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(2) ―認証基盤―

白木宏明*
原田篤史**
大沼聡久*

Security Platform for Cloud Computing Based Systems―Authentication Infrastructure―

Hiroaki Shiraki, Atsushi Harada, Akihisa Onuma

要　旨

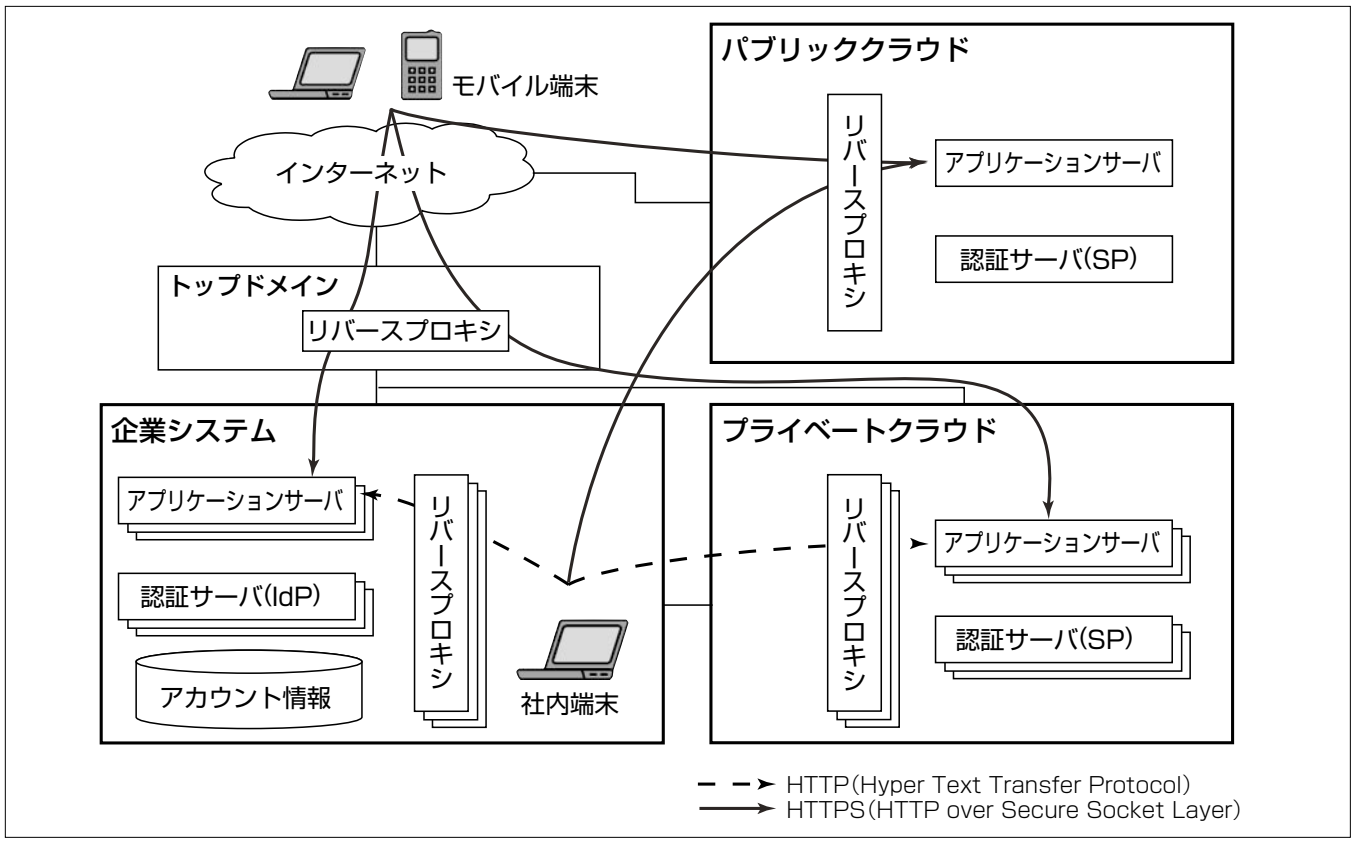
クラウドコンピューティングは今後，利用の拡大が期待されている[1]。しかし，クラウド環境を構築する際には，認証・認可や機密情報の管理等のセキュリティ上の問題が存在する。具体的には，機密情報であるアカウント情報を組織の外部となるクラウド環境中に保持することは避けるべきであり，かつ利用者の権限に応じてクラウド環境上のリソースに対するアクセスを制限しなければならないということである。

