

公表

技能五輪全国大会
IT ネットワークシステム管理職種
参加の手引き
競技課題概要
(2023 年 第 61 回大会用)

令和 5 年 6 月 27 日
競技委員作成

1. IT ネットワークシステム管理職種概要

ネットワークを通じて提供される広範囲な IT サービスは、日常業務や一般生活において必要不可欠なものとなっており、高い信頼性が求められます。IT ネットワークシステム管理者は、IT サービスのダウンやセキュリティ侵害などのリスクを回避し、顧客が求める IT サービスを継続的に提供する責任を負っています。信頼性の高い IT サービス環境は、各種ネットワーク機器やサーバ・クライアントを適切に設定することによって構築され、運用管理されています。また、システムトラブルが発生した際は、状況を的確に判断して対処する必要があります。これらの分野の業務を担う技術者は、一般にネットワークエンジニア・サーバーエンジニア・インフラエンジニアなどと呼ばれます。

IT ネットワークシステム管理職種における競技では、上記分野における知識と技能を総合的に競います。課題としては、ネットワークシステム構築課題とトラブルシュート課題があります。ネットワークシステム構築課題では、Cisco Systems 社製ネットワーク機器の設定、Linux サーバー・Windows サーバーによる各種サービス構築やセキュリティ設定などに関する知識と技能が問われます。また、トラブルシュート課題では、課題環境としてトラブルが内包されたネットワークシステム環境が与えられ、架空のシステム利用者からのシステムトラブルに関するクレームに対して、その原因と解決方法を調査し回答することが求められます。

2. 競技日程

- 競技開始の前日 11 月 17 日（金）
 - 9:30 集合
 - 9:40～11:00 競技内容の説明、競技場所の抽選、機材の確認
 - 11:00 解散
- 競技 1 日目（競技時間：計 6 時間） 11 月 18 日（土）
 - 8:40 集合
 - 8:45～ 9:00 説明
 - 9:00～11:00 競技「課題 1 トラブルシューティング」
 - 11:00～11:50 昼食
 - 12:00～16:00 競技「課題 2 クライアント・サーバー環境」
 - 16:10 解散
- 競技 2 日目（競技時間：計 3 時間） 11 月 19 日（日）
 - 8:40 集合
 - 8:45～ 9:00 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

3. 競技に使用する主な機器と支給部品

- 仮想化ホスト PC 1 式
CPU : 第 12 世代インテル® Core™ プロセッサー、メモリ : 64GB、ストレージ : 1TB 以上
OS : VMware ESXi (VMware vSphere Hypervisor) 7.0
- 管理用 PC 1 式
OS : Windows10
- LAN ケーブル (既製品) 1~2 本
- スイッチングハブ 1 台

4. 競技に使用する主なソフトウェア

- サーバーOS : Debian GNU/Linux 11.7 bullseye、Windows Server 2022 (評価版)
 - クライアント OS : Windows10 (評価版)
 - 仮想化基盤 : VMware ESXi (VMware vSphere Hypervisor) 7.0
 - ネットワーク仮想化・シミュレーション : Cisco Modeling Labs - Personal (CML-P) 2.x
 - その他 : TeraTerm (ターミナルソフト)、Thunderbird (メーラー)、VMware Remote Console
- ※実際の競技で使用するソフトウェアバージョンは、変更になることがあります。

5. 競技課題概要

競技課題としては、トラブルシューティングの課題、および、ネットワークシステム環境を構築する課題があります。課題環境は、「4. 競技に使用する主なソフトウェア」にて提示されているサーバーOS、クライアントOS、仮想化基盤、ネットワーク仮想化の各ソフトウェアによって、仮想環境として構成されます。課題として構築が求められるサーバーなども仮想マシンです。競技課題の内容は、大きく分けて下記のA～Cがあります。

A. 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ます。複数のネットワークノード（ルータやスイッチ）、サーバー、クライアント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ます。この課題環境はトラブルが内包された状態で提供されます。架空のユーザ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ます。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います。実際にトラブルを修復したか否かは問われません。採点対象となるのは下記の項目です。

- 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こと。
 - 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）

B. クライアント・サーバー環境

B. 1 Linux サーバー環境構築

サーバーOS として、Debian Linux を使用し、競技課題として示される要求仕様に基づいて Linux サーバー環境を構築することが求められます。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ます。下記リストは採点する可能性のある評価項目の例です。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してください。

- サーバーOS および必要ソフトウェアのインストール
- Linux 設定
 - 基本設定：環境変数、ユーザ設定、ファイアウォール(iptables)など
 - ネットワーク設定：アドレス設定、デフォルトゲートウェイ、bonding など
- DNS サーバー（使用ソフトウェア：Bind）
 - 正引き、逆引き、フォワード、ゾーン転送、委任など
- Web サーバー(使用ソフトウェア：Apache、Nginx、またはその他のソフトウェア)
 - HTTP、HTTPS 応答、認証、アクセス制御、コンテンツ同期、データベース連携など
 - Web アプリケーション配備（web メールシステム、CMS、監視システムなど）
- メールサーバー（使用ソフトウェア：いずれかの SMTP サーバーソフトおよび、いずれかの受信サーバーソフト）
 - メール送受信、中継、バックアップ、メッセージ制限、暗号化など
- ファイルサーバー(使用ソフトウェア：Samba、FTP、NFS、またはその他のソフトウェア)
 - ファイル共有、認証、アクセス制限など
- プロキシサーバー/リバースプロキシ/ロードバランサ(使用ソフトウェア：Squid、Nginx、HAProxy、またはその他のソフトウェア)
 - プロキシキャッシュ、認証、アクセス制限、負荷分散、バックエンド死活監視など
- ストレージサーバー（使用ソフトウェア：iSCSI、NFS、またはその他のソフトウェア）
- ディレクトリサーバー（使用ソフトウェア：OpenLDAP、またはその他のソフトウェア）
- その他： Syslog サーバー、NTP サーバー、SSH サーバー、各種クライアント設定など

B. 2 Windows サーバー環境構築

サーバーOS として、Windows Server を使用し、課題として示される要求仕様に基づいて Windows サーバー環境を構築することが求められます。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ます。下記リストは採点する可能性のある評価項目の例です。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してください。

- サーバーOS (Server Core およびデスクトップエクスペリエンス) のインストール
- ネットワーク設定
 - アドレス設定、デフォルトゲートウェイなど
- 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 証明書サービスなど
- 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など
- 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 ターゲットなど
- 仮想化サービス
 - Hyper-V、フェールオーバークラスタリング、ライブマイグレーションなど
- その他: Web サービス (IIS)、リモートデスクトップサービス、Windows 展開サービス、Windows Server バックアップ、各種クライアント設定など

※ 課題環境については、Windows、Linux の各ノードの混在環境として出題される可能性があることに注意してください。

C. ネットワーキング環境（Cisco ネットワーク環境構築）

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ます。実機環境ではなく、Cisco Modeling Labs - Personal（Cisco VIRL）による仮想環境を用いて競技を行います。構築規模としては、6～10 台程度の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ます。下記リストは採点する可能性のある評価項目の例です。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してください。

- 基本設定
 - ホスト名、パスワード認証、権限レベル、時間/タイムゾーンなど
- インタフェース設定
 - IP アドレス (IPv4/IPv6)、帯域幅、カプセル化、論理インタフェース作成など
- 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、経路フィルタなど
- NAT/NAPT 設定
- WAN 設定
 - PPPoE、IPSecVPN、GRE、DMVPN など
- ゲートウェイ冗長化設定
 - HSRP、VRRP、GLBP など
- サービス設定
 - DHCP、NTP、Telnet、SSH、TFTP、SNMP など
- セキュリティ設定
 - ポートセキュリティ、ACL、ファイアウォールなど
- L2/L3 スイッチ設定
 - VLAN、VTP、STP、リンクアグリゲーションなど

※ Cisco ネットワークノードについて、Web インタフェースでの設定が可能な機種であっても、競技において Web インタフェースで各種設定をすることを禁止します。

6. 採点および評価基準

採点では次の点を採点基準に基づき評価します。

- トラブルシューティングについて
 - トラブルの原因と解決方法について、正確な内容を明確な文章で報告しているか。
- 環境構築課題について
 - 課題で要求されたシステムが正確に実現されているか。

配点割合は、「A. トラブルシューティング」が 30%以下、「B. クライアント・サーバー環境」が 50%以下、「C. ネットワーキング環境」が 40%以下です。最終的な課題配点は、この配点割合の範囲内で合計 100%となるように調整されます。時間に応じた加点はありません。ただし、同点の場合には作業時間の短い方を上位とします。

7. 持参工具等

- 筆記用具等

8. 競技上の注意事項

- ✓ 各種マニュアル、参考書、ノート等の持ち込みは一切認めない。
- ✓ ソフトウェアの持ち込みは一切認めない。
- ✓ 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）の間に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。

