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

HITACHI
Inspire the Next

1.はじめに

1. はじめに

HITACHI
Inspire the Next

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、**「既知及び未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
２－２　標的型攻撃対策ソリューションの特長
２－３　標的型攻撃対策ソリューションメニュー
２－４　標的型攻撃対策ソリューション適用例

2 – 1. 課題

HITACHI
Inspire the Next

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	既知・未知問わず、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（ウイルス）に対する対策に困ってはいるが、セキュリティ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・運用費用等のコストを掛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	事前評価からシステム構築・導入、技術サポート保守、運用まで、お客さまのニーズに合わせた効果的なセキュリティ対策をワンストップで提供します。

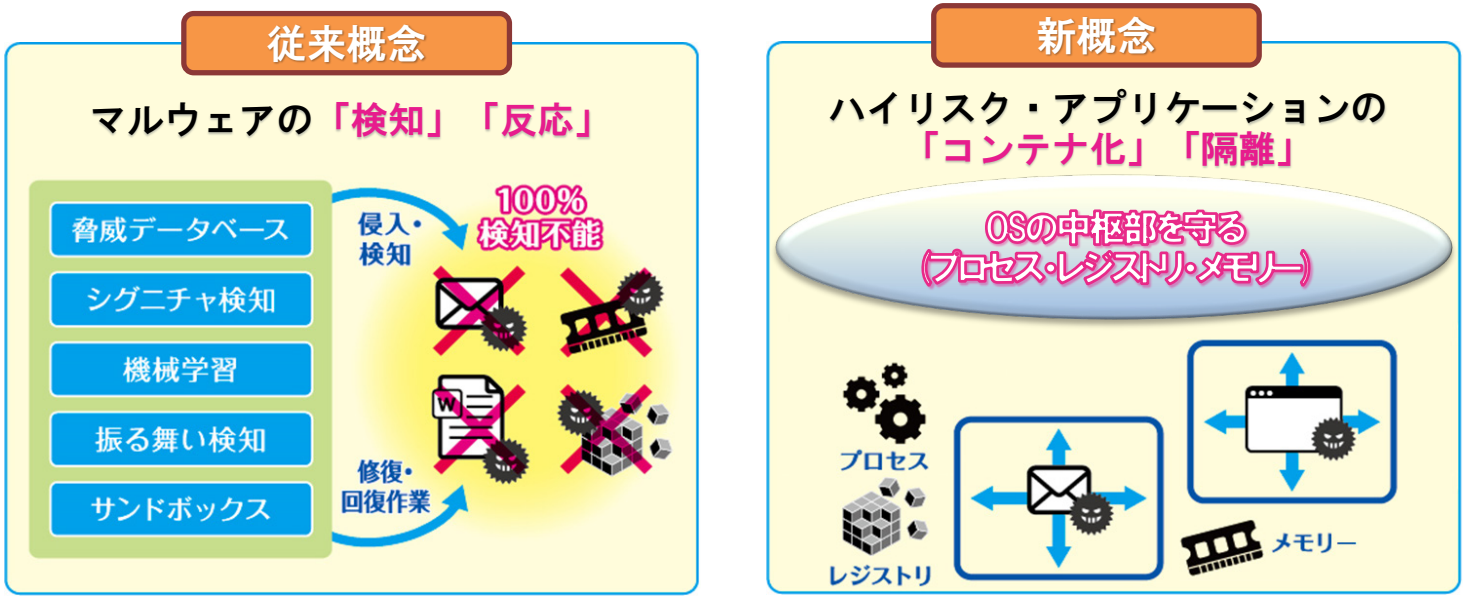
2 – 2. 標的型攻撃対策ソリューションの特長

HITACHI
Inspire the Next

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すること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の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。



感染リスクが高いハイリスクなアプリケーションは起動時に「コンテナ化」し、プロセスを「隔離」し、監視対象下に置きます。

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**となります。
（お客さまのニーズにより、検知型対策製品と併用することも可能です。）

