

CompTIA Network+ (2009 年版) 認定資格試験出題範囲

CompTIA Network+(2009 年版)は、IT ネットワークプロフェッショナルに必要な専門知識を証明する国際的に認められた認定資格です。

CompTIA Network+認定資格を取得することにより、ネットワークインフラストラクチャの管理、運用、トラブルシューティング、構築、変更を実施することができる知識およびスキルを証明し、また、ネットワーク技術やネットワーク設計の原理原則、ワイヤリング規格の実行、試験ツールの使用に対しての知識を証明します。

この試験で評価されるスキル及び知識は、業界全体におけるジョブ タスク アナリシス (JTA)に基づき、2008 年第 2 四半期に行われたグローバルレベルの調査ではその検討および検証がされています。この調査の結果を基に、試験分野の内容および全体に対する出題比率を検討し、内容の相対的な重要性の裏付けをしています。

CompTIA Network+ (2009 年版)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、またはそれ同等の知識・スキルを所有していること
(CompTIA A+は、CompTIA Network+受験の際の前提条件ではありません。)
- ・ IT ネットワークにおける最低 9～12 ヶ月の業務経験^{※1}

以下の表は試験分野および各分野の出題比率です。^{※2}

CompTIA Network+ 認定試験分野	出題比率
第 1 章 ネットワーク技術	20%
第 2 章 ネットワークメディアとトポロジー	20%
第 3 章 ネットワークデバイス	17%
第 4 章 ネットワーク管理	20%
第 5 章 ネットワークツール	12%
第 6 章 ネットワークセキュリティ	11%

<注記>

※1 「最低 9ヶ月～12ヶ月の業務経験」とは、必要な技術知識、スキル習得の訓練を受けた後、9ヶ月～12ヶ月程度の実務経験を有することを指し、日本に見受けられる職務遂行前の研修期間を過ぎた後、9ヶ月～12ヶ月程度の実務経験で必須である技術知識、スキル、問題解決能力を問うものです。入社後の経験年数を指すものではありません。

※2 分野別に取扱例があげられていますが、これらがすべての出題傾向を網羅しているわけではありません。また、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、あるいはタスクについて、試験に含まれる可能性があります。

本出題範囲は、予告なく変更される場合がございます。あらかじめご了承ください。

第 1 章 ネットワーク技術(20%)

1.1 一般的なネットワークプロトコルの機能について説明することができる。

- TCP
- FTP
- UDP
- TCP/IP スイート
- DHCP
- TFTP
- DNS
- HTTP (S)
- ARP
- SIP (VoIP)
- RTP (VoIP)
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP v2 / v3
- ICMP
- IGMP
- TLS

1.2 一般的に使用される TCP および UDP デフォルトポートを特定することができる。

- TCP ポート
 - ・ FTP—20、21
 - ・ SSH—22
 - ・ TELNET—23
 - ・ SMTP—25
 - ・ DNS—53
 - ・ HTTP—80
 - ・ POP3—110
 - ・ NTP—123
 - ・ IMAP4—143
 - ・ HTTPS—443
- UDP ポート
 - ・ TFTP—69
 - ・ DNS—53
 - ・ BOOTPS/DHCP—67
 - ・ SNMP—161

1.3 以下のアドレスフォーマットを特定することができる。

- IPv6
- IPv4
- MAC アドレス

- 1.4 あるシナリオを想定した場合において、以下のアドレッシング技術とアドレッシングスキームの適切な使用について評価することができる。
- アドレッシング技術
 - ・ サブネットティング
 - ・ クラスフル / クラスレス（例：CIDR、スーパーネットティング）
 - ・ NAT
 - ・ PAT
 - ・ SNAT
 - ・ パブリック(グローバル) / プライベート
 - ・ DHCP（静的、動的、APIPA）
 - アドレッシングスキーム
 - ・ ユニキャスト
 - ・ マルチキャスト
 - ・ ブロードキャスト
- 1.5 一般的な IPv4 と IPv6 ルーティングプロトコルを特定することができる。
- リンクステート（Link state）
 - ・ OSPF
 - ・ IS-IS
 - デイスタンスベクター（Distance vector）
 - ・ RIP
 - ・ RIPv2
 - ・ BGP
 - ハイブリッド
 - ・ EIGRP
- 1.6 ルーティングの目的と特性について説明することができる。
- IGP / EGP
 - 静的 / 動的
 - ネクストホップ
 - ルーティングテーブルと経路選択方法との関連について理解する
 - コンバージェンスについて説明することができる
- 1.7 ワイヤレス通信基準の特徴を比較する。
- 802.11 a / b / g / n
 - ・ 速度
 - ・ 距離
 - ・ チャンネル
 - ・ 周波数
 - 認証と暗号化
 - ・ WPA
 - ・ WEP
 - ・ RADIUS
 - ・ TKIP

