AppGuardご紹介

2025-11-27

ITガード

侵入されても
被害を受けず
業務を止めない

国内における主な医療機関導入事例

名寄市立総合病院様

**“サイバー攻撃対策のラストピースとして AppGuard に着目
侵入されても診療をストップさせない仕組みを整えた名寄市立総合病院”**

医療業
名寄市立総合病院 様
規模 病床 359床

日本最北の救急救命センターである名寄市立総合病院では、北海道北部地域の医療機関を結ぶネットワークを構築して救急患者の遠隔トリアージを行うなど、以前から ICT 技術を積極的に活用してきました。近年、国内の医療機関でランサムウェア感染による被害が続発したことを受け、「決して他人事ではない」と強い危機感を抱き、たとえ侵入されても診療を止めないアプローチとして AppGuard に着目。病院情報システムのサーバ約 70 台に導入しました。

他人事ではないと感じたランサムウェア感染事故、新たな方針での対策を模索

名寄市立総合病院は日本最北の救急救命センターとして、道北北部三次医療圏を支えています。
医療圏は広大で救急搬送に数時間要することもあり、患者搬送自体にもリスクがあります。そこでICTネットワークを構築し、二次医療圏中核病院との間で、患者の検査情報を共有・参照して遠隔救急トリアージを行い、限られた医療リソースを有効に活用して一人でも多くの命を救おうと試みてきました。「道北北部の医療機関全体がバーチャルな一つの大きな病院として機能する形を作ってきました」（名寄市立総合病院情報管理センター長、守屋潔氏）
今やこのネットワークは救急医療だけでなく、平時の診療連携や名寄市内の介護施設をつないだ地域包括ケアシステムも支える存在となっています。
一方で「外とつなぐことになると、やはり心配なのがサイバー攻撃です。特に2021年、徳島県の病院がランサムウェアの被害に遭った件がメディアでも大きく報じられましたが、とても他人事とは思えず、同じことが当院にも起こるかもしれないと危機感を抱きました」（守屋氏）
そこで2022年は「サイバー攻撃対策を強化する一年」と位置付け、「どんなことがあっても診療をストップさせない」という目標を掲げてさまざまな対策を進めました。まず、万一侵害を受けたとしても、電子カルテと医事会計のデータだけは守れるようにオフラインでデータを保存するバックアップ装置を導入しました。次に、それまで部門システムのベンダーが個別に設置していたリモート保守回線を名寄市立総合病院が用意した回線に集約することにしました。病院へのサイバー攻撃の侵入経路として部門システムのリモート保守回線の脆弱性が狙われるケースが多いからです。リモート保守回線を同院が一括管理することでシステムベンダーとの責任分界点も明確になります。
これでサイバー攻撃対策は一段落と安心していたところに、衝撃的なサイバー攻撃事案が発生しました。2022年10月大阪の大規模な病院で、給食事業者とつながるネットワーク経由で侵入されてランサムウェアの被害が発生したのです。
「いくら病院自身がきちんと管理していても、取引先から正規の通信を装って侵入されるとなるとお手上げです。不正な通信を検知してアラートを飛ばすシステムでは、防ぎようがありません。頭を抱えましたが、もはやサーバに侵入されることを前提に対策を考えるしかないと方針を大きく転換しました」（守屋氏）

津山中央病院様

**“医療を支える「絶対にやられてはいけないシステム」をAppGuard Serverで死守
EDRとの棲み分けで診療業務継続に取り組む津山中央病院”**


津山中央病院様　外観

医療業
津山中央病院様
規模 病床 約500床

医療機関がランサムウェアに感染し、長期間にわたって診療業務を停止せざるを得ないケースが複数報道されています。この事態を踏まえ津山中央病院では、万一に備えた手順の整備やクライアントPC対策の強化とともに、院内の中でも「絶対にやられてはいけないシステム」を守る手段を検討し、「AppGuard Server」を導入しました。大きな安心感が得られ、万一被害に遭うことを考えれば安い投資だと評価しています。

深刻なランサムウェア被害を目の当たりにして高まった危惧

500以上の病床数を備える津山中央病院は地域の中核病院として、津山市はもちろん、岡山県北部の高度な医療を支えてきました。
最近はしばしば「医療のデジタル化」が話題になりますが、津山中央病院は、1990年代後半という他の病院はもちろん社会全体で見ても早い時期から院内とインターネットを接続し、IT技術を活用してきました。いわゆる「クローズドなネットワーク」ではなく、ネットワーク境界での防御と、アンチウイルスソフトによる各端末での保護を組み合わせ、大規模なセキュリティ事故を起こすことなく運用してきました。
しかし「この数年、病院がランサムウェア攻撃に遭うケースが頻繁に報道されています。我々以上に大規模な病院でも被害を受けているのを目の当たりにし、インターネット系と電子カルテなどの情報系を分けていない我々の場合、万一侵害されたら甚大な影響を受けてしまうだろうという危惧が高まっていました」（津山中央病院　法人本部 システムグループ、村上公一氏）
しかも「パターンマッチングに基づくウイルス対策ソフトでは、ランサムウェアをはじめとする最近のウイルスは防げません」（村上氏）。こうした危惧に加え、厚生労働省がサイバーセキュリティ対策に関する新たなガイドラインを示したこともあり、津山中央病院はいくつかの対策に取り組み始めました。
まず、万一ランサムウェアに感染した場合でも診療業務を継続できるよう、以前から取得してきたデータのバックアップをより徹底するとともに、紙ベースで病院の運用を継続するためのマニュアルを整備しました。また各端末の保護も、いわゆるパターンファイル型のアンチウイルスソフトからAI技術も搭載したEDR製品に入れ替え、SOCサービスを活用して監視する体制を整えました。

絶対にやられてはいけないシステムの保護にAppGuard Serverを選択

しかし、それでも一抹の不安は拭えませんでした。
「EDRの検知に引っかかる時点で、すでに悪意あるソフトウェアが院内で活動していることになります。もし電子カルテの情報が攻撃され、暗号化されて使えなくなってしまっては、どうしようもありません」（村上氏）。長期間に渡って診療業務を止めることになれば、想像もつかない損害が生じる懸念がありました。
津山中央病院では、電子カルテにはじまり、各医局・検査システムなど約200台のサーバーが仮想基盤上で動作していいます。「中でも、病院の中でどうしても守らなければいけないものがあります。電子カルテ、オーダリングシステム（医事会計）、そしてPCを動かすためのドメインサー

相澤病院様

“プロセス制御を見える化し、ブラックボックス任せの処理を回避”

医療業
社会医療法人財団慈泉会 相澤病院 様
規模 病床 約460床

相澤病院では、医療情報システム全般の設計と構築に対して主体的に関わる形でシステム導入を推進している。増大するランサムウェアなどの脅威への対策において、「システムに必要となる最小限のサービスやプロセスに対して特定の挙動のみを許可し、それ以外はすべてブロックし動作を認めない」というコンセプトの分かりやすさを評価し、「AppGuard」を選択した。

