

CompTIA Server+認定資格試験の比較

SK0-004 vs. SK0-003

改訂の全体概要

- SK0-004 の出題内容の約 75%は、SK0-003 の出題内容のトピックと一致しています。
- SK0-004 の出題内容は、SK0-003 に比べて、ハードウェアの出題比率が減り、セキュリティ、仮想化、運用管理、ネットワークの出題比率が増えています。
- SK0-004 では、セキュリティの出題項目が独立した項目として出題されています。
- 下記の出題項目は、SK0-004 から新しく出題される項目です。そのほとんどが、セキュリティに関連する出題項目です。

3.4 与えられたシナリオに基づいて、将来的な成長を見越した適切なストレージ容量と計画を算出することができる。

4.2 与えられたシナリオに基づいて、サーバー要塞化の手法を適用することができる。

4.5 データセキュリティの方法とセキュアストレージの処分テクニックを実行することができる。

7.6 与えられたシナリオに基づき、適切なツールと方法を選択し、セキュリティ関連する障害を効果的に診断することができる。

- 試験実施の詳細は、試験番号、配信言語を除いて変更はありません。

以下は、上記全体概要の詳細です。

認定資格試験について

SK0-004 試験では、セキュリティと仮想化の出題が強化されています。詳細は、下記の黄色のハイライトを参照してください。

SK0-004	SK0-003
<p>CompTIA Server+は、ワールドワイドでベンダーニュートラルな認定資格です。CompTIA Server+認定資格試験は、サーバーの設計・構築、運用・管理に必要なファンデーションレベルのスキルと知識を評価し、世界中の IT プロフェッショナルや企業に活用されています。</p>	
<p>認定資格試験に合格することで、下記のスキルと知識を有していることを証明することができます。</p>	
<ul style="list-style-type: none"> • 構築、運用、トラブルシューティング、セキュリティ、仮想化を含むハードウェアとソフトウェアの管理に関するスキルと知識 • 環境問題の特定と配慮 • 災害復旧や一般的なセキュリティ手順への理解と遵守 • サーバーに関連する専門用語や概念 • サーバーの役割と様々に変化する IT 環境でのサーバーの相互作用への理解 	<ul style="list-style-type: none"> • 構築、運用、トラブルシューティング、ハードウェアとソフトウェアの管理に関するスキルと知識 • 環境問題の特定と配慮 • 災害と物理的な環境の復旧と、ソフトウェアセキュリティの手順への理解と遵守 • サーバーに関連する専門用語や概念 • サーバーの役割と、IT 環境の中でのサーバーの相互作用への理解

出題項目について

ハードウェアの出題比率が減り、セキュリティ、仮想化、運用管理、ネットワークの出題比率が増えています。

SK0-004	SK0-003
第1章 サーバー設計 12%	第1章 システムハードウェア 21%
第2章 サーバー管理 24%	第2章 ソフトウェア 19%
第3章 ストレージ 12%	第3章 ストレージ 14%
第4章 セキュリティ 13%	第4章 IT 環境 11%
第5章 ネットワーク 10%	第5章 災害復旧 11%
第6章 災害復旧 9%	第6章 トラブルシューティング 24%
第7章 トラブルシューティング 20%	

試験実施について

試験実施の詳細は、試験番号、配信言語を除いて変更はありません。

試験番号	SK0-004	SK0-003
配信開始日	2009年(英語) 2010年8月31日(日本語)	2015年7月31日(英語) 2016年1月18日(日本語)
問題数	100問	100問
出題形式	単一/複数選択	単一/複数選択
試験時間	90分	90分
合格点	750点(100-900のスコア形式)	750点(100-900のスコア形式)
前提スキル	CompTIA A+相当のクライアントに関連するスキル 18~24ヶ月のサーバーに関連するIT実務経験	CompTIA A+相当のクライアントに関連するスキル 18~24ヶ月のサーバーに関連するIT実務経験

出題範囲の詳細比較

下記の出題項目は、SK0-004 から新しく出題される項目です。そのほとんどが、セキュリティに関連する出題項目です。

- 3.4 与えられたシナリオに基づいて、将来的な成長を見越した適切なストレージ容量と計画を算出することができる。
- 4.2 与えられたシナリオに基づいて、サーバー要塞化の手法を適用することができる。
- 4.5 データセキュリティの方法とセキュアストレージの処分テクニックを実行することができる。
- 7.6 与えられたシナリオに基づき、適切なツールと方法を選択し、セキュリティ関連する障害を効果的に診断することができる。

さらに、両出題範囲を比べると、ハードウェアの出題比率が減り、セキュリティ、仮想化、運用管理、ネットワークの出題比率が増えていることがわかります。

SK0-004	SK0-003
<p>1.1 サーバフォームファクターの機能と役割について説明することができる。</p> <ul style="list-style-type: none"> ● ラックマウント <ul style="list-style-type: none"> ● 寸法 <ul style="list-style-type: none"> - 1U、2U、4U ● ケーブルマネジメントアーム ● レールキット ● タワー ● ブレードテクノロジー <ul style="list-style-type: none"> ● ブレードエンクロージャー(ブロードシャーシ) <ul style="list-style-type: none"> - バックプレーン/ミッドプレーン - 電源ソケット - ネットワークモジュール/スイッチ - 管理モジュール ● ブレードサーバー 	<p>1.2 シャーシの種類と適切なコンポーネントの配置を実施することができる。</p> <ul style="list-style-type: none"> ● 本体形状(タワー、ラック、ブレード) <ul style="list-style-type: none"> ● スペース活用(U サイズ、高さ、幅、深さ) ● リダンダント電源 ● シャーシイントリュージョン(シャーシの開閉) ● 電源ボタン ● リセットボタン ● 診断 LED ● Expansion bay
<p>1.3 与えられたシナリオに基づいて、サーバーコンポーネントの設置、設定、管理を実施することができる。</p> <ul style="list-style-type: none"> ● CPU <ul style="list-style-type: none"> ● マルチプロセッサとマルチコアの違い ● ソケットの種類 ● キャッシュレベル:L1、L2、L3 ● スピード <ul style="list-style-type: none"> - コア - バス 	<p>1.1 システムボードの種類、機能、コンポーネントの違いとそれらの用途について説明することができる。</p> <ul style="list-style-type: none"> ● ディップスイッチ / ジャンパー ● プロセッサ (シングルとマルチ) ● バスの種類とバススピード ● オンボードコンポーネント <ul style="list-style-type: none"> ● NIC ● ビデオ ● オーディオ

- クロック速度
- CPU ステッピング
- 設計
 - x86
 - x64
 - ARM
- RAM
 - ECC メモリとの non-ECC メモリの違い
 - DDR2、DDR3
 - ピンの数
 - SRAM と DRAM の違い
 - モジュールの設定
 - CAS レイテンシー
 - メモリタイミング
 - メモリペアリング
- バスの種類、バスチャネル、拡張スロット
 - 大きさの違いとビットレートの違い
 - PCI
 - PCIe
 - PCI-X
- NIC
- ハードディスク
- ライザーカード
- RAID コントローラー
- BIOS/UEFI
 - CMOS バッテリー
- ファームウェア
- USB インターフェース/ポート
- ホットスワップ対応コンポーネントとホットスワップ非対応コンポーネントの違い

