《基礎編》第2章

特定用途向けのネットワーク

この章では，特定用途向けのネットワークとして，WAN，ストレージネットワーキング，ユニファイドコミュニケーションについて解説する。
午後試験では，本文中で動作原理や仕組みを説明しており，要素技術を理解していれば解答できるように配慮されている。前章で解説したLAN関連技術に比べて習得が難しい分野だが，過去問題の出題例を踏まえて，基本的な用語や概念を理解しておきたい。

2.1 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。

2.1.1 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。

●WAN

アクセス回線について出題された例はあるが，午後試験ではあまり出題されない分野である。

表：WAN に関する出題例

出題例	内容
平成 19 年午後 I 問 1	・FTTx（GE-PON）の多重化技術 ・GE-PON の構成 ・光ファイバの利点 ・DHCP リレー情報オプションを利用し，加入者宅と接続している L3SW のポート番号を通知する

●ストレージネットワーキング

サーバ間でストレージを共有する事例や，広域災害に備えて遠隔地のバックアップサイトにリモートバックアップを行う事例がしばしば登場する。その中で，**ストレージネットワーキング**の基礎的な知識が問われている。

新技術である**拡張イーサネット**を使った設計など，応用問題が出題されたこともあった。とはいえ，本文中に動作原理が詳しく説明されていたので，基礎知識があれば解答できるように配慮されていた。

表：SAN に関する出題例

出題例	内容
平成 24 年午後Ⅱ問 1	・FCoE でカプセル化されたフレームや，TRILL でカプセル化されたフレームの解析（本文から推論する応用問題） ・TRILL を用いたファブリックの冗長化（本文から推論する応用問題） ・ホストからストレージ間のアクセスの冗長化
平成 23 年午後Ⅱ問 1	・拡張イーサネットにおける，仮想リンクごとの優先度付きバッファ制御の仕組みについて（本文から推論する応用問題） ・FSPF を用いた複数経路制御方式 ・FC-SAN のフロー制御（クレジット方式） ・SAN の冗長化設計
平成 23 年午後Ⅱ問 2	・ファイルサーバの集約（NAS の導入）に伴う，ネットワークの再構築 ・データ移行を含む，システムの移行
平成 18 年午後Ⅱ問 1	・SAN の新規導入に伴う，ネットワークの再構築 ・データ移行を含む，システムの移行

表：リモートバックアップに関する出題例

出題例	内容
平成 22 年午後Ⅱ問 1	・重複除外機能をもつバックアップ方式
平成 20 年午後Ⅰ問 2	・リモートコピーの同期式と非同期式の比較

●ユニファイドコミュニケーション

VoIP システムの設計やインスタントメッセージを利用したシステムの設計が出題されている。その中で，**SIP** のシーケンス，**SIP サーバ**や **VoIP GW** の役割などが問われている。

表：ユニファイドコミュニケーションに関する出題例

出題例	内容
平成 26 年午後Ⅱ問 2	・内線 IP 電話網と公衆 IP 電話網の接続に使用する，VoIP GW の機能（B2BUA），動作シーケンス ・SIP メッセージに記載されたプライベート IP アドレスが NAT 装置を通過するときに発生する問題とその解決 ・通話セッションの録音という要件を実現するための設計（本文から推論する応用問題）
平成 20 年午後Ⅱ問 2	・SIP のインスタントメッセージを利用したシステム構築という要件を実現するための設計（本文から推論する応用問題） ・SIP メッセージに記載されたプライベート IP アドレスが NAT 装置を通過するときに発生する問題 ・SIP シーケンス（Via フィールド）の仕組み

（表は次ページに続く）

出題例	内容
平成 19 年午後Ⅱ問 1	・フォレンジックシステムの構築という要件を実現するための設計（本文から推論する応用問題） ・収集する音声パケットの経路 ・経路の冗長化設計
平成 18 年午後Ⅱ問 1	・通話録音システムの構築という要件を実現するための設計（本文から推論する応用問題） ・呼量及び回線数の計算 ・障害時の影響分析（通話の切断）とその対策（通話の転送）

2.1.2 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。

●ストレージネットワーキング

FC-SAN，**IP-SAN**，**拡張イーサネット**など，ストレージネットワーキングの様々な利用形態が出題されている。とはいえ，問われている内容の多くは，要素技術の基本知識である。FC-SAN，IP-SAN，LAN と SAN の統合ネットワーク，NAS のそれぞれについて，特徴を学習しておく必要がある。特に，IP-SAN の **iSCSI**，**NAS** はしっかり理解しておきたい。

ストレージネットワーキングでは，高品質，高信頼性が求められている。バッファ枯渇を防ぐためのフロー制御の仕組み，ホストとストレージ間の経路冗長化の方式などが今後と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。

拡張イーサネットは，過去 2 回（平成 24 年，23 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。もしかすると，3 回目以降は，従来のようなヒントが本文中には書かれていない可能性がある。本章で基礎知識をしっかり学習しておくとよいだろう。

リモートバックアップは，本文で仕組みが解説されているので，知識習得の優先度を下げてよいだろう。余力があれば，世の中で使用されている方式について学習しておくとよい。

●ユニファイドコミュニケーション

SIP シーケンスの知識を前提とした，設計の応用問題がよく出題されている。

SIP サーバを利用したシーケンス，**VoIP GW** を介した二つの SIP ネットワークの接続とシーケンスについて，学習しておく必要がある。

SIP は，IP 電話網だけではなく，音声と映像を同時に利用したマルチメディア，プレゼンス情報の通知など，様々な形態のコミュニケーションの呼制御を行う要素技術である。次

世代ネットワーク（NGN）でも SIP が利用されている。

今後は，通話セッション以外のコミュニケーションシステムが出題されるかもしれない。どのような事例にも対応できるよう，SIP の仕様をしっかり理解しておくことが大切である。

2.2 WAN

午後試験において，WAN サービスやアクセス回線を利用する立場から問われることはあるが，その頻度は高くない。試験対策の観点から言えば，優先度を下げてよい分野である。もっとも，午後試験の事例には，IP-VPN や広域イーサネットなどの WAN サービスを利用したネットワークがよく登場する。WAN が問われることはないとしても，事例のネットワーク構成を理解するために，WAN を利用する立場でサービスの概要を学習しておくとよい。

2.2.1 アクセス回線

WAN やインターネットへのアクセス回線として，FTTx，xDSL，ワイヤレスなどが用いられている。ここでは，過去 10 年以内の午後試験で出題例がある，**FTTH** を取り上げる。

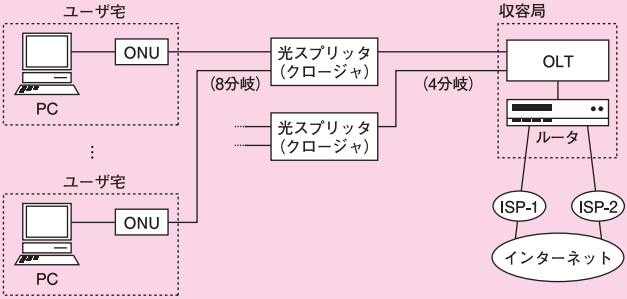
●FTTx

FTTx は，FTTH（Fiber To The Home），FTTC（Fiber To The Curb），FTTB（Fiber To The Building）などの総称で，通信事業者から各家庭（Home），街区（Curb），ビル（Building）までのアクセス回線を光ファイバで接続して，高速で広帯域な通信を行う方法である。

現在主流になりつつあるのは，IEEE802.3ah 標準の **GE-PON**（Gigabit Ethernet - Passive Optical Network）である。その接続構成例を次の図に示す（ただし，事業者によって詳細は異なる）。

試験に出る

FTTH（GE-PON）について，平成 19 年午後Ⅰ 問 1 で出題された



図：GE-PON の接続構成例

宅内の LAN と宅外の光回線を収容する装置は **ONU**（Optical Network Unit）と呼ばれ，電気信号と光信号を変換する機能をもつ。複数のユーザ宅の光回線は，電柱などに設置されたクロージャに収容される。その中に光スプリッタと呼ばれる装置があり，これが収容局からの光回線を分岐している。収容局の光回線終端装置は **OLT**（Optical Line Terminal）と呼ばれる。OLT は ONU と対になる装置で，OLT の先にインターネットが接続されている。ONU と OLT の間にある光ファイバや光スプリッタは，光信号を通すだけの「受動的」（Passive）な装置であり，**PON** という名称の由来となっている。OLT 側で，各 ONU に帯域を割り当て，信号のタイミングを調整することにより，複数の ONU を収容することができる。

2.2.2 WAN サービス

国内で利用されている WAN サービスは，**IP-VPN 網**，**広域イーサ網**などがある。IP-VPN や広域イーサネットを利用したネットワークは試験にもよく登場するが，WAN サービスそのものが問われることはあまりない。

ここでは，両サービスの一般的な特徴，通信事業者が提供する WAN サービスのプランについて，簡単に解説する。

● IP-VPN 網

IP-VPN サービスは，ネットワーク層プロトコルとして IP（Internet Protocol）を使用し，通信事業者の提供する閉域網を利用して VPN を実現するサービスである。

IP-VPN サービスの特徴を次に示す。

- **レイヤ 3 サービス**
  IP を用いて VPN を構築するサービスである。
  ネットワーク層プロトコルが IP に限定されるため，IP 以外のプロトコルを用いる場合は，カプセル化が必要になる。
- **VPN 通信**
  IP-VPN 網内は MPLS 技術を用いてパケットを転送してい

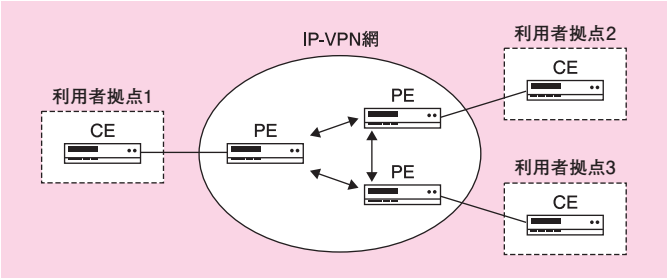
る。MPLSでは，利用者を識別する固有のVPN情報が，網に入るときにパケットに付与され，網を出るときにこれを除去する。よって，利用者はその存在を意識する必要がない。

網内では，このVPN情報に基づいて利用者ごとにルーティングテーブルが作られる。これによりVPNが実現され，専用線と同等のセキュリティが保たれる。

IP-VPN網を利用するときは，各拠点からIP-VPN網に接続する構成を採る。

利用者のネットワークに設置されるルータをCE（Customer Edge），IP-VPN網とアクセス回線の接続点に設置されるルータをPE（Provider Edge）という。CEのデフォルトゲートウェイは，対向側のPEに設定する。

IP-VPNサービスに接続している全拠点は，仮想的にフルメッシュで接続される。



図：IP-VPN網を用いたネットワーク構成の例

●広域イーサ網

広域イーサネットサービスは，通信事業者の提供するイーサネット閉域網を利用してVPNを実現するサービスである。

広域イーサネットサービスの特徴を次に示す。

- **レイヤ2サービス**
  イーサネットを用いてVPNを構築するレイヤ2（第2層）のサービスである。
  IP-VPNと異なり，ネットワーク層プトコルがIPに限定さ

用語解説

MPLS
Multi-Protocol Label Switching。IP-VPN網などLSR（Label Switching Router：MPLS対応ルータ）で構成された網では，「ラベルヘッダ」を用いてパケットを転送する。網の入口にあるルータ（PE: Provider Edge）がラベルヘッダを挿入し，出口にあるPEがこれを取り去る。ラベルヘッダは32ビットの固定長であり，このうちの20ビットが「ラベル」と呼ばれる識別子である。MPLSを利用したIP-VPN網ではラベルヘッダを二つ挿入し，網内の経路を識別するラベルと，利用者を識別するラベルを用いている

試験に出る

MPLSについて，平成24年午前Ⅱ問15，平成19年午前問27，平成18年午前問41で出題された

れることはない。

- **VPN 通信**

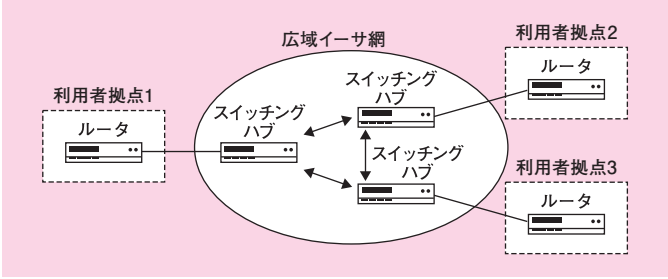
  広域イーサ網内の VLAN 技術を用いてパケットを転送している。網に入るときに独自の VLAN タグ（**拡張 VLAN タグ**）をパケットに付与し，網を出るときにこれを除去する。よって，利用者はその存在を意識する必要がない。

