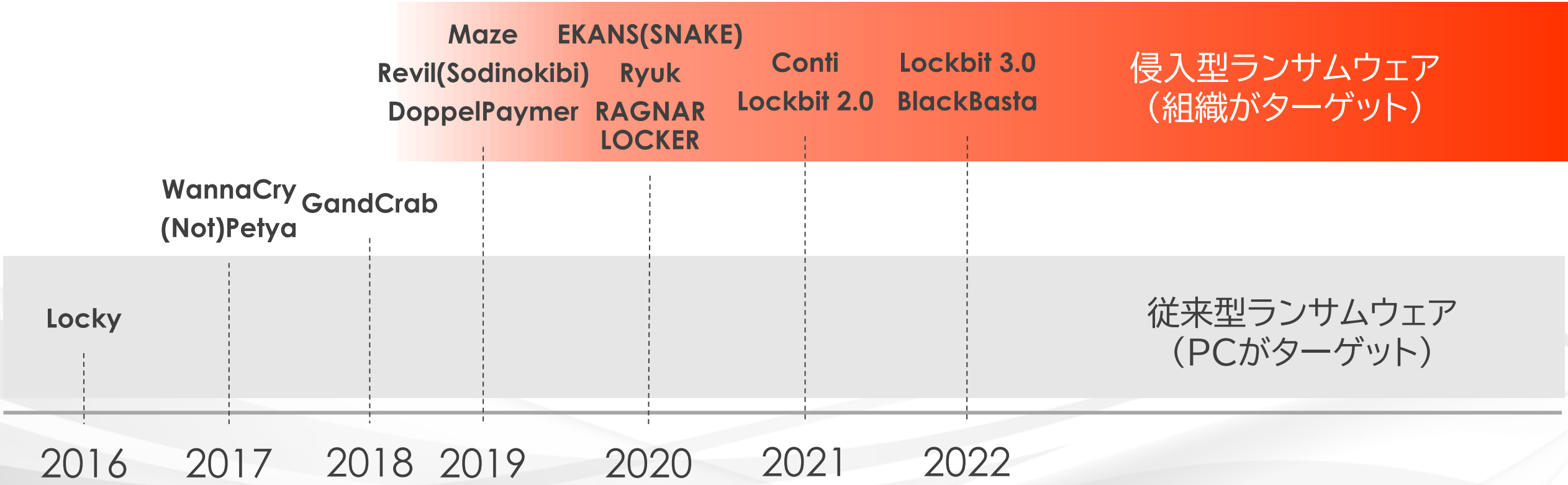
FortiGate＋OneGateで実現する 侵入型ランサムウェア対策としての認証強化

株式会社ソリトンシステムズ

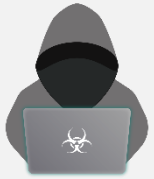
侵入型ランサムウェアとその対策

侵入型ランサムウェアの台頭(Human Operated Ransomware)