- USB
- HID (Human Interface Device)
- シリアル
- パラレル
- 拡張スロット
 - PCI
 - PCIe
 - PCIe
 - AGP
 - ISA
- BIOS
- ライザーカード / バックプレーン
- ストレージコネクタ
 - SCSI
 - SATA
 - IDE
 - フロッピー

1.3 メモリ機能/種類の違いを理解し、あるシナリオを想定した場合の適切なメモリを選択することができる。

- メモリのペアリング
- ECC と non ECC
- Registered と non registered
- RAID とホットスペア (ホットスタンバイ)
- メモリタイプ
 - DDR
 - FB-DIMM (Fully Buffered DIMM)
 - DDR2
 - SDRAM
 - DDR3
- メモリ互換性
 - スピード
 - サイズ
 - ピン (形状)
 - CAS レイテンシ
 - タイミング
 - ベンダー固有のメモリ
- On board とライザーカード (riser card)

1.4 ハードウェア互換性リスト (HCL) の重要性について説明することができる。

- ハードウェアのベンダー基準
- メモリとプロセッサの互換性
- 拡張カードの互換性
- 仮想化の要件

1.5 プロセッサの機能/種類について理解し、あるシナリオを想定した場合の適切なプロセッサを選択することができる。

- マルチコア
- マルチプロセッサ
- キャッシュレベル
- ステッピング
- スピード
- VRM
- Execute disable(XD)または not execute(NX)
- ハイパースレッディング
- VT または AMD-V
- AMD と Intel(互換性のない CPU)
- プロセッサアーキテクチャ(RISC, CISC)
- ベンダーのスロット種類
- 64bit と 32bit
- 放熱(ヒートシンク、ファン、液体冷却)

1.6 想定されたシナリオ下で、フォールトトレランスを考慮しながら適切な拡張カードをサーバーにインストールすることができる。

- メーカーの仕様
 - ・ Fax カード
 - ・ PBX カード
 - ・ カメラカード
 - ・ VoIP
- HBA
- NIC
- ビデオ
- オーディオ
- ストレージコントローラー(SCSI, SATA, RAID)
 - ・ SCSI(LVD/HVD)
 - ・ SCSI ID
 - ・ ケーブルとコネクタ
 - ・ アクティブとパッシブターミネーション
- ポート拡張カード

	<ul style="list-style-type: none"> ・ USB ・ IEEE1394 ・ シリアル ・ パラレル <p>1.7 適切なファームウェアのインストール、アップデート、設定をすることができる。</p> <ul style="list-style-type: none"> ● ドライバ/ハードウェアの互換性 ● ファームウェアアップグレードの失敗が及ぼす影響 (リダンダント BIOS) ● メーカーの取扱説明書とドキュメンテーションの確認
<p>1.4 電力と冷却のコンポーネントを比較対照することができる。</p> <ul style="list-style-type: none"> ● 電源 <ul style="list-style-type: none"> ・ 電圧 <ul style="list-style-type: none"> - 110v、220v、-48v の違い - 208v と 440v/460v/480v の違い ・ ワット数 ・ 消費電力 ・ 冗長性 ・ 単相電力 (1-phase power) と三相電力 (3-phase power) の違い ・ プラグの種類 <ul style="list-style-type: none"> - NEMA - Edison - ツインロック ● 冷却 <ul style="list-style-type: none"> ・ エアフロー ・ サーマルディスペンサー ・ バッフル/シュラウド ・ ファン ・ 液体冷却 	<p>1.2 シャーシの種類と適切なコンポーネントの配置を実施することができる。</p> <ul style="list-style-type: none"> ● 冷却 <ul style="list-style-type: none"> ・ ファン ・ 水冷 ・ パッシブ ・ アクティブ ・ シュラウド ・ ダクト ・ 冗長冷却 ・ ホットスワッピング ・ ベンティレーション ● 電源 <ul style="list-style-type: none"> ・ コネクター ・ 電圧 ・ Phase(位相) ●
<p>2.1 サーバー用 OS のインストールと設定をすることができる。</p> <ul style="list-style-type: none"> ● サーバーの役割と目的の決定 ● ファームウェアのアップデート ● BIOS/UEFI の設定 <ul style="list-style-type: none"> ・ 起動順序 	<p>2.1 NOS(Windows/*nix)のインストール、配置、設定、アップデートをすることができる。</p> <ul style="list-style-type: none"> ● インストール方法(オプティカルメディア, USB, ネットワーク共有、PXE) <ul style="list-style-type: none"> ・ イメージングシステムのクローニングと配置 (Ghost, RIS/WDS, Altiris, 仮想化テンプレート)

- ディスクの準備
 - RAID のセットアップ
 - パーティションの設定
 - フォーマット
 - ファイルシステムの種類
 - Ext 2、Ext3、Ext 4
 - NTFS
 - FAT32
 - ReiserFS
 - UFS
 - VMFS
 - ZFS
 - スワップ
- ホスト名の設定
- ローカルアカウントのセットアップ
- ネットワークへの接続
- ドメイン/ディレクトリの構成
- セキュリティ対策
 - パッチ
 - OS の要塞化
 - 企業における手順と標準のコンプライアンス
- サービスの有効化
- 機能/ロール/アプリケーション/ドライバーのインストール
- パフォーマンスベースライン
 - サーバーの最適化
 - スワップ/ページファイルの最適化
- 無人/リモートからのインストール
 - イメージとクローニングの展開
 - インストール用スクリプト
 - PXE ブート
 - TFTP

- ブートローダ
- ファイルシステム
- FAT
 - FAT
 - FAT32
 - NTFS
 - VMFS
 - ZFS
 - EXT3
- ドライバインストレーション
 - ドライバの取得
 - インストール方法
 - 必要となるメディア
- NOS の環境設定
 - イニシャルネットワーク
 - ユーザー
 - デバイス
 - 役割
 - OS 環境の設定
 - アプリケーションとツール
- パッチの管理

2.2 NOS セキュリティソフトウェアとその機能について説明することができる。

- ソフトウェアファイアウォール
 - ポートブロッキング
 - アプリケーションエラー (Application exception)
 - ACL
- マルウェアプロテクションソフトウェア
 - アンチウイルス
 - アンチスパイウェア
- ファイルの権限レベルと共有権の基本

