ＤＸ時代の
大前提！！

『ゼロトラスト
セキュリティ』
を知る

２０２１．１０．１５
ＮＴＴ東日本
東京事業部

K21-2361【2110-2203】

自己紹介

NTT東日本

ビジネスイノベーション部
第二マーケティンググループ
第一マーケティング担当
担当部長

黒　瀬　光　庸

東京2020ゴールドパートナー
（通信サービス）

つなぐ。それは、ECO

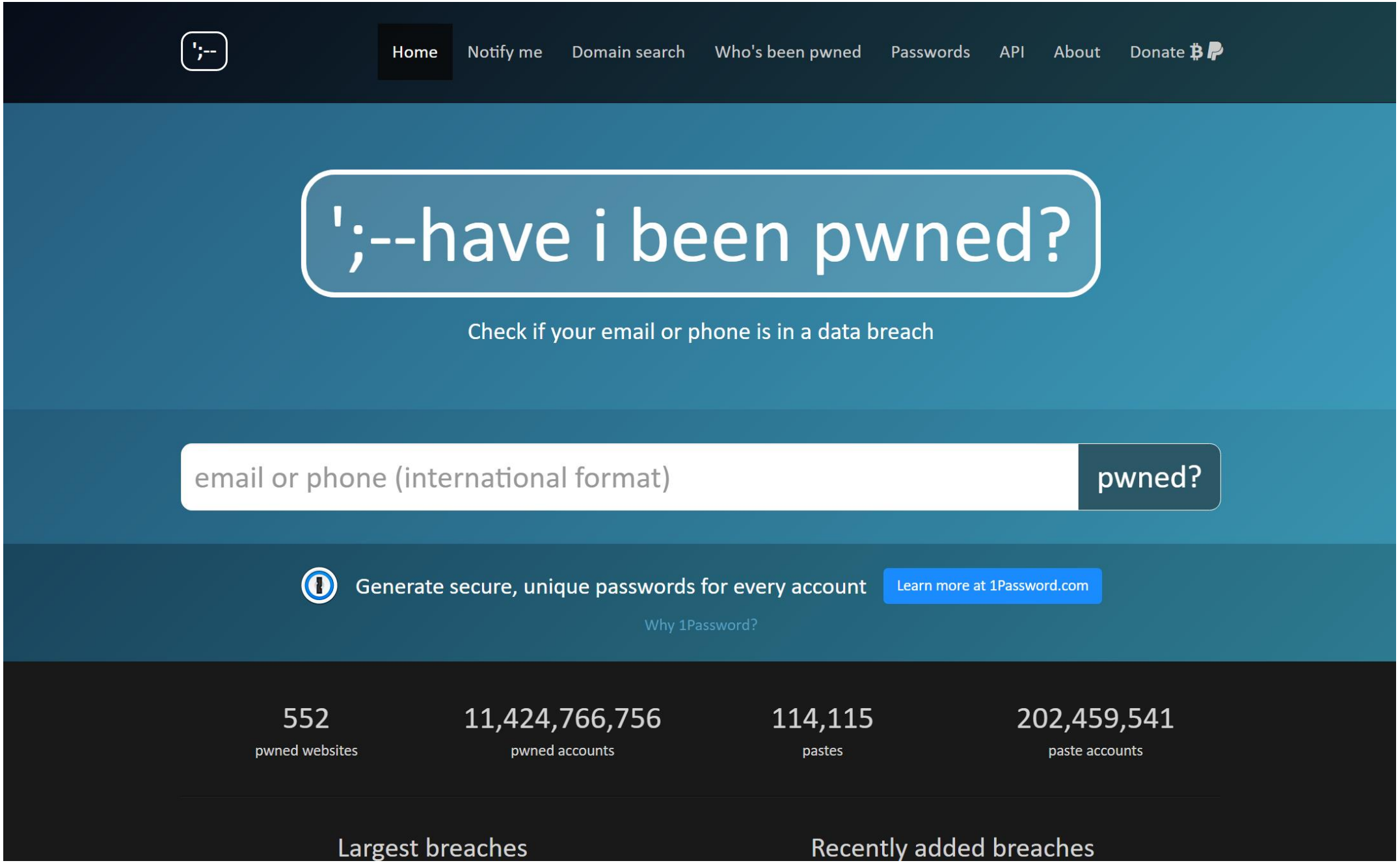
東日本電信電話株式会社

TEL (03)6712−9170　FAX (03)5479−4502
E-mail: mitsunobu.kurose@east.ntt.co.jp
〒108-8019 東京都港区港南1-9-1　NTT品川TWINS

- インサイドセールス
  Enterprise層、SMB層向けインサイドセールスの企画、運営　等
- ＩＣＴセミナー
  「情報セキュリティ」、「働き方改革」、「DX」等のセミナー企画、講師実施

▲オンライン名刺

パスワードは漏れてないですか？



出典:「Have I been Pwned」（HIBP）

出典:「Have I been Pwned」（HIBP）

サイバー空間における脅威は、極めて深刻な情勢

出典:警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」(2021/3/4)

被害金額はどのくらい？

事故1件あたりの平均損害賠償額は**約6億円**

事故件数	443件
想定損害賠償総額	2,684億5,743万円
１件あたりの 平均損害賠償額	6億3,767万円

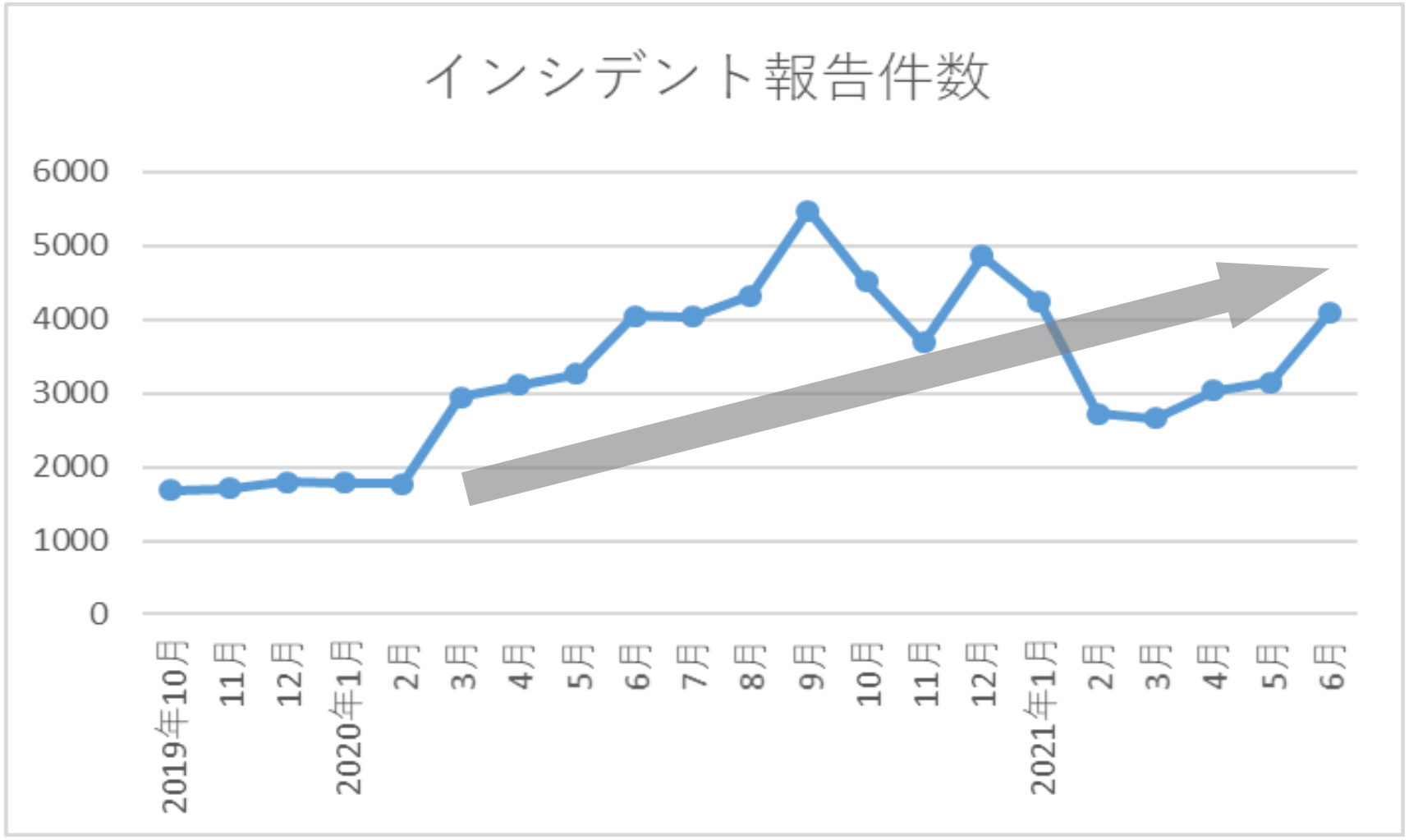
※2018年1月1日から2019年12月31日までに発生し、ウェブサイトなどで公表されている内容を元に集計
出典：NPO法人日本ネットワークセキュリティ協会（2019）「2018年 情報セキュリティインシデントに関する調査報告書（速報版）」

情報セキュリティの10大脅威　2021

順位	前年比	「組織」の10大脅威
1位	↗	**ランサムウェアによる被害**
2位	↘	標的型攻撃による機密情報の窃取
3位	**NEW**	**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	―	サプライチェーンの弱点を悪用した攻撃
5位	↘	ビジネスメール詐欺による金銭被害
6位	↘	内部不正による情報漏えい
7位	↘	予期せぬIT基盤の障害に伴う業務停止
8位	↗	**インターネット上のサービスへの不正ログイン**
9位	↘	不注意による情報漏えい等の被害
10位	↗	**脆弱性対策情報の公開に伴う悪用増加**

（出典）IPA（情報処理推進機構）による「情報セキュリティの10大脅威　2021」

コロナ禍以降、セキュリティインシデントは増加傾向



出典:JPCERT/CC インシデント報告対応レポート(2021/7/15)

サイバー攻撃は拡大・・・

新たなマルウェア　１日あたり約**37.6**万個

サイバー攻撃は国際的な**闇ビジネス**

(出典) https://eset-info.canon-its.jp/malware_info/special/detail/200206.html
「The AV-TEST_Security_Report　2018/19」

情報はいくらで取引される？

メールアドレス
とパスワード

$ 1~15（~約1,700円）

オンライン支払口座

$ 1~100（~約11,400円）

※日本円は2021.10.13のレートで計算

オンラインセキュリティの記事より（https://www.onlinesecurity.jp/feature/20200714.html）

サイバー攻撃、発覚するまで
どのくらいかかると思いますか？

サイバー攻撃、発覚するまで**平均1年以上**

2019年1月1日から2020年7月31日までに公表された法人・団体での不正アクセスにおいて、被害規模1000件以上の個人情報漏洩事案81件を対象に、サイバー攻撃の発生から発覚・公表までの期間を調査したもの

セキュリティ通信HPより（2020.9.8）https://securitynews.so-net.ne.jp/news/sec_30285.html

1日に受信する「電子メール」は何通ですか？

サイバー攻撃手法の実態

法人組織への3大脅威は“メールからの侵入”

