競技職種実施要領

ITネットワークシステム管理職種

Ver.1.1_2025年 6月12日

本競技職種実施要領は、以下の内容で構成される。

1 はじめに

1.1 競技職種の名称

ITネットワークシステム管理

1.2 競技職種に関連する職務または職業の説明

ITネットワークシステム管理者は、民間および公共セクターの小規模または大規模な組織で働き、日々のビジネスの運営にとって重要な広範囲のITサービスを提供している。「ダウンタイム」は常に組織に多大なコストを生じさせるため、ITネットワーク システム管理者には、ユーザーのニーズを満たし、ユーザーが業務を効果的に実行するのに必要なシステムとサービスレベルを継続できるよう、専門職として、ユーザーと意見を交わしながら職務を遂行する責任がある。

ITネットワークシステム管理者は、ネットワークオペレーションセンター、インターネットサービスプロバイダー、データセンター、温度・湿度管理されているサーバールームなど、多様な環境で働く。また、その時々にチームで、単独で、またはその両方で働くことがある。ITネットワークシステム管理者は、オペレーティングシステムおよびネットワーク機器のユーザーサポート、トラブルシューティング、ネットワーク/サービス設計、インストール/アップデート、コンフィギュレーションなどの知識とスキル（技能）をベースとして幅広いサービスを提供する。適切なコミュニケーション能力、業界の進歩について調査を怠らず最新情報に通じていることなどは、優れたITネットワークシステム管理者に共通する特性である。

訓練と経験を積んだITネットワークシステム管理者は高いレベルの個人的責任感および自主性を身に着けている。ITシステムへのセキュリティ侵害を防止し、ダウンタイムを最小限にとどめて事業運営の継続を保証することから、新しいシステムの設計への貢献にいたるまで、情報化社会において欠かせない重要な責務を担っている。

2 技能五輪全国大会職業標準

2.1 技能五輪全国大会職業標準（項目及び配点率）

項目		配点率（%）
1	作業組織と管理	
2	コミュニケーションと対人スキル	
3	データ転送ネットワークの設計/構築/運用	30
4	ネットワークサービスの設計/構築/運用	30
5	インフラストラクチャの自動化	10
6	トラブルシューティング	30

2.2 技能五輪全国大会職業標準（項目とその内容および相対重要性配点率(%)）

項目とその内容		相対重要性配点率(%)
1	**作業組織と管理**	
	各自は以下を知り、理解している必要がある。 • 安全衛生に関する法律、義務、規則、文書 • ESD（静電気放電）の場合など、個人用防護具（PPE）を使用しなければならない状況 • 特定の分野で経験や知識が不足している場合に、同僚に助けを求める能力 • ユーザーの機材や情報を扱う際の完全性とセキュリティの重要性 • 計画立案、スケジュール設定、優先順位付けの手法 • あらゆる業務の遂行における正確さ、確認、細部への注意の重要性 • 作業を順序立てて行うことの重要性 • 共同作業や調査の方法と技術 • 自身の専門性向上に継続的に取り組むことの価値 • IT システムの変化のスピードと常に最新情報を把握しておく必要性	
	各自は以下を実施できること。 • 安全衛生の基準、ルール、規則に従う。 • 安全な作業環境を維持する。 • ESD 対策用の適切な個人用防護具を特定し、使用する。 • 工具や機材を安全かつ確実に選択、使用、洗浄、保守、保管する。 • 効率を最大化するように作業エリアを計画し、定期的な整理整頓の規律を維持する。 • 優先順位の変化に応じて、定期的にスケジュールを設定、リスケジュールし、複数のタスクを実行する。 • 効率的に作業し、進捗や成果を定期的に確認する。 • Cisco、Microsoft、Linux など、少なくとも 1 つの特定分野に特化したさまざまな認定要件を満たす。 • 知識の向上に資するよう、綿密かつ効率的な調査手法を用いる。 • 新しい方法やシステムを積極的に試し、変化を受け入れる。 • 同僚と効果的に連携して、効率と学習を最大化する。 • プロジェクトチームの一員として効果的に業務を行う。	

2	**コミュニケーションと対人スキル**	
	各自は以下を知り、理解している必要がある。 • 効果的なコミュニケーションの一環としての傾聴の重要性 • 同僚の役割と必要条件、および最も効果的なコミュニケーション方法 • 同僚やマネージャとの生産的な仕事上の関係を構築し、維持することの重要性 • 効果的なチームワークのためのテクニック • 誤解や相反する要求を解決するためのテクニック • 困難な状況を解決するために緊張や怒りをコントロールするプロセス	
	各自は以下を実施できること。 • 優れた傾聴スキルや質問スキルを使用して、複雑な状況への理解を深める。 • 同僚との口頭および書面によるコミュニケーションに関して、一貫した効果的なコミュニケーション・マネジメントを行う。 • 同僚のニーズの変化を認識しそれに対応する。 • 強固で効果的なチームの育成に積極的に貢献する。 • 知識や専門技能を同僚と共有し、支え合う学習文化を育む。 • 緊張/怒りをコントロールし、各自に問題解決への自信を与える。	
3	**データ転送ネットワークの設計/構築/運用**	**30**
	各自は以下を知り、理解している必要がある。 • OSI モデルと TCP/IP プロトコルスタック • データリンク層、ネットワーク層、トランスポート層の各プロトコルの動作原理 • さまざまなネットワーク・コンポーネントの役割と機能 • ネットワークトポロジーの種類と使用シナリオ • VLAN によるネットワークの分割 • LAN および WAN の安全を確保するためのセキュリティ・プロトコル • IPv4 および IPv6 のネットワークアドレスの概念 • ルーティングとスイッチングの概念 • 冗長化と負荷分散の原理 • ネットワークプロトコルに対する一般的な攻撃の種類と対策 • アクティブネットワークの機器の管理方法 • ネットワーク機能の仮想化の概念と原理 • コントローラーベース/ソフトウェア定義のネットワーク管理アプローチ	

	各自は以下を実施できること。 • アクティブネットワークの機器の基本的な初期化を実行する。 • アクセス、アグリゲーション、コアの各レベルのスイッチを構成する。 • スタティックルーティングや OSPF、BGP、EIGRP などの内部および外部のゲートウェイ・ルーティング・プロトコルを使用して、全社的な接続を提供する。 • ネットワーク境界において基本的な外部接続構成を適用する。 • GLBP、HSRP、VRRP、LACP、PAgP などを使用して、ルーティングやスイッチング時にネットワーク負荷分散とフォールト・トレランスを実現する。 • コントロールプレーンとデータプレーンに基本的なセキュリティ構成を適用する。 • IPSec、SSL-VPN、OpenVPN、DMVPN、GRE などの VPN テクノロジーを使用して、リモート・ブランチ間のネットワーク接続を提供する。 • CDP、NetFlow、syslog、SNMP、tcpdump、Wireshark などのネットワーク検出ツールおよびトラフィック分析ツールを使用する。	
4	**ネットワークサービスの設計/構築/運用**	**30**
	各自は以下を知り、理解している必要がある。 • 一般的なアプリケーションプロトコルの動作の原理 • クライアントサーバー・アプリケーション対話モデル • アプリケーションのデプロイのためのオペレーティングシステムの組み込み機能 • サービス、アプリケーション、システムの異なるグループ間の依存構造 • Linux または Windows を使用したネットワークサービスの実装オプション	
	各自は以下を実施できること。 • ディレクトリサービス（ADDS、LDAP）のインストールと管理 • ドメイン名サービス（Windows DNS、BIND）のインストールと管理 • DHCP サービスのインストールと管理 • ネットワークアドレス変換サービスのインストールと管理 • NTP サービスのインストールと管理 • AAA（認証、認可、アカウンティング）サービスのインストールと管理 • IT インフラストラクチャ・リソース監視システムのインストールと管理 　○ Icinga2、Nagios、Cacti、Windows リソースモニターなど • メール送受信システム（SMTP、IMAP、POP）のインストールと管理	

	• PKI（公開鍵基盤）サービスの設定 　○ Active Directory 証明書サービス、OpenSSL • 共有サービス（SMB、DFS、NFS、FTP）のインストールと管理 • ウェブサーバー（Apache、Nginx、IIS）を使用したウェブホスティングサービスのインストールと管理 • 端末接続サービス（SSH、リモートデスクトップサービス、Telnet）のインストールと管理 • バックアップシステムのインストールと管理 　○ Windows Server バックアップ、rsync、スクリプトベースのバックアップ（bash、バッチ、PowerShell など） • クライアント・ワークステーション展開システムのインストールと管理 　○ Windows 展開サービス、グループポリシー • ファイルシステムの管理 　○ ソフトウェア RAID、mdadm、LVM/ダイナミックディスク 　○ NTFS、ReFS、ext4、NTFS などのファイル システム	
5	**インフラストラクチャの自動化**	**10**
	各自は以下を知り、理解している必要がある。 • 継続的インテグレーションと継続的デリバリー/デプロイメント・パイプラインの概念 • さまざまな自動化ツールの機能 • コードのバージョン管理の重要性 • インフラストラクチャ自動化ツールの動作	
	各自は以下を実施できること。 • さまざまなスクリプト/プログラミング言語を使用して、定期的なインフラ保守作業を設定して実行する。 　○ Bash 　○ PowerShell 　○ Python • システムのデプロイと構成管理に最新の自動化ツールを使用する。 　○ Git 　○ YANG 　○ RESTCONF 　○ NETCONF	

	• IaC（Infrastructure as Code）を記述して実装する。 　○ Python 　○ Ansible	
6	**トラブルシューティング**	**30**
	各自は以下を知り、理解している必要がある。 • ユーザーの予算要件を考慮した、特定のユーザー要件に適合するオペレーティングシステムの範囲とその機能 • さまざまな種類のハードウェアに対して適切なドライバーを選択するプロセス • ハードウェアの基本機能とセットアップ手順 • 取扱説明書に従うことの重要性と、従わない場合の結果/コスト • インストールまたはアップグレードの前に対処すべき使用上の注意 • インストールまたはアップグレードの完了を文書化する目的 • 適切なツールと技術を使用して行うコンピューターシステムのトラブルシューティング	
	各自は以下を実施できること。 • ユーザーの期待に確実に応えられるように、ユーザーのニーズを注意深く聞き、解釈し、正確に特定する。 • オペレーティングシステムを選択する：プロプライエタリ/オープンソース、顧客リソース関連の総所有コスト • ユーザー/メーカーの仕様に適合するために必要なハードウェアと適切なデバイスドライバーを正確に特定する。 • オペレーティングシステム/サーバーシステムの役割や特徴を選択する。たとえば、Active Directory ドメインサービス（役割）や Windows Server バックアップ（機能）など。 • 役割/機能に関して提案されたソリューションを議論し、ユーザー、同僚、上司などの関係者と合意する。 • ソリューションの詳細を反映した技術文書を作成して、合意および署名を求める。 • 製造元の指示または組織内の最良事例に従って、適切な役割/機能を構成する。 • テストして問題があれば修正し、必要に応じて再テストを行う。 • ユーザーの承認を得て、記録に残す。	

	• システムログを使用して問題を発見し特定する。 • ネットワークのパケット検査、接続確認ツールなどを使用して、ネットワークの問題のトラブルシューティングと特定を行う。	
	合計	**100**

3 採点方法、採点基準とその配点、公表方法

3.1 採点対象

区分
トラブルシューティング（課題１）
クライアント/サーバー環境（課題２）
ネットワーキング環境（課題３）

3.2 採点基準

項目 / 区分	採点基準概要	配点
トラブルシューティング（課題１）	以下について、回答文の正確性を評価する。 ● トラブル原因の特定 ● トラブルによって発生しているシステム挙動の特定 ● トラブル解決手順の提示	30
クライアント/サーバー環境（課題２）	以下について、課題の要求に対する正確性を評価する。 ● サーバー設定/動作 ● クライアント設定/動作	35
ネットワーキング環境（課題３）	以下について、課題の要求に対する正確性を評価する。 ● ルータ設定/動作 ● スイッチ設定/動作 ● ファイアウォール設定/動作 ● 到達性	35
合計		100

3.3 公表方法

主催者が指定する方法において、参加選手本人による照会の場合、原則として競技結果（順位、得点）を伝達する。また、要望に応じて競技主査から個別に伝達する。

4 競技課題の概要

4.1 競技課題の構成

競技課題は以下の表に示す独立した３つの課題から構成される。

課題番号	課題名	タスク概要
課題１	トラブルシューティング	トラブルシュート回答文作成
課題２	クライアント/サーバー環境	クライアント/サーバー設定
課題３	ネットワーキング環境	ルータ/スイッチ/ファイアウォール設定

4.2 競技課題の要求事項

課題１：トラブルシューティング

トラブルの原因と解決方法についての調査報告が求められる。本課題では、複数のネットワークノード（Ciscoルータ、スイッチ、ファイアウォール）、クライアント/サーバー（Windows、Windows Sever、Debian Linux）で構成されるネットワークシステム環境が課題環境として提供される。この課題環境はトラブルが内包された状態で提供される。架空のユーザーからのクレームに対して、トラブルの原因となっているノードや設定を特定し、その解決方法を回答することが求められる。回答は所定の様式に対して調査結果を記述することで行う。実際にトラブルを修復したか否かは問われない。明確で論理的な文章によって以下の点が記述されているかが評価される。

- トラブルの原因となっている装置や設定内容、および、それによって発生しているシステム挙動
- トラブルを解決するために必要となる作業手順（コマンドや操作を含め、第三者が再現可能な記述となっていること）

課題２：クライアント/サーバー環境

サーバーOSとしてDebian LinuxおよびWindows Server、クライアントOSとしてDebian LinuxおよびWindowsを使用し、競技課題として示される要求仕様に基づいてクライアント/サーバー環境を構築することが求められる。複数サーバーが連携してサービス提供を行う環境の構築が想定される。下記リストは採点する可能性のある評価項目の例である。最終決定の評価項目リストではなく、評価項目を網羅するものでもないことに注意すること。

Linux評価項目の例：

- Linux基本設定
  - ユーザー設定、ネットワーク設定
- DNSサーバー (bind)
  - 正引き、逆引き、フォワード、ゾーン転送、委任

- Webサーバー(apache、nginx)
  - HTTPS通信(証明書エラーなし)、認証、アクセス制御、リダイレクト
- Webアプリケーション配備
  - webメールシステム、CMS、監視システム
- メールサーバー (postfix、dovecot)
  - メール送受信、中継、バックアップ、メッセージ制限、認証、暗号化
- ファイルサーバー(samba、FTP、NFS)
  - ファイル共有、認証、アクセス制限
- プロキシサーバー/リバースプロキシ/ロードバランサ(squid、nginx、HAProxy)
  - 認証、アクセス制限、負荷分散、バックエンド死活監視
- ストレージサーバー（open-iscsi）
- ディレクトリサーバー（OpenLDAP）
- DHCPサーバー（isc-dhcp-server）
- 認証局（OpenSSL）
- サイト間VPN（StrongSwan、WireGuard）
- ファイアウォール(nftables)
- 自動化（Ansible、Bash）

Windows Server評価項目の例：

- Windows Server基本設定
  - ユーザー設定、ネットワーク設定
- Active Directory関連サービス
  - ADドメインサービス、ADフェデレーションサービス、AD証明書サービス、グループポリシー
- ネットワークサービス
  - DHCPサーバー（フェールオーバー）、DNSサーバー、ネットワークポリシーとアクセスサービス、Webサービス (IIS)、リモートデスクトップサービス
- ファイルサービスおよび記憶域サービス
  - ファイルサーバー、データ重複除去、DFS名前空間、ファイルサーバーリソースマネージャー、iSCSIターゲット
- 仮想化サービス
  - Hyper-V、フェールオーバークラスタリング
- 自動化（Ansible、PowerShell）
- その他：　Windows展開サービス、Windows Serverバックアップ

課題３：ネットワーキング環境

競技課題として示される要求仕様に基づいてネットワークを構築することが求められる。Cisco Modeling Labs – Personalによる仮想環境を用いて競技を行う。構築規模としては、10台前後のCiscoネットワークノード（ルータ、スイッチ、ファイアウォール）で構成されるネットワーク環境の構築が想定される。下記リストは採点する可能性のある評価項目の例である。最終決定の評価項目リストではなく、評価項目を網羅するものでもないことに注意すること。

