SCIS 2014 The 31st Symposium on Cryptography and Information Security
Kagoshima, Japan, Jan. 21- 24, 2014
The Institute of Electronics, Information and Communication Engineers

企業によるクラウドサービス利用時の ID ライフサイクル管理における運用負荷軽減に関する考察

A study on reduction of operation load by ID life-cycle management with the usage of cloud service in a corporate situation.

岩渕 琢磨* 後藤 厚宏*
Takuma IWABUCHI Atsuhiro GOTO

あらまし IT リソースの多様化に伴い，企業による ID 管理は，セキュリティ対策，コンプライアンス遵守，雇用形態・勤務形態の多様化などにより，複雑さを増しており，企業内で運用・管理しているアプリケーションのための ID ライフサイクル管理における運用負荷は増加傾向にある．また，ID 管理は運用負荷の増大だけでなく，管理が煩雑になることで，その組織におけるサイバーインシデントや内部からの情報漏洩の要因になりえる．さらに，クラウドサービスの利用規模拡大によって，それまで企業内で運用・管理していたアプリケーションと，クラウドサービス，双方の ID を管理する事が企業の管理者には求められ，これまでのような企業内だけの ID 管理に比べて，複雑性・運用負荷は，ともに増大することが想定できる．企業の ID 管理システムとクラウドサービス間とで ID を連携させるフェデレーションの取り組みがあり，その際のユーザ情報登録にかかる運用負荷を軽減する措置として，プロビジョニング用 API の活用，さらにその API 標準化が進んでいる．本稿では対策の一つとして，企業内とクラウド上のアイデンティティプロバイダを連携させることによる ID ライフサイクル管理の運用負荷軽減策を提案し，また，提案手法採用時に検討すべき課題を考察する．

キーワード 認証，クラウド，デジタルアイデンティティ

1 はじめに

企業による ID 管理の複雑性が増す中，企業内で運用・管理しているアプリケーションのためのデジタルアイデンティティ（以下，ID）ライフサイクル管理における運用負荷（運用工数・システム対応費用など含む）は増加傾向にある．

その要因のひとつである，IT リソースの多様化について， UNIX，Windows，さらには Linux などのプラットフォームの多様化や，複数のデータベース機種などにより，ID とそれに付与されるアクセス権限を管理すべき対象が増加したことで，従来のシステム管理の一環としてこれらを行うことが事実上不可能になっている[1].

コンプライアンスの面では，2006 年に改正された会社法および金融商品取引法，いわゆる内部統制への対応として，企業において ID 管理は喫緊の課題となっており，これらコンプライアンスの一環として，IT リソースへのアクセスを制御する ID 管理は，内部統制の重要な要素と言える．

また，業務のボーダーレス化に伴い，グローバル展開，グループ企業間や海外工場，海外企業と提携する場合など，日本国内の社員だけではなく国外に存在するユーザに対して，情報管理・情報共有を行うためのシステムを利用させるケースが増加傾向にある．グローバルでの ID 管理を行う場合については，そのグローバル展開を行う国々の商習慣や法律，文化などを踏まえる必要があり，たとえば，ミドルネームの取り扱い，現地語の対応，時差の考慮，ネットワークの距離遅延などを考慮する必要があり，これまでのような部署内や社内で完結するようなものから，会社間をまたいでの管理や，グローバルでの管理が発生している[1].

その他にも，M&A の活発化，BYOD（Bring your own device）の採用等によるデバイスの多様化，企業におけ

* 情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1．Institute of Information Security, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa 221-0835, JAPAN.

る雇用形態の多様化など，IT リソースの利用形態が多様化し，さらにそれらが重なることによって，近年の ID 管理は複雑性を増している．

電子商取引，ソーシャルネットワーク，クラウドサービスなど，様々なインターネット技術を利用したサービスが普及し，利用者もこのようなインターネットサービスに依存した生活が当たり前となっている．ただし，それらを利用する際にはそれぞれのサービスにユーザ情報の登録を行い，利用に際しては認証を行う必要がある．利用者にとっては，利用するサービスが多くなればなるほど，それぞれ独立した認証を求められる場面が多くなり，きわめて面倒であるばかりでなく，それぞれのログイン ID やパスワードを個別に覚えておくことが現実的ではなくなっている．また，インターネット上には，多くの脅威が存在する．中でも，悪意を持った攻撃者が正当なユーザになりすまして，不正なアクセスを行う危険性が組織内などクローズされた空間の比ではない[2].

