

# 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 (ver2.0)

西日本電信電話株式会社

# 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="#">ソフトウェアの動作仕様と注意</a>	8
<a href="#">インストール方法 (Windows・Mac)</a>	12
<a href="#">アンインストール方法 (Windows・Mac)</a>	26
<a href="#">インストール後の設定</a>	31
<a href="#">ソフトウェアの操作</a>	38
<a href="#">ソフトウェア使用上の注意</a>	48
<a href="#">管理コンソールへの初回ログイン</a>	52
<a href="#">エンタイトルメントコードの確認方法</a>	65
<a href="#">既知のトラブルと対処方法</a>	70
<a href="#">お問い合わせ先について</a>	72

# 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
4	2024/06/17	新ソフトウェア（ZTC）公開に伴い、旧ソフトウェア（ETP Client）の内容を一新 「ソフトウェアの動作仕様と注意」を追加 「既知のトラブルと対処方法」を追加 「お問い合わせ先について」を追加	2.0

## はじめに

---

本章では下記項目について説明します。

- [本資料の位置づけ](#)
- [ソフトウェアのサポートOS](#)
- [本サービスで提供しているテナントについて](#)

## はじめに（本資料の位置づけ）

---

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（以下本サービス）を、ご利用されるために必要な手順や情報を記載したものとなっております。

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初期セットアップツール一式をダウンロードするようお願いいたします。

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

**2024年6月17日よりソフトウェアが「ETP Client」から「Zero Trust Client」へと変更となりました。セキュリティ機能に変更はありませんが、サポートの観点からアップグレードするようお願い申し上げます。本マニュアルの[インストール方法](#)を実施頂くことで、そのままアップグレードされるようになっております。**

初期セットアップツール一式には下記が含まれております。

- Windows用
  - ZTC.msi（ソフトウェア）
  - cacert.cer（証明書）
- mac用
  - ZTC.pkg（ソフトウェア）
  - cacert.cer（証明書）

## はじめに（ソフトウェアのサポートOS）

ソフトウェア（ZTC5.3時点）は下記のOS及びプロセッサをサポートしております。  
記載のないものについてはサポートしかねますのでご注意ください。

	OSバージョン	プロセッサ	必要空きディスク容量
<b>Windows</b>	Windows10 Home/Enterprise/Pro 64-bit ・ 1803 or higher Windows11 ・ 21H2 ・ 22H2	Intel:x86_64	200MB以上
<b>macOS</b>	macOS 12 (Monterey) macOS 13 (Ventura) macOS 14 (Sonoma)	Intel:x86_64 Apple:M1,M2	

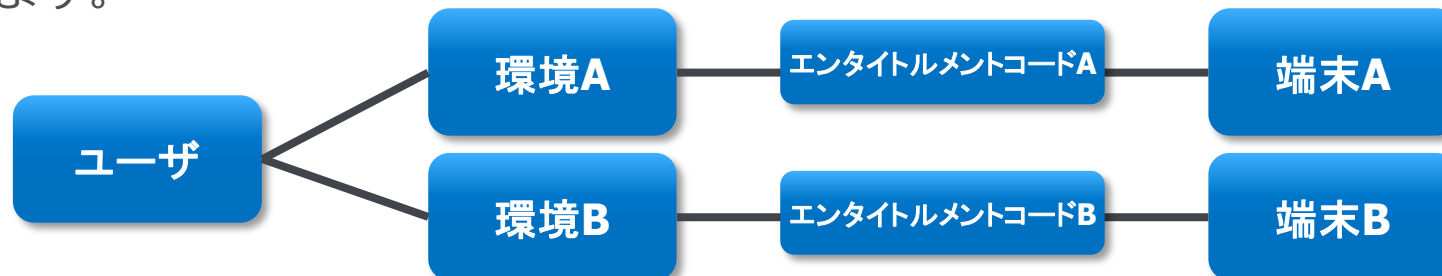
## はじめに（本サービスで提供しているテナントについて）

本サービスでは契約ごとにサービス提供の基盤となるテナントを一つ提供させて頂いております。テナントへは申込時に記載頂いたメールアドレスで作成しておりますユーザを通じてアクセスできます。

ユーザとテナントへのアクセスは、[管理コンソールへの初回ログイン](#)以降のスライドをご確認ください。各テナントにはサービス利用のために唯一のエンタイトルメントコードが存在し、こちらをソフトウェアインストール時に入力することで、テナントを特定しセキュリティ機能を利用できるようになります。



2023年12月より異なる契約で同一メールアドレスによる申込ができるようになりました。同一メールアドレスで複数の契約を頂いている場合、ユーザに二つ以上のテナントが紐づけられます。複数のテナントが紐づけられている場合、管理コンソールではテナントを切り替えて管理できます。テナントの切り替え方法は[エンタイトルメントコードの確認方法（複数契約者様向け）](#)にてご確認ください。



# ソフトウェアの動作仕様と注意

---

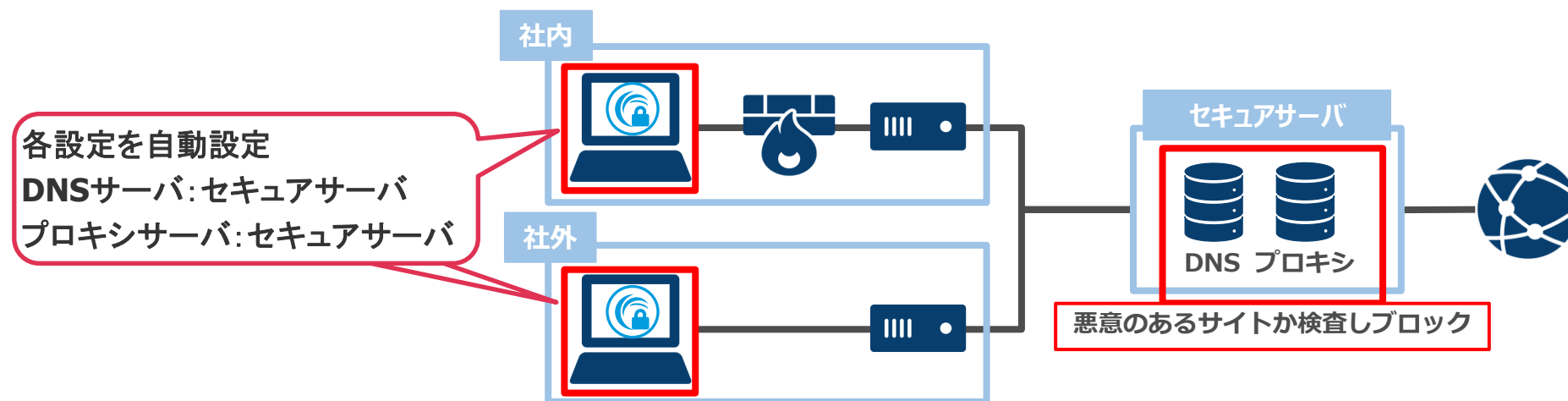
本章では下記項目について説明します。

- [ソフトウェアの動作仕様](#)
- [ソフトウェア利用時の注意](#)



## ソフトウェアの動作仕様と注意（ソフトウェアの動作仕様）

本サービスは提供ソフトウェアにより端末のDNSサーバとプロキシサーバの設定を変更することで、インターネットへ接続している時、HTTPおよびHTTPS通信がセキュアサーバを経由するようになります。セキュアサーバは通信を検査し悪意のあるサイトや不正な通信をブロックし、場所を問わずWebアクセスに対するセキュリティを提供します。



※なお本サービスで利用するソフトウェアはサービス提供のために必要な設定を自動で行うものであり、ソフトウェア自体にセキュリティ機能はないためご注意ください。

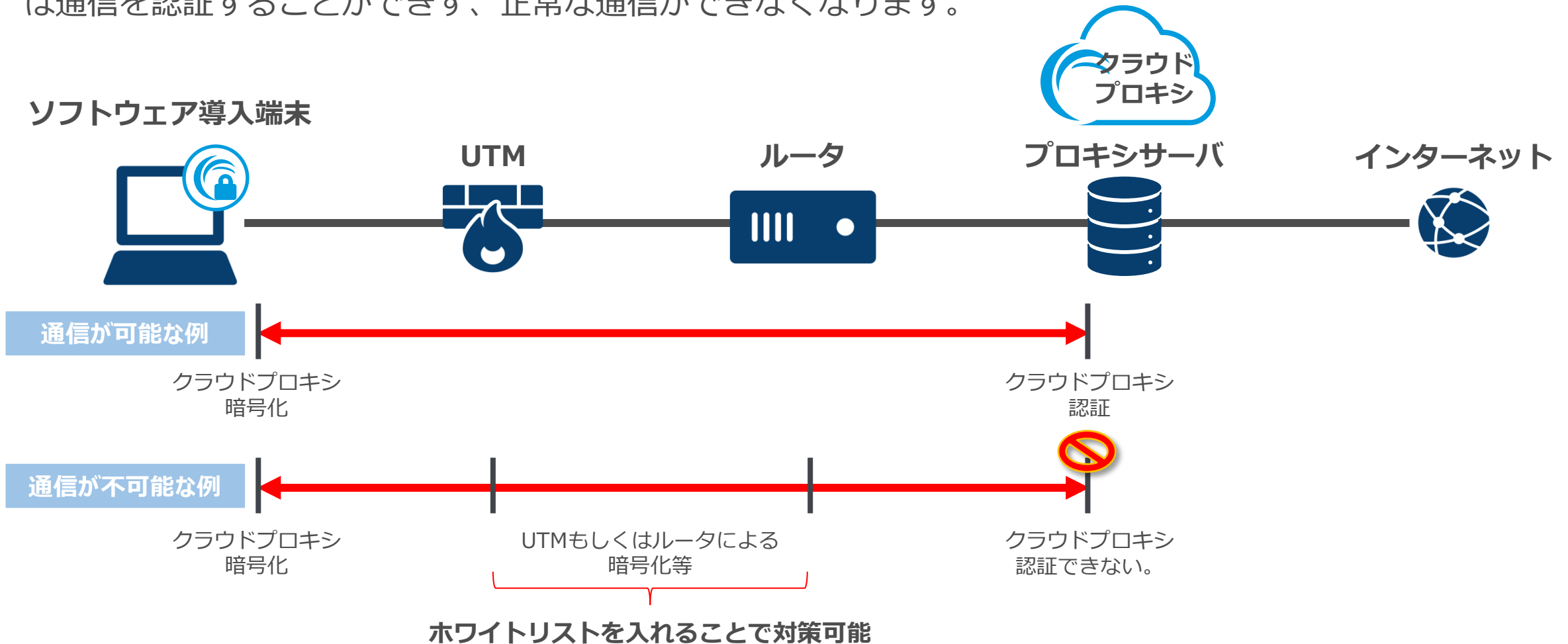
# ソフトウェアの動作仕様と注意（ソフトウェア利用時の注意）

本ソフトウェアは前スライドの動作仕様により、  
以下のようなサービスやソフトウェア、機器機能の利用時は動作サポート外のため注意が必要となります。

- 類似した動作や環境設定を行うサービスやソフトウェアと同時に使用する場合
  - 本ソフトウェアと競合し正常な機能提供ができなくなるため同時使用できません。
  - 対処として、競合しているソフトウェアの停止を行ってください。
- 以下例のようなUTMやルータの機能が有効なネットワーク環境下で本ソフトウェアを利用する場合
  - 例1：Cloud Edge HTTPS復号機能
  - 例2：FortiGate SSLインスペクション（Deep-inspection）
    - 本ソフトウェアの利用時、証明書によりプロキシサーバとの通信間を暗号化するため、その通信経路上でUTMやルータにより暗号化/復号化が実施されると、正常な認証ができず通信ができなくなります。（理由については次のスライドをご確認ください）
    - 対策として、下記ドメインをUTMやルータのホワイトリストに登録することで、本サービス用に通信経路を確保することができます。なお、過去同対応を実施されている場合は新ソフトウェア公開にあたり、「\*.akamai-zt.com」が新規追加となっているためご注意ください。
      - ❑ \*.akaetp.net
      - ❑ \*.akamai.com
      - ❑ \*.akamai-zt.com

# ソフトウェアの動作仕様と注意（ソフトウェア利用時の注意）

下図は前スライドで挙げた特定の機能が無効な場合と有効な場合で分けたイメージ図となっています。NG例のように端末とプロキシサーバ間の通信時に別途の暗号化等の処理がされた場合、プロキシサーバでは通信を認証することができず、正常な通信ができなくなります。



## インストール方法

---

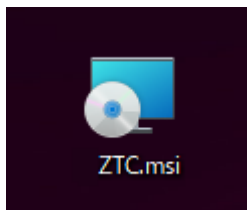
インストールは導入予定の端末のOSを確認頂き、  
下記リンクより適切な手順のご利用をお願いいたします。

