Blue Planet-works
Safety for the Connected World

AppGuardのご紹介

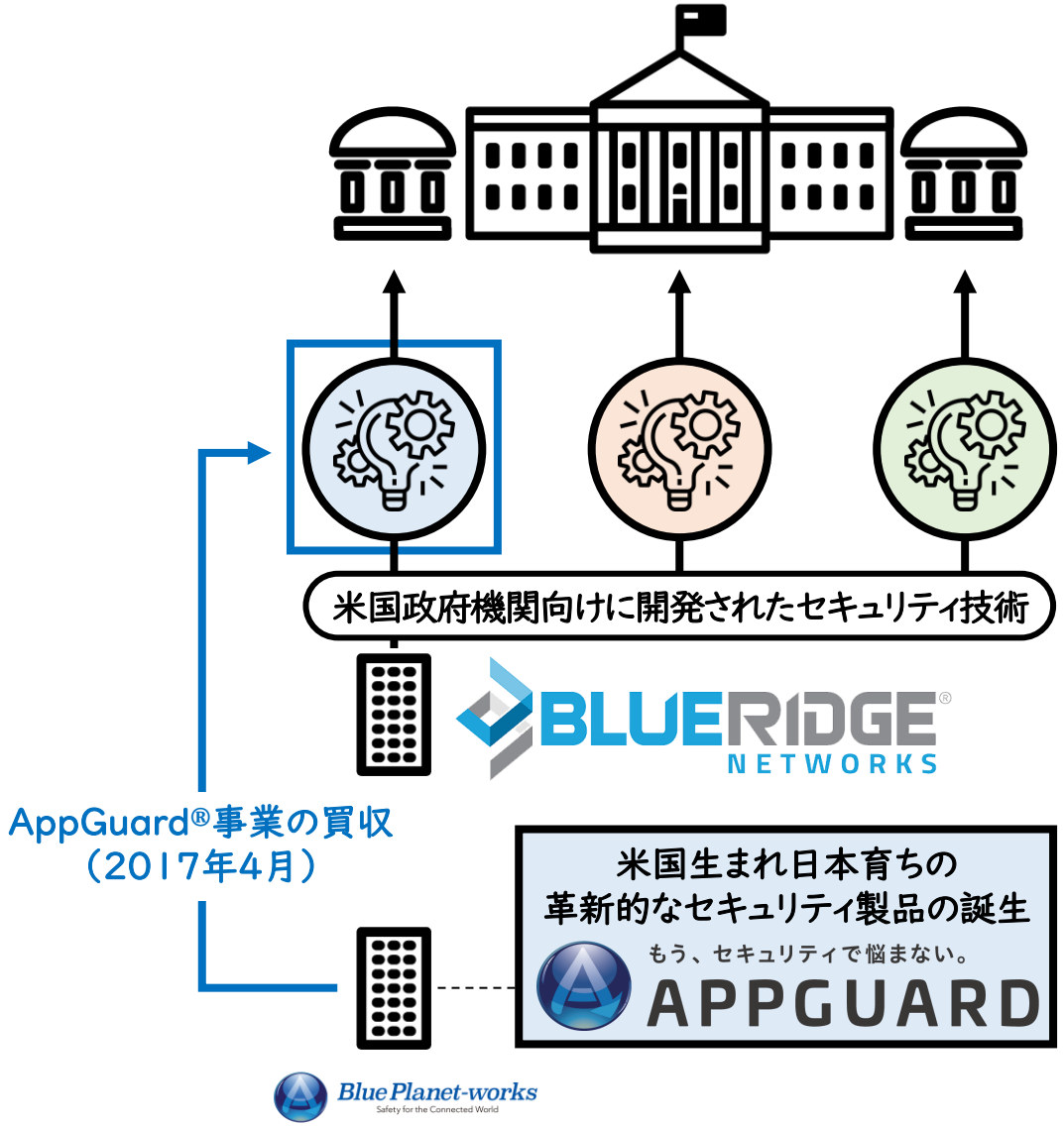
～ゼロトラスト型エンドポイントセキュリティ～

株式会社Blue Planet-works

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）

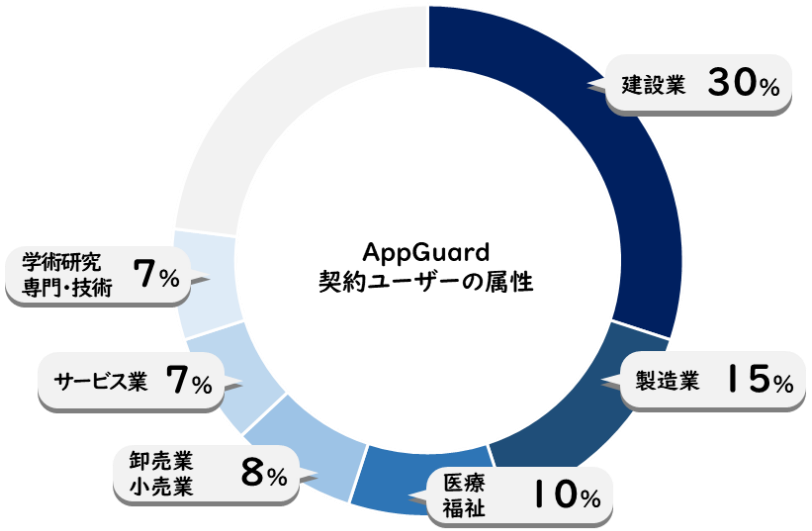
Blue Planet-works
Safety for the Connected World

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）

	2017末	2018末	2019末	2020末	2021末	2022Q1	2022Q2	2022Q3	2022Q4	2023Q1
系列1	16	189	928	5,843	11,097	12,231	13,890	15,040	15,974	16,687

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

理由①

いずれの検出技術も
過去の情報に依存せざるを得ない

過去の脅威から特徴点を抽出して教材として利用することで、独自の脅威判定ルールを作り出す。

機械学習解析

過去の脅威が行った振る舞いを分解して重み付けとスコアを設定し対象を評価するルールを作り出す。

振る舞い解析

