情報処理学会論文誌 Vol.0 No.0 1–7 (??? 1959)

帯域外リモート管理の継続が可能なマイグレーション手法

川原 翔[1] 光来 健一[1,2]

受付日 2013年7月4日, 採録日 2013年7月4日

概要：IaaS 型クラウドにおいて，ユーザは提供された VM であるユーザ VM をリモートから管理する．ユーザ VM を管理する権限を持った VM である管理 VM 経由で帯域外リモート管理を行うことで，ユーザ VM に障害が発生した場合でも管理を行うことが可能である．しかし，ユーザ VM を別のホストにマイグレーションすると，移動元のホストの管理 VM はユーザ VM にアクセスできなくなり，リモート接続が切断されてしまう．この問題を解決するために，本稿では，帯域外リモート管理の継続が可能なマイグレーションを実現するシステム *D-MORE* を提案する．D-MORE は，従来，管理 VM で動作していた VNC サーバと仮想デバイスをドメイン R と呼ばれるリモート管理用 VM で動作させ，ユーザ VM とドメイン R を同時にマイグレーションする．D-MORE を Xen に実装し，ドメイン R 経由でユーザ VM に入力を送ることができていることを確認した．さらに，ドメイン R を用いるオーバーヘッドが許容範囲内であることを確認した．

キーワード：仮想マシン，リモート管理，マイグレーション

A Migration Method for Continuing Out-of-band Remote Management

Sho Kawahara[1] Kenichi Kourai[1,2]

Received: July 4, 2013, Accepted: July 4, 2013

Abstract: In Infrastructure-as-a-Service (IaaS) clouds, users remotely manage the systems in provided virtual machines (VMs) called user VMs. Out-of-band remote management via the management VM allows users to manage their systems even on failures inside user VMs. However, the remote management is discontinued on the migration of user VMs because the management VM at a source host cannot access the user VMs. To solve this problem, we propose *D-MORE* for continuing out-of-band remote management after the migration of user VMs. D-MORE runs a VNC server and virtual devices, which conventionally run in the management VM, in a VM for remote management called Domain R. It migrates both a user VM and Domain R simultaneously. We have implemented D-MORE in Xen and confirmed that a VNC client could send input data to a user VM via Domain R. In addition, we showed that the overheads of D-MORE were within the acceptable range.

Keywords: Virtual machine, remote management, migration

1. はじめに

近年，ネットワークを介してユーザにサービスを提供するクラウドコンピューティングの利用が広がっている．その一つの形態として，ユーザに仮想マシン（VM）を提供する Infrastructure as a Service (IaaS) 型クラウドサービスがある．IaaS 型クラウドを利用することによって，ユーザはハードウェアを用意することなく，必要な時に必要なだけの VM を使用することができる．IaaS 型クラウドのユーザは VNC などのリモート管理ソフトウェアを用いて，提供された VM （ユーザ VM） にリモートからアクセスすることによって，内部のシステムの管理を行う．

その際に，ユーザ VM に直接アクセスするのではなく，ユーザ VM を管理する権限をもつ VM（管理 VM）経由でアクセスすることができる．この管理手法は帯域外リモート管理と呼ばれる．この手法において，VNC サーバは管

[1] 九州工業大学
Kyushu Institute of Technology
[2] 独立行政法人科学技術振興機構，CREST

理 VM 上で動作しており，仮想キーボードや仮想ビデオカードなどの仮想デバイスを使用して，ユーザ VM に直接アクセスする．この手法を用いることにより，ユーザ VM のネットワークが VM 内部の設定ミスによって切断されたり，システムクラッシュが起きたりするような障害が発生したとしても，ユーザは VM のリモート管理を継続することができる．

しかしながら，帯域外リモート管理を行っている場合に，ユーザ VM を別のホストにマイグレーションすると，リモート接続が切断されてしまう．これは，移動元の管理 VM がユーザ VM にアクセスできなくなるために発生する問題である．ユーザ VM のマイグレーションは，物理マシンのメンテナンスが必要となった時や負荷が高くなった時にユーザ VM を別のホストに移動させるために必要とされる．ユーザはリモート管理を再開するために，接続が切断された原因を特定した上で，どのホストの管理 VM に接続し直すかを調べ，再接続を行わなければならない．そのため，ユーザに多大な負担を強いることになる．

