

# セキュリティおまかせプラン クラウドプロキシ

## ユーザ操作マニュアル (ver1.2)

西日本電信電話株式会社 2024/04/01

# 目次

---

目次	開始スライド
<a href="#">改訂履歴</a>	3
<a href="#">はじめに</a>	4
<a href="#">対応OS</a>	5
<a href="#">インストール方法 (Windows・Mac)</a>	6
<a href="#">アンインストール方法 (Windows・Mac)</a>	22
<a href="#">インストール後の設定</a>	25
<a href="#">ソフトウェアの操作</a>	32
<a href="#">ソフトウェア使用上の注意</a>	37
<a href="#">管理コンソールへの初回ログイン</a>	46
<a href="#">Entitlement Codeの確認方法</a>	59

# 改訂履歴

No	Date	主な変更内容	Ver
1	2022/01/31	初版	1.0
2	2022/02/22	「目次」の記載を変更 「ETP Client使用上の注意」を追加	1.1
3	2024/04/01	目次の再編成 セクションの追加 「管理コンソールへのログイン」を追加 「Entitlement Codeの確認方法」を追加	1.2

## はじめに

---

本マニュアルはセキュリティおまかせプラン クラウドプロキシオプションを、ご利用されるために必要な手順や情報について記載しております。

まずはじめに下記URLのセキュリティおまかせプランのホームページより、最新の本マニュアルとセットアップツールをダウンロードのほどお願いいたします。

[https://www.ntt-west.co.jp/smb/security/security\\_omakase/](https://www.ntt-west.co.jp/smb/security/security_omakase/)

# 対応OS

---

セキュリティおまかせプラン クラウドプロキシオプションで使用するソフトウェアは、下記のOSに対応しております。記載のないOSについてはサポートしかねますのでご注意ください。

オペレーティングシステム	バージョン
Windows	11 10
Mac	Big Sur Monterey Ventura

## インストール方法

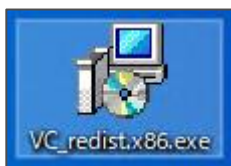
---

インストールは導入予定の端末OSを確認頂き、  
下記リンクより適切な方法のご利用をお願いいたします。

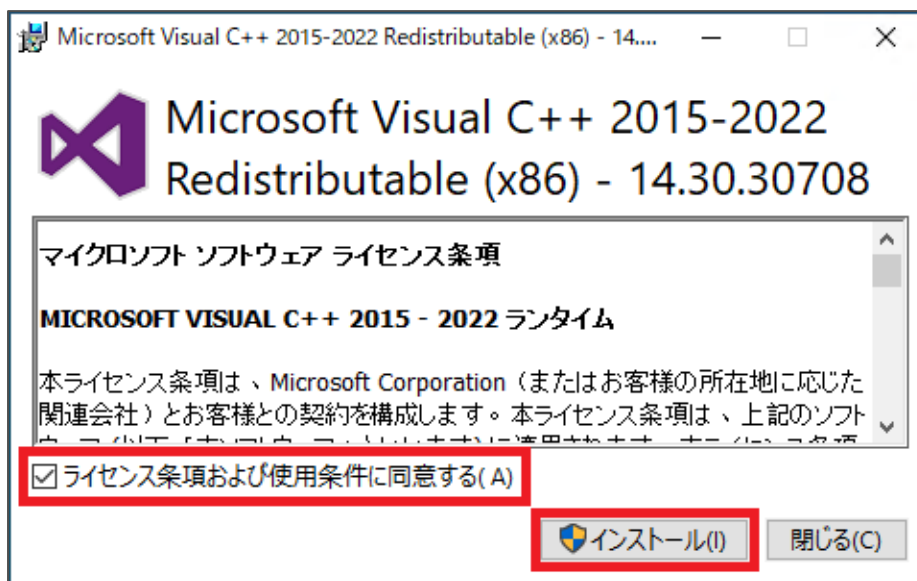
- [Windows](#)
- [MacOS](#)

# インストール方法

1. 配布されたパッケージファイルを解凍します。
2. パッケージから取り出したVC++再配布可能パッケージのインストーラを起動します。



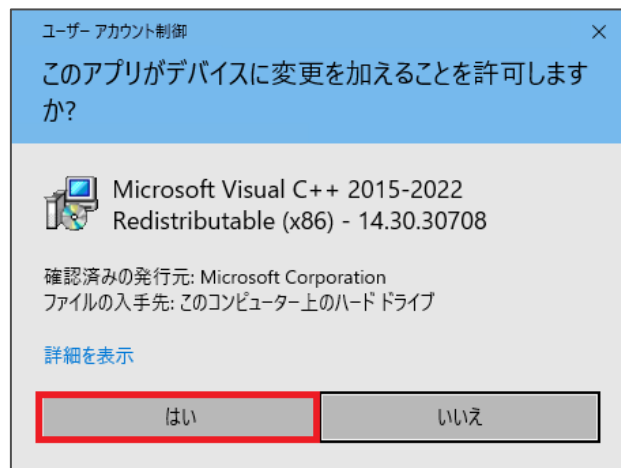
3. 「ETP Client」の前提ソフトウェアである「VC++再配布可能パッケージ」をインストールします。



「ライセンス条項および使用条件に同意する (A)」  
をチェックして、「インストール (I)」を押します。

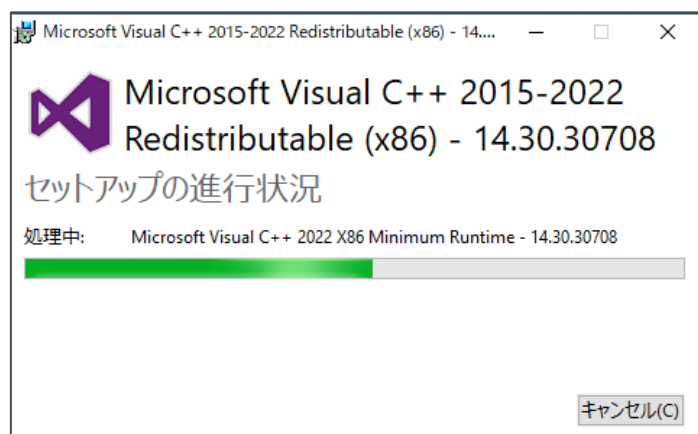
# インストール方法

4. ユーザアカウント制御イベントが出るので、「はい」を押します。



5. 「はい」を押すと、インストールが開始されます。

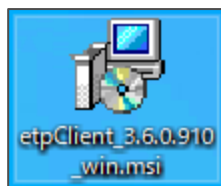
インストールが完了したら再起動を促されるので「再起動」を押して再起動してください。



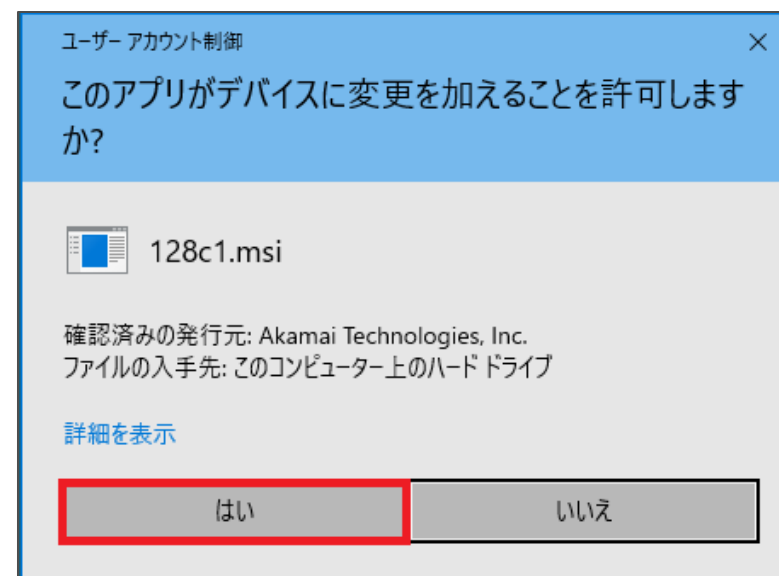
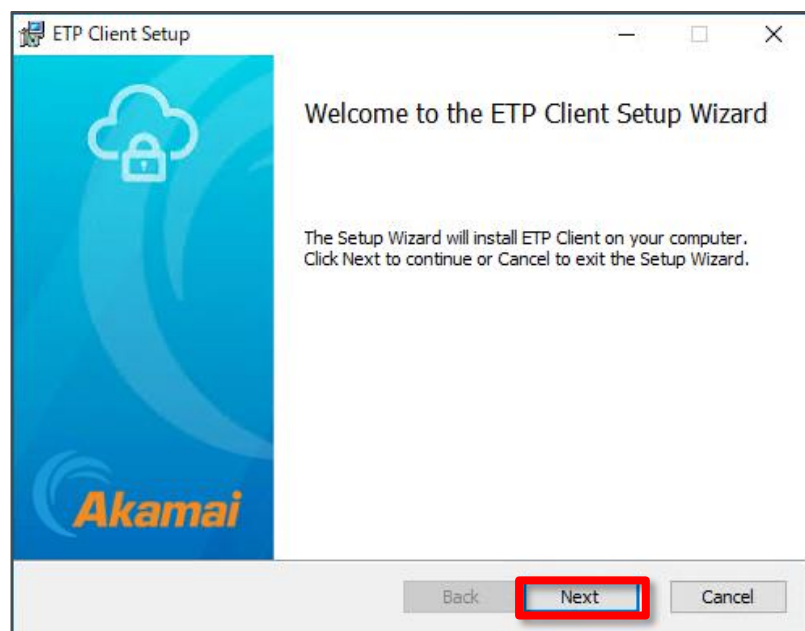


# インストール方法

6. パッケージから取り出したEtp Clientのインストーラを起動します。



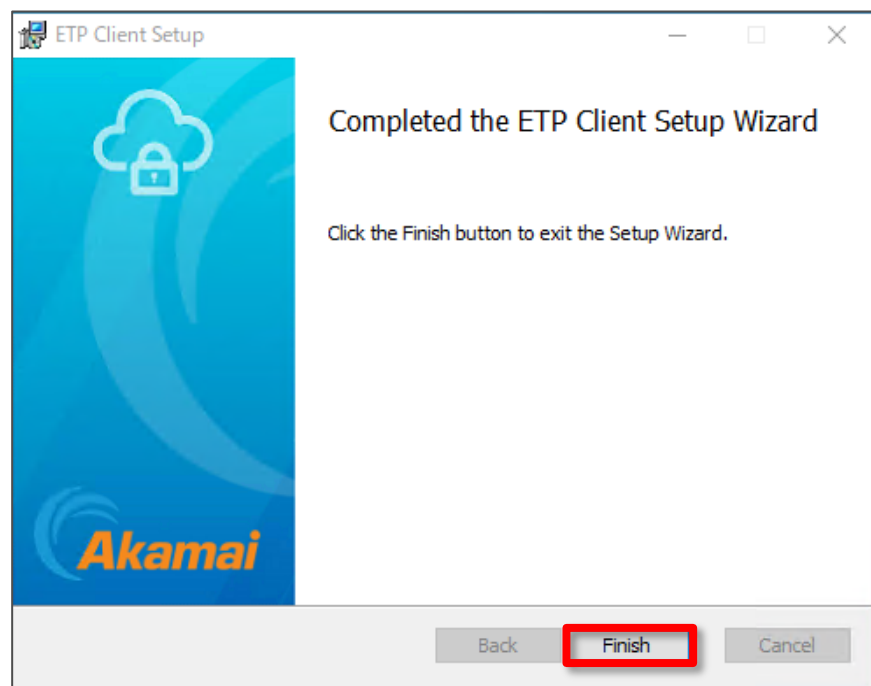
7. 「ETP Client」をインストールします。



「はい」を押します。

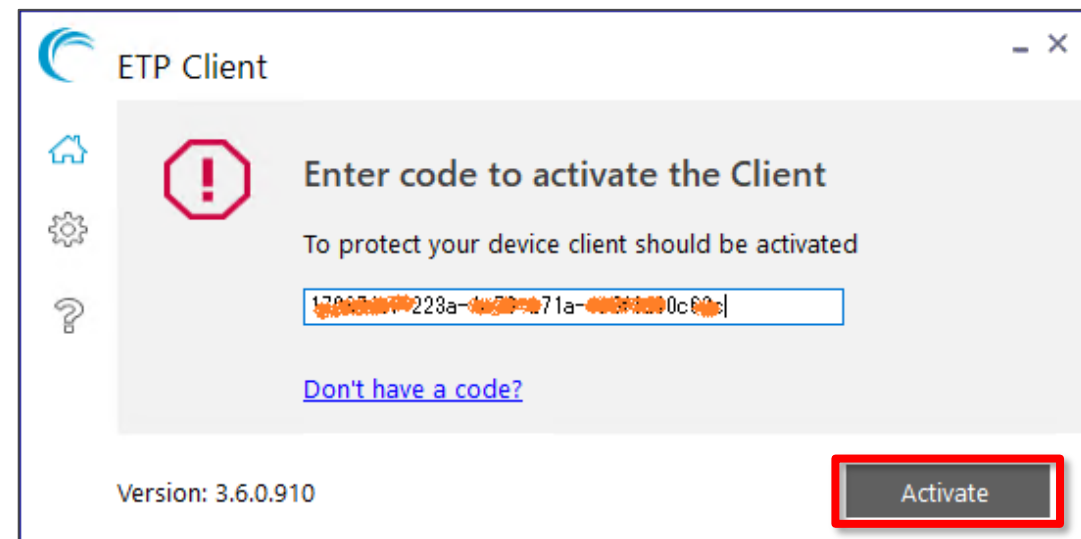
# インストール方法

8. インストールを完了して、別途メールにて代表者様に送付させていただいております、「Entitlement Code」を入力します。  
「Entitlement Code」の確認方法は[Entitlement Codeの確認方法](#)をご確認ください。



