分散協調による情報保護機構の提案 －Instant Message Webサービスへの実装と応用－

小瀬木 浩昭† 真柄 喬史† 武田 正之††

C/S 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等，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，プライバシー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，一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．提案モデルの実現例として，Web サービス技術を用いた Instant Message への実装を紹介し，有効性について考察する．また，双方向サービスにおいて用いられるサービス形態をパターンとして，各パターンに提案手法を適用する方法と適用による効果について考察する．

Distributed and Cooperative Information Protection

HIROAKI OZEKI ,† TAKAFUMI MAGARA † and MASAYUKI TAKEDA ††

This paper proposes a *information protected service model* on the Internet. We will propose information protected service mechanism where services are jointly and cooperatively provided, the 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.

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等，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，プライバシー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等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留め，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ー重視のサービス提供に関して研究を行ってきた[1)~4)]．その本質は，(i) ユーザを識別する「ID」と，それと結びつく，氏名や住所等サービスの登録・料金請求に必要となる「静的情報」と，実際にサービスを利用した際にサーバと送受信する情報や利用時刻等の「動的情報」の分離，(ii) 動的情報同士の分離と，サーバ選択性による送受信情報の分散，(iii) 権限証明書の導入と公開鍵基盤の活用による，構成主体の相互の成り済ましの防止，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個人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，各主体は扱う情報と機能が限定され，情報セキュリティ向上の効果が期待できる．他の主体への成り済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，提案モデルについて解説してから，提案モデルの実現例として Instant Message サービスへの適用例を紹介する．また，サーバを介したクライアント同士の双方向サービスにおいて用いられる形態をパターン化し，各パターンに提案手法を適用する方法と適用による効果について述べることで，提案手法の適用性を明確にする．

† 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 Engineering, Tokyo University of Science
†† 東京理科大学 理工学部 情報科学科
Information Science, Tokyo University of Science

2. 準 備

2.1 表記方法

本稿において，MD5 等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，$\langle\ldots\rangle_{S(X)}$ 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 $URI(Y)$ と表記する．主体 X が主体 Y に与えた権限を $Au(Y_X)$，有効期限を $V(Y_X)$，有効期限を含む，権限に対する制約条件を $Lim(Y_X)$ と表し，権限・制約条件組リスト $\{Au(Y_X), Lim(Y_X)\}$ を $ACL(Y_X)$ と表記する．なお，便宜上，主体 X における，主体 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，次で定義する**権限証明書**を用いる．

主体 X が，主体 Y に対して権限・制約条件組 $ACL(Y_X)$ を保証し，権限委譲の可否が $D(Y_X)$（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:

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

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 $ACL(Y_X)$ を持つと判断する．

2.3 権限証明書を用いた権限委譲

主体 X，Y，Z の 3 主体間において，「X から Y へ二次配布権を持つ権限証明書：**配布券** $Cert_{Au}Y_X$」，「Y から Z へ，$Cert_{Au}Y_X$ に基づき Y により作成される，X へ権限行使可能な権限証明書：**利用券** $Cert_{Au}Z_{Y\leftarrow X}$」を定義する．

利用券 $Cert_{Au}Z_{Y\leftarrow X}$ は次のように実現する．

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

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

なお，論文中，利用券 $Cert_{Au}Z_{Y\leftarrow X}$ に対応する秘密鍵 $S(Z)$ を明示的に $S(Z)_X$ と表現することがある．

利用券の正当性の検証：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 が利用券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券であることが証明される．

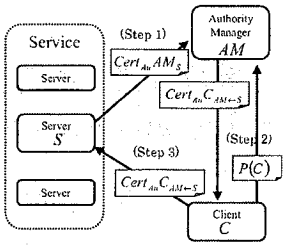

図 1　本提案モデルにおける権限委譲の流れ
Fig. 1　Process of Delegation.

