内閣サイバーセキュリティセンター
セキュリティガイドライン準拠製品

APPGUARD

株式会社ITガード

Ver1.2

会社概要

AppGuard ® 正規販売パートナー

株式会社 ITガード　（英名：IT Guard Corporation)
2015年設立　資本金（資本準備金含む）　4,100万

代表取締役　　前田 悟
執行役員　　吉川 剛史 (プロダクト技術マネージャー)

社員数：10名（役員、嘱託含む）
取引銀行：みずほ銀行

東京都千代田区霞が関３丁目２番５号
霞が関ビルディング13階

03-6550-8744
https://www.itgc.co.jp

ITガードが選ばれる３つの理由!!

１．圧倒的No1の導入実績

- AppGuard日本上陸時から販売開始
- 導入ライセンス＆導入社数 ともにダントツNo.1
- ㈱HIS様はじめ、様々な業種への豊富な導入実績

２．プロ集団の技術力

- 開発メーカー出身の技術者をはじめ、AppGuardを熟知したチームがフルサポート
- AppGuardに関することはもちろん、セキュリティに関するご要望にも柔軟に対応

３．迅速かつ正確な対応力

- 導入前のご案内から導入後のフォローまで専属チームが担当
- 顧客目線で正確に対応
- 独自の導入マニュアルやサポートツールを駆使して対応

さらに・・・

ITガードだけの専用サイバー保険付！

大規模なDDos攻撃、ゼロディ攻撃を起因したサイバー攻撃被害を
補償する当社専用のサイバー保険がAppGuardに自動付帯

セキュリティ全般の安全と安心をITガードはご提供致します。

ITガード専用サイバー保険

エンドポイント製品として業界初のサイバー保険を自動付帯　【※当社調べ】

補償内容

導入企業様に対して1ライセンスあたり

- **賠償責任**
- **事故対応特別費用**

合わせて500万円

※国内のみ担保
※使用人法令違反不担保
※支払責任限定特約（お支払いの対象となる損害参照）
※1証券限度額は5億円

補償額の例）

10ライセンス
保険金額：500万×10＝**5,000万円**

50ライセンス
保険金額：500万×50＝**2.5億円**

101ライセンス以上
保険金額：**支払い上限額5億円**

	概要
賠償責任に関する補償	AppGuard製品を購入した事業者に提起された損害賠償請求について、事業者が負担する損害賠償金等を補償します **損害賠償金**　**訴訟費用**　**弁護士報酬**
事故時または事故後の対策等に必要な費用の補償	損害賠償請求が発生するおそれがある場合に、その事故に対応するため、AppGuard製品を購入した事業者が支出した情報漏えい対応費用や再発防止実施費用等を補償します **原因調査費用**　**データ復旧費用**　**情報機器等修理費用** **ウェブサイト復旧費用**　**ネットワーク遮断対応委託費用**

お支払いの対象となる損害

10Gbps以上のDDos攻撃（注１）またはゼロデイ攻撃（注２、注５）を受けたことにより生じた、①または②の事由
①　ネットワークの所有、使用もしくは管理または情報メディアの提供にあたり生じた偶然な事由
②　情報漏えい、またはそのおそれ

（注１）DDos攻撃・・・ネットワークがサービスを提供できない状況にすること等を目的とし、複数のコンピューターに侵入し、侵入したコンピューターから一斉に、ネットワークに対して過剰な負担をかける意図的な行為をいいます。
（注２）ゼロデイ攻撃・・・情報の漏えい等を目的とし、セキュリティホール（注3）が発見されてから、修正プログラム（注4）が提供されるまでにネットワークに対して行う意図的な行為をいいます。
（注３）セキュリティホール・・・ソフトウェアの設計ミス等によって生じた、システムのセキュリティ上の弱点をいいます。
（注４）修正プログラム・・・ソフトウェアの修正を行うためのプログラムをいいます。
（注５）ゼロディ攻撃とは、未知のマルウェア等の未知の攻撃を含みます
※詳細な補償内容等不明な点は取扱代理店まで問い合わせください。

なぜ、いま AppGuard が注目されるのか？

最近のサイバー攻撃の動向

攻撃側

VS

企業側

企業側が圧倒的に不利

- １回でも突破できればOK
- 闇マーケットでマルウェアが簡単に入手可能
- セキュリティソフト回避ツールの普及
- 攻撃目的の多様化（国家・ビジネス・主張）

- 100%守られなければならない
- セキュリティ投資に消極的な経営側
- ICT環境の多様化

今、そこにある脅威

ゼロディ攻撃

OS・アプリの脆弱性を利用したマルウェアの実行

スピアフィッシング・標的型攻撃・ランサムウェア

Webやメールを媒介したドライブバイダウンロードによりマルウェアを実行

Web媒介攻撃・水飲み場型攻撃・悪意のある広告

Webを媒介したドライブバイダウンロードによりマルウェアを実行

ファイルレスマルウェア

レジストリやメモリを利用したスクリプト実行によるマルウェア攻撃

デジタル署名されたマルウェア

証明書を偽装しマルウェアを実行

武器化されたドキュメント

ドキュメント内に埋め込まれたマルウェアを実行

企業を狙うサイバー攻撃の実態

巧妙に仕掛けられる標的型攻撃

3%

大量に仕掛けられる
バラマキ型攻撃

97%

従来のアンチウィルス製品で
防御可能

出典：警視庁　平成29年中におけるサイバー空間をめぐる脅威の情勢等について

企業の守り方の変化～多層防御からの転換～

感染前提の対策にシフト → Endpoint Detection & Response

感染の兆候を検知し、いち早く対応する

本当に検知・対応できますか？

? 24H365Hの体制

? 何万件のログを分析

? 専門スキル人材

導入したけど、使いこなせていない・・・　分析できない・・・
何をしてよいかわからない・・・
運用がまわらない・・・

政府機関のセキュリティ対策のための統一基準（NISC）準拠製品

【基本対策事項】
< 6.2.2(1)(a)関連>

6.2.2(1)-1 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の導入にあたり、**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**フトウェアを導入すること。

（解説）
基本対策事項 6.2.2(1)-1「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」について
<抜粋>
ソフトウェアの脆弱性への適切な対策に加えて、シグネチャにより検知する方式以外の手法を用いる製品やサービスを導入することの重要性も高まっている。例えば、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書き込みを監視し**、不正プログラムの可能性がある処理を検知した場合には、**不正プログラムの実行を防止するとともに、これを隔離する**方式があり、攻撃にスクリプト等を使用するファイルレスマルウェアの対策としても効果が期待できる。

”未知のプログラムへの対策も可能 ”であることを明言

開発メーカー紹介

Blue Planet-works
Safety for the Connected World

米国政府機関で長年採用された革新的サイバーセキュリティ技術
“AppGuard”を2017年買収

2017年設立　代表取締役 中多 広志

■顧問
黒川 清（政策研究大学院大学名誉教授）
村井 純（慶應義塾大学　大学院　政策・メディア研究科委員長／環境情報学部　教授）
出井 伸之（クオンタムリープ株式会社 代表取締役）

■拠点
Global HQ: Tokyo
Americas Sales : New York
R&D : Virginia

2017年（平成29年）4月18日（火曜日）

サイバー防衛企業へ出資

電通・ANAなど8社

米の最新技術を優先利用

ANAホールディングス（HD）や電通など国内企業8社は18日にIT（情報技術）企業のブループラネットワークス（東京・渋谷、旧キープソリー）に合計55億円を出資する。出資することで同社が持つサイバー攻撃対策技術を優先的に低コストで使えるようにする。企業を狙うサイバー攻撃は巧妙さや悪質さが増しており、国内の産業界でも本格的な対策が急務となっている。

