
ニューノーマル時代のゼロトラストセキュリティ

株式会社 日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部 セキュリティマーケティング推進部
扇 健一

プロフィール



扇 健一

株式会社 日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部
セキュリティマーケティング推進部 部長
セキュリティエバンジェリスト

- ・約20年、セキュリティ関連業務に従事
- ・現在、セキュリティソリューション拡販業務、ソリューション企画業務*、各種講演・執筆活動に従事
(*サイバー攻撃対応BCP、ゼロトラストセキュリティ、クラウドセキュリティ強化、制御システムセキュリティ)
- ・情報漏洩防止ソフトウェア「秘文」、電子マネーシステム、ISO/IEC 15408 Common Criteria評価システムなど、各種ソフトウェア開発を10年以上経験
- ・「秘文」で、IPA Software Product of The Year 2012 受賞
- ・早稲田大学 グローバルエデュケーションセンター 非常勤講師
- ・横浜国立大学先端科学高等研究院「IoTセキュリティフォーラム」プログラム委員会
- ・新建新聞社 リスク対策.com「テレワーク時代のデジタルBCP基礎講座」連載寄稿
- ・NPO 日本ネットワークセキュリティ協会(JNSA) WG活動に参加(マーケティング部会、ソリューションガイド活用WGなど)

本日お伝えしたいこと

テレワークにおけるセキュリティ課題と主な解決策

ゼロトラストセキュリティの考え方

段階的にゼロトラストセキュリティに
移行するためのヒント

Contents

1. テレワークの課題とクラウドシフト
2. ゼロトラストセキュリティの考え方
