Soliton
OneGate

MFA実装の最適解

企業の重要データを守る
多要素認証サービス

テレワーク時代のゼロトラスト、鍵は「認証」

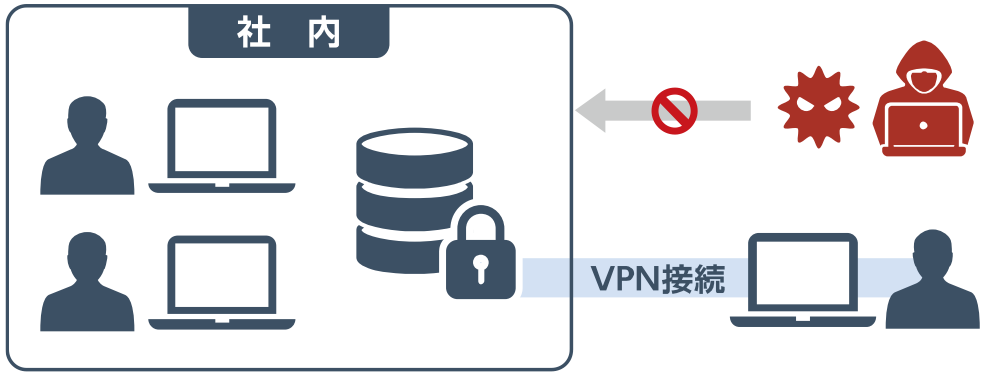
業務アプリケーションへの不正ログイン被害が急増

近年、クラウドサービスを始めとする業務アプリケーションへの不正ログイン被害が急増しています。

会社という箱の中にいれば　“正しいユーザー”であるという境界防御の前提がなくなる中、テレワーク時代の「認証」は従来とは考え方を変える必要があります。

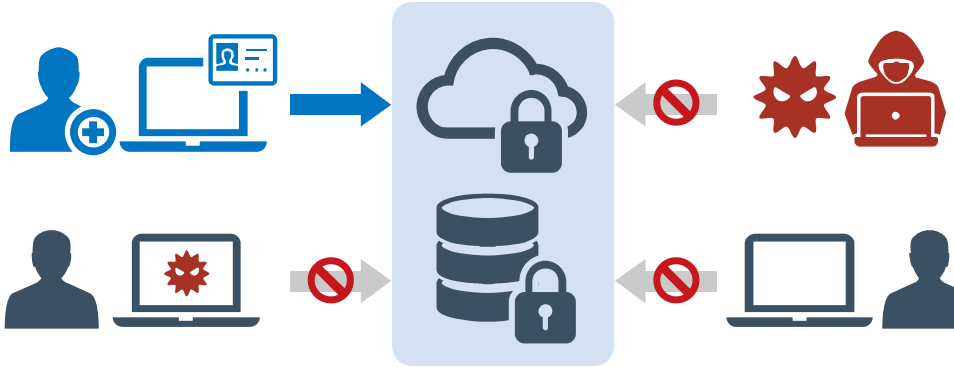
境界防御

「会社という箱の中にいれば、正しいユーザー」



ゼロトラスト

「情報資産は、信頼できるユーザーとデバイスが利用」



“パスワード漏えい”というセキュリティリスク

99% 以上の企業・団体で、社員のパスワード漏えいが発覚

ソリトンシステムズがこれまでに行った「漏えいアカウント被害調査」のうち、全体の 99.9%（ドメインベース）の企業・団体で、現職職員のパスワードを含むアカウント情報の漏えいが確認されました。
しかし、ほとんどの企業・団体は、自社職員のアカウント情報がインターネット上に漏えいしている事実に気付いておらず、調査によって初めて漏えいの被害が明らかになりました。

調査数 2500ドメイン以上

民間企業・政府機関・学術機関など
ソリトン「漏洩アカウント被害調査サービス」調べ

※パスワード攻撃のうち、漏えいしたアカウント情報を用いるものは、「クレデンシャルスタッフィング攻撃」（別名：「パスワードリスト攻撃」）と呼ばれ、近年被害が広がっています。

急増するフィッシング詐欺

簡易的なMFAを突破する フィッシング攻撃が増加

スマホ認証アプリ（Authenticatorアプリ）を利用する簡易的なMFAは、導入しやすさから広く利用されていますが、昨今、この弱点を突いたフィッシング攻撃（AiTM※）の被害がクレデンシャルスタッフィング攻撃とともに増加しています。

また、スマホ認証アプリは利用者本人の確認手段であり、**日本の企業・組織でニーズが非常に高い「利用端末の特定」に対応できない** 点にも注意が必要です。

※ Adversary-in-The-Middle

クレデンシャルスタッフィング攻撃

サイバー空間に漏えいしているパスワードを利用

フィッシング攻撃

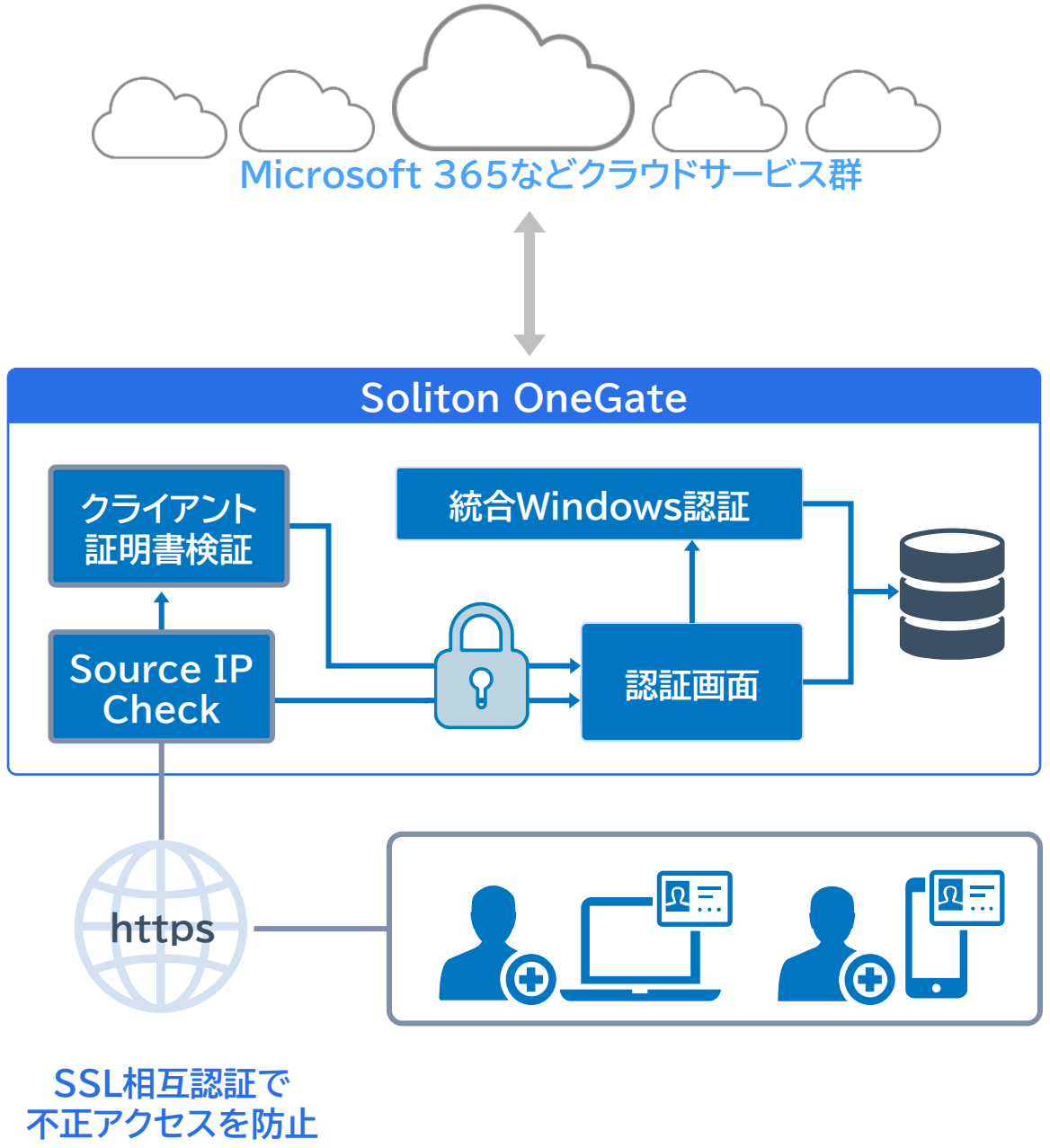
偽サイトに誘導し認証cookie等を不正入手

PKI の優位性とは

MFAの中でも優位性の高い「デジタル証明書」

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窃取や多要素認証突破攻撃を防止できるメリットがあります。

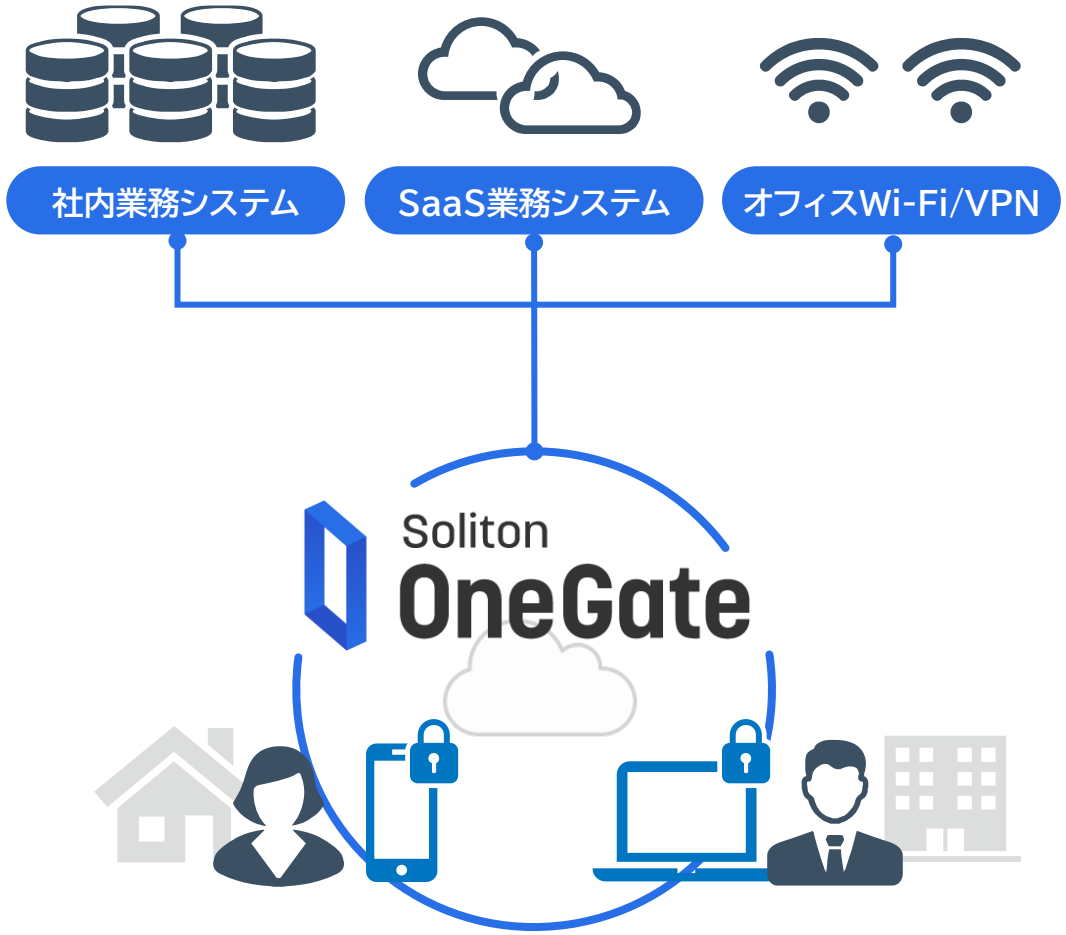
証明書を利用してクライアントとサーバーを相互認証するこの方式は、暗号化通信を確立する際にクライアント証明書をチェックすることとなり、正規の証明書でなければ通信が確立されません。他の認証手法とは異なり、正規の証明書を持たない攻撃者はログイン画面にたどり着けず、パスワードリスト攻撃対策になるだけでなく、脆弱性攻撃の成立も困難なものとします。



日本企業のニーズに対応する認証サービス

生産性向上に欠かせない業務アプリ。ID・パスワードだけで大丈夫ですか？

企業の大切な情報を管理する業務システムを、IDとパスワードだけで利用していたら、第三者にとって、乗っ取りは簡単です。また、会社が許可していない端末が繋がってしまう環境では、情報漏えいリスクは大きく高まります。OneGateは、パスワードの脆弱性を解決するデジタル証明書で、利用者と利用端末を特定し、企業の情報を不正アクセスから守ります。



Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等による MFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

4 Wi-Fi／VPNを堅牢にする

デジタル証明書によるネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

5 持ち出さない データ保護

重要システムはセキュアブラウザのみアクセスを許可
ブラウザ外への持ち出しをブロックするデータ保護を実現

Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等による MFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

