Blue Planet-works
Safety for the Connected World

デジタル化の推進に資するセキュリティ対策

～OSプロテクトに基づくゼロトラスト・エンドポイントセキュリティ～

株式会社Blue Planet-works

セキュリティアドバイザー 鴫原祐輔

最新のサイバー攻撃を従来の防御方法では防御できない

Blue Planet-works
Safety for the Connected World

検体採取日：2021年04月09日（金）～2021年05月26日（木）
検体調査日：取得した日と同日@Virus Totalにて検証

	A社	B社	C社	D社	E社	F社	G社	H社
検体01:Lokibot#1 採取日:2021年4月9日（金）	検知できず	検知できず	検知	検知できず	検知	検知	検知できず	検知できず
検体02:NJRAT 採取日:2021年4月9日（金）	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
検体03:bazarbackdoor 採取日:2021年5月5日（木）	検知	検知できず	検知できず	検知できず	検知できず	検知	検知できず	検知できず
検体04:Sodinokibi 採取日:2021年4月9日（金）	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
検体05:Trickbot 採取日:2021年4月9日（金）	検知できず	検知できず	検知	検知できず	検知できず	検知	検知できず	検知
検体06:Lokibot#2 採取日:2021年5月6日（木）	検知	検知	検知できず	検知できず	検知できず	検知	検知	検知できず
検体07:Dridex 採取日:2021年5月26日（木）	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず
検体08:IcedID 採取日:2021年5月26日（木）	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知できず
検体09:AgentTesla 採取日:2021年5月26日（木）	検知できず	検知できず	検知できず	検知できず	検知できず	検知	検知	検知できず
検体10:Qakbot 採取日:2021年5月26日（木）	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず	検知できず

検体#01:81238e53beb93a1c836e567c8335242b658735757d23b6f0f4afac96e672fdbc
検体#02:c608289cb10e1ba4d6faeae2545f9147ec65a363207c7d643aaf057f9508f199
検体#03:21382e955d23c9c2ff9aa617070f33f898745d568b82338c9a4c1a1652ae5a12
検体#04:3c20530c13d6736ec705786d1694052b2abf42bf87d3bbc359ea95b343fcf681
検体#05:21382e955d23c9c2ff9aa617070f33f898745d568b82338c9a4c1a1652ae5a12
検体#06:4e4b336ed42d4913d9c91776466e0b19ca31922lcc723d4dc21baff83eba497a
検体#07:f3d0740d9f33f2ae0821e0c30bcf90eb1363ad2407962cc3e5aa5cb9088f6707
検体#08:bfcb771bb9eb1cb4390094393f138e9686e3ee3323c09c231e16f2a102278edb
検体#09:c94498le841c36822c3db737337bd30a272c3a9d2c2a529febdca620d365928f
検体#10:980ab12028lb6ae0777363d99a3fcd9c6f93161 0bcb9b0f04f3e26a1fee54fe9

DISCLAIMER:
上記のテストは、Blue Planet-works Inc.（‘BPw’）内の厳密に管理されたテスト環境で実施されたものであり、他の環境での同様のテスト結果を保証するものではありません。BPwは、ソフトウェアテストの分野で実績を有するものを表明するものではなく、この文書に記載されている情報の使用は、お客様自身の責任で行ってください。BPwは正確な情報を提供するために最善をつくしておりますが、BPwはこのドキュメントの情報の正確性、信頼性、完全性について、明示的であるか黙示的であるかを問わず、いかなる保証もしません。

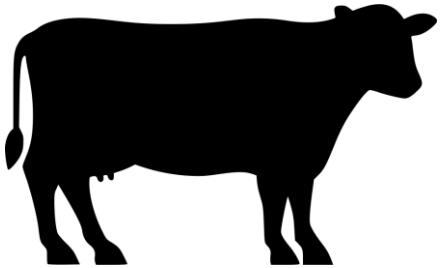
サイバー攻撃が市民生活に影響を及ぼす時代へ

Blue Planet-works
Safety for the Connected World

コロニアル・パイプライン
（Colonial Pipeline）

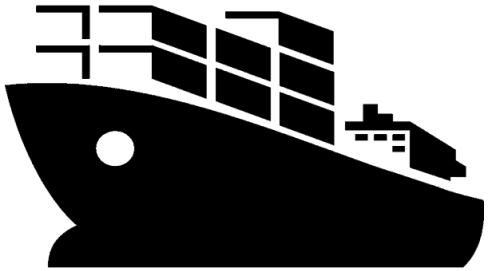
コロニアルパイプラインが提供する米国最大の燃料パイプラインがサイバー攻撃により5日間に渡って停止したことで、ガソリンのパニック買いが発生した。事態収拾のため、約4.8億円の身代金を攻撃者に支払った。

