

# 《基礎編》 第3章

## TCP/IP

この章では、まず IP, TCP, UDP について解説する。次に、IP ネットワークの制御用／管理用プロトコルである、ARP, ICMP, DHCP について解説する。また、今日の IP ネットワークにおいて欠かせない技術である、NAT, ルーティングについても解説する。

午後試験では、この知識を前提とした設計問題が出題されている。表面的な理解だけでなく、ネットワーク構成技術の中でこれらの要素技術がどのように機能しているか、しっかり学習しておく必要がある。

試験対策のアドバイス	3.1
IP	3.2
TCP／UDP	3.3
ARP	3.4
ICMP	3.5
DHCP	3.6
NAT	3.7
ルーティング	3.8
IPv6	3.9

# 3.1 • 試験対策のアドバイス

ここでは、午後試験の出題例を紹介し、試験対策として押さえておくべき事柄を解説する。出題傾向や難易度を踏まえた上で、効率よく学習していただきたい。

## 3.1.1 出題傾向

本章の項目に合わせて、出題傾向について解説し、主要な出題例を紹介する。

なお、本章の「試験に出る」には、ここに挙げたもの以外の出題例を含め、網羅的に掲載している。併せて参照していただきたい。

### ● IP/TCP/UDP

IPについては、新技術の扱いで **IPv6** が平成 24 年午後Ⅱ問 2 で出題された。TCP については、TCP の**再送処理**や**フロー制御**などの基本機能がしばしば出題されている。

表：IP/TCP/UDP に関する出題例

出題例	内容
平成 27 年午後Ⅱ問 1	<ul style="list-style-type: none"> <li>UDP は、TCP と異なりコネクション確立と終了の手順が不要であるため、性能が良い</li> <li>TCP コネクションの保持時間を短縮するため、再送タイムアウト値を調整する。ただし、正常な通信に支障が出ない範囲とする</li> </ul>
平成 26 年午後Ⅱ問 2	<ul style="list-style-type: none"> <li>TCP の再送処理</li> </ul>
平成 24 年午後Ⅱ問 2	<ul style="list-style-type: none"> <li>NAT64 方式の IPv6 トランスレータを用いた設計（本文から推論する応用問題）</li> </ul>
平成 22 年午後Ⅰ問 1	<ul style="list-style-type: none"> <li>プロキシサーバの先読み機能の有無による TCP コネクションの発生状況の相違</li> <li>TCP 通信のスループット</li> </ul>
平成 22 年午後Ⅰ問 2	<ul style="list-style-type: none"> <li>非優先の TCP 通信で発生する速度低下</li> </ul>

### ● ARP

ARP キャッシュを更新する必要性を問うものなど、応用問題が出題されている。

表：ARP に関する出題例

出題例	内容
平成 26 年午後Ⅰ問 2	<ul style="list-style-type: none"> <li>フェールオーバ時に、クライアント端末の ARP キャッシュを更新するために Gratuitous ARP を送信する</li> </ul>

(表は次ページに続く)

出題例	内容
平成 25 年午後 II 問 2	・モバイル IP を用いたローミングの設計において、Gratuitous ARP, Proxy ARP が使用される目的（本文から推論する応用問題）
平成 20 年午後 II 問 1	・仮想マシンのライブマイグレーション時に、同一ブロードキャストドメイン内のスイッチから見たときに仮想 MAC アドレスとポートの対応関係が変化する。スイッチの MAC アドレステーブルを更新するために RARP を送信する

## ● DHCP

DHCP スヌーピング、DHCP クライアントに固定 IP アドレスを割り当てる方法など、応用問題が出題されている。

表：DHCP に関する出題例

出題例	内容
平成 25 年午後 I 問 2	・DHCP スヌーピング ・DHCP クライアントの MAC アドレスに基づき、DHCP サーバから固定 IP を割り当てる方法
平成 19 年午後 I 問 1	・DHCP リレーエージェント
平成 17 年午後 I 問 2	・DHCP サーバがモバイル端末に割り当てる IP アドレスのリース期間

## ● NAT

NAT 越えの問題など、応用問題が出題されている。

表：NAT に関する出題例

出題例	内容
平成 28 年午後 II 問 1	・P2P 通信（ピアツーピア通信）の NAT 越えに STUN サーバを用いる
平成 27 年午後 II 問 2	・グローバル IP アドレス枯渇対策として、NAT444 を用いる（本文から推論する応用問題） ・NAT を越えるとき、IPsec 通信において、AH, ESP, IKE のそれぞれに問題があり、それを解決するために NAT トラバーサルが必要である
平成 26 年午後 II 問 2	・セッション生成時の SIP メッセージで発信元端末のプライベート IP アドレスを通知しているため、通常の NAT 装置を通過すると、通話セッションが行えなくなる
平成 24 年午後 II 問 2	・NAT64 方式の IPv6 トランслータを用いた設計（本文から推論する応用問題）
平成 22 年午後 II 問 2	・プライベート IP アドレスを割り当てられたモバイル端末から IPsec を使用するとき、IPsec では NAT を越えられないため、ルータに VPN パススルー機能が必要となる
平成 20 年午後 II 問 1	・NAT 環境下にある IPsec-VPN を使用するときは、ダミーの UDP ヘッダを使用しないと NAT を越えることができない

## ● ルーティング

ダイナミックルーティングプロトコルを使用した経路冗長化の設計、拠点間通信のパケットだけがVPNトンネルを通過するように経路制御する設計など、応用問題が出題されている。

表：ルーティングに関する出題例

出題例	内容
平成 28 年午後Ⅱ問 2	<ul style="list-style-type: none"> <li>インターネット VPN、広域イーサ網、専用線の 3 系統で WAN 回線を冗長化し、OSPF を用いてダイナミックルーティングを実施する。インターネット VPN では、GRE over IPsec にカプセル化して OSPF リンクステート情報を交換し合う。</li> </ul>
平成 26 年午後Ⅰ問 1	<ul style="list-style-type: none"> <li>OSPF を用いた冗長化設計において、障害時にどのような迂回ルートが選択されるか</li> <li>エリア境界ルータでどのようにアドレスが集約されるか</li> <li>PBR (Policy Based Routing) を用い、特定の IP アドレスとポート番号の組をもつパケットを特定のデバイスにルーティングする。その際、通常のルーティング方式よりも PBR の優先度を高く設定しておく</li> </ul>
平成 22 年午後Ⅱ問 2	<ul style="list-style-type: none"> <li>VRF (Virtual Router Forwarding)</li> </ul>
平成 23 年午後Ⅱ問 1	<ul style="list-style-type: none"> <li>VPN トンネルを使用したときのルーティングテーブルの設定（本文から推論する応用問題）</li> <li>ロングストマッチアルゴリズムでは同等の経路が複数存在する場合、最もメトリックの小さい経路が選択される</li> <li>null インタフェースを用いてパケットを破棄する</li> </ul>
平成 21 年午後Ⅰ問 3	<ul style="list-style-type: none"> <li>デフォルトゲートウェイとサブネットマスクの設定ミスによる障害の原因解析と解決策</li> </ul>
平成 21 年午後Ⅱ問 2	<ul style="list-style-type: none"> <li>ルーティングテーブルの設定ミスに起因する障害の原因分析と対策</li> </ul>
平成 20 年午後Ⅰ問 4	<ul style="list-style-type: none"> <li>正常時は待機系の経路にトラフィックを分散させない場合、待機系の経路側のインターフェースのコスト値を大きくする</li> <li>デフォルトではルータに直接接続しているインターフェースの帯域に基づいてコスト値が割り振られるため、構成によっては正常系と待機系の経路が等コストになってしまい、ルータは二つの経路にトラフィックを分散してしまう</li> </ul>
平成 18 年午後Ⅰ問 4	<ul style="list-style-type: none"> <li>ロングストマッチアルゴリズムの動作</li> </ul>
平成 17 年午後Ⅰ問 4	<ul style="list-style-type: none"> <li>BGP では経由する AS 数に基づいて経路選択が行われる</li> </ul>
平成 16 年午後Ⅱ問 1	<ul style="list-style-type: none"> <li>フローティングスタティックルーティングを用いたバックアップ経路設計</li> </ul>

### 3.1.2 学習ポイント

出題傾向を踏まえて、何をどのように学習したらよいかを解説する。

## ● IP/TCP/UDP

IPv6は、過去1回（平成24年）、新技術の扱いで出題され、本文に動作原理が詳しく解説されていた。その出題趣旨の中で、IPv6について「昨今、活用事例も増えてきた。IPv6は、ネットワーク技術者にとって避けて通ることのできない技術である」とコメントされていたことに注目できる。それゆえ、今後も出題される可能性が高いと考えられる。

次回は、近隣探索やアドレス自動設定など、IPv4との相違点が問われるかもしれません。

IPv6が出題されたとしたら、おそらく次回も「新技術」の扱いとなると考えられるので、本文にヒントが書いてあるはずだ。したがって、真に問われているのは、基礎知識の正確な理解である。本章でしっかりと身に付けておきたい。

TCPは、再送処理やフロー制御は今後も出題される可能性があるので、学習しておく必要がある。本章の「3.3.4 TCPコネクション」の「試験に出る」に出題例を詳しく列挙しているので、自分の目で確かめてみることをお勧めする。重要な着眼点は、繰り返し出題される可能性があるからだ。

## ● ARP

ARP自身の知識習得は易しいが、Gratuitous ARPなどの応用問題を解けるように学習しておく必要がある。

本章の「3.4.2 特殊な用途のARP」の「試験に出る」に出題例を詳しく列挙しているので、自分の目で確かめてみることをお勧めする。重要な着眼点は、繰り返し出題される可能性があるからだ。

## ● ICMP

ICMPの出題頻度は高くないが、ICMPの重要な応用である、ping、traceroute、経路MTUについて学習しておくとよいだろう。

ICMPについては、パケットフォーマットやメッセージの詳細な知識までは問われていない。知識習得の優先度を下げてよいだろう。

## ● DHCP

DHCPについては、DHCPスヌーピングなどの応用問題が出題されている。本文中に動作原理が解説されているので、基礎知識の習得が重要となる。初期リースの取得、リースの更新と解放、DHCPリレーエージェントなど、DHCPの一連の動作について学習しておく必要がある。

DHCPについては、パケットフォーマットやメッセージの詳細な知識までは問われていない。基本的なシーケンスの流れを学習しておけばよいだろう。

## ● NAT

NAT 自体の知識習得は易しいが、試験対策としては、**NAT 越え**などの応用問題を解けるように学習しておく必要がある。

本章の「3.7.2 NAT 越え」の「試験に出る」に挙げた出題例を読み、実際にどのように技術的課題が克服されているかを調べてみることをお勧めする。

## ● ルーティング

基本となる**ロングストマッチアルゴリズム**を、まずはしっかり学習しておく必要がある。

ルーティングについては、設計の応用問題として出題される傾向がある。本節で紹介した過去問題を参考にしながら、アドレスの集約、経路の冗長化などの設計能力を培っておく必要がある。

ダイナミックルーティングプロトコル（RIP, OSPF, BGP4）については、パケットフォームマットやメッセージの詳細な知識までは問われていない。この点については、知識習得の優先度を下げてよいだろう。

## 3.2 • IP

IPは、TCP/IPのネットワーク階層モデルではインターネット層に位置するプロトコルである。インターネットでは、TCPと並んで中核をなすプロトコルなので、プロトコルの特徴、ヘッダの主要なフィールドについてしっかり学習しておく必要がある。

### 3.2.1 IP の特徴

IP (Internet Protocol) は、TCP/IPのネットワーク階層モデルではインターネット層に位置するプロトコルである。次世代のバージョンとしてIPv6（バージョン6）の規格も定まっている。割当て可能なIPv4アドレスブロックの枯渇を機に、インターネットに公開しているサーバはIPv4とIPv6の双方に対応することが求められており、重要性を増していく技術である。以下、特に断りがない場合、「IP」という表記はIPv4を指すものとする。

IPはコネクションレス型のプロトコルである。通信する両端のホスト間でパケットを伝送する機能を有し、パケット単位のエラーチェック機能、MTUを超えるパケットの分割機能／再構築機能をもつ。パケット廃棄の検知及び再送が必要な場合は、上位層にTCPを用いて通信する。

IPはコネクション方式とは異なり、パケットの順序管理、パケット廃棄に伴う再送要求、ウインドウを用いたフロー制御、輻輳制御（スロースタートや輻輳回避）などを行わない。したがって、コネクション確立フェーズ、確認応答処理、再送処理、スロースタートといった、コネクション管理に特化したやり取りに伴う遅延が発生しない。



#### 用語解説

**MTU**  
Max Transfer Unit。データリンクの最大転送単位

## 3.2.2 IP ヘッダ

IP パケットは、次のような構造のヘッダをもつ。

### 関連RFC



RFC791 (STD5)



試験に出る

IP ヘッダについて、平成 18 年  
午前 問 22 で出題された



試験に出る

過去の午前問題の出題例があるものなど、試験対策上重要な項目に★印を付している



試験に出る

フラグメンテーションについて、  
平成 29 年午後 I 問 3、平成  
28 年午後 II 問 2、平成 26 年  
午後 I 問 3 で出題された。トン  
ネリングに伴うヘッダ追加により  
フラグメンテーションが発生す  
ることについて、平成 25 年午  
後 II 問 2 で出題された

0	4	8	16	19	31
Version(4) バージョン	IHL (4) ヘッダ長	Type Of Service (8) サービスタイプ	Total Length (16) パケット長		
Identification (16) 識別子			Flags (3) フラグ	Fragment Offset (13) フラグメントオフセット	
Time To Live (8) 生存時間		Protocol (8) プロトコル番号	Header Checksum (16) ヘッダチェックサム		
Source Address (32) 送信元IPアドレス			Options オプション		
Destination Address (32) 宛先IPアドレス			Padding パディング		

注：（）内の数字はビット数。

図：IP ヘッダ

それぞれの領域（フィールド）の意味を次に示す。

### ● バージョン

バージョン 4 を表す「0x04」が格納される。

### ● ヘッダ長

単位は 4 バイトである。オプションがない場合、IP ヘッダ  
は 20 バイトなので、「0x05」が格納される。

### ● サービスタイプ (TOS : Type Of Service) (★)

ルータがこのパケットを転送する際のサービス品質を表  
す。

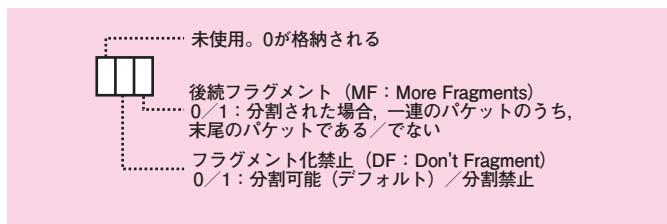
### ● 識別子

送信側で IP パケットを送出するたびに ID 値を割り当てる。

### ● フラグ、フラグメントオフセット (★)

ルータは、IP データグラムを転送する際、データグラムの  
長さがリンクの MTU (Max Transfer Unit, 最大転送単位)  
を超えていたら、MTU に収まるように IP データグラムを  
分割する。分割した各々のデータグラムに IP ヘッダを付  
加し、複数個の IP パケットを生成する。これを **フランクメ  
ンテーション** という。分割された IP パケットは、宛先ホス

トで再構築される。このフラグメント処理を行うため、IP ヘッダにフラグ（3 ビット）とフラグメントオフセット（13 ビット）が定義されている。フラグの種類には、フラグメント化禁止ビット、分割パケットの末尾であるか否かを表示するビットがある。送信ホストによって「分割禁止」がセットされていた場合、その IP データグラムの長さが MTU を超えたときはルータによって破棄される。その際、ルータは送信元ホストに ICMP パケット（宛先到達不能）を送信する。



図：フラグ（3 ビット）の内訳

フラグメントオフセットには、分割されたデータグラムがオリジナルデータのどこに位置していたかを示すオフセット値（単位は 8 バイト）が入っている。分割されたパケットが全て届いていれば、順番どおりではなくても、フラグメントオフセットを用いて元どおりに復元することができる。

#### ● 生存時間（TTL : Time To Live）（★）

ルータを経由するごとに、この値が一つずつ減っていく。この値が「0」になるとパケットは破棄され、ルータから ICMP パケット（時間超過）が送信元ホストへ送信される。

#### ● プロトコル番号（★）

上位層のプロトコルを識別する番号で、ICANN によって管理されている。最新情報は以下のサイトから入手できる。

<http://www.iana.org/assignments/protocol-numbers>

主要なプロトコル番号を次に示す。

**IGMP**

Internet Group Management Protocol。マルチキャストグループへの参加や離脱をホストが通知したり、マルチキャストグループに参加しているホストの有無をルータがチェックするときに使用するプロトコル

**IANA**

Internet Assigned Number Authority。インターネット上で利用される資源（IP アドレス、ドメイン名、ポート番号など）を管理する組織だったが、1998 年に ICANN に移管された

**ICANN**

Internet Corporation for Assigned Names and Numbers。インターネット上で利用されるアドレス資源（IP アドレス、ドメイン名、ポート番号など）を管理する組織で、1998 年に設立された民間の非営利法人である。IANA の後継に当たる



ルータは、APIPA で割り当てられた IP アドレスをもつパケットをルーティングしてはいけないとになっている。そのため、通信できる範囲は同一のブロードキャストドメイン内に限定される。デフォルトゲートウェイは設定されない

表：IP ヘッダのプロトコル番号

プロトコル番号	プロトコル
1	ICMP
2	IGMP
4	IP in IP (encapsulation)
6	TCP
17	UDP
46	RSVP
50	ESP
51	AH
89	OSPF (ICANN には「OSPFIGP」として登録)

## ● ヘッダチェックサム

IP ヘッダのビットレベルの整合性チェックを行う。TTL がルータを経由するたびに一つ減算されるため、このヘッダチェックサムもその都度再計算される。

## ● IP アドレス (★)

通信を行う両端ホストの IP アドレスである。

IP アドレスは ICANN によって管理されており、用途に応じて、以下の範囲が予約されている。

表：予約されている IP アドレス

IP アドレスの範囲	用 途
127.0.0.0 ~ 127.255.255.255	ループバックアドレス。通常は、127.0.0.1 が使用されている
169.254.0.0 ~ 169.254.255.255	リンクローカルアドレス。自動プライベート IP アドレス指定 (APIPA : Automatic Private IP Addressing) で使用される。APIPA とは、DHCP サーバがないとき、ホスト自身がこの範囲から IP アドレスをランダムに設定する機能である。なお、サブネットマスク長は 16 ビットである
224.0.0.0 ~ 239.255.255.255	マルチキャストアドレス
255.255.255.255 ~ 255.255.255.255	制限ブロードキャストアドレス。限定的ブロードキャストアドレスともいう。ネットワークアドレスを指定せずに、送信元ホストが所属するサブネットにブロードキャストを送出するときに使用する
10.0.0.0 ~ 10.255.255.255	プライベートアドレス
172.16.0.0 ~ 172.31.255.255	
192.168.0.0 ~ 192.168.255.255	

最新情報は以下のサイトから入手できる。

<http://www.iana.org/assignments/ipv4-address-space>

### 3.2.3 IP パケット

IP パケットは、その到達範囲により次の三つに分類できる。

- ユニキャストパケット

宛先が1台のホストであるパケット。

- マルチキャストパケット

宛先が特定の機能や役割をもつ複数のホストであるパケット（宛先は同一ネットワークに限定されてはいない）。

- ブロードキャストパケット

宛先が同一ネットワーク内の全てのホストであるパケット。

ブロードキャストパケットが到達する範囲を **ブロードキャストドメイン** という。ブロードキャストパケットには、次に示す二つの種類がある。

表：ブロードキャストパケットの種類

種類	説明
ディレクテッドブロードキャスト	指定されたサブネットの全ホストを宛先とするブロードキャスト。自分と異なるサブネットを指定することができる。宛先 IP アドレスは、ネットワーク部に送信対象のネットワークアドレスが指定され、ホスト部は全てのビットが「1」になる
ローカルブロードキャスト	ディレクテッドブロードキャストの一種であり、自分と同じサブネットの全ホストを宛先とするブロードキャスト。宛先 IP アドレスは、ネットワーク部に自己ネットワークアドレスが指定され、ホスト部は全てのビットが「1」になる
制限ブロードキャスト (リミテッドブロードキャスト)	宛先 IP アドレスに 255.255.255.255 を使用し、自分と同じサブネットの全ホストを宛先とするブロードキャスト。 制限ブロードキャストパケットを使用しているプロトコルの例は、DHCP である。DHCP クライアントは、ホストを起動した直後に DHCP 発見パケットを送信する。起動時には IP アドレスやサブネットなどの情報がないので、宛先 IP アドレスに制限ブロードキャストアドレスが用いられる

ルータは、ローカルブロードキャストと制限ブロードキャストパケットを中継しない。一方、他ネットワーク宛てのディレクテッドブロードキャストはルータを越えて中継されるが、DoS 攻撃 (smurf 攻撃など) を防ぐために、デフォルトで禁止しているルータがある (Cisco IOS など)。



