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

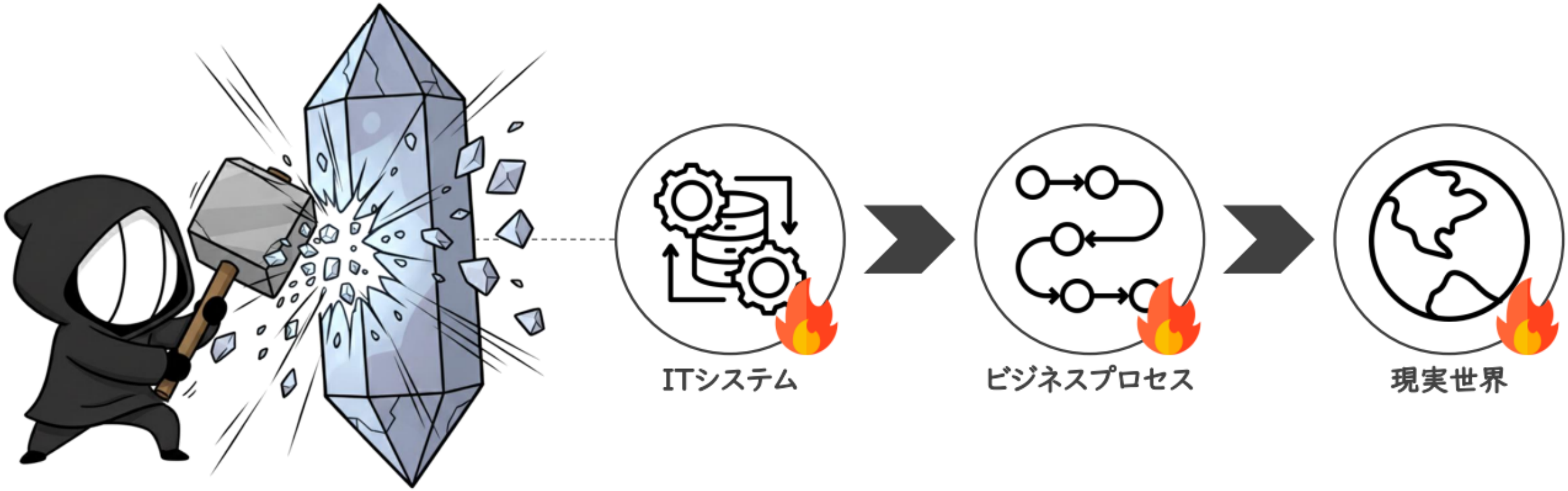
攻撃者の考え方とは

サイバーフィジカル・リスクによる脅威

APPGUARD

[サイバーフィジカル・リスクとは]

従来のサイバーセキュリティは、主に「情報」を守ること、すなわちデータの漏洩や改ざんを防ぐことに焦点が当てられてきた。一方、サイバーフィジカル・リスクとは、サイバー攻撃がデジタル空間を飛び越え、現実の物理世界に直接的な被害をもたらす危険性である。最大の違いは、守るべき対象である。従来の「情報（機密性）」の損失リスクに対し、こちらは人命や社会基盤の「安全（Safety）」と「安定稼働（Availability）」そのものが脅かされる点にある。



