様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月１８日現在

機関番号：14301
研究種目：挑戦的萌芽研究
研究期間：2009～2011
課題番号：21650016
研究課題名（和文）　段階的秘密交換プロトコルを利用した配達内容証明可能な電子メールシステム
研究課題名（英文）　Contents-certified e-mail delivery systems using the Gradual Secret Exchange Protocol
研究代表者
岡部　寿男（OKABE YASUO）
京都大学・学術情報メディアセンター・教授
研究者番号：20204018

研究成果の概要（和文）：電子メールなどの電子文書の配達において、第三者を介することなく、配達内容の証明機能を付加することを目的とする。本研究では、まず岡本、太田の段階的秘密交換プロトコルを利用した電子メールプロトコルを開発・実装し、その成果を国際会議 SAINT 2009 にて発表した。次に、その手法の問題点を検討し、安全性を残したまま計算量を削減したより単純なプロトコルを提案した。これを実装し、性能評価を行なった結果、30MB 程度のサイズの文書に対する内容証明が可能ということが分かった。この成果を国際会議 SAINT 2011 にて発表した。

研究成果の概要（英文）：The purpose of this research is to develop a contents-certified e-mail system without a trusted third party, using the so-called Gradual Secret Exchange Protocol. We first developed an e-mail protocol using Okamoto and Ohta's protocol, and implemented it. We presented this result at SAINT 2009. We then discussed problems of the previous protocol, particularly on its high computational complexity. To complement this, we improved the protocol, simplifying the previous one while retaining security. We implemented it and conducted experiments, which shows that our new system can treat documents of size up to 30MB. We presented this result at SAINT 2011.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,100,000	0	1,100,000
2010 年度	1,100,000	0	1,100,000
2011 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,100,000	270,000	3,370,000

研究分野：計算機ネットワーク
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：インターネット、電子メール、配達内容証明、マジックプロトコル、段階的秘密交換プロトコル、暗号、一方向関数

１．研究開始当初の背景

インターネットの浸透に伴い、オンライン取引やビジネス上の契約など重要な情報のやりとりがネット上で行われることが増えている。中でも電子メールはネット上の情報交換の中核的な手段であるが、その発展上の経緯から性善説に基づく枠組みで構築されている部分が

大きく、従来の郵便システムと比べて欠けている点が少なからずある。自分が送りたい相手にメールが届いたかどうかを相手の善意なしに確認する、送達確認や内容証明が困難であることもその一つである。ここでは送達確認と内容証明を同時に行うことを「配達内容証明」と呼ぶ。

電子メールの配達内容証明を扱った研究には、大別して、仲介人となり送信者と受信者の双方から信頼されうる第三者機関(Trusted Third Party;TTP)を利用するものと、TTP を仮定せず、送信者－受信者の二者間でやりとりが完結するかあるいは仲介人を利用しても信頼する必要がないものに分類することができる。TTP を介する方法はすでに ISO13888 として標準化もされており、また USPS（米国郵政公社）の『Certified Mail』など商用サービスも提供されていた。一方、TTP を仮定しない方法は、双方が信頼できる第三者を必要とせず余分なコストが生じない、第三者に通信の内容を明らかにする必要がない、など、第三者を介する方法に比べて明確なメリットが存在する。しかしながら、段階的秘密交換プロトコルと呼ばれる理論研究はあるものの、実用システムに向けた研究・開発は TTP を利用するプロトコルに比べてほとんど進んでいなかった。

２．研究の目的

本研究では、上記のような現状を踏まえ、第三者を利用しない一対一の内容証明を可能とするプロトコルを、電子メールの拡張として設計し、一般に利用しやすい形で電子メールシステムとして提供することを目的とした。

甲乙二者が持つ秘密をそれぞれ相手に伝え、甲が乙の秘密を受け取った場合は必ずかつその時に限り乙が甲の秘密を得るような手順を「秘密交換」と呼ぶ。TTP を仮定せずに秘密交換を実現する方法として、「段階的秘密交換プロトコル(gradual secret exchange protocol)」が知られている。これは、秘密データを相手に持ち逃げされる可能性を減ずるために、 データを一度に送付せず、暗号化して送付した上で、暗号鍵を細かい断片に分割してそれぞれ交互に送信することによって、情報交換者のどちらか一方だけが相手のデータ全体を持ち逃げすることを困難にするものである。

本研究では、段階的秘密交換プロトコルとして、岡本らによる一方向置換を用いた同時秘密交換プロトコルをベースとしたものを用いることとし、正確性と公平性を保ちつつそれを実際の計算機上で効率的に実現する方法を検討し詳細設計する。それに基づきやりとりされるメッセージのフォーマットを規定するとともに、電子メールクライアントソフトウェアとして実装して、利用者の煩わしい操作なく段階的秘密交換が行われるようにする。

