FUJITSU

組み込み機器向けホワイトリスト型セキュリティ製品 「WhiteSec」Windows版

ウイルス定義ファイル不要のマルウェア対策

組み込み機器向けホワイトリスト型セキュリティ製品「WhiteSec」は、従来のマルウェア対策製品のように、ウイルス定義ファイルを使用しないため、ウイルス定義ファイルの更新が困難な組み込み機器や閉域網でのマルウェア対策に最適です。

ホワイトリストによるプログラム実行制御

あらかじめ定義したホワイトリストに登録されたプログラムのみ、実行を許可することが可能です。

特定のプログラムの実行を禁止する、ブラックリスト方式と異なり、ウイルス定義ファイルの更新が不要です。

新種のマルウェアが侵入した場合でも、侵入したマルウェアはホワイトリストに登録されていないため、実行できません。

USBメモリなどのデバイス制御

デバイス制御機能は、USBメモリからのマルウェア感染を防止することが可能です。

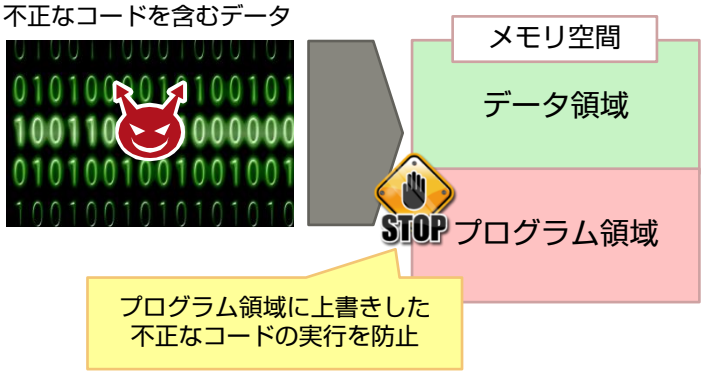
データ持ち出しを禁止するために、USBメモリの読み込みは許可するが、書き込みは禁止するという使い方も可能です。

メモリ保護による不正なコード実行の防止

メモリ保護機能は、バッファオーバーフローの脆弱性を利用した不正なコードの実行を防止することが可能です。

WhiteSecは、プログラム実行時にメモリ領域の整合性をチェックして、攻撃を防止します。

この機能により、ホワイトリストに登録されている正規のプログラムに脆弱性が発見された場合のリスクを低減できます。



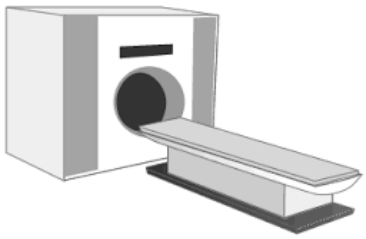
導入対象機器例

WhiteSecを導入可能な機器の例としては、以下のような機器があります。
以下に記載のない機器でも、Windows Embedded OSを使用していれば、本製品を導入することが可能です。

POS端末

ATM

KIOSK端末



医療機器

動作環境

WhiteSec Windows版のソフトウェアは、以下の環境にインストールして利用できます。

OS	Windows XP Embedded (32bit, 64bit) Windows Embedded 2009 (32bit, 64bit) Windows Embedded 7 (32bit, 64bit) Windows 7 Professional (32bit) Windows 10 IoT Enterprise (32bit, 64bit) ※上記に記載のないOSについては、個別にお問い合わせください。
CPU	x86, x64アーキテクチャ
RAM	25MB以上の空き容量
HDD/SSD/ROM	20MB以上の空き容量

※Linux OSの動作環境は、WhiteSec Linux版のパンフレットをご確認ください。

※記載の会社名、商品名は、各社の商標または登録商標です。
※記載された情報は、予告なく変更することがあります。
※記載の内容は、2018年11月現在のものです。

お問い合わせ先
株式会社富士通ソーシアルサイエンスラボラトリ(富士通SSL)
お問い合わせ総合窓口
〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
E-mail : ssl-info@cs.jp.fujitsu.com
当社ホームページ　http://www.fujitsu.com/jp/group/ssl/