Panasonic

ランサムウェアから守る！

製造業向け
実践的セキュリティ対策セミナー

ー身代金の支払いを回避するための防御術と復旧術ー

主催：パナソニック インフォメーションシステムズ　　共催：ITガード

ランサムウェア被害から製造業を守るための セキュリティ対策のポイント

パナソニック インフォメーションシステムズ株式会社

資料中の商品名、ロゴ等は各社の登録商標です

まつお　　かずよし

松尾 和世司

パナソニック インフォメーションシステムズ株式会社
営業統括部　セールスイノベーション部　マーケティングチーム

製造業における生産管理システムの構築、インフラ運用、
データセンターセキュリティ担当などを経て現職。

マーケティング施策の立案と実行および、
お客様にITのトレンドや最新技術情報をお届けする
エヴァンジェリストとして活動。

資格
経済産業省認定 情報処理安全確保支援士
（登録番号：007992）

パナソニック インフォメーションシステムズ Panasonic

Chapter - 1

製造業における
ランサムウェア被害のトレンド

データでみる　製造業におけるランサムウェア被害のトレンド

製造業における ランサムウェア攻撃の被害率

2023年	2024年
56%	65%

製造業における 悪意のあるメールによる被害

※2024年　被害原因1位

2023年	2024年
21%	29%

ランサムウェア攻撃の被害を 受けた製造業のうち

バックアップまで侵害を試みられた　93%

実際にバックアップまで侵害　53%

バックアップまで侵害された組織は・・・

- 身代金の要求額　2倍　中央値 100万ドル→200万ドル
- 身代金を支払う割合　大幅UP　49%→70%
- 全体的な修復コスト　2倍　中央値 37.5万ドル→75万ドル

