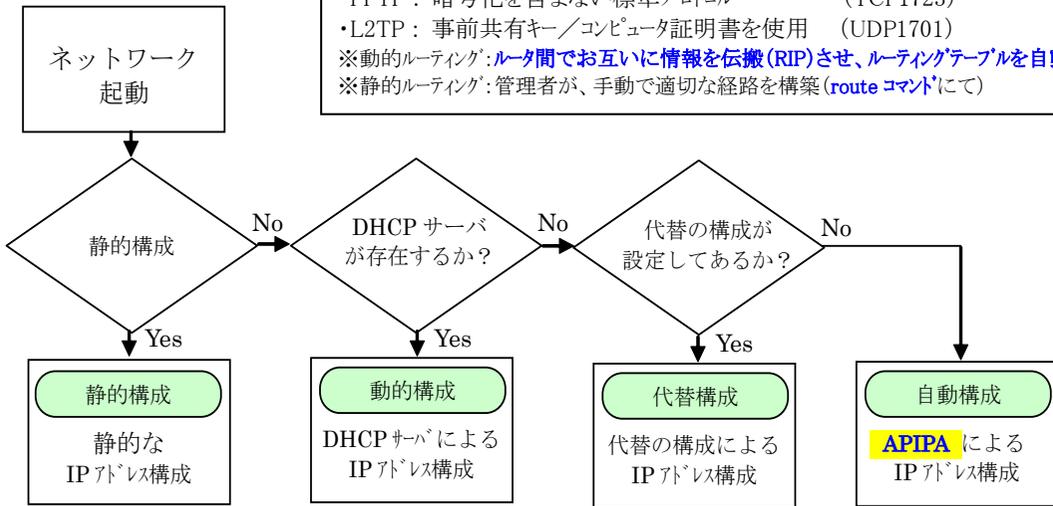


	IPv4 (ホストアドレス)	IPv6 (ネットワークレフィックス)
IP の表記例	192.168.0.1	1abe:21a0:b5aa:501d:2288a:1dd0:0001:10ee ★あるセクションが0で始まる場合、その0は省略可能 ★0が連続するところは、::で省略可能(ただし1カ所のみ)
アドレス形式	ユニキャスト / ブロードキャスト / マルチキャスト	ユニキャスト / マルチキャスト / エニキャスト 1546
ループバックアドレス (自分自身に送信)	127.0.0.1	0:0:0:0:0:0:0:1 (又は、::1)
未構成アドレス	0.0.0.0	0:0:0:0:0:0:0:0 (又は、::)
ブロードキャストアドレス	すべてのビットが1 (255)	
グローバルアドレス	世界中に 126 個存在し、それぞれに 16,777,214 台のコンピュータが接続可能 クラス A 1~126.x.x.x/8 (先頭1ビットが0) 世界中に 16,382 個存在し、それぞれに 65,534 台のコンピュータが接続可能 クラス B 128~191.x.x.x/16 (先頭2ビットが10) 世界中に 2,097,150 個存在し、それぞれに 254 台のコンピュータが接続可能 クラス C 192~223.x.x.x/24 (先頭3ビットが110) <small>クラスDは、IP マルチキャスト専用 クラスEは、実験用</small>	2001: から始まる (sTLA アドレス) sTLA は、 APNIC から直接取得することになっており、基本的に APNIC 会員でなければならない。ただし、小規模な ISP やエンドユーザは sTLA を持った ISP からアドレスを割り当ててもらえばよい。また、JPNIC では取得手続きの取り次ぎを行っており、JPNIC の指定事業者であれば JPNIC を介して sTLA の取得が可能である。
非グローバルアドレス (ローカルアドレス)	リンクローカルアドレス (APIPA 自動構成) 169.254.x.x /16 同一セグメント内通信可 プライベートアドレス 10.0.0.0~10.255.255.255/8 (クラス A) 172.16.0.0~172.31.255.255/16 (クラス B) 192.168.0.0~192.168.255.255/24 (クラス C)	リンクローカルアドレス (APIPA 自動構成) fe80::xxx/64 (xxx は、ランダムな 16 進数) 同一セグメント内通信可 グローバルユニークローカルアドレス fc00:: /8 fd00:: /8

