クラウド管理型製品

KOKOMO by APRESIA

アクセスポイント

×

MFA認証サービス

Soliton OneGate

# 認証連携設定例

## ～ Windows 11でのEAP-TLS認証 ～

APRESIA SYSTEMS

技術協力：株式会社ソリトンシステムズ

# はじめに

本書では、ソリトンシステムズ社の認証サービスSoliton OneGate（以下、OneGate）およびエッジアプライアンスNetAttest EPS-edge（以下、EPS-edge）において、KOKOMOの無線アクセスポイントとのWindows 11でのEAP-TLS認証について、設定例を示したものです。

設定例は、管理者アカウントでログインし、事前に設定可能な状態に準備が完了していることを前提として記述します。

# 目次

KOKOMO by APRESIA アクセスポイント × Soliton OneGate

# 1. OneGate / EPS-edgeの設定

# 1. OneGate / EPS-edgeの設定

本項では、OneGate / EPS-edgeの設定方法について説明します。

以下の順番でセットアップを行います。

1. EPS-edgeの設置とOneGate との接続
2. OneGateへのユーザーの登録
3. 同期の実行
4. クライアント証明書の発行

# 1-1 EPS-edgeの設置とOneGate との接続

インターネット接続が可能かつ、DHCPサーバーからIPアドレスが取得できる環境にEPS-edgeを接続して設定作業を行う場合には、事前のEPS-edge通信設定を省略し、EPS-edgeがOneGateと接続した後にOneGate管理画面側から設定を行うことが可能です。

本資料ではEPS-edgeシステム管理ページで通信設定を行う方法を説明します。

# 1-1-1 EPS-edge本体の設定

EPS-edge本体の「LAN4ポート」とPCの「LANポート」を接続します。

EPS-edgeの管理画面は、「LAN4ポート」からのみアクセス可能です。

LAN4のIPアドレスはデフォルトで「192.128.99.1/30」に設定されています。

管理用PCには、LAN4にアクセス可能なIPアドレス「192.128.99.2/30」を設定する必要があります。

# 1-1-1 EPS-edge本体の設定

接続した管理用PCからWebブラウザを起動し、EPS-edgeのシステム管理ページにアクセスします。

http://LAN4のIPアドレス:8888/

ユーザーID・パスワードの両方に「root」を入力しシステム管理ページにログインしてください。


| 項目 | 値 |
|---|---|
| ユーザーID | root |
| パスワード | root |

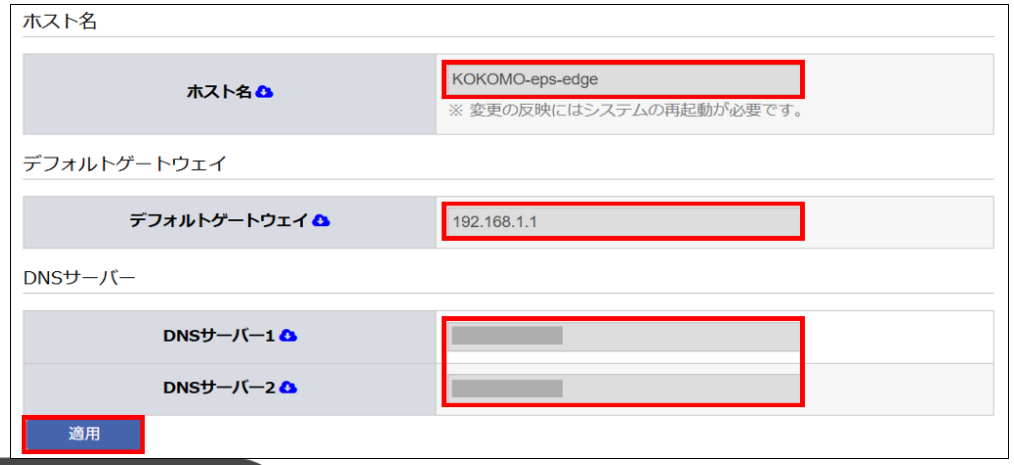
※OneGateとEPS-edgeの通信には「LAN1ポート」を使用します。

この時点ではまだ「LAN1ポート」と基幹ネットワークを接続しないでください。

# 1-1-1 EPS-edge本体の設定

EPS-edgeのネットワークインターフェイスの設定を行うため、メニューパネルの設定 ＞ ネットワークから、LAN1ポートにネットワークへ接続可能なIPアドレスを設定してください。


