競技職種実施要領

ITネットワークシステム管理職種

Ver.1.2_2026年 7月7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	35
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	25

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**	**35**
	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**	**25**
	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	25
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	40
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

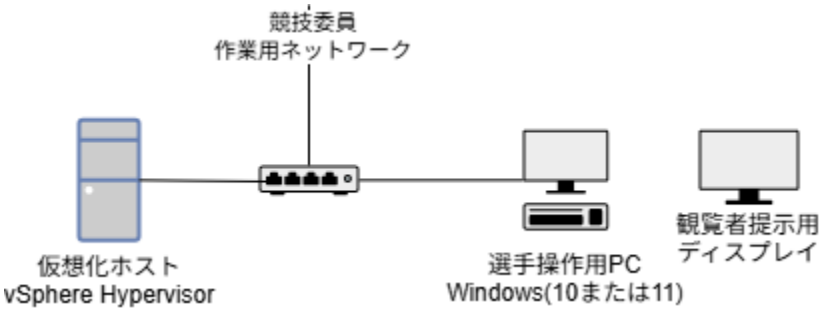
課題１については、競技前日の競技説明・機材確認の際にネットワークトポロジーなどの基本情報のみが記載された冊子を配布する。課題２および課題３については事前公表しない。

5 職種限定規則

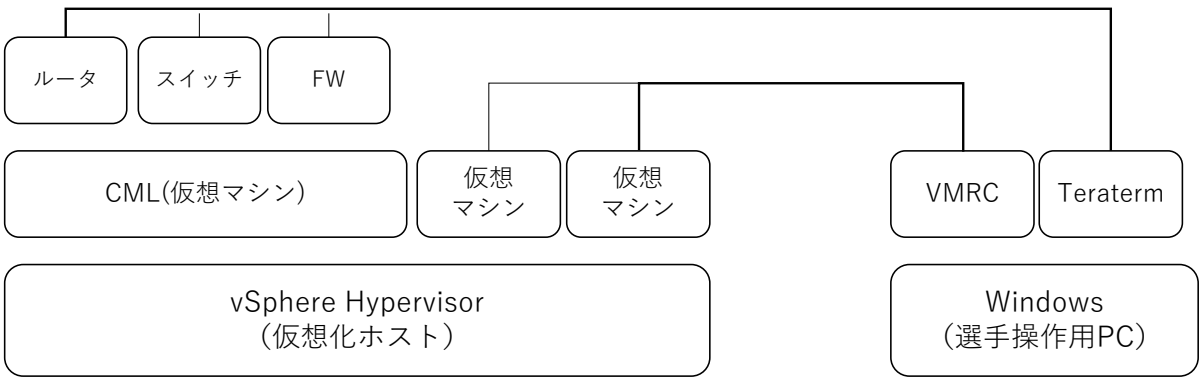
- 各種マニュアル、参考書、ノート等の持ち込みは認めない。
- ソフトウェアの持ち込みは認めない。
- 質問などがある場合には、質問票に記入して競技委員に申し出ること。質問する時間は、競技開始30分後から競技終了30分前までとする。ただし、ハードウェアトラブルまたはソフトウェアの初期設定不良などが疑われるケースについては随時質問可能とする。
- 競技終了の合図で、作業を直ちに終了すること。
- 競技時間内に作業を終了した場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
- 競技中に、トイレ、体調不良などが生じた場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
- 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Windows11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 13.4、Windows Server 2025 (評価版)
- 競技用クライアントOS： Debian GNU/Linux 13.4、Windows11 (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以降
- 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。（ただし、課題の構成によって下記の全てのノードタイプを使用するとは限らない）

- 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。

2026/12/3　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
2026/12/4　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
2026/12/5　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
2026/12/6　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１４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。前回の国際大会の競技課題については、https://worldskills.org/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 63 回 技能五輪全国大会

IT ネットワークシステム管理

課題 1 トラブルシューティング課題

競技課題

令和 7 年 10 月 17 日(金)

競技時間：2 時間 30 分（9：30～12：00）

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 2.5 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 63 回技能五輪全国大会 IT ネットワークシステム管理職種
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

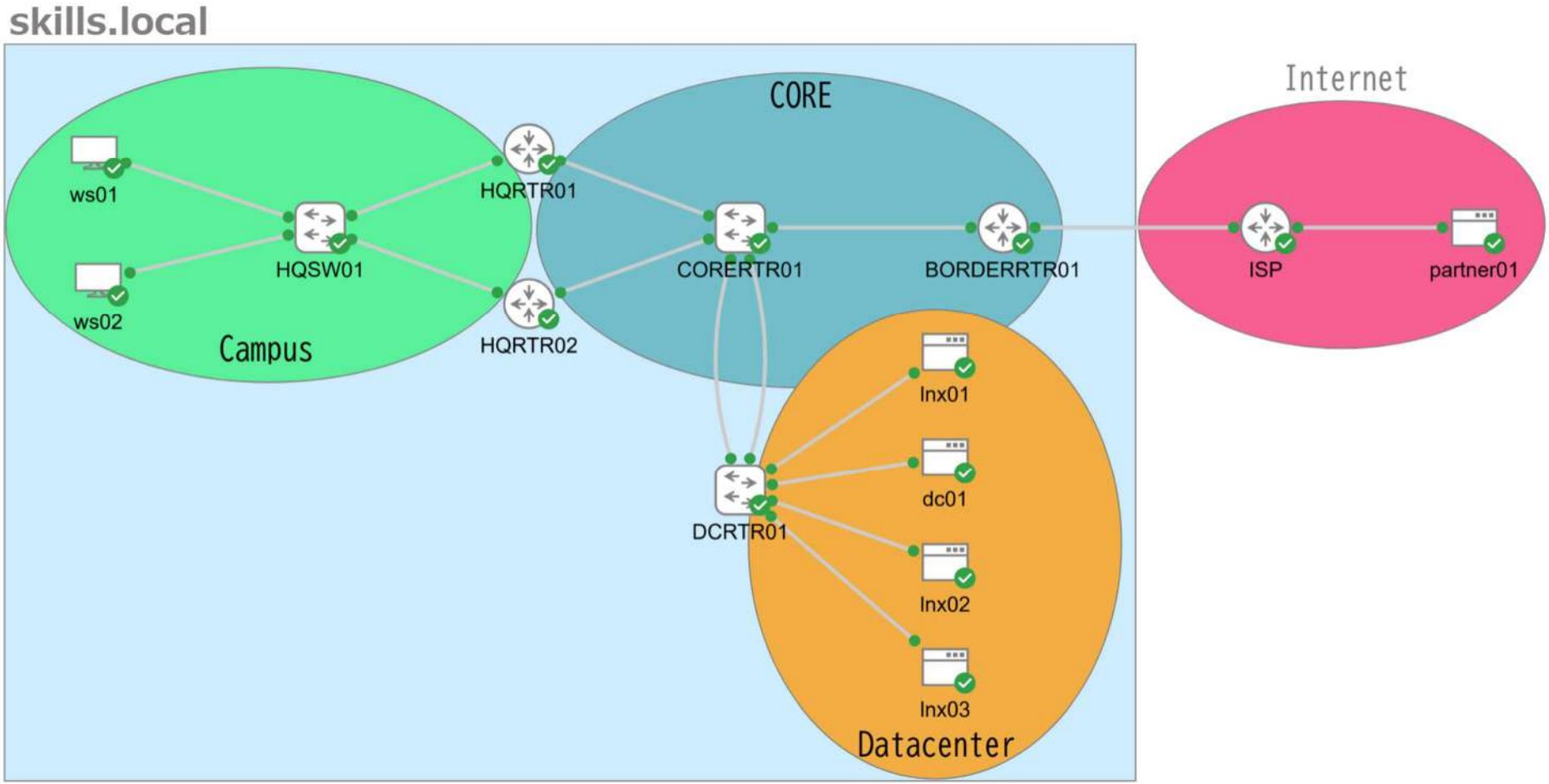
  ・トラブルを解決するために必要となる作業手順

  ・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。
- セッションエラーが出ることがあるので、解答をメモ帳と等に貼り付けて回答することをお勧めする。なおセッションエラーとなった場合はログインからやり直せば回復する。

