講演番号：66

マルチアカウントを活用したセキュア電子メールの性能評価

Performance Evaluation of Secure E-Mail System utilizing Multi-Accounts

B－6

篠原 峻輝† 宮保 憲治† 上野洋一郎†
Shunki SHINOHARA† Noriharu MIYAHO† Yoichiro UENO†
† 東京電機大学 情報環境学部 情報環境学科
† School of Information Environment. Tokyo Denki University

1. はじめに

電子メールサービスでは高速性に加え,セキュアな通信が求められ,ユーザ・プロバイダ間に SSL/TLS を用いた方法や,S/MIME を用いたエンド-エンド間での暗号化方式が適用されている.しかし,異なるプロバイダ間の中継時に,暗号方式変換の為に平文化が行われる場合もある.また,エンド-エンド間での暗号方式においても認証局（第三者機関）が公開鍵や送信者を保証するための運用管理上の問題が存在している.

前述した状況に鑑み，本稿では,HS-DRT(High Security-Distribution and Rake Technology)のコア技術[1]およびマルチアカウントを積極的に活用した,よりセキュアな電子メール[2]を提案し,実機により確認した性能評価を述べる.

2. 提案方式

提案方式の構成概要を図 1 に示す.提案方式では,Gmail などのフリーメールや組織で使用するメールなど,異なる通信事業者を同時に使用し,一つのメールを複数の断片メールに分割し，断片の地理的な経路分散を図る.その際,各々の断片メールは暗号化され，かつ全ての断片が集まらない限り解読困難となるため,全経路で同時に盗聴されない限り，第三者による解読は不能である.送信側では,メールの本文と添付ファイルを組み合わせた後に，HS-DRT 機能を用いて暗号化,分割を行う.元のメッセージに復号するための鍵情報を同時に作成し,これらのメッセージを相手クライアントへ異なる経路を用いて転送することでセキュリティ向上化が図れる.

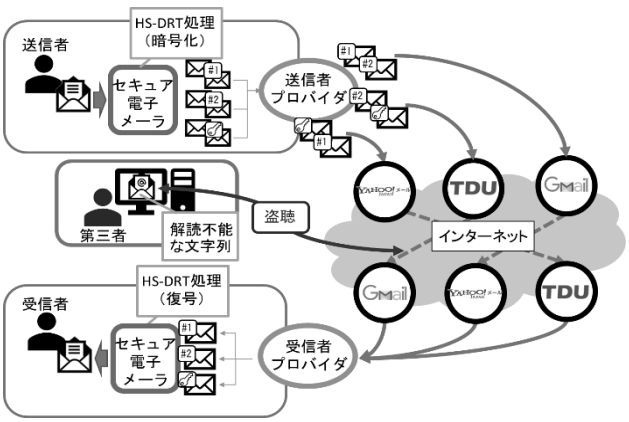

図１ セキュア電子メールシステムの構成概要

3. 性能評価

実験環境としては JavaScript，C++などを用い,当該の暗号処理機能を搭載したメールクライアントを開発した.

メールクライアントの開発に当っては，メールサーバが断片メッセージをスパムメールと誤認しない送信間隔に留意し,その条件下で処理時間を評価した.安全性を重視するため,HS-DRT 処理の適用時の分割数は 80 回,一体化数は 6 回とした.本実験では基本性能の評価に主眼を置き,複製処理は省略した.送信メールのサイズを 10～50MB と変化させ,暗号処理が開始されてから全断片メールの送信が完了するまでの時間(総計時間)を測定・評価した．評価結果を図 2 に示す.図 2 より,断片メッセージの送信間隔累積時間が全体の総計時間に占める割合は最も大きいことが判明した．また，分割ファイルサイズの増加による処理の適正化を図ることで，より短い送信間隔時間での送信が可能であることが判明した.

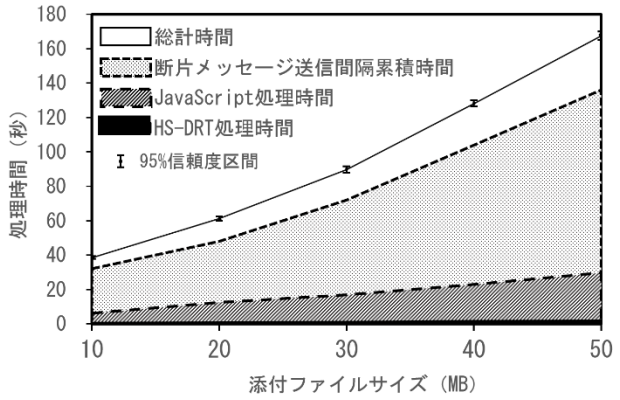

図 2. 送信側プログラムにおける処理時間

4. まとめ

HS-DRT 技術を活用したセキュア電子メールを提案し,送信メールを多数のファイルへ分割・暗号化した際の送信間隔を最適化し,実際にかかる送信時間を測定・評価した.今後は,多様な条件下での送信間隔の測定データを分析し,自動的に最適な送信間隔を判定し，適用できる電子メール方式の検討を進める.

5. 参考文献

[1] N. Miyaho, S. Suzuki, Y, Ueno, et all. Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications" IARIA Journals, vol.3, no.1, pp.276-278, 2010.
[2] 宮保他,“電子メールシステム”特願 2016-88837.28.4.27.