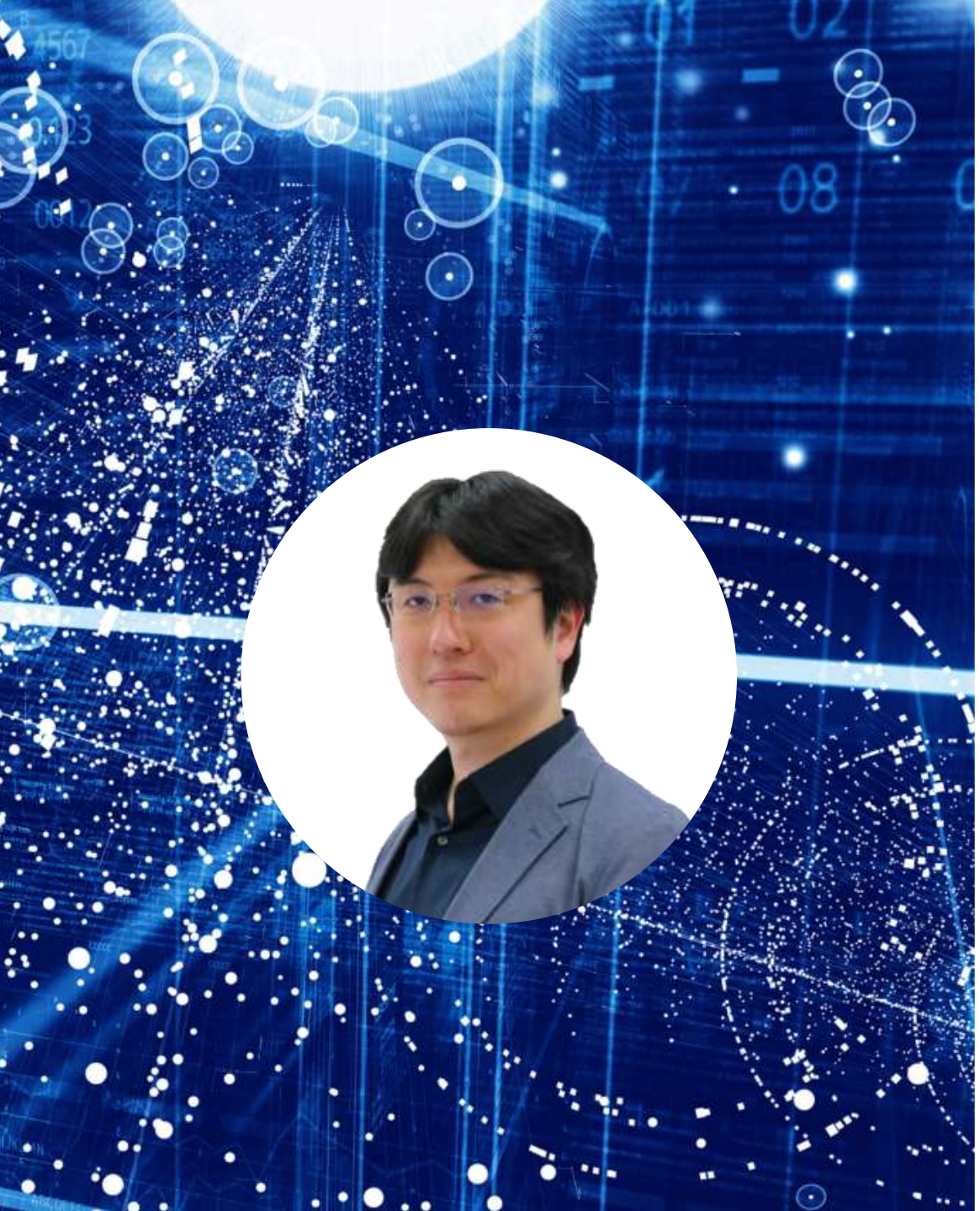
サイバー攻撃に備える！

地域医療を守るための セキュリティ対策 強化セミナー

主催：パナソニック インフォメーションシステムズ株式会社
共催：株式会社ITガード

医療機関におけるセキュリティ対策のトレンドと製品の選定ポイント

パナソニック インフォメーションシステムズ株式会社



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）

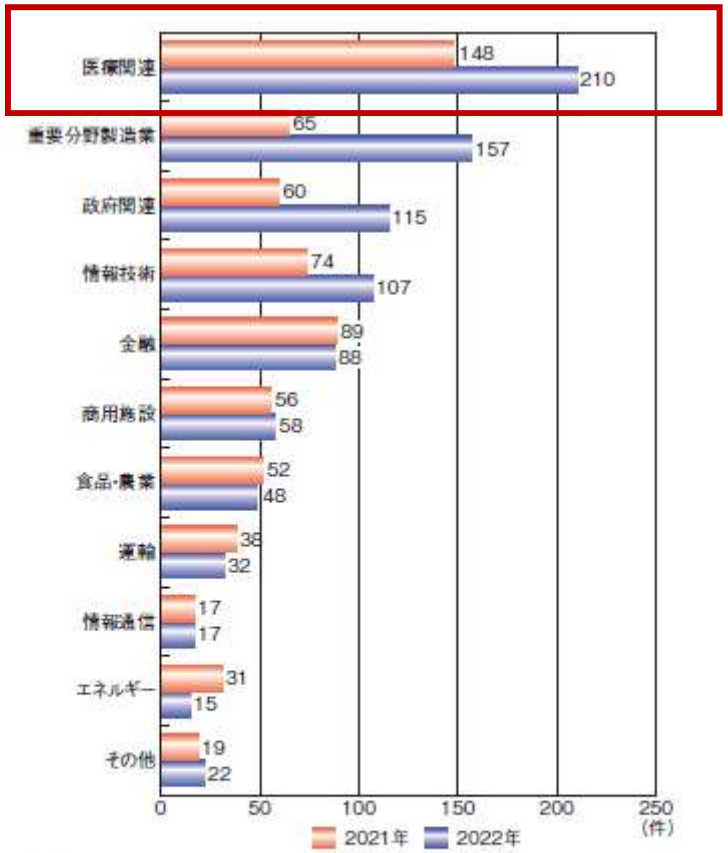
パナソニック インフォメーションシステムズ Panasonic

Chapter - 1

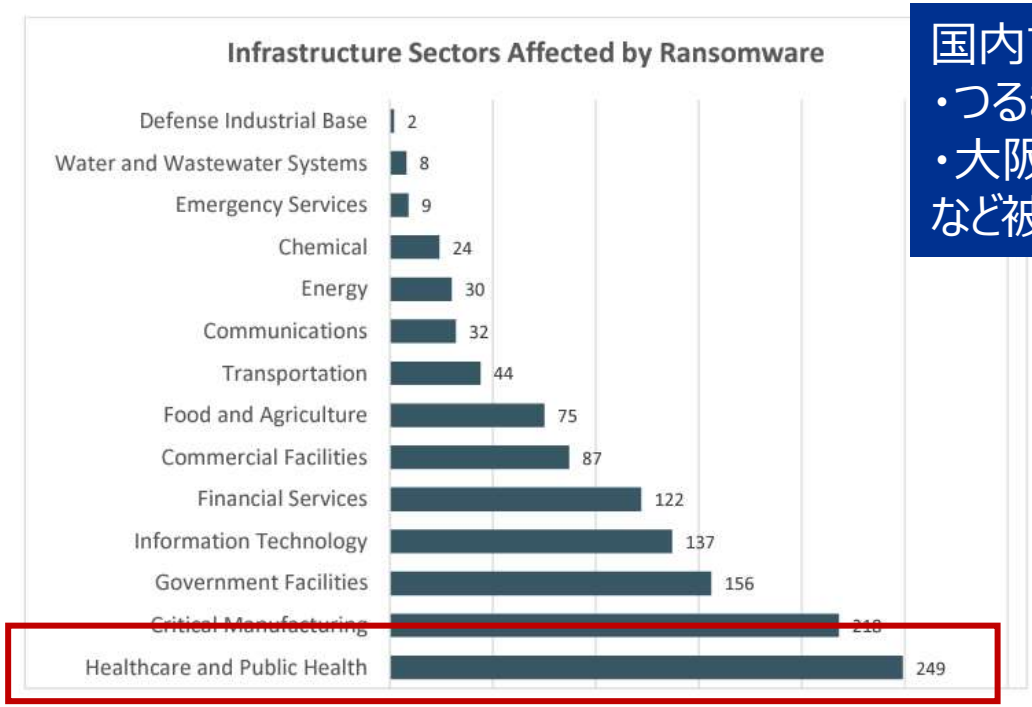
医療機関における セキュリティ対策のトレンド

後を絶たない医療機関におけるランサムウェア被害

医療関連業界を対象とするランサムウェア被害報告は年々増加



■図 1-1-7　攻撃対象となった業界ごとの被害報告件数（上位10業種、2021 年と 2022 年の比較）
（出典）FBI「Internet Crime Report 2021 ※10-1」「Internet Crime Report 2022」を基に IPA が編集



[9] Accessibility description: Chart shows Infrastructure Sectors Affected by Ransomware. Healthcare and Public Health was highest with 249; followed by Critical Manufacturing 218; Government Facilities 156; Information Technology 137; Financial Services 122; Commercial Facilities 87; Food and Agriculture 75; Transportation 44; Communications 32; Energy 30; Chemical 24; Emergency Services 9; Water and Wastewater Systems 8; Defense Industrial Base 2.

