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

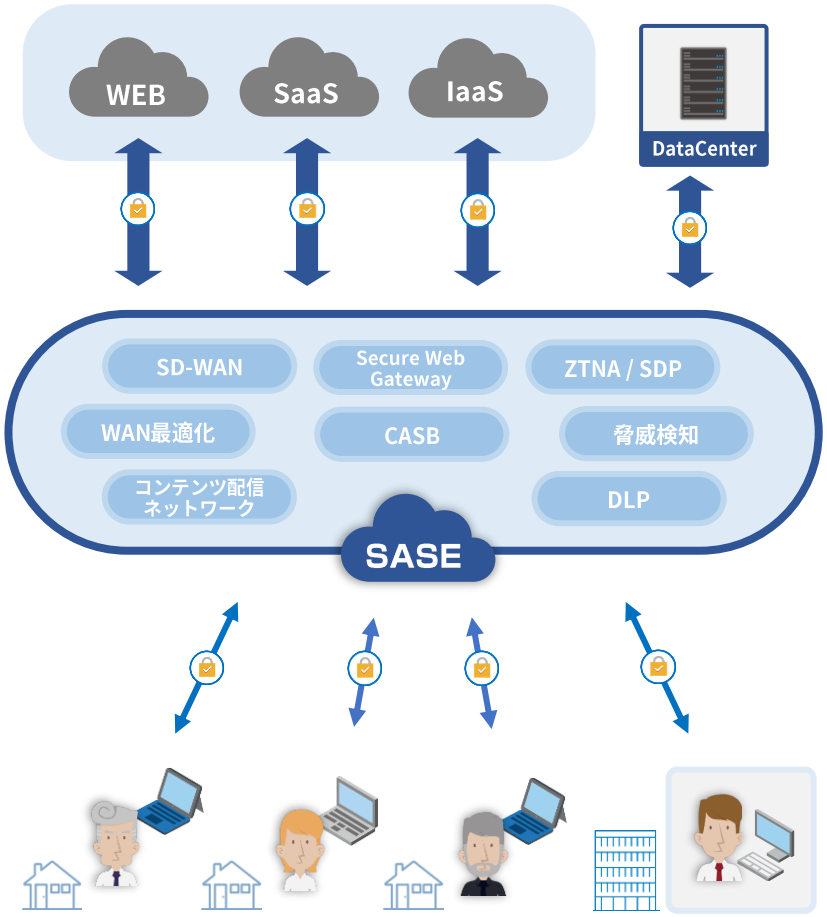
Soliton OneGate

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。

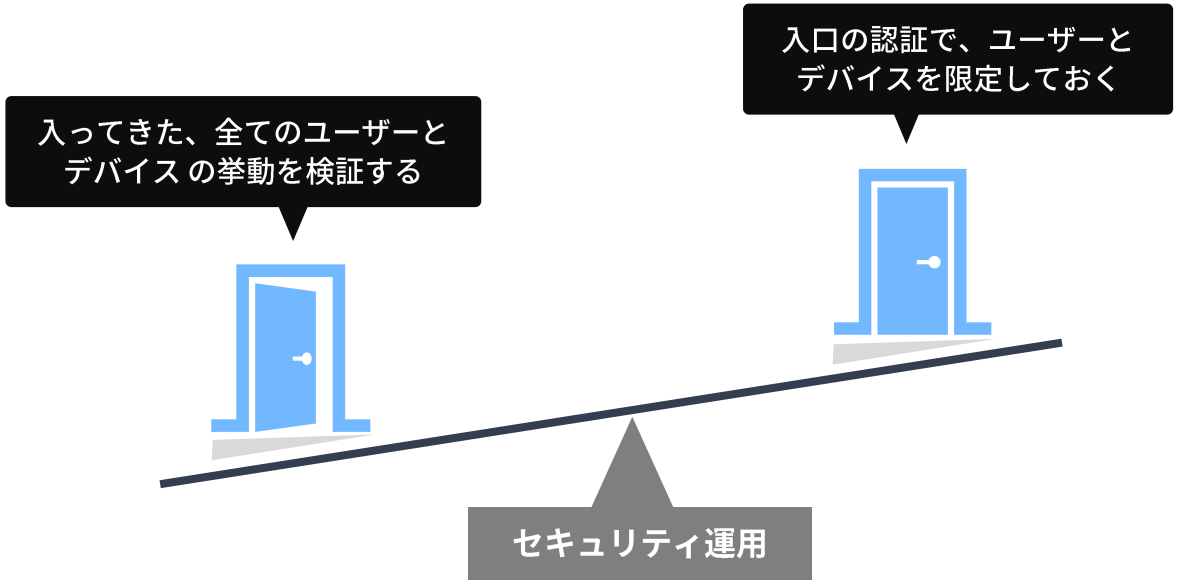


※ Secure Access Service Edgeの略。ネットワーク機能とセキュリティ機能をクラウド上で包含的に提供する考え方。ゼロトラストモデルを実現するための方法の一つ。

