第８章 IPv6

8.1 IPv4 の問題点

現在使用されている TCP/IP は，既に 40 年近く使用されており，昨今のネットワーク事情には即さない面もある。特に現在の IP，つまり IPv4（IP Version 4）には下記のような欠点が存在する。

- **IP アドレスの枯渇（32bit,約 43 億個）**
- **経路情報の複雑化**
- **複雑な設定**
- **貧弱なセキュリティ機能**
- **QoS 機能の欠如**

これらの問題の解決のため，IP の次期バージョンとして **IPv6（IP Version 6）** が策定され，現在 IPv4 から IPv6 への移行作業が進められている（ちなみに IPv5 は実験用のプロトコルである)。

IPv6 では IPv4 の問題への対応として，以下の解決策が採られている。

- **IP アドレスの枯渇　→　アドレスの拡張（128bit）**
- **経路情報の複雑化　→　管理の階層化による経路集約**
- **複雑な設定　　→　Plug and Play 機能の搭載**
- **貧弱なセキュリティ機能 → IPsec の標準搭載（IPv4 ではオプション）**
- **QoS 機能の欠如　　→　パケット種別に対する QoS 制御の搭載**

8.2 IPv6 での IP アドレス

8.2.1 IPv6 のアドレスの表記と構造

IPv4 の IP アドレスは 32bit であったが，IPv6 での IP アドレスは 128bit にまで拡張されている。従って，IPv6 では利用可能なアドレス数が単純計算で 2^128 ≒ 3.4x10^38 程あり，膨大なアドレス空間が利用できることになる。

IPv6 のアドレス表記では，16bit ずつ ：(コロン)で区切って 16 進で表す。

例）7b2d:4359:0102:0304:0506:0708:0900:6300

ただし，途中の連続する 0000 は，一箇所だけではあるが **::** で省略可能である（推奨は一番左側の箇所)。また,： で区切られた箇所の先頭部分の 0 も省略可能である(図 8.1)。

0000:0000:0000:0000:0123:4567:8900:0987 → ::0123:4567:8900:0987
→ ::123:4567:8900:987
0000:0000:**0100**:0000:0123:4567:8900:0987 → ::100:0:123:4567:8900:987
または → 0:0:100::123:4567:8900:987

図 8.1 IPv6 での IP アドレスの省略方法

Pv6 の IP アドレスの内部を大まかに分解すれば，**サブネットプレフィックス**と**インターフェイス ID** に分けられる（図 8.2)。多くの場合，サブネットプレフィックスは 64bit（0～63bit）であり，インターフェイス ID も 64bit（64～127bit）の値が使用される。サブネットプレフィックスは IPv4 と同様にサブネット化（ネットワークを再分割）することが可能で，その場合は CIDR のプレフィックス表記を用いてサブネット化を行う。

サブネットプレフィックス （通常は 0～63bit）	インターフェイス ID （通常は 64～127bit）

図 8.2 IPv6 アドレスの大まかな構造

8.2.2 IPv6 のアドレスの割り当て

IPv6 では次の 3 つの通信モードをサポートしている。

1）**ユニキャスト　　1 対 1 通信。IPv4 のユニキャストに同じ。**

2）**マルチキャスト　1 対多通信。IPv4 のブロードキャストとマルチキャストに相当。**

3）**エニーキャスト　1 対（特定グループ内の）1 通信。特定グループ内の最もネットワーク的に近いマシンが応答し，通信を行う。**

IPv6 では，ブロードキャスト通信はマルチキャスト通信の一部と見なされているため，両者を統合してマルチキャスト通信と呼ぶ。

また，**エニーキャスト通信は** IPv4 には存在しない通信モードで，特定グループのマシン群（通常は特定のサーバプロセスが作動しているマシン群）の内の何れか一台と通信を行うモードである。

ユニキャスト通信で使用される IPv6 のユニキャストアドレスは，アドレスの有効範囲（**スコープ**）によって，さらに 3 種類に分類される。即ち，**リンクローカルユニキャストアドレス**，**ユニークローカルユニキャストアドレス**，**グローバルユニキャストアドレス**である。なお，IPv4 のプライベートアドレスに相当する**サイトローカルユニキャストアドレス**は，その取り扱いの難しさから RFC3879 により廃止された。

