講演番号：75

マルチアカウントを用いたセキュア電子メール用サーバの実験評価

B－6　Evaluation Experiment of Secure E-Mail Server using Multi-Account

柳澤　宏伎†　宮保　憲治†　上野　洋一郎†
Hiroki Yanagisawa†　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

従来の電子メールシステムでは，メールデータの転送を，中継サーバを介してバケツリレー式に行い，相手先のアドレスまでメッセージを送り届ける方法が一般的である．このため，メールの内容が利用するプロバイダの中継サーバ等で解読される可能性や第三者がアクセス可能なメールサーバに蓄えられた段階で，盗聴される可能性がある．

上記の課題解決のため，ディザスタリカバリシステム 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，利用者のメーラに HS-DRT 機能を内蔵させたセキュア電子メールシステムを提案した[2]．本稿では上記の HS-DRT 機能を利用者が最初にアクセスするメールサーバに実装し，性能評価を行った．

2　提案方式

提案するメールサーバの方式構成を図 1 に示す．送信サーバではユーザからの送信要求の度に，対象メッセージに対して HS-DRT 処理を行い，複数のアカウント宛に閾値秘密分散方式に則り，断片メッセージと，元のメッセージに復号するために必要な情報が記述されたメタメッセージを，中継サーバ宛に送信する．その後，メタメッセージの収集に必要な情報が記述されたメタデータキーを，受信サーバのアドレス宛に送信する．通信相手側に配備された受信サーバでは，メタデータキーの受信を検知すると，その情報を基にメタメッセージを検索し，復元を行う．その後，メタメッセージの情報を基に断片メッセージを検索し，元のメッセージを復号する．

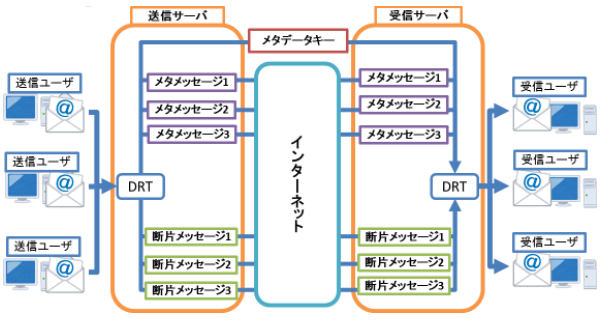

図 1 提案したメールサーバの方式構成

3　性能評価

実験環境として C++, Xmail 等を使用し，HS-DRT 機能を搭載したメールサーバを実装した．HS-DRT 処理の適用に当っては，一体化処理 6 回，分割数 10，(2, 3) 閾値秘密分散処理を採用した．各断片・メタメッセージ送信の際は，中継相手先のプロバイダからスパムメールと誤認されないようにキューイング機能を追加し，同時接続ユーザ数が増加しても等間隔で断片メッセージを送信する機能を実装した．本実験ではユーザからの送信要求毎にキューを設定する方式(方式 1)と断片・メタメッセージの送信毎にキューを設定する方式(方式 2)の 2 パターンに対して同時接続ユーザ数を変化に対応した通信時間の測定を行い，比較評価した．方式 1 と方式 2 の構成図を図 2 に，実験結果を図 3 に示す．同時接続ユーザ数が増加するほど方式 1 が方式 2 よりも平均通信時間が短くなることが判明した．また，方式 1 は平均通信時間の分散が小さく，通信が安定している．一方，方式 2 は平均通信時間の分散が大きく，通信時間にばらつきがあることが判明した．

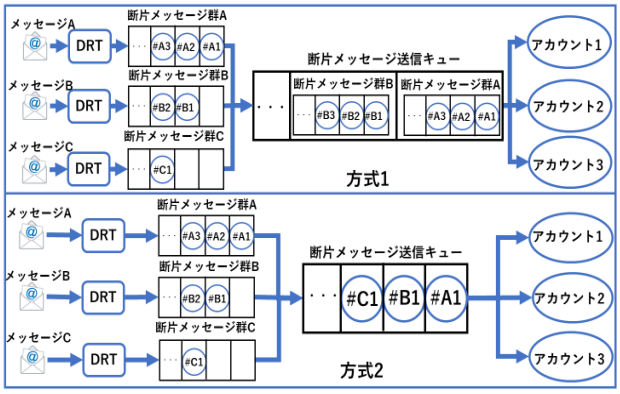

図 2 キュー構成図

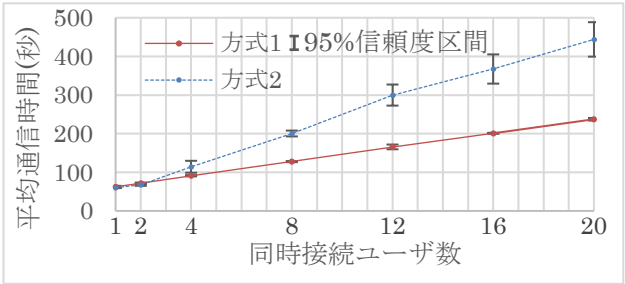

図 3 2 方式の平均通信時間

4　まとめ

従来の電子メールサーバを，複数のメールアカウントを使用し，かつ HS-DRT 機能を活用することで，セキュリティの向上と効率転送を実現する HS-DRT メールサーバとして実装する方式を提案した．本方式の性能評価を行うことで，適用領域を明確化した．

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.