ブループラネットワークスが実施した第三者割当増資に応じた。同社は2020年の東京五輪を見据え、自社でサイバー攻撃対策ソフトを活用する情報セキュリティー企業のためにブループラネットワークスに出資した。16年のロンドン五輪で英国の米ブルーリッジネットワークス（バージニア州）企業に対するサイバー攻撃が頻発したように、東京五輪でも攻撃の増加が懸念されている。

ANAHDや電通は2020年の東京五輪のスポンサーとして、情報を守り、電通は取引企業の情報を保護する

ウイルスの侵入を前提に被害を防ぐ
サイバー攻撃者
ウイルス送信
アプリケーション
ウイルスは検知せず
指令
不正な指令をブロック
OS
企業の情報システム

8社はセキュリティー対策技術に55億円を出資する
・ANAホールディングス
・電通
・電通国際情報サービス
・損保ジャパン日本興亜
・第一生命保険
・PCIホールディングス
・大興電子通信　など
米ブルーリッジネットワークス
新株発行
46億7000万円
22億円
セキュリティー事業
第三者割当増資 計55億円
ブループラネットワークス

出資企業
ANAホールディングス株式会社 / 株式会社JTB / 株式会社電通
株式会社電通国際情報サービス / 大興電子通信株式会社
PCIホールディングス株式会社 / 第一生命保険株式会社
損保ジャパン日本興亜株式会社 株式会社ITガード他

最新ニュース

単行本「決定版 サイバーセキュリティ：新たな脅威と防衛策」

2018年11月16日 東洋経済新報社 から発売

Amazonから引用
https://www.amazon.co.jp/dp/4492762450

内容紹介
「サイバー攻撃」など自分とは関係ないと思っているのなら、それは大間違いである。
スマートフォンやパソコンがこれだけ普及している今、サイバー攻撃は非常に身近な脅威となっている。
国家規模のサイバー戦争、大企業の情報漏洩やビジネスメール詐欺。国家や企業にとっては、存続が左右されることにもなりかねないサイバー攻撃であるが、こと個人にとっても見過ごすことができない問題となっている。
IoT時代を迎えて、すべてのものがネットにつながる状態になると、あらゆるもの、あらゆる場所、あらゆるタイミングでサイバー攻撃にさらされることになる。
それらを防ぐために、サイバーセキュリティ環境は今、どんな状況に置かれているのか。今、どんなセキュリティ対策がとられ、今後どうなっていくのか。

現在の複雑なネット環境、サイバー環境の中で、サイバーセキュリティはどうなっているのか。
そして、未来のサイバーセキュリティはどうなっていくのか。

コンピューターが苦手な人にもわかるサイバーセキュリティ入門の決定版。

メディア実績

■テレビ朝日系 報道ステーション
2017年9月26日放送

■フジテレビ系 THE NEWS α
2018年3月19日放送

■テレビ東京系 Newsモーニングサテライト
2018年2月28日放送

■テレビ東京系 日経プラス10
2017年11月3日放送

■ Mylife News Network 様
2018年7月26日

http://www.mylifenews.net/other/2018/07/itgappguard.html

■ ZDNet Japan 様
2018年5月7日

https://japan.zdnet.com/article/35118420/

■ ASCII.JP×TECH 様
2017年11月27日

http://ascii.jp/elem/000/001/591/1591834/

■リスク対策.com 様
2017年10月6日

http://www.risktaisaku.com/articles/-/3861

AppGuard導入実績

2019年1月21日現在

国内実績

販売開始から１年超で10万ユーザー以上

ANA　dentsu　JTB

いっしょに、明日のこと。 Share the Future SMBC日興証券　もっと世界を楽しもう H.I.S. Love, Peace, TRAVEL　吉本興業

BITPOINT　ECOHAI　株式会社 No.1

某大手法律事務所　某会計事務所　某地方都市教育委員会

海外実績

MAIDEN LANE MEDICAL　Columbia Bank　PeoplesBank A passion for what is possible℠　Community West Bank　TUCSON FEDERAL CREDIT UNION

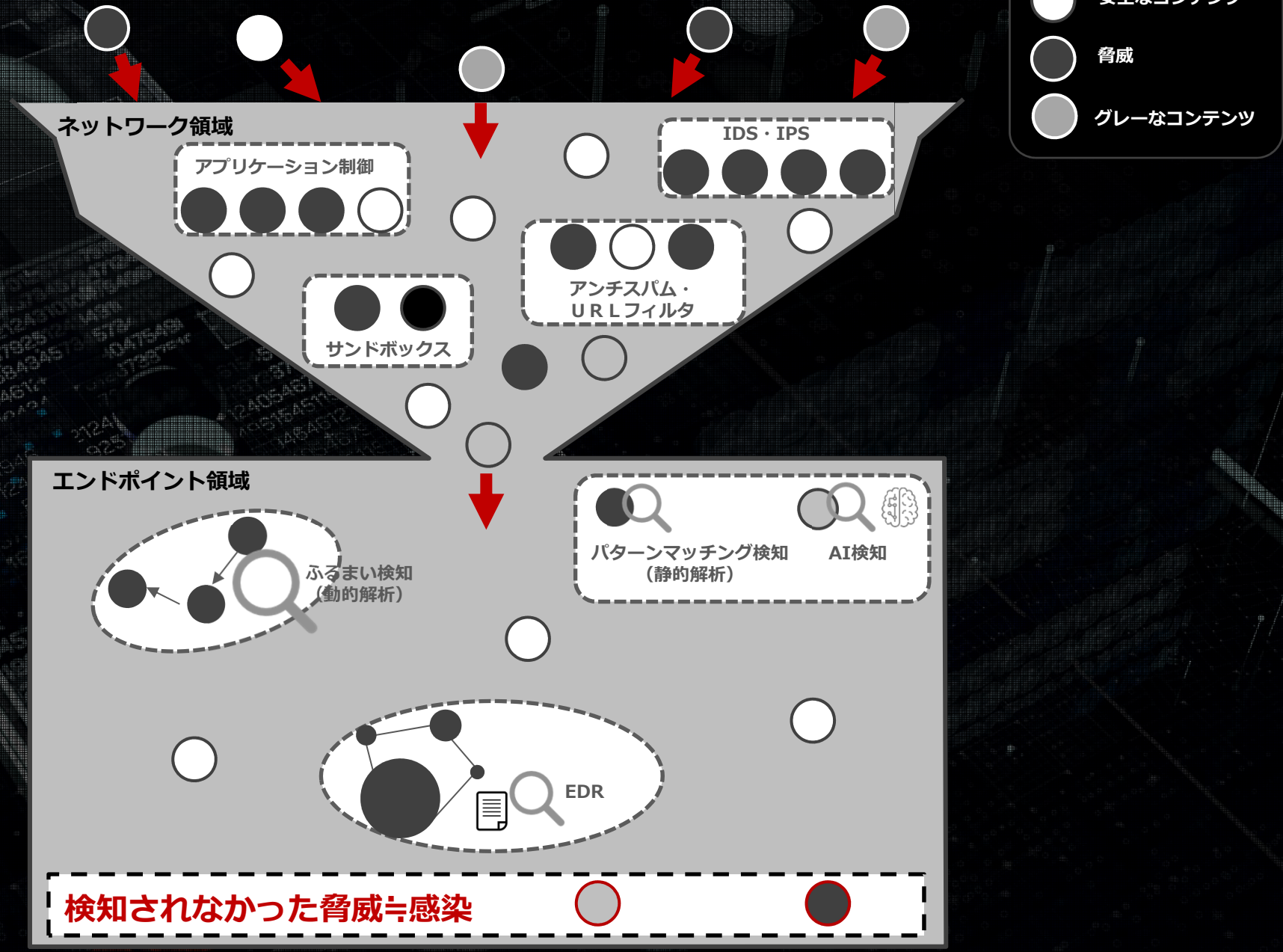
THE PORT AUTHORITY OF NY & NJ　AOL. TECH FORTRESS POWERED BY APPGUARD　Dutch Point CREDIT UNION　YAHOO!

