

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 ～



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

<b>1. OneGate / EPS-edgeの設定</b>	<b>4</b>
1-1 EPS-edgeの設置とOneGate との接続	6
1-1-1 EPS-edge本体の設定	7
1-1-2 EPS-edgeとOneGateの結び付け	9
1-1-3 RADIUS設定	13
1-2 OneGateへのユーザーの登録	15
1-3 同期の実行	18
1-4 クライアント証明書の発行	19
<b>2. KOKOMO Cloudの設定</b>	<b>23</b>
2-1 RADIUS認証設定	24
<b>3. Windows 11でのEAP-TLS認証</b>	<b>28</b>
3-1 Soliton KeyManagerのインストール	29
3-2 クライアント証明書のインストール	30
3-3 サプリカント設定	36

**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。

LAN1

IPv4アドレスの使用  使用する(固定) ▼

IPアドレス  サブネットマスク

詳細設定を表示 ▼

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。

ホスト名

ホスト名   
※ 変更の反映にはシステムの再起動が必要です。

デフォルトゲートウェイ

デフォルトゲートウェイ

DNSサーバー

DNSサーバー-1

DNSサーバー-2

適用

## 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。

### 新しいアプライアンスの追加

登録コード (REG) を使用してアプライアンスを追加

登録コード *	<input type="text" value="例 : aB0123456789"/>
自動承認	<input type="checkbox"/> 管理者による承認を省略する