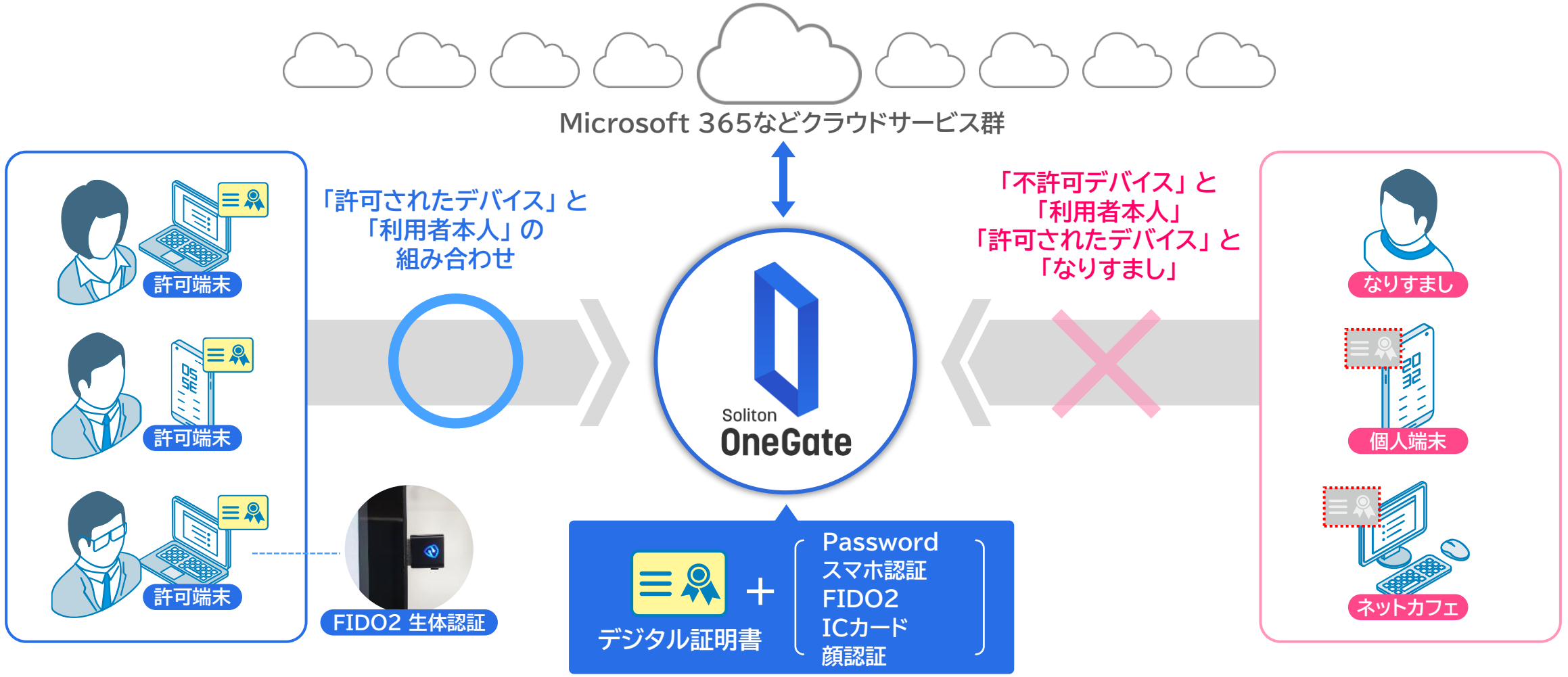
4 Wi-Fi／VPNを堅牢にする

デジタル証明書によるネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

5 持ち出さない データ保護

重要システムはセキュアブラウザのみアクセスを許可
ブラウザ外への持ち出しをブロックするデータ保護を実現

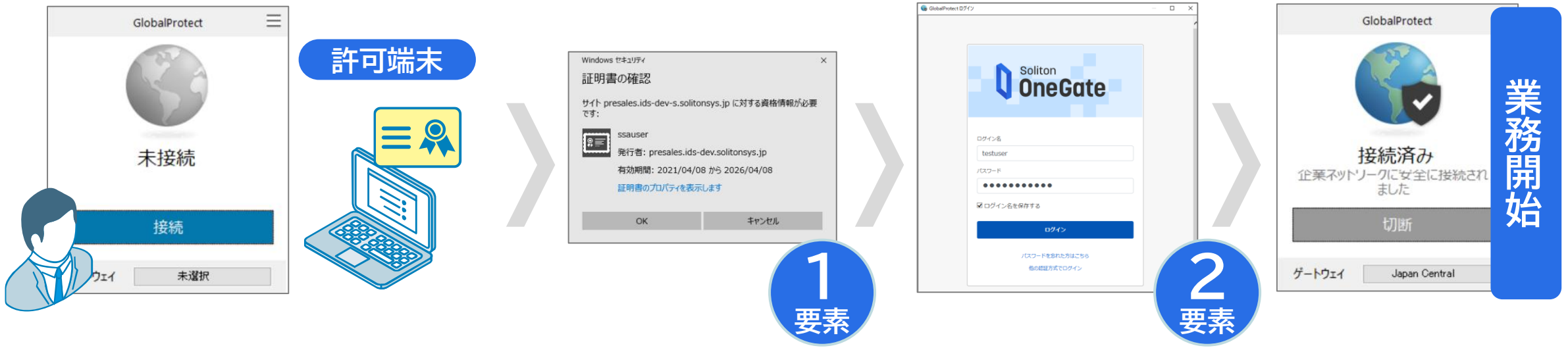
SASEやM365などクラウドサービスを、まとめてMFA



Tips

クラウドサービスへのアクセス制御には、インターネット標準の認証連携技術である「SAML」を利用します。SAML を利用することで、利用者の認証情報を ID認証サービス（OneGate）で一元管理することが可能となります。

利用者の認証の流れ - Prisma Access GlobalProtect の例(※)



Soliton OneGateログオン画面にアクセスできない

※Palo Alto Networks社 Prisma Accessのエージェント Global Protectにて、SAML認証連携した例です。

メニューに登録されていない任意のクラウドサービスも登録が可能です

連携先クラウドサービスにあわせて登録します

Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等による MFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

4 Wi-Fi／VPNを堅牢にする

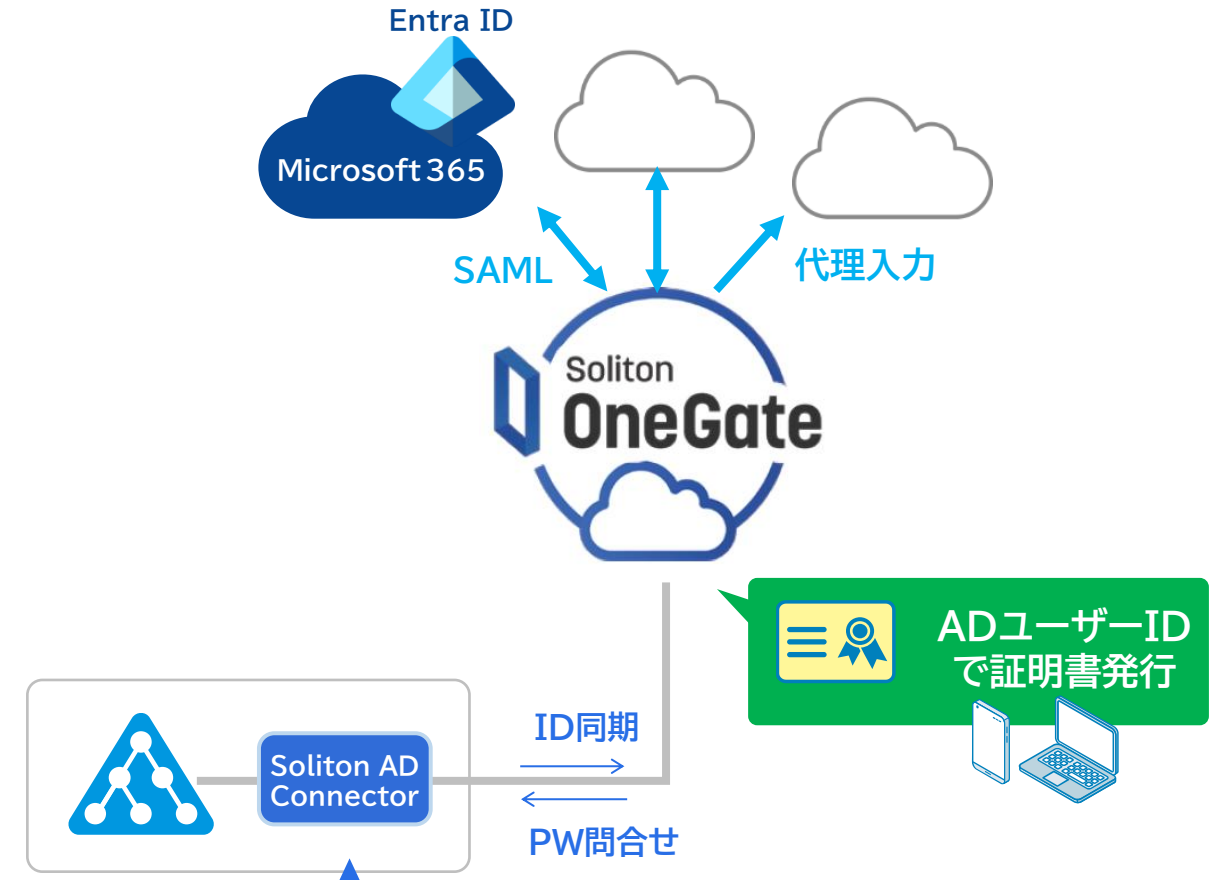
デジタル証明書によるネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

5 持ち出さないデータ保護

重要システムはセキュアブラウザのみアクセスを許可
ブラウザ外への持ち出しをブロックするデータ保護を実現

パスワード同期不要のAD/Entra ID連携方式

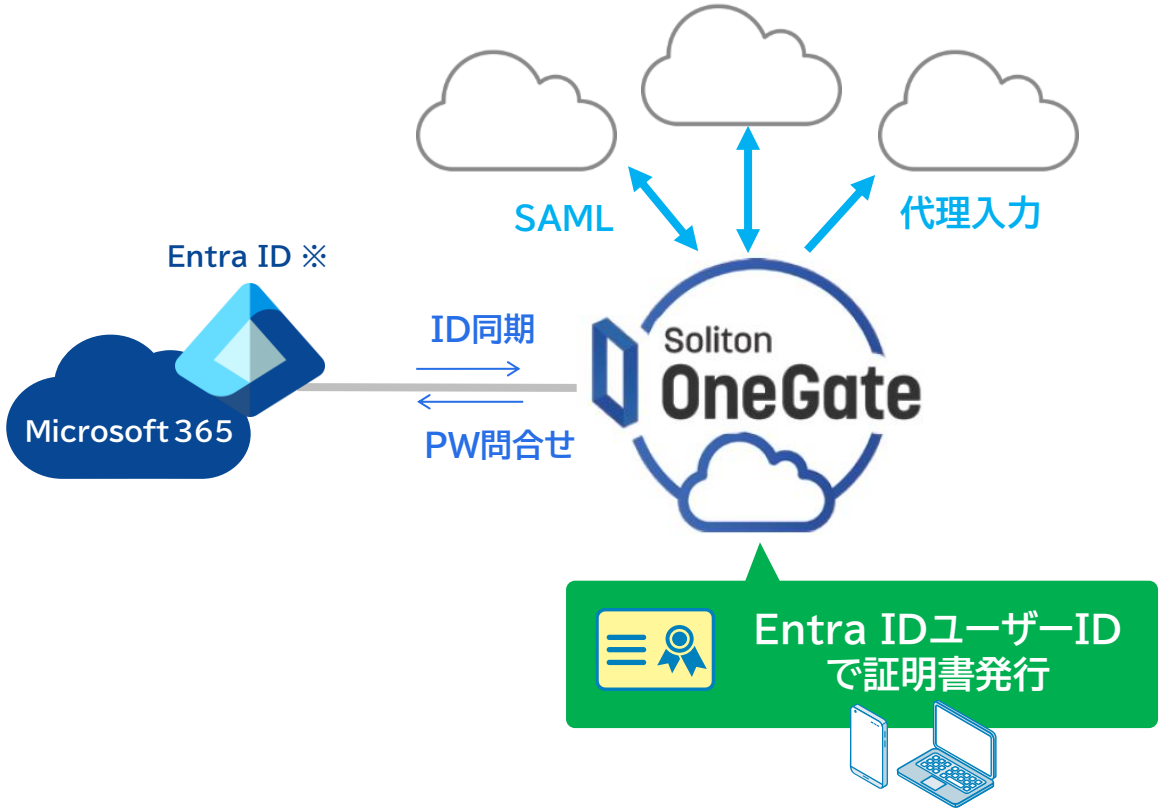
社内のADと連携



専用コネクターが、社内ADとOneGateとの通信セッションを確立。社内のファイアウォールに外部からの通信を許可する穴を開ける必要はありません

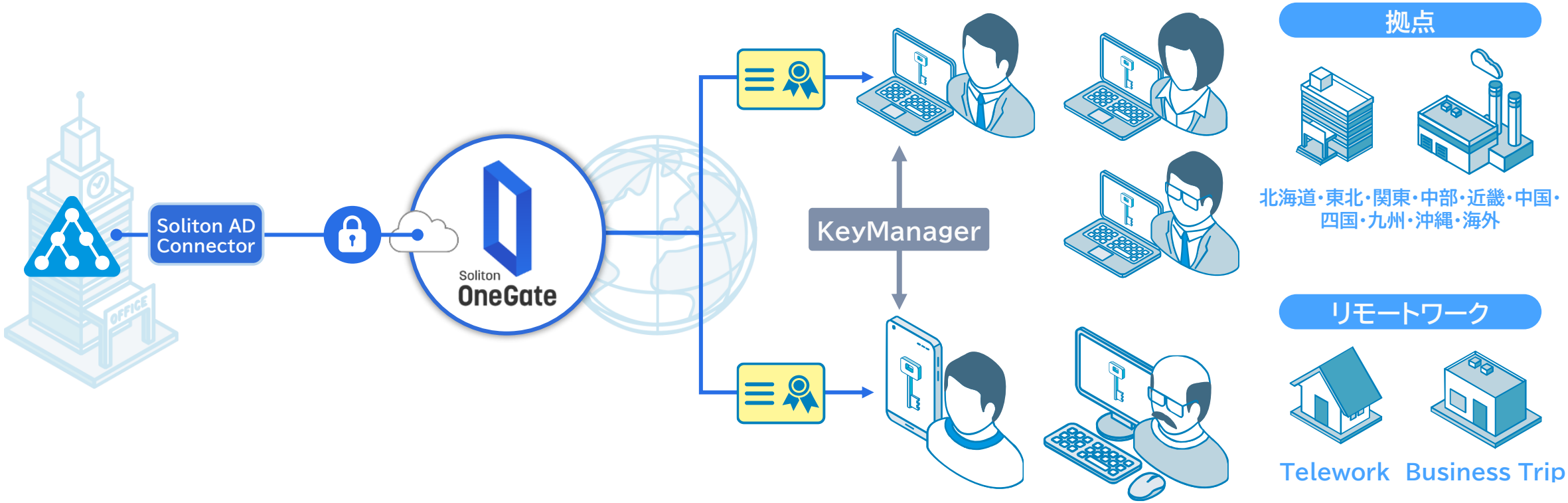
Entra ID(旧Azure AD)と連携

SAML SSO
代理入力SSO



※ ユーザー源泉のMicrosoft Entra IDと、フェデレーション先のMicrosoft Entra IDを同一ドメイン(FQDN)にする場合には注意事項があります。詳細はお問い合わせください。

