

# VPN クライアント導入/設定 (Mac – 10.15, 11以上)

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 **Mac 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

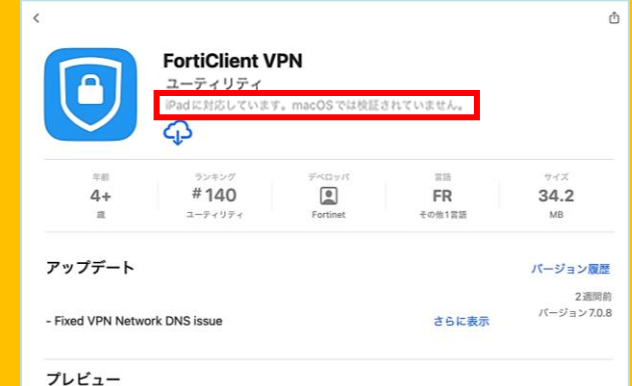
## 4. VPNの接続

## 5. VPN接続できない時は...

## 6. VPNの切断

### 注意

App StoreのFortiClient VPNは  
macOSでは検証されていません。  
公式サイトよりダウンロードしてください。



# 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 checked items: 'SSL VPN with MFA' and 'IPSEC VPN with MFA'. In the center, there are download buttons for Windows, Mac, Linux, iOS, and Android. The 'Mac' button is highlighted with a red rectangle. A yellow callout box with the 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Dock内のFortiClientVPN\_OnlineInstaller.dmgがあることを確認してください' points to the Mac download button. Below the callout, a download progress overlay is visible, showing 'Downloaded...' with a green checkmark and an 'Install Now' button. On the right, there is a 'Learn More' section with a 'SUBMIT' button.

**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 multi devices.

**Remote Access**

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

Download VPN for Windows

Download VPN for Mac OS

Download VPN for Linux

Download VPN for iOS

Download VPN for Android

**DOWNLOAD**

**DOWNLOAD**

**DOWNLOAD .rpm**

**DOWNLOAD**

**DOWNLOAD**

**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Dock内のFortiClientVPN\_OnlineInstaller.dmgがあることを確認してください**

**FortiClientVPN\_OnlineInstaller.dmg**

**Downloaded...**

**Install Now**

**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

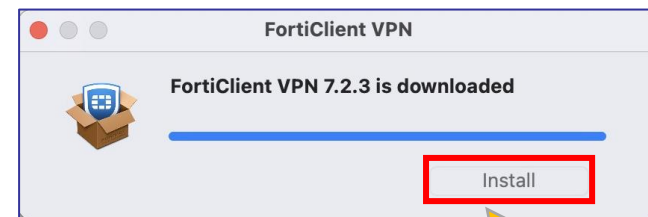
☐ I consent to receive promotional communications (which may include phone, email, and social) from Fortinet. I understand I may proactively opt out of communications with Fortinet at anytime.

**SUBMIT**

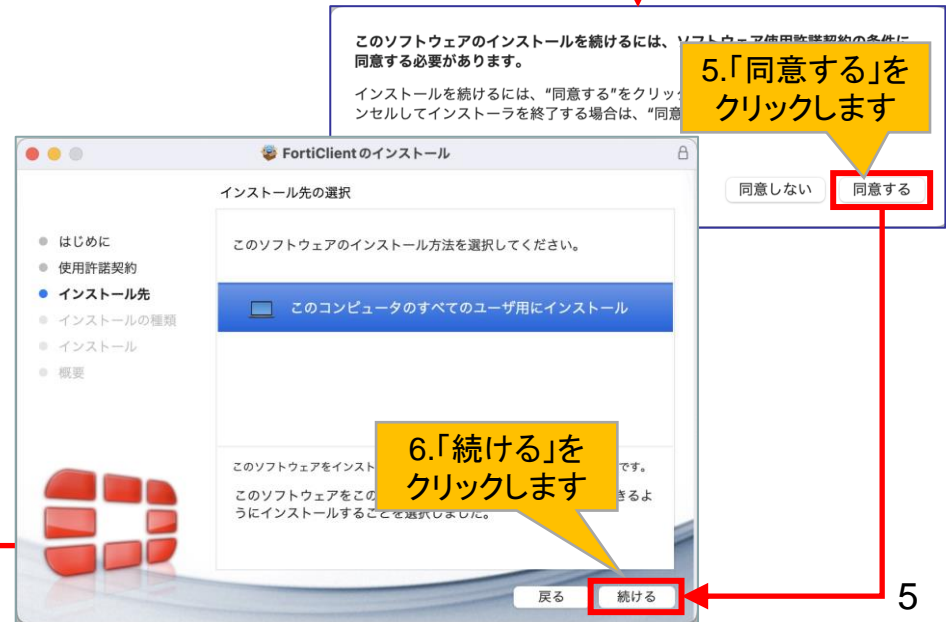
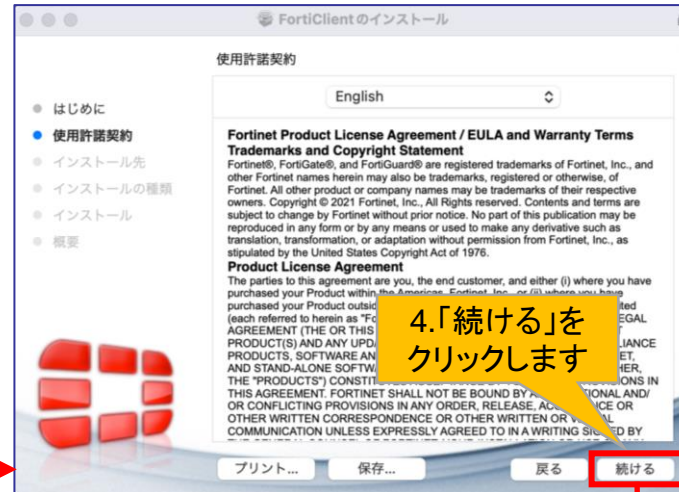
# 1-1 FortiClient VPN導入