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 から $P(AM)_S$ の提出を受け，配布券 $Cert_{Au}AM_S$ を発行する．C が提出した利用券 $Cert_{Au}C_{AM\leftarrow S}$ により C を認証し，C のサービス利用の制御を行う．

Authority Manager (AM): C への利用券発行主体．S からの，配布券の発行を受け，S の代理として C に利用券を発行する．

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

【前提条件】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，配布券，利用券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，必ずしも全ての S の善意を必要としないが，全体の機能を実現する上で支障の無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．

3.2 サービス利用の流れ

3.2.1 サービスを利用するまでの流れ（図 1）

Step1: S は AM に配布券 $Cert_{Au}AM_S$ を予め提供しておく．**Step2**: AM は既存の方法で C を認証した後，C から S の利用券を得るための公開鍵 $P(C)_S$ の提出を受け，S の利用券 $Cert_{Au}C_{AM\leftarrow S}$ を C に対して発行する．**Step3**: C は利用券を 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．

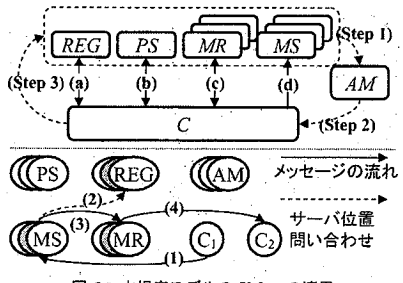

図 2 本提案モデルの IM への適用
Fig. 2 Application to Instant Message.

3.2.2 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．

4. 提案モデルの 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わかる「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 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．

4.2 提案モデルの Instant Message への適用

提案モデルを IM に適用する．先ず，【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 2** に示す．

4.3 サービスの利用

4.3.1 事前準備

C は予め，AM のアカウントの発行を受け，図 1 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．

4.3.2 サービスの利用

サービス利用の流れを図 2 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 のアドレスリスト $\{URI(S)\}$ 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 1 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，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 2**(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．

4.4 処理系

実装言語として Java2 SDK[5]，SOAP エンジンとして Apache AXIS[6]，HTTP サーバ及び Servlet コンテナとして Apache Tomcat[6] 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．また各主体間の通信には SOAP/HTTP を採用した．

4.5 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

* C のコンタクトリストに登録されるクライアント *Contact-Member* のアドレスリスト $\{URI(ContactMember)\}$.

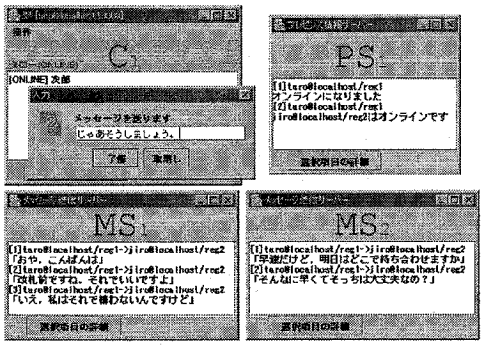

図 3　C_1 と C_2 の会話
Fig. 3　Talk C_1 with C_2.

表 1　各主体が把握できる C の個人情報
Table 1　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

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．

4.6　従来方式との比較

表 1 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全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，また閾値暗号との併用（後述）により，事前の鍵の授受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等，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】の適用により機能毎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わかる．

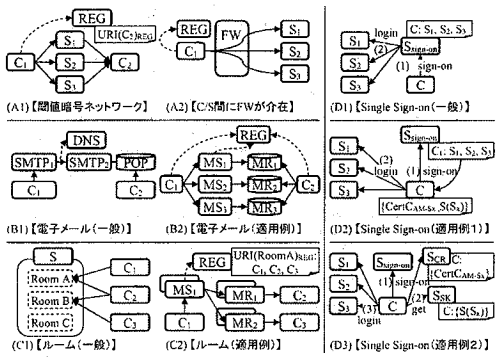

図 4　提案方式の適用パターン
Fig. 4　Pattern of Applications.

5.　提案方式の適用パターン

ネットワークを利用するシステムには様々な形態がある．その中から良く用いられる形態をパターン化し，適用性を明確にすると共に，適用による効果について考察する．以下の解説は**図 4** と対応する．

5.1　閾値暗号ネットワーク

(A1) では，C_1 と C_2 の間に複数の通信経路が形成されている．複数の通信経路を設けることで，閾値暗号[7] ☆ が利用可能となる．REG からサーバの位置情報を得ることで，複数のサーバを同時に，また動的に変化させて利用することが可能である．閾値暗号は，共通鍵方式や公開鍵方式と異なり，暗号化断片に復号情報を埋め込むことで，事前に相手方との鍵の受け渡しの必要が無く暗号化通信が可能という優位性がある．また，C と S の間の通信が既存のセキュアチャネルで暗号化されていれば，(A2) の構成で通信全てを傍受可能なサーバ FW に対しても秘匿性が保持できる．

5.2　メール（蓄積型）

(B1) は SMTP-POP 型の電子メール配送モデルを示す．電子メールシステムに提案モデルを適用したものが (B2) である．C_1 は複数の送信サーバ MS を利用し，C_2 が受信可能な受信サーバ MR まで配送される．MR は受信メールを蓄積し，C_2 は任意のタイミングで MR からメールを取得し閲覧する．また，閾値暗号を併用すれば，事前に鍵の交換ができない初対面

