個人情報の分散協調保護機構の提案と Web サービス上の Instant Message への適用

小瀬木 浩昭[†] 真柄 喬史[†] 武田正之[††]

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上の問題や情報漏れなどの危険性を潜在的にかかえている．また，会話サービスや文書変換サービスなど，サーバと送受信する情報自体をサーバから秘匿することは困難だが，プライバシへの配慮や情報漏えいを防止したい要求がある．本稿では，1 つのサービスを複数の主体が連携協調して提供し，個々のサーバに最小限の情報保持を可能とすることで，各構成主体に集約される情報を制限し，情報統合の未然防止を可能とするモデルを提案する．提案モデルの適用例として，Instant Message システムへの適用と，その Web サービス技術を用いた実装を紹介し，提案手法の実現例を示すとともに，その有効性について考察する．

Privacy Enhanced Distributed and Cooperative Mechanism

Hiroaki Ozeki,[†] Takafumi Magara[†] and Masayuki Takeda[††]

The authors consider that concentrating “user id”, “personal information” and “use information of services” on one service providing body has problems for privacy. This paper proposes a *privacy enhanced service model* on the Internet. We will propose privacy enhanced service mechanism where services are jointly and cooperatively provided, the personal information on each composition of the services are limited, and inappropriate integration of the information can be prevented. As a result, this model makes it difficult to trace users' behavior and enables service administration to give priority to privacy. This paper shows the implementation of our model based on public key infrastructure (PKI) and application to *Instant Message on Web Services*. This application also shows the effectiveness of the proposed privacy enhanced mechanism.

1. はじめに

C/S（Client/Server）型で提供されるサービスにおいて，会話サービスや文書変換サービスなど，サーバと送受信する情報自体をサーバから秘匿することは困難だが，プライバシへの配慮や情報漏えいを防止したい要求がある．特にチャットや電子メールなどの会話サービスにおいては，利用者同士の会話情報をどのように保護するかが重要である．本稿では，必要最小限の機能と情報を扱う複数のサーバの集合によりサービスを構成することで，各サーバに保持される情報を最小限にとどめ，利用者が利用サーバの選択権を持つモデルを提案する．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重視のサービス提供に関して研究を行ってきた[1)~3)]．本稿では，提案モデルの詳細について述べてから，提案モデルの適用例として Instant Message サービスへの適用とその Web サービス技術を用いた実装を紹介し，提案モデルの実現を示すとともに，その有効性について考察する．以下，2 章で 3 章以降の議論への準備を行う．3 章で本提案モデルについて述べ，4 章で提案モデルを Instant Message へ適用し，Web サービス技術を用いた実装を紹介する．5 章では提案モデルを様々な側面から考察する．6 章で関連研究との比較を行い，7 章で課題について述べ，8 章で本稿をまとめる．

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

2. 準備

2.1 表記方法

本稿において，MD5 などのハッシュ関数によるデータ A のハッシュ値を $H(A)$，データ B とデータ C の組 (B,C) のリスト $\{(B,C)\}$ を略記して $\{B,C\}$

と表記する．主体 X の公開鍵を $P(X)$ で，$P(X)$ に対応する主体 X の秘密鍵を $S(X)$ で表す．証明書の内容を $\langle , \rangle$ で括って表現し，その証明書に $S(X)$ で電子署名が施されていることを，$\langle ... \rangle_{S(X)}$ と表現する．主体 Y の ID を $ID(Y)$，Y のネットワーク上での識別子を $URI(Y)$，主体 X から主体 Y に与えられた権限を $Au(Y)$，有効期限を $V(Y)$ と表記する．なお，便宜上，主体 X における，Y の識別子，鍵などを，$ID(Y)_X$，$URI(Y)_X$，$P(Y)_X$，$S(Y)_X$ のように添え字を付して表現することがある．

2.2 権限証明書

本稿では，RFC2692，2693で規定されている**SPKI権限証明書**を用いる[4),5)]．

主体 X が，主体 Y に対して権限 $Au(Y)$ を有効期限 $V(Y)$ の間保証し，権限委譲の可否が D（ブール値．true または false.）で示される権限証明書を次のように定義し，$Cert_{Au}Y_X$ と表記する：

$$Cert_{Au}Y_X = \langle P(X), P(Y), D, Au(Y), V(Y) \rangle_{S(X)}$$

権限認証：権限証明書を利用した権限認証の手順は次のとおりである．**(i)** クライアント Y は，サーバ X に権限証明書 $Cert_{Au}Y_X$ を提出する．**(ii)** X は，Y がその証明書に含まれる公開鍵 $P(Y)$ に対応する秘密鍵 $S(Y)$ を保持することを確認する．**(iii)** X は，(ii) の処理が成功した場合に，Y が X に対して証明書に記された権限 $Au(Y)$ を有効期限 $V(Y)$ の間持つと判断する．