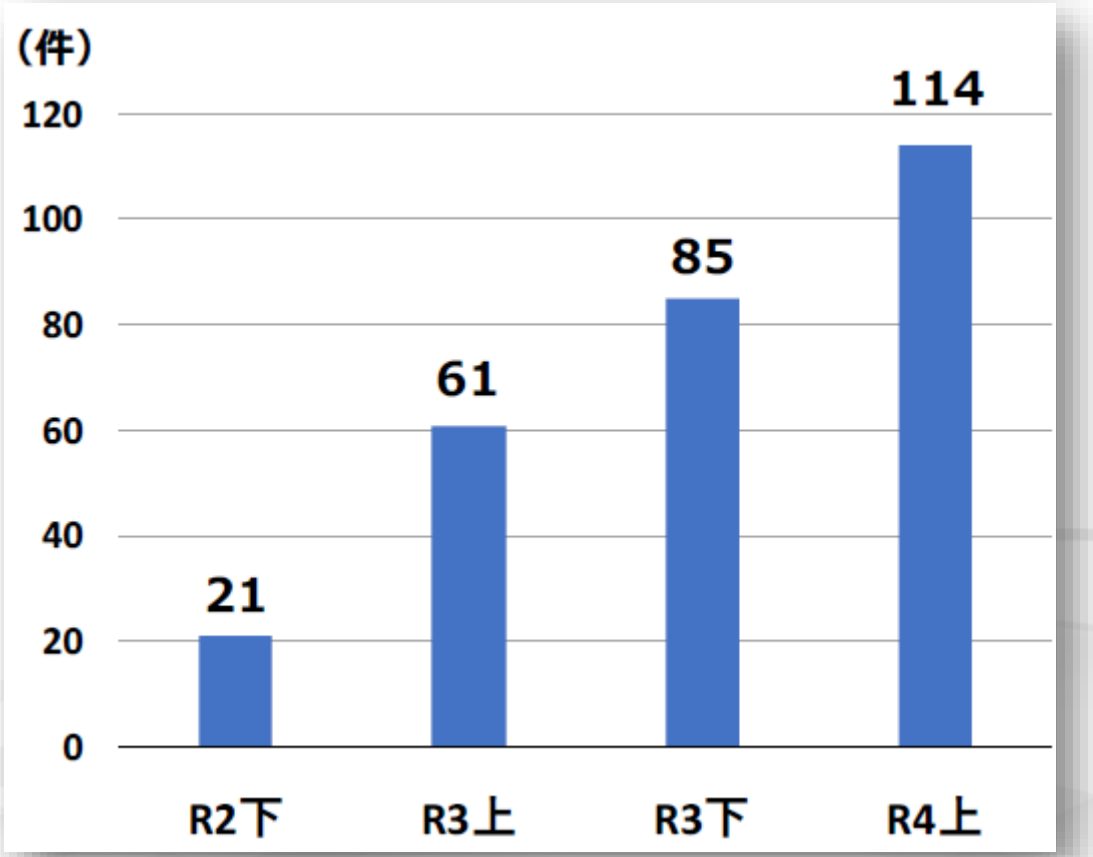
※Human Operated Ransomwareには、「多重脅迫ランサムウェア」「標的型ランサムウェア」などと表現される場合もありますが、ここでは「侵入型ランサムウェア」と記載しています。
※EKANSやRyukなどは、記載の年代以前から旧バージョンが報告されていますが、システム侵入型ランサムウェアの被害が多数報告された時期にて記載しています。

侵入型ランサムウェア被害の急増



侵入型ランサムウェア(※)

- 2019年～ 日本でも被害増加
- 企業・組織全体が狙われる
- 主な侵入経路はリモートアクセス
- 情報窃取、暗号化、恐喝

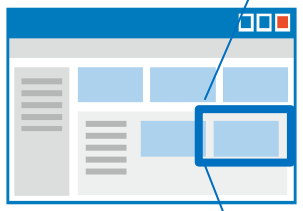


※侵入型ランサムウェア：二重恐喝型・暴露型・標的型ランサムウェアまたはHuman Operated Ransomwareとも言われる攻撃スタイル。システムに侵入後、情報窃取したうえで暗号化し、復号化のために金銭を要求。応じない場合は、窃取済みの情報を暴露するとしてターゲットを恐喝する。個人ではなく組織が狙われており、日本でも被害が急増しています。

令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和4年9月15日 警察庁）
図表1：企業・団体等におけるランサムウェア被害の報告件数の推移
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

リークサイトへの暴露例(イメージ)

実名公表される



企業・組織の実名や会社ロゴ

企業・組織のURL

企業・組織の住所

企業・組織の事業内容・沿革など

残り〇〇%

漏洩した総データ量と暴露の進捗

2022年12月31日まで

ファイル数[5.2TB]

