

利用端末を特定する MFA で、日本企業のニーズに対応

PKIでSASEの導入効果を高める

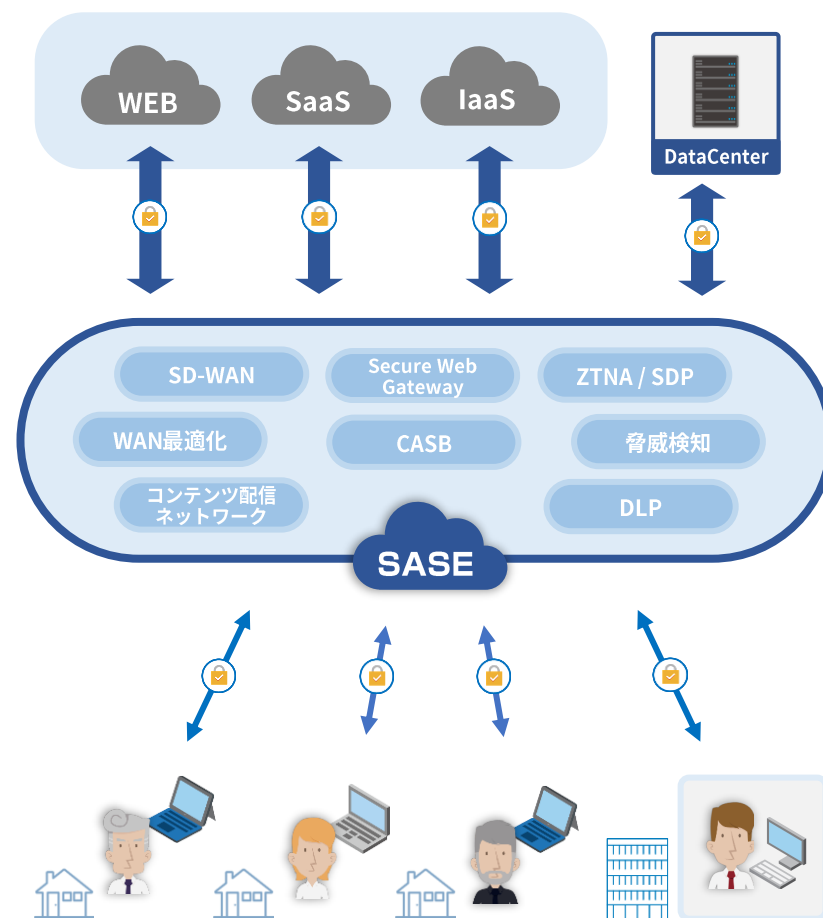


集約型ネットワークの限界、注目される SASE

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。

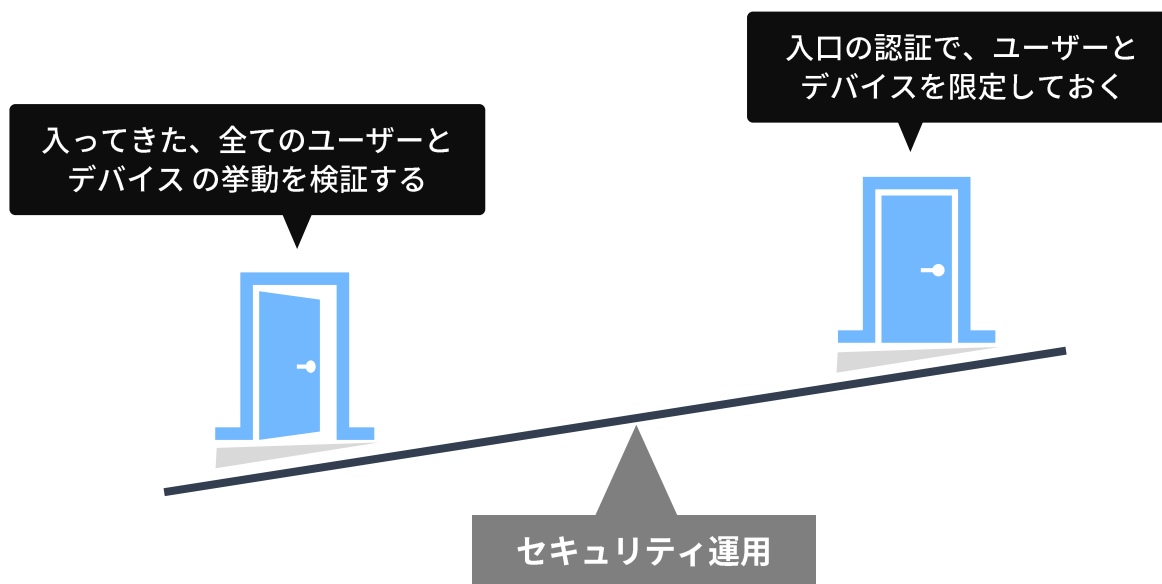