2.3 想定されたシナリオ下で、手順とガイドラインに基づき NOS 管理機能を実行し運営することができる。

- ユーザー管理
 - ユーザーの追加と削除
 - 権限の設定
 - グループメンバーシップ
 - ポリシー
 - ログインスクリプト

	<ul style="list-style-type: none"> ● リソースの管理 <ul style="list-style-type: none"> ・ ACL ・ クォータ(Quotas) ・ シャドウボリューム ・ ディスクマネージメント ・ パフォーマンスモニタリング ・ ベースラインの実行 ● モニタリング(ツールとエージェント) <ul style="list-style-type: none"> ・ SNMP(MIB) ・ WBEM(WMI)
<p>2.2 サーバーの役割と必要条件を比較対照することができる。</p> <ul style="list-style-type: none"> ● ウェブサーバー ● アプリケーションサーバー ● ディレクトリサーバー ● データベースサーバー ● ファイルサーバー ● プリンタサーバー ● メッセージングサーバー ● メールサーバー ● ルーティング/リモートアクセスサーバー ● ネットワークサービスサーバー <ul style="list-style-type: none"> ● DHCP ● DNS/WINS ● NTP 	<p>2.4 異なるサーバーの役割とそれらの用途、相互作用について説明することができる。</p> <ul style="list-style-type: none"> ● ファイルとプリンタサーバー ● データベースサーバー ● ウェブサーバー ● メッセージングサーバー ● DHCP サーバー ● ディレクトリサービスサーバー ● DNS サーバー ● アプリケーションサーバー <ul style="list-style-type: none"> ・ サーバーとプロキシサーバーのアップデート ・ フィルタリングサーバー ・ モニタリングサーバー ・ 専用アプリケーションサーバー ・ 分散アプリケーションサーバー ・ ピアツーピアアプリケーションサーバー ● リモートアクセスサーバー ● 仮想化サービス ● NTP サーバー ● ワークステーション、デスクトップ、サーバーの違いについて ● サーバーのシャットダウンと起動シーケンス(1 台のサーバー / 複数台のサーバー / 付属コンポーネンツ)
<p>2.3 与えられたシナリオに基づいて、サーバーを管理するためのアクセスとコントロールを使用することができる。</p> <ul style="list-style-type: none"> ● ローカルハードウェア管理 <ul style="list-style-type: none"> ● KVM ● シリアル 	<p>4.4 異なるサーバーアクセス方法の実行と設定を実施することができる。</p> <ul style="list-style-type: none"> ● KVM(ローカルと IP ベース) ● ダイレクト接続 ● リモート管理

<ul style="list-style-type: none"> ● 仮想管理コンソール ● ネットワークベースのハードウェア管理 <ul style="list-style-type: none"> ● KVM over IP ● ILO ● iDRAC ● ILOM ● ネットワークベースのオペレーティングシステム管理 <ul style="list-style-type: none"> ● RDP ● SSH ● VNC ● コマンドライン/シェル 	<ul style="list-style-type: none"> ● リモート制御 ● アドミニストレーション ● ソフトウェア展開 ● 専用の管理ポート
<p>2.4 与えられたシナリオに基づいて、適切なサーバー管理手法を実施することができる。</p> <ul style="list-style-type: none"> ● 変更管理 ● パッチ管理 <ul style="list-style-type: none"> ● OS のアップデート ● アプリケーションのアップデート ● セキュリティソフトウェアのアップデート ● ファームウェアのアップデート ● デバイスドライバのアップデート ● 互換性リスト <ul style="list-style-type: none"> - OS - ハードウェア - アプリケーション ● テストとバリデーション ● 停電と SLA(サービスレベルアグリーメント) <ul style="list-style-type: none"> ● 計画ダウンタイム ● 計画外ダウンタイム ● インパクト分析 ● クライアントへの通知 ● MTTR ● パフォーマンスの監視 <ul style="list-style-type: none"> ● CPU 利用率 ● メモリ利用率 ● ネットワーク利用率 ● ディスク利用率 <ul style="list-style-type: none"> - ディスク IOPS - ストレージ容量 	<p>4.2 あるシナリオを想定した場合の、業界のベストプラクティスを行うことの目的について説明することができる。</p> <ul style="list-style-type: none"> ● ベンダーサーバーのベストプラクティスの実行 <ul style="list-style-type: none"> ● ドキュメンテーション ● ツール ● ウェブサイト ● 変更事項を行う前に、及ぼす影響について調べる <ul style="list-style-type: none"> - 組織上の影響を考慮する ● 措置を行う前および、完了した時点でステークホルダーと連絡をとる ● 全ての地域法律/規制、業界および企業の規制に従う ● サービスレベルアグリーメント(SLA)の目的 ● 変更管理手順を追う ● 機材の廃棄処理方法

<ul style="list-style-type: none"> • パフォーマンスベースラインとの比較 • プロセス監視とサービス監視 • ログ監視 ● ハードウェアメンテナンス <ul style="list-style-type: none"> • システムヘルスインジゲータの確認 <ul style="list-style-type: none"> - LED - エラーコード - ビープコード - LCD メッセージ • 故障したコンポーネントの交換 <ul style="list-style-type: none"> - ファン - ハードディスク - RAM - バックプレーン - 電源装置 • 予防保守 <ul style="list-style-type: none"> - 埃の掃除 - 適切なエアフローの確認 • 適切なシャットダウン手順 ● フォールトトレランスと高可用性の手法 <ul style="list-style-type: none"> • クラスタリング <ul style="list-style-type: none"> - アクティブ/アクティブ - アクティブ/パッシブ • ロードバランス <ul style="list-style-type: none"> - ラウンドロビン - ハートビート 	
<p>2.5 資産管理と文書化の重要性を説明することができる。</p> <ul style="list-style-type: none"> ● 資産管理 <ul style="list-style-type: none"> • ライセンス • ラベリング • 保証書 • ライフサイクルマネジメント <ul style="list-style-type: none"> - 調達 - 利用 - エンドオブライフ - 廃棄/リサイクル • インベントリ(棚卸) <ul style="list-style-type: none"> - 作成 - 製品モデル 	<p>4.1 ドキュメンテーション、ダイアグラム、プロシージャの作成、活用、メンテナンスを実施することができる。</p> <ul style="list-style-type: none"> ● サーバーの構築やアップグレードを実行する際、プリンストールのプランに従う ● レーベリング ● サーバーラックと環境のトポロジーのダイアグラム作成 ● ハードウェアとソフトウェアのアップグレード、インストール、コンフィギュレーション、サーバーの役割と修理履歴(リペアログ) ● サーバーベースラインの記録(サービス前後に関して) ● ハードウェアの初期設定、サービススタグ、資産管理