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。

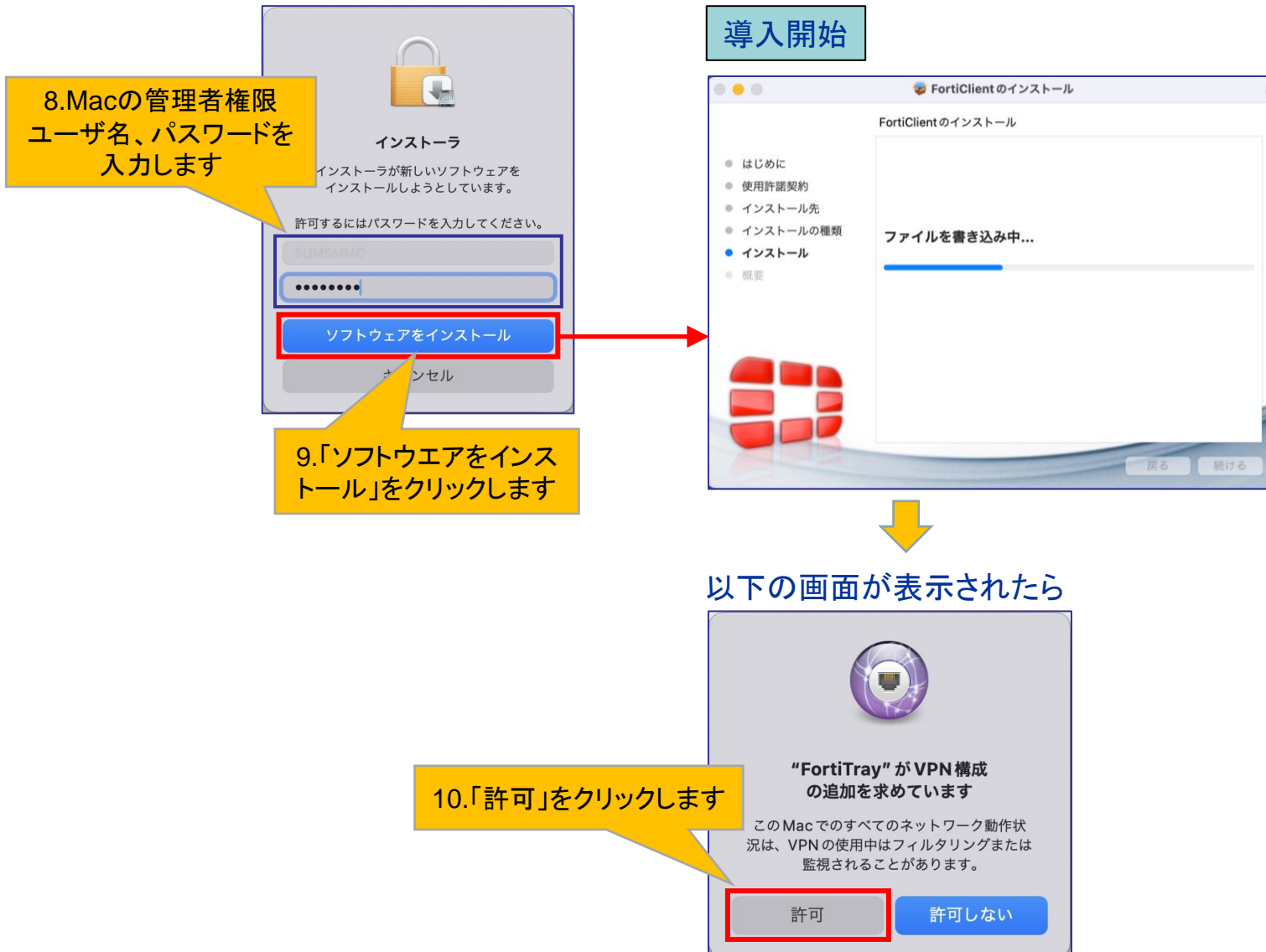
FortiClientVPNOnlineInstaller.dmg  
→FortiClientInstaller



