テレワーク時代のエンドポイントセキュリティ『AppGuard』

2021年5月14日

株式会社Blue Planet-works　松﨑 正徳
株式会社アイエスエフネット　土井 広毅

アジェンダ

1. 株式会社アイエスエフネット 会社概要
2. 今回のタッグのきっかけ
3. テレワーク化におけるセキュリティの悩み
4. AppGuardが求められる時代背景
5. サイバー攻撃に対抗する新しいアプローチ
6. AppGuardの外部評価
7. 導入実績
8. 製品ラインナップ

会社概要

設立	2000年1月12日
資本金	1億円
代表者	代表取締役　渡邉　幸義
役員	取締役　本村 誠基　　監査役　境 健一郎 取締役　若本 康平
従業員数	アイエスエフネット：2,317名 グループ全体： 2,440名（2021年1月1日現在）
提供サービス	クラウドソリューション、ITインフラ構築、ITフィールドサービス、 ITヘルプデスク、リモート監視、全国オンサイト保守、 EOSL保守サービス、グローバルサービス、 障がい者法定雇用率達成サポートエンジニアリングサービス 等
グループ	株式会社アイエスエフネットライフ、 株式会社アイエスエフネットジョイ、 特例子会社アイエスエフネットハーモニー、 一般社団法人アイエスエフネットベネフィット

エンジニア派遣

エンジニアを3,000名以上育成してきた
実績と、国内に広がる拠点を持つ
サポート体制により、迅速かつ柔軟な
対応が可能です。

ITヘルプデスクサービス

常時24時間365日対応可能な体制で、
お客さまにご安心頂けるサポートを
ご用意しています。

オンサイト保守

首都圏を中心に、専任のエンジニアが
責任を持って解決いたします。

ITフィールドサービス

ビル移転や事務所のレイアウト変更など、
小規模案件から大規模プロジェクトまで、
全国各地のお客さまの現場で
当社エンジニアが作業いたします。

ITインフラ構築

お客さまの現状・課題そして戦略を詳しく
ヒアリングすることで、課題に対して
最適なインフラ環境をご提供いたします。

クラウドソリューション

専任のコンサルタントが、貴社にとって
最適なクラウドサービス導入計画を
ご提案いたします。

ITインフラ領域での豊富な課題解決実績

ISF NET

×

Blue Planet-works

Safety for the Connected World

新時代のセキュリティサービスプロバイダー

こんなお悩みありませんか？

うちの社員 ITリテラシー低いんだよなぁ・・・

ZIPファイルとか何の疑いもなく開いちゃうからなぁ・・・

ファイルレス攻撃なんて防げないよ・・・

さらに

テレワーク環境で

＊しっかりとしたセキュリティ環境が作れない・・・

＊セキュリティに対する社内啓蒙が行き届かない・・・

そんなお悩み解決を行うのが

Blue Planet-works 社

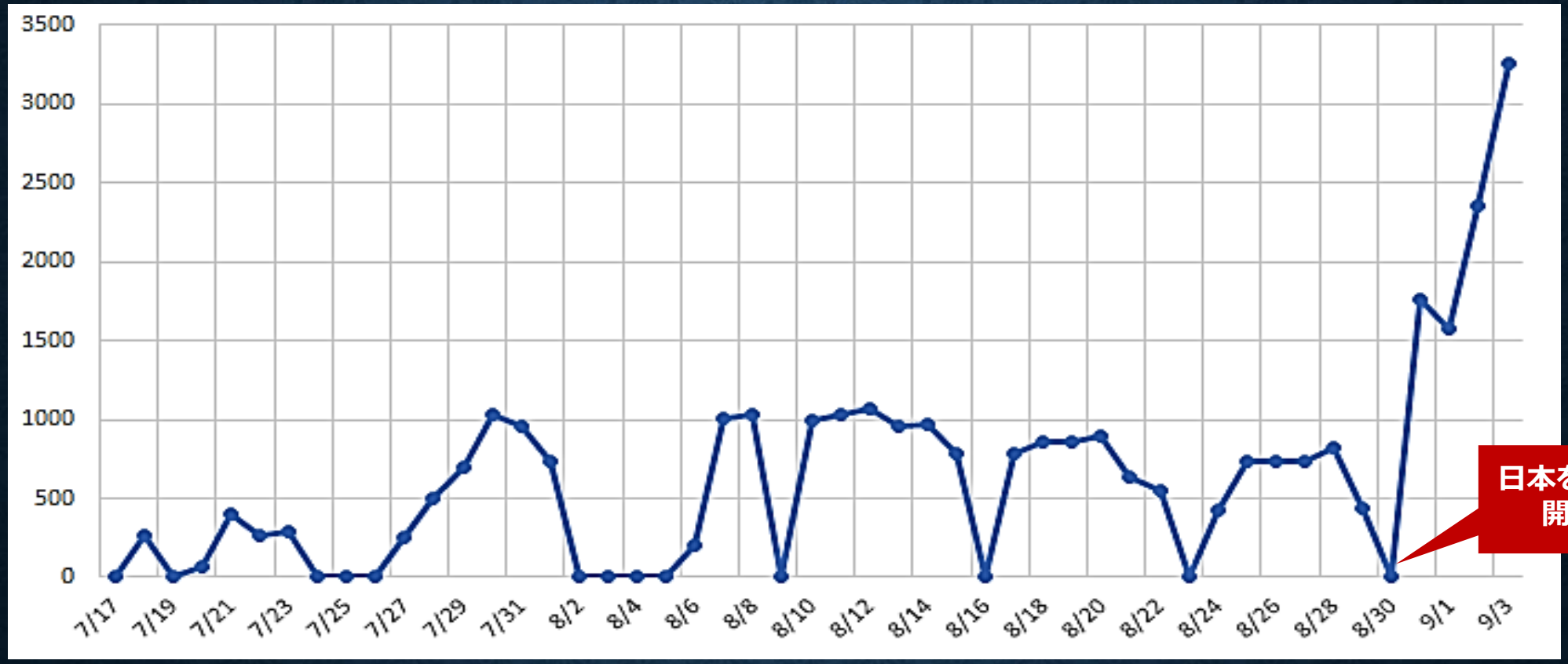
『*AppGuard*』

アンチウィルス入れてるから大丈夫！？

大丈夫ではございません。

最新のAI型検索エンジンを用いても**20%**が
セキュリティ網を通過してしまうのです。

アンチウィルス入れてるから大丈夫！？



2020年　Emotet感染被害社数　（出典：https://www.jpcert.or.jp/newsflash/2020090401.html）

3日間で3,000社以上が感染

Blue Planet-works
Safety for the Connected World

AppGuardのご紹介

～サイバー攻撃に対抗するための新しいアプローチ～

Blue Planet-works, Inc.