メールによる脅威

88%

ランサムウェア

①関係者を装うメールでクリック（ファイルオープンorURLリンク）を誘う
②不正なファイルorURLを使い　ランサムウェアでPCをロック

→ 身代金

標的型サイバー攻撃

①関係者を装うメールでクリック（ファイルオープンor URLリンク）を誘う
②開封後、ボットを侵入させ、次回以降の司令を出す

→ 情報窃取

ビジネスメール詐欺 (BEC)

①Office365偽ログイン画面に誘導しID/PWDを窃取
②メールを盗み見し、通常業務そっくりの振込依頼を送付し現金を引き出す。

→ 送金

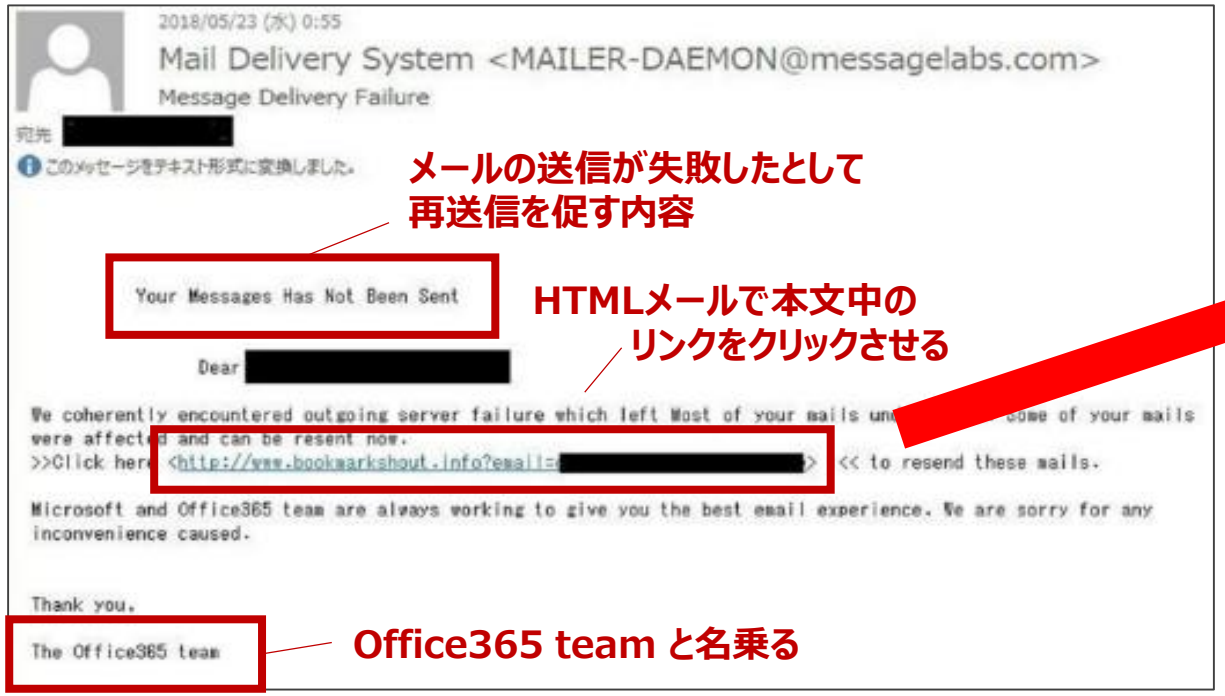
キーロガー
標的の端末にキーロガーを感染させ、メールアカウントの認証情報窃取や内部情報等を入手

フィッシング
クラウドメールサービスを利用している企業にフィッシングメールを送り、偽Webでのメールアカウントの認証情報を窃取

被害事例～クレデンシャルフィッシング～

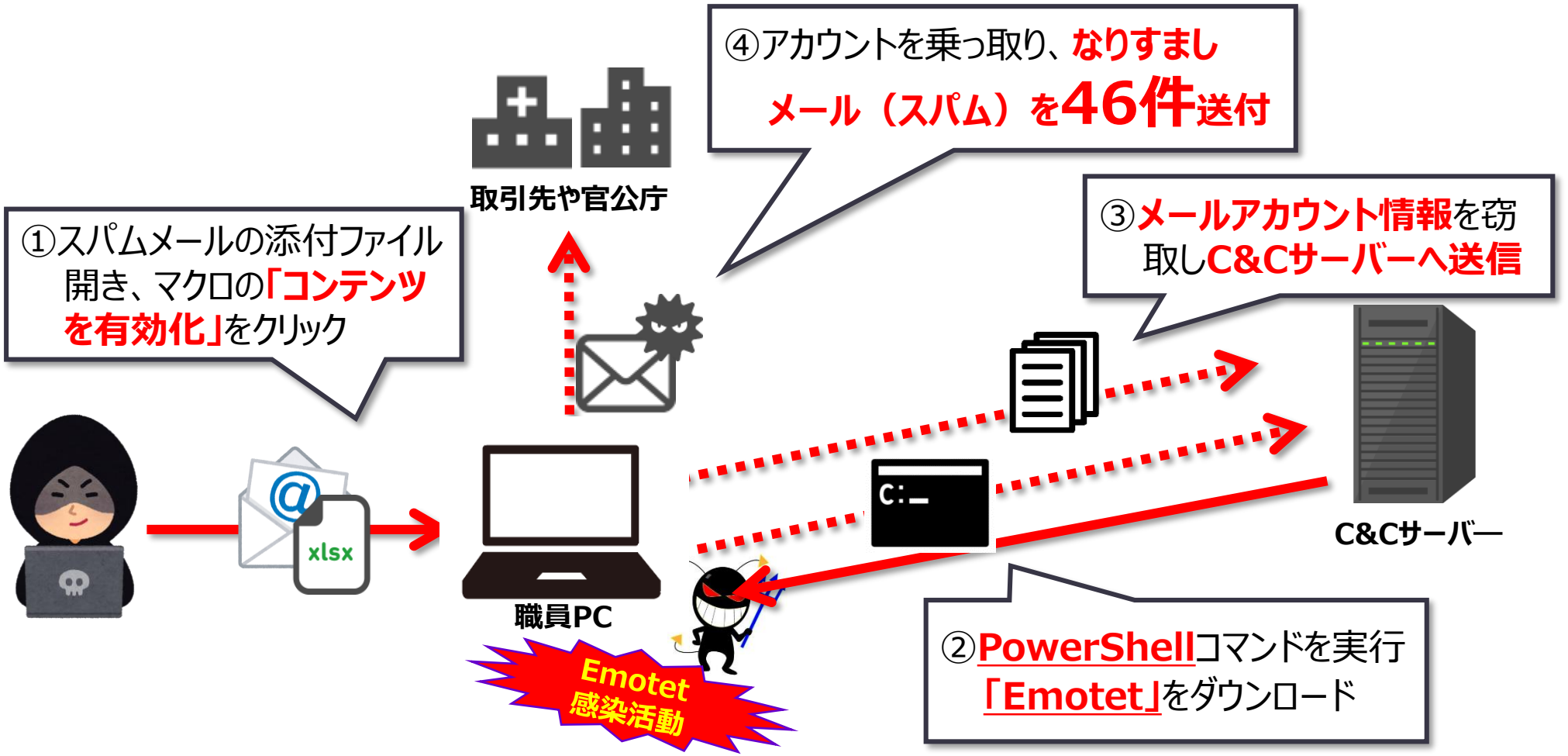
■Microsoftアカウントを狙った攻撃事例（H大学）

（漏洩）氏名、住所、電話番号、性別など2517件



被害事例～Emotet～　某都内医療センター

メールアカウント情報を窃取され、**クレデンシャル情報が漏洩**
アカウントが乗っ取られ、感染拡大を目的とした**スパムメールが拡散**



環境の変化①　リモートワークの拡大

働き方の変化

リモートワーク（自宅、外出先）

便利で柔軟な働き方が生産性を高める

⇒安心して働くため

セキュリティ対策と両立

環境の変化②　ＤＸの加速

企業の**ビジネスモデル（稼ぎ方）**が**デジタルによって変わる！！**

ＤＸ
（デジタル
トランスフォーメーション）

デジタライゼーション

ビジネスプロセスを
デジタル化

デジタイゼーション

アナログをデジタル
に置き換え

新たな価値、
ビジネスモデル
（社会の変革）

環境の変化②　ＤＸの加速

『データ』が肝になる　⇒　守るべき情報が増える

えびや様の例

出展:EBILAB様訪問撮影

セキュリティ対策は

皆様が

『やりたいことを実現するために必要』

なこと

セキュリティ対策のキーワード

ゼロトラスト

ゼロトラスト

（概念）

すべて信用しない（ネットワークは侵害されているとみなす）

「全ての通信を毎回チェックしましょう」

どのようにして信頼できる状態にするか？

ゼロトラストネットワーク設計

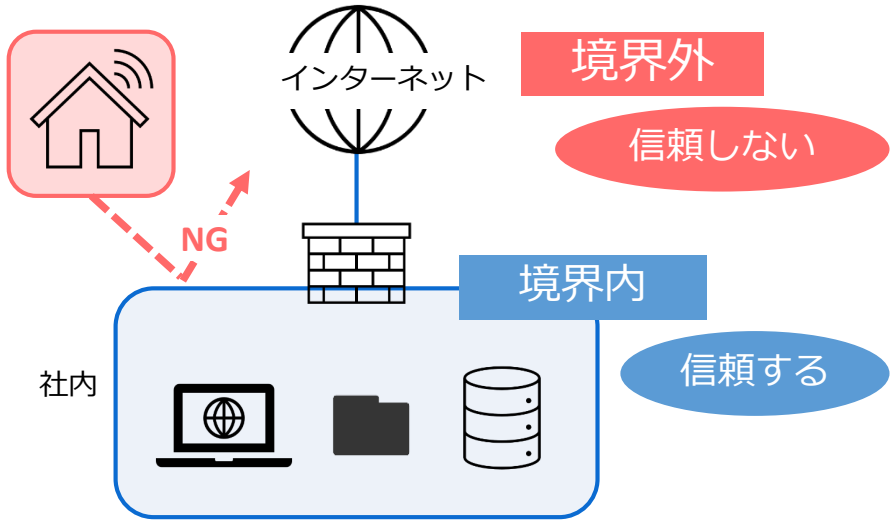
ゼロトラストという概念をもとに、

「安全なネットワーク、システムの設計をしましょう!!」

ゼロトラストモデル

境界防御モデル（従来）

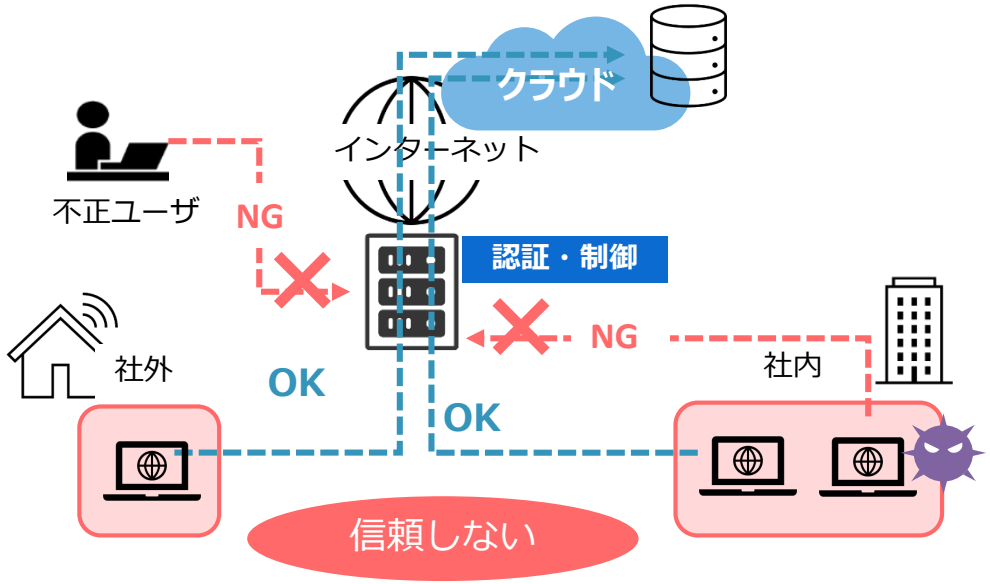
・**境界内（社内）は信頼**し、安全という考え方
・利用するシステム、端末は社内に設置
・社内と社外の境界でセキュリティ機器を導入し防御