「Finish」を押します。

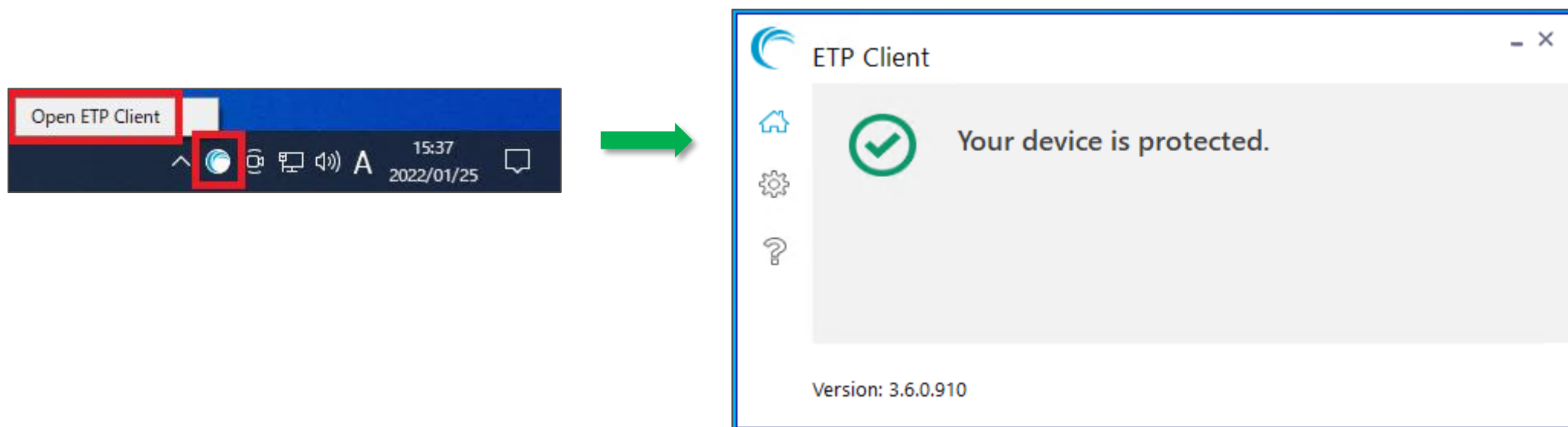
「ETP Client」が自動的に起動します。



「Entitlement Code」を入力して、「Activate」ボタンを押します。

# インストール方法

9. タスクトレイの「ETP Clientアイコン」を右クリックして「Open ETP Client」を選択します。

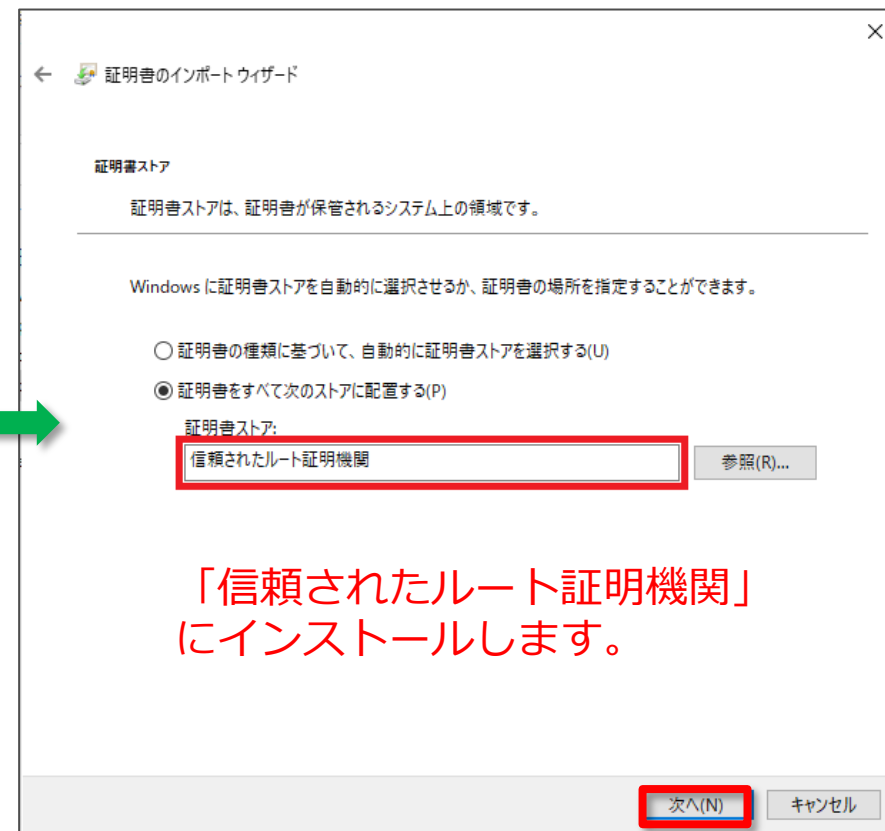
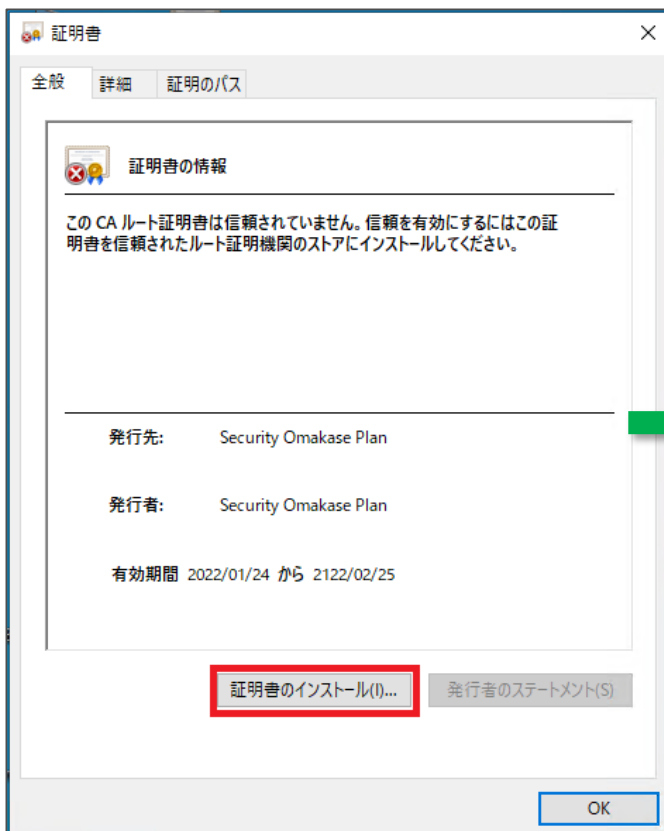


Your device is protected.  
になれば、ETPによる保護が有効です。

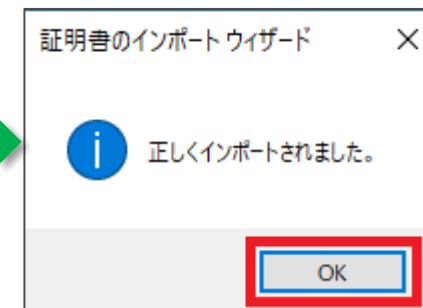
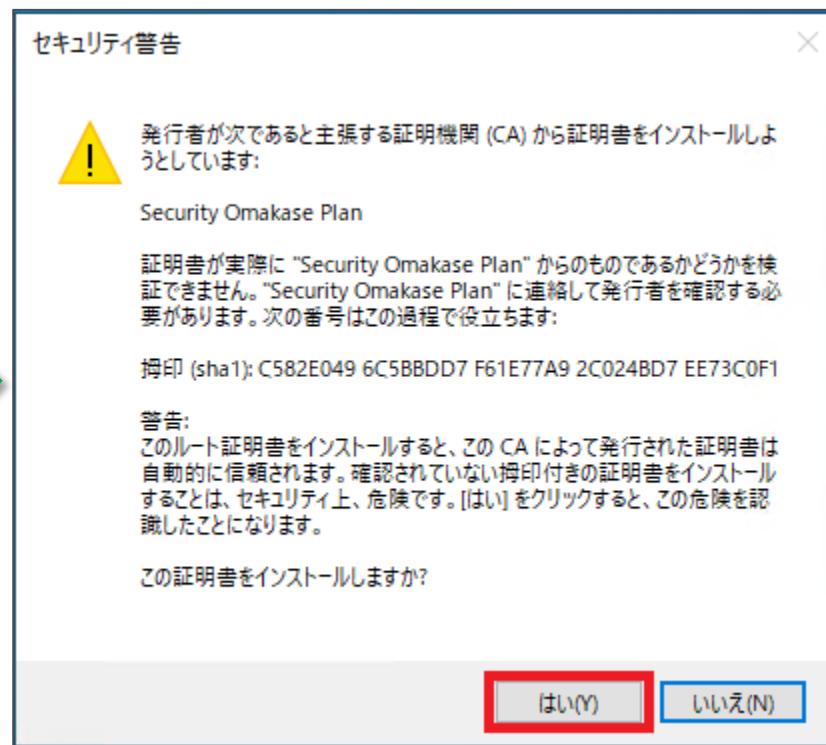
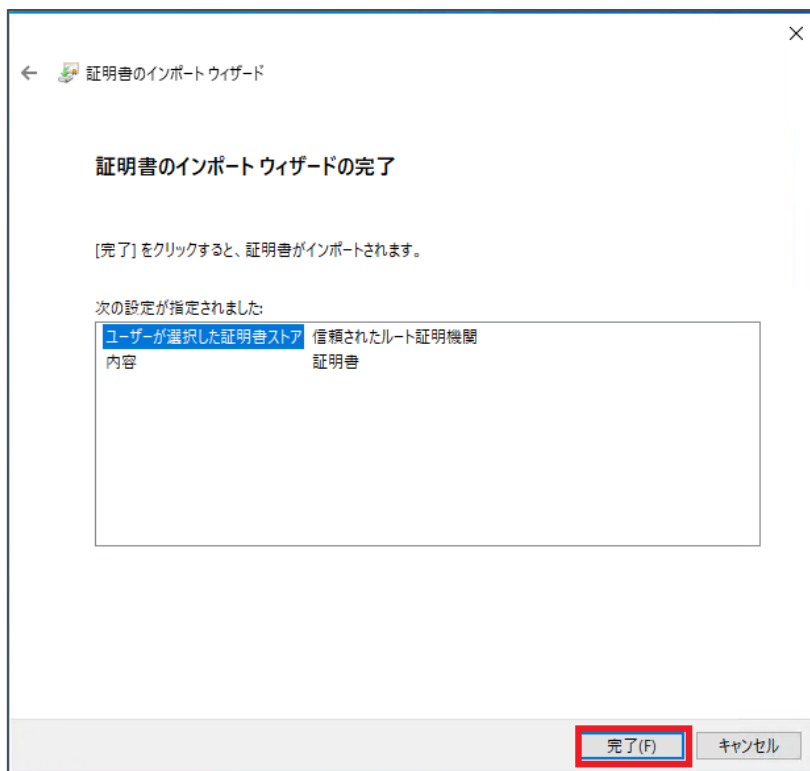
ブラウザの閲覧等には次ページ以降の証明書のインストールが必要です。

# インストール方法

10. パッケージから取り出したETP Proxy (SWG)用の証明書をインストールします。  
パッケージから取り出した「cacert.cer」ファイルを、ダブルクリックしてインストールを行います。



# インストール方法

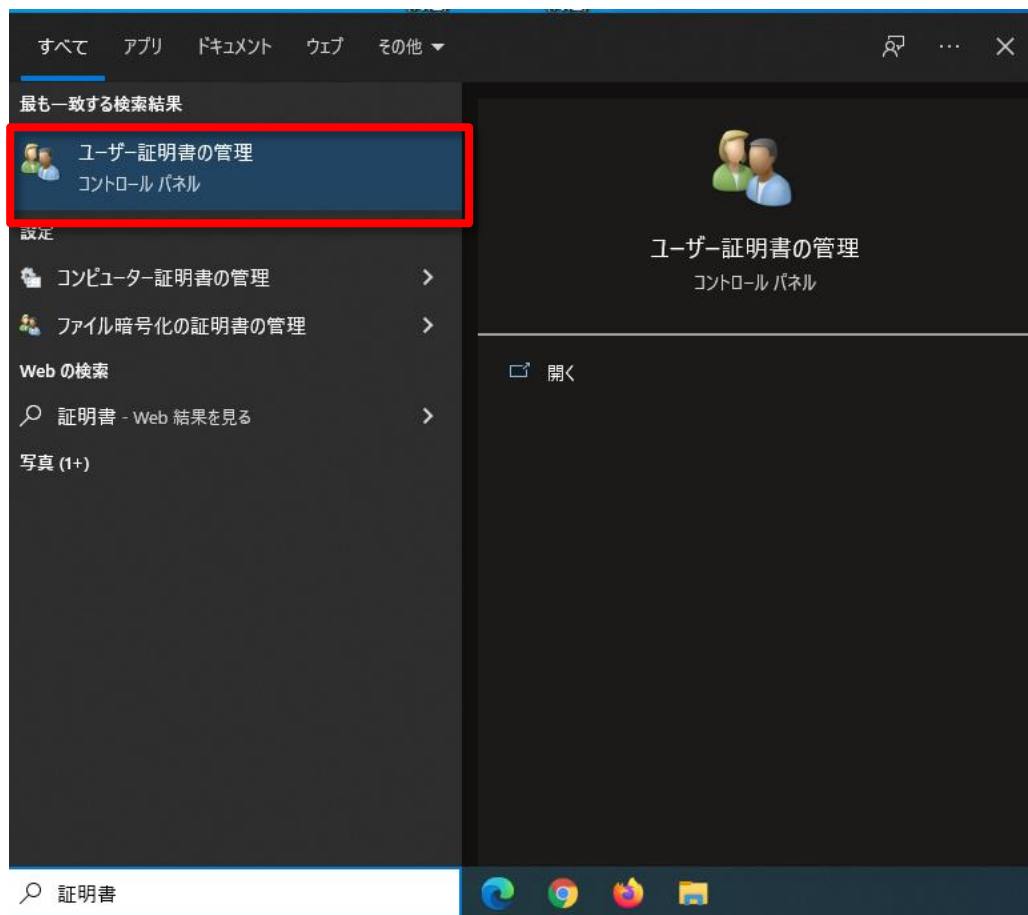


「はい」をクリックします。

# インストール方法

## 11. ETP Proxy (SWG)用の証明書がインストールされているかの確認方法

左下の検索バーもしくはWindowsボタン（キー）を押した直後にキーボードで「証明書」と入力することで、【ユーザ証明書の管理】が表示されるのでクリックします。



# インストール方法

11. ETP Proxy (SWG)用の証明書がインストールされているかの確認方法  
 証明書インストールのさいに指定したフォルダを開くと、フォルダ内に【Security Omakase Plan】があることが確認できます。証明書の確認は以上です。

The screenshot shows the Windows Certificate Manager window. The left pane shows the tree view with 'Trusted Root Certification Authorities' expanded. The main pane displays a list of certificates. The 'Security Omakase Plan' certificate is highlighted in blue and red.

