



# CompTIA Network+

## 認定資格試験

試験番号：**N10-007**



# 試験について

CompTIA Network+は、ファンダメンタルレベルのITネットワークプロフェッショナルに求められるスキルを評価する国際的に認知された認定資格です。

試験の目的：CompTIA Network+認定資格試験は、一般的なネットワーク機器のトラブルシューティング、構成、管理、基本的なネットワーク接続の確立、ネットワーク関連文書の理解と保管、ネットワークの制限と脆弱性の特定、ネットワークセキュリティ、規格、プロトコルなどについて、必要な知識とスキルを評価します。

受験者はクラウドと仮想化テクノロジーを含むエンタープライズテクノロジーについて基本的理解を持っている必要があります。

CompTIA Network+は、ISO 17024標準への準拠を米国国家規格協会 (ANSI) より認定されており、定期的な出題範囲の見直しおよびアップデートを行っています。

CompTIA Network+認定資格試験は、以下の条件を満たすITプロフェッショナルを対象としています。

- **CompTIA A+認定資格または同等の知識**
- **少なくとも9～12ヶ月のITネットワークングの業務経験**

## 認定資格試験の認証

CompTIA Network+は、国際標準化機構 (ISO) 17024 標準への準拠を米国国家規格協会 (ANSI) より認定されており、定期的な出題範囲の見直しおよびアップデートを行っています。

## 試験開発

CompTIA認定資格試験は、エントリーレベルのITプロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケート調査結果に基づいて策定されています。

## CompTIA認定教材の使用に関するポリシー

CompTIA Certifications, LLCは、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIAの認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIAでは、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、全員**CompTIA認定資格試験実施ポリシー**をご一読ください。CompTIAの認定資格試験を受験するための学習を始める前には、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者は**CompTIA受験者合意書**を遵守することが求められます。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA 担当窓口 (examsecurity@comptia.org) までお問い合わせください。

## 注意事項

箇条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。この出題範囲に掲載がない場合でも、各分野に関連する技術、プロセス、あるいはタスクを含む問題が出題される可能性があります。CompTIAでは、提供している認定資格試験の内容に現在必要とされているスキルを反映するため、また試験問題の信頼性維持のため、継続的な試験内容の検討と問題の改訂を行っています。必要な場合、現在の出題範囲を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

## 試験情報

試験	N10-007
問題数	最大90問
出題形式	単一/複数選択、シミュレーション
試験時間	90分
推奨経験	・ CompTIA A+認定資格または同等の知識 ・ ネットワークサポートもしくは管理、または 学校教育での9ヶ月以上のネットワーク学習経験
合格ライン	720（100～900のスコア形式）

## 出題範囲（試験分野）

下表は、この試験における試験分野（ドメイン）と出題比率の一覧です。

試験分野	出題比率
1.0 ネットワーキングの概念	23%
2.0 インフラストラクチャ	18%
3.0 ネットワークオペレーション	17%
4.0 ネットワークセキュリティ	20%
5.0 ネットワークのトラブルシューティングとツール	22%
計	100%



# 1.0 ネットワーキングの概念

1.1 ポートとプロトコルの目的と利用について説明することができる。

- **プロトコルとポート**
  - SSH 22
  - DNS 53
  - SMTP 25
  - SFTP 22
  - FTP 20, 21
  - TFTP 69
  - TELNET 23
  - DHCP 67, 68
  - HTTP 80
  - HTTPS 443
- **プロトコルの種類**
  - ICMP
  - UDP
  - TCP
  - IP
- **コネクション型とコネクションレス型の違い**
- **SNMP 161**
- **RDP 3389**
- **NTP 123**
- **SIP 5060, 5061**
- **SMB445**
- **POP 110**
- **IMAP 143**
- **LDAP 389**
- **LDAPS 636**
- **H.323 1720**

1.2 適切なOSIレイヤーのデバイス、アプリケーション、プロトコル、サービスを説明することができる。

- **レイヤー1-物理層**
- **レイヤー2-データリンク層**
- **レイヤー3-ネットワーク層**
- **レイヤー4-トランスポート層**
- **レイヤー5-セッション層**
- **レイヤー6-プレゼンテーション層**
- **レイヤー7-アプリケーション層**