2.3 権限証明書を用いた権限委譲の実現

提案モデルでは SPKI 権限証明書を応用し，3 主体間での権限委譲を次のように実現した（**図 1**）．

主体 X から主体 Y へ**権限証明書配布権** $Cert_{Au}Y_X = \langle P(X), P(Y), true, Au(Y), V(Y) \rangle_{S(X)}$ が与えられ，さらに主体 Y が主体 Z に証明書の二次配布を行った場合，その**利用権限証明書**を $Cert_{Au}Z_{Y \leftarrow X}$ と表記する．

$$Cert_{Au}Z_{Y \leftarrow X} = \langle H(Cert_{Au}Y_X), Cert_{Au}Z_Y \rangle$$

$$Cert_{Au}Z_Y = \langle P(Y), P(Z), false, Au(Z), V(Z) \rangle_{S(Y)}$$

利用権限証明書の正当性の検証：Z が X へ $Cert_{Au}Z_{Y \leftarrow X}$ を提示すると，X は **(i)** $H(Cert_{Au}Y_X)$ と，X に保管してある $Cert_{Au}Y_X$ から得られるハッシュ値 $H(Cert_{Au}Y_X)$ の一致により $Cert_{Au}Y_X$ の正当性を検証し，**(ii)** $Cert_{Au}Z_Y$ により，Y から Z が利用権限証明書の発行を受けたことの正当性を確認する．(i)，(ii) より，$Cert_{Au}Z_{Y \leftarrow X}$ は X から Y を通じて Z へ発行された正当な利用権限証明書であることが証明される☆．

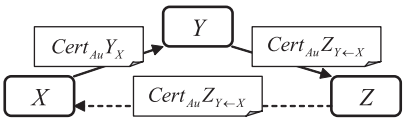

図 1 権限委譲
Fig. 1 Delegation of authority.

2.3.1 既存の提案手法との差異

文献 6) において，SPKI 権限証明書を用いた権限委譲の実現方法が提案されている．上述の論文では，本稿における $Cert_{Au}Z_{Y \leftarrow X}$ の機能を $\langle Cert_{Au}Y_X, Cert_{Au}Z_Y \rangle$ で実現しており，本稿では，同様の機能を $\langle \boldsymbol{H}(\boldsymbol{Cert}_{Au}\boldsymbol{Y}_X), Cert_{Au}Z_Y \rangle$ で実現している違いがある．

Z に渡す証明書 $Cert_{Au}Z_{Y \leftarrow X}$ に含めるのは，$Cert_{Au}Y_X$ そのものではなく，そのハッシュ値 $H(Cert_{Au}Y_X)$ であるべきである．$Cert_{Au}Y_X$ の中には，X が Y に保障する「証明の内容」が含まれているが，Z がその内容を知る必要はない．よって，必要以上の情報が含まれる証明書本体 $Cert_{Au}Y_X$ を直接 Z に渡すべきではない．

3. 本提案モデル

3.1 認証モデル

提案モデルは，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．

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，C が提出した利用権限証明書 $Cert_{Au}C_{AM \leftarrow S}$ によりサービス利用の制御を行う．

Authority Manager（AM）：C への利用権限証明書発行主体．S からの，権限証明書配布権の委譲を受け，S の代理として C に利用権限証明書を発行する．

Client（C）：サービスを享受する主体．AM から利用権限証明書を受け取り，その証明書を S に提示することによりサービスを享受する．

この 3 主体は，実社会の，映画館（S），チケットの売店（AM），客（C）に例えることができる．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．映画館は観覧券の所持を認証し，客がいつ，どの映画を観たか把握できるが，誰が観たか

☆ なお，権限証明書配布権より生成された利用権限証明書の権限，期限は，生成元の権限証明書配布権の権限，期限の範囲内でなければならない．仮に権限の範囲を逸脱していても，X が $Cert_{Au}Y_X$ との整合性を確認することで検出できる．

を知らない．チケットの売店は誰にチケットを販売したかを把握するが，チケットがどのように利用されたかを知らない．権限証明書配布権はチケットの発行権，利用権限証明書はチケットに対応する．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．