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。

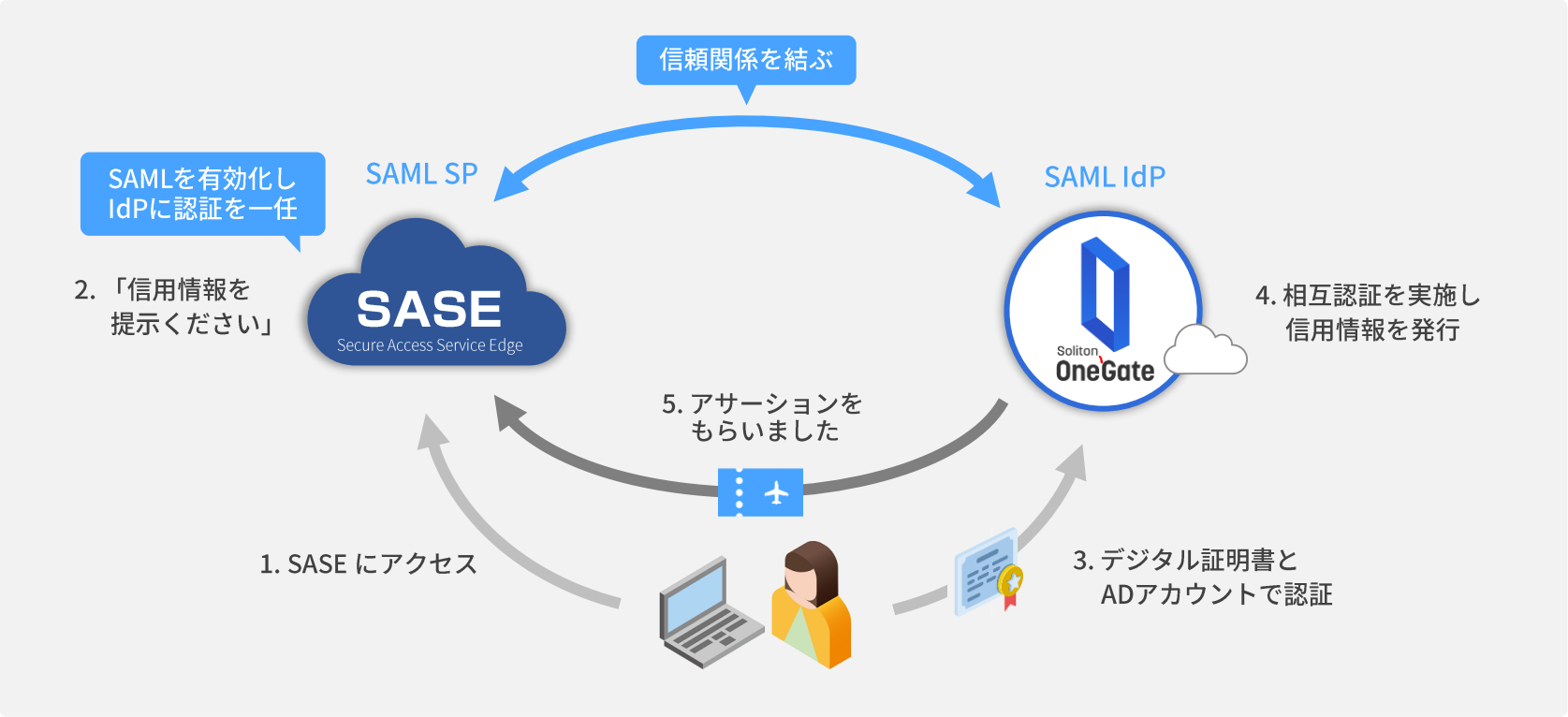
つまり、運用コストを抑えながら最大限の効果を出すために、**入口の認証を抑えておく**ことが、リモートファーストへの転換に向けた重要なファーストステップとなります。



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。

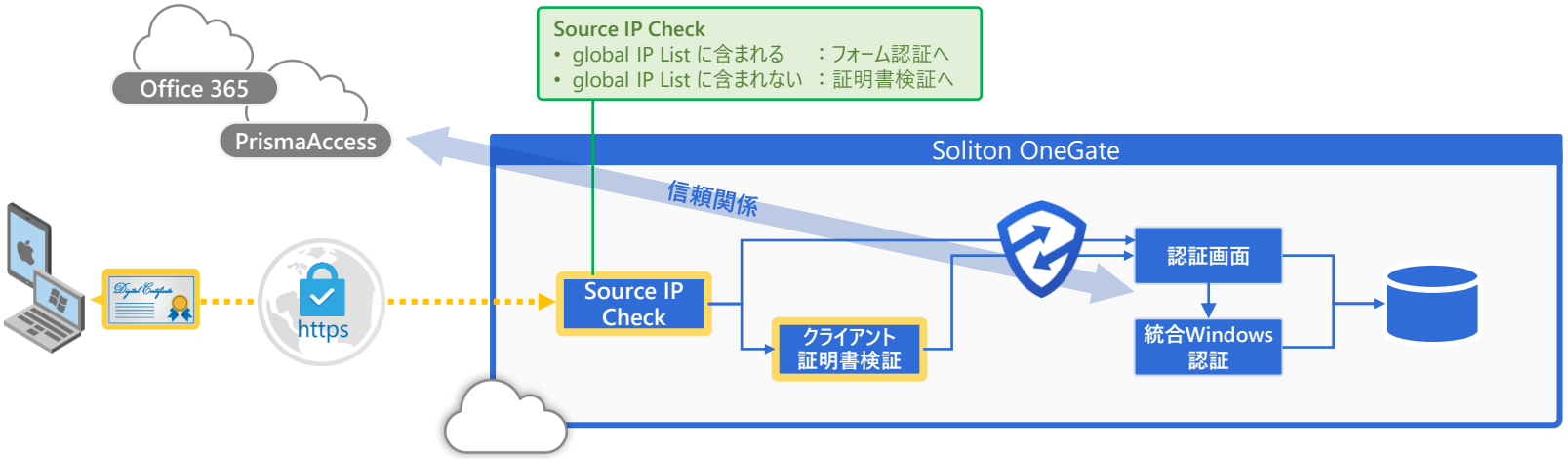
また、SMSワンタイムは利用者本人の確認手段であり日本国内でニーズの強い、**利用端末の特定に対応できない**点にも注意が必要です。

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、社員数が多ければ多いほど、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、**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されません。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します。