3. ゼロトラストセキュリティの実装イメージ

1. テレワークの課題とクラウドシフト

テレワークの浸透で見えてきたICT面での課題

モバイルPC確保

- レンタル/購入手続き
- 会社PC持ち帰り
- Web会議機材確保

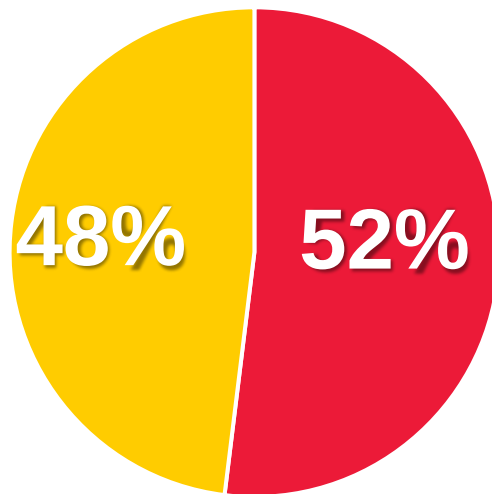
セキュリティ問題

- PCのセキュリティ
- インターネット接続のセキュリティ

業務への支障

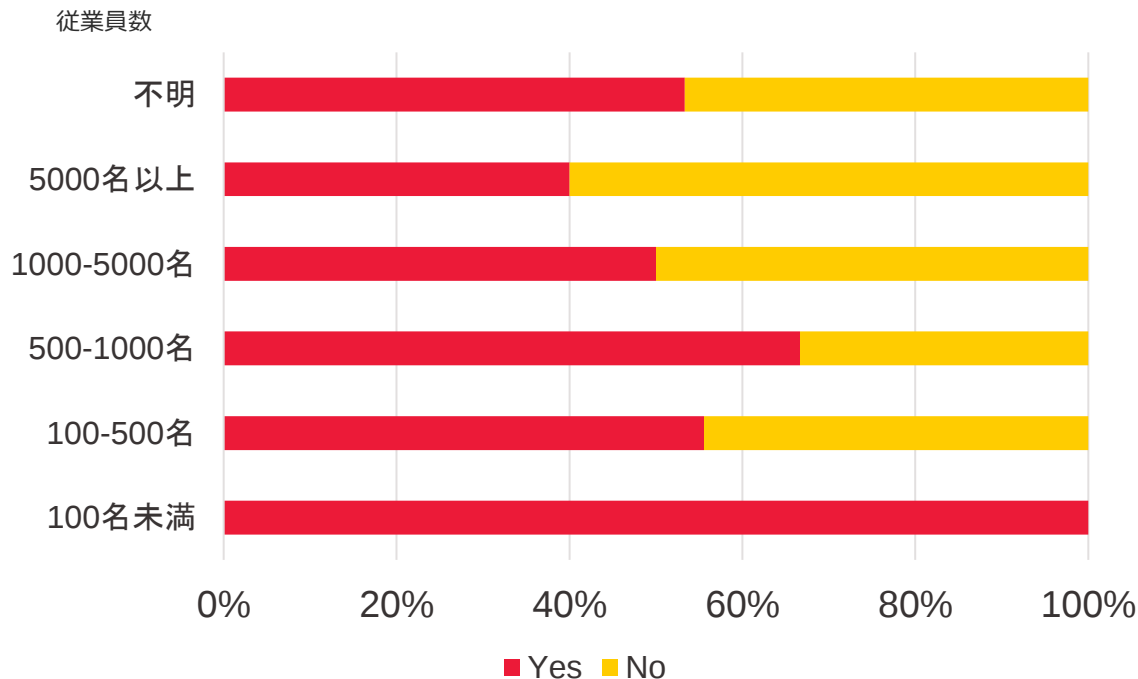
- VPN利用不可時の業務制限
- 高負荷なVPN回線

テレワーク用のPCから、直接インターネット接続できる環境を利用している人の割合

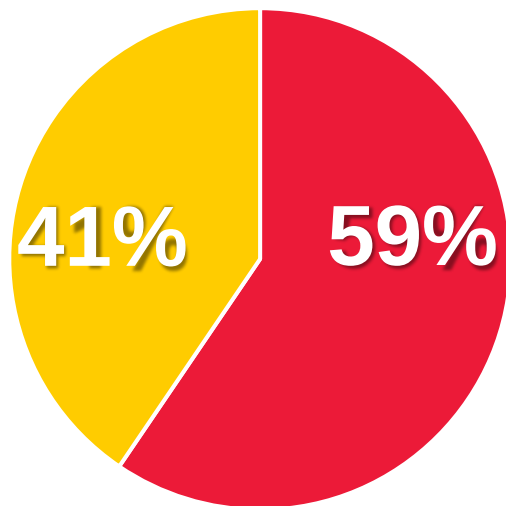


■ Yes ■ No

日立ソリューションズ調べ

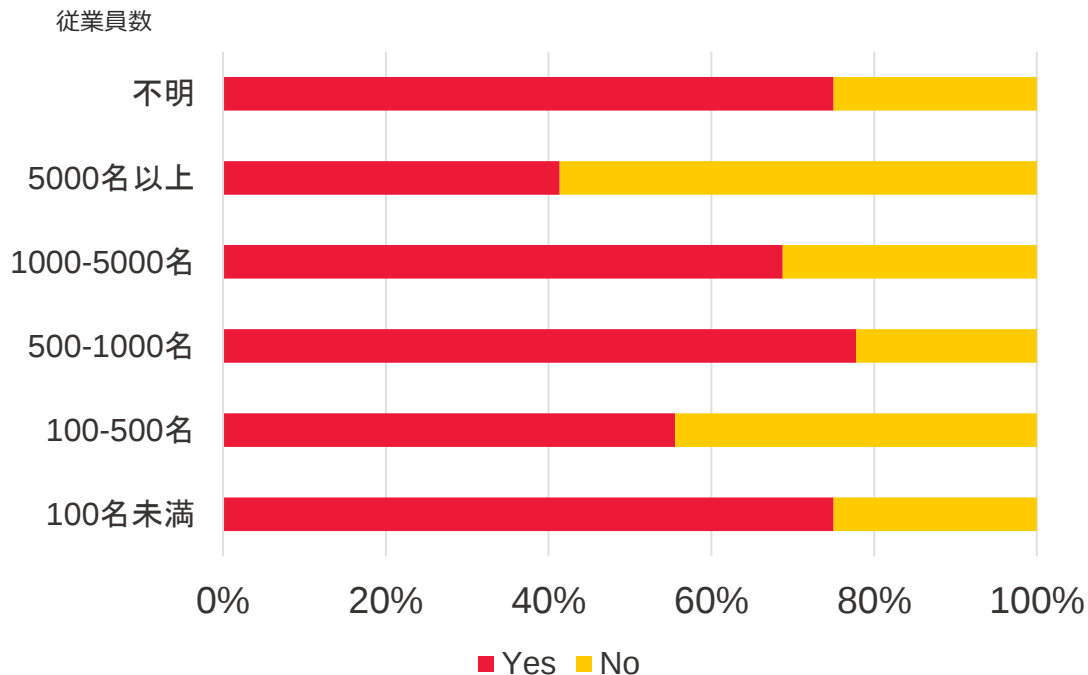


VPNの利用において、負荷による回線の遅さを経験した人の割合



■ Yes ■ No

日立ソリューションズ調べ



- 1 テレワークPCの追加に伴うVPNライセンスの追加
- 2 テレワークPCの追加に伴うVPNで利用する証明書ライセンスの追加
- 3 テレワークPCの追加に伴う情報漏えい対策
- 4 SD-WANによるインターネット接続負荷分散
- 5 端末からのインターネットブレイクアウトの実現
- 6 ゼロトラストセキュリティの実現
(クラウドでのID管理、未知マルウェア対策、SASE導入 etc.)

1-3 組織や個人に対するサイバー攻撃の発生

組織にとってのリスク



ランサムウェアによる
業務活動停止と脅迫

未知マルウェアによる
VPNアカウント情報の窃取

悪性Botによる
インターネット販売サイトでの
買い占め・転売

etc.

