属性ベース暗号による認証を用いたグローバルライブマイグレーション支援システムの開発

加森 剛徳[1,a)]　林 健汰[1]　前田 香織[1]　近堂 徹[2]　相原 玲二[2]

概要：コンピュータの仮想化技術やネットワークの広帯域化により，通信セッションを維持したままインターネットに接続された物理ホスト間で仮想マシン（VM）のグローバルライブマイグレーションが可能になっている．しかし，グローバルライブマイグレーションでは異なるクラウドプロバイダが提供する任意のクラウドで多数の利用者が資源を共有するので，それを前提としたライブマイグレーションの権限制御機構が求められる．これに対して本研究では，複数のクラウドプロバイダ間においても VM 利用者の権限に基づいた安全なライブマイグレーションができるような支援システムを開発する．この支援システムではマイグレーションの権限を利用者の属性によって認証する暗号文ポリシー属性ベース暗号を用いる．また，支援システムは異なるプロバイダのマイグレーションでもセッションを維持するため，移動透過通信機構も有する．本稿では支援システムの開発について述べる．また，実装したプロトタイプシステムを用いて，追加した認証機構や移動透過通信機構のオーバヘッドの実験的評価を行い，支援システムの実用性について述べる．

キーワード：仮想化技術，ライブマイグレーション，属性ベース暗号，移動透過通信

Development of a Global Live Migration Support System using Authentication Mechanism based on Attribute-Based Encryption

Yoshinori Kamori[1,a)]　Kenta Hayashi[1]　Kaori Maeda[1]　Tohru Kondo[2]　Reiji Aibara[2]

Abstract: Development of computer virtualization technology and broadband network enables global live migration. This migration allows different physical hosts connected to the Internet maintaining communication sessions. However, an authority authentication mechanism is required in global live migration since many users share any resources over clouds of different cloud providers. In this research, we develop a authentication system for secure live migration based on the authority of VM users among multiple cloud providers. In this system, we use a Ciphertext Policy Attribute-Based Encryption for authentication of the migration according to users' attributes. Also, the system supports a IP mobility mechanism to maintain sessions even if the VM migrates over clouds of different providers. This paper describes development of this system and show experimental evaluation on the overhead caused by the authentication mechanism and IP mobility mechanism using the implemented prototype system. Through the evaluations, we describe the usefulness of the system.

Keywords: Virtualization technology, Live migration, Attribute-based encryption, IP mobility

1. はじめに

近年，コンピュータの仮想化技術が進展している．仮想化技術では，仮想マシン（以降，VM: Virtual Machine）を管理する制御プログラム（以降，ハイパーバイザ）が，

[1] 広島市立大学大学院情報科学研究科
Graduate School of Information Sciences, Hiroshima City University
[2] 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University
[a)] kamori@v6.netsci.info.hiroshima-cu.ac.jp

ハードウェアと OS 間に介入した構造をもつ．仮想化技術の中でも VM のリソースおよびネットワーク環境を維持したまま，別の物理ホスト（以降，VMS : Virtual Machine Server）に移動させるライブマイグレーションも可能になっている．このとき，インターネットに接続された任意の VMS 上にセッションを維持したまま VM を移動することを可能にするグローバルライブマイグレーション技術の研究開発も進んでいる [1][2].

多数の VM による並列分散処理や VM とクライアントデバイスの連携処理が普及すると，異なるクラウドプロバイダが提供する任意のクラウド上での VM 動作が必要となり，アプリケーション特性に応じて適切なサイトへ VM を動的に移動させることが求められる．例えば，仮想デスクトップ環境（以降，VDI : Virtual Desktop Infrastructure）を例に考えると，VM を利用するユーザ（以降，VM 利用者）が，通信遅延の少ない状態で利用したいなどの理由で VM のライブマイグレーションを要求する可能性が考えられる．

しかし，多くの場合複数クラウド間のグローバルライブマイグレーション環境はインターネット上に構築され多数の利用者により資源が共有されるため，ライブマイグレーションの実行権限を適切に管理する必要がある．さらに，VM 利用者の増加に伴い認証用鍵の運用コストが大きくなるという問題も考慮しなければならない．

そこで本研究では， VM 利用者の権限に基づき複数のクラウドプロバイダ間で VM をマイグレーションさせることが可能なライブマイグレーション支援システムを開発する．システムでは，移動元および移動先の VMS で，属性とポリシーによる VM 利用者の認証を行い，VM 利用者の権限に基づきマイグレーション操作権限を提供することで安全性の問題を解決し，その認証において暗号文ポリシー属性ベース暗号（Cipher text Policy Attribute Based Encryption, 以降 CP-ABE）[3] を用いることでライブマイグレーションの権限をもつ VM 利用者が増えた時の鍵の運用コストの問題を解決する．また，異なるネットワークに位置する VM がライブマイグレーションした際のネットワークの再設定に伴う通信遮断の発生を，移動透過通信技術 [4] を用いることで解決する．

本論文の構成は以下の通りである．2 で関連研究を述べ，3 で VM のライブマイグレーションにおける権限管理への要求要件を整理する．4 で認証付きのライブマイグレーション支援システムの開発について述べ，5 でその評価を示す．最後に 6 でまとめと今後の課題について述べる．

