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] 近堂 徹[†2] 相原 玲二[†2]

概要：クラウドアプリケーションを利用したファイルの共有や共同作業を行う場合，作業者の属性に基づいてファイルへのアクセス権限や作業権限を設定できると管理コストを下げる効果がある．本研究ではクラウドアプリケーションとして仮想デスクトップを対象とし，利用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ー属性ベース暗号を用いる．これにより，利用者数や属性数が増えても鍵の管理が煩雑にならず，共同作業や引継ぎの安全性を向上できる．仮想デスクトップ上の画面共有を対象とする認証機構のプロトタイプシステムを実装し，それを用いて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を示す．属性数やその組み合わせを複雑にするとオーバヘッドは大きくなるが，その時間は実用上問題がないことを示す．また，RSA 暗号との比較により，開発する認証機構が複数利用者の画面共有において有用であることを示す．

キーワード：仮想デスクトップ，画面共有，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]
TOHRU KONDO[†2] REIJI AIBARA[†2]

Abstract: Sharing files and/or making joint works with cloud applications, it has the effect of lowering the management cost of file access authority and/or usage authority based on users' attributes of organizations. In this research, we focus on virtual desktop infrastructure as a cloud application, and develop an authentication mechanism based on users' attributes using Cyphertext-Policy Attribute-Based Encryption. Using the mechanism the management of encryption keys is not complicated even if the number of users and attributes increase, and joint works are securely completed. We implement a prototype system of a virtual window using the authentication mechanism as the joint work on the virtual desktop and show the overhead of the authentication processing of the system. We show that the proposed mechanism is practical even if the overhead becomes larger if the number of attributes increase and those combination is more complicated. In addition, we show that our developed authentication mechanism is useful for screen sharing with multiple joint workers by comparison with the RSA cryptosystem.

Keywords: Virtual desktop environment, Window 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をより求められる．クラウド上のデータの保管には暗号化がその対策の一つとなるが，クラウドサービスによるファイルの共有や作業の共有化に対して公開鍵暗号方式では必ずしもその要求に答えることができない．すなわち，暗号鍵と公開鍵が１対１のため，複数の共同作業者（以降，利用者）でファイルを共有する場合は１対１の鍵配布では鍵の管理が煩雑になる．また，対象者の属性のみを用いて，または属性の組み合わせで共有や共同作業の可否を判断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ー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）[3]を用いる．利用者の属性でファイルのアクセス可否を判断する場合，CP-ABE は有効であるが，クラウドアプリケーションを用いた共同作業を対象としたものではない．

そこで本研究では，クラウドアプリケーション提供側が許可した利用者のみに作業権限を付与し，クラウドアプリケーション上での共同作業を実現する．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 を用いた認証機構により， VDI 提供側での制御で VDI 利用者側に与えられた特定の属性を有する利用者に対してのみ安全に VDI 環境を引き継ぐことができるシステムを構築する．これにより，複数の VDI 利用者の属性とポリシーによる認証を行うことで作業権限の設

†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

定ミスや鍵の運用コストの問題を解決する．この認証機構の開発により，複数利用者の共同作業や引継ぎの容易性を向上させることを目指す．

本論文の構成は以下のとおりである．2 章で関連研究を述べ，3 章で VDI の共同作業においてどのような権限管理が必要かを整理する．4 章で VDI の利用権限委譲のプロトタイプシステムを示し，5 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．これらのサービスの多くは，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，[1]はファイルの閲覧権限を，[2]はファイル名やディレクトリ名の表示や編集権限の管理をしている．[1]や[2]は CP-ABE を使うことで，組織内など複数の利用者でグループを作成して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，本研究の共同作業時の 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 暗号文ポリシー属性ベース暗号(CP-ABE)

公開鍵暗号など従来の暗号方式ではクラウドにデータを保存することには使えるが，複数の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一種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ー（属性を AND 又は OR で結合したもの）を埋め込み，特定の属性集合を持つ利用者のみが復号できる公開鍵暗号方式の一種である．ポリシー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ー属性ベース暗号（CP-ABE）[3]である．

