《基礎編》第1章

LAN

この章ではイーサネットや無線 LAN などの LAN 関連の技術について解説する。さらに，フロー制御や VLAN といった LAN 関連のプロトコル／規格，スイッチの機能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，しっかりと学習しておく必要がある。

1.1 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。

1.1.1 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を含め，網羅的に出題例を掲載している。併せて参照していただきたい。

●イーサネット

基本となる要素技術であるが，午後試験では目立った出題例がない。基礎知識を問う穴埋め問題が幾つか存在する程度だ。

近年では，**拡張イーサネット**（SAN と LAN の統合），**オーバレイネットワーク**（レイヤ 3 のネットワーク上にレイヤ 2 のネットワークを構成），等の新技術の出題例がある。

出題例	内容
平成 27 年午後Ⅱ問 2	・マルチキャストと VXLAN を用いたオーバレイネットワークの構築（設問 5 のみ）
平成 25 年午後Ⅱ問 2	・VXLAN を用いたオーバレイネットワークのトンネリング技術（設問 1（2）のみ） （本問は全体として OpenFlow 技術が出題されており，オーバレイネットワークはその比較として軽く触れている程度である）
平成 24 年午後Ⅱ問 1	・フレームの解析，転送処理（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

ただし，これら新技術を出題する場合，その仕組みや動作を理解できるよう，問題本文の中で詳しく説明されている。つまり，特別な前提知識を必要としないよう，従来の要素技術の知識に基づいて解くことができるように，配慮されている。ここで問われているのは，本文中に説明された仕組みや動作を理解する能力，具体的な状況に適用する能力である。本書の第 1 章「1.1　午後試験の出題と試験対策のポイント」で述べたとおり，新技術を題材とする問題は，「応用問題」として作成されているわけだ。

したがって，それら新技術の出題傾向が近年見られるからと言って，これらを急いで勉

強する必要はない。むしろ，従来の要素技術をまずはしっかり学習することが先決である。どこかで時間を取って，新技術を題材とした過去問題を実際に解いてみることをお勧めする。前述のとおり，従来の要素技術の知識で解けるように配慮されていることを実感できるし，それら要素技術を学習することの大切さも改めて認識できるだろう。

拡張イーサネットは，ストレージネットワークと従来の IP ネットワークの統合を実現する技術である。ストレージネットワークは重要な要素技術であるため，《基礎編》第 2 章「2.2 ストレージネットワーキング」で解説しており，FC-SAN，IP-SAN と共に，拡張イーサネットについても取り上げている。出題傾向，学習ポイントについても，《基礎編》第 2 章を参照していただきたい。

オーバレイネットワークについては，本書の過去問題解説（Web に掲載）の中で，仕組みや動作を詳しく説明している。必要に応じて参照していただきたい。

●無線 LAN

複数のアクセスポイントが登場し，それらを無線 LAN コントローラで制御する事例がしばしば登場する。その中で，ローミング，**IEEE802.1X** を利用した認証などが出題されている。他には，IEEE802.11n と IEEE802.11a/g との**混在環境**が登場し，新しい伝送規格で採用された要素技術や，衝突を回避する方式などが出題されている。

表：無線 LAN 技術に関する出題例

出題例	内容
平成 29 年午後Ⅱ問 2 平成 25 年午後Ⅱ問 1	・IEEE802.1X の事前認証，PMK キャッシュ ・無線 LAN コントローラを使用したローミング ・AP の配置
平成 24 年午後Ⅰ問 2	・無線 LAN コントローラの導入に伴うトラフィック経路の分析，性能要件の再検討
平成 24 年午後Ⅰ問 3	・IEEE802.11n のチャネルボンディング，MIMO ・IEEE802.11a/g/n 混在環境の衝突回避（IEEE802.11n 端末がプリアンブルを付加）
平成 21 年午後Ⅱ問 1	・IEEE802.1X 認証（EAP-TLS）のシーケンス ・隠れ端末問題の解決のため，及び，IEEE802.11b/g 混在環境の衝突回避のために，CSMA/CA の RTS/CTS 方式を用いる
平成 21 年午後Ⅰ問 1	・バーチャル AP 機能（ESS ID ごとに VLAN を登録）

●LAN 関連のプロトコル／規格

LAN 関連の規格のうち，**VLAN** は必須の知識である。VLAN を使って構築されたネットワークの出題例は，枚挙にいとまがないからだ。

VLAN の出題例は多数ある。そこで，試験対策として重要なものに絞り，比較的難易度

が高く，かつ，今後とも出題される可能性の高いトピックを扱った出題例を幾つか挙げる。

表：LAN 関連のプロトコル／規格に関する出題例

出題例	内容
平成 25 年午後 I 問 3	・IEEE802.1Q トンネリング技術（VLAN の知識を前提とした応用問題）
平成 24 年午後 II 問 2	・MSTP（VLAN ごとにスパニングツリーを構成する技術）を用いた設計
平成 23 年午後 I 問 3	・通信条件を満たすように，VLAN をポートに割り当てる設計
平成 21 年午後 I 問 1	・バーチャル AP 機能（ESS ID ごとに VLAN を登録）

●スイッチ

スイッチがもつ機能のうち，アドレス学習機能と転送機能は，基本となる要素技術である。フェールオーバ時に MAC アドレステーブルを更新することや，MAC アドレステーブルがクリアされたときの動作など，応用問題が出題されている。

スイッチのほかの機能に関しては，ミラーリング機能の出題例が比較的多い。

表：スイッチに関する出題例

出題例	内容
平成 27 年午後 I 問 3	・IDS でパケットを収集するため，IDS を収容している SW のポートをミラーリングポートに設定し，IDS 側のネットワークポートをプロミスキャスモードに設定する
平成 27 年午後 II 問 2	・マルチキャストフレームはフラッディングされる ・IGMP スヌーピング機能を使用したときの，MAC アドレステーブルの推移（本文から推論する応用問題）
平成 26 年午後 I 問 2	・冗長構成において，主系から待機系に切り替わったときに MAC アドレステーブルを更新する必要がある
平成 26 年午後 II 問 2	・ミラーリング機能を利用したフレームの収集（仮想化技術との組合せ）
平成 24 年午後 II 問 2	・障害発生に伴ってスパニングツリーが再構築されると，スイッチの MAC アドレステーブルがクリアされる。その結果，ユニキャストフレームがフラッディングされる

1.1.2 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。

●無線 LAN

複数のアクセスポイントを使用する事例では，**ローミング**を行ったり，**電波干渉**を解消し

たりする必要がある。そのような課題を解決するために，要素技術がどのように使用されているかについて，学習しておく必要がある。

今日の AP は，基本となるブリッジ機能だけでなく，様々な機能をもっている。近年では無線 LAN コントローラを使用する事例も増えている。こうした技術動向を踏まえ，試験では，様々な機能をもつ AP や無線 LAN コントローラが登場している。本章の「1.3.3　AP と無線 LAN コントローラ」に代表的な機能をまとめているが，余力があれば，自分でも情報収集してみることをお勧めする。

IEEE802.11n が平成 24 年午後 I 問 3 で出題されていることを踏まえ，IEEE802.11ac についても，特徴を押さえておきたい。併せて，旧来の伝送規格との**混在環境**で衝突を回避する方式についても学習するとよい。

IEEE802.1X 認証をはじめとするセキュリティは出題頻度が高いので，学習するとよい。なお，セキュリティについて，詳しくは本書の第 4 章を参照していただきたい。

●LAN 関連のプロトコル／規格

VLAN 自体の知識習得は易しいが，試験対策としては，VLAN を使った設計について学習しておく必要がある。

本章で基礎知識を学習した後，VLAN が登場する出題例を読み，実際にどのように使われているか調べてみることをお勧めする。具体的に言うと，仮想化設計，LAN の信頼性設計，IEEE802.1X 認証スイッチを使った設計などに，VLAN が登場する。

仮想化設計については本書の第 1 章「1.2　仮想化設計」，信頼性設計については本書の第 2 章「2.2　冗長化構成」，IEEE802.1X については本書の第 4 章「4.4.3　IEEE802.1X」を，それぞれ参照していただきたい。

●スイッチ

今日のスイッチは，基本となるアドレス学習機能，転送機能だけでなく，様々な機能をもっている。本章の「1.5　スイッチ」に様々な機能をまとめているので，学習しておく必要がある。

機能自体の知識習得は易しいが，試験対策としては，応用問題を解けるように準備しておく必要がある。「1.5　スイッチ」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。

1.2 イーサネット

現在のLANにおいてイーサネットは不可欠な技術である。試験対策としては，DIX規格のフレームフォーマットを押さえておくとよい。午後試験の出題頻度は低いが，基本的な要素技術なので，しっかり理解しておく必要がある。

1.2.1 イーサネットの種類と仕様

イーサネットは，1973年にXerox社パロアルト研究所（Palo Alto Research Center）のRobert Metcalfe氏らによって，その原型が考案された。その後，Xerox社はDEC社（現：Hewlett-Packard社），Intel社とともに，1980年にCSMA/CDをアクセス制御方式とするDIX規格イーサネット（イーサネット1.0）を発表した。1980年2月にIEEE802委員会が設立され，翌年にイーサネットの標準化を審議するIEEE802.3ワーキンググループが発足した。以来，同グループは，10Mビット／秒，100Mビット／秒，1Gビット／秒，10Gビット／秒の伝送速度で動作する規格を次々に標準化していった。

一方，先の3社は1982年にDIX規格イーサネット（イーサネット2.0）を発表した。DIX規格とIEEE802.3規格は，フレーム構造や信号線のオプションなどが異なっているが，同一の媒体で両者を混在させることが可能である。

現在，普及しているのはDIX規格イーサネット2.0であり，本書ではこちらの規格を中心に解説していく。したがって，特に断りがない限り，本書では「イーサネット」という語はDIX規格イーサネット2.0を指すものとする。

● 規格の表記

イーサネットは，伝送速度，伝送方式，伝送媒体ごとに様々な規格が定められている。それらの規格を次の表に示す。

参考

IEEE

米国電気電子学会（The Institute of Electrical and Electronics Engineers, Inc.）は，電気・電子分野で世界最大の学会である。「アイトリプルイー」と呼ぶ。ISOのような公的な標準化団体ではないが，様々な規格を標準化している。例えば，情報通信技術分野では，本章で取り上げる有線LANや無線LANの規格を定めたIEEE802等が有名である

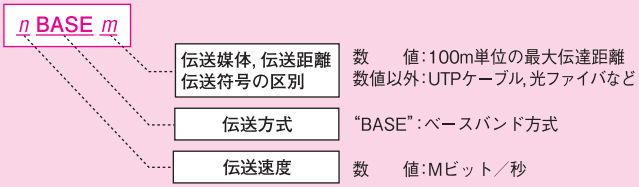
参考

IEEE802

LAN（Local Area Network），MAN（Metropolitan Area Network），PAN（Personal Area Network）の通信技術を定めた規格群（規格ファミリ）である。

IEEE802規格ファミリはIEEE802標準化委員会が管理しているが，標準化活動は下部組織に当たるワーキンググループ（WG：Working Group）が主体的に行っている。例えば，イーサネットの規格を標準化しているのは，IEEE802.3ワーキンググループである。

802という名称は，1980年2月に発足したことからその名が付いた



図：IEEE802.3 の規格の表記

表：標準化規格とその内訳（イーサネット規格）

タスクフォース名／標準化規格	主なイーサネット規格	制定年
IEEE802.3i	10BASE-T	1990 年
IEEE802.3u	100BASE-TX，100BASE-FX	1995 年
IEEE802.3z	1000BASE-SX，1000BASE-LX，1000BASE-CX	1998 年
IEEE802.3ab	1000BASE-T	1999 年
IEEE802.3ae	10GBASE-SR/SW，10GBASE-LR/LW，10GBASE-ER/EW，10GBASE-LX4	2002 年