3.2 システムの前提

最初の段階で，S，AM，C は互いに独立しているものとする．以降の独立性の保証は，権限証明書配布権，利用権限証明書に含まれる公開鍵に基づいた，成り済まし検出機構により実現する．また，S は複数存在し，各々のサービス提供で得られた C の情報の管理に責任を持つ．ただし，後述する「同機能選択」により選択利用される S については，必ずしもすべての S の善意を必要としないが，全体の機能を実現するうえで支障のない程度の品質でサービスを提供するものとする．権限管理主体 AM は保管する C の静的情報を善意に管理するものとする．

3.3 サービス利用の流れ

提案モデルにおけるサービス利用の流れについて解説する．以下 Client がサービスを利用するまでの流れ，連携・協調によるサービス提供の順に解説する．

(1) **サービスを利用するまでの流れ（図 2）**

Step1：S は AM に権限証明書配布権 $Cert_{Au}AM_S$ をあらかじめ提供しておく．

Step2：AM は既存の方法で C を認証した後，C から S の利用権限証明書を得るための公開鍵 $P(C)_S$ の提出を受け，S の利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ を C に対して発行する．

Step3：C は利用権限証明書を S に提示することで，S は C を権限認証し，C は S の提供するサービスを利用する．

(2) **連携・協調によるサービス提供（図 3）**

(i)【機能毎分割】複雑なサービスは，一般的に複数の機能の組合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う．分割したサービスごとに，異なる主体によりサービス提供を行えるよう再構成する．たとえば，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」「音声通信」「映像伝達」「黒板」「ファイル共有」「電子メール」「電子掲示板」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，サービス提供を行う．

(ii)【同機能選択】機能毎分割により分割を行った機能単位のうち，「チャット」，「音声通信」，「映像伝達」，「黒板」のように，前回の利用状態に依存しないサービスを抽出する☆．前回の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ことができる．たとえば，チャットサービスを提供する場合，利用者がメッセージごとに利用する S を変更できるような構成を実現できる．

(iii)【利用】C は，(i)，(ii) により分割された複数の S から，AM を介して利用権限証明書を取得し，利用の際 S に提示することで，S は C を認証し，C は S の提供するサービスを利用する．

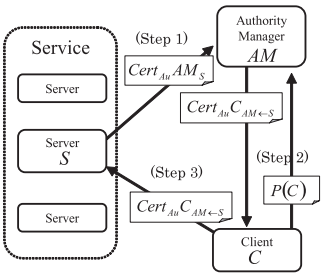

図 2 本提案モデルにおける権限委譲の流れ
Fig. 2 Process of delegation.

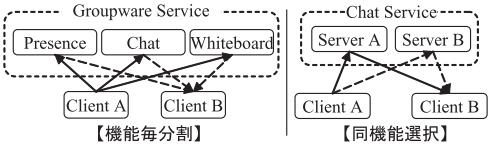

図 3 複数サーバによるサービスの連携
Fig. 3 Combination of services by multi-server.

4. Instant Message への適用

4.1 Instant Message

Instant Message（IM）は，会話を行う相手側の状態が事前に分かる「プレゼンス情報の通知」機能と，相手との会話を行う「メッセージ交換」機能を有した，ネットワークを介したコミュニケーション手段を提供するソフトウェアである．IM のモデルは RFC2778 で，要求仕様は RFC2779 で規定されている[7]．IM は，「ID」を介した「認証」を必要とする「コミュニケーション」（データのやりとり）という，双方向サービスの提供に必要な要素の本質を含んでいるため，本適用は，提案モデルの双方向サービスへの適用性を示すものである．

☆ 前回の利用状態に依存するサービスとは，利用するのに過去の利用情報が必要なサービスである．たとえば電子掲示板は「過去に書かれた文書」，電子メールは受信メールの蓄積を実現するため「過去に受け取ったメール」が必要であり，ファイル共有は「保存されたファイル」の保持を必要とする．

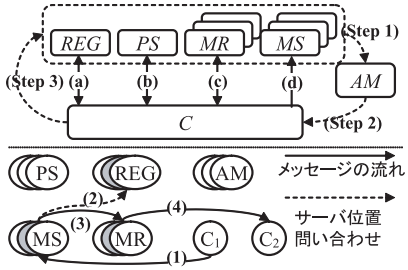

図 4 提案モデルの Instant Message への適用
Fig. 4 Application to Instant Message.