ネットワーク評価項目の例：

- 基本設定
  - ホスト名、パスワード認証、権限レベル、時間/タイムゾーン
- インタフェース設定
  - IPアドレス(IPv4/IPv6)、カプセル化、論理インタフェース作成
- IPルーティング設定(IPv4/IPv6)
  - スタティックルーティング
  - ダイナミックルーティング（RIP、OSPF、EIGRP、BGP）
  - 集約、メトリック操作、再配送、経路フィルタ
- NAT/NAPT設定
- WAN設定
  - PPPoE、IPSecVPN、GRE、DMVPN
- ゲートウェイ冗長化設定
  - HSRP、VRRP、GLBP
- サービス設定
  - DHCP、NTP、Telnet、SSH、TFTP、SNMP
- セキュリティ設定
  - ポートセキュリティ、ACL、ファイアウォール
- L2/L3スイッチ設定
  - VLAN、VTP、STP、リンクアグリゲーション

4.3 競技課題の公表

課題１については、競技前日の競技説明・機材確認の際にネットワークトポロジーなどの基本情報のみが記載された冊子を配布する。課題２および課題３については事前公表しない。

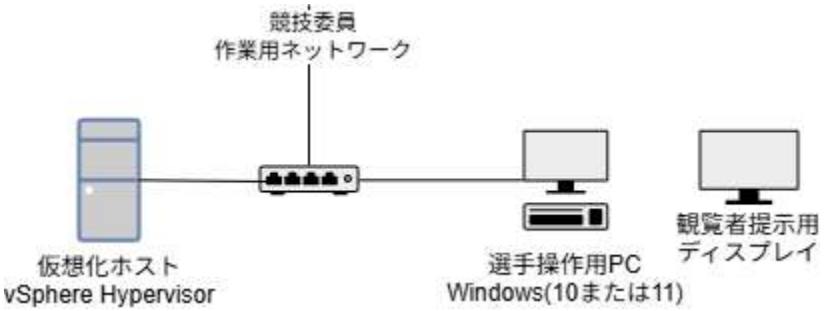
4.4 競技課題の変更

5 職種限定規則

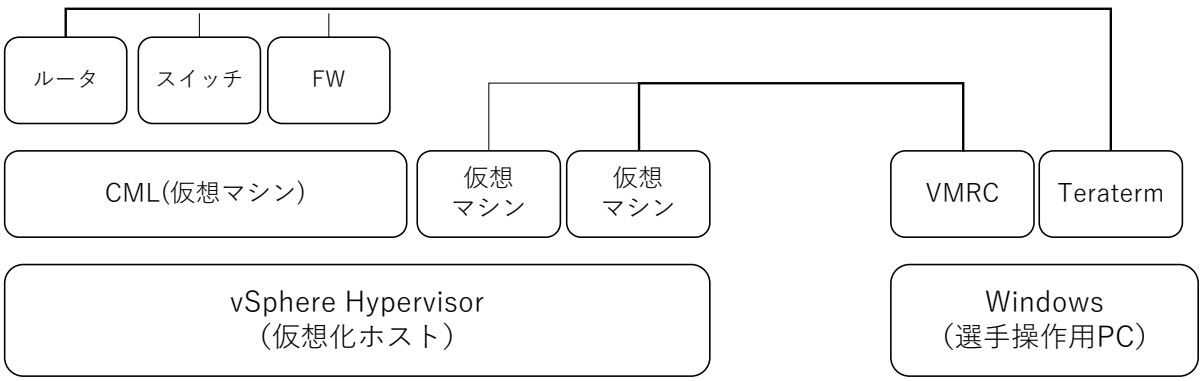
- 各種マニュアル、参考書、ノート等の持ち込みは認めない。
- ソフトウェアの持ち込みは認めない。
- 質問などがある場合には、質問票に記入して競技委員に申し出ること。質問する時間は、競技開始30分後から競技終了30分前までとする。ただし、ハードウェアトラブルまたはソフトウェアの初期設定不良などが疑われるケースについては随時質問可能とする。
- 競技終了の合図で、作業を直ちに終了すること。
- 競技時間内に作業を終了した場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
- 競技中に、トイレ、体調不良などが生じた場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
- 競技中の水分補給のための飲料水の持ち込みは認める。
- スマートフォン等（携帯電話やタブレットも含む）の電源は切っておくこと。
- 競技中に、モバイルルータや競技会場のフリーWi-Fiスポット等を使用してインターネットへアクセスすることは認めない。
- 競技中は、使用機器の落下や転倒によるケガ、椅子の転倒、VDT作業時間等に留意し、安全作業を常に心がけること。
- 競技中に、競技者と競技観覧者（引率者・指導者含む）の間で意図的な合図やコミュニケーション行為を行うことは認めない。
- 競技中に、競技観覧者（引率者・指導者含む）が競技者の競技課題冊子にフォーカスし、課題内容をカメラで撮影する行為、および、その行為を競技者がほう助する行為は認めない。
- 競技中に、競技観覧者（引率者・指導者含む）が自身の所属組織の選手およびその作業画面を撮影する行為は認める。
- 競技中に、競技観覧者（引率者・指導者含む）が自身の所属組織以外の選手およびその作業画面を撮影する行為は、被撮影者側の組織の許可を得ている場合のみ認める。

6 実施要領

競技環境で使用するPC（物理マシン）は各選手２台である。１台は仮想化ホストとして vSphere Hypervisor が動作し、１台は選手が操作するPCとしてWindows(10または11)が動作する。ディスプレイは各選手２台である。１台は選手作業用、１台は観覧者への提示用に使用する。各PCは下図の通りネットワーク接続された状態となっている。選手操作用PCのネットワーク設定を変更しないこと。また、仮想化ホスト(vSphere Hypervisor)のwebインタフェースやコンソールへ直接アクセスして操作する行為を禁止する。



競技は、Cisco Modeling Labs – Personal(CML) および vSphere Hypervisor を用いた仮想環境にて実施する。下図に競技環境におけるソフトウェア配置の概要を示す。CMLはvSphere Hypervisor上の仮想マシンとして構成され、競技課題に応じたネットワークシミュレーションを実行する。競技課題において設定や操作対象となるルータ/スイッチ/ファイアウォールはCML上で動作する仮想的なネットワークノードである。選手は操作用PCからTeratemを用いてこれらのノードへ接続し課題作業を実施する。また、競技課題において設定や操作対象となるクライアント/サーバー端末もvSphere Hypervisor上の仮想マシンとして構成される。選手は操作用PCからVMware Remote Console(VMRC)を用いてこれらの端末へ接続し課題作業を実施する。競技開始時点において、CMLによるネットワークシミレーション、各ネットワークノード、仮想マシンは起動しており、選手操作用PCから接続可能な状態で提供されるものとする。



競技に使用する主なソフトウェア：

本稿執筆時点で使用を予定している各ソフトウェア(およびバージョン)は以下の通りである。（ただし、大会開催時点までに変更になる場合がある）

- 競技用サーバーOS： Debian GNU/Linux 12.10、Windows Server 2022 (評価版)
- 競技用クライアントOS： Debian GNU/Linux 12.10、Windows10 (評価版)
- 仮想化ホストのOS： VMware vSphere Hypervisor 8.0U3e
- 選手操作用PCのOS：Windows11
- ネットワーク仮想化/シミュレーション： Cisco Modeling Labs – Personal 2.7.2
- その他： TeraTerm、VMware Remote Console

Cisco Modeling Labsにおける使用ノード：

CMLのネットワークシミュレーションで使用するノードタイプの範囲は次の通りである。

- ルータノード
  - ノードタイプ： IOSv
  - バージョン： IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.x
- スイッチノード
  - ノードタイプ： IOSvL2
  - バージョン： vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Version 15.x
- ファイアウォールノード
  - ノードタイプ： ASAv
  - バージョン： Cisco Adaptive Security Appliance Software Version 9.x
- 外部接続用ノード
  - ノードタイプ： External Connector
  - 仮想マシンや外部ネットワークとの接続用であり、競技における操作の対象ではない。
- 管理機能なしスイッチノード
  - ノードタイプ： Unmanaged Switch
  - L2レベルの接続用であり、競技における操作の対象ではない。

7 競技スケジュール

競技スケジュールは以下の通りである。

2025/10/16　木曜日	
14:00	集合
14:10 – 15:30	競技内容の説明、競技場所の抽選、機材の確認
15:30	解散
2025/10/17　金曜日	
9:10	集合
9:15 – 9:30	注意事項等の説明
9:30 – 12:00	競技「課題１：トラブルシューティング」
12:10	解散
2025/10/18　土曜日	
8:40	集合
8:45 – 9:00	注意事項等の説明
9:00 – 12:30	競技「課題２：クライアント/サーバー環境」
12:40	解散
2025/10/19　日曜日	
8:40	集合
8:45 – 9:00	注意事項等の説明
9:00 – 12:00	競技「課題３：ネットワーキング環境」
12:15	解散

8 支給材料

競技中に使用するメモ用紙は適宜配布する。

区　分	品　　名	寸法又は規格	数　量	備　考
	メモ用紙	A4	適宜	

9 選手持参工具・材料

各自筆記用具を持参すること。

区　分	品　　名	寸法又は規格	数　量	備　考
	筆記用具			

10　競技会場設備基準

各選手の作業エリア内の設備・機材は以下の通りである。

区　分	品　　名	寸法又は規格	数　量	備　考
	作業台	W1800xD900xH700	1	
	OA チェア	背あり/肘無し/キャスター付き	1	
	パソコン	CPU コア数 16 以上/メモリ 64GB/ストレージ(SSD)1TB 以上	1	仮想化ホスト
	パソコン	メモリ 16GB/ストレージ 256GB 以上	1	選手操作用 PC
	ディスプレイ	２７インチ液晶ディスプレイ	2	
	キーボード	日本語キーボード	1	
	マウス		1	
	スイッチングハブ		1	
	LAN ケーブル		2	

11　参考資料：昨年度全国大会競技課題および国際大会競技課題

参考資料として次項以降に昨年度大会の競技課題を添付する。また、技能五輪全国大会は国際大会（WorldSkills）の日本代表選手を選考する大会でもあり、国際大会競技課題との整合化をできるかぎり図っていく方針とする。前回の国際大会（WorldSkills2024）の競技課題については、

https://worldskills.org/internal/competition-documentation/lyon-2024/test-projects/

にて入手できる。ただし、アカウント登録（無料）が必要となる。

第 62 回 技能五輪全国大会

IT ネットワークシステム管理

1 日目 課題 1 トラブルシューティング課題

競技課題

令和 6 年 11 月 23 日(土)

競技時間：2 時間（9：00～11：00）

競技に関する注意事項：

- ✓ 競技開始の合図まで本冊子および別紙「競技チケット」を開かないこと。
- ✓ 携帯電話の電源はあらかじめ切っておくこと。
- ✓ 本冊子および「競技チケット」を綴じてある留め金は外さないこと。
- ✓ 競技が開始されたら、本冊子の下欄の座席番号及び競技者氏名を記入すること。
- ✓ 各種マニュアルや印刷物、記憶媒体の持ち込みは一切認めない。（事前公開資料を除く）
- ✓ 競技時間は 2 時間とする。作業手順は問わないので、効率を考えて作業を行うこと。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技中の水分補給のための飲料水の持ち込みは認める。
- ✓ 競技時間内に作業が終了した場合は、各仮想マシンは起動したままの状態とし、競技委員に申し出て退席許可を得ること。
- ✓ 仮想マシンおよび CML[2] のネットワークシミュレーションの接続の変更はしないこと。ただし必要に応じて、シャットダウンや再起動して構わない。
- ✓ 競技終了の合図で、直ちに作業を終了すること。
- ✓ 本冊子は持ち帰り厳禁である。机上に置いたまま退席すること。

座席番号	
氏　　名	

第 62 回技能五輪全国大会 IT ネットワークシステム管理職種
1 日目 課題 1 トラブルシューティング課題

競技について

- 事前に公開した課題環境資料に示した仮想ネットワーク環境を用いて競技をおこなう。事前公開した内容を次ページ以降にも掲載する。
- 競技課題となるトラブルと解答用紙は、別紙「競技チケット」に提示する。
- チケットは全部で 7 つある。チケットはどれから取り組んでも構わない。
- トラブルに対して適切な「原因」と対応した「処置内容」を、UVdesk ヘルプシステムから送信しなさい。
- すべてのチケットの問題は、原因が 2 つで構成されている。これら 2 つの原因を特定し、問題を解決するため処置内容を提示する必要がある。なお、2 つある原因のうち 1 つしか解決できない場合も加点対象になる。
- チケットへの回答は明確で論理的な文章によって、次の点が記述されていることがポイントとなる。

  「原因 」について

  ・原因となっている装置や設定内容、および、それによって発生しているシステム挙動

  「処置内容」について

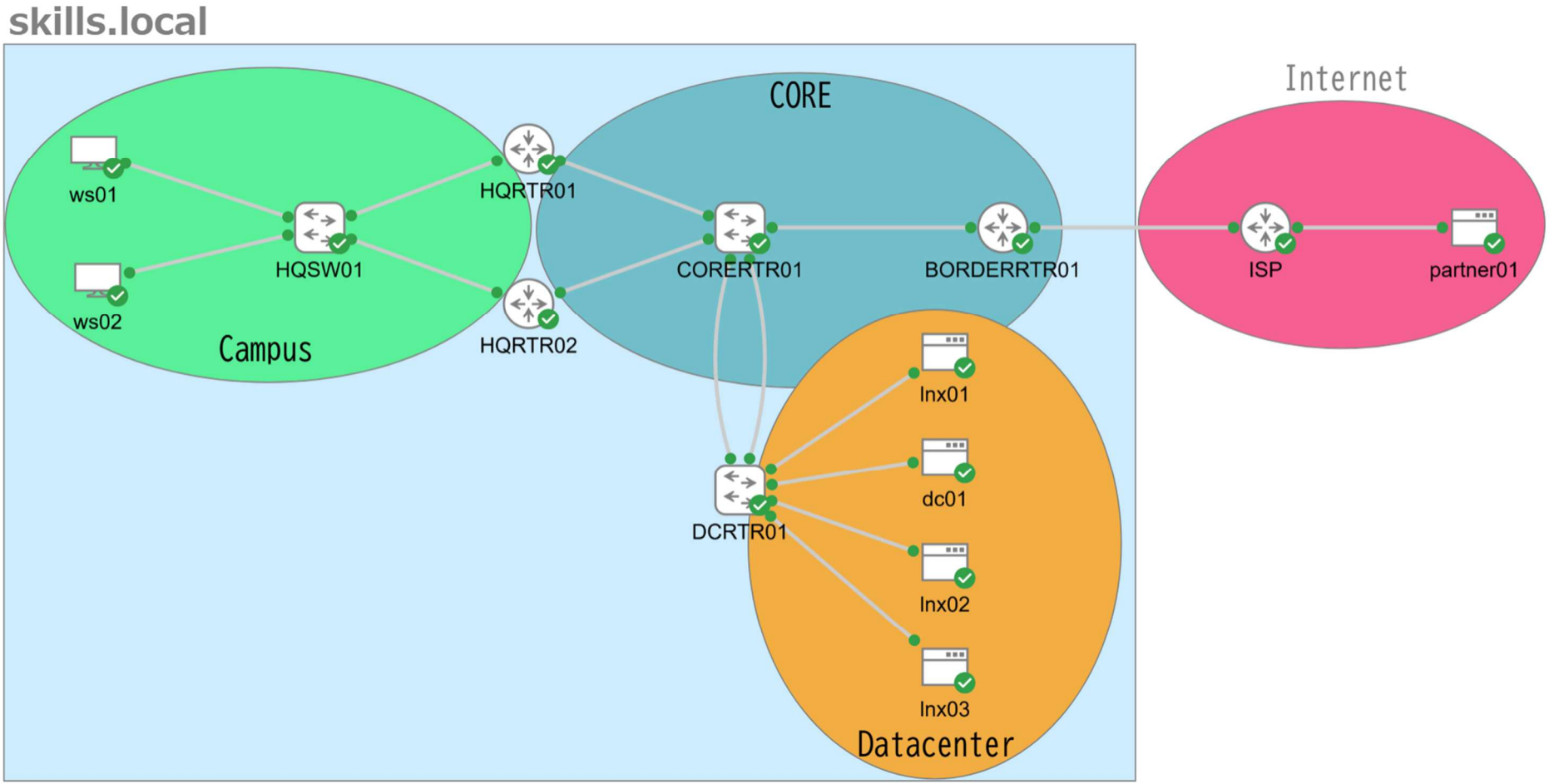
  ・トラブルを解決するために必要となる作業手順

  ・コマンドや操作を含め，第 3 者（競技委員）が再現可能な記述
- 本競技は UVdesk ヘルプシステムより送信された回答文章のみが採点対象となる。課題環境に対して実際に修復措置が適用されているか否かは問わない。
- 各ホストや UVdesk ヘルプシステムへは、管理用 PC のデスクトップ上にあるショートカットよりアクセスできる。接続に不具合がある場合は、速やかに競技委員まで申し出ること。

