Digital Security

KDDI × LAC

地方・中小企業も危ない！
専門家が伝える情報セキュリティについて

―最近のセキュリティのトレンド！事例を交えながら紹介

―中小企業が取るべきセキュリティ対策とは？

本日のセミナー内容

01

社会環境変化に伴いサイバー攻撃も変化

経営者・従業員、インターネットサービスを利用する一般の方においては、サイバー攻撃を十分に理解し対処する必要がある

本セミナーでは、社会環境変化に伴う注意点、
最新のインシデント事例と対策すべき事項を紹介

目次

講師について

講師

KDDIデジタルセキュリティ株式会社(略称KDSec)
CROSS本部セキュリティプランニング部　部長

志野 陽一

経歴

1999年	(現)富士通 入社。帝国データバンク様向けWebシステム（企業与信）開発担当
2001年	(現)ソニーグローバルソリューションズ 入社。本社役員専用OAインフラ周りを担当
2003年	(現)KDDI 入社。法人向けのマネージドセキュリティサービスなどを担当 並行してオンラインゲーム基盤（モンハン等）/au系エンタメシステムのセキュリティを担当
2007年	法人企業向けサイバーセキュリティ対策/インシデント緊急対応/KDDI本社SOCなどの業務に従事
2018年	LAC社との合弁企業KDSecに出向し現在に至る

主なPJ　愛知万博NW/東芝グローバルNW/中央省庁SOC/日韓半導体合弁工場（台湾）立上

インシデント対応　フィリピン（建設会社）、タイ（商社）、ロシア……など

※2011-2013 日本セキュリティ監査協会（JASA）委員　2015-2017幹事
※CISSP（ISC2)、情報処理安全確保支援士、公認システム監査人（CISA）等の資格保有

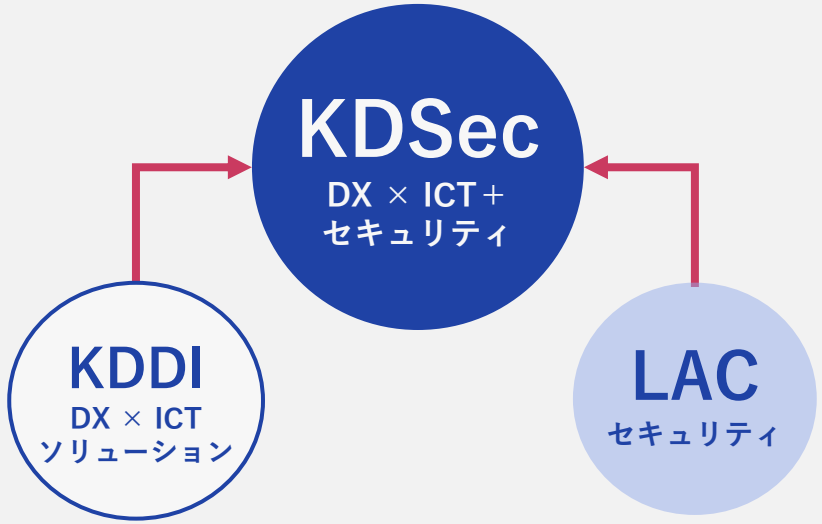
KDDIデジタルセキュリティ（KDSec）

01

サイバーセキュリティ事業 国内トップ企業であるLACと、KDDIの通信を主体とした様々なソリューション共創により、
DX×ICT＋セキュリティをワンストップでご提供

設立背景

セキュリティ＋DX×ICTの提供により
お客様事業の拡大に貢献



通信事業者としての
サイバー攻撃ノウハウ

サイバーセキュリティ分野
のフロントランナー

会社概要

社名	KDDIデジタルセキュリティ株式会社
英文社名	KDDI Digital Security Inc.
設立年月日	2018年2月19日
本社所在地	東京都千代田区九段南３丁目３－６ 麹町ビル５F
資本金	2.5億円
株主	KDDI51%　LAC49%
従業員	312名（2023年4月1日時点）
代表取締役長	菅　雅道

- 2018 会社設立
- 2019 Zscaler 提供開始
- 2020
- 2021 CrowdStrike 提供開始
- 2022 C119取次サービス 提供開始
- オリジナル診断サービス 提供開始

サイバー攻撃の脅威を意識せずに自社の事業に専念することができ、
万一サイバー攻撃にあっても、迅速に**被害を最小化できる世界を実現**

02

様々な環境変化

社会環境変化

02

環境変化

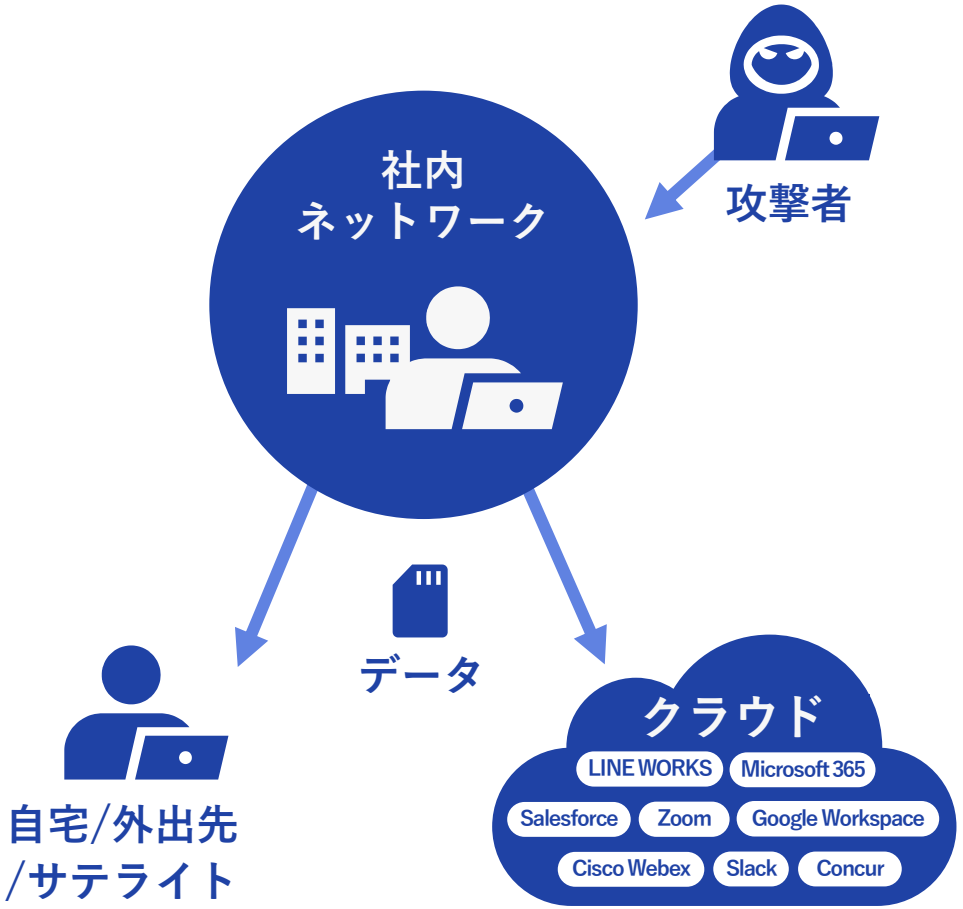
- コロナ
- テレワーク
- Web会議
- 業務場所
- クラウド利用
- DX活用
- 法律の変化（個人情報保護法改正等）
- 少子高齢化

課題

- インターネット回線の輻輳
- ITインフラ負担増
- サイバー攻撃の高度化
- クラウドサービス設定不備
- 人材不足
- 内部不正
- コスト削減
- 業務効率化
- 介護/育児

働き方の変化で変わる業務環境

「働きやすさ」と「セキュリティ」を両立したIT環境へ



01 | 働く場所

働き方の多様化
（PCが社外へ） → 利便性と
つながりやすさ

02 | データ・アプリ

業務のクラウド化
（データ・通信が社外へ） → データ保護と
認証・アクセス制御

03 | セキュリティ

サイバー攻撃の高度化 → 従来型対策の見直しと
エンドポイント強化

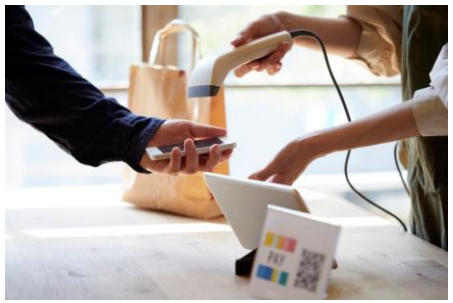
DX（デジタルトランスフォーメーション）とは

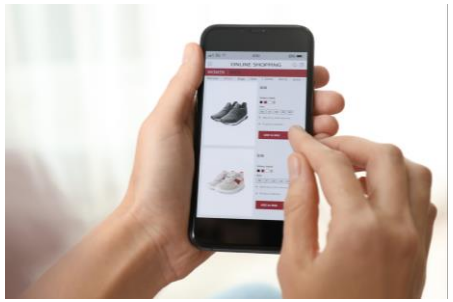
02

「(新しい)ITの浸透によって
人々の生活をあらゆる面でより良い方向に変化させること」

エリック・ストルターマン教授（2004年）

実際に我々の生活はITで便利に

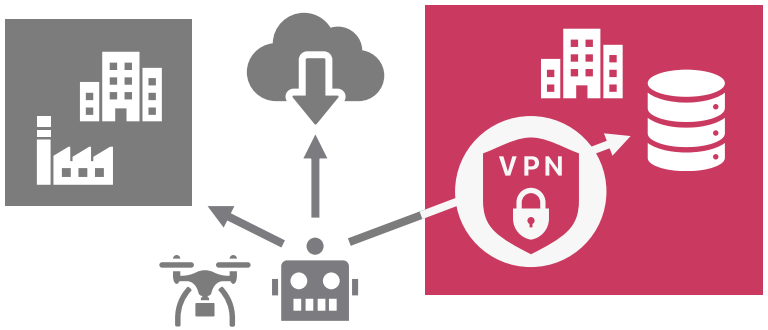




DXを事業として成功させた
企業の価値や企業評価が年々高まっている

しかしながらDXが進むと…

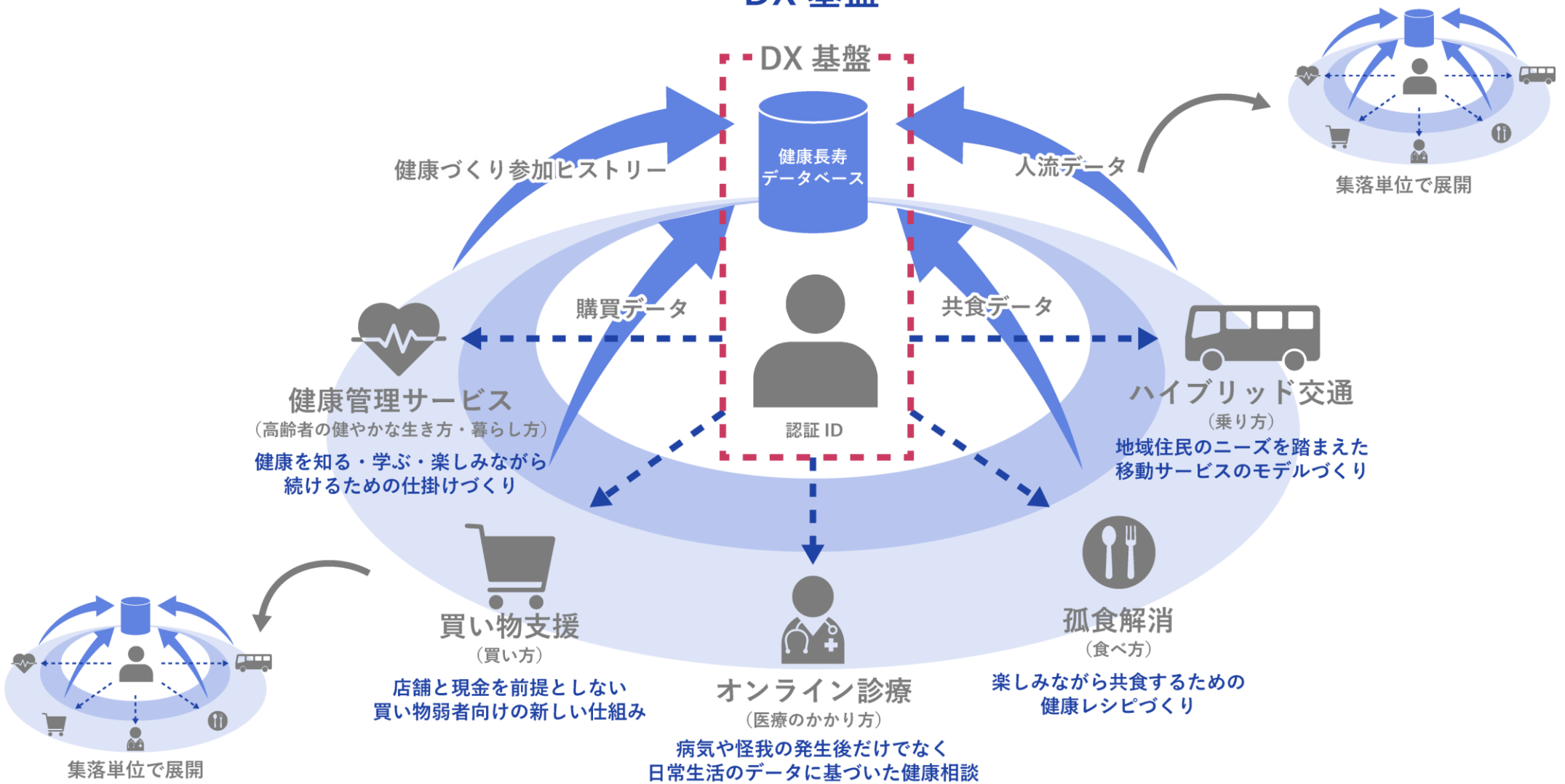
- 様々なデバイスが利用される
- クラウドと直接デバイスが連携
- システム開発は情シスだけで無くなる
- 他企業との垣根が無くなる