リスクパターンの変化を受けて次なる対策を模索

長野県松本市に位置する相澤病院は、一世紀以上にわたる地域への医療提供とともに病院改革を進め、情報システムの活用においても先進的な取り組みを行ってきた。1999年のオーダリングシステム導入以降、電子カルテや医療系部門システム、情報系システム、セキュリティ、ネットワークなどの範囲を情報システム部が担い、システムの設計から導入、運用サポートを医療機関主導で対応している。
「ベンダーに『丸投げ』する方法でもシステム導入は実現しますが、システムの最終責任は我々にあります。構成を理解しシステムの健全性や整合性など、システム全体への影響を評価できる体制を構築しなければ、情報インフラを安定的に提供する目的だけでなく、サイバー攻撃などの脅威に対しても大きなリスクを抱えることになります。そのため、ユーザーサイドに立ちながら、ベンダーと技術面でも対等に話ができる体制を整えてきました」（慈泉会本部 医療情報システム部 課長　小日向隆行氏）
システム導入においては、過去のインシデントも踏まえ、OS設定やシステム構成まで踏み込んだ交渉をベンダーと行う一方で、「良質な医療を提供するために新たなシステムを導入したい」といった現場の意向を尊重しつつ、「セキュリティ的にどこまでの自由度を許すのか」のラインを探り、バランスを取りながら対応している。
同院ではリスクベースのアプローチに基づき、サーバのアップデートや適切な設定・ポリシーによる堅牢化、エンドポイントセキュリティ製品の導入といったセキュリティ対策を実施してきたが、国内の医療機関で相次いで大規模なセキュリティインシデントが発生したことを受け、一層の対策強化が必要だと判断していた。「100%の防御は不可能であると認識しつつも、絶えず変化するリスクに対し、最適な対策の組み合わせを模索しています。『何がベストなのか？』という問いを胸に、日々考えています。」（小日向氏）

国内における主な医療機関導入事例

APPGUARD

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

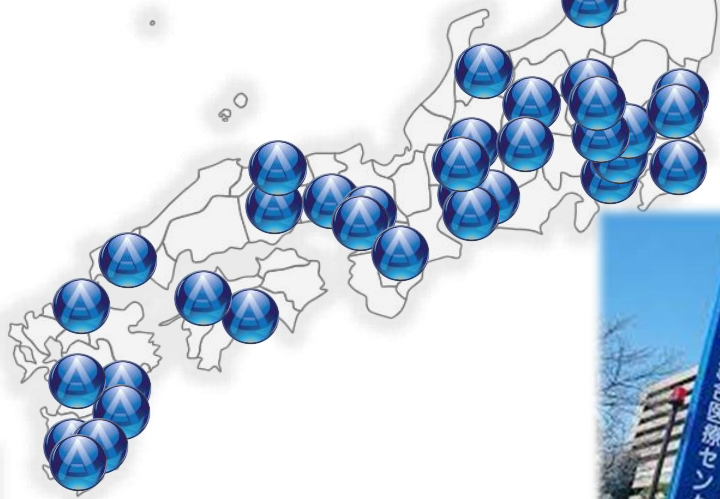
460床

名寄市立総合病院
Nayoro City General Hospital

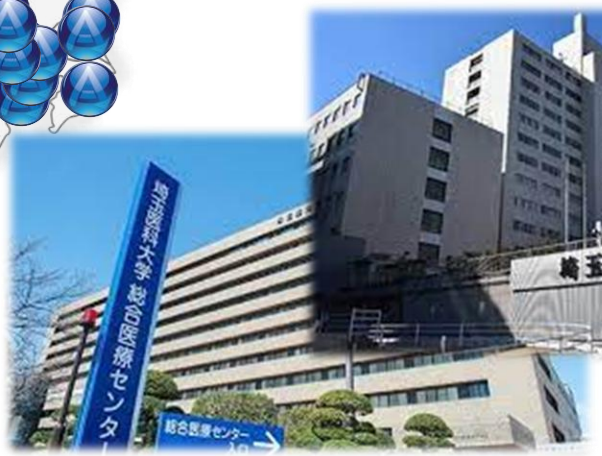
359床

特定医療法人 佐藤会
弓削病院

108床

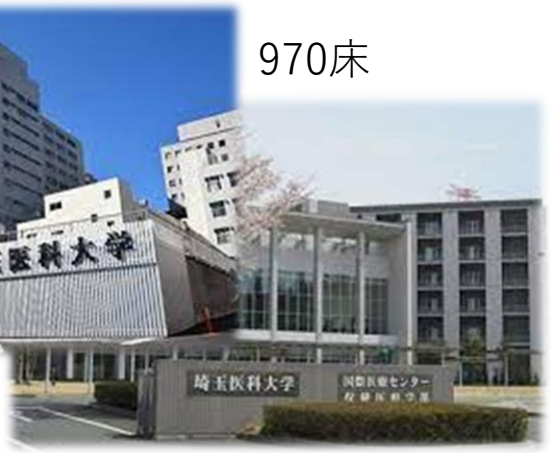


埼玉医科大学病院
Saitama Medical University Hospital



1053床

970床



700床

日本病院会様との連携

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：堺　常雄
〒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. 03-3264-9888

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、藤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、この新陣容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 日産厚生会 会長
玉川病院　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、公益財団法人日産厚生会玉川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ワーキンググループ、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。そのようなお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　常雄	専務取締役事業本部長	新井郁夫		
取締役	高木由利	取締役	佐合茂樹	取締役	齋藤　清
取締役	中嶋　昭（新任）	監査役	梶原　優	監査役	境野英雄
名誉顧問	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弓削病院等、50 以上の医療機関で採用されています。詳細は 2P ～ 3P および同封のパンフレットをご覧ください。

1

…ドポイントセキュリティ対策ツー
…ard は「攻撃者の目的を達成させ
…やサーバー上で「やって良いこと・
…けが継続的に実践されているか検
…、不正アクセスの成立）が発生し

…術（US Patent #7712143）を用い
…ゴン）を含む、複数の米国政府機
…ウ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保
…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 …御エンジンも 1 MB 以下と軽量化が

…管理に関するガイドライン第 6.0 版」
…「ゼロトラスト」の概念について言
…7「Zero Trust Architecture」では、
…サービスがリクエストを正確かつ最
…定義されています。

…現に寄与するものとしていくつかの
…T SP800-207 で規定される考え方に
…ガイドライン上では端末やサーバー
…おいては、電子カルテシステムや医
…に機微な個人情報等の死守しなけれ

…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
…きまとっていました。いつまでも
…ぐに導入を決定。防御力が高まっ
…ことで、導入前に比べてランニン

…tion and Response）」というセキュ
…を防ぎ切れないという前提に立ち、
…小限に留めることを目的とした対策
…、有効な対策だと考えられます。し
…なることから、十分に使いこなすこ

…ュリティリスクを洗い出し、日々
…ります。

担当：熊谷（くまがい）
…時まで　※年末年始を除く）

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：堺　常雄
〒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. 03-3264-9888