9. 競技環境

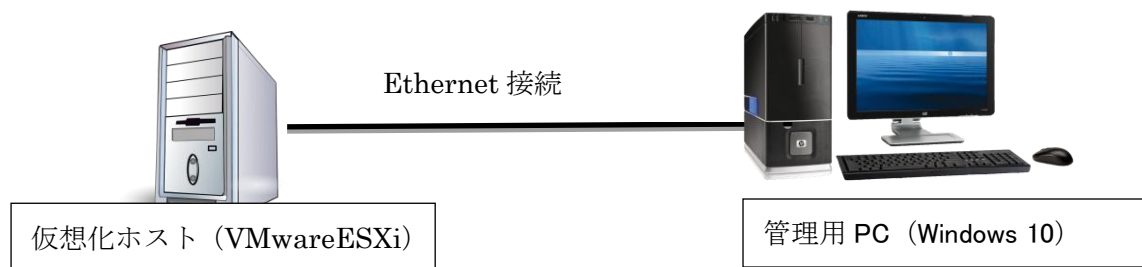


図 1：物理接続

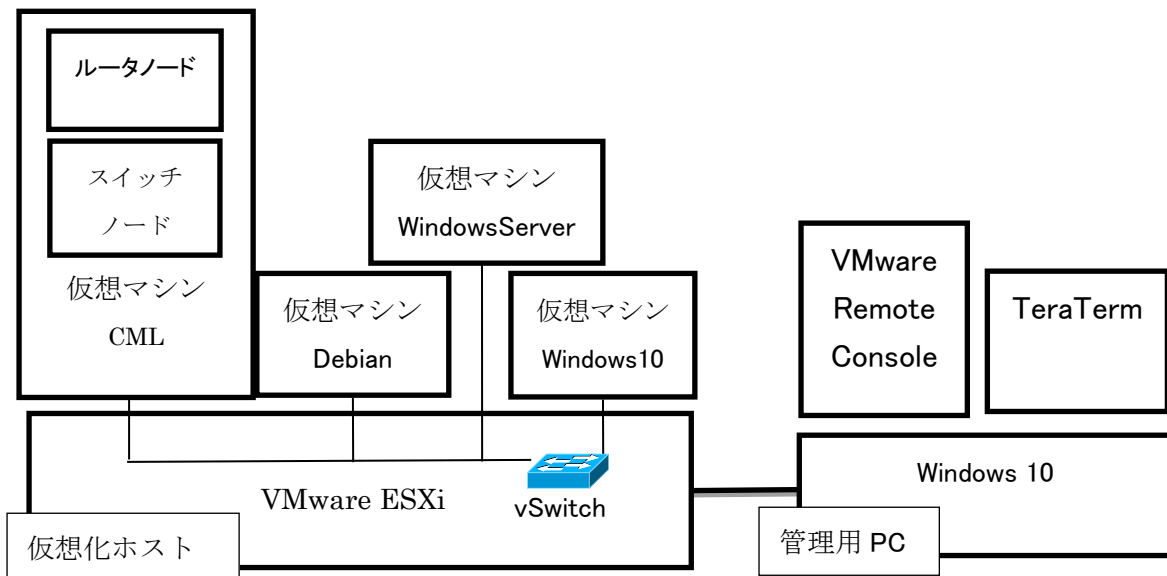


図 2：ソフトウェア配置イメージ

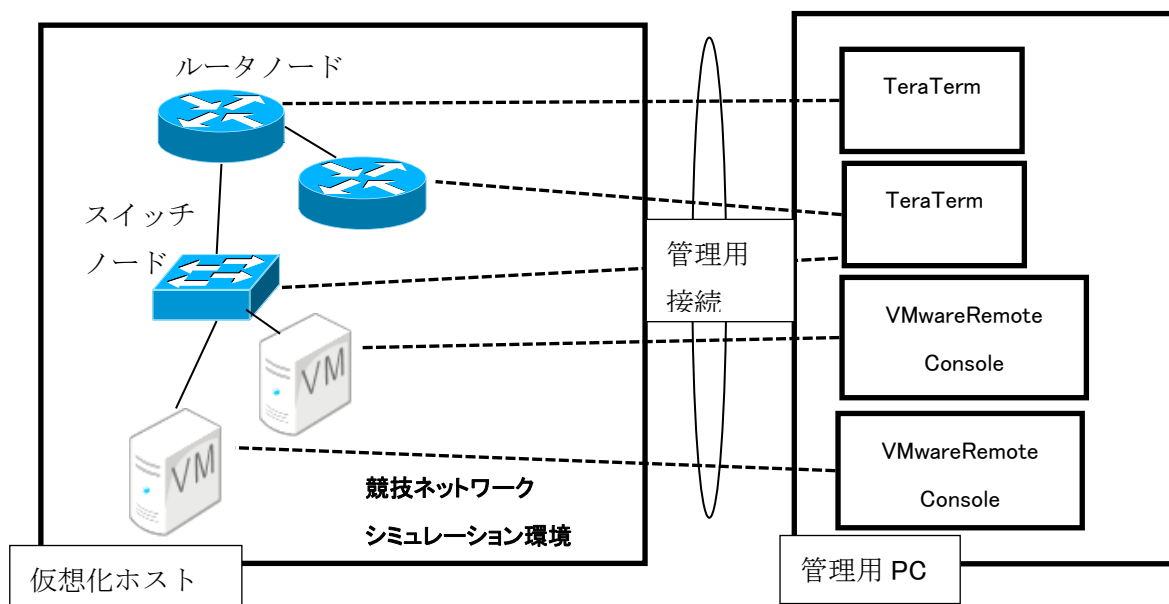


図 3：論理接続イメージ

本職種では、Cisco Modeling Labs - Personal (CML-P) および VMware ESXi を用いた仮想環境で競技を行います。

前項図 1 に示すように仮想化ホスト 1 台と管理用 PC 1 台を接続した環境で競技を実施します。前項図 2 に示すソフトウェア環境は競技委員によってセットアップされた状態で提供されます。ただし、競技として構築するサーバーについては、OS 未インストール状態の仮想マシンに対して OS のインストールを要求される場合があります。仮想ネットワーク環境 CML-P についても競技委員によってセットアップされた状態で提供されます。各ルータノード・スイッチノード・ファイアウォールノードおよびサーバー仮想マシン・クライアント仮想マシンは、仮想ネットワークに配置され、各ノード間も接続済みの状態で提供されます。仮想ネットワーク上の各ノードと VMware ESXi 上の各仮想マシンは、ESXi の仮想スイッチ (vSwitch) 経由で接続されますが、それらの設定作業は競技委員が行います。

競技開始時点において、ネットワークシミュレーションは起動された状態とします。各ルータノード・スイッチノード・ファイアウォールノード・仮想マシンも起動している状態です。この時、前項図 3 のように管理用 PC から各ノードへの接続が可能な状態となっています。各ルータノード・スイッチノード・ファイアウォールノードへの接続には、TeraTerm が使用可能です。各仮想マシンへの接続には VMware Remote Console が使用可能です。選手は課題の要求を満たすために各ノードを操作することができます。シミュレーションの開始処理は競技委員が競技開始前に行います。また、競技中や競技終了時において、ネットワークシミュレーションを終了する操作は行わないでください。

CML-P 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は次の通りです。

a) 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

b) スwitch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

c) 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

d) 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ありません。

e) 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ありません。

10. 参考資料

次項以降に過年度課題の一部省略版を添付します。また、技能五輪は国際大会（WorldSkills）の日本代表選手を選考する大会でもあります。そのため、技能五輪の競技課題内容は、国際大会（WorldSkills）競技課題との整合化をできるかぎり図っていく方針です。

前回の国際大会（WorldSkills2022）の競技課題については、

<https://worldskills.org/internal/competition-documentation/special-edition-2022/test-projects/>

前前回の国際大会（WorldSkills2019）の競技課題については、

<https://worldskills.org/internal/competition-documentation/worldskills-kazan-2019/test-projects/>

にて入手できます。ただし、アカウント登録（無料）が必要です。参考にしてください。

参考資料 A 第 60 回大会 課題 1（一部省略版）

参考資料 B 第 60 回大会 課題 2（一部省略版）

参考資料 C 第 60 回大会 課題 3（一部省略版）

参考資料 D 第 59 回大会 課題 1（一部省略版）

参考資料 E 第 59 回大会 課題 2（一部省略版）

参考資料 F 第 59 回大会 課題 3（一部省略版）

参考資料 G 第 58 回大会 課題 1 概要

参考資料 H 第 58 回大会 課題 2（一部省略版）

参考資料 I 第 58 回大会 課題 3（一部省略版）

参考資料 J 第 57 回大会 課題 1（一部省略版）

参考資料 K 第 57 回大会 課題 2（一部省略版）

参考資料 L 第 57 回大会 課題 3（一部省略版）

参考資料 A 第 60 回大会競技課題 課題 1 (一部省略版)

第 60 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

競技課題及び作業完了報告書

令和 4 年 11 月 5 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。(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。
- ✓ CML²のネットワークシミュレーションの停止および接続の変更はしないこと。
- ✓ 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	

競技課題の背景

「あなた」は、株式会社千葉スキルズに勤務する社内のサーバやネットワークを構築・運用管理する管理室の社員である。本社では明日 PC 教室（PCROOM）の開業を控えており、事務所、講師室が 2 部屋および管理室がある。PC 教室開業に伴い最近、講師室および PC 教室を新設した。

各部署からトラブルシュートの依頼が入っていて、管理担当の「あなた」は同僚とともに原因の調査とトラブルを解決しなければならない。

次頁以降のトラブルに対して適切な原因の把握と対応した処置内容を、各報告書に記載しなさい。なお、記載は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ことがポイントとなる。

- 「トラブルの原因」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
(課題によっては、架空の依頼者（トラブル報告者）への返答内容を含む)
- 本競技は報告書に記載された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。

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、管理用 PC に Wireshark.iso として用意しているものを適時利用すること。なお、課題はパケットキャプチャを利用しなくても解決可能となっている。

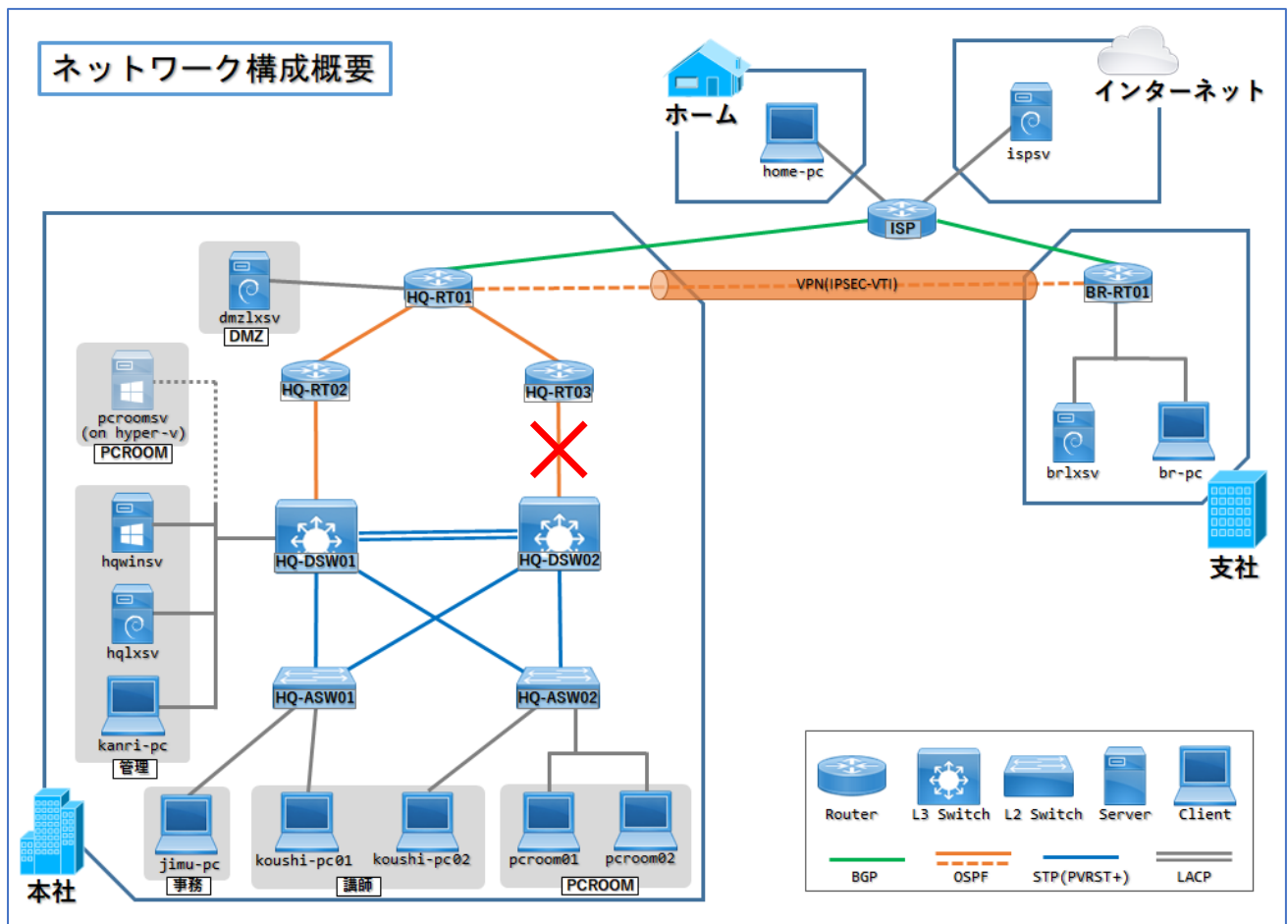
ネットワーク構成の概要

ネットワーク構成は課題環境資料（事前公開用）を参照しなさい。

また、競技は昨夜地震が本社地域に停電が発生した想定となっている。停電はすでに復旧をしているが、機器のリンクランプを確認したところ、HQ-RT02 と HQ-DSW02 間のリンクランプが消灯(※)しており、ケーブルが断線したものと想定され、ケーブルの即時復旧はできない状況である。ネットワーク構成上、冗長構成のため業務に支障は出ないはずだが・・・。

