

短期集中！

ネットワーク スペシャリスト 教本

for Network Specialist /
Applied Information Technology Engineer

Gene、ふたつ愛子、山田剛士 [著]



合格できる"ネットワーク理解力"を
最短で身に着けよう！



短期集中!

ネットワーク スペシャリスト教本

for Network Specialist /
Applied Information Technology Engineer

Gene、ふたつ愛子、山田剛士 [著]



本書のサポートサイト

本書に関する追加情報等について提供します。

<http://book.mynavi.jp/support/pc/5081/>

「ネットワークスペシャリスト」「応用情報技術者」試験と本書の関係について

- ・本書は経済産業省が行う情報処理技術者試験のうち、ネットワークスペシャリスト試験・応用情報技術者試験において取り上げられるネットワーク関連分野の技術において、特に重要と思われる技術分野を解説したものです。
- ・著者、株式会社マイナビは本書の使用による情報処理技術者試験の合格を保証いたしません。
- ・応用情報技術者試験は春・秋の年2回、ネットワークスペシャリスト試験は年に年1回行われています。試験の詳細は「情報処理技術者試験センター」のWebサイトで公開されています。
<http://www.jitec.jp/>
- ・本書で作成した情報処理技術者試験の問題および解答は、情報処理技術者試験センターが公開したものを一部引用しています。実際の過去問等は上記の情報処理技術者試験センターのサイトから取得できます。

- ・本書に記載された内容は情報の提供のみを目的としています。本書の制作にあたっては正確な記述に努めましたが、著者・出版社のいずれも本書の内容について何らかの保証をするものではなく、内容に関するいかなる運用結果についてもいっさいの責任を負いません。本書を用いての運用はすべて個人の責任と判断において行ってください。
- ・本書に記載の記事、製品名、URL等は2014年5月現在のものです。これらは変更される可能性がありますのであらかじめご了承ください。
- ・本書に記載されている会社名・製品名等は、一般に各社の登録商標または商標です。本文中では©、®、™等の表示は省略しています。

はじめに

Web ブラウザで Web サイトにアクセスして、ユーザ名とパスワードを入力してログイン。そして、Web ブラウザ上でいろんな情報を入力して業務を進めていく……。このような作業は、本書を手にとったあなたが日常的に行っていることでしょう。ビジネスだけではなくプライベートでインターネットのオンラインショッピングで買い物するときでもそうです。

現在は、当たり前のように使っている多くのシステムが Web ブラウザをインターフェースとした Web アプリケーションとして実装されています。

普段使っている Web アプリケーションのしくみがどのようになっているかということをネットワーク技術にウェイトを置いて解説することが本書のメインテーマです。Web アプリケーションを実現するためには、さまざまな技術を組み合わせています。それらの技術を簡潔に解説しています。ただ、読んでいただくだけではなく、理解の確認のためネットワークスペシャリスト試験の過去問題を中心とした例題を設けています。

本書を一読していただければ、Web アプリケーションを実現するために利用される主なネットワーク技術を一通り把握することができるでしょう。例題で主に取り上げたネットワークスペシャリスト試験の午後問題では、さまざまなネットワーク技術を複合させて出題がされています。試験対策として、まずは、個々の技術をしっかりと理解することが重要です。その目的でも本書を有効に活用していただけるものと考えています。そして、興味を持った技術があれば、より深くその技術を学んでいただっくりききっかけになることを願っています。

2014年5月 著者一同

目 次

第1章 LAN技術	001
1-1 MACアドレス	002
1-2 伝送媒体	006
1-3 イーサネット	013
1-4 無線LAN	018
第2章 WAN技術	029
2-1 WAN	030
2-2 IP-VPN	032
2-3 広域イーサネット	041
第3章 TCP/IPプロトコル	047
3-1 IP	048
3-2 IPアドレス	052
3-3 サブネットティング	060
3-4 IPv6	068
3-5 NAT	076
3-6 ICMP	084
3-7 ARP	091
3-8 TCP/UDP	097
3-9 DNS	106
3-10 DHCP	114
3-11 HTTP	119
3-12 SMTP/POP/IMAP	125

第4章 ネットワーク機器	131
4-1 レイヤ2スイッチ	132
4-2 VLAN	140
4-3 ルータ	151
4-4 レイヤ3スイッチ	155
4-5 セキュリティアプライアンス	160
4-6 ロードバランサ	168
4-7 ブロードバンドルータ	174
第5章 ルーティング	179
5-1 ルーティング	180
5-2 ルーティングプロトコル	188
5-3 VLAN間ルーティング	199
第6章 冗長化技術	203
6-1 冗長化技術の全体像	204
6-2 スパニングツリー	208
6-3 リンクアグリゲーション	219
6-4 スタック	225
6-5 VRRP	232
6-6 エンドツーエンドの通信経路の冗長化	239
6-7 NICチーミング	251
6-8 サーバクラスタ	260
第7章 ネットワーク管理	265
7-1 SNMP	266
7-2 Syslog	273
7-3 NTP	277
7-4 Telnet/SSH	283

第8章 Web アプリケーション	287
8-1 Webアプリケーションの動作	288
8-2 プロキシサーバ	294
8-3 デジタル証明書	299
8-4 セッション管理	305
第9章 セキュリティ技術	309
9-1 暗号化	310
9-2 VPN	315
9-3 IPsec VPN	319
9-4 SSL-VPN	331
9-5 IEEE 802.1X	338
第10章 仮想化	343
10-1 仮想化	344
10-2 ライブマイグレーション	352
索引	355

第1章

LAN 技術

- 1.1 MAC アドレス
- 1.2 伝送媒体
- 1.3 イーサネット
- 1.4 無線 LAN

1-1

MAC アドレス

目的

- MACアドレスはLAN環境で主に利用されるイーサネットにおいて住所情報 を定義し、ネットワーク機器（コンピュータ・ルータ等）の接続口に対して割り当てられ、データ送信時に宛先MACアドレス・送信元MACアドレスが ヘッダ情報にセットされる事によって、データ転送を実現している
- MACアドレスはIEEE802.3で標準化されている
- MACアドレスはネットワーク機器によって、「物理アドレス」や「イーサネットアドレス」と記載される事がある

1. MACアドレスのしくみ

イーサネットの通信では住所情報として **MAC** (Media Access Control) **アドレス** を利用し、通信方式は **CSMA/CD** を利用しています (CSMA/CDは現在のネットワーク 環境ではスイッチング製品の普及により実質適用されない事が多くなっています)。

MACアドレスはコンピュータの場合、**NIC** (Network Interface Card) に割り当てられ、クライアントコンピュータの場合、無線LANカードやオンボードNICという形式でマザーボードに元から設置されている機器に割り当てられます。

