Zscalerを導入する事でのメリット

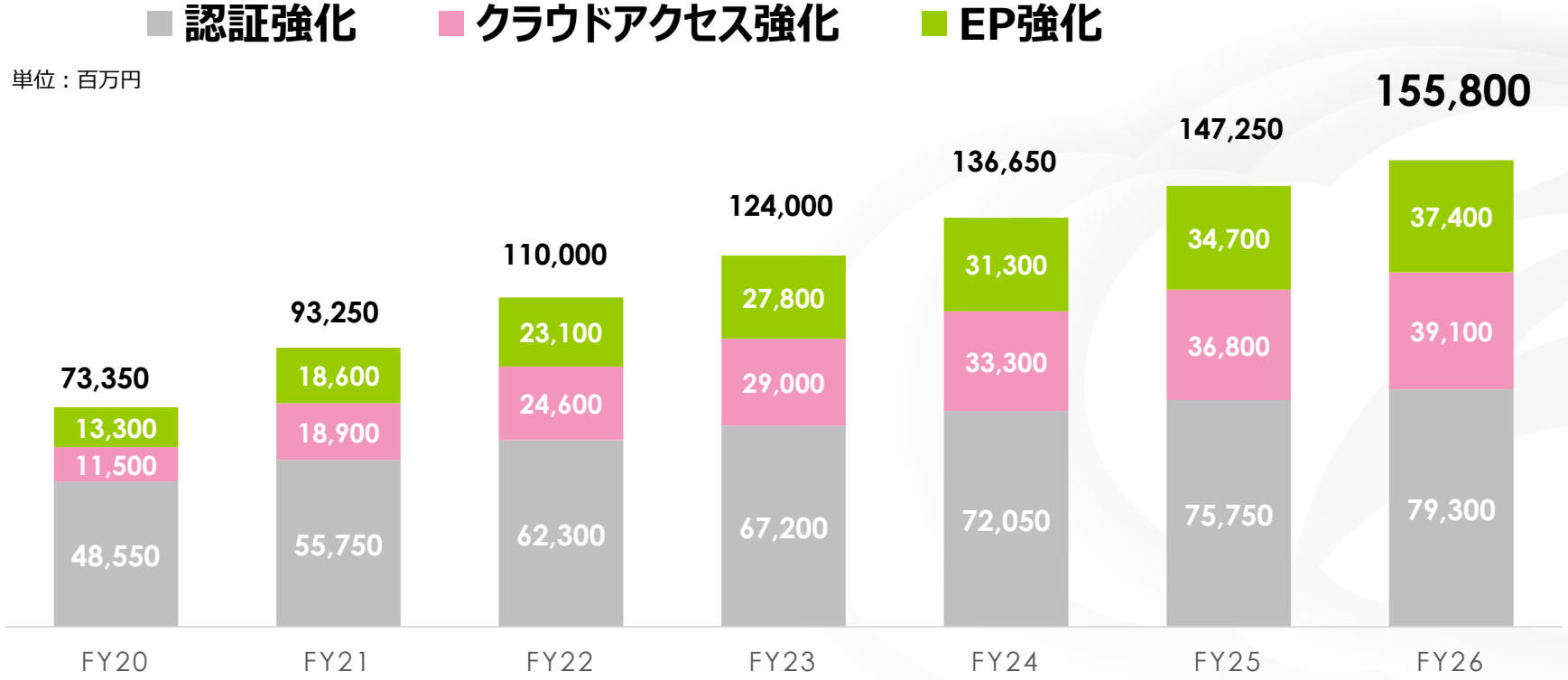
～ 未来をつくる、
新たな“次世代オールインターネット”プラットフォーム ～

企業の課題について

ゼロトラストの注目度の高まり

ゼロトラスト市場予測

CAGR:13.4%

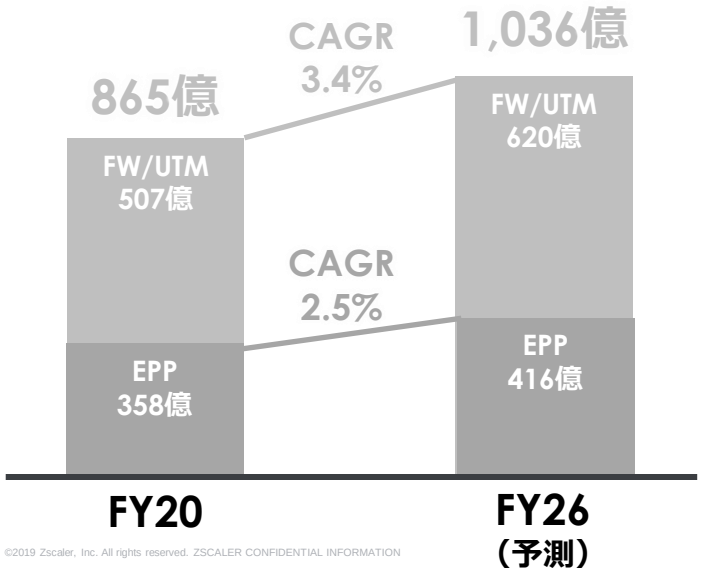


FY20→FY26で約2倍（1,500億超）の市場へ

出展：2021 ネットワーク セキュリティビジネス調査総覧市場編

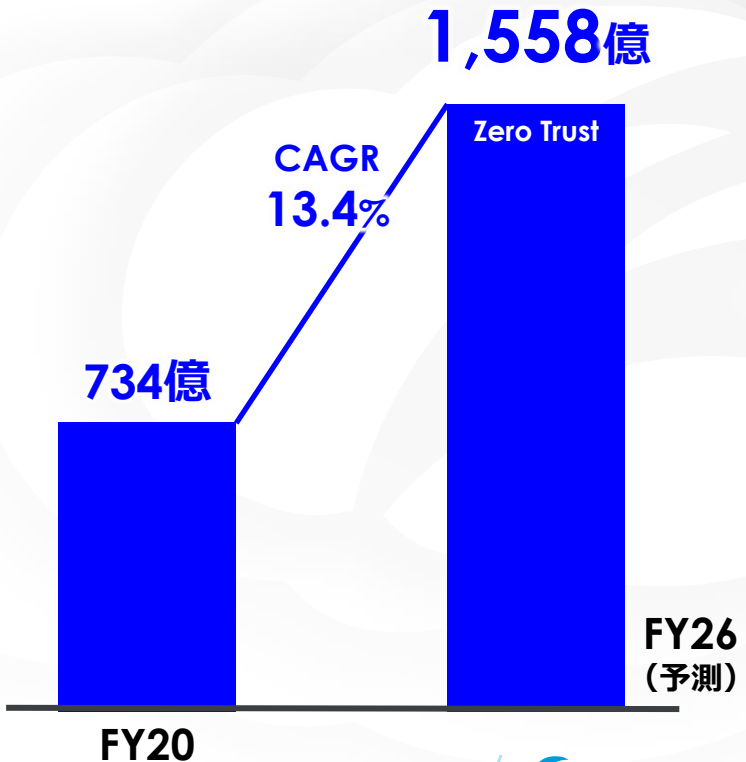
セキュリティ市場予測（従来型vsゼロトラスト）

従来型セキュリティ



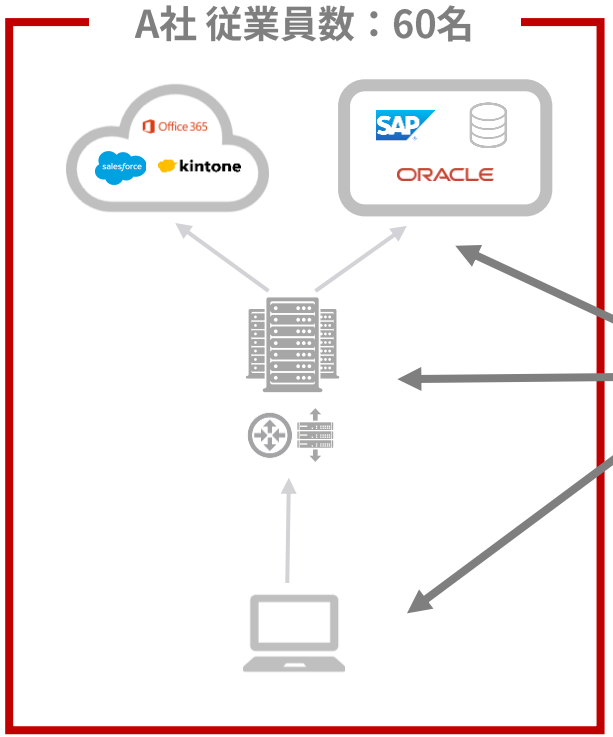
VS

ゼロトラストセキュリティ



中小企業特有の課題（1：人材不足）

情シス担当者が数名、もしくはいないため、**既存システムの維持稼働の負荷が高い**



①少ない人数で、
各システムや
機器のメンテナンスを
対応

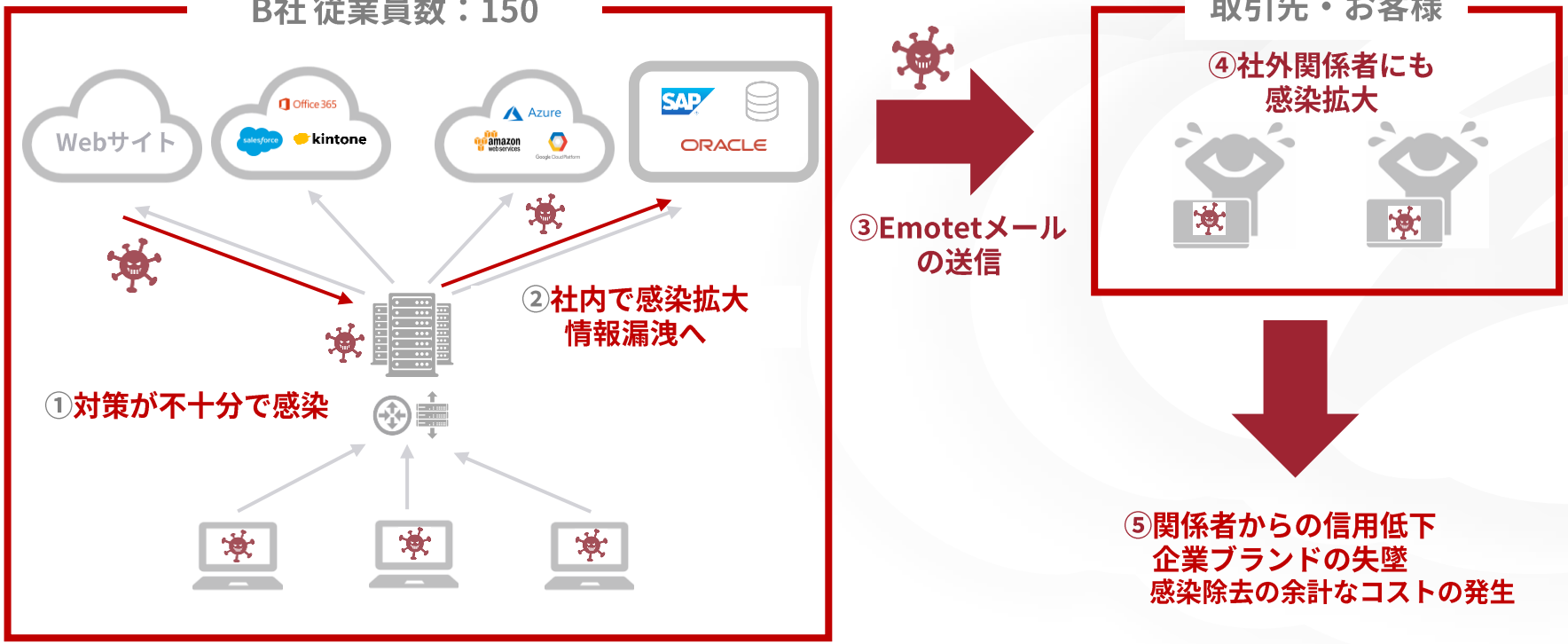
②既存環境の維持以外に稼働を割けない

③DX化が進められず、低い生産性のまま

④セキュリティも最新化できない

