

IT 資格道場

CCST ネットワーキング 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)

Cisco CCST Networking(100-150)出題範囲 Certiport「Objective Domains: CCST Networking」OD 0924(2026-10-09 取得)準拠
2026年10月版

ご利用にあたって

- このテキストは「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。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの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。

目次

この試験の範囲 [overview]

第1章 標準と概念

- 1.1 ネットワークの基礎的な部品 [1.1]
- 1.2 帯域幅とスループットの違い [1.2]
- 1.3 網の種類(LAN・WAN・MAN・CAN・PAN・WLAN)とトポロジ [1.3]
- 1.4 クラウドとオンプレミスの比較 [1.4]
- 1.5 代表的なプロトコルと使い方 [1.5]

サンプルはここまでです

この試験の範囲 [overview]

CCST ネットワーキング(試験コード 100-150)は、ネットワークがどう動くかを、機器・媒体・プロトコルの面から問う入門の試験です。対象は、ネットワークの技術者を目指す学生や実習生などです。次に進む資格は CCNA です(正式名称は Cisco Certified Network Associate)[^certiport-od-0924]。

範囲は 6 つの分野に分かれます。この教材も、同じ順に章を立てます(下の表)[^certiport-od-0924]。

分野	内容
1 標準と概念	モデル、帯域幅、網の種類、クラウド、プロトコル
2 IP アドレスとサブネット	プライベートとパブリック、IPv4、IPv6
3 端末と通信媒体	ケーブル、無線、端末、各 OS の確認方法
4 インフラストラクチャ	ランプ、配線、ポート、ルーティング、スイッチ
5 トラブルの診断	切り分けの手順、Wireshark、診断コマンド、遠隔操作、show コマンド
6 セキュリティ	ファイアウォール、基礎概念、無線の設定

第1章 標準と概念

1.1 ネットワークの基礎的な部品 [1.1]

OSI 参照モデルは、通信の働きを 7 つの層に分けて考えるための物差しです。層は下から数えます。番号と名前の組は、次の表のとおりです。試験でも、この組がそのまま問われます[^itu-x200-toc][^p-x200]。

層	名前	英語名
第 7 層	応用層	Application Layer
第 6 層	プレゼンテーション層	Presentation Layer
第 5 層	セッション層	Session Layer
第 4 層	トランスポート層	Transport Layer
第 3 層	ネットワーク層	Network Layer
第 2 層	データリンク層	Data Link Layer
第 1 層	物理層	Physical Layer

物理層は、データリンク層の間でビットを送るための、機械的、電氣的、機能的、手順的な手段を提供する層です(bit transmission)。データリンク層は、ネットワーク層同士のデータの受け渡しを支え、物理層で起きた誤りを検出する層です(error detection)[^p-x200]。

ネットワーク層は、データを運ぶ道筋の選び方や中継を受け持ち、上のトランスポート層にはその事情を意識させない層です。トランスポート層は、セッション層の間で、データを透過に(中身に手を加えずに)運ぶ層です[^p-x200]。

セッション層は、協力する上位の層の対話を整理し、同期を取り、データのやりとりを管理する層です。プレゼンテーション層は、応用層の間でやりとりするデータに、共通の表現を用意する層です。データ圧縮のような変換を受け持ちます。暗号化(encipherment)も、この層に置ける仕組みの 1 つです[^p-x200][^p-x800]。

インターネットで使う TCP/IP は、4 つの層で考えます。上から、応用層、トランスポート層、インターネット層、リンク層の順です(Application・Transport・Internet・Link)。TCP/IP の応用層は、OSI の応用層とプレゼンテーション層の働きをまとめて受け持ちます。TCP/IP は応用層をさらに分けません。OSI が 7 層で TCP/IP が 4 層なのは、同じ通信を別の切り方で見ているからです[^rfc1122]。

TCP/IP のトランスポート層は、端から端までの通信をアプリケーションのために受け持ちます。主なプロトコルは TCP と UDP の 2 つです。TCP は信頼できるコネクション型のサービスです。UDP はコネクションレス型で、「データグラム」のサービスと呼ばれます(datagram)[^rfc1122]。

