7H-04

スマートコントラクトによるフェデレーション メタデータ管理の自動化手法

出口 裕詞† 廣津 登志夫‡
法政大学情報科学部

1. 序論

認証連携を用いることで，組織が運用する複数の異なるサービスに単一の認証情報でアクセスすることができる．認証連携を複数の組織やサービス間で活用する仕組みを認証フェデレーションという．Shibboleth を用いたフェデレーションの運用では，参加する組織の情報であるメタデータが必要となるが，これはフェデレーションを運営する組織により中央のサーバで収集，管理され随時参加する組織に配布される．フェデレーションに参加すると，そこで配布されるメタデータを参照することで，認証情報を提供する IdP やサービスを提供する SP などの参加組織は連携の度に個別に情報を交換する必要が無くなり，連携の作業負担が軽減する．しかし，組織ごとに詳細に連携を制御する場合には個別にメタデータに修正を加える必要がある．

本研究ではこのフェデレーションにおけるメタデータ管理について，スマートコントラクトを用いた自動化手法を提案する．ここでは，ブロックチェーン技術である Hyperledger Fabric を用いることで，IdP・SP 間の個別のメタデータ交換に加えて，取り扱う属性情報に関する連携ポリシーの決定の自動化を実現する．

2. 関連研究

関連研究[1]では，従来のフェデレーションにおけるメタデータの集中管理に起因するパフォーマンスの低下と単一障害点の問題を指摘し，ブロックチェーンによる管理を提案している．ブロックチェーンは，P2P ネットワークと暗号技術を組みわせることでデータを複数の利用者間で分散的に共有する仕組みであり，各ブロックはハッシュ値に基づき連結されるため，データの改竄は困難である．ブロックチェーンにより処理を自動化したスマートコントラクトは，その処理が検証可能であるため，透明性が高いという特徴がある．この研究ではスマートコントラクトを利用することで高速なメタデータの共有と動的なフェデレーション作成の機能を実現している．個別のメタデータを収集し結合したフェデレーションメタデータの共有を中央サーバで行う代わりにブロックチェーンを利用して管理することで，メタデータの分散管理を実現し，可用性とスケーラビリティを向上させている．しかし，詳細な連携の制御を行う場合は個別に設定を変更する必要があり，特に IdP が連携する SP に送信する属性を制御する場合は組織間で連携ポリシーを調整する手間が生じる．

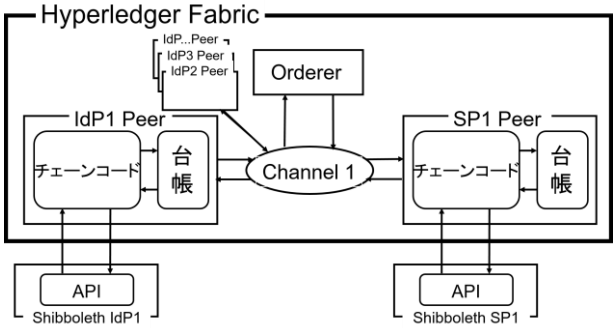

図 1 Fabric ネットワークの構成図

3. 設計

本研究ではメタデータの共有に加えて，取り扱う属性情報に関する連携ポリシーの決定についてもスマートコントラクトを利用することで自動化し，分散化されたフェデレーションの機能として実現する．図 1 に Hyperledger Fabric を用いた提案手法の構成を示す．Hyperledger Fabric では Peer はネットワーク内で同一内容の台帳とチェーンコードを保持しており，アプリケーションとの接続やチェーンコードの実行を行う．Orderer はブロックに書き込む情報や処理結果の順序付けを行い，Peer に送信する．Fabric ネットワークでは論理ネットワークとして複数の Channel を構築可能である．IdP と SP の連携に必要なメタデータは Shibboleth で利用するため XML 形式で記述されており，それぞれの組織の情報や証明書などで構成されている．台

Automatic Access Management Federation using Smart Contract
† Yuji Ideguchi, Hosei University
‡ Toshio Hirotsu, Hosei University