☆ 本稿で想定する閾値暗号は次の性質を持つものとする．**(i)** 情報を n 個の暗号化断片に分割し，任意の k 個（$k < n$）の収集により復号（(k, n) 閾値法）．**(ii)** 各断片は識別情報を含み，他の断片と混在した際も正常に復号できる．

の相手との暗号化メールの送受信が可能となる．

5.3 ルーム（グループ）

(C1) は複数の C 間で情報を共有したい場合に用いられる，S 上に形成されたルームを示す．(C2) は提案モデルを適用し，REG 上にルームの参加情報を登録し，メッセージの送受信は MS と MR を介して行なう．これにより，ルーム情報とメッセージ情報が分離され，また送受信メッセージは分散・断片化される．提案手法と閾値暗号を組み合わせた暗号化は鍵交換が不要であり，グループ鍵暗号方式におけるメンバ離脱の際の鍵更新等が発生せず，メーリングリスト等の蓄積系媒体にも適用できるという長所がある．また，グループへの参加・離脱が頻繁な場合，従来頻繁な鍵更新が必要であったが，本手法は鍵自体不要である．

5.4 シングル・サインオン

本節では，権限証明書を用いて Single Sign-on と同様の機能を実現する方法について検討する☆．(D1) は Single Sign-on を実現する仕様である SAML[8] の Push Model を示す．C がサインオンサーバ $S_{sign-on}$ にサインオンすると，$S_{sign-on}$ は連携している S_1，S_2，S_3 に代理ログイン（アクセス権を取得）する．(D2) は提案手法を適用し，(1)$S_{sign-on}$ へサインオンしその他の S の位置情報を得る，(2)C が直接 S へ権限認証によりログインする．これにより $S_{sign-on}$ へ，C が他のサーバを利用した情報（動的情報）を知られないでサービスを受けることが可能となる．なお，(D1) に比べログイン手順が長くなるが，この手順はソフトウェアによる自動化が可能である (D3) は，(D2) を発展させ，利用券 $\{Cert_{Au}C_{AM\leftarrow S}\}$ を保管するサーバ S_{CR}，対応する秘密鍵 $\{S(C)_S\}$ を保管するサーバ S_{SK} を導入し，(1)$S_{sign-on}$ へサインオンした後，(2)S_{CR} と S_{SK} から利用券と対応する秘密鍵を得て，(3) 各 S へログインする☆☆．

6. 考　　察

6.1 信頼性・可用性についての検討（図 5）

6.1.1 冗長化の検討

REG の冗長化について検討する．REG の冗長化手法には，ミラーリング，DNS 等に用いられている階層方式などが考えられる．ミラーリングは大規模になると複製コストがかさみスケーラビリティが無い．階層方式は効率的だが組織だった運営が不可欠である．そこで，C が REG に対して登録申請を行なう方式を提案する (E)．これは複数の REG を利用可能な C が，冗長化したい REG の情報を C 側から登録する．登録フィールドには public field と private field を設け，public field は他の C も参照でき，private field は登録者だけが参照できる．(E) の C_2 は，$URI(C_1)_{REG1}$ と $URI(C_1)_{REG2}$ の 2 つの REG 情報を取得し，利用中一時的に片方の REG に接続できなくなった際，もう一方の REG を利用して C_1 とコンタクトを取ることを可能にする．本方式の長所は，C の必要に応じて冗長化の範囲・規模が決められることと，REG への登録情報の伝播を C が制御できることである．

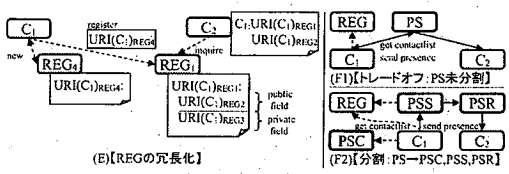

図 5　冗長化 / トレードオフ
Fig. 5　Redundance / Trade Off.

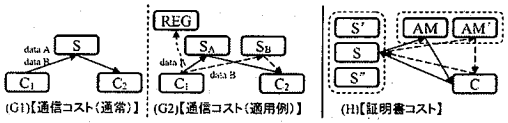

図 6　通信コスト / 証明書コスト
Fig. 6　Costs of Communication / Verification.

