

分散協調による情報保護機構の提案とその応用

Proposal of a Distributed and Cooperative Information Protection and Its Applications

小瀬木 浩昭†
Hiroaki Ozeki

武田 正之‡
Masayuki Takeda

1. はじめに

電子メールや文書変換サービス等、クライアント/サーバ型で提供されるサービスにおいて、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。例えば、電子メールのような会話サービスにおいて、メールサーバの管理者は、利用者が送受信した電子メールの全てを監視・閲覧することが可能である。このような重大な危険性が存在しながら、これまでこの事実は暗黙の了解とされてきた。通信の秘匿は暗号により保持されるが、実際にメールを暗号化して送信することは少ない。共通鍵方式では、事前に相手と暗号に用いる鍵の授受が必要、公開鍵方式では、公開鍵と本人との対応を保障する機構が必要であり、両方式とも鍵を取得した後にその鍵でメッセージを暗号化する必要があり、敷居が高いからである。さらに、メーリングリストでは、上述の条件を満たすことは事実上不可能に近い。

[1]の単にクライアントとサーバの間に身元保証サーバを置き権限認証を利用する手法は、ID と利用者本人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隠匿することはできない。[2]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、2章(ii)で述べるように、オフライン媒体には適用できない等、従来と同様のグループ鍵暗号上の問題を抱える。

本稿では、複数のサーバの連携協調により一つのサービスを構成することで、個々のサーバへの情報集中を防止し、情報統合の未然防止を可能とするモデルを提案する[3][4]。また、提案手法の適用により課題となる、サービスの信頼性と可用性についての改善策を検討する。提案モデルの適用により、個々のサーバの管理者は、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、単一の管理者が顧客に関する情報の全てを掌握することを防止することで、情報漏えいを予防し、サービス運営の管理リスクの軽減と情報セキュリティの向上をもたらす。

2. 本提案モデル

提案モデルは、(i) 機能毎分割、(ii) 同機能選択、(iii) 権限認証、で構成される(図1)。

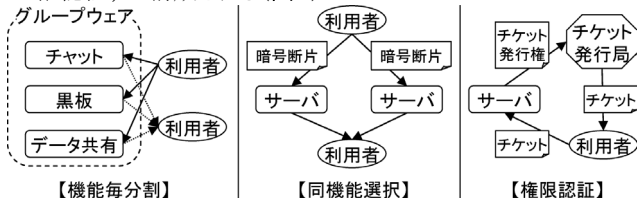


図1 提案モデルの概要

(i) サービスを、それぞれが依存しない機能単位に分割する。各サーバは、利用者の情報のうち、自らが提供する機能に関する情報だけが送受信され、複合サービスにおける情報統合によるプライバシー侵害を防止できる。

†東京理科大学大学院 理工学研究科 情報科学専攻,
Graduate School of 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

(ii) 分割したサービスの内、メッセージ交換や文書変換等、同機能のサービスを選択利用できるサービスについて、サーバを複数設置し利用者が選択的に利用できるようにする。例えば複数のチャットサーバを選択利用できれば、各サーバが収集できる会話情報は全体の一部分となる。さらに、複数の通信経路を同時・選択的に利用できる環境を整備することで、ネットワーク上での閾値暗号[5]の利用が可能となる。閾値暗号との併用により、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授受の必要が無く暗号化通信が可能となる。メーリングリストのような多人数が参加・離脱を行ったり、メンバ全員が常にオンラインで無いなど、従来提案されているグループ鍵暗号方式のようなメンバ間での鍵共有が困難なサービスの利用形態において、提案手法は、閾値暗号との併用により、共有鍵を用いないでサーバから会話情報を秘匿することができるなどの優位性がある。

(iii) 各サーバの認証には、公開鍵基盤を応用した、「権限」に基づく認証機構を整備する。この認証機構により、実世界の次のような状況がネットワーク上で実現される。実社会の、映画館(サーバ)、チケットの売店(チケット発行局)、客(利用者)に例示すると、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、誰が観たかを知らない。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。認証機構の詳細は[3]を参照されたい。