これらを解決するためには，クラウド環境上のシステムは，企業内システムでの認証システムと連携し，クラウド環境上の認証やリソースのアクセス制御を実現する必要がある。既存の企業内システムとクラウド環境間でアカウント情報の連携と保護を実現する手段を提供することが不可欠となる。

今回の“クラウド環境活用に向けた企業内既存システムとの連携実証実験”で，認証とアカウント情報を企業内に集約しつつ，クラウド環境上で認証・認可及びアクセス制御を実現することができる認証基盤の研究開発を行い，セキュリティ要件を満たすことの検証を目的として実証実験を実施した。

実証実験では，次の要件から評価を実施した結果，先に示したセキュリティ上の問題が解決されており，十分に実システムでの使用に耐え得ることを確認することができた。

(1) 企業内システムからクラウド環境へのシングルサインオン
(2) インターネットからクラウド環境へのシングルサインオン
(3) 認証情報に基づいたクラウド上のアプリケーションによるアクセス制御



認証基盤実証実験のシステム構成

クラウド環境活用に向けた認証基盤のシステム構成は，企業システムのクラウド移行を想定した企業システムとプライベートクラウド，パブリッククラウドからなる。アカウント情報は，企業システム内で管理を行う。クラウド環境上のアプリケーションを利用する場合には，企業システム上の認証サーバで認証を行い，その認証に基づきアクセス制御を実施する。

*情報技術総合研究所　**同研究所(情報学博士)

1. まえがき

現在，ITリソース調達の柔軟性や費用対効果などの面から，クラウド環境は企業システムのプラットフォームとして非常に魅力的であるが，セキュリティ実装の不明確さなどの課題が残されているため，企業システムとしてのクラウド環境の利用は制限されている[2]。

セキュリティ上の問題の一つとして，クラウド環境における認証・認可といったアカウント管理の機能が挙げられる。アカウント情報は個人情報を含む高度な機密情報であることから，組織から見て外部となるクラウド環境に保存することは避けるべきである。また，アカウント情報を含む各種の機密情報は，利用者サイドでアクセスコントロールすべきであり，システム上の特権ユーザーであるクラウド事業者に対するアクセスも制限する仕組みが必要である。このような機密情報の保護を実現した上で，既存の企業システムでの認証結果に基づきクラウド環境上のシステムと連携する手段，すなわち，認証連携を実現する。

クラウド環境におけるセキュリティ上の不安要素のうち，特にアカウント管理に焦点を当て，認証とアカウント管理機能を企業に集約しつつ，認証情報の連携によってクラウド上システムで利用できる認証基盤を研究開発し，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. 認証技術の動向

2.1 認証連携技術

認証連携(IDフェデレーション)技術は，ドメインを跨(またが)ったシステム間でのSSO(フェデレーテッド・シングルサインオン)や，ログアウト(グローバル・ログアウト)を実現するために，システム間で認証情報を伝播(でんぱ)する技術のことである。

2.1.1 主要技術

IDフェデレーションにおける主要技術としてSAML(Security Assertion Markup Language)，OpenID，CardSpaceがあり，**図1**に示すような関係となっている。