この問題を解決するために本稿では，ユーザ VM のマイグレーション時においても帯域外リモート管理の継続が可能なマイグレーションを実現するシステム *D-MORE* を提案する．D-MORE は，VNC サーバと仮想デバイスをドメイン R と呼ばれるリモート管理用の専用 VM 上で動作させる．ユーザ VM のマイグレーション時にはドメイン R も同時にマイグレーションさせる．このとき，D-MORE はドメイン R とユーザ VM の間の接続を仮想マシンモニタ（VMM）レベルで維持する．また，VNC クライアントと VNC サーバの間の接続はネットワークレベルで維持する．これにより，帯域外リモート管理中にマイグレーションを行ったとしても，リモート管理を継続できる．

我々は D-MORE を Xen 4.1.3 [1] に実装した．ドメイン U のメモリを監視できるように開発されたドメイン M [2] を基にドメイン R を実装し，ドメイン R とドメイン U の間で，イベントチャネルを確立できるように拡張した．これらの機能を用いて，ドメイン R 上の仮想デバイスはドメイン U にアクセスする．ドメイン R が提供する同時マイグレーション機能を用いることで，ドメイン R はマイグレーション後にドメイン U のメモリへのアクセスを継続することができている．ドメイン R 上で動作する VNC サーバは，RFBProxy [3] を基に作成した．D-MORE を用いた実験を行い，ドメイン R 経由で帯域外リモート管理ができること，および D-MORE のオーバーヘッドがほとんどないことを確認した．

以下，2 章では，帯域外リモート管理中のマイグレーション時に発生する問題について述べる．3 章でこの問題を解決する D-MORE について述べ，4 章でその実装の詳細について述べる．5 章で D-MORE を用いて行った実験について述べる．6 章で関連研究に触れ，7 章で本稿をまとめる．

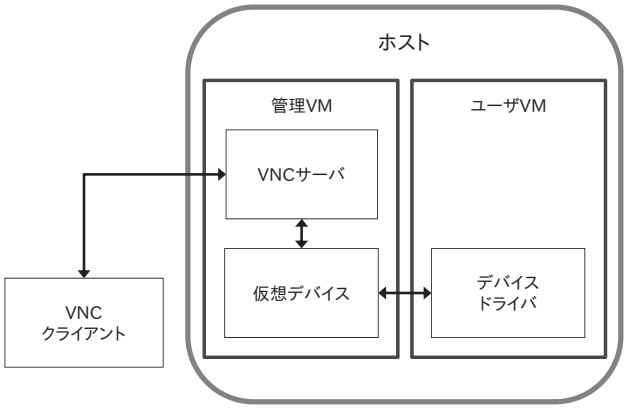

図 1 帯域外リモート管理

2. 帯域外リモート管理中のマイグレーション

2.1 帯域外リモート管理

IaaS 型クラウドのユーザは従来，提供されたユーザ VM に VNC サーバを導入し，VNC クライアントからリモート接続することによって，システムの管理を行っていた．この管理手法は管理対象のシステムに直接アクセスを行うため，帯域内リモート管理と呼ばれる．しかしながら，帯域内リモート管理にはユーザ VM 内部における障害に弱いという欠点が存在する．これは，ユーザ VM 内部でネットワークやファイアウォールの設定を誤った場合に，VNC サーバにネットワーク接続を行うことができなくなり，リモート管理できなくなるためである．さらに，ユーザ VM の OS を起動している間や，OS がクラッシュした場合には，VNC サーバ自体が動作していないため，リモート管理を行うことができない．このことは，リモートでシステムの詳細な挙動を把握したり，障害の究明を行う場合に問題となりえる．

このような状況下においてもユーザ VM の管理を継続できるようにするために，**図 1** のように管理 VM で VNC サーバを動作させ，ユーザ VM に間接的にアクセスする手法がある．この手法は**帯域外リモート管理**と呼ばれる．管理 VM とは，全てのユーザ VM にアクセスする特権を持った VM のことであり，ハードウェア上で直接動作するハイパーバイザ型の VMM において提供されることが多い．管理 VM の役割の一つは，ユーザ VM に提供される仮想デバイスのエミュレーションである．帯域外リモート管理では，管理 VM 内の VNC サーバがユーザ VM 用の仮想キーボードなどの仮想デバイスに直接アクセスする．そのため，ユーザ VM の VNC サーバやネットワークに依存しないリモート管理を実現することができる．

これにより，ユーザ VM に障害が発生した場合でも，ローカルコンソールからログインしているかのように操作を行うことができ，より柔軟な VM の管理が可能になる．例え

