IT資格道場

ネットワークスペシャリスト 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

IPA公式シラバス Ver.4.1(2023-12-25公開)準拠
2026年7月版

本書のご利用にあたって

- 本書は「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルであっても著作物です。本書の転載・改変しての再配布・二次販売を禁じます。
- 本書を AI モデルの学習データとして利用すること(学習目的の入力・データセット化を含む)を禁じます。
- 製品版(学習用テキスト・暗記用ノート・頻出度別ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

不正な配布を見つけた場合は info@shikaku-doujou.com までご連絡ください。

目次

はじめに —— この教材の使い方とスコープ

このテキストは、独立行政法人 情報処理推進機構(IPA)が実施する国家試験**ネットワークスペシャリスト試験(略号: NW)** の合格を目的に作られています。NW は情報処理技術者試験のなかで最上位の **スキルレベル 4(高度試験)** に位置づけられ、ネットワークの設計・構築・運用を担う専門家に求められる、プロトコル技術・セキュリティ実装・企画・運用の広く深い知識と技能を問います。

本書が対象とする範囲 —— 午前II(専門知識・多肢選択式)を軸に、午後試験(記述式)対策まで

ネットワークスペシャリスト試験は 4 つの試験区分で構成されます。**午前I(共通知識)・午前II(専門知識)** はどちらも多肢選択式(四肢択一)で、**午後I・午後II** はネットワーク構成図や設定を読み解いて答える記述式の長文事例問題です。

本書は、午前II(専門知識・多肢選択式)相当の対策を軸に構成しています(第1〜3部)。 午前II は、専門用語・プロトコルの挙動・計算・実装方式を「知っているか」で決まる知識確認型です。まずはここを確実に取り切ることが、午後へ進む前提になります。そのうえで **第4部(第13章)を午後試験(記述式)対策** にあて、本番の構成、本サイトに収録している記述式演習(令和7年度春期 午後I・午後II)で鍛えられる論点、答案の型をまとめました。

なお、2026 年度(令和 8 年度)からの CBT 方式移行に伴い、午前II は正式名称として **科目A-2** と呼ばれるようになりました(同様に、午前I → 科目A-1、午後I → 科目B-1、午後II → 科目B-2)。ただし **出題数・試験時間・出題形式・問われる知識の範囲は従来の午前II と変わりません(25 問・40 分・四肢択一)**。本書では学習者になじみのある「午前II」の呼称を用います。

午前II が合否を左右する理由 —— 段階別採点の「関門」

高度試験は **段階別採点** を採用しています。前の区分が基準点(100 点満点中 60 点)に達しないと、後続区分は採点されずに不合格になります。具体的には、**午前I が基準点未満なら午前II 以降は採点されず、午前II が基準点未満なら午後I・午後II は採点されません。**

投資でたとえるなら、午前II は **最初の建玉で含み損の許容ライン(損切り基準)を割ったら、その先のポジションを一切評価してもらえない** ようなものです。どれだけ午後の記述力を磨いても、午前II で 60 点(25 問中 15 問)を割れば、その答案は開かれないまま終わります。午前II は「足切りの関門」であり、確実に越えるべき最初の壁です。

試験の基本情報

項目	内容
試験名	ネットワークスペシャリスト試験(NW)。情報処理技術者試験のうち **スキルレベル 4(高度試験)**
実施	独立行政法人 情報処理推進機構(IPA)。経済産業省が所管する国家試験
本書の対象区分	**午前II(科目A-2)= 専門知識・多肢選択式**
午前II の出題数	**25 問**(全問必須解答)
午前II の試験時間	**40 分**
午前II の出題形式	**四肢択一式**(4 つの選択肢から 1 つ選ぶ)
午前II の基準点	**100 点満点中 60 点以上**(25 問中およそ 15 問正解が目安)

項目	内容
採点方式	**段階別採点**。前の区分が基準点未満だと後続区分は採点されない
午前I 免除	高度試験の午前I 通過者・応用情報技術者合格者などは、申請により**2 年間** 午前I が免除される(午前II は免除対象外)
実施方式・時期	**CBT 方式**(2026 年度から移行)。試験全体は前期・後期の 2 期制だが、**NW の実施は前期のみ(年 1 回)**
受験手数料	**7,500 円(税込)**
出題範囲	**シラバス Ver.4.1**(2023 年 12 月 25 日公開)ほか、公式の試験要綱・出題範囲に準拠