追加

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。

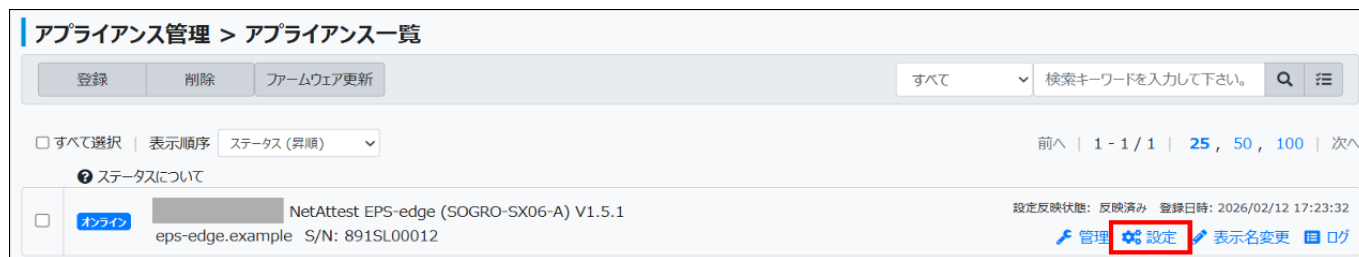
アプライアンス管理 > アプライアンス一覧 を表示します。

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。

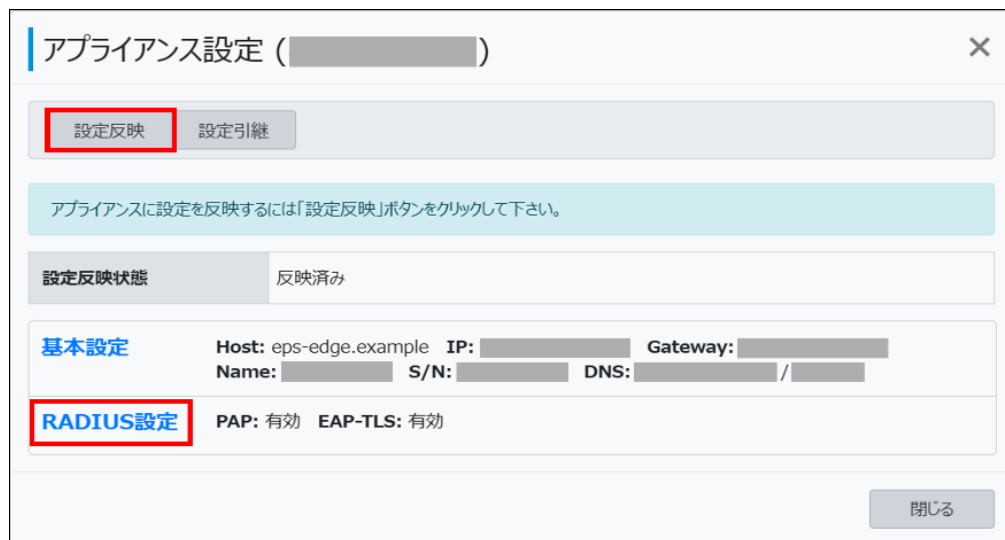
The screenshot shows the 'アプライアンス管理 > アプライアンス一覧' (Appliance Management > Appliance List) page. At the top, there are buttons for '登録' (Register), '削除' (Delete), and 'ファームウェア更新' (Firmware Update). A search bar contains 'すべて' (All) and '検索キーワードを入力して下さい。' (Enter search keyword). Below the search bar, there are options for 'すべてを選択' (Select all), '表示順序' (Display order) set to 'ステータス (昇順)' (Status (Ascending)), and pagination controls '前へ | 1 - 1 / 1 | 25, 50, 100 | 次へ'. A help icon and 'ステータスについて' (About status) link are also present. The main table lists one appliance with the status 'オンライン' (Online) highlighted in a red box. The appliance details are: 'NetAttest EPS-edge (SOGRO-SX06-A) V1.5.1', 'eps-edge.example S/N: 891SL00012', and '設定反映状態: 反映済み 登録日時: 2026/02/12 17:23:32'. Action buttons for '管理' (Manage), '設定' (Settings), '表示名変更' (Change display name), and 'ログ' (Log) are visible at the bottom right of the table row.

## 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。

### RADIUS設定 ( )

認証方式

	変更前	変更後
PAP *	<input type="checkbox"/> ユーザー名とパスワードによる認証を許可する	<input checked="" type="checkbox"/> ユーザー名とパスワードによる認証を許可する
EAP-TLS *	<input checked="" type="checkbox"/> クライアント証明書による認証を許可する	<input checked="" type="checkbox"/> クライアント証明書による認証を許可する

認証共通設定

	変更前	変更後
RADIUSクライアントシークレット *		
EAP-TTLS *	<input type="checkbox"/> EAP-TTLSを有効にする	<input type="checkbox"/> EAP-TTLSを有効にする
OCSP検証 (EAP-TLS時) *	<input checked="" type="checkbox"/> EAP-TLS認証時のOCSP検証を有効にする	<input checked="" type="checkbox"/> EAP-TLS認証時のOCSP検証を有効にする

詳細設定 >

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。



利用者管理 ▼ クラウド設定 ▼ AD設定 ▼ 証明書管理 ▼ ICカード管理 ▼ アプライアンス管理 ▼ 同期スケジュール設定 ▼ システム設定 ▼ ログ管理 ▼

**利用者一覧**

利用者管理 > 利用者一覧

\* AD連携によって作成されたユーザーの情報を変更するには、[AD連携設定](#) 画面から連携元設定の属性設定を選択し、変更したい属性の「変更を有効にする」チェックボックスを ON にしてください。

登録 強制同期 削除 インポート ▼ エクスポート ▼

## 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。

利用者登録

ログイン名 *	Test user
姓	Test
名	User
メールアドレス	user@example.com
言語	[ja] 日本語
タイムゾーン	[UTC+09:00] Asia/Tokyo

管理タグ  
※ 新しく管理タグを追加する場合はエンターキーで登録してください。

アプリケーションロール +

Webアプリ +  
※ ボール表示のみ

SSO User 1  
SSO User 2  
SSO User 3  
SSO User 4  
SSO User 5

ICカード +

パスワード *	*****
パスワード (確認入力) *	*****
利用者によるパスワード変更 *	<input checked="" type="checkbox"/> 次回ログイン時にパスワードの変更が必要