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：03-3264-9888（平日 9 時～ 17 時）

1

国内における導入実績

APPGUARD

ANA　SMBC日興証券　埼玉医科大学 Saitama Medical University　社会医療法人財団 慈泉会 相澤病院　JTB 感動のそばに、いつも。

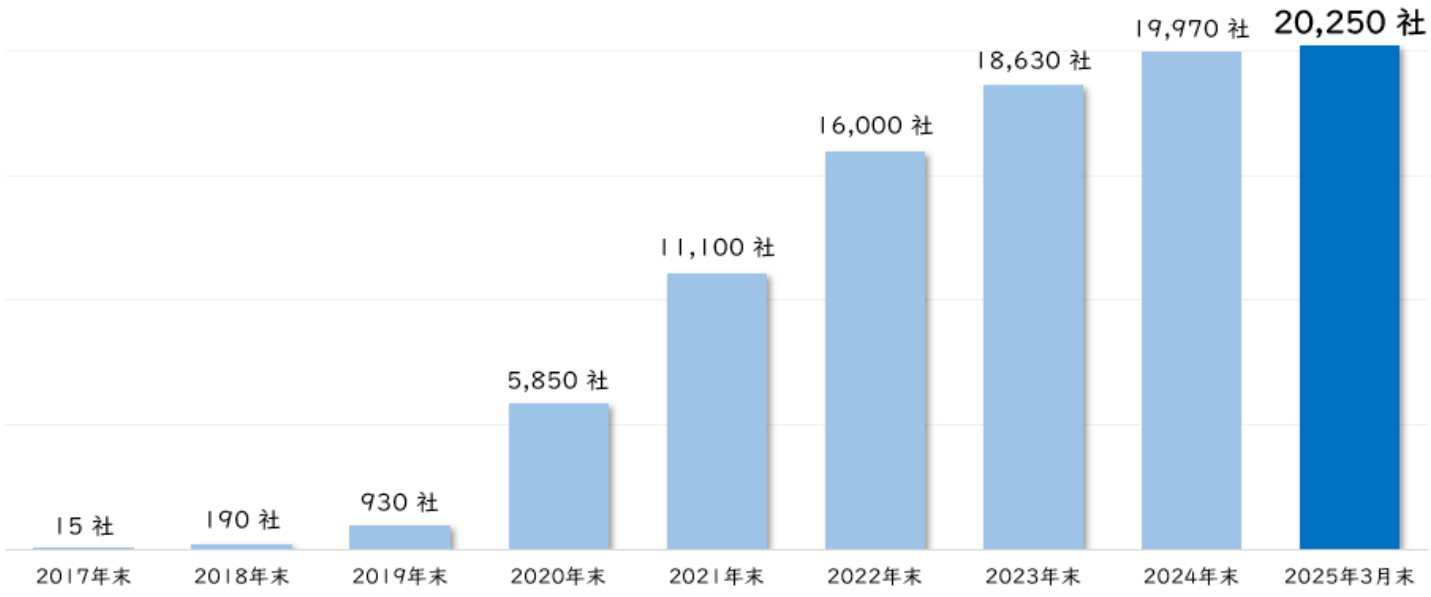
戸田建設　DAIKO XTECH　人・街・未来をまもる 東洋テック　pci PCI Solutions INC.　KAKUDAI

ecOHAI　社会福祉法人 千葉市社会福祉協議会　（白石市様）　NEC NECキャピタルソリューション　BANC OF CALIFORNIA　（アメリカ国防総省）

