## ●App Guard 導入事例　※国内2万2千社以上が導入し、過去1度も被害を受けた実績は有りません

航空：ANA
通信：DAIKO XTECH
旅行：JTB
医療：埼玉医科大学
建設：戸田建設
運送サービス：ecohai
製造：JFE / Pentel / KAKUDAI
証券業：SMBC日興証券
地方自治体：越前市 / （白石市様）
津山中央病院 / 柏澤病院 / 弓削病院 / 名寄市立総合病院
公益財団法人 日米医学医療交流財団
教育：日病学園
専門サービス：Deguchi
警備サービス：東洋テック
福祉サービス：千葉市社会福祉協議会
特殊団体：日本テニス協会
その他：アメリカ国防総省

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。「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。

### 組込みシステム用サイバー攻撃対応
### App Guard Industrial

**ある精密機器メーカー実例**
**課題**
1機器にサイバー対策機能追加の要望が増加
2ウイルスソフトのセキュリティが担保出来ない
**ウイルスソフトの課題**
1製品仕様において、自社開発プログラムを全て登録する導入プロセスに 障壁を感じる。また既に機器にマルウェアが潜伏している場合、そのプロセスもホワイトリスト(WL)化しリスク回避できない。
2WL型ではファイルレス攻撃から機器を守る事が出来ない
3ソフトウェア更新の際に個々に設定が必要で手間
**製品選考時の機能要求**
1CPU負荷が低く機器の生産性を劣化させない
2機器メーカーの定めるプロセス以外の動作を禁じる機能が有る
3機器内プログラム修正等に大きな影響を受けず高い運用性を有する
4未知・既知問わずマルウェアの攻撃を阻止可能
**実検証の結果、AppGuardが選ばれた理由**
1CPU負荷は非常に小さく生産能力に影響無し
2動作制限の機能要件を満たしている
3AppGuardの「自動継承機能 ※特許機能」が制御プログラム修正の影響を最小化できる
4防御機構上、非常に高い防御力と判断 ※実検体を使いペンテストを実施
5海外での組込み実績
App Guard Industrial導入開始済み、及び検証中の実例
精密機器メーカー、大手物流マテリアルハンドリングメーカー、大手機械製造会社、大手機械製造会社、大手食品原料加工メーカー、大手包装容器メーカー、
大手コンビニチェーン全店舗のPoS、Kiosk端末