CP-ABE は以下のアルゴリズムからなる．

A) Setup: パラメータ λ を入力とし，マスター公開鍵 PK とマスター秘密鍵 MK を出力する．

B) Encrypt: PK，平文 M，ポリシーA を入力とし，A が埋め込まれた暗号文 CT を出力する．

C) Keygen: MK，属性集合 S を入力とし，秘密鍵 SK を出力する．

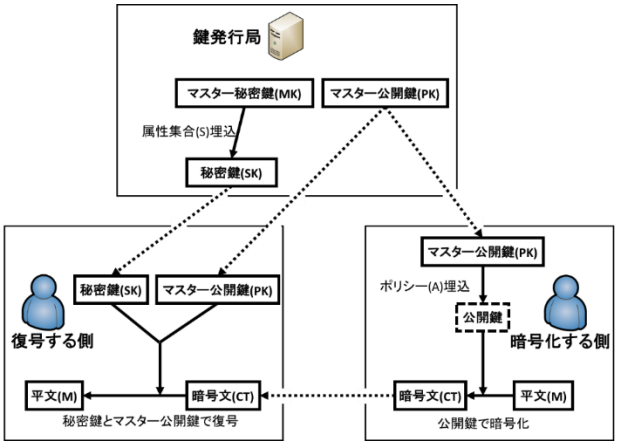


図 1 暗号文ポリシー属性ベース暗号の処理の概要

D) Decrypt: PK，CT，SK を入力とし，CT の A に SK が適合すれば平文 M を出力する．

CP-ABE の処理の概要を図 1 に示す．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に復号する側の属性集合を埋め込み秘密鍵を生成する．生成した秘密鍵とマスター公開鍵は復号する側，マスター公開鍵を暗号化する側に渡す．暗号化する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，生成した公開鍵で平文を暗号化する．暗号文を復号するには，マスター公開鍵と秘密鍵を使う．CP-ABE では，暗号文のポリシー（例：(情報科学部 AND 情報工学科) OR 教員）に対して秘密鍵の属性集合（例：情報科学部，情報工学科，4 年）が満たすとき，暗号文は秘密鍵によって復号される．

CP-ABE と RSA の公開鍵と秘密鍵の関係を図 2 に示す．CP-ABE は図 2 のように，公開鍵と秘密鍵が 1 対多の関係となり，ひとつの公開鍵に対して疑似的に複数の秘密鍵を共有することができる. 同様のことを RSA 暗号で実現するには 1 つの鍵を複数人で共有する必要があるため，共有している人のいずれかから秘密鍵が漏えいすれば，共有しているすべての秘密鍵および対応する公開鍵の交換が必要となる．

CP-ABE においては秘密鍵が漏えいしたとしても，秘密

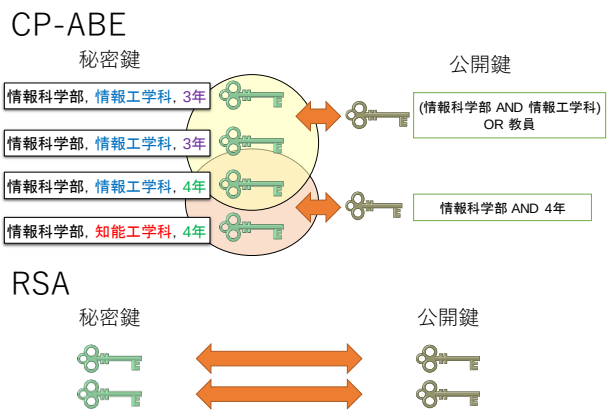


図 2 CP-ABE と RSA の公開鍵と秘密鍵の関係

鍵を失効リスト等で管理しておけば公開鍵を取り換える必要がないうえに，疑似的に共有している他の秘密鍵は別の秘密鍵であるため交換は不要である．

一方，CP-ABE では鍵発行局は信頼される機関である必要がある．復号する側が自身の秘密鍵を取得するとき，鍵発行局は復号する側と秘密鍵の対応を参照・認証し，適切な秘密鍵を TLS（Transport Layer Security）を用いるなどして安全に配布しなければならない．

CP-ABE 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の改良をする研究もある[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 アドレス等の 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もつような場合を表現することができない．

3. 共同作業時の VM の使用権限管理

本研究では，VDI を構成する VM の使用権限を同一の属性を持つ利用者に委譲し，VM（デスクトップ OS ）上の処理を安全に引き継ぐような場面を想定する．ここで「VM 上の仮想デスクトップ環境をネットワーク経由で利用する利用者」を VM 利用者と定義する．ここでは共同作業として複数の VM 利用者の画面共有を対象とし，VM 利用者を画面利用者と呼ぶ．このとき，VM 利用者がどのグループに属すかという属性に合わせて作業権限を設定できる認証機構が必要となり，利用者単位の認証は利用者数が増加したときの認証鍵の管理コストが課題となる．

