中堅中小企業におけるセキュリティ対策現場での取組

S&J株式会社
コンサルティング事業部
上原 孝之

Agenda

１．IT環境の変化と求められる対策

２．効果的なエンドポイントセキュリティ強化策

会社紹介

会社名	：	Ｓ＆Ｊ株式会社
代表	：	三輪 信雄
設立	：	2008年11月7日
住所	：	東京都港区西新橋2-4-12 西新橋PR-EX8階
資本金	：	4865万円
従業員数	：	66名（2022年2月現在）
許認可	：	ISMS（ISO27001）

Ｓ＆Ｊ＝ 千里眼と順風耳

西遊記にも登場する「千里眼」と「順風耳」は対になっていて、ともに媽姐(天上聖母菩薩)の守護神です。

千里眼(青鬼) は媽姐の進む先やその回りを監視します。

順風耳(赤鬼)は悪の兆候や悪巧みを聞き分けて、いち早く媽姐に知らせる役を持っています。

平時からインシデントの兆候を探り（検知）、事前に手を打ち（防御）、

事故が起こった際にも迅速に対応して（対応）、被害を最小限に

食い止めるようなサービスを提供したい、との思いが込められています

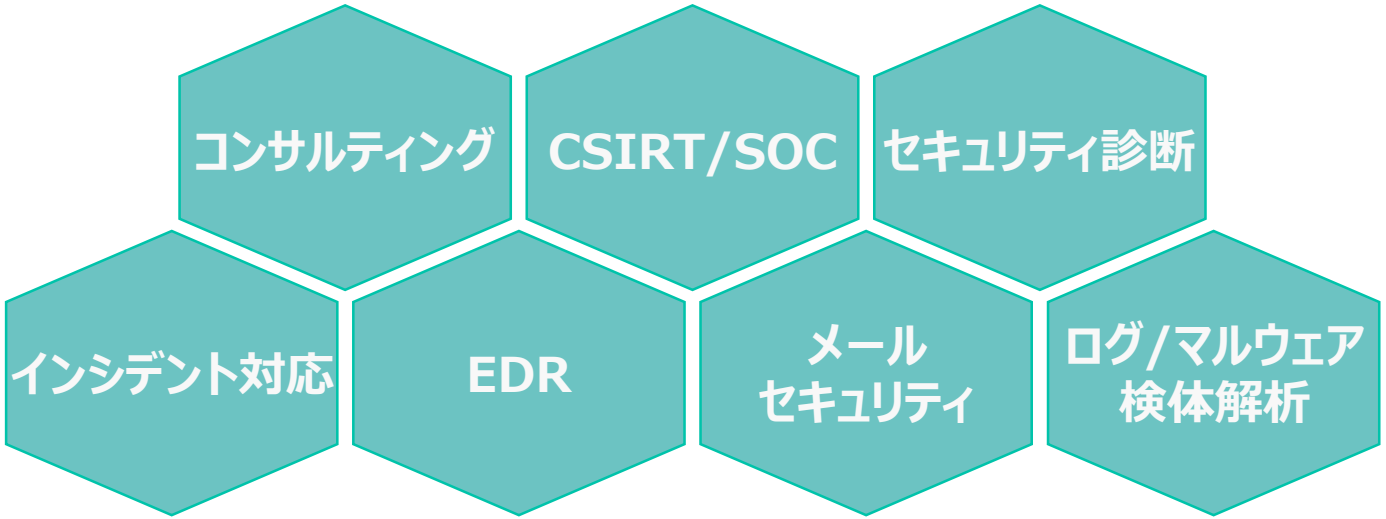
事業紹介

セキュリティエキスパート集団として、以下のサービスを提供いたします。

● いち早く予兆を検知し、対処できる態勢づくりや構築の支援

● やり過ぎず、不足しない、変化に合わせた最適なサービス

政府機関や大手民間企業におけるセキュリティアドバイザーやセキュリティ対策構築・運用、インシデント対応などの豊富な経験から、
お客様に最適で効果的なセキュリティ運用サービスを提供しています。
お客様からの高い要求に応えるため、効果的でより良いサービスの開発に積極的に取り込んでおります。
IT やセキュリティの視点のみならず、お客様の事業視点、経営視点で、セキュリティサービスを提供し、お客様の事業成長を支える環境作りに貢献いたします。



