

リモートファーストへの転換に向けた第一歩

---

# PKIでSASEの導入効果を高める

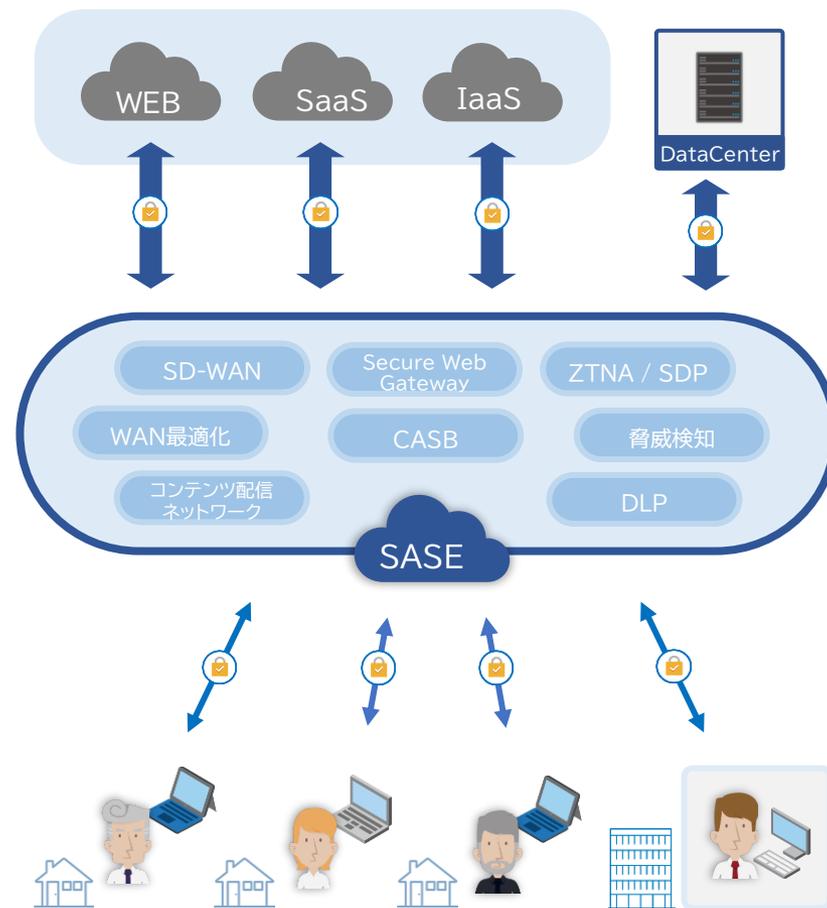


# 集約型ネットワークの限界、注目される SASE

昨年、テレワークの急拡大により、VPN回線やプロキシ負荷の逼迫による通信遅延など、集約型ネットワークに多くの課題が発生しました。そこで、リモート前提の働き方(=リモートファースト)へ転換するために、通信をLANに集約するのではなく、クラウドのSASE※に集約する対策に注目が集まっています。

目に見える物理的なオフィスからの接続を前提としないSASEにおいて、業務の入口となる「認証」は従来と同じ考え方で良いでしょうか。

インターネット空間では、成りすましリスクが一気に高まります。認証情報を窃取するサイバー攻撃も増加する中、集約型ネットワークでよく使われたAD認証連携は、もはや通用しません。また、社員が安全対策がとられていない私物デバイスを業務利用してしまうリスクなども考慮する必要がでてきます。



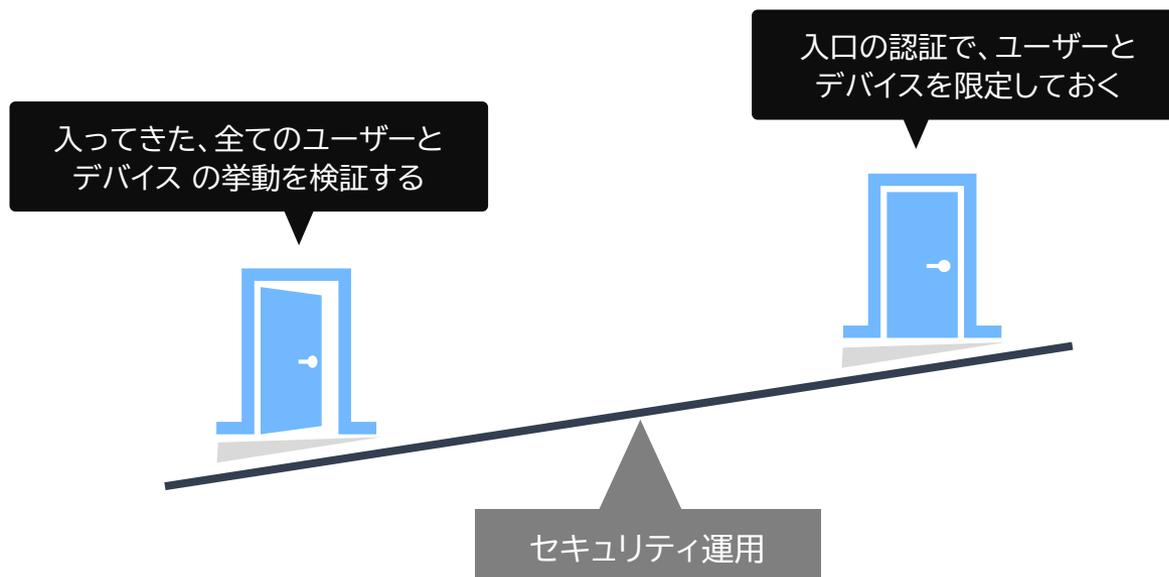
※ Secure Access Service Edgeの略。ネットワーク機能とセキュリティ機能をクラウド上で包括的に提供する考え方。ゼロトラストモデルを実現するための方法の一つ。