定義ファイルによる照合、機械学習や振る舞いに基づく解析は過去の脅威情報から検出するための特徴点や情報を利用しているため、**構造が難読化されたものや未知のものに対して脆弱**である。

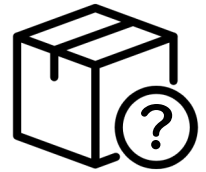
アンチウイルス

サイバー攻撃者が
圧倒的に有利な状態

攻撃者

理由②

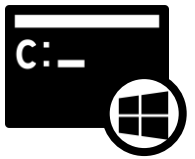
検出対象となるのは
「悪いモノ」として定義されるもの



危険かも？
要検査

不明なファイル

悪用



安全なはず！
検査不要

Microsoft提供

過去の情報に基づいて「悪性」又は「悪意ある動き」と規定されたものを検知するため、安全だと認識されている**正規のツールや機能を悪用する「環境寄生型」の攻撃に対しては脆弱**である。

アンチウイルスは長い歴史を持つが故に仕様を逆手に取った攻撃手法が多数存在している

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

<NIST（米国標準技術研究所）が提唱するサイバーセキュリティフレームワーク（NIST SP800-171）>

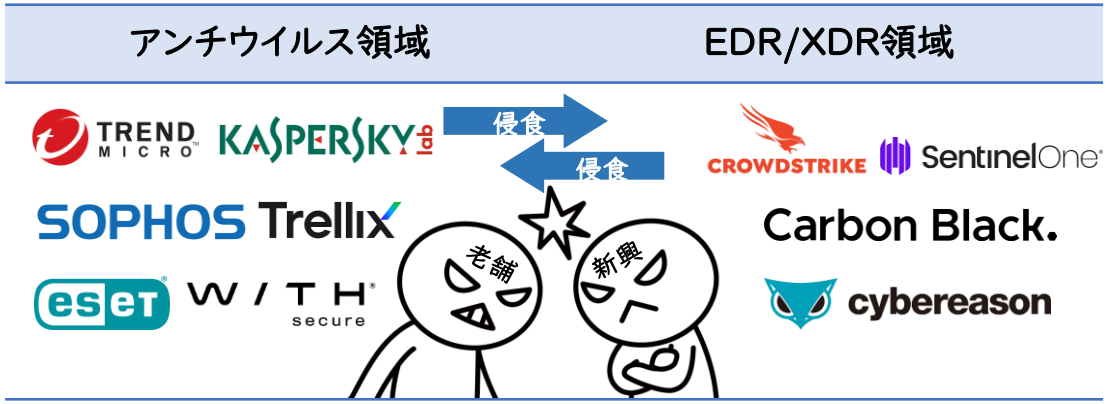
- アンチウイルスという概念だけでは脅威に対抗できないことが世界中で認知される。
- 各種ガイドラインで「可視性の向上」に投資をシフトするように言及するようになった。
- 欧米に追随する形でEDR/XDRといったソリューションが注目される。

