個人対応ＶＰＮ(Virtual Private Network)の概念

1Ｕ－6

後沢　忍　稲田　徹　宮川　明子
三菱電機（株）情報技術総合研究所

1．はじめに

インターネットなどのオープンネットワークを利用して、イントラネットやエクストラネットを構築するケースが増えている。これらのネットワークに対して、専用線と同等の安全性を確保するための技術として、暗号によるVPN(Virtual Private Network)がある。初期のVPNの発想は、専用線からの単純な置き換えであり、インターネット利用によるコストの削減が主な目的であった。最近では、ネットワーク犯罪の大半が社内犯行であるというレポートもあり、社内ネットワークも１つのオープンネットワークと見なし、目的に応じたVPNを構築する技術が求められている。

目的に応じたVPNとは、例えば人事や経理といった部門毎のVPNや複数部門に跨るプロジェクト単位のVPNなどである。これらは情報の性質によってVPNを構築するものであり、その情報を扱うことのできる個人の権限がVPNに反映されていると言える。本稿では、個人の権限とVPN構成単位との関連付けに着目し、個人対応のVPN構築手法について述べる。

2．ＶＰＮのモデル

筆者らが以前考案したシステム[1],[2]は、既存のネットワークに暗号装置（若しくは暗号ソフト）をアドオンすることによってネットワーク上を流れるデータを暗号化するものであり、インターネットに限らず社内LAN等に対しても広く適用できる（図１）。図１のモデルを本稿の議論のベースとする。

