OpenID Connect と SCIM の
エンタープライズ利用ガイドライン

一般社団法人 OpenID ファウンデーション・ジャパン
Enterprise Identity ワーキンググループ (EIWG) 著

作成日： 2016 年 3 月 28 日

リビジョン： 2.0

目次

第1章 エンタープライズ IT におけるフェデレーションとプロビジョニングの有用性

1.1. パブリッククラウドの普及に伴う新しいセキュリティ対策の必要性

ここ数年、企業や大学などの組織における様々な業務を支援する IT、いわゆるエンタープライズ IT の世界においても、PaaS、IaaS、SaaS など、様々な種類のパブリッククラウドサービスが普及してきている。先進的な企業の中には顧客管理システムをはじめとしたミッション・クリティカルな業務でさえも、SaaS に移行し始めているところがある。

これに伴い、これまで企業内部で厳重に保管・管理されてきた企業の機密情報が、クラウドサービス事業者の環境で保管されるケースは、ますます増える傾向にある。

そこで、クラウドサービス利用企業は、クラウドサービス事業者に預けた機密情報が、意図せずに漏えいすることを防止するためのセキュリティ対策を、検討、実施する必要性が高まった。

しかし、クラウドサービス利用企業とクラウドサービス事業者は別法人であるため、これまで社内で実施してきたセキュリティ対策をクラウド事業者に対して強制することは困難である。

（場合によっては、クラウドサービス利用企業は、クラウドサービス事業者のサービス・レベル・アグリーメント（SLA）の中に記載されてある、クラウドサービスの運用管理ポリシーや技術面の脆弱性をチェックした結果、自社のセキュリティポリシーや IT システムの運用管理ポリシーを、SLA に合わせて、見直さざるを得ないケースもある。）

そこで、クラウドサービス利用企業はセキュリティコントロールが効かない外部組織に機密情報を預けることを前提とした、従来とは異なる新たなセキュリティ対策が必要となる。

本書では、コンシューマ IT の世界で普及したフェデレーション技術が、この新しいセキュリティ対策として有効であること、さらにエンタープライズ IT に応用するためのポイントと、それに伴い必要となるプロビジョニング API の標準化について説明する。

1.2. コンシューマ IT で普及するフェデレーション技術

フェデレーション技術はコンシューマ IT の世界で普及してきた技術で、複数の Web サイト間で利用者の認証情報を受け渡すことで、シングルサインオンが可能になる。さらに、複数の Web サイト間の ID 情報連携機能により、利用者がある Web サイトに一度登録した ID 情報は、他のサイトでは直接入力する必要がなくなる。このことは、クラウド事業者にとっても、利用者のアイデンティティ情報を必要以上に保管・管理せずに、サービスを提供することが可能となり有用である。

例えば、航空会社のチケット予約用 Web サイトとレンタカー会社のレンタカー予約用 Web サイトがフェデレーション技術で連携されている場合、利用者があらかじめ ID 情報を登録した航空会社のチケット予約用 Web サイトで認証されれば、航空会社の Web サイトで行われた認証処理の結果は、ID トークンとしてレンタカー会社の Web サイトに引き渡されるため、レンタカー予約用 Web サイトであらためて ID、パスワードを入力するログイン処理は必要なくなる。

さらにレンタカー予約時に入力する必要がある利用者の住所や電話番号等の情報も、航空会社の Web サイトよりレンタカー会社の Web サイトに自動連携されるため、利用者が直接、入力する必要がなくなる。

1.3. エンタープライズ IT でのフェデレーションの有用性

パスワード等の認証に利用するアイデンティティ情報は特に機密性の高い情報であり、セキュリティ対策を検討する場合に要となる。これまでのエンタープライズ IT における認証処理は、ローカル認証方式と呼ばれ、アイデンティティ情報はアプリケーションから直接参照できる場所にまとめて保管され利用されてきた。（直接参照する方式は、主にアプリケーションが独自の認証用 DB を持ち、それを参照する方式と、LDAP サーバや Active Directory 等のディレクトリサーバに保管されたアイデンティティ情報を参照する方式の 2 通りの方式がある。） つまり、エンタープライズ IT がローカル認証方式をベースとしてクラウドサービスを利用する場合は、アイデンティティ情報をすべてクラウド事業者側に預ける必要があった。

クラウドサービス事業者がサイバーアタックを受け、情報漏えいが発生し、パスワード情報を含むすべてのアイデンティティ情報が漏えいしたとすると、アタッカーはこのアイデンティティ情報を利用して、別のクラウドサービスにあるサイバーアタックを受けた企業の機密情報へのアクセスを試みる可能性もあり、二次被害の拡大につながりかねない。

クラウドサービス利用企業が、クラウドサービス事業者にアイデンティティ情報を預ける場合でも、すべての情報をクラウドサービス事業者に預けるのではなく、パスワード情報など一部の情報だけでも社内に残し、自分たちのセキュリティポリシーに沿ったセキュリティコントロールが効くようにできればセキュリティ対策として大変、有効である。

これは、クラウドサービス利用企業のセキュリティポリシーが、クラウドサービス事業者のポリシーと合致しないケースにおいては特に効果的な対策となりうる。

そのためにはエンタープライズ IT で従来から利用されてきた、認証処理であるローカル認証方式を見直し、別の認証方式に変更する必要がある。それが、フェデレーション技術を利用した認証方式である。

このフェデレーション技術をエンタープライズ IT 環境に応用することで、クラウドサービス事業者（前述のコンシューマ IT の例ではレンタカー会社）が行ってきた認証処理を、クラウドサービス利用企業（前述のコンシューマ IT の例では航空会社）側に委譲し、アイデンティティ