出典：ソフォス社「製造/生産業のランサムウェアの現状 2024」

Panasonic

データでみる　製造業におけるランサムウェア被害のトレンド

製造業における データの暗号化率

2023年	2024年
68%	**74%**

データの復旧方法

	2023年	2024年
・バックアップから復元	73%	**58%**
・身代金を支払って復元	34%	**62%**

製造業における復旧コスト

2023年	2024年
108万ドル	**167万ドル**

製造業における復旧時間

	2023年	2024年
・1週間以内	46%	**35%**
・最大1カ月	28%	**33%**
・1～3カ月	13%	**20%**

出典：ソフォス社「製造/生産業のランサムウェアの現状 2024」

なぜ製造業が狙われるのか？

攻撃者の視点

レガシーシステムの利用

最新のセキュリティアップデート適用無し、サポート切れ。攻撃対象に

複雑なサプライチェーン

サプライヤーやパートナーとの連携でシステムやネットワークが複雑化

交渉のしやすさ

高いダウンタイムコスト

生産停止が直接的な損害に。身代金を要請しやすい

情報の価値

設計情報や特許情報など競争優位性に直結する情報が多い

出典：ラック社「製造業を狙うサイバー攻撃から見るセキュリティ対策」

二重脅迫型ランサムウェアの脅威

①ファイルを暗号化

②重要情報を公開

復旧コストがかかる
生産再開の遅れによる損害

身代金要求

競争優位性の喪失
市場信用の失墜

製造業は二重脅迫型ランサムウェアの格好の標的として今後も気が抜けない！

パナソニック インフォメーションシステムズ Panasonic

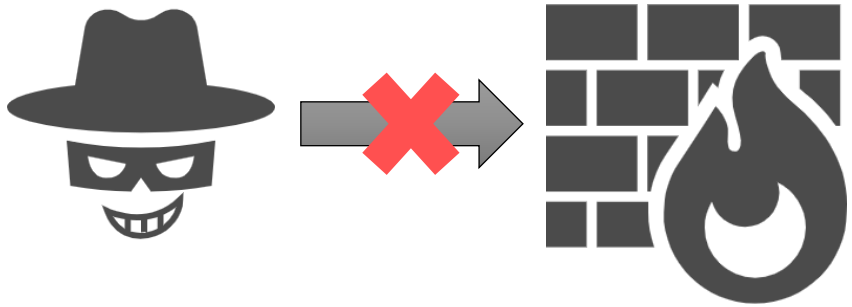
Chapter - 2

ランサムウェア被害を防ぐための セキュリティ対策

ランサムウェア被害を防ぐためのセキュリティ対策

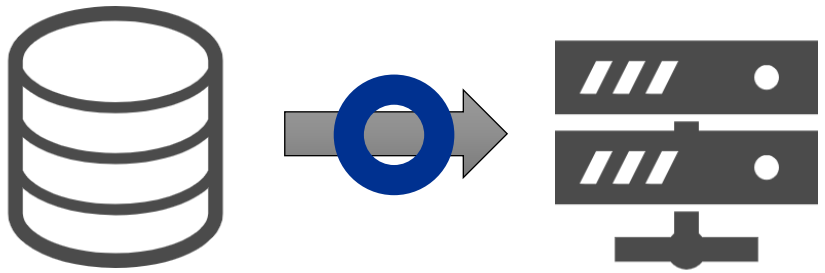
❶ 侵害させないこと

ランサムウェア被害から情報資産を守り、万が一にも身代金を支払わないために、まずはランサムウェアに**感染し、データを侵害させないことが何より重要**



❷ 復旧できること

万が一データを侵害された場合でも、バックアップから復旧できるように**バックアップデータを侵害させないことも同様に重要**



Panasonic

復旧を確実にするための「3-2-1ルール」

3 つの**データ**を ➡ 攻撃者はバックアップを狙う

2 つ以上の**異なる媒体**に ➡ 同時に被害に遭うのを防ぐ

1 つは**遠隔地保管** ➡ 災害などによる喪失の防止

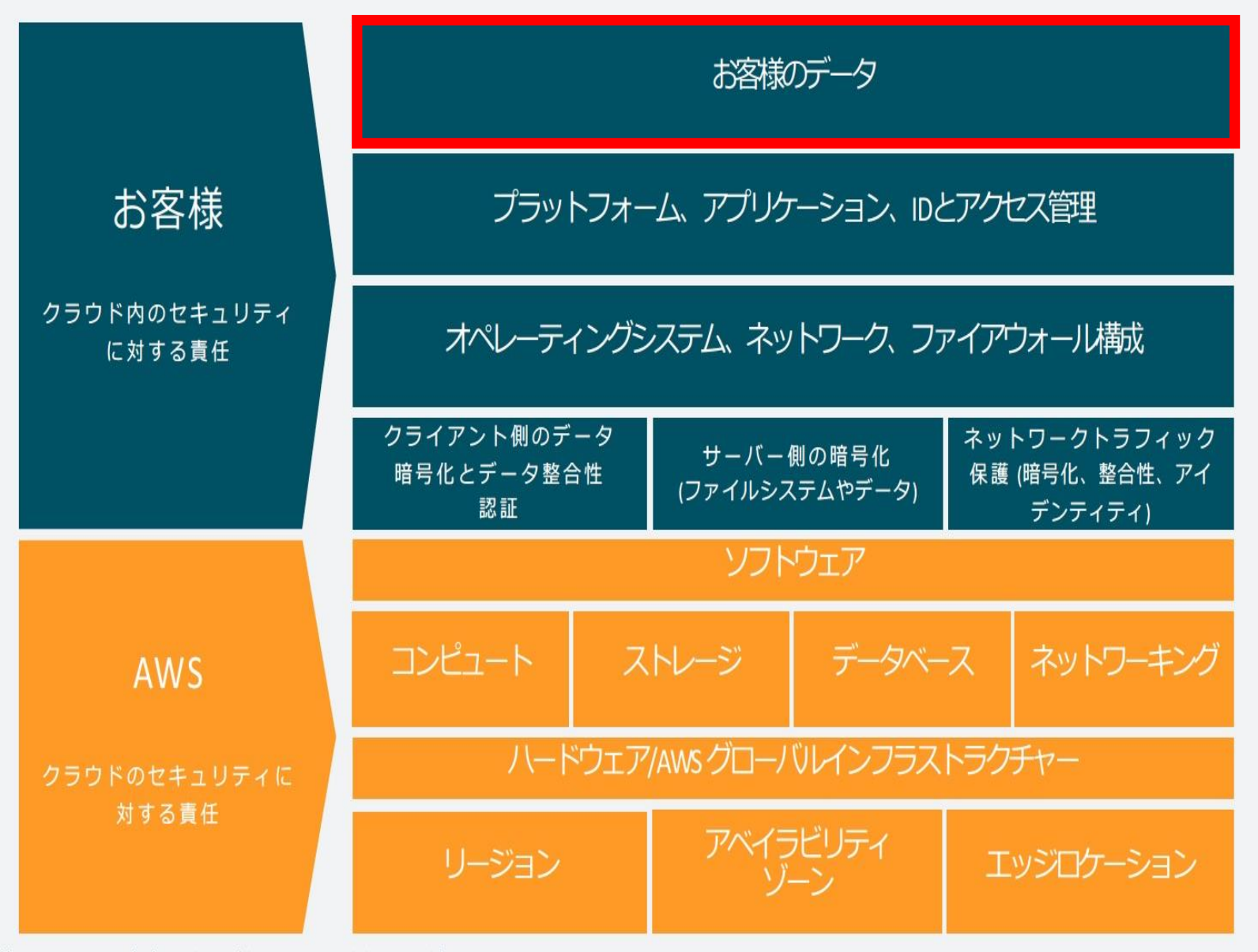
クラウドにバックアップは必要？

Q.クラウドはセキュリティがしっかりしているのに、**バックアップは必要**？

A. バックアップは必要です！

クラウドのバックアップは保証されない

AWS

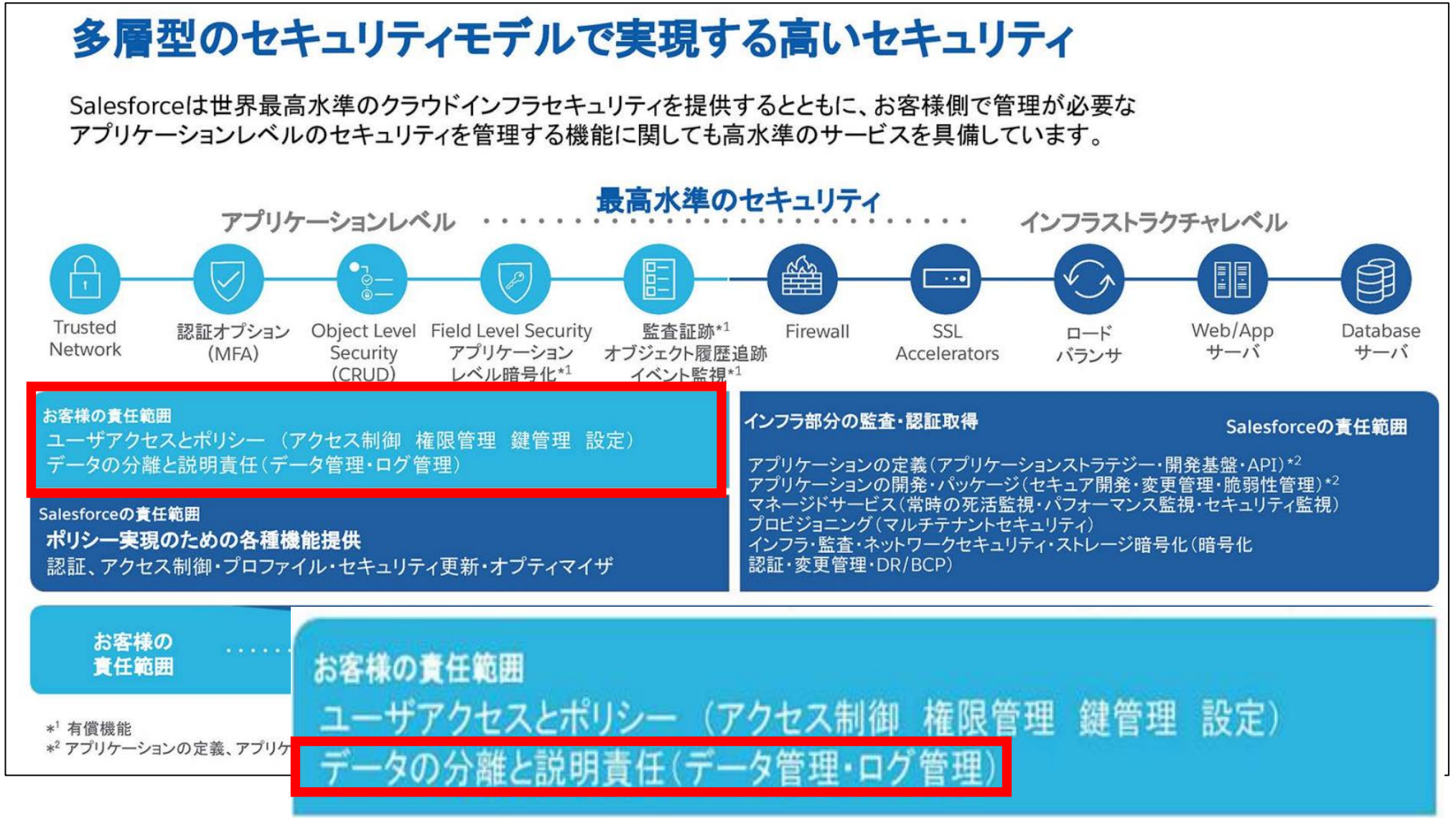


【参考文献】 https://aws.amazon.com/jp/compliance/shared-responsibility-model/

Panasonic

クラウドのバックアップは保証されない

Salesforce



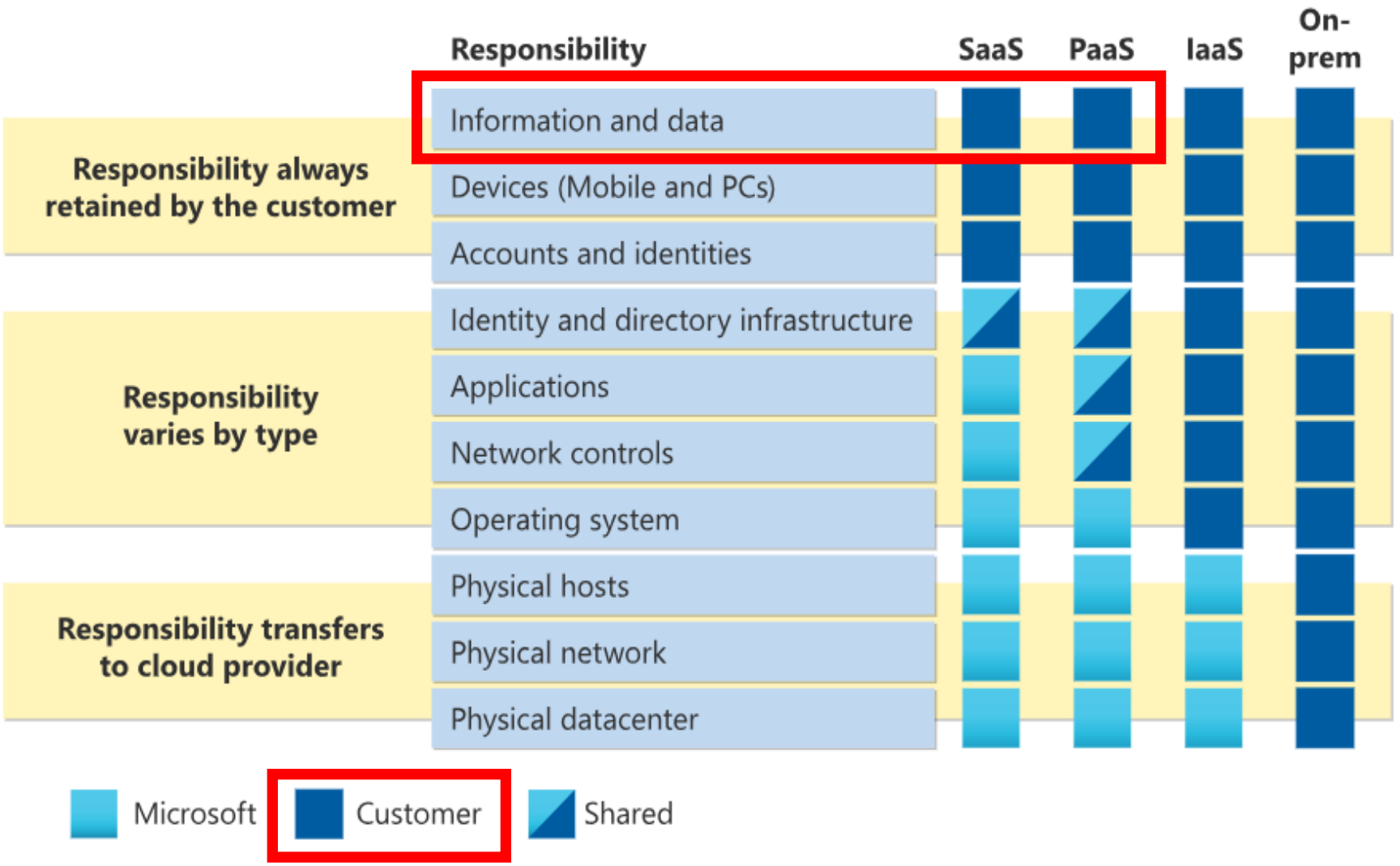
【参考文献】 https://www.salesforce.com/jp/company/shared-responsibility-model/

Panasonic

クラウドのバックアップは保証されない

Microsoftのサイトには「クラウドにおける**共同責任**」として、
SaaS（Microsoft 365含む）の情報およびデータの責任は顧客にあると明言。

Microsoft



責任共有モデル

SaaS提供者の責任	SaaS利用者の責任
プラットフォームの障害	SaaS上のデータ消失
インフラの障害	人為的ミス
アプリの不具合	ランサムウェア被害
災害によるシステム障害	内部脅威