#### 試験に出る

マルチキャスト通信を用いたオーバーレイネットワークの設計問題が、平成 27 年午後Ⅱ問 2 で出題された。なお、マルチキャスト通信の仕組みについては、本間に詳しく解説されていた。マルチキャストについて、平成 26 年午前Ⅱ問 4、平成 22 年午前Ⅱ問 12、平成 16 年午前問 24 で出題された。

マルチキャストへの参加と離脱をホストが通知したり、グループに参加しているホストの有無をルータがチェックしたりする機能をもつ IGMP について、平成 27 年午前Ⅱ問 8、平成 27 年午後Ⅱ問 2、平成 24 年午前Ⅱ問 11、平成 20 年午前問 30 で出題された



#### 用語解説

##### IP データグラム

IP のデータ転送の単位であり、IP ヘッダと IP データからなる。IP パケットと同義である。ただし、フラグメンテーションが発生したとき、一個の IP データグラムは複数の IP パケットに分割されるので厳密には両者は異なる

## 3.3 • TCP／UDP

IP 同様、午後問題において TCP／UDP そのものについて出題されることはない。しかし、TCP／UDP についても、表面的な理解だけでなく、構成例の中でそれぞれの技術がどのように機能しているかというところまで理解を深めてほしい。

### 3.3.1 TCP／UDP の特徴

**TCP** (Transmission Control Protocol) と **UDP** (User Datagram Protocol) は、TCP/IP のネットワーク階層モデルではトランsport 層に位置するプロトコルである。いずれも通信する両端のアプリケーション間でパケットを送受信する機能を有するが、TCP は**コネクション型**、UDP は**コネクションレス型**である点が異なる。IP ヘッダ中の IP アドレスにより両端のホストが識別され、TCP 又は UDP ヘッダ中の**ポート番号**により両端のアプリケーションが識別される。



#### コネクション

通信を行う両端のアプリケーション間に結ばれた仮想的な通信路

TCP はコネクションを確立した後、コネクション単位でパケットの**順序管理**を行う。エラーを検知した際は、**再送**要求を行うことにより、信頼性の高い通信を実現している。加えて**連續転送**や**フロー制御**など、様々な機能を実装している。

UDP はコネクションを確立しないので、IP と同様、パケット単位の通信を行う。そのため、アプリケーションデータ単位の通信では信頼性が保証されていない。その代わり、TCP よりもヘッダが簡略化されている分、1 パケットに占めるデータの割合が大きくなる傾向がある。さらに、確認応答処理や再送処理に伴う遅延が発生しない。したがって、単位時間当たりに通信できるデータ量は、TCP よりも UDP の方が多くなる傾向を示す。それゆえ、DNS など、概して要求／応答の 1 往復で事足りるプロトコルで、使用頻度が高い通信に用いられる。また、音声通信など、多少のパケット廃棄は許容できるので再送処理は不要であるが、大幅な遅延が問題視される通信に用いられる。なお、パケット廃棄の検知及び対応は、必要ならばアプリケーション層で行う。

## 3.3.2 TCP ヘッダ

TCP のヘッダフォーマットを次に示す。

0	4	10	16	19	31
Source Port (16) 送信元ポート番号	Destination Port (16) 宛先ポート番号				
Sequence Number (32) シーケンス番号					
Acknowledgement Number (32) 確認応答番号					
Data Offset(4)	Reserved (6)	Control flag (9)	Window (16)	Window (16)	Window (16)
Checksum (16) チェックサム	Urgent Pointer (16) 緊急ポインタ				
Options オプション	Padding パディング				

注：( )内の数字はビット数。

図：TCP ヘッダ

それぞれの領域（フィールド）の意味を次に示す。

- ポート番号（★）

通信を行うアプリケーション（アプリケーションプロトコル）を識別する番号である。パケットを受信したホストの OS は、宛先ポート番号に基づき、該当するアプリケーションにデータを受け渡す。HTTP などのように広く使用されているアプリケーションプロトコルは、ポート番号が標準で定められている。これは **ウェルノウンポート番号** (Well-known Port Number) と呼ばれ、ポート番号の 0 ~ 1023までの範囲がこれに該当する。（HTTP サーバなどの）サーバアプリケーションは、サーバホストの OS からポート番号が割り当てられた状態で起動しており、クライアントからのリクエストを処理できるよう待機している。通常、サーバアプリケーションのポート番号はウェルノウンポート番号（1023以下の値）を使用しているが、アプリケーションプロトコルによっては、別のポート番号を使用しているケースもある。例えば、パッシュモードの FTP サーバは、データチャネルのポート番号として 1024 以上のものを使用する（動的に決定される）。更



試験に出る

TCP ヘッダについて、平成 19 年午前 問 31（平成 17 年午前 問 26 と同じ問題）で出題された



TCP は RFC793 (STD7)。ただし、一部はアップデートされ、別の RFC で標準化されているので注意



試験に出る

過去の午前問題の出題例があるものなど、試験対策上重要な項目に★印を付している

1

2

3

4

に、ベンダ独自のプロトコルでは 1024 番以上のポート番号が使用されることが多い。例えば、RDBMS 製品の一つである Oracle は、リスナーのポート番号として 1521 番を使用している。Web ブラウザなどクライアントアプリケーションは、クライアントホストの OS が、起動時に動的にポート番号を割り当てる（通常は、1024 番以上のポート番号の中から割り当てられる）。ポート番号は ICANN が管理しており、最新情報は以下のサイトから入手できる。

<http://www.iana.org/assignments/port-numbers>

TCP と UDP における代表的なポート番号を次に示す。

表：代表的なウェルノウンポート番号（TCP）



TCP のポート番号について、平成 25 年午前 II 問 15 で出題された。TCP を使用するアプリケーションについて、平成 16 年午前 問 23 で出題された

ポート番号	プロトコル	説明
20	ftp-data	File Transfer Protocol [Data]
21	ftp-control	File Transfer Protocol [Control]
22	ssh	Secure Shell Remote Login Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transfer Protocol
43	nicname	Whois
53	domain	Domain Name System
80	http	Hyper Text Transfer Protocol
110	pop3	Post Office Protocol version 3
113	auth (ident)	Authentication Service
137	netbios-ns	NETBIOS Name Service
139	netbios-ssn	NETBIOS Session Service
143	imap	Internet Message Access Protocol
179	bgp	Border Gateway Protocol
389	ldap	Lightweight Directory Access Protocol
443	https	http protocol over TSL/SSL
445	microsoft-ds	Direct Hosting SMB Service

表：代表的なウェルノウンポート番号（UDP）

ポート番号	プロトコル	説明
53	domain	Domain Name System
67	dhcp-s	Dynamic Host Configuration Protocol Server
68	dhcp-c	Dynamic Host Configuration Protocol Client
69	tftp	Trivial File Transfer Protocol
123	ntp	Network Time Protocol
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
161	snmp	Simple Network Management Protocol
162	snmp-trap	Simple Network Management Protocol Trap
520	rip	Routing Information Protocol

### ● シーケンス番号 (★)

データ通信フェーズの期間中、送信したデータの順番はシーケンス番号によって管理されている。コネクションが確立された後、両端はシーケンス番号、確認応答番号（相手のシーケンス番号）を保持している。パケットを送信するとき、自分が保持しているシーケンス番号、確認応答番号をヘッダに格納する。その後、送信側は自分が保持しているシーケンス番号にデータのバイト数を加算する。なお、コネクション確立フェーズの SYN フラグ、コネクション切断フェーズの FIN フラグも、1 バイト分のデータと見なしでシーケンス番号に加算される。シーケンス番号、確認応答番号のサイズは 4 バイトであり、32 ビット値が巡回的に使用される（「0xFFFFFFFF」の次の値は「0x00000000」になる）。

### ● 確認応答番号 (★)

次に受信すべきシーケンス番号。送信側は、返された確認応答番号と次に送るシーケンス番号が同じであることを確認すれば、正常に通信が行われているか確認することができる。

### ● データオフセット

TCP セグメント内のデータ開始位置。事実上、ヘッダ長と同じ意味である。単位は 4 バイトである。オプションがない場合、TCP ヘッダは 20 バイトなので、「0x05」が格納される。

### ● 予約

将来のために予約されており、「0」が格納される。

### ● コントロールフラグ (★)

コントロールビットとも呼ばれ、次の図に示す 9 ビットで構成されている。各ビットを「**フラグ**」という。

N	C	E	U	A	P	R	S	F
S	W	C	R	C	S	S	Y	I
R	E	G	K	H	T	N	N	N

図：コントロールフラグ

## 参考

TCP/IPが規格化された当初は、ECNの仕組みがなかった。ECNを実現するため、IPヘッダのTOSフィールドの一部をECNフィールドとして再定義し、TCPヘッダにECN用のフラグを追加している。

ECNは、1往復のやり取りで、輻輳を通知する。簡単に説明すると、往路は輻輳通知の依頼と輻輳の検出、復路は輻輳通知である。

まず、往路では、輻輳発生を知りたいホストが、IPヘッダ中のECNフィールドを用い、「輻輳が発生していたら返信時に自分に通知してほしい」という依頼を通信相手に伝える。通信経路上のルータは、輻輳通知を依頼しているパケットを転送する際、実際に輻輳が発生していることを検出したならば、IPヘッダ中のECNフィールドにこれを記録する。

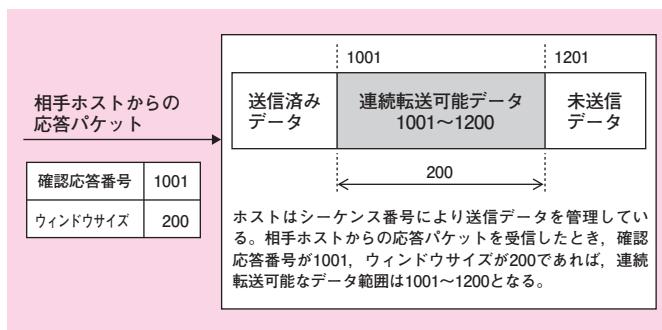
次に、復路では、通知依頼を受けた通信相手のホストが、TCPヘッダ中のECN用のビットを用いて、輻輳の有無を伝える

それぞれのフラグの意味を次に示す。

- ・ **NS (ECN-nonce)**
- ・ **CWR (Congestion Window Reduced)**
- ・ **ECE (ECN-Echo)**  
輻輳が発生していることを通信相手に通知する機能である、明示的輻輳制御(ECN: Explicit Congestion Notification)で使用する。
- ・ **URG (Urgent)**  
このビットが立っている場合、緊急に処理すべきデータが含まれていることを示している。ホストが緊急データを受信すると、受信アプリケーションの割込みが入るので、アプリケーションは緊急データをただちに処理する。
- ・ **ACK (Acknowledgement)**  
このビットが立っている場合、確認応答番号のフィールドが有効である。コネクション確立フェーズで最初に送られるパケット以外は、このビットは必ず「1」になっている。
- ・ **PSH (Push)**  
このビットが立っている場合、受信したデータはバッファリングされずに、ただちに上位アプリケーションに渡される。例えば、HTTPではサーバへファイル取得を要求するが、サーバから返信されるTCPセグメントには、PSHがセットされている。よって、クライアントOSは、受信したデータをブラウザに渡すことができる(複数セグメントに分割された場合は、最後のセグメントにPSHがセットされている)。
- ・ **RST (Reset)**  
このビットが立っている場合、コネクションが強制的にリセットされる。
- ・ **SYN (Synchronize)**  
コネクション確立フェーズで使用される。このビットが立っている場合、コネクション確立要求を意味している。
- ・ **FIN (Fin)**  
コネクション切断フェーズで使用される。このビットが立っている場合、コネクション切断要求を意味している。

### ・ ウィンドウサイズ

「**ウィンドウサイズ**」とは、受信確認を待たずに送信できるデータサイズの最大値であり、簡単には、「受信バッファの空き容量」と言い換えることができる。通常、ウィンドウサイズの初期値はTCPの**MSS**(Max Segment Size, 最大セグメント長)を整数倍した値が設定されるが、通信中の受信状態に応じて変動する。ホストは、送信時に現在の空き容量をウィンドウサイズに格納して相手に通知する。相手ホストは、通知されたウィンドウサイズに達するまで、確認応答を待たずにデータを連続転送することができる。確認応答パケットを受けると、次はそのパケットに格納されているウィンドウサイズまでデータを連続転送する。そのパケットに格納されている確認応答番号は、次に受信すべきシーケンス番号を示しているので、送信側から見た連続転送可能なデータ範囲は、確認応答番号を起算点とするウィンドウサイズ分となる。確認応答のたびに、連続転送可能な範囲がウィンドウで示され、これが次第に移動(スライド)していく。このような方式を**スライディングウィンドウ方式**と呼ぶ。この方式では、確認応答を待つ時間を省くことによって単位時間当たりのデータ転送量が増すので、効率の高いデータ通信を実現することができる。



図：スライディングウィンドウ方式

なお、受信側ホストのウィンドウサイズが「0」と通知され



ウィンドウサイズは、ウィンドウスケーリング(RFC1323)が有効でない限り、最大値は64KBである

1

2

3

4



試験に出る

ウィンドウサイズについて、平成28年午前Ⅱ問12で出題された。ウィンドウによるフロー制御について、平成29年午前Ⅱ問11、平成26年午前Ⅱ問14で出題された



図「スライディングウィンドウ方式」は、送信側ホストが管理しているウィンドウの説明である。これを「送信ウィンドウ」と呼ぶ。ホストは、同時に自分の受信バッファもスライディングウィンドウ機構によって管理している。つまり、受信済みデータはどの範囲か、バッファに残っている受信データ（上位アブリケーションに渡していないデータ）はどの範囲か、受信可能なウィンドウサイズ（現在の空き容量）はどれほどかを管理している。これを「受信ウィンドウ」という



ウィンドウプローブに格納されるデータは、スライディングウィンドウの枠外にある未送信データであり、受信側ホストで廃棄される仕組みになっている



### TCPセグメント

TCPのデータ転送の単位であり、TCPヘッダとTCPデータから構成されるパケットの領域を指す。TCPパケットともいう

ことがある。この場合、送信側ホストはこれ以上パケットを送信できない。この状態を「ゼロウィンドウ」という。受信側ホストは、ウィンドウサイズが0より大きくなったら送信側ホストに通知する。これを「ウィンドウ更新」といい、データを格納しない確認応答パケットが用いられ、ウィンドウ領域に更新された値がセットされている。この仕組みにより、送信を再開できる。しかし、ウィンドウ更新パケットが消失するリスクに備えて、送信側ホストは定期的に「ウィンドウプローブ」と呼ばれる、1バイト分のデータを格納したパケットを送信して、確認応答パケットの返信を促す。その確認応答パケットのウィンドウサイズが「0」より大きな値に更新されていれば送信を再開する。

- チェックサム

TCPセグメント(TCPヘッダとTCPデータ)のビットレベルの整合性チェックを行う。

- 緊急ポインタ

TCPセグメント内の緊急データの位置を示す。

### 3.3.3 UDPヘッダ

## UDPヘッダ



UDPについて、平成26年午前I問10、平成25年午前I問12で出題された。UDPは、TCPと異なりコネクション確立と終了の手順が不要であるため、性能が良い。この点について、平成27年午後II問1で出題された

UDPのヘッダフォーマットを次に示す。

0	4	10	16	19	31
Source Port (16) 送信元ポート番号			Destination Port (16) 宛先ポート番号		
Length (16) パケット長			Checksum (16) checksum		

注：( )内の数字はビット数。

図：UDPヘッダ

それぞれの領域(フィールド)の意味を次に示す。

- ポート番号(★)

通信を行うアプリケーション(アプリケーションプロトコル)を識別する番号である。詳細はTCPヘッダの項を参照のこと。同じポート番号でも、TCPとUDPでは異なる

過去の午前問題の出題例があるものなど、試験対策上重要な項目に★印を付している



アプリケーションに割り当てられることがある。

#### ● パケット長

単位はバイトで、データグラム（UDP ヘッダと UDP データ）の長さ。

#### ● チェックサム

データグラム（UDP ヘッダと UDP データ）のビットレベルの整合性チェックを行う。



#### UDP データグラム

UDP のデータ転送の単位であり、UDP ヘッダと UDP データからなる。UDP パケットと同義である

### 3.3.4 TCP コネクション

#### ● TCP 通信の三つのフェーズ

TCP 通信は、次の三つのフェーズからなる。

##### 1. コネクション確立フェーズ

コネクション確立フェーズは三つのパケット（SYN, ACK / SYN, ACK）のやり取りからなる。このスリーウェイハンドシェークと呼ばれるやり取りを通して、互いの IP アドレス、ポート番号、シーケンス番号、確認応答番号、ウィンドウサイズ、MSS などを交換し合い、以降の通信に備える。次の図は、ホスト A（クライアント）からホスト B（サーバ）へコネクション確立が要求される場合の、コントロールフラグ、シーケンス番号及び確認応答番号の推移を示している。

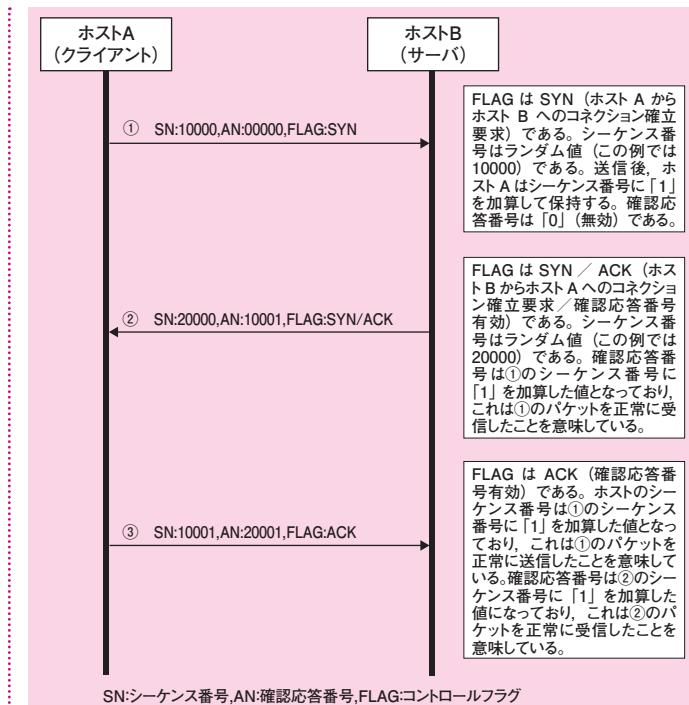


#### 試験に出る

スリーウェイハンドシェークについて、平成 25 年午前Ⅱ問 13、平成 23 年午前Ⅱ問 12 で出題された。TCP のデータ転送について平成 19 年午前 問 30 で、フロー制御について平成 18 年午前 問 21 で、コネクションについて平成 22 年午前Ⅱ 問 14、平成 18 年午前 問 24 で出題された

## 参考

通常、TCPはデータパケットを受信したとき、すぐには確認応答パケットを返信しない。これを遅延ACKという。遅延ACKの仕組みにより、そのACKと同じ方向にデータを送信する場合、そのデータパケットに便乗して確認応答を通知することができる。これをピギーバック(piggy-back, 便乗)という。この遅延ACKはタイムアウト値をもっており、多くの実装では200ミリ秒に設定されている。つまり、この時間以内にピギーバックできなければ、確認応答パケットを返信する。具体的には、図「通信フェーズ」で説明する。ホストBは、タイムアウト値以内に③を返信できれば、②の応答確認パケットの送信を省くことができる。なぜなら、③のデータパケットに格納されている確認応答番号(AN:11001)から、ホストAは、①が正常に受信できたことを確認できるからである。



図：コネクション確立フェーズ

## 2. 通信フェーズ

送信側のアプリケーションデータは、受信側のアプリケーションに順番どおり受信される。データのバイト数が MSS より大きい場合、MSS に収まるよう、複数個のパケットに分割されて送信される。このとき、相手に順番どおりデータが送られる事を保証するため、**シーケンス番号**と**確認応答番号**が用いられている。

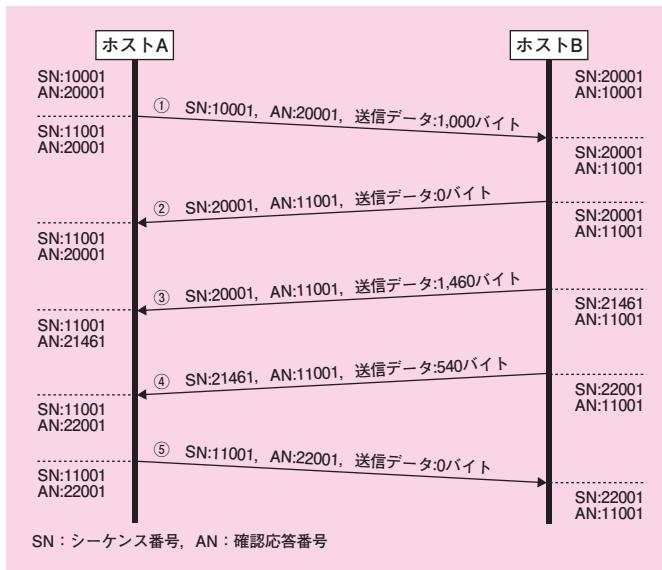
データを送信した後、送信側は自分のシーケンス番号に送信データのバイト数を加算した値を保持する。