情報をすべてクラウド事業者に預けずに、アイデンティティ情報の一部をクラウドサービス利用企業に残すことが可能となる。

さらに、クラウドサービス利用企業はクラウドサービス利用時の認証処理を自分たちで行えることで、クラウドサービス事業者の認証システムの制約を受けずに、例えば多要素認証に対応したシングルサインオンシステムを構築するなど、情報の機密レベルに応じた認証方式を自由に選択することができるようになる。今後の認証方式として話題に上ることが増えてきた FIDO（First IDentity Online の略で、米国の FIDO Alliance が策定を進めているオンライン認証の規格）を利用した多要素認証やパスワードレス認証を実装したい場合でも、このフェデレーション技術を併用してシステムを構築することは、クラウドサービス利用企業にとって大変に、有用である。

また、シングルサインオンの観点からもフェデレーション技術を採用することは効果がある。企業内のシステムに対するシングルサインオンは、対象システムが企業の管理下にあることを前提として、様々なシングルサインオン認証システム（パッケージソフト）を利用し、エージェント方式（管理対象システムにエージェントモジュールをインストールする方式）やリバースプロキシ方式によって実現される。

一方、クラウドサービスは利用企業の管理下にはなく、クラウド利用企業が多岐にわたるマルチテナント環境にあり、クラウドサービス事業者が、利用企業の採用している様々なシステム（パッケージソフト）や方式のシングルサインオンに逐次対応することは困難である。

また、企業外からのアクセスも可能であるクラウドサービスの特性から、アクセス制御を実施する箇所を企業内のアクセス制御用サーバに一元化するリバースプロキシ方式の採用は、クラウドサービス利用に際しては現実的とは言えない。そこで、クラウドサービスに対してシングルサインオンを行うには、フェデレーション技術を利用することが最善策となる。

1.4. 複数組織で情報共有する場合のフェデレーションの有用性

製造業でサプライチェーンに参加する複数の企業間や、共同研究や単位互換制度の運用を行う複数の大学間など、情報を共有する機会は益々増えてきている。（システムの提供形態としては、共有情報を所有する組織（オーナー組織）が中心となり、プライベートクラウド上で情報共有環境を構築する例が多く見受けられる。）

複数の組織で情報を共有する場合に、利用する認証方式が、前述のローカル認証方式である場合、オーナー組織が認証用のアイデンティティ情報を発行し、管理する必要がある。

これによりオーナー組織は、他組織のアイデンティティ情報の管理を行う必要があり、管理工数が増加するとともに、万が一情報が漏えいした場合のセキュリティリスク(賠償責任や組織の信頼を大きく損なう可能性)も抱えることになる。また、情報を共有する側の組織にとっても、

共有するシステムの数だけ自分たちのアイデンティティ情報が拡散されることになり、こちらもセキュリティリスクと言える。

そこで、フェデレーション技術を利用することで、オーナー組織（1.3 節のクラウドサービス事業者と同様の立場）から、認証処理を分離し、認証処理は情報を共有する各組織（1.3 節のクラウドサービス利用企業と同様の立場）内で行うことで、セキュリティリスクを低減することが可能となる。

フェデレーション技術の利用は他組織が発行・管理するアイデンティティ情報を信頼することが前提となり、フェデレーション技術自体を理解するだけではなく、トラストや身元確認の考え方も理解する必要がある。これについては第 3 章で詳しく説明する。

そして、このようなフェデレーションの仕組みとして今注目を浴びているのが、コンシューマ IT の世界で普及が進む OpenID Connect であり、これについては第 2 章の「OpenID Connect と SCIM の概略と構成例」と、「OpenID Connect と SCIM のエンタープライズ実装ガイドライン」で詳しく説明する。

1.5. フェデレーション利用におけるエンタープライズ IT 特有の考慮すべき点

コンシューマ IT の世界でフェデレーション技術を利用する場合、利用者は自らのアイデンティティ情報を、ID 情報連携の元となる Web サイト（1.2 節の例では航空会社の Web サイト）に登録を行うだけで、連携される Web サイト（1.2 節の例ではレンタカー会社の Web サイト）側では特にアイデンティティ情報の事前登録は必要ない場合が多い。連携される Web サイト側で利用者のアイデンティティ情報が必要となったときに、フェデレーションプロトコルのやり取りの中で、逐次、連携元の Web サイトから必要な情報の提供を受ける（＝Just In Time プロビジョニング）方法が活用されている。

一方、エンタープライズ IT の世界でよく利用されているスケジュール共有システムや営業支援システムでは、複数の従業員の間で、従業員個人を互いに識別し、それぞれの従業員のスケジュール等の情報を共有するため、ログインをしていない従業員の情報がアプリケーションデータとして予め必要となる。

また、アクセス制御情報は、単純に組織や役職によるだけではなく、業務上の役割や引き継ぎ期間等も考慮した複雑なロール管理を必要とする場合もあり、個人の識別に必要な属性情報（氏名、所属、メールアドレス等）だけでなく、アクセス制御に必要な属性情報（役職、業務上の役割等）が認証処理の前に整備され、ロール情報として加工されている必要がある場合も多い。

このようなアプリケーションデータとしてのアイデンティティ情報の処理や、複雑なアクセス制御のためのアイデンティティ情報の処理を、Just In Time プロビジョニング方式の中ですべて行うことは、処理内容的にも開発コスト的にも困難である。