2022年新規顧客契約フォルダ.zip

新製品設計書.zip

サンプルが公開されるケースもある

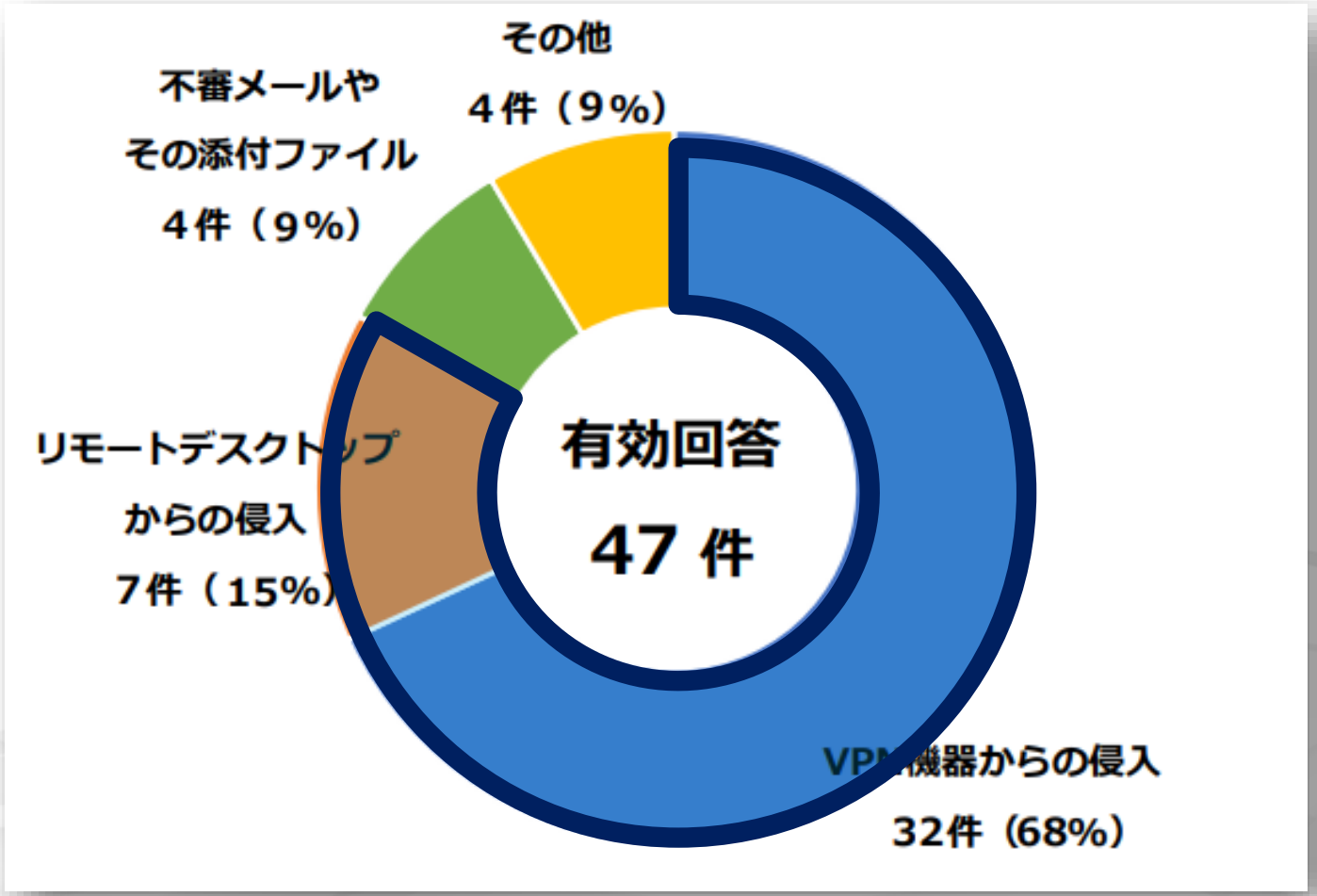
自社情報だけではなく、取引先とやり取りしたデータが漏洩するケースもある
当然、既に盗まれたデータであり、リークサイトからの削除はできない