《SSL相互認証で不正アクセスを防止》

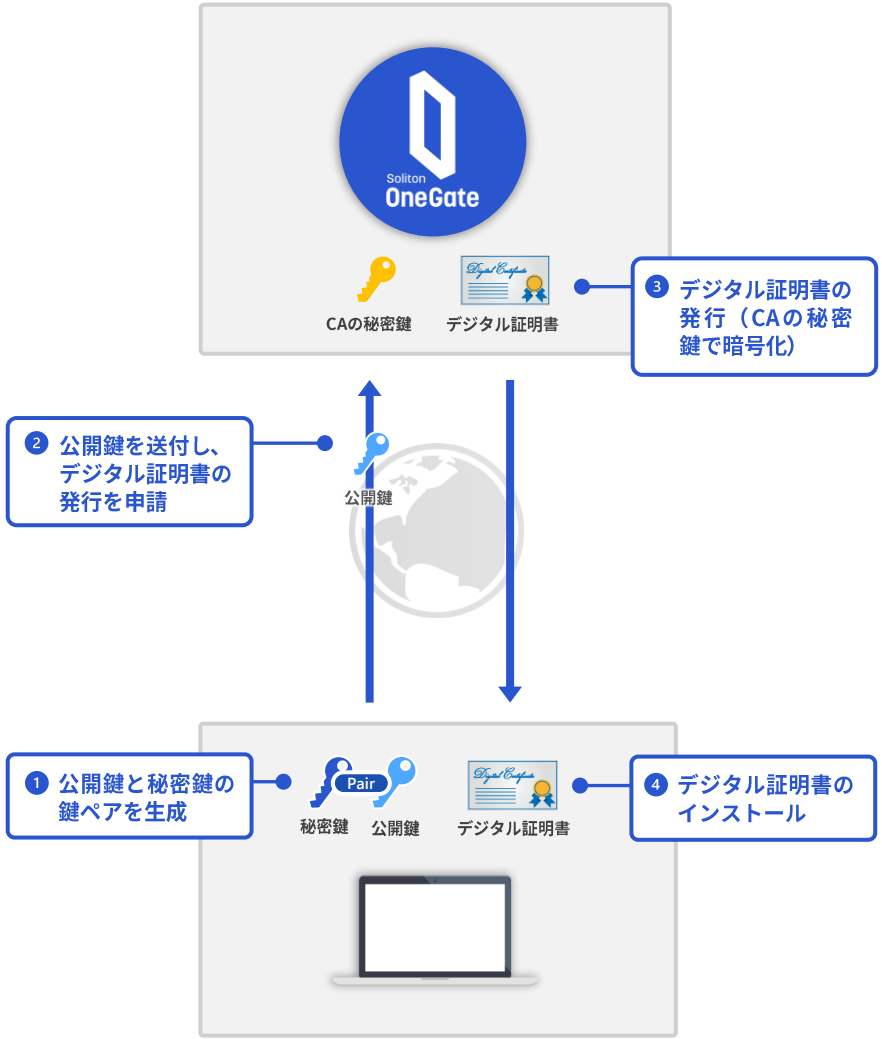
クライアント証明書の安全な配布手法

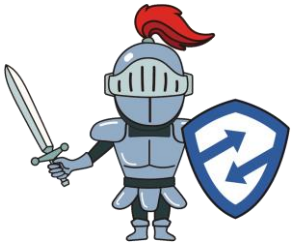
クライアント証明書は、P12ファイルという秘密鍵付きのファイル形式で配布することも可能ですが、一度発行したP12ファイルは容易にコピーすることができてしまいます。そのため、利用者へファイル形式で証明書を配布することは推奨されません。

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

SASE

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、Entity ID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**