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

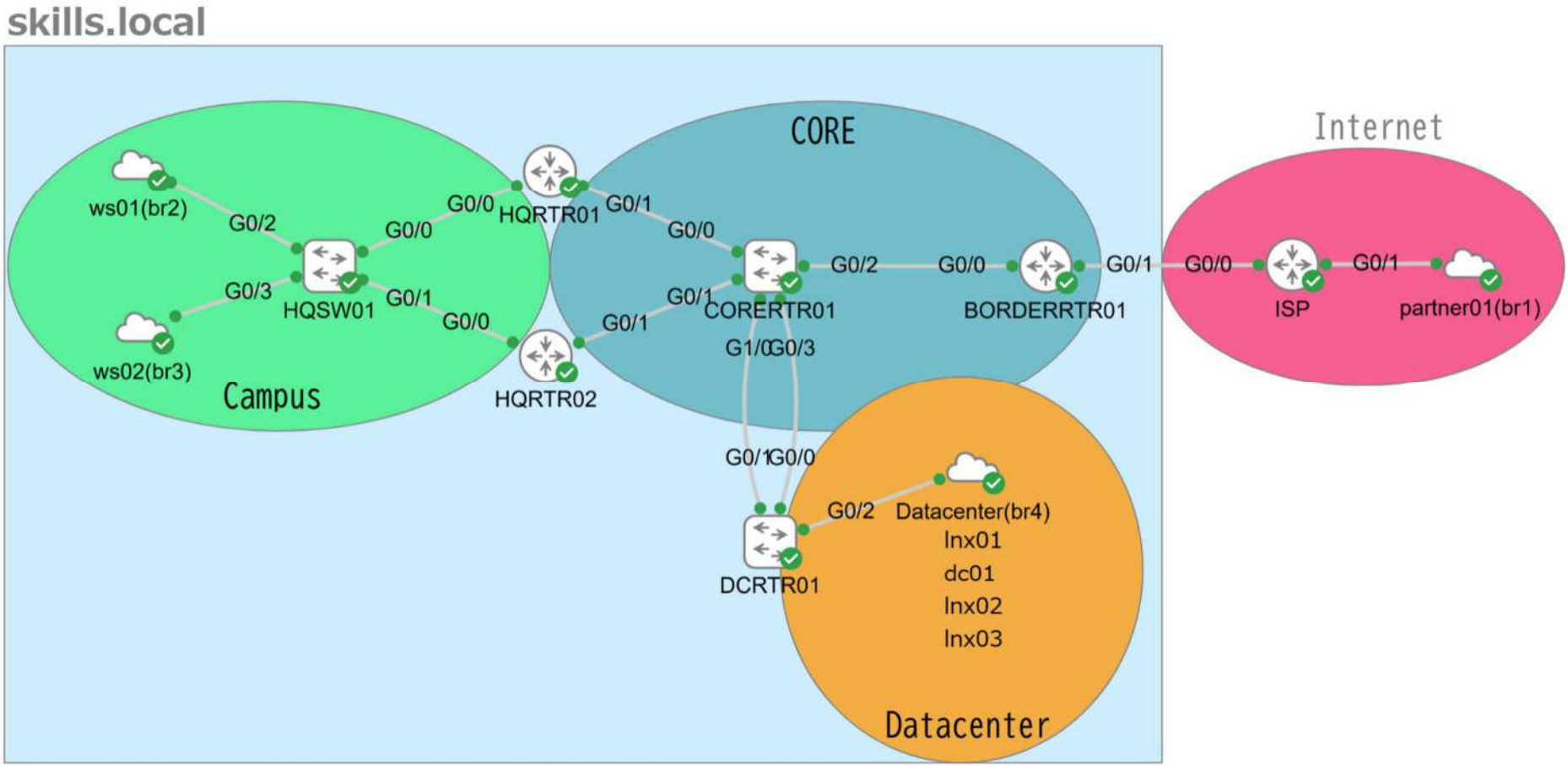
【ネットワークの情報】

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	Debian12.10 (CUI)	root user	Web, DHCP, DNS(skills.net)
lnx02	10.1.64.11/24	Debian12.10 (CUI)	root user	Web
lnx03	10.1.64.12/24	Debian12.10 (CUI)	root user	Web, Web Proxy
ws01	DHCP	Windows10	user(local)	
ws02	DHCP	Debian12.10 (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 Gi0/0:10.254.254.1/31 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 Gi0/1:20.20.1.193/29	Cisco IOS		
ISP	様々な IP アドレス	Cisco IOS		
partner01	31.22.11.32/24	Debian12.10 (GUI)	root user	Web, DNS(sky-expo.aichi)

※パスワードはすべて「Skills2025」

※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 63 回 技能五輪全国大会

IT ネットワークシステム管理

課題 1 トラブルシューティング課題

競技チケット

令和 7 年 10 月 17 日(金)

競技時間：2 時間 30 分（9：30～12：00）

・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が自分のユーザ名になり、クリックしてもエラーがでてアクセスできません。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、ファイルがコピーできません。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のだけど、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、lnx02 を起動しても、電源が落ちてしまいます。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。他にも色々なファイルを編集したり、コマンドを実行したりしたけど、何をしてしまったか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.local」を使用して、lnx03 にある app.skills.local 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.LOCAL」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。

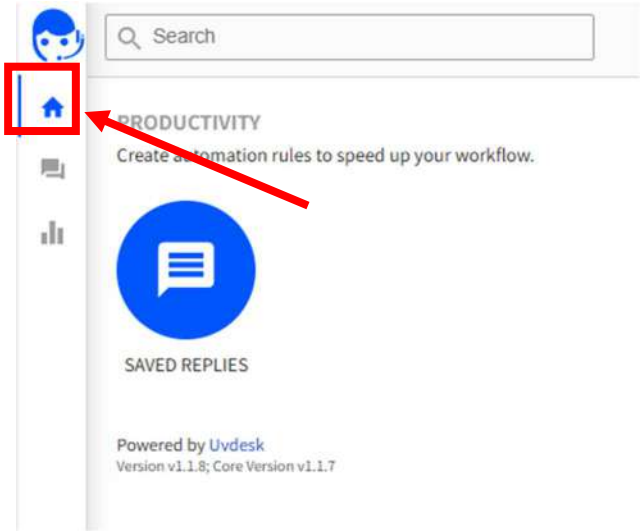
【MEMO】

別紙　UVdesk ヘルプデスクでの回答方法

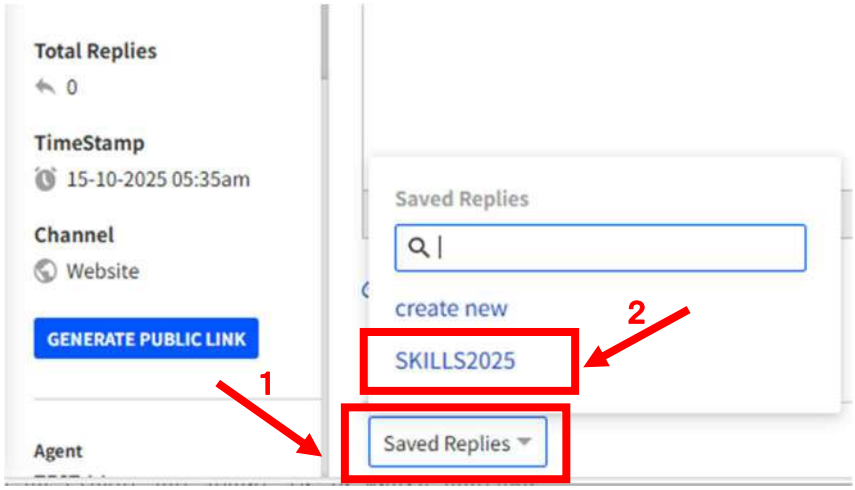
1. 管理 PC のデスクトップ上にある『UVdesk login』ショートカットから、UVdesk ヘルプデスクシステムにアクセスします。(URL: http://uvdesk.skills.jp/en/member/login)
2. 下記のログイン ID（メールアドレス形式）とパスワードでログインします。

座席番号	ログイン ID	パスワード
it1	player01@skills.jp	play7321

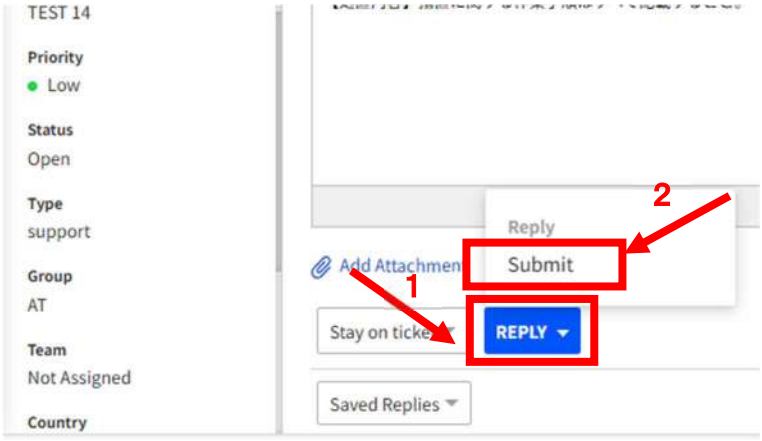
3. ログイン後、左のサイドバーにある『Tickets』をクリックし、チケットを確認します。下見環境では 3 チケットあります。



4. 回答するチケットをクリックし、表示される画面の一番下の『Save Replies』をクリックし、定義済みの回答テンプレートを使用します。



5. 「Write a Reply」のテキストボックスにトラブルに対する回答として『原因』と『処置内容』を入力します。（Forward および Note は使用しないこと。）
6. 入力が済んだら「Reply」をクリックし「Submit」を選択し回答を送信します。



7. 回答を送信後、修正・削除したい場合は、回答の左に表示される⋮から、『Edit Thread』および『Delete Thread』で可能です。なおメニューが表示されない場合はブラウザの横幅を広げてください。

・競技本番では回答は１つのみとします。１つのチケットに対し回答が複数ある場合は最後に送信された回答のみを評価します。

第 63 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

2025 年 10 月 18 日（土） 9:00～12:30（3 時間 30 分）

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、aichi-skills.jp及びsky.aichi-skills.jp の四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

・ルータR-Tky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、tsv2が、Internalネットワークにはサーバtsv3と、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. R-Tky

・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。
・tsv1とtsv2の IPv4 アドレスをそれぞれ10.0.3.253と10.0.3.252へ静的に変換するNAT設定。
・Internal ネットワークノードの IPv4 アドレスを10.0.3.201へ動的に変換するNAT設定。
・アクセス制御は未設定である。

2. 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が、Internalネットワークにはクライアント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。

2.1. osv1

・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。

2.1.1. DNS サービス

・正引き要求 osv1.osaka-skills.jp、www.osaka-skills.jp、www-v6.osaka-skills.jp(外部ネットワークからの要求のみ)、mail.osaka-skills.jp に応答する。
・MXレコードの問い合わせにmail.osaka-skills.jpを返す。

2.1.2. Mail サービス

osv1にユーザ taro が作成済みでありメールの送受信が可能である。なお、taro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.osaka-skills.jp/の要求に、文字列osaka-skills.jpを返す。
・http://www-v6.osaka-skills.jp/の要求に、文字列osaka-skills.jp [IPv6] site.を返す(外部ネットワークからの要求のみ)。

2.1.4. 導通確認

・osv1 へ、ユーザ ping-test でローカルログインすることにより、ルータ ISP への ping コマンドが自動実行される。なお、ping-test のパスワードは pass である。

3. aichi-skills.jp

・ルータ R-Ach 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 asv1 が、Internal ネットワークにはサーバ asv2、asv3 と、クライアント a-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. 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。

3.1.1. 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。

3.1.2. Mail サービス

・asv1 にユーザ jiro が作成済みでありメールの送受信が可能である。なお、jiro 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。

3.1.3. Web サービス

・http://www.aichi-skills.jp/の要求に、文字列 Aichi-skills.jp を返す(外部ネットワークからの要求のみ)。

4. sky.aichi-skills.jp

・ルータ R-Sky 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 ssv1 と、クライアント s-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。