表：イーサネット規格（ツイストペアケーブル）

	10BASE-T	100BASE-TX	1000BASE-T
伝送速度	10M ビット／秒	100M ビット／秒	1G ビット／秒
伝送符号	マンチェスタ符号	4B/5B+MLT-3	8B1Q4
伝送媒体	UTP カテゴリ 3，4，5	UTP カテゴリ 5	UTP カテゴリ 5 エンハンスト
最大伝達距離	100m	100m	100m

表：イーサネット規格（光ファイバ）

	100BASE-FX	1000BASE-SX	1000BASE-LX
光波長	1300nm	850nm	1300nm
伝送符号	4B/5B+NRZI	8B/10B	8B/10B
伝送媒体	光ファイバ（マルチモード）	光ファイバ（マルチモード）	光ファイバ(マルチモード，シングルモード)
最大伝達距離	2km	550m※	550m(マルチモード)※ 5km(シングルモード)

※光ファイバの種類により異なる

●プロトコル階層

イーサネットは，物理層とデータリンク層を規格化した仕様である。一方，IEEE802.3 は，データリンク層を **LLC**（Logical Link Control，論理リンク制御）副層と **MAC**（Media Access Control，媒体アクセス制御）副層の二つの副層に分け，物理層と MAC 副層の仕様を規格化している。LLC 副層は IEEE802.2 で規格化されており，トークンリングなど CSMA/CD 以外のアク

セス制御の伝送手順をサポートする機能をもつ。

●CSMA/CD

イーサネットが規格化された当初は**媒体共有型**のネットワークだったため，同時に複数のステーションがフレームを送信すると信号が衝突してしまい，通信できなくなってしまう。あるステーションが送信している間に別のステーションが送信しないようにするため，イーサネットはCSMA/CD方式で通信を制御している。

今日ではスイッチが一般的に使用されており，媒体共有型のネットワークではないため，全二重通信が可能である。したがって，CSMA/CD方式による制御は事実上行われていない。とはいえ，午前試験で出題されることがあるので，基礎知識として習得しておく必要がある。

CSMA/CD（Carrier Sense Multiple Access ／ Collision Detection，搬送波感知多重アクセス／衝突検出）方式の通信は，次の手順に従って行われる。

1. 送信ステーションは，伝送媒体のキャリア信号を監視し，ほかのステーションが送信中かどうかを確認する（搬送波感知）。ほかのステーションが送信中のときはキャリア信号がなくなるのを待ち，フレームギャップ時間（96ビット長の送信にかかる時間）が経過した後に，搬送波感知を再開する。
2. 送信ステーションは，フレームの送信を開始する。

複数のステーションがほぼ同時にフレームを送信すると，衝突が発生する。フレームの送信中に衝突を検出したときは，次の手順に従う。

3. フレームの送信を中断する。
4. ジャム信号を一定時間（32ビット長の送信にかかる時間）送信し，全てのステーションが確実に衝突を検知できるようにする（衝突又はジャム信号を検出したハブは，全てのポートからジャム信号を送信する）。
5. 送信ステーションは，バックオフ時間（乱数に従った待ち

試験に出る

CSMA方式のLAN制御について，平成24年午前Ⅱ問6，平成21年午前Ⅱ 問3，平成18年午前 問40，平成16年午前 問38で出題された

参考

データリンク層では，「ホスト」のことを「ステーション」や「端末」と表記するのが一般的である。これらは交換可能な用語だが，本章ではデータリンク層について説明している文脈の中では，「ステーション」を用いる

試験に出る

リピータハブで構築されたネットワークにおける（ただし，衝突が発生しない条件での），LANの利用率について，平成20年午前 問37（平成17年午前 問36は同じ問題）で出題された

時間）が経過するのを待つ。その後，手順 1. に戻る。

ステーション間で伝送媒体を共有している場合，単位時間当たりの送出フレーム数の増加に伴って，衝突頻度が増大する。平均フレーム長が 64 バイトの場合，利用率がおよそ 35 パーセントを超えたあたりから，伝送待ち時間が急激に増加してスループットが低下する。

1.2.2 DIX 規格のフレームフォーマット

インターネットで利用するホストについて定義されている RFC1122 の中で DIX 規格への適合が必須とされていることから，TCP/IP 通信では DIX 規格が利用されている。加えて，フロー制御やリンクアグリゲーションの制御用フレームにも DIX 規格が使用されている。

DIX 規格のフレームフォーマットを次に示す。

(8)	(6)	(6)	(2)	(46〜1500)	(4)
プリアンブル	宛先MAC アドレス	送信元MAC アドレス	タイプ	データ	FCS

注：(　)内の数字はオクテット長を表す。

図：DIX 規格のフレームフォーマット

それぞれの領域の意味を次に示す。

●プリアンブル

フレームを受信するステーションが，送信ステーション側のクロック周波数と同期をとることができるように，ステーションは送信フレームごとに**プリアンブル**を先頭に付加する。プリアンブルのデータ長は 64 ビットで，その中身は 16 進表記で「AA-AA-AA-AA-AA-AA-AA-AB」である。つまり，2 進表記で「10」が連続したストリーム（1010…）が 62 ビットにわたって送信された後に「11」が送信される。最後の 2 ビット「11」は，プリアンブルの切れ目を表しており，**SFD**（Start Frame Delimiter）という。

試験に出る

DIX 規格のフレームのフォーマットについて，平成 16 年午後I 問 1 で出題された

関連RFC

RFC1122：ネットワーク階層に関するインターネットホストに対する要求仕様
RFC894：DIX 規格にカプセル化して IP データグラムを転送する標準
RFC1042：IEEE802 規格にカプセル化して IP データグラムを転送する標準

参考

IANA

Internet Assigned Numbers 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。標準化団体である IANA に OUI が割り当てられている理由は，宛先 IP アドレスがマルチキャストであるとき，宛先 MAC アドレスは，特殊なマルチキャストアドレスになるからである。この MAC アドレスの上位 3 バイトが，IANA の OUI になる

●宛先 MAC アドレス／送信元 MAC アドレス

プリアンブルの直後に「宛先 MAC アドレス」「送信元 MAC アドレス」が続く。MAC アドレスはステーションを識別するアドレスで，イーサネットアドレス，もしくはステーションアドレスとも呼ばれ，6 バイト（48 ビット）で構成される。

前半の 3 バイトは **OUI**（Organizationally Unique Identifier，管理組織識別子）である。これは組織（製造メーカや標準化団体など）に固有の ID であり，IEEE によって管理されている。例えば，IANA の OUI は「00-00-5E」である。

後半の 3 バイトは，イーサネットインタフェースごとに固有な番号がベンダによって割り振られる。

さらに，上位 1 ビット目の I/G ビット，上位 2 ビット目の G/L ビット，上位 25 ビット目の I ビットが規格化されている。I ビットは OUI が IANA の場合に使用される。

参考

G/L ビットは U/L ビット（Universal/Local）とも呼ばれる

表：I/G ビット，G/L ビット，I ビット

	0 のとき	1 のとき
I/G ビット ※	単独のステーションアドレス	マルチキャストアドレス
G/L ビット ※	グローバル（IEEE 管理）	ローカル
I ビット	インターネット／マルチキャスト	それ以外

※ I/G は「Individual/Group」を，G/L は「Global/Local」を意味している。

全てのビットを「1」にセットした「FF-FF-FF-FF-FF-FF」は，**ブロードキャストアドレス**で，全てのイーサネットインタフェースに送信するときに用いられる。

宛先がマルチキャスト IP アドレスである IP データグラムをペイロードにもつイーサネットフレームは，その宛先 MAC アドレスがマルチキャスト MAC アドレスになる。

宛先がマルチキャスト IPv4 アドレスであるとき，宛先 MAC アドレスの上位 3 バイトは，IANA の OUI を指定した上で，I/G ビットを「1」に，G/L ビットを「0」にセットする。次いで，I ビットを「0」にセットする。残った下位 23 ビットは，IPv4 アドレスの下位 23 ビットをそのまま埋め込む。

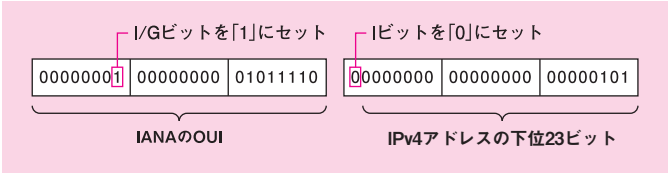
宛先がマルチキャスト IPv6 アドレスであるとき，宛先 MAC アドレスの上位 2 バイトは，「33-33」を指定する。下位 4 バイトは，IPv6 アドレスの下位 4 バイトをそのまま埋め込む。

例えば，OSPF ルータが宛先であることを示す「224.0.0.5」と

試験に出る

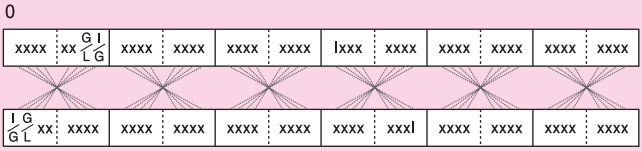
IP パケットの宛先がマルチキャスト IP アドレスであるとき，イーサネットフレームの宛先がマルチキャスト MAC アドレスになることについて，平成 27 年午後 II 問 2 で出題された

いうマルチキャスト IPv4 アドレスの場合，宛先 MAC アドレスは，「01-00-5E-00-00-05」となる。



図：IPv4 マルチキャストアドレスを MAC アドレスにマッピングする方法

イーサネットではバイト内のビット伝送は **LSB**（Least Significant Bit，最下位ビット）から **MSB**（Most Significant Bit，最上位ビット）の順に行われる（通常のパラレル→シリアル伝送も同様）。よって，第 1 バイトの LSB である I/G ビットから伝送されることになる。



図：MAC アドレスのバイナリ表記と伝送順序の違い

●タイプ

タイプ領域は，上位層のプロトコル種別を表している。その代表例を次に示す。

表：タイプ領域の代表例

タイプ（16 進表示）	意　味
0x0000 ～ 05DC	IEEE802.3 規格のデータ長（DIX 規格では未使用）
0x05DD ～ 05FF	未使用
0x0800	IPv4
0x86DD	IPv6
0x0806	ARP
0x8035	RARP
0x8100	IEEE802.1Q（VLAN）
0x8808	IEEE802.3x（フロー制御）
0x8809	IEEE802.3ad（リンクアグリゲーション）
0x8137	PPPoE Discovery Stage
0x8864	PPPoE Session Stage

試験に出る

「タイプ」領域の名称を記述する問題が，平成 16 年午後I 問 1 で出題された

試験に出る

CRC（巡回冗長検査）は，平成 16 年午前 問 31 で出題された

● FCS

FCS（Frame Check Sequence，フレームチェックシーケンス）は，宛先 MAC アドレスからデータ領域までのビット列に基づいて生成される，誤り検出用のデータである。このデータ生成には 32 ビットの CRC（巡回冗長検査）が用いられている。受信ステーションは FCS を用いて誤りを検出し，正常であれば上位層にデータを渡す。誤りがあればフレームを破棄し，再送要求は行わない。

1.2.3 IEEE802.3 規格のフレームフォーマット

MAC フレームには，DIX 規格のほかに，フレームフォーマットの異なる **IEEE802.3 規格**がある。スパニングツリープロトコルの **BPDU フレーム**（IEEE802.1D）など，TCP/IP 以外の通信では IEEE802.3 規格が使用されている。

IEEE802.3 規格のフレームフォーマットを次に示す。DIX 仕様との相違点は，「プリアンブル」領域が「プリアンブル」と「SFD」に分かれていること（ただし，ビット配列は同じ），「タイプ」領域が「データ長」に置き換わっていること，「データ」領域に LLC ヘッダが含まれていることである。

(8)	(6)	(6)	(2)	(46～1500)	(4)
プリアンブル／SFD	宛先MACアドレス	送信元MACアドレス	データ長	LLCヘッダ＋データ	FCS