サーバコンピュータでもオンボードNICの形式のものもありますが、ネットワー ク接続数に応じてNICを増設する事があります。

ルータの場合はイーサネットインターフェースに対してMACアドレスが割り当 てられます。

1つの機器に複数のNIC、インターフェースがあった場合でも、MACアドレスは それぞれの接続口ごとに異なるアドレスが設定されます。



図 1.1.1 イーサネット通信を行う機器のMACアドレス割り当て位置

MACアドレスは**48ビット**（6バイト）の情報で、ネットワーク機器の管理画面上では12桁の16進数で表示されます。16進数で表記する場合は12桁の数値を12:34:56:78:9A:BCといったように「:」で区切るか、12-34-56-78-9A-BCの「-」で区切れます。

このうち、前半24ビット（3バイト）は製造者を示すベンダ番号（OUI: organizationally unique identifier）が定義され、後半ビットでは製造者によって割り当てられるシリアル番号が割り当てられます。

この事によりMACアドレスが適用されるNW（ネットワーク）機器のアドレス重複を防いでいます。

また、MACアドレスでは先頭から7ビット目を**U/L**（Universal/Local）ビット、先頭から8ビット目を**I/G**（Individual/Group）ビットとして予約されています。



図 1.1.2 MACアドレスのしくみ

U/LビットはMACアドレスがグローバルアドレスかローカルアドレスかを識別しています。

グローバルアドレスはネットワーク機器製造メーカーによって割り振られたアドレスである事を示し、アドレスの重複がないように一意の値が定義されます。

ローカルアドレスはユーザが任意の数値を指定して設定されるアドレスですが、アドレス重複の可能性があるため通常は利用されません。

I/Gビットはアドレスの属性を示し、単体ネットワーク端末の通信はユニキャストアドレスと呼び、複数のネットワーク端末の通信にはマルチキャストアドレスが利用されます。

ユニキャストアドレスとマルチキャストアドレスの定義を以下に記載します。

ユニキャストMACアドレス	単体のネットワーク機器を宛先とした通信で、アドレス指定は宛先のネットワーク機器に割り振られたMACアドレスが指定される I/Gビットは0が指定される
マルチキャストMACアドレス	レイヤ3でマルチキャストIPアドレスを指定した際に、マルチキャストMACアドレスが指定される I/Gビットは1が指定され、具体的なアドレスは「01:00:5E+マルチキャストIPアドレスから算出された値」が指定される
ブロードキャストMACアドレス	マルチキャストMACアドレスの一部で一斉同報を示し、ネットワークセグメント全体へ通信を示す I/Gビットは1が指定され、具体的なアドレスは全てのビットが1に設定された「FF:FF:FF:FF:FF:FF」が指定される

例題

平成25年ネットワークスペシャリスト試験 午後I 問1抜粋

U君は、O主任に端末の管理強化策の案を説明した。O主任は、U君の案に對して次の3点を指示した。

- 端末登録システムの登録情報に、端末の機種名を加えること。MACアドレスの上位【**a**】ビットには、OUI（【**A**】に固有の値）があるが、端末の機種名を付け加えることによって、端末の特定がより容易になる。
- 特別に固定IPアドレスの割当てが必要な端末に対して、DHCPサーバから常に決まったIPアドレスが割り当てられるように機能を追加すること。
- 導入後、端末登録システムに端末の登録を完了するまでの暫定運用では、使用者の利便性を考慮したDHCPサーバの運用ができること。

設問1 本文中の【**A**】に入る適切な字句を答えよ。

設問2 本文中の【**a**】に入る適切な数値を答えよ。

例題解説 ➔➔➔

設問1 製造者

設問2 24

MACアドレスはネットワークの接続口に対して設定され、通常一意のアドレスであるグローバルMACアドレスが指定されます。MACアドレスは48ビットのうち、前半24ビットはOUIと定義されており、IEEEが機器製造者ごとに一意の値を管理しています。

そのためインターネット上のMACアドレス検索サイト等で機器のMACアドレスを指定すれば製造者情報を確認することができますが、今回の設問では端末登録システムに端末の名称を加える事によって、管理が容易になるという事が解説されています。

1-2

伝送媒体

目的

- ネットワーク端末間の通信を行うためには伝送媒体によって接続する必要がある
- 伝送媒体にはさまざまな種類があるが、現在主流で利用されている伝送媒体はツイストペアケーブルと光ファイバケーブル
- それぞれのケーブルにはさまざまな規格があり、規格ごとに通信速度や接続可能距離が異なる。試験対策としてはそれぞれの媒体の特徴と通信可能な速度等の数値を認識しておく必要がある

1. 伝送媒体のしくみ

ネットワーク通信ではコンピュータで処理されるビットの情報をさまざまな伝送媒体を通じて転送しています。

この項目では、はじめに伝送媒体が用いられる LAN 規格種類の解説を行った後に、主要な伝送媒体である同軸ケーブル・ツイストペアケーブル・光ファイバケーブルについて解説していきます。

表 1.2.1 LAN 通信規格

	アクセス方式	伝送媒体	トポロジ
イーサネット	CSMA/CD	同軸ケーブル UTP ケーブル STP ケーブル 光ファイバ	バス型 スター型 スターバス型
トーカンリング	トーカンパッシング	STP ケーブル	リング型
FDDI	トーカンパッシング	光ファイバ	リング型

2. イーサネット

イーサネット (Ethernet) は現在最も普及している LAN の規格であり、1973年にゼロックス社で考案され、1979年にゼロックス社、DEC社（現HP社）、インテル社が協力してイーサネットの標準化を進め、翌1980年にイーサネットの最初の仕様であるDIXイーサネット（イーサネットVer1.0）が発表され、1982年はイーサネットVer2.0が発表されました。

イーサネットVer2.0を元に IEEE (The Institute of Electrical and Electronics Engineers, Inc. 米国電気電子学会) が標準化を行い、**IEEE 802.3** が策定されました。

当初のイーサネットは同軸ケーブルを伝送媒体として利用していましたが、時代の流れとともに、UTP/STPケーブル、光ファイバと伝送媒体が移り変わっていき、それに合わせて通信速度が向上し続けています。

3. トーケンリング /FDDI

トーケンリングはIBM社によって開発された通信規格で1984年にトーケンリングが開発され、IEEE 802.5の規格が策定されています。通信速度は4Mbps /16Mbpsで、リング型に接続されたネットワーク上をトーケンと呼ばれる信号が巡回しデータを転送します。

FDDI (Fiber-Distributed Data Interface) はトーケンリングにおける課題であった通信速度・冗長性を改善する目的で開発され、通信媒体は光ファイバケーブルを用い100Mbpsの通信が可能です。また、リングを2重構造にすることによって冗長性を確保しています。