←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）

EDR/XDR

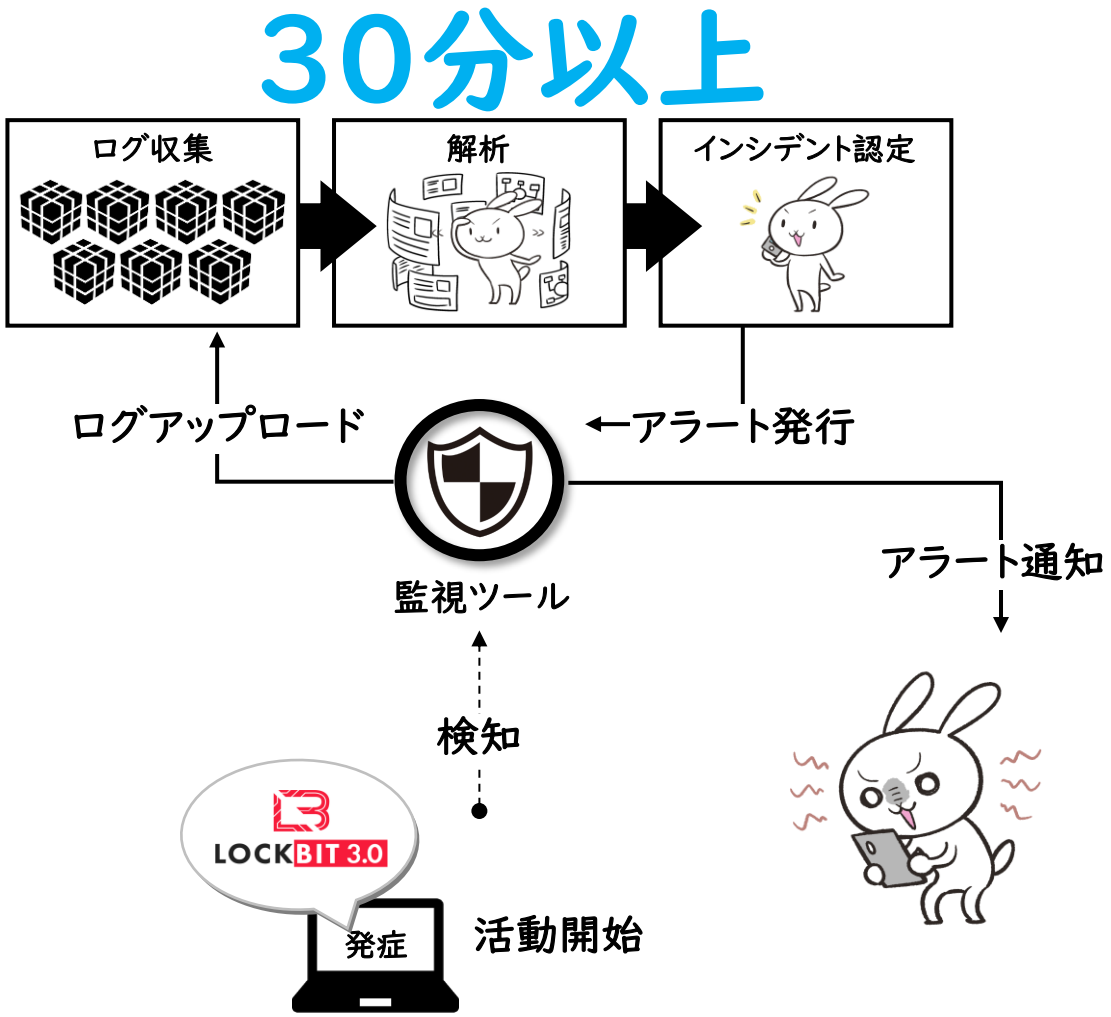
侵入されることを前提として迅速な対応によって被害拡大を防ぐことを目的として、IoC/IoAに基づいて不審な挙動や通信があれば分析し管理者に通知する仕組み。