信頼関係を結ぶ

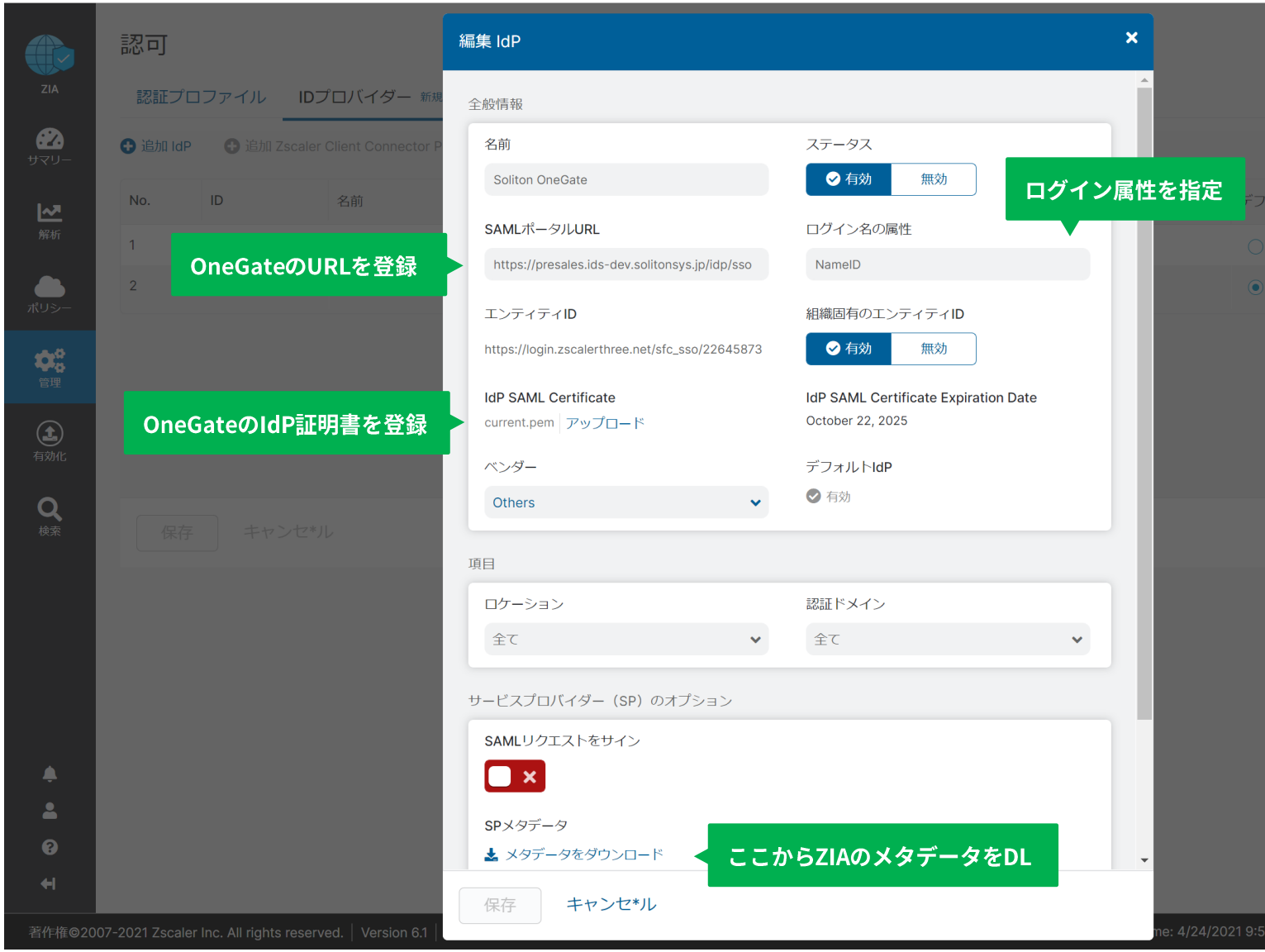
SAML IDプロバイダ（=IdP）

Soliton OneGate

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、Entity ID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**