データを受信したとき、受信側は自分が保持しているシーケンス番号とパケットの確認応答番号、及び自分が保持している確認応答番号とパケットのシーケンス番号が、ともに一致していることを確認する。正常に受信したことを確認できると、自分の確認応答番号に受信データのバイト数

を加算した値を保持する。

次の図は、通信フェーズにおける、シーケンス番号、及び確認応答番号の推移を示している。ホスト A から 1,000 バイト、ホスト B から 2,000 バイトを送信している。イーサネットの場合は MSS が 1,460 バイトなので、2,000 バイトを送信するため 2 パケットを要する（パケット③、④）。なお、パケット②、⑤は確認応答パケットであり、送信データはない。

連続転送が可能なデータの範囲は、受信した確認応答パケットに格納されている確認応答番号とウィンドウサイズの値から決定される。つまり、確認応答番号を起算点としたウィンドウサイズ分が、連続転送可能なデータの範囲となる。この範囲は、確認応答パケットを受信するたびに更新される。



図：通信フェーズ

通信フェーズでエラーが発生した場合、再送制御が行われる。それは大きく分けて、「再送タイムアウトによる方法」と、「高速再転送による方法」である。

送信したパケットに対する ACK パケットが返ってこなかつた場合、途中経路でパケットが消失したか、受信側で何ら



### 試験に出る

FW 等のセキュリティ機器がコネクションを強制的に切断したい場合、RST パケットを送付する方法が、タイムアウトを待つよりも性能面で優れていることについて、平成 27 年午後Ⅰ問 2 で出題された。

TCP コネクションの保持時間の短縮のため、再送タイムアウト値を調整する。ただし、正常な通信に支障が出ない範囲とする。この点について、平成 27 年午後Ⅱ問 1 で出題された。

FW がフェールオーバーしてもアプリケーション通信に支障がない理由は TCP がフェールオーバー時にパケットの再送処理を行っているためである。この点について、平成 26 年午後Ⅰ問 2 で出題された

1

2

3

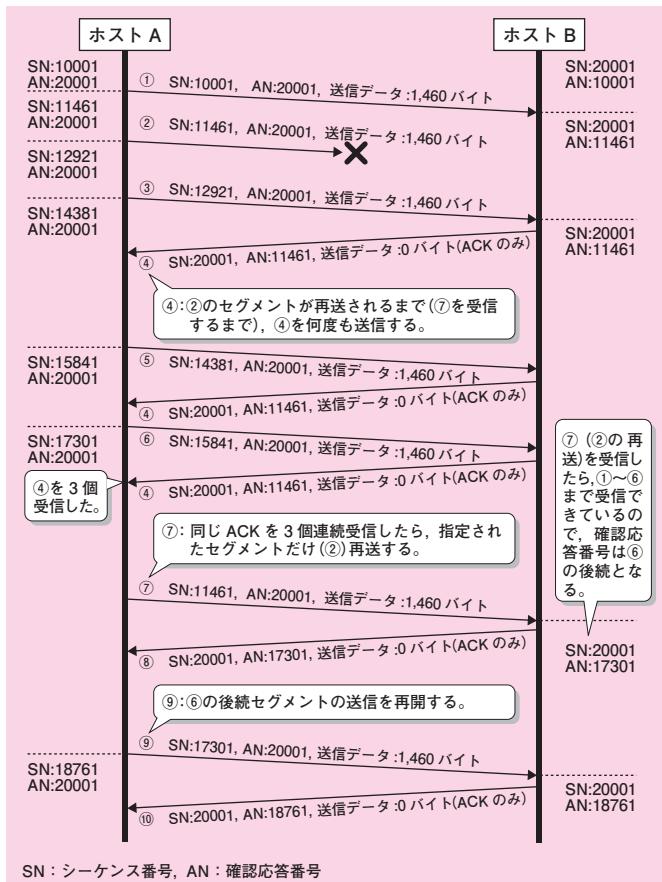
4

かのトラブルが発生して ACK を返せなかつたためと考えられる。このとき、送信側は一定期間待つてからパケットを再送する（再送するまでの時間を **RTO** (Retransmission Time Out, **再送タイムアウト**) と呼ぶ）。再送が繰り返し行われる場合は途中経路で輻輳が発生していることが原因として考えられる。そこで、RTO の値は再送のたびに 2 倍になり、最大で 64 秒になる。

TCP にはもう一つ、**高速再転送**と呼ばれる再送制御の仕組みが規定されている。これは、連続転送している状況下で特定の TCP セグメントだけが欠落した場合、受信ホストから送信ホストに対し、当該 TCP セグメントを再送するよう通知する仕組みである。その際、3 回以上連続して ACK を再送する（以下、便宜的に「重複 ACK」と称する）。ホスト A は、①、②及び③を送信する。しかし、②が途中で喪失している。ホスト B は、③を受信することにより、②が欠落したと判断する。そこで、①、③のセグメントをバッファに保存しておき、②のセグメントの再送をホスト A に要求する。これが④である。ホスト B は①まで正常に受信できているので、④は①の確認応答である。つまり、返信する確認応答番号（次に受信すべきシーケンス番号）は、②の先頭を示している。

その後、ホスト B は、ホスト A から⑤、⑥を受け取るたびに、②が欠落していることを伝えるために⑦を送信する。ホスト A は、3 個以上連続した④（重複 ACK）を受信する。④に格納された確認応答番号から、②のセグメントだけを再送する必要があると判断する。

ホスト A は、⑧（②の再送）を送信する。その後、ホスト B は⑨（⑦の確認応答）を送信する。⑥まで正常に受信できているので、このとき返信する確認応答番号（次に受信すべきシーケンス番号）は、⑥の後続（⑩の先頭）を示している。ホスト A は、⑪（⑩の後続）を送信する。その後、ホスト B は⑫（⑩の確認応答）を送信する。なお、連続転送を行っているので、ホスト A は⑧を受信する前に⑩を送信してもよい。

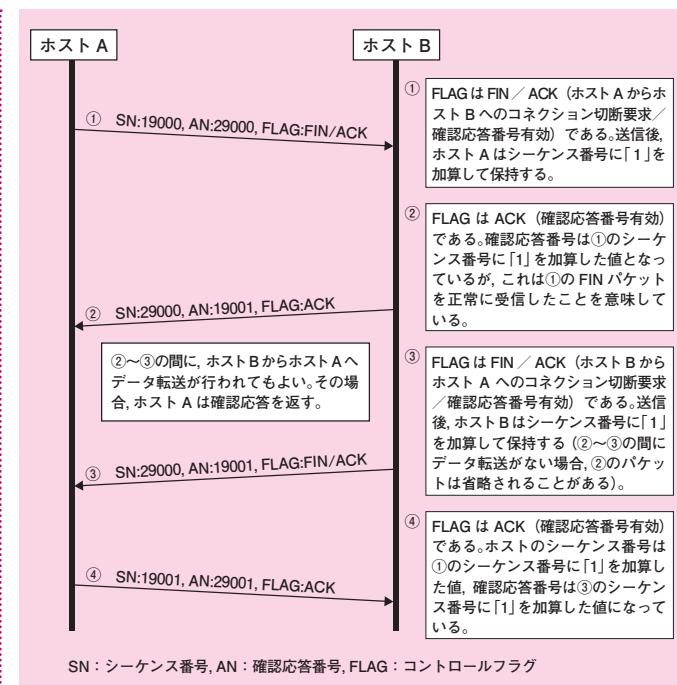


図：高速再転送

### 3. コネクション切断フェーズ

**コネクション切断フェーズ**は、四つのパケット（FIN／ACK, ACK, FIN／ACK, ACK）からなる（ただし、タイムアウトの場合など、例外もある）。

次の図は、コネクション切断フェーズにおける、コントロールフラグ、シーケンス番号、及び確認応答番号の推移を示している。



図：コネクション切断フェーズ

### ● フロー制御と輻輳制御

これまで解説したとおり、コネクション確立フェーズ中に、ホストは互いにウインドウサイズの最大値を通知し合う。また、通信フェーズ中、スライディングウインドウ機構により通知された受信可能なウインドウサイズは動的に変化する。これをフロー制御という。

さらに、輻輳を回避するため、ホストは「**輻輳ウインドウ**」と呼ばれる変数を管理している。最小値は  $1 \times \text{MSS}$ 、最大値はウインドウサイズ最大値である。ホストは、輻輳を回避するように輻輳ウインドウの値を調整する。これを**輻輳制御**といふ。

実際に送信されるバイト数は、輻輳ウインドウの値と、通知された受信可能ウインドウサイズの値を比較し、小さい方が採用される。



TCPのフロー制御について、平成22年午後I問2で出題された

### ・スロースタートアルゴリズム

ホスト同士が同じ LAN 上に存在しておらず、途中経路にルータや低速な回線が存在しているとき、ウィンドウサイズの最大値で通信するならば、通信能力の限界を超えて輻輳が発生する可能性がある。そこで、輻輳を生じさせずに十分な伝送効率が得られる適切なウィンドウサイズを探し出すため、**スロースタートアルゴリズム**が用いられる。

通信フェーズ開始時、輻輳ウィンドウを  $1 \times \text{MSS}$  から開始する。その後、確認応答パケットを受信した個数だけ、輻輳ウィンドウを  $\text{MSS}$  ずつ増やしていく。

具体的に数値を使って、この仕組みを説明する。最初は、輻輳ウィンドウ : 1, 送信パケット : 1 個である。確認応答パケット : 1 個を受信すると、輻輳ウィンドウ : 2 に更新される（輻輳ウィンドウ :  $1 + \text{確認応答パケット} : 1$ ）。次に、輻輳ウィンドウ : 2, 送信パケット : 2 個である。確認応答パケット : 2 個を受信すると、輻輳ウィンドウ : 4 に更新される（輻輳ウィンドウ :  $2 + \text{確認応答パケット} : 2$ ）。以降、輻輳ウィンドウは、8, 16, 32 という具合に指數関数的に増加する（ただし、送信パケット数 = 確認応答パケット数の場合）。

### ・輻輳回避アルゴリズム

重複 ACK (3 回以上連続した同じ ACK) を受け取ると、輻輳が発生したと判断し、ウィンドウサイズをいったん半分に縮小してから、輻輳ウィンドウを徐々に（直線的に）増やしていく。これを「**輻輳回避アルゴリズム**」という。この仕組みにより、輻輳がすぐに再発しないようにしている。



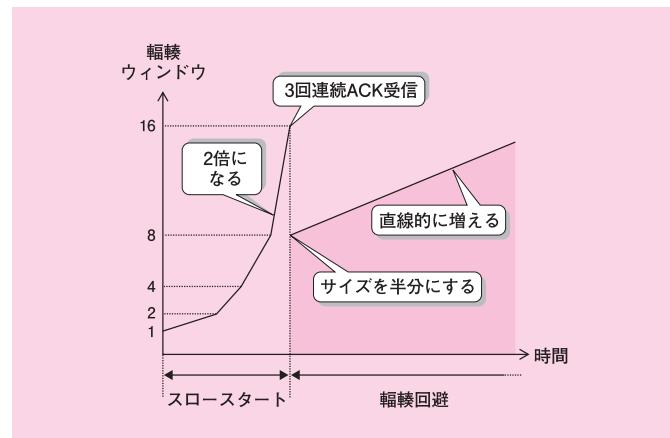
MSS の大きさに応じ、スロースタート時の輻輳ウィンドウのサイズを  $1\text{MSS}$  よりも大きな値から開始できる。例えば、イーサネットの場合は MSS は 1460 バイトとなるが、このときは  $3\text{MSS}$  (4380 バイト) から開始してよい

1

2

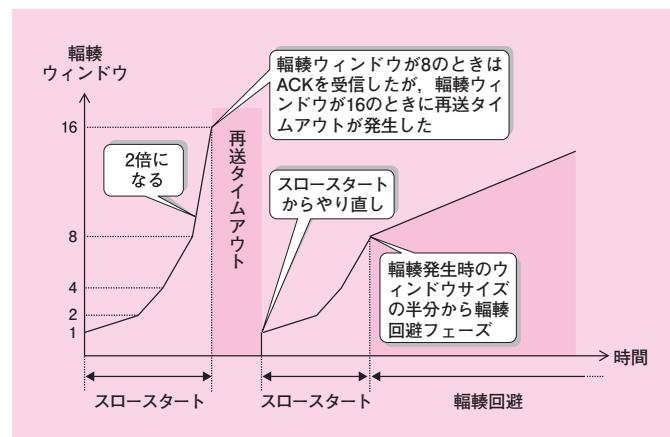
3

4



図：スロースタートと輻輳回避における輻輳ウィンドウの変化

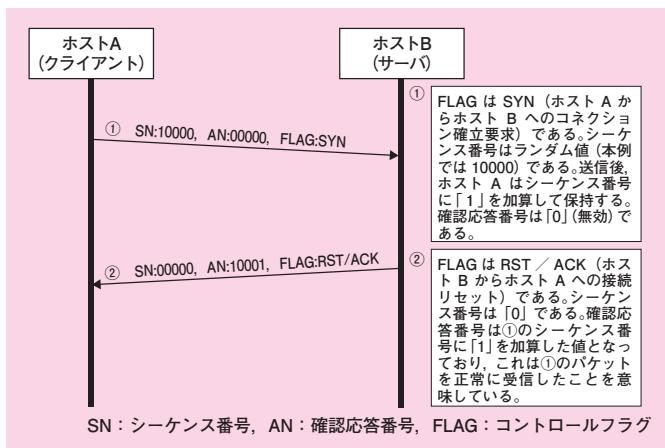
一方、再送タイムアウトが発生した場合は、スロースタートからやり直し、再送タイムアウトが発生した時点のウィンドウサイズの半分に到達してからは、輻輳回避フェーズに入る。



図：再送タイムアウト発生時の輻輳ウィンドウの変化

## ● TCP 接続リセット

コネクション確立フェーズ又は通信フェーズで、受信したTCPセグメントのヘッダに解決不能のパラメタが存在している場合、TCP接続がリセットされる。その代表例は、コネクション確立フェーズにおいて、最初の確立要求パケットの宛先ポート番号が、宛先ホスト上で実行されているアプリケーションで対応していない場合である。このとき、RST／ACKフラグをセットしたパケットが返信される。



図：コネクション確立フェーズの接続リセットビット

## ● TCP 通信のスループット

TCP通信の実効転送速度は、次の式で求まる。ここで、ラウンドトリップ時間とは、パケットの往復時間のことである。

$$\text{実効転送速度} = \frac{\text{ウインドウサイズ}}{\text{ラウンドトリップ時間}}$$

ホストAがホストBに向けてパケットを連続転送している様子を例に、この点を解説する。



UDPヘッダ中の宛先ポート番号が宛先ホストでサポートされていない場合は、当該ホストからICMPメッセージの「宛先到達不可 — ポート到達不可」が送信元に返信される

1

2

3

4



IDSの中には、不正な通信を検出したとき、これを遮断するため送信元と宛先の双方にRSTフラグをオンにしたパケットを送付する機能をもつものがある



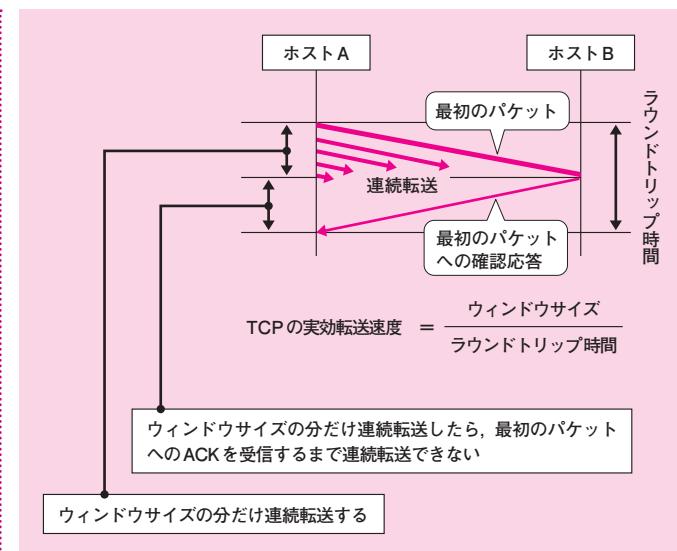
試験に出る

RSTフラグをオンにしたパケットにより通信を迅速に遮断できることについて、平成27年午後I問2で出題された



試験に出る

TCP通信のスループットについて、平成22年午後I問1で出題された。WAN高速化装置の導入によるスループット改善について、平成26年午後I問1、平成20年午後I問3で出題された



図：TCP の実効転送速度

ホスト A は、送信したいデータ量がウィンドウサイズ以下であれば、確認応答を待たずにデータを連続転送できる。しかし、送信したいデータ量がウィンドウサイズを超えている場合、ウィンドウサイズの分まで連続転送した後は、ホスト B から最初のパケットへの確認応答を受信するまで、後続するパケットを転送できない。この例から分かるように、ラウンドトリップ時間（パケットが往復する時間）に送信できるデータ量の上限値は、ウィンドウサイズとなる。したがって、TCP 通信のホスト間の実効転送速度は上の式で求まることになる。

通信フェーズの開始直後は、スロースタートアルゴリズムが作用し、ウィンドウサイズが小さい。例えば、Web 通信のように数往復でファイルの取得を終えてしまう通信の場合、ラウンドトリップが大きいと通信回線の帯域を十分に使い切れないことがある。現在、この問題を改良するための方式が幾つか提唱されており、一部ではあるが、対応している OS もある。

# 3.4 • ARP

ARPについては、基本的な ARP 要求／応答の動作だけでなく、Gratuitous ARP, Proxy ARP についても学習しておく必要がある。

## 3.4.1 ARP の仕組み

**ARP** (Address Resolution Protocol) は、IP アドレスから MAC アドレスを得るプロトコルである。宛先 IP アドレスしか分からぬ場合、ARP を用いることにより、宛先ホストが自らの MAC アドレスを通知する仕組みとなっている。宛先 MAC アドレスを取得した後、MAC フレームを生成して宛先ホストに IP パケットを送信する。

ARP 要求は、ヘッダに IP アドレスを格納し、ブロードキャストパケットを用いて全ホストに問い合わせる。該当する IP アドレスをもつホストは、自分の MAC アドレスをヘッダに格納し、ARP 応答を返す。ARP 応答にはユニキャストパケットが用いられる。

獲得した MAC アドレスは、**ARP テーブル**に一定期間キャッシュされる。これを**ARP キャッシュ**という。キャッシュされている間は、同じ ARP 要求を出さなくとも MAC フレームを送信することができる。

ARP のフレームフォーマットを次に示す。

(14)	(28)		(18)	(4)
MACヘッダ	ARPフレーム			パディング
			FCS	
(2)	(2)	(1)	(1)	(2)
H/W種別 [イーサネット]	プロトコル 種別[IP]	H/W アドレス 長[=6]	プロトコル アドレス 長[=4]	コード 要求: 1 応答: 2
				送信元H/W アドレス [イーサネット]
				送信元 プロトコル アドレス [IP]
				目標H/W アドレス [イーサネット]
				目標 プロトコル アドレス [IP]

H/W…「ハードウェア」の略

注:( )内の数字はオクテット長を表す。

図: ARP のフレームフォーマット



試験に出る

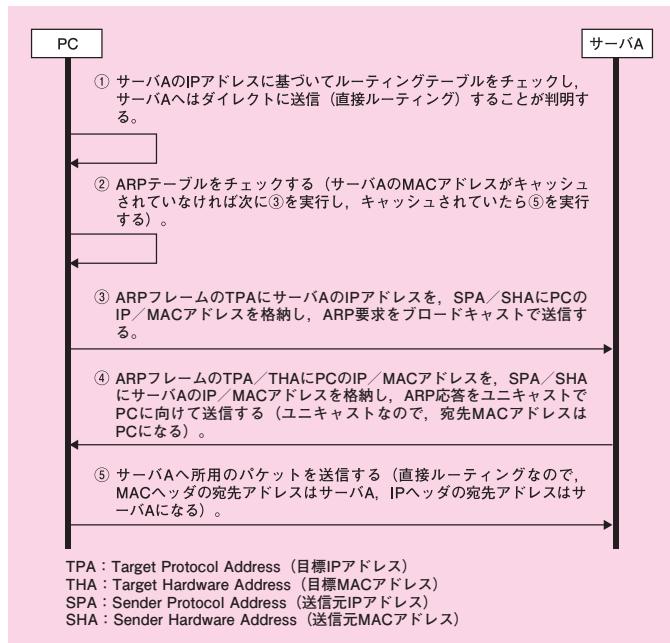
ARPについて、平成 25 年午後Ⅱ問 1、平成 21 年午前Ⅱ問 7、平成 16 年午前問 22 で出題された。また、MAC アドレスから IP アドレスを取得するプロトコルである RARP (Reverse ARP) について、平成 25 年午前Ⅱ問 12 (平成 21 年午前Ⅱ問 11 と同じ問題)、平成 19 年午前問 29 で出題された



RFC826 (STD37)

