完璧な守りは「Isolation（アイソレーション：隔離）技術」から

AppGuardは、OSそのものを特許取得済の「Isolation技術」で効果的に守ります。この技術は、米国政府機関で20年間一度も侵害されたことのない、特出した技術です。AppGuardは、米国陸軍の通信技術司令部（NETCOM）より、Certificate of Networthiness (CoN) の認証を得ました。これは、米国陸軍並びにアメリカ国防省の高水準なセキュリティ・スタンダードを満たしたことを証明するものです。

NISCガイドライン準拠

AppGuardは、NISC ～内閣サイバーセキュリティセンター～ より発行されている「不正プログラム対策のガイドライン」に準拠した製品です。このガイドラインは、政府機関等による情報セキュリティポリシー策定時に遵守すべきと定められた「統一基準」を解説するもので、同時に民間企業のセキュリティ責任者が折にふれて参考にするものです。この文書内で、未知の脅威への対策として「シグネチャに依存せずにOSのプロセスやメモリ、レジストリへの不正なアクセスや実行を防止する」という手法について明記しています。

準拠
NISC
ガイドライン
2018年版

製品ラインアップ

APPGUARD Enterprise

AppGuard Enterprise は、日々の端末利用で発生するリスクから企業を保護する、一元管理されたマルウェア対策ソリューションです。予め設定されている強固なポリシーで、エンドポイントを常時守り、例外設定や監視の際には、グループごとにポリシー設定やログの収集などの集中管理が可能です。管理はApp Guard管理システム (AGMS：AppGuard Management System)を用いて行います。

APPGUARD Solo

AppGuard Soloは、PC単体でユーザ自身が管理を行うことが可能なAppGuard製品です。PCにインストールするだけで、最新のランサムウェアや未知のマルウェアによる脅威からシステムを守り続けます。20名以下の規模の企業や、ユーザ自身で頻繁なチューニングを行う必要がある開発環境などにおすすめです。

	Enterprise（エージェント）	Solo
OS	Windows 7 SP1*(1), 8, 8.1, 10 全て32/64ビット対応	Windows 7 SP1*(1), 8, 8.1, 10 全て32/64ビット対応
CPU	Intel 1.8GHz以上	Intel 1.8GHz以上
メモリ	1GB以上	1GB以上
ディスク容量	50MB以上の空き容量	50MB以上の空き容量
仮想化環境	動作可能	動作可能
管理システム（AGMS ）	MSP（Managed Service Provider）より提供*(2)	不要

*(1) Windows 7 をご利用中の場合、Windows Update KB3035131、KB3033929 の適用が必須となります。
*(2) 自社保有（オンプレミス）をご希望の場合は、販売代理店にお問合せ下さい。

Blue Planet-worksについて

2017年4月設立。ANAホールディングス、第一生命保険、損保ジャパン、電通、電通国際情報サービス、大興電子、PCIホールディングス、JTB、吉本興業などの出資を受け、アメリカのBlue Ridge Networks社が保有するサイバーセキュリティ技術とその開発者、関連する知財などを買収。このサイバーセキュリティ技術は、検知をせずにコンピューターの不正動作を完全防御し、軽量でかつアップデートも不要という革新的な製品を生み出した。Blue Planet-worksはその技術を搭載した「AppGuard」とその派生商品の開発を行い、2017年後半より日米の法人向けに販売を開始。

Blue Planet-works
Safety for the Connected World

株式会社Blue Planet-works
〒150-0001 東京都渋谷区神宮前2-4-11 Daiwa 神宮前ビル 3F
www.blueplanet-works.com
お問合せ先：セールスインフォメーションセンター salesinfo@blueplanet-works.com