そこで、エンタープライズ IT の世界においては、フェデレーション技術を認証処理で利用する場合であっても、クラウドサービス利用開始前にこれらのアイデンティティ情報をクラウドサービスに登録しておく必要がある。

コンシューマ IT では、個人が自らのアイデンティティ情報をクラウドサービスに登録して、サービスを利用するが、エンタープライズ IT では、クラウドサービスを利用する企業の情報システム部門の ID 管理担当者が、利用契約に応じたライセンス数の範囲の中で、従業員のアイデンティティ情報をクラウドサービスに登録する。

さらに、企業では、新規登録だけではなく、組織改編、人事異動（入社、退社、昇格、所属変更、休職、復職、出向、復帰といったイベント）をアイデンティティ情報（属性情報）に反映させる、アイデンティティライフサイクル上の運用を考慮する必要がある。これは決算期末や期初に定期的に大規模に行われる場合もあれば、緊急に個別に発生する場合もある。

そして、アイデンティティのライフサイクル運用をベースとしたロール管理としては、発令日に先立って更新データを事前に入力しておき、発令日になると更新データが有効になるような仕組みや、発令後も当分は発令前の状態を併存させ異動猶予期間を設けるような仕組みなどが求められる場合もある。

これらのメンテナンス作業を情報システム部門の ID 管理担当者が、コンシューマ IT のように、利用するクラウドサービスの GUI（Graphical User Interface）を介して 1 ユーザ毎にメンテナンスを行うことは非常に手間がかかり、さらにオペレーションミスにつながる可能性も高く、別の処理方法を考える必要がある。

そこで、定期的な組織改編や一斉の人事異動に対応し、複数のアイデンティティ情報を CSV ファイルやクラウドサービスのアイデンティティ登録用の API に対してコマンドライン等で一括して登録できる機能や、実際のメンテナンス作業日とアクセス制御情報の適用日までの間に猶予期間を待たせることができる機能を有する、ID 管理システムを利用して、アイデンティティ情報をクラウドサービスに配布（プロビジョニング）することになる。

また、企業内（オンプレミス）に既に ID 管理システムを構築している場合、新たに利用しようとするクラウドサービスのアイデンティティ情報は企業内の各システムのアイデンティティ情報と統合管理したいという要求は非常に強く、この場合、アイデンティティ情報をクラウドサービスに配布（プロビジョニング）する機能は既存の ID 管理システムを拡張して行う場合が多い。

つまり、エンタープライズ IT の世界ではフェデレーション技術を活用する場合でも、ID 管理システムによる事前のプロビジョニング処理を併用することが重要なポイントであると言える。

2 つ目のポイントは、アイデンティティ情報と認証システムの基盤が企業内（イントラネット内）に存在することが挙げられる。

コンシューマ IT の場合、利用者個人が個人端末からクラウドサービスへアクセスする際の通信は、すべてインターネット上でやり取りされる。

一方、エンタープライズ IT の場合、利用者である従業員個人が企業端末からクラウドサービスへアクセスする際の通信は、企業内（イントラネット内）のネットワークからインターネットに接続され、やり取りされる。（モバイルアクセスにおいても企業内（イントラネット内）に存在する ID 管理・認証システムの基盤を介してやり取りされる場合が多い。）

そして、この企業内（イントラネット内）に存在する ID 管理・認証システムとクラウドサービスの間にはファイアウォール等のネットワーク境界が存在し、データ通信の出入りが制限されている。特に外部（インターネット）側から企業内（イントラネット内）のデータやシステムへアクセスすることは、通常厳しく制限されている。

つまり、エンタープライズ IT の世界でフェデレーション技術を用いた認証・認可処理を構築する場合は、ファイアウォール等のネットワーク境界を考慮し、クラウドサービス事業者からクラウドサービス利用企業への通信が制限される前提で、フェデレーション技術の適用方法を設計することが重要なポイントになる。

これについても「OpenID Connect と SCIM のエンタープライズ実装ガイドライン」で詳しく説明する。

1.6. エンタープライズ IT におけるプロビジョニング API の必要性

フェデレーション技術と ID 管理システムを併用することが重要なポイントとなるエンタープライズ IT の世界では、クラウドサービス事業者は、アイデンティティ情報を受け取り、メンテナンスするためのインターフェースとして、GUI の提供だけでなく、プロビジョニング用インターフェースを用意し公開することが求められる。

エンタープライズ IT の世界では、従来より、以下の２つの方法で、プロビジョニング用インターフェースが準備されているこが多い。

一つ目の方法は、アイデンティティ情報の一括取り込みに重きを置いた CSV ファイルを利用する方式である。しかし、CSV ファイルを受け取る方式の場合は、クラウドサービス事業者へのアイデンティティ情報の配布（プロビジョニング処理）が完了した後、CSV ファイルを即時に削除する仕組み(運用)になっているか否か、あるいは利用者が削除のタイミングを自ら設定できるかどうかは、利用企業のセキュリティの観点から非常に重要なポイントとなる。しかし、クラウドサービス事業者が CSV ファイルを後始末する仕組み(運用)について適切な説明を行って

いない場合が非常に多く、CSV ファイルの所有者であるクラウドサービス利用企業は、セキュリティ面から不安を感じることになる。

プロビジョニング用インターフェースとして CSV ファイルを利用する方式では、このような中間ファイルとしての CSV ファイルの扱いが課題となる。

二つ目の方法は、クラウドサービス事業者が各社それぞれで独自に API を作成し、プロビジョニング用インターフェースとして公開する方式である。

この場合、クラウドサービス利用企業が新たなサービスを利用するには、その都度、サービス単位で個別に提供されたプロビジョニング用インターフェースに対する連携システムを開発したり、ID 管理ツールの連携用オプション部品を購入したりしなければならず、クラウド利用企業のコスト負担は大きくなる。