1.3 ルーティングとスイッチングの概念と特徴を説明することができる。

- **ネットワークトラフィックのプロパティ**
  - ブロードキャストドメイン
  - CSMA/CD
  - CSMA/CA
  - コリジョンドメイン
  - プロトコルデータユニット
  - MTU
  - ブロードキャスト
  - マルチキャスト
  - ユニキャスト
- **セグメンテーションとインターフェースのプロパティ**
  - VLAN
  - トランキング (802.1q)
  - タグgingポートとアンタグgingポート
  - ポートミラーリング
  - スイッチンググループ
  - スパンニングツリー
  - PoEとPoE+ (802.3af, 802.3at)
- **DMZ**
- **MACアドレステーブル**
- **ARPテーブル**
- **ルーティング**
  - ルーティングプロトコル (IPv4とIPv6)
    - ディスタンスベクタルーティングプロトコル
      - RIP
      - EIGRP
    - リンクステートルーティングプロトコル
      - OSPF
      - ハイブリッド
        - BGP
  - ルーティングの種類
    - スタティック
    - ダイナミック
    - デフォルト
- **IPv6の概念**
- **アドレス指定**
- **トンネリング**
- **デュアルスタック**
- **ルーター広告**
- **近隣探索**
- **パフォーマンスの概念**
  - トラフィックシェーピング
  - QoS
  - Diffserv
  - CoS
- **NAT/PAT**
- **ポート転送**
- **アクセスコントロールリスト**
- **分散スイッチング**
- **パケット交換ネットワークと回線交換ネットワーク**
- **ソフトウェア定義ネットワーク**



1.4 与えられたシナリオに基づいて、適切なIPアドレスのコンポーネントを構成することができる。

- プライベートとパブリックの違い
- ループバックと予約済み
- デフォルトゲートウェイ
- 仮想IP
- サブネットマスク

- サブネッティング
  - クラスフル
  - クラスA、B、C、D、E
  - クラスレス
  - VLSM
  - CIDR表記法 IPv4とIPv6の違い

- アドレス割り当て
  - DHCP
  - DHCPv6
  - スタティック
  - APIPA
  - EUI64
  - IPアドレス予約

1.5 ネットワークトポロジー、種類、テクノロジーの特徴を比較対象することができる。

- 有線トポロジー
  - 論理と物理の違い
  - スター
  - リング
  - メッシュ
  - バス
- 無線トポロジー
  - メッシュ
  - アドホック
  - インフラストラクチャ

- 種類
  - LAN
  - WLAN
  - MAN
  - WAN
  - CAN
  - SAN
  - PAN

- IoT (モノのインターネット)を推進するテクノロジー
  - Z-Wave
  - Ant+
  - Bluetooth
  - NFC
  - IR
  - RFID
  - 802.11

1.6 与えられたシナリオに基づいて、適切なワイヤレステクノロジーと構成を実装することができる。

- 802.11規格
  - a
  - b
  - g
  - n
  - ac
- 携帯電話
  - GSM
  - TDMA
  - CDMA

- 周波数
  - 2.4GHz
  - 5.0GHz
- 速度と距離に関する要件
- チャンネル帯域幅
- チャンネルボンディング
- MIMO/MU-MIMO
- 指向性/全方向
- 現地調査



## 1.7 クラウドの概念とその目的を要約することができる。

- サービスの種類
  - SaaS
  - PaaS
  - IaaS
- クラウドデリバリーモデル
  - プライベート
  - パブリック
  - ハイブリッド
- 接続方法
- セキュリティの影響/考察
- ローカルリソースとクラウドリソースの関係

## 1.8 ネットワークサービスの機能を説明することができる。

- DNSサービス
  - レコードタイプ
    - A、AAAA
    - TXT (SPF、DKIM)
    - SRV
    - MX
    - CNAME
    - NS
    - PTR
  - 内向けDNSと外向けDNSの違い
  - サードパーティ/クラウドホスト型DNS
  - 階層
  - 正引きゾーンと逆引きゾーン
- DHCPサービス
  - MAC予約
  - ブール
  - IP除外
  - スコープオプション
  - リース期間
  - TTL
  - DHCPリレー/IP helper
- NTP
- IPAM



## 2.0 インフラストラクチャ

2.1 与えられたシナリオに基づいて、適切なケーブル配線ソリューションを展開することができる。

- **メディアの種類**
  - カッパーケーブル (銅線)
    - UTP
    - STP
    - 同軸
  - ファイバーケーブル
    - シングルモード
    - マルチモード
- **プレナムとPVCの違い**
- **コネクタの種類**
  - カッパーケーブル
    - RJ-45
    - RJ-11
    - BNC
    - DB-9
    - DB-25
    - F型
  - ファイバーケーブル
    - LC
    - ST
- **SC**
  - APC
  - UPC
  - MTRJ
- **トランシーバー**
  - SFP
  - GBIC
  - SFP+
  - QSFP
  - ファイバートランシーバーの特徴
    - 双方向
    - デュプレックス
- **端子**
  - 66ブロック
  - 110ブロック
  - パッチパネル
  - ファイバー配線パネル
- **カッパーケーブル規格**
  - CAT 3
  - CAT 5
  - CAT 5e
  - CAT 6
  - CAT 6a
  - CAT 7
  - RG-6
  - RG-59
- **カッパーケーブル終端規格**
  - TIA/EIA 568a
  - TIA/EIA 568b
  - クロスオーバー
  - ストレートスルー
- **イーサネット規格**
  - 100BaseT
  - 1000BaseT
  - 1000BaseLX
  - 1000BaseSX
  - 10GBaseT