国内導入累積社数

20,500社突破

（2025年6月末時点）



昨今のサイバー攻撃の特徴

サイバー犯罪者が持つ基本的な考え方

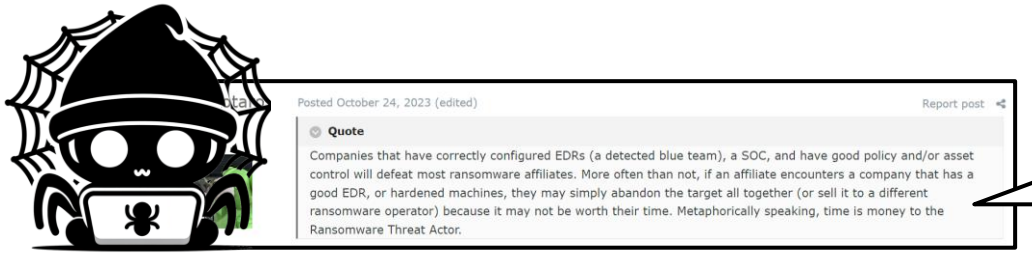
▶ ダークウェブ上のハッカーフォーラムの投稿から読み解く

意訳：（攻撃者としての）経験則から言える最適な対策は「攻撃者の攻撃コストを高くする」ことに尽きます。

攻撃コストが低い組織は標的にされる。

意訳：非常に簡単な安全対策（強力なパスワード、厳格なファイアウォールルール、内部ポリシーなど）で攻撃者の力を大幅に低下させることができます。

基本的なセキュリティ対策ができていない組織＝攻撃コストが低い



意訳：あなたたちの意見に同意する。攻撃者は優れた組織に出会った場合、時間をかける価値を見出だせないため、ターゲットを放棄します。

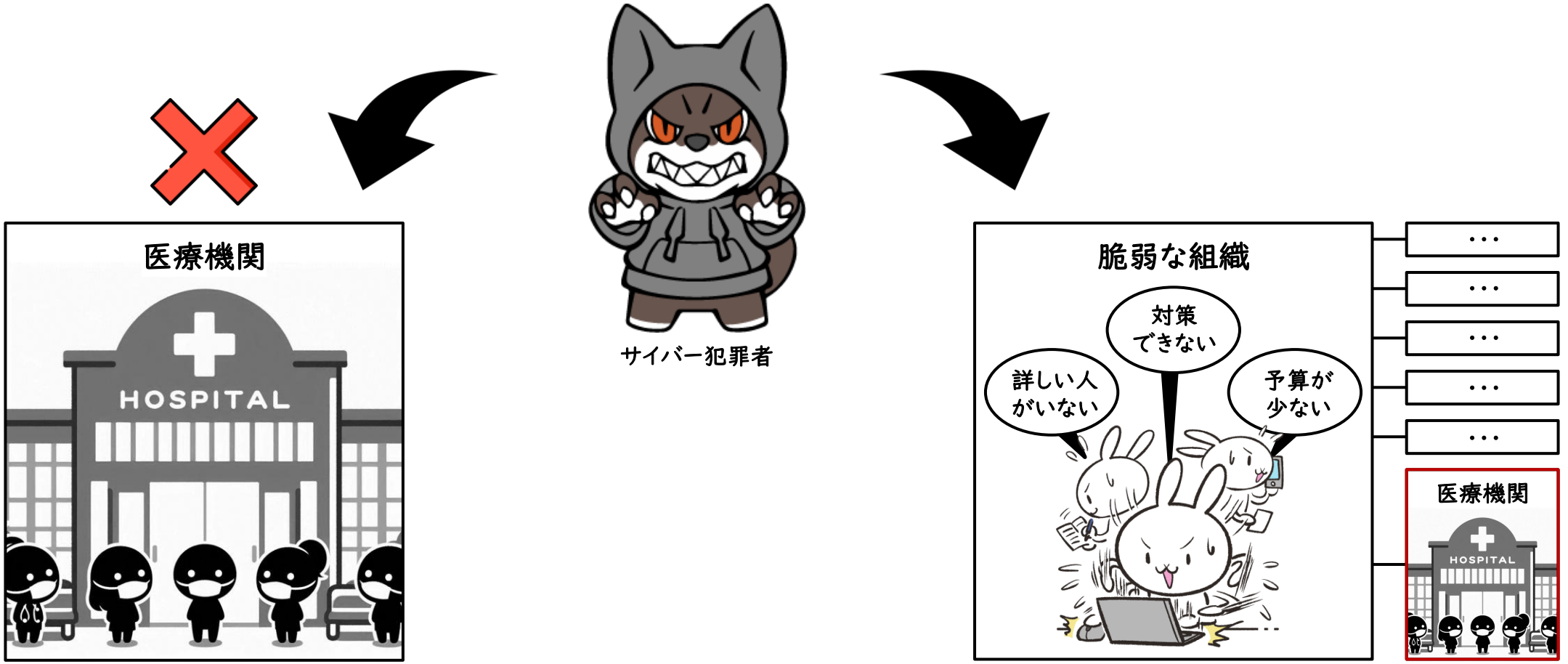
攻撃コストが低い組織を見つけた場合、最後まで攻め上げる。

サイバー犯罪者は医療機関を狙っている？

APPGUARD

▶ **低コストで攻略可能な相手を標的にする**

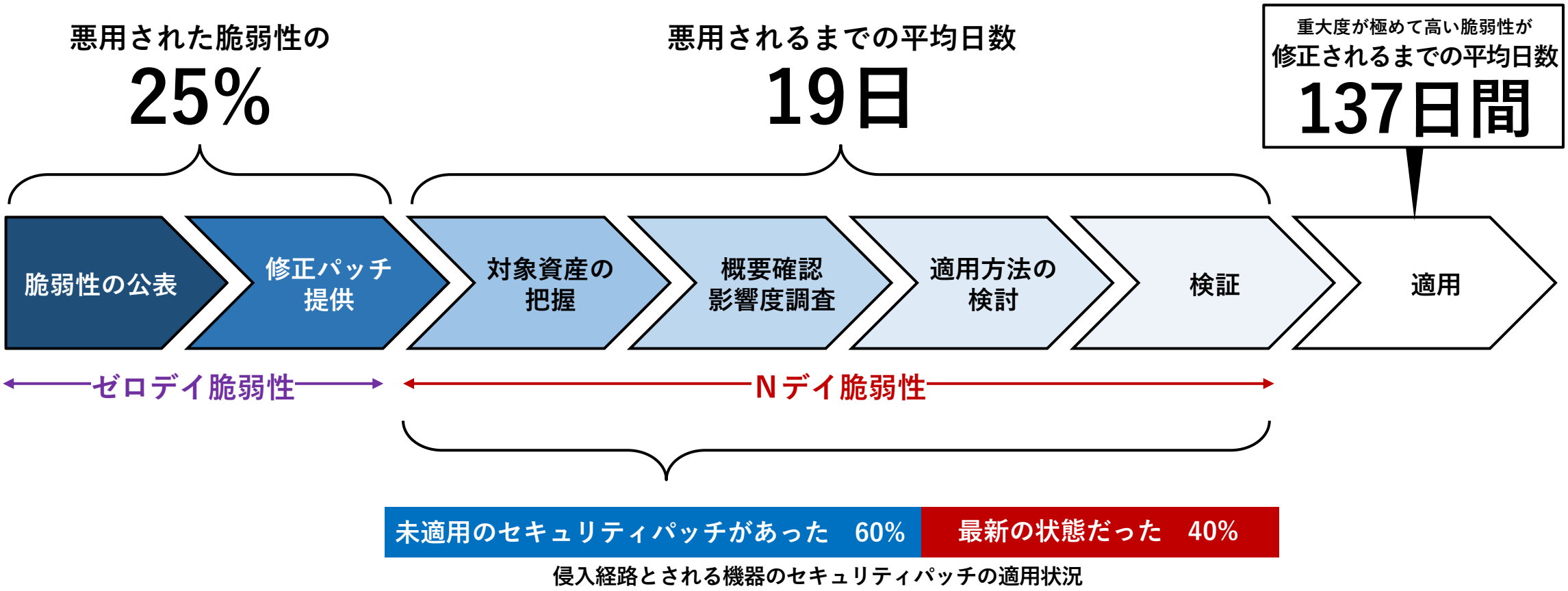
- 特定国家に関連付けられたサイバー犯罪者を除けば、その多くは侵害に際して低コストな（労力があまりかからない）相手を探し出して攻撃を仕掛ける傾向にある。つまり、医療機関だとわかった上で侵入するのではなく、侵入した結果、医療機関であると認識することが多い。



脆弱性の修正までに与えられる猶予期間はごくわずか

▶ 脆弱性の解消・緩和はより重要に

- 2023年にサイバー攻撃に利用された脆弱性は206件（公開されたのは26,447件）あり、武器化して展開するまでの日数は短縮傾向にある。
- 最新の状態を維持していたとしても悪用される脆弱性のうち25%はゼロデイであるとされている。



侵入経路とされる機器のセキュリティパッチの適用状況

出典：Qualys「2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is」
：警察庁「令和5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」
：BITSIGHT「Bitsight Reveals More than 60 Percent of Known Exploited Vulnerabilities Remain Unmitigated Past Deadlines in First-of-its-Kind Analysis of CISA's KEV Catalog」

2年半の間に「70」の新しい攻撃手法を検証

本検証結果は2025年10月30日時点のものです。(期間:2023年4月～2025年10月)

01	FIN11による攻撃キャンペーンで使用された攻撃ベクトル
02	「BIG HEAD HACKER Ransomware」で使用された攻撃ベクトル①
03	「BIG HEAD HACKER Ransomware」で使用された攻撃ベクトル②
04	「BIG HEAD HACKER Ransomware」で使用された攻撃ベクトル③
05	「Maldoc」を利用した「Cobalt Strike Beacon」展開用の攻撃ベクトル
06	「Maldoc in PDF」で使用された攻撃ベクトル
07	「APT37(Reaper)」による「CHMファイル」を悪用した攻撃ベクトル
08	「テクニカルサポート詐欺」による遠隔操作を目的とした攻撃ベクトル
09	「DarkGateマルウェア」の攻撃ベクトル
10	「ClearFakeを利用したDBD攻撃」の攻撃ベクトル
11	「Tropic Trooper」による標的型攻撃メールの攻撃ベクトル
12	「LummaC2 Stealer(タスクスケジューラー型)」の攻撃ベクトル
13	「LummaC2 Stealer(DLLダウンロード型)」の攻撃ベクトル
14	「HTML Smuggling」による「Cobalt Strike Beacon」の攻撃ベクトル
15	「HTML Smuggling」による「Xworm RAT」の攻撃ベクトル
16	「HTML Smuggling」による「Async RAT」の攻撃ベクトル
17	「TA571/TA866」による攻撃キャンペーンで利用された攻撃ベクトル