DXの推進（伊方町さまの例）

02

集落のグループホーム化に向けた DX 基盤



03

目の前にある脅威

目の前にある脅威

組織へのランサムウェア攻撃が増加 → **サプライチェーン含む組織間の繋がりを利用**

情報セキュリティ10大脅威(2023年)（組織）

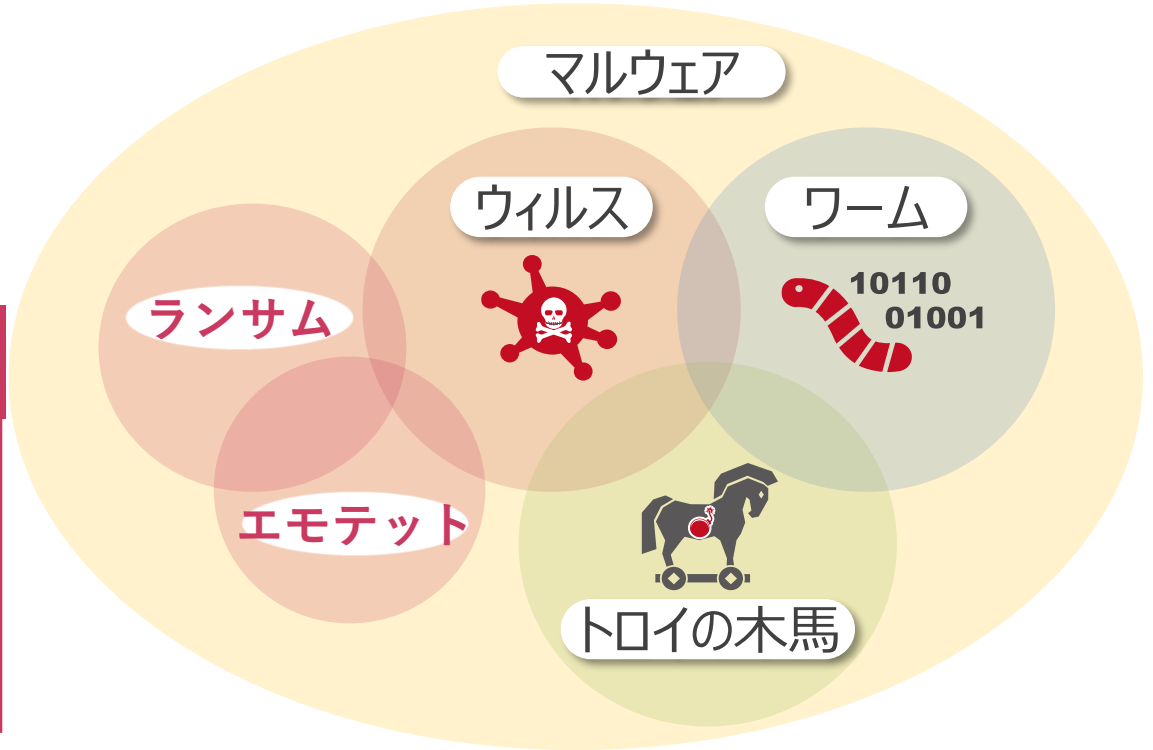
IPA（独立行政法人 情報処理推進機構）『情報セキュリティ10大脅威2023』

順位	昨年順位	脅威
1位	1位	ランサムウェアによる被害
2位	3位	サプライチェーンの弱点を悪用した攻撃
3位	2位	標的型攻撃による機密情報の窃取
4位	5位	内部不正による情報漏えい
5位	4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
6位	7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	8位	ビジネスメール詐欺による金銭被害
8位	6位	脆弱性対策情報の公開に伴う悪用増加
9位	10位	不注意による情報漏えい等の被害
10位	圏外	犯罪のビジネス化（アンダーグラウンドサービス）

- 組織への攻撃が活発化
- 攻撃された組織から別組織への攻撃も増加

マルウェアとは

サイバー攻撃の種類のうちの1つで、
“Malicious software”(悪意あるソフトウェア)
利用者が知らない間にコンピュータにアクセスし、
不正・有害な動作を行う意図で設計

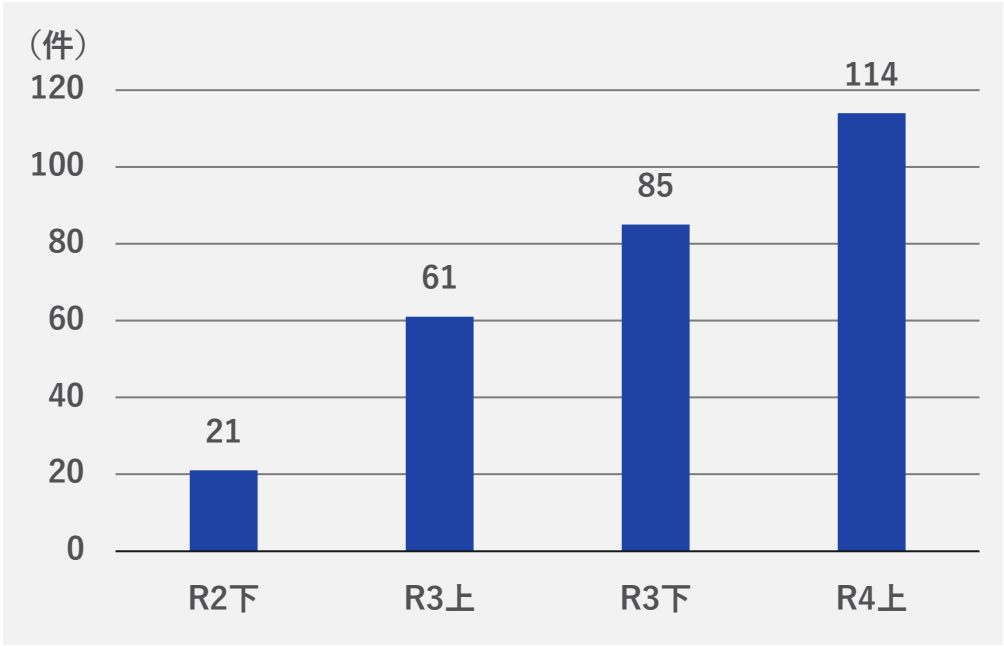


ランサムウェアが猛威

- 暗号化され身代金を要求
- エモテットと呼ばれるマルウェアを利用
- 脆弱性から侵入後利用されることも

警察庁 令和4年
ランサムウェアの情勢

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



出典：警察庁　令和4年　ランサムウェアの情勢
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

サイバー犯罪の高度化/頻発化

- 高度なサイバー攻撃手法が編み出された
- 手法が犯罪者集団同士で共有化
- データの換金性が高まり、金銭目的の攻撃が増加

「サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、
これまでの取組を継続するだけでは、対応困難に」

「ランサムウェア攻撃による被害への対応は企業の信頼に直結」

「盗んだデータを”暴露する”と脅し、金銭を要求する手法も横行」

出典：経済産業省 令和2年最近のサイバー攻撃の状況を踏まえた経営者への注意喚起より

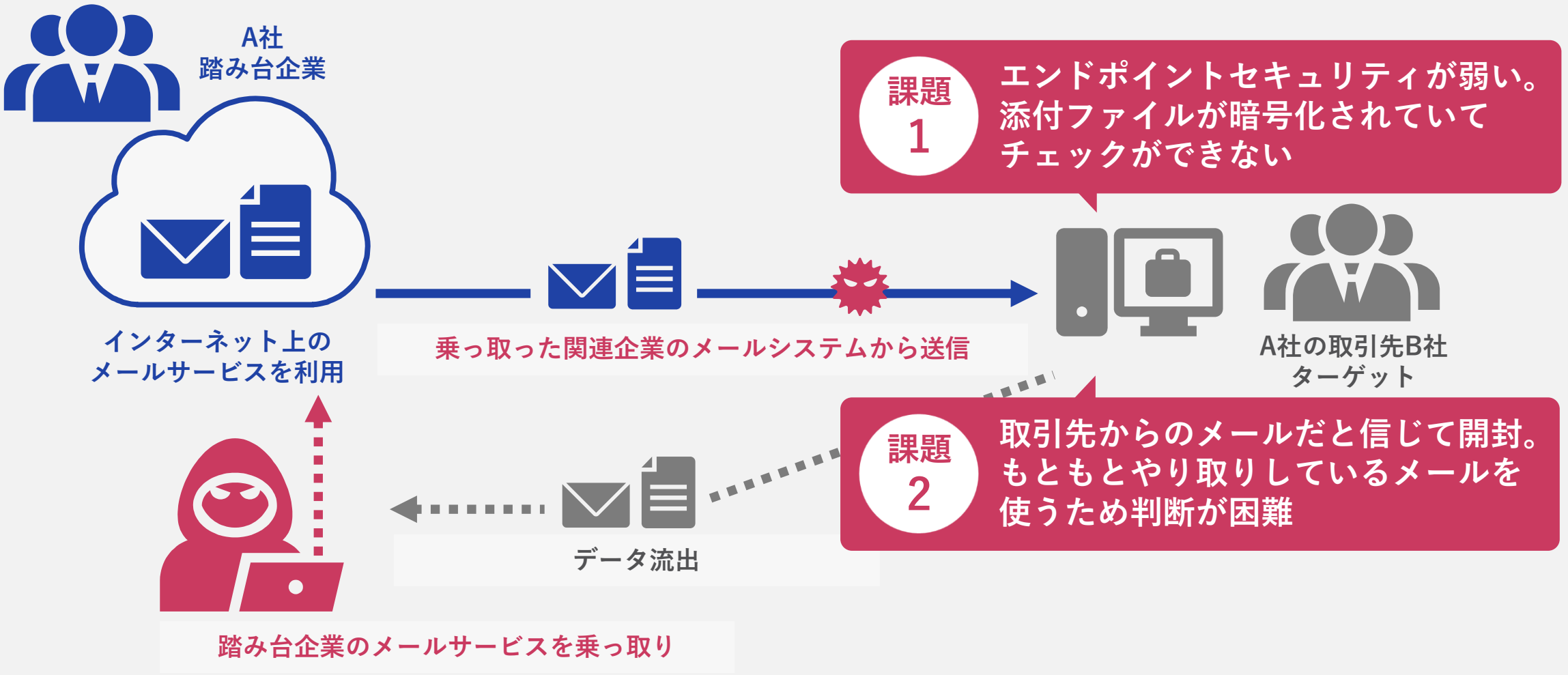
ランサムウェアの被害状況

令和4年度に判明した主なランサムウェア被害

時期	法人名・団体名	概要
3月	デンソー	独法人にサイバー攻撃　機密情報公開で脅迫
3月	トヨタ自動車	国内全工場を停止へ　部品会社にサイバー攻撃
3月	ブリヂストン	米子会社にサイバー攻撃、工場一時稼働停止
3月	三桜工業	北米子会社にサイバー攻撃　社内情報が流出
4月	月桂冠	システム障害　不正アクセスを確認
4月	コニカミノルタ	英子会社が不正アクセス被害
4月	パナソニックホールディングス	カナダ子会社、ランサムウエアに感染
5月	しまむら	商品取り寄せを利用できず　サイバー攻撃の影響
6月	TBカワシマ	「トヨタ紡織子会社にサイバー攻撃」　ハッカー集団表明
7月	安江病院	患者11万人情報流出か　岐阜の病院　不正アクセス
8月	SOMPOホールディングス	SOMPO傘下の台湾保険仲介にサイバー攻撃　漏洩なし
9月	大潟村農業協同組合（JA大潟村）	JAシステムがサイバー攻撃被害で情報流出の可能性
10月	大阪急性期・総合医療センター	徳島の被害病院と同一のVPN利用