国内でも
・つるぎ町立半田病院
・大阪急性期総合医療センター
など被害が多数確認

【引用元】情報セキュリティ白書2023(IPA)
2023 INTERNET CRIME REPORT(FBI)

Panasonic

なぜ医療機関が狙われるのか

① ITインフラの更改が難しい

古いシステムやセキュリティ対策の不足など、ITインフラやセキュリティに関する投資が限定的となり脆弱性を抱えたままとなりがちである

② 重要な個人情報を保有している

個人情報や医療記録など、機微なデータを保有しており、患者のプライバシーを保護するためデータの機密性・完全性が優先される

③ 医療機関における事業継続性の重要性

医療行為の停止は患者の健康や生命に直結するため、事業継続計画（BCP）の事前の立案・有事の発動による早急な復旧が急務となる

医療システムの停止は「災害時」と同等の対応が必要

ランサムウェア被害を
受けたA病院関係者

これはもう**災害として対応すべきだろう**という状況でしたので、**災害対策本部の設置と災害対策会議を開く準備**、そして、大学病院や中央病院の処方、検査内容等が見られる徳島県の医療情報ネットワークのウイルス感染を心配し、事務局への連絡も指示しました。また、警察への通報も行い、**災害時に対応する紙カルテの運用も開始**しました。

当院は基幹災害拠点病院ということで、さまざまな緊急対応をしていますが、今回のことも**非常事態ということですぐに幹部を招集**しました。会議では、状況的にトップダウンではなく、自発的に対応しなければという内容の話をしました。朝8時頃に異変に気づき、9時前には、**災害対策本部会議を開始**。その後、12時に**対策本部を設置**しました。

ランサムウェア被害を
受けたB病院関係者

【引用元】医療機関向けセキュリティ支援サイト「病院で発生した深刻なサイバー攻撃、当事者が被害と対策の全容を語る」（厚生労働省）

Panasonic

医療情報システムの安全管理に関するガイドライン 第6.0版

「医療情報システムの安全管理に関するガイドライン」とは・・・

医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号。以下「e-文書法」という。）等の法令等への適切な対応を目指し策定

主な改定履歴

2005年3月　初版制定

2007年3月　第2版
ネットワーク基盤の安全性、**災害・サイバー攻撃への対応**など

2008年3月　第3版
責任分界点のありかた、無線・モバイル利用時の考慮点

2013年10月　第4.2版
調剤済み処方箋及び調剤録等の外部保存
大規模災害への対応

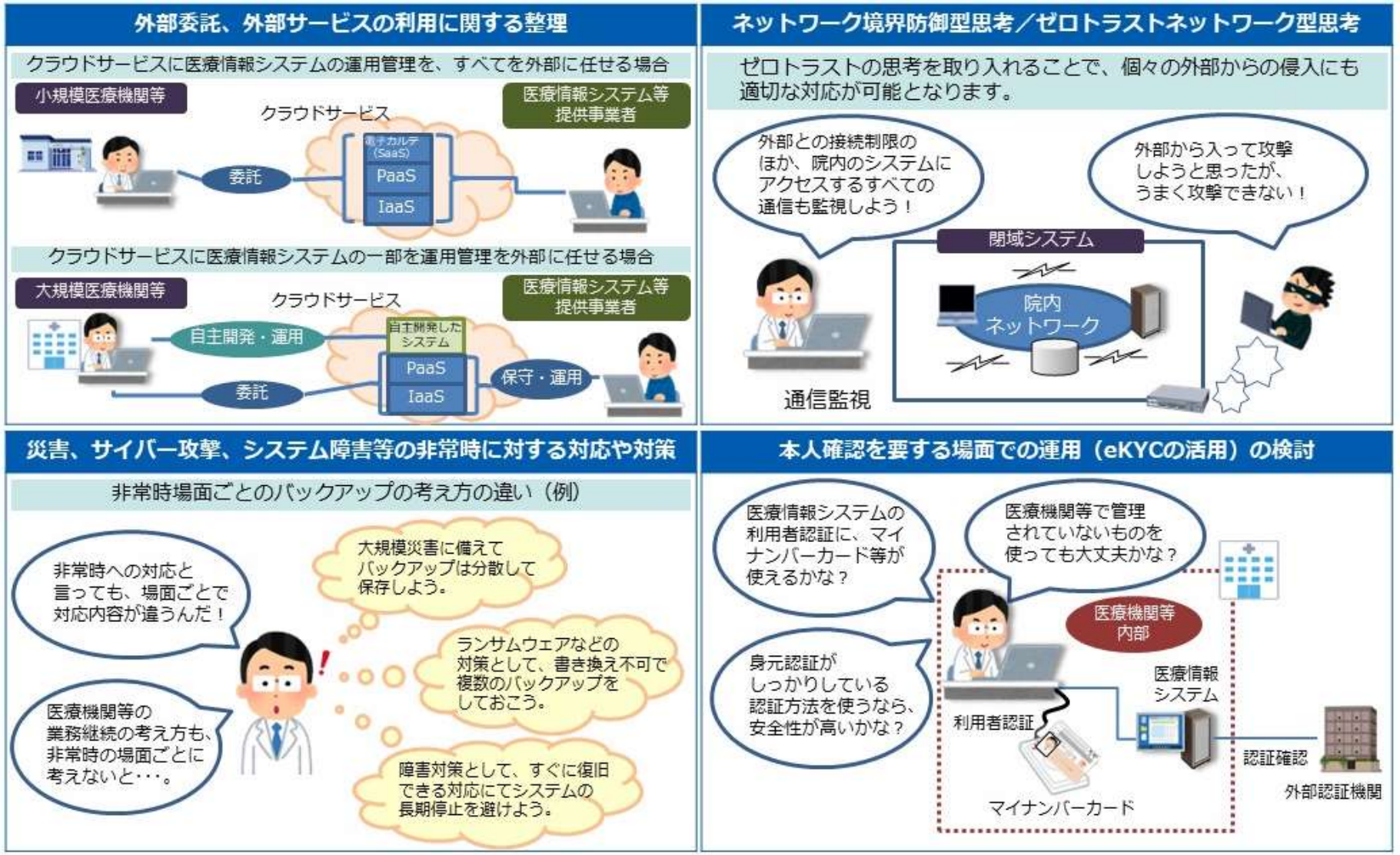
2017年5月　第5版
改正個人情報保護法への対応、**新たなセキュリティリスク**への対応（二要素認証、公衆無線LAN、BYOD等）

2022年3月　5.2版
ランサムウェア等攻撃への対策

2023年5月　第6.0版

Panasonic

第6.0版における改定のポイント



【引用元】医療情報システムの安全管理に関するガイドライン 第6.0版主な改定ポイント（概要）（厚生労働省）

Panasonic

概説編・経営管理編・企画管理編・システム運用編の4編で構成

経営層

安全管理者

運用担当者

①概説編

各編に共通する前提となる内容

②経営管理編

医療機関等における
医療情報システムの
安全管理の統制

③企画管理編

医療機関等全体の
医療情報システムの
安全対策の管理

組織的な対応に関する対策

④システム運用編

技術的な対応に関する対策

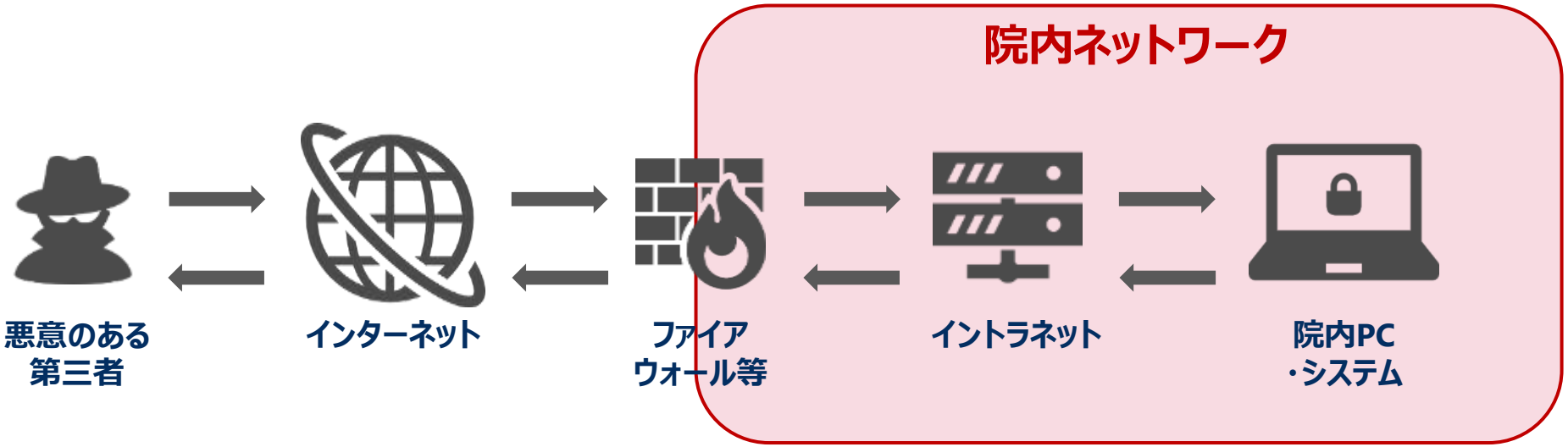
システム運用の形態に応じガイドライン上で参照すべき範囲を明記

	医療情報システムを 医療機関等に保有し運用 （いわゆる オンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆる クラウドサービス型）
システム運用専任の 担当者が いる	I	II
システム運用専任の 担当者が いない	III	IV

	経営管理編	企画管理編	システム運用編
I･III	すべて参照	すべて参照	すべて参照
II･IV	すべて参照	基本的にすべて参照 ※クラウド事業者との契約内容を確認	一部項目を参照 ※他はクラウド事業者との契約内容を確認