JBS
（JBS S.A.）



食肉加工世界最大手JBSに対するサイバー攻撃で米国及びオーストラリアの施設5箇所以上で操業を停止した。市場の混乱を避けるため、約12億円の身代金を攻撃者に支払ったことで被害を最小限に抑えた。

マサチューセッツ汽船公社
（Mass. Steamship Authority）



米国マサチューセッツ州の汽船公社がサイバー攻撃を受け、ウェブサイトがシャットダウンされたことで乗客の予約や変更処理、クレジットカード決済ができなくなる等、汽船の運航に大きな支障が出た。

オールズマー市水道局
（Oldsmar, Florida）

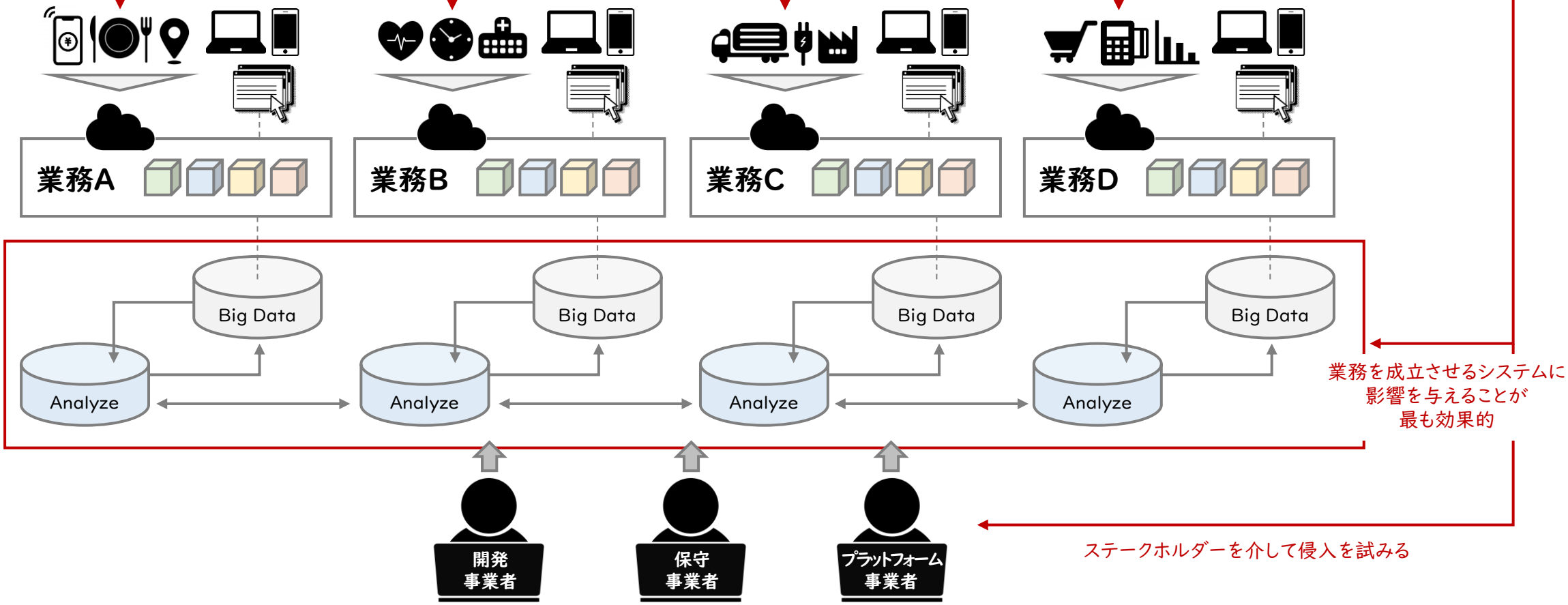
米国フロリダ州オールズマー上水道処理施設がサイバー攻撃を受け、SCADAシステムへ不正アクセスされた。攻撃者により水酸化ナトリウムの投与量が規定値の100倍に設定された。すぐに修正されたが重大事故につながる可能性があった。