18	「Redline Stealer」の攻撃ベクトル
19	「UNC4990」によるUSBデバイスを悪用した攻撃ベクトル
20	「Phobosランサムウェア」の亜種「FAUST」の攻撃ベクトル
21	「Gootloader+Cobalt Strike Beacon」の攻撃ベクトル
22	「Notion」に偽装した「LummaC2 Stealer」の攻撃ベクトル
23	偽の「Adobe Reader」を起点とする攻撃ベクトル
24	正規サイトを悪用する「AgentTesla」の攻撃ベクトル
25	「ScrubCrypt」を利用した「VenomRAT」の攻撃ベクトル
26	「IcedID」の後継モジュールを配布するキャンペーンの攻撃ベクトル
27	「CoralRader」が実施するキャンペーンの攻撃ベクトル
28	「WINELOADER」の感染を目的とした攻撃ベクトル
29	CERT-UAが公表したAPT28が利用した攻撃ベクトル
30	OrcusRATを配布するキャンペーンの攻撃ベクトル
31	APT28が実施するキャンペーンの攻撃ベクトル
32	DarkGateマルウェアの新たな攻撃ベクトル
33	「Kimusky」によるサイバースパイを目的として攻撃ベクトル
34	Sticky Werewolfによる攻撃キャンペーンの攻撃ベクトル
35	「InnoLoader」を利用した攻撃ベクトル
36	BECを介して配布される「SnakeKeylogger」の攻撃ベクトル
37	URLファイルを利用して配布される「Xworm」の攻撃ベクトル
38	スパイ活動用マルウェア「Voldemort」の攻撃ベクトル
39	偽のCAPTCHAテストを利用した「Click Fix攻撃」の攻撃ベクトル
40	エアギャップネットワークへ侵入する「GoldenJackal」の攻撃ベクトル
41	MSCファイルを悪用したマルウェアの攻撃ベクトル
42	Google Meetを装った「Click Fix攻撃」の攻撃ベクトル
43	デジタルマーケティング人材を狙った攻撃キャンペーンの攻撃ベクトル
44	Windows RDPを悪用したサイバースパイを目的とした攻撃ベクトル
45	GamaredonによるHTML Smugglingを用いた攻撃ベクトル
46	APT-C-60による「SpyGrace」配布キャンペーンの攻撃ベクトル
47	TA455による「Dream Job」を模倣した攻撃キャンペーンの攻撃ベクトル
48	CrowdStrikeの採用プロセスを悪用した攻撃キャンペーンの攻撃ベクトル
49	「著作権侵害の警告」等を題材に使った詐欺メールの攻撃ベクトル
50	添付ファイルヘッダを改造して配布される「ModiLoader」の攻撃ベクトル
51	偽のGoogle Meetを利用した「Phonzy」を配布する攻撃ベクトル
52	EarthKapreの配布する攻撃キャンペーンの攻撃ベクトル
53	重要交通インフラを標的とした攻撃キャンペーンの攻撃ベクトル
54	Browser Cache Smugglingを悪用した攻撃ベクトル
55	APT37によるフィッシングキャンペーンの攻撃ベクトル
56	Earth Kashaによる攻撃キャンペーンの攻撃ベクトル
57	偽オンラインファイル変換サービスを悪用したClick Fix攻撃の攻撃ベクトル
58	Operation Deceptive Prospectキャンペーンの攻撃ベクトル
59	有名ブランドからの偽求人を装ったキャンペーンの攻撃ベクトル
60	File Explorerを悪用するFile Fix攻撃の攻撃ベクトル
61	テクニカルサポート詐欺+Click Fix攻撃の攻撃ベクトル
62	大規模言語モデルを利用した「LAMEHUG」の攻撃ベクトル①
63	大規模言語モデルを利用した「LAMEHUG」の攻撃ベクトル②
64	Search-ms URIを利用したClick Fix攻撃の攻撃ベクトル
65	セクストーション機能を実装したInfoStealerの攻撃ベクトル
66	非技術者系人材を狙うDream Jobの攻撃ベクトル
67	正規機能を悪用する「EDR-Freeze」の攻撃ベクトル
68	Cache Smuggling+File Fix攻撃キャンペーンの攻撃ベクトル
69	APT-C-60(北朝鮮)による攻撃キャンペーンの攻撃ベクトル
70	日本を標的とした攻撃キャンペーン(HoldingHands)の攻撃ベクトル