注：（　）内の数字はオクテット長を表す。

図：IEEE802.3 規格のフレームフォーマット

Column ▶▶▶

DIX 規格フレームと IEEE802.3 規格フレームの同時使用

IEEE802.3 規格では，データ長の領域に設定される最大値は 1,500 バイトであり，これを 16 進数で表すと「0x05DC」となる。一方，DIX 規格では，タイプ領域に設定される値は「0x0600」以上のものが規定されている。したがって，IEEE802.3 規格と DIX 規格は一つの LAN に混在していたとしても，両者を区別できるため併用が可能である。

1.2.4 IEEE802.2 規格のフレームフォーマット

IEEE802 ワーキンググループは，データリンク層を上位の LLC（Logical Link Control）と下位の MAC（Media Access Control）の二つの副層に分け，別々に標準化している。

LLC 副層は **IEEE802.2** で規格化されており，メディア（物理媒体）に依存することなく，同じ手順でデータ転送を行う機能を提供している。つまり，メディアの違いを吸収して，上位層（ネットワーク層）から統一的に扱えるよう，LLC 副層が設けられている。

MAC 副層は，上位層（LLC 副層）で規定された手順に従い，物理媒体を制御してビット転送を行う機能を提供する。イーサネット（IEEE802.3）や無線 LAN（IEEE802.11）は，MAC 副層と物理層について規定している。MAC 副層の規定には，メディアアクセス制御である CSMA/CD などがある。物理層の規定には，CSMA/CD で使用するケーブルの仕様などがある。

●LLC ／ SNAP カプセル化

LLC は IEEE802.2 で標準化され，データリンクサービス（コネクション型又はコネクションレス型）を上位層へ提供する機能を有する。次の 3 種類が規定されており，イーサネット（IEEE802.3），無線 LAN（IEEE802.11）では「タイプ 1」が使用されている。

表：LLC タイプ

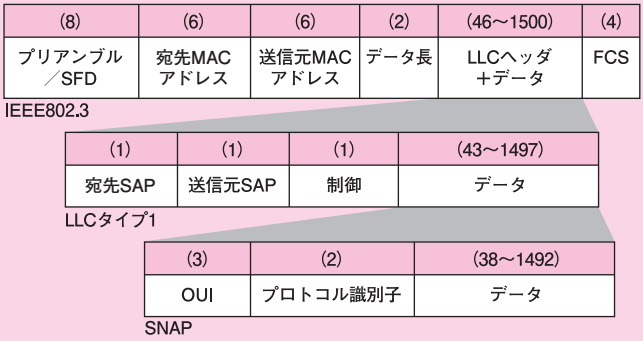
タイプ	サービス	内　容
1	コネクションレス型サービス	単純なベストエフォートのサービス
2	コネクション型サービス	HDLC を基に規格化された，コネクション型のサービス
3	確認応答コネクションレス型サービス	コネクションレス型なので，コネクションの確立，再送制御，フロー制御を行わないが，確認応答をサポートするサービス

LLC は SAP（Service Access Point）識別子を用いることで，ステーション内の DTE（Data Terminal Equipment，データ端末装置）を識別する。宛先 SAP（DSAP：Destination SAP）は宛先ステーションに複数の DTE がある場合の端末番号で，送信元 SAP（SSAP：Source SAP）は送信元ステーションに複数の DTE がある場合の端末番号である。

しかし，SAP 領域は長さが 1 バイトであるため，識別できる数が最大 256 種に限られている。そこで，より多くのサービスを指定できるよう，SNAP（Sub-Network Access Protocol）によるカプセル化が行われている。RFC1042 では，IEEE802.3（DIX 仕様は除外），IEEE802.4 及び IEEE802.5 で IP データグラムと ARP フレームを伝送する際，SNAP カプセル化を使用しなければならないと規定している。

SNAP でカプセル化する場合，DSAP と SSAP の値を「0xAA」に設定する。このとき，LLC 制御フィールドに続く 5 バイトが，SNAP の二つのフィールドとして解釈される。

LLC タイプ 1 SNAP のフレームフォーマットを次に示す。



注:(　)内の数字はバイト長を表す。

DSAP SSAP	スパニングツリーのBPDUは0x42。 IPデータグラム, ARPフレームは0xAA（SNAPカプセル化）
制御	BPDU, IPデータグラム, ARPフレームはHDLCプロトコルのUI（Unnumbered Information）に相当するため, 0x03
OUI	Organizationally Unique Identifier。後続のプロトコル識別子が属する組織を示す。IPデータグラム, ARPフレームは00-00-00
プロトコル識別子	上位層のプロトコルを示す。OUIが00-00-00の場合, DIX仕様のタイプと同じ値が採用される。 IPデータグラムは08-00, ARPフレームは08-06

図：LLC タイプ 1 ／ SNAP のフレームフォーマット

Column

予約されたマルチキャストアドレス

IEEE802.1D 規格と IEEE802.1Q 規格は，01-80-C2-00-00-00 ～ 0F のマルチキャストアドレスグループを，特殊な用途に割り当てている。一例を次の表に示す。ここに掲載したマルチキャストアドレスを宛先とするフレームは，一部の例外を除き，フラッディングしないことが定められている。

詳しくは，下記の URL に掲載されている。

http://standards.ieee.org/develop/regauth/grpmac/public.html

表：予約されたマルチキャストアドレスの例

アドレス	用　途
01-80-C2-00-00-00	STP（スパニングツリープロトコル：IEEE802.1D）（本書の第 2 章を参照）
	MSTP（IEEE802.1s）
	RSTP（IEEE802.1D:2004（旧 IEEE802.1w））
01-80-C2-00-00-01	IEEE802.3x の PAUSE フレーム
01-80-C2-00-00-02	スロープロトコル
	IEEE802.3ad の LACP（Link Aggregation Control Protocol）（本書の第 2 章を参照）
	IEEE802.3af の OAM（Operations, Administration, and Maintenance）
01-80-C2-00-00-03	IEEE802.1X（本書の第 4 章を参照）
	隣接するブリッジ間でやり取りされるマルチキャストフレーム ブリッジはこれをフラッディングしない （ただし，Two-Port MAC Relay は，このフレームを転送する）

さらに，「DIX 規格のフレームフォーマット」で解説したとおり，「01-00-5E-xx-xx-xx」のマルチキャストアドレスは，IP マルチキャストパケットの転送に用いられる。これもブリッジによってフラッディングされる。

なお，ここに述べたマルチキャストアドレスは全て，I/G ビットが「1:Group」にセットされている。

1.3 無線 LAN

無線 LAN は，屋内の LAN だけでなく，街中での公衆無線 LAN インターネット接続など，至るところで利用されている。しかし，無線という媒体共有型のネットワークであるがゆえに，スループットの低下，通信範囲の制限，通信の傍受などの問題が生じる。それらを克服すべく新しい規格が策定されたり，ベンダ独自の技術が用いられたりしている。

本節では，主に規格の基本知識を解説する。セキュリティは本書の第 4 章を参照していただきたい。無線 LAN 技術は午後試験の設計問題でしばしば登場するので，基本知識をしっかり身に付けて応用問題に対応できるようにしておく必要がある。

1.3.1 無線 LAN の種類と仕様

試験に出る

無線 LAN の導入について，平成 29 年午後Ⅱ問 2，平成 25 年午後Ⅱ問 1 で出題された。無線 LAN の標準規格について，平成 25 年午前Ⅱ問 3 で出題された。
ZigBee について，平成 29 年午前Ⅱ問 1，平成 27 年午後Ⅱ問 2，平成 22 年午前Ⅱ問 1 で出題された。Bluetooth について，平成 19 年午前 問 10，平成 16 年午前 問 21 で出題された。IEEE802.11b/g/a の混在環境，IEEE802.11n について，平成 21 年午後Ⅱ問 2 で出題された

無線 LAN は **IEEE802.11** ワーキンググループにより標準化されている。アクセス制御方式として **CSMA/CA** を採用している点がイーサネットと異なる。

また，半径 10 ～ 20m 以内のパーソナルエリアをターゲットにした **無線 PAN**（PAN：Personal Area Network）があり，**IEEE802.15** ワーキンググループによって標準化されている。無線 PAN の主な規格として，**Bluetooth**（IEEE802.15.1），ZigBee（IEEE802.15.4）がある。

なお本書では，IEEE802.11 を中心に解説しており，特に断りのない限り「無線 LAN」という語は IEEE802.11 を指すものとする。

● 規格の種類

無線 LAN の主な規格を次の表に示す。

表：無線 LAN の主な規格

規格(*1)	策定年	周波数帯	チャネル幅（最大）	空間ストリーム	公称の最大速度
11b	1999	2.4GHz	22MHz	1	11Mbps
11a	1999	5GHz	20MHz	1	54Mbps
11g	2003	2.4GHz	20MHz	1	54Mbps
11n	2009	2.4GHz 5GHz	40MHz(*2)	1 ～ 4	600Mbps
11ac	2014	5GHz	160MHz(*2)	1 ～ 8	6.93Gbps

(*1) 規格の名称は，正式名称から「IEEE802.」を削除した略称である。
(*2) チャネルボンディングを使用した場合。

●IEEE802.11g

IEEE802.11g は，最大伝送速度が 54M ビット／秒であり，2.4 GHz 帯の **ISM バンド**（Industrial Scientific and Medical band，産業科学医療用バンド）を使用する。この帯域は，電子レンジ，医療用加熱機器，さらには Bluetooth 規格の無線機器なども使用しており，混信に対する注意が必要である。混信があると伝送速度が低下したり，最悪の場合には通信できなくなったりする。

IEEE802.11g の周波数帯域は 13 個のチャネルに分かれている。通信を行うステーションは同一のチャネルを使用する。チャネルの周波数帯域は 20MHz あり，約 5Hz ずつ離れている。チャネルの番号が 5 つ離れていれば，チャネル同士の帯域が重なり合うことがないので信号が衝突しない。具体的に言うと，同じ環境に 3 台のアクセスポイントがあり，それらに 1 チャネル，6 チャネル，11 チャネルを割り当てたとき，アクセスポイントの電波が届く範囲がかぶっても衝突は起きない。

●IEEE802.11a

IEEE802.11a は，最大伝送速度が 54M ビット／秒であり，5.2GHz 帯の周波数帯域を使用する。

IEEE802.11a の周波数帯域は 19 個のチャネルに分かれている。使用できるチャネルは元から帯域が重なり合っていないため，19 個のチャネルを同一環境で使用することができる。

IEEE802.11a と IEEE802.11g とは周波数帯が異なるため，直接通信できない。しかし，アクセスポイント（AP）が IEEE802.11a/g の両方に対応している製品なら，アクセスポイントを介してステーション間の通信は可能である。

●IEEE802.11n

IEEE802.11n は，**MIMO**（Multiple Input Multiple Output），**チャネルボンディング**などの採用により，600Mbps の最大伝送速度を実現する規格である。

MIMO とは，複数のアンテナを用いて同時に複数のストリームを通信することで高速化を実現する技術である。

チャネルボンディングとは，隣り合う二つのチャネルを束ねる

IEEE802.11b は，IEEE802.11g と同じ 2.4GHz 帯を使用する。したがって，両規格を同一環境で使用したときに衝突を回避する必要がある。IEEE802.11b と IEEE802.11g の混在環境において，衝突を回避する方式には幾つかある。その一つに，RTS/CTS 方式（詳しくは本文中に後述）を利用する方法がある

電波干渉による速度低下について，平成 17 年午後I 問 2 で出題された

ことで送信データ量を 2 倍以上に増やす技術である。チャネルボンディング技術について，詳しくは「1.3.2　無線 LAN のフレームフォーマット」で解説する。

IEEE802.11n は，MIMO の空間ストリーム数の最大値が 4 個，チャネルボンディングで束ねることのできるチャネル数の最大値が 2 個である。使用する周波数帯域は，2.4GHz 帯と 5GHz 帯の二つである。