トランスポートのプロトコルは、どれも IP(インターネットプロトコル)を使って、送り手から受け手までデータを運びます。この層がインターネット層です。IP は届くことを保証しません。IP のデータグラムは、壊れて届くことも、重複することも、順序が入れ替わることも、届かないこともあります。信頼できる配送が要る時は、IP より上の層が受け持ちます[^rfc1122]。

リンク層は、直接つながった網へデータを送り出す層です。リンク層のプロトコルは、網の種類に合わせて多くの種類があります[^rfc1122]。

フレームとパケットは、どの層で扱う単位かで区別します(frame と packet)。パケットは、インターネット層とリンク層の間で受け渡す単位で、IP ヘッダとデータでできています。フレームは、リンク層で送る単位です。リンク層のヘッダ

の後ろにパケットが続く形をしています。したがってパケットはフレームの中身になります(link-layer header + packet)。フレームのヘッダは、パケットに含まれません[^rfc1122]。

アドレス指定は、IP の 2 つの基本の働きの 1 つです。もう 1 つは分割(フラグメンテーション)です。IP のデータグラムのヘッダには、送り手と受け手のアドレスが入っています。RFC 791 は、名前とアドレスと経路を分けて説明します。名前は探している物、アドレスはそれがあある場所、経路はそこへの行き方です(name・address・route)。IP が主に扱うのは、アドレスだけです(名前から アドレスへの対応づけは上の層の仕事)[^rfc791]。

IPv4 のアドレスは 32 ビットで、4 つのオクテット(8 ビットずつ)でできています。IP の仕様は、端から端までの信頼性や順序の整理の仕組みを含みません[^rfc791]。

具体例から見ます。パソコンから Web サーバーへデータを送る時、データは層を下りながら包まれます。アプリケーションのバイトの流れは、TCP のセグメントに入ります。TCP のセグメントは、IP のデータグラムとして送られます。IP のデータグラムは、イーサネットのフレームの中身(データ欄)に入って送られます[^rfc9293][^rfc894]。

イーサネットのフレームは、先頭のヘッダに、宛先と送信元のアドレスを持ちます。中ほどのデータ欄には、IP ヘッダとその後ろのデータが入ります。最後に、4 オクテット(32 ビット)の FCS(Frame Check Sequence)が付きます。MAC アドレスは、イーサネットのインタフェースの識別子で、48 ビットの長さです。世界で一意なものは EUI-48 とも呼ばれます[^rfc894][^rfc1042][^rfc7042]。

ARP(Address Resolution Protocol)は、IPv4 アドレス(32 ビット)に対応する、イーサネットの 48 ビットのアドレス(MAC アドレス)を見つけるプロトコルです。同じネットワークの別のノードへ IPv4 パケットを送るには、宛先の MAC

アドレスを知る必要があります。ARP は、その対応を調べる役目です(RFC 826)[^rfc826][^rfc894]。

IPv4 のヘッダには、TTL(Time to Live)のフィールドがあります。送り手が値を決め、経路の途中で処理されるたびに減らします。TTL が 0 になると、データグラムは破棄されます。届かないデータグラムを捨て、データグラムの寿命の上限を決めるための仕組みです。第5章の `tracert` は、この TTL を使って経路を調べます[^rfc791]。

分割(フラグメンテーション)は、大きなパケットを許す網から出たデータグラムが、小さなパケットしか許さない網を通る時に必要になります。データグラムに「分割するな」の印を付けることもできます(don't fragment)。印の付いたデータグラムは、どんな状況でも分割されません[^rfc791]。

プロトコルがどの層に属するかは、次の表のとおりです[^rfc1122]。

層(TCP/IP)	主なプロトコル
応用層	HTTP、FTP、DHCP、DNS、NTP など
トランスポート層	TCP、UDP
インターネット層	IP、ICMP、IGMP
リンク層	イーサネット、ARP

1.2 帯域幅とスループットの違い [1.2]

具体例から見ます。1 Gbps の回線を引いた事務所で、ファイルの転送に実際に流れた量が 300 Mbps だったとします。このとき、回線の帯域幅は 1 Gbps で、スループットは 300 Mbps です。帯域幅は、リンクが運べる理論上の最大のデータの量を指す言葉として使われます(capacity)。スループットは、実際