その他政府機関

AppGuard Protection ～主な防御機能～

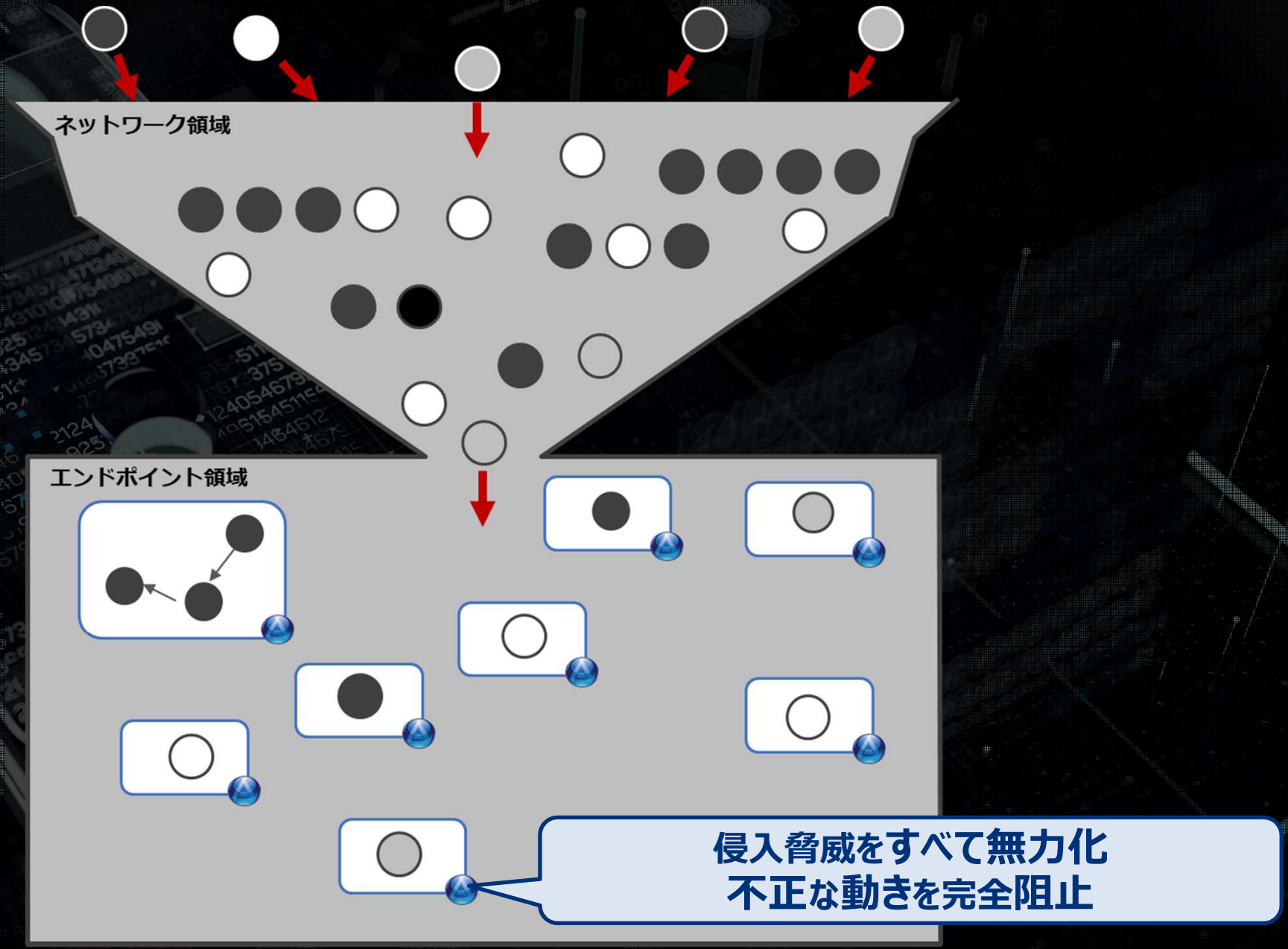
多層防御の限界

いたちごっこの世界・すり抜け発生



多層防御の課題を解決

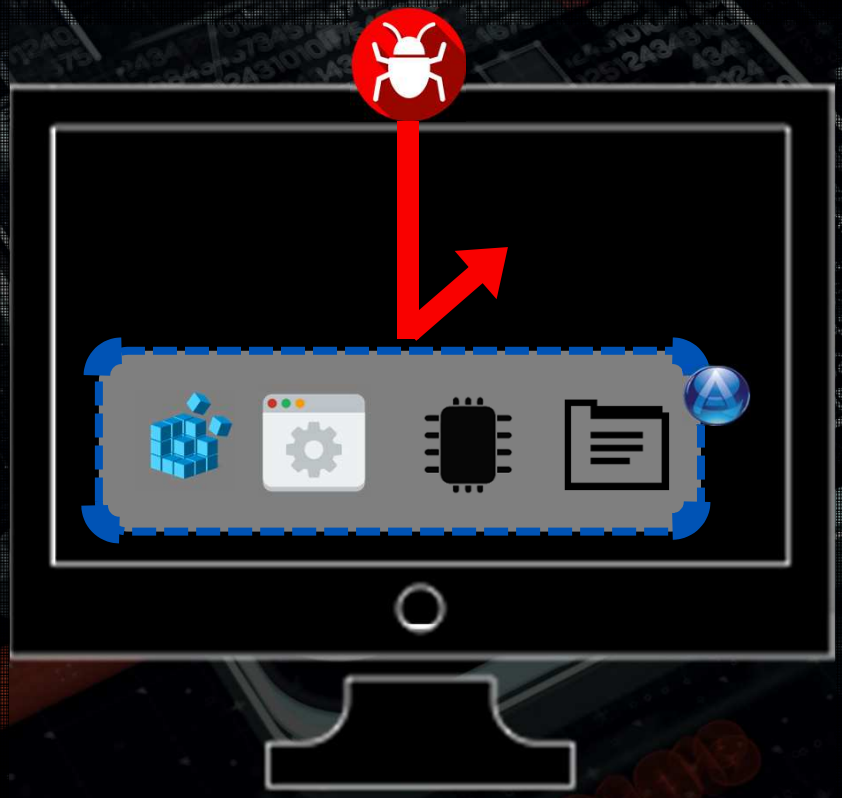
端末の脅威をAppGuardが完全に封じ込める



既存ソリューションとの違い

APPGUARD

OSを破壊させない
（感染させない）



システムに害を与えない

既存製品

過去の脅威情報（型・振舞・挙動）を
もとに検知・駆除

探し出す・予測・検知率・誤検知・過検知

比較表

	APPGUARD	アンチウイルス	振る舞い検知	AI機械学習	EDR	ホワイトリスト
目的	不正プログラムを動作させない	不正プログラムを見つけ出して、駆除する				
手法	プロセスコントロール	定義ファイルによる静的解析	動的解析	機械学習による静的解析	動きを記録・解析	決めたものだけ起動
未知・ランサムウェア・最新の脅威からの防御	○	×	△	△	△	×
ファイルレスマルウェアからの防御	○	×	△	△	△	×
メモリ攻撃からの防御	○	×	△	△	△	×
定期的なディスクスキャンの実施	○ 不要	× 必要	× 必要	△	× 必要	○ 不要
CPU負荷（軽量・軽快）	○ 軽量	× 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）	○ 不要	× 必要	× 必要	△ 年に数回	× 必要	○ 不要
マルウェアの駆除	× しない	△ 既知のみ	△ 既知のみ	△ 既知のみ	△ 既知のみ	× しない
常時ネットワーク接続	○ 不要	× 必要	× 必要	△	× 必要	○ 不要
運用コストの削減	○ 可能	× 不可能	× 不可能	× 不可能	× 不可能	× 不可能