発行先	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプレート
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	2039/10/23	<すべて>	Microsoft Time Sta...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ver...	2004/01/08	タイムスタンプ	VeriSign Time Stam...		
QuoVadis Root CA 2	QuoVadis Root CA 2	2031/11/25	クライアント認証, コー...	QuoVadis Root CA 2		
QuoVadis Root Certification Aut...	QuoVadis Root Certification Auth...	2021/03/18	クライアント認証, コー...	QuoVadis Root Cert...		
SecureTrust CA	SecureTrust CA	2030/01/01	クライアント認証, コー...	Trustwave		CA
Security Communication RootC...	Security Communication RootCA1	2023/09/30	クライアント認証, コー...	SECOM Trust Syste...		
Security Communication RootC...	Security Communication RootCA2	2020/05/20	クライアント認証, コー...	SECOM Trust Syste...		
<b>Security Omakase Plan</b>	<b>Security Omakase Plan</b>	<b>2122/02/25</b>	<b>&lt;すべて&gt;</b>	<b>&lt;なし&gt;</b>		
Starfield Class 2 Certification Au...	Starfield Class 2 Certification Auth...	2034/06/30	クライアント認証, コー...	Starfield Class 2 Cer...		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	2032/03/15	コード署名	<なし>		
thawte Primary Root CA	thawte Primary Root CA	2036/07/17	クライアント認証, コー...	thawte		
Thawte Timestamping CA	Thawte Timestamping CA	2021/01/01	タイムスタンプ	Thawte Timestampi...		
USERTrust RSA Certification Aut...	USERTrust RSA Certification Autho...	2038/01/19	クライアント認証, コー...	Sectigo		
UTN-USERFirst-Object	UTN-USERFirst-Object	2019/07/10	暗号化ファイル システ...	Sectigo (UTN Object)		
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Cer...	2036/07/17	クライアント認証, コー...	VeriSign		
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificati...	2037/12/02	クライアント認証, コー...	VeriSign Universal R...		

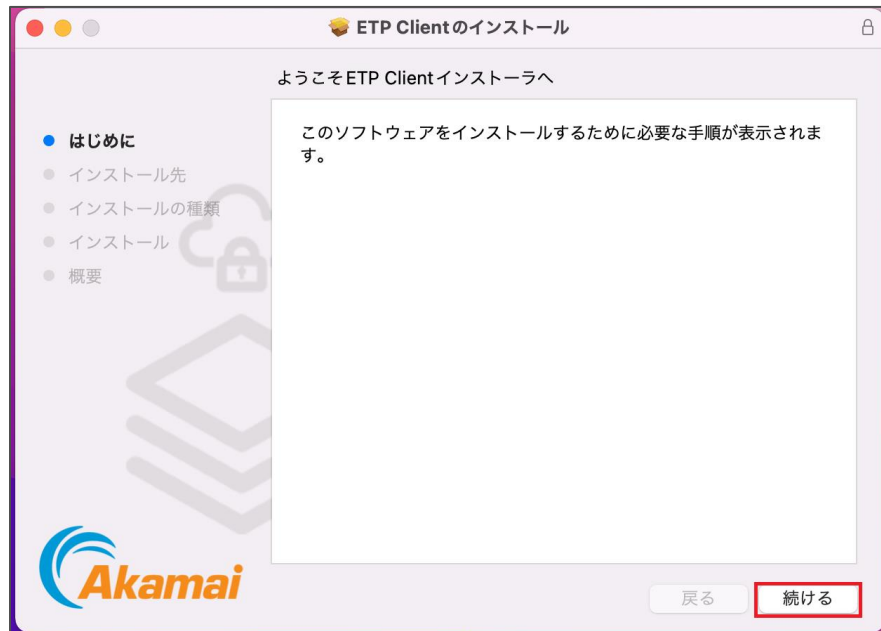
信頼されたルート証明機関 ストアには 51 個の証明書があります。

# インストール方法

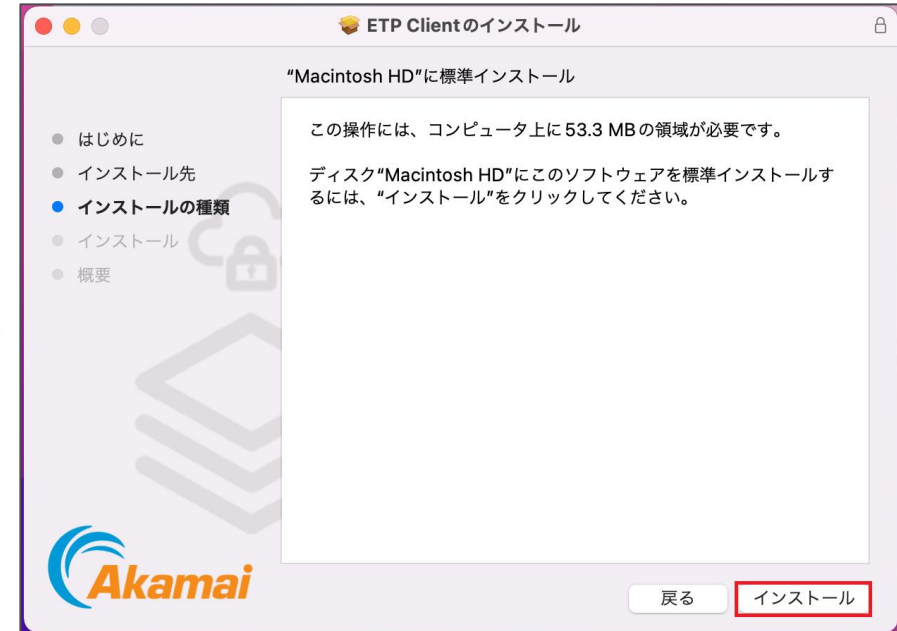
1. パッケージから取り出したMac版ETP Clientのインストーラを起動します。



2. 「ETP Client」をインストールします。



「続ける」を押します。



「インストール」を押します。



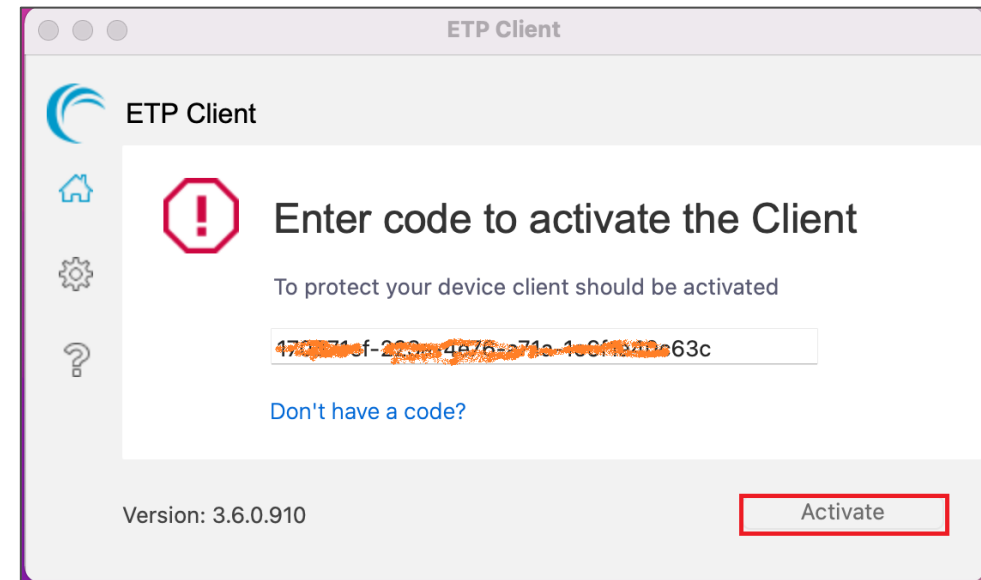
# インストール方法

3. インストールを完了して、別途メールにて代表者様に送付させていただいております、「Entitlement Code」を入力します。  
「Entitlement Code」の確認方法は[Entitlement Codeの確認方法](#)をご確認ください。



「閉じる」を押します。

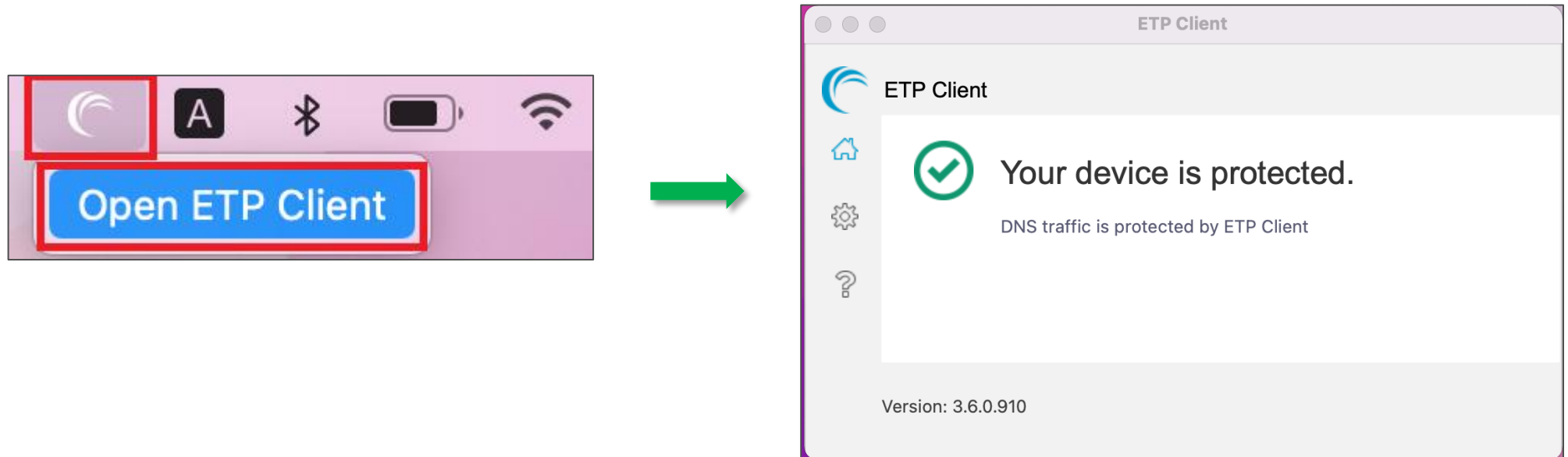
「ETP Client」が自動的に起動します。



「Entitlement Code」を入力して、「Activate」ボタンを押します。

# インストール方法

4. タスクバーの「ETP Clientアイコン」を右クリックして「Open ETP Client」を選択します。



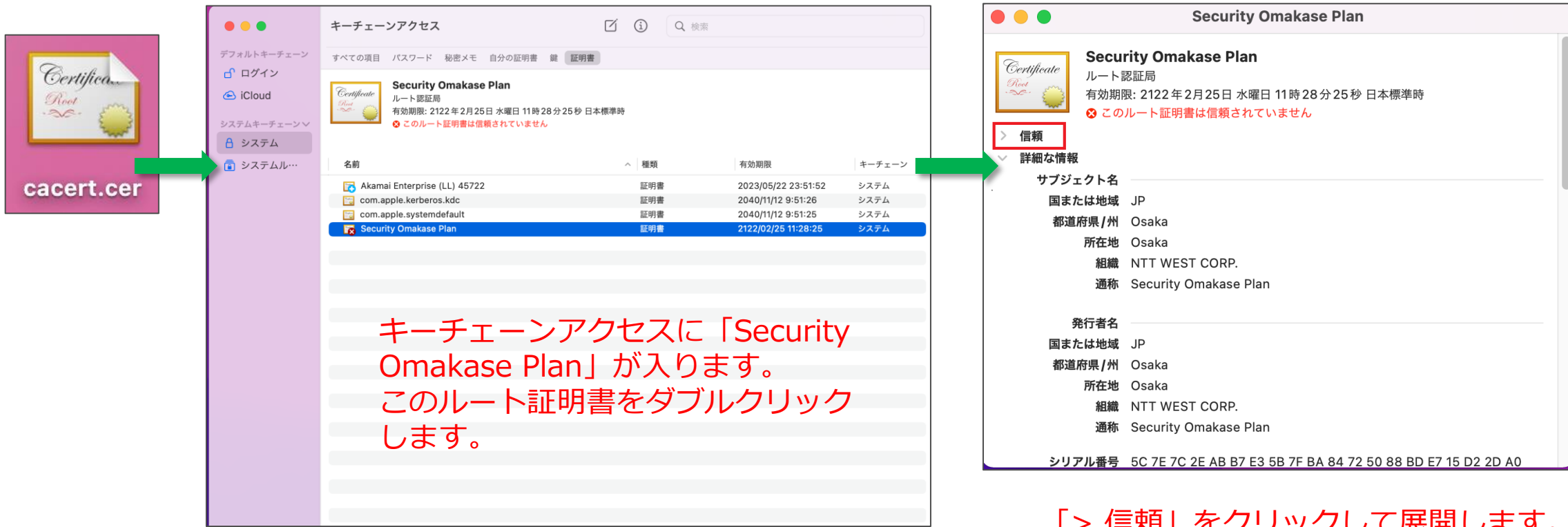
**Your device is protected.**  
になれば、ETPによる保護が有効です。