5. Public Internet Network

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

5.1. sv

sv では下記のサービスが稼働している。

5.1.1. 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。

5.1.2. Web サービス

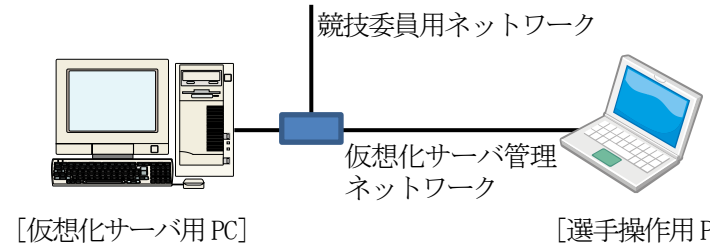
・http://www.itnetsys.org の要求に応答する。

5.1.3. SMTP サービス

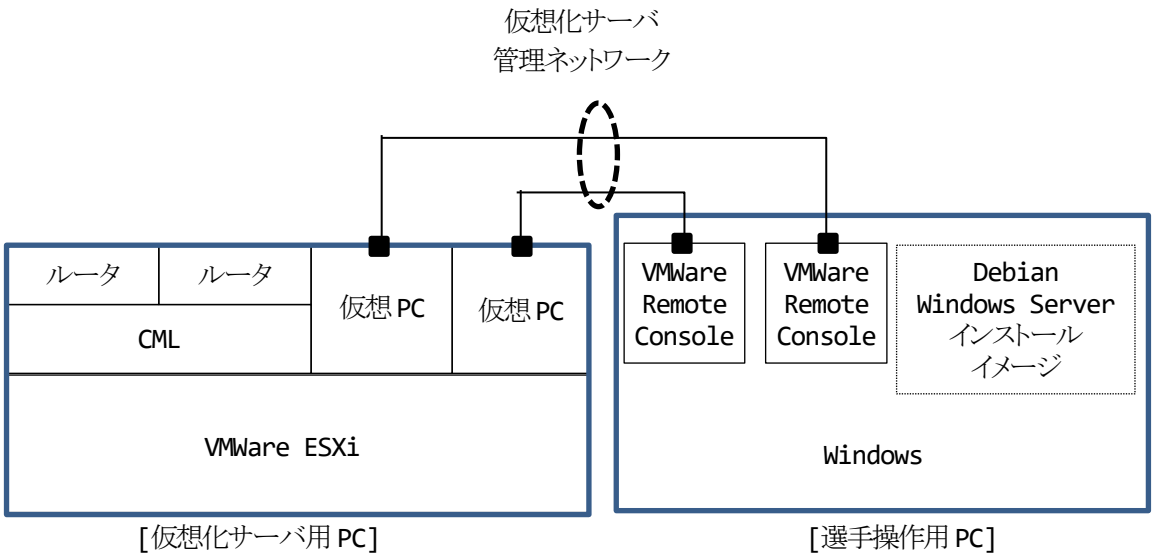
・manager@itnetsys.org 宛のメールを受信可能である。また、この受信メールに対して Subject「Auto Reply Mail」の空メールが自動返信される。

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 shortcuts 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 ノードには 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。
- Debian のインストールイメージ debian-12.10.0-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 tsv1、tsv2、tsv3、t-client、R-Osk、R-Ach、asv2、asv3、a-client、R-Sky、ssv1、s-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。
・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。

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、適切なゲートウェイ、及びホスト名を設定しなさい。

2. tokyo-skills.jp

2.1. tsv1

2.1.1. DNS サーバ

・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。
・使用するパッケージは bind9 とする。
・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。

A) 外部ネットワーク向けサービス

・www.tokyo-skills.jp の正引き問合せに tsv2 の IPv4 アドレスを応答する。
・www-v6.tokyo-skills.jp の正引き問合せに tsv2 の IPv6 アドレスを応答する。
・mail.tokyo-skills.jp の正引き問合せに tsv1 の IPv4 アドレスを応答する。
・MX レコードの問合せに mail.tokyo-skills.jp を応答する。
・再帰問合せを許可しない。

B) 内部ネットワーク向けサービス

・in-www.tokyo-skills.jp の正引き問合せに tsv3 の IPv4 アドレスを応答する。
・mail.tokyo-skills.jp の正引き問合せに tsv1 の IPv4 アドレスを応答する。
・MX レコードの問合せに mail.tokyo-skills.jp を応答する。

2.1.2. メールサーバ

・tokyo-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-imapd とする。
・LDAP ユーザを用いてサーバ接続時に認証を行う。
・LDAP ユーザ宛のメールをスプールする。
・tsv3 が発行するサーバ証明書を利用し、クライアント／サーバ間の通信は IMAPS(TCP/993)で暗号化する。

2.2. tsv2

2.2.1. DNS サーバ

・外部ネットワークに対し tokyo-skills.jp 正引きゾーンのスレイブサーバとしてサービスを提供する。
・再帰問合せを許可しない。

2.2.2. Web サーバ

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

2.2.3. リバースプロキシ

・使用するモジュールは Application Request Routing、URL Rewrite とする。なお、両モジュールのインストーラは、http://www.itnetsys.org/reverse_proxy/から入手すること。
・https://www.tokyo-skills.jp/の要求を、http://192.168.10.1/へリダイレクトする。

2.3. tsv3

2.3.1. 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 Skills2025 とする。
・3 個の LDAP ユーザ tuser01～tuser03 を登録する。パスワードは tPass2025 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/TOKYO-SKILLS@*user_name* とする。

2.3.2. Web サーバ

・使用するパッケージは nginx とする。
・http://192.168.10.1/の要求に対し、文字列 Tokyo Skills Secure Site を返す。
・http://in-www.tokyo-skills.jp/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。

2.3.3. 自動化

・使用するパッケージは ansible-core とする。
・tsv3 でユーザ master が以下のコマンドを実行することにより、t-client に/var/00Test ディレクトリが作成されること。

```
ansible-playbook /home/master/ansible-test.yaml
```

・プレイブックファイル ansible-test.yaml は、http://www.itnetsys.org/ansible/から入手すること。

2.3.4. 認証局

・競技課題の仕様から証明書が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 Tokyo Skills Sub CA とする。
・サーバ証明書①:www.tokyo-skills.jp
・サーバ証明書②:mail.tokyo-skills.jp

C) サーバ証明書のコピーを/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:sub_ca.pem
・サーバ証明書①:www.tokyo-skills.jp.pem
・サーバ証明書②:mail.tokyo-skills.jp.pem

2.4. t-client

2.4.1. LDAP クライアント

・使用するパッケージは libnss-ldapd libpam-ldapd ldap-utils とする。
・競技終了時に LDAP ユーザ tuser03 がログインした状態とする。また、t-client ローカルにユーザ tuser03 が存在しないこと。
・LDAP ユーザ tuser03 に sudo によるコマンドの root 権限実行を許可する。

2.4.2. メールクライアント

・Thunderbird に必要な設定を行い、LDAP ユーザ tuser03 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。

3. osaka-skills.jp

3.1. R-Osk

3.1.1. NAT・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。
・外部ネットワークと通信するために osv1 の IPv4 アドレスを 10.0.4.253 へ静的に変換する。
・osv1 発信トラフィックに対する戻りトラフィックを許可する。
・osv1 への IPv4 トラフィック(http、smtp、DNS、ping)を許可する。
・osv1 への IPv6 トラフィック(http、DNS、ping)を許可する。
・R-Osk への IPv4 トラフィック(ping)を許可する。
・R-Osk への IPv6 トラフィック(ping)を許可する。
・上記以外は許可しない。

3.1.2. DHCP サーバ

・使用するパッケージは isc-dhcp-server とする。
・Internal ネットワークに 192.168.20.101～120 の IPv4 アドレスを配布する。
・DNS サーバとして osv1 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。

4. aichi-skills.jp

4.1. R-Ach

4.1.1. サイト間 VPN

・Internal ネットワークと sky.aichi-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。

4.1.2. NAT

・外部ネットワークと通信するために DMZ、Internal ネットワークにあるノードの IPv4 アドレスを 10.0.1.253 へ動的に変換する。
・外部ネットワークから 10.0.1.253 宛パケット(http、smtp、DNS)を asv1 へポートフォワードする。

4.2. asv2

4.2.1. Active Directory

・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 Skills2025 とする。
・aichi-skills.jp ドメイン直下に組織単位 O_MASTER、O_CLIENT を作成する。
・O_MASTER にグループ G_MASTER を作成する。
・O_CLIENT にグループ G_CLIENT を作成する。
・O_MASTER にユーザ auser01～auser03 を作成する。パスワードは aPass2025 とする。
・O_CLIENT にユーザ auser04～auser06 を作成する。パスワードは aPass2025 とする。
・auser01～auser03 を G_MASTER のメンバとする。
・auser04～auser06 を G_CLIENT のメンバとする。
・auser01～auser06 のホームフォルダを¥¥aichi-skills.jp¥Home$¥*user_name* に設定し、Z:ドライブに割り当てる。

・auser01～auser06 のプロファイルパスを¥¥aichi-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。

4.2.2. DFS(名前空間とレプリケーション)

・共有フォルダ¥¥asv3¥Home$と¥¥asv3¥Profiles$を作成する。
・共有フォルダ¥¥asv2¥Home$を作成し、名前空間¥¥aichi-skills.jp¥Home$を設定する。
・共有フォルダ¥¥asv2¥Home$と¥¥asv3¥Home$をメンバとしてレプリケーションを設定する。
・共有フォルダ¥¥asv2¥Profiles$を作成し、名前空間¥¥aichi-skills.jp¥Profiles$を設定する。
・共有フォルダ¥¥asv2¥Profiles$と¥¥asv3¥Profiles$をメンバとしてレプリケーションを設定する。

4.2.3. グループポリシー

・O_MASTER に適用するグループポリシーを作成する。ポリシー名は for_MASTER とする。
・¥¥asv3¥Share_MASTER を Y:ドライブに割り当てる。
・ログオン時に Microsoft Edge を起動する。

4.2.4. DNS サーバ

・内部ネットワーク向けに aichi-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。
・内部ネットワーク向けに 1.168.192.in-addr.arpa 逆引きゾーンのマスタサーバとしてサービスを提供する。
・asv1.aichi-skills.jp の正引き問合せに asv1 の IPv4 アドレスを応答する。
・mail.aichi-skills.jp の正引き問合せに asv1 の IPv4 アドレスを応答する。
・asv2.aichi-skills.jp の正引き問合せに asv2 の IPv4 アドレスを応答する。
・MX レコードの問合せに mail.aichi-skills.jp を応答する。
・自身で名前解決が行えない場合は asv1 へ問い合わせる。

4.2.5. DHCP サーバ

・Internal ネットワークに 192.168.1.101～200 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。
・DNS 逆引きゾーンの PTR レコードを常に更新する。

4.3. asv3

4.3.1. Active Directory

・aichi-skills.jp のメンバとする。

4.3.2. 共有フォルダ

・下表に示す共有フォルダを作成する。

共有名	アクセス権
Share_Public	ASV3¥Administrators:フルコントロール Domain Users:読み取りと実行、フォルダ内容の一覧表示、書き込み その他のユーザ:なし
Share_MASTER	ASV3¥Administrators:フルコントロール G_MASTER:読み取りと実行、フォルダ内容の一覧表示、書き込み その他のユーザ:なし