ば，ネットワークの設定ミスによってユーザ VM へのネットワーク接続ができなくなったとしても，キーボード入力を行って設定ファイルを修正し，ネットワーク接続を復旧させることができる．また，仮想ビデオカードへのアクセスを通して，OS のクラッシュ時のメッセージを確認することが可能である．

2.2 マイグレーション時の問題

ユーザ VM を別のホストにマイグレーションする際には，従来の帯域内リモート管理を行っていればリモート管理を継続することができた．これは，VM のマイグレーションを行ったとしても，VNC クライアントから VM 内で動作している VNC サーバへのネットワーク接続は維持されるためである．マイグレーションは VM を停止させることなく別のホストに移動させられるため，様々な目的で必要とされる機能である．例えば，物理マシンのメンテナンスを行う際に，物理マシンを停止させると VM 上のサービスも停止してしまう．物理マシンのメンテナンスを行う前に，VM を別のホストにマイグレーションしておくことによって，サービスを継続したままメンテナンスを行うことができる．また，マイグレーションは負荷分散を行うためにも利用される．

しかしながら，帯域外リモート管理の場合，ユーザ VM をマイグレーションするとリモート接続が切断されてしまう．これは，管理 VM 上で VNC サーバが稼働しているが，ユーザ VM のマイグレーションに伴って，管理 VM 内に作られたユーザ VM 用の仮想デバイスが存在しなくなるためである．その結果，VNC サーバが仮想デバイスにアクセスできなくなり，VNC サーバが終了し，ユーザ VM の操作を行うことができなくなる．ユーザはリモート管理を再開するために，接続が切断された原因を特定した上で，どのホストに接続し直さなければならないかを調べ，再接続を行う必要がある．

また，マイグレーションの際にキーボード入力情報が失われる可能性がある．ネットワーク上の送信中の入力はリモート接続の切断によって破棄される．VNC サーバが受け取ったが，仮想キーボードに渡されていない入力も VNC サーバの終了とともに失われる．完全仮想化の仮想キーボードの場合には，入力を自身のバッファに保持しているため，ユーザ VM から読み込まれていない入力は仮想キーボードの消滅とともに失われる．このように失われたキーボード入力はユーザがもう一度入力する必要がある．

加えて，マイグレーション時に VNC サーバの IP アドレスとポート番号が変更されてしまうという問題もある．再接続する VNC サーバの IP アドレスはユーザ VM の移動先ホストの管理 VM のものになる．また，ユーザ VM ごとに VNC サーバが必要になるため，それぞれ異なるポート番号を使用する必要がある．近年，出口対策として，外部

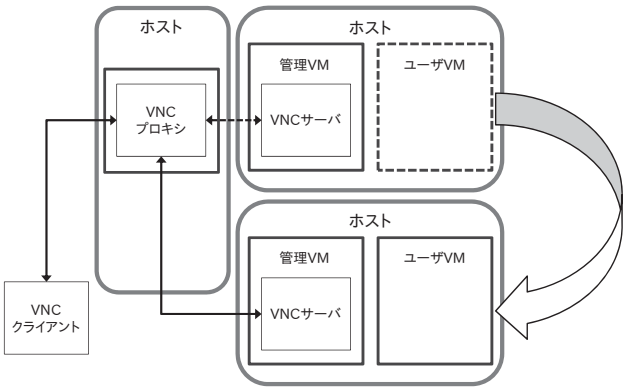

図 2 VNC プロキシを用いた解決手法

ホストに対しても特定の IP アドレスやポートにのみアクセスを許可するように，クライアント側のファイアウォールにルールを設定することが増えてきている．マイグレーションに対応するためには，クラウド内の管理 VM で使われている IP アドレスすべてと VNC サーバが使う可能性があるポート番号の範囲全体をファイアウォールで許可する必要があり，セキュリティが低下する．

2.3 既存のマイグレーション対応

マイグレーション時に帯域外リモート管理を継続する方法として，VNC プロキシサーバを用いる方法が挙げられる．この手法においては**図 2** のように VNC 用のプロキシサーバを稼働させ，ユーザは VNC クライアントからこの VNC プロキシを経由して VNC サーバに接続する．ユーザ VM 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 で動作する VNC サーバへ接続を切り替えることによって，帯域外リモート管理を継続させることができる．さらに，マイグレーション後も VNC プロキシの IP アドレスとポート番号は変わらないため，ファイアウォールのルールを最小限にすることができる．しかし，VNC プロキシがマイグレーション中に接続を切り替える際に送信中のデータおよび VNC サーバで処理が終わっていないデータに関しては，すべて破棄されてしまう．また，VNC プロキシが単一障害点になる可能性もある．

