暗号による仮想私設網の構築方式

2T－4

時庭康久　後沢忍　稲田徹　田口卓哉　永島規充
三菱電機(株)情報技術総合研究所

1.はじめに

インターネット等においてイントラネットなどの同一企業の拠点LAN間の接続だけでなく、他企業の拠点LAN同士の接続のニーズが高まっている。これに伴って、通信データの盗聴／改ざん、不正アクセスなどのセキュリティへの配慮が必要である。これらの問題を解決するために暗号を用いた仮想私設網(VPN:Virtual Private Network)を構築する。本稿では、仮想私設網のサービス概念と構築方式について述べる。

2.VPNのサービス概念

(1)広域網を介したLAN間、端末間を自由に結合して仮想的なネットワーク(VPN)として運用する。

(2)VPNの通信路において、通信データがセキュリティ的に保護されている。

通信路がインターネットなどの広域公衆網経由の場合、データの盗聴／改ざんが不可能な転送方法である。

(3)VPN外部との通信が可能で、外部からの不正アクセスを認めない。

VPNを構築すると同時に、インターネット上にある各種公開サーバ(WWWサーバ、FTPサーバ等)にアクセスしたいという要求があり、さらに電子メール、電子ニュース等のインターネットのサービスを受けたいという要求もある。外部アクセスの許可と同時に外部からの不正アクセスに対する防御を実施する。

(4)モバイル端末をVPNに収容する。

社外の不特定の携帯端末からのアクセスに対して、セキュリティ的に保護されたデータ転送を保証する。

(5)個々のVPNを容易に多重運用する。

異なるVPN間にまたがるようなVPNを構築できる。図1では、A社の本社、A社の支社で一つのVPNを構築し、A社の子会社B社で一つのVPNを構築しているが、横断的にA社とB社の人事部、経理部で別のVPNを構築している例である。

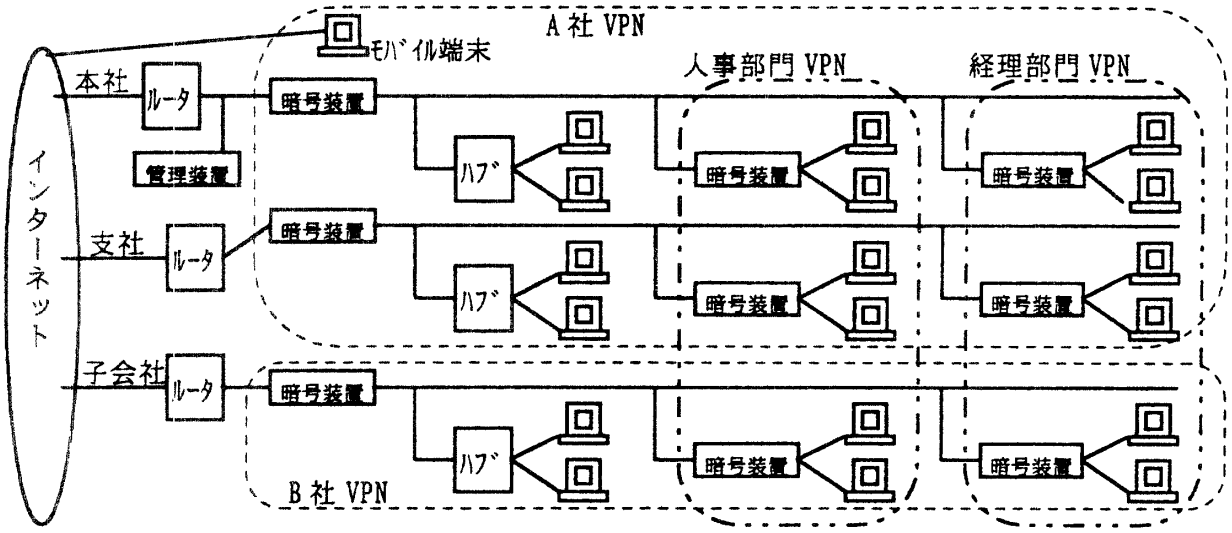


図1．ＶＰＮの構築例

3.VPNの構成要素

暗号を用いることによりVPNを構築する。VPNを実際に構築するためには以下の要求を満たす必要がある。

・既存設備を有効利用してVPNを構築する。
　ルータや端末等の既存設備の設定パラメータの変更も極力少なく済ませる。
・システム導入時だけでなくシステムの構成変更等に柔軟に対応するために、VPNの構成管理が一元管理で容易である。

VPNでは、端末そのものにVPN機能を実装する方法と中継装置にVPN機能を実装する方法が考えられる。既存システムに影響を与えない点に注目して、LANにおいては中継装置(暗号装置)を導入し実現する。モバイル端末では、中継装置を用いないで端末内蔵型の暗号ドライバソフトウェアとして実現する。また、これらの分散配置される暗号装置を一元管理する装置として専用の管理装置を導入する。

Construction Method of virtual private networks by encription

Yasuhisa TOKINIWA, Shinobu USHIROZAWA, Toru INADA, Takuya TAGUCHI, Norimitsu NAGASHIMA
Information Technology R&D Center, Mitsubishi Electric Corporation

