論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻

学生番号	11675002	氏　名	宇都宮　寿仁
論文題目	仮想マシンの監視を継続可能なマイグレーション機構		

1　はじめに

サーバへの不正アクセスを検出するために侵入検知システム (IDS) が用いられている。IDS はサーバのメモリ、ネットワーク、ストレージなどの監視を行う。しかし、近年、攻撃者は IDS を攻撃してからサーバへの攻撃を行うようになってきた。IDS への攻撃対策として仮想マシン (VM) を用いた IDS オフロードが提案されている。これは監視対象システムとそれを監視する IDS を別々の VM で動作させることで IDS のより安全な実行を可能にする。しかし、IDS オフロードを行うとオフロード先の VM は監視対象 VM と一緒に別のホストにマイグレーションすることができないため、監視を継続することができなくなる。

そこで、本研究では VM の監視を継続可能なマイグレーション機構を備えたオフロード専用 VM であるドメイン M を提案する。

2　ドメイン M

ドメイン M ではオフロードされた IDS を動作させて監視対象 VM を監視することができる。監視対象 VM のマイグレーション時にはドメイン M も同時にマイグレーションすることができ、空白期間なく監視を継続することができる。

2.1　VM の継続的な監視

ドメイン M は監視対象 VM のメモリページをマップすることでメモリ監視を行う。既存のシステムではマイグレーションできない管理 VM しか他の VM にアクセスできないが、ドメイン M にも指定した VM へのアクセス権を与える。メモリページをマップしたままマイグレーションを行うために、マップされているメモリページには監視ビットを立てておき、復元の際に再び監視対象 VM のメモリページをマップする。

ドメイン M は監視対象 VM のパケットを監視用インターフェースを通して取得することでネットワーク監視を行う。すべてのパケットは管理 VM を経由するため、管理 VM で監視対象 VM のパケットをドメイン M の監視用インターフェースに送信する。ドメイン M のマイグレーション時には、マイグレーション先の管理 VM で再びパケット複製の設定を行うことにより監視を継続できるようにする。

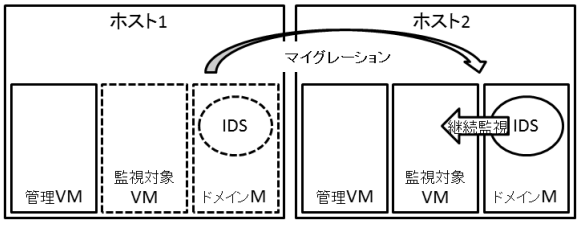

図 1: ドメイン M

ドメイン M は NFS サーバを用いることで監視対象 VM のストレージ監視を可能にする。NFS サーバ上に置かれた監視対象 VM のディスクイメージをドメイン M でもマウントすることで監視対象 VM のストレージを監視する。ドメイン M のマイグレーションを行ってもこの NFS マウントは自動的に継続される。

2.2　同時マイグレーション

ドメイン M は監視対象 VM と同期を取りながらマイグレーションすることで監視の空白期間が生じないようにする。マイグレーション元ではドメイン M が先に停止すると監視が途切れてしまうため、監視対象 VM が停止するまでドメイン M を待たせる。同様にマイグレーション先ではドメイン M が再開されるまで監視対象 VM を再開しない。

3　実験

ドメイン M を Xen 4.0.1 に実装し、監視の有無によるマイグレーション時間への影響を測定した。監視対象 VM、ドメイン M のメモリサイズをそれぞれ 1024MB, 512MB とし、2 つの VM を同時にマイグレーションした。マイグレーション時間の平均は監視無しの場合 15.3 秒、監視有りの場合 15.9 秒となり、監視有りのほうがわずかに遅いことが分かった。

4　おわりに

本研究ではマイグレーション後も監視対象 VM の監視を継続できるオフロード専用 VM であるドメイン M を提案した。ドメイン M はマイグレーション後に監視の状態を復元し、2 つの VM の同期をとりながらマイグレーションを行う。