



AI時代の新たな「自助」

～速度の非対称性を克服するシステム要塞化～

株式会社 AppGuard

上席セキュリティアドバイザー 嶋原祐輔

日本から世界へ「安心 (ANSHIN)」を届ける

会社名	株式会社AppGuard (旧:株式会社Blue Planet-works)
設 立	2017年4月
資本金	87億円 (2026年1月時点)
代 表	代表取締役会長 片地格人 代表取締役社長 坂尻浩孝
所在地	〒105-0001 東京都港区虎ノ門三丁目8番21号 虎ノ門33森ビル 2階
事 業	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
子会社	株式会社AppGuardジャパン (国内事業統括) AppGuard, Inc. (研究開発、欧米営業)



あるSOC担当者の悩み

～ Introduction ～

速すぎて人間では追えなくなっているという現実

ハンドオフするまでの時間
(後続グループの手にアクセス権が渡るまでの時間)

中央値
8時間
(2022年) ➡ 中央値
22秒
(2025年)



出典: Mandiant「M-Trends 2026 Report」

残された猶予時間
(侵入から横展開が開始されるまでの時間)

平均値
48分
(2024年) ➡ 平均値
29分
(2025年)



出典: CrowdStrike「CrowdStrike 2026 Global Threat Report」

目的達成までの時間
(侵入からデータ窃取完了までの時間)

全体の25%が
276分以下
(2024年) ➡ 全体の25%が
72分以下
(2025年)



出典: Unit42「Global Incident Response Report 2026」

一方で静かすぎて居座りが見えなくなる現実も

世界全体の潜伏期間
(Mandiantが調査した標的型攻撃を対象)

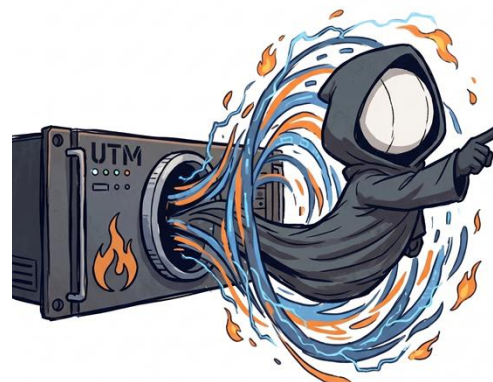
中央値
11日
(2024年) → 中央値
14日
(2025年)



出典: Mandiant「M-Trends 2026 Report」

標的環境への長期的なアクセス
(サイバースパイ活動を目的とした攻撃者を対象)

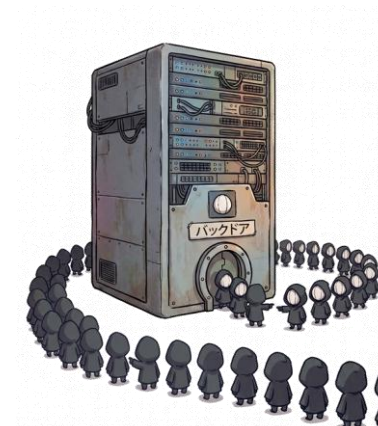
中央値
122日
(2025年)



出典: Mandiant「M-Trends 2026 Report」

標的環境への長期的なアクセス
(さくらインターネットの不正アクセス事案)

調査結果に基づく
3年以上※
(2026年)



※当該期間は必ずしも同一の攻撃者が潜伏していたとは限らない。

守るための仕組みそのものがもたらす限界や負荷と対峙

未調査のイベントが溜まる
(組織の規模に比例して調査待ちイベントは増える)



対処開始までに時間を要する
(外注SOCサービスを使うとさらに時間がかかる)



セキュリティとビジネスの目線が違う
(SOCアナリストだけでは組織の正解を判断できない)



二極化する脅威に対抗するための打ち手とそれを阻む課題

発報されるアラートが多過ぎて
全てを調査しきれない



対応要員を増やす



必要なスキルを持つ人材は奪い合い(需給ギャップ)

求められるスキルの非現実性

給料を上げるには管理職へ(キャリアパスの課題)

