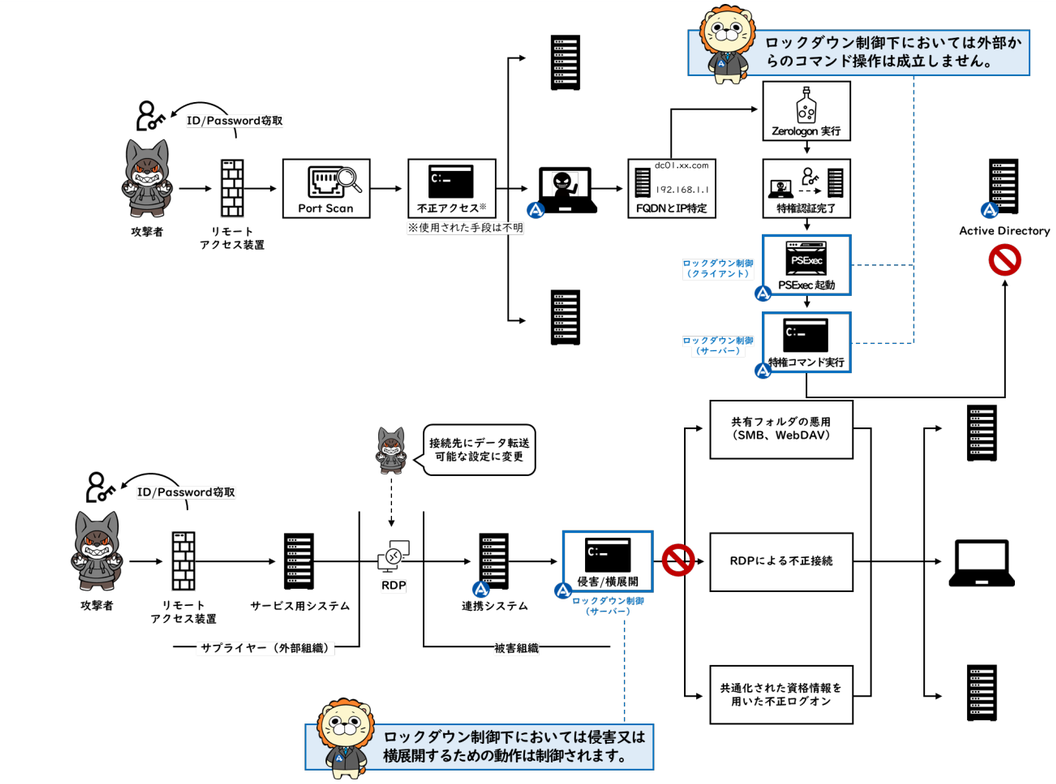
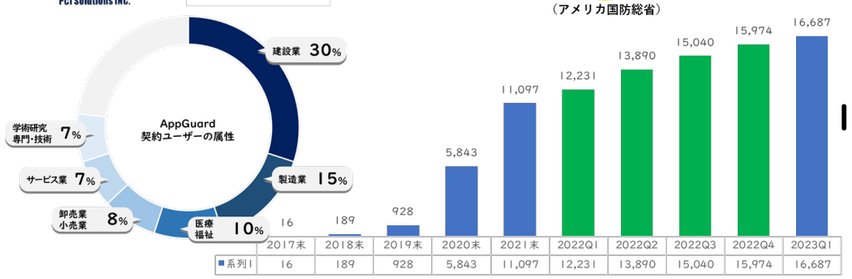
外部からの攻撃を受けても何も起きない【App Guardによるゼロトラスト化】



●App Guard 導入事例　※国内2万社以上が導入し、被害を受けた実績は１社も有りません

ANA / SMBC日興証券 / 埼玉医科大学病院 Saitama Medical University Hospital / 特定医療法人 佐藤会 弓削病院 / 戸田建設 / 人・街・未来をまもる 東洋テック / Fibergate Inc. 株式会社ファイバーゲート / KAKUDAI / UCHIDA / ecOHAI / 社会福祉法人 千葉市社会福祉協議会 / （白石市様） / dentsu / DAIKO / pci PCI Solutions INC. / NEC NECキャピタルソリューション / 吉本興業 / （アメリカ国防総省） / BANC OF CALIFORNIA / ColumbiaBank



国内導入累積社数
19,000社突破
（2024年3月末時点）

Cutting Edge!! カッティングエッジ!!

