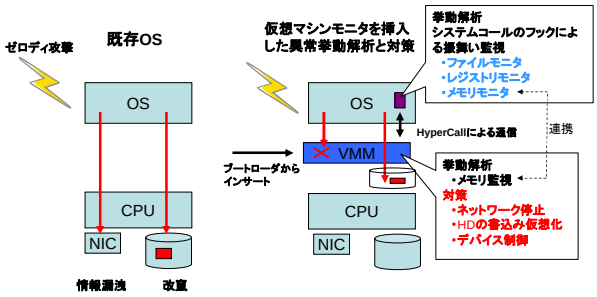
ゼロディ攻撃に対する異常挙動解析と挿入可能な仮想マシンモニタによるデバイス制御

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	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

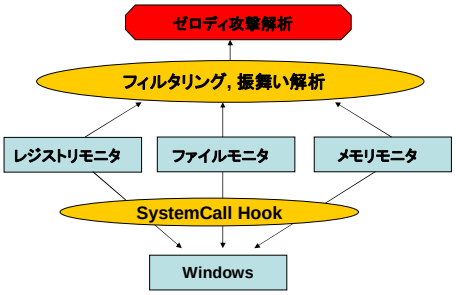


平成20-21年度　経済産業省　新世代情報セキュリティ研究開発事業（情報通信研究機構との共同提案）

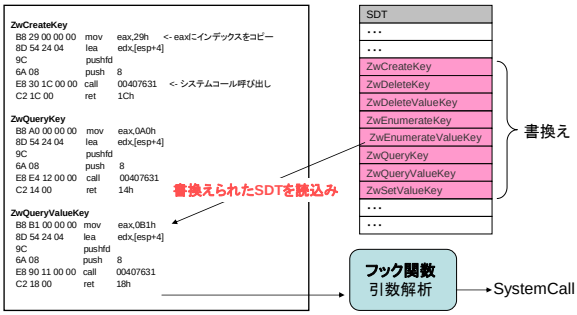
①　Windows上での異常挙動検出

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、挙動を多角的に解析して異常動作を検出する

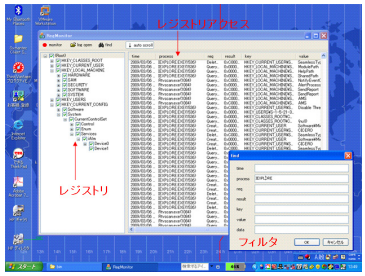
モニタ類と解析の関係



Windowsのシステムコールのテーブル(SDT: Service Descriptor Table)をドライバロード時に書換え、フック関数を通るようにする



レジストリモニタ動作図



②仮想マシンモニタインサーション

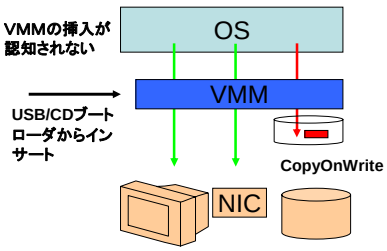
USB/CDから仮想マシンモニタを起動するが、ユーザから見れば通常のハードディスクWindowsが起動するようにみえる

USB/CD起動→仮想マシンモニタ(管理OS) → Windows on VM (Xen)

開発課題：　Windowsに仮想マシンモニタを気づかせない

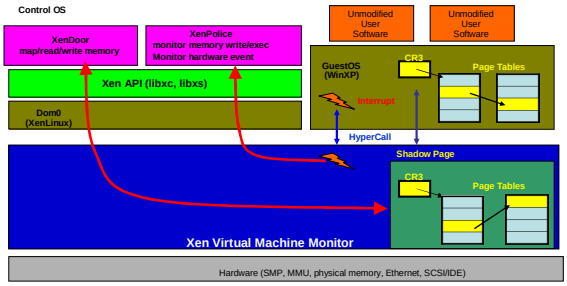
I/O PassThroughの技術を使ってほとんどのデバイスはWindowsが直接アクセス可能にする