イーサネットの高速化に伴い、1990年代以降あまり利用されていません。

4. 同軸ケーブル

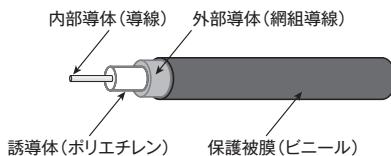


図 1.2.1 同軸ケーブル

同軸ケーブルはテレビを接続するケーブルと同様の形式でピット情報を電圧に変換し、内部導体と外部導体部分を通じて転送先のコンピュータに転送します。

同軸ケーブルはイーサネット初期から利用されていた形式ですが、データ転送速度が低速である事やネットワーク敷設時に配線の取り回しに手間がかかる事から現在のLAN環境ではありません。

同軸ケーブルでは10BASE-2と10BASE-5の2種類の規格を理解する必要があります。

表 1.2.2 同軸ケーブルの規格

名称	ケーブル形状	通信速度	伝送距離
10BASE-2	同軸ケーブル (RG-58)	10Mbps	185m
10BASE-5	同軸ケーブル (RG-11)	10Mbps	500m

5. ツイストペアケーブル

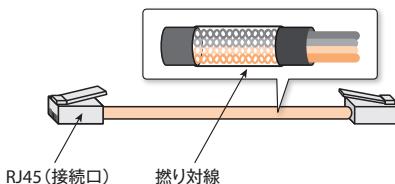


図 1.2.2 ツイストペア（より対）ケーブル

ツイストペアケーブルは現在のLAN環境でよく利用されるケーブルで、同軸ケーブルに比べて敷設時の取り回しに優れる事と高速な通信速度を実現する事が可能

です。

ツイストペアケーブルはゴム被膜の内部に8本の銅線が2本一組で撚られて内包されています。この銅線に対してシールドの有無によって **UTP ケーブル/STP ケーブル** に分類されます。

UTP (Unshielded Twisted Pair) ケーブル

8本の銅線がゴム被膜内にそのまま内包されています。一般家庭やオフィス環境で利用されます。

STP (Shielded Twisted Pair) ケーブル

2本一組で撚られた銅線をシールドで保護して、さらにゴム被膜で包みます。シールドは周囲の電磁波の影響が銅線に伝わる事を防止するため工場や野外等、周囲の電磁波の影響を受けやすい個所で利用されます。

さらに、ツイストペアケーブルには **カテゴリ** と呼ばれる規格があり、カテゴリごとに通信速度が定まっています。

表 1.2.3 ツイストペアケーブルのカテゴリ規格

カテゴリ	通信速度	最大周波数	用途
カテゴリ1	~20Kbps	-	電話線
カテゴリ2	~4Mbps	1Mhz	低速なデータ通信
カテゴリ3	~100Mbps	16Mhz	<ul style="list-style-type: none"> ・イーサネット 10BASE-T ・ファストイーサネット (100BASE-T2,T4) ・100VG-Any-LAN ・トーカンリング (4Mbps)
カテゴリ4	~100Mbps	20Mhz	<ul style="list-style-type: none"> ・カテゴリ3までの用途 ・トーカンリング (16Mbps) ・ATM (25Mbps)
カテゴリ5	~100Mbps	100Mhz	<ul style="list-style-type: none"> ・カテゴリ4までの用途 ・ファストイーサネット (100BASE-TX) ・ATM (156Mbps) ・CDDI (100Mbps ※ FDDIの銅線版)
カテゴリ5e	~1000Mbps	100Mhz	<ul style="list-style-type: none"> ・カテゴリ5までの用途 ・ギガビットイーサネット (1000BASE-T)
カテゴリ6	~1000Mbps	250Mhz	<ul style="list-style-type: none"> ・カテゴリ5eまでの用途 ・ATM (622Mbps/ATM1.2Gbps)

ツイストペアケーブルの両端には8本の銅線に対してRJ45ジャックが圧着され、ネットワーク端末の**RJ45ポート**に接続されます。

RJ45ポートには**MDI/MDI-X**と呼ばれる規格があり、ポートごとにどちらが適用されるかが定まっています。両者の違いは接続口内の8本のピンの送受信のピンの配置です。そのためネットワーク機器間の接続時にはMDI/MDI-Xの配列を理解しピン配列に適したケーブル、**ストレートケーブル**か**クロスケーブル**を利用する必要があります。

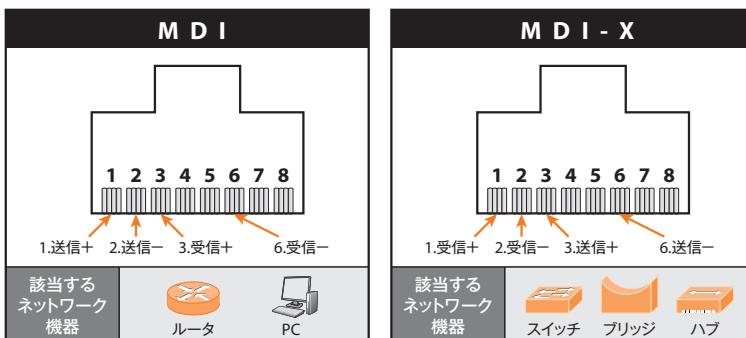


図1.2.3 RJ45ポートのピン配列

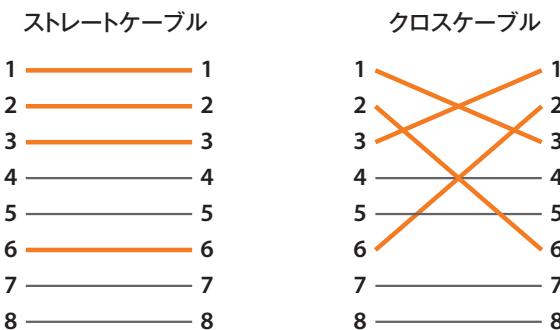


図1.2.4 ストレートケーブル/クロスケーブルのピン配列

ツイストペアケーブルはピン配列によってストレートケーブルとクロスケーブルに分類されます。

ストレートケーブルではケーブル両端のRJ45コネクタの1ピン～8ピンまでがそれぞれ同じピンが銅線で接続され、クロスケーブルでは1ピン \leftrightarrow 3ピン、2ピン \leftrightarrow 6ピンが銅線で接続され、4、5、7、8ピンはそれぞれ同じピンが接続されます。

そのため、ネットワーク機器間の接続は表1.2.3の組み合わせで行われます。

表1.2.3 MDI/MDI-Xとケーブルの接続組み合わせ

ポート	ケーブル	ポート
MDI	ストレートケーブル	MDI-X
MDI	クロスケーブル	MDI
MDI-X	クロスケーブル	MDI-X

異なるポート属性間の接続はストレートケーブルで接続し、ポート属性が同じ場合にはクロスケーブルで接続を行います。

接続する機器間のケーブル選択を誤るとネットワーク機器のリンクランプが点灯しませんので、その際にはケーブル種別が正しいかを確認しましょう。

また、現在では接続するネットワーク端末によって、MDIとMDI-Xの属性を自動的に切り替える、**AutoMDI/MDI-X**の機能を持つ端末が普及しています。



