アクセストークンを用いた情報交換と制御方式

五味 秀仁 †

† ヤフー株式会社 Yahoo! JAPAN 研究所
107-6211 東京都港区赤坂 9-7-1

hgomi@yahoo-corp.jp

あらまし ネットワーク上のサービス利用の際，利用者は自らの情報の提供を求められることが多い．利用者情報を必要とするサービスに対して既に登録されている利用者情報を送付すれば，利用者の利便性は向上するが，一方で，情報漏えいの危険性を考慮する必要がある．そこで，利用者とその情報の活用者とを利用者情報に関連付けしたアクセストークンを発行し，上記の情報活用者にだけ情報を適切に送付する情報交換及び制御方式を提案する．この方式により，利用者のプライバシーを保護しつつ安全な情報活用を促進できる．

Identity Information Exchange and Control with Access Token

Hidehito Gomi†

†Yahoo! JAPAN Research
9-7-1 Akasaka, Minato-ku, Tokyo 107-6211 Japan

hgomi@yahoo-corp.jp

Abstract Many on-line services require users to provide their own identity information. Although the propagation of users' information to services requiring it improves their convenience, the risk of private information leakage must be considered. An identity information exchange method is proposed for granting access from a service provider presenting an access token that is associated with an appropriate user and the provider for using his/her identity information. This method facilitates secure practical use of identity information while protecting users' privacy.

1 はじめに

ネットワーク上のサービス利用のため，利用者は様々な事業者に対して自らの情報を登録することが多くなっている．購買サービスの場合，住所や氏名などの個人情報を商品の配送先情報として入力することは多い．個々のサービスが個別の事業者によって管理されると，同じ情報を何度も入力することを求められ，不便に感じることは一般的である．

ある事業者に登録されている利用者に関する情報を，それを必要とする他の事業者に安全に送付することができれば，情報入力の煩雑さは軽減され，利用者の利便性は向上するはずである．しかし，秘密性の高い情報の送付は情報漏えいやプライバシーの侵害などの問題を起こす可能性があり，適切なアクセス管理方法は重要な課題である．

そこで本稿では，オンラインサービスの利用や取引において利用者に関する情報を必要とする際に，ある事業者が既に管理している利用者情報を異なる事業者に対して，プライバシーを保護しながら安全に送付する情報交換方式及びアクセス制御方式を提案する．

2　関連研究

SAML [1] は，アイデンティティ管理に関する包括的な仕様群であり，システムの参加主体間の信頼関係と，利用者のアカウント情報の連携を前提として，その属性情報を交換する．本稿では，上記前提条件を緩和し，利用者の判断でより柔軟に情報交換する枠組みを提案する．

また，SAML には，属性情報に関連付けられたチケット（アーティファクト）を発行し，その提示者に対してのみ情報提供を行う情報交換方式がある．本稿では，上記チケットの考え方を継承し，情報活用の範囲を広げると同時に情報制御を強化する．

Kerberos [2] は，通信経路上の安全が保証されていないネットワークで，サーバはクライアントをアクセス制御できる．あるサーバにアクセスしたいクライアントは，認証サーバで認証後，チケット交付サーバからサーバへのアクセスチケットの発行を受け，それをサーバに対して提示してアクセスを許可される．このチケットは，閉じた環境の所定のサーバへのアクセスに限定的に発行されるものである．それに対して本稿では，チケットの役割を拡大し，オープンな環境において，より柔軟な情報活用を目的とし，チケットの耐性を強化する．

梅澤ら [3] は，利用者を認証せず，その個人属性や権限を記載した証明書を用いてアクセス制御する方式を提案した．利用者による選択的情報の開示という点で関連するが，本稿では情報や権限の活用範囲を拡大する目的で，それらの安全な伝搬方式を中心に扱っている点で異なる．

本城ら [4] はプライバシー保護を想定した個人属性認証・アクセス制御システムを提案した．このシステムでは，利用者の認証時に必要最小限の情報を開示するにより，情報漏えいを防止することを目的とした．一方本稿では，認証自体の手続きよりむしろ，個人属性情報の交換とその制御手段に焦点を当てる．