<ul style="list-style-type: none"> - シリアルナンバー - 資産タグ ● 文書化 <ul style="list-style-type: none"> - サービスマニュアル - ネットワーク図 - アーキテクチャ設計書 - データフロー設計書 - リカバリー文書 - ベースライン文書 - 変更管理ポリシー - SLA(サービスレベルアグリーメント) - サーバー設定 ● セキュアに保管されるべき機密文書 	<p>と保証</p> <ul style="list-style-type: none"> ● ベンダー特定のドキュメンテーション <ul style="list-style-type: none"> ・ 正しいマニュアルの参照 ・ ウェブサイト ・ サポートチャネル(ベンダーのリスト)
<p>2.6 仮想化コンポーネントの目的と運用方法を説明することができる</p> <ul style="list-style-type: none"> ● ホストとゲスト ● 仮想マシン用の管理インターフェース ● ハイパーバイザー <ul style="list-style-type: none"> ● Type1 ● Type2 ● ハイブリッド ● ハードウェアの互換性リスト <ul style="list-style-type: none"> ● BIOS/UEFI の互換性サポート ● CPU 互換性サポート ● AMD-V / Intel VT ● ホストとゲスト間のリソース配分 <ul style="list-style-type: none"> ● CPU ● ストレージ ● メモリー ● ネットワーク接続 <ul style="list-style-type: none"> - ダイレクトアクセス(ブリッジング)と NAT の違い - 仮想 NIC - 仮想スイッチ ● ビデオカード 	<p>2.5 サーバー仮想化のコンセプト、機能、考慮すべき点について説明することができる。</p> <ul style="list-style-type: none"> ● リソースの活用 ● コンフィギュレーション ● インターコネクティビティ ● 管理サーバー ● 仮想化のリソース <ul style="list-style-type: none"> ・ コストと効果について ・ リダンダンシー ・ グリーンイニシアチブ ・ 障害復旧 ・ 環境テスト ・ 配置の容易性
<p>3.1 与えられたシナリオに基づいて、特定の仕様とインターフェースを使用しプライマリストレージデバイスをインストール、展開することができる。</p>	<p>3.3 異なる内蔵ストレージ技術のインストールと設定について説明することができる。</p> <ul style="list-style-type: none"> ● ホットスワップ対応機器と非対応機器 ● SCSI, Ultra SCSI, Ultra320(ターミネーション)、

<ul style="list-style-type: none"> ● ディスクの仕様 <ul style="list-style-type: none"> ● RPM ● 寸法/規格 ● 容量 ● バス幅 ● IOPS ● シークタイムとレイテンシー(遅延) ● ホットスワップ対応コンポーネントとホットスワップ非対応コンポーネントの違い ● インターフェース <ul style="list-style-type: none"> ● SAS ● SATA ● SCSI ● USB ● ファイバーチャネル ● ハードディスクと SSD の違い 	<p>LUN</p> <ul style="list-style-type: none"> ● SAS, SATA ● テープ ● オプティカル <ul style="list-style-type: none"> ・ DVD ・ DVD-R ・ CD-ROM ・ CD-R ・ CD-RW ・ Blu-Ray ● フラッシュメモリ ● フロッピー(USB) ● コントローラー(ファームウェアレベル) ● ハードドライブ(ファームウェア、JBOD)
<p>3.2 与えられたシナリオに基づいて、最適な方法(ベストプラクティス)を使用して RAID を設定することができる。</p> <ul style="list-style-type: none"> ● RAID のレベルとパフォーマンスの考慮 <ul style="list-style-type: none"> ● 0 ● 1 ● 5 ● 6 ● 10 ● ソフトウェア RAID とハードウェア RAID の違い <ul style="list-style-type: none"> ● パフォーマンスの考慮 ● 設定上の要件 <ul style="list-style-type: none"> ● 容量 ● バスの種類 ● ドライブ RPM ● ホットスワップのサポートと分岐 ● ホットスペアとコールドスペアの違い ● アレイコントローラー <ul style="list-style-type: none"> ● メモリー ● バッテリーバックアップ式キャッシュ ● 冗長コントローラー 	<p>3.1 異なる RAID 技術と、それぞれの機能と利点について説明することができる。</p> <ul style="list-style-type: none"> ● ホットスペア ● ソフトウェアとハードウェア ● キャッシュリード/ライトのレベル(データ損失の可能性) ● パフォーマンスベネフィットとトレードオフ <p>3.2 あるシナリオを想定した場合の適切な RAID レベルを選択することができる。</p> <ul style="list-style-type: none"> ● 0, 1, 3, 5, 6, 10, 50 ● パフォーマンスベネフィットとトレードオフ
<p>3.3 ハードウェアと様々なストレージテクノロジーの特性を要約することができる。</p>	<p>3.3 異なる内蔵ストレージ技術のインストールと設定について説明することができる。</p> <ul style="list-style-type: none"> ● ホットスワップ対応機器と非対応機器

<ul style="list-style-type: none"> ● DAS ● NAS <ul style="list-style-type: none"> ● CIFS/SMB ● NFS ● SAN <ul style="list-style-type: none"> ● iSCSI ● FCoE ● ファイバーチャネル ● LUN と LUN マスキング ● HBA とファブリックスイッチ ● JBOD ● テープ <ul style="list-style-type: none"> ● ドライブ ● ライブラリー ● 光学ドライブ ● フラッシュ/コンパクトフラッシュ/USBドライブ 	<ul style="list-style-type: none"> ● SCSI, Ultra SCSI, Ultra320 (ターミネーション)、LUN ● SAS, SATA ● テープ ● オプティカル <ul style="list-style-type: none"> ・ DVD ・ DVD-R ・ CD-ROM ・ CD-R ・ CD-RW ・ Blu-Ray ● フラッシュメモリ ● フロッピー (USB) ● コントローラー (ファームウェアレベル) ● ハードドライブ (ファームウェア、JBOD) <p>3.4 外付けストレージ技術の用途について説明することができる。</p> <ul style="list-style-type: none"> ● ネットワーク接続ストレージ ● ストレージエリアネットワーク ● テープライブラリ ● WORM (Write Once Read Many) ● オプティカルジュークボックス ● 転送メディア <ul style="list-style-type: none"> ・ iSCSI ・ SATA ・ SAS ・ SCSI ・ ファイバーチャネル
<p>3.4 与えられたシナリオに基づいて、将来的な成長を見越した適切なストレージ容量と計画を算出することができる。</p> <ul style="list-style-type: none"> ● 10 進数と 2 進数のディスクサイズの計算 (1000 と 1024 の違い) ● ディスククォータ ● 圧縮 ● 容量計画の考慮 <ul style="list-style-type: none"> ● オペレーティングシステムの拡張 <ul style="list-style-type: none"> - パッチ - サービスパック 	

<ul style="list-style-type: none"> - ログファイル • テンポラリーディレクトリー • データーベース • アプリケーションサーバー • ファイルサーバー • アーカイブ 	
<p>4.1 物理セキュリティの方法と概念を比較対照することができる。</p> <ul style="list-style-type: none"> ● 多要素認証 <ul style="list-style-type: none"> • 何を持っているか • 何を知っているか • 誰か ● セキュリティの概念 <ul style="list-style-type: none"> • マントラップ • RFID チップ • ID カード • バイオメトリック • キーパッド • アクセスリスト • セキュリティガード • セキュリティカメラ • キーロック(Keys&Locks) <ul style="list-style-type: none"> - キャビネット - ラックマウント - サーバー • 安全(Safe) 	<p>4.5 あるシナリオを想定した場合の、サーバーロケーションのための物理的セキュリティ対策について説明することができる。</p> <ul style="list-style-type: none"> ● 物理的なサーバーセキュリティ <ul style="list-style-type: none"> • ドアに鍵が掛けられていること • ラックドア • CCTV(Closed Circuit Television: 監視カメラ) • マントラップ • 警備員 ● アクセス制御デバイス(RFID, キーパッド、ピンパッド) <ul style="list-style-type: none"> • バイオメトリックデバイス(指紋スキャナ、網膜) ● セキュリティ対策 <ul style="list-style-type: none"> • アクセス制限 • アクセスログ • 時間制限 ● 多重防護—マルチレイヤーの防御 ● 物理的セキュリティを行う理由 <ul style="list-style-type: none"> • 盗難 • データロス • ハッキング ● サーバーに関連したセキュアなドキュメンテーション <ul style="list-style-type: none"> • パスワード • システムコンフィギュレーション • ログ
<p>4.2 与えられたシナリオに基づいて、サーバー要塞化の手法を適用することができる。</p> <ul style="list-style-type: none"> ● OS の要塞化 <ul style="list-style-type: none"> • 不必要なサービスの停止/不必要なポートを閉じる • 必要とされるソフトウェアのみをインストールする • 最新のシステムパッチをインストールする 	