## 1-2 FortiClient VPN導入

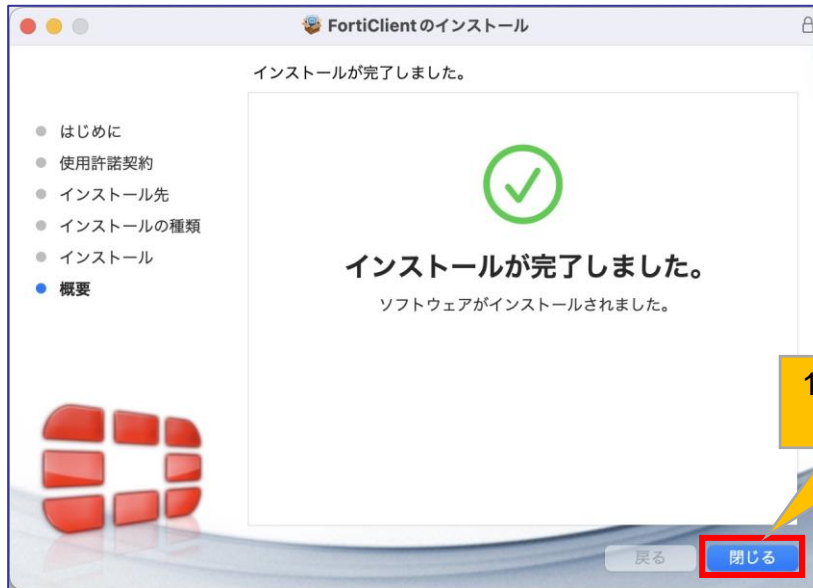


## 1-3 FortiClient VPN導入



## 1-4 FortiClient VPN導入

導入完了

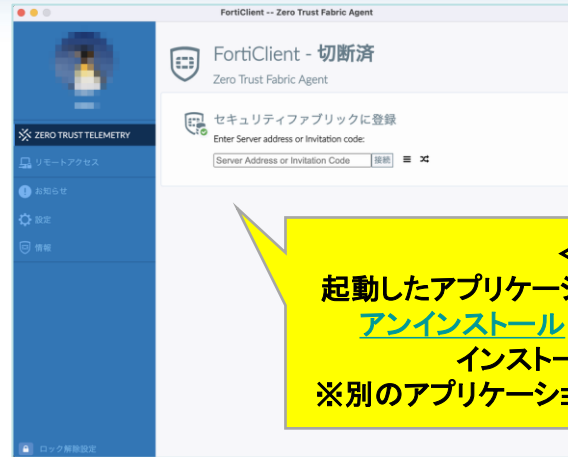


11.「閉じる」をクリックします

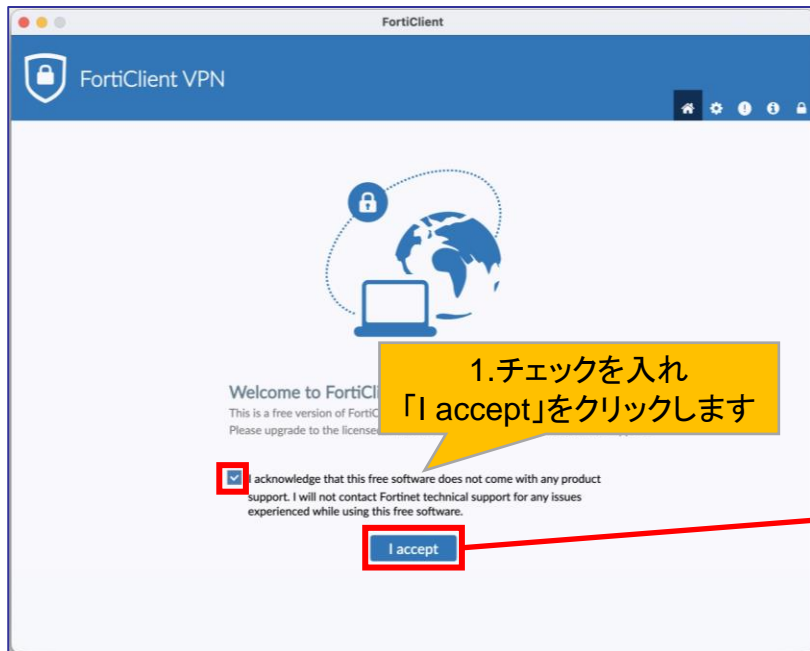


## 2-1 VPNの初期設定

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



1.チェックを入れ  
「I accept」をクリックします



2.「VPN 設定」を  
クリックします



## 2-2. VPNの初期設定

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

新規VPN接続

VPN

接続名

説明

リモートGW

クライアント証明書

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

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 VPN

Upgrade to the full version to access additional features and receive technical support.