侵入型ランサムウェアの経路

68%
VPN機器からの侵入
（脆弱性・漏洩済み認証情報の悪用）

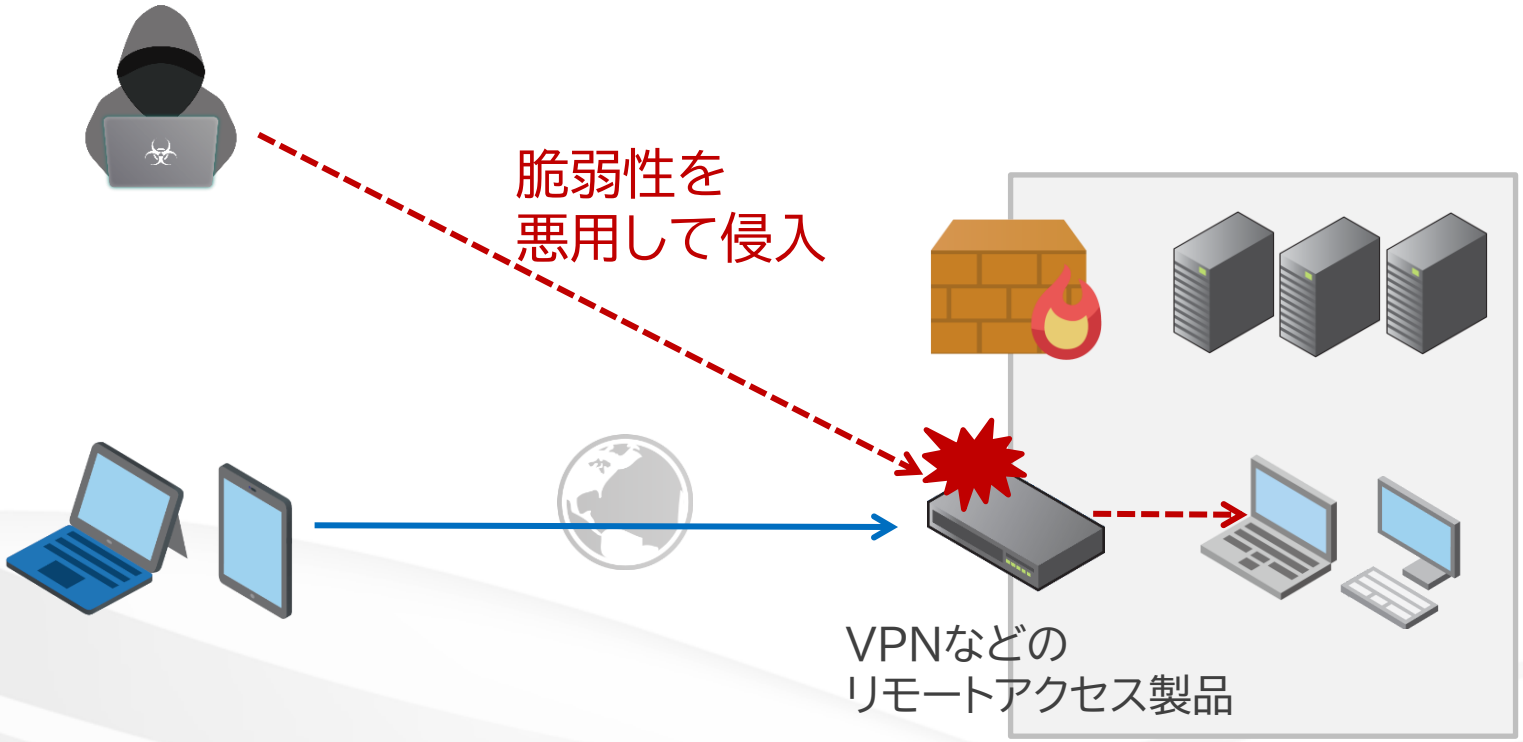
15%
リモートデスクトップ
（脆弱性・漏洩済み認証情報の悪用）

リモートアクセス経由
での侵入が多い



令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和4年9月15日 警察庁）
図表7：感染経路（注 図中の割合は小数第1位以下四捨五入しているため、総計が必ずしも100にならない。）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