3　システムモデル

本章では，提案システムのモデルと機能概要を説明する．まず，以下の用語を定義する．

利用者 (user) とは本システムの利用者であり，個人，または，組織を表す．利用者に準じ，利用者本人に代わる利用者を特に**代理者**と呼ぶ．

ユーザエージェント (user agent, UA) とは，本システムを利用者が操作する Web ブラウザなどのソフトウェアである．

情報管理者 (data manager, DM) とは，利用者に関する情報（以降，利用者の個人属性情報と呼ぶ）を管理する主体である．利用者を認証できる．

情報活用者 (data consumer, DC) は，利用者の個人属性情報を DM から取得し，その情報を活用したサービスを利用者に提供する．

提案システムでは，DM において既に管理している利用者の個人属性情報を，利用者あるいは利用者が認めた代理者が，DC において適切に活用する．DM と DC は異なるセキュリティドメインに属する．

3.1　システム要件

利用者が DM に管理委託する自らの個人属性情報を DC に送付して活用するため，以下のような要件を満たすシステムの実現を課題とする．

- オープンな環境において，利用者自ら個人属性情報を自らの判断で，適切な DC に柔軟に送付できる．
- プライバシー保護を考慮に入れ，利用者や DM に応じて情報を過多に送付することなく最小限の情報を送付し，漏えいを防止できる．
- 利用者は必要に応じて，適切な代理者に DC のサービスを代理で実行するように指示でき，代理者もその代理実行を要求できる．また，この代理実行に関して，利用者本人による実行の場合と可能な限り等価な設計にする．

3.2　システム概要と機能構成

提案システムにおいて，DM は，利用者の要求に応じて，利用者の個人属性情報を記載し，

電子署名などでその情報を保証する証明書を発行する（証明書の形式は本稿では扱わない）．DC は，DM が発行した証明書を検証し，その結果を利用者に対するサービス提供の認可判断に利用する．DM は，利用者の証明書を，ランダムな文字列（**アクセストークン**，以下 AT と呼ぶ）と関連付けて管理し，配布する．AT は証明書を入手するためのチケットの役割を担い，DM は適切な AT が提示される場合にのみ利用者の証明書を発行する．図 1 において提案システムの機能構成を示す．

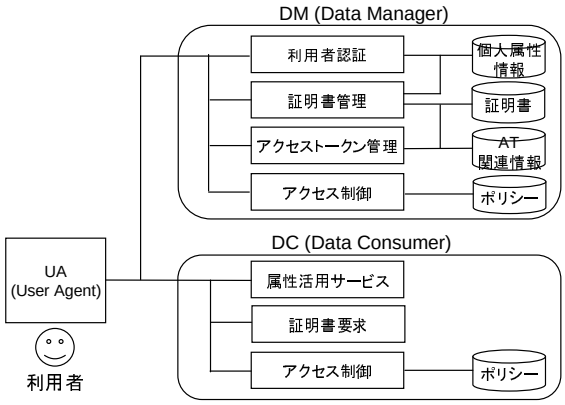

図 1: システム構成図.

DM において,「利用者認証」機能は，利用者にクレデンシャルの提示を要求して認証する．「証明書管理」機能は，利用者の認証結果情報や利用者の個人属性情報をもとにして証明書を発行し管理する.「アクセストークン管理」機能は，上記証明書に関連付ける AT を生成し，関連情報を管理するとともに，証明書の要求時に DC から提示される AT を検証する.「アクセス制御」機能は，証明書や AT の発行などの要求に対して，所定のアクセス制御ポリシーと照合し認可判断を行う．

DC において,「属性活用サービス」は，DM の発行する証明書記載の利用者の属性情報を活用したサービスを利用者に対して提供する.「証明書要求」機能は，DM に対して AT を提示し利用者の証明書を要求して取得する.「アクセス制御」機能は，上記 DM から取得した利用者の証明書などの情報をもとに，アクセス制御ポリシーを参照し，利用者の属性活用サービスへのアクセス要求に対する認可判断を行う．

4 アクセストークンの発行

本章では，AT の生成と配布に関わる処理とその流れを説明する（図 2）．

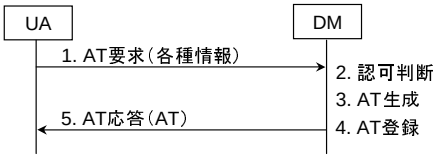

図 2: アクセストークン発行処理.

4.1 アクセストークン交換プロトコル

AT の交換では，利用者が DC に証明書を送付するための AT を DM に要求し，DM が発行する（図 2 ステップ 1）．本プロトコルは，利用者の属性情報を代理者が DC において活用する（権限委譲 [5]）の場合も想定する．表 1 において，権限委譲と，本 AT 要求を発信する利用者（要求者）と，DC において活用する利用者（活用者）が誰かに応じた分類を示す．

表 1: 権限委譲に関する AT 要求形式.