自己紹介

略歴：

- 株式会社リクルートにて、マシンセンター運用管理、スーパーコンピュータネットワーク構築、住宅情報関連システムの設計開発等に携わる。
- 1994年 株式会社ラックに入社。1996年より同社の情報セキュリティ関連事業の立上げ、推進に携わる。
- 2000年より、コンサルティング部門の責任者として、情報セキュリティポリシー策定、リスクアセスメント、情報セキュリティ監査等のサービスを主導する傍ら、執筆、講演活動を通じて情報セキュリティ人材の育成に注力する。
- 2009年より、セキュリティ診断技術を活用した新規ビジネス企画、開発、運用等に携わる。
- 2013年より、アプリケーションパフォーマンスマネジメント（APM）技術を活用した新規ビジネス開発、性能改善コンサルティングに従事。
- 2015年 S&J株式会社 入社（現職　取締役 コンサルティング事業部長）
- 2017年5月より、神奈川県警察 CSIRTアドバイザー

主な所有資格：

- 情報処理安全確保支援士（登録番号 第001659号）
- 情報処理学会　認定情報技術者　No.14000017
- ITストラテジスト
- システム監査技術者
- ネットワークスペシャリスト

CITP 認定情報技術者
Certified IT Professional

主な講演実績：

- 神奈川県警察
- 金融情報システムセンター（FISC）　金融部会
- 一般財団法人 日本情報経済社会推進協会（JIPDEC）
- みずほ総合研究所
- 早稲田大学理工学部
- TFS国際税理士法人
- 一般社団法人企業研究会

主な著書：

- ネットワーク危機管理入門（翔泳社）
- 社長のためのインターネット防犯マニュアル（すばる舎）
- 53のキーワードから学ぶ最新ネットワークセキュリティ（翔泳社）（共著）
- 情報処理教科書　情報処理安全確保支援士（翔泳社）
- 情報処理教科書　情報セキュリティマネジメント 要点整理＆予想問題集（翔泳社）（共著）