それぞれ独立して仕様が策定されたため，技術分野として共通する領域があり，これらの仕様間の相互接続を実現するための取組みが行われている。

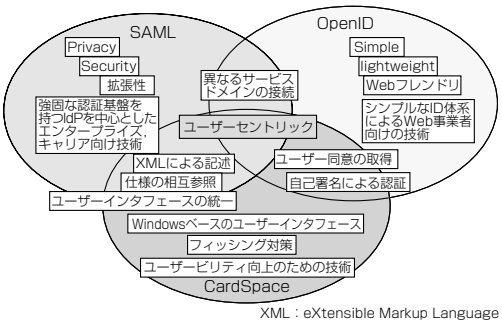


図1．IDフェデレーション主要技術の関係[2]

(1) SAML

SAMLはLiberty Allianceで策定されOASIS(Organization for the Advancement of Structured Information Standards)で標準化された技術仕様であり，認証，認可，属性といったセキュリティ情報をサービス間で交換するための表現形式及びプロトコルを規定している。強固な認証基盤を持つIdP(Identity Provider)を中心に高いセキュリティを必要とする企業，キャリア向けの認証連携の技術として主に用いられている[4][5]。

(2) OpenID

OpenIDはURL(Uniform Resource Locator)を利用し，サイトを越えて使用できる認証方式であり，シンプルでWebとの親和性が高いことから，ポータルサイトやブログなどWeb事業者向けの技術として主に利用されている[3]。

(3) CardSpace

Microsoft社が開発したインターネット上でのID管理，制御，交換のためのシステムである。.NET Framework 3.0の一部としてWindows Vista(注1)，XP等で使用可能な，ユーザービリティ向上のための技術である[4]。

(注1) WindowsとWindows Vistaは，Microsoft Corp.の登録商標である。

2.1.2 標準化の取組み

2009年6月に，IDフェデレーション技術を含めたID管理技術に関する標準化を目的としたカンターラ・イニシアティブ[3]が設立された(**図2**)。合わせて，これまで個別に活動してきたID管理技術の議論の場を1か所にまとめ，より広い視点からオープンに議論できる場を提供することも目的としている。

実質的な活動の中心は分科会活動で，ワークグループ(WG)とディスカッショングループ(DG)の2種類から構成される。WGは文書の発行，他団体への技術仕様のドラフト提出が可能であるが，DGは文書発行，提出する権限はなく，気軽に参加可能なフリーディスカッションの場として設立されている。

2.2 今後の動向

IDフェデレーションのプロトコルは，**2.1.1項**で述べた3技術に収束しつつあり，現在は各プロトコル間での相互運用の検討・実証実験の動きが盛んになっている。

クラウド環境において認証連携は不可欠な技術要素であ

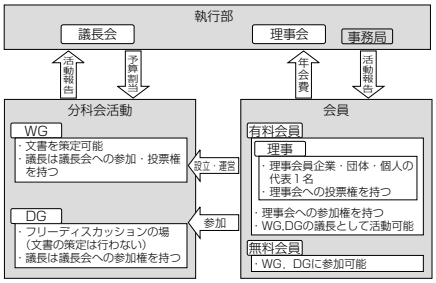


図2．カンターラ・イニシアティブの組織[2]

り，これらの標準化・相互運用の動きとともに，基盤技術としての利用が進むものと期待される。

3. 実証実験システム

3.1 認証基盤及びシステム構成

機密情報の保護が不可欠であるドメイン間の認証連携方式には，高いセキュリティを提供するSAML2.0[4]を用いた。また，クラウド環境内のシステムを隠蔽(いんぺい)するために，リバースプロキシ型シングルサインオン環境[6]をオープンソースソフトウェア(OSS)のOpenSSO Enterprise 8.0 Update1[7](以下“OpenSSO”という。)を使用し認証基盤を構築した。SAML2.0による認証連携をサポートしており，独自の認証機能をプラグインモジュールとして追加することが可能であるため，OpenSSOを採用した。

また，実証実験システムでは，企業システムのクラウド移行を想定した企業システム／プライベートクラウド／パブリッククラウドの3つの構成とした(**図3**)。なお，プライベートクラウドは，グループ企業への業務委託による運用を想定している。