形式	権限委譲	要求者	活用者
(1)	しない	利用者本人	利用者本人
(2)	する	利用者本人	代理者
(3)	する	代理者	代理者

AT 要求には，以下の情報を格納する．

- Recipients: 利用者の属性情報の証明書を受け取る DC の識別子のリストである．
- Attributes: 証明書に記載すべき個人属性情報の種類のリストである．
- OneTime: アクセストークンが一度限りの利用か否かを示すブール値である．
- Delegation: 権限委譲するか否か表すブール値である．`false` は表 1 の形式 (1) を意味する．
- Delegatee: 表 1 の形式 (2) の場合に設定する代理者を示す情報である．DM が代

理者を認証可能であればその識別子，認証可能でなければ DM が代理者に対するアクセス可能な情報（例えばメールアドレス）とする．

- Delegator: 表 1 の形式 (3) の場合に設定する利用者本人の識別子である．

上記の情報を含めた AT 要求を受け取った DM は，対応する証明書発行や権限に関して認可判断を行い（図 2 ステップ 2），4.2 節で後述の方法で AT を生成し（図 2 ステップ 3），4.3 節で後述の方法で AT を登録し（図 2 ステップ 4），UA に返信する（図 2 ステップ 5）．

4.2 アクセストークンの生成方法

利用者の同一の属性情報に関する証明書に関して，DC が DM に必要なアクセス回数を n として，DM は，アクセストークン AT_n を以下のような処理によって生成する．

$$AT_n = \begin{cases} F(K_u||N||DC), & \text{for } n = 1, \\ \mathrm{HMAC}(K_u, N||DC), & \text{for } n > 1. \end{cases}$$

ここで，$F(\cdot)$ は，衝突耐性や一方向性を持つ暗号技術的ハッシュ関数である．$\mathrm{HMAC}(K_u, \cdot)$ は，利用者 u の DM と共有する秘密鍵 K_u と，所定の暗号技術的ハッシュ関数を用いた鍵付き MAC [6] である．N はノンス（乱数）で，DC は DC を一意に示す識別子である．$(str1||str2)$ は，文字列 $str1$ と $str2$ の連結を表す．

通常の MAC 方式は，秘密鍵を共有する二者間で送付される情報を認証するために用いられるが本稿ではこれを応用し，AT を適切な DC や利用者と関連付けて生成し，その正当性を検証する仕組みを提供することによって，情報の不正拡散を防止する．

AT は上記の方法によって生成されたハッシュ値で，DM 以外の主体が，悪意をもって偽造することは困難である．また，この情報は利用者を特定可能な情報は含まれていない匿名化情報であり，悪意を持った主体に開示されても有用な情報はないだけでなく，万が一悪意を持った利用者や DC が AT を入手しても，利用者の証明書の不正入手ができない．

4.3 アクセストークンの管理

DM は生成した AT を，利用者の要求した証明書への参照情報として関連付けて AT 関連テーブルにおいて管理する．また，AT の検証を行う際に利用するため，AT 生成時に用いた情報も同様に AT と関連付けて格納しておく．図 3 は，AT 関連テーブルの一例である．

アクセストークン	利用者識別子	証明書識別子	代理者識別子	情報種別	ノンス
f3l9b4m2n3v8	usr001	crt001	···	利用者鍵、DC（URL）	88434238489

図 3: アクセストークン関連テーブル．

テーブル中の「利用者識別子」,「証明書識別子」,「代理者識別子」は，それぞれ，本 AT 要求の対象となる利用者，本 AT と関連付けられた証明書，権限委譲の場合の代理者の識別子であり，ここでは権限委譲していないことを示している.「情報種別」は該 AT 生成のために用いた情報であり，該利用者の鍵と DC の識別子としてその URL を含んでいる.「ノンス」は該 AT を生成したノンス情報である．

