個人情報の分散協調保護機構の提案と Instant Message Web サービスへの実装

小瀬木 浩昭† 小林 直記‡ 真柄 喬史† 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 ‡東京理科大学 理工学部 情報科学科

1. はじめに

従来からある C/S 型のシステムは，特定の主体に情報が集中し，管理者が連続的かつ統合された情報を容易に取得できるという点でプライバシー上の危険性を潜在的に抱えている．これまで我々はネットワーク上の複数の主体の分散協調によるプライバシー重視のサービス提供に関して研究を行ってきた[1][2]．その本質は，**(i)** ユーザを識別する「ID」と，それと結びつく「**静的情報**（氏名など固定のもの）」と「**動的情報**（サービスの利用情報，コミュニケーション情報など動的なもの）」の分離，**(ii)** 動的な情報の分離・分散，**(iii)** SPKI[3]の活用による各々の構成主体の他の主体への成りすましの防止，にある．独立した複数の主体の分散協調によりサービスを提供し，個々の主体に集約される情報を制限することで，各主体は利用者毎の詳細な情報の取得が困難になり，利用者のプライバシーに配慮したサービス運営が可能となる．また他の主体への成りすましを防止することで，各構成主体の独立と安全を保つことができる．本稿では，提案モデルの適用例として Web サービス上の Instant Message サービスへの実装を紹介する．

2. 提案モデルの概要

構成： 本モデル（**図1**）は，サービスを提供するサーバ(Server, *S*)，サービスを利用するクライアント(Client, *C*)，*S* の委任を受けて *C* に *S* の利用権限を付与する権限管理主体(Authority Manager, *AM*) から構成される．この3主体は，実社会の，映画館（*S*），チケットの売店（*AM*），客（*C*）に例えることが出来る．映画館は客がいつ，どの映画を観たか知っているが，誰が観たかを知らない．チケットの売店は誰にチケットを売ったかは知っているが，チケットがどのように利用されたかを知らない．このような3者の関係をサービスの関係としてネットワーク上で実現する．

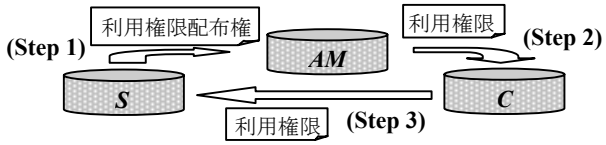

図1 本モデルにおける権限委譲の流れ

権限委譲とサービスの利用： 図1と対応させて解説する．**(Step 1)** *S* は，*AM* に対し「*S* のサービスを利用する権限を発行する権限」を与える**利用権限配布権証明書**を発行する．**(Step 2)** *AM* は，（利用権限配布権証明書に基づき）*C* に対して「*S* のサービスを利用する権限」を与える**利用権限証明書**を発行する．**(Step 3)** *C* は，*S* に対して利用権限証明書を提示して *S* のサービスを利用する．各証明書は，SPKI 権限証明書を拡張して実現した．詳細については[2]を参照されたい．

3. Web サービス上の Instant Message への実装

本実装では，提案モデルに基づき，各機能を複数のサーバが分散協調して提供することにより，Instant Message サービスを形成する．

処理系： 実装言語として Java2 SDK，SOAP エンジンとして Apache AXIS，Servlet コンテナとして Apache Tomcat を用いて，SOAP1.1，WSDL1.1 準拠の Web サービスとして実装を行った[4]．また各主体間の通信には SOAP/HTTP を採用した．

実装の構成（図2）： *PS*（Presence Server）はプレゼンス情報（現在の状態情報．「仕事中」「多忙」「離席中」等．）の通知機能を提供するサーバ群である．*MS*（Message Send Server）と *MR*（Message Receive Server）はメッセージ交換の機能を提供する．*REG*（Registry Server）は，*C* が利用するサーバのアドレスリストを管理する．

