HITACHI
Inspire the Next

標的型攻撃対策ソリューション
ご説明資料

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

Contents

1.はじめに

1.はじめに

近年、サイバー攻撃は、ネットワークでのセキュリティ対策を通過するなど、
より悪質で高度化したマルウェアが増加しており、**企業のITシステムだけでなく、制御システムにまで脅威が拡散し、工場の生産ラインが停止するなどの被害**がでています。

内閣サイバーセキュリティセンターが策定している「政府機関等の対策基準策定のためのガイドライン」でも、**「未知・既知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアの導入」**が順守事項に含まれており、検知型対策製品では検出することが困難な**未知のマルウェアに対するセキュリティ対策は社会課題**となっています。

HITACHI
Inspire the Next

2.標的型攻撃対策ソリューション

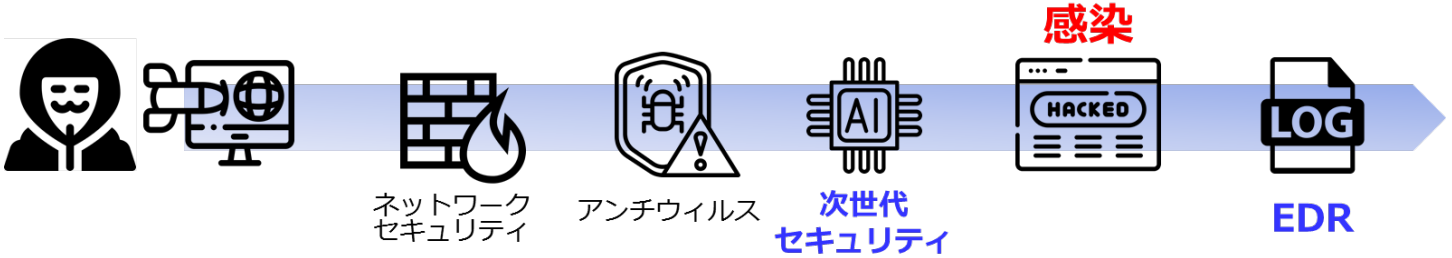
2 – 1. 課題

お客さまのシステムにおいて、このようなお悩みはありませんか？

課題	解決
ITシステム/制御システムの標的型攻撃対策を行いたい	未知・既知を問わず、マルウェアの実行を防止し、システムを標的型攻撃から守ります。
新たな脅威（ウィルス）に対する対策に困ってはいるが、セキュリティ対策に時間やコストをかけたくない	従来の検知型対策製品で必要だった定義ファイルの更新などの保守・運用費用コストをかけずに標的型攻撃対策が可能です。
ニーズに合わせた効果的なセキュリティ対策を支援してほしい	要件定義からポリシー設計／テスト、導入、運用サポートまで、お客さまのニーズに合わせた効果的な標的型攻撃対策をワンストップで提供します。

HITACHI
Inspire the Next

AV（Anti-Virus）すり抜けを前提とするソリューションの流行



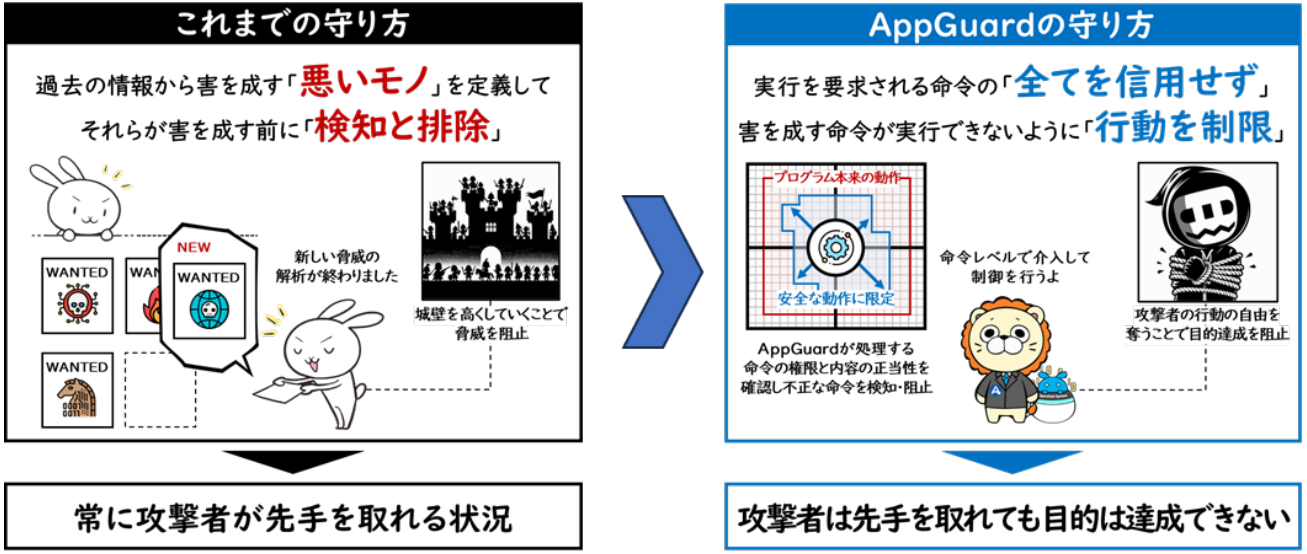
「検知型製品の構造的限界」と「攻撃者側の環境変化」により
感染後の対応迅速化を目的とした下記のソリューションが流行しています。
EDR（Endpoint Detection & Response）
AIを活用した次世代セキュリティ

しかし・・・
これらでは全ての新種マルウェアやゼロデイの攻撃は止められません。

2 – 2. 標的型攻撃対策ソリューションの特長

1.　ITシステム／制御システムの標的型攻撃対策が可能

　従来の検知型対策製品で検知が困難な未知のマルウェアを含め、
悪意のある不正プログラムの実行を防止し、OS中枢部を悪意のある行為から守ります。
　定期的なスキャンが不要でシステムへの負荷も少ないため、ITシステムはもちろんのこと、
環境のオープン化に向けて対策が急務とされている**制御システムの標的型攻撃対策にも有効**です。