そこで、利用するクラウドサービスの数が増加すればするほど、プロビジョニング用インターフェースの標準化が必要となる。クラウドサービス利用企業にとっては標準化されたプロビジョニング用インターフェースがあれば、アイデンティティ情報の連携システムとしては一度開発したシステムの再利用が可能になり、ID 管理ツールの連携用オプション部品の購入にしてもリーズナブルな販売価格の設定を期待することができる。一方、クラウドサービス事業者にとってもプロビジョニング用インターフェースについては、標準化されたものが存在し、これを利用することができれば、自ら独自に開発するより、開発工数を大きく削減することが可能になる。

プロビジョニング用インターフェースにおいて標準化の検討が進んでいるのが、SCIM（System for Cross-domain Identity Management）である。SCIM は 2015 年 9 月に RFC 7642～7644[1][2][3]として公開された。これについても「OpenID Connect と SCIM のエンタープライズ実装ガイドライン」で詳しく説明する。

第2章 OpenID Connect の概略と構成例

2.1. 用語の定義

本節では、本ガイドで利用する用語について解説する。

1. OpenID Provider (OP)

   クラウドサービス企業において、社内外の RP からの認証要求に対して、社内ユーザに対する認証処理を行い、その認証結果を返すシステム。

   OpenID 以外の文脈では、しばしば Identity Provider (IdP) と呼ばれる。

   第 1 章の例では、コンシューマサービスにおける航空会社、エンタープライズ IT におけるクラウドサービス企業が、この役割を果たしている。

2. Relying Party (RP)

   クラウドサービス事業者において、クラウドサービス企業に認証処理を要求し、その認証結果を受け取りクラウドサービスへのアクセス可否などを判断するシステム。

   OpenID 以外の文脈では、しばしば Service Provider (SP) と呼ばれる。

   第 1 章の例では、コンシューマサーヒスにおけるレンタカー会社、エンタープライズ IT におけるクラウドサービス事業者が、この役割を果たしている。

3. Attribute Provider (AP)

   クラウドサービス企業において、社内外の RP に対して、社内ユーザのアイデンティティ情報をプロビジョニングするシステム。図 1 においては ID 管理システムが該当する。

   本ガイドで扱う Attribute Provider は、実質的には SCIM Client だが、アイデンティティ情報を提供する抽象的な役割で捉えるために、Attribute Provider として扱う。

   第 1 章の例では、コンシューマサービスにおける航空会社、エンタープライズ IT におけるクラウドサービス企業が、この役割を果たしている。

2.2. クラウドサービス利用におけるフェデレーションとプロビジョニングを併用例

本節では、企業がクラウドサービスを利用することを想定し、事前に ID 管理システムからクラウドサービスに対してアイデンティティ情報の登録を行った上で、フェデレーション技術

（OpenID Connect）を認証処理で利用する場合の、クラウド利用者、OpenID Provider (OP)、Relying Party (RP) 間の認証処理連携方法について説明する。

クラウドサービス利用企業は社内に認証処理を行い、アイデンティティ情報の発行を行う役割を持つ OpenID Provider (OP) を構築する。

一方、クラウドサービス事業者はサービスを提供するために、認証処理を委譲し、アイデンティティ情報を受け入れる役割を持つ Relying Party (RP) を構築する。

クラウドサービス利用企業に新しい社員が入社し、この社員がクラウドサービスを利用する想定での一連の流れは図 1 の通りである。

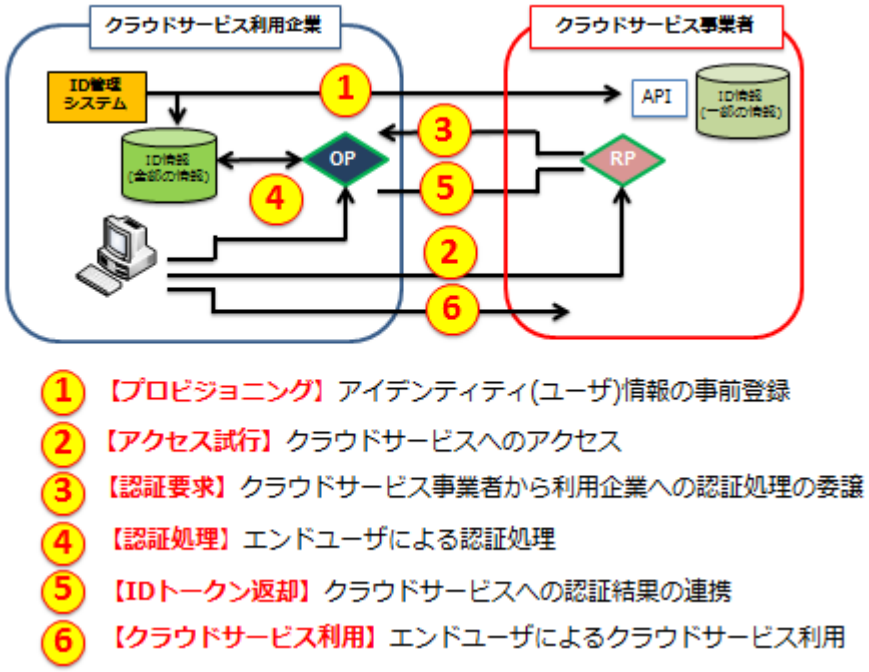

図 1　プロビジョニングとフェデレーションの流れ（例）

① クラウドサービス利用企業の IT 部門の ID 管理者は ID 管理システムを利用し、クラウドサービス事業者のプロビジョニング API を介してアイデンティティ(ユーザ)情報の事前登録を行う。
② 新入社員は、IT 部門の ID 管理者から発行された自身の従業員 ID を用いて、クラウドサービスを利用しようと、クラウドサービスにアクセスする。
③ クラウドサービス事業者に設置された RP は認証処理をクラウドサービス利用企業の OP に委譲する。
④ 新入社員は社内の OP に対して認証処理を行う。
⑤ OP は RP に対して認証処理結果を返す。
⑥ 認証ができた新入社員はクラウドサービスにアクセスできるようになる。