※ Secure Access Service Edgeの略。ネットワーク機能とセキュリティ機能をクラウド上で包含的に提供する考え方。ゼロトラストモデルを実現するための方法の一つ。

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。

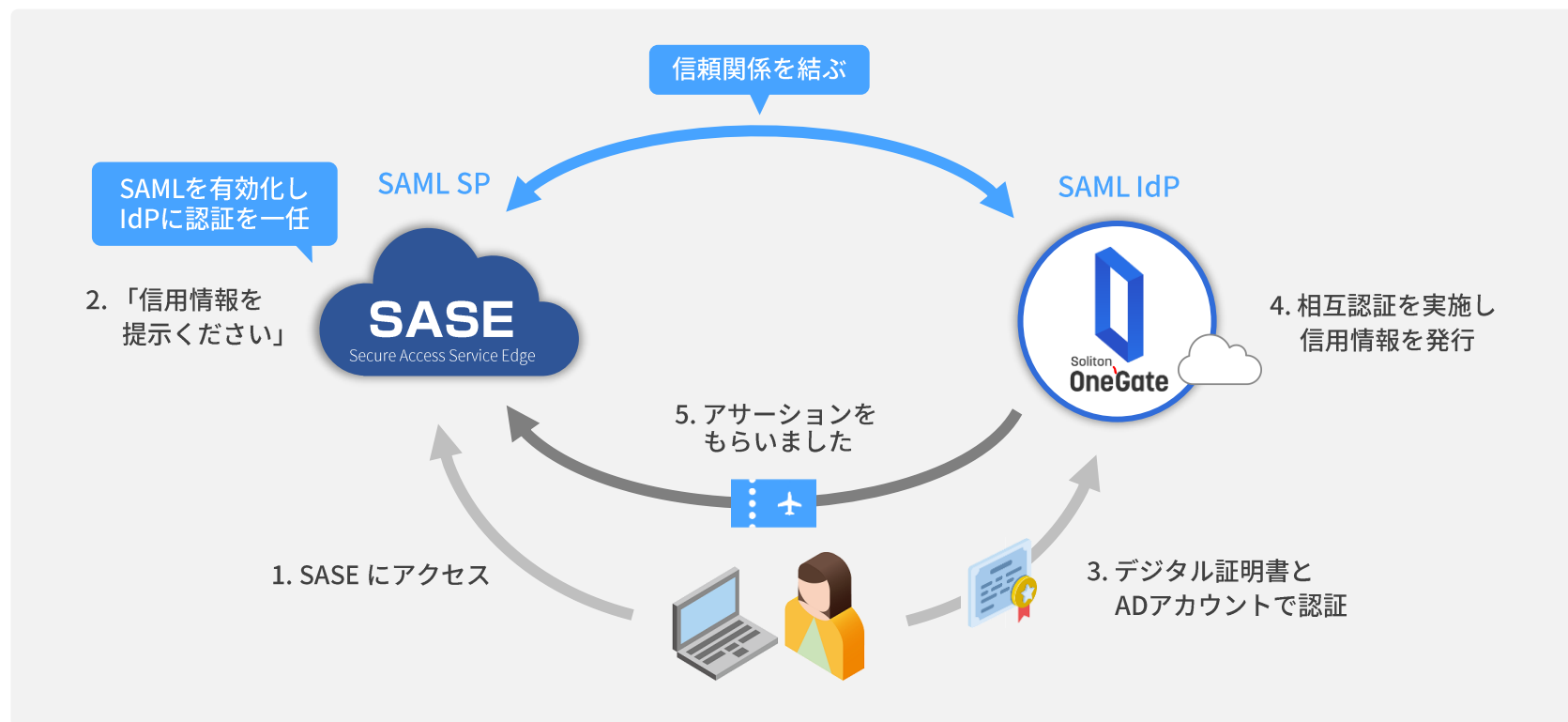
つまり、運用コストを抑えながら最大限の効果を出すために、**入口の認証を抑えておく**ことが、リモートファーストへの転換に向けた重要なファーストステップとなります。