ただし、Domain Users と G_MASTER は aichi-skills.jp ドメインのグループである。

4.4. a-client

4.4.1. OS の設定

・aichi-skills.jp のメンバとする。
・競技終了時に Active Directory ユーザ auser03 がログインした状態とする。
・ローカルの Administrator アカウントを有効とする。パスワードは Skills2025 とする。
・DHCP サーバから IPv4 アドレスの割り当てを受ける。
・対話型ログオン時に、前回ログオンしたユーザ名を表示しない。

5. sky.aichi-skills.jp

5.1. R-Sky

5.1.1. 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。
・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。

5.2. ssv1

5.2.1. Active Directory

・aichi-skills.jp の子ドメインとして、sky.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 Skills2025 とする。
・ドメインにユーザ suser01～suser03 を作成する。パスワードは sPass2025 とする。

5.2.2. DNS サーバ

・内部ネットワーク向けに sky.aichi-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。
・自身で名前解決が行えない場合は asv2 へ問い合わせる。

5.2.3. iSCSI

・仮想ディスクサイズ 1GB の iSCSI ターゲットを構成する。

5.3. s-client

5.3.1. Active Directory

・sky.aichi-skills.jp ドメインのメンバとする。
・使用するパッケージは samba、winbind、realmd とする。
・ドメインユーザのログインシェルを/bin/bash とする。
・ドメインユーザのホームディレクトリを/iscsi/home/*user_name*/とする。
・競技終了時にドメインユーザ suser01 がログインした状態とする。

5.3.2. iSCSI

・使用するパッケージは open-iscsi とする。
・iSCSI ターゲット(ssv1)の仮想ディスクを/iscsi にマウントする。

図1 ネットワーク構成図

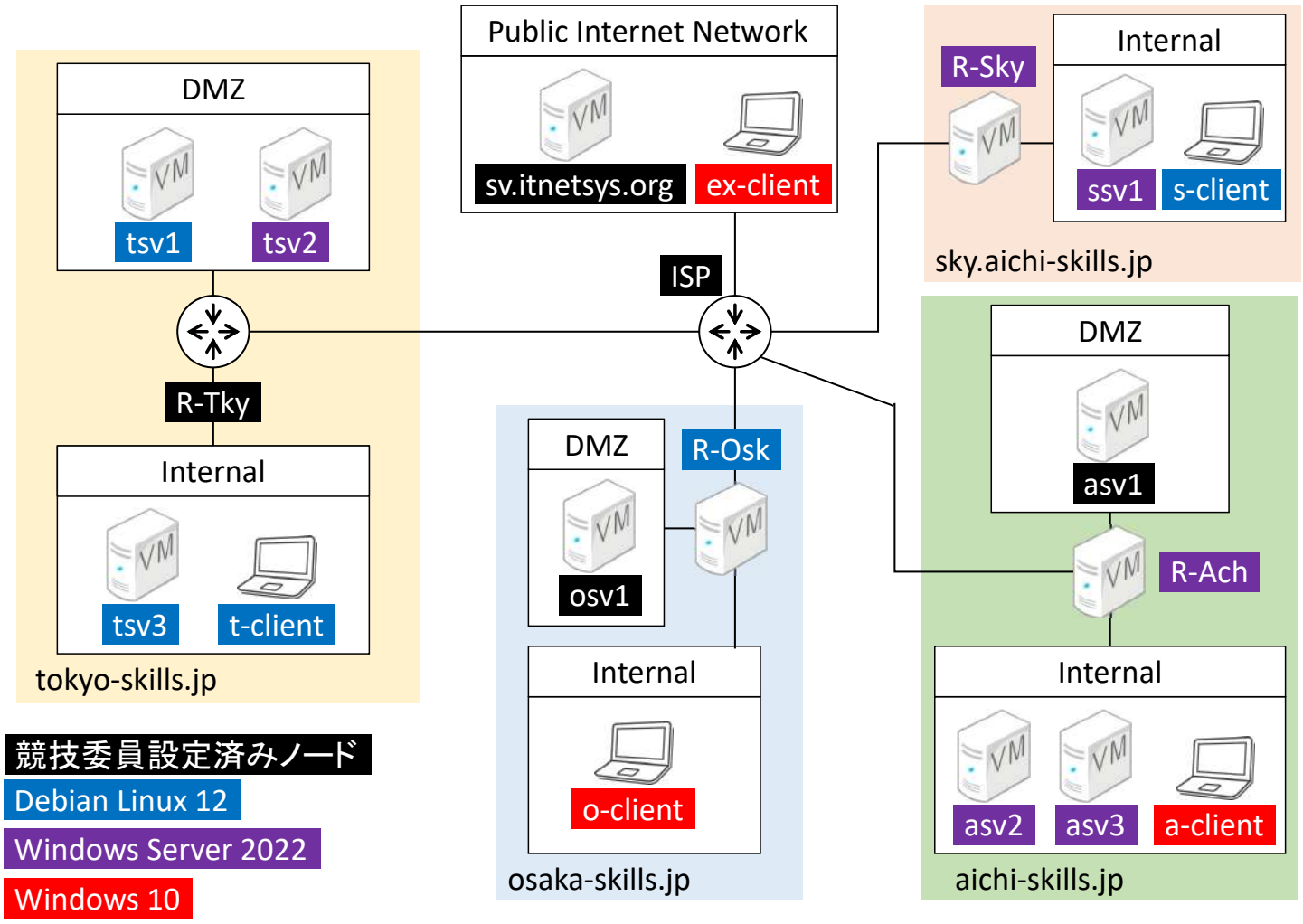


表1 ルータ接続，IPアドレス

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	10.0.1.1/24		R-Ach
	非公開	10.0.2.1/24		R-Sky
	非公開	10.0.3.1/24	2001:DB8:3:1::FF/64	R-Tky
	非公開	10.0.4.1/24	2001:DB8:4:1::FF/64	R-Osk
R-Ach	Ethernet0	10.0.1.254/24		ISP
	Ethernet1	100.0.1.254/24		DMZ
	Ethernet2	192.168.1.254/24		Internal
R-Sky	Ethernet0	10.0.2.254/24		ISP
	Ethernet1	192.168.2.254/24		Internal
R-Tky	非公開	10.0.3.254/24	2001:DB8:3:1::1/64	ISP
	非公開	100.0.2.254/24	2001:DB8:3:2::FF/64	DMZ
	非公開	192.168.10.254/24		Internal
R-Osk	ens192	10.0.4.254/24	2001:DB8:4:1::1/64	ISP
	ens256	100.0.3.254/24	2001:DB8:4:2::FF/64	DMZ
	ens161	192.168.20.254/24		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 12.10	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
R-Ach	Windows Server 2022	表1参照	表1参照	administrator	Skills2025
asv1	Debian Linux 12.10	100.0.1.1		非公開	非公開
asv2	Windows Server 2022	192.168.1.1		administrator	Skills2025
asv3	Windows Server 2022	192.168.1.2		administrator	Skills2025
a-client	Windows 10	DHCPで取得		user	なし
R-Sky	Windows Server 2022	表1参照	表1参照	administrator	Skills2025
ssv1	Windows Server 2022	192.168.2.1		administrator	Skills2025
s-client	Debian Linux 12.10	192.168.2.101		root	Skills2025
R-Osk	Debian Linux 12.10	表1参照	表1参照	root	Skills2025
osv1	Debian Linux 12.10	100.0.3.1	2001:DB8:4:2::1	非公開	非公開
o-client	Windows 10	DHCPで取得		user	なし

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
tsv1	Debian Linux 12.10	100.0.2.1	2001:DB8:3:2::1	root	Skills2025
tsv2	Windows Server 2022	100.0.2.2	2001:DB8:3:2::2	administrator	Skills2025
tsv3	Debian Linux 12.10	192.168.10.1		root	Skills2025
t-client	Debian Linux 12.10	192.168.10.101		root	Skills2025

※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 63 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

2025 年 10 月 19 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

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、構築対象となる検証用ネットワークには 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(ISP)は isp-a1/isp-a2/isp-a3/isp-sv 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-sv/hq-cl が接続するセグメントと pub-sv が接続する公開サーバ―セグメントがある。Branch1/Branch2 にはそれぞれクライアントセグメントがある。また、HeadQuarter/Branch1 拠点には子会社ネットワーク(Subsidiary)が共存している。

HeadQuarter/Branch1 間は広域イーサネットにて接続される。広域イーサネットは、検証用ネットワークでは管理機能なしスイッチ(widearea-ethernet)にて代替する。また、各拠点間はインターネット経由の DMVPN によって接続し HeadQuarter/Branch1 間について冗長性が確保されるものとする。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(HeadQuarter/Branch1/Branch2)および ISP のネットワークである。各端末(Linux VM)は設定済みであり設定変更は許可しない。また、管理機能なしスイッチは L2 レベルの接続用であり、設定の対象ではない。

