Blue Planet-works
Safety for the Connected World

AppGuardのご紹介

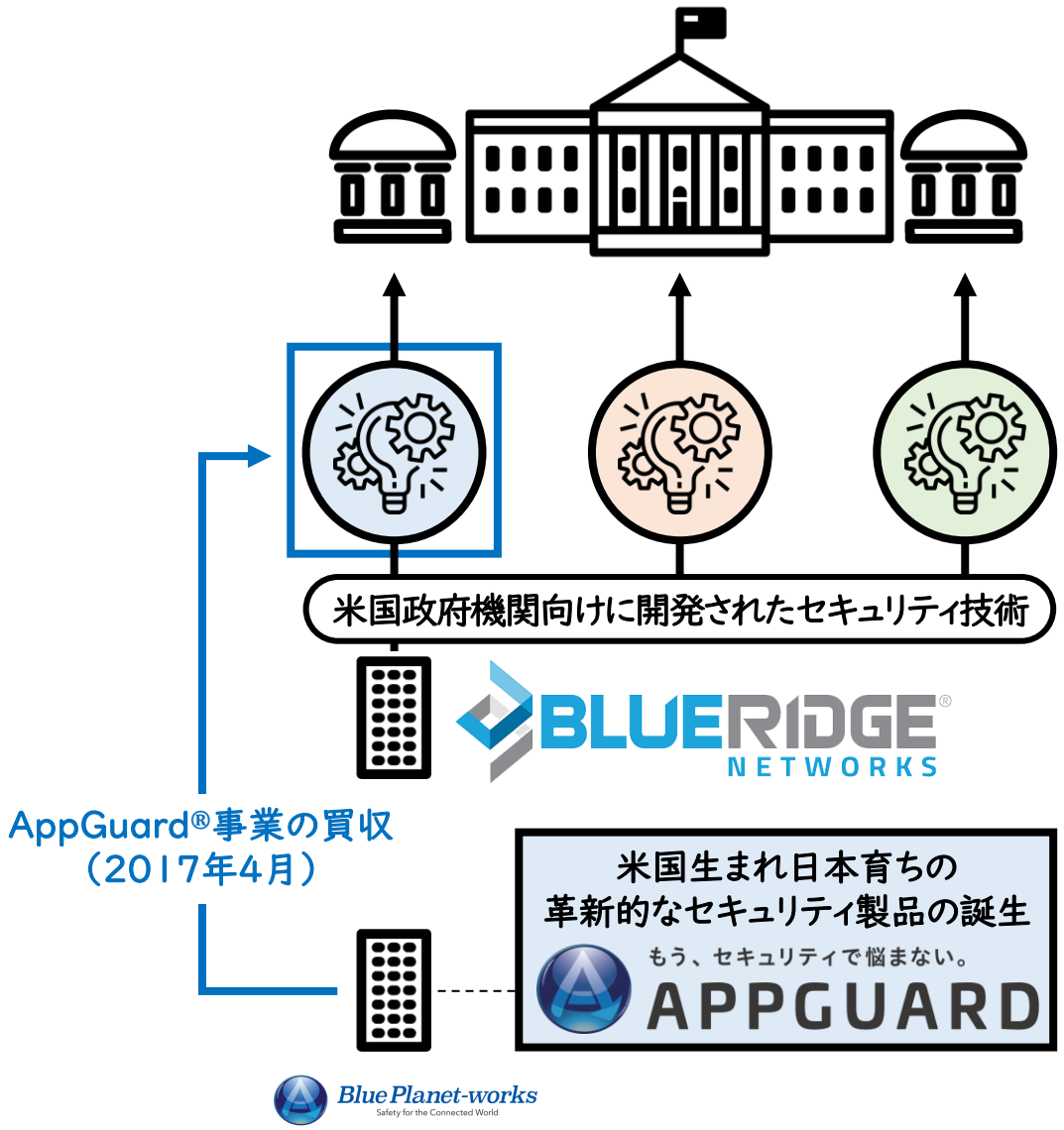
株式会社Blue Planet-works

AppGuard Evangelist　奥村 健太

株式会社Blue Planet-worksについて

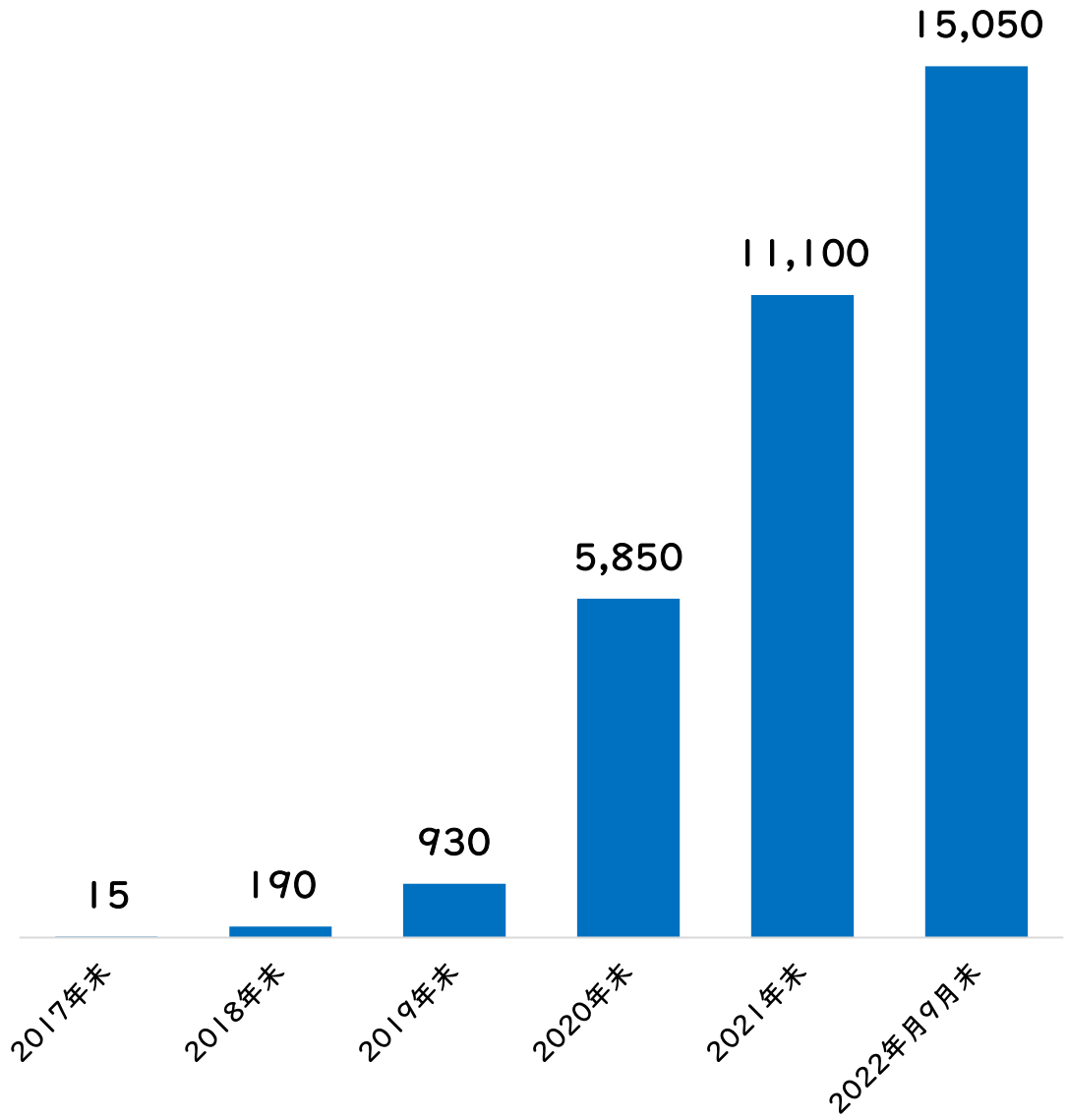
Blue Planet-works
Safety for the Connected World

