様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　５ 月 １７ 日現在

機関番号：１５４０１
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８０８

研究課題名（和文）属性に基づくアクセス制御が可能なクラウドアプリケーション実行基盤に関する研究

研究課題名（英文）Study on cloud application execution platform with attribute-based access control

研究代表者
相原　玲二（AIBARA, Reiji）

広島大学・情報メディア教育研究センター・教授

研究者番号：５０１８４０２３

交付決定額（研究期間全体）：（直接経費）　　12,500,000円

研究成果の概要（和文）：クラウドアプリケーションを用いたファイル共有や共同作業などクラウドサービス利用時の柔軟な認証方法として作業者の属性に基づくアクセス制御が有効である．本研究ではクラウドアプリケーションとして画面共有サービスを例として，作業者の属性に合わせた作業権限を設定できる認証機構を開発した．認証機構には暗号文ポリシー属性ベース暗号を利用した．これにより，作業者数や属性数が増えても鍵の管理が煩雑にならない．認証機構のプロトタイプシステム実装を行い，認証処理のオーバヘッドの評価を行った．さらに，複数組織で属性ベース暗号を利用するための拡張方式を検討し，中央管理機関を必要としない方式の詳細な評価を行った。

研究成果の学術的意義や社会的意義
多くの企業や大学等では、各組織が利用者のID 及び所属や役職等の属性情報を管理しており、本提案方式はその情報を利用してクラウド上の資源の割当や利用を安全に管理できることから、利用する組織にとって安全かつ利便性の高い方式である。本研究の成果により、条件を満たす属性を持つ他の利用者にアプリケーションの動作権限を委譲し、複数のクラウド事業者間で安全に動作を引き継ぐこと等が可能になる。現在クラウドコンピューティング事業が爆発的に普及・拡大している一方で、その安全性に不安を持つ利用者も多いく、本研究で開発する安全かつ柔軟なクラウドアプリケーション実行基盤の社会的意義は大きく、その波及効果は極めて大きい。

研究成果の概要（英文）：Attribute-based access control provides a flexible management of authentication in cloud services such as sharing and collaboration using cloud applications. In this research, we focus on Virtual Desktop Infrastructure (VDI) sharing as a cloud application. We have developed its authentication mechanism based on users' attributes using Ciphertext-Policy Attribute-Based Encryption. Using this mechanism, the management of encryption keys is not complicated even if the number of users and attributes increases. We implemented a prototype system of the authentication mechanism used in VDI sharing. We evaluated the overhead of the authentication processing of the system. In addition, we considered extension of decentralized key-management mechanisms for CP-ABE shared with multiple organizations.

研究分野：情報学

キーワード：サービス構築基盤技術　移動透過通信技術　クラウドアプリケーション　属性ベース暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

(1) 拡張性を考慮し適度に分割したアプリケーション（モジュール）単位で仮想計算機（VM）を構成し、必要に応じて VM を多数生成し、それらを連携して実行させることにより大規模な処理を高速に実行するクラウドネイティブアプリケーション技術の研究と実行環境構築が進んでいた。クラウドコンピューティング環境が急速に普及し低価格化していることから、新たなプログラミング及び分散処理のパラダイムとして注目されていた。一方、無線通信技術および携帯型コンピュータ等の普及にともない、コンピュータが移動中であっても通信を継続することができる移動透過通信の研究および標準化が進んでいた。VM が動作中であっても内部状態をあらかじめ移動先に転送しておき、移動時には内部状態の差分のみ転送することで転送時間と処理中断時間を短縮するライブマイグレーション技術が開発されているが、IP アドレスなどのネットワーク情報もそのまま複製するため同一 LAN 上の物理計算機間での移動が前提となる。研究代表者らは、移動透過通信技術を利用することでインターネットに接続された任意の物理計算機上に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を研究開発するとともに、マルチキャスト通信への拡張などを行っていた。