EPS-edgeのホスト名、デフォルトゲートウェイ、DNSサーバーを設定します。
設定が完了したら「適用」をクリックしてください。



# 1-1-2 EPS-edgeとOneGateの結び付け

OneGateのサービスポータルからEPS-edgeと連携するための設定を行います。

Webブラウザを起動し、以下へアクセスしてください。

https://<テナントコード>.ids.soliton-ods.jp/icon/seap/login

ログイン画面が表示されたらログイン名とパスワードを入力し、サービスポータルにログインしてください。

OneGateサービスポータルのアプライアンス管理 ＞ アプライアンス一覧　の「登録」をクリックしてください。

# 1-1-2 EPS-edgeとOneGateの結び付け

新しいアプライアンスとしてEPS-edgeを追加します。

「登録コード」にEPS-edge本体正面のシールに記載されている REG: の右のコードを入力し、

「自動承認」にチェックを入れてください。

設定が完了したら「追加」をクリックしてください。

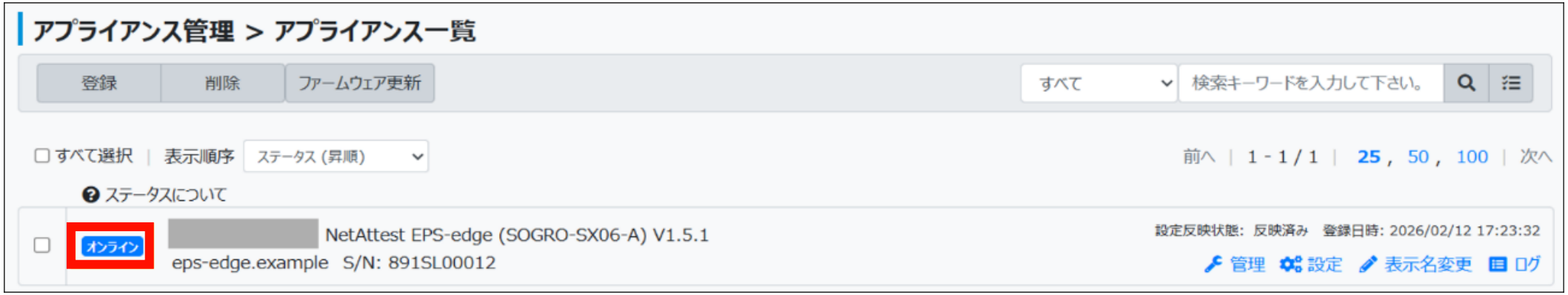

| 項目 | 値 |
|---|---|
| 登録コード | EPS-edge本体正面のシールに記載されている REG:の右のコード |
| 自動承認 | on |

# 1-1-2 EPS-edgeとOneGateの結び付け

EPS-edgeの「LAN1ポート」をOneGateへ接続できるネットワークに接続します。

アプライアンス管理 ＞ アプライアンス一覧　を表示します。

対象のEPS-edgeのステータスが「接続待ち」から「オンライン」に変わったことを確認してください。

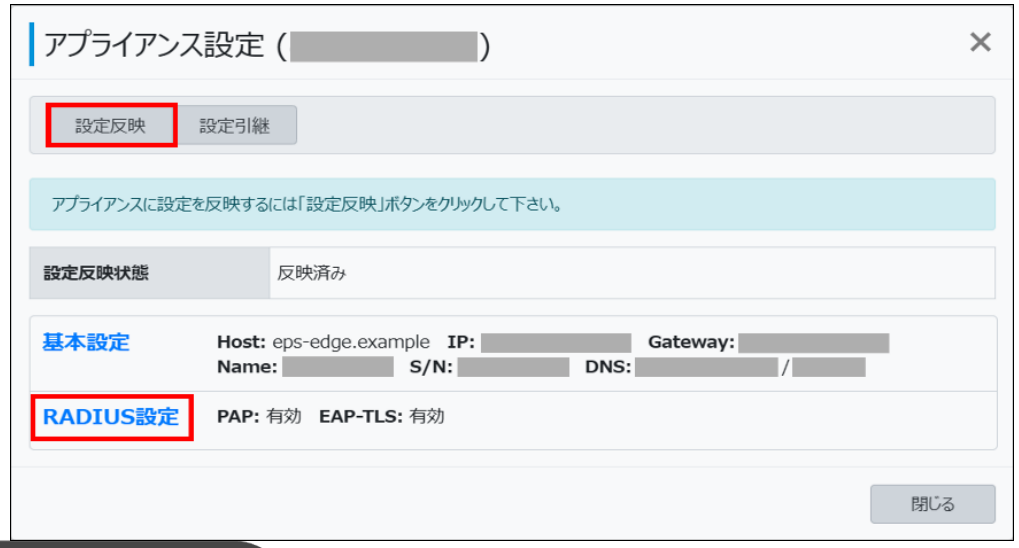


# 1-1-3 RADIUS設定

アプライアンス管理 ＞ アプライアンス一覧　から「設定」をクリックしてください。


表示される「RADIUS設定」をクリックすると、認証方式や認証共通設定が行えます。

設定を変更した場合は「設定反映」をクリックしてEPS-edge本体に反映してください。



# 1-1-3 RADIUS設定

EAP-TLSの「クライアント証明書による認証を許可する」にチェックをし、
RADIUSクライアントシークレットに任意の値を入力してください。
設定が完了したら「保存」をクリックしてください。