「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。



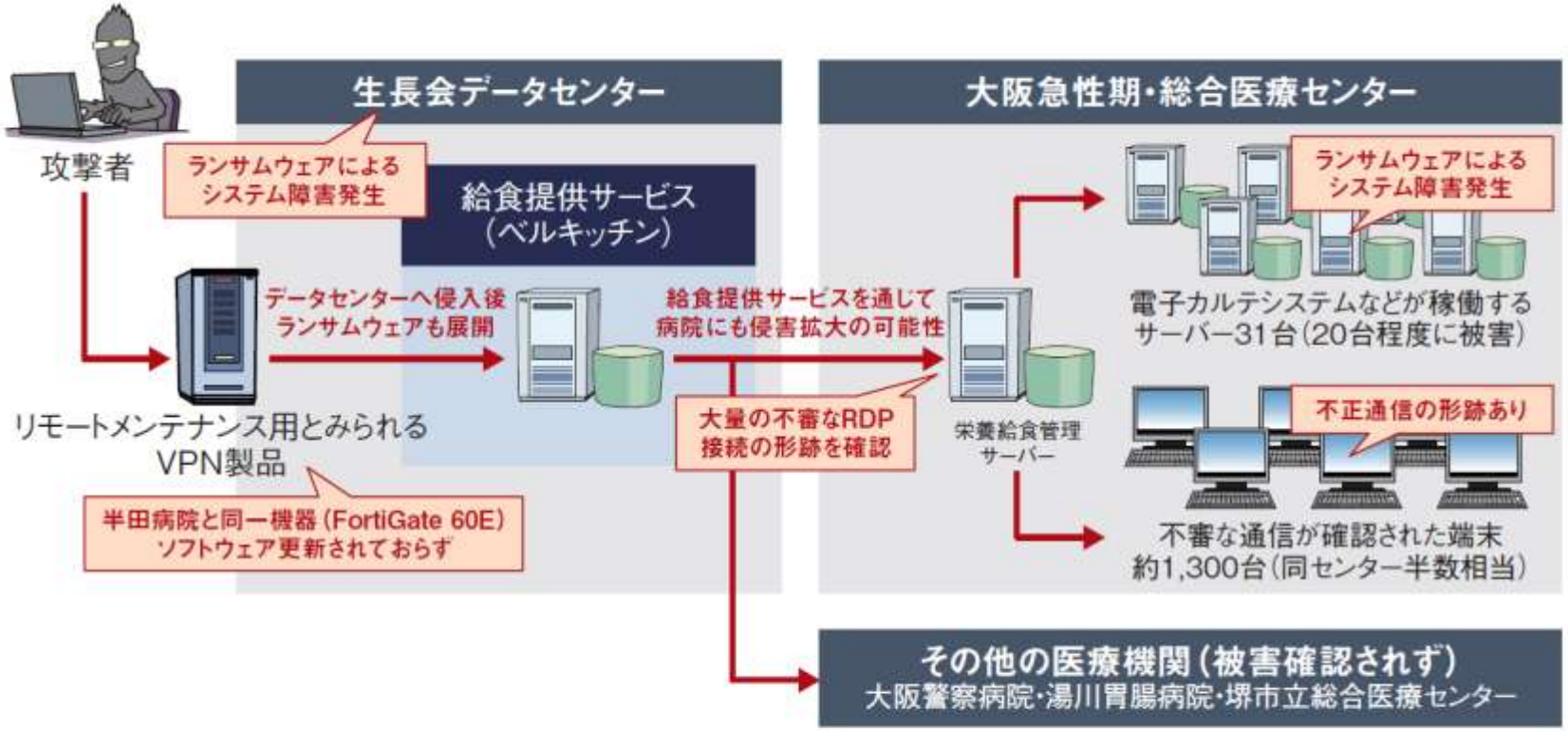
境界型セキュリティ思考

院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

たとえ院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

ゼロトラスト・ネットワークは医療を守るために必要に



■図 1-2-2　大阪急性期・総合医療センターが受けたと見られる攻撃の流れ
(出典)piyolog「ランサムウエア起因による大阪急性期・総合医療センターのシステム障害についてまとめてみた※30」を基に IPA が編集

関係する事業者すべてのセキュリティを担保するのは困難
→医療を守るためにも**ゼロトラスト・ネットワークの考え方が重要**に

【引用元】情報セキュリティ白書2023（IPA）

Panasonic

非常時に備えたBCP策定にも、事象に応じた想定が必要

例：非常時に備えたバックアップの考え方

災害	システム障害	サイバー攻撃
大規模広域災害等に備えた、遠隔保管を含めたバックアップ整備（3-2-1バックアップ等）	データやシステムのバックアップ確保、定期的なリストア訓練	バックアップデータの安全性確保（システム構成による分離、書き換え不能型バックアップ等）

BCP・・・Business Continuity Plan(事業継続計画)

チェックリスト・啓発ツール類

医療機関等におけるサイバーセキュリティ対策チェックリスト


医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果 (日付)	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は記入不要）		

○ 令和5年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*2（2）及び2（3）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果 (日付)			備考
1 体制確認	（1） 医療情報システム安全管理責任者を設置している。				
	医療情報システム全般について、以下を実施している。				
	（1） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。				
	（2） リモートメンテナンス（保守）を利用している機器の接続元				

ガイドラインの中でも
まずは**医療機関が**
優先的に取り組むべき
事項のチェックリスト

医療機関に対するサイバーセキュリティ対策リーフレット

医療機関において早急に
取り組むべきセキュリティ対策等に
ついての**意識啓発リーフレット**

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
https://www.mhlw.go.jp/content/10808000/001180153.pdf

Panasonic

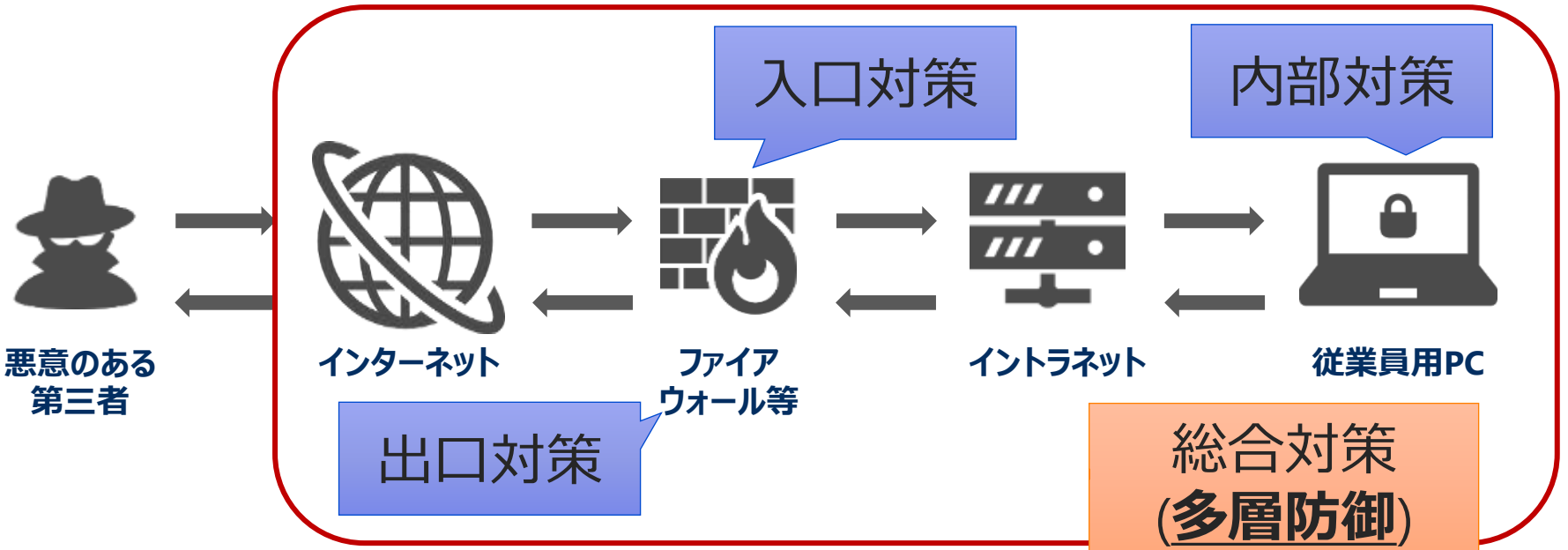
パナソニック インフォメーションシステムズ Panasonic

Chapter - 2

医療機関における セキュリティ対策のポイント

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)

