情報処理学会論文誌 Vol.60 No.3 750–757 (Mar. 2019)

# CP-ABEを用いたVDIの使用権限委譲機構の開発

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

受付日 2018年6月25日, 採録日 2018年12月4日

**概要**：クラウドアプリケーションを用いたファイルの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VDI共有を対象とし，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する．認証機構には暗号文ポリシ属性ベース暗号を用いる．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．VDI共有としてVNCを対象とした認証機構のプロトタイプシステムの実装について述べ，暗号文ポリシ属性ベース暗号を採用したことによる認証処理のオーバヘッドの評価により，それが利用者の作業にほとんど影響を及ぼさないことを示す．また，従来の公開鍵暗号方式との比較により，開発する認証方法の有用性を示す．

**キーワード**：クラウドアプリケーション，仮想デスクトップ，VDI共有，属性ベース暗号

# Development of a Usage Authority Transfer Mechanism of Virtual Desktop Infrastructure Using Cyphertext-policy Attribute-based Encryption

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

Received: June 25, 2018, Accepted: December 4, 2018

***Abstract:*** 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 VDI sharing as a cloud application, and develop its authentication mechanism based on users' attributes using Cyphertext-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 implement a prototype system of the authentication mechanism used in VNC as VDI sharing. We evaluate the overhead of the authentication processing of the system and show that it has little effect on practical use. In addition, we show the effectiveness of our developed authentication mechanism compared to authentication using the usual public key cryptosystem.

***Keywords:*** cloud application, virtual desktop environment, VDI sharing, cipher-policy attribute-based encryption

## 1. はじめに

通信網の発展により，あらゆることをクラウド上で実現できるようになり，組織内においても，ファイルの共有や共同作業でクラウドアプリケーションを用いることが多くなってきている．しかし，一般的にクラウドサービスの利用はクラウド上に保管されるデータやそれを使う作業の安全性がより強く求められる．クラウド上のデータ保管に対しては暗号化がその対策の1つとなるが，公開鍵暗号方式を用いる場合，対象データのアクセス権ごとにクラウドサービスの利用者（以降，サービス利用者）の秘密鍵と公開鍵の組を用いて暗号化しなければならず，鍵の数も増え，管理も煩雑になる．また，サービス利用者の属性のみを用いて，または属性の組合せで共有や共同作業の可否を判断

[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, Hiroshima 731–3194, Japan
[2] 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University, Higashi-Hiroshima, Hiroshima 739–8511, Japan
[a)] kaori@hiroshima-cu.ac.jp

© 2019 Information Processing Society of Japan

する場合にも対応できない．

これに対して，クラウドサービスの利用にも対応する暗号化を用いたファイル共有のためのシステムが提案されている [1], [2]．これらは，いずれも暗号文ポリシ属性ベース暗号（Cyphertext-Policy Attribute-Based Encryption: CP-ABE）[3] を用いる．許可された複数のサービス利用者でファイルの読み出しや保存をする（これをファイル共有と呼ぶ）場合，サービス利用者の属性でファイルのアクセス可否を判断する方法として CP-ABE は有効である．しかし，文献 [1], [2] は権限委譲されたサービス利用者間でクラウド上のアプリケーションを操作することは対象としていない．このような複数のサービス利用者間で権限を委譲してクラウドアプリケーションによる作業を行う際にも，ファイル共有と同様にクラウド上で安全に作業をするための権限管理が必要である．また，従来の公開鍵暗号方式で生じる鍵の管理の手間を軽減し，サービス利用者の負担にならない権限管理方法が求められる．

そこで本研究では，許可されたサービス利用者のみに作業権限を付与し，そのサービス利用者から他のサービス利用者へクラウドアプリケーションによる作業を委譲することを可能にするための使用権限委譲機構を開発する．クラウドアプリケーションとして仮想デスクトップ（VDI: Virtual Desktop Infrastructure）を想定し，CP-ABE を用いたサービス利用者の認証により，サービス利用者側に与えられた特定の属性を有するサービス利用者の間でのみ安全に VDI 環境を引き継ぐことができる権限委譲システムを構築する．VDI を用いた画面の共有によって，たとえば，表計算，文書作成，動画作成などの複数のアプリケーションを同時に，かつアプリケーションの動作環境も含めて引き継ぐことができる．複数のサービス利用者の属性とポリシによる認証を用いる権限管理方法によりサービス利用者に権限管理の手間やその作業のための処理時間をかけることなく，共同作業のために複数のサービス利用者間で安全に引継ぎが可能となることを目指す．