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（MFA）を実装するには、インターネット標準の認証連携技術であるSAMLの利用が一般的です。**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MFA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。

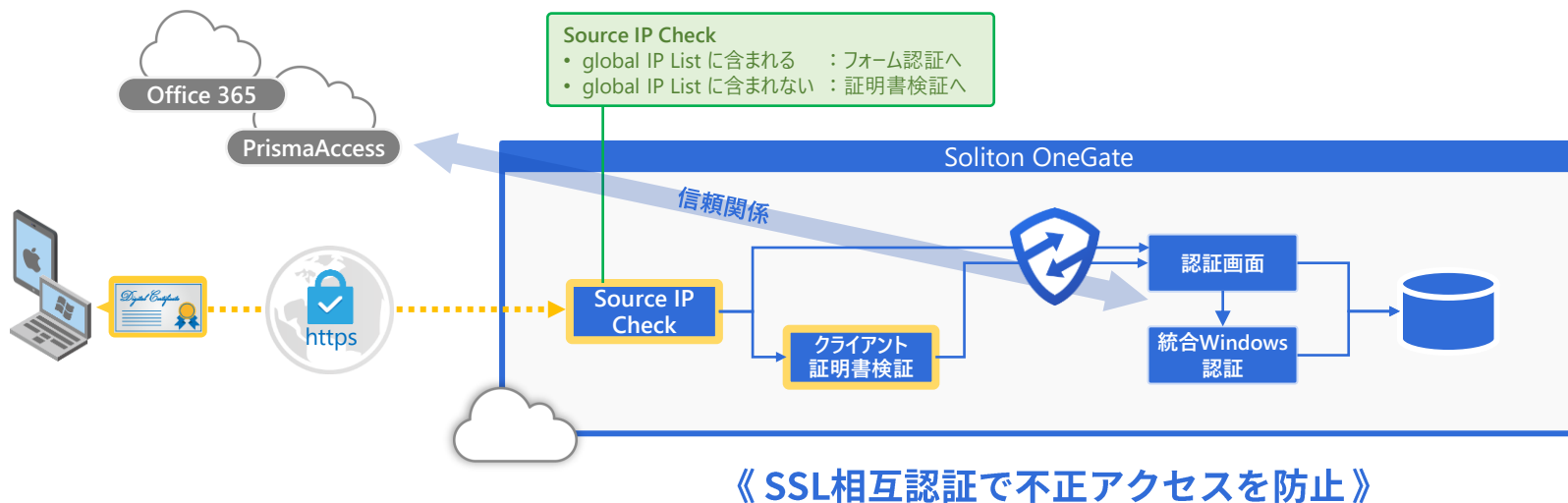
インターネット上のクラウドサービスは、IPアドレス制限をしていない限り、**誰でも、何度も、ログイン画面にアクセス**することができます。アカウント確認を装って、偽サイトに誘導し、フィッシングでSMS認証も突破することは、社員数が多いほど、容易にできてしまいます。



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う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、**MFA 方式の中でも高い優位性**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、他の認証手法とは異なり**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。