<ul style="list-style-type: none"> ● アプリケーションの要塞化 <ul style="list-style-type: none"> ● 最新のパッチをインストールする ● 不必要なサービス/役割/機能を無効にする ● エンドポイントセキュリティ <ul style="list-style-type: none"> ● HIDS ● アンチマルウェア ● 脆弱性スキャンを基にセキュリティの問題を修正する ● ハードウェアの要塞化 <ul style="list-style-type: none"> ● 不必要なハードウェア、物理ポート、デバイスを無効にする ● BIOS のパスワード ● WOL (Wake on LAN) を無効にする ● ブートの順序を設定する ● シャーシロック/侵入検知 	
<p>4.3 基本的なネットワークセキュリティシステムとプロトコルを説明することができる。</p> <ul style="list-style-type: none"> ● ファイアーウォール <ul style="list-style-type: none"> ● ネットワークベース ● ホストベース ● ポートセキュリティ/802.1x / NAC ● ルーターアクセスリスト ● NIDS ● 認証プロトコル <ul style="list-style-type: none"> ● LDAP ● RADIUS ● TACACS ● TACACS+ ● PKI <ul style="list-style-type: none"> ● 秘密鍵 ● 公開鍵 ● 認証局 (Certificate authority) ● SSL/TLS ● VPN ● IPsec ● VLAN ● セキュリティゾーン <ul style="list-style-type: none"> ● DMZ ● パブリックとプライベート 	<p>2.2 NOSセキュリティソフトウェアとその機能について説明することができる。</p> <ul style="list-style-type: none"> ● ソフトウェアファイアウォール <ul style="list-style-type: none"> ● ポートブロッキング ● アプリケーションエラー (Application exception) ● ACL ● マルウェアプロテクションソフトウェア <ul style="list-style-type: none"> ● アンチウイルス ● アンチスパイウェア ● ファイルの権限レベルと共有権の基本 <p>2.6 ネットワークに不可欠となる共通要素について説明することができる。</p> <ul style="list-style-type: none"> ● TCP/IP <ul style="list-style-type: none"> ● サブネットティング ● DNS ● DHCP ● クラス ● ゲートウェイ ● 静的とダイナミック ● IP スタック ● ポート ● イーサーネット <ul style="list-style-type: none"> ● 種類 ● スピード

<ul style="list-style-type: none"> ● イン트라ネットとエクストラネット 	<ul style="list-style-type: none"> ● ケーブル ● VPN ● VLAN ● DMZ
<p>4.4 企業のポリシーに基づいて、論理的なアクセス制御の方法を実装することができる。</p> <ul style="list-style-type: none"> ● アクセスコントロールリスト <ul style="list-style-type: none"> ● ユーザー ● グループ <ul style="list-style-type: none"> - 役割(ロール) ● リソース <ul style="list-style-type: none"> - ファイルシステム - ネットワーク ACL - 周辺機器 - 管理者権限 - 配布リスト ● パーミッション(権限) <ul style="list-style-type: none"> ● Read(読み取り) ● Write/Modify(書き込み/変更) ● Execute(実行) ● Delete(削除) ● フルコントロール/スーパーユーザー ● ファイルとシェアの違い 	<p>2.3 想定されたシナリオ下で、手順とガイドラインに基づき NOS 管理機能を実行し運営することができる。</p> <ul style="list-style-type: none"> ● ユーザー管理 <ul style="list-style-type: none"> ● ユーザーの追加と削除 ● 権限の設定 ● グループメンバーシップ ● ポリシー ● ログインスクリプト ● リソースの管理 <ul style="list-style-type: none"> ● ACL ● クォータ(Quotas) ● シャドウボリューム ● ディスクマネージメント ● パフォーマンスモニタリング ● ベースラインの実行
<p>4.5 データセキュリティの方法とセキュアストレージの処分テクニックを実行することができる。</p> <ul style="list-style-type: none"> ● ストレージの暗号化 <ul style="list-style-type: none"> ● ファイルレベルの暗号化 ● ディスクの暗号化 ● テープの暗号化 ● ストレージメディア <ul style="list-style-type: none"> ● ソフトウェアレベルでの消去 <ul style="list-style-type: none"> - ファイルの削除 ● ハードウェアレベルでの消去 <ul style="list-style-type: none"> - 全てのセクターのゼロアウト ● 物理的な破壊 ● リモートワイプ 	
<p>4.6 与えられたシナリオに基づいて、適切な環境管理と手法を実施することができる。</p>	<p>4.3 サーバーロケーションのための物理的環境を考慮することができる。</p>

<ul style="list-style-type: none"> ● 電源装置のコンセプトと最適な手法(ベストプラクティス) <ul style="list-style-type: none"> ● UPS <ul style="list-style-type: none"> - ランタイムとバッテリー容量の検討 - 接続されたデバイスの自動正常のシャットダウン - 電源の定期的なテスト - 最大負荷 - バイパス回路 - リモート管理 ● PDU(電源タップ) <ul style="list-style-type: none"> - 別々の回路へと接続する冗長的なラックPDU ● キャパシティ計画 <ul style="list-style-type: none"> - PDU の評価 - UPS の評価 - 潜在的な消費電力 ● 複数回路 <ul style="list-style-type: none"> - 電源を別にした PDU の冗長構成 ● 安全性 <ul style="list-style-type: none"> ● ESD の手順 ● 消火設備 ● 適切な持ち上げ方法 ● ラックの安全性 ● 床荷重の制限 ● シャープエッジとピンチポイント ● HVAC <ul style="list-style-type: none"> ● 部屋とラックの温度と湿度 <ul style="list-style-type: none"> - 監視とアラート通知 ● 空気の流れ <ul style="list-style-type: none"> - フィラーパネル/バッフル/ブランクパネル ● ホットアイルとコールドアイル 	<ul style="list-style-type: none"> ● 十分かつ専用の電源、適切なアンペア数、電圧の点検 <ul style="list-style-type: none"> ・ UPS システム(負荷、ドキュメントサービス、定期診断) ・ UPS 仕様(ランタイム、最大負荷、バイパス手順、サーバーコミュニケーション、シャットダウン、適切なモニタリング) ● サーバー冷却に関する考慮-HVAC <ul style="list-style-type: none"> ・ 室内の十分なクーリング ・ サーバーラック内の十分な冷却 ・ 温度と湿度の監視
<p>5.1 与えられたシナリオに基づき、IP アドレッシングとネットワークインフラストラクチャサービスを利用してサーバーを設定することができる。</p> <ul style="list-style-type: none"> ● IPv4 と IPv6 の違い ● デフォルトゲートウェイ ● CIDR 表記とサブネッティング 	<p>2.6 ネットワークに不可欠となる共通要素について説明することができる。</p> <ul style="list-style-type: none"> ● TCP/IP <ul style="list-style-type: none"> ・ サブネッティング ・ DNS ・ DHCP