(2) 多数の VM による大規模な処理を実行する技術とグローバルライブマイグレーション技術が普及すると、異なるプロバイダが提供する任意のクラウド上で VM を動作させることも可能になる。VM の動作権限を他の利用者に委譲して動作を引き継ぐことや、利用者の都合により VM が動作するサイトを変更すること等も可能になり、新たな利活用分野の創出が期待できる。しかし、多くの場合このような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ことから、安全な実行環境の実現が求められる。クラウドネイティブアプリケーションの実行環境では、VM の起動（実行）、VM に対する設定変更やデータ送信（書込み）、VM からのデータ受信（読出し）などに関する権限管理（アクセス制御）が必要となる。特定プロバイダが提供するクラウド上での動作を前提とした、従来の OS におけるユーザ ID、グループ ID による制御に類似の方法は提案されているが、異なるプロバイダが提供するクラウド間での安全なアクセス制御方法は提案されていなかった。

２．研究の目的

(1) 企業や大学等の組織において利用する場合、所属や役職等の属性およびその組合せに基づくアクセス制御を異なるプロバイダのクラウド間で実現するという要求は強いが、その直接的な解決手法は存在しない。本研究は、近年研究が進められている属性ベース暗号技術と移動透過通信技術を適用し、属性に対応した VM のアクセス制御を直接的に行うことができる安全なクラウドアプリケーション実行基盤技術を新たに研究開発することを目的とする。

(2) この技術により、例えば仮想デスクトップ(VDI: Virtual Desktop Infrastructure) 環境において VM の動作権限を同一の属性を持つ利用者に委譲し、デスクトップ OS 上の処理を安全に引き継ぐことが可能となる。また、利用者がデスクトップ OS を利用中に、異なるクラウド事業者間で該当する VM を安全に移動させることも可能となる。現在クラウドコンピューティング事業が爆発的に普及・拡大している一方で、その安全性に不安を持つ利用者も多いことから、本研究で開発する安全かつ柔軟なクラウドアプリケーション実行基盤の社会的意義は大きく、その波及効果が期待できる。

３．研究の方法

(1) 属性ベース暗号を利用するマイグレーション方式の実現

クラウド上のサービスに有効な公開鍵暗号方式として暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）が提案されている。CP-ABE は ID や属性値(所属、役職など) を利用した論理式で表現されるアクセス権を暗号文に埋め込む。利用者はアクセス権を公開鍵として利用することで復号できる利用者のグループを任意に設定できる。また、ユーザが管理する秘密鍵の個数は自身の属性数に依存するため、組織内でのファイル共有のような共有するグループ数が多くなる場合でも効率的に利用できる。研究代表者らは既に CP-ABE を利用した組織内におけるデータ共有システムの提案を行っているが、本研究では仮想計算機 (VM) が移動する際のデータ転送や VM のイメージを共有する場合などへの適用方式について調査検討を行った。その結果、移動透過通信アーキテクチャ MAT を利用した VM のマイグレーション方式を拡張し、クラウドネイティブアプリケーション実行環境に対応する設計と実装を行った。

(2) 移動透過通信を利用する仮想計算機のマイグレーション方式の拡張

研究代表者らが独自開発している移動透過通信アーキテクチャ MAT を利用した仮想計算機に対し、移動時に暗号機能および認証機能を使用するよう拡張する詳細設計を行った。また、属性ベース暗号を活用した安全なグローバルライブマイグレーション機能を実装するために必要な開発環境整備を行った。研究代表者らが開発した MAT を利用した VM は、ネイティブハイパーバイザ方式に分類される Linux OS の KVM (Kernel-based Virtual Machine)を利用してプロトタイプが実装されていた。本研究で利用するためにはハイパーバイザが持つライブマイグレー

ション機能に対し暗号機能や認証機能を追加する方法も考えられるが、この方法には技術的な困難が予想されたため、プロトタイプとしては移動元と移動先の物理計算機上にそれぞれマイグレーション支援のための VM を作成し、その支援機能を利用した暗号機能や認証機能を実現する設計とした。

(3) 鍵発行センターKGC 等の性能評価および拡張性の検討

属性ベース暗号において鍵発行センターKGC は重要な役割を果たす。単一組織がひとつの KGC を利用するのが基本であるため、まずその実装および性能評価を行った。また、複数組織がそれぞれ持つ KGC を連携して利用する拡張方式について調査検討し、複数組織がそれぞれ KGC を持つよう拡張した場合の性能評価を行った。