表 1 各主体が保持する情報
Table 1 Maintain information of each subjects.

主体	各主体の保持する情報
AM	C: $\{ID(C)_{AM}, H(Password_{AM}), \{Cert_{Au}C_{AM\leftarrow S}\}\}$ S: $\{Cert_{Au}AM_S, S(AM)_S\}$
REG	$\{URI(C)_{REG}, H(Password_{REG}), \{URI(S)\}\}$
PS	$\{URI(C)_{REG}, \{URI(ContactMember)\}\}$
MS	*none*
MR	*none*
C	AM : $\{ID(C)_{AM}, Password_{AM}\}$ REG: $\{URI(C)_{REG}, Password_{REG}\}$ S : $\{Cert_{Au}C_{AM\leftarrow S}, S(C)_S\}$

4.2 Instant Message への適用

提案モデルを IM に適用する．まず，【機能毎分割】により，IM を，プレゼンス機能 PS，メッセージ送信 MS，メッセージ受信 MR，そしてそれらのサービス群の位置情報を提供するレジストリ機能 REG，の 4 種類のサービスに分割する．次に，【同機能選択】が適用できるサービスは，メッセージ交換機能 MS，MR である．実現の概念図を**図 4** に示す．

4.3 主体の保持する情報と提供するサービス

提案モデルを構成する，AM，各構成 S，C について解説する．S は各々，権限証明書配布権と，対応する秘密鍵の組 $(Cert_{Au}AM_S, S(S)_{AM})$ を保持しているが，以下の記述では省略する．**表 1** は，各主体が保持する情報の一覧表である．

(1) **Authority Manager AM：**

AM は，各構成 S から権限証明書配布権 $Cert_{Au}AM_S$ を受け取り，C に対し，アカウント（AM における C の識別子 $ID(C)_{AM}$ とパスワード $Password_{AM}$ の対応）による認証を経た後，S の利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ の発行の代理を行う☆．なお，$P(C)_S$ に対応する秘密鍵 $S(C)_S$ は C が秘密裏に保持する．C の権限は，S が AM に与える $Cert_{Au}AM_S$ 中の権限の記述を基準として，AM が決定する．

(2) **Registry Service REG：**

C が利用する Server のアドレスリスト $\{URI(S)\}$ を管理し，アカウント（REG における C の識別子 $URI(C)_{REG}$ とパスワード $Password_{REG}$ の対応）により認証し，C へ利用可能 Server のアドレスリスト $\{URI(S)\}$ を与える．他の Server に対しては，C が現在利用している各 Server（PS_C や MR_C）を告知する機能を有する．

(3) **Presence Service PS：**

C のコンタクトリストの保持，コンタクトリスト登録メンバとのプレゼンス情報の送受信を行う．

(4) **Message Send Service MS：**

指定された宛先アドレスを管理する MR へメッセージを転送する．

(5) **Message Receive Service MR：**

MS から送信されたメッセージを自身の管理する Client へ転送する．なお，MR に現在接続している C の識別子のリスト $\{URI(C)\}$ を一時的に保持する．MS からのメッセージの転送の可否は $\{URI(C)\}$ を参照し決定する．

(6) **Client C：**

Client は各サービスを享受する主体である．

4.4 サービスの利用

(1) **事前準備**

C はあらかじめ，AM のアカウントの発行を受け，図 2 の Step1，2 の作業を終了させておく．次に，REG のアカウントの発行を受け，$URI(C)_{REG}$ を得ておく．

(2) **サービスの利用**

サービス利用の流れを図 4 と対応させて解説する．

開始：(a) C は REG へアカウントによる認証でログインし，自身の利用するサービスを提供する S の識別子のリスト $\{URI(S)\}$ を得る．**(b)**〜**(d)** (a) で得た URI を元に，$Cert_{Au}C_{AM\leftarrow S}$ の提出で認証（図 2 の Step3）を経た後，各 Server（PS，MR，MS）の提供するサービスを利用する．

プレゼンスの動作：主体 C と C' がお互いにコンタクトリストに登録されているとする．C がプレゼンス情報を変更（例．Work→Busy）する場合，C は自身の利用する PS_C へ変更の通知メッセージを送信し，PS_C は C のコンタクトリスト・テーブル☆☆を参

☆ 具体的には，C から，S に用いる公開鍵 $P(C)_S$ の提出を受け，それを元に $Cert_{Au}C_{AM\leftarrow S}$ を生成し，C に発行する．

☆☆ C のコンタクトリストに登録されるクライアントの URI のリスト $\{URI(ContactMember)\}$.