また明日の PCROOM の開業にともない、各装置の設定が完全でない個所もあるようだ。

※CML²の仕様上、競技環境では HQ-RT02 と HQ-DSW02 間は結線されていないが、各々のポートは up 状態になってしまう。



なお各 Web サーバにアクセスした場合に表示される画面イメージを以下に示す。ただし、CML²の転送速度が遅く画像が表示されない場合があり、画像以外の文字が表示されていれば、接続が確認できたと見なしてよい。



<http://tokyo-skills.jp/>



<http://world-skills.net/>



<http://www.chiba-skills.local>

課 題 1	神谷講師が、koushi-pc02 では、ログインできたが、明日の講座の準備で pcroom01 において自分のアカウントでログインしようとしたが、できなかったと連絡があった。なお今朝、佐々木講師はログインできたようだ。pcroom01 で神谷講師のアカウントでログインができるようにしてください。
原 因	
処置内容	措置に関する作業手順はすべて記載すること。

課 題 2	停電の影響を確認するために、「あなた」は kanri-pc から HQ-ASW01 に ping を飛ばしたが応答がなく、SSH によるログインもできなかった。kanri-pc から HQ-ASW01 に接続できない原因を調査しトラブルを解決してください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 3	新井講師から koushi-pc01 でメールが送信できないのでメールを使用できるようにしてください、と依頼された。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 4	jimu-pc からインターネットの閲覧ができなくなったと倉田さんから報告が入った。インターネットの閲覧ができるようにしてあげてください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 5	「あなた」は後輩の鈴木から kanri-pc から chiba-skills.local に ping を飛ばすと、応答があるが hqlxsv から chiba-skills.local に ping を飛ばすとエラーになるが原因がわからないと相談された。運用上は問題ないなと思いつつも、後輩な悩みを解決するため hqlxsv からでも応答があるように修正しなさい。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

参考資料 B 第 60 回大会競技課題 課題 2 (一部省略版)

第 60 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

(一部省略版)

2022 年 11 月 5 日(土) 12:00～16:00(4 時間)

目 次

競技に関する注意事項	P.1
競技課題の背景と概要	P.2～P.3
競技環境(仮想環境)に関する注意事項	P.4
競技課題	P.5～P.10

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。机の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 **chiba-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」に接続されている(別紙図 1「ネットワーク構成図」参照)。また、各サイトでは自ネットワーク以外を「外部ネットワーク」と呼ぶ。

1. tokyo-skills.jp

- ・1 台のルータ **R-Tky** 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 **tstv1**、**tstv2**、**tstv3** 及びクライアント **t-client** が配置される。
- ・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、及び適切な経路の設定。
- ・**tstv1** と **tstv2** の IP アドレスをそれぞれ **201.10.0.2** と **201.10.0.3** へ静的に変換する NAT 設定。
- ・**Internal** ネットワークと **chiba-skills.jp** の **Internal** ネットワーク間の GRE over IPsec VPN 設定。
- ・アクセス制御は未設定である。

2. osaka-skills.jp

- ・1 台のルータ **R-Osk** 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 **osv** とクライアント **o-client** が配置される。
- ・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. 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、及び適切な経路の設定。
- ・**osv** の IP アドレスを **201.10.0.18** へ静的に変換する NAT 設定。
- ・**Internal** ネットワークノードの IP アドレスを **201.10.0.17** へ動的に変換する NAPT 設定。
- ・アクセス制御は未設定である。

3. chiba-skills.jp

- ・1 台のファイアウォール **cfw** 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 **csv1** が、**Internal** ネットワークにはサーバ **csv2** とクライアント **c-client** が配置される。
- ・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. csv1

- ・別紙表 2「サーバ、クライアントの 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。
- ・下記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に応答する。
- ・MX レコードの問い合わせに **csv1** のアドレスを返す。

3.1.2. メールサービス

- ・**csv1** 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。

3.1.3. Web サービス

- ・Web サービスが稼働しており、80 番ポートへの接続に応答する。

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。各自の設定確認のためにこれらのサービスを利用して構わない。

4.1.1. DNS サービス

- ・sv.itnetsys.org、www.itnetsys.org の正引き要求に応答する。
- ・itnetsys.orgドメインの MX レコードが登録されている。

4.1.2. Web サービス

- ・http://www.itnetsys.org のリクエストに応答する。

4.1.3. SMTP サービス

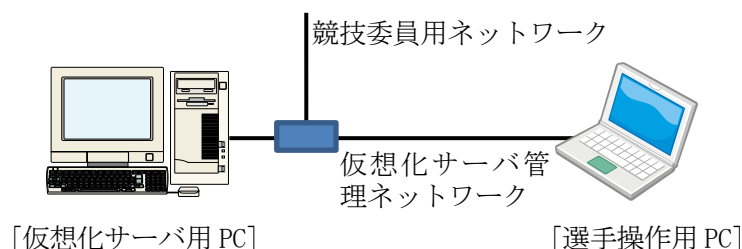
- ・manager@itnetsys.org 宛のメールを受信可能である。また、この受信メールに対して Subject「Auto Reply Mail」の空メールが自動返信される。

4.2. ex-client

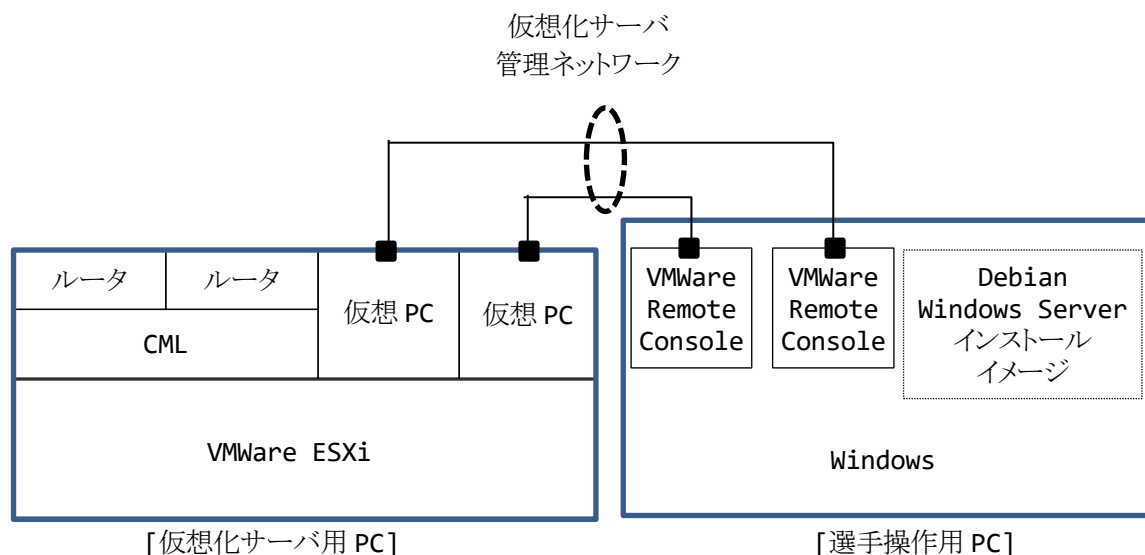
各自の設定確認のため自由に利用して構わない。

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「ショートカット」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。
- 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-Tky、R-Osk の操作を禁止する。
- Debian のインストールイメージ `debian-11.3.0-amd64-BD-1.iso` 及び Windows Server のインストール イメージ `17763.1158.200413-1759.rs5_release_svc_refresh_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**、**cfw**、**csv2**、**c-client**、**osv**、**o-client** である。
- ・採点対象ノードは別紙表 2 に記す OS が GUI 環境でインストール済みである。
- ・**tsv3** にはシステムドライブ以外に、各 1GB の HDD(未初期化)ディスク 1、ディスク 2、ディスク 3 が接続済である。
- ・課題ではパスワードなどの設定文字列を二重引用符(“”)で囲って示しているが、二重引用符を含めず設定すること。
- ・課題にある“ユーザ名”は各ユーザのユーザ名を示す。例えば、ユーザ名が **user01** の場合 `/home/“ユーザ名”` は `/home/user01` を示す。
- ・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が、競技委員はその作業に係る質問、トラブル等には一切対応しない。

1. 基本設定

- ・別紙表 1、2 を参考に各ノードに IP 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は各自の判断でインストールすること。

2. tokyo-skills.jp

2.1. tsv1

2.1.1. Active Directory

- ・tokyo-skills.jp のドメインコントローラを設定する。
 - ・tokyo-skills.jp ドメイン直下に **Accounts** と **Managers** の OU を作成する。
 - ・OU **Accounts** に **G_Accounts** グローバルグループを作成する。
 - ・OU **Managers** に **G_Managers** グローバルグループを作成する。
 - ・作成するユーザのパスワードは“**Skills2022**”とする。
 - ・OU **Accounts** にユーザ **win01** と **win02** を作成する。
 - ・OU **Managers** にユーザ **win03** と **win04** を作成する。
- 一部省略

2.1.2. DNS サーバ

- ・**www.tokyo-skills.jp** の正引き問合せに **tsv1** の IP アドレスを応答する。
- ・**www2.tokyo-skills.jp** の正引き問合せに **tsv1** の IP アドレスを応答する。

A) 外部ネットワーク向け

- ・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。
 - ・再帰問い合わせを許可しない。
- 一部省略

2.1.3. DHCP サーバ

- ・Internal ネットワークに **192.168.101.201**～**220** の IP アドレスを配布する。
- ・DNS サーバとして **tsv1** 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。

2.1.4. Web サーバ

- ・「<http://www.tokyo-skills.jp/>」の要求に対し、文字列“Tokyo Skills LTD”を表示する。
- ・「<https://www2.tokyo-skills.jp/>」の要求に対し、文字列“SSL Site”を表示する。
- ・認証局(osv)により署名されたサーバ証明書を利用する。

2.1.5. グループポリシー

- ・G_Accounts グループに所属するユーザに対し¥¥TSV3¥Accounts を Y:ドライブに割り当てる。
- ・G_Managers グループに所属するユーザに対し¥¥TSV3¥Managers を Y:ドライブに割り当てる。

2.2. tsv2

2.2.1. Active Directory

- ・使用するパッケージは winbind、libpam-winbind、libnss-winbind、krb5-config とする。
- ・tokyo-skills.jp ドメインのメンバとする。
- ・ドメインユーザでログインできること。
- ・ドメインユーザのホームディレクトリを/home/“ユーザ名”とする。
一部省略

