特集論文

クラウドシステム構築のためのセキュリティ基盤(1) ーモデルシステムと実証実験ー

村澤　靖*　高畑泰志**　津國　剛***　澤部直太***

Security Platform for Cloud Computing Based Systems—Testbed Experiments—

Yasushi Murasawa, Yasushi Takahata, Takeshi Tsukuni, Naota Sawabe

要　旨

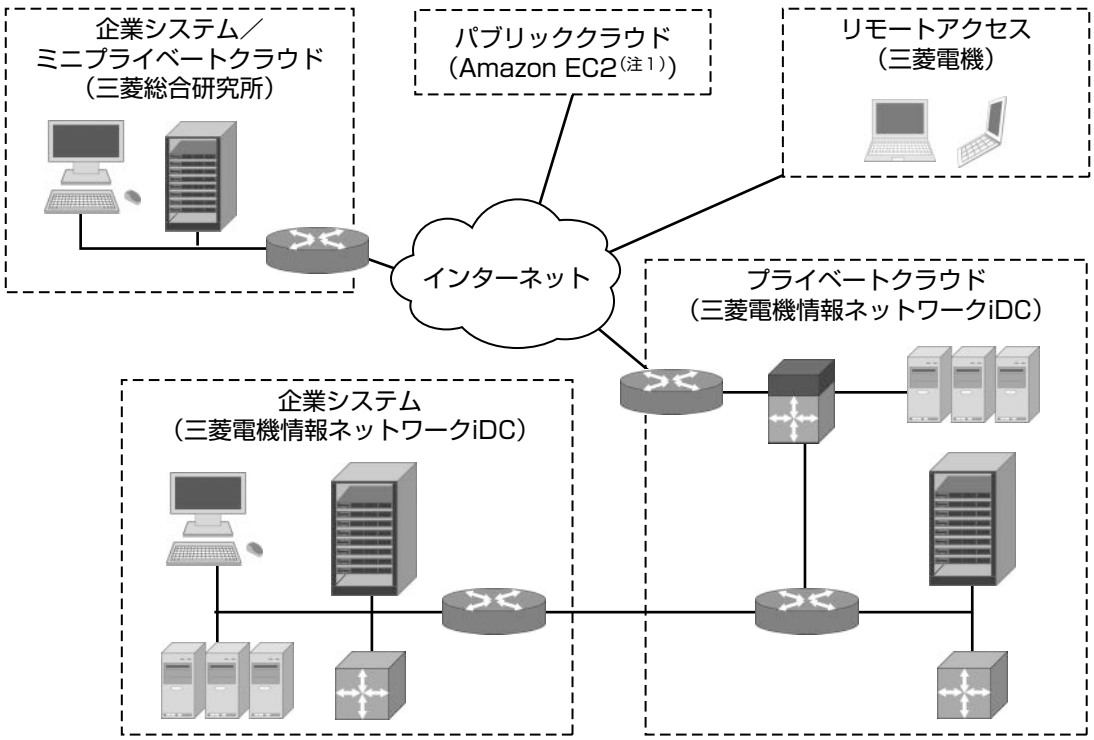
クラウドコンピューティングは，ITリソース調達の柔軟性や費用対効果などの面から，企業システムのプラットフォームとしての普及が期待されているが，セキュリティ上の課題が残されていることなどによって，企業システムとしての利用は一部に留(とど)まっている。クラウド環境へ移行したシステムを利用するに当たっては，従来の企業システムと同様に，データやネットワークなど様々なレベルでの利用者に応じたアクセス制御が必要である。その際，アカウント情報は個人情報であり，高度な機密情報であることから，アカウント情報を保護した上で実現する必要がある。

我々は，企業システムのクラウド環境への移行期を想定し，企業システムが置かれた企業環境と，プライベートクラウド，パブリッククラウドからなるクラウド環境及びリモートアクセス環境からなる実証実験システムを構築し，次の観点から検証した。