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


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@cut-edge.jp

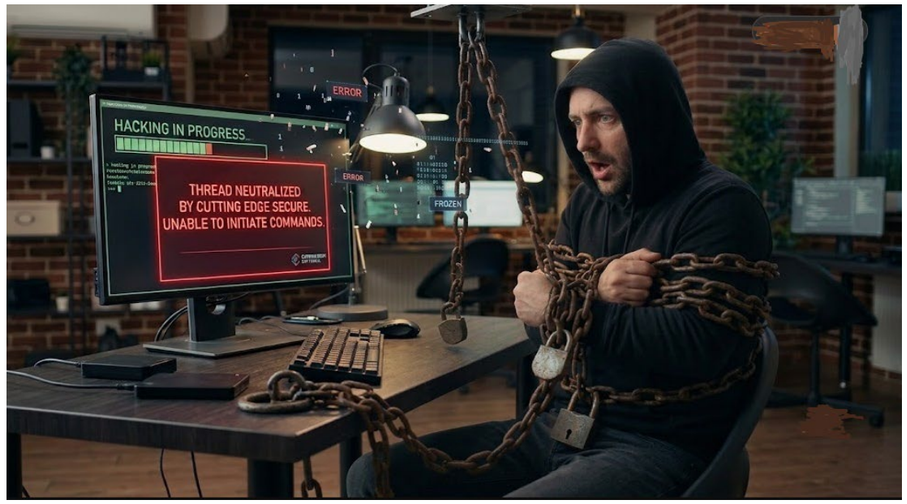

お問い合わせ先はこちら



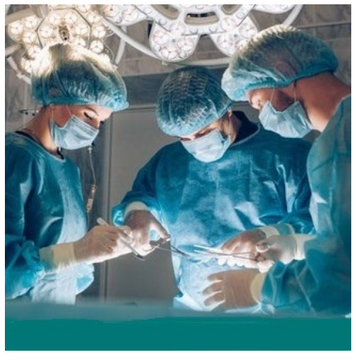
ゼロトラスト型エンドポイントセキュリティ APPGUARD

CUTTING EDGE

**侵入されても悪い事を何もさせない！**
**ウイルス感染したUSBを挿しても、怪しい添付ファイルを実行しても、**
**不正プログラムの実行は不可能！許可されたアプリケーションしか起動させない。**
**年間わずか6,000円、法人向7,200円！専門知識も専門担当者も不要！**
**米国政府、米国ペンタゴン、日本政府、防衛省等国内導入22,000社を突破！**
**26年間1度も破られた事の無いサイバー攻撃阻止ソリューション**



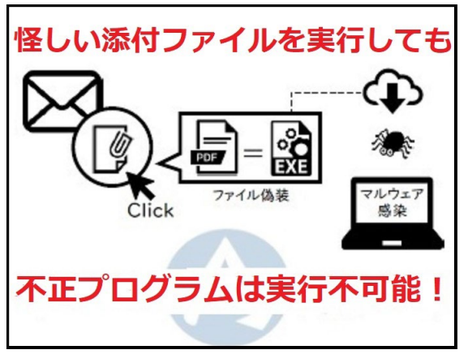


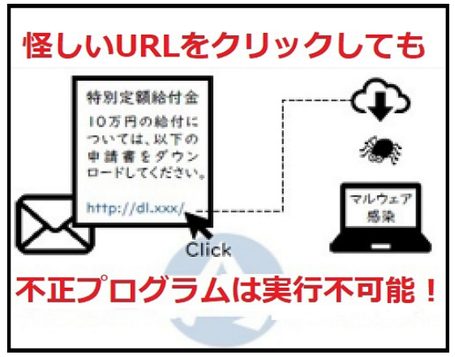


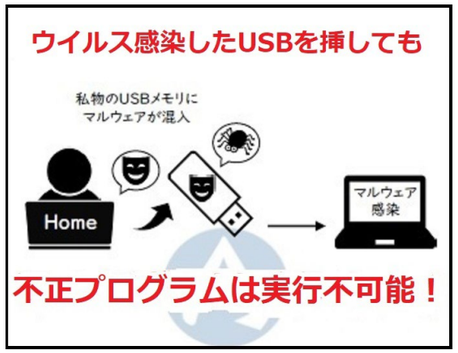
CUTTING EDGE

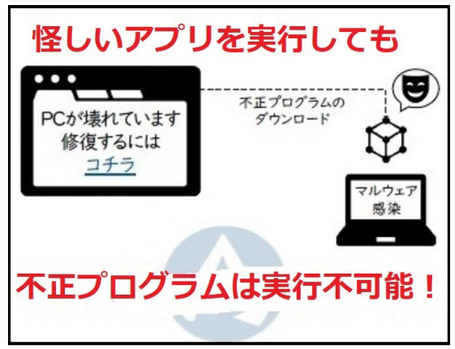
# 米国国防総省(ペンタゴン)で使うために開発されたAPP GUARDは、許可されたアプリケーションしか起動をさせない、究極のサイバー攻撃阻止ソリューション。政府、公共インフラ、ハイテク企業、銀行、大学、病院等国内2万2千社以上が導入！