6. 光ファイバケーブル

光ファイバケーブルではピット信号を光の点滅信号に変換し、ネットワーク端末間の通信を行っています。

光ファイバケーブルはコアとクラッドと呼ばれる部品で構成され、その直径比によってシングルモードファイバとマルチモードファイバに分類されます。

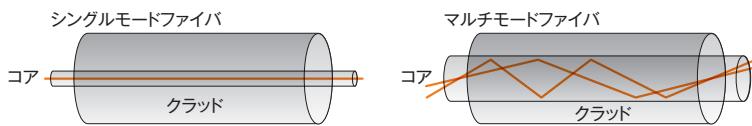


図1.2.5 光ファイバケーブルのシングルモードとマルチモード

シングルモードファイバ

シングルモードファイバはコアが9.2μm、クラッドが125μmとコアの直径が細く、光の信号は単一の位相で転送されるため到達時間にばらつきが発生しづらくなり、100kmまでの長距離伝送に対応することができますが、ケーブル単価は高く、配線時の曲げに弱いです。

マルチモードファイバ

マルチモードファイバはコアが $62.5\mu\text{m}$ 、クラッドが $125\mu\text{m}$ でコアの直径比はシングルモードファイバに比べて大幅に上がります。そのためコア内を伝送する光信号が分散される事となり、光信号の到達時間にはばらつきが発生しやすくなるため、長距離伝送には適していませんが、ケーブル単価は安く、配線時の曲げに強いです。

1-3

イーサネット

目的

- イーサネットでは伝送媒体、伝送方式、伝送速度によってさまざまな規格が適用されている
- イーサネットそれぞれの規格における通信速度や通信距離を認識しておく必要がある

イーサネット（Ethernet）は現在のLAN環境で主に利用されている通信規格であり、さまざまな通信媒体に対応し、MACアドレスを住所情報としてネットワーク機器間のデータ通信を実現します。



1. 通信規格の命名ルール

イーサネットは10BASE-2や100BASE-TXといったようにさまざまな通信規格名が存在します。以下に通信規格の命名ルールを記載します。

伝送速度	伝送方式	伝送媒体	ANSI規格
100	BASE	T	X

図1.3.1 100BASE-TXの命名ルール

伝送速度

伝送速度を示し、10の表記であれば10Mbps、100は100Mbps、1000は1000Mbps(1Gbps)、10Gは10Gbpsを示します。

伝送方式

ベースバンドシグナリング方式を示すBASEかブロードバンド方式を示すBROADが適用されますが、BASE方式が一般的に利用されます。

伝送媒体

数値、アルファベットが記載され、それにより以下の分類がされています。

表 1.3.1 伝送媒体の文字と種類

文字	媒体
2/5の数値	同軸ケーブル
T	ツイストペアケーブル
E/F/L/R/S	光ファイバ

規格

イーサネットはIEEEによって規格されていますが、Xが付いているケーブルは物理層仕様にANSI規格を流用している事を示しています。

表 1.3.2 通信規格一覧表

規格	標記	伝送媒体	波長	伝送距離
イーサネット (10Mbps)	10BASE-2	同軸ケーブル	-	185m
	10BASE-5	同軸ケーブル	-	500m
	10BASE-T	ツイストペアケーブル	-	100m
ファストイーサネット (100Mbps)	100BASE-TX	ツイストペアケーブル(CAT5以上)	-	100m
	100BASE-FX	マルチモードファイバ	1300nm か 850nm	半二重 412m 全二重 2000m
ギガビットイーサネット (1000Mbps)	1000BASE-T	ツイストペアケーブル(CAT5e以上)	-	100m
	1000BASE-SX	マルチモードファイバ	850nm	550m
	1000BASE-LX	マルチモードファイバ	1300nm	550m
		シングルモードファイバ	1300nm	5000m
10ギガビットイーサネット (10Gbps)	LAN PHY	10GBASE-T	ツイストペアケーブル(CAT6A以上)	-
		10GBASE-LX4	マルチモードファイバ	1310nm
			シングルモードファイバ	近辺の4つの 波長を多重化
		10GBASE-SR	マルチモードファイバ	850nm
		10GBASE-LR	シングルモードファイバ	1300nm
	WAN PHY	10GBASE-ER	シングルモードファイバ	1550nm
		10GBASE-SW	マルチモードファイバ	850nm
		10GBASE-LW	シングルモードファイバ	1300nm
		10GBASE-EW	シングルモードファイバ	1550nm
				40km

2. 通信規格の特徴

イーサネット

10Mbpsの通信速度を実現する通信規格をイーサネットと呼称します。

イーサネット開発当時は同軸ケーブルを利用したバス型トポロジを適用していましたが、敷設の柔軟性の高さからスター型トポロジに移行しツイストペアケーブルが利用されるようになりました。

ビットデータを送付するための伝送符号にはマンチェスタ符号が利用されます。

ファストイーサネット

ファストイーサネットでは100Mbpsの通信が定義されます。

現在一般的なコンピュータに搭載されるLANインターフェースはファストイーサネット対応のものが多く、広く利用されている規格です。

伝送媒体は、ツイストペアケーブルと光ファイバケーブルがあり、ツイストペアケーブルは伝送符号として4B/5B+MLT-3を利用し、ファイバケーブルでは4B/5B+NRZIを利用します。

ギガビットイーサネット

ギガビットイーサネットでは1000Mbps（1Gbps）の通信速度が定義されます。

符号化方式はツイストペアケーブルでは8B1Q4が利用され、ファイバケーブルでは8B10Bが利用されます。

10ギガビットイーサネット

10ギガビットイーサネットでは10Gbpsの通信速度が定義されます。

10ギガビットイーサネットでは符号化や光の波長等物理層の仕様によってさまざまな規格が存在していますが、大きく属性を分けるとLAN PHY（ランファイ）とWAN PHY（ワンファイ）の2つに分類されます。これらの違いはLAN PHYは近距離、WAN PHYは長距離というわけではなく、LAN PHYは従来のイーサネットを想定した接続性、WAN PHYはWAN回線のSONET/SDHとの接続性を想定しているところにあります。



3. イーサネットフレームフォーマット

イーサネット環境上でデータを送付する際には、フレームフォーマットに必要事項が登録された状態でデータ転送されます。

フレームフォーマットは**DIX仕様**とIEEE仕様がありますが、タイプの項目定義とオプションの有無以外は基本的に同様で、ネットワーク機器ではどちらの形式でも認識する事が可能です。