| 項目 | 値 |
|---|---|
| クライアント証明書による認証を許可する | on |
| RADIUSクライアントシークレット | 任意の値 |

# 1-2 OneGateへのユーザーの登録

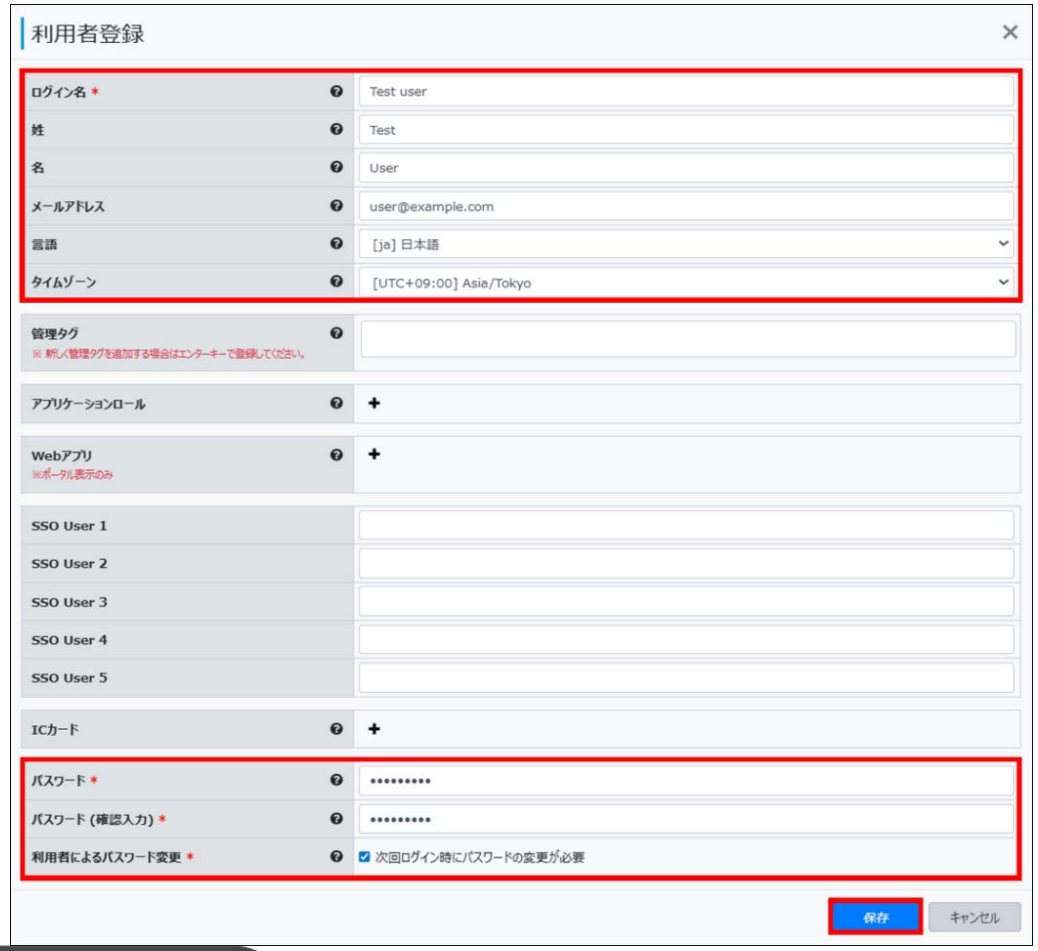
RADIUS認証を行うユーザーをOneGateに登録します。
OneGateにユーザーを登録する方法として、「Active Directoryのユーザーを連携する方法」と「OneGateに直接ユーザーを登録する方法」があります。
本資料では、「OneGateに直接ユーザーを登録する方法」を説明します。

ユーザー登録するには　利用者管理 ＞ 利用者一覧　から「登録」をクリックしてください。

# 1-2 OneGateへのユーザーの登録

利用者登録画面で利用者の情報とパスワードを設定し、OneGateユーザーを登録します。

利用者の情報を入力したら「保存」をクリックしてください。



# 1-3 同期の実行

OneGateにユーザーを登録後、同期処理を実行してOneGateのログインユーザーとして有効化します。

同期を実行するには　同期スケジュール設定 ＞ 同期スケジュール設定　から差分同期スケジュールの「即時実行」をクリックしてください。

確認画面が表示されたら「はい」をクリックしてください。

# 1-3 同期の実行

同期処理の実行結果を確認します。ログの確認をするには　ログ管理 ＞ 同期実行ログ　を選択します。

一覧で表示されているログで、一番上に表示されているものが直前に実行した実行結果です。

下の例のように「完了」と表示されていれば正常に処理が完了しています。


利用者管理＞利用者一覧から登録した利用者を確認すると「同期済み」と表示されています。

# 1-4 クライアント証明書の発行

EAP-TLS認証を行うためのクライアント証明書を発行します。

招待コードを使って証明書を発行する際に適用するプロファイル情報を「招待設定」で設定します。
特に設定が不要な場合は「招待設定」を作成する必要はありません。
証明書管理＞招待設定　から登録をクリックします。

# 1-4 クライアント証明書の発行

赤枠内の各項目について設定を行います。

設定が完了したら「保存」をクリックしてください。

# 1-4 クライアント証明書の発行

証明書管理 ＞ 招待コード管理　から「発行」をクリックしてください。


OneGateに登録されているユーザーの一覧が表示されます。招待コードを発行するユーザーのチェックボックスにチェックし、作成した招待設定を選択して「発行」をクリックしてください。