(4) 仮想デスクトップ環境の性能評価

鍵管理サーバ構築・運用コストと安全性に関する性能評価を行うための環境構築を行った。具体的には CP-ABE で使用される鍵発行センター(KGC)を実現するとともに、ユーザ認証機能を含めた鍵生成・配布時間等の性能評価を行った。CP-ABE ライブラリや KGC は可能な限り公開されている既存プログラムを利用した。実装した安全なグローバルライブマイグレーション機能について、動作検証を行うとともに、鍵管理サーバ構築・運用コストと安全性および移動時の途絶時間に関する性能評価を行った。さらに、本方式を仮想デスクトップ(VDI)利用環境に適用した。評価実験は、学術情報ネットワーク SINET5 に構築した実験環境等を利用した。評価実験により開発した仮想化技術の総合的な評価を行い、本提案方式の有効性および意義を示した。

４．研究成果

(1) 共同作業における権限委譲機構の要件の決定

本研究では、クラウドアプリケーションとして VDI 環境を対象とし、共同作業が許可されたサービス利用者（以後，VDI 利用者）間で VDI を利用する場面を想定した。このとき必要となる、複数の VDI 利用者間で使用権限を委譲するための委譲機構を開発した。この機構は以下の要件 1～3 を持つように開発した。

要件 1：共同作業を許可するグループの単位で認証が可能

要件 2：委譲機構が VDI 利用者にとって煩雑でなく、委譲作業が VDI 利用者の本来の作業時間に大きな影響を及ぼさない

要件 3：許可するグループが増えても委譲機構の管理コストが著しく大きくならない

既存研究において作業の共有化におけるサービス利用者の認証にいくつかの暗号化方式が用いてられている。本研究で開発する委譲機構も作業の共有化に適した暗号化方式を用いる。ここでは要件 1 を満たすため、CP-ABE を用いた。共同作業の許可ポリシーを暗号文に埋め込み、グループを属性集合として表現し、それを鍵に埋め込む CP-ABE 用いた認証が従来の公開鍵暗号方式より適す。委譲機構を導入することでサービス利用者やクラウドの管理者の手間が増えることはやむを得ないが、CP-ABE を採用しても要件 2 や要件 3 を満たすことを示した。

(2) 仮想デスクトップ(VDI)共有における権限委譲システムの設計

VDI を複数の VDI 利用者間で安全に引き継ぐことを目的とし、複数の VDI 利用者で VDI 共有をする権限委譲システムを開発した。権限委譲システムでは、CP-ABE を用いることで共同作業として複数の VDI 利用者が VM 上のデスクトップ OS の画面を共有し、それを VDI 利用者間で安全に引き継ぐことができるようにした。VDI には VNC (Virtual Network Computing) と呼ばれるソフトウェアを用いた。システム構成を図 1 に示す。

