L-036

プライバシー重視の分散協調型グループコミュニケーションモデルの提案とその評価

Privacy Enhanced Distributed and Cooperative Group Communication Model

鎌田 浩嗣‡ 大矢 健太‡ 小瀬木 浩昭‡ 武田 正之†
Hiroshi Kamata Kenta Ohya Hiroaki Ozeki Masayuki Takeda

1. はじめに

近年，個人情報漏洩問題が多数とりざたされているが，管理者などの内部犯行による情報漏洩が多くの割合を占めていることが報告されている(CSI/FBI Computer Crime and Security Survey). 従来からある C/S 型のシステムではサーバの情報管理，運営状況が不透明であり，かつサーバにあらゆる情報が集中する為，ユーザの静的情報(氏名などの身元情報に関する登録情報)と動的情報(サービス利用によって生じる行動パターンなどのサービス利用情報)が容易に関連付けられ，サービス提供者がどのユーザがいつ，どこで，誰と何をしているかというプライバシーに関する情報までも把握することが容易であった. しかしながら，通信内容の秘匿に対し鍵を使用する場合，第三者機関による鍵の正当性の保証や鍵の管理，更新などが必要でありユーザに負担がかかることが挙げられる. さらに，C/S 型の性質上，一度に多数のユーザの情報が漏洩してしまう危険性も存在した. 我々はこれまで，情報保護を実現する分散協調保護モデルを提案している[1]. 提案モデルは，必要最小限の機能を有する複数のサーバが分散・協調してサービスを提供し，各サーバが取得できる情報を最小限に留めることで情報保護を実現している. 本稿では，このモデルを多対多の双方向通信への対応が可能となるよう拡張する. さらに，秘密分散法の導入による鍵の管理，更新などを必要としない暗号通信を提案する. その適用例としてグループチャットシステムへ実装し，評価を行う.

2. 提案モデル

提案モデルは,**1.**認証機構，**2.**サービス分割，**3.**秘密分散法から構成される. 認証機構によりサーバ・クライアント間及びサーバ同士の結託，成りすまし，不正を防止する. サービス分割により各サーバが取得できる情報を制限し，さらに秘密分散法によりサーバに蓄積される情報を秘匿にする. なお，通信路の秘匿に対しては SSL などの既存のセキュアな通信路を用いることとする.

2.1. 認証機構

サーバ(S)，権限委譲局(AM)，クライアント(C)の 3 つの主体から構成される(図 1). ここで，AM はユーザの静的情報を管理し，S は動的情報を扱う主体である. 前提条件として S, AM, C は互いに独立していると仮定する. また，SPKI 権限証明書の拡張により 1. 匿名認証,2.構成要素間で成りすまし不可能であることを保証する. これにより，静的情報と動的情報の関連付けが困難となる. なお，SPKI 権限証明書は，権限と公開鍵の対応に，証明書の発行者が電子署名を付加したものである.

2.2. サービス分割

提案モデルではサービスを以下のように提供する.

・『サービス別提供』-独立した最小限のサービス毎にサーバを分割し，各サーバが独立してサービスを提供する. これにより複合サービスによって統合された情報の取得が防止できる.

・『同サービス提供』-前回の状態に依存しないサービスを提供するサーバを複数設ける. ユーザは事前に取得したサーバリストから使用したいサーバを選択・同時利用する. これにより，サービス別提供に加え各サーバが取得可能な情報が断片化される.

ただし，閾値以上(後述)のサーバが結託することはないとする.

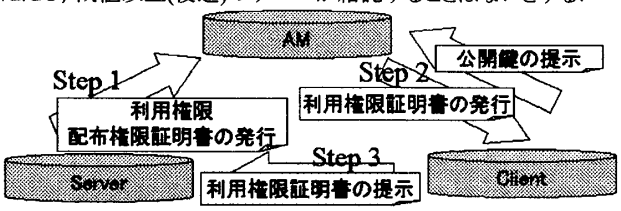

図 1 提案モデルにおける権限委譲の流れ

2.3. 秘密分散法

秘密分散法とは，次のような性質を有する手法である[2]. **(1)**秘密情報を n 個のシェア(暗号断片)に分割し，任意の k 個以上(k≦n)のシェアの収集により，秘密情報の復元が可能となる. **(2)**k 個未満のシェアの収集では，秘密情報に関する情報は全く得られない. これを，(k,n)閾値法という. また，k の値を閾値という.

