FUJITSU

ランサムウェア対策製品「WhiteSec」
～パッチを適用できない組み込み機器を保護～

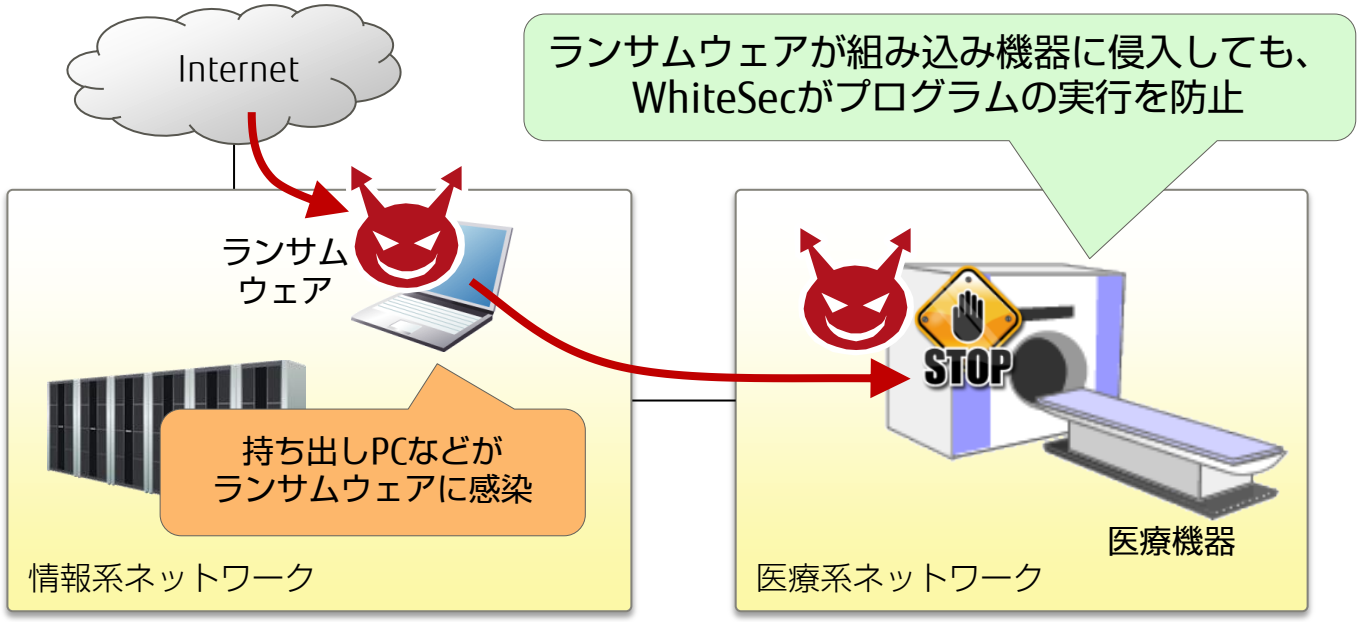
最近のランサムウェアは、OSの脆弱性を利用して感染します。（例：WannaCry）
組み込み機器の多くは、製品出荷時点のOSパッチのみ適用されており、新しい脆弱性に対応できません。そのような機器でも、ホワイトリスト型セキュリティ製品「WhiteSec」を導入することで、ランサムウェアの感染から保護できます。

組み込み機器におけるランサムウェア感染の影響

影響1	画面ロック、機能停止、ファイル暗号化による業務停止
影響2	ファイル暗号化によるデータロスト（または身代金要求による金銭支払い）
影響3	ランサムウェア感染による企業イメージの低下

組み込み機器に「WhiteSec」を導入することで
ランサムウェア感染の脅威から保護できます！

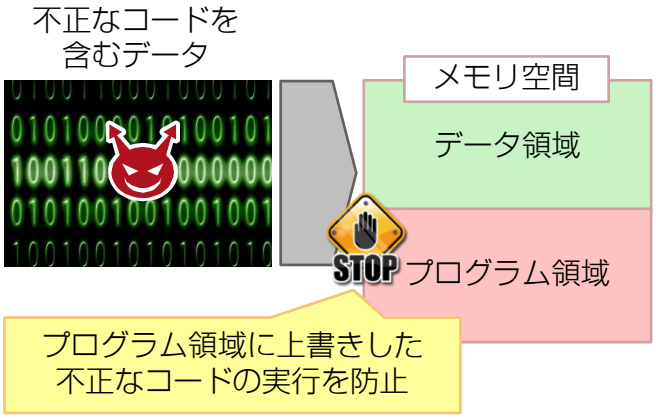
ランサムウェア感染防止のイメージ（例）



WhiteSecの機能

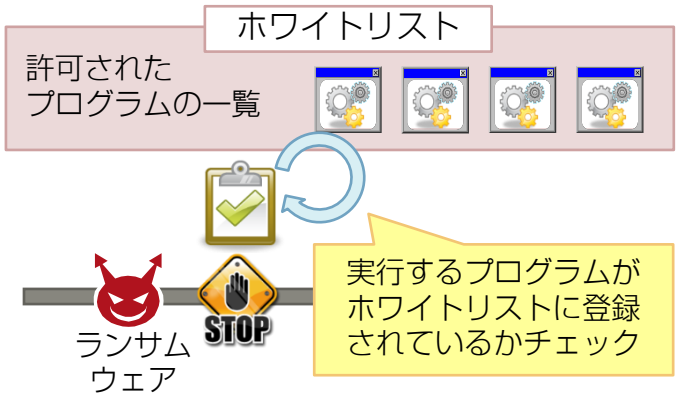
メモリ保護機能により 脆弱性を利用したコード実行を防止

バッファオーバーフローなど、脆弱性を利用したコードの実行を防止することが可能です。
組み込み機器は、運用中にパッチを適用することが困難なため、OSのプログラムに脆弱性が存在する場合があります。
メモリ保護機能では、プログラム実行時に、メモリ領域をチェックして、脆弱性を利用したランサムウェアの感染を防止します。



ホワイトリスト機能により 未許可のプログラム実行を防止

脆弱性を利用しない方法で、ランサムウェアが侵入した場合でも、あらかじめ許可したホワイトリストに登録されていないプログラムの実行を防止することが可能です。
パターンマッチングでウイルスの実行を防止するブラックリスト型と異なり、本製品はウイルス定義ファイルの更新が不要です。
そのため、新種/亜種のランサムウェアの対策が可能です。



動作環境

	Windows版エージェント	Linux版エージェント
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。	組み込みLinux ※お客様機器に合わせたポーティングを実施して提供
CPU	x86, x64アーキテクチャ	x86, x64, ARMアーキテクチャ
RAM	25MB以上の空き容量	2MB以上の空き容量
HDD/SSD/ROM	20MB以上の空き容量	2MB以上の空き容量

※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/