個人にとってのリスク



メールなどによる
給付金詐欺

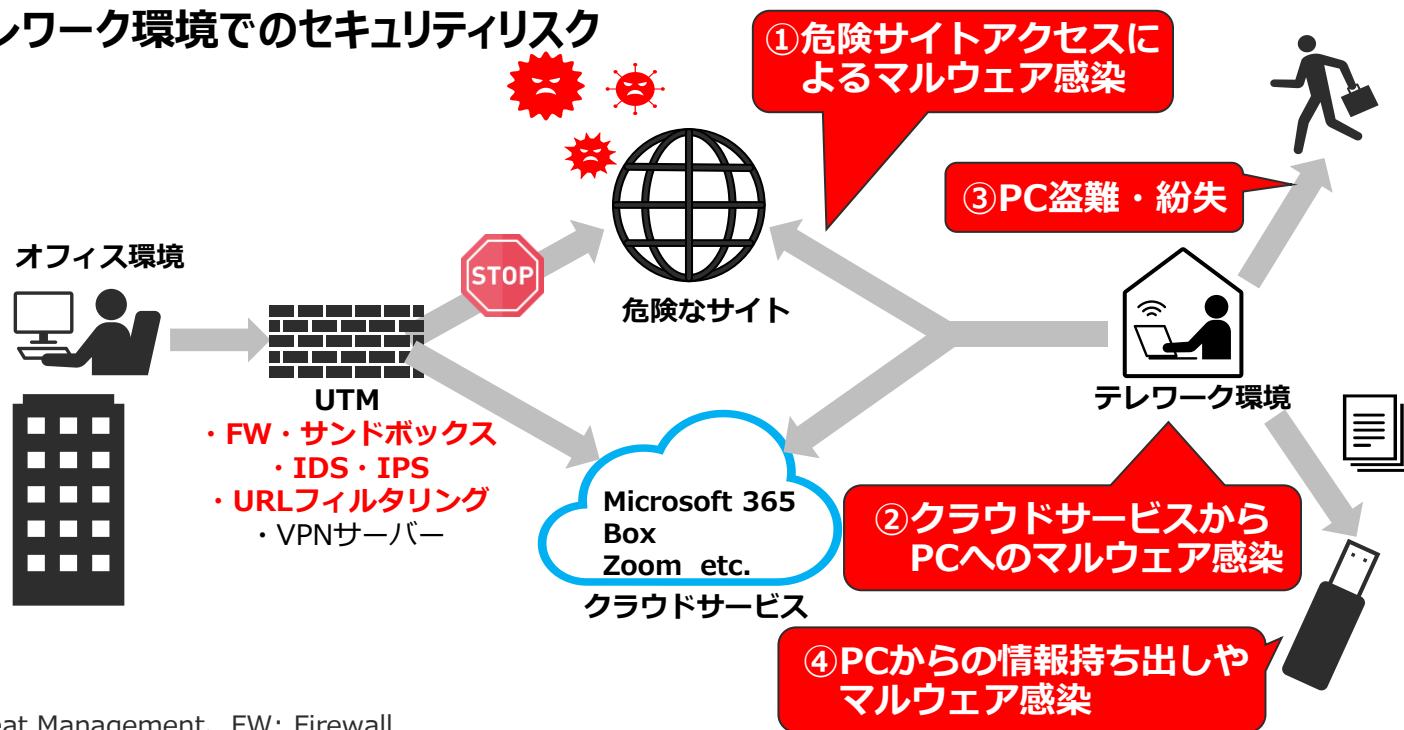
SMS、SNSでの宅配通知による
個人情報窃取

危険サイトアクセスによる
未知マルウェア感染と拡散

1-4 テレワーク環境でのセキュリティリスク

要件：快適なテレワーク環境を準備したい

課題：テレワーク環境でのセキュリティリスク

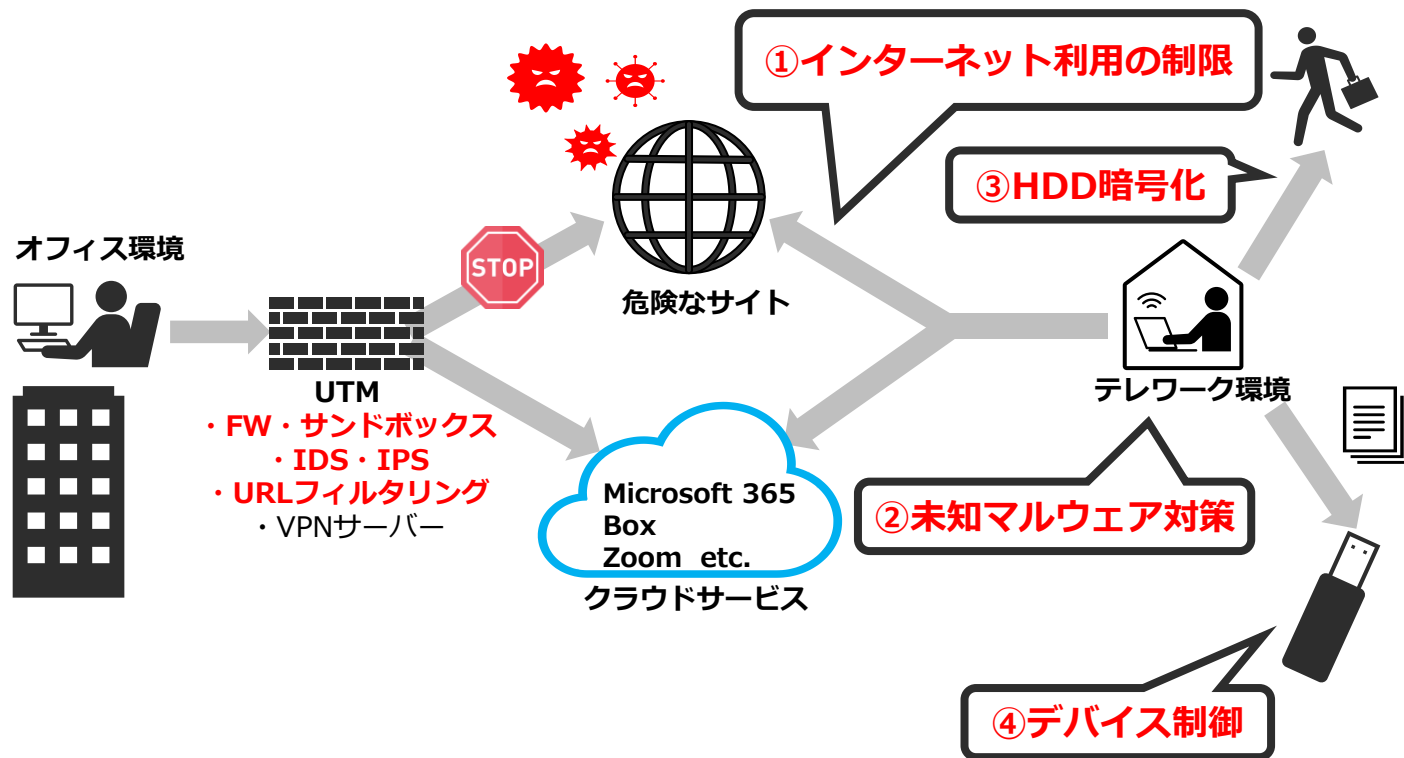


UTM: Unified Threat Management、FW: Firewall

IDS: Intrusion Detection System、IPS: Intrusion Prevention System

Microsoft 365は、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。Boxは、Box Inc.の商標または登録商標です。Zoomは、Zoom Video CommuNicationNs, INC.の米国およびその他の国における登録商標または商標です。

テレワーク環境でのセキュリティリスクに対する解決策



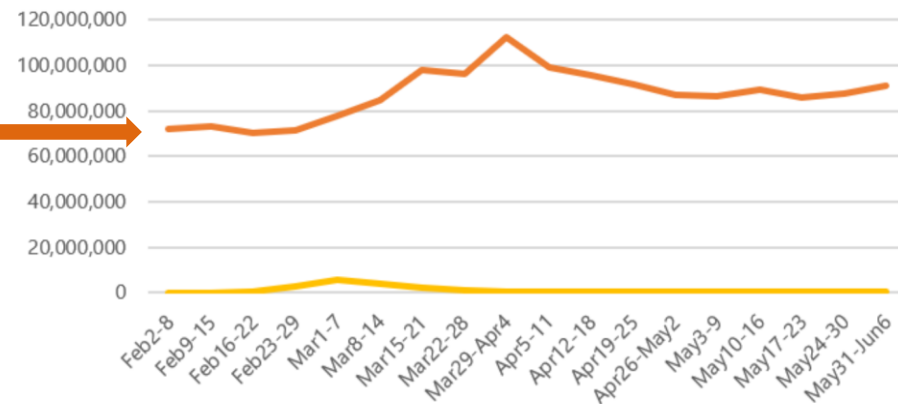
1-5 マルウェアによる脅威の拡大状況

攻撃の高度化、サプライチェーンの弱点を悪用、COVID-19感染拡大への便乗により
マルウェアの脅威は増大、すべての企業が被害者にも加害者にもなり得る状況にある

- マルウェア件数は2009年～2018年の10年で**約25倍**^{*1}に増加
- マルウェアの**96%**は「**使い捨て**」^{*2}
- 標的型攻撃は巧妙化し、**関連会社・取引会社なども標的に**
- セキュリティ対策が弱い箇所を**踏み台・足掛かりに**

