GB-1200を使ったネットワーク環境の構築例

中野, 智
九州大学応用力学研究所技術室

出版情報：九州大学応用力学研究所技術職員技術レポート. 6, pp.82-86, 2005-03. Research Institute for Applied Mechanics, Kyushu University
バージョン：
権利関係：

GB-1200 を使ったネットワーク環境の構築例

九州大学応用力学研究所技術室　　中野　智

１．目　的

稼動中だった研究室の Firewall マシンの老朽化、そして新たに総合研究棟に計算機室を設置することになったことで新たにネットワーク環境を構築する必要性が出てきた。このため、Firewall マシン GB-1200 を応力研内と総合研究棟内の各ナノメカニックス計算機室に設置し、２地点間を VPN で接続してより安全なネットワークの構築と遠隔操作による計算機の運用ということを目的に各種サーバの設定とネットワーク環境の構築を行うこととなった。

２．使用機器

Firewall マシン：　ソリトンシステムズ社製　GB-1200　　２台

サーバマシン　：　カスタム PC（OS はすべて Fedora Core を使用）　３台

３．GB-1200 を選択した理由

○　ネットワークセキュリティの提供に特化したものであり、ICSA 認定を受けている。

○　ユーザーインターフェースが日本語対応であり、また一般的な Web ブラウザを使用して操作できるため、管理用 PC の OS に関わらず、容易に操作できる。

○　拠点間 VPN 機能が搭載されている。

○　ユーザー数が無制限のライセンスである。

○　DNS/DHCP サーバ機能を有している。

４．ネットワークタイプ

GB-1200 は下記３タイプのネットワークから成り立っている。

○　外部ネットワーク・・・インターネット側の非保護ネットワーク。IP はグローバルアドレスを指定。エイリアスを設定してアドレス変換に利用。

○　内部ネットワーク・・・Firewall によって保護されているネットワーク。すべてのホスト、IP は外部や PSN から隠されている。IP はプライベートアドレスを指定。

○　PSN ネットワーク・・・外部に公開するサーバを設置しているネットワーク。外部から公開サーバへのアクセスは、アドレス変換を利用して特定のポートのみ許可。内部ネットワークに指定したものと異なるプライベートアドレスを指定。

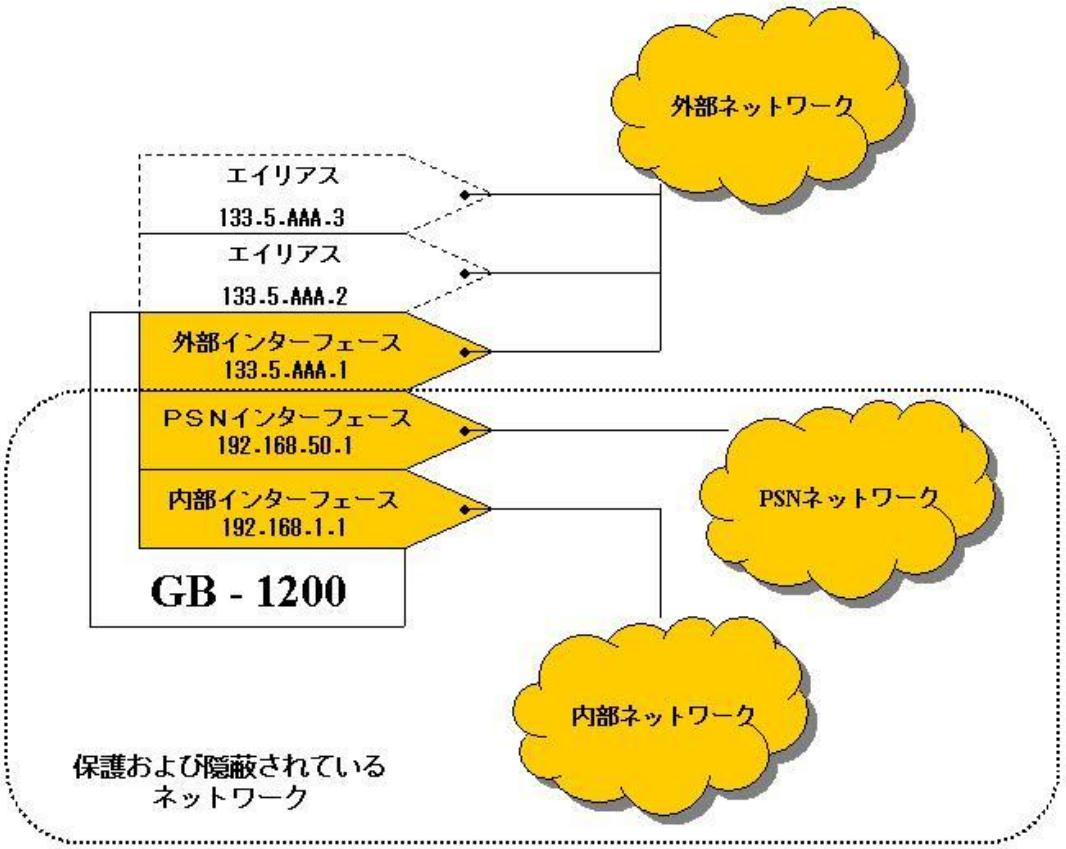

図１　ネットワークとネットワークインターフェース

５．GB-1200 で使用した主な機能

○　エイリアス機能

複数の IP アドレスをネットワークインターフェースに割り当てること。今回は外部ネットワークインターフェースにグローバルな IP を割り当てて、アドレス変換に利用している。