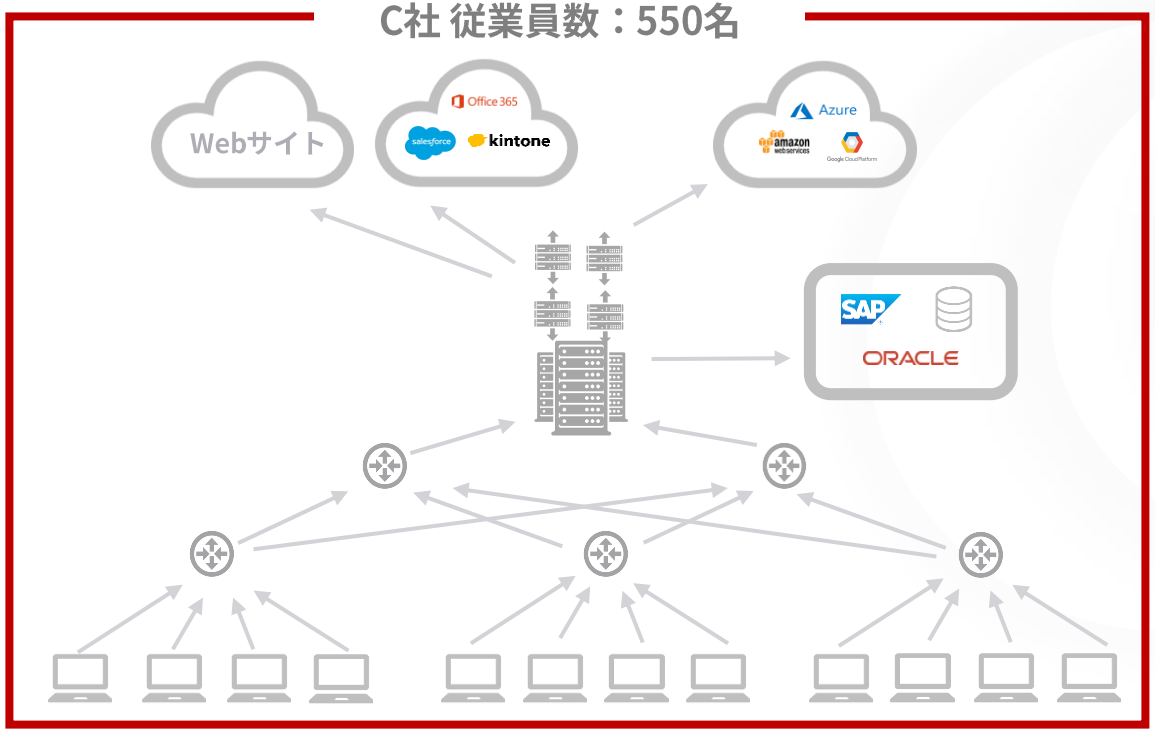
中小企業特有の課題（2：脆弱なセキュリティ環境）

セキュリティの最新化に力を割けず、**Emotet対策が不十分で感染。**
取引先、お客様にも感染を拡大させ、迷惑をかけてしまう



中小企業特有の課題（3：複雑なNW構成）

社内の**NW構成が属人的**で、その人が休んだり、退職すると**誰も手がつけられなくなる**
また、どのサービス・システムに**どのような経路で通信しているかわからない**



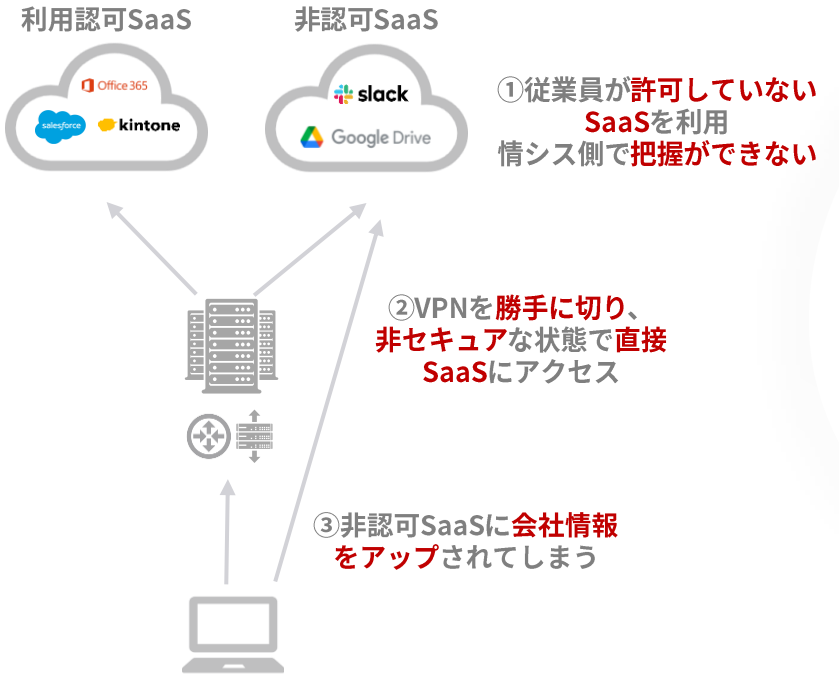
後任の担当者は**社内環境の解き明かし**が必要になる

本来必要のない業務で
時間と稼働を無駄にしてしまう

中小企業特有の課題（4：SaaSの可視化とガバナンス）

社員が**勝手にSaaSを利用**しており、
どのようなデータを誰が通信しているのか**全く把握できない**

D社 従業員数：300名



この課題によって生じる問題

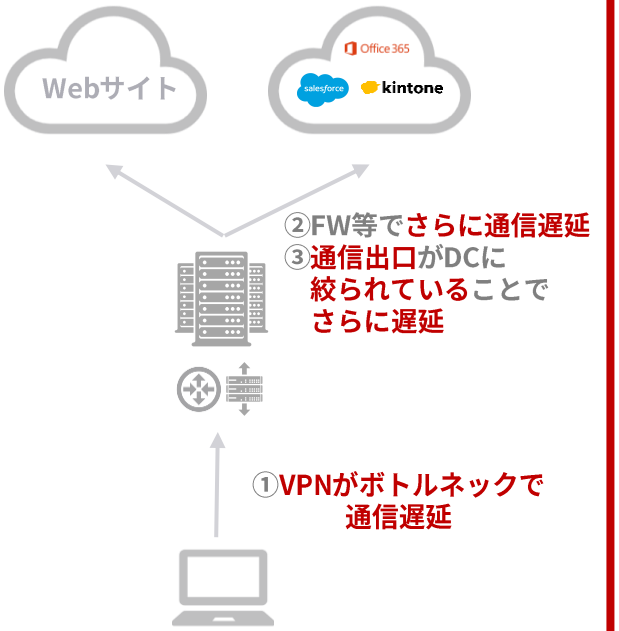
- 非認可SaaSのログを追えないので、
  誰が・いつ・どこに通信したか不明
- 危険なSaaSに非セキュアな状態で
  通信しているので、
  ウイルス感染の危険あり
- 会社情報の流出を
  故意・過失問わず防げない