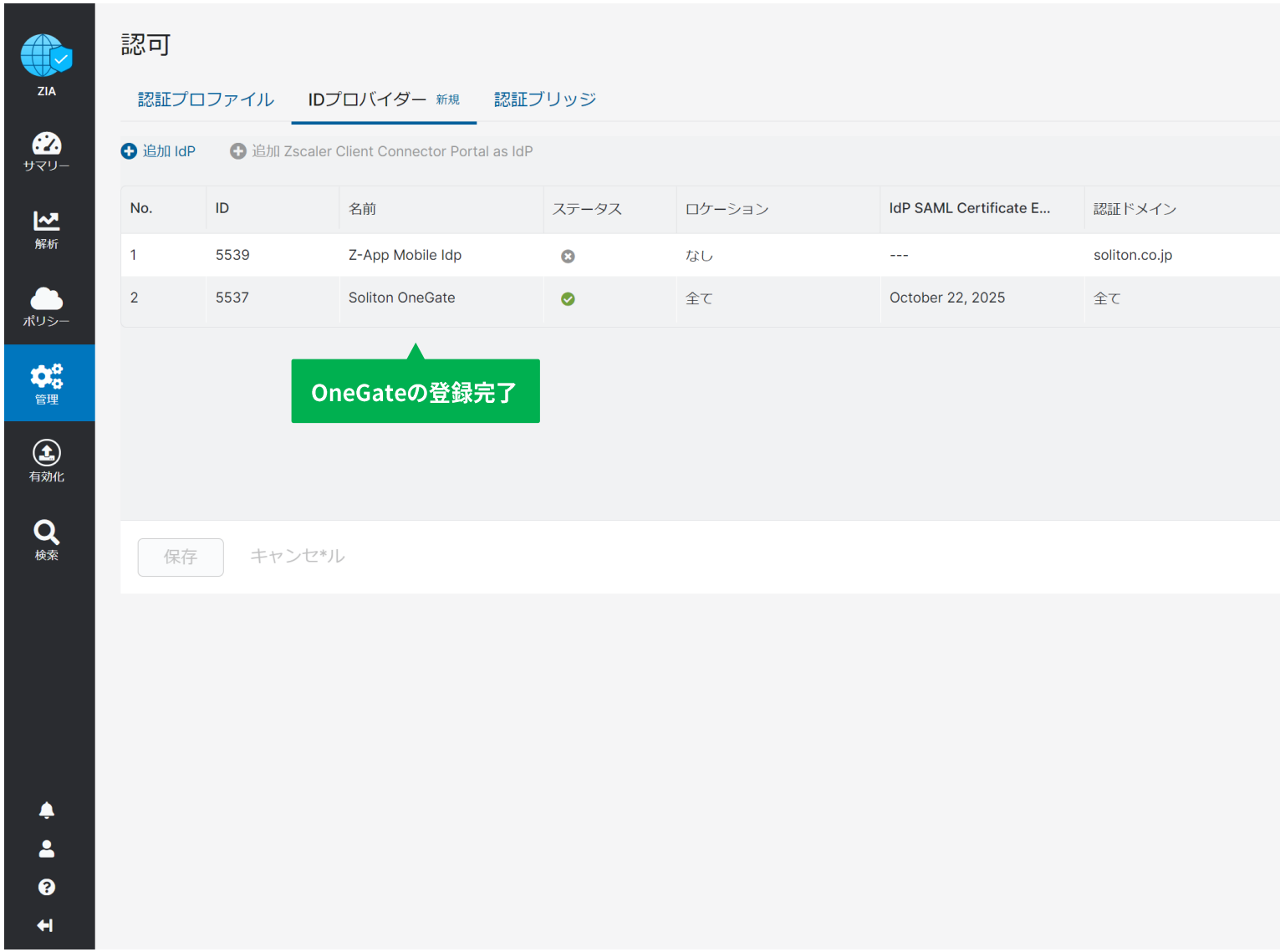
zscaler Internet Access のSAML設定画面 - 1

zscaler
Internet Access



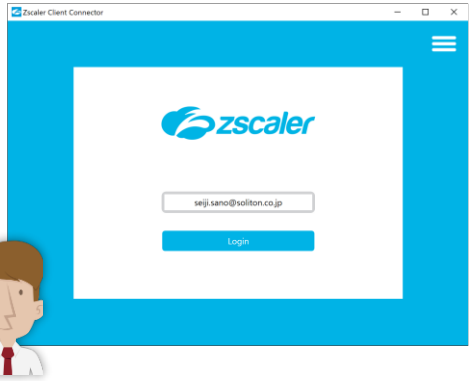
zscaler Internet Access のSAML設定画面 - 2

zscaler
Internet Access

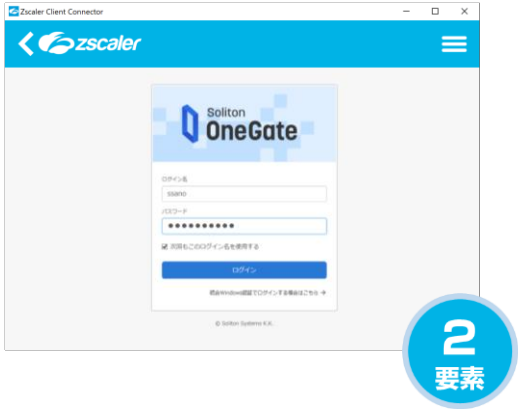