松﨑　正徳

まずはじめに

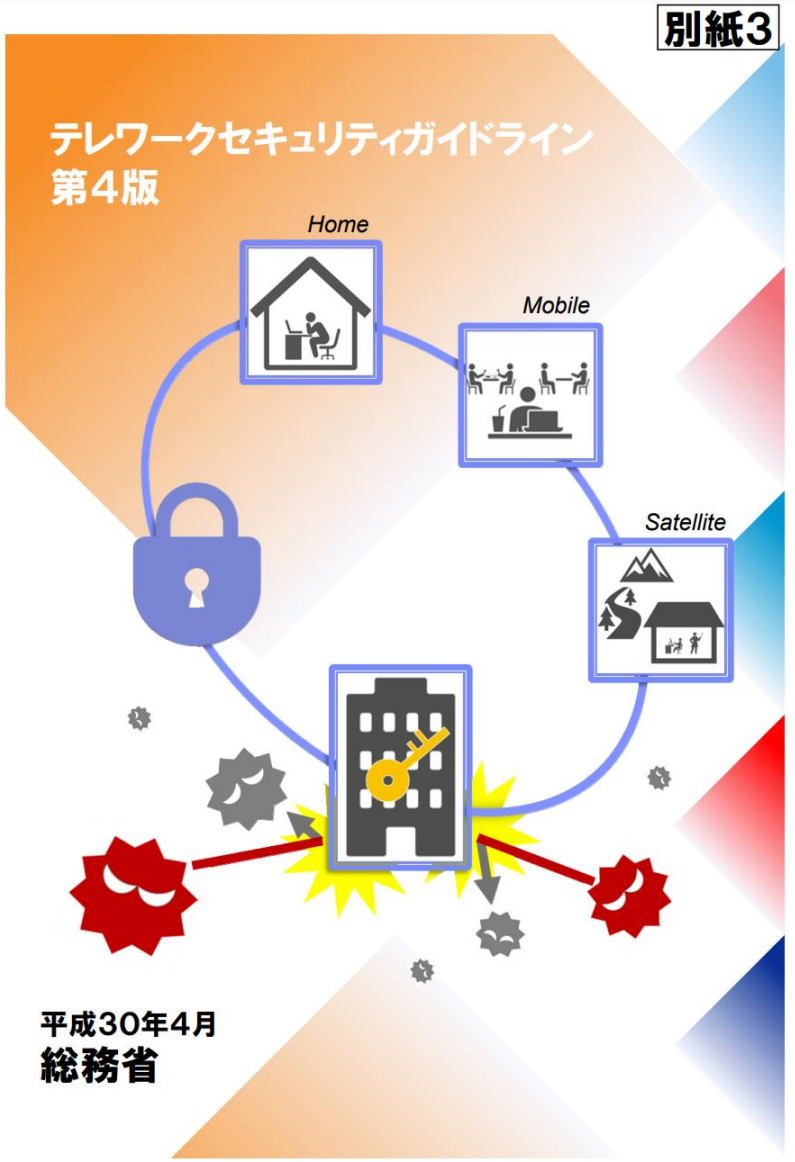
1-3月までPM11時からのWBS枠にてCM放映

～飛ぶぞデータ篇～

～感染を派手に告げる妖精編～

総務省によるテレワークセキュリティガイドライン

総務省ではテレワークにおける脅威と脆弱性について、
テレワークセキュリティガイドラインを通じて警鐘を鳴らしています。



テレワークにてサイバーセキュリティ被害が急増

Blue Planet-works
Safety for the Connected World

本田技研工業がテレワークが原因でマルウェアに感染し工場が操業停止に・・・

朝日新聞 DIGITAL

速報　朝刊　夕刊　連載　特集　ランキング　…

トップ　社会　経済　政治　国際　スポーツ　オピニオン　IT・科学　文化・芸能

朝日新聞デジタル ＞ 記事

独自

ホンダ、サイバー攻撃被害認める　身代金ウイルス拡大か

有料会員記事

稲垣千駿　編集委員・須藤龍也　2020年6月9日 20時01分

シェア　ツイート　ブックマーク　メール　印刷

list　69

ホンダの社内ネットワークで、ランサムウェアが活動していた痕跡を示す解析画面（三井物産セキュアディレクション提供）

ホンダ は9日、社内ネットワークシステムが サイバー攻撃 を受けたと明らかにした。8日に大規模な障害が発生し、原因を調べていた。この影響で同日、米国やトルコ、インドなどの計11工場の生産が停止した。このうち4工場の再開時期は未定としている。自動運転技術といった機密情報などの流出は確認されていないとしている。

同社によると、社内システムの障害は8

三菱重工がテレワーク時に感染したマルウェアから個人情報流出・・・

ニュース　2020.09.05

三菱重工、在宅勤務時に感染したマルウェアから個人情報流出

三菱重工業株式会社は8月7日、名古屋地区内の社内ネットワークが第三者による不正アクセスを受け、従業員の個人情報などが流出したと発表した。

流出したのは、三菱重工グループの従業員の名前やメールアドレスなどの個人情報のほか、サーバのログ、通信パケット、サーバ設定情報など。

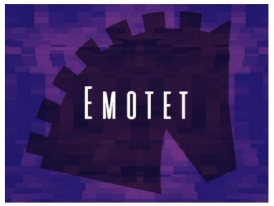
名古屋地区では民間航空機や宇宙開発などに関連する工場があるが、取引先や防衛、航空機開発関連など機密性の高い情報の漏えいは確認されていない。

三菱重工業によると、名古屋地区の従業員が4月末の在宅勤務時に社用のノートパソコンで、社内ネットワークを経由せずに会員制交流サイト（SNS）に接続した際、ソーシャルエンジニアリング（人間の心理的な隙や行動のミスにつけこんで情報を入手する方法）によって第三者から受信、ダウンロードしたファイルからコンピュータウイルスに感染。

その後、この従業員が出社し、社内ネットワークにウイルスに感染したパソコンを接続したことで、社内にウイルスが広がったという。

AppGuardが求められる時代背景

2019-2020年とEmotetの被害企業が急増



マルウェア「Emotet」の国内感染、少なくとも3200組織に

https://japan.zdnet.com/article/35149139/

NTT西日本のグループ社員がEmotetに感染、複数の不審メールが確認される

2019.12.19 2019.12.19 事務局 編集部

NTT 西日本グループ会社社員を装った不審なメール（なりすましメール）に関するお詫びと注意喚起について

この度、NTT 西日本グループ会社の社員のパソコンがマルウェア（Emotet）に感染し、NTT 西日本グループ会社の社員を装った第三者からの不審なメールが複数の方へ発信されている事実を確認いたしました。

現在、上記以外の事実関係について引き続き調査しておりますが、二次被害や拡散の防止に努めております。

上記メールを受信された皆さまには多大なご迷惑、ご心配をおかけしたことを心より深くお詫び申し上げます。

インシデント・事故 ／ インシデント・情報漏えい　2020年2月5日（水） 09時45分

社員のパソコンがEmotet感染、なりすましメールへの注意を呼びかけ（川本製作所）

ポンプの製造と販売を行う株式会社川本製作所は2月3日、同社社員のパソコンがウイルスEmotetに感染し個人情報等の流出が判明したと発表した。

JPCERT CC®

Emotet などのマルウェア感染に繋がるメールに引き続き警戒を

最終更新: 2020-12-22

https://www.jpcert.or.jp/newsflash/2020122201.html

経営リスクの拡大および個人情報保護法の改定

Blue Planet-works
Safety for the Connected World

カプコン襲ったハッカー集団の正体、経営陣を「2重苦」で恐喝

日経ビジネス

「暴露型ランサムウエア」と呼ばれる新手のコンピューターウイルスが、今春以降、世界的に猛威を振るっている。11月上旬にはゲーム大手のカプコンが襲われた。実行犯を名乗るハッカー集団は社外秘のデータを盗み出し、自前で立ち上げた暴露サイトに定期的に投稿している。カプコンが金銭を支払うまで小出しに投稿を続けると脅しており、じわじわと経営陣を追い詰めている。