2.2.2. iSCSI イニシエータ

- ・使用するパッケージは open-iscsi とする。
- ・iSCSI ターゲットの仮想ディスクを/iscsi にマウントする。
- ・システム起動時に自動マウントされること。

2.2.3. 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。
一部省略

2.3. tsv3

2.3.1. Active Directory

- ・tokyo-skills.jp ドメインのメンバとする。
- ・tokyo-skills.jp のドメインコントローラ(グローバルカタログは持たない)を設定する。

2.3.2. RAID

- ・ディスク 1、ディスク 2、ディスク 3 を用いて RAID5 を構成する。
- ・RAID5 ドライブを NTFS でフォーマットし V:ドライブに割り当てる。

2.3.3. ファイルサーバ

- ・V:¥Home を共有名 Home で共有する。
- ・V:¥Profile を共有名 Profile で共有する。
一部省略

2.3.4. 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。

2.4. t-client

2.4.1. OS の設定

- ・tsv1 の DHCP サーバから IP アドレス等の割り当てを受ける。
- ・“tokyo-skills.jp”ドメインのメンバとする。
一部省略

2.4.2. Web ブラウザ(Microsoft Edge)

競技終了時にログインしているユーザにより以下の設定となっていること。

- ・「<http://www.itnetsys.org>」サイトが閲覧できること。
- ・「<https://www2.tokyo-skills.jp/>」サイトが閲覧できること。

3. osaka-skills.jp

3.1. osv

3.1.1. 認証局

- ・CA 証明書は/ca/cacert.pem に保存すること。
- ・設定項目は以下のとおりとする。
Country Name: JP
State or Province Name: Osaka
Organization Name: Osaka Skills LTD
Common Name: ca.osaka-skills.jp
- ・競技課題の仕様から CA 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。

3.1.2. DNS サーバ

- ・使用するパッケージは bind9 とする。
- ・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

- ・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。
- ・再帰問い合わせを許可しない。

B) Internal ネットワーク向け

- ・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。
一部省略

3.1.3. 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 192.168.102.101～200 の IP アドレスを配布する。
- ・DNS サーバとして osv のアドレスを通知する。
一部省略

3.1.4. LDAP サーバ

- ・使用するパッケージは **slapd** とする。
- ・管理者パスワードは“**Skills2022**”とする。
- ・5 個の LDAP ユーザ **user01**～**user05** を作成する。パスワードは“**pass**”とする。
一部省略

3.1.5. Web サーバ

- ・使用するパッケージは **apache2** とする。
- ・認証局(**osv**)により署名されたサーバ証明書を利用する。なお、サーバ証明書の名前は **newcert.pem** とし/**etc/ssl/www** ディレクトリに保存すること。
- ・「**https://www.osaka-skills.jp/**」の要求に対し、文字列“**Osaka Skills LTD**”を表示する。
- ・HTTP 要求は HTTPS へリダイレクトする。
一部省略

3.1.6. メールサーバ

- ・使用するパッケージは **postfix** 及び **dovecot-pop3d** とする。
- ・認証局(**osv**)により署名されたサーバ証明書を利用する。なお、サーバ証明書の名前は **newcert.pem** とし/**etc/ssl/mail** ディレクトリに保存すること。
- ・LDAP サーバに登録されたユーザを用いて SMTP 認証を行う。
- ・SMTP 認証の成功したクライアント及び自身からのみメールの転送を許可する。
- ・LDAP サーバに登録されたユーザ宛のメールをスプールする。
- ・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。

3.1.7. NFS サーバ

- ・使用するパッケージは **nfs-kernel-server** とする。
- ・/**var/ldap-home** を共有ディレクトリとする。
- ・/**var/ldap-home** ディレクトリは **Internal** ネットワークへ、読み書き可能な状態で NFS マウントを許可する。

3.2. o-client

競技終了時にログインしているユーザで以下の設定となっていること。

3.2.1. OS の設定

- ・**osv** の DHCP サーバから IP アドレス等の割り当てを受ける。
- ・LDAP サーバを用いたユーザ認証を行いローカルシステムにログインできること。
- ・競技終了時に LDAP ユーザ **user05** がログイン状態とする。
- ・LDAP サーバに登録されたユーザが初めてログインする際ホームディレクトリが自動作成されること。

3.2.2. NFS クライアント

- ・使用するパッケージは **nfs-common** とする。
- ・**osv** の共有ディレクトリ/**var/ldap-home** を/**mnt/ldap-home** へマウントする。
- ・システム起動時に自動マウントされること。

3.2.3. メールクライアント

- ・Thunderbird を利用し LDAP ユーザ **user05** でメールの送受信が可能であること。

3.2.4. Web ブラウザ

- ・Firefox を用い「https://www.osaka-skills.jp/」サイトが閲覧できること。
- ・上記サイト閲覧の際、“潜在的なセキュリティリスクあり”の警告が表示されないこと。

4. chiba-skills.jp

4.1. cfw

4.1.1. サイト間 VPN

tokyo-skills.jp の Internal ネットワークと GRE over IPsec VPN を設定しなさい。

- ・使用するパッケージは strongswan とする。
- ・Tun0 の名前でトンネルインタフェースを作成し IP アドレスを 10.1.1.2 とする。
- ・暗号化アルゴリズムは aes 256 を用いる。
- ・ハッシュアルゴリズムは sha 256 を用いる。
- ・事前共有鍵認証方式を用い、“MAKUHARI”をパスフレーズとする。
一部省略

4.1.2. 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 csv1 の IP アドレスを 201.10.0.10 へ静的に変換する。
- ・外部ネットワークと通信するために Internal ネットワークノードの IP アドレスを 201.10.0.9 へ動的に変換する。

4.1.3. ファイアウォール

- ・使用するパッケージは nftables とする。

A) 着信トラフィック

- ・発信トラフィックの戻りトラフィックを許可する。
- ・GRE over IPsec VPN に係るトラフィックを許可する。
- ・cfw 自身への ping トラフィックを許可する。
- ・csv1 への http、smtp、DNS、ping トラフィックを許可する。
- ・上記以外のトラフィックを拒否する。

B) 発信トラフィック

- ・GRE over IPsec VPN に係るトラフィックを許可する。
- ・cfw からの ping 応答トラフィックを許可する。
- ・DMZ ネットワークからのトラフィックを許可する。
- ・Internal ネットワークから外部ネットワークへの http トラフィックを許可する。
- ・Internal ネットワークから csv1 への pop3、smtp、DNS、ping トラフィックを許可する。
- ・上記以外のトラフィックを拒否する。

4.2. csv2

4.2.1. Active Directory

- ・使用するパッケージは samba、krb5-config、winbind とする。
- ・chiba-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“Skills2022”とする。
- ・5 個のドメインユーザ dom01～dom05 を作成する。なお、パスワードは“Skills2022”とする。
- ・移動ユーザプロフィールを/var/lib/samba/profiles に置く。
一部省略

4.2.2. DNS

- ・ **samba** 内臓の DNS サーバを利用する。
 - ・ **Internal** ネットワークにサービスを提供する。
 - ・ 自身で名前解決が行えない場合は **csv1** へ問い合わせる。
 - ・ **chiba-skills.jp** 正引きゾーンを管理する。
 - ・ **192.168.1.0** 逆引きゾーンを管理する。
- 一部省略

4.3. c-client

競技終了時にログオンしているユーザで以下の設定となっていること。

4.3.1. OS の設定

- ・ “**chiba-skills.jp**”ドメインのメンバとする。
- ・ ドメインユーザがログオンした際、**Z:**ドライブにホームディレクトリが割り当てられること。
- ・ **Internal** ネットワーク内ノードからの **ICMP** 要求に応答すること。

4.3.2. メールクライアント

- ・ **Thunderbird** をインストールする。
- ・ **csv1** の登録ユーザ **taro** でメールの送受信を可能とする。

参考資料 C 第 60 回大会競技課題 課題 3 (一部省略版)

第 60 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

(一部省略版)

2022 年 11 月 6 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。
- ✓ 競技時間内に作業が終了した場合、VIRL(CML-P)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の **startup-config** 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。
- ✓ VIRL(CML-P)の web インターフェースへ接続することは許可しない。
- ✓ ネットワーク構成図における ISP および ISP srv は競技委員が用意する構成済みの「仮想的なインターネットエリア」である。実際のインターネットには接続されていないが、競技課題中では単に「インターネット」あるいは「外部ネットワーク」と呼ぶ。
- ✓ 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、IP 到達性について、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 構成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（IT SKILLS LTD）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(本社)/Tokyo/Makuhari** の各拠点が存在する。Headquarter には **client-hq** が接続するクライアントセグメントと **hq-srv** が接続する社内サーバーセグメントがある。Tokyo には **tokyo-srv** が接続するサーバーセグメントがある。Makuhari には **client-m** が接続するクライアントセグメントがある。Headquarter -Tokyo 拠点間の接続は、インターネット（ISP）経由の IPsecVPN によって到達性とセキュリティを確保する。Headquarter -Makuhari 拠点間の接続は、通信事業者がサービスする広域イーサネットによって冗長性を確保する。検証環境においては、広域イーサネット環境を **widearea-ether1,2**（管理機能なしスイッチノード）にて代替する。Makuhari 拠点からのインターネット接続、および、Tokyo 拠点への接続については、Headquarter 経由で行うものとする。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、Headquarter(本社)/Tokyo/Makuhari 各拠点のネットワークノードである。ISP、および各端末（ISP srv, tokyo-srv, hq-srv, client-hq, client-m, client-ext）は設定済みである。また、**unmanaged-sw1,2** および **widearea-ether1,2** については、管理機能なしスイッチノードであり設定不要である。