リモートアクセス経由での侵入



ランサムウェアの侵入経路

■国内事例
・SSL-VPN経由が多数

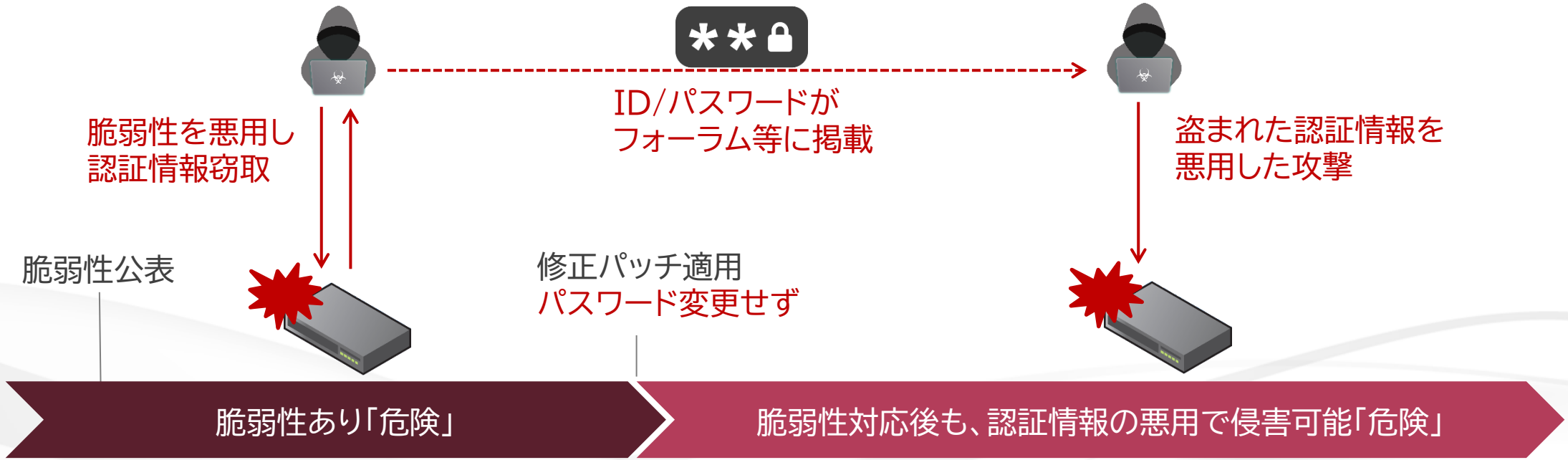
■海外事例
・SSL-VPN経由
・Windows Exchange脆弱性
・Log4j脆弱性　など

リモートアクセス製品の対策強化は、脆弱性対策が基本

侵入型ランサムウェア攻撃の初動対応のポイント（JPCERT/CC、2022年3月）
https://www.youtube.com/watch?v=nDOSn_ss7zI