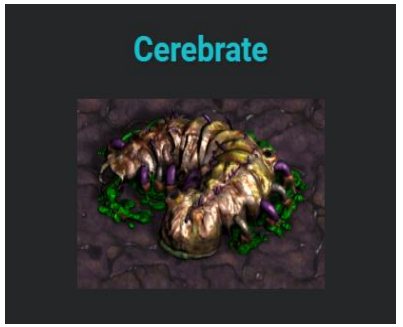
アンチウイルスベンダーはEDR/XDR領域へ製品を拡張
EDR/XDRはアンチウイルス領域へ製品を拡張

ランサムウェアの高速化

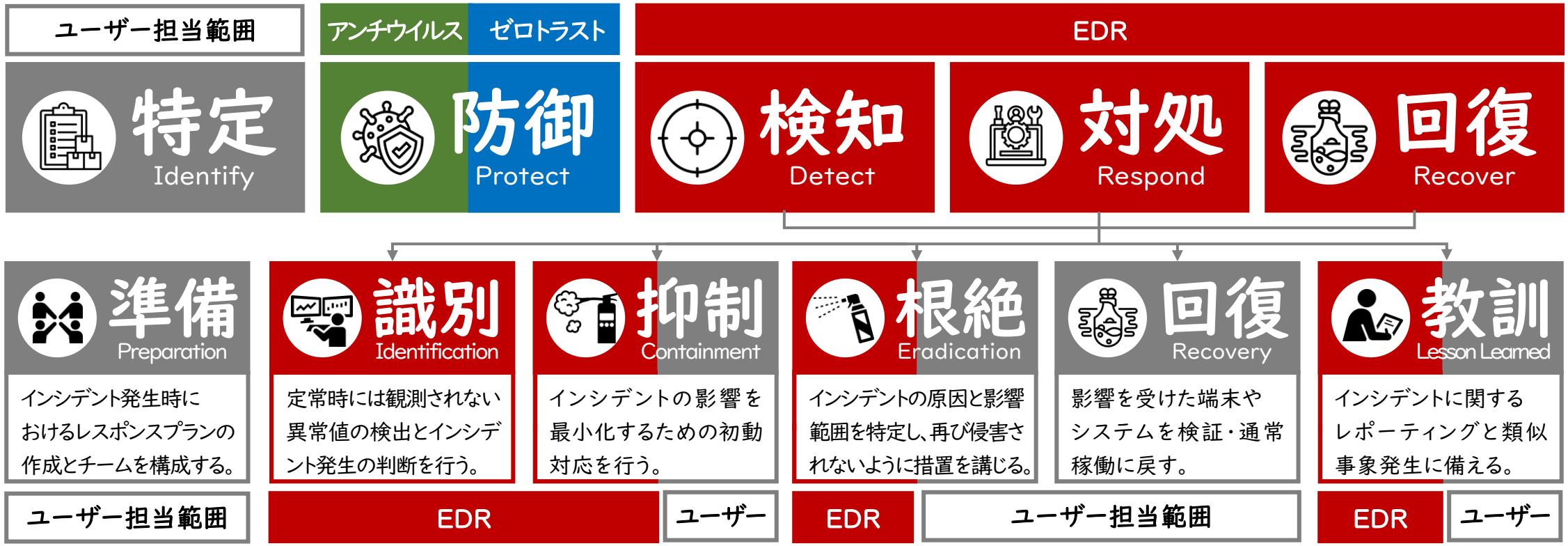
- ランサムウェアを中心にEDR/XDRの検知をバイパスする手法が検討される。
- ランサムウェアの暗号化速度を高速化することで検知を回避する手段が有効であると判断される。



高速化を謳うランサムウェア	暗号化速度	
	中央値（1GBの暗号化速度）	100GB換算（中央値×100GB）
LockBit 3.0	8秒	5~6分
LockBit 2.0	33秒	55分