各社、サードパーティ製品でのバックアップを推奨

なぜSaaSのバックアップが重要なのか

人為的ミス

SaaS上のデータ損失の最大の原因は、
エンドユーザーによる削除が全体の約70%

ランサムウェア被害

SaaSのアカウントの乗っ取り、ネットワークを通じてランサムウェアによる暗号化の被害も増加

内部脅威

悪意のある操作が行われたかの証跡を追うために、バックアップデータが必要となる

ランサムウェア時代に必要なバックアップの視点

3 つの**コピーデータ**を

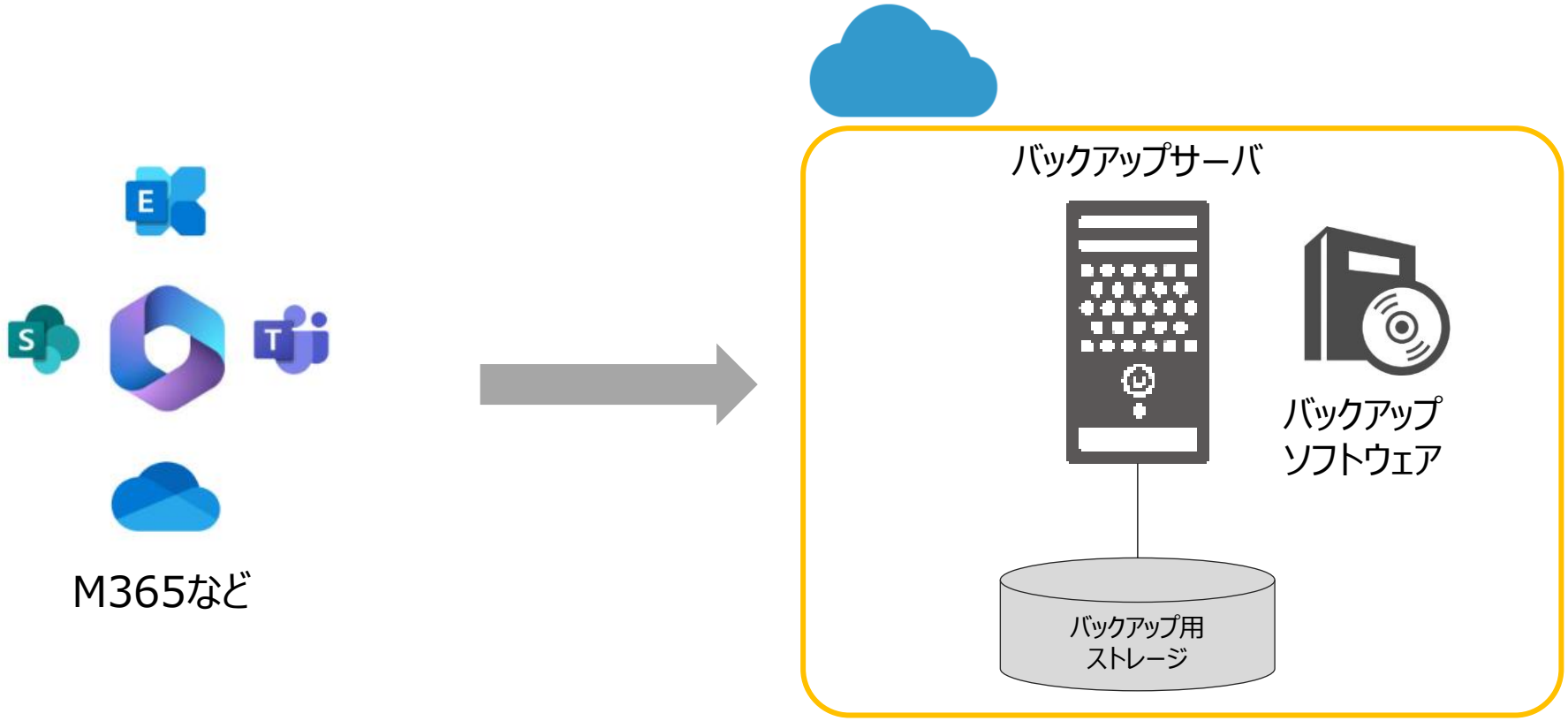
2 つ以上の**異なる媒体**に

1 つは**遠隔地保管**

クラウドストレージによる**イミュータブルバックアップ**

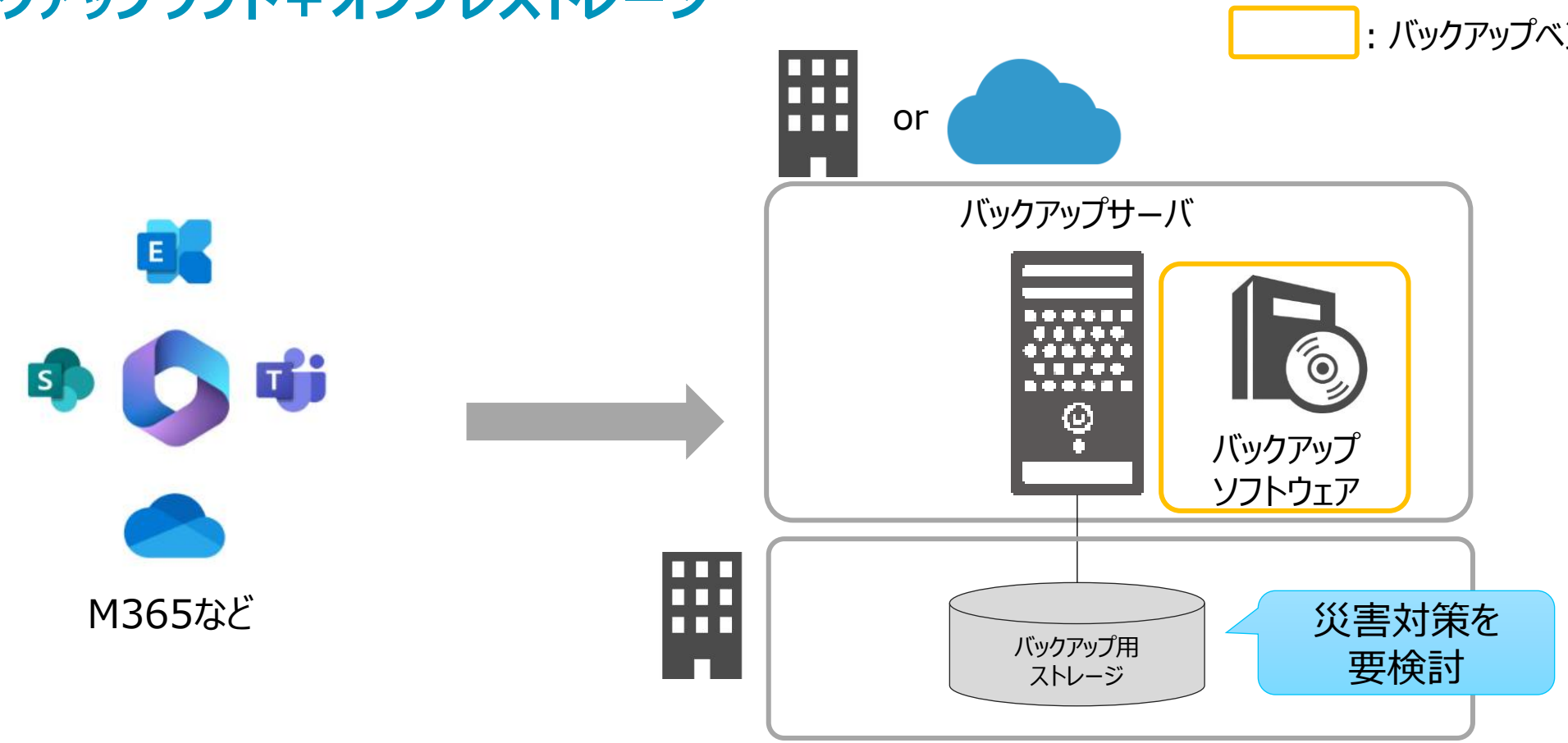
案①　バックアップサービス(BaaS)の利用

：バックアップベンダー提供



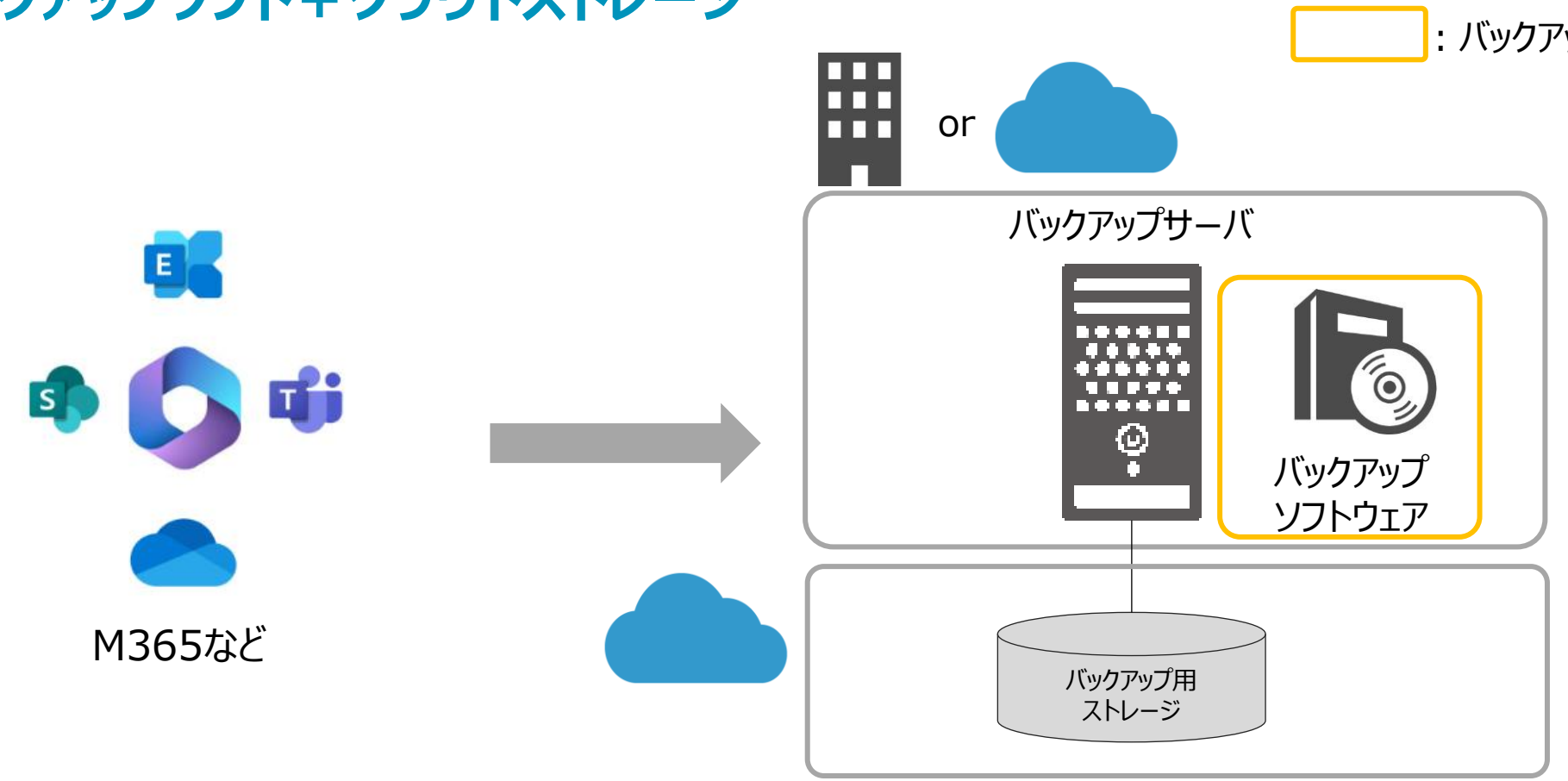
サーバ、ストレージ、ソフトウェアをすべてバックアップベンダーがクラウドで提供

案②　バックアップソフト＋オンプレストレージ



ソフトウェアのみバックアップベンダーが提供し、お客様（またはSIer）がサーバ、オンプレストレージを準備

案③　バックアップソフト＋クラウドストレージ



ソフトウェアのみバックアップベンダーが提供し、お客様（またはSIer）が
サーバ、クラウドストレージを準備

自社の業務要件に合ったバックアップ保存方法・保存先を検討

	バックアップサービス（BaaS）	バックアップソフト＋オンプレストレージ	バックアップソフト＋クラウドストレージ
概要	サーバ、ストレージ、ソフトウェアをすべてバックアップベンダーがクラウドで提供	ソフトウェアのみバックアップベンダーが提供し、お客様（またはSIer）がサーバ、オンプレストレージを準備	ソフトウェアのみバックアップベンダーが提供し、お客様（またはSIer）がサーバ、クラウドストレージを準備
メリット	M365アカウント情報を準備するだけで、バックアップをすぐに始められ、バックアップ以外の運用をすべてベンダーにまかせられる。	M365以外のバックアップ基盤と同様の構成をとることが出来、従来のスキルを多くの部分で活用できる。	M365以外のバックアップ基盤と同様の構成をとることが出来、従来のスキルを多くの部分で活用できる。
デメリット	バックアップベンダーのサービスに依存する為、ベンダーの仕様変更の影響を受けやすい(価格やサービス内容)。	バックアップデータが格納されたストレージの災害対策をさらに検討する必要がある。	選択するクラウドストレージによっては、リストア時にデータを取り出すコストが発生する。(サービスによっては無償)
オススメのお客様	運用メンバーが少人数で可能な限りベンダーに任せたい。	従来のスキルや資産をフル活用したい。	コストパフォーマンスに優れた新しいバックアップを導入したい。

PISCがオススメするクラウドストレージソリューション「Wasabi」

Wasabiの特徴

1 圧倒的低価格

5TBで月額6,670円～※と、他のクラウドストレージと比較し約80%安価。データ転送料も無料

2 ハイパフォーマンス

Wasabi独自のテクノロジーで高速ファイルシステムを実現

3 強固なセキュリティ

99.999999999%のオブジェクト耐久性。オブジェクトロック機能で簡単にランサムウェア対策を実現可能。GDPRなど各種セキュリティ法にも準拠

※年間契約の場合（2024年5月現在）

お客様のご要件に応じて最適化されたクラウドストレージサービスを提供

1. SaaSバックアップ用途

M365など

バックアップサーバ

2. ファイルサーバ用途

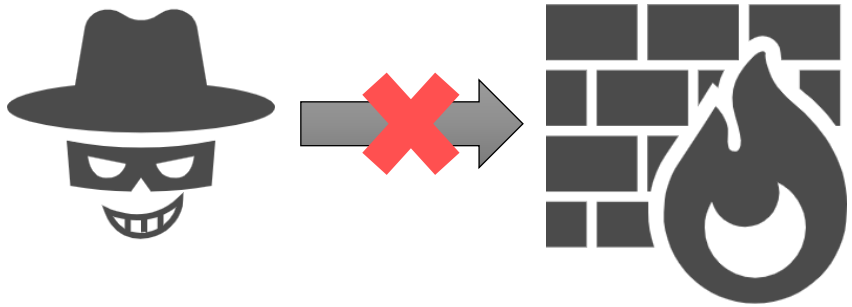
利用者

ファイルサーバ

ランサムウェア被害を防ぐためのセキュリティ対策

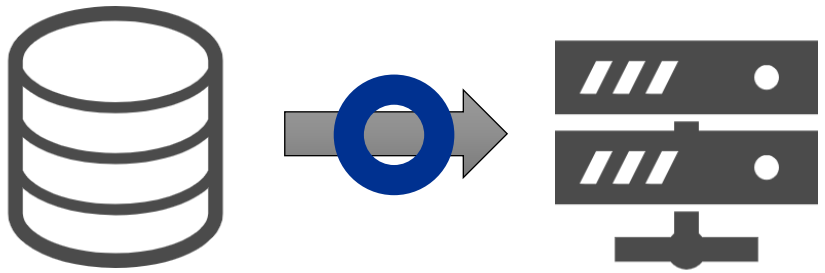
❶ 侵害させないこと

ランサムウェア被害から情報資産を守り、万が一にも身代金を支払わないために、まずはランサムウェアに**感染し、データを侵害させないことが何より重要**



❷ 復旧できること

万が一データを侵害された場合でも、バックアップから復旧できるように**バックアップデータを侵害させないことも同様に重要**



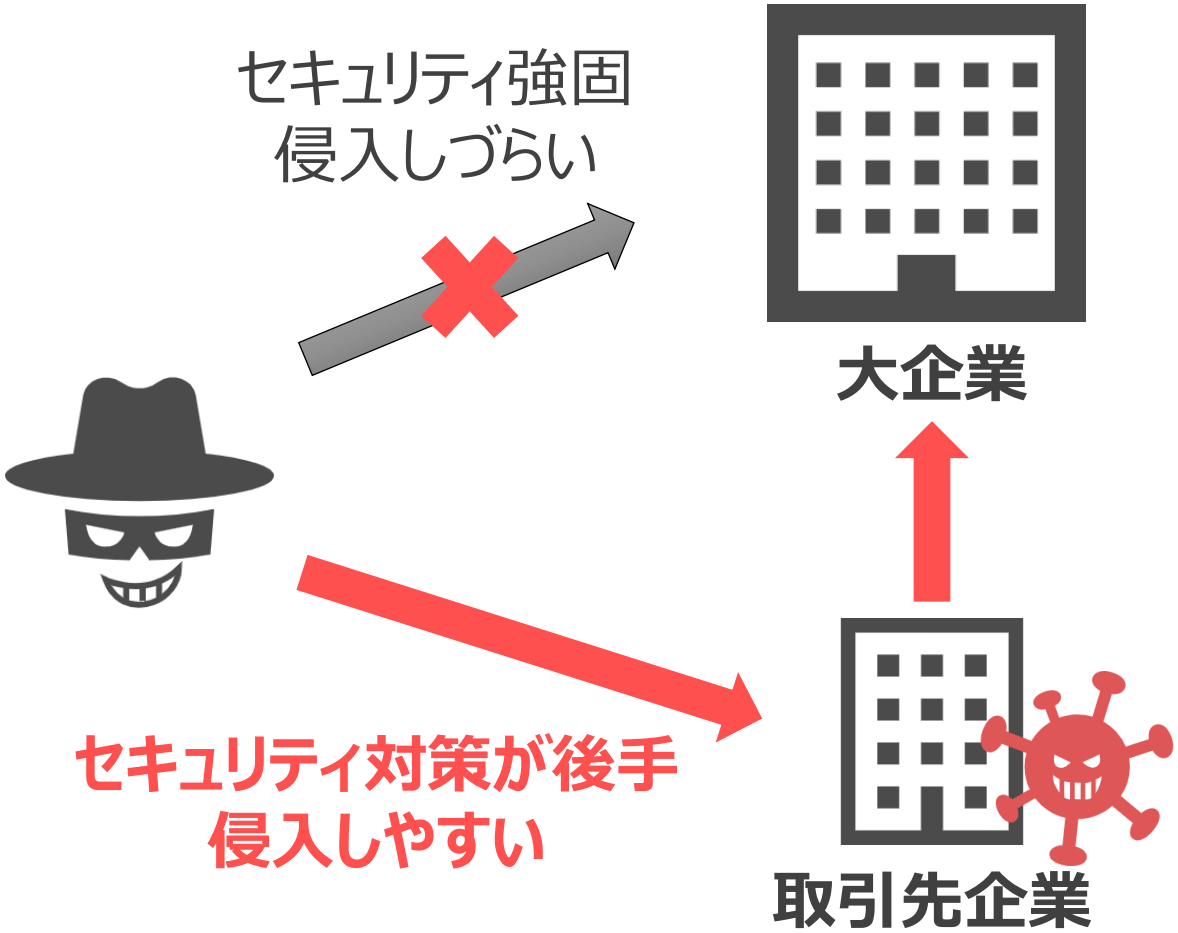
Panasonic

サプライチェーンの弱点を悪用した攻撃が多発

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	**サプライチェーンの弱点を悪用した攻撃**	**2019年**	**6年連続6回目**
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