  網内では，拡張 VLAN タグ内の VLAN ID が，利用者を識別する固有の VPN 情報として用いられる。これに基づいて利用者ごとに VLAN が作られ，VPN が実現される。なお，この拡張 VLAN タグは，利用者が使用する IEEE802.1Q の VLAN タグより前の位置に挿入されるため，利用者側は自由に VLAN を用いることができる。

広域イーサ網を利用するときは，各拠点から広域イーサ網に接続する構成を採る。

通常，各拠点にルータを設置して，ブロードキャストドメインを分割する。このとき，各拠点のルーティング設計は利用者が行う必要がある。

通信事業者が提供する回線終端装置のインタフェースは，イーサネットになっていることが多い。それゆえ，各拠点の LAN をシームレスに接続し，一つの巨大な LAN を構築するイメージとなる。



図：広域イーサ網を用いたネットワーク構成の例

●WAN サービスのプラン

IP-VPN 網にせよ，広域イーサ網にせよ，通信事業者が閉域網のプランを提供するときは，次に示すようなメニューを提供する。

参考

試験では，広域イーサネットサービスの VPN 網のことを「広域イーサ網」と表記している。本書でもそれに倣って記述する

参考

試験では，WAN サービスのプランが問われることはない。とはいえ，帯域保証があることや，SLA が提供されていることなどを知っておくことは，試験に登場する事例を理解するのに役立つだろう。なお，ここに示したのはあくまで参考例に過ぎない。通信事業者のホームページにアクセスし，自分の目で様々なプランを確かめてみるとよいだろう

- **契約帯域**

  1Mbps ～ 10Gbps の中から，契約する通信帯域を選択できる。

- **品質**

  ギャランティード（帯域保証）型，**ベストエフォート**型など，品質保証のプランを選択できる。

  必要最小限の帯域（契約帯域よりも狭い帯域）を保証し，保証帯域から契約帯域までをベストエフォートとすることでコストを下げるプランなど，通信事業者によって市場のニーズを踏まえた様々なプランを提供している。

- **信頼性**

  アクセス回線の種類，及び，アクセス回線を二重化するか否かを選択できる。

  閉域網のバックボーンネットワークは，国内の主要な通信事業者であれば，高信頼性が確保されていると考えてよい。もちろん，必要であれば，閉域網を二重化してもよいだろう。

- **サービス**

  24 時間体制で利用者からの電話相談を受け付けたり，故障を検知したら迅速に利用者に通知したり，トラフィックレポートを定期的に報告したりするなど，充実したサポートが提供されている。

  国内の主要な通信事業者は，**SLA**（Service Level Agreement）を提供している。具体的なサービス品質の指標として，パケット往復遅延時間（RTT：Round Trip Time），故障通知時間，故障回復時間，パケット損失率などがある。

2.2.3 WAN 高速化装置

WAN 高速化装置（以下，WAS と称する）は，WAN 回線経由の拠点間ファイル転送を高速化する機能をもつ装置である。

WAS は，WAN 回線を挟んだ 2 拠点のそれぞれ（WAN 回線の両端）に設置する。詳しい説明は後述するが，WAS 独自のデータ一括転送を，回線両端の WAS 間で行う。この仕組みにより，

WASは，回線を経由するファイル転送の高速化を実現している。

WASを用いたネットワーク構成の例を次に示す。解説を分かりやすくするため，以下，この例をたびたび登場させることにしよう。なお，この例ではWAN回線に広域イーサ網を選んでいるが，IP-VPN網でも変わりはない。

図：WASを用いたネットワーク構成

この図の中で，本部のファイルサーバ（以下，FSと称する）と支部のPCとの間でファイル転送を行う。ファイル転送には，ファイル共有プロトコルが用いられているものとする。

本部と支部間の通信はWASを経由している。WASは，ファイル共有における受信確認を**代理応答**し，WAS間ではサーバとPC間よりも大量のデータを**一括転送**する仕組みになっている。

WASが高速化を実現できる理由を理解するには，WAN回線経由のファイル転送の特徴について理解する必要がある。そこで，まずはその点について解説する。次いで，WASの特徴である代理応答と一括転送に着目しながら，WASによる高速化の仕組みを解説する。

●WAN回線経由のファイル転送の特徴

SMBなどのファイル共有プロトコルは，基本的に，「リクエストとレスポンス」の組（1往復）を単位にして，やり取りが行われる。例えば，PCがFSからファイルを読み出すとき，PCはリクエスト（読出しのコマンド）を送信する。FSはレスポンス（指定されたファイルのデータ）を返信する。

ファイル共有プロトコルの例として，SMB 1.0（CIFS）を取り上げる。CIFSの仕様上，リクエストとレスポンスの1往復でやり取りできるデータサイズには，上限がある。したがって，この上限値よりも大きいファイルサイズを読み出すには，リクエスト

WAN高速化装置について，平成26年午後I問1，平成20年午後I問3で出題された

SMB

SMBはWindowsに搭載されたファイル共有プロトコルであり，Windowsネットワークで他のPCにアクセスするとき，暗黙裡に使用されるものである。例えば，Windowsのエクスプローラーを開いて「ネットワーク」をクリックすると他のPCが見えたり，他のPC上で共有設定したディレクトリが見えたりするが，このときにSMBのやり取りが行われている

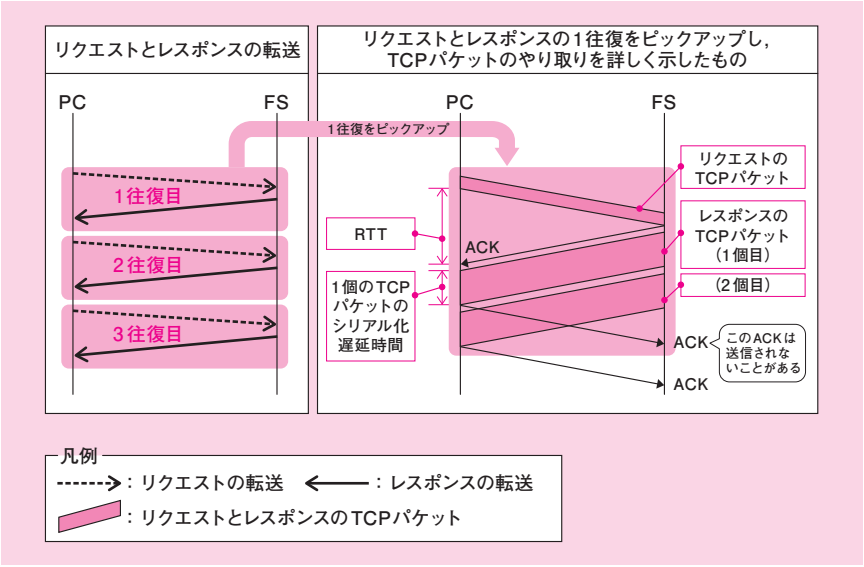
本書の解説は，平成26年午後I問1の出題例を参考にしている。その問題では，ファイル共有プロトコルとしてSMB 1.0（CIFS）が採用されていた。SMB 1.0は，ここで解説しているとおり，リクエストとレスポンスの組（1往復）のやり取りが主に行われている。

今日では，SMB 2.0以降が広く用いられている。SMB 2.0では，1回のリクエストパケットで複数のコマンドを送信する機能，直前のリクエストに対するレスポンスを待たずに次のリクエストを送信する機能など，数々の機能強化が図られている

とレスポンスの組が何往復もやり取りされることになる。

さらに，リクエストとレスポンスの1往復でやり取りできるデータサイズとして，TCPパケットの最大長よりも大きな値を指定することができる。このとき，レスポンスは複数のTCPパケットに分割される。

ここまで解説した内容に基づき，PCがFSから1個のファイルを読み出すときのシーケンスを次の図で示す。



図：リクエストとレスポンスの転送シーケンス

ここで，図の左側は，CIFSのリクエストとレスポンスのやり取りを示している。ここでは，1個のファイルを読み出すのに3往復のやり取りをしている。

図の右側は，リクエストとレスポンスの1往復をピックアップし，TCPパケットのやり取りを詳しく示している。ここでは，リクエストのサイズはTCPパケットの1個分，レスポンスのサイズはTCPパケットの2個分としている。FSからPC宛てにレスポンスを転送するとき，TCPの連続転送の仕組みにより，2個のTCPパケットを，ACK（確認応答パケット）を待たずに転送している。

ピックアップした図のPC側に示した「**シリアル化遅延時間**」は，パケットを1ビットずつ伝送するのに要する時間である。シリア

ル化遅延時間は「伝送時間」ともいう。伝送効率を無視すると，シリアル化遅延時間は次の式で求められる。

$$\text{シリアル化遅延時間[秒]} = \frac{\text{パケットサイズ[ビット]}}{\text{帯域[ビット／秒]}}$$

同じくピックアップした図の PC 側に示した「**RTT**」（Round Trip Time）は，パケットの往復時間（相手ノードに TCP パケットを送信してから，相手ノードからの ACK パケットを受信するまでの時間）である。

したがって，1 往復当たりの所要時間は，シリアル化遅延時間と RTT の合計値となる。

$$\text{1 往復当たりの所要時間[秒]} = \text{シリアル化遅延時間[秒]} + \text{RTT[秒]}$$

前述のとおり，CIFS は，「リクエストとレスポンス」の組（1 往復）を単位に，やり取りを行う。支部の PC と本部の FS 間で CIFS のやり取りを行うとき，PC は，リクエストを送信すると，RTT が経過してレスポンスを受信するまで，新たなリクエストを送信できない。したがって，1 個のファイルを読み出すのに何往復も必要とする場合，転送の所要時間はその往復分の時間となる。つまり，次の式で求められる。

$$\text{転送の所要時間[秒]} = \text{1 往復当たりの所要時間[秒]} \times \text{往復数}$$

具体例として，前述したネットワーク構成図に基づき，ファイル転送の所要時間を次の条件に従って求めてみよう。

表：転送の所要時間を求めるための条件

広域イーサ網の帯域幅	100×10^{6}[ビット／秒]
広域イーサ網の RTT	30×10^{-3}[秒]
ファイルサイズ	60,000,000 バイト
1 往復当たりの転送データサイズ	3,000 バイト
往復数	20,000 回（＝ 60,000,000÷3,000）

$$\text{シリアル化遅延時間[秒]} = \frac{3000\times8\text{[ビット]}}{100\times10^{6}\text{[ビット／秒]}} = 0.24\times10^{-3}\text{[秒]}$$

1往復当たりの所要時間［秒］
$= 0.24\times10^{-3}$［秒］$+ 30\times10^{-3}$［秒］
$= 30.24\times10^{-3}$［秒］

転送の所要時間［秒］　$= 30.24\times10^{-3}$［秒］$\times 20000$
$= 604.8$［秒］

この具体例から分かることは，1往復当たりの所要時間の大半を，RTTが占めていることである。これが，WAN回線経由のファイル転送の特徴である。

シリアル化遅延時間はRTTに比べて無視できる程度まで小さいので，広域イーサ網の帯域幅を増速させても，所要時間を短縮する効果はほとんどない。

●WASの代理応答と一括転送の仕組み

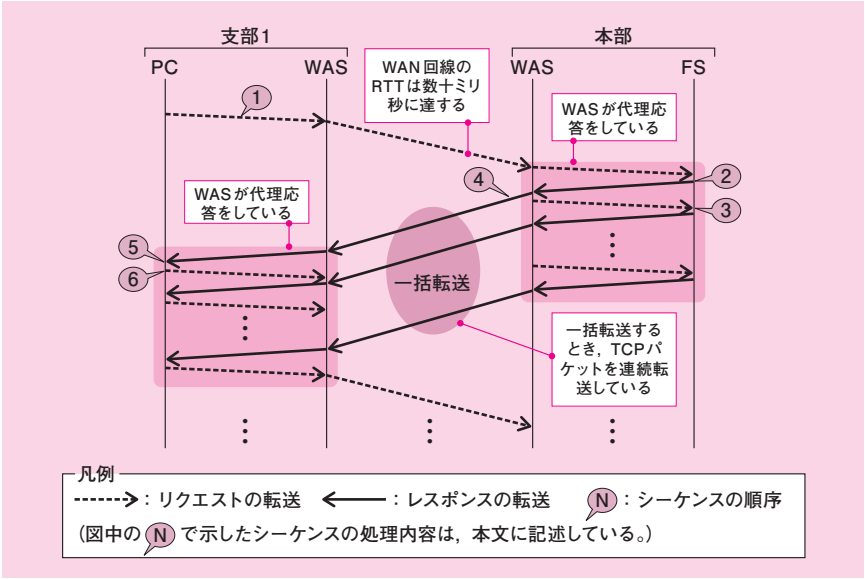
WASは，代理応答と一括転送の仕組みにより，WAN経由のファイル転送を高速化することができる。