IEEE802.11n を IEEE802.11a/g と同一環境で使用する場合，下位規格である IEEE802.11a/g 端末が上位規格である IEEE802.11n 端末のフレームを検知できるようにする必要がある。下位規格端末との混在環境において衝突を回避する仕組みについて，詳しくは「1.3.2　無線 LAN のフレームフォーマット」で解説する。

参考

MIMO は，送信データを複数のストリーム（信号）に分割し，各ストリームをそれぞれ異なるアンテナを使って同時に送信する仕組みになっている。そのため，理論上はストリーム数に比例して伝送速度が増加する。
ストリーム数が 4 でチャネルボンディングを使用した場合，理論上の伝送速度は 600Mbps となる

試験に出る

IEEE802.11n について，平成 24 年午後Ⅰ問 3 で出題された。IEEE802.11ac について平成 29 年午後Ⅱ問 2 で出題された。チャネルボンディングと MIMO を使用した場合の伝送速度について，平成 29 年午後Ⅱ問 2 で出題された

●IEEE802.11ac

IEEE802.11ac は，IEEE802.11n で採用された MIMO，チャネルボンディングなどをさらに改良し，6.93Gbps の最大伝送速度を実現する規格である。IEEE802.11ac は，MIMO の空間ストリーム数の最大値が 8 個，チャネルボンディングで束ねることのできるチャネル数の最大値が 8 個である。使用する周波数帯域は，5GHz 帯のみである。

●プロトコル階層

IEEE802.3 と同様，IEEE802.11 はデータリンク層を LLC 副層と MAC 副層の二つの副層に分け，物理層と MAC 副層の仕様を規格化している。LLC 副層は，LLC タイプ 1 を用いる。

●アドホックモードとインフラストラクチャモード

今日の無線 LAN 環境は，アクセスポイント（以下，AP と称する）を介した通信形態で構築するのが一般的である。AP とは，無線 LAN におけるブリッジである。

もちろん，AP を使用せず，ステーション同士が直接通信する形態を採ることもできる。

AP を使用するとき，ステーションの通信モードをインフラスト

ラクチャモードに設定する。APを使用しないとき，ステーションの通信モードをアドホックモードに設定する。

●BSS，ESS

無線LANのセグメントは，**BSS**と**ESS**の二つに大別される。

- **BSS（Basic Service Set）**

  インフラストラクチャモードにおいては，1台のAPで構成された無線LANのセグメントである。

  アドホックモードにおいては，通信し合う1対のステーションのみで構成された無線LANのセグメントである。IBSS（Independent BSS）とも呼ばれる。

  BSSを識別するため，48ビットの長さをもつBSS IDが自動的に設定される。

  インフラストラクチャモードでは，APのMACアドレスがBSS IDに採用される。アドホックモードではAPを使用しないため，ユニークなBSS IDを生成する。

- **ESS（Extended Service Set）**

  1台のAPだけでは電波の到達距離に限界がある。そこで，AP同士を有線LANなどで接続し，より大規模な無線LANセグメントを構成する。これを**ESS**という。

  AP同士を結んだネットワークをDS（Distribution System）という。なお，DSは一般に有線LANだが，AP同士が無線LANで通信し合うWireless DS（WDS）も構成可能である。

  同一環境に複数のESSを構築することができる。そこで，ネットワークを構築する際，ESSを識別するために**ESS ID**を設定する。ESS IDは，最大32文字までの英数字で表される，なお，ESS IDを**SSID**（Service Set ID）と呼ぶことが多い。

●CSMA/CA

無線LANは**媒体共有型**のネットワークであるため，複数のステーションが同時にフレームを送信すると衝突が発生してしまう。しかし，無線通信の場合は受信レベルが不安定であり，さらに，

参考

アドホックモードで自動生成されるBSS IDは，I/G（Individual/Group）ビットが「0」で，G/L（Global/Local）ビットが「1」にセットされ，残り46ビットを乱数が占める。ステーションのMACアドレスはI/Gビットが「0」，G/Lビットが「0」であり，マルチキャストアドレスはI/Gビットが「1」，G/Lビットが「0」なので，BSS IDはどのアドレスとも重複しない値になる

試験に出る

SSID（ESS ID）について，平成18年午前 問38で出題された。同一環境に複数のESSを設け，ESS IDごとにVLANを登録する技術について，平成21年午後I問1で出題された

試験に出る

CSMA/CAについて，平成18年午後I 問2，平成19年午前 問46，平成17年午前 問41（平成14年午前 問35と同じ問題）で出題された

ステーション同士の位置関係によっては「**隠れ端末問題**」（詳しくは後述）が発生するため，衝突を検出できない可能性がある。そこで，無線 LAN ではアクセス制御方式として **CSMA/CA**（Carrier Sense Multiple Access with Collision Avoidance，搬送波感知多重アクセス／衝突回避）方式を採用している。

簡単に説明すると，これは衝突を検出するのではなく，衝突を回避する方法を採っている。CSMA/CA 方式では，**ACK**（Acknowledgement，確認応答）制御方式と **RTS/CTS**（Request To Send ／ Clear To Send）制御方式の二つの方式が規格化されている。

ACK 制御方式では，次の手順に従って通信を行う。

1. 送信ステーションは，通信中のステーションがほかにないことを確認する。
2. ステーションは，送信前にランダム時間待つ。この期間を「コンテンションウィンドウ」又は「バックオフウィンドウ」という。この仕組みにより，直前の通信が終了してから一定時間が経過した後で，複数のステーションが一斉に送信する事態を防ぐことができる。
3. 送信ステーションは，データフレームを送信する。フレームのデュレーション領域には通信を予約する時間が格納される。この時間を NAV（Network Allocation Vector，ネットワーク割当てベクタ）という。ほかのステーションは，フレームを受信すると NAV 値を更新し，その予約期間が満了するまで送信を行わない。この仕組みにより，送信が完了するまで衝突が回避される。
4. 正常に通信できたら，AP は ACK フレームを送信ステーションに返信する。なお，ACK フレームの NAV 値には「0」がセットされる。
5. 送信ステーションは ACK フレームを受信する。一定期間内に ACK フレームを受信できなかった場合，通信障害が発生したと判断してフレームを再送する。

次の図は，ACK 制御方式において，ステーション A がフレー

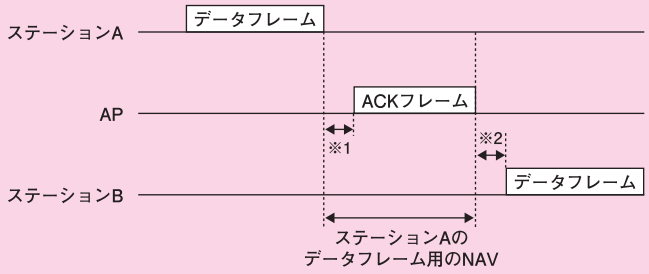
試験に出る

媒体共有型の通信である以上，多数のステーションが一斉に通信すれば，当然ながら各ステーションの実効転送速度が低下し，通信遅延も発生するはずである。
平成 23 年午後Ⅰ問 1 では，その着眼点について出題された

参考

ACK フレームの NAV 値に「0」がセットされるのは，フラグメンテーションが発生しないときである。通常は「0」がセットされる

ムを送信し，次にステーション B が送信するまでの様子を示している。NAV には ACK フレームの送信が終わる時間までが含まれている。よって，ステーション A の送信が完了するまで，ほかのステーションに邪魔されることはない。



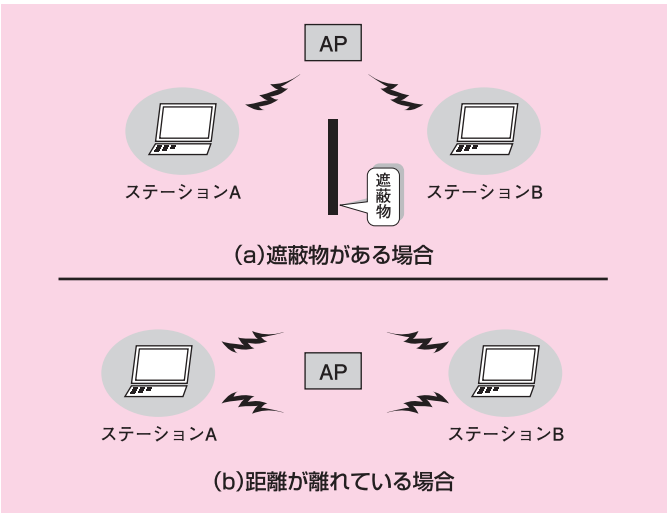
※1：SIFS（Short Inter-Frame Space）と呼ばれる期間，APは待機する。
※2：DIFS（Distributed Inter-Frame Space）と呼ばれる期間，ステーションBは待機する。その後，手順2で解説したコンテンションウィンドウだけ更に待機する。

図：ACK 制御方式で送信が行われる様子

しかし，次の図に示すように，ステーション A とステーション B の間に遮蔽物があったり，ステーション A とステーション B の距離が離れていたりする場合，ステーション A から送信された電波は AP に届くがステーション B には届かない。これを「**隠れ端末問題**」という。このとき，NAV による衝突回避が行えなくなる。

試験に出る

隠れ端末問題を解決するため，及 び，IEEE802.11b と IEEE 802.11g の混在環境で衝突を回避するために，**RTS/CTS 方式**が用いられている。その点について，平成 21 年午後Ⅱ問 1 で出題された



図：隠れ端末問題

隠れ端末問題を抱えている無線 LAN 環境では，フレームのサイズが大きくなるに従って衝突する可能性が高くなり，伝送効率が低下する。この問題を解決するため，データサイズが一定の値を超えたときには，RTS/CTS 方式を用いて通信を行う。これは，次の手順に従って行われる。

1. 送信ステーションは，通信中のステーションがほかにないことを確認する。
2. 送信する前に，ステーションはコンテンションウィンドウの時間，待機する。
3. 送信ステーションは，RTS フレームを送信し，AP に対しての送信権の獲得を要求する。フレームのデュレーション領域には，RTS フレーム用の NAV 値が格納されている。
4. AP は当該ステーションに送信権を割り当てる。それを全てのステーションに通知するため，CTS フレームを送信する。全てのステーションは，AP とは通信できるので，CTS フレームを受信する。フレームのデュレーション領域には，CTS フレーム用の NAV 値が格納されている。
5. 送信ステーションは CTS フレームを受信し，自分が送信権を獲得したことを確認する。残りのステーションは，当

参考

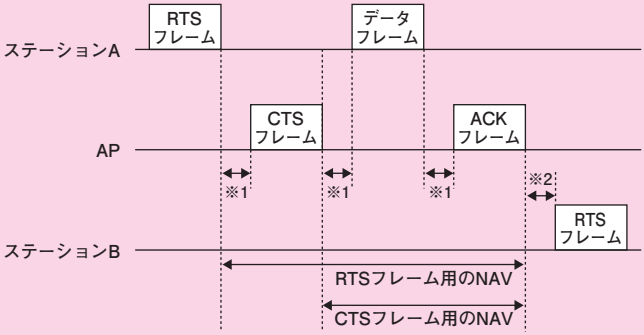
RTS/CTS 方式は，隠れ端末問題を解決するためだけでなく，IEEE802.11b と IEEE802.11g の混在環境で衝突を回避する方法の一つとして用いられることがある。
RTS/CTS 方式を用いる場合，IEEE802.11g ステーションと AP 間でデータフレームと ACK フレームをやり取りするときには，IEEE802.11g の変調方式と伝送速度を用いる。しかし，RTS フレームと CTS フレームの伝送には，IEEE802.11b の変調方式と伝送速度を用いる仕組みになっている。なぜなら，IEEE802.11b ステーションを含む全てのステーションはこれを受信して NAV 値を更新することができるので，その結果，衝突が回避されるからである

該ステーションが送信権を獲得したことを知る。

6. 送信ステーションは，データフレームを送信する。
7. 正常に通信できたら，APはACKフレームを送信ステーションに返信する。
8. 送信ステーションはACKフレームを受信する。