本論文の構成は以下のとおりである．2 章で関連技術や既存研究について述べ，3 章で共同作業における権限委譲機構について述べる．4 章で VDI の利用権限委譲のシステムについて述べ，5 章でその評価をする．最後に 6 章でまとめと今後の課題について述べる．

## 2. 関連研究

### 2.1 クラウド資源の権限管理

クラウド資源の利用において，Dropbox などのオンラインストレージサービスが広く利用されるようになっている．オンラインストレージサービスの多くは，権限のないサービス利用者からのアクセス制御などによりデータを保護している．一方で，クラウド上のストレージの管理者による覗き見などからもデータを保護するためにサービス利用者側でファイルを暗号化する方法がある [4]．また，オンラインストレージを対象に，文献 [1] はファイルの閲覧権限を，文献 [2] はファイル名およびディレクトリ名の表示や編集権限の管理をしている．文献 [1] や [2] は CP-ABE を使うことで，組織内など複数のサービス利用者でグループを作成してグループ内でのファイル共有や共有作業をするときに必要な鍵の管理コストを下げている．これらはいずれもデータアクセスに関する権限管理を対象とした権限管理の提案であり，本研究が対象とする共同作業時の VDI 使用権限の管理コストを対象としたものとは異なる．

### 2.2 暗号文ポリシ属性ベース暗号（CP-ABE）

公開鍵暗号など従来の暗号方式では暗号強度が十分な場合，クラウドにデータを安全に保存することには使えるが，複数のサービス利用者でファイルを共有したり，クラウドアプリケーションを利用したりする場合は 1 対 1 の鍵配布では鍵の管理が煩雑になる．そこでクラウドサービスに適した暗号方式の 1 つとして属性ベース暗号（Attribute-Based Encryption: ABE）がある．

ABE は鍵もしくは暗号文に属性の論理式で表されたポリシ（属性を AND または OR で結合したもの）を埋め込み，特定の属性集合を持つサービス利用者のみが復号できる公開鍵暗号方式の一種である．個人に付与される社会的な属性は ABE の属性集合で表すことができ，ABE のポリシによって集団を特定することが可能であるため，本研究が対象とする共同作業時のグループ定義に利用することができる．ポリシを暗号文に埋め込み，属性集合を鍵に埋め込む方式が暗号文ポリシ属性ベース暗号（CP-ABE）[3] である．

CP-ABE は以下の 4 つのアルゴリズムからなる．

- Setup($1^\lambda$)：セキュリティパラメータ $\lambda$ を入力とし，マスタ公開鍵 $PK$ とマスタ秘密鍵 $MK$ を出力する．
- Encrypt($PK, M, A$)：マスタ公開鍵 $PK$ と平文 $M$ とポリシ（アクセス権）$A$ を入力すると，$A$ が埋め込まれた暗号文 $CT$ を出力する．
- Keygen($MK, S$)：マスタ秘密鍵 $MK$，秘密鍵を識別するための属性集合 $S$ を入力すると，秘密鍵 $SK$ を出力する．
- Decrypt($PK, CT, SK$)：マスタ公開鍵 $PK$，秘密鍵 $SK$，暗号文 $CT$ を入力とし，$CT$ に埋め込まれたポリシ（アクセス権）$A$ にマッチする $SK$ のみ平文 $M$ を復号する．

一般的な CP-ABE の暗号化と復号の処理の概要を**図 1** に示す．最初に鍵発行局でマスタ秘密鍵とマスタ公開鍵が生成される（図 1：①）．鍵発行局はマスタ秘密鍵に復号側の属性集合を埋め込み秘密鍵を生成する（図 1：②）．生成した秘密鍵とマスタ公開鍵は復号側（図 1：③），マスタ公開鍵を暗号化側に渡す（図 1：④）．復号側はマスタ秘密鍵

© 2019 Information Processing Society of Japan

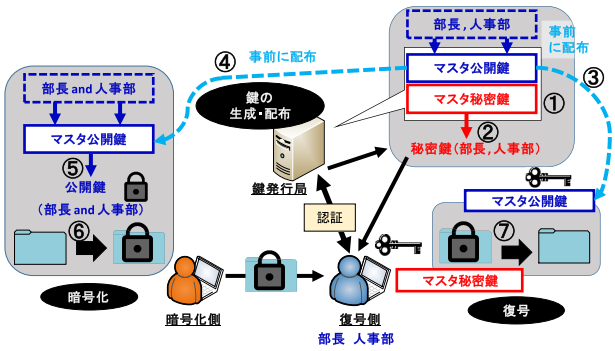



図 1 暗号文ポリシ属性ベース暗号の暗号化と復号の処理の概要
**Fig. 1** Outline of ciphyertext-policy attribute-based encryption.