カプコンの格闘ゲーム「ストリートファイター」のキャラクター、リュウもハッカーにはかなわない？（写真：アフロ）

改定個人情報保護法

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会□からの命令への違反	行為者	６月以下	**１年以下**	３０万円以下	**100万円以下**
	法人等	-	-	３０万円以下	**１億円以下**
個人情報データベース等の不正提供等	行為者	１年以下	１年以下	５０万円以下	５０万円以下
	法人等	-	-	５０万円以下	**１億円以下**
個人情報保護委員会□への虚偽報告等	行為者	-	-	３０万円以下	**５０万円以下**
	法人等	-	-	３０万円以下	**５０万円以下**

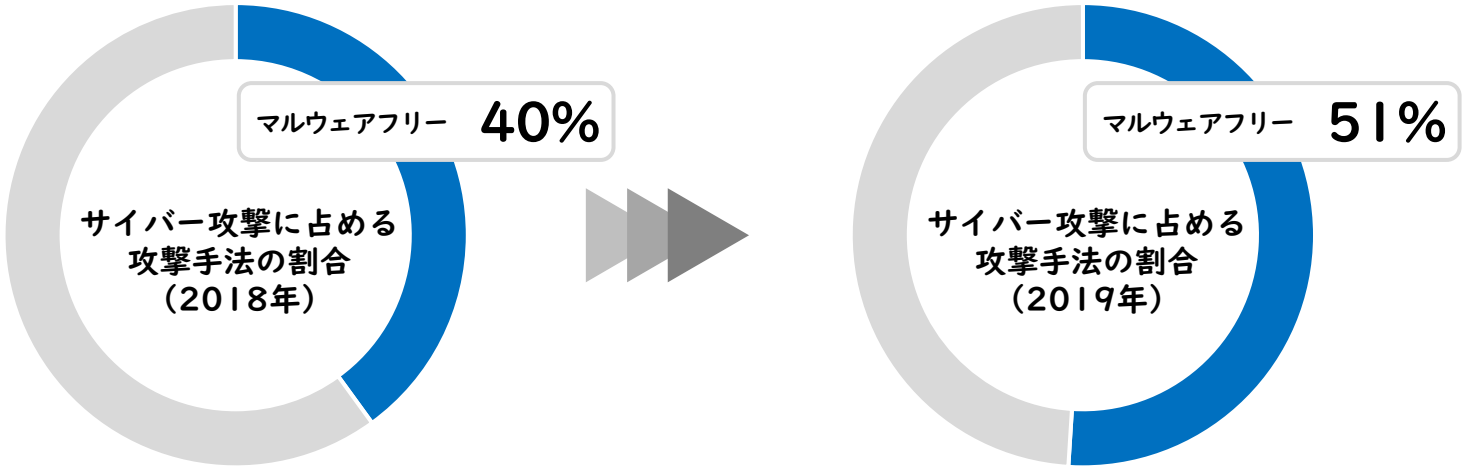
罰則規定も設けられ2022年度の春からは、不正アクセスによる情報流出などが発生した場合において、当局や被害者への報告を怠った企業に対して、最大1億円の罰則が科されることになりました。

**企業においては調査による経済的な費用も、相当な負担です。
今回の法改正では企業に「当局や被害者への詳細な報告」を求めており
この詳細な報告を行うためのデジタルフォレンジック調査費用は、
パソコン1台あたり約100万円相当と非常に高額な費用がかかります。**

近年はインシデント発生時の経済的な損失をカバーするサイバー保険なども登場していますが、国内においては導入が進まず、企業全体のうち1割程度の加入率にとどまっている現状が指摘されています。

Blue Planet-works
Safety for the Connected World

アンチウイルスを回避する「マルウェア・フリー」がサイバー攻撃の主流になりつつある



マルウェアフリーに分類される攻撃手法	特徴
Living off the Land Attacks（環境寄生型攻撃）	アンチウイルスが「安全なもの」として認識しているパソコン内のシステムツール等を悪用する。
File less Attacks（ファイルレス攻撃）	アンチウイルスの検査対象となる「ファイル」という形式を持たずにパソコン内のメモリに直接攻撃をロードする。

出典：CrowdStrike「2020年版グローバル脅威レポート」

Emotetに対抗できていないアンチウイルス

Blue Planet-works
Safety for the Connected World

Emotetの検体をランダムで採取してVirus Totalにて検出可能か検査（2020.10.27 AM04:00時点）

	Symantec	TrendMicro	McAfee	F-Secure	ESET	Kaspersky	Microsoft	Cylance
Emotet検体#1	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
Emotet検体#2	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
Emotet検体#3	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
Emotet検体#4	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
Emotet検体#5	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
Emotet検体#6	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
Emotet検体#7	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
Emotet検体#8	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
Emotet検体#9	検知できず	検知できず	検知	検知できず	検知	検知できず	検知	検知できず
Emotet検体#10	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

Emotet検体#1:d9b79ac09c1bfb45e09d5d9a10303ef99eb66572df7e48e1695a7cdc661904ae
Emotet検体#2:49073674853bc96f1b5d761177cc31b2e48f0c5bd7cf6acc57571ec2e101a997
Emotet検体#3:d09ff7972acdc57a90d3a820d60bcacb3fe23695380388c82ae39dfdf9c7d9e1
Emotet検体#4:911 22e95b67345a679500db2d868651 9d700fc0209878065f774b69b1d1b94995
Emotet検体#5:8f33f8964ac7ae087988eec8f692539de1cd11e6bd47480fee2797aaf2336bc3
Emotet検体#6:a904b40bf78d71b91006ea203a7263cd11782c27f7de186355 14a38a45e67eeb
Emotet検体#7:72f3867ffdfb88733bb3f134b0a2a53f39f70475dbb3e45be29499ada36727eb
Emotet検体#8:111e7539b5400 1557afd9dd62b4cb9d0bd5681 5d5 1bcca8e2027ede590a3b87f2
Emotet検体#9:8a7fd67f95a36 1993 1f66425060437758cdd4c698 12c2e8e5202 19dbaa5ce6db
Emotet検体#10:3674df9b29f7c99f3ec320f0e4af600844f2438dba4a2d948770e44a9e6c83d0