○　インバウンドトンネル機能

GB-1200 の外部あるいは PSN のホストから PSN あるいは内部ネットワークのホスト、つまり通常は隠蔽されていてアクセスできないホストに対して、アクセスできるようにする機能。

○　フィルター機能

GB-1200 のすべてのネットワークインターフェースにあるインターフェースやエイリアス宛のパケットのアクセスを規制する機能。このフィルター機能は、適用するプロトコルやインターフェース、アドレス、オブジェクト、ポート番号などをターゲットの IP アドレスとポート番号に関連づけて設定可能なため、詳細な条件設定が可能となる。

○　ネットワークアドレス変換（NAT）機能

GB-1200 によって隠蔽されている IP アドレスを、外部ネットワークインターフェースの IP アドレスに変換する機能。内部ネットワークから外部ネットワークおよび PSN、PSN から外部ネットワーク宛のアウトバウンドパケットに適用される。

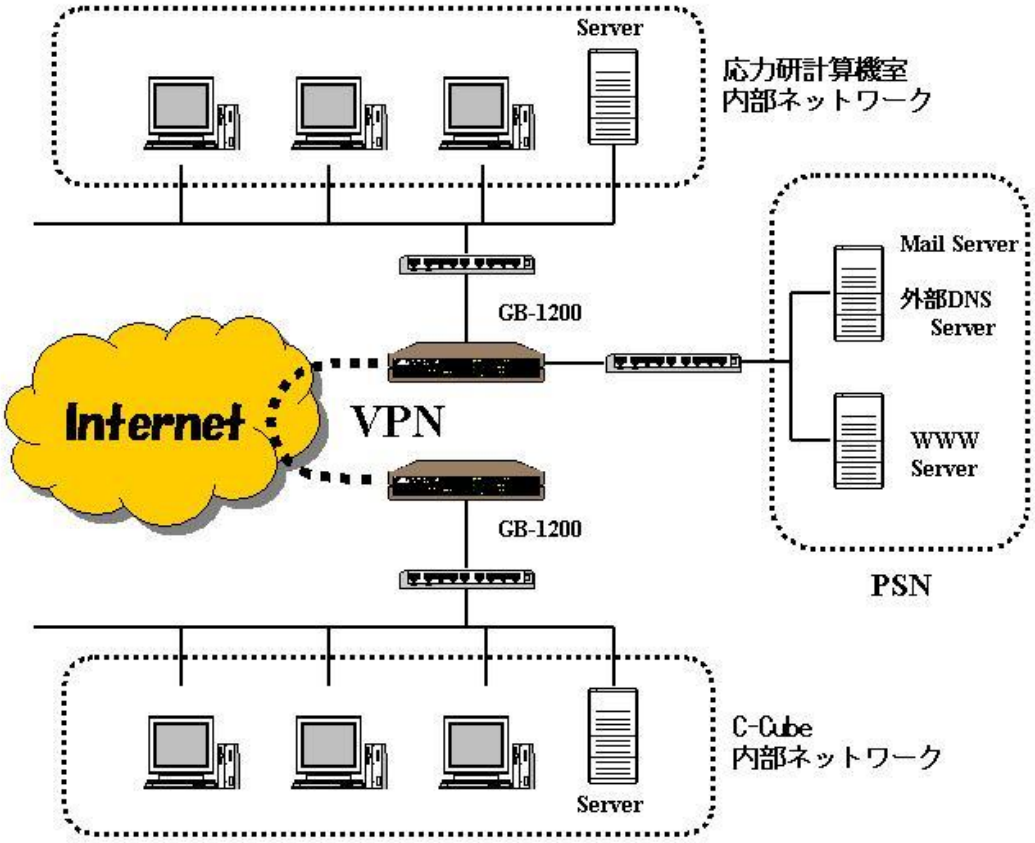

図２　ネットワーク構成図

６．VPN とは

VPN とは Virtual Private Network の略で、インターネット上の拠点間を専用線のように接続して不正アクセスを防ぎ、安全な通信を可能にする技術のことである。パブリックネットワークを使ってプライベートネットワークを実現しようということである。インターネットを経由しているにもかかわらず、同一ネットワーク上にいるかのような利便性と１対多の接続が容易であるというメリットがある。VPN の機能は大きく分けて２つある。