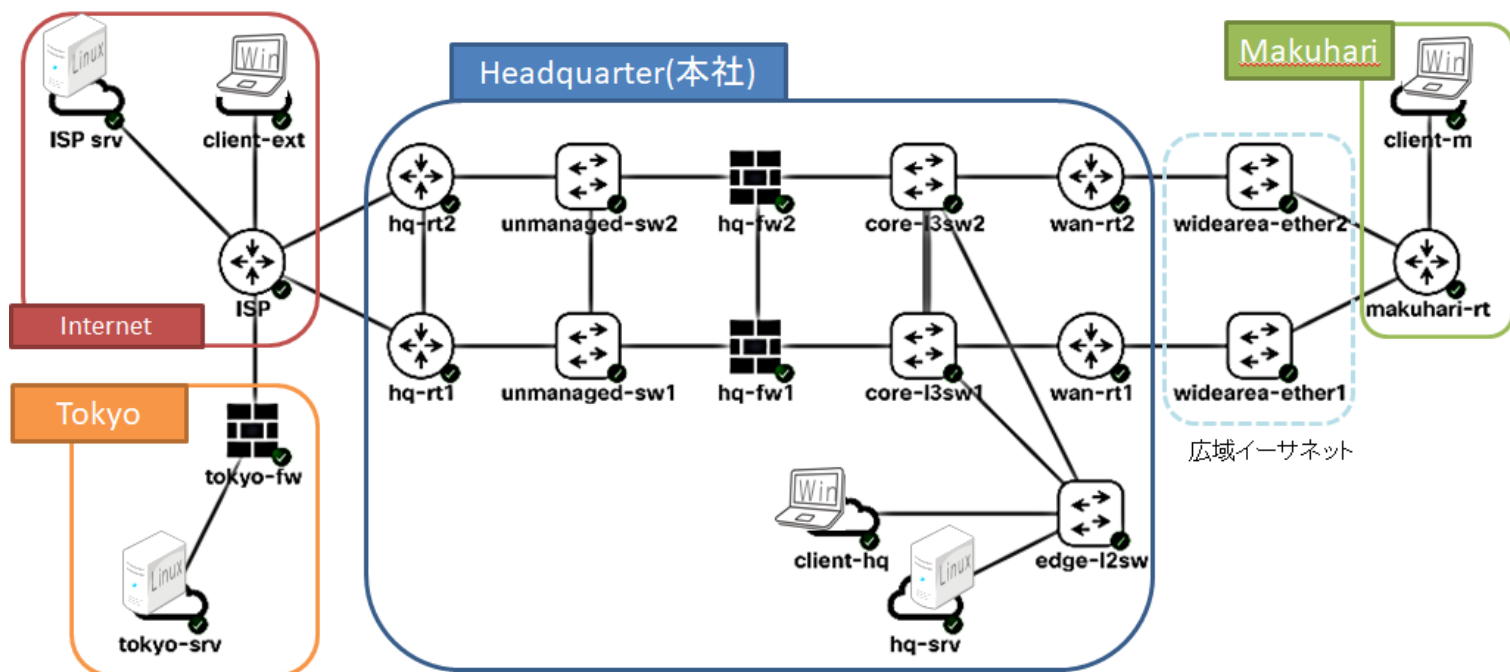


図1: ネットワークサイト構成

2 仮想マシンに関する基本情報

2.1. サーバー仮想マシン tokyo-srv、hq-srv 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、Debian11.3 がインストールされており**設定済み**である。下表に設定および動作の概要を示す。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	pass

仮想マシン : tokyo-srv

ホスト名	tokyo-srv.skills.it.jp
IP設定	IP: 192.168.100.1/24 GW: 192.168.100.254 DNS: 127.0.0.1
DNS サービス	• skills.it.jpドメインのマスタサーバーとして動作している。 • tokyo-srv.skills.it.jpの正引きが登録されている。 • 社内向けに hq-srv.skills.it.jpの正引きが登録されている。 • 社内向けに hq-srv6.skills.it.jpの正引き(AAAA)が登録されている。 • skills.it.jpドメインのMXレコードが登録されている。 • 保持していないレコードの問い合わせについては、ISP srvへ回送する。
SMTP サービス	• skills.it.jpドメインのSMTPサーバーとして動作している。 • 自ドメイン宛でのメールをスプールする。 • クライアントからのメール送信をサブミッションポートにて受け付ける。
IMAP サービス	• IMAPサービスが動作している。 • プレーンテキスト認証が許可されている。

仮想マシン : hq-srv

ホスト名	hq-srv.skills.it.jp, hq-srv6.skills.it.jp
IP設定	IP: 10.0.250.1/24 GW: 10.0.250.254 DNS: 192.168.100.1 IPv6: 2001:db8:250::100/64 GW: fe80::1
SAMBA サービス	• /shareが共有名shareとして共有されている。 • 共有へのアクセスアカウントとして、smbuserおよびro_smbuserが登録されている。いずれもパスワードは pass である。 • smbuserは読み書き可、ro_smbuserは読み取りのみ許可されている。
WEB サービス	• IPv4サイト https://hq-srv.skills.it.jp/ が公開されている。 • IPv6サイト https://hq-srv6.skills.it.jp/ が公開されている。

2.2. クライアント仮想マシン client-hq、client-m 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、Windows10が既にインストールされている。管理者アカウントとして user（パスワード無し）が設定されている。パスワードの変更は禁止する。サービス利用のためのクライアント設定は既に設定済みの状態であり、設定変更は許可しない。設定変更以外の動作確認のための操作は許可する。各クライアントが正常にネットワークサービスを利用するためには、各サーバーとの到達性が確保される必要がある。初期状態ではネットワークノード未設定のため到達性は確保されていない。下表に設定および正常時動作の概要を示す。

仮想マシン：client-hq

IP設定	IP: 10.0.10.1/24 GW: 10.0.10.254 DNS: 192.168.100.1
メール クライアント (Thunderbird)	・ メールアドレス muser01@skills.it.jp を用いてメールを送受信できる。 ・ 自身宛てのメールを送受信できる。 ・ master@itnetsys.org 宛てのメール送信に対して、ISP srv からの自動返信メールを受信できる。
SAMBA クライアント	・ hq-srvの/shareがz:ドライブとして割り当てられている。 ・ z:ドライブに対して読み書き可能である。
WEBブラウザ	・ https://www.itnetsys.org/ のページを表示できる。 ・ https://hq-srv.skills.it.jp/ のページを表示できる。

仮想マシン：client-m

IP設定	IP: 10.1.0.1/24 GW: 10.1.0.254 DNS: 192.168.100.1 IPv6: 自動取得
SAMBA クライアント	・ hq-srvの/shareがz:ドライブとして割り当てられている。 ・ z:ドライブに対して読み取りのみ可能である。
WEBブラウザ	・ https://www.itnetsys.org/ のページを表示できる。 ・ https://hq-srv.skills.it.jp/ のページを表示できる。 ・ https://hq-srv6.skills.it.jp/ のページを表示できる。

2.3. 仮想マシン client-ext 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、Windows10が既にインストールされている。管理者アカウントとして user（パスワード無し）が設定されている。IPの初期設定は下表の通りである。パスワードの変更は禁止する。自身の動作検証のために設定変更/接続先変更してもよい。各仮想マシンの接続先については別添ネットワーク構成図表・表3に示す。

仮想マシン：client-ext

IP設定	IP: 200.99.2.1/24 GW: 200.99.2.254 DNS: 200.99.1.1
------	--

2.4. 仮想マシン ISP srv について

インターネット（想定）上に ISP srv（ホスト名：ns.itnetsys.org）が設置されている。下記のサービスが稼働している。自身の動作確認のためにアクセスしてよい。この仮想マシンのコンソールへのログインは許可されない。

仮想マシン：ISP-srv

ホスト名	ns.itnetsys.org
IP設定	IP: 200.99.1.1/24 GW: 200.99.1.254 DNS: 127.0.0.1
DNS サービス	• itnetsys.orgドメインのマスタサーバーとして動作している。 • ns.itnetsys.org の正引きと逆引きが登録されている。 • ns.itnetsys.orgの別名としてwww.itnetsys.orgが登録されている。 • itnetsys.orgドメインのMXレコードが登録されている。 • skills.it.jpドメインのNSレコードが登録されている。 • DNSクエリ（再帰検索含む）について、制限は設けていない。
SMTP サービス	• itnetsys.orgドメインのSMTPサーバーとして動作している。 • master@itnetsys.org宛て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」のメールを自動返信する。
WEB サービス	• IPv4サイト https://www.itnetsys.org/ が公開されている。

3 各ノードへの接続方法

3.1. 各仮想マシンへの接続について

各仮想マシンに接続するための `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” にある。仮想マシン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。

※初回アクセス時には証明書に関する警告が表示される場合がある。その場合「この証明書を持つこのホストを常に信頼する」にチェックをつけ、接続してください。

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” 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. ISP への接続について

1. ユーザモード（非特権モード）でのアクセスは許可する。
2. 特権モードでのアクセス、設定変更は許可しない。

1. 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下の設定項目に従い、ネットワークノード（tokyo-fw、hq-rt1、hq-rt2、hq-fw1、hq-fw2、core-l3sw1、core-l3sw2、edge-l2sw、wan-rt1、wan-rt2、makuhari-rt）を設定し、拠点内・拠点間およびインターネット接続における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。※tokyo-fw、hq-fw1、hq-fw2 のイネーブルパスワードは“cisco”が設定されている。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。

1. 別添ネットワーク構成図表・表 1 に従い各インターフェースに IP アドレスを設定する。（※hq-fw1 と hq-fw2 については、4.5 の 3 に示す通り、ファイアウォールフェイルオーバー機能によるアクティブ/スタンバイ構成となることに注意すること）
2. hq-rt1、hq-rt2 について、タイムゾーンを日本標準時に設定する。
3. hq-rt1、hq-rt2 について、ntp サーバーとして ISP(9.9.9.9)を指定し、時刻同期すること。

4.2 スイッチ L2 設定

core-13sw1、core-13sw2、edge-12sw について以下の通り各種 L2 設定を行いなさい。

1. 各スイッチの VTP モードはトランスペアレントとする。
2. Headquarter(本社)の VLAN10、VLAN250、VLAN254 について、別添ネットワーク構成図表・表 2 の通り、VLAN 名を定義し、アクセスポートを設定する。
3. edge-12sw の Gi0/2 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。
4. edge-12sw の Gi0/2 において、BPDU を受信した場合、このポートを err-disable とするように設定する。
5. core-13sw1 と core-13sw2 間の接続について、LACP(IEEE802.3ad)を使用した Etherchannel を以下の通り動作させる。
 - A) Gi0/1 と Gi0/2 を Port-channel 1 として構成する。
 - B) core-13sw1 からネゴシエーションを開始し、core-13sw2 はパッシブリスナーとなる。

一部省略

4.3 ルーティング設定

tokyo-fw、hq-rt1、hq-rt2、hq-fw1、core-13sw1、core-13sw2、wan-rt1、wan-rt2、makuhari-rt について以下の通りルーティング設定を行いなさい。

1. ファイヤーウォールノード(tokyo-fw、hq_fw1)ではルーティングプロトコルを動作させない設計とする。関連して必要な静的経路(IPv4)を次の通り登録する。4.5 のフェイルオーバー設定を考慮した適切な経路設定となること。
 - A) tokyo-fw、hq_fw1、core-13sw1、core-13sw2 において、インターネット(ISP)への経路として適切なデフォルトルートを静的に登録する。
 - B) hq-fw1 において、Headquarter(本社)の各 VLAN および Makuhari 拠点への経路を静的に登録する。/8 に集約した経路とすること。
2. インターネット接続回線の冗長化を BGP にて制御する。ISP において、AS 番号 9500 として BGP が動作している。また、ISP は自身をデフォルトルート先とする経路を eBGP ネイバー(hq-rt1 と hq-rt2)へアドバタイズする設定となっている。別添ネットワーク構成図表・図 5 の IPv4 ルーティングトポロジー (BGP トポロジー) に従い、次の通り BGP を動作させる。
 - A) hq-rt1 および hq-rt2 は、AS 番号 65000 として、ISP と eBGP ピアを確立する。MD5 によるネイバー認証を使用する。パスワードは cisco である。
一部省略
3. Headquarter(本社)と Makuhari 拠点における IPv4 セグメントの通信を可能とする。別添ネットワーク構成図表・図 5 の IPv4 ルーティングトポロジー(OSPF トポロジー)に従い、次の通り OSPF を動作させる。
 - A) core-13sw1、core-13sw2、wan-rt1、wan-rt2、makuhari-rt において、OSPF トポロジーに従い、隣接関係を確立し、経路交換を行う。
 - B) core-13sw1、core-13sw2 において、OSPF が有効なインターフェースでの OSPF トラフィックの送信をデフォルト停止とし、必要なインターフェースでのみ OSPF トラフィックの送信を行う。
 - C) core-13sw1 および core-13sw2 は、デフォルトルートをアドバタイズする。
一部省略