VPN名称

SAML Login

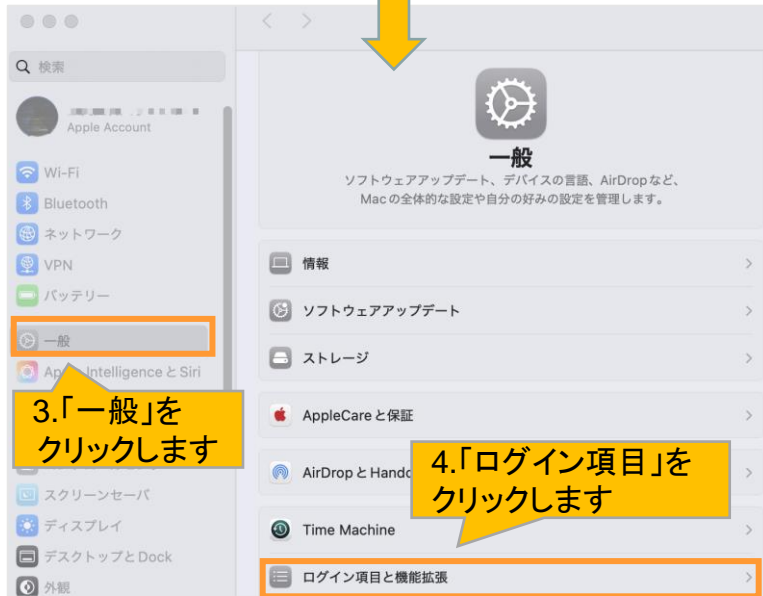
# ポイント macOS 15 Sequoia ネットワーク拡張機能の設定

macOS 15 Sequoiaの場合は以下のネットワーク拡張機能の設定を行ってください。

1.クリックします



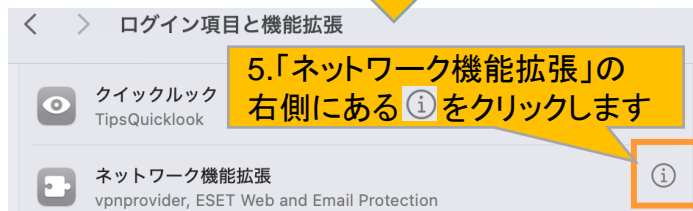
2.「システム設定」をクリックします



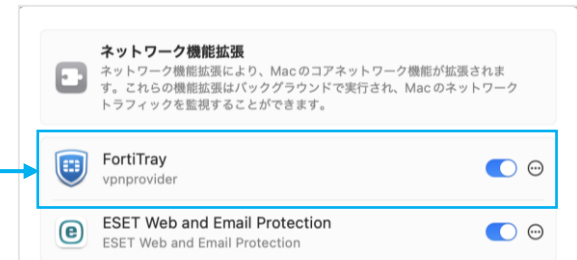
3.「一般」をクリックします

4.「ログイン項目」をクリックします

5.「ネットワーク機能拡張」の右側にある ⓘ をクリックします



に表示が変わります



8.「完了」をクリックします

完了

6.右方向へスライドします



7. Macの管理者 (Macにログインする際) のパスワードを入力し、OKをクリックします



10

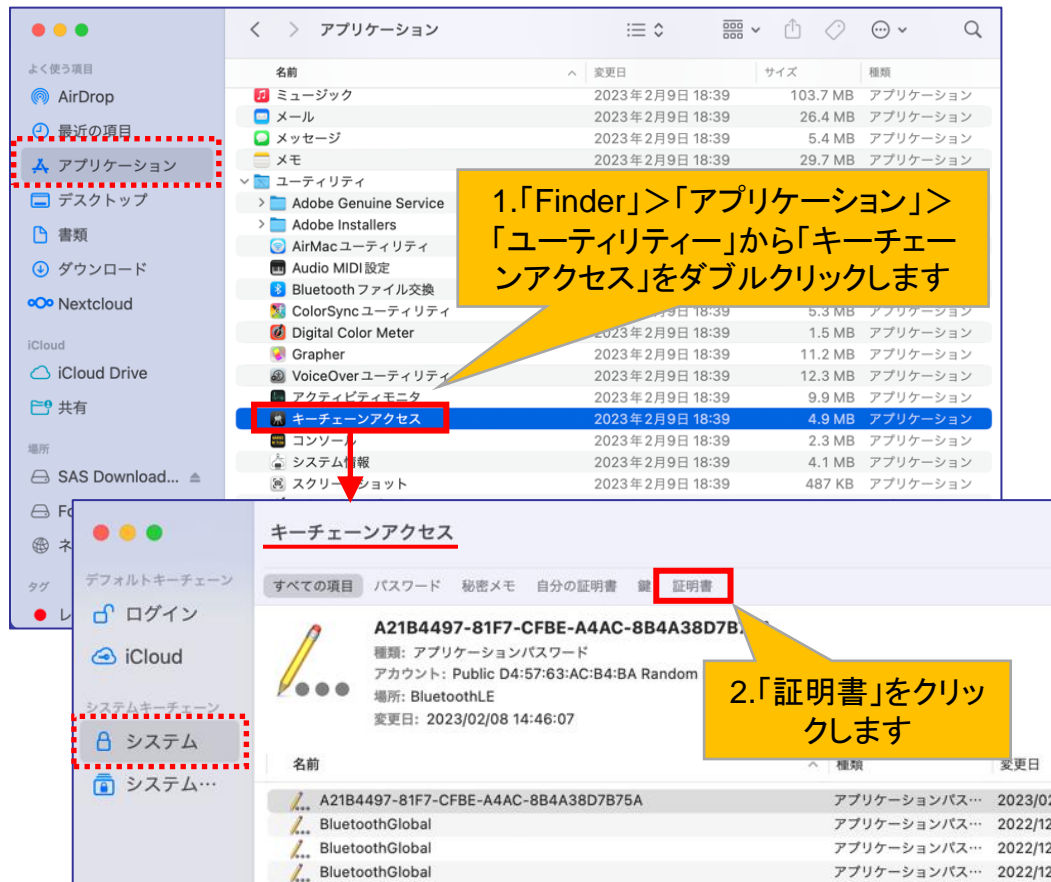
完了

### 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](https://www.shiga-med.ac.jp/mmc/service/vpn/Fortinet_CA_SSL.cer)



管理者のパスワードを求められれば  
Macの管理者パスワード入力ください

## 3-1-2 CA証明書の導入

Firefox以外のブラウザ(  や  )を使用する場合

キーチェーンアクセス

すべての項目 パスワード 秘密メモ 自分の証明書 鍵 証明書

デフォルトキーチェーン  
ログイン  
iCloud  
システムキーチェーン  
システム  
システム...