リンクローカルユニキャストアドレスは**ローカルリンク**内で有効なユニキャスト用アドレスである。**ローカルリンク**とはブロードキャストの届く範囲を示し，いわゆる（OSI 参照モデルの第 3 層の）ネットワークと同義語である。

ユニークローカルユニキャストアドレスは廃止の決まった**サイトローカルアドレス**に代わって定義されたアドレスである。これもプライベートネットワークを形成するためのアドレスであるが，サイトローカルユニキャストアドレスと違い，二つプライベートネットワークを接続してもアドレスが重複しないようになっている。

グローバルユニキャストアドレスは IPv4 のグローバルアドレスと同様に，インターネット全体に有効なアドレスである。

図 8.3 に IPv6 の IP アドレスのプレフィックスによる分類とその用途を，図 8.4 にアド

レスの有効範（スコープ）における IP アドレスの構造を示す。

プレフィックス	用　　途
::/8, ::1/8	未指定，ローカルループバック
2000::/3	グローバルユニキャストアドレス
2001::/16 ～ 2c00::/16	IPv6 インターネット用グローバルユニキャストアドレス（IANA より実際に配布が行われているプレフィックス）（2021 7/8）
fc00::/7	ユニークローカルユニキャストアドレス（いわゆるプライベート IP）
fe80::/10	リンクローカルユニキャストアドレス
fec0::/10	サイトローカルユニキャストアドレス（廃止）
ff00::/8	マルチキャストアドレス
ff02::1/128	リンクローカルの全てのノードへのマルチキャストアドレス
ff02::2/128	リンクローカルの全てのルータへのマルチキャストアドレス

図 8.3 IPv6 アドレスの分類とその用途

[1] グローバルユニキャストアドレス

bit	0 47	48 63	64 127
	グローバルルーティング プレフィックス	サブネット ID	インターフェイス ID

[2] ユニークローカルユニキャストアドレス

bit	0 6	7	8 47	48 63	64 127
	1111 110	0	グローバル ID	サブネット ID	インターフェイス ID

[3] リンクローカルユニキャストアドレス

bit	0 9	10 63	64 127
	1111 1110 10	00000000000……0000000000	インターフェイス ID

図 8.4 各スコープにおける IPv6 アドレスの構造

また IPv6 で使用される特殊な IP アドレスとして以下の様なものがある。

- **未指定アドレス**

  自分のアドレスが決まっていないときに使用される特殊アドレスで 0:0:0:0:0:0:0:0, つまり **::** が使用される。

- **ループバックアドレス**

  IPv4 での 127.0.0.1 に相当するアドレスで，IPv6 では **::1** が使用される。

- **IPv4 互換アドレス（廃止）**

  IPv4 ネットワーク（IPv6 用のルータが存在しないネットワーク）上で IPv6 パケットをトンネリングするときに使用するアドレスである（トンネリングは両端の IPv6 対応ルータで自動的に行われる）。プレフィックス長は 96bit で，ルーティングアドレスはプレフィックス部のビットを全て 0 にした **::/96** である。ただし，ノード部には IPv4 アドレスの表記が用いられる。　例）**::202.26.155.16**

  しかしながら現在では IPv6 の自動トンネルが廃止されたため，このアドレス表記も廃止となった。

・ IPv4 マップ（射影）アドレス

マップアドレスは IPv6 のノードが，IPv6 をサポートしない IPv4 のノードと通信を行う場合に用いるアドレスである。プレフィックス長は 96bit で，ルーティングアドレスは ::ffff:0:0/96 である。ただし，ノードに部は互換アドレスと同様に IPv4 アドレスの表記が用いられる。　例）::ffff:192.168.1.1

しかしながらこの IPv4 マップアドレスも現在ではあまり使用されることはない。現在のネットワーク環境では，各ノードはほぼ IPv4/IPv6 の両方に対応しているからである（デュアルスタック）。IPv4/IPv6 のデュアルスタック搭載の場合，通常は最初に IPv6 での接続を試み，それに失敗した場合は IPv4 で接続を試みるようになっている（注：そのため IPv4/IPv6 のデュアルスタック環境から IPv4 しかない環境に接続する場合は，最初の接続時に時間が掛かる場合がある）。

[1] ローカルループバックアドレス

Bit	0 ・・・ 111	112 127
	0000000000000000・・・・・・・・・・・・・・・・・・・・・・・・・0000000000000000000000000000000	0001