(1)暗号装置

暗号装置は、VPN の境界となる端末間の通信路上に配置される。暗号装置は、通信路上の中継データを暗号化／復号したり廃棄することにより VPN の機能を実現する。

(2)暗号ドライバソフトウェア

モバイル端末内蔵の暗号ドライバソフトウェアとして VPN の機能を実現する。

(3)管理装置

管理装置は、暗号装置との管理通信が保証されていればシステムの任意の場所に配置してよい。暗号装置に対してセッション鍵の配送、動作パラメータの設定、動作状態の収集などの機能を実現する。

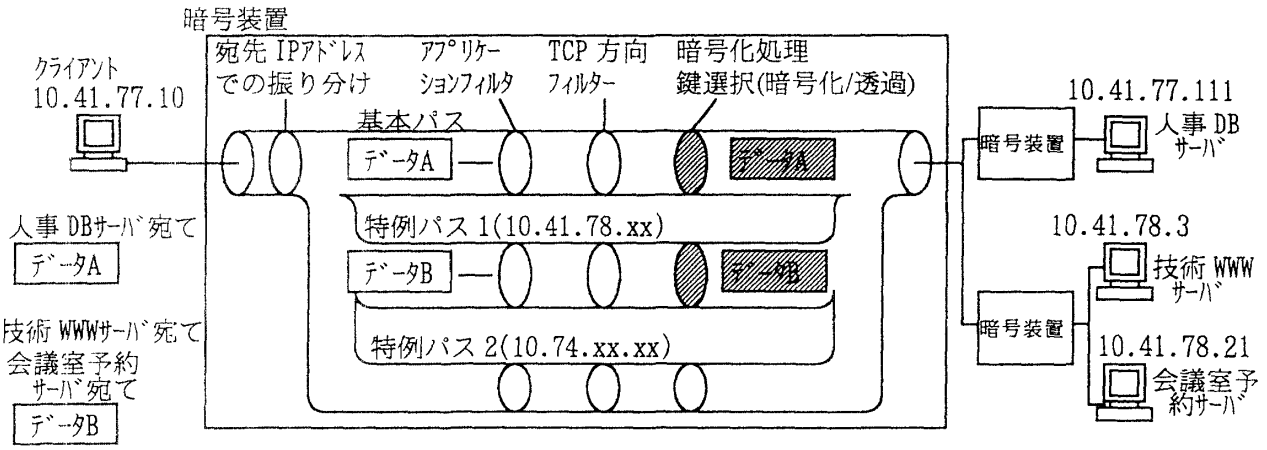
4.VPN の構築方式

VPN は同一のセッション鍵を用いた暗号通信によって実現し、暗号に使用するセッション鍵を管理装置から暗号装置に配送している暗号鍵事前共有型システムである。データのネットワークルーティングのためのヘッダ部分は平文で、残りのユーザデータ部分を暗号する。個々の VPN が異なれば別のセッション鍵を用いた暗号通信を行う。データの暗号通信により、データの盗聴／改ざんの脅威から守ることができる。不正アクセスに対しては、復号によりデータが壊されるので不正侵入が不可能となる。VPN 外部端末との通信は、暗号を実行せずに平文通信により実現する。

通信経路上に暗号装置が複数存在した場合、暗号されたデータを受信した暗号装置が、暗号化処理においてデータのユーザデータ部分の二重暗号機能や宛先アドレスによる選択的透過の機能を実現し、図１のような VPN の多重運用を可能とする。

(1)暗号装置の動作

管理装置より通信相手端末のアドレス、アプリケーション種別及び暗号化(セッション鍵選択)／透過中継を設定し運用する。通信相手端末のアドレスとアプリケーションの種別の比較により暗号化(復号)／透過中継／廃棄を実行し中継する。これらの中継処理では、設定された条件により処理を決定する特例パスの概念とデフォルトの処理を行う基本パスの概念がある。図２に示すような運用が可能である。特例パスの機構によりユーザニーズに合ったきめの細かな対応が可能である。



	アプリケーションフィルタ	TCP 設定方向	暗号化処理
基本パス	TCP/UDP 全通過	なし	セッション鍵１で暗号
特例パス１	HTTP、TELNET のみ通過	OUT のみ許可	セッション鍵５で暗号

図２．特例パスの利用例

(2)暗号ドライバソフトウェアの動作

終端端末であるのでアプリケーション種別の組み合わせによりセッション鍵／透過中継を設定し、暗号装置の動作と同様に、送受信データのヘッダ情報のフィルタにより処理を決定する。

(3)管理装置の動作

セッション鍵の生成と暗号装置への配送／暗号通信ドライバへの設定を実現し、VPN の動作パラメータを暗号装置へ設定する。GUI による容易な入力設定を実現する。

5.まとめ

暗号を用いた仮想私設網の構築方法を検討した。今後は、ファイアウォールとの共存や 100Mbps 程度の伝送速度における性能条件などについて検討を行う予定である。

参考文献

[1]横山他：”ＬＡＮ用暗号装置の実現方式”，97 春季信学全国大会
[2]永島他：”集線型暗号装置の認証機構”，97 春季信学全国大会