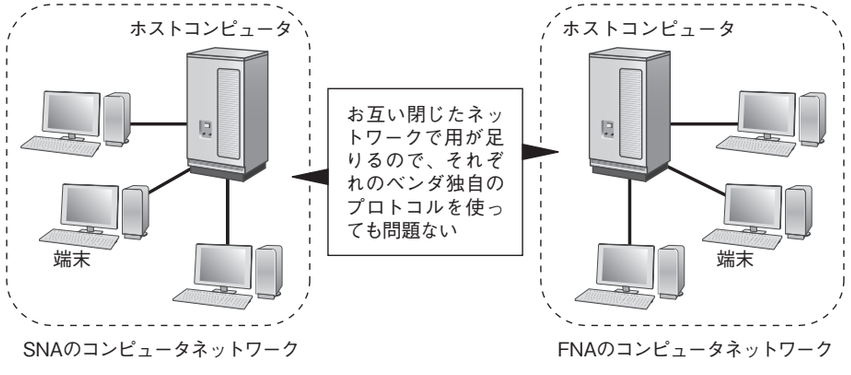
1-2-2 通信プロトコルの標準化

インターネットが生まれる前まで、コンピュータネットワークは中央集中型の形態でした。中央集中型ネットワークにおいて、ハイスペックマシンのホストコンピュータがすべての端末からの要求を処理します。端末とホストコンピュータ間の通信が主だったため、ベンダ独自の通信プロトコルでもまったく問題がありませんでした。このごろは、コンピュータネットワークの鎖国時代のような時代でした（**図1.2.1**）。ちなみにベンダ独自の通信プロトコルとして有名なのは、IBMのSNA[注1]、富士通のFNA[注2]、電電公社のDCNA[注3]などがあります。

○図1.2.1：コンピュータネットワークの鎖国時代



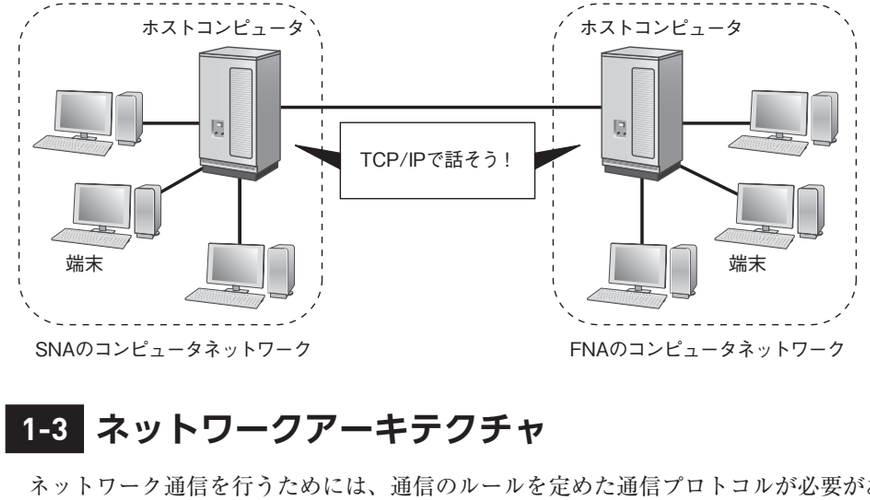
また、後ほど述べる分散型ネットワークよりも中央集中型ネットワークのほうが低コストです。なぜなら、ホストコンピュータ以外の端末にそれほど高いスペックが必要としません。コンピュータネットワークの形態がずっと中央集中型のままと思いきや、時代は突如中央集中型から分散型に移り変わっていきます。

中央集中型ネットワークの一番の弱点は、すべての処理がホストコンピュータに集中することです。ホストコンピュータが故障してしまうと、すべての機能が停止してしまいます。米ソ冷戦時代において、軍事利用のコンピュータを相手国からの攻撃を守るため、ホストコンピュータを何ヵ所に分散させて、仮に一部のコンピュータが破壊されたとしても残りのコンピュータで継続利用ができる必要がありました。そこで、アメリカ国防総省のARPA[注4]という研究機関が、分散するコンピュータネットワークを相互接続する「ARPANET」と呼ばれる軍事用ネットワークを構築しました。ARPANETで採用されたプロトコルがTCP/IPで、ARPANETが一般向けのインターネットに移り変わったと同時に、TCP/IPが標準プロトコルとして瞬く間に普及しました（**図1.2.2**）。

注1　Systems Network Architecture
注2　Fujitsu Network Architecture
注3　Data Communication Network Architecture
注4　Advanced Research Projects Agency