社外からのアクセス遮断による利便性の低下
社内からの攻撃に対応が出来ない

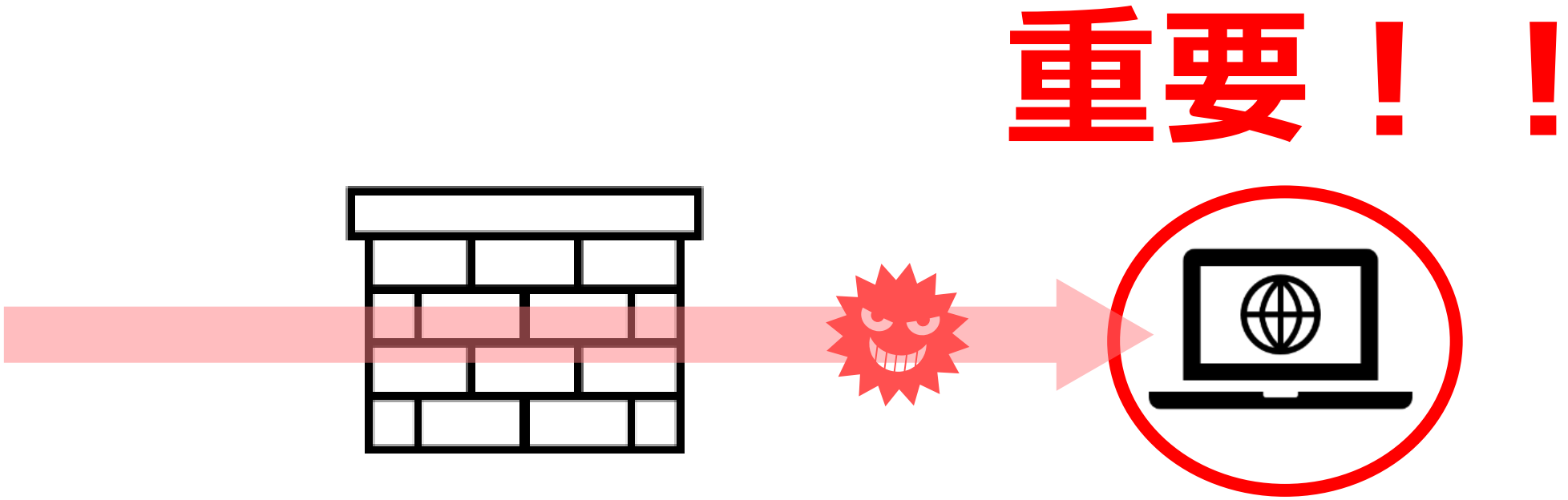
ゼロトラストモデル（今後）

・社内外問わず、**全アクセスを信頼せず**認証・制御する
・利用するシステム、端末は社内外どちらも想定
・認められた機器かどうか、端末の振舞いなどを見て防御

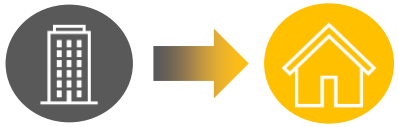


社内外を問わない働き方で利便性が向上
社内外の情報資産への攻撃もしっかり防御

エンドポイント対策が重要！！

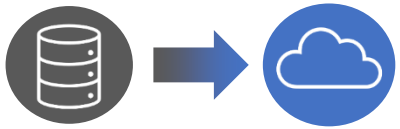


ゼロトラストモデルが必要な背景



働き方の変化

- 在宅勤務の増加
- コミュニケーションスタイルの変化



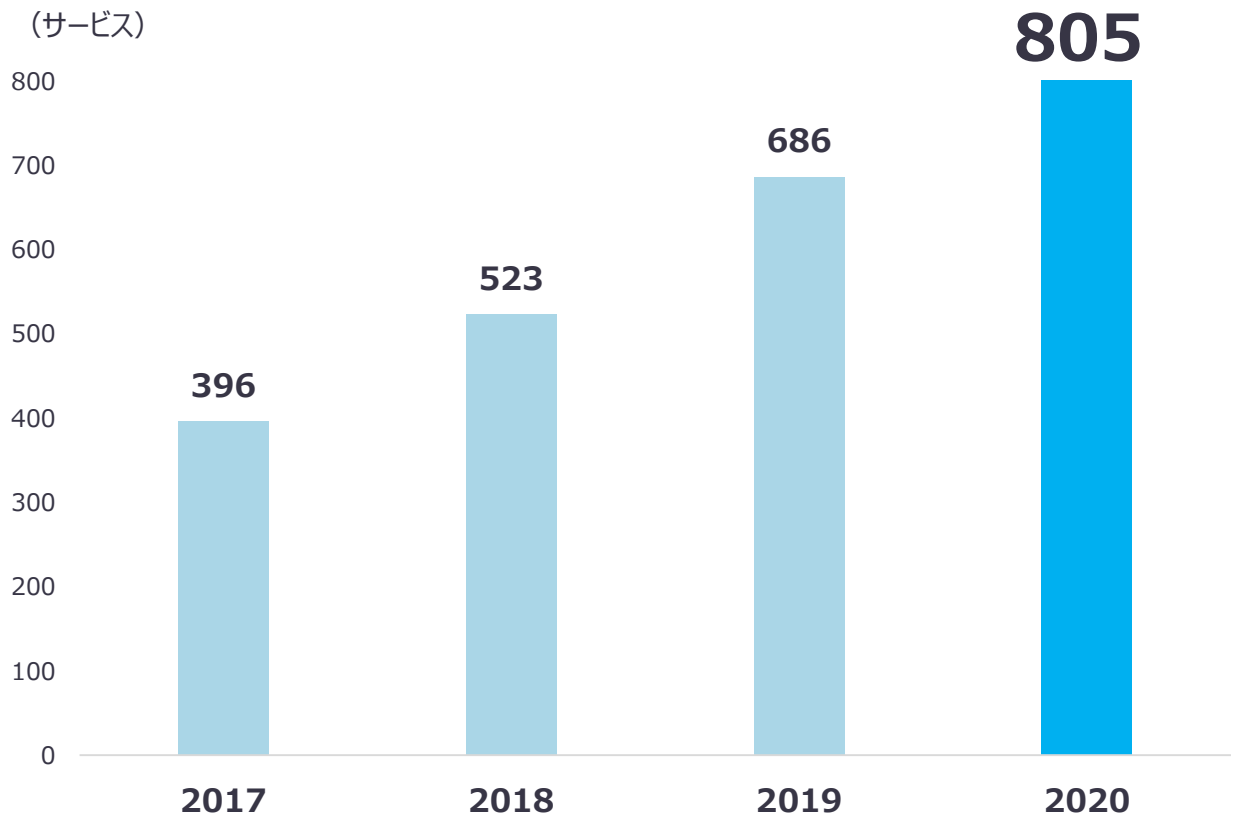
クラウドサービス利用拡大

- アプリケーション開発から利用(SaaS)にシフト
- パブリッククラウド等(IaaS)の利用が増加

Saasはカオスの状態

ＤＸを進めるためのSaasは『多種多様』（カオスの状態）

※Saas：Software as a Service（クラウドで提供されるソフトウェア）



【主なSaasのサービス数】

Web会議システム　**32**種類
（WebEX、BellFace、V-CUBE 等）

会計　**22**種類
（freee、勘定奉行、ちまたの会計 等）

ビジネスチャット　**31**種類
（Teams、slack、Chatwork 等）

オンラインストレージ　**20**種類
（OneDrive、Google Drive 等）

※SMARTCAMP「Saas業界レポート2020」より

働き方の多様化にともなう変化

導入のしやすさ、利便性からクラウドアプリのメール活用が増加

社内・自宅・外出先とどこでも同一ドメイン・アドレスで利用できる
クラウドアプリのメールを利用する企業が増加
（MS365やGoogleWorkSpace）

＜主な導入理由＞

- 導入が手軽（NW設計不要）
- サーバ運用不要
- どこでも使える（ネット接続のみ）
- サブスクモデル

メール機能の他、標準機能として実装している
「ストレージ」「ビジネスチャット」「Web会議」機能も利用

- Teams
- OneDrive・Googleドライブ
- SharePoint

便利なITツールとともに問題になるのは

利便性の高いITツールやアプリの増加とともに問題視されているのが・・・

シャドーIT

企業・組織側が把握せずに従業員または部門が業務に
利用しているデバイスやクラウドサービスなどのITのこと

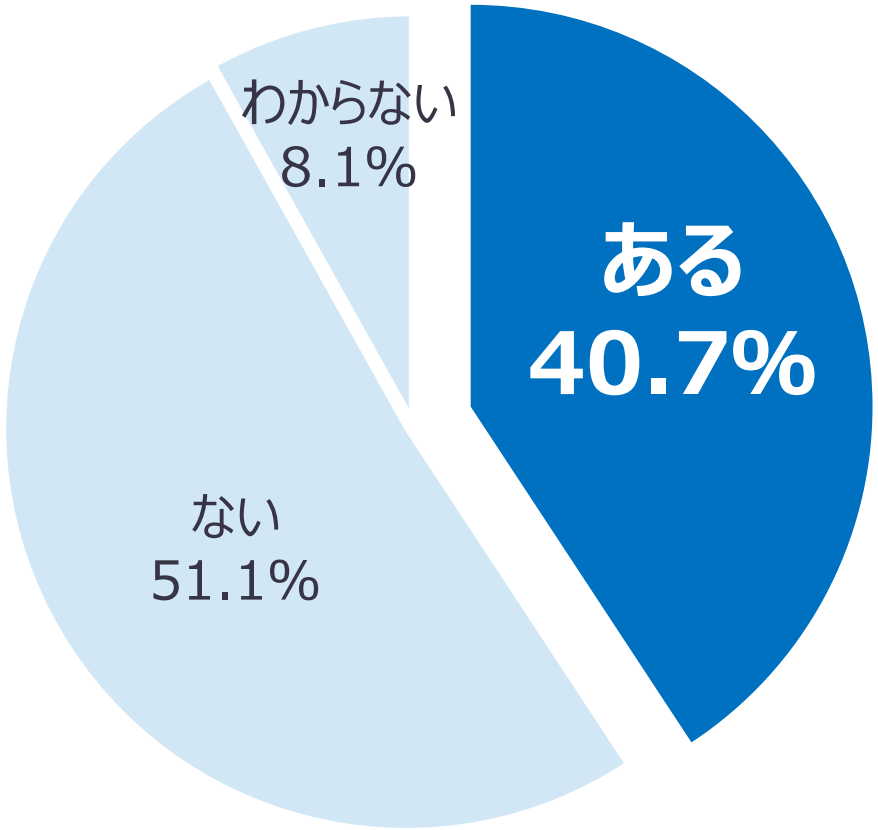
※wikipediaより

シャドーITの具体例

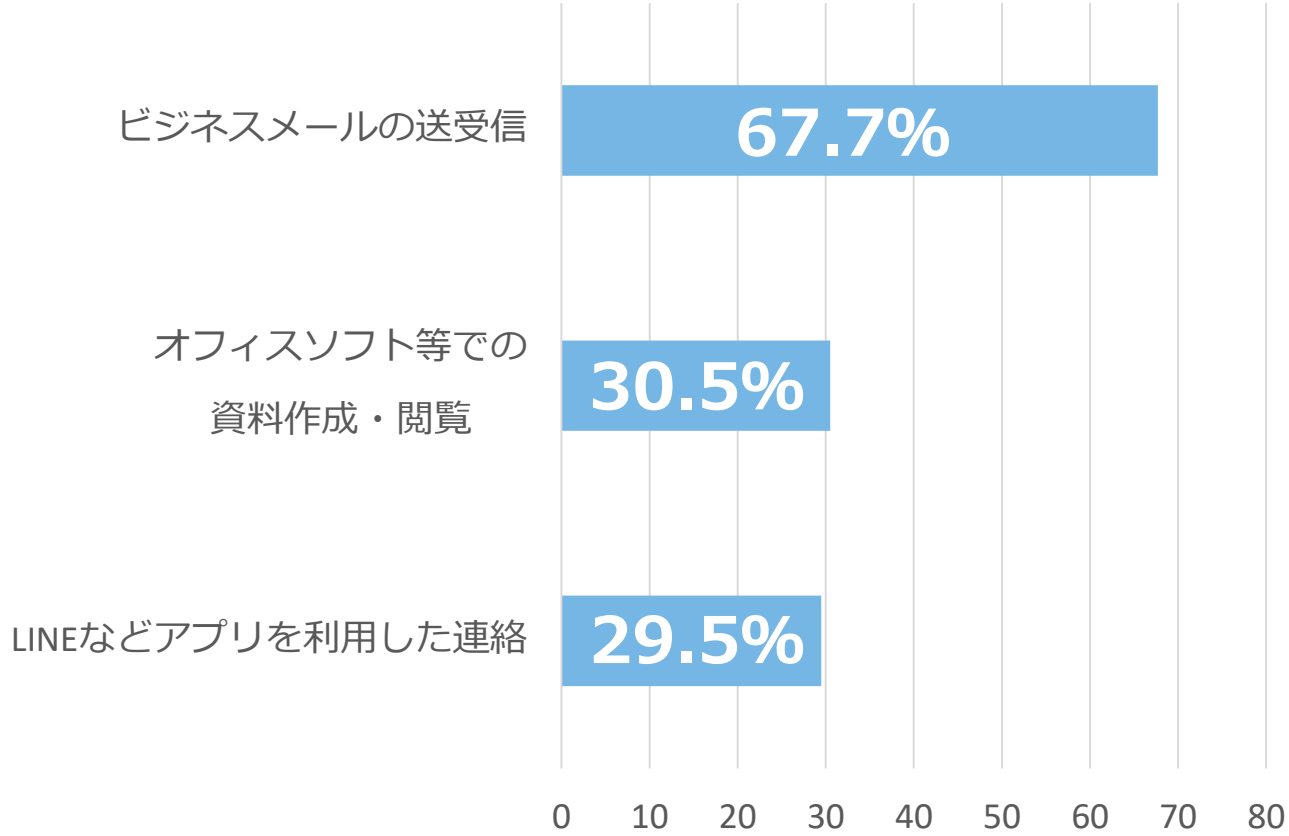
- スピーディにコミュニケーションしたい　→　**チャットアプリ**
- 業務の続きを個人パソコンで　→　**オンラインストレージ/ファイル共有アプリ**
- 出先で仕事したい　→　**個人スマホでテザリング/無料WiFi接続　など**

シャドーITの実態①

個人所有の端末を、勤務先の業務に使用したことはありますか？（n=700）



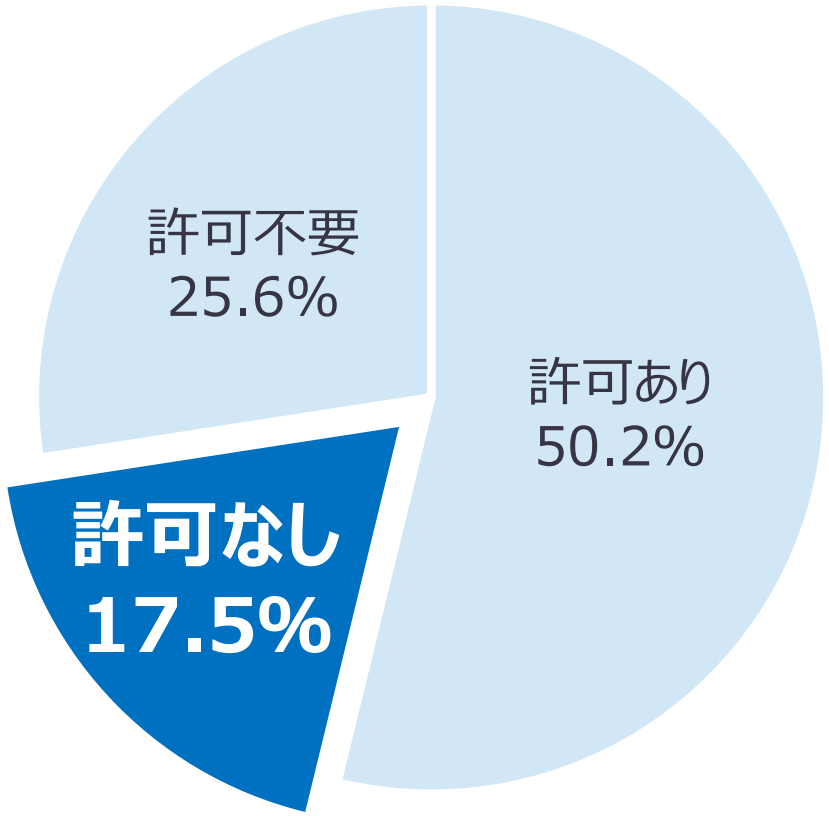
個人所有の端末で、どのような業務を行いましたか？（n=285）



（出典）キャノンマーケティングジャパン株式会社 「情報セキュリティ意識に関する実態調査レポート～把握しておくべき『シャドーIT』の実態について～」2020年3月13日