脆弱性対策だけでは不十分なことも

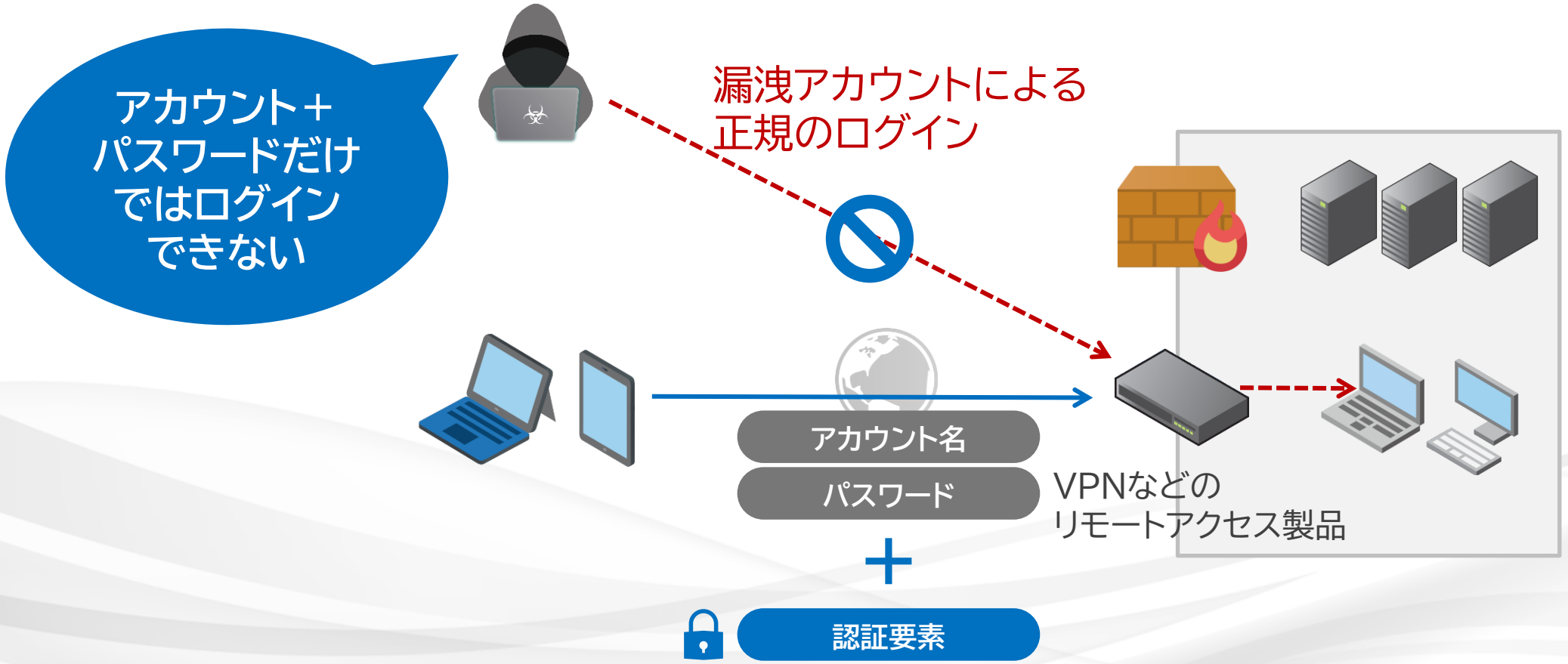
VPN機器での脆弱性公表～認証情報を悪用した攻撃のタイムライン例



漏洩済み認証情報を悪用した攻撃（脆弱性対策しても危険）

最近のサイバー攻撃とインシデント対応のポイント（JPCERT/CC，2021年2月）
https://www.isaca.gr.jp/cism/img/2021_kouen1.pdf
VPNのパスワードはどう流出したのか、国内企業を襲ったサイバー攻撃の真相（日経クロステック／日経NETWORK、2020.08.28）
https://xtech.nikkei.com/atcl/nxt/column/18/00001/04507/

リモートアクセス経由での侵入への対策



多要素認証によるリモートアクセス認証強化で、予防できる

多要素認証(Multi-Factor Authentication; MFA)

異なる複数の認証要素を組み合わせて認証を行う

知識

Something you know(SYK)

・導入運用は容易
・コピー可能であり、漏洩しやすい

所有

Something you have(SYH)

・導入運用性・コストのバランスから広く利用される
・USBキー、デジタル証明書など

通信確立時に認証するのはデジタル証明書だけ

生体

Something you are(SYA)

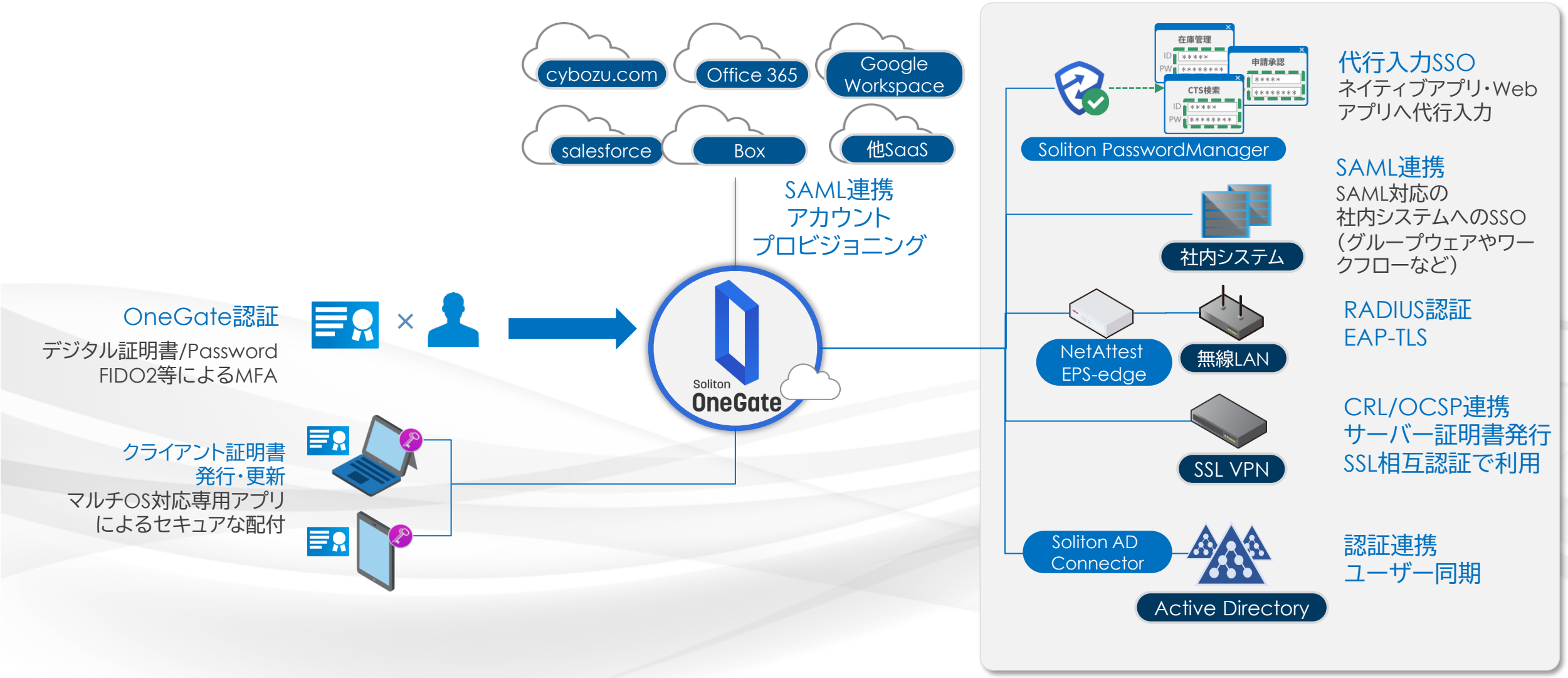
・導入・運用コストとも、比較的高め
・ユーザーの利便性が高い場合もある
・漏洩時の対応に限界がある
・指紋、顔、光彩、静脈など