## リモートファースト転換へのファーストステップとは？

信頼せず、入ってくる全てのユーザーとデバイスの挙動を検証する「ゼロトラスト」の考え方は理想ですが、どこまで検証すればよいのかというゴールが作りにくく、疑わしいというアラートにどう対処していくか、検討することも膨大です。それよりも、入口の認証で、接続してくるユーザーとデバイスを限定し特定することができれば、守るべき端末が絞り込まれているので エンドポイント対策も徹底でき、**SASE側で考慮すべきリスク対策を減らす**ことが可能となります。

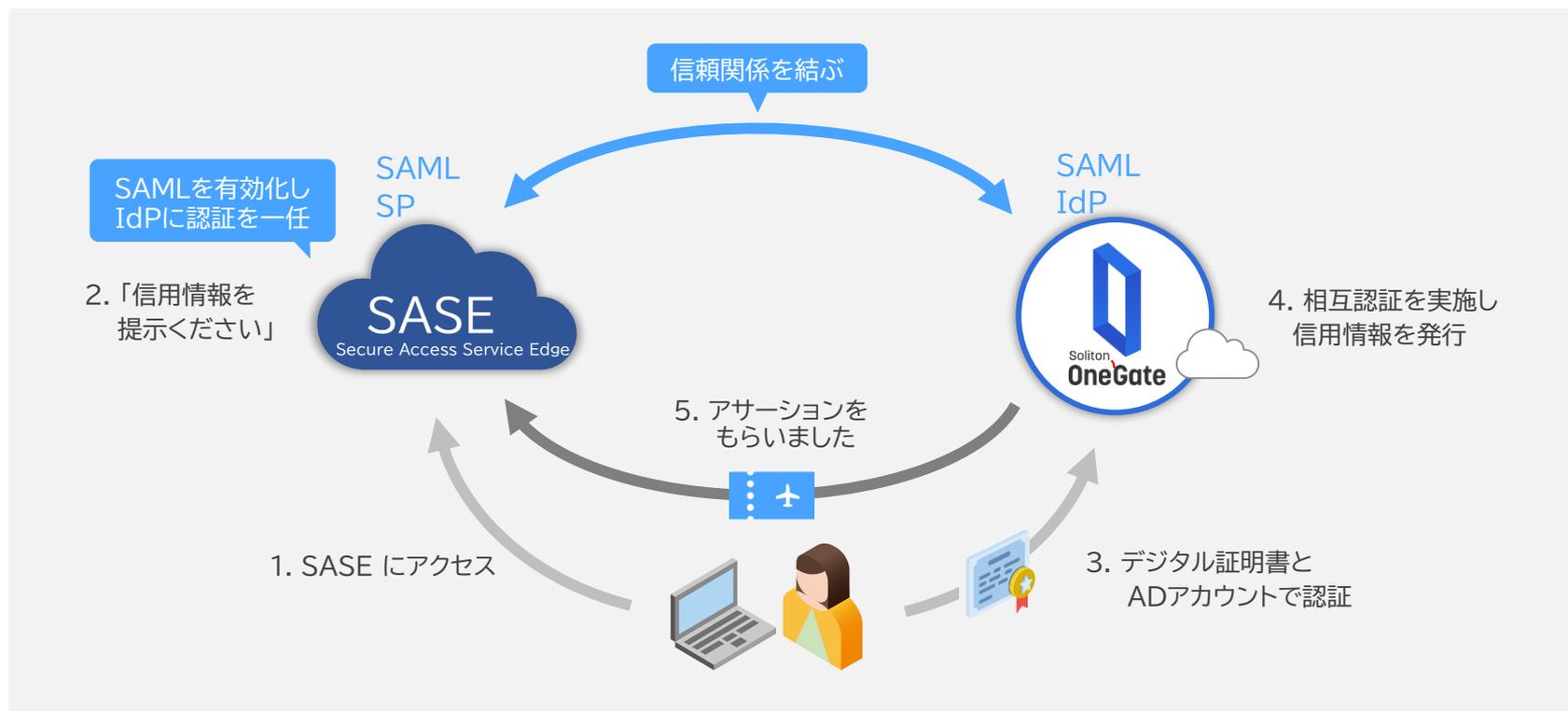
つまり、運用コストを抑えながら最大限の効果を出すために、**入口の認証を抑えておく**ことが、リモートファーストへの転換に向けた重要なファーストステップとなります。



# Wi-Fi だけじゃない、SASEにもPKI認証が適用できる

Wi-FiやSSL-VPNによるLANアクセスでは、外部認証サーバーを用いた、クライアント証明書によるPKI認証の適用がデファクトの認証強化手法となっており、多くの企業が採用しています。