サービス分割によりサーバが取得可能な情報が分離・分散されるが，その内容自体は秘匿とならない. そこで，提案モデルでは秘密分散法を併用して構成することで，内容の取得を困難にする.

2.4. グループコミュニケーション

グループコミュニケーションの本質は，ID による認証，双方向通信，同報通信であり，ネットワーク通信の基本要素を含む.

提案手法は従来に比べ 1.柔軟なサービスの組み合わせが可能，2.利用情報分散，3.仕組みの単純化，4.リスク分散，5.可用性の向上という特徴がある. 以下に従来のコミュニケーション手法との比較を示す.

表 1 従来のコミュニケーション手法との比較

	ML	IM	IRC	提案手法
サーバの選択性	×	×	△	○
情報分散の度合	×	×	△	○
システムの柔軟性	×	×	△	○
通信コスト	○	○	○	×
管理コスト	○	○	△	×

3. グループチャットシステムへの実装

提案手法の適用例の一つとして，SOAP1.1,WSDL1.1 準拠の Web サービスを用いたリアルタイムグループチャットシステムへの実装を行った. 実装言語として Java2 SDK を使用し，各サーバ間の通信には SOAP/HTTP を採用した. 秘密分散法のアルゴリズムは閾値が分割数と同じ値である(n, n)閾値法を用いて，会話内容となる文字数や分割数を変化させ，評価を行った.

‡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

3.1. システムの概要と動作画面

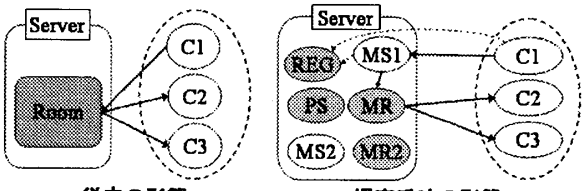

図 2 従来のモデルとの比較

従来のグループチャットシステムは『サービス別提供』を適用することで，プレゼンス情報を扱うサーバ:PS，メッセージ送信，受信を行うサーバをそれぞれ:MS,MR，上記のサーバ群の位置情報とルームを管理し，ユーザに位置情報を提供，サーバに対してはユーザの使用しているサーバを通知するサーバ:REGから構成できる．そのうち，MS,MR は「同サービス提供」が適用できる(図 2)．

図 3 に実際の動作画面を示す．

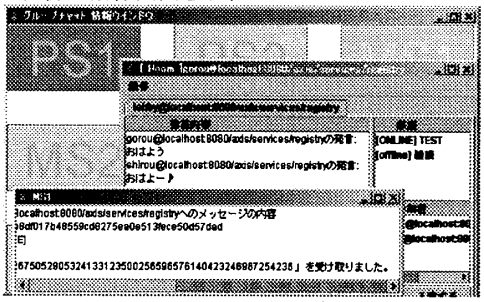

図 3 チャットウィンドウとサーバの利用情報

4. 考察

4.1. 情報分散

各サーバが把握する情報の従来のモデルとの比較を表 2 に示す．この表が示す通り，各サーバが取得できる情報が従来に比べ分散していることが分かる．

表 2 従来と提案手法における各サーバが取得可能な情報

		AM	REG	PS	MS	MR	従来
静的情報							
氏名・住所などの登録情報		■	○	○	○	○	■
動的情報							
ユーザが使用しているサーバ		○	■	▲	▲	▲	■
グループ情報	ルームの参加情報	○	■	▲	○	○	■
	ルームのメンバ登録情報	○	■	▲	○	○	■
	ルームNickName	○	○	■	○	○	■
グループプレゼンス情報	Online/Offline	○	■	■	▲	▲	■
	プレゼンス情報	○	○	■	○	○	■
プレゼンス情報	Online/Offline	○	■	■	▲	▲	■
	プレゼンス情報	○	○	■	○	○	■
メッセージ	送信の有無	○	○	○	▲	▲	■
	受信の有無	○	○	○	▲	▲	■
	メッセージ本文	○	○	○	△	△	■