サイバー犯罪者が持つ基本的な考え方

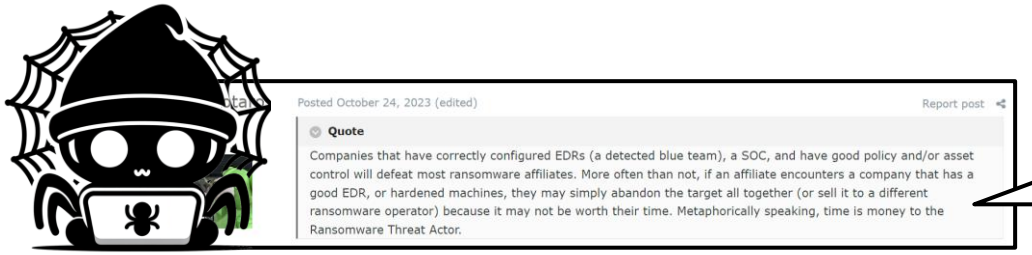
▶ ダークウェブ上のハッカーフォーラムの投稿から読み解く

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。

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

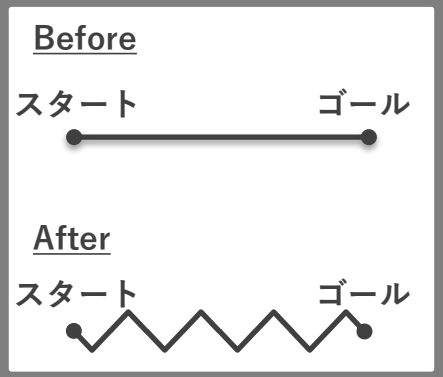
APPGUARD

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