DXの進展でAttack Surface（攻撃対象領域）が拡大

Blue Planet-works
Safety for the Connected World

人手不足 ⇨ 業務のシステム化 ⇨ 業務の自動化 ⇨ システム依存の業務 ⇨

インターネット接続やネットワーク間で相互接続する「モノ」の数が飛躍的に増加（Attack Surfaceの拡大）



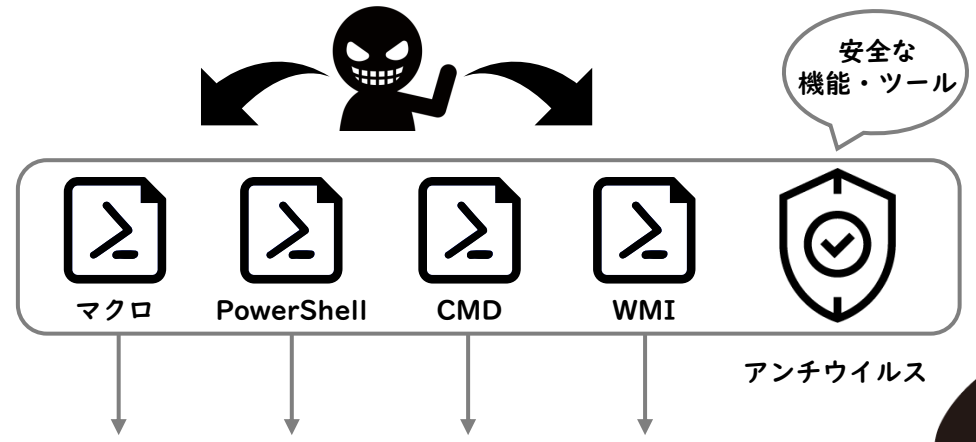
業務を成立させるシステムに
影響を与えることが
最も効果的

ステークホルダーを介して侵入を試みる

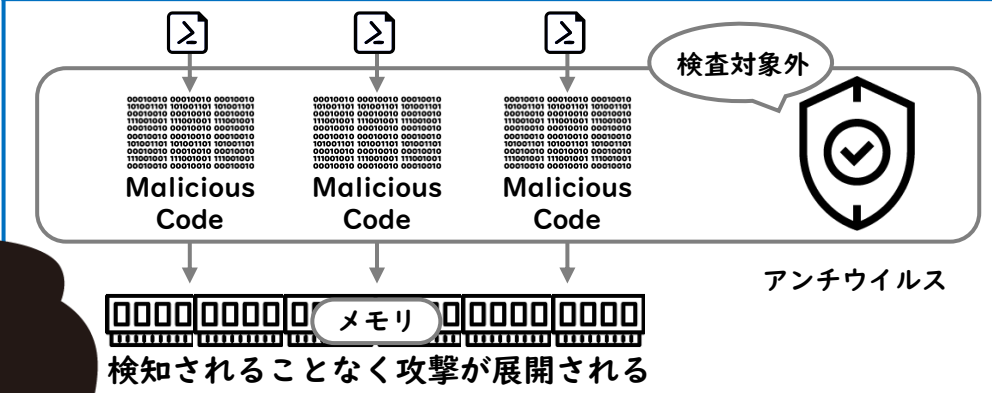
従来の対策では止められない“マルウェアフリー”の台頭

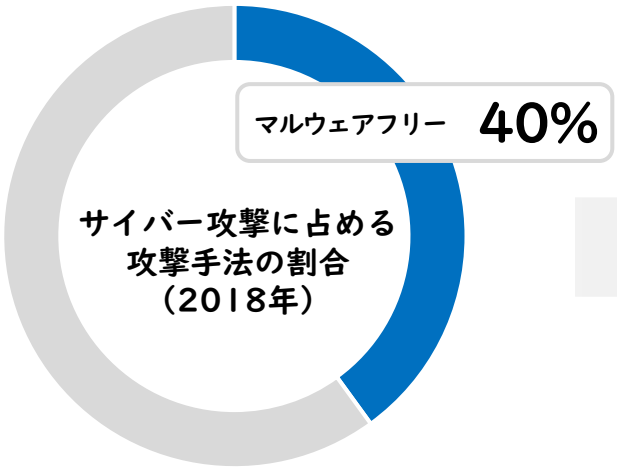
Blue Planet-works
Safety for the Connected World