第2章 ネットワークメディアとトポロジー(20%)

2.1 一般的なケーブル種類と特性を特定することができる。

種類:

- CAT3、CAT5、CAT5e、CAT6
- STP、UTP
- マルチモードファイバー、シングルモードファイバー
- 円軸ケーブル (Coaxial)
 - ・ RG-59
 - ・ RG-6
- シリアル
- プレナム / 非プレナム

特性:

- 通信速度
- 距離
- デュプレックス (全二重)
- ノイズ耐性 (セキュリティ、EMI)
- 周波数

2.2 一般的なコネクタの種類を特定することができる。

- RJ-11
- RJ-45
- BNC
- SC
- ST
- LC
- RS-232
- RG-59
- RG-6

2.3 一般的な物理的ネットワークトポロジーを特定することができる。

- Star
- Mesh
- Bus
- Ring
- ポイントツーポイント (Point to point)
- ポイントツーマルチポイント (Point to multipoint)
- ハイブリッド

2.4 あるシナリオを想定した場合において、適切なワイヤ規格を特定し、実装することができる。

- 568A
- 568B
- ストレート / クロスオーバー
- ロールオーバー
- ループバック

2.5 WAN 技術の種類と特性について区別することができる。

種類:

- フレームリレー
- E1/T1
- ADSL
- SDSL
- VDSL
- ケーブルモデム
- 衛星
- E3/T3
- OC-x
- ワイヤレス
- ATM
- SONET
- MPLS
- ISDN BRI
- ISDN PRI
- POTS
- PSTN

特性:

- 回路スイッチ
- パケットスイッチ
- 速度
- 伝送媒体
- 距離

2.6 LAN 技術の種類と特性について区別することができる。

種類:

- イーサネット
- 10Base-T
- 100Base-TX
- 100Base-TF
- 100Base-FX
- 1000Base-T
- 1000Base-X
- 10GBase-SR
- 10GBase-LR
- 10GBase-ER
- 10GBase-SW
- 10GBase-LW
- 10GBase-EW
- 10GBase-T

特性:

- CSMA/CD
- CSMA/CA
- ブロードキャスト
- コリジョン
- ボンディング (Bonding)
- 速度

- 距離
- WRED

2.7 一般的な論理ネットワークポロジとその特徴について説明することができる。

- ピアツーピア
- クライアント/サーバー
- VPN
- VLAN

2.8 配線装置を実装することができる。

- 垂直コネクと水平クロスコネク
- 配線盤
- 66 Block
- MDF
- IDF
- 25 ペア
- 100 ペア
- 110 Block
- Demarc
- Demarc 拡張
- スマートジャック
- 配線装置の確認
- 配線終端の確認

第3章 ネットワークデバイス(17%)

3.1 一般的なネットワークデバイスを設定、構成、区別することができる。

- ハブ
- リピーター
- モデム
- NIC
- メディアコンバーター
- スイッチ
- ブリッジ
- ワイヤレスアクセスポイント
- ルーター
- ファイアーウォール
- DHCP サーバー

3.2 特化したネットワークデバイスの機能を特定することができる。

- マルチレイヤースイッチ
- コンテントスイッチ
- IDS/IPS
- ロードバランサー(負荷分散装置)
- 多機能ネットワークデバイス
- DNS サーバー
- 帯域幅制御装置(Bandwidth shaper)
- プロキシサーバー
- CSU/DSU

3.3 スイッチの拡張機能について説明することができる。

- PoE
- スパニングツリー
- VLAN
- トランッキング
- ポートミラーリング
- ポート認証

3.4 基本的なワイヤレスネットワークを実装することができる。

- クライアントの設定
- アクセスポイントの配置
- アクセスポイントの設定
 - ・ 適切な暗号化の構成
 - ・ チャネルと周波数の構成
 - ・ ESSID とビーコンの設定
- 設定を確認する

第4章 ネットワーク管理(20%)

4.1 OSI モデルの各レイヤー機能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

4.2 構成管理文書の種類を特定することができる。

- 配線図
- 物理/論理ネットワーク構成図
- ベースライン
- ポリシー、手順、設定情報
- 規定

4.3 あるシナリオを想定した場合において、構成管理文書に基づいたネットワークを評価することができる。

- 配線図、物理/論理ネットワーク構成図、ベースライン、ポリシー、手順、構成を、実際のネットワークデバイスやネットワークインフラストラクチャと比較する
- 配線図、物理/論理ネットワーク構成図、構成、作業ログを必要に応じて更新する