2. 関連研究

2.1 仮想マシンのグローバルライブマイグレーション

ライブマイグレーションでは稼働中の VM の RAM のデータや仮想 CPU のレジスタ情報などを転送することで，VM 内部のアプリケーションの動作状態を保持したまま異なる VMS へ移動させる．このとき，ハイパーバイザは同一ネットワーク上でのマイグレーションを想定しているため，WAN を経由する場合などマイグレーション前後で VM が接続するネットワークが異なるとアプリケーション層で確立されたセッションが切断されてしまう．

この問題の解決方法として，[5] では VPN を使って WAN 上の複数データセンターにまたがった仮想的なリソースを同一ネットワークリソースとして扱う．同じく同一ネットワーク上のリソースとして扱う方法としては L2 ネットワークを拡張する LISP[6] を用いたライブマイグレーションも提案されている [7].

IP アドレスをアプリケーションで用いる静的に付与されたホームアドレスと，実際のネットワーク接続用のモバイルアドレスに分離し，VM のマイグレーション時にホームアドレスと現在使っているモバイルアドレスの対応付けの機構を VM や通信経路中のサーバに持たせることによって，見かけ上マイグレーション前後で IP アドレスが変化しない IP 層における移動透過通信機能（以降，IP モビリティ）を用いる方法もある．筆者らは本方式をグローバルライブマイグレーションとよんでいる． [1] は IP モビリティとして MAT[4] を，[2] は MIPv6[8] を用いたマイグレーション支援のシステムを開発している．

2.2 グローバルライブマイグレーションにおける課題

2.1 のグローバルライブマイグレーションに関する既存研究では，VM に対する IP モビリティのみが提供され，VM 利用者に対するマイグレーションの操作に関わる権限管理や認証などがサポートされていない．そのため，VM 利用者に対して権限に基づいたライブマイグレーションの操作を提供するための制御機構が必要であるが，VM 利用者との認証において公開鍵認証を用いると，利用者毎に鍵の管理が必要となり，利用者数が多くなったときの鍵の管理コストに関する考慮も必要となる．

現在，ライブマイグレーションの実行は，ハイパーバイザの管理を支援する libvirt[9] 等のソフトウェア（以降，仮想化管理機構）を用いて VM が動作する VMS の管理者が行うことが一般的であるが，仮想化管理機構は VMS の管理者が使うことを想定しているため，前述のような利用者の権限に基づいた制御機構はもっていない．

3. ライブマイグレーションの権限管理

VM のライブマイグレーションには前述のような課題を解決するためのマイグレーション時の VM 利用者の権限管理や認証のための鍵管理の機構を提供しなければならない．本研究では暗号文ポリシー属性ベース暗号（CP-ABE）を用いて，ライブマイグレーション時に VM 利用者が VMS と認証を行うことで問題を解決する．

3.1 権限管理における設計方針

本研究では，VM 利用者に対してライブマイグレーションのみの権限を与え，実行時に移動元と移動先の VMS 上で動作する開発システムと VM 利用者が認証を行うことで，複数のクラウドプロバイダ間で VM を VM 利用者の権限に基づきマイグレーションさせることを可能とする．

ここで，マイグレーションにおいて必要な権限管理について検討する．一般的にライブマイグレーションの実行には VM が動作している VMS 上の仮想化管理機構を操作する権限が必要である．しかしながら，マイグレーションを実行したい VM 利用者に対して権限を与えると，2.2 で述べた課題が生じ，セキュリティ面で安全性が著しく低下する．そのため，移動元 VMS とユーザ間において，任意の VM に対して VM 利用者の権限にてライブマイグレーション操作の可否を認証する必要がある．本稿では，このように移動元 VMS と行う認証を「LM 元認証」とよぶ．

また，移動先 VMS はマイグレーションを実行する VM 利用者ごとにマイグレーション受け入れ制限をかけることができないため，移動先 VMS の意図しないユーザが VM をライブマイグレーションさせてきてしまうという問題が発生する．そのため，移動先 VMS と VM 利用者間において，VM 利用者の権限にてライブマイグレーションを受け入れる権限があるか認証する必要がある．本稿では，このように移動先 VMS と行う認証を「LM 先認証」とよぶ．

3.2 暗号文ポリシー属性ベース暗号（CP-ABE）

ユーザ単位の認証は VM 利用者数が増加したときの認証鍵の管理コストも問題となる．一般的にクライアントとサーバ間における認証では，公開鍵と秘密鍵が 1 対 1 の関係となる RSA 暗号などが使用されているが，VM 利用者ごとの認証鍵の登録や管理を行うための運用コストの問題がある． そのため，開発するシステムでは CP-ABE[3] を用いる．CP-ABE は公開鍵と秘密鍵にアクセス権の機能を持たせることができることが特徴のひとつである．

