大学機関でのパブリッククラウド利用時の課題と解決法

西垣 直美
日本ヒューレット・パッカード株式会社
テクノロジーサービス事業統括　IceWall ソフトウェア本部

概要：パブリッククラウド利用時に想定される課題及びその解決策に関し、具体的なソリューションの最新情報を交えご紹介いたします。

キーワード：シングルサインオン、ID 管理、クラウド、認証連携

1. はじめに

少子化や経済環境の悪化にともない、国内においての学校経営もますます厳しくなってきています。そのような中、コスト削減、IT の効率的利用に向けて、クラウドサービスの利用を検討される教育機関様が急増しています。

しかし、その一方、クラウドサービスが混在しIT 環境が複雑化する中でのセキュリティと利便性の両立、またプライベートクラウド、パブリッククラウドへの接続性は大きな課題になっています。

今回は、パブリッククラウド利用時に想定される課題及びその解決策に関し、具体的なソリューションの最新情報を交えご紹介いたします。

2. パブリッククラウド利用時の課題

パブリッククラウドを利用する際には、以下のような課題があります。

・ID、パスワードのライフサイクル管理

学内のポータルなどからパブリッククラウドにアクセスするにはシステム、サービス毎に認証を受ける（ログインする）必要があり利用者の利便性が大きく低下します。

また、利用者に複数の ID、パスワードを管理させることになる為、ID、パスワード情報が外部に漏えいする可能性も高まり、セキュリティも大きく低下します。

更には、利用者のパスワード忘れも増加し、その対応の為のヘルプデスク業務のコストも増加します。

運営に関しても、学内のシステムや各パブリッククラウドへの ID 登録、変更、削除などを個別に行う必要があります。システム、サービス毎の管理となりますので、ID の消し忘れなどのセキュリティリスクが増加します。また、システム、サービスの数分 ID の管理作業が発生しますので、運用工数、コストも増加します。

・学内全体でのセキュリティポリシー整備及びルール化の徹底が困難

学部や研究室単位でパブリッククラウドを利用するケースもあるかと思われます。その場合、管理が研究室単位となるため、学内全体の状況を把握することができず、思わぬセキュリティリスクが発生する可能性があります。

・学外からのアクセス

インターネットに公開されたパブリッククラウドは全世界のどこからでも利用できることが大きなメリットの一つです。

しかし、どこからでもどんな PC からでも ID とパスワードさえ入力すればアクセスできてしまうパブリッククラウドの利用は大きなリスクを伴います。

ウィルスに感染した PC よりパブリッククラウドのアプリにデータをアップロードしてしまう可能性もあります。それらリスクを軽減するには、正しく管理された端末しかアクセスできない仕組みを作るなどの対策が必要です。

また、各パブリッククラウドへのアクセスログの一元管理は難しく、情報漏洩などの問題が発生した場合、解析が困難です。

図１　パブリッククラウドとの接続時の課題

3.　クラウド間のシングルサインオンを実現する認証連携

認証連携とは、それぞれ個別に認証機能を持つサイト間でのシングルサインオンのことです。サイト間で認証結果を交換し信用することにより、連携した別サイトにアクセスする際にも認証を有効にします。これによって、一度認証を受ければ再度認証を受けずに（ユーザー ID/ パスワードの入力等なしに）連携した他サイトの Web システムにアクセスできるようになります。

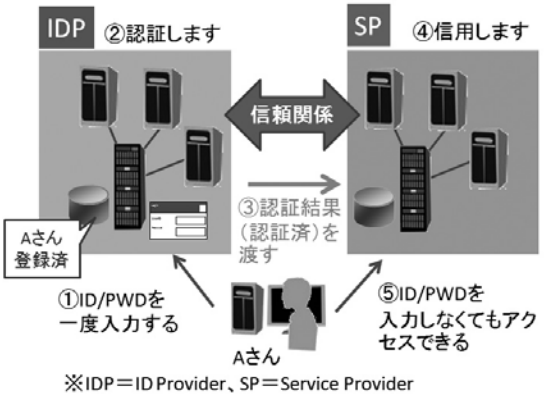

図２　認証連携

この仕組みを学内システムとパブリッククラウド間に適用することが可能です。

例えば、学内システムと Google Apps 間で認証連携を行えば、利用者は学内システムに一回ログインすれば、再度 ID、パスワードを入力することなく、Google Apps を利用することができます。