パケットキャプチャとして Wireshark を利用してよい。Wireshark(Win 版)のインストーラは、競技者が操作する管理用 PC のデスクトップに Wireshark.iso として用意しているものを適時利用して構わない。なおパケットキャプチャを利用しなくても解決は可能となっている。

Debian に関しても、ISO イメージを管理用 PC のデスクトップに用意しているので、適時使用して構わない。

【ネットワークの構成】


skills.local
Internet
CORE
ws01
ws02
HQSW01
HQRTR01
HQRTR02
Campus
CORERTR01
BORDERRTR01
ISP
partner01
DCRTR01
lnx01
dc01
lnx02
lnx03
Datacenter

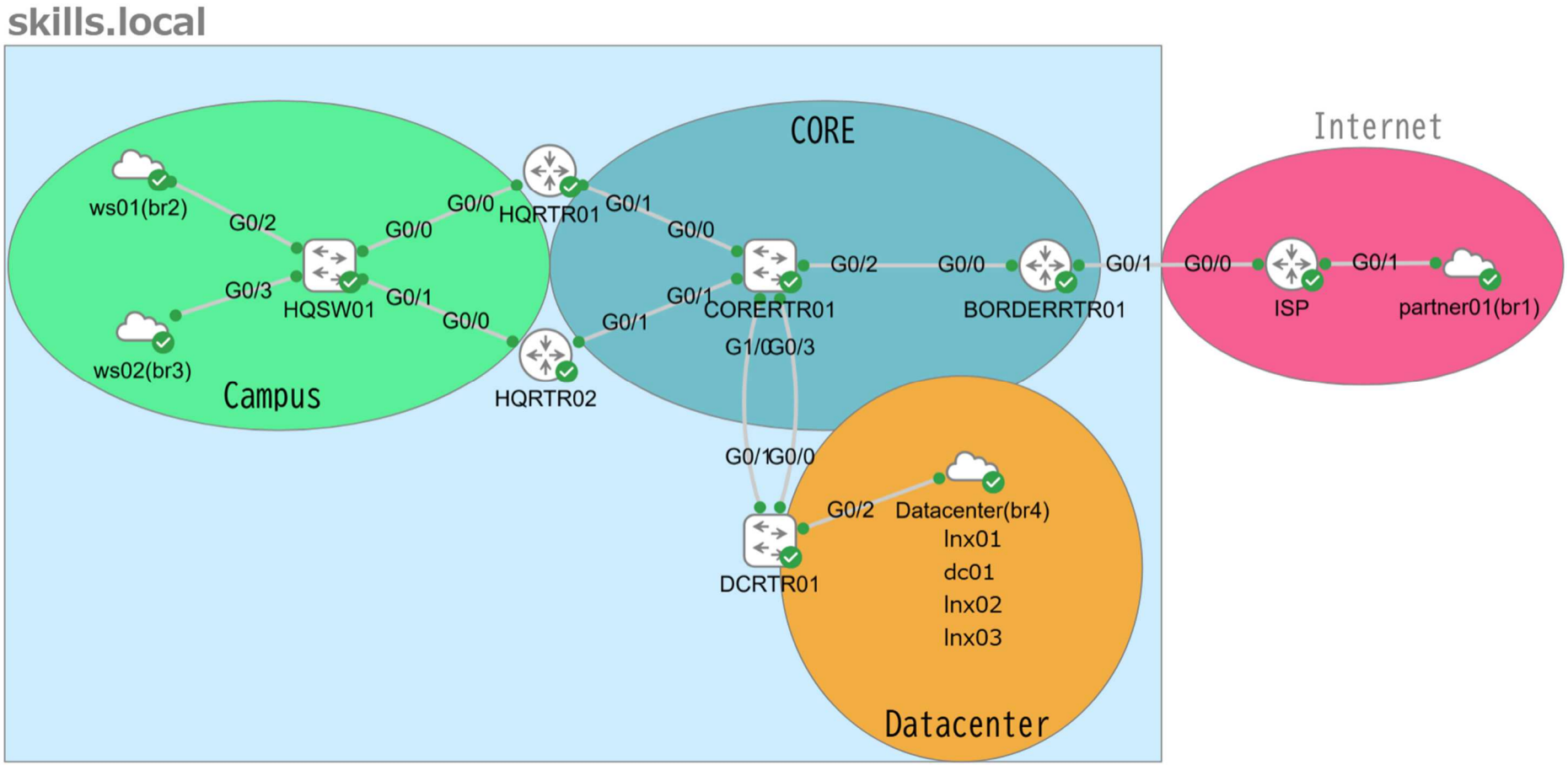
【ネットワークの情報】

ホスト	IP アドレス	OS	認証情報	サービス
dc01	10.1.64.20/24	Windows Server2022	administrator 他 AD ユーザ	AD DS, File Sharing, DNS(skills.local)
lnx01	10.1.64.10/24	Debian12.5 (CUI)	root use	Web, DHCP, DNS(skills.net)
lnx02	10.1.64.11/24	Debian12.5 (CUI)	root user	Web
lnx03	10.1.64.12/24	Debian12.5 (CUI)	root user	Web, Web Proxy
ws01	DHCP	Windows10	user(local)	
ws02	DHCP	Debian12.5 (GUI)	root user	
HQSW01	VLAN150:10.1.128.10/23	Cisco IOS		
HQRTR01	Lo0:10.254.1.11/32 Gi0/0.100:10.1.0.2/23 Gi0/0.150:10.1.128.2/23 Gi0/1:10.254.254.0/31	Cisco IOS		
HQRTR02	Lo0:10.254.1.12/32 Gi0/0.100:10.1.0.3/23 Gi0/0.150:10.1.128.3/23 Gi0/1:10.254.254.2/31	Cisco IOS		
CORERTR01	Lo0:10.254.1.10/32 Gi0/0:10.254.254/31 Gi0/1:10.254.254.3/31 Gi0/2:10.254.254.7/31 Po1:10.254.254.5/31	Cisco IOS	root user	
DCRTR01	Lo0:10.254.1.13/32 Po1:10.254.254.4/31 VLAN200:10.1.64.1/24	Cisco IOS	root user	
BORDERRTR01	Lo0:10.254.1.14/32 Gi0/0:10.254.254.6/31 Gi0/1:20.20.1.193/31	Cisco IOS		
ISP	様々な IP アドレス	Cisco IOS		
partner01	31.22.11.32/24	Debian12.5 (GUI)	root user	Web, DNS(sky-expo.aichi)

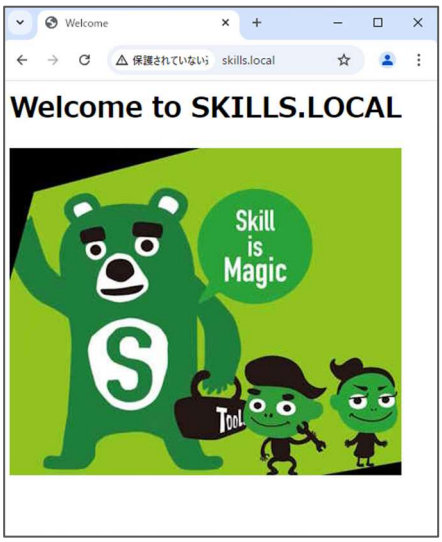
※パスワードはすべて「Skills2024」

※DNS の()内のドメイン名は、そのドメインのマスターサーバ

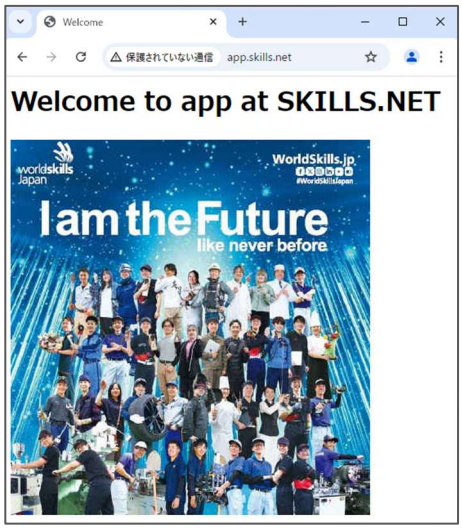
【競技環境の CML^2 の構成】



【競技環境の Web ページ】

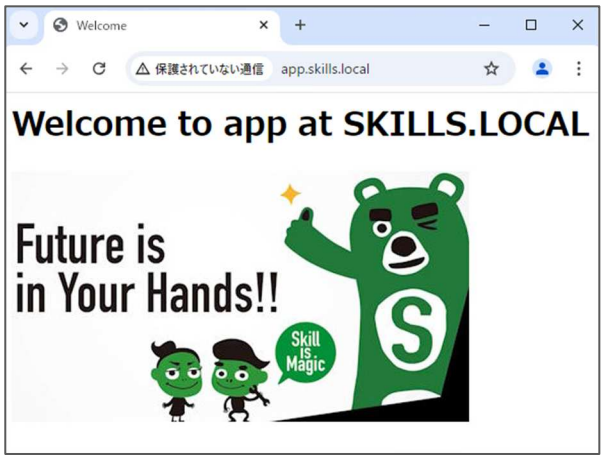


http://www.skills.local

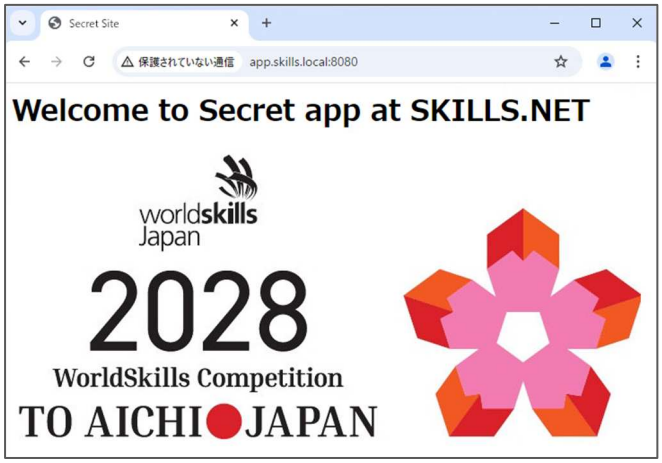


http://app.skills.net

http://www.skills.net



http://app.skills.local



http://app.skills.local:8080

http://www.sky-expo.aichi

第 62 回 技能五輪全国大会

IT ネットワークシステム管理

1 日目 課題 1 トラブルシューティング課題

競技チケット

令和 6 年 11 月 23 日(土)

競技時間：2 時間（9：00～11：00）

・各チケットの内容は、UVdesk ヘルプシステム上からも閲覧できる。
・本冊子は各自持ち帰りしても構わない。

トラブルシュート　チケット 1

こんにちは、学生の柴田と申します。ws01 に自分のアカウント「shibata」ログインしたのですが、ドキュメントフォルダにファイルが書き込めません。また、今日中に「X:¥学生用¥レポート提出」にレポートを提出するように大野教授に言われているのですが、X ドライブが表示されません。このままだと単位を落としてしまい非常に困っています。急いで直してもらえませんか？

【MEMO】

トラブルシュート　チケット 2

知多教授(アカウント:chita)からサポートに、「昨日は学会があり、午後 1 時 30 分に出勤して ws01 の電源を投入したが、ネットワークにうまく繋がらなかった。暫くしたら繋がったけど一応報告します」と連絡があった。その時間は HQRTR01 のファームウェアのアップデートをしていたが、その間 HQRTR02 が接続を引き継ぐはずなのだが、うまく動作しなかったようだ。
次も同じことが起きるとよくないので、原因を調査してください。

【MEMO】

トラブルシュート　チケット 3

おはようございます。購買部の五輪だけど、ws02 からパートナーさんの Web サイトを確認したいだけど、インターネットにアクセスできませんでした。
URL は http://www.sky-expo.aichi です。私のアカウント名は itsuwa です。
よろしくお願いします。

【MEMO】

トラブルシュート　チケット 4

パートナー企業の者です。いつも当社のサービスをご利用いただきありがとうございます。当社から、貴校が新たに公開した Web サイト http://app.skills.net の Web ページにアクセスできないようです。こちらの DNS サーバの設定は問題ないと思うのですが、確認していただけないでしょうか？

【MEMO】

トラブルシュート　チケット 5

先輩、俺やっちゃいました。lnx02 を操作していたのですが、root でログインできなくなっちゃいました。やっちゃいけないってわかっていたのに、面倒で passwd とか shadow ファイルとかを直接編集してしまいました。それが原因だと思います。他にも色々なファイルを編集したけど、混乱してよく覚えていません。俺、どうしたらいいかわからないです。本当にごめんなさい。先輩しか頼る人がいません、お願いです、どうか助けてください。

【MEMO】

トラブルシュート　チケット 6

お疲れ様。今、新しい Web システムを lnx03 で作成を進めていて、動作確認のため hosts ファイルにエントリを追加して、名前解決を上書きした。
だけど、コマンド「curl　-L　app.skills.net」を使用して、lnx03 にある app.skills.net を curl しようとすると、lnx01 ではなく、lnx03 のページをダウンロードして「Welcome to the NEW webpage of SKILLS.NET」のような文字が表示されるはずなのだが、うまくいかない。すまんが、ちょっと見てもらっていいかなぁ？

【MEMO】

トラブルシュート　チケット 7

サポートの皆様、いつも有難うございます。教授の大野だが、キャンパス構内から ping で 8.8.8.8 に疎通が通らないです。インターネットへのアクセス確認に使いたいので、8.8.8.8 だけでいいので疎通を通るようにしてください。よろしく頼みます。

【MEMO】

第 62 回 技能五輪全国大会
IT ネットワークシステム管理
課題 2 クライアント・サーバ環境

2024 年 11 月 23 日（土） 12:00～16:00（4 時間）

目　次

競技に関する注意事項:

- ✓ 競技開始の合図まで本冊子を開かないこと。
- ✓ 携帯電話の電源はあらかじめ切っておくこと。
- ✓ 本課題冊子を綴じてある留め金は外さないこと。
- ✓ 競技が開始されたら、下欄の座席番号及び競技者氏名を記入すること。
- ✓ 各種マニュアルや印刷物、記憶媒体の持ち込みは一切認めない。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技課題の仕様を満たすならば、どのような設定を行っても構わない。課題中に設定する値や設定項目の指定がない場合は、競技者が自身で判断して仕様を満たす設定を行うこと。
- ✓ 競技課題に記述がない項目に関しては採点対象としない。
- ✓ 競技時間内に作業が終了した場合は、競技委員に申し出て退席許可を得ること。
- ✓ 競技終了の合図で、直ちに作業を終了すること。
- ✓ 本課題冊子及び別紙は持ち帰り厳禁である。机上に置いたまま退席すること。

座席番号	競技者氏名

競技課題の背景と概要

あなたはサーバやネットワークを構築・運用管理する IT 企業に勤務している。今回、ある企業のネットワークシステムの更改業務を受注し、あなたがそのプロジェクトに携わることになった。ネットワークの設計やサーバの構築内容は既に完成している。

構築するネットワークシステムは tokyo-skills.jp、osaka-skills.jp 及び aichi-skills.jp の 3 つのサイトで構成され、ルータ ISP を経由して「仮想インターネットエリア(Public Internet Network)」に接続されている(別紙図 1「ネットワーク構成図」参照)。

1. tokyo-skills.jp

・ファイアウォール tfw により DMZ ネットワークと Internal ネットワークが構成される。DMZ ネットワークにはサーバ tsv1 が、Internal ネットワークにはサーバ tsv2、tsv3 及びクライアント t-client が配置される。
・Internal ネットワークと DMZ ネットワークを内部ネットワークと呼ぶ。
・内部ネットワーク以外を外部ネットワークと呼ぶ。
・以下のノードは各項目が競技委員により設定済みである。

1.1. tsv1

・別紙表 2「各ノードの IP アドレス及びアカウント、パスワード」に示すインタフェースのアドレス設定、及び適切な経路の設定。
・以下のサービスが稼働している。

1.1.1. DNS サービス

・外部ネットワークからの正引き要求(tsv1.tokyo-skills.jp、www.tokyo-skills.jp、www-v6.tokyo-skills.jp、mail.tokyo-skills.jp)に応答する。
・MX レコードの問い合わせに mail.tokyo-skills.jp を返す。
・内部ネットワークに対しスレーブサーバとしてサービスを提供する。