別の方法として，SPICE [4] を用いる方法が挙げられる．SPICE は VNC と同様のリモートデスクトップ環境である．VM のマイグレーション時には，**図 3** のようにマイグレーション元の SPICE サーバが SPICE クライアントにマイグレーション先の情報を通知する．その後，クライアントはマイグレーション先にリモート接続を切り替えることができる．そのため，マイグレーション時においても，帯域外リモート管理を継続させることが可能である．しかし，マイグレーション時に IP アドレスとポート番号が変更されるため，クライアント側のファイアウォールで広範

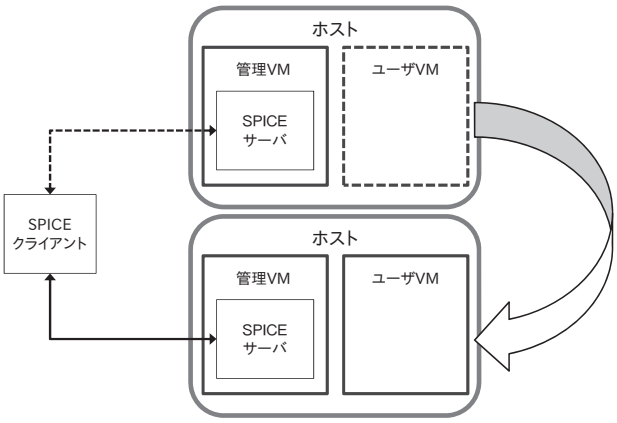

図 3 SPICE を用いた解決手法

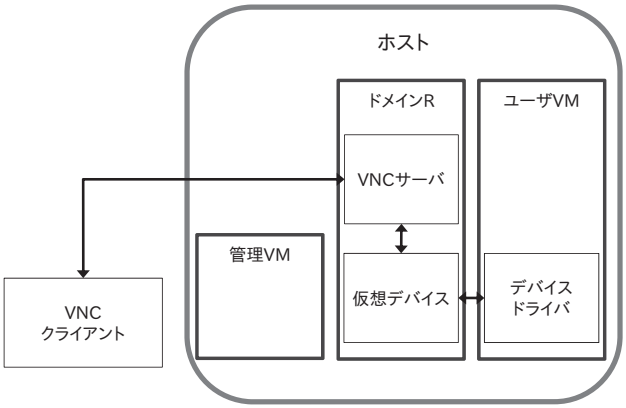

図 4 D-MORE のシステム構成

囲な IP アドレスとポート番号を許可する必要がある．また，SPICE 標準の *semi-seamless migration* では，マイグレーション時にデータが失われる可能性がある．

3. D-MORE

この問題を解決するために，本稿では，帯域外リモート管理の継続が可能なマイグレーションを実現するシステム *D-MORE* を提案する．D-MORE では，**図 4** のように，従来，管理 VM 上で動作していた VNC サーバおよび仮想デバイスのうち仮想キーボード，仮想マウス，仮想ビデオカードをリモート管理用の専用 VM であるドメイン R 上で動作させる．そして，ユーザ VM のマイグレーション時にはドメイン R も同時にマイグレーションする．この際に，D-MORE がドメイン R の仮想デバイスとユーザ VM 内のデバイスドライバ間の接続を維持する．また，VNC クライアントとドメイン R の VNC サーバ間の接続はネットワークレベルで維持される．このようにして，帯域外リモート管理におけるリモート接続を維持する．

D-MORE では，ドメイン R 上で動作する VNC サーバを経由してユーザ VM に間接的にアクセスすることで帯域外リモート管理を行う．ドメイン R で動作する仮想デバイスとユーザ VM のデバイスドライバ間の通信は共有メモリと仮想割り込みを用いて行われる．VNC クライアントから送られた入力情報は，ドメイン R の VNC サーバを経由して仮想デバイスに送られる．ユーザ VM で準仮想化デバイスドライバが用いられている場合，仮想キーボードや仮想マウスは入力情報を共有メモリ上のバッファに格納し，仮想割り込みを用いてユーザ VM に通知する．画面出力に関しても同様に，ユーザ VM のデバイスドライバが共有メモリ上のフレームバッファを更新し，仮想割り込みを用いて仮想ビデオカードに通知する．画面の更新情報は VNC サーバを経由して VNC クライアントに送信される．