さらには，インターネットの爆発的な拡大とクラウド化の流れに伴い，B2B や B2C といった電子商取引が増加する中で，IT の役割が重要となり，ID 管理が一層複雑化してきている．たとえば，電子商取引では，ユーザは複数のドメインのサイトを行き来してサービスを利用する状況において，ID 情報を管理することは，極めて複雑となる [1].

このように，企業による ID 管理の複雑性が増す中，ID 管理の運用負荷増大だけでなく，運用管理が煩雑になることで，その組織におけるサイバーインシデントや内部からの情報漏洩の要因になりえる[3]．さらにクラウドサービスの利用によって，それまで企業内で運用・管理していたアプリケーションと，クラウドサービス，双方の ID を管理することが，企業の ID 管理者には求められる．その場合，これまでのような企業内だけの ID 管理に比べて，複雑性・運用負荷は，ともに増大することが想定できる．

本稿では，企業によるクラウドサービスの利用が増えていった際のユーザ ID ライフサイクル管理の中でプロビジョニングを中心に，社内環境からクラウド環境展開時のプロビジョニングにおける運用負荷削減方法について整理と提案，および課題の考察を行う．

2　クラウドサービスにおける ID 管理

2.1　クラウドサービスの拡がり

クラウドサービスなどのインターネット上のサービスは企業においても広く利用されるようになってきた[4]．特に企業においては，グループウェア，SFA（Sales Force Automation），その他業務アプリケーションなどの SaaS（Software as a Service）への投資が増加傾向にある[5]．これらのサービスは，誰もがアクセスし閲覧できるコンテンツの利用にとどまらず，利用者は社内のシステムやアプリケーションを利用する際と同様に，インターネット上のサービスを利用するにあたって認証を求められる．利用者を識別する識別子（ID）およびそれに付随した属性情報をサービス側で保持したうえで，それらの情報の検索，更新，同期等を行いながら，利用者の属性や権限に基づいて最適化されたサービスを提供するようになっている．また，組織内で管理されている ID 情報とインターネット上のサービスで管理する ID 情報を相互に交換することによって，その一意性，および本人確認・身元確認の信頼性を確保することもある[2].

インターネット技術の利用は，ひとつの組織内での利用にとどまらず，ドメインをまたいで利用されており，ID 情報もドメイン横断的に管理する必要がある．「B2B」，「B2C」，「B2E」などの組織を超えたサイト間／Web サービス間での ID 情報の交換をはじめ，クラウドサービス間でも ID 情報の交換が求められている．また，組織をまたいでの情報の連携が必要となるため，事前の信頼関係構築が必要となる．

2.2　ID 連携

ID 連携（ID フェデレーション）とは，サービスプロバイダ（Service Provider，以下 SP）から認証処理を切り離し，SP 側と認証処理をつかさどるアイデンティティプロバイダ（Identity Provider，以下 IdP）側が互いに信頼し合うことで，認証処理を一元化する仕組みである．

従来から ID 情報交換は，同じネットワーク内（あるいは同じドメイン内）の利用者やシステムに対して，セキュリティを確保するために行われてきたが，利用者が外部のシステムにアクセスしたり，外部の利用者が内部システムにアクセスしたりすることも多くなってきた．このため，システムと利用者の分離は重要課題となり，企業間，運用管理ドメイン間の ID 情報の連携の必要性から生まれた手法である[2].

ID 連携によって，これまで各 SP が個別に管理していた ID 情報を，事業者間で連携させることにより，ユーザは複数のサービスをシームレスに利用できるようになる．企業間での ID 連携は，パートナー企業やグループ企業間に適用されることがほとんどであったが，近年は，特に SaaS 事業者において，ID 連携をベースにサービス連携を強化していく動きが活発になってきている[6].

認証結果を含む ID 情報を連携するための標準的な仕様はいくつか存在しており，サービス提供者側が複数の選択肢を用意していることも少なくない．目立ったところだと，SAML，WS-Federation，OpenID（または OpenID Connect）などが挙げられる．これらの ID 連携技術を利用することにより，企業内で管理されている ID 情報や認証状態をクラウドサービスに連携することができ，クラウドサービスを社内システムと変わらない方式で利用できるようになる[1].

SAML については，企業向け業務アプリケーションを

中心に採用され，OpenID はコンシューマ向けサービスを中心に利用が拡がっている．

こうしたプロトコルのほかにも，ID 連携では，参加する多数の IdP 及び SP の間で，交換されるデータのスキームの共通化やポリシーの合意を行うことで，相互運用性を実現している．IdP と SP がそれぞれ個別に行わなければならなかった交渉や技術検証を連合体として行い，ノウハウの共有や蓄積を行う枠組みとしても，ID 連携は有効である[7].

