

# AppGuardご紹介

2025-08-27

ITガード 小川真佳

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頻発したことを受け、「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りました。」(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を支える存在となっています。一方で「外とつながることになると、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」という目標を掲げさまざまな対策を進めました。まず、万が一被害を受けたとしても、電子カルテと医療会計のデータだけは守られるようにオフライン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、それらを部門システムのベンダーが固め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なりました。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固型接続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故が発生しました。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。「いらい病院自身がきちんと管理しているつもりで侵入されるとお手上げです。不正な通信を検知してアラート飛ばすシステムでは、防ぎようがありません。頭を悩ませましたが、もはやサーバに侵入されることを前提に対策を考えないかという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 との棲み分けて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後継報道されています。この事態を踏まえ津山中央病院では、万が一備えた字種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機

500 以上の病床数を擁す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います。最近しばしば「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ぬ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「クラウドなネットワーク」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さず運用してきました。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発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、万一被害されたら甚大な影響を受けてしまうだろうという危機が高まってきました。」(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新のウイルスは防げません。」(村上氏)。こうした危機に加え、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んできました。

まず、万が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に、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、それでも一瞬の不安は拭きませんでした。「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うのは、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、電子カルテをはじめ、各医局・検査システムなど約 200 台のサーバが仮想基盤上で動作しています。「中でも、病院の申でどうしても守らなければならないものがあります。電子カルテ、オーダリングシステム(医療会計)、そして PCR 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、「システムに必要な最小限のサーバ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、電子カルテや医療高門システム、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。

病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・ポリシーによる標準化、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、最速で対策の組み合わせを構築しています。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

一般財団法人津山慈風会  
**津山中央病院**  
Tsuayama 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

 **埼玉医科大学病院**  
Saitama Medical University Hospital



970床

1053床

700床

特定医療法人 佐藤会  
**弓削病院**  
HOSPITAL YUZE



108床



## 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：堀 常雄  
〒102-0075 東京都千代田区三番町 9-1F  
ホスピタルプラザビル 1F  
TEL. 03-3264-9888

#### 取締役交代のお知らせ

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、日病病院総合医療事業の各種委員、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。

新型コロナウイルス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よう尽力いたす所存です。どうぞよろしくお願いたします。

#### ●役員一覧

代表取締役 堀 常雄 専務取締役 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 (代表) 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

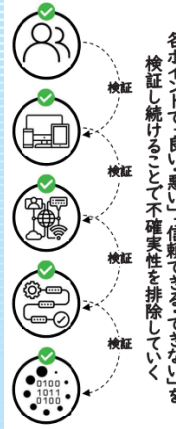
#### 侵入されても発症しない 新しいサイバー攻撃対策のご案内

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 (アップガード)」は、米国防総省 (俗称：ペンタゴン) を含む、複数の米国防務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円形病院等、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。



各ポイントで「良い・悪い」信頼できる「まがら」を  
検証し続けることで「不確実性を排除していきな

下ポイントセキュリティ対策ツールは「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」が継続的に実践されているか検証、不正アクセスの成立) が発生し

害 (US Patent #7712143) を含む、複数の米国防務機関ウェアが米国防軍の定めるセキュリティでも ANA や JTB といった 6 月時点で 17,000 社以上に導入されていることを紹介します。

を調じられること  
がる行為を一切成立させない環境と一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ワートポイントで対象イベントに制御を即エンジも 1MB 以下と軽量化が

なセキュリティ対策に加え、振るう手法を使ったサイバー攻撃やきまとなっていました。いつまでもぐに導入を決定。防御力が高まことで、導入前に比べてノン

セキュリティリスクを洗い出し、日々

担当：熊谷 (くまがい) 時まで ※年末年始を除く)

## 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：堀 常雄  
〒102-0075 東京都千代田区三番町 9-1F  
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担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

米国防総省 (俗称：ペンタゴン) を含む米国防務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。

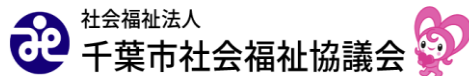
「AppGuard」は、「ゼロトラスト」の概念を実装したエンドポイントセキュリティ対策ツールです。端末やサーバー上で「やって良いこと・悪いこと」を明確に規定した上で「やって良いこと・信頼できること」だけが継続的に実践されているか検証し続け、イレギュラー (コンピューターウイルス等のマルウェアの発症、不正アクセスの成立) が発生しない環境に作り変えます。

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、名古屋立総合病院など、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>