2 – 2. 標的型攻撃対策ソリューションの特長

HITACHI
Inspire the Next

2.　セキュリティ対策全体の運用コストの削減が可能

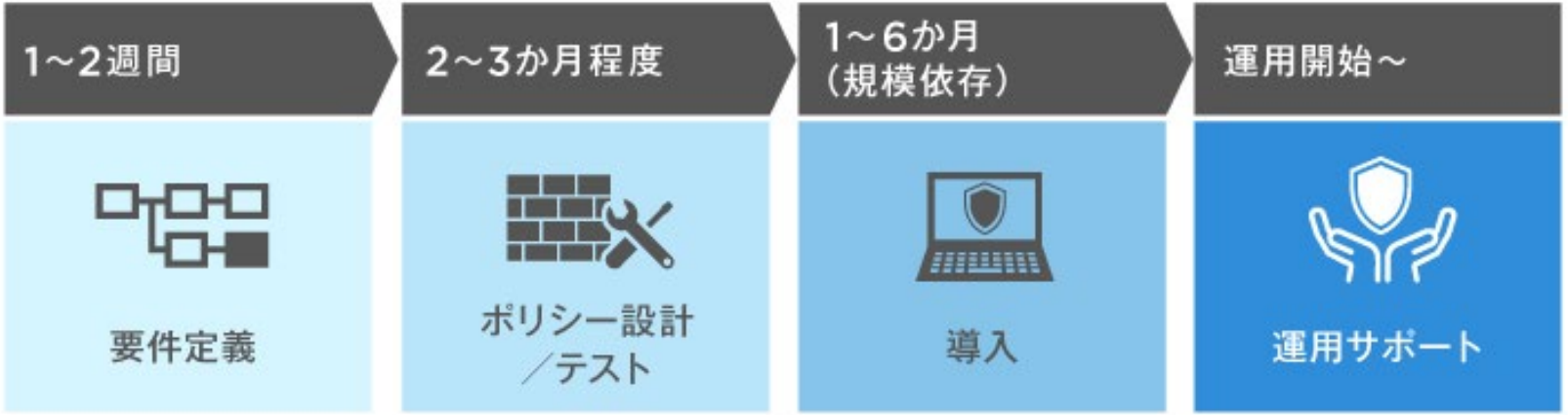
攻撃の段階で脅威を遮断する新概念により、定期的なセキュリティポリシーの更新は不要です。
このため、従来の検知型対策製品から置き換えた場合には、**定義ファイルの更新などの保守・運用費用の削減が可能**です（お客さまのニーズにより、検知型対策製品との併用も可能です）。

※本ソリューションでは標的型攻撃を遮断する手段として「AppGuard®」を活用しています

HITACHI
Inspire the Next

3.　効果的なセキュリティ対策をワンストップで提供

標的型攻撃対策ソリューションでは、要件定義からポリシー設計／テスト、導入、運用サポートまで、お客さまのニーズに合わせた効果的な標的型攻撃対策をワンストップで提供します。



2 – 3. 標的型攻撃対策ソリューションメニュー

HITACHI
Inspire the Next

ソリューションメニュー

項目	内容	
導入支援サービス	要件定義	セキュリティポリシーの確認
		導入範囲の定義
	ポリシー設計/テスト	ポリシー設計/作成
		ポリシーテスト/チューニング
	導入	適用対象へのポリシー導入作業
	運用サポート	問い合わせ対応
		システム変更対応などの運用支援
管理サーバー構築サービス	システム構成、接続方法などの設計	
	管理サーバーの構築	
	稼働テスト	
トレーニングサービス	運用者・管理者を対象としたトレーニング	

2 – 4. 標的型攻撃対策ソリューションの適用例

HITACHI
Inspire the Next

ソリューション適用例

ITシステム

OA系

利用者端末、業務サーバーなどの汎用機器

組込み系

デジタルサイネージ、POS、ATMなどの専用機器

制御システム

制御系

監視用端末、監視制御サーバーなどの汎用機器やPLC、HMIなどの制御機器

HITACHI
Inspire the Next

3.AppGuard®のご紹介

HITACHI
Inspire the Next

AppGuard®の特長

AppGuard®は、新概念の「ゼロトラスト型エンドポイントセキュリティ製品」です。

従来型 **検知型**

過去にない新しい振舞や未知の攻撃パターンから守れない

従来型 **ホワイトリスト型**

アプリケーションの追加やバージョンアップなどを行うたびにリストの更新が必要なため、汎用パソコンで運用するのは困難

新概念！ **ゼロトラスト型**

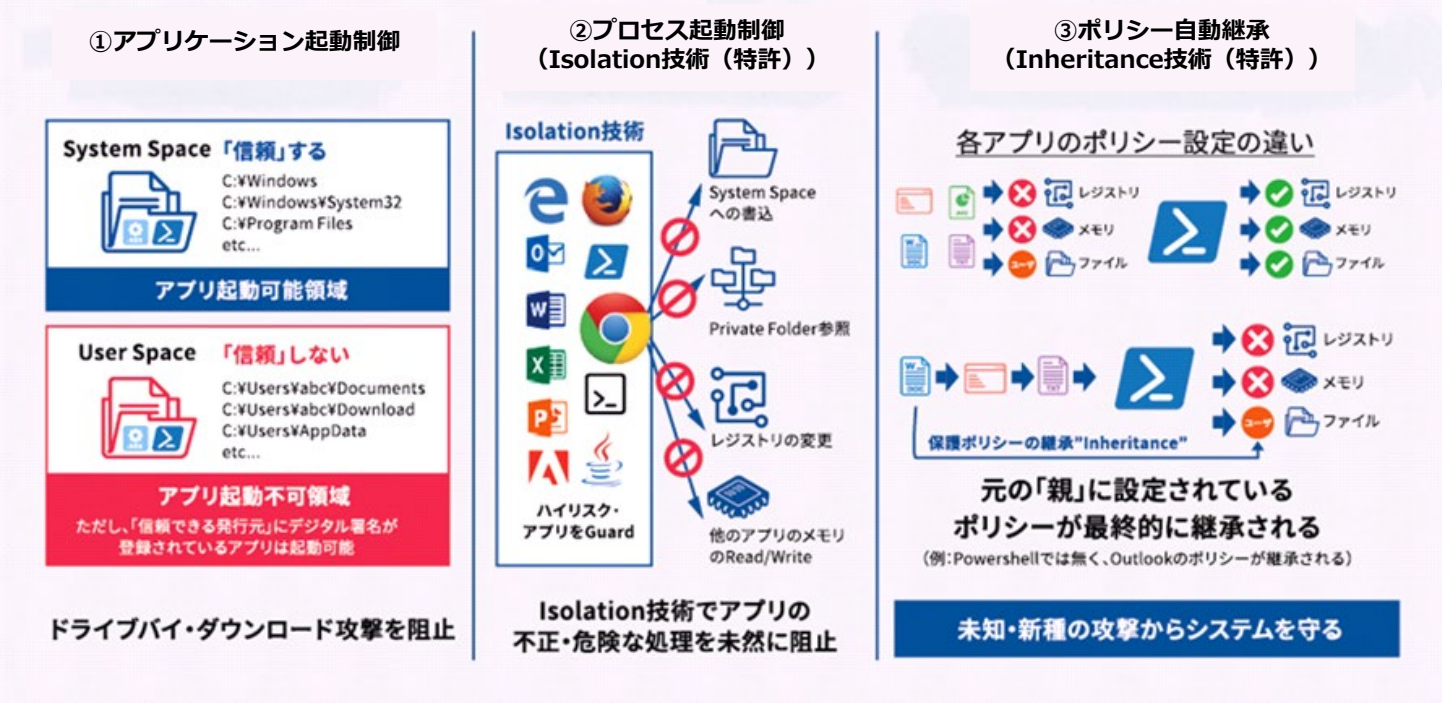
5つの観点でプロテクト！
①信頼するアプリケーションのみ起動
②信頼できてもOSへの動作は防御
③システムスペースを防御
④メモリーを防御
⑤重要データを保護

