1T－8

多段ファイアウォール環境に対応したVPN構築方式の提案

萱島 信‡　藤山 達也‡　寺田 真敏‡　小泉 稔‡　平山 和成†
（株）日立製作所 システム開発研究所‡
（株）日立製作所 ソフトウェア開発本部†

1．はじめに

近年、企業間や事業部間をオープンなインターネットで接続して協調連携したいというニーズが大きくなっている。その一方で、企業内／事業部内の各部門では、それぞれ独自に持っている重要情報について、他部署からの権限を越えたアクセスからガードしたいというニーズもある。前者のニーズに対応する技術がインターネット上に仮想的な専用線を提供するVPN(Virtual Private Network)であり、一対のファイアウォールもしくはルータに暗号通信機能を組み込むことで実現される[1]。一方、後者のニーズは企業や事業部の単位だけでなく、部門単位できめ細かくファイアウォールを設置することで対応できるが、結果としてファイアウォールが多重に設置されることになり、従来の一対のファイアウォールを用いたVPNでは対応できないという問題が発生する。

本論文では図1のように多段ファイアウォール環境下でVPNを実現できるVPN構築方式として「シームレスVPN」を提案する。シームレスVPNは、多重にファイアウォールが設置された環境を前提に、正しいユーザが途中のファイアウォールを意識することなく、通信相手の部門との情報交換を可能とするもので、従来のVPNのデータ暗号化機能に加えて(1)ファイアウォールにおいてユーザ認証を行い、指定された通信先へのアクセス権限をチェックする「ユーザベースアクセス制御機能」、および(2)正しい権限を持ったユーザのデータをファイアウォールが連携して目的の部門まで安全に中継する「中継経路制御機能」を各ファイアウォールに搭載することにより実現される。

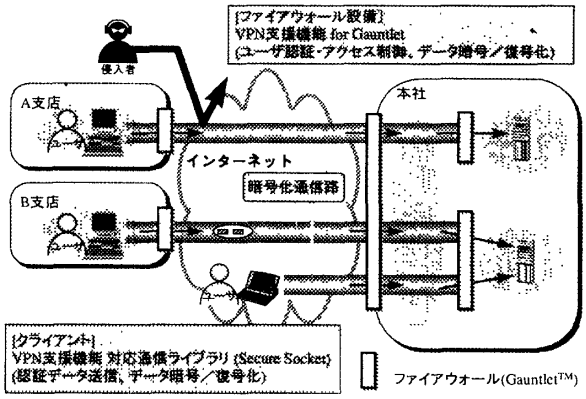

図1．シームレスVPN適用環境

2．シームレスVPNの構成要素及び機能

シームレスVPNの構成要素を図2に示す。

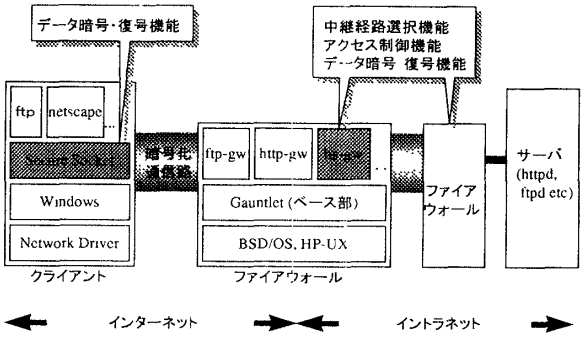

図2．システム構成図

シームレスVPNは、socksV5[2]と同様に(1)フ

Proposal of VPN construction method for multiple firewall environment.
Makoto KAYASHIMA, Tatsuya FUJIYAMA, Masato TERADA, Minoru KOIZUMI, Kazunari Hirayama
HITACHI Ltd.

ァイアウォール上に設置したトランスポートレイヤゲートウェイプログラム(hs-gw)と、(2)クライアント用セキュリティ機能付きソケットライブラリ(Secure Socket)により構成される。シームレスVPNは、hs-gwに「ユーザベースアクセス制御機能」と、「中継経路制御機能」を持たせることにより、多段のファイアウォール環境下で、ユーザが途中のファイアウォールを意識することなくTCPベースのアプリケーションプログラムを利用できる環境を提供する。

2.1 ユーザベースアクセス制御機能

シームレスVPNでは、クライアントがサーバまでの経路上のすべてのファイアウォールとISO/IEC9798-2[3]で規定された共有鍵による相互認証を実行する。クライアントと各ファイアウォールで共有する暗号鍵はユーザ毎に異なるものであり、ファイアウォールではユーザ単位でのアクセス制御を行っている。また、通信データの暗号化は、ISO/IEC9798認証手順を実行する際に交換したデータを元にセッション鍵を生成するようになっている。

通信データ暗号化に使用する暗号方式は、通信開始時にネゴシエーションにより決定する。現在は日立が開発した(1) MULTI暗号あるいは、(2)圧縮機能と暗号化機能を融合した新開発の圧縮暗号化方式を用いているが、将来的には他の暗号方式を利用することもできるようになっている。

2.2 中継経路制御機能

図3のようなネットワーク構成例で、food.co.jpドメイン内のサブネットワークfruit.food.co.jpとvegetable.food.co.jpがそれぞれ内部のファイアウォールlemonとpotatoで防御されている場合、サブネットワークvegetableのクライアントcarrotが、サブネットワークfruitのサーバkiwiに接続するためにはlemonでの明示的な認証動作が必要であった。

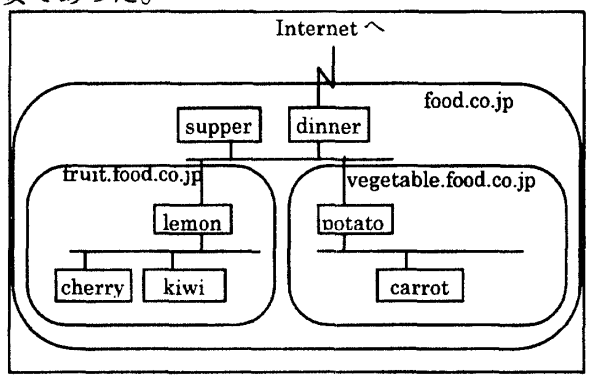

図3.ネットワーク構成例

シームレスVPNでは、各ファイアウォール上に設置したhs-gwが通信先ネットワークとそのネットワークへの中継を担当するhs-gwの対応関係を記述した中継経路テーブルを持ち、クライアントの通信要求に応じて適切なhs-gwに接続することにより、複数のファイアウォールでネットワークが分断された環境をユーザに意識させずにＶＰＮを構築することができる。

3. おわりに

大規模なイントラネットを想定した多段ファイアウォール環境において、透過的なアクセスを実現するシームレスVPNシステムを提案した。本システムの持つユーザ単位のきめ細かいVPNの構築は、今後のインター／イントラネット環境において重要な役割を果たすものと考える。

参考文献

[1] IPSec, IETF RFC1825～1829

[2] SocksV5, IETF RFC1928

[3] ISO/IEC9798-2,Information technology Security techniques -Entity authentication -