防御スコープ

※ネットワークの脆弱性を利用した攻撃は、AppGuardで防御することはできません。侵入後にドロッパー等を利用して実行型マルウェアを介するタイプの攻撃は防御可能です。

全く新しい概念でシステムの安全性を確保

すべてのプロセスを監視、安全性を脅かすプロセスを隔離
Windowsの設計思想にそぐわない動きを止める

STAGE①
プロセス起動前制御

- カーネルモードで動作
- CPU使用率　1%以下

STAGE②
プロセス起動後制御

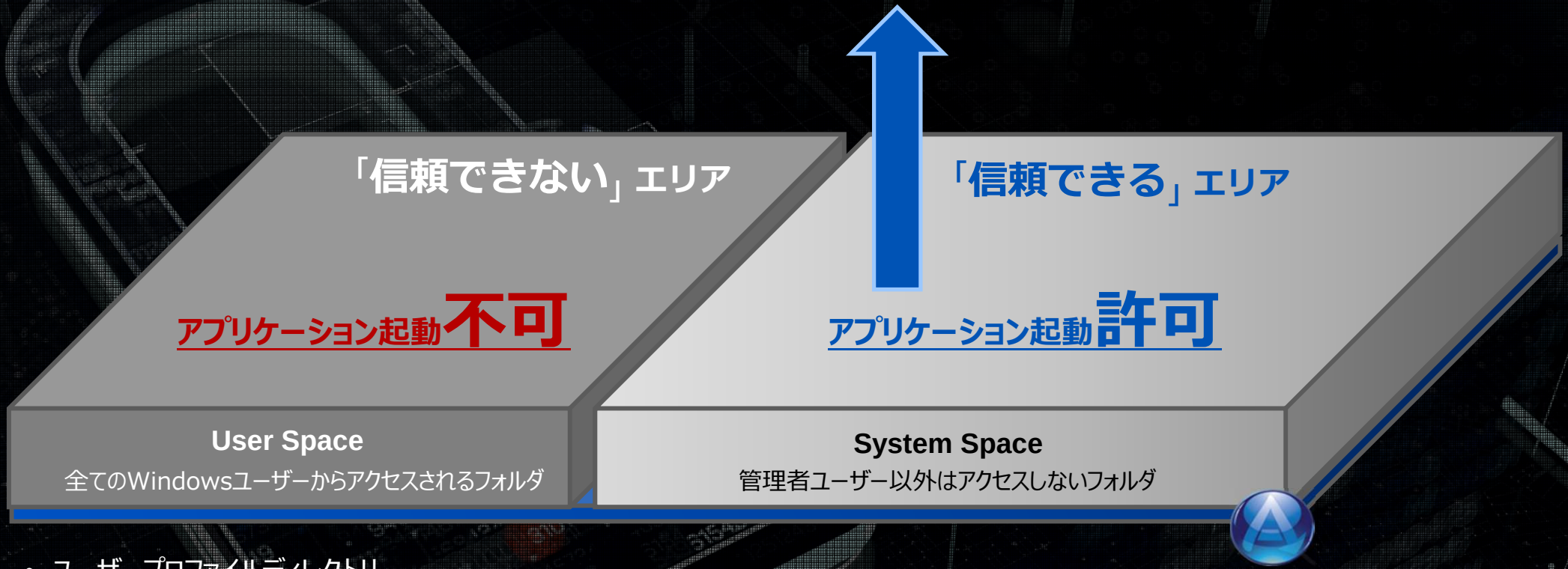
- インストール容量　僅か10MB
- オフライン環境で動作可能

XP以降のWindows OSに対応

STAGE①　起動前の制御

信頼できるアプリのみ起動

デジタル署名やファイルの場所に基づき起動



- ユーザープロファイルディレクトリ
- My Documents, Desktop etc.
- リムーバブルストレージ
- ネットワークドライブ

等

- C:¥Program Files
- C:¥Windows
- C:¥

等

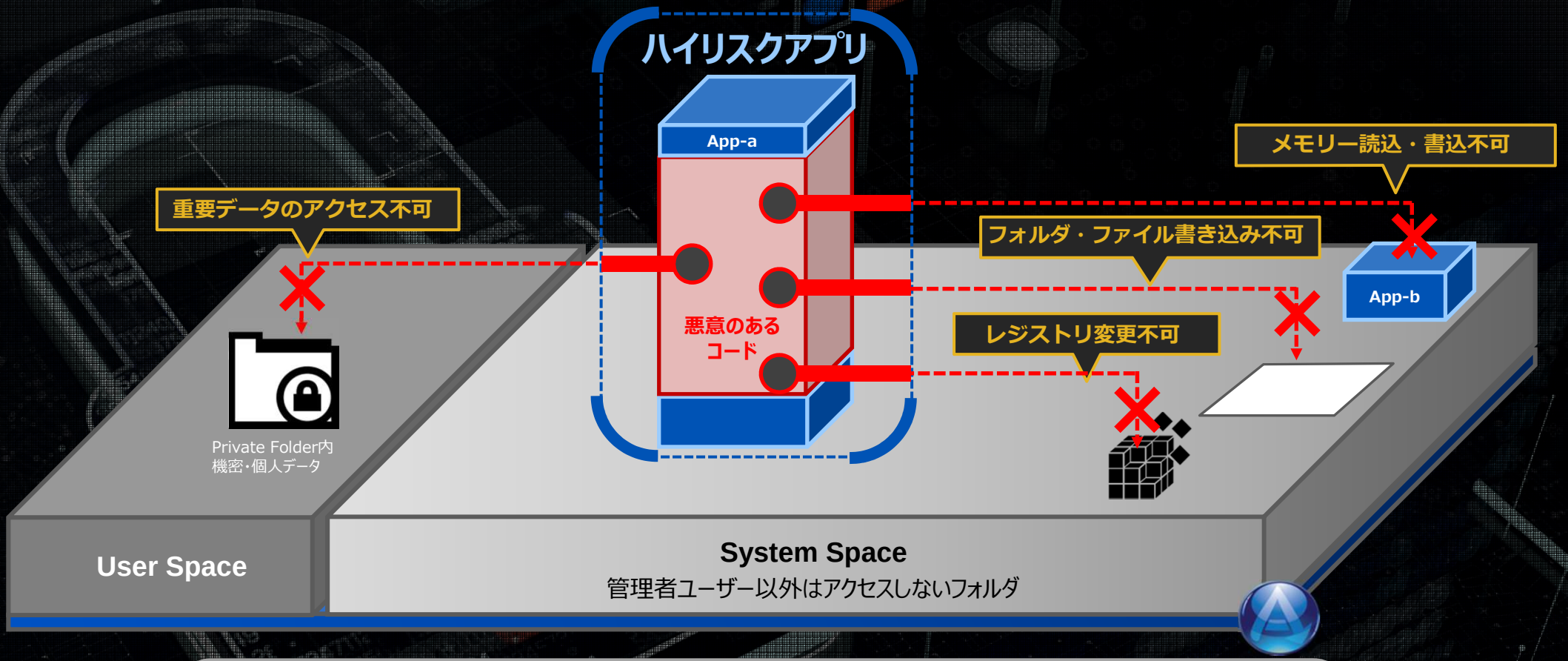
Low-level kernel interceptors
<no hooks, no non-standard API's>