※再起動を実施いただかないと有効にならない場合がございます。

ブラウザの閲覧等には次ページ以降の証明書のインストールが必要です。

# インストール方法

5. パッケージから取り出したETP Proxy (SWG)用の証明書をインストールします。  
パッケージから取り出した「cacert.cer」ファイルを、ダブルクリックしてインストールを行います。



cacert.cer

キーチェーンアクセス

Security Omakase Plan

名前	種類	有効期限	キーチェーン
Akamai Enterprise (LL) 45722	証明書	2023/05/22 23:51:52	システム
com.apple.kerberos.kdc	証明書	2040/11/12 9:51:26	システム
com.apple.systemdefault	証明書	2040/11/12 9:51:25	システム
Security Omakase Plan	証明書	2122/02/25 11:28:25	システム

キーチェーンアクセスに「Security Omakase Plan」が入ります。  
このルート証明書をダブルクリックします。

Security Omakase Plan

ルート認証局  
有効期限: 2122年2月25日 水曜日 11時28分25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

詳細な情報

サブジェクト名

国または地域 JP  
都道府県/州 Osaka  
所在地 Osaka  
組織 NTT WEST CORP.  
通称 Security Omakase Plan

発行者名

国または地域 JP  
都道府県/州 Osaka  
所在地 Osaka  
組織 NTT WEST CORP.  
通称 Security Omakase Plan

シリアル番号 5C 7E 7C 2E AB B7 E3 5B 7F BA 84 72 50 88 BD E7 15 D2 2D A0

「> 信頼」をクリックして展開します。

# インストール方法



「この証明書を使用するとき:」の  
「システムデフォルトを使用」を変更し  
ます。

「常に信頼」を選択した後に、  
閉じます。

# インストール方法

6. ETP Proxy (SWG)用の証明書がインストールされて、すべてのユーザにとって信頼されているものとして指定されている状態になった事を確認します。

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**

**Security Omakase Plan**  
ルート認証局  
有効期限: 2122年2月25日 水曜日 11時28分25秒 日本標準時  
+ この証明書はすべてのユーザにとって信頼されているものとして指定されています

名前	種類	有効期限	キーチェーン
Akamai Enterprise (LL) 45722	証明書	2023/05/22 23:51:52	システム
com.apple.kerberos.kdc	証明書	2040/11/12 9:51:26	システム
com.apple.systemdefault	証明書	2040/11/12 9:51:25	システム
<b>Security Omakase Plan</b>	<b>証明書</b>	<b>2122/02/25 11:28:25</b>	<b>システム</b>

## アンインストール方法

---

アンインストールは端末OSを確認頂き、  
下記リンクより適切な方法のご利用をお願いいたします。

- [Windows](#)
- [MacOS](#)

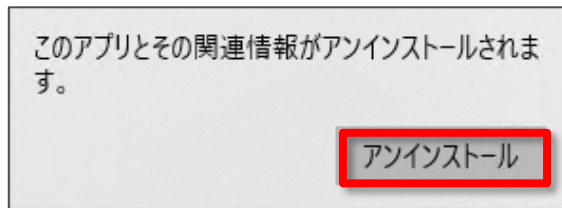
# アンインストール方法

1. Windowsの画面左下の（スタートボタン）を右クリックし、表示された「クイックリンク」メニューから「アプリと機能」をクリックします。
2. ETP Clientを見つけて、クリックして選択します。

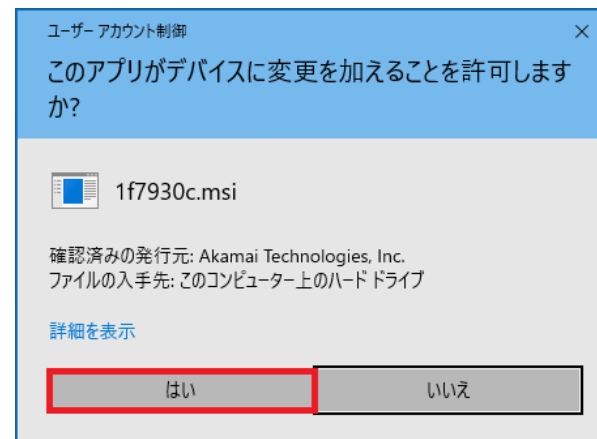


アンインストールを押します。

3. アンインストールの確認画面がでます。



アンインストールを押します。



「はい」を押します。

## アンインストール方法

---

1. Macのターミナルウィンドウを起動して、以下のコマンドを入力します。

```
sudo /Library/Application\ Support/Akamai\ ETP\ Client/uninstall_etpclient
```



## インストール後の設定


---

# インストール後のFirefoxの追加設定

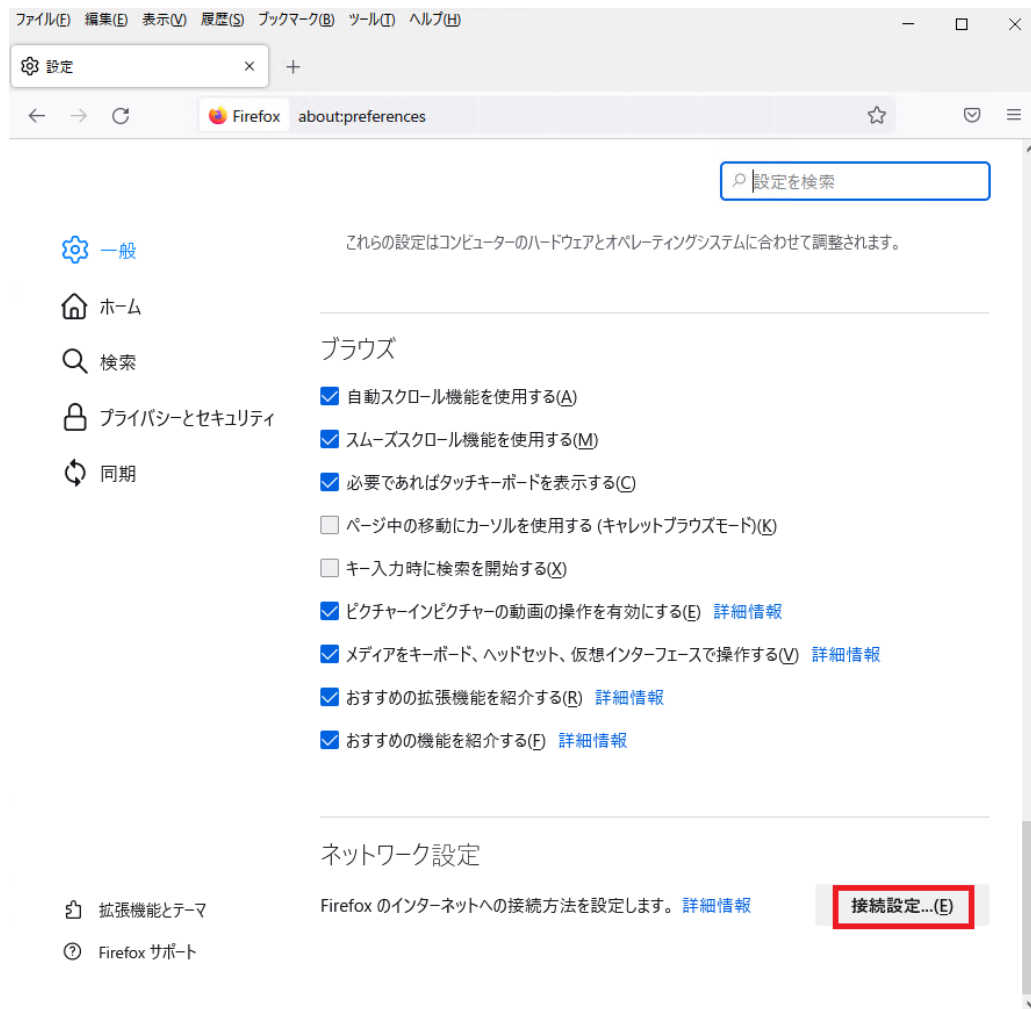
Chrome, Edge, Firefox, Safari, IE, Opera で、2021年12月時点の日本のWebブラウザのシェアのほぼ100%をカバーします。  
この内、Firefox のみ以下の追加設定が必要になります。

1. 古いバージョンのFirefoxをインストールしてバージョンアップしながら使い続けている場合は、FirefoxがOS側のProxy設定を使用しない設定になっている可能性があります。この場合に、ETP Clientが正しく動作するためには、追加の設定が必要です。



右上の  メニューをクリックして「設定」を押します。

# インストール後のFirefoxの追加設定



一番下にスクロールして、ネットワーク設定の「接続設定」を押します。

# インストール後のFirefoxの追加設定

インターネット接続

インターネット接続に使用するプロキシの設定

プロキシを使用しない(Y)

このネットワークのプロキシ設定を自動検出する(W)

システムのプロキシ設定を利用する(U)

手動でプロキシを設定する(M)

HTTP プロキシ(X)  ポート(P)

このプロキシを HTTPS でも使用する(S)

HTTPS プロキシ(H)  ポート(Q)

SOCKS ホスト(C)  ポート(T)

SOCKS v4(K)  SOCKS v5(V)

自動プロキシ設定スクリプト URL(A)

再読み込み(E)

プロキシなしで接続(N)

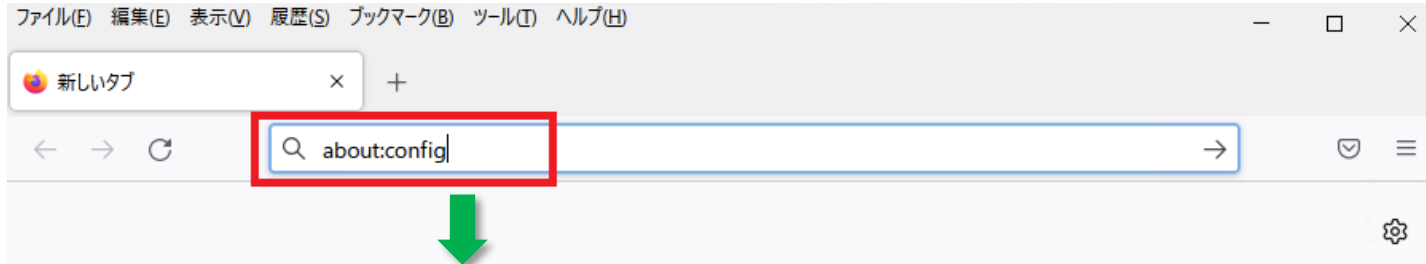
例: .mozilla.org, .net.nz, 192.168.1.0/24  
localhost, 127.0.0.1/8, ::1 ^は常にプロキシなしで接続します。

キャンセル ヘルプ(H)