3.2 評価方針

このシステムで，企業システムにアカウント情報と認証機能を集中することで，クラウド上にアカウント情報を持たない認証基盤を構築し，認証連携を実システムへ適用するための次の要件を満足することを検証する。

(1) 企業内システムからのシングルサインオン

企業内システムにID／パスワード認証でログインしたユーザーが，再度認証を要求されることなくクラウド上のアプリケーションにアクセス可能である。

(2) インターネットからのシングルサインオン

モバイル端末からクラウド上のアプリケーションにアクセスする際，PKI(Public Key Infrastructure)認証／PUZZLET認証[8]が行われる。

最初の認証後，企業システム又は別のクラウド上のアプリケーションに対して，再度認証を要求されることなくアクセス可能である。

(3) ユーザーを識別したサービス提供

アカウント情報を持たないクラウドにシングルサインオンしたユーザーのIDを，クラウド上のアプリケーションが利用可能である。

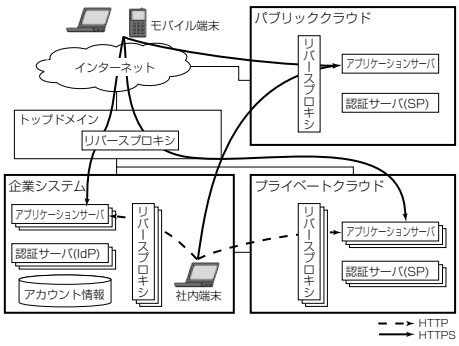


図3．システム構成

なお，企業システム内の認証はID／パスワード方式を採用しているが，セキュリティ上の観点から，インターネットからクラウド上のアプリケーションへのアクセスを許可する場合には，より強固な認証方式を採用することが望ましい。そこで，モバイル端末に対してはPKI認証(クライアント証明書を用いた認証)とPUZZLET認証(三菱電機独自のモバイル認証)を切り換えて利用できるようにした。

3.3 実証方法

実証実験システムでは，認証基盤上に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において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[1]。

(1) 処理概要

企業システムの社内LAN上の端末から，又はインターネット上のモバイル端末から，各ドメインのWebアプリケーションが利用可能である。すべてのドメインへのアクセスについて，必ず企業システムの認証サーバへリダイレクトされ，認証が行われる。一度認証をパスしたあとは，その認証セッションが継続する間，再度の認証を求められることなく任意のドメインのアプリケーションにシングルサインオンが可能である。認証は必ず企業システムの認証サーバが提供する認証機能を用いて行われ，アカウント情報は企業システム内にしかないことが特徴である。

ドメイン間のシングルサインオンは，SAML2.0のプロトコルを利用して実現している。企業システムの認証サーバがIdPとして認証機能を提供し，クラウド上の認証サーバがSP(Service Provider)としてサービスを提供する。ユーザーがクラウド上のアプリケーションにアクセスすると，クラウド上の認証サーバ(SP側)によって認証済みかどうかのチェックが行われ，認証がまだ行われていなければ，SAML2.0プロトコルに従って企業システムの認証サーバ(IdP側)にユーザー認証の実施を要求する。IdPはユーザー認証を実施し，ユーザーの認証情報(SAMLアサーション)をSPに送信する。SPは認証情報を検証し，ユーザーが認証に合格したことを確認すると，ユーザーにSP側のアプリケーションへのアクセスを許可する(シングルサインオン)。ここで，クラウド上のSPにはアカウント情報が存在しないため，ユーザーは認証セッションが継続する間のみ有効な一時アカウントを利用する。ユーザーIDはIdPからSPに送信され，アプリケーションで利用可能だが，アカウント情報として保存されることはない。

(2) 検証シナリオ

3.2節の要件を検証するためのシナリオは次のとおりである。

①企業システムを経由してプライベートクラウド上のシステムを利用

②プライベートクラウド上のシステムを直接利用
③パブリッククラウドのシステムを利用
④プライベートクラウドを経由して企業システムを利用
⑤プライベートクラウドを経由してパブリッククラウドのシステムを利用