中小企業特有のニーズ（1/2）

SaaSに移行したが、**NW構成はそのまま**なので
快適な通信というSaaSのメリットを活かせない

A社

生産性の観点でDXとは言い難い



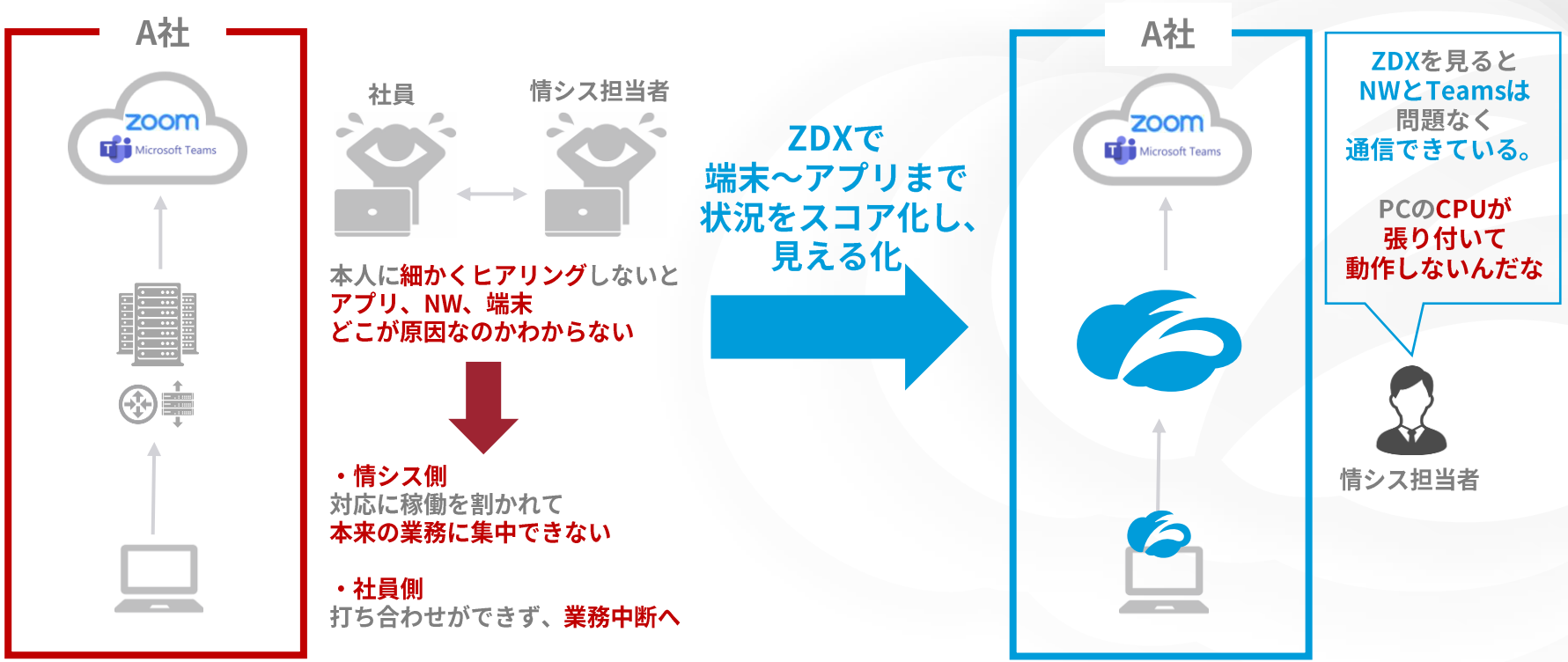
原因は
通信の**ボトルネックが**
多いこと

A社（A～D社全ての課題解決可能）

将来の拡張性も持った真のDX化へ

中小企業特有のニーズ（2/2）

リモート会議をすると、**頻繁に遅延や切断が起きる**

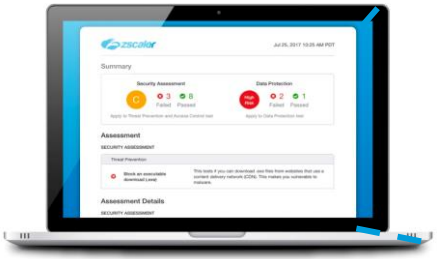


Appendix

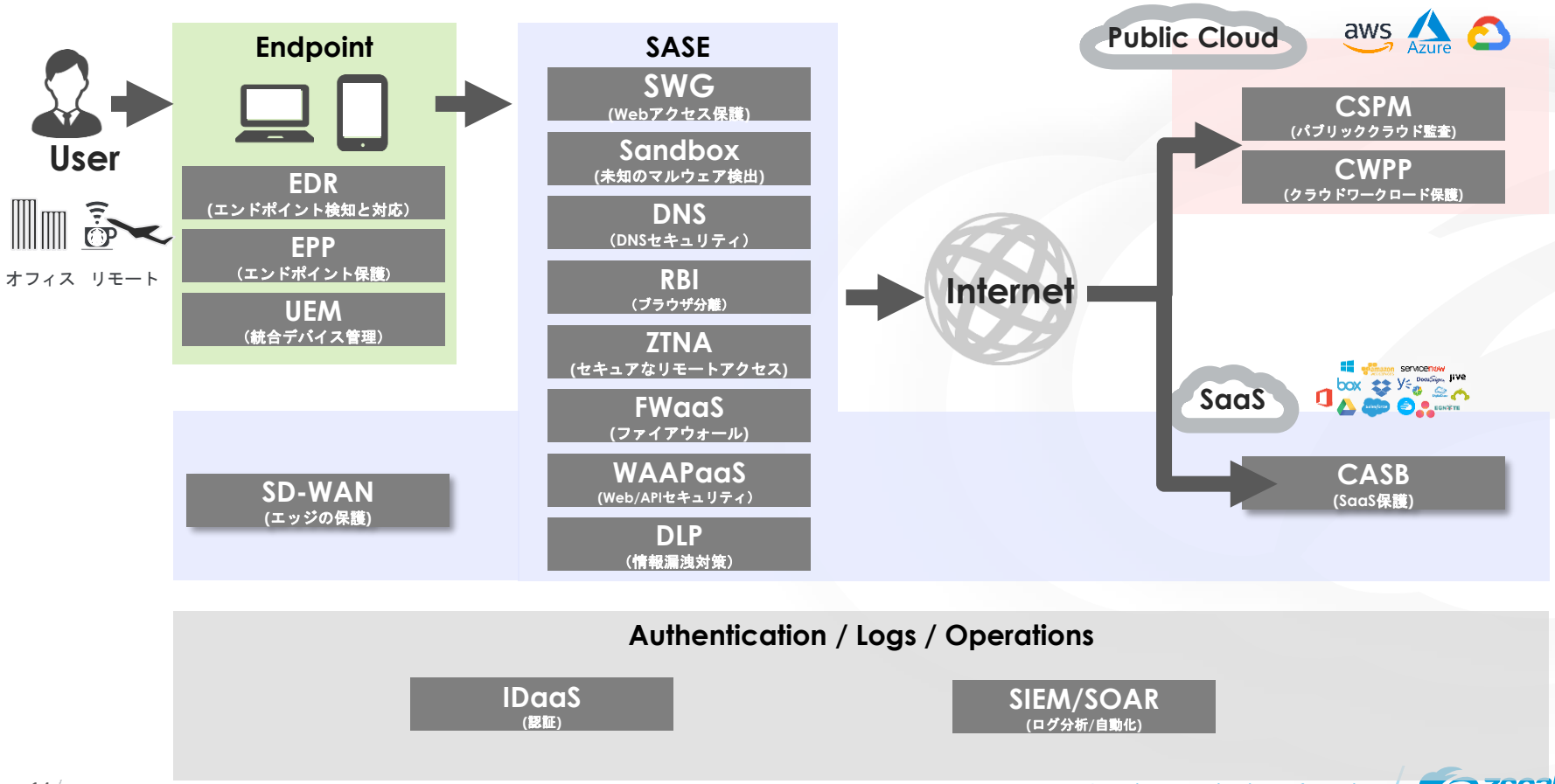
まず始めに: 現状のインターネット脅威に対する対応状況

セキュリティレベルを診断しましょう（クリック）

Zscalerによる即座のリスク評価、Security Previewでセキュリティの強度を確認しましょう。こちらは無料で利用でき、情報が外部に公開されることはありません。このリスク評価を実行した企業の85%において、直ちに対応が必要な脆弱性が見つかっています。