1.1.2. Mail サービス

・tsv1 にユーザ bob が作成済みでありメールの送受信が可能である。なお、bob のパスワードは pass である。

A) SMTP

・smtp サーバが稼働しており、25 番ポートへの接続要求に応答する。
・通信は暗号化されない。
・ユーザ認証は行わない。

B) POP3

・pop3 サーバが稼働しており、110 番ポートへの接続要求に応答する。
・通信は暗号化されない。
・平文によるユーザ認証を行う。

1.1.3. Web サービス

・http://www.tokyo-skills.jp/の要求に、文字列 tokyo-skills.jp を返す。
・http://www-v6.tokyo-skills.jp/の要求に、文字列(v6) tokyo-skills.jp を返す。

1.1.4. Proxy サービス

・Proxy サーバが稼働しており、内部ネットワークのノードに対し 8080 番ポートへの接続要求に応答する。
・ユーザ認証は行わない。

2. aichi-skills.jp

・ファイアウォール afw により Internal ネットワークが構成される。Internal ネットワークにはサーバ asv1、asv2 及びクライアント a-client が配置される。
・Internal ネットワークを内部ネットワークと呼ぶ。
・内部ネットワーク以外を外部ネットワークと呼ぶ
・以下のノードは各項目が競技委員により設定済みである。

2.1. asv1

・別紙表 2「各ノードの IP アドレス及びアカウント、パスワード」に示すインタフェースのアドレス設定、及び適切なデフォルトルートの設定。
・以下のサービスが稼働している。

2.1.1. DNS サービス

・外部ネットワークからの正引き要求(asv1.aichi-skills.jp、www.aichi-skills.jp、mail.aichi-skills.jp)に応答する。
・外部ネットワークからの MX レコードの問い合わせに mail.aichi-skills.jp を返す。
・内部ネットワークに対しスレーブサーバとしてサービスを提供する。

2.1.2. Mail サービス

・asv1 にユーザ alice が作成済みでありメールの送受信が可能である。なお、alice のパスワードは pass である。

A) SMTP

・smtp サーバが稼働しており、25 番ポートへの接続要求に応答する。
・通信は暗号化されない。
・ユーザ認証は行わない。

B) POP3

・pop3 サーバが稼働しており、110 番ポートへの接続要求に応答する。
・通信は暗号化されない。
・平文によるユーザ認証を行う。

2.1.3. Web サービス

・http://www.aichi-skills.jp/の要求に、文字列 aichi-skills.jp を返す。

3. osaka-skills.jp

・ルータ R-Osk により DMZ ネットワークと Internal ネットワークが構成される。DMZ ネットワークにはサーバ osv1 及び osv2 が、Internal ネットワークにはサーバ osv3 及びクライアント o-client が配置される。
・Internal ネットワークと DMZ ネットワークを内部ネットワークと呼ぶ。
・内部ネットワーク以外を外部ネットワークと呼ぶ。
・以下のノードは各項目が競技委員により設定済みである。

3.1. R-Osk

・別紙表 1「ルータ接続、IP アドレス」に示すインタフェースのアドレス設定、及び適切なデフォルトルートの設定。
・osv1 と osv2 の IPv4 アドレスをそれぞれ 201.10.0.10 と 201.10.0.11 へ静的に変換する NAT 設定。
・アクセス制御は未設定である。

4. Public Internet Network

・sv.itnetsys.org(以降 sv)と ex-client が稼働している。

4.1. sv

sv では下記のサービスが稼働している。

4.1.1. DNS サービス

・正引き要求(sv.itnetsys.org、www.itnetsys.org)に応答する。
・MX レコード問い合わせに sv.itnetsys.org を返す。

4.1.2. Web サービス

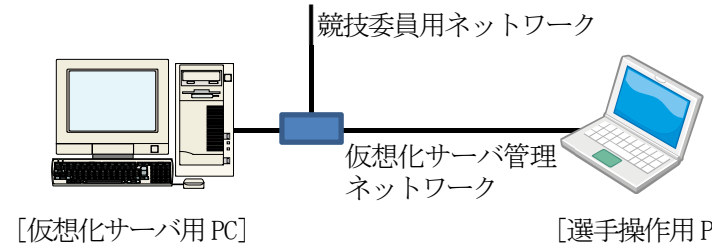
・http://www.itnetsys.org の要求に応答する。

4.1.3. SMTP サービス

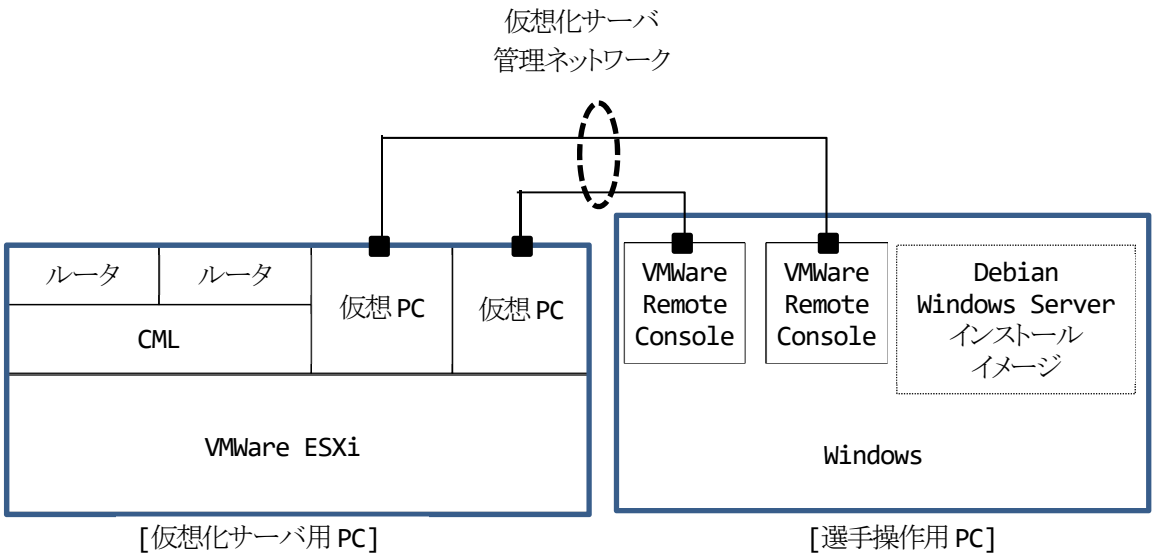
・manager@itnetsys.org 宛のメールを受信可能である。また、この受信メールに対して Subject「Auto Reply Mail」の空メールが自動返信される。

競技環境(仮想環境)に関する注意事項

競技で使用する PC 等の配置、役割は以下の通りである。



- [選手操作用 PC]には、競技に必要なネットワーク設定がされている。このネットワーク設定変更を禁止する。
- 「競技委員用ネットワーク」は競技委員が採点等で利用するネットワークであり、競技には使用しない。
- [仮想化サーバ用 PC]の直接操作を禁止する。



- [仮想化サーバ用 PC]の仮想 PC は VMWare Remote Console を用いて操作を行う。
- VMWare Remote Console のショートカットは、デスクトップの shortcut フォルダ内にある。このショートカットのプロパティ(リンク等)変更を禁止する。
- VMWare Remote Console において、CD/DVD ドライブ以外の設定変更を禁止する。
- すべての仮想 PC は競技開始時に電源 ON の状態である。
- すべての Windows 10 ノードでは Tera Term と Thunderbird のインストールプログラムを C:ドライブのルートディレクトリに置いてある。
- ローカル、リモートにかかわらず、VMWare ESXi の直接操作を禁止する。
- ルータ ISP、R-Osk の操作を禁止する。
- Debian のインストールイメージ debian-12.5.0-amd64-BD-1.iso 及び Windows Server 2022 のインストールイメージ SERVER_EVAL_x64FRE_ja-jp.iso は[選手操作用 PC]のデスクトップ ISO フォルダ内にある。これらは、VMware Remote Console のメニューにおいて「VMRC(V)」-「取り外し可能デバイス(R)」-「CD/DVD ドライブ 1」-「ディスクイメージファイル(iso)に接続(C)…」を選択しマウント可能である。

競技課題

・以降の設定項目を良く読み、各ノードの設定を行い顧客事業所のシステムを構築しなさい。
・設定項目は、ノード構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。
・採点対象ノードは tfw、tsv2、tsv3、t-client、afw、asv2、a-client、osv1、osv2、osv3、o-client 及び ex-client である。
・各ノードは別紙表 2 に記す OS がインストール済みである。
・選手自身の判断により採点対象ノードへ OS を再インストールすることは自由である。ただし、競技委員は再インストール作業に係る質問、トラブル等には一切対応しない。
・課題にある *user_name* は各ユーザ名を示す。例えば、ユーザ名が auser01 の場合/home/*user_name* は /home/auser01 を示す。

1. 基本設定

・別紙表 1、2 を参考に各ノードへ IPv4、IPv6 アドレス及び適切なゲートウェイを設定しなさい。
・指示がなくても競技課題の仕様から必要となるパッケージまたは機能を、各自の判断でインストール及び追加すること。

2. tokyo-skills.jp

2.1. tfw

2.1.1. サイト間 VPN

Internal ネットワークと aichi-skills.jp の Internal ネットワーク間で IPsec VPN を設定する。
・使用するパッケージは strongswan とする。
・鍵交換には IKEv2 を用いる。
・競技終了時に対向と接続済みであること。
・事前共有鍵認証方式を用い、SKYEXPO をパスフレーズとする。

2.1.2. NAT

・使用するパッケージは nftables とする。
・外部ネットワークと通信するために tsv1 の IPv4 アドレスを 201.10.0.2 へ静的に変換する。

2.1.3. パケットフィルタリング

・使用するパッケージは nftables とする。
・tsv1 から外部ネットワークへのトラフィックを許可する。
・tfw から外部ネットワークへのトラフィックを許可する。
・外部ネットワークから tsv1 への IPv4 トラフィック(http、smtp、DNS、ping)を許可する。
・外部ネットワークから tsv1 への IPv6 トラフィック(http、DNS、ping)を許可する。
・外部ネットワークから tfw への IPv4 トラフィック(ping)を許可する。
・外部ネットワークから tfw への IPv6 トラフィック(ping)を許可する。
・外部ネットワークへ発信したトラフィックの戻りトラフィックを許可する。
・Internal ネットワークから DMZ ネットワークへのトラフィックを許可する。
・DMZ ネットワークから Internal ネットワークへのトラフィックを許可する。
・IPsec VPN に係るトラフィックを許可する。
・上記以外は許可しない。

2.2. tsv2

2.2.1. Active Directory

tokyo-skills.jp のドメインコントローラを設定する。

・管理者パスワードを Skills2024 とする。
・tokyo-skills.jp ドメイン直下に組織単位 O_MKT 及び O_SALSE を作成する。
・O_MKT にグループ G_MKT を作成する。
・O_SALES にグループ G_SALES を作成する。
・O_MKT にユーザ tuser01～tuser05 を作成する。なお、パスワードは tPass2024 とする。
・O_SALES にユーザ tuser06～tuser10 を作成する。なお、パスワードは tPass2024 とする。
・tuser01～tuser05 を G_MKT のメンバとする。
・tuser06～tuser10 を G_SALES のメンバとする。
・tuser01～tuser10 のホームフォルダを¥¥tokyo-skills.jp¥Home¥*user_name* に設定し、Z:ドライブに割当てる。
・tuser01～tuser10 のプロファイルパスを¥¥tokyo-skills.jp¥Profiles¥*user_name* に設定し、移動ユーザプロファイルを有効にする。
・O_MKT に共有フォルダ Share_MKT を作成する。

2.2.2. グループポリシー

・O_MKT のユーザに対し、壁紙を wallpaper.png に設定する。wallpaper.png は tsv2 の C:ドライブ直下に保存されている。
・O_MKT のユーザに対し、共有フォルダ Share_MKT を Y:ドライブに割当てる。

2.2.3. DNS サーバ

・内部ネットワーク向けに tokyo-skills.jp 正引きゾーンのマスタサーバとしてサービスを提供する。
・MX レコードの問い合わせに tsv1 の正規名として mail.tokyo-skills.jp を返す。
・自身で名前解決が行えない場合は tsv1 へ問い合わせる。
・競技課題の仕様から必要となるレコードは各自の判断で追加すること。

2.2.4. DHCP サーバ

・Internal ネットワークに 192.168.101.201～220 の IPv4 アドレスを配布する。
・DNS サーバとして tsv2 及び tsv3 のアドレスを通知する。
・デフォルトゲートウェイのアドレスを通知する。
・tsv3 とホットスタンバイモードでフェールオーバーを構成する。

2.2.5. DFS(Distributed File System)

・¥¥tsv2.tokyo-skills.jp¥Home と ¥¥tsv3.tokyo-skills.jp¥Home から名前空間 ¥¥tokyo-skills.jp¥Home を作成する。
・¥¥tsv2.tokyo-skills.jp¥Profiles と¥¥tsv3.tokyo-skills.jp¥Profiles から名前空間¥¥tokyo-skills.jp¥Profiles を作成する。
・¥¥tsv2.tokyo-skills.jp¥Home と¥¥tsv3.tokyo-skills.jp¥Home のレプリケーションを設定する。
・¥¥tsv2.tokyo-skills.jp¥Profiles と¥¥tsv3.tokyo-skills.jp¥Profiles のレプリケーションを設定する。

2.3. tsv3

2.3.1. Active Directory

tokyo-skills.jp に追加のドメインコントローラを設定する。

2.3.2. DHCP サーバ

tsv2 とホットスタンバイモードでフェールオーバーを構成する。

2.4. t-client

2.4.1. OS の設定

・Active Directory のメンバとなっていること。
・競技終了時に Active Directory ユーザ tuser03 がログインした状態とする。
・DHCP サーバから IPv4 アドレスの割り当てを受ける。

2.4.2. Web ブラウザ(Microsoft Edge)

・Proxy の設定を行い http://www.itnetsys.org/のサイトが閲覧可能であること。

3. aichi-skills.jp

3.1. afw

3.1.1. サイト間 VPN

・Internal ネットワークと tokyo-skills.jp の Internal ネットワーク間で IPsec VPN を設定する。
・鍵交換には IKEv2 を用いる。
・常時接続の設定とし、競技終了時に対向と接続済みであること。
・事前共有鍵認証方式を用い、SKYEXPO をパスフレーズとする。

3.1.2. NAT

・外部ネットワークと通信するために Internal ネットワークにあるノードの IPv4 アドレスを 201.10.0.18 へ動的に変換する。
・外部ネットワークから 201.10.0.18 宛パケット(http、smtp、DNS)を asv1 へポートフォワードする。

3.2. asv2

3.2.1. Active Directory

・使用するパッケージは samba、krb5-user、winbind とする。
・aichi-skills.jp のドメインコントローラを設定する。
・管理者パスワードを Skills2024 とする。
ユーザ auser01～auser05 を作成する。パスワードは aPass2024 とする。
・¥¥asv2¥*user_name* を auser01～auser05 のホームフォルダに設定し、Z:ドライブに割当てる。
・¥¥asv2¥Profiles¥*user_name* を auser01～auser05 のプロファイルパスに設定し、移動ユーザプロファイルを有効にする。
・グループ G_Sales を作成する。
・ユーザ auser01 と auser02 を G_Sales のメンバとする。

3.2.2. DNS サーバ

・使用するパッケージは bind9 とする。
・samba と連携し Active Directory ドメインコントローラの DNS バックエンドとして機能する。
・MX レコードの問い合わせに mail.aichi-skills.jp を返す。
・自身で名前解決が行えない場合は asv1 へ問い合わせる。
・競技課題の仕様から必要となるレコードは各自の判断で追加すること。

3.2.3. DHCP サーバ

・使用するパッケージは isc-dhcp-server とする。
・内部ネットワークに 192.168.102.201～220 の IPv4 アドレスを配布する。
・DNS サーバとして asv2 のアドレスを通知する。
・デフォルトゲートウェイのアドレスを通知する。

3.3. a-client

3.3.1. OS の設定

・Active Directory のメンバとなっていること。
・競技終了時に Active Directory ユーザ auser03 がログインした状態とする。
・DHCP サーバから IPv4 アドレスの割り当てを受ける。