１．IT環境の変化と求められる対策

企業等を取り巻く近年の状況

IT環境の変化

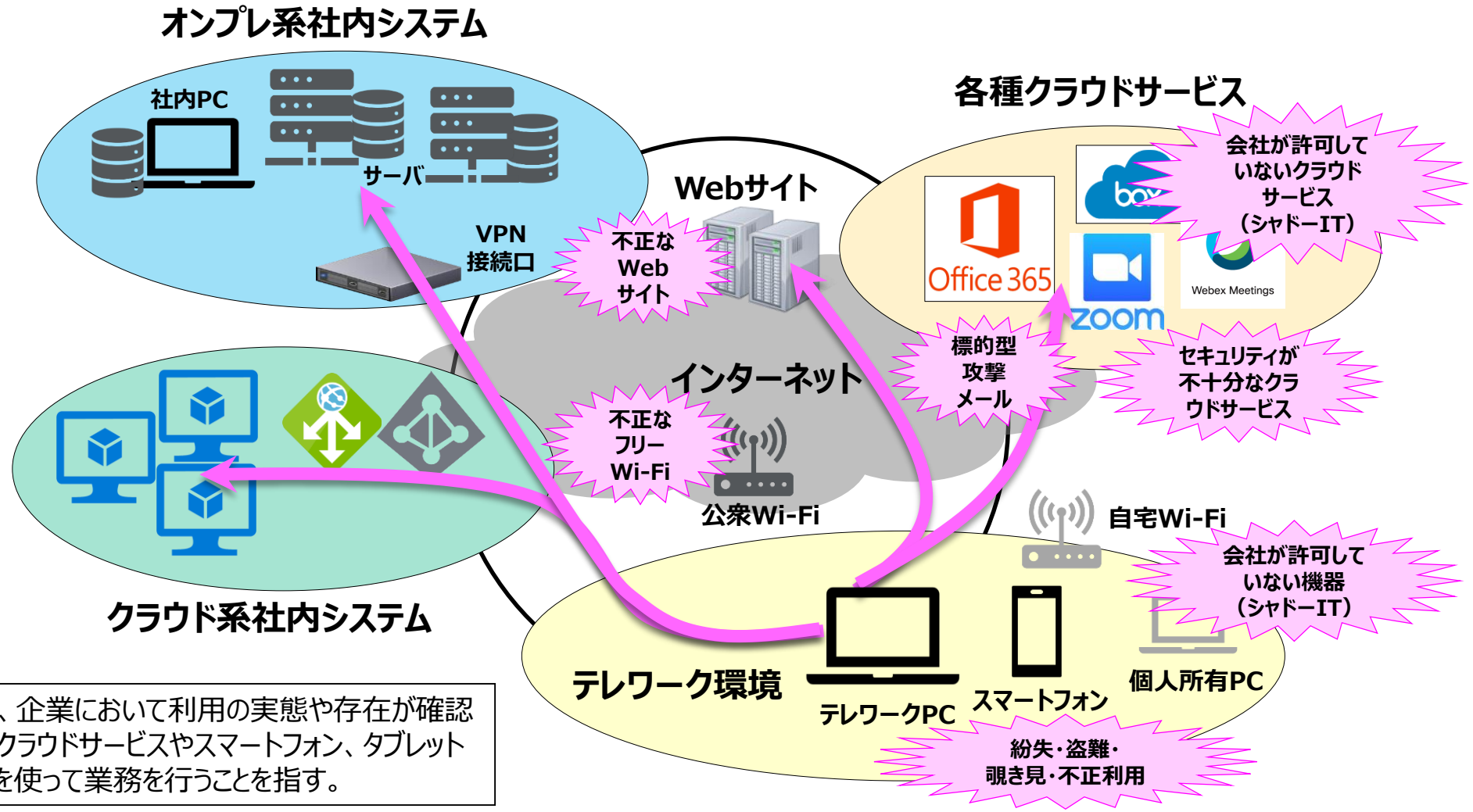
- **各種クラウドサービスの普及**
  - ⇒ Microsoft 365（Office365）, Box, Zoom, GCP, AWS, Azure等の普及
  - ⇒ 従来からのオンプレ社内システムをクラウド環境に移行する流れが加速
- **働き方改革、新型コロナウイルス対策による勤務形態の多様化**
  - ⇒ テレワークの普及
  - ⇒ 社内ネットワークを経由しないインターネットアクセスの増加
- **Webサイトの総https化の進行**
  - ⇒ 2022年1月時点で上場企業の常時https化率は87.7%（※）