4. 権限委譲機構付き画面共有システム

VDI を複数の VM 利用者間で安全に引き継ぐことを目的とし，複数利用者で画面共有をするシステムに適用する認証機構を開発する．

本認証機構では，属性ベース暗号を用いることで，共同作業として複数の VM 利用者が VM 上のデスクトップ OS の画面を共有し，それを複数の利用者間で安全に引き継ぐことができるようにする．画面共有には VNC（Virtual Network Computing）[7]を用いる．

4.1 実現する機能

本システムでは VDI を利用しようとする VDI 利用者を属性により認証する機能と，権限を委譲することで複数の VDI 利用者間で作業を引き継ぐことができる機能を実現する．

4.2 システム構成

使用権限委譲可能な認証システムの構成を図 3 に示す．画面利用者端末には VNC クライアントと画面利用認証クライアントが，VDI 提供ホストには VNC サーバと画面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，画面利用者と VDI 提供ホストに必要な鍵を提供する．

VNC クライアントが VNC サーバの画面を利用する際，画面利用認証サーバと画面利用認証クライアントの間で認証が行われる．その際，CP-ABE を用いて画面利用者の作業権限を認証する．また，既に認証された画面利用者から別の利用者に作業を引き継ぎたい場合，別の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

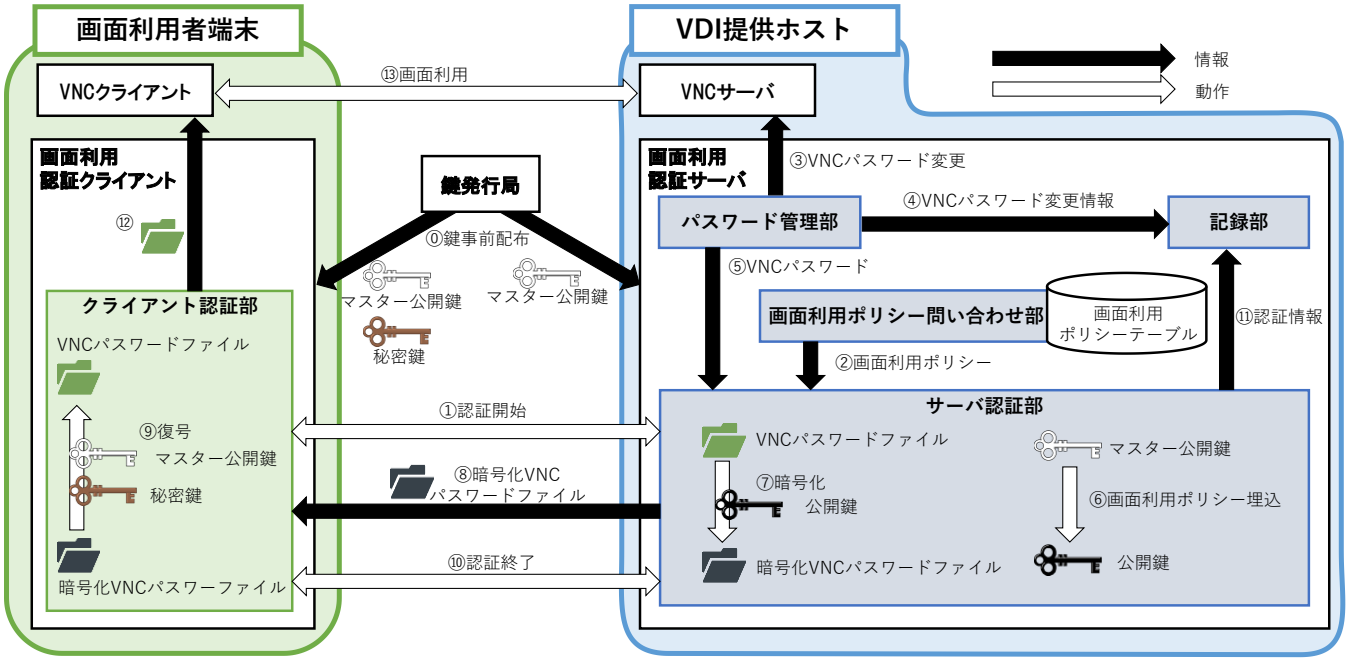


図 3 システム構成図

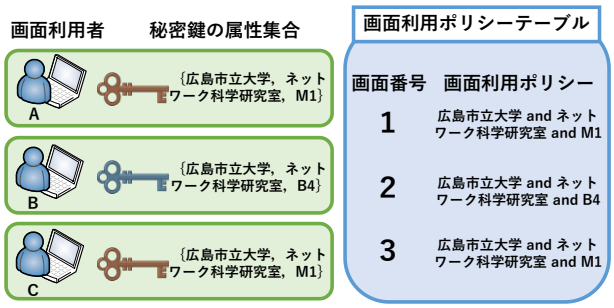


図 4 システムの秘密鍵の属性集合とポリシーの関係

ば使用権限委譲を行う．使用権限移譲が行われた際，混乱を防ぐためにそれまでの画面利用者の利用は強制終了となる．

画面利用認証クライアントや画面利用認証サーバで必要な秘密鍵及びマスター公開鍵は図 3 の鍵発行局から事前に必要な鍵を受け取っておくものとする．

システムの利用者が持つ秘密鍵の属性集合と画面利用のためのポリシーの関係を図 4 に示す．図 4 の画面番号（VNC サーバで稼働する画面の番号）に対応する画面利用ポリシーは図 3 の画面利用認証サーバ内の画面利用ポリシーテーブルに格納される．画面利用者のごとの属性は図 3 の画面利用認証クライアントの秘密鍵に埋め込まれる．図 4 の場合，VDI 提供ホストで画面 1 を利用できるのは画面利用者 A と C となる．

4.3 動作フロー

画面共有システムの認証機構の動作フローを図 5 に示す．

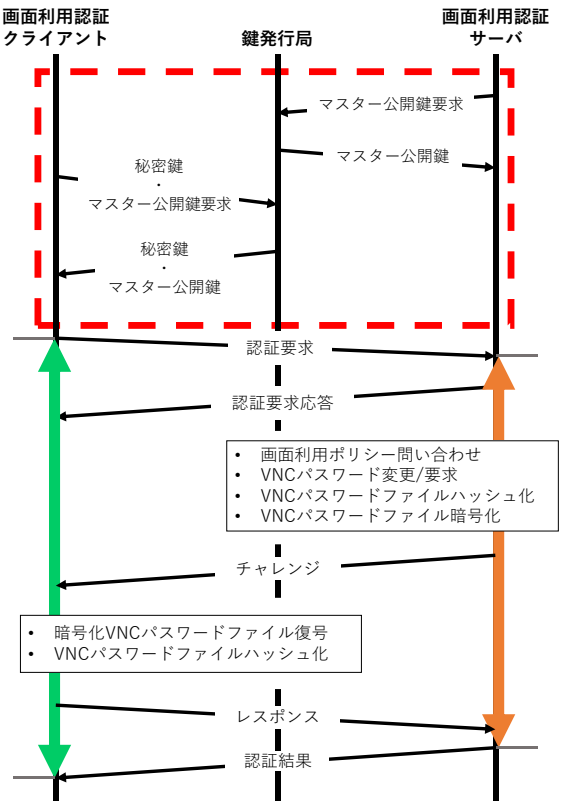


図 5 画面共有システムの認証機構の動作フロー

