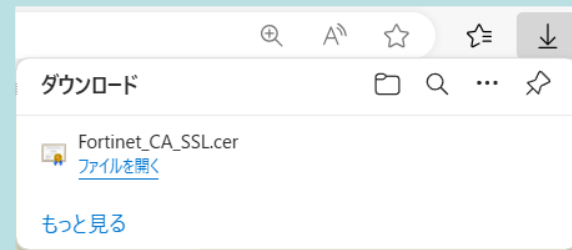
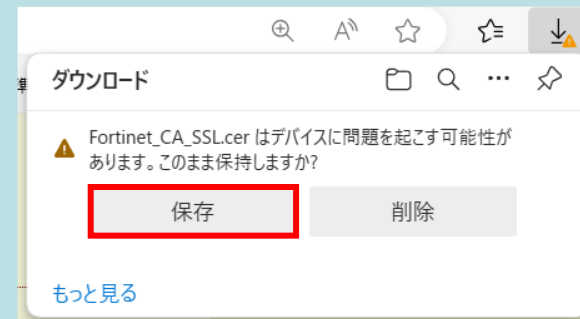
https://www.shiga-med.ac.jp/mmc/service/vpn/Fortinet_CA_SSL.cer



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

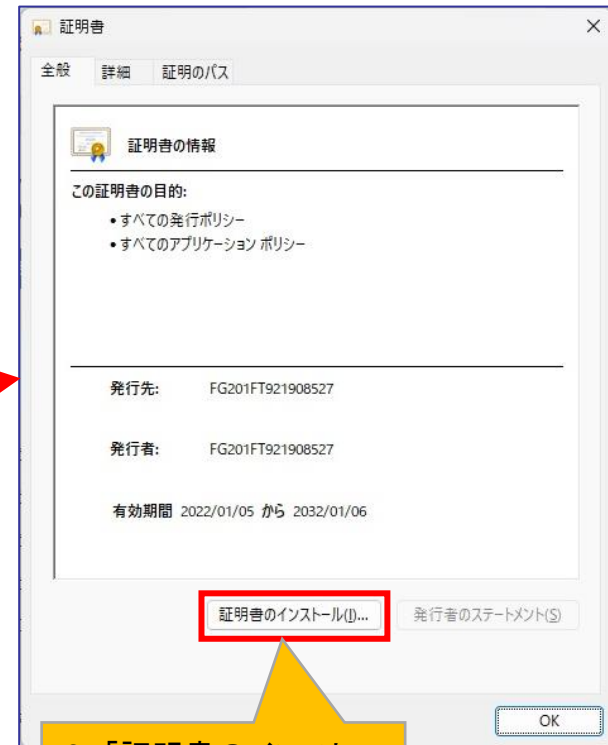
下記の表示が出た場合は、「保存」をクリックしてください。



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

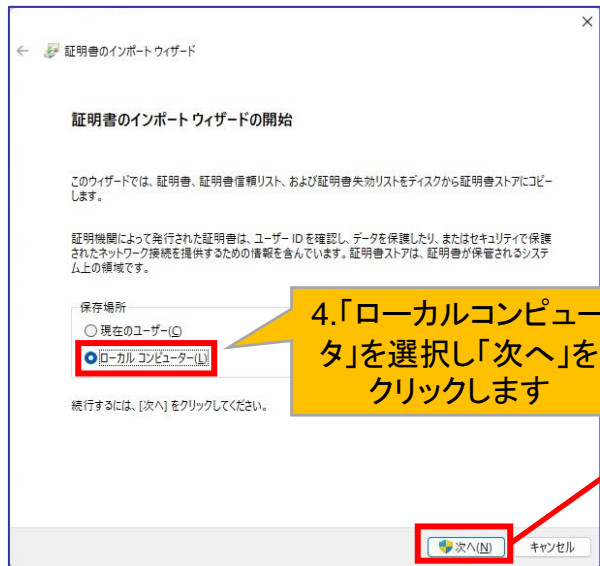
2. 「このファイルを開きますか?」で「開く」をクリックします



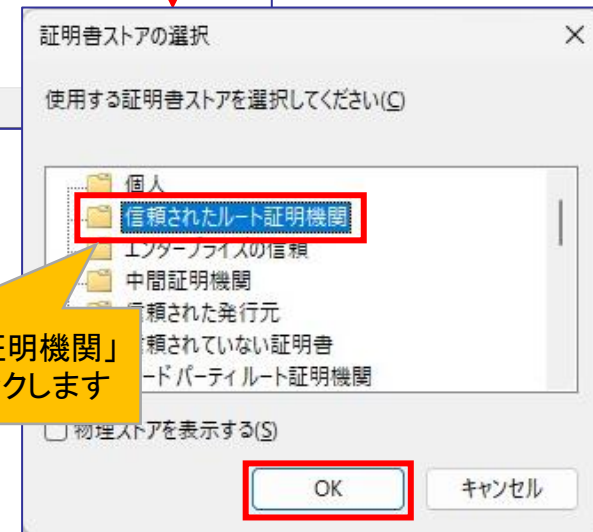
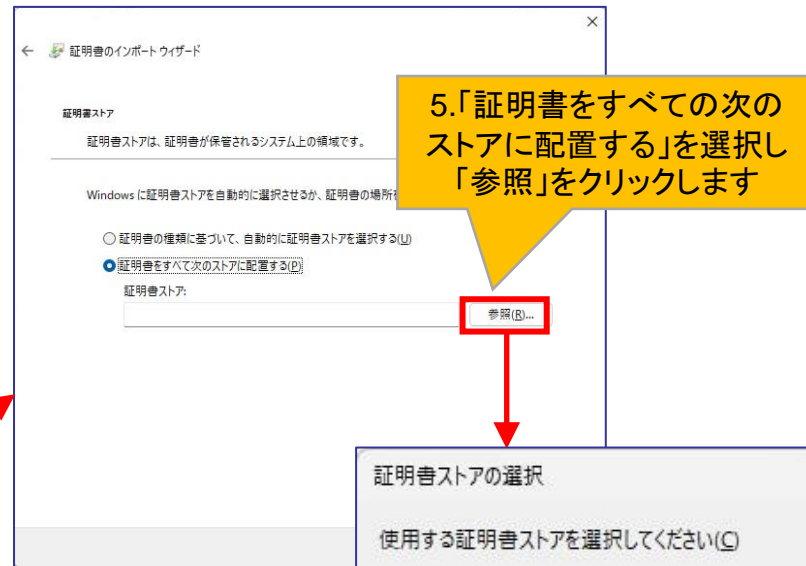
3. 「証明書のインストール」をクリックします