# 1-4 クライアント証明書の発行

招待コード管理画面で対象のユーザーに招待コードが発行されていることを確認してください。

招待コードの有効期限は10日間です。


招待コードの発行まで完了しました。

ユーザーには、メールでクライアント証明書の取得のための招待URLが届きます。

ユーザーは、そのURLをクリックすることでクライアント証明書の取得が可能です。

KOKOMO by APRESIA アクセスポイント × Soliton OneGate

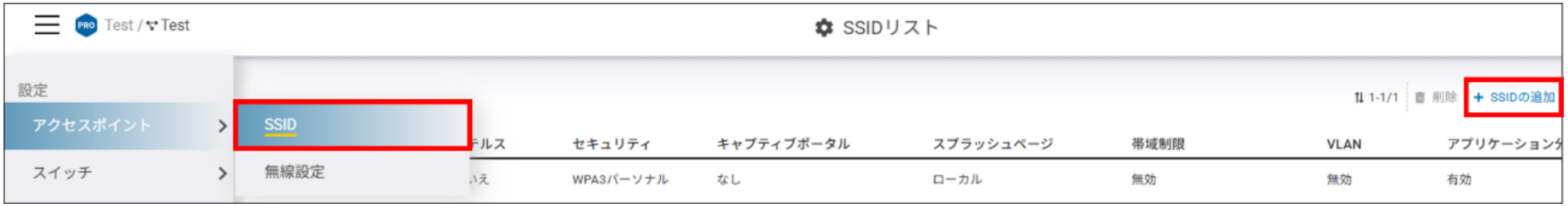
# 2. KOKOMO Cloudの設定

# 2-1 RADIUS認証設定

KOKOMO Cloudにログインし、 設定＞アクセスポイント＞SSID　から「SSIDの追加」をクリックしてください。

- KOKOMO CloudログインURL

  https://lan.kokomocloud.com/



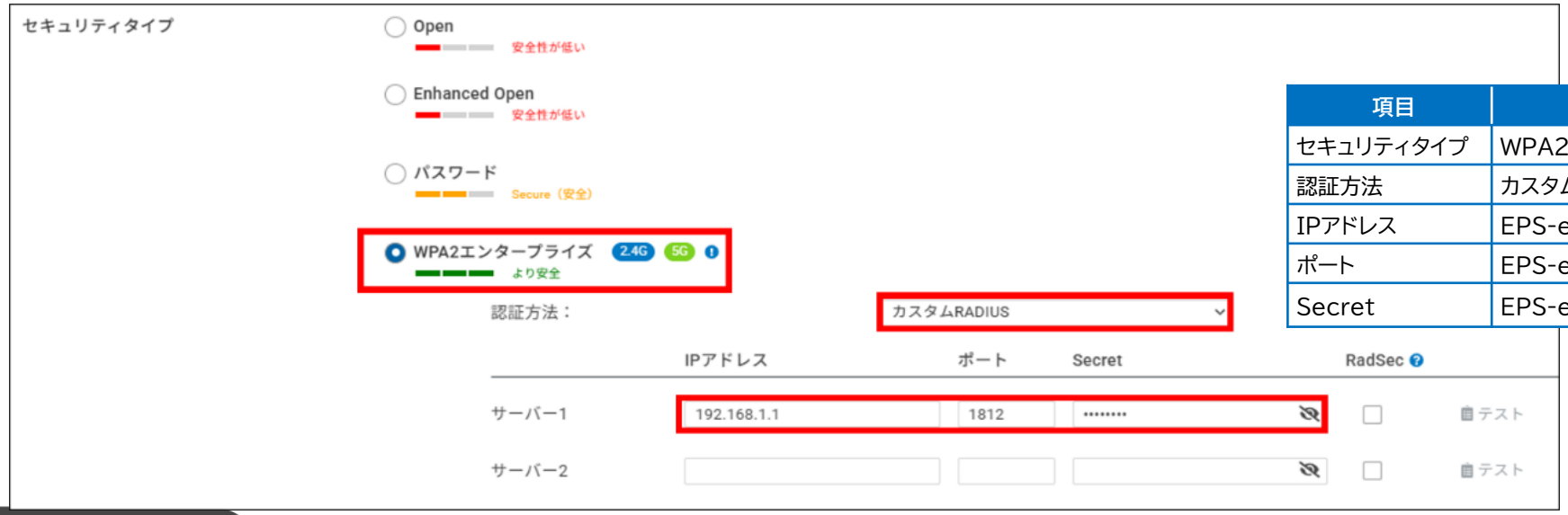
# 2-1 RADIUS認証設定

基本設定のセキュリティタイプから「WPA2エンタープライズ」を選択してください。

認証方法に「カスタムRADIUS」を選択し、EPS-edgeに設定したIPアドレス、ポート番号、Secretを入力します。

Secretには「 1-1-3 RADIUS設定 」でRADIUSクライアントシークレットに入力した値を設定してください。

設定が完了したら「適用する」をクリックしてください。




| 項目 | 値 |
|---|---|
| セキュリティタイプ | WPA2エンタープライズ |
| 認証方法 | カスタムRADIUS |
| IPアドレス | EPS-edgeに設定したIPアドレス |
| ポート | EPS-edgeに設定したポート番号 |
| Secret | EPS-edgeに設定したRADIUSクライアントシークレット |

# 2-1 RADIUS認証設定

アクセスポイントに設定が反映されたら「テスト」をクリックし、EPS-edgeとアクセスポイントで
RADIUS認証ができているか確認してください。


テストを開始するために、OneGateの利用者登録で登録した「ユーザー名（ログイン名）」と
「パスワード」を入力してください。
入力が完了したら「テストを開始します。」をクリックしてください。