インシデント事例と企業の対策例

事例1　サプライチェーンによるランサムウェア攻撃



事例2　VPN機器の脆弱性からの侵入

ターゲット企業C社
従業員

VPN

課題
2
VPN装置の先の
アクセス権限が緩い

VPN装置を踏み台に
内部侵入

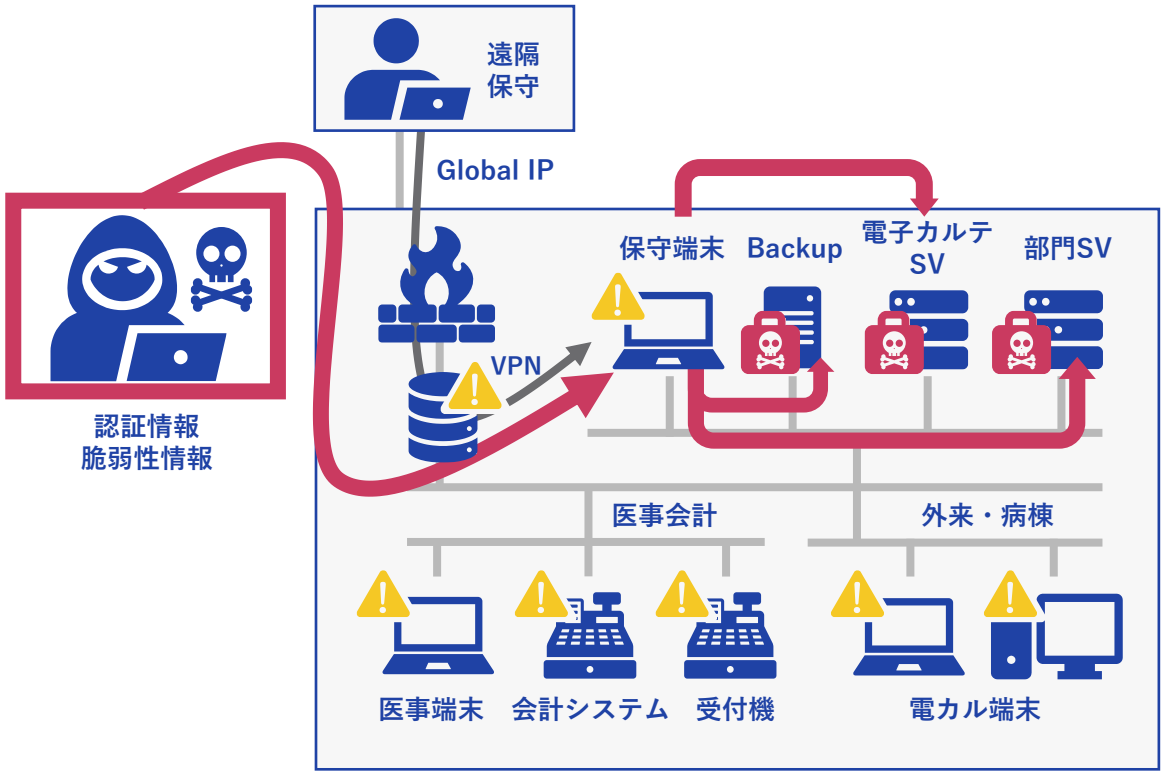
調査は
どこまでも
必要に…

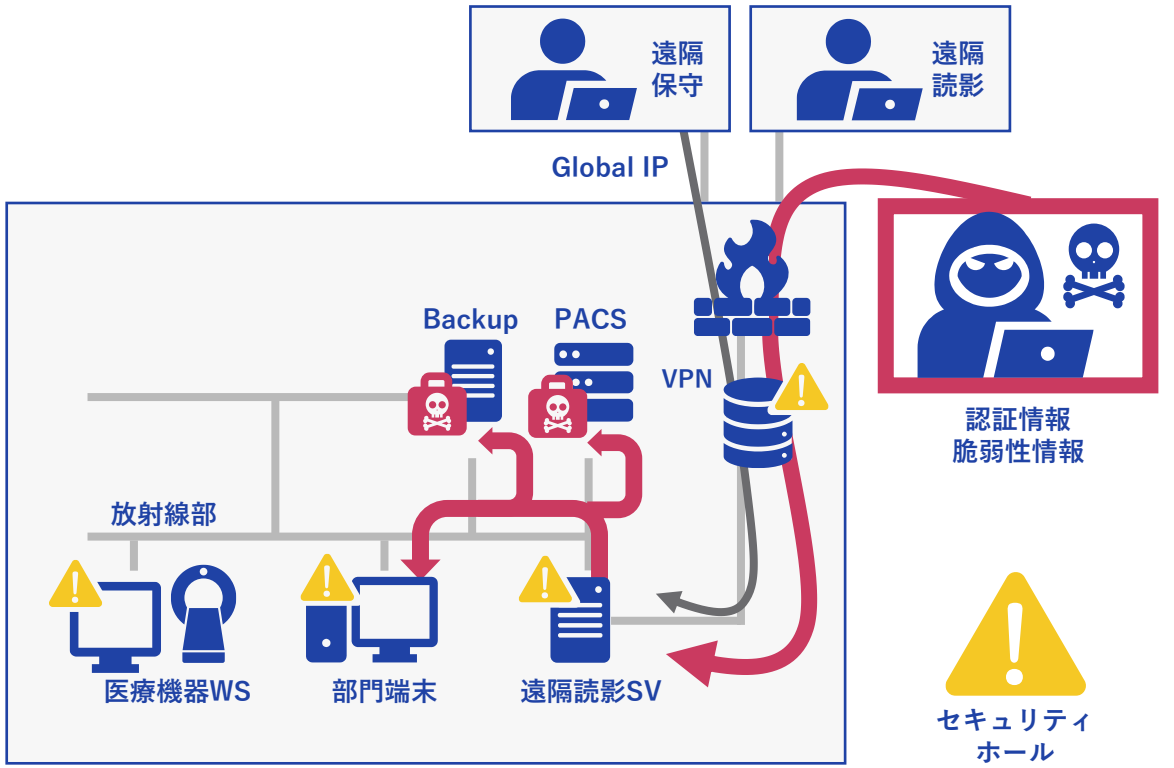
課題
1
✓ パッチ未適用
✓ 監視なし

脆弱性を突き侵入
情報はネットにも公開

ほかのC社PC
にも侵入

補足　国内病院への攻撃手法 狙われるポイント





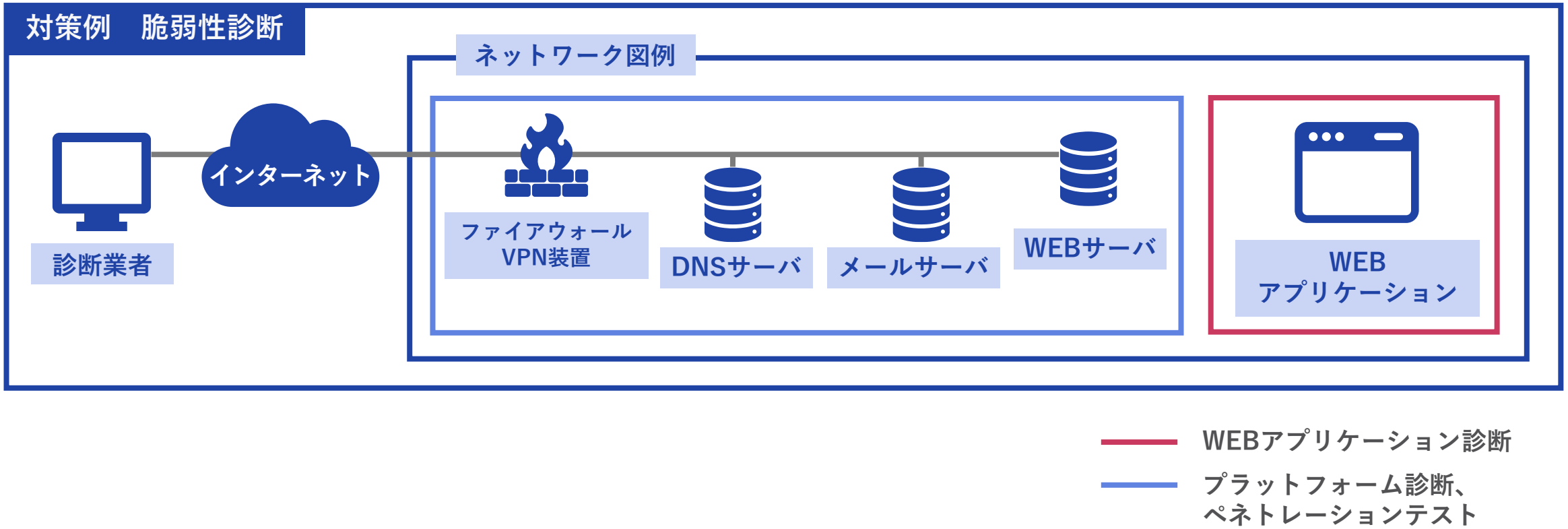
入口における ポイント	● アクセスポイントの脆弱性 ● アクセスポイントの認証情報窃取 ● VPN接続後の不十分な内部アクセス制限