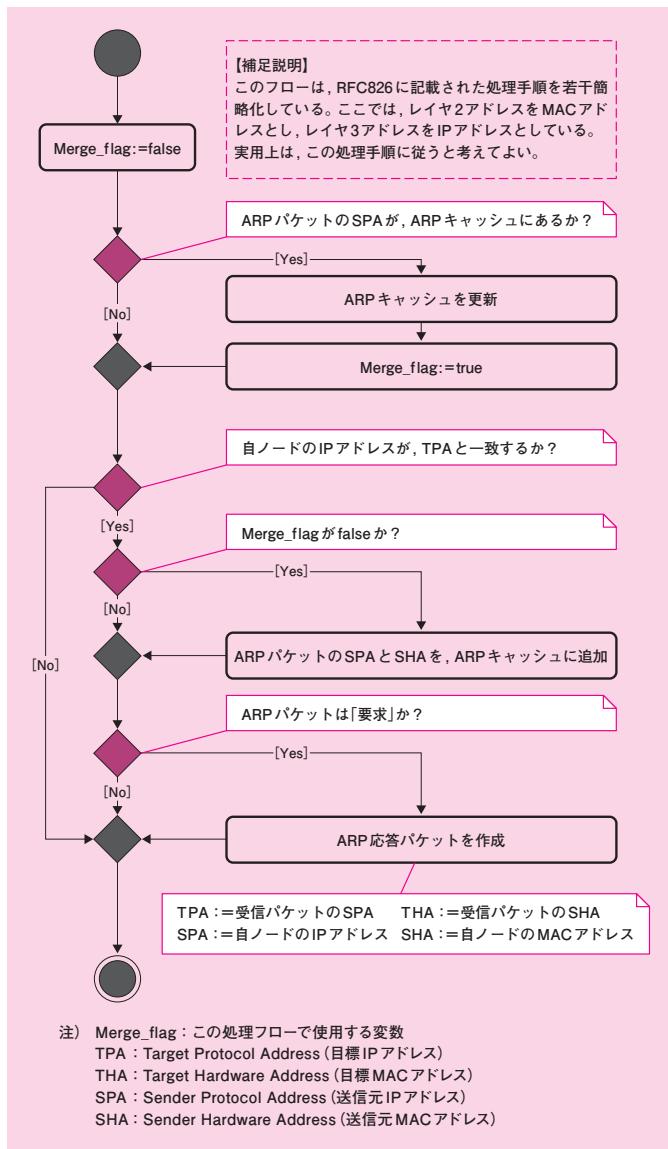
MAC ヘッダのタイプ領域には ARP フレームを表す値(0x0806)が格納される。ARP フレームは 28 バイトであるため、最小データ長の 46 バイトになるよう 18 バイト分がパディングされる。

図は、PC から IP パケットを転送する際に ARP がどのように用いられているかを示している。まず、サーバ A が PC と同じサブネット上にあり、直接ルーティングにより所用のパケットを送信する例を示す。



図：直接ルーティングにおける ARP フレーム及び IP パケットの送信

受信した ARP パケットを処理するフローを次の図に示す。



図：ARP の処理フロー

## 3.4.2 特別な用途の ARP

特別な用途で用いられる ARPとしてGratuitous ARPとProxy ARPがある。



試験に出る

Gratuitous ARPによるARPキャッシュ更新について、平成26年午後I問2、平成25年午後II問1、平成20年午後II問1で出題された。Gratuitous ARPの説明について、平成28年午前II問6で出題された。



図「ARP処理フロー」を見ると、既にARPキャッシュを保持しているノードは、受信したARPパケットのSPAがARPキャッシュのIPアドレスと一致していたとき、ARPキャッシュを上書きすることが分かる。

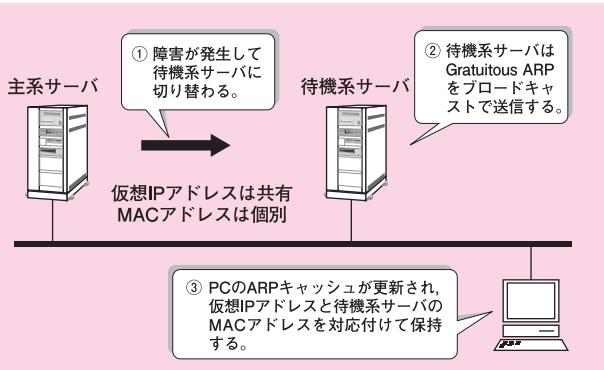
Gratuitous ARPは、この仕様を利用して、同一ブロードキャストドメイン内のARPキャッシュを更新している

### ● Gratuitous ARP

Gratuitous ARPは、**重複IPアドレス**の検知などに利用されるARPである。ホストは自IPアドレスを目標プロトコルアドレスに格納してARP要求を送信する。もし、このARP要求に対してもかのホストからARP応答があれば、そのホストは自分と同じIPアドレスをもっている（つまり、IPアドレスが重複している）と判断する。

Microsoft社のWindows OSでは、このGratuitous ARPを用いて、電源投入後の重複IPアドレスのチェックを行っている。これは、誤った設定などによってIPアドレスが重複してしまう可能性があるためである。

ほかにも、図のようにサーバが二重化されているシステムでもGratuitous ARPは活用されている。この構成では、主系サーバと待機系サーバは仮想IPアドレスを共有しているが、MACアドレスは個別に保持しているものとする。



図：Gratuitous ARPを使用したフェールオーバーの仕組み

主系サーバがダウンし、待機系サーバに切り替わると、仮想IPアドレスも待機系サーバに引き継がれる。このとき、待機系サーバはGratuitous ARPをブロードキャストで送信する。Gratuitous ARPを受信した全てのホストは、ARPキャッシュを更新する仕組みとなっている。これにより、それまで仮想IPアドレスと主系サーバのMACアドレスを対応付けていたホストは、今後は待機系サーバのMACアドレスと対応付けることになる。

なお、VRRPのような仮想IPアドレスと仮想MACアドレスを共有する方式で二重化を行っている場合は、Gratuitous ARPでARPキャッシュを更新する仕組みを導入する必要はない。

## ● RARP

RARP(Reverse Address Resolution Protocol)とは、外部記憶装置を持たないノードが、RARPサーバから自装置のIPアドレスを取得するために用いるデータリンク層のプロトコルである。

電源オン時に自ノードのネットワークインターフェースから(ROMに書かれた)MACアドレスを取得し、RARPサーバに対し、そのMACアドレスに対応するIPアドレスを応答するように要求する。クライアントはRARPサーバのMACアドレスを保持していないため、RARP要求にはブロードキャストフレームが利用される。そのフレームの中には自装置のMACアドレスが格納されている。RARPサーバはこのフレームを受け取ると、ユニキャストフレームを用いてクライアントのIPアドレスを応答する。

前記が従来のRARPフレームの目的であったが、今日ではRARPを必要とするノードを使用しないので、RARPサーバを設置することはない。この状況を踏まえ、本来とは全く異なる用途で、RARPが使用される。

主系サーバから待機系サーバへ切り替わると、待機系サーバが主系の仮想IPアドレスと仮想MACアドレスを引き継ぐ方式を探ることがある。この切替え時に、主系サーバと待機系サーバが収容されたブロードキャストドメイン内で、スイッチのMACアドレステーブルを更新する必要がある。

なぜなら、主系サーバから待機系サーバに切り替わったとき、仮想MACアドレスとポート番号との対応付けが変化するスイッ



### 試験に出る

RARPフレームとは明記されていないが、主系サーバから待機系サーバに切り替わったときMACアドレステーブルを更新することについて、平成26年午後II問2で出題された。MACアドレステーブルの更新は、仮想マシンのライブマイグレーションでも必要となる。仮想マシンが別の物理サーバに移動した結果、仮想マシンのMACアドレスとポート番号の対応付けが変化するスイッチが存在するからだ。

ライブマイグレーション時にMACアドレステーブルを更新するため、RARPフレームが使用されることについて、平成20年午後II問1で出題された。

チが存在するからである。

この MAC アドレステーブルの更新のために、切替え直後にサーバから RARP 要求が用いられることがある。

RARP 要求フレームの宛先はブロードキャストアドレスであり、送信元アドレスは送信元ホストの MAC アドレスである。今述べている切替え動作においては、仮想 MAC アドレスが送信元となる。

したがって、RARP 要求フレームを送信すれば、ブロードキャストドメイン内の全てのスイッチに到達でき、切替え先のサーバが存在するポートの位置に応じて、MAC アドレステーブルを適切に更新できる。

実は、MAC アドレステーブルの更新には、必ずしも RARP を用いる必要はない。宛先がブロードキャストアドレスであり、送信元が仮想 MAC アドレスであれば、どのフレームでもよい。

RARP が用いられる理由は、MAC アドレステーブルを更新する以外に副作用がないからである。今日、RARP サーバが設置されることはないので、RARP は無害なフレームである。RARP サーバ以外のホストは、RARP パケットを受信すると、ただ単にこれを破棄するだけである。

## ● Proxy ARP



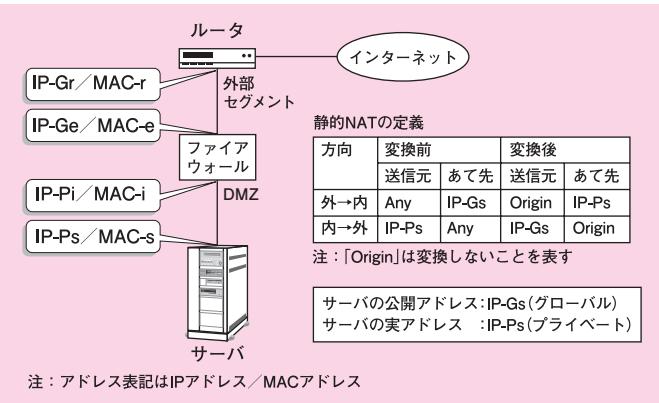
RFC1027: Proxy ARP

**Proxy ARP** は、あらかじめ登録された IP アドレスに対する ARP 要求を受けると、あたかも自ホストがその IP アドレスをもっているかのようにふるまい、自ホストの MAC アドレスを回答とする ARP 応答を返信する機能である。ルータやファイアウォールがこの機能を装備している。

例えば、次の図のネットワークでは、非武装セグメント (DMZ) にサーバが収容されており、プライベートアドレス (IP-Ps) を割り当てているものとする。外部に公開するサーバのアドレスはグローバルアドレス (IP-Gs) であるため、ファイアウォールの Proxy ARP 機能を活用する。



Proxy ARP 機能について、平成 25 年午後Ⅱ問 1、平成 19 年午後Ⅱ 問 2 で出題された



図：Proxy ARP が使用されるネットワークの構成例

インターネットからサーバ (IP-Gs) にアクセスするパケットは、ルータを経由する。ルータは、IP-Gs を目標プロトコルアドレスとする ARP 要求を送信する。ファイアウォールは、Proxy ARP 機能により外側セグメントの MAC アドレスである MAC-e を ARP 応答として返信する。

この結果、ルータからファイアウォールに向けて、次の図のとおり MAC フレームが送信される。

あて先MACアドレス MAC-e	送信元MACアドレス MAC-r	タイプ	IP-Gs向けの IPパケット	FCS
---------------------	---------------------	-----	--------------------	-----

図：ファイアウォールへ送信される MAC フレーム

ファイアウォールがこの MAC フレームを受信すると、静的 NAT の定義に従い、宛先 IP アドレスに格納されている公開アドレス IP-Gs を実アドレス IP-Ps に変換する。

その後、ファイアウォールは、DMZ に向けて、IP-Ps を目標プロトコルアドレスとする ARP 要求を送信する。サーバは、通常の ARP 機能により MAC-s を ARP 応答として返信する。

この結果、ファイアウォールからサーバに向けて、次の図のとおり MAC フレームを送信する。

あて先MACアドレス MAC-s	送信元MACアドレス MAC-i	タイプ	IP-Ps向けの IPパケット	FCS
---------------------	---------------------	-----	--------------------	-----

図：ファイアウォールから送信される MAC フレーム

## 3.5 • ICMP

ICMP は、ping などで馴染み深いプロトコルだが、ほかにも様々な機能や役割を担っている。エコー要求／応答、宛先到達不能、リダイレクト、時間超過など、主要な ICMP メッセージの仕組みについて学習しておく必要がある。

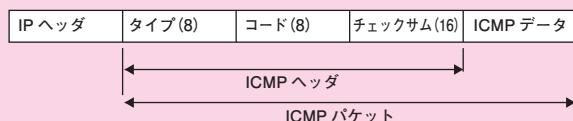
### 3.5.1 ICMP のパケットフォーマット



RFC792 (STD5)

**ICMP** (Internet Control Message Protocol) は、IP から見ると上位プロトコルとなるが、機能的には OSI 基本参照モデルの第3層（ネットワーク層）に類別される。

ICMP のパケットフォーマットを次に示す。



注：( )内の数字はビット数。

図：ICMP のパケットフォーマット

なお、ICMP データのフォーマットは、次に説明する ICMP メッセージごとに規定されている。

### 3.5.2 ICMP メッセージ



ICMP の役割について、平成 24 年午前 II 問 10、平成 19 年午前 問 24 で出題された

ICMP は、IP パケットの転送でエラーが発生した場合、それを送信元に通知する機能や、接続性を確認するエコー要求／応答メッセージを転送する機能などをもつ。代表的な ICMP メッセージの種類を次に示す。

表：ICMP メッセージ

タイプ	コード	内 容	照 会	エラー
0	0	エコー応答	○	
3		宛先到達不能（エラーメッセージ）		
	0	ネットワーク到達不能		○
	1	ホスト到達不能		○
	2	プロトコル到達不能		○
	3	ポート到達不能		○
	4	フラグメンテーションが必要だが、DF ビット（フラグメント化禁止ビット）が設定されている		○
	5	送信元ルート失敗		○
	6	宛先ネットワーク不明		○
	7	宛先ホスト不明		○
		送信元ホスト隔離		○
		宛先ネットワークとの通信が管理上禁止されている		○
		宛先ホストとの通信が管理上禁止されている		○
		ToS のためネットワーク到達不能		○
		ToS のためホスト到達不能		○
		ファイアウォールが原因で通信が管理上禁止されている		○
	6	宛先ネットワーク到達不能		○
	7	宛先ホスト到達不能		○
4	0	送信元抑制		○
5		リダイレクト		○
	0	ネットワークへのリダイレクト		○
	1	ホストへのリダイレクト		○
	2	特定の ToS を要求するネットワークへのリダイレクト		○
	3	特定の ToS を要求するホストへのリダイレクト		○
8	0	エコー要求	○	
9	0	ルータ広告	○	
10	0	ルータ要請	○	
11	0	時間超過		○
12	0	パラメタ異常		○
13	0	タイムスタンプ要求	○	
14	0	タイムスタンプ応答	○	
15	0	情報要求	○	
16	0	情報応答	○	
17	0	アドレスマスクの要求	○	
18	0	アドレスマスクの応答	○	

ICMP メッセージは、照会メッセージとエラーメッセージの二つに分類できる。ICMP エラーメッセージを格納した IP データグラムの転送に失敗したとき、そのための ICMP エラーメッセージは例外的に通知されない。よって、エラー通知の失敗が新たなエラー通知を誘発するという悪循環が避けられることになる。

以下、主要な ICMP メッセージについて解説する。

### ● エコー要求／応答

**エコー要求／応答**は最もよく使われる ICMP 機能であり、ネットワークのループバックテストに使用されている。エコー要求メッセージは、**ping** コマンドを実行することにより送信される。宛先 IP アドレスはコマンドの引数で渡される。エコー要求を受け取ったホストは、その要求元にエコー応答メッセージを返信する。

### ● 宛先到達不能

経路途中のルータで転送エラーが発生したときや、宛先ホストで受信エラーが発生したときは、エラーとなった IP パケットを破棄した上で、その送信元ホストに向けて**宛先到達不能メッセージ**を送信する。宛先到達不能メッセージでは、ICMP ヘッダのコード領域に値をセットする。全部で 14 種類あるメッセージのうち、代表的なものを次に示す。

表：主要な宛先到達不能メッセージ

コード（値）	説明
ホスト到達不能 (0x1)	宛先へのルートがルーティングテーブル内に見つからない
プロトコル到達不能 (0x2)	プロトコル（IP ヘッダのプロトコル番号領域で指定）が受信ホストで使用されていない
ポート到達不能 (0x3)	UDP ヘッダ内の宛先ポートが受信ホストで使用されていない（なお、TCP ヘッダ内の宛先ポートが見つからない場合は接続リセットを返信する）
フラグメンテーションが必要だが、DF ビットが設定されている (0x4)	途中経路のルータがフラグメント化を試みたが、DF ビットが設定されているために失敗した（データリンクの MTU の値が返答される）



ICMP リダイレクトについて、平成 29 年午前Ⅱ問 7、平成 27 年午前Ⅱ問 7 で出題された

### ● リダイレクト

同一サブネットに 2 台以上のルータが存在しており、送信元ホストが最適ではないルータを経由して IP パケットを送信したとする。このとき、そのルータはパケットを適切なルータへ転送する。同時に、送信元ホストに**リダイレクトメッセージ**を送信し、同一サブネット上には自分より適切なルータが存在することを通知する。これを受け、送信元ホストはルーティングテーブルを変更する。それ以降は、最適なルータを経由して IP パケットを送信するようになる。なお、途中経路のルータが最適ではないルートを使って IP パケットを転送しても、リダイレクトメッセージは発行されない。

### ● 時間超過

ルータは IP パケットを転送する際、IP ヘッダ内の **TTL** 領域を読み取り、値を一つ減らして格納し直す(このとき、ヘッダ内のチェックサム領域も更新される)。TTL 領域の値が「0」になったとき、ルータは IP パケットを破棄して、送信元ホストに時間超過メッセージを送信する。TTL 領域の値が「0」になる典型的なケースは、ルーティングループが発生して IP パケットが複数のルータを循環して転送されている状態である。

## 3.5.3 ICMP の利用

ICMP の利用例は次のとおりである。

### ● ping コマンド

IP ホストの接続性を検査する目的で使用される。利用者は、検査対象のホスト（以下、「目標ホスト」）を指定して **ping コマンド** を投入する。OS はエコー要求（タイプ：8）を送信し、目標ホストから規定時間内にエコー応答（タイプ：0）を受信できれば、接続性が確保できていると判断する。一方、IP ホストや途中経路がダウンしているときはエコー応答が返信されないため、タイムオーバによって、障害を検知する。なお、ダウンではなくエラーが発生した場合、宛先到達不能（タイプ：3）が返信されることがある。  
ping コマンドは、応答時間も計測しているので、合否判定結果も併せて出力する。

### ● traceroute コマンド

OS が提供するコマンドで、IP ホストに到達する経路上の IP ホスト（ルータ）を調査する目的で使用される。これは、ルータが IP パケットをルーティングする際、IP ヘッダの TTL 値が「0」になつたら、送信元ホストに時間超過メッセージ（タイプ：11）を通知する仕組みを応用したものである。利用者は、検査対象のホスト（目標ホスト）を指定して **traceroute コマンド** を投入する。



試験に出る

ping が ICMP を使用していることについて、平成 29 年午後 I 問 3、平成 20 年午前 問 31、平成 18 年午前 問 28、平成 17 年午前 問 49 で出題された



参考

traceroute は、目標ホストに向けて送信する IP パケットとして、Linux では UDP パケットを、Windows ではエコー要求パケットを用いる。また、IP ヘッダ中の TTL 領域の最大値は「255」だが、調査する TTL 値の上限をオプションで指定することができる

OSは、目標ホストを宛先とするIPパケットを送信する際、最初は「TTL = 1」にセットする。すると、最初のパケットは1個目のルータで「TTL = 0」となるので、そこからICMPの時間超過メッセージを受け取る。これにより、このルータのIPアドレスを取得することができる。

次は「TTL = 2」、その次は「TTL = 3」という具合に、一つずつTTL値を増やしながら、目標ホストに向けてIPパケットを送信する。すると、2個目、3個目という具合に経路上のルータから時間超過メッセージを受信し、これらのIPアドレスを順次取得することができる。なお、ルータが時間超過メッセージに対応していない場合は、タイムオーバーとなる。そのとき、IPアドレスは不明であるが、「ルータをホップしている」という事実は判明する。

最終的に目標ホストから同メッセージを受け取ることで、コマンド実行が完遂される。この結果、目標ホストに至るルータのIPアドレスのリスト、すなわち通信経路を取得することができ、コマンドはこのリストを出力する。

### ● 経路 MTU

**経路 MTU**とは、宛先ホストまでパケットを送信する際、フラグメント化が必要とならない最大MTUである(つまり、経路上のデータリンクの最小MTUである)。送信元ホストで事前に経路MTUのサイズに分割して送信すれば、途中のルータでフラグメンテーションを発生させないので、多くのOSが実装している。経路MTUの検出では、IPヘッダのDFビット(フラグメント化禁止ビット)を設定して、パケットを送る。途中経路のデータリンクのMTUを超えていた場合、そのルータからICMP到達メッセージのコード「0x4」が返答される。これによりMTUを取得できるので、この値を経路MTUに採用し、次からはこのサイズに分割してパケットを送信する。これを繰り返し、ICMP到達メッセージが返答されなくなった時点で、真の経路MTUの値が得られたことになる。なお、経路MTUの値は、約10分間キャッシュすることになっている。よって、10分経過した後は検出を再開する。