[2] IPv4 互換アドレス（廃止）

Bit	0 ・・・ 79	80 95	96 127
	000000000000・・・・・・・・・・・・・・・・・・・・・・0000000000000000000	0000	IPv4 アドレス

[3] IPv4 マップアドレス

bit	0 ・・・ 79	80 95	96 127
	000000000000・・・・・・・・・・・・・・・・・・・・・・0000000000000000000	ffff	IPv4 アドレス

図 8.5 IPv6 における特殊なアドレスの構造

8.3 ルーティングアドレスの集約

グローバルユニキャストアドレスは**集約可能グローバルユニキャストアドレス**とも呼ばれ，上位 48bit の**グローバルルーティングプレフィックス**によりインターネット上でのルーティング情報を集約させることが可能である（図 8.6）。

グローバルルーティングプレフィックスにおけるルーティング情報の集約は，アドレス管理の階層構造化により実現される。管理の階層構造は，IPv4 と同様に通常，IANA（ICANN）→ RIR → NIR → LIR/ISP → EU（End User）の順を辿る。しかし，IPv4 では初期の頃はこの管理階層は存在せず，エンドユーザやサイトにフラットな空間の IP アドレスを多数割り当てたため，現在でも集約困難な状況が続いている（例えば連続する C クラスのアドレスが違う ISP を通してエンドユーザに割り当てられた）。

IPv6 において，IANA（ICANN）が現在実際に割り振りを行っているのは，グローバルユニキャストアドレスに指定されているアドレス空間（2000::/3）中の 2001::/16～2c00::/16（2021 7/8）のサブ空間である。IANA はこの中からプレフィックス /23 のアドレス空間を各 RIR に割り当てている。RIR は自分達に割り振られたアドレス空間のサブ空間を，さらに

下位組織である NIR や ISP に割り当てる（割り当てるプレフィックスは，割り当て対象のレジストリにより変化する）。

最終的には各エンドユーザ（サイト）にはプレフィックス /48 のアドレス空間が割り当てられる。各エンドユーザ（サイト）が割り当てられた /48 のアドレスでは，16bit のサブネット ID を指定することができるので，自組織内に最大 2^16 個のサブネットを作成することが可能である（図 8.6）。

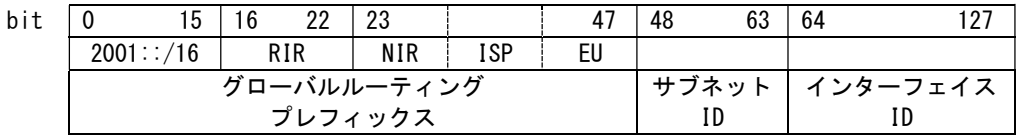

図 8.6 グローバルユニキャストアドレスの構造

8.4 Plug and Play

一般のエンドユーザにとって，ネットワークの設定は決して容易なものではない。IPv4 でも DHCP などにより設定の簡略化を図って来たが，IPv6 では DHCP などのサーバが無い状況でも自らの IP アドレスを自動生成できる Plug and Play の機能を持っている。

IPv6 アドレスのノード部に相当するインターフェイス ID は，NIC の MAC アドレスから決定する。MAC アドレスは世界的に一意である筈なので，MAC アドレスを使用してインターフェイス ID を生成すれば，これもまた世界的に一意となる筈である（ただし手動で設定したインターフェイス ID とは重複する可能性がある）。

MAC アドレスは 48bit であり，インターフェイス ID は 64bit であるので，MAC アドレスからインターフェイス ID への変換は Modified EUI-64 と呼ばれる手法により行われる。Modified EUI-64 では，先ず MAC アドレスを 24bit ずつ 2 つに分け，間に fffe を挿入する（ffff を挿入するとブロードキャスト用のインターフェイス ID が生成される可能性があるため）。さらにアドレスの先頭 7bit 目（Universal/Local bit）を反転させる（図 4.46）。これにより 64bit のインターフェイス ID が完成する。

通常では Universal/Local bit は，その MAC アドレスが世界的に一意であるかどうかを保障するフラグであり、0 が Universal を示し、1 が Local を示す。しかし Modified EUI-64 では 0 が Local，1 が Universal と変更されており，手動（Local）で インターフェイス ID を設定する場合に余計な Bit が立たないようになっている（Universal/Local bit の定義を逆にしているので “Modified” が付加されている）.

