VM監視を継続するための同時マイグレーション機構

宇都宮 寿仁　光来　健一

仮想マシン (VM) を用いて侵入検知システム (IDS) をオフロードする際に、VM のマイグレーション後も監視を継続できるようにする同時マイグレーション機構を提案する。IDS はサーバへの不正アクセスを検出するために用いられているが、IDS 自身が攻撃されてしまうとセキュリティが低下してしまう。そこで IDS とサーバを別々の VM で動かし、安全に監視する IDS オフロードと呼ばれる手法が提案されている。しかし、監視対象の VM を別のホストにマイグレーションをするとオフロードした IDS は監視を継続することができなくなる。そこで我々は、ドメイン M と呼ぶオフロード専用 VM を導入し、2 つの VM を同時にマイグレーションしてマイグレーション後もストレージやメモリの監視を継続できるようにする。

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検知システム (IDS) が用いられている。IDS はストレージ、メモリ、ネットワークなどのを監視を行い侵入や攻撃を検知すると監視者に即座に通知する。しかし近年、攻撃者は IDS を攻撃して停止させてからサーバへの攻撃を行うようになってきた

IDS への攻撃を緩和する方法として仮想マシン (VM) を用いた IDS オフロードという手法が提案されている。これは監視対象のマシンとそれを監視する 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 オフロードを行った際に問題となるのが監視対象 VM のマイグレーションである。IDS をオフロードした先の 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を行うことができないため、マイグレーション後には監視を継続することができなくなってしまう。

そこで、我々はオフロードされた IDS を動作させることができ、監視対象 VM と同時にマイグレーションを行い監視を継続できるオフロード専用 VM であるドメイン M を提案する。

2　ドメイン M

2.1　監視対象 VM の監視

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。監視対象 VM は NFS サーバ上に置かれたディスクイメージを使って起動し、ドメイン M も同じディスクイメージを NFS マウントする。これによりドメイン M は監視対象 VM のストレージの監視を行うことができる。ドメイン M と監視対象 VM のマイグレーションを行っても NFS マウントが継続されるため、監視を継続することができる。

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。従来はドメイン 0 と呼ばれる特権 VM 以外は他の VM にアクセスすることができなかったため、Xen のスタブドメインの機能を利用することで指定した VM へのアクセスを可能とした。監視を継続したままドメイン M のマイグ

Co-migration for Continuous Monitoring of VMs.
Hisato Utsunomiya, Kenichi Kourai, 九州工業大学, Kyushu Institute of Technology.

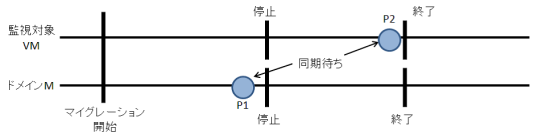

図 1　マイグレーション元での同期

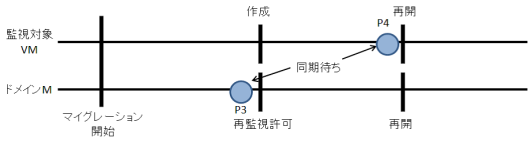

図 2　マイグレーション先での同期

レーションを可能にするために、マイグレーション先では監視対象 VM のメモリページのマップ状態についても復元する。

2.2　同時マイグレーション

監視対象 VM をほぼ停止させずに行うライブマイグレーション中に監視が途切れないようにするために、ドメイン M は監視対象 VM と同期をとりながら同時にマイグレーションする。マイグレーション元では図 1 のように 2 か所の同期するポイントがある。これを順に P1、P2 とする。ドメイン M は監視対象 VM が動いている間、監視し続ける必要があるため、ドメイン M は P1 で監視対象 VM が停止するまで待つ。監視対象 VM が動いている状態でドメイン M が停止してしまうと、監視できない期間ができて危険である。一方、ドメイン M はマイグレーション中に監視対象 VM の情報を得る必要があるためドメイン M が終了するまで P2 で監視対象 VM を停止して待たせる。

マイグレーション先でも図 2 のように 2 か所の同期ポイントがある。これを順に P3、P4 とする。ドメイン M はメモリ監視のためのアクセス権限を得るために監視対象 VM の情報を必要とするため、監視対象 VM が生成されるまで P3 で待つ。またドメイン M が動いていない状態で監視対象 VM を動かすと監視ができないため、ドメイン M が再開されるまで P4 で監視対象 VM を停止して待たせる。