4.4 以下を使用して、パフォーマンスと接続性に関する問題を特定するためネットワークの監視を実行することができる。

- ネットワーク監視ユーティリティ (例: パケットスニファァ、接続ソフトウェア、負荷テスト、スループットテスト)
- システムログ、ヒストリーログ、イベントログ

4.5 ネットワークパフォーマンスを最適化のための様々な方法と根拠について説明をすることができる。

手法:

- QoS
- トラフィックシェーピング (Traffic shaping)
- ロードバランシング (負荷分散)
- ハイアベイラビリティ (高可用性)
- キャッシングエンジン
- フォールトトレランス

根拠:

- 遅延検出 (Latency sensitivity)
- 高帯域幅アプリケーション
 - ・ VoIP
 - ・ ビデオアプリケーション
- アップタイム

4.6 あるシナリオを想定した場合において、以下のネットワークトラブルシューティング方法を実行することができる。

- 情報収集 – 現象と問題を特定する
- ネットワークで問題が発生しているところを特定する
- 変更された部分の有無を判明する
- 最も可能性の高い原因の仮説を立てる
- エスカレーションが必要であるかを判断する
- 可能性のある影響を考慮して対応計画と解決策を策定する
- 解決策を実施およびテストする
- 解決策の結果と効果を特定する
- 解決策と全プロセスを文書化する

4.7 あるシナリオを想定した場合において、一般的な接続問題の適切な解決策を選択しトラブルシューティングすることができる。

物理的問題:

- クロストーク
- 減衰
- コリジョン
- ショート
- エコー
- 干渉

論理的問題:

- ポート速度
- ポートデュプレックスミスマッチ
- 誤った VLAN 設定
- 誤った IP アドレス設定
- 間違ったゲートウェイ設定
- 間違った DNS
- 間違ったサブネットマスク

特定され、エスカレートされるべき問題:

- ・ スイッチングループ
- ・ ルーティングループ
- ・ ルーティングトラブル
- ・ proxy arp
- ・ ブロードキャストストーム

ワイヤレス問題:

- ・ 干渉 (ブリード、環境要因)
- ・ 間違った暗号化
- ・ 間違ったチャンネル
- ・ 間違った周波数
- ・ ESSID の不一致
- ・ 規格の不一致 (802.11 a/b/g/n)
- ・ 距離
- ・ バウンス
- ・ 間違ったアンテナの配置

第5章 ネットワークツール(12%)

5.1 あるシナリオを想定した場合において、適切なコマンドラインインターフェースを選択し、機能を確認するため出力を読み取ることができる。

- traceroute
- ipconfig
- ifconfig
- ping
- arp ping
- arp
- nslookup
- host
- dig
- mtr
- route
- nbtstat
- netstat

5.2 ネットワークスキャナの目的について説明することができる。

- パケットスニファ
- IDS(Intrusion Detection System/侵入検知システム)
- IPS(Intrusion Prevention System/侵入防止システム)
- ポートスキャナー

5.3 あるシナリオを想定した場合において、適切なハードウェアツールの活用することができる。

- ケーブルテスター
- プロトコルアナライザー
- サーティファイアー(認証機器)
- TDR
- OTDR
- マルチメーター
- トナープローブ
- 試験用電話機(Butt set)
- パンチダウンツール
- ケーブルストリッパー
- スニップス
- 電源アナライザー
- 温度モニター

第6章 ネットワークセキュリティ (11%)

6.1 ハードウェアおよびソフトウェアセキュリティデバイスの機能について説明することができる。

- ネットワークベースのファイアウォール
- ホストベースのファイアウォール
- IDS
- IPS
- VPN 装置

6.2 一般的なファイアウォールの機能について説明することができる。

- アプリケーションレイヤー / ネットワークレイヤー
- ステートフル / ステートレス
- スキャンサービス
- コンテンツフィルタリング
- シグニチャー照合
- ゾーン

6.3 ネットワークアクセスセキュリティの方法について説明することができる。

フィルタリング:

- ACL
 - ・ MAC フィルタリング
 - ・ IP フィルタリング
- トンネリングと暗号化
 - ・ SSL VPN
 - ・ VPN
 - ・ L2TP
 - ・ PPTP
 - ・ IPSec
- リモートアクセス
 - ・ RAS
 - ・ RDP
 - ・ PPPoE
 - ・ PPP
 - ・ VNC
 - ・ ICA