に正しく届いたビットの数を、時間で割った実測の値です。帯域幅は上限、スループットは実測の値です。2 つは同じ物ではありません[^rfc5136]。

遅延(レイテンシ、latency、delay)は、パケットが届くまでにかかる時間です。RFC 7679 は、送り手が最初のビットを送った時刻から、受け手が最後のビットを受け取った時刻までの差を、片道の遅延と定めています。帯域幅は量の話で、遅延は時間の話です。ping は往復時間(round-trip time)を表示するので、遅延を見る手近な道具になります[^ms-ping][^rfc7679]。

スピードテスト(speed test)と iPerf は、どちらも速度を測りますが、測る区間が違います。スピードテストは、ブラウザなどから、インターネット上の測定用のサーバーとの間を測ります。iPerf は、TCP、UDP、SCTP の速度を測る道具で、サーバー役とクライアント役の間に実際に通信を流して、速度を出します(測る 2 台は自分で選ぶ)[^iperf][^certiport-od-0924]。

iPerf は、サーバー役とクライアント役の 2 台で動かします。サーバー側は `iperf -s` で待ち受けます。クライアント側は `iperf -c <ホスト>` で、サーバーにつながります。iPerf3 の既定のポート番号は 5201 です。ポートを指定しない時は、この 5201 が使われます(既定値)[^iperf]。

iPerf の主なオプションは次の 6 つです[^iperf]。

オプション	働き
<code>-u</code>	TCP の代わりに UDP で測る
<code>-b</code>	目標の帯域幅を決める。既定は UDP が 1 Mbit/秒、TCP は無制限
<code>-t</code>	測る時間を秒で決める
<code>-R</code>	向きを逆にする。サーバーが送り、クライアントが受ける

オプション	働き
-P	同時に流す本数(並列ストリーム)を決める
-O	最初の n 秒を集計から外す。TCP のスロースタートを除くため

`-i` は報告の間隔を秒で決めるオプションです。n 秒ごとに、帯域幅、ジッタ(揺らぎ)、損失が表示されます。ジッタは、パケットの遅延の変動です。RFC 3393 は、選んだパケットの片道の遅延の差を、遅延の変動(ipdv)と呼びます [^iperf][^rfc3393]。

単位時間あたりに正しい宛先へ届いたビットの数から、失われた分や再送された分を除いた値は、グッドプット(goodput)と呼びます (RFC 2647) [^rfc2647]。

iPerf の `-f` は、速度を表示する単位の文字を決めます。k は Kbits/秒、K は KBytes/秒、m は Mbits/秒、M は MBytes/秒です。大文字と小文字で、ビットとバイトが入れ替わります。`--sctp` は、TCP の代わりに SCTP で測ります [^iperf]。

具体例から見ます。拠点 A のパソコンで `iperf -s` を動かし、拠点 B のパソコンで `iperf -c <拠点 A のアドレス> -t 30 -P 4` を動かします。B から A へ向けて、4 本の並列ストリームで 30 秒間、TCP の速度を測ります。A に着いた量が、2 台の間のスループットです。iPerf3 のサーバー側は、同時に 1 つの接続しか受けません(only one iperf connection at a time)[^iperf]。

1.3 網の種類(LAN・WAN・MAN・CAN・PAN・WLAN)とトポロジ [1.3]

網の種類は、広がりと範囲で呼び分けます。LAN(Local Area Network)は、比較的狭い範囲に散らばったコンピューターなどを、通信の経路でつないだ網

です。WAN(Wide Area Network)は、LAN より多くの独立した利用者へデータ通信を届ける網で、LAN より広い地域に広がるのが普通です。本社と、離れた地域の支店をつなぐ網は、WAN の例です[^certiport-od-0924][^x-nist-lan][^x-nist-wan]。

LAN と WAN のほかに、MAN、CAN、PAN、WLAN の呼び分けがあります。MAN は Metropolitan Area Network の略で、WAN と同じく LAN より広い地域に広がり、いくつもの LAN をつなぐことがあります。CAN(Campus Area Network)は、いくつもの建物が並ぶ敷地のような、近くの地域に散らばった LAN のまとまりをつないで作る網です[^certiport-od-0924][^p-n-metropolitan_area_network][^cisco-what-is-lan][^cisco-campus-design]。