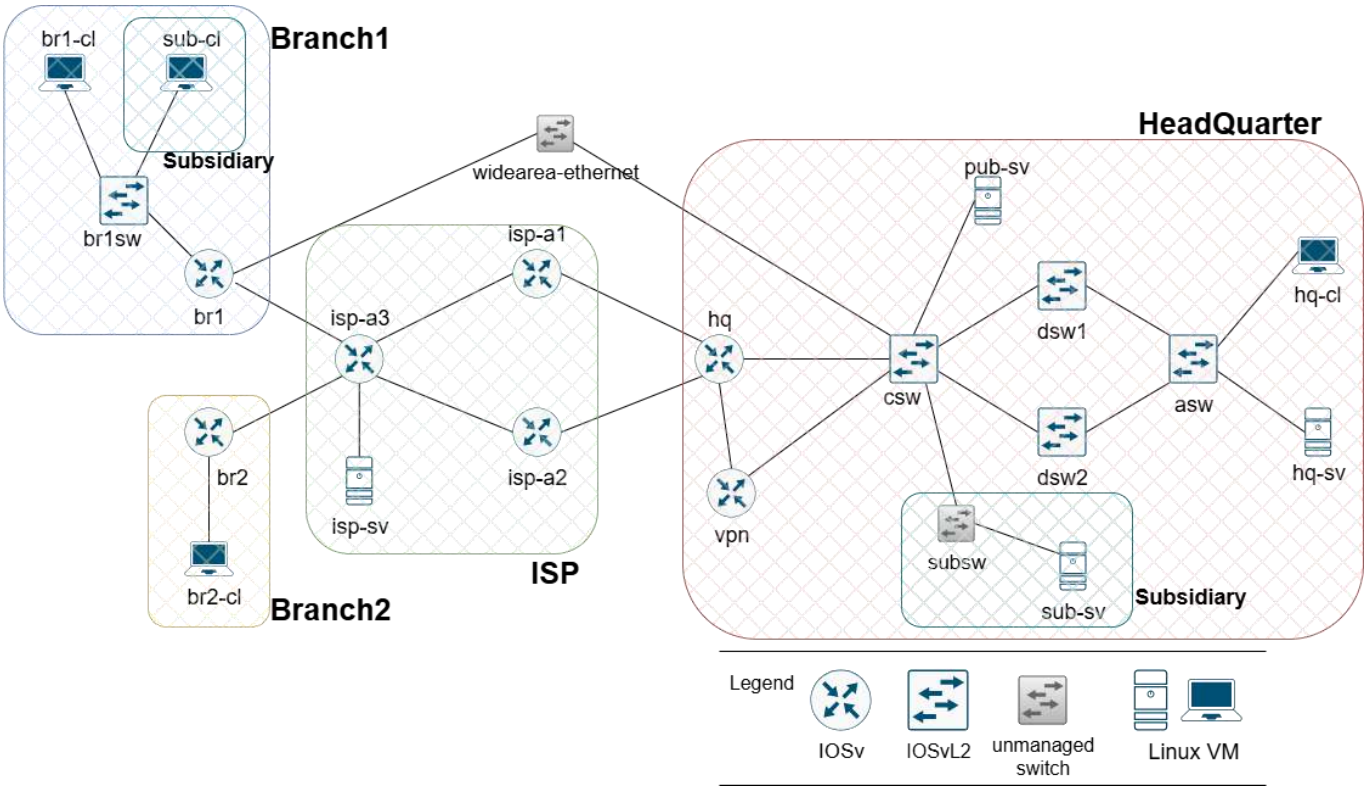


図１　ネットワークサイト構成

２ 仮想マシンに関する基本情報

2.1. isp-sv / hq-sv / sub-sv / pub-sv / hq-cl / br1-cl / br2-cl / sub-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、Debian12.10 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。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。

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（hq/vpn/csw/dsw1/dsw2/asw/isp-a1/isp-a2/isp-a3/br1/br2/br1sw）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。なお、全ネットワークノードについてホスト名、no ip domain lookup、exec-timeout 0 0 が設定済みである。isp-a1/isp-a2/isp-a3 についてはアドレス設定済みである。また、csw/br1 には VRF 名 SUB に所属するインターフェースがあり、重複アドレスとなっていても誤りではない。VRF 設定については後述する。

2. asw/br1sw について、L2 機能のみを使用するためルーティング機能をオフにすること。

3. asw のデフォルトゲートウェイ(IPv4)を静的に設定する。

4. br2 について、特権モードパスワードを br2epass とする。パスワードはタイプ９で暗号化されること。※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。

5. br2 について、ドメイン名を skills.it.jp とする。

6. 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。パスワードはタイプ９で暗号化されること。

7. br2 への SSH(バージョン 2)での接続を許可する。上記６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。（br2-cl から ssh コマンドで接続確認できること）

8. br2 へ SSH ログインした場合、特権モードへ自動的に移行すること。

4.2　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. dsw1/dsw2/asw の VTP モードはトランスペアレントとする。

2. dsw1/dsw2/asw/br1sw 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. 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) dsw1/asw 間
   B) dsw2/asw 間
   C) br1/br1sw 間

4. asw の Gi0/0 について、STP の計算を待つことなく、接続したホストが直ちにフレームを転送できるようにする。

5. asw の Gi0/0 において、BPDU を受信した場合、このポート err disable とするように設定する。

4.3　インターネットゾーンルーティング

インターネットゾーンにおけるルーティング設定を以下の通り行い、所定の到達性を確保しなさい。

1. isp-a1/isp-a2/isp-a3 において、OSPF(IPv4)を次の通り動作させる。
   A) isp-a1/isp-a2/isp-a3 間における各 Loopback0 への到達性を確保するため経路交換を行う。
   B) 上記の到達性確保に不要なインターフェースで OSPF を動作させないこと。

2. isp-a1/isp-a2/isp-a3 において、OSPFv3(IPv6)を次の通り動作させる。
   A) isp-a1/isp-a2/isp-a3 間における各 Loopback0 への到達性を確保するため経路交換を行う。
   B) 上記の到達性確保に不要なインターフェースで OSPFv3 を動作させないこと。

3. 別添ネットワーク構成図表・図３の BGP(**IPv4/ IPv6**)ルーティング概要に従い、次の通り BGP を動作させる。
   A) isp-a1/isp-a2/isp-a3 は AS 番号 65000 として BGP を動作させる。
   B) isp-a1/isp-a3 間および isp-a3/isp-a2 間で iBGP ピアを確立する。Loopback0 のアドレスをネイバーアドレスとして使用すること。
   C) isp-a3 は、iBGP で受け取った経路を別の iBGP ピアに再配布すること。
   D) hq は AS 番号 65010 として isp-a1/isp-a2 と eBGP ピアを確立する。
   E) isp-a1/isp-a2 は、自身をデフォルトルート先とする経路を eBGP ピアへアドバタイズする。
   F) 別添ネットワーク構成図表・図３に示されている各サブネットの経路情報がアドバタイズされ到達性が確保されること。100.100.100.0/28 については集約経路であることに注意すること。（※HeadQuarter 拠点内のルーティングについては後述）
   G) hq において IPv4 トラフィックの出口経路の優先度を設定する。isp-a1 側を優先経路、isp-a2 側をバックアップ経路とすること。
   H) hq において IPv6 トラフィックの出口経路の優先度を設定する。isp-a1 側をバックアップ経路、isp-a2 側を優先経路とすること。

4. br1/br2 においてデフォルトルートを静的に設定する。デフォルトルートは isp-a3 を指すものとする。

4.4 VRF (Virtual Routing and Forfowarding)

別添ネットワーク構成図表・図４に示す通り子会社ネットワークには、sub-cl と sub-sv が接続するセグメントがあり、これらのセグメントは広域イーサネット(widearea-ethernet)で接続されている。

子会社ネットワークの経路情報については、VRF を用いて HeadQuarter/Branch1 拠点のその他の経路情報（グローバルルーティング）と分離する。以下の通り VRF 設定を行い sub-cl/sub-sv 間の到達性を確保しなさい。

1. csw/br1 において、子会社ネットワークの経路をグローバルルーティングから分離して管理するために VRF を定義する。VRF 名は SUB とする。

2. 別添ネットワーク構成図表・表２の通り、csw/br1 において子会社ネットワークのトラフィックを送受信するインターフェースについて VRF SUB 所属とする。

3. 子会社ネットワークのトラフィックを分離識別するために、csw/br1 の各サブインタフェースにて IEEE802.1Q によるタグ付けを設定する。

4. sub-cl/sub-sv 所属セグメント間での到達性を確保できるように VRF SUB に静的経路を登録する。

5. sub-cl 所属セグメントからインターネット接続を可能とするために、br1 の VRF SUB にデフォルトルートを静的に登録する。デフォルトルートは isp-a3 を指すものとする。

4.5 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(br1-cl 所属セグメント)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。br1 の外側インターフェース(Gi0/0)のアドレスに変換されること。

2. Branch1 拠点内子会社セグメント(sub-cl 所属セグメント、VRF SUB)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。br1 の外側インターフェース(Gi0/0)のアドレスに変換されること。

3. HeadQuarter 拠点内セグメント(172.16.0.0/16)からのインターネットゾーンとの接続について、hq にて NAPT(PAT)を適用する。出口インターフェースが Gi0/1(isp-a1 側)となる場合は Gi0/1 のアドレスに変換されること。

4. HeadQuarter 拠点内セグメント(172.16.0.0/16)からのインターネットゾーンとの接続について、hq にて NAPT(PAT)を適用する。出口インターフェースが Gi0/2(isp-a2 側)となる場合は Gi0/2 のアドレスに変換されること。

※上記 3, 4 について、sub-sv 所属セグメントは考慮しなくてよい。

4.6 DMVPN

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. vpn/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) vpn における Tunnel0 のトンネルソースは Loopback0 を使用する。
   B) br1/br2 における Tunnel0 のトンネルソースは Gi0/0 を使用する。
   C) vpn 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。
   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。

4.7 拠点間および拠点内ルーティング

拠点間および拠点内におけるルーティング設定を以下の通り行い、所定の到達性を確保しなさい。

1. 別添ネットワーク構成図表・図６の OSPF ルーティング概要に従い、br1/br2/vpn/csw において、OSPF(IPv4)を次の通り動作させる。
   A) 別添ネットワーク構成図表・図６に示す通り Area 分割を行い、br1/br2/vpn/csw 間で経路交換を行う。(※図６中の Area 1 は br1-cl 所属セグメントである。VRF で分離されている sub-cl 所属セグメントの経路ではないことに留意すること。)
   B) vpn および csw は ASBR として動作し、HeadOuarter 拠点の集約アドレス 172.16.0.0/16 のみを OSPF へ再配布する。

2. 別添ネットワーク構成図表・図７の EIGRP(IPv4)ルーティング概要に従い、hq/vpn/csw/dsw1/dsw2 において、次の通り EIGRP(IPv4)を動作させる。
   A) 名前付きモードの仮想インスタンス名を HQ とし、AS 番号を 100 とする。
   B) 別添ネットワーク構成図表・図７の通り、hq/vpn/csw/dsw1/dsw2 間で隣接関係を確立し、vpn の Loopback0、公開サーバーセグメント(100.100.100.8/29)、VLAN10,20 およびピアリングのアドレス帯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) hq において、BGP 経路のうちデフォルトルートのみを EIGRP に再配布する。
   D) vpn において、OSPF 経路を EIGRP へ再配布する。ただし、ループ防止のため拠点内部経路(172.16.0.0/16)が EIGRP へ再配布されないようにフィルタすること。
   E) hq の外側インタフェース(Gi0/1,Gi0/2)で EIGRP を有効にしないこと。
   F) 端末接続セグメント(VLAN10,20)に対して、EIGRP パケットを送信しないこと。

3. HeadQuarter 拠点の端末接続セグメント(VLAN10,20)から Branch1 拠点(br1-cl 所属セグメント 10.1.0.0/24)への通信経路について、優先経路が広域イーサネット(widearea-ethernet→br1)、バックアップ経路が vpn(DMVPN→br1)となること。

4. HeadQuarter 拠点の端末接続セグメント(VLAN10,20)から Branch2 拠点(10.2.0.0/24)への通信経路について、広域イーサネット経由(widearea-ethernet→br1→DMVPN→br2)ではなく、vpn(DMVPN→br2)経由となるように経路優先度を調整しなさい。