AD/Entra IDアカウントで、デジタル証明書が配布できる



マルチOS対応

全OS同じ手順で
デジタル証明書を取得

利用者も管理者も低負担

ブラウザの設定やActiveXは不要
ヘルプデスク工数ほぼゼロ

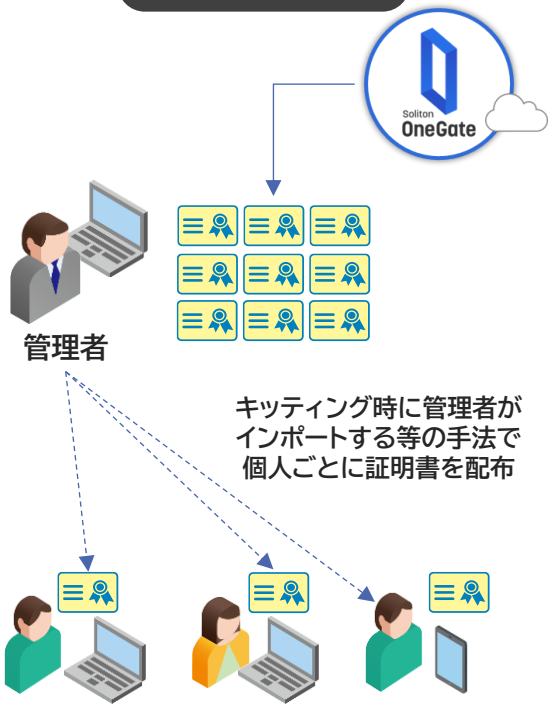
不正コピーが一切できない

不正接続を許さない仕組みで
リモートワークを促進

Soliton OneGateで利用可能な証明書発行方式

PKCS#12ファイル

専用アプリ不要



- 証明書を発行する利用者のログイン名とパスフレーズを記載したCSVファイルを利用して一括発行することも可能

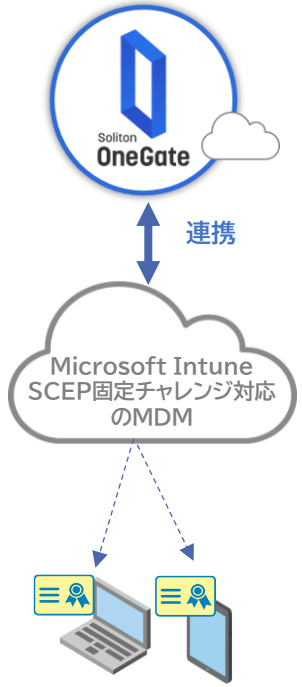
ソリトン独自方式
（招待コード利用の「ワンタッチ証明書配布」）

不正コピー制御　遠隔&いつでも取得

- 招待コード発行回数、有効期限の設定（1回のみの発行に限定可能）
- 端末にインストールした電子証明書は取り出し不可
- Windows端末の参加ドメイン名を限定した証明書配布
- ワンタッチ証明書配布をOffとし、招待コードを手動入力させることも可能

MDM連携
（Intune/SCEP固定チャレンジ）

デバイス限定　不正コピー制御



- SCEP固定チャレンジを利用したMDMでの証明書配布では、証明書取得の有効期限、許可するIPアドレス範囲が指定可能
- Google Workspaceと連携しChromebookに証明書配布も可能です

※P12ファイルをMDMで配布するなどの方法もありますが、ここでは省略しています。

手間なく安全なデジタル証明書の配布・運用

Soliton KeyManager

Soliton OneGateやNetAttest EPS/EPS-apとともに利用する
クライアントでのデジタル証明書導入・運用アプリ。
Windows、iOS/iPadOS、Android、macOS、Chromebookに対応。

- ユーザー操作を最小限にするワンタッチ証明書配布
- MDMで管理していない、**協力会社・取引先の端末・ユーザーにも手間なく安全にデジタル証明書を配布**する仕組み
- 証明書が外部に漏れないプロトコルSCEPでのセキュアな配布
- 無理のない証明書更新の運用を支援する機能
- クライアント証明書配布時に、SASE/VPNで必要となる**外部証明書やプロファイルなどをまとめて配布可能**
  - 外部CA証明書（SSL-VPNやSASEで必要となる場合に。Windows、iOS/iPadOS向け。）
  - VPNプロファイル（iOS/iPadOS向け）
  - Wi-Fiプロファイル（Windows、iOS/iPadOS向け）

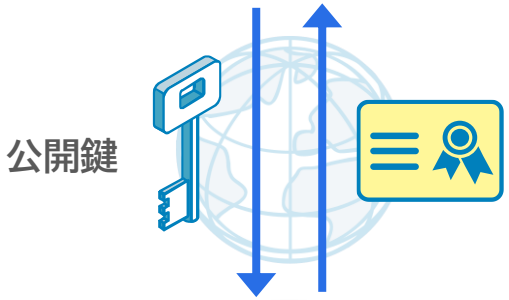
うら側の、証明書発行自動化の仕組み

1. 公開鍵と秘密鍵の鍵ペアを生成
（秘密鍵はエクスポート禁止状態で生成）

2. 鍵ペアの公開鍵だけを送付、
デジタル証明書の発行を申請

3. デジタル証明書の発行
（認証局の秘密鍵で暗号化）

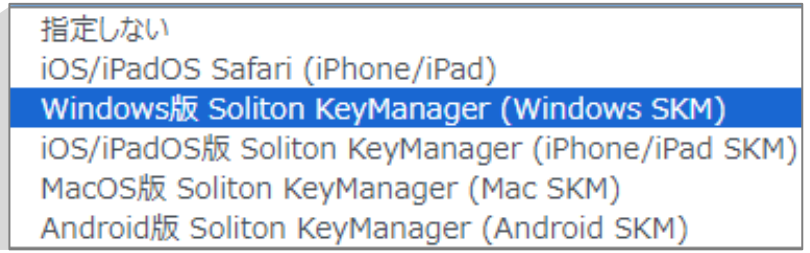
4. デジタル証明書のインストール



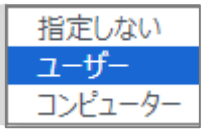
ユーザー認証に加え、

招待コード、OS、ドメイン名、
デバイス名を確認

証明書管理画面 – 招待設定詳細



発行先OSの指定



証明書格納先の指定（入れ間違い防止）

証明書取得時のパスワード入力スキップも可能※

証明書取得を組織のドメイン管理下端末に限定

外部CA証明書をまとめて配布
（SASEのSSL復号化用CA証明書など）

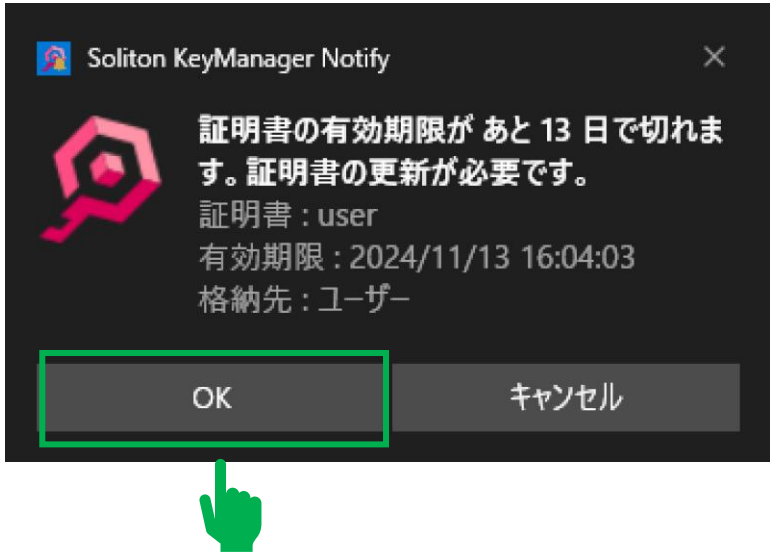
利用者に発行する証明書発行・メール通知をカスタマイズでき、組織に最適な証明書配布ができます。

※「パスワードレス」をチェックすると、URL/QRコードでの証明書発行時に利用者パスワード入力をスキップできますが、セキュリティレベルが下がりますのでご注意ください。

証明書更新のユーザーへの通知

①期限切れ通知メール

②アプリの通知機能



メール・アプリによる証明書更新通知から、簡単に更新が可能です

Soliton OneGate

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 | ☰ demoadmin

端末紛失時は
ユーザー名で検索

証明書管理 > 証明書一覧

操作 | CRL更新反映(即時) | エクスポート

☐ 失効・期限切れを含む　すべて　maruyama

- 再発行許可
- 再発行拒否
- 失効

紛失デバイスだけ

開始日時(降順)

前へ | 1 - 6 / 6 | 25 , 50 , 100 | 次へ

☐			シリアル番号: 789680a8271883ab42028b1f235665d3 発行元: demo-2nd 発行先詳細: 私物端末(iPhone) 開始日時: 2023/10/24 11:09:43 終了日時: 2028/10/24 11:09:43
☐	利用者 有効	丸山 修平 maruyama CN=maruyama	シリアル番号: 0d3ee0b4abaff5b72e7b7fdd62e0532c 発行元: demo-2nd 発行先詳細: 私物端末(windows) 開始日時: 2023/10/23 21:08:19 終了日時: 2028/10/23 21:08:19
☐	利用者(招待) 有効 再発行可	丸山 修平 maruyama CN=maruyama	シリアル番号: 7bc9930d193fd7696312b7629b5653da 発行元: demo-2nd 発行先詳細: Android SKM (sdk_gphone64_x86_64) 開始日時: 2023/10/19 17:38:56 終了日時: 2028/10/19 17:38:56
☐	利用者(招待) 有効 再発行可	丸山 修平 maruyama CN=maruyama	シリアル番号: 1cc839057a4101a4bffd68b1aa5b2e80 発行元: demo-2nd 発行先詳細: Mac SKM (s18149) 開始日時: 2023/10/19 17:35:10 終了日時: 2028/10/19 17:35:10
☐	利用者(招待) 有効 再発行可	丸山 修平 maruyama CN=maruyama	シリアル番号: 047c46617a334d50d65cecfcd3ef1d38 発行元: demo-2nd 発行先詳細: Windows SKM (DESKTOP-TM9V1UA) 開始日時: 2023/10/19 17:27:29 終了日時: 2028/10/19 17:27:29
☑	利用者(招待) 有効 再発行可	丸山 修平 maruyama CN=maruyama	シリアル番号: 2ef381c89f17b347dba8b5d40848e4ff 発行元: demo-2nd 発行先詳細: iPhone SKM (iPhone) 開始日時: 2023/10/19 17:25:00 終了日時: 2028/10/19 17:25:00

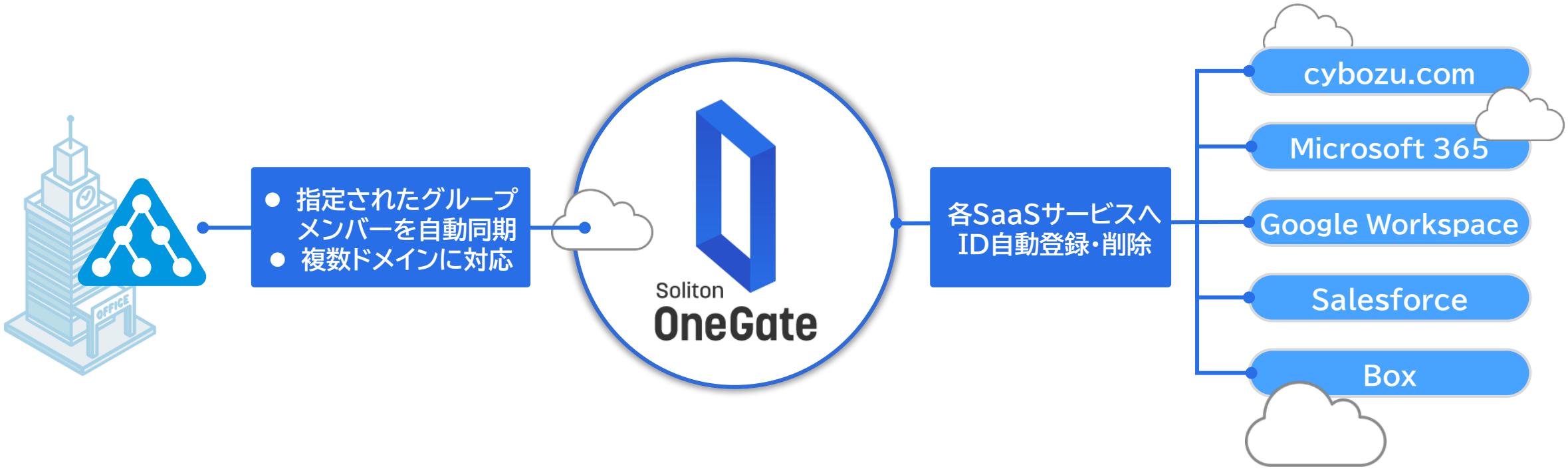
PKCS#12形式では
管理者が任意設定

端末種別を確認可能

端末情報はOneGateが自動記録。証明書の発行から失効までのかんたん運用を支援します。

※発行先詳細はOneGateが自動的にOS判別して記録します。PKCS#12ファイルでの発行時は、管理者で任意指定(例：私物端末(windows))も可能です。

主要なクラウドアプリは、社内ADとIDを自動同期



不要なアカウントがクラウドに残らない

Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等による MFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応
PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