→ 未知・既知に関わらず、悪意のある不正プログラムの実行を防止し、OSの中枢部を悪意のある行為から守ります

HITACHI
Inspire the Next

AppGuard®の機能

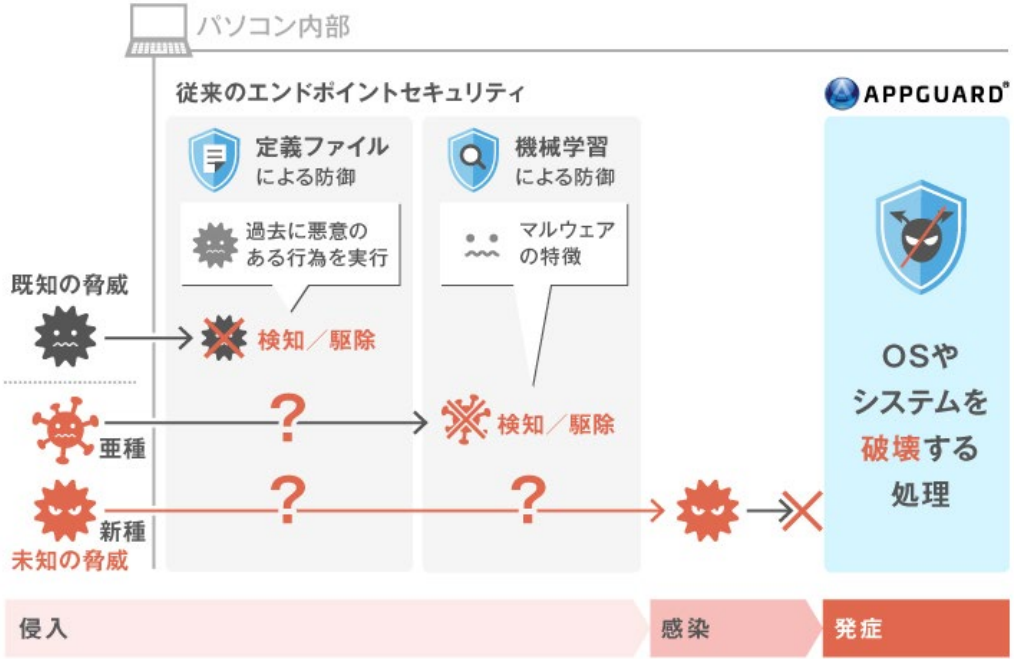
AppGuard®は3つの機能で、OSの中枢部を悪意のある行為から守ります。



HITACHI
Inspire the Next

AppGuard®は攻撃を成立させない

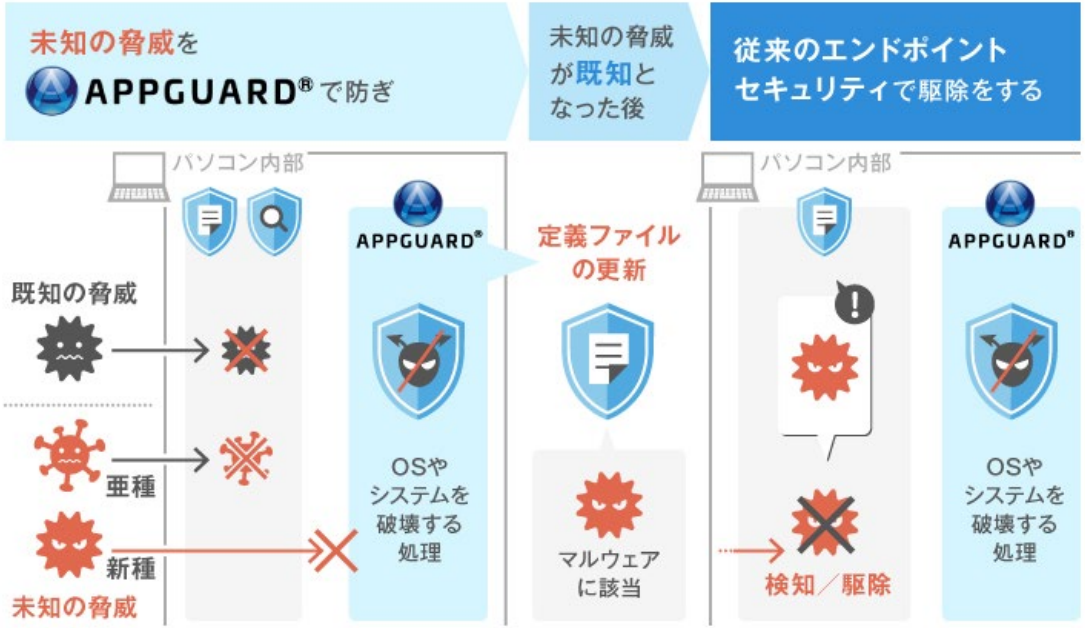
AppGuard®は、従来のセキュリティ製品のようにマルウェアを検知/駆除するのではなく、不正な行為を監視/遮断するものです。こうした機能は未知の脅威に完全には対応できない従来型のセキュリティ製品の弱点をカバーします。