2.2 与えられたシナリオに基づいて、ネットワーク上における適切なネットワーク機器の配置を決定し、設置／構成することができる。

- **ファイアウォール**
- **ルーター**
- **スイッチ**
- **ハブ**
- **ブリッジ**
- **モデム**
- **ワイヤレスアクセスポイント**
- **メディアコンバーター**
- **WiFi中継器 (ワイヤレスエクステンダー)**
- **VoIPエンドポイント**



### 2.3 高度なネットワーク機器の目的と利用事例を説明することができる。

- マルチレイヤスイッチ
- ワイヤレスコントローラー
- ロードバランサー
- IDS/IPS
- プロキシサーバー
- VPN コンセントレーター
- AAA/RADIUSサーバー
- UTMアプライアンス
- NGFW/L7ファイアウォール
- VoIP PBX
- VoIPゲートウェイ
- コンテンツフィルター

### 2.4 仮想化とネットワークストレージテクノロジーの目的を説明することができる。

- 仮想ネットワークングコンポーネント
  - 仮想スイッチ
  - 仮想ファイアウォール
  - 仮想NIC
  - 仮想ルーター
  - ハイパーバイザー
- ネットワークストレージの種類
  - NAS
  - SAN
- 接続の種類
  - FCoE
  - ファイバーチャネル
  - iSCSI
  - InfiniBand
- ジャンボフレーム

### 2.5 WANテクノロジーを比較対象することができる。

- サービスの種類
  - ISDN
  - T1/T3
  - E1/E3
  - OC-3 - OC-192
  - DSL
  - メトロイーサネット
  - ケーブルブロードバンド
  - ダイヤルアップ
  - PRI
- 伝送媒体
  - 衛星
  - カッパーケーブル
  - ファイバーケーブル
  - ワイヤレス
- サービスの特徴
  - MPLS
  - ATM
  - フレームリレー
  - PPPoE
  - PPP
  - DMVPN
  - SIP Trunk
- 終端
  - 責任分界点
  - CSU/DSU
  - スマートジャック





## 3.0 ネットワークオペレーション

3.1 与えられたシナリオに基づいて、ネットワーク管理のために適切な文書と図面を使用することができる。

- 図の記号
  - 標準操作手順/作業指示
  - 論理図と物理図の違い
- ラック図
  - 変更管理ポリシー
  - 配線位置とポート位置
  - IDF/MDFの文書化
- ラベリング
  - ネットワークの構成とパフォーマンスのベースライン
  - インベントリ管理

3.2 事業継続と災害復旧の概念を比較対象することができる。

- 可用性の概念
  - フォールトトレラランス
  - 高可用性
  - ロードバランシング
  - NICチーミング
  - ポート集約
  - クラスタリング
- パワーマネージメント
  - バッテリーバックアップ/UPS
  - 発電器
  - 二重化電源
  - 冗長回路
- リカバリ
  - コールドサイト
  - ウォームサイト
  - ホットサイト
- バックアップ
  - 完全
  - 差分
  - 増分
  - スナップショット
- MTR
- MTBF
- SLA要件

3.3 一般的なスキャン、モニター、パッチプロセスについて説明し、期待されるアウトプットを要約することができる。

- プロセス
  - ログのレビュー
  - ポートスキャン
  - 脆弱性スキャン
  - パッチ管理
    - ロールバック
  - ベースラインのレビュー
  - パケット/トラフィック解析
- イベント管理
  - 通知
  - アラート
  - SIEM
- SNMPモニター
  - MIB
- メトリクス
  - エラーレート
  - 使用状況
  - パケットドロップ
  - 帯域幅/スループット

3.4 与えられたシナリオに基づいて、適切なリモートアクセス方式を使用することができる。

- VPN
  - IPSec
  - SSL/TLS/DTLS
  - Site-to-site
  - Client-to-site
- RDP
- SSH
- VNC
- Telnet
- HTTPS/management URL
- リモートファイルアクセス
  - FTP/FTPS
  - SFTP
  - TFTP
- アウトオブバンド管理
  - モデム
  - コンソールルーター