ドライブバイ・ダウンロード攻撃などを阻止

どんなWebやメールを開いても感染しない

STAGE②　起動後の制御（isolation Technology）

プロセス隔離・監視（特許技術）



ハイリスクアプリ：マルウェアの攻撃に対して脆弱なアプリケーション

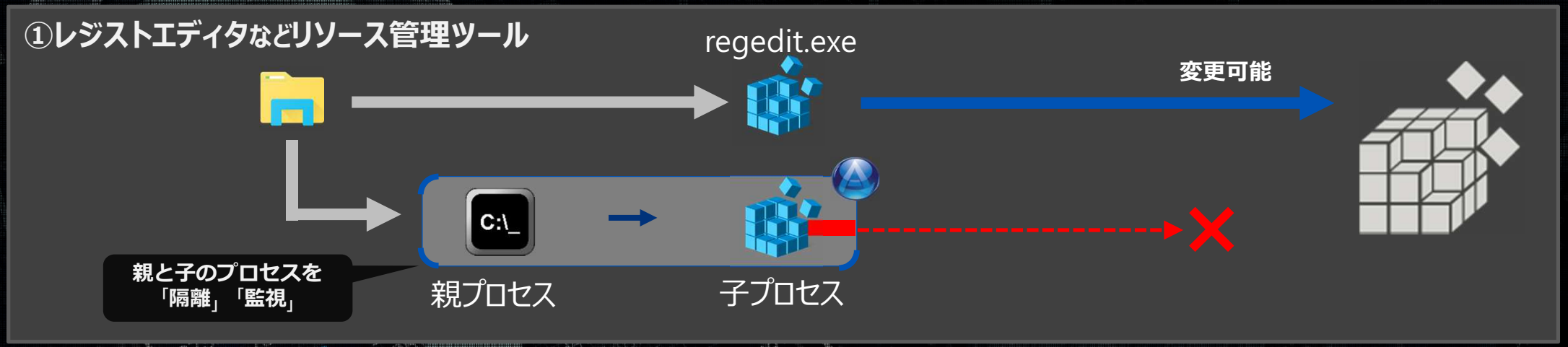
世の中で広く使用され、インターネット通信により不特定ソースからの情報*を扱う

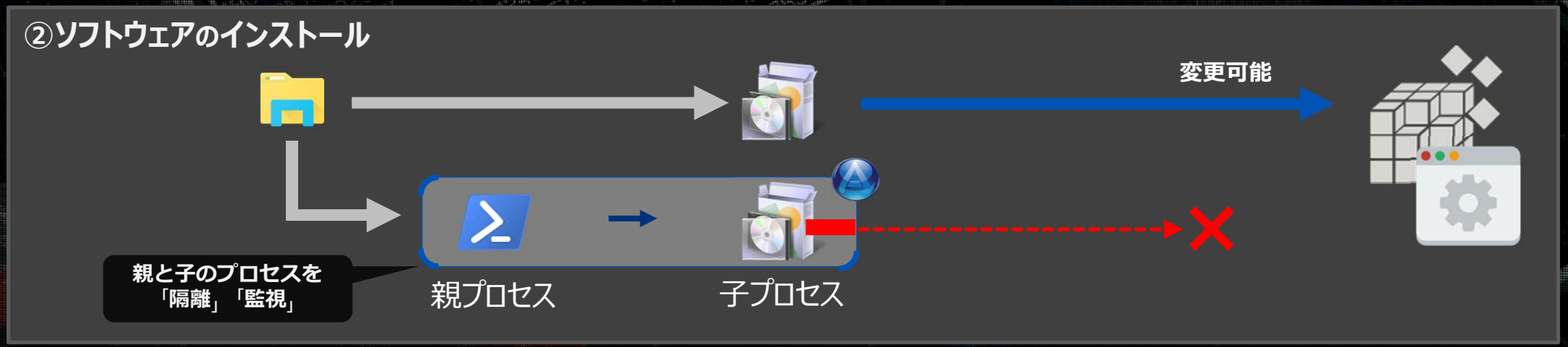
*メールの添付ファイル、インターネットからダウンロードしたドキュメントなど

ファイルレスマルウェア、エクスプロイト攻撃などを阻止

Inheritance 技術
プロセス隔離・監視対象の自動継承（特許技術）

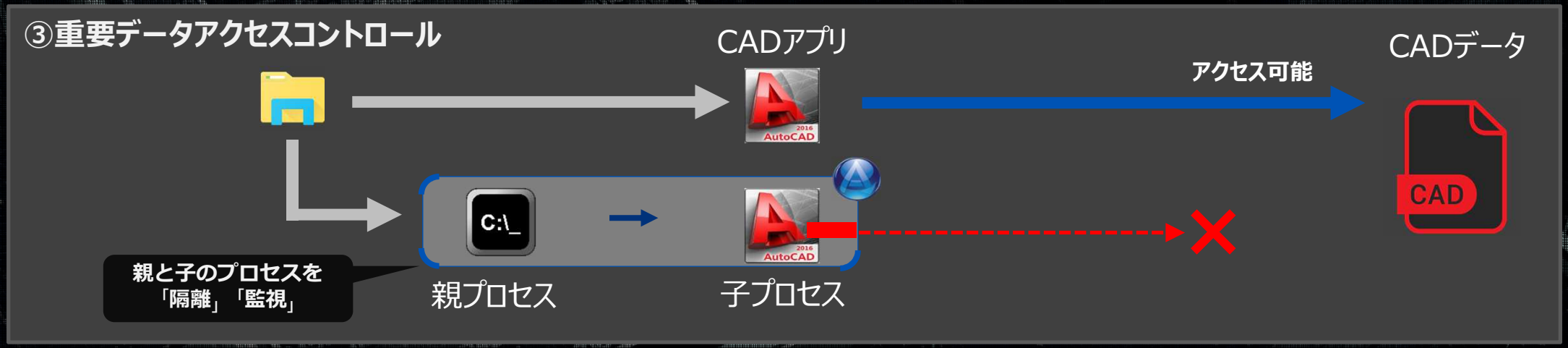
アプリ単体では無く動的環境下で不正か否かを判断





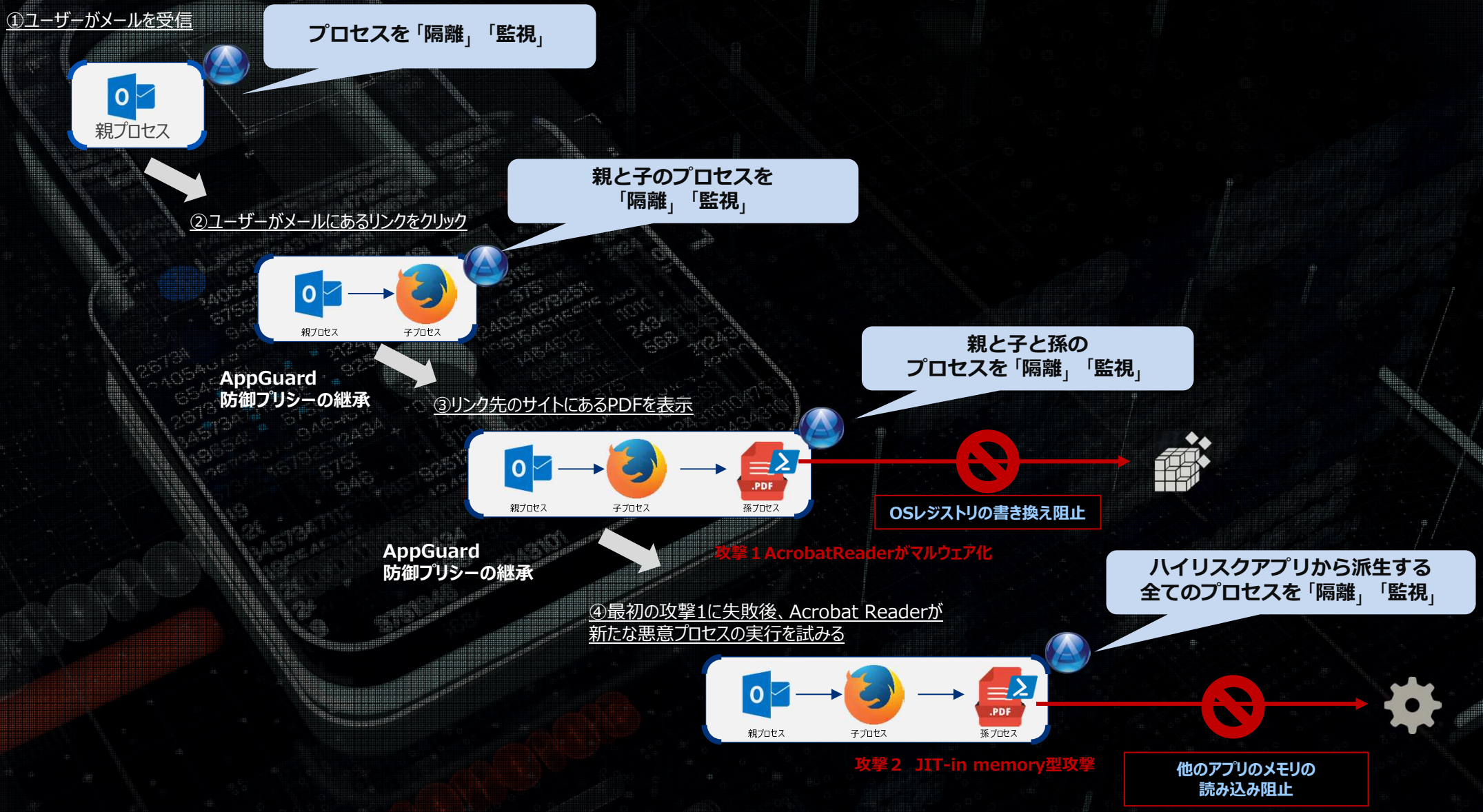
Inheritance 技術
プロセス隔離・監視対象の自動継承（特許技術）

アプリ単体では無く動的環境下で不正か否かを判断



「Inheritance」技術
プロセス隔離・監視対象の自動継承（特許技術）

アプリ単体では無くダイナミックな動的環境下で不正か否かを判断



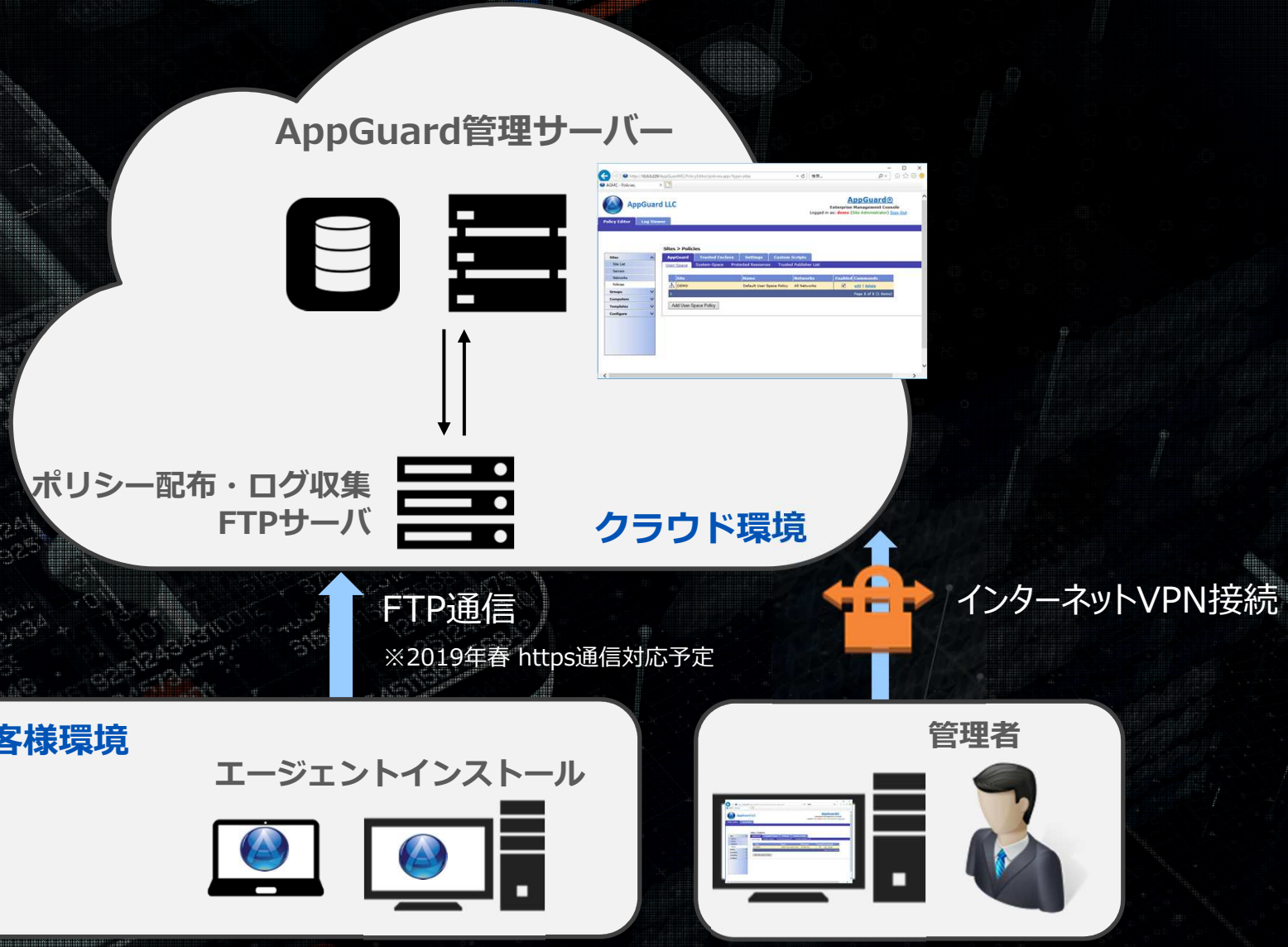
AppGuard Policy Concept

	STAGE① プロセス起動前制御 信頼できるプロセスのみ起動	STAGE② プロセス起動後制御 システムに害を与えるプロセスを停止
