TLSにおける電子メールに特化した圧縮方式の性能評価*

熊谷祐輔† 木村成伴‡ 海老原義彦‡

筑波大学 第三学群 情報学類†
筑波大学大学院 システム情報工学研究科‡

1 はじめに

TLS (Transport Layer Security)はアプリケーションに認証，暗号化，改竄検出及び圧縮の機能を提供する．TLSで利用できる圧縮アルゴリズム DEFLATE は汎用圧縮アルゴリズムであるため，送信するデータによっては圧縮率が低下するなどの問題があった．これを踏まえ，著者らはアプリケーションに特化した TLS のための圧縮方式を提案している[1][2]．文献[2]では電子メールに特化した圧縮方式を提案している．本研究では，この圧縮方式を IMAP に適応したときの性能評価を行う．

2 電子メールに特化した圧縮方式

TLS では，アプリケーションから送られてきたデータをフラグメントに細分化し，これらに対して圧縮と暗号化の処理を施す．しかし，全てのフラグメントを一律に圧縮するため，その内容によっては圧縮率が低下する．本章では，電子メールに特化した圧縮方式[2]について述べる(図 1参照)．

2.1 データの細分化

電子メールでは US-ASCII 文字しか送ることができない．このため，電子メールにバイナリファイルを添付する場合，バイナリファイルを US-ASCII 文字にエンコードする他，ファイルの境界やファイルの種類，エンコード方式などを MIME 形式で表記する．これを利用し，文献[2]の方式では，電子メールのデータをテキストデータとエンコードされたバイナリデータに切り離し，各々でフラグメントに分割する．

2.2 データの圧縮

バイナリデータをエンコードしたまま圧縮すると，エンコードせずに圧縮した場合と比べて圧縮率が下がる可能性がある．このために，エンコードされたバイナリデータは，元のバイナリデータにデコードする．その後，テキストデータとバイナリデータを圧縮するが，後者のデータについては未圧縮の場合のみ圧縮する．

2.3 データのマージ処理

圧縮後のデータサイズの多少から元のデータの種類を推測しやすくなる．そこで，圧縮後のデータにここで用いた圧縮方式やエンコード方式，及び圧縮後のデータ長からなるヘッダを付加し，これらのデータをマージしたものを一定長に分割してから暗号化を行う．

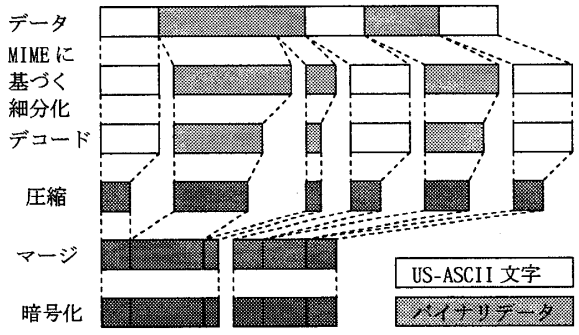

図 1 電子メールに特化した圧縮方式におけるデータの処理

3 評価実験

評価実験はサーバマシンとクライアントマシンの 2 台を使用して行う．サーバマシン及びクライアントマシンの CPU は Pentium4 3.0GHz，OS として FreeBSD 5.5，TLS として OpenSSL 0.9.8a に DEFLATE 及び電子メールに特化した圧縮方式を追加したものを用いる．サーバマシンでは IMAP サーバアプリケーションとして courier-IMAP 4.2.1，クライアントマシンでは IMAP のクライアントアプリケーションとして Sylpheed 2.4.7 を用いる．サーバマシンとクライアントマシンは 1Gbps の LAN で接続し，様々な回線速度を実現するために，IPFW 及び dummynet を用いて帯域制限をかける．

3.1 圧縮率の比較

まず，圧縮無し，DEFLATE 及び電子メールに特化した圧縮方式の電子メールの圧縮率を比較す

*Performance Evaluation of the TLS Compression Method Specialized for E-mail
†Yusuke Kumagai, College of Information Science, Third Cluster of College, University of Tsukuba
‡Shigetomo Kimura and Yoshihiko Ebihara, Graduate School of Systems and Information Engineering, University of Tsukuba

るために，各方式でファイルを添付した電子メールを実際に圧縮した結果を図 2に示す．ここで，添付したファイルには US-ASCII テキスト，文字のみを入力した Word ドキュメント及び JPEG ファイルを用いた．各ファイルは約 40KByte である．Word ドキュメントは無圧縮の，JPEG ファイルは圧縮済みのバイナリファイルである．また US-ASCII テキストを添付すると BASE64 エンコードを行うクライアントもあるため，US-ASCII テキストに関しては BASE64 エンコード無し及び有りの両方においての圧縮率を計測した．図より，電子メールに特化した圧縮方式は DEFLATE と比較して，BASE64 エンコードでファイルを添付した電子メールの圧縮率が 3.28%～35.52%高くなることが分かった．