SASEで多要素認証を行うには、インターネット標準の認証連携技術であるSAMLの利用が一般的となっていますが、PKIに対応したSAML IdP(IDプロバイダ)であれば、LAN 同様に SASE に対しても、手早く確実な認証強化が可能です。



# 急増するフィッシング詐欺のリスク

インターネットの世界で利用されている認証方式の一つに“SMSワンタイム”がありますが、昨今、この弱点を突いたフィッシング攻撃の被害が増加しており、NIST(米国立標準技術研究所)の認証に関するガイドラインでも非推奨となっています。

また、SMSワンタイムは利用者本人の確認手段であり日本国内でニーズの強い、利用端末の特定に対応できない点にも注意が必要です。

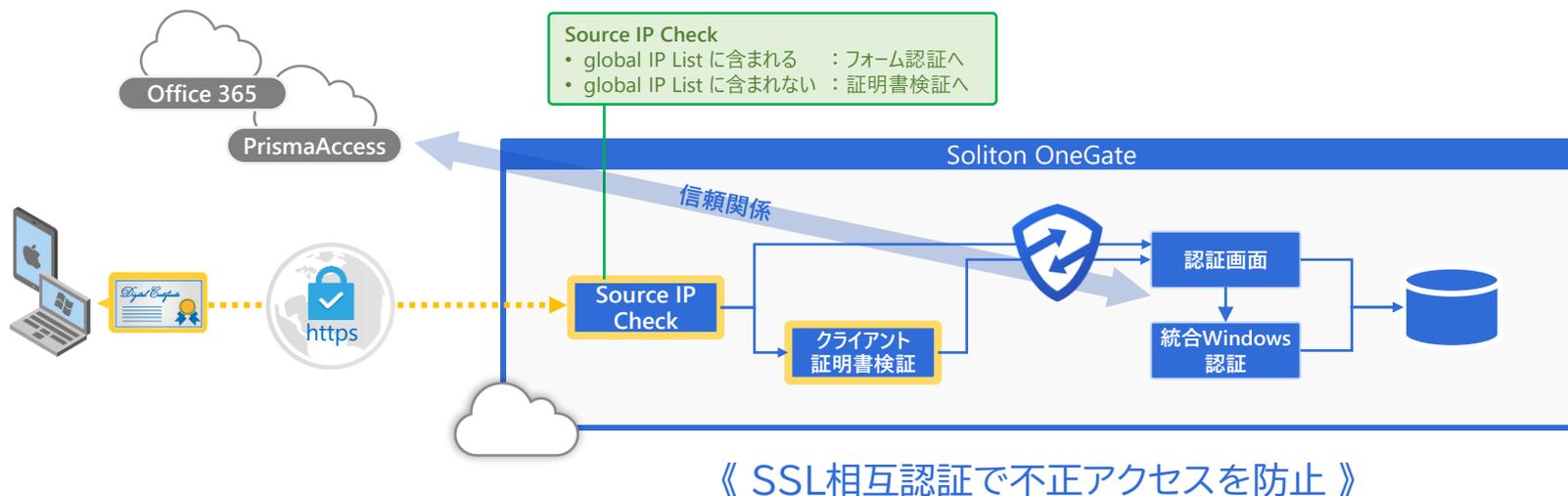
インターネット上のクラウドサービスは、IPアドレス制限をしていない限り、誰でも、何度も、ログイン画面にアクセスすることができます。アカウント確認を装って、偽サイトに誘導し、フィッシングでSMS認証も突破することは、社員数が多いほど、容易にできてしまいます。



# PKIの優位性、情報資産の保護に絶大効果

クライアント証明書を用いたPKI認証は、利用端末が特定できる上、フィッシングによる認証情報詐取を防止できるといったメリットがあります。また、攻撃対象領域の極小化という観点でも、他の認証方式と比べ高い優位性があります。

証明書を利用してクライアントとサーバーを相互認証するこの方式では、暗号化通信を確立する際にクライアント証明書をチェックすることになるため、正規の証明書がなければ通信が確立できません。つまり、他の多要素認証とは異なり**正規のクライアント証明書を持たない攻撃者はログイン画面にたどり着くこともできない**ため、パスワードリスト攻撃対策になるだけでなく、脆弱性攻撃の成立も困難なものとなります。



