講演番号： 59

ディザスタリカバリ技術を応用したセキュア電子メールシステムの検討

B-6 Study of Secure E-Mail System using Disaster Recovery Technology

高橋 佑太† 宮保 憲治† 上野洋一郎†
Yuta TAKAHASHI† 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

現在，コミュニケーションツールとして電子メールの普及が進み，個人だけでなくビジネスにおいても利用されている．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ている．そのため,ユーザ・プロバイダ間にSSL/TLS (Secure Socket Layer/Transport Layer Security)を用いて安全にメール配送を行う方法が一般的である．しかしながら，送受信者のアカウントを管理するプロバイダ同士の中継区間(メールサーバ間)では，SSL/TLS が用いられない場合がある．加えて，メールサーバで保持されるメッセージファイルは平文であるため，盗聴や情報漏洩に対しても安全性を担保できる対処策を設ける必要がある．

一方，S/MIME ではエンド-エンドでの暗号化が行われるが，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上の問題や公開鍵暗号の活用による速度低下の問題が指摘されている．

前述した状況に鑑み，HS-DRT (High Security-Distribution and Rake Technology)のコア技術[1]及びマルチアカウントを活用したセキュアな電子メールを提案した[2]．

本稿では，従来，機能検証のために既存のメールクライアントのプラグインとして C 言語を用いて実装したプログラムに対して，ディザスタリカバリ機能を含めた電子メールクライアント全体を新規に実装し，将来の機能追加・検証の容易化を実現すると共に，ユーザビリティの向上を図った．更に，JavaScript を用いて実装した HS-DRT 処理の性能向上を図るため,C++で置換して再実装した.当該メールクライアントの性能評価を計測した評価結果を以下に述べる．

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 や組織のメールなど，異なるメールサービスのアカウントを複数個使用することで，複数の異なる転送経路を用いて，暗号化・断片化されたメールの送受信を行う電子メール配信を実現できる．送信側では，ストリーム暗号処理と一体化処理[1]を組み合わせて暗号化後，複数のメッセージに分割する(以後，断片メッセージと呼称)．元のメッセージに復号するために必要な鍵情報が記述されたメッセージ(以後，メタメッセージと呼称)を同時に作成し，これらの全てのメッセージを相手クライアントへ，異経路を用いて転送する．全ての断片メッセージは暗号化されたまま，相手側の複数のプロバイダへ送信され，受信端末に到達するため，中継区間での盗聴を不可能にできる．受信側では全断片メッセージとメタメッセージを受信した後，メタメッセージに記述された鍵情報を用いて，元のメッセージを復号する．

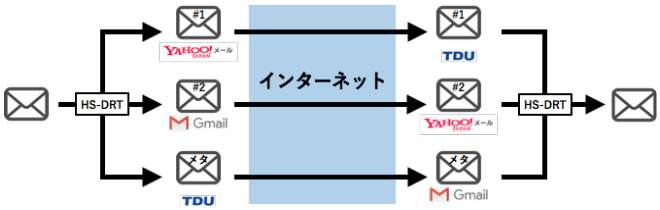

図 1. セキュア電子メールシステムの構成概要

3. 性能評価

実験環境としては JavaScript，C++などを用いて，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．

本稿では，1.で述べたように，本メールクライアントのプログラム処理の最適化を行い，処理時間を比較評価した．具体的に，1MB から 5MB までのメッセージを送信する際の処理時間を計測し，有効性を定量的に評価した．評価結果を図 2 に示す．図 2 より，C++を最適に活用して実装することにより，5～6倍の高速化を実現すると共に，データサイズ増加時のオーバヘッドの減少を図ることができた．C++を最適に実装することで,大容量の添付ファイルを含むメッセージ送信に対しても，分割数を適切に選択することにより，本提案方式の有効性は飛躍的に高められることを検証した．

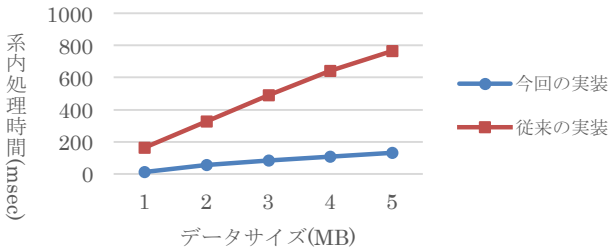

図 2. 送信側のプログラムにおける処理時間

4. まとめ

セキュアな電子メール方式の C++による最適実装を提案し，従来のプラグイン方式における処理性能の低下に関わる問題を解消できることを定量的に示した．今後は，多様な閾値秘密分散方式を導入した電子メール方式の検討を進める．

参考文献

[1] N. Miyaho, S. Suzuki, Y. Ueno, et al. “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] 宮保憲治他，“電子メールシステム” 特願 2016-088837, 2016.