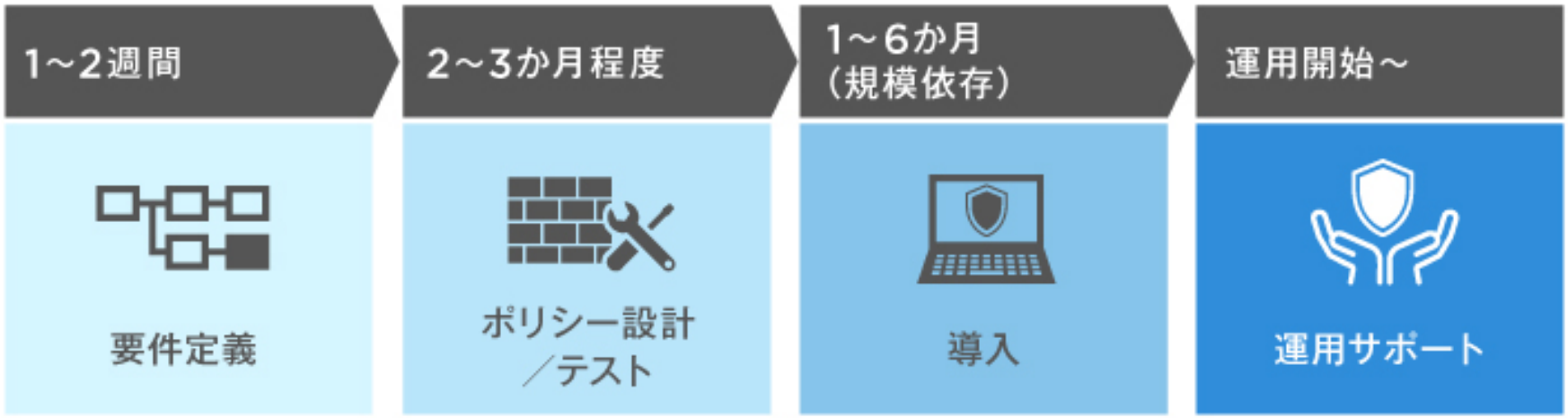
※本ソリューションでは標的型攻撃を遮断する手段として「AppGuard®」を活用しています

2 – 2. 標的型攻撃対策ソリューションの特長

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、要件定義からシステム構築/導入、技術サポート保守、運用まで、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	

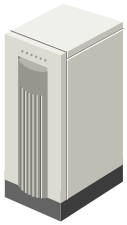
2 – 4. 標的型攻撃対策ソリューションの適用例

HITACHI
Inspire the Next

ソリューション適用例

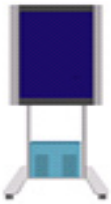
ITシステム

OA系



利用者端末、業務サーバー
などの汎用機器

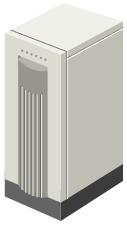
組み込み系



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

3 - 1　AppGuard®の特長
3 - 2　AppGuard®の機能
3 - 3　マルウェアの侵入経路とAppGuard®による防御
3 - 4　AppGuard®の製品ラインアップ
3 - 5　AppGuard®の構成
3 - 6　AppGuard®の動作環境
3 - 7　補足資料

HITACHI
Inspire the Next

AppGuard®の特長

AppGuard®は、新概念の
「OSプロテク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る舞いや未知の攻撃パターンから完全には守れません・・・