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

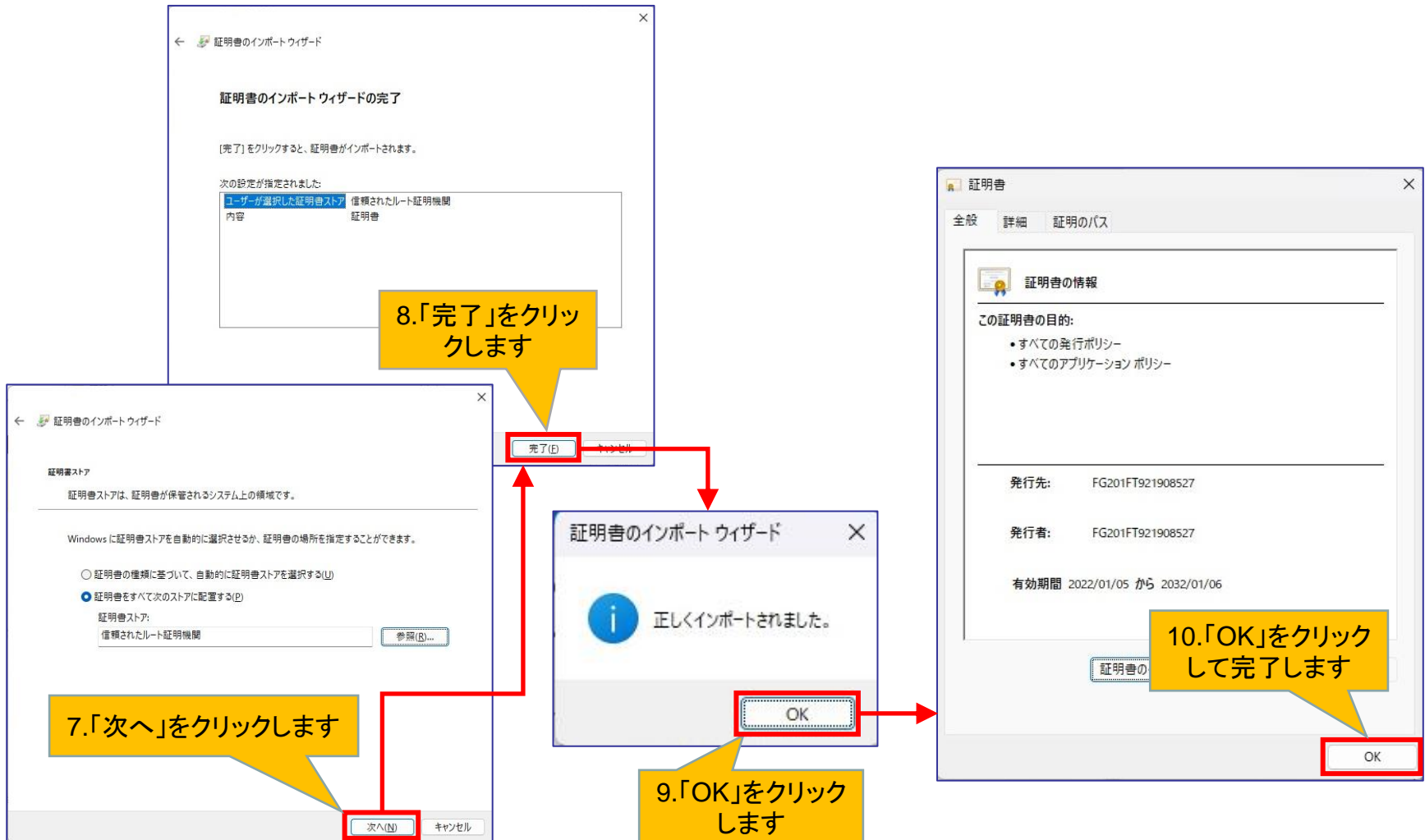


※ユーザーアカウント制御画面が表示されたら、「はい」をクリックします。



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



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 Firefox browser window with three numbered steps for accessing the settings to import a CA certificate:

- 1. ☰ をクリックします** (Click the menu button): A red box highlights the menu button (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 background shows the Firefox settings page with the "プライバシーとセキュリティ" (Privacy & Security) section selected.

3-2-2 CA証明書の導入 Firefox()を使用する場合

一般

- ☒ 危険な詐欺コンテンツをブロックする(B) [詳細情報](#)
- ☒ 危険なファイルのダウンロードをブロックする(D)
- ☒ 不要な危険ソフトウェアを警告する(C)

ホーム

検索

プライバシーとセキュリティ

同期

Mozilla からのご案内

証明書

- ☒ OSCP レスポンダーサーバーに問い合わせで証明書の現在の正当性を確認する(Q)

HTTPS-Only モード

HTTPS は Firefox とあなたが訪れるウェブサイトは HTTPS に対応しており、HTTPS-Only モードで接続されます。

証明書を表示...(C)

セキュリティデバイス...(D)

