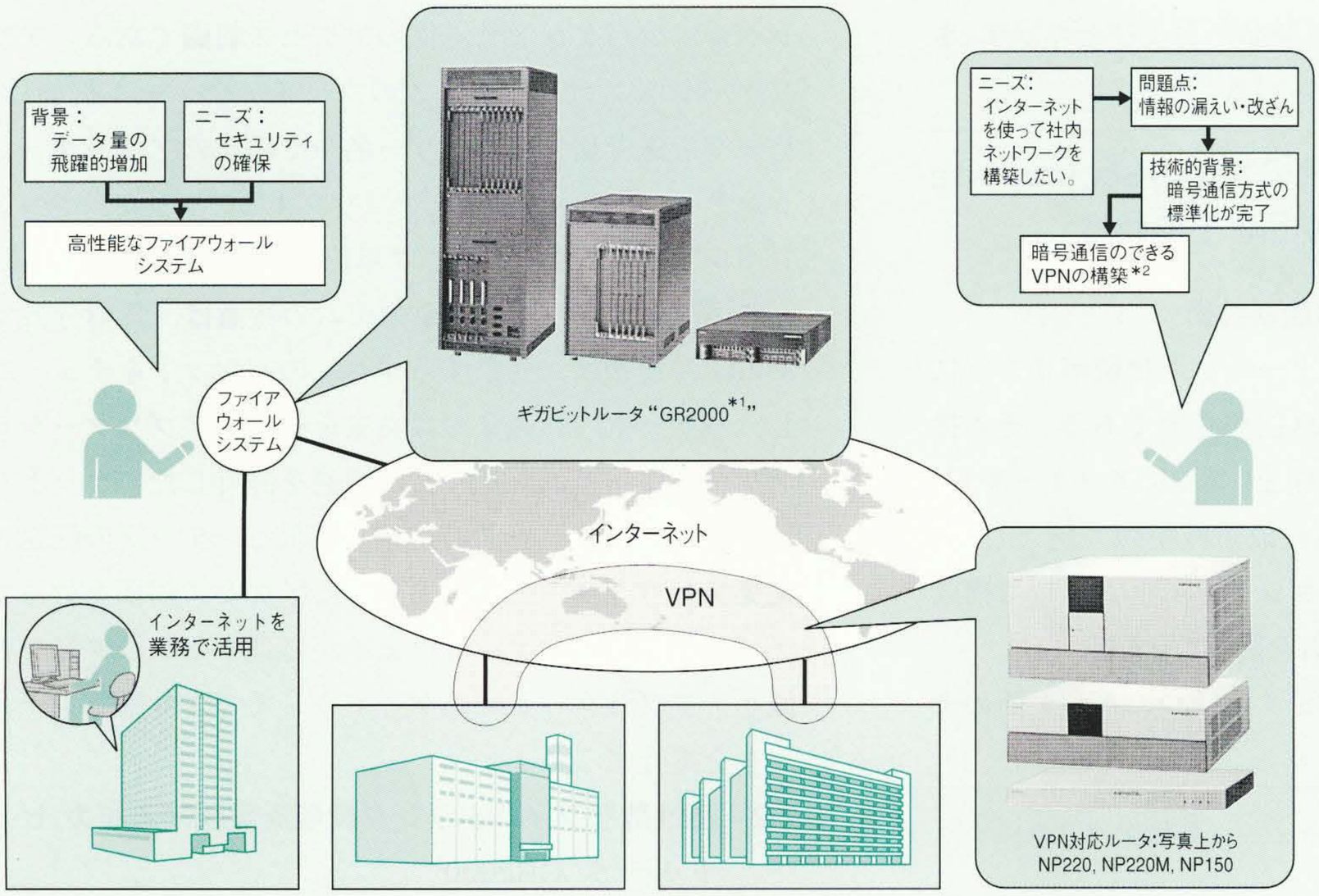
セキュアな情報ネットワークシステムを実現するSecureplazaのハードウェア製品とその特徴