代理応答について具体的に言うと，WASは次のように動作する

- 支部1においては，支部1のWASがあたかもFSであるかのように振る舞う。
- 本部においては，本部のWASがあたかもPCであるかのように振る舞う。

代理応答をする目的は，WAS間で一括してデータを送信するためであり，この一括転送こそ高速化の鍵を握っている。

この様子を次の図に示す。



図：WAS を用いた，リクエストとレスポンスの転送シーケンス

1. 支部 1 の PC は，支部 1 の WAS にリクエスト（1 回目）を転送する。支部 1 の WAS は，本部の WAS にこれを転送する。本部の WAS は，FS にこれを転送する。
2. FS は，リクエストを受信すると，本部の WAS にレスポンス（1 回目）を転送する。
3. 本部の WAS は，すぐに，FS にリクエスト（2 回目）を転送する。この WAS の振舞いは，「代理応答」と呼ばれている。この代理応答は，何度も行われる。LAN 上でやり取りしているため，RTT はほぼゼロである。
4. 本部の WAS は，代理応答をすると共に，レスポンスをキャッシュする。このキャッシュしたデータを支部 1 の WAS に一括転送する。支部 1 の WAS も，一括転送されたデータをキャッシュする。
5. 支部 1 の WAS は，PC にレスポンス（1 回目）を転送する。
6. 支部 1 の PC は，すぐに，支部 1 の WAS にリクエスト（2 回目）を転送する。支部 1 の WAS は，キャッシュしたデータからレスポンス（2 回目）を転送する。この WAS も，「代理応答」をしている。

この代理応答と一括転送によって，転送の所要時間はどのように改善されるのだろうか。先ほどの具体例で確かめてみよう。

新たに付け加える条件として，一括転送するデータサイズをレスポンスの10回分としてみる。その結果，1往復当たりの転送データサイズは10倍に，往復数は0.1倍になる。

表：転送の所要時間を求めるための条件

一括転送するデータサイズ	レスポンスの10回分
1往復当たりの転送データサイズ	30,000バイト（＝3,000×10）
往復数	2,000回（＝20,000÷10）

$$\text{シリアル化遅延時間[秒]} = \frac{30000\times 8[\text{ビット}]}{100\times 10^{6}[\text{ビット}/\text{秒}]} = 2.4\times 10^{-3}[\text{秒}]$$

$$\text{1往復当たりの所要時間[秒]} = 2.4\times 10^{-3}[\text{秒}] + 30\times 10^{-3}[\text{秒}] = 32.4\times 10^{-3}[\text{秒}]$$

$$\text{転送の所要時間[秒]} = 32.4\times 10^{-3}[\text{秒}] \times 2000 = 64.8[\text{秒}]$$

この例では，転送の所要時間は約1/10になることが分かる。その理由は，往復数が0.1倍になったからである。1往復当たりの所要時間の大半をRTT（30ミリ秒）が占めているため，往復数が減った分だけ転送の所要時間が短くなるわけだ。

このように，**RTTが大きい場合**，WASの高速化処理の効果がより高くなることが分かる。

2.3 ストレージネットワーキング

午後試験では，サーバ間でストレージを共有する事例や，広域災害に備えて遠隔地のバックアップサイトにリモートバックアップを行う事例がしばしば登場する。その中で，ストレージネットワーキングの基礎的な知識が問われる場合がある。過去には設計の応用問題が出題されたこともあったが，本文中に動作原理が詳しく説明されており，基礎知識から推論できるように配慮されていた。したがって，基礎知識をしっかり学習しておくことが大切である。

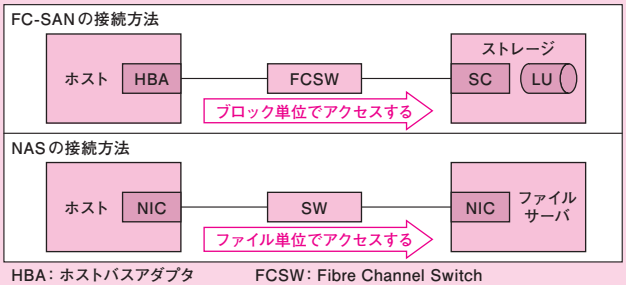
2.3.1 SAN と NAS

複数のサーバ間で，ネットワークを介した磁気ディスク装置の共有を可能にする技術として，**SAN**（Storage Area Network），**NAS**（Network Attached Storage）がある。

SAN のストレージデバイスは，サーバに直接接続された SCSI のストレージデバイス（raw デバイス）と機能的に同等である。ホストとロジカルユニット間のデータのやり取りには SCSI コマンドを使用し，**ブロック単位**でアクセスしている。

NAS は，ファイルサーバと機能的に同等である。ネットワーク上のストレージに対し，ファイル共有プロトコルを使用し，**ファイル単位**でアクセスしている。

両者のアクセス方法を次の図に示す。



図：SAN と NAS のアクセス方法

試験に出る

SAN と NAS の比較について，平成 23 年午前Ⅱ問 7，平成 18 年午後Ⅱ問 2，平成 17 年午後Ⅱ問 1 で出題された

なお，この図に登場するSANは，SANの一種である**FC-SAN**である（FC-SANについては後述する）。

ホストとSANのストレージは，**ファイバチャネルスイッチ**（以下，FCSWと称する）を介して接続している。ホストのインタフェースは**ホストバスアダプタ**（以下，HBAと称する）である。ストレージのインタフェースは，**ストレージコントローラ**（以下，SCと称する）である。

SANのストレージには，物理ディスク装置が何台も搭載されている。RAIDコントローラにより物理ディスクを束ねた上で，各ホストが必要とする容量に基づき，全体を幾つかに区分する。区分された個々の領域が，外部に提供する論理的なディスクとなる。この論理なディスクを**ロジカルユニット**（以下，LUと称する）と呼ぶ。

このLUに対し，ホストはSCSIコマンドを使用してブロック単位でアクセスする。

一方，ホストとNASは，通常のスイッチ（以下，SWと称する）を介して接続している。NASはファイルサーバと同等であるので，ホストとNASはIPアドレスをもっている。

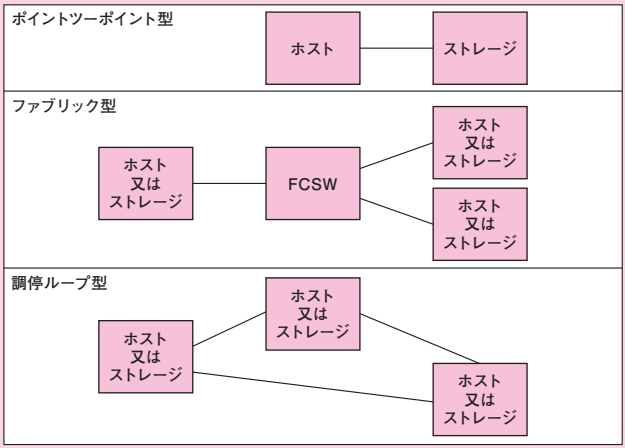
●ファイバチャネル

ファイバチャネル（FC：Fiber Channel）は，ANSIのT11で標準化された，高速かつ高信頼性を特徴とするデータ転送の規格である。

FCのトポロジには，ポイントツーポイント型（Point to Point），**ファブリック**型（Fabric），調停ループ型（Arbitrated Loop）の3種類があるが，SANで一般的に用いられているのは，ファブリック型である。

ファブリック型は，1台のスイッチに対し，1台以上のホスト又はストレージが接続される構成である。スイッチ同士を接続することもできる。

SANのファブリック型トポロジについて，平成18年午前問4で出題された



図：FC のトポロジ

●WWN とポートアドレス

WWN（World Wide Name）とは，FC のノード対して，全世界で一意に割り当てられた番号である。ここで言う「ノード」とは，ホストの HBA，FCSW，ストレージの FC インタフェースなどを指す。WWN は，ちょうどイーサネットの MAC アドレスに似ている。

HBA や FCSW のポートには，ポートアドレスが動的に割り当てられる。

●ゾーニング

FCSW に接続するサーバやストレージを複数のグループに分けることができる。このグループのことを**ゾーン**という。1台のスイッチに複数のゾーンを定義する機能のことを，**ゾーニング**という。

異なるゾーンに所属する機器（サーバ，ストレージ）は，互いに通信することができない。ゾーンの定義はポート単位又は WWN 単位で行う。1 個のポートを複数のゾーンに所属させることができる。

試験に出る

ゾーニングについて，平成 18 年午後Ⅱ問 2 で出題された

試験に出る

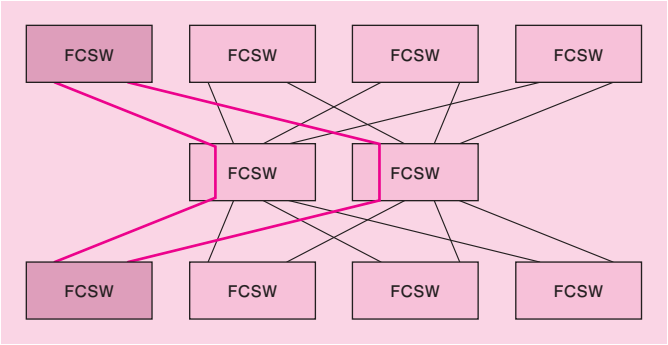
FSPFについて，平成23年午後Ⅱ問1で出題された。ホストとLU間の経路の冗長化について，平成24年午後Ⅱ問1で出題された

●FCの冗長構成

スイッチ間の経路を複数持たせ，冗長構成にすることもできる。FCが規定している経路制御方式である**FSPF**（Fabric Shortest Path First）は，FCSWのホップ数をコストとして評価し，SPF（Shortest Path First）アルゴリズムに基づいて最小コストの経路を決定する仕組みになっている。

コストが等しい経路が複数あるとき，それら経路を同時に使用できる。

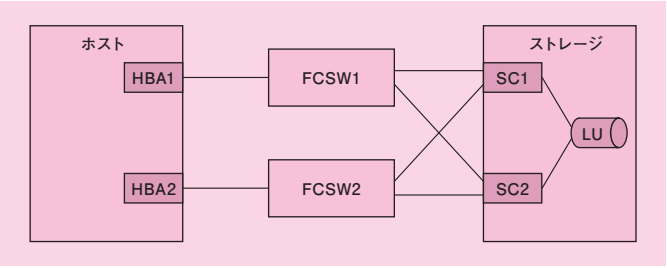
冗長構成を採ったファブリックの例を次の図に示す。左上のFCSWと左下のFCSW間の経路は二つあり，どちらもコストが等しいので，同時に使用される。



図：冗長構成を採ったファブリックの例

ホストとLU間の経路を冗長化するときは，ホストのHBA，FCSW，ストレージのSCをそれぞれ冗長化する。例えば，次の図では，ホストとLU間の経路は四つある。

経路①：ホスト→ HBA1 → FCSW1 → SC1 → LU
経路②：ホスト→ HBA1 → FCSW1 → SC2 → LU
経路③：ホスト→ HBA2 → FCSW2 → SC1 → LU
経路④：ホスト→ HBA2 → FCSW2 → SC2 → LU



図：ホストと LU 間の経路を冗長化した例

●FC-SAN と IP-SAN

SAN は，FC-SAN と IP-SAN に大別される。

FC-SAN は，FCSW によって構成される，ストレージ共有のためのネットワークである。

IP-SAN は，FC フレーム又は SCSI フレームを TCP/IP にカプセル化し，IP ネットワーク上に SAN を構築するものである。

IP-SAN について，詳しくは本章の「2.3.2　SAN のプロトコル」で解説する。

●拡張イーサネット（統合ネットワーク）

拡張イーサネットとは，IEEE802.1 委員会の DCB タスクグループで規格化されている **DCB**（Data Center Bridging）のことである。