HITACHI
Inspire the Next

従来型のセキュリティとの組み合わせで、より強力なセキュリティ対策を実現

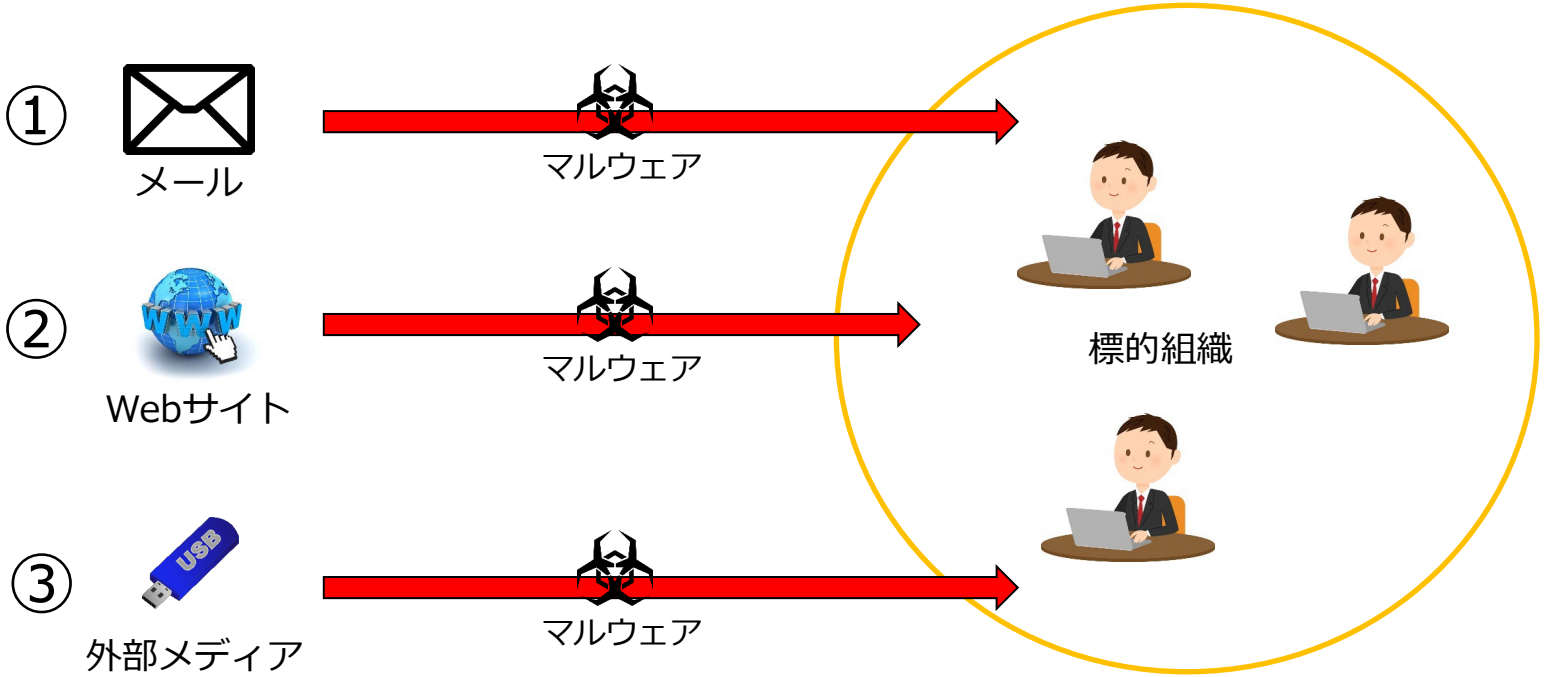
AppGuard®は、未知の脅威が不正な行為を実行する前にその行為を阻止し、その上で「既知の脅威」として認定します。これにより、従来型のセキュリティ製品に脅威を識別させ、駆除させることができます。
従来型のセキュリティ製品と組み合わせることで、より効果的なセキュリティ対策が可能です。



HITACHI
Inspire the Next

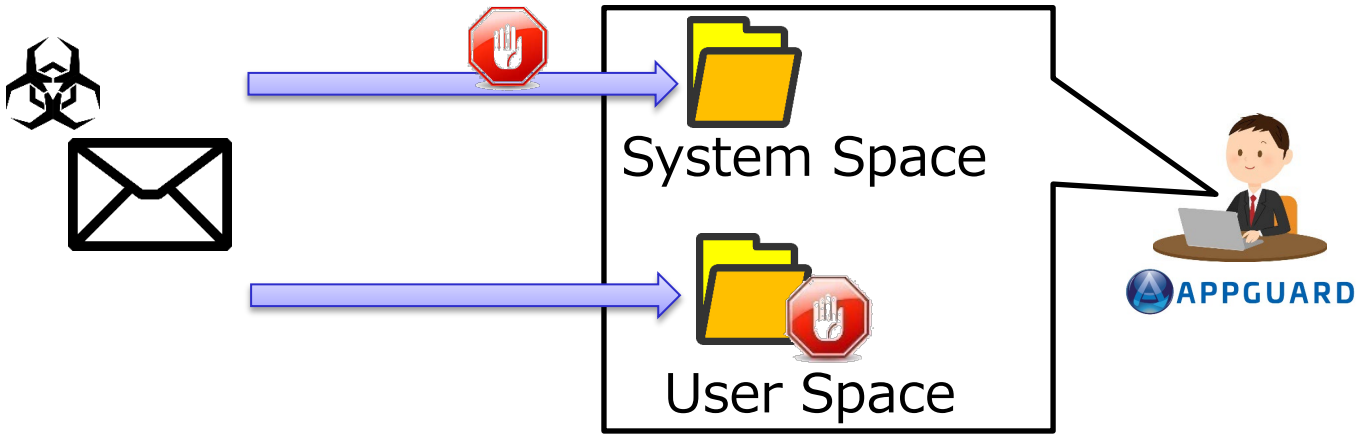
マルウェアの侵入経路

マルウェアの侵入経路には大きく「①メール」、「②Webサイト」、「③外部メディア」の3つがあります。



1．メール経由のマルウェアに対するAppGuard®の動作

AppGuard®は、メールに添付されたファイルをSystem Space（※1）へ保存させません。
User Space（※2）への保存は可能ですが、万一マルウェアが侵入した場合でも、マルウェアを起動させません。

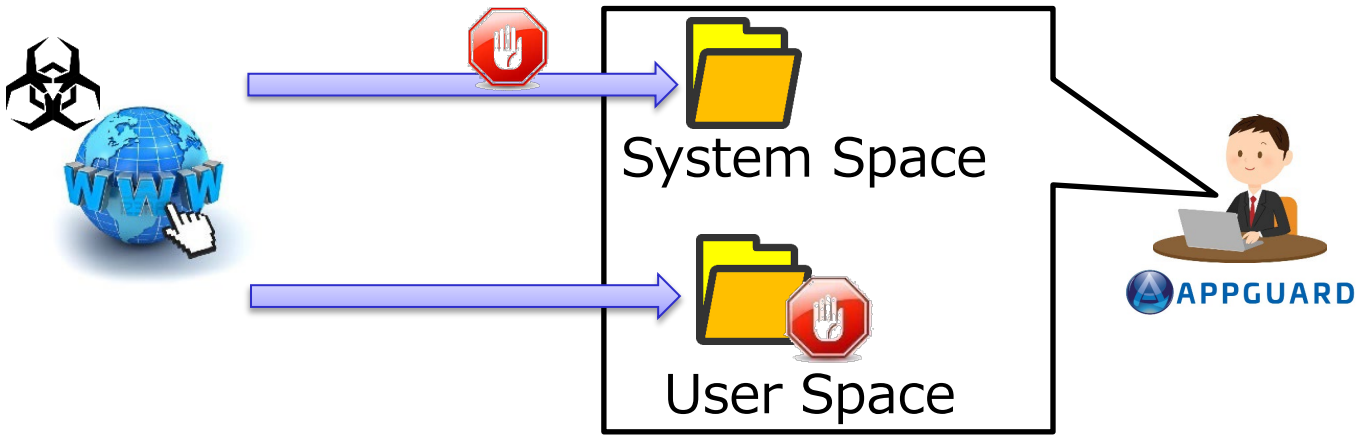


※1.System Space
AppGuard®が定義する、OSに関わるPC領域のこと　（例.Cドライブ直下のWindowsフォルダやProgram Filesフォルダなど）

※2.User Space
AppGuard®が定義する、ユーザーがファイル操作する機会の多いPC領域のこと　（例.デスクトップ、マウントされた外部メディアなど）

