マルチデバイス時代のリモートアクセス整備ガイド

- NetAttest EPSによる二要素認証とセキュアブラウザの活用

Soliton Systems K.K.

目次

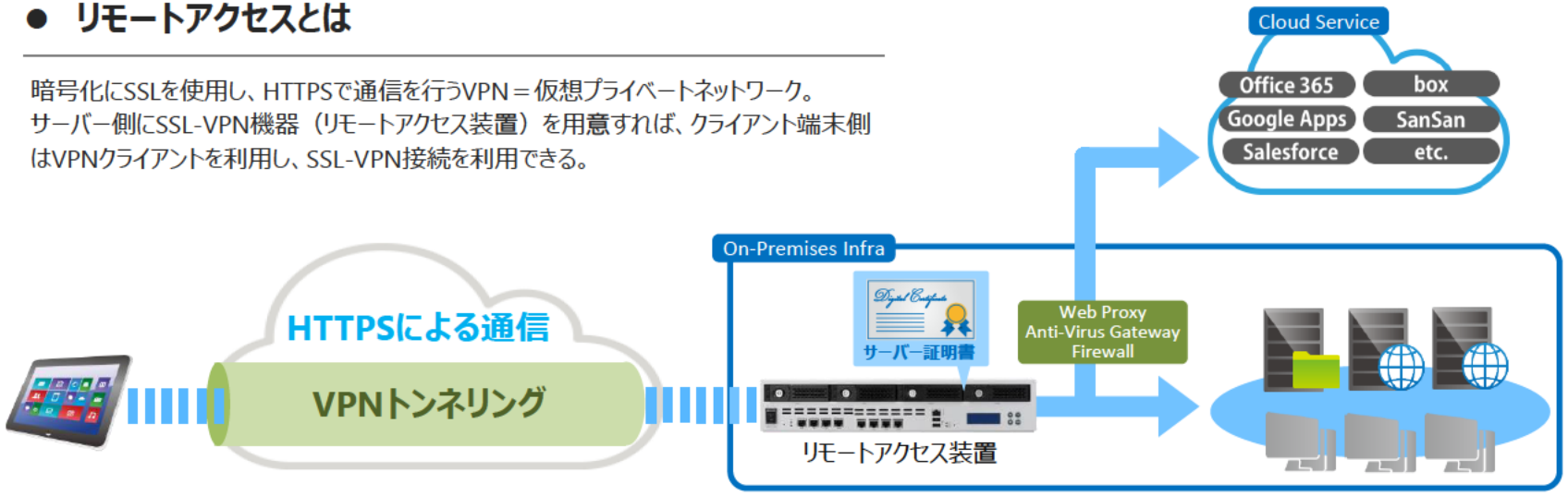
会社のゲートウェイを利用させる、リモートアクセス装置

Office365やGoogle Appsをはじめとする業務システムのクラウド化をきっかけに、外出先や自宅からも、業務システムを利用したい、という声が増えています。

社員が自宅のPCから直接、これらのクラウドにアクセスしてしまった場合には、会社のセキュリティポリシーが適用できず、悪意のあるなしに関わらず、深刻な情報漏えいにつながりかねません。そこで、会社のゲートウェイを必ず通過させ、社内セキュリティポリシーが適用されるよう、リモートアクセス装置の導入や見直しを進める動きが進んでいます。

● リモートアクセスとは

暗号化にSSLを使用し、HTTPSで通信を行うVPN＝仮想プライベートネットワーク。
サーバー側にSSL-VPN機器（リモートアクセス装置）を用意すれば、クライアント端末側はVPNクライアントを利用し、SSL-VPN接続を利用できる。



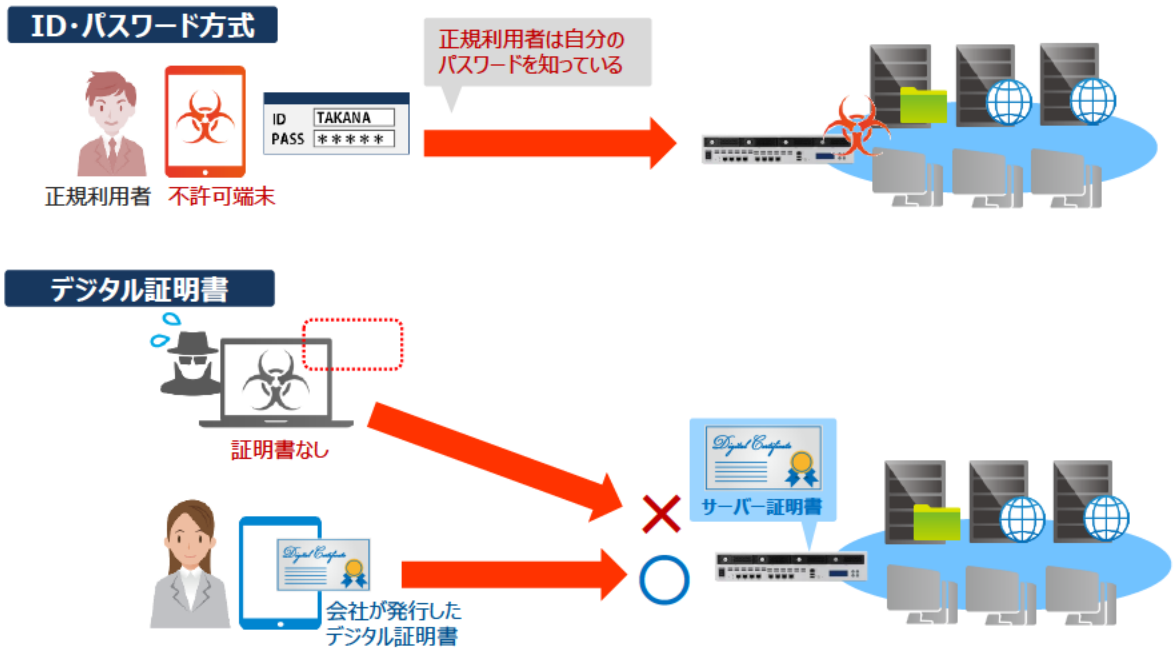
従来からある技術だが、デバイスが多様化する中で考慮すべき点は？

マルチデバイス時代に最適な、二要素認証とは

従来の認証強化は、USB接続装置を利用したICカード認証や生体認証などが検討されてきました。しかし、スマートデバイスではPC用認証ソフトが利用できなかったり、USB接続の読取装置も利用できないため、これらに代わる認証手段が必要となります。
また、社員が会社が許可していない私物デバイスをつないでしまう、シャドーIT対策もとる必要があります。※

これらの課題を解決するのが **デジタル証明書** です。企業規模に関わらず先進企業様では、Windowsにもスマートデバイスにも適用できる、デジタル証明書を用いた二要素認証の導入が進んでいます。

● デジタル証明書による認証とは



デジタル証明書とは、公開鍵暗号を利用してユーザーの身分などを証明するデータのセットである。公開鍵暗号方式は、公開鍵と秘密鍵という鍵ペアを使い、片方で暗号化したデータは、ペアのもう一方の鍵でしか復号できない性質を持つ。

なお、秘密鍵はデバイス内にエクスポート禁止の状態で格納することができ、利用者認証だけでなく、端末認証の要素としても利用することができる。

※ ワンタイムパスワードやイメージマトリクスも有効な利用者認証強化の手段ですが、端末の特定を行うことができません。