通常のTCP/IPネットワークではDIX仕様が適用されます。

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
8バイト	6バイト	6バイト	2バイト	46~1500バイト	4バイト

図1.3.2 DIX仕様イーサネットフレームフォーマット

プリアンブル

フレームの先頭には**プリアンブル**と呼ばれる、フレームの始まりを示す情報が格納されます。この情報は101010……と1と0のビットが62ビット続き、最後の2ビットは11にセットされ、その次の6バイトを宛先MACアドレス、次の6バイトを送信元アドレスとして認識します。

MACアドレス

MACアドレスの詳細は1章の1.1節を参照してください。

タイプ

フレームで転送するデータ部分の上位層プロトコルを識別します。

識別には以下のコードが定義されています。

表1.3.3 プロトコルとタイプコード

プロトコル	タイプコード
IPv4	0x0800
ARP	0x0806
IEEE 802.1Q	0x8100
IPv6	0x86DD
IEEE 802.3ad（リンクアグリゲーション）	0x8809

FCS (Frame Check Sequence)

FCSはデータの終端に位置し、フレームのエラーチェックを行うための情報が含まれています。

この情報は送信元がフレームを生成する際に計算して追加され、受信側はフレーム受信時に同じ計算をし、情報が一致しなければエラーフレームと判断し、フレームを破棄します。

例題

平成23年ネットワークスペシャリスト 午後I 問1 改題

問 宿泊施設へのLAN導入に関する次の記述を読んで、設問に答えよ。

○主任からLAN設計を指示されたU君は、製品の選定に着手した。

各製品の親機とL2スイッチ間の配線について検討した。各製品の親機のLANポートは、1000BASE-T規格である。製品P及び製品Cでは、親機の接続箇所と設備室間に新たな配線工事が必要になる。その配線長は、1000BASE-T規格の最大セグメントである【a】m以下であるが、配線経路の電磁環境を考慮すると波長850nmの光信号で通信を行う1000BASE-【ア】規格で中継することが望ましい。そのためには、UTPではなくマルチモード光ファイバでの配線とメディアコンバーターが必要になる。

設問 文章内の【a】と【ア】に入れる適切な字句を答えよ

例題解説 ➡➡➡

a 100

最大セグメント=1本のケーブルあたりの接続距離を示しているため、1000BASE-Tの規格から考察する。Tと付いているためツイストペアケーブルであることがわかるため、最大接続距離は100メートルとなる。

ア SX

通信規格については波長から推察する必要があり850nmの波長で1000Mbpsの通信が可能な規格は1000BASE-SXとなるためSXと回答します。

1-4

無線 LAN

目的

- 無線 LAN ではビットの信号を電波情報に変換し大気中に伝播させる事で通信を可能にしている
- さまざまな通信規格が存在するが、まずは周波数について理解をする必要がある

無線 LAN は電波を通じて LAN ネットワークを実現する技術であり、無線 LAN アクセスポイントを中心に数十メートル程度以内のネットワーク端末間の通信を可能にしています。

無線 LAN は日々技術進化を重ねており、「IEEE 802.11」で始まる通信規格が複数リリースされています。規格により通信速度・周波数・通信方式が異なるため目的に応じた規格を選択する必要があります。

また、電波による通信になるため有線 LAN にはない電波干渉や電波傍受といった点にも注意する必要があります。

1. 周波数

周波数の単位は「ヘルツ (Hz)」であり、1 ヘルツは 1 秒間に 1 回の周波数と定義されており、大気中に伝播されるさまざまな無線信号は、ヘルツを使い分ける事によって信号の混線を防いでいます。

身近な例で例えるとラジオのチャンネルは周波数で設定されており、私たちは受信機であるラジオの周波数ダイヤルを調整し、受信したいラジオ局のチャンネルを選択する事が出来ます。

つまり待機中の無線情報は送信するタイミングである周波数によって識別されており、この特性から、異なる情報源の周波数が重複、もしくは近い場合、電波干渉の状態になり情報伝達の効率が下がり、最悪、通信が不可能になってしまう場合があります。

2. 無線 LAN の規格

無線 LAN は数十メートル程度の範囲での高速データ通信に適した無線アクセス方式として、1990年代初頭に設立された IEEE 802.11 ワーキンググループで標準規格の策定が開始されました。現在、主に利用されている無線 LAN の通信規格は以下の4点です。

表 1.4.1 無線 LAN 通信規格の詳細

通信規格	周波数帯	制御方式	変調方式	最大速度	策定年
IEEE 802.11a	5GHz帯	CSMA/CA	OFDM	54Mbps	1999年
IEEE 802.11b	2.4GHz帯		CCK	11Mbps	1999年
IEEE 802.11g	2.4GHz帯		OFDM	54Mbps	2003年
IEEE 802.11n	2.4G/5GHz帯		OFDM	600Mbps	2009年

3. 無線 LAN 通信規格の用語解説

周波数帯・制御方式・変調方式について解説した後に各通信規格について解説します。

周波数帯

無線 LAN 向けの通信規格は主に 2.4GHz 帯と 5GHz 帯が利用されます。

2.4GHz 帯

ISM (Industry Science Medical) バンドと呼ばれる周波数帯で、産業科学医療バンドと呼ばれることもあり、さまざまな分野の無線機器に適用されています。

身近な機器としては電子レンジやコードレス電話、Bluetooth 等が 2.4GHz 帯を利用しており、無線 LAN ネットワーク構築時には 5GHz 帯の周波数と比べ電波干渉について留意する必要があります。

5GHz 帯

2005 年以前は日本独自で 5.15~5.25GHz の J52 を使用していましたが、電波法改正に伴い、世界標準のチャンネルに変更され 5.15~5.25GHz の W52 と 5.25G~5.35G の W53 が策定されました。この周波数帯は屋内での利用に限定され

していましたが、屋外用の周波数帯として5.47~5.725GHzのW56が2007年に追加で割り当てられました。

制御方式

無線LANでは、**CSMA/CA**(Carrier Sense Multiple Access with Collision Avoidance) 方式で端末間の通信制御を行っています。

無線LANは半二重の通信になるため同じ周波数帯で同時に電波を発信する端末が存在した場合にはコリジョンが発生します。

そのためCSMA/CAの制御により無線通信回線が一定時間継続して空いている状態を確認してから電波を送出し、複数の端末からの電波発信の混線を回避しています。

変調方式

変調方式はビットの信号を電波に変換して転送する際の方式です。無線LANの変調方式ではCCK方式とOFDM方式があります。

CCK変調方式

CCK (complementary code keying) はビットを電波信号に変換する際に、拡散符号という信号を掛け合わせて送信します。拡散符号によって電波の強弱（0と1を示す信号）が緩やかな信号となり、そのまま送付する場合に比べて周囲の電波干渉に強くなります。