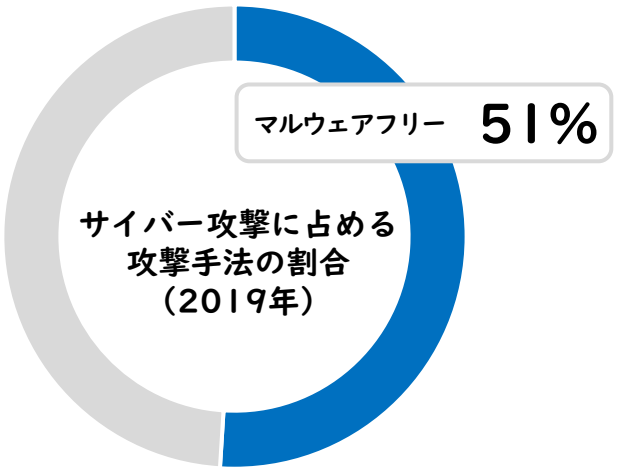
環境寄生型攻撃（Living off the land Attack）



ファイルレス攻撃（Fileless Attack）







出典：CrowdStrike「2020年版グローバル脅威レポート」

「悪いモノ」を見つける仕組みだけでは不十分な時代へ

Blue Planet-works
Safety for the Connected World

悪くないモノ

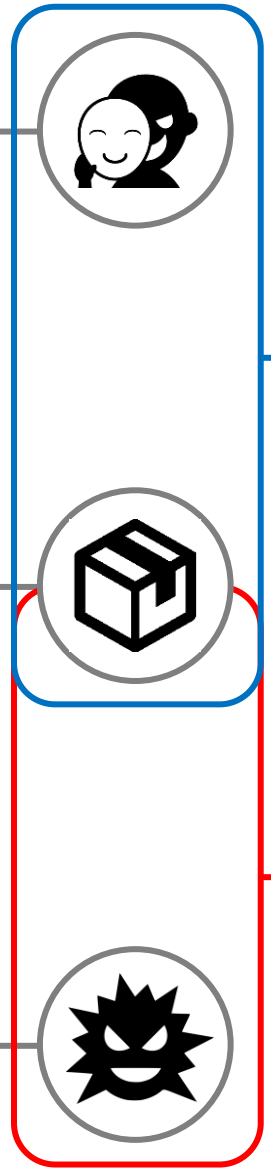
- マルウェアフリーを用いた脅威
- アンチウイルスが安全と認識している機能やツールを悪用
- ファイル形式を持たずにメモリに直接悪性コードを挿入

悪いかどうかわからないモノ

- マルウェア本体を特定されないように構造を難読化
- 難読化は流通するマルウェアの約80%が獲得している※
- 平均して20%以上のすり抜けが発生する※

悪いモノ

- 標準的なマルウェア



選択肢①：事前対策の強化

選択肢②：事後対策の強化

従来のセキュリティ対策は
“悪いモノ”に対するアプローチ

多層的に対策機構を積み上げても、そのコンセプトが故に対処できない脅威が存在し続ける。

出典：Symantec「インターネットセキュリティ脅威レポート」
出典：Network and Distributed Systems Security (NDSS) Symposium 2020「When Malware is Packin’ Heat;Limits of Machine Learning Classifiers Based on Static Analysis Features」