デジタル証明書認証 vs 他の多要素認証

	デジタル証明書	他の多要素認証（所有、生体）
通信段階で認証できる	○ 攻撃者に、ログイン画面まで到達させない。ログイン画面の脆弱性攻撃にも効果あり。	× 攻撃者は、ログイン画面まで到達できてしまう
紛失時の対応	○ 証明書を失効させることで、確実に認証不可にできる。再発行すればよい。	△ 緊急時の代替認証の手順を整備する必要がある。物理デバイスの場合は代替機が必要。
様々な用途に活用できる	○ VPNだけでなく、無線LAN、クラウドサービスなど様々な認証に利用できる	△ 無線LAN認証に利用できないなど、用途が限られる
マルチOS	○ デジタル証明書自体は実績豊富で信頼性が高い技術。Windows, macOS, iOS, Android, Chromebookで実績あり	△ OSごとに、利用可能な認証要素が異なる場合がある

Soliton OneGate

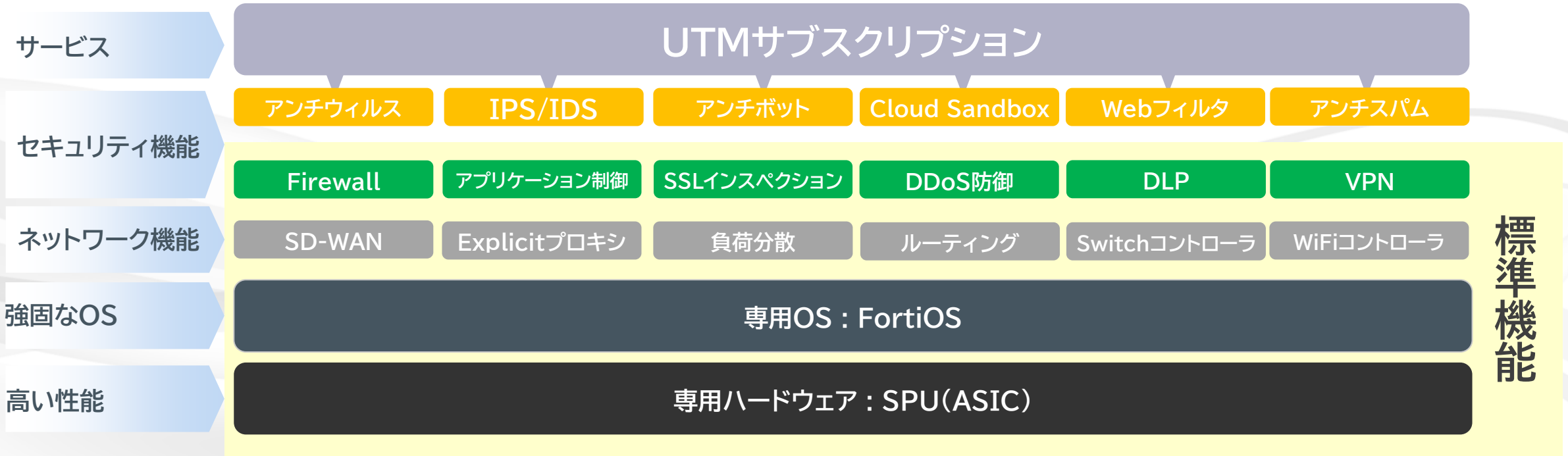
デジタル証明書(PKI)を活用した多要素認証で クラウドサービス・社内システムへのアクセスを安全に管理する



