4G-5　ＶＰＮ(Virtual Private Network)構築技術の検討・管理手法

宮川 明子　後沢 忍　時庭 康久　稲田 徹　永嶋 規充
三菱電機（株） 情報技術総合研究所

１．はじめに

近年、ネットワークシステムが多様化、大規模化したことに伴い、ネットワークの管理手法に対する関心が高まっている。特に、VPN システムを構築する場合、セキュリティという観点からも管理手法を検討することは、非常に重要である。

本稿では、VPN システムを対象に、システムを運用していく上で必要な管理機能の中から VPN 装置を制御している管理装置と VPN 装置の間でやりとりされる管理通信に着目し、留意すべき点とその対策方法について提案する。

２．管理機能

VPN システムは、VPN 装置と管理装置によって構成される。VPN システムの構成を図１に示す。

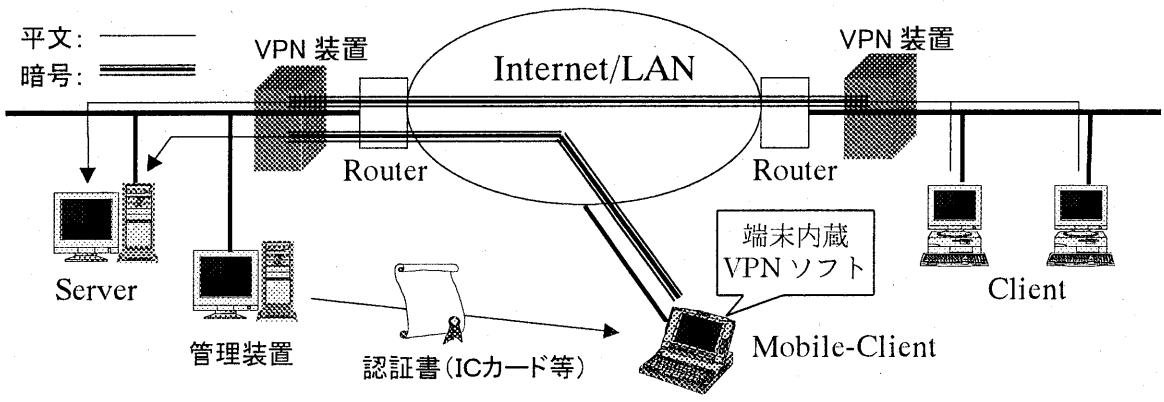

図１：VPN システムの構成

図１のような VPN システムに必要な管理機能として、主に次に示す３つの機能が考えられる。

（１）通信制御機能：各 VPN 装置の稼動状況を監視し、適切な設定・変更を行う

（２）認証書管理機能：VPN 装置毎の認証書情報を取得し、管理情報として活用する

（３）操作表示機能：管理装置において、各 VPN 装置の情報表示、編集を行う

このうち、（１）は VPN システムにおいて、VPN 装置の鍵交換や緊急時の対処など最も多岐にわたる機能である。我々は、この（１）の機能を管理装置と VPN 装置との独自プロトコルによる通信によって実現しており、本稿ではこの通信のことを管理通信と呼ぶ。

管理通信を利用することによって、管理装置での GUI 操作による VPN 装置のリモート管理が可能となり、システムの管理負荷を軽減している。

A Study of Management for VPN System

Akiko MIYAGAWA, Shinobu USHIROZAWA, Yasuhisa TOKINIWA, Toru INADA and Norimitsu NAGASHIMA
Information Technology R&D Center, Mitsubishi Electric Corporation 5-1-1 Ofuna, Kamakura, 247 Japan
(E-mail : m-akiko@isl.melco.co.jp)

3．管理通信における留意点

（1）セキュリティ対策

管理通信では、VPNシステムを運用していく上で重要な情報がやりとりされるため、この通信が正常に機能しない場合、VPNシステムの致命的な損害を引き起こす危険性がある。したがって、盗聴、改竄、なりまし、リトライ攻撃といったネットワーク上の脅威について、十分な対策を取る必要がある。

そこで、我々は、送受信する情報（管理コマンド）に認証のためのデータ部を設けた、UDP上の独自プロトコルによる管理通信を実現している。セキュリティ対策を施したプロトコルにはセキュアSNMPやSSL等もあるが、これらの標準プロトコルは既製品の管理ツールにVPN装置の存在を知られやすい、独自プロトコルの方が顧客のニーズに合わせてカスタマイズしやすいという観点から、独自プロトコルを採用した。図2に管理コマンドフォーマットの概略を示す。各フィールドの意味は以下の通りである。

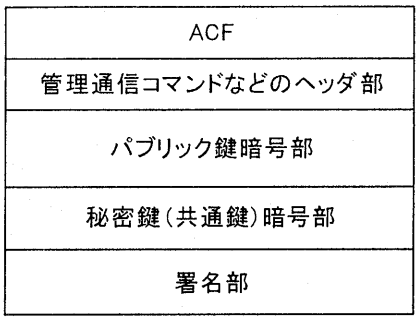

図2：管理コマンドフォーマットの概略

- ACF（Anti-CrackingField）
  リトライ攻撃対策用の乱数を利用したハッシュ値
- 管理通信コマンドなどのヘッダ部
  管理コマンドの種別情報で、処理高速化のため平文データ
- パブリック鍵暗号部
  なりすまし防止用の公開鍵暗号による認証用暗号化データ
- 秘密鍵暗号部
  盗聴防止用の共通鍵暗号による送信内容の暗号化データ
- 署名部：改竄防止用の公開鍵暗号による暗号化データ

（2）処理時間の考慮

暗号化によるセキュリティ対策の一方で、暗号化処理が増える分だけ、管理通信処理にかかる時間も長くなる。公開鍵暗号部だけでも盗聴防止にはなるが、図2では、演算時間の長い公開鍵暗号部だけでなく、暗号処理が高速な秘密鍵（共通鍵）暗号部も併用することによって、管理通信処理時間を短縮している。

また、管理通信では、送信情報のサイズによるフォーマットサイズの調整を行っている。送信データが大きくなると、管理通信の送信パケットはネットワーク上でプロトコルスタックにより自動的にフラグメントされるが、フラグメントされたパケットの内一つでも消失すると、消失したパケットのシーケンスだけでなく、もう一度初めから再送される。このようなシーケンスの再送をできるだけ少なくするため、送信情報のサイズがIPのMTUを超える場合、あらかじめ送信データを分割して送信することによって、伝送効率を上げている。ただし、複数回に分けたデータが確実に受信されたことを双方で確認するために、管理コマンドフォーマットにシーケンス番号を付け、受信側ではシーケンス番号による処理制御を行うことが必要となる。

4．まとめと今後の課題

本稿では、VPNシステムにおける管理機能の概要と、管理機能の一つである通信制御を実現する管理通信について、留意点および対策方法を述べた。

今後は、モバイル端末からのリモートアクセスを含めた管理手法として、ICカード等を利用したVPN利用者の認証方法の検討、より快適で安全なVPNシステムの実現のためQoSやポリシー管理との連携を課題としたい。

参考文献

[1] 後沢他：“暗号によって構成されるVPNとその管理手法”，信学技報IN97－113