上記のように AT を登録した後，DM は DC からの AT を含めた証明書要求を制御できるように，適切な権限を設定する．

5 証明書の発行

本章では，証明書の発行とそのアクセス制御に関わる処理とその流れを説明する（図 4）．

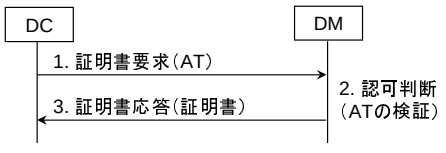

図 4: 証明書発行処理．

5.1 証明書交換プロトコル

DC は DM に対して，UA から受け取った AT を含めた証明書要求を送付し（図 4 ステップ 1），その AT を 5.2 節で後述する方法で検証し（図 4 ステップ 2），その結果を先の証明書要求の認可判断情報として利用し，認可された場合に要

求された証明書を返信する（図 4 ステップ 3）．本プロトコルは，AT の種類に依存せず，その制御は AT を検証することによって行う．

5.2　アクセストークンの検証

DCからの証明書要求を受けたDMは，そのメッセージに含まれる AT を取得して，検証する．

まず，受け取った AT（要求 AT，AT_{R} と呼ぶ）が，AT 関連テーブルの情報を参照して，その存在を調べる．存在する場合，AT_{R} をキーにして得られる各種関連付けられた情報を元にして新たに AT（検証 AT，AT_{V}）を生成する．AT_{V} の生成に必要な情報は，必要に応じて，本証明書を要求した DC と UA から取得する．例えば，図 3 の例では，利用者鍵情報に関しては DM が管理する利用者「usr001」の属性情報から取得し，DC 情報は証明書要求している主体の URL を取得する．これらを入力値として，4.2 節の方法によって AT_{V} を生成し，$AT_{\mathrm{R}} = AT_{\mathrm{V}}$ であれば，要求 AT は適切であると判定する．

6　応用例

本章では，前章で述べた提案システムを 2 つのユースケースに適用する．

図 5 は，ビジネス上の信頼関係のない DM と DC1 において，DM に既にアカウントを保有する利用者 A が，その属性情報を活用して DC1 に新規アカウントを登録する場合を示す．

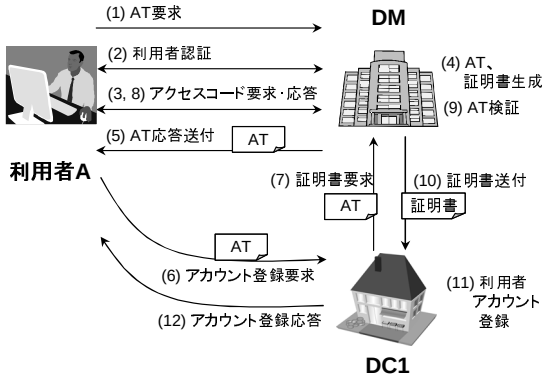

図 5: アカウント登録．

(1) DC1 に送付すべき属性情報を指定し，AT 要求を DM に送付する．(2) DM は A を認証し，(3) A の秘密鍵として，アクセスコードの入力を要求し，A は応答する．(4) DM は，先のアクセスコードを利用して，AT と対応する証明書を生成し，(5) 生成した AT を A に発行する．次に，A は，DC1 にアクセスして，(6) 先の AT を含めたアカウント登録要求を行う．(7) DC1 は該 AT を含む証明書要求を DM に対して送付する．(8) DM は該 AT が A に関連していることを確認し，A に電子メールにより，該 AT を検証するためにアクセスコードの入力を A に促す通知を行い，A は DM にアクセスし入力する．(9) DM は，上記アクセスコードをもとにして，該 AT を検証する．(10) DM は該 AT を検証できれば，関連付けられた証明書を DC1 に送付し，(11) DC1 は受け取った証明書を検証した上で，新規にアカウントを生成，先の証明書の情報を登録する．最後に，(12) DC1 は A にアカウント登録が完了した旨を通知する．

以上のように，利用者は，DM とビジネス上の信頼関係が構築されていない DC1 に対しても，利用者の判断のもとで属性情報を送付できる．

図 6 は，利用者 A が図 5 の状況から，DM に対して代理者 B に DC2 を通じて権限委譲するように権限を設定し，B が DC2 から A の属性情報に代理アクセスする一例を示す．