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

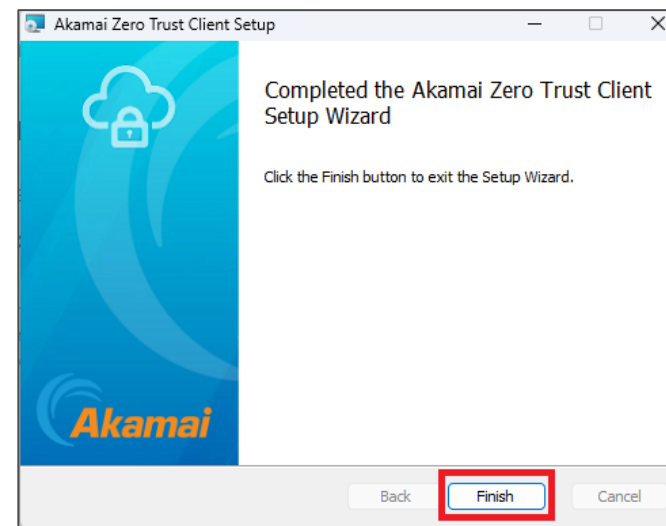
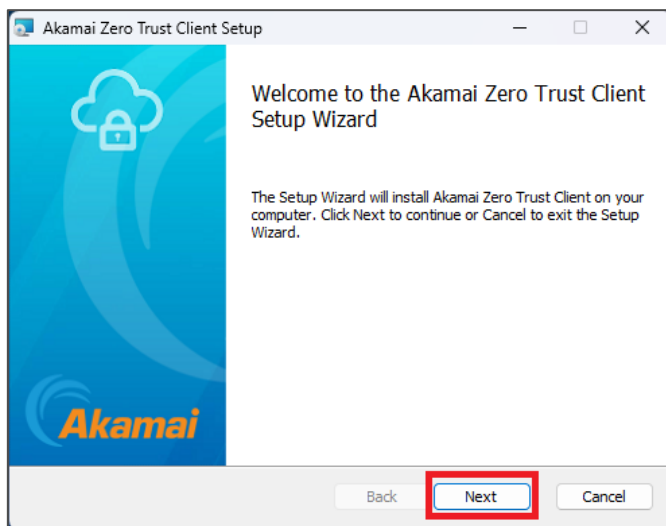
※また旧ソフトウェア（ETP Client）をご利用の方は、  
本手順の新ソフトウェア（ZTC）をインストールする過程で、  
自動的に旧ソフトウェア（ETP Client）がアンインストールされるため、  
事前のアンインストール作業は不要となっております。

# インストール方法

1. 初期セットアップツール一式を解凍し取り出した「ZTC.msi」をクリックし実行します。

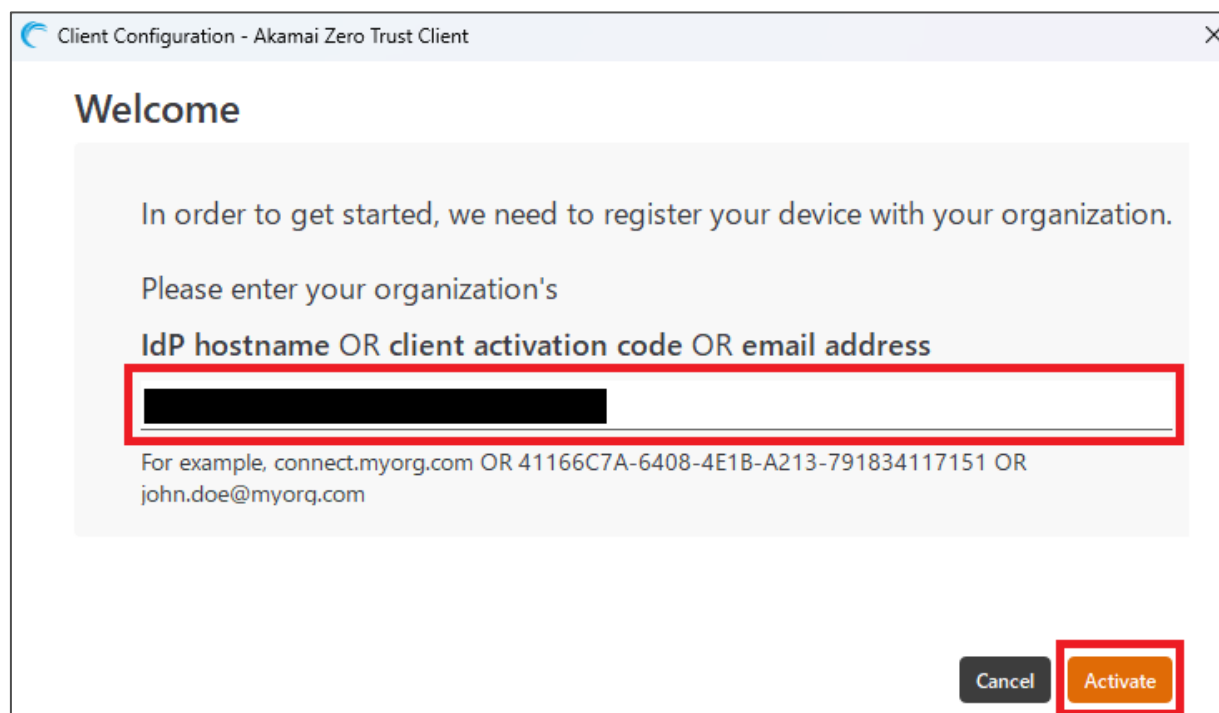


2. 赤枠をクリックしインストールを続けます。  
※旧ソフトウェア（ETP Client）をインストールされている場合は、  
このタイミングで自動的に旧ソフトウェアがアンインストールされます。



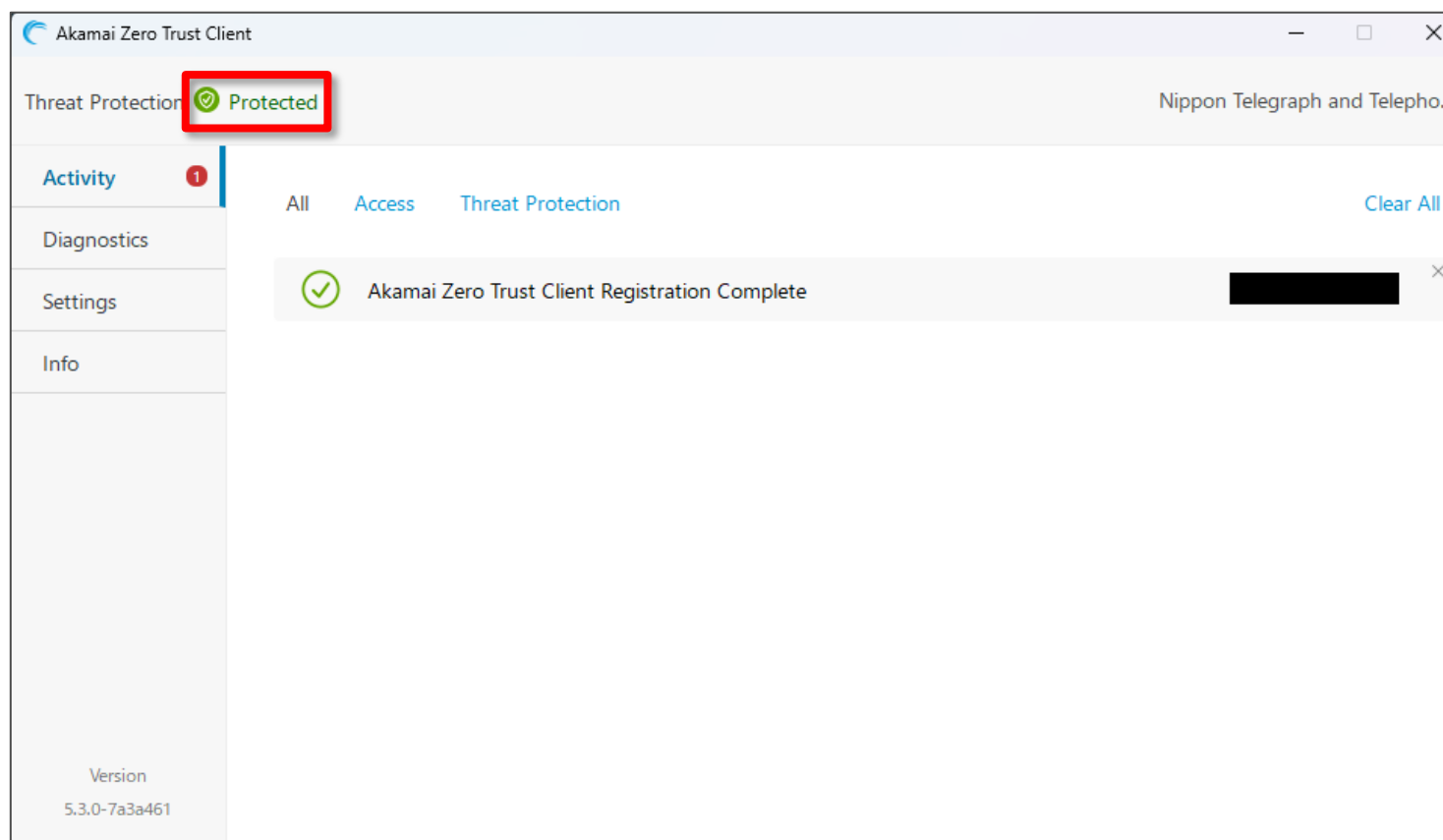
# インストール方法

- インストール完了後、ソフトウェアが起動します。  
もしソフトウェアが起動しない場合は[こちら](#)をご参照ください。  
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。  
「エンタイトルメントコード」を入力してください。  
[エンタイトルメントコードの確認方法](#)にて管理コンソールで確認する方法を記載しています。



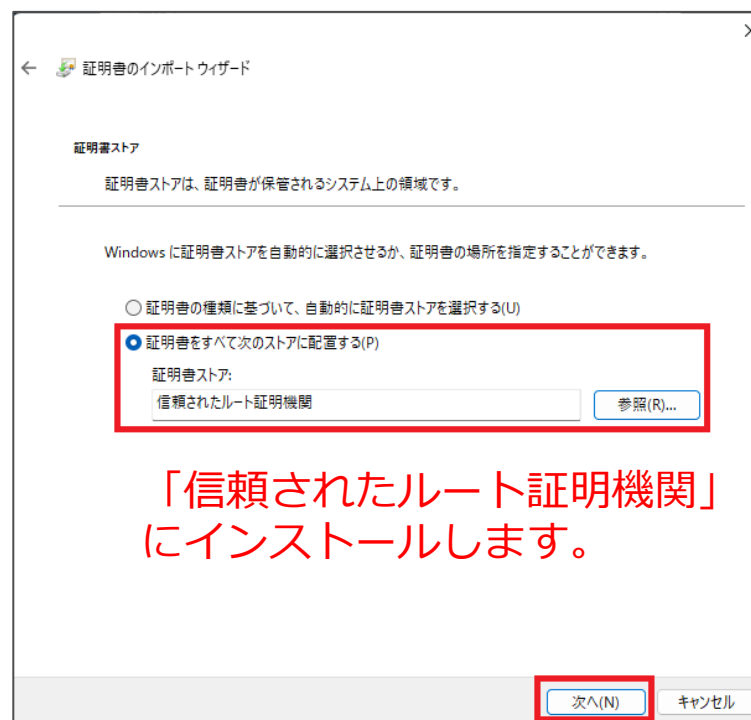
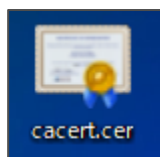
# インストール方法

4. 「エンタイトルメントコード」入力後、Protectedが表示されれば設定完了となります。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となります。



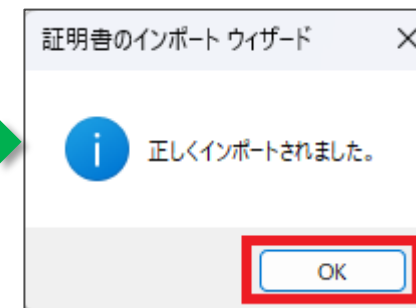
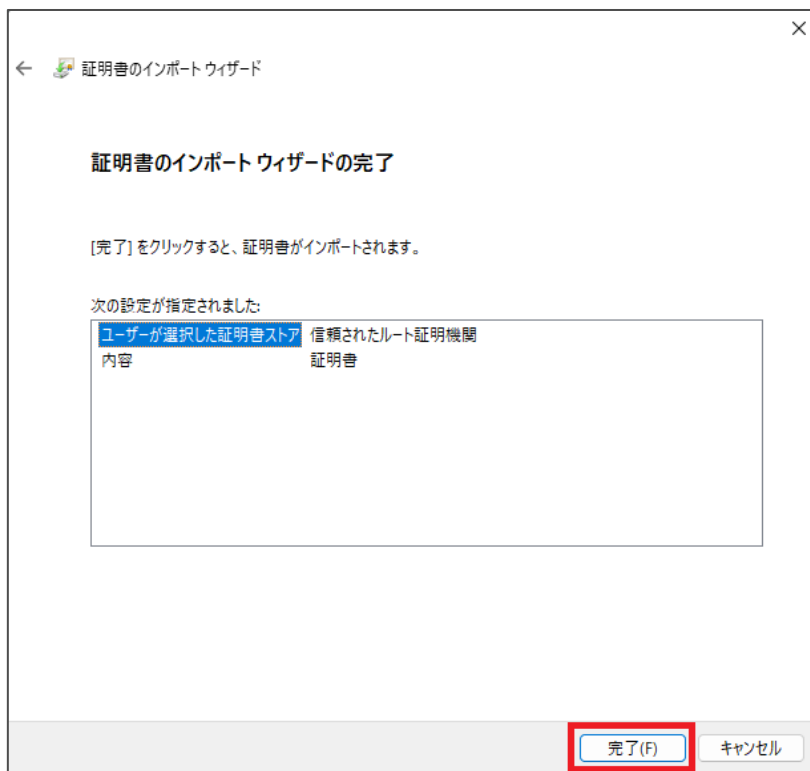
# インストール方法

5. 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。  
※旧ソフトウェアからアップグレードされている場合は本手順は不要となります。