D-MORE はマイグレーション時にドメイン R とユーザ VM の間の共有メモリと仮想割り込みチャネルを透過的に維持する．そのため，ドメイン R 上で動作している VNC サーバや仮想デバイスはマイグレーションを意識する必要がない．マイグレーション後も同じメモリアドレス，割り込みチャネルを用いてユーザ VM にアクセスすることができる．ドメイン R とユーザ VM をマイグレーションする際には，D-MORE が同期を取りながら同時にマイグレーションを行う．ドメイン R はユーザ VM のメモリを読み書きする必要があるため，ドメイン R が稼働している間は必ずユーザ VM が稼働した状態になるようにする．

D-MORE では，マイグレーション中に帯域外リモート管理の入力情報が失われることはない．ドメイン R 上で動作している VNC サーバおよび仮想デバイスで処理中のデータに関しては，ドメイン R とともにマイグレーションされるため保持することができる．VNC クライアントから VNC サーバに送信中のネットワーク上のデータはネットワークの切り替え時に失われる可能性があるが，TCP により再送される．これにより，マイグレーション用のプロトコルを用いることなく，入力情報を保持することができる．また，ユーザ VM ごとに専用のドメイン R が用意されるために，単一障害点にならないという利点もある．

さらに, D-MORE では, マイグレーション後も VNC サーバの IP アドレスおよびポート番号が変わらない．VNC サーバが動作しているドメイン R の IP アドレスはマイグレーション後も同一であるためである．そのため，クライアント側のファイアウォールでは，固定の VNC サーバの IP アドレスとポート番号だけを許可すればよい．一方，D-MORE ではドメイン R 用にグローバル IP アドレスを新たに一つ割り当てる必要がある．この問題は，ドメイン R にプライベート IP アドレスを割り当てて，NAT 変換を行うことで解決することができる．VNC サーバ用のポートへのアクセスだけをユーザ VM のパブリック IP アドレスからドメイン R のプライベート IP アドレスに変換すればよい．

4. 実装

我々は D-MORE を Xen 4.1.3 [1] に実装した．Xen においては管理 VM はドメイン 0，ユーザ VM はドメイン U となる．ドメイン U 内で動作させるゲスト OS として準仮想化 Linux 3.2.45 を対象とした．

4.1 VNC サーバと仮想デバイス

ドメイン R では，ドメイン 0 内の VNC サーバの機能を分離し，ドメイン R 内で動作させられるようにした．ドメイン R の実装については 4.2 節で述べる．Xen では，VNC サーバは QEMU と呼ばれるエミュレータの中に組み込まれている．QEMU から VNC サーバの機能を分離するのは容易ではなかったため，RFBProxy [3] を基に VNC サーバを作成した．現在の実装では，キーボードとマウスのイベントを処理することができる．画面関連のイベントについては，ドメイン 0 上の既存の VNC サーバに転送して処理している．

D-MORE では，ドメイン 0 内の仮想デバイスのエミュレーション機能についても分離し，ドメイン R 内で動作させられるようにした．現在の実装では，キーボードとマウスの仮想デバイスに対応している．これらの仮想デバイスは**図 5** のように，VNC サーバから入力を受け取り，ドメイン U 内のバッファに書き込む．このバッファは I/O リングと呼ばれ，準仮想化デバイスドライバに入出力情報を受け渡すために用いられる．その後，仮想デバイスはイベントチャネルを使ってドメイン U にイベントを送り，入力があることを通知する．これにより，ドメイン U 内のデバイスドライバは従来通りに，I/O リングから入力情報を取り出すことができる．

ドメイン R 内の仮想デバイスは，I/O リングやイベントチャネルの情報をドメイン 0 経由で取得する．ドメイン R からドメイン U 内の I/O リングにアクセスするには，I/O リングの置かれているメモリの情報（MFN）が必要になる．また，イベントチャネルを確立するにはドメイン U 側のポート番号が必要になる．これらの情報はドメイン U の起動時にドメイン 0 に送られるため，ドメイン R は仮想デバイスの作成時にドメイン 0 から情報を取得する．