シャドーITの実態②

個人所有の端末は、業務利用できるよう勤務先から許可を得られていますか？（n=285）

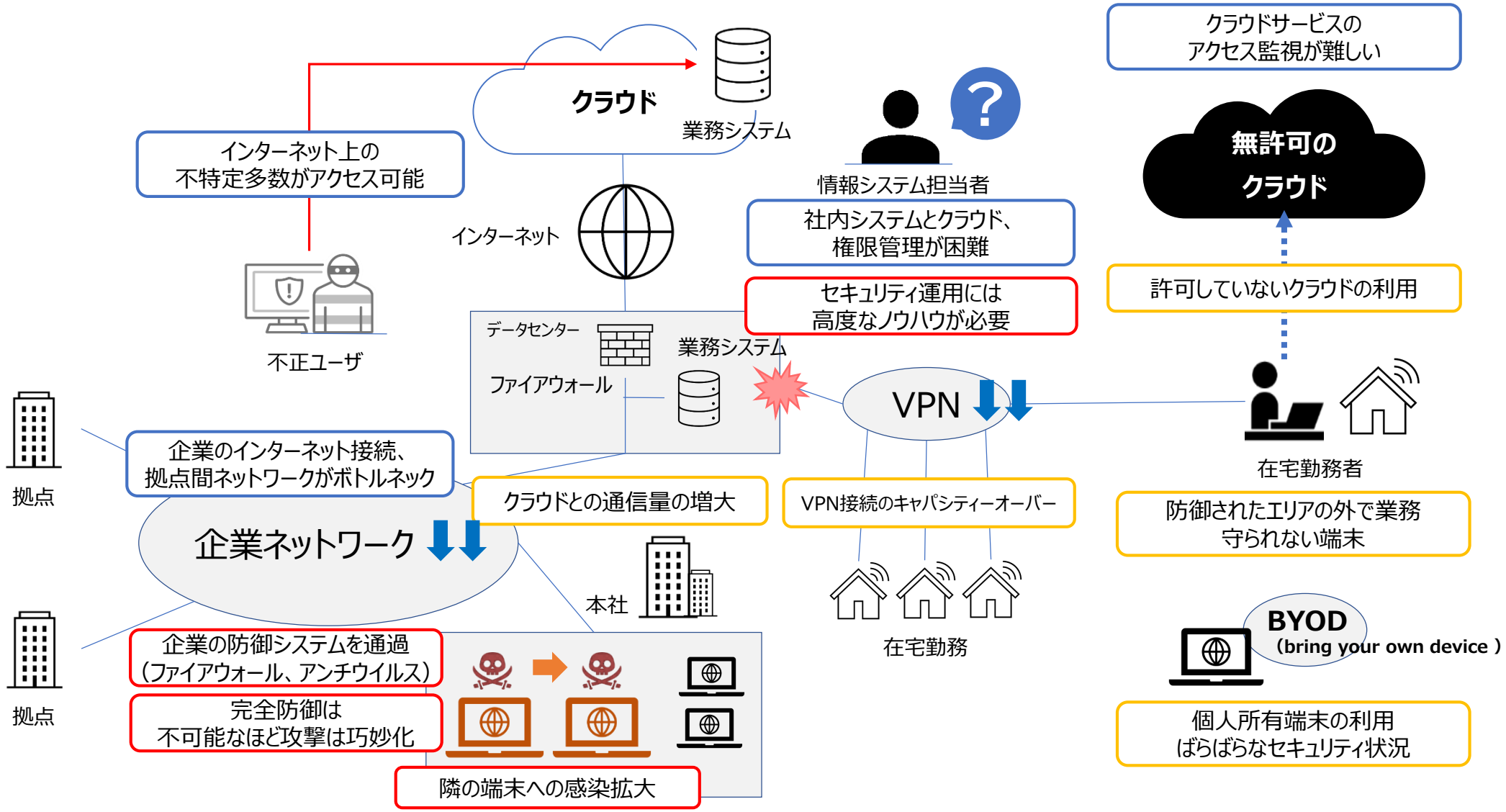


セキュリティリスクが極めて高い！

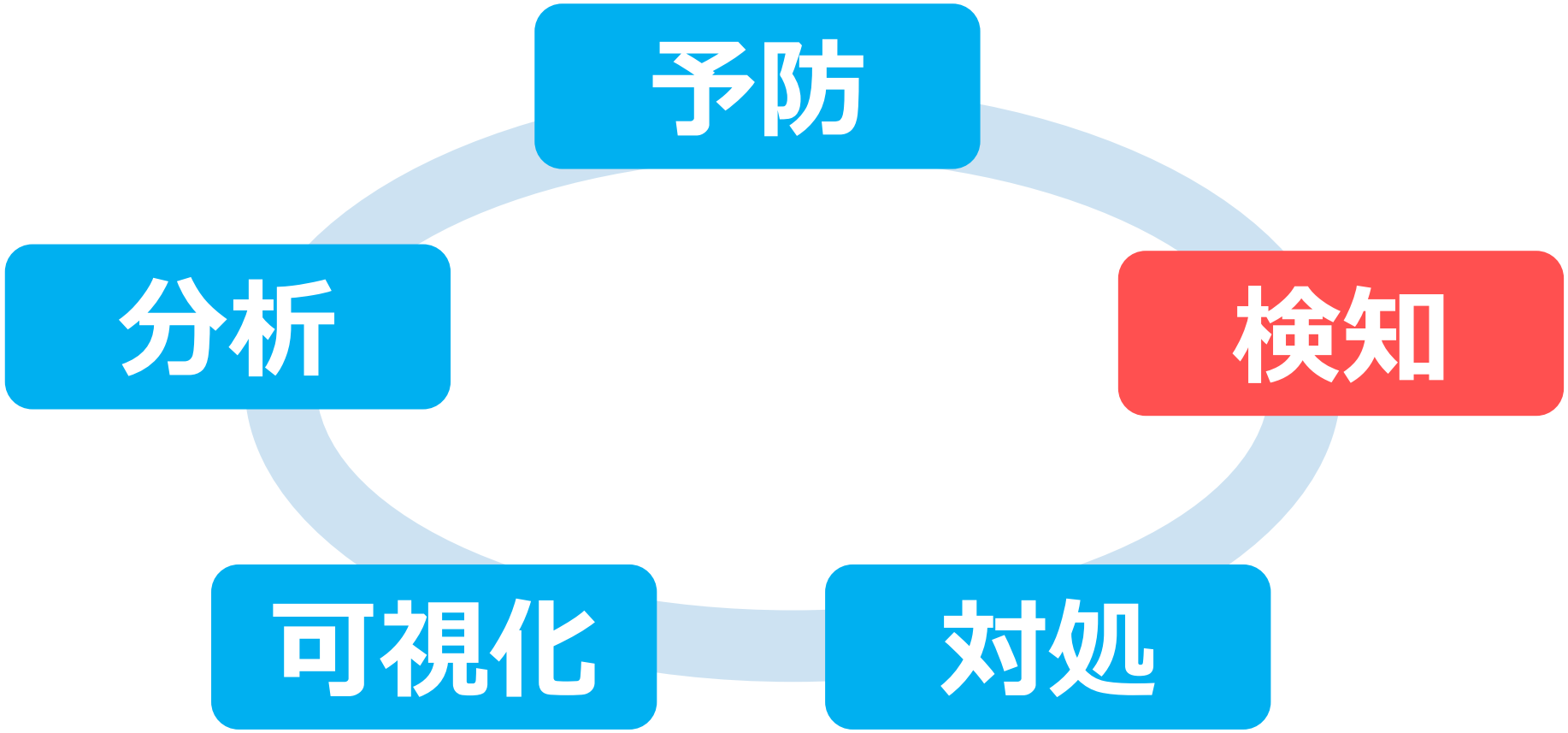
（出典）キャノンマーケティングジャパン株式会社 「情報セキュリティ意識に関する実態調査レポート～把握しておくべき『シャドーIT』の実態について～」2020年3月13日

対策のポイント

企業ネットワークにおける課題



求められるセキュリティ脅威への対策



伝えたいポイントは大きく**4**つ

①環境把握
②エンドポイント対策（ＥＤＲ）
③Saas利用対策
④社員教育

現在の状況を棚卸しする

デバイス（機器類）	認証	メール	Saas（クラウド）

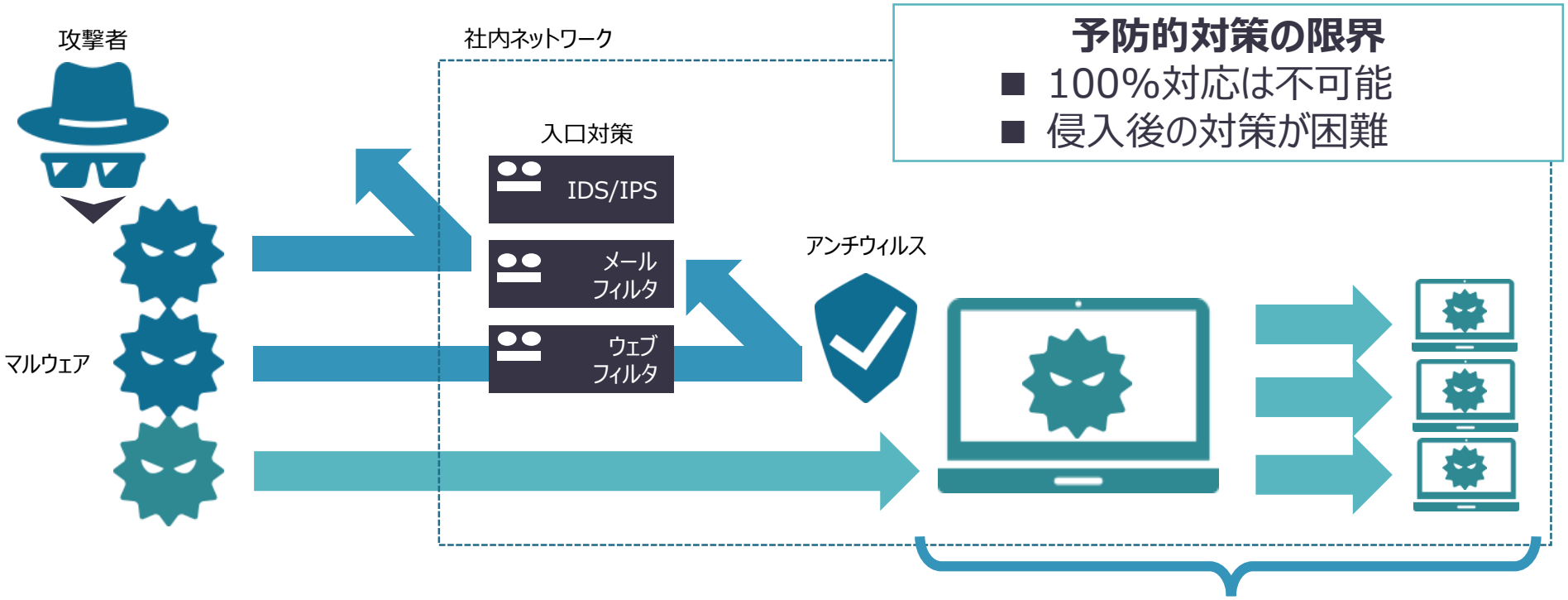
セキュリティ対策

導入時期、利用サービスもバラバラな場合もある
働き方の変化によって、使うものも変化
把握しきれない場合　⇒　外部に任せる

対策ポイント②

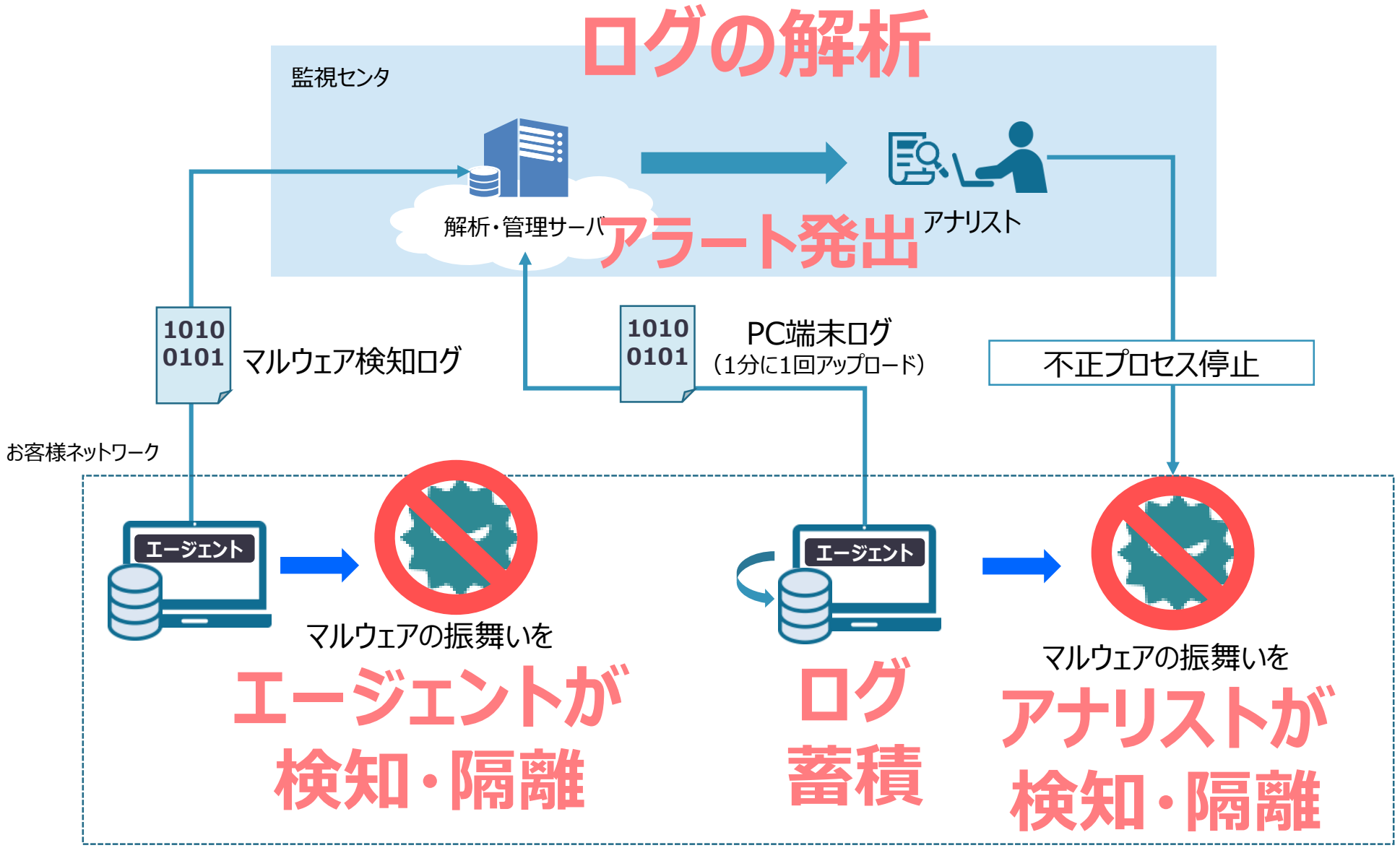
脅威の侵入を前提としたソリューション

高度化を続ける脅威の侵入を完全に予防することは困難であるため、予防的対策だけに頼らず、脅威の侵入を前提として被害拡大を回避する



EDRは内部に侵入したセキュリティ脅威の痕跡を検出、影響範囲の特定と対応を実現

EDRの仕組み


ログの解析
監視センタ
解析・管理サーバ
アラート発出
アナリスト
1010
0101
マルウェア検知ログ
1010
0101
PC端末ログ
（1分に1回アップロード）
不正プロセス停止
お客様ネットワーク
エージェント
エージェント
マルウェアの振舞いを
エージェントが
検知・隔離
ログ
蓄積
マルウェアの振舞いを
アナリストが
検知・隔離