例えば図 4.46 では，ノードの MAC アドレス 01:AA:12:23:98:0E がインターフェイス ID 3aa:12ff:fe23:980e に変換されている。

次にノードは，自分がローカルリンクに接続しているとして，サブネットプレフィックス fe80::/64 を用いてリンクローカルユニキャストアドレスを生成する。さらに，念の為生成したアドレスがローカルリンク内で使用されていないことを確認する（アドレスが重

複した場合は自動生成を中止する)。

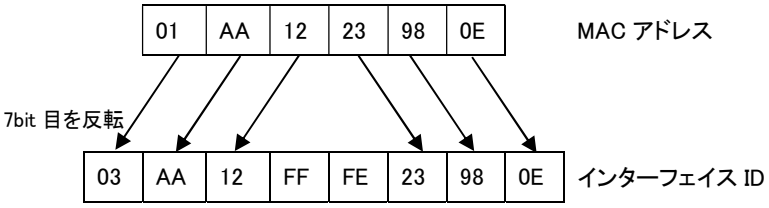

図 8.7 EUI-64

リンクローカルユニキャストアドレスの生成に成功した場合は，そのアドレスを使用した **NDP**（近隣探査：Neighbor Discovery Protocol）によりルータを探索し，グローバルユニキャストアドレスを生成する。具体的にはノードからルータへ，**ルータ要請**（Router Solicitation: **RS**）がマルチキャストで送信され，ルータがネットワークのプレフィックス情報などを**ルータ広告**（Router Advertisement: **RA**）として返信することにより設定が行われる（インターフェイス ID は EUI-64 で生成したものがそのまま使用される)。NDP を使用するとその他にも様々な情報を収集することが可能となる。

もしルータが返信を返さなければ，グローバルユニキャストアドレスの生成は中止される。

以上をまとめると，IPv6 では，Plug and Play 機能により，以下の手順で IP アドレスの自動生成が行われる。

1) **MAC アドレスから EUI-64 を用いて，インターフェイス ID を生成する**
2) リンクローカルのプレフィックス **fe80::/64** と**インターフェイス ID** を用いて，リンクローカルユニキャストアドレスを生成する
3) **生成したアドレスが他のノードのアドレスと重複しないか確認する**
4) **NDP によりルータを検索し，その情報から**グローバルユニキャストアドレスを生成する

当然サーバなどで IP アドレスが変化するのが好ましくない場合は，グローバルユニキャストアドレスを手動で決定することも可能である。

8.5 一時 IPv6 アドレスとゾーンインデックス

前節でみたように IPv6 では，**Modified** EUI-64 により MAC アドレスを用いてクライアント用のインターフェイス ID を自動的に決定することができる（グローバルユニキャストアドレスも同じインターフェイス ID を使用する)。このことは，通信相手に自分のノードの MAC アドレスを知られてしまう危険性があることを意味する。MAC アドレスは（基本的には）世界的に一意であるので，場合によってはユーザの匿名性が失われることにもなり兼ねない。実際に Apple や Google などでは無線 LAN の AP の MAC アドレス情報を収集してデータベース化し，その情報をユーザの位置情報決定の精度向上などに利用している。

このため実は現在では **Modified** EUI-64 の使用は非推奨となっており，近年の MS

Windows のデフォルト状態では乱数によりインターフェイス ID を生成している（設定コマンドによって **Modified** EUI-64 を使用するようにもできる)。

さらに **Plug and Play** で生成したグローバルユニキャストアドレスを用いずに，一時的に別のグローバルユニキャストアドレスを生成して，実際の通信ではそちらを使用することが可能である。この一時的に生成・使用されるアドレスを**一時 IPv6 アドレス（匿名アドレス）**と呼び，一定時間経過後またはノードの再起動時に更新される。IPv6 では一つのインターフェイスに複数のアドレスを持つことができるため，このようなことが可能となる。