民間団体での通信プロトコルの標準化として、国際標準化機構のISO[注5]のOSI[注6]が挙げられます。OSIプロトコルはあまり普及していませんが、通信を7層の機能に分割したOSI参照モデルは一般的なネットワークアーキテクチャとして認識されています。ちなみに、TCP/IPはIETFによって標準化されたプロトコルで、仕様はRFC[注7]と呼ばれる文書として一般公開されています。

○図1.2.2：通信プロトコルの標準化によるネットワークの相互接続



1-3 ネットワークアーキテクチャ

ネットワーク通信を行うためには、通信のルールを定めた通信プロトコルが必要があると述べました。ネットワーク通信で使われる通信プロトコルにはたくさんの種類があり、これらの通信プロトコルの集合がネットワークアーキテクチャです。ネットワークアーキテクチャは、ネットワーク通信に必要な機能を提供します。さらに、ネットワークアーキテクチャにおいて、機能を理解しやすいように階層化されています。ここでは、OSI参照モデルとTCP/IPのネットワークアーキテクチャを紹介して、ネットワークアーキテクチャの階層化構造における通信の様子をみていきます。

1-3-1 OSI参照モデル

OSI参照モデル（**図1.3.1**）は、ネットワーク通信の標準的な概念を定めた規定です。ネットワーク通信に必要な機能を7つの階層に分けて整理するにより、ネットワーク通信の構造が理解しやすくなります。英語の勉強はアルファベットから覚えるのと同じように、ネットワークの場合、OSI参照モデルの7層を諳んじることから始めます。なぜなら、ネットワークの用語はしばしばOSI参照モデルを基準として考えているからです。ちなみに、OSI参照モデルはネットワークアーキテクチャではなく、ネットワークアーキテクチャのモデルです。

注5　International Organization for Standardization
注6　Open Systems Interconnection
注7　Request For Comment

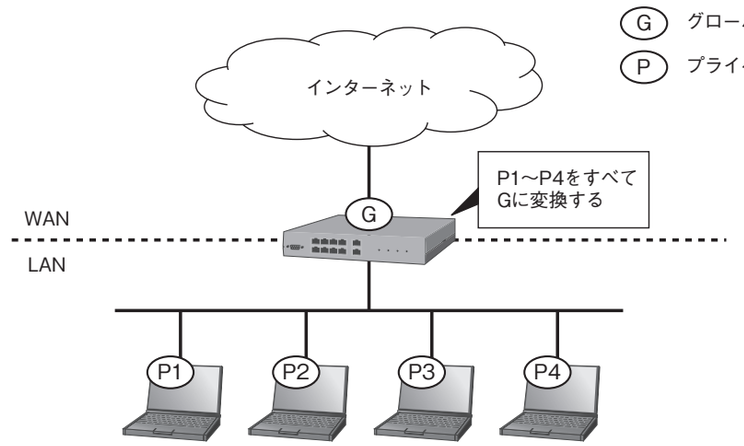
8-1 NATの概要

NAT（Network Address Translation）は、その利用目的に応じて種類分けされます。一般的に知られているNATの種類として、静的NAT、動的NAT、IPマスカレード（NAPT）、デスティネーションNATがあります。これらのNATは、それぞれ違った用途に使われ、当然IPアドレスの変換ロジックも互いに異なります。

8-1-1 NATの目的

NATが一番使われているのは、インターネット接続時のプライベートIPアドレスとグローバルIPアドレスの変換です。パソコンに直接グローバルIPアドレスを付与すればNATは不要となりますが、グローバルIPアドレスの数に限界があるため、LAN内のパソコンはできるだけグローバルIPアドレスを共有するようにしたのがNATです。この場合、NATはグローバルIPアドレスの節約という目的に使われます（**図8.1.1**）。