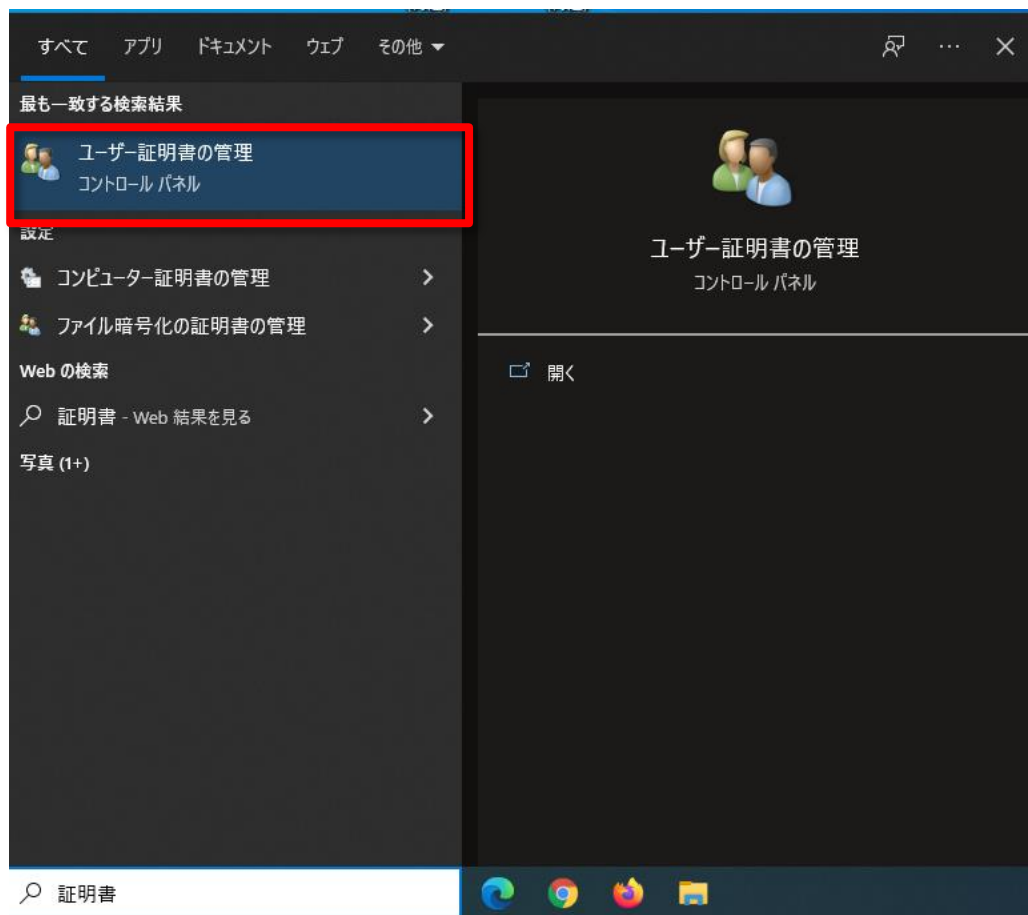
# インストール方法



# インストール方法

## 6. 証明書の確認方法

検索バーもしくはWindowsキーを押した後に「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

## 7. 証明書の確認方法

証明書インストール時に指定したフォルダを開き、  
フォルダ内に【Security Omakase Plan】があることが確認できれば、証明書の確認は以上です。

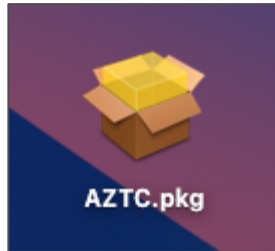
The screenshot shows the Windows Certificate Manager window titled 'certmgr - [証明書 - 現在のユーザー-信頼されたルート証明機関\*証明書]'. The left sidebar shows the tree view with '信頼されたルート証明機関' (Trusted Root Certification Authorities) expanded and highlighted with a red box. The main pane displays a list of certificates with the following columns: 発行先 (Issued By), 発行者 (Issued To), 有効期限 (Expiration Date), 目的 (Intended Purposes), フレンドリ名 (Friendly Name), 状態 (Status), and 証明書テンプレート (Certificate Template). The 'Security Omakase Plan' entry is highlighted in blue and outlined in 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...		
Security Omakase Plan	Security Omakase Plan	2122/02/25	<すべて>	<なし>		
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...		

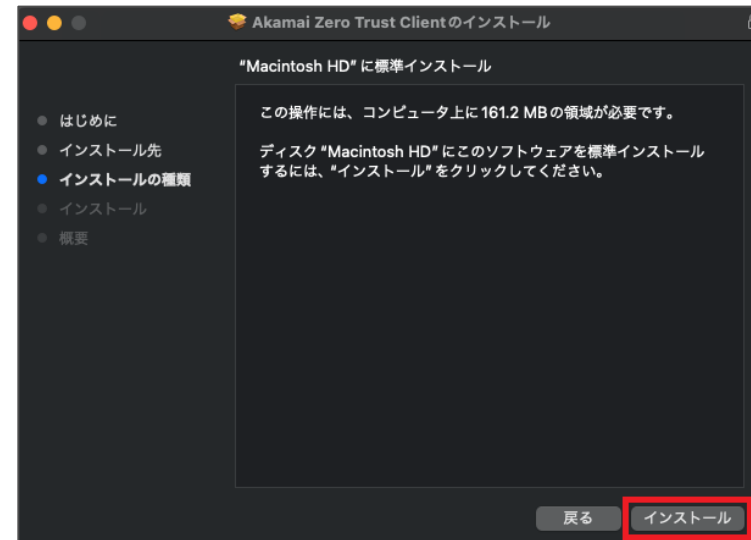
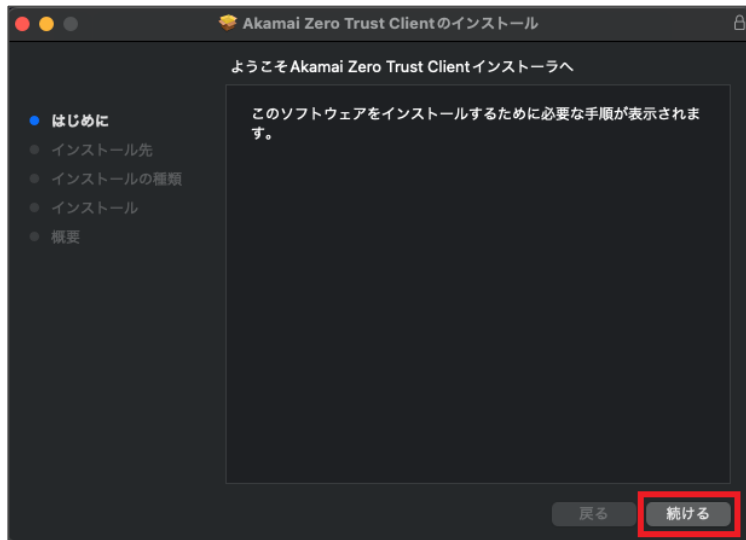
信頼されたルート証明機関 ストアには 51 個の証明書があります。

# インストール方法

1. 初期セットアップツールを解凍し取り出した「ZTC.pkg」をクリックし実行します。

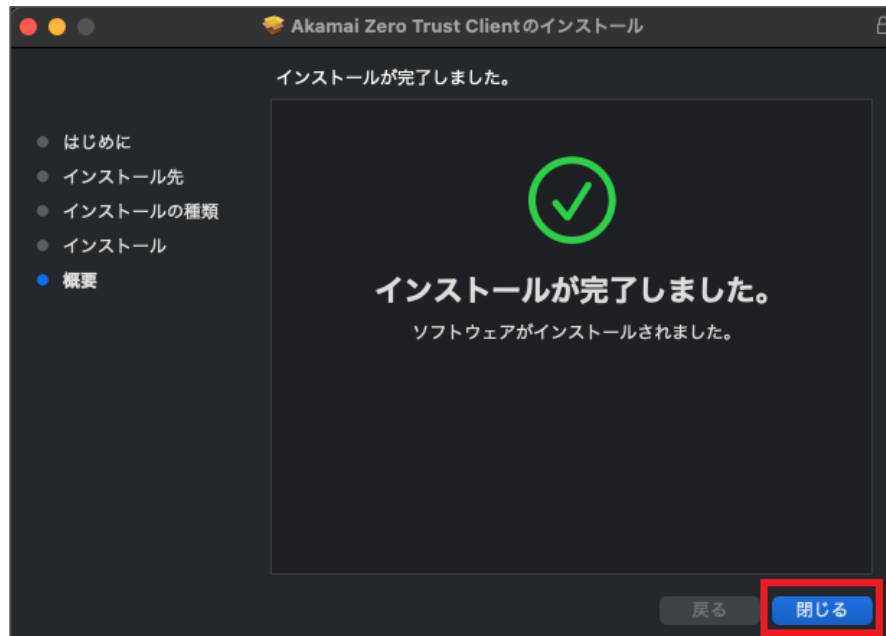


2. 赤枠をクリックしインストールを続けます。  
※旧ソフトウェア（ETP Client）をインストールされている場合は、  
このタイミングで自動的に旧ソフトウェアがアンインストールされます。



# インストール方法

3. インストール完了後、ソフトウェアが起動します。  
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。  
「エンタイトルメントコード」を入力してください。  
[エンタイトルメントコードの確認方法](#)にて管理コンソールで確認する方法を記載しています。



### Welcome

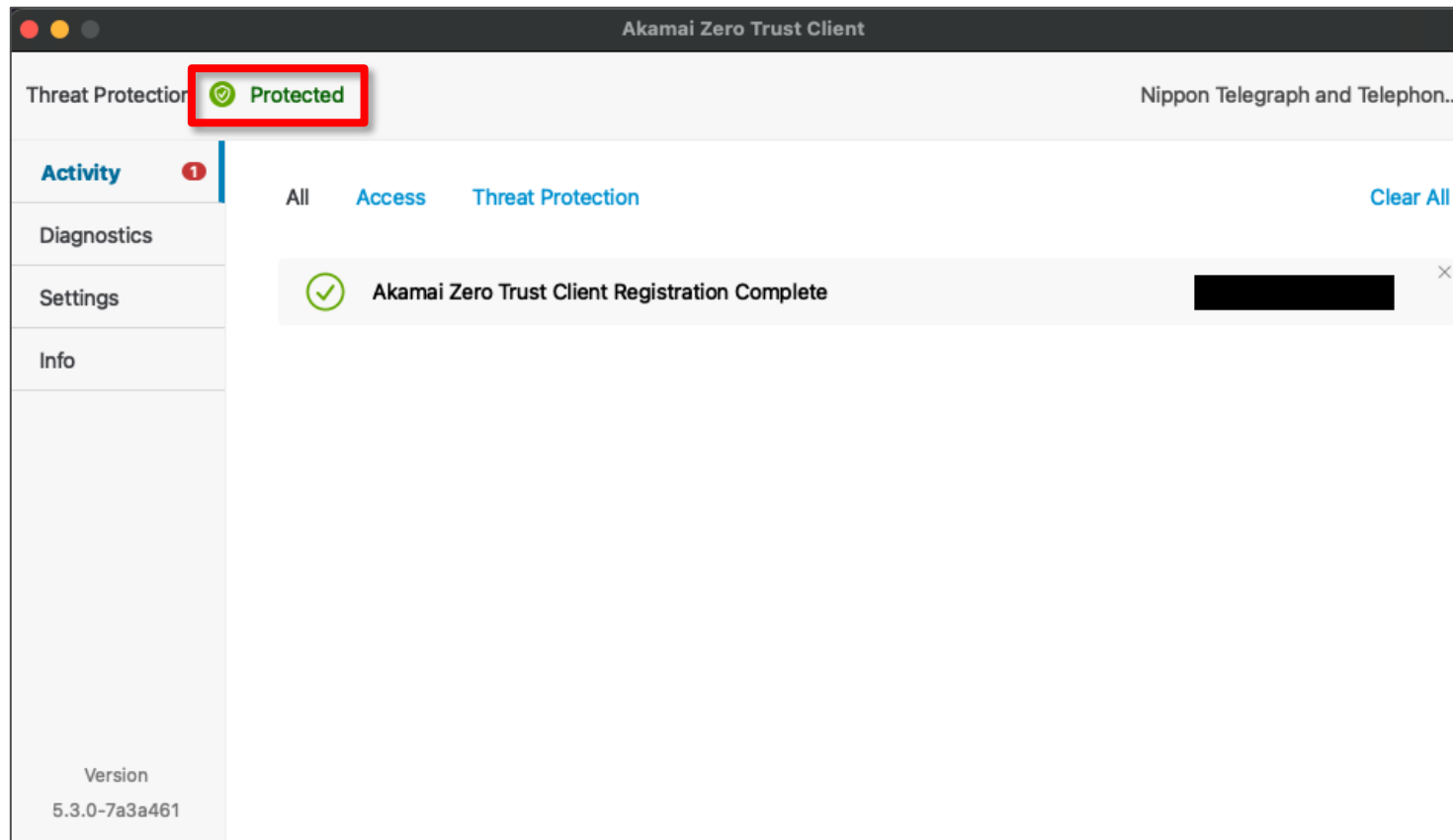
In order to get started, we need to register your device with your organization.

