中継サーバを利用した暗号通信の実現*

1S－1

堤 俊之　藤岡 秀樹†
日立ソフトウェアエンジニアリング(株)‡

1　はじめに

インターネットは、電子メールや電子ニュース、ファイル転送、遠隔ログインといった、インターネットを有効に利用できるアプリケーションの開発によって、大きく発展してきた。近年では、World Wide Webと呼ばれるハイパーテキスト的ユーザインタフェースを用いた情報探索システムの出現により、文字や音声、画像などのマルチメディア情報を手軽に通信できるようになり、注目を集めている。また、商用インターネットが運用を開始して、インターネットにおける商業的な利用も始まっている。

一方、インターネット上での通信は、通信データの盗聴、改ざんといった危険性があるため、個人情報や取引情報、機密情報といった重要なデータの通信が簡単に行えない状況にある。そこで、盗聴や改ざんを防止できる通信サービスの提供するために、様々な研究が行われている。例えば、標準的なプロトコルにセキュリティ機能を付加する研究(swIPe[1])や、アプリケーション自身がセキュリティ機能を実現する方式(PEM)が提案されている。しかし、それら研究成果は、実装するためにオペレーティングシステムやアプリケーションを変更する必要性があり、通常ソースコードを入手できない既存オペレーティングシステムや市販アプリケーションには適用することが難しいという問題がある。

そこで、本論文では、オペレーティングシステムに変更を加えずに、既存のサーバクライアントシステムに安全な通信を提供する枠組として、中継サーバを利用した方式を提案する。また、実装したシステムの性能測定した結果について報告する。

2　通信の危険な範囲

本論文では、サーバやクライアントの起動するマシンの属している組織内ネットワークの通信は安全であるとする。通信が安全であるとは、盗聴、改ざん、なりすまし、といった危険にさらされないことである。

逆に言うと、サーバのある組織内ネットワークとクライアントのある組織内ネットワークの間の通信が上記の危険にさらされているので、これらの問題を解決する必要がある。

3　中継サーバを利用した暗号通信システム

3.1　システムの概要

暗号通信システムは、既存のサーバとクライアントが直接通信を行うのではなく、中継サーバを介して行うものである。図1にその構成を示す。既存クライアントからのデータは、同一組織内ネットワークにある既存クライアント側のスレーブ中継サーバに送られる。スレーブ中継サーバは、データを暗号化して復号処理に必要な制御データと一緒に既存サーバ側のマスタ中継サーバに転送する。マスタ中継サーバは受信したメッセージを復号化して既存サーバに送信する。こうして、中継サーバ間で通信されるデータの盗聴や改ざんを防止することができる。

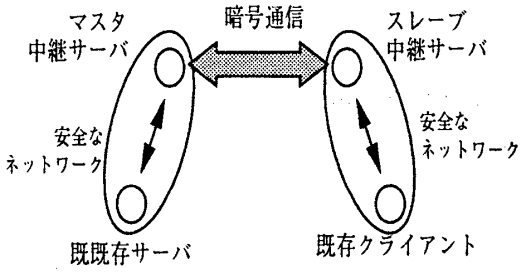

図1: システムの概要

3.2　システムの特徴

本システムは、通信の危険を防止しつつ、既存サーバクライアントシステムの運用に支障をきたさない応答時間を実現できるように、以下に示す特徴を持っている。

1. 暗号・復号と応答時間
   盗聴を防止する暗号化・復号化は計算コストの大きな処理なので、応答時間を長くする原因となり、

*Development of Secure Communication with Proxy Servers
†Toshiyuki Tsutsumi, Hideki Fujioka
‡Hitachi Software Engineering Co.,Ltd.

