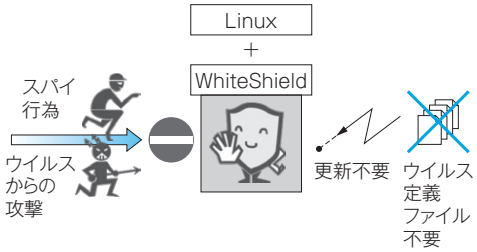
Linux向けホワイトリストセキュリティソフトウェア

鈴木　実 Minoru Suzuki
大竹康弘 Yasuhiro Otake

キーワード　セキュリティ，ホワイトリスト，ウイルス対策

概　要



Linux向けホワイトリストセキュリティソフトウェア

コンピュータシステムにおけるセキュリティが問題となり始めて20年以上が経過している。

当社では，WindowsをセキュアOS（security-focused Operating System）化するWhiteShieldを10年以上前にリリースし，現在も保守と利用を継続している。WhiteShieldでは，ホワイトリスト方式というあらかじめ許可された動作を定義する方式を採用し，未知のセキュリティ脅威にも対応可能としている。

セキュリティへの重要度が増す中，Linuxでもホワイトリスト方式を採用し，LinuxのセキュアOS化に対応した。

当社のコンピュータ製品は，制御・監視を行う組み込み製品である。セキュリティパッチなどによるソフトウェアの変更が不要で，中央演算処理装置（CPU）への負荷が少ないホワイトリスト方式が適している。

1　まえがき

2010年頃までにLinuxのフリーソフトウェアコミュニティによって，LinuxをセキュアOS（security-focused Operating System）(注1) 化する機能が開発された。

そのため基本的な機能は，Linux内にセキュアOSモジュールとして標準的に組み込まれている。しかし，実際に運用を行うために必要なホワイトリストはあらかじめ用意されていない。なぜならば，Linuxの下で動作する全てのソフトウェアに対して適切な許可を与える必要があり，用途に応じた対応が必要なためである。

今回，当社製品の運用に即したホワイトリストを構築し，製品化した。**本稿では，ホワイトリスト及びその方式を紹介する。**

2　対応するセキュリティ

コンピュータのセキュリティ対策と言っても幅広い意味を表す。対象は，コンピュータウイルスなどの「悪意のあるソフトウェア」への対応である。コンピュータの利用者に対して不利益をもたらす「悪意のあるソフトウェア」は細かく分類され多くの呼び名があるが，ここでは総称してウイルスとして表記する。

また，コンピュータのセキュリティに関連して「ぜい弱性」という言葉がある。これはコンピュータのソフトウェアで，ウイルスを送り込み，動作させてしまう隙間があることを意味する。

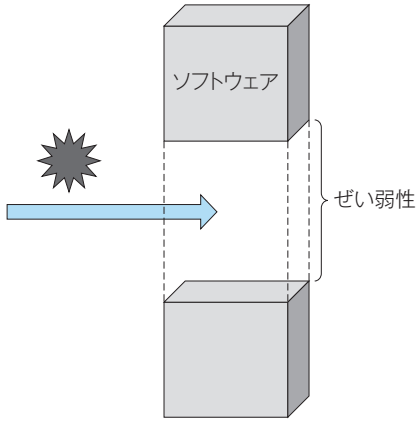
2.1　ぜい弱性と悪意のあるソフトウェア

ウイルスが送り込まれ動作するまでは，一例として以下のような流れとなる。

(1) ぜい弱性を利用してウイルスの本体を送り込む「踏み台」が作成される。**第 1 図**にぜい弱性の利用を示す。
(2)「踏み台」を利用して，ウイルスの本体とウイルスを自動で実行する仕掛けが作成される。ウイルスの本体とは，ディスク上の実行ファイルである。また自動実行する仕掛けは存在するファイルの内容の改ざんによって作成される。**第 2 図**に踏み台の利用を示す。
(3) 自動実行の仕掛けによってウイルスが実行され，悪意のある行為が行われる。**第 3 図**にウイルスの動作を示す。