保存 キャンセル

## 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。

同期スケジュール設定

有効	無効
<input type="checkbox"/>	<input checked="" type="checkbox"/>

同期スケジュール	同期スケジュール	即時実行
<input type="checkbox"/> <b>無効</b> 差分同期スケジュール 日指定 05:00/1日毎 通知: 通知しない	変更が必要なユーザー情報だけ同期します。	<input checked="" type="button" value="即時実行"/>
<input type="checkbox"/> <b>無効</b> 完全同期スケジュール 1回のみ 2000/01/01 00:00 通知: 通知しない	全てのユーザー情報を同期します。	<input type="button" value="即時実行"/>

## 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。

The screenshot shows the 'ログ管理' (Log Management) menu with '同期実行ログ' (Sync Execution Log) selected. The main content area displays a log entry for '差分同期スケジュール[225]' with a green progress bar and a '完了' (Completed) status. The '完了' status is highlighted with a red box.

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。

The screenshot shows a user entry for 'Test User' with the email address 'user@example.com'. The status '同期: 同期済み' (Sync: Synced) is highlighted with a red box.

## 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。

### 招待設定登録

基本設定

表示名 *	?	Test
発行先 *	?	Windows版 Soliton KeyManager (Windows SKM) ▼
証明書の格納先 *	?	ユーザー ▼
パスワードレス *	?	<input checked="" type="checkbox"/> 有効にする
ドメイン名	?	例 : example.co.jp

詳細設定 ?

**通知設定**

**証明書設定**      国名(C): 未設定   都道府県名(S): 未設定   市区町村名(L): 未設定  
組織名(O): 未設定   部署名(OU): 未設定

**CA証明書配付設定**      配付するCA証明書: 1件

**Wi-Fi設定**

**VPN設定**

**保存**      キャンセル

## 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。



The screenshot shows the 'Invitation Code Management' page. At the top, there are buttons for '発行' (Issue), '無効化' (Deactivate), '再通知' (Resend), and 'エクスポート' (Export). A filter for '期限4日以内' (Within 4 days) is set to 'すべて' (All). A search bar contains the text '検索キーワードを入力して下さい'. Below the filters, there are options for 'すべて選択' (Select all) and '表示順序' (Sort order) set to '発行日時(降順)' (Issue date (descending)). A table lists the invitation codes. The first row shows a user named 'Test User' with email 'user@example.com'. The invitation code is 'GgeYro', which is highlighted with a red box. The invitation status is '未使用' (Unused). The issue date is '2026/02/20 09:23:07' and the expiration date is '2026/03/02 09:23:07'. The invitation settings are 'default'.

<input type="checkbox"/>	未使用	Test User Test User user@example.com	招待コード: GgeYro 招待設定: default	発行者: [REDACTED]	発行日時: 2026/02/20 09:23:07 有効期限: 2026/03/02 09:23:07
--------------------------	-----	---	--------------------------------	-----------------	--

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/>



The screenshot shows the 'SSIDリスト' (SSID List) page in the KOKOMO Cloud management interface. The left sidebar shows the navigation menu with '設定' (Settings) expanded to 'アクセスポイント' (Access Point) > 'SSID'. The main content area displays a table of SSID configurations. The '+ SSIDの追加' button is highlighted with a red box.

SSID	プロファイル	セキュリティ	キャプティブポータル	スプラッシュページ	帯域制限	VLAN	アプリケーション
	なし	WPA3/パーソナル	なし	ローカル	無効	無効	有効

## 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

	IPアドレス	ポート	Secret	RadSec	
サーバー-1	192.168.1.1	1812	.....	<input type="checkbox"/>	自テスト
サーバー-2				<input type="checkbox"/>	自テスト

## 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。

認証方法:	カスタムRADIUS			
	IPアドレス	ポート	Secret	RadSec
サーバー1	<input type="text" value="192.168.1.150"/>	<input type="text" value="1812"/>	<input type="text" value="....."/>	<input type="checkbox"/>
サーバー2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