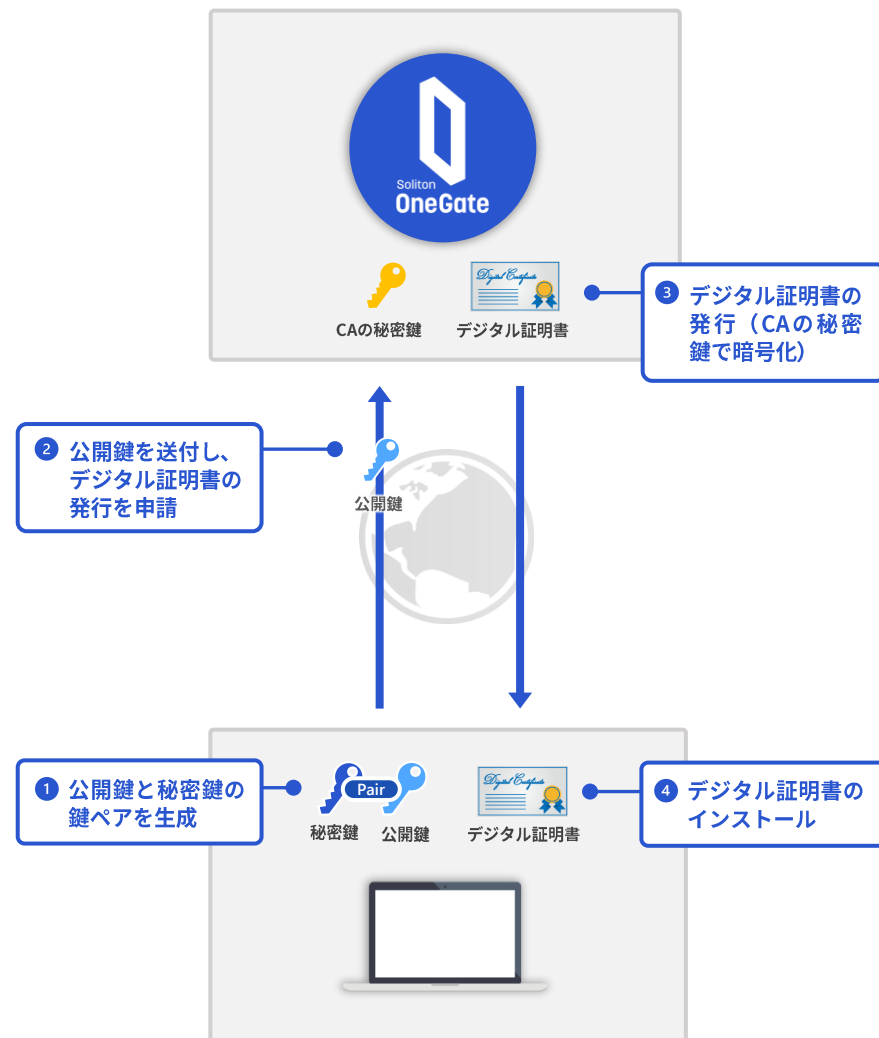
クライアント証明書の安全な配布手法

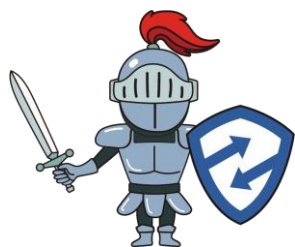
クライアント証明書は、P12ファイルという秘密鍵付きのファイル形式で配布することも可能ですが、一度発行したP12ファイルは容易にコピーすることができてしまいます。そのため、利用者へファイル形式で証明書を配布することは推奨されません。

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

SAML連携設定の流れ

SAML サービスプロバイダ (=SP)

zscaler ibOSS PRISMA Netscope



信頼関係を結ぶ

SAML IDプロバイダ (=IdP)



① SAML認証の設定を開始する

② IdPに渡す情報を確認する

- SPの情報（Entity ID、応答URL等）を確認

③ IdPサーバー設定を行う

- IdPの情報（アクセス先URL、EntityID等）を登録
- IdP証明書をアップロードする

④ 設定を保存、SAML認証を有効化する

① SPに渡す情報を確認・ダウンロード

- IdPの情報（アクセス先URL、EntityID等）を確認
- IdP証明書をダウンロードする

② クラウドサービス登録を行う

- SPの情報（Entity ID、応答URL等）を登録

③ 設定を保存する



zscaler Internet Access のSAML設定画面 - 1

zscaler
Internet Access

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		

OneGateのURLを登録

OneGateのIdP証明書を登録

ログイン属性を指定

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

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](#)

ここからZIAのメタデータをDL

保存 キャンセル

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





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



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 https://presales.ids-dev.solitonsys.jp/idp/sso

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 crt.OneGate_presales_SAML.shared

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 https://presales.ids-dev.solitonsys.jp/idp/sso

アイデンティティ プロバイダ SLO URL https://presales.ids-dev.solitonsys.jp/idp/logout

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) 60



Prisma Access

認証プロファイル

?

