VM マイグレーションに対応した IDS オフロード機構

宇都宮　寿仁[†]　光来健一[†,††]

1. はじめに

サーバへの不正アクセスが年々増加してきている。このような攻撃を検出するために侵入者検知システム (IDS) が用いられている。IDS はストレージやメモリ内容、ネットワークの監視を行う。しかし近年、IDS を停止させた後で被害を及ぼす攻撃が増加している。そこで IDS への攻撃を緩和する方法として仮想マシンを用いた IDS オフロードという手法が提案されている[?)]。この手法はサーバのサービスと IDS を別々の仮想マシンで動作させることで IDS の安全な実行を可能にする。しかし IDS のオフロードを行うと IDS オフロードを行ったマシンは監視対象のマシンと一緒に別のマシンにマイグレーションを行うことができないという問題が発生する。これは、Xen においてはドメイン 0 という特殊な仮想マシンでしか IDS を動かすことができないが、ドメイン 0 はマイグレーションできないためである。

そこで本研究ではオフロードした IDS を動作させることができ、マイグレーションも行うことができるオフロード専用マシンドメイン M を提案する。

2. ドメイン M

ドメイン M 上の IDS は現在のところ、ドメイン U のストレージとメモリを監視することができる。

2.1 ストレージの監視

ドメイン M は図 1 のように NFS サーバを用いることでストレージの監視を可能にする。ドメイン 0 は NFS サーバ上に置かれたドメイン U のディスクイメージを使ってドメイン U を起動する。ドメイン M もこのディスクイメージを同様に NFS マウントする。これによってドメイン M からドメイン U のストレージの監視を行うことができる。NFS サーバを用いることでドメイン M のマイグレーション後もドメイン U のストレージ監視を継続することができる。ドメイン M はマイグレーション後も IP アドレスが変わらないため NFS マウントが継続されるためである。またドメイン M をマイグレーションするためにドメイン M のイメージファイルも NFS サーバ上に配置する。

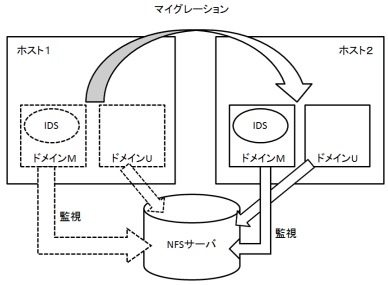

図 1　マイグレーション後のストレージの監視

2.2 メモリの監視

ドメイン M はドメイン U のメモリページをマップすることでメモリの監視を行う。しかし、従来はドメイン 0 以外はドメイン U にアクセスすることができなかった。そこで Xen のスタブドメインの機能を利用することで指定したドメイン U へのアクセスを許可する。ドメイン M に特定のドメイン U のアクセス権を与えるには、ドメイン 0 から domctl ハイパーコールを用いて行う。

さらに、ドメイン U のメモリにアクセスできるようにドメイン M の Linux カーネルに privcmd インタフェースを追加し、ドメイン U のメモリページをマップ可能にした。ドメイン U のメモリページをマップする際にドメイン 0 は privcmd インターフェースを用いてマップを行うが、ドメイン 0 以外には privcmd インターフェースが存在しなかった。加えて、ドメイン U のメモリ情報を取得するために呼び出す domctl ハイパーコールの実行許可をドメイン M を与えた。このハイパーコールはドメイン U を管理するために用いるものであり、ほとんどはドメイン 0 にしか許可されていなかった。

監視を継続したままドメイン M のマイグレーションを可能にするために、ドメイン M のメモリイメージ

† 九州工業大学
†† 独立行政法人科学技術振興機構, CREST

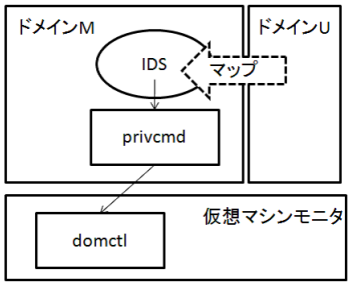

図 2 ドメイン M におけるメモリマップ

の保存を行う際にドメイン U のメモリページのマップ状態についても保存を行う。そのために、ドメイン M のページテーブルに DomU ビットというドメイン U のマップ状態を記録するためのビットを追加する。保存したメモリイメージを送信した後、マイグレーション先でドメイン M を復元する際にページテーブルエントリの DomU ビットを確認する。DomU ビットが立っていれば監視しているドメイン U のメモリを再マップし監視の継続を行う。

マイグレーションを行うと監視対象のドメイン U へのアクセス権限が失われる。そこでドメイン M のコンフィグに target_uuid オプションを追加し、このオプションに監視しているドメイン U の UUID を設定しておく。マイグレーション先でコンフィグ内の UUID を基に監視対象のドメイン U を見つけ出し、再びアクセス権限を与える。

3. 実　　験

ドメイン M を Xen 4.0.1 に実装し、オフロードした IDS の性能及びマイグレーションのオーバーヘッドを調べる実験を行った。

まずドメイン M の NFS マウントの有無がマイグレーション時間に与える影響を調べた。マイグレーション時間を計測した平均値を表 1 に示す。この結果より NFS マウントの有無にかかわらず、マイグレーション時間はほぼ同じであることが分かった。

表 1 NFS マウントのマイグレーション時間への影響

	時間 (秒)
NFS マウントなし	92.6
NFS マウントあり	92.3

ドメイン M がメモリマップを行っている状態と、行っていない状態でそれぞれマイグレーションを行い、その時間を計測した。10 回計測した平均値を表 2 に示す。メモリマップの状態に関わらずマイグレーション時間はほぼ同じであることが分かった。

表 2 メモリ監視時のマイグレーション時間への影響

	時間 (秒)
メモリマップなし	92.6
メモリマップあり	92.2

4. ま と め

本研究ではマイグレーション後も監視を継続することができる IDS オフロード機構であるドメイン M を提案した。ドメイン M には IDS をオフロードでき、監視しているドメイン U と一緒にマイグレーションを行うことができる。今後の課題はライブマイグレーションに対応させ、ネットワークの監視を実装することである。

参 考 文 献

1) Garfinkel, T. and Rosenblum, M.: A Virtual Machine Introspection Based Architecture for Intrusion Detection, *Proc. Network and Distributed Systems Security Symp.*, pp. 191–206 (2003).