4. Headquarter(本社)と Makuhari 拠点における IPv6 セグメントの通信を可能とする。別添ネットワーク構成図表・図 6 の IPv6 ルーティングトポロジー(EIGRP for IPv6 トポロジー)に従い、次の通り EIGRPv6 を動作させる。

A) core-l3sw1、core-l3sw2、wan-rt1、wan-rt2、makuhari-rt において、EIGRPv6 トポロジーに従い、隣接関係を確立し、経路交換を行う。

一部省略

4.4 IPsecVPN 設定

hq-fw1 と tokyo-fw 間において、IPsecVPN による拠点間接続を以下の通り動作させなさい。

1. hq-fw1 および tokyo-fw において、192.168.255.0/30 のアドレスを使用したトンネルインターフェース Tunnel1 を作成し、IPSec VTI(Virtual Tunnel Interface)として動作させる。インターフェース名は vti とする。

一部省略

4.5 フェイルオーバー設定

hq-rt1 と hq-rt2、hq-fw1 と hq-fw2、core-13sw1 と core-13sw2 について、それぞれ以下の通りフェイルオーバー構成を実現しなさい。アクティブシステム（稼働系）がダウンした場合においてもスタンバイシステム（待機系）によって全ての通信を継続できること。

1. hq-rt1 と hq-rt2 において、HSRP を次の通り動作させる。
 - A) hq-rt1 をプライマリ/アクティブ、hq-rt2 をセカンダリ/スタンバイとする。
 - B) 仮想 IP アドレスは、200.20.2.3 を使用する。一部省略

2. core-13sw1 と core-13sw2 において、HSRP を次の通り動作させる。
 - A) core-13sw1 をプライマリ/アクティブ、core-13sw2 をセカンダリ/スタンバイとする。
 - B) VLAN10、VLAN250、VLAN254 において HSRP を動作させる。仮想 IP アドレス(IPv4)は、使用可能な最老番のアドレスを使用する。
 - C) VLAN250 において IPv6 通信用の HSRP を動作させる。仮想 IP アドレスは、fe80::1 を使用する。一部省略

3. hq-fw1 と hq-fw2 において、ファイアウォールフェイルオーバー機能を次の通り動作させる。

※この設定が不可能な場合は、関連する得点は与えられないが、hq-fw1 単体の設定を行うことで必要な到達性を確保し課題を継続できる。

 - A) hq-fw1 をプライマリ/アクティブ、hq-fw2 をセカンダリ/スタンバイとする。hq-fw2 は hq-fw1 と設定同期するものとする。hq-fw1 に障害が発生した場合は、hq-fw2 がアクティブとなり hq-fw1 の機能/通信セッションを引き継ぐものとする。

※フェイルオーバー機能による設定同期によって、hq-fw2 ノードのホスト名が hq-fw1 と同じになるが、問題ない。
 - B) Gi0/0 (outside) について、アクティブ IP アドレスおよびスタンバイ IP アドレスを設定する。設定する IP アドレスは別添ネットワーク構成図表・表 1 を参照すること。一部省略

4.6 ファイアウォールセキュリティ設定

hq-fw1 および tokyo-fw において、以下の通りセキュリティ設定を行いなさい。

1. hq-fw1 について次の設定を行う。

- A) インターフェース名について、インターネット側(Gi0/0)を **outside**、内側(Gi0/2)を **inside** とする。**outside** はセキュリティレベルが低く、**inside** はセキュリティレベルが高くなること。
- B) Headquarter(10.0.0.0/16)および Makuhari 拠点(10.1.0.0/16)からのインターネットへの接続について、hq-fw1 にて **NAPT** を適用する。インターネット側のインターフェースアドレスに変換されること。
- C) **ICMP** インスペクションを有効にし、内側からその他のセグメントへの **ICMP** による到達確認を許可する。

2. tokyo-fw について次の設定を行う。

- A) インターフェース名について、インターネット側(Gi0/0)を **outside**、内側(Gi0/1)を **inside** とする。**outside** はセキュリティレベルが低く、**inside** はセキュリティレベルが高くなること。
- B) **tokyo-srv** をインターネットと相互接続可能とするために、tokyo-fw にてスタティック **NAT** を適用する。**100.99.1.3** にて接続が行えるようにすること。

一部省略

第 59 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

競技課題及び作業完了報告書

令和 3 年 12 月 18 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。（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。
- ✓ CML²のネットワークシミュレーションの停止および接続の変更はしないこと。
- ✓ 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。机の上に置いたまま退席すること。

座席番号	
氏名	

競技課題の背景

「あなた」は、株式会社東京スキルズに勤務する社内のサーバやネットワークを構築・運用管理する管理室の社員である。PC 教室（PCROOM）を運営しており、1 階に教室と事務所、2 階に講師室と管理室がある。各部署からトラブルシュートの依頼が入っていて、「あなた」は原因の調査とトラブルを解決しなければならない。

次頁以降のトラブルに対して適切な原因の把握と対応した処置内容を、各報告書に記載しなさい。なお、記載は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ことがポイントとなる。

- 「トラブルの原因」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
(課題によっては、架空の依頼者（トラブル報告者）への返答内容を含む)
- 本競技は報告書に記載された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。

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、管理用 PC に Wireshark.iso として用意しているものを適時利用すること。なお、課題はパケットキャプチャを利用しなくても解決可能となっている。

ネットワーク構成の概要

ネットワーク構成は課題環境資料（事前公開用）を参照しなさい。

また、各 Web サーバにアクセスした場合に表示される画面イメージを以下に示す。ただし、CML²の転送速度が遅く画像が表示されない場合があり、画像以外の文字が表示されていれば、接続が確認できたと見なしてよい。



<http://tokyo-skills.jp/>



<http://world-skills.net/>

課 題 1	新入社員の管理部の鈴木が、kanri-pc から ssh で hqlxsv にログインできないと「あなた」に相談があった。ログインができるようにしてください。
原 因	
処置内容	措置に関する作業手順はすべて記載すること。

課 題 2	HQ-2F に新たに事務セグメントを接続することになり、「あなた」は kanri-pc からリモートで HQ-2F にログインし設定を変更しようとしたが、HQ-2F に接続できなかった。kanri-pc から HQ-2F に接続できない原因を調査しトラブルを解決してください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 3	事務の篠本さんから、『お客様（user@world-skills.net）からのメールが受信できない』と連絡が入った。先日までは受信できていたようだ。この前、原田さんがサーバメンテナンスしていたので、なにか誤った操作をしたのかもしれない。ちなみに先方へはメールの送信はできるようだ。メールが受信できるように原因を調査しトラブルを解決してください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 4	新井講師から、『PC 教室にある pcroom01 の st00 ユーザから koushi-pc の「共有」フォルダにアクセスできないので、できるようにして欲しい』と要望があった。 「あなた」としては、初めから利用できるように構築されているものと思っていた。アクセスできない原因を調査しトラブルを解決してください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 5	コロナ感染防止にともないテレワーク中の佐々木講師から「telwork01 から VPN で接続をして、pcroomsv にリモートデスクトップを使い administrator でログインしたいが接続できない」と連絡が入った。なお koushi-pc には、佐々木講師のアカウントでリモートデスクトップできるようだ。pcroomsv にもリモートデスクトップできるようにしてください。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

参考資料 E 第 59 回大会競技課題 課題 2 (一部省略版)

第 59 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 2 Linux/Cisco 環境

(一部省略版)

2021 年 12 月 18 日 (土)

競技時間 : 4 時間 (12:00~16:00)

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。
- ✓ 競技時間内に作業が終了した場合、VIRL(CML-P)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。机の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

- ✓ 競技中および競技終了時において VIRL(CML-P)シミュレーションを終了させないこと。
- ✓ 競技終了時に指定された設定が各ネットワークノードの `startup-config` 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。
- ✓ VIRL(CML-P)の web インターフェースへ接続することは許可しない。
- ✓ ネットワーク構成図における ISP1、ISP2 および ISP server は競技委員が用意する構成済みの「仮想的なインターネットエリア」である。実際のインターネットには接続されていないが、競技課題中では単に「インターネット」あるいは「外部ネットワーク」と呼ぶ。
- ✓ 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、IP 到達性について、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 構成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（IT SKILLS LTD）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やサーバーの構築内容は既に完成している。これをもとに検証用の環境を構築する。

1.1. 構築ネットワークの概要

図 1 に示すように「社内」には **TOKYO・YOKOHAMA** の各拠点が存在する。TOKYO には sv1 が接続する DMZ セグメントと sv2 が接続する社内向けサーバセグメントがある。TOKYO と YOKOHAMA には各種サービスを利用するクライアント PC(client-t, client-y)がある。TOKYO-YOKOHAMA 拠点間の通信は、インターネット（ISP2）経由の VPN、及び、通信事業者がサービスする閉域 IP 網(IP-VPN)によって冗長性を確保する。社内端末のインターネット接続については、TOKYO 拠点の FW (tokyo-fw) で统一的にセキュリティを管理する。そのため、YOKOHAMA 拠点の端末(client-y)がインターネットアクセスする場合は、いったん TOKYO 拠点を經由し tokyo-fw からアクセスするものとする。

また、IPv6 ネットワークの検証用として、図 1 に示すように **v6net** を構成する。端末 client-v6 が所属するセグメントは IPv6 シングルスタックとする。nat64-rt 及び sv3 にて NAT64/DNS64 を構成し、IPv6 シングルスタッククライアント(client-v6)から IPv4 サーバー(sv1、ISPserver)への接続を可能とする。また、各種接続検証のために client-ext を配置する。詳細については、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、TOKYO・YOKOHAMA の各拠点と v6net ゾーンである。IP-VPN、ISP1、ISP2、ISPserver は設定済みである。