4 Wi-Fi／VPNを堅牢にする

デジタル証明書によるネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

5 持ち出さないデータ保護

重要システムはセキュアブラウザのみアクセスを許可
ブラウザ外への持ち出しをブロックする
データ保護を実現

セキュリティ VS 業務効率 の課題

DXが進む組織ほど
パスワード管理は急務！

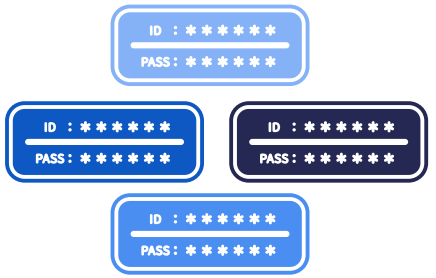
デジタル化やDX、クラウド利用などによって、業務効率化を進める組織ほど、利用するシステムが増え、パスワード管理が課題となっています。

攻撃者は、パスワードの使い回しや、ブラウザに保存されたパスワード情報を狙い、攻撃の突破口として悪用する事例が増えています。

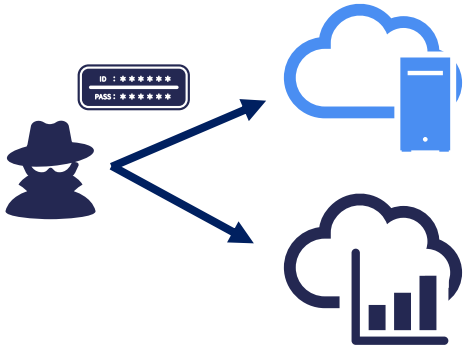
またインターネットに公開されているクラウドサービスは特に攻撃対象となりやすく、脆弱なパスワードを利用することは高いリスクとなります。

DX推進で
利用システムが急増

**パスワードの使い回しや
ブラウザへの保存が増加**



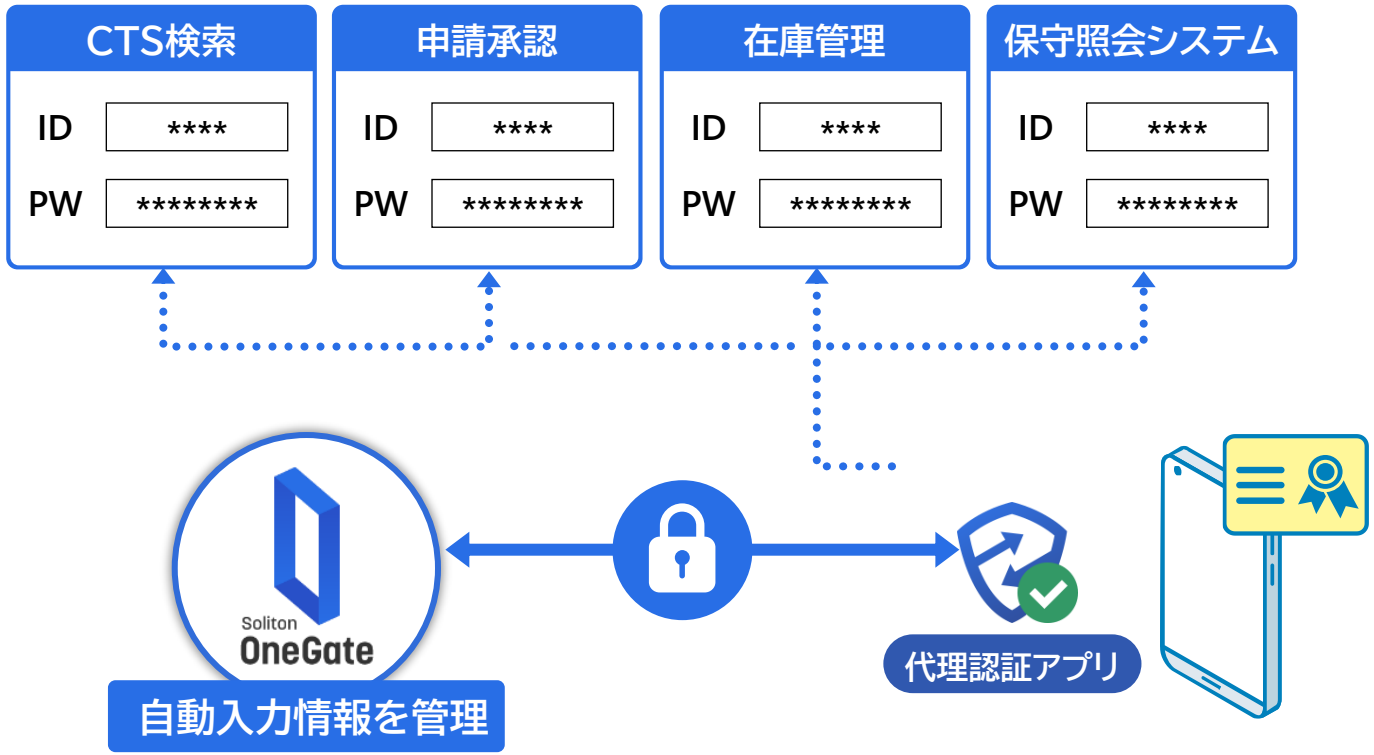
誰でもアクセスできる
クラウドシステムは
攻撃対象になりやすい
（弱いパスワードは危険）



既存システムも、パスワード入力から解放する - 実績豊富の代行入力サインオン

Soliton PasswordManager

- SmartOnなどエンドポイント製品で実績のある、エージェント型SSOがスマホにも対応
- 利用者覚えなくても良いので、パスワードは限界まで複雑化可能
- 認証後、クライアントで一時保管するSSOデータは暗号保存
- Agentタイプで、ネイティブアプリにも対応
- Windows、iOS、Androidに対応



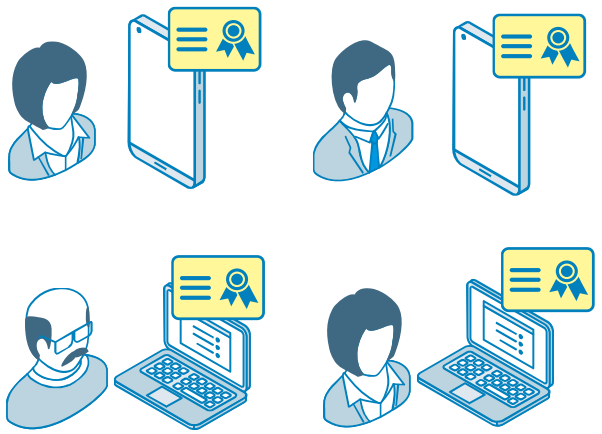
ネイティブアプリへの証明書認証＋代行入力サインオンは、ソリトンだけの独自方式

SAML非対応システムでもパスワードレスを実現

管理者が各業務システムへのログイン情報
（IDとランダム化したパスワード）を登録

デジタル証明書＋
ADパスワード認証

業務アプリのパスワードは知らない



代理認証アプリ

SSO

ログイン情報を
代行送出

ID
ランダム
パスワード

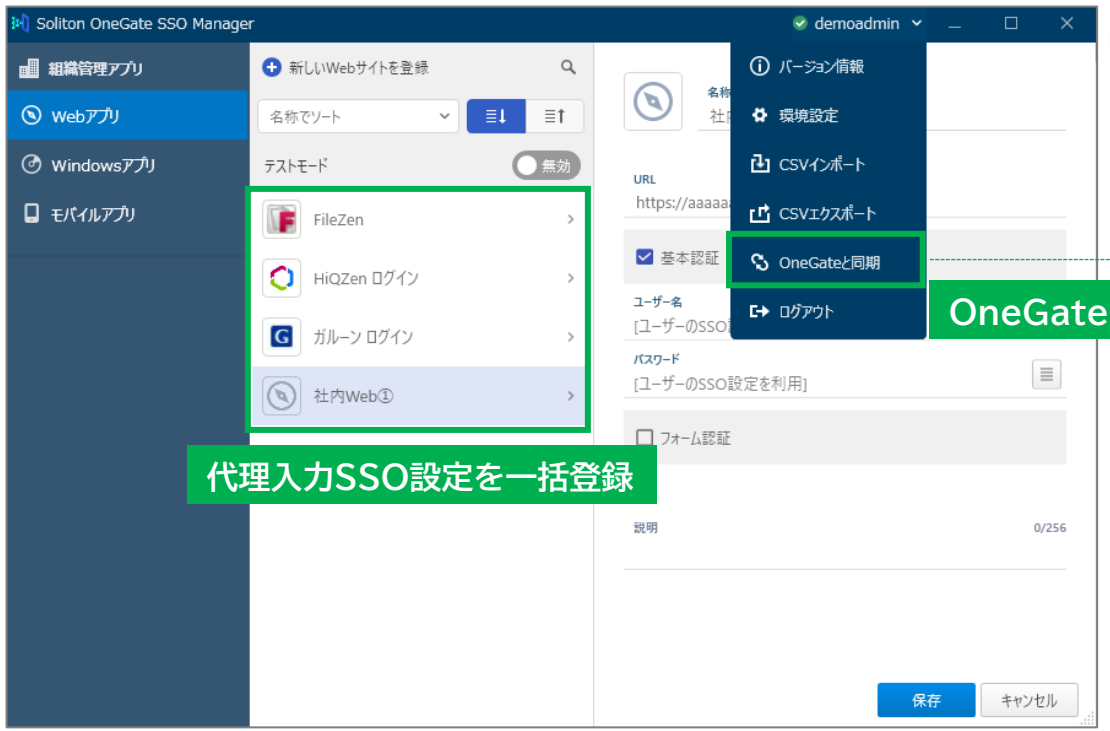
パスワード漏洩リスクを低減

パスワードを利用者に知らせない運用が可能

管理者も利用者も、SSO設定が可能

- 管理者が代理入力設定を行う場合

代理入力情報を管理



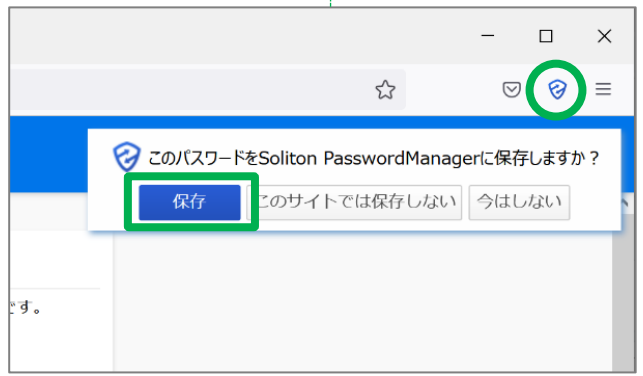
代理入力SSO設定を一括登録

OneGateと同期

専用ツールで全ユーザーのSSO設定を一括登録

- 利用者が代理入力設定を行う場合

認証情報を入力してログイン



入力した認証情報はOneGateへ保存

ブラウザの拡張機能で自動保存

Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等による MFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

4 Wi-Fi／VPNを堅牢にする

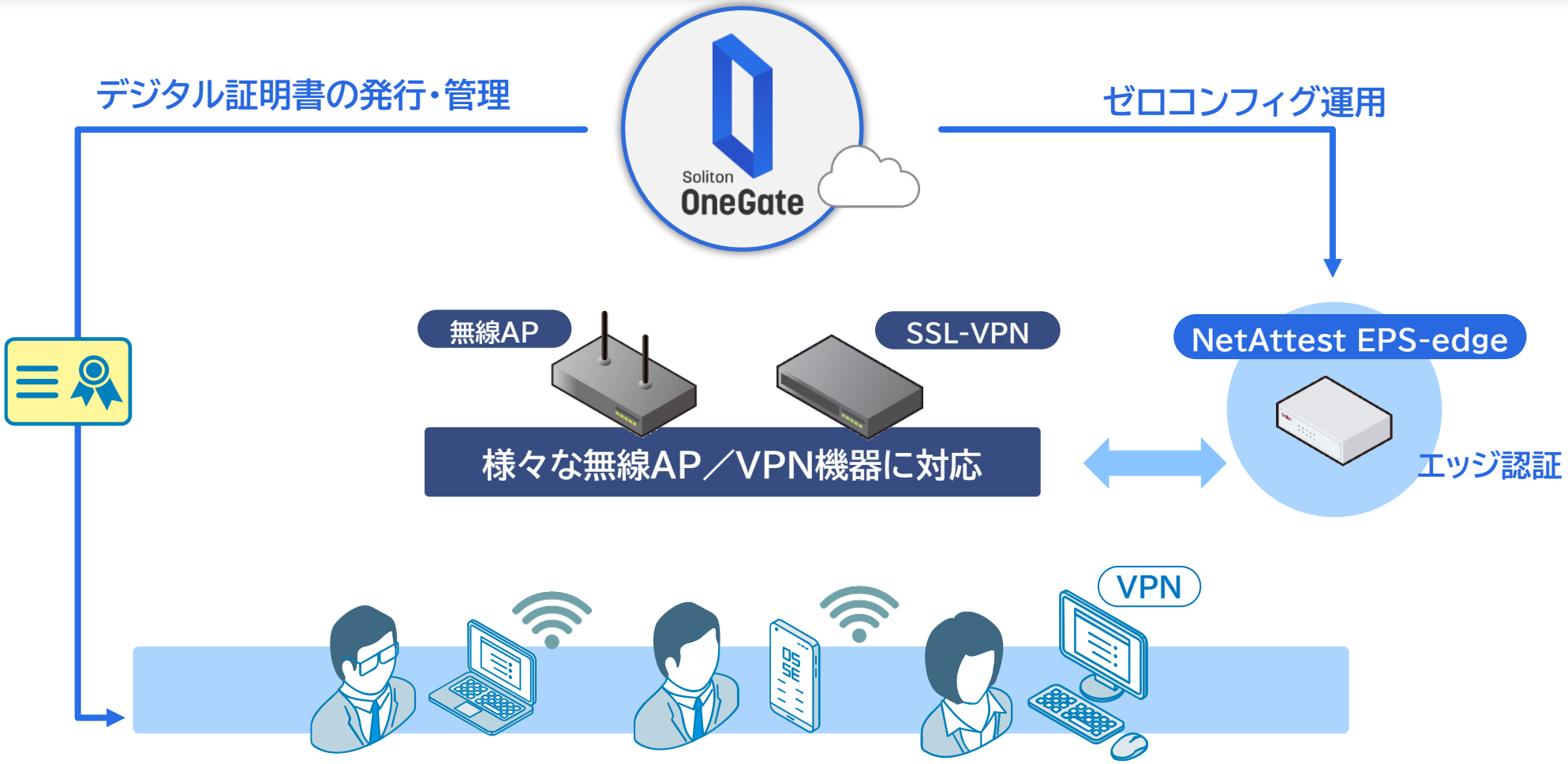
デジタル証明書による
ネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