サーバー1の「自テスト」ボタンが赤枠で強調されています。

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。

テスト

RADIUSへの接続をテストします: 192.168.1.150 : 1812

ユーザー名

パスワード

× キャンセル

## 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。

テスト

RADIUSへの接続テストが完了しました : 192.168.1.150 : 1812

アクセスポイントの合計数: 2  
アクセスポイントのファームウェアがv1.x.75未満: 0  
アクセスポイントを通過: 1  
アクセスポイントが失敗しました: 0  
アクセスポイントをテストできません。: 1

0個のアクセスポイントがRADIUSサーバに接続できず、RadSec証明書がアップロードされていません。

名前	MACアドレス	機種	アクション
利用可能なデータはありません。			

1台のアクセスポイントはテストを実行できません。

名前	MACアドレス	機種	アクション
AP-8F-W220-PJ	FC:6D:D1:8F:2C:1C	KOKOMO-W220AX-IS	<a href="#">詳細情報</a>

× キャンセル

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.x.75未満	ファームウェアv1.x.75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**

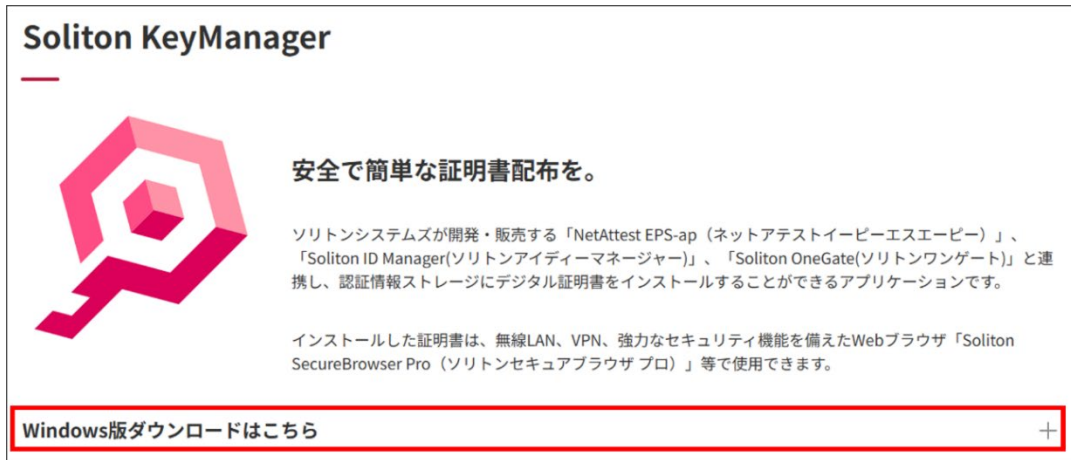
### 3. Windows 11でのEAP-TLS認証

## 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](https://www.soliton.co.jp/download/ssx_download.html)



**Soliton KeyManager**



安全で簡単な証明書配布を。

ソリトンシステムズが開発・販売する「NetAttest EPS-ap（ネットアテストイービーエスエーピー）」、「Soliton ID Manager(ソリトンアイディーマネージャー)」、「Soliton OneGate(ソリトンワンゲート)」と連携し、認証情報ストレージにデジタル証明書をインストールすることができるアプリケーションです。

インストールした証明書は、無線LAN、VPN、強力なセキュリティ機能を備えたWebブラウザ「Soliton SecureBrowser Pro（ソリトンセキュアブラウザ プロ）」等で使用できます。