セキュリティ人材を評価・維持できない人事制度

人間が必ず間に入るため
初動対応が遅れる



自律型SOC構築



人間が判断すべき領域は最上流へ押し上がる

影響度に応じた自動化の線引きを設計し続ける

権限・意思決定・復旧のガードレール設計

AIの判断根拠を人間がレビューできる透明性の担保

「要塞化」というアプローチ

～ AppGuardについて～

アメリカ生まれ日本育ちの「AppGuard」



米国で「戦闘システム」を
保護することを目的に開発



2017年に技術・知的財産含めて
事業買収して日本へ



「AppGuard」として
日本から世界へ

システムへ到達されても攻撃者の目的を達成させない「要塞化」の要求

要 求 仕 様

管理システムから数週間切り離された状態でも自律的に防御力を維持し続けて健全な状態で復帰すること。

要 求 仕 様

過去のマルウェアや攻撃シグネチャに依存することなく新しい攻撃を防御する能力を有すること。

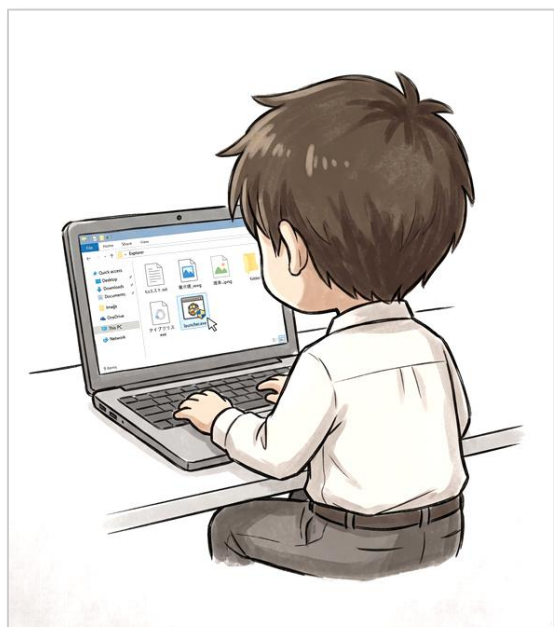
要 求 仕 様

配備された作戦に関わる重要システムがパッチ適用やアップデートなしでも防御し続けられること。



「AppGuard」は実行要求される「命令」に対してアプローチ

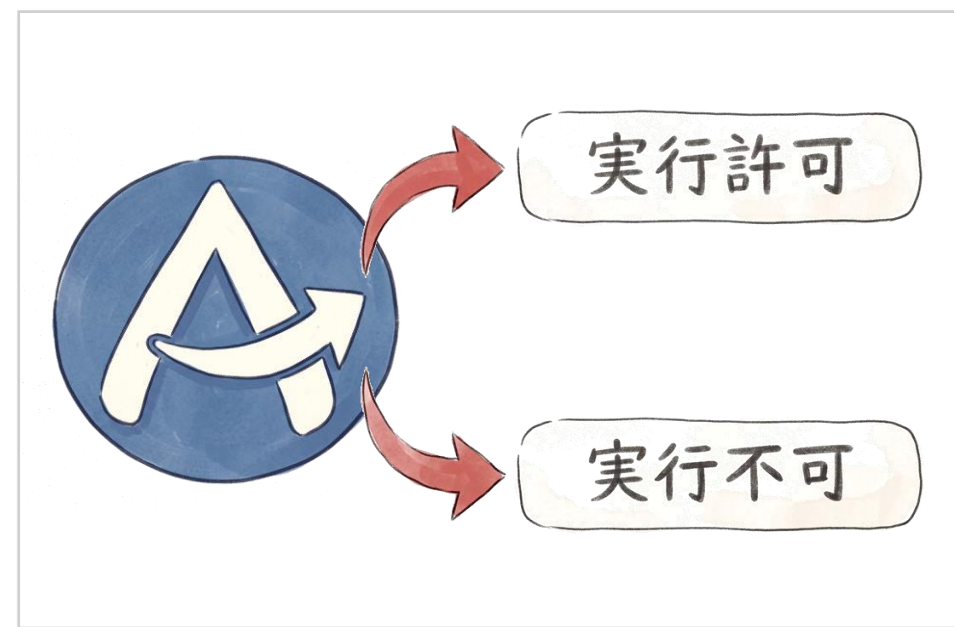
OSの仕様と攻撃セオリーに基づき「やってはいけないこと」を強制制御し
抵触してしまう正当な業務操作のみを最小権限の原則に基づいて開放