Please enter your organization's  
**IdP hostname OR client activation code OR email address**

For example, connect.myorg.com OR 41166C7A-6408-4E1B-A213-791834117151 OR john.doe@myorg.com

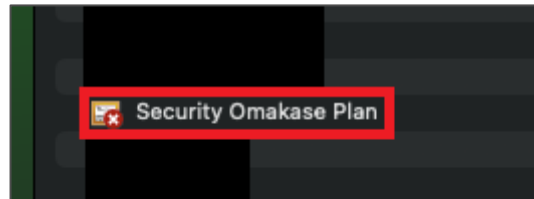
# インストール方法

- 「エンタイトルメントコード」入力後、Protectedが表示されれば設定完了となります。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となります。



# インストール方法

5. 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。  
※旧ソフトウェアからアップグレードされている場合は本手順は不要となります。

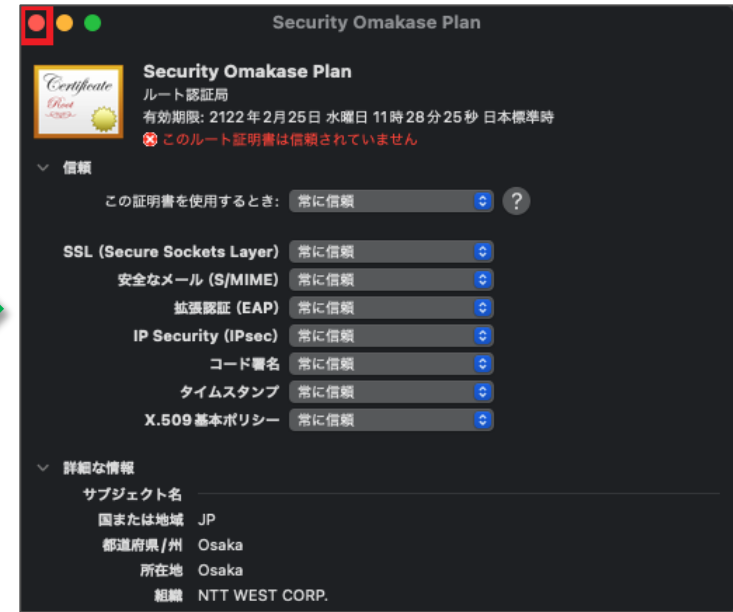
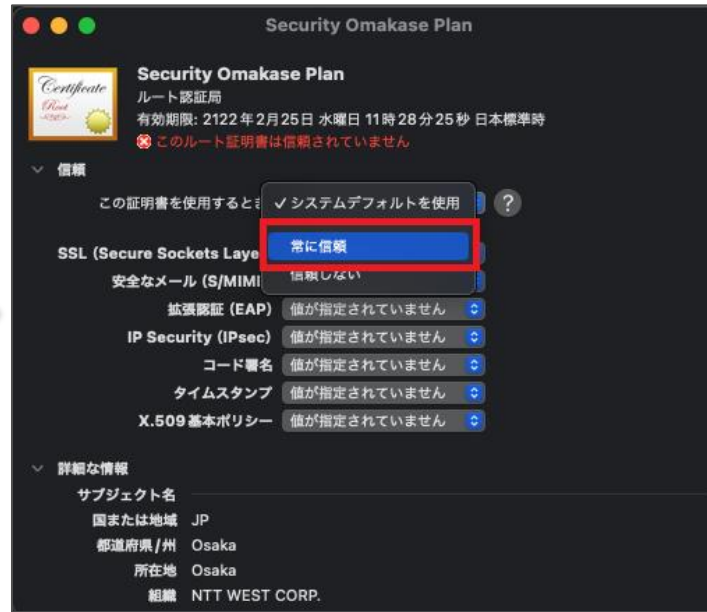


キーチェーンアクセスに  
「Security Omakase Plan」が入ります。  
このルート証明書を実ダブルクリックします。



「> 信頼」をクリックして展開します。

# インストール方法



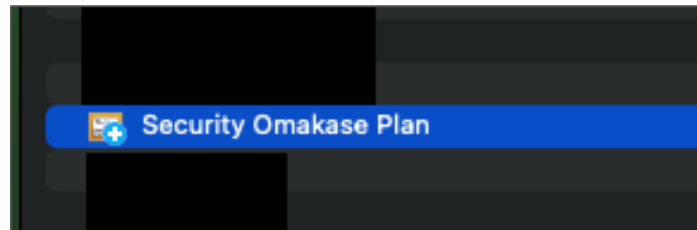
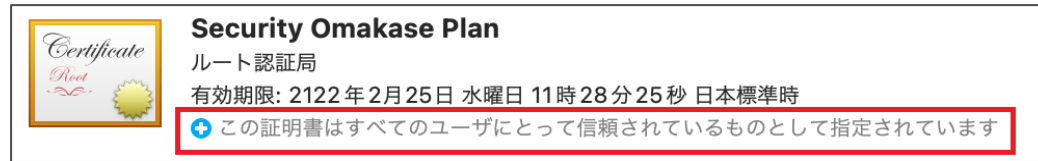
「この証明書を使用するとき:」の「システムデフォルトを使用」を変更します。

「常に信頼」を選択した後に閉じます。



# インストール方法

6. 証明書がインストール後、下図の状態になった事が確認できれば完了となります。



## アンインストール方法

---

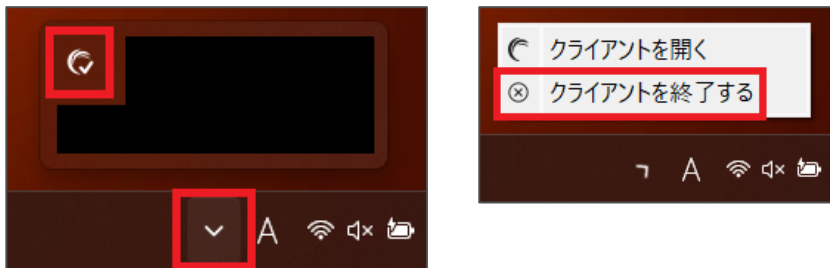
アンインストールは端末OSを確認頂き、  
下記リンクより適切な方法のご利用をお願いいたします。

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

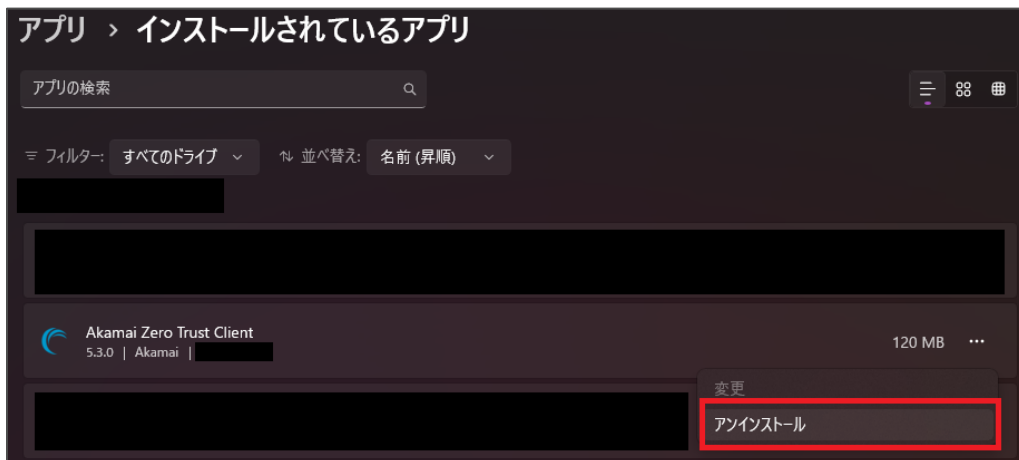
※また旧ソフトウェア（ETP Client）から新ソフトウェア（ZTC）へのアップグレードに際し、事前に旧ソフトウェアのアンインストール作業は**不要**となっております。  
新ソフトウェア（ZTC）のインストールの過程で自動的にアンインストールされます。  
アンインストールのタイミングは[こちら](#)を参照ください。

# アンインストール方法

1. はじめにタスクトレイで実行中のソフトウェアを終了します。終了後はアイコンが消えます。



2. 設定のインストールされているアプリより、「Akamai Zero Trust Client」をアンインストールします。



# アンインストール方法

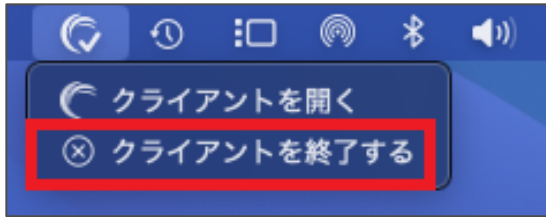
1. ソフトウェアのアンインストール後、証明書も削除する必要があります。  
検索バーもしくはWindowsキーを押した後に「証明書」と入力することで、【ユーザ証明書の管理】が表示されるのでクリックします。
2. 証明書フォルダに格納されている「Security Omakase Plan」を右クリックし、削除→はいと続け削除します。
3. アンインストール手順は以上となります。

The screenshot illustrates the steps to delete a certificate in Windows. On the left, the Windows Settings app is open to 'User Certificate Management'. The 'Certificates' folder is selected under 'Trusted Root Certification Authorities'. The 'Security Omakase Plan' certificate is highlighted in the list. A context menu is open over it, with 'Delete (D)' selected. A warning dialog box is displayed, asking for confirmation to delete the certificate, with 'Yes (Y)' selected.

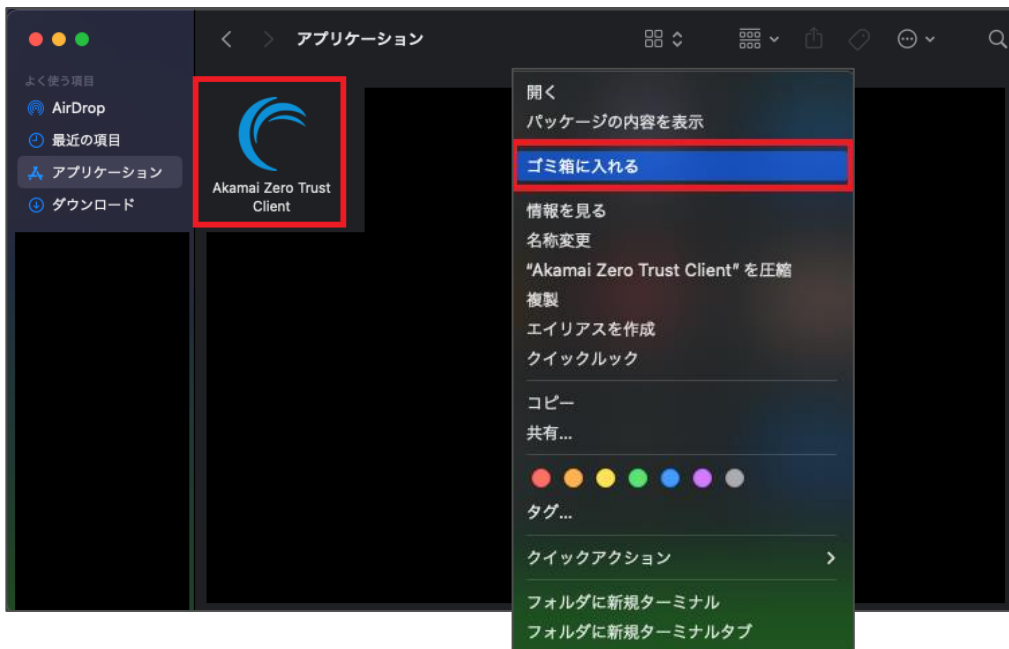
発行先	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプレート
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	2039/10/23	<すべて>	Microsoft Time Sta...		
NO LIABILITY ACCEPTED, (c)97 Ver...	NO LIABILITY ACCEPTED, (c)97 Ver...	2004/01/08	タイムスタンプ	VeriSign Time Stam...		
QuoVadis Root CA 2	QuoVadis Root CA 2	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 System...		
Security Communication RootC...	Security Communication RootCA2	2023/09/30	クライアント認証, コー...	SECOM Trust System...		
Security Omakase Plan	Security Omakase Plan	2122/02/25	<すべて>	<なし>		

# アンインストール方法

1. はじめにタスクトレイで実行中のソフトウェアを終了します。終了後はアイコンが消えます。

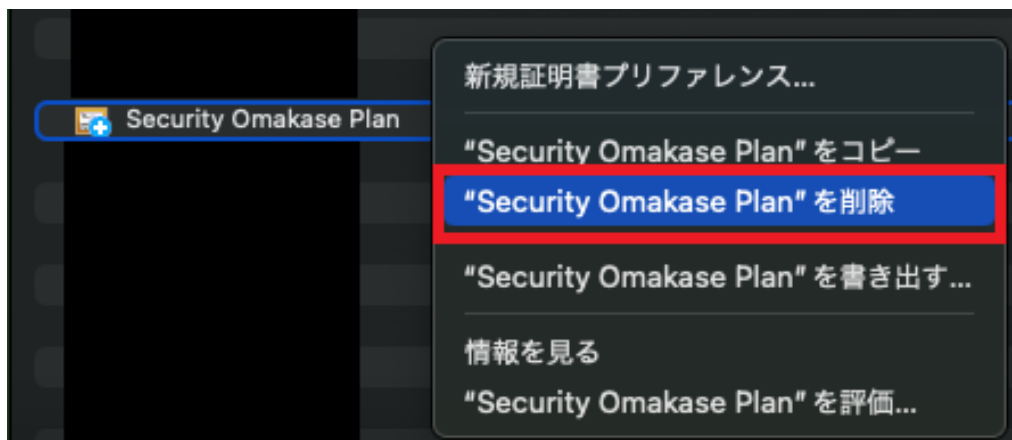


2. ソフトウェア終了後、ファイnderからアプリケーションを開き、「Akamai Zero Trust Client」をゴミ箱に入れるを選択することでアンインストールとなります。



## アンインストール方法

1. ソフトウェアのアンインストール後、証明書も削除する必要があります。  
キーチェーンアクセスを開き、登録中の「Security Omakase Plan」を右クリックし、「Security Omakase Plan」を削除をクリックし、削除を実施します。
2. アンインストール手順は以上となります。