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

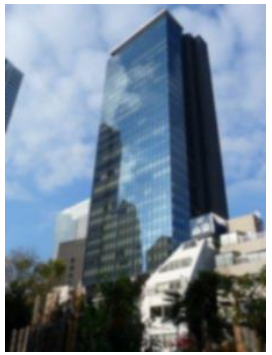
Kojima

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

「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」 -

AppGuardの守り方

Blue Planet-works
Safety for the Connected World

これまでの守り方

悪い物を見つけて排除する

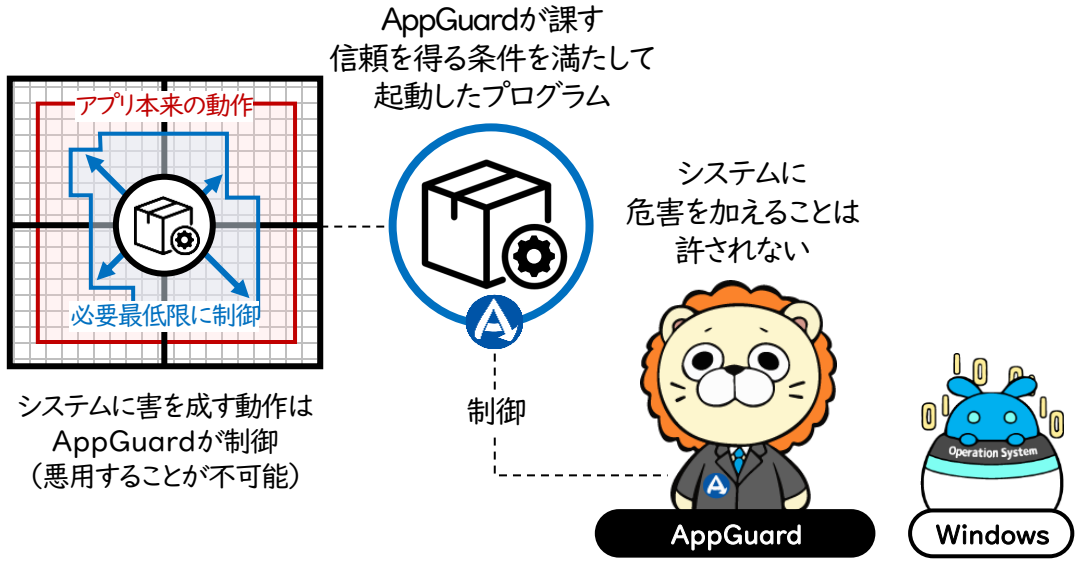
過去の情報から害を成す悪いモノを例外として排除

攻撃者は新しい攻撃を作ればよい