クラウドサービスを利用するにあたり，ユーザは自身が正当な利用者であることをサービス提供者に対して証明する必要がある．また，サービス提供者は適切なユーザに適切なサービスを提供する必要がある．また，オンプレミスのシステムを対象とした ID 管理のみを行う場合と違い，パブリックなネットワークを介して ID 情報をやり取りする必要がある．そのため，極力サービス側に認証機能や ID 情報を直接持たせない，またはサービス側から直接オンプレミスの ID 情報を参照させないといった構成が必要となる．特にクレデンシャル情報（資格情報）などの重要な情報がパブリックネットワークを介してやり取りされないように認証機能の配置が必要となる．また，サービス利用者・提供者との関係にビジネス的な契約関係が発生することも考慮する必要がある[1].

2.3 企業とクラウド間の ID 連携時のユーザプロビジョニング

ユーザプロビジョニングとは，IT リソースへのアクセス権を，ユーザに提供するプロセスで，具体的には，IT リソースのアカウントを実際に作成，変更，削除することである．ID 管理の中で最も重要な機能が，プロビジョニングである．標準化団体 OASIS（Organization for the Advancement of Structured Information Standards）では「プロビジョニングとは，ユーザやシステムのアクセス制御または電子的に発行されたサービスに関連するデータを管理（セットアップ，修正，削除）するために必要なすべてのステップの自動制御のことである」と定義されている[1].

クラウドサービスの利用に伴い，プロビジョニングの対象となる IT リソースへのコントロールが組織内だけの場合と比較して困難となるケースがあるため，クラウドサービスを利用する上では十分に検討が必要となる[1]．企業とクラウドサービスとの ID 連携時には，企業側の ID 管理システムからサービス側へ連携に必要となる最低限のユーザ情報のプロビジョニングが事前になされている必要がある．

プロビジョニングを手動で行う場合，企業の ID 管理者は，人事システムなどから社員の情報を入手し，それをもとに，利用するクラウドサービス上の Web 画面から手作業でユーザ情報の登録を行ったり，定型フォーマットファイルの作成，およびアップロードを行うなど，利用対象サービスへのプロビジョニングを行う作業が発生する（図 1）.

社員の入退社や組織変更等による社員の異動が発生する度に，対象サービス分だけ作業をすることは，対象サービスが少ない状態であれば，それほどの負荷にはならないかもしれないが，対象サービス数が増えるに比例して，運用負荷も増大する．そのため，プロビジョニングにおける運用負荷軽減が必要となる．

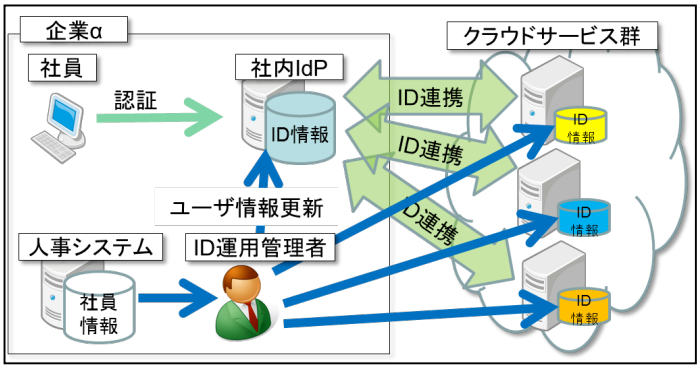

図 1 クラウドサービス利用時のユーザプロビジョニングイメージ

3 クラウドサービス利用時のユーザプロビジョニングにおける負荷軽減策

クラウドサービス利用時の ID 連携のためのユーザプロビジョニングにおける ID 管理者の負荷軽減策として，Just-in-Time Provisioning やユーザプロビジョニング用 API の利用が挙げられる．Just-in-Time Provisioning については，ID 連携の対象となる IdP からのユーザアクセス時に，IdP からクラウド上の SP へ送付される情報をベースにユーザ ID をサービス上で自動登録または，更新する機能で，salesforce.com において機能提供がなされている．しかしながら，この機能では，管理者が介在せずにユーザ ID が作成，更新されてしまうことがあり，企業側の ID 管理規則の遵守の観点から企業での本格的な利用は難しい．

ユーザプロビジョニング用 API の利用に関しては，クラウドサービスにて公開されているプロビジョニング用 API を用いて，IdP と SP 間でのインタフェースを構築することで，その間でユーザ情報を同期させる機能である．GoogleApps や salesforce.com などで機能が提供されており，運用負荷軽減の手法として用いられている．