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ほぼ不可能・・・

新概念！ **OSプロテクト型**

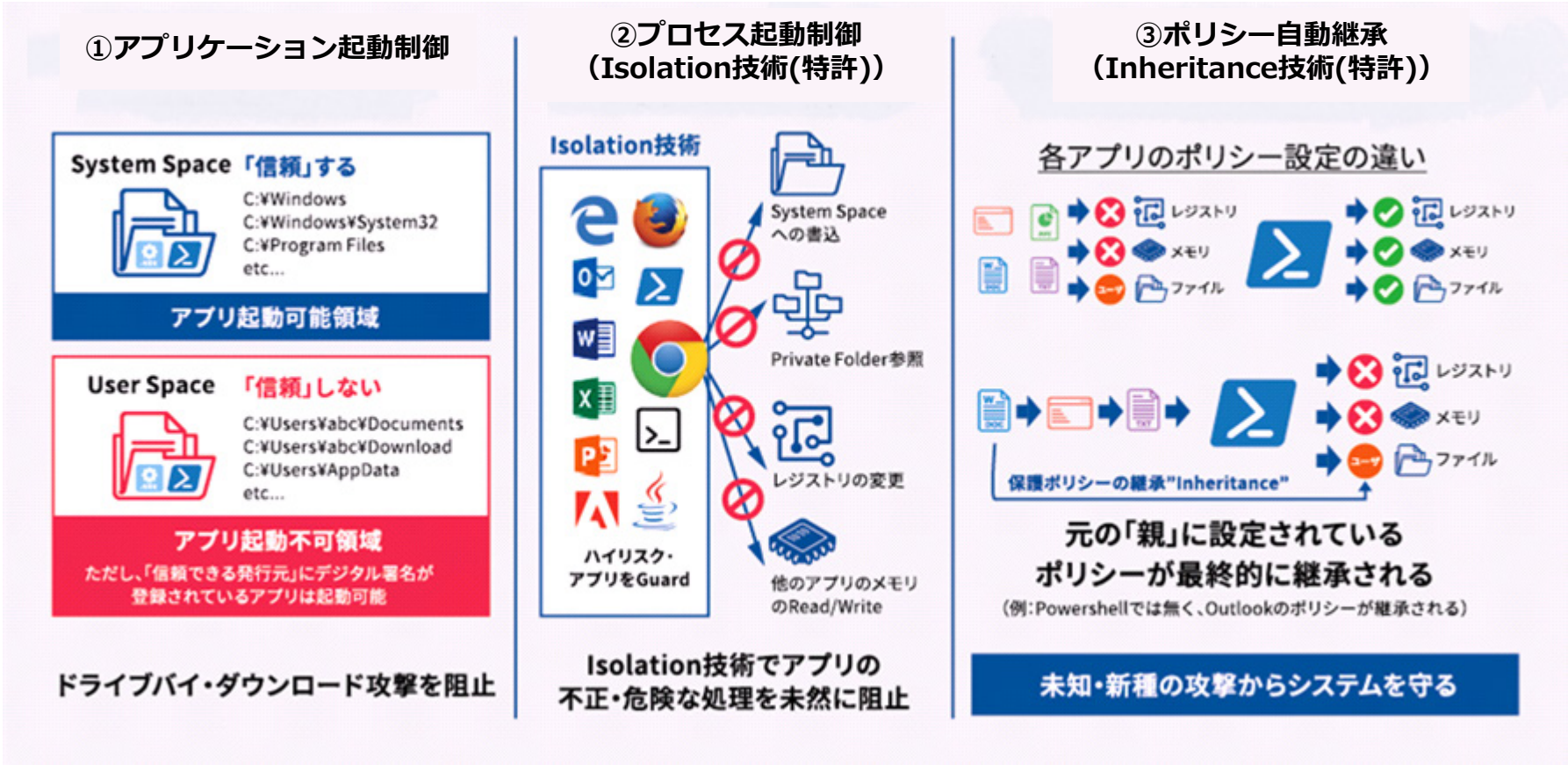
５つの観点でプロテクト！
①信頼するアプリケーションのみ起動
②信頼できてもOSへの動作は防御
③システムスペースを防御
④メモリーを防御
⑤重要データを保護