4.「証明書を表示」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。

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

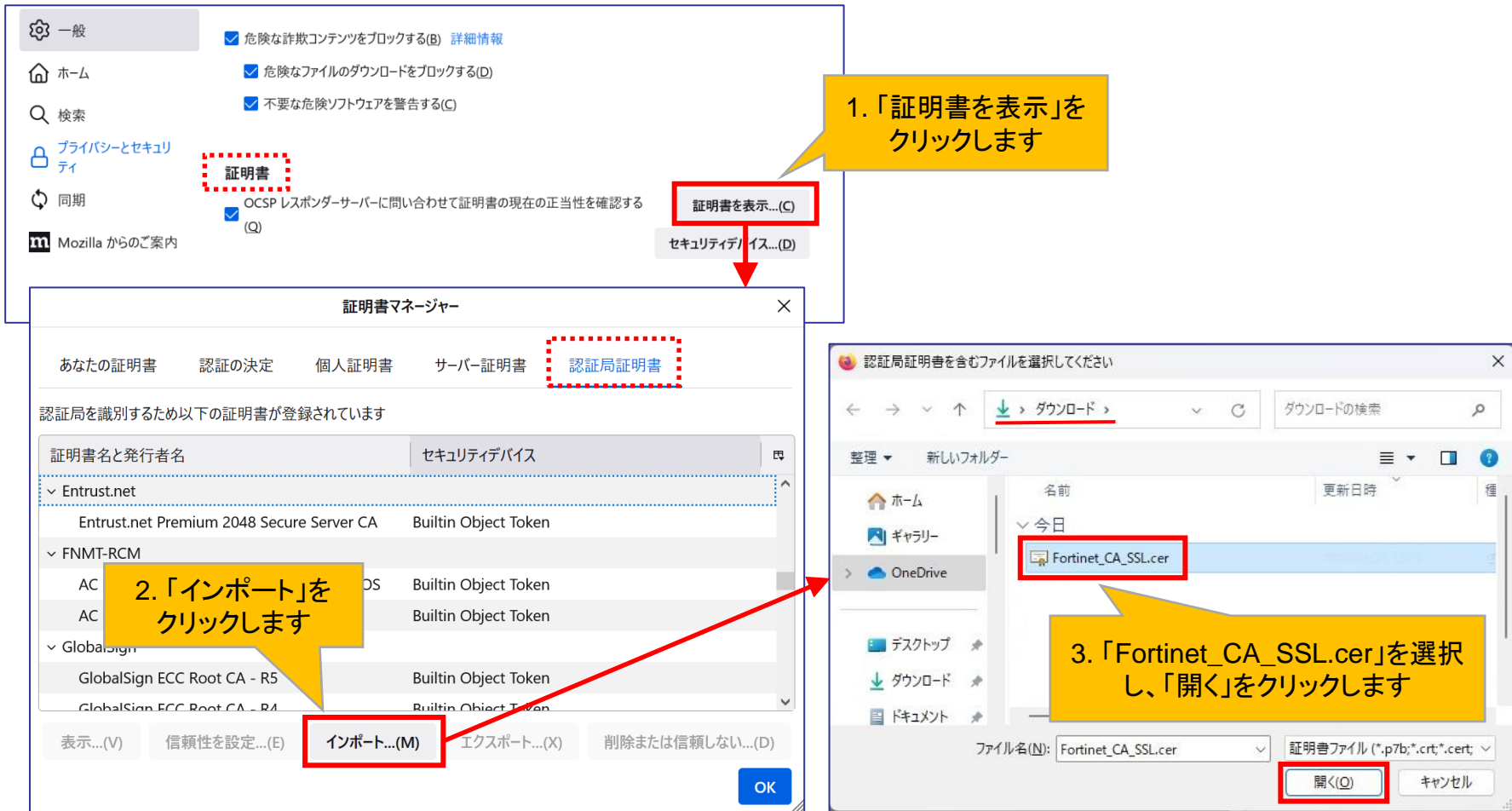
証明書名と発行者名	セキュリティデバイス
AC RAIZ FNMT-RCM	Builtin Object Token
▼ Fortinet	
FG201FT921908527	Software Security Device
▼ GlobalSign	
GlobalSign ECC Root CA - R5	Builtin Object Token
GlobalSign ECC Root CA - R4	Builtin Object Token
GlobalSign Root CA - R6	Builtin Object Token
GlobalSign Root CA - R3	Builtin 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

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 menu, where the 'Certificates' option is selected. Then, the 'Certificates' window is