IT環境の分散化/多様化が進むとともに通信の秘匿化も進む

※ https://www.feedtailor.jp/report_aossl/

企業等を取り巻く近年の状況

テレワークでは、**端末が組織の外部にある**ことから、オフィス以上にに**セキュリティ対策として考慮すべきことが増える**



シャドーITとは、企業において利用の実態や存在が確認できていない、クラウドサービスやスマートフォン、タブレットなどのIT機器を使って業務を行うことを指す。

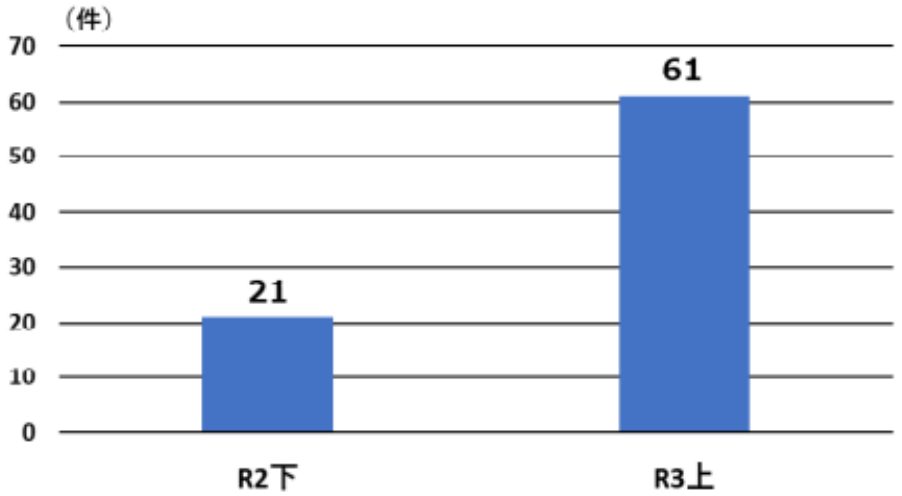
企業等を取り巻く近年の状況

サイバー攻撃の脅威動向

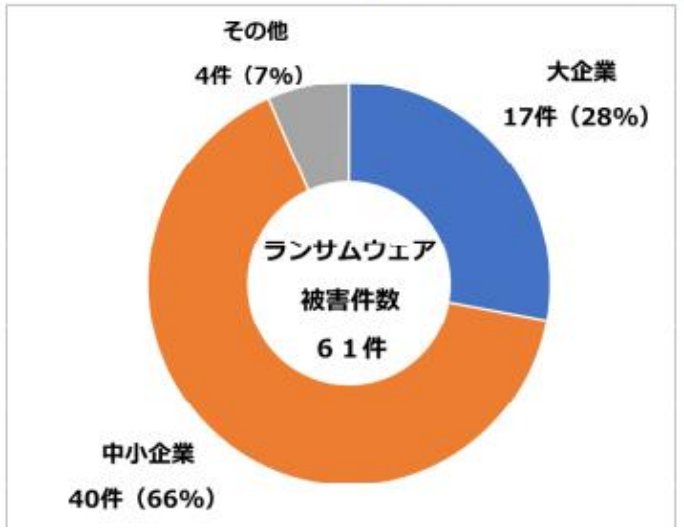
- **VPNから内部ネットワークに侵入されるケースが急増**
  ⇒ VPN製品の重大な脆弱性が狙われる。脆弱なベンダ保守用VPNが狙われるケースも多発
- **Active Directoryが陥落し、内部情報の大量流出や大規模なシステムダウンが発生するケースが急増**
  ⇒ ADサーバのアップデートが行われておらず、重大な脆弱性が狙われる
  ⇒ ドメイン管理者アカウント設定/管理の不備や認証方式の脆弱性が狙われる
- **マルウェアの感染力が増しており、一旦侵入を許すと内部ネットワーク全体に被害が拡大**
  ⇒ 多くの組織でLAN内部でのアクセス制限は厳格に行われていないため、ラテラルムーブメント（横方向への感染拡大）を阻止できない
- **Webサイトの総https化の進行及びマルウェアによる通信のhttps化の進行**
  ⇒ 通信経路上のセキュリティ対策が無力化し、攻撃の「見えない化」が進行

企業等を取り巻く近年の状況

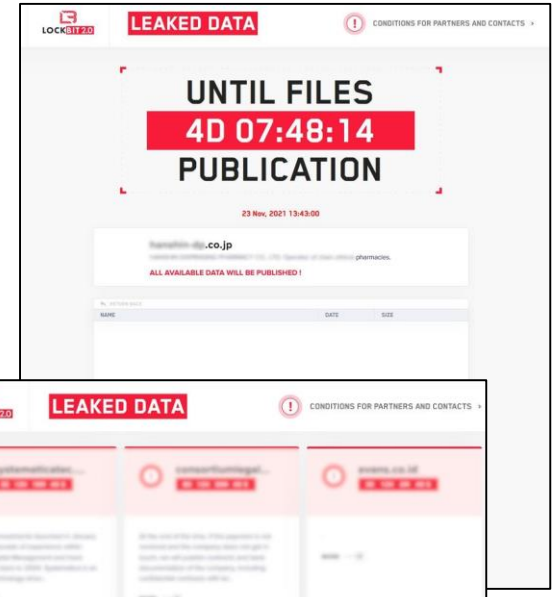
【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】