公開鍵暗号に基づく電子署名と暗号の理論は、公開鍵認証基盤(PKI)として広く社会に展開され、Web のアクセスにおける SSL 通信をはじめ日常的に利用される実用技術に成熟している。本研究は、同じような考え方で、段階的秘密交換の理論に基づく実用技術を開発し、メールの送達確認ならびに受信者による送達の否認を防止できるようになり、電子メールにおける電子署名・暗号化方式である S/MIME や PGP などと組み合わせて用いることで、インターネットを安全・安心な社会基盤へと高めるための着実な一歩となると考える。

３．研究の方法

まず、段階的秘密交換のためのプロトコルの設計とメッセージフォーマットの規定を行う。本研究では、前提として、すべてのメッセージが RFC2822 に基づくインターネットメッセージでやりとりされるものとし、電子メール配送以外の特別のプロトコルが利用できることを仮定しない。すなわち、送信者と受信者の間で RFC2822 に基づくメッセージの交換ができることだけを前提とし、それ以外のプロトコルが利用できなくても配達内容証明ができるようにする。

利用者に面倒な操作の繰り返しを強いることは現実的でないことから、送信者と受信者双方の MUA (Mail User Agent)による自動処理を前提に設計する。特に送信者の側でメールを送信後、能動的な動作の必要なく受領の通知を待てばよいような設計は「Send-and-Forget」と呼ばれ、利用者の負担を考慮する上で非常に有用である。

この際、できるだけ利用者側の操作を防ぐために、受信側 MUA は、配達内容証明付メールとして届いた最初のメッセージに対して受信者が配達内容証明の手続きを開始したら、以後はそれに対する応答メッセージは特別なものとして扱い、受信者の関与なく自動的に処理して応答を送る。同様に、送信側 MUA は、自らが送信した配達内容証明付メールに対する応答メッセージは特別なものとして扱い、送信者の関与なく自動的に

処理して応答を送る。送信側 MUA、受信側MUAとも十分短い時間間隔で定期的にメールサーバに対してPOPなどによりメールを取り込むような設定にしておく。実装には sendmail や OpenSSL などの既存の OSS を活用する。

さらに、ソフトウェアの完成度を高めるとともに、配達内容証明および不正が生じた場合の第三者への証明の自動化について詳細化を行う。配達内容証明だけでなくやりとりが途中で中断した場合においても、どこまでのやりとりが完了しどこで相手が不正を行った可能性があるかの証明を自動化する。利用者が、このプロトコルに関する詳細な知識なしに、トラブルに巻き込まれた場合に第三者に立証するための手続きをシステムとして提供できるようにする。そのために、プロトコルの各段階において起こりうる不正を系統的かつ網羅的に列挙し、それぞれを防ぐために必要な証跡を相手の署名付で受領し自動的に記録するようにする。

４．研究成果

まずは現状の調査を行った。その結果として分かった(1) 配達証明付き電子メールサービスの現状、(2) プロトコル開発研究の現状、について、以下に報告する。

(1) 電子メールでの配達証明は商用化も進んでおり，その枠組は ISO13888 として標準化されている．海外で提供されているサービスの例としては，Goodmail Systems の CertifiedEmail，DataMotion の SECURE MAIL などがある。また国内でも，NTT コミュニケーションズの V-Pack，IIJ のセキュア MX サービスでの GDX Mail などがあり，到達性を保証している．しかしいずれも，サービスプロバイダがTTPとして機能しており，プロバイダの信頼性にシステムは依存してしまう．

(2) Nenadic 他や今本他は、TTP を用いない方法の場合の問題点を挙げ，TTP を利用した電子メールの配達証明の手法を提案している．しかし、Ray 他は，TTP はシステムのボトルネックとなってしまうため，TTP に依存しない公平な秘密交換プロトコルが，よい研究対象となりうるだろうと述べている．Even 他、岡本他、Barhreman 他は，忘却通信、一方向性置換、ビットコミットメント，ゼロ知識証明などの暗号プロトコルを用いて、TTP を用いないプロトコルを提案している．