（参考）　公的機関からも求められるEDR導入

経済産業省
サイバーセキュリティ経営ガイドライン※1

ITサービス等を供給する企業、経営戦略上IT利活用が不可欠な企業の経営者を対象とする文書。
この文書に基づいた「サイバーセキュリティ経営ガイドライン Ver2.0実践のためのプラクティス集」の

「5-1.多層防御」でEDRの利用を例示

※1
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

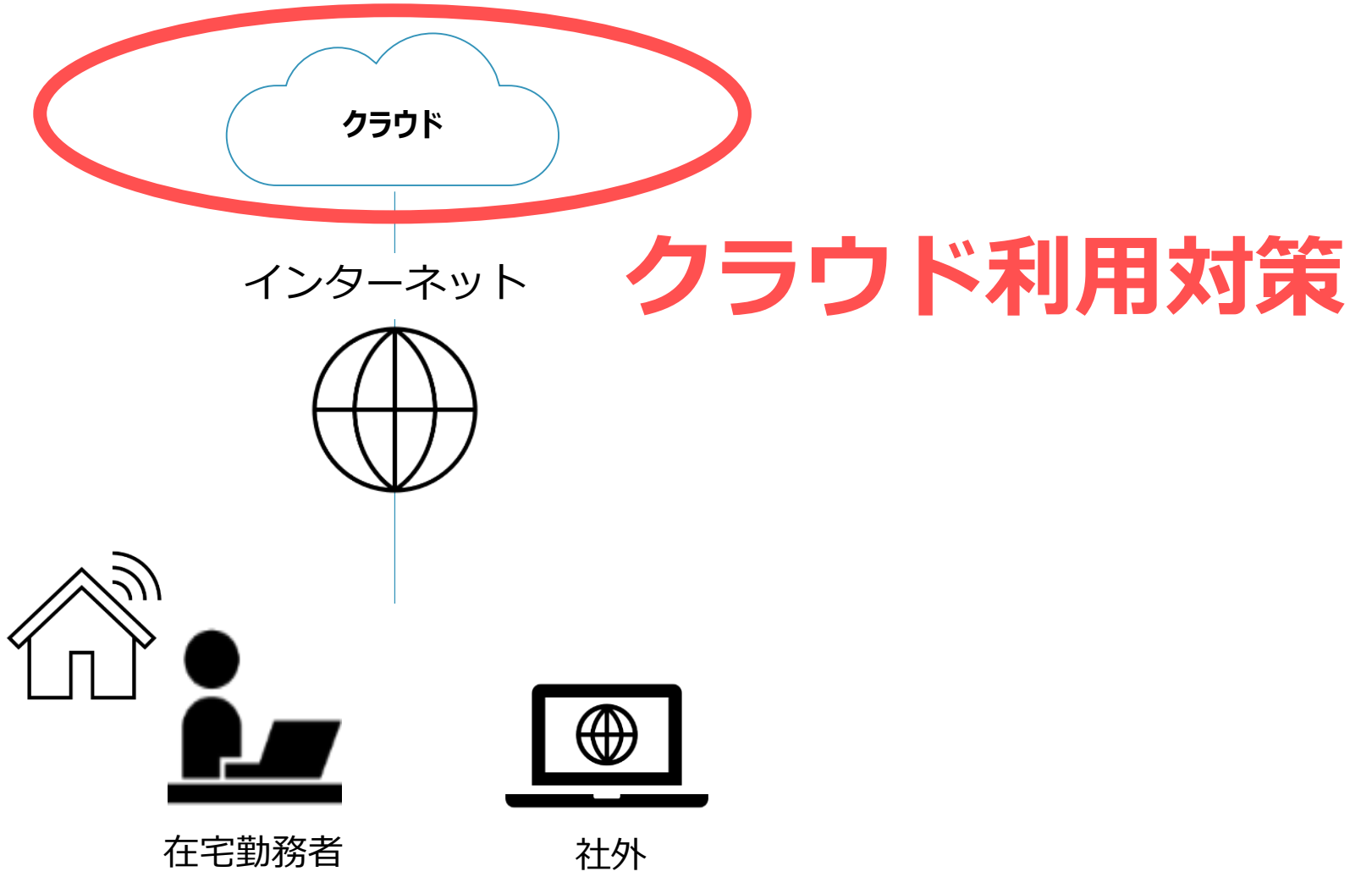
内閣サイバーセキュリティセンター
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針※3