# 2-1 RADIUS認証設定

RADIUSテストの結果は以下のように表示されます。


認証に失敗・実行できなかったアクセスポイントは、
テスト結果の下にデバイスの情報が表示されます。

今回の結果ではアクセスポイントが2台登録されており、
1台は認証に成功していますが、もう1台は認証を実行できなかったということが分かります。

| 項目 | 値 |
|---|---|
| アクセスポイントの合計数 | ネットワークに登録されているアクセスポイント台数 |
| アクセスポイントのファームウェアがv1.x75未満 | ファームウェアv1.x75未満のアクセスポイント台数 |
| アクセスポイントを通過 | 認証に成功したアクセスポイント台数 |
| アクセスポイントが失敗しました | 認証に失敗したアクセスポイント台数 |
| アクセスポイントをテストできません | 認証を実行できなかったアクセスポイント台数 |

KOKOMO by APRESIA アクセスポイント × Soliton OneGate

# 3. Windows 11でのEAP-TLS認証

# 3-1 Soliton KeyManagerのインストール

WebサイトからSoliton KeyManagerをダウンロードし、任意の場所に保存・展開してください。

- Windows版Soliton KeyManagerダウンロード先URL
  https://www.soliton.co.jp/download/ssx_download.html


生成されたフォルダー内の Soliton KeyManager インストーラーをダブルクリックして実行し、指示に従ってインストールを行ってください。

# 3-2 クライアント証明書のインストール

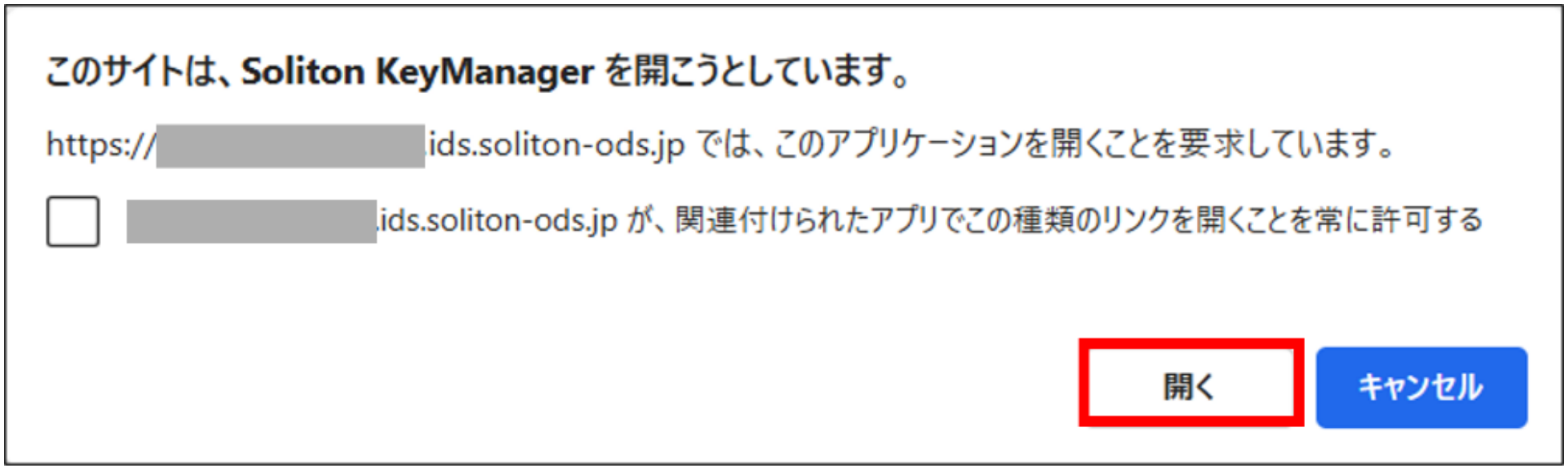
ユーザーに届いているメールからSoliton KeyManager用URLをクリック、