IPA「情報セキュリティ10大脅威 2024」より抜粋

関連企業や取引先を経由し不正侵入するサイバー攻撃



事例：某医療機関

給食業者のNW機器の脆弱性を悪用し侵入。一部診療が不可となり復旧に2ケ月を要した

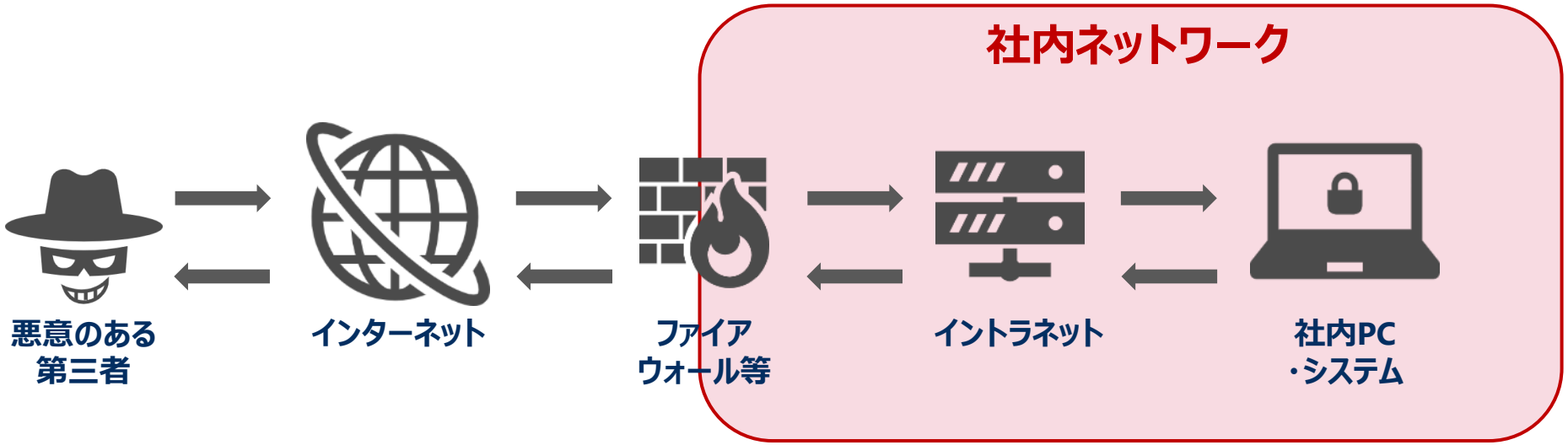
事例：某自動車製造

子会社のリモート接続機器の脆弱性を悪用しマルウェアの被害に。
14か所の工場のラインが1日停止し約1万3000台の生産に影響。

自社を守るためにも、「取引先は信用できる」でなくゼロトラストで

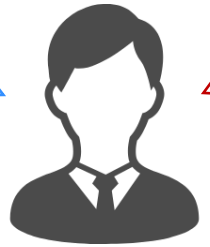
「ゼロトラスト・ネットワーク」とは・・・

「信頼（Trust）を何に対しても与えない（Zero）」という前提に立ったセキュリティ対策の考え方。
従来の「境界型セキュリティ」とは異なり、境界内（イントラネット等）の端末についても常に検証を必要とする。
要するに**「侵入されることを前提として」セキュリティを強化する**考え方。



境界型セキュリティ思考

社内ネットワークは許可されない人は
入って来れないから**安全**だな

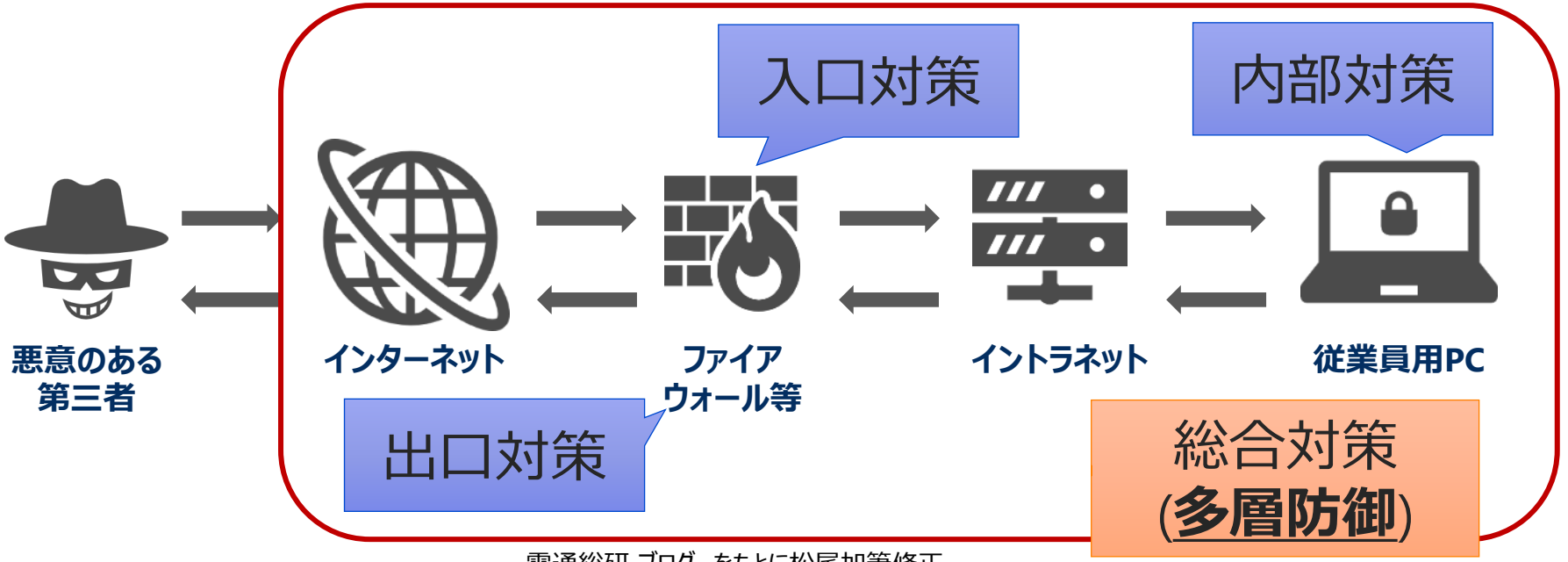


ゼロトラスト的思考

たとえ社内ネットワークといえど**悪意のある**
第三者が入ってくる前提で対策せねば

セキュリティ対策においては要所要所での対策が必要となる

入口対策	ランサムウェア等の脅威を「侵入させない」
内部対策	もし脅威に侵入されてしまっても「発症させない」
出口対策	発症させてしまった際に「被害を拡大させない」



電通総研 ブログ をもとに松尾加筆修正
https://itsol.dentsusoken.com/appguard/blog/security-measures-role-vol16-3499/

セキュリティ製品の種類

ファイアウォール（FW）	入口対策・出口対策	・侵入してきたトラフィックの信頼性を判断し、不審な通信を遮断 ・IPアドレスやポート開放により通信ルールを規定
Web Application ファイアウォール(WAF)、次世代型ファイアウォール(NGFW)	入口対策・出口対策	・従来のFW機能に加え、アプリケーション層までカバーして動作し通信制御をおこなう ・通信パケットの中身を判断し脅威を拡散しない

EPP	AV	入口対策	・脅威侵入を防御する入口対策 ・既定の脅威に関するデータとのパターンマッチングを基にした脅威の検知
	NGAV	入口対策	・AVを拡張し、ふるまい検知やAI、機械学習などを活用し脅威を検知
EDR		内部対策 出口対策	・侵入した脅威の検知とその後の対応をサポート
NDR		内部対策 出口対策	・社内のトラフィックを包括的に監視し、ネットワーク全体を可視化。脅威に対してリアルタイムで対応

電通総研ブログをもとに加筆修正
https://itsol.dentsusoken.com/appguard/blog/security-measures-role-vol16-3499/

セキュリティ製品トレンドの変遷

FW、アンチウイルス

特徴

・過去の攻撃方法に基づく防御
・**誰かが攻撃を受ける**ことで初めてシグネチャが作成される

入口対策

EDR

特徴

・過去の攻撃パターンを学習
・未知のマルウェアに対応するため、**感染後の「ふるまい」**を検知

出口対策

先進セキュリティ

特徴

・深層学習やAI等の先進技術を活用し**未知のマルウェアの発症を未然に防ぐ**

総合対策

入口対策への回帰

なぜ入口対策への回帰が起こるのか①

最速のランサムウェアは10万個のファイルを4分で暗号化

(Splunk)SURGeが公開した「ランサムウェアの暗号化速度に関する調査レポート」では、Lockbit、REvil、Blackmatterを含む10種類の主要なランサムウェア株が、**100,000個のファイルを暗号化する速度を計測**しています。その結果、中央値は42分52秒でした（ファイルサイズは合計53.93GB）。

ただし、ファイルを暗号化する速度は、ランサムウェアの系統や感染したPCのリソースによって異なり、**最速のランサムウェアは約4分で暗号化を完了**しました。最長は3時間半でした。(2022年5月)

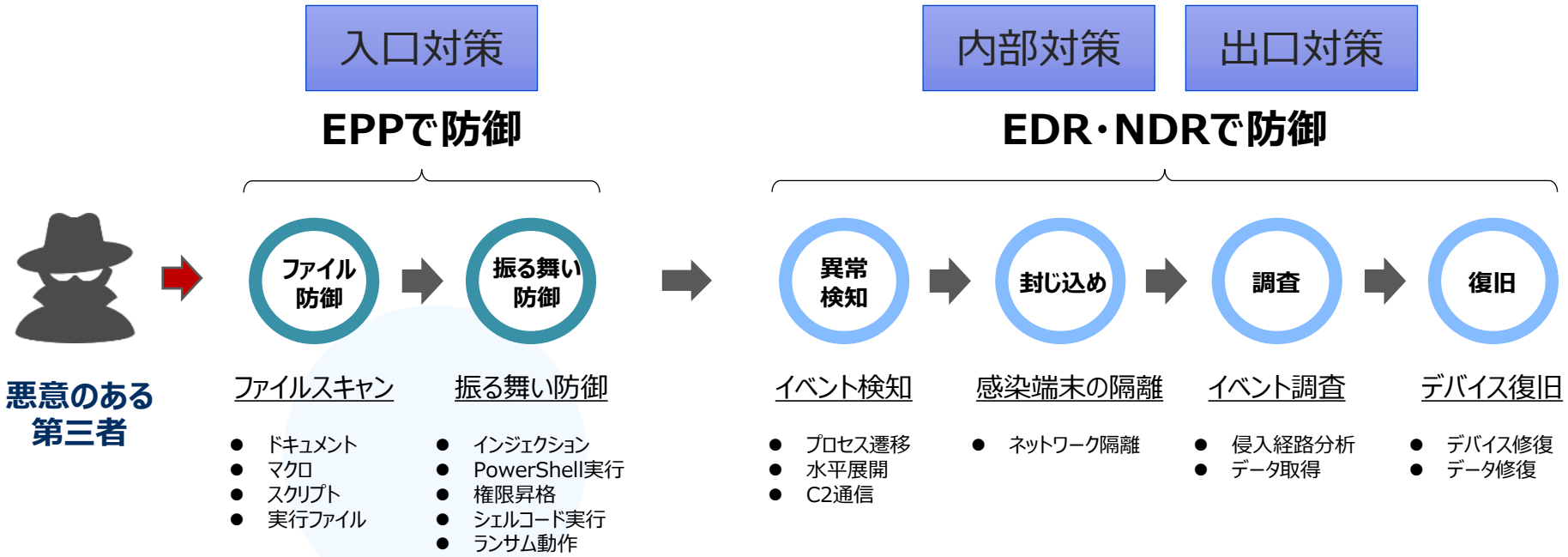
攻撃の巧妙化・PCの性能向上により被害範囲が拡大

→**「マルウェアが発症しない」入口対策～内部対策のニーズの高まり**

https://www.splunk.com/ja_jp/blog/leadership/splunk-publishes-global-research-report-on-ransomware-encryption-speed-and-current-state-of-security.html

なぜ入口対策への回帰が起こるのか②

出口対策はコストがかかるため、発症しないに越したことはない



対策コスト ¥ ¥¥ ¥¥¥

更に万が一発症した際の**調査や復旧には莫大なコスト**がかかる
（CSIRT等の運用体制も必要）

Panasonic

本セッションのまとめ

- 製造業を狙ったランサムウェア被害は増加傾向にある
- 万が一のランサムウェア被害を防ぎ、身代金の支払いをしないために「復旧できる」「侵害させない」両軸での対策が必要
- バックアップの強化のために「イミュータブルバックアップ」を導入し、万が一の場合も復旧できる備えを
- セキュリティの強化にあたっては「多層防御」を基本とし、特に「発症させない対策」に重きを置くことは有用