既知・未知に関わらず、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

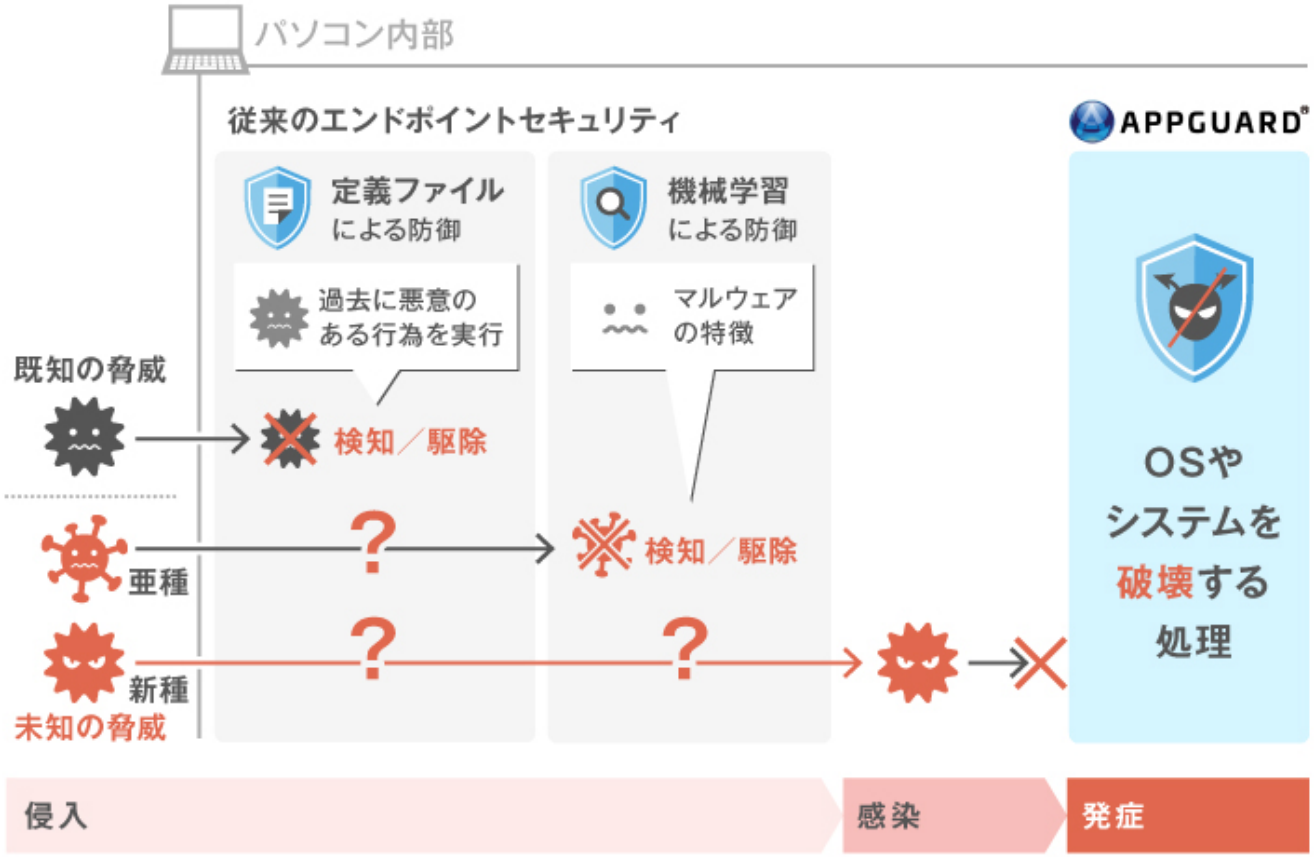
AppGuard®は3つの機能で、OSの中枢部を悪意のある行為から守ります。



HITACHI
Inspire the Next

AppGuard®はノーガード

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（ノーガード）、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。