「システムのプロキシ設定を利用する(U)」を選択し、「OK」ボタンを押します。

# インストール後のFirefoxの追加設定

2. Firefoxはデフォルトでは、OS側のルート証明書を参照しないので、ETP Clientが正しく動作するには、追加の設定が必要です。



Webアドレスを入力するところに「about:config」と入力しEnterキーを押します。



左の画面が表示されるので、「危険性を承知の上で使用する」を押します。

# インストール後のFirefoxの追加設定

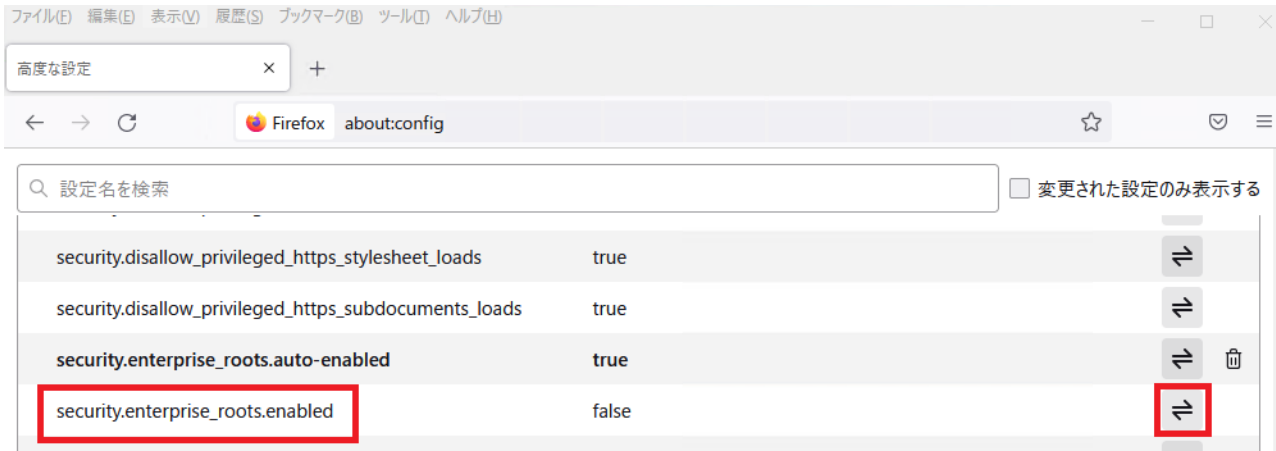


「すべて表示」を押します。

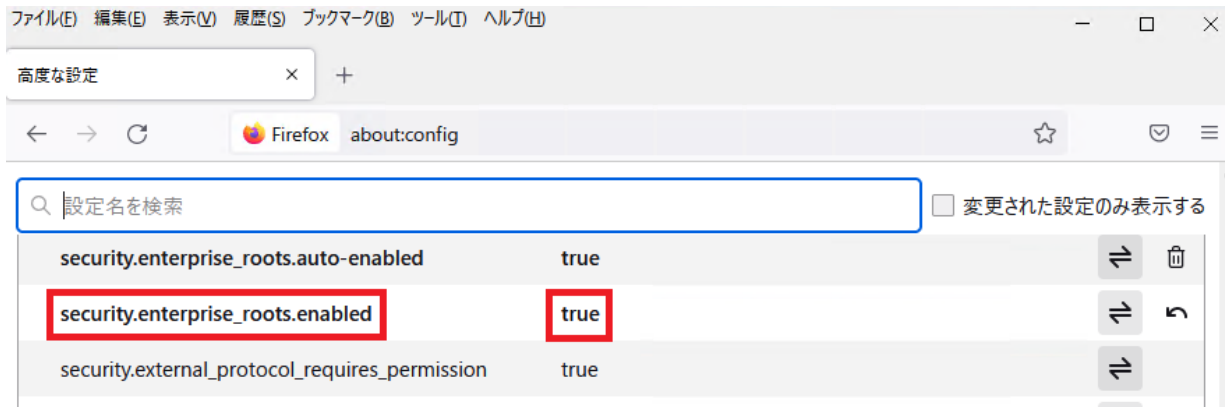


これらの設定を変更すると、Firefox のセキュリティ、パフォーマンスに深刻な問題を引き起こす恐れがあります。

# インストール後のFirefoxの追加設定



「security.enterprise\_roots.enabled」  
見つけてfalseになっている場合は、  
⇌ を押して、trueに変えます。



trueに変わったことを確認します。  
即時に有効になりますが、一度、Firefox  
を閉じてから、再度スタートします。

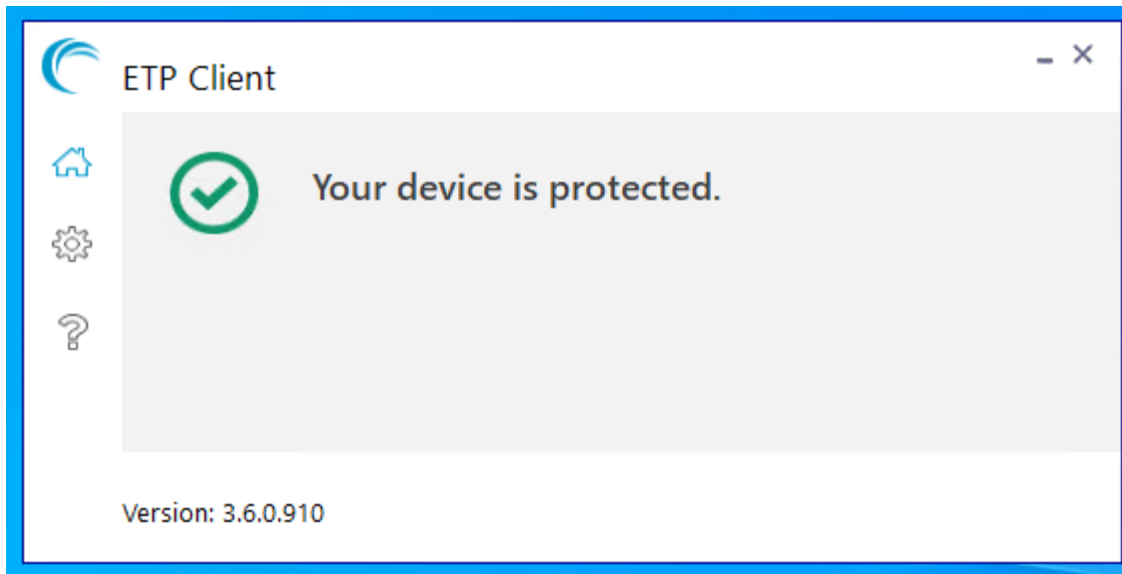
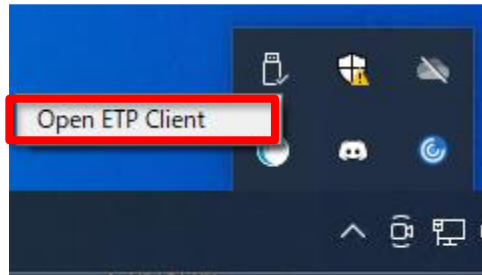
# ソフトウェアの操作方法

---



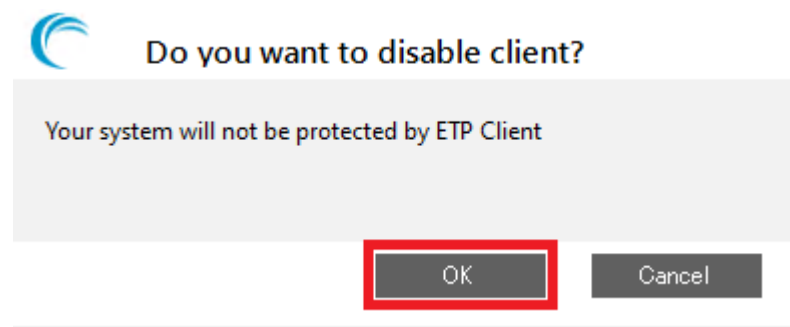
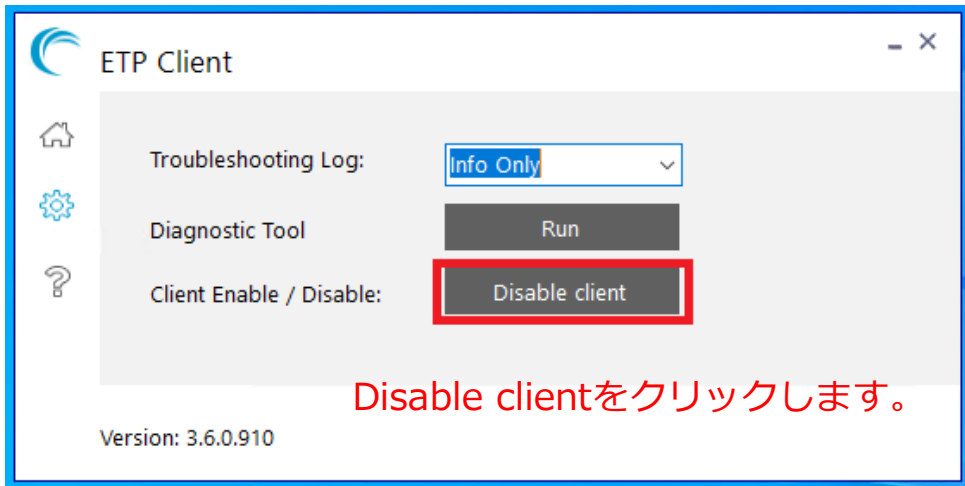
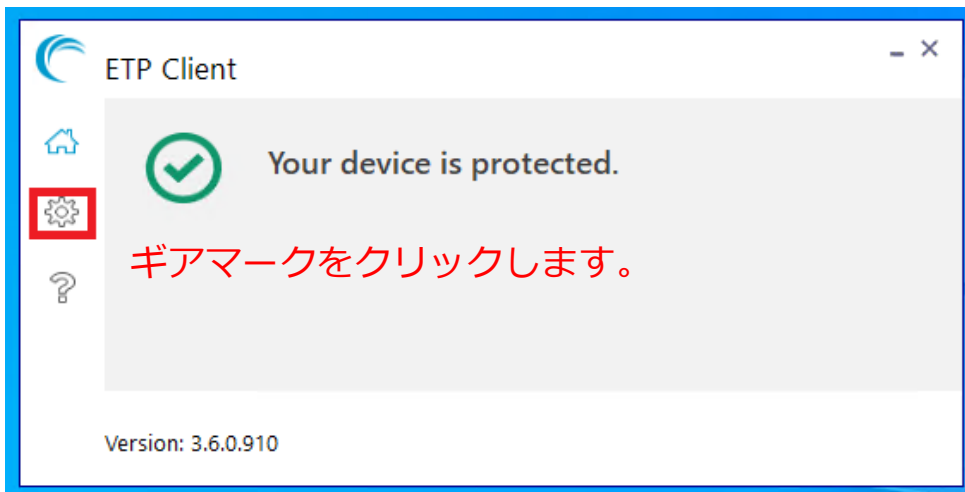
# ソフトウェアの操作方法

操作画面に到達するには、タスクバーのETP Clientアイコンを右クリックして「Open ETP Client」を選択します。

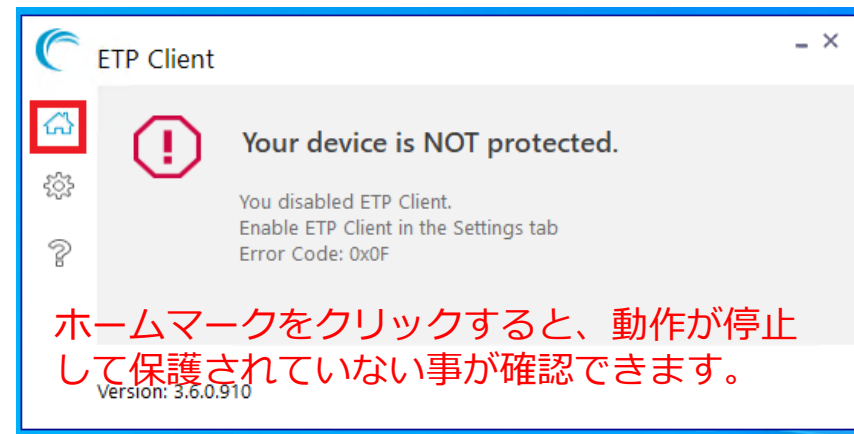


# ソフトウェアの操作方法

## 1. ETP Clientの動作を停止したい場合

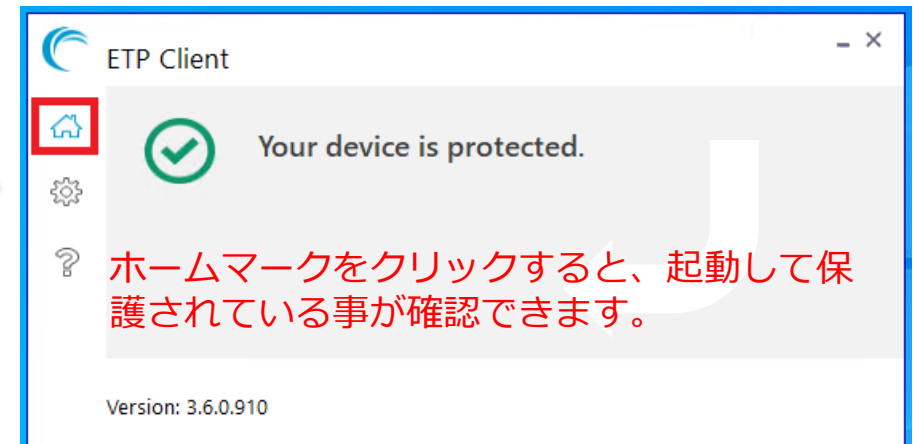
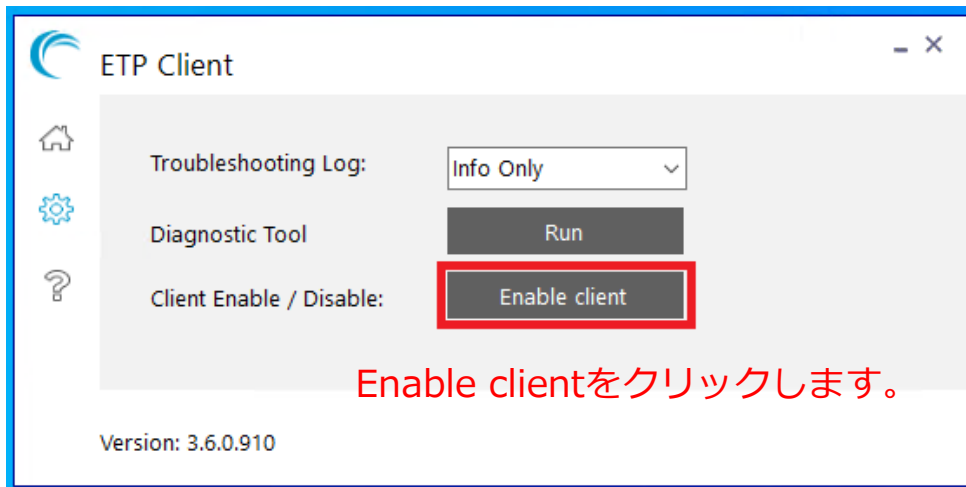
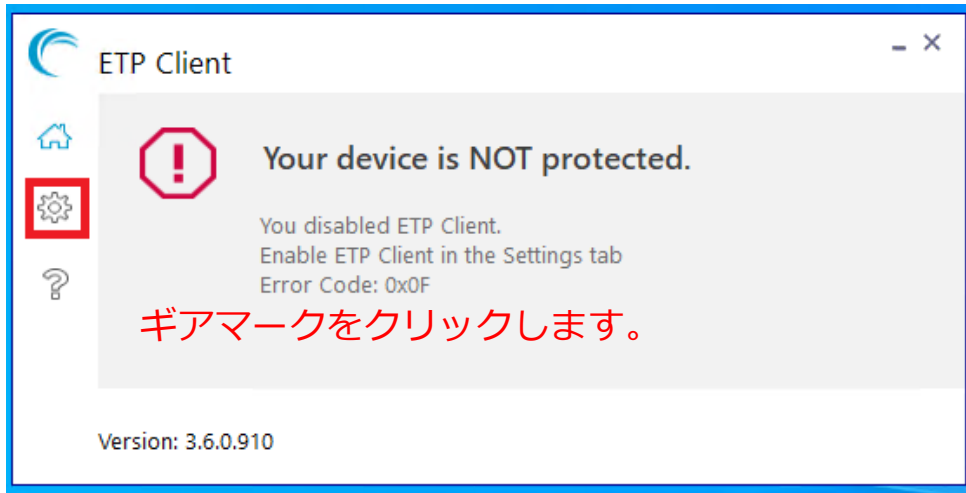