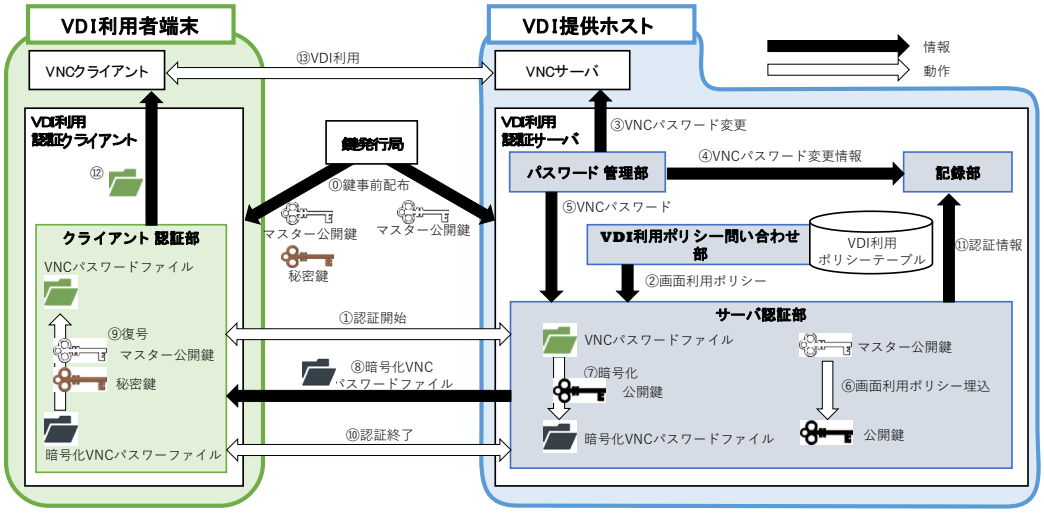
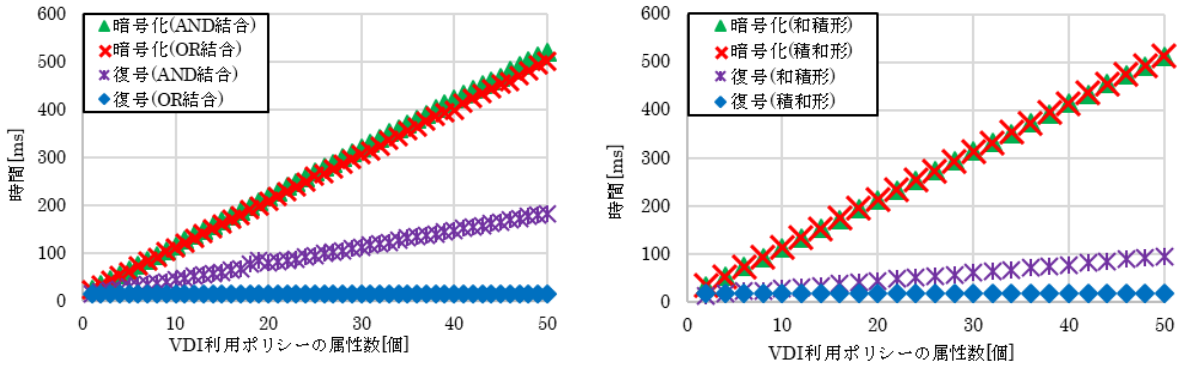


図１　権限委譲システムの構成

(3) VDI 利用ポリシーの属性数増加時の暗号化と復号の時間の測定

VDI 利用ポリシーの属性数を A and B and C and D のように属性を AND 結合で 50 個まで増やした場合、A or B or C or D のように属性を OR 結合で 50 個まで増やした場合の暗号化と復号にかかる時間を測定した。測定には clock_gettime 関数を用い、1000 回試行の平均を求めた。CP-ABE の鍵長は 2048bit とした。また、VDI 利用ポリシーの属性数を(A and B) or (C and D)のように属性を積和形で 50 個まで増やした場合、(A or B) and (C or D)のように属性を和積形で 50 個まで増やした場合も同様に測定した。これらの結果を図２に示す。



(a) AND/OR 結合の場合　　(b) 和積形/積和形の場合

図２　ポリシーの属性数増加に対する暗号化/復号時間

(4) CP-ABE の処理負荷の測定

CP-ABE の暗号化と復号にかかる端末への負荷がどの程度あるかを確認するため、以下の 2 つのパターンを実行したときの平均 CPU 使用率を算出した。

(ア)パスワードファイルを VDI 利用ポリシーの属性数を AND 結合 50 個で 100 回連続暗号化

(イ)VDI 利用ポリシーの属性数を AND 結合 50 個で暗号化したパスワードファイルを適合する属性集合を持つ秘密鍵で 100 回連続復号

測定には linux の top コマンドを用い、(ア) と (イ) を実行中に CP-ABE の暗号化と復号の際のプロセスの CPU 使用率を抽出し、その合計値を抽出回数で割った値を平均 CPU 使用率とした。CP-ABE の鍵長は 2048bit とした。その結果、(ア) は平均 CPU 使用率が 71.84%、(イ) は平均 CPU 使用率が 76.42%であった。