基本 Policy	ベストプラクティスなデフォルト保護ポリシー	
＋	＋	＋
追加 Policy	**起動を許可する信頼できるアプリ** デジタル署名付くアプリを信頼するか どのフォルダ内のアプリを信頼するか	**起動を禁止するアプリ** **リスクの高いアプリ** **保護リソースへアクセスさせるアプリ**

各企業毎に“信頼できるアプリは異なる“ため、導入前に”ポリシーチューニング”が重要

このプロセスを通じ、企業の特徴を尊重しつながら、リスクと利便性のバランスを確保

AppGuard Enterprise システム構成の特徴



＜ポリシーファイル・ログファイルの安全性＞
サーバー～エージェント間で完全に保護。各転送ファイル毎に異なる暗号鍵を利用し、すべての情報の解読を不可能に

- ログ＆ポリシー の暗号化としてAESを採用
- 暗号鍵として端末毎の固有IDとグループIDの組み合わせで署名
- 鍵の交換方式としてPFS*技術を適用(*Perfect Forward Secrecy)

システム要件

AppGuard エージェント

- Windows XP、Vista、Windows 7、Windows 8 および 8.1、Windows 10、Windows Server バージョン 2008 R2 および 2012 R2 をサポート
- デスクトップ PC、ノート PC、タブレット、VDI、ATM、POS デバイスで動作
- AppGuard Enterprise エージェントは、Citrix XenDesktop や Amazon WorkSpaces などの非永 続的な仮想デスクトップ インフラストラクチャ (NP-VDI) にも展開可能。NP-VDI 環境のサポートは ベータ版の機能。