ACK方式と異なるのは，データフレームの送信に先立ち，RTSフレームとCTSフレームをやり取りして，送信権を獲得することである。

次の図は，RTS/CTS方式において，ステーションAがフレームを送信し，次にステーションBが送信する様子を示している。隠れ端末問題はステーション同士の位置関係に起因する問題であり，全てのステーションはAPとは通信できる。よって，少なくともCTSフレームを受信することができ，そのNAV値が満了するまでの間，衝突を回避することができる。



※1：SIFS（Short Inter-Frame Space）と呼ばれる期間，APは待機する。
※2：DIFS（Distributed Inter-Frame Space）と呼ばれる期間，ステーションBは待機する。その後，手順2で解説したコンテンションウィンドウだけさらに待機する。

図：RTS/CTS方式で送信が行われる様子

1.3.2 無線 LAN 規格のフレームフォーマット

試験に出る

IEEE802.11 フレームフォーマットについて，平成 24 年午後Ⅰ問 2，平成 21 年午後Ⅱ問 1，平成 18 年午後Ⅰ 問 2 で出題された

IEEE802.11 には様々な伝送速度をもつ規格が存在している。とはいえ，フレームフォーマットは，データリンク層以上の部分はどれも同じである。

ステーションが送受信するデータフレームのフォーマット（全体）を次に示す。

図：IEEE802.11 データフレームのフォーマット（全体）

下位規格のステーションと同じチャネルを共有するとき，下位規格の方が識別できるよう，物理層のヘッダを送信するときの速度は，上位規格の方が下位規格に合わせる。データリンク層以上は，上位規格本来の速度で伝送する。詳しくは，「●下位規格との混在環境における衝突回避」で後述する。

データフレームのフォーマット（データリンク層以上）を次に示す。

(2)	(2)	(6)	(6)	(6)	(2)	(2)	(0〜2312)	(4)
フレーム制御	デュレーション/ID	アドレス1	アドレス2	アドレス3	シーケンス制御	アドレス4	LLCヘッダ+データ	FCS

MACヘッダ

注:（　）内の数字はバイト長を表す。
アドレス4はオプションであり,WDSのときに使用される。

図：IEEE802.11 データフレームのフォーマット（データリンク層以上）

●フレーム制御，デュレーション /ID

フレーム制御領域は，フレームのタイプ（管理用／制御用／データ用），WEP 暗号化の有無，ToDS，FromDS などを設定する。

表：フレームタイプ領域（データフレームの場合）

	0 のとき	1 のとき
ToDS	宛先がステーション	宛先が AP
FromDS	送信元がステーション	送信元が AP

デュレーション /ID 領域は，ステーションがデータを送信できるようになるまでの待機時間などを表す。

●フレームアグリゲーション

フレームアグリゲーションは，宛先が同じ複数のフレームを連結して送信する技術である。CSMA/CA 方式におけるスループットの低下を軽減するために，IEEE802.11n から導入された。

IEEE802.11 は，CSMA/CA 方式を用いてフレームの衝突を回避している。CSMA/CA 方式は，その仕組み上，スループットの低下をもたらす要因を二つ抱えている。

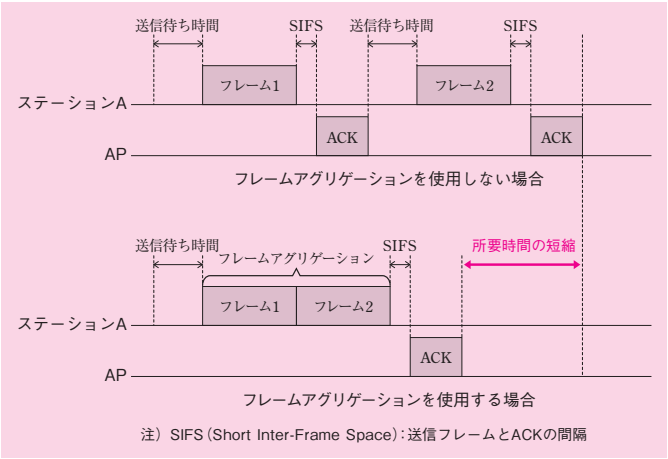
CSMA/CA 方式では，送信ステーションがフレームを送信するたびに，受信ステーションは確認応答を返信する仕組みになっている。つまり，フレーム送信と確認応答の 1 往復のやり取りがセットになっている。したがって，スループットの低下をもたらす一つ目の要因として，「フレームを送信するたびに，確認応答が発生すること」を挙げることができる。

さらに，CSMA/CA 方式は，フレームの衝突を回避するため，あるステーションが送信している間（つまり，CSMA/CA 方式の 1 往復のやり取りが完了するまでの間），残り全てのステーションは送信を差し控える仕組みになっている。したがって，スループットの低下をもたらす二つ目の要因として，「ステーションがフレームを送信している間，送信待ち時間が発生すること」を挙げることができる。まとめると，CSMA/CA 方式におけるスループットの低下要因は，「確認応答」と「フレームの送信待ち時間」である。

フレームアグリゲーションを使用することによって，フレームを 1 個ずつ送信する従来の方法と比べると，「確認応答」と「フレームの送信待ち時間」の回数を減らすことができる。したがって，全フレームの送信にかかる所要時間を短縮できるので，CSMA/CA 方式におけるスループットの低下が軽減される。

試験に出る

IEEE802.11n のフレームアグリゲーションについて，平成 24 年午後Ⅰ問 3 で出題された



図：フレームアグリゲーションによる所要時間の短縮

なお，フレームアグリゲーションを使用すると，1フレーム当たりの送信時間が長くなるので，無線チャネルを占有する時間が長くなる。この結果，ほかのステーションの送信待ち時間も長くなってしまう。

●下位規格との混在環境における衝突回避

無線LAN環境では，最新の規格に対応したステーションと，旧来の低速な下位規格に対応したステーションとが混在していることがある。無線LANに割り当てられた周波数帯域は限られているため，上位規格と下位規格を同一環境で使用する場合，CSMA/CA方式に従って衝突を回避する。

衝突の回避には，あるステーションが送信したフレームを，別のステーションが検知できなければならない。この点，上位側は，低速な下位側のフレームを容易に検知できる。一方，下位側は，上位規格本来の伝送速度でフレームを送信されると，これを検知できない。

この問題を解決するため，上位側は，下位側が検知できるようにプリアンブルを付加した上で，フレームを送信する。

IEEE802.11nを例に，この仕組みを解説する。

IEEE802.11nが使用する周波数帯域は，IEEE802.11gと同じ2.4GHz帯と，IEEE802.11aと同じ5GHz帯の二つである。それ

ゆえ，IEEE802.11a/g ステーションと IEEE802.11n ステーションの混在環境において，衝突の回避が必要となる。

IEEE802.11n には，IEEE802.11a/g との混在環境に対応した **mixed mode** が規定されている。mixed mode では，IEEE802.11a/g と同じプリアンブルを付加して送信する。

このプリアンブルは，IEEE802.11a/g ステーションが解釈できる OFDM 方式のフォーマットである。しかも，IEEE802.11a/g ステーションが検知できるように低速でプリアンブルを送信する。

OFDM 方式では，プリアンブルの中に格納されている情報だけを読み取れば，「どれほどの期間，送信を控えなければならないか」が分かるようになっているため，衝突を回避できる。したがって，IEEE802.11n ステーションが mixed mode でフレームを送信すれば，同じチャネルを使っている IEEE802.11a/g ステーションもプリアンブル部分を読み取ることができるので，CSMA/CA 方式に従って衝突を回避することができる。

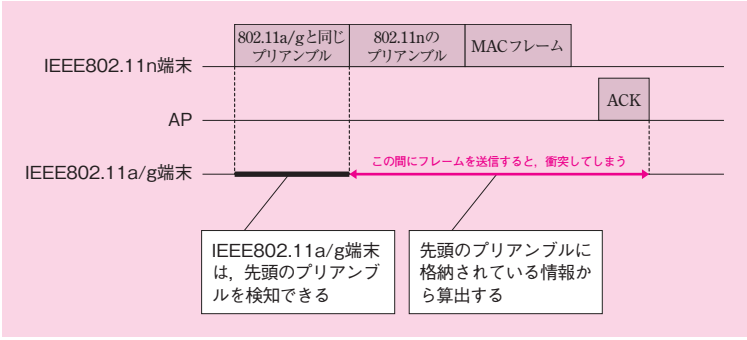
衝突を回避するには，IEEE802.11a/g ステーションがプリアンブルの後続部分を読む必要はない。そこで，mixed mode では，プリアンブルの後続部分を IEEE802.11n 本来の高速な伝送速度で送信することで，スループットをできるだけ損なわないようにしている。

参考

ここでは，「プリアンブル」を付加すると説明しているが，より正確に言うと，同期を確立するための PLCP プリアンブルと，SIGNAL（物理層ヘッダの一部）を付加している。
IEEE802.11 では，送信ステーションがフレームを送信するたびに，受信ステーションは確認応答を返信する。それ以外のステーションは，衝突を回避するため，フレームの送信と確認応答の 1 往復のやり取りに費やす期間を算出した上で，その期間は送信を差し控えなければならない。SIGNAL の中に，この期間を算出するための情報が格納されている

試験に出る

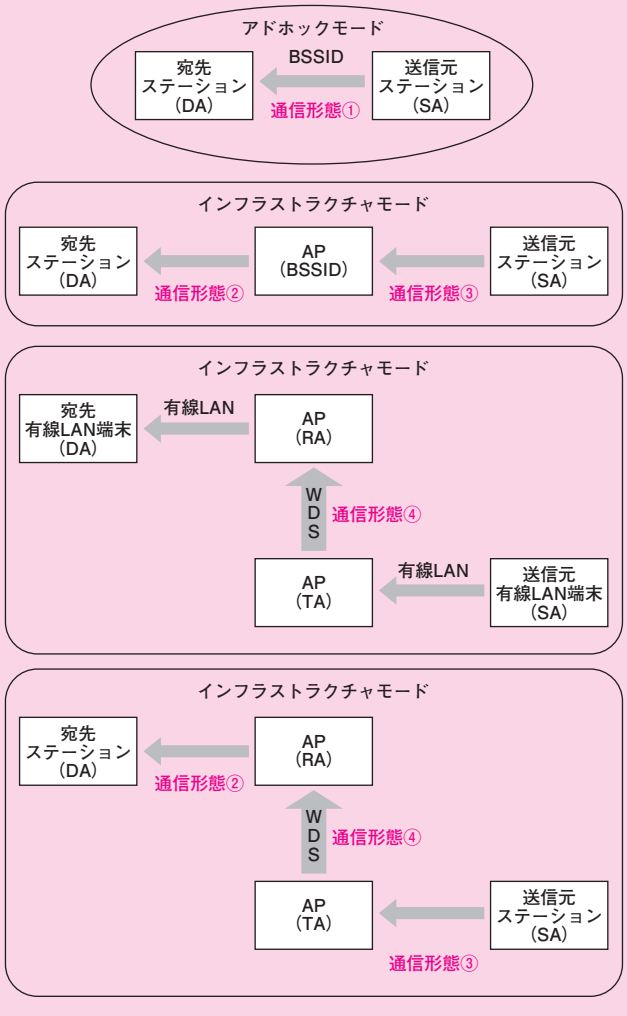
IEEE802.11n の mixed mode について，平成 24 年午後Ⅰ問 3 で出題された



図：mixed mode を用いた送信プロテクション

●通信形態

無線 LAN の通信形態は 4 種類ある。それぞれの通信形態によって，アドレス領域に格納される値は異なる。各通信形態を次に示す。



通信形態	通信形態		フレーム制御		アドレス				適　用
	宛先	送信元	ToDS	FromDS	1	2	3	4	
①	無線	無線	0	0	DA	SA	BSSID	なし	アドホックモード
②	無線	有線	0	1	DA	BSSID	SA	なし	インフラストラクチャモード
③	有線	無線	1	0	BSSID	SA	DA	なし	
④	無線	無線	1	1	RA	TA	DA	SA	Wireless DS（WDS）