- **COVID-19感染拡大への便乗**^{*3}
オレンジの線は、世界におけるマルウェア検知の傾向を示す。2020年2月末から増加し、4月初旬をピークとしているが、COVID-19の第2波に合わせたかのように、6月初旬においても再び増加傾向にある。

COVID-19 themed attacks vs. all malware ^{*2}



*1 AV-TEST 「total Malware」

*2 出典:ITmedia エンタープライズ:

<http://www.itmedia.co.jp/eNterprise/articles/1712/11/News012.html>

マイクロソフト社が3カ月間(2017年7月～9月)マルウェアを分析した結果、同じマルウェアが2回以上検出されたケースは全体の4%

*3 出典: COVID-19 に便乗した脅威が横行: 感染拡大時におけるサイバー犯罪者の動向とは

<https://News.microsoft.com/ja-jp/2020/06/18/200618-exploitiNg-a-crisis-how-cybercrimiNals-behaved-duriNg-the-outbreak/>

COVID-19 total encounters

Sum of total reports

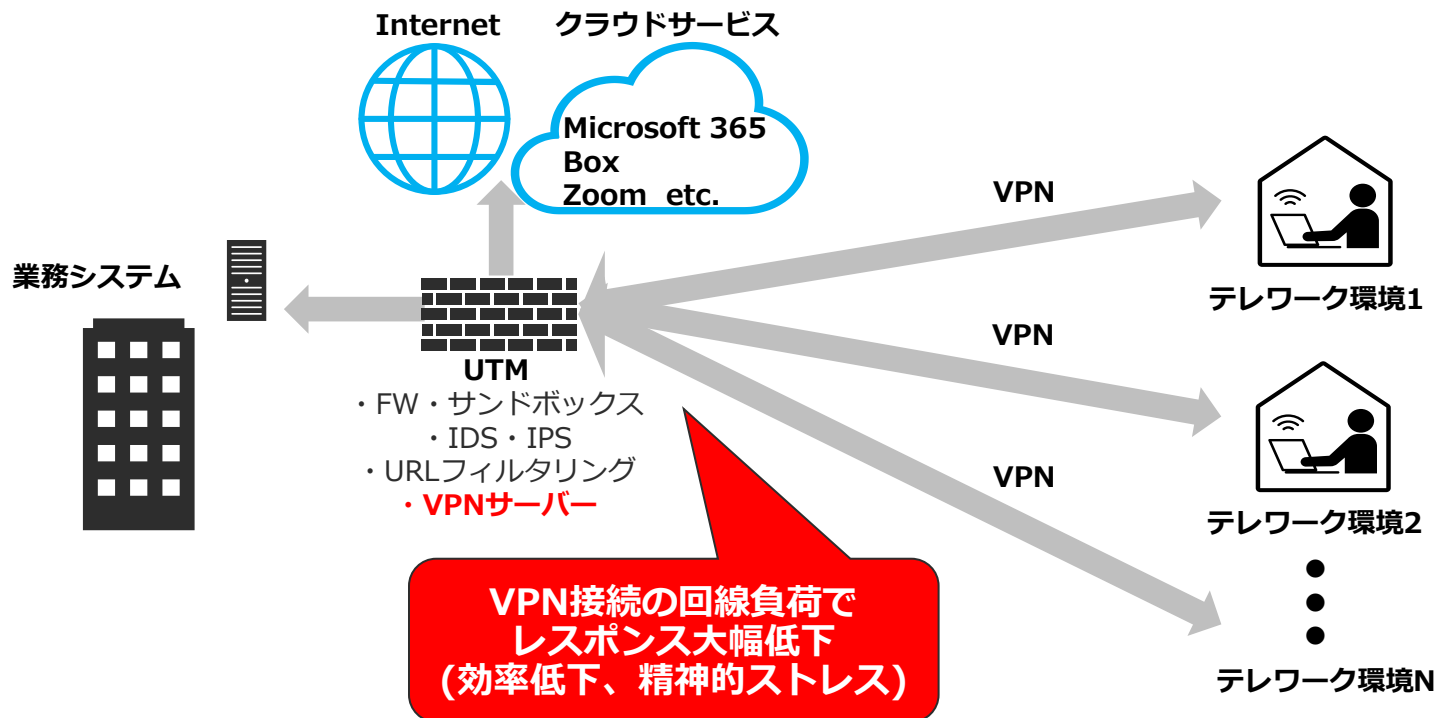
COVID-19関連の攻撃数

世界におけるマルウェア検知の傾向

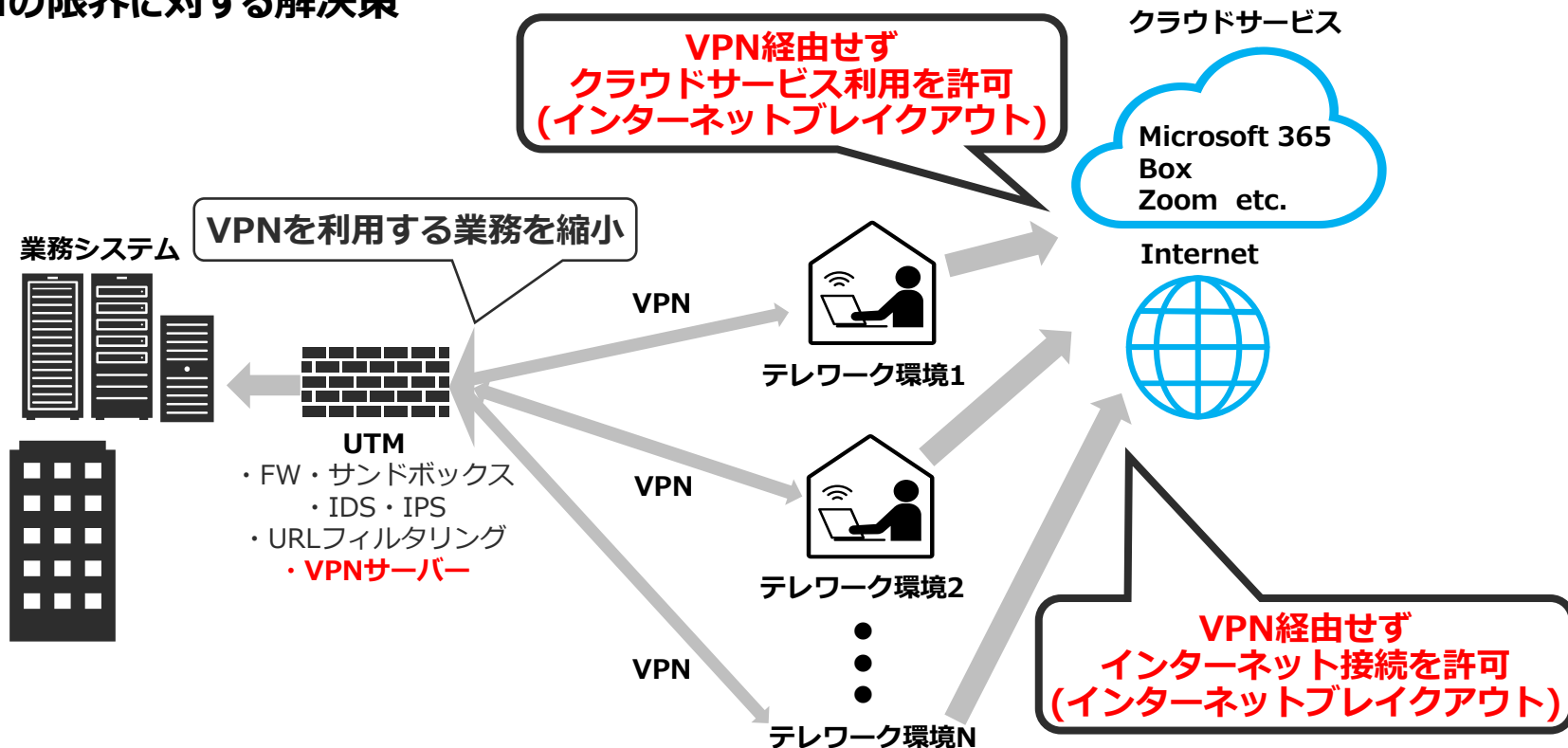
1-6 VPN利用によるテレワーク環境の限界

要件：テレワーク業務とテレワーク人員を増やしたい

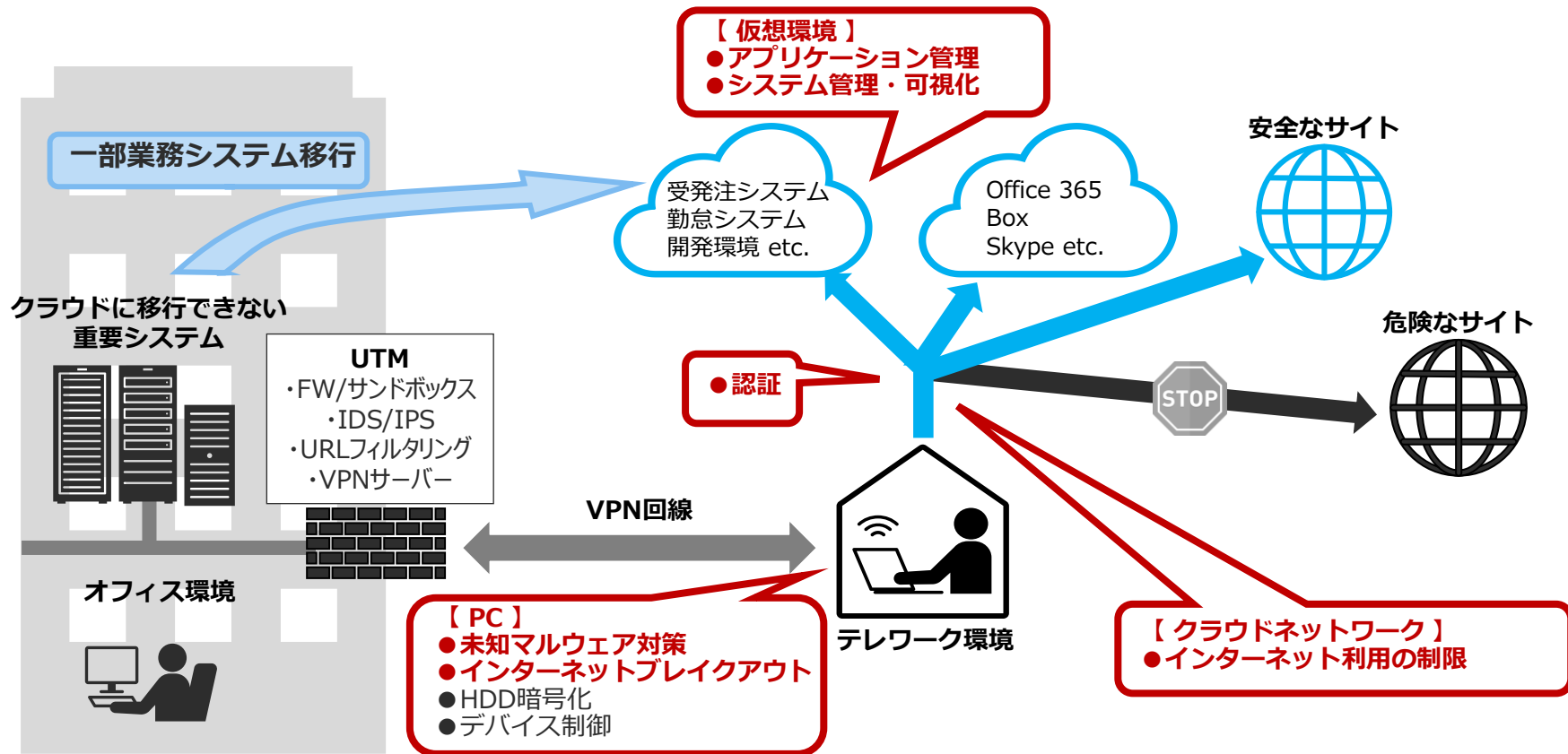
課題：VPNの限界



VPNの限界に対する解決策



1-8 テレワーク環境へのゼロトラストセキュリティの適用