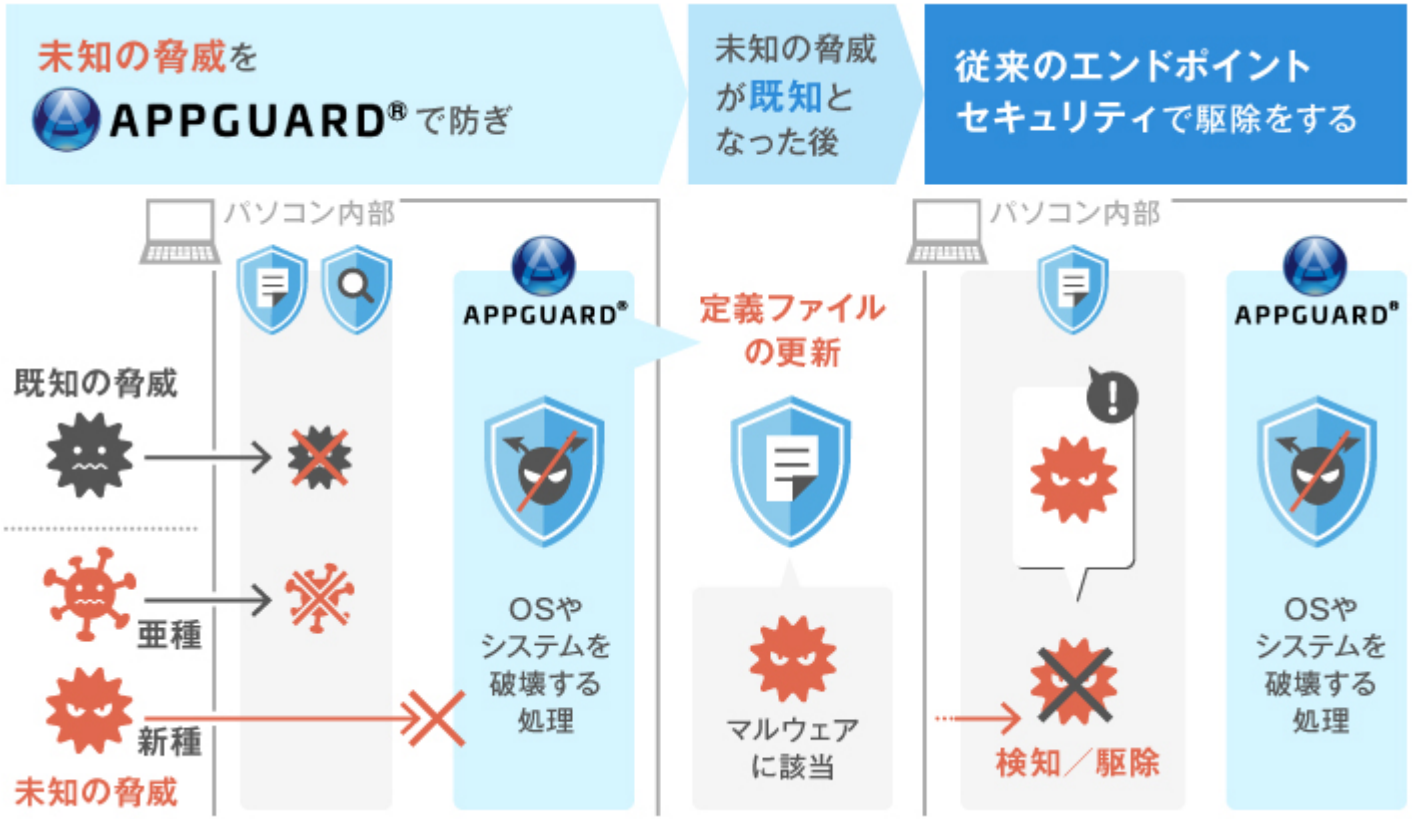


3 – 2. AppGuard®の機能

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

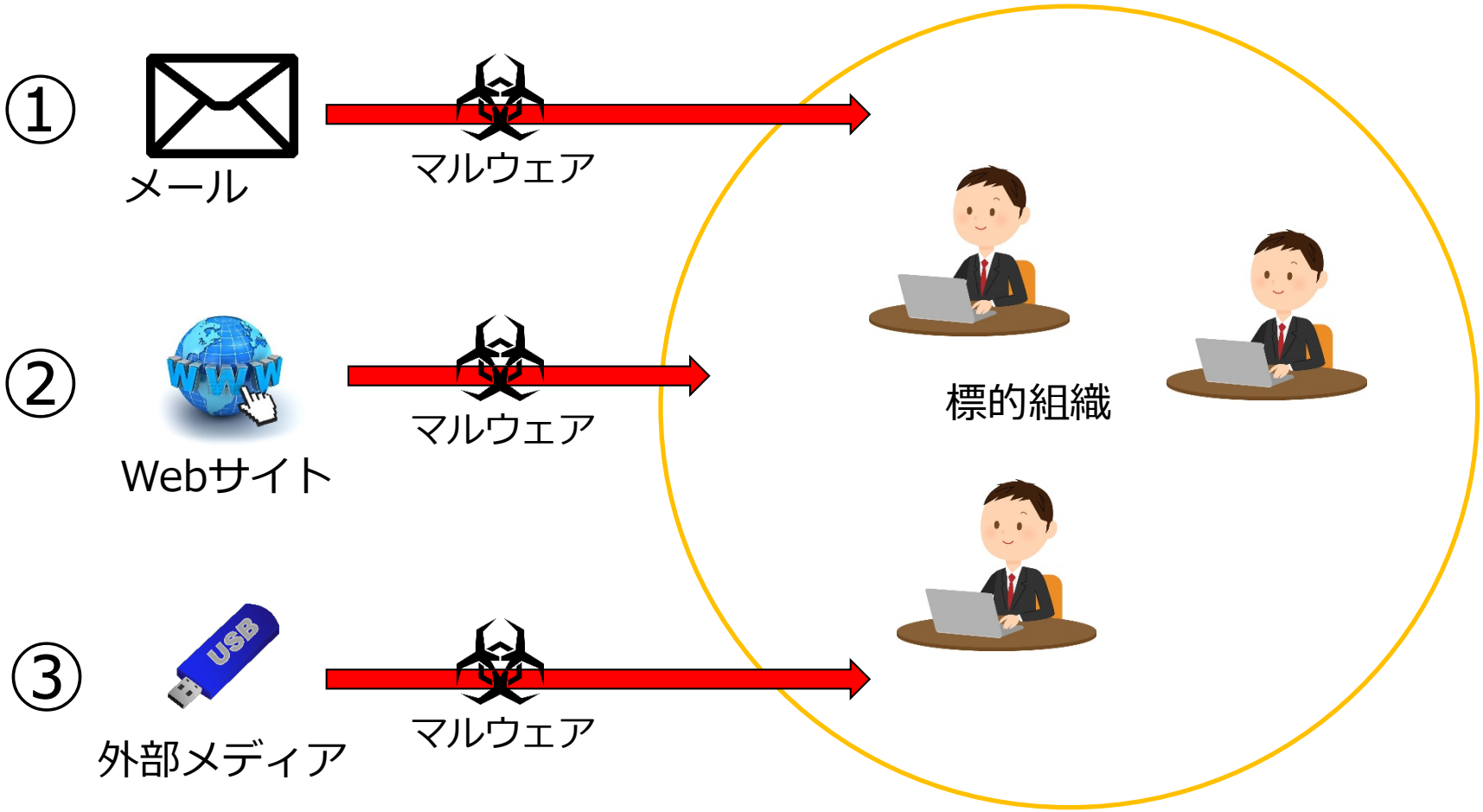
AppGuard®は、未知の脅威が不正な行為を実行する前にその行為を阻止し、そのうえで「既知の脅威」として認定します。これにより、従来型のセキュリティ製品に脅威を識別させ、駆除させることができます。従来型のセキュリティ製品と組み合わせることで、より効果的なセキュリティ対策が可能です。