5. 別添ネットワーク構成図表・図８の EIGRP(IPv6)ルーティング概要に従い、hq/csw/dsw1/dsw2 において、次の通り EIGRP(IPv6)を動作させる。
   A) 名前付きモードの仮想インスタンス名を HQ とし、AS 番号を 100 とする。
   B) 別添ネットワーク構成図表・図８の通り、hq/csw/dsw1/dsw2 間で隣接関係を確立し、VLAN20(2001:DB8:ABCD:20::/64)への到達性が確保されること。
   C) hq において、BGP 経路のうちデフォルトルートのみを EIGRP に再配布する。
   D) hq の外側インタフェース(Gi0/1,Gi0/2)で EIGRP を有効にしないこと。

E) 端末接続セグメント(VLAN20)に対して、EIGRP パケットを送信しないこと。

※留意点：EIGRP について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。

4.8 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. VLAN10 において、HSRP を次の通り動作させる。
   A) dsw1 をアクティブ、dsw2 をスタンバイとする。
   B) 仮想 IP アドレスは 172.16.10.254 を使用する。
   C) 切り戻しを有効にする。
   D) dsw1 の Gi0/0 がリンクダウンした場合、dsw2 がアクティブ、dsw1 がスタンバイとなること。

2. VLAN20 において、HSRP を次の通り動作させる。
   A) dsw1 をスタンバイ、dsw2 をアクティブとする。
   B) 仮想 IP アドレスは 172.16.20.254 を使用する。
   C) 切り戻しを有効にする。
   D) dsw2 の Gi0/0 がリンクダウンした場合、dsw1 がアクティブ、dsw2 がスタンバイとなること。

3. VLAN20 において、HSRP(IPv6 用)を次の通り動作させる。
   A) dsw1 をスタンバイ、dsw2 をアクティブとする。
   B) 仮想 IP アドレスは FE80::20 を使用する。
   C) 切り戻しを有効にする。
   D) dsw2 の Gi0/0 がリンクダウンした場合、dsw1 がアクティブ、dsw2 がスタンバイとなること。

4.9 アクセスコントロール

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。以下の通りアクセスコントロールを行いなさい。

1. Branch2 拠点内セグメント(10.2.0.0/24)から他セグメントへのアクセスは、172.16.0.0/16 宛および 10.0.0.0/8 宛のみ許可する。
   ※br2 でアドレス変換を行わないため、Branch2 拠点内からのインターネットゾーンとの通信は元からできないが、明示的にフィルタすること。

2. pub-sv 所属セグメント(100.100.100.8/29)から 172.16.0.0/16 宛および 10.0.0.0/8 宛の新規セッションは許可しない。その他の通信は許可する。

4.10 Ansible

以下の通り Ansible による自動化処理を構成しなさい。

1. br2-cl の master ユーザアカウントにおいて、ホームディレクトリで以下のコマンド
   ansible-playbook -i inventory.ini get_show_ip_route.yml
   を実行可能とし、これによって br2 の show ip route の結果が
   /home/master/br2log/br2_route.txt
   に保存されること。
   なお、実行に必要なソフトウェアは br2-cl にインストール済みであり、
   /home/master/inventory.ini は完成したものが用意されている。
   /home/master/get_show_ip_route.yml は不完全であるため、これを完成させなさい。
   ※ansible-playbook コマンド実行時に WARNING（〜 does not support Ansible version 2.14.18）が表示されるが実行上問題ない。

第63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

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-sv	hq-cl	br1-cl	br2-cl	isp-sv	pub-sv	sub-cl	sub-sv
hq-sv		○	○	○	○	○	×	×
hq-cl	○		○	○	○	○	×	×
br1-cl	○	○		○	○	○	×	×
br2-cl	○	○	○		×	×	×	×
isp-sv	×	×	×	×		○	×	×
pub-sv	×	×	×	×	○		×	×
sub-cl	×	×	×	×	○	○		○
sub-sv	×	×	×	×	×	×	○	

（２）　IPv6到達性

要求側＼応答側	hq-cl	isp-sv
hq-cl		○
isp-sv	○	

○：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。

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
isp-a1	Gi0/0	1.1.1.2/30	hq
	Gi0/1	192.168.13.1/24	isp-a3
	Loopback0	192.168.0.1/32	
isp-a2	Gi0/0	2.2.2.2/30	hq
	Gi0/1	192.168.23.2/24	isp-a3
	Loopback0	192.168.0.2/32	
isp-a3	Gi0/0	3.3.3.2/30	br1
	Gi0/1	4.4.4.2/30	br2
	Gi0/2	192.168.13.3/24	isp-a1
	Gi0/3	192.168.23.3/24	isp-a2
	Gi0/4	200.99.1.254/24	isp-sv
	Loopback0	192.168.0.3/32	
hq	Gi0/0	172.16.0.1/30	csw
	Gi0/1	1.1.1.1/30	isp-a1
	Gi0/2	2.2.2.1/30	isp-a2
	Gi0/3	172.16.0.5/30	vpn
vpn	Gi0/0	172.16.0.6/30	hq
	Gi0/1	172.16.0.9/30	csw
	Loopback0	100.100.100.1/32	
	Tunnel0	10.0.0.10/24	
csw	Gi0/0	172.16.0.2/30	hq
	Gi0/1	172.16.0.13/30	dsw1
	Gi0/2	172.16.0.17/30	dsw2
	Gi0/3	172.16.10.254/24 (VRF SUB所属)	subsw
	Gi1/0	100.100.100.14/29	pub-sv
	Gi1/1	10.100.0.1/24	widearea-ethernet
	Gi1/1.110	10.110.0.1/24（VRF SUB所属）	
	Gi1/2	172.16.0.10/30	vpn
dsw1	Gi0/0	172.16.0.14/30	csw
	Vlan10	172.16.10.252/24	
	Vlan20	172.16.20.252/24	
dsw2	Gi0/0	172.16.0.18/30	csw
	Vlan10	172.16.10.253/24	
	Vlan20	172.16.20.253/24	
asw	Vlan20	172.16.20.251/24	
br1	Gi0/0	3.3.3.1/30	isp-a3
	Gi0/1.10	10.1.0.254/24	br1sw
	Gi0/1.110	10.1.0.254/24 (VRF SUB所属)	
	Gi0/2	10.100.0.2/24	widearea-ethernet
	Gi0/2.110	10.110.0.2/24（VRF SUB所属）	
	Tunnel0	10.0.0.11/24	
br2	Gi0/0	4.4.4.1/30	isp-a3
	Gi0/1	10.2.0.254/24	br2-cl
	Tunnel0	10.0.0.12/24	

表２つづき：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
hq-sv	ens192	172.16.10.1/24	asw
hq-cl	ens192	172.16.20.1/24	asw
br1-cl	ens192	10.1.0.1/24	br1sw
br2-cl	ens192	10.2.0.1/24	br2
pub-sv	ens192	100.100.100.10/29	csw
isp-sv	ens192	200.99.1.1/24	isp-a3
sub-cl	ens192	10.1.0.10/24	br1sw
sub-sv	ens192	172.16.10.10/24	subsw

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
isp-a1	Gi0/0	2001:DB8:1:1::2/64	hq
	Gi0/1	2001:DB8:0:13::1/64	isp-a3
	Loopback0	2001:DB8:0:1::1/128	
isp-a2	Gi0/0	2001:DB8:2:2::2/64	hq
	Gi0/1	2001:DB8:0:23::2/64	isp-a3
	Loopback0	2001:DB8:0:2::2/128	
isp-a3	Gi0/2	2001:DB8:0:13::3/64	isp-a1
	Gi0/3	2001:DB8:0:23::3/64	isp-a2
	Gi0/4	2001:DB8:200:99:1::254/64	isp-sv
	Loopback0	2001:DB8:0:3::3/128	
hq	Gi0/0	FE80::1（リンクローカル）	csw
	Gi0/1	2001:DB8:1:1::1/64	isp-a1
	Gi0/2	2001:DB8:2:2::1/64	isp-a2
csw	Gi0/0	FE80::C0（リンクローカル）	hq
	Gi0/1	FE80::C1（リンクローカル）	dsw1
	Gi0/2	FE80::C2（リンクローカル）	dsw2
dsw1	Gi0/0	FE80::D1（リンクローカル）	csw
	Vlan20	2001:DB8:ABCD:20::D1/64	
		FE80::20D1（リンクローカル）	
dsw2	Gi0/0	FE80::D2（リンクローカル）	csw
	Vlan20	2001:DB8:ABCD:20::D2/64	
		FE80::20D2（リンクローカル）	
asw	Vlan20	2001:DB8:ABCD:20::A/64	
isp-sv	ens192	2001:DB8:200:99:1::1/64	isp-a3
hq-cl	ens192	2001:DB8:ABCD:20::1/64	asw

表４：　VLAN設定表

各スイッチのVLAN設定は、次の通りである。

（１）dsw1/dsw2のVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
10	HQSV		172.16.10.0/24	本社サーバーセグメント
20	HQCL		172.16.20.0/24 2001:DB8:ABCD:20::/64	本社クライアントセグメント

（２）aswのVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
10	HQSV	Gi0/0	172.16.10.0/24	本社サーバーセグメント
20	HQCL	Gi0/3	172.16.20.0/24 2001:DB8:ABCD:20::/64	本社クライアントセグメント

（３）br1swのVLAN設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
10	BR1CL	Gi0/1	10.1.0.0/24	支社クライアントセグメント
110	SUBCL	Gi0/2	10.1.0.0/24	子会社クライアントセグメント