## 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。

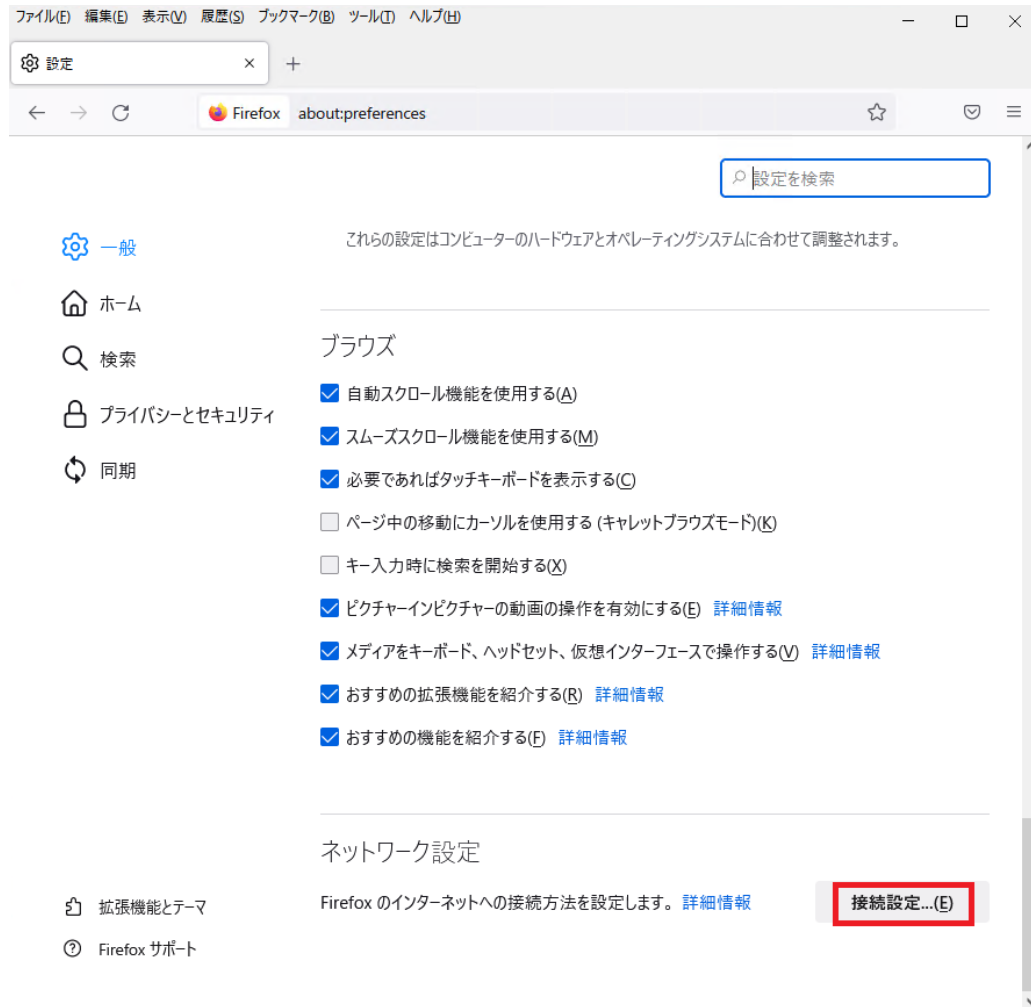
1. 古いバージョンのFirefoxをインストールしてバージョンアップしながら使い続けている場合は、FirefoxがOS側のProxy設定を使用しない設定になっている可能性があります。この場合に、ETP Clientが正しく動作するためには、追加の設定が必要です。



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)

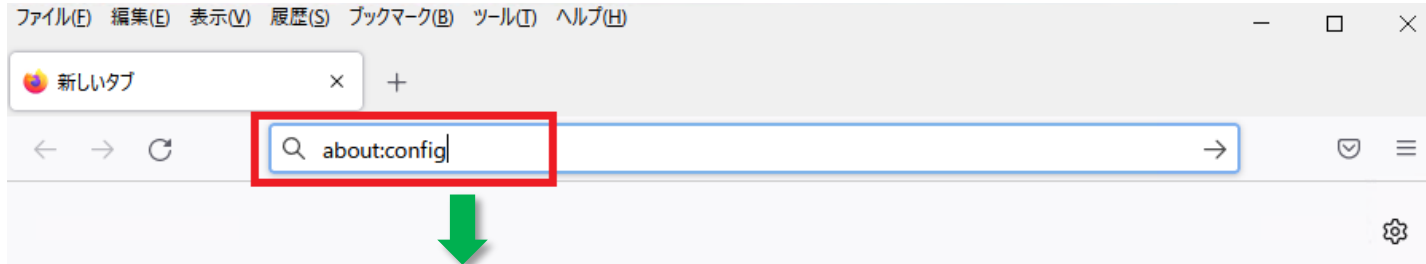
例: .mozilla.org, .net.nz, 192.168.1.0/24  
localhost, 127.0.0.1/8, ::1 ^は常にプロキシなしで接続します。

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



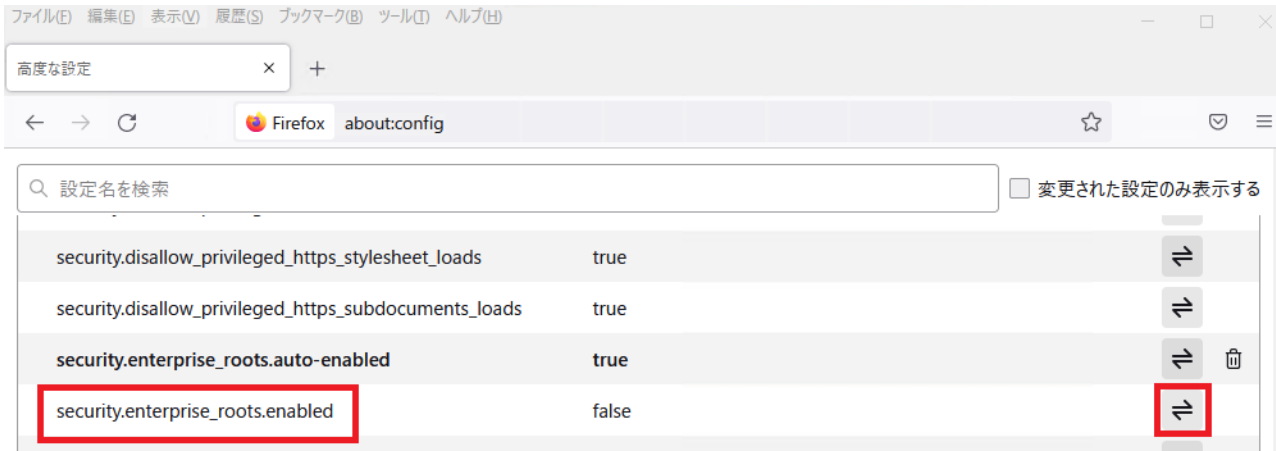
すべて表示



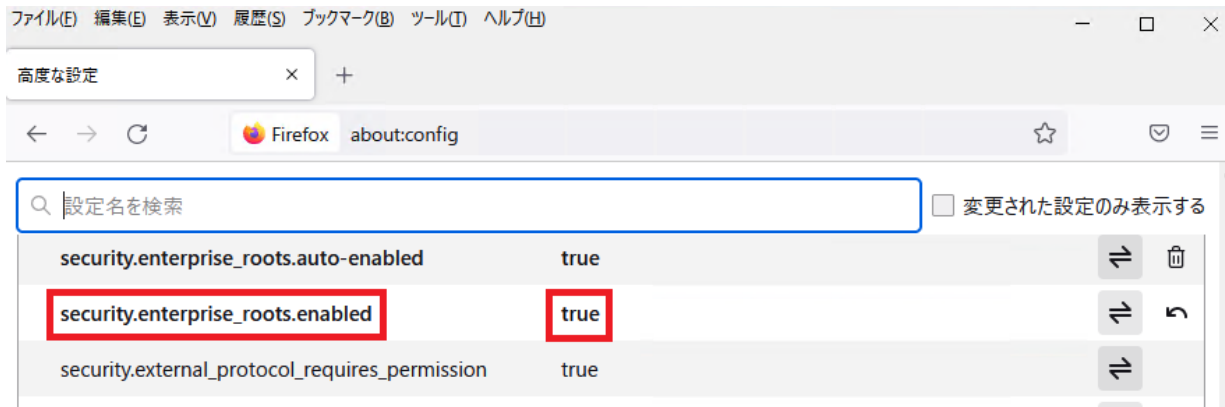
これらの設定を変更すると、Firefox のセキュリティ、パフォーマンスに深刻な問題を引き起こす恐れがあります。

「すべて表示」を押します。

# 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

---

本章では下記項目でソフトウェアの操作を説明します。

- [操作画面の表示方法](#)
- [操作画面の言語変更方法](#)
- [機能停止方法](#)
- [機能再開方法](#)
- その他画面説明
  - [動作状況](#)
  - [診断](#)
  - [情報](#)

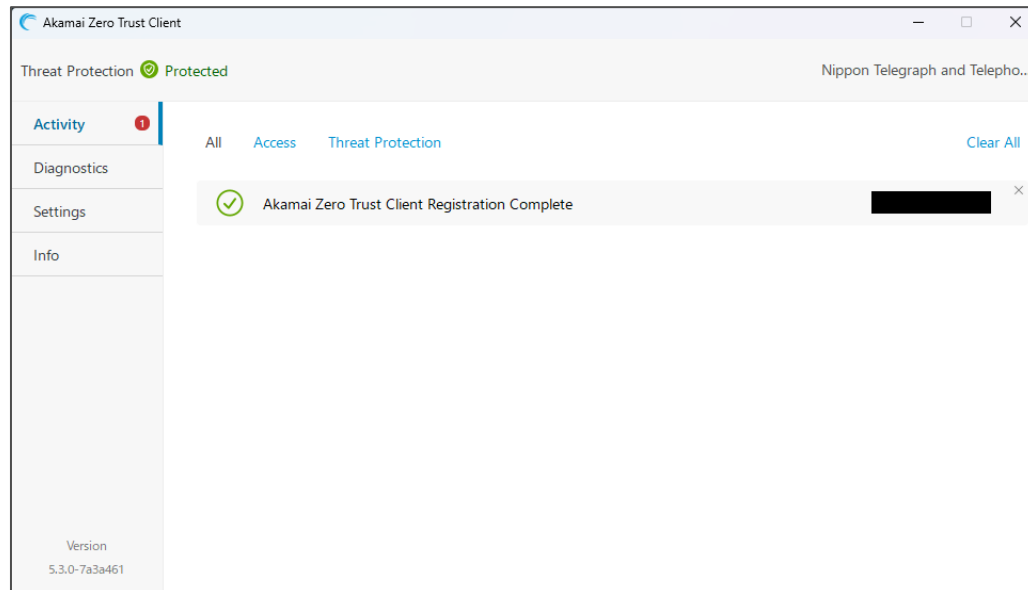
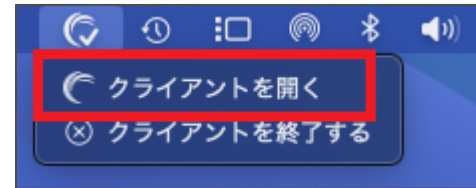
# ソフトウェアの操作方法（操作画面の表示方法）