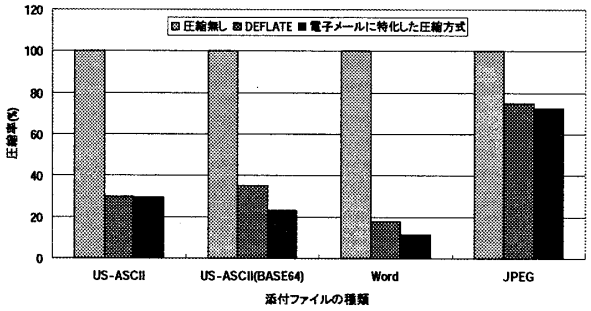

図 2　圧縮方式ごとの電子メールの圧縮率

3.2　転送時間の比較

圧縮無し，DEFLATE 及び電子メールに特化した圧縮方式それぞれで 3.1 節で用いたファイルを添付した電子メールを実際に 10 回転送し，その平均転送時間を測定した結果を図 3に示す．電子メールの転送には，IMAP を使用した．また，回線速度は実際のアクセスラインを想定し，64kbps，3Mbps 及び 1Gbps に設定した．図 3から，電子メールに BASE64 エンコードでファイルを添付した場合，電子メールに特化した圧縮方式では DEFLATE よりも電子メールの転送にかかる時間が 2.53 %～32.82 %短いことが分かった．また，回線速度を上げて転送するファイルのサイズが転送時間に及ぼす影響を少なくしても，電子メールに特化した圧縮方式は圧縮無しや DEFLATE と転送時間がほぼ同じであり，圧縮率やセキュリティの問題を解決するために 2 章で追加された処理によって特に大きな負荷は追加されていないと言える．

4　まとめ

本研究では TLS における電子メールに特化した圧縮方式を IMAP に適応させたときの性能評価を行った．今回の実験では回線速度を上げることでファイルサイズが転送時間に及ぼす影響を少なくし，その上でファイルの転送時間を比較することで処理にかかる時間の比較を行ったので，各圧縮方式の転送時間を抜いた処理のみの時間の正確な比較はできていない．そこでファイル転送の処理を省き，各圧縮方式の処理のみにかかる時間の比較を行うことで，電子メールに特化した圧縮方式の正確な負荷の追加について調査することが今後の課題である．

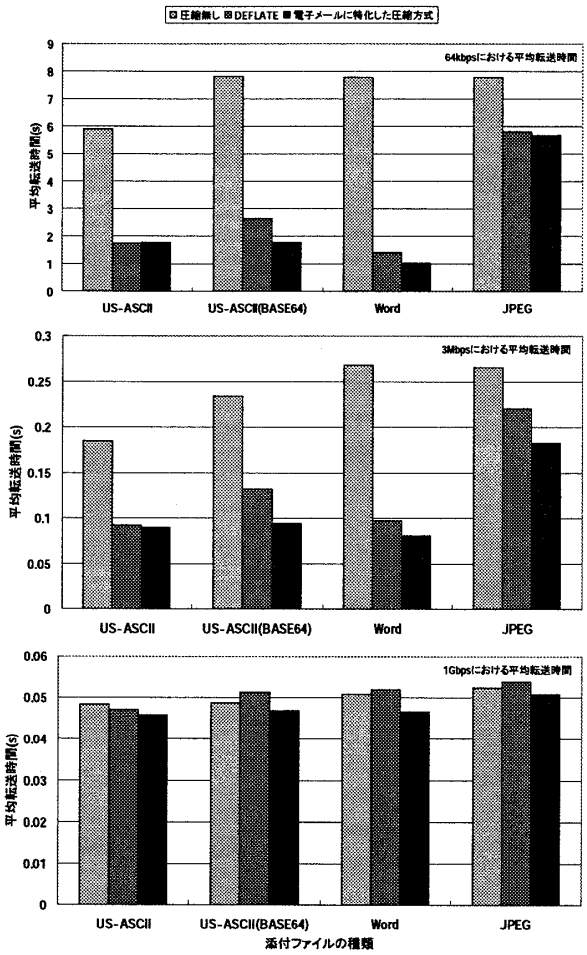

図 3　電子メールの平均転送時間

5　参考文献

[1] N. Okamoto, S. Kimura, and Y. Ebihara, “An Introduction of Compression Algorithms into SSL/TLS and Proposal of Compression Algorithms Specialized for Application,” Proceedings of AINA2003, pp. 817-820, March 2003.

[2] D. Manabe, S. Kimura, and Y. Ebihara, “A Compression Method Designed for SMTP over TLS,” Proceedings of ICOIN2006, pp. 803-812, January 2006.