伝送速度は 10Gbps であるが，従来のイーサネットをただ単に広帯域化したものではない。これは，FC-SAN（Fibre Channel Storage Area Network）を伝送することを目的として，イーサネットの機能を拡張し，FC が有していた高信頼性（ロスレス）などの優れた特性にできる限り近づけたものである。

拡張イーサネットでは，**CNA**（Converged Network Adapter）と呼ばれるネットワーク接続アダプタを使用する。これは，1 個のアダプタで HBA と NIC を兼ね備える機能をもつ。

今日，IP ネットワークはイーサネット上に構築されている。したがって，高信頼性を有する拡張イーサネットを構築すれば，FC-SAN と IP ネットワークを統合することができる。そのメリットは多々ある。まずは，IP ネットワークの側からすれば，レイヤ 2 の機能拡張がもたらす高信頼性を享受できる。ネットワーク全

拡張イーサネット（SAN と LAN の統合）について，平成 24 年午後Ⅱ問 1，平成 23 年午後Ⅱ問 1 で出題された

体からすれば，ネットワークの統合によるケーブリングの簡素化，省電力化，運用負荷の軽減などが期待できる。

拡張イーサネットについて，詳しくは本章の「2.3.2　SAN のプロトコル」で解説する。

2.3.2 SAN のプロトコル

用語解説

ロスレス
損失がないこと。ストレージトラフィックにおいては，特に，パケットロスがないことをいう

ここでは，FC-SAN，IP-SAN，拡張イーサネットのプロトコルについて解説する。

ストレージトラフィックでは，高信頼性（**ロスレス**）が求められている。高品質の光ファイバを伝送路として使用すれば，伝送路上でのビット誤りはまず発生しない。それゆえ，パケットロスの要因は，通常，**バッファの枯渇**である。

バッファの枯渇を防ぐには，適切な**フロー制御**が欠かせない。そこで，各プロトコルのフロー制御についても解説する。

●FC-SAN

FC のプロトコルスタックは，次に示す階層構造をしている。

表：FC のプロトコルスタック

階層	内容
FC-4 層	上位プロトコルとのマッピングを規定する（上位プロトコルのカプセル化に加え，上位層プロトコルの伝送手順を FC の下位層の該当するものに割り当てる場合がある）
FC-3 層	暗号化機能などを規定する（規定されているが，実装している製品は存在しない）
FC-2 層	フロー制御，伝送手順などを規定する
FC-1 層	8B/10B と呼ばれる符号化方式，パラレル／シリアル変換を規定する
FC-0 層	コネクタ，ケーブル，伝送メディアなどの物理的インタフェースを規定する

SCSI は，FC の上位プロトコルに位置する。SCSI をカプセル化した FC-4 層のプロトコルは，FCP である。それゆえ，FC-SAN では FCP が用いられている。

●FC-SAN のフロー制御

FC-SAN のフロー制御は，TCP のそれと比較すると理解しやすい。「相手が受信できるだけのフレームしか送信しない」という

点で，TCP とよく似ているからだ。

具体的に言うと，FC-SAN のフロー制御は，次のような仕組みになっている。

- **準備**
  通信を開始する前に，隣接するノード間で，自分の空きバッファ数を相手に通知しておく。相手側の空きバッファ数のことを「**クレジット**」という。
  FC-SAN は，クレジットを管理しながらフロー制御を行っている。

- **送信と受信**
  1. 相手に 1 フレーム送信したら，クレジットを 1 つ減らす。
  2. 相手から応答が返ってきたらクレジットを 1 つ増やす。

- **連続転送**
  FC-SAN では，クレジットが 0 になるまでは複数のフレームを連続転送することができる。クレジットが 0 になったら，相手から応答が返ってくるまで，フレームを送信しない。

FC-SAN の「クレジット」を TCP の「ウィンドウサイズ」に読み替えれば，FC-SAN と TCP/IP のフロー制御は，似ていることが分かるだろう。

しかし，両者には大きな相違点がある。

それは，「準備」のところで触れたとおり，FC-SAN では，「隣接するノード間」でフロー制御を行っている点だ。

つまり，TCP/IP のフロー制御が **End-to-End** で制御されるのに対し，FC-SAN では **Buffer-to-Buffer** で制御されているのである。

TCP/IP の場合，経路途中のどこかのノードでバッファ枯渇が発生したとしても，エンドシステムは（少なくともウィンドウサイズからは）そのことを知ることができない。したがって，ウィンドウサイズが 0 でなければ，相手のバッファ容量には余裕があると判断し，パケットを送信する。その結果，バッファ枯渇が発生したその場所で，パケットがロスしてしまうことになる。

一方，FC-SAN の場合，Buffer-to-Buffer であるため，**隣接ノー**

ド間の局所的なバッファ枯渇に対処できる。

前述のとおり，FC-SAN のフロー制御は，バッファの容量を相互に逐次確認し合うことで，相手のバッファが枯渇しないように，相手の状況に応じてフレームを送信している。FC-SAN は，通信経路上のあらゆる隣接ノード間で，このバッファ管理に基づくフロー制御を実施している。

したがって，各ノードのバッファが枯渇せず，枯渇に起因するフレームのロスを防止することができる。

試験に出る

FC-SANのフロー制御について，平成 23 年午後Ⅱ問 1 で出題された

●IP-SAN

IP-SAN の通信規格には，**iSCSI**（Internet SCSI），iFCP（Internet Fibre Channel Protocol），FCIP（Fibre Channel over IP）がある。

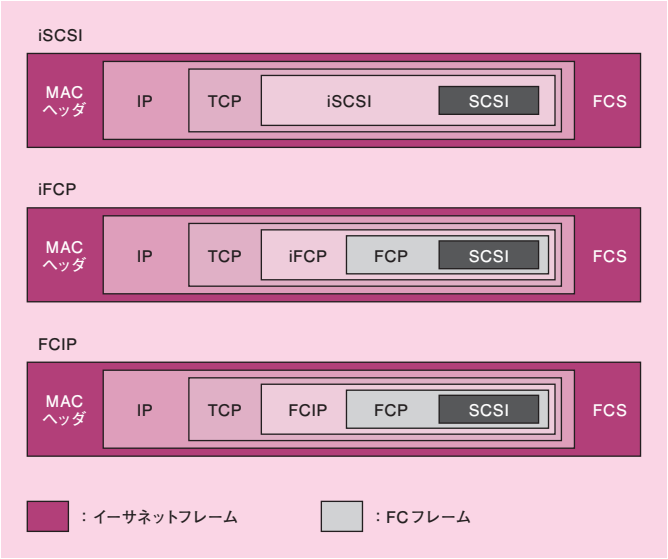
iSCSI は SCSI コマンドを TCP/IP パケットにカプセル化しており，FC デバイスを用いることなく，IP ネットワークだけで構成する。

これに対し，iFCP，FCIP は，FC-SAN の通信で用いられている FC フレームを TCP/IP パケットにカプセル化している。

これら三つのプロトコルのプロトコルスタックを次の図に示す。

試験に出る

IP-SAN について，平成 23 年午後Ⅱ問 1，平成 22 午後Ⅱ問 1，平成 20 午後Ⅰ問 2，平成 18 午後Ⅱ問 2 で出題された。iSCSI のイニシエータやターミネータについて，平成 22 年午後Ⅱ問 1 で出題された



図：IP-SAN のプロトコルスタック

- **iSCSI**

  iSCSI は，iSCSI 対応のストレージを用意するだけで，既設の IP ネットワーク環境に共有ストレージ環境を構築できる。その導入容易性から，IP-SAN の中で最もよく用いられている。

  iSCSI は，イニシエータからターゲットに SCSI コマンドを発行することによって，サーバとストレージ装置間でブロックデータの入出力が実現される仕組みになっている。

  イニシエータとは，サーバで稼働し，SCSI コマンドを発行するソフトウェアである。**ターゲット**とは，ストレージ装置で稼働し，SCSI コマンドの処理を実行するソフトウェアである。

  なお，イニシエータソフトウェアをサーバにインストールする代わりに，iSCSI のプロトコル処理をハードウェアで実行する iSCSI HBA をサーバに搭載してもよい。

- **iFCP と FCIP**

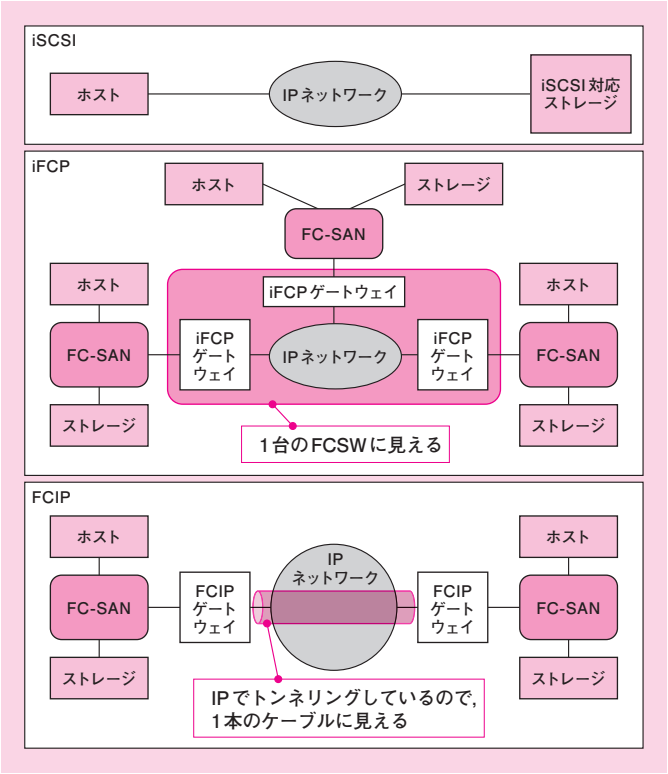
  iFCP と FCIP は，プロトコルスタックだけなら，どちらも同じように見える。事実，両者とも FCSW 間を IP ネットワークで接続し，あたかも FC-SAN の伝送距離を延長しているような構成になっている。

  とはいえ，iFCP と FCIP は，FC から IP ネットワークがどのように見えるかが異なっている。これが，両者の接続方式に相違をもたらしている。

  iFCP からは，IP ネットワークがあたかも 1 台の FCSW のように見える。したがって，IP ネットワークに対し，3 拠点以上の FC-SAN を接続することができる。

  一方，FCIP からは，IP ネットワークがあたかも 1 本のケーブルのように見える。なぜなら，FC フレームを IP でトンネリングして転送しているからだ。したがって，IP ネットワークに対し，2 拠点の FC-SAN だけを接続することができる。

  比較のために，iSCSI，iFCP，FCIP の接続方式を次の図に示す。



図：IP-SAN の接続方式

●IP-SAN のフロー制御

iSCSI は，TCP/IP のフロー制御を行っている。

iFCP，FCIP は，IP ネットワーク上の伝送では TCP/IP のフロー制御を行っている。

●拡張イーサネット（統合ネットワーク）

FC-SAN と統合ネットワークをフレームフォーマットで比較してみると，「統合」のイメージをつかみやすくなる。

- **FC から見た下位層**

  FC フレームは，FC-SAN によって伝送されている。

  一方，統合ネットワークでは，FC フレームを **FCoE**（Fibre Channel over Ethernet）フレームでカプセル化し，この

FCoE フレームを拡張イーサネットフレームがカプセル化している。そして，拡張イーサネットフレームは，統合ネットワークによって伝送されている。

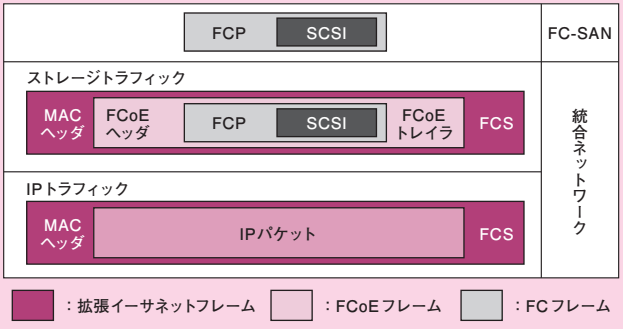
したがって，FCoE のカプセル化の仕組みにより，FC の観点からは，FC-SAN と統合ネットワークは，自分を伝送する媒体（物理層）に見える。