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。

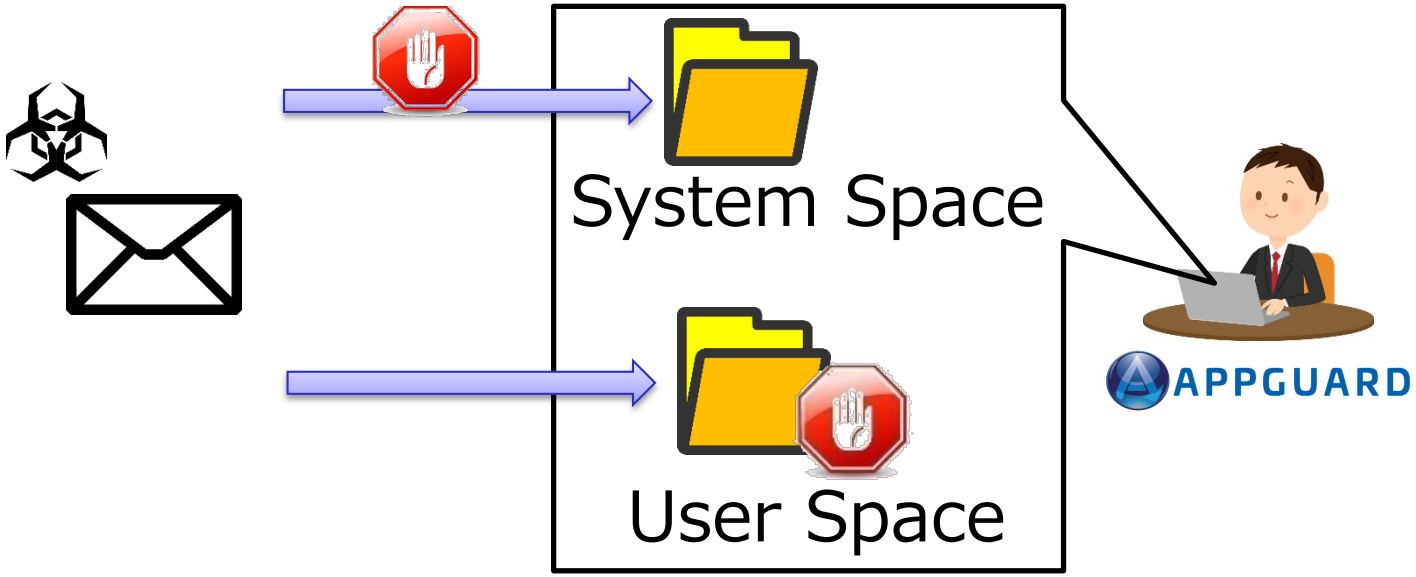


HITACHI
Inspire the Next

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)

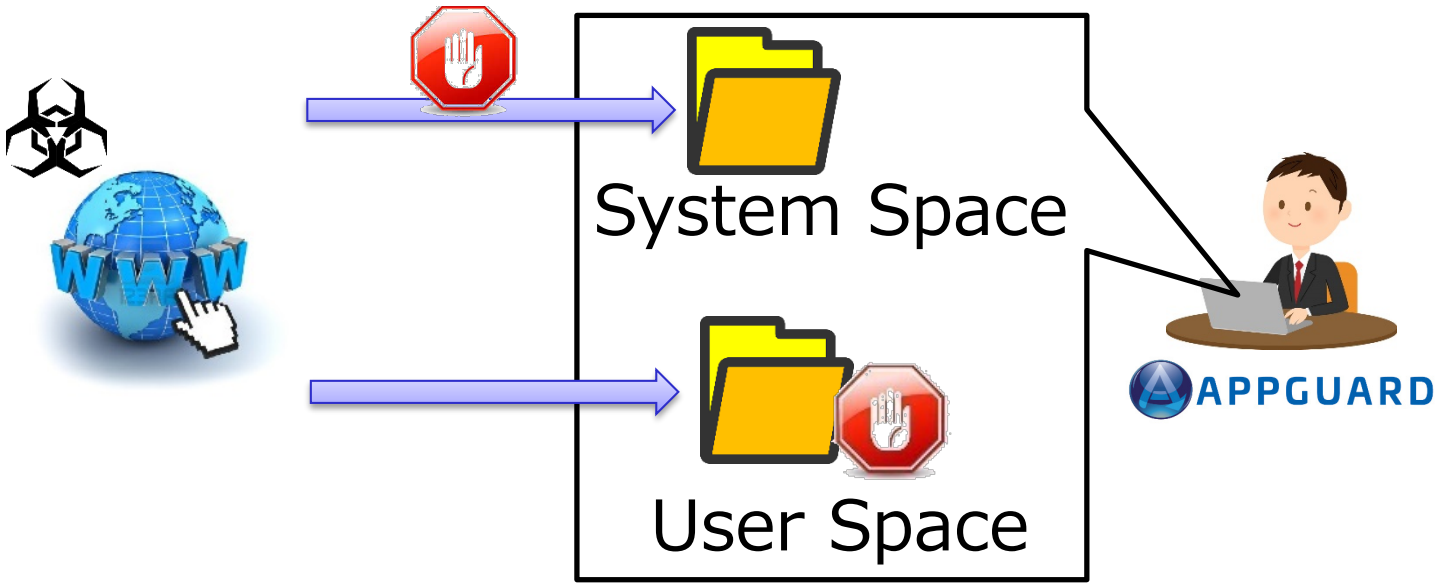
※2.User Space
AppGuard®が定義する、ユーザーがファイル操作する機会の多いPC領域のこと
(例.デスクトップ、マウントされた外部メディアなど)

