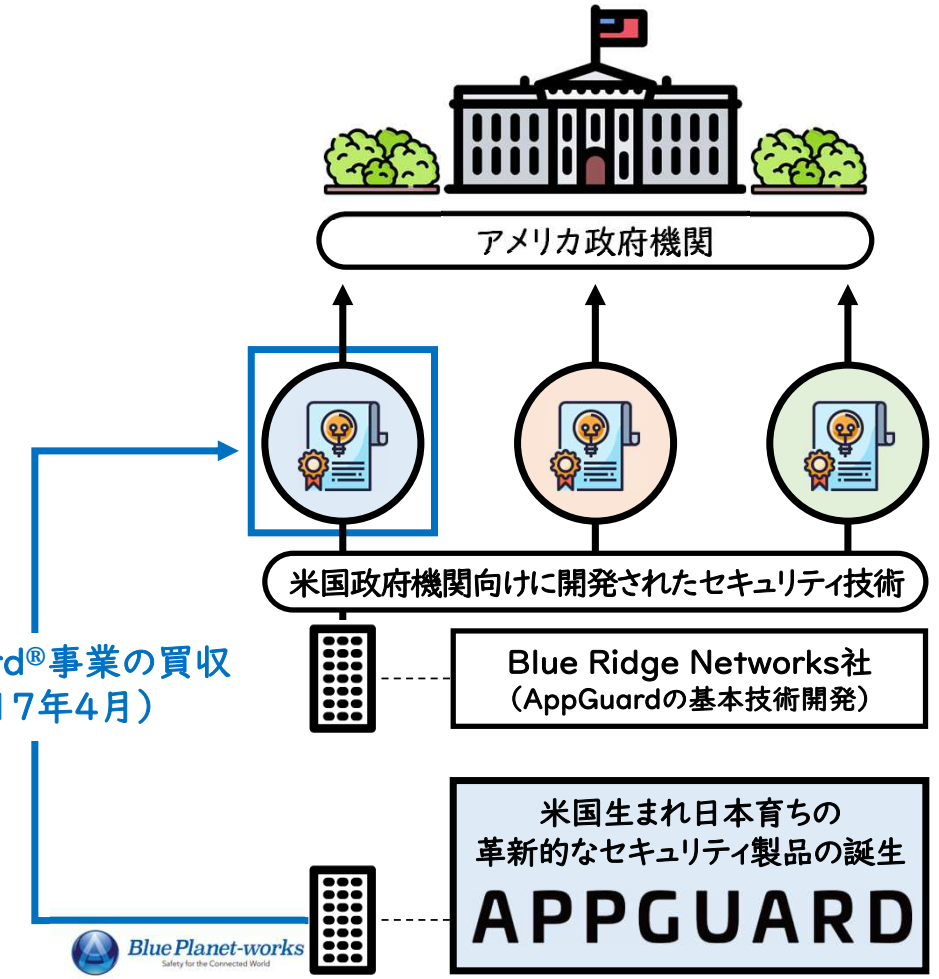
# 01 Blue Planet-worksについて

APPGUARD

Blue Planet-works
Safety for the Connected World

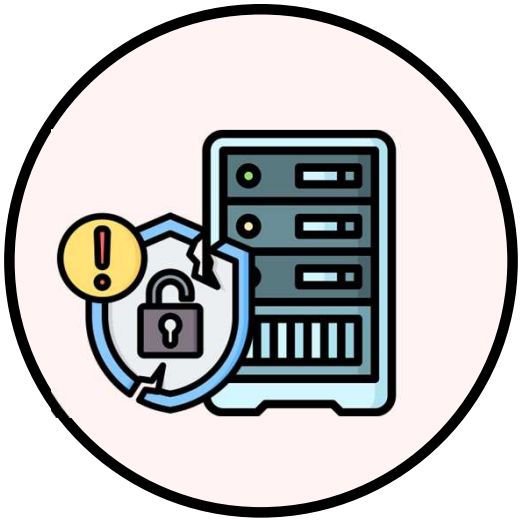
| | |
|---|---|
| 商号 | 株式会社Blue Planet-works |
| 英文社名 | Blue Planet-works, Inc. |
| 住所 | 141-0032 東京都品川区大崎4-1-2 ウィン第2五反田ビル3F |
| 設立 | 2017年4月 |
| 資本金 | 84億円 |
| 代表取締役社長 | 坂尻浩孝 |
| 事業内容 | 「AppGuard」の技術を応用したサイバーセキュリティプロダクトの開発・販売及び付帯サービスの提供 |
| 従業員数 | 29名（2025年4月時点） |
| 株主 | 株式会社東京ウェルズ<br>SBIインベストメント株式会社<br>Blue Ridge Networks, Inc.<br>PCIホールディングス株式会社<br>ANAホールディングス株式会社<br>富士フイルムビジネスイノベーション株式会社<br>株式会社電通グループ<br>株式会社JTB<br>第一生命保険株式会社<br>損害保険ジャパン株式会社<br>他多数 |