次に、(2)のうち岡本らのプロトコルを用いて、具体的にメール交換を実現する手法を提案し、国際会議 SAINT 2009 にて発表した。

さらに、SAINT 2009 で発表したプロトタイプに対する問題点を指摘し、これに対する改良を行なった。段階的秘密交換プロトコルでは、最初に秘密を（内容を明かさないまま）相手に預け、その秘密と同じ秘密を各ステージごとに送信する。もし最初に預けた秘密と異なるものが送られてきた場合には、即座にその不正を確認できる。しかし、最初に預けた秘密が実際と異なるものであった場合は、不正を最後まで見抜けないことになる。また、段階的秘密交換プロトコルは毎ステージ公開鍵暗号を使った暗号化と復号を行うため、計算コストが高い。この理由から、段階的秘密交換プロトコルを使用しない設計とした。安全性については、即座に不正を見破ることが出来るという制約を緩め、最終的に相手の不正を第三者に証明できればよいものとした。これにより、プロトコルの簡単化と計算コストの削減を達成した。また、受領証を陽に定義せず、受信者からの確認応答を持って受領証としたため、送信者側の全探索による不正を原理的に不可能とした。この結果、非対称なプロトコルとなり、計算能力に差がある二者間でも公平にプロトコルを実行することができるという利点が出来た。次に、このプロトコルを実装し性能を評価した。実装モデルは以前の実装と同じものを用いた。実装には JAVA 言語を用いた。5 つのテストファイルを用いて研究室内の LAN で通信実験をし、(i) 送信ファイルの暗号化、(ii) プロトコルの実行にかかる時間をそれぞれ計測した。その結果、本実装では 30MB 程度のファイルを扱うことができることを確認できた。

以上の内容を、ドイツで開かれた国際会議 SAINT 2011 に投稿し採録され、発表した。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 10 件）

① 島岡政基，片岡俊幸，谷本茂明，西村健，山地一禎，中村素典，曽根原登，岡部寿男，“大学間連携のための全国共同認証基盤UPKIのアーキテクチャ設計　（招待論文）”，電子情報通信学会論文誌，Vol.J94-B, No.10, pp.1246-1260, Oct. 2011.

② 谷本茂明，島岡政基，片岡俊幸，西村健，山地一禎，中村素典，曽根原登，岡部寿男，“大学間認証連携のためのキャンパスPKI共通仕様(研究速報)”，電子情報通信学会，Vol.J94-B，No.10，pp.1383-1388，Oct. 2011.

③ Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Daisuke Inoue, Masashi Eto, Koji Nakao, “A Comparative Study of Unsupervised Anomaly Detection Techniques Using Honeypot Data”, IEICE Transactions on Information and Systems, Vol.E93-D, No.9, pp.2544-2554, Sep. 2010. （査読有）

④ 大平健司，宋中錫，高倉弘喜，岡部寿男，“様々なアプリケーションへの攻撃活動を察知する汎用性の高いハニーポットシステムの構築と運用”，電子情報通信学会論文誌，Vol.J93-D，No.7（システム開発論文特集号），pp.1125-1134，2010年7月．（査読有）

⑤ 鈴木和也，馬場俊輔，和田英彦，中尾康二，高倉弘喜，岡部寿男，“状況把握のためのトラヒック振る舞い分類システムの構築と評価”，電子情報通信学会論文誌，VolJ93-B，No.7（システム開発・ソフトウェア開発論文特集号)，pp.916-927，2010年7月．（査読有）

⑥ 大平健司，隅岡敦史，北岡有喜，古村隆明，藤川賢治，岡部寿男，“公衆無線インターネット接続サービス「みあこネット」の設計と運用”，電子情報通信学会論文誌，Vol.J93-B，No.5，pp.759-768，2010年5月．（査読有）

⑦ Mitsuo Okada, Yasuo Okabe, Tetsutaro Uehara, “Privacy-Secure Image Sharing System for a Purchaser and Recorded Subjects Using Semi-Blind Fingerprinting”, Procedia - Social and Behavioral Sciences, Vol.2, Issue 1, pp.137-142, Mar. 2010.

⑧ 鈴木和也，馬場俊輔，和田英彦，中尾康二，高倉弘喜，岡部寿男，“複数手法によるリアルタイム解析を支援するトラヒックデータ配送システムの実装と評価”，電子情報通信学会論文誌，Vol.J92-B，No.10（セキュアでサステイナブルなインターネットアーキテクチャ特集号），pp.1619-1630，2009年10月．（査読有）

⑨ 鈴木和也，馬場俊輔，和田英彦，中尾康二，高倉弘喜，岡部寿男，“迅速な障害対応を支援するトラヒック可視化システムの構築と評価”，電子情報通信学会論文誌，Vol.J92-B，No.7（システム開発・ソフトウェア開発論文特集号），pp.1072-1083，2009年7月．（査読有）

⑩ Jungsuk Song, Hiroki Takakura, Yasuo Okabe and Yongjin Kwon, “Unsupervised Anomaly Detection Based on Clustering and Multiple One-class SVM”, IEICE Transactions on Communications, Vol.E92-B, No.6, pp.1981-1990, Jun. 2009. （査読有）

〔学会発表〕（計34件）

① Yasuo Okabe, “The University PKI Architecture in Japan and the LoA”, Tao of Attributes Workshop, Kyoto, Dec.2, 2011.