2. ゼロトラストセキュリティの考え方

今まで

境界を前提としたセキュリティ対策

これから

境界に頼らない、
クラウドを中心としたセキュリティ対策

データ

社内 ➡ クラウド、モバイル端末 など

仕事場

社内 ➡ 自宅、カフェ、乗り物 など

サイバー攻撃

パターン ➡ 人やシステムを騙す



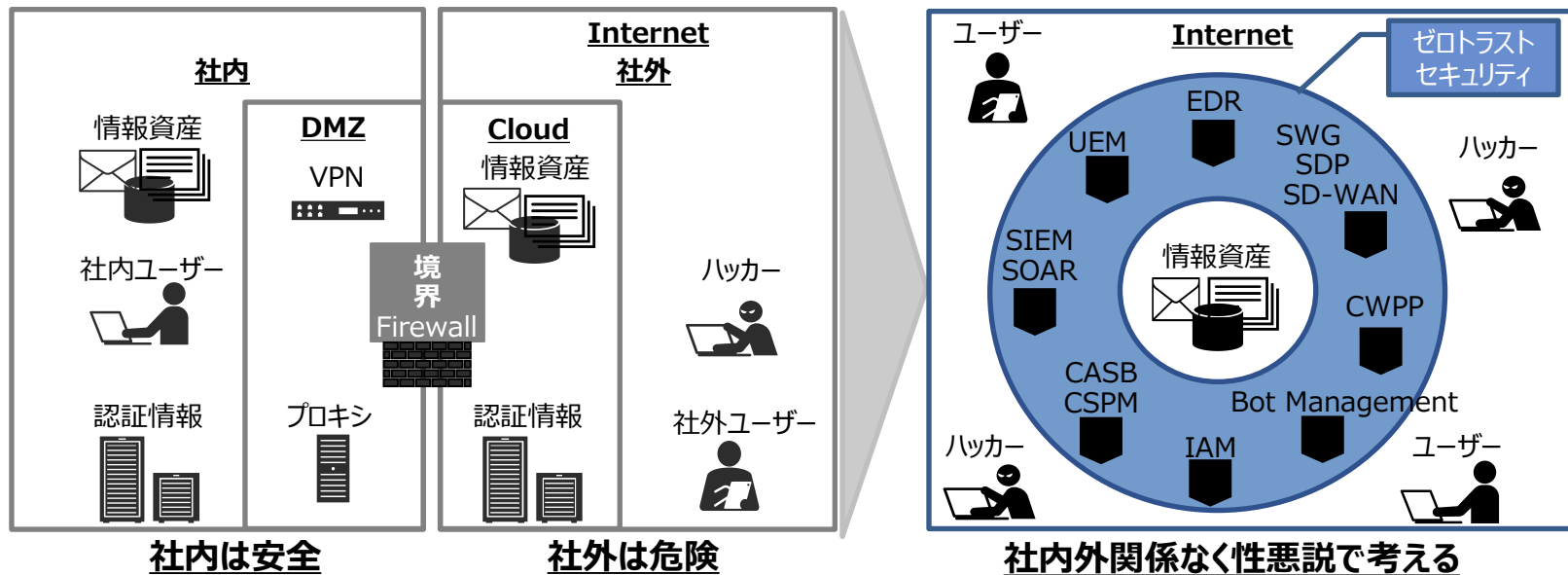
“境界”を設けるのは困難

ネットワーク、デバイス、ユーザー、アプリケーションは、信頼しきることはできない。
境界を通らないアクセスや、境界を突破されることを想定して、対策を考える必要がある。

2-2 ゼロトラストセキュリティ概念

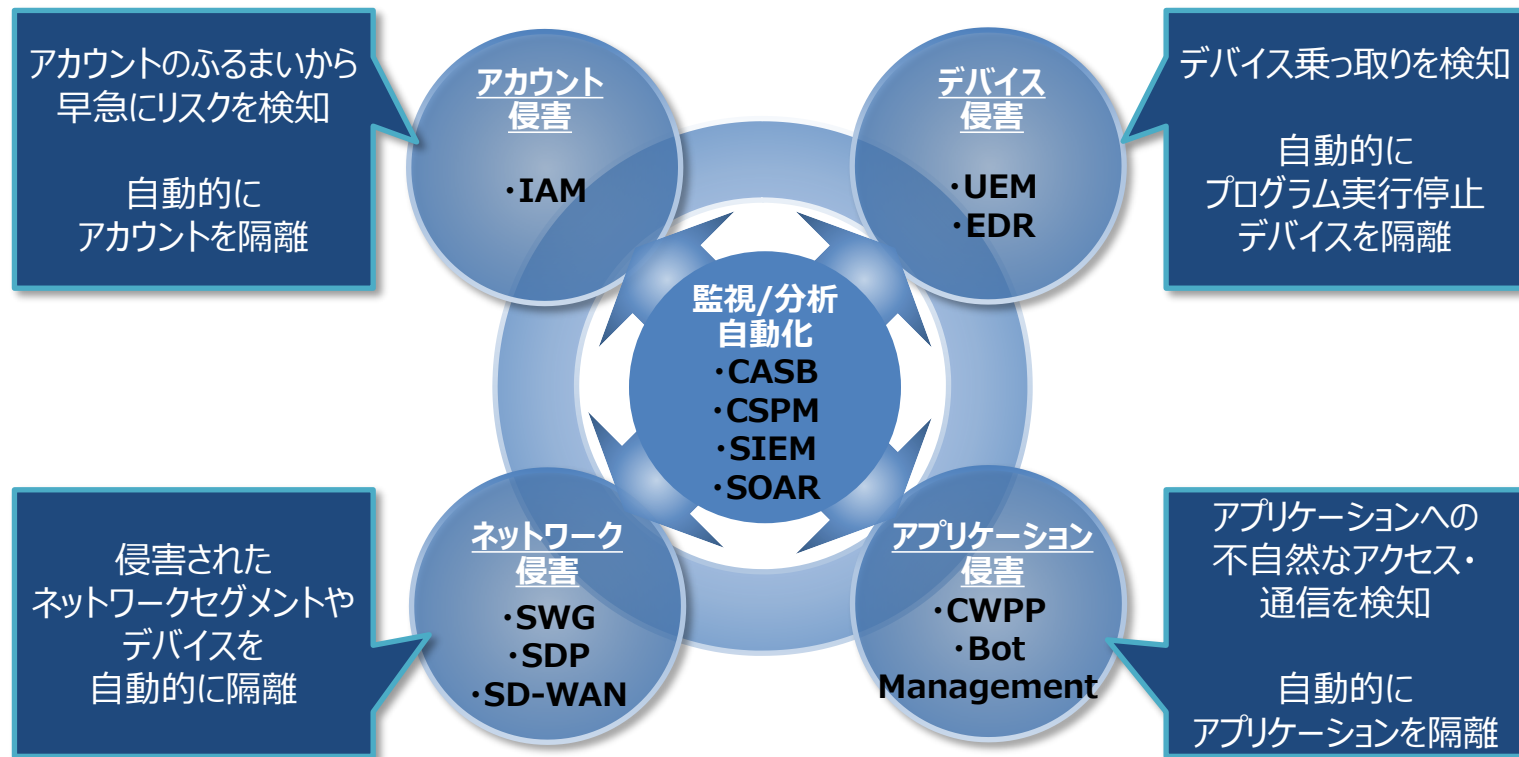
ゼロトラストセキュリティの世界では、情報資産にアクセスするすべてのトラフィックを信用しない