**4.「FG201\*\*\*\*\*」の証明書をダブルクリックします**

名前	種類	有効期限	キ
com.apple.kerberos.kdc	証明書	2041/03/28 6:39:28	シス
com.apple.systemdefault	証明書	2041/03/28 6:39:28	シス
<b>FG201FT921908527</b>	証明書	2032/01/06 10:11:07	シ

ルート認証局  
有効期限: 2032年1月6日 火曜日 10時11分07秒 日本標準時  
✖ このルート証明書は信頼されていません

**FG201FT921908527**

ルート認証局  
有効期限: 2032年1月6日 火曜日 10時11分07秒 日本標準時  
✖ このルート証明書は信頼されていません

**5.「信頼」の左側にある「>」をクリックします**

信頼

詳細な情報

組織 Fortinet  
部署 Certificate Authority  
通称 FG201FT921908527  
その他の名前 support@fortinet.com

発行者名

その他の名前 US  
その他の名前 California  
その他の名前 Sunnyvale  
組織 Fortinet  
部署 Certificate Authority  
通称 FG201FT921908527

**FG201FT921908527**

ルート認証局  
有効期限: 2032年1月6日 火曜日 10時11分07秒 日本標準時  
✖ このルート証明書は信頼されていません

信頼

この証明書を使用するとき: システムデフォルトを使用 ?

SSL (Secure Sockets Layer) 値が指定されていません

安全なメール (S/MIME) 値が指定されていません

拡張認証 (EAP) 値が指定されていません

IP Security (IPsec) 値が指定されていません

コード署名 値が指定されていません

タイムスタンプ 値が指定されていません

X.509 基本ポリシー 値が指定されていません

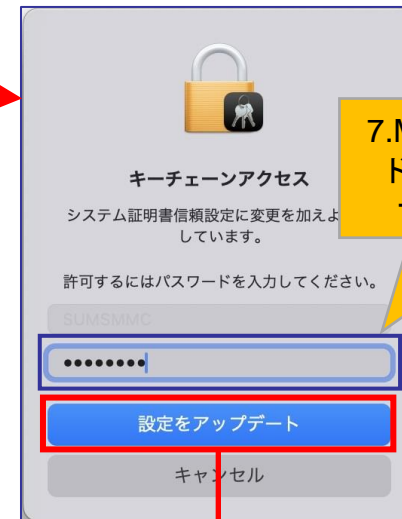
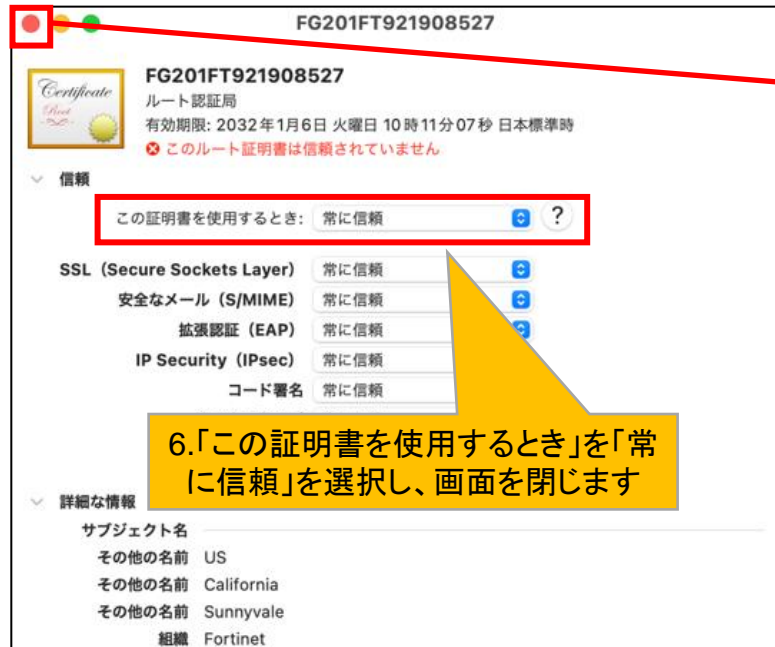
詳細な情報

サブジェクト名

その他の名前 US  
その他の名前 California  
その他の名前 Sunnyvale  
組織 Fortinet

### 3-1-3 CA証明書の導入

Firefox以外のブラウザ(  や  )を使用する場合



7. Macの管理者のパスワードを入力し「設定をアップデート」をクリックします



証明書が信頼されるものとなり完了です



## 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](https://www.shiga-med.ac.jp/mmc/service/vpn/Fortinet_CA_SSL.cer)



1. ☰ をクリックします

2. 「設定」をクリックします

3. 「プライバシーとセキュリティ」をクリックします

一般

ホーム

検索

プライバシーとセキュリティ

同期

Mozilla カスタマイズ

拡張機能とテーマ

Firefox サポート

起動

☐ 前回のウィンドウとタブを開く(S)

☐ Firefox が既定のブラウザーか確認

☒ Firefox は既定のブラウザーに

☒ 新しいウィンドウではなく新しいタブ

☐ リンク、画像、メディアを新しいタブで開く

☐ 同時に複数のタブを閉じる前に確認

☐ タスクバーにタブのプレビューを表示する

## 3-2-2 CA証明書の導入 Firefox( )を使用する場合

一般

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

☒ 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)

**証明書**

☒ OCSP 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)

**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
AC RAIZ FNMT-RCM	Built-in Object Token
▼ Fortinet	
FG201FT921908527	Software Security Device
▼ GlobalSign	
GlobalSign Root CA - R6	Built-in Object Token
GlobalSign Root CA - R3	Built-in Object Token

表示...    信頼性を設定...    読み込む...    書き出す...    削除または信頼しない...