既存の公開鍵認証（RSA 暗号）の場合，ユーザごとに公開鍵を追加する必要があるが，CP-ABE は公開鍵と秘密鍵が一対多の関係になっているため新たな公開鍵の登録の必要がなく，鍵管理も容易である．また，秘密鍵の属性に有効期限を表す数値（例：有効期限 = 2018/03/31）をもたせ，公開鍵のポリシーに「有効期限 ≤ 現在の日時」のような条件を含めることで期限内の鍵の失効が可能である．

最初に鍵発行局でマスター秘密鍵とマスター公開鍵が生成される．鍵発行局はマスター秘密鍵と復号側の属性集合より秘密鍵を生成し，マスター公開鍵と秘密鍵を復号側に配布する．生成した秘密鍵とマスター公開鍵は復号処理に，マスター公開鍵は暗号化処理に利用する．暗号化側はマスター公開鍵にポリシーを埋め込んだ公開鍵を生成し，公開鍵で平文を暗号化する．暗号文を復号するには，復号

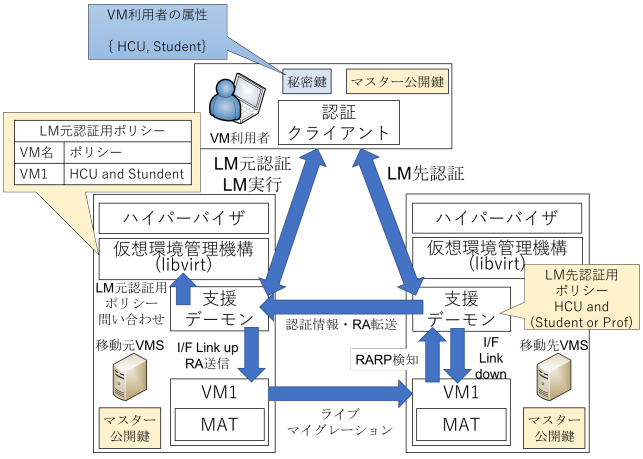


図 1 支援システムの構成図
Fig. 1 System configuration

側でマスター公開鍵と秘密鍵を使う．CP-ABE では，公開鍵のポリシー（例：(情報科学部 AND 学年≧ 3) OR 教員）を秘密鍵の属性集合（例：情報科学部，情報工学科，学年=4）が満たすとき，秘密鍵によって暗号文が復号される．

CP-ABE はユーザが暗号化時にアクセス条件として，数値比較（例：学年≧ 2 AND 学年≦ 4）などの設定が可能であり，柔軟にアクセス条件を設定することが可能であるため，クラウド上の資源管理に CP-ABE を使う既存研究がいくつか行われている．[10] ではオンラインストレージのファイル共有システムに CP-ABE を適用しているが，マイグレーションに使用しているものはない．

4. 認証付きライブマイグレーション支援システム

3 での検討をもとに設計をした，権限制御機構を有するライブマイグレーション支援システム（以降，本システム）の開発について述べる．

本システムは，クラウドプロバイダが VM 利用者の権限に基づいて，ライブマイグレーションの操作のみを VM 利用者に対して提供すること，また，その際に認証時間がライブマイグレーションの処理時間に大幅な影響を与えないこと，加えて，ライブマイグレーション時に VM 利用者と VM 間のセッションを維持することを目的とする．その目的を実現するために，CP-ABE を用いた認証機能と，IP モビリティ機能を導入する．

4.1 システムの構成

開発したライブマイグレーション支援システムの全体構成を図 1 に示す．本システムの実装においてハイパーバイザとして KVM と qemu[11] を用い，仮想化管理機構は libvirt API を用いた．マイグレーション支援デーモン（以降，支援デーモン）は，VMS 上で動作し，VM 利用者との認証機能と IP モビリティ機能を提供する．また，認証ク

ライアントは VM 利用者のコンピュータ上で動作し，支援デーモンとの認証機能と，ライブマイグレーションの実行機能を提供する．図 1 の属性とポリシーはこれらの関係性の例を示している．ここで，秘密鍵は KGC が VM 利用者の属性を証明するもので，公開鍵はそれを確認するための鍵であり，認証はその 2 つを用いて秘密鍵の属性が公開鍵のポリシーに適合することを支援デーモンが証明するための作業となる．

支援デーモンが移動元と移動先の VMS において動作しており，VM 上では MAT[4] が動作している．また，ライブマイグレーションを実行するユーザのマシンには認証クライアントと MAT が動作しており，VM に対する通信相手ノード（以降，CN: Correspondent Node）となる．プロトタイプシステムの実装に用いた MAT の実装は IPv6 のモビリティ機能を提供するため，今回のシステムは IPv6 ネットワーク間のマイグレーションを対象としている．本システムを使用する際の前提条件を以下に示す．

- 移動先 VMS のネットワークでは Router Solicitation（以降，RS）により，プレフィクスオプションを含む Router Advertisement（以降，RA）が取得可能である
- 予め鍵発行局から秘密鍵とマスター公開鍵の交付を受けている
- 移動元と移動先の VMS において，libvirt daemon 同士の認証に必要な認証の設定（公開鍵やサーバ証明書等）が完了しており，ライブマイグレーションの実行が可能である
- libvirt が管理する VM の定義ファイル内（XML 形式）のメタデータノードに LM 元認証用ポリシーが記述されている