マルウェア・ランサムウェア被害を未然に防ぐには？

当社がお薦めするエンドポイントセキュリティの一つ

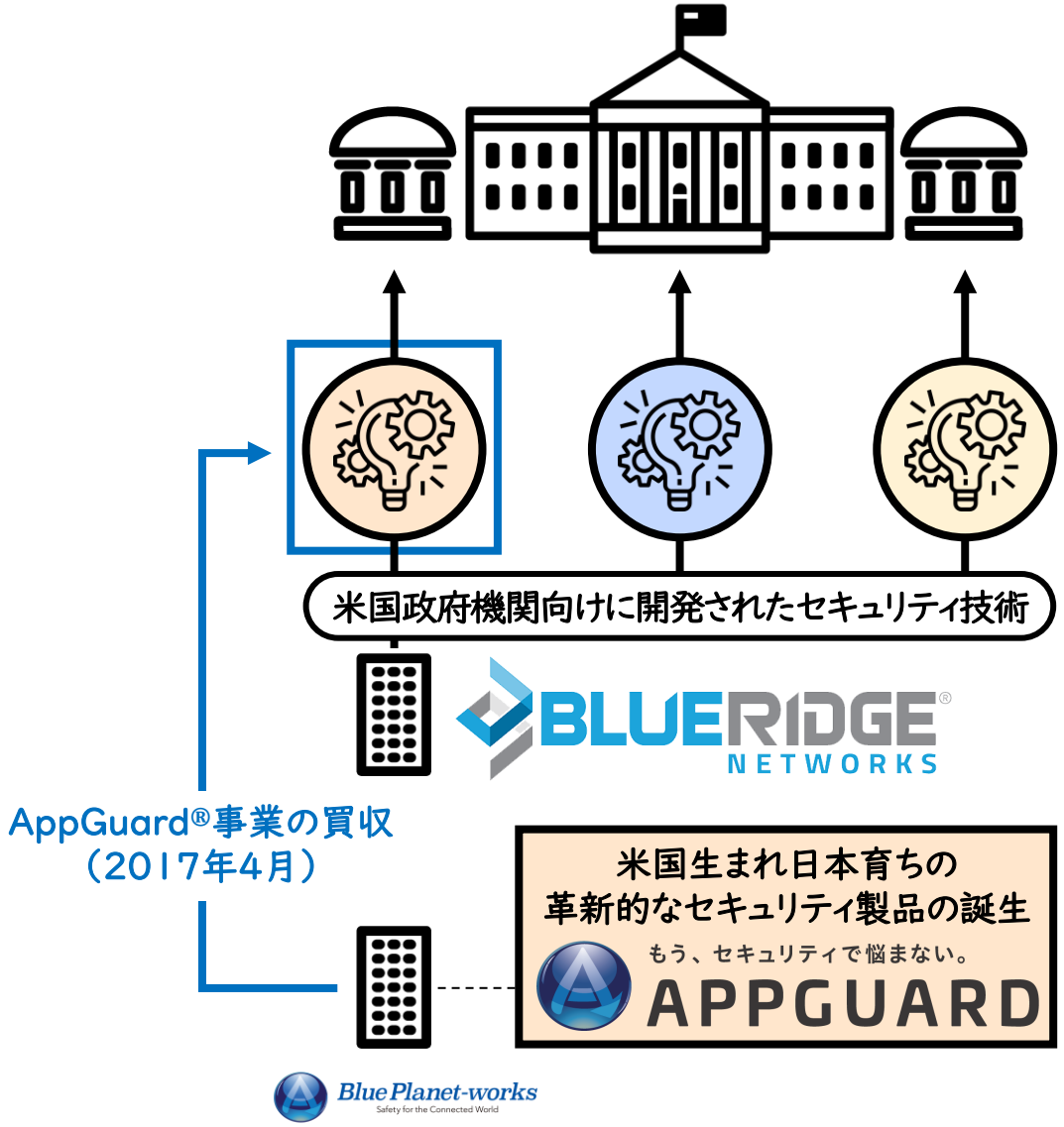
Session – 2

感染しない！させない！
攻撃が成立しないセキュリティ対策製品
AppGuard

株式会社ITガード

株式会社Blue Planet-worksについて

商号	株式会社Blue Planet-works
住所	141-0032 東京都品川区大崎4-1-2 ウィン第2五反田ビル3F
設立	2017年4月
資本金	85億円（2023年12月時点）
代表取締役社長	坂尻浩孝
事業内容	「AppGuard」の技術を応用したサイバーセキュリティプロダクトの開発・販売及び付帯サービスの提供
従業員数	28名（2023年12月時点）
関連会社	株式会社ITガード、AppGuard Inc
株主	株式会社東京ウェルズ SBIインベストメント株式会社 Blue Ridge Networks, Inc. PCIホールディングス株式会社 ANAホールディングス株式会社 富士フイルムビジネスイノベーション株式会社 株式会社電通グループ 株式会社JTB 第一生命保険株式会社 損害保険ジャパン株式会社 他多数

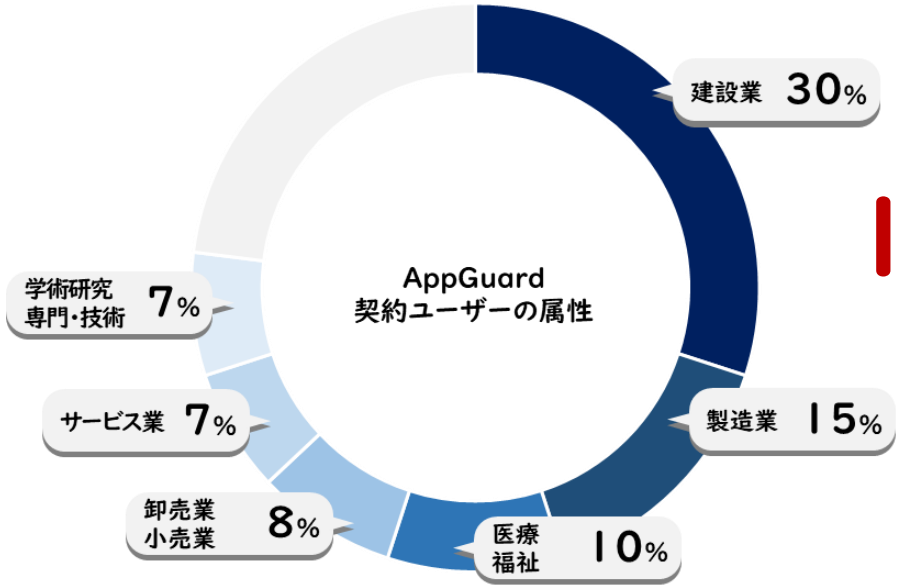


株式会社ITガードについて

商号	株式会社ITガード
住所	141-0032 東京都品川区大崎4-1-2 ウィン第2五反田ビル3F
設立	2017年7月
資本金	6,100万円
役員	代表取締役　鬼澤 禎 取締役CTO　吉川 剛史
事業内容	エンドポイントプロテクション製品AppGuardおよびそれに付帯するソリューションを提供
ITガードの強み	1．圧倒的No1のAppGuard販売・導入実績 主な導入実績：戸田建設様5,300台、SBI証券様1,100台、千葉工業大学　200台、他100社以上 相澤病院、名寄市立総合病院、弓削病院など多数の病院導入事例あり 2. プロ集団の技術力 AppGuardを熟知したチームがお客様目線でフルサポート 3. 付加価値サービスのご提供 導入支援パック、運用サービスのご提供 当社専用サイバー保険のご提供

AppGuardビジネスの堅調な推移（AppGuard採用企業実績）

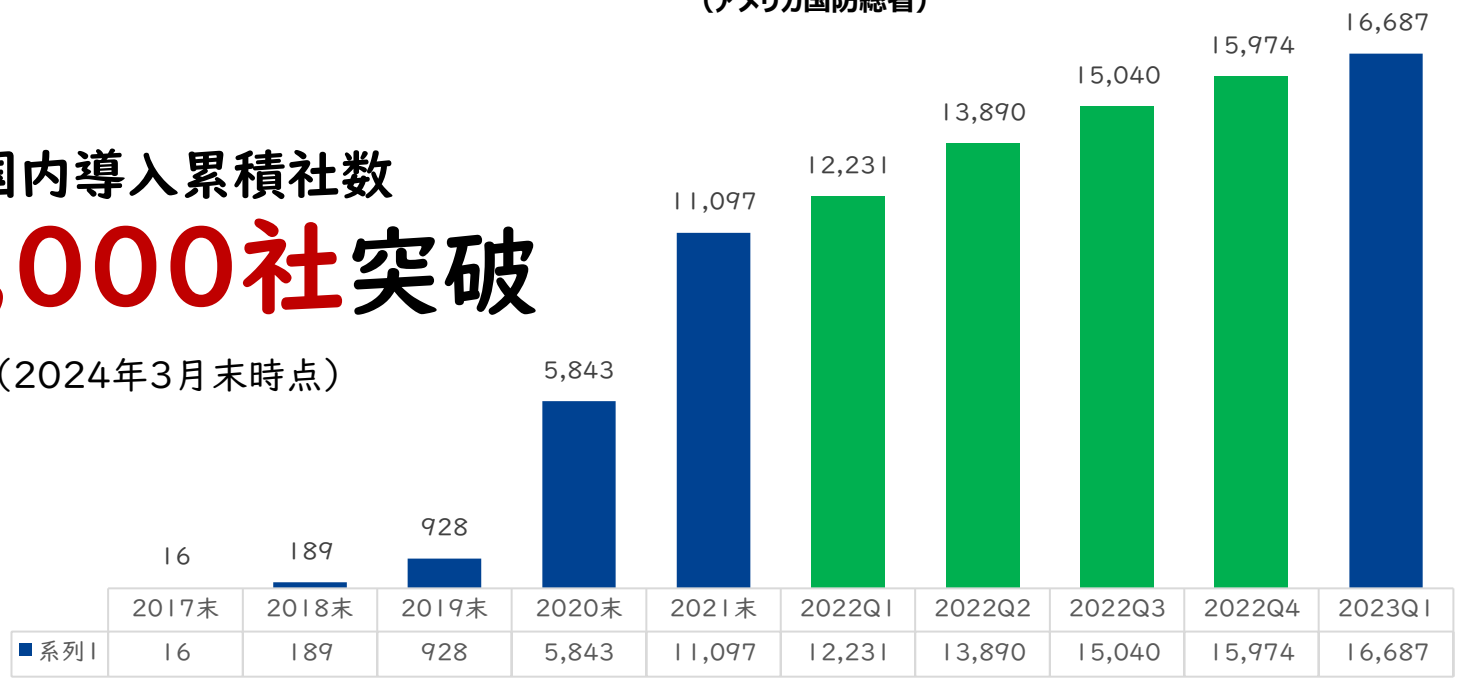
ANA
SMBC日興証券
埼玉医科大学病院 Saitama Medical University Hospital
特定医療法人 佐藤会 弓削病院
戸田建設
UCHIDA
人・街・未来をまもる 東洋テック
Fibergate Inc. 株式会社ファイバーゲート
KAKUDAI
ecoHAI
社会福祉法人 千葉市社会福祉協議会
（白石市様）
dentsu
DAIKO
PCI Solutions INC.
NEC NECキャピタルソリューション
吉本興業
BANC OF CALIFORNIA
（アメリカ国防総省）
ColumbiaBank



国内導入累積社数

19,000社突破

（2024年3月末時点）

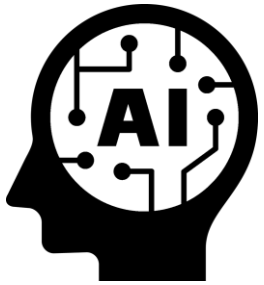


エンドポイントセキュリティの市場動向

- アンチウイルスに代わる何かを求めて -

アンチウイルスは昨今の脅威に対して不十分

過去の情報に依存



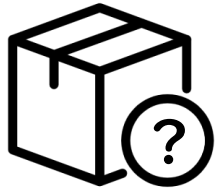
機械学習解析

振る舞い解析

過去の脅威情報から特徴を抽出

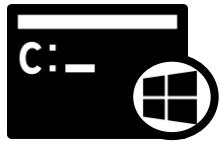
未知の攻撃
構造の難読化
に弱い

検出対象は「悪いモノ」だけ



危険かも？

要検査



安全なはず！

検査なし

「悪意あり」と規定したものを検知

正規ツールの悪用
正規機能の悪用
に弱い

アンチウイルスソフトの実態

	S社	T社	M社	Microsoft	E社	K社	W社	C社
検体#1:BitRat	検知できず	検知できず	検知できず	検知	検知できず	検知できず	検知できず	検知できず
検体#2:FromBook	検知	検知できず	検知	検知	検知できず	検知	検知できず	検知できず
検体#3:Remocos	検知	検知できず	検知	検知	検知できず	検知	検知できず	検知できず
検体#4:Wacatac	検知できず	検知できず	検知できず	検知	検知できず	検知	検知できず	検知できず
検体#5:AgentTesla	検知できず	検知	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
検体#6:Gcleaner	検知できず	検知できず	検知	検知	検知	検知できず	検知出来ず	検知できず
検体#7:LockBit	検知できず	検知できず	検知	検知できず	検知できず	検知できず	検知できず	検知
検体#8:LockBit	検知	検知できず	検知できず	検知	検知できず	検知	検知できず	検知
検体#9:LockBit	検知できず	検知できず	検知できず	検知できず	検知	検知できず	検知できず	検知できず
検体#10:AgentTesla	検知	検知	検知できず	検知	検知できず	検知	検知できず	検知できず

