組込み機器向けホワイトリスト型マルウェア対策ソフトウェア「SecNucleus WhiteEgret」

当社はこのほど、組込み機器向けマルウェア対策ソフトウェア「SecNucleus WhiteEgret」を商品化しました。軽量なモジュール構成と高速動作を可能にしたホワイトリスト型のソフトウェアで、組込み機器をマルウェアから保護します。今後はポーティング、保守を含め、お客様の製品開発をワンストップで支援できるよう、幅広いIoT機器へ向けた拡販を進めていきます。

組込み機器のマルウェア対策が不可欠の時代に

IoT時代を迎え、あらゆるデバイスや機器がネットワークに繋がるようになりました。ウイルスやワームといったマルウェアによる被害は、これまでのPCやサーバーなどから組込み機器にも及んでいます。オフィス機器、ネットワークカメラをはじめとした産業機器はもちろん、自動車のECUや社会インフラ設備など、改ざんなどによる誤動作や停止が決して許されない組込み機器も数多く、今後の万全なマルウェア対策が不可欠となってきます。

こうした時代に対応すべく、当社は、「SecNucleus WhiteEgret」をこのほど提供開始しました。本製品は、組込み機器向けに特化した、非常に軽量で高速なLinux向けホワイトリスト型マルウェア対策ソフトウェアで、㈱東芝の研究開発センターの基礎技術をベースに商品化したものです。

マルウェア対策については、PC用にはさまざまなツールが市販されていますが、その多くは、従来型のセキュリティ手法であるブラックリスト型で、定期的に更新されるマルウェア定義ファイルやパターンファイルを用いてマルウェアを検知します。一方、ホワイトリスト型は、まったく逆の発想で、動作を許諾するプログラムの一覧を内部に持たせ、一覧にないプログラムは一切実行できないという仕組みで高速処理が可能です。組込み機器の中に不正な実行ファイルを保存して実行させようとするマルウェアがあっても、ホワイトリストで定義されていない限り動作することはできません(**図-1**)。

当社のSecNucleus WhiteEgretは、ホワイトリストの中に実行ファイルのハッシュ値も記録されています。このため、万一、既存の実行ファイルを別のものに置換するマルウェアがあった場合でも、置き換えられたことが分かるため、偽物を動作させない仕組みとなっています。

組込み機器に最適なホワイトリスト方式

PC向けのブラックリスト型のマルウェア対策ソフトウェアでは、新しい脅威に対応するためには、頻繁にパターンファイルを更新する必要があります。組込み機器は、常にパターンファイルを更新できる環境にあるとは限りません。また、ライフサイクルが長い組込み機器においては、パターンファイルの肥大化が進む恐れがあり、ブラックリスト型のマルウェア対策ソフトウェアは、組込み機器への適用が難しい場合があります。

それでは、ホワイトリスト方式が組込み機器のマルウェア対策に適しているのでしょうか。一般的に、組込み機器は機能が限定されているため、機器の動作に必要なプログラムが容易にリストアップできます。プログラムの追加搭載や機能更新も、PCと比べるとはるかに少ないため、出荷時に作成したホワイトリストが長期に渡って使用でき、保守の手間も軽減できます。未知のマルウェアに対してもホワイトリスト型なら容易に実行制御をかけることができます。

また、ホワイトリスト型のマルウェア対策では、機器のファームウェアの更新などの対応を懸念されるかもしれませんが、こちらも、ファームウェアの更新と同時にホワイトリストを更新することによって対応が可能