4.2 提供する機能

4.2.1 CP-ABE を用いた認証と権限管理

本システムではライブマイグレーションを VMS の外部から安全に実行するために，ライブマイグレーションの可否を，実行するユーザごとに判断する．認証は，3.1 での検討の通り，LM 元/先認証を CP-ABE を用いて行う． CP-ABE の処理には [3] の著者らが開発した cpabe toolkit[12] という CP-ABE のライブラリを使用した．このライブラリでは，CP-ABE の処理において秘密分散法を利用することで，AND や OR で表現されるポリシーを用いた暗号化と属性集合を用いた復号の処理を実現している．

CP-ABE を用いた認証では，VM 利用者が自身の属性が埋め込まれている秘密鍵を保持しており，移動先/移動元 VMS がマスター公開鍵を保持している．移動先/移動元 VMS は LM 先/LM 元認証用ポリシーを用いて公開鍵を生成し，その公開鍵により暗号文を生成する．VMS 毎に設定されている LM 先認証用ポリシーは LM 先認証で用いられ，どの属性を持つ VM 利用者が VM を稼働させることができるかを示す．また，VM 毎に設定されている LM 元認証用ポリシーは LM 元認証で用いられ，どの属性を持つ VM 利用者がその VM に対してライブマイグレーションを実行できるかを示す．ここで，3.2 に記述の通り，ポリシーに適合する属性が埋め込まれた秘密鍵を保持する VM 利用者のみが認証に成功する．各認証で用いられる認証用ポリシーを適切に設定することで，ライブマイグレーションの実行が可能な VM 利用者を指定することができる．

4.2.2 IP モビリティ

本システムではグローバルライブマイグレーション時に，VM が異なるネットワーク間をマイグレーションすることで発生する VM 利用者と VM 間での通信途絶を解決するために，IP モビリティアーキテクチャとしての MAT[4] を用いて IP モビリティをサポートする．

MAT は移動ノードや通信相手ノードに専用の IP モビリティ機構を動作させる．ネットワーク上の IP アドレス（モバイルアドレス）とアプリケーションで使用する IP アドレス（ホームアドレス）を分離し，そのアドレス管理をアドレス変換テーブルで管理する．このテーブルはアドレス管理サーバ（Internet Address Mapping Server, 以降 IMS）とともに移動ノードや通信相手ノードも管理することで，通信時にはアドレス変換用の仲介サーバを経由することなく，移動ノードと通信相手ノードが直接通信できる．

しかし，MAT ではノードの I/F の削除，またはリンクダウンの検知によりネットワークの移動を検知しているため，VM のマイグレーション時に VM 自身でネットワーク移動の判断ができず，異なるネットワークへのマイグレーション時の通信途絶時間が長くなる．

そこで，VM を 2 つのネットワーク I/F を持つデュアル I/F 構成としておき，マイグレーションの前処理としてマイグレーション先のネットワークから RA を取得し，取得した RA によりセカンダリ I/F へマイグレーション先のプレフィクスのアドレスを事前付与する．この前処理により，VM のセカンダリ I/F にはマイグレーション先のプレフィクスのアドレスが付与され，IMS へマッピング情報の更新がネットワークを移動する前に行われるため，本来ライブマイグレーション後に行わなければならない IP モビリティに関する処理を削減できる．後処理として，ライブマイグレーションが完了した後に，ライブマイグレーション前のプレフィクスのアドレスが設定されているプライマリ I/F をリンクダウンすることで VM がセカンダリ I/F を用いて通信を行うようになる．この後処理により，VM 上で動作する MAT がライブマイグレーションによるネットワークの移動を検知することが可能となる．プライマリ I/F をリンクダウンするトリガーとして，ライブマイグレーション後に移動先 VMS で発生する RARP（Revers Address Resolution Protocol）を用いた．