3.5 ポリシーとベストプラクティスを特定することができる。

- 特権ユーザーアグリーメント
- パスワードポリシー
- オンボーディング/オフボーディング手続き
- ライセンス制限
- 国際輸出管理
- 情報漏えい防止
- リモートアクセスポリシー
- インシデント対応ポリシー
- BYOD
- AUP
- NDA
- システムライフサイクル
  - 資産の処分
- 安全手順と方針



## 4.0 ネットワークセキュリティ

4.1 物理的セキュリティデバイスの目的を要約することができる。

### •検知

- 人感センサー
- ビデオ監視
- アセットトラッキングタグ
- タンパー検知

### •予防

- バッジ
- 生体認証
- ICカード
- キーフォブ
- ロック

4.2 認証とアクセスコントロールについて説明することができる。

### •認証・認可・アカウントिंग (AAA)

- RADIUS
- TACACS+
- Kerberos
- シングルサインオン
- ローカル認証
- LDAP
- 証明書
- 監査とログ

### •多要素認証

- Something you know
- Something you have
- Something you are
- Somewhere you are
- Something you do

### •アクセスコントロール

- 802.1X
- NAC
- ポートセキュリティ
- MACフィルタリング
- キャプティブポータル
- アクセスコントロールリスト

4.3 与えられたシナリオに基づいて、基本的なワイヤレスネットワークをセキュアに接続することができる。

- WPA
- WPA2
- TKIP-RC4
- CCMP-AES

### •認証と認可

- EAP
- PEAP
- EAP-FAST
- EAP-TLS
- シェアードとオープン
- 事前共有鍵
- MACフィルタリング

### •ジオフェンシング



#### 4.4 一般的なネットワーク攻撃を要約することができる。

- DoS攻撃
  - Reflective
  - Amplified
  - Distributed
- ソーシャルエンジニアリング
- インサイダー脅威
- ロジックボム
- 不正なアクセスポイント
- エビルツイン(Evil twin)
- ウォードライビング
- フィッシング
- ランサムウェア
- DNSポイズニング
- ARPポイズニング
- スプーフィング
- 認証取り消し(Deauthentication)
- ブルートフォース攻撃
- VLANホッピング
- 中間者攻撃
- エクスプロイトと脆弱性

#### 4.5 与えられたシナリオに基づいて、ネットワーク機器のハードニングを実装することができる。

- デフォルトの認証情報を変更する
- よく使われるパスワードを避ける
- ファームウェアをアップデートする
- パッチとアップデートを適用する
- ファイルハッシング
- 不要なサービスを無効化する
- セキュアプロトコルを使用する
- 新しいキーを生成する
- 未使用のポートを無効化する
  - IPポート
  - デバイSPORT (物理と仮想)

#### 4.6 一般的な緩和手法とその目的について説明することができる。

- 署名管理
- デバイスのハードニング
- ネイティブVLANの変更
- スイッチポートの保護
  - スパニングツリー
  - フラッドガード
  - BPDUガード
  - ルートガード
  - DHCPスヌーピング
- ネットワークのセグメンテーション
  - DMZ
  - VLAN
- 特権ユーザーアカウント
- ファイル完全性モニタリング
- 職務分掌
- ACLによるアクセス制限
- ハニーポット/ハニーネット
- ペネトレーションテスト



## 5.0 ネットワークのトラブルシューティングとツール

### 5.1 ネットワークのトラブルシューティングの手法について説明することができる。

- 問題を特定する
  - 情報を収集する
  - 可能であれば、問題を再現する
  - ユーザーに質問する
  - 症状を特定する
  - 変更の有無を確認する
  - 複数の問題に個別に取り組む
- 想定される原因の仮説を立てる
  - 明白と思われる点も確認する
  - 複数の方法を考える
    - OSIモデルの上位層から下位層へ/下位層から上位層へ
- 分割統治
- 仮説を検証して原因を特定する
  - 仮説が証明された場合、問題解決に向けた今後の対応を決定する
  - 仮説が証明されなかった場合、仮説を立て直すか、エスカレーションする
- 問題解決のための対応計画を策定し、潜在的な影響を識別する
- 計画を実行するか、必要に応じてエスカレーションする
- システム全体の機能を検証し、必要に応じて予防対策を実施する
- 原因、対策、結果を文書化する

### 5.2 与えられたシナリオに基づいて、適切なツールを利用することができる。

- |                |  |            |
|----------------|--|------------|
| • ハードウェアツール    | • ソフトウェアツール                                |            |
| - クリンパー        | - パケットスニフアー                                | - ipconfig |
| - ケーブルテスター     | - ポートスキャナー                                 | - ifconfig |
| - パンチダウンツール    | - プロトコルアナライザー                              | - iptables |
| - OTDR         | - WiFiアナライザー                               | - netstat  |
| - 露出計          | - ブロードバンドスピードテスター (Bandwidth speed tester) | - tcpdump  |
| - トーンジェネレーター   | - コマンドライン                                  | - pathping |
| - ループバックアダプター  | - ping                                     | - nmap     |
| - マルチメーター      | - tracer, traceroute                       | - route    |
| - スペクトラムアナライザー | - nslookup                                 | - arp      |
|                |  | - dig      |