2．Webサイト経由のマルウェアに対するAppGuard®の動作

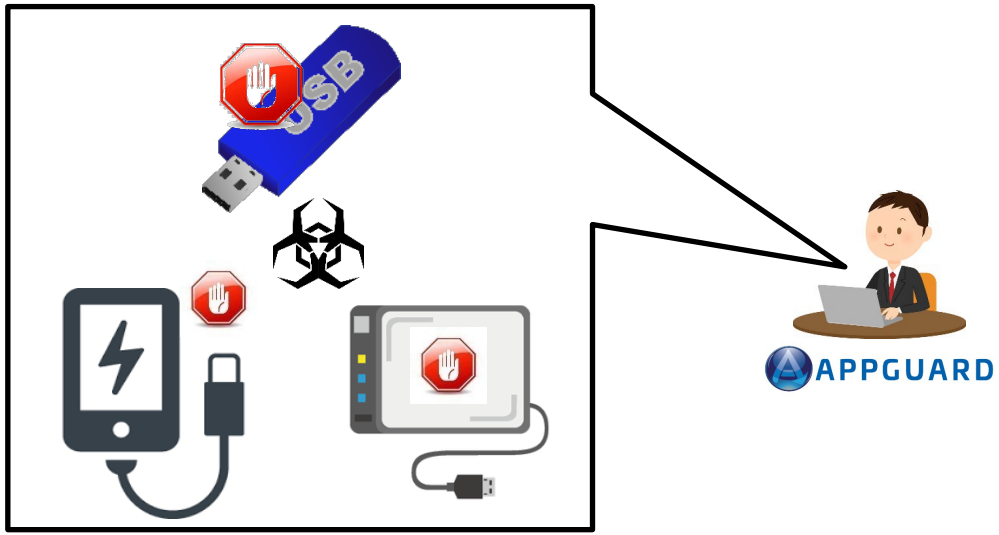
AppGuard®は、Webサイトからダウンロードしたファイルを System Spaceへ保存させません。
User Spaceへの保存は可能ですが、万一マルウェアが侵入した場合でも、マルウェアを起動させません。



HITACHI
Inspire the Next

3．外部メディア経由のマルウェアに対するAppGuard®の動作

AppGuard®は、USBデバイス経由でマウントしたドライブから、アプリケーションを起動させません。



HITACHI
Inspire the Next

AppGuard®の製品ラインアップ

AppGuard®は、現在３つのエディションを提供しています。

APPGUARD Enterprise

**利用者端末、組込み系の専用端末、制御機器などの
Windows PCを対象に、未知のマルウェアの実行を防止します。**

APPGUARD Solo

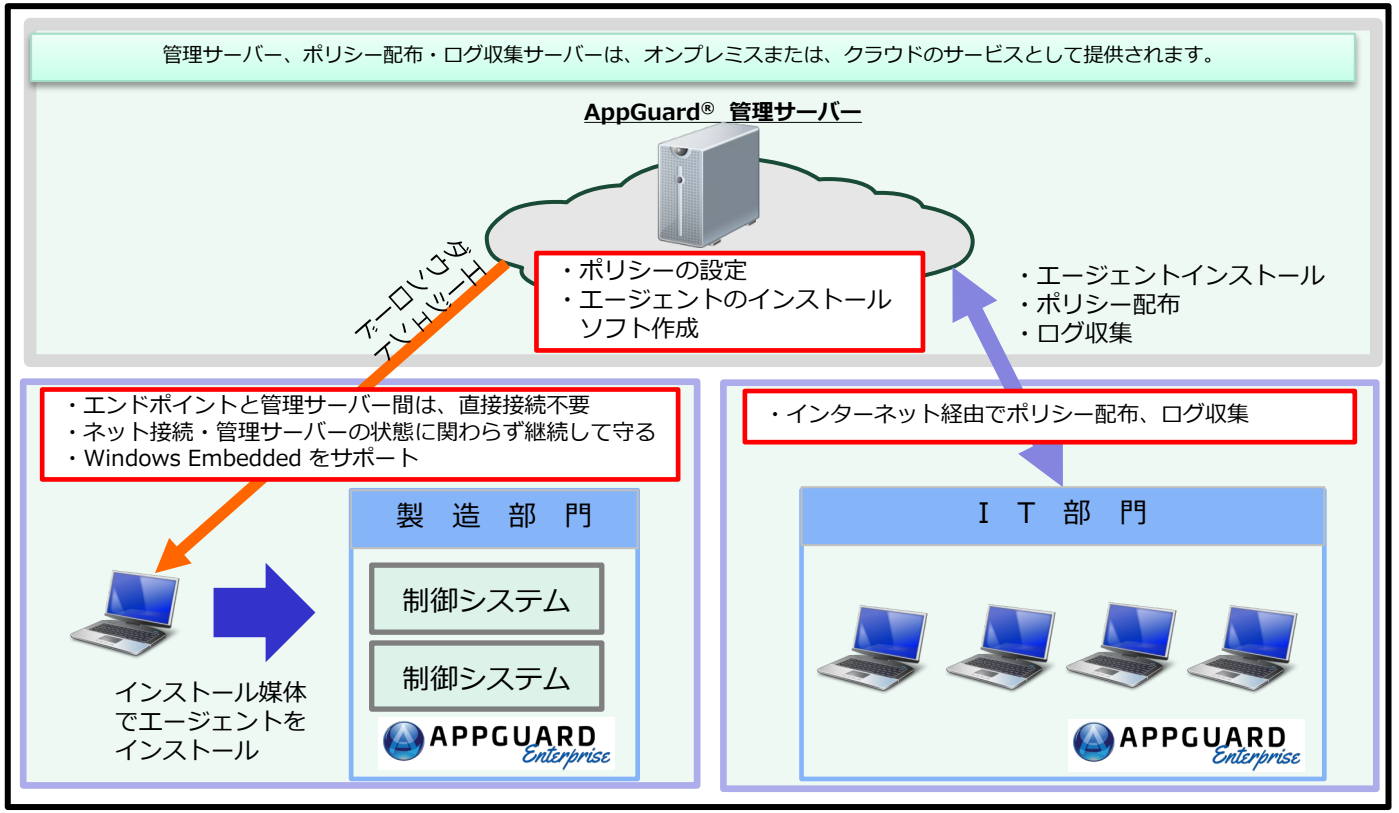
**スタンドアロン型で、小規模環境のWindows PCを対象に
未知のマルウェアの実行を防止します。**