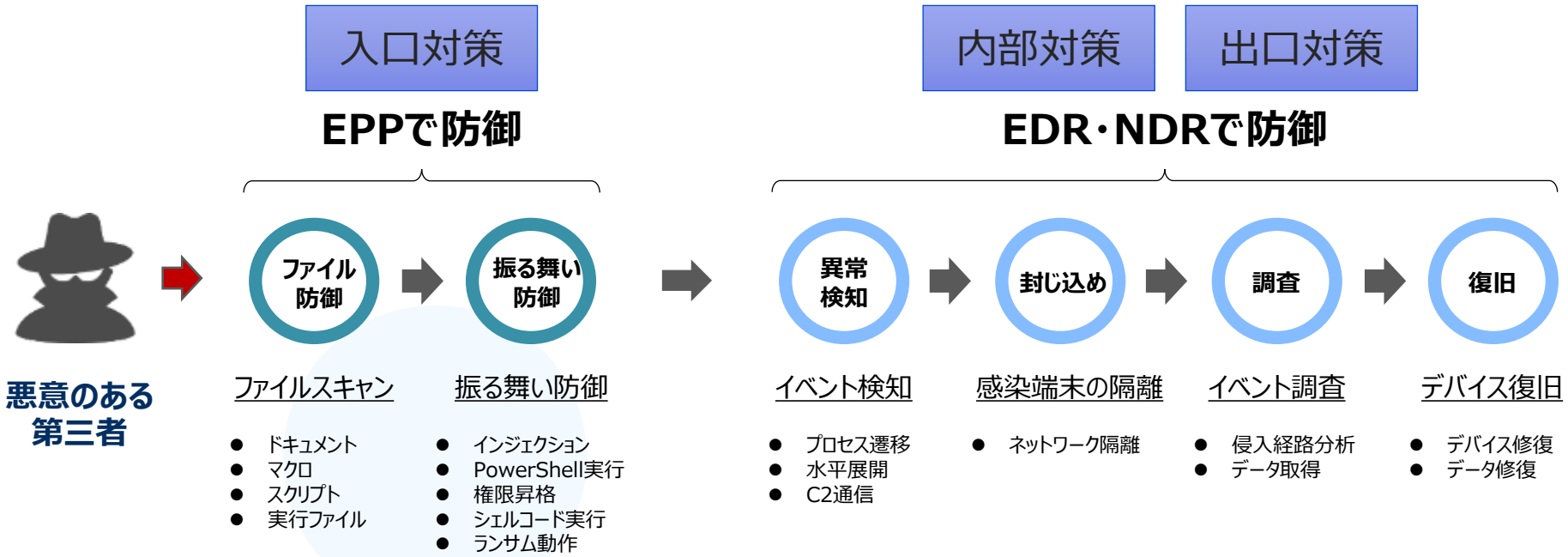
攻撃の巧妙化・PCの性能向上により被害範囲が拡大

→**「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）

本セッションのまとめ

- 医療機関を狙ったマルウェア被害は年々増加
- 医療情報システムの安全管理ガイドラインを適切に参照し
  ゼロトラスト・ネットワークも視野に入れたセキュリティ強化が急務
- セキュリティ技術の進化とともに製品トレンドも変遷。
  全方位でセキュリティを守る「多層防御」の考え方が主流に
- リソースが限られる中でのセキュリティの強化にあたっては
  「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

Blue Planet-works
Safety for the Connected World

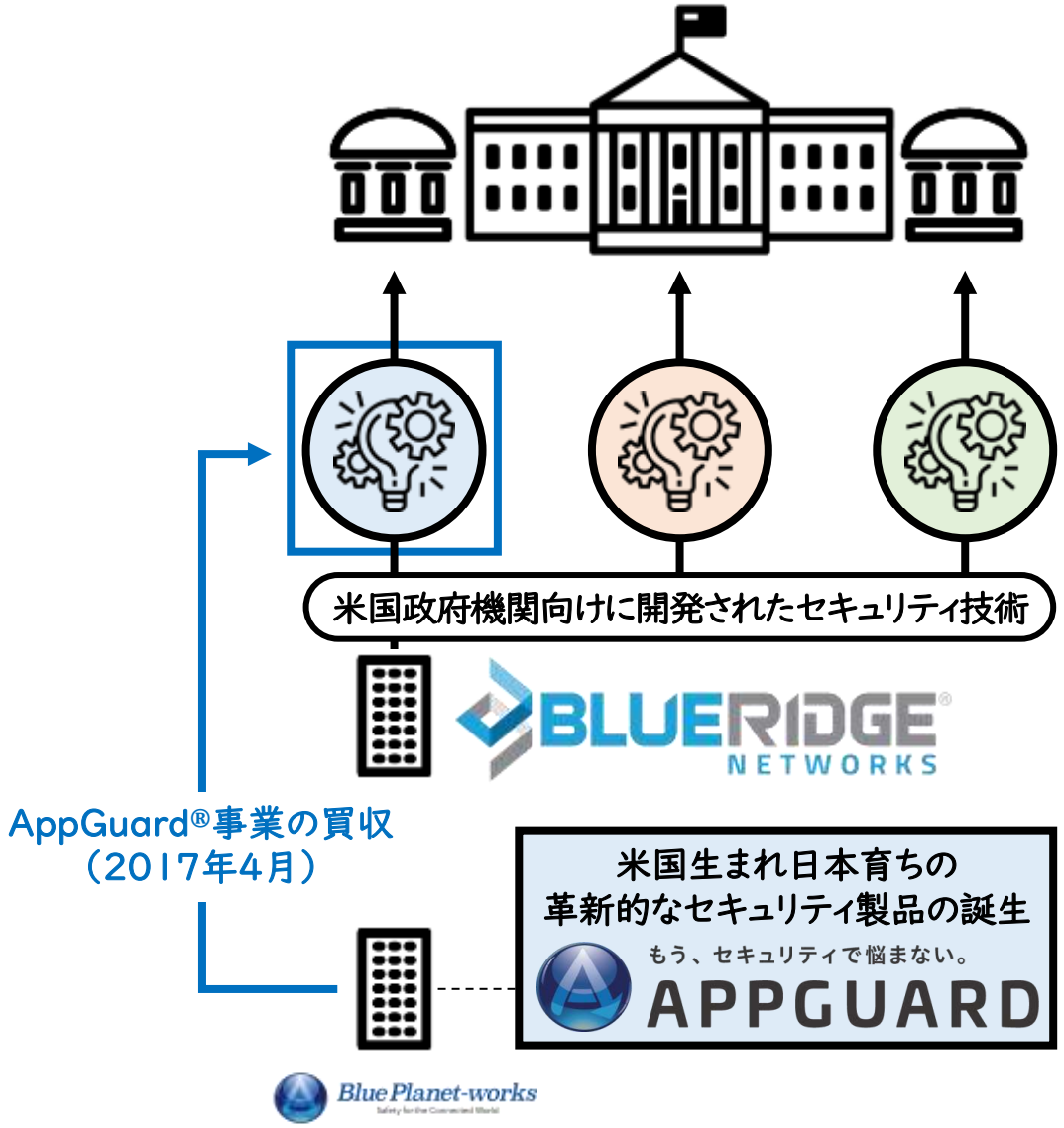
Session – 2

革新的技術で医療機関を守る
ゼロトラスト型エンドポイントセキュリティ
AppGuard ご紹介

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



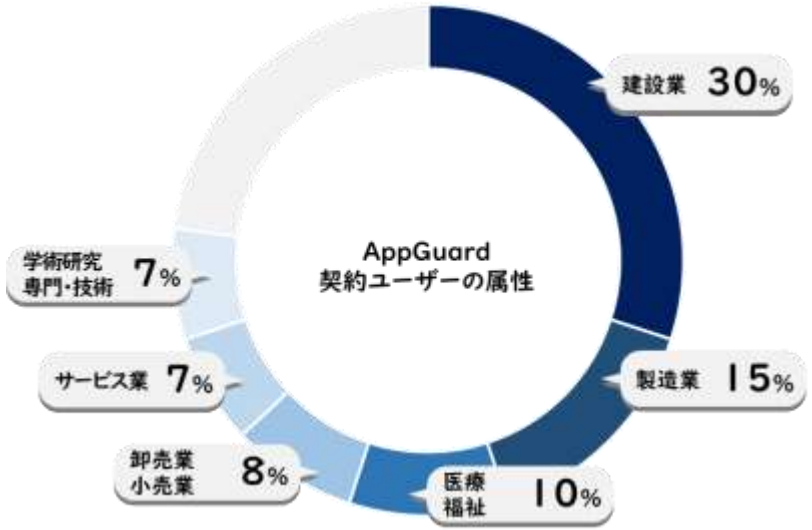
株式会社ITガードについて

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

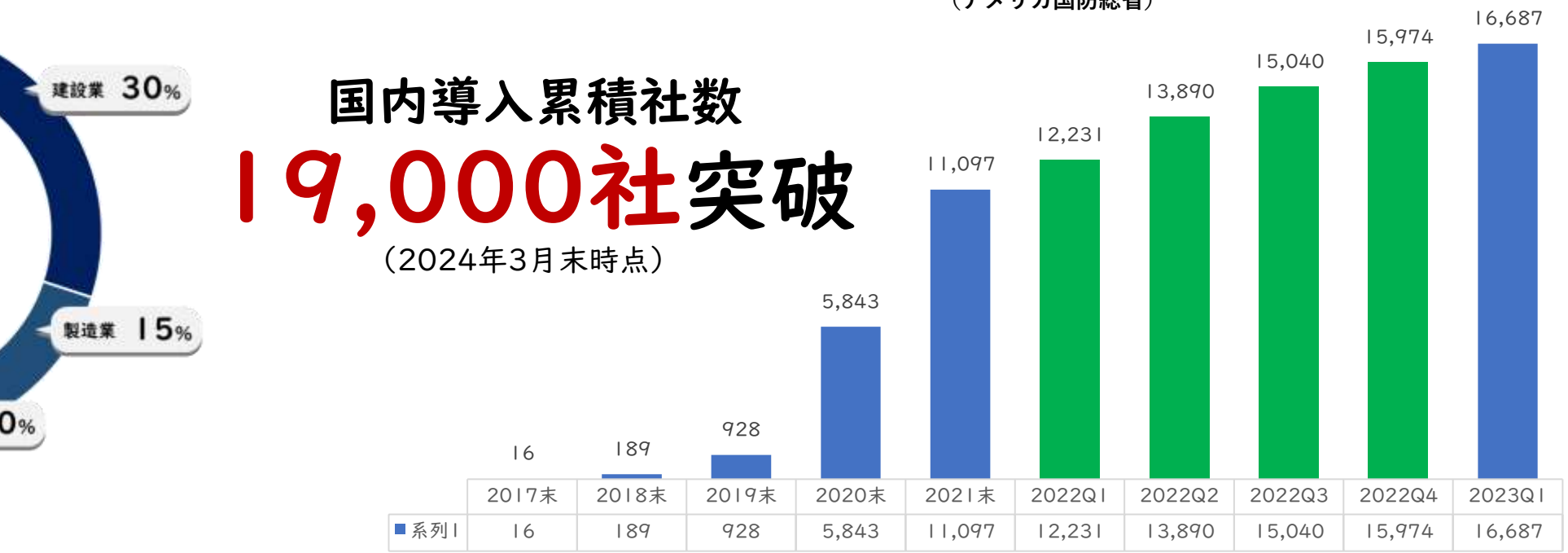
AppGuardビジネスの堅調な推移（AppGuard採用企業実績）

Blue Planet-works
Safety for the Connected World

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 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