5.3 与えられたシナリオに基づいて、有線ネットワークの接続とパフォーマンスの一般的な問題をトラブルシューティングできる。

- ・減衰
- ・レイテンシー
- ・ジッター
- ・クロストーク
- ・EMI
- ・オープン/ショート
- ・誤ったピン配列
- ・誤ったケーブルの種類
- ・不正なポート
- ・トランシーバーの不一致
- ・TX と RX の逆転
- ・デュプレックス/速度の不一致
- ・ケーブルの破損
- ・ピンが曲がっている
- ・ボトルネック
- ・VLAN の不一致
- ・ネットワークステータスLED

5.4 与えられたシナリオに基づいて、無線ネットワークの接続とパフォーマンスの一般的な問題をトラブルシューティングできる。

- ・反射
- ・屈折
- ・吸収
- ・レイテンシー
- ・ジッター
- ・減衰
- ・誤ったアンテナの種類
- ・干渉
- ・誤ったアンテナの配置
- ・チャネルのオーバーラップ
- ・容量超過
- ・距離の制限
- ・周波数の不一致
- ・誤ったSSID
- ・誤ったパスワード
- ・セキュリティタイプの不一致
- ・電力レベル
- ・信号対雑音比 (S/N比)

5.5 与えられたシナリオに基づいて、ネットワークサービスの一般的な問題をトラブルシューティングできる。

- ・名前が解決していない
- ・誤ったゲートウェイ
- ・誤ったネットマスク
- ・IPアドレスの重複
- ・MACアドレスの重複
- ・IPアドレスの期限切れ
- ・不正なDHCPサーバー
- ・信頼できないSSL証明書
- ・誤った時間設定
- ・DHCPスコープの枯渇
- ・ブロックされているTCP/UDP
- ・誤ったホストベースのファイアーウォール設定  
設定が正しくない
- ・誤ったACL設定
- ・サービスが応答しない
- ・ハードウェア障害

# Network+略語一覧

下記はCompTIA Network+認定資格試験で使用される略語の一覧です。受験者には、試験準備の一環として、これらの用語を復習し、理解することをお勧めします。

略語	詳細説明	略語	詳細説明
AAA	Authentication Authorization and Accounting	CASB	Cloud Access Security Broker
AAAA	Authentication, Authorization, Accounting and Auditing	CAT	Category
ACL	Access Control List	CCMP	Counter-mode Cipher Block Chaining Message Authentication Code Protocol
ADSL	Asymmetric Digital Subscriber Line	CCTV	Closed Circuit TV
AES	Advanced Encryption Standard	CDMA	Code Division Multiple Access
AH	Authentication Header	CSMA/CD	Carrier Sense Multiple Access/Collision Detection
AP	Access Point	CHAP	Challenge Handshake Authentication Protocol
APC	Angle Polished Connector	CIDR	Classless Inter-Domain Routing
APIPA	Automatic Private Internet Protocol Addressing	CIFS	Common Internet File System
APT	Advanced Persistent Tool	CNAME	Canonical Name
ARIN	American Registry for Internet Numbers	CoS	Class of Service
ARP	Address Resolution Protocol	CPU	Central Processing Unit
AS	Autonomous System	CRAM-MD5	Challenge-Response Authentication Mechanism-Message Digest 5
ASCII	American Standard Code for Information Exchange	CRC	Cyclic Redundancy Checking
ASIC	Application Specific Integrated Circuit	CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
ASP	Application Service Provider	CSU	Channel Service Unit
ATM	Asynchronous Transfer Mode	CVE	Common Vulnerabilities and Exposures
AUP	Acceptable Use Policy	CVW	Collaborative Virtual Workspace
Auto-MDX	Automatic Medium-Dependent Interface Crossover	CWDM	Coarse Wave Division Multiplexing
BCP	Business Continuity Plan	Daas	Desktop as a Service
BERT	Bit-Error Rate Test	dB	Decibel
BGP	Border Gateway Protocol	DCS	Distributed Computer System
BLE	Bluetooth Low Energy	DDoS	Distributed Denial of Service
BNC	British Naval Connector/Bayonet Niell-Concelman	DHCP	Dynamic Host Configuration Protocol
BootP	Boot Protocol/Bootstrap Protocol	DLC	Data Link Control
BPDU	Bridge Protocol Data Unit	DLP	Data Loss Prevention
BRI	Basic Rate Interface	DLR	Device Level Ring
BSSID	Basic Service Set Identifier	DMVPN	Dynamic Multipoint Virtual Private Network
BYOD	Bring Your Own Device	DMZ	Demilitarized Zone
CaaS	Communication as a Service	DNAT	Destination Network Address Translation
CAM	Content Addressable Memory	DNS	Domain Name Service/Domain Name Server/Domain Name System
CAN	Campus Area Network	DOCSIS	Data-Over-Cable Service Interface Specification
CARP	Common Address Redundancy Protocol	DoS	Denial of Service