事前対策と事後対策の間に存在するギャップ

Blue Planet-works
Safety for the Connected World

NISTサイバーセキュリティフレームワークに潜む課題

事前対策

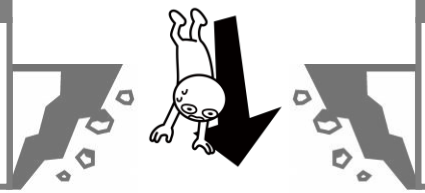
特定 Identify

システム・資産・データ・機能に対するセキュリティ・リスクの特定を行う。

防御 Protect

特定したセキュリティ・リスクに対して適切な予防策を講じる。

多くの組織は
ギャップを超えられない



事後対策

検知 Detect

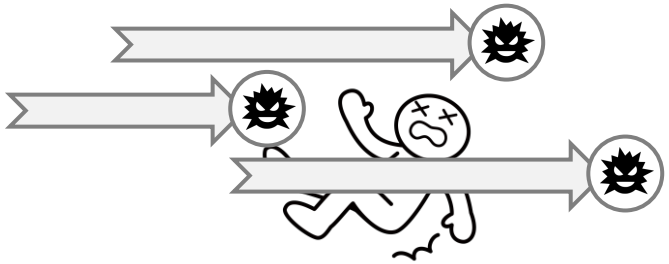
侵入した脅威や生じているインシデントを検出するための対策を講じる。

対処 Respond

検知された問題に対処するための適切な対応プロセスを構築する。

回復 Recover

阻害された箇所を正常に状態に戻すための措置を施す。



マルウェアフリー等の従来のアプローチでは対処ができない脅威がすり抜ける。

そもそも単一のデータソースでは全体像はわからない。専門人材によるHuntingが不可欠である。

侵害された痕跡から脅威や攻撃を特定して対処に当たるため業務の継続性は失われる。

「いつすり抜けるのか？」「どこに着弾するのか？」「どのように炎上するのか？」
事前に予測することはできないため監視体制と対応人員の“練度”に依存

侵入した脅威を無効化する「AppGuard（アップガード）」

Blue Planet-works
Safety for the Connected World

サイバー攻撃（不正ソフトウェアの起動/不正アクセスによる乗っ取り）を成立させないことで ユーザーの業務継続性を担保

悪くないモノ

悪いかどうかわからないモノ

悪いモノ

アンチウイルス
（Protect）

アンチウイルスは過去の情報に基づいて定義された「悪いモノ」を見つけて駆除する。「悪いかどうかわからないモノ」「悪くないモノ」にはアプローチできない。

AppGuard
（Prevention）

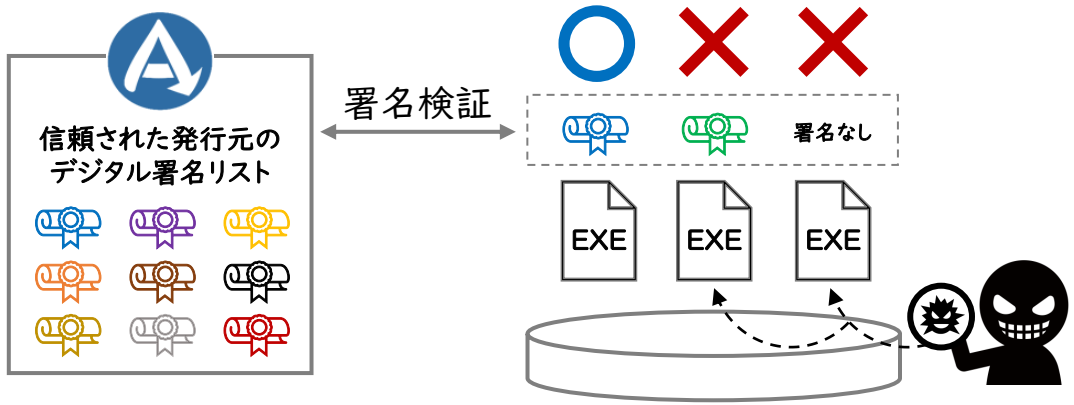
AppGuardは実行主体に関係なくシステムに対して害を与える不正な行為を制御して無効化する。つまり、端末上で「悪いコト」を実行できない状態を作り出す。

AppGuardが提供する2つの制御

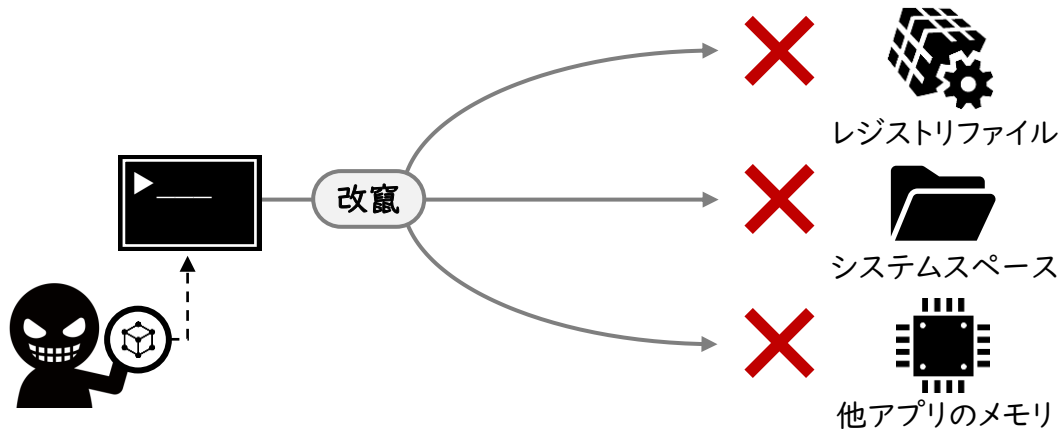
Blue Planet-works
Safety for the Connected World