Blue Planet-works
Safety for the Connected World

過去の情報に依存

機械学習解析

振る舞い解析

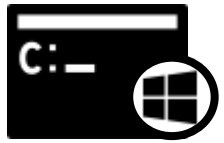
過去の脅威情報から特徴を抽出

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

Blue Planet-works
Safety for the Connected World

	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

Blue Planet-works
Safety for the Connected World

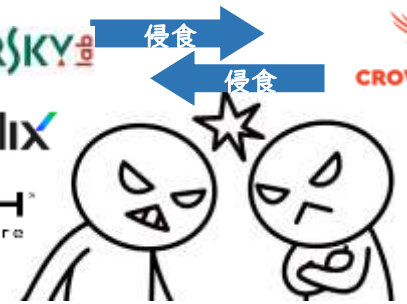
UTM・アンチウイルス | EDR/XDR

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）→

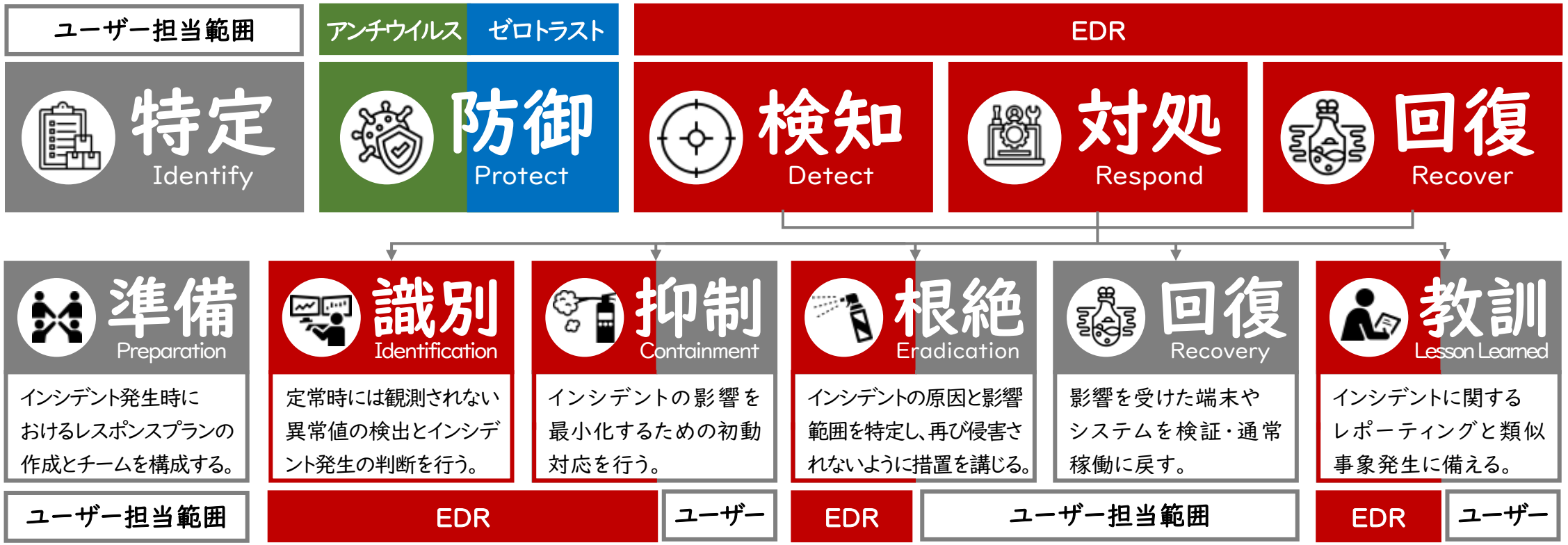
←これまで投資してこなかった領域（事後対策）→

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

Blue Planet-works
Safety for the Connected World

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

Kojima

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

JPCERT CC

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

医療機関へのサイバー攻撃被害

Blue Planet-works
Safety for the Connected World

ランサムウェア感染	ランサムウェア感染	不正アクセス	Emotet感染	Emotet感染	ランサムウェア感染	Emotet感染
つるぎ町立半田病院	春日井リハビリテーション病院	名古屋大学医学部附属病院	那須南病院	東京都済生会向島病院	医療法人ラポール会青山病院	秋田赤十字病院
2021年10月	2022年01月	2022年02月	2022年03月	2022年03月	2022年04月	2022年05月
2023年9月	2023年7月	2023年1月	2022年10月	2022年10月	2022年07月	2022年06月
ランサムウェア感染	ランサムウェア感染	ランサムウェア感染	ランサムウェア感染	ランサムウェア感染	不正アクセス	ランサムウェア感染
京都(某病院)	福岡徳洲会病院	宇治病院	大阪急性期・総合医療センター	田沢病院	安江病院	鳴門山上病院