HITACHI
Inspire the Next

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。

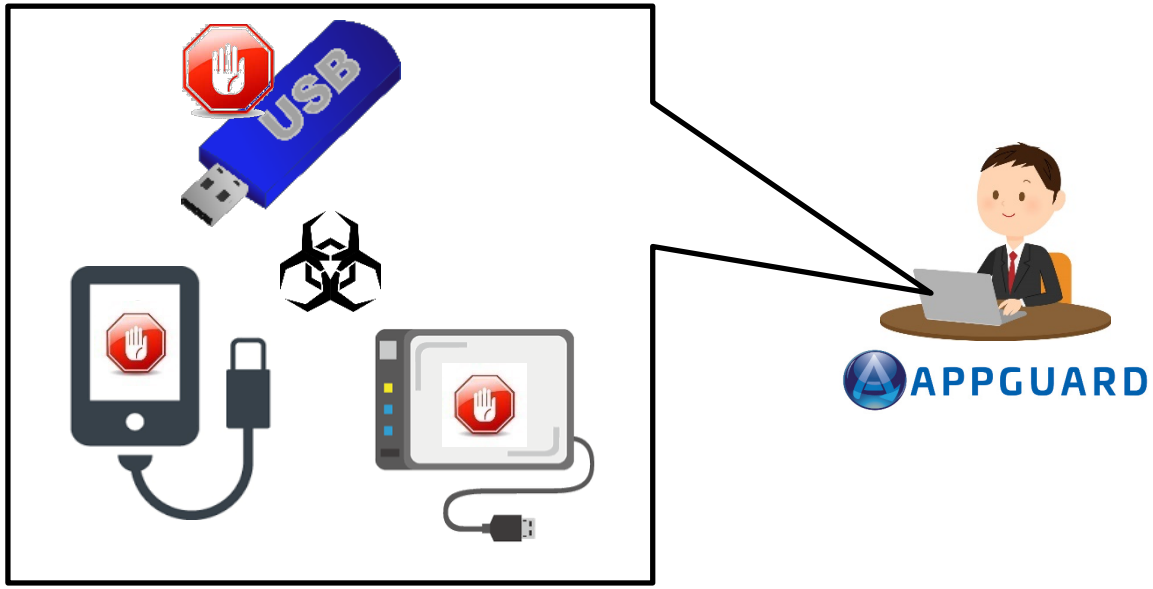
User Spaceへの保存は可能ですが、万一マルウェアが侵入した場合でも、マルウェアを起動させません。



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
WindowsPC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WindowsPC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サーバーを対象に
未知のマルウェアの実行を防止します。**

HITACHI
Inspire the Next

AppGuard®の構成

管理サーバー、ポリシー配布・ログ収集サーバーは
オンプレミスまたは、クラウドのサービスとして提供されます。

**AppGuard®
管理サーバー**

ポリシー配布

ログ収集

Windows
P C

Windows
Embedded

APPGUARD Enterprise

Windows
サーバー

APPGUARD SERVER

グループ毎にポリシー設定を行い、
各端末にエージェントをインストールします。

製造元の管理サーバーにて
ライセンスが管理されます。

**製造元
管理サーバー**

Windows
P C

APPGUARD Solo

スタンドアロン型で、ポリシー設定や
ログの参照などは、全てインストール
された端末上で行います。

3 – 6. AppGuard®の動作環境

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	Windows Server 2012R2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	4GB以上
			ディスク容量	利用環境による
AppGuard® Enterprise エージェント	○	ー	OS	WindowsXP SP3以降（2023年8月まで対応） Windows 7,Windows8および8.1,Windows10 Windows Embededd Standard 7,Windows 10 IoT Enterprise
			CPU	Intel 1.8GHz以上
			メモリー	1GB以上
			ディスク容量	50MBの空き容量

3 – 6. AppGuard®の動作環境

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	Windows 7（KB3035131,KB3033929適用） Windows8 および8.1,Windows10
			CPU	Intel 1.8GHz
			メモリー	1GB
			ディスク容量	50MBの空き容量

3 – 6. AppGuard®の動作環境

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	Windows Server 2012R2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	4GB以上
			ディスク容量	利用環境による
AppGuard® SERVER エージェント	○	ー	OS	Windows Server 2008 R2 SP1（KB3033929適用） 2012 R2,2016
			CPU	Intel 2GHz以上
			メモリー	2GB以上
			ディスク容量	40MBの空き容量

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
Weponized 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

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

電話でのお問い合わせ

0120-954-536

受付時間 10:00～17:30 月曜日～金曜日（祝日、当社休業日を除く）

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。
- 本資料に記載の会社名、製品名などは、それぞれの会社の商標または登録商標です。

■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、2019年6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

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）及び
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。