以上の手順の中で①で説明したプロビジョニング API について標準化の検討が進んでいるのが SCIM である。また②～⑤のやりとりが OpenID Connect である。それぞれの適用範囲を図 2 に示す。

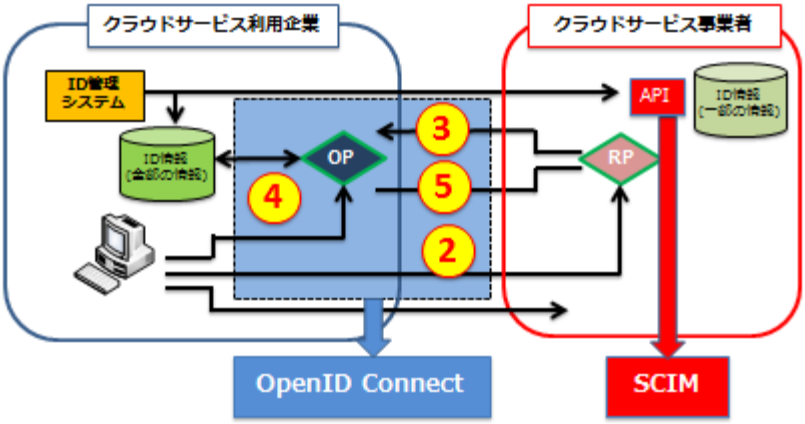

図 2　SCIM と OpenID Connect の適用部分

第3章 アイデンティティとトラスト

3.1. なぜトラストが大事なのか

第 2 章で説明し OpenID Connect を実際のシステムで有効活用するためには、他組織が発行・管理するアイデンティティ情報を信頼することが前提となり、トラストや身元確認の考え方を理解する必要がある。本章ではトラストや身元確認の考え方について説明する。

クラウドコンピューティングの発展と普及により、SaaS のように複数のシステムを連携させた複雑なサービスが柔軟かつ迅速に構築できるようになっただけでなく、ビジネスや組織の側にも、こうしたサービスの変化に合わせて柔軟かつ迅速に自ら(ビジネスや組織)を構成できる能力が求められるようになってきた。第 1 章で述べたような複数組織間での情報共有なども、こうした社会の変化に迅速に対応するためのひとつの現れと言えるだろう。SCIM のようなアイデンティティの分散管理技術、OpenID Connect のようなフェデレーション技術は、こうしたビジネスや組織の疎結合性を高める技術として役立つ。

OpenID Connect や SCIM といった技術の普及が進むことで、エンタープライズ IT がクラウドサービスを活用するにあたってのフェデレーションはますます有用になってくる。エンタープライズ IT は、フェデレーション技術の発展普及によってその ID 管理をより柔軟に実現できるようになり、またクラウドサービスをより安全に利用できるようになる。特に、拠点が各地に分散している企業や、グループ企業や部門毎に IT システムが分散しているケースでは、個々の IT システムで既に運用している ID 管理システムや認証情報を、そのまま利用することが可能になる。ID 管理を一極集中させることには管理コストの集約など一定の意義はあるが、ID 発行時の身元確認やクレデンシャルの発行などは、分散の規模などによっては集約よりも分散管理の方が安全面でもコスト面でも合理的な場合がある。また 1.4 節で述べたように、オーナー組織が他組織のアイデンティティ情報管理を行うことの課題も、分散 ID 管理によって解決可能となる。フェデレーションの発展・普及は、こうした分散 ID 管理が有利なケースを中心にエンタープライズ IT でのクラウドサービス活用を推進することが期待される。

ただし、フェデレーションを利用する上で考慮すべき点もいくつかある。中でも ID 管理を分散するケースにおいては、各 ID 管理システムの運用部門（運用部門が他組織である場合も含まれる）において、十分な身元確認を行っているか、退職した社員の ID を適切なタイミングで無効化しているか、といった、運用管理面での懸念が少なからずあるだろう。これは、「分散する（他組織の）ID 管理に対する信頼」の問題として捉えることができ、運用管理面の問題であるが故に技術のように画一的に実現しづらいこと、また組織毎の裁量が大きく影響する部分であることなどが、問題の単純化を阻んでいる。

このような分散 ID 管理のトラスト問題を解決するために、LoA（Level of Assurance）という概念が役に立つ。これは、各組織が一定の運用管理基準にもとづいて ID 管理を行っているこ

とを保証するための概念であり、RP から IdP (OP) に対して ID 管理に関する一定の信頼性を要求するものである[4]。

一方、IdP (OP) から RP に対して要求するものとして Level of Protection (LoP) というものがある。これは、SCIM による属性情報のプロビジョニングや、フェデレーションにおける属性交換を行うにあたって、IdP (OP) の提供した属性情報が RP においてどれだけ安全に管理されているかを示す尺度である[5]。