ソフトウェアの操作画面を表示する場合、タスクトレイのアイコンを右クリックし、「クライアントを開く」をクリックすることで表示できます。

## Windows

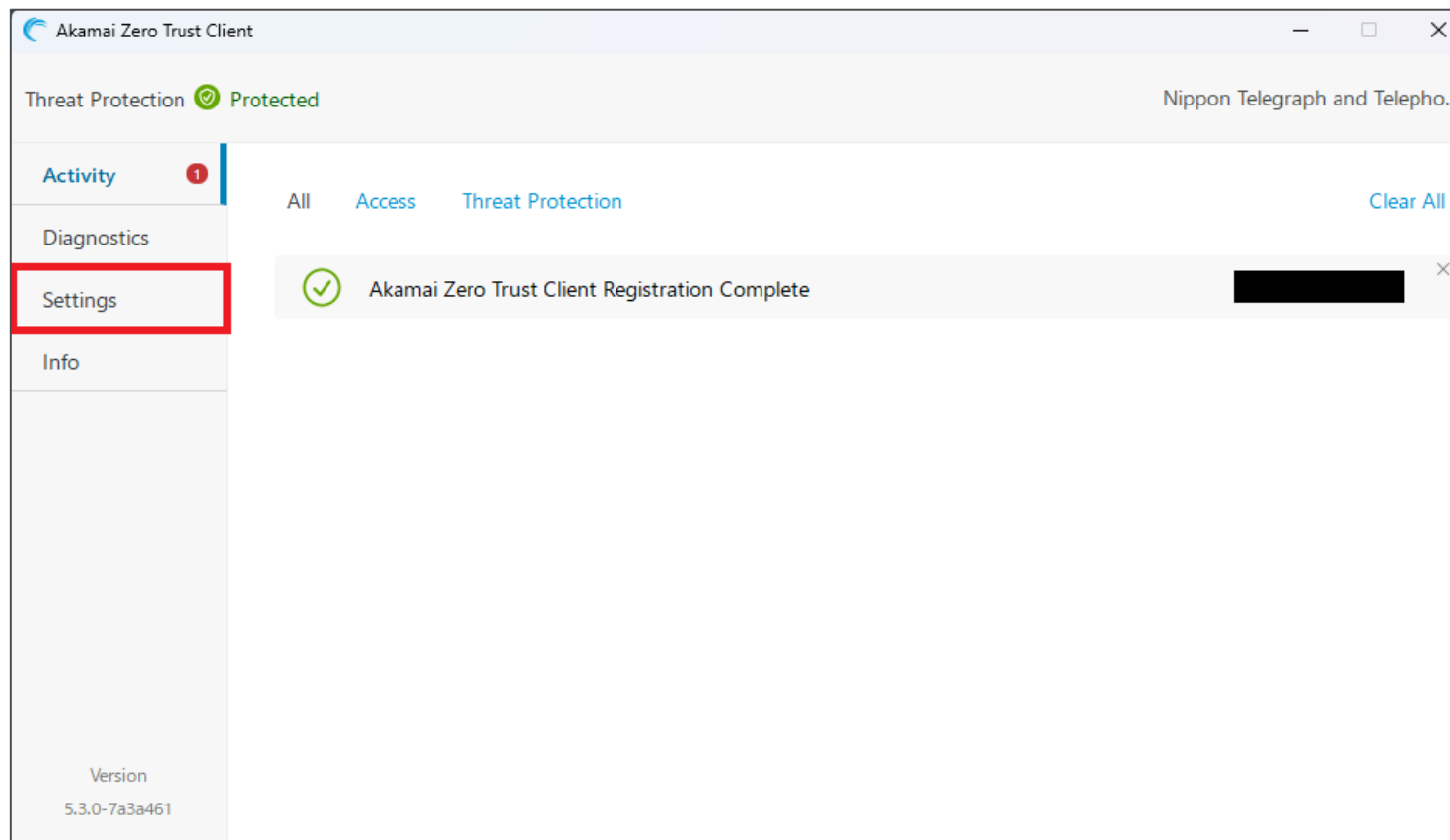


## macOS



# ソフトウェアの操作方法（操作画面の言語変更方法）

初期設定では言語が英語に設定されております。  
手順通りに赤枠をクリックすることで、言語を日本語に設定できます。

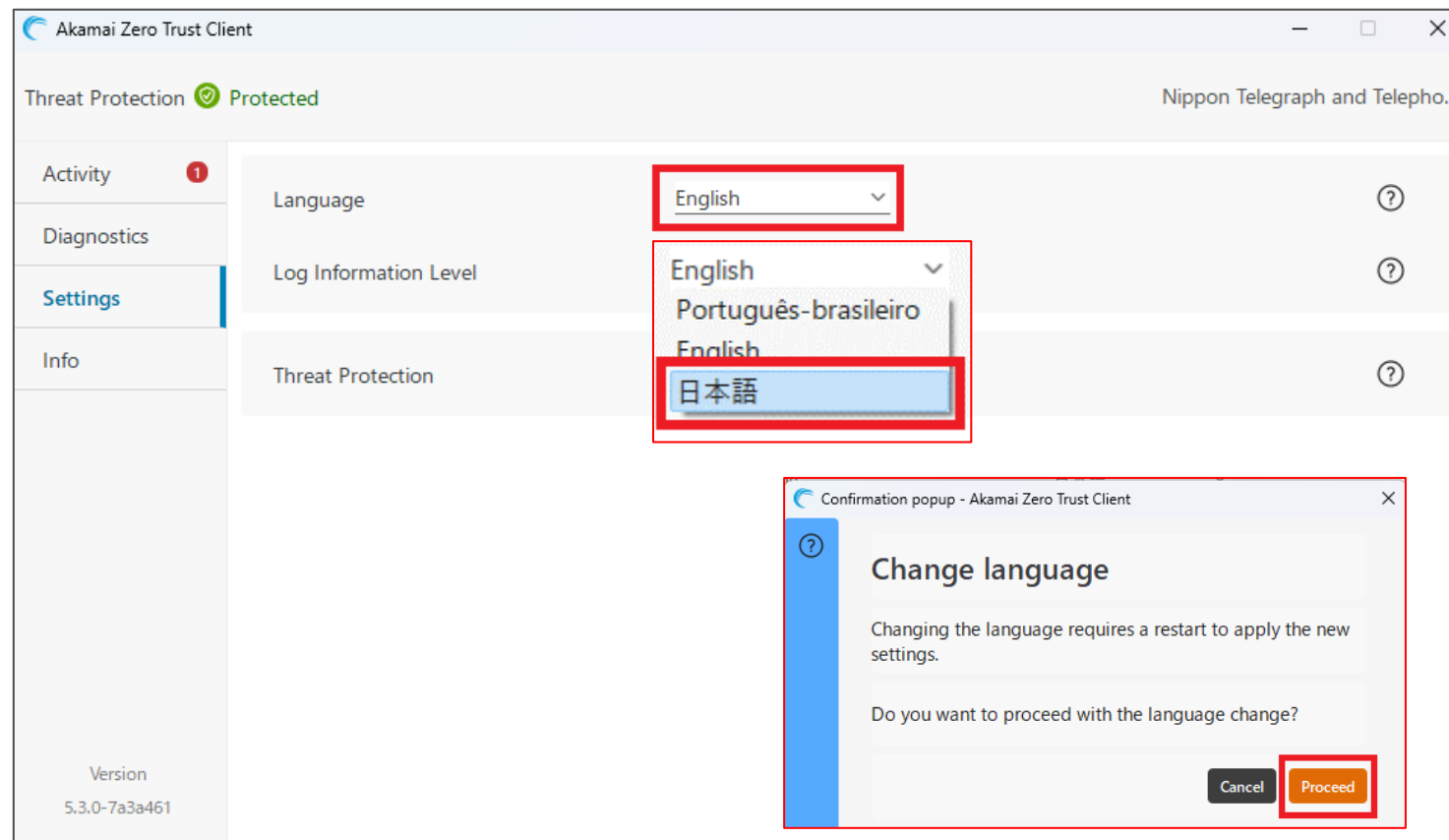




# ソフトウェアの操作方法（操作画面の言語変更方法）

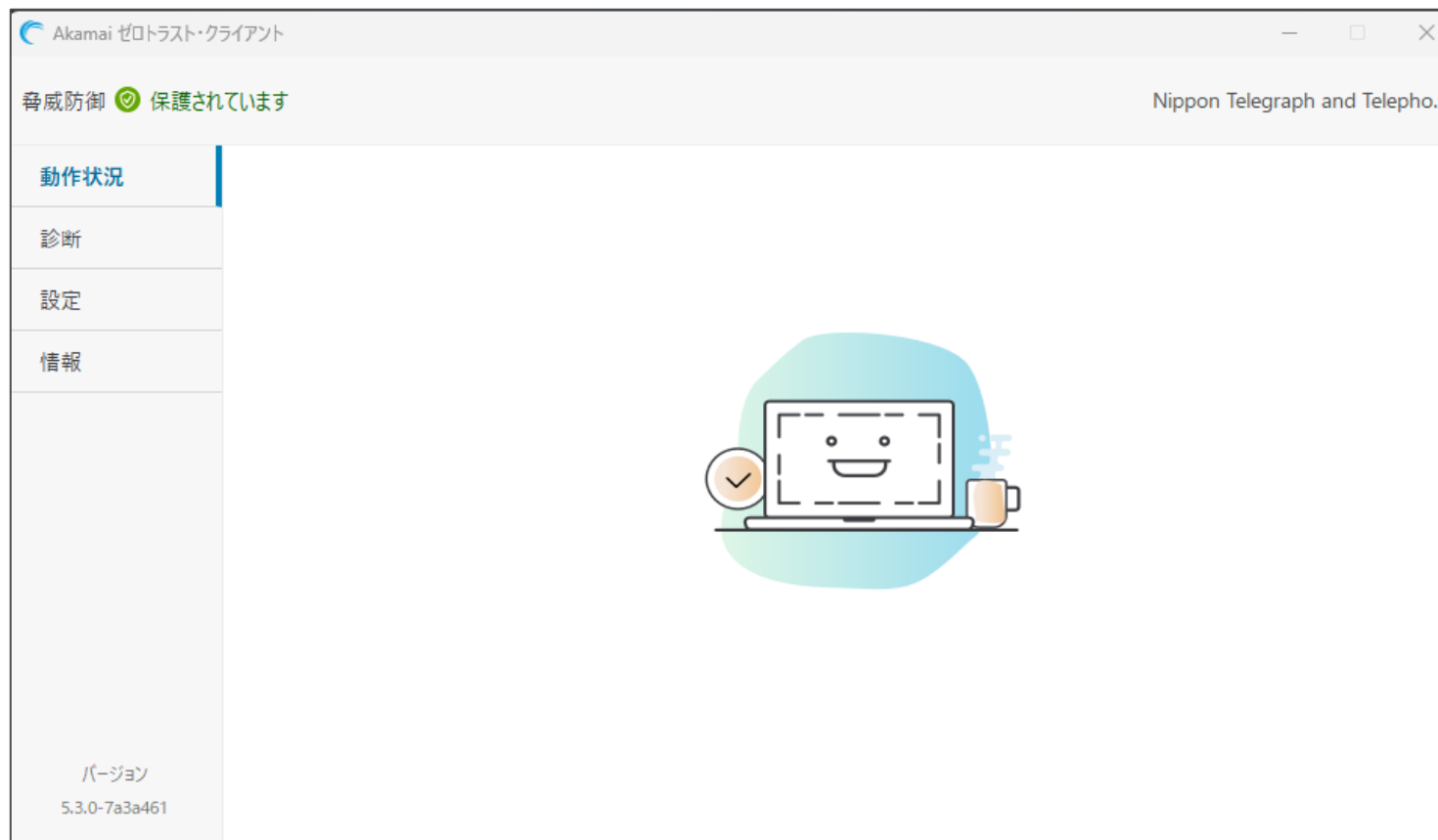
初期設定では言語が英語に設定されております。

手順通りに赤枠をクリックすることで、言語を日本語に設定できます。



# ソフトウェアの操作方法（操作画面の言語変更方法）

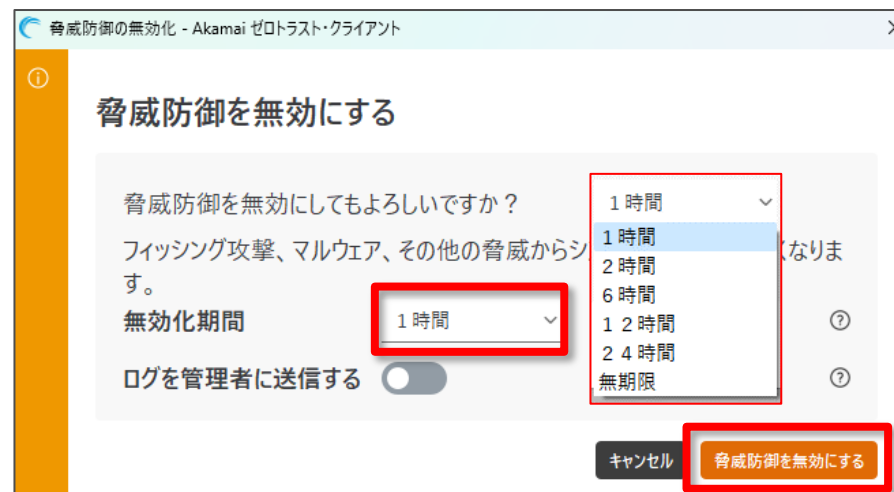
ソフトウェアが再起動し日本語表示の画面に切り替われば完了となります。



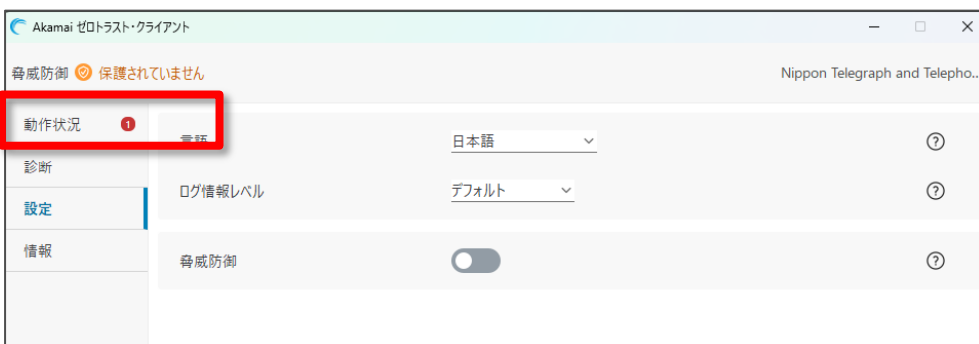
# ソフトウェアの操作方法（機能停止方法）

## 1. 機能を停止したい場合

「設定」をクリックし、緑色の脅威防御のボタンをクリックすることで停止できます。停止に際し無効化期間を選択する必要があり、任意で期間を変更できます。



## 2. 無効化後、灰色にボタンが変わり、保護が外れます。



# ソフトウェアの操作方法（機能再開方法）

## 1. 機能を再開したい場合

脅威防御の灰色のボタンをクリックすることで再開できます。

無効化期間で無期限以外を選択していた場合でも同様の動作となります。

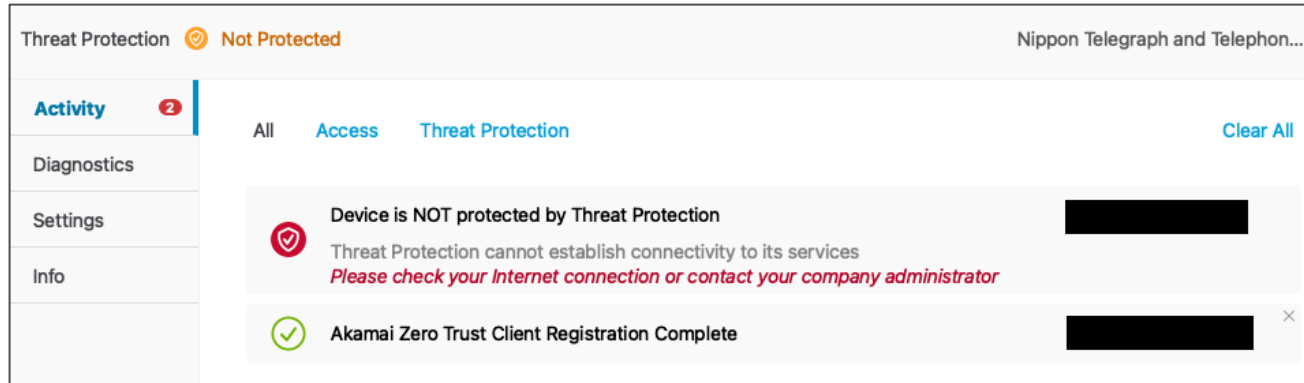


## 2. 有効化後、「保護されています」が表示されれば有効化完了となります。



# ソフトウェアの操作方法（動作状況）

1. 「動作状況」では、脅威防御の有効状態やポリシーによるアクセスを遮断されたHTTPリクエストの通知などが表示されます。



2. 下記例ではポリシーによりSportsカテゴリをブロック指定し、アクセスを試みたものになります。赤枠の図は該当ページへアクセス時に表示される通知と画面になります。



# ソフトウェアの操作方法（診断）

1. 「診断」では接続不良等のトラブル発生時に原因特定を補助する機能が提供されます。クイックテストでは簡易的に端末チェックを実施し問題個所を特定できます。
2. フル診断やアラートで取得可能な情報はメーカー調査用となるため、サポートセンタの指示のもとご利用ください。

Akamai ゼロトラスト・クライアント

脅威防御 保護されています

Nippon Telegraph and Telepho...