商号	株式会社Blue Planet-works
英文社名	Blue Planet-works, Inc.
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	82億円（2021年12月時点）
代表取締役	小林ヤンネ孝貢(会長) 原口直道(社長)
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	42名（2021年12月時点）
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



国内における累積導入者数と事例ユーザー

AppGuard累積導入社数の推移（国内）



AppGuard導入事例企業（国内）

特定医療法人 佐藤会 弓削病院
ANA
dentsu
戸田建設
諏訪信用金庫
UCHIDA
Pentel
白石市
吉本興業
iSiD
KAKUDAI
DAIKO
SMBC日興証券
宮崎電子機器

国内導入累積社数

15,000社突破

（2022年9月末時点）

今こそ新しい守りのカタチが求められている

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

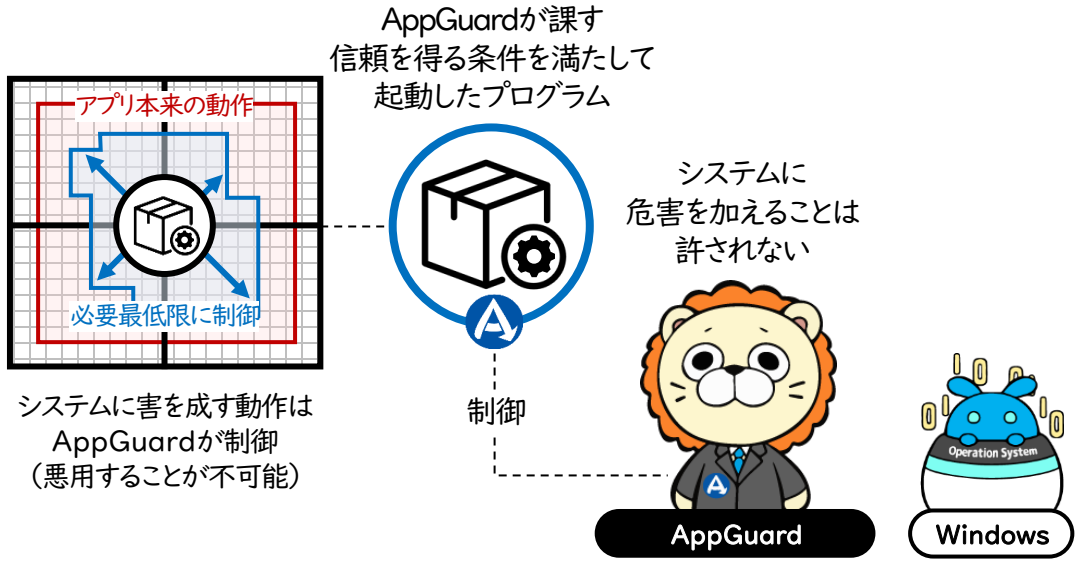
過去の情報から害を成す悪いモノを例外として排除

攻撃者が先手を取れる状況を覆せない

これからの守り方

悪い事をさせない環境を作る