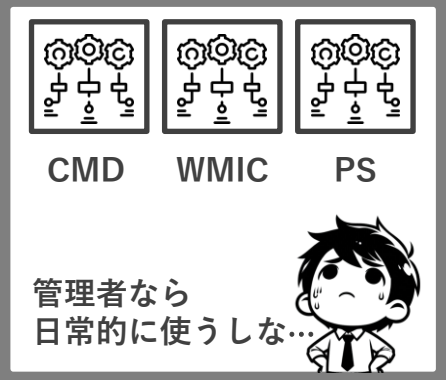
回りくどい



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

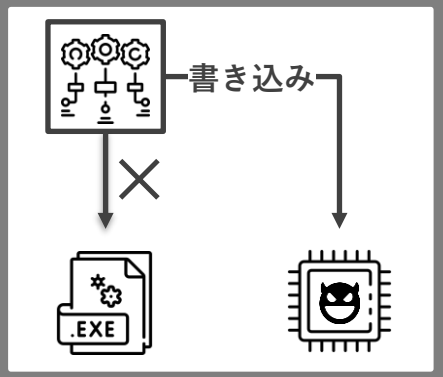
極めてグレー



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

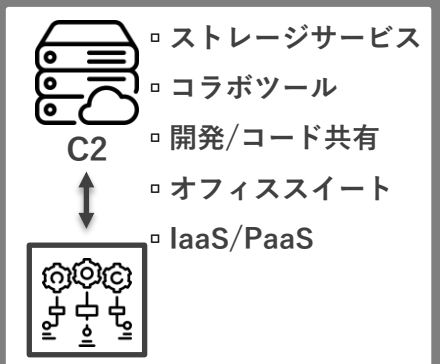
ファイルがない



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

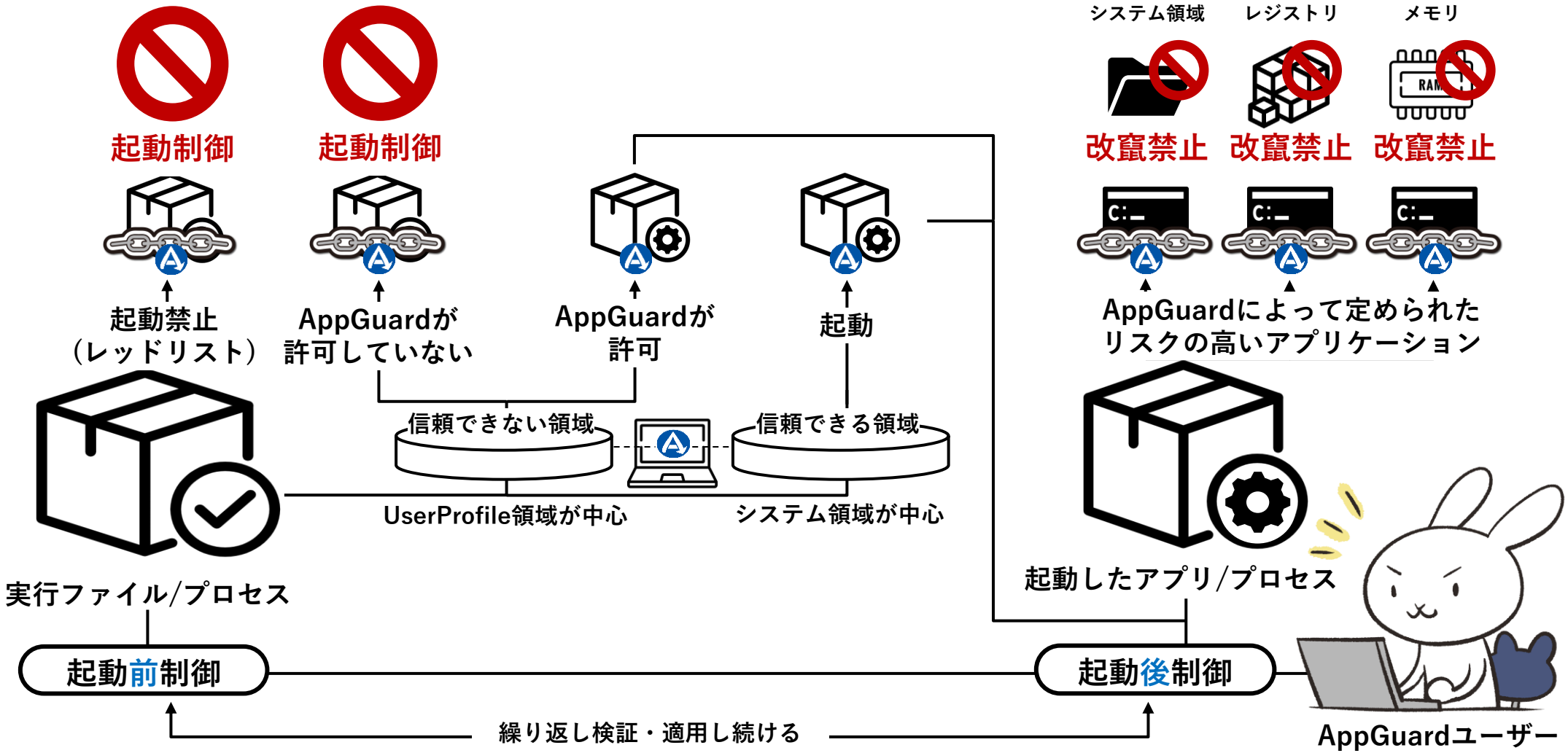