ETP Clientが停止する確認画面が出ますので、OKを押します。



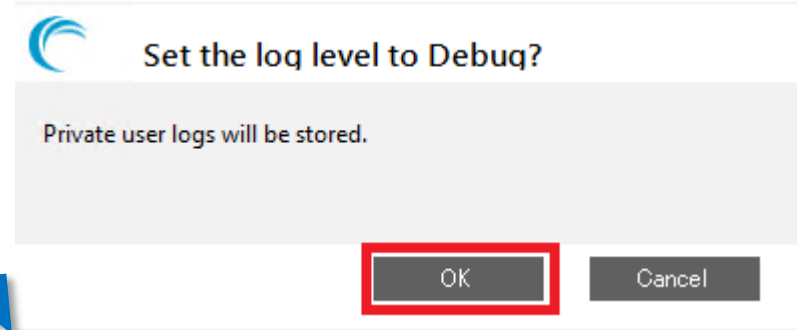
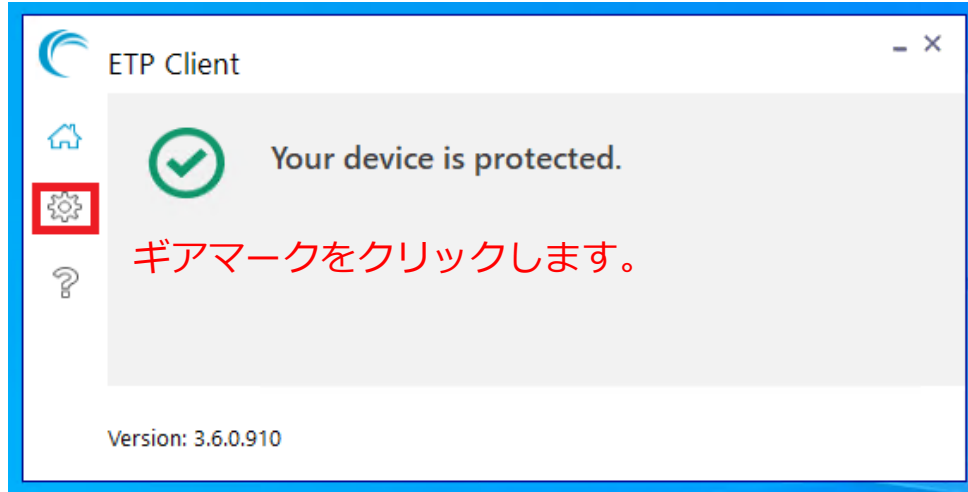
# ソフトウェアの操作方法

## 2. ETP Clientを停止状態から起動したい場合

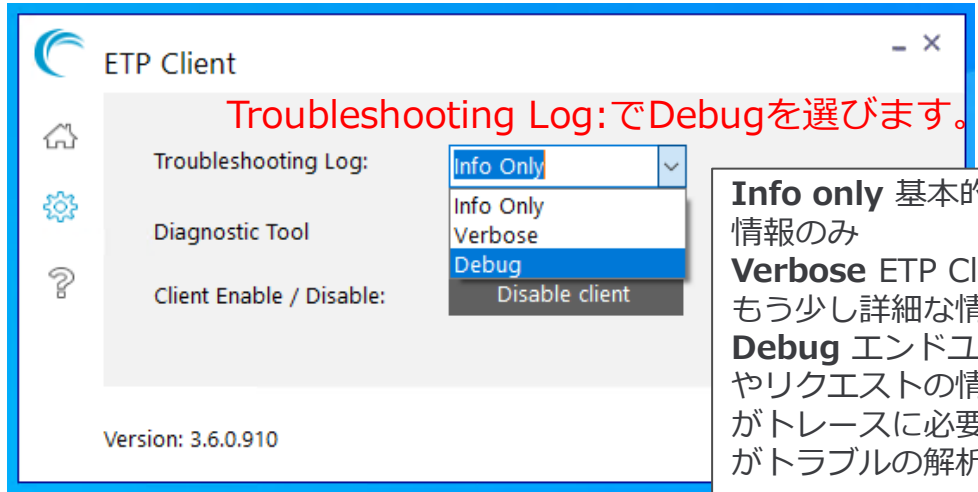


# ソフトウェアの操作方法

## 3. ETP Clientのトラブルシューティング用のログを収集したい場合

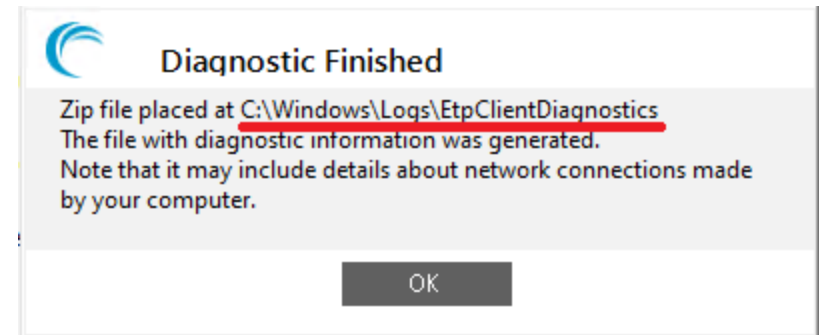


私的なユーザのアクセスログを保存する確認画面が出ますので、OKを押します。



Troubleshooting Log: で Debug を選びます。

**Info only** 基本的なサービスの通信情報のみ  
**Verbose** ETP Clientの健康状態ともう少し詳細な情報  
**Debug** エンドユーザのDNSクエリやリクエストの情報を含むIT管理者がトレースに必要なログ。アカマイがトラブルの解析に必要なレベル



ログの保存場所を確認してからOKを押します。

## ソフトウェア使用上の注意

---

# ソフトウェア使用上の注意

1-1. ETP Clientの動作を停止した場合とアンインストールした場合、PCのネットワーク設定の各項目がETP Clientインストール前の設定値に戻らないパターンがあります。

	PCのネットワーク設定の項目	ETP Clientインストール前の設定値	ETP Clientが動作中の設定値	動作停止とアンインストール後の設定値
①	IPアドレス (サブネットマスク、デフォルトゲートウェイ)	次のIPアドレスを使う(S):	次のIPアドレスを使う(S): (左記と変わらず)	次のIPアドレスを使う(S):
	DNSサーバのアドレス	次のDNSサーバのアドレスを使う(E):	127.0.0.1	次のDNSサーバのアドレスを使う(E):
②	IPアドレス (サブネットマスク、デフォルトゲートウェイ)	IPアドレスを自動的に取得する(O)	IPアドレスを自動的に取得する(O) (左記と変わらず)	IPアドレスを自動的に取得する(O)
	DNSサーバのアドレス	DNSサーバアドレスを自動的に取得する(B)	127.0.0.1	DNSサーバアドレスを自動的に取得する(B)
③	IPアドレス (サブネットマスク、デフォルトゲートウェイ)	IPアドレスを自動的に取得する(O)	IPアドレスを自動的に取得する(O) (左記と変わらず)	IPアドレスを自動的に取得する(O)
	DNSサーバのアドレス	次のDNSサーバのアドレスを使う(E):	127.0.0.1	DNSサーバアドレスを自動的に取得する(B)

動作停止やアンインストール後に、インストール前の設定値に戻らないため、再設定が必要です  
※画面遷移は次頁以降参考

# ソフトウェア使用上の注意

## 1-2. ①、②実際の画面推移。

①

インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): 192 . 168 . 11 . 2

サブネット マスク(U): 255 . 255 . 255 . 0

デフォルト ゲートウェイ(D): 192 . 168 . 11 . 1

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 192 . 168 . 11 . 1

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル



インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): 192 . 168 . 11 . 2

サブネット マスク(U): 255 . 255 . 255 . 0

デフォルト ゲートウェイ(D): 192 . 168 . 11 . 1

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 127 . 0 . 0 . 1

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル



インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): 192 . 168 . 11 . 2

サブネット マスク(U): 255 . 255 . 255 . 0

デフォルト ゲートウェイ(D): 192 . 168 . 11 . 1

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 192 . 168 . 11 . 1

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル

設定値は元に戻ります

②

インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネット マスク(U): . . .

デフォルト ゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): . . .

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル



インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネット マスク(U): . . .

デフォルト ゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 127 . 0 . 0 . 1

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル



インターネット プロトコル バージョン 4 (TCP/IP v4) のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネット マスク(U): . . .

デフォルト ゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): . . .

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル

ETP Client起動/  
インストール後

ETP Client停止/  
アンインストール後

# ソフトウェア使用上の注意

## 1-3. ③実際の画面推移。

DNS設定が消えるため、  
再設定が必要になります。

③

インターネットプロトコルバージョン4 (TCP/IPv4)のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネットマスク(U): . . .

デフォルトゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 192 . 168 . 11 . 15

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル

インターネットプロトコルバージョン4 (TCP/IPv4)のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネットマスク(U): . . .

デフォルトゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 127 . 0 . 0 . 1

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル

インターネットプロトコルバージョン4 (TCP/IPv4)のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I): . . .

サブネットマスク(U): . . .

デフォルトゲートウェイ(D): . . .

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): . . .

代替 DNS サーバー(A): . . .

終了時に設定を検証する(L) 詳細設定(V)...