受験手数料・実施時期・制度は改定されることがあります。申し込み時に IPA の公式サイトで最新情報を必ず確認してください。

午前II の性格 ―― 「プロトコルとセキュリティ」に山がある

午前II は範囲こそ広いものの、出題の重心ははっきりしています。本書では、直近 3 回(令和 5〜7 年度春期)の公開された午前II 問題 計 75 問を、分野ごとに数え直しました。その結果は次のとおりです。

出題分野(本書の区分)	実測(75 問中)	目安比率
ネットワーク方式・プロトコル技術	約 38 問	約 51%
ネットワークセキュリティ実装技術	約 16 問	約 22%

出題分野(本書の区分)	実測(75 問中)	目安比率
運用・保守/サービス活用/関連法規	約 9 問	約 12%
企画・要件定義・設計(性能・信頼性設計を含む)	約 4 問	約 5%
参考: 共通テクノロジ系(コンピュータ構成・開発技術など)からの出題	約 7 問	約 9%

プロトコル技術とセキュリティ実装の 2 分野だけで、午前II のおよそ 4 分の 3 を占めます。限られた学習時間は、まずこの 2 本柱に厚く投じるのが最短です。企画・運用・法規は午前II では出題数こそ少ないものの(午後で厚く問われる領域です)、確実に数問は出るため、用語と考え方は押さえておきます。また、午前II には毎回 2 問前後、コンピュータ構成やソフトウェア開発といった共通テクノロジ系からの出題も混じります(詳しい格付けは「頻出度別ノート」を参照)。

3 ステップ学習法

購入者限定テキストは 3 冊で 1 セットです。次の順番で使うと最短です。

- **STEP 1(理解する)**: 本書「学習用テキスト」を通読し、プロトコルの挙動とセキュリティ実装の全体像を頭に入れる
- **STEP 2(覚える)**: 「暗記用ノート」の一問一答で、用語↔意味・略号↔役割を即答できるまで繰り返す
- **STEP 3(仕上げる)**: 「頻出度別ノート」で頻出度 A の論点から総点検し、本サイトの問題演習で四肢択一の形式と計算の速さに慣れる

時間がなければ、先に「頻出度別ノート」で頻出度 A(サブネット計算・ルーティング・IPsec/TLS・認証・攻撃対策)を確認し、そこを含む章から読み始めても構いません。

本書の構成(全 13 章・4 部)

出題の重心に沿って、プロトコル技術を最初に厚く置いています。

- **第 1 部 ネットワーク方式・プロトコル技術**(第 1〜6 章)… 最頻出。OSI/TCP-IP・アドレッシング・ルーティング・スイッチング・WAN/無線・QoS/IPv6
- **第 2 部 ネットワークセキュリティ実装技術**(第 7〜9 章)… 第 2 の柱。FW/IDS/IPS・VPN/暗号/認証・攻撃対策/ゼロトラスト
- **第 3 部 企画・設計と運用・保守**(第 10〜12 章)… 企画・要件定義・設計/運用・サービス活用/標準化・関連法規
- **第 4 部 午前IIから午後試験へ**(第 13 章)… 午前II で身につけた知識を、午後(記述式)にどうつなげるかの橋渡し

第1部 ネットワーク方式・プロトコル技術

第1章 OSI 参照モデルと TCP/IP プロトコルスタック

ネットワークの土台は「通信を階層に分けて考える」ことです。ここを曖昧にすると、上位のルーティングやセキュリティの理解がすべてぶれます。

1-1 OSI 参照モデルの 7 階層

OSI 参照モデルは、通信機能を 7 つの層に分けた国際標準の枠組みです。各層は「上の層にサービスを提供し、下の層のサービスを利用する」役割分担で動きます。

層	名称	主な役割	代表的な要素
第 7 層	アプリケーション層	利用者に近い通信サービス	HTTP・SMTP・DNS
第 6 層	プレゼンテーション層	データ表現形式の変換(文字コード・暗号・圧縮)	TLS の一部・文字コード変換
第 5 層	セション層	通信(セション)の確立・維持・終了の管理	セション管理
第 4 層	トランスポート層	端点間の通信制御・多重化	TCP・UDP・ポート番号
第 3 層	ネットワーク層	経路選択(ルーティング)・論理アドレス	IP・ルータ
第 2 層	データリンク層	同一セグメント内の中継・誤り検出	イーサネット・MAC アドレス・スイッチ