IP アドレス構成の流れ



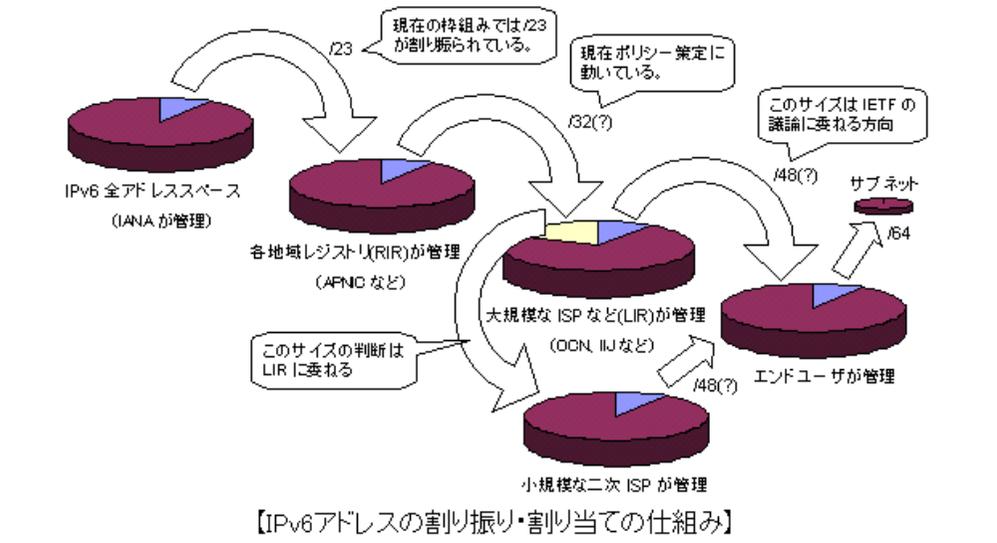
例) 192.168.0.x/24

例) **169.254.x.x/16**
(リンクローカルアドレス)

【ルーティングプロトコル】

- **SSTP** : Secure Socket トンネリングプロトコル (**TCP443**)
- PPTP : 暗号化を含まない標準プロトコル (TCP1723)
- L2TP : 事前共有キー/コンピュータ証明書を使用 (UDP1701)

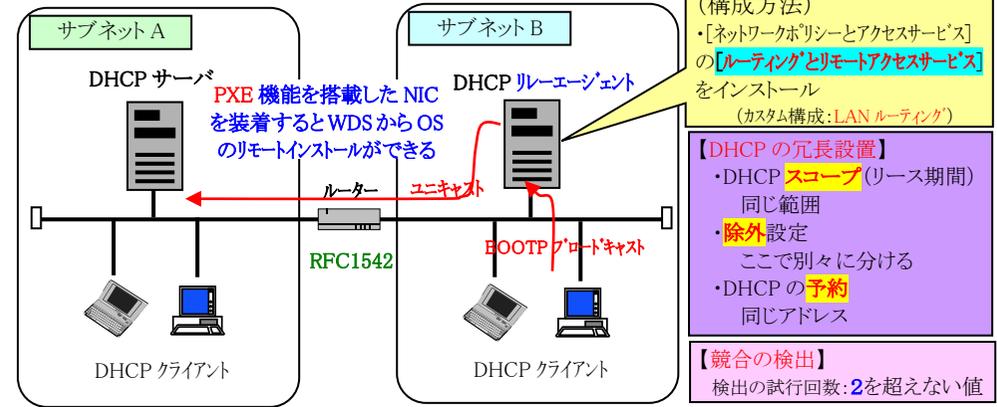
※動的ルーティング: ルータ間でお互いに情報を伝搬 (RIP) させ、ルーティングテーブルを自動構築
※静的ルーティング: 管理者が、手動で適切な経路を構築 (route コマンドにて)



【IPv6アドレスの割り振り・割り当ての仕組み】

Enterprise Admins 権限で DHCP コンソールから DHCP サーバサービスを承認する。 / アクティブ化。

- ※DHCP サーバの認証: Active Directory で承認しないとサービスは起動されない
- ※DHCP データベースのコンパクト化: **jetpack.exe** を実行する
- ※DHCP による IP の重複を防ぐ: **競合検出**の試行 (試行回数: **2** を超えない値を設定)



(構成方法)
• [ネットワークポリシーとアクセスサービス] の **ルーティングとリモートアクセスサービス** をインストール
(カスタム構成: LAN ルーティング)