を鍵発行局から受け取るとき，鍵発行局との間でマスタ秘密鍵を受け取る権利があるかを認証する．暗号化側はマスタ公開鍵にポリシを埋め込んだ公開鍵を生成し（図 1：⑤）生成した公開鍵で平文を暗号化する（図 1：⑥）．暗号文を復号するには，マスタ公開鍵と秘密鍵を用いて暗号文を復号する（図 1：⑦）．CP-ABE では，暗号文のポリシ（例：（部長 AND 人事部））に対して秘密鍵の属性集合（例：｛部長，人事部｝）が満たすとき，暗号文は秘密鍵によって復号される．

このように CP-ABE では公開鍵と秘密鍵は 1 対 1 に対応していない．従来の公開鍵暗号では公開鍵と秘密鍵は 1 対 1 対応なので，属性の論理式で表現されたアクセス権の種類ごとに鍵ペアを用意しなければならない．これに対して，CP-ABE では属性の論理式で表現されたアクセス権は暗号文に埋め込まれているので，公開鍵はアクセス権を満たす属性を持つ秘密鍵すべてに対応する．

公開鍵基盤（PKI）で，公開鍵暗号を利用した鍵の証明書の発行や失効を認証局によって管理する．CP-ABE においても信用できる鍵発行局が必要である．また，PKI と同様に鍵発行局が安全に秘密鍵を配布する機構も必要である．

CP-ABE を認証に用いる場合の端末側の課題として，属性数に依存して暗号化や復号にかかる時間が増加する点がある．モバイル環境でクラウドサービスの利用を想定した場合，処理能力の低いモバイル端末では計算に時間がかかることもある．これに対して，モバイル端末の処理負荷を軽減するように属性ベース暗号を改良した提案もある [5]．

なお，CP-ABE に類似している暗号として ID ベース暗号（ID-Based Encryption: IBE）[6] がある．IBE は email アドレスなどの ID を公開鍵として用いることのできる公開鍵暗号方式の一種である．しかし，IBE は単一の属性しか表現できず，本研究で対象としているグループごとに複数の属性を持つような場合を表現することができない．

## 3. 共同作業における権限委譲機構の要件

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する．このときに必要となる，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する．この機構は以下の要件を持つように開発する．

- 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

1 章で述べたとおり，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 を用いる．2.1 節で述べたとおり，共同作業の許可ポリシ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る．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えないが，CP-ABE を採用しても要件 2 や要件 3 を満たすことは 5 章で示す．

なお，暗号化方式に必要な PKI や鍵発行局など鍵管理の基盤は信頼できる第三者機関で管理されることを前提とし，開発する権限委譲システムの対象外とする．

## 4. VDI 共有における権限委譲システム

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する．

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する．VDI には VNC（Virtual Network Computing）[7] を用いる．

### 4.1 システム構成

VDI の利用権限を委譲するための権限委譲システムの構成を図 2 に示す．VDI 利用者が使用する VDI 利用者端末には VNC クライアントと VDI 利用認証クライアントが，VDI 提供ホストには VNC サーバと VDI 利用認証サーバが動作している．鍵発行局は信頼された第三者であり，VDI 利用者と VDI ホスト提供に必要な鍵を提供する．

VNC クライアントが VNC サーバのデスクトップ画面を利用する際，VDI 利用認証サーバと VDI 利用認証クライアントの間で認証が開始される（図 2：①）．その際，CP-ABE を用いて VDI 利用者の作業権限を認証する．VDI 利用ポ