端末のプロセスをゼロトラスト化し侵害行為を許さない

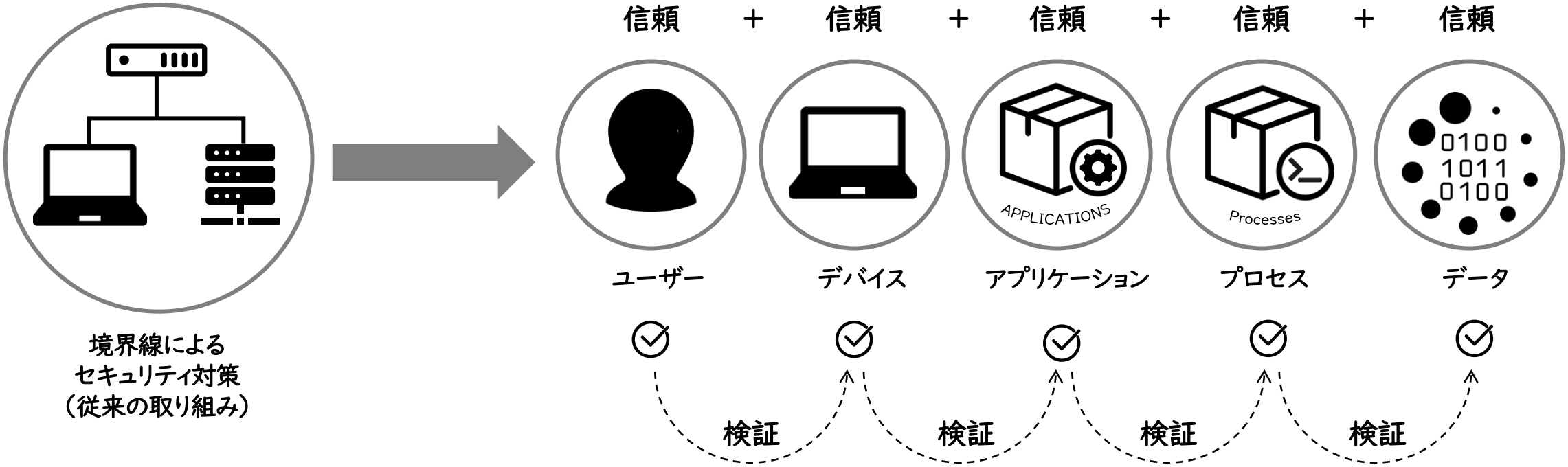


攻撃者は先手を取れても目的は達成できない

エンドポイントをゼロトラストする防御へ

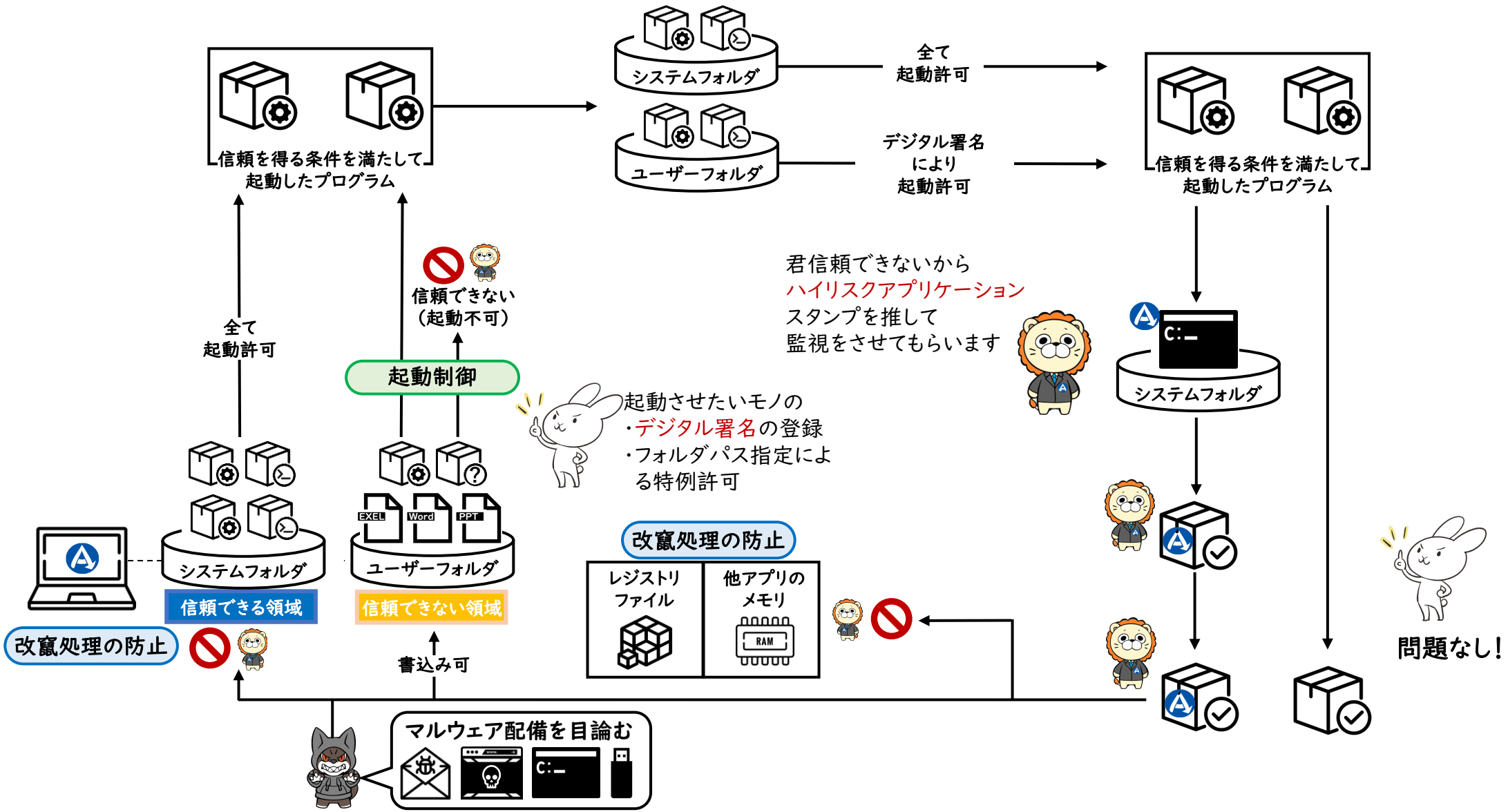
今のエンドポイントセキュリティはアプリケーションの起動やそのプロセス中で悪意のある動きを検知する仕組みが一般的です。ゼロトラストの概念にのっとり、アプリケーションへの信頼とそのプロセスを検証し続けるゼロトラストの仕組みをエンドポイント内で実装することが重要です。

ゼロトラストは特定のツールを指すものではなく
小さな信頼をつなぎ合わせて不確実性を逓減していくための戦略



境界線による
セキュリティ対策
（従来の取り組み）

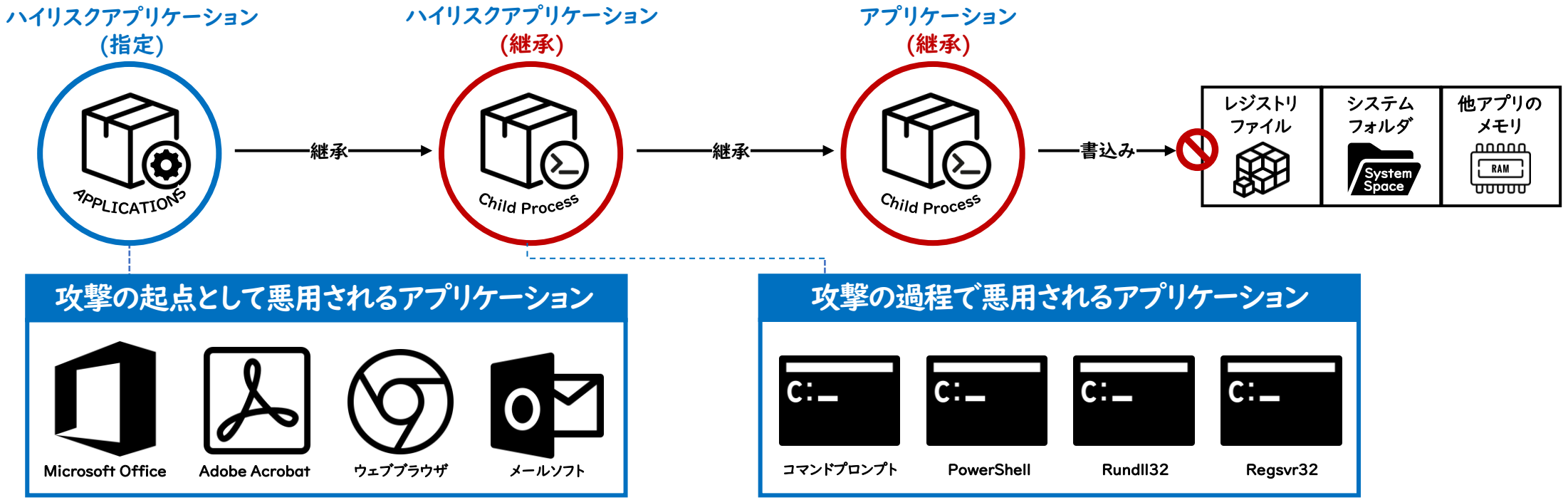
新しいゼロトラストの守り方



ゼロトラストを可能にしたAppGuardの検証技術

Blue Planet-works
Safety for the Connected World

AppGuardが持つ特許技術が可能にする「ポリシーの自動継承機能」



AppGuardでは、攻撃に利用されやすいアプリケーションをハイリスクアプリケーションとあらかじめ定めています。攻撃者は攻撃プロセスの中で1度でもハイリスクアプリケーションを起動させると、その後の挙動は全て監視、検証され続け、改竄処理の禁止ルールを適用し続けます。