AppGuardが提唱する守り方

悪い事をさせない環境を作る

PCが衛生的で健康的な状態ならウイルスにかからない



ウィルス(攻撃)は発症しない

AppGuardの守り方

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~~

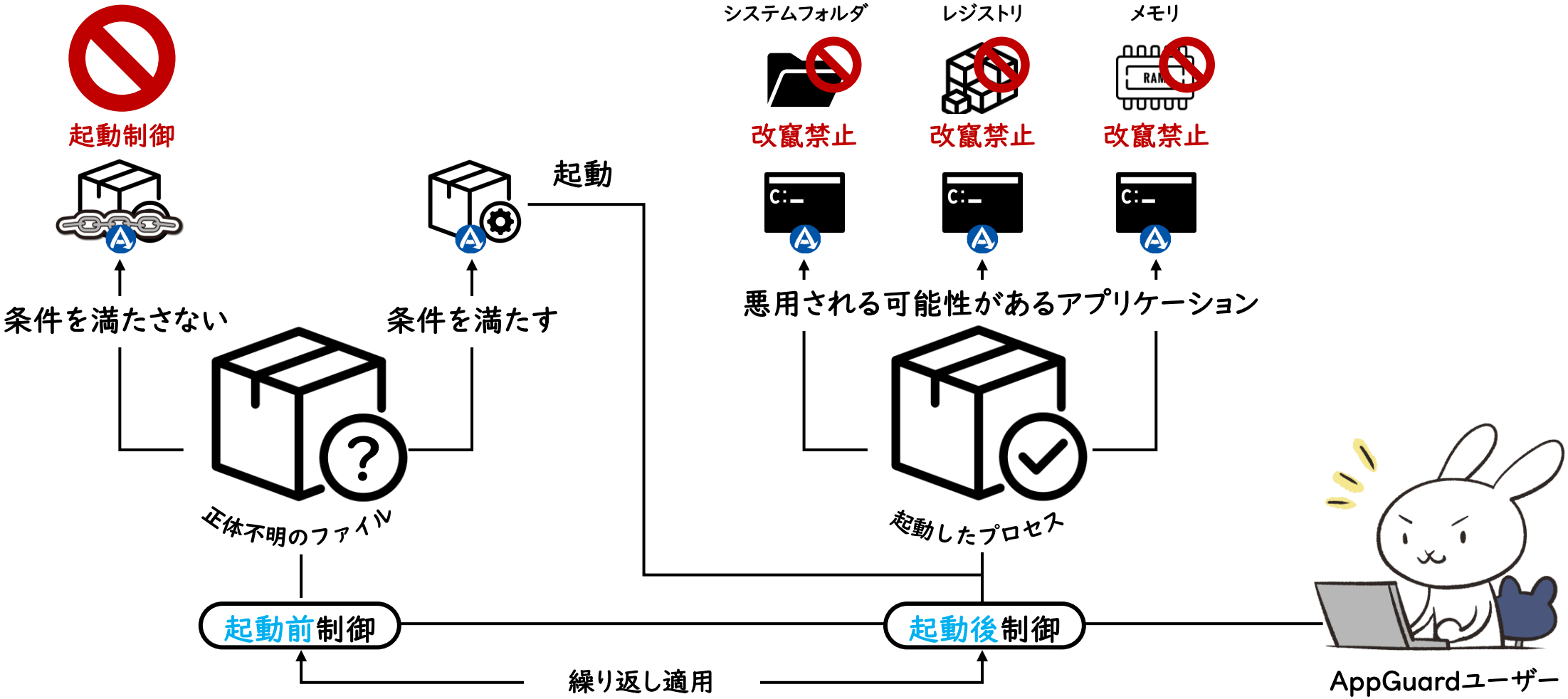
~~マルウェアの駆除~~

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

攻撃プロセスの成立を阻止する仕組み

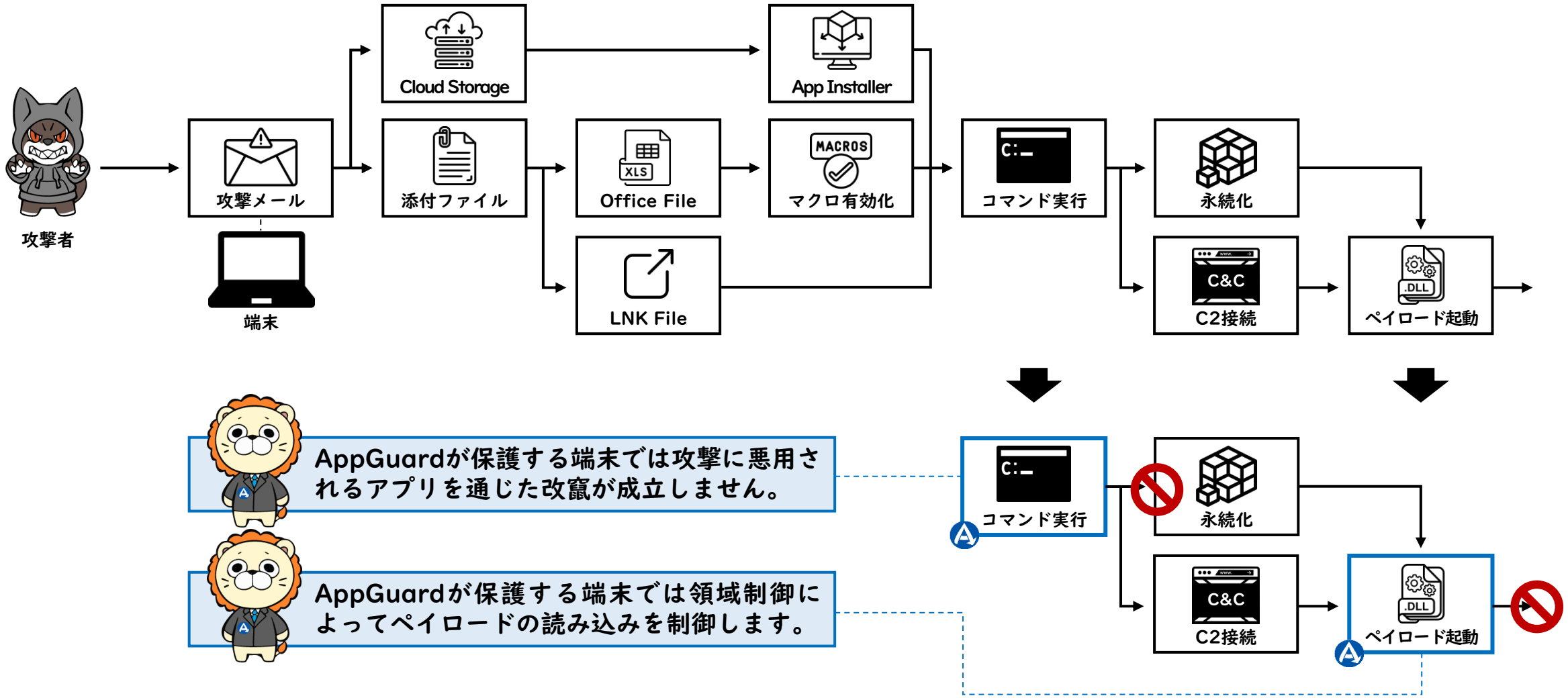
「やって良いこと・悪いこと」を明確に規定し
「やって良いことだけ」が常に実践されているか検証し続ける