次々と新しい攻撃方法が
登場するな…

新しい攻撃手法から見えてきたこと

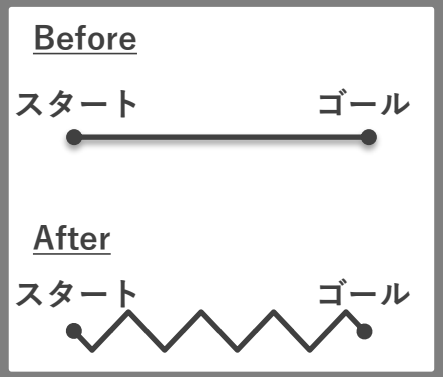
APPGUARD

アンチウイルスの検知回避は「クリア済みの課題」

現在はEDRに対していかに検知されないかを意識していると考えられる

マルウェアが到着するまで

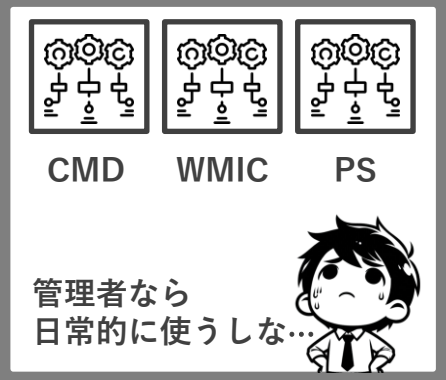
回りくどい



単一のマルウェアファイルに頼るのではなく、多段階の攻撃ステップを踏む。

攻撃なのかどうか

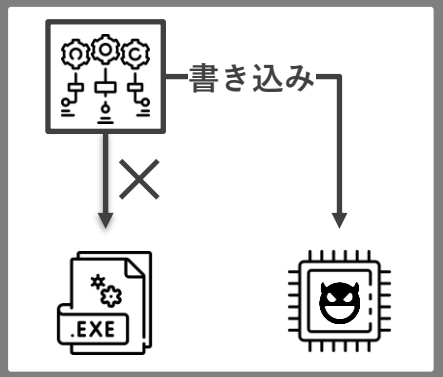
極めてグレー



OSに標準装備されているシステム管理者が使う正規のツールを悪用する。

検知すべき悪意ある

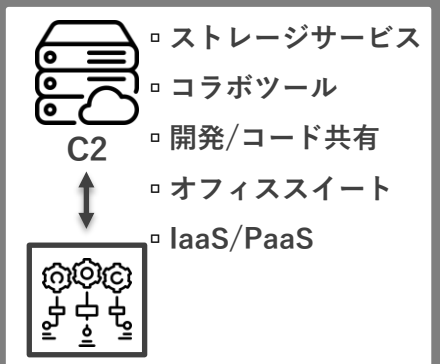
ファイルがない



ディスク上のファイルとして存在せず、メモリ上のみで実行される。

自分たちも使うので

遮断できない



組織が信頼し、業務で利用しているクラウドサービスを積極的に悪用する。

AppGuardとは

【侵入されても発症しない】AppGuardの守り方

APPGUARD

従来の製品

- ◆ 攻撃の特徴を学習
- ◆ 攻撃を検知する
- ◆ 侵入を防ぐ or アラートで知らせる

侵入されてしまうと防ぐ術がない

AppGuard

- ◆ 業務に必要な命令のみを実行許可
- ◆ 許可した命令以外は実行できないようにポリシーで制限する

侵入されても攻撃を成立させない

【侵入されても発症しない】システムを守り抜くセキュリティ

APPGUARD

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

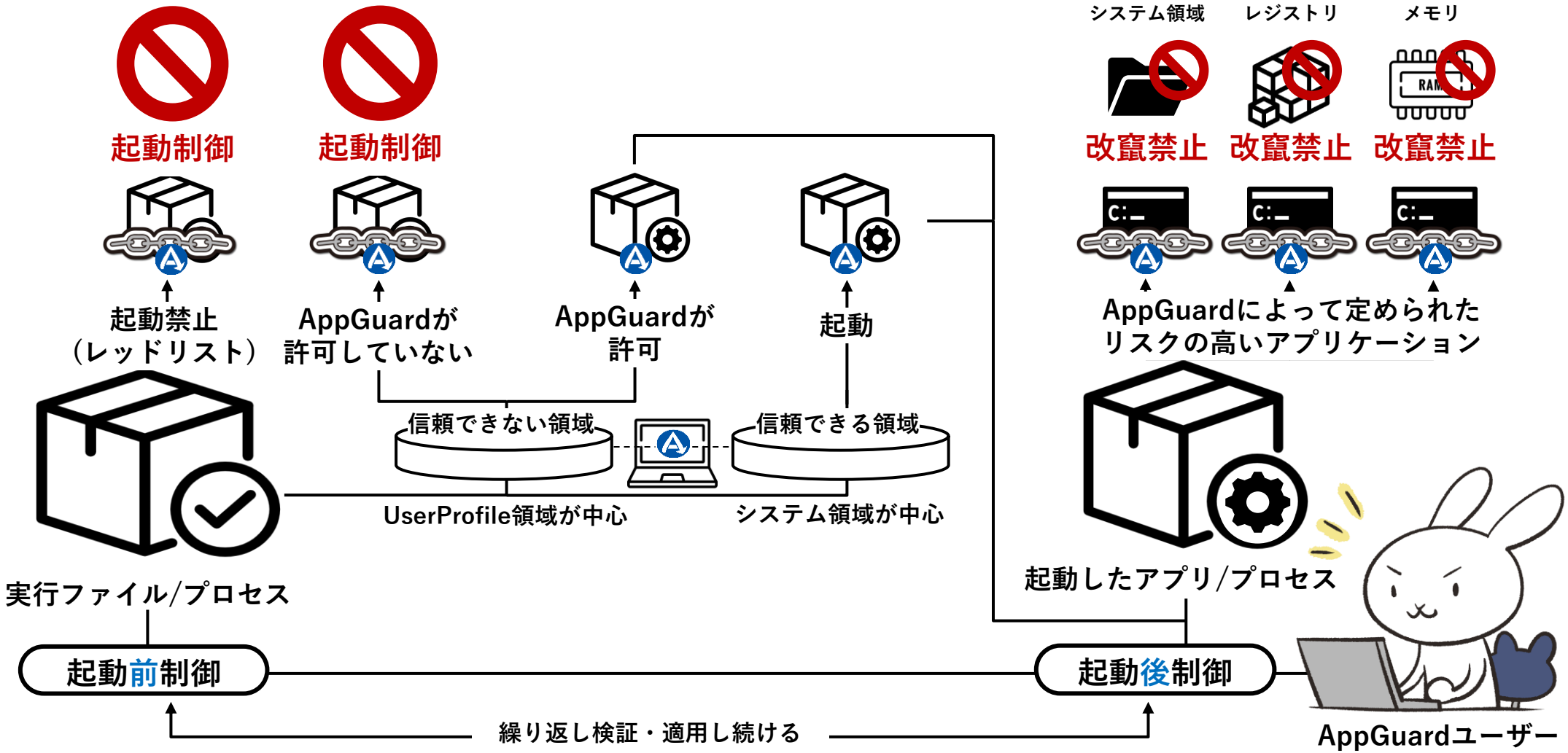
AppGuardの保護の特徴-アンチウイルスやEDRとの比較-

項目	アンチウィルス	AppGuard	EDR
区分	防御	予防	事後対応
期待される効果	侵入時の水際対策での防御	侵入されても攻撃を成立させない	脅威への早期対処・被害状況の把握
機能するタイミング	侵入時	攻撃実行前	攻撃実行後
既知のマルウェアへの対応	○（検知機能）	○（動作制御機能※）	○（検知機能）
未知の脅威への対策	△（新しい検知モデルが必要）	○（保護可能）	△（新しい検知モデルが必要）
正規の機能を悪用した攻撃への対応	×（検知不可）	○（保護可能）	△（利用者の対処スキルに依存）
未知の脆弱性を悪用した攻撃への対処	×（検知不可）	○（保護可能）	△（利用者の対処スキルに依存）

※駆除機能はなし

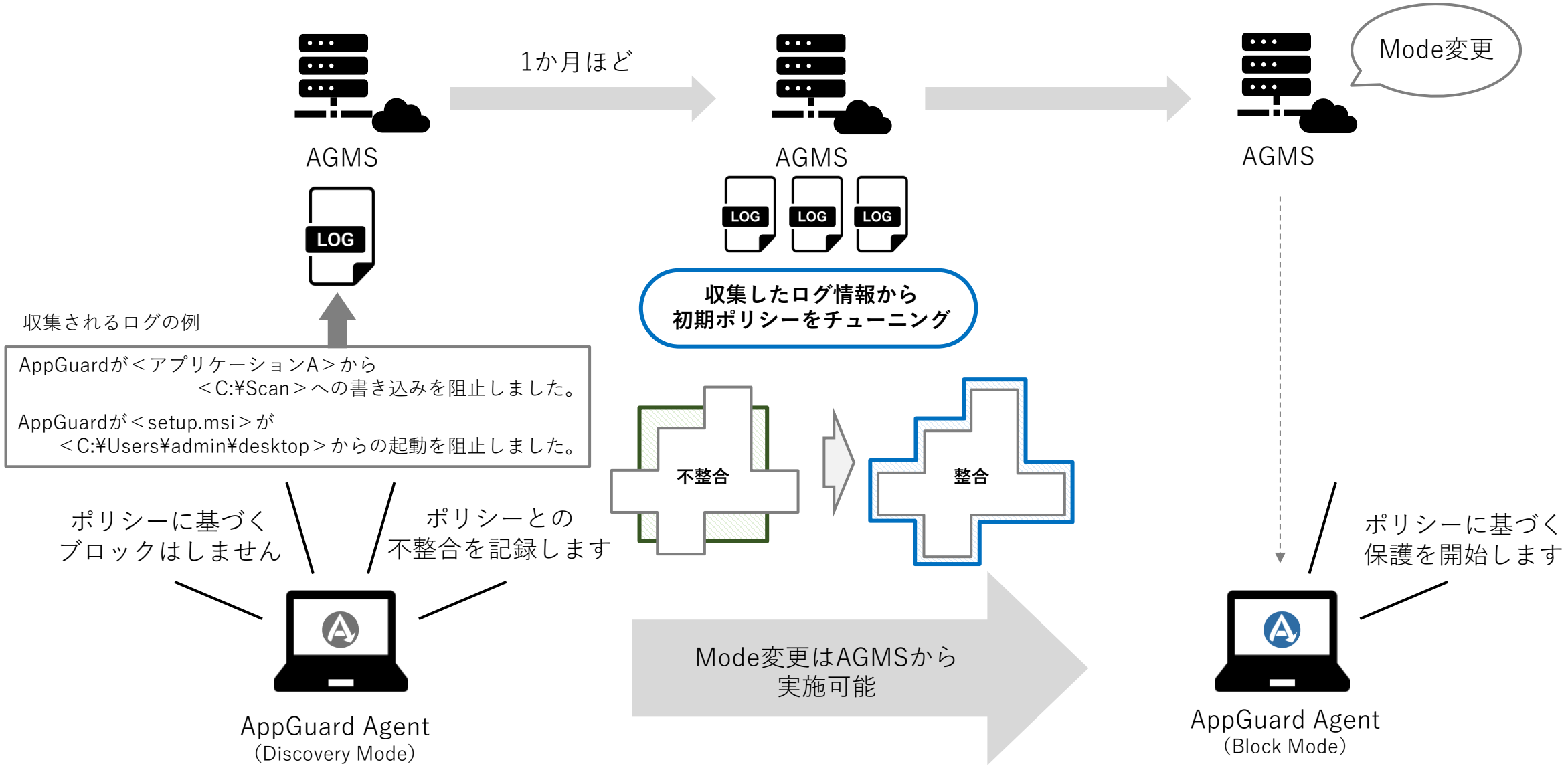
攻撃プロセスの成立を阻止する仕組み

①普段ユーザーが利用しないようなアプリはそもそも信頼せず起動禁止
②ユーザーが利用するアプリは信頼が与えられた場所からでないと起動が出来ない
③起動許可したアプリであっても常に監視し続ける