図 5 C_1 と C_2 の会話において各主体が把握する情報
Fig. 5 Talk C_1 with C_2.

照し，$URI(C')_{REG'}$ を発見する．それに基づき，C' の利用する $REG'_{C'}$ に問い合わせ，C' が現在利用している $PS_{C'}$ を確認し，$PS_{C'}$ へ向けて変更通知を転送する．$PS_{C'}$ は C' へ変更通知を転送し，C' は通知を受信する．

メッセージの送受信： 主体 C から C' へ向けてメッセージを送信する場合，図 4 **(1)** C は自身の利用する MS リストから任意に選んだ MS_C へ向けて，メッセージ（例.「From: $URI(C)_{REG}$, To: $URI(C')_{REG'}$，メッセージ本文」）を送信する．**(2)** MS_C は $URI(C')_{REG'}$ から C' の利用する $REG'_{C'}$ に問い合わせ，C' が現在利用している $MR_{C'}$ を確認し，**(3)** メッセージを転送する．**(4)** $MR_{C'}$ は C' へメッセージを転送し，C' は受信する．C' は受信を完了すると正常受信完了通知を先程と逆の手順で送信し，C はメッセージが正常に受信されたことを知る．

4.5 処 理 系

実装言語として Java2 SDK，SOAP☆エンジンとして Apache AXIS[8]，HTTP サーバおよび Servlet コンテナとして Apache Tomcat[8]を用い，SOAP1.1，WSDL☆☆ 1.1 準拠の Web サービスとして実装を行った．各主体間の通信には SOAP/HTTP を採用した．

4.6 実 行 例

図 5 は C_1 と C_2 が何件かのメッセージを送りあ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．

☆ SOAP: Simple Object Access Protocol
☆☆ WSDL: Web Services Description Language

表 2 各主体が把握できる個人情報
Table 2 Personal information in the grasp of each subjects.

		PS	*MR*	*MS*	*REG*	*AM*	単一
静的情報	氏名等登録情報	○	○	○	○	■	■
サーバ発見	サーバ位置情報	▲	▲	▲	■	○	■
プレゼンス	オンラインか否か	■	▲	▲	▲	○	■
	プレゼンス通知	■	○	○	○	○	■
	コンタクトリスト	■	▲	▲	○	○	■
メッセージ	メッセージの存在	○	▲	▲	▲	○	■
	送信メッセージ	○	△	△	○	○	■
	受信メッセージ	○	△	△	○	○	■

○ 情報取得不可能　△ 断片情報取得可能だが秘匿可能
▲ 断片 / 不確実情報取得可能　■ 全体 / 確実に情報取得可能

5. 考 察

5.1 提案方式の有効性

5.1.1 従来方式との比較

表 2 は，Instant Message を利用する C の個人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すべてのサービスを提供する方式を「単一」として掲載してある．○は情報がその主体に届かないため，情報が取得できないことを示す．△は，情報の断片を取得できるが，意味の分からない程度の断片情報に分割でき，また秘密分散法との併用（後述）により，事前に鍵の共有，あるいは公開鍵の授受などの作業を必要とせずに，主体に対して秘匿性を実現できることを示す．▲は，不確実な情報の一部を取得可能，あるいはメッセージを受信できるならばオンラインであるなど，間接的に情報を推測できる場合があることを示す．■は，情報の全体，あるいは一部でも確実に情報が取得できることを示す．表より，AM と S を分けることで静的情報と動的情報の分離が，【機能毎分割】の適用により機能ごとの動的情報の分離が，【同機能選択】により動的情報が分散されることが分かる．

5.1.2 分割のトレードオフ

Instant Message への適用において，厳密には，PS はさらに，プレゼンス情報送信サーバ PSS，プレゼンス情報受信サーバ PSR，コンタクトリスト保管サーバ PSC，の 3 つに分割することができる．この構成の場合，プレゼンス情報の送受信は，送信元 C が PSC から通知相手先アドレスを得る → PSS により送信 → PSR により受信 → 受信先 C という流れになる．しかし，プレゼンス通知機能には高い即時伝達性が要求されることから，今回の設計では，プレゼンス機能は分割は行わず 1 つのサービスとした．このように，サービスの分割にはトレードオフの関係が存在する．