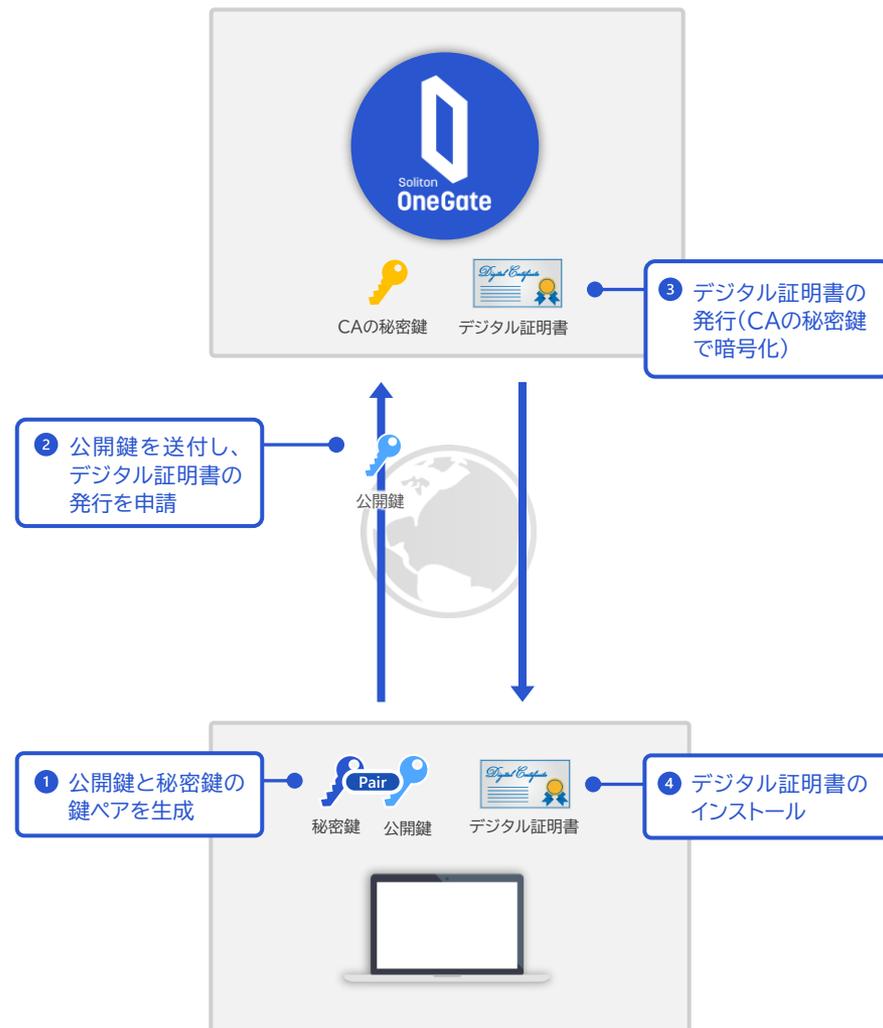
# クライアント証明書 of 安全な配布手法

クライアント証明書は、P12ファイルという秘密鍵付きのファイル形式で配布することも可能ですが、一度発行したP12ファイルは容易にコピーすることができてしまいます。そのため、利用者へファイル形式で証明書を配布することは推奨されません。

クライアント証明書の配布は

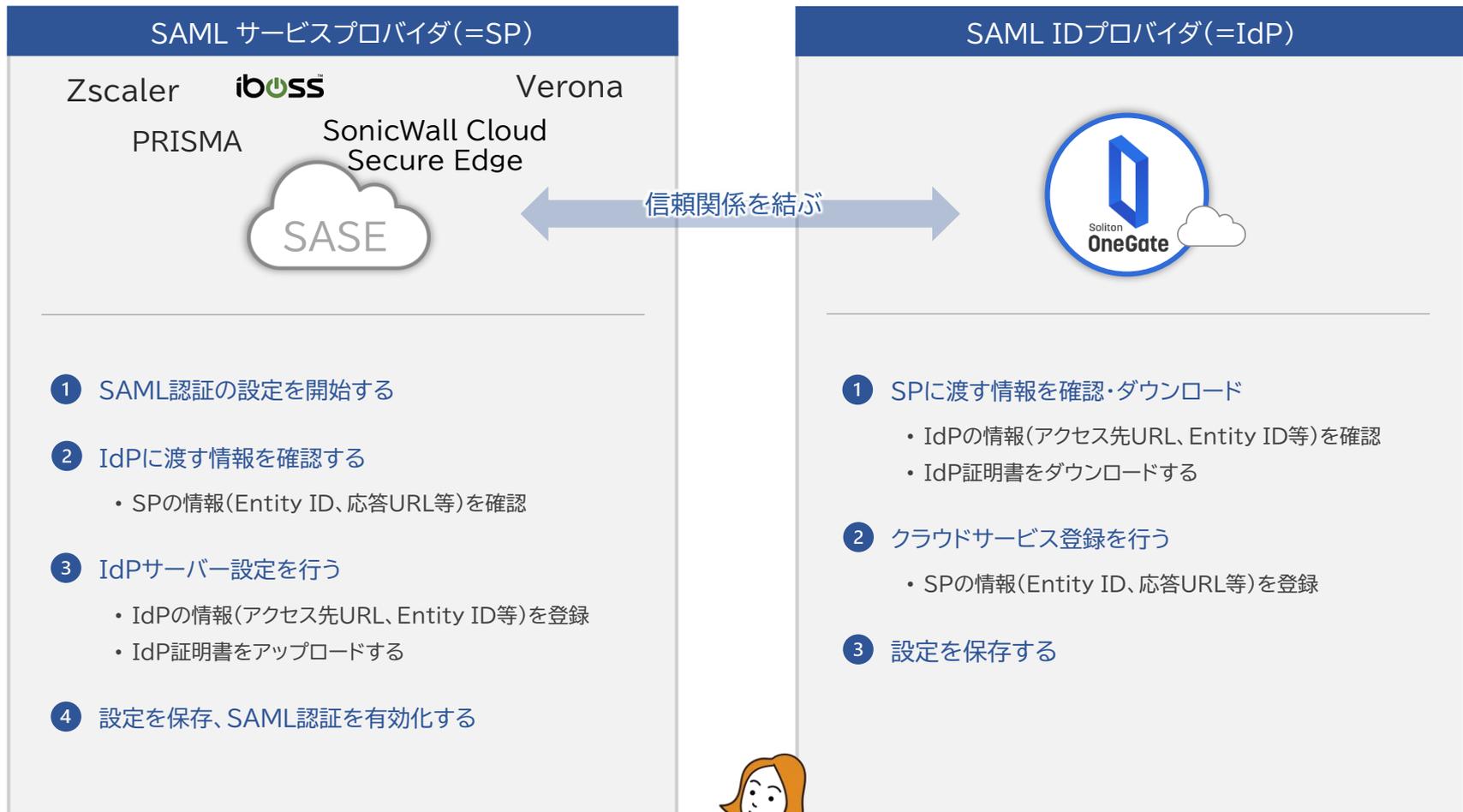
- 利用申請時に端末内で、公開鍵と秘密鍵の鍵ペアを自動生成する
- 公開鍵のみ認証局へ署名要求し、秘密鍵は端末外に一切出さない