層	名称	主な役割	代表的な要素
第 1 層	物理層	ビット列を物理信号に変換して伝送	ケーブル・コネクタ・リピータ

午前II では「ある機能はどの層か」を問う設問が繰り返し出ます。押さえるべき対応は次の 3 つです。

- **ルーティング(経路選択)= 第 3 層(ネットワーク層)**。宛先 IP アドレスを見て経路を決める
- **スイッチング(MAC 中継)・誤り検出 = 第 2 層(データリンク層)**。宛先 MAC アドレスでフレームを中継する
- **ポート番号による多重化・信頼性制御 = 第 4 層(トランスポート層)**

1-2 TCP/IP モデルとの対応

実際のインターネットは、OSI より簡素な **TCP/IP モデル(4 層)** で動いています。両者の対応を押さえます。

TCP/IP モデル	対応する OSI の層	代表プロトコル
アプリケーション層	第 5〜7 層	HTTP・DNS・SMTP
トランスポート層	第 4 層	TCP・UDP
インターネット層	第 3 層	IP・ICMP
ネットワークインタフェース層	第 1〜2 層	イーサネット

インターネット層 = OSI 第 3 層(ネットワーク層) の対応が定番の問われどころです。

1-3 カプセル化 —— データが下位層へ渡る順序

送信側では、上位層のデータに各層のヘッダが順に付加されていきます。この過程を **カプセル化** といい、単位の名前が層ごとに変わります。

データ →(トランスポート層で TCP/UDP ヘッダ付与)→ セグメント →(ネットワーク層で IP ヘッダ付与)→ パケット(データグラム)→(データリンク層でヘッダ・トレーラ付与)→ フレーム →(物理層)→ ビット列

受信側では逆順にヘッダを外していきます(非カプセル化)。「セグメント → パケット → フレーム」の順序(上位から下位)が逆転していないかを問う設問が頻出です。

1-4 TCP と UDP —— 信頼性か即時性か

トランスポート層の 2 大プロトコルは、性格が正反対です。

	TCP	UDP
接続方式	**コネクション型**(通信前に接続を確立)	**コネクションレス型**(接続確立なしで送る)
信頼性	高い(再送・順序制御・フロー制御)	低い(送りっぱなし)
オーバーヘッド	大きい	小さい・低遅延
主な用途	Web・メール・ファイル転送	音声・映像・DNS 問合せ・SNMP

TCP と UDP の両方のヘッダに共通して存在するのは、送信元ポート番号・宛先ポート番号 です。宛先 IP アドレスや TTL は IP ヘッダの情報であり、トランスポート層のヘッダには含まれません。この区別が問われます。

1-5 TCP のコネクション制御(3 ウェイハンドシェイク)

TCP は通信開始時に、3 段階のやり取りで接続を確立します。これが **3 ウェイハンドシェイク** です。

1. クライアント → サーバ: **SYN**(接続要求)
2. サーバ → クライアント: **SYN + ACK**(要求受理と自分側の要求)
3. クライアント → サーバ: **ACK**(受理の確認)

このとき、サーバは待ち受け状態(**LISTEN**)で SYN を受け取り、応答を返して **SYN-RECEIVED** 状態へ遷移します。切断は原則 **4 回**(双方向にそれぞれ FIN と ACK)のやり取りで行われます。シーケンス番号は送信データのオクテット数だけ増加し、受信側は「次に受け取るべきシーケンス番号」を確認応答番号として返します。

再送と性能にかかわる仕組み(2026-08-18 追記)

- **選択確認応答(SACK)**: 受け取れた範囲を**飛び飛びで個別に**伝える拡張。損失より後ろのセグメントが届いていることを送信側が知れるので、**失われたセグメントだけを送り直せます**(SACK が無いと、そこから先をまとめて送り直すことになりがち)
- **遅延確認応答(遅延ACK)と Nagle アルゴリズム**: **Nagle = 小さなデータを確認応答が返るまでためて 1 つにまとめる／遅延ACK = 確認応答を少し待ってから返す。両方が効くと「待ち合わせ」が起きて応答時間が伸びる**ため、対話型の用途では Nagle を無効にすることがあります
- **ウィンドウスケールオプション**: TCP ヘッダのウィンドウサイズは **16 ビット(最大 64K バイト強)** しか表せません。**帯域遅延積がこれを超える長距離・高速の経路**では確認応答待ちで止まってしまうため、このオプションで