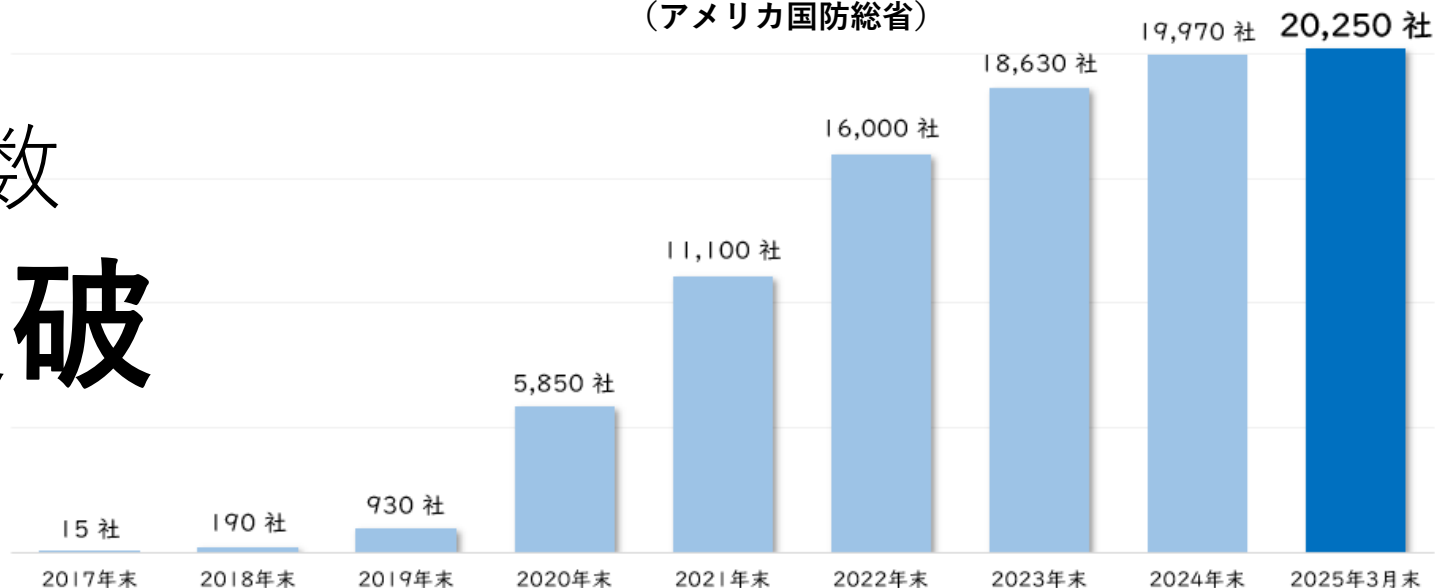
株式会社日本病院共済会 営業統括部 熊谷 TEL：03-3264-9888 (平日 9 時 ~ 17 時)

# 国内における導入実績



(アメリカ国防総省)

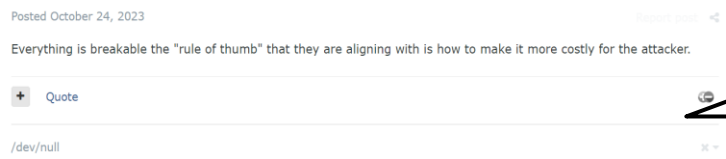
## 国内導入累積社数 20,500社突破 (2025年6月末時点)