または添付のQRコードを読み取ってクライアント証明書をインストールしてください。

# 3-2 クライアント証明書のインストール

Webブラウザが起動し、Soliton KeyManager起動許可の確認画面が表示されます。

「開く」をクリックしてSoliton KeyManagerを起動してください。



# 3-2 クライアント証明書のインストール

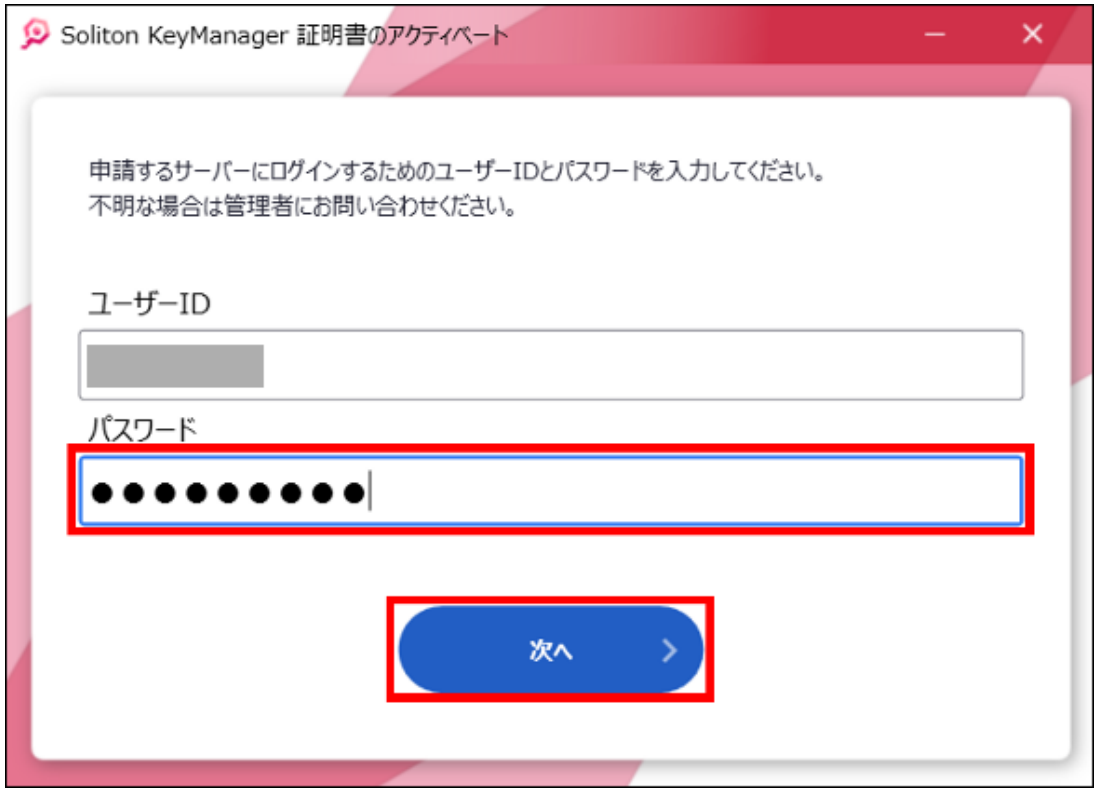
クライアント証明書の用途に合わせ、証明書格納先を「ユーザー」か「コンピューター」から選択してください。

招待設定で証明書の格納先を指定している場合はこの手順はスキップされます。

本資料ではユーザーを選択する場合を例に説明します。

# 3-2 クライアント証明書のインストール

OneGateの利用者登録時に設定したパスワードを入力し「次へ」をクリックすると、証明書のインストールが始まります。

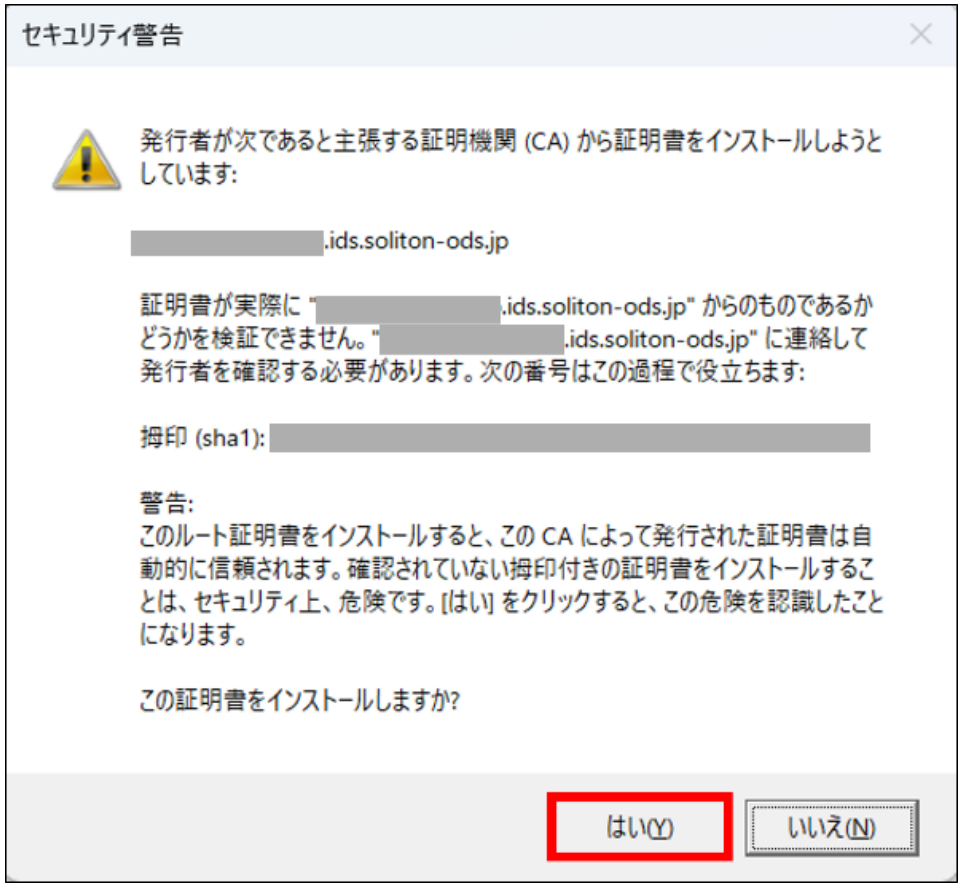



| 項目 | 値 |
|---|---|
| ユーザーID | OneGateの利用者登録時に設定したユーザーID |
| パスワード | OneGateの利用者登録時に設定したパスワード |