内部環境における ポイント	● クライアントOS/サーバOSの脆弱性 ● セキュリティ対策されていない重要ホスト ● 更新不十分、設定不十分なセキュリティ対策

対策例①　インターネット公開システムに対する対策

03

- 脆弱性診断の実施
- セキュリティパッチの適用
- 運用監視をアウトソース



対策例②　エンドポイントセキュリティの強化

03

NIST『サイバーセキュリティフレームワーク』

EPP
（Endpoint Protection Platform）

「様々なサイバー攻撃から防御する」

- アンチウイルス製品(AV)
  パターンマッチング
- 次世代アンチウイルス(NGAV)
  ・AIエンジンによる検出

＋

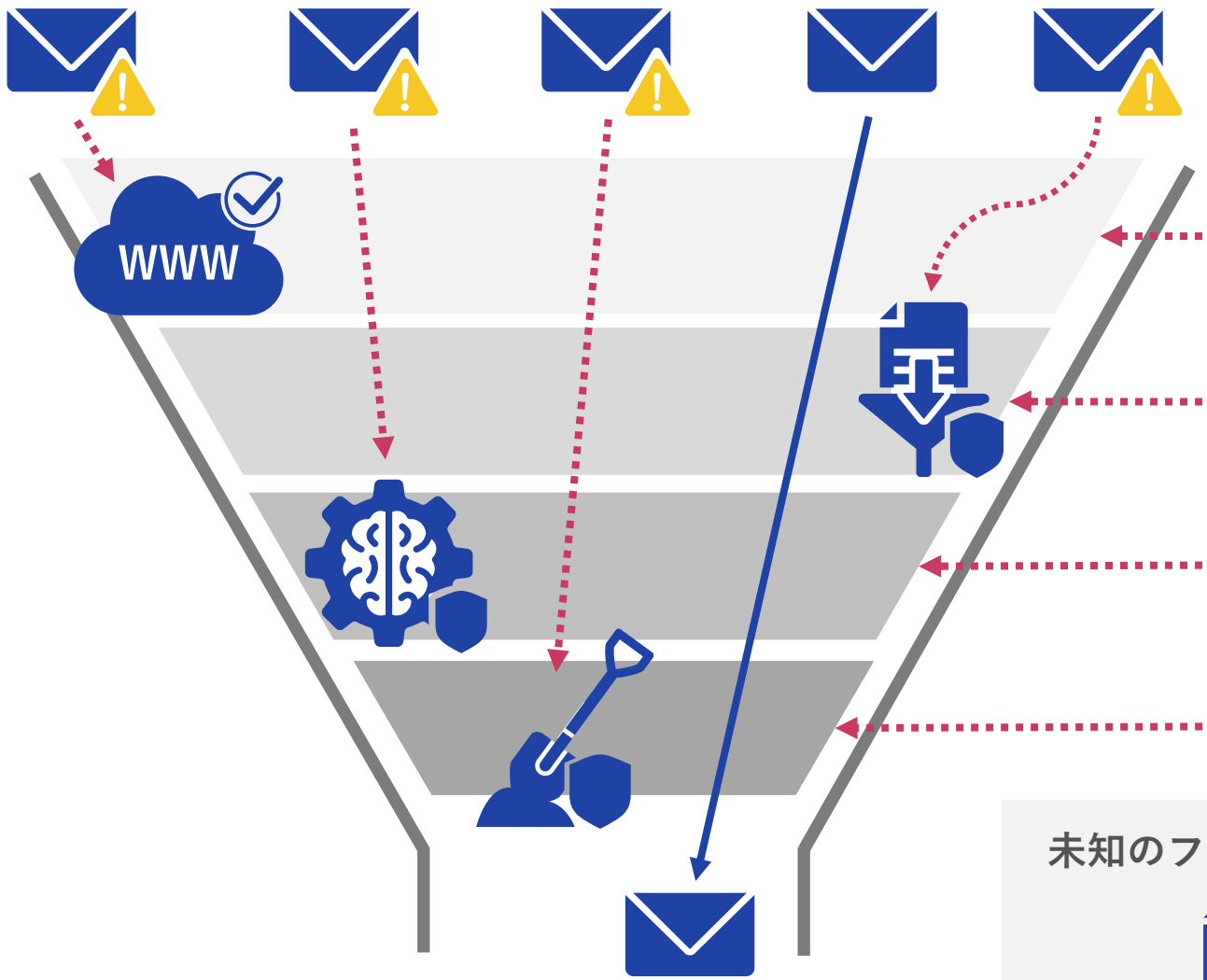
EDR
（Endpoint Detection and Response）

「サイバー攻撃を**いち早く検知し、その後の対応を行う**」

- 振る舞いによる検知
- 原因究明
- 端末の封じ込め
- 復旧

対策例③　マルウェア添付や不正URLメールへの多層防御

03



Webレピュテーション

パターンマッチング

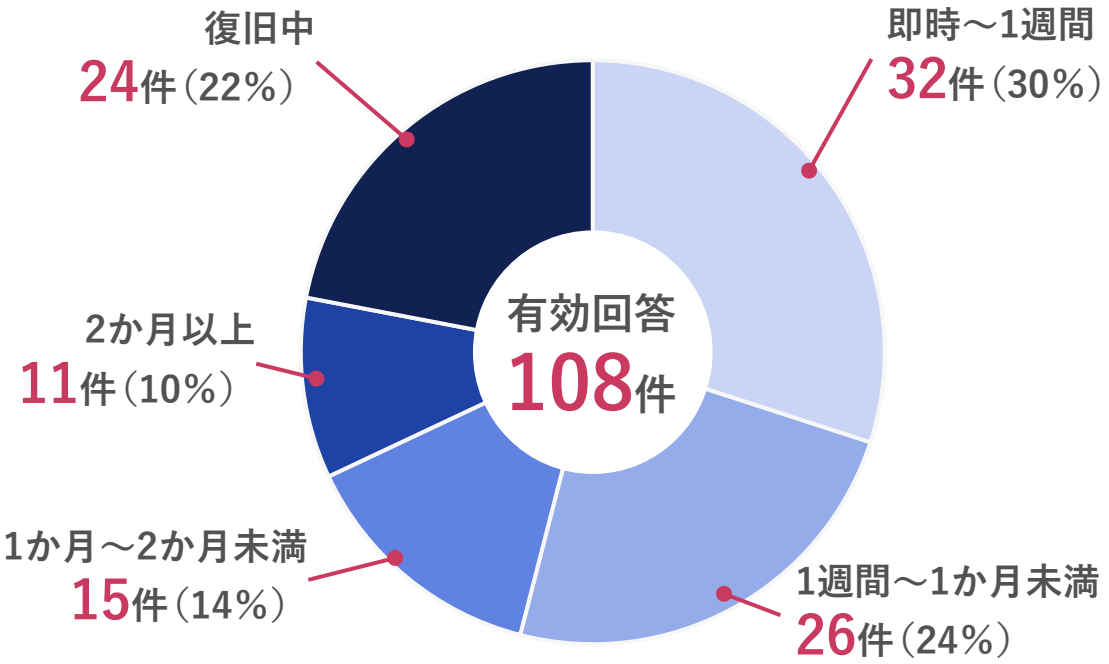
機械学習

サンドボックス

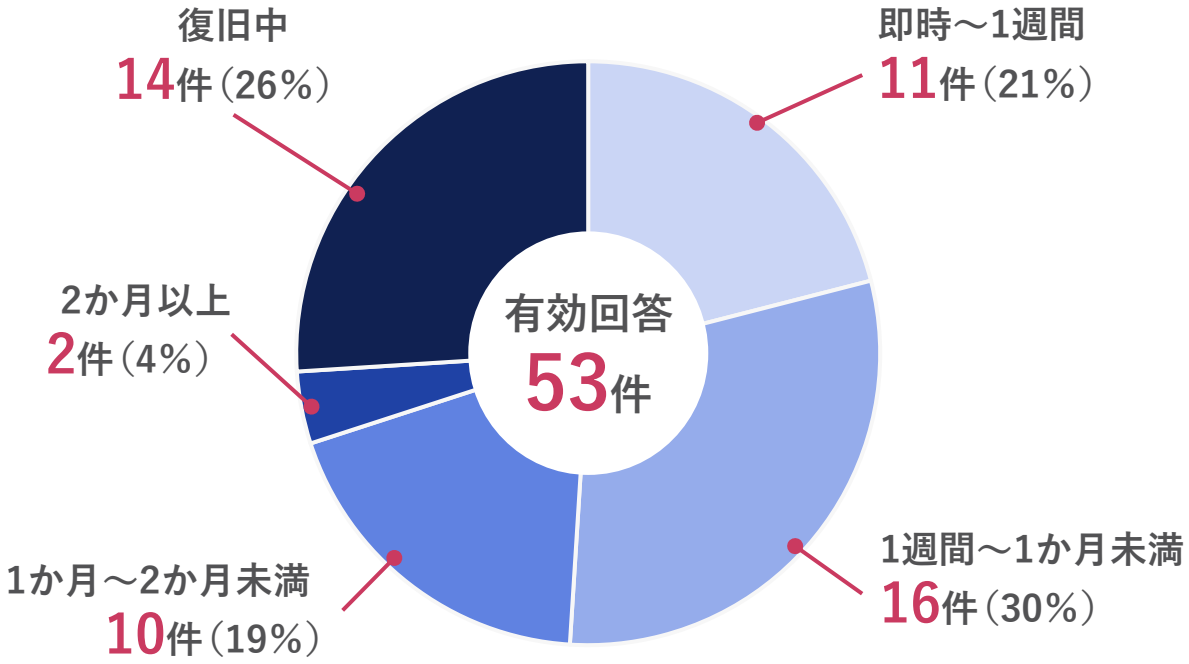
未知のファイル/URL　解析　ブロック・隔離

対策例④　バックアップの対策

復旧までに要した時間



警視庁　令和３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 より



警視庁　令和４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 より

早期のシステム復旧には下記ポイントが重要

- バックアップデータの暗号化を防ぐ仕組み
- リストアの時間を想定してシステムを検討

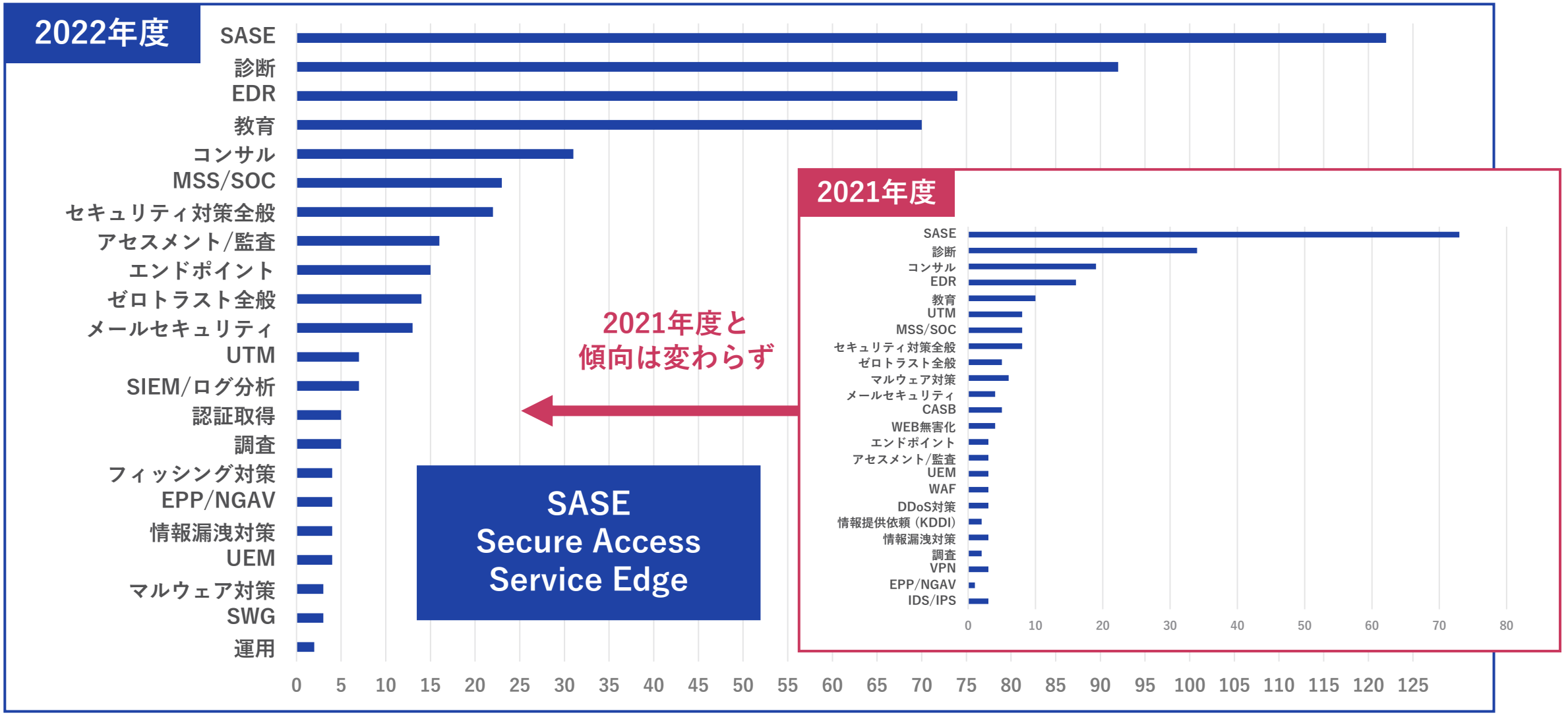
サイバー攻撃の脅威のトレンド

脅威の種類	攻撃タイプ		フェーズ		被害リスク			概要
	標的型	ばらまき	侵入	侵害	停止	漏えい	展開	
ランサムウェア	○	△		○	○	○		従来の暗号化に加え、機密漏えいを煽り脅迫
メールから侵入		○	○			○	○	Emoteによるパスワードzip利用など手法が多様化
サーバ・NW脆弱性	○			○	○	○	○	標的型で用いられる。定常的な手当てが求められる
テレワーク環境	○		○				○	リモートから攻撃しやすいVPN装置やRDPなどの脆弱性を狙い侵入
クラウド利用	△	△		○		○		クラウドの設定不備などによる漏えいなど