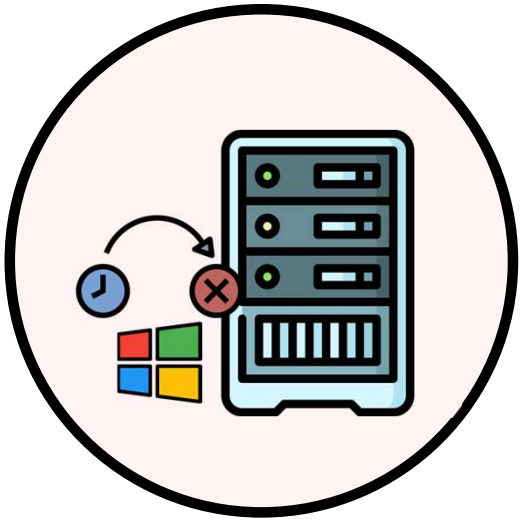
# 02 こんな悩みを抱えていませんか？

APPGUARD

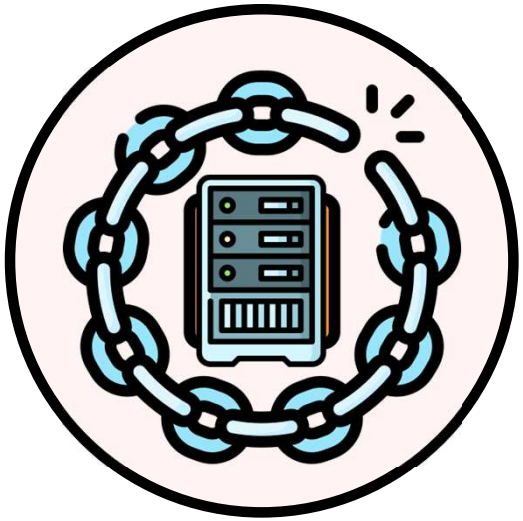
正規ツールを悪用する
新しい攻撃を阻止したい



未解消の脆弱性に対する
悪用リスクを解消したい



サポート切れOSに対する
脆弱性リスクを解消したい



ミッションクリティカルな
システムを絶対に守りたい

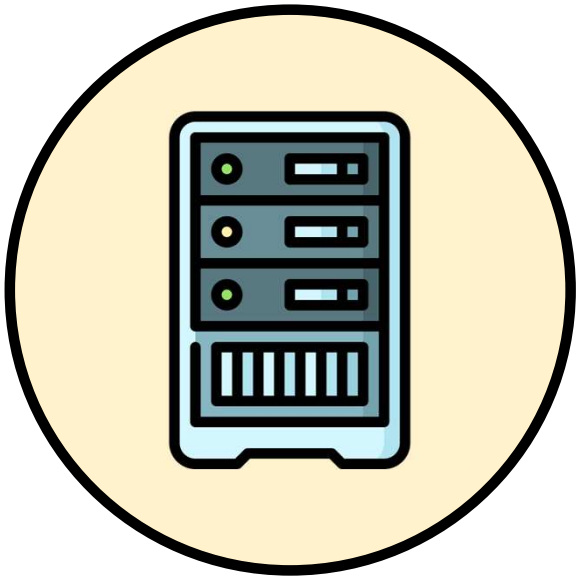
## あっ！そういえば・・・と思い当たる方は聞いて下さい

# 03 「Windowsデバイス」を保護することに特化



## APPGUARDは
## 稼働環境を選ばず「Windowsデバイス」を要塞化して保護

Windows クライアント