OFDM変調方式

OFDM (Orthogonal Frequency Division Multiplexing) は直交周波数分割多重を示し、複数のサブキャリアと呼ばれる搬送波を周波数上に重ねて配置する事ができ、周波数帯を効率よく利用し高速な通信を実現することができます。

4. 無線LAN通信規格

IEEE 802.11a

1999年に策定された通信規格で5Gヘルツ帯の周波数を利用しOFDM変調方式で最大54Mbpsの通信を実現しています。

IEEE 802.11b

1999年に策定された通信規格で2.4Gヘルツ帯の周波数を利用しCCK変調方式で

最大11Mbpsの通信を実現しています。

IEEE 802.11g

2003年にIEEE 802.11bの高速化を目的に策定された方式で、OFDM変調方式にすることで最大54Mbpsの通信を実現しています。周波数帯はIEEE 802.11bと同じ2.4GHz帯を利用しているため、IEEE 802.11bとIEEE 802.11gが混在する環境では下位互換によって通信速度の低下を招きます。

IEEE 802.11n

IEEE 802.11nは2009年に策定され、複数の電波を利用した通信をすることによって高速通信を実現した通信規格です。IEEE 802.11nは次の技術によって高速通信を実現しています。

1) チャネルボンディング

無線LANでは通信に利用する周波数の幅が広いほど、多くの電波を伝送できるため高速通信が可能になります。**チャネルボンディング**では隣接する20MHz幅のチャネルを束ねて40MHz幅にする事が可能です。

2) MIMO

MIMO (Multiple input Multiple Output) は送信、受信にアンテナを複数利用してデータを分散して同時に送信する事を可能にする技術です。

IEEE 802.11nではストリームと呼ばれる通信経路を送信用、受信用に最大4本利用する事が可能で、チャネルボンディング・ストリームの組み合わせで表1.4.2の通信速度が実現可能です。

表1.4.2 IEEE 802.11nチャネルボンディングとMIMOの組み合わせによる通信速度

MIMO	20MHz	40MHz
1ストリーム	72.2Mbps	150Mbps
2ストリーム	144.4Mbps	300Mbps
3ストリーム	216.7Mbps	450Mbps
4ストリーム	288.9Mbps	600Mbps

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送信データを多数連結することによって、1回のフレームで大量のデータを送信し、データ送信している時間の割合を増やす技術です。

プロック ACK

プロック ACKはフレームの受信を確認する ACKを一括で行う技術で、最大64Kバイトのデータに対してまとめて1回の ACKを返す事によって待ち時間を短縮し転送速度を向上させる事が可能です。

また、IEEE 802.11nはIEEE 802.11a、IEEE 802.11b、IEEE 802.11gとの互換性を保つために3つのモードが定義されています。

表1.4.3 IEEE 802.11nの3つのモード

モード	対応可能規格	解説
レガシーモード (Legacy Mode)	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n	レガシーモードでは他の通信規格との互換性が担保され相互接続が可能だが、IEEE 802.11nの高速通信は実現できない
ミックスモード (Mixed Mode)	IEEE 802.11a IEEE 802.11g IEEE 802.11n	IEEE 802.11nのフレームの先頭にIEEE 802.1a/gのプリンブルを付加することで、IEEE 802.11a/gとの混在通信が可能になる しかしIEEE 802.11nからしてみればプリンブルが付加する事によってデータ量が増加してしまう
グリーンフィールドモード (Greenfield Mode)	IEEE 802.11g	IEEE 802.11nクライアントのみで動作するモードで、IEEE 802.11n本来の接続速度を実現する事ができる

5. 無線 LAN のモード

無線 LAN の通信モードにはアドホックモードとインフラストラクチャモードがあり、それぞれ通信に利用する機器が異なります。

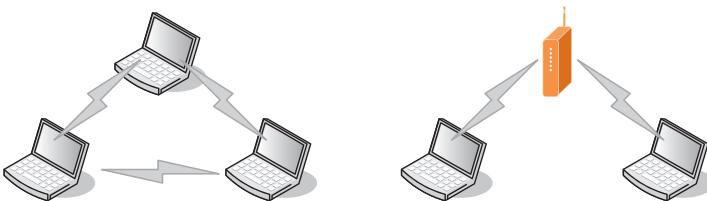


図 1.4.1 アドホックモードとインフラストラクチャモード

アドホックモード

無線 LAN クライアント端末に備わった無線 LAN カードのみを利用し、相互に通信するモードです。コンピュータどうしを直接通信させる場合や携帯ゲーム機等で主に利用されます。

アドホックモードは別名 IBSS (Independent Base Service Set) と呼ばれます。

インフラストラクチャモード

無線 LAN アクセスポイントを経由して無線 LAN クライアント端末が通信するモードで、企業内ネットワークや携帯キャリアが提供する無線 LAN スポットで利用されています。

6. 無線 LAN SSID

上記のインフラストラクチャモードでは複数の無線 LAN 端末がアクセスポイントを介して通信を行います。

無線 LAN の接続は電波で行いアソシエーションと呼ばれる論理的な接続を確立します。この際、どのアクセスポイントに接続するかの識別子として無線 LAN アクセスポイントに設定された **SSID** (Service Set ID) を利用しています。

SSID には BSSID (Basic Service Set ID) と ESSID (Extended Service Set ID) があり、BSSID ではアクセスポイントの識別子に MAC アドレスを使用し、ESSID では任意に設定された最大 32 文字の英数字を使用し、一般的な無線 LAN アクセスポイント

ではESSIDが適用されます。

管理者が無線LANアクセスポイントを設定する際に任意の文字列のESSIDを設定する事によって、ビーコン信号と呼ばれる制御信号が送信されます。ビーコン信号を受信した無線LANクライアント端末には、接続可能なアクセスポイントとしてESSIDの識別子が表示され、接続するESSIDを選択する事によって無線LANネットワークに接続できます。

この際、認証・暗号化等のセキュリティが適用されていない場合にはそのまま接続する事が可能ですが、多くの無線LAN環境では後述する無線LANセキュリティが適用されているため認証やパスワード入力の条件をクリアして接続する事が可能です。



7. 無線LANのセキュリティ

無線LANのセキュリティは主に認証と暗号化によって定義され、認証では無線LANに接続するユーザが正規の通信端末かを識別し、暗号化では無線で送信するデータが他のユーザに読み取られない形式に変換されます。

無線LANのセキュリティにはさまざまな技術があり、通常認証と暗号化を組み合わせて利用しています。

表 1.4.4 無線LANセキュリティ

無線LAN 初期		WPA		WPA2	
認証	・ステルスSSID ・MACアドレスフィルタリング ・オープン認証	認証	・IEEE 802.1X ・PSK	認証	・IEEE 802.1X ・PSK
暗号化	・WEP	暗号化	・TKIP・MIC	暗号化	・AES-CCMP