境界 → 情報資産を中心に構成

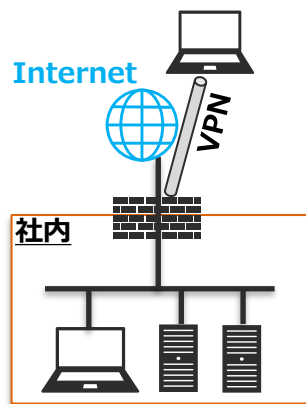


DMZ: Demilitarized Zone、EDR: Endpoint Detection and Response、SWG: Secure Web Gateway、SDP: Software Defined Perimeter
CWPP: Cloud Workload Protection Platform、IAM: Identity and Access Management、CASB: Cloud Access Security Broker
CSPM: Cloud Security Posture Management、SIEM: Security Information and Event Management
SOAR: Security Orchestration and Automation Response、UEM: Unified Endpoint Management

情報資産へのアクセスの利便性を損なわず、以下を実現



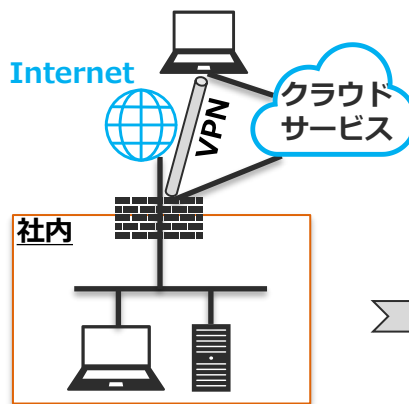
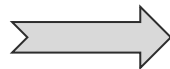
2-4 ゼロトラストセキュリティへの移行



Step 0
レガシー(イントラ)のみ

外からのアクセスはVPNを基本、
社外からの攻撃は
イントラとの境界で守る

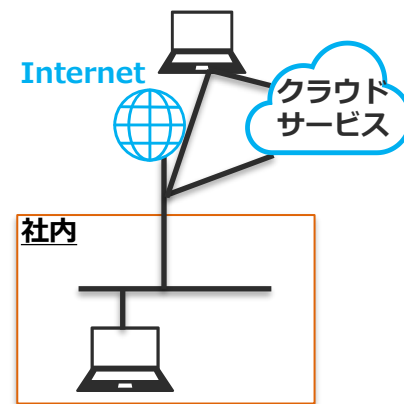
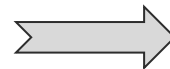
境界(多層)防御