5.1.3 安 全 性

提案システムの安全性について論ずる．

(1) **通信路中・サーバに対する安全性：**

C–S 間の通信は既存のセキュアチャネルにより暗号化できる．また，複数の S を介した通信経路を設けることで，ネットワーク上での秘密分散法[9]の利用が可能となる．たとえば，情報を n 個の暗号化断片に分割し，そのうち任意の k 個（$k < n$）の収集で復号（(k,n) 閾値法）できる暗号方式を用い，暗号断片をそれぞれ別の S を経由して送信する．本方式は，事前に相手先 C との鍵（共通鍵，あるいは公開鍵）の授受の必要なく，暗号利用の際の事前準備が不要という点で優位性が期待できる．

(2) **権限証明書に関わる安全性：**

(i)【偽装】提案モデルでは C が S のサービスを利用する際，利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ を提示する．S はサービスを提供する際，$Cert_{Au}C_{AM\leftarrow S}$ に含まれている C の公開鍵 $P(C)$ と秘密鍵 $S(C)$ の対応を確認することで，AM や他の S などが C に成り済まし S からサービス提供を受けることを防止する☆．同様の作業により，S は AM，C に，AM は S，C に，C は S，AM に，互いに成り済ましによる偽装を防止する．

(ii)【本人のコピーによる証明書の二重使用】S がサービスを提供する際に，C の提出する証明書を検証しない場合，この問題が発生する．その場合，使用された証明書に含まれる C の公開鍵 $P(C)$ を，その証明書の有効期間内は S が記録しておき，証明書の検証の際にそのリストを参照することで発見ができる．また，S の提供するサービスに応じて証明書の有効期限の長短の工夫ができる．

(iii)【複製された証明書の他人による使用】S がサービスを提供する際に C の提出する証明書を前述の手順で検証することで防止できる．ここで対応する秘密鍵 $S(C)$ が漏洩した場合の責任は C にある．$S(C)$ はパスワードと同じく C が責任を持って管理するデータである．

(iv)【破棄された証明書の使用】利用権限証明書が C によって破棄申請，または AM により破棄される場合，AM は破棄する証明書のハッシュ値を各 S に通知することで防止できる．各 S は，証明書のハッシュ値から該当する証明書を探して無効にする．

(v)【1 回限りの証明書の実現と不正の防止】AM が発行する S の利用権限証明書の利用回数を 1 回限りにしたい場合がある．その場合は C が証明書を提出してサービスを享受した際，利用権限証明書のハッシュ値 $H(Cert_{Au}C_{AM\leftarrow S})$ を，受け取った S が AM に通知し，AM は対応する $Cert_{Au}C_{AM\leftarrow S}$ を検索し，C の利用を不可にしたい他の S へ証明書の無効を通知することで実現できる．また，複数回使用可能な利用権限証明書は複数枚の証明書の発行で実現する．なお，実現には別途排他制御などの適切な機構が必要である．S が通知する $H(Cert_{Au}C_{AM\leftarrow S})$ には S の利用情報などは含まれず，AM を代理とするため他の S へは証明書の無効通知だけが伝わるため，動的情報は保護される．

(3) **各サーバの独立性・信頼性・品質の保証：**

提案モデルの前提条件として，各 S，AM は独立であり，全体の機能を実現するうえで支障のない程度の品質でサービスを提供することがある．SPKI 権限証明書には，つねに証明書発行者の公開鍵が含まれており，成り済ましが検出できることから，技術面からの独立性が保証可能である．提供するサービスの信頼性と品質の保証は運用によるが，各 S については，AM が $Cert_{Au}AM_S$ の提出を受けた際に身元照会をすることで保障が可能である．AM 自体の保障については，PKIX[10]など，既存の PKI 技術を用いた独立した第三者による身元保証と監査が必要である．

5.1.4 適 用 性

提案手法の適用性に関して考察する．

Web 上の仮想コミュニティやグループウェアなどの複合サービスは，独立した複数の機能で構成されており，機能毎分割の適用が容易である．チャットや電子メール☆☆などの双方向型会話サービスや，文書データ形式変換サービスなどの，前回の利用状態に依存しない関数的なサービスについては，同機能選択の適用が可能である．サービスの性質上，サーバにデータ本体を与えざるをえないようなサービスにおいては，サーバを選択的に利用することで，単一のサーバ（管理単位）への情報集中を防止することができる．

5.2 集中方式と分散方式の比較

5.2.1 事業者/利用者からの特長

一般的な C/S 型のシステムはサービス提供者が単一であるため**集中方式**，本稿の提案モデルはサービスの

☆ 具体的には，利用権限証明書 $Cert_{Au}C_{AM\leftarrow S}$ に含まれる C の公開鍵 $P(C)$ を用いて，S が $P(C)$ で暗号化したデータを C に送信し，C が $S(C)$ を用いて複号したデータを S に送り返し，送り返されたデータと元のデータの一致により検証する．これにより，C の正当性が保障される．

☆☆ IM への適用例において，MR に蓄積性を備えることでサーバへのメッセージ保管ができる．また REG 上に参加者リストを登録することでメーリングリストと同等の機能が実現できる．

表 3 事業者/利用者双方からみた特長
Table 3 Merit of providers and users.