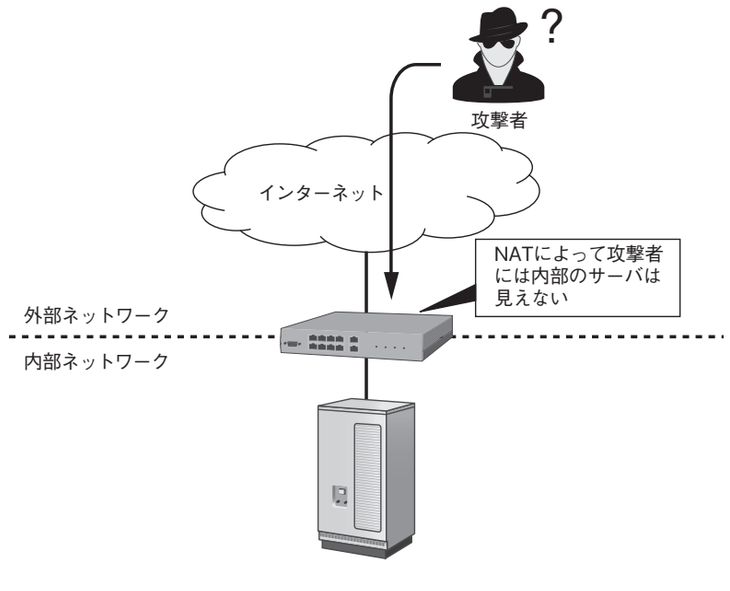
○図8.1.1：グローバルIPアドレスの節約のためのNAT利用



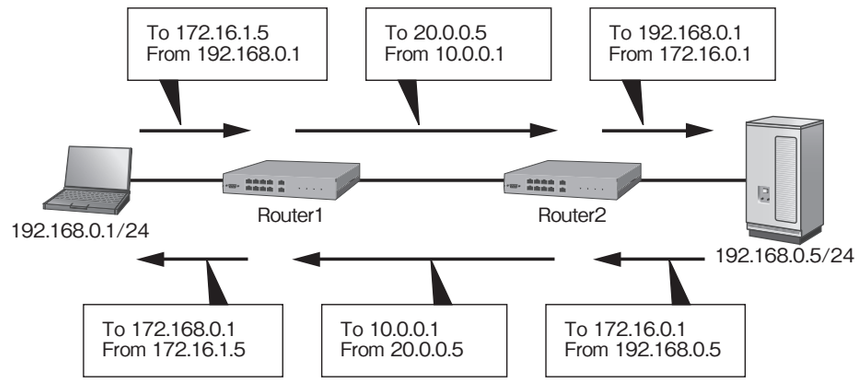
NATを使うと、内部のIPアドレスを隠蔽できるので、ネットワークのセキュリティを高められます。なぜなら、内部ネットワークへの攻撃を試みる攻撃者は、変換後のIPアドレスしか見えていないので､攻撃対象のサーバを一意に識別することが困難となるためです（**図8.1.2**）。

同じネットワークアドレス帯を持つネットワーク同士を統合するとき、IPアドレスの重複を避けるためNATを使うときもあります。**図8.1.3**は、同じネットワークアドレス帯のネットワーク同士がNATを使って通信する例です。この例では、パソコンもサーバも同じ192.168.0.0/24のネットワークに属していますが、Router1とRouter2で発着信パケットのソースアドレスを変換することで、パソコンとサーバ間の通信ができるようになります。

○図8.1.2：内部ネットワークの隠蔽のためのNAT

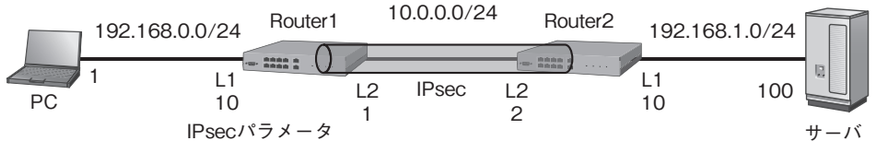


○図8.1.3：IPアドレスの重複防止のためのNAT



最後に紹介するNATの用途は負荷分散です。このとき、NATされるのは送信元アドレスではなく宛先アドレスとなります。**図8.1.4**は、NATを使ったwebサーバの負荷分散の例です。この例では、クライアントからリクエストを内部ネットワークの複数のwebサーバに振り分けています。

○図10.1.4：IPsecによる拠点間接続①（ヤマハルーター）



IKEフェーズ	パラメータ	パラメータ値	
		Router1	Router2
1	事前共有鍵	yamaha	yamaha
2	暗号アルゴリズム	aes-cbc	aes-cbc
	ハッシュアルゴリズム	sha-hmac	sha-hmac

○リスト10.1.4a：Router1の設定（ヤマハルーター）

```
Router1# ip route 192.168.1.0/24 gateway tunnel 1  ❶
※サーバのネットワークへの通信はTunnel1インタフェースに渡す
Router1#
Router1# ip lan1 address 192.168.0.10/24  ❷
Router1# ip lan2 address 10.0.0.1/24
Router1#
Router1# ipsec ike keepalive use 1 on  ❸ ※IKEキープアライブを有効にする
Router1# ipsec ike local address 1 10.0.0.1  ❹
Router1# ipsec ike pre-shared-key 1 text yamaha  ❺ ※事前共有鍵を設定する
Router1# ipsec ike remote address 1 10.0.0.2  ❻
Router1#
Router1# ipsec sa policy 101 1 esp aes-cbc sha-hmac  ❼ ※IPsec SAを設定する
Router1#
Router1# ipsec auto refresh on  ❽ ※IKEの鍵交換を始動する
Router1#
Router1# tunnel select 1  ❾
Router1tunnel1# ipsec tunnel 101  ❿
Router1tunnel1# tunnel enable 1  ⓫
```