APPGUARD SERVER

**業務サーバーや監視制御サーバーなどのWindows Serverを対象に
未知のマルウェアの実行を防止します。**

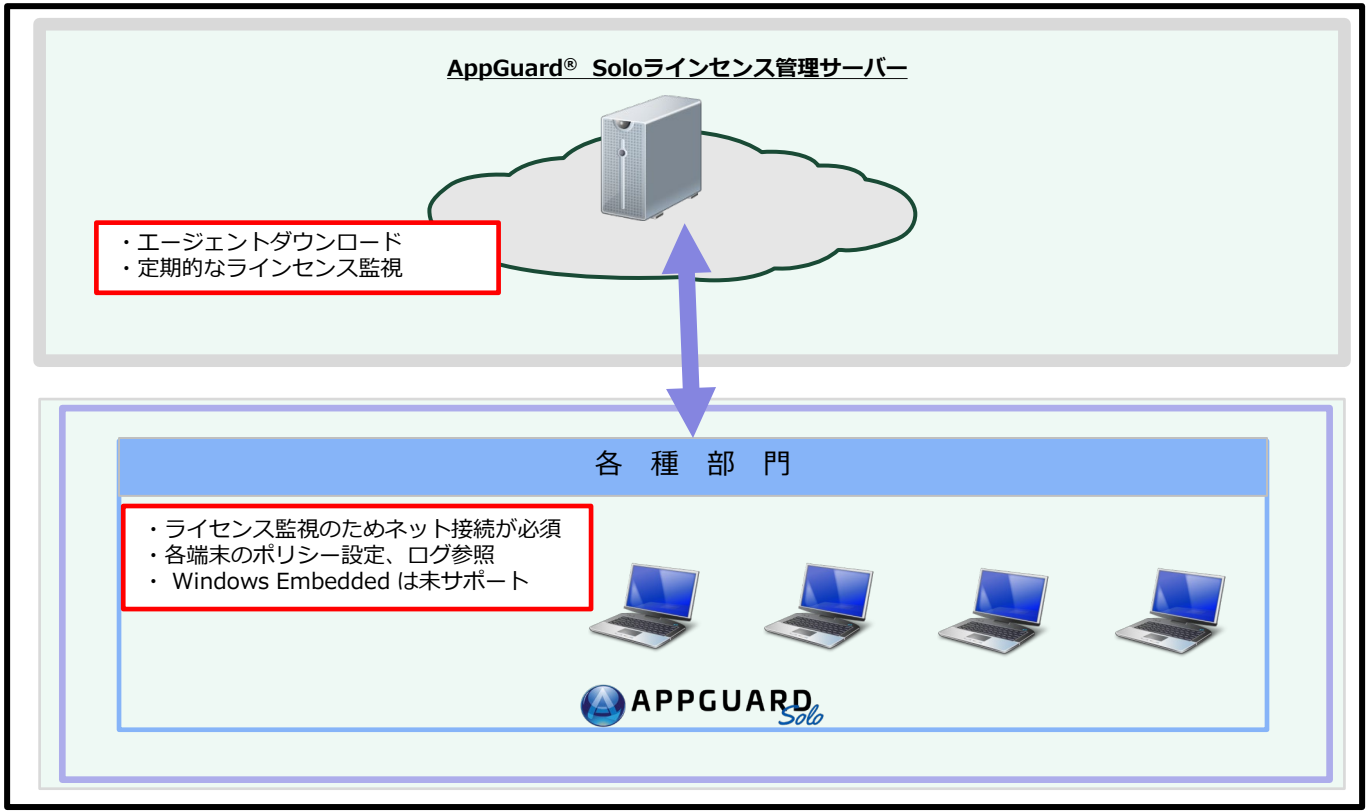
3 － 5 . AppGuard® Enterpriseの構成

AppGuard®管理サーバーでポリシーの設定、エージェント作成、配布、ログ収集を行います。



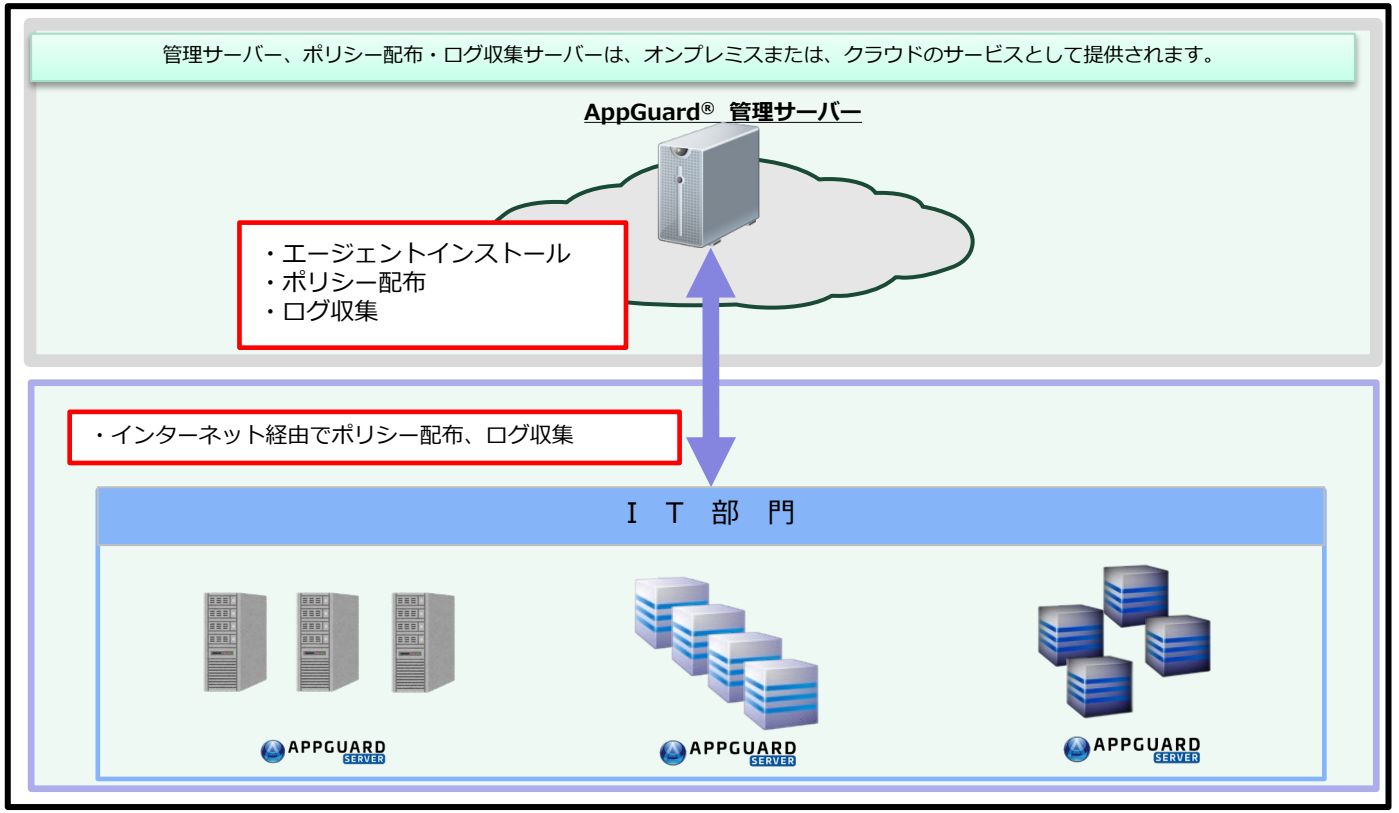
3 – 6. AppGuard® Soloの構成

スタンドアロン型、ポリシー設定やログの参照など、全てインストールされたパソコン上で行います。



3 – 7. AppGuard® Serverの構成

AppGuard®管理サーバーでポリシーの設定、エージェント作成、配布、ログ収集を行います。



HITACHI
Inspire the Next

AppGuard® Enterprise

ソフトウェア	提供形態		対応OS	
	サブスクリプション	オンプレミス		
AppGuard® 管理サーバー	○	○	OS	x64 Windows Server 2016以上
			CPU	タイプ：シングルコアまたはデュアルコアの最新のCPU, またはクアッドコア 速度：3GHz以上
			メモリー	16GB以上
			ディスク容量	利用環境による
AppGuard® Enterprise エージェント	○	-	OS	Windows10, Windows11 他
			CPU	Intel 1.8GHz以上
			メモリー	32bit OS 1GB以上 64bit OS 2GB以上
			ディスク容量	100MB以上の空き容量