図 8.8 に MS Windows での IPv6 アドレス設定の状況例を示す(ipconfig コマンド使用)。

```
C:¥Users¥guest> ipconfig /all
.....
イーサネット アダプター ローカル エリア接続:
   .....
   説明. . . . . : Intel(R) Ethernet Connection (2) I218-V
   物理アドレス. . . . . : D0-50-99-38-DA-B6
   DHCP 有効 . . . . . : はい
   自動構成有効. . . . . : はい
   IPv6 アドレス . . . . . : 2400:4051:8164:f00:f1c0:c16b:ccab:2888(優先)
   一時 IPv6 アドレス. . . . . : 2400:4051:8164:f00:10b8:68ee:2254:aed(使用されていません)
   一時 IPv6 アドレス. . . . . : 2400:4051:8164:f00:9cd8:b70d:50c1:6665(優先)
   リンクローカル IPv6 アドレス. . : fe80::f1c0:c16b:ccab:2888%4(優先)
   IPv4 アドレス . . . . . : 192.168.27.230(優先)
   サブネット マスク . . . . . : 255.255.255.0
   リース取得. . . . . : 2021 年 3 月 1 日 21:10:09
   リースの有効期限. . . . . : 2021 年 3 月 6 日 5:10:15
   デフォルト ゲートウェイ . . . . : fe80::225:36ff:fe8a:c89c%4
                                  192.168.27.127
.....
```

図 8.8 MS Windows での IPv6 アドレスの設定状況例

図 8.8 の例ではリンクローカル IPv6 アドレスとデフォルトゲートウェイのアドレスの最後に **%4** の表示があるが，これは**ゾーンインデックス（ゾーン ID）**と呼ばれている。複数のネットワークインターフェイス（NIC）を持つノードの場合，リンクローカルアドレスでは全て fe80:: のプレフィックスを持つアドレスになってしまうため，複数のネットワークインターフェイス（NIC）間でルーティングができなくなってしまう。そこで IPv6 アドレスの最後に **%数字** を付加してインターフェイスを識別している。

ゾーンインデックスはノード自身が識別できればそれで良いので，**%** 以降の書式に特に決まりはなく OS に依存する。**%数字** は MS Windows での書式であり（数字はインターフェイス番号),Linux などでは **%インターフェイス名**(例:**%eth0**)となる。なお **%** は URI(Uniform Resource Identifier）または URL で IPv6 アドレスを指定する場合に，不都合を回避するための **URL エンコード**用である。

8.6 IPsec（IP security)

IPsec は IP レベルでパケットの暗号化と認証を行う機能である。IPv4 では搭載はオプシ

ョンであるが，IPv6 では必須機能となっている（必ず搭載しなければならないが，アプリケーションがそれを使用するかどうかは任意)。IPsec ではパケットに**AH ヘッダ**と**ESP ヘッダ**を追加することにより，暗号化と認証の機能を追加する。また，ここで使用される暗号化鍵は**IKE**（Internet Key Exchange）プロトコルによって End-to-End で交換される。

なお，IPsec には End-to-End の通信を行うための**トランスポートモード**（図 8.9）と IPsec-VPN を行うための**トンネルモード**がある（図 8.10)。

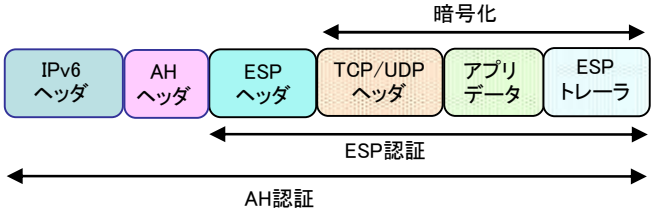

図 8.9 IPsec のトランスポートモード

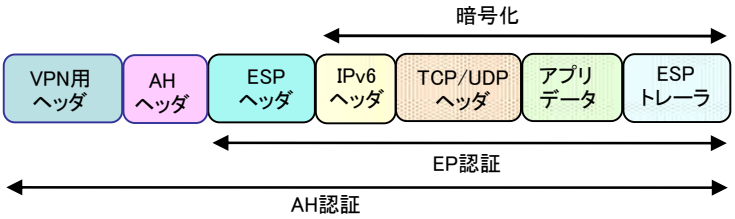

図 8.10 IPsec のトンネルモード

AH（認証ヘッダ：Authentication Header）では，パケット全体の認証や改ざんの検出を行うことが可能である。認証および改ざん検出を行うための認証コードは，**IKE** による秘密鍵とハッシュ関数（MD5, SHA1 または SHA2）により生成される。