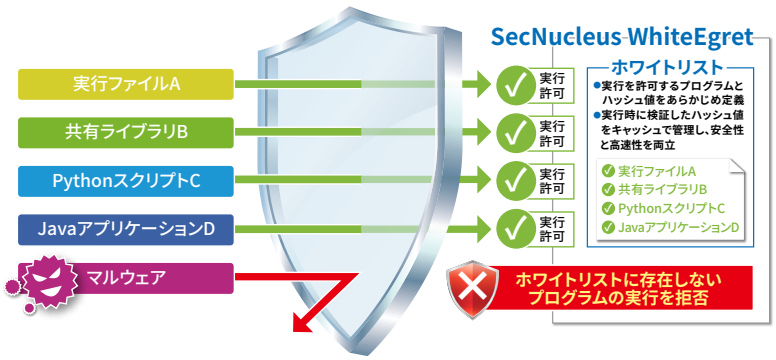

図-1　ホワイトリスト型マルウェア対策のイメージ

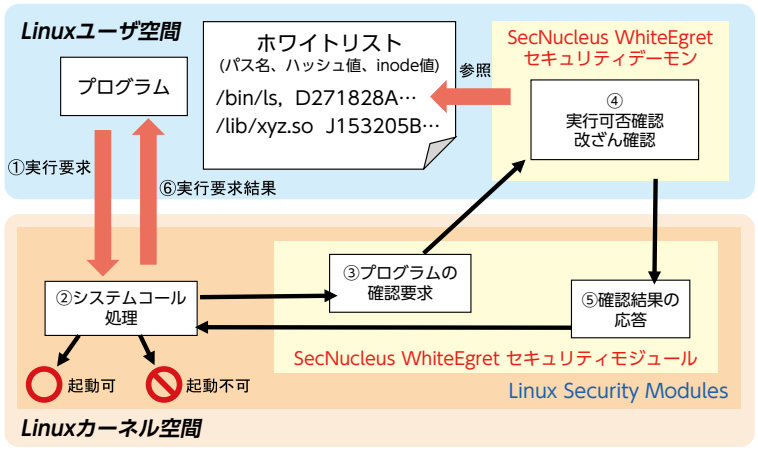

図-2　「SecNucleus WhiteEgret」の動作概要

となります。SecNucleus WhiteEgretには更新機能を搭載したアプリケーションが付属されていますので、それを使用すれば、ホワイトリストの更新が可能です。ただし、セキュリティ上、運用管理者以外がホワイトリストを更新することは望ましくありません。運用管理者の負荷を軽減する方法として、プリンタなどの場合は、保守要員にホワイトリストの更新も一任する、あるいはファームウェア配布時にホワイトリストも配布するといった工夫も考えられます。

SecNucleus WhiteEgretのシステム構成は**図-2**のとおりで、Linuxユーザ空間とLinuxカーネル空間からなり、軽量なモジュール構成となっています。アプリケーション実行時は、Linuxはカーネルに命令を送ります。現在のLinuxは、カーネル内にLinux Security Modulesという仕組みを持っており、ここで登録されたモジュールが呼び出されます。SecNucleus WhiteEgretを導入した組込み機器では、SecNucleus WhiteEgretセキュリティモジュールが登録されています。このセキュリティモジュールにより、確認要求がユーザ空間のセキュリティデーモンに送られ、セキュリティデーモン側でホワイトリストを確認し、結果をカーネル側のセキュリティモジュールに送り返すことで実行可否が決定されます。これにより、ホワイトリストにないプログラムは一切動作することができません。

SecNucleus WhiteEgretは、ホワイトリストによる実行制御、改ざん検知による実行制御といったマルウェア対策基本機能のほか、ホワイトリストの追加・削除・反映・一覧表示の機能を搭載しています。

ホワイトリストに登録可能なファイルは、実行ファイル、共有ライブラリ、スクリプト、Javaアプリケーションで、さらに、スクリプト言語にも対応しているのも大きな特徴です。例えば、Perl言語であれば実行ファイルはPerlになりますが、従来のホワイトリスト型製品ではPerlのスクリプトに不正動作させるものを仕込まれれば、Perl自体を許可してしまうため、実行されてしまいます。本製品はPerl上で動作するスクリプトの実行制御が可能なので、そうしたリスクも防止することができます。

お客様のセキュアな機器開発をトータルで支援

このように、SecNucleus WhiteEgretは、組込み機器の特性を十分考慮し、基本機能に絞ったことで、軽量なモジュール構成と高速な動作を実現しています。また、他社製品にはない独自機能も搭載しています**(表-1)**。

その1つが、高速化機能です。本製品にはセキュリティ向上のため、ハッシュ値の確認機能を搭載していますが、初回のアプリケーション起動時にハッシュ値検証を行った結果をキャッシュし、同じアプリケーションの2回目以降の起動時の検証処理を省略するものです。これにより、当該ファイルがアップデートされない限り、2回目の起動を即時実行できるようになります。さらに、システム起動時に登録されたアプリケーションのハッシュ値検証を予め行いキャッシュに保存する機能も搭載し、アプリケーションの初回起動の遅延抑制も実現しています。

SecNucleus WhiteEgretの適用領域は広いと考えています。MFP(プリンタ複合機)をはじめとしたオフィス機器、FA機器、ネットワーク機器など、制御系でLinuxを活用している組込み機器の市場に対し、積極的に拡販を進めていきます。また、製品の提供のみならず、保守、移植やカスタマイズなどエンジニアリングサービスの提供も含め、お客様の製品開発を支援していきます。

(エンベデッドシステム事業部　関根 正騎)

表-1　他社製品との機能比較

機　能		概　要	SecNucleus WhiteEgret	A社製品	B社製品
アプリ実行制御機能	バイナリ実行ファイル	未登録の実行ファイル/共有ライブラリの実行拒否	○	○	○
	Javaプログラム	未登録のクラスファイルのJava VM 実行拒否	○	○	○
	スクリプトファイル制御(Perl, Pythonなど)	未登録のスクリプトファイルの実行拒否	○	△ 拡張子による検証のみ	△ 拡張子による検証のみ
	ハッシュやチェックサムによる完全性検証	実行時にハッシュやチェックサムを確認してアプリファイルの完全性を検証	○	○	× ファイル入出力監視のみ
高速化(起動時バッチ検証)機能		端末起動時に事前にハッシュ検証を行うことで起動時の遅延を最小化	○	×	ハッシュ検証機能なし
ホワイトリスト無停止更新機能		アプリケーションやホワイトリスト制御を止めることなくホワイトリストをセキュアに更新	○	○	○
マルチプラットフォーム対応		ARM等のCPUへの対応	○	×	○
OS対応		Linuxだけでなく Windows OSなどへの対応	×	○	○