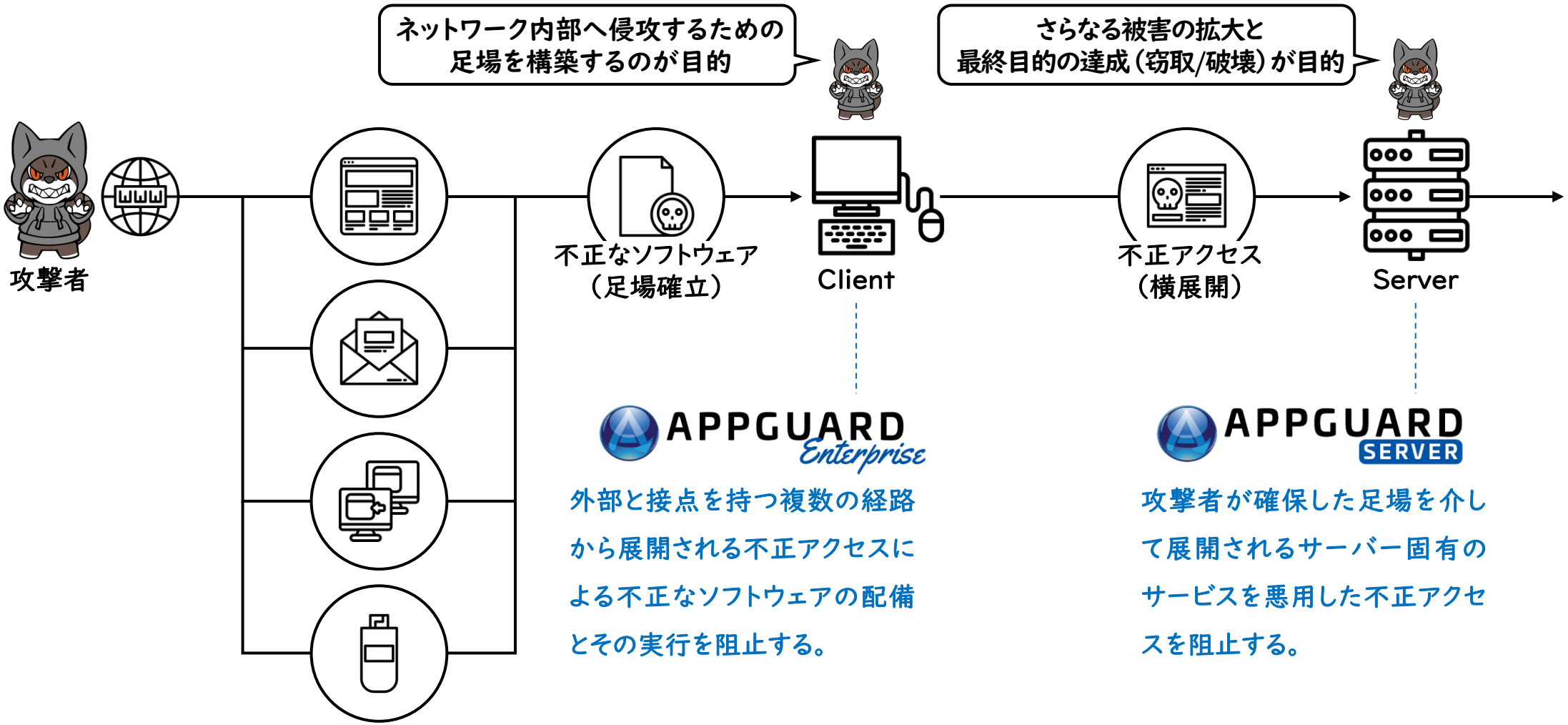
守るべき箇所をピンポイントで守る

- ロックダウンが実現するAppGuard Serverの絶対防御 -

サーバーとクライアントは同じ保護ポリシーではダメ

Blue Planet-works
Safety for the Connected World

▶ サイバー攻撃に対して守りたい場所に応じた適切な保護ポリシーが必要



APPGUARD Enterprise

外部と接点を持つ複数の経路から展開される不正アクセスによる不正なソフトウェアの配備とその実行を阻止する。

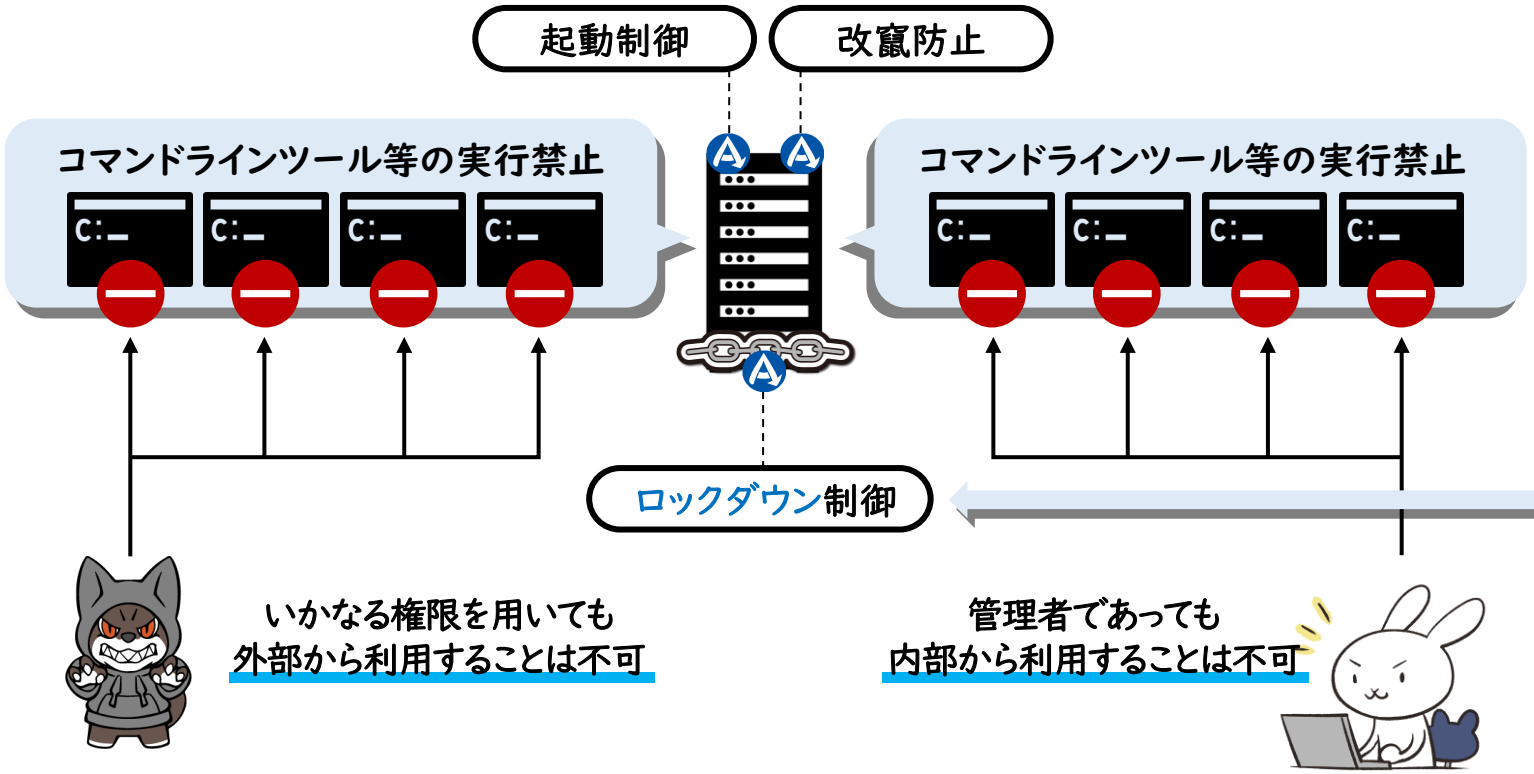
APPGUARD SERVER

攻撃者が確保した足場を介して展開されるサーバー固有のサービスを悪用した不正アクセスを阻止する。

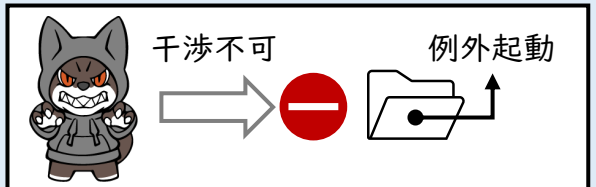
サーバー版のロックダウン制御

Blue Planet-works
Safety for the Connected World

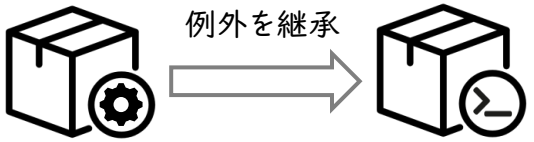
Windows Serverに対して脆弱性を悪用したRCEを成立させないように