■情報取得可能　▲断片/不確実情報取得可能
△断片情報取得可能だが秘匿可能(*2)　○情報取得不可能
*2 秘密分散法と併用により秘匿可能。
注)グループ情報取得可能とは同グループに所属する3人以上の情報が取得可能な場合を指す

4.2. 実用性についての考察

4.2.1. 通信量と通信回数

サーバは N 種類のサービスを提供し，サービス X による通信量を $p(X)$，通信回数を $q(X)$，秘密分散法による分割数を n，全体の通信量を T，通信回数を F，例えば，ルームのメンバ情報問合せのような，従来からあるルームに関する情報を除いた情報を取得するための，REG へのアクセスに対する通信量を $p(REG')$，通信回数を $q(REG')$とする．

すると，通信量は従来のモデルでは $T=\sum_{i=1}^{N} p(X_i)$ であり，提案手法では $T=n\sum_{i=1}^{N} p(X_i)+p(REG')$ となる．通信回数は従来のモデルでは $\max_{i=1}^{N} q(X_i) \le F \le \sum_{i=1}^{N} q(X_i)$ であり，提案手法では $F=n\sum_{i=1}^{N} q(X_i)+q(REG')$ となる．つまり，通信量，通信回数は REG へのアクセス及び秘密分散法を用いている部分で増加するといえる．なお，これは同報通信を MS に委託している際のコストである．また，秘密分散法を使用した場合，分割数倍だけ通信量，回数が増加する．

提案手法では，REG に対し，サーバ問合せなどのためにアクセスする必要がある．そこで，簡易な測定を行ったところ，サーバ間通信を含め通信回数全体に占める REG へのアクセス回数，通信量は 20%程度であった．図 4 はその結果であり，通信の割合を示すグラフである．ただし，秘密分散法を使用していない場合((1,1)閾値法)の結果である．これは，秘密分散法のアルゴリズムや分割数により，通信の割合に変化が生じるためである．

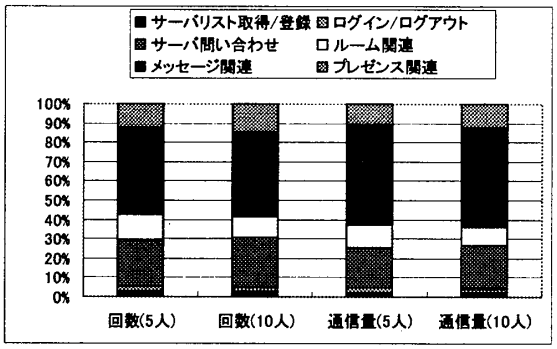

図 4 全通信における通信回数および通信量の割合

4.2.2. 秘密分散法における分割数と処理時間の関係

分割数と処理時間の関係を図 **5**, 図 **6** に示す．図が示す通り暗号化，復号化ともに必要な処理時間は文字，閾値の増加に伴い増加していることがわかる．ただし，復号化にかかる処理時間については通信の遅延は考慮していない．今回の実装では，暗号化，復号化に要した時間は 1～2 秒弱であった．

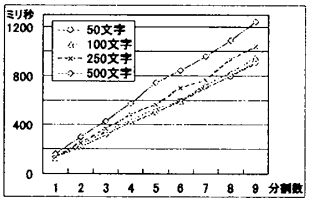

図 5 分割数毎の暗号化に必要な時間

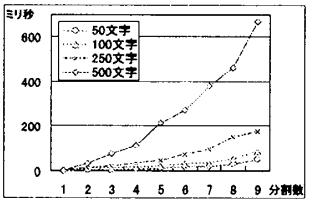

図 6 分割数毎の復号化に必要な時間

4.3. 通信コストについての考察

4.3.1. 同報通信

同報通信を C が行った場合，メッセージ送信の際，グループのメンバ数に比例して通信コストが増加するため，大規模なグループと比較し，多数のスモールグループによる構成の方が，提案手法での通信コストは有利である．[3]で IRC における 1 チャンネルあたりの人数は 90%が 20 人以下であるということが示されており，実運用ではスモールグループが多数であると予想される．ビデオチャットなどの通信量の多いコミュニケーションを行う際に通信帯域が狭くサービスを満足に享受できない，一時的なグループでありメンバ情報が取得されても問題とならない場合，MS に同報送信を委託することで通信コストを削減できる．ただし委託した場合，MS にグループのメンバ情報が取得されてしまい，通信コストとのトレードオフである．