認証連携には SAML（Security Assertion Markup Language）が使用されます。SAML とは、標準化団体 OASIS によって策定された、ID やパスワードなどの認証情報を安全に交換するために XML 仕様です。

SAML を使用すれば、認証連携は実現できますが、安全に効率良くパブリッククラウドとの認証連携を実現するには、特定のパブリッククラウドとの接続性を検証済みで、設定方法のマニュアルと共にサポートが受けられる製品を利用するのが現実的です。

日本 HP は、認証基盤として国内の教育機関様はもとより企業のイントラネット、BtoB、BtoC 環境でも多数お使い頂いている Web シングルサインオンソリューション「HP IceWall SSO」を開発、販売しています。

オプション製品である「HP IceWall Federation」は、パブリッククラウドやプライベートクラウド環境で認証連携を行うために特化した製品です。

SAML の知識がなくても、Google Apps や salesforce などのクラウドサービスとの認証連携を簡単に安全に実現できます。

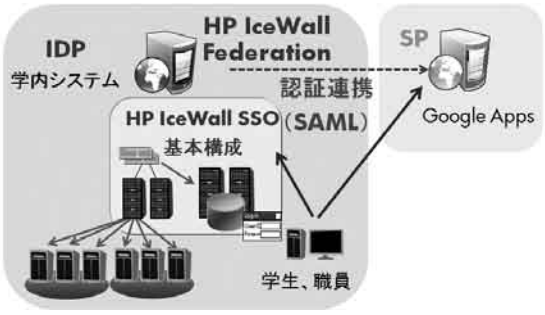

図３　Google Apps への認証連携

また、HP IceWall Federation は、現在教育機関様で多く利用されている Shibboleth にも対応しています。

4. クラウドサービス導入を支援する統合 ID・アクセス管理ソリューション

認証連携によるクラウド間のシングルサインオンにより、利用者の利便性や ID、パスワードの漏洩リスクなどの課題は解決できます。

しかし、学内システムとクラウドサービス間での ID 管理の負荷増大や ID の消し忘れなど、セキュリティリスクへの対応という大きな課題はまだ残っています。

このような複雑な課題に対応するために、前述の認証連携と ID 管理を組み合わせたソリューションを検討される教育機関様が増えています。

ソリューションの具体例として、HP IceWall を中心とした、学内システムと代表的なクラウドサービスである Google Apps の ID 情報、アクセス制御を一元管理するソリューションをご紹介いたします。

■ Google Apps 対応統合 ID・アクセス管理ソリューション概要

学内と Google Apps の ID 情報を統合管理します。また、学内と Google Apps 間のシングルサインオンを実現します。

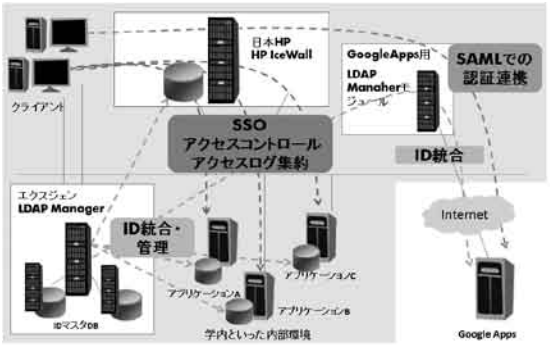

図 4　Google Apps 対応統合 ID・アクセス管理ソリューション概要

ID 情報の統合管理に、エクスジェン・ネットワークス株式会社の LDAP Manager を、学内及び Google Apps へのシングルサインオンに、HP IceWall SSO を使用します。

本ソリューションでの ID 管理の大きな流れは以下の通りです。

LDAP Manager は、人事マスタや Active Directory、複数のレポジトリに対するプロビジョニング、承認ワークフローの提供などを実現する統合 ID 管理製品です。

LDAP Manager が人事マスタやマスタ DB からの ID 情報の取り込みを行います。また、管理者がブラウザからユーザー情報を管理することも可能です。Active Directory との ID 情報の連携も可能です。

取り込まれた ID 情報は、各学内システムのレポジトリに必要なフォーマット・接続形式でプロビジョニングされます。HP IceWall SSO の認証 DB もプロビジョニング対象となります。

Google Apps 用 LDAP Manager モジュールにより、Google Apps に対して非同期でユーザー情報の更新処理が行われます。

次にユーザーが各システムを使用する際の流れをご紹介します。

ユーザーはまず HP IceWall SSO にログインします。HP IceWall SSO では、LDAP Manager によってプロビジョニングされたユーザー情報が反映された認証 DB を参照の上、認証・アクセス権チェックを行い、学内 Web システムに代行でリクエストを行います。認証の必要なものに対しては代行ログインを行います。