内外からのコマンドラインツール等の実行を禁止してロックダウン状態にして
サーバー固有のサービスを悪用した窃取・削除・暗号化等を阻止



必要なアプリケーションを
安全に動かす仕組み（例外設定）



特定フォルダから実行される
プログラムやスクリプトの例外化



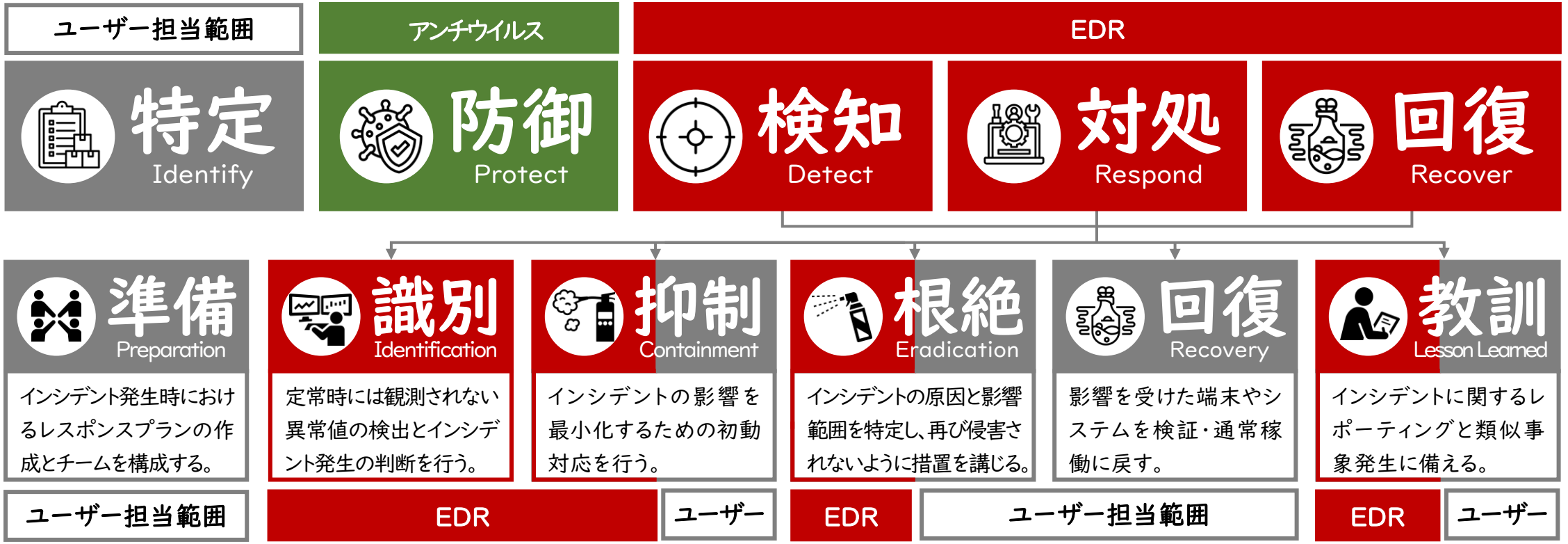
特定アプリケーションを起点として
派生プロセスを制御対象外指定

特定アプリケーションを
他のプロセスから分離して稼働

AppGuardが実現する新しい多層防御のカタチ

NIST SP800－171に潜む課題

▶ 導入しても使いこなせない可能性を払拭することが困難



【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）】

ツール（EDRとその運用含む）を配備するだけでは
事後対策の強化にはつながらないのか…
（自組織内に専門人材の配備や運用体制の構築が必要）

「予防」の概念はセキュリティの考え方を変える

Blue Planet-works
Safety for the Connected World

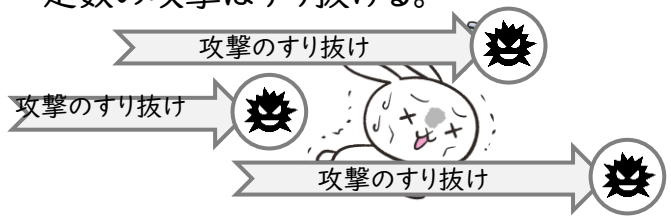
NIST（米国標準技術研究所）が提唱するサイバーセキュリティフレームワーク（NIST SP800－171）

