複数サーバの連携によるプライバシー重視のサービス提供モデルの提案

小瀬木浩昭† 武田正之†
東京理科大学大学院 理工学研究科 情報科学専攻

現在インターネットにおいてサーバ／クライアント形態のサービスは多いが, 個人情報の保護に関しては必ずしも十分ではない. 事業者が定める「個人情報保護規約」も遵守されていることをユーザが検証する手段が無いのが実情であり, 個人を識別する「ID」と登録した際の「個人情報」と「サービスの利用情報」の3種類の情報がひとつの母体に集中することはプライバシー上の大きな問題である. 本提案モデルは, サービスを複数の主体が連携・協調して提供することにより, 各々の構成主体に集約される個人情報を制限し, それらの情報の統合を防止することが目的である. 本稿ではプライバシー重視のサービス提供モデルの提案とその応用について述べる.

1. はじめに

匿名はプライバシー重視の究極のモデルであるが, 個人を特定する ID が無いと困る場合がある. 電子メールや Instant Message (IM)☆等コミュニケーションサービスの実現においては, ID に対する匿名性よりもむしろ Server とClient 間でやり取りする情報, Client の ID と関連して Server が保持する情報がプライバシー上問題となる場合が考えられる. これまで暗号基盤に基づいたセキュリティ確保によるプライバシー保護の提案がいくつかなされてきたが, 電子メールを代表に多くのコミュニケーションツールにおいては, その導入の煩雑さ, 互換性, 他者間暗号化通信で生じる問題, 通信のボトルネックになる等の理由で平文がインターネットを流れているのが現状である.

2. 本提案モデル

2.1. ネットワークモデル

本モデルは, サーバ (Server, S), 権限管理主体 (Authority Manager, AM), クライアント (Client, C) の3つの主体から構成されるネットワークモデルを想定する:

Server(S) :あるサービスの提供主体. AM に権限証明書配布権 ($Cert_{Au}AM_S$) を委譲し, Client が提出した権限証明書 ($Cert_{Au}C_{AM\leftarrow S}$) によりサービス利用の制御を行う.

Authority Manager (AM) :Client への権限証明書発行主体. Server からの委任を受け, Server の代理として Client に権限証明書証明書 ($Cert_{Au}C_{AM\leftarrow S}$) を発行する.

Client(C) :サービスを享受する主体. Authority Manager から権限証明書 ($Cert_{Au}C_{AM\leftarrow S}$) を受け取り, その証明書を Server に提出することによりサービスを享受する主体.

なお, 権限証明書については SPKI 権限証明書[2][3]の利用を想定している. SPKI 権限証明書は, それ自身に ID 情報を含んでいない為, 権限の発行主体と権限の行使先の分離など, プライバシーに対する柔軟な配慮が可能であるからである. また, 証明書には有効期限の設定も可能である.

2.2. 本提案モデル

本提案モデルは, 提供するすべてのサービスをひとつの主体で管理運営するのではなく, 複数のサービス提供主体が連携・協調してひとつの有益なサービスを提供する. 以下, (1)Client がサービスを利用するまでの流れ, (2)連携・協調によるサービス提供 の順に解説する.

(1) Client がサービスを利用するまでの流れ 図 1)

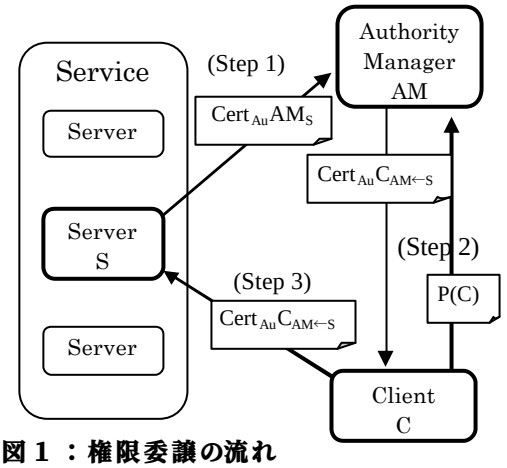

図 1 ：権限委譲の流れ

Step1 :サービス提供主体 (Server, S) は権限管理主体 (Authority Manager, AM) に対し, S の利用権限を配布する権限を持つ権限証明書 (利用権限配布権証明書) $Cert_{Au}AM_S$ を予め提供しておく.

Step2 :AM は Client から C の公開鍵 P(C)の提供を受け, Server の利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ を Client へ発行する.

Step3 :Client は AM から得た利用権限証明書を Server に提示し, Server が提供するサービスを任意に利用する.

Privacy-Enhanced Cooperative Service Model
by Hiroaki Ozeki, Masayuki Takeda
†Graduate School of Sciences and Engineering,
Tokyo University of Science
☆Instant Message インターネットに接続している個人同士が, リアルタイムに交換するメッセージ. あるいはそれを実現するソフトウエア.