ESP（暗号ペイロード：Encapsulating Security Payload）では，**IKE** による秘密鍵を用いて DES，3DES または AES での暗号化をサポートする。また認証トレーラ機能を使用するとパケットデータ（セグメント）の認証および改ざん検出を行うことが可能である。なお，AH ではパケット全体の認証が可能であるが，ESP ではデータ（セグメント）部分のみの認証であることに注意されたい。ただし ESP の認証で十分であると考えられる場合には AH を省略することもできる。

一方実際問題として，AH の MD5/SHA1 や ESP の DES は既に陳腐化しており，現在では SHA2 や AES を使用する方が賢明である。また IPv6 では IPsec は搭載必須となっているが，アプリケーションがその機能を使用するかどうかは任意であり，大抵の場合はそのオーバヘッドを嫌って使用されない事の方が多いようである。唯一 IPsec-VPN（トンネルモード）での使用が目立つ程度である。

8.7 QoS (Quality of Service)

IPv4 には QoS 機能は存在しない。全てのパケットが同等に通信路を流れるのである。これは高速道路上で人や自転車や自家用車，スポーツカー，高速バス，トラックなどが車線の規制なしに好き勝手に通行している状況に似ている。IPv6 では QoS 機能を実現し，高速道路（ネットワーク）上にそれぞれの車種（パケット種別）に適した幅員の専用車線（帯域）を作り出すことが可能である。

IPv6 では，ヘッダ内の**「トラフィッククラス」**フィールドによりパケット転送の優先順位を決定し，ネットワークが混雑してきた場合は，優先順位の高いパケットを先行転送することができる。

また**「フローラベル」**フィールドを利用してデータ転送の帯域を確保することも可能である。データの帯域確保は経路上の全ての機器（主にルータ）に対して行わなければ意味を成さない。そのため，この資源予約用に **RSVP**（Resource reSerVation Protocol）と呼ばれるプロトコルが用意されている。

8.8 IPv6 パケットの構造

IPv6 パケットの構造を図 8.11 に示す。IPv4 のパケット（図 5.7）と比べて構造が単純になっているが，これはヘッダを**基本ヘッダ**と**拡張ヘッダ**に分け，複雑な設定を拡張ヘッダとして独立させたためである。IPv6 のヘッダでは**「次ヘッダ」**フィールドを利用して**拡張ヘッダ**を次々に続けることが可能である（図 8.12)。

また，基本ヘッダでは IPv4 のチェックサムが削除されているが，これは今日のネットワークの品質の向上により，ネットワーク層でのエラー検査は処理負荷に比べて効果が薄く，冗長的である為である（エラーが発生した場合は上位層で処理する)。

( ) 内は該当データのビット長

バージョン(4)	トラフィッククラス(8)	フローラベル(20)
ペイロード長(16)	次ヘッダ(8)	ホップリミット(8)
送信元 IP アドレス(128)		
送信先 IP アドレス(128)		
拡張ヘッダ（複数可：可変長）		
データ（セグメント：可変長）		

- バージョン：常に 6 が設定される.
- トラフィッククラス：転送の優先順位. IPv4 の TOS に相当.
- フローラベル: QoS 制御のための識別子.
- ペイロード長：データ（ペイロード）の長さ（バイト単位）
- 次ヘッダ：次の拡張ヘッダの種別. ICMP:1, TCP:6, UDP:17, AH:51, ESP:52 など.
- ホップリミット: IPv4 の TTL と同じ. 通過できるルータの最大値. ルータを通る度に -1 され, 0 になるとパケットは破棄される.
- 送信元 IP アドレス：送信元の IP アドレス.
- 送信先 IP アドレス：宛先の IP アドレス.
- 拡張ヘッダ：IPv6 基本ヘッダの拡張として, 次に続くヘッダ. 複数の拡張ヘッダを続ける事が可能.
- データ：上位層（トランスポート層）のデータ（セグメント）.

図 8.11 IPv6 パケットの構造

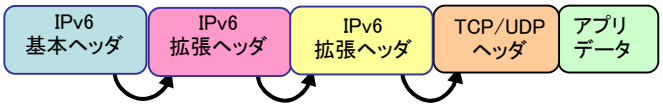

図 8.12 IPv6 パケットの基本ヘッダと拡張ヘッダ