ZeroTrust ポートフォリオ



情報セキュリティ10大脅威への対応について

ZscalerでIPA発表の情報セキュリティ10大脅威への対応が可能に

■「情報セキュリティ10大脅威 2023」 圏外：昨年はランクインしなかった脅威

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

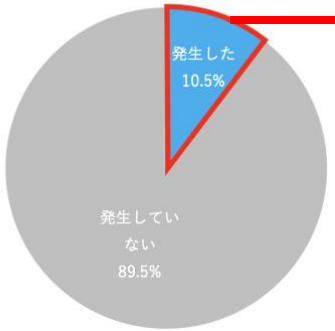
Zscalerの機能でそれぞれ対策可能です

中小企業の情報セキュリティのトラブルについて

Zscalerで**中小企業で起こりがちなインシデントやトラブルの防止**が可能に

過去3年間にサイバーセキュリティ上の事故やトラブルが発生したか

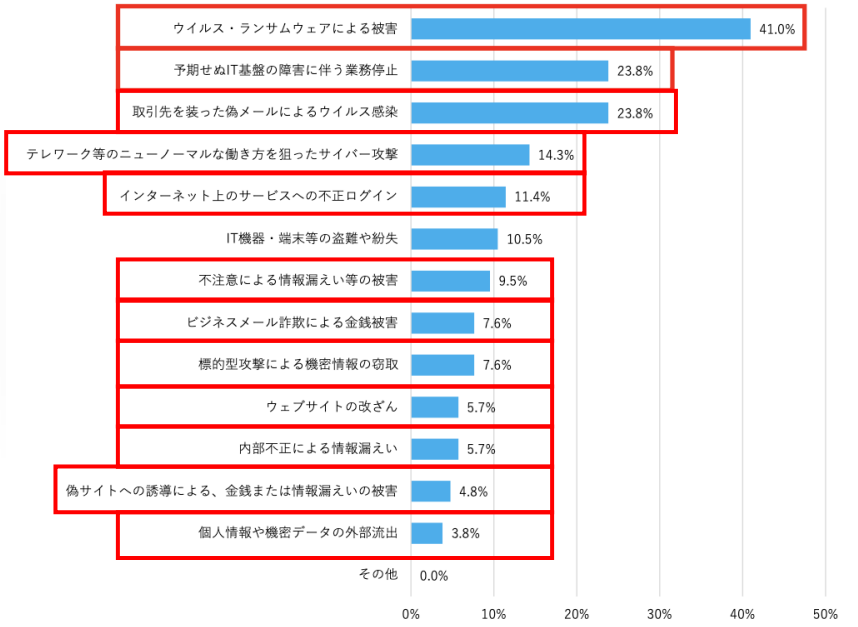
（n=中小企業に勤務する人 1,000人／単回答）



Zscalerで防止できるインシデント

過去3年間で発生したサイバーセキュリティ上の事故やトラブルの内容

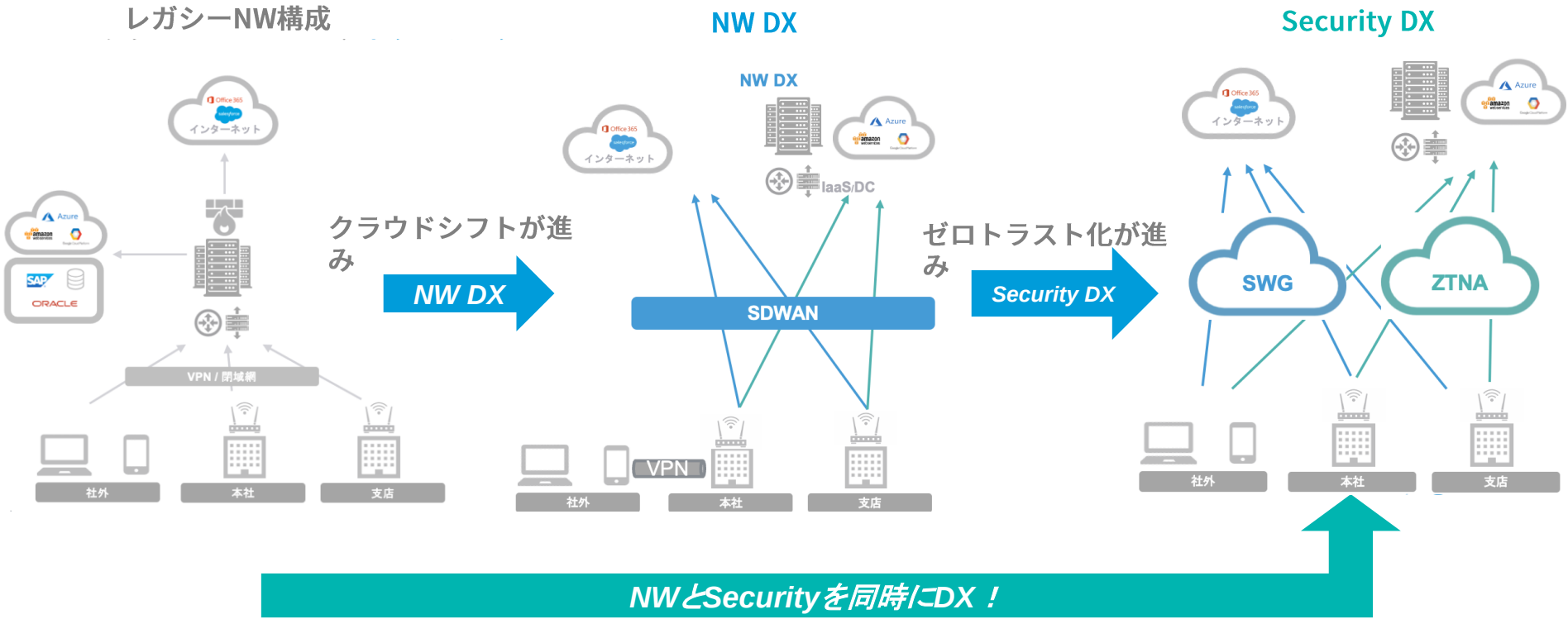
（n=過去3年間でサイバーセキュリティ上のトラブルが発生した中小企業に勤務する人 105人／複数回答可）



出典：IPA　中小企業従業員アンケート

ネットワーク環境におけるニーズの変化

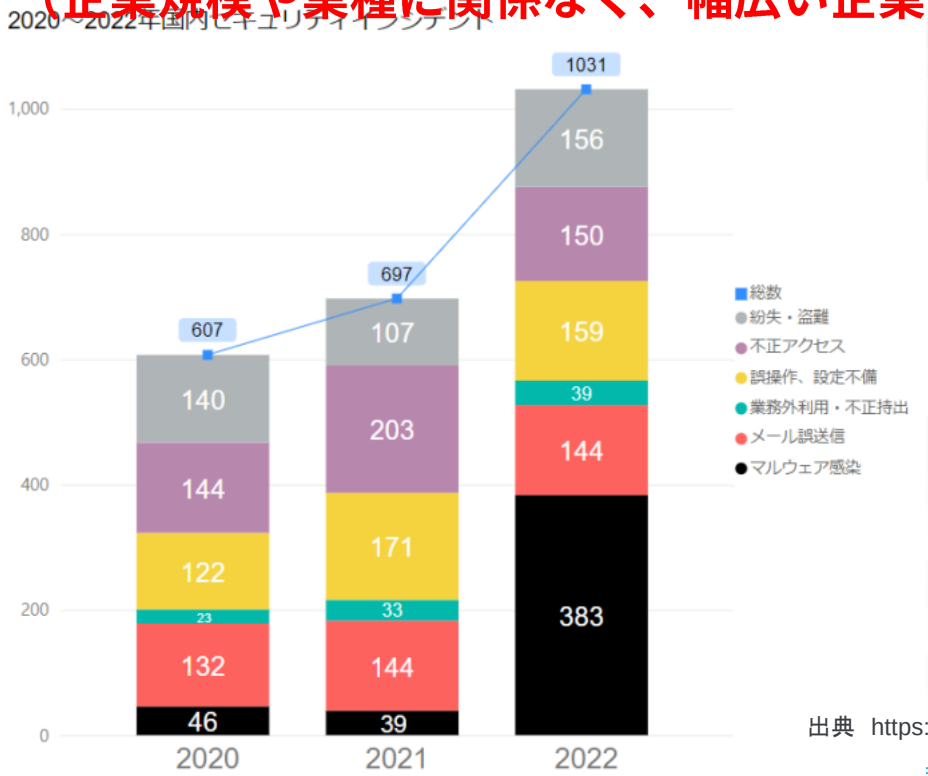
クラウドシフトに伴い、**ネットワークとセキュリティのシンプル化**が進んでいます