AppGuardによる攻撃阻止パターン #1

Emotetが用いた攻撃パターンについて

Emotetを展開する常套手段として使われるテクニックに対してもAppGuardは貢献します。

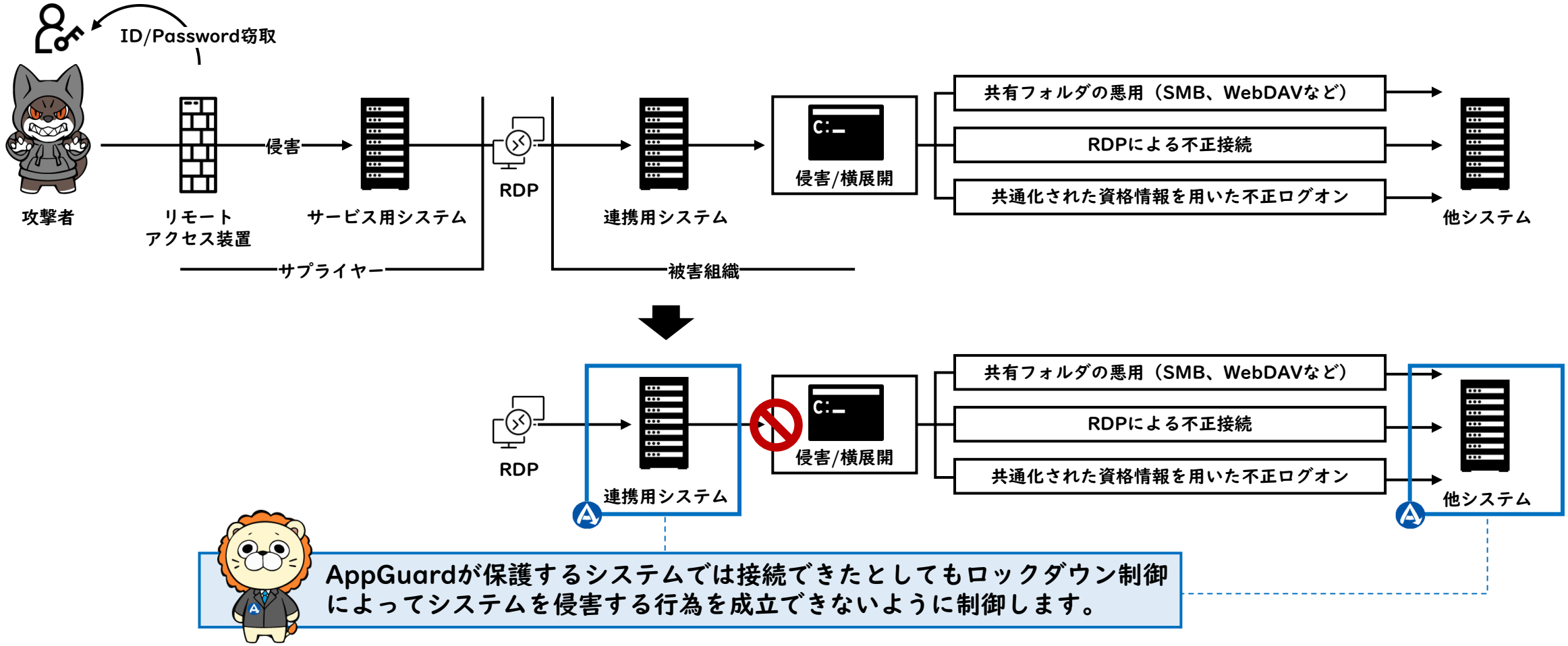


AppGuardによる攻撃阻止パターン #2

Blue Planet-works
Safety for the Connected World

サプライヤーからのRDP接続を介して侵入された場合の攻撃パターンについて（例：大阪急性期・総合医療センターのケース）

接続性を持つ外部組織から不正アクセスされるテクニックに対してもAppGuardは貢献します。

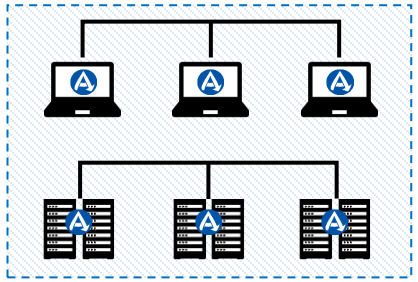


出典：「大阪急性期・総合医療センター」及び「社会医療法人生長会」の侵害事案について当該組織又はメディア等で報道された内容を基に構成

AppGuardの部分導入

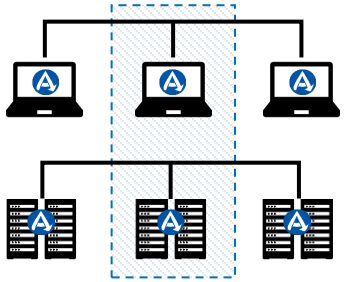
