分散協調情報保護機構の Instant Message Web サービスへの実装

Implementing Distributed and Cooperative Information Protection to Instant Message Web Services

真柄 喬史† 小瀬木 浩昭† 武田 正之‡
Takafumi Magara Hiroaki Ozeki Masayuki Takeda

1. はじめに

一般的な C/S 型のシステムは，特定の主体に情報が集中し，主体の管理者が連続・結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問題や情報漏えい等の危険性を潜在的に抱えている．我々は，複数の独立した主体が分散・協調してサービスを提供することで情報の集中を防ぐモデルを提案している[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)** 権限証明書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，このモデルの Instant Message Web サービスへの実装を紹介し， 単一の主体だけで提供する場合よりもプライバシー上の問題が改善されることを示す．また，提案モデルの効果を視覚的に示す GUI を実装したので，それについて解説する．

2. 提案モデルの概要

2.1. 権限による認証機構

構成： 提案モデル（**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．

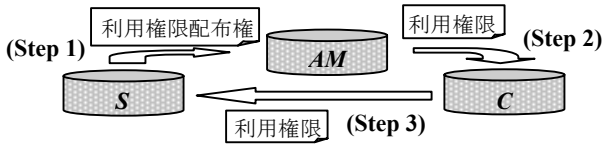

図1 本モデルにおける権限委譲の流れ

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[3]を拡張して実現した．詳細については[1]を参照されたい．

†東京理科大学大学院 理工学研究科 情報科学専攻,
Graduate School of Science and Technology,
Tokyo University of Science
‡東京理科大学 理工学部 情報科学科,
Dept. of Information Sciences, Tokyo University of Science

2.2. サーバ分割

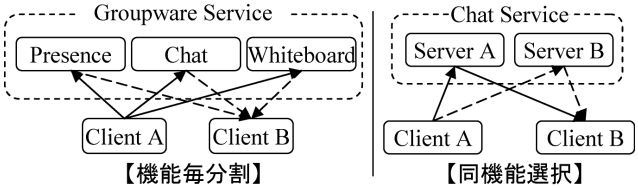

図2 連携・協調によるサービス提供

(i)【機能毎分割】

複雑なサービスは，一般に複数の機能の組み合わせで構成されている．サービスを分析し，他の機能に対して独立性を持つ機能単位にサービスの分割を行なう．分割したサービス毎に，異なる主体によりサービス提供を行なえるよう再構成する．例えば，ある「グループウェア」サービスを分析し，「プレゼンス情報通知」，「チャット」，「黒板」の各サービスにより構成されていたならば，それらを別々の機能として異なる主体により構成し，サービス提供を行なう．

(ii)【同機能選択】

機能毎分割により分割を行なった機能単位のうち，「チャット」や「文書変換」のように，前回の利用状態に依存しないサービスは，同機能のサービスを複数設置し，利用者が選択して利用する構成ができる．例えば，チャットサービスを提供する場合，利用者がメッセージ毎に利用する *S* を変更できるような構成を実現できる．

3. Instant Message Web サービスへの実装

3.1. 実装システムの概要

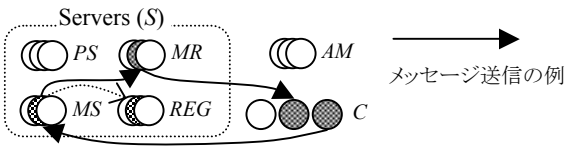

図3 Instant Message の構成とメッセージ送受信の流れ

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3）： *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．各 *S* を利用するための利用権限証明書の配布は済んでいるとし，*AM* については図3では省略する．

3.2. 実行例

3.2.1. デモンストレーション画面

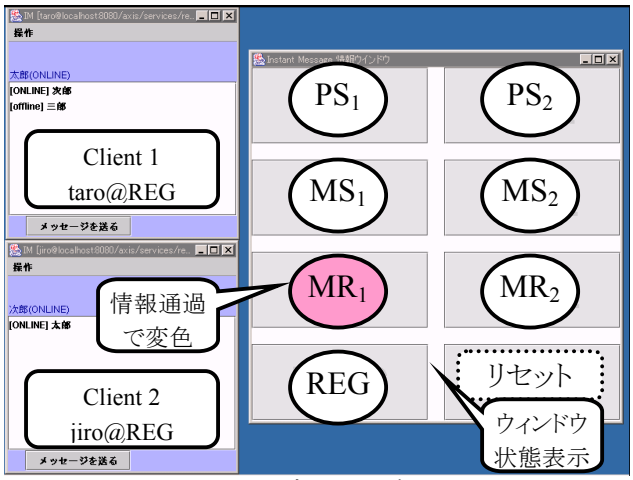

図4　デモ画面の概要

図5　プレゼンス情報の変更 / メッセージ送受信 の様子

図4, 図5は，Instant Message への実装のデモンストレーション画面である．左上が Client1(taro@REG)，左下が Client2(jiro@REG)の GUI で，右の大きなウィンドウは，各サーバへの情報の流れを表示する．Instant Message の機能を利用すると，情報が通過したサーバは変色して示される．図5 左がプレゼンス情報の変更の際の様子．右が Client1 と Client2 でメッセージを送受信した際の様子である．

3.2.2. チャット

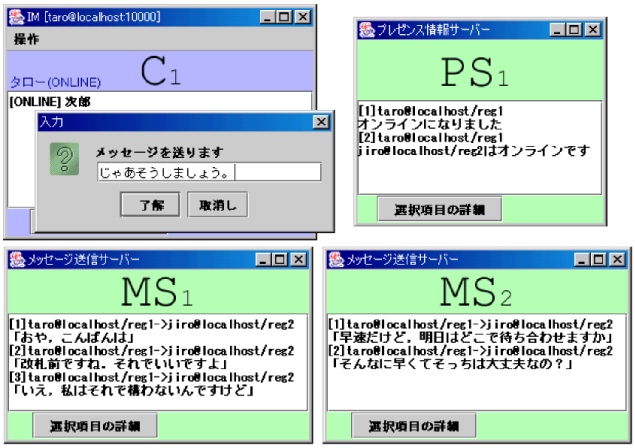

図6　C_1 と C_2 の会話において各主体が把握できる情報

図6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．PS にはプレゼンス情報変更の様子が，MS にはメッセージ情報が流れているが，MS_1, MS_2 は互いに会話の断片情報しか把握しておらず，会話内容の全容を知ることが出来ていないことがわかる．

4. 考察

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

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．また，モデル適用による効果を視覚的に示す GUI を添えることで，モデルの有用性や効果について視覚的に理解できる環境について紹介した．

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，定量的な評価，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，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，FIT2003，LM-15，情報技術レターズ，pp.357-359 (Sep. 2003).

[2] 小瀬木浩昭，小林直記，真柄喬史，武田正之：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，インターネットコンファレンス(IC2003)，p.121 (Oct. 2003).

[3] C. Ellison: SPKI Requirements, RFC2692 (Sep. 1999).

[4] http://java.sun.com ; http://jakarta.apache.org