4. osaka-skills.jp

4.1. osv1

4.1.1. DNS サーバ

・osaka-skills.jp 正引きゾーンのマスタサーバとしてサービスを提供する。
・競技課題の仕様から必要となるレコードは各自の判断で追加すること。

A) 外部ネットワーク向けサービス

・www.osaka-skills.jp の正引き問合せに osv1 の IPv4 アドレスを応答する。
・www2.osaka-skills.jp の正引き問合せに osv2 の IPv4 アドレスを応答する。
・www-v6.osaka-skills.jp の正引き問合せに osv1 の IPv6 アドレスを応答する。
・www2-v6.osaka-skills.jp の正引き問合せに osv2 の IPv6 アドレスを応答する。
・MX レコードの問合せに mail.osaka-skills.jp を応答する。
・再起問合せを許可しない。

B) 内部ネットワーク向けサービス

・www.osaka-skills.jp の正引き問合せに IPv4 アドレス 10.2.0.1 を応答する。
・www2.osaka-skills.jp の正引き問合せに IPv4 アドレス 10.2.0.2 を応答する。
・osv3.osaka-skills.jp の正引き問合せに osv3 の IPv4 アドレスを応答する。
・MX レコードの問合せに mail.osaka-skills.jp を応答する。
・自身で名前解決が行えない場合は sv へ問い合わせる。

4.1.2. Web サーバ

・osv3 の発行するサーバ証明書利用する。
・https://www.osaka-skills.jp/の要求に対し、文字列 Osaka Skills LTD を返す。
・http://www-v6.osaka-skills.jp/の要求に対し、文字列(v6) Osaka Skills LTD を返す。

4.1.3. iSCSI ターゲット

・仮想ディスクサイズ 1GB の iSCSI ターゲットを構成する。

4.2. osv2

4.2.1. Web サーバ

・使用するパッケージは apache2 とする。
・osv3 の発行するサーバ証明書を利用する。
・HTTP 通信を HTTPS へリダイレクトする。
・https://www2.osaka-skills.jp/の要求に対し、文字列 www2.osaka-skills.jp site を返す。
・https://www2.osaka-skills.jp/auth/の要求に対しユーザ認証を行い、LDAP ユーザのみにアクセスを許可する。また、文字列 for LDAP users を返す。

4.2.2. メールサーバ

・osaka-skills.jpドメインのメールサーバを構築する。
・使用するパッケージは postfix、dovecot-pop3d とする。
・LDAP ユーザを用いて SMTP 認証を行う。
・LDAP ユーザを用いて POP3 認証を行う。
・LDAP ユーザ宛のメールをスプールする。
・osv3 が発行するサーバ証明書を利用し、クライアントーサーバ間の smtp 及び pop3 通信は SSL/TLS で暗号化する。

4.2.3. Proxy サーバ

・使用するパッケージは squid とする。
・ポート番号 8080 でサービスを提供する。
・内部ネットワークのノードの LDAP ユーザのみにサービスを提供する。

4.2.4. iSCSI イニシエータ

・使用するパッケージは open-iscsi とする。
・iSCSI ターゲット(osv1)の仮想ディスクを/iscsi にマウントする。

4.3. osv3

4.3.1. 認証局

・競技課題の仕様から証明書の必要となるノードへ各自の判断でインストールすること。

A) ルート CA を構築する。
・CA のサブジェクト名(CN)を Skills Root CA とする。

B) 中間 CA を構築し、以下のサーバ証明書を発行する。
・CA のサブジェクト名(CN)を Osaka Skills Sub CA とする。
・サーバ証明書①:www.osaka-skills.jp
・サーバ証明書②:www2.osaka-skills.jp
・サーバ証明書③:mail.osaka-skills.jp

C) サーバ証明書のコピーを/opt/grading/ca ディレクトリへ、以下に示すファイル名で保存すること。
・ルート CA:ca.pem
・中間 CA:services.pem
・サーバ証明書①:web1.pem
・サーバ証明書②:web2.pem
・サーバ証明書③:mail.pem

4.3.2. DNS サーバ

・使用するパッケージは bind9 とする。
・内部ネットワークに対して osaka-skills.jp 正引きゾーンのスレーブサーバとしてサービスを提供する。
・自身で名前解決が行えない場合は osv1 へ問い合わせる。

4.3.3. LDAP サーバ

・使用するパッケージは slapd、ldap-utils とする。
・管理者パスワードを Skills2024 とする。
・5 個の LDAP ユーザ ouser01～ouser05 を登録する。パスワードは oPass2024 とする。
・LDAP ユーザのログインシェルを/bin/bash とする。
・LDAP ユーザのホームディレクトリを/home/*user_name* とする。

4.4. o-client

4.4.1. OS の設定

・競技終了時に LDAP ユーザ ouser03 がログインした状態とする。
・Linux システにムユーザ ouser01～ouser05 が存在しないこと。

4.4.2. メールクライアント

・Thunderbird に必要な設定を行い、LDAP ユーザ ouser03 でメールの送受信を可能とする。
・サーバ証明書のエラー例外がないこと。

5. Public Internet Network

5.1. ex-client

5.1.1. OS の設定

・競技終了時にローカルユーザ User がログインした状態とする。

5.1.2. Web ブラウザ(Microsoft Edge)

・http://www-v6.osaka-skills.jp/のサイトが閲覧可能であること。
・証明書エラーがなく、https://www.osaka-skills.jp/のサイトが閲覧可能であること。

5.1.3. グループポリシー

・対話型ログオンに、Ctrl+Alt+Delete を必要とする。
・対話型ログオン時に以下の画面を表示する。

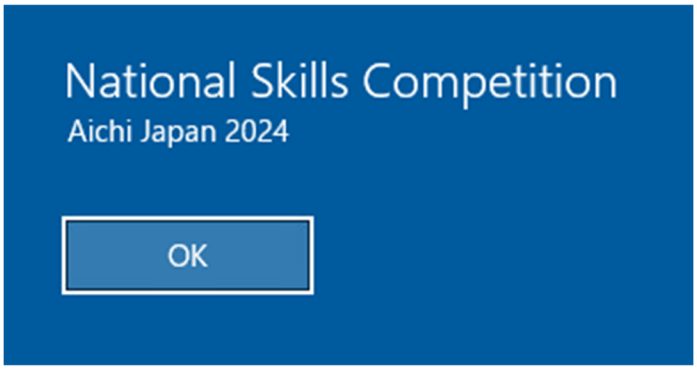


図1 ネットワーク構成図

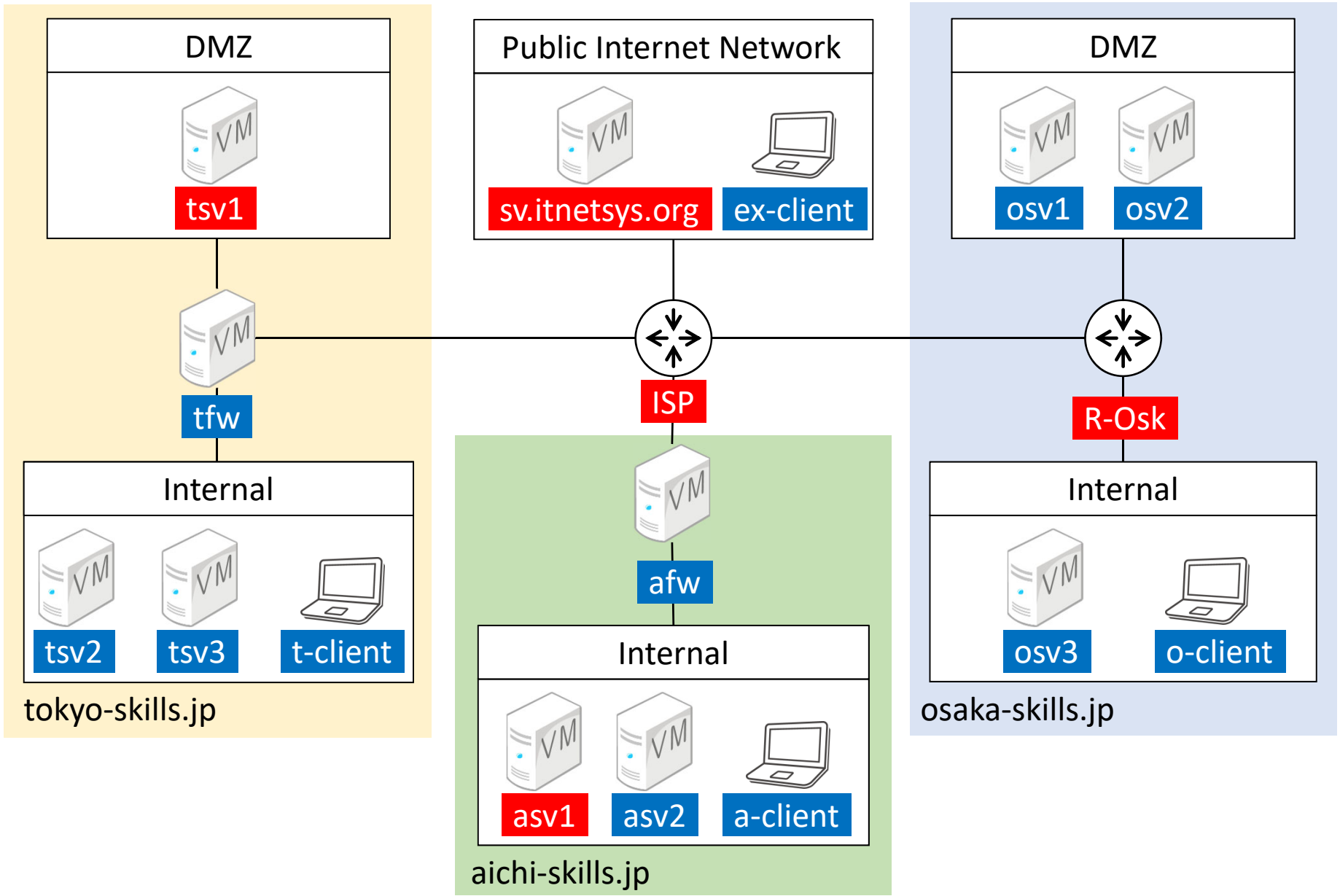


表1 ルータ接続，IPアドレス

ノード名	インタフェース	IPv4アドレス	IPv6アドレス	接続先
ISP	非公開	200.99.1.254/24	2001:DB8:1:1::FF/64	Public Internet
	非公開	201.10.0.6/29	2001:DB8:3:1::FF/64	tfw
	非公開	201.10.0.14/29	2001:DB8:2:1::FF/64	R-Osk
	非公開	201.10.0.22/29		afw
tfw	ens192	201.10.0.1/29	2001:DB8:3:1::1/64	ISP
	ens256	10.1.0.254/24	2001:DB8:3:2::FF/64	DMZ
	ens161	192.168.101.254/24		Internal
R-Osk	非公開	201.10.0.9/29	2001:DB8:2:1::1/64	ISP
	非公開	10.2.0.254/24	2001:DB8:2:2::FF/64	DMZ
	非公開	192.168.1.254/24		Internal
afw	Ethernet0	201.10.0.17/29		ISP
	Ethernet1	192.168.102.254/24		Internal

表2 各ノードのIPアドレス及びアカウント，パスワード

ノード名	OS	IPv4アドレス	IPv6アドレス	管理者アカウント	パスワード
sv	Debian Linux 12.5	200.99.1.1	2001:DB8:1:1::1	非公開	非公開
ex-client	Windows 10	200.99.1.101	2001:DB8:1:1::101	user	なし
tfw	Debian Linux 12.5	表1参照	表1参照	root	Skills2024
tsv1	Debian Linux 12.5	10.1.0.1	2001:DB8:3:2::1	非公開	非公開
tsv2	Windows Server 2022	192.168.101.1		administrator	Skills2024
tsv3	Windows Server 2022	192.168.101.2		administrator	Skills2024
t-client	Windows 10	DHCPで取得		user	なし
osv1	Windows Server 2022	10.2.0.1	2001:DB8:2:2::1	administrator	Skills2024
osv2	Debian Linux 12.5	10.2.0.2	2001:DB8:2:2::2	root	Skills2024
osv3	Debian Linux 12.5	192.168.1.1		root	Skills2024
o-client	Debian Linux 12.5	192.168.1.201		root	Skills2024
afw	Windows Server 2022	表1参照	表1参照	administrator	Skills2024
asv1	Debian Linux 12.5	192.168.102.1		非公開	非公開
asv2	Debian Linux 12.5	192.168.102.2		root	Skills2024
a-client	Windows 10	DHCPで取得		user	なし

※採点対象のDebian Linuxには、一般ユーザmaster(パスワードpass)が作成済みである

第 62 回　技能五輪全国大会
IT ネットワークシステム管理

競技課題 3 ネットワーキング環境

2024 年 11 月 24 日（日）
競技時間：3 時間（9:00～12:00）

競技に関する注意事項：

- ✓ 競技開始の合図まで本冊子を開かないこと。
- ✓ 携帯電話の電源はあらかじめ切っておくこと。
- ✓ 本課題冊子を綴じてある留め金は外さないこと。
- ✓ 競技が開始されたら、下欄の座席番号および競技者氏名を記入すること。
- ✓ 各種マニュアルや印刷物、記憶媒体の持ち込みは一切認めない。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技時間内に作業が終了した場合、CML シミュレーションおよび各仮想マシンは起動したままの状態とし、競技委員に申し出て退席許可を得ること。
- ✓ 競技終了の合図で、直ちに作業を終了すること。
- ✓ 本課題冊子は持ち帰り厳禁である。机上に置いたまま退席すること。

座席番号	競技者氏名

1　競技課題に関する注意事項

- ✓ 競技終了時に指定された設定が各ネットワークノードに保存されていること。
- ✓ ESXi ホストの管理画面に接続することは許可しない。
- ✓ CML の web インターフェースへ接続することは許可しない。
- ✓ 競技課題文書はシステム構築のための手順書ではないことに注意する必要がある。課題中に設定する値や設定項目に関する具体的な指定がない場合は、競技者が自身で判断して仕様を満たす設定を行う必要がある。
- ✓ ネットワーク技術は階層的に規定されている。多くの場合、個々の技術は基盤となる他の技術上で実行することを前提としている。あなたがそのような技術階層の途中で課題の指示通りの解決策を考えつくことができなかったとしても、それは残りの課題が全く採点されないというわけではないことを理解することが重要である。例えば、課題の指示通りの動的ルーティングを設定することができなくても、スタティックルートを使用することによって、その上で実行される全てのものの作業を継続することができる。また、VPN について課題の指示通りの構成を設定することができなくても、代替となるよりシンプルなトンネル接続を採用することができる。この場合、課題の要求を満たせなかった部分に対する得点は与えられないが、その基盤技術の上で実行される上位階層技術の機能テストに成功すれば、その部分に対する得点は与えられる。

1　競技課題の背景

あなたはネットワークシステムの構築を専門とする企業のエンジニアである。ある企業のネットワークシステムの更改業務を受注し、そのプロジェクトリーダーとなった。ネットワークの設計は既に完成している。これをもとに検証用のネットワーキング環境を構築する。

1.1. 構築ネットワークの概要

図１に示すように、構築対象となるネットワークには HeadQuarter/Branch1/Branch2 の各拠点があり、それらがインターネットに接続している。検証用のインターネットゾーンは isp1/isp2/isp3/is/isp1-ipv6sv/isp2-ipv4sv にて構成されており、以下、単にインターネットと記述した場合はこのゾーンを指すものとする。HeadQuarter には hq-sv3/hq-cl が接続するセグメントと hq-sv1/hq-sv2 が接続する公開サーバ―セグメント(DMZ)がある。Branch1/Branch2 にはそれぞれクライアントセグメントがある。HeadQuarter/Branch1/Branch2 の拠点内セグメント同士は DMVPN によって接続する。詳細については、以降の本文および別添ネットワーク構成図表に示す。

競技における設定対象は、各拠点のネットワークノードおよび is である。isp1/isp2/isp3 及び各端末(LinuxVM)は設定済みであり設定変更は許可しない。