AppGuardの保護の特徴-アンチウイルスやEDRとの比較-

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

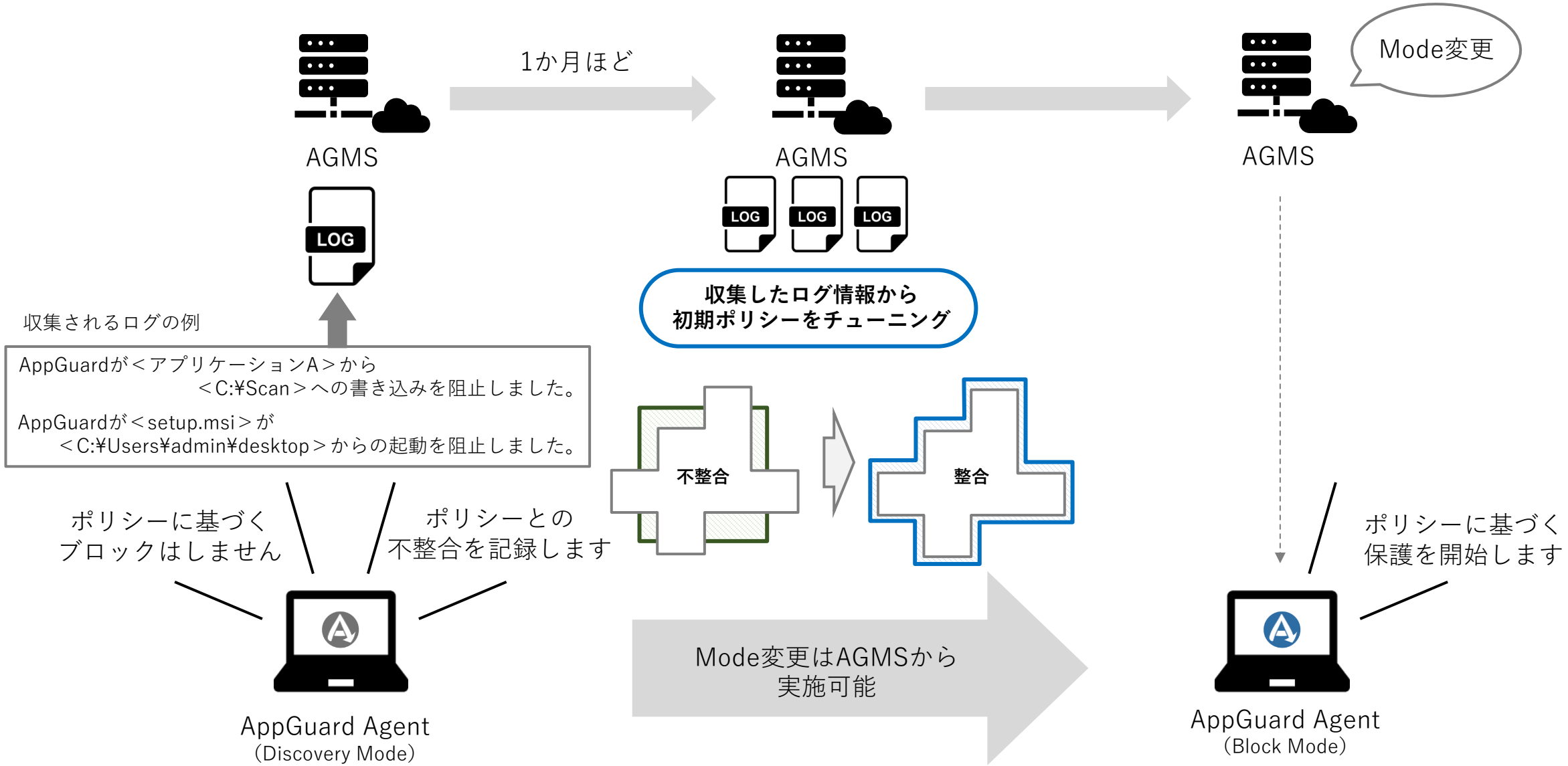
攻撃プロセスの成立を阻止する仕組み

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

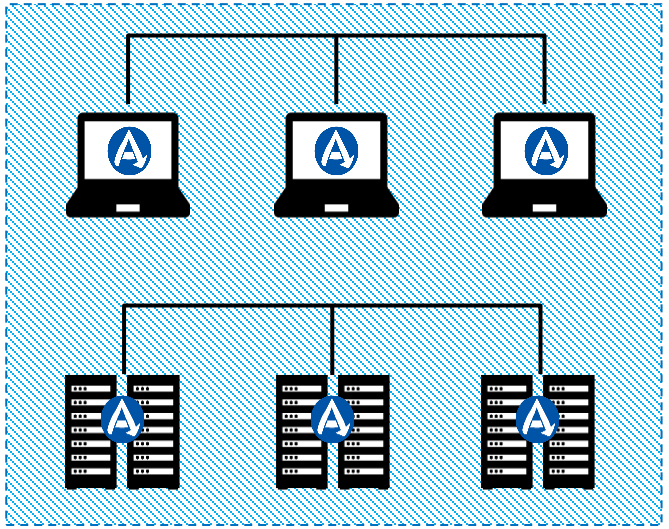
※各種支援メニューの内容は販売店によってサービス名及び提供仕様が異なります。詳細については各販売店にお問い合わせください。