アプリケーションの実行



実行要求



カーネル空間でAppGuardが介入して制御

特許
取得

常に命令が「正しいものか」を検証する仕組み

▶ 3つの基本制御と自動継承機能が特許技術 (US Patent #7712143、#7809955)

起動制御



攻撃者に悪用されやすいツールの直接起動を禁じ、許可されたアプリケーション経由の実行のみを認める制御。

行動制御



ブラウザなどの動作を制限し、システム改ざんやメモリ操作などの致命的な振る舞いを遮断する制御。

領域制御



信頼された場所以外でのプログラム実行を禁じ、不正ファイルや部品の読み込みを阻止する制御。

自動継承



行動制御対象のアプリケーションが呼び出した子や孫のアプリケーションには行動制御を自動的に継承。

新たに発見された攻撃手法に対する「AppGuard」の有効性を検証



本検証結果は2026年9月14日までに検証を行ったものです。(期間:2023年4月~2026年9月)



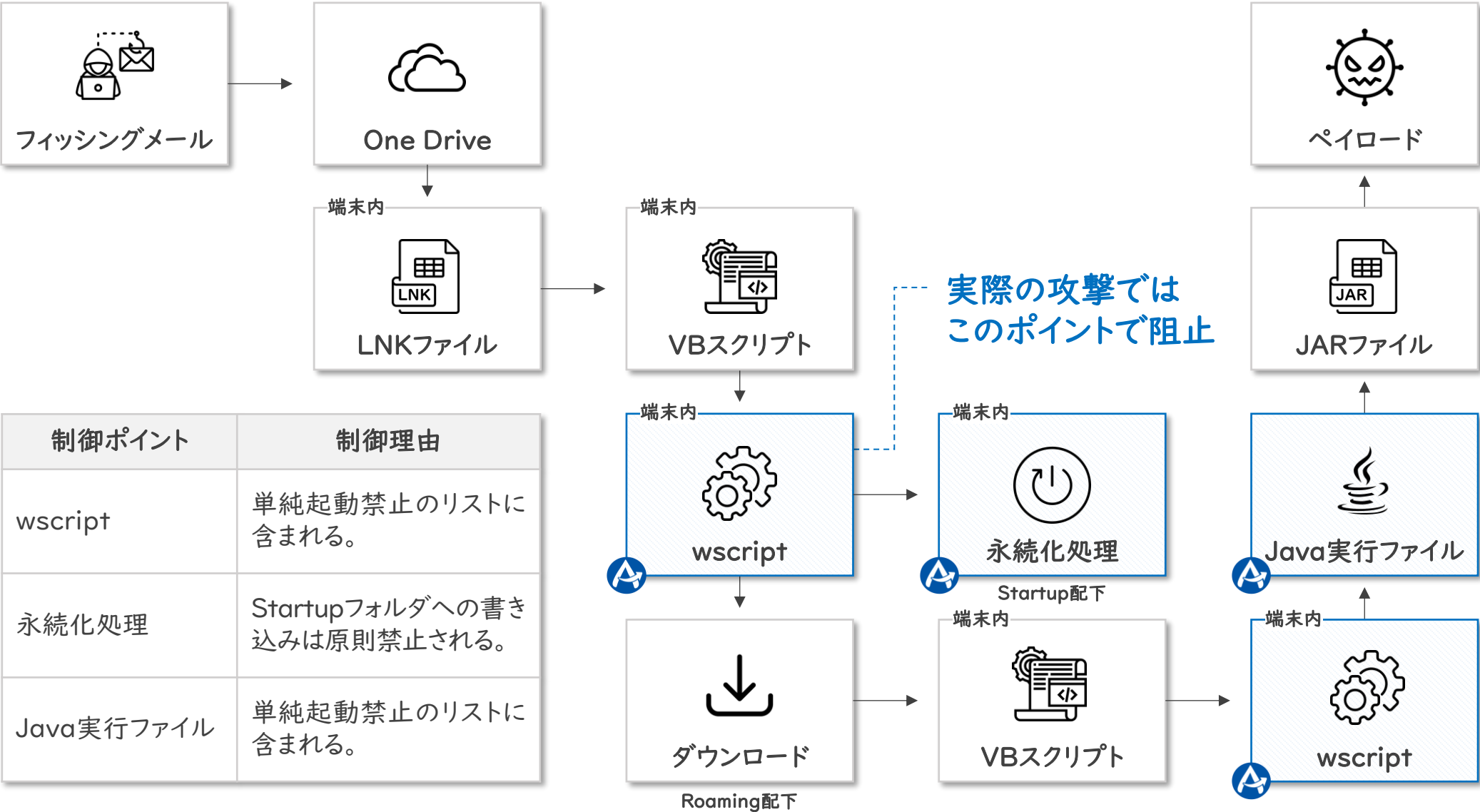
No.	2026年 有効性検証実施済み攻撃シナリオ
78	APT28によるCVE-2026-21259を悪用した攻撃ベクトル
79	Notepad++のアップデートプロセスを悪用したLotus Blossomの攻撃ベクトル
80	Silver Dragonが東南アジア及び欧州で展開するキャンペーンの攻撃ベクトル
81	Atosが報告したClickFixの新しい変異体の攻撃ベクトル
82	LeakNetによるステルスローダーの配信を目的として攻撃ベクトル
83	Volt Typhooの攻撃ベクトル
84	Mustang PandaによるPulgXローダーの配布を目的とした攻撃ベクトル
85	net useコマンドを利用する新しいClick Fixの攻撃ベクトル
86	ベネズエラのエネルギー/公共インフラセクターを狙ったLotus Wiperの攻撃ベクトル
87	PySoxyの設置を目論むClick Fixの攻撃ベクトル