CopyOnWriteによる書込み抑制を行うデバイスのドライバ作成



③仮想マシンモニタによるデバイス制御

仮想マシン上のメモリ内容を変更できるXenDoor、およびハードウェアイベントの通知を受けるXenPoliceを開発



National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

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

情報セキュリティ研究センター（RCIS）

ソフトウェアセキュリティ研究チーム

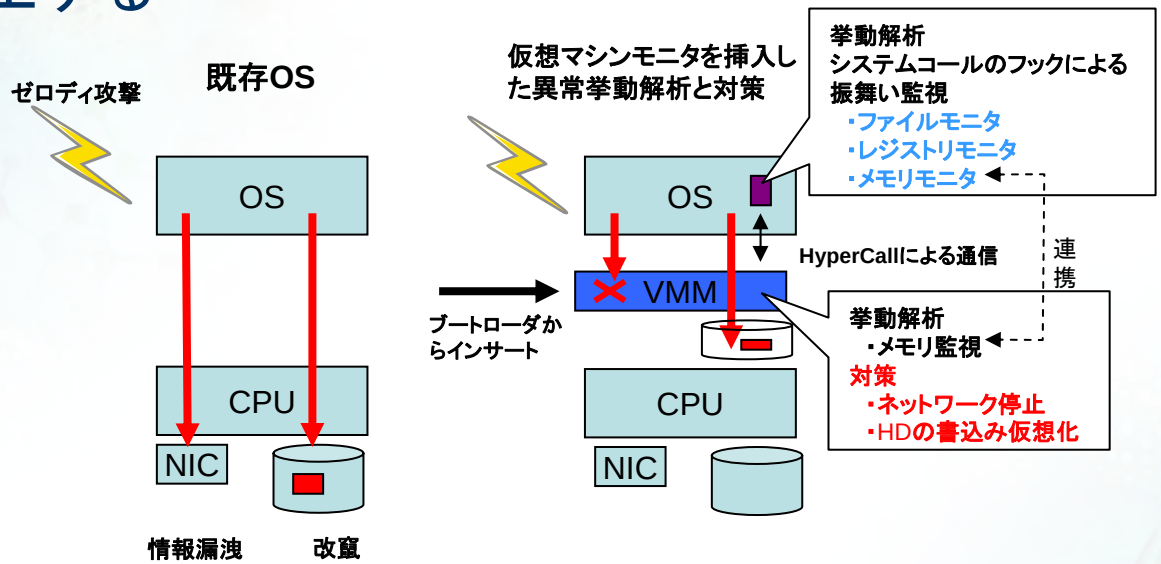
須崎有康

National Institute of Advanced Industrial Science and Technology
AIST

研究概要

Research Center for Information Security

- 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デバイス制御」*することより情報漏洩、改竄を防止する



- 開発項目
  - ① Windows上での異常挙動検出
  - ② 仮想マシンモニタインサーション
  - ③ 仮想マシンモニタによるデバイス制御

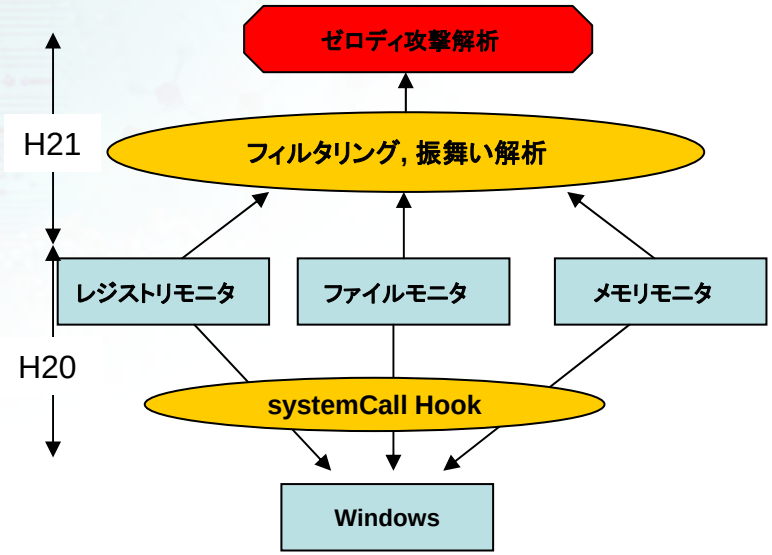
平成20-21年度　経済産業省　新世代情報セキュリティ研究開発事業
情報通信研究機構(NICT)との共同提案