# 3-2 クライアント証明書のインストール

PCにCA証明書がインストールされていない場合、CA証明書インストール画面が表示されます。

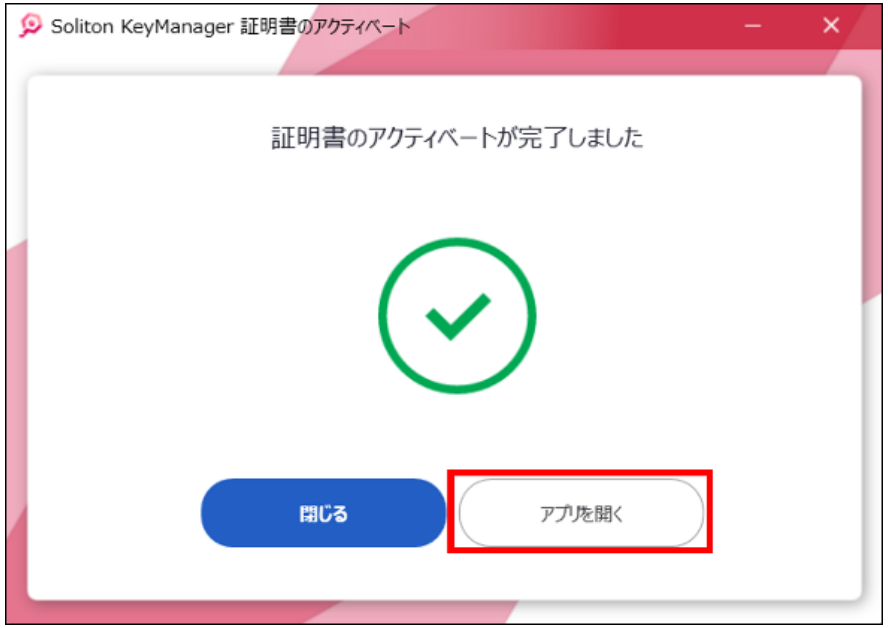
「はい」をクリックしてください。



# 3-2 クライアント証明書のインストール

証明書のインストールが完了すると、「証明書のアクティベートが完了しました」のメッセージが表示されます。

「アプリを開く」をクリックし、Soliton KeyManagerアプリ内の証明書一覧からインストールされた証明書を確認してください。




# 3-3 サプリカント設定

Windows標準サプリカントでTLSの設定を行います。

コントロールパネルを開き、ネットワークとインターネット＞ネットワークと共有センター をクリックします。

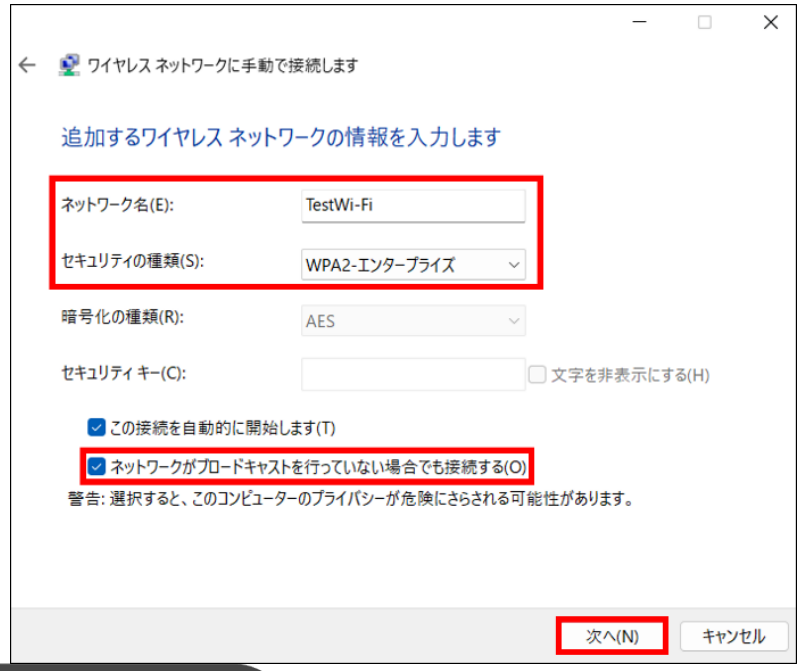
# 3-3 サプリカント設定

使用するSSIDの名前を入力し、セキュリティの種類を選択します。

セキュリティの種類は「WPA2-エンタープライズ」を選択してください。

ご利用の環境でSSIDをブロードキャストしていない場合は、「ネットワークがブロードキャストを行っていない場合でも接続する」を有効にします。

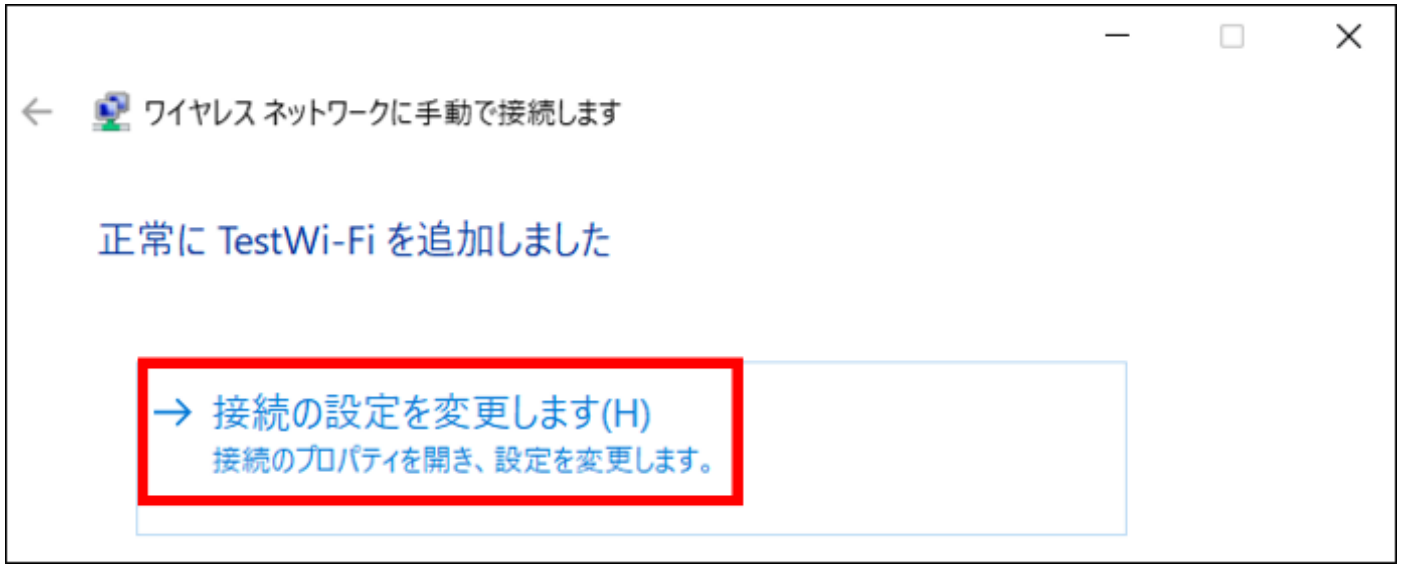
