4E-1

クラウド向け認証基盤プラットフォームの実装と検証

鷲尾 元太郎　村澤 靖

三菱電機株式会社 情報技術総合研究所

1 はじめに

1.1 背景

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となっている．しかしクラウド環境は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．[1]

そのため，高いセキュリティが求められる企業システムをクラウド上で構築する場合，プライベートクラウドもしくは信頼できる IaaS (Infrastructure as a Service)上に SaaS(Software as a Service)として企業システムを構築することが多い．

しかし，図 1に示す通り，各 SaaS アプリケーションでユーザ認証やユーザ管理を実現する場合，SaaS アプリケーション毎に認証基盤を構築する必要があり，開発コストが増大するという課題がある．

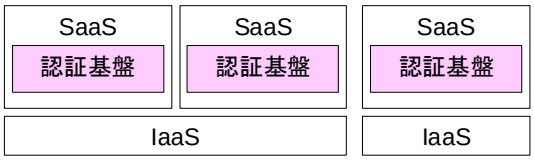

図 1 クラウドにおける一般的な認証基盤

1.2 目的

そこでヘルスケア分野[2]や金融分野など高いセキュリティが求められる SaaS に対して汎用的に使える図 2のような認証基盤プラットフォームの検討および実装を行った．本稿では，認証基盤プラットフォームを構築する上で検討を行ったユーザ管理モデルおよび ID マッピングの説明と，今後認証基盤プラットフォームを運用する上での課題について報告する．

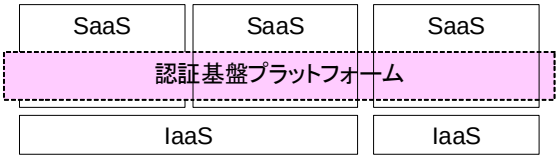

図 2 認証基盤プラットフォームの狙い

Implementation and Verification of Authentication Platform for Cloud Computing Based Systems.
G.Washio, Y.Murasawa
Information Technology R&D Center, Mitsubishi Electric Corporation

2 認証基盤プラットフォーム

2.1 ターゲットとする SaaS

本プラットフォームは，高いセキュリティが求められる SaaS と，その他の一般的な SaaS が混在する環境で共通して利用可能な認証基盤プラットフォームの検討を行った．

また，将来的に国民 ID の IC カードが配付された場合に容易に対応できる認証基盤プラットフォームの構築を行った．

2.2 要件

本プラットフォームでは以下の要件を満たすよう設計を行った．

(1) 複数の認証方式サポート

高いセキュリティが求められる SaaS で要求される電子証明書による SSL(Secure Socket Layer)クライアント認証のサポートと，一般的に利用されている ID/パスワード認証の 2 方式をサポートする．

(2) 認証認可，ユーザ管理のマルチテナント

SaaS を提供する事業者（SaaS 事業者）間の独立性を確保したマルチテナントな認証認可およびユーザ管理を行う．

(3) SaaS 事業者間のシングルサインオン

複数の SaaS 事業者に跨ったユーザの管理と，複数の SaaS 事業者が提供する SaaS を横断的に利用可能なシングルサインオンサービス

(4) 認証連携

異なる IaaS 上に構築された SaaS との認証連携や，他の認証基盤との認証連携を行うために SAML2.0 (Security Assertion Markup Language)による認証連携をサポートする．

(5) ユーザの複数組織の兼務

SSL クライアント認証の場合，ユーザは電子証明書 1 枚で認証を行うが，その 1 枚の電子証明書で複数の組織を兼務することが可能とする．これは将来国民 ID の IC カードが配付された場合にその IC カード 1 枚で認証可能な構成とするためである．

3 認証基盤プラットフォームの実装

3.1 システム構成図

今回実装した認証基盤プラットフォームの構成図を図 3に示す．今回の実装では，オープンソ

ースのシングルサインオンソフトウェアである OpenSSO を活用し，そこに認証基盤プラットフォームで必要とされる機能をアドオンする形で開発を行った．ユーザの SaaS へのアクセスは基本的にリバースプロキシ経由で行われ，そのリバースプロキシと連携する OpenSSO サーバで認証認可が行われる．また，利用ユーザの登録・変更やサービス契約変更等のインターフェースを提供するユーザ管理サービスを構築し，SaaS 管理者が利用可能な構成とした．