FortiGate + OneGateで実現するVPN認証強化

FortiGate とは

- 高機能複合脅威セキュリティアプライアンス
- セキュリティマーケットでシェアNo.1
- 幅広い機能に加えサブスクリプションライセンスでリアルタイム保護



FortiGateユーザー様からお伺いする課題

- 不正アクセスリスクが顕在化、対策必須に
  - ID/PASSだけの認証では不正アクセスを防げない
  - 多要素認証による認証強化が必要

- デバイス特定方法の見直し
  - MACアドレスベースのデバイス認証が出来なくなったことから、別の手段が必要
    - FortiClient（無償版） V6.2～、FortiClient（有償版）V7.0～

- クラウド活用も重要な経営課題、インフラ整備が必要
  - クラウドには社内を経由しない直接アクセスへ
  - 認証やネットワークなど、クラウド最適なインフラ整備が必要
    - 認証強化はVPNだけではない。クラウドアプリ、無線LANなどにも適用したい。

これらの課題は FortiGate + OneGate で解決できます！

FortiGate + Soliton OneGate 連携構成

SAML連携による構成（推奨）

- 強固な証明書認証をカンタン・安全に
- 未許可デバイスの接続ブロック
- ゼロトラスト時代の共通認証インフラに
- コストメリット

RADIUS連携による構成

- ゼロコンフィグの認証アプライアンスで簡単導入
- 同じアプライアンスをWi-Fi認証でも利用可能

LDAP連携による構成

- SSL証明書認で利用する証明書を発行
- コスト最優先時の構成

システム構成：SAML連携時（推奨構成）

・FortiGate上でSAML連携を有効化、連携先（信頼先）としてOneGateを設定
・FortiGate（SSL-VPN）の認証には、OneGateの認証機能を利用（認証画面リダイレクト）
・利用者は、OneGateで発行したクライアント証明書、FIDO2での生体認証、パスワード認証で、多要素認証によるSSL-VPN接続を行う
・パスワード認証利用時のID/PW確認は、OneGate →ADへ実施
・クラウドサービス利用時のデバイス制御、多要素認証＆SSOにも利用可能

SAML連携提案のメリット

① 強固な証明書認証をカンタン・安全に

認証局(CA)運用はクラウドサービスであるSoliton OneGateにおまかせ
Soliton OneGateでは、iOS/Androidでもカンタン・安全に証明書配付が可能

② 未許可デバイスの接続ブロック

Soliton OneGateでセキュアに証明書を配付、証明書未保持端末をブロック(デバイス認証)
FortiGate旧バージョンで実施していた「MACアドレス認証」よりも運用が楽！

③ ゼロトラスト時代の共通認証インフラに

クラウドサービス利用時の多要素認証、シングルサインオンにも利用可能
Wi-Fi接続時の証明書認証(802.1x/EAP-TLS認証)でも利用可能(要EPS-Edge)
利用アカウントをまとめて管理できる(AD連携も可能)

④ コストメリット

初期費用無し、月額300円/ユーザーで実現可能(推奨のSAML認証構成時)

パートナー様向け FortiGate＋OneGate連携提案メリット

- アップセル・クロスセルにつながる（案件単価UP）
  - 様々な切り口で提案できるので、VPN認証だけではなく、他課題で提案出来る可能性がある
  - ネットワーク認証として、Wi-Fi認証までカバーできる
  - 共通インフラとして利用出来ることで顧客の囲い込みが出来るため、アプリケーション認証へのアップセルや他サービスのクロスセルがやりやすい

- トレンドにあった提案できる
  - ゼロトラスト、クラウド志向の高い顧客にも受け入れやすい提案ができる

- 導入自体が楽、手離れが良い
  - 面倒な証明書配付方法やCAの運用を考えなくてよい
    - SAML認証構成なら、OneGateの証明書配付が利用できる。CA運用も考えなくてよい。

まとめ

- 侵入型ランサムウェア対策として、侵入経路であるVPNの認証強化は急務
- 証明書認証は、攻撃耐性が強い
- FortiGate + OneGateの連携により、
  強固な証明書認証を手軽・安価に実現可能

製品ページ https://www.soliton.co.jp/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

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