企業の関心状況

2022年度サイバーセキュリティご相談状況

ソリューション種類別　案件件数



04

サイバー攻撃から企業や個人を守るためには

サイバー攻撃への基本的な対策を理解する

04

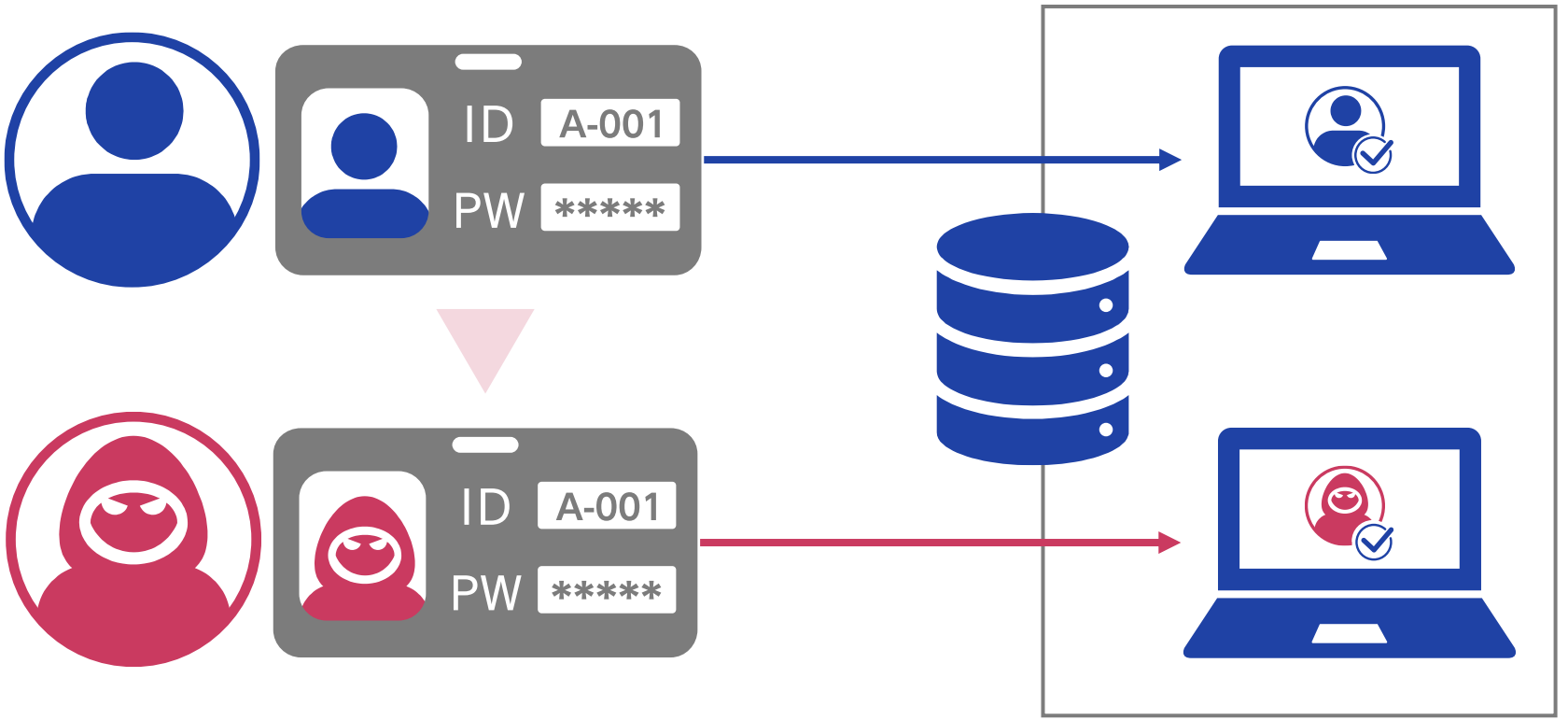
- 公開システムの現状把握とリスク
- ID・パスワードに対するセキュリティ対策
- インターネットの安全な利用方法
- 電子メールの安全な利用方法
- クラウドサービス利用時のリスク
- 外部記憶媒体利用のリスク
- 内部不正

ID・パスワードに対するセキュリティ対策

ID・パスワードの漏洩によるリスク

04

利用者IDとパスワードが不適切な管理や攻撃などで盗まれてしまうと、
なりすましなどの不正行為により**情報漏洩のリスクが高まります**



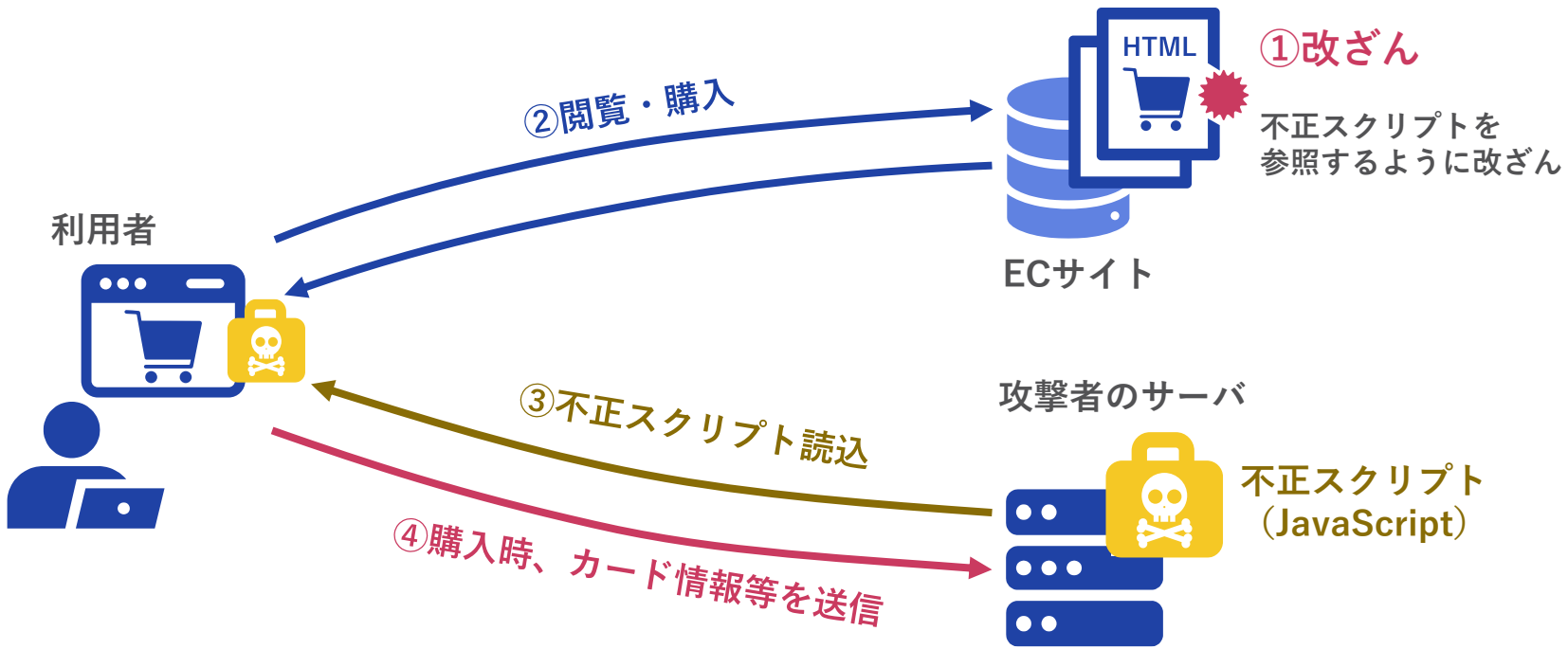
インターネットの安全な利用方法

インターネットアクセスの注意点

不用意にWebサイトにアクセスすることで、
マルウェア感染につながったり、**個人情報漏洩が発生することも**

※特にメールのリンクは気を付ける

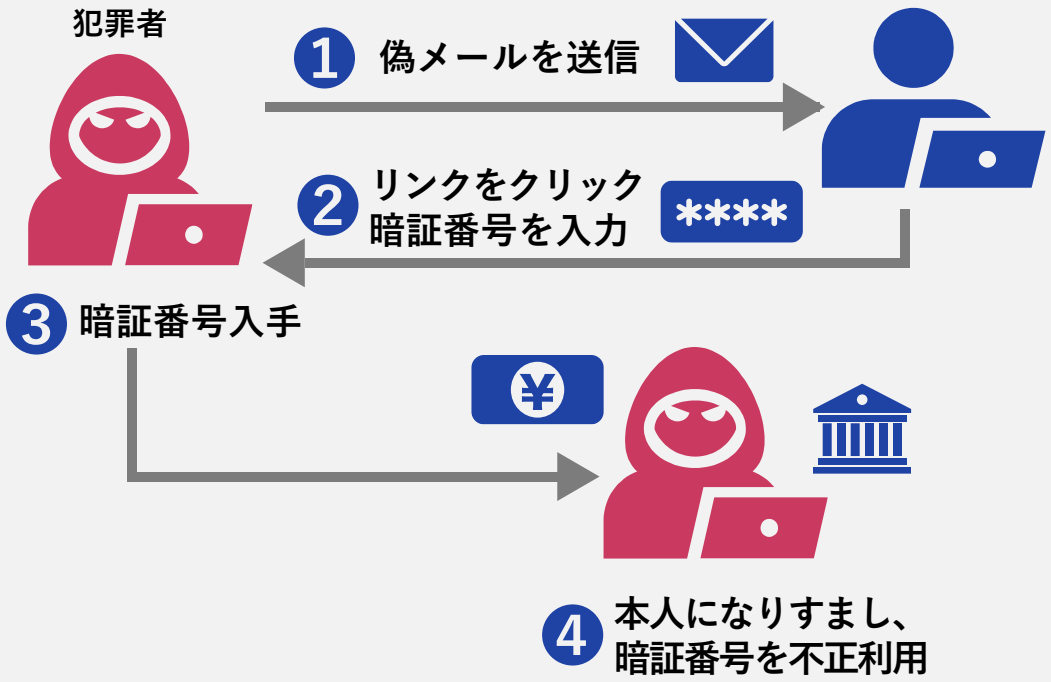
クレジットカード情報等が窃取されるまでの流れ



大手企業を装うフィッシング詐欺

実在の銀行やショッピングサイトなどを装った
メールを送付し、そっくりの偽サイトに誘導して
重要情報を入力させて搾取する、
「フィッシングメール」が急増しています。

フィッシング詐欺のしくみ(一例)