4.3.2. 秘密分散法に対する検討

秘密分散法を使用した場合，データサイズの増加，分割数の増加により，処理時間，通信量が増加するため，同報通信と同様にビデオチャットなどの通信量の多い通信を行う場合には，有効

な手法であるとはいえない．そこで，データ自体に秘密分散法を適用するのではなく，鍵を併用し，鍵に秘密分散法を適用する手法を考える．データを I，提案手法を用いた際の暗号化，復号化にかかる処理時間を $E(\cdot)$, $D(\cdot)$，暗号化に用いる鍵を K，鍵 K を用いた際の暗号化・復号化に必要な時間を $E_K(\cdot)$, $D_K(\cdot)$とすると，$E(I)+D(I)=E(K)+D(K)+E_K(I)+D_K(I)$となるデータ I のサイズが求まる．これが，提案手法を用いた場合と鍵を併用した手法の場合のどちらが効率的かの境界となる．分割数，通信量に関しても同様に，データIと鍵Kのサイズを $S(I)$, $S(K)$，さらに鍵 K による暗号化後のデータサイズを $S_K(x)$とすると $S(I)\times n=S(K)\times n+S_K(I)$となるデータ X のサイズが求まり，分割数・通信量に関して効率的な方法が求まる．

4.4. サーバの不正・故障に対する検討

図 7 より不正サーバの割合が多い場合，情報漏洩しないために閾値を増やすことが有効であるといえる．同様に図 8 より故障サーバの割合が多い場合，情報を正常に届けるためには，閾値を下げることが有効である．なお，分割数は 5 として算出した．

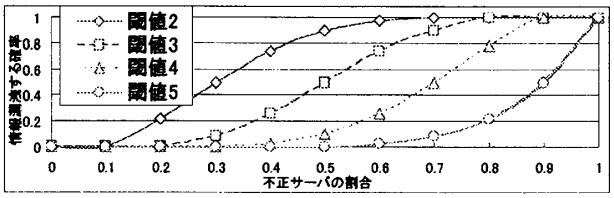

図 7 不正サーバの割合と情報漏洩の可能性の関係(注)

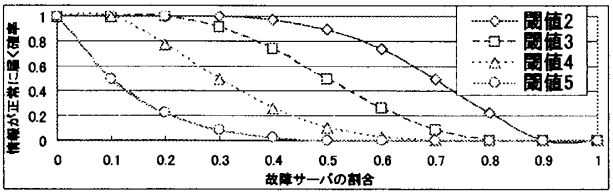

図 8 故障サーバの割合と情報が正常に届く確率の関係(注)

4.5. REG サーバにおける特徴

本手法では，REG の導入により複数の経路をもつ動的なネットワーク構成が可能となる．同様に複数の経路をもつIRCのようなシステムでは，サーバが単一のシステムに比べ負荷分散がなされるが，接続先を直接選択する場合，一部のサーバに負荷が偏る可能性がある．それに対し本手法では，ユーザがサーバリストを取得する際，REG が負荷の少ないサーバを提示しロードバランシングを行うことができる．耐故障性の向上に対しても同様である．

4.6. REG の冗長化

実際の運用では，REG の負荷が問題となることが心配される．REG が停止してしまうと位置情報が取得できなくなるため，サービスの継続が不可能となる．したがって，既存の DNS のような階層化や冗長化を行うことでサービスの継続を図る．ここでは，REG の冗長化に対し，秘密分散法を使用した登録方法を提案する(図 9)．使用するサーバを登録する際に，単一の REG の情報では意味をなさない情報に分割して複数の REG に登録する．そのうちのいくつかが集まると初めて情報となる．図 9 はテキスト秘密分散法で表現されており，■は情報が取得できないことを表している．例えば，URI(C1)REG1 を取得するためには，3 つの REG のうち，2 つ以上の REG に問い合わせることにより URI(C1)REG1 を取得することができる．また，登録サーバ，分割数，閾値の決定権はユーザに委ね，それによりユーザが情報を制御できるようにする．

