6Q-01

電子マネー向けファイアウォールの検討

佐久間 剛★
エヌ・ティ・ティ コミュニケーションズ★
e-mail : t.sakuma@ntt.co.jp★

竹内 宏典★★
NTT 情報流通プラットフォーム研究所★★
take@dsa.isl.ntt.co.jp★★

1. はじめに

インターネットの普及に伴い、企業内に構築されたネットワークはファイアウォールを介してインターネットに接続され企業間や消費者との間でインターネットを経由した電子的な取引が行われるようになってきた。このような電子的な取引の決済手段の1つに電子マネーがあり、実証実験も多く行われている。[1]ネットワーク上で電子マネーをやり取りする場合、セキュリティを確保するため、一般的に秘匿通信（暗号化）が行われる。このためファイアウォールを通過するデータも暗号化されており、従来のファイアウォールで実施している上位レイヤーのプロトコル通過制御は困難になっている。本稿では、電子マネーの伝送特性に着目したファイアウォール通過制御方式を検討し電子マネーを利用するシステムのセキュリティ向上を図る。

2. 電子マネーの伝送特性

一般的な電子マネーの主な伝送特性を以下に示す。

(1) 秘匿通信

従来のバンキングシステム等で用いられていた専用ネットワークに比べて、電子マネーで用いるインターネットは第3者による盗聴・改竄などの危険性が大きい。このため電子マネーの伝送時にはデータの暗号化が行われる。例えば、下位の通信プロトコルとしてSSLが用いられている。

(2) 署名通信

また、インターネットを介した通信は成りすましの危険性もある。このため通信時に相手を確認（認証）する署名通信が行われている。例えば、SSLを利用してサーバ認証が行われている。

(3) セッション制御

さらに、上位の通信プロトコルでは電子マネーの正当性を保証するため複数のセッションで確認・送受信などを実施している。このため電子マネーの伝送時にはセッション制御が行われている。例えば、電子マネーが格納されているICカードの認証のためのチャレンジレスポンスや途中でネットワーク障害などが発生し通信が切断されたときに正しく再開するための同期点制御が行われている。

3. 課題

電子マネーの伝送特性を考慮してシステム構築をした時の課題を以下に示す。

(1) ファイアウォールは、主にパケットフィルタリング機能・アプリケーションゲートウェイ機能でデータの通過制御を行い許可したアクセスのみを内部ネットワークに接続することでインターネットからの不正アクセスなどの攻撃を防御している。しかし、秘匿通信の場合データが暗号化されているため、平文での通信に比べファイアウォールで十分な通過制御を行うことができずパケットフィルタリング機能のみになり、DoS攻撃や不正データの侵入を防ぐことができない。この結果、内部のサーバが直接インターネットに曝されやすい問題点がある。

(2) 電子マネーでは電子署名を用いた認証を実施し第3者から成りすましによる不正なデータなどの攻撃を防いでいる。しかし、電子マネーは利用者の匿名性を確保しているため、データの認証はできても利用者の認証ができないため不正アクセス時に攻撃者を特定することが難しい。

(3) 現状の監視方法は、アクセスされた各サーバのログを元に不正進入の検知を行っている。しかし、電子マネーは複数のセッションで通信するためアクセスログだけでは何を実施したかわからない問題点がある。さらに、不特定多数のアクセスがあるためネットワーク上のマシン毎に監視を行うと情報が氾濫し適切な管理が難しく、マシン毎にログを表示するため、アクセスされたクライアント毎に通信経路を関連付けて監視する事ができない問題点がある。

4. 提案方式

これらの課題を解決するために「SSL代理応答方式」[2]と「統合ログ監視方式」[3]を用いた検討を行った。

○ SSL代理応答方式

クライアントからの暗号通信データは、サーバまで直接送信されずにいったんSSL代理応答システムで受信して平文に復号化した後にファイアウォールを再度通過させてサーバに送信される。これによりファイアウォール上でアプリケーション層の通過制御が可能となる。（図1）

A Study of Firewall for Electric Money
Tsuyoshi SAKUMA★, Hironori TAKEUCHI★★
NTT Communications★
NTT Information Sharing Platform Laboratories★★