Step 1
一部がクラウドへ移行

外でクラウド上のシステムを
利用することが発生
➡境界で守ることに限界

境界(多層)防御
+ ゼロトラストの一部



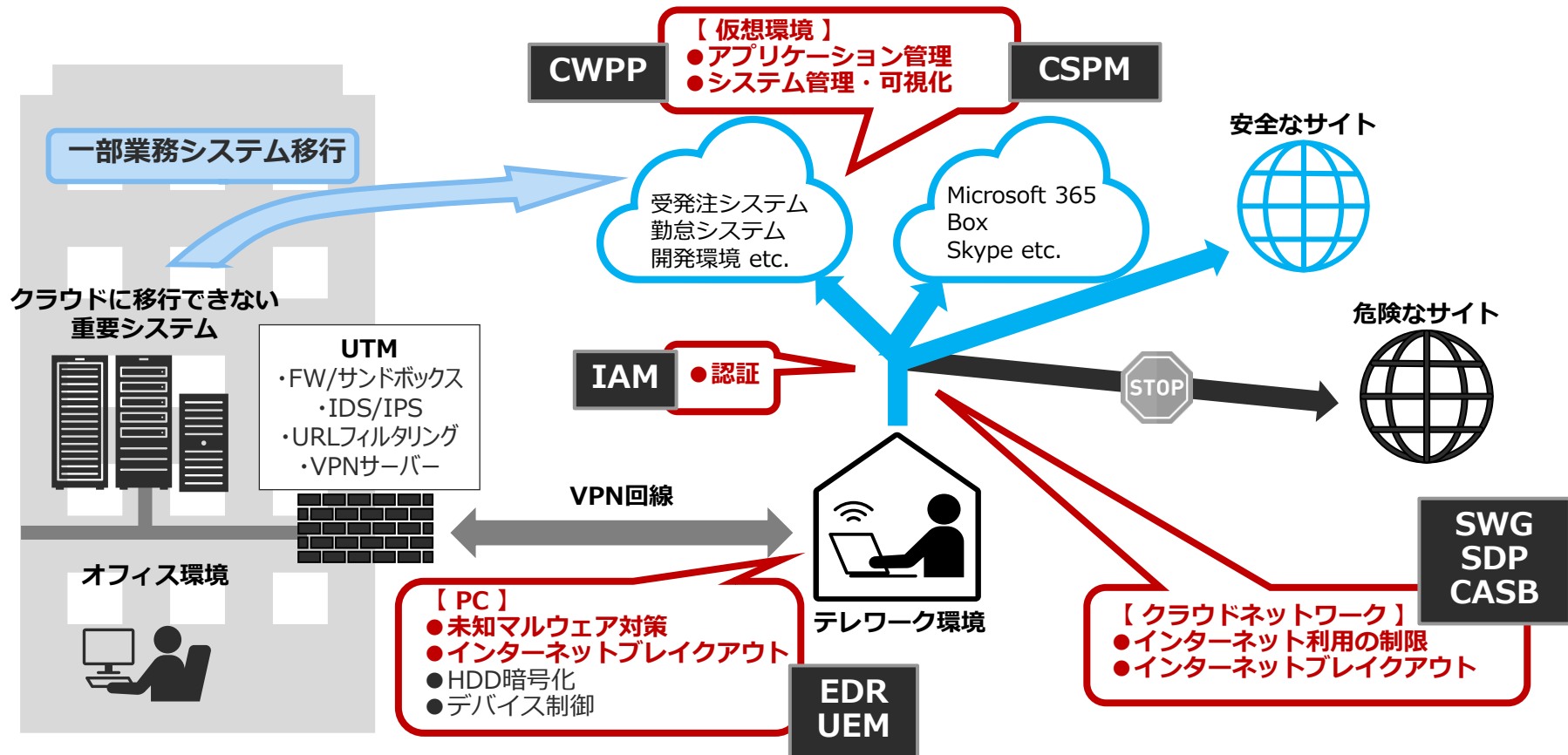
Step 2
全システムがクラウドへ移行

どこからでも使えるシステムに
境界なし、結果としてVPNは
不要

ゼロトラストのみ

3. ゼロトラストセキュリティの実装イメージ

3-1 テレワーク環境へのゼロトラストセキュリティの適用



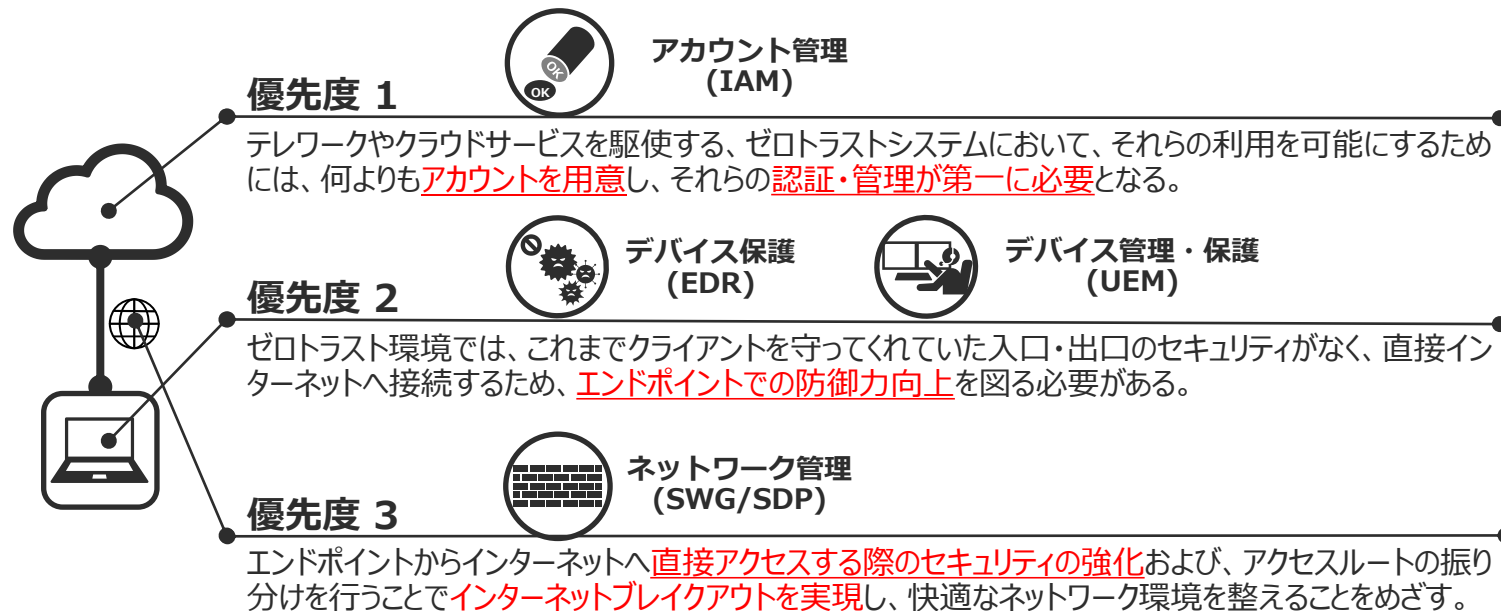
投影のみ

投影のみ

3-4 ゼロトラストセキュリティ、どこから始めるか

物理的なロケーション拘束の解放をめざし、クラウド促進と境界防御脱却

ゼロトラストシステムを実現するにあたって、第一に「**業務を可能とするアカウントの認証・管理強化**」、第二に「**社外ネットワークに晒されるエンドポイントの防御力向上**」、第三に「**ネットワークセキュリティの実装**」が必要。

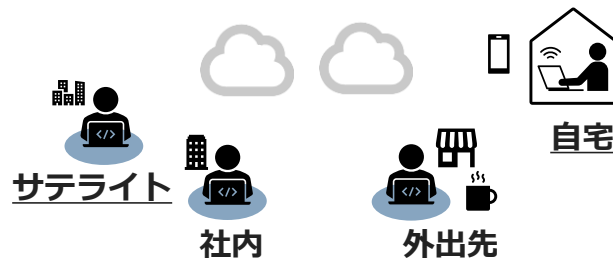


3-5 【最後に】ゼロトラストセキュリティが確立すると

時間と場所の制約から解放、業務変革に柔軟に対応するための「ゼロトラストセキュリティ」

利用者視点

働き方改革、モダンワークスタイルへの対応



いつでも、どこでも、どんなデバイスからでも
セキュアかつ、効率的に業務が遂行できる

- ☑ テレワークでもコミュニケーションが自由にとれる
- ☑ 社内にいなくても、ネットワーク環境さえあれば、セキュアに業務できる

経営・管理者視点

デジタルトランスフォーメーションへの対応

経営のグローバル化 お客さま・パートナー

M&A

協業・協創

デジタルシフト

経営・事業への貢献、環境変化への追従、
セキュリティの確保

- ☑ M&Aや組織の統廃合に迅速に対応できる柔軟性(即応性)
- ☑ パンデミックなどによるBCP発動時、柔軟、かつ迅速にIT環境を増強・縮小できるスケーラビリティ

END

ニューノーマル時代のゼロトラストセキュリティ

株式会社 日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部 セキュリティマーケティング推進部
扇 健一

Hitachi Social Innovation is

POWERING GOOD

世界を輝かせよう。

HITACHI
Inspire the Next 