(1)　企業システムとクラウド間の認証連携の実現
(2)　データの利用者権限管理の実現
(3)　仮想ネットワークによるアクセス制御の実現
(4)　大規模ユーザー環境への対応の実現
(5)　システム運用者に対するシステム操作制御の実現

検証では，企業ユーザーがクラウド環境で社内外のユーザーとファイルを共有するシーンを想定したファイル共有アプリケーションを使って，企業が業務でクラウド環境を利用する各種場面を想定したシナリオを実施し，実装した認証基盤やデータ利用権管理機能などの有用性を確認した。

本稿では，実証実験システムとその実証実験の概要を中心に述べる。なお，認証基盤及び仮想ネットワークについては，別稿で詳しく述べる。



（注1）Amazon EC2は，Amazon Technologies, Inc. の登録商標である。

iDC：internet Data Center

実証実験環境の全体像

実証実験環境は，企業環境とクラウド環境に大きく分かれている。クラウド環境は，プライベートクラウドとパブリッククラウドから構成した。パブリッククラウドは，Amazon EC2(Elastic Compute Cloud)サービスを利用した。また携帯電話などリモートアクセスも可能とした。

*三菱電機㈱ 情報技術総合研究所　**同社 同研究所(情報学博士)　***㈱三菱総合研究所

1. まえがき

企業システムは，ホストコンピュータを用いた業務システム，クライアント・サーバシステムを経て，現在ではWebコンピューティング技術の活用によって，業務の効率性の向上や法規制，各種の脅威などに対応するものとなってきている。一方，ここ数年で台頭してきたクラウドコンピューティングについては，ITリソース調達の柔軟性や費用対効果などの面から，企業システムのプラットフォームとしては非常に魅力的である。しかし，クラウド環境におけるセキュリティ実装の不明確さなどによって，データ保護への懸念などの課題が残されており，企業システムとしてクラウド環境を利用することを躊躇(ちゅうちょ)させる原因となっている。仮に，クラウド環境の利用を考慮する場合，一般には既存のIT資産があることから，すべてのシステムを一度にクラウドに移行することは少ないと考えられる。現実的には，既存システムを機能別，役割別にサブシステムに分割し，クラウド環境が同等の機能を提供している部分から移行していき，既存サブシステムとの連携を図るといった移行シナリオを用いることが想定される。クラウド環境へ移行したシステムを利用するに当たっては，従来の企業システムと同様に，データやネットワークなど様々なレベルでの利用者に応じたアクセス制御が必要である。その際，アカウント情報は個人情報であり，高度な機密情報であることから，アカウント情報を保護した上で実現する必要がある。この課題に取り組むため，実証実験システムを構築して検証した結果について述べる。

2. 実証実験システム

2.1 実証実験環境の全体像

実証実験環境の全体像を**図1**に示す。

システムは，企業環境とクラウド環境に大きく分かれており，**表1**に示すようにそれぞれ企業システム，及びプライベートクラウド，パブリッククラウドから構成した。パブリッククラウドの構築に当たってはAmazon EC2サービスを利用した。また，携帯電話やモバイル端末からインターネット経由でリモートアクセスも可能とした。

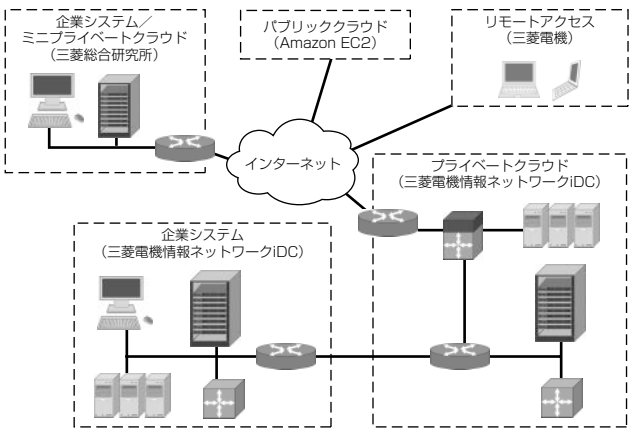


図1．実証実験環境の全体像

ソフトウェアはOSS(Open Source Software)をできる限り活用するとともに，認証機能やデータのアクセス制御機能の実装に当たり，SAML(Security Assertion Makeup Language)やXACML(eXtensible Access Control Markup Language)といった標準仕様を採用した。また，仮想ネットワーク[(1)]やPUZZLET認証[(2)]といった三菱電機の保有技術も活用した。