EDR・XDRの登場

UTM・アンチウイルス

EDR/XDR

特定 Identify

防御 Protect

検知 Detect

対処 Respond

回復 Recover

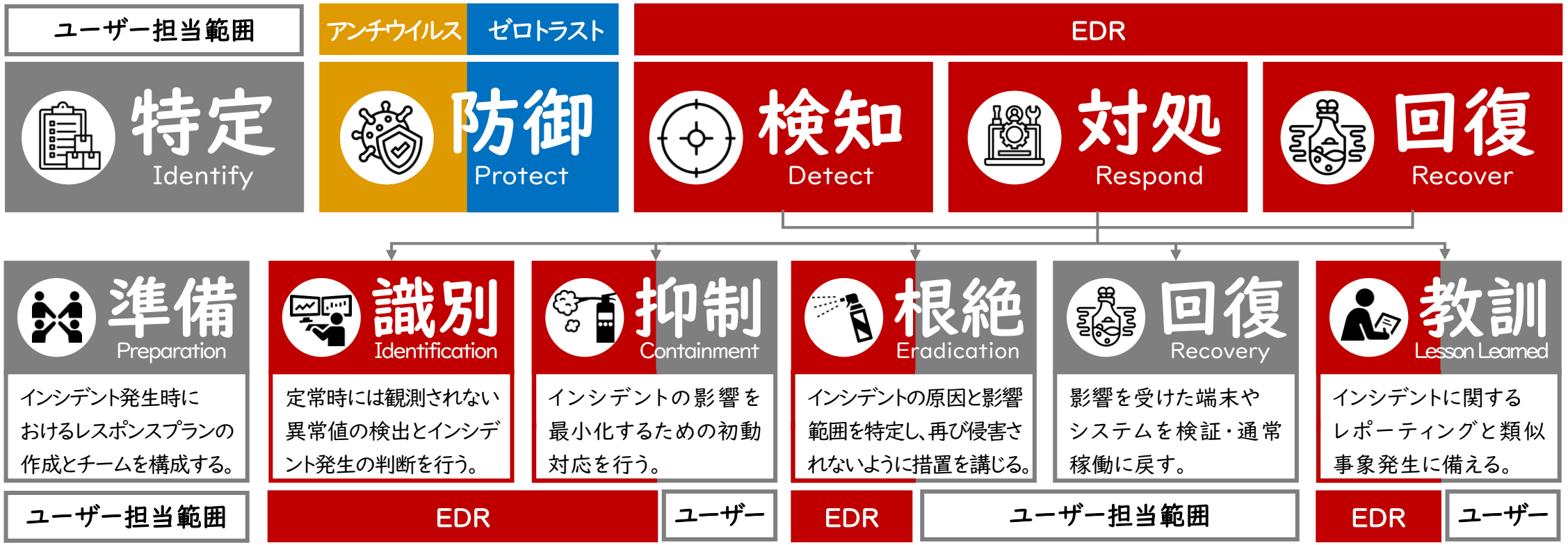
←これまで投資してきた領域（事前対策）→

←これまで投資してこなかった領域（事後対策）→

アンチウイルス領域	EDR/XDR領域
TREND MICRO / KASPERSKY / SOPHOS / Trellix / eset / WITH secure	CROWDSTRIKE / SentinelOne / Carbon Black. / cybereason