もちろん，これはあくまでフレームフォーマット上の話である。伝送媒体を FC-SAN から統合ネットワークに置き換えるには，同等の伝送品質を提供できなければならないので，従来のイーサネットからの機能拡張が必要となったわけだ。

- **拡張イーサネットから見た上位層**

拡張イーサネットフレームのフォーマットは，通常のイーサネットのタグ VLAN 付きフレームと同じである。FCoE フレームと IP パケットは，イーサネットフレームのタイプ値が異なるだけである。イーサネットの観点からは，どちらも上位層に見える。

したがって，フレームフォーマット上は，ストレージトラフィックと IP トラフィックを統合できていることになる。

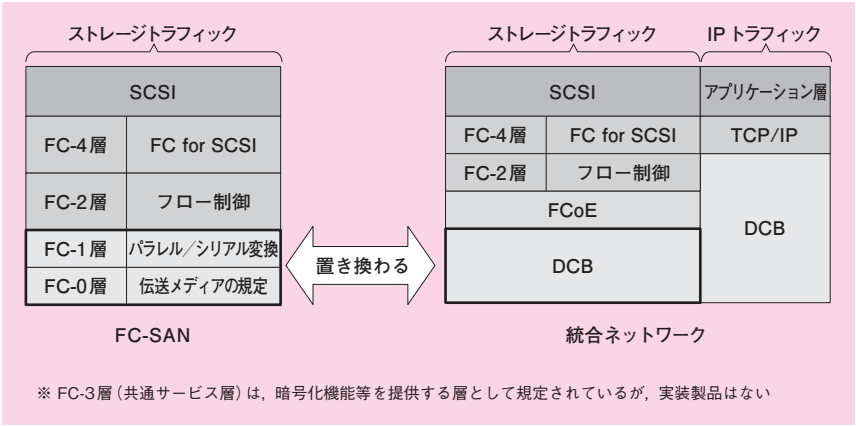


厳密に言うと，FC フレームの前後には，SOF（Start Of Frame）と EOF（End Of Frame）が付与される。FCoE ヘッダは FC の SOF を，FCoE トレイラは FC の EOF を，それぞれ格納している（SOF，EOF のコード値を変換した上で，格納している）。

図：フレームフォーマットの比較

FC-SAN の階層を統合ネットワークのプロトコルスタックに当てはめてみると，次の図「プロトコルスタックの比較」となる。

ただし，この比較は，厳密なものではない。



図：プロトコルスタックの比較

簡単に言うと，拡張イーサネットは，FC の FC-0 層～ FC-1 層に置き換わっている。

FC-SAN は，SCSI を使用した raw デバイスへのアクセスをネットワーク経由で提供している。FC は，ストレージに送受信する SCSI コマンドやデータを FC フレームにカプセル化する機能を有する。SCSI はパケットロスを前提としないプロトコルなので，SCSI の下位層が信頼性を確保する必要がある。まさしく FC はその信頼性を提供しており，フロー制御など，高信頼性を確保する機能が実装されている。

IP ネットワークとの統合を果たすには，FC-0 層～ FC-1 層をイーサネットに置き換える必要がある。しかし，FC-SAN と統合するには，イーサネットは信頼性の点で劣っている。そこで拡張イーサネットが必要になったわけだ。

●統合ネットワークのフロー制御

前述のとおり，FC-SAN の FC-0 層～ FC-1 層が，拡張イーサネットに置き換わる。

ストレージトラフィックの場合，上位層は FC-2 層～ FC-4 層と

なる。前述の「クレジット」を用いたフロー制御は FC-2 層なので，拡張イーサネットには，上位層の信頼性の水準を損なわないことが求められる。

拡張イーサネットは，FC フレームをカプセル化しているが，フロー制御は拡張イーサネットの方式を使用することが規定されている。従来の FC-2 層のクレジット方式のパラメータは使用せず，無視している。

既存のイーサネットは，隣接ノード間でフロー制御（IEEE 802.3x）を行っている。これは，クレジット方式のような，相手のバッファの容量を考慮に入れた方式ではない。自分のバッファが枯渇しそうになったら，PAUSE フレームを送り，物理リンクのトラフィックを一時的に止めるように相手に通知する仕組みしかもたない。

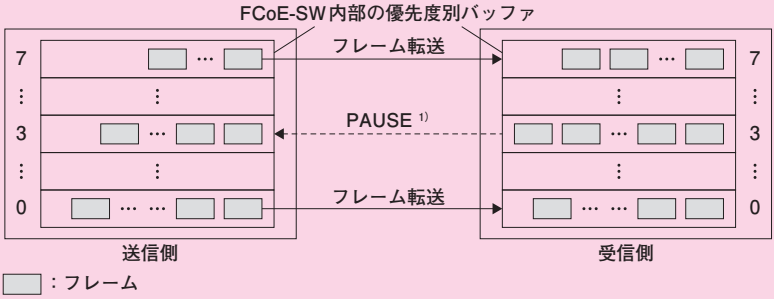
これでは，統合ネットワークにおいて，ストレージトラフィックの信頼性を確保するには不十分である。なぜなら，統合ネットワークでは，ストレージトラフィックや IP トラフィックなど，優先順位の異なるトラフィックが同じ物理リンク上を流れるからである。

TCP はウィンドウ制御を行っているが，これをエンドシステム間で行っているので，局所的なバッファ枯渇には対応し切れない。そのため，経路上のどこかで輻輳しているにもかかわらず，パケットを送り続ける可能性を秘めている。輻輳している場所がイーサネット上であれば，隣接ノード間で IEEE802.3x のフロー制御が働く。この結果，リンクを流れるトラフィックの種類を識別することなく，物理リンク全体のトラフィックを止めてしまう。イーサネット上で輻輳したら，ストレージトラフィックも影響を受けてしまうのだ。

そこで，拡張イーサネットは，IEEE802.3x の仕様を拡張し，FC-2 層のクレジット方式に代わる新しいフロー制御の方式を規定した。それは，「仮想リンクごとの優先度付きバッファ制御」（PFC），「仮想リンクごとの帯域制御」（ETS），「スイッチ間のプロパティ交換」（DCBX）の三つである。

- **仮想リンクごとの優先度付きバッファ制御**
  まず，1 本の物理リンク上に最大 8 本の仮想リンクを構築し，仮想リンクごとに，優先度付きのバッファをもたせる

機能を追加した。ノードは，自分のバッファが枯渇しそうになったら，優先度の低い仮想リンクの通信を一時的に止めるようにPAUSEフレームを送る仕組みを備えている。



注1)　受信側バッファの枯渇を防止するために送出する。
注記　0～7の数字は，バッファの優先度を示す。数字が大きいほど優先度が高い。

図：優先度付きバッファ制御機能(平成23年午後Ⅱ問1の図5より作成)

試験に出る

優先度付きバッファ制御の仕組みについて，平成23年午後Ⅱ問1で出題された。ただし，本文の中でこの仕組みは詳しく解説されており，従来技術のPAUSEフレームの知識から推論できるように配慮されていた

ある優先度のバッファが枯渇した場合，どうなるだろうか。当該優先度の通信だけを抑止できるので，他の優先度の通信に影響を及ぼさないようにできる。

この結果，優先度の高い通信と低い通信が同時に発生した場合，低い方の通信が大量であったとしても，低い方の帯域を一定量以下に抑えることができる。なぜなら，あらかじめ設定しておいたバッファ容量が枯渇した時点で，PAUSEフレームが送出され，低い方の送信が抑止されるからだ。その結果，優先度の高い方の通信が妨害されることはない。

トラフィックに優先順位を付与する機能は，PFCP（Priority-based Flow Control，優先度ベースのフロー制御）と呼ばれ，IEEE802.1Qbbで規格化されている。

物理リンクを流れるパケットがどの仮想リンクを流れているか(つまり，どの優先順位が付与されているのか)をスイッチが識別するため，パケットのVLANタグ（IEEE802.1Q）にある優先度フィールドを使用する。

- **仮想リンクごとの帯域制御**
  拡張イーサネットは，優先度付きバッファ制御に加え，仮想リンクごとに帯域制御を行う機能も追加している。
  トラフィックごとに帯域制御を行う機能は，ETS（Enhanced Transmission Selection，拡張伝送選択）と呼ばれ，IEEE802.1Qaz で規格化されている。
  PFC と ETS により，統合ネットワークにおいて，ストレージトラフィックの「ロスレス」を実現できる。ストレージトラフィックを流す仮想リンクに対し，高い優先順位と一定の帯域を与えればよいからだ。
- **スイッチ間のプロパティ交換**
  各スイッチが PFC と ETS を装備していようとも，隣接するスイッチ間で，PFC と ETS の設定情報の整合性がとられていないならば，FC-SAN のクレジット方式に比肩する Buffer-to-Buffer のフロー制御を実現できない。
  拡張イーサネットは，IEEE802.1AB（LLDP：Link Layer Discovery Protocol）の機能を利用して，拡張イーサネット対応スイッチ間でプロパティの交換を行うことができる。これは，DCBX（Data Center Bridging Exchange）と呼ばれている。

2.3.3 リモートバックアップ

広域災害時の事業継続性を確保するため，信頼性の指標として，**目標復旧時点**（**RPO**：Recovery Point Objective）を定めることがある。

RPO とは，障害発生時点から遡って，どの時点までデータを復旧するかを定めた目標値である。例えば，RPO を 24 時間に定めた場合，障害発生時点から 24 時間以内の業務データが復旧の対象となる。

試験に出る

RPO について，平成 26 年午前Ⅰ問 21，平成 20 年午後Ⅰ問 2，平成 16 年午後Ⅱ問 2 で出題された

●RPO を 24 時間に定めた場合の対策

広域災害を想定して RPO を 24 時間に定めた場合，その具体的な対策として，被災を免れる遠隔地に副系拠点を設け，主系拠

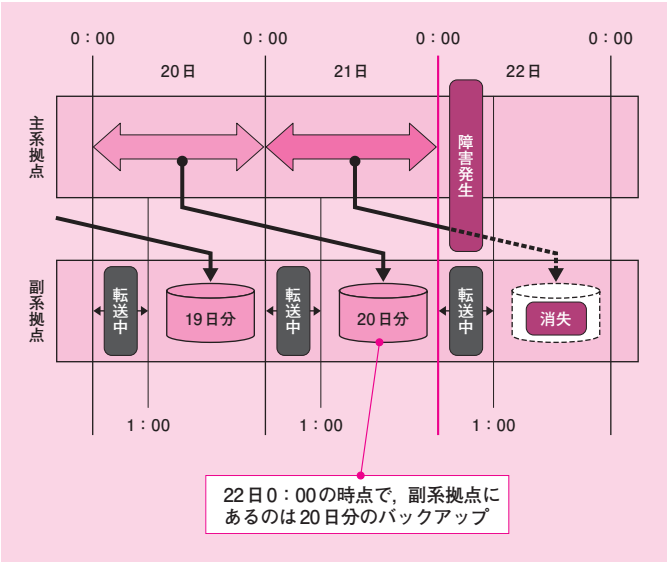
点の 24 時間以内の業務データを副系拠点にバックアップしておく方法が考えられる。

このとき，ネットワーク回線を経由して業務データを副系拠点に転送するのであれば，転送の所要時間を考慮に入れて，バックアップ取得の間隔と頻度を計画する必要がある。

例えば，24 時間無停止で業務を行っている例を取り上げてみよう。主系拠点の 1 日分の業務データ（前日 0：00 ～本日 0：00 の直前）を毎日 0：00 から転送するものとし，その所要時間が 1 時間であるとする。

22 日の 0：00 の時点で，20 日分の業務データが副系拠点にバックアップされている。

22 日の 0：00 から，21 日分のバックアップを開始する。その転送を行っている最中（0：00 ～ 1：00）に主系拠点が被災するならば，どうなるだろうか。



図：バックアップ転送のスケジュール

障害発生以前の全データが主系拠点で消失する可能性，及び，今まさに転送中の前日分データがネットワーク回線で消失する可能性がある。被災を免れているのは，副系拠点で安全に保管された一昨日までのデータなので，この方法では 24 時間という