「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

Blue Planet-works
Safety for the Connected World

UTM・アンチウイルス

EDR・XDR

←――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）

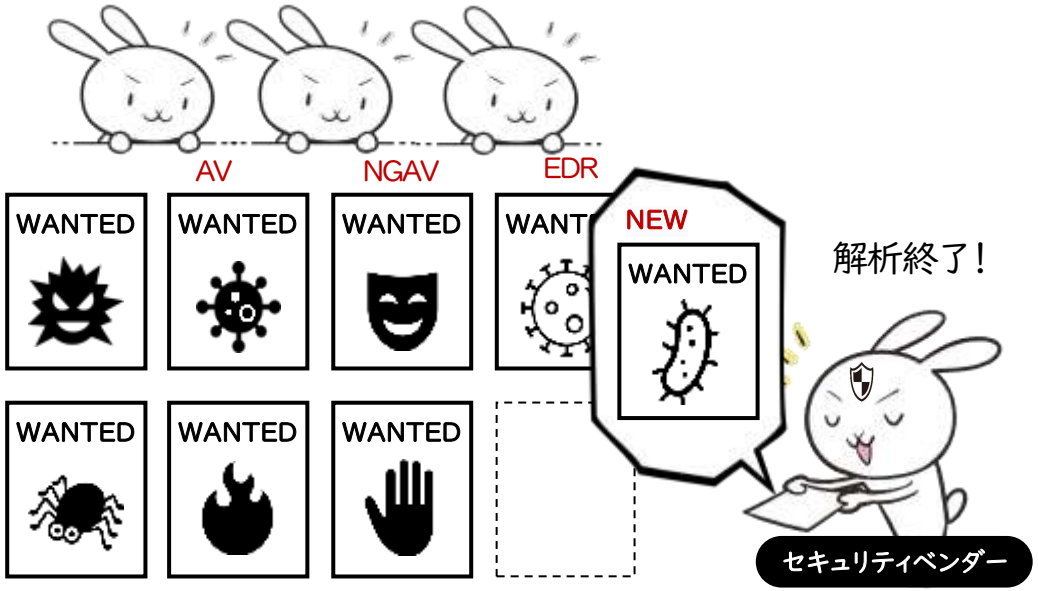
すり抜ける脅威を阻止 ⟷ そもそも攻撃が成立しない

求められる新しい守り方

Blue Planet-works
Safety for the Connected World

これまでの守り方

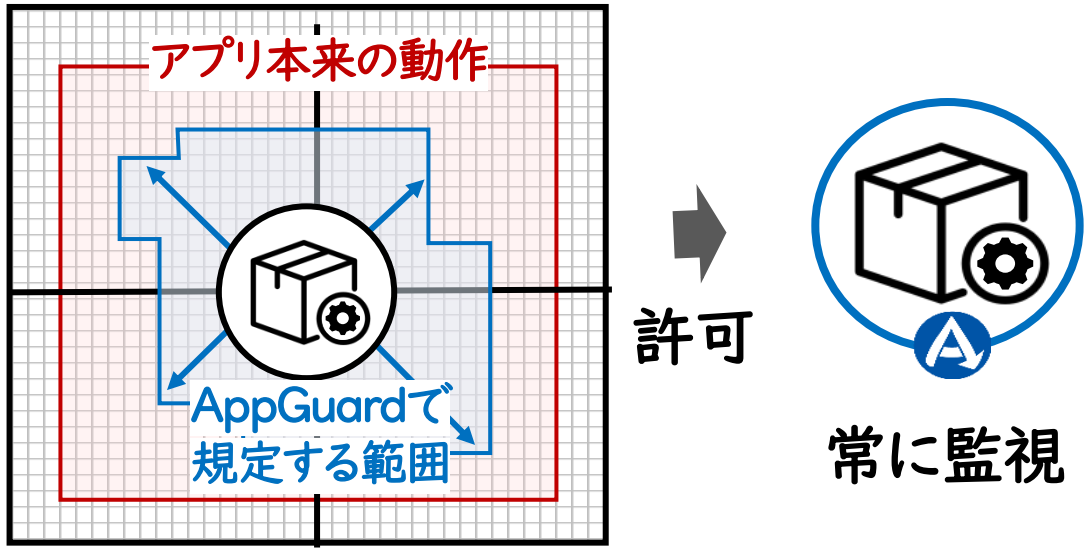
悪いものを見つけて排除



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

Blue Planet-works
Safety for the Connected World

~~悪意があるかの判断~~

~~マルウェアの検知~~

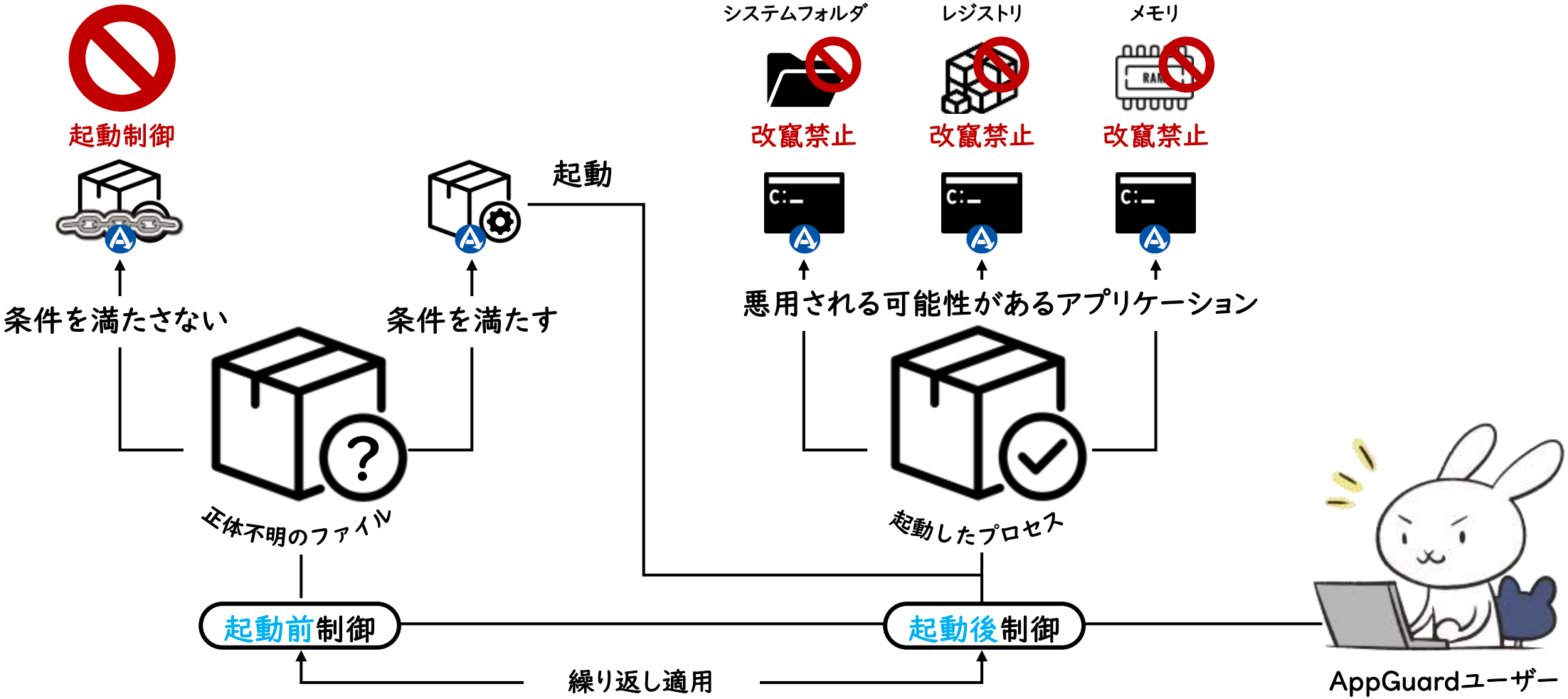
~~マルウェアの駆除~~

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

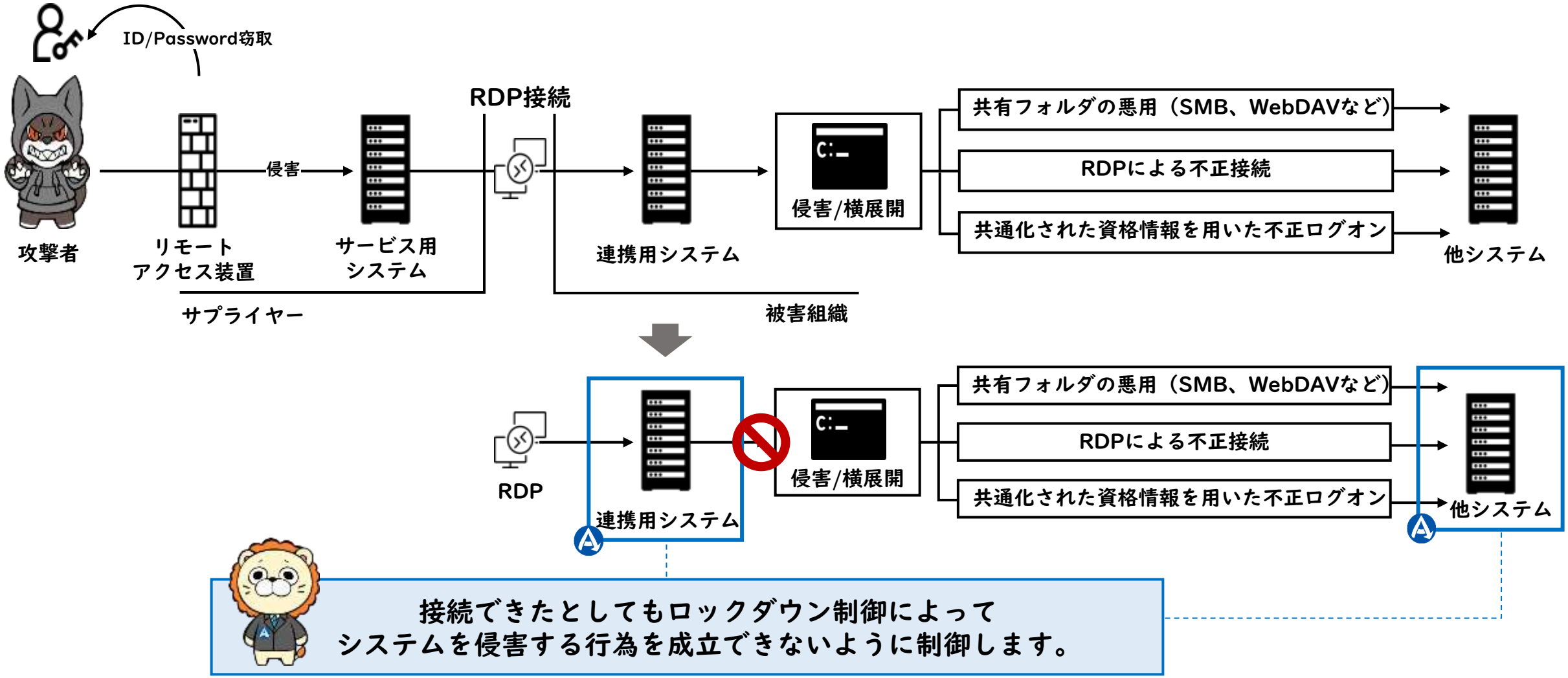
AppGuardが攻撃プロセスの成立を阻止

「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

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）



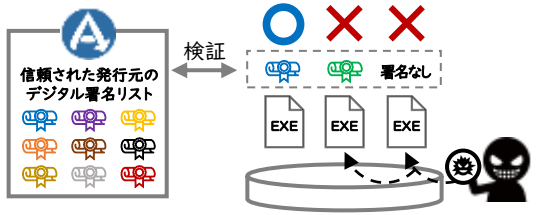
出典：「大阪急性期・総合医療センター」及び「社会医療法人生長会」の侵害事案について当該組織又はメディア等で報道された内容を基に構成

AppGuardのラインナップ

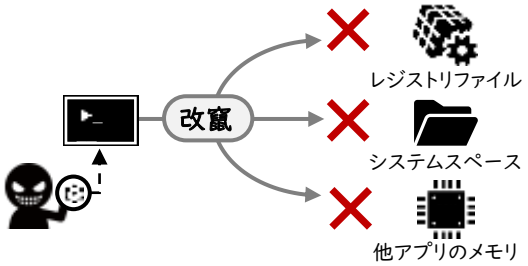
Blue Planet-works
Safety for the Connected World

ゼロトラスト型 エンドポイントセキュリティ

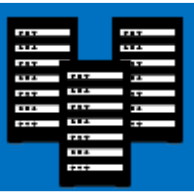
信頼された アプリケーションしか 起動させない



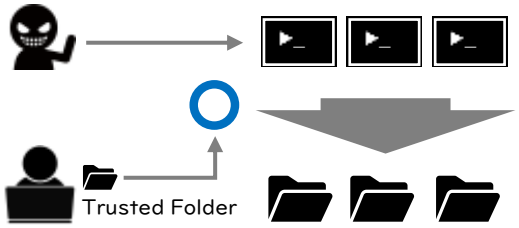
不正アクセスにおける 侵攻プロセスを 成立させない



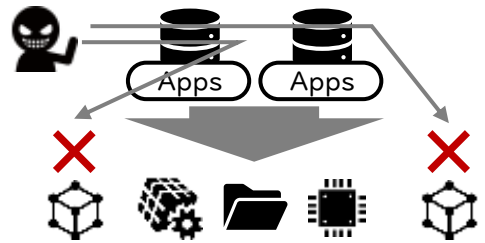
ロックダウン型 サーバーセキュリティ



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



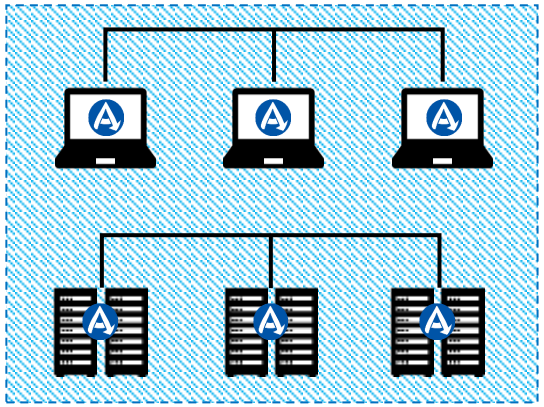
AppGuard Enterprise/SBE/Solo

AppGuard Server

部分導入が可能

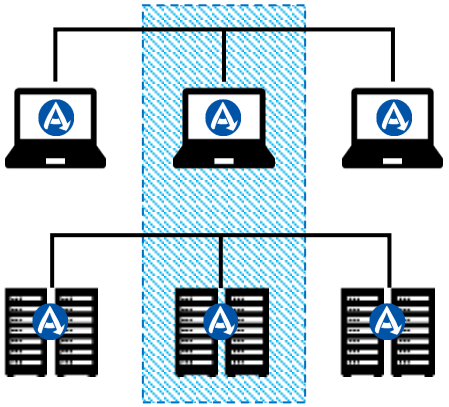
Blue Planet-works
Safety for the Connected World