【DHCP の冗長設置】

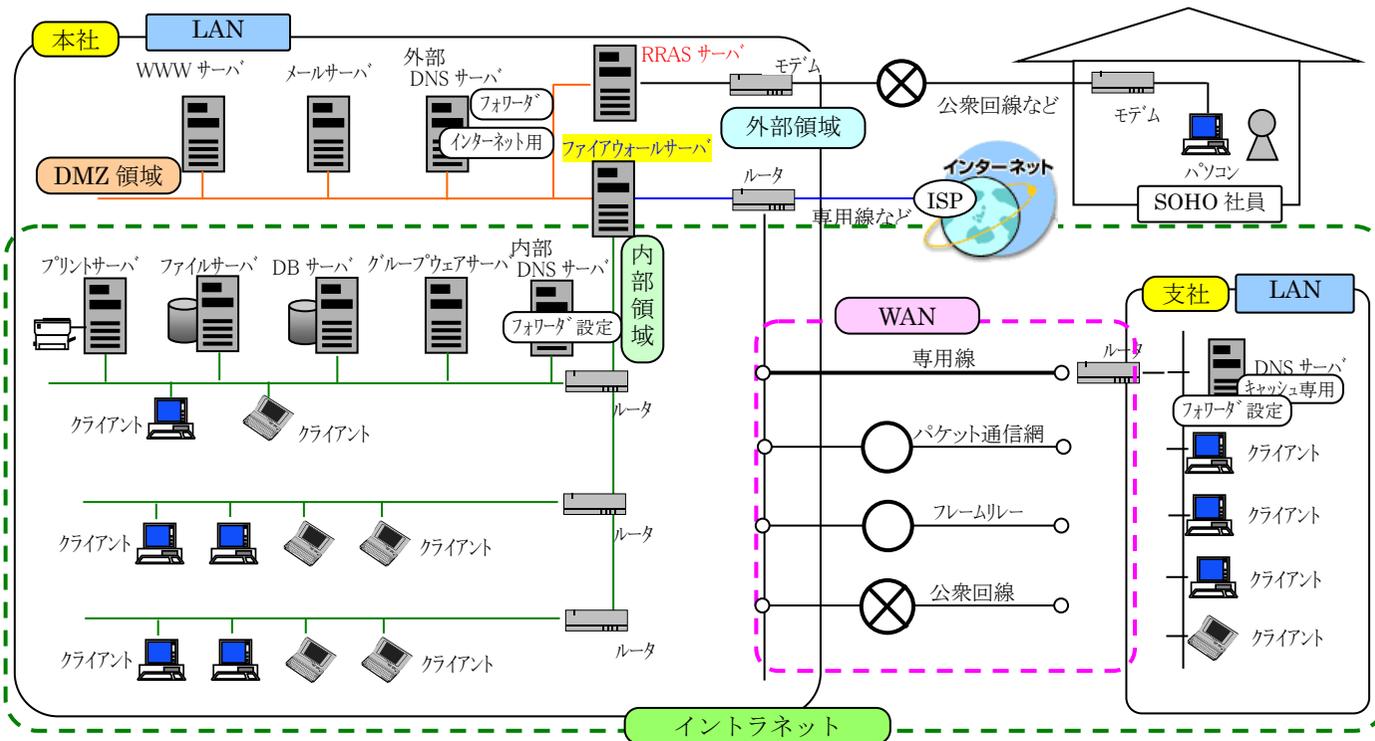
- DHCP **スコープ** (リース期間) 同一範囲
- **除外設定** ここで別々に分ける
- DHCP の **予約** 同一アドレス

【競合の検出】
検出の試行回数: **2** を超えない値

- 第1案: 各々のサブネットに、各々 DHCP サーバを設置する。
- 第2案: DHCP サーバを1台設置し、サブネット間のルータを **RFC1542 準拠** にすると、DHCP の **BOOTP ブロードキャスト** が別のサブネットにも通過できるようになる。
- 第3案: 1つのサブネットに DHCP サーバを1台設置し、他のサブネットには、DHCP の **リレーエージェント** (コンピュータ又はルータ) を置いて、**ユニキャスト** で通信させる。
(この場合は、サブネット間のルータは **RFC1542 準拠** でなくてもよい。)

【DHCP オプション】

- 003 ルータ、•006 DNS サーバ、•015 DNS ドメイン名、•044 WINS/NBNS サーバ、•046 WINS/NBT ノードタイプ



WANの種類	内容
専用線	TCP/IP
パケット交換	遅い/PADでパケットに変換して通信/X.25
フレームリレー	早い/PVC機能/HDLC/CIR/FRAD
ATM	非同期転送モード/53バイトのブロック単位での転送
ADSLなど	上りと下りの速度が非対称
公衆回線	ISDN(B,D,Hチャネルなど)