Discovery Mode

注：Discovery ModeはAppGuard Soloでは利用できません。



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

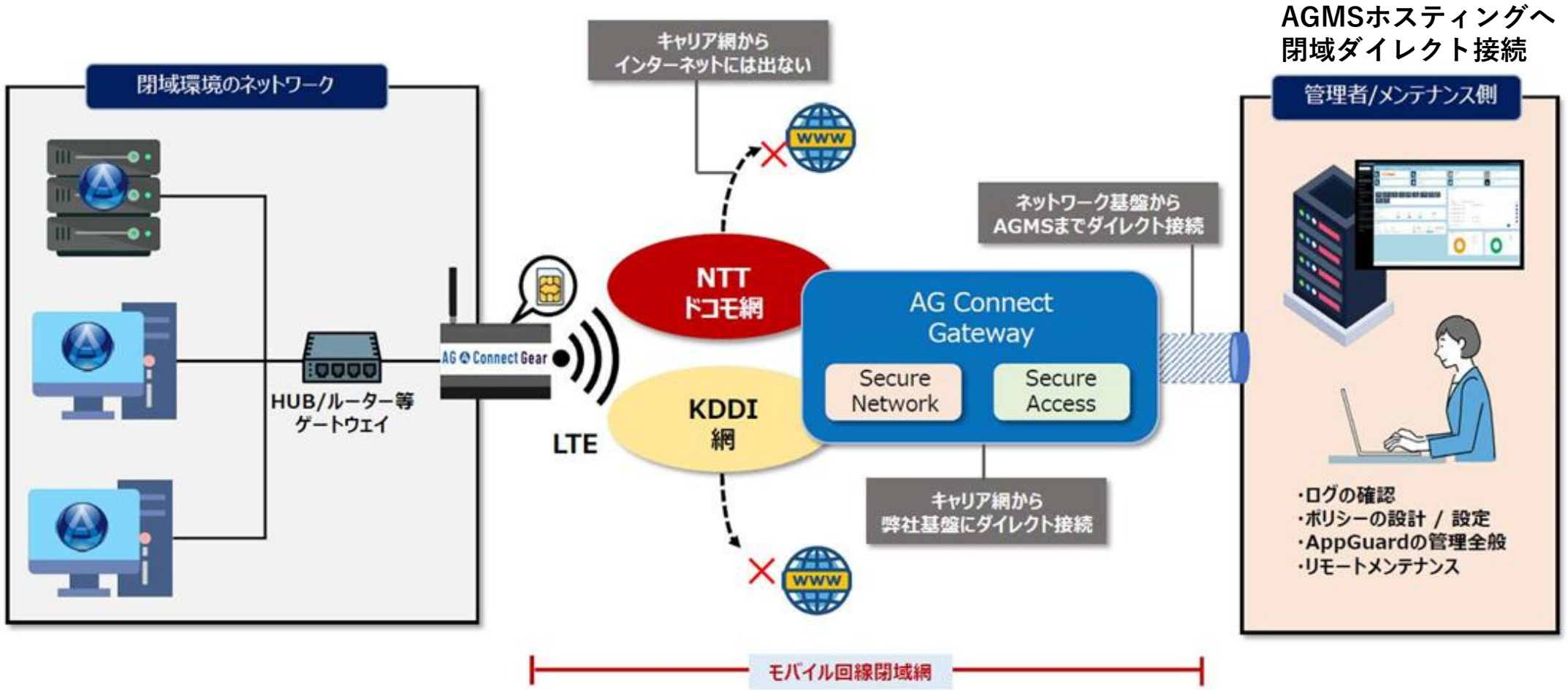
AppGuard運用パッケージ

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

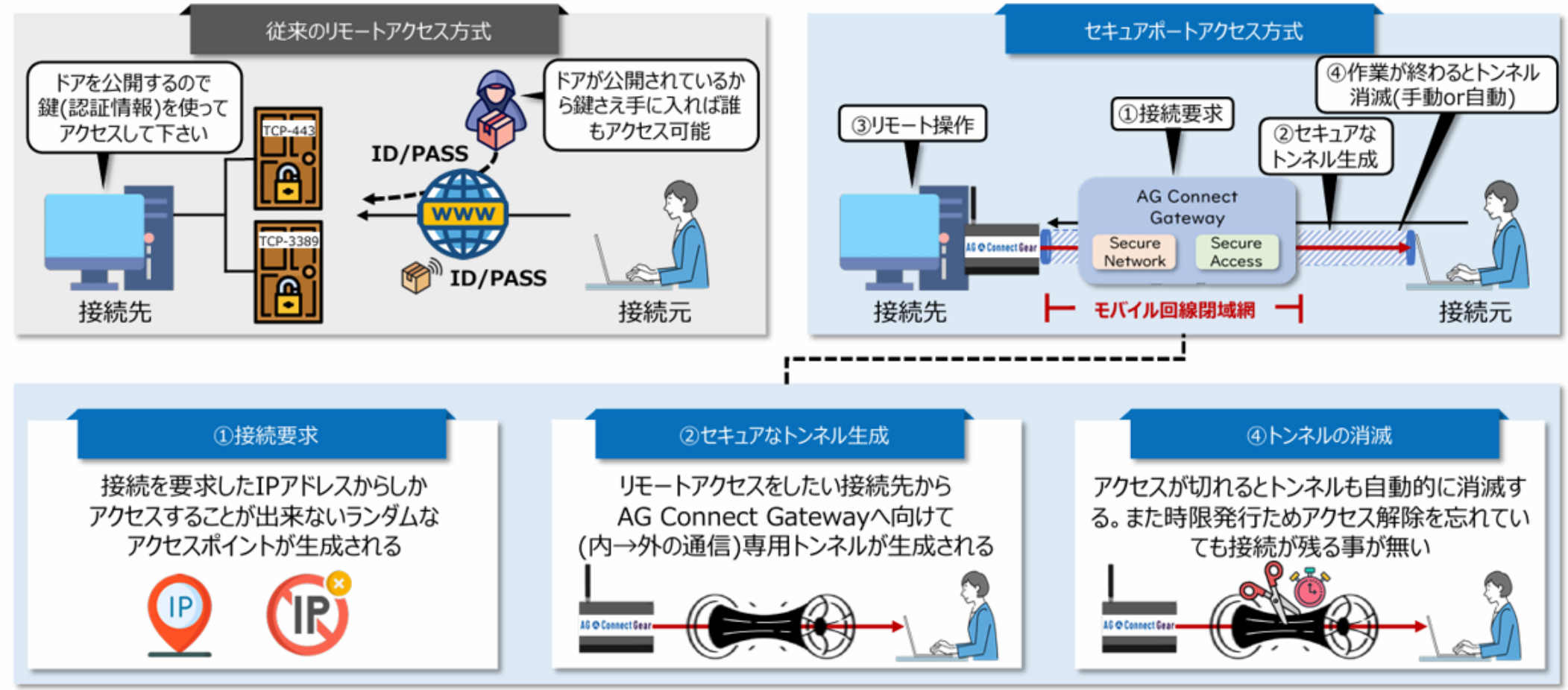
※各種支援メニューの内容は販売店によってサービス名及び提供仕様が異なります。詳細については各販売店にお問い合わせください。

高セキュリティ閉域リモート接続サービス「AG Connect」

- ✓ インターネット接続が原則許されない医療情報システムを守るセキュアなリモート接続サービス
- ✓ インターネット上へのポート開放やアクセス認証の煩雑さを解消します（外部からのポートは非公開）
- ✓ リモート保守回線の一元化を実現します



高セキュリティ閉域リモート接続サービス「AG Connect」



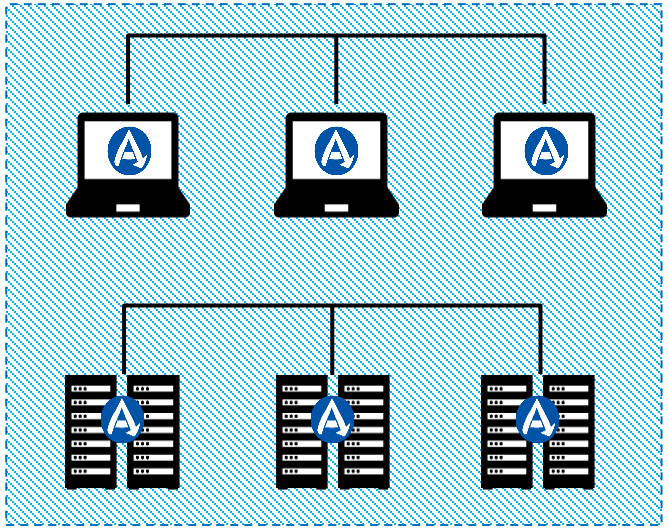
- ✓ セキュリティポリシーに基づきアクセス制限や設定が可能⇒**許可した機器・曜日・時間以外は接続できない**
- ✓ リモート接続時は必ずお客様の許可が必要⇒**病院担当者が承認した際に、リモート接続開始**