正規販売代理店 **カッティングエッジ株式会社**

〒101-0044 東京都千代田区鍛冶町1-9-6
TEL / FAX：03-6822-5613
https://cuttingedge-tech.jp/
sales@ctg-edge.jp

お問い合わせ先はこちら

●カタログの内容は予告無く変更する場合がありますので、ご了承願います。　●カタログの写真や色は印刷により若干異なる場合が有ります。　●このカタログの制作は2025年6月です。

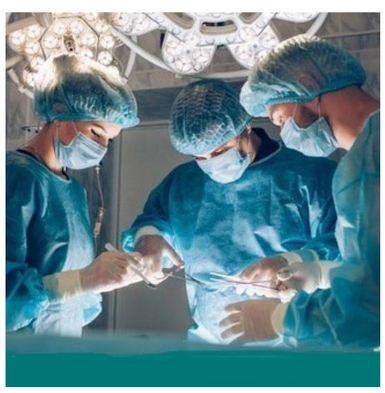
Blue Planet-works Safety for the Connected World

Cutting Edge!! カッティングエッジ!!

日本のハイテク技術、金融資産、公共インフラを守る最強の対策ソリューション
侵入され感染しても、許可しない行為を阻止
米国ペンタゴン向けに開発され、24年間１度も破られた事が無い

ゼロトラスト型エンドポイントセキュリティ
APPGUARD

1ライセンス年額わずか¥7,500(税別)、安心のサイバー保険付



Cutting Edge!! カッティングエッジ!!

米国国防総省(ペンタゴン)で使うために開発されたAPP GUARDは、国内約2万社を突破した、アメリカ生まれ日本育ちの、サイバーセキュリティ・ツールです。政府、公共インフラ、ハイテク企業、銀行、大学、病院等、多くの方が導入しています。

個人や中小企業はサイバー攻撃を受けないと考えていませんか？
ハッカー集団がマルウェア等で盗んだ情報を出品するマーケットプレースと言う商談の場があります。
2024年5月1日から1か月間に、日本人の情報が2,883人台出品されており、銀行情報、クレジットカードのID、パスワード、実名、写真、住所を含んだ様々な詳細な情報が販売されております。
その多くは、下記個人の端末から侵入した事が分かりました。
1. フェースブック　885台（31%）
2. DMM　748台（26%）
3. Discord　662台（23%）　※ゲーム用アプリ
4. インスタグラム　626台（22%）
5. アダルトサイト　422台（15%）
しかし、情報を盗まれた本人は何も気付いておりません。
サイバー攻撃者は、簡単に侵入出来る個人や中小企業のパソコンから攻撃を行い、感染と同時に大きな被害をもたらすランサムウェアや、マルウェアを送り、そこから勤務先のサーバーに侵入します。さらにサプライチェーン等の大手企業のサーバーに到達して、重要な資産を盗みます。つまり、個人や中小企業のパソコンが最も狙われ易いターゲットとなります。ウイルスソフトは、被害情報に基づいたウイルスだけを特定した検知方法を取っており、対策アップデートは約3週間掛かります。その間に攻撃者が常に先手を取るため、攻撃をくい止める事が出来ず、ウイルスソフトでは現実的に全く効果が有りません。

感染したらどうなる？
・端末、サーバーを乗っ取られ、機能不全となり、リモートコントロールされる
・感染した端末の持ち主の名前で、Word等添付メールを社内/社外/友人に配布し、周りの端末を全て感染させる
・パスワード、クレジットカード情報、銀行情報、個人情報、企業秘密情報、資産情報、技術情報等が盗まれ売却される
・情報を暗号化し、身代金を数日以内に支払う様要求される（最近の身代金平均額約16億円　※1千万ドル）
・データが改ざんされたり、破壊される
・PCのカメラとマイクから持ち主の顔、声をコピーし、本人になりすましたAI 画像やAI 音声を作り、政治、株操作、犯罪に使われる
・最近現れたInfo Stealerと言うマルウェアは、本人に盗まれた事を気付かれない様に情報を盗み販売する最も怖い攻撃です。

App Guardの大きな特長と機能

App Guardは侵入される事を前提として、侵入した攻撃者の行動の自由を奪い、目的を達成させない事が可能なツールです。
従来のウイルスソフトでは対応出来ない、未知のサイバー攻撃の対応が可能です。