（参考）国内でのセキュリティインシデントの状況

組織やマスコミから報道公開されたマルウェア感染が前年比約10倍と爆発的に増加

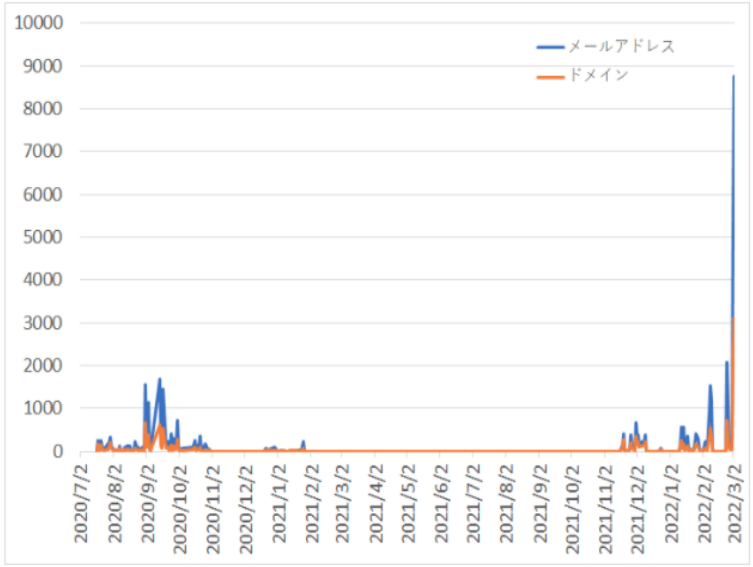
（企業規模や業種に関係なく、幅広い企業が感染被害）

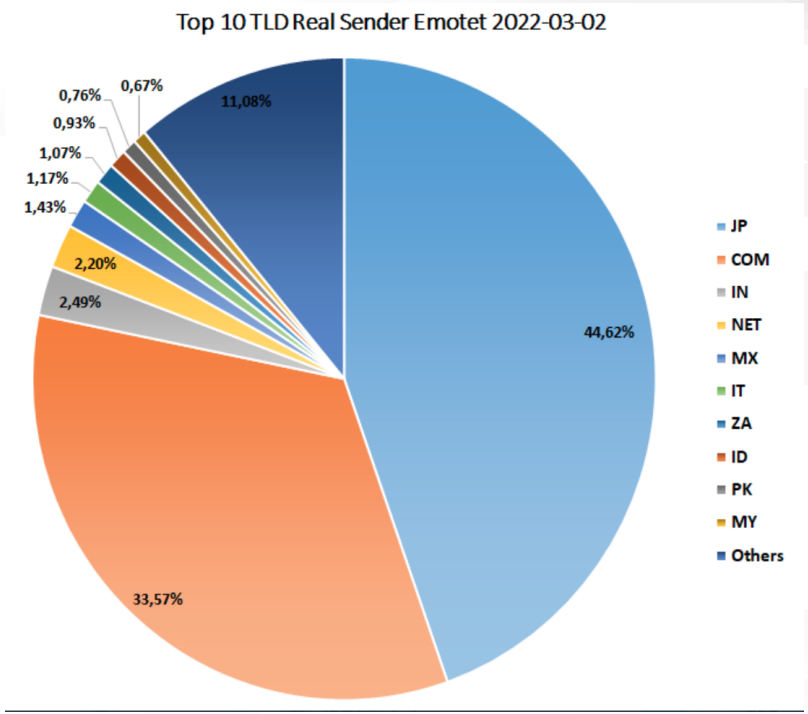


出典　https://www.agara.co.jp/article/253366

（参考）国内でのEmotetの感染拡大について

日本での**感染が拡大**し、**Emotet**メール送信元として**世界No1**になってしまう





［図1： Emotetに感染しメール送信に悪用される可能性のあるjpメールアドレス数の新規観測の推移 (外部からの提供観測情報) (2022年3月3日更新) ］

サイバーセキュリティ経営ガイドラインの更新

昨今のサイバー攻撃の情勢を受けて、より具体的な内容にまもなく更新予定

Ver 2.0 （現在）		Ver 3.0 （まもなく）
セキュリティ対策の実施を「コスト」と捉えるのではなく、 将来の事業活動・成長に必要なものと位置付けて「投資」 と捉えることが重要	成長への投資 セキュリティの捉え方	サイバーセキュリティ対策は 「投資」 (将来の事業活動・成長に必須な費用) と位置付けることが重要。 企業活動におけるコストや損失を減らすために必要不可欠な投資
セキュリティ投資は 必要不可欠かつ経営者としての責務	より重い責任 セキュリティの責任	サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、 企業として果たすべき社会的責任であり、 その実施は経営者としての責務
経営責任や法的責任が問われる可能性がある	より重い責任 ステークホルダーへの責任	善管注意義務違反や任務懈怠に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う

Emotet防御の実績_Zscaler日本国内のお客様

Sandbox推奨ではあるものの、ATPのみでも、Emotet防御の実績あり

お客様	概要	拠点 / 規模	ご利用製品
A社様（製造業 / 化学・電子部材）	全社員のインターネットアクセス用	国内・アジア・欧米 5万 user	ZIA-Business - AV ：◯ - ATP ：◯ - Adv FW ：× - Adv Sandbox：×
B社様（製造業 / 電気・電子）	全社員のインターネットアクセス用	国内・関係会社・海外拠点 3.5万 user	ZIA-Transformation - AV ：◯ - ATP ：◯ - Adv FW ：◯ - Adv Sandbox：◯
C社様（製造業 / 電気・電子）	全社員のインターネットアクセス用	国内・関係会社・海外拠点 2万 user	ZIA-Business - AV ：◯ - ATP ：◯ - Adv FW ：× - Adv Sandbox：×
D社様（製造業 / 部品メーカー）	全社員のインターネットアクセス用	国内・アジア・国内関係会社 1万 user	ZIA-Business - AV ：◯ - ATP ：◯ - Adv FW ：× - Adv Sandbox：×

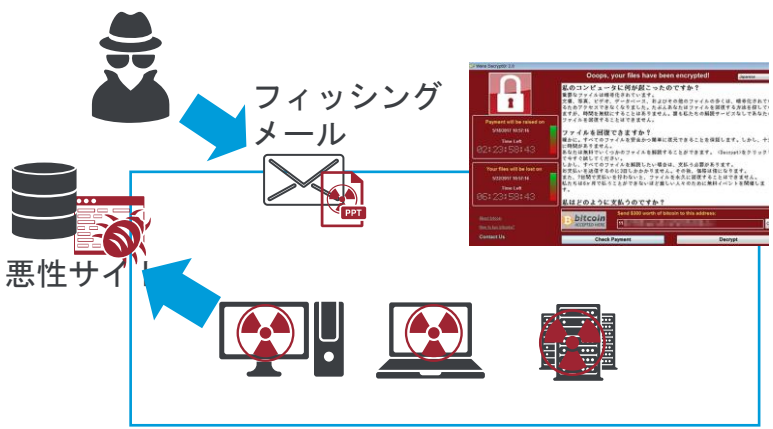
*その他、金融系企業様でも防御出来たことが確認出来ております。

ランサムウェアの進化（1/2）

攻撃手法がより高度になり、**身代金を支払わざるを得ない**ような状況を作り出されてしまう

従来のランサムウェア

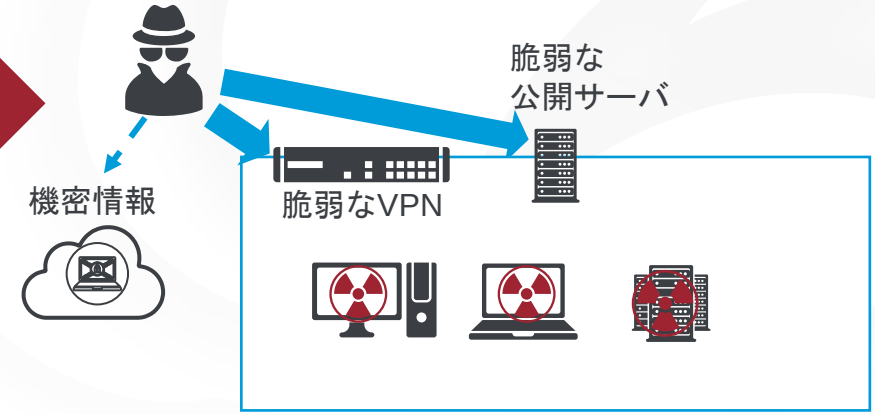
フィッシングメールや**悪性サイト**で**感染**させ
重要資産を暗号化し
復号キーを渡す代わりに金銭を要求



