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

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。

詳説

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

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

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

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

<table>
<tr><th>スコープの種類</th><th>アドレスの構造</th></tr>
<tr><td>グローバル</td><td>グローバルユニキャストアドレスの構造
<table>
<tr><td>1 ～ 48 ビット</td><td>グローバルルーティングプレフィックス※</td></tr>
<tr><td>49 ～ 64 ビット</td><td>サブネット ID</td></tr>
<tr><td>65 ～ 128 ビット</td><td>インタフェース ID</td></tr>
</table>
※ 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。</td></tr>
<tr><td>ユニークローカル</td><td>ユニークローカルユニキャストアドレスの構造
<table>
<tr><td>1 ～ 7 ビット</td><td>fc00::/7
（現在使用できるのは fd00::/8）</td></tr>
<tr><td>8 ～ 48 ビット</td><td>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</td></tr>
<tr><td>49 ～ 64 ビット</td><td>サブネット ID</td></tr>
<tr><td>65 ～ 128 ビット</td><td>インタフェース ID</td></tr>
</table></td></tr>
<tr><td>リンクローカル</td><td>リンクローカルユニキャストアドレスの構造
<table>
<tr><td>1 ～ 10 ビット</td><td>fe80::/10</td></tr>
<tr><td>11 ～ 64 ビット</td><td>全て 0</td></tr>
<tr><td>65 ～ 128 ビット</td><td>インタフェース ID</td></tr>
</table></td></tr>
</table>

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，残りのインタフェースID（後半の64ビット）をホストのインタフェースを識別するために用いる。

●インタフェースID

インタフェースIDは，同一サブネット内でインタ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。

インタフェースIDは，次に示す三つの方法がある。

- **MACアドレスから生成（RFC4291）**
  MACアドレス（48ビット）から，Modified EUI-64と呼ばれる方法で64ビットのIDを生成する。
  グローバルIPアドレスとして使用されると，MACアドレスが不特定多数に開示されるという懸念がある。
- **Temporary Address（RFC4941）**
  定期的に変化するランダムなインタフェースIDを使用する。この方法で生成されたIPアドレスは値が変化してしまため，企業ネットワークで管理しづらいという欠点がある。
- **Stable Privacy Address（RFC7217）**
  プレフィックスやシークレットキーなどから一意なインタフェースIDを生成する。この方法で生成されたIPアドレスは，プレフィックスが固定であれば値が変化しないため，企業ネットワークで管理しやすい。

●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。

- **ユニキャストアドレス**
  ユニキャストアドレスは，同じアドレスをもつインタフェースが一つしかないものである。アドレス

関連RFC

RFC4941 Privacy Extensions for Address Configuration in IPv6
RFC7217 A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)

詳説

最近のLinux，MacOS，AndroidはRFC7217に対応している。Windows10は独自の方法でインタフェースIDを生成している（2020年9月時点）。

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。

詳説

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 に共通する機能である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

● 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フェースである
インタフェース 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
ff02:0:0:0:0:0:0:1	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
ff02:0:0:0:0:0:0:2	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

3.9.3 近隣探索とアドレス自動設定機能

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。

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

●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
通信パラメタ設定	リンクMTUや最大ホップ数など，各種パラメタを発見する
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， ● 経路設定（送信元アドレスをデフォルトルータとする） ● アドレス自動設定（プレフィックス，DNS サーバ（RDNSS 対応の場合）を取得する） ● 通信パラメタ設定（MTU などを取得する） が行われる	ルータ要請の応答： 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→ 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

詳説

ルータ要請メッセージでは，送信元インタ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

詳説

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，DNS サーバ，MTU などはオプションである

表：近隣要請メッセージ

メッセージ	内容			送信元→宛先
	機能	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

詳説

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

表：近隣広告メッセージ

メッセージ	内容			送信元→宛先
	機能	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ス
	自ノードのリンク層アドレス通知	自ホストのアドレス		

詳説

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：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（知っていた場合）	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。

詳説

RA（Router Advertisement；ルータ広告）メッセージから，グローバルIPアドレスのプレフィックス，デフォルトゲートウェイ，MTUなどが通知される。
さらに，RDNNSに対応していれば，RAメッセージからDNSサーバのIPアドレスも通知される

・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。

・**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。

ノードに DNS サーバを設定する方法は，次の四つである。

- **手動で設定**
- **DHCPv6 で通知**
- **DHCPv4 で通知**
- **RDNSS**

DHCPv6 で通知する方法は，ステートフルアドレス自動設定で解説した方法である。DHCPv6 サーバから，IP アドレスと共に DNS サーバも通知してもらう。

DHCPv4 で通知する方法は，IPv4 と IPv6 を同時に使っていることが前提である。従来の IPv4 用 DNS サーバも，AAAA レコードを使用すれば IPv6 アドレスを取得できるので，これを利用する方法だ。

最後に挙げた RDNSS について，以下で解説する。

- **RDNSS（Recursive DNS Server）**
これは，RA（Router Advertisement：ルータ広告）メッセージを使って DNS サーバの IP アドレスを通知する方法である。この方法に従えば，ステートレスアドレス自動設定で，IP アドレス，デフォルトルート，DNS サーバが一通り設定できるというメリットがある。

関連RFC

RFC8106（IPv6 Router Advertisement Options for DNS Configuration）

3.9.4 パケットフォーマットの簡略化

詳説

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RFC8200で規格化されている

試験に出る

IIPv6のヘッダについて，平成24年午後Ⅱ問2で出題された

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。

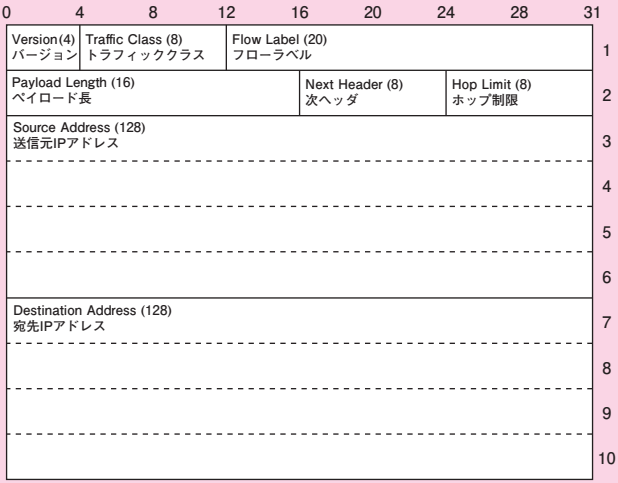
フラグメンテーションがIPv6ヘッダから拡張ヘッダに移され，分割が必要なときだけ拡張ヘッダ（フラグメントヘッダ）が追加されるように変更されている。

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。
- **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

関連RFC

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

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

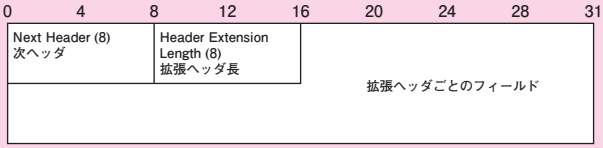
減っていく。この値が「0」になるとパケットは廃棄され，ICMPv6 パケットが送信元ノードへ送信される。

- **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。

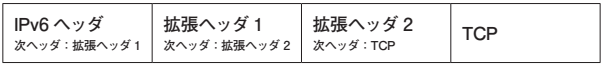
拡張ヘッダの構造を次に示す。



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 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。

関連RFC

拡張ヘッダは RFC8200 で規格化されている

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。

詳説

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

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

- 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 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。

「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