5 持ち出さないデータ保護

重要システムはセキュアブラウザのみアクセスを許可
ブラウザ外への持ち出しをブロックする
データ保護を実現

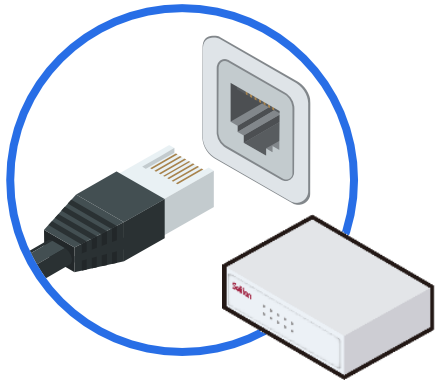
社内ネットワークを不正侵入から守る、Wi-Fi／VPN認証オプション

OneGateは、企業の無線LANやVPN環境を不正侵入から守る、Wi-Fi／VPN認証サービス 機能を提供します。
安全性と運用性の両面で優れるデジタル証明書を用いた認証で、悪意あるユーザー・不適切な端末の進入を防ぎます。



ゼロコンフィグだから、これだけ

1 ネットワークケーブルを接続



NetAttest EPS-edge

電源を入れるとクラウドに接続
（DHCPでIPアドレスを取得して、自動接続）

2 クラウド管理画面で、アプライアンス登録

本体シールの登録コードを入力、
あとは自動でアクティベート

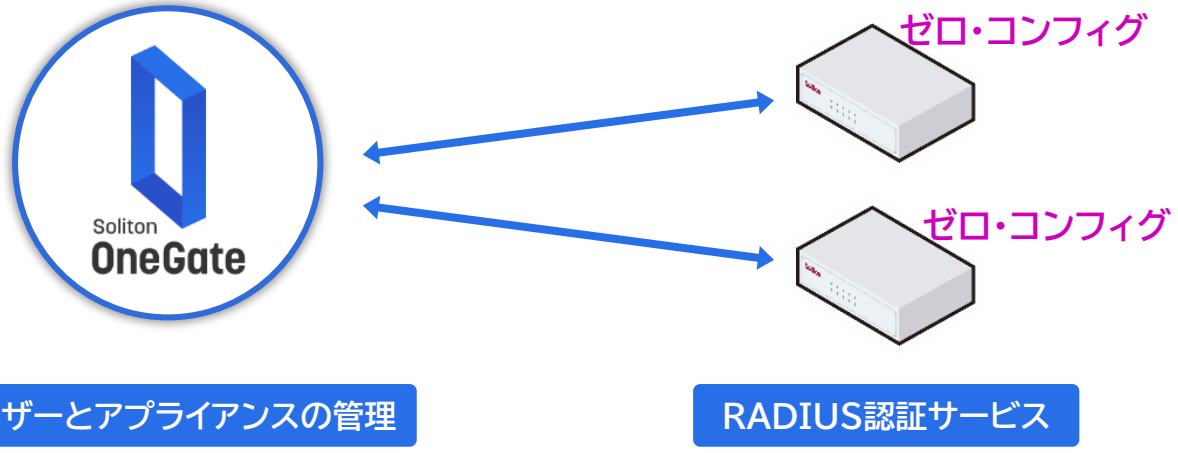
Wi-Fi／VPN認証オプションについて

RADIUSサーバー機能

- 無線LAN認証（EAP-TLS）、VPN認証（PAP）
- RADIUSサーバーは、複数台設置する事で負荷分散、障害対策などに柔軟に対応
  （RADIUSクライアント側で複数のRADIUSサーバーを指定）
- RADIUSクライアント数の制限はありません

クラウド上の管理機能

- ユーザー情報の一元管理（社内AD、Microsoft Entra ID同期）
- EPS-edgeアプライアンスの管理
  - オンライン・アクティベーション
  - ステータス確認
  - ログ管理
  - ファームウェアアップデート

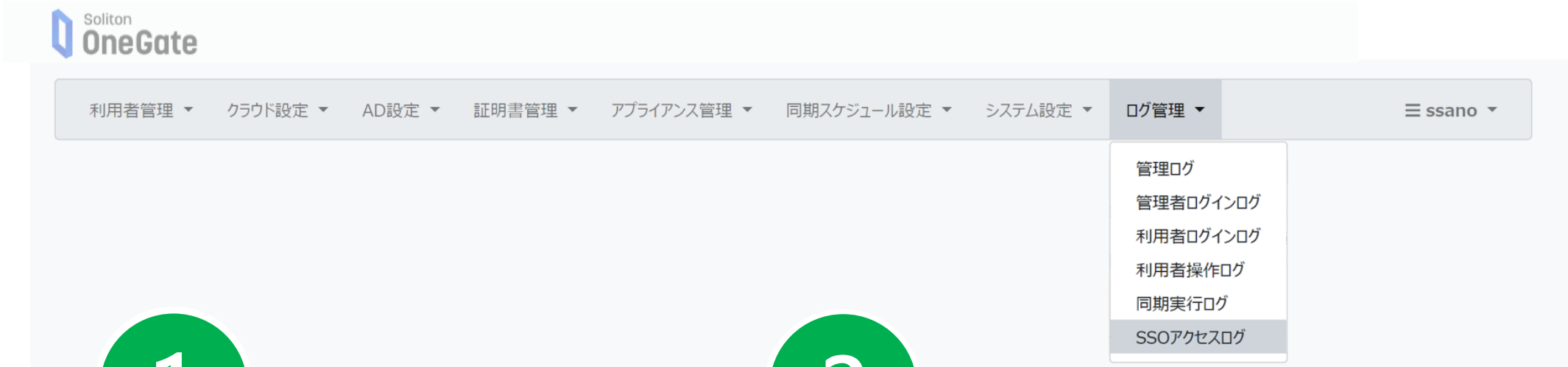


他社サービスとの違い

	海外サービス A	国内サービス B	Soliton OneGate
SAML対応アプリの シングルサインオン	●	●	●
SAML非対応アプリの シングルサインオン	○	×	● ネイティブアプリにも対応できる
Wi-Fi／VPN認証	▲ ID・パスワード認証のみサポート	×	● 証明書認証をサポート
デジタル証明書の 安全発行	× P12ファイルをダウンロード	○ 秘密鍵は利用端末外で生成	● 秘密鍵は利用端末内で生成
デジタル証明書の 運用工数（※）	×	▲ 事前に端末情報の登録が必要	● 別組織の端末にも安全・簡単に配布

※組織を超えてデータ共有するDX案件では、組織のMDMで管理できない協力会社の端末に対する、安全・簡単な証明書配布が求められます。

監査への対応 ・・・＞ 詳細なログを残す

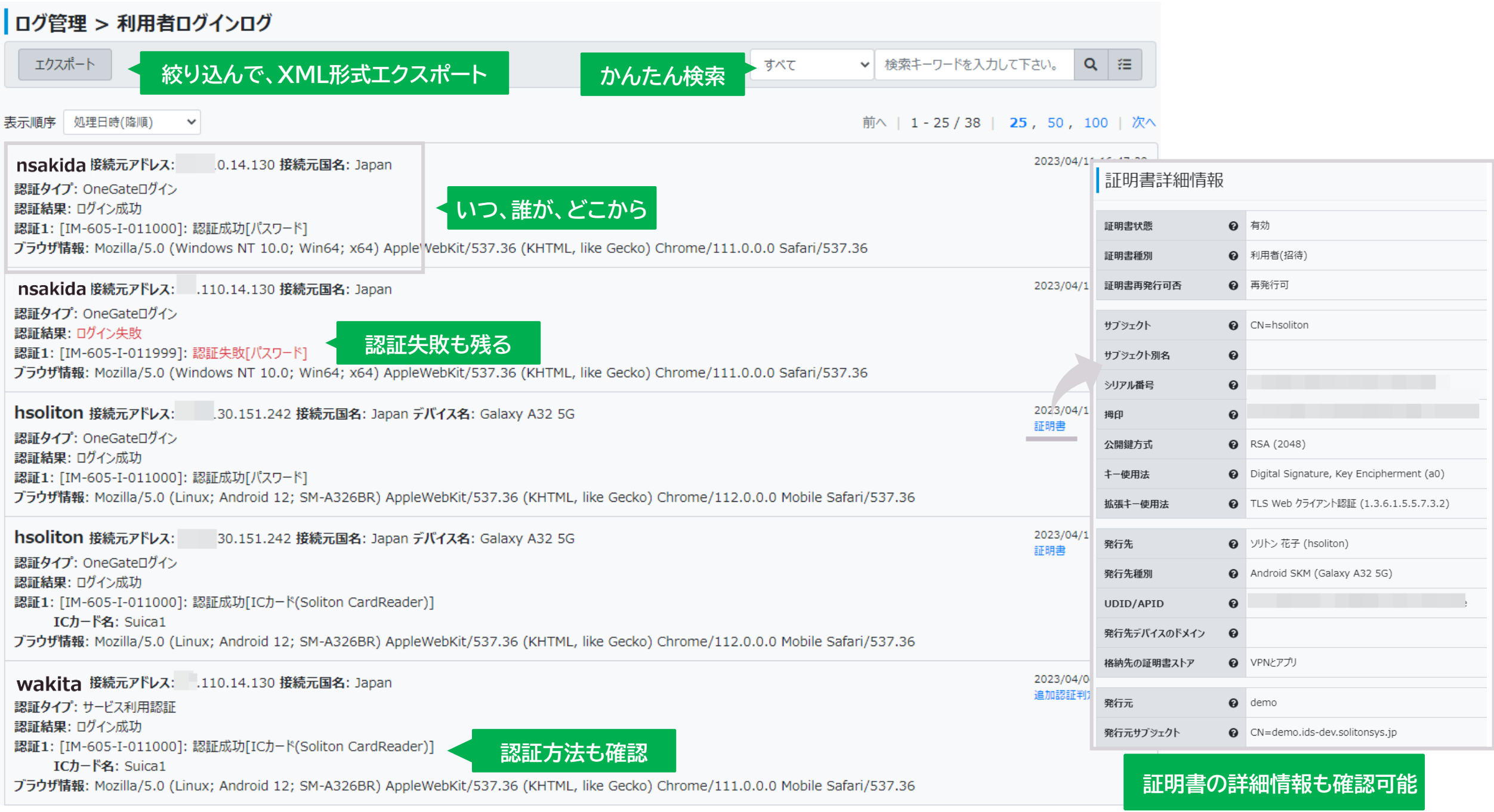


1 特権利用ログ

- 管理ログ
  - ✓ いつ、誰が、どのブラウザ/接続元IPから どのような 管理者権限操作をしたか
- 管理者ログインログ
  - ✓ いつ、誰が、どのブラウザ/接続元IPから

2 利用者ログ

- 利用者ログインログ
  - ✓ いつ、誰が、どこから、どの認証方式で、どのブラウザ/接続元IP/接続元国名から
- SSOアクセスログ
  - ✓ いつ、誰が、どこから、どのサービスに、どのブラウザ/接続元IPから



ログ管理 > SSOアクセスログ

エクスポート

絞り込んで、XML形式エクスポート

かんたん検索

すべて

検索キーワードを入力して下さい。

- すべて
- ログイン名
- 接続元アドレス
- クライアント情報
- ログコード
- 内容
- 処理日時
- 接続先サービス
- サービスアカウント
- 設定名
- URL
- 認証プロトコル

表示順序 処理日時(降順)

1 - 25 / 195 | 25 , 50 , 100 | 次へ

tyamada 接続元アドレス: 114.19.83 2023/10/20 13:13:51

内容: [SP-611-I-001000] アクセス許可
接続先サービス: Google Workspace
サービスアカウント: tyamada@sog-demo.netattest.tech
クライアント情報: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/11 36

詳細ログ

demotaro 接続元アドレス: 110.14.130 2023/10/20 13:09:30

いつ、誰が、どこから
どの SaaS に

内容: [SP-611-I-001000] アクセス許可
接続先サービス: Google Workspace
サービスアカウント: demotaro@sog-demo.netattest.tech
クライアント情報: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36

詳細ログ

demotaro 接続元アドレス: .110.14.130 2023/10/20 13:09:23

内容: [SP-611-I-001000] アクセス許可
接続先サービス: HiQZen
サービスアカウント: demotaro@sog-demo.netattest.tech
クライアント情報: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36