6.4 ユーザー認証の方法について説明することができる。

- PKI
- Kerberos
- AAA
 - ・ RADIUS
 - ・ TACACS+
- ネットワークアクセスコントロール
 - ・ 802.1x
- CHAP
- MS-CHAP
- EAP

6.5 デバイスセキュリティに影響を及ぼす問題について説明をすることができる。

- 物理セキュリティ
- ローカルおよびリモートアクセスの制限
- セキュアな方法 / 非セキュアな方法
 - ・ SSH、HTTPS、SNMPv3、SFTP、SCP
 - ・ TELNET、HTTP、FTP、RSH、RCP、SNMPv1/2

6.6 一般的セキュリティ脅威と緩和技術を特定することができる。

セキュリティ脅威

- DoS
- ウイルス
- ワーム
- アタッカー
- Man in the middle(中間者攻撃)
- スマーフ
- 不正アクセスポイント
- ソーシャルエンジニアリング (例:フィッシング)

緩和技術

- ポリシーと手順の決定
- ユーザートレーニング
- パッチとアップデート

CompTIA Network+ 略語一覧

AAA	—	Authentication Authorization and Accounting
ACL	—	Access Control List
ADF	—	Automatic Document Feeder
ADSL	—	Asymmetric Digital Subscriber Line
AH	—	Authentication Header
AM	—	Amplitude Modulation
AMI	—	Alternate Mark Inversion
APIPA	—	Automatic Private Internet Protocol Addressing
ARP	—	Address Resolution Protocol
ATM	—	Asynchronous Transfer Mode
BDF	—	Building Distribution Frame
BERT	—	Bit-Error Rate Test
BGP	—	Border Gateway Protocol
BNC	—	British Naval Connector / Bayonet Niell-Concelman
BootP	—	Boot Protocol /Bootstrap Protocol
BRI	—	Basic Rate Interface
CHAP	—	Challenge Handshake Authentication Protocol
CIDR	—	Classless inter domain routing
CNAME	—	Canonical Name
CRAM-MD5	—	Challenge-Response Authentication Mechanism – Message Digest 5
CSMA / CA	—	Carrier Sense Multiple Access / Collision Avoidance
CSMA / CD	—	Carrier Sense Multiple Access / Collision Detection
CSU	—	Channel Service Unit
dB	—	decibels
DHCP	—	Dynamic Host Configuration Protocol
DLC	—	Data Link Control
DNS	—	Domain Name Service / Domain Name Server / Domain Name System
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
DSL	—	Digital Subscriber Line
DSU	—	Data Service Unit
E1	—	E-Carrier Level 1
EAP	—	Extensible Authentication Protocol
EGP	—	Exterior Gateway Protocol
EIGRP	—	Enhanced Interior Gateway Routing Protocol
EMI	—	Electromagnetic Interference
ESSID	—	Enhanced Service Set Identifier
ESP	—	Encapsulated security packets
FDM	—	Frequency Division Multiplexing
FHSS	—	Frequency Hopping Spread Spectrum
FM	—	Frequency Modulation
FQDN	—	Fully Qualified Domain Name / Fully Qualified Distinguished Name
FTP	—	File Transfer Protocol
GBIC	—	Gigabit Interface Converter
Gbps	—	Giga bits per second
HDLC	—	High-Level Data Link Control

HTTP	—	Hypertext Transfer Protocol
HTTPS	—	Hypertext Transfer Protocol Secure
Hz	—	Hertz
IANA	—	Internet Assigned Numbers Authority
ICA	—	Independent Computer Architecture
ICMP	—	Internet Control Message Protocol
IDF	—	Intermediate Distribution Frame
IDS	—	Intrusion Detection System
IEEE	—	Institute of Electrical and Electronics Engineers
IGMP	—	Internet Group Multicast Protocol
IGP	—	Interior Gateway Protocol
IKE	—	Internet Key Exchange
IMAP4	—	Internet Message Access Protocol version 4
IP	—	Internet Protocol
IPS	—	Intrusion Prevention System
IPSec	—	Internet Protocol Security
IPv4	—	Internet Protocol version 4
IPv6	—	Internet Protocol version 6
ISDN	—	Integrated Services Digital Network
IS-IS	—	Intermediate System - Intermediate system
ISP	—	Internet Service Provider
IT	—	Information Technology
Kbps	—	Kilobits per second
L2F	—	Layer 2 Forwarding
L2TP	—	Layer 2 Tunneling Protocol
LACP	—	Link aggregation control protocol
LAN	—	Local Area Network
LC	—	Local Connector
LDAP	—	Lightweight Directory Access Protocol
LEC	—	Local Exchange Carrier
LED	—	Light Emitting Diode
LLC	—	Logical Link Control
MAC	—	Media Access Control / Medium Access Control
Mbps	—	Megabits per second
MBps	—	Megabytes per second
MDF	—	Main Distribution Frame
MDI	—	Media Dependent Interface
MDIX	—	Media Dependent Interface Crossover
MIB	—	Management Information Base
MMF	—	Multimode Fiber
MPLS	—	Multi-Protocol Label Switching
MS-CHAP	—	Microsoft Challenge Handshake Authentication Protocol
MT-RJ	—	Mechanical Transfer-Registered Jack
MX	—	Mail Exchanger
NAT	—	Network Address Translation
NetBEUI	—	Network Basic Input / Output Extended User Interface
NetBIOS	—	Network Basic Input / Output System