© 2019 Information Processing Society of Japan

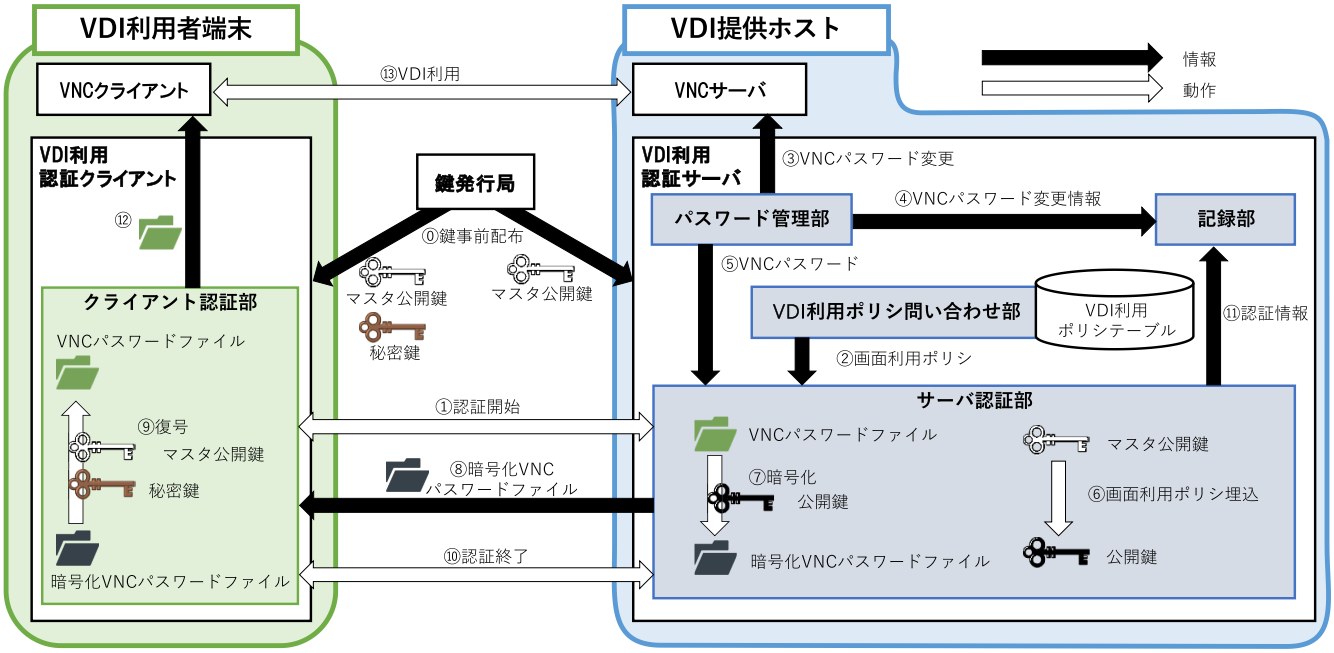



図 2 システム構成図
**Fig. 2** System configuration.

リシ問合せ部は VNC サーバが VNC のデスクトップ画面ごとに一意に割り振っている VDI 番号に対するポリシを格納している VDI 利用ポリシテーブルに対してポリシの問合せを行いサーバ認証部にポリシを渡す（図 2：②）．パスワード管理部は認証に必要な VNC パスワードの変更を行い，変更済みの VNC パスワードをサーバ認証部へ渡す（図 2：③，⑤）．サーバ認証部へ渡されたこれらのデータを用いてサーバ認証部とクライアント認証部は認証を行う（図 2：⑥～⑩，⑫）．サーバ認証部とクライアント認証部の詳細な動作は 4.3 節で述べる．VDI 利用認証サーバ側では VNC パスワードの変更情報とサーバ/クライアント認証部間での認証結果を認証部に保存する（図 2：④，⑪）．その後，VNC サーバ/クライアント間で VDI の利用が開始される（図 2：⑬）．

すでに認証された VDI 利用者から別の VDI 利用者に作業を引き継ぐ場合，別の VDI 利用者に与えられた属性が VDI 提供ホストの指定した属性に適合すれば使用権限委譲を行う．使用権限委譲が行われた際，現在の VDI 利用者に対して次の VDI 利用者への引継ぎの可否の確認を行う．

VDI 利用認証クライアントや VDI 利用認証サーバで必要な秘密鍵およびマスタ公開鍵は図 2 の鍵発行局から VDI 利用者端末を利用する VDI 利用者や VDI 提供ホストの管理者の認証情報をもとに，VDI 利用者端末と VDI 提供ホストが鍵発行局と認証をしたうえで事前に取得する．

### 4.2 VDI 利用ポリシ

システムの利用者が持つ秘密鍵の属性集合と VDI 利用のためのポリシの関係を図 3 に示す．図 3 のポリシ（アクセス権）は Access Tree で管理されている．ポリシの表現の詳細は文献 [3] で述べられているため，本文では簡易的な表現を用いて説明する．図 3 の VDI 番号（VNC サーバで稼働するデスクトップ画面の番号）に対応する VDI 利用ポリシは図 2 の VDI 利用認証サーバ内の VDI 利用ポリシテーブルに格納される．VDI 利用者ごとの属性は図 2 の VDI 利用認証クライアントの秘密鍵に埋め込まれる．

| VDI利用者 | VDI利用者が持つ秘密鍵の属性集合 |
|---|---|
| A | 情報科学研究科，学年=1年，卓球部 |
| B | 芸術学部，学年=4年，卓球部 |
| C | 情報科学研究科，学年=1年，テニス部 |

(a) VDI利用者に対応する秘密鍵の属性集合

| VDI番号 | VDI利用ポリシ |
|---|---|
| 1 | 情報科学研究科 and 学年=1年 |
| 2 | 情報科学研究科 or 芸術学部 |
| 3 | 卓球部 |

(b) VDI提供ホストにおける各VDIごとのVDI利用者を指定するポリシ

図 3 属性集合とポリシの例
**Fig. 3** Example of a set of attributes and policies.

