境界線防御から
ゼロトラストモデルへ

次世代に通用する認証手法とは

Soliton®

ITシステムは、所有から利用へ

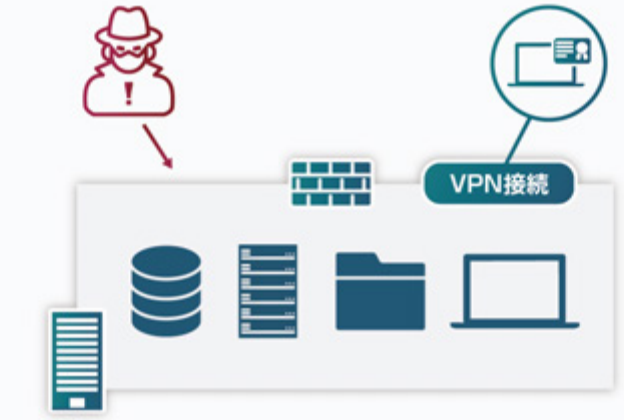
E-mailのクラウド化をきっかけに、国内さまざまな企業・組織において、ITシステムのクラウド移行を目指す動きが始まっています。日本政府においてもクラウド・バイ・デフォルトとして、政府情報システムの整備はクラウドサービスを第一義的に検討すべきという原則を発表しています。

クラウドシフトが進む以前のセキュリティモデルは、ITシステムは自社で構築・所有し

- **社内ネットワークの中は信頼できるものとして、脅威はネットワークの境界線で防御する**
- **社外からはVPN接続（デジタル証明書などで認証強化）により、社内ネットワークを利用させる**

といった形が基本でした。しかし、デジタルトランスフォーメーションが促進されクラウド化が進むと、情報資産は社内だけでなくクラウド上にも分散することになります。また、利用する端末も社内設置の端末だけでなく、インターネットに直接繋がるモバイル端末の活用も必須となってきます。

情報資産が境界内にかたまっており、境界線だけで守れていた従来の環境とは異なってくるため、情報資産の守り方も考え方を変える必要がでてきます。



従来は、社内で情報資産を所有、
境界線で防御する。

さまざまな場所の情報資産を
どう守るか？

求められる「ゼロトラストモデル」

そこで、従来のネットワークでの境界線防御に変わる概念として注目を集めているのが、ゼロトラストという考え方です。トラストがゼロ、つまり、信頼せず常に確認するというセキュリティモデルです。

アクセス制御地点をネットワークの境界から個々のデバイスやユーザーに移すことで、従業員が従来のようにVPNを介さなくても「信頼できないネットワーク」を通じて、安全に働くことが可能となります。