OK キャンセル

ETP Client起動/  
インストール後

ETP Client停止/  
アンインストール後



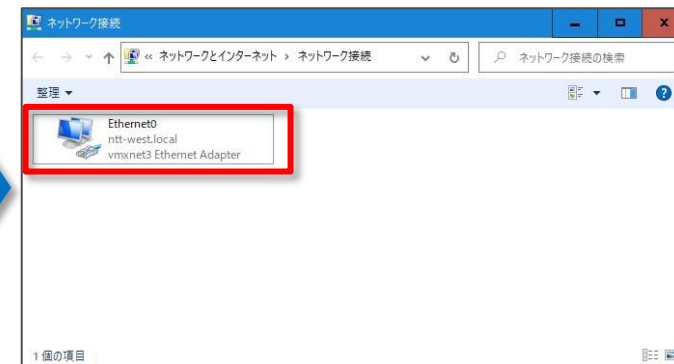
# 【参考】ネットワーク設定の確認方法1

前述のネットワーク設定の確認方法を説明致します。

- ① Windowsボタンもしくは、検索ボタンをクリック後、
- ② 「ネットワークの状態」と入力後、
- ③ 「ネットワークの状態」をクリックします。

次に「アダプターのオプションを変更する」をクリックします。

Ethernet0（ご使用の環境によって異なります）をダブルクリックします。

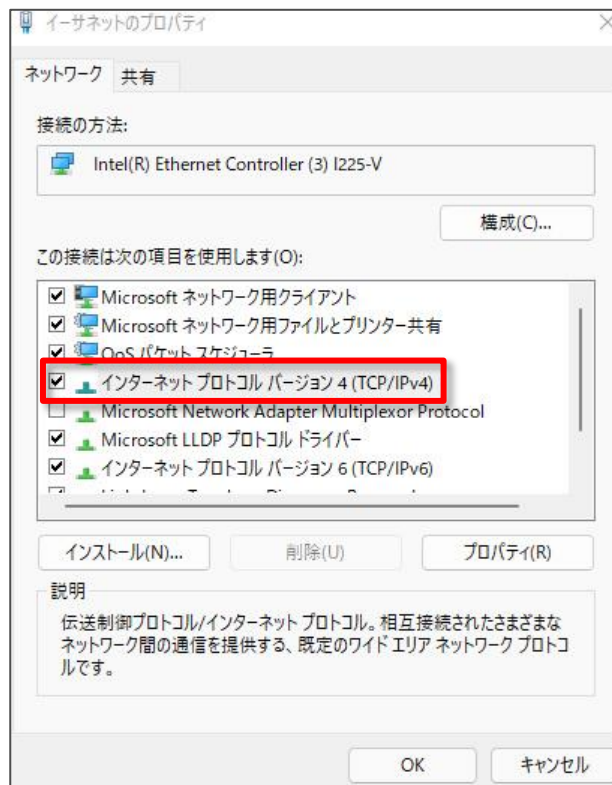


## 【参考】 ネットワーク設定の確認方法2

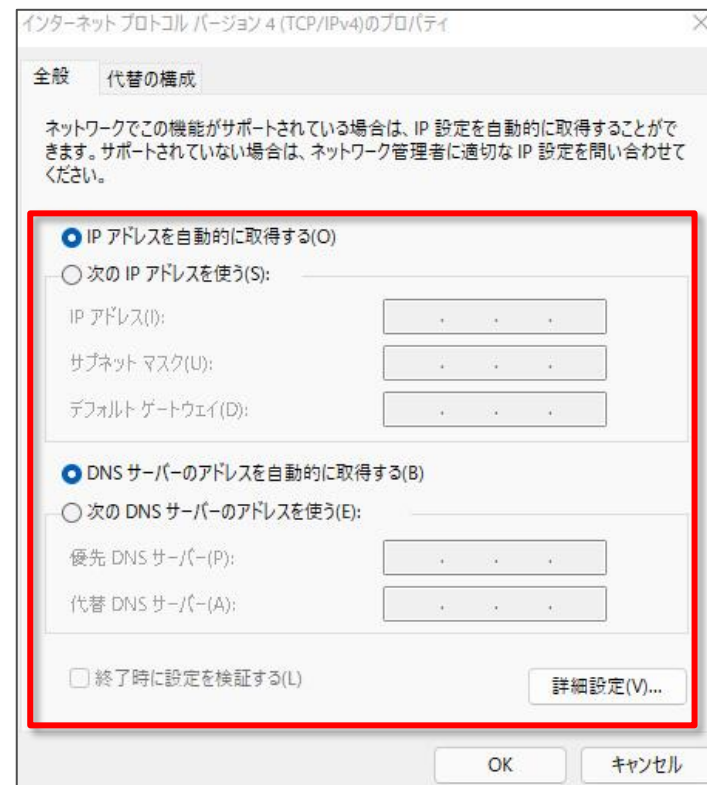
「プロパティ(P)」をクリックします。



「インターネット プロトコルバージョン4(TCP/IPv4)」をダブルクリックします。



以下の画面で設定確認と変更ができます。



# ソフトウェア使用上の注意

2-1. ETP Clientの動作を停止した場合とアンインストールした場合、  
PCのプロキシ設定がETP Clientインストール前の設定値に戻らないパターンがあります。

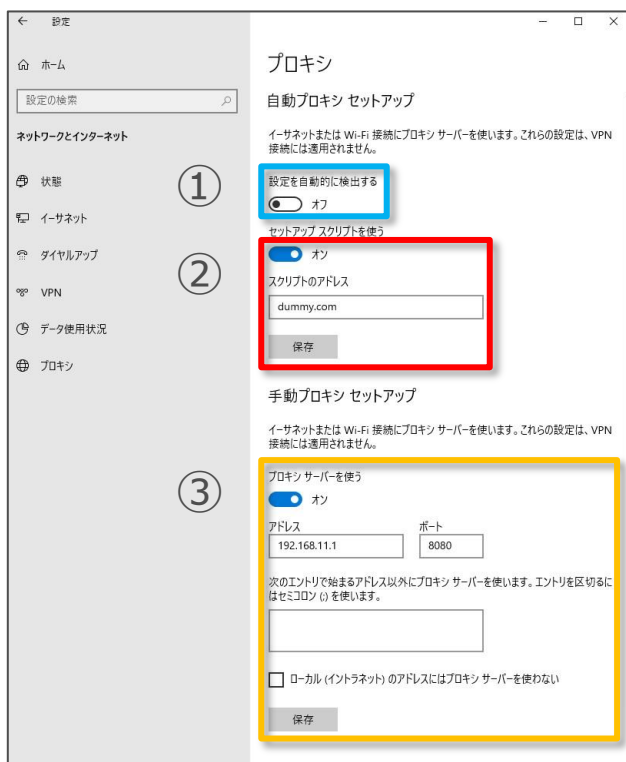
	PCのプロキシ設定の項目	ETP Clientインストール前の設定値	ETP Clientが動作中の設定値	動作停止とアンインストール後の設定値
①	自動プロキシ セットアップ 設定を自動的に検出する	オン	オン	オン
		オフ	オフ	オン
②	自動プロキシ セットアップ セットアップスクリプトを使う	オン	オフ	オフ (スクリプトのアドレスの設定値が クリアされる)
		オフ	オフ	オフ
③	手動プロキシ セットアップ プロキシ サーバーを使う	オン	オン (http=127.0.0.1:80 80;https=127.0.0.1: 8080)	オフ (アドレスなどの設定値が クリアされる)
		オフ	オフ	オフ

動作停止やアンインストール後に、インストール前の設定値に戻らないため、再設定が必要です  
※画面推移は次頁参考

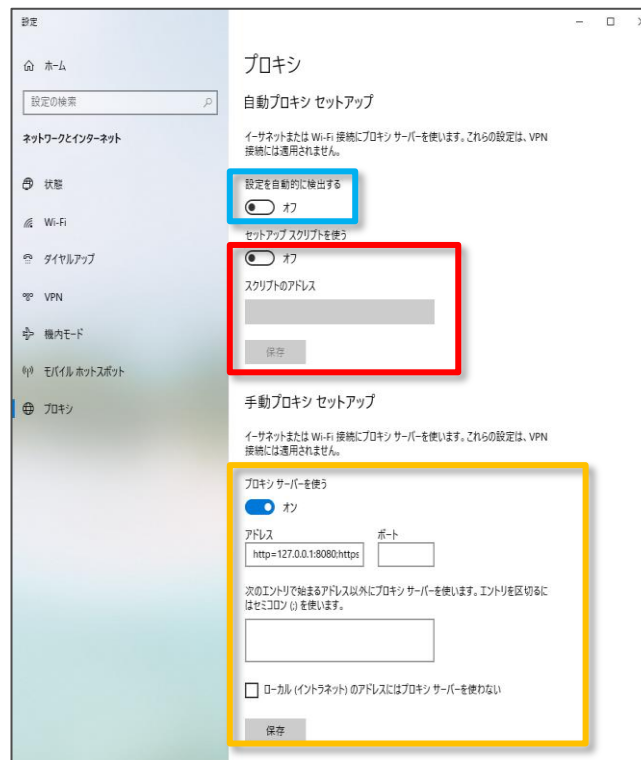
# ソフトウェア使用上の注意

## 2-2. 実際の画面推移。

【ETP Clientインストール前の設定値参考例】

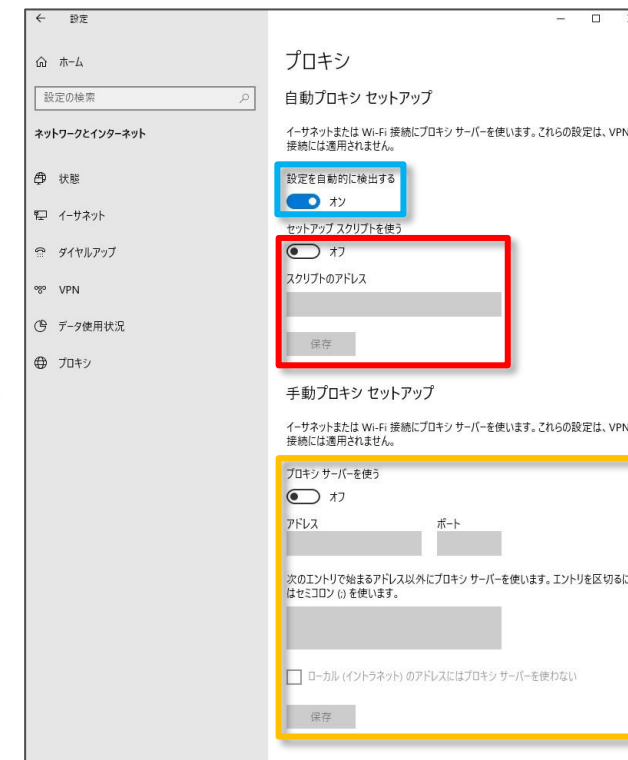


ETP Client起動/  
インストール後



ETP Client停止/  
アンインストール後

下記画像の設定に戻るため、ETP Clientインストール前と設定値が異なる場合は再設定が必要です。



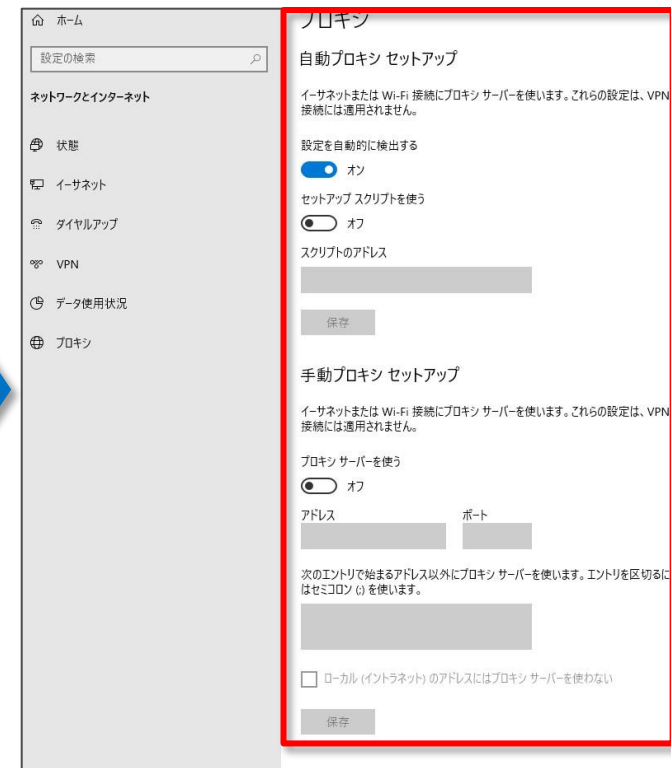
# 【参考】プロキシ設定の確認方法

前述のネットワーク設定の確認方法を説明致します。

- ① Windowsボタンもしくは、検索ボタンをクリック後、
- ② 「ネットワークの状態」と入力後、
- ③ 「ネットワークの状態」をクリックします。

左側の「プロキシ」タブをクリック

以下の画面で設定確認と変更ができます。



# 管理コンソールへの初回ログイン

---

# 管理コンソールへの初回ログイン

1. 開通メールを確認し下記ブラウザへアクセスします。
2. 申込時に登録したメールアドレスを入力します。
3. メールアドレスの入力後、「次へ」をクリックします。

2

3

# 管理コンソールへの初回ログイン

4. パスワード設定のため、「パスワードを紛失した場合」をクリックします。





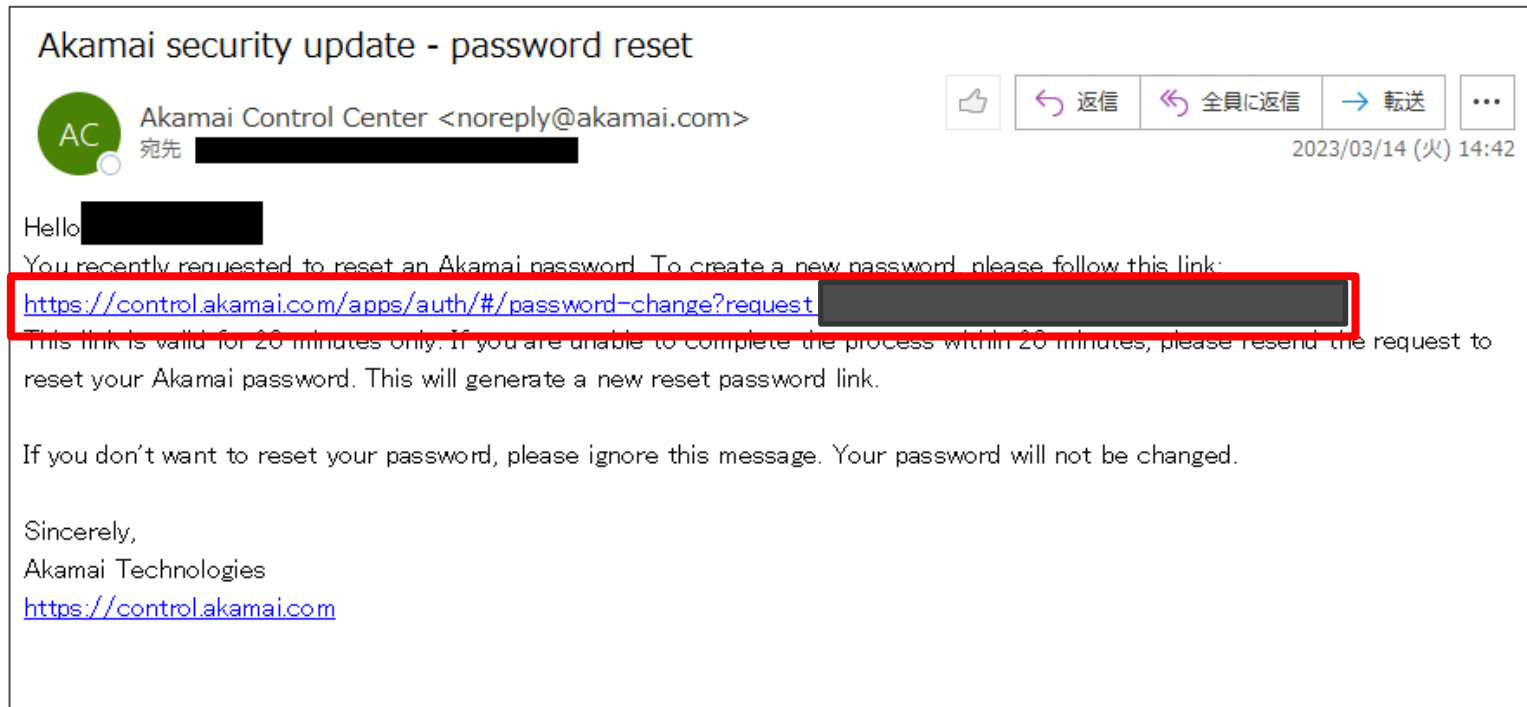
# 管理コンソールへの初回ログイン

5. パスワード設定用のメールが送信されるので、メールを確認します。



# 管理コンソールへの初回ログイン

6. 受信したメールのうち図のようにURLとなっている部分をクリック、またはコピーしブラウザでアクセスします。



# 管理コンソールへの初回ログイン

7. パスワード設定画面が開きますので、要件を満たすパスワードを入力します。
8. パスワードの入力後、「パスワードの変更」をクリックします。

日本語

**Akamai**  
CONTROL CENTER

① 変更後のパスワードが組織のセキュリティ設定に適合しているか検証するため、パスワードの変更には数秒かかります。

パスワードの変更

Eメール: [REDACTED]