値を拡張します(シーケンス番号の一周対策はタイムスタンプオプションで、別物)

1-6 同一セグメントを支える補助プロトコル

- **ARP(アドレス解決プロトコル)**: 同一セグメント内で、宛先 **IP アドレスから MAC アドレスを解決** する。IPv4 で使われる
- **ICMP**: 到達性の確認やエラー通知を行う。`ping` (エコー要求/応答)で到達性を確かめ、`traceroute` は生存時間(TTL)を段階的に増やして経路上の各ルータを割り出す。到達不能・時間超過などのエラーも ICMP で通知される。IPv4 パケットが ICMP メッセージを運んでいることは、**IP ヘッダのプロトコル番号** で識別できる
- **DNS**: ドメイン名と IP アドレスを相互変換する(第 11 章で詳述)

1-7 ポート番号 —— どのアプリ宛かを見分ける

トランスポート層は **ポート番号** で通信を多重化します。よく使われるサービスには決まった番号(ウェルノウンポート)が割り当てられており、午前II ではこの対応がそのまま問われます。

ポート	プロトコル	用途
20 / 21	FTP(TCP)	ファイル転送(データ/制御)
22	SSH / SFTP(TCP)	暗号化された遠隔操作・転送
23	Telnet(TCP)	遠隔操作(平文)
25 / 587	SMTP(TCP)	メール送信・転送
53	DNS(UDP/TCP)	名前解決

ポート	プロトコル	用途
67 / 68	DHCP(UDP)	アドレス自動配布
80 / 443	HTTP / HTTPS(TCP)	Web
110 / 143	POP3 / IMAP4(TCP)	メール受信
123	NTP(UDP)	時刻同期
161 / 162	SNMP(UDP)	機器監視(問合せ/トラップ)
514	syslog(UDP)	ログ集約
1812 / 1813	RADIUS(UDP)	利用者認証(1812)/アカウンティング(1813)

DNS は短い問合せに UDP、大きな応答やゾーン転送に TCP を使う、というように 1 つのサービスが両方を使う場合もあります。番号と用途、そして UDP か TCP かをセットで覚えます。

1-8 イーサネットフレームと MTU

同一セグメントを流れるデータは、データリンク層で **イーサネットフレーム** に収められます。基本的なフレームは、宛先 MAC アドレス・送信元 MAC アドレス・タイプ(または長さ)・データ(ペイロード)・**FCS(フレームチェックシーケンス)** で構成され、FCS で誤りを検出します。

- **フレーム長の計算**: フレーム長は「ヘッダ各フィールド + ペイロード + FCS」の合計オクテット数として求められます。ペイロードには最小長・最大長の規定があり、上位から渡されたデータ量にヘッダとトレーラの固定長を足して算出します

- **MTU(最大転送単位)**: 1 つのフレームで運べるペイロードの最大長。イーサネットでは一般に 1,500 オクテットが標準です
- **フラグメンテーション**: 送るデータが MTU を超えると、IP は複数のパケットに分割(フラグメント化)して送り、受信側で組み立て直します。フラグメント化されずに一度に送れる上位データの最大長は、「MTU − IP ヘッダ − トランスポート層ヘッダ」で求められます

例題(本書オリジナルの考え方): MTU が 1,500 オクテット、IP ヘッダが 20 オクテット、TCP ヘッダが 20 オクテットのとき、フラグメント化されずに送れる TCP のデータ部は 1,500 − 20 − 20 = **1,460 オクテット** です。フレーム長を問う場合は、ここにさらに MAC ヘッダと FCS を足します。ヘッダの固定長を正確に足し引きできるかが得点の分かれ目です。

- **パス MTU 探索(Path MTU Discovery)**: 経路の途中に MTU の小さい区間があると、そこで分割か破棄が起きます。送信側は IP ヘッダの **分割禁止(DF)ビット** を立てたパケットを送り、MTU を超えて通せないルータから **ICMP の到達不能メッセージ(分割が必要)** を受け取ります。このメッセージには **次ホップの MTU** が入っており、送信側はそれに合わせて送信サイズを下げます。経路上のファイアウォールがこの ICMP を落とすと、通信が止まったまま原因が見えない状態(ブラックホール)になります
- **IPv4 と IPv6 の違い**: IPv4 では経路途中のルータもパケットを分割できますが、**IPv6 では途中のルータは分割しません**。分割が必要なら送信元が行う設計なので、**IPv6 ではパス MTU 探索の重要性が高い**
- **フラグメントの再構成**: 分割された IP パケットは**最終的な宛先ホストだけ**が組み立て直します。途中のルータは再構成しません。**断片が 1 つでも失われると元のパケット全体が失われた扱い**になり、上位層から見ると 1 つのパケットの喪失として現れます