Hardware Platforms for Secure Network System Solutions

大浦哲生　*Tetsuo Ôura*
渡辺義則　*Yoshinori Watanabe*
矢崎武己　*Takeki Yazaki*



注：略語説明ほか
VPN(Virtual Private Network)
＊1 高性能なフィルタリング機能を持つ。収容できるインタフェース数によって3モデル(写真左からモデル20, モデル10, モデル4)がある。
＊2 国際間での暗号通信を規制している国もある。

企業におけるインターネット活用のイメージ

企業がインターネットを活用するためには，セキュリティの確保が重要である。最新のセキュリティ技術を取り込んだ高性能なファイアウォールシステムやVPNが，セキュアなネットワークシステムの構築を可能にする。

情報化社会の進展に伴い，インターネットを利用した企業ネットワークの構築が進んでいる。社内ネットワークを安全に，かつ機能的にインターネットに接続することが企業のニーズである。ファイアウォールシステムとVPN(Virtual Private Network)は，それらのニーズにこたえる手段である。ファイアウォールシステムは，社内ネットワークを守る役割を担う。インターネットの発展に伴って，ファイアウォールシステムには高度化した機能と高い性能が必要となっている。また，VPNは，インターネット上に安全な暗号通信路を仮想的に構築する。VPN暗号通信の仕様は，IETF(Internet Engineering Task Force)が標準化を進めている。

日立製作所が開発した“Secureplaza”のハードウェア製品は，これらの最新のセキュリティ技術をいち早く取り込んだものである。セキュリティの強化のために，独自の強固な暗号アルゴリズム“MULTI4”も採用した。これらの製品により，高性能なネットワークシステムの構築が実現できるものと考える。今後も，急速に発展し続けるインターネットに対応して，ネットワークシステムに必要なセキュリティの先端技術と製品の開発に取り組んでいく。

1　はじめに

インターネットは，情報化社会の発展に伴って急速に普及してきた。普及の要因の一つは，企業が今日のスピーディな高度情報化時代に対応するために，インターネットを利用したWWW(World Wide Web)や電子メールなどを業務に取り込んだことにある。WWWは情報公開・収集の場として，また，電子メールは電話と肩を並べるほどの情報交換・伝達の手段として，それぞれが企業にとって不可欠のものとなっている。もう一つの要因は，インターネットを用いた企業ネットワーク“VPN(Virtual Private Network)”の構築である。企業は，従来の独自社内ネットワークをVPNに置き換えることにより，設備・運用コストの削減を実現した。企業間ネットワーク(エクストラネット)も，VPNを利用して構築が可能である。

一方，社内ネットワークをインターネットに接続する

企業の課題は，セキュリティと運用性の確保である。また，企業は，ユーザーの増加などに伴うネットワーク構成の変更に柔軟に対応できるシステムの構築を必要としている。

ここでは，セキュアネットワーク技術の最新動向，インターネット接続技術とVPN構築技術を用いた“Secureplaza”のハードウェア製品，およびセキュア ネットワーク システムについて述べる。

2 インターネット接続のためのSecureplazaのハードウェア新製品とその特徴

2.1 ファイアウォール構築の最新技術

社内ネットワークでのインターネット接続ポイントには，社内ネットワークを守る機能が必要である。その接続ポイントの不正侵入抑止機能を「ファイアウォール」と呼ぶ。ファイアウォール構築の最新技術の一例として，二つのルータとアプリケーションゲートウェイ※1)で構成するファイアウォールシステムを**図1**に示す。

アプリケーションゲートウェイを二つのルータ間のセグメントに配置する。このセグメントを「バリアセグメント」と呼ぶ。バリアセグメントには，ホームページなどを社外に公開するための公開サーバも配置する。ルータのファイアウォール機能は，「フィルタリング」である。フィルタリングとは，通信する装置のアドレスやアプリケーションの種類，アクセスの方向といったネットワークレベルでのパケット※2)単位のアクセス制御である。アプリケーションゲートウェイのファイアウォール機能は，データを送受信するユーザー名やその他のアプリケーションデータそのものなどをチェックするアプリケーションレベルでのユーザー・データ単位のアクセス制御である。