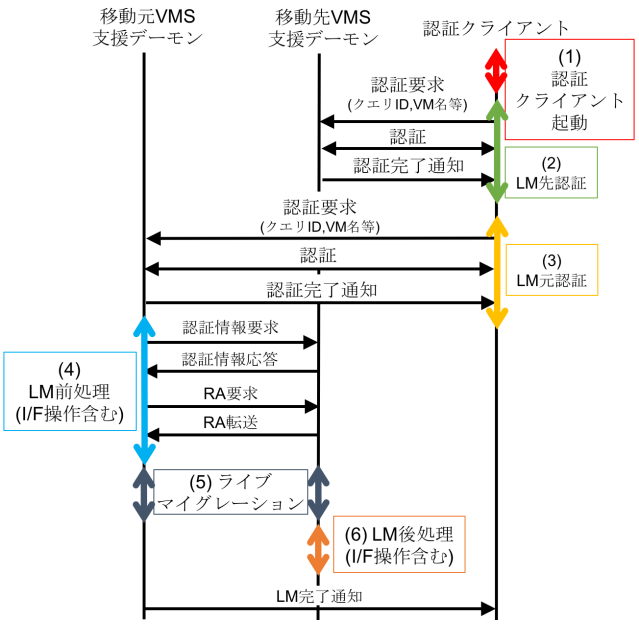
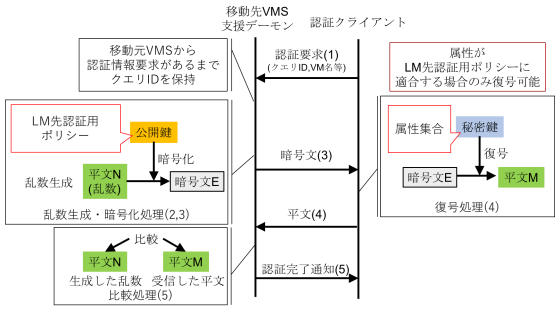
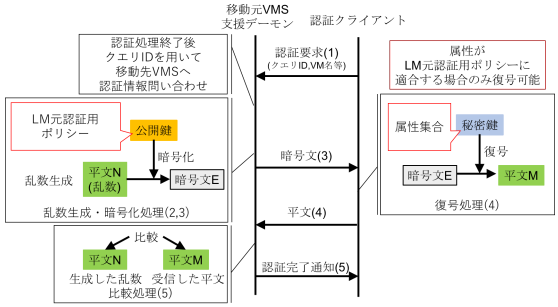


図 2　支援システムの動作フロー

Fig. 2　Processing flow of the system



(a) LM 先認証



(b) LM 元認証

図 3　認証部分の動作フロー

Fig. 3　Authentication flow

4.3　動作フロー

本システムの全体動作フローを図 2 に示す．ここでは図 1 のように認証クライアントからの要求を受け，移動元 VMS から移動先 VMS へ VM がライブマイグレーションを行う場合を考える．また，この動作フローにおける通信は全て TLS 通信を用いるものとする．

(1) 認証クライアント起動

ライブマイグレーションを要求する VM 利用者は，VM 名，移動先と移動元の VMS の IP アドレスを指定し，認証クライアントを起動する．このとき，ライブマイグレーションの要求と一対一に対応するクエリ ID が生成される．

(2) LM 先認証

図 3 の (a) に LM 先認証の詳細なフローを示す．

1) 認証クライアントは，移動元 VMS の IP アドレス，VM 名とクエリ ID を含む LM 先認証の要求を送信する．
2) 移動先 VMS の支援デーモンは図 1 の LM 先認証用ポリシーとマスター公開鍵から公開鍵を生成する．
3) 移動先 VMS の支援デーモンは乱数を用いて平文 N を生成し，LM 先認証用ポリシーが埋め込まれた CP-ABE の公開鍵を用いて平文 N を暗号化し，暗号文 E を送信する．
4) 認証クライアントは属性が埋め込まれた CP-ABE の秘密鍵を用いて暗号文 E の復号を行い，得られた平文 M を移動先 VMS の支援デーモンへ送信する．この時，VM 利用者の秘密鍵の属性が LM 先認証用ポリシーに適合する場合は平文 M が平文 N と等しくなり，ポリシーに適合しない場合は平文 M が得られず認証失敗となる．
5) 移動先 VMS の支援デーモンは平文 M を受け取ると，上記 3) で生成された平文 N と受信した平文 M を比較し，一致すると認証完了通知を送信する．平文 M が平文 N と同一であった場合のみ，秘密鍵の属性が LM 先認証用ポリシーに適合していることが証明される．
6) 移動先 VMS の支援デーモンは認証要求に含まれているクエリ ID 等の情報を，移動元 VMS の支援デーモンから認証情報要求があるまで保持しておく．

(3) LM 元認証

図 3 の (b) に LM 元認証の詳細なフローを示す．

1) 認証クライアントは，移動先 VMS の IP アドレス，VM 名とクエリ ID を含む LM 先認証の要求を送信する．
2) 移動元 VMS の支援デーモンは VM 毎に設定されている図 1 の LM 元認証用ポリシーを仮想化管理機構（libvirt）に対して問い合わせ，ポリシーとマスター公開鍵から公開鍵を生成する．
3) 移動元 VMS の支援デーモンは乱数を用いて平文 N を生成し，LM 元認証用ポリシーが埋め込まれた CP-ABE の公開鍵を用いて平文 N を暗号化し，暗号文 E を送信する．
4) 認証クライアントは属性が埋め込まれた CP-ABE の秘密鍵を用いて暗号文 E の復号を行い，得られた平文 M を移動元 VMS の支援デーモンへ送信す

る．この時，VM 利用者の秘密鍵の属性が LM 元認証用ポリシーに適合する場合は平文 M が平文 N と等しくなり，ポリシーに適合しない場合は平文 M が得られず認証失敗となる．

5) 移動元 VMS の支援デーモンは平文 M を受け取ると，上記 3) で生成された平文 N と受信した平文 M を比較し，一致すると認証完了通知を送信する．平文 M が平文 N と同一であった場合のみ，秘密鍵の属性が LM 元認証用ポリシーに適合していることが証明される．