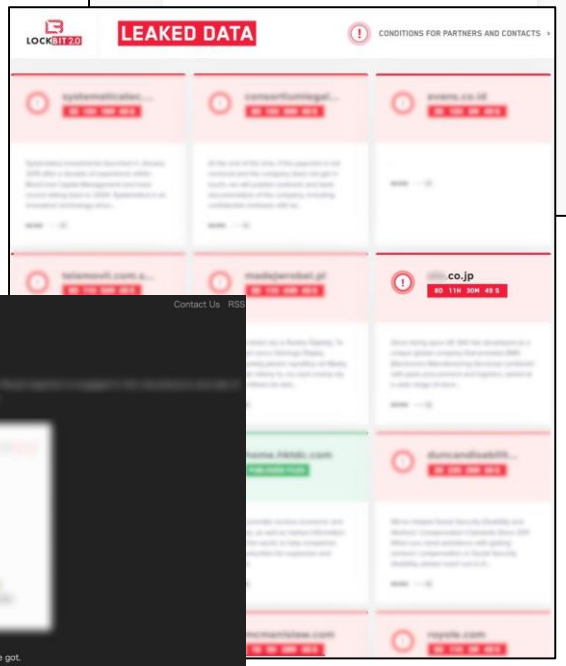


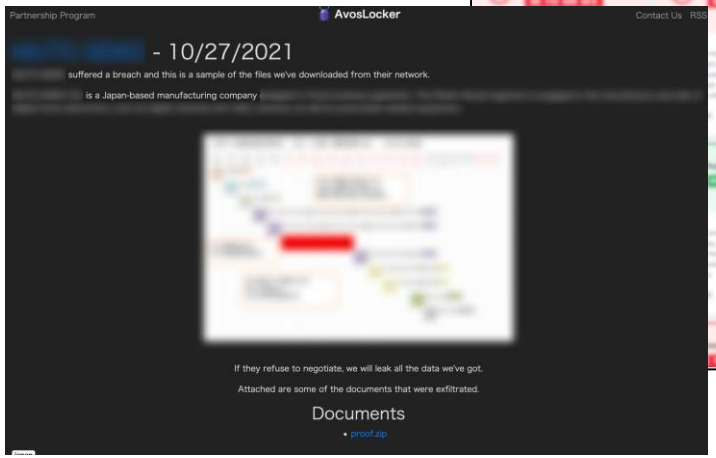
【図表４：ランサムウェア被害の被害企業・団体等の規模別報告件数】

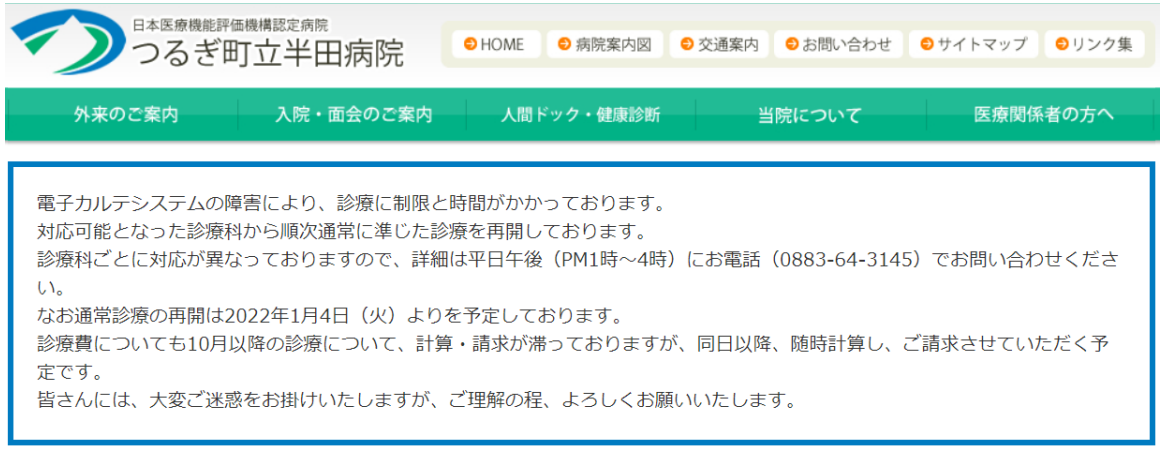


令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf



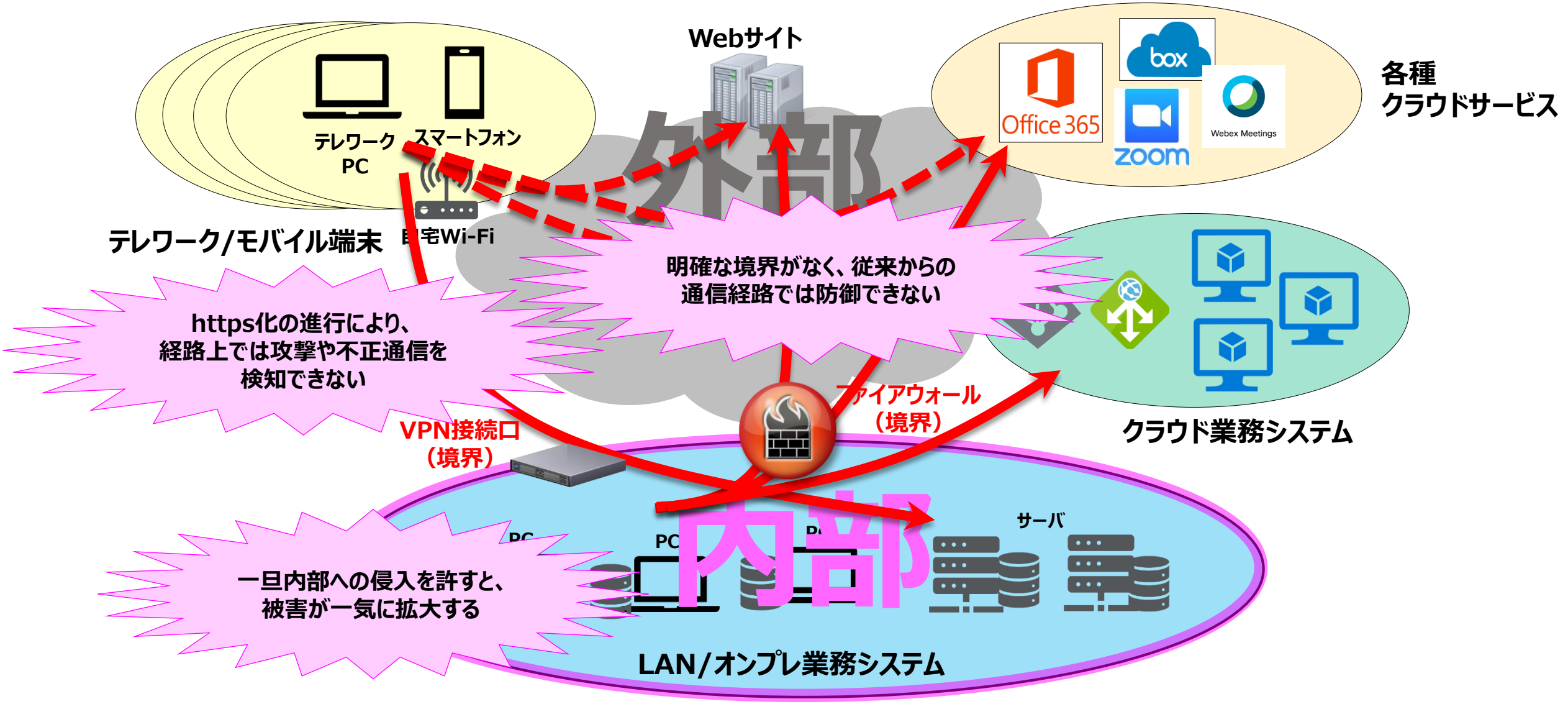






境界防御に頼った従来からの対策の限界

●境界防御モデルにおける問題の例



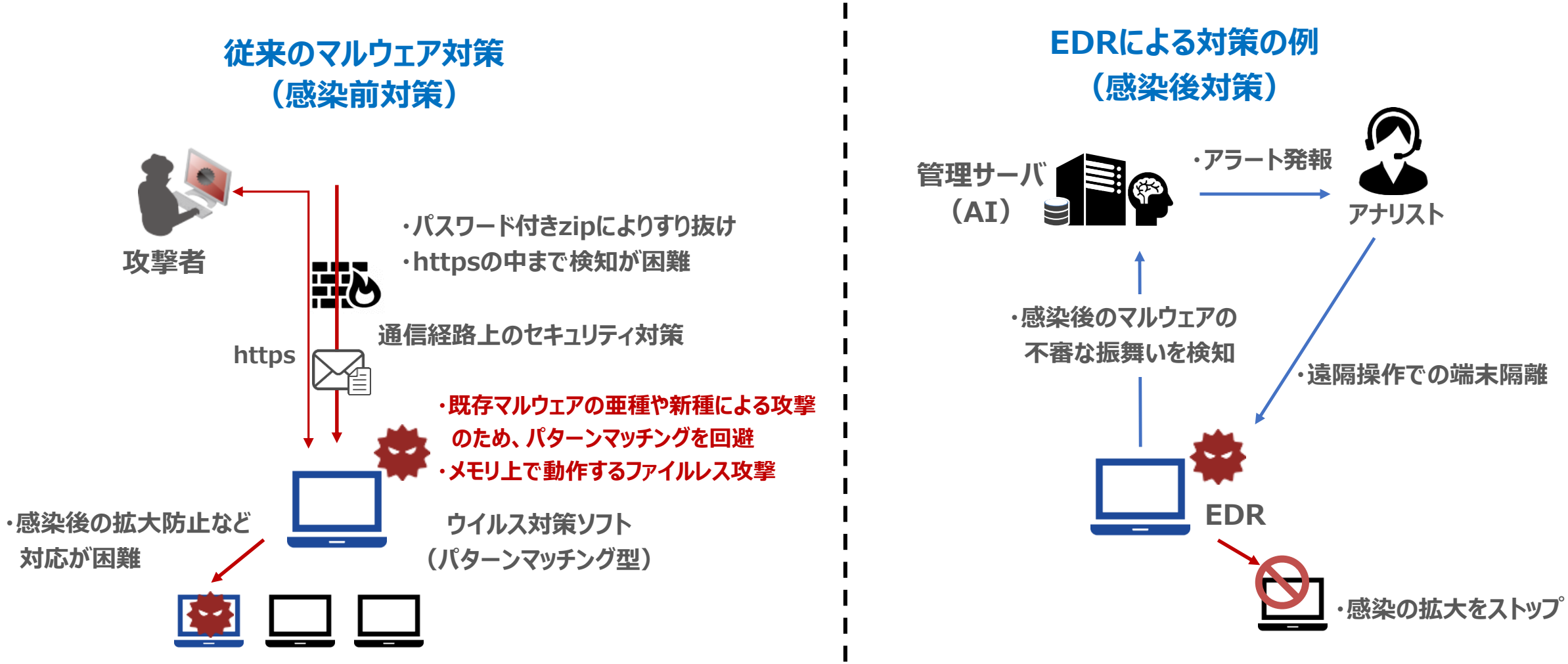
ゼロトラストの概要

- 「ゼロトラストモデル」「ゼロトラストセキュリティ」とも呼ばれており、2010年に米国Forrester Research 社の John Kindervag 氏が提唱したセキュリティの概念モデル
- ゼロトラストを直訳すると「何も信頼しない」だが、その意味するところは、組織の情報システムを構成する各種機器やアプリケーション、ネットワーク、端末、ユーザ等は「いずれも安全ではない可能性がある」という考え方に基づいてセキュリティ対策を行う、というもの
- 具体的には、エンドポイント（個々の端末やサーバ）でセキュリティを確保し、ユーザがアプリケーション等に対して何らかのリクエストを発行するごとに、その信頼性を都度確認するといった仕組みを実装することで、境界防御に頼らないセキュリティモデルを確立する