詳細ログ

demotaro 接続元アドレス: 110.14.130 2023/10/20 13:09:11

内容: [SP-611-I-001000] アクセス許可
接続先サービス: Office 365
サービスアカウント: demotaro@sog-demo.netattest.tech
認証プロトコル: SAML
クライアント情報: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36

詳細ログ

Soliton OneGate の特長

1 クラウドをまとめて多要素認証（MFA）

SASE や M365などのクラウドサービスに、デジタル証明書＋FIDO2／スマホ認証／パスワード等によるMFA を適用

2 ID・認証管理の自動化を支援

社内のADやEntra IDと連携し、クラウドID管理を自動化
デジタル証明書の運用を強力に支援

3 社内システムもシングルサインオン

デジタル証明書対応
PC・スマホで動く代理認証アプリでSAML非対応システムもシングルサインオン

4 Wi-Fi／VPNを堅牢にする

デジタル証明書によるネットワーク認証に対応する唯一のIDaaS
Wi-Fi／VPNの認証情報も一元管理

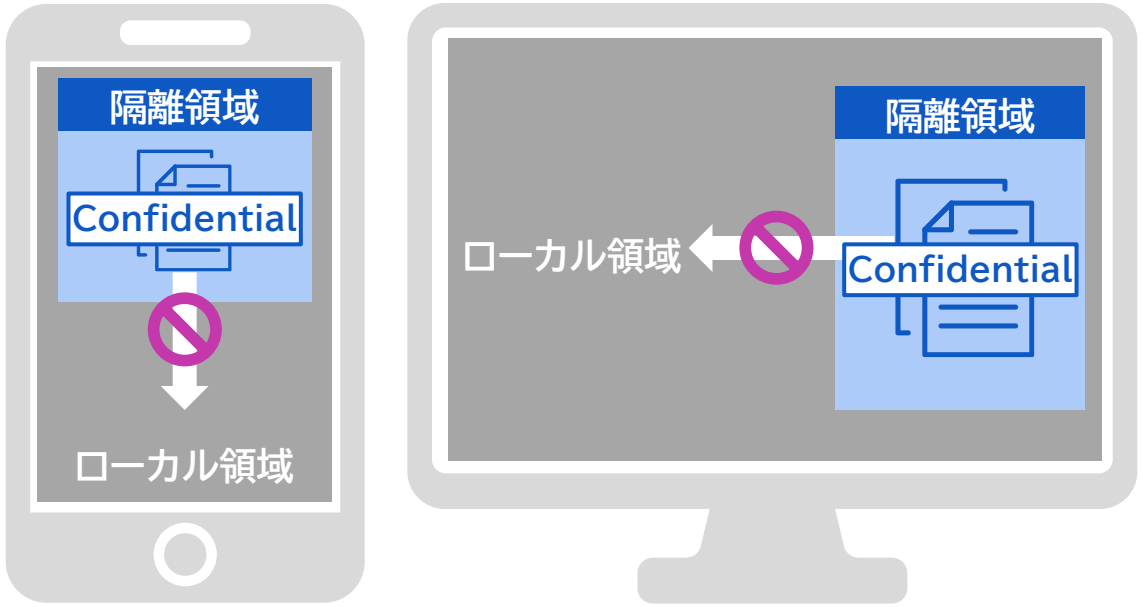
5 持ち出さないデータ保護

重要システムは
セキュアブラウザのみ
アクセスを許可
ブラウザ外への持ち出し
をブロックする
データ保護を実現

セキュアブラウザ

Soliton SecureBrowser

データ持ち出しを禁止するセキュアブラウザによる データ保護ソリューション

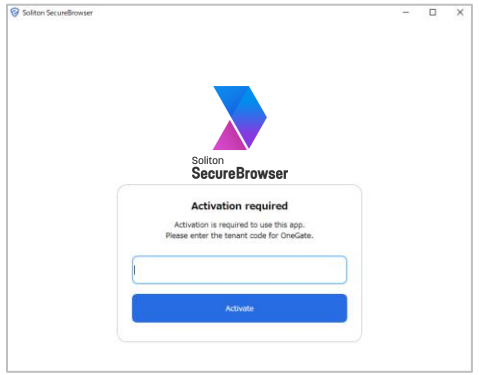


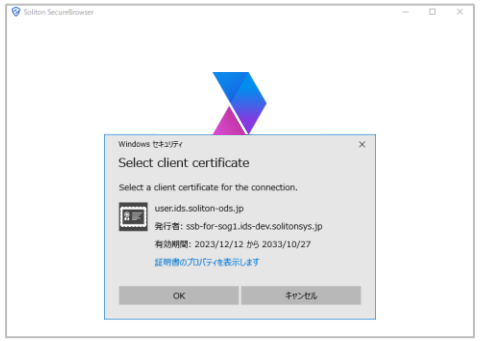
- セキュアブラウザ利用時に証明書認証
- 隔離領域外へのデータ保存禁止
- 隔離領域外へのコピー＆ペースト禁止
- ブラウザ終了時にキャッシュ全削除
- 印刷禁止等の各種制御
- マルチデバイス対応
- 様々なクラウドサービスの閲覧に対応

端末内で仮想的な隔離領域を作り、隔離領域外にデータを持ち出させないことで
情報漏えいを防ぐとともに、端末紛失時の被害を最小限にすることができます

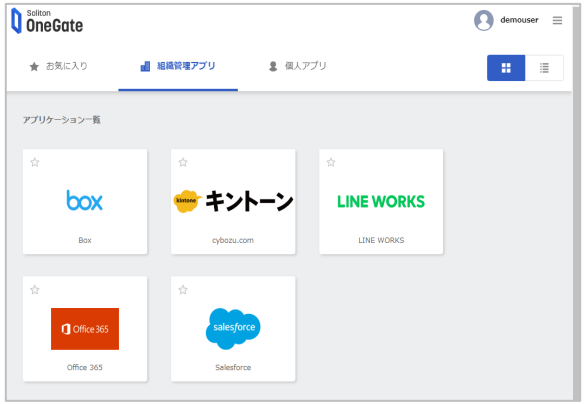
セキュアブラウザの利用イメージ

1 デジタル証明書認証

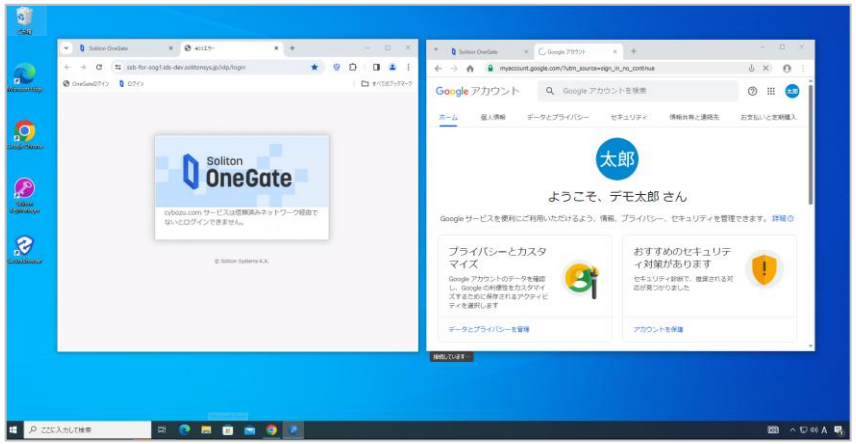




2 OneGateポータル



3 セキュリティレベル高サイトにアクセス



通常ブラウザ

Soliton SecureBrowser

アクセス禁止

アクセス可能

隔離領域外へのデータ持出や
コピー＆ペースト・印刷等を禁止

デモ動画はこちら

セキュアブラウザのユースケース

業種

人材派遣業

要件

- 顧客の個人情報を含む人材データベースの情報の情報漏えい対策をしっかり行いたい
- 人材データベースは、社内外で活用するため、端末紛失時の情報漏えい対策も行いたい

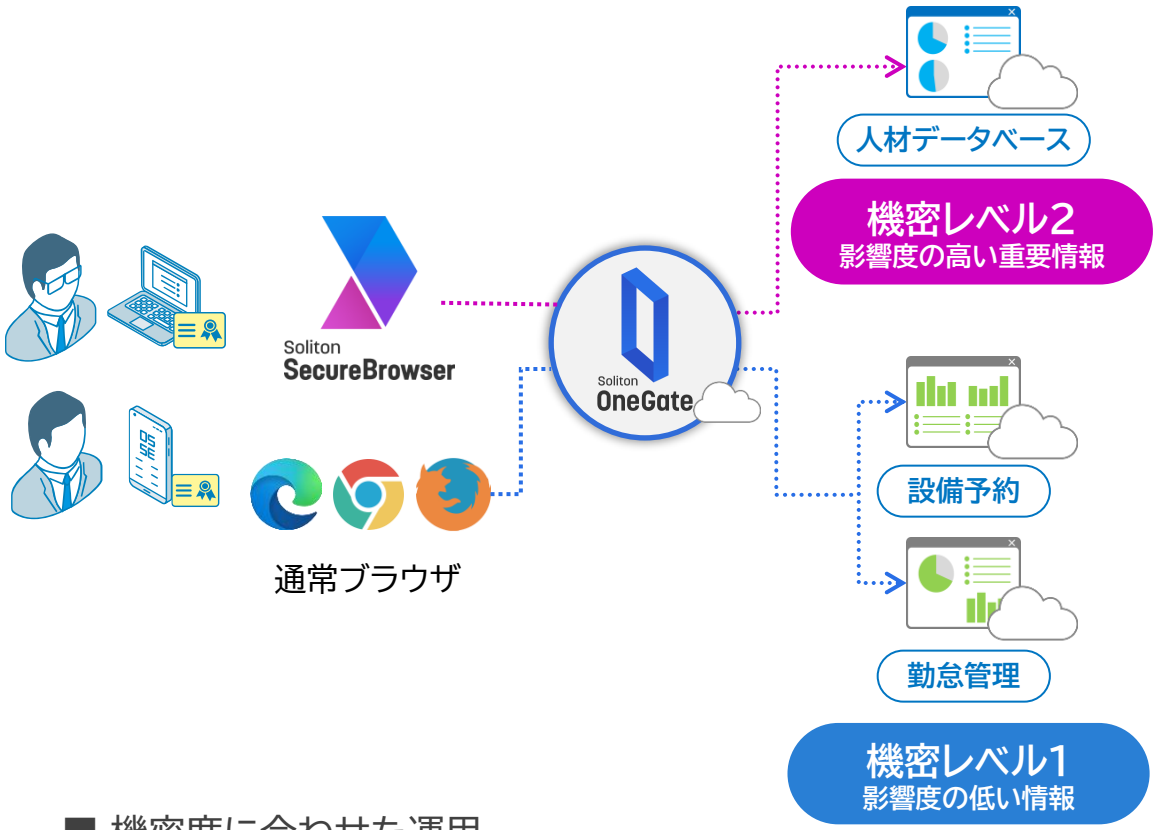
選定ポイント

- 多要素認証・シングルサインオンだけでなく本格的なデータ保護を実現できるか？
- 通常ブラウザと変わらない操作性か？（業務効率重視）
- 機密度にあわせたデータ保護で、業務影響を最小限にできるか？

導入効果等

- 機密度に合わせたデータ保護が実現できた
- 安全に社内外からデータ活用できるようになったことで、業務効率が上がった
- Windowsだけではなく、iOSでの展開も進める予定

人材派遣会社様 利用イメージ



■ 機密度に合わせた運用

- 機密レベル2のシステムは、セキュアブラウザのみ、通常ブラウザは禁止
- 機密レベル1のシステムは、通常ブラウザ・アプリOK
- 機密レベルに関わらず、常時、多要素認証・シングルサインオン