# 3.6 • DHCP

DHCP は単純なプロトコルだが、実際の運用において注意しなければならないことも多く、運用上の出題が多い。初期リースの取得、リースの更新と解放、リレーなどの動作の仕組みについて学習しておく必要がある。

## 3.6.1 DHCP の機能

**DHCP** (Dynamic Host Configuration Protocol) は、クライアントがネットワーク設定をサーバから自動的に読み込むためのプロトコルである BOOTP を拡張し、アドレス情報などの設定情報の動的な割当て機能を追加したプロトコルである。

DHCP を使用すると、クライアント端末の設定情報を DHCP サーバが自動的に割り当てるため、管理者の運用負担が軽減される。主な設定情報として、クライアントの IP アドレスとサブネットマスク、デフォルトゲートウェイの IP アドレス、ローカル DNS サーバの IP アドレスなどがある。なお、DHCP から割り当てられた設定情報には有効期限がある。これを**リース期間**という。

## 3.6.2 DHCP による設定情報の割当て順序

DHCP は UDP の上位アプリケーションプロトコルであり、DHCP サーバはポート番号 67 番を、DHCP クライアントはポート番号 68 番を使用する。

起動時、DHCP クライアントの IP アドレス、サブネットマスクは「0.0.0.0」が設定されている。DHCP サーバとのやり取りでは、**制限ブロードキャストアドレス** (255.255.255.255) が用いられる。

なお、同一サブネットに複数の DHCP サーバを設置する場合は、それぞれのサーバがプールしている IP アドレスの範囲が重複しないように設定しておく。

以下、設定情報の割当て順序について解説する。



## 試験に出る

DHCP の機能を使った端末管理と DHCP スヌーピング機能について、平成 25 年午後 I 問 2 で出題された。DHCP がブロードキャストを用いることについて、平成 16 年午後 I 問 1 で出題された。



下記のメッセージは、通常、ブロードキャストされる。

DHCPDISCOVER

DHCPOFFER

ただし、DHCP の標準を定めた RFC2131 によれば、DHCP サーバの IP アドレスが分かれている場合はユニキャストで送信してもよいことになっている〔4.4.4 Use of broadcast and unicast〕を参照)。

DHCPOFFER, DHCPACK は、ブロードキャスト又はユニキャストで送信される。どちらで送信するかは、DHCPDISCOVER, DHCPOFFER パケットの中で指定する。

DHCPOFFER, DHCPACK のブロードキャスト送信が指定可能になっている理由は、クライアント端末の中には、IP アドレス等のネットワーク情報が設定されるまで、ユニキャストパケットを処理できないものがあるからである

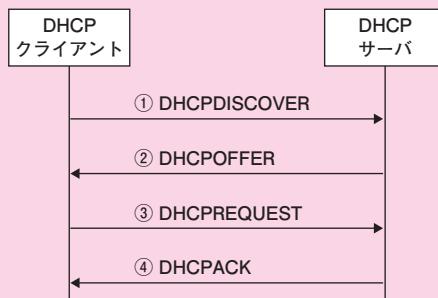


## 試験に出る

リースの更新について、平成 17 年午後 I 問 2 で出題された

## ● 初期リースの取得

DHCP 設定情報の割当て順序を次に示す。なお、ここでは説明を簡単にするため、構成情報として「IP アドレス」についてのみ言及する。



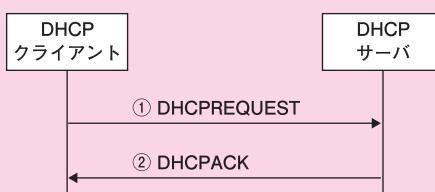
- ① クライアントは、サーバを見つけるため、DHCPDISCOVERを送信する。
- ② サーバは、クライアントにIPアドレスを提供するため、DHCPOFFERを送信する。サーバが複数ある場合、クライアントは複数のDHCPOFFERを受信する。
- ③ クライアントは、提供されたIPアドレスの割当てを要求するため、DHCPREQUESTを送信する。複数のサーバからDHCPOFFERを受信した場合、その中から一つを選び、提供されたIPアドレスやサーバID (DHCPOFFERパケットに格納) をセットして要求する。
- ④ サーバは、確認応答としてDHCPACKを送信する。その際、提供したIPアドレスが割当て可能かどうかをチェックし、この時点でIPアドレスが割当て不能だった場合、DHCPNACKを送信する。サーバが複数ある場合、DHCPACKを送信するのは、DHCPREQUESTで指定を受けたサーバだけである。

図：DHCP の IP アドレス割当ての順序

## ● リースの更新と解放

クライアントが起動されたとき、まだ IP アドレスのリース期間内であれば、同じ IP アドレスの取得を要求する。これを **リースの更新** という。リース期限の残り半分を過ぎていた場合は、自動的にリースの更新（延長）を要求する。

このとき、DHCPREQUEST パケットが DHCP クライアントから送信され、DHCP サーバから DHCPACK パケットが返信される。クライアントの実行中もリース更新は定期的に行われる。なお、サーバの IP アドレスを取得済みなので、クライアント実行中はユニキャストでやり取りする。



- ① クライアントは、DHCPREQUESTをサーバに送信してリースの更新を要求する。  
 ② サーバは、DHCPACKを返信する。

図：DHCP のリースの更新

クライアントがIPアドレスのリース期間前にIPアドレスの使用を終了するときは、サーバにDHCPRELEASEパケットをユニキャストで送信する。このパケットを受け取ったサーバはIPアドレスを解放してプールに戻す。なお、サーバはこのパケットに対して、確認応答を返さない。

### ● IP アドレス重複の検出

DHCP クライアントは、DHCP サーバから設定情報を受け取つた後、Gratuitous ARP を送信し、IP アドレスの重複チェックを行う。これは、手動による設定などで、IP アドレスが同一サブネット内に重複してしまう可能性があるためである。

### ● DHCP リレー

DHCP クライアントが DHCP サーバから TCP/IP 設定情報を取得するときには、ブロードキャストパケットを用いたやり取りが行われる。DHCP クライアントと DHCP サーバがルータを通して接続されている場合、両者は異なるブロードキャストドメインに収容されているため、ブロードキャストパケットが到達しない。そこで、ルータ上で **DHCP リレーエージェント** 機能を動作させる必要がある。

DHCP リレーエージェントを使用する際は、DHCP サーバの IP アドレスをあらかじめ登録しておく。DHCP リレーエージェントは DHCP クライアントが送信したブロードキャストパケットを受信すると、そこに格納されている DHCP メッセージを取り



試験に出る

DHCP リレーについて、平成 25 年午後 I 問 2、平成 20 年午後 II 問 1、平成 18 年午前問 44、平成 16 年午後 I 問 1 で出題された。リレーエージェント情報オプション（オプションコード: 82）について、平成 19 年午後 I 問 1 で出題された

出し、ユニキャストパケットを用いて DHCP サーバに転送する。DHCP サーバはそれを受信すると、ユニキャストパケットを用いて DHCP リレーエージェントに応答する。DHCP リレーエージェントはそれを受信すると、そこに格納されている DHCP メッセージを取り出し、ブロードキャストパケットを用いて DHCP クライアントに転送する。このように DHCP リレーエージェントを中継して、DHCP クライアントと DHCP サーバ間でやり取りを行うことができる。

サーバは、DHCP パケット内の情報から、クライアントからの要求がリレーエージェントを経由したものであることを識別して、適切な IP アドレスを提供する。

リレーエージェントが RFC3046 で規定された DHCP リレー情報オプションをサポートしているとき、DHCP クライアントから受け取った DHCP パケットにリレーエージェント固有の情報を附加して、DHCP サーバに転送することができる。その情報は、**リレーエージェント情報オプション**（オプションコード：82）として DHCP オプションの最後に追加される仕組みになっている。付加される情報は二つあり、一つはリモート ID サブオプションと呼ばれ、リレーエージェント（L3SW）の MAC アドレスが格納される。もう一つは回線 ID サブオプションと呼ばれ、DHCP クライアントからのパケットを受信したポート番号など（ほかには VLAN 番号なども付加可能）である。

# 3.7 • NAT

NATは利用頻度が高いため、その仕様について詳細に把握している学習者も多いだろう。ここでは、基本的な項目について網羅的に解説するので、理解が不十分な部分がないかを確認してほしい。

## 3.7.1 NAT／NAPT

今日ではNAPTが一般的に用いられていることから、広義のNATにNAPTを含めて説明している文献が増えつつある。しかし、狭義のNATとNAPTは異なっている。狭義のNATは、IPアドレスの変換だけを行い、NAPTはIPアドレスとポート番号の変換を行う。

なお、NAPTはRFC3022などで規定された正式名称であるが、一般にはIPマスカレードとも呼ばれている。

NATとNAPTの違いを次に示す。

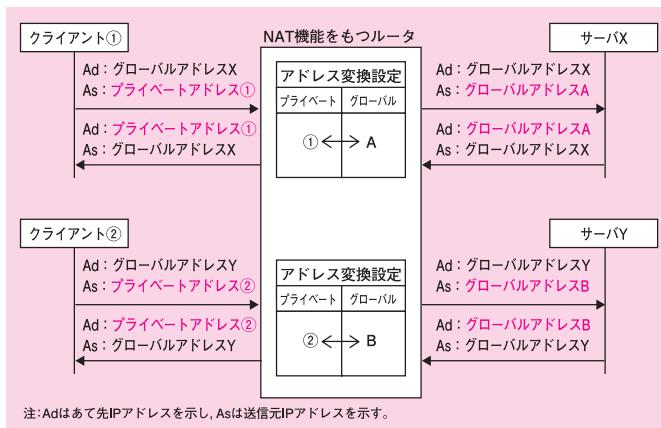


図:NATのアドレス変換の機能



RFC3022



試験に出る

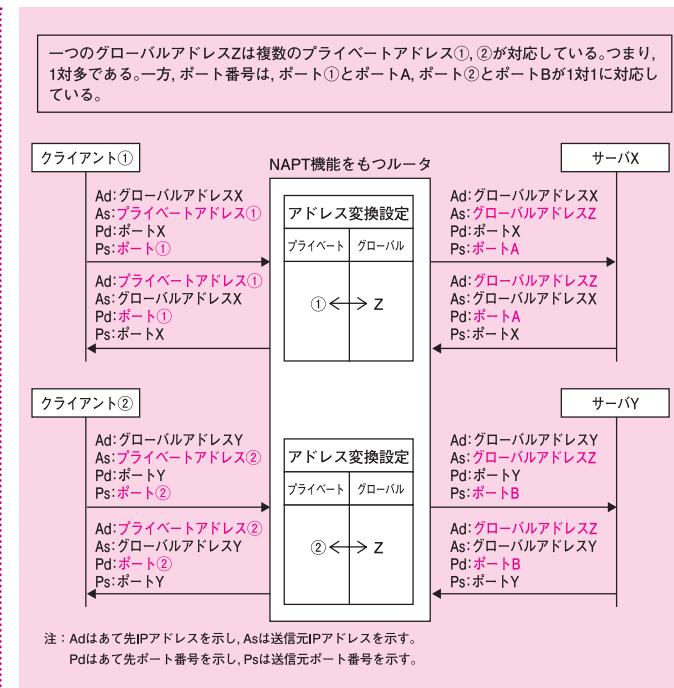
NAT技術の応用問題としてNAT444（グローバルIPアドレス枯渇対策）が平成27年午後Ⅱ問2で出題された。NATトラバーサルについて、平成27年午後Ⅱ問2、平成22年午後Ⅱ問2、平成20年午後Ⅱ問2で出題された。なお、IPsecのNATトラバーサルについては、詳しくは本書の第4章「4.4.4 IPsec」を参照していただきたい。

1

2

3

4



図：NAPT のアドレス変換の機能

## 3.7.2 NAT 越え

参考

ここに挙げた二つのケース以外にも、プロトコルによっては通信に支障が出る場合がある。例えば、IPsec のセキュリティプロトコルを AH にした場合、IP ヘッダがメッセージ認証の対象となるため、NAT で IP ヘッダを書き換えると認証エラーになる

NAPT は、IP ヘッダと TCP (又は UDP) ヘッダを書き換える。この動作は、次に示す二つのケースにおいて、通信に支障をもたらす。

1. IP の上位層がポート番号をもたないプロトコルである。
2. アプリケーション層に、送信元ホストの IP アドレスやポート番号の情報を格納している。

これら二つのケースについて、それぞれ、NAT を越えるための対応が必要となる。

### ● IP の上位層がポート番号をもたないプロトコルである

NAT の対象であるトランスポート層が TCP 又は UDP でない

ならば、ポート番号に該当するフィールドを書き換えると、通信できなくなってしまう。

これを解決するには、次のいずれかの方法を採る。

### 1. UDP ヘッダの挿入

NAT に対応できるように、IP の上位層の位置に UDP ヘッダを挿入する。この UDP ヘッダのポート番号を NAT 装置に書き換えさせることで、通常の通信と同様に NAT を通過できる。

ただし、この通信の送信元で UDP を付与し、宛先で UDP を除去する処理が必要となる。

### 2. パススルー

IP ヘッダのプロトコルフィールド（上位層のプロトコルを表すフィールド）を見て、上位層がポート番号をもたないことが分かったとき、IP ヘッダの IP アドレスだけを書き換え、ポート番号を書き換えずに転送する。

このケースに該当するプロトコルとして、IPsec がある。

IPsec を使用したインターネット VPN を例に取り上げ、NAT に起因する問題とその解決策を紹介する。

#### ● インターネット VPN の仕組み

送信側の拠点と受信側の拠点の間にインターネットが存在し、インターネットを経由した業務用通信を暗号化したい場合、インターネット VPN で通信する。

このとき、送信側拠点と受信側拠点のそれぞれに VPN 处理用のゲートウェイを設置し、両拠点間の通信はゲートウェイを必ず経由するようとする。

送信側のゲートウェイでは、送信元端末から業務用の IP パケットを受け取ると、これを暗号化してから VPN 用の IP パケットにカプセル化する。これを、受信側の VPN ゲートウェイに転送する。この仕組みにより、インターネット上では、この VPN 用の IP パケットが転送されている。

受信側の VPN ゲートウェイは、VPN 用の IP パケットを受け取ると、カプセル化を解除し、業務用の IP パケットを取り出して復号する。そして、これを宛先端末に転送する。

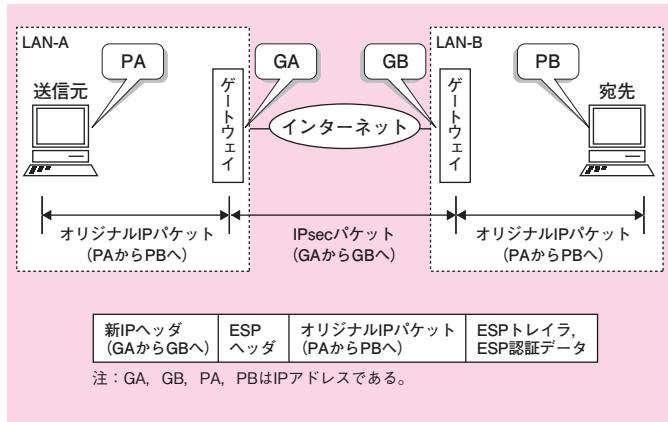
1

2

3

4

この様子を次の図に示す。ここでは LAN-A 拠点と LAN-B 拠点の間で、インターネット VPN 通信を行っている。「オリジナル IP パケット」と書かれているのが、業務用の IP パケットであり、「IPsec パケット」と書かれているのが VPN 用の IP パケットである。「ESP ヘッダ」と書かれているのが、IPsec のヘッダである。



図：インターネット VPN 通信のパケット転送

### ● NAT に起因する問題

IPsec パケット (VPN 用の IP パケット) の ESP ヘッダはポート番号をもたない。

インターネット VPN 通信のカプセル化処理を行うゲートウェイがプライベート IP アドレスをもち、VPN 用の IP パケットが NAT 装置を通過する構成になっていると、NAT の書換えにより通信が行えなくなる。

### ● 解決策

インターネット VPN では、前述した二つの方法がいづれも使われている。

一つ目の方法は、**NAT トラバーサル**と呼ばれている。この点について、詳しくは本書の第4章「4.4.4 IPsec」の「● NAT 環境下の IPsec の利用形態」で解説しているので、参照していただきたい。

二つ目の方法は、**VPN パススルー**と呼ばれている。



一つ目の方法 (NAT トラバーサル) について、平成 27 年午後Ⅱ問 2、平成 20 年午後Ⅱ問 1 で出題された。二つ目の方法 (VPN パススルー) について、平成 22 年午後Ⅱ問 2 で出題された。

## ● アプリケーション層に、送信元ホストのIPアドレスやポート番号の情報を格納している

アプリケーションの中には、自ホストのIPアドレスやポート番号をアプリケーション層（ヘッダ又はペイロード）に格納し、互いに通信相手に通知し合う仕様になっているものがある。そして、何かしらの状態遷移により、通知し合ったIPアドレスで新しい通信を開始することがある。

例えば、ホストがプライベートIPアドレスをもっており、かつ、インターネット経由で通信するとき、プライベートIPアドレスを相手に通知するならば、状態遷移後の新しい通信に失敗してしまう。プライベートIPアドレスはインターネットを経由できないからだ。

これを解決する方法は、NATの対象外であるアプリケーション層を解析し、適切なグローバルIPアドレスに置換することである。

このケースに該当するプロトコルの例として、SIPがある。

VoIPを例に取り上げ、NATに起因する問題とその解決策を紹介する。

### • VoIPの仕組み

VoIPは、二つのフェーズからなる。一つ目は、SIPを用いたセッション生成である。二つ目はRTPによる通話セッションである。

セッションを生成する際、端末同士は直接やり取りせず、プロキシ機能をもつSIPサーバを経由することができる。SIPサーバを経由する場合、TCPコネクションは、SIPサーバで終端する。



### 試験に出る

アプリケーション層にIPアドレスやポート番号の情報を格納している通信で、NATやNAPTが介在するために不具合が生じることについて、しばしば出題されている。

FTPのアクティブモードでは、インターネット上のサーバから、クライアントが指定したポートに対してTCPコネクションの確立を試みる。このポート番号がNATで変換されると不具合が生じる。この点について、平成27年午後II問2で出題された。SIPでは、通信相手に対し、自分のIPアドレスを通知する（詳しくはこのページの解説を参照）。このIPアドレスがNATで変換されると不具合が生じる。この点について、平成26年午後II問2で出題された。

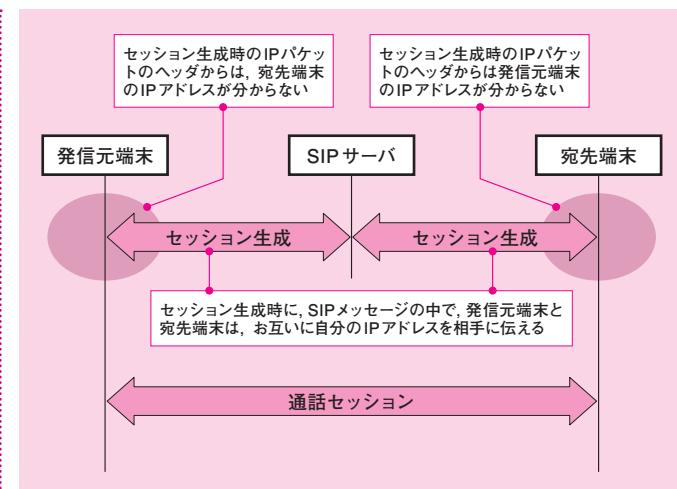
P2P通信でNAT越えを行うとき、STUNサーバをインターネット上に設置しておき、自端末とインターネットの間にNATが介在するか否かをSTUNサーバで事前に調べてからP2P通信を開始する方法が採られる。NATが介在する場合、送信元IPアドレスと送信元ポート番号がどのように変換されてインターネットに出てゆくかをSTUNサーバから通知してもらい、これを相手端末に伝えた後、P2P通信を実施する。この方法について、平成28年午後II問1で出題された

1

2

3

4



図：セッション生成時と通話時の通信

この状況を端末から見ると、セッション生成時にIPパケットをやり取りするのはSIPサーバであり、通話セッション時にIPパケットをやり取りするのは相手端末となる。言い換えると、セッション生成時に発信元から受信したIPパケットの送信元IPアドレスは、通信の相手ではない。

このようなSIPサーバを経由した通信形態に対応するため、セッション生成時にやり取りするSIPメッセージの中で、端末が自分のIPアドレスを通信相手に通知する仕様になっている。通話セッションは、このとき通知し合ったIPアドレスで通信する。

#### • NATに起因する問題

端末がプライベートIPアドレスをもっており、かつ、インターネット経由で通信するとき、セッション生成時の通信がNAT装置を経由するなら、通話セッションが行えなくなる。

SIPメッセージで通知された相手端末のIPアドレスはプライベートIPアドレスなので、通話セッションがインターネットを経由できないからである。

#### • 解決策

通話セッションを中継する機能をもつVoIPゲートウェイを

用意し、これにグローバル IP アドレスをもたせる。  
そして、セッション生成時に通知し合う IP アドレスを、  
VoIP ゲートウェイのグローバル IP アドレスに変換する。  
NAT に起因する SIP の問題とその解決策について、詳しく述べ  
くは《基礎編》第 2 章「2.2.2 VoIP ネットワーク」の「●  
NAT に起因する問題」「● NAT トラバーサル」を参照して  
いただきたい。