概要解説

無線LAN初期のセキュリティ

初期の無線LANではMACアドレスの認証やSSIDを通知しないステルスSSIDといった認証方式とWEPによる暗号化方式が用いられていましたが、技術の進歩によりセキュリティが容易に看破されるようになってしまいました。

WPA (Wi-Fi Protected Access)

2002年に WiFi Alliance が策定した規格で、従来の無線 LAN に採用されていた WEP の脆弱性を改善する目的で開発され、WPA では従来の SSID と WEP キーに加えてユーザ認証機能を備え、暗号鍵を一定時間ごとに変更する TKIP の機能を採用しています。

WPA2 (Wi-Fi Protected Access 2)

IEEE が無線 LAN のセキュリティ規格の標準化を IEEE 802.11i の名称ではじめ、2004年に IEEE 802.11i と WPA2 が策定されました。

WPA2 は WPA と認証部分では共通点が多く、IEEE 802.11x や PSK を利用しています。異なる点は WPA2 では暗号化方式に AES-CCMP を採用しており強力な暗号化を実現する事ができます。

詳細技術解説

ステルス SSID

通常 SSID はビーコン信号によってアクセスポイントが通信可能な範囲に伝播され、無線 LAN クライアント端末の選択可能な無線 LAN 一覧に表示されますが、ステルス SSID ではビーコン信号による SSID の伝播を停止し、無線 LAN クライアント端末から手動で SSID が設定された時に接続を許可するため、ステルス SSID の文字列を知っているユーザのみ接続をする事が可能です。

しかし無線ネットワークのデータを傍受すればステルス SSID の文字列が表示されてしまうためセキュリティリスクがあります。

MAC アドレスフィルタリング

無線 LAN クライアント端末に設定されている MAC アドレスを無線 LAN アクセスポイントに事前に登録しておくことにより、通信を許可する端末として認証をする事ができます。

しかし、MAC アドレスは通信を傍受する事で存在する MAC アドレスを知ることができると、MAC アドレスを偽装する事も可能であるためセキュリティリスクがあります。

オープン認証

アクセスポイントの SSID と無線 LAN クライアント端末の SSID が一致すれば通信を許可する方法で、実質認証はされていない状態に等しいです。

共有鍵認証

アクセスポイントにパスフレーズとして共有鍵を設定し、無線LANクライアント端末がSSIDを指定して接続をしてきた際に正しいパスフレーズを入力できれば通信を許可する端末として認証します。

パスフレーズは乱数で暗号化されてアクセスポイントとクライアント端末間で交換されますが、この際、暗号化前の情報と暗号化後の情報がネットワーク上に流れるため、通信傍受によってパスフレーズが解読されてしまう恐れがあります。

WEP

WEPはIEEEで標準化されたRC4と呼ばれるアルゴリズムをベースにした秘密鍵方式での暗号化を実現します。

秘密鍵には40ビットか128ビットのデータを利用することができますが、WEP自体にさまざまな脆弱性が発見されておりWEPのキーを数秒で解読できる方法も存在するため安全な暗号化方式とは言えません。

IEEE 802.1X

無線LAN、有線LAN上でネットワーク端末を認証する事ができる技術で、RADIUSサーバとネットワーク端末間でPPPを改良したEAP（Extensible Authentication Protocol）プロトコルによって認証を行い、その際に暗号化キーの元となるPMK（Pairwise Master Key）を生成し配布します。

また、IEEE 802.1Xでは認証に関する機器の役割対して以下の名称が定義されています。

サブリカント	無線LANクライアント端末
オーセンティケータ	無線LANアクセスポイント
オーセンティケーションサーバ	認証サーバ(RADIUSサーバ)

PSK (Pre Shared Key)

アクセスポイント上で設定する事ができ、アクセスポイントとクライアント端末間で同一文字列を設定し認証を行います。その際にRADIUSサーバ同様、PMKを生成しクライアント端末に配布されます。

TKIP (Temporal Key Integrity Protocol)

WEPと同じRC4の暗号化アルゴリズムを使用しますが、IEEE 802.11x/PSKとの組み合わせによって暗号化キーの生成が複雑化されているためWEPに比べて暗

号化強度は高いです。また、接続を行う度に暗号化キーを生成するので暗号化キーが固定化しません。

MIC (Message Integrity Check)

無線LAN端末間で送付されるデータの整合性をチェックしデータ改ざんを防止します。

AES-CCMP

暗号化アルゴリズムにAESを採用しTKIPに比べて強力な暗号化を実現し、データの整合性チェックを行う事もできます。

AESでは128ビット・192ビット・256ビットの3種類の鍵長が利用でき、米国標準の暗号化方式として採用されています。

例題

平成24年ネットワークスペシャリスト 午後I 問3

モバイル端末を利用したシステムの構築に関する次の記述を読んで、設問に答えよ。

〔無線LANの設計〕

システム企画課のG君は、まず、社内の無線LANの設計に着手した。次は、無線LANネットワークの設計に関する、G君と上司のH氏の会話である。

H氏：今日は無線LANの規格としてIEEE 802.11nを利用できるということだが、今まで使っていたIEEE 802.11gとはどこが違うのかな。

G君：はい。IEEE 802.11gでは帯域幅20MHzであったのに対し、IEEE 802.11nでは40MHzも利用可能になっています。これらは隣り合う20MHzのチャネルを二つ束ねる事によって、送信データ量を2倍以上に増やす【ア】という技術を使ったものです。これによって、例えば20MHzでは論理地で144Mビット／秒であった伝送速度が、最大で【イ】Mビット／秒になります。

また、送信側と受信側の双方で複数のアンテナを使い、同時に異なるデータを送信して受信時に合成する【ウ】という技術によって、データをより高速にやり取りする事ができます。

H氏：同時に、従来のIEEE 802.11gを引き続き利用しても問題ないのかな。

G君：IEEE 802.11nとIEEE 802.11gで同じチャネルを使った場合には、通

信ができないことがあります。それを回避するために、IEEE 802.11n の mixed mode では、フレームの先頭に IEEE 802.11g と同じ【 イ 】を付加して通信のタイミングをとり、同時利用を可能にすることができます。ただし、遅い方の通信速度に影響を受けて、スループットが低下します。