② 西村健，中村素典，山地一禎，大谷誠，岡部寿男，曽根原登，“日本における学術認証フェデレーション“学認”の展開”，大学ICT推進協議会2011年度年次大会，2011年12月2日.

③ 大神渉，古村隆明，岡部寿男，“プライバシ情報の逆流出に対するSAML/Shibbolethの仮名性強化手法”，平成23年度情報処理学会関西支部支部大会，F-30，2011年9月22日.

④ Wataru Oogami, Takaaki Komura, Yasuo Okabe, “Toward Robust Pseudonymity in Shibboleth/SAML Federation against Backflow of Personal Information”, AsiaFI, 2011 Summer School, August.21, 2011.

⑤ Satoshi Ishibashi, Shuichi Miyazaki, and Yasuo Okabe, “Design and Implementation of a Certified Document Delivery System without a Trusted Intermediate Authority”, The 11th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT2011), pp. 20-26, July.22, 2011. （査読有）

⑥ 岡部寿男，“信頼のおけるアイデンティティ連携の確立に向けて：学術認証フェデレーション「学認」”，Security Day 2010，2010年12月22日.

⑦ 石橋聡，宮崎修一，岡部寿男，“第三者機関の仲介を必要としない配達証明付き電子メールシステムの設計”，信学技報，vol. 110, no. 304, IA2010-54, pp. 19-24，2010年11月24日.

⑧ 山地一禎，中村素典，片岡俊幸，西村健，Tananun Orawiwattanakul，曽根原登，岡部寿男，“学術認証フェデレーションGakuninの本格運用”，第27回インターネット技術第163委員会（ITRC）研究会CIS分科会，2010年5月20日.

⑨ 中村素典，山地一禎，片岡俊幸，西村健，庄司勇木，古村隆明，岡部寿男，

“学術認証フェデレーションを活用するサービスの展開”，第27回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会，2010 年 5 月 20 日.

⑩ 古村隆明，岡部寿男，中村素典，“SAML 連携を用いてロケーションプライバシを守る eduroam アカウント利用方式”，信学技報，vol. 109, no. 438, IA2009-109, pp. 153-158, 2010 年 3 月 1 日.

⑪ 西村健，島岡政基，中村素典，曽根原登，岡部寿男，“UPKI 証明書自動発行検証プロジェクトのシステム移行における課題と対策”，信学技報，vol. 109, no. 438, IA2009-113, pp. 225-228, 2010 年 3 月 1 日.

⑫ 島岡政基，西村健，中村素典，曽根原登，岡部寿男，“UPKI サーバ証明書プロジェクトにおける証明書自動発行支援システムの開発”，信学技報，vol. 109, no. 438, IA2009-114, pp. 229-234, 2010 年 3 月 1 日.

⑬ 西村健，島岡政基，並木登美幸，樋口秀樹，中村素典，岡部寿男，曽根原登，“サーバ証明書プロジェクトに見る共同利用基盤の構築と移行”，全国共同利用情報基盤センター研究開発論文集，No.31，pp.99-103，2009 年 11 月 6 日.

⑭ Keita Shimizu, Shuichi Miyazaki, Yasuo Okabe, “Design and Implementation of a Certified Mail Exchange System Using Simultaneous Secret Exchange”, The 2009 International Symposium on Applications and the Internet (SAINT2009), pp. 37-42, July.22, 2009. （査読有）

⑮ Toshiyuki Kataoka, Takeshi Nishimura, Masaki Shimaoka, Kazutsuna Yamaji, Motonori Nakamura, Noboru Sonehara, Yasuo Okabe, “Leveraging PKI in SAML2.0 Federation for Enhanced Discovery Service”, The Third Workshop on Middleware Architecture in the Internet (MidArc2009) (held as a part of SAINT2009), July.21, 2009. （査読有）

〔図書〕（計 1 件）

① 岡部寿男，情報ネットワーク(5 章，6 章,12 章担当）共立出版(未来へつなぐデジタルシリーズ 3)，2011 年 11 月.

〔その他〕

ホームページ等

http://www.net.ist.i.kyoto-u.ac.jp/ja/index.php?%CF%C0%CA%B8

６．研究組織

(1)研究代表者

岡部　寿男（OKABE YASUO）

京都大学・学術情報メディアセンター・教授

研究者番号：20204018

(2)研究分担者

宮崎　修一（MIYAZAKI SHUICHI）

京都大学・学術情報メディアセンター・准教授

研究者番号：00303884