なお，図は認証部分に焦点を当てて説明するため，VNC サーバおよびクライアントについては省略している．

まず，画面利用認証クライアントと画面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（赤色破線部分）．

次に，認証処理について説明する．具体的には以下の手順となる．画面利用者は画面利用開始時に画面番号と共に認証要求を画面利用認証サーバへ送る．画面利用認証サーバは画面認証クライアントに認証要求応答を返し，認証要求に含まれる画面番号に対応する画面利用ポリシーとマスター公開鍵から公開鍵を生成する．生成された公開鍵で画面番号に対応する VNC のパスワードファイルを暗号化し，画面利用認証クライアントにチャレンジとして送る．その際，画面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．画面利用認証クライアントでは属性集合が埋め込まれた画面利用者の秘密鍵とマスター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画面利用認証サーバへレスポンスとして送る．画面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，認証結果を画面利用認証クライアントへ返して認証を終了する．画面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，画面の利用が開始する．

4.4 プロトタイプシステムの実装

4 章の設計をもとにプロトタイプシステムを実装した．画面利用認証クライアントと画面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．

表 1 VM の仕様

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

項目	内容
コンパイラ	gcc (GCC) 4.8.5 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), openssl 1.0.1 (RSA)

表 3 認証時間 [単位:ms]

		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	—	—	—

5. 評価

5.1 実験目的

開発したシステムは CP-ABE を用いる．一つ目に，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評価する．二つ目に，暗号化と復号にかかる時間は画面利用ポリシーの属性数とその結合方法によって変化する．画面利用ポリシー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．三つ目に，CP-ABE の暗号化と復号にかかる端末への負荷を測定し，実用的な負荷であるかを考察する．