設定が完了したら「次へ」をクリックしてください。




| 項目 | 値 |
|---|---|
| ネットワーク名 | 使用するSSIDの名前 |
| セキュリティの種類 | WPA2-エンタープライズ |
| ネットワークがブロードキャストを行っていない場合でも接続する | on |

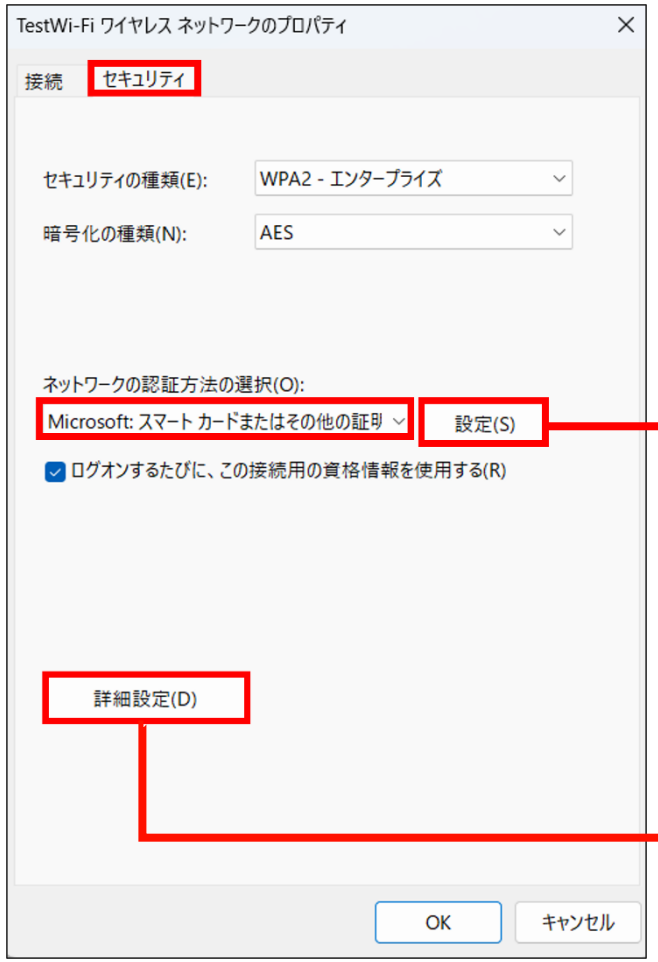
# 3-3 サプリカント設定

SSIDが追加出来たら「接続の設定を変更します」をクリックし、ネットワークのプロパティを設定してください。



# 3-3 サプリカント設定

「ワイヤレスネットワークのプロパティ」のセキュリティから以下の設定を行います。




| 項目 | 値 |
|---|---|
| セキュリティの種類 | WPA2 – エンタープライズ |
| 暗号化の種類 | AES |
| ネットワーク認証方法の選択 | Microsoft:スマートカードまたはその他の証明書 |


| 項目 | 値 |
|---|---|
| このコンピューターの証明書を使う | on |
| 単純な証明書の選択を使う | on |
| 証明書を検証してサーバーのIDを検証する | on |
| 信頼されたルート証明機関 | ＜テナントコード＞.ids.soliton-ods.jp |


| 項目 | 値 |
|---|---|
| 認証モードを指定する | ユーザー認証 |