図 3 の場合，VDI 提供ホストで VDI 番号 2 を利用できるのは VDI 利用者 A と C となる．図 3 の VDI 利用者が持つ秘密鍵の属性集合に変更がある場合，図 2 の⓪鍵事前配布で鍵発行局から秘密鍵を再発行する必要がある．しかし，再発行前の秘密鍵は VDI 利用者が本来持つ属性と異なるため，鍵発行局で再発行前の秘密鍵を失効させなければならない．今回のシステムでは失効機能を実装していないが，今後，文献 [1] で実装されている秘密鍵の失効機能のプロトタイプシステムを用いて実装することも可能と考えている．

© 2019 Information Processing Society of Japan

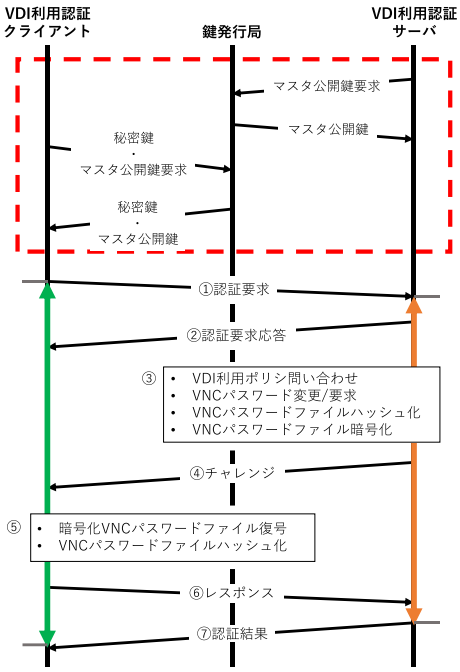



図 4 VDI 共有システムの認証機構の動作フロー
**Fig. 4** Authorization processing flow of the VDI sharing system.

### 4.3 動作フロー

VDI 共有システムの権限委譲システムの動作フローを**図 4** に示す．なお，図 4 は権限委譲システムの利用者の認証部分に焦点を当てているため，VNC サーバおよびクライアントにかかわる動作フローは省いている．

まず，初期動作として，図 4 の赤色破線で囲まれた部分のように，VDI 利用認証クライアントと VDI 利用認証サーバは鍵発行局に対して最初に 1 回のみ鍵の要求を行う．次に認証処理が始まり，VDI 利用者は VDI 利用開始時に VDI 番号とともに認証要求を VDI 利用認証サーバへ送る（図 4：①）．VDI 利用認証サーバは VDI 認証クライアントに認証要求応答を返し（図 4：②），認証要求に含まれる VDI 番号から対応する VDI 利用ポリシを図 2 の VDI 利用ポリシテーブルから参照し，それとマスタ公開鍵から公開鍵を生成する．生成された公開鍵で VDI 番号に対応する VNC のパスワードファイルを暗号化し（図 4：③），VDI 利用認証クライアントにチャレンジとして送る（図 4：④）．その際，VDI 利用認証サーバでは VNC パスワードファイルのハッシュ値を計算して保持する．VDI 利用認証クライアントでは属性集合が埋め込まれた VDI 利用者の秘密鍵とマスタ公開鍵を用いて暗号化 VNC パスワードファイルを復号し，VNC パスワードファイルのハッシュ値を計算して（図 4：⑤），VDI 利用認証サーバへレスポンスとして送る（図 4：⑥）．VDI 利用認証サーバは受け取ったハッシュ値と事前に計算したハッシュ値を比較し，認証結果を VDI 利用認証クライアントへ返して認証を終了する（図 4：⑦）．VDI 利用認証クライアントは認証結果を受け取り，認証成功の場合，復号した VNC パスワードファイルを VNC クライアントに渡し，VNC クライアントと VNC サーバ間で VNC による認証が行われ，VDI の利用が開始する．

表 1 VM の仕様
**Table 1** Specification of VMs.

| 項目 | 内容 |
|---|---|
| OS | CentOS Linux release 7.2.1511 (Core) |
| Kernel | Linux 3.10.0-327.28.3.el7.x86_64 |
| CPU | Intel Xeon E312xx 2.2GHz 2core |
| RAM | 2GB |

表 2 開発環境
**Table 2** Development environment.

| 項目 | 内容 |
|---|---|
| コンパイラ | gcc (GCC) 4.8.5<br>20150623 (Red Hat 4.8.5-4) |
| 開発言語 | C |
| データベース | sqlite3.7.17 |
| ライブラリ | cpabe toolkit 0.11 (CP-ABE),<br>openssl 1.0.1 (RSA) |