次節以降で、これら LoA や LoP について説明する。

3.2. 身元確認と（認証情報の）LoA

「分散する ID 管理に対する信頼」問題を解決するためには、ID 管理を行う各組織が一定の運用管理基準にもとづいて ID 管理を行っていることを保証することが有効である。この運用管理基準に求められるレベルが LoA であり、いくつかの評価軸によって決められることになる。

ITU-T X.1254（ISO/IEC 29115）[4] では、表 1 に示す 4 段階の LoA を規定するとともに、その評価軸として IdP (OP) の運用について 3 つのフェーズ – 加入 (Enrolment) フェーズ、クレデンシャル管理 (Credential Management) フェーズ、エンティティ認証 (Entity Authentication) フェーズ – に分け、それぞれにおいて、どの程度の安全性・信頼性を確保できているかを評価することが規定されている。加入フェーズでは、加入者が ID を入手するための申請方法、本人確認方法、加入情報の登録方法などが定義される。クレデンシャル管理フェーズでは、後のエンティティ認証フェーズで用いるクレデンシャルの生成・発行・保管方法や失効・休止方法などが定義される。これらを定義することは即ちクレデンシャルのライフサイクル管理について定義することでもある。エンティティ認証フェーズでは、クレデンシャルを用いた認証方法が定義される。なお、X.1254 における LoA は抽象的な定義にとどまっており、各レベルの詳細な基準は、各フェデレーションにおいて個々に規定することを想定していること、また民間での実質的な利用において想定される LoA はたかだか LoA2[1]であり、これを 3 段階に細分化する議論もあることに留意されたい。国内においては、政府 IT 戦略本部が策定した「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」において規定された事例がある[6]。同ガイドラインでは、例えば加入フェーズにおける LoA1 要件としてメールの到達性確認、LoA2 要件として身分証の提示などが挙げられている[2]。

このように様々な評価軸から認証情報の確からしさを保証する仕組みが整備されることによって、他組織が運用管理する認証情報であっても一定の範囲で信頼することが可能となる。また、

[1] これは 4 段階 LoA の起源が政府機関を対象としているためで、[6]においても、ユースケースとしては LoA3 で大規模政府調達、LoA4 では司法当局による犯罪歴データベースへのアクセスなどが挙げられており、例えば住所変更などの行政手続きは LoA2 として示されている。

[2] なお、各要件は対面確認・リモート確認など条件に応じて詳細に定義されており、また加入フェーズ以外においてもそれぞれに要件が規定されているため、具体的な内容については同ガイドラインを参照されたい。

この仕組みは技術のみによって実現されるものではなく、継続的な評価すなわち運用を伴って実現されるものである点は極めて重要である。

表 1　保証レベル

保証レベル	定義
レベル 1（低い保証）	特定される身元識別情報の信用度がほとんどない
レベル 2（中程度の保証）	特定される身元識別情報の信用度がある程度ある
レベル 3（高い保証）	特定される身元識別情報の信用度が相当程度ある
レベル 4（かなり高い保証）	特定される身元識別情報の信用度が非常に高い

3.3. 身元確認と属性の LoA

X.1254 を始めとする多くの LoA は認証情報をスコープとしたものであるが、アイデンティティ情報には認証情報以外にも多様な属性情報がある[7]。一般に認証情報とは、識別子（ID や公開鍵証明書）とそれにひもづくクレデンシャル（パスワードや私有鍵）が対象であり、識別子やクレデンシャルを発行し同一性を保証する権威（Authority）が存在することを前提としている。一方の属性情報は、属性種（「職種」や「趣味」）とその値（「課長」や「読書」）が対象であり、その権威の扱いは認証情報とは大きく異なる。例えば職種の場合は所属組織が権威に相当するが、趣味の場合は権威に相当する組織が存在しない（強いて言えば本人）。さらには、住所の場合に自治体は明らかな権威と言えるが、住民票を確認した企業や運転免許証を確認したサービス提供者などを権威と位置づけられるかどうかは議論が分かれるところである[3]。このように、発行組織が必ずしも明に唯一存在するとは限らない点で、属性情報は認証情報と大きく異なる。

属性情報においても認証情報と同様にその確からしさが重要となる場合があり、ここでは LoAA（Level of Attribute Assurance）と呼ぶ。典型的には職種や所属部局に応じた権限管理・アクセス制御を行う場合が挙げられる[8]。このようなケースでは、発行された職種に間違いがあったり異動後も所属部局が未更新のままであったりすると、適切な権限管理・アクセス制御が実現できない恐れがある。即ち、LoAA においては、アイデンティティ情報同様に、属性情報の確からしさに加えて属性のライフサイクル管理の重要性もまた強く求められることになる[9]。

このような LoAA は、カナダ政府などいくつかの組織で策定されている[10][11]。LoA においては、IdP（OP）の運用管理基準に対して評価軸を定めることによって、LoA の信頼を実現して

[3] 同一性を保証する原簿を直接確認可能な前者（自治体など）を一次機関、一次機関が発行する情報（住民票の写しや運転免許証）をもとに間接的に確認可能な後者（企業やサービス提供者）を二次機関と位置づけるなどレベルを分けて扱う考え方もある。

いるように、LoAA においても AP の運用管理規準に対する評価軸を定めることが、LoAA の信頼を構築することにつながる。LoAA のレベル分けについては、まだ世界的に十分な合意形成ができているとは言えないものの、カナダ政府の例をはじめ LoA と同様に 4 段階（あるいは 4 段階の LoA とマッピングしやすい形で）で規定して相互運用性を確保しようという流れのようである。