1

2

3

4

## 3.8 • ルーティング

試験では、経路設計についてしばしば出題されている。ルーティングの仕組み（ロングストマッチアルゴリズム）、スタティックルーティング、ダイナミックルーティングについて学習しておく。ダイナミックルーティングプロトコルの代表例として、OSPF、BGPの基本動作を押さえておく。

### 3.8.1 ルーティングの仕組み

ルータはパケットを受け取ると、宛先 IP アドレスを調べる。宛先が自分ではない場合、ルーティングテーブルに基づき、次に転送するホストの IP アドレスを決定する。

#### ● ルーティングテーブル

ルータの OS によって違いはあるが、ルーティングテーブルの主要な構成要素を次に示す。

表：ルーティングテーブル

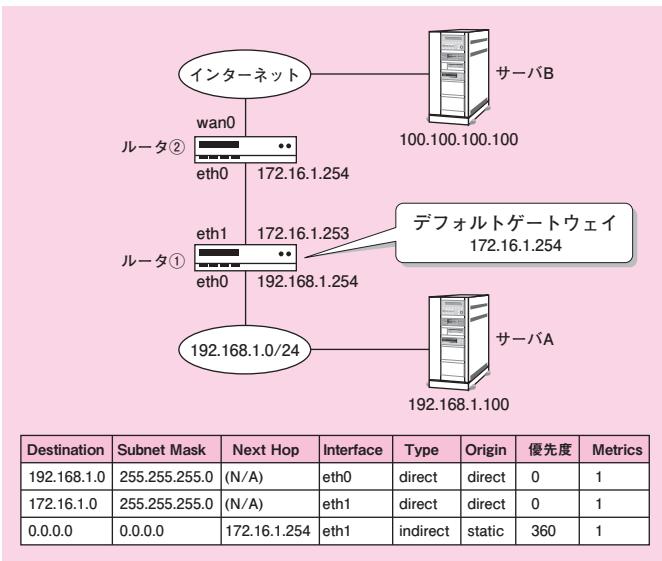
1	Destination	宛先ネットワークアドレス
2	Subnet Mask	サブネットマスク
3	Next Hop	パケットを転送するホストの IP アドレス
4	Interface	パケットを送信するインターフェース
5	Type	直接ルーティング 「direct」 を指定（※） 間接ルーティング 「indirect」 を指定（※）
6	Origin (入手方法)	経路情報のソースプロトコル 直接ルーティング 「direct」 を指定（※） 間接ルーティング 静的経路 「static」 を指定（※） 動的経路 rip, egp, ospf など、プロトコルを指定（※）
7	優先度	複数の Origin (入手方法) が存在するとき、最も優先度の高いものが選択される。値が小さいほど優先度は高い。優先度のデフォルト値は Origin (入手方法) ごとに異なるが、管理者が優先度を設定し直すことが可能である
8	Metrics	メトリック（コスト）。特定の Origin (入手方法) が選ばれ、複数の経路が存在する場合、最もメトリックの小さい経路が選択される。rip や ospf といった Origin (入手方法) の種類によって、Metrics の算出方法や設定内容は異なっている

※ルータの OS により指定方法は異なる。



ロングストマッチアルゴリズムでは同等の経路が複数存在する場合、最もメトリックの小さい経路が選択される点について、平成 23 年午後 II 問 1 で出題された。ルーティングテーブルの中からどの経路情報が採択されるかについて、平成 28 年午前 II 問 13 で出題された。

ルーティングテーブルの設定例を次に示す。



図：ルーティングテーブル（設定例ルータ①）

## ● ロンゲストマッチアルゴリズム

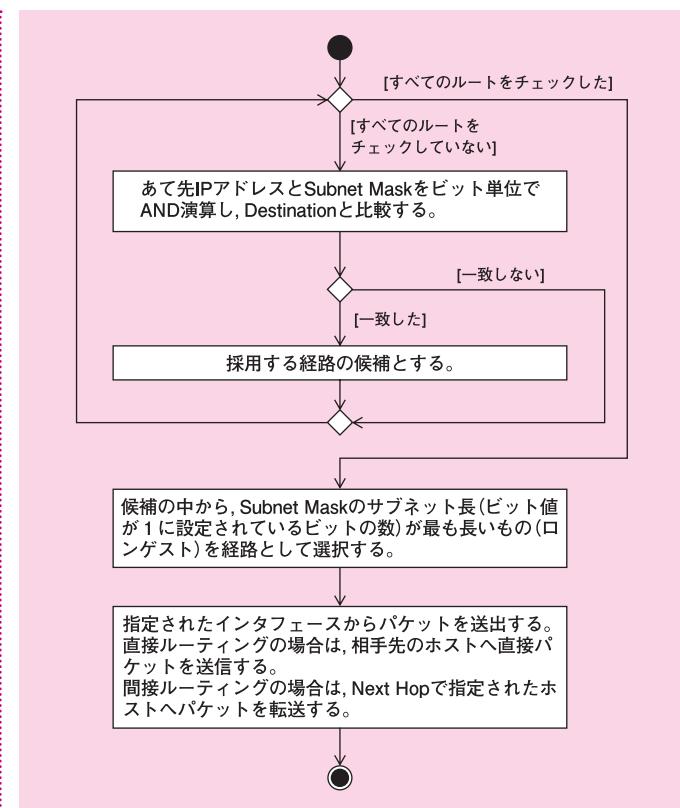
ルータが経路を決定する際、**ロンゲストマッチアルゴリズム**が使用される。Subnet Mask がロンゲストであるということは、宛先ネットワークに存在し得るホストの数を最も限定している経路情報であることを意味している。

図のネットワーク構成の場合、ルータ①において、ロンゲストマッチアルゴリズムは次のように動作する。なお、ルータ①は、eth0, eth1 という二つのイーサネットのインターフェースをもつ。ルータ①のデフォルトゲートウェイは eth1 側のネットワークにあるルータ② (172.16.1.254) である。



試験に出る

ロンゲストマッチアルゴリズムの仕組みについて、平成 18 年午後Ⅰ問 1 で出題された



図：ロングストマッチアルゴリズム

### [サーバBへ送信する場合]

サーバBのIPアドレスは100.100.100.100である。この場合、候補となるのは前ページにあるルーティングテーブルの3行目しかない。よって、eth1を通じて172.16.1.254へ間接ルーティングされる。

### [サーバAへ送信する場合]

サーバAのIPアドレスは192.168.1.100である。この場合、候補となるのは1行目と3行目の二つある。Subnet Maskがロングストなものは1行目である。よって、eth0を通じて192.168.1.100へ直接ルーティングされる。

## ● null インタフェース

ルータにパケットを破棄させたいとき、ルーティングテーブルの転送先インターフェースとして、**null インタフェース**を指定することができる。これは仮想的なインターフェースであり、ここを転送先とするパケットをルータは破棄する仕組みになっている。

null インタフェースを使用すべき典型例として、ルーティングループの回避がある。

例えば、ある拠点のネットワークが「10.1.0.0/16」であり、外部からは、拠点ネットワークの宛先が自ルータに指定されているものとする。しかし、拠点ネットワークの中には、未使用的範囲「10.1.100.0/24～10.1.255.0/24」が存在しているとしよう。

この構成において、未使用的範囲を宛先とするパケットを受け取ったときは、パケットをどこにも転送してはならない。つまり、ルータがパケットを破棄するように設定しておく必要がある。そこで、null インタフェースを転送先とする経路情報をルーティングテーブルを登録しておくのである。

ここで、仮に、「10.1.100.0/24～10.1.255.0/24」の宛先をデフォルトゲートウェイに指定したとすると、ルーティングループが発生してしまう。外部からは「10.1.0.0/16」の宛先が自分に指定されているので、パケットが送り返されるからだ。

## ● ポリシベースルーティング

**ポリシベースルーティング** (PBR:Policy Based Routing) とは、通常の経路制御とは異なる方法で経路を選択する経路制御である。PBR を動作させるには、優先度を最も高くしておく必要がある。

PBR で使用する経路制御の条件には、例えば次のようなものがある。なお、許容される条件設定は製品により異なっている。

- IP アドレス
- ポート番号
- プロトコル
- パケットサイズ
- ToS (Type of Service) 値



試験に出る

null インタフェースについて、平成 23 年午後Ⅱ問 1 で出題された

1

2

3

4



試験に出る

ポリシベースルーティングを行う際に優先度を最も高くすることについて、平成 26 年午後Ⅰ問 1 で出題された



VRFについて、平成25年午後I問3で出題された

PBRを行うときは、ルートマップを作成する。

ルートマップとは、条件と処理内容を記述したもので、条件に合致した処理内容が実行する仕組みになっている。

なお、ルートマップは、PBR以外にもルータの様々な動作を指定するのに使用することができる。

### ● VRF

**VRF** (Virtual Routing and Forwarding) 機能は、1台のルータの中に、複数の独立した仮想ルータを稼働させる機能である。各々の仮想ルータはそれぞれ固有のルーティングテーブルをもち、個別に経路制御を行っている。

VRF機能の設定は、物理ルータのインターフェースごとに、経路制御に使用する仮想ルータを1個指定する仕様になっている。仮想ルータはそれぞれ独立しているため、使用する仮想ルータが異なるインターフェース同士は通信できない。それゆえ、経路制御の対象となるアドレスブロックは、仮想ルータ間で重複していてもよい。

なお、製品によっては、仮想ルータをまたぐ経路制御を行えるものがある。このときは、当然ながら、経路制御の対象となるアドレスブロックが仮想ルータ間で重複してはならない。

## 3.8.2

## スタティックルーティング／ダイナミックルーティング

経路情報を登録する方法は**スタティックルーティング**と**ダイナミックルーティング**という二つに大別できる。クライアント端末やSOHOルータなど、経路情報が少ないホストではスタティックルーティングが使用され、大規模なネットワークの経路情報を管理するルータではダイナミックルーティングが使用されるのが一般的である。それぞれに長所と短所があるため、その特徴をつかんで両者を使い分けることが必要である。

表：スタティックルーティングとダイナミックルーティングの特徴

	ダイナミックルーティング	スタティックルーティング
管理の容易さ	使用するプロトコルの知識が必要となる。ネットワークが大規模の場合、経路情報の維持管理が自動的に行われるため、スタティックルーティングより管理は容易となる	設定が容易に行えるため、経路情報が少ない場合、管理は容易である。デフォルトゲートウェイだけを設定するような、クライアント端末やSOHOルータで使用される
耐障害性	経路上の機器、回線の障害を自動的に検知する。迂回ルートがある限り、ルーティングテーブルを自動的に書き換えて迂回ルートを設定する	障害の検知、ルーティングテーブルの書換えを手動で行う必要があるため、障害発生時に時間と労力がかかる
負荷分散	プロトコルによっては、負荷分散を行うことができる	負荷分散を行うことはできない
トラフィック	プロトコルによってトラフィック量の差異はあるが、ルータ間で経路情報を維持するためにトラフィックが発生する	経路情報維持のためのトラフィックは発生しない

スタティックルートとダイナミックルートを混在させたり、複数のダイナミックルーティングプロトコルが公告したルートを混在させたりすることも可能である。例えば、スタティックルートの優先度を下げておき、障害発生などでダイナミックルートが失われたときだけ利用されるように設定しておくことができる。これを**フローティングスタティック**という。

スタティックの経路情報を、ダイナミックルーティングプロトコルを使って通知することが可能である。同様に、二つのダイナミックルーティングプロトコルを動かしておき、一方のプロトコルの経路情報を他方に通知することが可能である。これを**再配布**という。



試験に出る

スタティックルーティングと比較したダイナミックルーティングの利点について、平成29年午後I問3で出題された

1

2

3

4



試験に出る

フローティングスタティックルーティングを用いたバックアップ経路設計について、平成16年午後II問1で出題された。  
BGPからOSPFへの再配布について、再配布されたものを再び自分に再配布することに起因するルーティングループの発生について、平成29年午後I問3で出題された

### 3.8.3 EGP / IGP

インターネットでは、IPアドレスの全空間をICANNが管理しており、AS(Autonomous System、自律システム)と呼ばれる組織にIPアドレスをまとめて割り振っている。ASとは、同一のポリシによって管理されるネットワーク群であり、2オクテット又は4オクテットのAS番号がICANNから割り当てられている。さらに、ASは、独自にポリシを定めて経路情報を維持運用し、ほかの組織にIPアドレスを割り当てる。



試験に出る

ASについて、平成29年午後I問3で出題された

参考

### プライベート AS 番号

AS 番号 64512～65535 は、プライベート AS 番号と呼ばれる。これは、自 AS 内で閉じたネットワークでのみ使用することができ、インターネットに経路広告してはならない。ちょうど、IPv4 のプライベート IP アドレスをインターネットで使用できないのと同じだ。

平成 29 年午後 I 問 1 に登場する事例では、自社拠点とクラウド事業者拠点間を VPN トンネルで接続し、BGP を用いて経路情報を交換している。VPN 接続されており、インターネットと接続していないことから、自社拠点にはプライベート AS 番号が割り当てられている



試験に出る

RIP について、平成 26 年午前 II 問 11、平成 18 年午前 問 30 で出題された。

これら AS は、具体的に言うと、大規模な ISP、地域ネットワークなどである。そして、AS が IP アドレスブロックを割り当てる、より小規模のサイトには、中規模の ISP、企業、大学などがある。

このように経路情報は階層構造で管理されており、そこで使用されるルーティングプロトコルもそれぞれ異なっている。プロトコルを大別すると、AS 間で使用される **EGP** (Exterior Gateway Protocol)、AS 内で使用される **IGP** (Interior Gateway Protocol) に分類できる。EGP では、BGP (ver4) が広く用いられている。IGP では、OSPF、RIP (ver2) が広く用いられている。

### ● RIP

RIP は、AS 内を接続するルーティングプロトコルであり、**距離ベクトル方式**が採用されている。RIP の概要を次の表に示す。

表 : RIP の概要

EGP / IGP の種別	IGP
経路制御の方式	距離ベクトル方式
下位プロトコル	UDP
通信形態	マルチキャスト (224.0.0.9)

### ● 経路制御の特徴と仕組み

RIP は、比較的小規模な AS 内で使用されている。後述する OSPF と比べると、シンプルな経路制御の仕組みをもつ。その主要な特徴と仕組みは、次のとおりである。

1. 経由するルータのホップ数が最小の経路を選択する。
2. ルータが広告するのは、ルーティングテーブルにエントリされた全ての経路情報である。
3. 上記 2 のやり取りは死活監視を兼ねている。
4. RIP は、バージョン 1 (RIPv1) とバージョン 2 (RIPv2) の 2 種類がある。前者はサブネットマスクに対応していないが、後者は対応している。

1 番目の特徴に挙げた経路選択は、経路ベクトル方式と呼ばれている。これは、宛先ネットワークとそのサブネットマスクが等しい経路情報が複数存在する場合（つまり、ロングリストマッチアルゴリズムでは同等の経路である場合）、経由するルータのホッ

プ数が最小の経路を選択する方式である。

RIP は、ホップ数が 15 を超える経路は、経路選択の対象から除外する仕組みになっている。言い換えるなら、宛先に到達可能なホップ数は、15 が最大になる。

2 番目と 3 番目の特徴に述べたとおり、経路広告は死活監視を兼ねているため、たとえ経路情報が変化しなくとも一定期間で実施される。この経路広告の間隔は、30 秒である。経路障害が発生したと判断する時間の長さは、その 6 回分（180 秒）である。

このため、広告する経路情報が多いと、帯域を圧迫してしまう。したがって、RIP は小規模なネットワークで使用するべきである。

## ● OSPF

OSPF (Open Shortest Path First) は、AS 間を接続するルーティングプロトコルであり、**リンクステート方式**が採用されている。OSPF の概要を次の表に示す。

表：OSPF の概要

EGP / IGP の種別	IGP	
経路制御の方式	リンクステート方式	
下位プロトコル	IP	
通信形態	マルチキャスト	
	224.0.0.5	Hello の交換
	224.0.0.6	DR/BDR 宛てのリンク状態情報の送信

## ● 経路制御の特徴と仕組み

OSPF は、比較的大規模な AS 内で使用されている。その主な特徴と仕組みは、次のとおりである。

1. 最小の**コスト**で到達できる経路を選択する。
2. **エリア**を単位とする経路制御を行う。
3. ルータが広告するのは、**LSA** (Link State Advertisement) と呼ばれるリンク状態の情報である。各ルータのルーティングテーブルは、LSAに基づいて構成される。
4. **Hello** パケットを交換して死活監視を行う。
5. 可変長サブネットマスクに対応している。

それでは、OSPF を特徴付ける経路選択、エリア、LSA、死活監視について、以下で解説しよう。



試験に出る

OSPF については、出題例が多いので午前試験と午後試験を分けて列挙しよう。

午前試験では、プロトコルの特徴を問うものが比較的多く出題されている。平成 29 年午前Ⅱ問 3、平成 28 年午前Ⅱ問 4（平成 25 年午前Ⅱ問 4、平成 21 年午前Ⅱ問 4 と同じ問題）、平成 27 年午前Ⅱ問 4、平成 24 年午前Ⅱ問 7、平成 21 年午前Ⅱ問 4、平成 21 年午前Ⅱ問 4、平成 20 年午前Ⅱ問 4、平成 20 年午前Ⅱ問 28、平成 19 年午前Ⅱ問 28、平成 18 年午前Ⅱ問 23 で出題された。

午後試験では、冗長化設計の観点からコスト計算が出題されており、OSPF の内容そのものは深く問われていない。平成 29 年午後Ⅰ問 3、平成 28 年午後Ⅱ問 1、平成 26 年午後Ⅰ問 1、平成 20 年午後Ⅰ問 4 で出題された。

なお、OSPFは、ネットワークの種類（ブロードキャスト通信が可能であるか否か、マルチアクセスかポイントツーポイントであるか）により、動作が若干異なっている。

本書は、試験対策として重要なポイントに的を絞って解説することを趣旨としている。そこで、イーサネット（ブロードキャスト可能なマルチアクセスネットワーク）を対象とした、ごく基本的な仕組みを解説する。

より詳しい内容は専門書を参照していただきたい。

### ● 経路選択

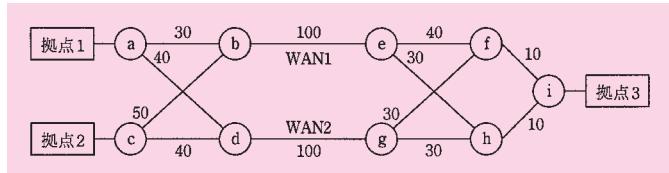
OSPFは、リンクごとにコストを設定することができる。なお、コストを明示的に設定しなかった場合、物理ポートの帯域幅に基づき、帯域幅が大きいほどコストが小さくなるように、自動的に割り当てられる。

OSPFの経路選択は、宛先ネットワークとそのサブネットマスクが等しい経路情報が複数存在する場合（つまり、ロングストマッチアルゴリズムでは同等の経路である場合）、コストが最小の経路を選択する。

コストが最小の経路が複数ある場合は、それら経路間でトライフィックを分散する。これを**イコールコストマルチパス機能**という。なお、パケットを各経路に振り分けるアルゴリズムには様々なものがあり、ベンダや機器に依存している。

コストに基づく経路選択の例として、平成28年午前Ⅱ問4に登場したネットワークを取り上げて解説しよう（一部改変している）。

この図で、○印はルータを表しており、リンクに割り当てられた数値はコストを表している。



図：コストに基づく経路選択の例

拠点1から拠点3に至る経路は、次の表に示すとおり、4通りが考えられる。

このうち、最小コストをもつ経路は、項番②である。したがって、この経路が選択される。

表：拠点 1 から拠点 3 に至る経路

	経路	コスト
①	拠点 1 → a → b → e → f → i → 拠点 3	$30 + 100 + 40 + 10 = 180$
②	拠点 1 → a → b → e → h → i → 拠点 3	$30 + 100 + 30 + 10 = 170$
③	拠点 1 → a → d → g → f → i → 拠点 3	$40 + 100 + 30 + 10 = 180$
④	拠点 1 → a → d → g → h → i → 拠点 3	$40 + 100 + 30 + 10 = 180$

拠点 2 から拠点 3 に至る経路は、次の表に示すとおり、4 通りが考えられる。

このうち、最小コストをもつ経路は、項番③、④である。したがって、イコールコストマルチパス機能の働きにより、これら二つの経路がともに選択されてトラフィック分散が行われる。

表：拠点 2 から拠点 3 に至る経路

	経路	コスト
①	拠点 2 → c → b → e → f → i → 拠点 3	$50 + 100 + 40 + 10 = 200$
②	拠点 2 → c → b → e → h → i → 拠点 3	$50 + 100 + 30 + 10 = 190$
③	拠点 2 → c → d → g → f → i → 拠点 3	$40 + 100 + 30 + 10 = 180$
④	拠点 2 → c → d → g → h → i → 拠点 3	$40 + 100 + 30 + 10 = 180$