(4) LM 前処理

1) 移動先 VMS の支援デーモンに対して認証情報要求を送信する．この要求には VM 名とクエリ ID が含まれている．
2) 認証情報要求を受け取った移動先 VMS の支援デーモンは，認証情報要求と一致する VM 名とクエリ ID の組を自身が保持しているか参照し，参照結果を移動元 VMS の支援デーモンへ認証情報応答を送信する．
3) 移動元 VMS の支援デーモンは受け取った認証情報応答を確認する．ここで，認証情報応答の内容が参照成功であれば，認証クライアントと移動先 VMS の間で LM 先認証が成功していることが確認できる．
4) 移動元 VMS の支援デーモンは，RA 取得の要求を移動先 VMS の支援デーモンに対して送信する．
5) 移動先 VMS の支援デーモンは，RS を送信し，RA のパケットを取得し，移動元 VMS の支援デーモンへ転送する．
6) 移動元 VMS の支援デーモンは，VM のセカンダリ I/F をリンクアップし，受信した RA を I/F へ送信する．

(5) ライブマイグレーション

libvirt API を用いてライブマイグレーションを実行する．

(6) LM 後処理

1) 移動先 VMS の支援デーモンが，ライブマイグレーションに伴って送出される RARP を検知する．
2) マイグレーション前のネットワークのアドレスが設定されているプライマリ I/F をリンクダウンする．

これにより，VM 利用者の権限に基づく VM のライブマイグレーションの実行と，マイグレーションに伴う通信断の回避が可能である．

5. 評価実験

5.1 実験目的

本評価実験では以下の時間を測定し，ライブマイグレーションに認証機能と IP モビリティ機能を追加したことによる影響を定量的に示す．

- VM のライブマイグレーション時に CP-ABE を用いた認証を加えることによるライブマイグレーション処理時間
- 異なるプレフィクスのネットワークに位置する VMS へライブマイグレーションした時の双方向での通信途絶時間

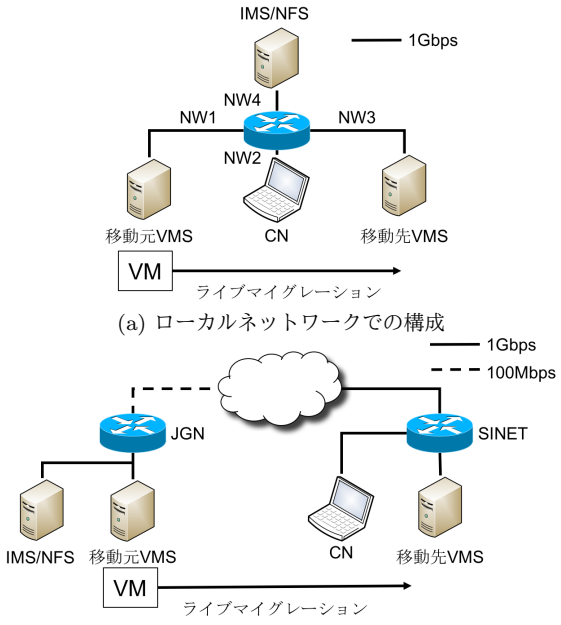


図 4 ネットワーク構成図
Fig. 4 Network configuration diagram

5.2 実験環境

実験では，異なるネットワーク間を VM がマイグレーションする（L3 マイグレーション）場合と，同一ネットワーク上でマイグレーション（L2 マイグレーション）する場合でのシステム全体の処理時間と通信途絶時間を測定した．L2 マイグレーションでは IP モビリティのサポートは不要で，L3 マイグレーションの途絶時間の比較対象として行うため支援システムを用いない．図 4 は L3 マイグレーション用のネットワーク構成で，CN の接続ネットワークと，VM がマイグレーション前後にそれぞれ接続するネットワークが全て異なる．(a) はそれをローカル環境に，(b) は SINET や JGN を用いて構成した場合である．(b) の場合 VMS 間の RTT は 25.67ms である．L2 マイグレーション用の構成は図 4 の (a) において VM のマイグレーション前後のネットワークが同一ネットワークになる．実験に用いた機器の諸元を表 1 に示す．実験では移動元と移動先の VMS で同一の NFS 上のストレージ領域をマウントし，VM の HDD イメージファイルにアクセスしている．

表 1　測定に使用した機器の諸元
Table 1　Specification of machines used for the measurement

項目	移動元 VMS	移動先 VMS	CN	VM
OS	CentOS 7.3	CentOS 7.2	CentOS 7.2	Cent OS 7.3
Kernel	3.10.0-514	3.10.0-327	4.4.39	4.4.39
CPU	Intel Xeon E5-2609 v3	Intel Core i7-4790K	Intel Core i7-4610QM	Intel Core i7 9xx 相当
RAM	8GB	16GB	8GB	2GB