このファイアウォールシステムの特徴は，負荷分散である。ルータは，受信するすべてのパケットをチェックし，パケットの通過または廃棄を行う。アプリケーションゲートウェイは，ルータが通過を許可したパケットだけを組み立ててデータの意味を解釈し，データの転送・廃棄を行う。ルータでおおまかなアクセス制御を行ってアプリケーションゲートウェイが処理するデータ量を軽減し，アプリケーションゲートウェイでより厳しいチェックを実行する。

※1) アプリケーションゲートウェイ：各種アプリケーションの代理サーバなど

※2) パケット：ネットワーク上を流れる一塊のデータ

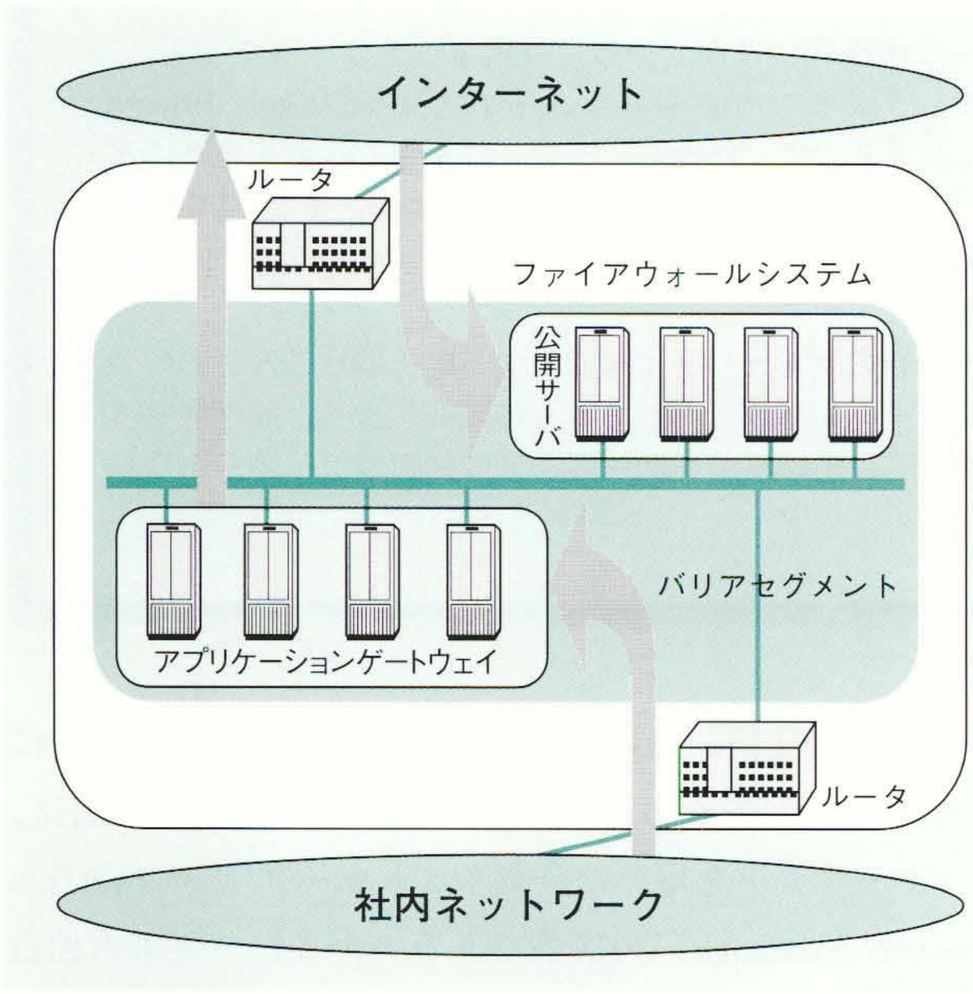


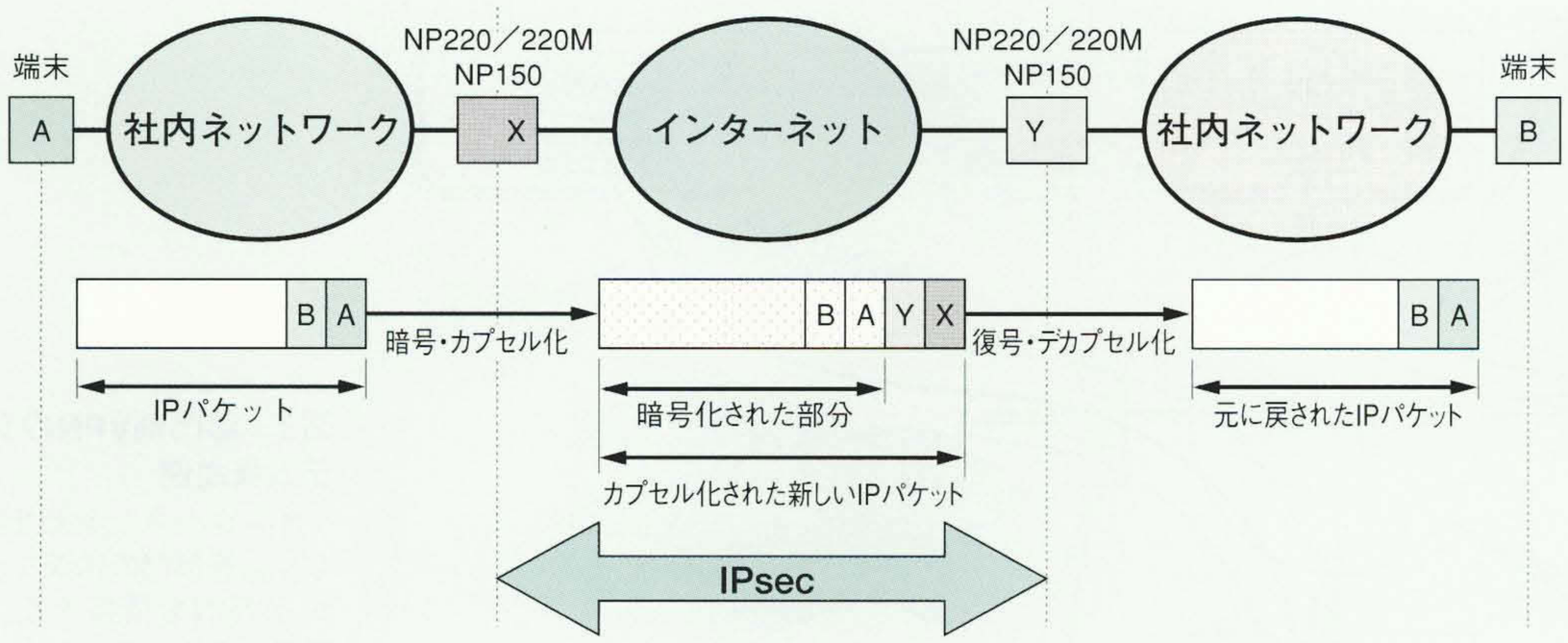
図1 最新技術を用いたファイアウォールシステムの構成例
矢印は，ルータが許可するアクセスの例を示す。インターネットからは，公開サーバにしかアクセスできない。社内ネットワークからは，アプリケーションゲートウェイを介してしかインターネットにアクセスできない。

2.2 高性能なフィルタリング機能を実現するギガ ビット ルータ“GR2000”