# 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

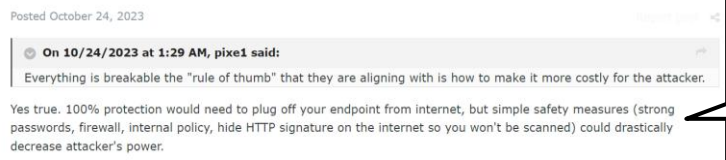
## ▶ ダークウェブ上のハッカーフォーラムの投稿から読み解く



意識：（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。



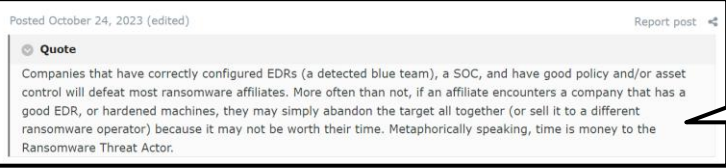
攻撃コストが低い組織は標的にされる。



意識：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



意識：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。

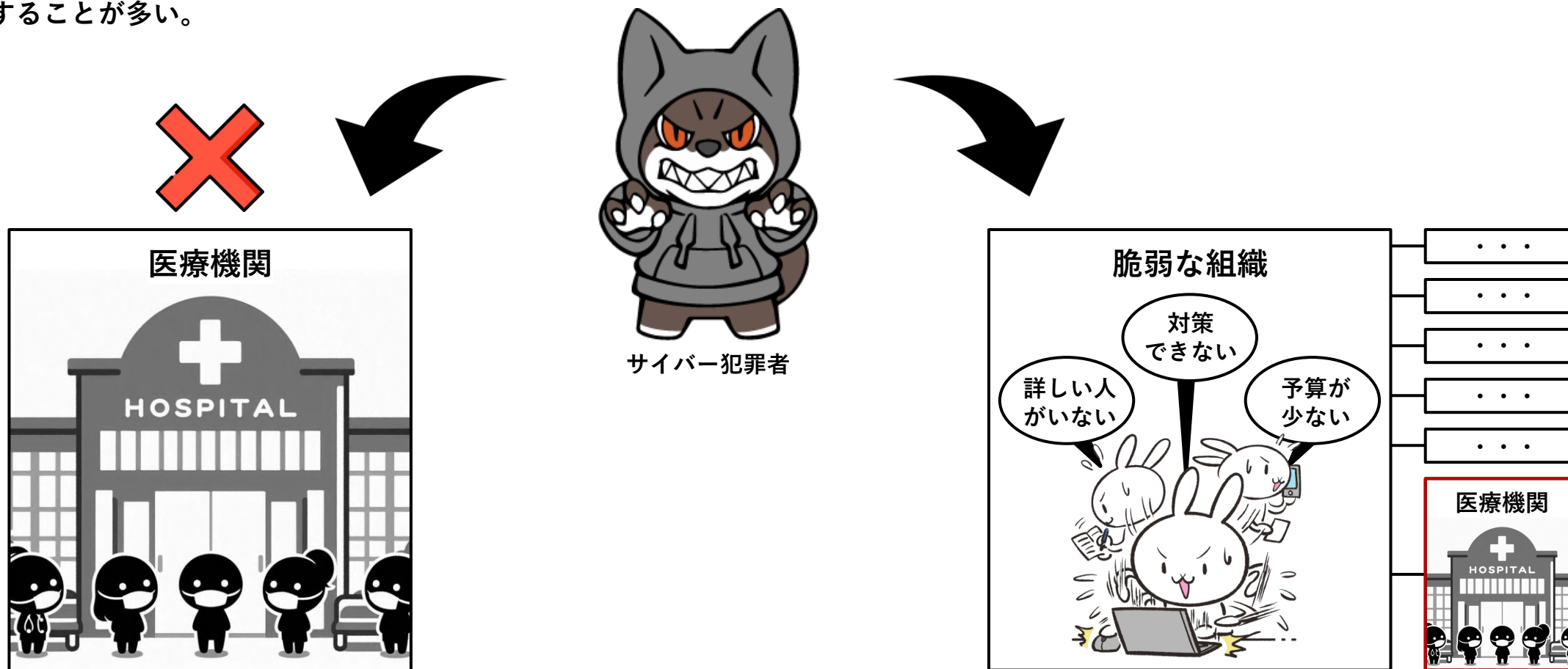


攻撃コストが低い組織を見つけた場合、最後まで攻め上げる。

# サイバー犯罪者は医療機関を狙っている？

## ▶ 低コストで攻略可能な相手を標的にする

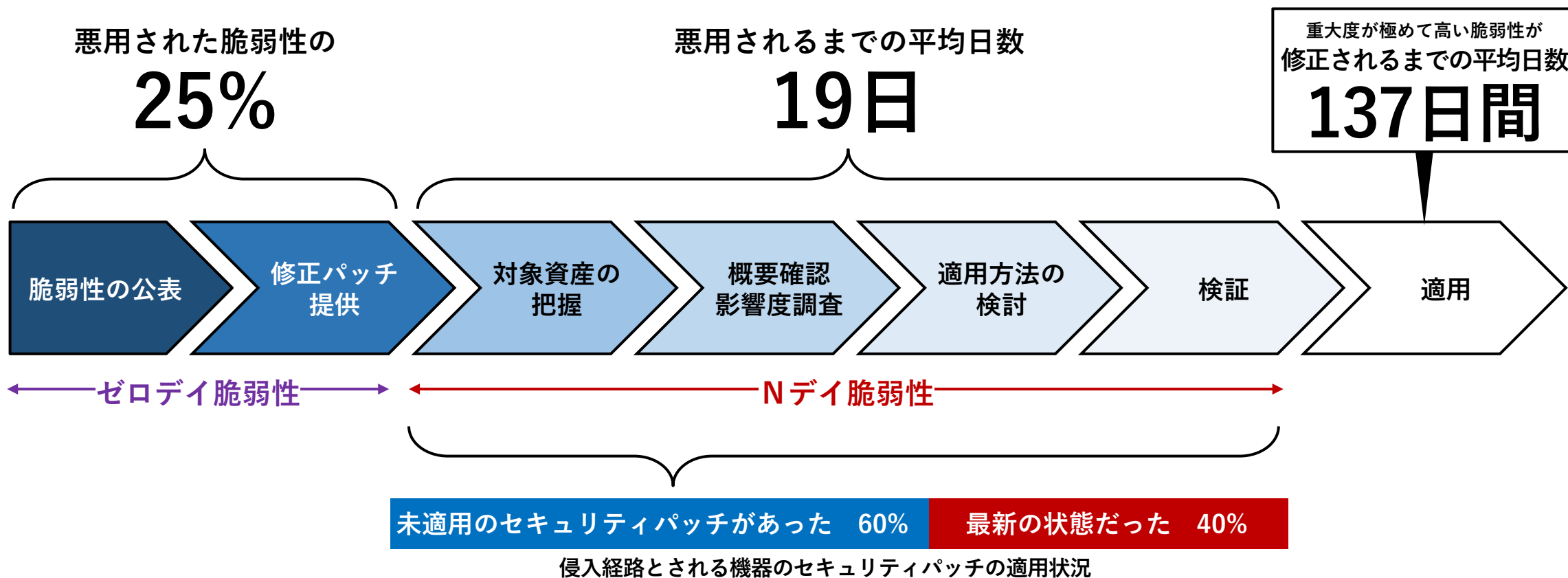
特定国家に関連付けられたサイバー犯罪者を除けば、その多くは侵害に際して低コストな（労力があまりかからない）相手を探し出して攻撃を仕掛ける傾向にある。つまり、医療機関だとわかった上で侵入するのではなく、侵入した結果、医療機関であると認識することが多い。