という、証明書の不正コピーを許容しない安全性の高い仕組みがあってこそ、リモートファースト時代にも通用する適切な端末認証が可能となります。





## 連携設定とPKI認証の例



認可

認証プロファイル IDプロバイダー 新規

+ 追加 IdP + 追加 Zscaler Client Connector P

No.	ID	名前
1		
2		

保存 キャンセル

編集 IdP

全般情報

名前 Soliton OneGate ステータス  有効  無効

SAMLポータルURL <https://presales.ids-dev.solitonsys.jp/idp/sso> ログイン名の属性 NameID

エンティティID [https://login.zscalerthree.net/sfc\\_sso/22645873](https://login.zscalerthree.net/sfc_sso/22645873) 組織固有のエンティティID  有効  無効

IdP SAML Certificate current.pem アップロード IdP SAML Certificate Expiration Date October 22, 2025

ベンダー Others デフォルトIdP  有効

項目

ロケーション 全て 認証ドメイン 全て

サービスプロバイダー (SP) のオプション

SAMLリクエストをサイン  ×

SPメタデータ [メタデータをダウンロード](#)

保存 キャンセル

OneGateのURLを登録

OneGateのIdP証明書を登録

ログイン属性を指定

ここからZIAのメタデータをDL

著作権©2007-2021 Zscaler Inc. All rights reserved. | Version 6.1 | 4/24/2021 9:5



Zscaler  
Internet Access

## 認可

認証プロファイル IDプロバイダー **新規** 認証ブリッジ

+ 追加 IdP + 追加 Zscaler Client Connector Portal as IdP

No.	ID	名前	ステータス	ロケーション	IdP SAML Certificate E...	認証ドメイン
1	5539	Z-App Mobile Idp	✖	なし	---	soliton.co.jp
2	5537	Soliton OneGate	✔	全て	October 22, 2025	全て

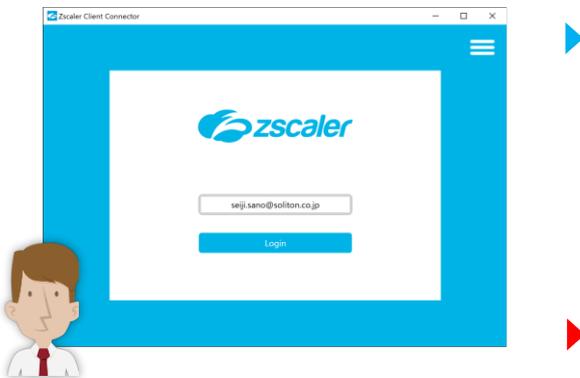
OneGateの登録完了

保存

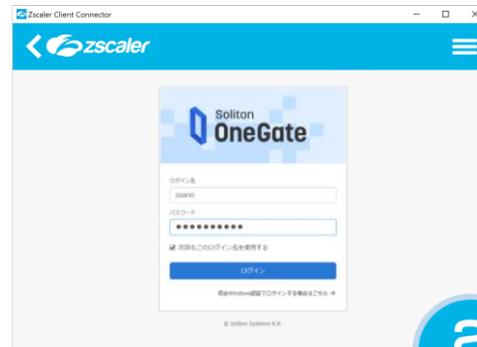
キャンセル



# Zscaler Internet Access × PKI認証 のイメージ



1  
要素



2  
要素

業務開始

業務禁止



# Prisma Access

## SAML アイデンティティ プロバイダ サーバー プロファイル



プロファイル名 OneGate\_presales\_SAML

場所 共有

管理者使用のみ

### アイデンティティ プロバイダ設定

アイデンティティ プロバイダ ID

OneGateのエンティティIDを登録

アイデンティティ プロバイダ証明書

IDP が SAML メッセージに署名するために使用する証明書を選択します

OneGateのIdP証明書を登録

アイデンティティ プロバイダ SSO URL

アイデンティティ プロバイダ SLO URL

OneGateのURLを登録

IDP への SSO 要求の SAML HTTP バインド  公表  リダイレクト

IDP への SLO 要求の SAML HTTP バインド  公表  リダイレクト

アイデンティティ プロバイダ証明書の検証

IDP への SAML メッセージの署名

最大クロック スキュー (秒)



# Prisma Access

認証プロファイル ?