4.2 ドメイン R

ドメイン R はドメイン M [2] を拡張して開発した．ドメイン R は従来，ドメイン 0 のみが有していたドメイン U のメモリにアクセスする特権を持った VM である．Xen のスタブドメイン [5] の機能を利用し，OS や VMM のアクセス制限を変更することによって，指定した VM のメモリへのアクセスを可能とした．ドメイン R とドメイン U の関連づけはドメイン 0 で行う．この機能を用いることにより，ドメイン R はドメイン U の I/O リングが置かれたメモリページをマップし，読み書きを行うことができる．

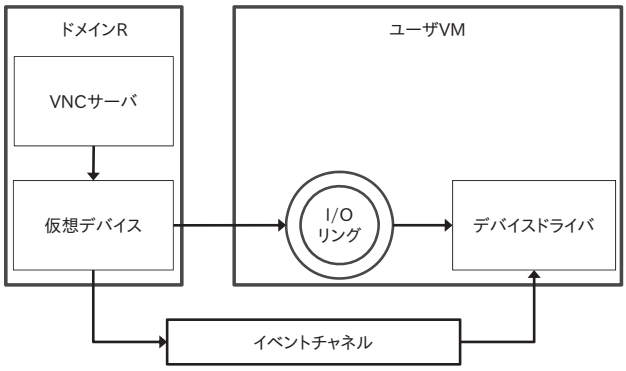

図 5 I/O リングとイベントチャネル

ドメイン R はドメイン 0 と違い，マイグレーションすることができる．管理対象のドメイン U のメモリマップを行ったままドメイン R のマイグ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管理対象のドメイン U のメモリページのマップ状態を自動的に復元する．ドメイン U のメモリページをマップしている時には，対応するページテーブルエントリの監視ビットをセットする．マイグレーション先では監視ビットがセットされていればドメイン U のメモリを再マップする．

ドメイン R では，ドメイン U との間で，イベントチャネルを確立する機能も提供する．イベントチャネルは，ある VM でバインドしたポート番号を取得し，それを指定して接続することで確立することができる．しかし，ドメイン U の既存のデバイスドライバはドメイン 0 を指定してバインドを行うため，ドメイン 0 しか接続を行うことができなかった．そこで，このドメイン U に関連づけられたドメイン R からであればドメイン U のポートに接続することができるように，VMM への拡張を行った．これによって，ドメイン U に修正を加えずにドメイン R との間にイベントチャネルを確立することができる．

D-MORE はドメイン R とドメイン U のマイグレーション時に，イベントチャネルを維持する必要がある．イベントチャネルの情報は VMM 内で管理されており，マイグレーションによって失われる．マイグレーション後にドメイン U のデバイスドライバはマイグレーションを認識して再度バインドを行うためポート番号が変更される．一方，ドメイン R の仮想デバイスはマイグレーションを認識しないため，再接続を行わない．この問題を解決するために，VMM 内でドメイン R のポートとドメイン U の新しいポートを自動的に再接続することができる機能を実装する必要がある．この機能については，現在未実装である．