3.1 ユーザプロビジョニング用 API の標準化による負荷軽減策

ユーザプロビジョニング用 API を利用する場合，SP ごとに API の仕様がまちまちであり，互換性がない．そのためユーザ企業の IdP からクラウド上の SP へのプロ

ビジョニングを行うためには，たとえばユーザの追加・削除といった単純な操作であっても，SP ごとに異なる API に対応しなくてはならない[8]．このため，対象サービスの追加時や，各サービスの API の仕様変更が発生する度に，IdP 側の改修や設定変更等の対応が必要となるという課題が表面化する．その課題の対策として，プロビジョニング API の標準規格である，SPML（Service Provisioning Markup Language）と SCIM（Simple Cloud Identity Management） の 2 つが提案されている．

企業向けサービスの特徴として，複雑なアクセス制御方式，すなわちロール管理が用いられることや，コンテンツとしての ID 情報処理，たとえば SFA やスケジュール機能のように他人を識別するようなコンテンツとしての ID 情報が必要となることが挙げられる．企業向けサービスでの ID 管理・連携時にはこういったことに事前に考慮したプロビジョニング設計が必要となる．ID 情報のメンテナンス機能として，ユーザインタフェースの提供が SP には求められるだけではなく，プロビジョニング用 API の提供についての要望も今後増していくことが想定できる．API を個別に SP によって開発するよりも，標準化されたユーザプロビジョニング用の API が存在する方が，SP としても開発工数を鑑みると望ましいという考えからも標準化が検討されている．

3.1.1. SPML

SPML は，OASIS のサービス・プロビジョニング技術委員会によって策定されたもので，2003 年にバージョン 1.0 が，2006 年に同 2.0 が OASIS によって承認されている．SPML は従前に存在した 3 つのプロビジョニング製品ベンダーの外部インタフェースを統一した仕様であり，これに代わる他の仕様は存在しなかったことから，この分野では SPML が主流になるとみられていた．しかし，SPML の普及は進んでおらず，この背景には，仕様が汎用的であるがゆえに複雑であることと，SPML に対応する製品・サービスが少ないことが挙げられる[8]．

3.1.2. SCIM

このような状況に対し，クラウドサービスのユーザプロビジョニングのインタフェース統一を目指す動きとして，SCIM が検討されている．

SCIM は現在策定中のプロビジョニング標準規格で，クラウドサービスにフォーカスしたシンプルな仕様を目指して策定されている．また，SPML のときにはプロビジョニング製品ベンダーが中心となっていたが，Google や salseforce.com，Cisco，VMware といった有力なクラウドサービス事業者が積極的に仕様策定の議論に関与していることから普及の期待が掛かっている[8]．

標準で採用される属性についても検討が進められており，日本企業向けのオプションとして拡張属性を持たせる議論も進んでいるが，SPML が普及しなかったことの要因として，このような属性の複雑化も挙げられるため，どこまで盛り込むのかが課題である．

4 IdP-IdP 連携方式

4.1 クラウド上で SP を束ねる IdP

ID 連携時のユーザプロビジョニングにおける運用負荷軽減のための方式として，IdP-IdP 連携方式を提案する．これは，SP を束ねたクラウド上の IdP と，企業内 IdP とを連携させることによって，プロビジョニング時の ID 管理者の負荷を軽減させることを狙う方式である．

図 2 は提案方式のイメージである．クラウド上で SP と IdP 間で信頼関係が構築され，ID 連携が行える環境を準備する．その SP を束ねたクラウド上の IdP と企業内の IdP 間で連携を行うことで，企業内のユーザ（社員）は社内 IdP への認証を行い，その結果を用いてクラウド上の SP によるサービスを利用することができる．そのため，企業の ID 管理者は，クラウド上の IdP の先にある SP を，社内の IdP に手を加えることなくユーザが利