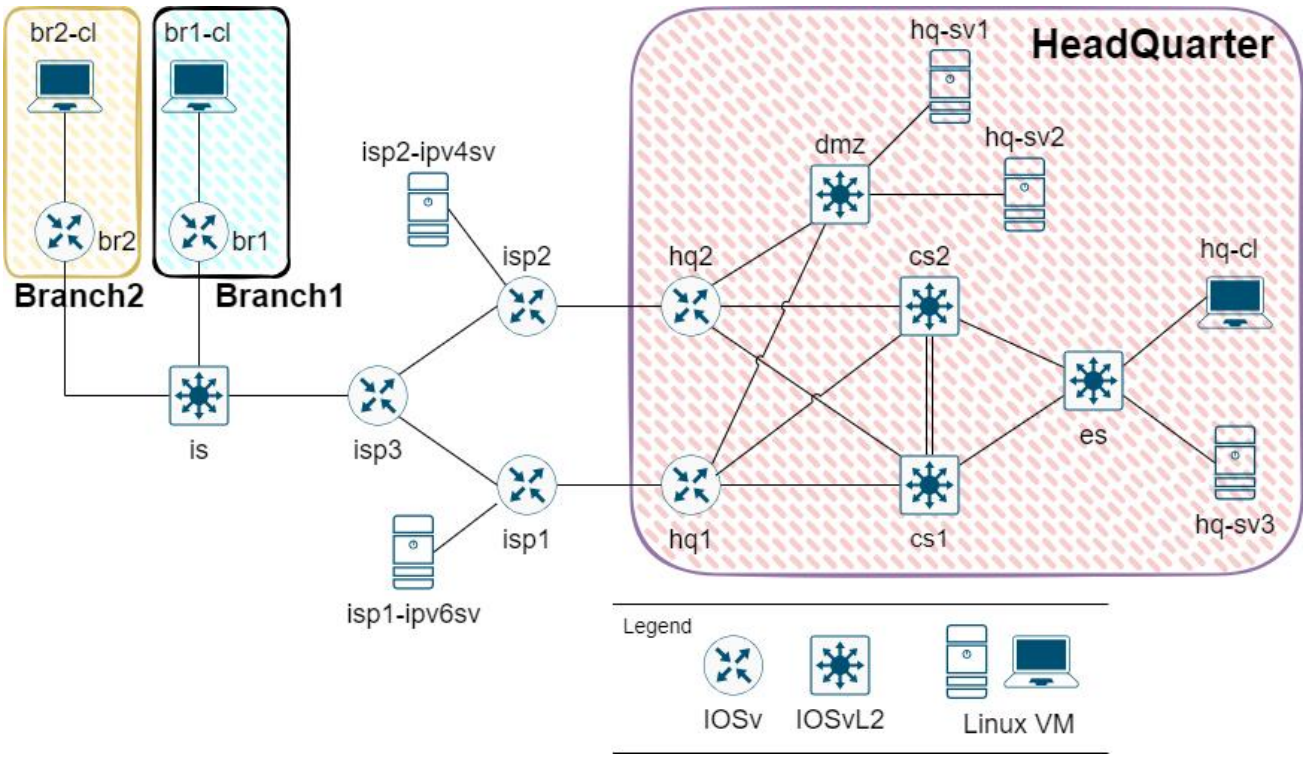


図１　ネットワークサイト構成

２ 仮想マシンに関する基本情報

2.1. isp1-ipv6sv/isp2-ipv4sv/hq-sv1/hq-sv2/hq-sv3/hq-cl/br1-cl/br2-cl について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Debian12.5 がインストールされており**アドレス設定済み**である。全ての端末に標準システムユーティリティ、SSH サーバー、curl、nmap がインストールされている。デスクトップ環境はインストールされていない。サーバー端末(～sv～)上では DNS、Web、SMTP、POP の各サービスが稼働している（ただしポートオープンのみ)。動作確認のための**一般ユーザアカウントでのログインは許可する。管理者アカウントでのログインおよび設定変更は許可しない。**

共通設定

一般ユーザアカウント名	master
一般ユーザのパスワード	p@ss

３ 各ノードへの接続方法

3.1. 各仮想マシン端末への接続について

各仮想マシン端末に接続するための vmrc ショートカットは、管理用 PC デスクトップ上のフォルダ shortcuts 内のフォルダ VM にある。端末名と同名のショートカットアイコンをダブルクリックしてアクセス可能である。

3.2. 各ネットワークノードへの接続について

各ネットワークノードのコンソールにアクセスするための Teraterm ショートカットは、管理用 PC デスクトップ上のフォルダ shortcuts 内のフォルダ NET にある。ノード名と同名のショートカットアイコンをダブルクリックし、ターミナル起動後、「Enter」キーを押すことで応答する。

※ダブルクリックしたショートカットアイコン名と、起動したコンソール画面のプロンプトに表示されるホスト名が一致していることを確認すること。一致していない場合は競技委員へ申し出ること。

3.3. isp1/isp2/isp3（設定済みルータノード）への接続について

動作確認のための非特権モードでのアクセスは許可する。

特権モードでのアクセス、設定変更は許可しない。

４ Cisco ネットワークノード設定課題

別添ネットワーク構成図表および以降の設定項目に従い、
ネットワークノード（hq1/hq2/dmz/cs1/cs2/es/is/br1/br2）を設定し、別添ネットワーク構成図表・表１に示す所定の IP 到達性を確保しなさい。設定項目は、ネットワーク構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。また、設定項目として明記されていなくても、競技課題の仕様上必要ならば、各自の判断で設定追加すること。

4.1 基本設定

以下の通り基本設定を行いなさい。

1. 別添ネットワーク構成図表・表２に IPv4 アドレス表、表３に IPv6 アドレス表、図２にインターフェース接続構成を示す。ネットワークノードの各インターフェースに IP アドレスを設定しなさい。

2. isp3 は DHCP サーバーとして設定済みであり、アドレス帯として 130.130.130.0/24、デフォルトルートとして 130.130.130.254 を配布している。br1 及び br2 は、Gi0/0 のアドレスとデフォルトルートを isp3 の DHCP サーバーから取得すること。
   ※留意点：この設定が不可能な場合でも、静的に設定することで課題を継続できる。

3. br2 について、特権モードパスワードを br2epass とする。
   ※その他のネットワークノードについてはパスワードを設定しないこと。

4. br2 について、ドメイン名を skills.it.jp とする。

5. br2 にてローカルユーザを登録する。ユーザ名は admin とし、パスワードは aichi123 とする。

6. 上記 3,5 で設定したパスワードは暗号化されること。

7. br2 への SSH(バージョン 2)での接続を許可する。上記 5 で登録したユーザ/パスワードを使用して認証できること。

4.2 アドレス変換

以下の通りアドレス変換設定を行いなさい。

1. Branch1 拠点内セグメント(10.1.0.0/24)からのインターネットゾーンとの接続について、br1 にて NAPT(PAT)を適用する。外側のインターフェースのアドレスに変換されること。

2. Branch2 拠点内セグメント(10.2.0.0/24)からのインターネットゾーンとの接続について、br2 にて NAPT(PAT)を適用する。外側のインターフェースのアドレスに変換されること。

3. HeadQuarter 拠点内セグメント(17.17.0.0/16)からのインターネットゾーンとの接続について、hq1 にて NAPT(PAT)を適用する。変換先アドレスとして 100.100.100.18 と 100.100.100.19 を使用する。

4. HeadQuarter 拠点内セグメント(17.17.0.0/16)からのインターネットゾーンとの接続について、hq2 にて NAPT(PAT)を適用する。外側のインターフェースのアドレスに変換されること。

5. hq-sv1 をインターネットと相互接続可能とするために、hq1/hq2 にてスタティック NAT を適用する。インターネット側から 100.100.100.1 にて接続が行えるようにすること。

6. hq-sv2 をインターネットと相互接続可能とするために、hq1/hq2 にてスタティック NAT を適用する。インターネット側から 200.200.200.1 にて接続が行えるようにすること。

4.3 スイッチング

以下の通り各種スイッチ設定を行いなさい。

1. cs1/cs2/es の VTP モードはトランスペアレントとする。

2. dmz/cs1/c2/es における各 VLAN について、別添ネットワーク構成図表・表４の通り設定する。

3. cs1/cs2 間のリンクについて、Etherchannel を以下の通り動作させる。
   A) Gi0/2 と Gi0/3 を Port-channel 1 として構成する。
   B) ネゴシエーションプロトコルを使用せずに静的に構成する。

4. 以下のリンクを IEEE802.1Q のトランクリンクとして構成する。
   A) cs1/cs2 間
   B) cs1/es 間
   C) cs2/es 間
   D) dmz/hq1 間
   E) dmz/hq2 間

5. cs1/cs2/es における STP について、次の通り設定する。
   A) 各スイッチにおいて、IEEE802.1w(RSTP)を有効にする。
   B) VLAN10 について、ルートブリッジを cs1 とし、セカンダリルートブリッジを cs2 とする。
   C) VLAN11 について、ルートブリッジを cs2 とし、セカンダリルートブリッジを cs1 とする。

6. is にて DHCP スヌーピングを以下の通り動作させる。
   A) VLAN 1 にて DHCP スヌーピングを有効にする。
   B) DHCP Option82 フィールドの挿入を無効にすること。
   C) isp3 が正規の DHCP サーバーとなるように Gi0/0 を信頼ポートとする。
   D) br1/br2 との接続ポート(Gi0/1, Gi0/2)について、DHCP パケットの受信を１秒当たり 10 パケットに制限する。

4.4 フェイルオーバー

以下の通りゲートウェイ冗長化を構成しなさい。

1. VLAN100 において、VRRP を次の通り動作させる。
   A) hq1 をマスター、hq2 をバックアップとする。
   B) 仮想 IP アドレスは 172.17.100.254 を使用する。

2. VLAN10 において、HSRP を次の通り動作させる。
   A) cs1 をアクティブ、cs2 をスタンバイとする。
   B) 仮想 IP アドレスは 172.17.10.254 を使用する。
   C) 切り戻しを有効にする。

3. VLAN11 において、HSRP を次の通り動作させる。
   A) cs1 をスタンバイ、cs2 をアクティブとする。
   B) 仮想 IP アドレスは 172.17.11.254 を使用する。
   C) 切り戻しを有効にする。

4. VLAN11 において、HSRP(IPv6 用)を次の通り動作させる。
   A) cs1 をスタンバイ、cs2 をアクティブとする。
   B) 仮想 IP アドレスは FE80::1 を使用する。
   C) 切り戻しを有効にする。

4.5　BGP ルーティング

別添ネットワーク構成図表・図３に BGP ルーティング概要を示す。以下の通り BGP を構成し、インターネットゾーン/HeadQuarter 拠点間の到達性を確保しなさい。isp1/ips2/isp3 については設定済みであり、それらの間の eBGP ピアは確立している。なお、isp1(AS100)は、hq1(AS300)に対してデフォルトルートと 100.99.0.0/16 の経路をアドバタイズする設定となっている。isp2(AS200)は、hq2(AS300)に対してデフォルトルートと 200.99.0.0/16 の経路をアドバタイズする設定となっている。

1. hq1/hq2 において、BGP を次の通り動作させる。
   A) AS 番号 300 として BGP を動作させる。
   B) keepalive メッセージの送信間隔を 10 秒、ホールドタイムを 30 秒とする。
   C) ピアに対して集約経路 100.100.100.0/27 及び 200.200.200.0/27 をアドバタイズする。集約前の経路についてはアドバタイズしない。
   D) hq1/hq2 間で iBGP ピアを確立する。ネイバーアドレスとして Loopback0 のプライマリアドレスを使用すること。
   E) hq1/hq2 の iBGP ピアについて、ネクストホップとして自身を指定すること。
   F) iBGP 経路の IGP への再配布を可能とすること。（EIGRP へ再配布するため）
   G) hq1/isp1 間で eBGP ピアを確立する。
   H) hq2/isp2 間で eBGP ピアを確立する。
   I) インターネット側(isp3)から 100.100.100.0/27 のアドレス帯へのアクセスについて、isp1(AS100)経由の経路が優先経路となるように経路制御すること。isp3 からの traceroute の例を以下に示す。

```
isp3>traceroute 100.100.100.1
Type escape sequence to abort.
Tracing the route to 100.100.100.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.99.2.5 [AS 100] 2 msec 1 msec 2 msec
  2 100.99.2.2 [AS 100] 3 msec 4 msec 4 msec
  3 100.100.100.1 [AS 300] 6 msec 7 msec 6 msec
```

   J) インターネット側(isp3)から 200.200.200.0/27 のアドレス帯へのアクセスについて、isp2(AS200)経由の経路が優先経路となるように経路制御すること。isp3 からの traceroute の例を以下に示す。

```
isp3>traceroute 200.200.200.1
Type escape sequence to abort.
Tracing the route to 200.200.200.1
VRF info: (vrf in name/id, vrf out name/id)
  1 200.99.2.5 [AS 200] 2 msec 1 msec 1 msec
  2 200.99.2.2 [AS 200] 2 msec 4 msec 1 msec
  3 200.200.200.1 [AS 300] 5 msec 3 msec 6 msec
```

   K) 上記 I)J)において、isp1 または isp2 側のいずれか一方に障害が発生した場合でも、残った経路に切り替わり通信を継続できること。（例えば、hq2 の Gi0/0 を shutdown した場合、J)の通信は isp1(AS100)経由の通信に切り替わること）

4.6　EIGRP(IPv4)ルーティング

別添ネットワーク構成図表・図４に EIGRP(IPv4)ルーティング概要を示す。以下の通り EIGRP を構成し、HeadQuarter 拠点の到達性を確保しなさい。

1. hq1/hq2/cs1/cs2 において、EIGRP(IPv4)を次の通り動作させる。
   A) 名前付きモードの仮想インスタンス名を A2024 とし、AS 番号を 100 とする。
   ※留意点：名前付きモードで設定できない場合はクラシックモードを使用することで課題を継続できる。
   B) 別添ネットワーク構成図表・図４の通り、hq1/hq2/cs1/cs2 間で隣接関係を確立し、hq1/hq2 の Loopback0、全ての/30 ネットワーク、VLAN10,11,100 のアドレスがアドバタイズされ、拠点内の到達性が確保されること。
   C) 端末接続セグメント(VLAN10,11,100)に対して、EIGRP パケットを送信しないこと。
   D) hq1 において、isp1 から受信した BGP 経路（デフォルトルート及び 100.99.0.0/16）を EIGRP へ再配布する。再配布時のメトリック調整について F)を参照のこと。
   E) hq2 において、isp2 から受信した BGP 経路（デフォルトルート及び 200.99.0.0/16）を EIGRP へ再配布する。再配布時のメトリック調整について F)を参照のこと。
   F) D)E)で再配布されるデフォルトルートについて、cs1/cs2 のルーティングテーブル上において hq1(→isp1)を経由するルートが優先となること。cs2 から isp3(130.130.130.254)への traceroute の例を以下に示す。

```
cs2#traceroute 130.130.130.254
Type escape sequence to abort.
Tracing the route to 130.130.130.254
VRF info: (vrf in name/id, vrf out name/id)
  1 172.17.0.5 1 msec 1 msec 2 msec
  2 100.99.2.1 3 msec 4 msec 5 msec
  3 100.99.2.6 3 msec *  4 msec
```

   ※ただし、200.99.0.0/16 のアドレス帯宛は hq2(→isp2)を経由するルートとなる。

   G) hq1(→isp1)の経路に障害が発生した場合でも、hq2(→isp2)を経由するルートがデフォルトルートのバックアップ経路となること。例えば、hq1 の Gi0/0 を shutdown した場合の cs2 から isp3(130.130.130.254)への traceroute の例を以下に示す。

```
cs2#traceroute 130.130.130.254
Type escape sequence to abort.
Tracing the route to 130.130.130.254
VRF info: (vrf in name/id, vrf out name/id)
  1 172.17.0.9 3 msec 2 msec 2 msec
  2 200.99.2.1 4 msec 4 msec 4 msec
  3 200.99.2.6 4 msec *  6 msec
```

   H) hq2 において、OSPF 経路を EIGRP へ再配布する。（OSPF は DMVPN で接続する拠点間ルーティングに使用する）

4.7　VPN

別添ネットワーク構成図表・図５に DMVPN 構成の概要を示す。DMVPN による拠点間接続を以下の通り動作させなさい。

1. hq2/br1/br2 間において、トンネルインターフェース Tunnel0 を次の通り動作させる。
   A) hq2 における Tunnel0 のトンネルソースは Loopback0 を使用する。
   B) hq2 をハブルータ、br1/br2 をスポークルータとする DMVPN を構成する。
   C) br1/br2 のスポーク間通信が発生した際は、ハブルータを経由しない直接経路が動的に確立すること。
   D) IKEv2/IPsec によってセキュリティを確保する。

※留意点：これらの指示通りのトンネル構成が不可能な場合であっても、あなたが設定可能なトンネル構成を採用することで拠点間の到達性を確保できるならば、トンネル上で動作する関連課題を継続できる。