略語	詳細説明	略語	詳細説明
DPI	Deep Packet Inspection	IANA	Internet Assigned Numbers Authority
DR	Designated Router	ICA	Independent Computer Architecture
DSCP	Differentiated Services Code Point	ICANN	Internet Corporation for Assigned Names and Numbers
DSL	Digital Subscriber Line	ICMP	Internet Control Message Protocol
DSSS	Direct Sequence Spread Spectrum	ICS	Internet Connection Sharing/Industrial Control System
DSU	Data Service Unit	IDF	Intermediate Distribution Frame
DTLS	Datagram Transport Layer Security	IDS	Intrusion Detection System
DWDM	Dense Wavelength Division Multiplexing	IEEE	Institute of Electrical and Electronics Engineers
E1	E-Carrier Level 1	IGMP	Internet Group Message Protocol
EAP	Extensible Authentication Protocol	IGP	Interior Gateway Protocol
EBCDIC	Extended Binary Coded Decimal Interchange Code	IGRP	Interior Gateway Routing Protocol
EDNS	Extension Mechanisms for DNS	IKE	Internet Key Exchange
EGP	Exterior Gateway Protocol	IMAP4	Internet Message Access Protocol version 4
EMI	Electromagnetic Interference	InterNIC	Internet Network Information Center
ESD	Electrostatic Discharge	IoT	Internet of Things
ESP	Encapsulated Security Payload	IP	Internet Protocol
ESSID	Extended Service Set Identifier	IPAM	IP Address Management
EUI	Extended Unique Identifier	IPS	Intrusion Prevention System
FC	Fibre Channel	IPSec	Internet Protocol Security
FCoE	Fibre Channel over Ethernet	IPv4	Internet Protocol version 4
FCS	Frame Check Sequence	IPv6	Internet Protocol version 6
FDM	Frequency Division Multiplexing	ISAKMP	Internet Security Association and Key Management Protocol
FHSS	Frequency Hopping Spread Spectrum	ISDN	Integrated Services Digital Network
FM	Frequency Modulation	IS-IS	Intermediate System to Intermediate System
FQDN	Fully Qualified Domain Name	ISP	Internet Service Provider
FTP	File Transfer Protocol	IT	Information Technology
FTPS	File Transfer Protocol Security	ITS	Intelligent Transportation System
GBIC	Gigabit Interface Converter	IV	Initialization Vector
Gbps	Gigabits per second	Kbps	Kilobits per second
GLBP	Gateway Load Balancing Protocol	KVM	Keyboard Video Mouse
GPG	GNU Privacy Guard	L2TP	Layer 2 Tunneling Protocol
GRE	Generic Routing Encapsulation	LACP	Link Aggregation Control Protocol
GSM	Global System for Mobile Communications	LAN	Local Area Network
HA	High Availability	LC	Local Connector
HDLC	High-Level Data Link Control	LDAP	Lightweight Directory Access Protocol
HDMI	High-Definition Multimedia Interface	LEC	Local Exchange Carrier
HIDS	Host Intrusion Detection System	LED	Light Emitting Diode
HIPS	Host Intrusion Prevention System	LLC	Logical Link Control
HSPA	High-Speed Packet Access	LLDP	Link Layer Discovery Protocol
HSRP	Hot Standby Router Protocol	LSA	Link State Advertisements
HT	High Throughput	LTE	Long Term Evolution
HTTP	Hypertext Transfer Protocol	LWAPP	Light Weight Access Point Protocol
HTTPS	Hypertext Transfer Protocol Secure	MaaS	Mobility as a Service
HVAC	Heating, Ventilation and Air Conditioning		
Hz	Hertz		
IaaS	Infrastructure as a Service		