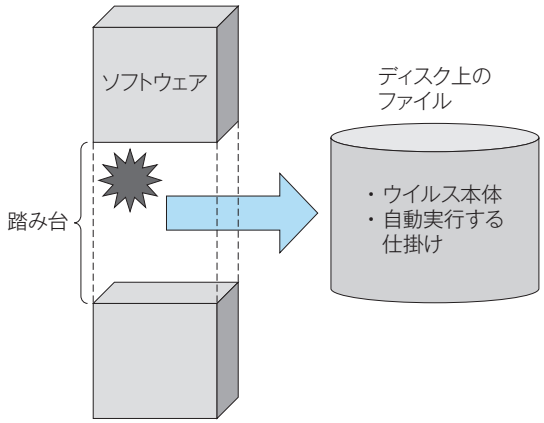
2.2 ホワイトリスト方式

特定のソフトウェアでは，ウイルスの実行ファイルを作成する動作，存在するファイルを改ざんする動作は通常は行われない。そこで，通常の動作を「ホワイトリスト」として登録し，「ホワイトリスト」に存在しない動作を遮断するようにしたものがホワイトリスト方式である。**第 4 図**にホワイトリストの概要を，**第 1 表**にホワイトリスト方式と通常のセキュリティソフトに採用されているブラックリス



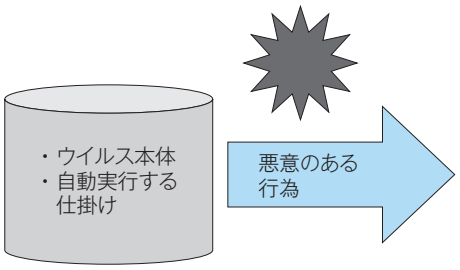
第 1 図　ぜい弱性の利用

ぜい弱性を利用してウイルスを送り込む「踏み台」が作成される。



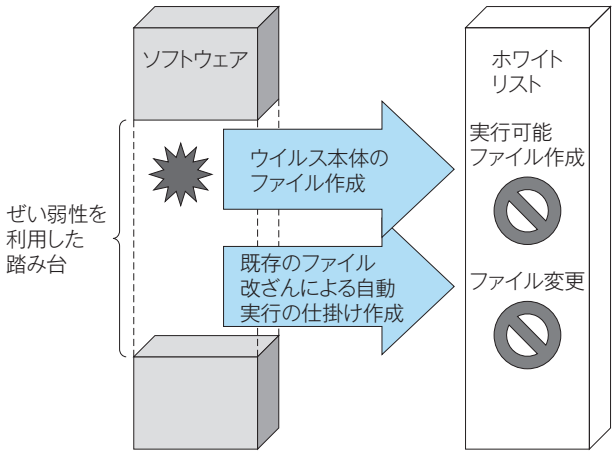
第 2 図　踏み台の利用

踏み台を利用してウイルスの本体が送り込まれる。



第 3 図　ウイルスの動作

自動実行の仕掛けによってウイルスが実行される。



第 4 図　ホワイトリスト概要

ホワイトリストに登録されていない動作を遮断する。

第 1 表　ホワイトリスト方式とブラックリスト方式の比較

ホワイトリスト方式とブラックリスト方式の特徴を示す。

項目	ホワイトリスト方式	ブラックリスト方式
リストの更新	不要	必要
未知の脅威への対応	可能	不可能
CPU負荷	軽微な負荷	ブラックリスト照合操作時に，制御・監視処理に負担になる負荷
リストの作成	自分で作成する必要がある（自動作成機能有り）	セキュリティソフトウェアベンダーから配布される

第２表　TOMOYO Linux と SELinux の比較

TOMOYO Linux と SELinux の特徴を示す。

項目	TOMOYO Linux	SELinux
Linux ディストリビューションでの採用	無し	Red Hat Enterprise Linux など
ホワイトリスト（ポリシー）に対する方針	自動学習によって生成カスタマイズも可能	ディストリビューション向けのリファレンスポリシーを提供
ホワイトリスト（ポリシー）に対する一般的な見解	セキュリティの専門家でなくても扱うことができるように仕様を策定	セキュリティの専門家でないと扱いが困難
組み込み Linux 対応	自動学習は組み込み系 Linux でも同様に可能	リファレンスポリシーが提供されていないため，対応が困難
ファイルシステム対応	ファイルシステムに依存しない	特定のファイルシステムに依存する機能がある