zscaler Internet Access × PKI認証 のイメージ

許可端末



1 要素



2 要素

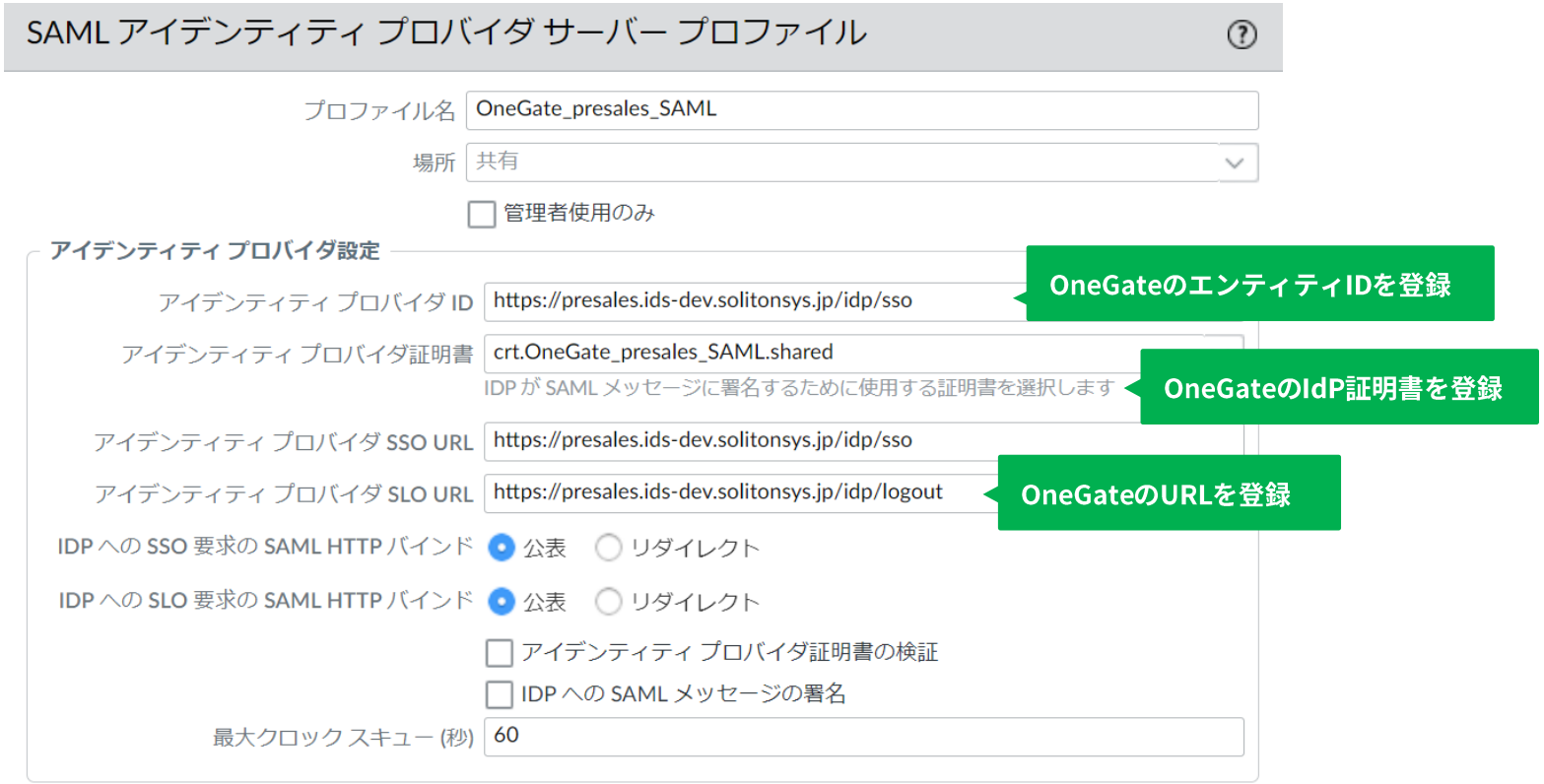
業務開始

証明書無

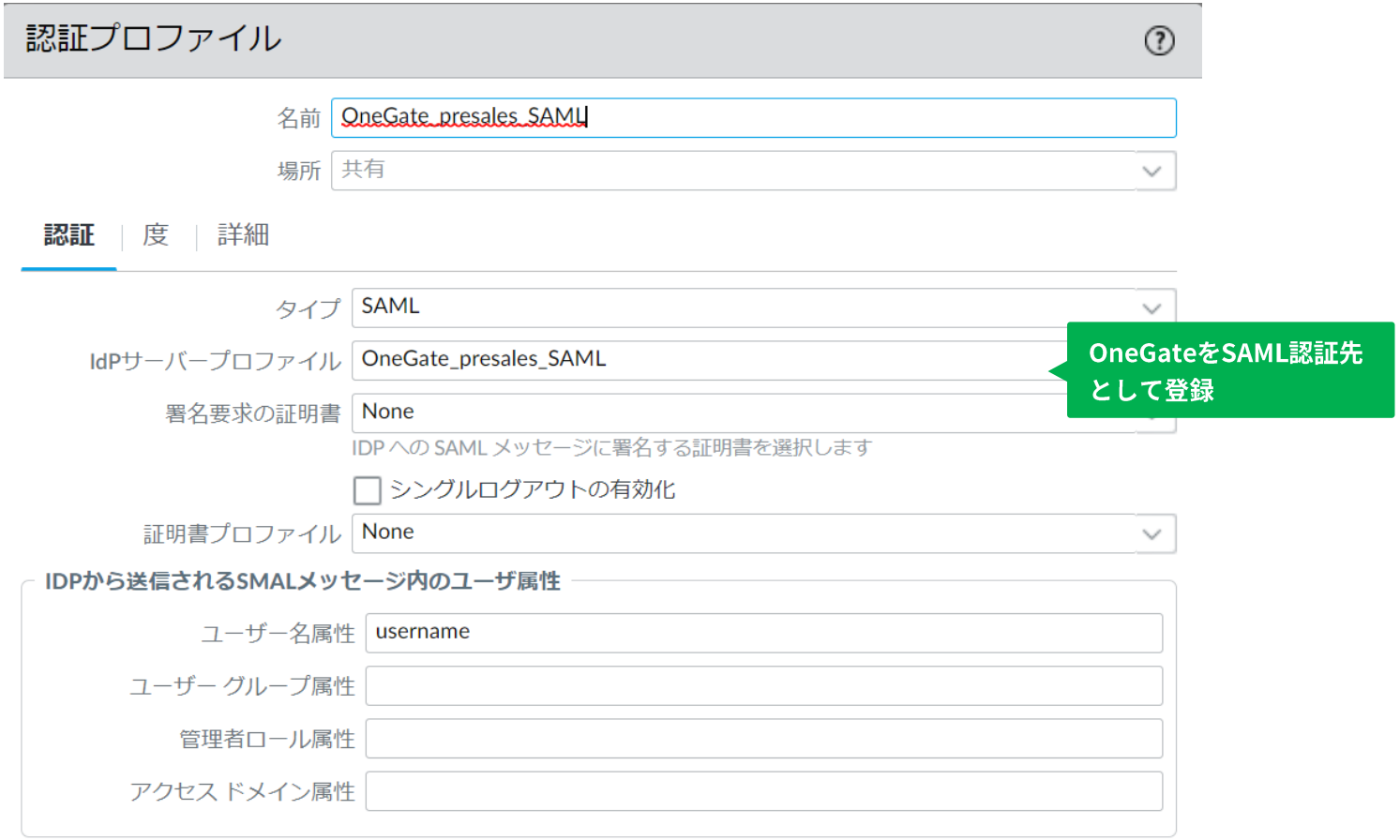
非管理端末

業務禁止

Prisma Access



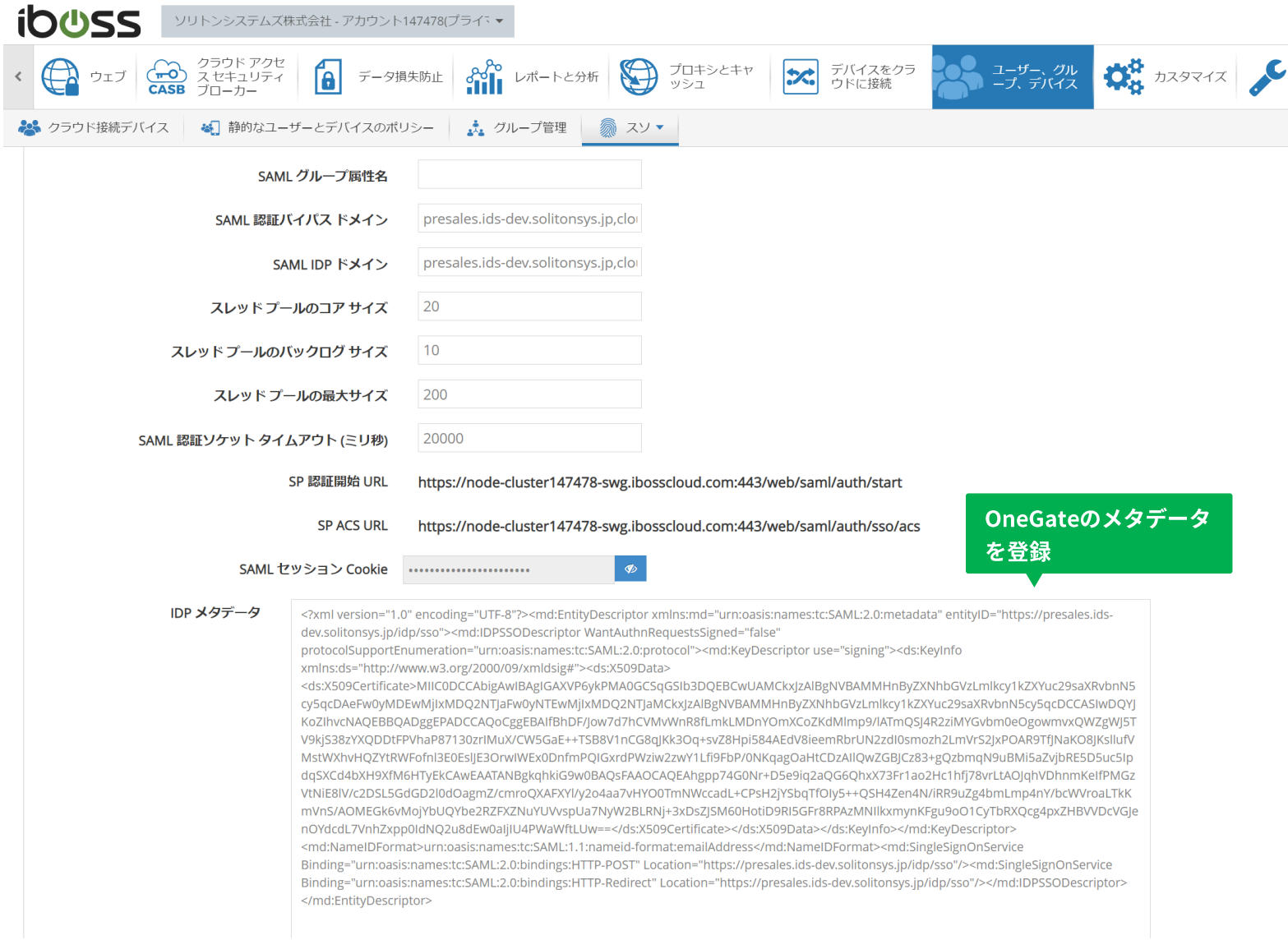
Prisma Access



Prisma Access × PKI認証 のイメージ