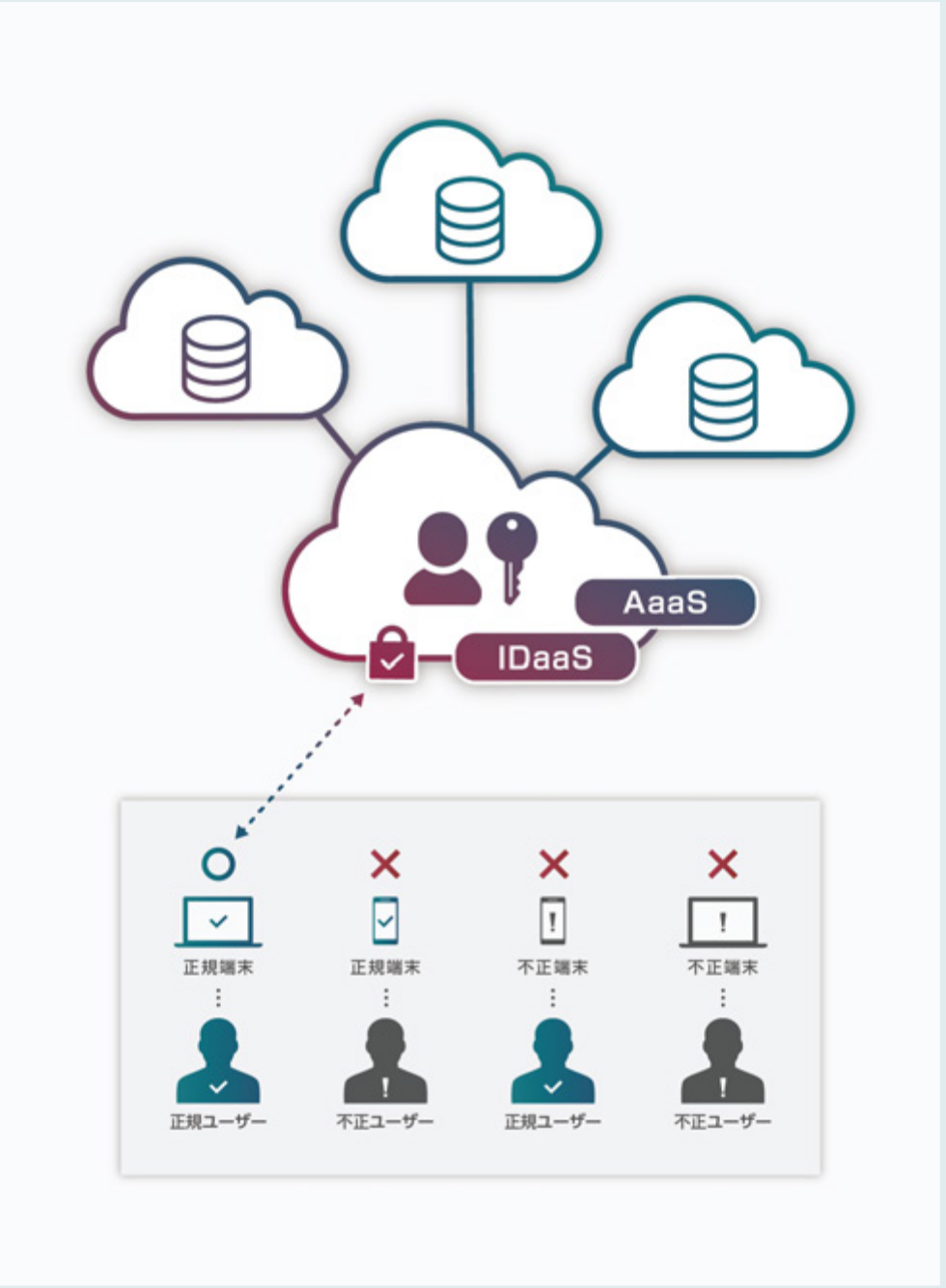
このVPNを前提としない、ゼロトラストモデルで重要となるのは、

- **情報資産への徹底したアクセス管理**
- **情報資産へアクセスする「人＝ID」と認証の管理**
- **情報資産へアクセスする「デバイス」と認証の管理**
- **可視化と継続的な監視**

です。

このクラウド上の情報資産を守る要（かなめ）となる“認証”を統合管理するのが、IDaaS（Identity as a service）の役割です。

IDaaSは、様々なロケーションにある業務システムにアクセスする「人＝ID」と「端末」を識別し、それぞれに適切な認証を要求することで、インターネット上の情報資産への不正アクセスを確実に防止します。



人＝ID の認証は利便性で選ぶ

世界中で起きているハッキング事件によってインターネット上に流出したアカウント情報には、メールアドレスのほかユーザーIDやパスワードなどが含まれており、日本（JPドメイン）の漏洩アカウントも多数確認されています。

Soliton がこれまでに行った漏えいアカウント被害調査のうち、実に全体の98.9%（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洩が確認されており、もはやパスワードだけに頼った認証は限界を迎えていると言えます。

パスワードに頼らない認証方式は、多要素認証／MFA（Multi-Factor Authentibation）という言葉で定義されますが、パスワードなどの「知識」、ICカード・USBトークンなど「所有」、指紋・顔・静脈など「生体」を組み合わせ本人認証を要求します。

多要素認証は利用者に手間がかかると不満が高まるため、利便性の高い方式を選ぶことが重要となりますが、最近では「所有」するスマホとFace IDなどスマホの「生体」認証を組み合わせた多要素認証にも注目が集まっています。

なお後述するデジタル証明書は「所有」の認証要素となるため、従来からVPN認証などで利用されてきた、デジタル証明書＋ADパスワードによる多要素認証も、手早く認証強化を行いたい際の有効な手段と言えます。

端末の認証は安全性で選ぶ

マルチOSで利用でき、安全性が高く改ざんできないデジタル証明書は、端末認証の手段としてデファクトスタンダードとなっており、無線LAN認証の用途でも数多くの企業・組織に導入されています。