特定 Identify | 防御 Protect | 予防 Privent | 検知 Detect | 対処 Respond | 回復 Recover

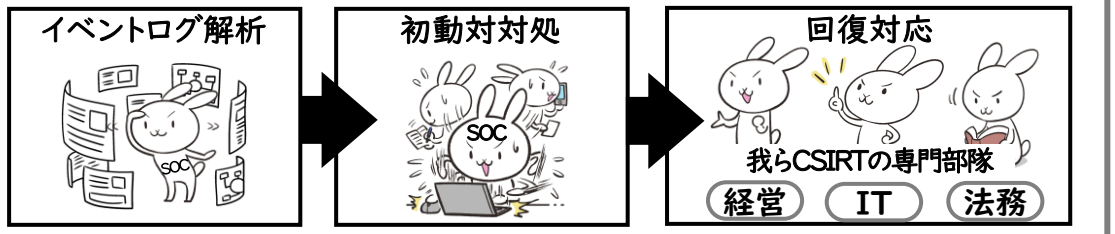
←これまでも対策してきた領域→　新たな要素として追加　←出来れば取り組みたいが人材、予算等の都合上、新たな投資が困難な領域→

■これまでのカタチ

一定数の攻撃はすり抜ける。



多くの企業は
このギャップを超えられない

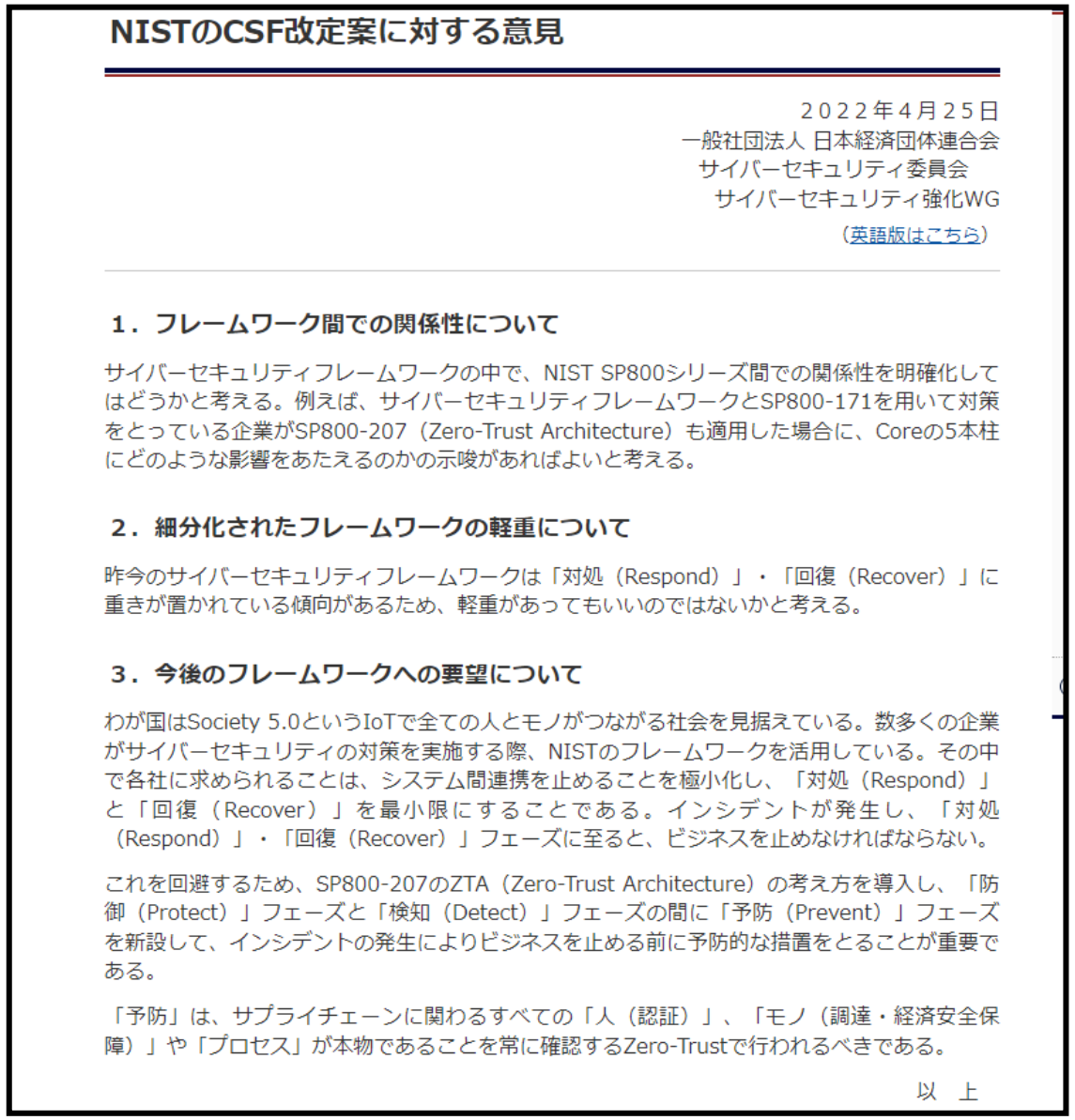


■これからのカタチ

一定数の攻撃はすり抜ける。

NISTへ提言されたAppGuardが提唱する「予防」の位置付け

Blue Planet-works
Safety for the Connected World



NISTのCSF改定案に対する意見

2022年4月25日
一般社団法人 日本経済団体連合会
サイバーセキュリティ委員会
サイバーセキュリティ強化WG
（英語版はこちら）

1．フレームワーク間での関係性について

サイバーセキュリティフレームワークの中で、NIST SP800シリーズ間での関係性を明確化してはどうかと考える。例えば、サイバーセキュリティフレームワークとSP800-171を用いて対策をとっている企業がSP800-207（Zero-Trust Architecture）も適用した場合に、Coreの5本柱にどのような影響をあたえるのかの示唆があればよいと考える。

2．細分化されたフレームワークの軽重について

昨今のサイバーセキュリティフレームワークは「対処（Respond）」・「回復（Recover）」に重きが置かれている傾向があるため、軽重があってもいいのではないかと考える。

3．今後のフレームワークへの要望について

わが国はSociety 5.0というIoTで全ての人とモノがつながる社会を見据えている。数多くの企業がサイバーセキュリティの対策を実施する際、NISTのフレームワークを活用している。その中で各社に求められることは、システム間連携を止めることを極小化し、「対処（Respond）」と「回復（Recover）」を最小限にすることである。インシデントが発生し、「対処（Respond）」・「回復（Recover）」フェーズに至ると、ビジネスを止めなければならない。