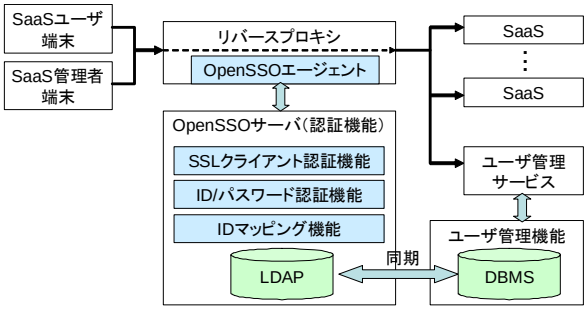

図 3 認証基盤プラットフォームの構成

3.2 ユーザ管理モデル

前述の要件を満たすために，認証基盤プラットフォームでは図 4示すユーザ管理モデルでユーザ管理を行っている．

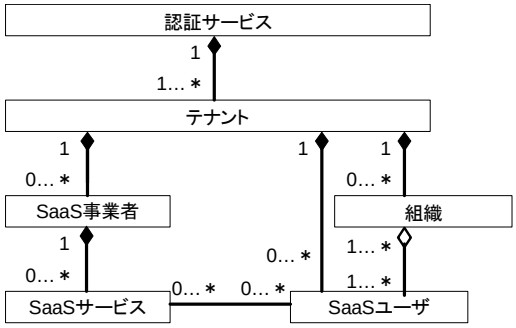

図 4 ユーザ管理モデル

本プラットフォームが提供する認証サービスでは，テナントという概念を取り入れ，その下に SaaS 事業者が属する構成とした．SaaS 事業者間で認証連携を行う可能性がある場合は，同一テナントに SaaS 事業者を配置するが，独立して認証を実施したい場合や他の IdP(Identity Provider)とのみ連携する場合は別テナントとして管理し，認証サービスのマルチテナントを実現している．また，組織とユーザの関係については，一般的な日本の組織では階層化された組織に利用ユーザが所属し，組織単位で SaaS サービスを契約することが多いが，今回は利用ユーザ単位でサービス契約可能な構成とした．

3.3 ID マッピング

SaaS 間でシングルサインオンを行う際，SaaS に対してユーザを識別するために ID を受け渡しする必要があるが，SaaS 間で共通した ID を利用できない場合がある．また，SaaS で従来から利用していた ID を引き続き利用したい場合もあり，これらの SaaS の ID 間のマッピングを行う必要がある．そこで，本認証基盤プラットフォームでは，ID マッピング機能を実装した．

図 5に示すように認証サービスとして 1 つの ID をユーザに割当て，それを各 SaaS のユーザ ID と紐付けを行った．各 SaaS サービスにユーザがアクセスする際にマッピングされた ID 情報を各 SaaS に伝えることで，ユーザの識別を行う．

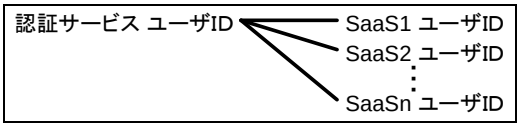

図 5 ID マッピング例

4 今後の課題

実開発を行った結果、本プラットフォームを運用する上で以下の課題があることが分かった．

(1) SaaS 間のセキュリティレベルが異なる場合に，低いセキュリティレベルの SaaS から高いセキュリティレベルへのアクセスが可能となってしまう場合が発生する．

(2) どの SaaS 間でシングルサインオンを許可するかを認証サービスの運用者と当該 SaaS の運用者間で検討する必要がある．

5 おわりに

本稿では，クラウドにおいて高度なセキュリティを実現する認証プラットフォームの開発を行った．本プラットフォームを構築する上で必要となったユーザ管理モデルと ID マッピングの検討を行った．今後は，様々な SaaS 事業者への適用を想定した認証基盤プラットフォームの評価や，今回の開発で明らかになった運用上の課題の解決策検討を実施していく予定である．

参考文献

[1] 村澤，他：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 Vol.84, No.7, 2010, pp. 412-414

[2] 茗原，他：ヘルスケアセキュリティ SaaS への取組み，三菱電機技報 Vol.84, No.7, 2010, pp. 395-398