iboss のSAML設定画面 - 1

iboss のSAML設定画面 - 2

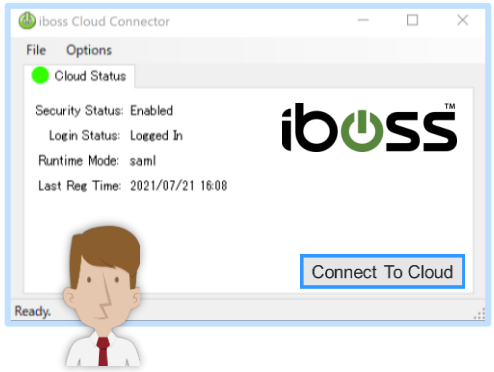


iboss のプロキシ設定画面

iboss × PKI認証 のイメージ

許可端末

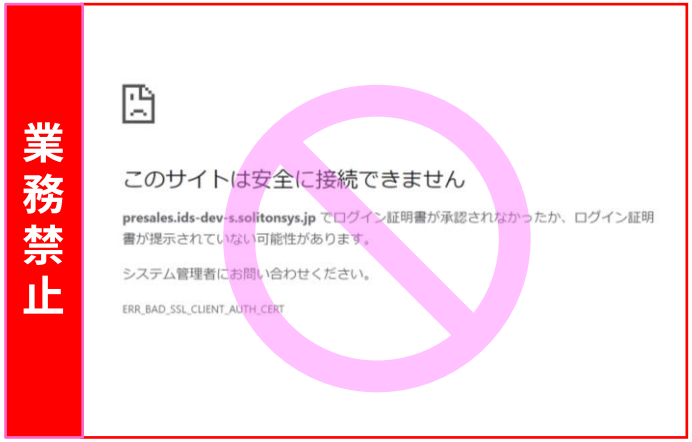
業務開始



証明書無

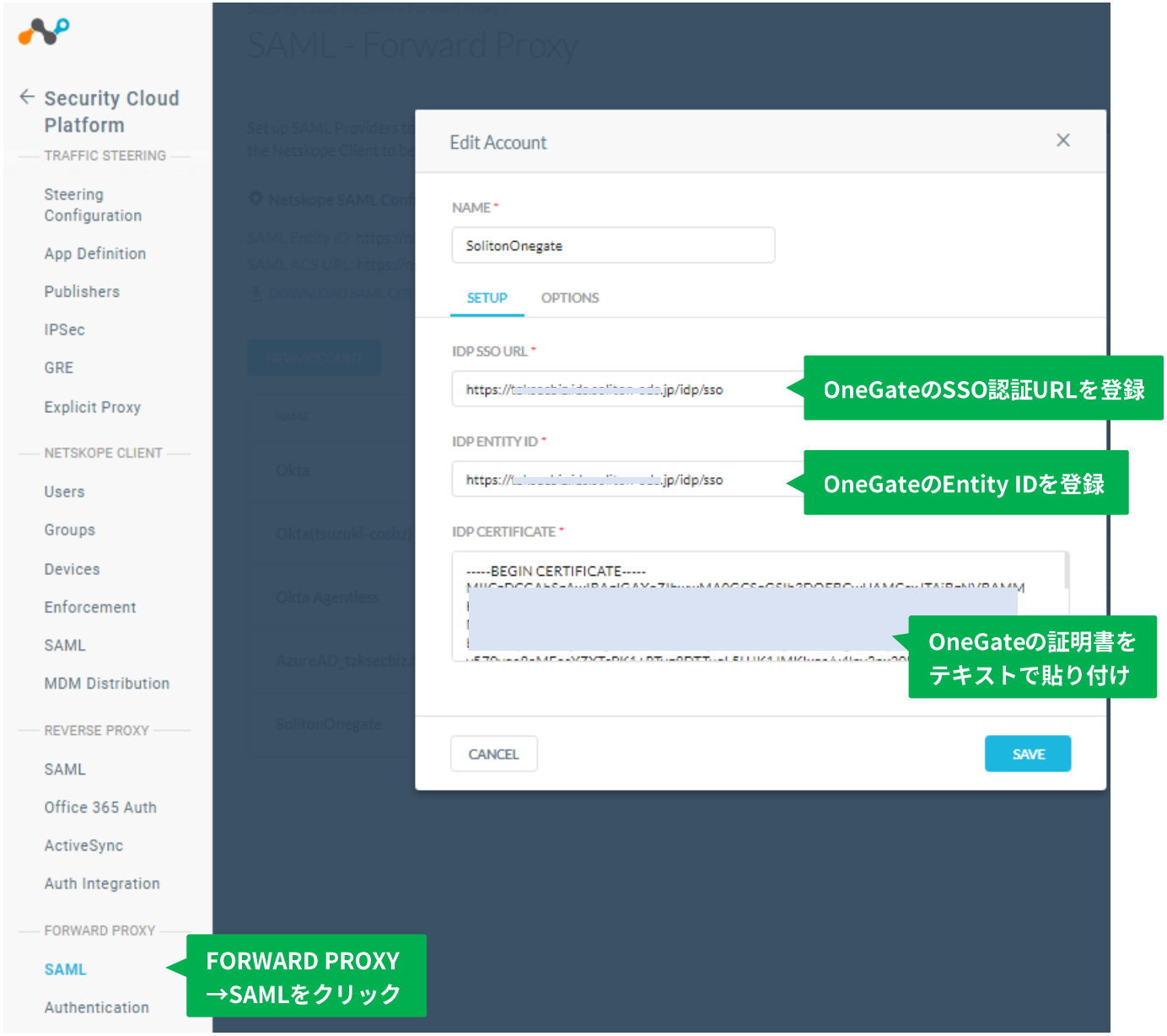
非管理端末

業務禁止



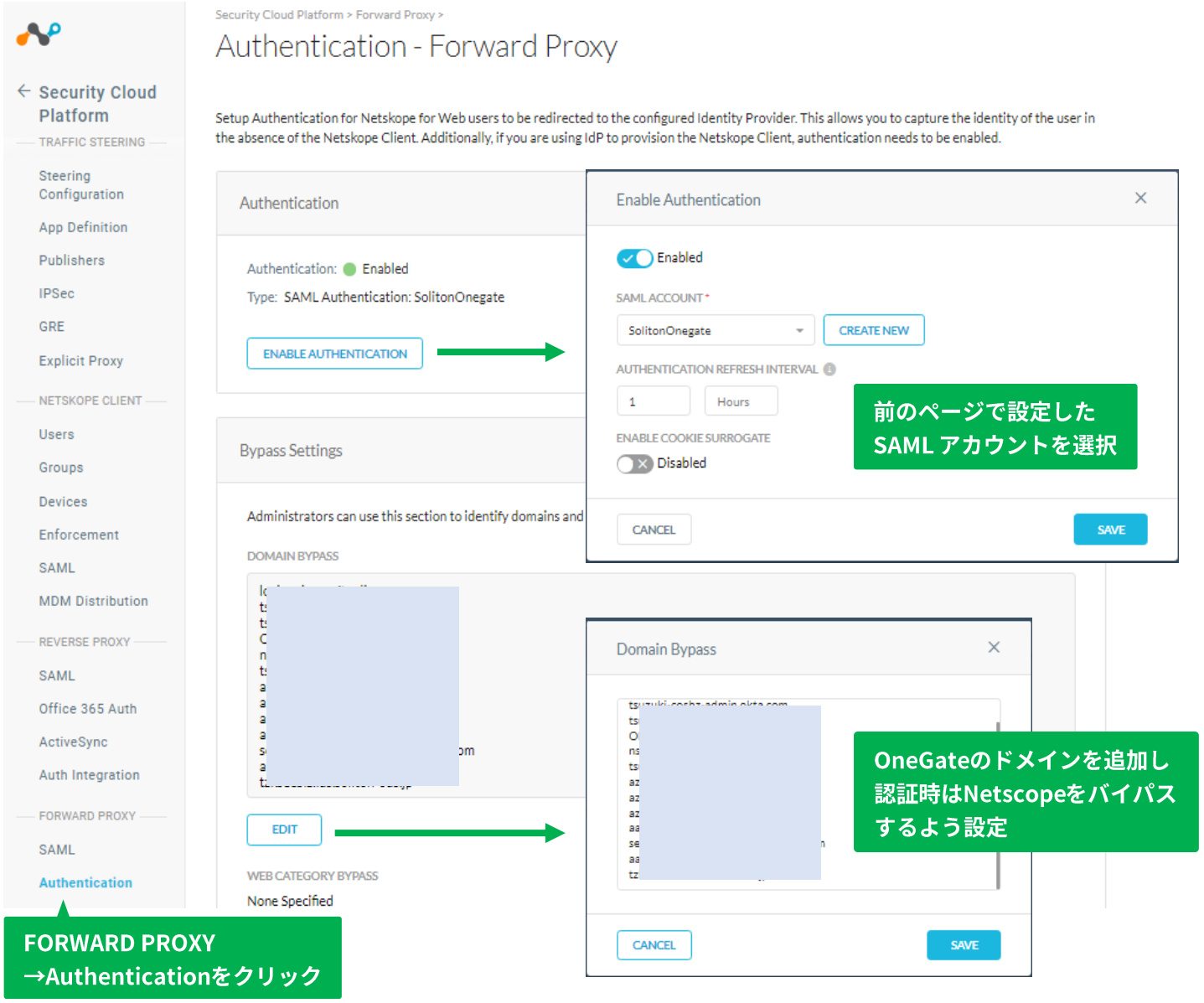