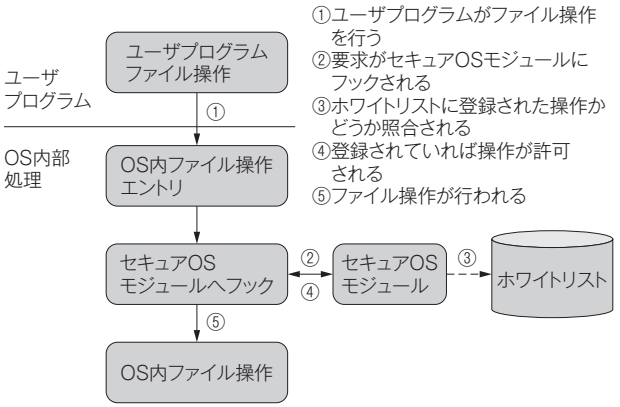
ト方式の比較を示す。ホワイトリスト方式の利点は，リストの更新が不要で中央演算処理装置（CPU）への負荷が少ないことである。

3　Linux セキュア OS モジュール

Linux のセキュア OS モジュールとして，SELinux が代表的である。しかしながら，今回は TOMOYO Linux を採用した。**第２表**に TOMOYO Linux と SELinux の比較を示す。TOMOYO Linux の特徴の一つである「セキュリティの専門家ではなくとも使える」という点に着目し，採用するに至った。

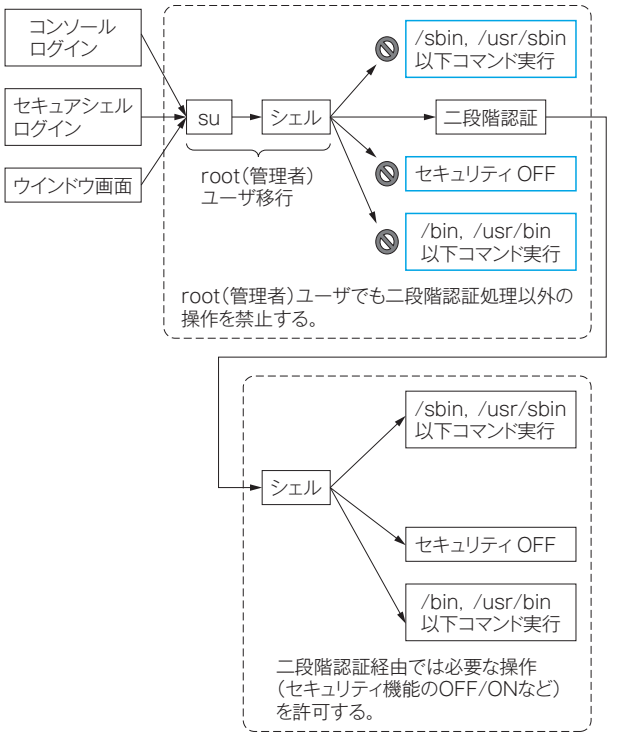
3.1　セキュア OS モジュールとホワイトリスト

ユーザプログラムがファイルの操作を行った場合，セキュア OS モジュールに一旦処理をフックする機能が組み込まれている。フックされた要求をホワイトリストと照合し，操作を許可するか否かを判断するのがセキュア OS モジュールである。ファイル操作は，ここで許可されたもののみ行われる。**第５図**にセキュア OS モジュールとホワイトリストの概要を示す。



第５図　セキュア OS モジュールとホワイトリスト

ファイル操作がセキュア OS モジュールでホワイトリストと照合される。



第６図　セキュリティと運用の両立の考え方

root（特権）ユーザでも二段階認証前は操作が制限される。

4　運用に対する考慮

セキュリティは強固であることが望ましいが，保守などの運用との両立も必要である。Linux では管理者による管理，保守はシェルというコマンドライン操作で行うことが通常である。今回は，シェルの操作で，通常の root（管理者）ユーザに対し，二段階認証を設けることでセキュリティと運用の両立を図った。**第６図**にその考え方を示す。

5　むすび

Linuxにおけるホワイトリスト方式のセキュリティソフトウェアを紹介した。当社製品では，Windowsだけではなく，Linux（組み込みLinuxを含む）もセキュリティ対策を実現した。

今後もお客様に安心して当社製品を使用していただけるように，機能と対応の拡充を図る所存である。

（注記）

注1．セキュアOS：アクセス権限を強化し，通常よりもセキュリティを強化したOS

《執筆者紹介》

鈴木　実
Minoru Suzuki
製品技術研究所
産業用コントローラ製品の基本ソフトウェア開発業務に従事

大竹康弘
Yasuhiro Otake
製品技術研究所
産業用コントローラ製品の基本ソフトウェア開発業務に従事