



もう、セキュリティで悩まない。

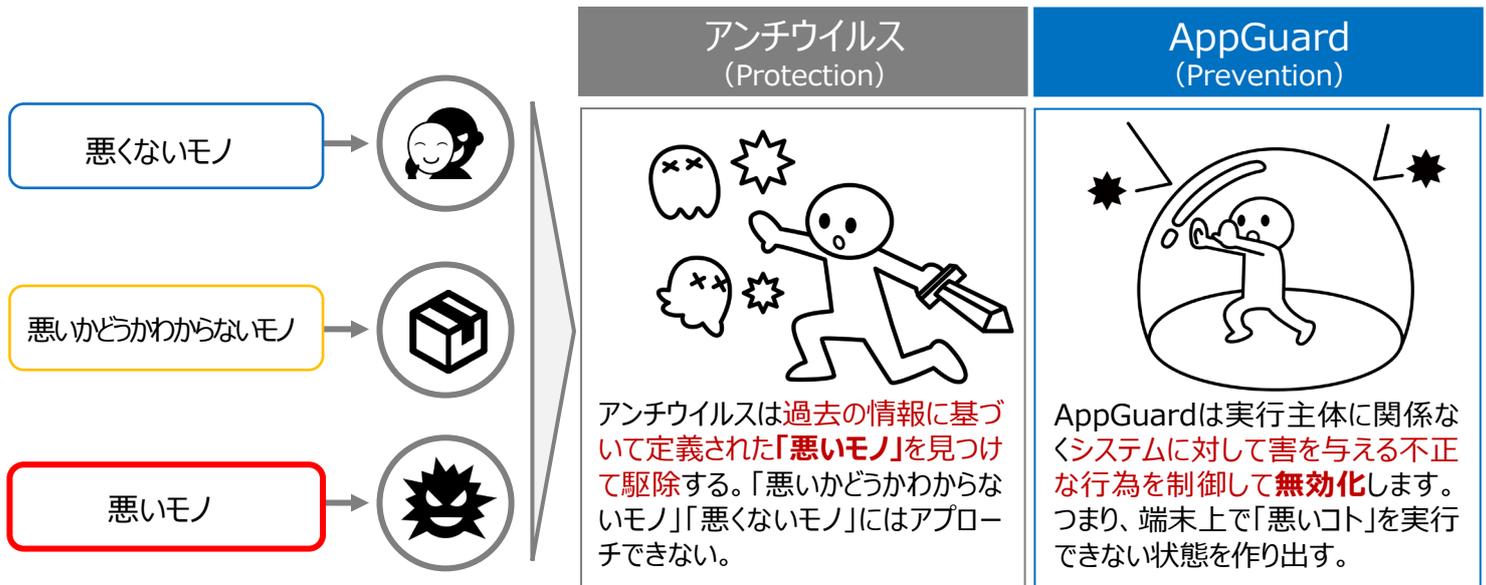
# APPGUARD のご紹介

# AISEL

## 「マルウェアフリー」の登場でアンチウイルスだけでは対処できない時代へ

マルウェアフリーとは「**アンチウイルスでは防御することが難しい攻撃方法の総称**」で、2019年時点で既に攻撃全体の51%を占めている、近年最もよく使われる攻撃手法です。  
 このマルウェアフリーの代表的な攻撃方法に「**環境寄生型攻撃**」があり、**アンチウイルスにとって安全だと認識**している機能やサービスを悪用して攻撃を発動させます。  
 例えば、MS Officeのマクロ機能やWindows標準ツールのコマンドプロンプト、PowerShellなど、アンチウイルスはこれらの動作を邪魔しないように設計されているため、悪用されるとアンチウイルスでは対処することができません。  
 また、マルウェアフリーが問題視されるようになったきっかけが、**2020年に猛威を奮った「Emotet」の登場**です。日々数十万種とも言われる新種の中でも極めて異例の感染力を誇った背景にはマルウェアフリーを用いていたことが要因として挙げられます。