NISTサイバーセキュリティフレームワークのギャップを埋める

Blue Planet-works
Safety for the Connected World

AppGuardはNIST CSFにおける防御と検知のギャップを埋める
攻撃を「阻止」するという概念を補完

NISTサイバーセキュリティフレームワーク

UTM/アンチウイルス

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。

すり抜けてしまう脅威

ほとんどの組織は
ギャップを超えられない

EDR

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。

ヒト・モノ・カネ・スキルの全ての要素が必要になる

NISTサイバーセキュリティフレームワークに足りない要素

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。

防止 Prevent
侵害活動の成立を阻止することでインシデントを発生させない。

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。

すり抜ける脅威の活動を阻止 ⇔ 組織の運用負担を大幅に軽減

AppGuard 誕生のきっかけ

AppGuardの開発者であるFatihは自身のセキュリティ対策環境の運用経験から１つの結論にたどり着く

ファティ・コムレコグル
（AppGuard開発者）

アンチウイルスとは・・・

- 端末に侵入する「悪いモノ＝マルウェア」を見つけるための仕組みである。
- 例えるのであれば「警察」であり、様々な捜査手法で犯人を追い詰めるが、時には誤認し、時には取り逃がすことがある。
- 「悪いモノ」を見つけるために過去の「悪いモノ」から検出対象のモデルデータを作る。
- 過去の情報に依存しているので新しいタイプの「悪いモノ」をすぐに見つけることができない。
- 製品の特性上、常に攻撃者優位のいたちごっこという構図ができてしまう。

「悪いモノ＝マルウェア」を捕まえてもすぐに別の新しい「悪いモノ」が生み出され続けてしまうため

それらを「検出」するという守り方では根本的な対策に至らない。

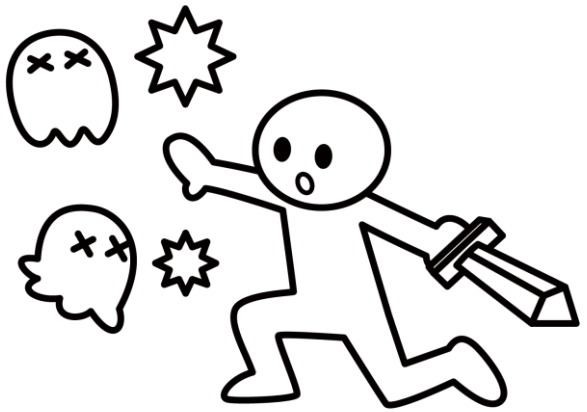
過去の情報に依存せず「悪いコト」をできないようにする仕組みがあれば問題は解決するはず！

異なる視点で端末を保護する「AppGuard（アップガード）」

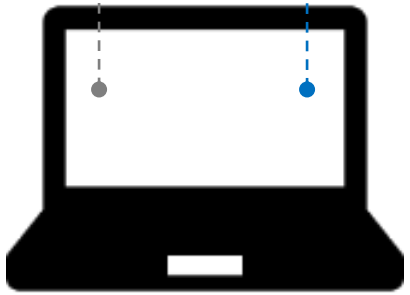
Blue Planet-works
Safety for the Connected World

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

アンチウイルス



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。

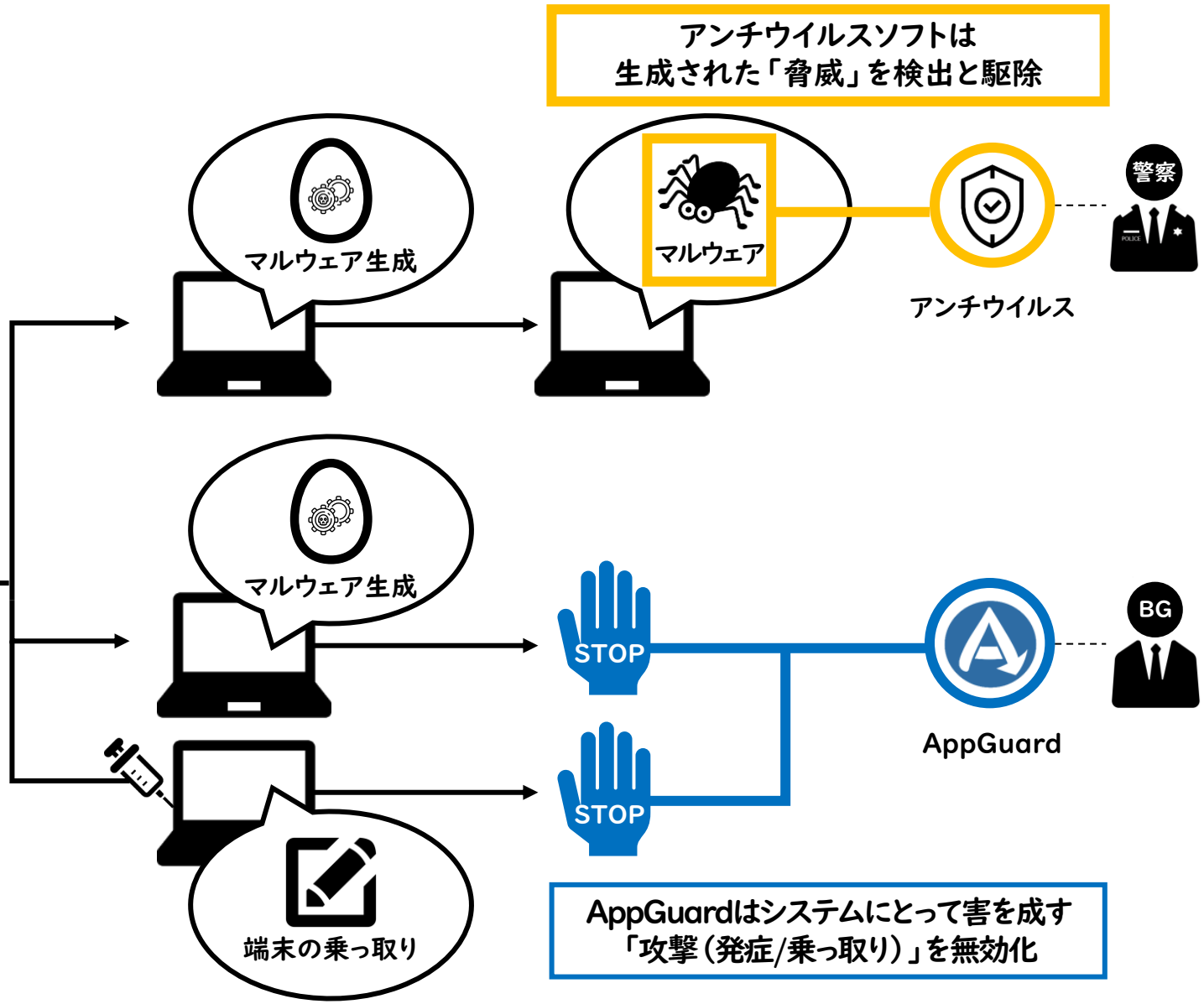


AppGuard

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。

「アンチウイルスソフト」と「AppGuard」の違い

	アンチウイルス	AppGuard
役割	悪いヤツを見つける	悪いことをさせない
マルウェアの検知	○	×
マルウェアの駆除	○	×
マルウェアの生成阻止	×	○
マルウェアの起動阻止	×	○
端末乗っ取り	△	○