略語	詳細説明	略語	詳細説明
MAC	Media Access Control/Medium Access Control	OOB	Out of Band
MAN	Metropolitan Area Network	OS	Operating System
Mbps	Megabits per second	OSI	Open Systems Interconnect
MBps	Megabytes per second	OSPF	Open Shortest Path First
MDF	Main Distribution Frame	OTDR	Optical Time Domain Reflectometer
MDI	Media Dependent Interface	OUI	Organizationally Unique Identifier
MDIX	Media Dependent Interface Crossover	PaaS	Platform as a Service
MFA	Multifactor Authentication	PAN	Personal Area Network
MGCP	Media Gateway Control Protocol	PAP	Password Authentication Protocol
MIB	Management Information Base	PAT	Port Address Translation
MIMO	Multiple Input, Multiple Output	PC	Personal Computer
MLA	Master License Agreement/ Multilateral Agreement	PCM	Phase-Change Memory
MMF	Multimode Fiber	PDoS	Permanent Denial of Service
MOA	Memorandum of Agreement	PDU	Protocol Data Unit
MOU	Memorandum of Understanding	PGP	Pretty Good Privacy
MPLS	Multiprotocol Label Switching	PKI	Public Key Infrastructure
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol	PoE	Power over Ethernet
MSA	Master Service Agreement	POP	Post Office Protocol
MSDS	Material Safety Data Sheet	POP3	Post Office Protocol version 3
MT-RJ	Mechanical Transfer-Registered Jack	POTS	Plain Old Telephone Service
MTU	Maximum Transmission Unit	PPP	Point-to-Point Protocol
MTTR	Mean Time To Recovery	PPPoE	Point-to-Point Protocol over Ethernet
MTBF	Mean Time Between Failures	PPTP	Point-to-Point Tunneling Protocol
MU-MIMO	Multuser Multiple Input, Multiple Output	PRI	Primary Rate Interface
MX	Mail Exchanger	PSK	Pre-Shared Key
NAC	Network Access Control	PSTN	Public Switched Telephone Network
NAS	Network Attached Storage	PTP	Point-to-Point
NAT	Network Address Translation	PTR	Pointer
NCP	Network Control Protocol	PUA	Privileged User Agreement
NDR	Non-Delivery Receipt	PVC	Permanent Virtual Circuit
NetBEUI	Network Basic Input/Output Extended User Interface	QoS	Quality of Service
NetBIOS	Network Basic Input/Output System	QSFP	Quad Small Form-Factor Pluggable
NFC	Near Field Communication	RADIUS	Remote Authentication Dial-In User Service
NFS	Network File Service	RARP	Reverse Address Resolution Protocol
NGFW	Next-Generation Firewall	RAS	Remote Access Service
NIC	Network Interface Card	RDP	Remote Desktop Protocol
NIDS	Network Intrusion Detection System	RF	Radio Frequency
NIPS	Network Intrusion Prevention System	RFI	Radio Frequency Interference
NIU	Network Interface Unit	RFP	Request for Proposal
nm	Nanometer	RG	Radio Guide
NNTP	Network News Transport Protocol	RIP	Routing Internet Protocol
NTP	Network Time Protocol	RJ	Registered Jack
OCSF	Online Certificate Status Protocol	RPO	Recovery Point Objective
OCx	Optical Carrier	RSA	Rivest, Shamir, Adelman
OID	Object Identifier	RSH	Remote Shell
		RSTP	Rapid Spanning Tree Protocol
		RTO	Recovery Time Objective
		RTP	Real-Time Protocol