## ● エリア

OSPF は、ネットワークを複数のエリアに分割することができる。分割しない場合、エリアは一つだけとなる。

どのようにエリアを構成するにせよ、必ず存在しなければならないエリアがある。これを**バックボーンエリア**という。バックボーンエリアの番号は 0 番である。基本的に、バックボーンエリアを除く全てのエリアは、バックボーンエリアに隣接させる。

## ● エリア内の経路広告とリンク状態情報の同期

イーサネットの場合、同一エリアの同一サブネットワークの中で、**DR** (Designate Router、代表ルータ)、**BDR** (Backup Designate Router、バックアップ代表ルータ) が選出される。

エリア内のルータは、DRとの間、及び、BDRとの間でのみ、Adjacency (隣接関係) を確立する。二つ以上のサブネットワークに接続しているルータは、それぞれのサブネットワークにおいて、DR / BDR の間で Adjacency を確立する。



DR と BDR の選出は、Hello パケットの交換を通して自動的に行われる仕組みになっている(詳細は割愛する)

全てのルータは、Adjacencyを確立した後、自分のリンク状態情報をDRルータに向けてマルチキャスト(224.0.0.6)で広告する。これを受けたDRルータは、このリンク状態情報を全てのルータに向けてマルチキャスト(224.0.0.5)で広告する。この結果、同一エリアの中で、リンク状態情報の同期が取られる。

各ルータは、自分のリンク状態情報を受信したリンク状態情報に基づき、ルーティングテーブルを生成する。

障害発生等によりネットワークの構成が変化したならば、前述の振る舞いと同様に、リンク状態の変化したルータがこれをDRルータに向けてマルチキャスト(224.0.0.6)で広告する。これを受けて、DRルータは、このリンク状態情報を全てのルータに向けてマルチキャスト(224.0.0.5)で広告する。こうして、ネットワークの構成が変化したときにも、エリア内でリンク状態情報が伝播され、ルーティングテーブルが動的に変化する。

なお、ネットワークの構成が変化しなくとも、30分間隔でリンク状態の情報を交換する仕様になっている。



### 試験に出る

BGPネットワークからOSPFネットワークへの再配布について、平成29年午後I問3で出題された

## ● エリア外での経路広告と経路情報の集約

バックボーンエリアとその他のエリア間は、**エリア境界ルータ(ABR)**(Area Border Router)を介して接続され、リンク状態情報が交換される。

ABRは、エリア内の経路情報を集約して、他のエリアに送信することができる。ABRの**経路集約**は自動的に行われるわけではないため、どのように行うかを明示的に設定する必要がある。

OSPFネットワークは、OSPF以外のダイナミックルーティングプロトコルで経路制御されたネットワーク(外部ネットワーク)との間で、経路情報を交換することができる。両者の間は、**AS境界ルータ(ASBR)**(Autonomous System Border Router)で接続される。

このとき、ASBRは、一方のルーティングプロトコルの経路情報を他方のものに変換してから送信する必要がある。これを**再配布**という。

ASBRは、再配布する際、経路情報を集約して、他のエリアに送信することができる。ASBRの再配布と**経路集約**は自動的に行われるわけではないため、どのように行うかを明示的に設定する

必要がある。

## ● LSA

LSA (Link State Advertisement) とは、ルータ間で交換されるリンク状態の情報である。LSA パケットには、ルータがもつインターフェースやルータに接続されたネットワークの情報などが格納されている。

LSA は複数の Type がある。作成するルータ、役割、交換される範囲などが、Type により異なっている。その主なものを次に示す。

表：LSA の複数の Type

Type	名称	作成ルータ	役割	範囲
1	Router-LSA	全 OSPF ルータ	自ルータのリンク情報を通知する	エリア内部
2	Network-LSA	代表ルータ(DR)	自エリアのネットワーク情報を通知する	エリア内部
3	Network-Summary-LSA	代表ルータ(DR)	他エリアのネットワーク情報を通知する	エリア内部
4	ASBR-Summary-LSA	エリア境界ルータ(ABR)	非 OSPF ネットワークへ接続する ASBR(AS 境界ルータ)の情報を通知する	エリア内部
5	AS-External-LSA	AS 境界ルータ(ASBR)	非 OSPF ネットワークの経路情報を OSPF ドメインに通知する	OSPF ドメイン全体(スタブエリア以外)

## ● 死活監視

OSPF は、Hello パケットを交換し合って死活監視を行う。この Hello の間隔は 10 秒、経路障害が発生したと判断する時間の長さは 40 秒である（いずれもイーサネットの場合）。



試験に出る

## ● BGP

BGP-4 は、AS 間を接続するルーティングプロトコルであり、**経路ベクトル方式**が採用されている。BGP の概要を次の表に示す。

表：BGP の概要

EGP / IGP の種別	EGP
経路制御の方式	経路ベクトル方式
下位プロトコル	TCP
通信形態	ユニキャスト (TCP コネクション)

## ● 経路制御の特徴と仕組み

インターネットのバックボーンで交換される経路情報は、数十万に上る。BGP は、この膨大な経路情報の交換を実現するために、様々な工夫を取り入れている。

BGP は、RIP や OSPF ほど出題例は多くない。午前試験と午後試験に分けて列挙しよう。  
午前試験では、平成 26 年午前 II 問 7 (平成 25 年午前 II 問 6, 平成 22 年午前 II 問 8 と類似の問題)、平成 24 年午前 II 問 1, 平成 22 年午前 II 問 8、平成 19 年午前 問 23, 平成 18 年午前 問 42, 平成 17 年午前 問 25, 平成 17 年午後 I 問 4, 平成 16 年午前 問 41 で出題された。  
午後試験では、平成 29 年午後 I 問 3, 平成 17 年午後 I 問 4 で出題された。平成 29 年午後 I 問 3 は、BGP と OSPF を組み合わせた経路の冗長化設計が出題されており、BGP から OSPF への再配布が問われていた。

その主な特徴と仕組みは、次のとおりである。

1. 経路選択はパスアトリビュートによって行われる。これには様々な種類があり、ASのポリシに基づく柔軟な経路選択を可能にしている。
2. ルータが広告するのは、NLRI(Network Layer Reachability Information)とパスアトリビュートである。
3. 経路が変化したときだけ差分を送信する仕組みにより、経路情報の交換にかかるトラフィックを抑えている。
4. 経路広告する通信の信頼性を確保するため、TCPのコネクションを用いている。コネクションを張る2台のルータをBGPピアと呼ぶ。
5. KEEP ALIVEパケットを交換して死活監視を行う。



インターネットのバックボーンで交換される経路情報の総数(フルルート)は、IPv4が60万超、IPv6が4万超もある(2017年12月現在)。この数は年々増加している。

それでは、BGPを特徴付ける経路選択、BGPピア、死活監視について、以下で解説しよう。

### ● 経路選択

NLRIは、ネットワークアドレスとサブネットマスクの組である。パスアトリビュートは、数ある経路の候補の中からベストパス(NLRI)を一つ選択するために用いられる。このベストパスが、ルーティングテーブル上の経路選択に使用される。

パスアトリビュートは、他のルーティングプロトコルのメトリックに相当するものだ。RIPでは距離が、OSPFではコストが用いられているのに対し、BGPでは様々な種類の属性が定義されているという特徴をもつ。

数々のパスアトリビュートには優先順位があり、それを調整することで、ASは、自ら定めたポリシに基づいてベストパスを選択することができる

BGPの主要なパスアトリビュートは、AS\_PATHである。

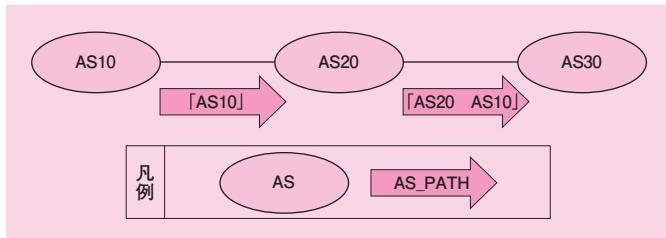
これは、宛先ネットワークに至る経路(パス)を表す属性である。このパスが、「AS番号の羅列」で記述されている。

AS\_PATHに基づいてベストパスを決定するときは、AP\_PATH長が短いものを選択する仕様になっている。要するに、経由するASの合計数が少ない方を優先するわけだ。

BGPは、特にパスアトリビュートの調整をしなければ、AS\_PATHに基づいてベストパスを選択する。BGPが経路ベクトル方式と呼ばれる理由はここにある。

具体例を挙げて説明しよう。

今ここに、AS10, AS20, AS30という三つのASがあるとする。



図：AS\_PATH の例

AS10が自ネットワークを経路広告するとき、AS\_PATHは「AS10」である（見やすくするために「AS10」というAS名を記したが、本当はAS番号である）。

AS20がこれを受け取り、AS30に経路広告するとしよう。このときAS20は、AS\_PATHの先頭に「AS20」を追加してから広告する。この結果、AS20が経路広告する、「AS10ネットワークの経路情報」のAS\_PATHは、「AS20 AS10」となる。

AS30がこれを受け取ると、AS10ネットワークに到達するには「AS20 → AS10」というパスを通ることが分かる。

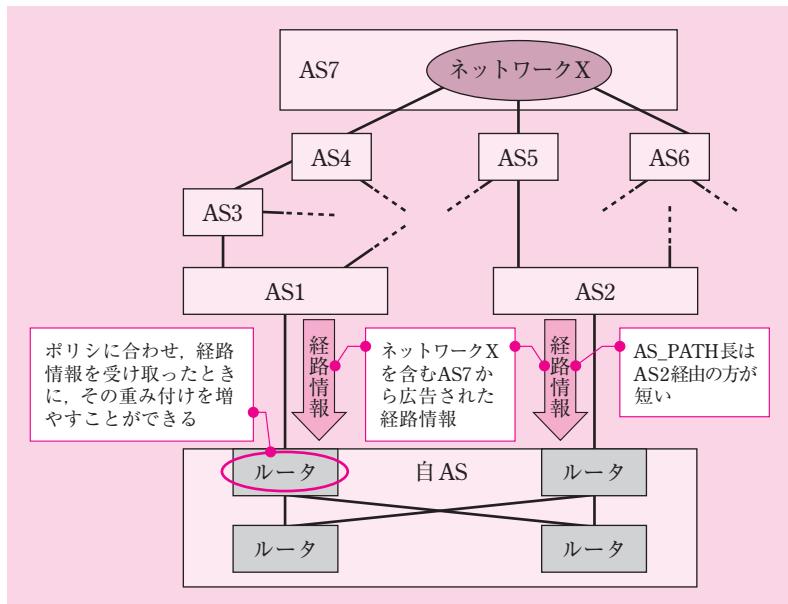
AS30が他のASからもAS10ネットワークの経路情報を広告されている場合は、AS\_PATH長を比較し、経由するASの合計数が少ない方を優先する。

それでは、AS\_PATH以外のパスアトリビュートを組み合わせた場合、どのように経路選択が行われるのだろうか。そのときは、パスアトリビュートごとに定められた優先順位に従う仕組みになっている。

例として、次の図に示すネットワークを使って説明する。自ASは、あるネットワークXに至る経路情報をAS1とAS2から受け取っているとしよう。要は、自ASからネットワークXに到達できる経路として、AS1経由とAS2経由の2通りがあるわけだ。



自律システム間のルーティングを行うBGP-4は、同一IPアドレスをもつノードがインターネット上の複数の拠点（自律システム）に存在していても、送信元から見て経路上最も近い拠点をベストパスに選んで、そこからルーティングする機能をもつ。したがって、IPv4ネットワークにおいて、BGP-4を利用したエニーキャスト通信が実現されている。BGP-4を利用したエニーキャスト通信を利用している実例が、ルートDNSサーバである。実を言うと、半数以上のルートDNSサーバは、同一IPアドレスをもつホストが複数の異なる地域に分散配置されている。世界中のリゾルバからの問い合わせは、エニーキャスト通信の仕組みによって、各々のリゾルバから最も近いホストに向けて送信されている。この技術は、RFC3258 (Distributing Authoritative Name Servers via Shared Unicast Addresses) で文書化されている。



図：BGP のパスアトリビュートを活用した経路制御

このとき、例えば次のような経路制御が可能となる。

- パスアトリビュートの AS\_PATH を見ると、ネットワーク X に到達するまでに通過する AS のパス長は、AS1 経由が「AS1 → AS3 → AS4 → AS7」の 4 個分であり、AS2 経由が「AS2 → AS5 → AS7」の 3 個分なので、AS2 経由の方が短い。そこで、AS2 経由の方をベストパスにしよう。
- パスアトリビュートの AS\_PATH に基づけば、AS2 経由の方を選択するのが適切だ。しかし、このたびは意図的に AS1 経由の方を選択したい。これを実現するため、AS1 から受け取った経路情報に、パスアトリビュートの LOCAL\_PREF を設定して重み付けを増やし、AS1 経由がベストパスになるように自 AS 内の全 BGP ルータに学習させよう（これは、LOCAL\_PREF の方が AS\_PATH より優先順位が高いことを利用した設定である）。

この例に示したように、ポリシに基づくきめ細かな設定を実施することで、AS は膨大な経路情報の交換を適切に制御し、日々

運用しているのである。

### ● BGP ピア

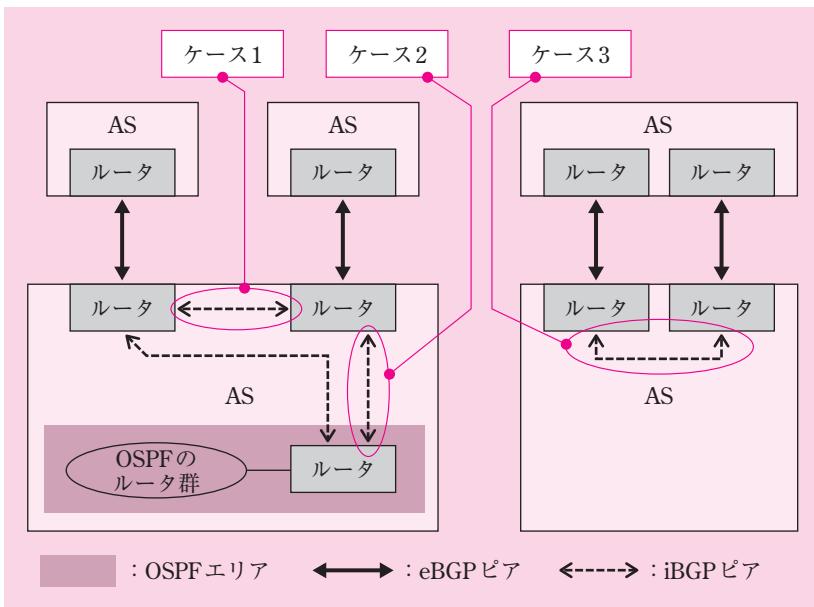
BGP 接続を行う 2 台のルータ間では、TCP の 179 番ポートを使用し、経路情報の交換を行う。このコネクションを BGP ピアと呼ぶ。

自 AS の BGP ルータは、他 AS の BGP ルータと BGP ピアを設定し、経路情報を交換している。このように、異なる AS に属するルータ間で設定される BGP ピアを、eBGP ピア (external BGP ピア) と呼ぶ。

自 AS の BGP ルータは、自 AS 内の別の BGP ルータとも BGP ピアを設定し、経路情報を交換している。このように、同じ AS に属するルータ間で設定される BGP ピアを、iBGP ピア (internal BGP ピア) と呼ぶ。

iBGP ピアを設定する目的は、自分が受け取った経路情報を、ピアを張る相手に伝えるためである。ただし、どのように伝え合うかに着目すると、その役割には幾つか種類がある。

主だったケースを三つ示す。



図：eBGP ピアと iBGP ピア

- ケース 1：他 AS の情報を共有する

このiBGPピアは、自ASの境界に位置する2台のBGPルータが、それぞれ異なるASから経路情報を受けている。この経路情報を自AS内で共有している。

- ケース 2：自 AS の内部に情報を伝える

このiBGPピアは、自ASの境界に位置するBGPルータが、自ASの内部に位置するBGPルータに経路情報を伝えている。AS内ではOSPFが稼働しており、この内部BGPルータに接続している。

この内部BGPルータでは、BGPとOSPFの二つが稼働している。このルータは、OSPFルータから転送されたパケットを受け取った後、今度はBGPの経路情報を使ってルーティングしAS外へと転送する役割をもつ。さらに、境界BGPルータから転送されたパケットを受け取った後、今度はOSPFの経路情報を使ってルーティングしAS内へと転送する役割をもつ。いわば、このルータはOSPFとBGPの間を橋渡しする存在だ。

なお、小規模なネットワークであれば、境界のルータが橋渡しする役割も兼務すればよい。ケース2のような、橋渡しするためのBGPルータを内部に別途設ける必要はない。

- ケース 3：隣接 AS 間の経路を冗長化する

このiBGPピアは、隣接ASとの経路の冗長化のために、iBGPピアを張る2台のBGPルータがともに隣接ASと接続している。

通常、iBGPピアは、AS内の全てのBGPルータ同士でフルメッシュ接続する。iBGPピアを張る相手から学習した経路情報は、他のiBGPピアに通知しない。これは、AS内でBGPによるルーティングループを防ぐためである。

iBGPピアで結ばれた2台のBGPルータは、直に接続していくてもよい。つまり、非BGPルータ(BGPが稼働していないルータ)を中継していても構わない。その場合、それら2台のBGPルータ、及び、それらを中継する位置にある非BGPルータは、全て、何らかのIGP(例えばOSPF)が稼働している必要がある。2台

のBGPルータがやり取りするパケットは、IGPの経路制御により、AS内でルーティングされる。

### ●死活監視

BGPピアは、KEEP ALIVEパケットを送信して、両者間のTCPコネクションの死活監視を行う。

KEEP ALIVEの送信間隔は、ベンダにより異なる。Cisco Systems社の場合、30秒である。KEEP ALIVEが3回途絶えたとき、経路障害が発生したと判断する。

1

2

3

4

## 3.9 • IPv6

ネットワーク技術者にとって IPv6 は必須の習得知識になっている。午後試験で出題されることが予想されるため、主な機能を取り上げる。

### 3.9.1 IPv4 からの主な変更点



IPv4 から IPv6 へ移行したとしても、下位のデータリンク層や上位のトランスポート層のプロトコルは継続利用が可能である。しかし、ICMP、DHCP、ルーティングプロトコルなど管理用プロトコルは IPv6 用に規格化されており、IPv6 への移行に合わせて使用しなければならない。さらに、アドレス長が拡張されたり、ソケットの構造体や API が変更されたりしているため、アプリケーション層のネットワークソフトウェアも IPv6 対応のバージョンに変更する必要がある。

インターネット層の基本的機能は、IPv4 も IPv6 も同じである。すなわち、エンドシステム間のパケット通信はインターネット層が担い、通信の信頼性確保は上位層 (TCP や UDP) が担う。その信頼性品質の程度は、上位層の機能に委ねられる。

IPv6 は、IPv4 の基本機能を受け継ぎながら、機能の追加やパケットフォーマットの簡略化が施されている。

IPv4 からの主な変更点は、次の 3 点である。

1. アドレス空間の拡張
2. 近隣探索とアドレス自動設定機能
3. パケットフォーマットの簡略化

以下、順を追って解説する。

### 3.9.2 アドレス空間の拡張

IPv6 では、アドレス長が 32 ビットから **128 ビット** に拡張された。アドレスのスコープや用途に応じて、広大なアドレス空間が階層的に割り当てられている。

#### ● アドレススコープ

アドレススコープとは、アドレスを使用できる範囲のことであ

る。グローバルアドレス、ユニークローカルアドレス、リンクローカルアドレスなどが規定されており、それぞれにアドレス空間が割り当てられている。

グローバルアドレスは、使用できる範囲が限定されていない。これはIPv4のグローバルアドレスと同じであり、インターネットで使用できるアドレスである。ユニークローカルアドレスは、使用できる範囲が一つのサイトに限定されるアドレスである。これはIPv4のプライベートアドレスに相当し、インターネットに接続できない。リンクローカルアドレスは、使用できる範囲が一つのリンクに限定されるアドレスである。これはIPv4アドレスのリンクローカルアドレス(169.254.0.0/16)に相当し、ルータを超えた通信を行えない。

アドレススコープのアドレスの構造を次の表に示す。

表：アドレススコープごとのアドレスの構造

スコープの種類	アドレスの構造	
グローバル	グローバルユニキャストアドレスの構造	
	1～48ビット	グローバルルーティングプレフィックス*
	49～64ビット	サブネットID
	65～128ビット	インターフェースID
※ RFC2374は、現在利用可能なものを先頭3ビットが「001」であるものと定めている。		
ユニークローカル	ユニークローカルユニキャストアドレスの構造	
	1～7ビット	fc00::/7 (現在使用できるのは fd00::/8)
	8～48ビット	Global ID サイト内で自由に設定できるが、乱数を用いることが推奨されている。Global IDが一致する可能性は低いため、ほぼユニークなアドレスであると言える
	49～64ビット	サブネットID
	65～128ビット	インターフェースID
リンクローカル	リンクローカルユニキャストアドレスの構造	
	1～10ビット	fe80::/10
	11～64ビット	全て0
	65～128ビット	インターフェースID



