拡張性を考慮した認証サービス活用術

Salesforceへデジタル証明書による MFA を適用する利点とは

Soliton OneGate

Salesforce が 2022年2月からMFAを必須化

チャットアプリなどコンシューマー向けアプリケーションで二段階認証の設定を推奨する案内がよく来ていますが、なぜ推奨されるのかというと、**実際に利用者のアカウントが乗っ取られる不正アクセス被害が発生**しているからです。コンシューマー向けアプリの世界で起こっていることは法人向け業務アプリでも発生しているのが現実で、CRMで有名な**Salesforceが今年の2月より MFA（多要素認証）適用の必須化を決定**したことが話題となっています。

テレワークが長く続く中、**漏えいアカウントを利用されるなど、クラウドサービスへの不正アクセス被害が増加**していますので、今後、他のクラウドサービスも MFA 必須化の動きに追随してくるかもしれません。

漏えいアカウント被害調査を行った 99.9% の企業で
社員のパスワード漏えいが発覚

調査数 1660 ドメイン（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

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。

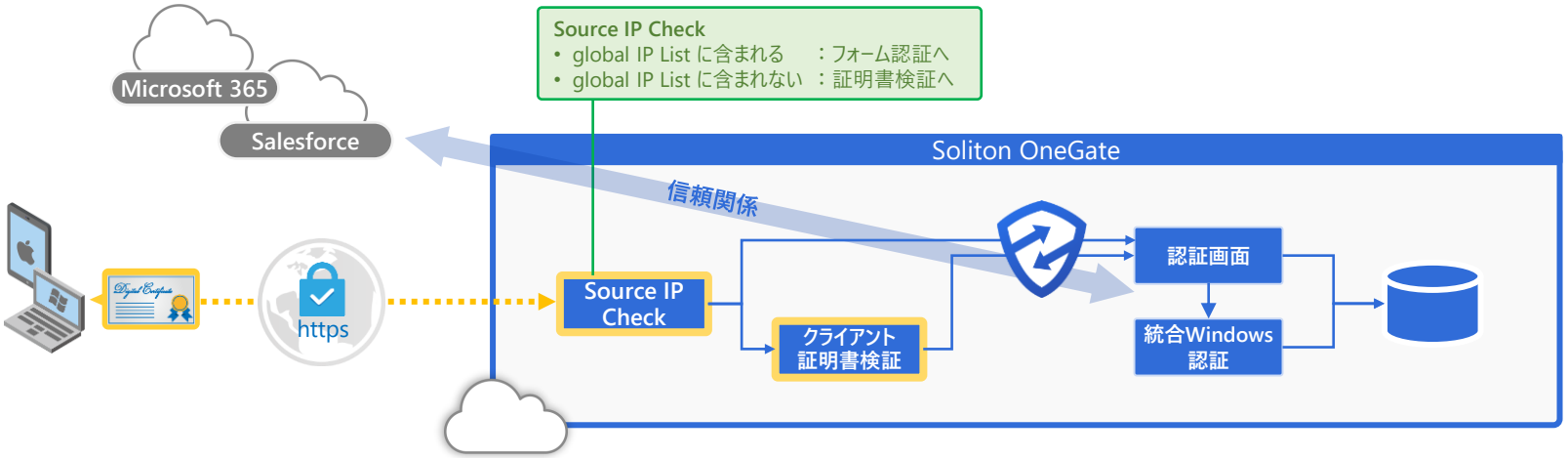
また、SMSワンタイムは利用者本人の確認手段であり日本国内でニーズの強い、**利用端末の特定に対応できない**点にも注意が必要です。

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、社員数が多ければ多いほど、容易にできてしまいます。

デジタル証明書認証の優位性、情報資産の保護に絶大効果

クライアント証明書による認証は、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されません。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にすることができます。