表 1 台帳に保存する属性情報

名称	概要
id	属性の固有名
type	属性定義のタイプ
attributeNames	属性の固有名
name_1_3	Shibboleth ver1.3 での定義名
name_2_x	Shibboleth ver2 系での定義名
friendlyName	属性の略称
isRequired	必須/選択属性の情報
category	属性の分類

表 2 属性の分類

分類名	概要
物理的な連絡先	実世界の個人との連絡手段
オンライン上の連絡先	オンラインでの連絡手段
固有の ID	個人を識別する ID
資格情報	設備を使用するための資格や権限情報
人口統計学的データ	個人を特徴づけるデータ

帳に保存する属性情報を表 1 に示す．ここでは IdP, SP の各組織はメタデータと属性情報の管理を行うために Fabric ネットワーク内で Peer を制御して，フェデレーションの連携に必要なメタデータと取り扱う属性情報を Fabric で共有する．情報を保存する台帳は Channel 単位で構成されるため，IdP は連携する SP の参加する複数の Channel に参加することでそれぞれメタデータと属性情報の共有を行うことができる．各組織は Fabric ネットワーク外部の Shibboleth アプリケーションから API を通して自組織の Peer 内のチェーンコードを呼び出すことで台帳の操作と取得を行う．取得した台帳が保持しているメタデータと属性情報に基づいて Shibboleth IdP の設定ファイルを動的に更新する．

また，必須・選択属性の情報(表 1,isRequired 属性)と，属性の種類に応じた分類(表 2,category 属性) について，その要・不要に応じたフィルタリングの機能を提供する．表 2 に属性の分類例をあげる．IdP は選択属性について，自組織が送信を許可する範囲で任意の category の属性を予め指定して取得する．SP には指定して取得した属性のみを送信することにより，各 IdP のポリシーに沿った属性の制御を可能とする．

4. 実装

Hyperleger Fabric 上でメタデータ管理を行うチェーンコード fabmetadata および，属性の情報を取り扱う fabattribute の実装について説明する．実装には Hyperledger Fabric v2.2 を使用し，Node.js および JavaScript で記述した．チェーンコード fabmetadata と fabattribute は Fabric ネットワークに参加する Peer にインストールして実行される．メタデータと属性情報は台帳に JSON 形式で保持し，チェーンコードを呼び出す際に JSON から XML へ変換される．

5. 考察

従来の単一の運営主体が担っていたメタデータ交換のプロセスを，分散管理されるブロックチェーン基盤に置き換えたことにより，単一障害点を排除することができた．これにより，システムとしての信頼性は向上したといえる．また，提案手法では各プロバイダは利用する必要最小限のメタデータのみを取り扱う．そのため，プロバイダはメタデータの管理にかかっていたストレージや計算リソースのオーバーヘッドを軽減することができる．国際的なフェデレーションサービスである eduGAIN のフェデレーションメタデータのサイズは約 59MB で項目数は約 7200 にのぼる．同様に米国内の学術フェデレーション InCommon のフェデレーションメタデータのサイズは約 77MB で項目数は約 6000 である．日本国内の学術フェデレーション「学認」のフェデレーションメタデータのサイズは約 3MB で項目数は約 350 である．上記から，一項目(単一プロバイダ)当たりの平均メタデータサイズは以下の式で表すことができる．

$$\frac{(59\mathrm{MB} + 77\mathrm{MB} + 3\mathrm{MB})}{(7200 + 6000 + 350)} \approx 10\mathrm{KB/provider}$$

これはフェデレーションメタデータと比較して非常に小さく，特にフェデレーションに参加する IdP は利用するサービスの数に応じてこれらのメタデータを数十セット保持しても大幅にオーバーヘッドを削減することができる．

5. まとめ

スマートコントラクトを利用して必要最小限のメタデータ共有と柔軟な属性管理を行う機能の設計と実装を行った．その結果，属性情報とメタデータの管理にかかるオーバーヘッドを低減することを示すことができた．

参考文献

[1] M. Grabatin and W. Hommel, ″Reliability and scalability improvements to identity federations by managing SAML metadata with distributed ledger technology,″ *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, 2018, pp. 1-6, doi: 10.1109/NOMS.2018.8406310.