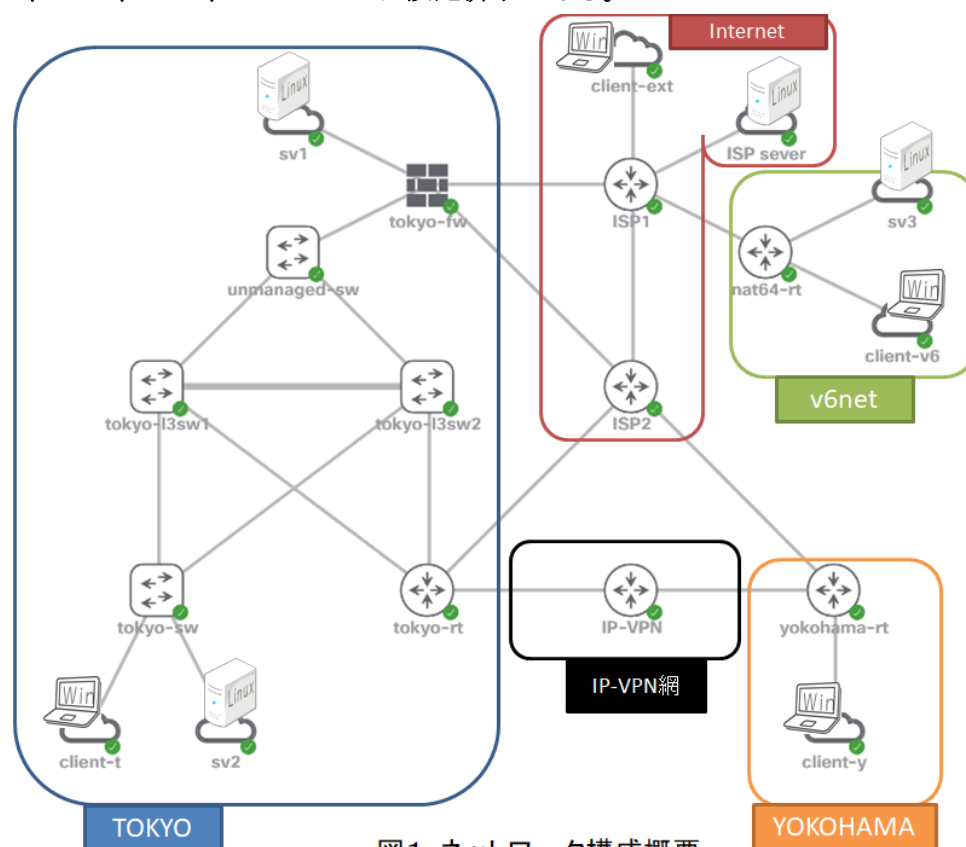


図1: ネットワーク構成概要

2 仮想マシンに関する基本情報

2.1. 仮想マシン sv1、sv2、sv3 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、Debian10.9 がインストールされており、初期インストールにおいて「Debian デスクトップ環境」、「標準システムユーティリティ」と「SSH サーバー」が選択されインストールされた状態となっている。下表の初期設定状態となっている。パスワードの変更は禁止する。

Debian10.9 がプリインストールされている仮想マシンに対して、上書きで Debian10.9 を新規インストールすることは可能であるが、それによって発生したトラブルについて競技委員側では対処しない。

共通設定

キー配列	日本語キーボード
言語	日本語
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	password
一般ユーザアカウント名	master
一般ユーザのパスワード	pass

仮想マシン：sv1

ホスト名	sv1
------	-----

仮想マシン：sv2

ホスト名	sv2
------	-----

仮想マシン：sv3

ホスト名	sv3
------	-----

2.2. 仮想マシン client-t、client-y、client-v6、client-ext 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、Windows10 が既にインストールされている。管理者アカウントとして user（パスワード無し）が設定されている。パスワードの変更は禁止する。client-ext については自身の動作検証のために自由に使用してよい。client-ext は採点の対象にならない。

2.3. 仮想マシン ISPserver（検証用サーバー：200.99.1.1）について

インターネット（想定）上に ISPserver（ホスト名：sv.itnetsys.org）が設置されている。下記のサービスが稼働している。自身の動作確認のためにアクセスしてよい。この仮想マシンのコンソールへのログインは許可されない。

1. 次の通り DNS サーバーが稼働している。
 - A) sv.itnetsys.org (200.99.1.1)の正引きが登録されている。
 - B) sv.itnetsys.org の別名として www.itnetsys.org が登録されている。
 - C) itnetsys.org ドメインの MX レコードが登録されている。
 - D) skills.it.jp ドメインの NS レコードが登録されている。
 - E) このサーバーへの DNS クエリ（再帰検索含む）について、制限は設けていない。
2. Web サーバーが稼働しており、次の URL で Web アクセス可能である。
http://200.99.1.1 または http://www.itnetsys.org
3. Mail(SMTP)サーバーが稼働しており、master@itnetsys.org 宛て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」のメールが自動返信される。ただし、返信先ドメインは MX レコードを公開している必要がある。

3 各ノードへの接続方法

3.1. 各仮想マシンへの接続について

各仮想マシンに接続するための **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” にある。仮想マシン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。

※初回アクセス時には証明書に関する警告が表示される場合がある。その場合「この証明書を持つこのホストを常に信頼する」にチェックをつけ、接続してください。

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” 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、IP-VPN への接続について

1. ユーザモード（非特権モード）でのアクセスは許可する。
2. 特権モードでのアクセス、設定変更は許可しない。

4 その他の基本情報

4.1. Debian10.9 isoイメージについて

管理用 PC のデスクトップ上に “debian_iso” フォルダがあり、Debian 10.9 の iso ファイルが置かれている。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、iso イメージをマウント可能である。

5. 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下の設定項目に従い、ネットワークノード (**tokyo-fw**、**tokyo-rt**、**tokyo-13sw1**、**tokyo-13sw2**、**tokyo-sw**、**yokohama-rt**、**nat64-rt**) を設定しなさい。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。

5.1. ネットワークノード共通基本設定

tokyo-fw、**tokyo-rt**、**tokyo-13sw1**、**tokyo-13sw2**、**tokyo-sw**、**yokohama-rt**、**nat64-rt** について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3の通り、各インターフェースに IP アドレスを設定する。
※**tokyo-fw** のイネーブルパスワードは“**cisco**”が設定されている。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。

5.2. スイッチ L2 設定

tokyo-13sw1、**tokyo-13sw2**、**tokyo-sw** について以下の通り各種 L2 設定を行いなさい。

1. 各スイッチの VTP モードはトランスペアレントとする。
2. TOKYO 拠点の VLAN10、VLAN20 について、別添ネットワーク構成図表・表2の通り、VLAN 名を定義し、**tokyo-sw** にアクセスポートを設定する。
3. **tokyo-sw** の Gi1/0 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。
4. **tokyo-sw** の Gi1/0 において、BPDU を受信した場合、このポートを **err-disable** とするように設定する。
5. **tokyo-13sw1** と **tokyo-13sw2** 間の接続について、LACP(IEEE802.3ad)を使用した Etherchannel を以下の通り動作させる。
(一部省略)
6. スイッチ間のリンクについて、適切にトラंकリンク(IEEE802.1Q)を設定する。
7. 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。
(一部省略)

5.3. TOKYO 及び YOKOHAMA 拠点におけるルーティング設定

- 全体的な動作の概要は次の通りとする。
 - 拠点内・拠点間において、課題として要求される各種サービスと通信可能とする。
 - TOKYO 拠点・YOKOHAMA 拠点の端末は必ず **tokyo-fw** 経由でインターネット接続する。
 - **tokyo-fw** のインターネット接続は、ISP1（メイン）と ISP2（バックアップ）の冗長リンクとして構成する。
 - 拠点間の通信について、IP-VPN（閉域網）を通る経路と ISP2(**tokyo-rt** と **yokohama-rt** 間の IPsecVPN トンネル)を通る経路によって冗長性を確保する。IP-VPN 側を優先経路とする。
 - **tokyo-l3sw1** または **tokyo-l3sw2** のいずれか一方に障害が発生した場合でも、通信を継続できること。

tokyo-fw、**tokyo-rt**、**tokyo-l3sw1**、**tokyo-l3sw2**、**yokohama-rt** について以下の通りルーティング設定を行いなさい。（参考：別添ネットワーク構成図表・図3ルーティングプロトコル概要）

1. 静的経路を次の通り登録する。

- A) **tokyo-fw** において、デフォルトルートの優先経路として ISP1 側の回線を静的に登録する。
- B) **tokyo-fw** は対向の ISP1 インターフェースを **icmp** にて死活監視し、障害が発生した場合は、バックアップ経路として ISP2 側の回線にデフォルトルートが切り替わること。
- C) **tokyo-rt** と **yokohama-rt** 間の IPsecVPN を ISP2 経由で構成するための静的経路を、**tokyo-rt** と **yokohama-rt** のそれぞれに登録する。

（一部省略）

2. TOKYO 拠点内の経路交換のために次の通り EIGRP を動作させる。AS 番号は 1 とする。

- A) **tokyo-fw** は内側インターフェース **Gi0/2** でのみ EIGRP を動作させ、デフォルトルートを配信する。
- B) **tokyo-rt** にて EIGRP を動作させる。ただし、ISP2 側、IP-VPN 側のインターフェースでは EIGRP を動作させない。
- C) **tokyo-rt** は、YOKOHAMA 拠点(**172.17.0.0/16**)宛ての静的経路を EIGRP にて再配布する（再配布対象の静的経路は上記 1.D)で登録したものである）。この経路以外の静的経路を再配布しないこと。

（一部省略）

3. IP-VPN において AS 番号 9500 として BGP が動作している。拠点間の経路交換のために **tokyo-rt**、**yokohama-rt** において、次の通り eBGP ピアを確立する。

- A) **tokyo-rt** は AS 番号 65001 として、IP-VPN と eBGP ピアを確立する。
- B) **tokyo-rt** は、自身をデフォルトルート先とする経路を eBGP にてアドバタイズする。
- C) **yokohama-rt** は AS 番号 65002 として、IP-VPN と eBGP ピアを確立する。
- D) **yokohama-rt** は、**172.17.0.0/16** に集約された経路のみを eBGP にてアドバタイズする。

4. **tokyo-rt** は、YOKOHAMA 拠点への経路を TOKYO 拠点内に配信するために、次の通り **iBGP** ピアを確立する。
(一部省略)

5.4. IPsecVPN 設定

tokyo-rt と **yokohama-rt** 間において **ISP2** 経由の **IPsecVPN** 接続を以下の通り動作させなさい。

(参考：別添ネットワーク構成図表・図2 拠点間接続概要)

1. **172.31.254.0/30** (**tokyo** 側が若番) のアドレスを使用したトンネルインターフェース **Tunnel0** を作成し、**IPSec VTI(Virtual Tunnel Interface)**として設定する。
2. **TOKYO-YOKOHAMA** 拠点間通信のバックアップ経路として機能すること。

5.5. ゲートウェイ冗長化設定

tokyo-l3sw1 と **tokyo-l3sw2** において、以下の通りゲートウェイの冗長構成を実現しなさい。

1. **VLAN10** について、**HSRP** を次の通り動作させる。
A) **tokyo-l3sw1** を **Active** ルータとする。
(一部省略)
2. **VLAN20** について、**HSRP** を次の通り動作させる。
A) **tokyo-l3sw2** を **Active** ルータとする。
(一部省略)

5.6. ファイアウォールセキュリティ設定

tokyo-fw において、以下の通りセキュリティ設定を行いなさい。

1. **tokyo-fw** のインターフェース名について、**ISP1** 側(**Gi0/0**)を **outside**、**ISP2** 側(**Gi0/1**)を **backup**、内側(**Gi0/2**)を **inside**、**DMZ** 側(**Gi0/3**)を **dmz** とする。
2. **outside** と **backup** についてはセキュリティレベルが最も低く、**inside** はセキュリティレベルが最も高く、**dmz** はその中間のセキュリティレベルとすること。
3. アドレス変換 (**NAT**、**NAPT**) を以下の通り動作させる。
A) **TOKYO** 拠点(**172.16.0.0/16**)及び **YOKOHAMA** 拠点(**172.17.0.0/16**)からのインターネットへの接続について、**tokyo-fw** にて **NAPT** を適用する。インターネット側のインターフェースアドレスに変換されること。**outside** と **backup** いずれのインターフェースから発信される場合も **NAPT** が適用されること。
(一部省略)
4. **ICMP** インспекションを有効にし、拠点内からその他のセグメントへの **ICMP** による到達確認を許可する。
(一部省略)