代替困難なサービスを提供する事業者の業務システム等を重要インフラと位置づけ、安全基準等をまとめた文書。
「急速な被害拡大に繋がる攻撃が行われる可能性」に対する

平時の対策として、「EDR(影響範囲の特定と被害端末の隔離)」
を規定

※2　https://www.nisc.go.jp/materials/index.html

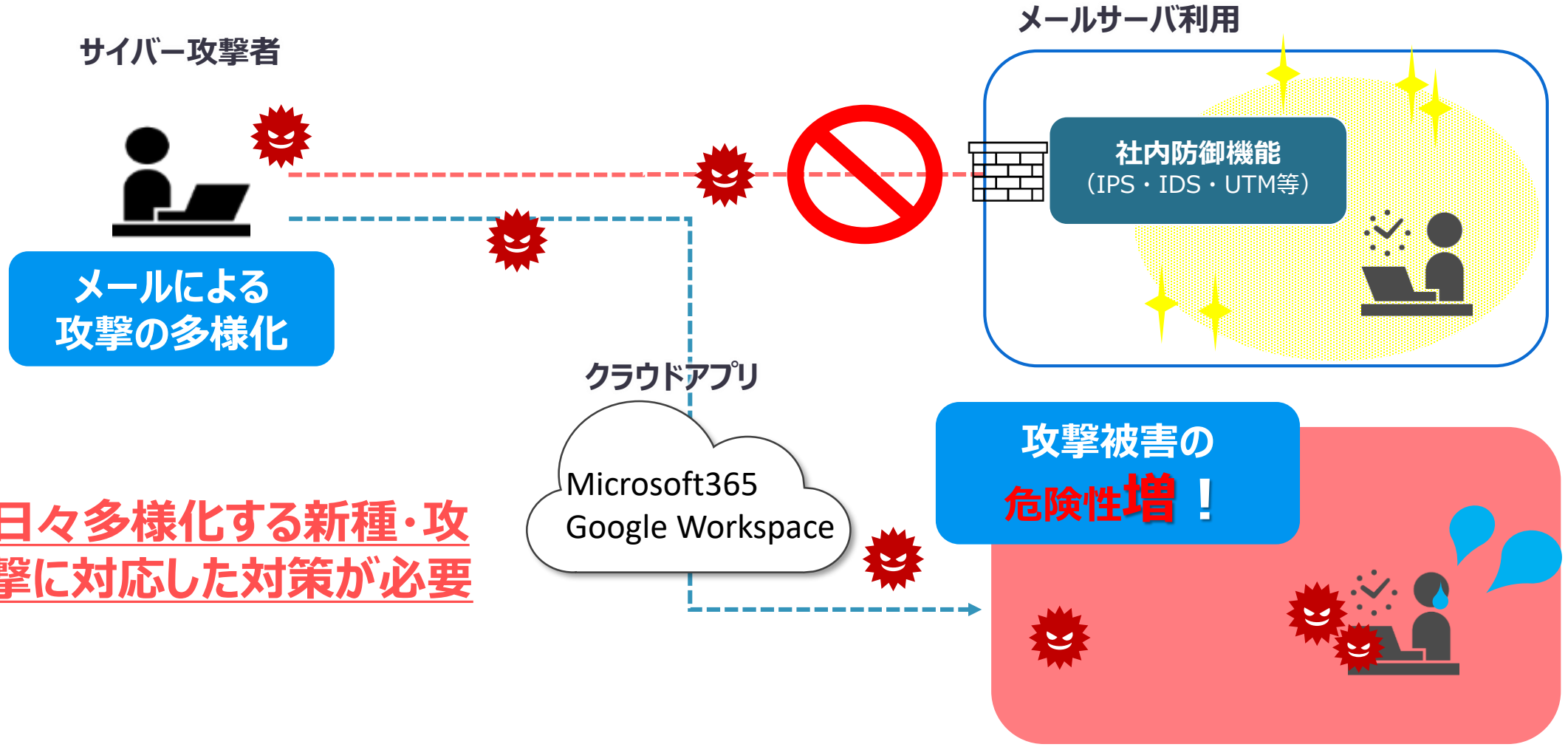
対策ポイント③



クラウド利用対策

クラウドアプリ型メールにはセキュリティ機能が働かない？

社内ネットワーク対策のUTM等のセキュリティ機能が働かない？

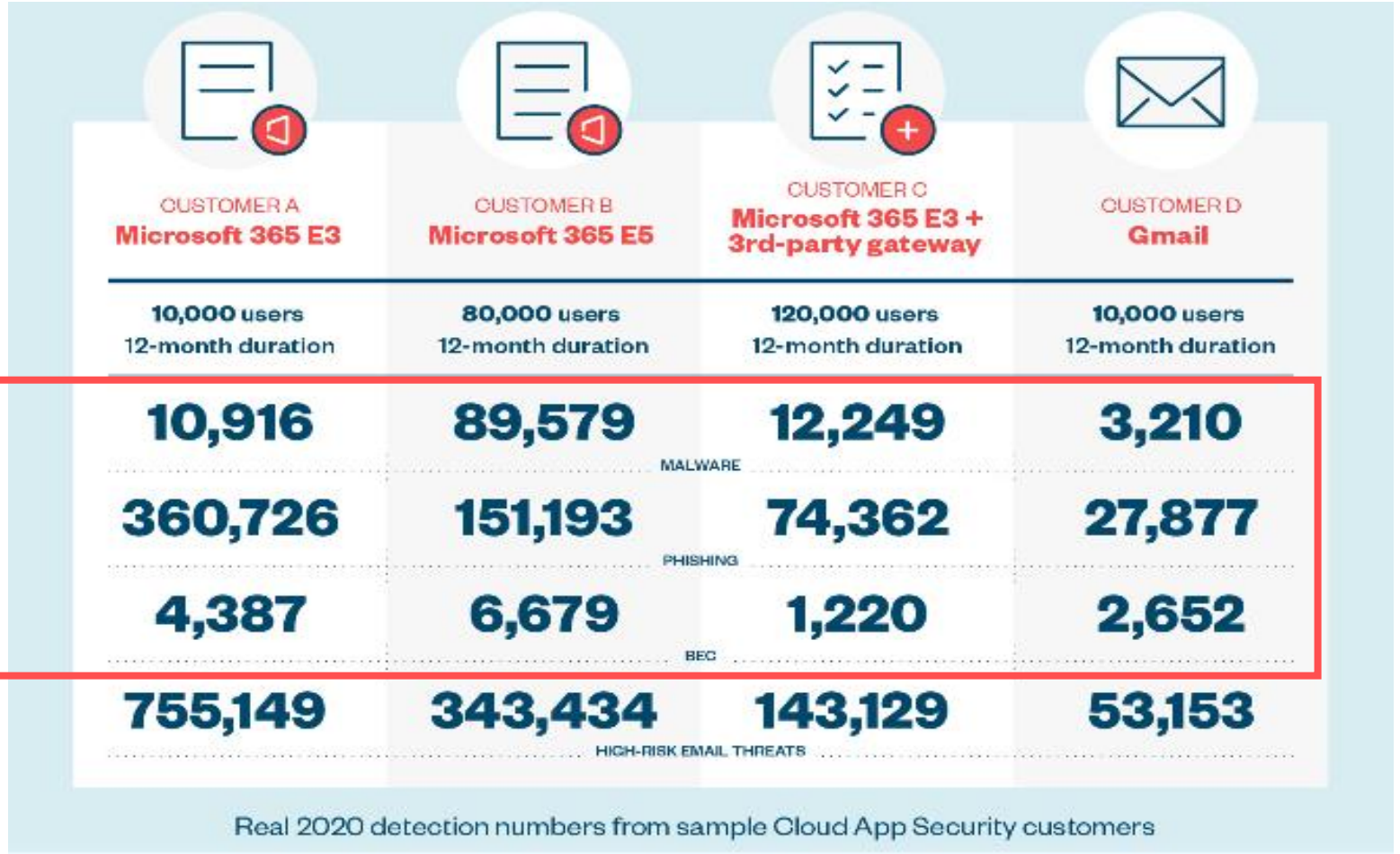


日々多様化する新種・攻撃に対応した対策が必要

セキュリティをすり抜けた脅威の数

膨大な数の脅威がセキュリティフィルタをすり抜けている現実
⇒クラウド時代にマッチしたセキュリティ対策を推奨

Trend Micro Cloud App Securityのユーザ側で検知された数値



マルウエア

フィッシング

ビジネスメール詐欺

Saasセキュリティ対策

クラウドアップセキュリティ

■クラウドアプリに対する
脅威検知・防御

■導入・初期
設定支援

■運用サポート
■セキュリティレポート報告
■ウイルス感染時の**遠隔**
駆除支援

ＡＩがメールを分析！！

経営者等のメールの
書き方（特徴）を分析
（500~800通のメール）

大文字の利用頻度
文章の長さ
空白の頻度　等

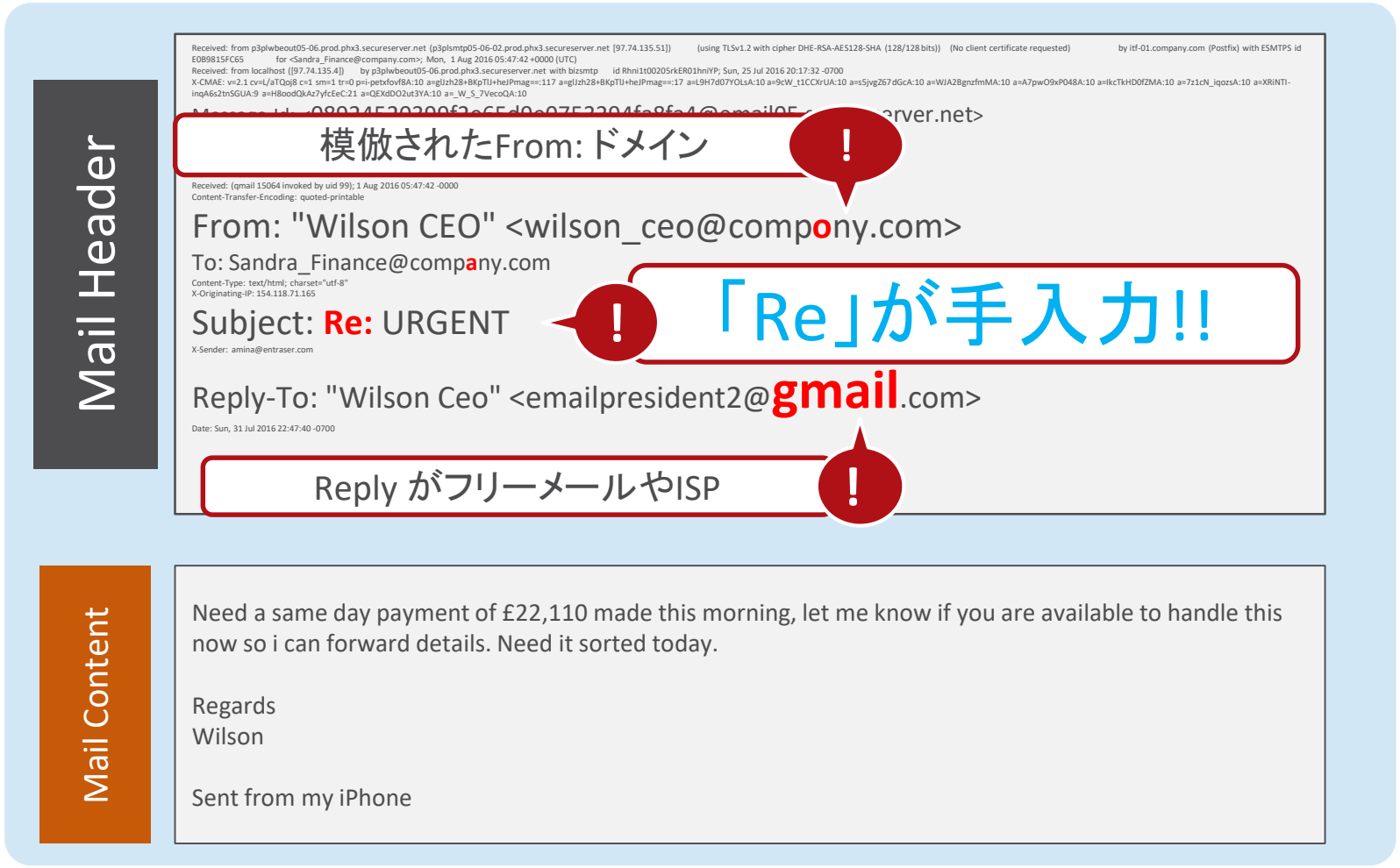
約7,000の特徴

いくつかの**特徴と一致しない怪しいメール**は・・・

「①偽装された本当の経営幹部」、「②企業の管理者」、
「③宛先の受信者」へ**警告や通知！！**

機械学習機能

機械学習により、模倣されたドメインや、FromメールアドレスとReplyメールアドレスの違い等を検知



対策ポイント④

社員教育

人的リスク対策の必要性

リモートワークの拡大　⇒　**周りの目がない**

⇒ **リスクが高まる**

能動的＆密なコミュニケーションが大事ですが・・・

効果的な人的対策ソリューション

体系的・体験的学習で、社員の意識を向上

eラーニング（学科）

体系的な知識の習得・確認

学習による全社員の知識の平準化

標的型攻撃メール訓練（実技）

標的型攻撃メールを疑似体験

情報セキュリティ意識に
対する現状把握

攻撃メール例

金融機関を騙った文面やコロナ感染症に関する文面での攻撃メール

・件名：
＜重要＞〇〇ご利用確認のお願い

・本文：
いつも弊社カードをご利用いただきありがとうございます。

昨今の第三者不正利用の急増の伴い、弊社では「不正利用監視システム」を導入し、24時間365日体制でカードのご利用に対するモニタリングを行っております。

このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認に協力をお願いいたします。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承ください。

■ご利用確認はこちら
https://〇〇〇〇

■発行者
〇〇〇〇〇
〒〇〇〇〇〇〇

クレジットカード会社を騙ったフィッシングメール

・件名：
通知2020 Jan 29

・添付：
instruction Jan 29 2020.doc

・本文：
管内　通所・施設系障害福祉サービス事業者　様

お世話になっております。