集中方式	分散方式
【事業者】 利用者の囲い込み 利用動向の把握が容易 課金しやすい 人気サービスを発見しやすい 利用動向よりプッシュ型提供	【事業者】 顧客情報保護・情報漏えいの予防 内部不正の予防・リスク分散 サーバ機能限定・仕組みの単純化 負荷分散・障害耐性の向上
【利用者】 証明書処理・手続きの簡素化 趣向に応じたサービスの享受	【利用者】 プライバシー重視 事業者 / サービス選択性の向上 サービスの柔軟な組み合わせ

分散協調によるので**分散方式**，として，サービス事業者/利用者双方からの，両方式の特長を一覧にまとめた（**表 3**）．集中方式には事業者側からの長所が多く，分散方式には利用者側からの長所が多くあげられた．情報セキュリティの観点から考察すると，情報漏えいの防止や顧客情報の保護は最優先される事柄である．情報漏えいの多くが内部犯であるとの指摘もあり，単一の事業者でサービスを提供する場合においても，保護すべき情報が集中管理されている状態は好ましくない．管理は人間が行うものであり，必ずしもつねに善意を想定できないからである．問題発生の「予防」を可能とする提案方式は，事業者にとっても利点がある．

5.2.2 サービスの性質に応じた柔軟な動的構成

提案モデルの「性質による分散」の効果として，各サービスの性質に応じたサーバの分割が可能となる．今回実装した例では，PS は相手先 C が不意の回線切断などでオフラインになるような場合を検出するため高い即時伝達性が求められるが，MS，MR については PS を通して相手が現在メッセージを受け付けられる状態か否か分かるので PS ほどの即時伝達性は求められない．REG は，必要ならば他の S から負荷・故障などの情報の報告を受けて，適切な利用可能サーバリストを C に提案することも可能である（あくまで利用の選択権は C にあることに注意されたい）．ほかにも記憶容量，ネットワーク帯域，サーバの性能などを考慮し，適切なサービス提供の構成を設計することができる．

5.2.3 Web サービスとの関連

本稿で実装技術として採用した Web サービスは，ネットワークを介したソフトウェア・サービス連携の基盤技術である．複数の提供者の連携で構成される複合サービスにおいては，個々の提供主体がセキュリティを高めても「**信頼すべき善意の主体**」の数が飛躍的に増加してしまう危険性がある．本手法は，各々の構成主体に必要最小限の情報保持を可能とし，信頼度を最小限にとどめる．流れ作業によるサービスの連携は，個々の主体の信頼度の掛け算の信頼度が必要であるが，本手法の適用されたシステムでは個々に任せられた機能の範囲内に信頼度をとどめることができる．

6. 関 連 研 究

梅澤ら[6]は，SPKI 権限証明書を利用し，サーバはアクセス権を認証することで，利用者は匿名で認証が必要なサービスを享受できる，**匿名アクセス制御方式**を提案した．上述の手法は，利用者 ID と利用者情報との対応付けを防止したい要求には有効であるが，クライアントがサーバと送受信する情報自体をサーバから保護することはできない．そのため，適用対象が Web ページの閲覧制御など 1 方向の媒体に限られる．提案手法では，会話サービスなどの双方向型や文書変換サービスなどへの適用が期待でき，上述の手法と比べて適用対象を広げることが可能となる．

末松ら[11]，大瀧ら[12]は，利用者とサービス提供者との間での利用料金徴収分配業務を，「料金回収センタ」と「料金分配センタ」に分割することで，利用者の住所・氏名・口座番号などと，実際の利用内容とを別々に管理することで，利用者情報と利用内容との対応付けを防止し，プライバシに配慮した業務を行うことを可能にする，**センタ分割方式**を提案した．一連の業務フローを切り分け，そのセンタの業務に不要な部分を部分的に暗号化する上述の手法は，提案手法と直行性を持ち，併用可能な手法である．本提案モデルにおいて，上述の論文中のコンテンツ提供者はサービス提供主体（S）に対応する．料金徴収・分配は，権限管理主体（AM）に対応するため，AM を「料金徴収センタ」と「料金分配センタ」に分離することで，上述の手法は本手法にも応用可能な手法である．