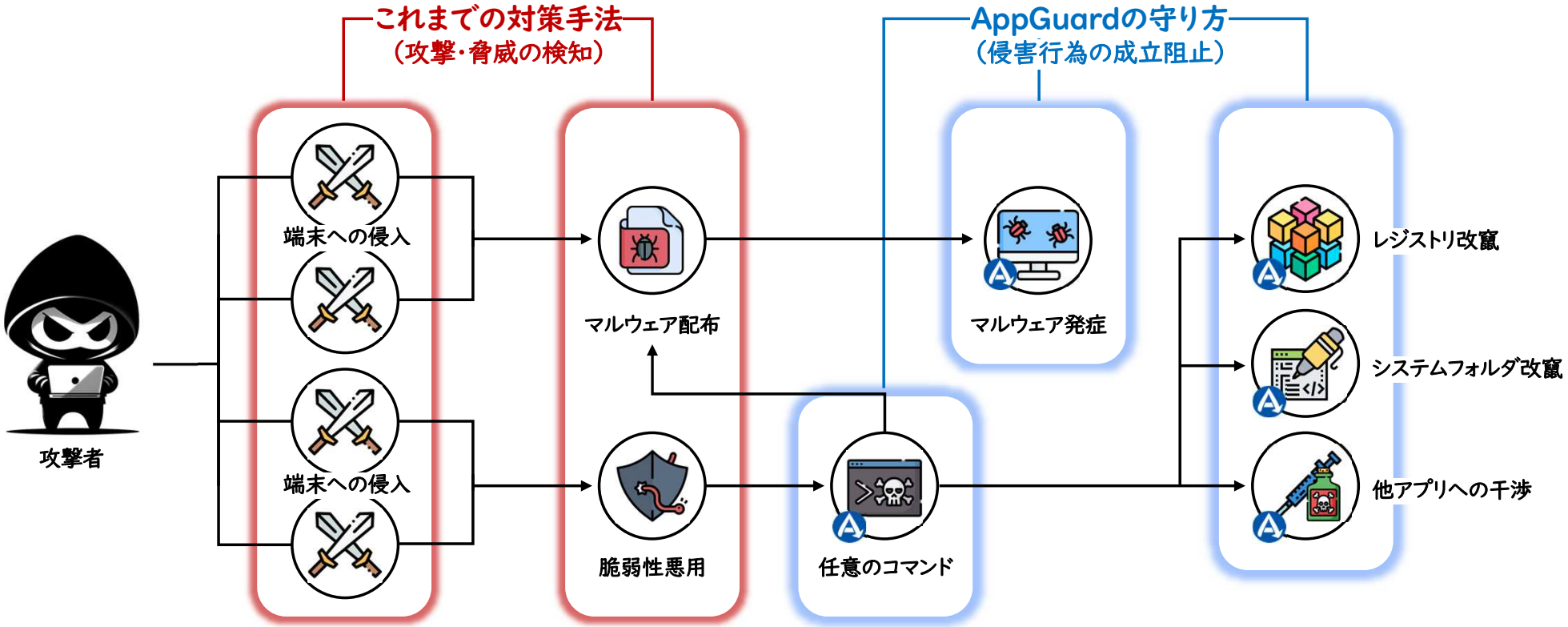


Windows サーバー

# 04 脅威に対するアプローチを変える

APPGUARD

従来のセキュリティアプローチは「イタチごっこ」の構図から抜けられず、かつ、過去の情報に依存しているため攻撃者が優位な状況を覆すことができないことが課題である。



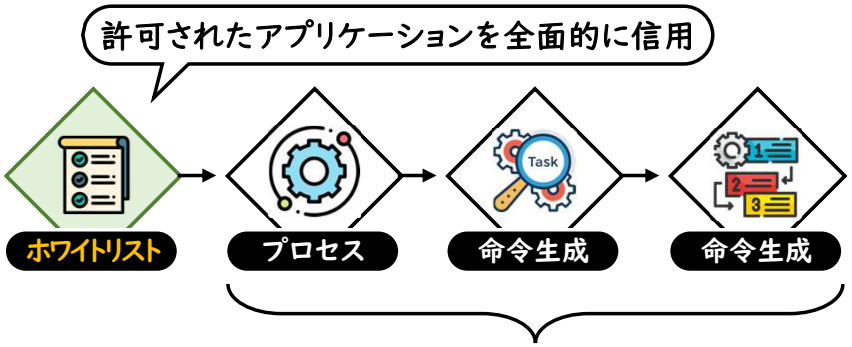
# 05 「AppGuard」とホワイトリスト型製品の違い

APPGUARD

## APPGUARDは ホワイトリスト型製品の弱点を克服

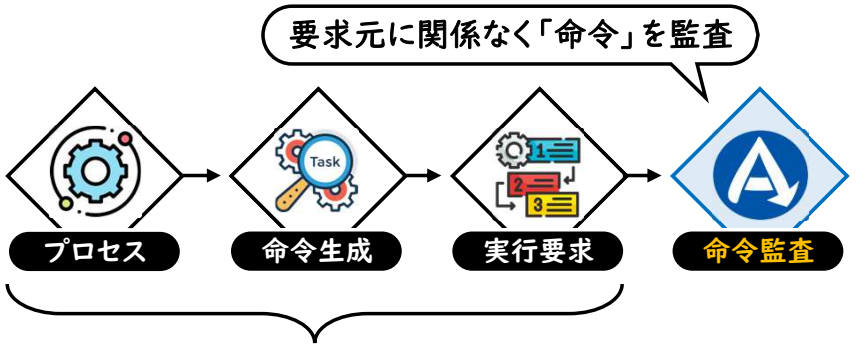
### ホワイトリストの考え方

ホワイトリスト型製品はあらかじめ定義されたホワイトリストに基づいてアプリケーションの動作可否を判断する。許可されたアプリケーションが悪用されることは想定されていない。