4.8　OSPF ルーティング

別添ネットワーク構成図表・図６に OSPF ルーティング概要を示す。以下の通り OSPF を構成し、拠点間の到達性を確保しなさい。

1. hq2/br1/br2 において、OSPF を次の通り動作させる。
   A) DMVPN 上にて OSPF の経路交換を動作させる。
   B) hq2 が DR、br1/br2 が DROTHER となること。
   C) DMVPN(10.0.0.0/24)を Area 0、Branch1 拠点を Area 1、Branch2 拠点を Area 2 とする。
   D) hq2 は ASBR として、HeadOuarter 拠点の集約アドレス 172.17.0.0/16 のみを OSPF ネイバーへアドバタイズする。
   E) br1 は ABR として、Branch1 拠点の集約アドレス 10.1.0.0/16 をアドバタイズする。
   F) br2 は ABR として、Branch2 拠点の集約アドレス 10.2.0.0/16 をアドバタイズする。
   G) Branch1/Branch2 拠点内セグメントに対して OSPF パケットを送信しないこと。

4.9　IPv6 ルーティング

別添ネットワーク構成図表・表３に IPv6 アドレス表を示す。また、図７に EIGRP(IPv6)ルーティング概要を示す。以下の通り IPv6 ルーティングを構成し、IPv6 セグメント間の到達性を確保しなさい。

1. hq1 において、IPv6 のデフォルトルートを静的に設定しなさい。デフォルトルートは isp1 を指すものとする。

2. hq1/cs1/cs2 において、EIGRP(IPv6)を次の通り動作させる。
   A) 名前付きモードの仮想インスタンス名を A2024 とし、AS 番号を 100 とする。
   ※留意点：名前付きモードで設定できない場合はクラシックモードを使用することで課題を継続できる。
   B) 別添ネットワーク構成図表・図７の通り、hq1/cs1/cs2 間で隣接関係を確立する。
   C) hq1 は上記 1 で設定したデフォルトルートを EIGRP(IPv6)へ再配布する。
   D) hq1 の Gi0/0 で EIGRP(IPv6)を動作させないこと。
   E) VLAN11 に対して、EIGRP(IPv6)パケットを送信しないこと。

4.10　ファイアウォールセキュリティ

別添ネットワーク構成図表・表１に端末間の IP 到達性を示す。 br1 において以下の通りファイアウォール設定を行いなさい。

1. Branch1 拠点内(br1 の Gi0/1 側)からインターネットゾーン(br1 の Gi0/0 側)へのアクセスについて、ICMP と HTTPS(TCP443)のみ許可する。
   A) インターネットゾーンから Branch1 拠点内へのトラフィックについては、戻りの通信についてのみ動的に許可されること。
   B) トンネル経由の拠点間通信及び br1 自身の発着信については、阻害しないこと。

   ※留意点：この設定は ZBFW(Zone-Based Policy Firewall)での実施を想定しているが、あなたが設定可能ないずれかの方法を採用して構わない。

表２：IPv4アドレス表（赤字は設定済み）

ノード名	インターフェース	IPv4アドレス	隣接
isp1	Gi0/0	100.99.2.1/30	hq1
	Gi0/3	100.99.2.5/30	isp3
	Loopback0	100.99.1.1/24	
isp2	Gi0/0	200.99.2.1/30	hq2
	Gi0/1	200.99.1.254/24	isp2-ipv4sv
	Gi0/2	200.99.2.5/30	isp3
isp3	Gi0/0	130.130.130.254/24	is
	Gi0/1	100.99.2.6/30	isp1
	Gi0/2	200.99.2.6/30	isp2
hq1	Gi0/0	100.99.2.2/30	isp1
	Gi0/1	172.17.0.1/30	cs1
	Gi0/2.98	172.17.0.21/30	
	Gi0/2.100	172.17.100.254/24	
	Gi0/3	172.17.0.5/30	cs2
	Loopback0	100.100.100.11/32 200.200.200.11/32（セカンダリ）	
hq2	Gi0/0	200.99.2.2/30	isp2
	Gi0/1	172.17.0.9/30	cs2
	Gi0/2.98	172.17.0.22/30	
	Gi0/2.100	172.17.100.253/24	
	Gi0/3	172.17.0.13/30	cs1
	Loopback0	200.200.200.22/32 100.100.100.22/32（セカンダリ）	
	Tunnel0	10.0.0.1/24	
cs1	Gi0/0	172.17.0.2/30	hq1
	Gi1/0	172.17.0.14/30	hq2
	Vlan10	172.17.10.252/24	
	Vlan11	172.17.11.252/24	
	Vlan99	172.17.0.17/30	
cs2	Gi0/0	172.17.0.10/30	hq2
	Gi1/0	172.17.0.6/30	hq1
	Vlan10	172.17.10.253/24	
	Vlan11	172.17.11.253/24	
	Vlan99	172.17.0.18/30	
br1	Gi0/0	DHCPにて取得	is
	Gi0/1	10.1.0.254/24	br1-cl
	Tunnel0	10.0.0.2/24	
br2	Gi0/0	DHCPにて取得	is
	Gi0/1	10.2.0.254/24	br2-cl
	Tunnel0	10.0.0.3/24	
hq-sv1	ens192	172.17.100.1/24	dmz
hq-sv2	ens192	172.17.100.2/24	dmz
hq-sv3	ens192	172.17.10.1/24	es
hq-cl	ens192	172.17.11.1/24	es
br1-cl	ens192	10.1.0.1/24	br1
br2-cl	ens192	10.2.0.1/24	br2
isp2-ipv4sv	ens192	200.99.1.1/24	isp2

表３：IPv6アドレス表（赤字は設定済み）

ノード名	インターフェース	IPv6アドレス	隣接
isp1	Gi0/0	2001:DB8:ABCD:1::1/64	hq1
	Gi0/2	2001:DB8:CAFÉ::1/64	isp1-ipv6sv
hq1	Gi0/0	2001:DB8:ABCD:1::2/64	isp1
	Gi0/1	リンクローカルアドレス(自動生成)	cs1
	Gi0/3	リンクローカルアドレス(自動生成)	cs2
cs1	Gi0/0	リンクローカルアドレス(自動生成)	hq1
	Vlan11	2001:DB8:ABCD:11::C1/64	
		FE80::C1/64	
	Vlan99	リンクローカルアドレス(自動生成)	
cs2	Gi1/0	リンクローカルアドレス(自動生成)	hq1
	Vlan11	2001:DB8:ABCD:11::C2/64	
		FE80::C2/64	
	Vlan99	リンクローカルアドレス(自動生成)	
hq-cl	ens192	自動(RA)	es
isp1-ipv6sv	ens192	2001:DB8:CAFÉ::100/64	isp1

第62回　技能五輪全国大会
ITネットワークシステム管理
2日目　課題3

別添ネットワーク構成図表

表1：本課題で要求される各端末間のIP到達性

（1） IPv4到達性

要求側＼応答側	hq-sv1	hq-sv2	hq-sv3	hq-cl	br1-cl	br2-cl	isp2-ipv4sv
hq-sv1		○	○	○	○	○	○
hq-sv2	○		○	○	○	○	○
hq-sv3	○	○		○	○	○	○
hq-cl	○	○	○		○	○	○
br1-cl	○(172.17.100.1宛) ※(100.100.100.1宛)	○(172.17.100.2宛) ※(200.200.200.1宛)	○	○		○	ICMP, TCP443のみ可
br2-cl	○	○	○	○	○		○
isp2-ipv4sv	○(100.100.100.1宛)	○(200.200.200.1宛)	×	×	×	×	

○：要求側から応答側への到達性が確保され、正常に応答が返る。
×：要求側から応答側への通信は確立しない。
～のみ可：フィルタリングによって限定的な接続のみ可能とする。
※: 100.100.100.1，200.200.200.1宛ての場合はICMP，TCP443のみ可

（2） IPv6到達性

要求側＼応答側	hq-cl	isp1-ipv6sv
hq-cl		○
isp1-ipv6sv	○	

表4： VLAN設定表

各スイッチのVLAN設定は、次の通りである。

dmzのVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
98	HQ_P2P		172.17.0.20/30	hq1-hq2間ピア接続用
100	DMZ1	Gi0/2, Gi0/3	172.17.100.0/24	DMZセグメント

cs1/cs2のVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
10	SERVER		172.17.10.0/24	サーバーセグメント
11	CLIENT_1		172.17.11.0/24	クライアントセグメント
99	L3_P2P		172.17.0.16/30	cs1-cs2間ピア接続用

esのVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
10	SERVER	Gi0/2	172.17.10.0/24	サーバーセグメント
11	CLIENT_1	Gi0/3	172.17.11.0/24	クライアントセグメント

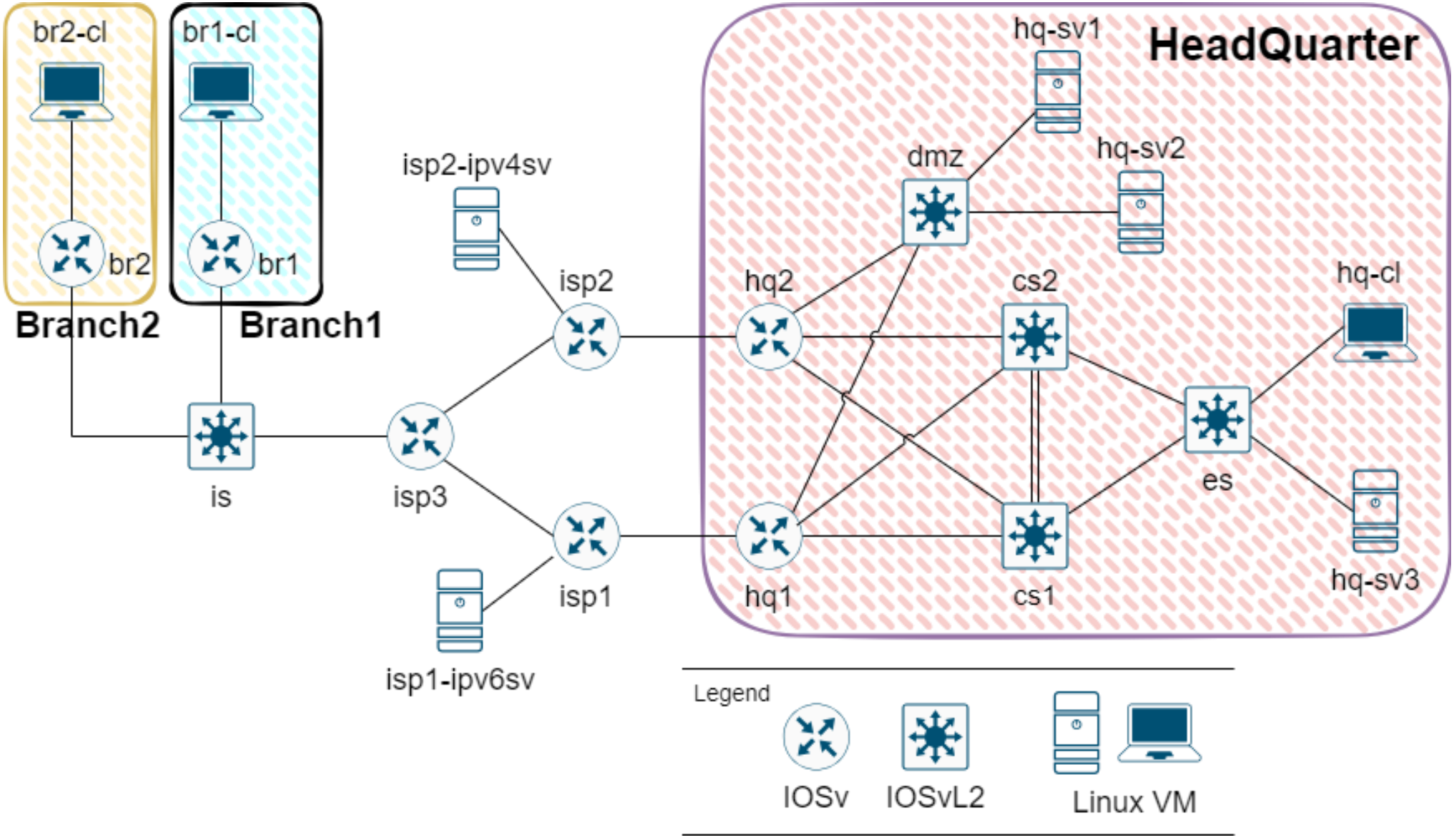
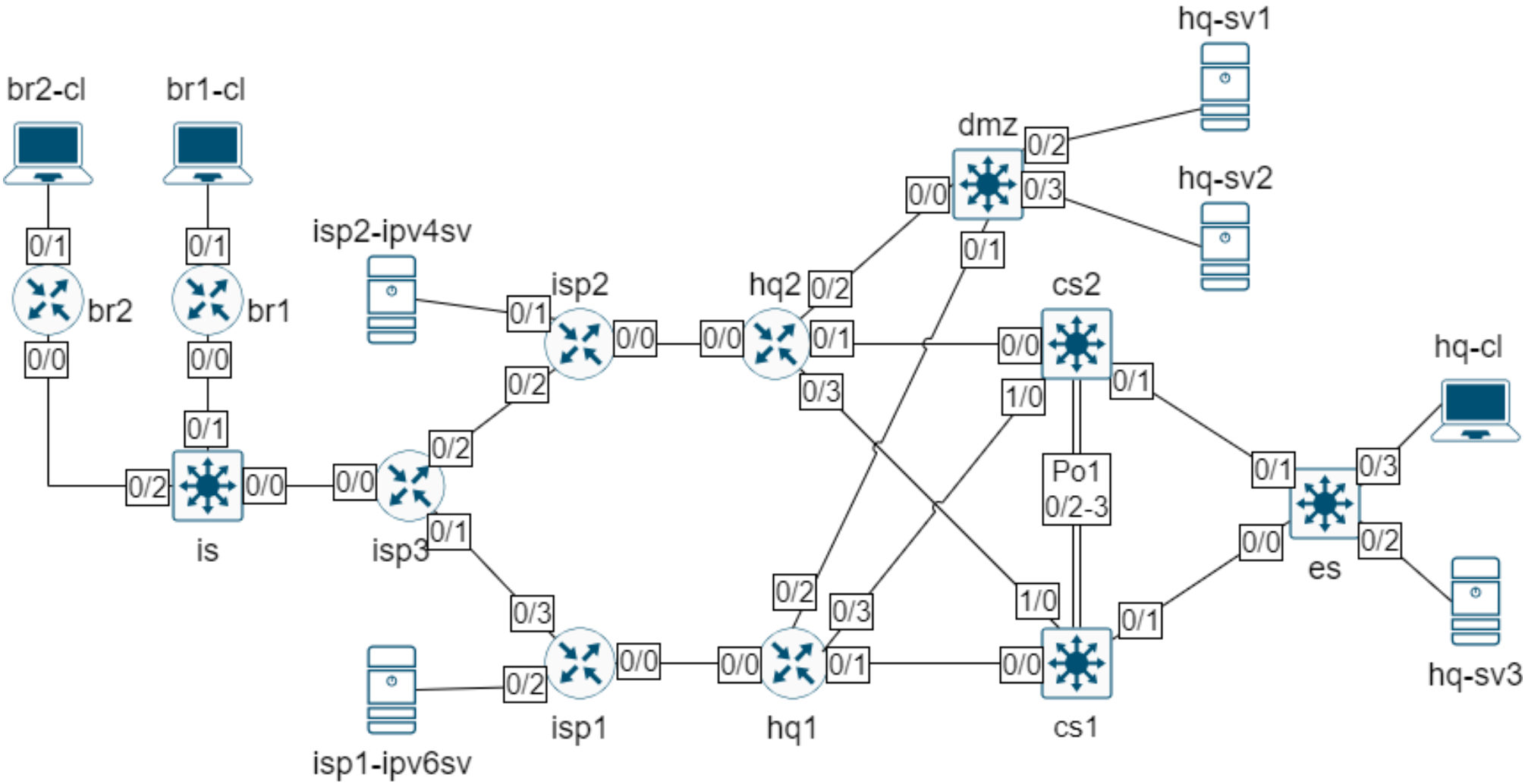


図1：ネットワークサイト構成



※本図に各ノードの接続インターフェース番号を示す。
使用インタフェースは全てGigabitEthernetである。
（0/0の表記は、GigabitEthernet0/0の略記）