PAN(Personal Area Network)は、個人の身の回りの機器をつなぐ網です。Bluetooth は、短い距離の無線で、無線 PAN(WPAN)を作るために主に使われます(NIST SP 800-121)。WLAN(Wireless LAN)は、アクセスポイントとその周りの設備でできた、限られた範囲の無線の網です。ふつう有線 LAN の延長として作られ、利用者の動きやすさを高めます。WLAN の無線は、802.11 です(Wi-Fi)[^certiport-od-0924][^p-nist121][^p-n-wireless_local_area_network]。

トポロジは、網のつなぎ方の形です。試験の範囲には、物理的なトポロジと論理的なトポロジを見分けて、図に描くことが挙がっています。図に描く時は、どちらを描くのかを先に決めます(physical か logical か)[^certiport-od-0924]。

VLAN は、論理的なトポロジの代表例です。機能、プロジェクトチーム、アプリケーションなどの単位で論理的に分けたスイッチ網で、機器の物理的な場所

は問いません。たとえば、複数の階に散らばった営業部の機器を、1つのVLANにまとめられます[^cisco-9300-vlan]。

1.4 クラウドとオンプレミスの比較 [1.4]

試験の範囲には、クラウドとオンプレミスのアプリケーションとサービスを比べることが挙がっています。クラウドは、共有された設定可能な計算資源の集まりを、ネットワーク越しに、必要な時に使うやり方です。クラウドの分類は、NISTの文書が3つのサービスモデルと4つの配置モデルで定めています(SP 800-145)[^nist-800-145][^certiport-od-0924]。

具体例から見ます。Webブラウザで使うメールのサービスは、SaaS(Software as a Service)です。利用者は、提供者のアプリケーションを使うだけです。ネットワーク、サーバー、OS、ストレージを、利用者は管理しません[^nist-800-145]。

PaaS(Platform as a Service)は、利用者が作ったアプリケーションを、提供者の基盤に載せて動かす形です。利用者が管理するのは、載せたアプリケーションと、その動かす環境の設定です。ネットワーク、サーバー、OS、ストレージは管理しません。自社で作ったアプリケーションを、サーバーやOSを管理せずに動かしたい時はPaaSが合います[^nist-800-145]。

IaaS(Infrastructure as a Service)は、処理能力、ストレージ、ネットワークなどの基盤を借りる形です。利用者は、その上でOSやアプリケーションを自由に動かせます。管理するのはOS、ストレージ、載せたアプリケーションです。下にあるクラウドの基盤は、利用者の管理の外にあります[^nist-800-145]。

サービスモデルは、利用者が何を管理するかで比べると区別できます[^nist-800-145]。

モデル	利用者ができること	利用者が管理しないもの
SaaS	提供者のアプリケーションを使う	ネットワーク、サーバー、OS、ストレージ
PaaS	自分のアプリケーションを載せ、動かす環境を設定する	ネットワーク、サーバー、OS、ストレージ
IaaS	OS、ストレージ、載せたアプリケーションを管理する	その下のクラウドの基盤

配置のモデルは 4 つあります(deployment models)[^nist-800-145]。

モデル	使う人
パブリッククラウド	一般の人に開かれた利用のために用意される
プライベートクラウド	1 つの組織だけが使う
ハイブリッドクラウド	2 つ以上の別々のクラウドを組み合わせた形
コミュニティクラウド	共通の関心を持つ特定の利用者の集まりだけが使う

プライベートクラウドは、組織の敷地の中にあるとは限りません(on or off premises)[^nist-800-145]。

クラウドの特徴は、次の 5 つです[^nist-800-145]。

特徴	意味
オンデマンド・セルフサービス	利用者が、人手を介さずに、必要な時に必要な分の資源を用意できる

特徴	意味
幅広いネットワークアクセス	ネットワーク越しに、携帯電話やノート PC など、様々な端末から使える
資源の共用(リソースプール)	提供者の資源をまとめて、複数の利用者に割り当てる
素早い伸縮	需要に合わせて、資源を増やしたり減らしたりできる
使った量を測る(従量)	資源の使用量を測り、監視し、報告する

繁忙期だけ処理の能力を増やし、過ぎたら減らす使い方は、素早い伸縮の特徴を生かした例です[^nist-800-145]。

リモートワークは、自宅などの社外から、社内の網やクラウドの資源を使って働く形です。ハイブリッドワークは、出社とリモートワークを組み合わせる働き方です。どちらも、クラウドや VPN のように、社外から資源に届く手段があることを前提にします[^certiport-od-0924]。