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 three screenshots from the Firefox browser interface, illustrating the steps to import a Fortinet CA certificate when it is not listed in the built-in certificate authorities.

**Step 1:** In the Firefox Settings (General tab), the "Certificates" section is expanded. The "Certificates" link is highlighted with a red dashed box. A yellow callout bubble points to the "Certificates" link with the text: "1.「証明書を表示」をクリックします".

**Step 2:** The "Certificates" dialog box is shown. The "Certificates" tab is selected. The "Certificates" link is highlighted with a red dashed box. A yellow callout bubble points to the "Certificates" link with the text: "2.「読み込む」をクリックします".

**Step 3:** The "Certificates" dialog box is shown. The "Certificates" tab is selected. The "Certificates" link is highlighted with a red dashed box. A yellow callout bubble points to the "Certificates" link with the text: "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

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](#)

キャンセル

OK

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**

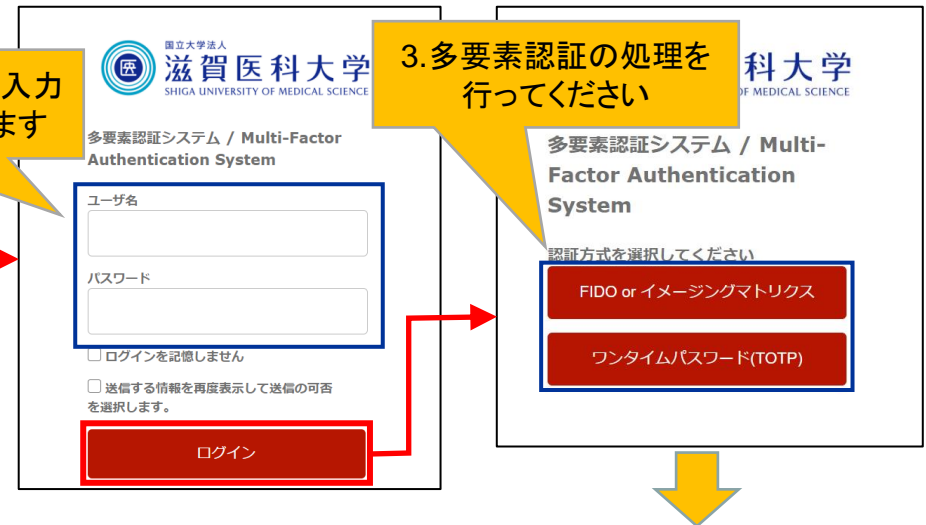
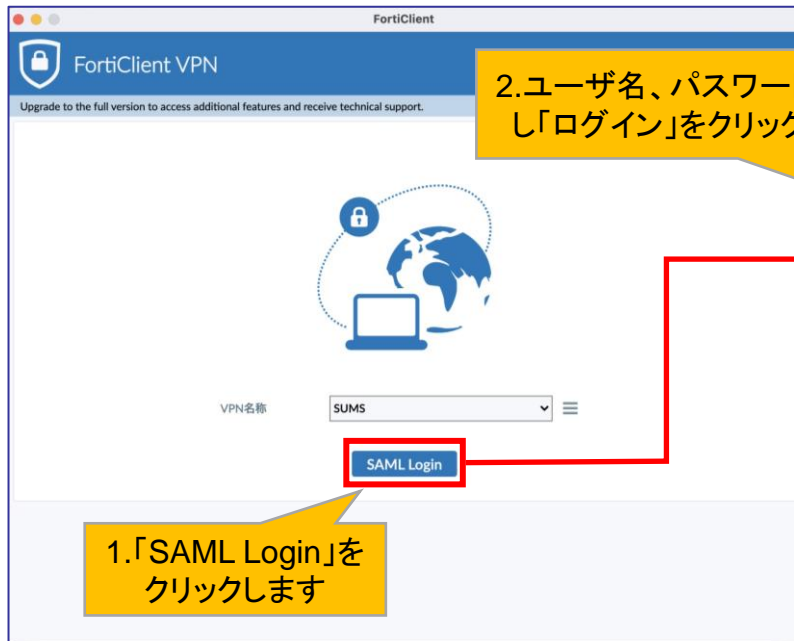
認証局を識別するため以下の証明書が登録されています

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

表示...    信頼性を設定...    読み込む...    書き出す...    削除または信頼しない...

OK

## 4. VPN接続方法



接続ができなかった場合は、  
次ページ以降の設定をしてください

## 5-1. VPN接続できない時は...

– Permission required for VPNが表示された時 –

**Permission required for VPN**

To connect to a VPN with FortiClient, open Security & Privacy Settings and allow system software from FortiTray.