# 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。



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」

# AppGuardとは

**AppGuardと  
他製品の  
違いは何か？**

他製品



◆ 攻撃の特徴を学習

◆ 攻撃を検知

◆ 侵入を防ぐ

アラートで知らせる



侵入されると

防ぐ術がない

# AppGuard



- ◆ 業務で使用するアプリケーションをAppGuardに登録
- ◆ 登録した挙動以外は即時すべて止める



侵入されても

攻撃を

すべて止める



インシデントが

発生しない

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

規定したことを以外は  
『誰であって』 『どんなことでも』

実行できない

APPGUARD

項目	AppGuard	アンチウイルス
役割	悪い事ができない端末環境を作る	悪いものを見つけて排除する
マルウェアの検知	× (検知機能なし)	○ (検知機能あり)
マルウェアの駆除	× (駆除機能なし)	○ (駆除機能あり)
マルウェアを用いない攻撃への対応	○ (保護可能)	× (検知不可)
正規の権限を悪用した攻撃への対応	○ (保護可能)	× (検知不可)
正規の機能を悪用した攻撃への対応	○ (保護可能)	× (検知不可)
未知の攻撃への対応	○ (保護可能)	△ (検知困難)

# AppGuardと事後対策(EDR)の違い

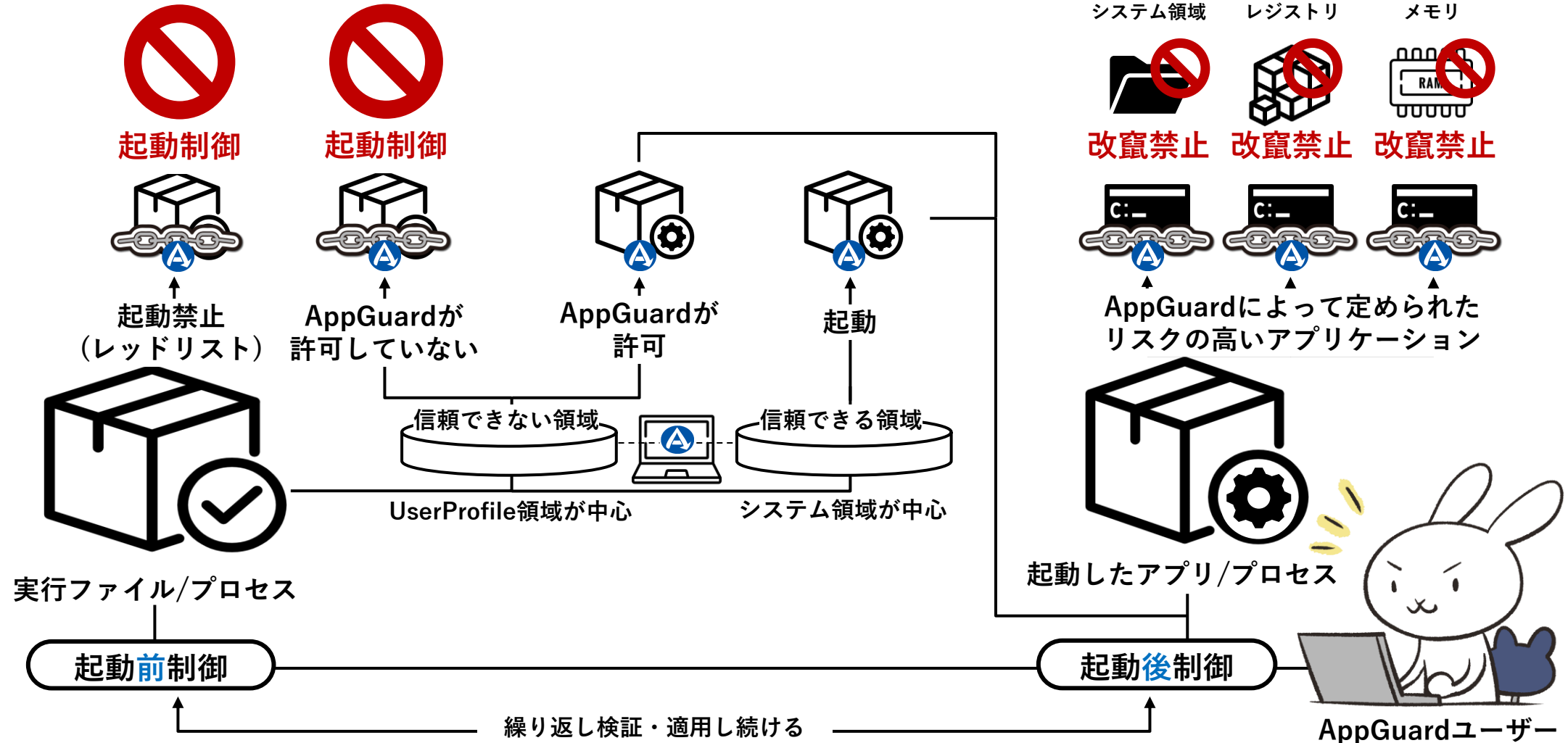


項目	AppGuard	事後対策 (EDR)
区分	予防	事後対応
提供する機能	アプリケーションとプロセスのゼロトラスト化	NIST SP800-171に基づく防御・検知・対処
期待する成果	攻撃の成立を阻止	脅威の検知・特定及び関連イベントの 相関関係整理
成果を得るための手法	許可したことのみが実践されているか継続検証	侵害中又は侵害された痕跡と モデルデータの照合
機能するタイミング	攻撃実行前	攻撃実行後
トータルコスト (ライセンス+サービス+社内人件費)	安い	高い
未知の脅威対策	○	△
環境寄生型攻撃対策	○	△
未知の脆弱性対策	○	△
脅威の特定/攻撃の 可視化	△	○
レポートニング	×	○

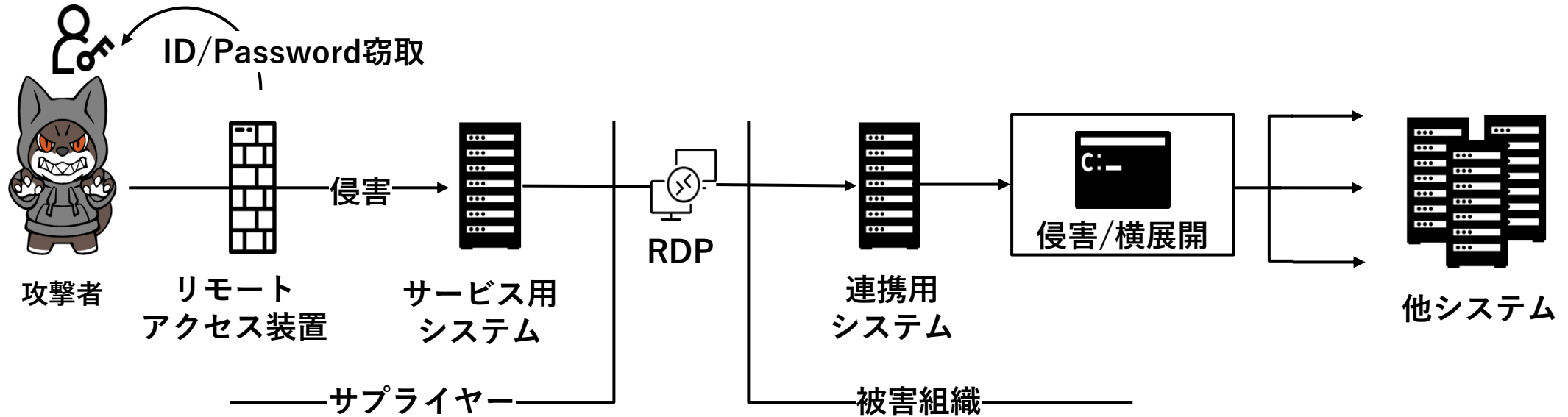
# 攻撃プロセスの成立を阻止する仕組み



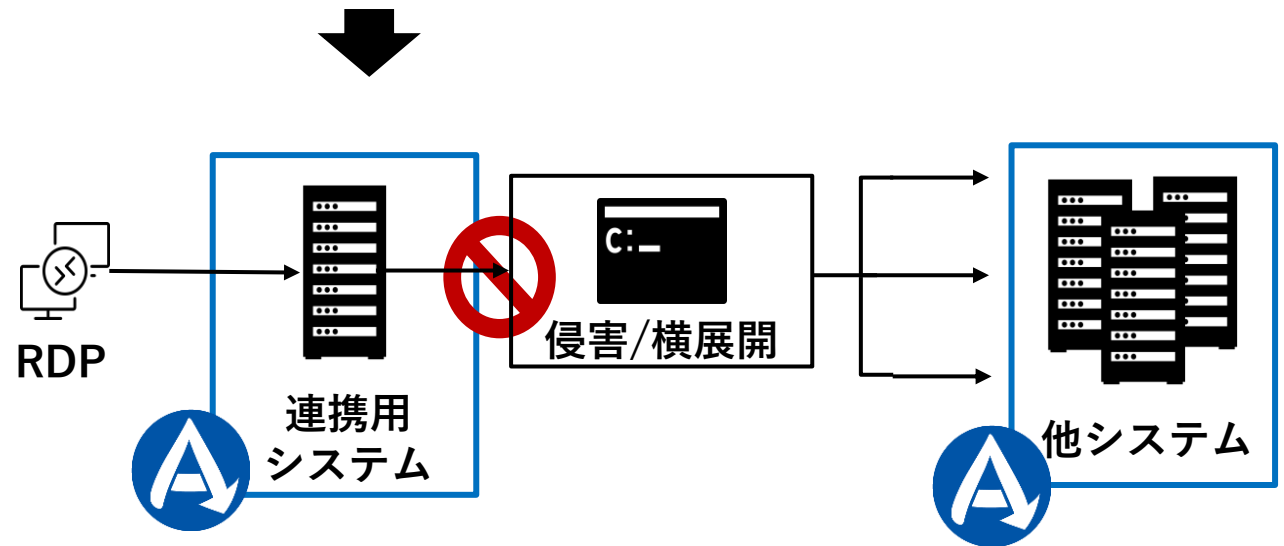
- ① 普段ユーザーが利用しないようなアプリはそもそも**信頼せず起動禁止**
- ② ユーザーが利用する**アプリは信頼が与えられた場所**からでない**と起動が出来ない**
- ③ 起動許可したアプリであっても**常に監視し続ける**