(5) 複数組織対応属性ベース暗号の評価

CP-ABE を用いたファイル共有サービスを複数組織間で相互利用可能にする拡張方法について、複数の KGC が存在可能な属性ベース暗号(Multi-Authority Attribute-Based Encryption: MA-ABE)を用いた方法について検討した。複数組織での鍵発行センターKGC を分散管理するための提案方式を図３に示す。中央機関を必要とせず複数の KGC が存在可能な属性ベース暗号として Lewko の方式と Yannis らの方式について、実装を行い詳細に比較した。また、処理速度や必要なメモリ量の評価、KGC やストレージへのアクセス等の通信時間を含めた評価を行った。

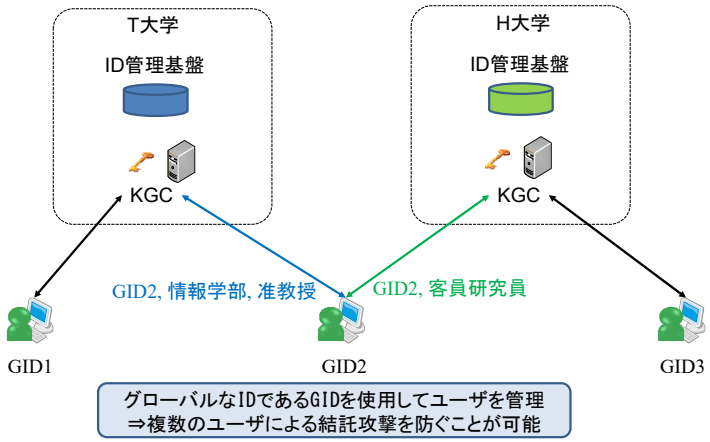


図３　複数組織での鍵発行センターKGC 管理の概要

５．主な発表論文等

〔雑誌論文〕（計１１件）

① 林健汰，加森剛徳，前田香織，近堂徹，相原玲二，CP-ABE を用いた VDI の使用権限委譲機構の開発，情報処理学会論文誌，Vol.60，No.3，2019，750～757，査読有
http://id.nii.ac.jp/1001/00195304/

② Suzuki Tatsuya, Emura Keita, Ohigashi Toshihiro, A Generic Construction of Integrated Secure-Channel Free PEKS and PKE and its Application to EMRs in Cloud Storage, Journal of Medical Systems, 43, 2019, 1～1, 査読有
DOI: 10.1007/s10916-019-1244-2

③ Ishikawa Naoki, Ohishi Yasuhiro, Maeda Kaori, Nulls in the Air: Passive and Low-Complexity QoS Estimation Method for a Large-Scale Wi-Fi Network Based on Null Function Data Frames, IEEE Access, vol. 7, 2019, 1～1, 査読有
DOI: 10.1109/ACCESS.2019.2902182

④ 平空也，高野知佐，前田香織，拡散型フロー制御を用いる自律分散的な DDoS 攻撃緩和システム，情報処理学会論文誌，Vol.59，No.9，2018，1656～1665，査読有
http://id.nii.ac.jp/1001/00191373/

⑤ Kamori Yoshinori, Hayasi Kenta, Maeda Kaori, Kondo Tohru, Aibara Reiji, A Secure Sharing System for Cloud Desktop Applications Migrating with Optimized User Experience, Proc. the 2018 IEEE 42nd Annual International Computers, Software and Applications Conference, vol. 2, 2018, 947～950, 査読有
DOI: 10.1109/COMPSAC.2018.00164

⑥ Kondo Tohru, Isawaki Keita, Maeda Kaori, Development and Evaluation of the MEC Platform Supporting the Edge Instance Mobility, Proc. the 2018 IEEE 42nd Annual International Computers, Software and Applications Conference, vol. 2, 2018, 193～198, 査読有
DOI: 10.1109/COMPSAC.2018.10228

⑦ Emura Keita, Kimura Hayato, Ohigashi Toshihiro, Suzuki Tatsuya, Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions and Its Implementations, The Computer Journal, 62, 2018, 614～630, 査読有
DOI: 10.1093/comjnl/bxy135