shown, where the 'Certificates' tab is active. A list of certificates is displayed, and the 'Import...' button is highlighted. Finally, a file selection dialog is shown, where the file 'Fortinet_CA_SSL.cer' is selected and the 'Open' button is clicked.

1. 「証明書を表示」をクリックします

2. 「インポート」をクリックします

3. 「Fortinet_CA_SSL.cer」を選択し、「開く」をクリックします

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

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

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

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

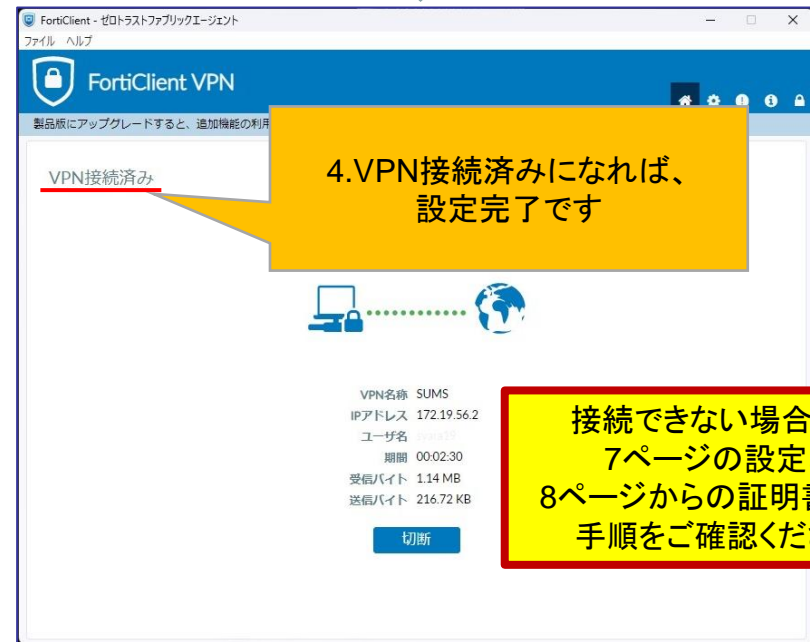
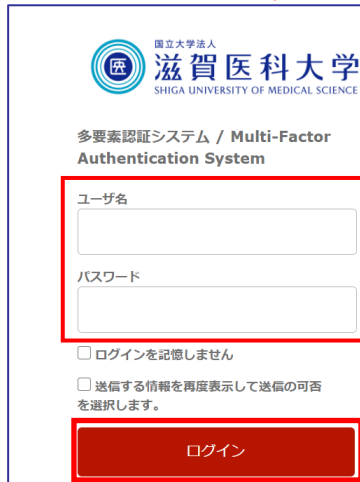
認証局を識別するため以下の証明書が登録されています