AppGuardの得意領域・導入事例

AppGuardの部分導入事例

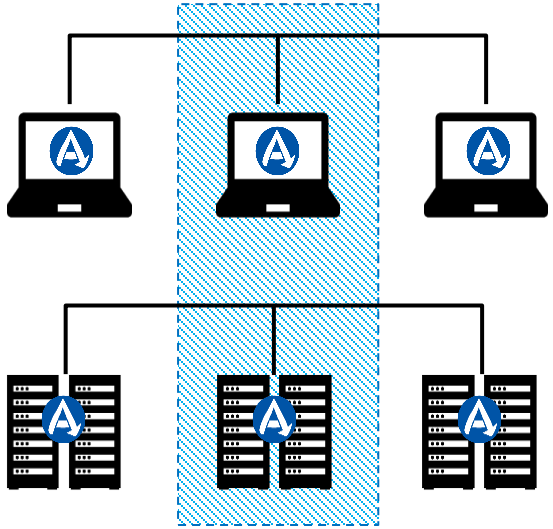
APPGUARD

全体に導入



OR

部分的に導入



優先順位の高いところにだけ導入することも可能
アンチウイルスやEDRとの併用も可能

AppGuardの部分導入事例

死守したい端末やサーバー

- 攻撃者に狙われやすく被害が甚大となる
  ADサーバーや重要端末へ導入
- 業務以外の挙動は止めるので
  攻撃の被害を受けず、掌握されない

レガシーOS

- Microsoftのサポートが切れたレガシー
  OSも保護能力を落とさず守ることが可能
- 脆弱性を利用して侵入されても
  攻撃が成立しないため安心

OT環境/閉域環境

- パターンファイルの更新が必要ない
- 業務で使用されるアプリケーションの
  挙動が変わらないければ半永久的に守る
- 検知をしないため負荷が軽い

導入事例と適用範囲

APPGUARD

社会医療法人財団 慈泉会 相澤病院

・電子カルテサーバー
・電子カルテ利用PC(１０台)
・Active Directory
・医療画像管理システム(PACS)
・文書管理システム

広域紋別病院

・電子カルテサーバー (令和5年度予算)
・ActiveDirectory(令和5年度予算)
・部門システムサーバー(令和6年度予算)
・医療情報システムを扱うPC(令和7年度予算)

埼玉医科大学病院
Saitama Medical University Hospital

【連結３病院(合計約3,000床)への導入】
・院内の全サーバー(300台)
・院内の全PC(約6,000台)
※電子カルテサーバーは対象外OSのため断念。現在導入作業が始動中

名寄市立総合病院
Nayoro City General Hospital

・電子カルテサーバー
・ActiveDirectory
・部門システムサーバー

弓削病院
YUGE NEUROPSYCHIATRIC HOSPITAL

・院内の全PC(約200台)への導入

津山中央病院
Tsuyama Chuo Hospital

・ActiveDirectory
・部門システムサーバー(内視鏡)
・オーダリングシステムサーバー

導入事例　津山中央病院様

■AppGuard導入前の取り組み

ウイルス感染やサイバー攻撃を早期に発見し診療業務を継続できるよう、オフラインバックアップの取得や、EDR＋外部SOCサービスを活用して監視体制を整えていた

■感じていた課題

EDRの検知に引っかかる時点で、すでに悪意のある行為が行われ活動しているということになる。
絶対に死守しなければいけないシステムは検知する仕組みではなくやられない仕組みが必要

■AppGuardでの解決

約200台のサーバーが稼働している中、事業を継続するために必要な「電子カルテ」「オーダリングシステム」「ActiveDirectory」を絶対死守領域と定めAppGuardを導入。EDRでPCを中心に攻撃の検知に努めつつ、やられてはいけない重要なシステムはAppGuardによって、攻撃手法に左右されずに守ることが可能となった。

導入事例　名寄市立総合病院様

“サイバー攻撃対策のラストピースとして AppGuard に着目
侵入されても診療をストップさせない仕組みを整えた名寄市立総合病院”

医療業
名寄市立総合病院 様
規模　病床 359床

日本最北の救急救命センターである名寄市立総合病院では、北海道北部地域の医療機関を結ぶネットワークを構築して救急患者の遠隔トリアージを行うなど、以前から ICT 技術を積極的に活用してきました。近年、国内の医療機関でランサムウェア感染による被害が続発したことを受け、「決して他人事ではない」と強い危機感を抱き、たとえ侵入されても診療を止めないアプローチとして AppGuard に着目。病院情報システムのサーバ約 70 台に導入しました。

他人事ではないと感じたランサムウェア感染事故、新たな方針での対策を模索

名寄市立総合病院は日本最北の救急救命センターとして、道北北部三次医療圏を支えています。
医療圏は広大で救急搬送に数時間要することもあり、患者搬送自体にもリスクがあります。そこでICTネットワークを構築し、二次医療圏中核病院との間で、患者の検査情報を共有・参照して遠隔救急トリアージを行い、限られた医療リソースを有効に活用して一人でも多くの命を救おうと試みてきました。「道北北部の医療機関全体がバーチャルな一つの大きな病院として機能する形を作ってきました」（名寄市立総合病院情報管理センター長、守屋潔氏）
今やこのネットワークは救急医療だけでなく、平時の診療連携や名寄市内の介護施設をつないだ地域包括ケアシステムも支える存在となっています。
一方で「外とつなぐことになると、やはり心配なのがサイバー攻撃です。特に2021年、徳島県の病院がランサムウェアの被害に遭った件がメディアでも大きく報じられましたが、とても他人事とは思えず、同じことが当院にも起こるかもしれないと危機感を抱きました」（守屋氏）
そこで2022年は「サイバー攻撃対策を強化する一年」と位置付け、「どんなことがあっても診療をストップさせない」という目標を掲げてさまざまな対策を進めました。まず、万一侵害を受けたとしても、電子カルテと医事会計のデータだけは守れるようにオフラインでデータを保存するバックアップ装置を導入しました。次に、それまで部門システムのベンダーが個別に設置していたリモート保守回線を名寄市立総合病院が用意した回線に集約することにしました。病院へのサイバー攻撃の侵入経路として部門システムのリモート保守回線の脆弱性が狙われるケースが多いからです。リモート保守回線を同院が一括管理することでシステムベンダーとの責任分界点も明確になります。
これでサイバー攻撃対策は一段落と安心していたところに、衝撃的なサイバー攻撃事案が発生しました。2022年10月大阪の大規模な病院で、給食事業者とつながるネットワーク経由で侵入されてランサムウェアの被害が発生したのです。
「いくら病院自身がきちんと管理していても、取引先から正規の通信を装って侵入されるとなるとお手上げです。不正な通信を検知してアラートを飛ばすシステムでは、防ぎようがありません。頭を抱えましたが、もはやサーバに侵入されることを前提に対策を考えるしかないと方針を大きく転換しました」（守屋氏）

■AppGuard導入前の取り組み

日本最北端の救命センターを持つが、広大な北海道では救急車搬送に3時間を要すこともあり、インターネットを活用した医療ICTを早くから実施。数ある医療ベンダーが利用するネットワーク回線の集約などセキュリティ強化の取り組みは日頃より取り組んでいた。

■感じていた課題

大阪急性期総合医療センターのランサムウェア被害から、「いかに通信を制御しても正規の通信を悪用されるならお手上げだ」と考えていた。エンドポイントまで到達される前提での対策を模索したが、EDRなどの検知と対処のために24/365での監視体制を整えるリソースはないと判断していた。

■AppGuardでの解決

「やって良い事しかできない」という思考は今のサイバー攻撃に対抗する唯一の手段だと共感。また侵害されないことに重点を置く対策であり、24/365での体制を整えなくても望んだ対策を実現した。

サイバー攻撃者との戦いに終止符を打つ

侵入されても発症しない

APPGUARD