表 2　属性とポリシー
Table 2　Attributes and policies

項目	ポリシーまたは属性
秘密鍵の属性	HCU, Netsci, M1
LM 先認証用ポリシー	HCU and M1
LM 元認証用ポリシー	B4 or M1

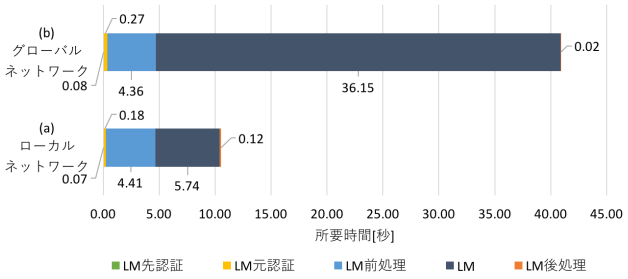


図 5　認証付きマイグレーション処理時間
（RAM 使用率 80%の場合）
Fig. 5　Processing time of migration with authentication
(When the RAM usage rate is 80%)

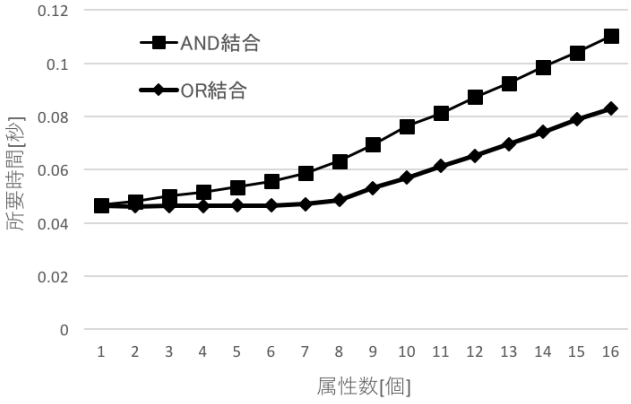


図 6　属性数による認証時間の変化
Fig. 6　Authentication time and the number of attribututes

表 3　通信途絶時間
Table 3　Communication interruption time

		RAM 使用率 [%]		
		40	60	80
途絶時間 [秒]	L3 ローカル	0.76	0.82	0.73
	L3 グローバル	1.00	1.17	1.14
	L2	0.32	0.34	0.33

5.3　実験方法と実験結果

5.3.1　支援システムがマイグレーション処理に与える影響

本システムの処理がライブマイグレーションの処理時間にどの程度影響を及ぼすか検証をするために，本システムの処理時間を測定した．本システムの動作は，図 2 の動作フローのように，LM 先認証，LM 元認証，LM 前処理，ライブマイグレーション，LM 後処理の 5 つに大別される．各処理の測定を，clock_gettime 関数を用いて行った．測定は L3 マイグレーション用の図 4 の (a) と (b) のそれぞれで行った．実験に用いた属性と各ポリシーを表 2 に示す．RAM の使用率を 40,60,80%と変化させ，各 10 回ずつ測定を行い，その平均を算出した．いずれの結果においても同様の結果となったため，本稿では RAM 使用率が 80%の場合を図 5 に示す．

5.3.2　属性数と認証時間の関係

支援システムの処理時間のうち，2 回行われる認証の所要時間はポリシーや秘密鍵に埋め込まれている属性数により変化する．そのため，ポリシーと秘密鍵の属性数を増加させ，ポリシーが AND 結合または OR 結合の場合において，表 1 の移動先 VMS で認証時間の変化を測定した．このときの各属性は 10 文字のランダムな文字列で，秘密鍵の属性集合 { 属性 1, 属性 2,…, 属性 N} に対して，ポリシーが AND 結合の場合は（属性 1 and 属性 2 and … and 属性 N）である．

測定はマイグレーション支援システムの認証モジュール部分のみを用いた測定用プログラムで行った．1000 回の計測結果の平均を図 6 に示す．

5.3.3　通信途絶時間

本システムを用いて L3 マイグレーション時に通信の継続性を検証するため，図 4 の (a) と (b) のそれぞれの場合で，マイグレーション時の CN（VM 利用者）と MN（VM）の通信途絶時間を測定した．CN から VM に対して ICMPv6 echo request パケットを 0.1 秒間隔で送信し，ライブマイグレーション前後での ICMPv6 echo reply パケットの途絶時間を通信途絶時間とした．また，比較対象として，L2 マイグレーションの場合の途絶時間も測定した．測定では，5.3.1 と同様に RAM 使用率を変化させ，各 10 回ずつ測定を行いその平均を算出した．測定結果を表 3 に示す．

5.4　考察

図 5 の結果から，支援システムの処理時間において，LM

先認証より LM 元認証の方で認証時間が長い傾向が見られるが，これは後者の認証時に LM 元認証用ポリシーを仮想化環境機構に問い合わせているためであると考えられる．全体の処理時間からライブマイグレーションの処理時間を引いた時間が，支援システムを用いたことによって生じる処理時間で，合計で最大 4.78 秒となっている．このうち，IP モビリティ用の LM 前処理時間がほぼ占める．LM 前処理時間のうち，4 秒はリンクダウン状態であったセカンダリ I/F をリンクアップした後，I/F が通信可能になるまで処理を待機している時間で，VM 内の OS の仕様によっても異なる．このことから，IP モビリティ処理そのものにかかる時間は小さいことがわかる． また，CP-ABE を用いた認証部分の処理時間は合計で最大 0.35 秒となっており，CP-ABE による認証はライブマイグレーション全体の処理時間からすると十分に小さい．