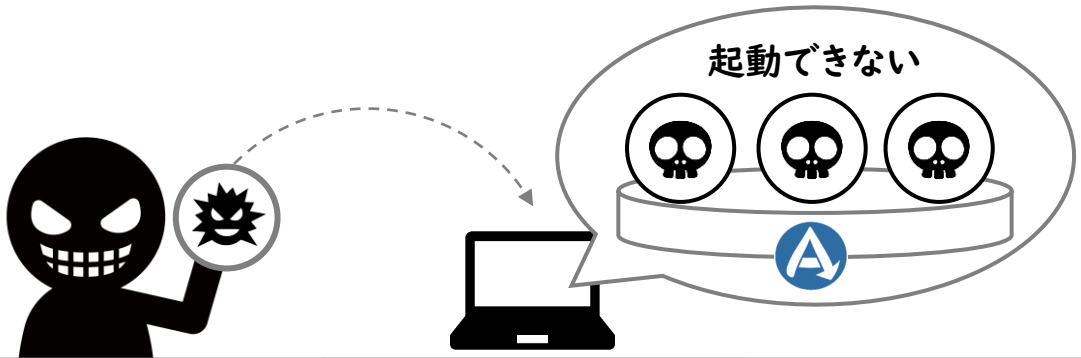


Blue Planet-works
Safety for the Connected World

AppGuardは2つの制御で「マルウェアの生成と感染」と「端末の乗っ取り」を阻止

AppGuardはマルウェアを発症させない

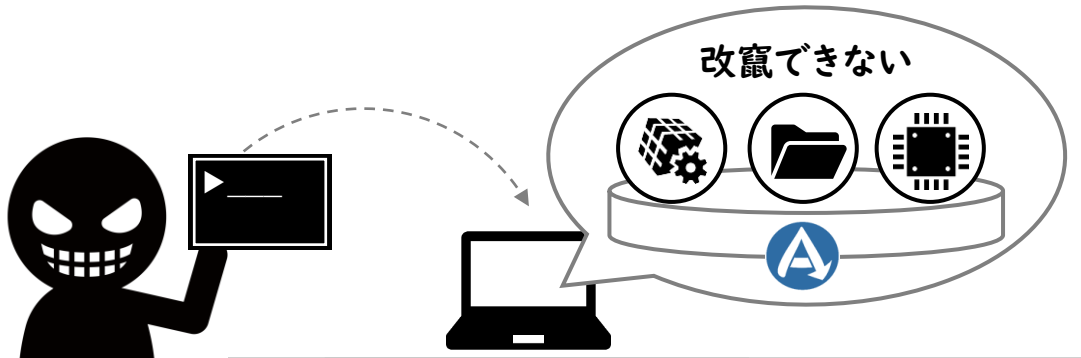
（攻撃者が送り込む悪性の実行ファイルを起動制御）



スペースルール

AppGuardは端末を乗っ取らせない

（悪用されやすいアプリケーションを通じた改竄行為を防止）



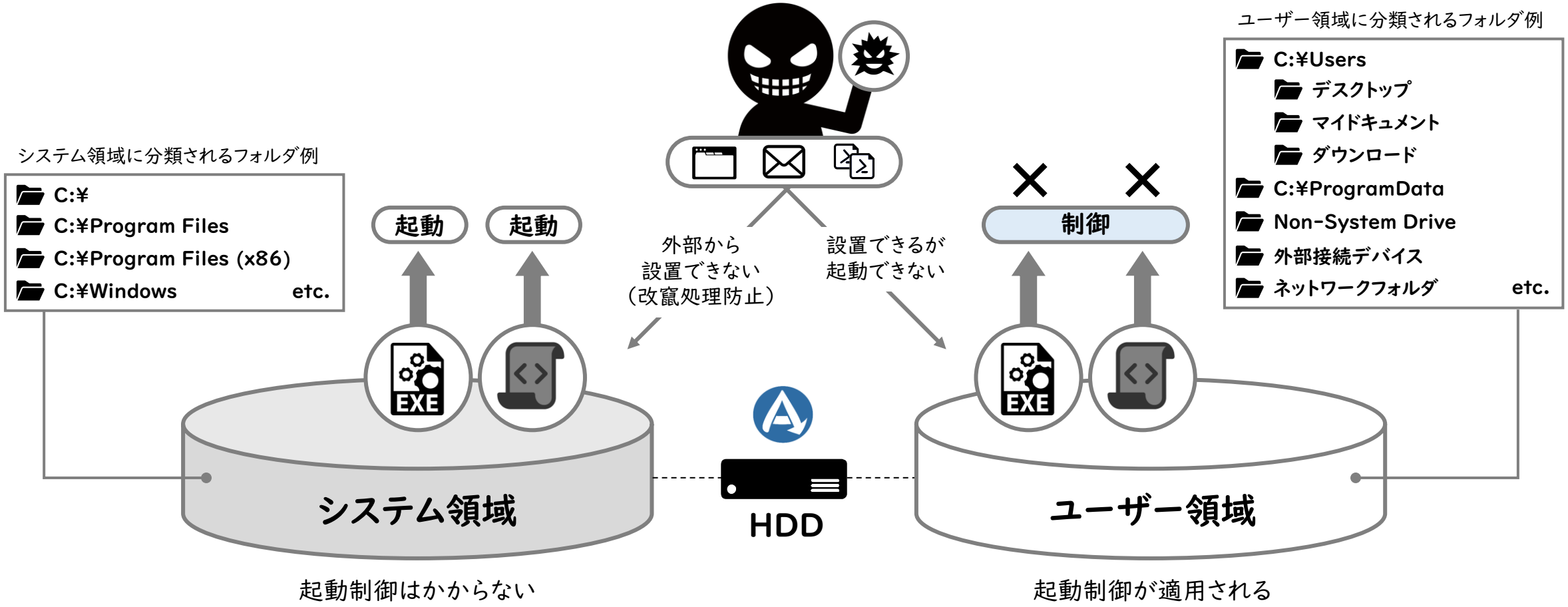
改竄処理の防止

AppGuardが提供する2つの制御：スペースルール

Blue Planet-works
Safety for the Connected World

ユーザー領域に適用される起動制御

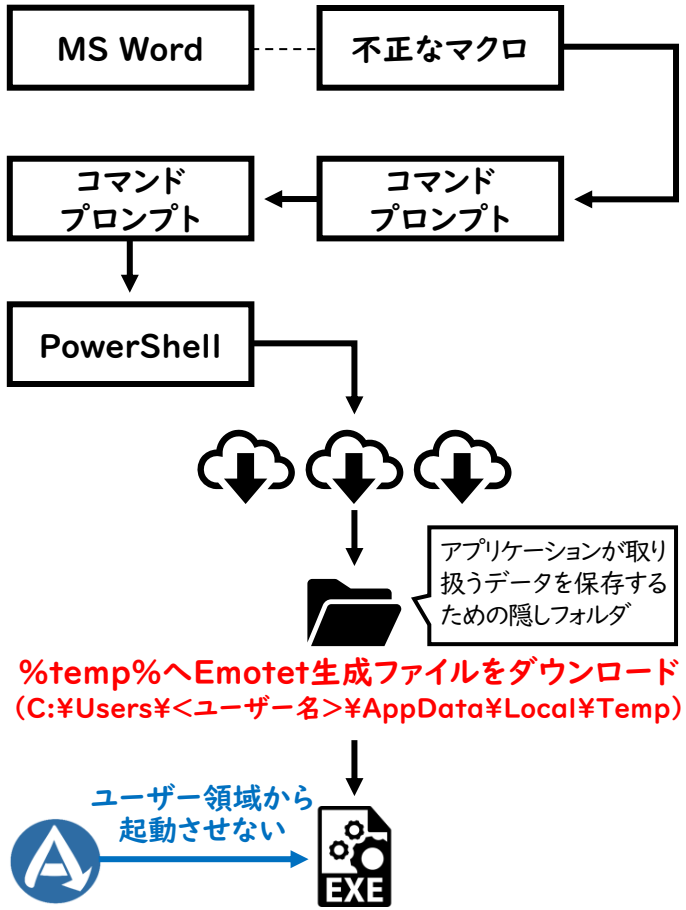
AppGuardに登録された デジタル署名を保持している	AppGuardに登録された デジタル署名を保持していない	デジタル署名を保持していない
起動許可	起動不可	起動不可