名前

場所

認証 | 度 | 詳細

タイプ

IdPサーバープロファイル

署名要求の証明書   
IDP への SAML メッセージに署名する証明書を選択します

シングルログアウトの有効化

証明書プロファイル

IDPから送信されるSMALメッセージ内のユーザ属性

ユーザー名属性

ユーザーグループ属性

管理者ロール属性

アクセスドメイン属性

OneGateをSAML認証先として登録





## SAML 設定

保存 | すべての SAML ユーザーのログアウト | アクション | 更新

### 一般設定

- SAML を有効にする  YES
- クラスタSAMLを使用する  YES
- 初期化ステータス Ready
- 診断用メッセージ ログを有効にする  YES
- 診断用エラー ログを有効にする  YES
- CORS の互換性  YES
- SSL の使用  YES
- SAML 認証方法 Cookie ベース
- IDP バインディング手法 POST
- SAML 最大認証時間のずれ (秒) 86400
- SAML セッションタイムアウト (分) 15
- SAML エンティティ ID iboss-gateway-sp
- SAML グループ属性名
- SAML 認証バイパス ドメイン presales.ids-dev.solitonsys.jp, cloi
- SAML IDP ドメイン presales.ids-dev.solitonsys.jp, cloi

各設定を有効化

SAML認証方法と  
バインディングを設定

OneGateのドメインを設定



SAML グループ属性名	<input type="text"/>
SAML 認証バイパス ドメイン	<input type="text" value="presales.ids-dev.solitonsys.jp,clou"/>
SAML IDP ドメイン	<input type="text" value="presales.ids-dev.solitonsys.jp,clou"/>
スレッド プールのコア サイズ	<input type="text" value="20"/>
スレッドプールのバックログ サイズ	<input type="text" value="10"/>
スレッドプールの最大サイズ	<input type="text" value="200"/>
SAML 認証ソケット タイムアウト (ミリ秒)	<input type="text" value="20000"/>
SP 認証開始 URL	<input type="text" value="https://node-cluster147478-swg.ibosscloud.com:443/web/saml/auth/start"/>
SP ACS URL	<input type="text" value="https://node-cluster147478-swg.ibosscloud.com:443/web/saml/auth/sso/acs"/>
SAML セッション Cookie	<input type="text" value="....."/>