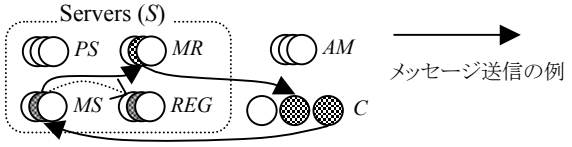

図2 Instant Message の構成とメッセージ送受信の流れ

実行例： **図3**は C_1 と C_2 が何件かのメッセージを送り合い会話を交わした場面のスクリーンショットである．左上は C_1 の GUI である．その他は PS_1，MS_1，MS_2 がメッセージの送信について把握できた情報を表示しているウインドウである．

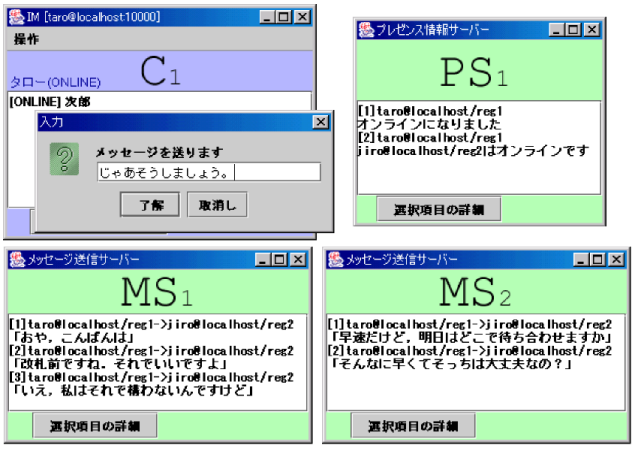

図3 C_1 と C_2 の会話

表1 各主体が把握できる *C* に関する情報

	PS	*MR*	*MS*	*REG*	*AM*	従来
コンタクトリスト	●	⊗	⊗	○	○	●
プレゼンス情報	●	⊙	⊙	⊙	○	●
メッセージの存在	○	⊗	⊙	⊗	○	●
会話の内容	○	⊗	⊙	○	○	●
氏名など	○	○	○	○	●	●

○ 全く分からない ⊙ ほとんど分からない
⊗ 一部分かる ● 全て分かる

4. 考察

表1は，Instant Message を利用する *C* の情報がどの主体に把握されるかをまとめたものである．比較のために単一の主体が全てのサービスを提供する方式を「従来」として掲載してある．表より静的情報と動的情報の分離に成功していることがわかる．動的情報については，プレゼンス情報の通知に関わる情報とメッセージ交換に関わる情報を両方とも把握できる主体が存在しない．特にメッセージ交換については何れの主体も意味のある情報を収集できない．各主体は提供する機能に必要ない情報を扱わないよう構成してあるが，メッセージを受信できるならばオンラインである等，間接的に情報を推測できる場合もあるため，それらの項目は灰色で区別してある．このように，本実装は単一のサーバでサービスを提供する方式よりもプライバシーの保護という観点から優れているといえる．

5. まとめ

本稿では，提案モデルを Instant Message に適用し実装することを通して，モデルが実現可能であり，実際にプライバシー保護に役立つことを示した．今後我々は，実際のサービスで想定されるような大規模な運用に耐え得るかの検討，モデルの他のサービスへの適用を行うなど，本研究の有用性を強化するための課題に取り組んでいきたい．

参考文献

[1] 小瀬木浩昭，武田正之：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，情報処理学会第 65 回全国大会, 5X-5 (Mar. 2003).
[2] 小瀬木浩昭，小林直記，真柄喬史，滝本宗宏，武田正之：個人情報の分散協調保護機構の Web サービスへの適用とその実現，第2回情報科学技術フォーラム(FIT2003), LM-015，情報技術レターズ, pp.357-359 (Sep. 2003).
[3] C. Ellison: SPKI Requirements, RFC2692 (Sep. 1999).
[4] http://java.sun.com ; http://jakarta.apache.org