これを回避するため、SP800-207のZTA（Zero-Trust Architecture）の考え方を導入し、「防御（Protect）」フェーズと「検知（Detect）」フェーズの間に「予防（Prevent）」フェーズを新設して、インシデントの発生によりビジネスを止める前に予防的な措置をとることが重要である。

「予防」は、サプライチェーンに関わるすべての「人（認証）」、「モノ（調達・経済安全保障）」や「プロセス」が本物であることを常に確認するZero-Trustで行われるべきである。

以　上

Point

①「対処」(Response)、「回復」(Recover)に重きが置かれすぎている

「対処(response)、回復(recover)のフェーズに入った時点でビジネスを止めなければいけない。

②新しい概念「予防」(Prevent)が必要である

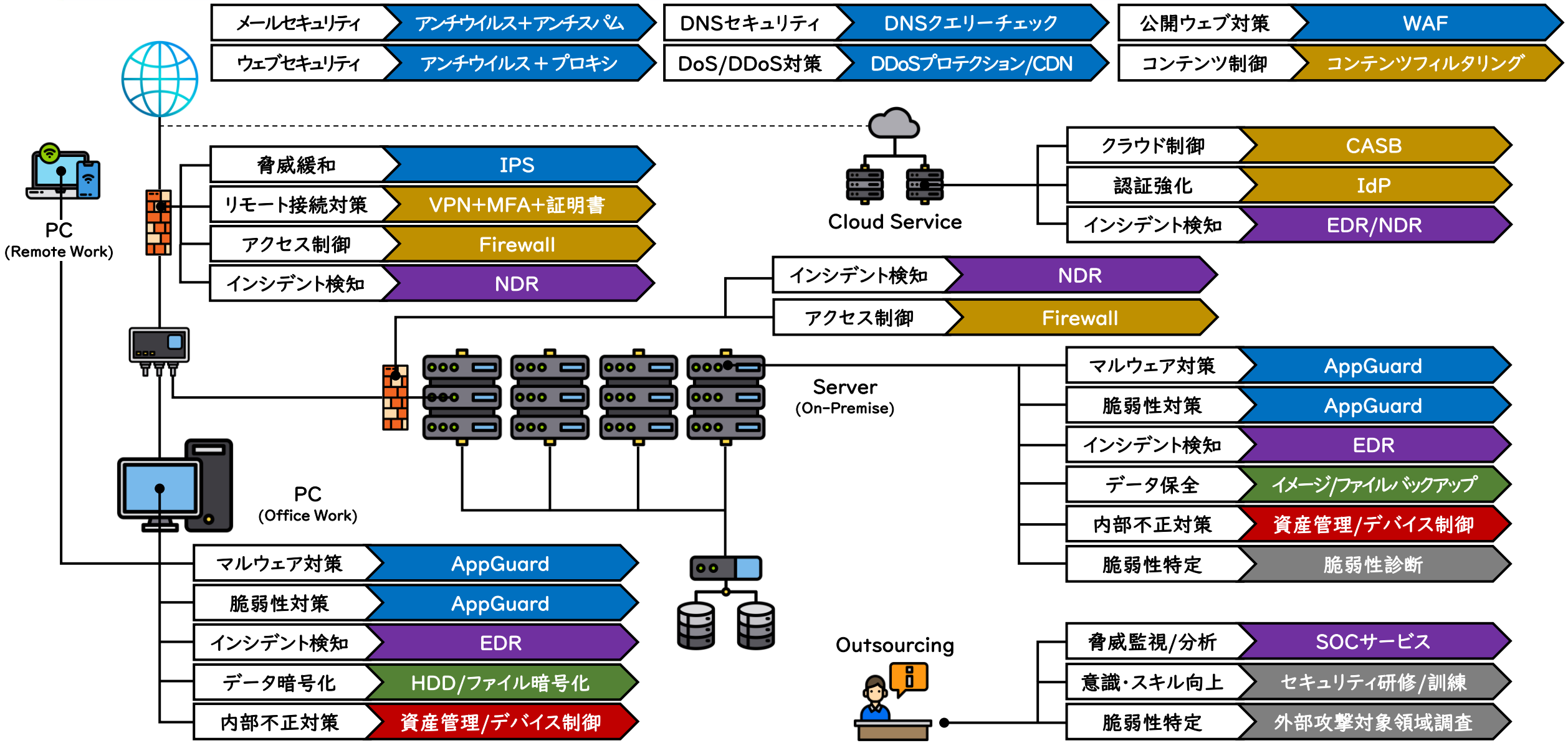
従来の「検知」(Protect)と「検知」(Detect)の間に「予防」(Prevent)が必要であり、ビズネスを止める前の措置をとることが重要。