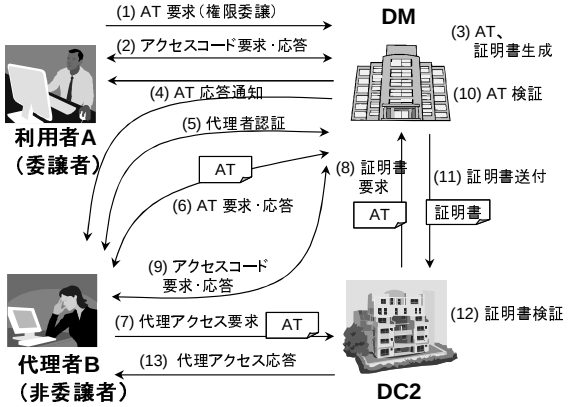

図 6: 権限委譲による代理アクセス．

(1) 利用者 A は，DM に既にアカウントを持つ利用者 B に対する権限委譲のための AT 生成を要求する．(2) DM は A にアクセスコードを要求し，A は入力する．(3) DM は先のアクセスコードを使って，利用者 B の秘密鍵を生成し，AT と証明書を生成する．(4) DM は A と B に

AT が生成したことを通知する．(5) 先の通知を受け，B は DM にアクセスして認証される．(6) B は DM に AT を要求し，取得する．(7) B は，先の AT を提示して DC2 に代理アクセス要求する．(8) DC2 は該 AT を添付し，DM に対して証明書要求を行う．(9) DM は，電子メールで B にアクセスコードを入力するように通知し，B は DM に保管されたコードを入力する．(10) DM は AT を検証し，(11) 対応する証明書を送付する．(12) DC2 は証明書を検証し，(13) B の代理アクセスによるサービスを提供する．

以上のように，図 5 と同様のシステム設計とプロトコルによって，権限委譲の場合に対するアクセス制御も実現できる．

7 考察

AT は偽造に対する耐性があり，悪意を持つ利用者や DC の AT 偽造による情報の不正入手は困難である．提案手法では HMAC を応用しており，同一の AT を再利用する場合には伸長攻撃 (extension attack) に対して耐性を持つ．

AT には利用者や DC の真正性の検証機能があり，悪意を持つ利用者や DC の属性情報の不正入手は困難である．本稿では割愛したが，利用者の UA 固有の識別子も AT と関連付けることで，さらに不正利用への耐性を強化できる．

AT は匿名性がある上，AT の有効時間を短く設定することで AT と関連付けた利用者のトラッキングは困難となり，プライバシー保護に有効である．また，AT は証明書と比較して短い文字列であるので，送付可能な文字数に制限がある UA においても容易に送付できる．

AT は所定の権限に対応している．上記の真正性の保証や匿名性の性質から，AT はセキュアな通信路ではなくても配布が容易で，オープンな環境において，限定的な権限をきめ細かく交付でき，情報活用の範囲を拡大できる．

オープンな環境における代理者の認証や鍵情報の伝搬方法は課題である．図 6 のユースケースで，DM が既に代理者の認証方法を持っていない場合には，別途代理者の本人確認を行った上で秘密鍵を生成するか，あるいは，安全に鍵情報を伝搬する方式が必要である．

本稿では，AT の応用領域を特に個人属性情報サービスのアクセス制御としたが，広く汎用的なサービスのアクセス制御手法に適用できる．

8 おわりに

本稿ではアクセストークンを用いたアクセス制御方式を提案し，本技術により個人属性情報の漏えいを防止しつつ活用を促進できることを示した．今後，本技術を応用し，汎用的なサービスに対するアクセス制御の研究を進める．

参考文献

[1] Cantor, S., Kemp, J., Philpott, R. and Maler, E.: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0 (2005).

[2] Steiner, J., Neuman, C. and Schiller, J.: Kerberos: An Authentication Service for Open Network Systems, in *Proceedings of Usenix Conference*, pp. 191–202 (1988).

[3] 梅澤健太郎, 齋藤孝道, 奥乃博：プライバシーを重視したアクセス制御機構の提案, 情報処理学会論文誌, Vol. 42, No. 8, pp. 2067–2076 (2001).

[4] 本城信輔, 洲崎誠一, 齋藤司, 三浦信治：プライバシに配慮した WWW における個人属性認証・アクセス制御システム, 情報処理学会論文誌, Vol. 43, No. 8, pp. 2573–2586 (2002).

[5] Gomi, H., Hatakeyama, M., Hosono, S. and Fujita, S.: A Delegation Framework for Federated Identity Management, in *Proceedings of the 2005 ACM Workshop on Digital Identity Management (DIM'05)*, pp. 94–103 (2005).

[6] Krawczyk, H., Bellare, M. and Canetti, R.: HMAC: Keyed-Hashing for Message Authentication (1997), RFC 2104.