LoAA と LoA との違いとしては、その評価軸だけでなく、RP に流出するプライバシーの度合いもまた大きく異なる。前者は単に IdP (OP) が AP に変わるだけでなく、前述の通り発行機関が明に唯一存在するわけではないということを意味しており、後者は認証結果のような単純な情報だけでなく、（同意した上での場合も含めて）本人のプライバシーに関わり得る情報自体が流出するということを意味する。

3.4. 属性情報の保護と LoP

フェデレーションによって認証情報を与えた他組織、SCIM によって属性情報を与えた他組織が、受け取った情報を安全に管理してくれるか、という問題もある。認証情報を提供する側が、提供する情報の信頼性を保証するのと同様に、情報を受取る側も、受け取った情報の安全性について保証することが求められる。このように RP が扱う（IdP (OP) や AP から提供を受けた）属性情報の安全性の尺度として、LoP いう概念が広まりつつある。特に属性情報は、それ自体が直接プライバシーに関わるものである場合が多いこと、また二次利用や再配布などの可能性を技術的に制御するのが難しいこと、更には古い属性情報を更新せずに使い続ければ適切な認証認可が行えない場合があることなどから、提供先事業者 (RP) に対して一定の LoP を求める必要が出てくる。

LoP の評価尺度としては、例えば収集した情報の保存期間や、ISMS など適切なセキュリティ管理標準への準拠性、一定のプライバシー保護対策など（例えば属性値の仮名化など）の評価軸が必要になると考えられているが、まだ標準的なものは確立しているとは言い切れない。LoP も LoA や LoAA 同様に 4 段階、あるいはこれらとマッピングしやすい形で規定することで、相互運用性が確保しやすくなると考えられる。

第4章　権限委譲の適用と課題

エンタープライズにおける認証認可に関する課題のひとつに ID の共用による権限委譲がある。OpenID Connect や SCIM に限らず、これまでも ID 管理/ID 連携のエンタープライズ活用を行う上でこの課題は避けて通れないものであった。しかしながらクラウドの活用が進んでいる現在、従来は企業自身のオンプレミスシステムにおいて曖昧な運用によって対処してきたこの課題をこれ以上先送りにすることが困難になってきている。

本節では、ID 共用による権限委譲に関する課題の整理を行い、適正な ID 運用に求められる要件および対応するテクノロジ・トレンドの紹介を行う。

4.1. 企業における ID に対する認識と運用上の課題

エンタープライズとコンシューマにおける ID の取り扱いにおいて根本的に異なる点として「ID の持ち主と利用目的」が挙げられる。

コンシューマにおける ID 利用の目的は個人がサービスを受けることにあるため、ユーザが自発的に ID を取得し利用する。一方でエンタープライズにおいて ID は業務を遂行する目的で組織によって発行され個人に貸与されるものである。

表 2　コンシューマとエンタープライズでの ID の取り扱いの差異

	コンシューマ	エンタープライズ
持ち主	個人	組織
利用目的	自身がサービスを受けるため	業務を遂行するため

特に歴史的に見て職務権限や責任範囲が個人レベルに落とし込まれにくい日本企業においては、業務を個人の責任で遂行するのではなく、職場全体で業務を遂行していく、という意識や風潮が強い。結果として、共同で業務を遂行するのであれば ID の共用や貸与を行っても特に問題にならない、と考えられがちなのである。

しかし一方で近年は企業内における統制の強化が叫ばれ、職務権限の明確化と個人のアクセス権限の厳格化、そして監査証跡の取得が必要となってきており、実際の業務遂行方法や個々の従業員の意識との乖離がうまれている。

現実問題として、企業向けの ID の利用実態を調査すると、事実上の権限委譲と称して秘書が担当の役員の ID を使ってシステムを利用したり、委託先ごとに共通の ID が代々引き継がれていたり、工場のラインでは ID が機械を動かすための単なる儀式として共有されていたり、と個

人 ID を発行する側のシステム部門の意図に反した使われ方が実際は横行しているケースがしばしば見られる。

このことにより、

- 実際は誰が ID を使っているのかがわからない
- 証跡の取得が出来ない
- ID の又貸しが行われている／出来てしまう

など、近年声高に叫ばれている内部不正対策やセキュリティ・統制強化を行う際に大きな課題に直面することも少なくない。

4.2. 代理アクセスのあるべき姿と必要な機能

では、これらの実情を踏まえた上でエンタープライズにおける ID をどのように管理していくべきなのだろうか？

本質的には業務の整理や職務分掌の明確化をきっちりと行い、業務上の役割と個人の 1 対 1 のマッピングが行われれば ID の利用方法もおのずと正しい方向へ向かうはずだが、長い歴史の中で培われてきたものを変更するのは非常に困難である。特に運用やインフラ領域とみなされている ID/アクセス管理を正確に行うため、という理由では現場の理解を得ることは非常に困難である。

現場の既存運用を優先することで実現される効率性を維持しつつ、ID/権限管理の統制を行うために必要となるのは、ID 自体の貸し借りで権限を委譲するのではなく、委譲先の主体に必要な「権限」を貸し出し、貸し出し状況のコントロール／可視化を行うことであろう。

表 3　代理アクセスの手法としての共用 ID と権限の貸与

	共用 ID（ID の貸し借り）	権限の貸与
利用者個人の特定、可視化	✖	o
業務上必要な権限の利用	o	o
運用	現場（個人）に依存	システム側での対応が必要

これまでも ID ワークフローシステムや特権 ID 管理ソリューションを利用することで、ファイルサーバの特定のフォルダへアクセスするための権限を一時的に個人やセキュリティ・グループに付与するなど、単位・粒度が比較的大きい権限を対象として ID/権限管理の自動化・セルフサービス化は行われてきた。