猛威を奮ったマルウェアも発症前に起動制御で無効化

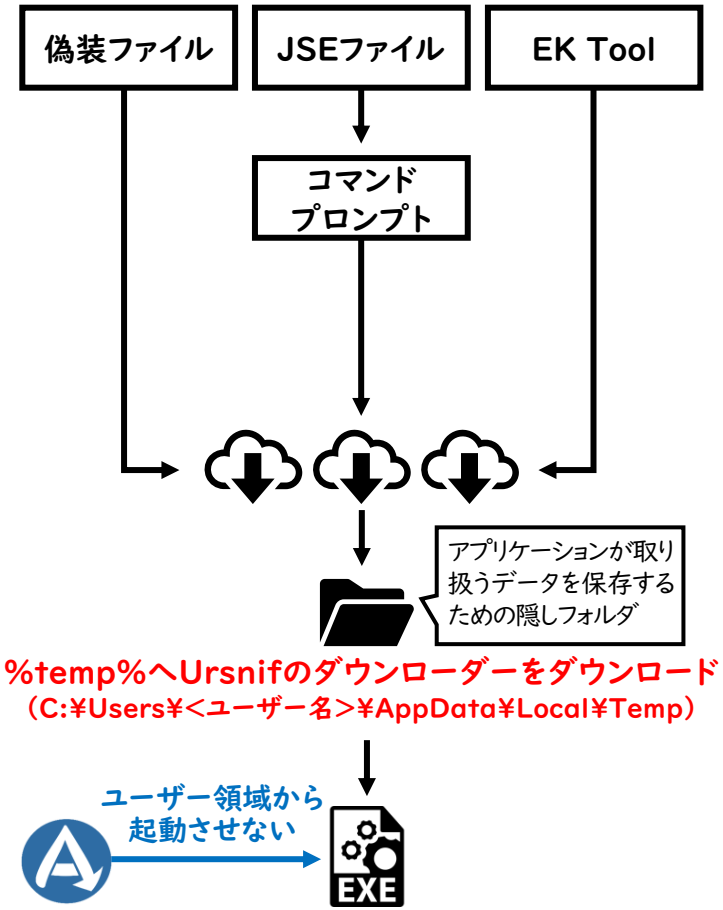
Blue Planet-works
Safety for the Connected World