5.2 実験環境

画面利用者端末（画面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（画面利用認証サーバ/VNC サーバが動作する端末）は同一 IPv6 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．

5.3 実験方法と実験結果

5.3.1 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，画面利用認証サーバの認証時間（図 5 の橙色線区間）と画面利用認証クライアントの認証時間（図 5 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画面利用ポリシーの属性数は 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 2048bit 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 1000 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．

5.3.2 画面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

画面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する．測定方法は前節と同様に 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 とする．また，画面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する．結果を図 6 に示す．

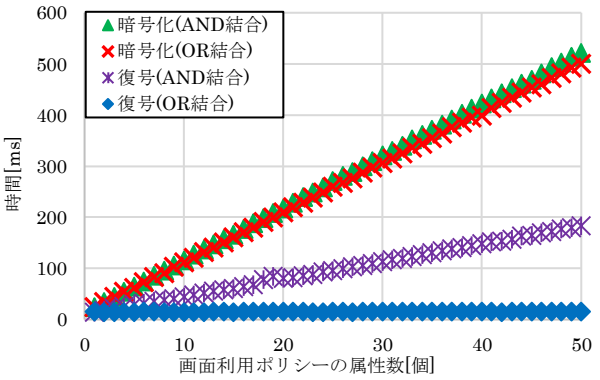
5.3.3 CP-ABE の処理負荷の測定

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．

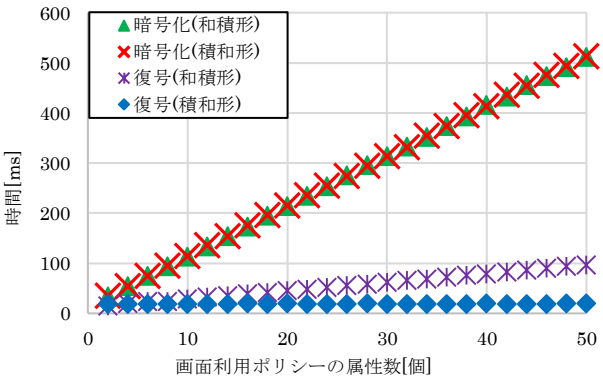
(ア) パスワードファイルを画面利用ポリシーの属性数を AND 結合 50 個で 100 回連続暗号化

(イ) 画面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



(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 6 ポリシーの属性数増加時の暗号化/復号時間

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 2048bit 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．

5.4 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，この認証は画面利用者が画面を利用開始する時に 1 度だけに行われるものであり，100ms は実用上問題ないと考えられる．

図 6 (a)より，OR 結合の復号化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．復号化の OR 結合の場合では約 15ms から 16ms の間でほぼ一定であった．図 6 (b)についても図 6 (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．画面利用ポリシーの属性がすべて 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．画面利用ポリシーの属性がすべて 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になると考えられる．

5.3.3 の負荷測定において，（ア）（イ）共に平均 CPU 使用率は 70%台と高かったが，一般的に仮想デスクトップ環境をネットワーク経由で利用者が用いる端末は PC であると想定されることから，画面利用前の一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．

実験を通して，CP-ABE は RSA 暗号では難しい属性の表現や複数の利用者間で疑似的な秘密鍵の共有ができることから画面共有の認証に有効であることを示した．また，画面利用ポリシーの属性数が増加しても CP-ABE での作業権限の認証や複数人での作業の引継ぎ，安全性や利便性に影響を与えるものでないことを示した．

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，共同作業として画面共有を対象とし，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，画面利用者端末と VDI 提供ホストは鍵発行局からマスター公開鍵と秘密鍵をあらかじめ取得した状態で認証を行っている．そのため，鍵発行局との認証をした上で鍵を取得するなどといった改良を行う．また，既に認証を終えた先行の画面利用者と次の認証済みの画面利用者との間で引き継ぎの確認をせず強制的に引き継いでいるため，確認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システムを様々なクラウドシステム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，有益なコメントを頂いた東海大学情報通信学部 大東俊博講師に感謝します. 本研究の一部は日本学術振興会科学研究費助成金 15K00130，16H02808 の支援を受けて実施しています.

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, Jan. 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, Mar. 2014.

[3] J. Bethencourt, A. Sahai, and B. Waters, “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 2011-IOT-15(7), pp.1-5, Sep. 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, Oct. 2011

[6] Shamir, “Identity Based Cryptosystems and Signature Schemes,” CRYPTO 1984, Vol.196 of LNCS, pp.37-53, 1984. DOI: 10.1007/3-540-39568-7_5

[7] TigerVNC, http://tigervnc.org/ (Jan. 2017 参照).

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