2.2 各サブシステムの構造

企業システム，プライベートクラウド，パブリッククラウドのシステム構造は共通であり，その概略構成を**図2**に示す。

(1) 企業システム

企業システムでは，ブレードサーバ上に仮想化ソフトウェアとしてVMware[(注2)]を搭載し，シングルサインオン機能を実現するOSS のOpenSSO(Single Sign-On)を使った認証認可サーバ，Webサービスによるアプリケーション連携機能を実現するOSSのServiceMixを使ったESB(Enterprise Service Bus)サーバなどを動作させた。10万人分のアカウント情報を認証認可サーバ内に保管した。また，大規模ユーザー環境に対応するため，ロードバランサを使ってサーバの処理を負荷分散している。

(2) プライベートクラウド

プライベートクラウドでは，ブレードサーバ上に仮想化ソフトウェアとしてXen[(注3)]を搭載し，企業システムと同様，認証認可サーバ，ESBサーバやロードバランサなどから構成している。また，インターネットアクセス用にDMZ(DeMilitarized Zone)を構築し，メールサーバなどを個別に設置した。

表1．各サブシステムの説明

分類	システム名	説明
企業環境	企業システム	従来の企業システムの中核部分が動作するシステム。利用者のアカウント情報を保管している。
クラウド環境	プライベートクラウド	従来の企業システムの一部が移行した社内向けサブシステムの位置付け。社内利用のデータを保管している。
	パブリッククラウド	従来の企業システムの一部が移行した社外向けサブシステムの位置付け。社外とやり取りするデータを保管している。

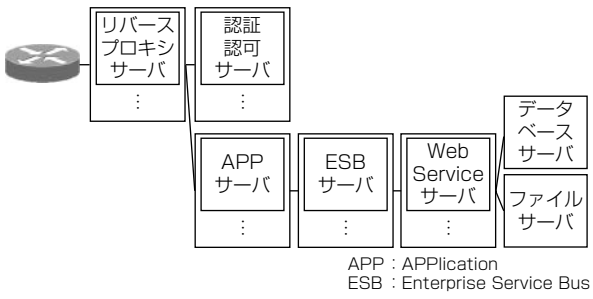


図2．各サブシステムの構造

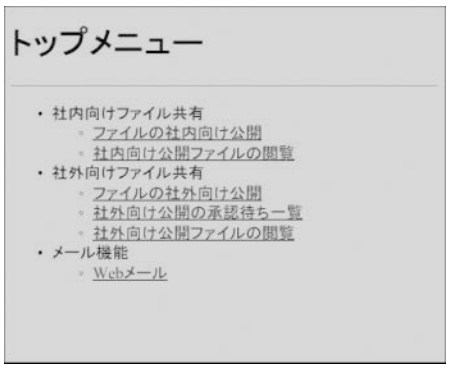


図3．トップメニュー画面

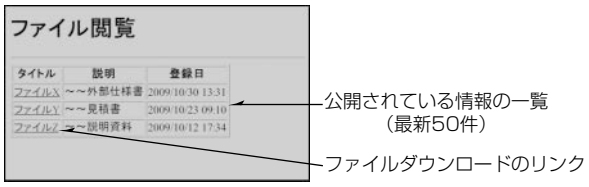


図4．ファイル一覧画面

(3) パブリッククラウド

パブリッククラウドは，Amazon EC2サービスを利用して，固定IP(Internet Protocol)アドレスを割り当てた7台のサーバ上に，企業システムと同様認証認可サーバ，ESBサーバなどを動作させた。