AGMC サーバーのハードウェア要件

- プロセッサのタイプ：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
- プロセッサの速度：推奨：3 GHz 以上
- メモリ:推奨:4GB以上
- 合計容量が 800 GB 以上の複数のディスク ドライブ (この数値はシステムを使用して展開するAppGuard エージェントの数に応じて異なります)

AGMC サーバーのソフトウェア要件

- Windows Server 2012 R2 以上
- SQL Server 2012 Standard エディション、Service Pack 2 以上
- 大規模な展開の場合、SQL Server は専用のサーバーにインストールする必要があります。
- AGMC と SQL Server が同じサーバーにインストールされていない場合は、AGMC サーバー に SQL Server コマンド ライン クエリ ユーティリティをインストールする必要があります。
- IIS バージョン 8.5 以上
- .NET Framework 4.5

AppGuardが選ばれる理由

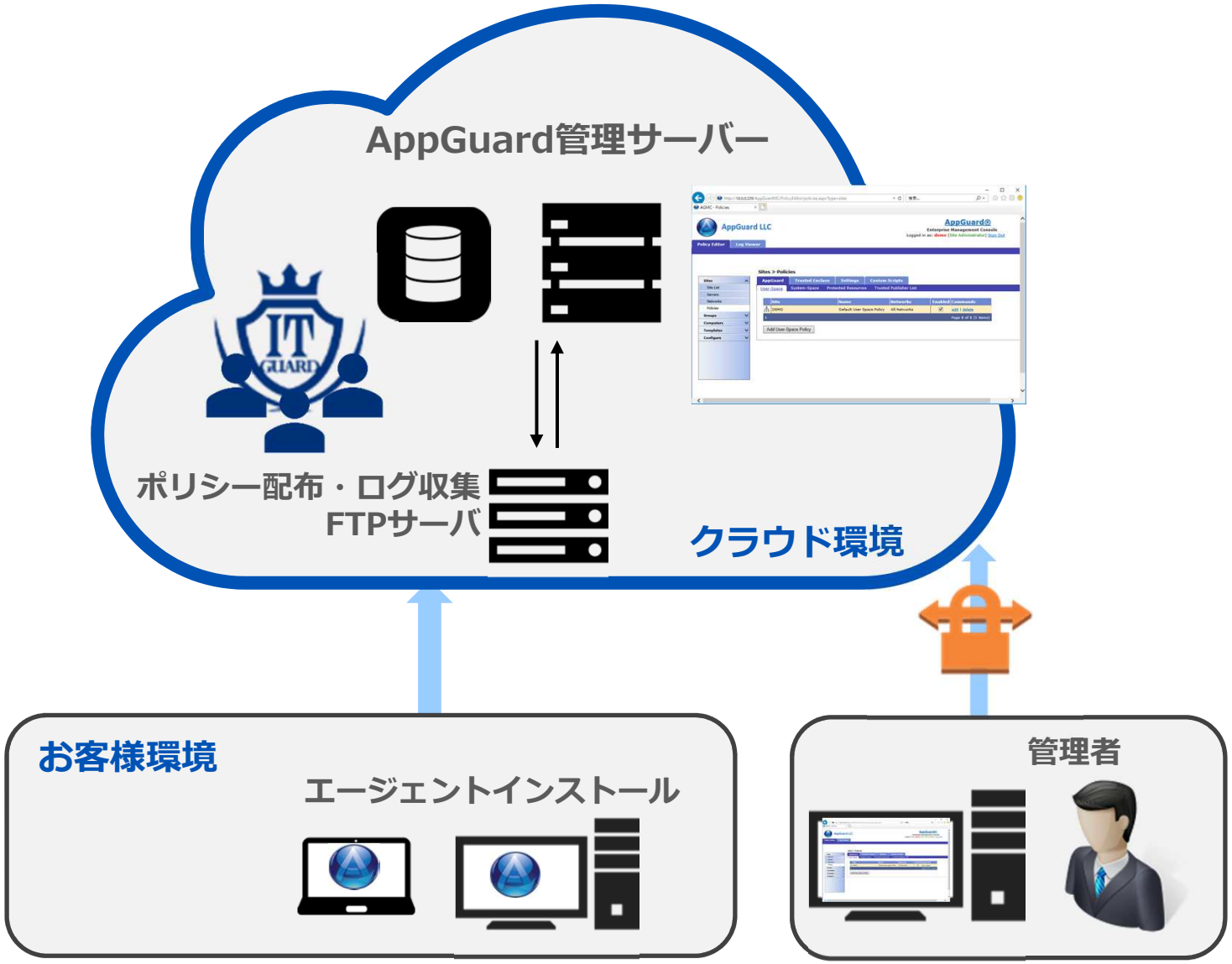
「常時ネットワーク接続不要」、「軽量・軽快」、「運用が簡単」 だから

1. 標的型攻撃への対策はこれ１つでOK
2. 圧倒的な防御力であらゆる攻撃を阻止する
3. 従業員のストレスを軽減できる（端末負荷なし、メール開封可）
4. インターネット通信速度が阻害されない
5. オフラインなど特殊な環境も幅広くカバーしている（常時ネットワーク接続不要）
6. サポート切れOSに対応している（Win7など延命策）
7. 出張先でのリスクを極小化できる
8. 働き方改革を推進できる（安全なリモートワーク環境を構築）
9. 専門スキル・専門家が不要である
10. セキュリティオペレーション工数を削減できる

提供サービス・製品

ITGクラウドセキュリティサービス

AppGuard Enterpriseをクラウドサービスとしてご提供



サービス料金

年間のサブスクリプションサービスとしてご提供

サービス内容

- AppGuard Enterprise Agentライセンス
- AppGuard Management Console（クラウド）
- 保守・メンテナンス
- ITガード専用サイバー保険自動付帯

基本利用料金

台数ボリューム	1～99	100～499	500～999	1,000～2,499	2,500～4,999	5,000～9,999	10,000～19,999	20,000～
ITGクラウドセキュリティサービス	¥14,000	¥12,000	¥11,000	¥9,800	¥8,700	¥8,000	¥7,500	¥6,800

※クライアントPC向け1台あたりの単価（年間）
※初期設定費用が別途発生いたします。
※クラウドサーバーはマルチテナント型の共有インスタンスでのご提供です。
専用インスタンスの場合は別途お見積りとなります。