Google Apps へは、SAML による認証連携によるログインを行います。

ログイン後のユーザーは、ID・パスワードの入力なしで Web システムや Google Apps を利用できます。

本ソリューションの導入により、利用者の使用する ID・パスワードは 1 つだけとなり、Google Apps にログインするために、別の ID・パスワードをあらためて入力する必要がありません。

運営面では、学内システムにおけるユーザー管理（追加・変更・削除）がシームレスに Google Apps と連携されるため、運用負荷が軽減します。そして何より ID の消し忘れなどのセキュリティリスクが大幅に低減します。

さらに他のソリューションやクラウドサービスとの連携が容易に可能となり、拡張性の高いシステムとなります。

5. 統合認証基盤の効果

認証連携、統合 ID・アクセス管理ソリューションにより、パブリッククラウド利用における ID、パスワード管理に係る課題が解決できます。

それらの土台となるのは統合認証基盤です。イントラネット、プライベートクラウド、パブリッククラウドへの認証、アクセス制御、監査証跡を一元管理します。

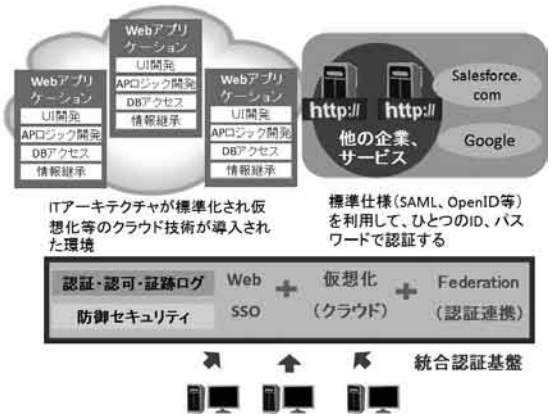

図 5　統合認証基盤

統合認証基盤を導入することにより、前述の認証連携や外部サービスとの連携導入の効率性があがるだけではなく、統合認証基盤に IC カード、生体認証、ワンタイムパスワード等二要素認証における認証強化を行うことにより、システム、サービス全体のセキュリティを強化することができます。例えば、統合認証基盤に指紋認証や端末認証を導入しておけば、その後、新たにパブリッククラウドサービスを追加する際にも、そのセキュリティレベルが適用されます。正しく管理された端末以外のアクセスを許可しないことにより、ウィルス感染のリスクを低減することもできます。

統合認証基盤を導入し、パブリッククラウドを含めた全システム、サービスへのアクセスを全て統合認証基盤経由にすれば、統合認証基盤に適用されたセキュリティポリシーが全システム、サービスでも適用されます。

また、全てのアクセスが統合認証基盤を通して行われますので、アクセスログを一元管理することもできます。

統合認証基盤、統合 ID 管理、認証連携の導入により、パブリッククラウド利用時の代表的な課題を効率良く解決することができます。

6. 最後に

めまぐるしい社会情勢の変化により、教育機関様に求められる IT 環境も日々変化しています。

変化に対し効率的に対応するには、まず統合認証基盤を構築することが必須と考えられます。

他社サイトとの連携やクラウドサービスとの接続などによって、統合認証基盤の対象範囲および関係者の数が急速に拡大し、学内・学外を含めた大規模環境にも適応できるミッションクリティカルな統合認証基盤が求められています。クラウドや仮想化環境での操作、もしくはその環境との接続が必要条件となります。

また、ステークホルダーが増加し、統合認証基盤の更新が益々容易ではなくなります。

HP IceWall SSO *はこうした統合認証基盤への新たなニーズにいち早く対応し、拡張性、可用性、運用性を大幅に向上させ、クラウドや仮想化への対応強化を図った国内シングルサインオン市場で No.1 シェアを持つシングルサインオンソリューションです。

今後も教育機関様に求められるその時代に最適な技術を提供し、安全で快適な教育環境の構築を支援し続けていきたく考えております。

---

*　出荷金額ベース
国内 Web シングルサインオンパッケージ市場 No.1
日本 HP：43.8%
（出典：ミック経済研究所「個人認証型セキュリティソリューション市場の現状と将来展望 2010」2010 年 10 月刊）