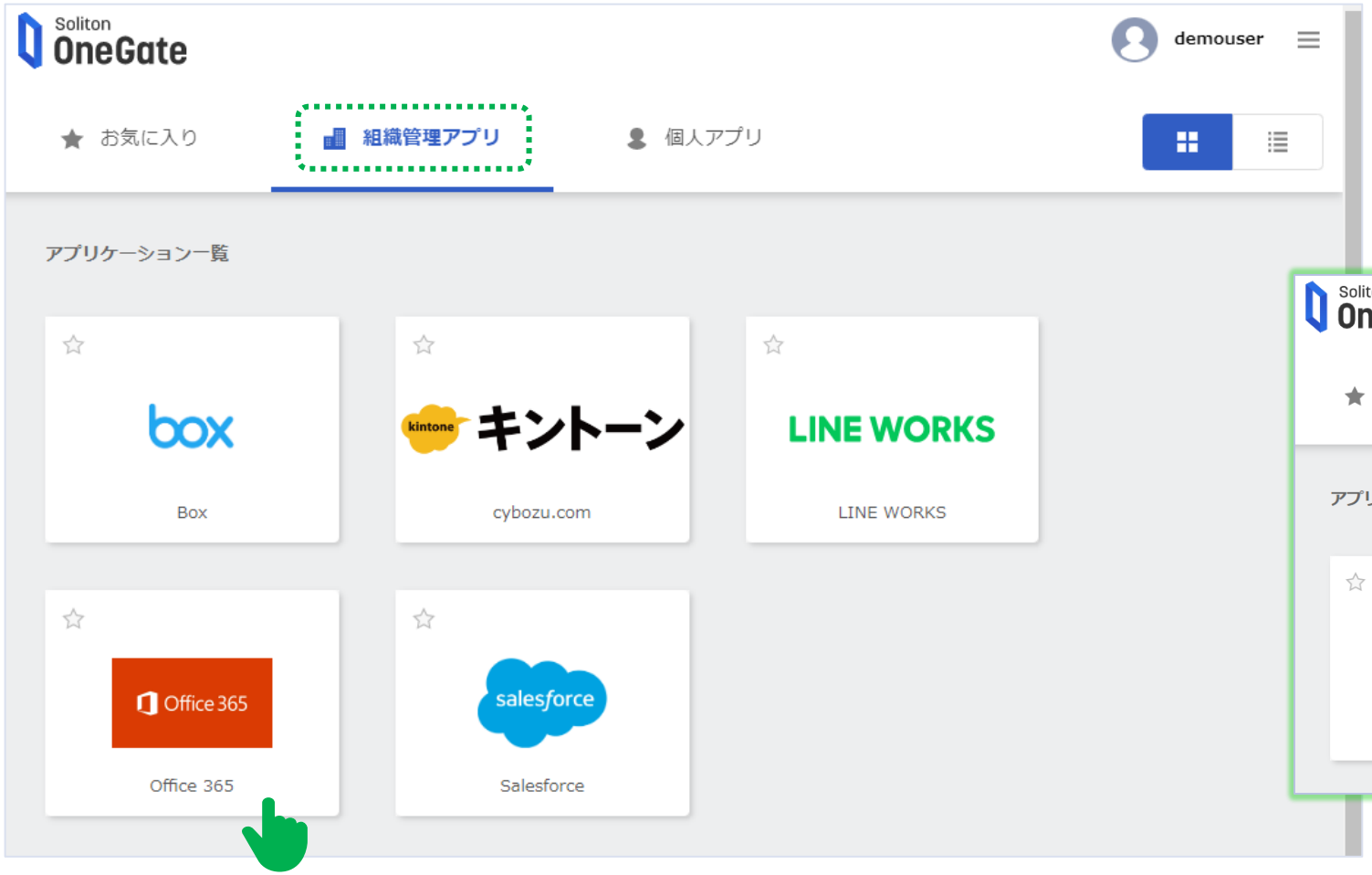
Soliton OneGate
その他の機能・特長

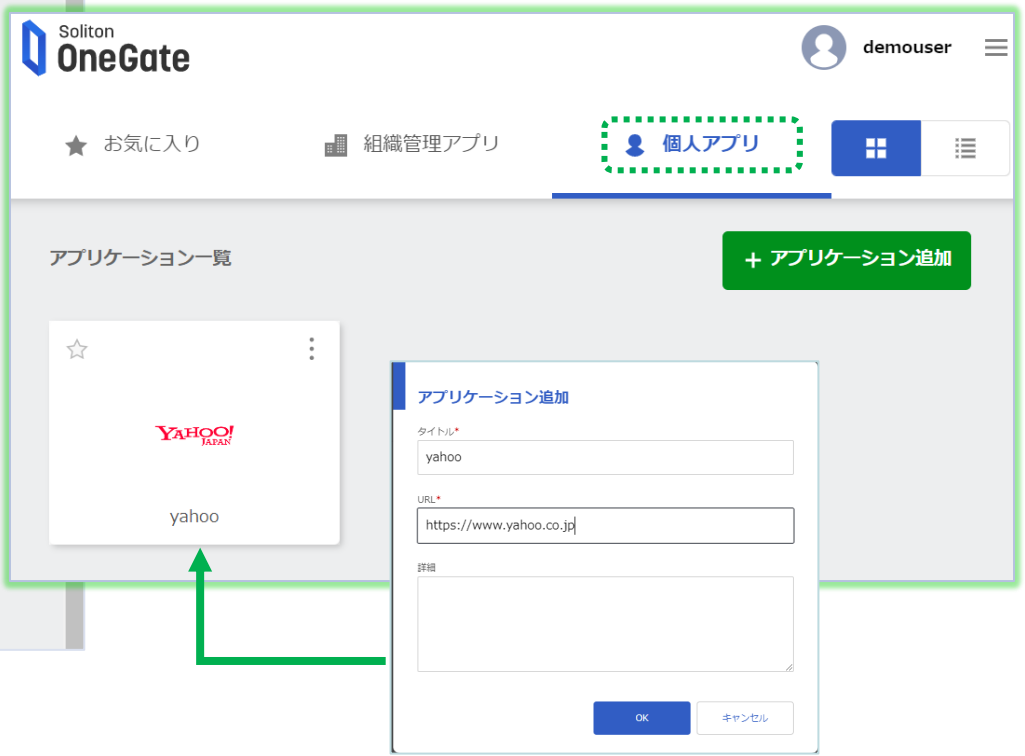
Soliton OneGateでは、セキュリティ機能の追加・向上だけではなく、利用者がより使いやすく、管理者がより運用しやすくなる機能強化を行っています。

また、クラウドサービスを安心してご利用いただけるよう第三者認証の取得にも取り組んでいます。

- 利用者ポータル
- 2ステップ認証・追加認証
- ポリシー／リスクベース認証
- Windowsサインイン
- 利用者管理タグ・利用者運用の委任
- クラウドサービスの安全性・信頼性 / 第三者認証

利用者ポータル





利用アプリケーションに、最短でたどり着ける

利用者ポータル – ユーザー自身による管理

有効な証明書

ユーザーで証明書失効操作ができる

未取得の招待コード

メールが利用できない環境でも、QRコード・URLから証明書インストール可能

FIDO2登録・削除

Authenticatorアプリ登録・削除

2ステップ認証・追加認証

コンテキストに合わせて認証強度を変える、2ステップ認証・追加認証

利用者の場所（ネットワーク）、アクティビティ、利用アプリケーション、アクセス先クラウドサービスに基づき、
通常のOneGateログイン認証に加え、異なる認証要素でさらなる認証を求めることができます。

2ステップ認証

- 信頼できないネットワークからのアクセス
- 通常とは異なるアクティビティを検知
  【Standard Preview】
- 例外アプリケーションからのアクセス

SAML認証時の追加認証【Standard Preview】

- 信頼できないネットワークからのアクセス
- セキュリティレベル「高」サービスへのアクセス
- 通常とは異なるアクティビティを検知

ポリシー／リスクベース制御

OneGateログイン時に2ステップ認証を行う

認証方式(1つ以上の選択必須)
- ☐ ワンタイムパスワード(メール通知)
- ☐ Soliton Authenticator
- ☑ 顔認証
  - ☐ OneGateパスワード必須

2ステップ認証を要求する条件 (1つ以上の選択必須)
- ☐ 信頼できないネットワークからのアクセス
- ☐ 通常とは異なるアクティビティを検知【Standard Preview】
- ☐ アクセス制御設定で登録した例外アプリケーションからのアクセス

SAML認証時に追加認証を要求する【Standard Preview】

認証方式(1つ以上の選択必須)
- ☐ ワンタイムパスワード(メール通知)
- ☑ FIDO2
  - ☐ UserVerification必須
- ☐ Soliton Authenticator
- ☑ ICカード
  - ☐ OneGateパスワード必須
- ☑ 顔認証
  - ☐ OneGateパスワード必須

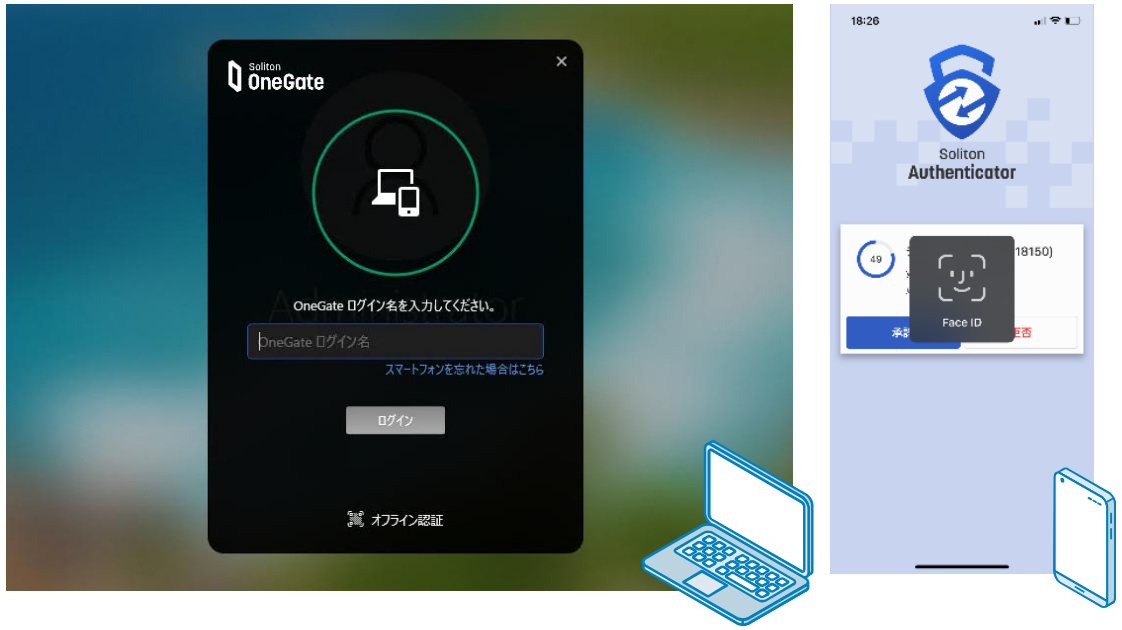
追加認証を要求する条件(1つ以上の選択必須)
- ☐ 信頼できないネットワークからのアクセス、かつ2ステップ認証を行っていない
- ☐ セキュリティレベル「高」のサービスへのアクセス
- ☐ 通常とは異なるアクティビティを検知

通常とは異なる
異常なログオン挙動を検知し
追加の認証を要求

※ This product includes GeoLite2 data created by MaxMind, available from https://www.maxmind.com.

Windowsサインイン

多要素認証でWindowsサインインを強化。各システムにも自動認証、利便性向上も可能です。



Windows
デスクトップへ

- ユーザーポータル
- Google Workspace
- Microsoft 365
- 社内システム

自分のスマホ or 顔認証でログオン承認 ※1

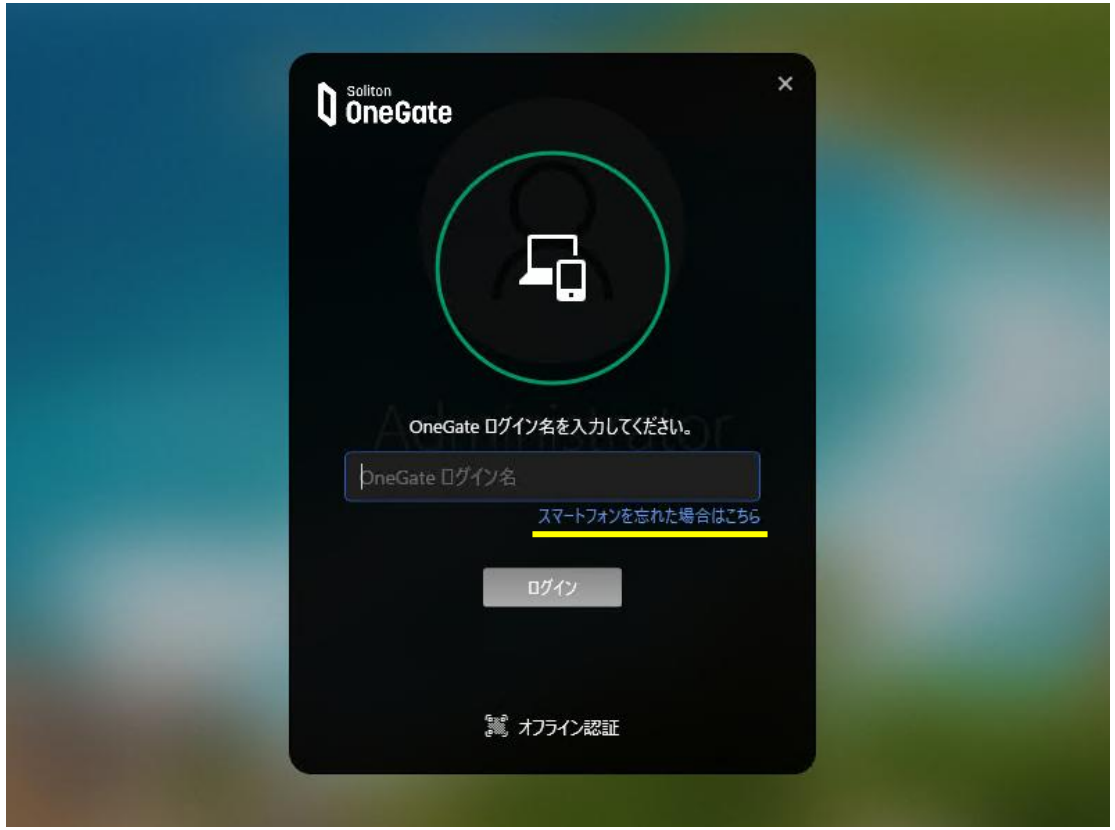
パスワードレスで一気通貫 ※2

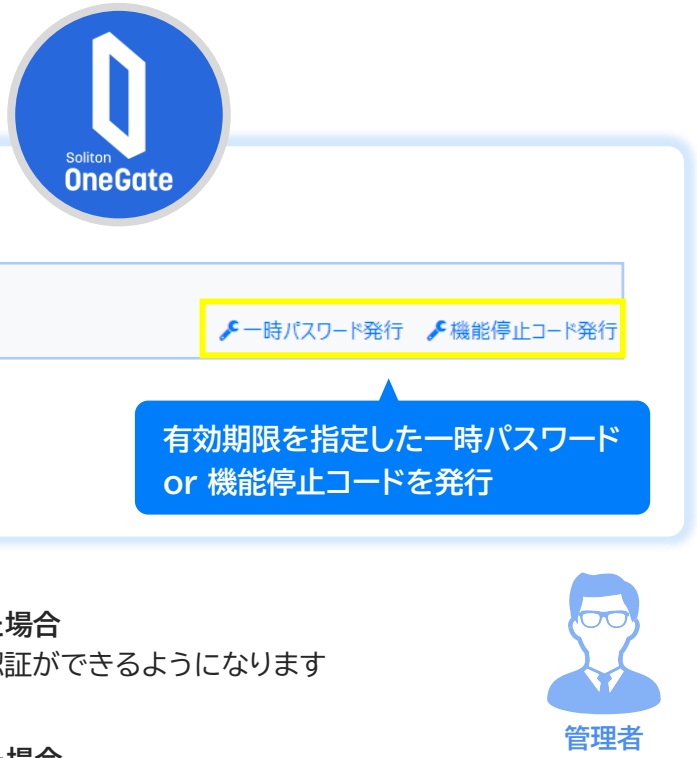
デモ動画はこちら

※1 Windowsサインイン機能は、Soliton Authenticatorあるいは顔認証が利用できます。オフラインで利用する場合は、Soliton Authenticatorをご利用ください。
※2 Windowsサインイン認証が完了していても、SAML認証/利用者ポータル認証は別途必要です。ただし、「統合Windows認証機能」や「クライアント証明書による自動認証機能」を利用することでユーザーのID/Pass入力を省略可能です。これを組み合わせることで、WindowsサインインからSAML認証/利用者ポータル認証まで、パスワードレスで一気通貫に利用することが可能です。

