個人対応 VPN（Virtual Private Network）の管理手法

1U－7

稲田　徹　後沢　忍　宮川　明子
三菱電機株式会社　情報技術総合研究所

1．はじめに

近年、モバイル通信が発達し、企業内情報を外部からアクセスするニーズが高まっている。従来の外部からのアクセスは電話網を使用したアクセスが主体であったが、通信コストの削減などのため、インターネットを使用したアクセスに変わりつつある。一方、アクセスされる側の企業網内の暗号化のニーズ（セキュリティ犯罪の7割は内部ユーザの犯行というデータもある）も高まりつつある。これらを暗号化方式の面から捉えると、インタネットの暗号化（インタネット VPN）は、ほぼIPSEC（ex.DES 40Bits）に固まりつつあり、国内を中心とした企業網の暗号化（企業内 VPN）は、IPSEC で標準的に使用されている暗号よりも強度の強い暗号（ex.MISTY 128Bits）が使用される傾向がある。

個人ベースの VPN システムにおいては、ユーザが移動するため、一人のユーザがインタネットＶＰＮと企業内 VPN の双方を使用する可能性が高い。一般に、VPN の管理は暗号化方式ごとに実施されるため、個人ベースの VPN システムでは、これら複数の暗号化方式の VPN を一元的に管理する管理手法の検討が必要となる。

2．管理手法の検討

複数の暗号化方式の VPN を一元的に管理するためには、VPN 処理の上位レイヤに管理パラメータを置く必要がある。本検討では、VPN 処理の上位レイヤに Group-ID を定義することにより、複数の暗号化方式の VPN を一元的に管理することとした。図1に端末内部での処理構成を示す。

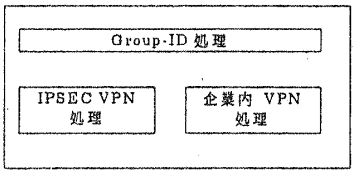

図1　端末内部の処理構成

2．1　Group-ID の割り当て

複数の VPN を一元管理するために、各サーバへのアクセス権限を表す Group-ID を決定する。Group-ID は、管理装置によって管理／運営され、ユーザがサーバアクセス時に管理装置に要求し、管理装置側でユーザ認証後、配送される。図2に企業内で VPN を使用する場合と、ユーザが移動して(図例では、A,B 共にインタネット上へ移動している)インタネット経由で VPN を使用した場合の Group-ID 単位で見た VPN の管理イメージを示す。

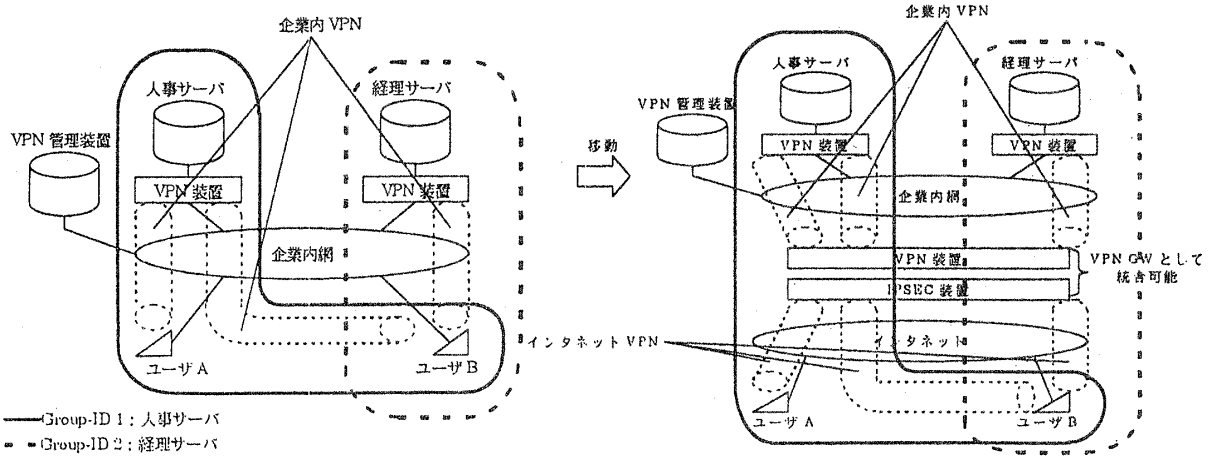

図2　Group-ID 管理イメージ

A Study on Management Method of Individual VPN System

Toru INADA, Shinobu USHIROZAWA, and Akiko MIYAGAWA
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa, 247 Japan