動作状況

診断

設定

情報

バージョン  
5.3.0-7a3a461

クイックテスト フル診断 アラート

クイックテストでは多く見られる問題を検出します。通常は1分以内に完了します。

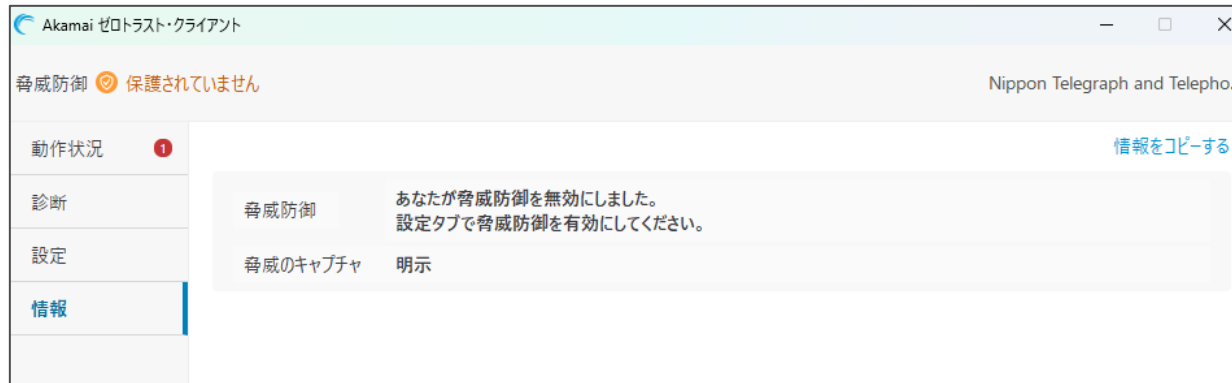
クイックテストを実行する

テスト結果の出所： 2024-06-06 06:20:54

- ✓ インストールチェック
- ✓ ネットワーク接続チェック
- ✓ コンポーネントチェック
- ✓ 設定チェック

# ソフトウェアの操作方法（情報）

1. 「情報」では簡易的に脅威防御が有効にならない場合の情報が表示されます。トラブルシューティング時の初期に参考頂けます。



2. 脅威防御が問題なく機能している場合は以下のように表示されます。



# ソフトウェア使用上の注意

---

本章ではソフトウェア使用上の注意を説明します。



# ソフトウェア使用上の注意

- ソフトウェアは動作時にプロキシ設定を上書きし、動作停止時やアンインストール時に設定を初期化します。ソフトウェアインストール前に手動で設定を行っていた場合、元の設定に戻らないため、再設定が必要となりますのでご注意ください。

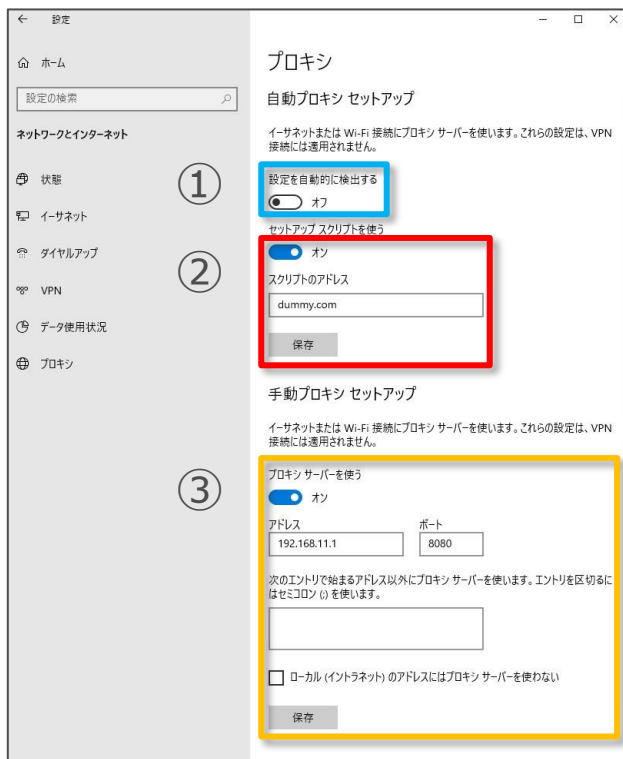
	PCのプロキシ設定の項目	ETP Clientインストール前の設定値	ETP Clientが動作中の設定値	動作停止とアンインストール後の設定値
①	自動プロキシ セットアップ 設定を自動的に検出する	オン	オン	オン
		オフ	オフ	オン
②	自動プロキシ セットアップ セットアップスクリプトを使う	オン	オフ	オフ (スクリプトのアドレスの設定値が クリアされる)
		オフ	オフ	オフ
③	手動プロキシ セットアップ プロキシ サーバーを使う	オン	オン (http=127.0.0.1:80 80;https=127.0.0.1: 8080)	オフ (アドレスなどの設定値が クリアされる)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

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

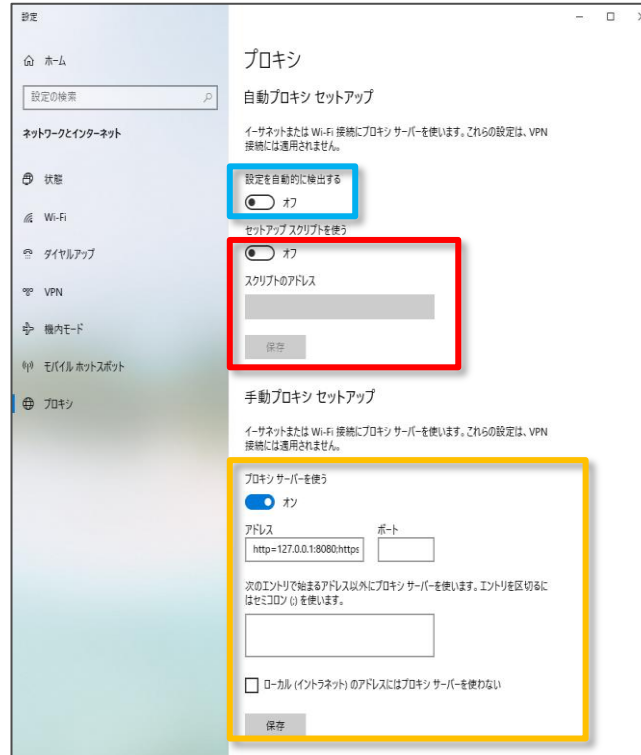
# ソフトウェア使用上の注意

## 2. 実際の画面推移となります。

【ソフトウェアインストール前の設定値参考例】

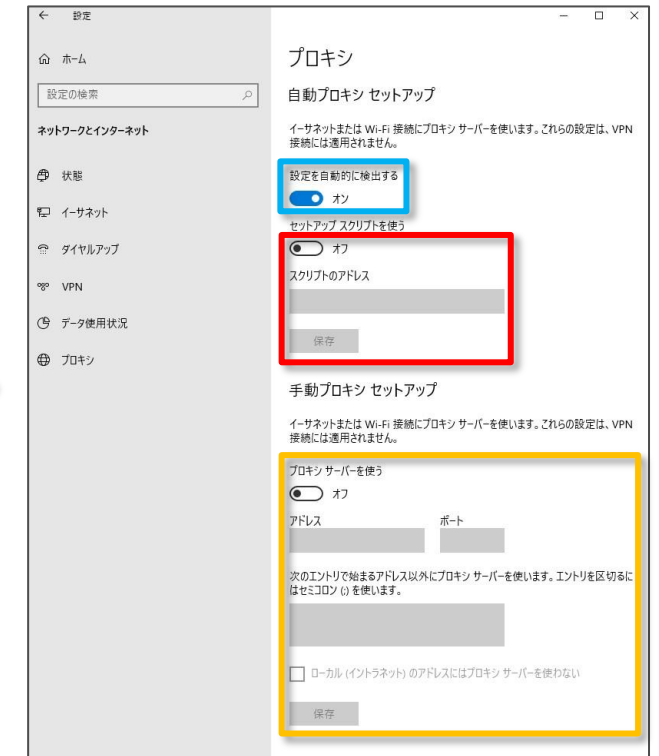


ソフトウェア動作時/  
インストール後



ソフトウェア停止/  
アンインストール後

下記画像の設定値へと初期化されるため、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。



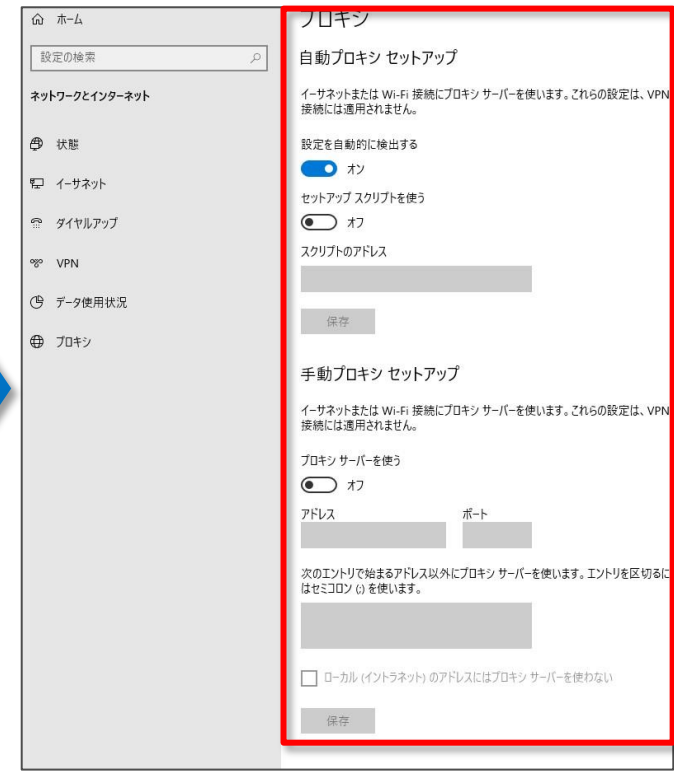
# 【参考】プロキシ設定の確認方法

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

---

本章では管理コンソールへの初回ログイン方法について説明します。  
初回ログイン後は設定したパスワードと2要素認証を用いることでログインできます。

# 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

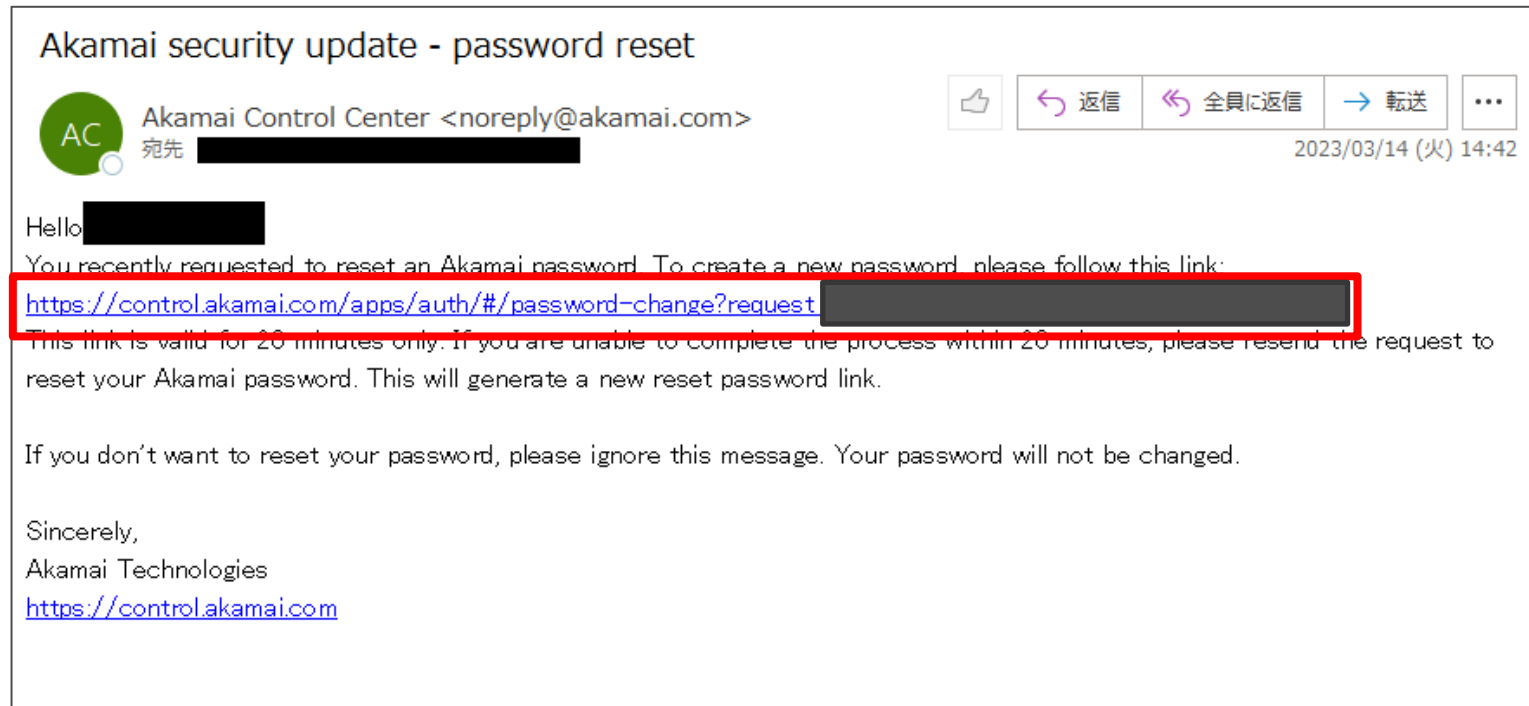
5. パスワード設定用のメールが送信されるので、メールを確認します。



# 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。

6





# 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 [REDACTED]

[REDACTED]