２．効果的なエンドポイントセキュリティ強化策

従来のウイルス対策ソフトでは検知できないマルウェアも検知・防御するEDR

従来のウイルス対策ソフトや通信経路上での対策では昨今のIT環境や、高度化するサイバー攻撃への対策が不十分なため、EDR（Endpoint Detection and Response）の導入が推奨される



EDR導入における課題の例

EDRが多くのベンダから提供されているが、セキュリティ専門家が運用する前提の製品が多く、以下のような理由から適切に運用できず、導入しただけの状態になっている場合もある

①　EDR導入時の構築作業、初期設定作業が手間

EDRの導入に管理サーバや過検知を防ぐための初期設定が必要となり、導入に手間がかかる。

②　EDRで検知したアラートへの対応で本来の業務に集中出来ない

一般的なEDR製品は検知した大量のアラートがマルウェア起因のものかをお客様自身が分析/判断した上で対応まで行う必要がある。そのため、お客様にセキュリティの知見が求められ、運用負荷もかかる。

③　EDR導入後のホワイトリスト追加作業等の運用が煩雑

アラートが過検知だった場合はホワイトリストへの追加、ファイル復旧、バージョンのアップデート対応などの運用にも稼働がかかる。

EDRを導入している企業でのランサムウェア感染事例

- 人事部に採用への応募を装った添付ファイル付きメールが届く
- テレワーク端末で開封してランサムウェアに感染
- **VPN経由でファイルサーバが暗号化され、かつ情報も漏えいし、身代金の要求を受ける**

- エンドポイント対策：**XXX製EDR**＋Windows Defender
- ゲートウェイ対策：プロキシサーバログ/ファイアウォールログ取得（監視/分析はしていない）
- 添付ファイルは、マクロ付きWordファイルで、中身は応募としては不自然な内容であった
- EDRでアラートがあがっていたものの、**監視していなかった**ためPCの隔離はできていなかった

EDRを導入する際の主な検討ポイント

① **遮断モード**にするか**監視/検知モード**にするか

- 監視/検知モードの場合は検知後の対応（内容確認、隔離等）を行う必要がある

② **初期導入時の作業内容や料金体系、導入後**のホワイトリスト登録作業はどうなっているか

- ホワイトリスト登録作業等が別途料金になっていないか
- 導入した企業側で行わないといけないのか

③ **EDR監視サービスや検知後の対応を行うサービス**があるか

- EDRが検知したアラートへの対応の判断をセキュリティ専門家が24/7体制で提供してくれるか
- 24/7で（通知だけでなく）対応してもらえるか
- 「**マルウェア感染が疑われるPCは隔離**」という一次対応が可能か
- **業務影響のある誤検知に迅速に対応**してもらえるか

まとめ

- クラウドサービスやテレワークの普及等によって企業のIT環境は大きく変化しており、セキュリティと業務効率/利便性とのバランスを考慮した対応が求められている
- 従来からの境界防御では十分な対策効果が得られなくなってきており、エンドポイントとクラウドサービス等によるゼロトラスト志向のセキュリティ対策へ移行していく必要がある
- テレワークPCがサイバー攻撃の標的となり、クラウドサービスを悪用したり、VPNを経由したりして、社内の重要なサーバ等が被害に遭う事例が増加している
- PCを「守る」には従来からのウイルス対策ソフトでは不十分であり、EDR＋監視が有効である
- 導入後の運用を考慮し、監視や必要なサポートが受けられるEDRを選択すべき

ご清聴ありがとうございました

S&J

私たちは、最適なセキュリティサービスをより多くのお客様へ提供し、
事業の成長を支える環境づくりに貢献いたします。

S & J 株式会社
〒105-0003 東京都港区西新橋2-4-12 西新橋PR-EX8階
TEL : 03-6205-8500　FAX : 03-6205-8510
https://www.sandj.co.jp