全体に導入



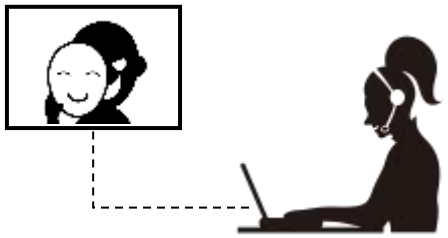
OR

部分的に導入

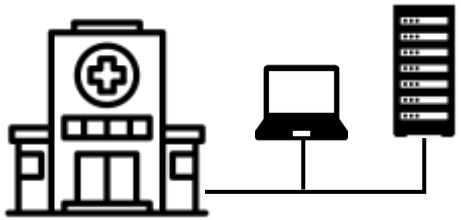


機密情報を扱う部署

業務上リスクが高いユーザー



閉域環境の特殊端末



レガシーな端末

死守したい端末

医療業界でのAppGuard導入事例

AppGuard病院導入事例

Blue Planet-works
Safety for the Connected World

一般財団法人津山慈風会
津山中央病院
Tsuyama Chuo Hospital

515床

社会医療法人財団 慈泉会
相澤病院

460床

名寄市立総合病院
Nayoro City General Hospital

359床

特定医療法人 佐藤会
弓削病院

108床

埼玉医科大学病院
Saitama Medical University Hospital

970床

1053床

700床

埼玉医科大学様におけるAppGuardの決め手

＜要件を満たす製品が「AppGuard」以外に存在しなかった＞

要件

過去のサイバー攻撃事例を想定した効果的な予防措置が可能なこと

閉域環境でも保護能力が低下しないこと

導入対象のシステム・端末に負荷を与えないこと

検知型の
製品では難しい

侵入されても攻撃が成立しない新しいアプローチを実現

事前に規定した「やってよい事」以外のイレギュラーな動作を生じさせない仕組み

クラウド上の脅威インテリジェンスや脅威解析基盤が必要ない

定義ファイルの更新を伴わないためインターネット接続を必要としない

ディスク/ファイルスキャン等の負荷の高い動作を行わない

攻撃の検知をしないため、デバイスのパフォーマンスを低下させない

ランチョンセミナーでの事例紹介

Blue Planet-works
Safety for the Connected World

第61回全国自治体病院学会 ランチョンセミナー（2023年9月1日）

ランチョンセミナー15　第8会場（札幌コンベンションセンター　2階　207）

演題	「「医療業界におけるサイバー攻撃の動向とこれからの対策」　“名寄市立総合病院様サイバー攻撃対策事例ご紹介”」
演者	守屋　潔（名寄市立総合病院　情報管理センター長） 昆　貴行（名寄市立総合病院　情報管理センター係長） 奥村　健太（株式会社Blue Planet-worksエバンジェリスト）
座長	邉見　公雄（公益社団法人全国自治体病院協議会名誉会長／一般社団法人全国公私病院連盟会長／特定非営利活動法人地域医療・介護研究会JAPAN会長）
共催	株式会社ITガード

第73回日本病院学会 ランチョンセミナー（2023年9月22日）

LS22　医療業界におけるサイバー攻撃の動向とこれからの対策

“相澤病院様、埼玉医科大学様の事例ご紹介”

座長　堺 常雄（一般社団法人 日本病院会 名誉会長、株式会社日本病院共済会 代表取締役）

演者　鴫原 祐輔（株式会社Blue Planet-works 上席セキュリティアドバイザー）
「 ゼロトラスト型エンドポイントセキュリティAppGuardの紹介」
米山 弘（社会医療法人財団 慈泉会 相澤病院 慈泉会本部 情報システム部 部長）
「医療業界のセキュリティ課題からAppGuard導入選択に至る事例紹介」
佐藤 巨樹（学校法人 埼玉医科大学 国際センター 情報システム部 課長）
「 AppGuard導入から運用に至る事例紹介」

日本病院会・共済会推奨

Blue Planet-works
Safety for the Connected World

日本病院会プラザ　推奨（2023年7月）

日本病院共済会
NEWS
VOL.165
2023. 7

発行：株式会社日本病院共済会
年4回発行
発行人：甲　英雄
〒102-0075 東京都千代田区三番町 9-15
ホスピタルプラザビル 1F
TEL. 03-3264-8888

取締役交代のおしらせ

2023年5月26日に開催した弊社第49回定時株主総会におきまして、春原秀臣取締役の退任に伴い、新たに取締役を選任し、就任しました。

今後は、この新陳代謝をもちまして社業の発展に邁進する所存でございますので、何卒一層のご指導ご支援を賜りますようお願い申し上げます。

新任取締役

公益財団法人 日本原生会 会長
玉井病院 名誉院長
中嶋 昭

この度、株式会社日本病院共済会の取締役を仰せつかりました。公益財団法人日本原生会玉井病院の中嶋昭でございます。日本病院会には長年に渡って常任理事、理事として参加させていただき、専門医に関する委員会やそのリーキンググループ、日病病院総合医育成事業の各種委員、ニュース編集委員などのお手伝いをさせて頂きました。この間、多大な情報と貴重なご教示を頂き、病院管理者として自信を得、成長することができました。深く感謝いたしております。

新型コロナ感染症による甚大な影響からの脱却や働き方改革・医療DXの推進など日本の病院医療は大きな課題を抱えて今後に臨まなければなりません。そのような立場にある日本病院会会員の先生方に、少しでもお役に立てるよう尽力いたす所存です。どうぞよろしくお願いいたします。

●役員一覧

代表取締役	堺　宗雄	取締役	新寺 保夫				
取締役	高永 由利	取締役	佐合 茂樹	取締役	齋藤　清		
取締役	中嶋　昭	監査役	梶原　優	監査役	境野 美雄		
常任顧問	山本 修三	顧問	黒川 政義				

侵入されても発症しない
新しいサイバー攻撃対策のご案内
アンチウイルスでもEDRでもないゼロトラスト型エンドポイントセキュリティ

APPGUARD

アメリカ国防総省が採用

「AppGuard（アップガード）」は、米国国防総省（俗称：ペンタゴン）を含む、複数の米国政府機関で導入実績のあるセキュリティ技術です。2017年に「株式会社Blue Planet-works（ブループラネットワークス）」がその特許技術、知財を含むAppGuard事業を買収しました。その後、開発と改善を行い、2018年より民間向けのエンドポイントセキュリティ対策ツール「AppGuard」として販売を開始しました。

Blue Planet-worksの株主でもあるANAやJTBといった日本を代表する企業を始め、国内で17,000社超の導入実績（2023年6月時点）を有しています。医療機関においても埼玉医科大学や引頭病院等、50以上の医療機関で採用されています。詳細は2P～3Pおよび別冊のパンフレットをご覧ください。

（US Patent #7712143）を用い
ン）を含む、複数の米国政府機
ェアが米国陸軍の定めるセキュ
国内でもANAやJTBといった
6月時点で17,000社以上に導入さ
できることを紹介します。

を講じられること
がる行為を一切成立させない環境と
ースを想定した検証において、攻撃

プロセスを制御するため、インター
利用はなく、閉域環境であっても強

せることができること

といった端末やサーバーのパフォー
ンポイントで対象イベントに制御を
部エンジンも1MB以下と軽量化が

なセキュリティ対策に加え、振る
しい手法を使ったサイバー攻撃や
まとっていました。いつまでも
ごに導入を決定。防御力が高ま
ことで、導入前に比べてランニン

ュリティリスクを洗い出し、日々
います。

担当：熊谷（くまがい）
時まで　※年末年始を除く）

1　2　3

資本業務提携（2024年4月）

日本病院共済会
NEWS
VOL.168
2024.4

発行：株式会社日本病院共済会
年4回発行
発行人：甲　英雄
〒102-0075 東京都千代田区三番町 9-15
ホスピタルプラザビル 1F
TEL. 03-3264-8888

サイバーセキュリティ製品「AppGuard」開発会社 株式会社 Blue Planet-works との資本提携のお知らせ

株式会社日本病院共済会（以下：当社）は、2024年1月にサイバーセキュリティ製品「AppGuard」の開発会社、株式会社 Blue Planet-works（本社：東京都品川区大崎 4-1-2 ウィン第2五反田ビル3F、代表取締役社長：坂尻浩孝、以下：BPw社）と資本提携を行いました。

近年、病院を標的としたサイバー攻撃は増加の一途をたどり、攻撃手法は巧妙化が進んでいます。ランサムウェアの被害により診療を長期間停止せざるを得ない事態も起こっているため、より一層強固なセキュリティ対策が求められています。一方、アンチウイルスソフトやEDRでは防ぎきれない攻撃、セキュリティ対策の業務負荷の増大などの課題が顕在化してきました。

「AppGuard」は、ランサムウェア等のマルウェアが侵入しても発症させず、業務負荷も軽減できるサイバーセキュリティ製品です。当社は、日本病院会会員病院をサイバー攻撃から守る最適な製品だと判断し、2023年6月、当社、BPw社および株式会社ITガード（BPw社100%子会社）の三者間で業務提携を行いました。