以下Blue Planet-works社HPより抜粋。最新情報については、当社にお問い合わせください。
https://www.blueplanet-works.com/solution/appguard.html

HITACHI
Inspire the Next

AppGuard® Solo

ソフトウェア	提供形態		対応OS	
	サブスクリプション	オンプレミス		
AppGuard® Solo	○	-	OS	Windows10, Windows 11 他
			CPU	Intel 1.8GHz
			メモリー	32bit OS 1GB以上 64bit OS 2GB以上
			ディスク容量	100MBの空き容量

以下Blue Planet-works社HPより抜粋。最新情報については、当社にお問い合わせください。
https://www.blueplanet-works.com/solution/appguard.html

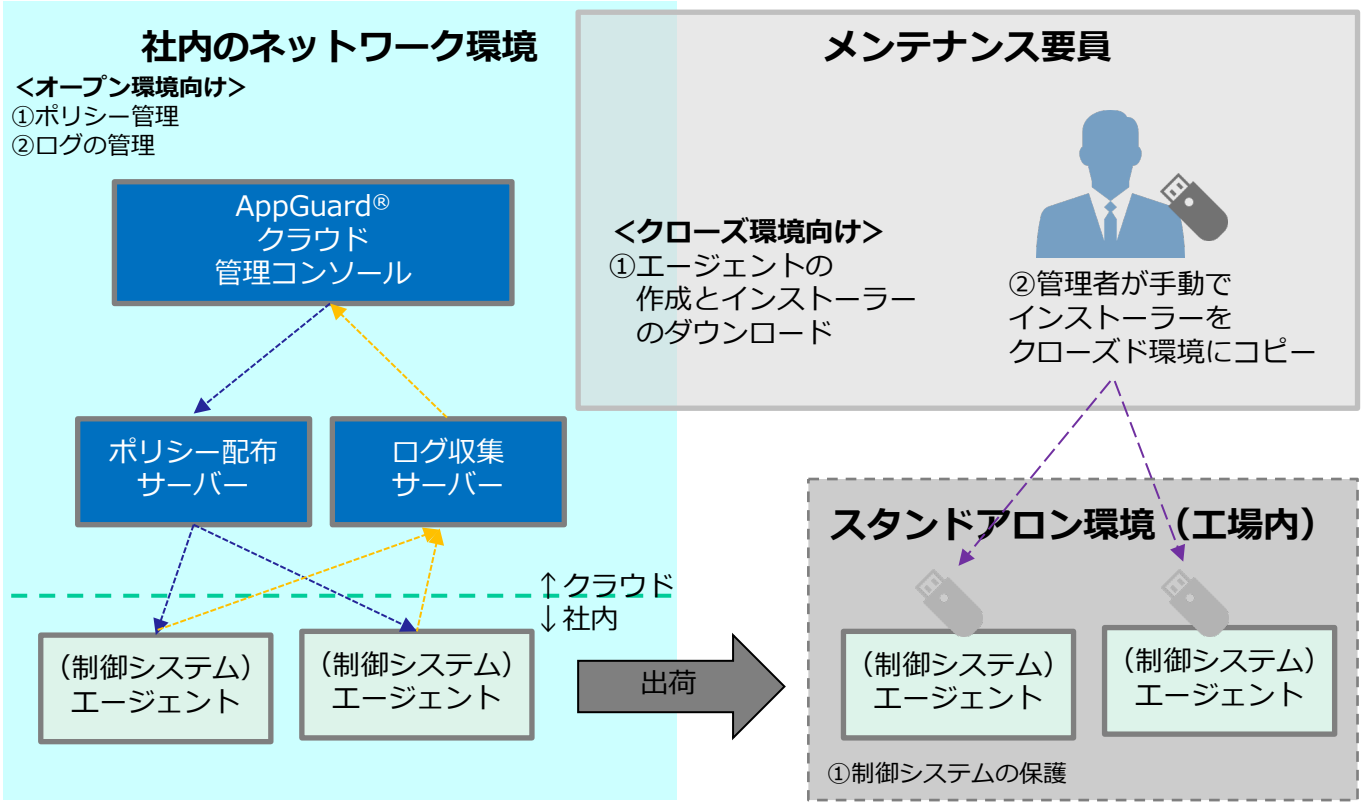
HITACHI
Inspire the Next

AppGuard® SERVER

ソフトウェア	提供形態		対応OS	
	サブスクリプション	オンプレミス		
AppGuard® SERVER 管理サーバー	○	○	OS	x64 Windows Server 2016以上
			CPU	タイプ：シングルコアまたはデュアルコアの最新のCPU, またはクアッドコア 速度：3GHz以上
			メモリー	16GB以上
			ディスク容量	利用環境による
AppGuard® SERVER エージェント	○	-	OS	Windows Server 2016,2019,2022 他
			CPU	Intel 1.8GHz以上
			メモリー	32bit OS 1GB以上 64bit OS 2GB以上
			ディスク容量	100MBの空き容量

以下Blue Planet-works社HPより抜粋。最新情報については、当社にお問い合わせください。
https://www.blueplanet-works.com/solution/agserver.html

3 – 9. 運用/メンテナンスのイメージ



HITACHI
Inspire the Next

AppGuard®と他ソリューションとの違い

	APPGUARD	アンチウイルス	振舞検知	AI機械学習	EDR End Point Detection & Response	ホワイトリスト
未知、ランサムウエア、武装化、最新の脅威からの防御	✓	✗	△	△	✗	✓ Unknown binary ✗ Weaponized
ファイルレスマルウエアからの防御	✓	✗	△	✗	✗	✗
最新のメモリ攻撃からの防御	✓	✗	△	✗	✗	✗
定期的なディスクスキャン	✓ 不要	✗ 必要	✗ 必要	✗ 必要	✗ 必要	✓ 不要
軽量、軽快	✓	✗ 重い	✗ 重い	✗ 重い	✗ 重い	✗ 重い
アップデート（定義ファイル、AIエンジンダウンロード）	✓ 不要	✗ 必要	✗ 必要	✗ 必要	✗ 必要	✓ 不要
マルウエアの駆除	✗ 駆除しない	△ 既知のみ	△ 既知のみ	△ 既知のみ	△ 既知のみ	✗ 駆除しない
業務OA　PCへの適用性	✓	✓	✓	✓	✓	✗ 特定用途
常時ネットワーク接続: 継続してシステムを守る	✓ 不要	✗ 必要	✗ 必要	✗ 必要	✗ 必要	✓ 不要
運用コストの削減	✓ 大幅削減	✗	✗	✗	△	✗