新型コロナウイルス関連肺炎については、中国武感市を中心に患者が報告され、国内でも〇〇県　で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。
なお、並行してワムネット〇〇〇ページへの掲載準備をしております。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
〇〇〇〇保健所福祉室（担当：〇〇）
〒〇〇〇〇〇〇〇〇〇〇〇〇〇〇〇
電話：〇〇〇〇〇
FAX：〇〇〇〇
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

新型コロナウイルスを題材とした攻撃メールの例

こんなメールを受領したら・・・

【緊急】標的型攻撃メールの対応について

従業員各位

当社宛てに標的型攻撃メールが多数届いています。
各自以下のURLをクリックし、自分のパソコンの状況を確認して下さい。

<URL>・・・・

「危険」判定が出ましたら一刻も早く情報セキュリティ部に連絡して下さい

https://special.nikkeibp.co.jp/atclh/NXT/19/ntteast/10/

（余談ですが・・・）
私がひっかりそうになった訓練メール

■実在する大学の学生からの履歴書送付

■社内システム関係の緊急対処

こんなメールきました・・・

【重要なお知らせ】

楽天銀行株式会社
残念ながら、あなたのアカウントを更新できませんでした。
これは、カードが期限切れになったか。
請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。
今アカウントを確認できます。
楽天銀行ログイン <https://rakuten…>
なお、12時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただくことを警告いたします
パスワードを変更した覚えがない場合は、至急 （01）20-●●-●● までお電話ください。

自ら成長し、仕事を通じて、社会の発展・変革に寄与し、より良い世界を実現する
人間の可能性を信じ、仲間と顧客をEmpowerすることにコミットする人と社会を（ネットを通じて）Empowermentし、自らの成功を通じ社会を変革し豊かにする。
当事者意識・経営者意識を持ち、日々の業務に邁進する。

⇒SPAMメール扱い

⇒経営理念は、本物のＨＰを見ると似たようなことが書いてありました・・・

添付ファイルは開かない・・・？

訓練メールの開封率

25.4%

142通/560通

（参考）

建設・不動産	36.2%
経営者・経営幹部	33.3%

（出典）東京商工会議所 「標的型攻撃メール訓練実施結果」（2019年6月）
https://www.tokyo-cci.or.jp/page.jsp?id=1018002

標的型メール訓練の効果

訓練メールの開封率は、2回目で約半分に

1回目

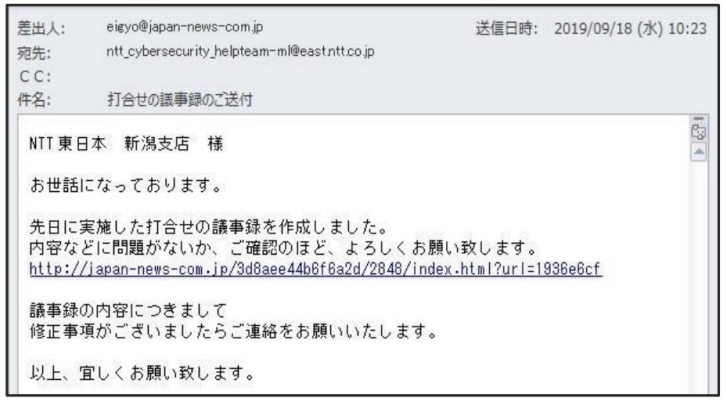
20.7%

41通/198通

2回目

13.6%

27通/198通


差出人: eigyo@japan-news-com.jp　送信日時: 2019/09/18 (水) 10:23
宛先: ntt_cybersecurity_helpteam-ml@east.ntt.co.jp
CC:
件名: 打合せの議事録のご送付

NTT東日本　新潟支店　様

お世話になっております。

先日に実施した打合せの議事録を作成しました。
内容などに問題がないか、ご確認のほど、よろしくお願い致します。
http://japan-news-com.jp/3d8aee44b6f8a2d/2848/index.html?url=1936e8cf