<ul style="list-style-type: none"> ● パブリック IP アドレスとプライベート IP アドレス ● 静的 IP 割り当てと DHCP の違い ● DNS <ul style="list-style-type: none"> ● FQDN ● プライマリ DNS サフィックス/ドメイン検索 ● WINS ● NetBIOS ● NAT/PAT ● MAC アドレス ● ネットワークインターフェースカードの設定 <ul style="list-style-type: none"> ● NIC チーミング <ul style="list-style-type: none"> - 全二重 - 半二重 - オート ● 速度 <ul style="list-style-type: none"> - 10/100/1000 Mbps - 10 Gbps 	<ul style="list-style-type: none"> ● クラス ● ゲートウェイ ● 静的とダイナミック ● IP スタック ● ポート ● イーサネット <ul style="list-style-type: none"> ● 種類 ● スピード ● ケーブル ● VPN ● VLAN ● DMZ
<p>5.2 様々なポートとプロトコルを比較対照することができる。</p> <ul style="list-style-type: none"> ● TCP と UDP の違い ● SNMP 161 ● SMTP 25 ● FTP 20/21 ● SFTP 22 ● SSH 22 ● SCP 22 ● NTP 123 ● HTTP 80 ● HTTPS 443 ● TELNET 23 ● IMAP 143 ● POP3 110 ● RDP 3389 ● FTPS 989/990 ● LDAP 389/3268 ● DNS 53 ● DHCP 68 	<p>2.6 ネットワークに不可欠となる共通要素について説明することができる。</p> <ul style="list-style-type: none"> ● TCP/IP <ul style="list-style-type: none"> ● DNS ● DHCP ● ポート
<p>5.3 与えられたシナリオに基づき、ケーブルを敷設し、適切な</p>	<p>2.6 ネットワークに不可欠となる共通要素について説明することができる。</p>

<p>ケーブル管理手順を実施することができる。</p> <ul style="list-style-type: none"> ● カッパー・ケーブル(銅線) <ul style="list-style-type: none"> ● パッチケーブル <ul style="list-style-type: none"> - クロスオーバー - ストレート - ロールオーバー ● CAT5 ● CAT5e ● CAT6 ● ファイバーケーブル <ul style="list-style-type: none"> ● シングルモード ● マルチモード ● コネクタ <ul style="list-style-type: none"> ● ST ● LC ● SC ● SFP ● RJ-45 ● RJ-11 ● ケーブルの設置とルーティング <ul style="list-style-type: none"> ● ケーブルチャネル ● ケーブルマネジメントトレイ <ul style="list-style-type: none"> - 縦配線用 - 横配線用 ● ラベリング ● 曲げ半径 ● ケーブルバンド 	<ul style="list-style-type: none"> ● イーサネット <ul style="list-style-type: none"> ・ 種類 ・ スピード ・ ケーブル
<p>6.1 災害復旧原則の重要性を説明することができる。</p> <ul style="list-style-type: none"> ● サイトの種類 <ul style="list-style-type: none"> ● ホットサイト ● コールドサイト ● ウォームサイト ● バックアップ(複製)の方法 <ul style="list-style-type: none"> ● Disk to disk ● Server to server ● Site to site ● 運用の継続 <ul style="list-style-type: none"> ● 災害復旧計画 	<p>5.2 あるシナリオを想定した場合の、異なるレプリケーション方法の比較と対比することができる。</p> <ul style="list-style-type: none"> ● ディスクからディスク ● サーバーからサーバー <ul style="list-style-type: none"> ・ クラスタリング ・ アクティブ/アクティブ ・ アクティブ/パッシブ ● サイトからサイト ● サイトの種類 <ul style="list-style-type: none"> ・ コールドサイト ・ ホットサイト ・ ウォームサイト

<ul style="list-style-type: none"> ● 事業継続計画 ● ビジネスインパクト分析 <ul style="list-style-type: none"> - 誰が影響を受けるか - どんな影響を受けるか - 影響の重要度 	<ul style="list-style-type: none"> ● 距離に関する要件 <p>5.3 データ保持と廃棄のコンセプトについて説明することができる。</p> <ul style="list-style-type: none"> ● 潜在する法的要件について ● 潜在する企業ポリシー要件について ● アーカイビングとバックアップの違いについて
<p>6.2 与えられたシナリオに基づき、適切なバックアップの手法を実行することができる。</p> <ul style="list-style-type: none"> ● バックアップ手法 <ul style="list-style-type: none"> ● フル/通常 <ul style="list-style-type: none"> - コピー ● 増分 ● 差分 ● スナップショット ● 部分バックアップ ● ベアメタル回復 ● オープンファイル ● データ復元と OS 復元の違い ● バックアップメディア <ul style="list-style-type: none"> ● リニアアクセス <ul style="list-style-type: none"> - テープ ● ランダムアクセス <ul style="list-style-type: none"> - ディスク - リムーバルメディア - 光メディア ● メディアと復元の最適手法(ベストプラクティス) <ul style="list-style-type: none"> ● ラベリング ● 整合性の検証 ● 復元のテスト ● テープのローテーションと保持 ● メディアの保管場所 <ul style="list-style-type: none"> ● オフサイト ● オンサイト ● セキュリティの検討 ● 保管環境の検討 	<p>5.1 バックアップとリストア方法、メディアの種類とコンセプトについて比較対比することができる。</p> <ul style="list-style-type: none"> ● 方法論(フル、増分、差分) <ul style="list-style-type: none"> ● スナップショット ● コピー ● ベアメタル ● オープンファイル ● データベース ● データと OS リストア ● ローテーションと維持 (grandfather、father and son、ハノイの塔ローテーション方式 (Learning tower)) ● メディアの種類 <ul style="list-style-type: none"> ● テープ ● ディスク <ul style="list-style-type: none"> ● WORM (Write Once Read Many) ● オプティカル ● フラッシュメモリ ● バックアップセキュリティとオフサイトストレージ ● バックアップとリストアプロセスをテストすることの重要性 <p>5.4 想定されたシナリオ下において、災害復旧プランの基本ステップを実施することができる。</p> <ul style="list-style-type: none"> ● 災害復旧テストのプロセス ● 緊急処置の実施 (人命優先の行動) ● 消化剤の適切な使用 ● 緊急時のエスカレーション手順の実施 ● システムの区分 (復旧時の優先順位の決定)
<p>7.1 トラブルシューティングの理論と方法を説明することができる。</p>	<p>6.1 問題と範囲を特定することができる。</p> <ul style="list-style-type: none"> ● 問題を特定しスコープを絞る <ul style="list-style-type: none"> ● ユーザー/ステークホルダーに問合せ、サーバー/