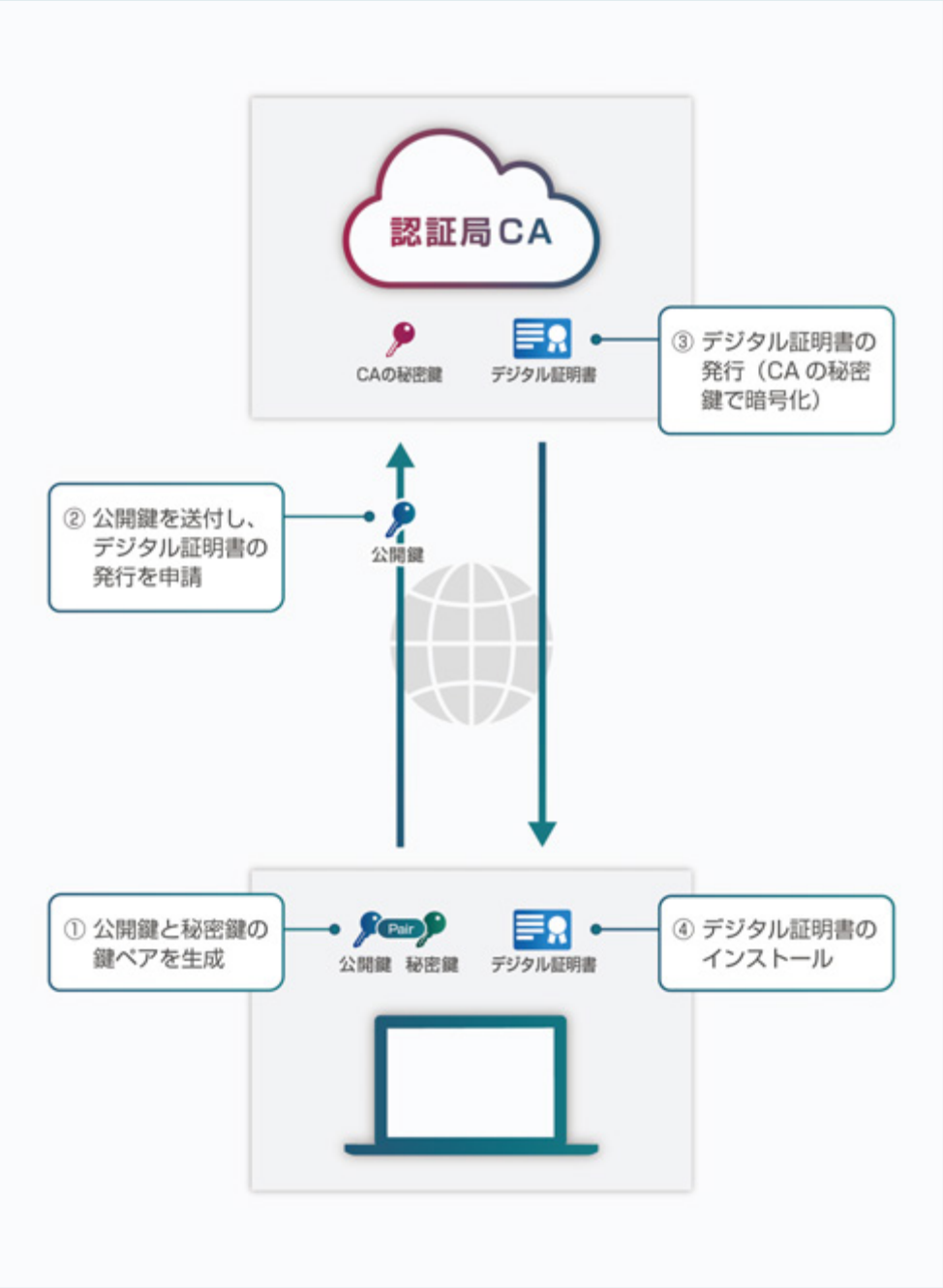
従来の境界線防御モデルでは、IT管理者が社内の支給端末にデジタル証明書を配布するケースが中心でしたが、ゼロトラストモデルにおいては、リモートワーク端末やBYOD端末へのデジタル証明書配布を考慮する必要がでてきます。

デジタル証明書は、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、このP12ファイル自体は容易にコピーできるため、利用者へこれを直接配布することは推奨されません。

デジタル証明書の配布は

- **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、適切な端末認証が可能となります。



国産IDaaS「Soliton OneGate」

Soliton が国内開発・提供する IDaaS「Soliton OneGate」は、これまで数多くの国内企業・組織に販売してきた認証製品・サービスのノウハウが集約されています。

官公庁、地方自治体、民間企業で幅広く利用されているエンドポイントの情報漏えい対策サービス「SecureBrowser」「WrappingBox」との親和性も高く、端末管理に縛られず BYOD端末利用を促進することができます。また「NetAttest」で運用しているデジタル証明書を、そのままクラウド認証用途に利用したり、社内の多要素認証システム「SmartOn」とシームレスに連携することも可能であり、VDIから脱却しゼロトラストモデルを最短で推し進めることも可能となります。

Solitonでは、オンプレミスの業務システムも含めた統合ID運用やパスワードレス化のコンサルティングも行っております。クラウド移行期における課題・お悩みが ございましたら、お気軽にお問合せください。

お問い合わせ

株式会社ソリトンシステムズ ITセキュリティ営業部

〒160-0022 東京都新宿区新宿2-4-3
TEL： 03-5360-3811
E-mail：netsales@soliton.co.jp
URL： https://www.soliton.co.jp/