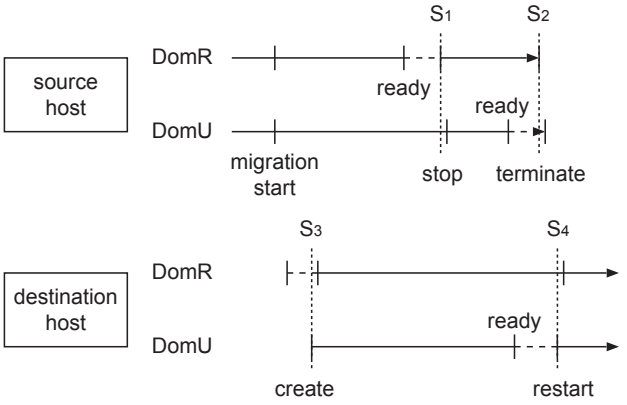

図 6 マイグレーション時の同期

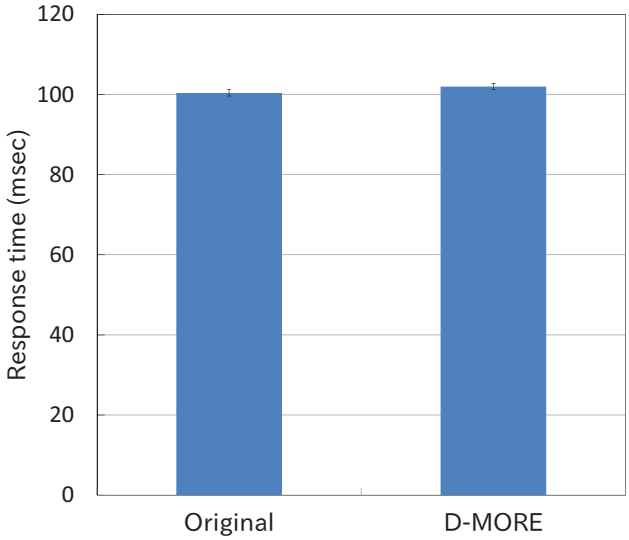

図 7 キーボード入力の平均レスポンスタイム

4.3 同時マイグレーション

ドメイン R が実装のベースとしたドメイン M は，マイグレーション中に監視対象のドメイン U の監視が途切れないようにするために，同期を取りながら同時にマイグレーションを行う機能を提供している．マイグレーション元においては，監視対象のドメイン U が稼働している間，監視を継続する必要があるため，ドメイン M はドメイン U が停止するまで待機する．一方，ドメイン M はマイグレーション中に監視対象のドメイン U の情報を得る必要があるため，ドメイン M が終了するまでドメイン U を停止させて待機させる．マイグレーション先において，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のドメイン U の情報を必要とするため，ドメイン U が生成されるまで待機する．さらに，ドメイン M が稼働していない状態で監視対象のドメイン U を稼働させた場合は監視することができないため，ドメイン M が再開されるまでドメイン U を停止させて待たせる．このように，ドメイン U が稼働している間は，ドメイン M が常に稼働しているようになっている．

しかしながら，D-MORE の場合には，ドメイン R が稼働している間はドメイン U が常に稼働しているようにする必要がある．ドメイン U が停止した状態で，ドメイン R の仮想デバイスがドメイン U の I/O リングに書き込みを行うと，そのデータは失われてしまう可能性があるためである．その一方で，ドメイン R は VNC クライアントからのリクエストを処理するため，できるだけ停止しないことが望ましい．

そこで，ドメイン R とドメイン U の両方がライブマイグレーションの最終段階に入った時点で，ドメイン R，ドメイン U の順に停止させ，マイグレーション先ではドメイン U，ドメイン R の順に再開させる．マイグレーションにおけるドメイン R とドメイン U の同期は**図 6** のようになる．

5. 実験

D-MORE を用いた場合のキーボード入力の応答時間を測定するための実験を行った．実験には，Intel Xeon E3-1270 3.40GHz の CPU を搭載したマシンを VM 用と VNC クライアント用に 1 台ずつ用意し，ギガビットイーサネット・スイッチで接続した．VM 用のマシンにおいては，仮想化ソフトウェアとして Xen 4.1.3 を用い，ドメイン 0 で Linux 3.2.0，ドメイン U とドメイン R で Linux 3.2.45 を動作させた．このマシンは 8GB のメモリを搭載しており，ドメイン 0 には 3.75GB，ドメイン U には 256MB のメモリをそれぞれ割り当てた．クライアントマシンでは，VNC クライアントとして TigerVNC を Linux 3.2.0 上で動作させた．

キーボード入力一回あたりのレスポンスタイムを D-MORE と従来のシステムで比較した．VNC クライアントでキーボード入力を行い，文字が表示されて画面が書き換わることで送られてくるフレームバッファ変更要求をクライアントが受け取るまでの時間を測定した．キーボード入力を 100 回行った際の実験結果を**図 7** に示す．D-MORE は従来のシステムと比較して 1.6ms の遅延が見られた．ただし，D-MORE の現在の実装では，画面更新要求はドメイン 0 の VNC サーバに転送して処理している．この結果から，現状では，D-MORE において，ドメイン R 経由で帯域外リモート管理を行うオーバーヘッドはほとんど発生しないことが確認された．

6. 関連研究

SPICE [4] は KVM 用に開発されているリモートデスクトップ機構である．SPICE は管理 VM 経由の帯域外リモート接続であっても，マイグレーション時にサーバがクライアントにマイグレーション先のホストを通知すること

によって，接続を切り替えることができる機能を持っている．そのため，マイグレーションを行った場合であっても，リモート接続が切断されることがなく，リモート管理を継続させることができる．ただし，SPICE が従来からサポートする *semi-seamless migration* では，マイグレーション時にデータが失われる可能性がある．SPICE が新しくサポートした *seamless migration* では，クライアントは送信中のデータを全て送信し終えた後に通信を停止し，マイグレーション先のサーバに接続を切り替えて，通信を再開するため，送信中のデータが失われることはない．いずれにせよ，マイグレーション時に SPICE サーバの IP アドレスとポート番号が変更されるため，クライアント側でのアクセス制限を行いにくい．また，現時点で VNC と比較して普及率が低く，利用できるクライアントの種類が限られている．