試験に出る

IPv6のリンクローカルユニキャストアドレスについて、平成26年午前Ⅱ問1で出題された

1

2

3

4

企業向け IPv6 接続サービスに契約した場合、グローバルルーティングプレフィックス（先頭の 48 ビット）がプロバイダから割り当てられる。残りの 80 ビットのうち、サブネット ID（後続する 16 ビット）をサブネットを識別するために用い、残りのインターフェース ID（後半の 64 ビット）をホストのインターフェースを識別するために用いる。

### ● インタフェース ID

インターフェース ID は、同一サブネット内でインターフェースを識別する番号であり、アドレスの後半 64 ビットを占めている。

インターフェース ID は、リンク層アドレス（MAC アドレスなど）から生成する方法と、ランダム値から生成する方法が規定されている。どちらのアドレスもインターフェースに割り当てることができる。ランダム値からインターフェース ID を生成したアドレスは、一時アドレス（temporary address）と呼ばれる。

MAC アドレスからインターフェース ID を生成する場合、「Modified EUI-64」形式に従う。これは、次の手順に従って生成する。

- ① 上位 24 ビット（OUI）と下位 24 ビットの間に、0xffffe を挿入する（①が完了した時点で、EUI-64 形式になっている）。
- ② U/L ビット（Universal/Local：先頭から 7 ビット目）を「1」（Local）にする。

例）MAC アドレスが「00:11:22:33:44:55」の場合、インターフェース ID は次のようになる。

- ① 「00:11:22:33:44:55」 → 「00:11:22:**ff:fe**:33:44:55」
- ② 「00:11:22:ff:fe:33:44:55」 → 「**02**:11:22:ff:fe:33:44:55」

### ● 宛先アドレスの種類

宛先アドレスは、その到達範囲により次の三つに分類されている。



RFC3041 (Privacy Extensions for Address Configuration in IPv6)

### ● ユニキャストアドレス

同じアドレスをもつインターフェースが一つしかないものである。アドレスの構造は、アドレススコープごとに異なっている。

### ● エニーキャストアドレス

エニーキャストアドレスは、同じアドレスをもつインターフェースが複数あり、そのいずれかに届けられるものである。どのインターフェースに届くかは、そのときの経路による。アドレスの構造は、ユニキャストと同じである。

### ● マルチキャストアドレス

マルチキャストアドレスは、同じアドレスをもつインターフェースが複数存在し、その全てに届けられるものである。IPv6では**ブロードキャストアドレスが廃止**され、代わりにマルチキャストを使用することになっている。マルチキャストアドレスは先頭が ff00::/8 から始まり、用途に応じてアドレス構造がきめ細かく定められている。

## ● 特別な用途のために割り当てられたアドレス

次の表は、特別な用途のために割り当てられたアドレスである。

表：予約されたアドレス

アドレス	名 称	意 味
::	未指定アドレス	アドレスがないことを示す
::1	ループバックアドレス	自分自身を意味する仮想インターフェースである
インターフェース ID が全て 0 にセット	サブネットルータエニーキャストアドレス	サブネット上のルータを宛先とするエニーキャストアドレス
ff02:0:0:0:0:0:1	リンクローカル全ノードマルチキャストアドレス	近隣探索のルータ広告や近隣広告などに利用される。 IPv6 ノードが必ず参加するマルチキャストアドレスである
ff02:0:0:0:0:0:2	リンクローカル全ルータマルチキャストアドレス	近隣探索のルータ要請などに利用される。 IPv6 ルータが必ず参加するマルチキャストアドレスである
ff02:0:0:0:0:1: ff00/104	リンクローカル要請ノードマルチキャストアドレス	近隣探索の近隣要請などに利用される。 下位 24 ビットには、用途に応じ、送信元又は宛先ホストのアドレスの下位 24 ビットが埋め込まれる



RFC2526 は幾つかのエニーキャストアドレスを予約している



試験に出る

IPv4 と IPv6 に共通する機能としてマルチキャストについて、平成 24 年午前Ⅱ問 13 で出題された

1

2

3

4

### 3.9.3

## 近隣探索とアドレス自動設定機能



試験に出る

IPv6 のアドレス自動設定について、平成 29 年午前Ⅱ問 8、平成 20 年午前問 27 で出題された。ICMPv6 について平成 26 年午前Ⅱ問 9 で出題された。

IPv4 では、ARP を用いてリンク層のアドレス解決と重複アドレスの検出を実現していた。IPv6 では ARP が廃止され、代わりに ICMPv6 (Internet Control Message Protocol version 6) に規定された近隣探索の仕組みを用いてこれらを実現する。さらに、近隣探索の仕組みを用いてホストのグローバルアドレスを自動的に設定することができる。

### ● 近隣探索の機能

**近隣探索**とは、IPv6 パケットを送信するために必要な機能を実現する仕組みである。RFC4861 (Neighbor Discovery for IP version 6 (IPv6)) で規定されている。

その主な機能を次の表に示す。

表：近隣探索の機能

機能	内 容
経路設定	リンク内に存在するデフォルトルータを自動的に発見する
アドレス自動設定	グローバルユニキャストアドレスのプレフィックスを発見し、グローバルユニキャストアドレスを自動的に設定する
通信パラメータ設定	リンク MTU や最大ホップ数など、各種パラメータを発見する
リンク層のアドレス解決	リンク層のアドレス解決を行う (IPv4 の ARP に相当する)
	アドレス解決の際、そのやり取りで得た情報に基づいて近隣キャッシュを更新する (アドレス解決の要求側と応答側の双方で更新する)
	自ノードのリンク層アドレスが変更された場合、自発的に全ノードに通知する
到達不能検出	通信が途絶えて一定期間経過した近隣ノードに対し、通信できるかを確認する (上位層プロトコルが通信している場合、その状態に基づいて到達不能を検出する)
重複アドレス検出	アドレス自動設定により設定したアドレスがリンク内で重複していないかを検出する
リダイレクト	自分より適したネクストホップを通知する

## ●近隣探索で使用されるメッセージ

近隣探索の機能は、ICMPv6 の 5 種類のメッセージを用いて実現されている。

**ルータ要請メッセージとルータ広告メッセージ**を用いて、経路設定、アドレス自動設定及び通信パラメータ設定の機能が実現されている。

**近隣要請メッセージと近隣広告メッセージ**を用いて、リンク層のアドレス解決、到達不能検出及び重複アドレス検出の機能が実現されている。

**リダイレクトメッセージ**を用いて、リダイレクトの機能が実現されている。

ICMPv6 の 5 種類のメッセージを次の表に示す。

表：ルータ要請メッセージとルータ広告メッセージ

メッセージ	内容と機能	送信元→宛先
ルータ要請 Router Solicitation	リンク内のデフォルトルータを探索するため、ホストから全ルータに送信する	ホストの送信元インターフェースのアドレス→全ルータマルチキャストアドレス
ルータ広告 Router Advertisement	ルータが自分の存在を通知する。 このメッセージに基づいて、 <ul style="list-style-type: none"><li>● 経路設定（送信元アドレスをデフォルトルータとする）</li><li>● アドレス自動設定（プレフィックスを取得する）</li><li>● 通信パラメータ設定（MTUなどを取得する）</li></ul> が行われる	ルータ要請の応答： ルータの送信元インターフェースのリンクローカルアドレス→ルータ要請の送信元アドレス  定期的な通知： ルータの送信元インターフェースのリンクローカルアドレス→全ノードマルチキャストアドレス



ルータ要請メッセージでは、送信元インターフェースにアドレスが未割当ての場合、未指定アドレスになる



ルータ広告メッセージを受信したホストは、ルータ有効期間が 0 でない場合、パケットその送信元アドレスをデフォルトルータとする。また、プレフィックス、MTU などはオプションである

参考

近隣要請メッセージの送信元リンク層アドレスは、宛先が要請ノードマルチキャストアドレスの場合、必ず格納される

参考

近隣広告メッセージのターゲットリンク層アドレスは、近隣要請の送信元アドレスの宛先が要請ノードマルチキャストアドレスの場合（つまり、アドレス解決、重複アドレス検出の場合）、必ず格納される

表：近隣要請メッセージ

メッセージ	機能	内 容		送信元→宛先
		ターゲット アドレス	送信元リンク層 アドレス	
近隣要請 Neighbor Solicitation	リンク層の アドレス 解決	対象ホスト のアドレス	自ホストの リンク層 アドレス	ホストの送信元インタフェースのアドレス→ 対象ホストに応じた要請ノードマルチキャストアドレス
	到達不能 検出	対象ホスト のアドレス		ホストの送信元インタフェースのアドレス→ 対象ホストのアドレス
	重複 アドレス 検出	自ホストの アドレス	なし	未指定アドレス→ 自ホストに応じた要請ノードマルチキャストアドレス

表：近隣広告メッセージ

メッセージ	機能	内 容		送信元→宛先
		ターゲット アドレス	ターゲット リンク層 アドレス	
近隣広告 Neighbor Advertisement	リンク層の アドレス 解決	近隣要請の ターゲット アドレス	自ホストの リンク層 アドレス	ホストの送信元インタフェースのアドレス→ 近隣要請の送信元アドレス
	到達不能 検出			
	重複 アドレス 検出	近隣要請の ターゲット アドレス		ホストの送信元インタフェースのアドレス→ 全ノードマルチキャストアドレ
	自ノードの リンク層 アドレス 通知	自ホストの アドレス		

表：リダイレクトメッセージ

メッセージ	内 容		送信元→宛先
	ターゲット アドレス	ターゲット リンク層 アドレス	
リダイレクト Redirect	ルータが、自分を経由するパケットを受信した際、ホップ数がより少なくなるネクストホップ（パケットの送信元から見た第1ホップ）のリンクローカルアドレス	ターゲット アドレスの リンク層ア ドレス（知つ ていた場合）	ルータの送信元インタフェースのリンクローカルアドレス→リダイレクト通知先のアドレス

## ● アドレス自動設定機能

ノードの IP アドレスを設定する方法は、次の三つである。

- 手動設定
- ステートレスアドレス自動設定
- ステートフルアドレス自動設定

ここでは、ステートレスアドレス自動設定とステートフルアドレス自動設定について解説する。

### ・ステートレスアドレス自動設定

ルータ要請／ルータ広告のやり取りを通して、ホストのグローバルアドレスを自動設定することができる。これを**ステートレスアドレス自動設定**という。設定の手順は次のとおり。

#### ①開始

インタフェースが起動すると、ステートレスアドレス自動設定が開始される。

#### ②リンクローカルアドレスの割当て

1. インタフェース ID からリンクローカルアドレスを生成する。
2. 重複アドレス検出を行う。
3. 重複していない場合、当該アドレスを割り当てる。

#### ③グローバルアドレスの割当て

1. インタフェース ID からリンクローカルアドレスを生成する。
2. ルータ要請メッセージを送信する。
3. ルータ広告メッセージを受信する。
4. ルータ広告メッセージからプレフィックスを取り出す。  
プレフィックス及びインターフェース ID からグローバルアドレスを生成する。
5. 重複アドレス検出を行う。
6. 重複していない場合、当該アドレスを割り当てる。

1

2

3

4

### ・ステートフルアドレス自動設定

DHCPv6 サーバを用いてアドレスなどの情報を自動的に取得できる。これを**ステートフルアドレス自動設定**という。

ルータ広告メッセージの Other configuration フラグが ON になっていた場合、ステートレスアドレス自動設定を用いてアドレスとデフォルトルートを設定し、それ以外の情報 (DNS サーバの IP アドレスなど) を **DHCPv6 サーバ**から取得する。つまり、ステートレスアドレス自動設定と DHCPv6 サーバによる設定を組み合わせることができる。

なお、DNS サーバの設定は、従来どおり TCP/IP (IPv4) の手動設定、又は DHCPv4 による自動設定でも構わない。AAAA レコードの問合せにより、サーバの IPv6 アドレスを取得することができるからである。

## 3.9.4

## パケットフォーマットの簡略化



IPv6 では、エンドシステム間のパケット通信はインターネット層のプロトコルが担い、通信の信頼性確保は上位層 (TCP や UDP) のプロトコルが担う。信頼性確保の程度は、上位層プロトコルが提供する機能に委ねられる。例えば、UDP はデータグラム型通信であるため、パケット単位でチェックサムを計算する以外に信頼性は確保されない。なお、UDP のチェックサムは、IPv4 ではオプションであったが IPv6 では必須になっている。

### 関連RFC



IPv6 ヘッダは RFC2460 で規格化されている

IPv6 のヘッダは、フィールドが IPv4 より簡略化されている。

IPv6 ではチェックサムフィールドが廃止されており、ルータがチェックサムを計算する負荷が軽減されている。

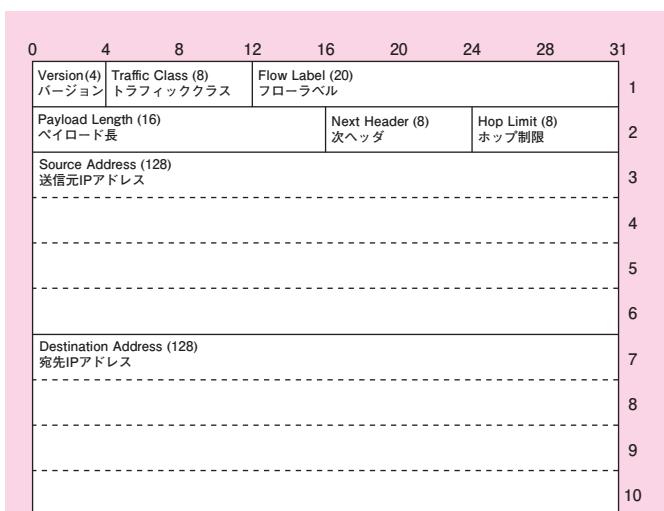
フラグメンテーションが IPv6 ヘッダから拡張ヘッダに移され、分割が必要なときだけ拡張ヘッダ（フラグメントヘッダ）が追加されるように変更されている。

ヘッダ長は、IPv4 では可変長であったが、IPv6 では固定長（40 バイト）である。そのため、ヘッダ長フィールドは廃止された。ヘッダ長が固定であることは、ルーティング処理が簡素になり高速化が図られるというメリットをもたらす。

オプションの機能は、IPv4 ではフィールドを追加することにより実現されていたが、IPv6 では必要に応じて**拡張ヘッダ**を追加することによって実現されている。拡張ヘッダは宛先ノードでのみ処理される。つまり、拡張ヘッダはルーティング処理では扱われないため（ホップバイホップオプションヘッダを除く）、ルータから見れば拡張ヘッダの存否にかかわらず IPv6 ヘッダ長は固定である。

## ● IPv6 ヘッダ

IPv6 ヘッダの構造を次に示す。



注：( )内の数字はビット数

図：IPv6 ヘッダ

それぞれの領域（フィールド）の意味を次に示す。

### ● バージョン

バージョン 6 を表す「0x06」が格納される。

### ● トラフィッククラス

リアルタイムトラフィックを転送するときに使用する。トラフィッククラスフィールドを用いることで、ほかのトラフィックとの差別化を図ることができる。パケット IPv4 のサービスタイプフィールドに該当する。

### ● フローラベル

リアルタイムトラフィックを転送するときに使用する。フローラベルフィールドを用いることでフローを識別することができ、途中経路のノードが同一フローのパケットを同じように扱うことができる。トラフィッククラスフィールドと一緒に用いることで、リアルタイムトラフィックのフローの優先制御が実現される。



試験に出る

IPv6 のヘッダについて、平成 24 年午後Ⅱ問 2 で出題された

1

2

3

4



トラフィックフィールドの定義は、RFC2474 で規格化されている

### ●ペイロード長

ペイロード長が格納される。ペイロードとは、パケットの中でヘッダに続く部分である。IPv4ではヘッダを含むパケット長が格納されるのに対し、IPv6ではペイロード長が格納される。なお、拡張ヘッダはペイロードの一部とみなされる。

### ●次ヘッダ

IPv6ヘッダに続くヘッダの種類が格納される。ペイロードがTCPやUDPなど上位層である場合、そのペイロードの種類が格納される。次ヘッダに格納される値は、IPv4のプロトコル番号と同じである。

必要に応じて拡張ヘッダが使用される場合、IPv6ヘッダと上位層の間に挿入される。つまり、ヘッダの順序は、IPv6ヘッダ、拡張ヘッダ、TCPやUDPなどの上位層、となる。

主要な次ヘッダを次に示す。なお、拡張ヘッダは「拡張ヘッダ」欄に○を記している。

表：主要な次ヘッダ

値	内 容	拡張ヘッダ
0	ホップバイホップオプションヘッダ	○
4	IPv4	
6	TCP	
17	UDP	
41	IPv6	
43	経路制御ヘッダ	○
44	フラグメントヘッダ	○
47	GRE	
50	ESP	○
51	AH	○
58	ICMPv6	
59	次ヘッダなし	
60	宛先オプションヘッダ	○
89	OSPF	

### ● ホップ制限

ルータをホップできる回数の上限が格納される。IPv4 の TTL と同じであり、ルータを経由するごとに値が一つずつ減っていく。この値が「0」になるとパケットは廃棄され、ICMPv6 パケットが送信元ノードへ送信される。

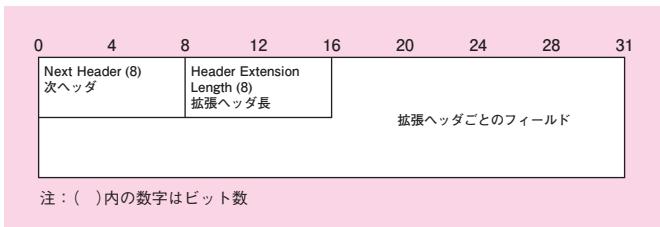
### ● アドレス

通信を行う両端ノードの IP アドレスである。

## ● IPv6 拡張ヘッダ

IPv6 パケットは、0 個以上の拡張ヘッダ (Extension Header) をもつことができる。拡張ヘッダは IPv6 ヘッダと上位層プロトコルヘッダの間に挿入される。

拡張ヘッダの構造を次に示す。

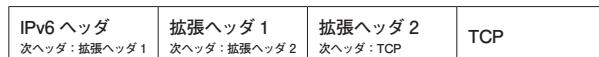


図：拡張ヘッダ

拡張ヘッダに共通している領域（フィールド）の意味を次に示す。

### ● 次ヘッダ

IPv6 ヘッダの次ヘッダフィールドと同じく、自ヘッダに後続するヘッダの種類が格納される。次の図は、拡張ヘッダが複数ある場合の例である。



### ● 拡張ヘッダ長

単位は 8 バイトである。拡張ヘッダの長さは 8 バイトの倍数になっている。このフィールドには、拡張ヘッダ長から

## 関連RFC



拡張ヘッダはRFC2460で規格化されている

## 参考

ルータはフラグメント化しないため、DFビット（フラグメント化禁止ビット）は定義されていない

8バイトを引いたサイズが格納される。例えば、拡張ヘッダ長が8バイトの場合は「0」、16バイトの場合は「1」となる。

拡張ヘッダは、次の6種類である。

- ホップバイホップオプションヘッダ (Hop-by-Hop Options Header)

経路上の全てのノードが処理する必要のあるオプションが格納される。IPv6ヘッダのすぐ後に置かれる仕様になっている。ほかの拡張ヘッダと異なり、ルータはこれを処理する必要がある。

- 経路制御ヘッダ (Routing Header)

経由する必要がある中継ノードのリストが格納される。

- フラグメントヘッダ (Fragment Header)

IPv6はIPv4と同様にフラグメンテーションの機能をもつ。しかし、IPv4とは異なり、IPv6では途中経路のルータはパケットをフラグメント化しない。IPv6は、送信元ノードがパケットをフラグメント化する仕様になっている。ルータは、転送先リンクのMTUがパケットサイズより小さいとき、送信元ホストにICMPv6エラーメッセージ (Packet Too Big) を通知する。このメッセージには、当該リンクのMTU値が格納されているので、この値に基づいて、送信元ホストはパケットをフラグメント化して再送する。フラグメント化されたパケットを再構成するのは、IPv4と同じく宛先ノードである。

このヘッダには、IPv4ヘッダと同じフィールド（フラグメントオフセット、フラグ、識別子）がある。

フラグメント化する可能性のあるノードの数は、IPv4では途中経路の複数のルータであるのに対し、IPv6では多くとも送信元ノード1つになっている。また、フラグメント化が発生する箇所は、IPv4ではMTUの小さいリンクを収容しているルータに集中する傾向があるのに対し、IPv6では全ての送信元ノードに分散されている。

- 宛先オプションヘッダ (Destination Options Header)  
宛先ノードが処理する必要のあるオプションが格納される。
- AH (Authentication Header)
- ESP (ESP Header)  
AH と ESP は IPv6 ヘッダの拡張ヘッダとして規定されているが、事実上は IPsec のセキュリティプロトコルである AH と ESP がそれぞれ格納されている。格納される位置は、5 バイト目以降である。



## 試験に出る

IPv6 で IPsec を使用できることについて、平成 27 年午前Ⅱ問 9 で出題された



「次ヘッダ」「拡張ヘッダ長」の後に 2 バイトの予約領域があり、その後に AH, ESP が格納される

1

2

3

4