Netscope のSAML設定画面 - 1

Netscope

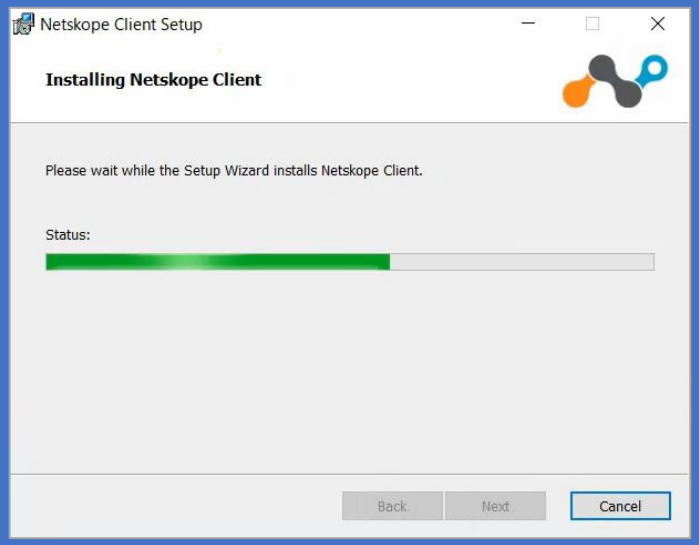


Netscope のSAML設定画面 - 2

Netscope



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

Soliton OneGate

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

2022年 1月

SOGWP-PKIS-02