名前

OneGate_presales_SAML

場所

共有

▼

認証

度

詳細

タイプ

SAML

▼

IdPサーバープロファイル

OneGate_presales_SAML

署名要求の証明書

None

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

None

▼

IDPから送信されるSAMLメッセージ内のユーザ属性

ユーザー名属性

username

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





iboss のSAML設定画面 - 1

ソリトンシステム株式会社 - アカウント147478(プライマ

ウェブ

CASB

クラウド アクセスセキュリティブローカー

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

クラウド接続デバイス

静的なユーザーとデバイスのポリシー

グループ管理

スソ

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	各設定を有効化
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	SAML認証方法と バインディングを設定
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,clou	OneGateのドメインを設定
SAML IDP ドメイン	presales.ids-dev.solitonsys.jp,clou	

iboss のSAML設定画面 - 2



iboss

ソリトンシステムズ株式会社 - アカウント147478(プライマ

ウェブ

クラウド アクセスセキュリティブローカー

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

クラウド接続デバイス

静的なユーザーとデバイスのポリシー

グループ管理

スロ

SAML グループ属性名

SAML 認証バイパス ドメイン

SAML IDP ドメイン

スレッド プールのコア サイズ

スレッドプールのバックログ サイズ

スレッドプールの最大サイズ

SAML 認証ソケット タイムアウト (ミリ秒)

SP 認証開始 URL

SP ACS URL

SAML セッション Cookie

IDP メタデータ

presales.ids-dev.solitonsys.jp, clo

presales.ids-dev.solitonsys.jp, clo

20

10

200

20000

https://node-cluster147478-swg.ibosscloud.com:443/web/saml/auth/start

https://node-cluster147478-swg.ibosscloud.com:443/web/saml/auth/sso/acs

.....

```
<?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>MIIIC0CCABigAwIBAgIGAXVP6ykPMA0GCSqGSIb3DQEBCwUAMCkxjzAlBgNVBAMMHnByZXNhbnVzLm1kcy1kZXYuc29saXRvbnN5cy5qcDCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIFBhDFJow7d7hCVMvWnR8fLmLMDnYomXC0KdMlmp9/ATmQ5J4R2ziMYGvbm0eOgowmvxQWZgWj5TV9kJS38zYXQDDtFPVhaP87130zrIMuX/CW5GaE++TSB8V1nCG8qJkK3Oq+svZ8Hpi584AEdV8ieemRbrUNZ2dl0smozh2LmVrS2jxPOAR9TfjNaKO8JkSlulFV MstWXhvhQZytrWfOfnI3E0EslJE3OrwIWEx0DnfmPQIGxrdPWziw2zwY1Lf9FbP/ONKqagOaHtCDzAllQwZGBJ/Cz83+gQzbmqN9uBMi5aZvjBRE5D5uc5lp dq5XCd4bXH9FM6HTyEkCawEAATANBgkqhkiG9w0BAQsFAAOCAQEAhggpp74G0Nr+D5e9lq2aQG6QhxX73Fr1ao2Hc1hfj78vLtaOjqhVdHnmKelfPMGz VtNiE8lV/c2DSL5GdGD2l0dOagmZ/cmroQXAFXYl/y2o4aa7vHYO0TmNwccadL+CPsH2jYSbqTFOly5++Q5H4Zen4N/iRR9uZg4bmLmp4nY/bcWVroaLTkK mVnS/AOMEGk6vMojYbUQYbe2RZFXZNUyUvVspUa7NyW2BLRNj+3xDsZJSM60HotiD9RI5GFr8RPazMNIllkxmyNKFguo01CyTbRXQcg4px2HBVVDcVgJe nOYdcL7VnhZxpp0ldNQ2u8dEw0aijU4PWaWftLUw==</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>
```

OneGateのメタデータ
を登録



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

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

インライン プロキシを有効にする

NO

追加のプロキシ ポートを有効にする

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

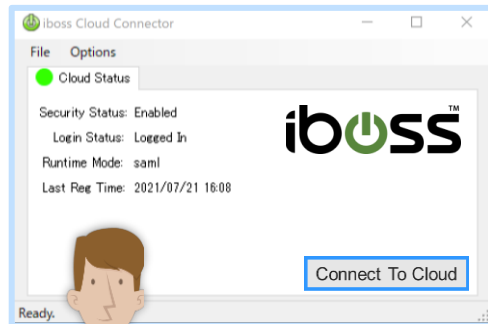
node-cluster147478-swg.ibosscloud.com

ブラウザベースSAMLを指定





許可端末



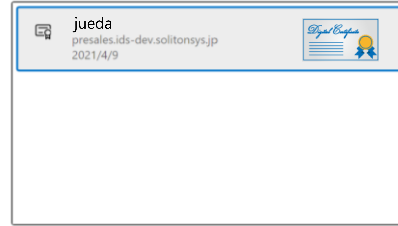
証明書無



非管理端末

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





Netscope

Security Cloud Platform > Forward Proxy >

Authentication - Forward Proxy

Setup Authentication for Netscope for Web users to be redirected to the configured Identity Provider. This allows you to capture the identity of the user in the absence of the Netscope Client. Additionally, if you are using IdP to provision the Netscope Client, authentication needs to be enabled.