設問 文中の【 ア 】～【 イ 】に入る適切な字句を答えよ。

例題解説 →→→

ア チャネルボンディング

チャネルを束ねる技術はチャネルボンディングです。

イ 300

問題文章に 20MHz の際の通信速度が 144M ビット／秒(bps)と記載されているため MIMO の 2 ストリームを利用している事が想定されます。

アの解答のチャネルボンディング後の最大速度は 300M ビット／秒です。

ウ MIMO

複数のデータストリームを通じて通信する MIMO を示しています。

エ プリアンブル

IEEE 802.11n の互換性に関する問題で、IEEE 802.11a/g との混在通信を可能にする mixed mode では IEEE 802.11 n のフレームに対してプリアンブルを付加します。

第2章

WAN 技術

- 2.1 WAN
- 2.2 IP-VPN
- 2.3 広域イーサネット



試し読みはお楽しみ
いただけましたか？

ここからはManatee
おすすめの商品を
ご紹介します。

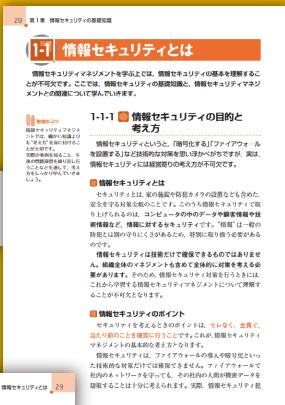
Tech Book Zone
Manatee 

1

**試験範囲を徹底分析&網羅!
初学者でも安心のSG対策書**

本書は、長年の指導経験に基づく試験分析とオリジナルAIによる分析を組み合わせて徹底的に改訂したSG(セマネ)対策書の決定版です。セキュリティ以外にも、テクノロジ系、ストラテジ系の基礎知識をしっかりと積み上げながら、関連度の高い周辺知識を合わせてていねいに解説し、初学者でも安心して学習ができる内容となっています。また、随所に演習問題を組み込み、巻末には平成28年度秋期試験の過去問題&解説を提供しています。

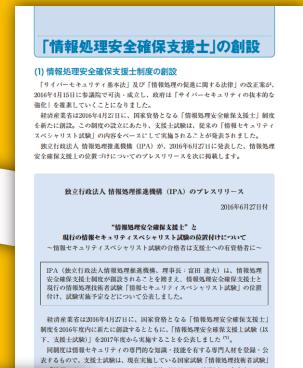
インプットした知識をしっかりと記憶に残せる、合格力がしっかりと身に付く構成



2

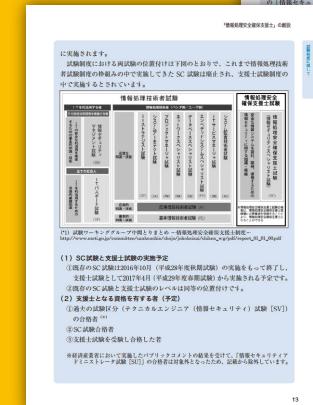
見て覚える! 短期集中型の試験問題対策書

情報処理安全確保支援士試験のため「どうすれば効率良く学習できるか」を最大限考慮した対策テキストです。試験そのものはこれまでの「情報セキュリティスペシャリスト試験」と変わらないため、たくさんストックされてきた過去問題を使う試験対策がベスト。本書も過去問題を最大限活用しながら学習が進むように構成しています。具体的には記述式の“過去問題”資産を使い分け、合格に重要な“午後問題”に絞り込み構成しました。



資格試験

演習問題を組み込むほか、
ダウンロード読者特典に
解説などを提供



徹底攻略 情報セキュリティ マネジメント教科書 平成29年度



IPA 試驗

これで合格!
情報処理安全確保
支援士試験





DTP エキスパート認証試験
唯一無二の詳細解説書！

その他



3

JAGAT DTP エキスパート認証試験
スーパーカリキュラム 第 12 版準拠

DTP エキスパートカリキュラム、最新第 12 版に準拠した詳解書です。カリキュラム解説+過去問題+公式模試で、合格できる力が身につきます。十分な用語解説（索引項目数約 2,000）、過去問題、模擬試験問題も掲載。

マイナビ出版
野尻研一（著者）
376 ページ 價格：4,860 円 (PDF)

CCENT/CCNA の
ICND1 新試験



6

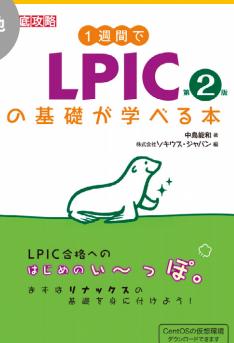
徹底攻略 Cisco CCENT/CCNA
Routing & Switching 教科書
ICND1 編 [100-105J] [200-125J] V3.0 対応

100-105J および 200-125J の試験範囲を丁寧に解説します。暗記においてはうが良い箇所や、試験対策に必要な知識も分かりやすくまとめてあります。演習問題もたくさん収録されているので、本番の試験対策もバッチャリ！

インプレス
株式会社ソキウス・ジャパン（著者）
864 ページ 價格：4,104 円 (PDF・書籍)

Linux 環境構築もラクラク
LPIC の基礎固めに最適な本

その他



4

1 週間で LPIC の基礎が学べる本
第 2 版

本書は、初心者がスムーズに試験対策を行えるよう、事前に基礎固めを行うための Linux 入門書です。試験情報や練習問題も数多く掲載しているので、資格取得を視野に入れた効率的な基礎学習が行えます。

インプレス
中島能和（著者）
296 ページ 價格：2,376 円 (PDF)

Java SE 7/8 Bronze 合格に
必要な知識をしっかり習得



7

徹底攻略 Java SE 7/8 Bronze
問題集 [1Z0-814] 対応

Java プログラマ資格の試験「Java SE 7/8 Bronze」(1Z0-814)に対応。Web からダウンロードできる模擬問題 60 開を付属した計 256 開を収録。初心者でも基礎が身に付くように配慮された問題構成が他にはない特徴です。

インプレス
志賀澄人・山岡敏夫（著者）
328 ページ 價格：2,484 円 (PDF)

コミカルな会話で理解する
IT パスポート対策書

IPA 試験



5

文系女子のための IT パスポート合格
テキスト&問題集

数学やパソコンが苦手な【ゆいさん】と学ぶ！会話形式でコミカルに読める文系人向けの IT パスポート学習書です。最新シラバス 3.0 に対応した丁寧な解説と巻末の問題集で、基礎学習から試験前の仕上げまでバッチャリ！

インプレス
滝口直樹（著者）
560 ページ 價格：1,490 円 (PDF)

Oracle Database 11g の
新機能もバッチャリ解説！



8

徹底攻略 ORACLE MASTER
Bronze DBA11g 問題集 [1Z0-018J] 対応

経験豊富な認定講師が 303 問を書き下ろし。その解説には設問のポイントが的確に解説されていて、合格に必要な知識を無理なく習得できます。さらに最終章には実際の試験を想定した模擬問題を掲載しました。

インプレス
小林圭、ソキウス・ジャパン（著者）
248 ページ 價格：2,777 円 (PDF)