お問い合わせ

AGCAT201901A

脅威を探さないエンドポイントセキュリティ、APPGUARD 誕生。

Innovative Concept 旧概念 vs 新概念

増大するマルウェア数

2013年 検知されたマルウェア数
1億8,300万個

2018年 検知されたマルウェア数
8億5,500万個
（新種のマルウェア1億3,600万個）

Source：AV-TEST - The Independent IT-Security Institute

サイバーセキュリティの課題

これまでのセキュリティ対策は、脅威をいち早く見つけ出して駆除することが目的でした。しかしながら今日、1日平均40万個以上発生する新種のマルウェアをすべて見つけ出して100%その脅威に対処することは、従来の検知型セキュリティソフトでは困難です。

多層防御すれば安全ですか？

パターンマッチング方式のアンチウイルスソフトだけでなく、振る舞い検知型やホワイトリスト型のセキュリティ対策を併用する、いわゆる多層防御も普及しています。振る舞い検知は、疑わしいプログラムを実際に動かすことで脅威を探し出す手法ですが、過去の脅威情報に基づいているため、未知の脅威を完全に見つけ出すことはできません。ホワイトリストでは、あらかじめ登録した信頼できるプログラムだけ起動を許可しますが、プログラム更新のたびにポリシーの検証が必要になるなど管理が煩雑です。加えて、ファイルレスマルウェアのような防御できない攻撃が存在します。

Why Innovative? 悪さをさせない！

従来の「検知型」エンドポイント・セキュリティ概念

革新は、違うカタチをしている。
APPGUARD
BPw, reinventing Cybersecurity

OSに対して害のある行為を阻止

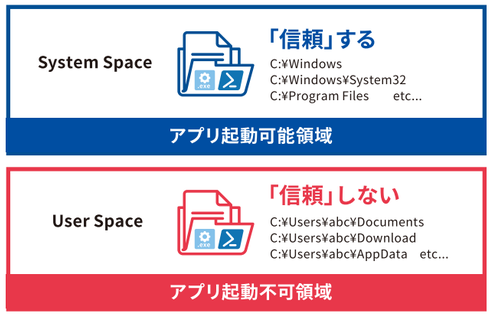
OSの中枢部を
悪意のある
行為から守る

「悪さ」をさせない

OSの安全性を確保：正常な動作を守る

Features AppGuardの特徴

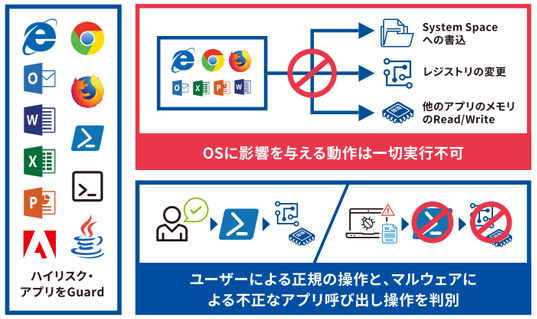
未知のマルウェア実行防止



信頼できる場所にあるアプリだけを起動

マルウェアが侵入しやすい領域から不正な実行ファイルを起動させません。

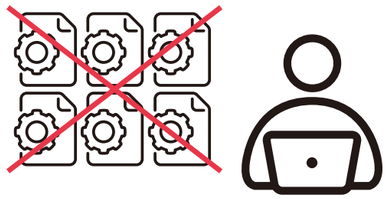
ファイルレスマルウェア実行防止



ブラウザやメール、コマンドプロンプトなど、狙われやすいアプリを隔離して不正な動きをブロック

不正なプログラムによる操作とユーザによる操作をしっかり見分けるので使い勝手に影響を与えません。

面倒な設定不要！ホワイトリストではありません！



サードパーティ製のアプリや、専用開発のアプリをたくさん使っている場合も面倒な設定は不要

ホワイトリスト型の脅威対策製品とは異なり、アプリごとの起動ポリシー定義は原則不要です。（User Spaceから起動するアプリの許可など）必要最低限のポリシー設定でお使いいただけます。

APPGUARDの主な特徴

- ☑ 未知のマルウェア実行防止
- ☑ ランサムウェア実行防止
- ☑ ドライブバイダウンロード実行防止
- ☑ ファイルレスマルウェア実行防止
- ☑ マルウェアによる機密情報漏洩の防止
- ☑ OS 改ざん防止