7. 今後の課題

(i) 効率化についての検討：通信コスト，証明書発行/検証コストについては，適用対象とするサービスにより異なると考えられる．今後，サービス形態別の理論的算定，シミュレーションや評価実験などを通して明確にしていきたい．

(ii) 信頼性・可用性の検討：本稿で示した適用例において，AM や REG に対する信頼性の確保が重要である．冗長性を持たせる解決は従来と同様のプライバシ上の問題が懸念されるが，冗長性を持たせる情報が静的情報（の必要な一部）に限定できるという点で従来より改善が見込める．たとえば，REG 自体には「クライアントが利用するサーバリスト」が保管されているだけであり，それ単体で有益な情報価値をもたらすものではない．

(iii) 他のサービスへの適用：本稿では Instant Message への適用を行い，双方向会話サービスや複合サービスに有効であることを示した．複雑な状態遷移をともなう手続き的なサービスにおいても，相互に独立した複数の関数的なサービスに分割することで，本手法が適用できる場合があると考えられる．今後，適用方法についてモデル化や形式化を行い，サービスの分割手順についてより明確にしていきたい．

8. ま と め

本稿では，独立した複数のサーバの協調動作によりサービスを提供し各々の主体に集約される情報を制限することで，利用者の情報を保護し，プライバシに配慮したサービスを実現可能なモデルを提案した．提案方式の適用例として Web サービス上の Instant Message への実装を紹介し，その有効性について議論した．以上の本稿で提案したサービス提供モデルにより，サーバと送受信する情報自体をサーバから秘匿することは困難だが，プライバシへの配慮や情報漏えいを防止したいという，従来研究では困難であった要求を実現するためのサービス提供の枠組みを与えることができた．

謝辞 懇切丁寧に，洞察力の豊富なコメントをいただきました査読者各位に感謝いたします．

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，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) 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 Web サービス上の Instant Message への適用，データベースと Web 情報システムに関するシンポジウム（DBWeb2003），pp.155-162 (Nov. 2003).
4) Ellison, C.: SPKI Requirements, IETF, RFC2692 (Sep. 1999).
5) Ellison, C., et al.: SPKI Certificate Theory, IETF, RFC2693 (Sep. 1999).
6) 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).
7) Day, M., et al.: A Model for Presence and Instant Messaging, IETF, RFC2778 (Feb. 2000).
8) http://jakarta.apache.org
9) Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
10) Public-Key Infrastructure (X.509), IETF.
11) 末松俊成，今井秀樹：ユーザのプライバシー保護が可能な超流通ラベル配送形超流通システム，電子情報通信学会論文誌，Vol.J81-A, No.10, pp.1377–1385 (1998).
12) 大瀧保広，河原正治：超流通における使用記録の回収とプライバシー保護，情報処理学会論文誌，Vol.41, No.11, pp.2978–2984 (Nov. 2000).

(平成 15 年 9 月 25 日受付)
(平成 16 年 1 月 19 日採録)

（担当編集委員 石川 博，市川 哲彦，原 隆浩，佐藤 聡，土田 正士）

小瀬木浩昭（学生会員）
昭和 54 年生．平成 14 年東京理科大学理工学部情報科学科卒業．平成 16 年東京理科大学大学院理工学研究科情報科学専攻修士課程修了．同年同大学院博士課程進学．技術士補（情報工学部門）．日本技術士会会員．

真柄 喬史（学生会員）
昭和 55 年生．平成 14 年東京理科大学理工学部情報科学科卒業．同年東京理科大学大学院理工学研究科情報科学専攻修士課程進学．

武田 正之（正会員）
昭和 52 年東京理科大学理工学部電気工学科卒業．昭和 57 年東京工業大学大学院博士課程（電子物理工学専攻）修了．同年東京理科大学理工学部情報科学科助手となり，現在同大学教授．工学博士．著書（共著）に『Prolog とその応用 2』，（総研出版，昭和 60 年）等がある．プログラミング言語の意味論，並列・分散システム，知識情報処理に興味を持つ．昭和 57 年度情報処理学会論文賞受賞．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，ACM 各会員．