(注2) VMwareは，VMware, Inc.の登録商標である。
(注3) Xenは，Citrix Systems, Inc.の登録商標である。

2.3 評価用アプリケーション

今回，評価用業務アプリケーションとして，社内ユーザーがクラウド環境で社内外のユーザーとファイルを共有するシーンを想定したファイル共有アプリケーションを開発した。社内ユーザーが他の社内ユーザーへファイルを公開したり，社外ユーザーへ上長承認を経てファイルを公開したりするためのユーザーインタフェースを提供する。トップメニューを**図3**に，ファイル一覧画面を**図4**に示す。

ファイルの閲覧やワークフローなど，アプリケーションで共通的に利用する機能はサービスとしてWeb Serviceサーバ上で動作する。アクセス元アプリケーション，及び利用者の権限の組合せによって各サービスへのアクセスを制御するサービス認可も実装した。

3. 実証実験

実証実験は，企業が業務でクラウド環境を利用する各種場面を想定した10個のシナリオに基づく検証を行った。その概要について述べる。

(1) 企業システムとクラウド間の認証連携

企業システム及びクラウドの相互間で，認証及び認可が適切に連携できることを検証した。企業システムで認証されたユーザーAが，プライベートクラウドへ再認証することなくアクセスするシナリオの一部を次に示す。

①ユーザーAが企業システム上のパソコンからファイル共有アプリケーションにログオンする(**図3**が表示される)。
②ユーザーAは“ファイルの社内向け公開”を選択し，ファイルXを作成し，ファイルXに対して，ユーザーBはアクセス許可，ユーザーCはアクセス不可の設定を行う。
③ユーザーAはファイルXを登録すると，ファイルXがプライベートクラウド内に保管される(ユーザーAでプライベートクラウドへ認証連携機能によってシングルサインオンが実行される)。

シナリオに沿った操作を実施し，システム動作時に出力されるアプリケーションやミドルウェアのログによって，想定した機能が動作していることを確認した。

(2) データの利用者権限管理

プライベートクラウド，パブリッククラウドで，ユーザー単位でデータの利用が適切に制御できることを検証した。ユーザーCには参照不可の設定がされているプライベートクラウド上のファイルXが保護されていることを確認するシナリオの一部を次に示す。

①ユーザーCが企業システム上のパソコンからファイル共有アプリケーションにログオンする(**図3**が表示される)。
②ユーザーCは“社内向け公開ファイルの閲覧”を選択する(**図4**が表示される)。
③ユーザーCはファイルXを指定するが，ファイルを読み出すことができない。

シナリオに沿った操作を実施し，システム動作時に出力されるアプリケーションやミドルウェアのログによって，想定した機能が動作していることを確認した。また，②において，“社外向け公開ファイルの閲覧”を選択することで，パブリッククラウド上のファイルについても同様に確認した。

(3) 仮想ネットワークによるアクセス制御

IPv6を活用した仮想ネットワークによって，クラウド環境に配置される各サーバへのアクセスが適切に制御されることを検証した。具体的には，企業システム～プライベートクラウド間通信路を論理的に分割し，pingによるサーチによって，あらかじめ許可された組合せの装置間だけが通信可能で，他の組合せでは通信不可能となるように制御できていることを確認した。

(4) 大規模ユーザー環境への対応

大規模ユーザー環境での実証実験システムの動作を評価するため，1万ユーザーがアクセスし，ファイル一覧画面表示の認証連携機能に関する応答性能(応答時間)やエラー発生率を測定した。測定に当たっては，**図5**に示すようにユーザー操作をシミュレーションする性能負荷ツールによ