OneGateのメタデータを登録

IDP メタデータ

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://presales.ids-dev.solitonsys.jp/idp/sso"><md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIICODCCAbigAwIBAgIeGAXVp6ykPMA0GCsqG5Ib3DQEBCwUAMCkxjzAlBgnVBAMMHnByZXNhbGVzLmllcy1kZYXuc29saXRvbnN5cy5qcDCCASlwdQVjKoZlhvcNAQEbbQADggEPADCCAQoCggEBAIFBhDFJow7d7hCVMvWnR8fLmLMDnYOMxCoZKdMlmp9/IATmQsJ4R2ziMYGvbm0eOgwwmvxQWZgWJ5TV9kjS38zYXQDdtFPVhaP87130zrIMuX/CW5GaE++TSB8V1nCg8qJk3Oq+svZ8Hpi584AEdV8ieemRbrUNZ2dl0smozh2LmVrS2jxPOAR9TfjNaKO8jKsllufMstWXhvhQZYtRWFofnl3E0eSjE3OrwiWEX0DnfmPQIGxrdPWziw2zwY1Lf9FbP/ONKqagOaHtCDzAllQwZGBJ/Cz83+gQzbmqN9uBmi5aZvjBRE5D5uc5lpdq5XCd4bXH9XFm6HTyEkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAhgp774G0Nr+D5e9lq2aQG6QhxX73Fr1ao2Hc1hfj78vLtaOjqhVDhnmKelfPMGzVtNiE8IV/c2DSL5GdGD2I0dOagmZ/cmroQXAFXY/y2o4aa7vHYO0TmNwccadL+CPsH2jYSbqTfOly5++Q5H4Zen4N/iRR9uZg4bmlmp4nY/bcWVroaLTKkmVnS/AOMEGk6vMojYbUQYbe2RZFXZNUyUvVspUa7NyW2BLRNj+3xDSzJSM60HotiD9RI5GFR8RPazMNIllkxmynkFgu9o01CyTbRXQcg4p2HBVVDcVgJeNOYdcL7VnhZxpp0ldNQ2u8dEw0ajjU4PWaWftLUw==</ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://presales.ids-dev.solitonsys.jp/idp/sso"/><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://presales.ids-dev.solitonsys.jp/idp/sso"/></md:IDPSSODescriptor></md:EntityDescriptor>
```



**iboss** Soliton Systems K.K. - Account 147478 (Primary)

Cloud Access Security Broker | データ損失防止 | レポートと分析 | **プロキシとキャッシュ** | デバイスをクラウドに接続 | ユーザー、グループ、デバイス | カスタマイズ | ツール

プロキシ設定 | SSL 復号化

## プロキシ

保存 | DNS キャッシュのクリア | プロキシキャッシュのクリア

設定 | SSL/TLS | IP サロゲートと匿名認証 | **プロキシ PAC** | Socks プロキシ | キャッシュ設定 | 転送プロキシ | 追加のプロキシポート | キャッシュ規則 | ICAP サービ

### 一般設定

プロキシ設定を有効にする  
 YES  NO

オンライン プロキシを有効にする  
 YES  NO

追加のプロキシ ポートを有効にする  
 YES  NO

プロキシ モード  
標準プロキシ

プロキシ ポート  
80

既定のランディング ページ  
www.google.com

次のポートへのプロキシ アクセスを許可

ユーザー認証方法  
ブラウザベースSAML

識別できないユーザーのアクション  
既定のフィルター グループを使用する

Basic 認証タイムアウト  
300

DNS サフィックスのリスト

既定のフィルター グループ  
Default

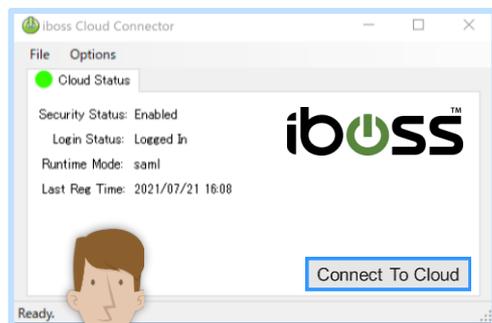
DNS ホスト  
node-cluster147478-swg.ibosscloud.com

**ブラウザベースSAMLを指定**





許可端末



証明書無



非管理端末



1  
要素



2  
要素

業務開始



業務禁止



# SonicWall Cloud Secure Edge

The screenshot shows the 'Settings' page for 'Identity and Access' in the SonicWall Cloud Secure Edge interface. The left sidebar contains navigation options: Home, Private Access, Internet Access, Trust, Networks, Directory, Settings (highlighted), and Get Help. The main content area is titled 'Settings' and has tabs for 'Identity and Access', 'SonicWall CSE Client', 'Configuration', and 'Certificates'. Under 'Identity and Access', there are sub-tabs for 'End User', 'Device', and 'API Keys'. The 'End User' tab is active, showing the 'User Identity Provider' configuration section. This section includes a description: 'Connect Cloud Secure Edge to your own Identity Provider. See [step-by-step instructions](#) in our help docs. Export current IDP configuration to a file on your device.' The configuration fields are: 'Provider Name' (a dropdown menu with 'Other' selected), 'Provider Protocol' (a dropdown menu with 'SAML' selected), 'Redirect URL' (a text input field containing 'https://<Cloud Secure Edge Name>.portal.banyanops.com/v2/call'), and 'Entity Issuer (optional)' (a text input field containing 'https://<Cloud Secure Edge Name>.portal.banyanops.com/v2/call').

OneGateをSAML認証先として登録



## SonicWall Cloud Secure Edge

The screenshot shows the 'IDP Settings' configuration page in the SonicWall Cloud Secure Edge interface. The page includes a sidebar with navigation options: Home, Private Access, Internet Access, Trust, Networks, Directory, Settings (highlighted), and Get Help. The main content area is titled 'IDP Settings' and contains several fields for configuring an Identity Provider (IDP). The 'IDP Metadata Method' is set to 'Manual'. The 'IDP SSO Uri' field contains the URL 'https://[redacted].ids.soliton-ods.jp/idp/sso'. The 'IDP CA Certificate' field contains a base64-encoded certificate string. The 'Username' field contains the URL 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd'. The 'Email' field contains the value 'email'. The 'Groups' field contains the value 'groups'. The 'Group Delimiter (optional)' field is empty. At the bottom of the page, there is a 'SCIM Provisioning' section with a toggle switch that is currently turned off. A 'Sign Out' button is located in the bottom left corner of the sidebar.