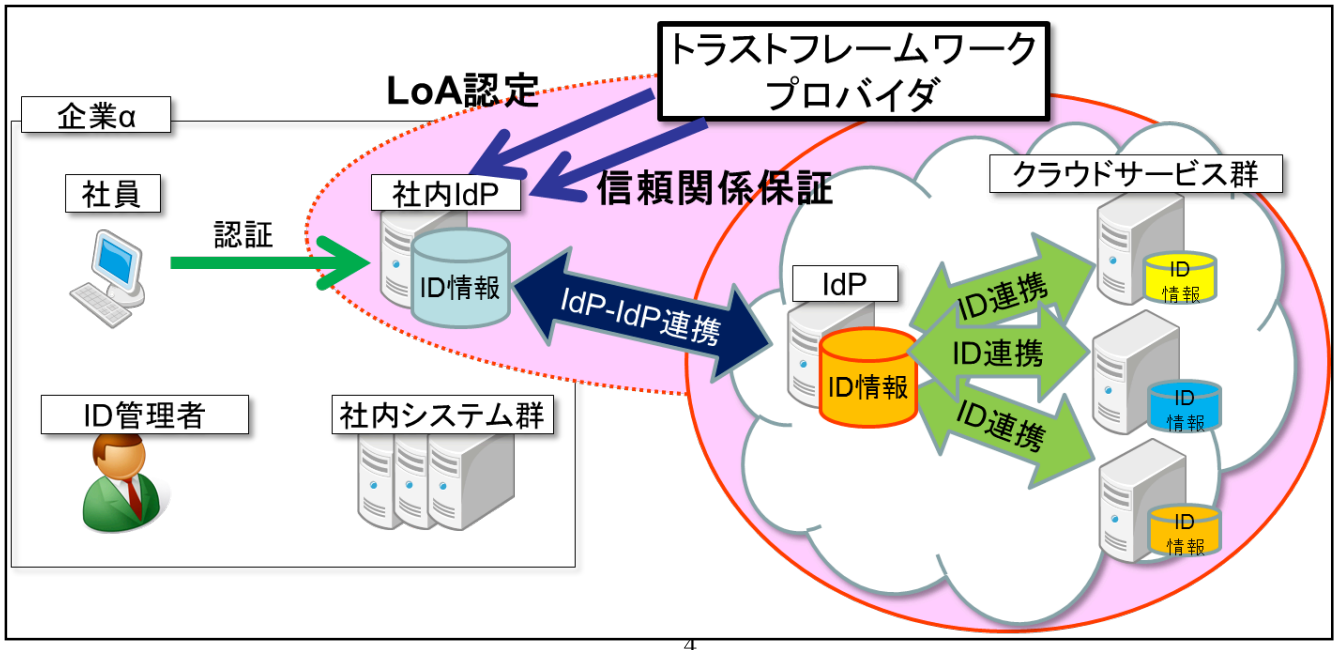

図 2 IdP-IdP 連携方式のイメージ

用できる環境が実現できる．また，クラウド上の各 SP へのプロビジョニングを行う必要がなくなるため，運用負荷の削減効果が期待できる．

4.2 IdP-IdP 連携に必要となる信頼関係構築

従来の ID 連携技術では, IdP と SP との間の相互信頼構築を前提とし，電子署名や暗号化の検証に必要な公開鍵等にかかわる情報（メタデータ）を事前に相互共有する必要がある．この，IdP と SP との信頼関係をトラストサークルと呼ぶ．SP は IdP の提示するルールに従うことで，信頼が構築されており，そのため，一度利用者認証が行われると，トラストサークル内のほかの SP は IdP が現在保持している認証結果を利用できることになる．

しかし，ID 情報を管理する IdP，その ID 情報を利用してサービス提供する SP，及び，ユーザの三者間での合意のもとに ID 連携を行なうため，このようなモデルの場合，IdP と SP が相互に契約して信頼関係を構築する必要があり, ID 連携機関の数に比例して信頼関係構築の数が膨大に増えてしまう．このため, ID 連携の規模拡張性に課題がある．たとえば IdP が新たにトラストサークルに加わる場合，サークル内の SP それぞれとトラストを結ぶ必要が発生する．SP が新たにトラストサークルに加わる場合も同様である．

この課題の解決策として，トラストフレームワークモデルという概念がある（図 3）．トラストフレームワークは，IdP，SP，ユーザの三者に加えて，ポリシー作成者，監査機関，トラストフレームワークプロバイダ（Trust Framework Provider, 以下 TFP）で構成され，オンラインサービスを利用・提供する際に，ユーザ認証の信頼性を保証し合い，ユーザ情報を，事業者間で安全に流通させるための，ガバナンス／プライバシー／テクノロジを包括することを目的とする枠組みである．ポリシー作成機関は ID 連携機関の信頼性や, 取り扱う ID 情報の正当性, セキュリティレベル, NIST800-63 の Levels of Assurance（以下，LoA）などに関するポリシーを作成する．次に，TFP はポリシー作成機関が作成したポリシーをもとに, ID 連携機関の監査を監査機関に依頼する．監査機関は TFP の依頼をもとにして ID 連携機関を監査する．最後に TFP は監査結果が作成されたポリシーに準ずる内容かどうかを照合し，ID 連携機関の ID 連携メタデータを公開する．なお，SP が提供する ID 情報の正当性を保証することを目的として SP の ID 連携メタデータを TFP が公開する場合など，片方の ID 連携機関の ID 連携メタデータのみを TFP が提供すればよいケースが考えられる．この場合，TFP が提供しない ID 連携メタデータは従来通り ID 連携機関自身のシステムで ID 連携メタデータを提供することで ID 連携可能である [9][10][11].