図2：インターフェース接続構成

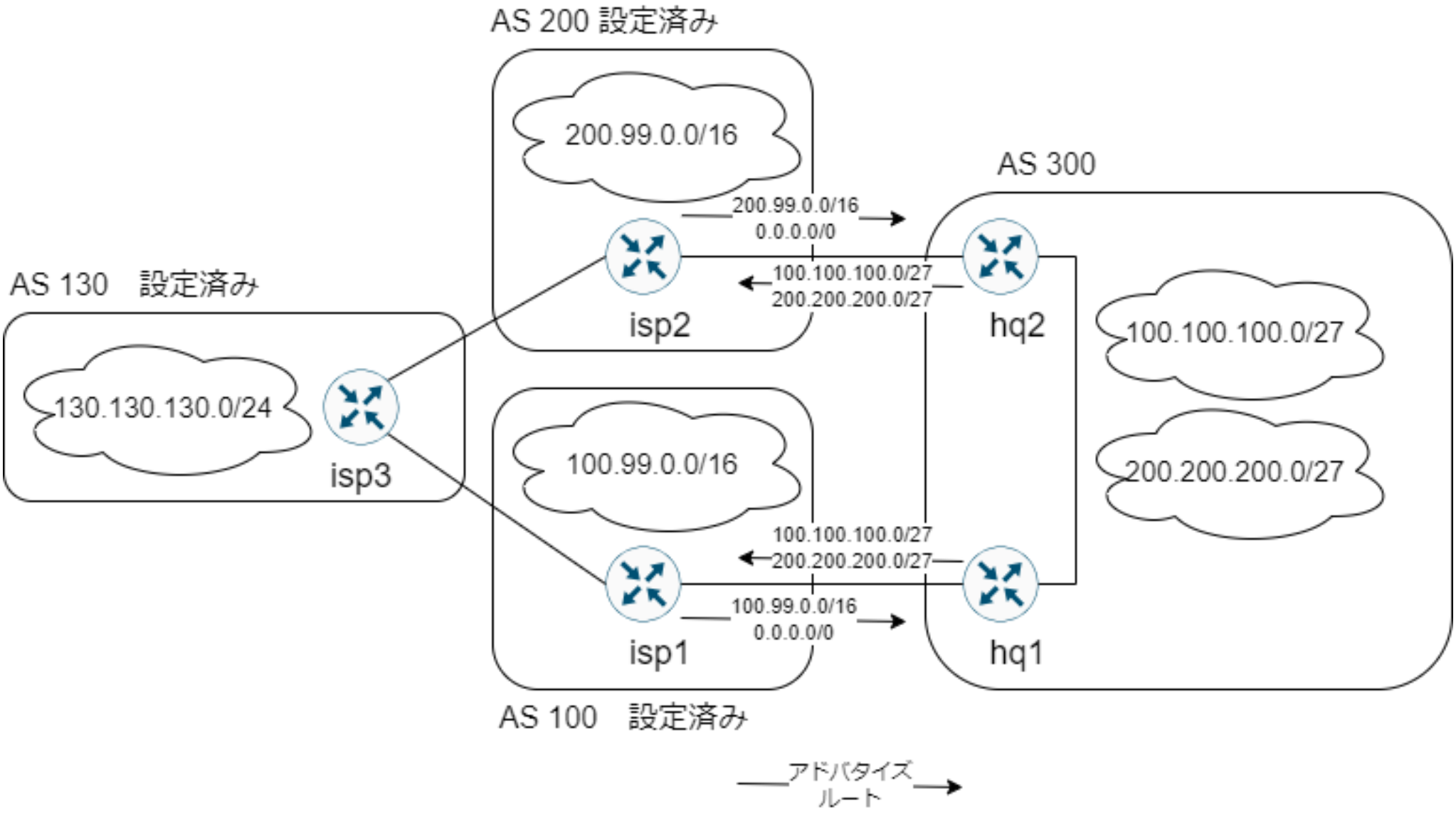


図3：BGPルーティング概要

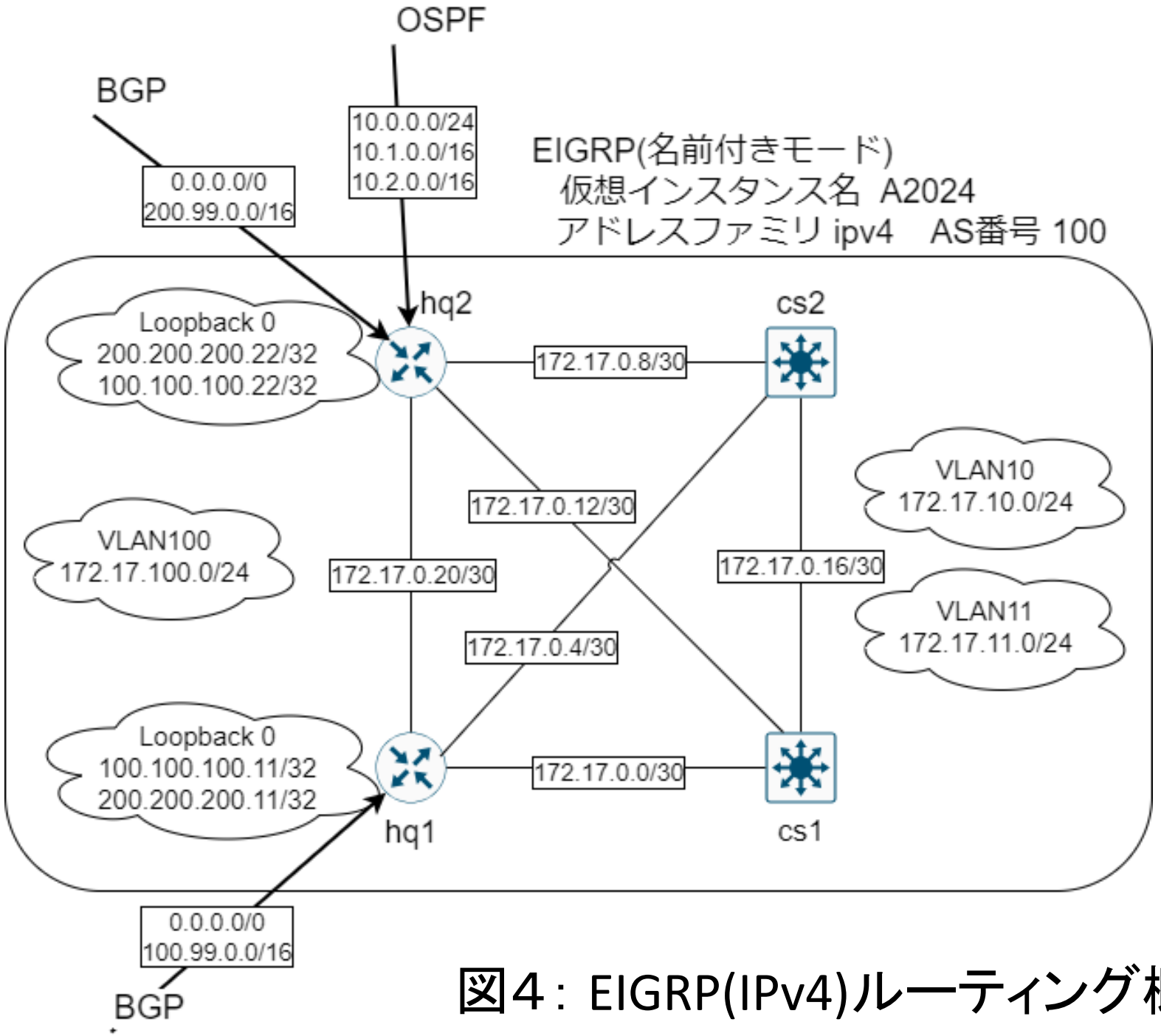


図4：EIGRP(IPv4)ルーティング概要

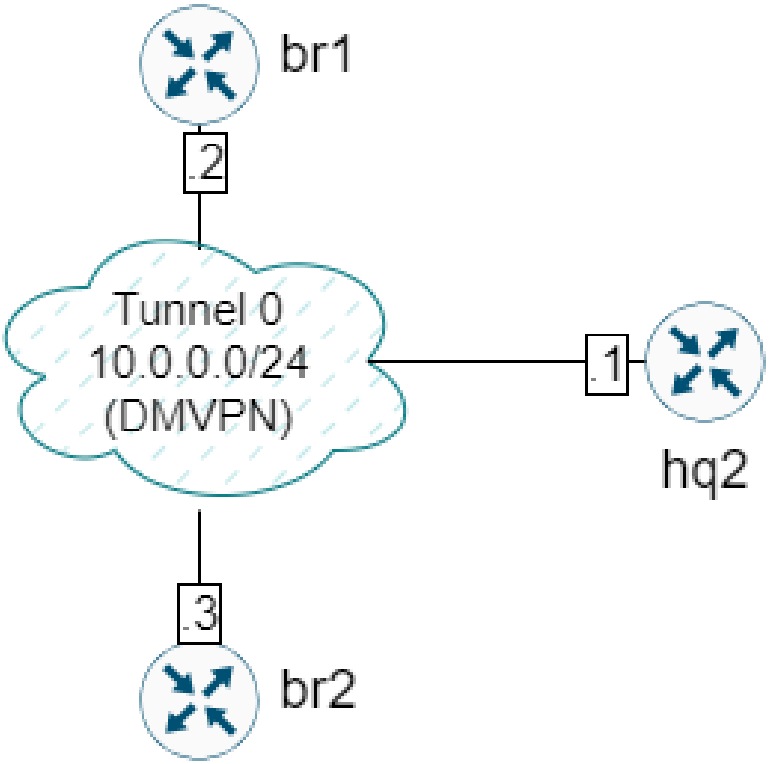


図５：DMVPN構成概要

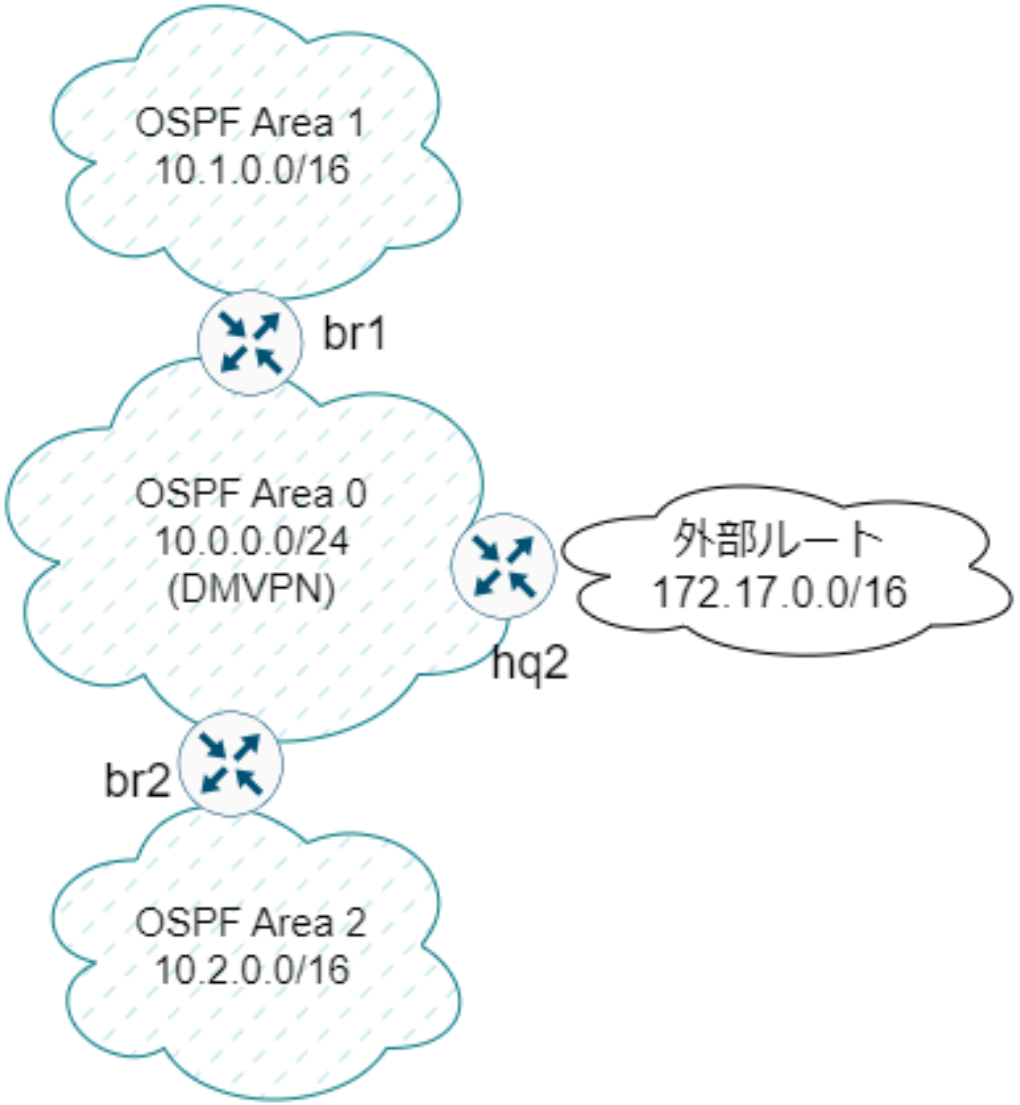


図６：OSPFルーティング概要

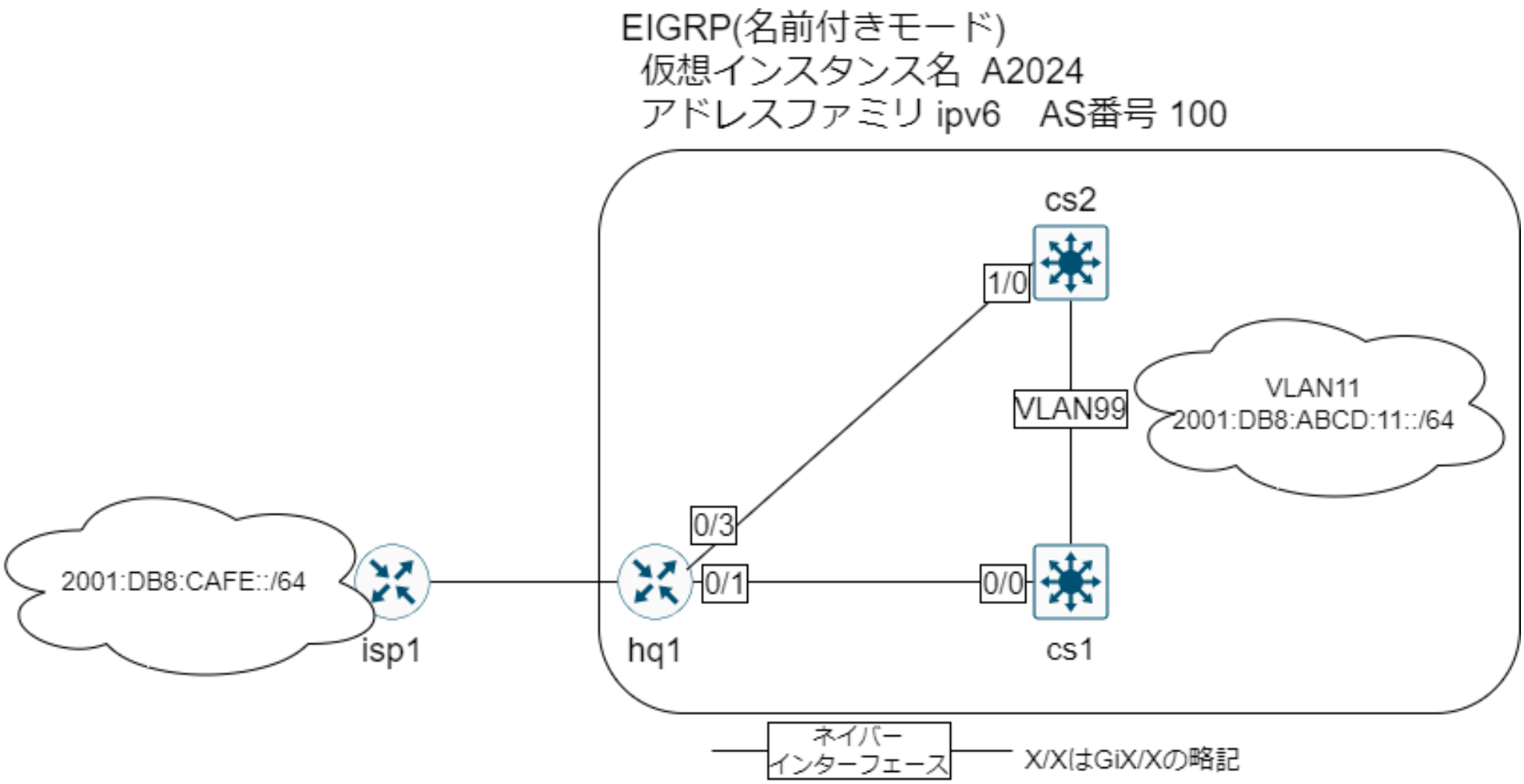


図7：IPv6ルーティング概要