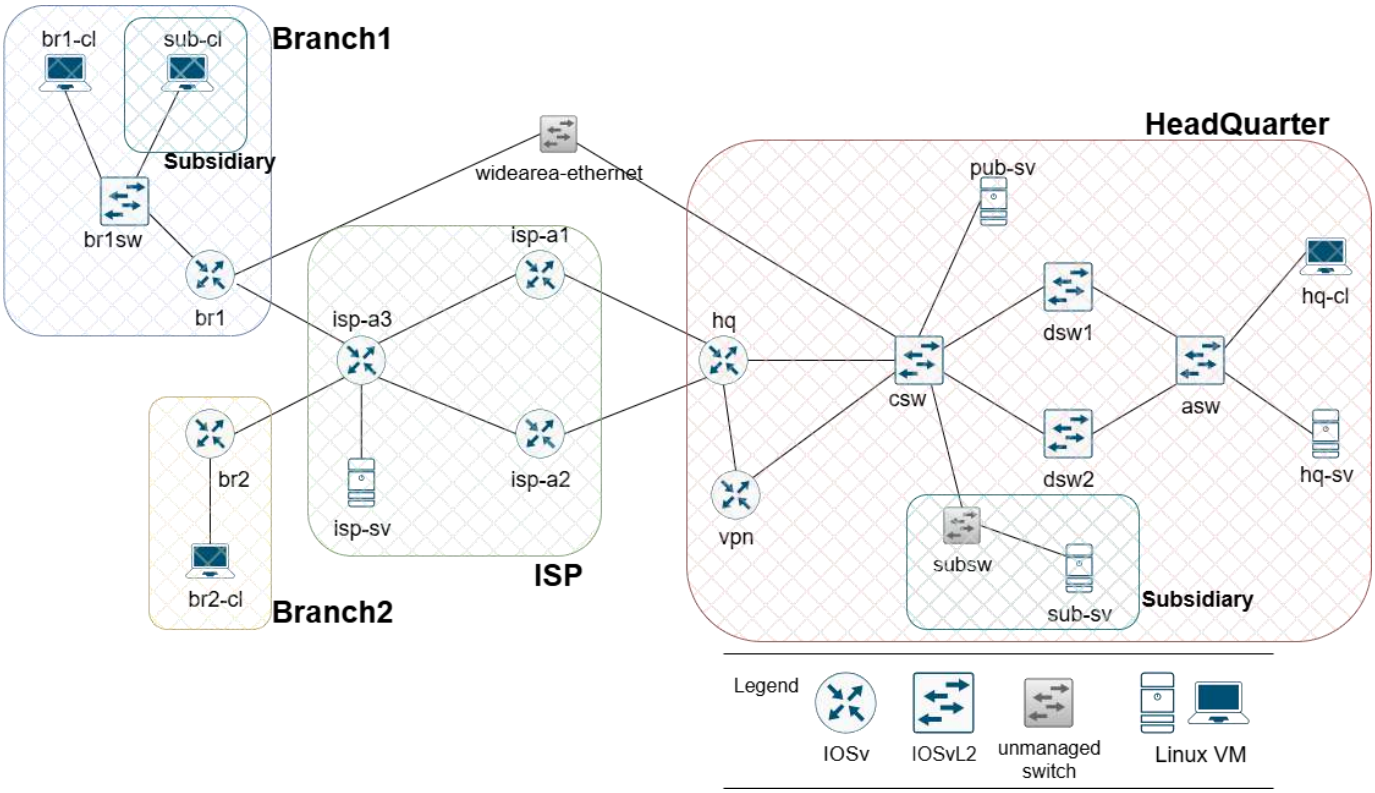
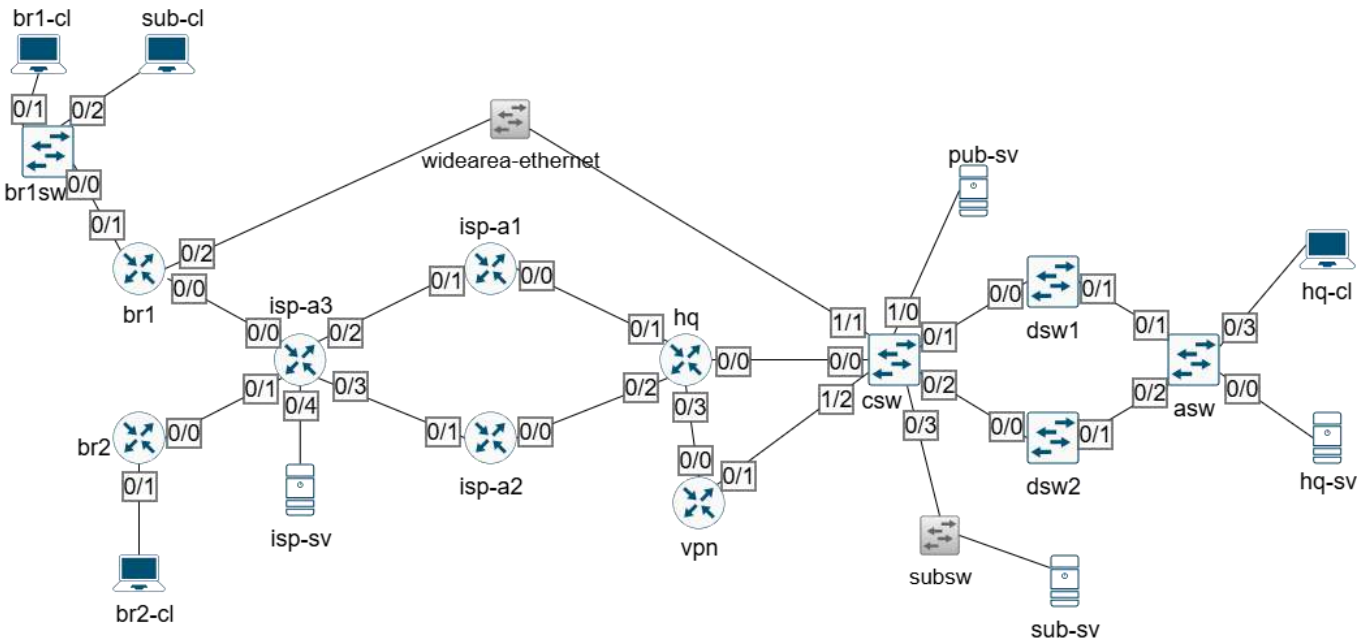


図１：ネットワークサイト構成



※本図に各ノードの接続インターフェース番号を示す。
使用インターフェースは全て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

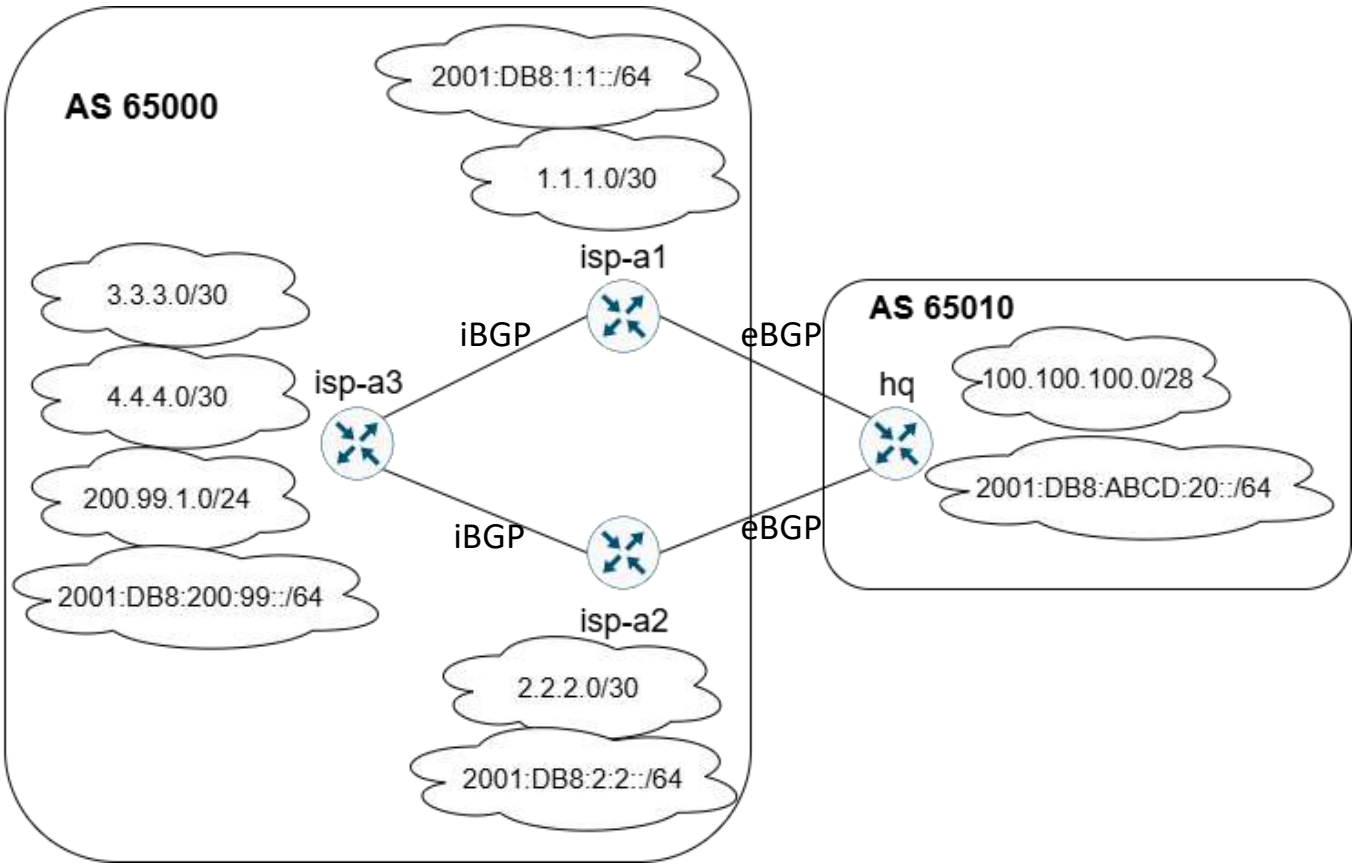


図３： BGP(IPv4/IPv6)ルーティング概要

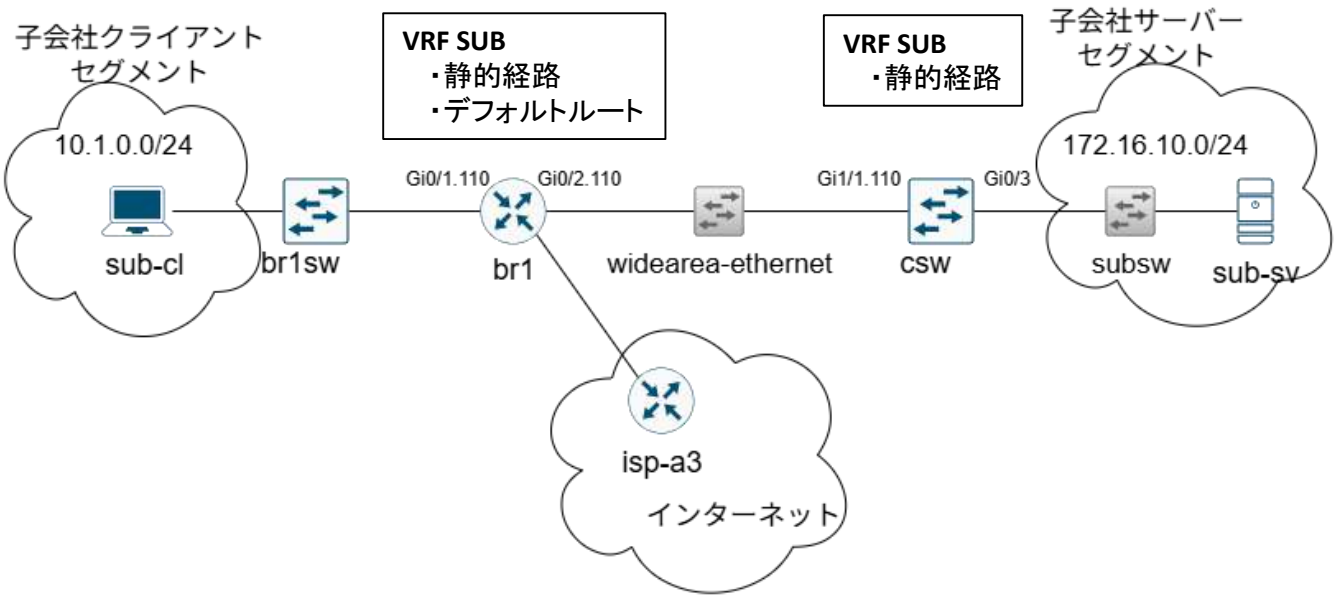


図４： 子会社ネットワーク構成概要 (VRF)