手口が巧妙化

二重強迫型のランサムウェア

攻撃者の手により**高度な手法で進入**
重要資産の暗号化及び、**データ公開脅迫**で
金銭を要求

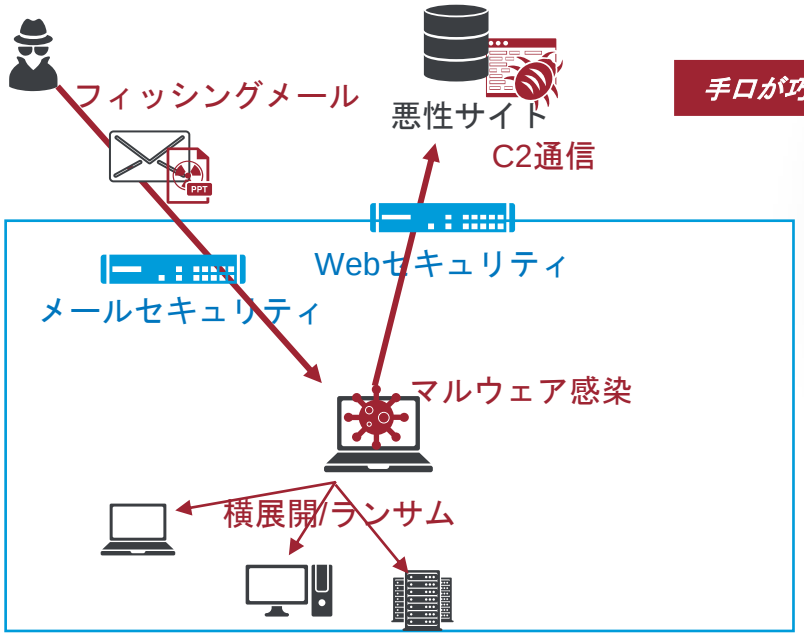


ランサムウェアの進化（1/2）

攻撃を避けるため、**ネットワーク全体で対策**が必要になっている

従来の侵入方法

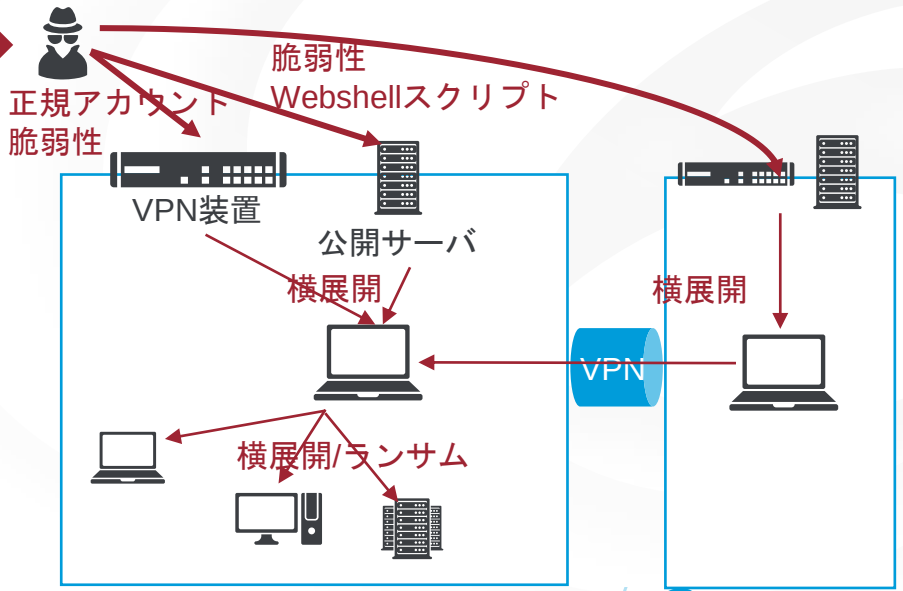
初期侵入と経路が限定的で
メール/Webセキュリティによる対策が非常に重要



手口が巧妙化

現在の侵入方法

インターネットに面する**全システムをターゲット**に
対策が弱い部分から侵入し、
ラテラルムーブメントにより**感染拡大**



（参考）VPN機器の脆弱性を悪用した攻撃（1/2）

朝日新聞デジタル ＞ 記事

VPN欠陥つくサイバー攻撃　国内外900社の情報流出

会員記事

2020年8月25日 11時58分

シェア　ツイート　ブックマーク　メール　印刷

list　24

社外から企業内のネットワークに接続するときに使う「仮想プライベートネットワーク（VPN）」の 通信機器 の欠陥をついたとみられる サイバー攻撃 があり、国内外900社が機器を使う際の情報が流出していたことが内閣サイバーセキュリティセンター（NISC）への取材でわかった。VPNは テレワーク の拡大もあり、利用者が広がっている。

出典：朝日新聞デジタル

「急遽テレワーク導入」に落とし穴　国内約40社が被害
「VPN不正アクセス事件」が他人事とは限らない理由 (1/3)

2020年09月08日 07時00分 公開　[高橋睦美，ITmed

印刷　55　Share　B! 7　0

新型コロナウイルスの感染拡大に伴い、リモートワークが広がる中、8月下旬に「VPN（Virtual Private Network）のアカウント情報が盗まれ、ネット上で公開された」という事件がメディアを賑わせました。VPN接続に利用されるパルセキュア社の製品の脆弱（ぜいじゃく）性を突かれてアカウント情報が盗まれたというものです。世界で約900社が被害を受け、中には約40社の日本企業も含まれていました。新聞の一面を飾ったこともあり、「うちの会社は大丈夫か？　同じような攻撃を受けないか？」と不安に感じた読者もいるのではないでしょうか。

もしかすると「このベンダーの製品を使っていないから大丈夫」と思われた方もいるかもしれません。ですが、実はそうとは限りません。この一件にはいくつか他山の石にしたいポイントがあります。

出典：IT Media

日本経済新聞

朝刊・夕刊　ストーリー

トップ　速報　マネー　経済・金融　政治　ビジネス　マーケット　テクノロジー　国際　オピニオン　スポーツ　社会

VPN脆弱性対応、日本企業に隙 「ゼロトラスト」不可欠
暗証番号など流出

データの世紀

2020/8/24 21:40 | 日本経済新聞　電子版

保存　共有　その他

不正侵入を前提とした「ゼロトラスト」（信頼しない）と呼ばれる対策が求められている

安心してデータをやり取りする仕組みが逆にサイバー攻撃の標的になった。38社の日本企業を含む約900社について、社内システムに接続するVPN（仮想私設網）の暗証番号などが流出した。日本企業がテレワークを急拡大する中、セキュリティー対策も一新する必要性が浮かぶ。不正侵入を前提とした「ゼロトラスト」と呼ばれる対策が求められている。

出典：日本経済新聞

（参考）VPN機器の脆弱性を悪用した攻撃（2/2）

小島プレス工業株式会社　システム停止事案調査報告書（第１報）

小島プレス工業株式会社（以下、「当社」といいます。）は、３月１日付け「ウィルス感染被害によるシステム停止事案発生のお知らせ」にてシステム障害発生等について公表したとおり、当社ファイルサーバが第三者による不正アクセスを受けた（以下、「本件」といいます。）ことを確認し、さらなる攻撃予防のため取引先様及び外部とのネットワークを遮断しました。

当社は、ネットワーク遮断後、緊急対策本部を立ち上げ、侵害調査と緊急対策のために、外部のセキュリティ専門家を起用し、本件被害の全容解明と復旧、さらには再発防止に向けて総力を挙げて取り組んでいるところです。

お客様、取引先様をはじめとする関係者の皆様には、多大なるご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。

現在判明している事実関係およびこれまでの当社の対応についてお知らせいたします。

なお、判明した事実のうち一部は二次的影響を鑑みて非公表とさせていただいておりますが、関係官庁ならびに警察関係者には詳細を相談しております。ご理解ご容赦のほどお願い申し上げます。