これにより, TFP によってあらかじめ策定されたポリシーにのっとり，参加機関が認定されることで，サイバー空間をより安全で信頼可能なものにし，この枠組みの中で流通する情報について，正確に管理されていることが保証され，IdP 側と SP 側との信頼関係の構築が容易になり，利便性の高いオンラインサービスの創出につながると期待されている [9].

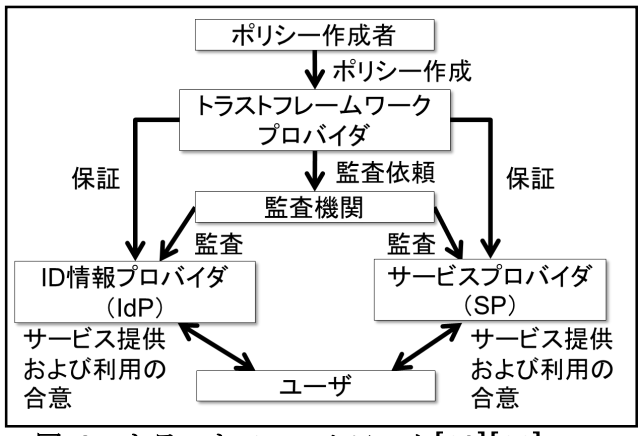

図 3　トラストフレームワーク[10][11]

米国政府の国民 ID 戦略の中で採用されたほか，米国以外の政府や，ISO や ITU-T などの国際標準化団体，世界経済フォーラム（ダボス会議）などでもプロジェクト化され，普及に向けた国際協調や制度的／技術的相互運用性について議論されている．国内では全国の大学等と国立情報学研究所が連携して,「学術認証フェデレーション（通称：GakuNin，以下，学認）」として運用が開始されている．

トラストフレームワークを用いることによって，新たな IdP または SP がトラストに参加する場合, TFP による認証を受けるだけとなるため，従来のトラストサークルによる信頼関係構築に比べ，工数の削減につながる．

トラストフレームワークの利用目的として，SP がサービスを提供する場合に IdP を評価するという側面もある. ID 連携のように完全な分散環境でサービスを提供する場合，SP が IdP を制御できない．そのため，ID の品質について何らかの評価が必要となる．

本稿で提案する IdP-IdP 連携方式において，IdP・SP ともに連携する相手先が増える都度，信頼関係を構築するための工数が発生する．これについてはトラストフレームワークモデルを適用することにより，トラストフレームワークに新しい IdP または SP が参加する際には, TFP の定めるポリシーに準拠していることを, 監査を通じ, 認証することで, トラストの構築が可能となるため, 信頼関係構築に要する工数が抑制されることが期待できる．

また，信頼関係の構築においては，クラウド側に企業内の IdP の運用の正当性を示す必要が発生する．SP 側から見た際に，企業内の IdP が正しく運用・メンテナンスされているか見えない．たとえば学認のように，IdP を運用している機関が大学など公的機関であれば，SP 側へも安心できるであろうが，対象が企業になった場合

には対象先の運用体制，セキュリティに対する取り組みなど見えづらくなることも多くなる．この対策として，トラストフレームワークモデルを利用し，フレームワーク上の監査を活用することが挙げられる．

図 2 において，クラウド上の IdP および SP がこの TFP による認証を受け，トラストが構築された状態（実線の範囲）であるとする．そこへ企業α内の IdP がこのトラストフレームワークに参加する場合（破線の範囲へトラストの範囲を拡大）に，TFP または監査による認証を受け，このトラストに参加することを示している．このとき，外部監査によって運用体制や運用方法などを第三者が保証することによって，セキュリティレベルの向上と安心を得られることにつなげられる．これは企業側から見たときに，SP が正しく運用されていることを第三者機関にて保証されていることにもなるため，サービスの採用判断基準にも利用できる．