[Windows版ダウンロードはこちら](#) +

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。

このサイトは、**Soliton KeyManager** を開こうとしています。

https://[redacted]ids.soliton-ods.jp では、このアプリケーションを開くことを要求しています。

[redacted]ids.soliton-ods.jp が、関連付けられたアプリでこの種類のリンクを開くことを常に許可する

**開く** **キャンセル**

## 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。

Soliton KeyManager 証明書のアクティベート

申請するサーバーにログインするためのユーザーIDとパスワードを入力してください。  
不明な場合は管理者にお問い合わせください。

ユーザーID

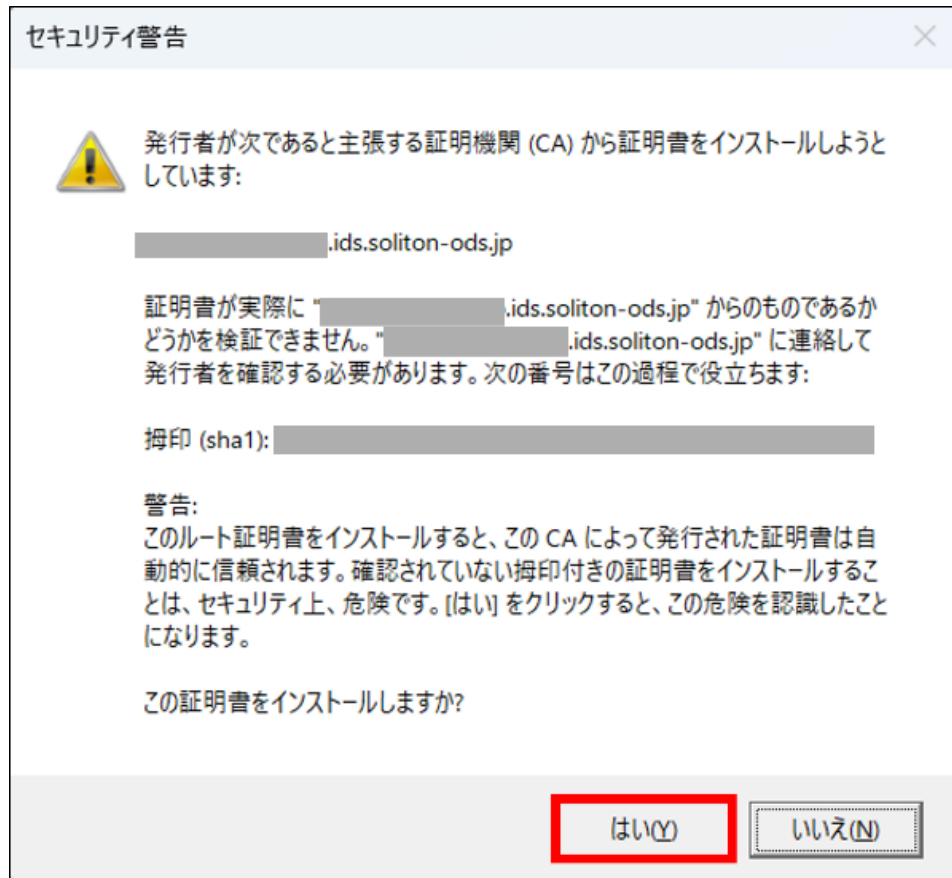
パスワード

次へ >

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

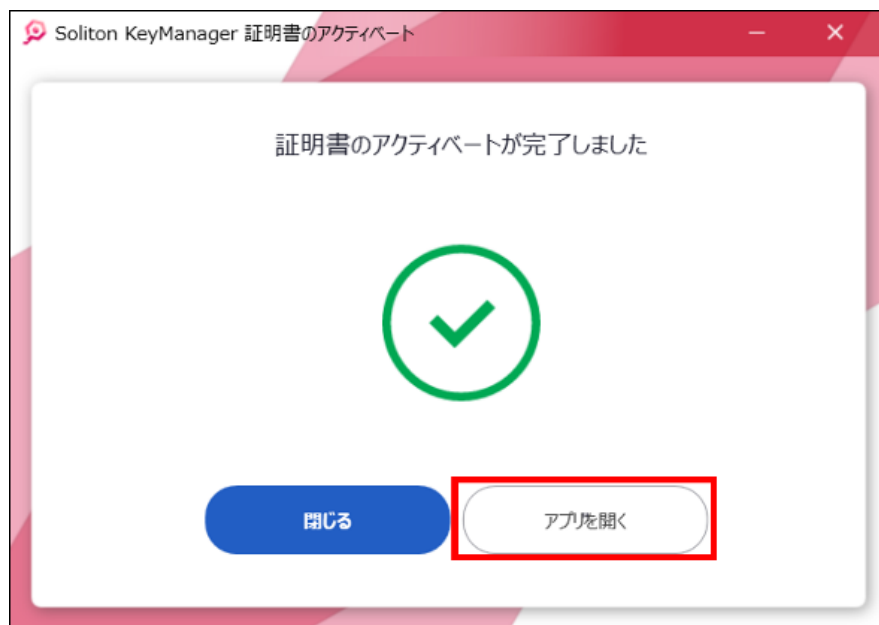
PCにCA証明書がインストールされていない場合、CA証明書インストール画面が表示されます。「はい」をクリックしてください。