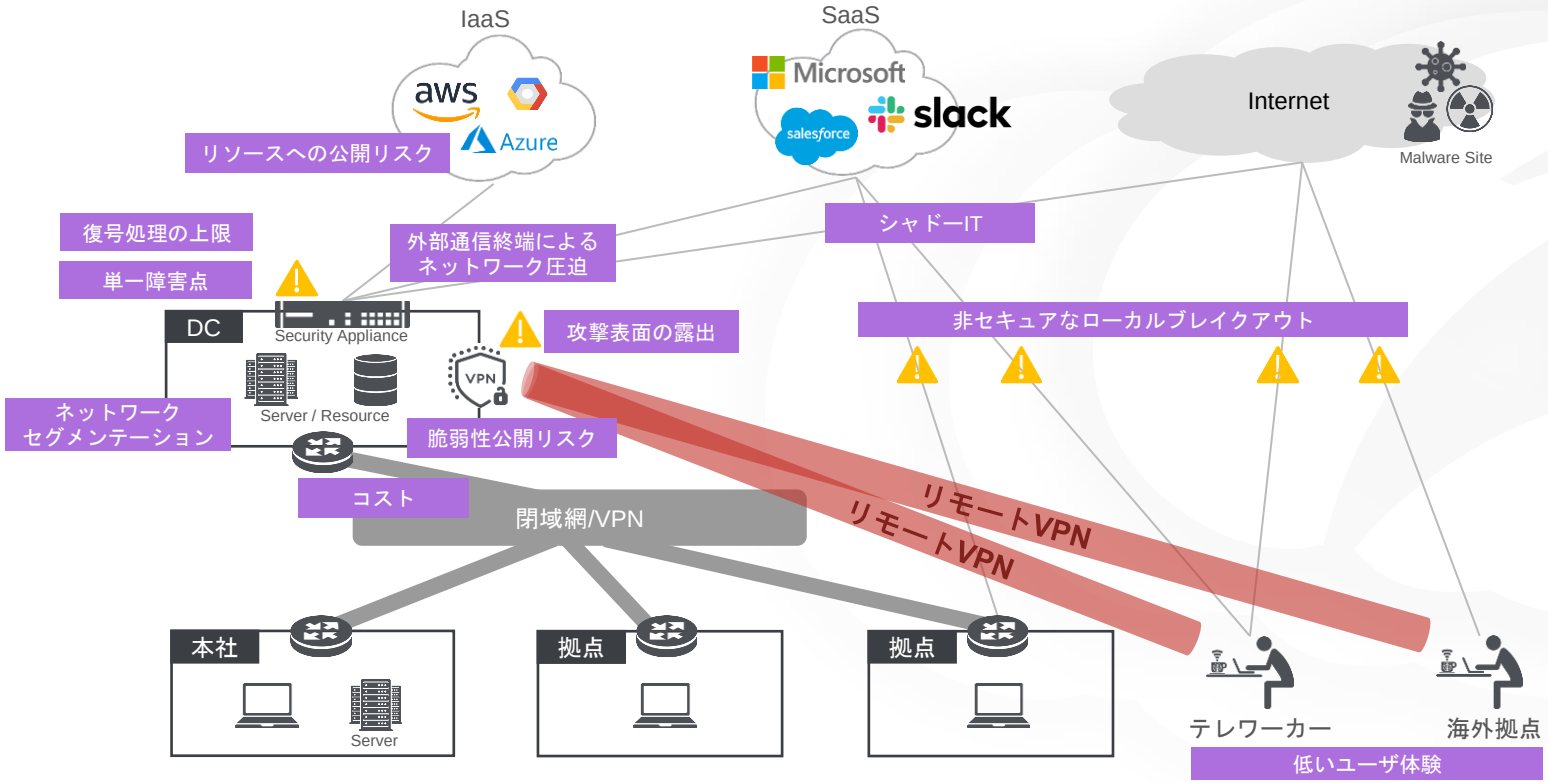
１．現段階で判明している事実

【侵害経路の概要】

本件の外部不正アクセスは、子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器に脆弱性があり、そのことがきっかけとなり不正アクセスを受けました。攻撃者はそのリモート接続機器から子会社内のネットワークに侵入し、さらに当社内ネットワークへ侵入して、２月 26 日 20 時過ぎにサーバやパソコン端末へ攻撃を受けた痕跡を確認しています。

Zscaler導入前 (As Is)