3.4 実証実験結果

3.3節⑵に示した5個のシナリオを実施した結果，**3.2節**で取り上げた要件を満足していることが検証できた。次に，検証結果をまとめる。

⑴ シナリオ①の結果から，企業内システムとプライベートクラウドのアプリケーション間のシングルサインオンが可能であることを確認できた。

⑵ シナリオ②③④⑤の結果から，社内・社外等のアクセス場所に合わせた認証が行われることを確認できた。

⑶ シナリオ④⑤の結果から，プライベートクラウドと企業内システム／パブリッククラウド間のシングルサインオンが可能であることを確認できた。

⑷ シナリオ①②③の結果から，プライベートクラウドとパブリッククラウド環境で，企業内の認証システムから渡されたユーザーのIDを利用可能であることを確認できた。

3.5 評　価

3.2節で述べた⑴～⑶の検証項目については，機能，性能面ともに問題なく動作することが検証できた。今回の評価結果について述べる。

⑴ アカウント情報管理

クラウド環境上にアカウント情報を持たずに，安全な企業内でアカウント情報の管理を行うことで，セキュリティ的に問題なくクラウド環境上のシステムを利用可能なことを検証することができた。

⑵ 企業，クラウド間のシングルサインオン

複数の企業システムと複数のクラウド環境上のシステム間における様々な形態のシングルサインオンが可能なことを検証することができた。

⑶ OSSの利用技術

複数の企業システムと複数のクラウド環境上のシステム認証連携の基本的なプロトコルであるSAML2.0について，利用者の要件に合わせた形での利用技術を確立することができた。また，今回のようなID管理，認証連携システムを構築するために商用ソフトウェアを利用すると高額であるため，OSSを利用したが，その有効性の検証や技術蓄積が限られていた。この検証によって，OSSを利用して独自の認証連携システムを安価に構築する技術を確立できた。

4. むすび

企業間連携の標準プロトコルであるSAML2.0を利用し，企業内システムのID情報を用いて，アカウント情報を持たないクラウドとの連携を可能にする認証基盤の構築を行い，実システムでも十分に利用可能なことが検証できた。また，複数の企業システム及びクラウド上に構築したシステム間での認証連携が可能となり，企業システムをクラウド上に移行させる上で基本的な認証連携の技術ノウハウが蓄積できた。

今回の実証実験では，アカウント情報を企業内で一元管理し，クラウド上に構築した認証システムは，その情報を用いて認証を行っていた。しかし，実際にクラウドを用いる場合，不特定多数の企業がシステムを共有するケースが多くなる。その際，各企業内で管理しているアカウント情報を利用する形で認証を行うケースも増えていくであろう。

クラウド環境利用の拡大をめざして，クラウド上におけるシステム構築技術開発を進めるに当たり，次に示す課題を解決していく。

⑴ OpenIDによる認証連携

OpenIDは，Web事業者向けの認証連携技術として，SAMLと並び普及が進んでいる。将来，様々なWeb事業者が展開するクラウド環境との連携を考えた場合，認証手段の一つとして組み込んでいく必要がある。

⑵ アカウント情報連携の構築手法

各企業内で管理しているアカウント情報をクラウドから利用するため，アカウント情報に対しリンクを張ることで認証を行う方式の実装及び検証を行っていく。

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”によって実施したものである。

参考文献

⑴ 村澤　靖，ほか：クラウドシステム構築のためのセキュリティ基盤(1)－モデルシステムと実証実験－，三菱電機技報，**84**，No.7，411～414（2010）
⑵ 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）
⑶ カンターラ・イニシアティブ
http://kantarainitiative.org/
⑷ 日本PKIフォーラム，PKI-Jジャーナル2007(最終号)
⑸ OASIS，SAML仕様
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20
⑹ IPA：大規模サイトのネットワークセキュリティ
http://www.ipa.go.jp/security/fy14/contents/enterprise/pdf/enterprise.pdf
⑺ The OpenSSO Project
https://opensso.dev.java.net/ja/
⑻ 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）