RPO を満たすことができない。

したがって，この例においては，バックアップデータの転送を1日2回以上実施する必要がある。

●RPO を 0 時間に定めた場合の対策

RPO を 0 時間に定めた場合は，データの消失を一切許容しないことを意味する。

その具体的な対策として，主系拠点から副系拠点に向けて，**同期式コピー**を取る方法が考えられる。

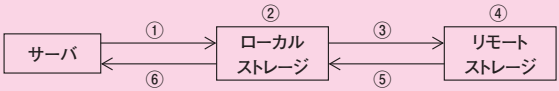
同期式コピーでは，主系拠点のサーバからローカルストレージに書込み命令を出すと，副系拠点のリモートストレージにも書込み命令が出される。そして，リモートストレージからの書込み完了通知を待って，ローカルストレージはサーバに書込み完了通知を行う。つまり，ローカルストレージとリモートストレージは同期を取っている。

平成 20 年午後 I 問 2 には，リモートコピーの方式として，同期式と非同期式を比較する問題が出題されている。参考までに該当箇所を掲載する。

試験に出る

リモートコピーの同期式と非同期式の比較について，平成 20 年午後I問 2 で出題された。重複排除の技術を用いたリモートコピーについて，平成 22 年午後Ⅱ問 1 で出題された

リモートコピーの方式には，同期式と非同期式がある。同期式コピーは，リモート側でのデータ更新を待ってサーバに更新完了報告を行う方式であり，非同期式コピーは，リモート側でのデータ更新完了に左右されずに更新完了報告を行う方式である。図 1 に，同期式コピーの仕組みの例を示す。



処理順序
①ローカルストレージへの書込み命令
②ローカルストレージでの書込み処理（T_1）
③リモートストレージへの書込み命令（T_2）
④リモートストレージでの書込み処理（T_1）
⑤リモートストレージからの書込み完了通知（T_3）
⑥［　a　］

T_n：処理時間
注　②と③は同時に実行される。

図 1　同期式コピーの仕組みの例

図 1 では，⑥の実行によってデータ更新が完了するので，障害発生直前のデータまで保証される。しかし，ネットワークでの遅延や送受信におけるエラーリカバリ処理などによって，サーバの［　オ　］が低下する。ネットワークでの遅延は，機器や伝送媒体の性能にも左右されるが，光の速度（約 3×10^5km／秒）そのものが制約となり，距離に応じて発生するので，バックアップサイトとの距離を考慮する必要がある。

図：リモートコピーの方式（平成 20 年午後 I 問 2 より引用）

ここには，「⑥の実行によってデータ更新が完了するので，障害発生直前のデータまで保証される」と記述されている。したがって，この方式を採用すると，RPO を 0 時間にすることができる。

2.4 ユニファイドコミュニケーション

午後試験では，SIP の基礎知識を前提とした，VoIP 電話網を設計する問題が出題されている。SIP は，IP 電話の通話セッションだけでなく，音声と動画を組み合わせたビデオ会議セッションにも使用できるし，インスタントメッセージやプレゼンス情報の通知などにも使用できる。このように，SIP はユニファイドコミュニケーションにおいて重要な役割を果たしている。今後とも出題される可能性があるので，応用問題にも対応できるようにしっかり理解しておく必要がある。

2.4.1 SIP

SIP（Session Initiation Protocol）は，端末間で，**セッション**の生成，変更，転送，切断などを行うプロトコルである。SIP では，端末のことを**ユーザエージェント**（以下，**UA** と称する）と呼ぶ。

試験に出る

SIP の説明について，平成 20 年午前 問 35（平成 18 年午前 問 31 と同じ問題），平成 19 年午前 問 39 で出題された

●SIP の機能

SIP で規定されているのは，主に**セッションを制御する機能**である。セッション上でやり取りされるデータそのものについては規定されていない。セッションを生成した後，リアルタイムデータ（音声，映像）の転送には，別のプロトコルが用いられる。一般的に言って，リアルタイムデータの転送に使用されるプロトコルは，**RTP**（Real-time Transport Protocol）である。

SIP の基本的な機能であるセッション制御に関する規格は，RFC3261 で規定されている。その後，機能の追加や拡張が行われており，インスタントメッセージを交換する機能，イベントを通知する機能なども規定されている。

インスタントメッセージ機能は，RFC3428 で規定されている。これは，チャットのように，利用者間でテキスト情報を交換する機能である。

イベント通知機能は，RFC6665 で規定されている。これは，イベントを通知する側とそのイベントを購読する側とを事前に登録しておき，通知側 UA でイベントが発生する都度，購読側 UA に

そのイベントが通知される機能である。よく利用されるイベント情報として，「利用者が今どんな状況にあるか」（「在席中」「離席中」「休憩中」など）といったプレゼンスに関する情報がある。

表：SIP で規定されている機能

機能	主な内容
セッション制御	セッションの生成を要求する セッションを変更する 別の UA にセッションを転送する セッションを切断する
インスタントメッセージ	インスタントメッセージを送信する
イベント通知	プレゼンス情報の購読をサーバに申し込む プレゼンス情報をサーバに送信する サーバから購読者にプレゼンス情報を通知する

SDP について，平成 26 年午後Ⅱ問 2，平成 22 年午前Ⅱ問 16 で出題された

● SDP

リアルタイムデータの通信を始める前に，上位アプリケーション間でどのような通信を行うかについて，情報を交換しておく必要がある。その情報とは，具体的に言うと，例えば次に示すものがある。

- UA の IP アドレス
- リアルタイムデータ転送用プロトコルが使用するポート番号
- 音声や映像といったメディアの種別，及び，そのメディアで用いられる符号化方式

この情報の記述方法を規定したものが，**SDP**(Session Description Protocol）である。

この情報交換は，SIP がセッションを生成している間に行われる仕組みになっている。これをネゴシエーションという。ネゴシエーションについては，「● SIP のシーケンス（基本）」で後述する。

なお，ここで言う「メディア」とは，UA 間で送受信される音声や映像などのデータのことである。SIP は，一つのセッションの中で，複数のメディアを同時に送受信することができる。例えば，音声通話のセッションを生成したり，音声と映像を組み合わせたビデオ会議のセッションを生成したりすることができる。

●RTP

RTP（Real-time Transport Protocol）は，音声や映像などリアルタイム性のあるデータをストリーミング配信する仕組みを備えたプロトコルである。

送信ホストは，シーケンス番号とタイムスタンプをパケットごとに付与している。受信ホストは，パケット間の時間差を調整し，リアルタイム性を確保しながらデータを再生することができる。

●SIP の構成要素

SIP を構成する要素は，UA，SIP サーバである。

- **UA**

  UA の識別には，**SIP URI** が用いられる。その書式は，「sip: 利用者識別子 @ ドメイン名」という URI 形式である。「利用者識別子」の部分には，電話番号を入れることができる。同一ドメイン内の通信であれば，「@ ドメイン名」を省略してもよい。

- **SIP サーバ**

  UA で電話をかけるとき，発呼する側は，着呼する側の電話番号や利用者識別子を知っている。

  このとき，もしも着呼側 UA の IP アドレスを知っていれば（発呼側 UA に登録されていれば），UA 間で SIP 通信を直接やり取りし，セッションを生成することができる。この場合，SIP サーバは不要である。

  それでは，もしも着呼側 UA の IP アドレスを知らない場合，どうしたらよいだろうか。実際，相手の UA の IP アドレスまでは知らないことが多いのではないだろうか。このとき，UA 間のセッション生成を仲介するために，SIP サーバが必要となる。

  SIP サーバを用いる場合，UA は，自分の利用者識別子，自分の IP アドレスを含む登録メッセージを SIP サーバに事前に送信しておく。SIP サーバは，これを受信し，自分が仲介する全ての UA について，SIP URI と IP アドレスの対応付けを登録しておく。

試験に出る

SIP サーバについて，平成 26 年午後Ⅱ問 2，平成 20 年午後Ⅱ問 2，平成 17 年午前問 46，平成 17 年午後Ⅰ問 3 で出題された

参考

SIP サーバの役割を次の三つに分類することがある。

- レジストラ
  REGISTER リクエストを受け付け，SIP URI と IP アドレスの対応付けをロケーションデータベースに登録する
- プロキシサーバ
  UAC と UAS の両方の機能を持ち，セッション生成のやり取りを仲介する
- リダイレクトサーバ
  通信相手のアドレスが変更されていた場合，ロケーションサーバに問い合わせて，宛先 UA の適切な URI を回答する。プロキシサーバと異なり，リクエストを仲介しない

通話するとき，UA は SIP サーバにセッションの生成を要求し，その要求メッセージの中で，着呼側の SIP URI を指定する。SIP サーバは，指定された SIP URI から IP アドレスを割り出すことができるので，セッション生成を仲介することができる。

SIP サーバを用いた SIP のメッセージシーケンスについては，「● SIP のシーケンス（SIP サーバを用いる場合）」で後述する。

● SIP のメッセージ

SIP のメッセージの種類には，発呼側 UA から着呼側 UA に送信するリクエストと，着呼側 UA から発呼側 UA に返信するレスポンスがある。

・リクエスト

主なリクエストメッセージは，次のとおりである。

表：主なリクエストメッセージ

機能	メソッド	内容
セッション制御	INVITE	セッションの生成を要求する
	ACK	セッションの生成を確認する
	BYE	セッションを切断する
	CANCEL	完了していないリクエストを取り消す
	OPTIONS	サーバの機能を問い合わせる
	REGISTER	ロケーションデータベースへの登録を要求する
	INFO	セッションの状態を通知する
	REFER	セッションを転送する
インスタントメッセージ	MESSAGE	インスタントメッセージを通知する
イベント通知	SUBSCRIBE	プレゼンスサーバに対し，プレゼンス情報の購読を申し込む
	PUBLISH	プレゼンス情報をプレゼンスサーバに登録する
	NOTIFY	プレゼンスサーバが購読者にプレゼンス情報を通知する

・レスポンス

レスポンスメッセージには，次に示す 3 桁のレスポンスコードが含まれている。1 桁目の値によって六つのクラスに分類される。

表：主なレスポンスコード

タイプ	クラス	意味		
Provisional（暫定応答）	1XX	100	Trying	処理中
		180	Ringing	着呼側を呼出し中
Final（最終応答）	2XX	200	OK	成功
	3XX	リダイレクション，フォワーディング		
	4XX	クライアント起因によるリクエスト失敗		
	5XX	サーバエラー		
	6XX	一般的なエラー（ビジー，拒否など）		

※クラスの２桁目，３桁目の XX には，０～９の数値が入る。

- **メッセージフォーマット**

SIP メッセージは，次の図に示すとおり，スタートライン（先頭行），ヘッダ，ボディからなる。なお，ボディは必要に応じて追加されるものであり，ボディをもたないメッセージがある。

ボディは MIME 形式で記述することが定められている。とはいえ，記述内容に関する規格は，SIP では規定されていない。

セッション制御機能の INVITE や ACK などのリクエストでは，ボディにセッションの属性が記述される。「● SDP」で解説したとおり，その記述に用いられるのが SDP である。インスタントメッセージ機能の MESSAGE リクエストでは，ボディにテキストの内容が記述される。