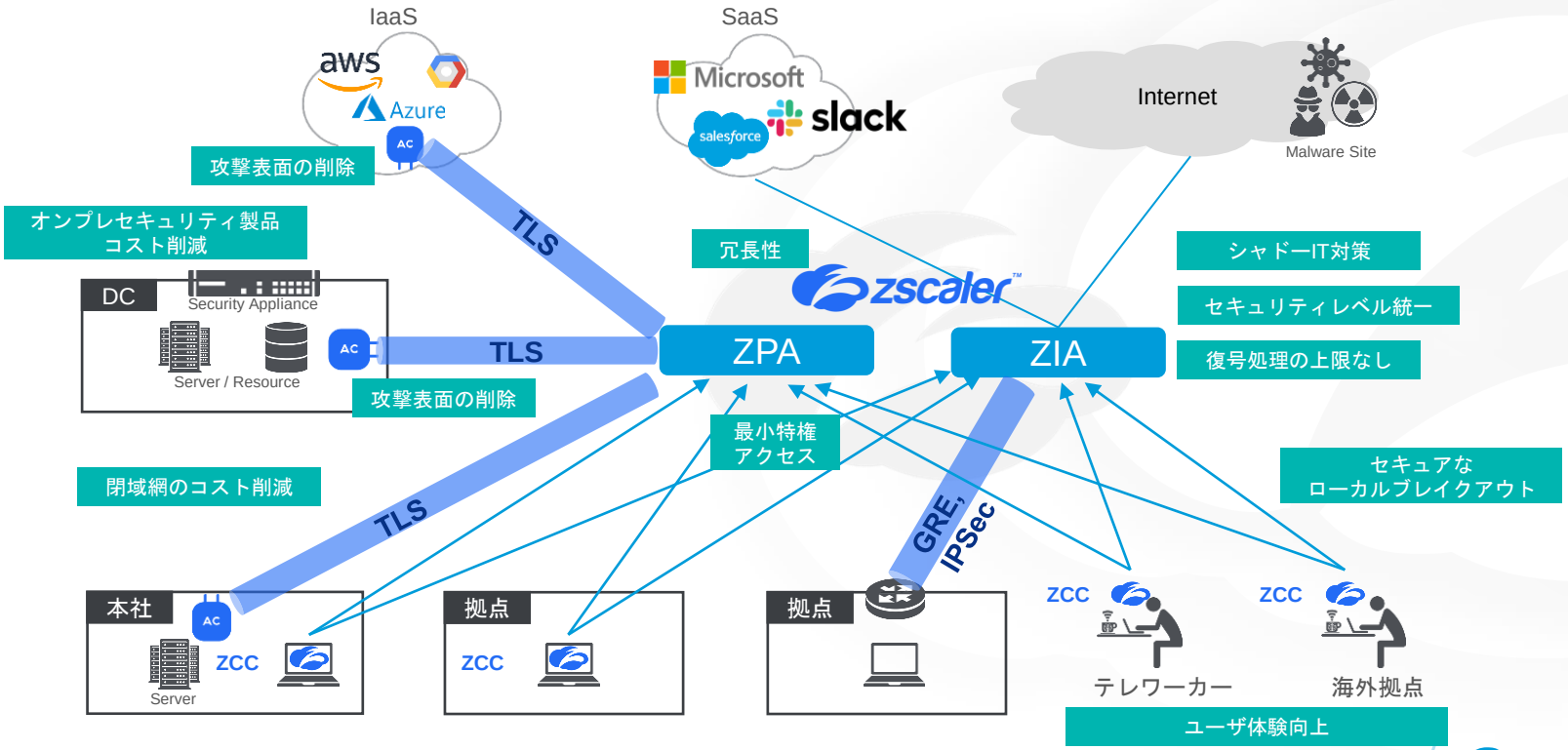
従来のネットワークモデルでは、**課題が多発**



ZIA、ZPA導入後（To Be像）

脱閉域網で、**オールインターネット/セキュアなローカルブレイクアウトへ**

DX推進の効果を最大化へ



脅威に対する多層防御

Zscalerではサイバー攻撃の各フェーズにおいて多層防御が可能

サイバー攻撃の流れ

Full SSL Inspection

不要なサイト・未知カテゴリへのアクセス制御
既知マルウェアファイルのブロック

URLフィルタリング & CASB

マルウェアプロテクション

レピュテーションベースでの制御
IPS シグネチャ・AI/MLでの解析
Web・非Webに対する防御

Advanced Cloud Firewall with IPS

高度な脅威保護

DNS Security

振る舞い分析
世界中で検知された脅威は即時シェアされる

クラウドサンドボックス

Browser and Document Isolation

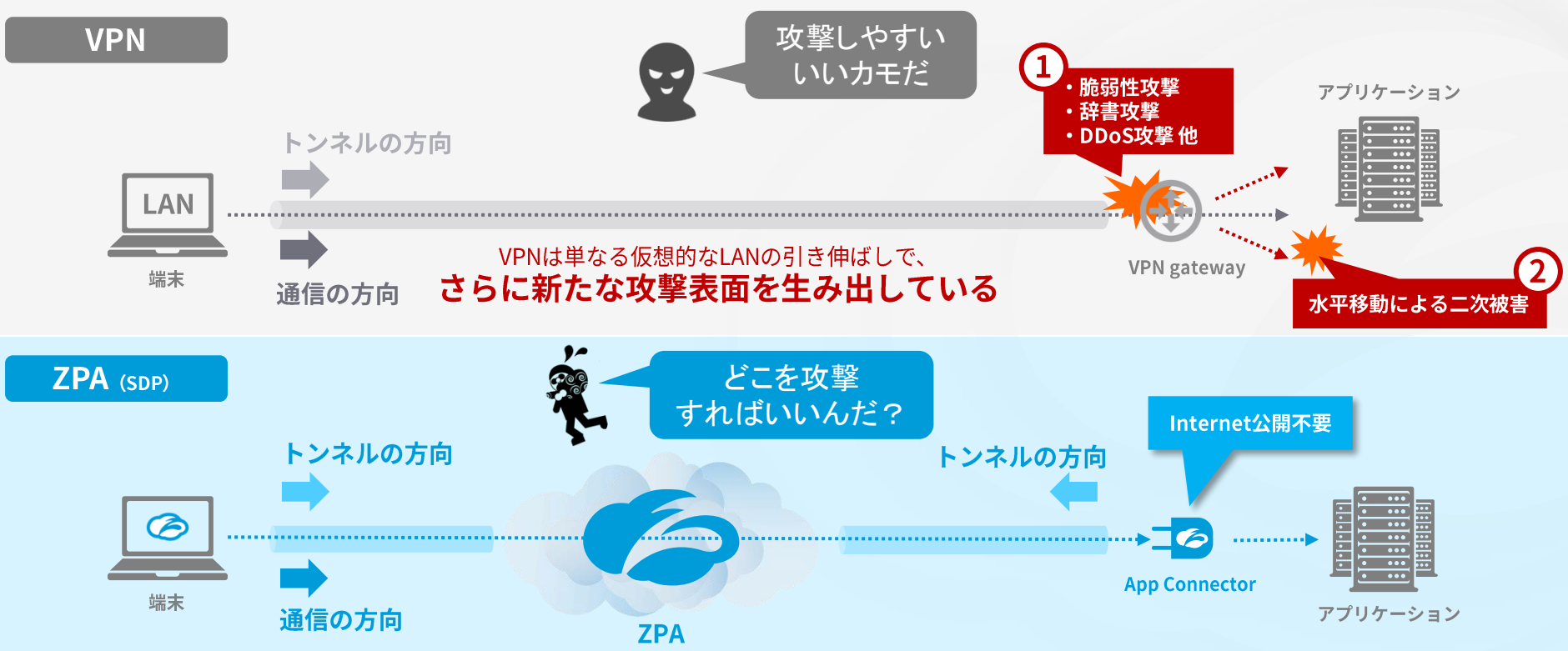
Data Protection

DLP

ZPA

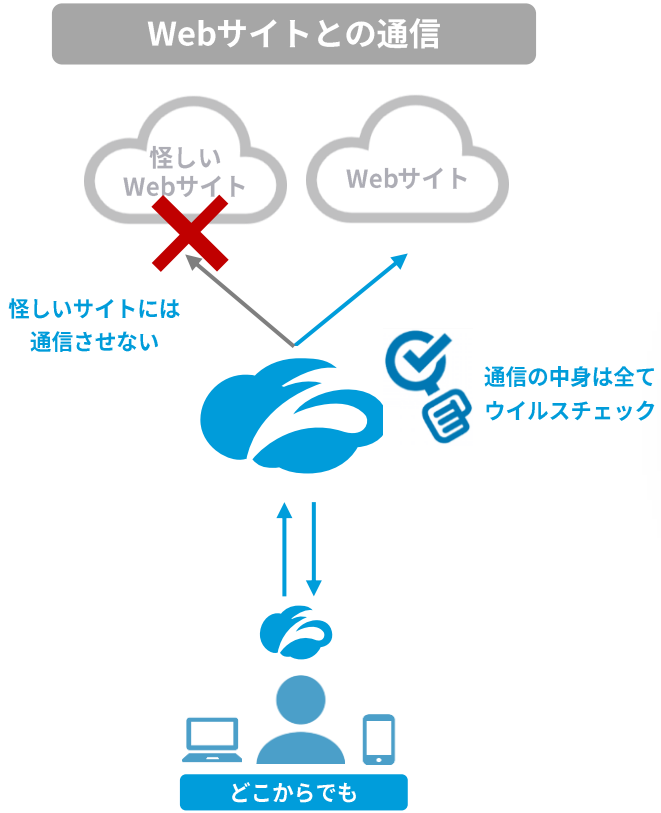
脅威に対する多層防御（ZPA）

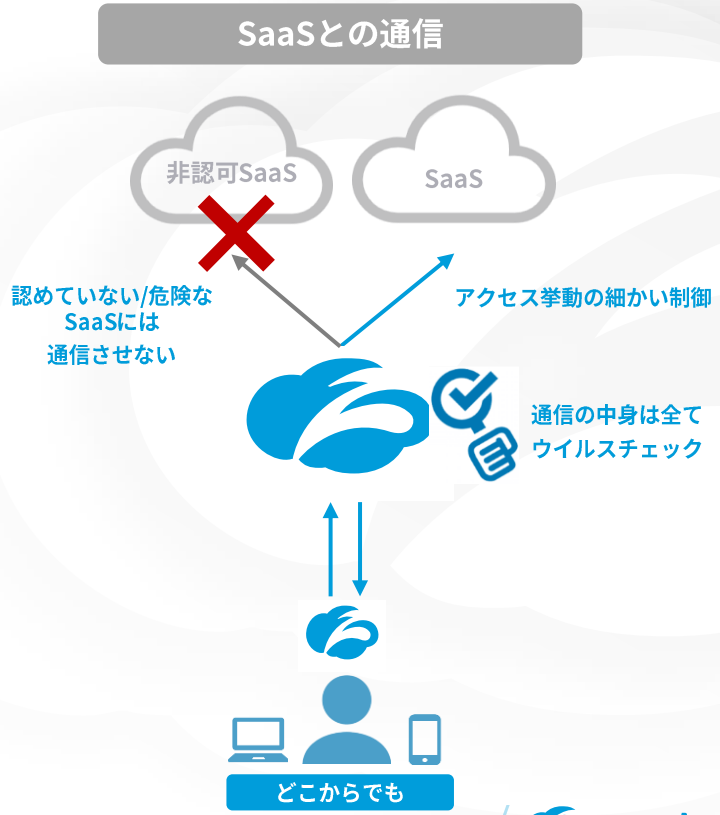
ZPAでそもそも攻撃させない・攻撃できない環境を実現



脅威に対する多層防御（ZIA）

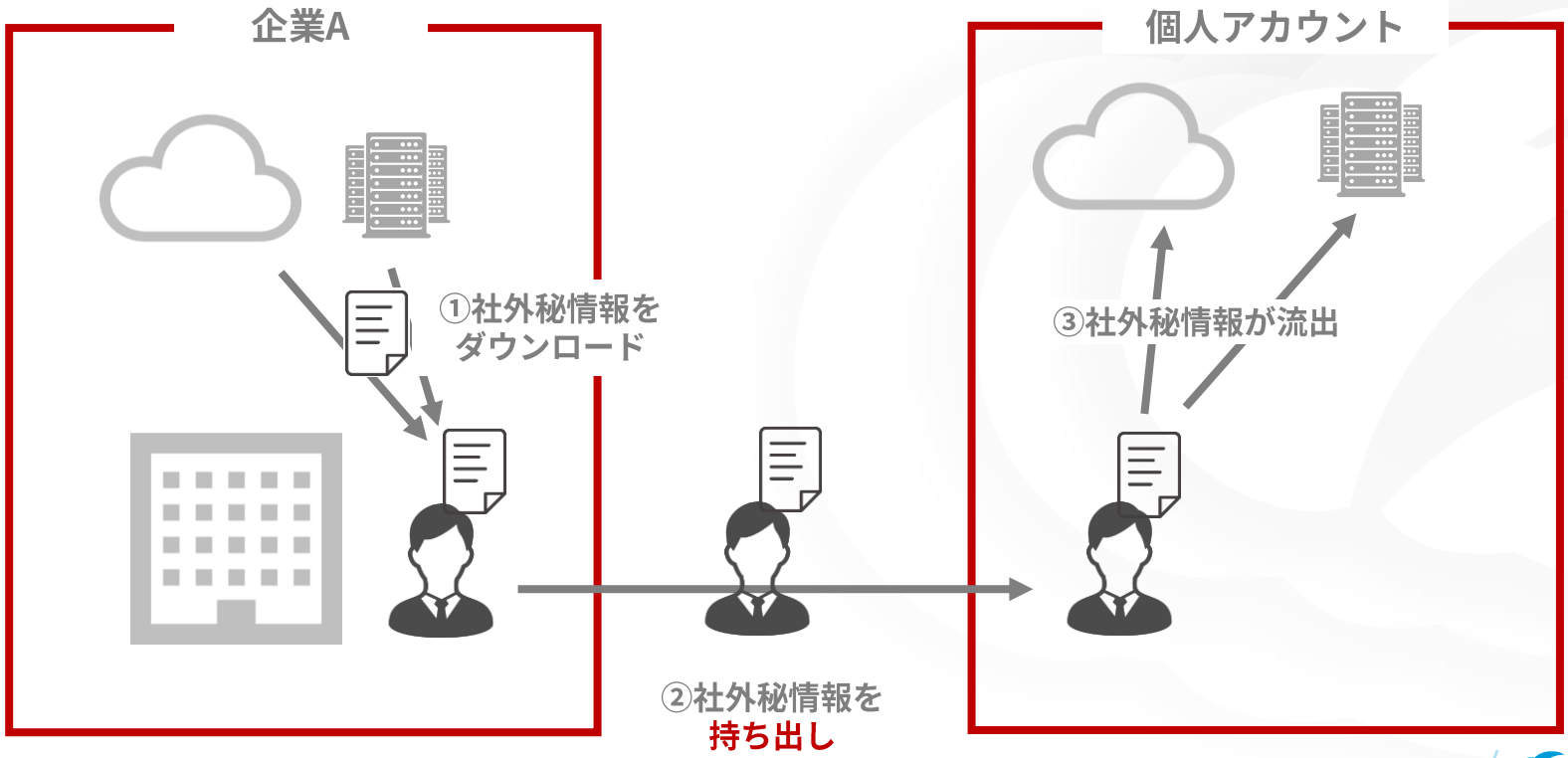
ZIAで怪しい通信をさせない・最新のウイルス検査環境を実現





情報流出の課題

従業員に**顧客情報等の社外秘情報を勝手に持ち出され、情報が流出してしまう**



Zscalerの情報漏洩対策方法