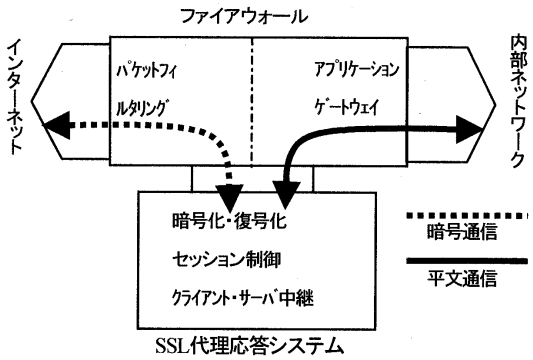

図1　SSL代理応答システム図

SSL 代理応答方式により秘匿通信機能がないサーバも秘匿通信が可能となり、通信上の盗聴・改竄などの不正ができなくなる。

○ 統合ログ監視方式

統合ログ監視マシンに集められ分析されたログをクライアント毎にシステム内のアクセス経路を時間順に表示する。選択された経路での各マシンの詳細なアクセス情報を表示する。(図2)

また、クライアント単位・一定時間単位で統計する機能を持つ。

(表示例　経路)

```
[Client IP:Port]192.168.128.64:2000
[経路情報]     FW->SR->FW->AP
[処理数] 15 [正常] 12 [異常] 3
```

(表示例　詳細)

[Client IP:Port]
192.168.128.64:2000

```
[経路情報]     [完了、詳細情報]
FW->SR          OK  TCP/IP Connect
FW->SR          OK  Client Hello
FW<-SR          OK  Server Finished
    SR->FW->AP OK TCP/IP Connect
FW->SR->FW->AP OK CMD_A
FW<-SR<-FW<-AP OK ANS_A
FW->SR->FW->AP OK CMD_B
```

図2　画面表示例

統合ログ監視方式によりインターネットからのアクセス経路(マシンのアクセス順)の追跡が可能になり、どこから不正アクセスがあったか調査することが可能となり、同様の不正アクセスを防ぐことができるようになる。

5. 解決方法と構成

2つの方式を用いて電子マネー向けのシステム構築を行った。以下に各課題の解決内容を示す。

(1) クライアントからのアクセスがSSL代理応答システムを介してサーバへ行われるため、サーバへの直接攻撃はされない。これにより、Dos 攻撃などの大量接続攻撃はファイアウォールまたはSSL代理応答システムで防ぐことができる。

(2) インターネットからの入り口であるSSL代理応答システムで電子証明認証してシステム内のアクセス経路を監視することにより不正アクセス時の攻撃者を特定することができる。サーバ側では利用者の認証を行わないためサーバに対する匿名性は保つことができる。

(3) 統合ログ監視マシンに各サーバのログを収集・分析し統合表示することによりシステム管理者の負担を軽減させることができる。また、システム内のアクセス経路を追跡でき、不正アクセスの進入経路の追跡や手段を把握することができる。

「SSL 通過制御方式」と「統合ログ監視方式」を用いた電子マネーシステム構成を示す。(図3)

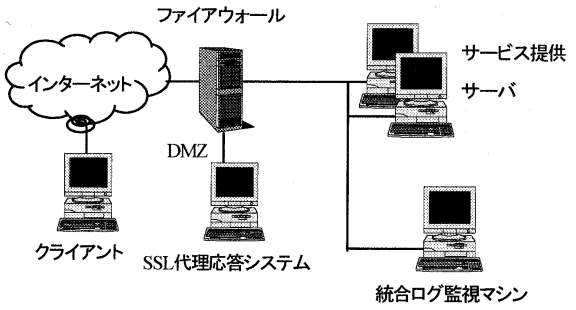

図3　システム構成図

6. まとめ

電子マネーシステムに要求されるセキュリティを満足させるため、本稿では暗号化された電子マネーの通過制御方式の検討と複数のサーバマシンにおける不特定多数のアクセス監視の効率化及びアクセスの追跡が可能な監視方式の検討を行い、電子マネーに適したシステム構成を提案した。

7. 謝辞

本研究は、通信・放送機構(TAO)委託研究「電子マネーの伝送技術に関する研究開発」の課題イ「電子マネーの伝送特性に着目したファイアウォール通過制御技術の研究開発」の一環として実施されたものである

8. 参考文献

[1] インターネットキャッシュ(http://www.icash.gr.jp/)
スーパーキャッシュ(http://www.s-cash.gr.jp/)他
[2]佐久間,河田「SSL暗号通信の通過制御に関する一考察」第58回情報処理学会全国大会(平成11年前期)
[3] 佐久間,竹内「アクセスログの監視方法に関する検討」2000年電子情報通信学会総合大会(平成12年3月)