4.3 保証レベル

ID 情報を利用したサービスや認証提供者の数が増加するにつれて，認証における信頼性が求められ，認証保証フレームワークの必要性が高まることが予想される[12]．具体的には，機密性のレベルに合わせて，認証強度を上げ下げさせることで，可用性と機密性のバランスを取った運用が求められる．たとえば，高い情報を取り扱う場合，採用するクラウドサービスへアクセスした際の認証そのものの安全性を考慮する必要がある．この安全性を測る認証強度の基準として保証レベル（LoA）がある．

保証レベルとは，認証方式の強度の違いを表す抽象的な指標であり，たとえば電子署名の検証，あるいはアクセス元に対する認証によって特定される識別情報の「信用度」を表す概念である[13]．この考えを ID 連携技術に取り入れ，連携時のユーザ ID の保証基準および，運用適合性の監査基準を規定したものが，各 TFP によって策定されている．

たとえば，Kantara Initiative の，Identity Assurance Working Group （IAWG）が規定した IAF（Identity Assurance Framework）が挙げられる．IAF は，ID 連携を行う事業者間における，情報の信頼性の相互確認等を，より簡素化するための ID の保証レベル，保証レベル毎に事業者が満たすべき要件，事業者のシステム，運用に対する監査要件を規定する標準としてまとめられており，2010 年 5 月に IAF 2.0 が公開されている．認証時の ID 保証レベルは，LoA として，IAF にて 4 段階で規定されている[14][15]．機密情報にアクセスする際の認証時には，どこまでの保証レベルを用いて，各ユーザからのアクセスを許可するのか検討が必要であり，その要件を満たすことのできるクラウドサービス事業者を選定することが必要となる．

サービスを利用するユーザ企業として，利用する情報の重要度に応じて認証強度を高めたいという要件が考えられる．また，サービスを提供する側である SP も同様に，扱っている情報の重要度や機密性が高ければ高いほど，正当なユーザのみに提供することがさらに求められる．この対策として，LoA の採用が挙げられる．

図 2 において，情報の重要度・機密性に基づき，トラストフレームワークのポリシーで定めた認証強度に応じて，TFP または監査機関によって，LoA の認証を受けることにより，その認められたレベルに応じて，トラストフレームワーク内で利用できる対象のサービスを制限することが可能である．

5 運用負荷削減方法に関する考察

5.1 IdP-IdP 連携方式の検討

本稿での提案方式である，IdP-IdP 連携の場合，ユーザ企業の視点では，社内 IdP からの連携対象が最小化されるというメリットと，トラストフレームワークへ参加する必要性があることが挙げられる．連携対象が絞られることについては，プロビジョニングにおける工数も最小化されることにつながる．一方，トラストフレームワークへの参加が前述のとおり必要となるという手間が発生する．ただし，第三者機関からの認証を得ることによって，内部統制に対応する工数の削減といった副次的な効果が期待できる．

SP 側としては，サービスを束ねることに要する工数が発生するというデメリットと，顧客の囲い込みによるメリットが挙げられる．サービスを束ねることに関しては，少なからず工数が掛かるため，その分の工数が発生する．しかしながら，それによって，たとえば小さなサービスが集合することで，顧客側へのメリットを提示することができ，顧客の囲い込みにつなげられることも期待できる．

5.2 SCIM と提案方式の比較検討

5.2.1. トラストの構築

これまで述べたように ID 連携のためには事前のトラスト構築が必要となる．そのトラスト構築に関しては，SCIM，提案方式，いずれの場合でも，トラストフレームワークモデルを用いることで事前作業の効率化が図れる．企業内の IdP を用いてクラウド上の SP と連携させる際には，正しく運用がなされていることをクラウド側に提示するためにもトラストフレームワークモデルを用いる必要があると考える．

5.2.2. ユーザプロビジョニング

ユーザプロビジョニングに関しては，SP 側で公開されているプロビジョニング用の API を用いることによって，工数の削減が可能である．さらに API の標準化がなされることによって，利用するクラウドサービスが多くなってもその効果が継続して得られることは前述のと

おりである．しかしながら，利用するサービスが増える際の設定作業は発生することと，SP 側がこの標準規格に対応している必要があることが今後の課題と言える．

提案方式に関しては，企業内の IdP と，クラウド上で SP を束ねた IdP との連携を行うだけであるため，その工数は削減できることが期待でき，標準化が進まない場合の工数削減策として受け皿になると考えられる．