DA	Destination Address	宛先端末の MAC アドレス
SA	Source Address	送信元端末の MAC アドレス
BSS ID	Basic Service Set ID	アドホックモード：乱数から生成
		インフラストラクチャモード：AP の MAC アドレス
TA	Transmitter Address	送信側 AP の MAC アドレス
RA	Receiver Address	受信側 AP の MAC アドレス

図：通信形態に応じたアドレス領域の役割の区別

1.3.3 APと無線LANコントローラ

今日の無線LAN環境は，APを介したインフラストラクチャモードで構築するのが一般的である。

このとき，APはブリッジとして機能する。すなわち，有線LAN（イーサネット）のスイッチと同じく，MACアドレステーブルをもち，アドレス学習機能と転送機能を装備している。加えて，無線LANと有線LANを接続する機能をもつ。

無線LANの普及に伴い，APに求められる機能が増えている。例えば，ローミング機能，バーチャルAP機能，セキュリティ機能などがある。

今日では，多数のAPを配置した無線LAN環境において，APを一元管理する目的で**無線LANコントローラ**の普及が進んでいる。

●ローミング機能

無線LAN環境を構築する際，APの電波が届く範囲を考慮に入れる必要がある。1台のAPでは広い空間をカバーすることができないので，複数のAPを設置することが多い。隣接するAPは，電波干渉を避けるために異なるチャネルを用いなければならない。

その空間内をステーションが移動する際，通信が途絶えないようにするには，移動しながら最寄りのAPに自動的に接続する機能が必要となる。この機能を**ローミング**という。

ステーション，及び，ローミングの移動範囲に配置された全てのAPは，同一のESSに属している必要がある。

●バーチャルAP機能

1台のAPの上で，複数の仮想的なAP（バーチャルAP）を稼働させる機能を，**バーチャルAP**機能という。

個々のバーチャルAPは，それぞれがAPとしての機能を装備している。したがって，別個にESS IDやVLANを割り当てることができる。

試験に出る

無線LAN（IEEE802.11）のローミング機能について，平成29年午後Ⅱ問2，平成25年午後Ⅱ問1，平成24年午後Ⅰ問2，平成16年午前問40で出題された。PMKキャッシュ機能について，平成25年午後Ⅱ問1で出題された。ESS IDごとにVLANを登録する技術について，平成21年午後Ⅰ問1で出題された。

本書で説明を割愛したAPの機能についても，出題例を挙げておく。ステルス機能について，平成28年午後Ⅰ問2で出題された。プライバシセパレータ機能（アクセスポイントアイソレーション）について，平成28年午前Ⅱ問21で出題された

参考

WPA2
無線 LAN の業界団体 Wi-Fi Alliance が定めた，無線 LAN の認証と暗号化の規格。認証方式として，IEEE802.1X，PSK を定めている。暗号化方式として，AES を定めている

●セキュリティ機能

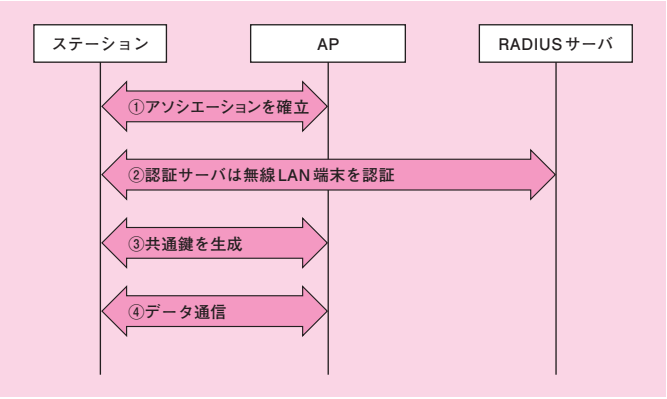
無線 LAN のセキュリティを強化する目的で，**WPA2** 準拠の認証と暗号化の機能をもつ AP の導入が広がりを見せている。WPA2 とは，無線 LAN の認証と暗号化を規定した，業界標準のセキュリティ規格である。WPA2 は，無線 LAN のセキュリティ規格の国際標準である **IEEE802.11i** をベースに策定されている（IEEE802.11i を拡張している）。

認証機能は，認証に成功したステーションだけが無線 LAN 通信を行えるようにする機能である。IEEE802.11i 規格では，**IEEE 802.1X** 規格に基づく認証を行うことができる。IEEE802.1X 規格では，実際の認証を認証サーバ（RADIUS サーバ）が実行する仕組みになっている。

暗号化機能は，無線 LAN 通信を傍受されないように，ステーションと AP 間の通信を暗号化する機能である。

実際の認証を RADIUS サーバが実行する場合，ステーションが AP に接続してからデータ用通信を行うまでのシーケンスは，おおよそ次のとおりとなる。

①ステーションが AP に接続し，アソシエーションが確立される。
②RADIUS サーバはステーションを認証する。AP は，両者のやり取りを中継する。
③認証に成功すると，AP は，ステーションとの間で共通鍵を生成する。
④ステーションは，AP を経由したデータ用通信を行う。その際，③で生成した共通鍵で通信を暗号化する。



図：IEEE802.11i 規格のシーケンス

②の認証に成功すると，ステーションと RADIUS サーバは，共通鍵の基になる乱数情報を共有する。これを **PMK**（Pairwise Master Key）という。②の処理の終了時に，RADIUS サーバは PMK を AP に送信する。その後，③の処理に移る。

③の処理では，ステーションと AP 間で乱数を交換し，その乱数と PMK から共通鍵を生成する。この共通鍵は，アソシエーションを確立するたびに生成されるもので，いわば寿命の短い鍵である。同じ鍵が長い間使われ続けると暗号を解読される危険が高まるので，この仕組みは暗号化通信のセキュリティ強化に役立っている。

IEEE802.11i 規格のセキュリティ機能をもたない無線 LAN 環境では，①でアソシエーションを確立したら，ただちに④のデータ用通信を行う。

IEEE802.1X 認証に対応した機能をもつ AP のことを，IEEE 802.1X 規格の用語で「**オーセンティケータ**」と呼ぶ。オーセンティケータがもつべき機能には，②のやり取りを中継すること，認証が成功するまでは④の通信を許可しないことなどがある。

なお，これまでの解説に登場した，WPA2，IEEE802.11i，IEEE802.1X について，詳しくは本書の第 4 章で解説している。WPA2，IEEE802.11i 規格は「4.4.6　無線 LAN」，IEEE802.1X 規格は「4.4.3　IEEE802.1X」をそれぞれ参照していただきたい。

試験に出る

IEEE802.1X 認証を導入する場合，AP がオーセンティケータの機能を実装する必要があることについて，平成 26 年午前Ⅱ問 18 で出題された

● 無線 LAN コントローラ

無線 LAN コントローラ（以下，WLC と称する）は，複数の AP を**一元管理**する機器である。通常，WLC とその管理下にある AP は，製造元が同じ製品である。WLC と AP は管理用の通信を行うので，IP アドレスをもつ。

WLC が装備している機能は，製品により様々であるが，例えば次に示す機能をもつものがある。

- **AP の設定情報の管理と更新**
  AP の設定情報を WLC で一元管理し，WLC から AP に設定情報を配信して更新する。
- **AP の監視**
  AP の稼働状態を監視する。
- **AP の電波干渉の検知と回避**
  管理外の AP が発信する電波の影響を受けるなど，様々な原因で管理下の AP が電波干渉を起こすことがある。その状況を検知し，AP のチャネルを適宜変更して電波干渉を回避する。
- **AP の負荷分散**
  複数の AP が設置されている無線 LAN セグメント内で，多数の無線 LAN 端末が接続している場合，AP の負荷を分散するために，無線 LAN 端末とアソシエーションを確立する AP を調整する。
- **セキュリティ機能とローミング機能の強化**
  IEEE802.1X 規格の認証処理を，個々の AP が実行するのではなく，WLC が実行する。すなわち，WLC がオーセンティケータとなる。このとき，AP は，ステーションと WLC 間の認証用通信のフレームを中継する役割を担う。
  WLC の中には，PMK をキャッシュする機能をもつものがある。移動に伴って別の AP とアソシエーションを確立したとき，キャッシュされた PMK を再利用できるので，ローミングの処理が高速化される。
- **DHCP**
  管理下にある AP に対し，IP アドレス，サブネットマスク，

無線 LAN コントローラがもつ様々な機能（AP の負荷分散，セキュリティ機能，ローミング機能など）について，平成 29 年午後Ⅱ問２で出題された

デフォルトゲートウェイ等のネットワーク情報を自動的に設定するため，WLC が DHCP サーバの機能をもち，AP が DHCP クライアントの機能をもつ。

製品によっては，WLC がブリッジとして機能するものがある。このとき，AP は，ステーションと WLC 間のデータ用通信のフレームを中継する役割を担う。このような機能をもつ WLC を使用する場合，ステーションを送信元／宛先とするデータ用通信は，必ず，WLC を経由することになる。このトラフィックの集中に起因する性能劣化が生じないよう，ネットワークを設計する必要がある。

試験に出る

WLC の導入に伴うトラフィック経路の分析，性能要件の再検討について，平成 24 年午後Ⅰ問２で出題された

1.4 LAN関連のプロトコル／規格

ここでは，フロー制御，オートネゴシエーション，VLANといった，LAN関連のプロトコルや規格について解説する。このうち，VLANは午後試験に頻出の要素技術である。IEEE802.1Q規格のポートベースVLAN，タグVLANの基礎知識をしっかり身に付けておく必要がある。

1.4.1 フロー制御

ここではイーサネットの各種フロー制御方式について解説する。全二重モードでは**IEEE802.3x**，半二重モードではバックプレッシャ方式が用いられている。

●IEEE802.3x

イーサネットの全二重モードにおけるフロー制御方式を規定したのがIEEE802.3xである。輻輳（ふくそう）を検知したスイッチングハブは，フレームを送信している端末に対し，**PAUSEフレーム**を送出する。PAUSEフレームを受け取ったステーションは，一定時間フレームの送信を延期する（フレームの中に，停止時間が格納されている）。こうして，フレームがスイッチングハブのバッファからあふれるのを防ぐ。

参考

PAUSEフレームのフォーマットはDIX規格である。宛先MACアドレスは「01-80-02-00-00-01」（フラッディングされないマルチキャストアドレス），送信元MACアドレスは送信元ステーションのMACアドレス，タイプ領域の値は「0x8808」である

●バックプレッシャ方式

半二重モードには，フロー制御方式に関する標準規格は存在しない。しかし，多くのスイッチングハブはバックプレッシャ方式によりフロー制御を実現している。バックプレッシャ方式では，スイッチングハブが衝突を検知すると，フレームを送信している端末に対し，架空のジャム信号を送出する。半二重モードでは，CSMA/CDの仕組みにより，ジャム信号を受け取った送信ステーションは，バックオフ時間（乱数による待ち時間）が経過するまでフレームの送信を延期する。こうして，フレームがスイッチングハブのバッファからあふれるのを防ぐ。

1.4.2 オートネゴシエーション／オート MDI/MDI-X

ここではオートネゴシエーションとオート MDI/MDI-X について解説する。ツイストペアケーブルを使用する 10BASE-T ／ 100BASE-TX ／ 1000BASE-T と光ファイバケーブルを使用する 1000BASE-SX ／ 1000BASE-LX との違いを把握しておく。

● 10BASE-T ／ 100BASE-TX ／ 1000BASE-T

1 台のスイッチングハブに 10BASE-T，100BASE-TX，1000BASE-T のステーションを収容する場合，スイッチングハブの各ポートとステーションの間で，伝送速度と伝送モード（全二重／半二重）を同一にする必要がある。これを自動的に判別して設定する仕組みが，**オートネゴシエーション**である。