インターネットに接続する社内ネットワークシステムが大規模化すると，ルータに設定するフィルタ条件も複雑化し，増大する。これまでルータは，各パケットごとにこの多くのフィルタ条件をチェックしながら，パケットの転送・廃棄を高速に判定することが望まれていた。

世界トップクラスの高性能なフィルタリング機能を実現したのがギガ ビット ルータ“GR2000”である(21ページの写真参照)。GR2000は，ギガ ビット クラスの転送性能を持つ高性能ルータであり，フィルタリング機能を含むほとんどの機能をハードウェアで処理している。フィルタの条件は，最大1,024エントリまで設定できる。フィルタリング機能にはパケット長などを含むきめ細かな条件を設定でき，既知の攻撃手法も防御可能である。このハードウェアフィルタにより，GR2000は，フィルタリング条件を増やしても高性能な転送能力を維持することができる。

2.1で述べたファイアウォールシステムのルータにGR2000を適用することにより，拡張性の高いシステムを構築できる。ユーザーの増加などによって特定のアプリケーションゲートウェイの能力が足りなくなった場合には，アプリケーションゲートウェイの装置を高性能なも



注：記号説明
A, B；社内ネットワーク内のIPアドレス
X, Y；インターネット側のIPアドレス

図2　IPsecの動作概要

端末Aから端末BへのIPパケットの流れを示す。端末Aが送信した元のIPパケットは，インターネット上では完全に暗号化され，新しいIPヘッダでカプセル化される。そのため，インターネット上では，社内ネットワーク用のIPアドレスを盗み取ることができない。