National Institute of Advanced Industrial Science and Technology AIST

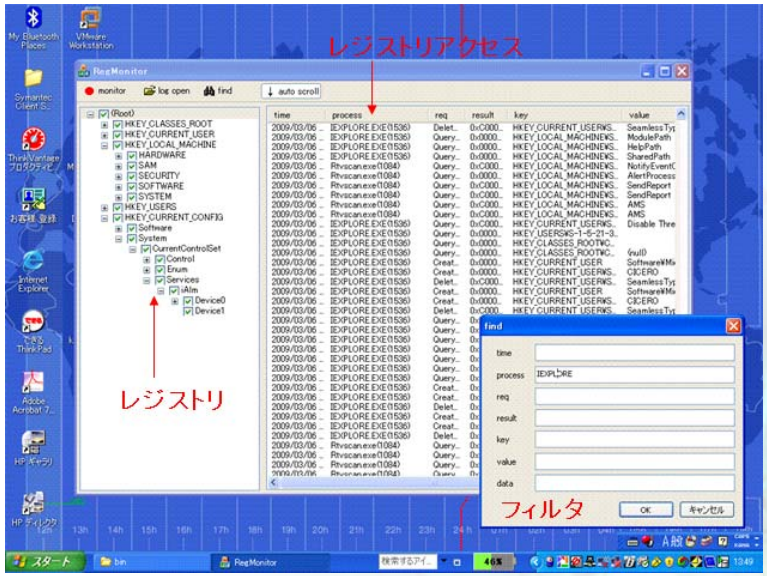
①Windows上での異常挙動検出

Research Center for Information Security

- Windowsのシステムコール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、挙動を多角的に解析して異常動作を検出する



レジストリモニタの動作



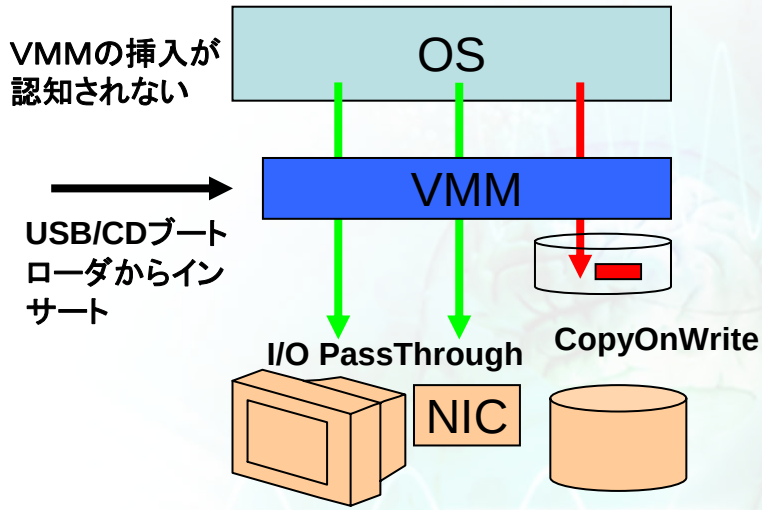
- 今後の開発
  - 異常動作の振舞いをシーケンスから検出
    - 例: GetProcAddress -> kernel32dll -> Loadlibrary -> URLdownload
  - 振舞いのシーケンスが既知の場合、シーケンスを外れた時に異常動作と検出

National Institute of Advanced Industrial Science and Technology AIST

②挿入可能な仮想マシンモニタ

Research Center for Information Security

- 既存のWindowsで簡単に採用できるように外部から挿入(インサーション)できる仮想マシンモニタを開発
  - USB起動→仮想マシンモニタ(管理OS) → Windows on VM
    - USB/CDから仮想マシンモニタを最初に起動するが、最終的にはハードディスクのWindowsが起動する。ユーザから見れば通常のWindowsが使うことができる。
  - 仮想マシンモニタは独自のデバイスモデルを持つが、I/O PassThrough (Intel VT-d, AMD IOMMU)を使ってデバイスの直接アクセス可能にする。制御が必要なデバイスは仮想化する。



③仮想マシンモニタによるデバイス制御

- 異常を検知した場合、仮想マシンモニタがネットワークやハードディスクの抑制・制御を行う。
  - 仮想マシン上のメモリ内容を変更できるXenDoor、およびハードウェアイベントの通知を受けるXenPoliceを開発
  - このツールを使ってネットワークのフィルタリングやCopyOnWriteなどの機能を統合