アンチウイルスベンダーはEDR/XDR領域へ
EDR/XDRはアンチウイルス領域へ
互いに製品を拡張

EDR利用における留意事項

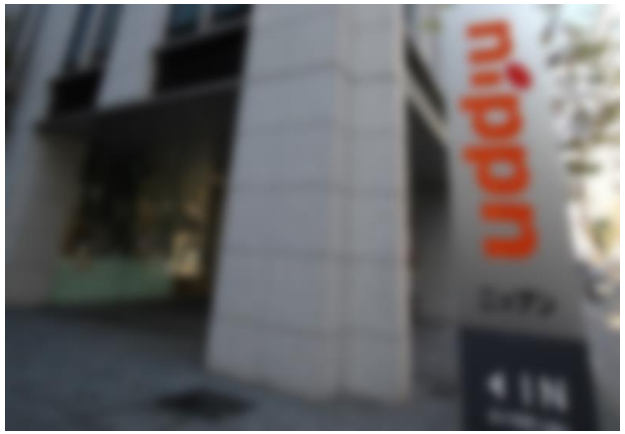


【SANS Instituteにおけるインシデントレスポンスの構成要素（EDR導入に際して設計・構築が必要なスキーム）】

24時間365日リアルタイムで対応できる
専門人材の配置・運用体制の構築が必須

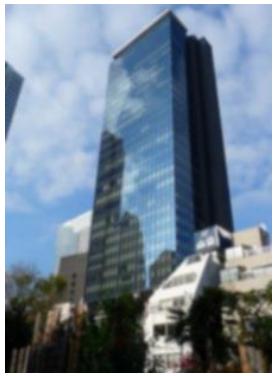
セキュリティ業界を騒がせた主なニュース

トヨタグループのサプライチェーン内の
企業がランサムウェアの被害に遭い
トヨタグループの全工場がストップ



・四半期決算報告を延期
・約9割のシステムで被害が発生し帳票処理が手作業に

2022年3月に入りEmotetに感染し
メール送信に悪用される可能性のある
.jpメールアドレス数が2020年の
感染ピーク時の約5倍以上に急増



東京都や千葉県市川市から業務委託を
受けていた建設コンサルタント会社が
ランサムウェアの被害に遭い、
7億5千万の特別損失を計上

日本最大級の港へのサイバー攻撃

・日本最大級の港がサイバー攻撃の被害に
・コンテナの積み下ろしができない状態に

地方町立病院を襲ったランサムウェア

・8万5千人分の電子カルテが消失
・新規患者受け入れ2ヵ月間停止

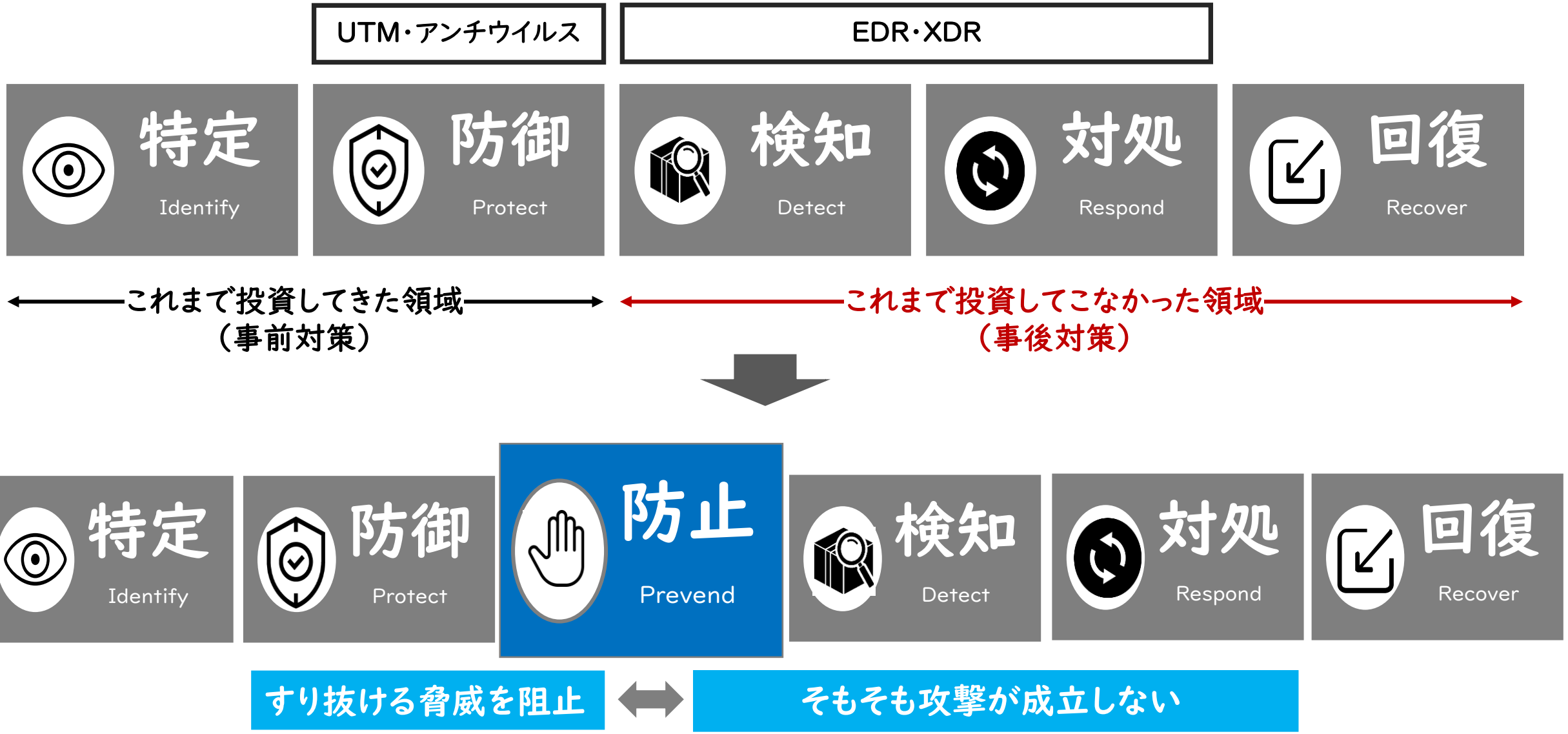
大阪の病院への攻撃

・取引先から感染し電子カルテ含む基幹システムが使用不能に
・通常医療体制に戻るまで約2か月半かかった

「防御」ではなく「防止」するという考え方

- ゼロトラスト型エンドポイントセキュリティ「AppGuard」 -

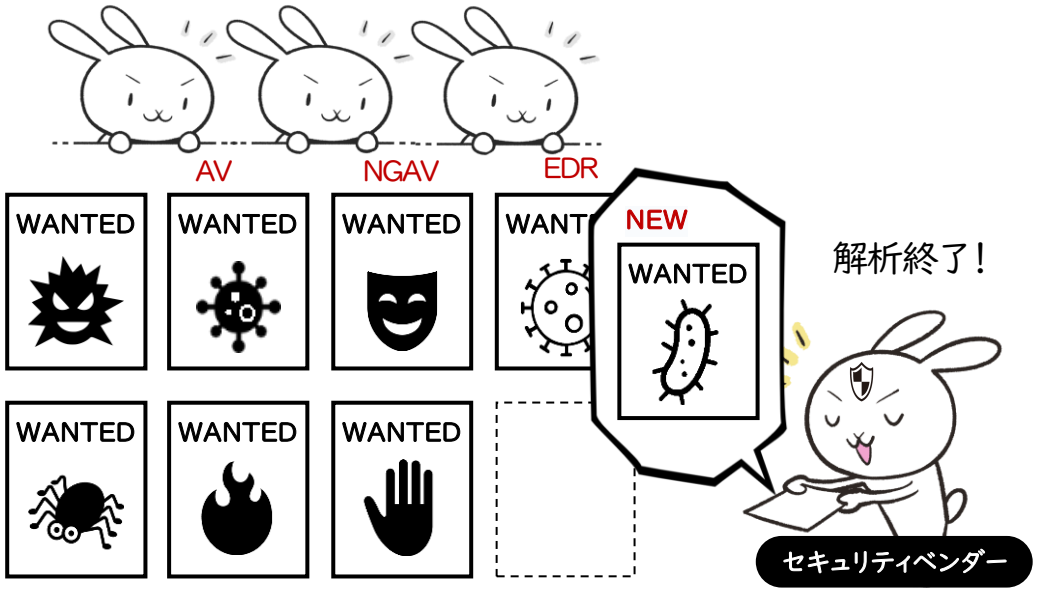
“攻撃を「防止」する”という概念を補完



求められる新しい守り方

これまでの守り方

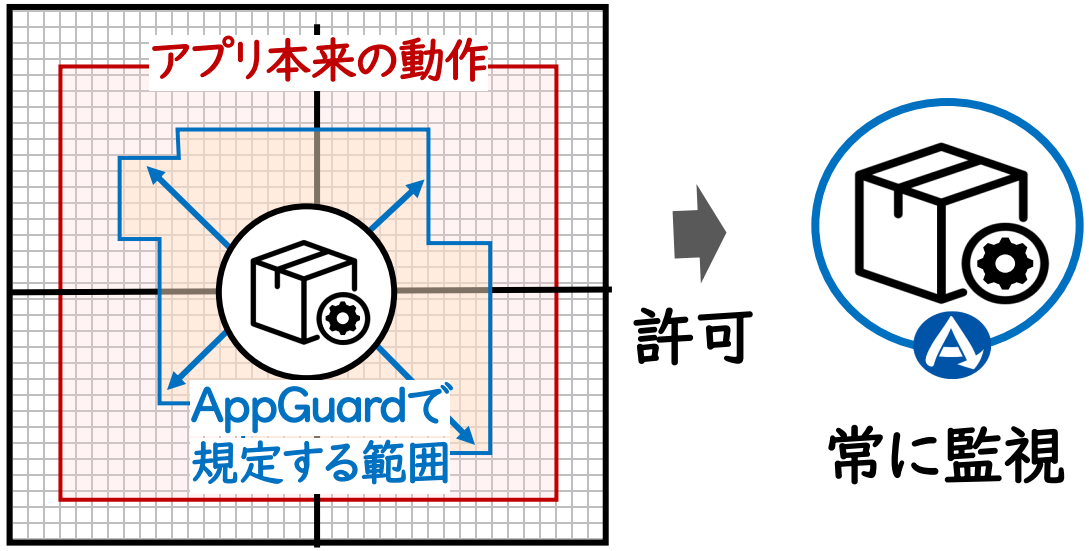
悪いものを見つけて排除



新しい攻撃を作れば攻撃者の勝利

AppGuardの守り方

悪い事をさせない環境を作る



ウイルスは発症しない

求められる新しい守り方

~~悪意があるかの判断~~

~~マルウェアの検知~~

~~マルウェアの駆除~~

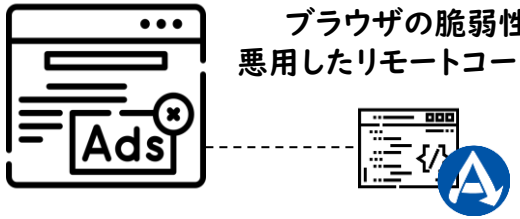
規定したこと以外は
『誰であっても』『どんなことでも』実行できない

もう、セキュリティで悩まない。

APPGUARD

「AppGuard」ならやらかしても大丈夫

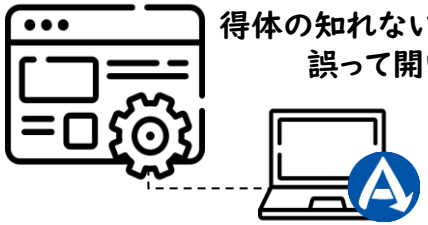
ウェブサイトの怪しい広告に騙される



ブラウザの脆弱性を
悪用したリモートコード実行

不正アクセスは成立しない

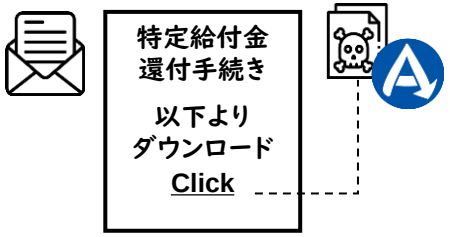
怪しい実行ファイルを誤って起動



得体の知れないファイルを
誤って開いた

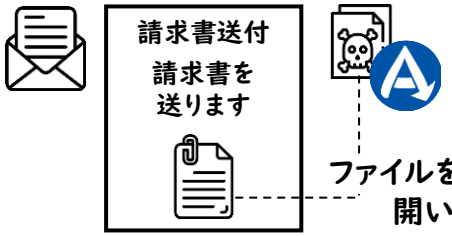
不正なファイルは起動しない

メール本文の怪しいURLをクリック



不正なファイルは起動しない

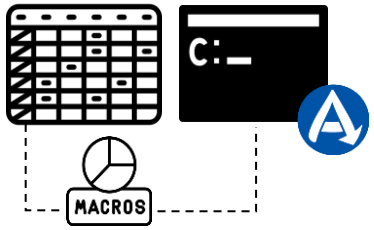
メールに添付された怪しいファイルを開く



ファイルを誤って
開いた

不正なファイルは起動しない

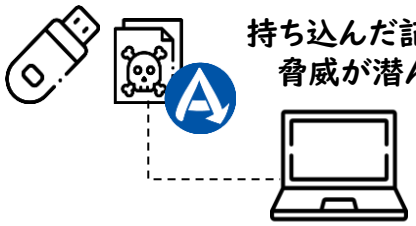
見知らぬマクロやスクリプトを有効化



仕掛けを誤って
有効化

スクリプトを介した攻撃は成立しない

未認可の外部記憶装置を接続

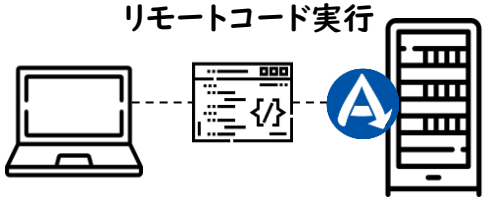


持ち込んだ記憶装置に
脅威が潜んでいた

不正なファイルは起動しない

乗っ取られた端末からリモートコード実行

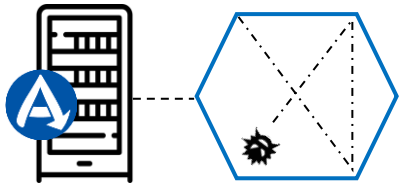
到達性のある端末からサーバーへ
リモートコード実行



リモートコード（RCE）の実行は不可

サーバーへ不正侵入して足場の構築

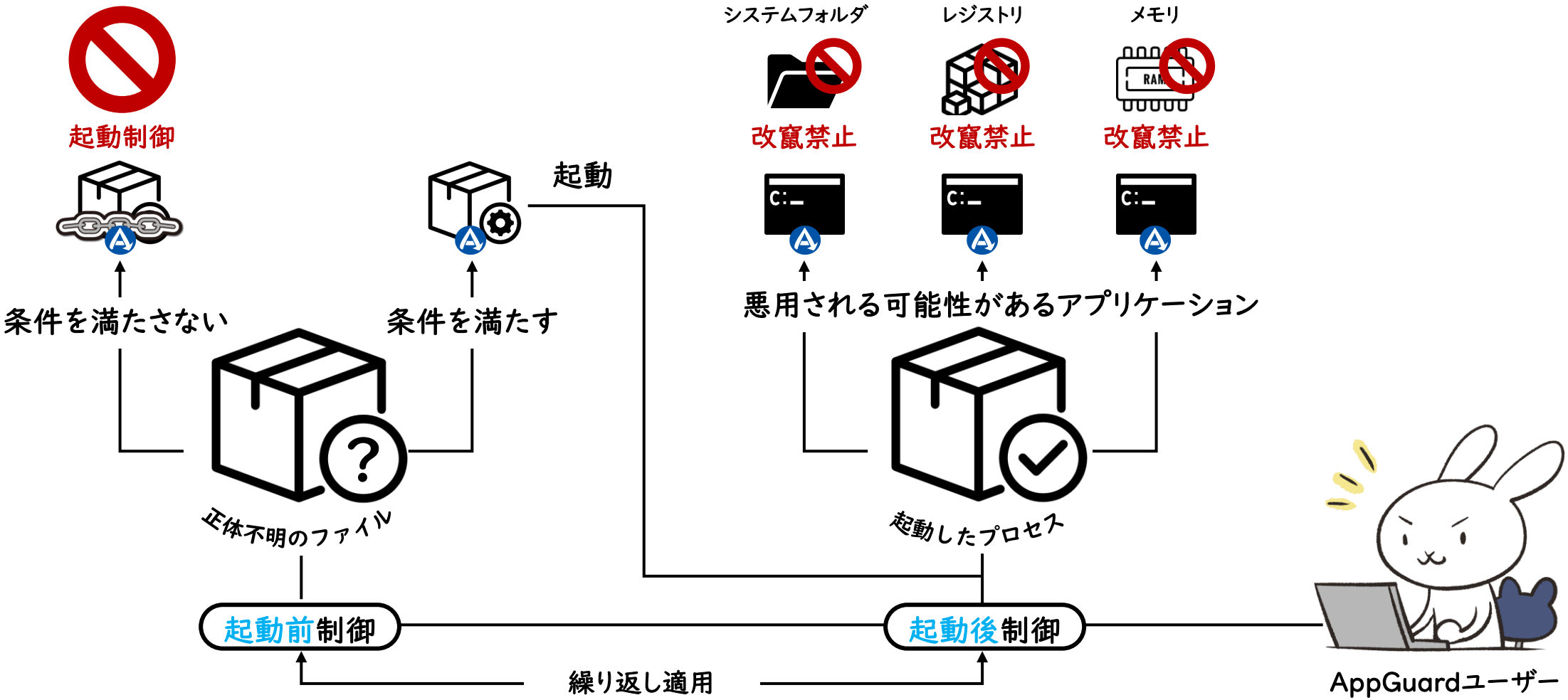
攻撃者に侵入される



侵入できても何もできない

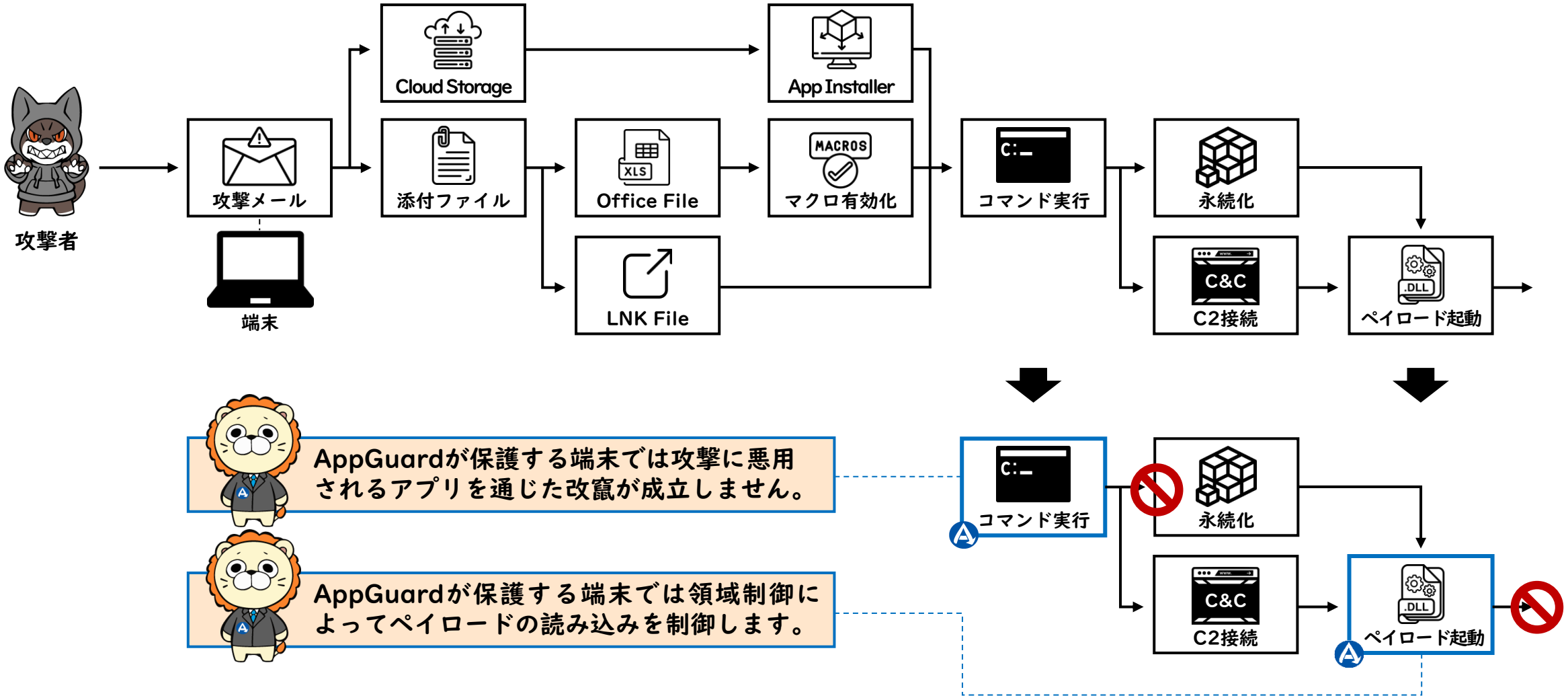
AppGuardが攻撃プロセスの成立を阻止

「やって良いこと・悪いこと」を明確に規定し
「やって良いことだけ」が常に実践されているか検証し続ける



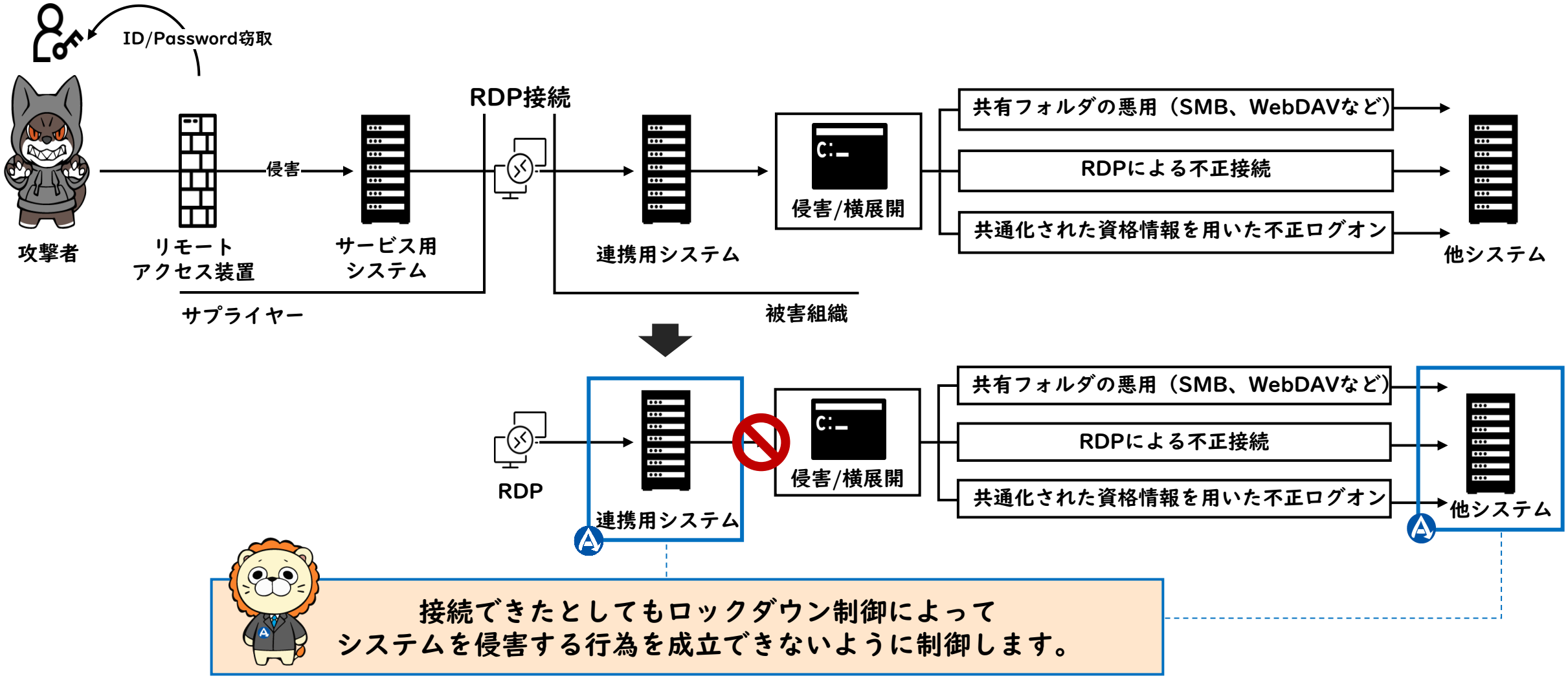
AppGuardによる攻撃阻止パターン #1

Emotetが用いたケース



AppGuardによる攻撃阻止パターン #2

サプライヤーからのRDP接続を介して侵入されたケース（例：大阪急性期・総合医療センターの事例）

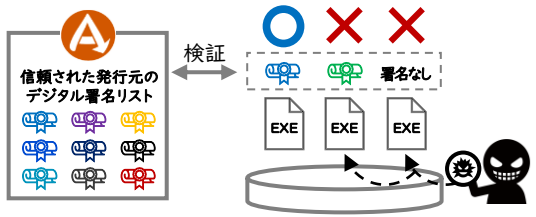


出典：「大阪急性期・総合医療センター」及び「社会医療法人生長会」の侵害事案について当該組織又はメディア等で報道された内容を基に構成

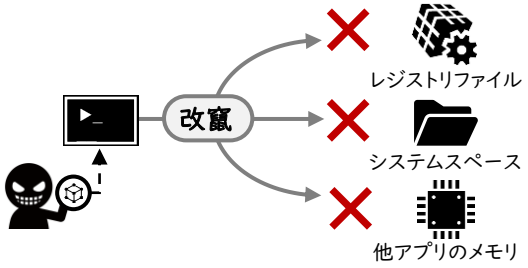
AppGuardのラインナップ

ゼロトラスト型 エンドポイントセキュリティ

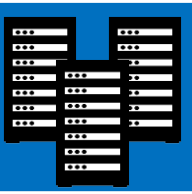
信頼された アプリケーションしか 起動させない



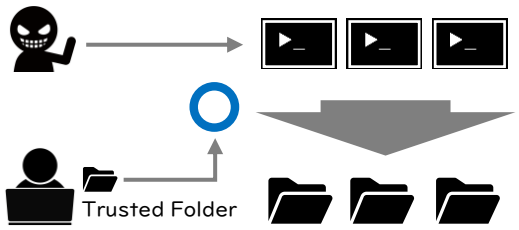
不正アクセスにおける 侵攻プロセスを 成立させない



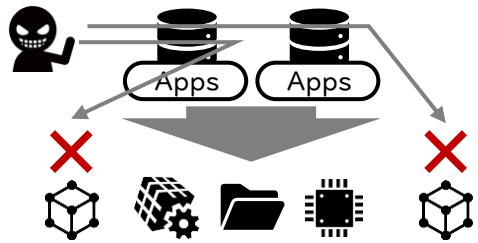
ロックダウン型 サーバーセキュリティ



サイバー攻撃の ライフサイクルを 分断する



想定外のプロセスを サーバー上で 起動させない