5.3 トラストフレームワーク上の監査として第三者による認証制度採用における課題

トラストフレームワークへの参加の際に，TFP または第三者による監査が求められることを述べた．しかしながら，クラウドサービスにおける第三者認証制度の利用に関しては，2012 年に発生したファーストサーバ社によるデータ消失事件等による問題点も指摘されている[16][17]．また，トラストフレームワークモデルの場合，クラウド側だけでなく，企業内の IdP の運用についても正当性を示すために監査が必要であることを述べた．ID 管理は，ユーザの正当性を突き詰めればその分技術的な対策や運用工数などのコストが大きくなり，それらをいい加減に行うことは不正アクセスのリスク増大につながる．この意味でも ID の管理はコストとリスクのバランスを鑑みる必要があり，トラストフレームワークモデルにおける監査に関してもかかる工数についてはバランスを考える必要があると言える．

6 まとめ

本稿では，企業によるクラウドサービスの利用が増えていった際のユーザ ID ライフサイクル管理の中で，社内環境からクラウド環境展開時のプロビジョニングにおける運用負荷削減方法について，プロビジョニング用 API とその標準化について整理し，企業内 IdP とクラウド上の IdP 連携について提案・検討した．

また，運用コスト削減方法採用時に検討すべき課題の整理として，トラスト構築時の課題と対応策を整理するとともに，提案手法について対応策を適用した場合を検討した．

今後は複数のプロトコルでの実現や，ロール管理を取り込むことについて検討していきたい．

参考文献

[1] 特定非営利活動法人日本ネットワークセキュリティ協会，クラウド環境におけるアイデンティティ管理ガイドライン，株式会社インプレスコミュニケーションズ，2011.

[2] 独立行政法人情報処理推進機構，アイデンティティ管理技術解説，独立行政情人情報処理推進機構，2013.

[3] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ, 2009 年情報セキュリティインシデントに関する調査報告書，http://www.jnsa.org/result/incident/data/2009incident_survey_v1.1.pdf（2013 年 9 月 19 日アクセス）

[4] 株式会社ノークリサーチ，2012 年以降に向けた国内クラウド市場規模調査報告，http://www.norkresearch.co.jp/pdf/2011SaaS_usr_rel.pdf.（2012 年 9 月 1 日アクセス）

[5] 片山博之，日本企業の IT 支出予測：2013 年ー日本のユーザー企業は，何に投資し，何に投資しないのか，ガートナージャパン，http://www.gartner.co.jp/b3i/analyst/130214/（2013 年 12 月 14 日アクセス）

[6] LatifMather，Subra Kumaraswamy，ShahedTim，クラウドセキュリティ&プライバシー　ーリスクとコンプライアンスに対する企業の視点ー, 株式会社オーム社, 2010.

[7] 西村健，中村素典，山地一，佐藤周行，大谷誠，岡部寿男，曽根原登，多様なポリシーを反映可能な認証フェデレーション機構の実現, 電子情報通信学会論文誌 D J96-D(6)，pp.1400-1412，2013-06.

[8] 独立行政法人情報処理推進機構セキュリティセンター，情報セキュリティ技術動向調査タスクグループ報告書（2011 年上期），52-61，2011-9.

[9] 八木晃二，内山昇，山崎崇生，共通番号制度の実現に向けた「本人確認」のあるべき姿, 知的資産創造, 20(6), 48-61, 2012-06.

[10] 城間政司，長田智和，谷口祐治，名嘉村盛和，玉城史朗，トラストフレームワークモデルを適用した OpenID 拡張手法の提案，電子情報通信学会論文誌. D, 情報・システム J95-D(12), 2021-2030, 2012-12-01

[11] M.Rundle, E.Maler, A.Nadalin, D.Reed, M.Rundole, and D.Thibea, “The opne identigy trust framework (oitf) model,” http://openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf, 2010.

[12] 財団法人日本規格協会情報技術標準化研究センター，アイデンティティ管理技術標準化調査研究　成果報告書，2010-03.

[13] 電子政府ガイドライン作成検討会，オンライン手続におけるリスク評価及び電子署名・認証ガイドライン，2010.

[14] 伊藤宏樹，クラウドにおけるアイデンティティ管理の課題，日本電信電話株式会社，情報処理，51(10)，1610-1619，2010-10.

[15] Colin Soutar, Joni Brennan, Identity Assurance framework: Overview, Kantara Initiative, 2010.

[16] 栗田克己，クラウド・コンピューティングにおける非対称情報の解消について，情報通信学会誌 30(1), 15-26, 2012-05.

[17] 佐藤栄城，クラウドサービスにおける第三者認証制

度利用の問題点に関する考察，情報セキュリティ大学院
大学 2012 年度特定課題研究報告書