### 4.4 プロトタイプシステムの実装

前述の設計をもとにプロトタイプシステムを実装した．VDI 利用認証クライアントと VDI 利用認証サーバはどちらも VM 上に実装した．これらが動作する VM の仕様を**表 1** に，開発環境を**表 2** に示す．CP-ABE の処理には cpabe toolkit ライブラリ [8] を使用した．

## 5. 評価

3 章で述べたように，提案する CP-ABE を用いる権限管理方法を用いることで VDI 利用者の作業時間が増大したり，クラウドアプリケーション（ここでは共同作業用）を提供するプロバイダにとって権限管理の手間が大きくなったりしてはならない．本章ではこれらの点に関する開発システムの評価を示す．

### 5.1 権限管理の手間に関する考察

クラウドアプリケーションを提供する側の管理負荷について，鍵の管理コストの点で提案方法と RSA 暗号を比較する．RSA 暗号で属性を表現する場合は公開鍵と秘密鍵の 1 組が 1 属性となる．1 つのデスクトップ画面に対して $N$ 個の属性によるポリシを設定するとき，RSA 暗号でそのポリシを表現するには $N$ 個の鍵を紐付ける必要がある．VDI 提供者は属性として鍵を紐付けているため，VDI 利用者が持つ属性がデスクトップ画面自体に紐付けられている属性に適合しているかを確認するにはそれぞれで暗号化と復号の処理をすることになる．CP-ABE の場合は 1 つ

© 2019 Information Processing Society of Japan

表 3 VDI 利用者あたりの認証時間 [単位：ms]
**Table 3** Detail of authorization processing time.

| | | 暗号化 | 復号 | ハッシュ化 | その他処理 | 全体 |
|---|---|---|---|---|---|---|
| サーバ側 | CP-ABE | 28.28 | — | 0.02 | 58.4 | 86.69 |
| | RSA | 6.34 | — | — | — | — |
| クライアント側 | CP-ABE | — | 15.46 | 0.09 | 74.92 | 90.47 |
| | RSA | — | 9.43 | — | — | — |

の公開鍵の中に $N$ 個の属性を埋め込むことができるので，デスクトップ画面に対して紐付ける鍵の数は 1 個となる．そのため，本システムを採用した鍵管理コストは RSA 暗号を用いたものに比べて $N$ 分の 1 だけ低減できる．

### 5.2 VDI 利用者の作業時間に関する評価

VDI 利用者の作業時間の増加に関する評価では，1 つ目に，本システムで利用する CP-ABE と他の一般的な公開鍵暗号を，暗号化と復号にかかる時間で定量的に比較する．ここでは RSA 暗号と比較する．2 つ目に，暗号化と復号にかかる時間は VDI 利用ポリシの属性数とその結合方法によって変化する．VDI 利用ポリシの属性数の変化がどのように本システムの認証時間に影響を与えるかを定量的に調べる．3 つ目に，VDI 利用者の利用端末への CP-ABE の暗号化と復号にかかる負荷を測定し，実用上問題ない負荷であるかを考察する．

#### 5.2.1 実験環境

VDI 利用者端末（VDI 利用認証クライアント/VNC クライアントが動作する端末）と VDI 提供ホスト（VDI 利用認証サーバ/VNC サーバが動作する端末）は同一ネットワークに接続されている．実験に使用した各端末の仕様は表 1 と同じである．

#### 5.2.2 実験方法と実験結果

**(1) CP-ABE と RSA の認証時間の比較**

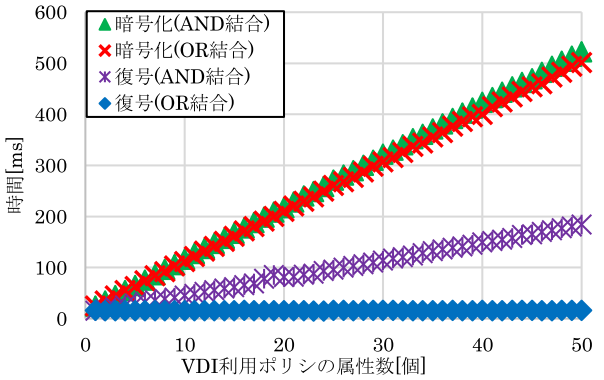
CP-ABE による認証にかかる時間を調べるため，VDI 利用認証サーバの認証時間（図 4 の橙色線区間）と VDI 利用認証クライアントの認証時間（図 4 の緑色線区間）を測定する．