Emotet（エモテット）



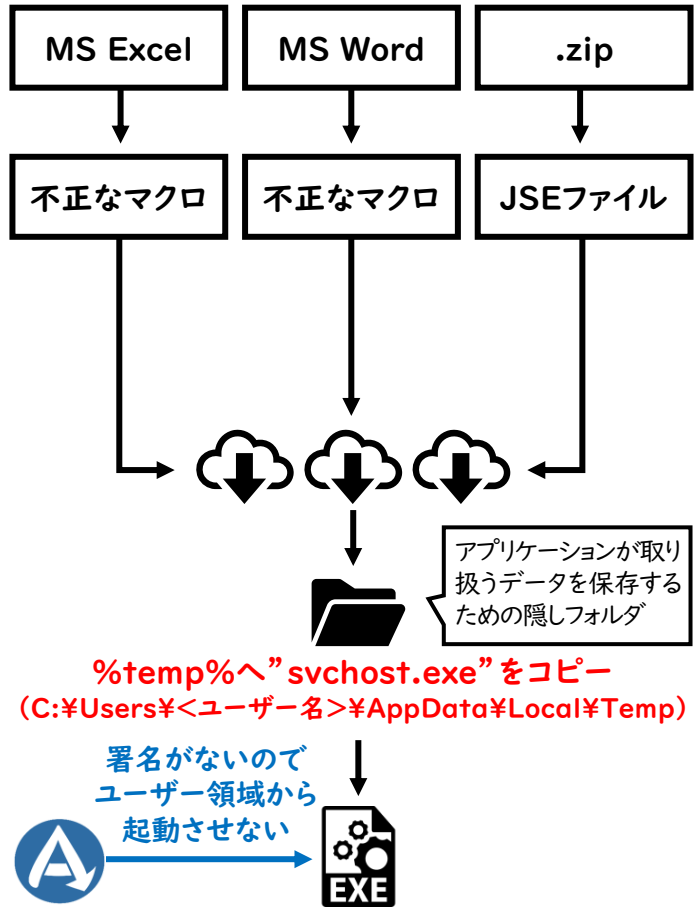
Emotet生成ファイルの実行

Ursnif（アースニフ）



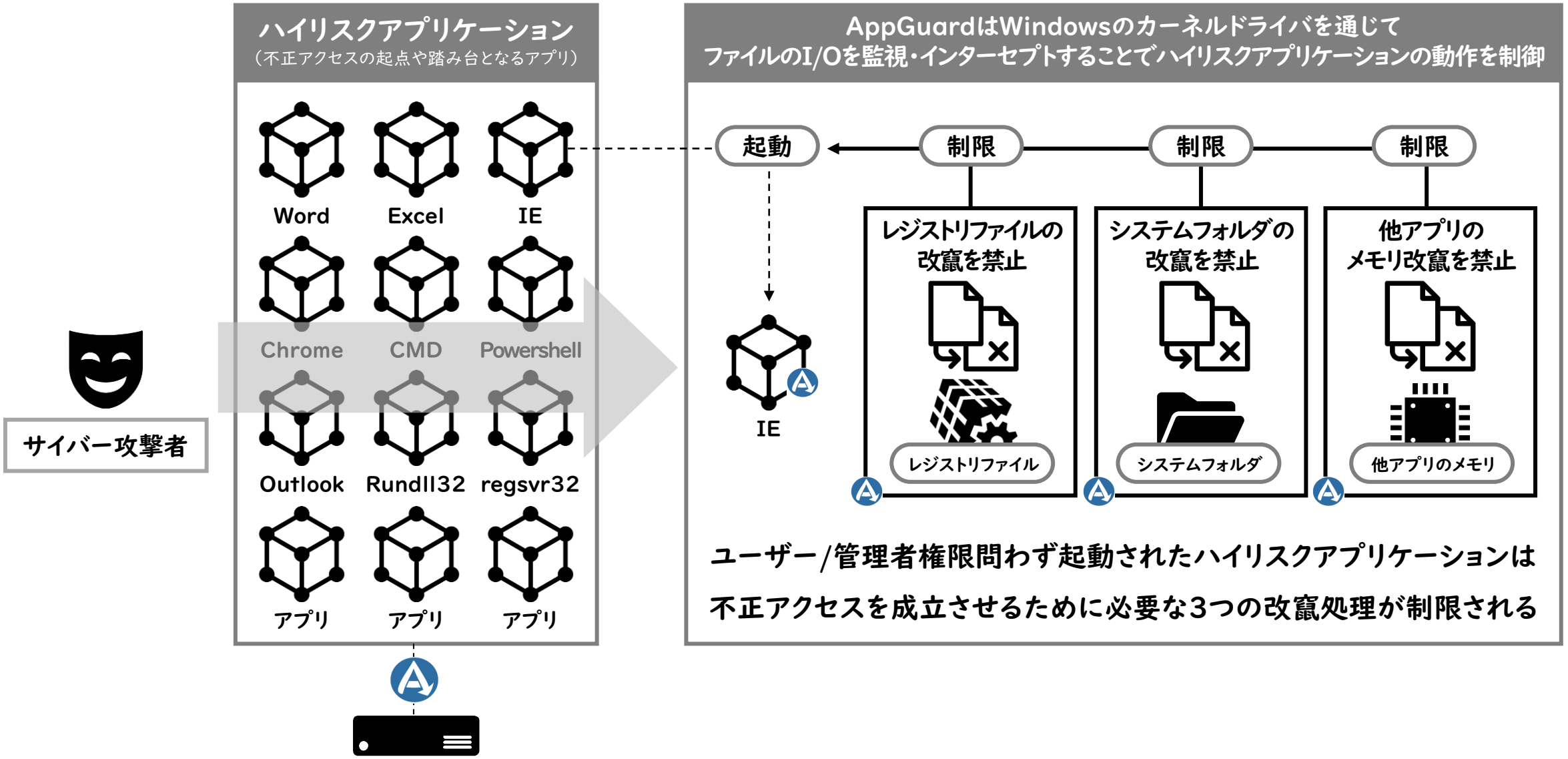
Ursnifを取得するためのダウンローダの実行

Locky（ロッキー）



svchost.exeをメモリにマッピングして再起動を試みる

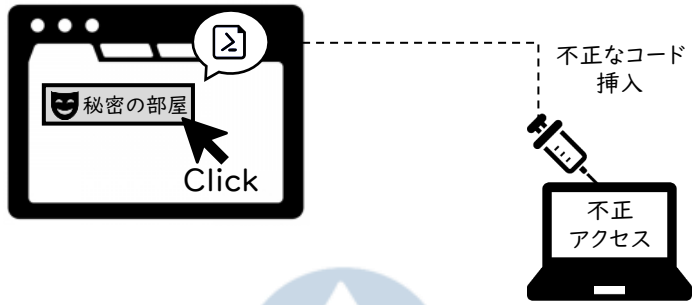
AppGuardが提供する2つの制御：改竄処理の防止



ユーザはサイバー攻撃を気にせず日常業務を遂行する事ができます

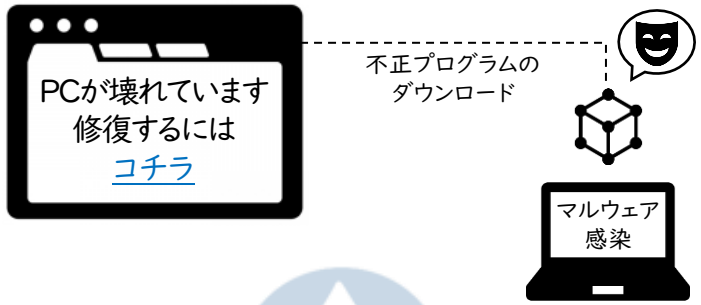
Blue Planet-works
Safety for the Connected World