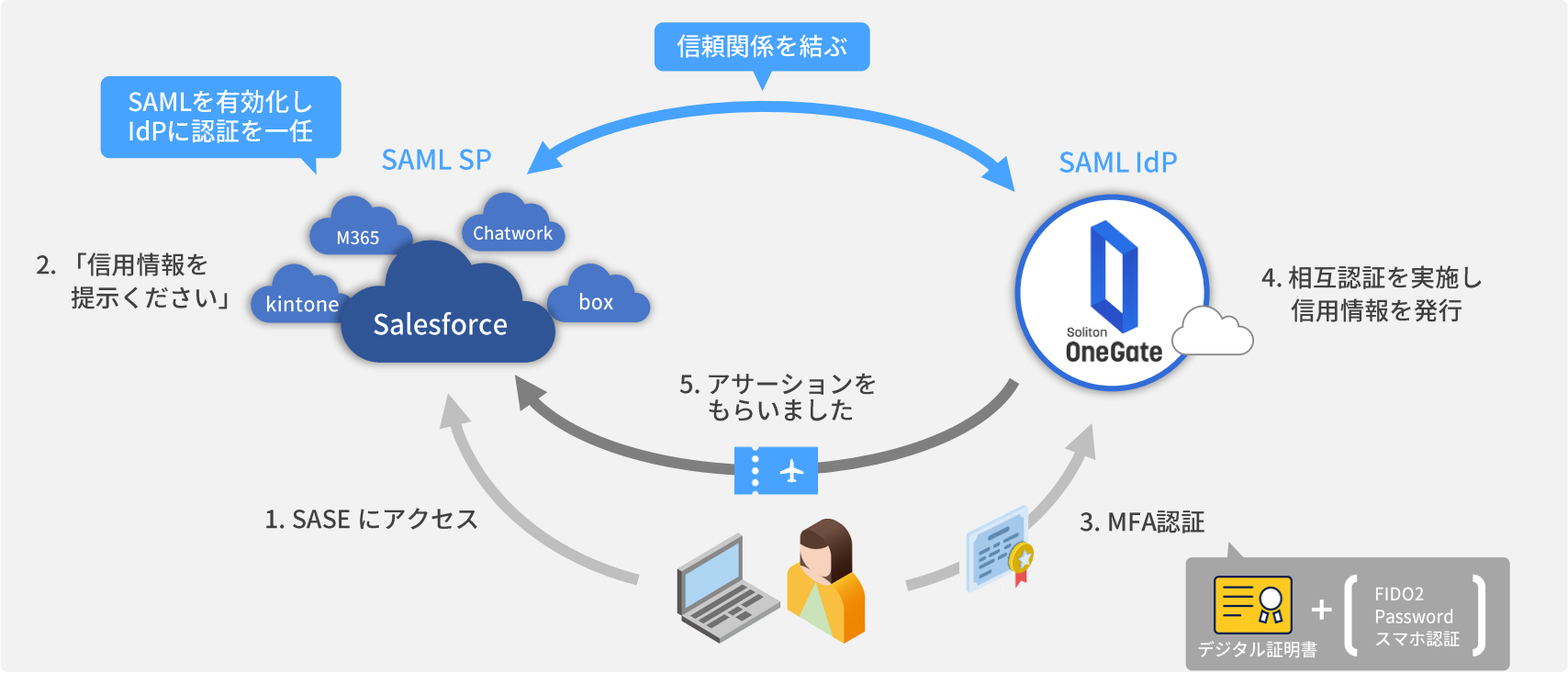


《SSL相互認証で不正アクセスを防止》

利用中のクラウドサービスをまとめて MFA 適用

Salesforce の MFA 適用は、専用スマホアプリ（Salesforce Authenticator）を用いる方法と、IDaaS と呼ばれるサードパーティの認証サービスを利用する方法があります。IDaaS にはコストがかかりますが、**利用するクラウドサービスを一度の認証で利用でき、認証情報を個別に管理する必要がなくなるという運用面での大きな利点**があります。