(2) 連携・協調によるサービス提供　図 2)

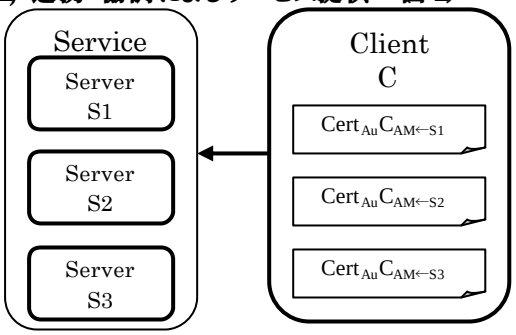

図 2 ：複数サーバによるサービスの連携

ここで, **(i) 同等の機能を持つ Server が複数存在する場合**を想定する. すると, Client はあらかじめ AM から利用したい複数の Server の利用権限証明書を得ておくことで, 利用する Server を任意に選択することが可能となる. 例えば, チャット機能を利用したい場合, 毎回異なる Server に切り替えてチャットを行うことも可能である.

次に, **(ii) 異なる機能を持つ Server が相互に補完し合いながらひとつの有益なサービスを構成する場合**を想定する. すると, Client はそれぞれの Server に対して利用権限証明書を提示することで, 各 Server の提供するサービスを同時に利用し, Client 内でそれらのサービスを結合することにより, ひとつの有益なサービスを利用することが可能になる. 例えば, コミュニケーション相手の状態を表すプレゼンス情報を通知するサービス, ホワイトボード共有サービス, ビデオチャットサービスを組み合わせて利用することで, 電子会議が可能となる.

複数の Server が連携・協調してひとつの大きなサービスを提供することにより, 各 Server が保持する Client に関する情報が限定され, プライバシーに対しての配慮が可能となる. **(i)**では, 毎回異なる Server を利用することで Server に Client のサービス利用状況を把握される危険性を防止できる. **(ii)**では, 複数のサービスをひとつの Server で利用することにより, Server がそれらのサービスの利用状況を結合して Client のプライバシーにかかわる情報を得る危険性を防ぐことができる.

現在, ポータルサイトや統合サービスサイトが存在するが, ユーザの行動情報が詳細に特定の主体に集中しているのが現状である. それらのサイトでは「個人情報保護規約」を定め安全性を謳っているものもあるが, ユーザは規約が遵守されているか確認する術を持たないのが実情である.

本提案モデルは, 権限管理主体 (AM) を設けることで, 各々のサービス提供主体 (S) の品質について一定の保証を持たせることが可能である. (AM が S からのサービス利用権限配布権を受けとる際に, 同時に S に関する情報を得ることで S を選定することが可能であるから). また, 複数の S と AM との連携・協調によりサービスを提供することで, 特定の主体にプライバシー情報 (ユーザの行動情報) が集中することを防ぐことができる. また Client (C) 以外のどの構成主体も, 単独では(ある C に関する全ての情報を得る権限を持たない (よって得ることは出来ない) 特徴がある. さらに, AM は単一に限定されなく, Server の場合と同様に, Client は複数の AM の中から任意のいくつかの AM を選択して利用することが可能である.

3. 考察

本提案モデルのアプローチは既存の暗号基盤を利用したそれとは根本的に異なり, また従来の手法と併用することでより強力にユーザのプライバシーを保護することが可能となる. セキュリティを保つ為に平文を解読困難な形式に暗号化するように, プライバシーを保護する為にユーザの個人情報の取得・結合を困難にする. 本モデルは各々のサービス提供主体が取得・保持できる個人情報をあらかじめ制限している.

プライバシーを重視するアプローチとして[1]等があるが, それらの既存の提案方式と本提案モデルとの違いのひとつに, 「全面的に信頼すべき主体」の必要を前提としないことが挙げられる. 本提案モデルにおいて AM や各構成 Server は, 仮にどれかひとつが悪意を持った, あるいは実装上の脆弱性を突かれハッキングを受けた場合でも, 2.2 節の仕組みにより, 影響をその主体の権限により提供される機能の範囲内に留めることが可能である. さらに, 複数の主体の連携・協調によるサービスの提供形態は, 負荷分散, 耐障害性が上がり, 同時に近年問題となっている DoS 攻撃への耐性も上がる. さらに, 利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ は C が S を利用した利用証明書の意味も持ち, これを証拠として, AM に対しサービス提供料を請求するようなビジネスモデルの実現も可能である.

また, 本提案モデルは特定のサービス・アーキテクチャを前提としない, 汎用的なサービス提供モデルである. 例えばピア・ツー・ピアで提供されるサービスへも本モデルは適用可能であろう. 本モデルで Client と記述したサービス享受主体も, それがさらに別の Client へサービスを二次提供するような拡張も可能である等, 本提案モデルの適用範囲は広い.

4. まとめ

本稿では, 各々が独立した複数のサービス提供主体の協調動作によりサービスを提供することで, ユーザのプライバシーを配慮したサービス提供モデルを提案した. 今後は, 本提案モデルを電子メールや IM 等のコミュニケーションシステムに実際に適用し, その有効性を評価したい.

参考文献

[1] 梅澤健太郎, 齋藤孝道, 奥乃 博 :X.509 証明書と SSL を用いた簡潔な匿名アクセス制御方式, 情報処理学会第 62 回全国大会, 2S-04, Mar. 2001.

[2] C. Ellison: SPKI Requirements, RFC2692, Sep. 1999.

[3] C. Ellison, et al.: SPKI Certificate Theory, RFC2693, May 1999