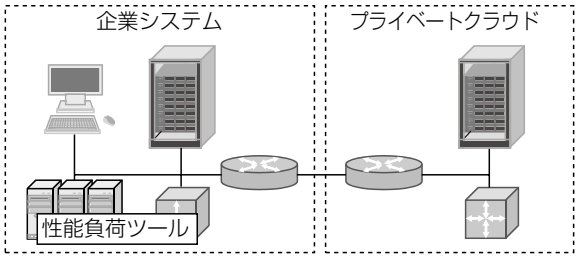


図5．スケーラビリティ検証での構成

表2．スケーラビリティ検証結果

性能指標	目標	測定値
応答性能(ms)	3秒以内	358.0
エラー発生率(%)	0.05未満	0.01

って，企業システムからプライベートクラウドのリソースへのアクセスを実施した。

表2に示すようにそれぞれ目標性能を満たすことを確認した。

(5) システム運用者に対するシステム操作の制御

企業システムのクラウド環境移行時に想定されるセキュリティ脅威の1つとして，クラウドのシステム運用者が管理者権限でクラウドを利用するケースが想定される。この実証実験では，高度なセキュリティ機能が付加されたSELinuxの機能を利用した。プライベートクラウドのシステム運用者によるファイルへのアクセスを防ぐセキュリティポリシーを設定し，OSのログによって想定した機能が動作していることを確認した。

4. むすび

クラウドコンピューティングの普及によって，**図6**に示すようにこれまで企業内に閉じていたシステムが，今後アカウント情報は企業内で管理した状態で，外部のクラウド環境に移行すると考えられる。業務の遂行に必要な共通機能は，サービスとしてクラウド環境で提供され，グループ企業間などでクラウド環境を共同利用する形態も進展すると考えられる。今回の実証実験によって，このような新たなシステム形態で必要となる次の機能を検証することができた。

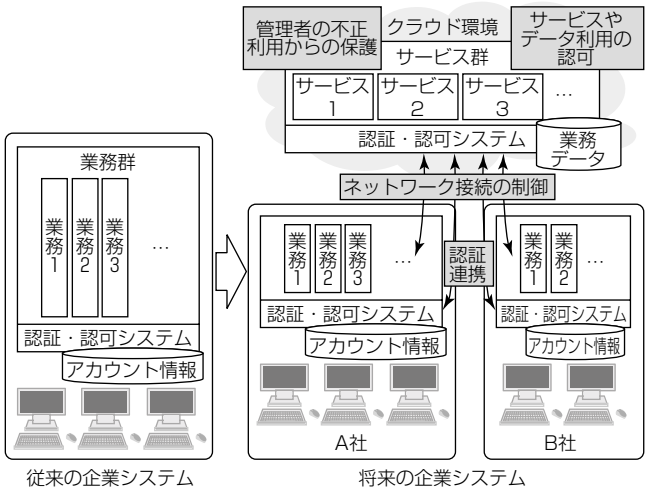


図6．将来の企業システムの形態

(1) アカウント情報を企業システム内のみに保管するとともに，セキュリティ要件に応じた複数の認証機能を提供するセキュアなシングルサインオン

(2) 企業システム又はクラウド上に配置されたサービス，データへのアクセス制御

(3) アドレス資源の豊富なIPv6を活用した仮想ネットワークによるネットワークレベルでのアクセス制御

(4) 管理者権限を持っているシステム運用者の操作の制御

実適用に向けては，信頼性や運用性などの非機能面についても検証が必要であり，今後取り組んでいく。

なお，この研究開発は，経済産業省平成21年度“新世代情報セキュリティ研究開発事業[3]”によって実施したものである。

参考文献

(1) 平井　肇，ほか：分散型仮想ネットワークにおける転送効率化方式の検討と試作機開発，電子情報通信学会技術研究報告，**107**，No.525，265～270（2008）

(2) 桜井鐘治，ほか：背景配列の移動量を用いた個人認証方式ののぞき見に対する安全性評価，情報処理学会論文誌，**49**，No.9，3038～3050（2008）

(3) 経済産業省：平成21年度“新世代情報セキュリティ研究開発事業（クラウドコンピューティングセキュリティ技術研究開発）”公募仕様書（2009）