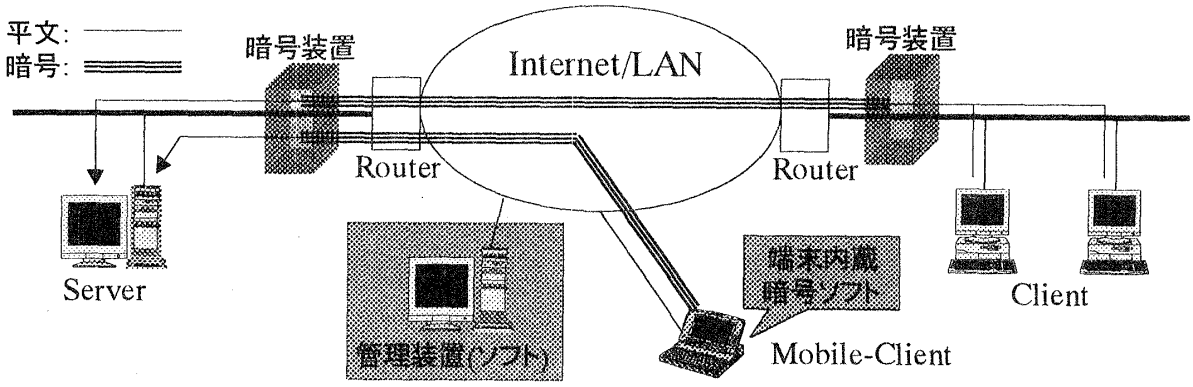


図１．個人対応ＶＰＮモデル

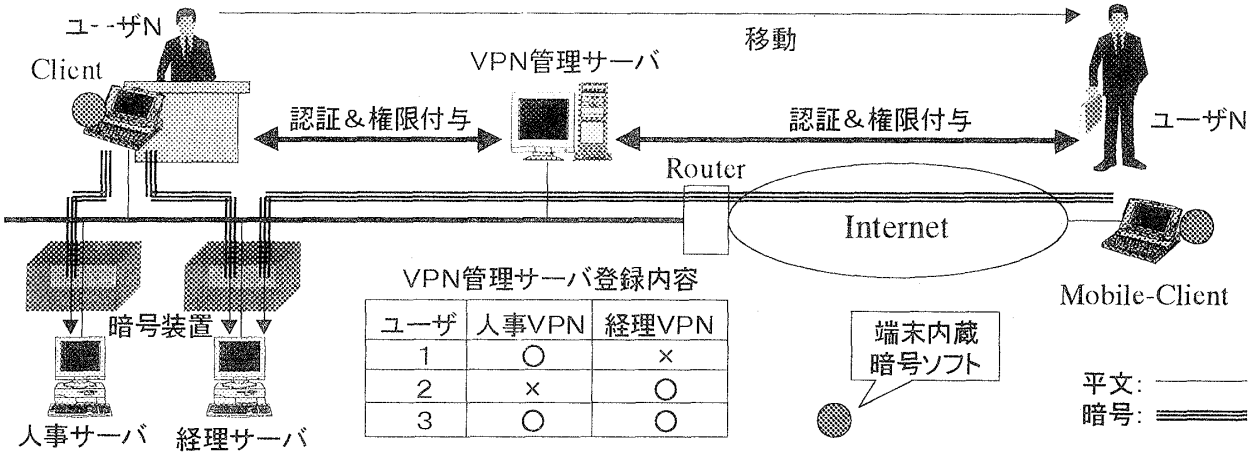
図はクライアント・サーバシステムの単純な例であり、オープンネットワーク(Internet/LAN)を流れるデータを暗号化することによってVPNを構築している。管理装置は暗号鍵の管理（鍵生成や配送）や暗号装置への暗号条件等のパラメータ設定を行うための運用ツールである。

A Concept of Individual VPN (Virtual Private Network) System

Shinobu USHIROZAWA , Toru INADA and　Akiko MIYAGAWA
Information Technology R&D Center, Mitsubishi Electric Corporation , 5-1-1 Ofuna, Kamakura, 247 JAPAN　(E-mail) ussy@isl.melco.co.jp

3．個人対応 VPN の構築手法

図１において、両暗号装置によって構成される VPN が主に社外や組織外への情報秘匿を目的とする組織単位の VPN のモデルである。一方、Mobile-Client が構成する VPN は、個人対応 VPN のモデルであり、特定個人以外への情報秘匿が目的である。組織単位 VPN の場合、Client が VPN へ加入するためには物理的に暗号装置の平文側にいる必要がある。さらに平文側の Client 同士の区別は一般的にはなく、例えば人事という VPN の中で人事部長だけは経理情報にアクセスできるというような木目細かな制御が困難である。この２点に着目し、VPN の物理的な制約がなく、かつ個人単位の権限付けが可能な”個人対応 VPN”を実現する。個人対応 VPN の実施例を図２に示す。



ユーザ	人事VPN	経理VPN
1	○	×
2	×	○
3	○	○

図２．個人対応 VPN の実施例

図のように、人事サーバと経理サーバが暗号装置を介してネットワークに接続されており、各サーバと通信するためには直上の暗号装置と暗号通信（VPN の構築）する必要がある。暗号通信を行うためには、暗号ソフトを内蔵した Client を用い、かつ暗号通信用の権限が付与されなければならない。この場合の権限とは、暗号通信を行うための暗号鍵や暗号鍵をネゴシェーションするための秘密情報などである。権限は VPN 管理サーバによってユーザ毎に管理されており、ユーザはネットワーク経由で認証を受けた後に権限を付与してもらう。ユーザは個人の ID と認証情報（例えば公開鍵など）を持ち歩くことにより、VPN 管理サーバとの間で確実な個人認証を行う。また、権限のコントロールは個人ではなく、管理者が一括して行うべきものである。本方式では、VPN 管理サーバ上に権限が一括管理されているので、認証情報を発行した後からでも管理者側の任意のタイミングで帰属 VPN の増減が可能である。

4．まとめと今後の課題

本方式によれば、ユーザは物理的な位置に左右されることなく、自己の権限に応じた VPN に帰属することが可能になる。今後は、IPSEC などの標準技術と本方式の融合や個人の ID と認証情報の効率的な運用管理手法について検討していく予定である。

参考文献

[1]横山他“LAN 暗号装置の実現方式”，電子情報通信学会総合大会，1997
[2]後沢他 "暗号によって構成される VPN とその管理手法"，信学技法ＩＮ９７－１１３