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

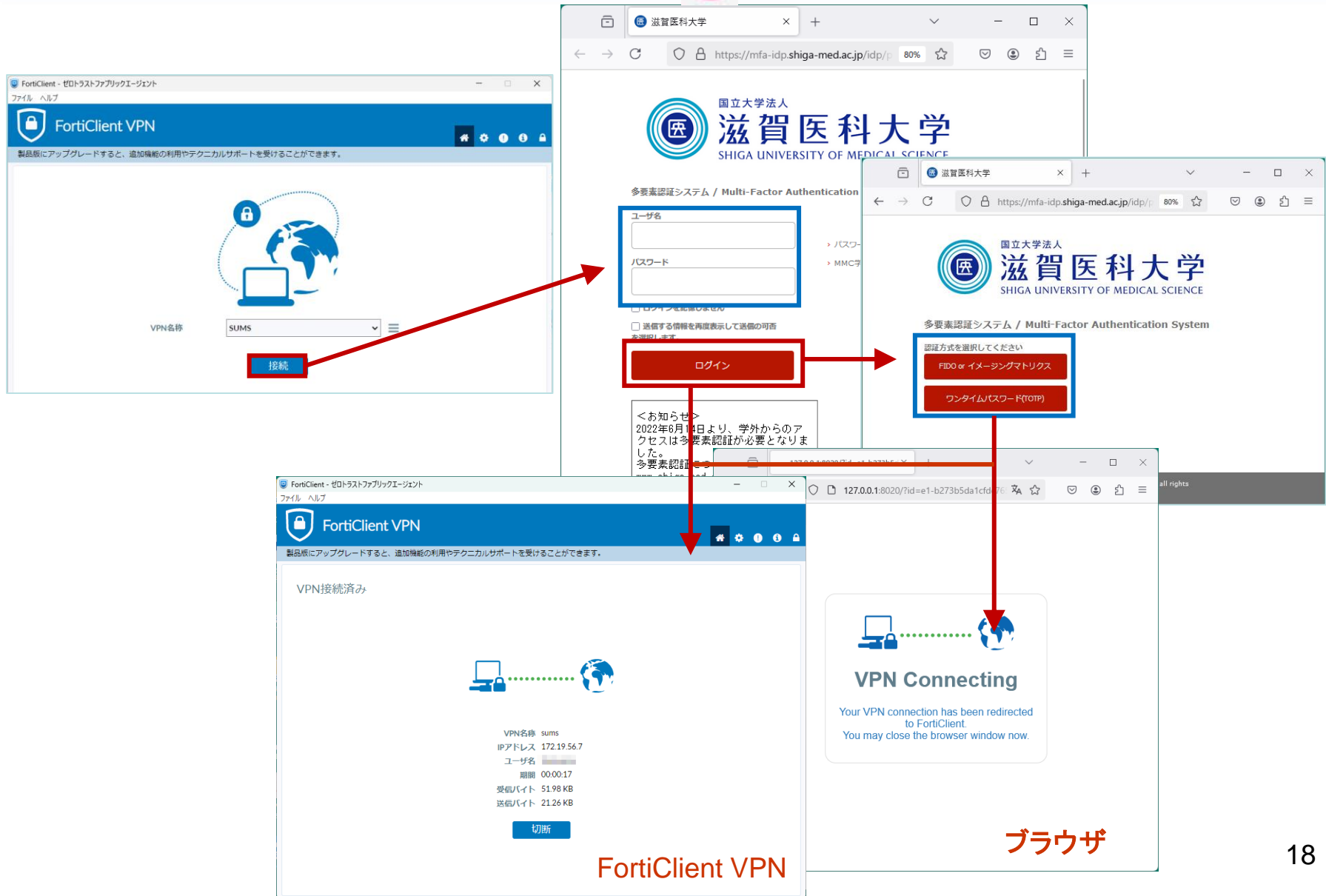


5. VPN接続できない時は... —多要素認証画面が表示されない場合—

ユーザー認証をブラウザ(edge  ・Chrome  ・Firefox )で行う



FortiClientにログインすると、ブラウザ(例: )でユーザー認証画面が表示されます。



6. VPNの切断