IPSec

Windows2008では、IPSecの構成がWindowsファイアウォールと統合IPパケットを暗号化及び認証を行い、セキュアな通信を提供する。通信には、「サーバ」又は「セキュリティで保護されたサーバ」ポリシーが必要ネゴシエーション(IKEと呼ばれるプロトコルを使って、SAを確率する)を行う(認証: Kerberos V5プロトコル/事前共有キー/証明書)

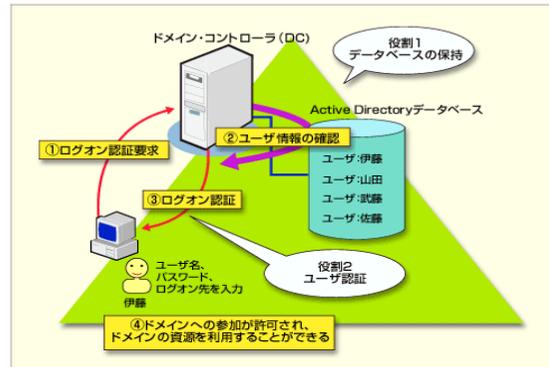
- AH(完全性の確保[改ざん防止]と送信元の認証[なりすまし防止])
- ESP(上記に、機密性の確保[暗号化]を追加したもの)

IPSecポリシー

- クライアント: 応答のみ(自分からIPSec通信を要求しない)(相手からIPSecを要求されると既定の応答規則を使用してIPSec通信を行う)
- サーバ: セキュリティが必要(常に相手にIPSec通信を要求)(通信相手が応じなければ、IPSecを使用しない通常の通信を行う)
- セキュリティで保護されたサーバ: セキュリティが必要(常に相手にIPSec通信を要求)(通信相手が応じなければ、接続を拒否して通信を行わない)

Windows Server 2008/Windows Vistaにおける名前解決

- 1) **ホスト名解決** (TCP/IPでの名前解決手段)(ドメイン毎管理)
 - HOSTS/DNSによる名前解決
 - ①静的解決:(DNSより優先) HOSTSファイルにリスト作成 (DNSリゾルバキャッシュ)
 - ②動的解決:(コンピュータ数の増加への自動化、分散管理) DNSサーバが動的にリストを作成可
 - 2) **GlobalNamesゾーン**による名前解決(単一ラベル) Windows2008以上
 - 3) **LLMNR**による名前解決(IPv6での新しいプロトコル:同一サブネット内)
 - マルチキャストによる名前解決(UDPポート:5355) WindowsXPは、ダメ
 - 4) **NetBIOS名解決** (NetBEUIプロトコル用の名前解決手段)
 - LMHOSTS/WINS/ブロードキャストによる名前解決
 - ①NetBIOS名キャッシュ:一度名前解決を行ったときの情報
 - ②動的解決:(セグメントを超えるため)(Pノード) WINSサーバが動的にリストを作成可
 - ③ブロードキャスト:(ローカルネットワーク上なら応答)
 - ④静的解決:(Bノード) LMHOSTSファイルにリスト作成 (NetBIOSキャッシュ)
- Windows2008では、**Hノード**(先にPノード、次にBノード)が規定値
Windows2003では、**Mノード**(先にBノード、次にPノード)が規定値



ドメインコントローラ(DC)の役割
ドメインコントローラは、ユーザー情報をActive Directoryデータベースに格納し、ログオン認証要求があれば、ユーザー名やパスワードなどの情報がデータベース内の情報と一致しているかどうかを調べるとして認証作業を行い、それに基づきドメインへの参加を許可する。

FQDN(完全修飾ドメイン名:ホスト名.ドメイン名)
フルコンピュータ名

	ポリシーの割り当てなし	クライアント	サーバ	セキュリティで保護されたサーバ
ポリシーの割り当てなし	IPSecなし	IPSecなし	IPSecなし	通信不能
クライアント	IPSecなし	IPSecなし	IPSec可	IPSec可
サーバ	IPSecなし	IPSec可	IPSec可	IPSec可
セキュリティで保護されたサーバ	通信不能	IPSec可	IPSec可	IPSec可