怪しい広告をクリックしても



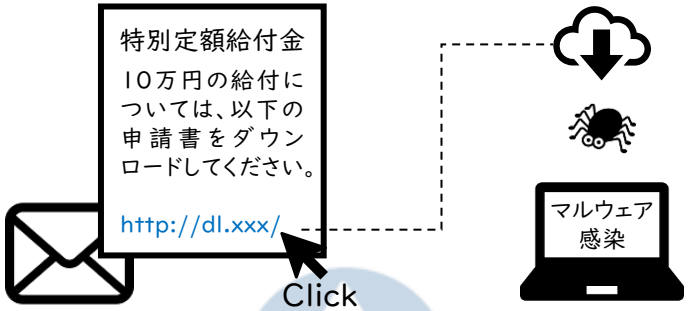
不正アクセスは成立しない

騙されて怪しいアプリを実行しても



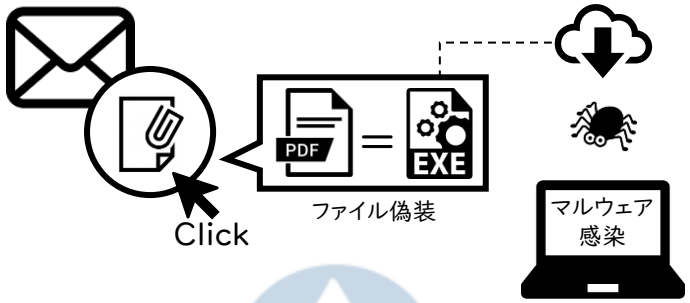
不正プログラムは実行不可

本文の怪しいURLクリックしても



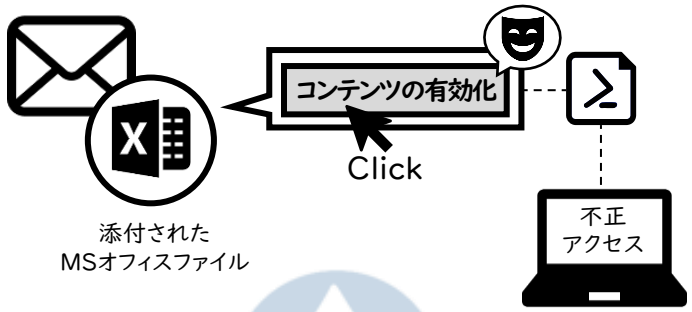
不正プログラムは実行不可

怪しい添付ファイルを実行しても



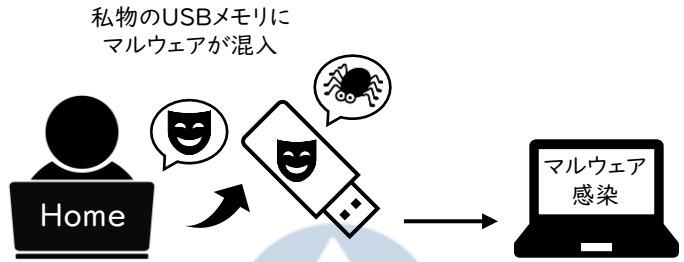
不正プログラムは実行不可

添付ファイルのマクロを有効化しても



不正プログラムは実行不可

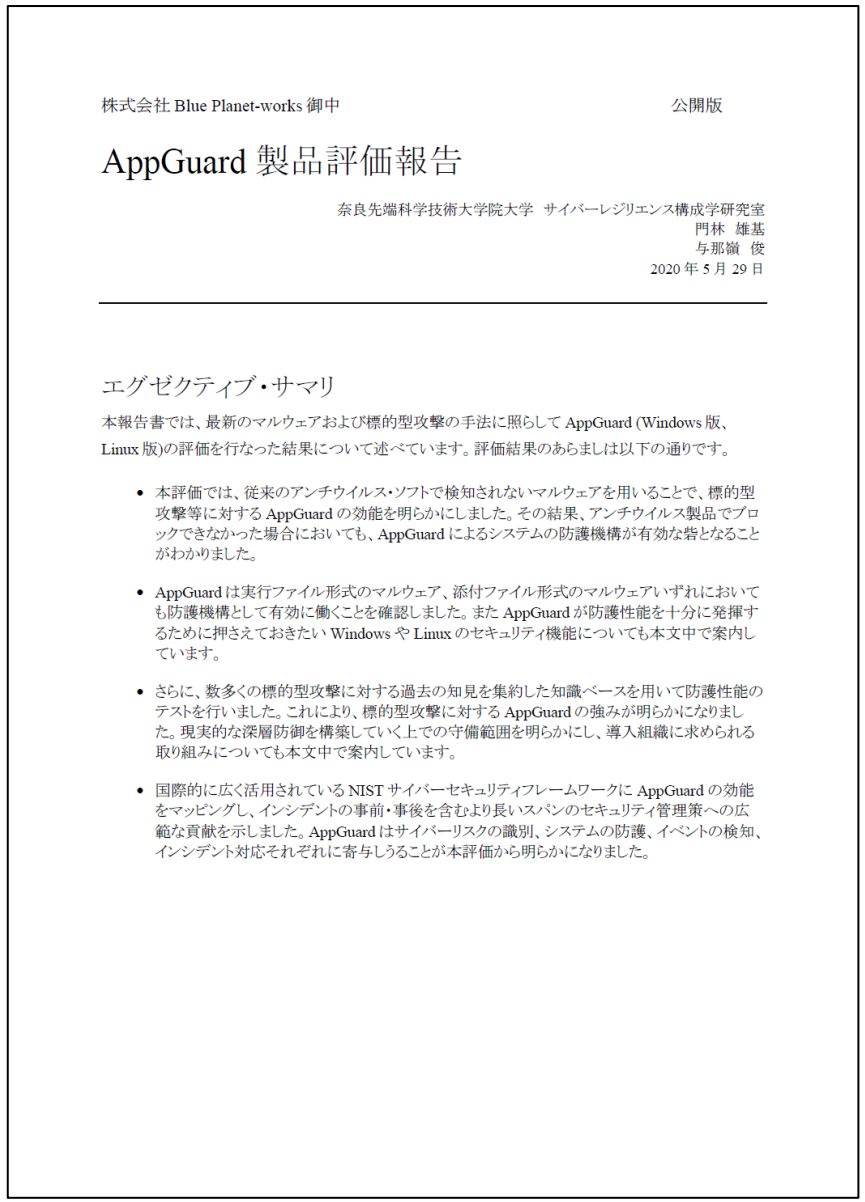
マルウェア入りUSBメモリを挿しても



不正プログラムは実行不可

AppGuardの外部評価

NAISTサイバーレジリエンス構成学研究室による評価



株式会社 Blue Planet-works 御中　　公開版

AppGuard 製品評価報告

奈良先端科学技術大学院大学　サイバーレジリエンス構成学研究室
門林　雄基
与那嶺　俊
2020 年 5 月 29 日

エグゼクティブ・サマリ

本報告書では、最新のマルウェアおよび標的型攻撃の手法に照らして AppGuard (Windows 版、Linux 版)の評価を行なった結果について述べています。評価結果のあらましは以下の通りです。

- 本評価では、従来のアンチウイルス・ソフトで検知されないマルウェアを用いることで、標的型攻撃等に対する AppGuard の効能を明らかにしました。その結果、アンチウイルス製品でブロックできなかった場合においても、AppGuard によるシステムの防護機構が有効な砦となることがわかりました。
- AppGuard は実行ファイル形式のマルウェア、添付ファイル形式のマルウェアいずれにおいても防護機構として有効に働くことを確認しました。また AppGuard が防護性能を十分に発揮するために押さえておきたい Windows や Linux のセキュリティ機能についても本文中で案内しています。
- さらに、数多くの標的型攻撃に対する過去の知見を集約した知識ベースを用いて防護性能のテストを行いました。これにより、標的型攻撃に対する AppGuard の強みが明らかになりました。現実的な深層防御を構築していく上での守備範囲を明らかにし、導入組織に求められる取り組みについても本文中で案内しています。
- 国際的に広く活用されている NIST サイバーセキュリティフレームワークに AppGuard の効能をマッピングし、インシデントの事前・事後を含むより長いスパンのセキュリティ管理策への広範な貢献を示しました。AppGuard はサイバーリスクの識別、システムの防護、イベントの検知、インシデント対応それぞれに寄与しうることが本評価から明らかになりました。

＜以下、報告書からの抜粋＞

実行ファイル型マルウェア・サンプルが一般ユーザのフォルダに置かれた場合、AppGuardの防護機構によって実行が阻止され、マルウェアとして一切機能しないことを確認しました。これを迂回する攻撃手法はこれまで発見されておらず、また今回の評価においても防御機構に抜け漏れがないか探索を行いましたが、見つけることができませんでした。

AppGuardはシグネチャ型のアンチウイルスで検知されない未知のマルウェアであっても、その実行を阻止することができます。

また、AppGuardは特権昇格につながるさまざまなテクニックを効果的に阻止することが確認できました。攻撃検知を迂回するテクニックとして、他プロセスのメモリ空間に攻撃コードを挿入するProcess Injectionが多用されることは広く知られていますが、AppGuardはProcess Injectionを阻止します。攻撃プロセスと被攻撃プロセスがログに出力されるため、Process Injectionによる検知迂回は非常に困難だと言えるでしょう。また、EDRによる検知を迂回するためのテクニックとして、親プロセスを偽装するParent PID Spoofingが用いられますが、AppGuardはParent PID Spoofingについても効果的に阻止します。

米国政府機関での採用実績多数

Blue Planet-works
Safety for the Connected World

AppGuardは、米国陸軍の「CoN認証」を取得したセキュリティ製品です。米国政府機関でも長年の利用実績があります。

「CoN（Certificate of Networthiness）認証」はAppGuardが米国陸軍並びに米国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示します。

米国政府関連での導入実績

元CIA最高情報セキュリティ責任者（CISO）のロバート・ビッグマン氏からの推薦コメント

“AppGuard should be on every Windows system in the world.”

「全てのWindowsシステムにAppGuardを搭載すべきだ。」

Robert Bigman
Former Chief Information Security Officer
Central Intelligence Agency (CIA)

※AppGuardは開発されてから20年にわたり一度も破られたことがありません

Blue Planet-works
Safety for the Connected World

導入実績

AppGuard 採用実績

Blue Planet-works
Safety for the Connected World

Miami Dade

導入企業５,000社超

ご清聴ありがとうございました

ご不明点・お問い合わせは以下までお願い申し上げます

株式会社アイエスエフネット
首都圏営業本部　エンタープライズ営業 第二部
土井 広毅（doi.koki@isfnet.com）

Blue Planet-works
Safety for the Connected World