1.「Open Security & privacy settings」をクリックします

表示されない場合は、5-2の手順へ

Cancel Open Security & Privacy Settings

**プライバシーとセキュリティ**

検索

アクセシビリティ  
コントロールセンター  
SiriとSpotlight  
プライバシーとセキュリティ  
デスクトップとDock  
ディスプレイ  
壁紙  
スクリーンセーバ  
バッテリー  
ロック画面

2.「プライバシーとセキュリティ」が表示されることを確認します

3.「アプリケーションのシステムソフトウェアの読み込みがブロックされました」の「許可」をクリックします

許可

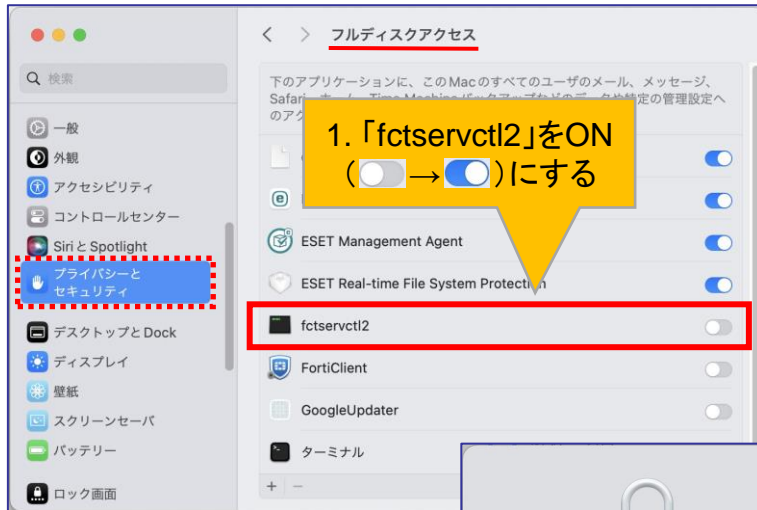
4. Macの管理者ユーザ名、パスワードを入力し「設定を変更」をクリックします

許可ボタンが表示されていない場合や、本ページ設定後もVPN接続できない場合は、次ページの設定を追加で行ってください。

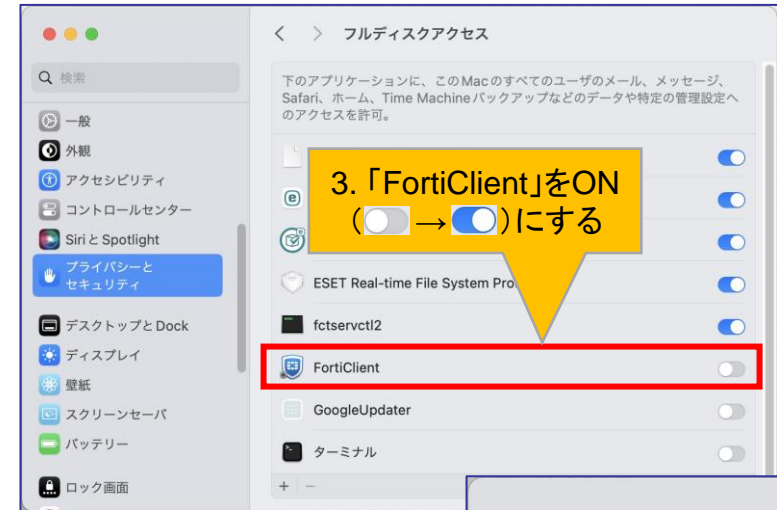
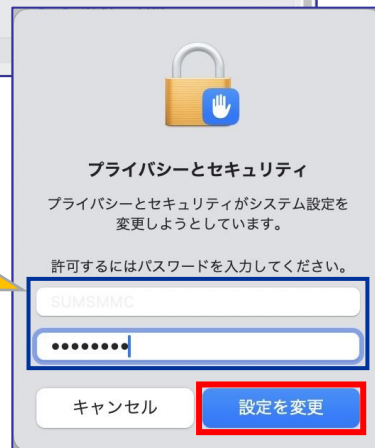
キャンセル 設定を変更