図1に示したように、Group-IDを割り当てることにより、移動によってVPN構成が変更されても、移動前の管理単位で管理可能となる。

3．通信シーケンス

Group-IDを割り当てた場合の通信シーケンス(図2の移動後の経理サーバとユーザB)を図3に示す。なお、図2におけるインタネット側のVPN装置とIPSEC装置はVPN GWとして統合して示している。

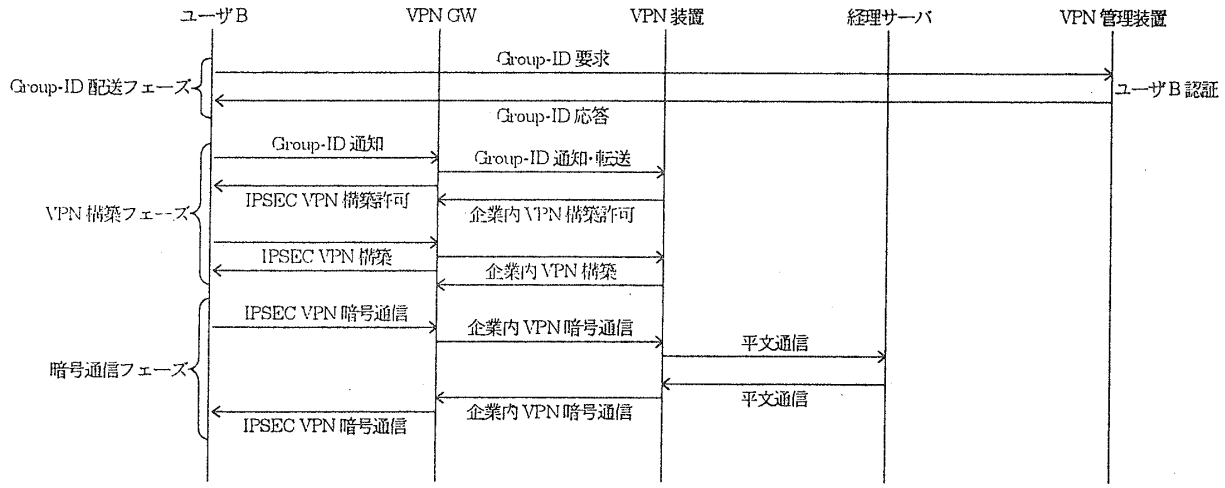

図3　通信シーケンス

・Group-ID 配送フェーズ

暗号通信に先立って、ユーザは、管理サーバに対して Group-ID を要求する。管理サーバは、ユーザ認証後、そのユーザの Group-ID を配送する。この時の認証に IC カードなど外部媒体を使用してセキュリティを高めることも可能である。

・VPN 構築フェーズ

ユーザは、管理サーバより配送された Group-ID を VPN GW に通知し、インタネット VPN を構築する。また、Group-ID を通知された VPN GW 装置は、(企業内)VPN 装置に通知された Group-ID を転送して、企業内 VPN を構築する。

・暗号通信フェーズ

VPN 構築フェーズで構築した VPN を使用して、目的のサーバと暗号通信を実施する。

4．今後の課題

本稿では、VPN 構築レイヤの上位に Group-ID という定義を導入して、複数の暗号化方式の VPN を一元的に管理する管理手法について述べた。実際には、企業内暗号化方式と IPSEC の一元管理に使用される可能性が高いため、今後、以下の検討が必要である。

・IPSEC における設定負荷の大部分をしめる SPD（Security Policy Database）との連携、例えば、Group-ID をキーとして、IPSEC トンネルの対向側の装置を自動的に認識するなど、の検討。

・複数の暗号化方式の VPN を接続する VPN GW の技術的検討。

参考文献

[1]渡辺他：“暗号技術を用いたセキュア通信グループの構築方式とその実現” 情報処理学会論文誌第 38 巻,No4.1997

[2]時庭他：“暗号による仮想私設網の構築方式” 情報処理学会第５５回全国大会　１９９７

[3]田口他：“暗号システムの管理方式” 情報処理学会第５５回全国大会　１９９７

[4]後沢他：“暗号システムへのリモート端末収容方式” 情報処理学会第５５回全国大会　１９９７