No.	2026年 有効性検証実施済み攻撃シナリオ
88	Twill TyphoonによるFDMTPバックドア攻撃キャンペーンの攻撃ベクトル
89	Atlas RATを展開する攻撃キャンペーンの攻撃ベクトル
90	Romulus Loaderを展開する攻撃キャンペーンの攻撃ベクトル
91	Silent Run Loaderを展開する攻撃キャンペーンの攻撃ベクトル
92	Python RATを展開する攻撃キャンペーンの攻撃ベクトル
93	APT-C-60が国内組織を狙って展開する攻撃キャンペーンの攻撃ベクトル
94	「Avalon」マルウェアフレームワークの攻撃ベクトル
95	日本の製造業を狙ったSilver Foxの攻撃キャンペーンの攻撃ベクトル
96	Terminal Fix攻撃キャンペーンの攻撃ベクトル
97	世界時計ユーティリティを悪用したSystemBC配布攻撃ベクトル

国内で確認された攻撃ベクトルに対する「AppGuard」の有効性検証例



AppGuardが攻撃を阻止する制御ポイント



決定論的アプローチで多くの組織が抱える課題の解決に貢献

[AppGuardはNGAV/EDRと併用可能な新たな防御層]

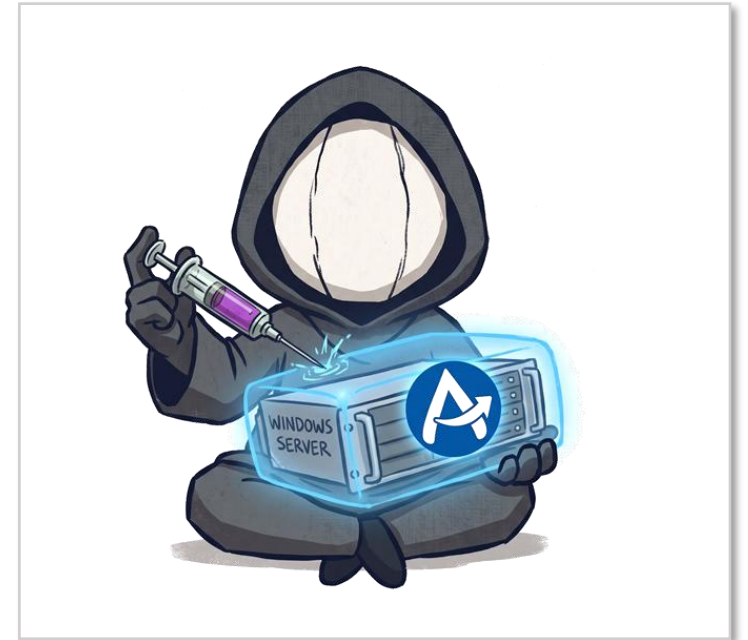
正規ツールを悪用した攻撃の阻止



重要システムの保護



脆弱性悪用時のリスク低減



テクノロジーと知性の力で世界にANSHINを届ける