Web経由の攻撃に対する対処例

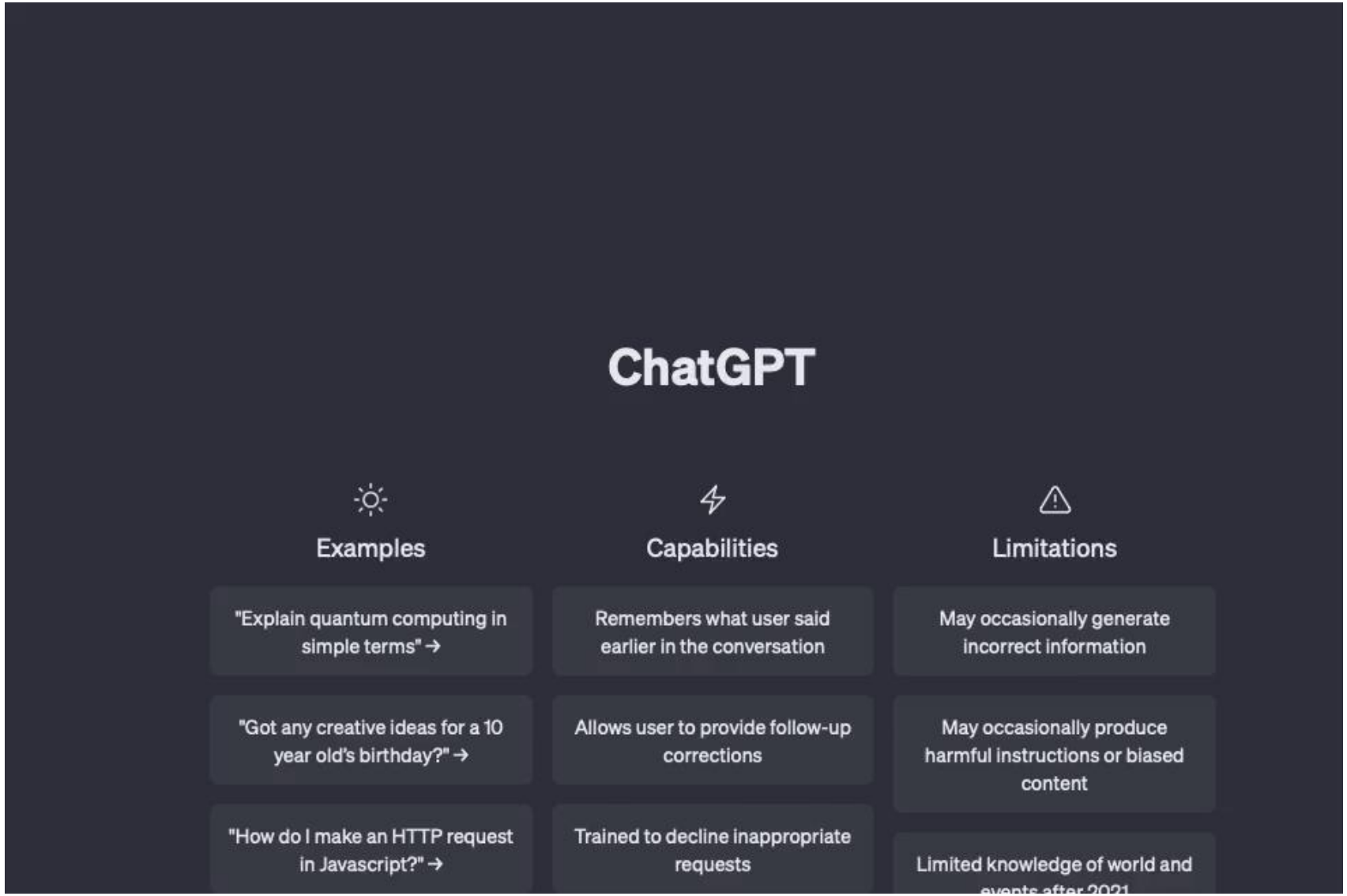
既存のWebアクセス制御の課題

- 社外においてもWebアクセス対策が必要
- 暗号化通信のチェックは高額設備に
- 設備を定期的に保守、リプレイスが必要
- 人数が多くなると設備のリプレイスが必要

SWGが効果的

- 社内外で利用できる
- 暗号化通信のチェックも可能
- マルウェアの悪意ある通信を検知
- 不適切なサイトへの接続を制御可能

補足　ChatGPTのウソ　本当の情報でしょうか？



電子メールの安全な利用方法

電子メールの安全な利用方法

受信したメールの添付ファイルを安易に開かない

知らない送信者名、
心当たりのない英文の件名のメールは注意する

送信者が知人であっても
添付ファイル付きのメールは疑ってかかる

他社情報が残存したデータ送付による情報漏洩

04

メールへ添付したファイルに、
他社情報が記載されていた（残存していた）ことによる情報漏洩事故

POINT 1

別のお客様の**見積書を流用**
ファイルの中に機密情報が残存
したまま見積書を作成

情報漏洩

POINT 2

添付ファイルの内容を十分に
確認せず見積書をメールで送付
Excelファイルには**非表示行があり、**
その中には他社情報が含まれていた

情報漏洩

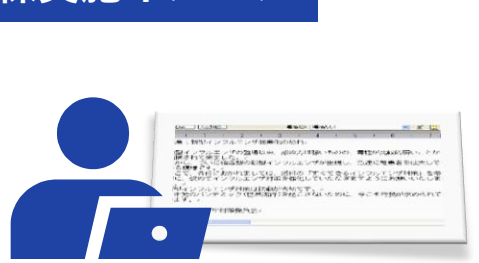
標的型攻撃メール訓練などの活用

04

既存のセキュリティ対策では発見が困難な標的型攻撃に対して、疑似的な標的型攻撃メール（訓練メール）を
社員へ送付することで、標的型攻撃メールへの対応力を高める体験型学習サービスです

■サービス例　訓練メールを配信し、添付ファイルの開封またはURLリンクのクリック（開封率）を確認します

訓練実施イメージ

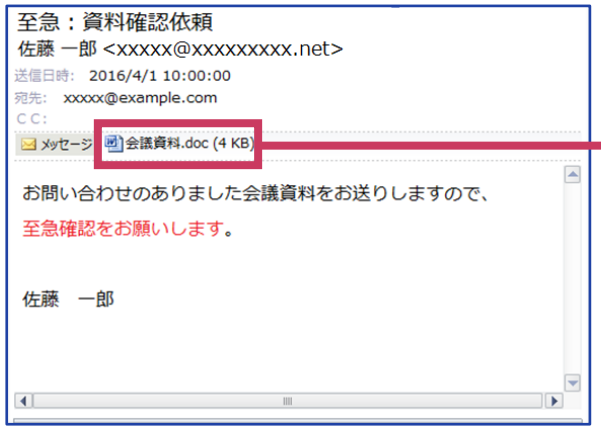


訓練メールを配信

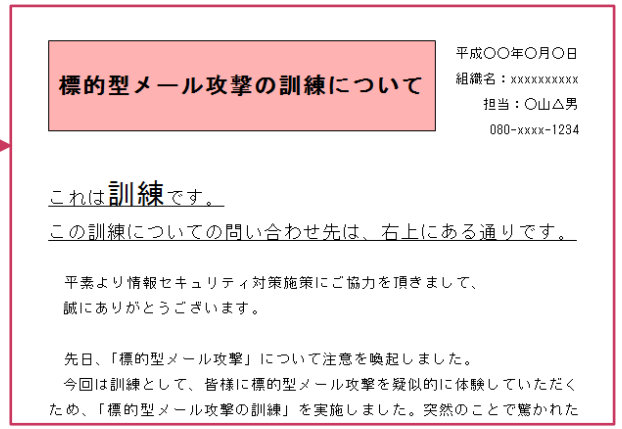
サービス提供企業の
メールサーバから、
訓練対象者へ訓練
メールを配信します

訓練メールを見抜けなかった
社員には訓練であることを説明

標的型攻撃に警戒感をもつ社員は
適切に対処(メール削除、報告など)



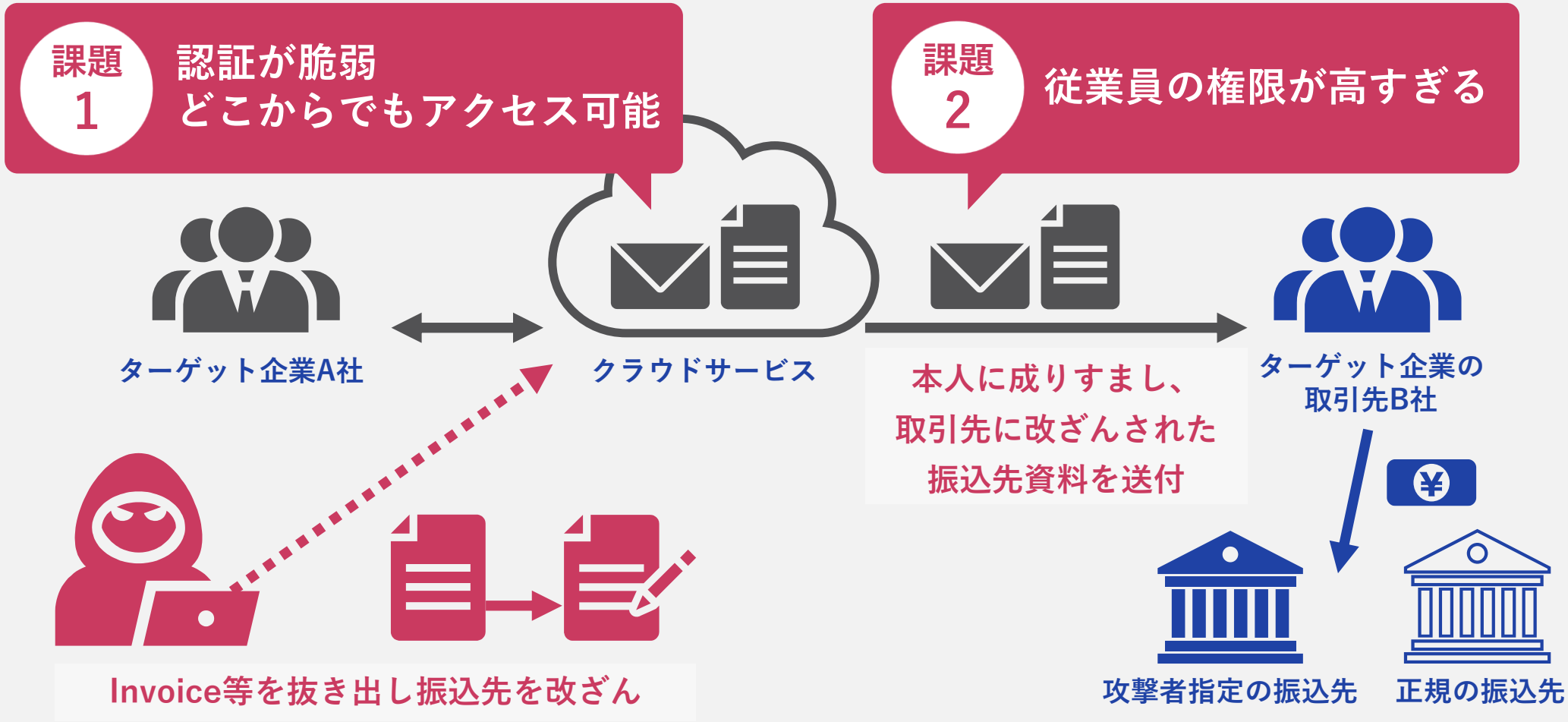
訓練メールの例



添付ファイルの開封、
またはURLリンクの
アクセス時に教育用
のコンテンツが表示
されます

教育用コンテンツ例

実際にあったビジネスメール詐欺 攻撃内容と被害

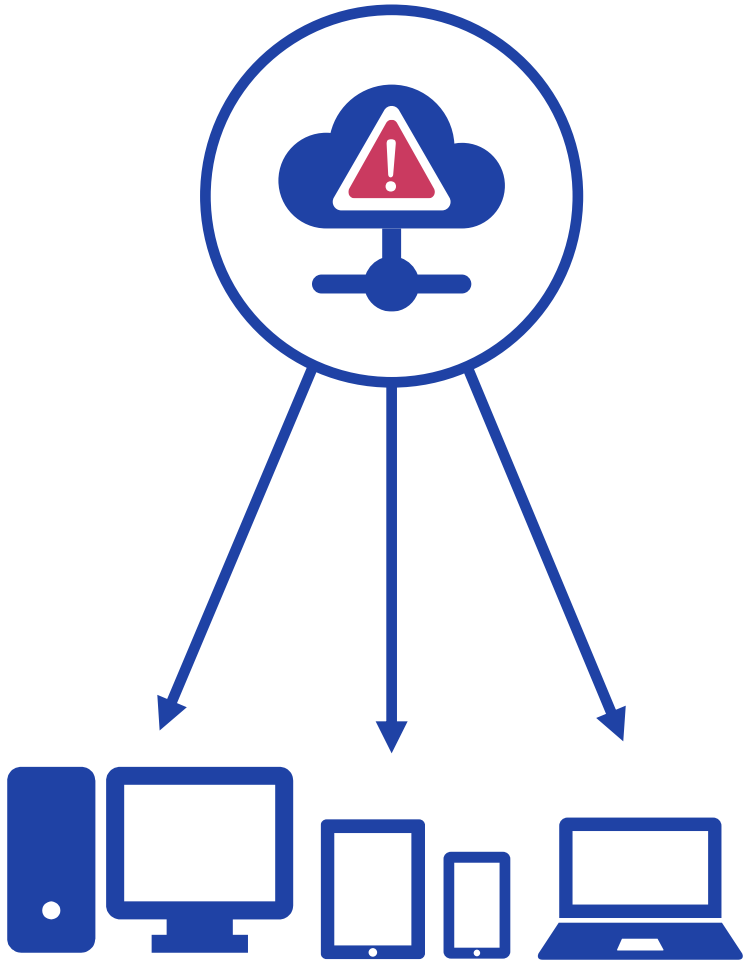


クラウドサービス利用時のリスク

クラウドサービスを利用することによるリスク

データの移動が
制限・監視されていない

設定の不備により
情報漏洩が起こる危険性あり！



情報公開設定のミスが原因

13団体がセールスフォースの「設定不備」で不正アクセスを確認、委託先が発表

山端 宏実、鈴木 慶太　日経クロステック／日経コンピュータ

2021.02.13

両備システムズ（岡山市）は2021年2月12日、セールスフォース・ドットコムのクラウドサービスの「設定不備」を巡り、13団体で外部の第三者による意図しない情報へのアクセスを確認したと発表した。既に両備システムズが手掛けるシステムを利用する神戸市や千葉県船橋市などで不正アクセスの被害の可能性が明らかになっている。