1.5 代表的なプロトコルと使い方 [1.5]

まず TCP と UDP の違いを見ます (connection-oriented と connectionless)。TCP はコネクション型で、信頼できる、順序どおりのバイトの流れを届けます。UDP はコネクションレス型で、配送や重複の防止を保証しません。順序どおりで信頼できる配送が要るアプリケーションは、TCP を使うべきだと UDP の仕様が述べています (RFC 768)[^certiport-od-0924][^rfc1122][^rfc9293][^rfc768]。

TCP の接続は、3 ウェイハンドシェイクで確立します。クライアントが SYN を送り、サーバーが SYN と ACK を返し、クライアントが ACK を返します。UDP には、この手順がありません[^rfc9293]。

FTP(File Transfer Protocol)は、サーバーとクライアントの間でファイルを転送します。制御用の接続(コマンドと応答のやりとり)とデータ用の接続を分けて使います。制御用のポートは TCP 21 で、データ用のポートは 20 です[^iana-ports][^rfc959]。

SFTP(SSH File Transfer Protocol)は、SSH2 で使う標準のファイル転送のプロトコルで、安全なファイル転送の機能を提供します。SSH の上で動くので、ポートは SSH と同じ TCP 22 です。FTP とは別のプロトコルです[^iana-ports][^p-sftp13]。

TFTP(Trivial File Transfer Protocol)は、ごく単純なファイル転送のプロトコルです。UDP の上に作られていて、ポートは UDP 69 です。TFTP には、利用者を認証する仕組みがありません[^iana-ports][^rfc1350]。

HTTP は、接続の上でメッセージをやりとりする、要求と応答のプロトコルです。クライアントが要求を送り、サーバーが応答を返します。ポートは TCP 80 です。HTTPS は、TLS の上で HTTP を動かす形で、ポートは TCP 443 です。暗号化されるのは HTTPS だけです(HTTP over TLS)。HTTP の通信は、暗号化されません[^iana-ports][^rfc9110]。

DHCP は、ホストに IP アドレスなどの設定を自動で渡すプロトコルです。サーバーは UDP 67、クライアントは UDP 68 を使います。流れは 4 段階です。クライアントが DISCOVER を同じサブネットに一斉送信し、サーバーが OFFER で候補のアドレスを示します。クライアントは REQUEST で選んだ設定を求めます(request)。サーバーは ACK で確定します (DISCOVER → OFFER → REQUEST → ACK)[^iana-ports][^rfc2131]。

DNS(Domain Name System)は、ドメイン名から機器の IP アドレスを引くしくみです。ポートは 53 です。DNS は、ドメインの木の構造を持つネームサーバーが、情報を分けて持つ、分散した名前のサービスです。名前を引くのは DNS

で、アドレスを配るのは DHCP です。2 つの役割は混ぜません[^iana-ports][^rfc1034]。

用途からプロトコルを選ぶ練習をします。名前から IP アドレスを引くなら DNS です。機器へ IP アドレスなどの設定を自動で渡すなら DHCP です。時計を合わせるなら NTP です。暗号化された安全なファイル転送なら SFTP です (SSH の TCP 22)。ごく単純なファイル転送なら、TFTP(UDP 69)です[^iana-ports][^rfc1350][^rfc2131]。

ICMP は、データグラムの処理の誤りを知らせるプロトコルです。エコー要求とエコー応答は、ICMP のメッセージで、ping が使います (Echo and Echo Reply)[^rfc792]。

NTP(Network Time Protocol)は、インターネットで、コンピューターの時計を合わせるためのプロトコルで、ポートは 123 です。時刻の元になるサーバーは階層に並び、層の番号を stratum で表します。主サーバーが stratum 1 で、その下のサーバーは 1 つずつ大きい番号になります。番号が大きいほど、精度は落ちます[^iana-ports][^rfc5905]。

UDP のヘッダは短く、送り手のポート、宛先のポート、長さ、チェックサムでできています。送り手のポートは、省略もできるフィールドです。長さは、ヘッダとデータを合わせたオクテット数で、最小値は 8 です[^rfc768]。