インタラクティブな通信を要求するアプリケーションに対応できない場合がある。そこで、秘密鍵暗号方式を利用して、運用に支障をきたさない応答時間を実現する。

2. 改ざんの検出
第三者による通信内容の改ざんを完全に防止するのは、大きな処理コスト必要として、応答時間を伸ばすことになる。そこで、本システムでは一方向性関数を利用した認証用データを付加して、改ざんの有無を検出して、改ざんの防止を実現している。

3. 中継サーバのなりすまし防止
中継サーバになりすますことができると、盗聴や改ざんの危険が発生する。そこで、チャレンジレスポンス認証方式を利用して中継サーバ間の認証を行い、なりすましを防止している。

4. 暗号鍵の交換のタイミング
秘密鍵暗号方式を利用する場合、同じ暗号鍵を長時間使用することは第三者が 暗号鍵を発見する手助けとなる。 一方、暗号鍵を交換することはそれ自体コストの大きな処理でなので、 頻繁な暗号鍵の交換は応答時間を長くする結果に繋がる。そこで、本システムではコネクション毎に暗号鍵の交換を行い、安全性と応答時間のバランスを保っている。

5. 暗号鍵の交換方法
暗号鍵の交換は公開鍵暗号方式を利用する方法が一般的であるが、この方式は計算コストの高い処理である。そこで、本システムでは秘密鍵暗号方式の暗号鍵を暗号鍵交換用とデータ暗号用の２つ用意して、暗号鍵交換用の暗号鍵を中継サーバ間で予め共有し、必要に応じてデータ暗号用の暗号鍵を暗号交換用の暗号鍵で暗号化して交換するようにしている。

4 性能測定

実装したシステムを利用して既存サーバクライアントシステムを起動した時の応答時間を測定した。

4.1 環境

実装として秘密鍵暗号方式には Multi2 暗号 [2] を、一方向関数には MD5 ハッシュ関数を利用している。

既存サーバとマスタ中継サーバは同一のマシンに、既存クライアントとスレーブ中継サーバはそれぞれ別のマシンで稼働している。それぞれのマシン性能を表1に示す。

表 1: 実装システムの構成

マシン機能	ハード・ソフト構成
データベースサーバ 既存サーバ側中継サーバ	CPU: 486DX2 66MHz Memory: 52MB
既存クライアント側 中継サーバ	CPU: 486DX2 66MHz Memory: 52MB
表示クライアント	CPU: 486DX2 66MHz Memory: 40MB

4.2 結果

既存サーバクライアントシステムとして、データベースサーバに蓄積されたデータをクライアントが画面に表示するシステムを利用し、(1) アプリケーションの起動、(2) 文字データの表示、(3) グラフデータの表示、(4) 履歴データの表示、の操作を行うものとする。

表 2には、中継サーバを使用しなかった場合の通信回数と通信量および応答時間と、中継サーバを利用した時の応答の増加時間を示す。

結果より、既存システムに支障のある応答時間の増加でないことが確認できる。

表 2: 通信回数と通信バイト数、応答時間、増加時間

項目	(1)	(2)	(3)	(4)
通信回数 (回)	70	57	10	160
通信バイト数 (B)	4308	7887	1452	25021
応答時間 (秒)	43.1	12.9	13.5	17.5
増加時間 (秒)	+1.2	+0.2	+0.8	+0.0

5 おわりに

本論文では、中継サーバを利用した暗号通信システムの提案を行った。これにより、オペレーティングシステムに変更を加えずに、既存のサーバクライアントシステムに安全な通信を提供することができる。また、提案したシステムを実装して性能測定を行った結果、実用的な応答時間で通信を行うことが確認できた。今後は、様々な既存システムに適応していく予定である。

参考文献

[1] IOANNIDIS, J. and M.BLAZE, The architecture and implementation of network-layer security under unix, Proceedings of the Fourth Usenix UNIX Security Symposium (10 1993).

[2] 宝木和夫 他２名 マルチメディア向け高速暗号方式, 電子情報通信学会技術研究報告 マルチメディア通信と分散処理 (5 1989).