3. 提案モデルの Instant Message への適用

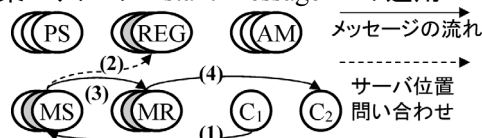


図2 Instant Message の構成とメッセージ送受信の様子

図2は、提案モデルのインスタントメッセージ(IM)への適用例である。IM を、利用者の状態情報を提供するプレゼンス機能 PS、メッセージ送受信機能 MS、MR、分割されたサーバの利用者からの発見を手助けするサーバ位置提供 REG、チケット発行局 AM、に分割した。

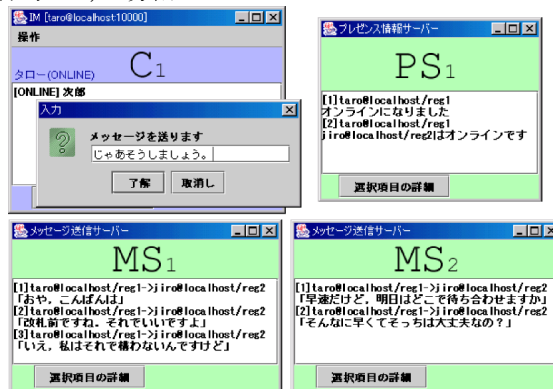


図3 C1とC2の会話において各主体が把握できる情報

図3は、IM の実装画面で、 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 が把握できた情報を表示している。プレゼンス情報については PS だけが、メッセージについては MS_1 , MS_2 がそれぞれ会話の断片情報を取得していることがわかる。

4. 考察

4.1. 従来方式との比較

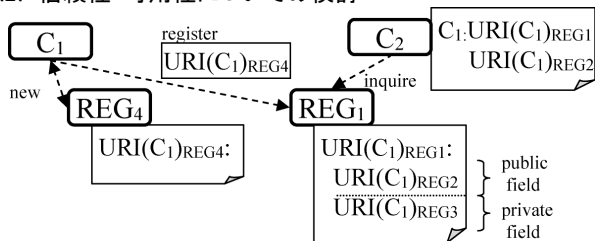
表1 各主体が把握できる C の個人情報

		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

表1は、Instant Message を利用する C の個人情報な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。

4.2. 信頼性・可用性についての検討



【REGの冗長化】

図4 REGの冗長化

IM への適用において、 REG がトラブルで停止すると利用サーバが発見できずサービスが十分に享受できない可能性がある。本節では、 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(図4)。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。本方式は、 C の必要に応じて冗長化の範囲・規模が決めることと、 REG への登録情報の伝播を C が制御できることによりプライバシーに配慮できる、などの長所があると考えられる。

4.3. 適用性

提案手法の適用性に関して考察する。手法が効果的に適用できるものとしては、チャット、電子メール等、利用者同士がサーバを介してコミュニケーションを行なう双方向型会話サービスがあげられる。また、文書データ形式変換サービス等の、前回の利用状態に依存しない関数型サービスへの適用も効果的であると考えられる。サービスの性質上、サーバにデータ本体を与えざるを得ないが、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。独立した複数のサービスの組み合わせで提供される複合サービス、サーバに対して情報を秘匿化困難な状況下や、サーバに情報が集中・統合することを防止したい要望が高いシステムにおいて、本手法は有効に働くと考えられる。

5. 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。現在、定量的な評価を進め、大規模な運用における検討課題に取り組んでいる。本手法は、サーバに情報を管理している様々なサービスにおいて有用であると考えられる。今後、検討課題を克服し、本手法が広く普及する為に必要な条件を整備して行きたい。

参考文献

- [1] 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).
- [2] 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).
- [3] 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).
- [4] 小瀬木 浩昭, 真柄 喬史, 武田 正之: 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—, 分散システム/インターネット運用技術シンポジウム(DSM2004), pp.13-18 (Jan. 2004).
- [5] Shamir, A: How to share a secret, Communication of the ACM, Vol.22, No.11, pp.612-613 (1979).