AppGuardは“侵入されても発症しない”
その真髄は“攻撃者の最終目的を達成させない”こと

信頼されたアプリケーションしか起動させない
（不正ソフトウェアの生成及び発症を制御）



不正アクセスにおける侵攻プロセスを成立させない
（不正アクセスを成立させるために必要な3つの行動を制御）



スペースルール

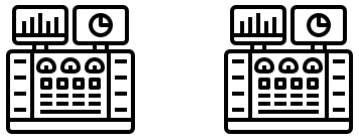
改竄処理の防止

デジタル化の推進に向けてAppGuardであらゆるシステムを守る

Blue Planet-works
Safety for the Connected World

今後の展望

産業システム

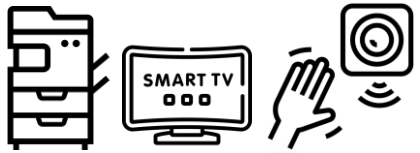


生産領域などで利用される産業システムを保護する。

業務システム

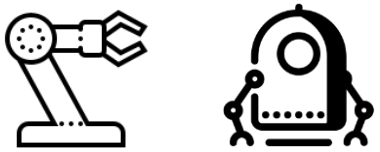
業務で利用される様々なシステムを保護する。

IoTデバイス



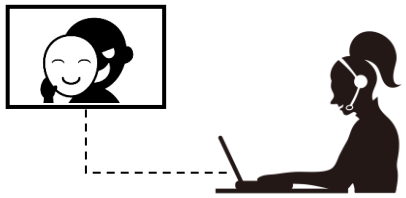
ネットワーク接続される様々なデバイスを保護する。

ロボット



ネットワーク接続して制御されるロボットを保護する。

業務上リスクが高い端末

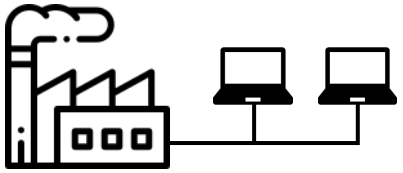


サポートセンターなどの不特定多数の相手と情報のやり取りが発生する端末を保護する。

レガシーな端末

Windows 7などのサポートが終了したOSをやむを得ず継続利用している端末を保護する。

閉域環境にある端末



生産領域などインターネットに接続できない環境にある端末を保護する。

機密情報を扱う端末

法務、購買、IR、R&Dといった組織内でも特に機密性の高い情報を扱う端末を保護する。

重要インフラを担う企業の端末

情報通信	金融	航空
空港	鉄道	電力
政府・行政	医療	水道
物流	化学	クレジット
ガス	石油	

国民生活及び社会経済活動の基盤となり停止することが許されない領域の端末を保護する。

AppGuard採用実績

Blue Planet-works
Safety for the Connected World

“AppGuardは、世界のすべてのWindowsシステムに導入されるべきだ”

Robert Bigman
元 Chief Information Security Officer, CIA

主要グローバルクライアント

クライアントの声

AppGuardは検証、運用における継続的なセキュリティ問題から救ってくれました。

全日本空輸（ANA）

AppGuardを使用することでインシデントは発生しなくなり、重要なインフラストラクチャが安全であるという安心感が得られています。コスト効率が高く、効果的なソリューションです。

米国大手国際法律事務所

2019年より導入を開始し、働き方改革の一環でAppGuardがインストールされているPCだけを対象に社外への持ち出しを許可する運用ルールを制定。コロナ禍におけるテレワークもスムーズに移行ができました。

戸田建設

AppGuardの概念を知るにつれて、これはサイバーセキュリティ界の最終兵器ではないか、と考え導入を決定しました。

諏訪信用金庫

Blue Planet-works
Safety for the Connected World

ありがとうございました。