### AppGuardの考え方

「AppGuard」は実行主体を問わず実行要求された「命令」を自身が持つ制御ルールと照合し、システムを害する命令を検知・制御することで安全な状態を確保する。(命令志向のゼロトラスト)

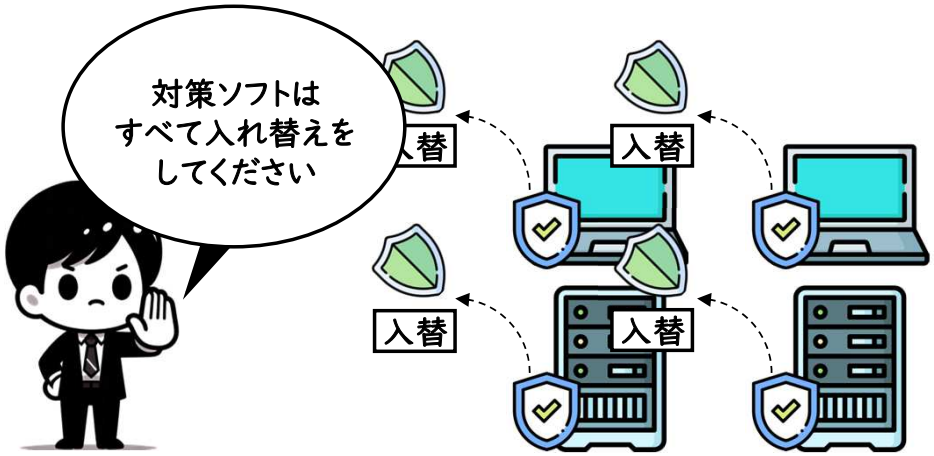


# 06 AppGuardは守りたいところを守ることができる

APPGUARD

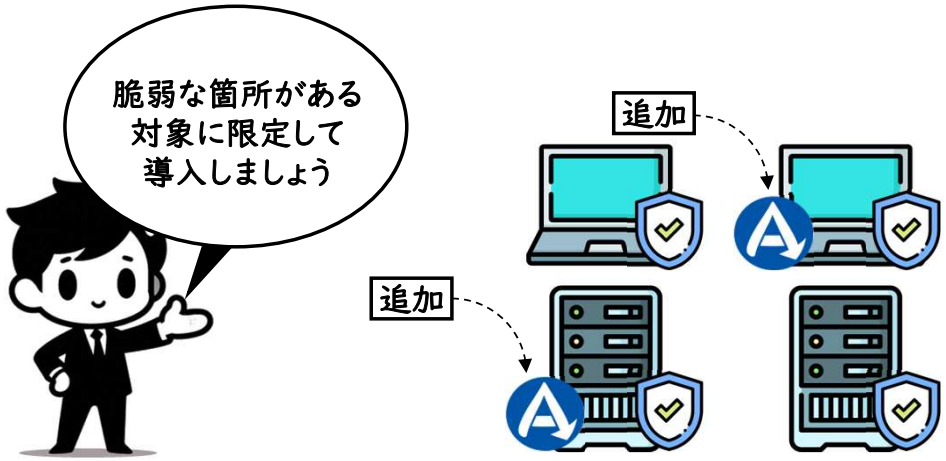
## 従来の検知型セキュリティアプローチ（NGAV/EDR）

すべての保護対象デバイスから情報（悪性ファイルや異常動作）を収集して分析することで攻撃や脅威を特定する必要があるため、「全体」に導入する。




## AppGurd（要塞化による防止）のセキュリティアプローチ

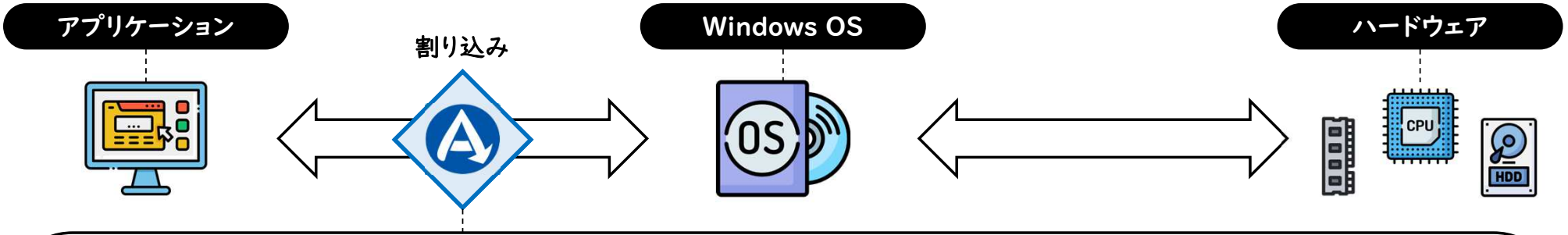
脅威であるか否か関係なく規定された命令以外は実行できないように要塞化する。既存の投資を否定せず「ミッションクリティカルなデバイスに限定」して導入することができる。