1. マルウェア起動阻止機能
なりすましメールやランサムウェア等のマルウェアの起動を阻止、侵入されても発症させず、未知の脅威から端末を守ります。

2. 改ざん処理防止機能
悪用される可能性があるアプリに対して制御し不正アクセスをさせません。侵害されてもシステムへの改ざん行為を制御します。

3. プライベートフォルダ
個人情報や機密情報の格納されたフォルダを、サイバー攻撃からのアクセスを遮断し守ります。ランサムウェア対策に有効です。

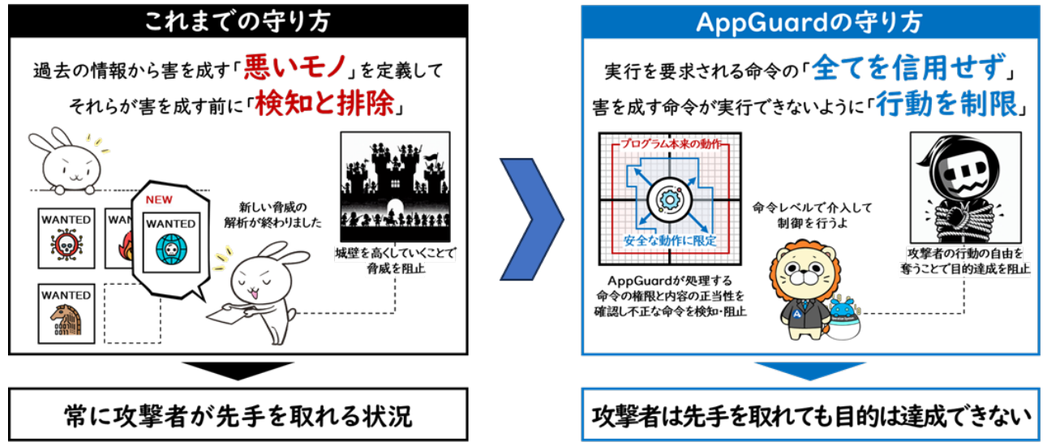
4. ファイル更新・アップデートが不要
従来のウイルスソフトとは異なり、ファイルの更新やAI/機械学習エンジンのアップデートは不要です。

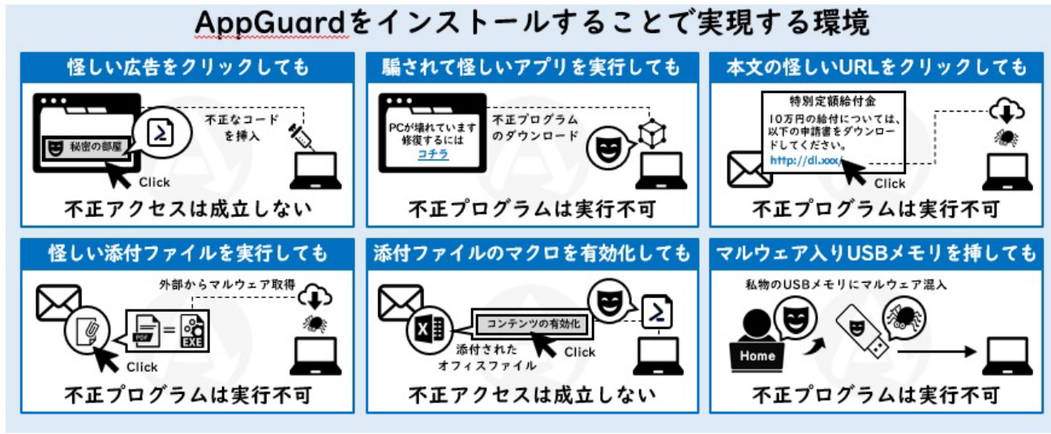
5. 運用管理の簡素化とコストダウン
1度インストールするだけで、継続的にシステムの安全性を維持し、EDR方式の様に専門知識は不要で、ウイルスソフトの経費・人的負荷軽減が可能です。

6. 現在使用中のセキュリティ製品との併用が可能
App Guardは、プラスアルファのセキュリティ対策として現在使用中のウイルスソフトと併用してお使い出来ます。

7. 1年間、1ライセンスわずか￥7,500（税別）、会社1社当たり最大1億円のサイバー保険も付いており、非常に安心です。

App Guardを短時間で理解する事が可能な動画を右QRコードから閲覧する事が出来ます





APPGUARDの主な特徴

- 未知のマルウェア実行防止
- ランサムウェア実行防止
- ドライブバイダウンロード実行防止
- ファイルレスマルウェア実行防止
- マルウェアによる機密情報漏洩の防止
- OS 改ざん防止

米国政府関連での導入実績

App Guardは、日本病院共済会推奨製品となりました

近年、医療機関を標的としたサイバー攻撃は増加の一途をたどり、攻撃手法の巧妙化も進んでいます。現実に病院がランサムウェアの被害により診療を長 期間停止した事例も多く発生しており、医療機関が一層強固なセキュリティ対策が求められています。
一方、ウイルスソフトやEDRでは防ぎきれない攻撃の発生や、セキュリティ対策業務の負荷増大などの課題も顕在化しています。
「AppGuard」は、2023年6月、日本病院共済会から、日本病院会会員病院をサイバー攻撃から守る最適な製品とのご評価を頂き業務提携を致しました。