属性数増加による認証時間の変化は図 6 より，ポリシーが AND 結合の場合よりも，OR 結合の場合において認証時間が少ないことがわかる．これは，4.2.1 で記述のとおり，実装した CP-ABE のアルゴリズムで秘密分散法を利用しており，OR 結合のポリシーによって暗号化された暗号文を復号する時の時間は属性数に関わらず一定であるが，暗号化の時間は属性数によって線形増加するためである．また，認証時間は最大でも 0.11 秒となっている．本システムでは認証を 2 回行うが，属性数 16 の場合でも認証にかかる時間は合計でも 0.22 秒で，ライブマイグレーションの処理への影響をほとんどないことが分かる．

途絶時間においては，表 3 から RAM の使用率にかかわらず，L2 マイグレーションよりも，支援システムを用いた L3 マイグレーションでは，VMS 間の帯域や RTT の影響により，ライブマイグレーションの処理時間が長くなってしまうため，途絶時間が長くなっている．さらに，L3 マイグレーションでは，ライブマイグレーション後に VM が IMS へ I/F の切り替えを通知し，通信相手の CN が IMS からその情報を受け取る処理が必要で，その時間分は途絶時間が長くなるということも影響している．しかしながら，途絶時間は最大でも 1.17 秒でセッションの維持はできており，実際の利用に問題はないと考えられる．

6. まとめ

本稿では，属性ベース暗号を用いた認証と IP モビリティをサポートするライブマイグレーション支援システムの開発と評価について述べた．支援システムでは，VM の移動元・移動先の VMS 上で動作する支援デーモンと VM 利用者等が認証を行うことで，VM 利用者の権限に基づいてライブマイグレーションの操作を提供でき，さらに IP モビリティをサポートすることでライブマイグレーションに伴う通信途絶の問題を解決する．また，認証には CP-ABE を用いることで鍵の管理コストに関する問題を解決した．

評価では CP-ABE による認証処理がライブマイグレーションの処理時間に影響を及ぼしてないこと，ライブマイグレーションの前後では通信途絶を抑制できており，さらに相互の通信性も確保できていることを示した．

今後の予定として，VDI 環境などとの連携部分について設計を行い，ライブマイグレーションに対応した仮想化環境の開発を行う．

謝辞 本研究にあたり，有益なコメントを頂いた東海大学情報通信学部 大東俊博講師，株式会社インターネットイニシアティブの大石恭弘氏に感謝します．本研究の一部は日本学術振興会科学研究費助成金 15K00130，16H02808，総務省 SCOPE 受付番号 (162108102) の支援を受けて実施しました．

参考文献

[1] 渡邉英伸，大東俊博，近堂徹，西村浩二，相原玲二，“ＩＰモビリティと複数インタフェースを用いたグローバルライブマイグレーション，”電子情報通信学会論文誌，Vol.J93-B No.7，pp.893-901，Jul.2010.

[2] 広渕崇宏他，中田秀基，伊藤智，関口智嗣，“仮想マシンに対して透過的な Client Mobile IPv6 トンネリング機構，” 電子情報通信学会論文誌 B， Vol.195-B，No.10，pp.1239-1252，Oct.2012.

[3] John Bethencourt，Amit Sahai，Brent Waters，“Ciphertext-Policy Attribute-Based Encryption，”IEEE Symposium on Security and Privacy，pp.321-334，May.2007.

[4] 相原玲二，藤田貴大，前田香織，野村嘉洋，“アドレス変換方式による移動透過インターネットアーキテクチャ，”情報処理学会論文誌，Vol.43.12，pp.3889-3897，Dec. 2002.

[5] Timothy Wood, K. K. Ramakrishnan, Prashant Shenoy, et.al,“CloudNet: dynamic pooling of cloud resources by live WAN migration of virtual machines,” IEEE/ACM Trans. Netw. 23, 5, pp.1568-1583, Oct. 2015, DOI: http://dx.doi.org/10.1109/TNET.2014.2343945

[6] D.Farinacci, et.al.“The Locator/ID Separation Protocol (LISP),”IETF, RFC6830, Jan 2013.

[7] P. Raad, S. Secci, D. C. Phung, A, “Cianfrani, P. Gallard and G. Pujolle, ”Achieving Sub-Second Downtimes in Large-Scale Virtual Machine Migrations with LISP,”IEEE Transactions on Network and Service Management, Vol. 11, No. 2, pp. 133-143, June 2014. doi: 10.1109/TNSM.2014.012114.130517

[8] D. Johnson, C.Perkins, and J.arkko, “Mobility support in IPv6,” IETF RFC5213, 2008.

[9] libvirt: The virtualization API，https://libvirt.org/ (Aug, 2017 参照)

[10] 大東俊博，後藤めぐ美，西村浩二，相原玲二，“暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価，”情報処理学会論文誌, Vol.55, No.3, pp.1126-1139, Mar. 2014.

[11] QEMU，https://www.qemu.org/ (Aug. 2017 参照)

[12] Advanced Crypto Software Collection，http://acsc.cs.utexas.edu/cpabe/ (Aug. 2017 参照).