のに置き換えるか，台数を増やすことによって対応する。

3　VPN構築技術の最新動向とSecureplazaのハードウェア製品群

3.1　VPN構築を実現する技術とSecureplazaのハードウェア製品群

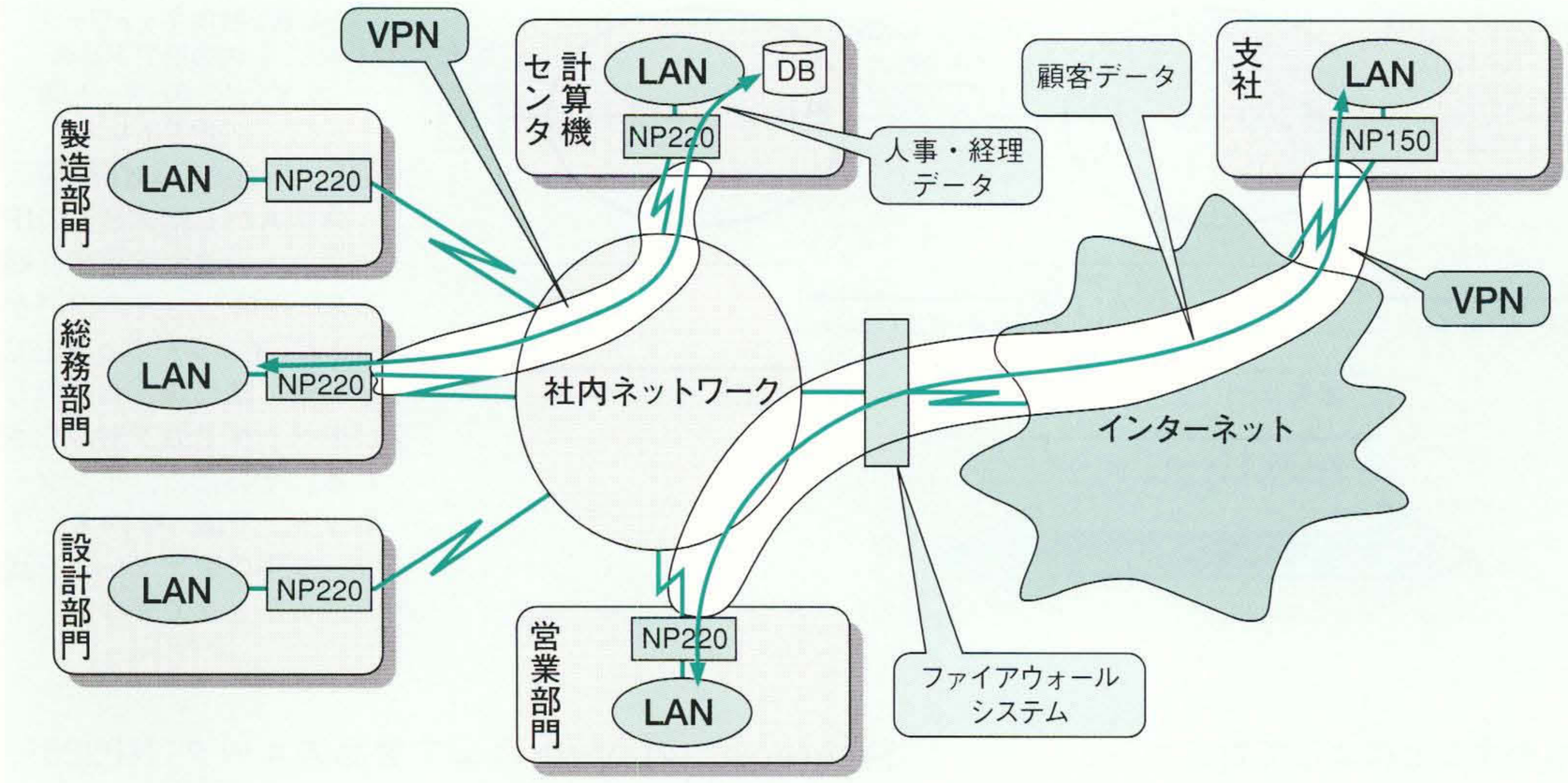
企業から，インターネットに企業情報やユーザー情報を含んだパケットをそのまま流すことはできない。インターネット上に暗号技術を用いたVPNを構築することにより，企業は，インターネットを安全に利用することができるようになる。暗号通信方式としては，“IETF(Internet Engineering Task Force)※3)”が標準仕様の“IPsec(Internet Protocol Security)”を規定している。IPsecはパケットレベルでの暗号方式であり，認証機能も備えている。認証は，パケットに含まれるデータの改ざん，システムを攻撃する多量のコピーパケットを検出するための機能である。IPsecをルータ間で使用した場合の動作概要を**図2**に示す。ルータは，端末が送信したIPパケットをユーザーデータだけでなく，IPアドレスを含むヘッダ部も暗号化する。暗号化したパケットをさらにIPカプセル化して相手のルータに送信することにより，ユーザーデータだけでなく，IPアドレスなどの社内のネットワーク情報を守ることが可能となる。

Secureplazaのハードウェア製品のルータ“NP220”，“NP220M”とルータ“NP150”(21ページの写真参照)は，IETFでの標準化作業段階からIPsecをサポートしている。IPsecで用いる標準暗号アルゴリズムには，かぎ長※4)が56ビットの“DES(Data Encryption Standard)※5)”が採用された。NP220/NP220MおよびNP150では，DESに加えてかぎ長が256ビット※6)の強固な日立製作所独自暗号アルゴリズム“MULTI4※7)”もサポートしている。MULTI4は，DESに比べて暗号・復号処理が高速であり，アルゴリズム自体や使用している演算子を公開していないので，安全性がより高い暗号アルゴリズムである。

3.2　Secureplazaのハードウェア製品群を用いた部門別VPN構築例

特定部門外に公開できない情報を社内ネットワーク上に流す場合にも，情報を守る手段が必要である。特定顧客のデータや人事データ，経理データなどの管理データが一例である。その解決手段の一つが，特定部門間でのVPNシステムである。その構成例を**図3**に示す。社内ネットワークでも，インターネット上と同様に，ネットワークやコンピュータの知識を持つ者が暗号化されていないパケットを解析してデータを入手することは不可能ではない。これを防止するのが，社内ネットワーク上での暗号通信VPNである。暗号通信VPNは，人事データや経理デ