しかし、今後エンタープライズにおいてもアプリケーションのアーキテクチャが更に分散化する傾向にあり、API レベルでの権限コントロールへの対応も求められてくると思われる。

これらを踏まえ、権限の貸し出しに関する管理要件を整理した例を下記に挙げる。

＜管理要件＞

- 事前に定義されたポリシーに従って貸し出しが制限できること
- 貸し出しに関する記録が取得・保持できること

＜管理項目＞

- 貸し出し主体は誰か
- 対象リソースと貸し出す権限は何か
- いつから、いつまで貸し出すのか
- 誰に対して貸し出すのか

＜対象となるリソースの単位＞

- 分散システムに対応した単位（API 単位）

今後、これらの要件を満たす形で ID/権限管理を効率化するためのシステム化が進めば、エンタープライズにおいて ID 共用に代わる権限委譲のソリューションとなり得るはずである。

4.3. 権限委譲に関するテクノロジ・トレンド

一方でコンシューマの世界における API レベルでの権限委譲を行うためのテクノロジとしては OAuth が主流である。しかし、これまでも述べてきたようにコンシューマでは他者との共同利用を意識した ID の使い方ではなく、あくまで自身の代わりにアプリケーション（OAuth クライアント）がリソース（API）へアクセスする権限を委譲する、Person-to-self というユースケースのみが想定されてきていた。

この仕組みによりアプリケーションにユーザの ID やパスワードを直接渡す必要がなくなり安全かつ便利に分散システムが構築できるようになるという利点はあるものの、企業や組織の業務上で行われる人から人への権限委譲というユースケースへは対応ができなかった。

この課題に対してカンターラ・イニシアティブで検討されてきたのが、2015 年 3 月に承認された OAuth2.0 のプロファイルの一つである User-Managed Access（UMA）である。UMA はリソースを利用する主体がリソースの持ち主とは別のユーザや組織であるという前提で設計されており、このことにより、例えば別のユーザが利用しているクライアントに対するファイル等へのアクセス許可など、自身の代わりに処理（API）を実行させることが可能となる。

表 4　UMA で想定されているユースケース一覧

ユースケース	説明
Person-to-self	自分が使うクライアントが、自身のリソースにアクセスできるようにする （現在の OAuth と同様のユースケース）
Person-to-person	別ユーザが使うクライアントが、自身のリソースにアクセスできるようにする
Person-to-organization	別ユーザ（特定の組織もしくは組織に所属する個人）が使うクライアントが、自身のリソースにアクセスできるようにする

出典）https://kantarainitiative.org/confluence/display/uma/UMA+FAQ

もちろん対象となるリソース（API）や認可サーバの対応が必要となるが、エンタープライズにおいても UMA のようなテクノロジを上手に活用していくことで積年の懸案事項であった業務実態に合わせた権限委譲のコントロールを行うことが出来るようになる日がくることも十分に考えられる。

尚、UMA に関する技術概要や仕様については[12][13][14]を参考にされたい。

参考文献

[1] LI, K., Ed., Hunt, P., Khasnabish, B., Nadalin, A., and Z. Zeltsan, "System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements", RFC 7642, DOI 10.17487/RFC7642, September 2015, <http://www.rfc-editor.org/info/rfc7642>.

[2] Hunt, P., Ed., Grizzle, K., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Core Schema", RFC 7643, DOI 10.17487/RFC7643, September 2015, <http://www.rfc-editor.org/info/rfc7643>.

[3] Hunt, P., Ed., Grizzle, K., Ansari, M., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Protocol", RFC 7644, DOI 10.17487/RFC7644, September 2015, <http://www.rfc-editor.org/info/rfc7644>.

[4] “ITU-T Recommendation X.1254 (2012)– ISO/IEC 29115:2013, Entity authentication assurance framework”, ITU, September, 2012.

[5] May Rundle, et al., “The Open Identity Trust Framework (OITF) Model ”, March 2010.

[6] 各府省情報化統括責任者(CIO)連絡会議，”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”，内閣官房， 2010 年 8 月.

[7] 情報処理推進機構，”アイデンティティ管理技術解説”，情報処理推進機構，2013 年 3 月.

[8] Cloud Security Alliance(著), 日本クラウドセキュリティアライアンス(訳)，”クラウドコンピューティングのためのセキュリティガイダンス”，V3.0, Cloud Security Alliance，2013 年 5 月 8 日.

[9] ASP・SaaS における情報セキュリティ対策に関する研究会，”ASP・SaaS における情報セキュリティ対策ガイドライン”，総務省，2008 年 1 月 30 日.

[10] “Pan-Canadian Assurance Model”, Treasury Board of Canada Secretariat, March 2010.

[11] “Standard on Identity and Credential Assurance”, Treasury Board of Canada Secretariat, February 2013.

[12] IPA「情報セキュリティ技術動向調査（2010 年上期）」, https://www.ipa.go.jp/security/fy22/reports/tech1-tg/a_05.html

[13] @IT「ユーザー中心のアクセス管理の実現を目指す User Managed Access」, http://www.atmarkit.co.jp/ait/articles/1305/09/news003.html

[14] カンターラ・イニシアティブ「User-Managed Access (UMA) Profile of OAuth

2.0」, https://docs.kantarainitiative.org/uma/rec-uma-core.html

著者一覧

江川 淳一　　エクスジェン・ネットワークス株式会社

島岡 政基　　セコム株式会社

富士榮 尚寛　　伊藤忠テクノソリューションズ株式会社