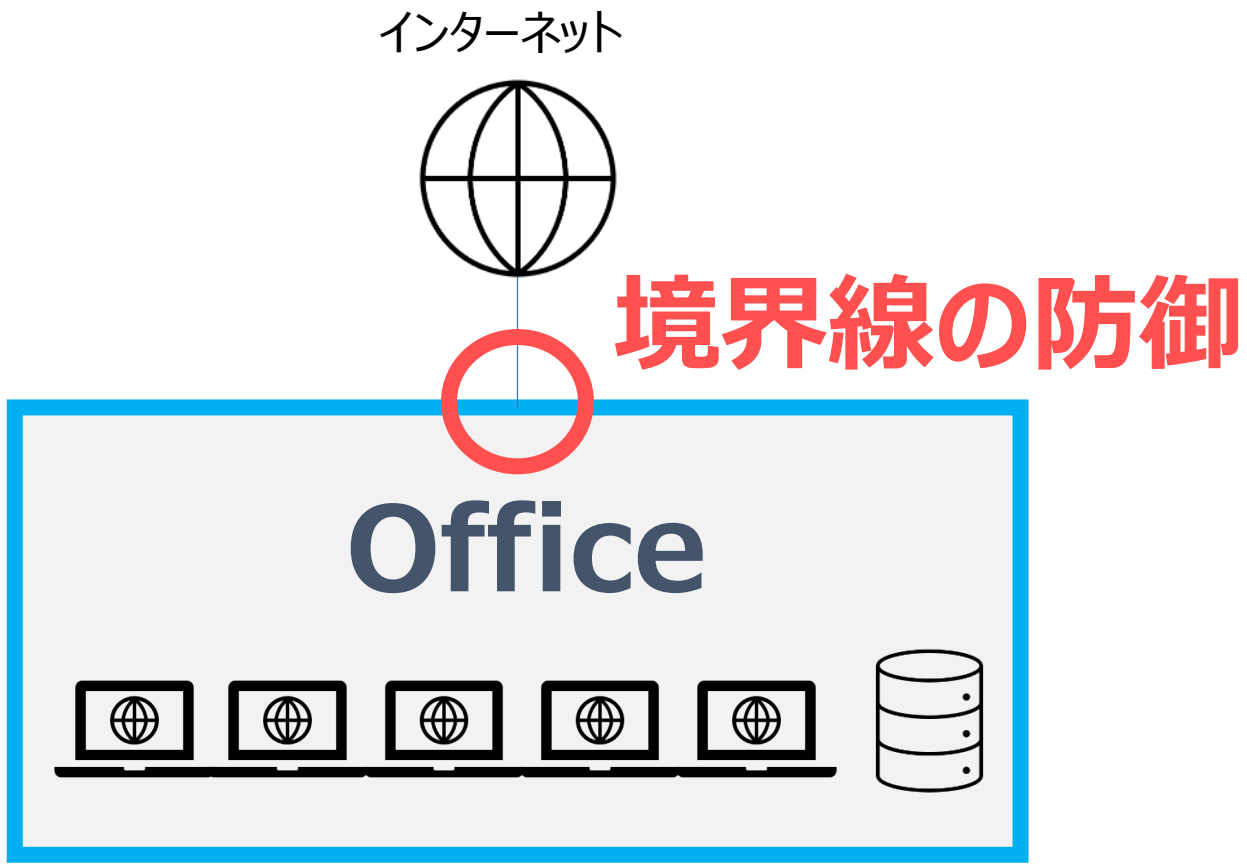
議事録の内容につきまして
修正事項がございましたらご連絡をお願いいたします。

以上、宜しくお願い致します。

2回目のみ開封者	**2回とも開封者**
13名	**14名**

（出典）成果報告書 - IPA 独立行政法人 情報処理推進機構「中小企業向けサイバーセキュリティ事後対応支援実証事業」
https://www.ipa.go.jp/files/000082726.pdf

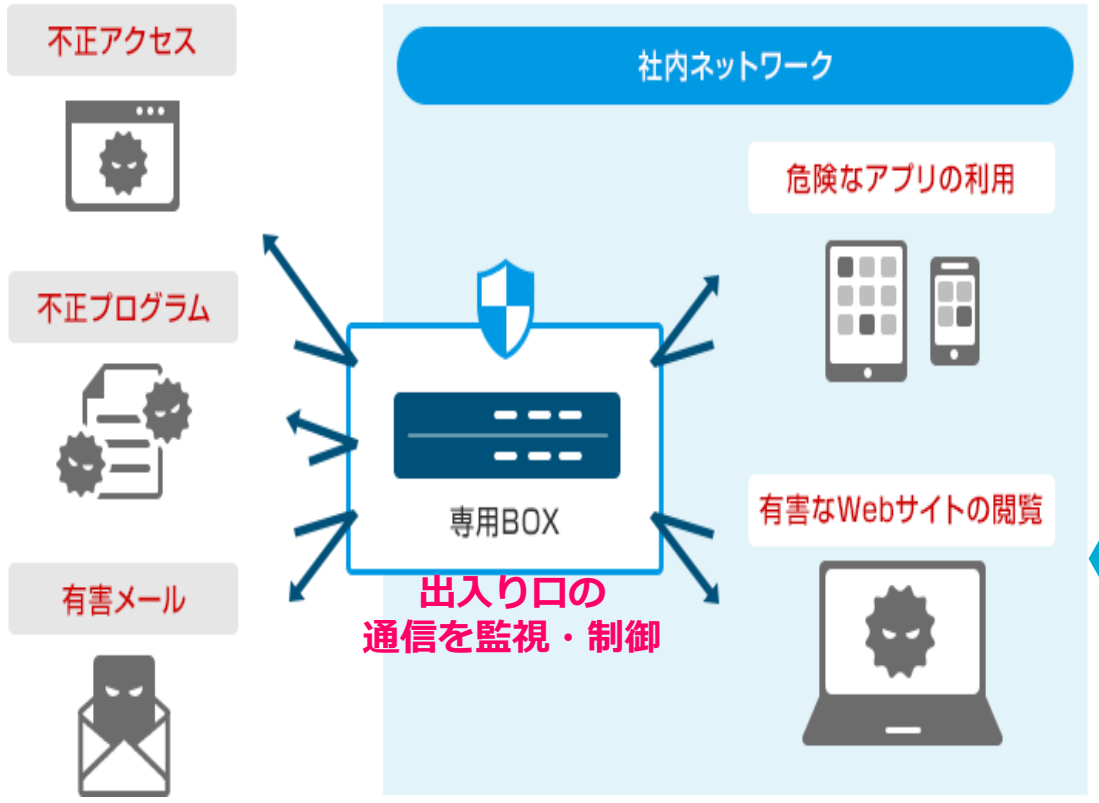
（参考）基本的な対策



基本の出入り口対策

社内ネットワークを守るUTM＋サポートサービス

- 侵入防御・侵入検知
- ウィルス対策
- 不正メール対策
- Webサイト フィルタリング



- 感染時の駆除 復旧支援
- 365日ヘルプデスク

お伝えたえしたポイントは **4** つ

①環境把握
②エンドポイント対策（ＥＤＲ）
③Saas利用対策
④社員教育

セキュリティ対策は

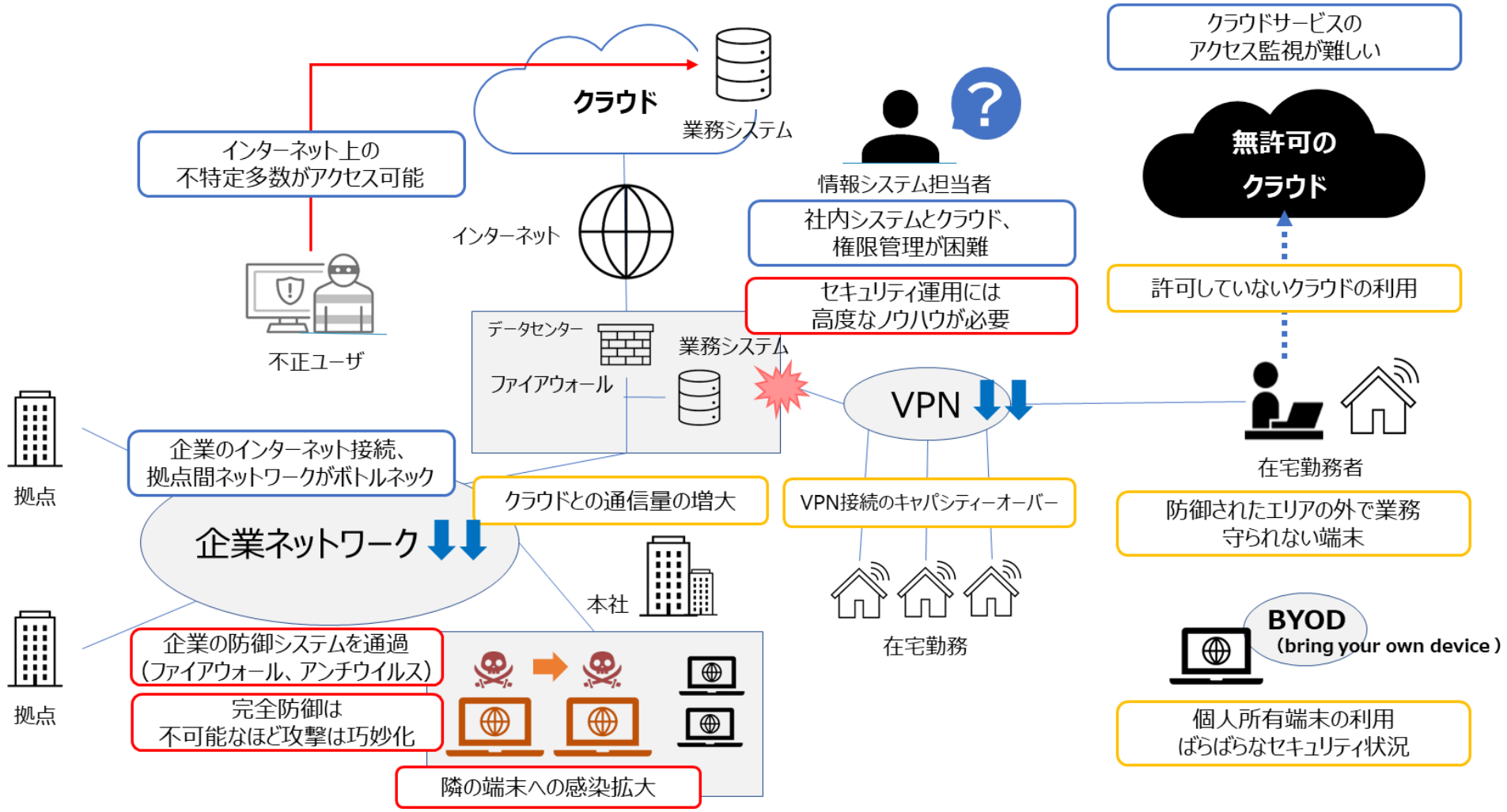
皆様が

『やりたいことを実現するために必要』

なこと

（まとめ）企業ネットワークにおける課題

働き方の変化に伴い、利便性とセキュリティの両立が必要



働き方の変化

クラウド利用拡大

サイバー攻撃多様化

NTT東日本のゼロトラストセキュリティソリューション

ゼロトラストセキュリティを実現するため、
最適なネットワークおよびセキュリティを検討し、
導入から運用サポートまで一元サポート！

検討

現状課題を整理
最適案を
一緒に検討

商品選定

社内外問わず、
お客さまに最適
な商品を選定

導入

導入に伴う
サポートを実施

運用

お客さま稼働の
最小化のため
に、
弊社で一部運用
代行可能


ICTる？
ICTで、地域とともに
地域活性化×NTT東日本グループ