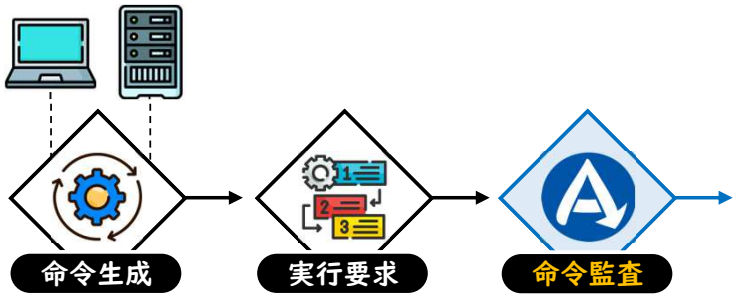
# 07 システムに害を成す命令は実行できなくなる

APPGUARD

## AppGuardにより「やって良い命令・悪い命令」が明確に規定され「やって良い命令」だけが常に実践されているか検証され続ける

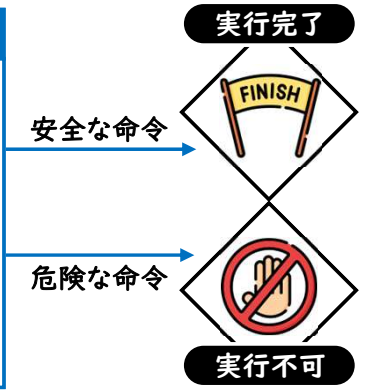



「AppGuard」が実行要求された命令の権限と内容の正当性を確認し不正な命令を検知・阻止



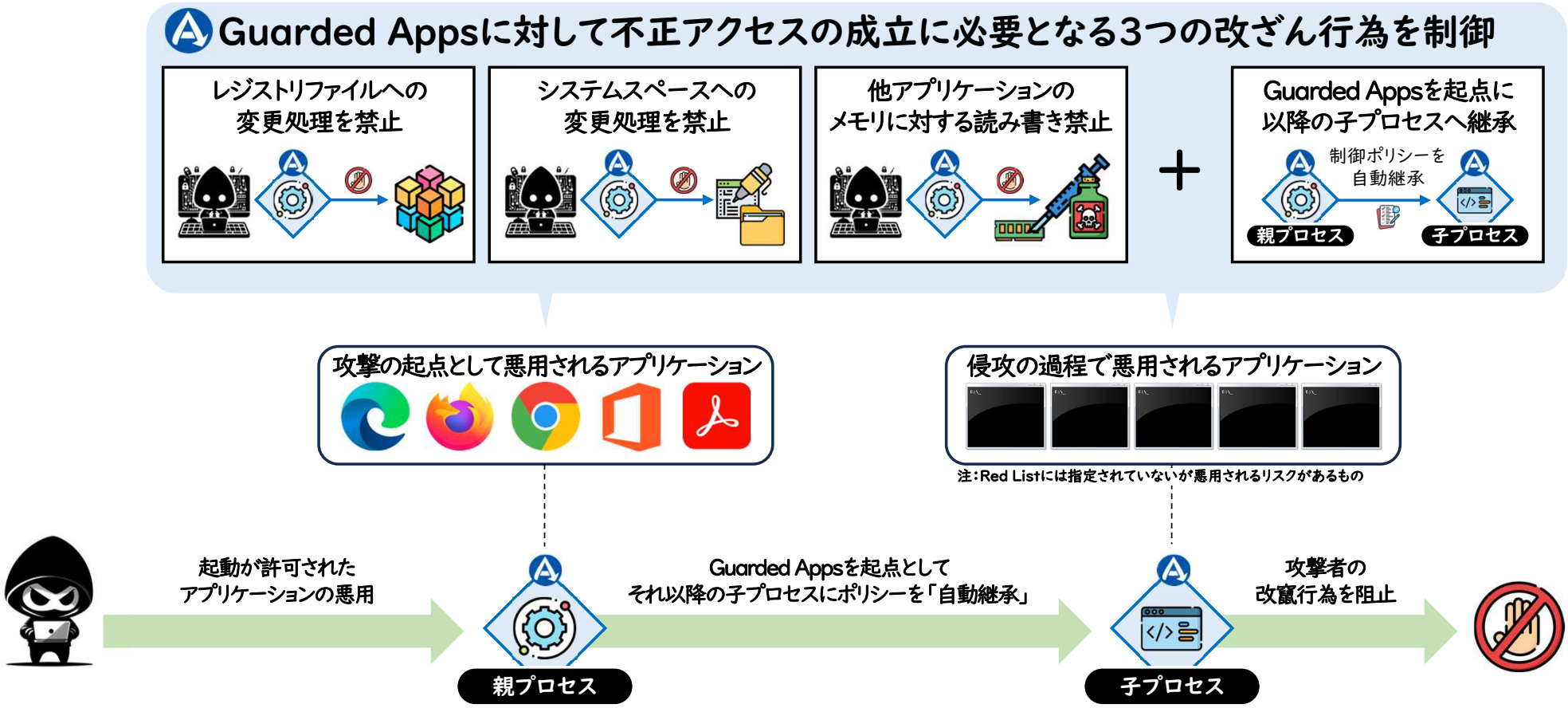

**実行要求された「命令」を制御ルールと照合**

- ☐ 起動が禁止されたプログラムを起動
- ☐ 信頼できない領域からプログラムを起動
- ☐ 信頼できない領域からプログラムコードを読み込む
- ☐ 信頼できる領域にリスクのあるプログラムから書き込み
- ☐ レジストリに対してリスクのあるプログラムから書き込み
- ☐ 他アプリのメモリに対してリスクのあるプログラムから読み書き