○　カプセル化・・・パケットに新しいヘッダを加え、カプセル化して通信を行う。トンネリングと呼ばれ、通信を外部から隠蔽する。

○　暗号化・・・・・パケットを暗号化する。これにより、トンネリングされたパケットの盗聴を防止し、かつ通信相手先（通信経路）を隠蔽することができる。

７．VPN を使用するためのプロトコルと暗号鍵

○　IPSec（Internet Protocol Security）

VPN で最も一般的に用いられている暗号通信のためのプロトコル。インターネットの標準化団体である IETF(Internet Engineering Task Force)が VPN の標準プロトコルとして規定している。次のセキュリティ機能を提供する。

・ IP データグラムの発信元が正しいことを保証。
・ IP データグラムが改ざんされていないことを保証。
・ IP データグラムを暗号化。

IPSec とは暗号化通信を実現する複数のプロトコルの総称である。今回は下記に示すプロトコルを使用した。

・ IKE（Internet Key Exchange）
  IPSec による認証や暗号化のためには、通信する双方で最初に暗号鍵を交換せねばならない。この鍵をどのように相互で共有するかといった鍵管理方法の取り決めが必要である。IKE とは IPsec による通信に先立って通信相手の認証を行い、ESP や AH で用いる秘密情報（鍵）の交換を行う鍵交換プロトコルである。
・ ESP（Encapsulating Security Payload）
  IPSec ではパケットごとに暗号化がなされる。そこで ESP とよばれる入れ物にパケットをパックして送信する。ESP は発信元の認証、データの完全性（改ざんされていないかどうか）認証、リプレイアタックの阻止、データの暗号化機能を提供するプロトコルである。

８．VPN の主な設定によるパケットの流れ

○ アウトバウンド（内部ネットワークから外部への通信）
1 内部ネットワークインターフェースにパケットが届くと、SA(Security Association)をチェックし、宛先が VPN かどうか確認
2 宛先がリモートの VPN でない場合には通常の IP パケット処理
3 宛先がリモートの VPN の場合、パケットに対してフィルターを適用
4 パケットがフィルターに適合した場合、あらかじめ設定していた VPN 変換が行われる
5 パケットがフィルターに適合しない場合、パケットを破棄

○ インバウンド（外部から内部ネットワークへの通信）
1 外部インターフェースに到達した VPN パケットに対してフィルターがかけられる
2 フィルターに適合しないパケットはアクセス拒否
3 フィルターに適合した場合、SA をチェックし、該当するものがあればパケットをデコード
4 パケットの復号化に成功した場合、フィルターによってパケットを受入れるかどうか判断
5 フィルターに適合した場合には、ターゲットの IP アドレスまでルーティング
6 フィルターに適合しない場合、パケットを破棄

９．Firewall の主な設定内容

○ 応力研、C-Cube 両計算機室の内部ネットワーク同士は、上記 VPN の設定にて通信可。
○ 内部ネットワークから外部ネットワークへのアクセスはすべて許可。
○ 外部インターフェースにエイリアスを作成。アドレス変換に利用。
○ アドレス変換を使用して外部からの通信を許可する場合、宛先は外部インターフェース、

あるいはエイリアスのアドレスとなる。(外部側ホストから内部側ホストの IP アドレスは隠れていて見えない。リプライパケットもすべてアドレス変換される。)

○ 外部ネットワークからは PSN 上のサーバ上の特定のサービスに対するアクセスのみ許可。

○ アドレス変換が定義されたインターフェースやエイリアスにパケットが到着すると、インバウンド機能やフィルター機能などで設定した内容にしたがって IP アドレス変換が行われ、対応する PSN や内部ネットワークのホストに対して通信に変換されたパケットを送出する。

１０．Firewall マシン導入の成果

新しい Firewall を導入したことで、外部からのネットワーク攻撃や不正アクセスを防ぐことへの効果がより向上したと思われる。また、応力研、総合研究棟の両計算機室の研究空間を VPN で結ぶことにより、どちらからも１つのネットワークとして認識することが可能となった。その結果、離れている２地点のワークステーションやサーバを双方から自由に操作することが可能になり、利便性も高まった。さらに、プライベートネットワークを使用することで、限られた資源であるグローバルネットワークアドレスの使用数を大幅に制限できている。

１１．今後の方針

現在は内部ネットワークから外部への通信を自由に許可しているが、これを制限するために内部にウイルス対策機能を備えたプロキシサーバをたてて、内部ネットワーク上の利用者はプロキシを介してのみしか通信を許可しないようにし、セキュリティをより強固にしたいと考えている。

謝　辞

本報告はナノメカニックス分野の研究に関連している。柿本浩一教授には技術報告の作成に関して御理解とご指導をいただいた。また応用力学研究所技術室の石橋道芳氏に技術的な助言とご指導をいただいた。ここに記して感謝の意を表します。