<ul style="list-style-type: none"> ● 問題を特定し、影響範囲を判断する <ul style="list-style-type: none"> ● ユーザー/ステークホルダーに質問を行い、サーバー/環境に加えた変更について特定する ● 必要となる文書/ログを収集する ● 可能であれば、必要に応じて問題を再現する ● 可能であれば、変更を行う前にバックアップを実行する ● 明確な質問により、可能性の高い原因の仮説を立てる <ul style="list-style-type: none"> ● 複数の問題を引き起している障害に共通の要素があるかどうかを確認する ● 原因を判断する理論をテストする <ul style="list-style-type: none"> ● 理論が裏付けられたら、問題解決のための次のステップを決定する ● 理論が裏付けられない場合は、新しい理論を確立するか、エスカレーションを行う ● 問題を解決するための対応計画を策定し、影響のあるユーザーに通知する ● 解決策を実行し、必要に応じてエスカレーションする <ul style="list-style-type: none"> ● 一度に一つの変更のみを行い、問題が解決するかをテスト/確認する ● 問題が解決しない場合は、実施した変更を元に戻し、新しい変更を実施する ● システム全体の機能を確認し、該当する場合には、適切な予防策を講じる ● 根本的な原因分析を実施する ● 発見事項、対応、結果を文書化する 	<p>環境にされた変更事項を特定する</p> <ul style="list-style-type: none"> ● ドキュメンテーション/ログの収集 ● 問題の正確な再現(可能であれば) ● 変更前のバックアップ(可能であれば) <ul style="list-style-type: none"> ● 予想される原因のセオリーを立てる(明確な項目を問う) <ul style="list-style-type: none"> ● 複数の問題を引き起こす症状に共通要素があるか確かめる ● 原因を確かめるため、セオリーをテストしてみる <ul style="list-style-type: none"> ● セオリーが正しいことを確認した後、問題解決のための次段階を判断する ● セオリーが正しくない場合は、新たにセオリーを立てるか、問題をエスカレーションする ● 問題解決のための実行計画を立て、影響を受けたユーザーに通知する ● 解決策を実行するか、適切に問題をエスカレーションする <ul style="list-style-type: none"> ● 一度に一つの変更を行い、その変更点が問題解決につながったかテスト/確認する ● 問題が解決されない場合は、適切であればその変更点を保留とし、新たな変更項目を実施する ● 全システムの機能を確認し、該当する場合、予防措置を実施する ● 根本的原因の分析を行う ● プロセスを通してわかったこと、実行されたアクション、結論を記録する
<p>7.2 与えられたシナリオに基づき、適切なツールと方法を選択した上で、ハードウェアに関連する問題のトラブルシューティングを実施することができる。</p> <ul style="list-style-type: none"> ● 一般的な障害 <ul style="list-style-type: none"> ● POST の失敗 ● 加熱 ● メモリーの障害 ● オンボードコンポーネントの障害 ● プロセッサの障害 ● 不正なブートシーケンス 	<p>6.2 想定されたシナリオ下において、適切なツールと方法を選択してハードウェア問題を効果的にトラブルシューティングすることができる。</p> <ul style="list-style-type: none"> ● 共通する問題 <ul style="list-style-type: none"> ● POST エラー ● オーバーヒート ● メモリ障害 ● 内蔵コンポーネントの障害 ● プロセッサ障害 ● 不正なブートシーケンス

<ul style="list-style-type: none"> • 拡張カードの障害 • Operating system not found エラー • ドライブの障害 • 電源装置の障害 • I/O の障害 ● 障害に共通する原因 <ul style="list-style-type: none"> • サードパーティにより提供されているコンポーネント、または互換性のないコンポーネント • 互換性のない、または不適切な BIOS • 冷却装置の障害 • コンポーネントの不一致 • バックプレーンの障害 ● 環境の問題 <ul style="list-style-type: none"> • 埃 • 湿度 • 温度 • 電源サージ/故障 ● ハードウェアツール <ul style="list-style-type: none"> • 電源テスター(マルチメーター) • ハードウェアの診断 • エアダスター(Compressed air) • ESD(静電気放電)設備 	<ul style="list-style-type: none"> • 拡張カードの障害 • オペレーティングシステムが見つからない • ドライブ障害 • 電源障害 • I/O 障害 ● 共通問題の原因 <ul style="list-style-type: none"> • サードパーティコンポーネントまたは互換性のないコンポーネント • 互換性のない、または不正な BIOS 設定 • クーリングの障害 • 適合しないコンポーネント • バックプレーンの障害 ● 環境問題 <ul style="list-style-type: none"> • ほこり • 湿度 • 温度 • 電源サージ / 障害 ● ハードウェアツール <ul style="list-style-type: none"> • 電源テスター(マルチメーター) • システムボードテスター • コンプレストエア • ESD(Electrostatic Discharge: 静電気放電)
<p>7.3 与えられたシナリオに基づいて、適切なツールと方法を選択し、ソフトウェアに関連する障害を効果的にトラブルシューティングすることができる。</p> <ul style="list-style-type: none"> ● 一般的な障害 <ul style="list-style-type: none"> • ユーザーがログインできない • ユーザーがリソースにアクセスできない • メモリーリーク • ブルースクリーン(BSOD)/STOP エラー • OS boot failure • ドライバの問題 • プロセスの暴走 • ドライブをマウントできない • システムログの書き込みができない • OS のパフォーマンスが遅い • パッチアップデートの失敗 • サービスの失敗 • シャットダウンできない 	<p>6.3 想定されたシナリオ下において、適切なツールと方法を選択してソフトウェア問題を効果的にトラブルシューティングすることができる。</p> <ul style="list-style-type: none"> ● 共通する問題 <ul style="list-style-type: none"> • ユーザーのログインができない • ユーザーがリソースにアクセスできない • メモリーリーク • BSOD/stop • OS ブート障害 • ドライバの問題 • Runaway プロセス • ドライブをマウントすることができない • システムログに書き込みができない • OS のパフォーマンス低下 • パッチアップデートの障害 • サービス障害 • シャットダウンできない