# 08 【Guarded Apps】悪用リスクのあるプログラム行動を制御

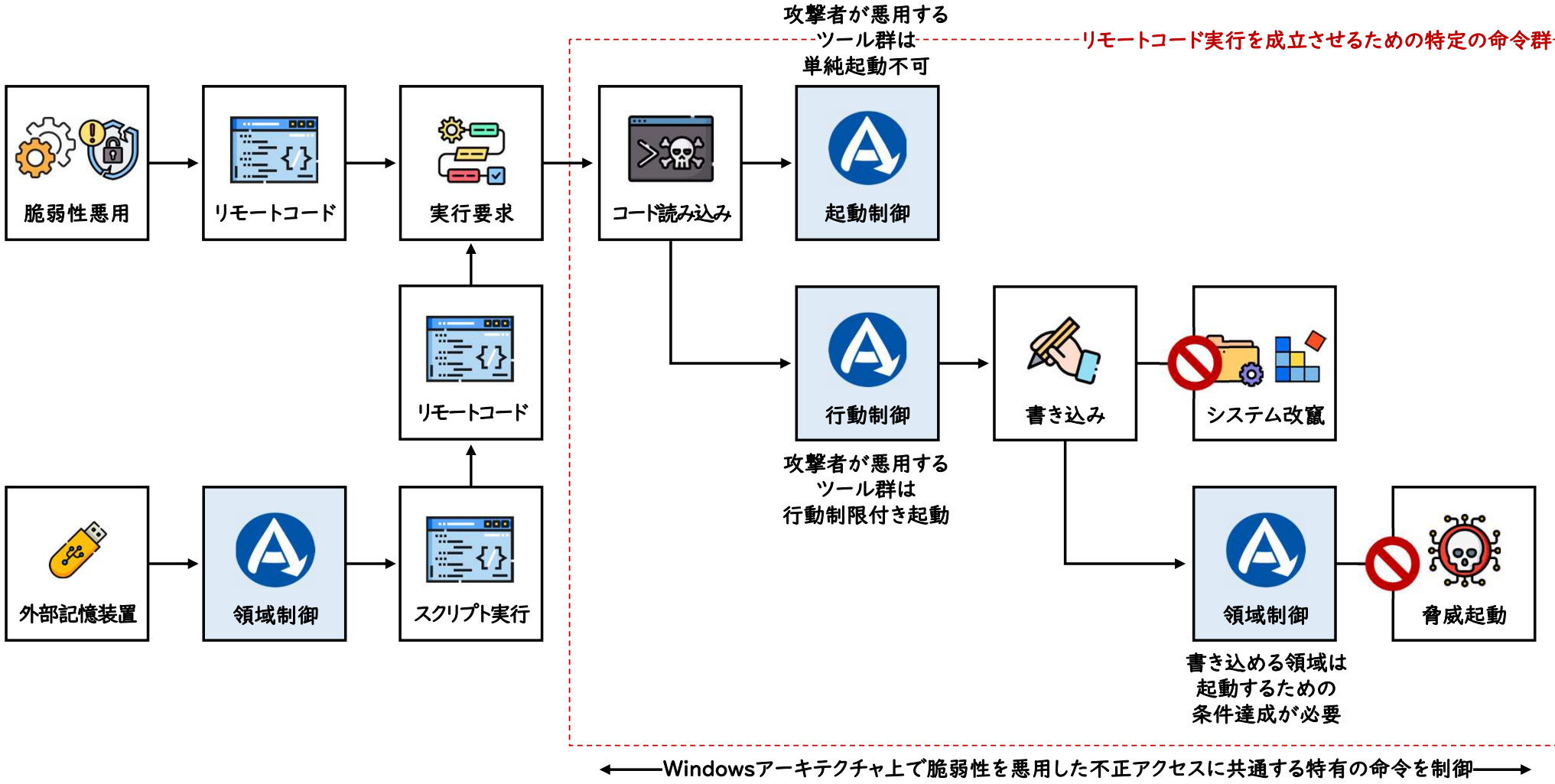
APPGUARD




※ 本スライド上で「ハイリスクアプリケーション」として紹介しているアプリケーションは一例です。

# 09 脆弱性を悪用したリモートコード実行への対応例

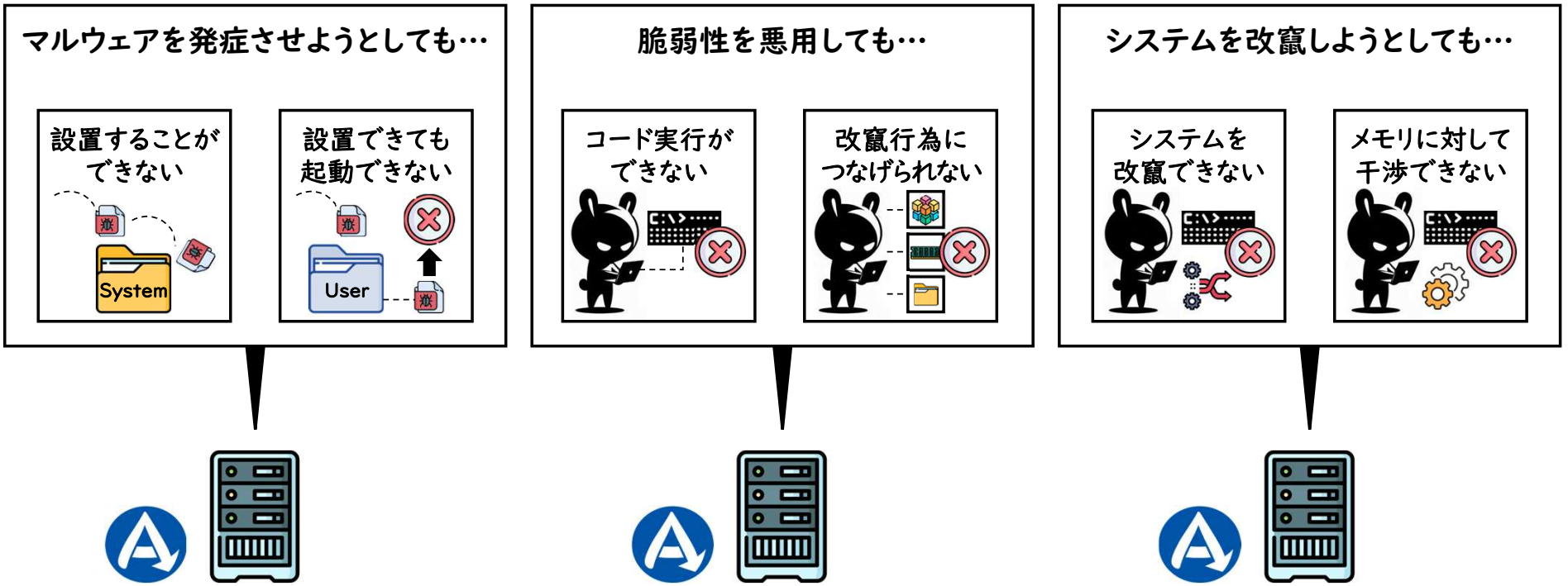
APPGUARD



# 10 AppGuardを導入することで得られるメリット

APPGUARD