# AppGuardの攻撃阻止パターン

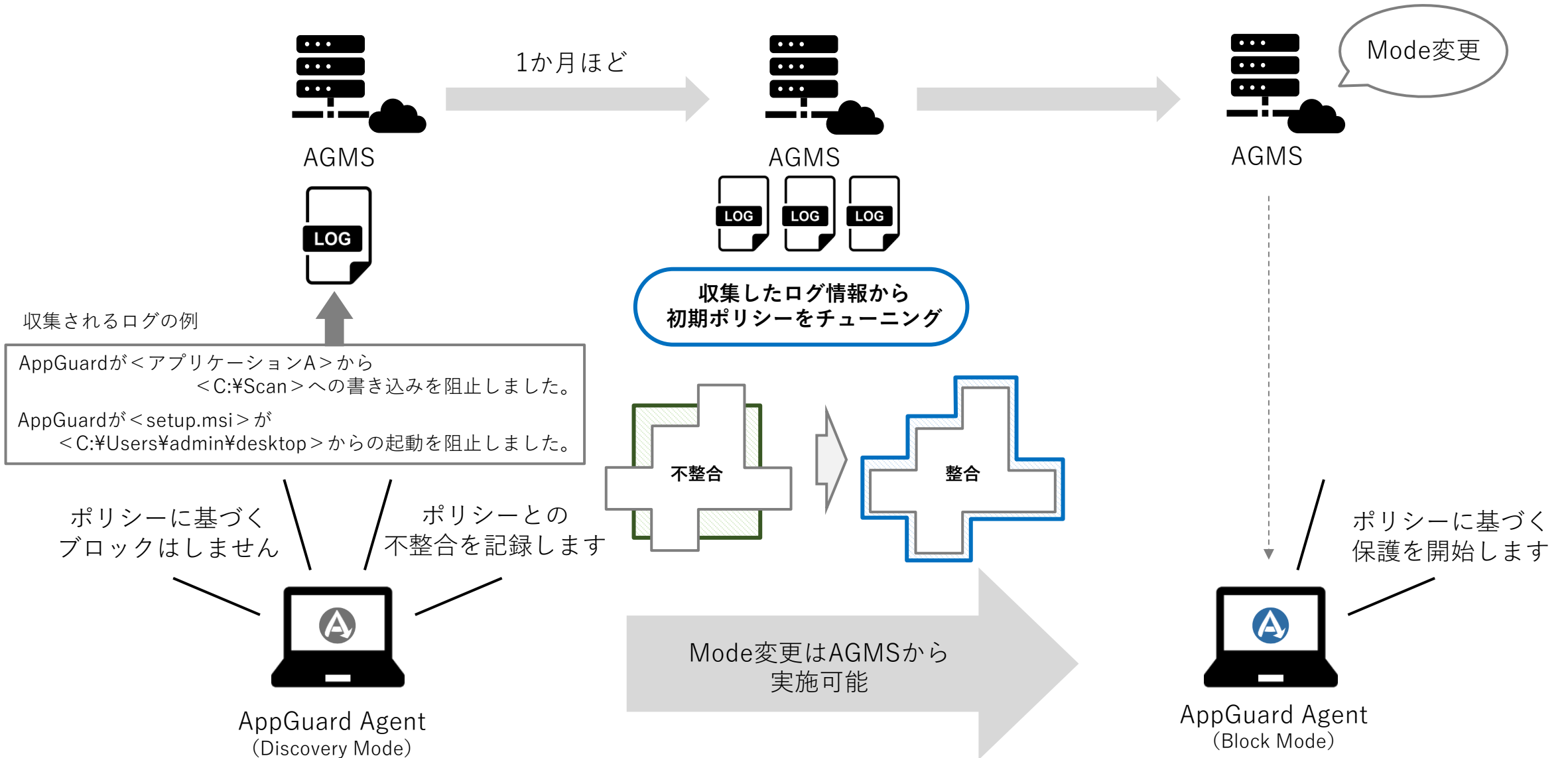


侵入できたとしても  
システムを侵害する行為を  
成立できない



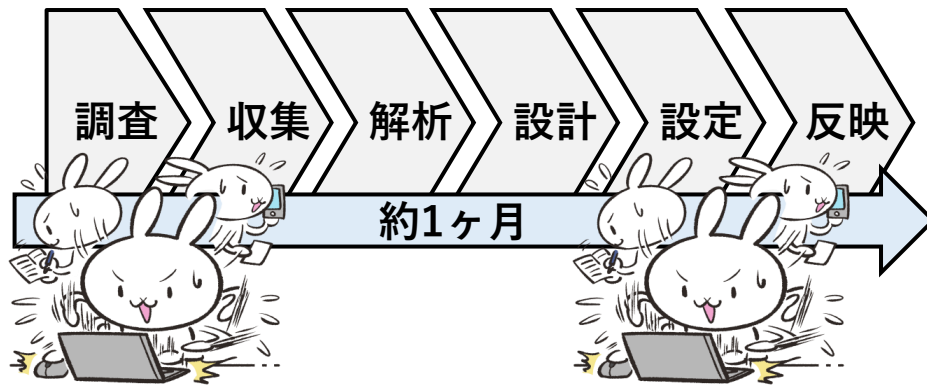
# Discovery Mode

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



## 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

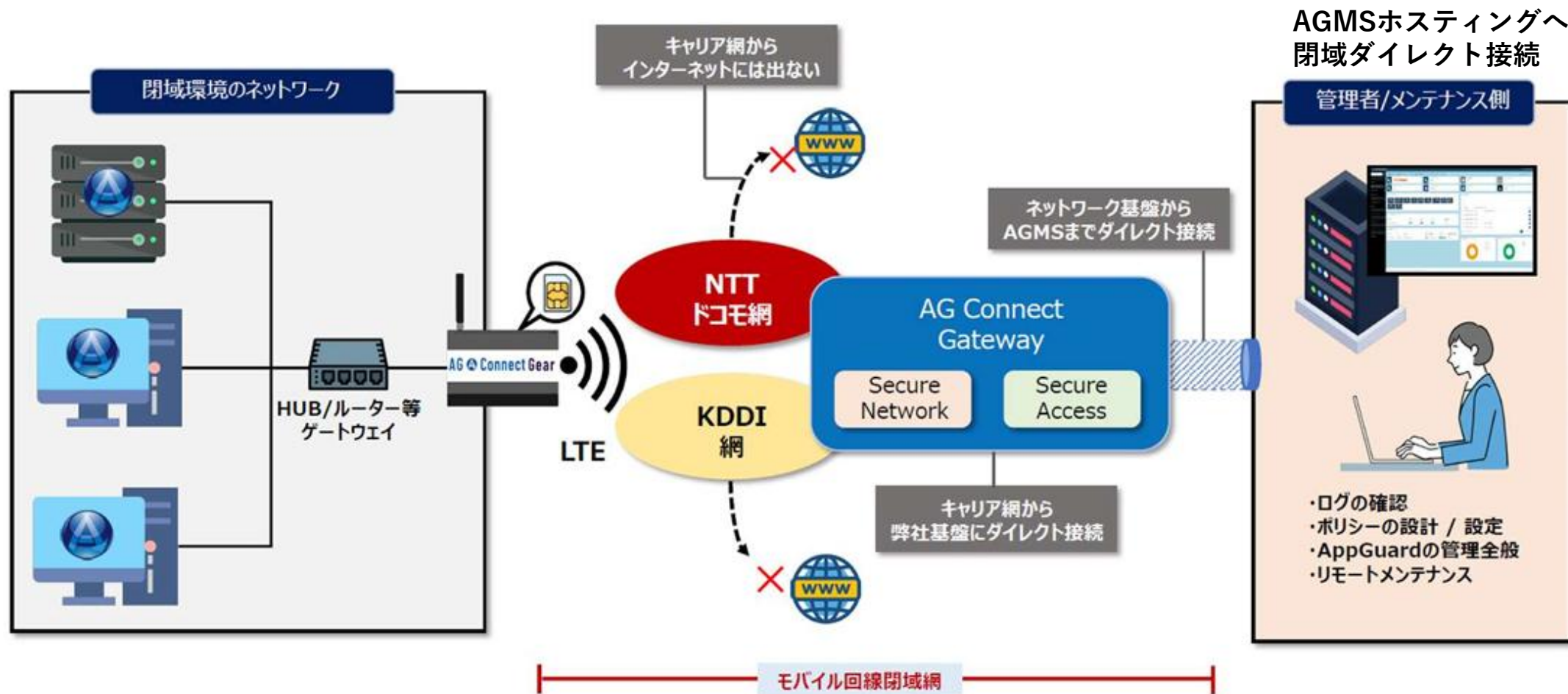
### AppGuard運用パッケージ

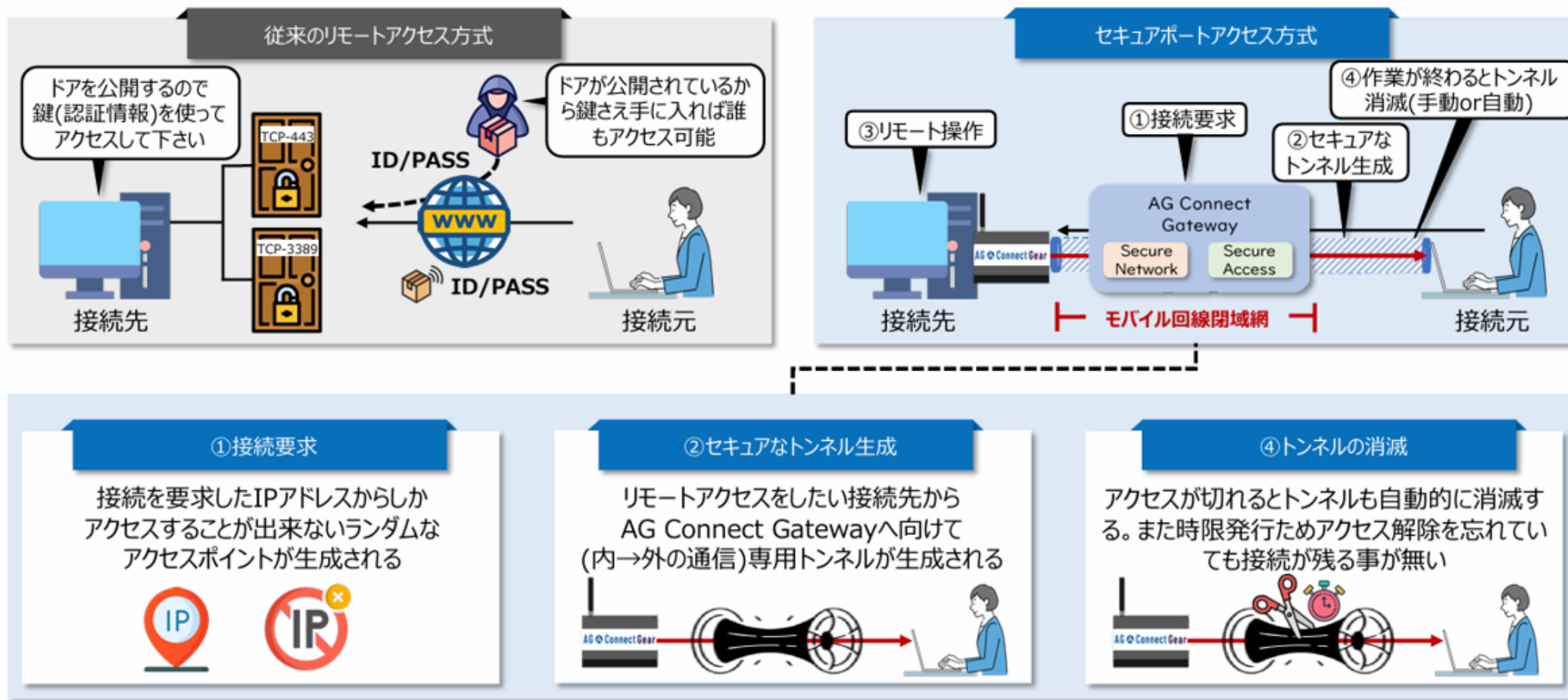


AppGuardの運用を支援するサービスデスクをご提供し基本的な操作方法だけでなく、お客様に代わって調査・解析に基づくポリシー設計・設定・反映なども実施します

# 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





- ✓ 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

① 死守したい端末やサーバー

② レガシーOS

③ 閉域環境

## 死守したい端末やサーバー

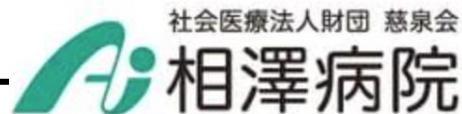
- 被害が甚大となる  
ADや電子カルテサーバーへ導入
- 攻撃されても医療を止めない  
システムの掌握も阻止

## レガシーOS

- Windowsのサポート切れOSも  
保護能力を落とさず守る
- 脆弱性を悪用した侵入も  
インシデントにつながらない

## 閉域環境

- パターンファイルの更新なし  
外部インターネット未接続の  
閉域環境も保護可能
- 検知をしないため負荷が軽い



- ・ 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

## 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



- ・ 院内の全PC(約200台)への導入



- ・ 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)



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



- ・ 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



“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

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機

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。最近ではしばしば「医療のデジタル化」が課題になりますが、津山中央病院は、1990年代後半という他の病院はもろ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り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ようという危機が高まってきました」(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)。こうした危機に加え、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きませんでした。「EDRの検知に引っかけると時点で、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うとは、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、電子カルテをはじめ、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(医療会計)、そしてPCを動かすためのドメインサー

## ■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。



“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頻発したことを受け、「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故が発生しました。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