本資本提携により、さらに強固な関係性を構築し、会員病院のサイバーセキュリティ対策強化に寄与してまいります。

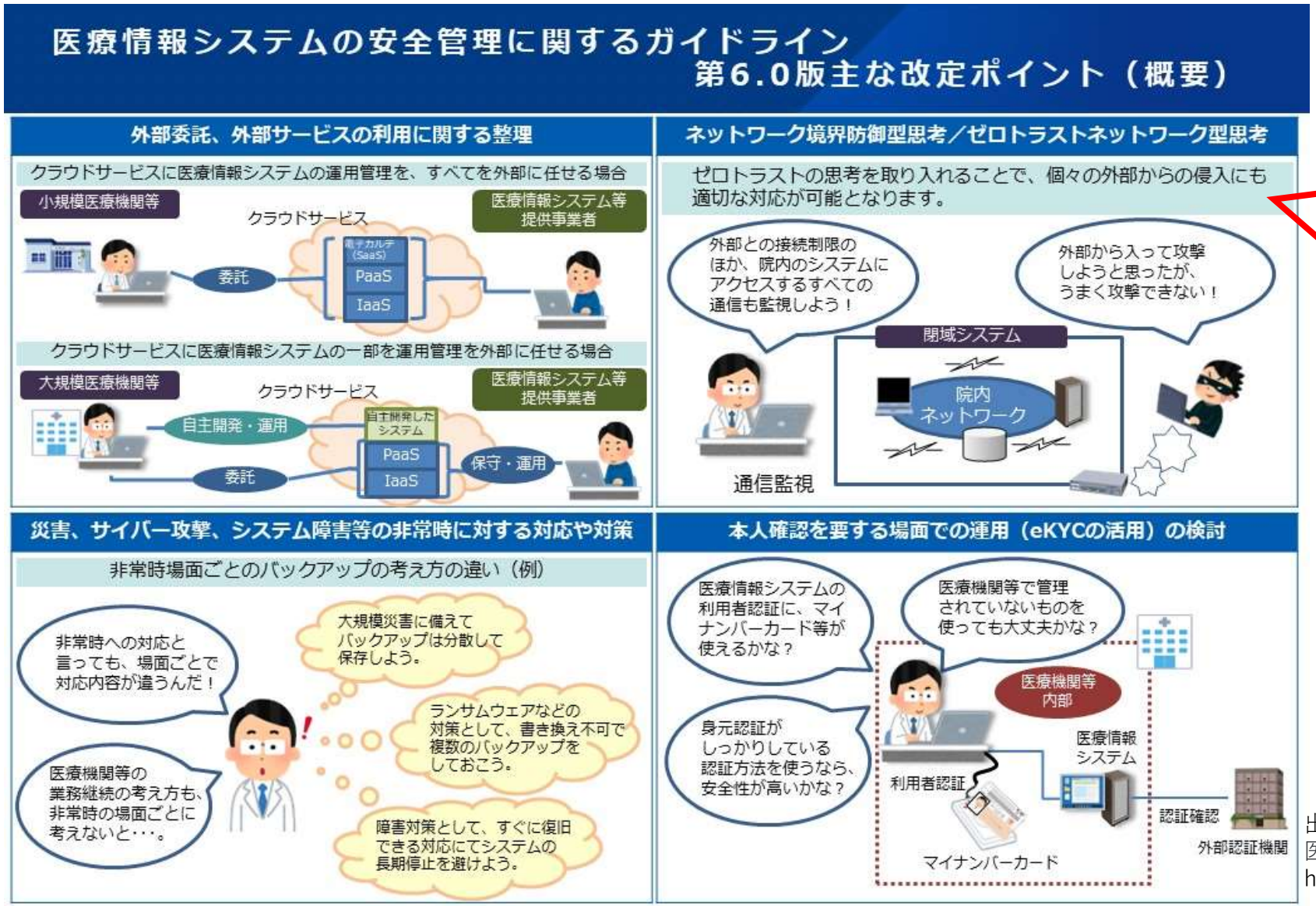
■業務提携および資本提携の主な内容
・AppGuardの日本病院会会員病院向け特別パッケージの設定
・当社および株式会社ITガード（BPw社100%子会社）との会員病院への共同提案
・当社がBPw社による第三者割当増資を引受け

■サイバーセキュリティ製品「AppGuard」について
米国国防総省（俗称：ペンタゴン）を含む米国政府機関で導入実績のあるセキュリティ技術です。この技術は、2000年代にアメリカ国内にて開発がすすめられ2017年にBPw社がその特許技術、知財を含むAppGuard事業を買収しました。その後、日本発の製品として開発と改善を行い、2018年より民間向けのエンドポイントセキュリティ対策ツール「AppGuard」として販売を開始しました。
「AppGuard」は、「ゼロトラスト」の概念を実装したエンドポイントセキュリティ対策ツールです。端末やサーバー上で「やって良いこと・悪いこと」を明確に規定した上で「やって良いこと・信頼できること」だけが継続的に実践されているか検証し続け、イレギュラー（コンピューターウイルス等のマルウェアの発症、不正アクセスの成立）が発生しない環境に作り変えます。
全日本空輸（ANA）など日本を代表する企業を始め、国内で18,000社超の導入実績（2023年12月時点）を有しています。医療機関においても埼玉医科大学、相澤病院、名寄市立総合病院など、約100病院に導入されています。

<本件に関するお問い合わせ先>
株式会社日本病院共済会　営業統括部　熊谷　TEL：03-3264-8888（平日9時～17時）

1

医療情報システムの安全管理に関するガイドライン　第6.0版



侵入されても発症しない

ゼロトラスト型
エンドポイントセキュリティ
AppGuard

出展：厚生労働省
医療情報システムの安全管理に関するガイドライン第6.0版
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

医療機関におけるサイバーセキュリティ対策チェックリスト

Blue Planet-works
Safety for the Connected World

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（1） サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

○ 参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	端末 PC について、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
3 インシデント発生に備えた対応	（2） インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（3） サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

2024年度 診療報酬改定（診療録管理体制加算の見直し）

Blue Planet-works
Safety for the Connected World

診療録管理体制加算の見直し

診療録管理体制加算の見直し

➢ 適切な診療記録の管理を推進する観点から、「医療情報システムの安全管理に関するガイドライン」を踏まえ、非常時に備えたサイバーセキュリティ対策等の整備に係る要件及び評価を見直す。

現行	改定後
【診療録管理体制加算１】　100点 ［施設基準］ ・許可病床数400床以上の保険医療機関については、専任の医療情報システム安全管理責任者を配置すること。	【診療録管理体制加算１】　140点 ［施設基準］ ・許可病床数200床以上の保険医療機関については、専任の医療情報システム安全管理責任者を配置すること。
（新設）	・非常時に備えた医療情報システムのバックアップを複数の方式で確保し、その一部はネットワークから切り離したオフラインで保管していること。
（新設）	・非常時を想定した医療情報システムの利用が困難な場合の対応や復旧に至るまでの対応についての業務継続計画（ＢＣＰ）を策定し、少なくとも年１回程度、定期的に訓練・演習を実施すること。また、その結果を踏まえ、必要に応じて改善に向けた対応を行っていること。
【診療録管理体制加算２】　30点 ・区分の見直し（診療録管理体制加算１→２）	【診療録管理体制加算２】　100点 ・許可病床数200床以上の保険医療機関については、専任の医療情報システム安全管理責任者を配置すること。
（新設） ・区分の見直し（診療録管理体制加算２→３）	【診療録管理体制加算３】　30点

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。

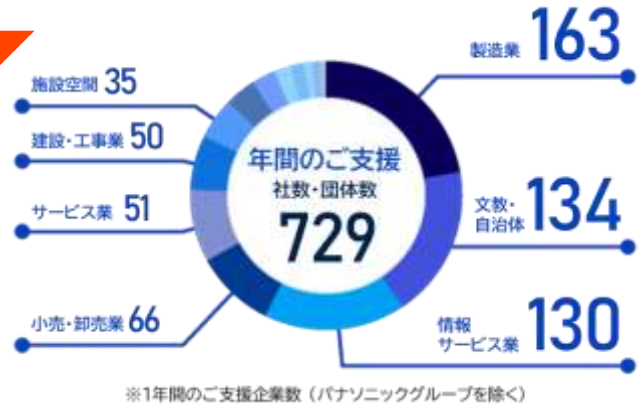
私たちはOne Panasonic ITです。
認め合い、学び合い、高め合って、皆で成長し続けます。

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

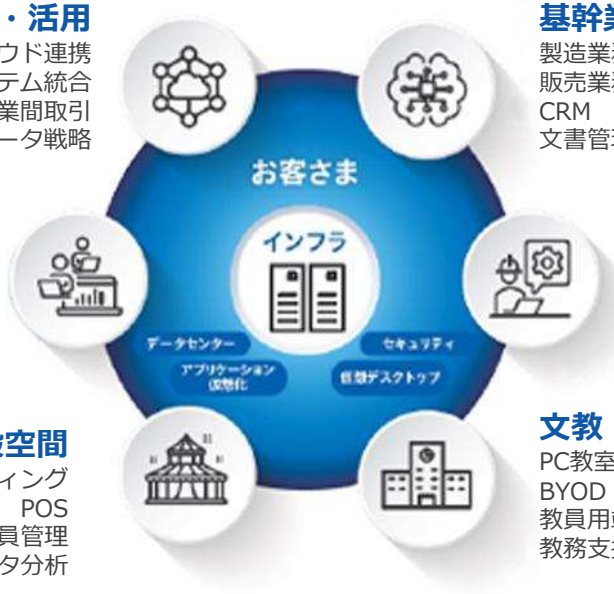


※1年間のご支援企業数（パナソニックグループを除く）

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

AppGuard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