オンプレミス向けプランもご用意可能です。

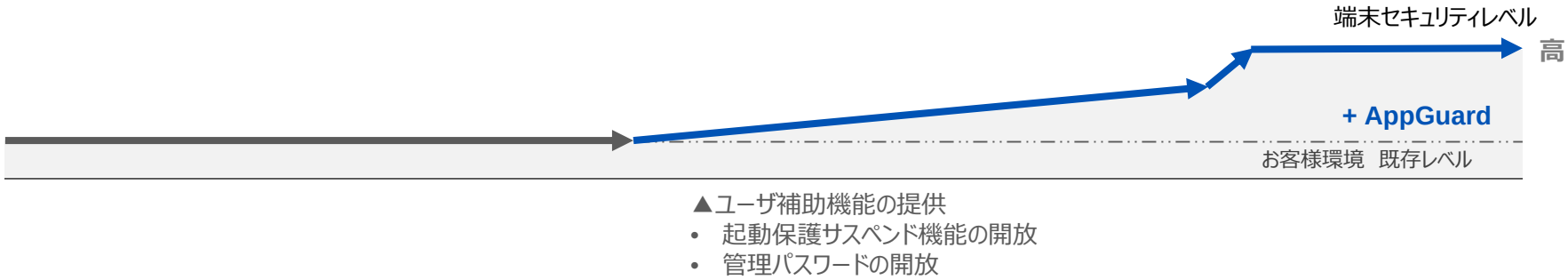
小規模企業向けにはスタンドアロン型AppGuard Soloもご提供可能

- AppGuard Solo Agentライセンス
- ITガード専用サイバー保険　　1台1年 9,800円（税抜）

AppGuard 導入までの流れ

導入までの流れ

お客様　ITガード



▲ユーザ補助機能の提供
- 起動保護サスペンド機能の開放
- 管理パスワードの開放

ご契約手続き → 環境アセスメント → ポリシー設定 → 試験導入（ポリシーチューニング期間） → 正式導入

2～3週間　1～2か月

■アセスメントシート記入
■端末情報収集
□モニタリングモード配布

■ポリシー確認

■エージェント配布

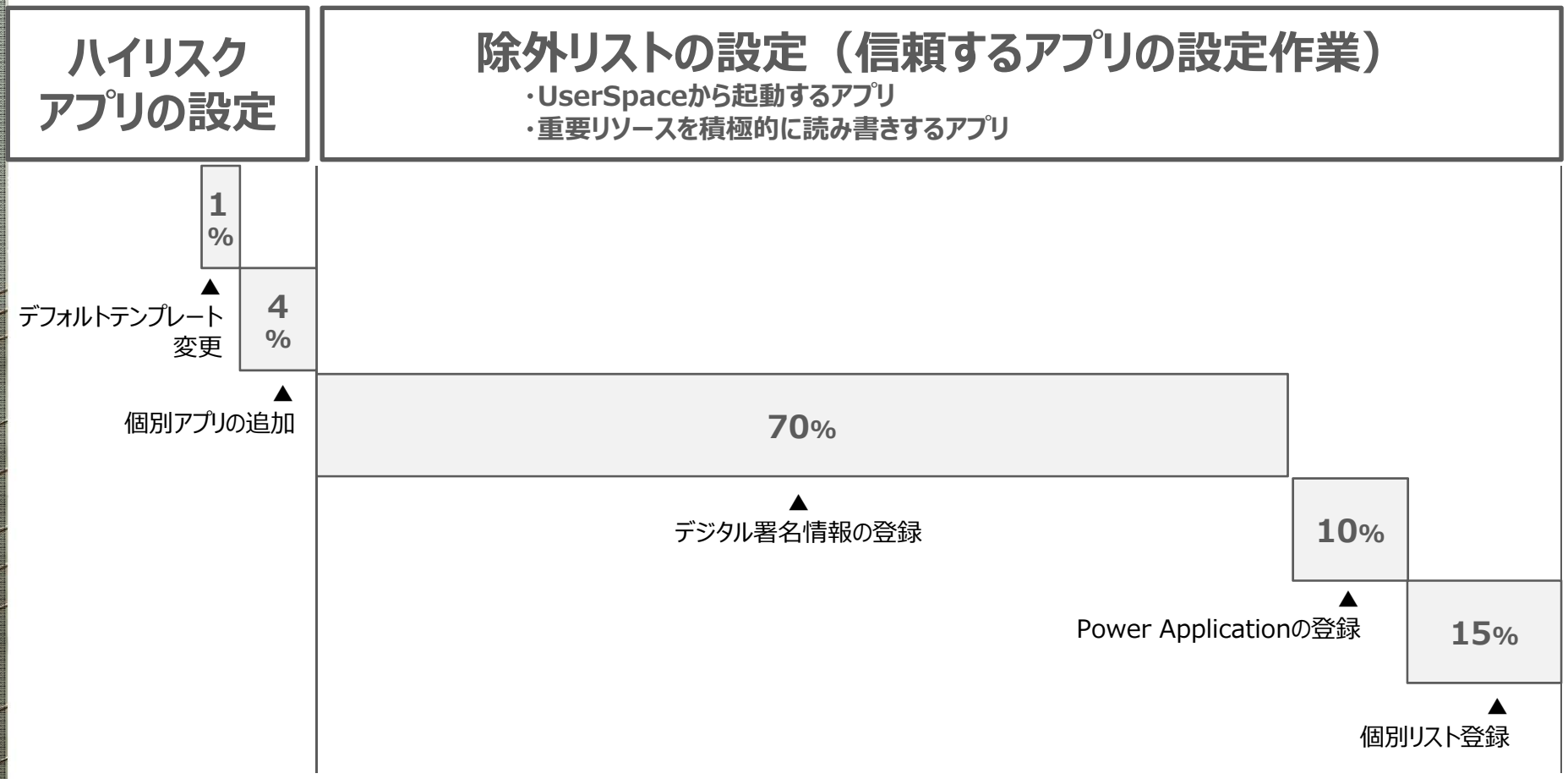
■アセスメントシート解析
■端末情報解析
□モニタリングモードによるログ解析

■ポリシーチューニング
ユーザ補助機能の使用頻度チェックし
より詳細な調査並びに運用ルールの策定

■ポリシー設定作業

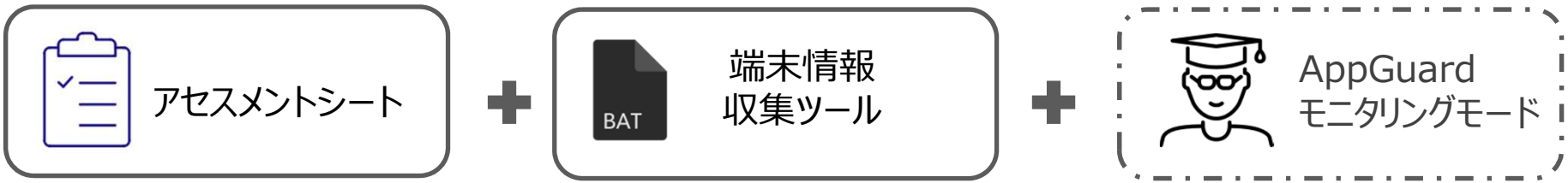
AppGuardポリシー設定作業（内訳）

企業毎に“信頼できるアプリは異なる“ため、企業の特徴を尊重しながら、
リスクと利便性のバランスを確保し、除外リストを設定



導入プロセスの肝

一番重要な作業は、**除外対象の特定と最小化**である。



①ポリシーへの反映

②運用設計・見直し

製品の検討・導入に向けた PoCプログラムのご案内

PoC（実証実験）の目的

AppGuardを導入する前にPoCプログラムを実施することで
製品の検討並びにその後の導入から運用までをスムーズに行うことができます。

＜目的＞

AppGuardの有効性・適応性の検証

- 外部脅威に対するAppGuardの防御力、使用環境・性能の把握
- 運用負荷の把握

＜実施内容＞

- AppGuard製品の理解
- 防御力の把握
- 既存環境における潜在的脅威の確認
- 社内アプリケーション・既存アプリケーションとの干渉具合の把握
- 本番展開時の課題の把握
- 端末への負荷、ネットワークへの負荷の把握
- 運用負荷の把握

PoCスケジュール（サンプル）

KICK OFF **１時間**	■ PoCの進め方ご説明 ■ スケジュールの日程決定 ■ アクションアイテムの確認
評価① **～ハンズオン** **トレーニング～** **２時間**	■ AppGuard機能理解（エージェント、管理画面） ■ 検証端末へのインストール ■ 調査Modeグループ作成 ■ 評価端末台数と対象ユーザーの検討（20台程度） ■ マルウェアテストの実施検討
２週間後	
評価② **～中間報告～** **1.5時間**	■ 製品Q&A ■ 調査Modeによるログ分析 ■ 潜在脅威分析 ■ チューニング内容の説明 ■ マルウェアテスト(任意)
２週間後	
評価③ **～最終報告～** **１時間**	■ 検証レポートのご提出並びにご説明 ■ お客様ご感想 ■ コスト・今後の流れ

お問い合わせ先

株式会社ITガード

03-6550-8744
sales@itgc.co.jp