⑧ JHA Sonu, BANIK Subhadeep, ISOBE Takanori, OHIGASHI Toshihiro, SARKAR Santanu, Theoretical Understanding of Some Conditional and Joint Biases in RC4 Stream Cipher, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E101.A, 2018, 1869～1879, 査読有
DOI: 10.1587/transfun.E101.A.1869

⑨ Tohru Kondo, Hidenobu Watanabe, Toshihiro Ohigashi, Development of the Edge Computing Platform based on Functional Modulation Architecture, Proc. the 2017 IEEE 41th Annual International Computers, Software and Applications Conference, vol 1, 2017, 284-285, 査読有
DOI: 10.1109/COMPSAC.2017.108

⑩ 新谷隆文，前田香織，無線 LAN の通信品質における MAC 層情報の有効性調査，情報処理学会論文誌，Vol.58，No.3，pp.664-671，2017，査読有
http://id.nii.ac.jp/1001/00178487/

⑪ Yuta Ukida, Kaori Maeda, Tohru Kondo, Hidenobu Watanabe, Reiji Aibara, Yasuhiro Ohishi, A Design and Evaluation of User-space IP Mobility Implementation, MOBIQUITOUS '16 Adjunct Proceedings, 2016, 査読有
DOI: 10.1145/3004010.3004046

〔学会発表〕（計２５件）

① Hidenobu Watanabe, Tohru Kondo, Toshihiro Ohigashi, Implementation of Platform Controller and Process Modules of the Edge Computing for IoT Platform, IEEE PerCom 2019, Work in Progress (Mar. 11-15, 2019)（国際学会），2019

② 加森剛徳，前田香織，近堂徹，相原玲二，CP-ABE による認可機構を備えたクラウドアプリケーション共有基盤の開発，電子情報通信学会インターネットアーキテクチャ研究会（2019 年 3 月 7 日～8 日），2019

③ 小林海，木村隼人，大東俊博，渡邉英伸，相原玲二，近堂徹，動的な機能変更を可能にするエッジコンピューティング基盤の実装と評価，情報処理学会インターネットと運用技術研究会（2019 年 3 月 7 日～8 日），2019

④ 石橋拓哉，小林海，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二，複数組織対応属性ベース暗号を用いたファイル共有システムの評価および考察，情報処理学会インターネットと運用技術研究会（2019 年 3 月 7 日～8 日），2019

⑤ Kenta Hayashi, Kaori Maeda, Tohru Kondo, A Design of Failure Injection Testing considering Edge Computing Environment, Internet Conference 2018 (Nov. 26-27, 2018)

（国際学会），2018
⑥ Tatsuya SUZUKI, Keita EMURA, Toshihiro OHIGASHI, A Generic Construction of Integrated Secure-Channel Free PEKS and PKE, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018) (Sep. 25-27, 2018) (国際学会), 2018
⑦ 石橋拓哉，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二，複数組織対応属性ベース暗号を用いたファイル共有システム，情報処理学会インターネットと運用技術シンポジウム2018（2018年12月6日～7日），2018

６．研究組織

(1)研究分担者

研究分担者氏名：近堂　徹

ローマ字氏名：(KONDO, Tohru)

所属研究機関名：広島大学

部局名：情報メディア教育研究センター

職名：准教授

研究者番号（8桁）：90437575

研究分担者氏名：岸場　清悟

ローマ字氏名：(KISHIBA, Seigo)

所属研究機関名：広島大学

部局名：情報メディア教育研究センター

職名：助教

研究者番号（8桁）：30274137

研究分担者氏名：大東　俊博

ローマ字氏名：(OHIGASHI, Toshihiro)

所属研究機関名：東海大学

部局名：情報通信学部

職名：准教授

研究者番号（8桁）：80508127

研究分担者氏名：前田　香織

ローマ字氏名：(MAEDA, Kaori)

所属研究機関名：広島市立大学

部局名：情報科学研究科

職名：教授

研究者番号（8桁）：00264953

(2)研究協力者

研究協力者氏名：西村　浩二

ローマ字氏名：(NISHIMURA, Kouji)

研究協力者氏名：田島　浩一

ローマ字氏名：(TASHIMA, Koichi)

研究協力者氏名：渡邉　英伸

ローマ字氏名：(WATANABE, Hidenobu)