引用：https://xtech.nikkei.com/atcl/nxt/news/18/09648/

「Microsoft Power Apps」の設定ミスで3800万件の個人情報が流出

Larry Dignan （ZDNet.com） 翻訳校正： 矢倉美登里 吉武稔夫 （ガリレオ） 2021年08月24日 13時22分

情報セキュリティ企業UpGuardによると、アプリ開発ツール「Microsoft Power Apps」の設定ミスにより、新型コロナワクチンの接種予約に使われた個人情報、社会保障番号、氏名、メールアドレスなどの機密データが流出したという。

UpGuardの研究チームは米国時間8月23日、外部からアクセスできるよう設定されたMicrosoft Power Appsポータルを通じて複数のデータ流出があり、計3800万件のデータレコードが漏えいしたことを明らかにした。

引用：https://japan.cnet.com/article/35175625/

Trello設定ミスで個人情報が全世界に公開。免許証、パスポート、健康診断結果… 検索エンジンからも閲覧可能に

4/6(火) 12:15 配信　187

BuzzFeed JAPAN

Trello

タスク管理ツール「Trello」上で、パスポートや免許証、住所などの個人情報が誰でも閲覧できる状態になっているケースが多数あることがわかった。Trelloの設定が「公開」になっていると、誰にでも検索・アクセスすることができてしまう。利用者は速やかに公開設定を確認してほしい。【BuzzFeed Japan / 千葉雄登】

免許証、パスポート 、住所も…

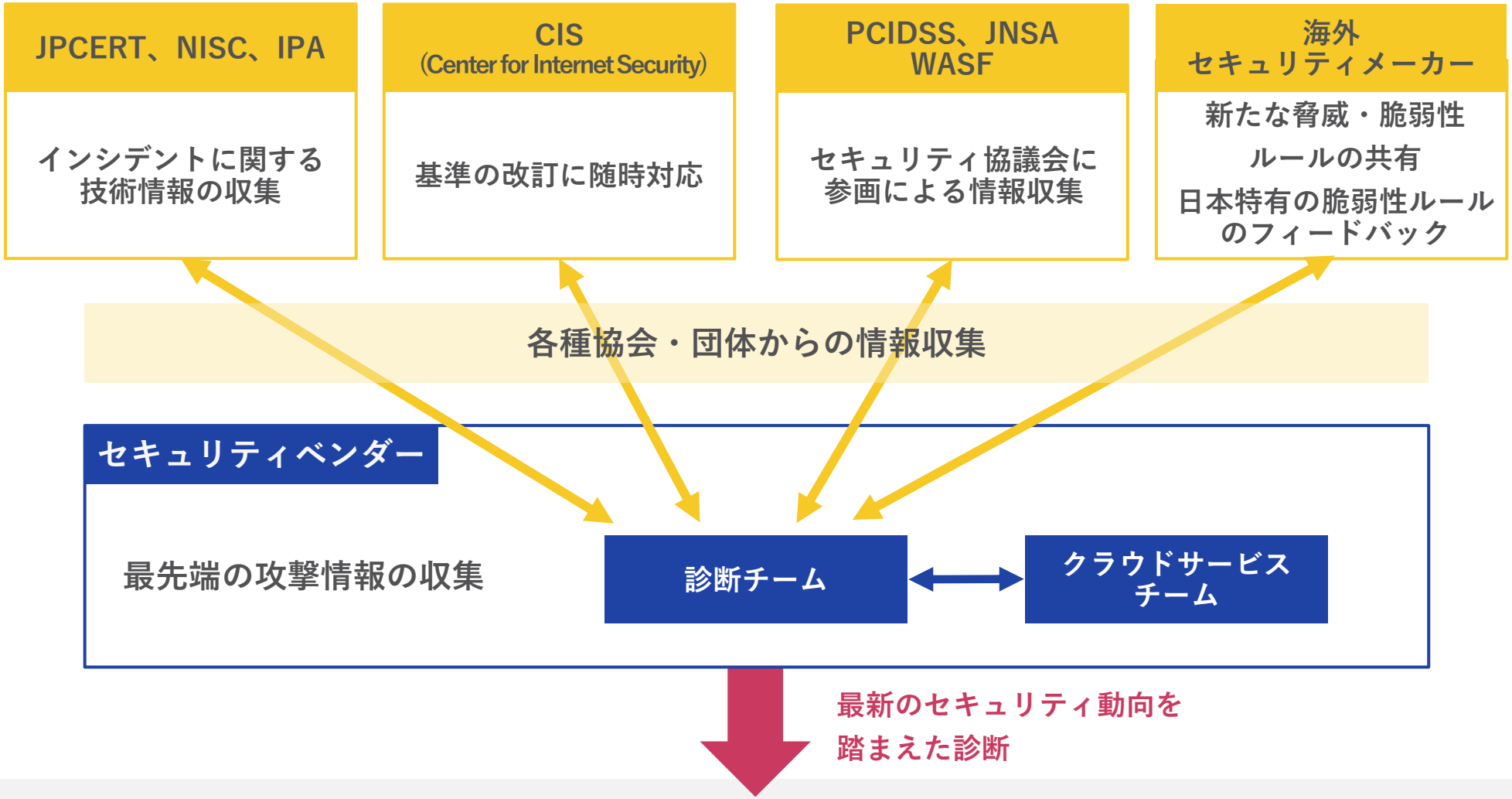
Trello上での個人情報流出に関する情報は、ネット掲示板で話題となり、Twitterで拡散された。

なぜ、このような問題が起きたのか？ 原因は利用者の情報の公開設定にある。

引用：https://news.yahoo.co.jp/articles/f378e7b4ad44c30ff27af55137427ae7635844ff

クラウドサービスの設定診断について

04



定期的に診断項目を見直し**常に最新のセキュリティ基準**で診断を実施

外部記憶媒体利用リスク

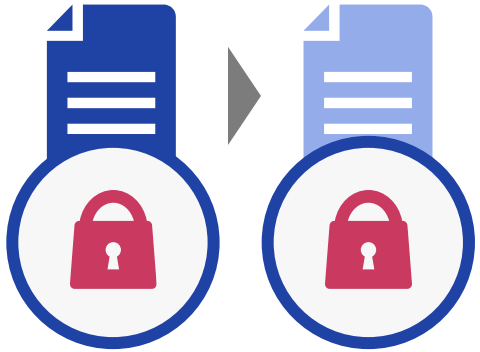
USBメモリ等の使用による情報漏洩の予防に効果的な対策

04

データ利用

業務外の
データ利用を禁止

暗号化



移動するデータは
暗号化する

セキュリティ機能

セキュリティ機能
付きのUSBメモリ
等を使用する

USBメモリ禁止

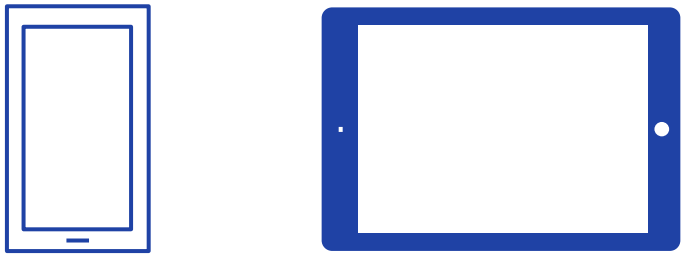
個人所有の
USBメモリ等の
使用を禁止する

資産管理ソリューションを導入しPC及び外部媒体も管理を実施

04

MDM（モバイルデバイス管理）

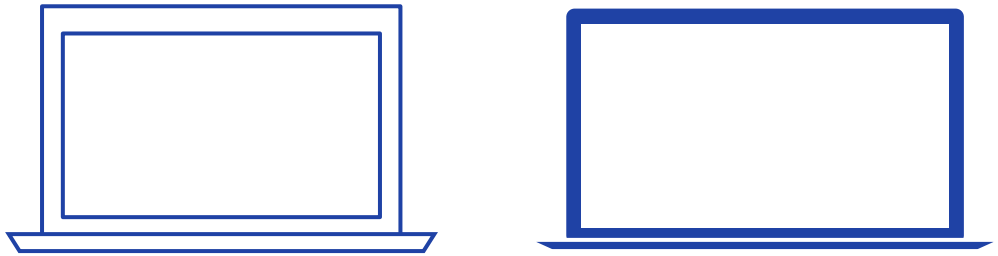
Android　　iOS



- デバイス紛失時のリモートロック・ワイプ
- セキュリティポリシーやアプリの配布、管理
- 位置情報取得や利用機能の制御

IT資産管理ツール

Windows　　macOS

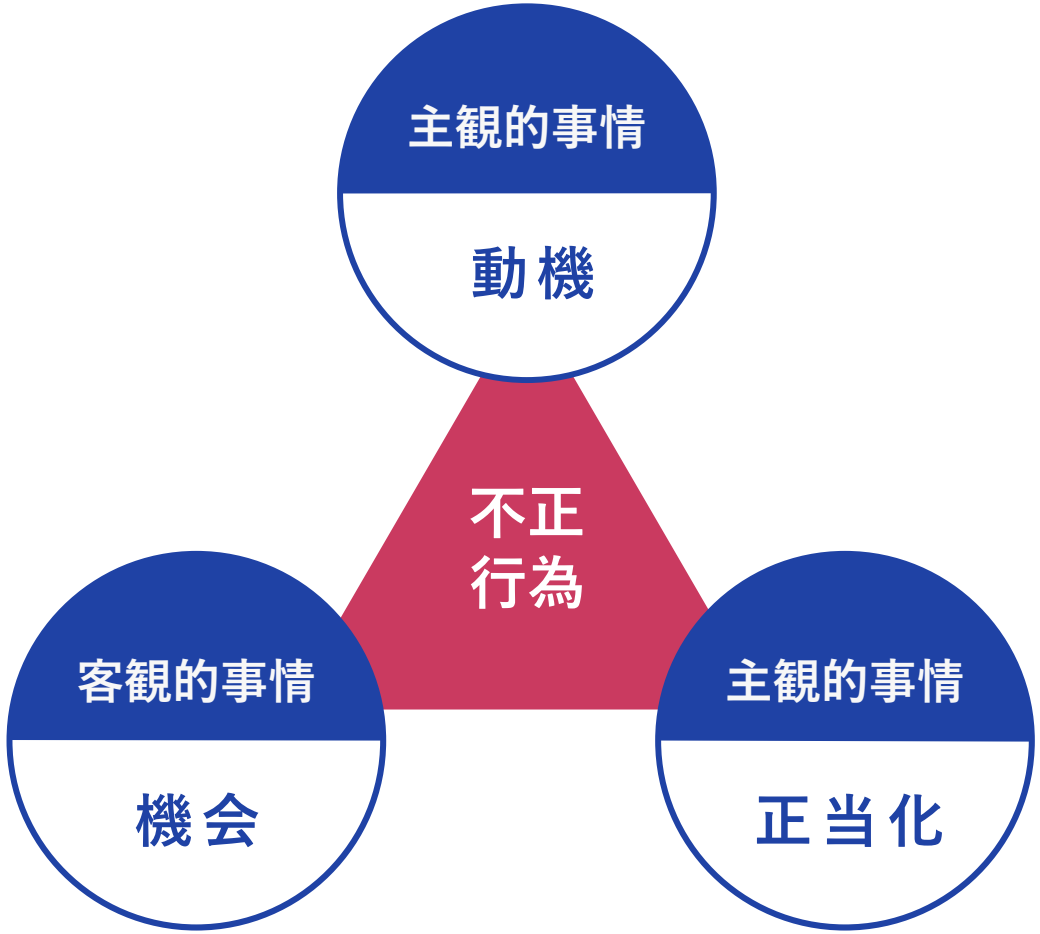


- デバイスやソフトウェアの情報収集、管理
- セキュリティパッチやソフトウェアの配布
- 操作ログ取得や利用機能の制御

内部不正

内部不正行為について

不正のトライアングル



動機 不正を働く動機	自分の望み・悩みを解決するには、 不正行為を実行するしかない という考えに至った心情
機会 不正を働く機会	不正行為を働こうと思えば、 いつでもできるような職場環境のこと
正当化 不正を働く口実	自分に都合の良い理由をこじつけて、 不正行為を働く際に感じる 「良心の呵責」を乗り越えてしまうこと