TCP は、データを送る前に接続を確立します。この手順が 3 ウェイハンドシェイクです(コネクション型)。UDP は、データグラムの形のメッセージを送る仕組みで、配送も重複の防止も保証しません(コネクションレス型)[^rfc768]。

順序どおりに信頼できる配送が要るデータの流れは、TCP を使うべきだと UDP の仕様が述べています[^rfc768]。

HTTP のメソッドのうち、GET は対象の資源を取得します。POST は、対象の資源に、要求に入れたデータを処理させます[^rfc9110]。

HTTP の応答にはステータスコードが付きます。200 は要求が成功した印です。404 は、対象の資源が見つからない印です。500 は、サーバーが想定外の状態になり、要求を処理できなかった印です。404 は Not Found、500 は Internal Server Error の略称で呼ばれます[^rfc9110]。

HTTPS は、HTTP の通信を TLS(以前は SSL)で暗号化した形です。「HTTP over TLS」とも呼ばれます[^rfc2818]。

DHCP は、BOOTP をもとに、再利用できるアドレスの自動割り当てなどを足したプロトコルです。サーバーのポート 67 とクライアントのポート 68 は、BOOTP の番号を引き継いだ物です。REQUEST を受けたサーバーが、割り当てを確定し、設定を ACK に入れて返します。割り当ては、一定の期間だけ有効な貸し出し(リース)の形を取ります(lease)[^rfc2131][^iana-ports]。

DNS は、3 つの部品でできています。名前空間とリソースレコードは、木の形をした名前と、それに結び付いたデータの仕様です。ネームサーバーは、ドメインの木の構造や情報を持つサーバーのプログラムです。リゾルバーは、クライアントの要求を受けて、ネームサーバーから情報を取り出すプログラムです[^rfc1034]。

ICMP のメッセージは、型(Type)で区別します。エコー要求は型 8、エコー応答は型 0 です。型 11 は時間切れで、コード 0 は、経路の途中で TTL が尽きたことを示します。第5章の `tracert` は、この時間切れの応答で、途中のルーターを見つけます[^rfc792][^ms-tracert]。

型 3 は、宛先に届かないことを知らせます。コードで理由が分かれ、0 はネットワークに届かない、1 はホストに届かない、2 はプロトコルに届かない、3 はポ

ートに届かない、です[^rfc792]。

DNS のリソースレコードは、種類(TYPE)で区別します[^rfc1035]。

種類	意味
A	ホストのアドレス
NS	権威のあるネームサーバー
CNAME	別名の正式な名前
SOA	ゾーンの権威の始まりを示す
PTR	ドメイン名へのポインタ
MX	メールの交換先
TXT	文字列

TFTP は、ファイルを 512 バイトの固定長のブロックで送ります。1 つのデータパケットに 1 ブロックが入り、確認応答のパケットを受けるまで、次を送りません。512 バイトより小さいデータパケットが、転送の終わりの印です[^rfc1350]。

FTP のデータ用の接続は、データを転送する全二重の接続です。受け身のデータ転送の処理は、データ用のポートで待ち受け、能動側の処理からの接続を受けて、データ用の接続を開きます。命令と応答のやりとりは、制御用の接続を使います[^rfc959]。

NTP には、対称、クライアントとサーバー、ブロードキャストの 3 つの動作の形があります[^rfc5905]。

ポート番号を、まとめて表にします[^iana-ports]。

プロトコル	トランスポート	ポート
FTP(制御)	TCP	21
FTP(データ)	TCP	20
SSH・SFTP	TCP	22
TFTP	UDP	69
HTTP	TCP	80
HTTPS	TCP	443
DHCP(サーバー)	UDP	67
DHCP(クライアント)	UDP	68
DNS	TCP と UDP	53
NTP	UDP	123

サンプルはここまでです

続き(第2章～巻末)は、CCST ネットワーキング 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

CCST ネットワーキング 学習用テキスト(無料サンプル)

版

2026年10月版(Cisco CCST Networking(100-150)出題範囲 Certiport「Objective Domains: CCST Networking」OD 0924(2026-10-09 取得)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

Cisco、Cisco Systems、CCST は、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式の出題範囲の内容を基に作成したもので、Cisco および Certiport との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。