- **ジャンボフレーム**: 標準の 1,500 オクテットを超える MTU(9,000 前後が一般的)を扱う拡張。1 フレームあたりの上位データが増えるためヘッダの割合とインタフェース処理の回数が減りますが、**経路上の機器がそろって同じ MTU を扱えることが前提**です。1 台でも標準 MTU の機器が挟まると、そこで分割か破棄が起きます

1-9 通信品質の基礎 —— 誤り率とスループット

- **ビット誤り率**: 1 ビットあたり誤りが起きる確率。データを一定サイズの電文に区切って送るとき、「誤りを含む電文の平均個数 ≒ 総ビット数 × ビット誤り率」で概算できる(電文数ではなく総ビット数に誤り率を掛ける点に注意)
- **誤り検出・訂正**: FCS(CRC)による検出、パリティや前方誤り訂正(FEC)による訂正など。検出だけか訂正までできるかで用途が変わる
- **伝送時間の計算**: 送るデータ量を回線の実効速度で割ると転送時間が出る(転送時間 = データ量 ÷ 実効速度)。実効速度は回線速度に伝送効率を掛けた値で、bit と byte(1 byte = 8 bit)の単位換算を取り違えないことが要点
- **回線利用率**: 単位時間に実際に流れたビット数を回線速度で割った割合。**利用率 =(1 秒あたりのフレーム数 × 1 フレームの平均長 × 8)÷ 回線速度**。ここでもフレーム長がバイトで与えられることが多いので、**8 倍してビットにそろえてから**割ること
- **帯域遅延積(BDP)**: **帯域幅 × 往復遅延時間(RTT)** で求める「確認応答が返るまでに回線上を飛んでいられるデータ量」。TCP の**ウィンドウサイズがこの値を下回ると、送信側が応答待ちで止まり回線を使い切れません**。例: 100M ビット/秒 × 0.04 秒 = 4M ビット = **500K バイト**。長距離・高速回線ほど大きくなるため、ウィンドウスケールオプションが要ります

- **PPP**: 2 点間を接続するデータリンク層のプロトコル。専用線でも交換網でも使え、**リンク確立の後に認証プロトコル(PAP/CHAP)を実行できる**。ダイヤルアップや WAN 接続の基礎として問われる

第1章の試験ポイント

- **経路選択=第 3 層/MAC 中継・誤り検出=第 2 層/ポート多重化=第 4 層**。TCP/IP のインターネット層=OSI 第 3 層
- カプセル化の順序: **セグメント → パケット → フレーム**(上位から下位)
- **TCP=コネクション型で信頼性重視/UDP=コネクションレスで低遅延**。共通ヘッダは**送信元・宛先ポート番号**
- 3 ウェイハンドシェイク=**SYN → SYN+ACK → ACK**。サーバは **LISTEN** で SYN を受ける
- **ARP=IP から MAC を解決/ICMP=到達性確認とエラー通知(ping)**
- ウェルノウンポート: **HTTP80/HTTPS443・SMTP25・DNS53・DHCP67-68・NTP123・SNMP161** など
- フラグメント化されない上位データ最大長=**MTU − IP ヘッダ − トランスポート層ヘッダ**。誤り電文数は**総ビット数 × ビット誤り率**
- **パス MTU 探索=DF ビット + ICMP 到達不能で次ホップ MTU を知る。IPv6 は途中のルータで分割しない**。ジャンボフレームは**経路全体で MTU をそろえるのが前提**
- **回線利用率=(毎秒フレーム数 × 平均フレーム長 × 8)÷ 回線速度、帯域遅延積=帯域幅 × RTT**。どちらもバイトとビットの換算が先

サンプルはここまでです

続き(第2章〜巻末)は、ネットワークスペシャリスト 問題集のご購入で、暗記用ノート・頻出度別ノートと合わせて3点すべてダウンロードできます。

ネットワークスペシャリスト 学習用テキスト(無料サンプル)

版

2026年7月版(IPA公式シラバス Ver.4.1(2023-12-25公開)準拠)

発行

IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com