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

Akamai  
CONTROL CENTER

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

13. 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

13

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

14. 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。
15. 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

16. 「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

16

# 管理コンソールへの初回ログイン

17. 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](#)

17

### 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

18. 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**

18



## エンタイトルメントコードの確認方法

---

ソフトウェアのインストールに際し、  
エンタイトルメントコードを入力いただく必要があります。  
本章では管理コンソールでエンタイトルメントコードを確認する方法を説明します。

他にも開通時に届く開通案内メールにて確認することができます。  
件名：【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

# エンタイトルメントコードの確認方法

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

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

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

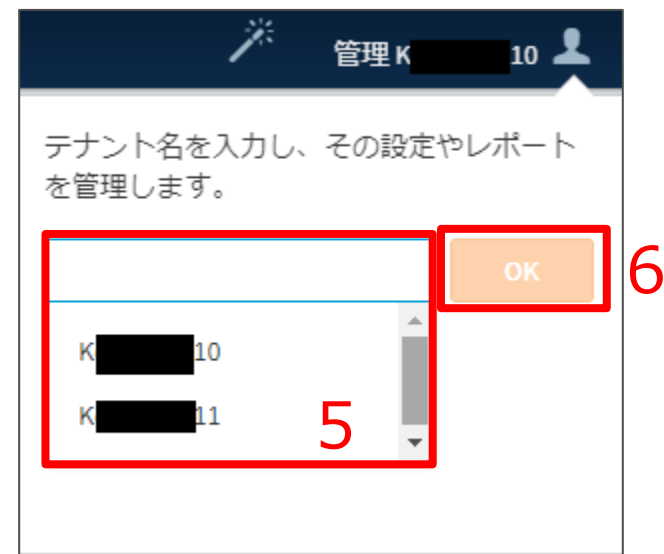
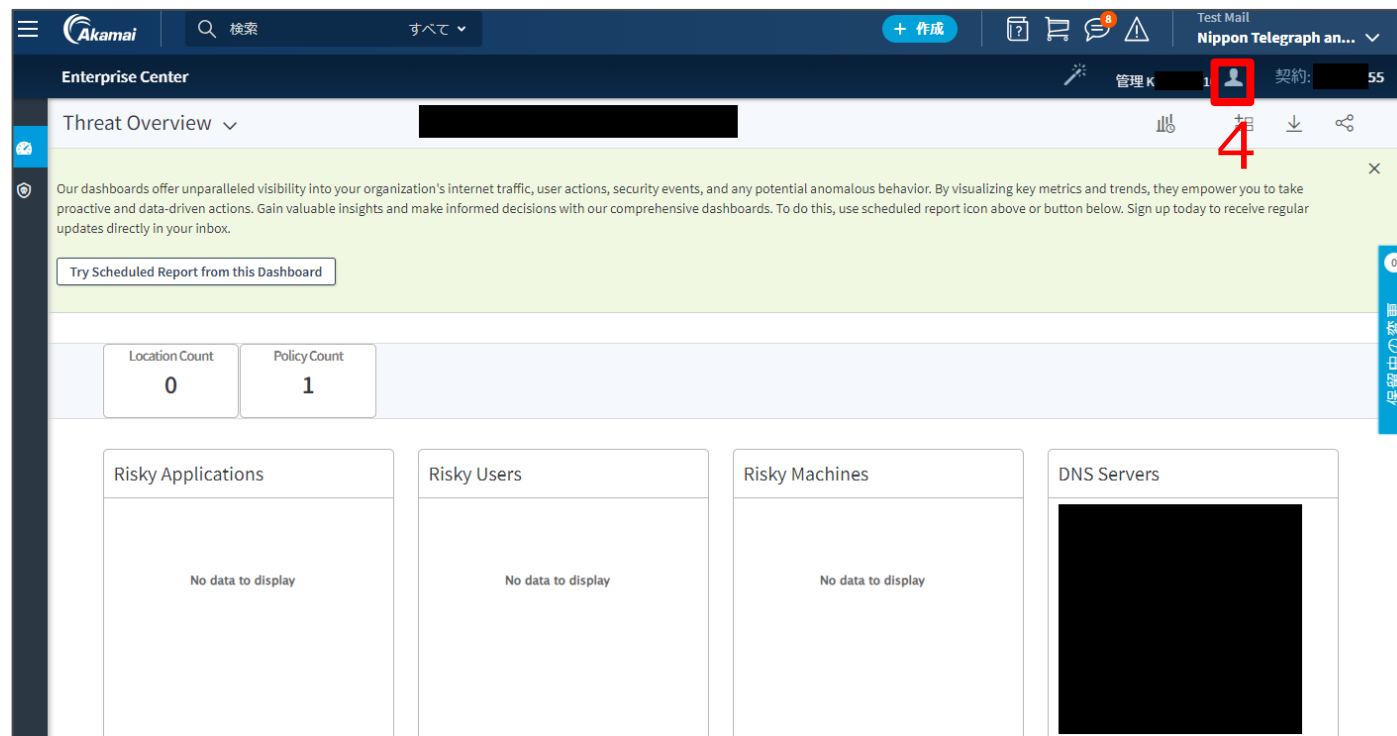
Enterprise Center

アカウント管理者

- ID およびアクセス契約
- SLA テスト
- Marketplace

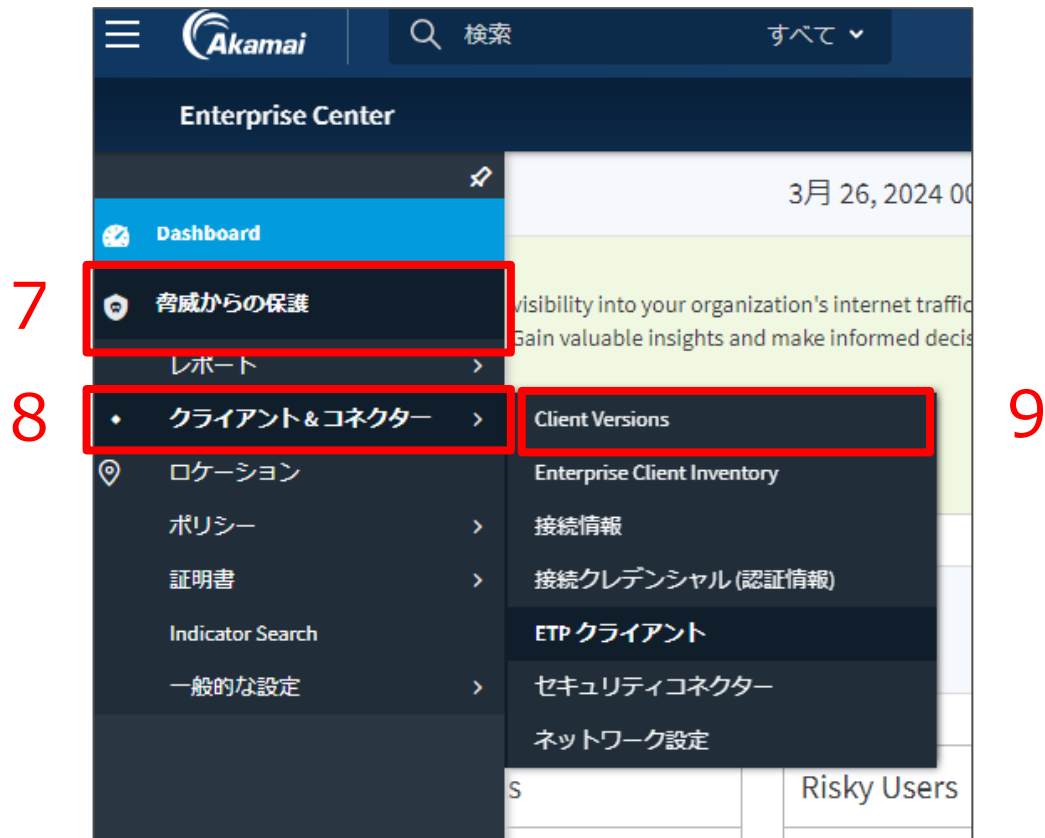
## エンタイトルメントコードの確認方法（複数契約者様向け）

3. 同一のメールアドレスにより複数の契約を頂いている場合、一つのユーザに複数のテナントが割り当てられております。次の手順でテナントを切り替えて管理することができます。
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テナント名が表示されるので、任意のものを選択します。なおテナント名はお客様IDが登録されております。
6. 「OK」をクリックすると、選択したテナントに切り替わります。



# エンタイトルメントコードの確認方法

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、「Client Versions」をクリックします。



# エンタイトルメントコードの確認方法

10. 「Activation」をクリックします。
11. エンタイトルメントコードを確認することができます。  
画面上「Activation Code」と表記されますが、エンタイトルメントコードと同一のものになります。
12. 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。

脅威からの保護 > クライアントとコネクター

## CLIENT VERSIONS

Version Control    設定    **Activation** 10

Activate Managed Devices 12

**Activation Code** 11    3315471d-b831-48ed-a621-17042a74a8e3    [Copy] [Refresh]

Activate Unmanaged Devices

Corporate domains    企業のメールアドレスを入力

You can send users an email that contains an activation code or you can download codes in a CSV file.  
If you download codes in a CSV file, you need to communicate the codes to users. You can generate a maximum of 1000 codes.  
Enter valid email addresses or identifiers for your users.

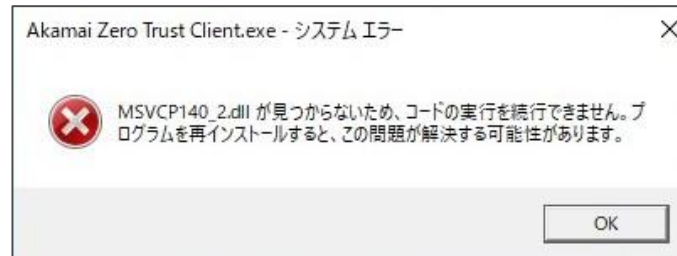
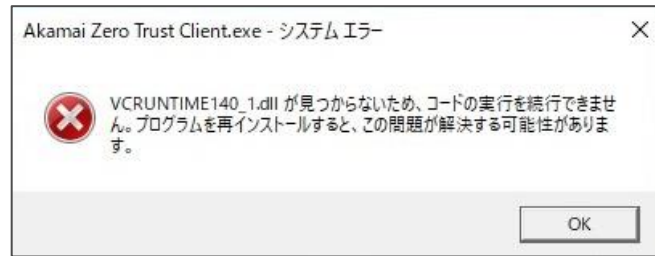
## 既知のトラブルと対処方法

---

- [新ソフトウェアインストール時のトラブル](#)

# 既知のトラブルと対処方法（新ソフトウェアインストール時のトラブル）

旧ソフトウェア（ETP Client）から新ソフトウェア（ZTC）へアップグレード時、ソフトウェアが起動しない場合があります。  
まずはアプリの一覧から「Akamai Zero Trust Client」を起動してください。



上記エラーが出た場合お手数ですが、以下の手順を実施頂くことで解消が見込めます。  
もし本手順で解消しない場合は、サポートセンタまでお問い合わせ頂きますようお願い申し上げます。  
また、エンタイトルメントコードの再入力が必要となりますのでご注意ください。

1. **Microsoft Visual C++ 2015 – 2022 Redistributable (x86) – 14.30.30708**  
のアンインストール
2. Akamai Zero Trust Clientのアンインストール
3. [インストール方法](#)を参照し再度インストールを実施  
※証明書のインストールは不要となります。

## お問い合わせ先について

---

本サービスに関するお問い合わせやトラブルはサポートセンターまでご連絡ください。  
サポートセンターの連絡先については、下記メールや営業担当よりご確認ください。

開通時に届く開通案内メール

件名：【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