HITACHI
Inspire the Next

AppGuard®が阻止する攻撃例

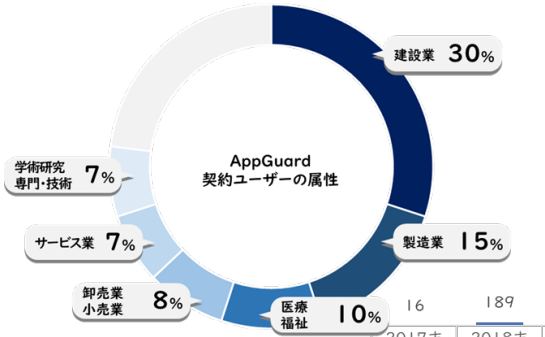
攻撃		防御方法
高度標的型攻撃 フィッシング	インターネット上でネットバンクなどの正規のサービスになりすまし、ユーザーからIDやパスワードなどの個人情報を盗み出す	メールの添付ファイル、悪意のあるURLからのダウンロードなど、マルウェア（またはファイルレス）の起動・コード実行を阻止
ドライブバイ ダウンロード	ユーザーが気付かないうちに、ブラウザーからマルウェアがダウンロードされる	マルウェアの起動を阻止
ファイルレス	悪意のあるコードを実行可能ファイルとしてファイルシステム上に保存することなく、メモリー上で直接実行し、情報を盗み出す	他プロセスのメモリーへのアクセスを阻止
ランサムウェア	エンドポイントやサーバーのデータを暗号化する	不正なリモート操作やファイルの改ざん、レジストリの改ざんを阻止
トロイの木馬	エンドポイント上に常駐し、情報の窃取や不正処理を実施する	システム領域への書込み、メモリーへのアクセスなどを阻止
Weaponized Doc （武装化ドキュメント）	Word、PDFなどの添付ファイルに潜み、ドキュメントが開かれたときに悪質なスクリプトを実行する	スクリプトの実行を阻止
ゼロデイ攻撃	脆弱性が発見されて修正プログラムが提供される日（One day）より前に、その脆弱性を攻略する	システム領域への書込み、メモリーへのアクセスなどを阻止

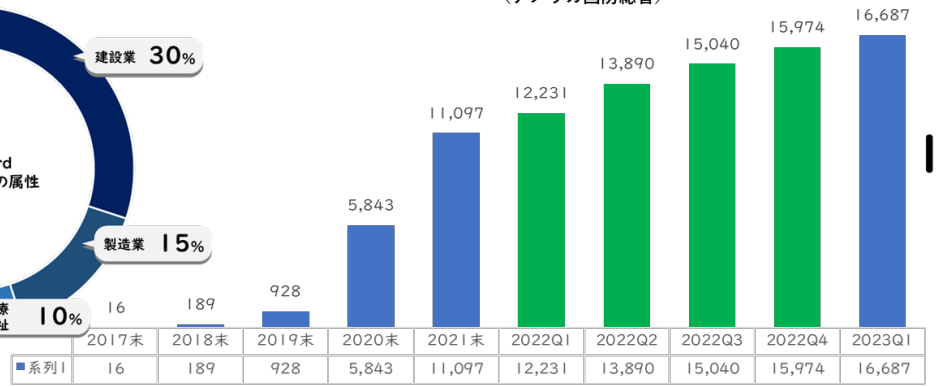
HITACHI
Inspire the Next

AppGuard®の販売実績

（白石市様）

（アメリカ国防総省）





国内導入累積社数
19,000社突破
（2024年3月末時点）

HITACHI
Inspire the Next

防御力の強さを示すユーザーテストの結果

米国政府機関で利用されている中で20年間破られていない技術です

国内大手流通企業S社

8社の次世代ソリューションをそろえ、
既知マルウェアとサンプルや
自作の未知マルウェアでペンテストを実施。
AppGuard®は未知・既知ともに攻撃を
100%阻止

国内大手証券企業O社

システム担当者が未知でかつ、
メールゲートウェイなどをすり抜ける
各種マルウェア25個で攻撃するも100%阻止

国内大手航空企業A社

5社の次世代ソリューションに、
未知・既知を合わせて145種のマルウェアで
攻撃するペンテストを実施し、
AppGuard®は攻撃を100%阻止

公共機関

多数のセキュリティソリューションに
未知・既知を合わせて400種のマルウェアで
攻撃するペンテストを実施し、
AppGuard®は攻撃を100%阻止

3－10．補足資料（組込みライセンスについて）

HITACHI
Inspire the Next

	項目	組込みライセンス	通常ライセンス		備考
1	対象製品	AppGuard® Industrial	AppGuard® Enterprise	AppGuard® Solo	組込みライセンスは別途取扱契約が必要
2	対応OS	Windows 10 IoT	Windows7,8,8.1,10,10 IoT	Windows7,8,8.1,10	Embedded/IoT系は検証が必要
3	出荷形態	装置にインストールされた状態	ライセンス単体		
4	ライセンス形態	5年、7年、無期限	サブスクリプション （1年）		
5	使用用途	特定（組込まれた装置用）	一般事務		
6	販売可能最少数	1,000ライセンス相当／年	1ライセンス		ライセンス相当定義：年間台数＊使用期間 例）200台＊5年＝1,000ライセンス相当
7	最少販売単位	1本	1本		
8	価格テーブル基準	年間目標数量ベース	都度発注数量ベース		
9	別OS、別装置への移行	不可	可（PCの入れ替えなど）		
10	サポート	無（別途有償）	有		有償対応は要件により別途ご相談
11	バージョンアップ版提供	無（バージョンアップは有償）	有		
12	修正版提供	有（通常Windows用）	有		リリース後３年間（出荷後にあらず）
13	エンドユーザーによる転売	不可	不可		転売の場合、使用権は失効します 貴社の引取・再販売は、ご相談
14	価格表示	AppGuard®の部分の価格が単独で見えない価格付け	単独での価格表示		
15	輸出	輸出先ごとに事前に要相談	無		非該当証明書の発行は可能

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

表示に関する注意事項

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- AppGuard® 、AppGuard®のロゴ は米国法人AppGuard, Inc. 、または株式会社Blue Planet-works
  及びその関連会社の、米国、日本またはその他の国における登録商標、または、商標です。
- Microsoft Windows、Microsoft Embedded、PowerShell、Office製品は、米国、その他の国における米国Microsoft Corp.の登録商標です。
- IntelはIntel Corporationの登録商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2024年12月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

お問い合わせ情報についてご相談・ご依頼いただいた内容は回答などのため、
当社の関連会社（日立ソリューションズグループ会社）および
株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。