❶ Tunnel1インタフェースをネクストホップとする192.168.1.0/24へのスタティックルートを設定する IOS ip route
❷ LAN1インタフェースのIPアドレスを設定する IOS interface ⇒ ip address
❸ セキュリティゲートウェイ識別子1に対して、IKEキープアライブ機能を有効にする
IOS crypto isakmp keepalive
❹ セキュリティゲートウェイ識別子1に対して、自分のセキュリティゲートウェイのIPアドレスを10.0.0.1に設定する IOS –
❺ セキュリティゲートウェイ識別子1に対して、事前共有鍵を「yamaha」に設定する
IOS crypto isakmp policy ⇒ authentication pre-share ⇒ crypto isakmp key
❻ セキュリティゲートウェイ識別子1に対して、相手のセキュリティゲートウェイのIPアドレスを10.0.0.2に設定する IOS crypto map ⇒ set peer
❼ IPsec SAポリシー番号101とセキュリティゲートウェイ識別子1に対して、使用する暗号アルゴリズムとハッシュアルゴリズムをそれぞれ「aes-cbc」、「sha-hmac」に設定する IOS crypto ipsec transform-set ⇒ crypto map ⇒ set transform-set
❽ IKEの鍵交換は能動的に始動する IOS –
❾ Tunnle1インタフェース1を選択する IOS –
❿ IPsec SAポリシー番号101のポリシーをTunnle1インタフェースに適用する IOS interface ⇒ crypto map
⓫ Tunnle1インタフェース1を有効にする IOS –

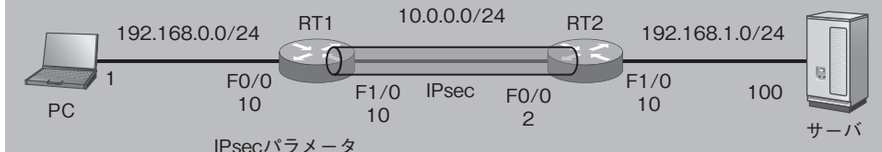
○リスト10.1.4b：Router2の設定（ヤマハルーター）

```
Router2# ip route 192.168.0.0/24 gateway tunnel 1
※PCのネットワークへの通信はTunnel1インタフェースに渡す
Router2#
Router2# ip lan1 address 192.168.1.10/24
Router2# ip lan2 address 10.0.0.2/24
Router2#
Router2# ipsec ike keepalive use 1 on ※IKEキープアライブを有効にする
Router2# ipsec ike local address 1 10.0.0.2
Router2# ipsec ike pre-shared-key 1 text yamaha ※事前共有鍵を設定する
Router2# ipsec ike remote address 1 10.0.0.1
Router2#
Router2# ipsec sa policy 101 1 esp aes-cbc sha-hmac ※IPsec SAを設定する
Router2#
Router2# ipsec auto refresh on ※IKEの鍵交換を始動する
Router2#
Router2# tunnel select 1
Router2tunnel1# ipsec tunnel 101
Router2tunnel1# tunnel enable 1
Router2tunnel1#
```


Ciscoルーターの場合

ネットワーク図は**図10.1.5**で、Ciscoルーターでの設定は**リスト10.1.5a**と**10.1.5b**のようになります。

○図10.1.5：IPsecによる拠点間接続①（Ciscoルーター）



IKEフェーズ	パラメータ	パラメータ値	
		RT1	RT2
1	事前共有鍵	cisco	cisco
2	暗号アルゴリズム	esp-aes	esp-aes
	ハッシュアルゴリズム	esp-sha-hmac	esp-sha-hmac

○リスト10.1.5a：RT1の設定（Ciscoルーター）

```
RT1#configure terminal
RT1(config)#crypto isakmp policy 1
RT1(config-isakmp)#authentication pre-share
RT1(config-isakmp)#exit
RT1(config)#crypto isakmp key 0 cisco address 10.0.0.2
RT1(config)#crypto ipsec transform-set IPSEC esp-aes esp-sha-hmac
RT1(cfg-crypto-trans)#exit
RT1(config)#access-list 100 permit ip 192.168.0.0 0.0.0.255 192.168.1.0
0.0.0.255
```

（つづく）