デジタル証明書認証に対応したIDaaSを採用すれば、利用者と利用端末を素早く特定できる、安全性と利便性の高い多要素認証環境の実現が可能となります。



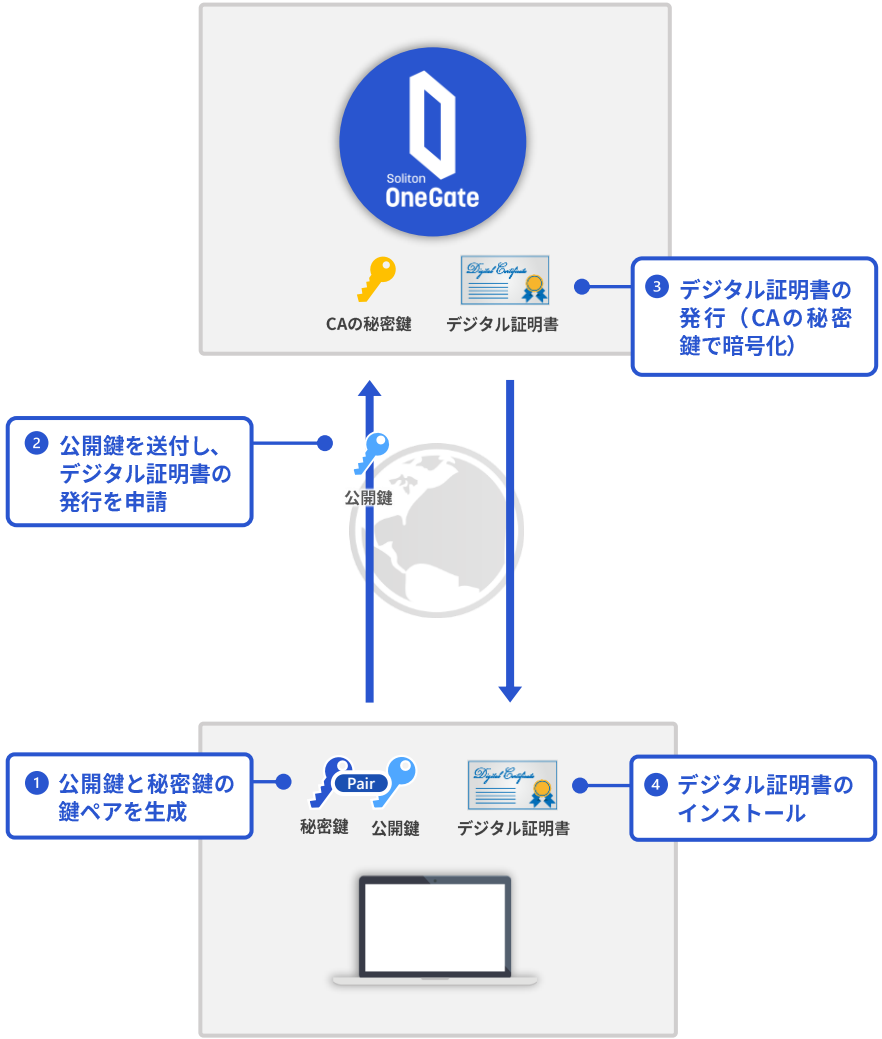
デジタル証明書の安全な配布手法

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。



MFA 認証連携設定の流れ

SAML サービスプロバイダ（=SP）

Salesforce／box／M365／Chatwork／etc.

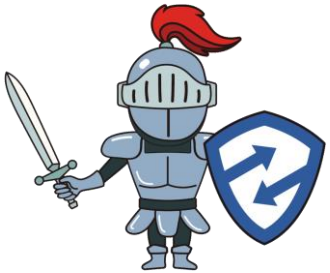
信頼関係を結ぶ

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**

SAML IDプロバイダ（=IdP）

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**

各設定ガイドなど公開中



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

2022年 3月

SOGWP-SFMFA-01