Blue Planet-works
Safety for the Connected World

AppGuardを全体へ導入



OR

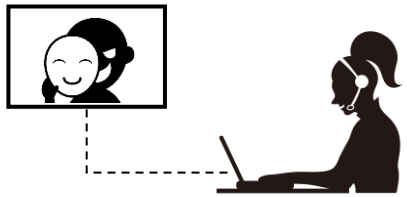
AppGuardを部分的に導入



機密情報を扱う部署

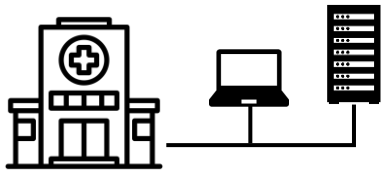
組織内でも特に機密性の高い情報を扱う端末を保護

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

Blue Planet-works
Safety for the Connected World

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

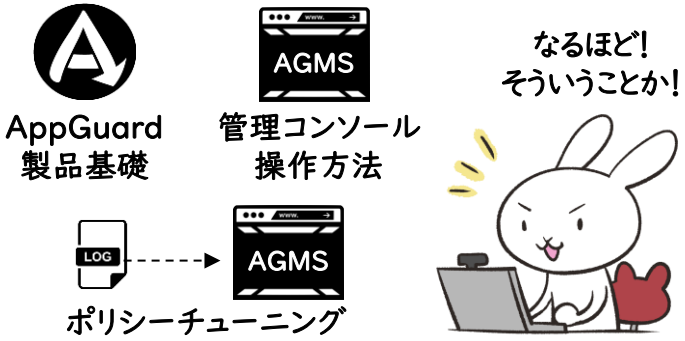
AppGuard導入パッケージ

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。