オートネゴシエーションは，専用の制御フレームではなく，リンクパルスを利用して制御を行っている。オートネゴシエーションに対応している機器の場合，NLP と同時に，FLP バースト（Fast Link Pulse バースト）と呼ばれる，NLP よりもパルス幅がはるかに小さいパルスを送信する(NLP 信号の上に FLP 信号を相乗りさせている)。FLP に乗せて，自分がサポートする伝送速度／伝送モードを相手に伝える（複数指定可）。自分と相手がサポートする伝送速度／伝送モードのうち，最も優先度の高いものが選択されて，オートネゴシエーションを完遂する。その後,FLP バーストは送信されなくなる。

一方の機器のオートネゴシエーションを有効にし，他方の機器を無効にした場合，有効な側は FLP バーストを受信しないため，相手が全二重に対応していないと判断してしまう。無効な側からアイドル信号を受信した場合は 100M 半二重，NLP を受信した場合は 10M 半二重で接続されることになる。よって，全二重で通信したい場合は，両方の機器でオートネゴシエーションを有効にするか，無効にして手動で伝送速度と伝送モードを設定する必要がある。

また，IEEE によって標準化された機能ではないが，一部のスイッチングハブは**オート MDI/MDI-X** と呼ばれる機能を装備している。これは，ポートに接続されたツイストペアケーブルがストレートかクロスかを自動的に判別して，「Tx」と「Rx」の極性の違いをポート側で吸収する機能である。

試験に出る

オートネゴシエーションの失敗について，平成 20 年午後Ⅰ問 4 で出題された。オート MDI/MDI-X について，平成 28 年午前Ⅱ問 1，平成 21 年午後Ⅰ問 1 で出題された

用語解説

リンクパルス

イーサネット上で，通信機器（NIC，ハブ，スイッチ）同士が互いの接続性を常時確認するために，アイドル期間中に送信するパルス信号のこと。10BASE-T では NLP（Normal Link Pulse，ノーマルリンクパルス）を，100BASE-TX ではアイドル信号を常時やり取りしている。NLP とアイドル信号は周波数や電圧値が違うため，通信速度の相違を自動認識できる。ただし，全二重／半二重の相違は識別できない

参考

オートネゴシエーションの優先順位は，
① 1000BASE-T の全二重
② 1000BASE-T の半二重
③ 100BASE-T2 の全二重
④ 100BASE-TX の全二重
⑤ 100BASE-T2 の半二重
⑥ 100BASE-T4 の半二重
⑦ 100BASE-TX の半二重
⑧ 10BASE-T の全二重
⑨ 10BASE-T の半二重
の順番となっている

リモートフォルト機能について，平成 17 年午後Ⅰ問 4 で出題された

● 1000BASE-SX ／ 1000BASE-LX

1000BASE-SX ／ 1000BASE-LX では，通常は全二重及び 1G ビット／秒固定であるため，オートネゴシエーションを使用する必要はない。しかし，オートネゴシエーションの規格に含まれる**リモートフォルト**（remote fault）機能を用いるために使用されるケースがある。

光ファイバでは，2 芯あるファイバのうち 1 芯だけが切断するという障害が発生することがある。このとき，一方のスイッチングハブ（受信側）ではリンクダウンを検出するが，もう一方（送信側）はリンクアップのままという単方向通信状態に陥る。

リモートフォルト機能を動作させることにより，両端の装置で障害を検知し，リンクダウンさせることができる（その後は，スパニングツリーなど何らかの仕組みが働いて，う回ルートが設定される）。

1.4.3 VLAN

VLAN（Virtual LAN）機能とは，端末をグループ化し，論理的なサブネットを構成する機能である。一つのグループは，あたかも一つの LAN セグメント（ブロードキャストドメイン）に属しているかのように通信できる。VLAN 機能は IEEE802.1Q で規定されており，ポートベース VLAN とタグ VLAN がある。

VLAN のセグメント化によるセキュリティ効果について，平成 25 年午前Ⅱ問 20 で出題された。通信条件を満たすように VLAN をポートに割り当てる設計について，平成 23 年午後Ⅰ問 3 で出題された。タグ VLAN について，平成 24 年午後Ⅱ問 2，平成 21 年午後Ⅰ問 1 で出題された。ポートベース VLAN について，平成 15 年午前 問 41 で出題された

● ポートベース VLAN

グループを一意に識別する番号は VLAN ID である。グループ化の設定は，スイッチングハブのポートごとに VLAN ID を割り当てる方式が採用されている。この方式を**ポートベース VLAN** という。

なお，VLAN 機能を装備しているスイッチングハブの全てのポートは，デフォルトで VLAN ID が「0x1」の VLAN に収容されている。この VLAN（VLAN ID が「0x1」の VLAN）のことを，**デフォルト VLAN** と呼ぶ。

● タグ VLAN

タグ VLAN とは，所属する VLAN が異なる複数の論理的なリンクを，1 本の物理的なリンクの上に束ねる技術のことであり，

IEEE802.1Qで規格化されている。その物理リンクを収容するポートは，タグVLANで束ねた全てのVLANに所属することになる。タグVLANを用いない場合と用いる場合の違いは次ページの図のとおりである。なお，この構成では，スイッチングハブをまたがって，VLAN10，VLAN20の二つのVLANセグメントが存在している。

図の上段に示した構成は，タグVLANを用いない場合の構成である。この場合は，単純にポートベースVLANを使用することになるので，スイッチングハブのポートには一つのVLAN IDを登録する。よって，VLANごとに1本ずつのリンクを用意する必要がある。

一方，図の下段に示した構成は，タグVLANを用いる場合の構成である。図から明らかなとおり，スイッチングハブ間の物理リンクが1本になっている。実は，VLAN10，VLAN20，それぞれのVLANには1本ずつの論理リンクが用意されており，論理的な構成はタグVLANを用いない場合と同等だが，この2本の論理リンクが1本の物理リンクに重畳されている。つまり，タグVLANを使用することで，VLANごとに論理リンクを設けることができるというメリットを得ることができる。

これらの論理リンクを識別するため，この物理リンク上を流れるフレームには，「**タグフレーム**」と呼ばれる特別なフレームが用いられている。これは，「**VLANタグ**」と呼ばれる4バイトのデータが挿入されたフレームである。このVLANタグの中には，VLAN IDが格納されている。例えば，VLAN10に収容されたステーション間で通信する場合，タグフレームには「VLAN ID = 10」が格納される。同様に，VLAN20間で通信する場合は，「VLAN ID = 20」が格納される。

タグVLANを使用してネットワークを構成する場合，スイッチングハブのポートに対し，格納できるVLAN IDの値を事前に設定しておく必要がある。図の下段の例では，「10」と「20」の二つである。

なお，タグフレームを送受信するポートを「タグポート」と呼ぶ。タグポートから送信されるとき，フレームにはVLANタグが挿入され，送信元ステーションが収容されているVLAN IDの値が格納される。そして，対向のタグポートでフレームが受信されるとき，

試験に出る

IEEE802.1Qトンネリング技術（IEEE802.1ad）について，平成25年午後I問3で出題された。広域イーサネットサービスで利用されているタグVLAN技術について，平成16年午後I 問3で出題された

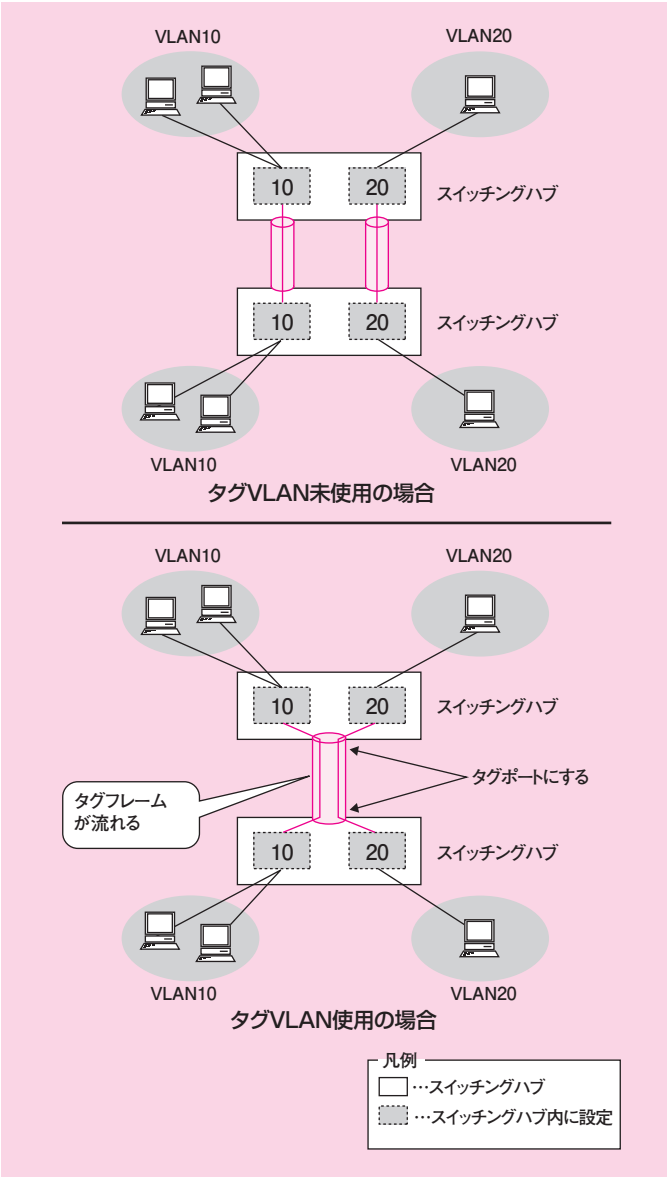
参考

IEEE802.1Qトンネリングは，IEEE802.1QのVLANタグ付きのパケットを，さらに別のVLANタグを付けることによってカプセル化する技術である。これは，IEEE802.1adによって標準化されている。

IEEE802.1adのVLANタグは，IEEE802.1QのVLANタグの前に挿入される（IEEE802.1QのVLANタグがないフレームであれば，タイプ領域の前に挿入される）。

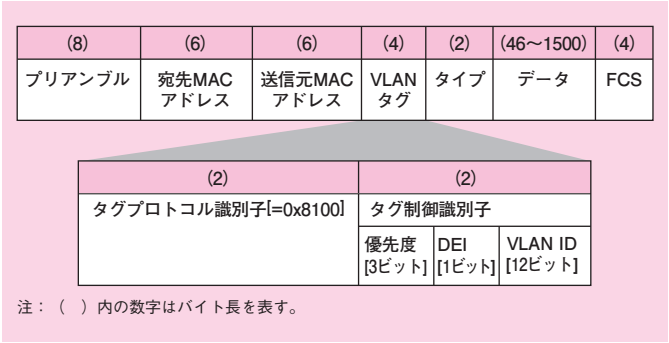
VLANタグの構造は，IEEE802.1Qと同じである。すなわち，2バイトのタグプロトコル識別子（TPID）と，2バイトのタグ制御識別子（TCI）で構成される。VLANタグの各領域の意味も，IEEE802.1Qと同じである。異なるのは，TPIDの値である。IEEE802.1adは，TPIDの値を「0x88A8」と定めている。TPID領域の位置は，VLANタグがないときのタイプ領域の位置に該当する。それゆえ，「0x88A8」というTPIDの値は，事実上，フレームのタイプが「IEEE802.1ad規格のVLANタグ付きフレーム」であることを意味している。このVLANタグ付きフレームを受信したネットワーク機器は，TPIDの値を見て，後続の2バイトをTCIとして解釈することになる。このTCIの中に格納されているVIDが，トンネルの識別子となる

タグが取り除かれて VLAN ID の値が評価される。その後，スイッチングハブ内の各 VLAN のアドレステーブルの値に従い，フレームが転送される。



図：タグ VLAN

タグ VLAN のフレームフォーマットを次に示す。



注：（ ）内の数字はバイト長を表す。

図：VLAN タグフレームのフォーマット

DIX 規格ではタイプ領域の前に VLAN タグが挿入される。VLAN タグのバイト長は 4 バイトであり，2 バイトの**タグプロトコル識別子**（TPID：Tag Protocol Identifier）と，2 バイトの**タグ制御識別子**（TCI：Tag Control Identifier）で構成される。

