Blue Planet-works
Safety for the Connected World

本資料の記載内容は、2018年7月25日にNISCウェブサイトに掲載された「政府機関等の対策基準策定のためのガイドライン（平成30 年度版）」を参照の上作成しています。

Source: https://www.nisc.go.jp/active/general/pdf/guide30.pdf

当ガイドラインは「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」に準拠して、府省庁対策基準を策定する際に参照可能な基本対策事項を定めたものです。併せて、府省庁対策基準の策定手順や統一基準の遵守事項を満たすために採られるべき基本的な対策事項の例示、考え方等を解説するものです。

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

政府機関等の対策基準策定のためのガイドライン
平成30年度版

遵守事項：不正プログラム対策の実施

基本対策事項：既知及び**未知の不正プログラム**の検知及びその**実行の防止の機能**を有するソフトウェアの導入。

要約：既知の不正プログラムについては…一方で、**(A)未知の脅威への対策**… **シグネチャにより検知する方式以外**の手法を用いる製品やサービスを導入… 例えば、**(B)シグネチャに依存せず**にOSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、**不正プログラムの実行を防止**するとともに、これを**隔離する方式**があり、攻撃にスクリプト等を使用する**ファイルレスマルウェアの対策としても効果**が期待できる。なお、不正プログラム対策ソフトウェア等の選定に当たっては、ソフトウェアの稼働によって端末及びサーバ装置への**(C)負荷が増加し**、業務に影響を与えるおそれがあること等も勘案した上で判断する必要がある。

Source: https://www.nisc.go.jp/active/general/pdf/guide30.pdf

対する APPGUARD の特徴は？

「軽量」でシステムを防御する、「新概念」。
Isolation Technology
（アイソレーション： 隔離技術） 特許取得済 (US Patent# 7,712,143)

(A) 未知の脅威への対策
- 不正な動作を未然に阻止
- ファイルレスマルウエア、In Memory攻撃、ランサムウエア、最新の攻撃から守る

(B) シグネチャに依存しない
- シグネチャーファイル不要（依存しない）
- 特許の隔離技術: Isolation Technology
- OSのプロセスやメモリ、レジストリへの不正アクセスを監視

(C) 端末への負荷の軽減
- 軽量、軽快（エンジンは1MB以下）
- アップデート不要
- スキャン不要：システム負荷を軽減

NISCガイドライン準拠製品

NISCとは:

National center of Incident readiness and Strategy for Cybersecurity

- 情報システムに対する不正活動の監視・分析
- 重大事象の原因究明調査
- 行政各部に対する監査等
- **サイバーセキュリティに関する企画・立案、総合調整**

定義

・政府機関等の対策基準策定のためのガイドライン（以下「本ガイドライン」という。）は、国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）が政府機関等の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」とう。）の規定を遵守するための対策事項について、対策基準を策定する際に参照するものであり、統一基準の遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）を例示するとともに、対策基準の策定及び実施に際しての考え方等を解説するものである。これにより、機関等が、統一基準を遵守するための対策事項として、本ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて対策基準を定められるようにすることを目的とする。

・「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。