Stub Domains [5] は，Xen 3.3 から搭載された，VNC サーバ（QEMU）を動作させることができる特殊な仮想マシンである．Xoar [6] でも，QEMU を QemuVM と呼ばれる専用の VM で動作させる．これらは，専用 VM の中で小さな OS である Mini-OS を動かすことによって，VM が攻撃を受ける可能性を低くすることを目的として開発されたものである．VNC サーバを独立させる点においては本手法と同じであるが，Stub Domains および Xoar の専用 VM はマイグレーションさせることができないため，これらの VM を用いて，帯域外リモート管理の継続を実現することはできない．

ドメイン M [2] は，IDS をオフロードして監視対象 VM を監視することができる仮想マシンである．オフロードされた IDS によって行われる監視を継続したままマイグレーションすることができる．ドメイン M は VM のメモリの監視に加え，ディスクやネットワークの監視を継続することもできる．D-MORE においては，ドメイン M を拡張してドメイン R を開発している．ドメイン R 内で仮想デバイスを動作させられるようにするには，イベントチャネルへの対応および，同時マイグレーションのタイミングの修正が必要となる．

FBCrypt [7] は，帯域外リモート管理を行う際にクラウドの管理者への入出力情報の漏洩を防ぐシステムである．キーボード入力はユーザの VNC クライアントで暗号化し，クラウド側の VMM で復号化する．画面出力は VMM で暗号化し，VNC クライアントで復号化する．管理 VM で取得できる入出力情報は暗号化されており，復号化した入出力情報には管理 VM からアクセスできないようになっている．FBCrypt は D-MORE にも適用することが可能である．

VMware vSphere Hypervisor（ESXi) [8] では VMM 内で VNC サーバを動作させており，VNC クライアントは VMM 経由でユーザ VM の帯域外リモート管理を行うことができる．このため，ユーザ VM のマイグレーション時にはリモート接続が切断されてしまう．

7. まとめ

本稿では，ユーザ VM のマイグレーション時においても帯域外リモート管理の継続を可能にするシステム D-MORE を提案した．D-MORE では，管理 VM から VNC サーバと仮想デバイスを切り離し，マイグレーション可能なリモート管理専用の VM であるドメイン R で動作させる．ユーザ VM とドメイン R を同時にマイグレーションすることにより，帯域外リモート管理においてもユーザ VM へのリモート接続を維持することができる．D-MORE を Xen に実装し，ドメイン R 上の VNC サーバを経由してユーザ VM に入力を行えていることを確認した．さらに，D-MORE のオーバーヘッドが現状では十分小さいことを確認した．

現在のところ，ユーザ VM からの画面出力に対応していないため，VNC サーバで画面更新要求を処理できるようにし，仮想ビデオカードを実装することが今後の課題である．また，マイグレーション時にイベントチャネルを維持できるようにし，同期を取れるようにする必要がある．現在は準仮想化のみに対応しているが，完全仮想化への対応も予定している．

参考文献

[1] Barham et al, Xen and the Art of Virtualization, In Proceedings of the 19th Symposium on Operating Systems Principles，pp.164-177，2003.

[2] 宇都宮寿仁，光来健一．VM マイグレーションを可能にする IDS オフロード機構．第 28 回日本ソフトウェア科学会大会, 2011.

[3] rfbproxy, `http://rfbproxy.sourceforge.net/` (参照 2013/07/04).

[4] Spice - Home page, `http://www.spice-space.org/` (参照 2013/07/04).

[5] StubDom - Xen, `http://wiki.xen.org/wiki/StubDom` (参照 2013/07/04).

[6] P. Colp, M. Nanavati, J. Zhu, W. Aiello, G. Coker, T. Deegan, P. Loscocco, and A. Warfield. Breaking Up is Hard to Do: Security and Functionality in a Commodity Hypervisor. In Proceedings of the 23rd ACM Symposium on Operating Systems Principles, pp.189-202, 2011.

[7] T. Egawa, N. Nishimura, and K. Kourai. Dependable and Secure Remote Management in IaaS Clouds. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science, pp.411-418, 2012.

[8] VMware Inc.: VMware vSphere Hypervisor, `http://www.vmware.com/` (参照 2013/07/04).