試験に出る

SIP のメッセージについて，平成 26 年午後Ⅱ問２，平成 20 年午後Ⅱ問２で出題された

スタートライン	リクエストではリクエストライン レスポンスではステータスライン
ヘッダ	メッセージの属性を表す
ボディ	セッションの属性を表す

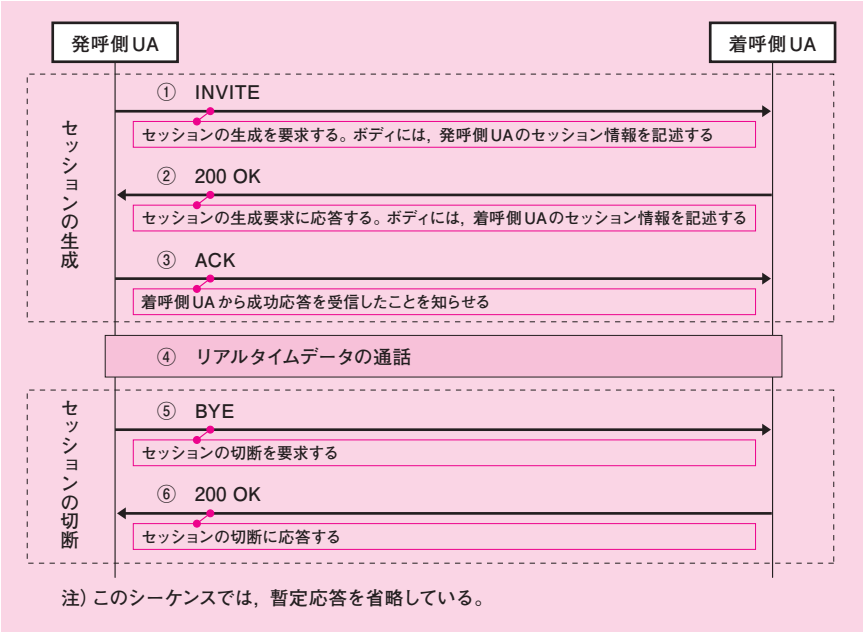
図：SIP のメッセージフォーマット

●SIP のシーケンス（基本）

SIP でセッションを生成するときの基本となるメッセージは，**INVITE** リクエスト，200 OK レスポンス，ACK リクエストの１

往復半からなるやり取りである。SIP の規格を定めた RFC は，これをスリーウェイハンドシェークと呼んでいる（RFC3261, 15 ページ）。

SIP の基本的なシーケンスを次の図に示す。なお，この図では暫定応答を省略している。



図：SIP の基本的なシーケンス

①発呼側は，セッションの生成を要求するため，INVITE リクエストを送信する

このボディには，発呼側のセッション情報を記述する。

②着呼側は，セッション生成要求に応答するため，200 OK（成功応答）レスポンスを送信する

このボディには，着呼側のセッション情報を記述する。

着呼側は，INVITE リクエストの SIP メッセージに記載された情報から，発呼側の IP アドレス，通話に使用するポート番号，などのセッション情報を知ることができる。

着呼側が 200 OK を返信したことは，これら発呼側のセッ

ション情報を受け付けたことを意味している。

③発呼側は，着呼側から成功応答を受信したことを知らせるため，ACK リクエストを送信する

発呼側は，200 OK レスポンスの SIP メッセージに記載された情報から，着呼側の IP アドレス，通話に使用するポート番号，などのセッション情報を知ることができる。

発呼側が ACK を送信したことは，これら着呼側のセッション情報を受け付けたことを意味している。③が終了した時点で，セッションが生成される。

④リアルタイムデータの通話を行う

通話に用いるプロトコルは，①～②のセッション情報交換で決めたものである。通常，音声や映像などのリアルタイムデータの通話には，RTP が用いられる。

通話に用いる IP アドレスは，①～②のセッション情報交換で決めたものである。

⑤セッションの切断を要求するため，BYE リクエストを送信する

切断の要求は，発呼側，着呼側のどちらから送信してもよい。

⑥切断要求に応答するため，200 OK（成功応答）レスポンスを送信する

セッション生成時のスリーウェイハンドシェークを通し，発呼側と着呼側はセッション情報を交換し，かつ，双方が合意した属性でセッションを生成する。「● SDP」でも触れたが，このやり取りのことを，ネゴシエーションと呼んでいる。このネゴシエーションを経て，リアルタイムデータの通信に移ることができる。

ネゴシエーションについて補足すると，発呼側が INVITE を送信する際，複数のセッション情報の候補を列挙することができる。このとき，着呼側は，その中から一つを選んで成功応答を返信する。あるいは，発呼側が INVITE を送信する際，セッション情報を一切記載しないこともできる。このとき，着呼側はセッション情報を自由に指定して成功応答を返信する。

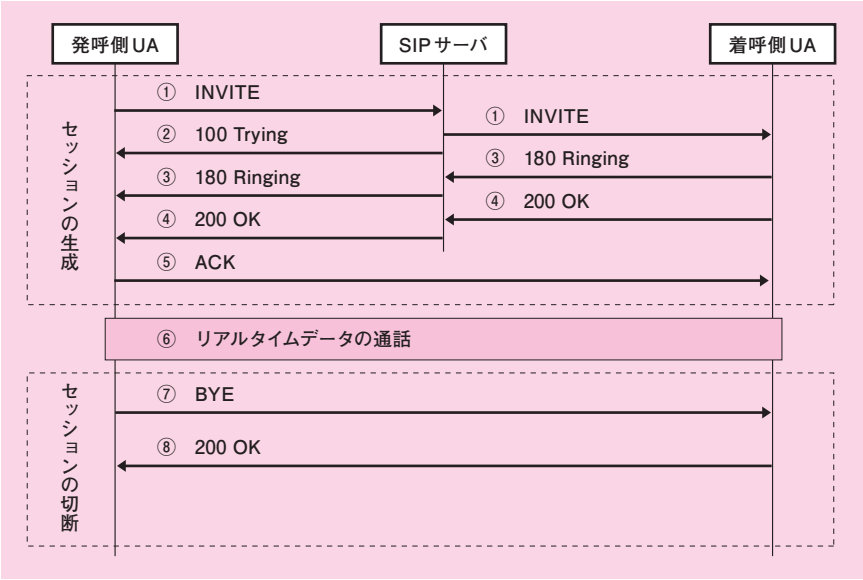
試験に出る

SIP サーバを用いたシーケンスについて，平成 26 年午後Ⅱ問 2，平成 20 年午後Ⅱ問 2，平成 19 年午後Ⅱ問 1 で出題された

●SIP のシーケンス（SIP サーバを用いる場合）

「● SIP の構成要素」で触れたが，UA が互いの IP アドレスを把握していない場合，SIP サーバを仲介してセッションを生成する。各 UA は，SIP URI と IP アドレスの対応付けを SIP サーバに初期登録しておく。

SIP サーバを使用した場合のシーケンスを次の図に示す。この図では暫定応答も記している。



図：SIP サーバを仲介した場合のシーケンス

①発呼側は，SIP サーバに INVITE メッセージを送信する
SIP サーバは，INVITE リクエスト中の着呼側 SIP URI から IP アドレスを割り出し，着呼側にこれを転送する。

②SIP サーバは，INVITE リクエストの転送を知らせるため，発呼側に 100 Trying（処理中）レスポンスを送信する

③着呼側は，INVITE メッセージを受信すると，利用者を呼び出す（電話であれば，呼出し音を鳴らす）
呼出し中であることを知らせるため，着呼側は SIP サーバに，SIP サーバは発呼側に，180 Ringing（呼出し中）レスポンスを送信する。

④着呼側は，セッション生成要求に応答するため，200 OK（成功応答）レスポンスを SIP サーバに送信する

SIP サーバは，発呼側にこれを転送する。

⑤発呼側は，着呼側から成功応答を受信したことを知らせるため，ACK リクエストを送信する

「● SIP のシーケンス（基本）」で述べたとおり，発呼側は，200 OK（成功応答）レスポンスを受信することで，着呼側の IP アドレスを知ることができる。そのため，ACK リクエストは，SIP サーバを介さずに直接相手に送信することができる（SIP サーバを経由して ACK を送信してもよい）。

⑥リアルタイムデータの通話を行う

⑦セッションの切断を要求するため，BYE リクエストを送信する

⑧切断要求に応答するため，200 OK（成功応答）のレスポンスを送信する

● Via フィールドの働き

Via フィールドは，リクエストが経由したパスを示している。

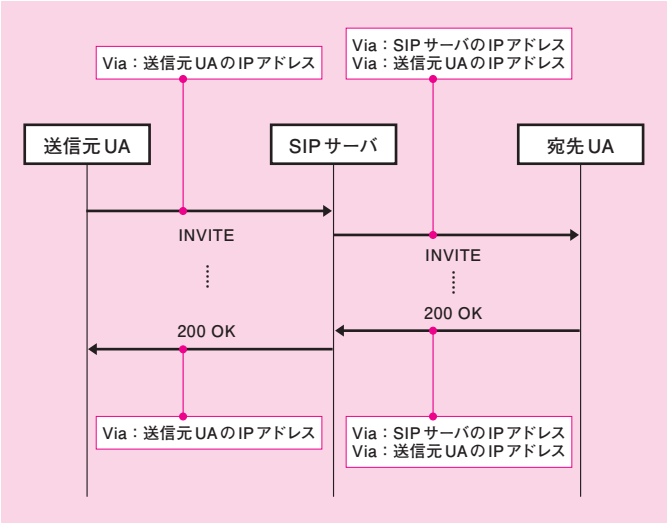
まず，送信元 UA が自分の IP アドレス（又はホスト名）を格納した Via フィールドを記述する。

SIP サーバはリクエストを中継する際，自分を経由したことを示すために Via フィールドを 1 行追加する。追加する位置は既存の Via フィールドの上位である。

宛先 UA は，レスポンスを返信する際，受け取った Via フィールドをそのままヘッダに記述する。そして，Via フィールドの最上位に格納されたホストにレスポンスを返す。

SIP サーバはレスポンスを中継する前に，Via フィールドの最上位を削除する。つまり，自分が付与した行を削除することになる。その結果新たに最上位となった Via フィールドは，SIP サーバがレスポンスを返す相手を示している。

Via フィールドについて，平成 20 年午後Ⅱ問 2 で出題された



図：Via フィールドの加除

2.4.2 VoIP ネットワーク

自社の内線 IP 電話網は，IP-PBX に SIP サーバの役割をもたせることで構築できる。

公衆 IP 電話網と自社の内線 IP 電話網を接続するには，二つの SIP ネットワークを接続する **VoIP ゲートウェイ**（以下，VoIP GW と称する）が必要となる。

以下，公衆 IP 電話網と自社の内線 IP 電話網を例に取り上げ，VoIP ネットワークをどのように設計するかを解説する。ここでは，自社電話機を識別するための 050 電話番号は，公衆 IP 電話網の通信事業者から割り当てられるものとする。

● VoIP GW の役割

VoIP GW は，自社の内線 IP 電話網と公衆 IP 電話網との境界に位置している。

自社の内線 IP 電話網の中に SIP サーバ（IP-PBX）が存在し，通信事業者の公衆 IP 電話網の中にも SIP サーバが存在する。それゆえ，VoIP GW は，B2BUA（Back-to-Back User Agent）になる。

B2BUA とは，一方の SIP ネットワーク側では着呼側，他方の SIP ネットワーク側では発呼側として振る舞う。つまり，両方の SIP ネットワークに対して UA として振る舞う特殊な UA である，

VoIP GW は，SIP ネットワークの境界に存在してセッション生成を仲介するとともに RTP パケットの中継も行う Session Border Controller（以下，SBC と称する）と呼ばれる機能をもつ。

自社電話機は，起動後，IP-PBX に対し，SIP URI と IP アドレスの対応付けを事前に登録しておく。

同様に，B2BUA も，二つの SIP ネットワークの SIP サーバに対し，SIP URI と IP アドレスの対応付けを事前に登録しておく。つまり，IP-PBX，公衆 IP 電話網の SIP サーバのそれぞれに対して行う。

●シーケンスの具体例

例として，公衆 IP 電話網の VoIP 対応電話機から，自社電話機に電話をかける場面を取り上げる。

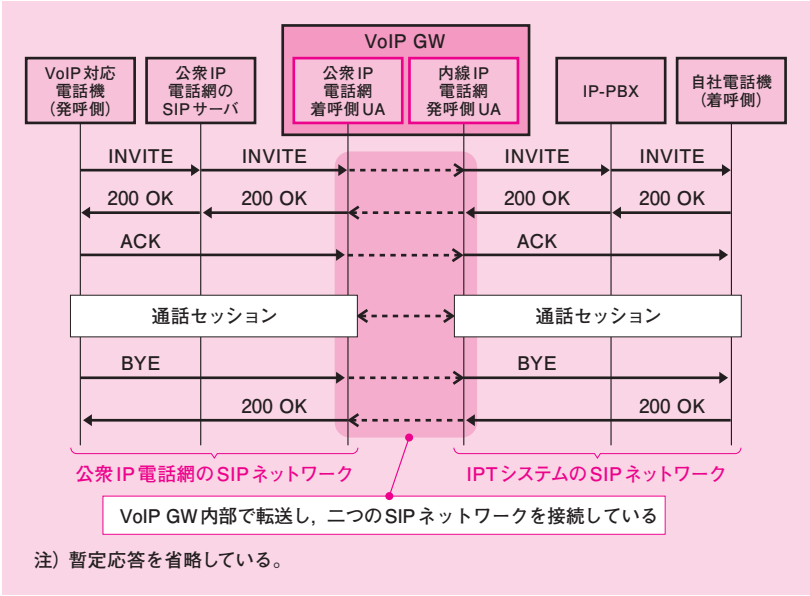
電話をかける以上，公衆 IP 電話網の利用者は，着呼する相手の 050 電話番号を知っている。この電話番号は通信事業者が自社に払い出したものなので，通信事業者は，公衆 IP 電話網経由で自社の SIP ネットワークに接続すればよいことを把握している。