## 5-2. VPN接続できない時は... – フルディスクアクセスを設定する –

システム環境設定＞プライバシーとセキュリティ＞フルディスクアクセス



2. Macの管理者ユーザ名、パスワードを入力し「設定を変更」をクリックします



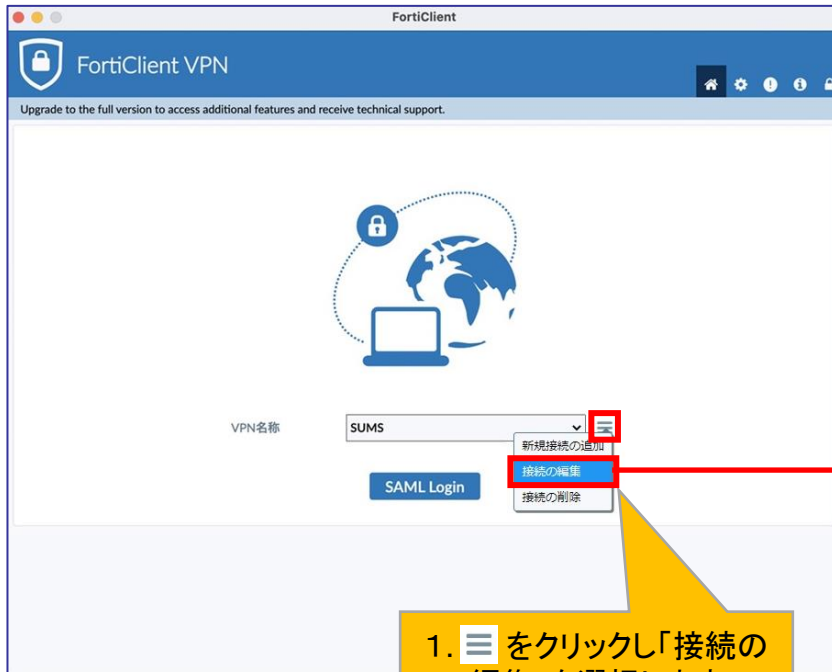
4. 「終了して再度開く」をクリックする



※FortiClientを起動していない場合は表示されません。

## 5-3-1. VPN接続できない時は...

– ユーザー認証をブラウザ(  や  や  )で行う –



1. [Menu Icon] をクリックし「接続の編集」を選択します



2. 「Use external browser as...」の項目にチェックを入れ、保存します

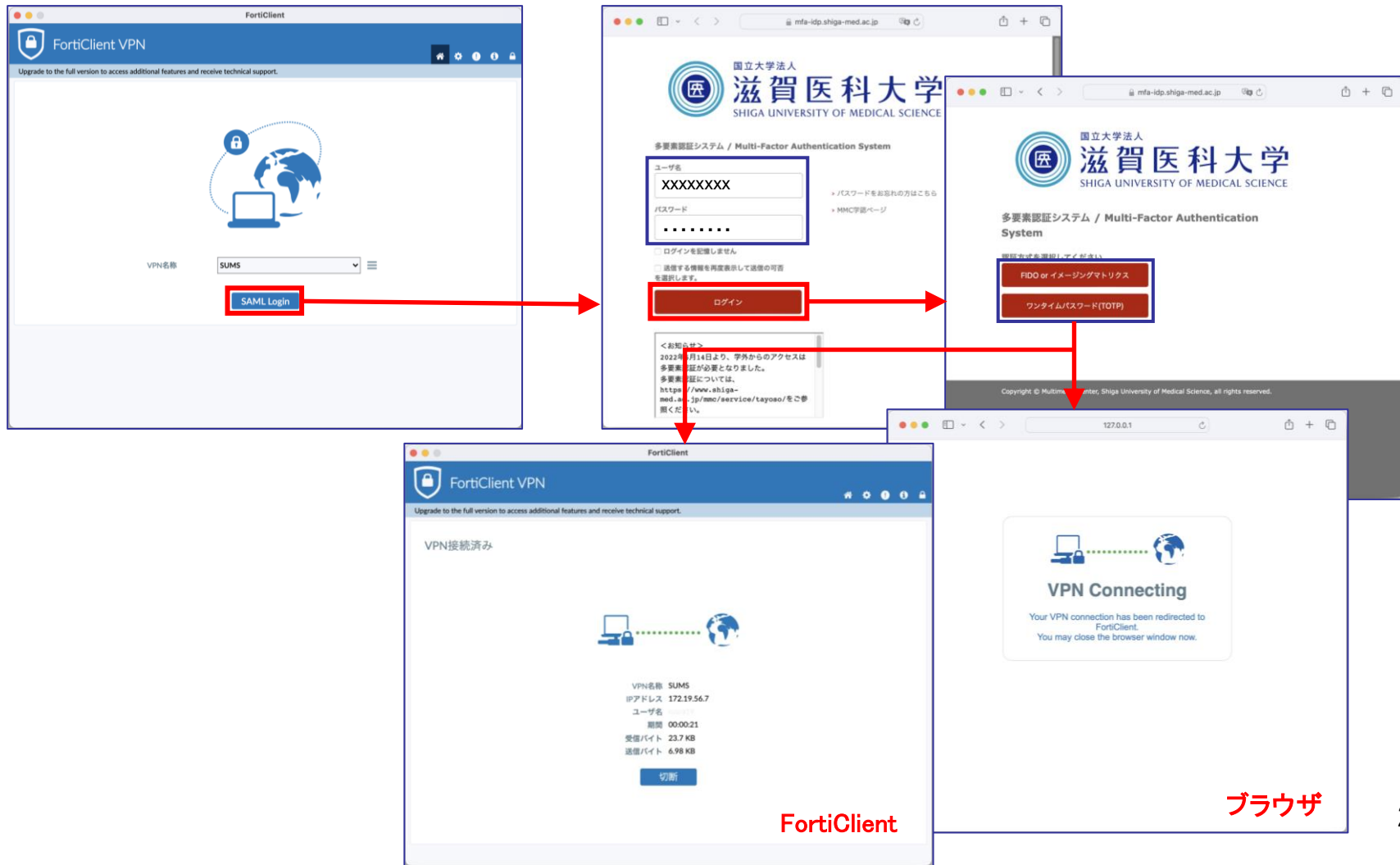
※あわせて9ページの設定をご確認ください。



## 5-3-2. VPN接続できない時は...

－ ユーザー認証をブラウザ(  や  や  )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