## 侵入されてもインシデント化させないのが「AppGuard」

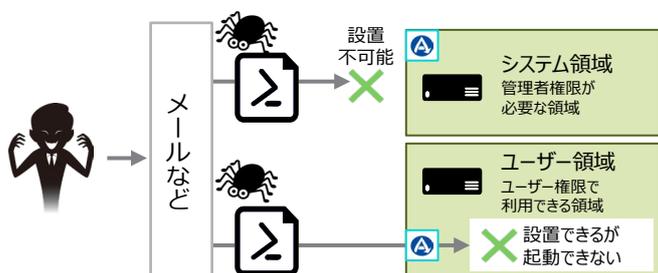


## AppGuard による「不正行為の無効化」の仕組み

### ● 2つの制御で悪意のある行為は絶対に発動できない

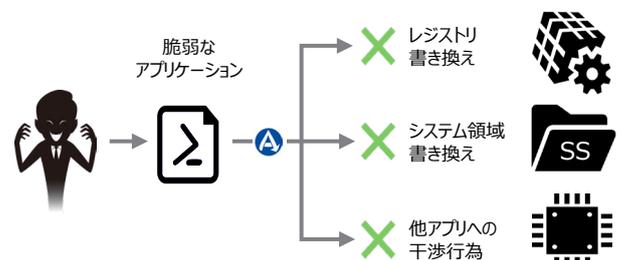
#### ① 起動制御

HDD内を2つの領域に分類し、システム領域には、外部からアプリケーションを通じて攻撃者がファイルを設置することができず、ユーザー領域には、設置できても信頼されていない実行ファイルやスクリプトは起動することができません。



#### ② 改ざん処理の防止

攻撃に悪用されるリスクのあるアプリケーションを通じて、不正なアクセスを成立させるために必要な改ざん行為（レジストリの改ざん、システム領域の改ざん、他アプリケーションのメモリへ干渉）を防止、端末の乗っ取りに必要な侵害行為を成立させません。



## AppGuardで実現する確実に安心できる環境

### ●ユーザーの「うっかり」があっても確実に守られる

AppGuardがあれば、ユーザーが誤った操作をしても問題なし！！

|   |   |  |
|---|---|--|
| <p><b>怪しい広告をクリックしても</b><br/>不正なコードを挿入</p> <p>不正アクセスは成立しない</p>     | <p><b>騙されて怪しいアプリを実行しても</b><br/>不正プログラムのダウンロード</p> <p>不正プログラムは実行不可</p> | <p><b>本文の怪しいURLをクリックしても</b></p> <p>不正プログラムは実行不可</p>                          |
| <p><b>怪しい添付ファイルを実行しても</b><br/>外部からマルウェア取得</p> <p>不正プログラムは実行不可</p> | <p><b>添付ファイルのマクロを有効化しても</b><br/>添付されたオフィスファイル</p> <p>不正アクセスは成立しない</p> | <p><b>マルウェア入りUSBメモリーを挿しても</b><br/>私物のUSBメモリーにマルウェア混入</p> <p>不正プログラムは実行不可</p> |

## さらに「Final Code」との組み合わせで強固な情報漏えい対策も実現

### ●改正個人情報保護法は 2022年4月より施行されました。

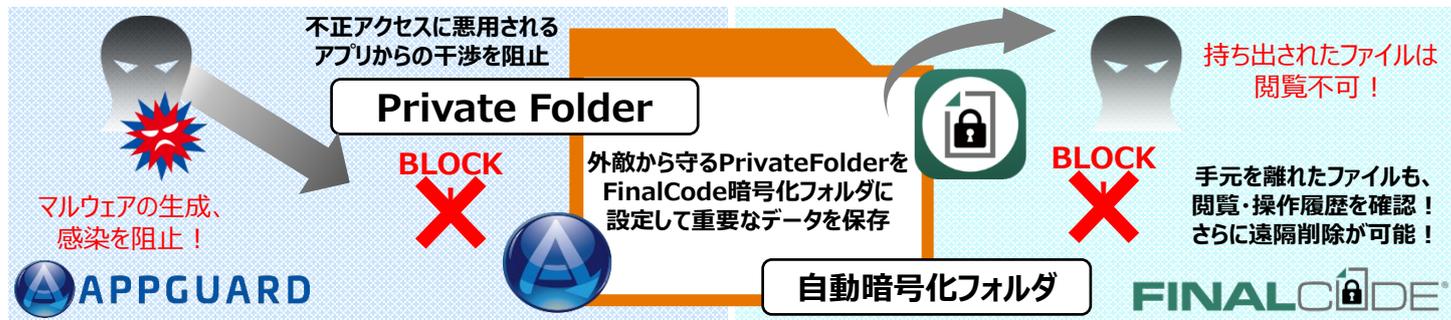
・かんたん操作で、確実なIRMを実現する「FinalCode」

FINALCODE

フォルダへファイルを保存するだけで情報漏洩リスク低減が可能。

業務フローの見直し・変更は不要です。  
重要情報を補完するフォルダを自動暗号化設定するだけ。

- ・開封者指定
  - ・印刷/編集などの操作制限
  - ・閲覧期間
- などが設定された暗号化されたファイルが完成します。



AppGuard と FinalCode の組み合わせ導入はアイセルにお任せください！

## お問合せ

株式会社 アイセル

〒110-0005 東京都台東区上野3-24-6  
上野フロンティアタワー12F

03-5652-5236 (AppGuard担当まで)

[appguard-sales@aisel.ne.jp](mailto:appguard-sales@aisel.ne.jp)

<https://appguard.aisel.ne.jp/>