前述のとおり，公衆 IP 電話網の SIP サーバに対し，自社の SIP URI（自社に払い出された 050 電話番号）と IP アドレス（VoIP GW の IP アドレス）の対応付けを事前に登録しているので，公衆 IP 電話網から自社に電話をかけることができる。

自社電話機から社外に電話をかけるときは，逆方向にして考えればよい。内線 IP 電話網から見ると，公衆 IP 電話網の UA は，VoIP GW になっている。IP-PBX には VoIP GW を UA として事前に登録してあるので，内線 IP 電話網から社外に電話をかけることができる。

試験に出る

B2BUA について，平成 28 年午後Ⅱ問 1，平成 26 年午後Ⅱ問 2 で出題された



図：公衆 IP 電話網から自社電話機に電話をかけるときのシーケンス

●NAT に起因する問題

自社電話機（VoIP 対応電話機）に割り当てられている IP アドレスは，プライベート IP アドレスである。

インターネット網を経由して，SIP を使った通話を行う場合，アドレス変換を行う必要がある。このとき，標準的な NAT 装置では，通話セッションが生成できないという問題が発生する。

平成 26 年午後Ⅱ問 2 でこの点が出題されたので，出題例の紹介を兼ねて解説する。

まず，SIP メッセージの中に，発信元 UA の IP アドレスが含まれている点について述べる。

「● SIP のシーケンス（SIP サーバを用いる場合）」で解説したとおり，着呼側 UA は，INVITE リクエストを受信する。その SIP メッセージに記載された発信元 IP アドレスの情報から，発呼側 UA の IP アドレスを知ることができる。

発呼側 UA は，200 OK レスポンスを受信する。その SIP メッセージに記載された発信元 IP アドレスの情報から，着呼側 UA の IP アドレスを知ることができる。

通話セッションで用いるIPアドレスは，このときに通知し合った発信元IPアドレスである。

次の図は，セッション生成開始時に使われるINVITEリクエストの内容例を示したものである。

```
INVITE sip:050yyyy1234@example.ne.jp;user=phone SIP/2.0                    ← 先頭行
Via: SIP/2.0/UDP （発信元のIPアドレス）:5060;branch=（省略）                  ┐
Max-Forwards: 70                                                           │
From: <sip:050yyyy5678@example.ne.jp>;tag=（省略）                          │
To: <sip:050yyyy1234@example.ne.jp;user=phone>                             │ SIPヘッダ
Call-ID: （省略）                                                          │
CSeq: （省略） INVITE                                                      │
Contact: <sip:050yyyy5678@（発信元のIPアドレス）>                           │
Content-Type: application/sdp                                              │
Content-Length: （省略）                                                   ┘
                                                                           ← 空白行
v=0                                                                        ┐
o=- （省略） （省略） IN IP4 （発信元のIPアドレス）                          │
s=-                                                                        │ ボディ
c=IN IP4 （発信元のIPアドレス）                                            │ （SDP）
t=0 0                                                                      │
m=audio 5090 RTP/AVP 0                                                     │
a=rtpmap:0 PCMU/8000                                                       ┘
```

注記　yyyyは，URIの利用者識別子の一部を構成する数字を表す。

図：INVITEリクエストに記載されている発信元IPアドレス（平成26年午後Ⅱ問2の図3より作成）

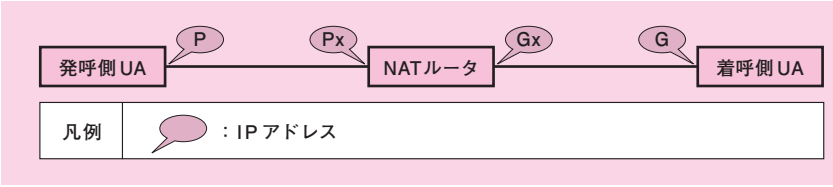
この図を見ると，SIPメッセージのヘッダとボディの随所に，発信元のIPアドレスが記載されていることが分かる。通話セッションに入ると，着呼側が送信するRTPパケットの宛先IPアドレスは，このINVITEリクエストに記載された発信元IPアドレスとなる。

SIPメッセージに発信元UAのIPアドレスが含まれていることが分かったところで，次に，NATに起因する問題について解説する。

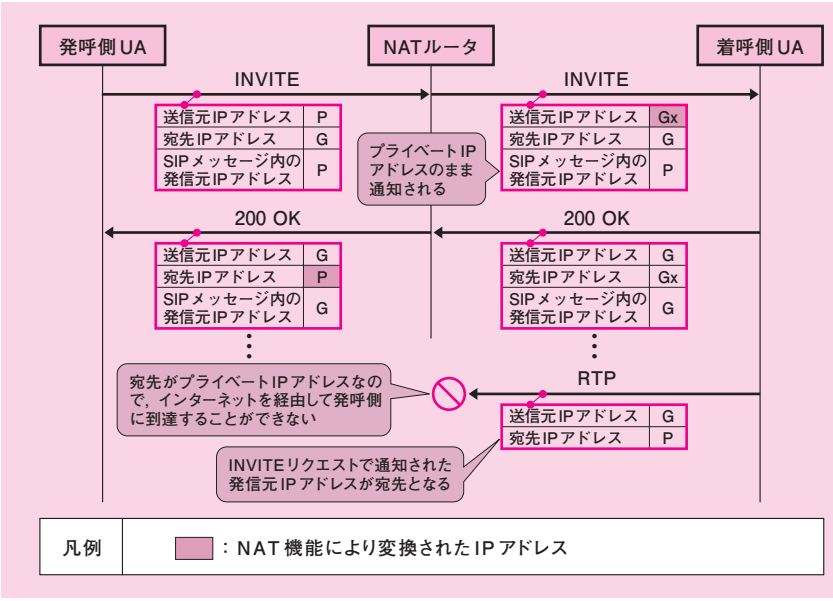
ここでは，発呼側UAがプライベートIPアドレスをもち，着呼側UAがグローバルIPアドレスをもつものとして，SIPのセッション生成，RTPの通話のシーケンスを考察してみる。

NAT機能をもつルータ（以下，NATルータという）を経由した通信を，次の図に示す。構成図にIPアドレスを割り振ってい

るので，これと対応させながらシーケンスを見ていただきたい。
　なお，この図では暫定応答は省略している。



図：NAT ルータを経由した通信の構成図



図：NAT ルータを経由した通信の動作シーケンス

　この図では，シーケンスを分かりやすく示すため，SIP サーバを仲介せず，発呼側 UA は着呼側 UA の IP アドレスを知っているものとする（SIP サーバを用いる場合でも，シーケンスの本質は同じである。発呼側 UA から送信された SIP パケットは，最終的に着呼側 UA に到達する。両者の間に SIP サーバが介在していようがいまいが，そのことに変わりはないからだ）。
　発呼側 UA から送信されたパケットが NAT ルータを通過すると，送信元 IP アドレスがグローバル IP アドレスに変換される。

しかし，SIP メッセージに記載された発信元 IP アドレスは，NAT ルータのアドレス変換の対象ではない。したがって，発呼側 UA のプライベート IP アドレスのまま，着呼側 UA に通知されてしまう。

通話セッションで用いる IP アドレスは，セッションの生成時に通知し合った発信元 IP アドレスである。したがって，着呼側 UA から見ると，通話セッションの相手の IP アドレスは，発呼側 UA のプライベート IP アドレスとなる。それゆえ，着呼側 UA から送信した RTP パケットは，宛先がプライベート IP アドレスなので，インターネットを経由して発呼側 UA に到達することができない。

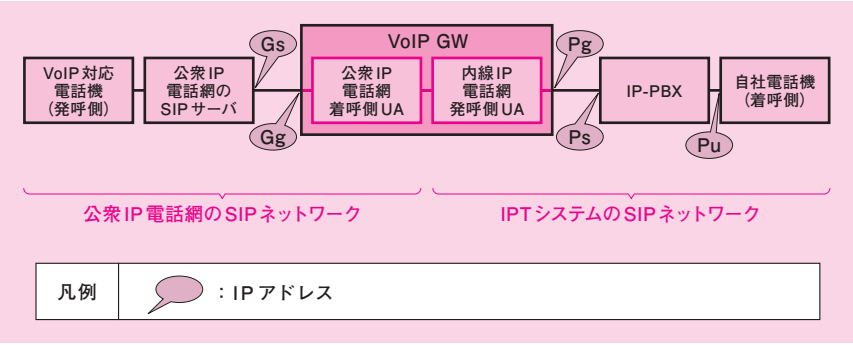
●NAT トラバーサル

NAT に起因する問題は，VoIP GW の「NAT トラバーサル」の機能を使って解決する。

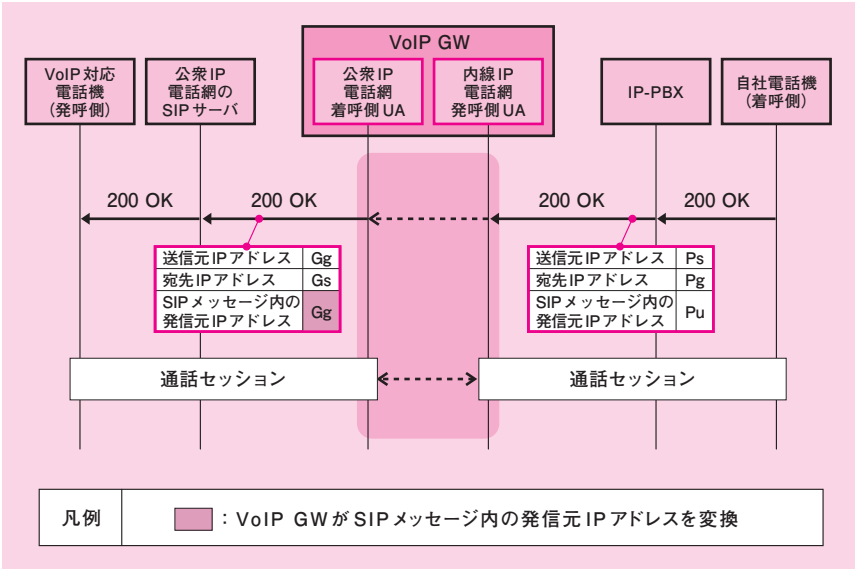
「● VoIP GW の役割」で解説したとおり，VoIP GW は，両方の SIP ネットワークに対して UA として振る舞う特殊な UA である B2BUA になる。VoIP GW は，SIP ネットワークの境界に存在してセッション生成を仲介するとともに RTP パケットの中継も行う。

公衆 IP 電話網と内線電話網を接続する場合の，VoIP GW を経由した通信を，次の図に示す。

構成図に IP アドレスを割り振っているので，これと対応させながらシーケンスを見ていただきたい。なお，この図では暫定応答は省略している。



図：VoIP GW を経由した通信の構成図



図：VoIP GW を経由した通信の動作シーケンス

VoIP GW は，内線 IP 電話網の側から受け取った 200 OK レスポンスの SIP メッセージを，そのまま転送しているのではない。そこに記載された発信元 IP アドレスは，内線 IP 電話網の着呼側 UA（自社電話機）のアドレスなので，プライベート IP アドレスになっている。このまま転送するなら，通話セッションに失敗してしまう。そこで，200 OK レスポンスの SIP メッセージ内の発信元IPアドレスを，自分自身のグローバルIPアドレスに変換する。このアドレスは，公衆 IP 電話網の側からは着呼側 UA のアドレスになっているので，通話セッションに成功する。

内線 IP 電話網において，VoIP GW は発呼側 UA として振る舞う。今度は，自分自身のプライベート IP アドレスを，INVITE リクエストのメッセージ内で着呼側 UA に通知している。詳しいシーケンスは省略する。

VoIP GW が SIP メッセージの変換も行うことで，二つの SIP ネットワークにおいて，通話セッションを成立させている。この通話データを中継することで，公衆 IP 電話から自社電話機に電話をかけることができる。