AppGuardの得意領域・導入事例

AppGuardの部分導入事例

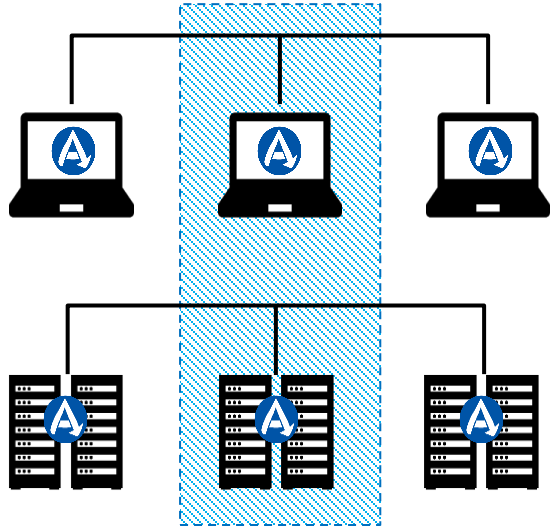
APPGUARD

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

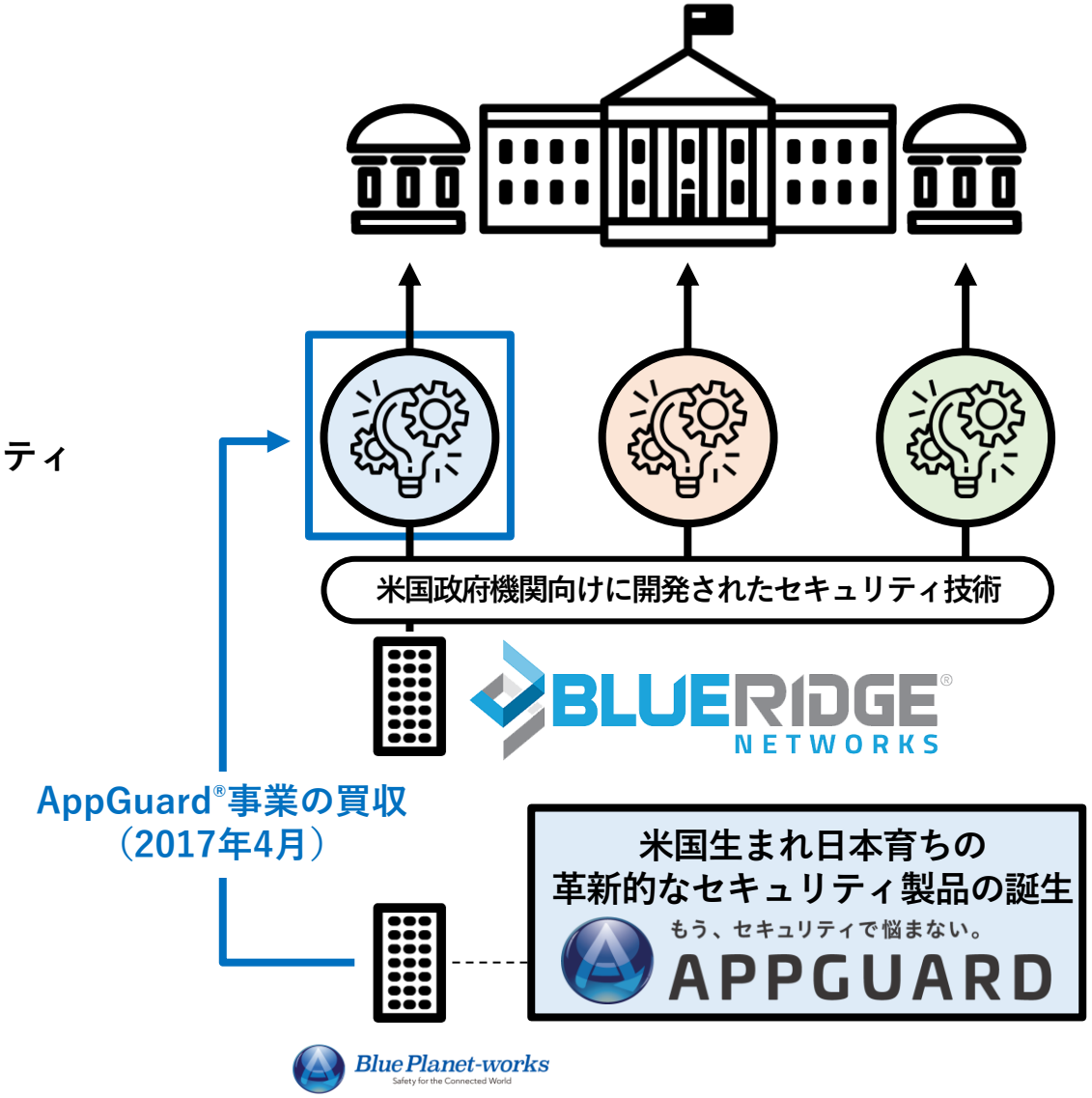
- Microsoftのサポートが切れたレガシー
  OSも保護能力を落とさず守ることが可能
- 脆弱性を利用して侵入されても
  攻撃が成立しないため安心