以上のことより，REG がサービス不能になった場合にも，他の REG を使用することができ，サービスの継続が可能となる．同時に，単一の REG からユーザの情報が漏洩することもなくなる．

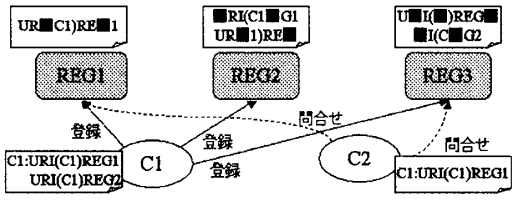

図 9 REG の冗長構成の概念図

4.7. グリッドへの応用

図 10 に示す通り，提案手法はグリッドに対して親和性が高く，REG がロードバランサの役割をすることで適用することができる．また，従来に比べ，ユーザに選択性があり情報発信を制御できるため情報保護をすることができる．

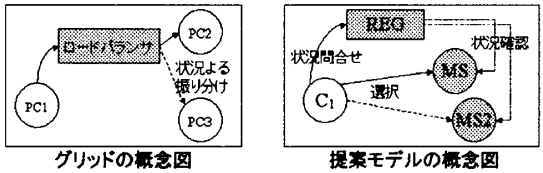

図 10 グリッドと提案手法の比較

5. 関連研究

プライバシー重視のアクセス制御の研究として[4]があるが，双方向のサービスをサポートしない．[5]では，動的グループでの暗号化通信を評価しており，公開鍵を利用した場合の処理時間は，30 人のグループで約 41 秒となっている．なお，実装は Microsoft Visual C++によるものである．一方，本手法で同様のことを行った場合，処理時間は同程度である．本手法の場合，鍵の交換，更新をする必要がないため優位である．また，テキスト秘密分散法[6]との併用により，シェアが意味をもつ文章となり，文章中に秘密情報が含まれているということ自体も隠蔽することが可能である．

6. 結論

本稿では，サーバに取得されるユーザの情報を制限し，さらに秘密分散法の導入により，ユーザのプライバシーを保護し，かつ鍵を必要としないセキュアなネットワークの提案，評価を行った．今後，通信方法，データサイズに関しての効率的な手法や閾値の最適値などを検討していきたい．

参考文献

[1] 小瀬木浩昭，真柄番史，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，Vol. 45, No. SIG7 pp.85-92 (June 2004).

[2] Shamir, A : How to share a secret, *Communication of the ACM*, Vol. 22, No. 11, pp. 612-613 (1979).

[3] 松澤智史，中山雅哉：グループコミュニケーションにおける Small Group Multicast の有用性，分散システム/インターネット運用技術シンポジウム，Vol. 2004, No. 3, pp. 49-54.

[4] 本城信輔ら：プライバシに配慮した WWW システムにおける個人属性認証・アクセス制御システム，情報処理学会論文誌，Vol. 43, No. 8, pp. 2573-2586 (Aug. 2002).

[5] 渡辺浩朗ら：P2P 環境下における動的グループ生成用暗号利用方式の評価，情報処理学会論文誌，Vol. 44, No. 8, pp. 2155-2162 (Aug. 2003)

[6] 滝澤修ら：自然言語テキストを用いた秘密分散法，情報処理学会論文誌，Vol. 45, No. 1, pp. 320-323(Jan. 2004).

(注) 図 7，図 8 の計算は全サーバ数を s，図 7 では不正サーバを w，図 8 では故障サーバを w としての次の式を用いた．

図 7 $\sum_{i=0}^{}({}_{s-w}C_{k+i}\cdot{}_{s-w}C_{n-(k+i)})+{}_sC_n$　図 8 $\sum_{i=0}^{}({}_{s-w}C_{k+i}\cdot{}_wC_{n-(k+i)})+{}_sC_n$