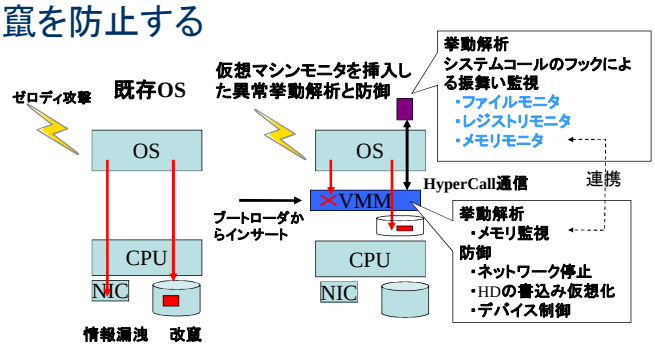
ゼロディ攻撃に対する異常挙動解析と挿入可能な仮想マシンモニタによるデバイス制御

須崎有康（ソフトウェアセキュリティ研究チーム）

Windowsのゼロディ攻撃に対して***「振舞いから異常動作を検出」***し、***「仮想マシンモニタでのデバイス制御」***をすることより情報漏洩、改竄を防止する

開発項目	計画概要
①Windows上での異常挙動検出	レジストリやファイル関連のシステムコールをフックし，その振舞いを解析する
②仮想マシンモニタインサーション	USB/CDから仮想マシンモニタを起動するが，仮想マシンモニタ上でハードディスクのWindowsが普通に使えるようにする
③仮想マシンモニタによるデバイス制御	仮想マシンモニタでのデバイス抑制/停止して漏洩・改竄を防止

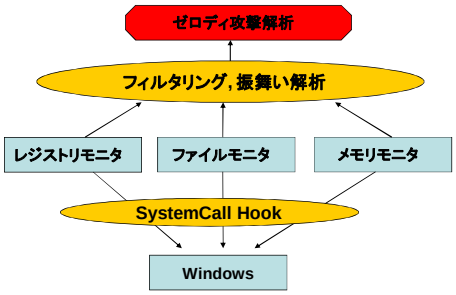


平成20-21年度　経済産業省　新世代情報セキュリティ研究開発事業（情報通信研究機構との共同提案）

①　Windows上での異常挙動検出

WindowsのシステムコールAPIをフックしてレジストリ、ファイル、メモリのアクセスをモニタするツールを開発し、挙動の状態遷移を解析して異常動作を検出する

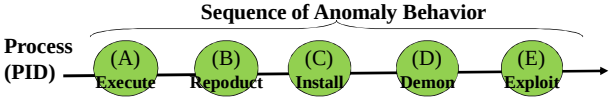
モニタ類と解析の関係



Black Listベースの異常挙動検出

マルウェアは自己複製，インストール，常駐化など特定のシステムコール呼出し手順があるので，その状態遷移を検出する

Labeled Action	Windows API	Object (Argument for API)
(A) Execute　生成	CreateProcess, CreateFile, OpenProcess	(Wild Card)
(B) Reproduction　複製	CreateRemote Thread	SVCHOST.EXE　Expolore Exe
(C) Installation　インストール	CreateCopy	Windows Directory　C:¥Windows¥System32
(D) Daemonize　常駐化	(Wind Card)	avrserve.exe process　memory
(E) Exploitation　報告	WSAsend, Send	Networked Computer

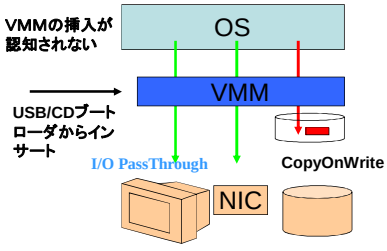


②仮想マシンモニタインサーション

USB/CDから仮想マシンモニタを起動するが、ユーザから見れば通常のハードディスクWindowsが起動するようにみえる

開発課題：　Windowsに仮想マシンモニタを気づかせない

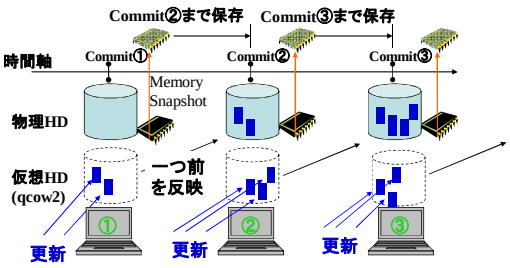
I/O PassThroughの技術を使ってほとんどのデバイスはWindowsが直接アクセス可能した



③仮想マシンモニタによるデバイス制御

・CopyOnWriteによる書込み抑制・ロールバックを行える仮想デバイス作成

書込み抑制
(遅延書込み)



ロールバック