Windowsサインインの運用機能

「OS標準認証」を非表示とし、スマホ認証を必須にしながら、
スマホ忘れ対策が出来ます





一時パスワードで解除した場合
OneGateのパスワード認証ができるようになります

機能停止コードで解除した場合
通常のWindowsサインイン画面で認証できるようになります

管理者

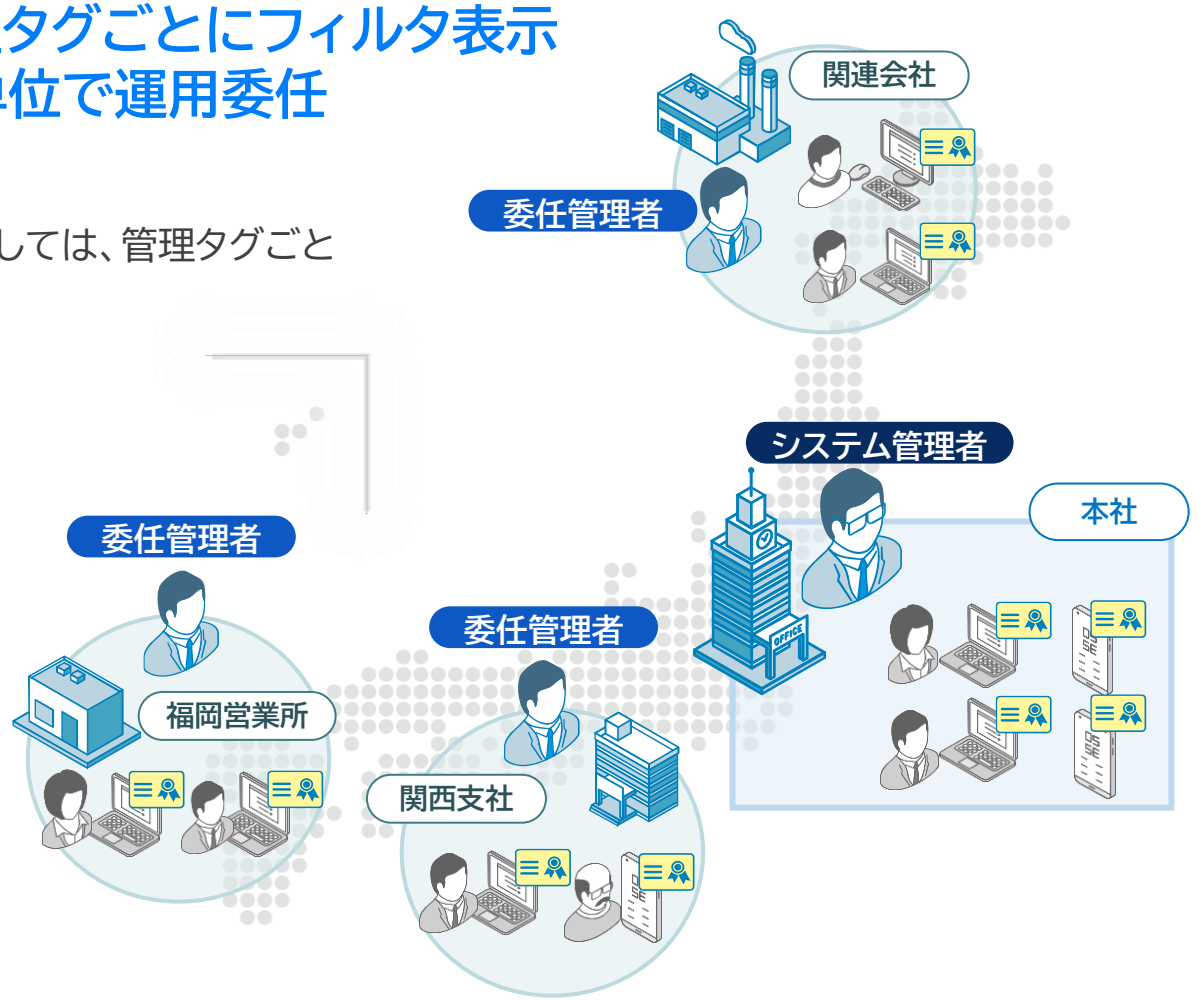
1 管理者へ一時パスワード発行を申請

2 発行した一時パスワードを連絡

利用者管理タグ/利用者運用の委任

利用者に任意の管理タグを付与し、利用者を管理タグごとにフィルタ表示
日々の運用に関わる業務は、利用者の管理タグ単位で運用委任

利用者情報に対して管理タグを付与し、一覧をフィルタ表示。
また、日常的なヘルプデスク対応で必要となる利用者向けの運用に関しては、管理タグごとに簡単・安全に分担できます。



システム管理者

- 全ての管理権限を保有(全ての利用者が対象)
- システム全体の設定変更が可能

委任管理者

- 委任された利用者の証明書発行・失効等
  日々の運用に必要な機能のみ可能
- システム全体の設定変更は不可

現場に近い管理者に、必要な機能のみを委任する運用が可能です

クラウドサービスとしての安全性・信頼性の確保

Soliton OneGateでは、お客様により安心してご利用いただくため、クラウドサービスの安全性・信頼性向上に努めるとともに、ISMAPをはじめとする各種第三者認証を取得しています

Soliton OneGateの取り組み

- お客様にサービスを提供するサプライチェーンの一員として安全性・信頼性の向上と第三者認証の取得に取り組んでいます
- 準拠法は国内法・認証局もISMAP言明範囲

  データは国内で処理・保管され、国内法に準拠するクラウドサービスです。また、高い信頼性が求められるデジタル証明書の認証局もISMAP言明範囲です。

取得済み第三者認証

- ISMAP（登録番号: C24-0074-2） 国産IDaaS初
- ISO27001（ISMS適合性評価制度）
- ISO27017（ISMSクラウドセキュリティ認証）
- ISO9001:2015/JIS Q 9001:2015（品質マネジメントシステム）
- プライバシーマーク 第10821699（09）号

ソリトンが取得しているセキュリティ認証一覧は以下をご参照ください：
https://www.soliton.co.jp/company/profile.html

公共・民間で求められる第三者認証

- **政府機関（中央省庁、独立行政法人、指定法人）**

  原則、クラウドサービス導入時はISMAP登録サービスから調達 ※1
- **自治体**

  クラウドサービス調達時、ISMAP登録の確認が求められる ※2
- **教育機関**

  クラウドサービス評価時の第三者認証としてISMAPを想定 ※3
- **重要インフラにおける特定重要設備**

  経済安全保障推進法に基づく、重要インフラ事業者の特定重要設備調達の際、ISMAP登録を行った事業者がベンダーやサプライヤーとなる場合には、一定の届出事項の省略が認められる ※4
- **その他の民間企業**

  その他の民間企業においても、政府機関が要求する基準をクリアした信頼できるクラウドサービスとして、ISMAPは有効な評価基準となる

※1 政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）
※2 地方公共団体における情報セキュリティポリシーに関するガイドライン（令和7年3月）
※3 教育情報セキュリティポリシーに関するガイドライン（令和7年3月）
※4 基幹インフラ役務の安定的な提供の確保に関する制度（内閣府）

OneGate無料トライアル～導入までの流れ

1

事前準備

評価・導入目的を定め、認証方式、対象システム・ユーザーなどを検討・確認します（※1）。

2

お申込み

Webフォームより、無料トライアルをお申込みください。

3

無料トライアル

お申込みから最短5営業日で、トライアル用テナントをご用意します（※2）。
ご利用予定の機能などをお試しください（無料トライアルは30日間）。

4

本番運用へ

正式発注いただき、本契約へ。
トライアル環境をそのまま利用した本番移行も可能です（※3）。

最短 約1か月半で導入

※1 ご評価内容によって準備が必要なものは変わります。詳細はFAQをご参照ください。
※2 お申し込み時のメールアドレスに、テナント利用のためのアカウント情報をお送りします。
※3 トライアル環境を利用した本番移行は、トライアル申し込み者と同一組織による本番利用に限ります。詳細はお問い合わせ下さい。

OneGate 機能一覧

ユーザー情報管理
- AD連携／Entra ID(旧 Azure AD)連携（PW非同期方式）
- 管理UIから直接登録（セルフPWリセット対応）

プライベートCA
- クライアント証明書発行(1ユーザー10枚まで)
- 証明書配布＆失効管理支援機能
- サーバー証明書発行
- MDM連携による証明書発行（Intune連携、Chrome OS対応）

MFA・多要素認証
- パスワード認証（AD連携／Entra ID(旧Azure AD)連携）
- 統合Windows認証
- デジタル証明書認証
- FIDO2／WebAuthen
- 顔認証
- Soliton Authenticator（スマホ認証）
- ICカード

シングルサインオン
- SAML連携(IdP機能／プライベートアプリ登録)
- 代理入力サインオン（Windows/iOS/Android版 PasswordManager）
- 利用者ポータル
- アプリケーションロール機能

IDプロビジョニング
- Microsoft 365 / Google Workspace / cybozu.com / Salesforce / Box / Splashtop Enterprise Cloud

Wi-Fi／VPN認証
- RADIUS認証(EAP-TLS / PAP)
- Wi-Fi/VPNプロファイルの配布

ポリシー／リスクベース制御
- 重要アプリへの追加認証設定
- 通常とは異なるアクティビティの検知

Windowsサインイン
- スマホ認証によるパスワードレスPCログオン
- 顔認証によるパスワードレスPCログオン

セキュアブラウザ
- 隔離領域外へのデータ持ち出しを禁止する専用ブラウザ
- ファイルダウンロード・受け渡し制御
- データ初期化(ブラウザ終了時/特定のタイミング)
- マルチOS対応 ※

ログ管理
- 特権利用ログ(管理ログ／管理者ログインログ)
- 利用者ログ(利用者ログインログ／SSOログ)
- ログ転送(SIEM連携)

※Windows、iOS/iPadOSに対応。Android版も順次対応予定です。

動作環境は、https://www.soliton.co.jp/products/onegate/specification.html をご確認ください。

Soliton OneGate

		License Pack ※1		
		PKI	Basic	Standard
		￥100	￥300	￥600
ユーザー情報管理	AD連携 / Entra ID連携 / 管理UIから直接登録	●	●	●
プライベートCA	クライアント証明書発行（1ユーザー10枚まで）	●	●	●
MFA・多要素認証	証明書 / パスワード / FIDO2 / 統合Windows認証 / スマホ認証(Soliton Authenticator) / ICカード	※2	●	●
シングルサインオン	SAML連携（連携数無制限）	-	●	●
	代理入力サインオン(PasswordManagerオプション Web/App)	オプション ￥200	オプション ￥200	●
Wi-Fi／VPN認証 ※3	RADIUS認証（EAP-TLS/PAP）	●	●	●
プロビジョニング	対応SaaSへのIDプロビジョニング	-	●	●
リスクベース認証制御	重要アプリの追加認証 / 通常とは異なる挙動の検知	-	-	●
Windowsサインイン	スマホ認証によるパスワードレスPCログオン (PasswordManagerオプション Windows サインイン)	オプション ￥200	オプション ￥200	●
セキュアブラウザ	隔離領域外へのデータ持ち出しを禁止する専用ブラウザ	-	●	●
ログ管理	管理者ログ / 利用者ログ	●	●	●
顔認証	顔認証によるMFA / Windowsサインイン ※4（顔認証オプション）	オプション ￥300 ※2	オプション ￥300	オプション ￥300
API利用	APIキー発行/ログ転送	-	●	●
NetAttest EPS-edge 	アプライアンス利用料	● SXモデル 初期費用：198,000円／台 ● SXモデル 月額費用：6,000円／台		

※1　契約開始日は、サービス開始日の翌月1日です。この日より月額課金対象となります。最低利用期間は契約開始後3か月、契約は1年単位での自動更新が基本となります。発注単位は10です。PKIの最小契約数は200ユーザー、ベーシックの最小契約数は70ユーザー、スタンダードの最小契約数は40ユーザーです。（Wi-Fi／VPN認証またはPasswordManagerオプションを利用される場合のPKIの最小契約数は100ユーザーです）
※2　PasswordManagerオプション Web/App利用時に、OneGateログイン認証においてMFAが利用可能です。　※3　別途アプライアンス利用料が必要です。
※4　顔認証オプションには、PasswordManagerオプション Windowsサインインが含まれます。また顔認証機能はオンラインでの利用を前提としています。オフライン利用が想定される環境でWindowsサインインに顔認証を利用する場合は、スマホ認証（Soliton Authenticator）などとの組み合わせでご利用ください。※5　海外拠点におけるご利用もご提案が可能です。詳細はお問い合わせください。

Soliton OneGate

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

Soliton®

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

大阪営業所 06-7167-8881
札幌営業所 011-242-6111
福岡営業所 092-263-0400
名古屋営業所 052-217-9091
東北営業所 022-716-0766