比較対象として CP-ABE と同様に公開鍵暗号方式の一種である RSA 暗号の暗号化と復号にかかる時間も測定する．どちらの暗号化においても VDI 利用ポリシの属性数は RSA 暗号で表すことのできる 1 とし，鍵長は CP-ABE と RSA で一般的に使われる 2,048 bit とする．

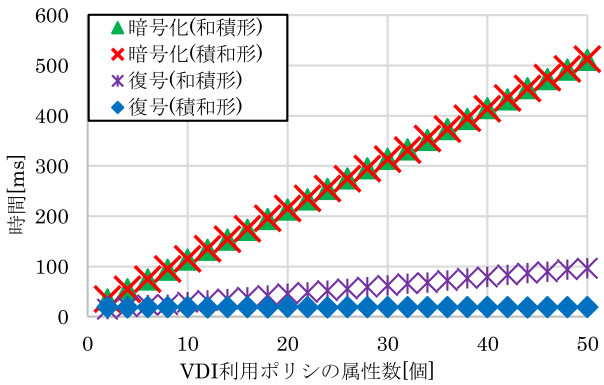
測定には clock_gettime 関数を用い，暗号化と復号をそれぞれの暗号で 1,000 回試行の平均を**表 3** に示す．ここで，暗号化，復号，ハッシュ化はいずれもパスワードファイルに対するそれぞれの処理時間を示す．

**(2) VDI 利用ポリシ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する．測定方法は (1) と同様に clock_gettime 関数を用い，1,000 回試行の平均を求めた．CP-ABE の鍵長は 2,048 bit とする．また，VDI 利用ポリシの属性数を (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する．結果を**図 5** に示す．




(a) AND/OR 結合で増やした場合




(b) 和積形/積和形で増やした場合

図 5 ポリシの属性数増加時の暗号化/復号時間
**Fig. 5** Encryption/decryption time and the number of policies.

**(3) 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 利用ポリシの属性数を

© 2019 Information Processing Society of Japan

AND 結合 50 個で 100 回連続暗号化

（イ） VDI 利用ポリシの属性数を 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，抽出した CPU 使用率を足し合わせたものを抽出回数で割った値を平均 CPU 使用率とする．CP-ABE の鍵長は 2,048 bit とする．

測定結果は，（ア）の場合の平均 CPU 使用率は 71.84%で，（イ）の場合の平均 CPU 使用率は 76.42%であった．

#### 5.2.3 VDI 利用者の作業時間に関する考察

表 3 より，CP-ABE の暗号化にかかる時間は RSA 暗号の約 4.5 倍，復号にかかる時間は RSA 暗号の約 1.6 倍であった．CP-ABE は RSA 暗号より時間がかかるが，サーバ，クライアント側いずれも 100 ms 以下である．この認証は VDI 利用者が VDI を利用開始するときに 1 度だけに行われるものであり，その時間は VDI 利用者の作業時間を大きく増大するものでなく，クラウドアプリケーション自体の動作にも影響を与えない．表 3 のハッシュ化は図 4 の VDI 利用認証サーバ/クライアントにおける VNC パスワードファイルのハッシュ化にかかる時間であり，その他の処理は図 4 における各種メッセージの伝送遅延（1 ms/メッセージ），VDI 利用ポリシ問合せ，VNC パスワード変更/要求にかかる時間である．

図 5 (a) より，OR 結合の復号以外すべての場合で同様に線形増加するが，暗号化のほうがその傾きが大きい．復号の OR 結合の場合では約 15 ms から 16 ms の間でほぼ一定であった．図 5 (b) も図 5 (a) と同様の傾向が見られた．cpabe toolkit では秘密分散法を用いて AND と OR での演算を実装している．VDI 利用ポリシの属性がすべて AND 結合の場合，秘密情報を $n$ 個に分割した分散情報がすべてそろう必要がある．すべての分散情報に対して処理が行われるため，AND 結合に比例して CP-ABE の処理時間が増加すると考えられる．VDI 利用ポリシの属性がすべて OR 結合の場合，$n$ 個の分散情報のうちどれか 1 つでも得られれば元の情報を得る．OR 結合の場合，暗号化の際は AND 結合と同様に $n$ 回の暗号化処理が必要となるが，復号の際は合致する属性が見つかった時点で 1 回だけ復号するので，属性数が増えても処理時間はほぼ一定である．このことから属性数が増えて VDI 利用者の作業時間が大きく増大することはない．

(3) の負荷測定において，（ア），（イ）ともに平均 CPU 使用率は 70%台と高かったが，一般的に VDI 環境をネットワーク経由で VDI 利用者が用いる端末は PC であり十分な能力があると想定されることから，VDI 利用前の 1 度の認証においてこの使用率となっても実用上支障ないと考えられる．モバイル端末で必要な場合は文献 [5] のような端末の処理負荷の軽減も提案されている．