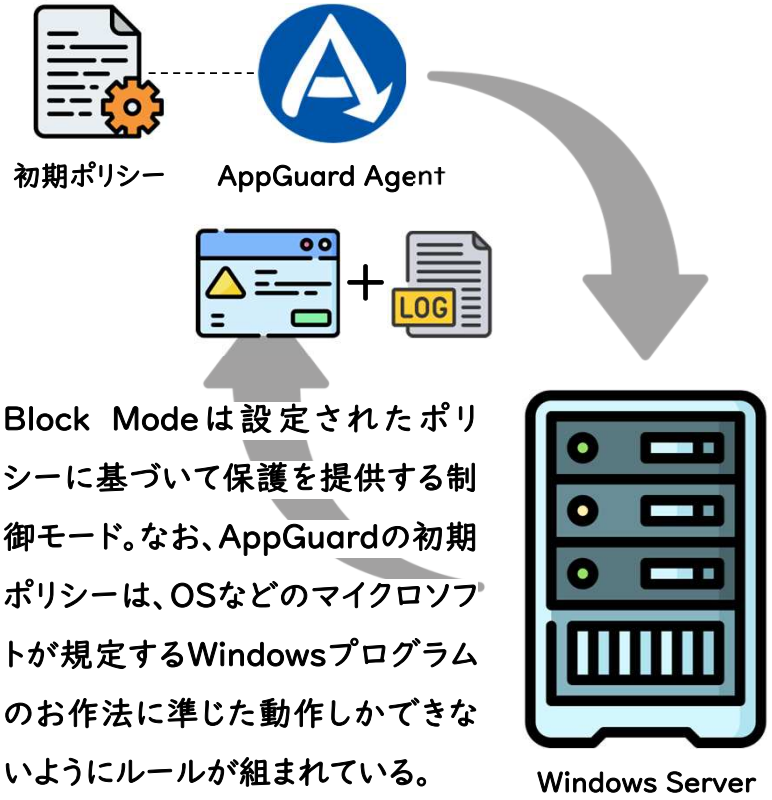
**攻撃者は攻撃成立に不可欠な「特定の命令」を実行することができない**
**ゼロトラスト思考の副次的な効果でサイバー攻撃は失敗に終わる**



# AppGuardの制御モードについて

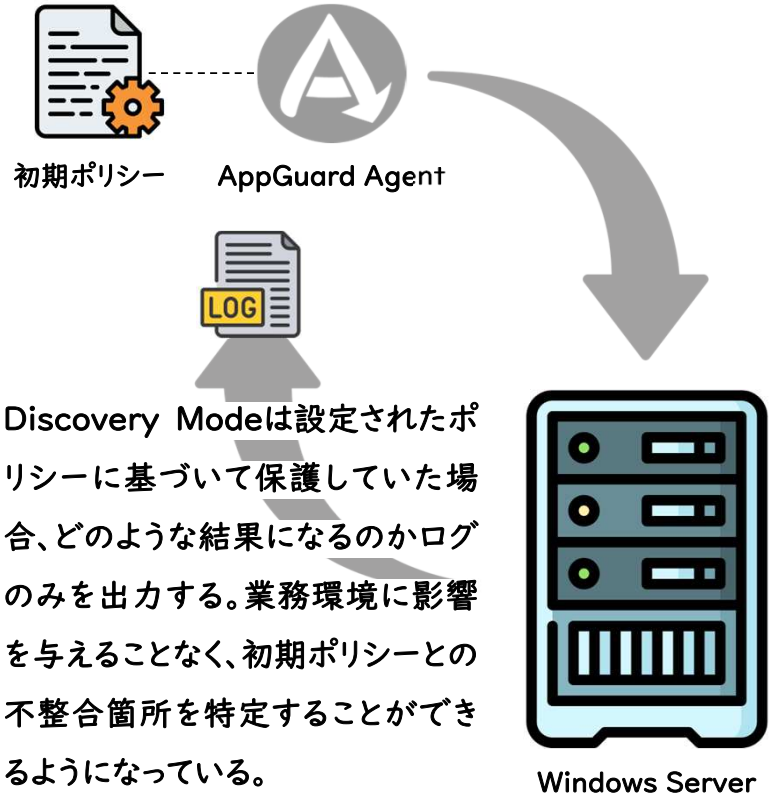
APPGUARD

## Block Mode（保護モード）




Block Modeは設定されたポリシーに基づいて保護を提供する制御モード。なお、AppGuardの初期ポリシーは、OSなどのマイクロソフトが規定するWindowsプログラムのお作法に準じた動作しかできないようにルールが組まれている。

## Discovery Mode（監査モード）




Discovery Modeは設定されたポリシーに基づいて保護していた場合、どのような結果になるのかログのみを出力する。業務環境に影響を与えることなく、初期ポリシーとの不整合箇所を特定することができるようになっている。