前半 2 バイトのタグプロトコル識別子は，フレームのタイプが「IEEE802.1Q タグフレーム」であることを意味している。これにより，ステーションは後続の 2 バイトをタグ制御識別子として解釈することになる。

イーサネットフレームは最大 1,518 バイトであるため，VLAN タグが付くことにより，最大 1,522 バイトになる。

タグ制御識別子の中身は，先頭ビットから順に，次の表のとおりになっている。

表：タグ制御識別子の中身

領　域	ビット数	内　容
優先度	3	VLAN ID が「0」であるとき，「優先度タグ付きフレーム」として扱われ，この領域が解釈される
DEI (Drop Eligible Indicator)	1	「1」であるとき，輻輳時に優先的に破棄してもよいフレームとなる
VLAN ID	12	VLAN を識別する番号。「1」～「4094」までを使用する。「0」は「優先度タグ付きフレーム」

試験に出る

VLAN ID のビット数について，平成 29 年午前Ⅱ問 4 で出題された

参考

優先度は，デフォルトが「0」で，最高が「7」だが，値が大きいほど優先度が高いわけではない。また，デフォルトより低い優先度も規定されている。
詳しくは本書の第 3 章「3.2 QoS 制御」を参照していただきたい

1.5 スイッチ

午後試験では，スイッチのアドレス学習機能，転送機能などの基礎知識を前提とした，設計の問題が出題されている。スイッチの機能は基本的な要素技術であるが，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。

1.5.1 アドレス学習機能と転送機能

どのスイッチも必ず装備している機能は，アドレス学習機能と転送機能である。

●アドレス学習機能

スイッチは，MAC フレームの受信を契機に，受信したポートの先に送信元ノードが存在していることを学習する。ただし，直接収容しているのか，別のスイッチを介して収容しているのかまでは分からない。

このとき学習した内容（受信ポートと送信元 MAC アドレスの対応付け）を，**MAC アドレステーブル**に登録する。これが**アドレス学習機能**である。

スイッチを VLAN で分割している場合，**VLAN ごとに** MAC アドレステーブルが存在する。

言うまでもなく，ポートと MAC アドレスの対応付けは，変化し得るものである。例えば，PC をスイッチからいったん切り離し，別のポートにつなぎ直すかもしれない。

その点を考慮し，スイッチは，**エージングタイム**と呼ばれる期間内に同一の内容を再学習しないと，MAC アドレステーブルからその登録を抹消する。

試験に出る

ミラーポートから出力されたフレームを取り込んでそれを別のポートから送出するためにアドレス学習機能を停止する必要があることについて，平成 26 年午後Ⅱ問 2 で出題された

参考

多くの製品では，エージングタイムは 300 秒である

●転送機能

スイッチは，MAC フレームを受信すると，どのポートの先にどのノードがあるかを MAC アドレステーブルから判定し，特定のポートからフレームを送り出す。これが**転送機能**である。

しかし，スイッチが特定のポートからフレームを転送せず，（受信ポートを除く）各ポートから一斉にフレームを転送することがある。この動作を**フラッディング**という。

スイッチがフラッディングするのは，次に示す三つのケースである。

- **ブロードキャストフレームの転送**
  ブロードキャストフレームは，必ずフラッディングする。
- **マルチキャストフレームの転送**
  マルチキャストフレームは，特別なマルチキャストアドレスを宛先とするフレームを除き，フラッディングする。
  IEEE802.1D 規格と IEEE802.1Q 規格は，様々な用途のマルチキャストアドレスを規定している。このうち，隣接するスイッチ間で用いられるものは，フラッディングしないことを規定している。詳しくは，本章の「1.2.4 IEEE802.2 規格のフレームフォーマット」のコラム「予約されたマルチキャストアドレス」を参照していただきたい。
- **宛先ノードのアドレス学習が済んでいない場合のユニキャストフレームの転送**
  ユニキャストフレームを受信した際，その宛先 MAC アドレスが MAC アドレステーブルに登録されていない場合がある。当然ながら，スイッチは，どのポートから転送したらよいかを判断することができない。
  それゆえ，宛先ノードがどのポートの先に存在するかをまだ学習していないユニキャストフレームを受信すると，スイッチはこれをフラッディングする。

●MAC アドレステーブルの更新

サーバの信頼性を向上させるため，主系と待機系の 2 台のサーバを稼働させ，主系の障害時に待機系に切り替える方式を採ることが多い。

主系から待機系に切り替わるとき，IP アドレスと MAC アドレスを引き継ぐ方式がある。同一セグメント内にあるスイッチの MAC アドレステーブルには，MAC アドレスと収容ポートとの対応付けがキャッシュされている。したがって，サーバの切替えに

試験に出る

障害発生に伴ってスパニングツリーが再構築されると，スイッチの MAC アドレステーブルがクリアされる。その結果，ユニキャストフレームがフラッディングされることについて，平成 24 年午後Ⅱ問 2 で出題された。
IEEE802.1X 認証で用いられる EAP フレームは，マルチキャストフレームである。EAP フレーム透過機能をもつスイッチを除き,通常のスイッチは,EAP フレームをフラッディングしない。EAP フレーム透過機能をもつスイッチについて，平成 25 年午後Ⅱ問 2 で出題された。マルチキャストフレームがフラッディングされることについて，平成 27 年午後Ⅱ問 2 で出題された

試験に出る

冗長構成において，主系から待機系に切り替わったときに MAC アドレステーブルを更新する必要性について，平成 26 年午後 I 問 2 で出題された。仮想マシンがライブマイグレーションしたときに MAC アドレステーブルを更新する必要性について，平成 20 年午後Ⅱ問 1 で出題された

伴って，スイッチとサーバとの物理的な位置関係が変化するので，このキャッシュを更新しなければならない。

参考

MAC アドレステーブルの更新に用いるフレームは，標準化されていない。ある製品は，RARP を用いる。RARP について，詳しくは《基礎編》の第 3 章「3.4.2 特別な用途の ARP」を参照していただきたい

●ブロードキャストストーム

ブロードキャストドメインの中で，スイッチを介した経路がループ状になっていると，ブロードキャストフレームがループした経路を巡回し続ける。なぜなら，フラッディングしたフレームを再び受け取ってしまうため，フラッディングによる転送を繰り返すことになるからだ。

ブロードキャストフレームは，ARP 要求をはじめ様々な種類があり，通信には欠かせない存在である。それゆえ，四六時中，端末はブロードキャストフレームを送信している。このブロードキャストフレームがいつまでも消えることなく転送されているなら，ブロードキャストフレームの数が増えるにつれて，ネットワークの帯域を次第に埋め尽くしてゆく。これを**ブロードキャストストーム**という。

ブロードキャストストームが発生すると，通常のデータ用通信の転送処理が追いつかなくなり，通信に支障が生じる。スイッチの CPU 使用率が高まってダウンしてしまうこともある。

試験に出る

ブロードキャストストームについて，平成 21 年午後Ⅰ問 1，平成 21 年午後Ⅱ問 2 で出題された

1.5.2 スイッチの様々な機能

製品により異なるが，世の中には様々な機能をもつスイッチがある。

午後試験の出題例を挙げると，本章の「1.4　LAN 関連のプロトコル／規格」に挙げたオートネゴシエーションや VLAN，リンクアグリゲーションやスパニングツリーなどの冗長化機能，ミラーリング，認証スイッチ，MAC アドレスフィルタリング，ループ防止，SNMP エージェントなどがある。

ここでは，前述の機能の中から，ミラーリングとその後に列挙した各機能について解説する。

なお，リンクアグリゲーションとスパニングツリーについて，詳しくは本書の第 2 章「2.2.1　リンク，スイッチングハブの冗長化」を参照していただきたい。

●ミラーリング

ミラーリング機能とは，あるポートを経由するフレームを，特定のポートにコピー（ミラーリング）して出力する機能である。

ミラーリングしたフレームを出力するポートを，ミラーポートという。

ミラーリング機能は通信フレームを収集する目的で主に使用される。その際，フレームを取り込む端末を，ミラーポートに接続する。

この端末の NIC は，プロミスキャスモードに設定しておく必要がある。通常の NIC は，自分を宛先としないユニキャストフレームを破棄する仕様になっている。しかし，ミラーポートから出力されたフレームを取り込む場合，自分を宛先としないユニキャストフレームを受信するように動作させる必要がある。このような NIC の動作を，プロミスキャスモードという。

ミラーリング機能を利用したフレームの収集について，平成 26 年午後Ⅱ問 2，平成 25 年午後Ⅰ問 2，平成 21 年午後Ⅰ問 1，平成 21 年午後Ⅱ問 2，平成 19 年午後Ⅱ問 1，平成 18 年午後Ⅱ問 1，平成 17 年午後Ⅱ問 1 で出題された

●認証スイッチ

IEEE802.1X 規格に準拠したスイッチは，ポートに割り当てる VLAN を動的に切り替える機能をもっている。切り替える VLAN ID は，認証サーバから受け取る仕組みになっている。

IEEE802.1X について，詳しくは本書の第 4 章「4.4.3 IEEE802.1X」を参照していただきたい。

IEEE802.1X 認証機能をもつスイッチ(無線 LAN の AP を含む)について，平成 29 年午後Ⅱ問 2，平成 25 年午後Ⅱ問 2，平成 21 年午後Ⅱ問 1，平成 20 年午後Ⅱ問 1，平成 19 年午後Ⅰ問 2，平成 17 年午後Ⅱ問 1 で出題された

●MAC アドレスフィルタリング

特定の MAC アドレスを送信元とするフレームだけを転送するアクセス制御機能を，MAC アドレスフィルタリング機能という。これにより，あらかじめ登録された端末だけが LAN を利用できるように制限できる。

MAC アドレスフィルタリングについて，平成 25 年午後Ⅱ問 2，平成 18 年午後Ⅱ問 2 で出題された

●ループ防止

経路がループしているとブロードキャストストームが発生するので，ネットワーク障害の原因となる。

そこで，ブロードキャストフレームの巡回を検知すると，そのブロードキャストフレームを破棄してブロードキャストストームの発生を未然に防ぐ機能をもつスイッチがある。この機能をルー

プ防止機能という。

ループを検知する方法は，前述のもののほかにも幾つか存在する。スイッチによっては，複数の方法を用いてループを検知し，ループの経路上にあるポートを閉塞してループを遮断する。

スイッチがループを検知する方法として，例えば次に示すものがある。

- **ループ検知用フレームの定期送信**
  スイッチは，ループ検知用のフレームを定期的に送信する。これを自分が再び受信すると，ループしていると判断する。
- **フラッピングの検知**
  経路がループしていると，「同じ MAC アドレスを送信元とするフレームを複数のポートからほぼ同時に受信する」という現象が見られることがある。
  スイッチは，別のポートから受信するたびに，アドレス学習機能により MAC アドレステーブルを更新する。経路がループしているとき，この更新が短時間のうちに頻発してしまう。この現象を**フラッピング**や**スラッシング**という。
  フラッピングが発生すると，ループしていると判断する。

フラッピングについて，平成 22 年午後Ⅱ問 2 で出題された

● SNMP エージェント

SNMP の監視対象とする場合，スイッチは**SNMP エージェント**機能をもつ。SNMP マネージャと通信するため，IP アドレス，サブネットマスク，デフォルトゲートウェイをスイッチに設定する。

このように IP アドレスをもつスイッチを，**インテリジェントスイッチ**という。

なお，SNMP によるネットワーク監視について，詳しくは本書の第 5 章「5.5　ネットワーク監視」を参照していただきたい。

L2 スイッチが監視対象となることについて，平成 25 年午後Ⅰ問 3 で出題された