6.1.2 分割のトレードオフ

Instant Message への適用 (F1) 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 (F2)．この構成の場合，プレゼンス情報の送受信は，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，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，プレゼンス機能はこれ以上の分割は行なわず 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．

6.2 効率化についての検討（図 6）

6.2.1 通信コスト

通信量：S は，N 種類のサービスを提供しており，サービス X による通信量を $m(X)$ と表すと，全体の通

☆ Single Sign-on で提供されるサービスにおいても，【機能毎分割】，【同機能選択】により分割されたサーバで全体を構成することで，サーバへの情報集中を防止でき有効性がある．

☆☆ 権限証明書の認証には $Cert_{Au}C_{AM\leftarrow S}$ と対応する $S(C)_S$ の組が必要であるため，お互い片方しか持たない S_{CR}，S_{SK} は C に成り済ましてサービスを受けることはできない．また，$Cert_{Au}C_{AM\leftarrow S}$ と対応する $S(C)_S$ は，お互い容易に推測できない．これは公開鍵基盤において公開鍵と秘密鍵がお互い容易に推測できない特性に基づいている．

信量 t は，通常方式 (G1) の場合は $t = \sum_{k=1}^{N} m(X_k)$ であり，提案方式 (G2) の場合は $t = \sum_{k=1}^{N} m(X_k) + m(REG_k)$ である．

通信回数：S は，N 種類のサービスを提供しており，サービス X による通信の回数を $n(X)$ と表す．複数のサービスが同時に情報を送る場合，TCP における piggyback 方式のように，一つのデータにまとめて一緒に送り，通信回数を削減できるとする．全体の通信回数を f とすると，通常方式 (G1) の場合は次のようになり，

$\max_{k=1}^{N} n(X_k) \leqq f \leqq \sum_{k=1}^{N} n(X_k)$

提案方式 (G2) の場合は次のようになる．

$f = \sum_{k=1}^{N} n(X_k) + n(REG_k)$

以上より，提案手法の適用による，通信量の増加は少ないが，通信回数が増加することが予想される．新しいセッションを開くための S にかかる負荷の増大や，遅延のボトルネックとなることが予想される．利用頻度の高い通信セッションは次の情報送信に備えてセッションを保持するなど，通信回数の削減のための工夫が必要であるといえる．

6.2.2 証明書発行・検証コスト

発行：新規証明書の発行は，証明書毎に $S \rightarrow AM \rightarrow C$ の一巡である (H)．よって発行にかかるコストは発行する証明書の枚数に比例する．

検証：S に提出される C の利用券の検証回数は，毎回権限認証を正確に行なう場合，C が S に権限認証を求める回数と同じであるが，一時的に接続が切れて再接続した際などの再認証には，前回の C との同一性を確認できれば良いので，あらかじめ同一の乱数などを交換しておき再接続の際にはその一致を確認することで，再接続の際の権限認証のコストを回避できる．

有効期限の長い利用券においては，発行処理一回に対し，検証処理は何度も繰り返される処理である．よって，上述したような検証処理の効率化は重要である．

7. 関連研究

9) のような単なる権限認証によるプライバシ保護は，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，本稿のような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したい要求には，本手法が有効である．10) での料金徴収分配業務の分割の手法は，本稿のサーバ (S) をコンテンツ提供者に，権限管理主体 (AM) を「料金徴収センタ」と「料金分配センタ」に分割し，論文中のそれぞれのセンタと対応させることで，本手法と組み合わせることが可能である．11) では Instant Message に特化した暗号化プロトコルを提案しているが，本稿で指摘したように，オフライン媒体には適用できない等の従来と同様のグループ鍵暗号上の問題を抱える．

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，プライバシー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 Instant Message への適用を紹介し，その有効性について議論した．また，双方向サービスにおいて用いられるパターンへの提案手法の適用方法と効果について述べた．論文中，信頼性・可用性，効率化についての検討を行なったが，今後，定量的な評価等を通して明確にしていきたい．

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) 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).
4) 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).
5) http://java.sun.com
6) http://jakarta.apache.org
7) Shamir, A.: How to share a secret, *Communication of the ACM*, Vol. 22, No. 11, pp. 612–613 (1979).
8) Security Assertion Markup Language, OASIS.
9) 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 (Aug. 2001).
10) 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).
11) 菊池浩明, 多田美奈子, 中西祥八郎: 管理者に対して秘匿性を保障したセキュアインスタントメッセージングプロトコル, 情報処理学会論文誌, Vol. 44, No. 8, pp. 2042–2050 (Aug. 2003).