## 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。

ワイヤレス ネットワークに手動で接続します

追加するワイヤレス ネットワークの情報を入力します

ネットワーク名(E): TestWi-Fi

セキュリティの種類(S): WPA2-エンタープライズ

暗号化の種類(R): AES

セキュリティキー(C):   文字を非表示にする(H)

この接続を自動的に開始します(T)

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(O)

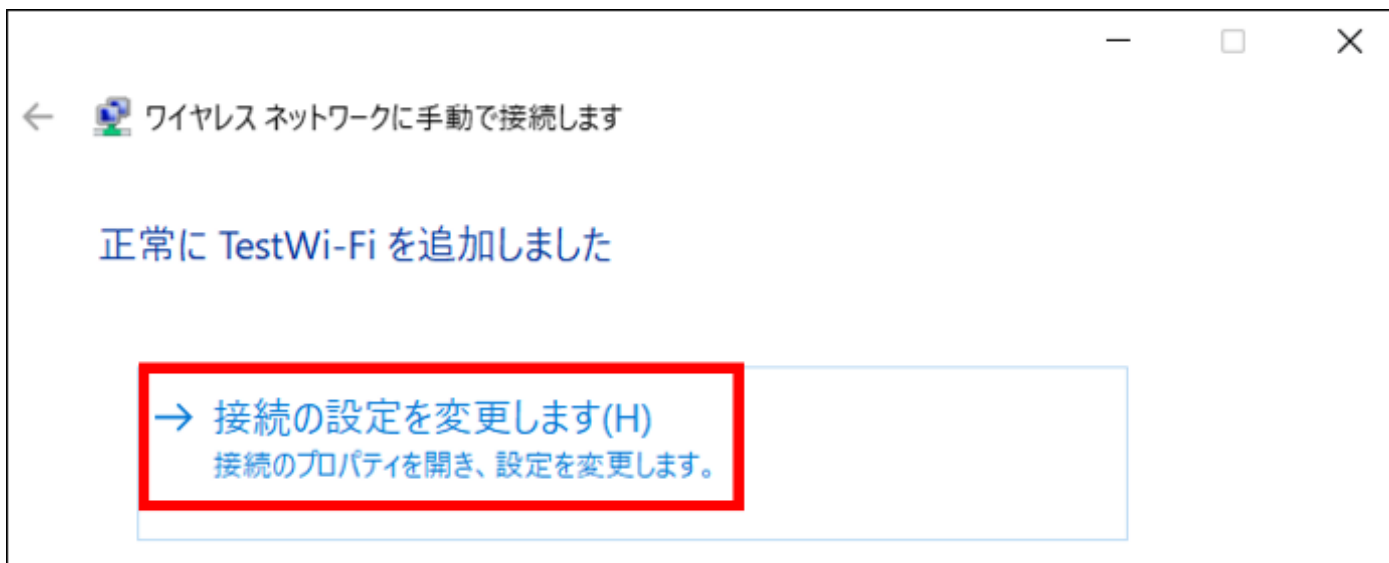
警告: 選択すると、このコンピュータのプライバシーが危険にさらされる可能性があります。

次へ(N) キャンセル

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