Authentication

Authentication: ● Enabled
Type: SAML Authentication: SolitonOneGate

[ENABLE AUTHENTICATION](#)

Bypass Settings

Administrators can use this section to identify domains and

DOMAIN BYPASS

[EDIT](#)

WEB CATEGORY BYPASS
None Specified

Enable Authentication

☒ Enabled

SAML ACCOUNT *

SolitonOneGate [CREATE NEW](#)

AUTHENTICATION REFRESH INTERVAL ⓘ

1 Hours

ENABLE COOKIE SURROGATE

☐ Disabled

[CANCEL](#) [SAVE](#)

前のページで設定した SAML アカウントを選択

Domain Bypass

ts.muklocshz-admin.okta.com

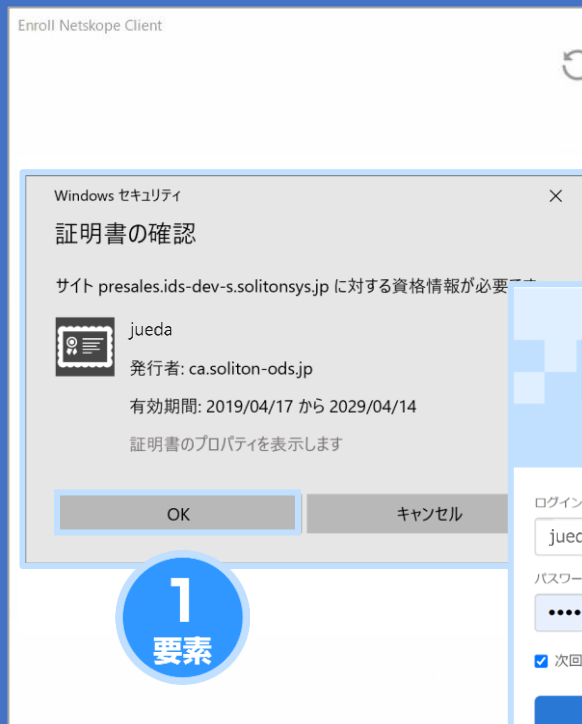
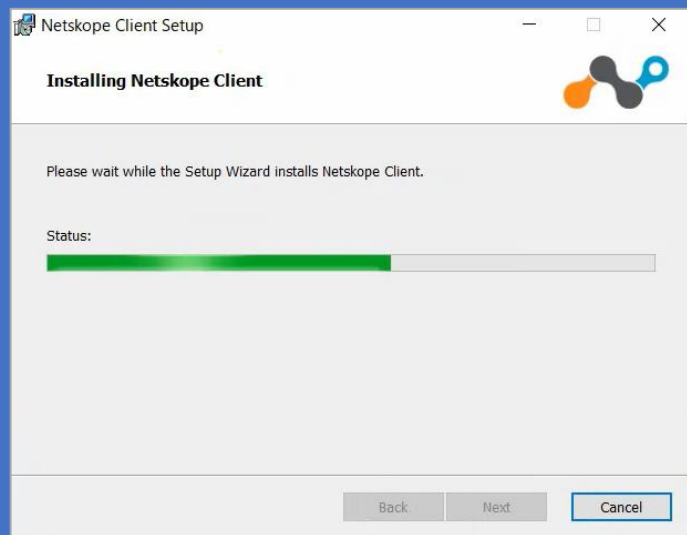
[CANCEL](#) [SAVE](#)

OneGateのドメインを追加し 認証時はNetscopeをバイパス するよう設定

FORWARD PROXY
→Authenticationをクリック



Netscope × PKI認証 のイメージ



Netscope Clientのインストール時に※ OneGateで多要素認証を実行



※ batファイルによるインストール展開は、都築電気株式会社にて検証実施しています。

導入相談はこちら ▶ 都築電気株式会社 テクノロジーデザイン統括部 セキュリティビジネス推進室 secbiz@tsuzuki.co.jp





株式会社 ソリトンシステムズ

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 netsales@soliton.co.jp

製品ページ <https://www.soliton.co.jp/onegate>

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.

2022年 1月

SOGWP-PKIS-02