③「予防」(Prevent)の概念はZero-Trustであるべき

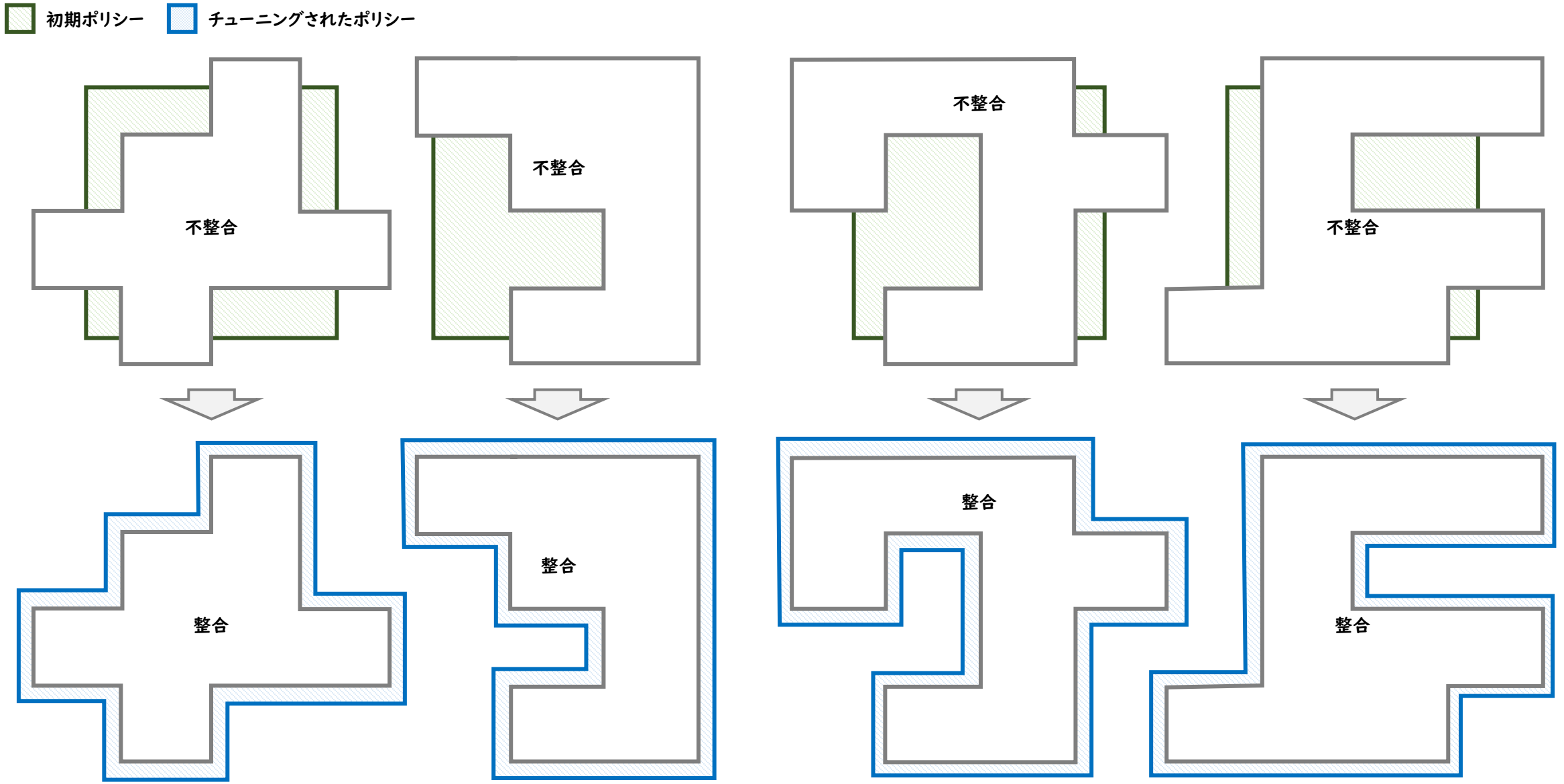
「人」、「モノ」、「プロセス」が本物であることを常に確認する必要がある。

AppGuardを用いたサイバーセキュリティソリューションマッピング

Blue Planet-works
Safety for the Connected World



お客様の環境に合わせた「型」を成型する

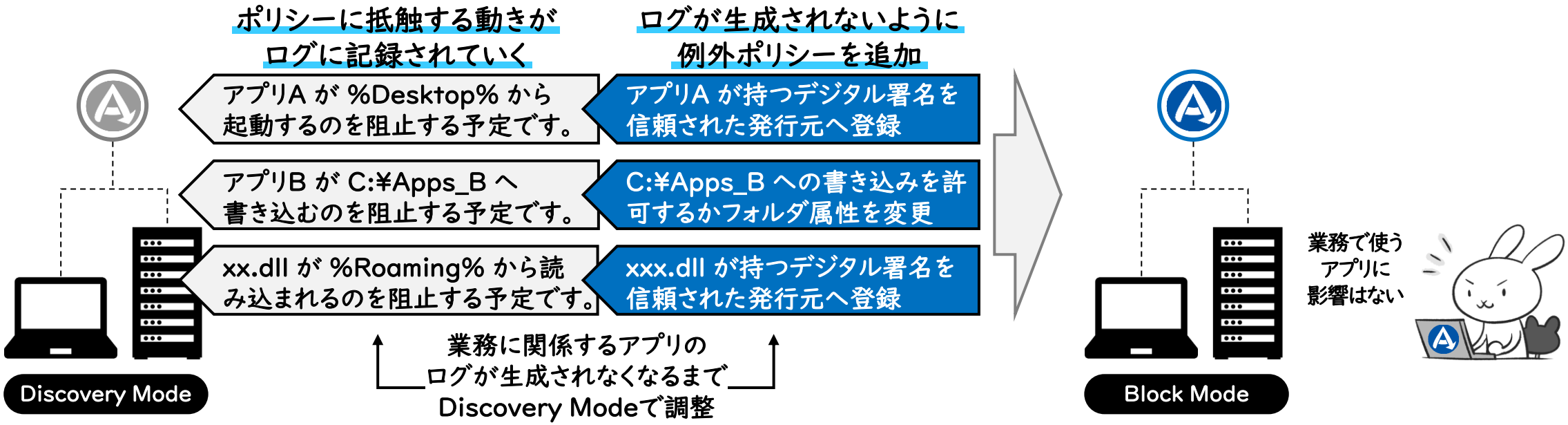


DiscoveryModeを利用したログの分析とポリシー設計

Blue Planet-works
Safety for the Connected World

▼Discovery Modeとは

AppGuardはポリシー設計に利用する「Discovery Mode」という業務に影響を与えずに初期ポリシーと対象の不整合箇所をログとして抽出する機能があります。
この機能を利用して初期ポリシーによって誤って制御された業務上必要なアプリケーションを特定し、必要な例外ルールを適用することで業務に影響を与えることのないポリシーを効率的に設計できます。



運用メニューの活用方法

AppGuardの運用で頻出する対応ケース

- 初期ポリシー設定後に新規導入するアプリケーション
- 初期ポリシー設定後に制御される動作が確認された
- 端末の配置換によるグループの移動
- 緊急対応における管理者モード移行

上記のようなAppGuardの運用は全部おまかせ！

※運用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。

02:AppGuard製品概要

AppGuard製品名	販売商品名称	サービス内容	価格	備考
AppGuard Enterprise	ITGあんしんセキュリティパック For AppGuard Enterprise	AppGuard Enterpriseライセンス	@7,500円/年～	年額サブスクリプション
		ITGクラウドセキュリティサービス(AGMSホスティングサービス)		
		サイバーセキュリティ保険		
	AppGuard運用サービス For AG-E	お問合せ全般	@1,200円/年～	年額サブスクリプション
		ポリシー運用、エージェント運用		
		月次、年次レポート		
導入支援パック	スタンダード導入支援パック AppGuard Enterprise	初回のヒアリングからポリシー設計、管理者トレーニング、本番展開支援までAppGuard Enterpriseの導入プロセスが一通り含まれた標準的なパッケージサービス（～500台）	1,500,000円～	初年度料金

AppGuard製品名	販売商品名称	サービス内容	価格	備考
AppGuard Server	ITGあんしんセキュリティパック For AppGuard Server	AppGuard Serverライセンス	@75,000円/年～	年額サブスクリプション
		ITGクラウドセキュリティサービス(AGMSホスティングサービス)		
		サイバーセキュリティ保険		
	AppGuard運用サービス For AG-S	お問合せ全般	@12,000円/年～	年額サブスクリプション
		ポリシー運用、エージェント運用		
		月次、年次レポート		
導入支援パック	スタンダード導入支援パック AppGuard Server	初回のヒアリングからポリシー設計、管理者トレーニング、本番展開支援までAppGuard Serverの導入プロセスが一通り含まれた標準的なパッケージサービス（1ロール設定）	750,000円～	初年度料金

Blue Planet-works
Safety for the Connected World

ありがとうございました。