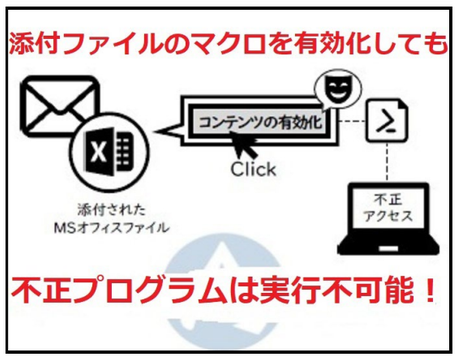
## App Guardの大きな特長

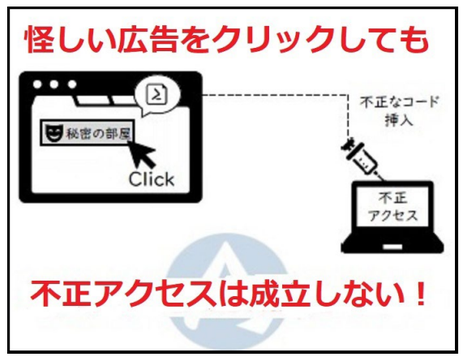



**1. マルウェア起動阻止機能**
なりすましメールやランサムウェア等の起動を阻止、侵入されても発症させず、未知の脅威から守ります。

**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。

**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**
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￥7,200（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。**

### フィッシング詐欺には対応しません

フィッシング詐欺とは、大手通販会社、宅配業者等のなりすましメールを送りつけ、貼り付けたリンクをクリックさせて偽のホームページに誘導し、クレジットカード番号やアカウント情報（ユーザID、パスワードなど）などの重要な情報を盗み出す詐欺のことです。フィッシング詐欺は、サイバー攻撃とは異なり、自らが重要情報を入力してしまうため、対策としては十分に注意をするしか有りません。

## App Guardとアンチウイルスソフトの大きな違い

| 製品 | App Guard | アンチウイルス |
|---|---|---|
| 目的 | 悪い事をさせない | 悪い奴を見つける |
| マルウェア検知 | × | ○ |
| マルウェア駆除 | × | ○ |
| マルウェア生成阻止 | ○ | × |
| マルウェア起動阻止 | ○ | × |
| 端末乗っ取り | ○ | △ |

アンチウイルスソフトは、被害情報に基づいたウイルスだけを特定して検知し駆除する方法を取っており、対策アップデートが配布される迄には約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未知の攻撃に対して効果が全く有りません。
一方**App Guardは、許可したアプリケーションだけしか起動させない究極の方法を取っており、侵入した攻撃者のアプリケーションは許可されていないためフリーズさせ、プログラムを起動させません。攻撃者の行動の自由を奪い、目的を達成させない理想的なツールです。新旧、種類、攻撃手法に関係無く、どの様なサイバー攻撃にも対応が可能です。**
Microsoft365に無料で付属の**ディフェンダー**が、時間とともに、ウイルスを検知され、駆除します。

## App GuardとEDRの大きな違い

| 製品 | App Guard | EDR |
|---|---|---|
| 目的 | **予防** | **事後対応** |
| 機能 | アプリケーションとプロセスのゼロトラスト化 | NIST SP800-171に基づく防御、検知、対処 |
| 手法 | **攻撃の成立を阻止** | **脅威の検知・相関関係整理** |
| 成果 | **「やって良い事」が実践されているかの検証** | **侵害中又は侵害された痕跡とデータの照合** |
| 機能のタイミング | **攻撃実行前** | **攻撃実行後** |
| コスト | **安い (¥5,500～¥7,200 / 年)** | **非常に高い(人件費+諸経費)** |
| 未知の脅威、環境寄生型攻撃、未知の脆弱性 | **App Guardは、マルウェアの発症、不正アクセスに因る侵害を成立出来ない状態にするため、脅威の新旧や種類、攻撃手法に依存しない** | **EDRの特性上、新しい脅威や攻撃にたいしては新しい検知モデルが必要であり、最終的には利用者側の対処スキルに大きく依存する** |

EDRは、攻撃を受けた時の防御、検知、対処を行うツールで、専門教育を受けた担当者数人を24時間体制で監視させる必要が有ります。そのため、人件費、スキルアップのための教育コスト等非常に大きな経費が掛かります。また、攻撃を受けた際の防御方法、対処方法等が担当者のスキルや判断に因るため、相関関係整理が重要となります。
一方、**App Guardは、パソコンやサーバーにアプリケーションをインストールするだけで、専門知識も専門担当者も不要です。許可したアプリケーションしか開く事が出来ないため、マルウェア等はフリーズした様な状態となり、起動する事が出来ません。そのため、気づかないうちに、裏側ではApp Guardがサイバー攻撃をストップさせて守ってくれています。**