### 5.3 評価のまとめ

実験や考察を通して，CP-ABE は RSA 暗号では難しい属性の表現や VDI 利用者間で秘密鍵の共有ができることから VDI 共有の認証に有効であることを示した．また，VDI 利用ポリシの属性数が増加しても VDI 利用者の作業時間は大幅に増大させることなく，CP-ABE での作業権限の認証や複数人での作業の引継ぎの利便性に影響を与えるものでないことを示した．これにより，3 章で示した認証機構の要件 2 を満たすことができている．さらに，5.1 節の鍵管理コストの比較により開発した認証システムは要件 3 も満たすことを示した．

## 6. おわりに

本研究では公開鍵暗号方式の一種で，属性を柔軟に変更することができる CP-ABE に着目して，共同作業として VDI 共有を対象とし，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．

現在，本認証機構において作業の共有のために VDI 共有を用いているが，共有される VDI 上では意図しないアプリケーションが委譲される可能性が考えられる．そのため，VDI 上でアプリケーション単位の委譲ができる仕組みが必要である．今後は属性ベース暗号を用いた認証システムを様々なクラウドサービスへ適用し管理負荷の面で改善を行う．

**謝辞** 本研究にあたり，有益なコメントをいただいた東海大学情報通信学部大東俊博准教授に感謝します．本研究の一部は日本学術振興会科学研究費助成金 18K11266, 16H02808 の支援を受けて実施しました．

### 参考文献

[1] 松本悦宜, 苦木大輔, 内田 恵, 近藤伸明, 満永拓邦, 五十嵐寛，力宗幸男：属性ベース暗号を用いたオンラインストレージサービス用クライアントの実装評価，電子情報通信学会技術研究報告，Vol.111, No.393, LOIS-69, pp.73–78 (2012).

[2] 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 (2014).

[3] Bethencourt, J., Sahai, A. and Waters, B.: Ciphertext-policy attribute-based encryption, *IEEE Symposium on Security and Privacy*, pp.321–334, IEEE Computer Society (2007), DOI: 10.1109/SP.2007.11.

[4] 永見健一，伊波源太，笹川 浩，脇谷康宏：セキュアなオンラインストレージシステムの提案，情報処理学会研究報告，Vol.2011-IOT-15, No.7, pp.1–5 (2011).

[5] 石黒 司，清本晋作，三宅 優：モバイルクラウド環境における属性ベース暗号の改良，コンピュータセキュリティシンポジウム 2011 論文集，Vol.2011, No.3, pp.421–426 (2011).

[6] Shamir, A.: Identity Based Cryptosystems and Signa-

© 2019 Information Processing Society of Japan

ture Schemes, *CRYPTO 1984*, LNCS, Vol.196, pp.37–53 (1984), DOI: 10.1007/3-540-39568-7_5.
[7] TigerVNC, available from ⟨http://tigervnc.org/⟩ (accessed 2018-06).
[8] Advanced Crypto Software Collection, available from ⟨http://acsc.cs.utexas.edu/cpabe/⟩ (accessed 2018-06).

**林 健汰**

2017 年広島市立大学情報科学部卒業．現在，同大学大学院情報科学研究科前期課程在籍．クラウド基盤に関する研究に従事．

**加森 剛徳**

2017 年広島市立大学情報科学部卒業．現在，同大学大学院情報科学研究科前期課程在籍．クラウド基盤に関する研究に従事．

**前田 香織** （正会員）

1982 年広島大学総合科学部卒業．同大学工学部助手，（財）放射線影響研究所技術員，広島市立大学情報科学部助手，同大学情報処理センター助教授を経て，現在，同大学大学院情報科学研究科教授．博士（情報工学）．コンピュータネットワーク，マルチメディア通信に関する研究に従事．電子情報通信学会，IEEE 各会員．

**近堂 徹** （正会員）

2001 年広島大学工学部第二類（電気系）卒業．2006 年同大学大学院工学研究科博士課程修了．現在，広島大学情報メディア教育研究センター准教授．博士（工学）．コンピュータネットワーク，リアルタイムマルチメディア通信，仮想化技術に関する研究に従事．電子情報通信学会会員，IEEE 各会員．

**相原 玲二** （正会員）

1981 年広島大学工学部第二類（電気系）卒業．1986 年同大学大学院工学研究科博士課程後期修了．同大学助手，同大学集積化システム研究センター助教授を経て，現在，同大学情報メディア教育研究センター教授．工学博士．コンピュータネットワークに関する研究に従事．電子情報通信学会，IEEE Communications Society 各会員．

© 2019 Information Processing Society of Japan