内部不正行為への対策

「正当化」に関しては、個人の価値観に依拠することが多いため、
完全になくすことは難しいが、
「動機」と「機会」に関しては、不正のできない環境づくりによって減らし、
不正のトライアングルの３要素が揃わないようにすることが可能

「機会」の低減

適切な権限管理を実施する

- 特定の人物に権限が集中しないよう
  権限を分散する
- 利用者同士が相互に監視し、
  不正や見落としがない環境を作る
- 利用者のログは、
  利用者以外の者が定期的に確認し監視する

「動機」の低減

ログの記録を従業員へ周知する

- 抑止の観点から、業務担当者に
  ログが記録されていることを通知する

出典： IPA　組織における内部不正対策　-内部不正防止ガイドライン第3版-

補足　攻撃の予兆

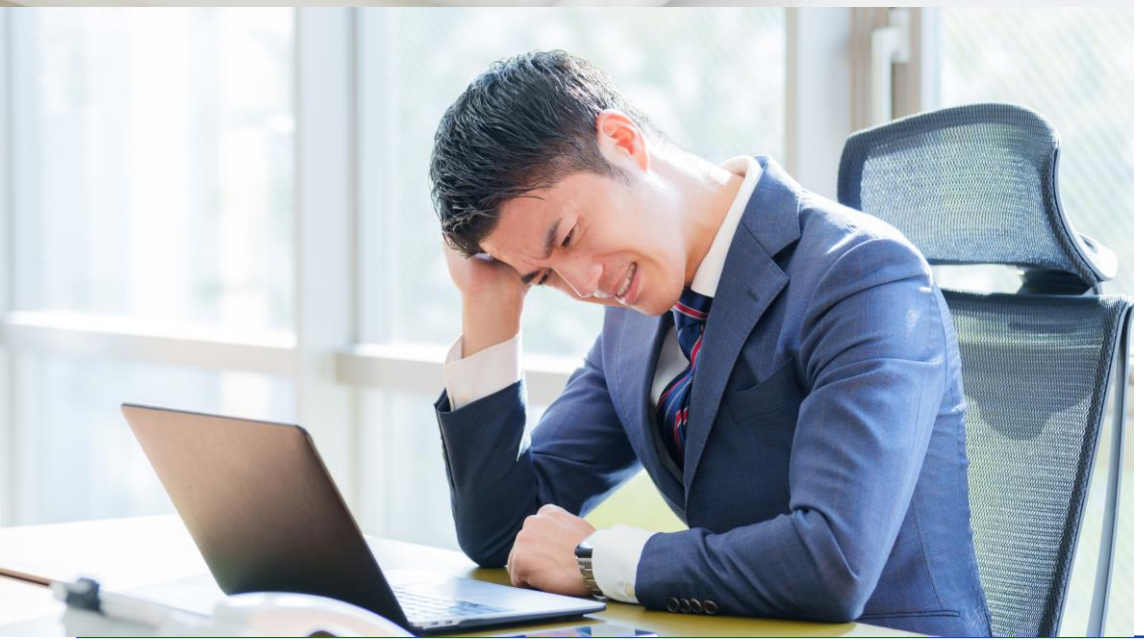
サイバー攻撃に対する予兆・前兆　例

- PCの動作が不安定
- ネットワーク使用率が突然増えた
- メール数が突然増えた
- ファイルが勝手に消えた

05

サイバーセキュリティ対策の必要性について

サイバーセキュリティ対策イメージ



- 保険のようなもの
- 上層部の理解がなく導入しにくい
- 費用対効果がない
- お金がないので対策できない
- 対策しても意味はない

?

サイバーセキュリティ対策は「人」「物」「金」を守り、利便性を向上

05

従業員へ責任が・プライバシー情報の漏洩

システム利用不能・お客様への影響

被害調査費用・システム停止に伴う違約金

お金がなくとも最低限今すぐやっておくべき対策

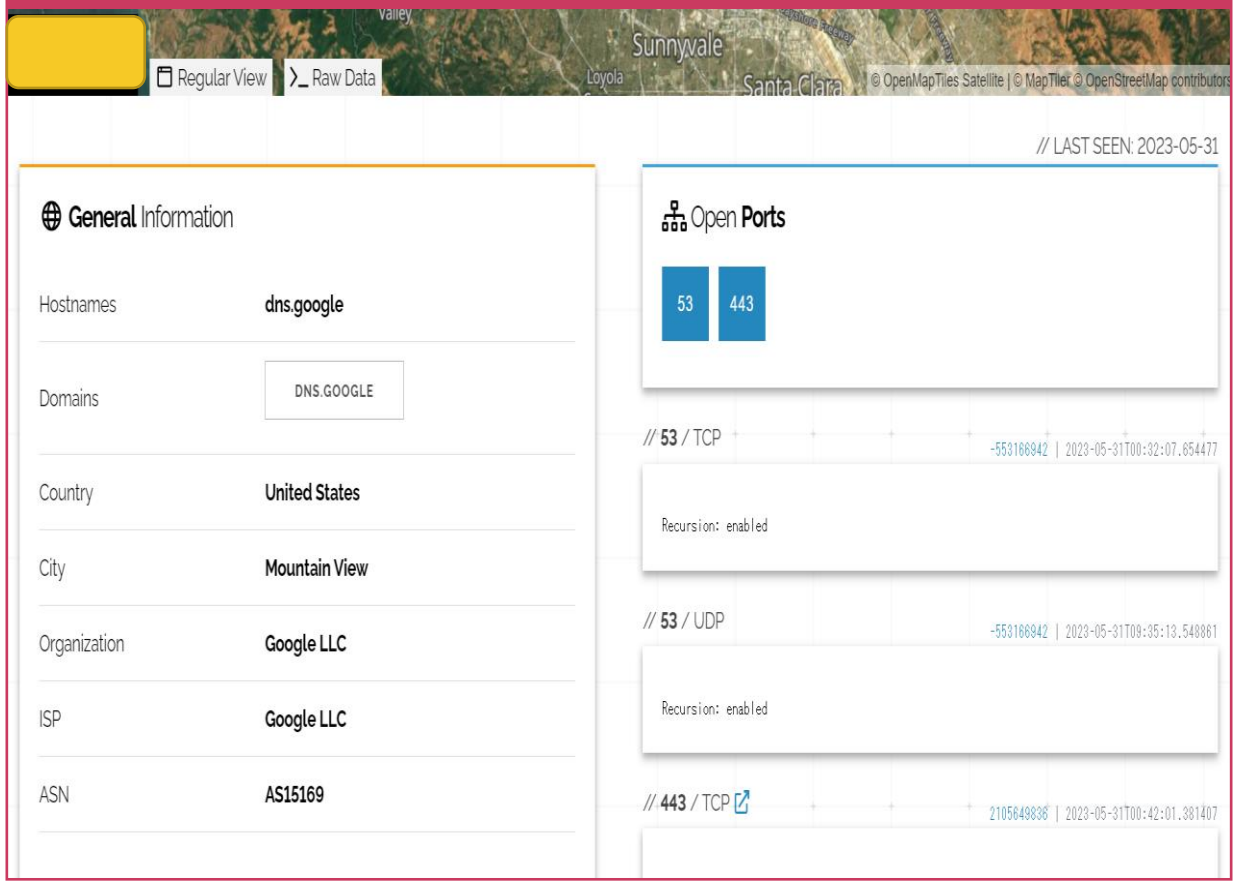
05

- マルウェア（ウイルス）対策ソフトの導入
- セキュリティパッチの適用
- インターネット公開システムのセキュリティ対策
- バックアップ
- 社員教育
- 経営者のサイバーセキュリティへの意識向上

OSINTの活用（Open Source Intelligence）

OSINT（オシント）とは合法的に入手できる情報を収集分析し突合せる手法

SHODAN画面



OSINTの例　SHODAN

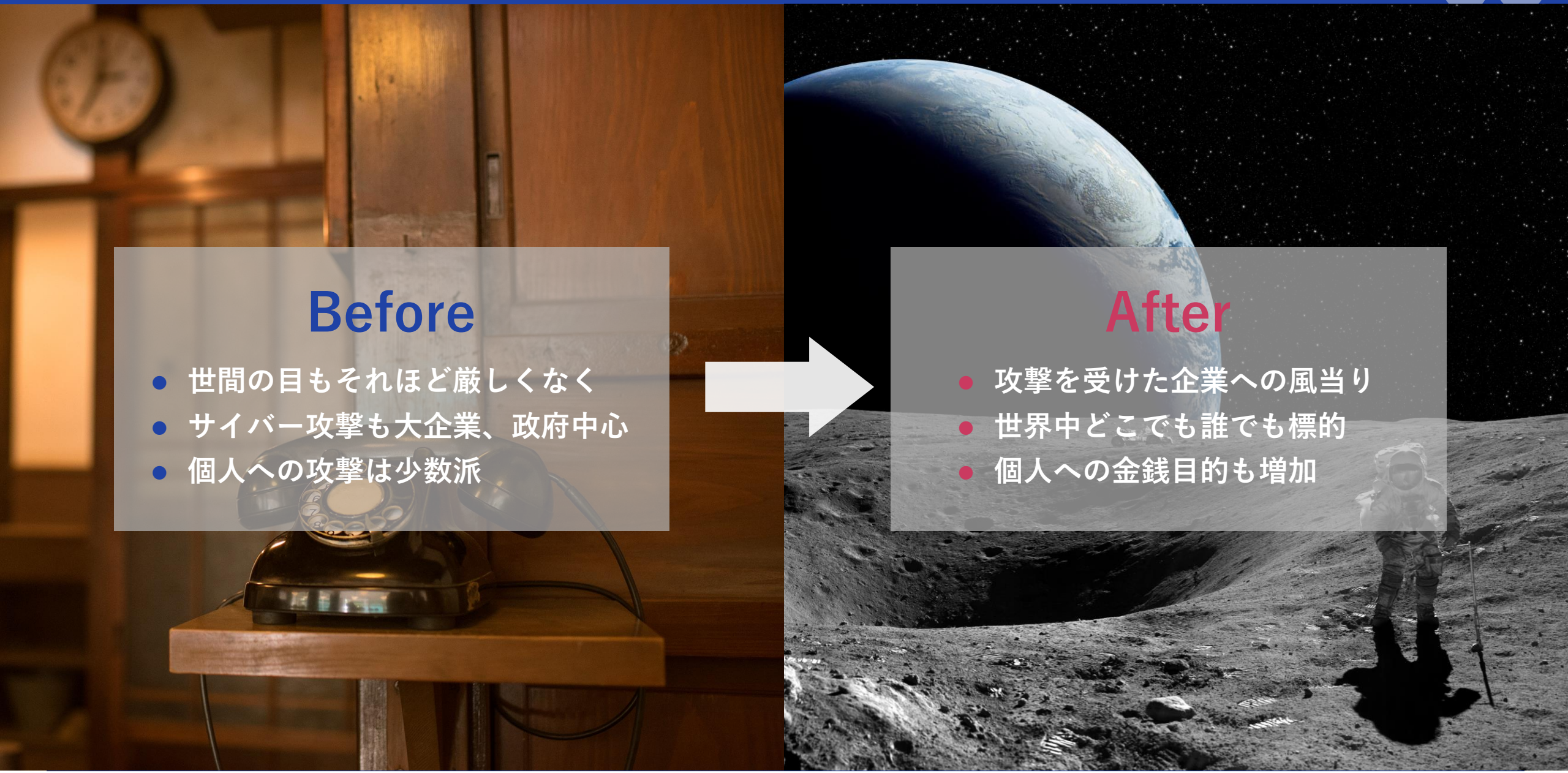
- www.shodan.io
- IPアドレスで検索
- Webサーバや、メールサーバ、NW機器など調査可能
- 機器のバージョン、匿名接続の可否、初期IDやPW情報などが確認可能
- 無償

06

まとめ

さいごに

06



Before

- 世間の目もそれほど厳しくなく
- サイバー攻撃も大企業、政府中心
- 個人への攻撃は少数派

After

- 攻撃を受けた企業への風当り
- 世界中どこでも誰でも標的
- 個人への金銭目的も増加