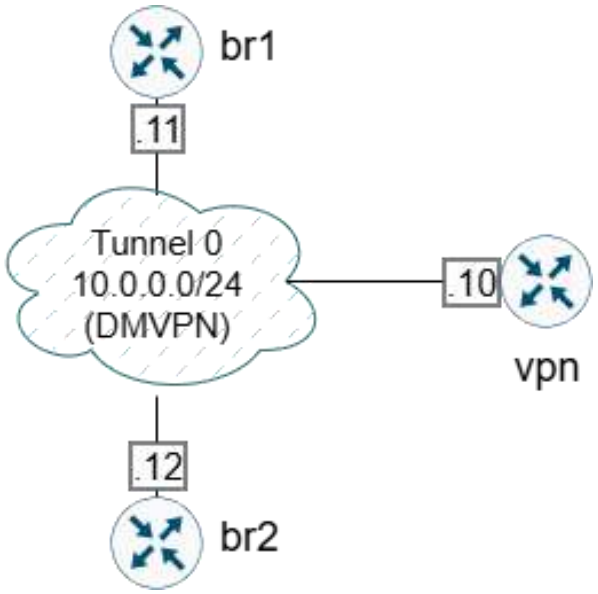


図５：DMVPN構成概要

※br1-cl所属セグメント

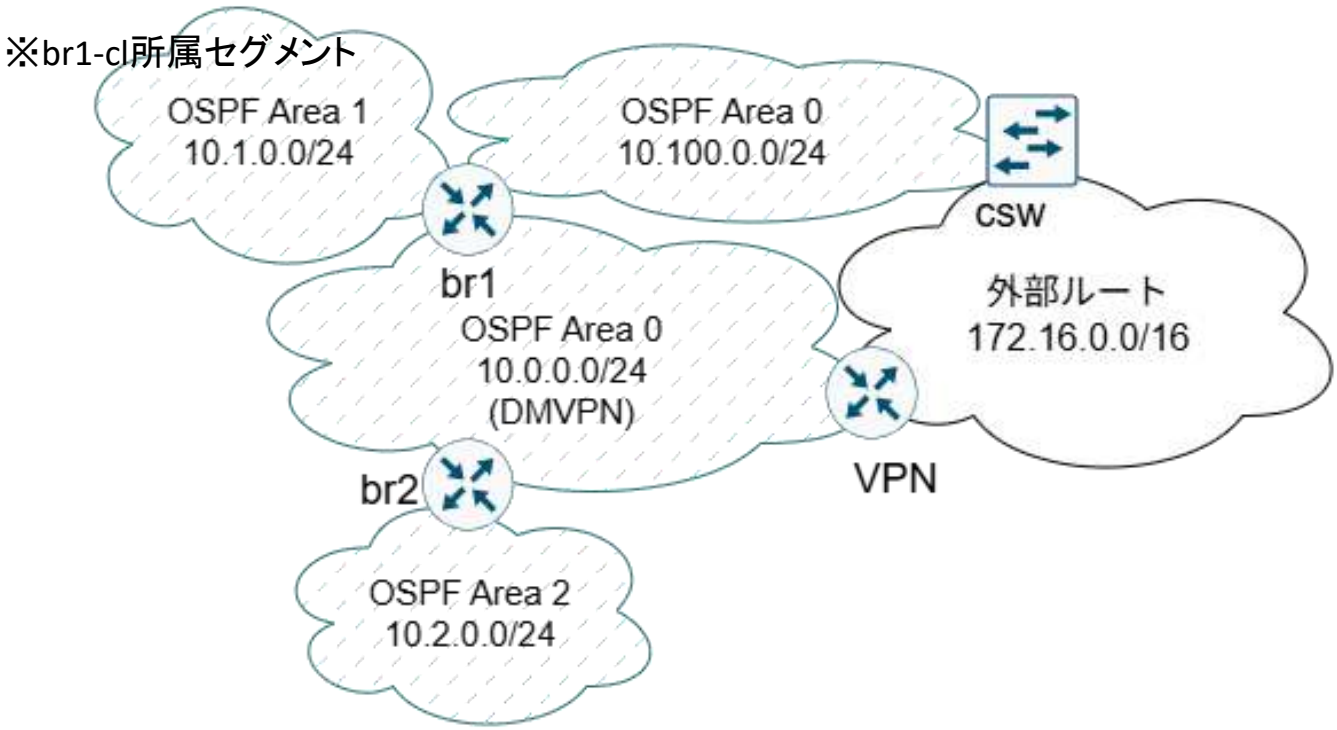


図６：OSPFルーティング概要

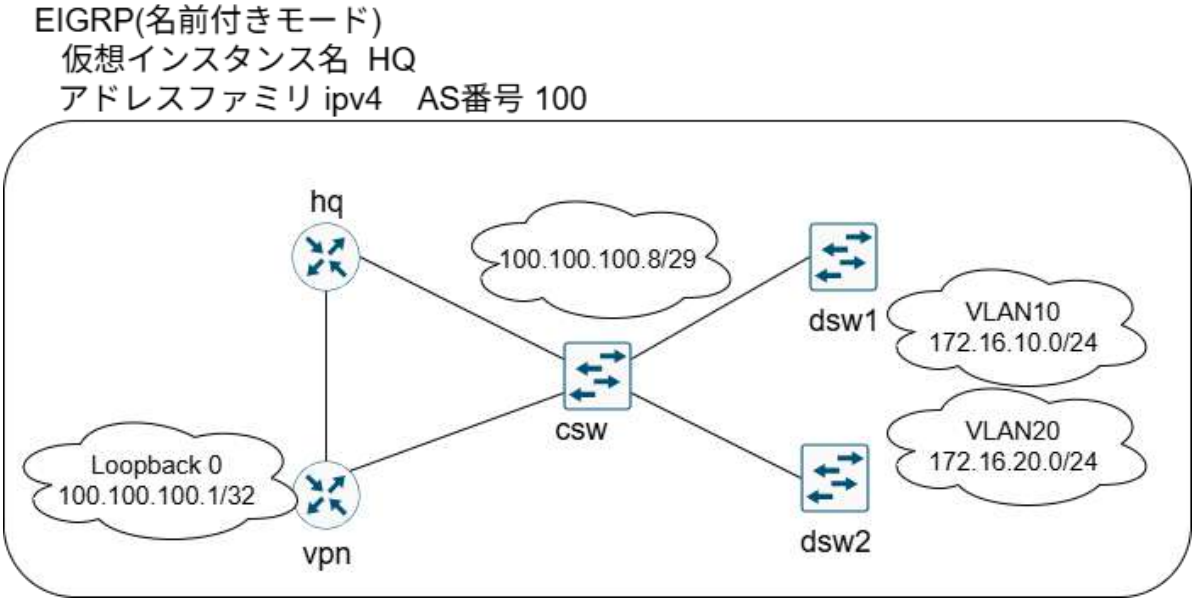


図７：EIGRP(IPv4)ルーティング概要

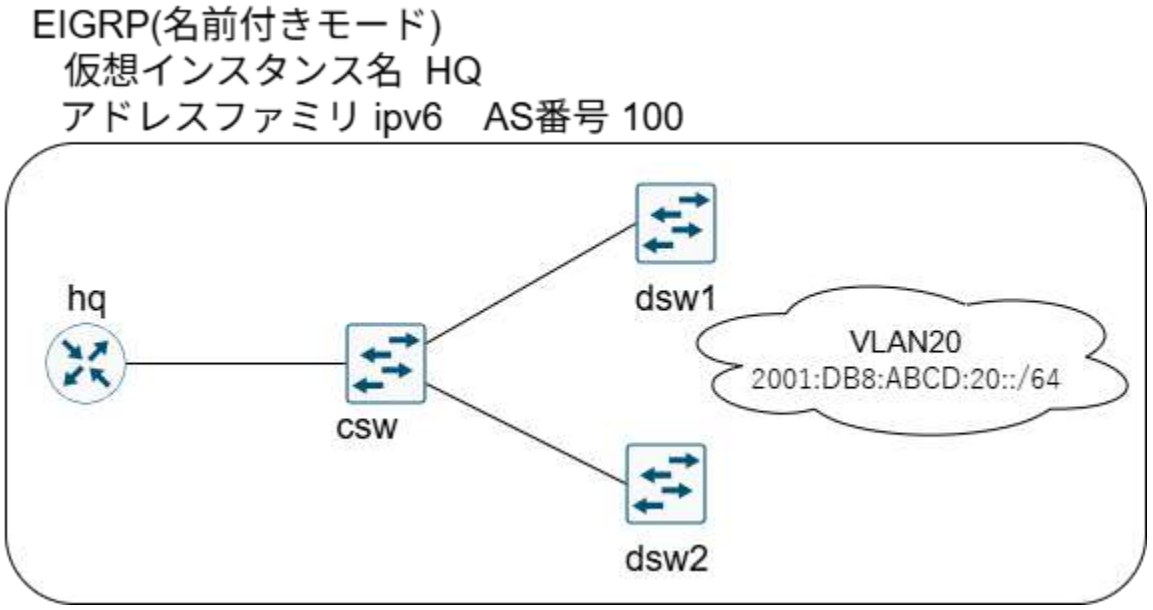


図８：EIGRP(IPv6)ルーティング概要