※3) IETF：インターネットの標準化団体
※4) かぎ：暗号の変換パターンを決定する変数。かぎは，通信するものどうしだけが知る秘密情報である。また，暗号の強度は，暗号アルゴリズム自体とかぎ長による。
※5) DES：米国民生用暗号標準アルゴリズム
※6) MULTI4のかぎ：かぎ長の異なる長さの三つのかぎで構成する。かぎ長の合計は320ビットである。NP220／NP220MとNP150では，二つのかぎを固定しているので，有効かぎ長は256ビットになる。
※7) MULTI4：MULTI2の技術を応用して再設計された暗号強度強化版である。MULTI2は，ISO9979/009に登録されており，国内の衛星放送で用いる暗号の標準仕様として規定されている。



注：略語説明
DB(Database)

図3 部門別VPNのシステム構成例
インターネット上だけでなく，各部門の代表ルータからVPNを構築する。部門ごとの固有データが，社内ネットワーク上でも暗号化される。ファイアウォールシステムは，図1に示すような構成とする。

ータが流れる計算機センタと総務部門のそれぞれの社内ネットワーク接続用ルータ間に適応する。また，特定顧客のデータなどが流れる，営業部門の社内ネットワーク接続用ルータ間と支社のインターネット接続用ルータ間にも適応できる。この場合，一つの暗号通信VPNで，社内ネットワーク上とインターネット上の両方でデータの盗聴・改ざんを防ぐことができる。一方，社内ネットワークシステムをインターネットに接続するためのファイアウォールシステムでは，暗号化されたパケットを他の通常のパケットと同様に扱う。パケットの集中するファイアウォールシステムは負荷の高い暗号・復号処理を実行しないので，高いシステム性能を維持することができる。

この部門間VPNネットワークシステムは，企業間のエクストラネットにも適応が可能である。特定事業や製品について特定部署が他社とアライアンスを組み，情報交換を行う場合などがその例である。この場合，特定部署の社内ネットワーク接続用ルータと相手の企業のインターネット接続用ルータ間で暗号通信VPNを構築する。

NP220／NP220MとNP150は，豊富なネットワークインタフェースをサポートし，これらの暗号通信VPNを実現するものである。

4 おわりに

ここでは，企業がインターネットを利用する場合のセキュリティとして，インターネットに接続するためのファイア ウォール システムの最新技術，VPNを構築するための最新技術，およびこれらの技術を取り込んだSecureplazaのハードウェア製品群とその特徴について述べた。

今後も，最新のセキュリティ技術を取り込んだ製品開発を通じ，インターネットを有効にかつ安全に活用できる高性能なセキュリティ ネットワーク システムを提案していく考えである。

参考文献

1) 佐々木，外：インターネットセキュリティ，オーム社(1996)
2) 宝木，外：ファイアウォール インターネット関連技術について，昭晃堂(1998)
3) S. Garfinkel，外：UNIX＆インターネットセキュリティ，オライリー・ジャパン(1998)

執筆者紹介

大浦哲生
1984年日立製作所入社，情報・通信グループ コンピュータ事業本部 エンタープライズサーバ事業部 ネットワークシステムセンタ 所属
現在，インターネットセキュリティ関連製品の開発に従事
E-mail：oura @ ebina. hitachi. co. jp

渡辺義則
1987年日立製作所入社，システム開発研究所 セキュリティシステム研究センタ 所属
現在，ネットワークセキュリティ技術の研究開発に従事
電子情報通信学会会員
E-mail：y-watana @ sdl. hitachi. co. jp

矢崎武己
1995年日立製作所入社，中央研究所 ネットワークシステム研究室 所属
現在，ルータにおける通信品質制御の研究開発に従事
E-mail：yazaki @ crl. hitachi. co. jp