略語	詳細説明	略語	詳細説明
RTSP	Real-Time Streaming Protocol	TA	Terminal Adaptor
RTT	Round Trip Time or Real Transfer Time	TACACS	Terminal Access Control Access Control System
SA	Security Association	TACACS+	Terminal Access Control Access Control System+
SaaS	Software as a Service	TCP	Transmission Control Protocol
SAN	Storage Area Network	TCP/IP	Transmission Control Protocol/Internet Protocol
SC	Standard Connector/Subscriber Connector	TDM	Time Division Multiplexing
SCADA	Supervisory Control and Data Acquisition	TDR	Time Domain Reflectometer
SCP	Secure Copy Protocol	Telco	Telecommunications Company
SCSI	Small Computer System Interface	TFTP	Trivial File Transfer Protocol
SDLC	Software Development Life Cycle	TIA/EIA	Telecommunication Industries Association/ Electronic Industries Alliance
SDN	Software Defined Network	TKIP	Temporal Key Integrity Protocol
SDP	Session Description Protocol	TLS	Transport Layer Security
SDSL	Symmetrical Digital Subscriber Line	TMS	Transportation Management System
SECaaS	Security as a Service	TOS	Type of Service
SFP	Small Form-factor Pluggable	TPM	Trusted Platform Module
SFTP	Secure File Transfer Protocol	TTL	Time to Live
SGCP	Simple Gateway Control Protocol	TTLS	Tunneled Transport Layer Security
SHA	Secure Hash Algorithm	UC	Unified Communications
SIEM	Security Information and Event Management	UDP	User Datagram Protocol
SIP	Session Initiation Protocol	UNC	Universal Naming Convention
SLA	Service Level Agreement	UPC	Ultra Polished Connector
SLAAC	Stateless Address Auto Configuration	UPS	Uninterruptible Power Supply
SLIP	Serial Line Internet Protocol	URL	Uniform Resource Locator
SMB	Server Message Block	USB	Universal Serial Bus
SMF	Single-Mode Fiber	UTM	Unified Threat Management
SMS	Short Message Service	UTP	Unshielded Twisted Pair
SMTP	Simple Mail Transfer Protocol	VDSL	Variable Digital Subscriber Line
SNAT	Static Network Address Translation/Source Network Address Translation	VLAN	Virtual Local Area Network
SNMP	Simple Network Management Protocol	VLSM	Variable Length Subnet Mask
SNR	Signal-to-Noise Ratio	VNC	Virtual Network Connection
SNTP	Simple Network Time Protocol	VoIP	Voice over IP
SOA	Start of Authority	VPN	Virtual Private Network
SOHO	Small Office Home Office	VRF	Virtual Routing Forwarding
SONET	Synchronous Optical Network	RRP	Virtual Router Redundancy Protocol
SOP	Standard Operating Procedure	VTC	Video Teleconference
SOW	Statement of Work	VTP	VLAN Trunk Protocol
SPB	Shortest Path Bridging	WAF	Web Application Firewall
SPI	Stateful Packet Inspection	WAN	Wide Area Network
SPS	Standby Power Supply	WAP	Wireless Application Protocol/ Wireless Access Point
SSH	Secure Shell	WEP	Wired Equivalent Privacy
SSID	Service Set Identifier	WLAN	Wireless Local Area Network
SSL	Secure Sockets Layer	WMS	Warehouse Management System
SSO	Single Sign-on	WPA	WiFi Protected Access
ST	Straight Tip or Snap Twist	WPS	WiFi Protected Setup
STP	Spanning Tree Protocol/Shielded Twisted Pair	WWN	World Wide Name
SVC	Switched Virtual Circuit	XDSL	Extended Digital Subscriber Line
SYSLOG	System Log	XML	eXtensible Markup Language
T1	Terrestrial Carrier Level 1	Zeroconf	Zero Configuration

# Network+ハードウェアとソフトウェアの一覧

本リストは、CompTIA Network+の受験準備として役立てていただくためのハードウェアとソフトウェアのリストです。トレーニングを実施している企業でも、トレーニングの提供に必要な実習室コンポーネントを作成したい場合にも役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

## 機材

- ・オプティカル/銅パッチパネル
- ・パンチダウンブロック (110)
- ・レイヤー2/3スイッチ
- ・PoEスイッチ
- ・ルーター
- ・ファイアウォール
- ・VPNコンセントレーター
- ・ワイヤレスアクセスポイント
- ・仮想化をサポートするベシックノートパソコン
- ・タブレット/携帯電話
- ・メディアコンバーター
- ・コンフィグレーションターミナル (TelnetとSSH)
- ・VoIPシステム (電話を含む)

## 予備のハードウェア

- ・NICs
- ・電源
- ・GBICs
- ・SFPs
- ・マネージドスイッチ
- ・ハブ
- ・ワイヤレスアクセスポイント
- ・UPS

## 予備のパーツ

- ・パッチケーブル
- ・RJ-45コネクタ、モジュージャック
- ・RJ-11コネクタ
- ・非シールドツイストペアケーブルスプール
- ・同軸ケーブルスプール
- ・Fコネクタ
- ・ファイバーコネクタ
- ・アンテナ
- ・Bluetooth/ワイヤレスアダプター
- ・コンソールケーブル (RS-232-USBシリアルアダプター)

## ツール

- ・Telco/ネットワーククリンパー
- ・ケーブルテスター
- ・パンチダウンツール
- ・ケーブルストリッパー
- ・同軸ケーブルクリンパー
- ・ワイヤーカッター
- ・トーンジェネレーター
- ・ファイバー終端キット
- ・光パワーメーター

## ソフトウェア

- ・パケットスニファア
- ・プロトコルアナライザ
- ・端末エミュレーションソフトウェア
- ・Linux/Windows OS
- ・ソフトウェアファイアウォール
- ・ソフトウェアIDS/IPS
- ・Network mapper
- ・ハイパーバイザーソフトウェア
- ・仮想ネットワーク環境
- ・WiFiアナライザ
- ・スペクトラムアナライザ
- ・ネットワーク監視ツール
- ・DHCPサービス
- ・DNSサービス

## その他

- ・サンプルネットワーク文書
- ・サンプルログ
- ・欠陥のあるケーブル