**SONICWALL**  
CLOUD SECURE EDGE

**Home**  
**Private Access**  
**Internet Access**  
**Trust**  
**Networks**  
**Directory**  
**Settings**  
**Get Help**

**Sign Out**

### IDP Settings

**IDP Metadata Method**  
You can either enter the Identity Provider metadata URL, or manually enter values from your Identity Provider

**IDP SSO Uri**  
Enter the SSO URL from the Identity Provider used for login

**IDP CA Certificate**  
Enter the SAML certificate from Identity Provider. If you have downloaded the certificate (base64), click Upload to select the certificate and insert into this field

**Username**  
Enter the client ID provided by your Identity Provider

**Email**  
Enter the client secret provided by your Identity Provider

**Groups**  
This is the Identity Provider claim for the groups attribute. The attribute may be used to assign a role to a user and/or device in CSE

**Group Delimiter (optional)**  
(Optional) A group delimiter helps CSE identify user groups sent by your IDP. The value entered into this field (e.g., ';' ) must align with the one already used by your IDP. Leave this field empty unless directed in our documentation

**SCIM Provisioning**  
Ensure that an Identity Provider has been configured to authenticate your end users. Once these settings are configured, SonicWall CSE's local user management will no longer be available to use.

Supported formats: .cer, .cert **Upload**

**Cancel** **Save**

**OneGateのURLを登録**

**OneGateのIdP証明書を登録**

**OneGateから連携するEmail属性名を設定**

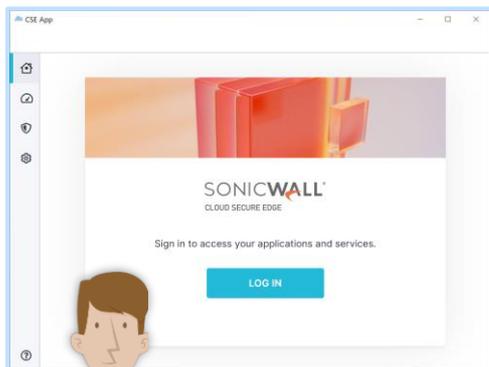
**OneGateから連携するGroups属性名を設定**



# SonicWall Cloud Secure Edge × PKI認証 のイメージ



許可端末



証明書無



非管理端末

## 認証用の証明書の選択

サイト presales.ids-dev-s.solitonsys.jp:443 では資格情報が必要です:



証明書情報

OK

キャンセル

1  
要素



ログイン名

ssano

パスワード

\*\*\*\*\*

次回もこのログイン名を使用する

ログイン

FIDO2 パスワードレス

統合Windows認証でログインする場合は

2  
要素

業務開始

業務禁止



このサイトは安全に接続できません

presales.ids-dev-s.solitonsys.jp でログイン証明書が承認されなかったか、ログイン証明書が提示されていない可能性があります。

システム管理者にお問い合わせください。

ERR\_BAD\_SSL\_CLIENT\_AUTH\_CERT



## Verona

Verona Cloud Server01 > SOLITON-TEST Network All Cloud

オーナー

オーナー編集

基本情報 ユーザープロビジョニング シングルサインオン SASE

シングルサインオン  有効  無効

SAML JIT プロビジョニング  有効  無効

識別子 (エンティティ ID) <https://c01-verona.all-cloud.jp/SOLITON-TEST>

応答Uri <https://c01-api-verona.all-cloud.jp/id/saml2/acs>

ログインUri

ログアウトUri <https://c01-api-verona.all-cloud.jp/id/saml2/logout>

Issuer識別子\*

Verona ClientログインUri <https://c01-api-verona.all-cloud.jp/id/saml2/login?ownerId=SOLITON-TEST>

SAML署名証明書

証明書ファイル

OneGateのURLを登録

OneGateをSAML認証先として登録

## Verona

Verona Cloud Server01 > SOLITON-TEST Network All Cloud

ログインUrl

ログアウトUrl

Issuer識別子\*

Verona ClientログインUrl

更新

SAML署名証明書

証明書ファイル **アップロード済**

ファイルを選択 選択されていません

OneGateのIdP証明書を登録

コモンネーム

フィンガープリント 3D  B9

有効期限 2026/04/08 14:13:24

アップロード 削除

Copyright © AMIYA Corporation All rights reserved.



Verona Client

ログインするとユーザー専用機能が使用出来るようになります。

※ログインは事前にVerona Cloudで設定が必要です。  
※ログインしなくてもVPN接続は可能です。

**Microsoft Entra ID**

ログイン後にアプリ選択画面が表示されるので「Verona Client」をクリックしてください。

**Verona Cloud, IDaaS**

初回はログインURLを入力してからログインしてください。  
 ログインURLをリセットする

許可端末



認証用の証明書の選択

サイト presales.ids-dev-s.solitonsys.jp:443 では資格情報が必要です:

jueda	
presales.ids-dev-s.solitonsys.jp	
2021/4/9	

証明書情報

OK キャンセル

1 要素

Soliton OneGate

ログイン名  
ssano

パスワード  
\*\*\*\*\*

次回もこのログイン名を使用する

ログイン

FIDO2 パスワードレス  
統合Windows認証でログインする場合は

2 要素

業務開始

証明書無

非管理端末



業務禁止

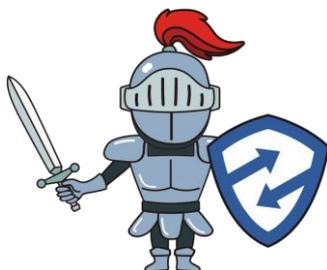


このサイトは安全に接続できません

presales.ids-dev-s.solitonsys.jp でログイン証明書が承認されなかったか、ログイン証明書が提示されていない可能性があります。

システム管理者にお問い合わせください。

ERR\_BAD\_SSL\_CLIENT\_AUTH\_CERT



資料のダウンロード、トライアル申込は

ソリトンワンゲート

検索

株式会社 ソリトンシステムズ <https://www.soliton.co.jp/>

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 [netsales@soliton.co.jp](mailto:netsales@soliton.co.jp)

記載の会社名及び製品名は、各社の商標または登録商標です。

Copyright © Soliton Systems K.K. All rights reserved.

2025年 7月

SOGWP-PKIS-03