<ul style="list-style-type: none"> • ユーザーが印刷できない ● 一般的な障害の原因 <ul style="list-style-type: none"> • ユーザーアクセスコントロール (UAC/SUDO) • 破損したファイル • ハードディスクの空き容量の不足 • システムリソースの不足 • 仮想メモリー (設定のミス、破損) • フラグメンテーション • プリンターサーバーのドライバー/サービス • プリントスプーラー ● ソフトウェアツール <ul style="list-style-type: none"> • システムログ • 監視ツール (リソースモニター、パフォーマンスモニター) • デフラグツール • ディスク管理ツール (使用領域、空き領域、ボリューム/ドライブマップ) 	<ul style="list-style-type: none"> • 印刷障害 ● 共通問題の原因 <ul style="list-style-type: none"> • マルウェア • 承認されていないソフトウェア • ソフトウェアファイアウォール • ユーザーアカウント制御 (UAC/SUDO) • 不適切な権限 • 破損したファイル • ハードドライブスペースの不足 • システムリソースの不足 • 仮想メモリ (設定不良、破壊) • フラグメンテーション • 暗号化 • プリンターサーバー ドライバー/サービス • プリントスプーラー ● ソフトウェアツール <ul style="list-style-type: none"> • システムログ • モニタリングツール (リソースモニター、パフォーマンスモニター) • デフラグメンテーションツール
<p>7.4 与えられたシナリオに基づき、適切なツールと方法を選択し、ネットワークに関連する障害を効果的に診断することができる。</p> <ul style="list-style-type: none"> ● 一般的な障害 <ul style="list-style-type: none"> • インターネットに接続できない • メールの送受信ができない • リソースが使用できない • DHCP サーバーが正しく設定されていない • 機能しない、または到達しない • Destination host unreachable エラー • Unknown host エラー • デフォルトゲートウェイが正しく設定されていない • サービスプロバイダーでの障害 • ホスト名/FQDN を検索できない ● 一般的な障害の原因 <ul style="list-style-type: none"> • 不適切な IP アドレス • VLAN の設定 	<p>6.4 想定されたシナリオ下において、適切なツールと方法を選択してネットワーク問題を効果的に診断することができる。</p> <ul style="list-style-type: none"> ● 共通する問題 <ul style="list-style-type: none"> • インターネット接続の障害 • Eメールの障害 • リソース利用不可 • DHCP サーバーの設定不良 • 動作不良、または到着不可 • ホスト名が見つからない • デフォルトゲートウェイの設定不良 • サービスプロバイダーの障害 • IP アドレスではアクセスできるが、ホスト名ではアクセスできない ● 共通問題の原因 <ul style="list-style-type: none"> • 不適切な IP 設定 • VLAN 設定 • ポートセキュリティ

<ul style="list-style-type: none"> • ポートセキュリティ • 不適切なサブネッティング • コンポーネントの障害 • 誤った OS ルーティングテーブル • ケーブル不良 • ファイアウォール(正しく設定されていない、ハードウェアの故障、ソフトウェアの不具合) • NIC が正しく設定されていない、ルーター/スイッチの障害 • DNS と DHCP いずれか/両方の障害 • hosts ファイルが正しく設定されていない • IPv4 と IPv6 の不適切な設定の違い ● ネットワークツール <ul style="list-style-type: none"> • ping • tracert / traceroute • ipconfig / ifconfig • nslookup • net use / mount • route • nbtstat • netstat 	<ul style="list-style-type: none"> • 不適切なサブネッティング • コンポーネント障害 • 不適切な OS ルートテーブル • ケーブル不良 • ファイアウォール(設定不良、ハードウェア障害、ソフトウェア障害) • 設定不良の NIC、ルーティング / スwitchの問題 • DNS および DHCP 障害 • ホストファイルの設定不良 ● ネットワークツール <ul style="list-style-type: none"> • ping • tracert / traceroute • ipconfig / ifconfig • nslookup • net use / mount • route • nbstat • netstat
<p>7.5 与えられたシナリオに基づき、適切なツールと方法を選択し、ストレージに関連する障害を効果的にトラブルシューティングすることができる。</p> <ul style="list-style-type: none"> ● 一般的な障害 <ul style="list-style-type: none"> • ファイルへのアクセスが遅い • OS not found エラー • データが利用できない • バックアップが実行できない • エラーランプ • デバイスのマウントができない • ドライブが利用できない • 論理ドライブにアクセスできない • データの破損 • I/O パフォーマンスが遅い • リストアの障害 • キャッシュの失敗 • 複数ドライブの障害 ● 一般的な障害の原因 	<p>6.5 想定されたシナリオ下において、適切なツールと方法を選択してストレージ問題を効果的にトラブルシューティングすることができる。</p> <ul style="list-style-type: none"> ● 共通する問題 <ul style="list-style-type: none"> • ファイルアクセスが遅い • OS が見つからない • データの利用ができない • バックアップの失敗 • エラーランプ • デバイスの実装ができない • ドライブが利用できない • 論理ドライブにアクセスできない • データ破損 • I/O のパフォーマンスが遅い • リストアの失敗 • キャッシュの破損 • 複数ドライブの不具合 ● 共通問題の原因

<ul style="list-style-type: none"> • メディアの障害 • ドライブの障害 • コントローラーの障害 • HBA の障害 • 接続が緩んでいる • ケーブルの障害 • 正しく設定されていない • 不適切なターミネーション • ブートセクターの破損 • ファイルシステムテーブルの破損 • アレイの再構築 • 不適切なディスクパーティション • セクター不良 • キャッシュバッテリーの障害 • キャッシュの遮断 • 容量不足 • 不適切な RAID の設定 • 不適切なドライブ • バックプレーンの障害 ● ストレージツール <ul style="list-style-type: none"> • パーティショニングツール • ディスク管理 • RAID アレイ管理 • アレイ管理 • システムログ • net use / mount コマンド • 監視ツール 	<ul style="list-style-type: none"> • メディア障害 • ドライブ障害 • コントローラー障害 • ホストバスアダプタ(HBA)の障害 • コネクターのゆるみ • ケーブルの不具合 • ミスコンフィギュレーション • 不適切なターミネーション • ブートセクターの破損 • ファイルシステムテーブルの破損 • アレイの再構築 • 不適切なディスクパーティション • 不良セクター • キャッシュバッテリーの障害 • キャッシュがオフになっている • スペースが不十分である • 不適切な RAID コンフィギュレーション • 適合しないドライブ • バックプレーンの障害 ● ストレージツール <ul style="list-style-type: none"> • パーティショニングツール • ディスクマネージメント • RAID アレイ管理 • システムログ • Net use/マウントコマンド • モニタリングツール
<p>7.6 与えられたシナリオに基づき、適切なツールと方法を選択し、セキュリティ関連する障害を効果的に診断することができる。</p> <ul style="list-style-type: none"> ● 一般的な障害 <ul style="list-style-type: none"> • ファイルの完全性の問題 • 権限昇格 • アプリケーションが読み込むことができない • ネットワークファイル/共有ファイルにアクセスできない • ファイルを開くことができない • 過度のアクセス • 過度のメモリー使用率 	

- 一般的な障害の原因
 - 開放されたポート
 - 有効なサービス
 - 無効なサービス
 - 侵入検知の設定
 - アンチマルウェアの設定
 - ローカルポリシー/グループポリシー
 - ファイアウォールルール
 - 不適切に設定された権限
 - ウイルス感染
 - 悪意のあるプロセス/悪意のあるサービス
- セキュリティツール
 - ポートスキャナー
 - スニファー
 - 暗号化
 - チェックサム
 - telnet クライアント
 - アンチマルウェア