ユーザー名: [REDACTED]

7

パスワードの要件:

- ✓ ユーザー名またはEメールを含めることはできません
- ✓ 8文字以上でなければなりません
- ✓ 英字を最低1文字含む必要があります
- ✓ 数値を最低1文字含む必要があります
- ✓ 連続して2文字繰り返すことはできません
- ✓ 過去4回以内に使用したパスワードは使用できません
- ✓ パスワードを一致している必要があります

8

パスワードの変更

# 管理コンソールへの初回ログイン

9. パスワードの設定完了後、再度メールアドレスを入力します。
10. メールアドレスの入力後、「次へ」をクリックします。



# 管理コンソールへの初回ログイン

11. 次にパスワードを入力します。
12. パスワードの入力後、「サインイン」をクリックします。

11

お客様の Akamai アカウントでサインインします。

Eメール:

[パスワードを紛失した場合](#)

[戻る](#) [サインイン](#)

12

# 管理コンソールへの初回ログイン

14. スマートフォンまたはタブレットを使いいずれかの任意のソフトウェアを入手します。

Akamai  
CONTROL CENTER

二要素認証の設定

以下の手順に従って、Control Center アカウントに2要素認証（2FA）を設定します。

お客様のアカウントへの2FAの使用は、Akamaiのポータル利用規約およびお客様（またはお客様の会社）がAkamaiと締結した顧客契約の条件に従うものとします。

1. 次のいずれか、または別の認証アプリを選択し、ご使用のモバイルデバイスにインストールします。

Google Authenticator	iOS	Android
Microsoft Authenticator	iOS	Android
Twilio Authy	iOS	Android

14

2. モバイルデバイスに認証アプリをインストールしたら、次のいずれかのオプションを選択して設定し、画面の指示に従います。

シークレットコードで設定    QRコードで設定

# 管理コンソールへの初回ログイン

15. QRコードまたは、各Storeへのリンク、Eメールでのリンク送信のいずれかを用いてソフトウェアを入手します。下記はIOSでGoogle Authenticatorを選択した場合のサンプルとなります。
16. ソフトウェアの入手後、「閉じる」をクリックします。



# 管理コンソールへの初回ログイン

17. 「シークレットコードで設定」または「QRコードで設定」のいずれかを使用し、2要素認証の登録を完了します。

**Akamai**  
CONTROL CENTER

### 二要素認証の設定

以下の手順に従って、Control Center アカウントに2要素認証 (2FA) を設定します。

お客様のアカウントへの2FAの使用は、Akamaiの [ポータル利用規約](#) およびお客様（またはお客様の会社）がAkamaiと締結した顧客契約の条件に従うものとします。

1. 次のいずれか、または別の認証アプリを選択し、ご使用のモバイルデバイスにインストールします。

Google Authenticator	iOS	Android
Microsoft Authenticator	iOS	Android
Twilio Authy	iOS	Android

2. モバイルデバイスに認証アプリをインストールしたら、次のいずれかのオプションを選択して設定し、画面の指示に従います。

シークレットコードで設定    QRコードで設定

17



# 管理コンソールへの初回ログイン

18. 下記はサンプルとなります。いずれかの方法で2要素認証の登録を完了します。

### シークレットコードによる 2FA の設定

認証アプリを設定し、Control Center アカウントに接続します。

1. このシークレットコードを使用して 6 桁の検証コードを取得します。

**YHTHT3U6OL7M7MMDG**

2. 認証アプリが生成した 6 桁の検証コードを入力し、完了をクリックします。

[キャンセル](#)

18

### QRコードによる 2FA の設定

認証アプリを設定し、Control Center アカウントに接続します。

1. この QR コードをスキャンして、6 桁の検証コードを取得します。



**Sample**



2. 認証アプリが生成した 6 桁の検証コードを入力し、完了をクリックします。

[キャンセル](#)

# 管理コンソールへの初回ログイン

19. 2要素認証の設定が完了すると下記画面となります。「続行」をクリックするとログインします。

**Akamai**  
CONTROL CENTER

二要素認証が設定されました。

### 二要素認証の設定

以下の手順に従って、Control Center アカウントに2要素認証 (2FA) を設定します。

お客様のアカウントへの2FAの使用は、Akamaiの [ポータル利用規約](#) およびお客様（またはお客様の会社）がAkamaiと締結した顧客契約の条件に従うものとします。

1. 次のいずれか、または別の認証アプリを選択し、ご使用のモバイルデバイスにインストールします。

Google Authenticator	iOS	Android
Microsoft Authenticator	iOS	Android
Twilio Authy	iOS	Android

2. モバイルデバイスに認証アプリをインストールしたら、次のいずれかのオプションを選択して設定し、画面の指示に従います。

シークレットコードで設定    QRコードで設定    **続行**

19

## Entitlement Codeの確認方法

---

インストールの中でEntitlement Codeを入力いただく必要がございます。  
本スライドでは管理コンソールで、Entitlement Codeを確認する方法を説明します。

または

【NTT西日本セキュリティおまかせプラン】クラウドプロキシのご案内のメールより  
確認することができます。

# Entitlement Codeの確認方法

1. ログイン後、右図のような画面が表示されるので、左上の三ををクリックします。
2. メニューが表示されるので、「Enterprise Center」をクリックします。

1

2

すべてのサービスからフ...

サービス

- 共通サービス
  - トラフィックレポート
  - アラート
  - Event Center
  - スケジュール済みレポート
- エンタープライズセキュリティ
  - Enterprise Center**
- アカウント管理者
  - ID およびアクセス契約
  - SLA テスト
  - Marketplace

Akamai Control Center へようこそ

レポート  
0件のスケジュール済みレポート  
利用可能なレポート

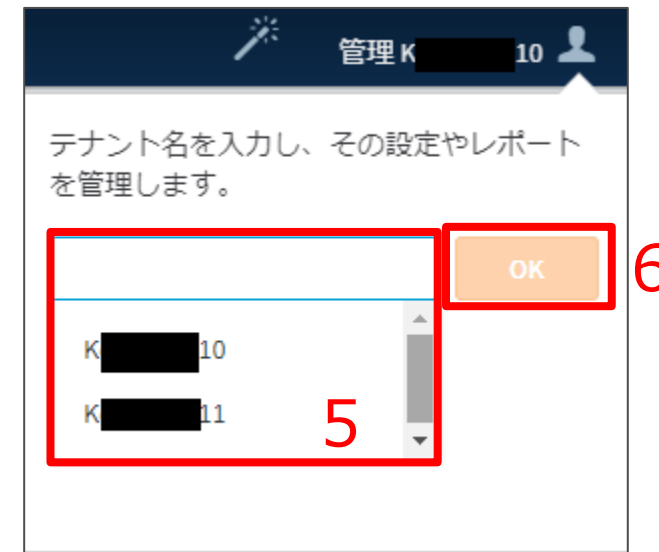
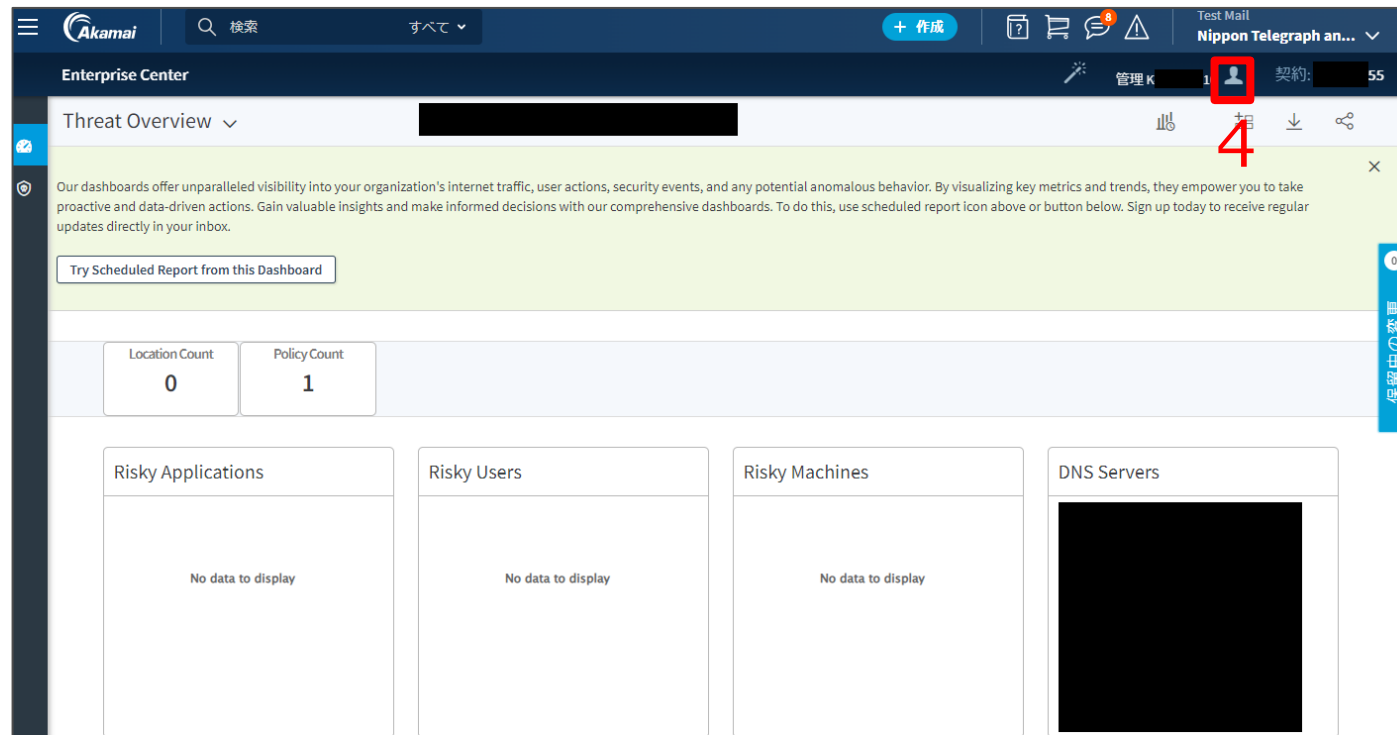
学ぶ  
Akamai について学ぶ

Try our cloud computing services  
Increase cost savings, performance, and speed to market.  
Note: Trials require a valid payment method. To explore other options, please contact your account executive.

アクティビティ  
Enterprise Center in Enterprise Security  
直前

# Entitlement Codeの確認方法（複数契約者様向け）

3. 複数の契約で同一のメールアドレスによる申込をされている場合、複数の環境が割り当てられています。次の手順で環境切り替えることができます。
  4. 「Enterprise Center」画面で人型のマークをクリックします。
  5. テナント名の選択画面で枠をクリックすることで関連付けられている環境（テナント名※）が表示されるので、任意のものを選択します。
  6. 「OK」をクリックすると、選択した環境に切り替わります。
- ※テナント名については、送付されるお客様IDをご確認ください。



# Entitlement Codeの確認方法

9. 7→8とカーソルを合わせることで下記メニューが表示されますので、「ETPクライアント」をクリックします。

The screenshot shows the Akamai Enterprise Center interface. The navigation menu on the left is expanded, and the 'ETPクライアント' (ETP Client) option is highlighted. Red boxes and numbers indicate the steps: 7 points to '脅威からの保護' (Protection from threats), 8 points to 'クライアント&コネクター' (Clients & Connectors), and 9 points to 'ETPクライアント'.

- 7: 脅威からの保護
- 8: クライアント&コネクター
- 9: ETPクライアント

# Entitlement Codeの確認方法

10. Entitlement Codeを確認することができます。

11. 左側のボタンでコピー、右側のボタンはコードの更新を行います。

コードの更新をした場合、それまでのコードは無効となりますのでご注意ください。

すでにアクティベート済みの端末へは影響はございません。

設定 レポート バージョン管理 アクティベーション

10 Entitlement Code [Redacted] [Copy] [Refresh] 11

ETPクライアントの有効化

Allow users to disable the client

Allow disable action with entitlement code

Windows 上でのアンインストールの許可

ETPクライアントのロールバック