3　実験

ドメイン M を Xen 4.0.1 に実装し、同時マイグレーションによるオーバヘッドを調べる実験を行った。

まず、ドメイン M と監視対象 VM を同時にマイグレーションした際にドメイン M と監視対象 VM の同期がマイグレーション時間にどのくらい影響するかを調べた。比較のために 2 つの VM を同期をとらずにマイグレーションした場合の時間も測定した。2 つの VM のライブマイグレーションが完了するまでの時間を 10 回測定した平均値を図 3、図 4 に示す。図 3 では監視対象 VM のメモリサイズを 1024MB に固定し、図 4 ではドメイン M のメモリサイズを 1024MB に固定した。同期をとらない場合と比べると、2 つの VM のメモリサイズに差ができると、マイグレーション時間が長くなっていることが分かった。

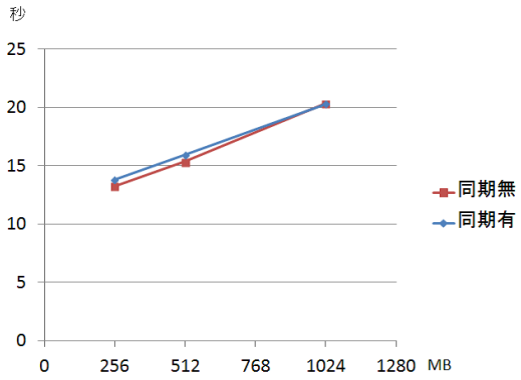

図 3　ドメイン M のメモリサイズを変更した時のマイグレーション時間 (秒)

次に、各同期ポイント P1～P4 においてどのくらい同期待ちするのかを調べた。10 回計測した平均値を表 1、表 2 に示す。表 1 では監視対象 VM のメモリサイズを 1024MB に固定し、表 2 ではドメイン M のメモリサイズを 1024MB に固定した。実験結果からドメイン M と監視対象 VM のメモリサイズの小さいほうがもう一方の VM を待っていることが分かった。

また、監視対象 VM のダウンタイムを計測した。マ

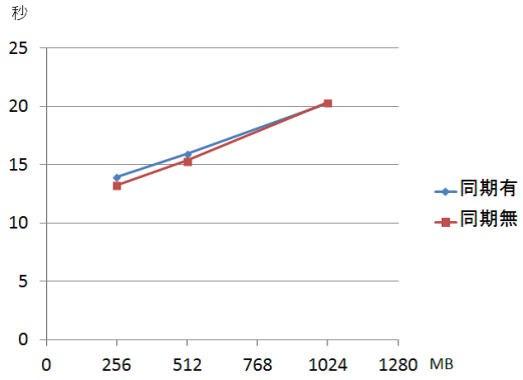

図 4　監視対象 VM のメモリサイズを変更した時のマイグレーション時間 (秒)

表 1　ドメイン M のメモリサイズを変更した時の同期待ち時間 (ミリ秒)

	1024MB	512MB	256MB
P1	74	5200	7736
P2	92	18	14
P3	0	0	0
P4	69	51	25

表 2　監視対象 VM のメモリサイズを変更した時の同期待ち時間 (ミリ秒)

	1024MB	512MB	256MB
P1	74	0	0
P2	92	5109	7696
P3	0	0	0
P4	69	101	51

イグレーション元のホストで VM が停止してからマイグレーション先のホストで再開されるまでの時間を計測した。10 回計測した平均を表 3、表 4 に示す。表 3 では監視対象 VM のメモリサイズを 1024MB に固定し、表 4 ではドメイン M のメモリサイズを 1024MB に固定した。表 3 より、ダウンタイムはメモリサイズの合計が小さいほど短くなることが分かった。一方、表 4 から監視対象 VM のメモリサイズが相対的に小さくなると、ダウンタイムが増大することが分かった。これは P2 での同期待ち時間が長いことが原因である。しかし、一般的には監視対象 VM のほうがドメイン M よりメモリサイズは大きいため、問題にはならないと考えられる。

表 3　ドメイン M のメモリサイズを変更した時のダウンタイム (ミリ秒)

	1024MB	512MB	256MB
ダウンタイム	1055	870	786
同期待ち時間	219	108	63

表 4　監視対象 VM のメモリサイズを変更した時のダウンタイム (ミリ秒)

	1024MB	512MB	256MB
ダウンタイム	1112	5971	8493
同期待ち時間	219	5268	7780

4　まとめ

本稿ではマイグレーション後も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 には IDS をオフロードすることができ、監視対象 VM と同時にマイグレーションすることで安全にマイグレーションを行うことができる。今後の課題はドメイン M におけるネットワーク監視を実装することである。

謝辞

本研究の一部は, 科学技術振興機構 戦略的創造研究推進事業 (CREST) 研究領域「実用化を目指した組み込みシステム用ディペンダブル・オペレーティングシステム」による.