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

株式会社BluePlanet-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	87億円（2024年3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（2024年3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



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。

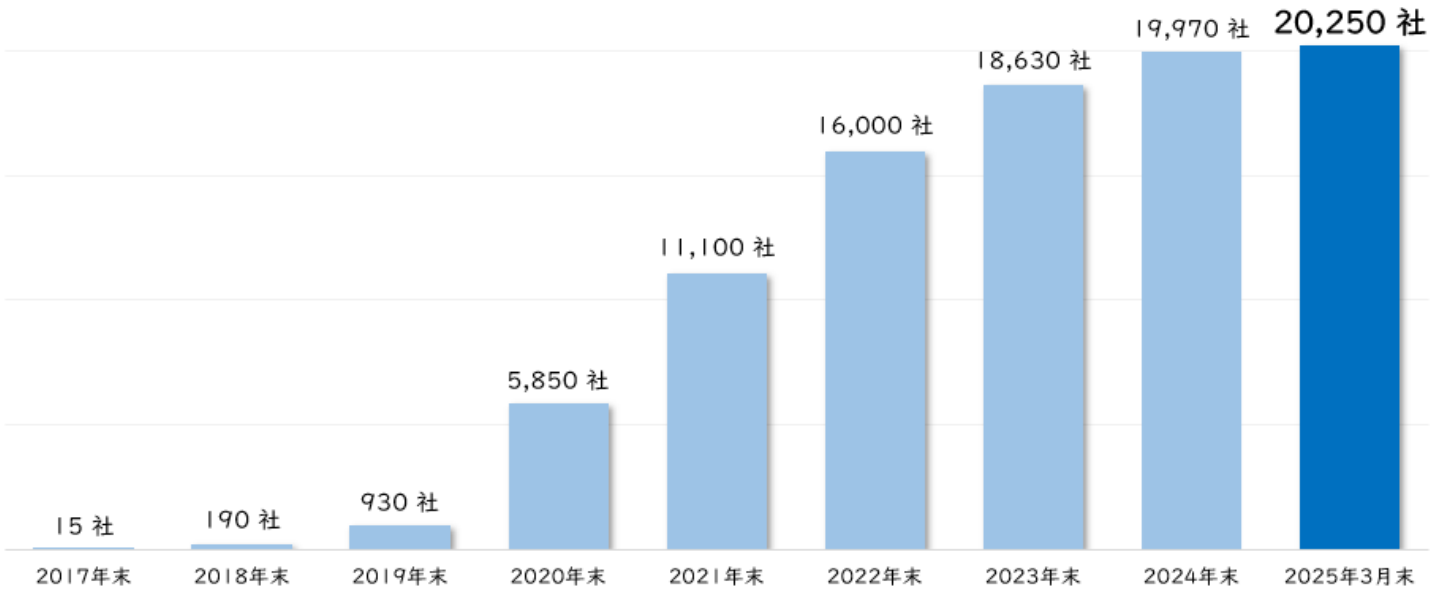
戸田建設　DAIKO XTECH　人・街・未来をまもる 東洋テック　pci PCI Solutions INC.　KAKUDAI

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）



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