AppGuard Enterprise/SBE/Solo

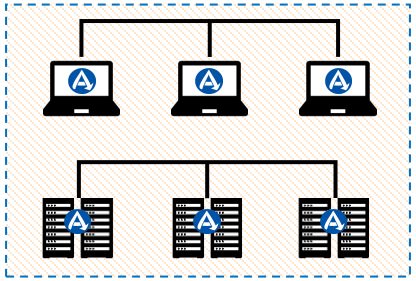
AppGuard Server

AppGuardの導入パターン

・アンチウイルスやEDRと併用可能

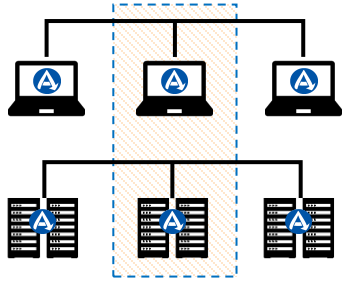
構成①	Windows Defender（Windows標準コンポーネント）	AppGuard
構成②	3rd Partyアンチウイルス	AppGuard
構成③	EDR with NGAV機能	AppGuard

AppGuardを全体へ導入



OR

AppGuardを部分的に導入

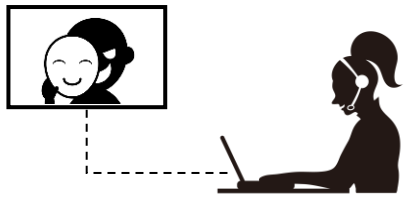


・部分的な導入も可能

機密情報を扱う部署

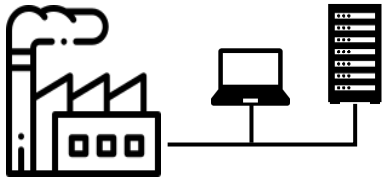
組織内でも特に機密性の高い情報を扱う端末を保護

業務上リスクが高いユーザー



不特定多数の相手と情報のやり取りが発生する端末を保護

閉域環境にある特殊端末



生産領域や医療ネットワーク等インターネットに接続できない環境にある端末を保護

残ってしまったレガシーな端末

Windows 7等のサポートが終了したOSをやむを得ず継続利用している端末を保護

絶対に死守したい端末

インシデントが発生すると被害拡大、業務停止、大規模損失につながる端末を保護

安心の各種付帯サービス

AppGuardご利用時に必要な各種作業や運用を
専門のエンジニアが手厚くサポート

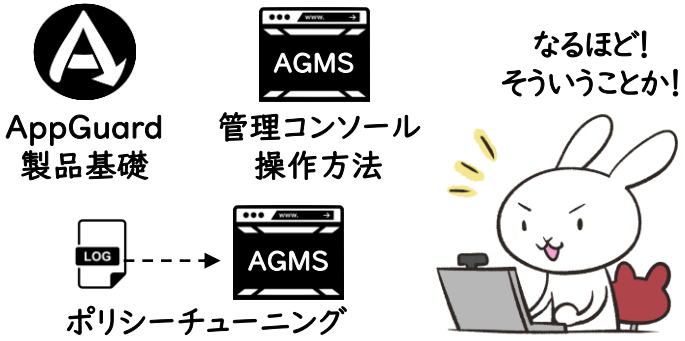
AppGuard導入パッケージ

AppGuardをご利用いただくための
「環境調査」「ログ収集」「解析」「設計」
「設定」「反映」の全てのフェーズを代行し
スムーズに本番展開できるように支援します

AppGuard運用パッケージ

AppGuardの運用を支援するサービスデスクを
ご提供し、基本的な操作方法だけでなく、
お客様に代わって調査・解析に基づくポリシー
設計・設定・反映なども実施します

AppGuard教育パッケージ



AppGuardをご利用いただく管理者のために
必要となる教育を行います。製品の基礎知識や
管理コンソールの操作方法、生成されたログに
基づくチューニング方法などが含まれます

※各種支援メニューの内容は販売店によってサービス名及び提供仕様が異なります。詳細については各販売店にお問い合わせください。

パナソニック インフォメーションシステムズについて

ONE Panasonic IT

私たちの使命

デジタルと人の力で
「くらし」と「しごと」を幸せにする。

PX
Panasonic Transformation

MISSION

お客さま、お取引先さま、従業員に、
ITによる本質的な価値を提供、経営に直接貢献。

ITを創る喜びを

- お客さまの → 便利と嬉しいへ
- お取引先さまとの → シナジーへ
- 従業員の → キャリア形成と成長へ

VISION

私たちはビジネスに寄り添う、Co-Creatorです。
お客さまの「くらし」と「しごと」を共に考え、共に創ります。

私たちはInnovatorです。
新しい技術、働き方で、スピーディに、想像の先を実現します。

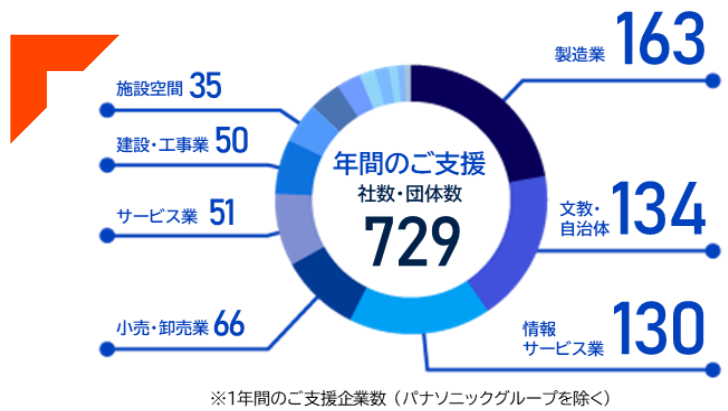
私たちはOne Panasonic ITです。
認め合い、学び合い、高め合って、皆で成長し続けます。

VALUE

- **想像、その先を創造**
  お客さまの夢をかなえるために
  ITの匠集団として、
  想像の先を創造する
- **多様性、信頼、成長**
  多様性を認め合い、
  時にぶつかり、高め合う
- **速く、広く、深く、つなぐ**
  つなぐ価値を最大化
  ビジネスとIT、人や組織、
  人のこころをつなぐ
- **データが語る、語らせる**
  答えのヒントは
  データにある。
  データに語らせる
- **衆知・自律化集団**
  全員参加で衆知を集め、
  変革を常態化
- **主役は、「わたし」**
  変革の主役は「わたし」

一般市場向けビジネス

パナソニックグループでの挑戦を通じ、B2B市場へ価値を提供



※1年間のご支援企業数（パナソニックグループを除く）

データ統合・活用
クラウド連携
システム統合
企業間取引
データ戦略

働き方改革
テレワーク
RPA
勤務管理
クラウドストレージ

施設空間
チケッティング
POS
会員管理
データ分析

基幹業務
製造業務
販売業務
CRM
文書管理

製造現場支援
製造IoT
映像監視
フィールド業務支援
業務モバイルアプリ

文教・自治体
PC教室管理
BYOD
教員用端末
教務支援

会社概要

会社名	パナソニックインフォメーションシステムズ株式会社
本社所在地	大阪　〒530-0013 大阪府大阪市北区茶屋町19番19号 TEL：06-6906-2801（代表） 東京　〒104-0061 東京都中央区銀座8丁目21番1号 TEL：03-5148-5634（代表）
設立年月日	1999年2月22日
事業内容	情報サービス
資本金	1,040百万円
主要取引銀行	三井住友銀行 大阪本店営業部 三井住友信託銀行 大阪本店営業部
許認可など	特定建設業 電気通信工事業　（特-3）第157588号 一般建設業電気工事業　（般-3）第157588号 届出電気通信業者　E-63-00084
関係会社	親会社　パナソニックホールディングス株式会社 連結子会社　パナソニック ネットソリューションズ株式会社 松下信息系統（上海）有限公司

国内 35 拠点、海外 9 拠点

海外地区別
アメリカ / ドイツ / 北京 / 上海
タイ［コンケン］/ シンガポール
マレーシア / ベトナム / インド

セキュリティ製品についてもっと詳しく知りたい方へ

お気軽にお問い合わせください

お問い合わせ