SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

組込み型ハイパーバイザにおけるVirtIOを利用した不正ファイルアクセス監視方法

Malicious File Access Monitoring using VirtIO in Embedded Hypervisor

大野　仁 *　　今本　吉治 *　　安齋　潤 *
Ono Hitoshi　　Imamoto Yoshiharu　　Anzai Jun

キーワード　VirtIO，ハイパーバイザ，監視，IDS，ファイル入出力

あらまし

近年の自動車業界において，制御用 ECU の増加や自動運転技術の発展に伴う制御系機能の一元化に伴い，複数の ECU が持つ機能を 1 つの ECU 上で動作させる統合 ECU という概念が重要になっている．統合 ECU では仮想技術を用いて一つの ECU 上に複数の ECU 機能を実現することが一般的であり，仮想環境を実現するための基本技術として仮想環境を動作させるハイパーバイザや，準仮想 IO ドライバとして VirtIO[1]が用いられる．

ハイパーバイザは大きく TYPE1 型と TYPE2 型の 2 種類に分けられ，動作するレイヤーでそれぞれ区別されている．TYPE1 型はベアメタル型と呼ばれハードウェア上で直接動作をし，ゲスト OS の管理を行う．TYPE1 型のハイパーバイザは，ハイパーバイザ上にゲスト OS からのデバイス操作リクエストのスケジューリング処理等をするホスト OS を動作させて，効率的に処理をする場合がある．TYPE2 型は特定の OS 上で動作するアプリケーションとして動作する．

ハイパーバイザ上で動作する VM（Virtual Machine）のセキュリティに関する研究はこれまでも多く行われており，仮想化環境を利用したセキュリティ技術についての議論も多くされている．文献[2]では TYPE2 型のハイパーバイザにフック関数を挿入し，ゲスト OS からのリクエストコマンドを監視することで，ゲスト OS に導入されている HIDS（Host-based Intrusion Detection System）等が無効化されていた場合でも不正な動作等を検出できるとしている．

本稿では文献[2]で示されていないブロックデバイスの操作を監視する方法を提案する．TYPE1 型のハイパーバイザが搭載された環境において，VirtIO の通信を監視し不正なファイル操作を検知する手法である．本稿のシステムを図 1 に示す．VirtIO という準仮想 IO ドライバの監視を行うことで，幅広い対象に適用できるという利点がある．また，文献[2]での課題として，フックを入れるためにハイパーバイザに変更を加える必要があるという点が挙げられる．しかし，本稿ではハイパーバイザ自体への変更はせずに，ホスト OS における BE-VirtIO（BackEnd-VirtIO）でゲスト OS からのブロックデバイスの操作リクエストログを取得することでゲスト OS のファイル操作を取得し監視を行った．

また本稿では本技術を導入した際のコストや，VirtIO の操作リクエストログの内容から，ゲスト OS（Linux）のファイルシステムベースのルールに適用するためのデータベースのサイズ等の観点から評価結果を報告する．

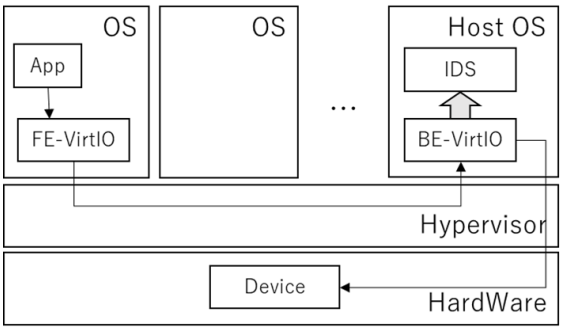

図 1　ホスト OS でファイルの不正検知システム

参考文献

[1] Virtual I/O Device，https://www.oasis-open.org/
[2] Tal Garfinkel, Mendel Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. Proceedings of Network and Distributed Systems Security Symposium (NDSS03), San Diego, USA. 2003.

* パナソニック株式会社，大阪府門真市大字門真 1006 番地，
Panasonic Corporation, 1006, Kadoma, Kadoma City, Osaka, Japan. E-mail:ono.hitoshi@jp.panasonic.com