NIC	—	Network Interface Card
nm	—	nanometer
NNTP	—	Network News Transport Protocol
NTP	—	Network Time Protocol
OCx	—	Optical Carrier
OS	—	Operating Systems
OSI	—	Open Systems Interconnect
OSPF	—	Open Shortest Path First
OTDR	—	Optical Time Domain Reflectometer
PAP	—	Password Authentication Protocol
PAT	—	Port Address Translation
PC	—	Personal Computer
PKI	—	Public Key Infrastructure
PoE	—	Power over Ethernet
POP3	—	Post Office Protocol version 3
POTS	—	Plain Old Telephone System
PPP	—	Point-to-Point Protocol
PPPoE	—	Point-to-Point Protocol over Ethernet
PPTP	—	Point-to-Point Tunneling Protocol
PRI	—	Primary Rate Interface
PSTN	—	Public Switched Telephone Network
PVC	—	Permanent Virtual Circuit
QoS	—	Quality of Service
RADIUS	—	Remote Authentication Dial-In User Service
RARP	—	Reverse Address Resolution Protocol
RAS	—	Remote Access Service
RDP	—	Remote Desktop Protocol
RFI	—	Radio Frequency Interface
RG	—	Radio Guide
RIP	—	Routing Internet Protocol
RJ	—	Registered Jack
RSA	—	Rivest, Shamir, Adelman
RSH	—	Remote Shell
RTP	—	Real Time Protocol
SC	—	Standard Connector / Subscriber Connector
SCP	—	Secure Copy Protocol
SDSL	—	Symmetrical Digital Subscriber Line
SFTP	—	Secure File Transfer Protocol
SIP	—	Session Initiation Protocol
SLIP	—	Serial Line Internet Protocol
SMF	—	Single Mode Fiber
SMTP	—	Simple Mail Transfer Protocol
SNAT	—	Static Network Address Translation
SNMP	—	Simple Network Management Protocol
SOA	—	Start of Authority
SOHO	—	Small Office / Home Office
SONET	—	Synchronous Optical Network

SPS	—	Standby Power Supply
SSH	—	Secure Shell
SSID	—	Service Set Identifier
SSL	—	Secure Sockets Layer
ST	—	Straight Tip
STP	—	Shielded Twisted Pair
T1	—	T-Carrier Level 1
TA	—	Terminal Adaptor
TACACS+	—	Terminal Access Control Access Control System+
TCP	—	Transmission Control Protocol
TCP / IP	—	Transmission Control Protocol / Internet Protocol
tcsh	—	turbo C shell
TDM	—	Time Division Multiplexing
TDR	—	Time Domain Reflectometer
Telco	—	Telephone Company
TFTP	—	Trivial File Transfer Protocol
TKIP	—	Temporal Key Integrity Protocol
TLS	—	Transport Layer Security
TTL	—	Time to Live
UDP	—	User Datagram Protocol
UNC	—	Universal Naming Convention
UPS	—	Uninterruptible Power Supply
URL	—	Uniform Resource Locator
USB	—	Universal Serial Bus
UTP	—	Unshielded Twisted Pair
VDSL	—	Variable Digital Subscriber Line
VLAN	—	Virtual Local Area Network
VNC	—	Virtual Network Connection
VoIP	—	Voice over IP
VPN	—	Virtual Private Network
VTP	—	Virtual Trunk Protocol
WAN	—	Wide Area Network
WAP	—	Wireless Application Protocol / Wireless Access Point
WEP	—	Wired Equivalent Privacy
WINS	—	Window Internet Name Service
WPA	—	Wi-Fi Protected Access
www	—	World Wide Web
Zeroconf	—	Zero Configuration