5.7. IPv6 検証用ネットワーク(v6net)設定

nat64-rt において以下の通り IPv4 及び IPv6 設定を行いなさい。

1. IPv4 及び IPv6 のデフォルトルートとして ISP1 を指す経路を静的に登録する。
2. ISP1 に対して RA(Router Advertisement)を送信しない。
3. sv3 を IPv4 にてインターネットと相互接続可能とするために、スタティック NAT を適用する。
201.10.0.2 にて接続が行えるようにすること。
4. client-v6 に対する IPv6 アドレス及びデフォルトゲートウェイの配布は RA を使用する。DNS サーバーのアドレスについては DHCPv6 にて配布する。client-v6 が利用する DNS サーバーは sv3 とする。
5. IPv6 アドレスのみを持つ端末(client-v6)から IPv4 ネットワークのサービスへの接続を可能とするために、nat64-rt において以下の通り NAT64 設定を行う。

(一部省略)

6 Linux サーバー設定課題

以下の設定項目に従い、Linux サーバー仮想マシン (**sv1**、**sv2**、**sv3**) を設定しなさい。設定項目は、サーバー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。

6.1. sv1 の設定

以下の通り、**sv1** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
- B) ネームサーバーアドレスとして自身を参照する。
- C) システムアカウント **muser01** を作成する。パスワードは **pass** とする。

2. DNS サーバー

- A) 使用するパッケージは **bind9** とする。
- B) **skills.it.jp** ドメインのマスタサーバーとして動作させる。
- C) DNSSEC の検証は無効にする。
- D) 内部ネットワーク (**172.16.0.0/16**、**172.17.0.0/16** 及び自身)からの問い合わせを処理する **view** を定義し、次の正引きに対して到達可能なアドレスを応答する。
 - ① **sv1.skills.it.jp** の問い合わせに対して、**sv1** の IPv4 アドレスを返す。
(一部省略)
- E) 上記内部ネットワーク以外の外部からの問い合わせを処理する **view** を定義し、次の正引きに対して到達可能なアドレスを応答する。
 - ① **sv1.skills.it.jp** の問い合わせに対して、**sv1** の IPv4 アドレスを返す。
(一部省略)
- F) 再帰問い合わせは、内部ネットワーク (**172.16.0.0/16**、**172.17.0.0/16** 及び自身)からのみ許可する。
- G) 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. SMTP サーバー

- A) 使用するパッケージは、**postfix** とする。
- B) **skills.it.jp** ドメインの SMTP サーバーとして動作させる。
- C) 自ドメイン宛てのメールをスプールする。

(一部省略)

4. POP サーバー

- A) 使用するパッケージは、**dovecot-pop3d** とする。
- B) 受信プロトコルとして **pop3s** のみを有効にする。TCP110 番(**pop3**)をオープンしないこと。

6.2. sv2 の設定

以下の通り、**sv2** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
- B) ネームサーバーアドレスとして **sv1** を参照する。
- C) システムアカウント **smbuser** 及び **ro_smbuser** を作成する。パスワードは **pass** とする。これらのアカウントでのローカルログインは無効とすること。

2. Samba サーバー

- A) 使用パッケージは **samba** とする。
 - B) **/share** を共有ディレクトリとする。共有名は **share** とする。共有ディレクトリへのアクセス制限は次の通りとする。
 - ① **172.16.10.0/24** 及び **172.17.0.0/24** からのアクセスのみを許可する。
- (一部省略)

6.3. sv3 の設定

以下の通り、**sv3** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
- B) ネームサーバーアドレスとして自身を参照する。
- C) システムアカウント **webmaster** を作成する。パスワードは **pass** とする。このユーザのホームディレクトリは **/var/www** とする。

2. DNS サーバー

- A) 使用するパッケージは **bind9** とする。
- B) DNSSEC の検証は無効にする。
- C) キャッシュ専用サーバーとして構築する。
- D) キャッシュに保持していないレコードの問い合わせについては、ISPServer(200.99.1.1)へ回送する。
- E) sv3 自身及びその所属セグメントと **client-v6** 所属セグメントからの問合せのみを許可する。
- F) IPv6 ノードからの正引き問い合わせに対して、IPv4 アドレスの回答しか得られなかった場合、IPv4-IPv6 変換によって合成された IPv6 アドレスを返す。ただし、IPv4-IPv6 変換プリフィックスとして、Well-known prefix(64:ff9b::/96)を使用すること。

3. Web サーバー

- A) 使用するパッケージは **nginx** とする。
- B) 次の通り、IPv4 用 web サイトを作成する。
 - ① IPv4 トラフィックによる **http** リクエストに応答する。表示内容は"IPv4 test site"とする。
 - ② IPv4 サイトのドキュメントルートは/var/www/html とする。
- C) 次の通り、IPv6 用 web サイトを作成する。
 - ① IPv6 トラフィックによる **http** リクエストに応答する。表示内容は"IPv6 test site"とする。
 - ② IPv6 サイトのドキュメントルートは/var/www/html6 とする。

4. FTP サーバー

- A) 使用するパッケージは **vsftpd** とする。
 - B) **client-v6** 所属セグメントからのアクセスのみを許可する。
 - C) **webmaster** ユーザの FTP 接続を次の通り可能とする。
 - ① IPv4 用 web サイト及び IPv6 用 web サイトのドキュメントルートディレクトリに対して、ファイルアップロード・ダウンロードを可能とすること。
- (一部省略)

7 クライアント設定課題

以下の設定項目に従い、クライアント仮想マシン (**client-t**、**client-y**、**client-v6**) を設定しなさい。

7.1. client-t の設定

以下の通り、**client-t** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
- B) ネームサーバは **sv1** を参照する。

2. メールクライアント(Thunderbird)の設定

- A) ユーザ **muser01** が **sv1** を利用してメールを送受信できる。
(**sv1** のサーバ証明書が"不正な証明書です"と警告される場合、セキュリティ例外を承認して作業をすすめること。)

3. Samba クライアントの設定

- A) ユーザ **smbuser**、パスワード **pass** を用いて、**sv2** の **/share** を **Z:** ドライブに割り当てる。
- B) Windows 再起動後も **Z:** ドライブの割り当てが有効となること。

4. Web ブラウザの動作

- A) URL: <http://www.itnetsys.org/> のページが表示できる。
- B) URL: <http://www.skills.it.jp/> のページが表示できる。

7.2. client-y の設定

以下の通り、**client-y** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
- B) ネームサーバは **sv1** を参照する。

2. Samba クライアントの設定

- A) ユーザ **ro_smbuser**、パスワード **pass** を用いて、**sv2** の **/share** を **Z:** ドライブに割り当てる。
- B) Windows 再起動後も **Z:** ドライブの割り当てが有効となること。

3. Web ブラウザの動作

- A) URL: <http://www.itnetsys.org/> のページが表示できる。
- B) URL: <http://www.skills.it.jp/> のページが表示できる。

7.3. client-v6 の設定

以下の通り、**client-v6** を動作させなさい。

1. 基本設定

- A) 別添ネットワーク構成図表・表 3 の通り、IPv4 は無効、IPv6 は自動取得となるように IP 設定を行い、ネットワーク接続を可能とすること。
(ネームサーバーのアドレスを自動で取得できない場合は、sv3 を手動で指定すること。)

2. FTP クライアントの設定

- A) FTP クライアント FFFTP の接続先として sv3 を登録し、ユーザ **webmaster** で接続できる状態とすること。

3. Web ブラウザの動作

- A) URL: <http://www.itnetsys.org/> のページが表示できる。
- B) URL: <http://www-v6.skills.it.jp/> のページが表示できる。

参考資料 F 第 59 回大会競技課題 課題 3 (一部省略版)

TEST PROJECT

(競技課題)

IT NETWORK SYSTEM ADMINISTRATION

DAY 2

WINDOWS 環境

(一部省略版)

令和 3 年 1 2 月 1 9 日

9 時～1 2 時 (3 時間)

東京ビッグサイト (Tokyo Big Sight)

注意事項

- 競技会に個人の資料やソフトウェアを持ち込まないでください。
- 携帯電話は使用しないでください。
- 競技の資料/情報を競技の間に誰かに開示しないでください。
- デュアルディスプレイを使って、見学者にメッセージを送らないようにしてください。
- 作業を開始する前に、この競技課題を良く読んでください。
- 作業の順番等を計画して競技に取り組んでください。

座席番号	氏名

1. INTRODUCTION

競技は開始時間と終了時間が決められています。3 時間です。選手は時間をどのように使うかは自由です。

重要：このドキュメントは手順書ではありません。必要とされる事項を記述していますが、そのために必要な手順を全て記述している訳ではありません。要求を満足するために必要な処理があれば、記載されていなくても実行してください。ただし、そのために要求を満たせなくなつては困ります。要求と矛盾するかどうかは選手各自で判断する必要があります。なお文章はほんの少し難解な表現（google 翻訳程度）かもしれませんが、読み間違えないように十分注意し、各自で解読判断してください。

- ・競技で使用する全てのシステムは VMWare ESXi 上にネスト（入れ子）した Windows Server 2019 上の仮想マシンで実現しています。（実装図を参照）
- ・Hyper-V コンソールを使って、各仮想マシンを操作します。（物理トポロジー図と実装図を参照）
- ・Hyper-V ホストマシン(WinSV2019)の administrator パスワードは"Skills2021"（引用符なし）です。
- ・ドメインの administrator パスワードも"Skills2021"（引用符なし）です。その他のパスワードも指定のない限り" Skills2021"（引用符なし）を使用してください。

この課題では以下のファイルなどが用意されています。

1. OS インストール用の ISO イメージファイル（使わなくても競技課題は完遂可能です。）
2. connecttest.txt
3. basic.html, web.html, WorldSkillsJapan ロゴファイル（2 種）

これらのファイルは Hyper-V ホストマシン(WinSV2019)の administrator のデスクトップ上の share フォルダに置かれ変更可能で共有されています。自由に使って構いません。

2. DESCRIPTION OF PROJECT AND TASKS

概要

あなたは情報システムを担当する IT エンジニアです。 ネットワークを改善するために、タスクを実施することにしました。あなたは社内の人々がアクセスするいくつかの Web サイトを完全に実装しなければなりません。社内のサーバーインフラストラクチャを改善していきます。指示に従ってプロジェクトを完遂してください。

このプロジェクトでは以下の事項を実現します。

1. アプリケーションサービスを提供するためのサーバーを構成します。
2. 認証システムを構成します。

Work Tasks

社内のインフラストラクチャを構築します。システムはブレインストールしただけです。現状は課題の最後にある VM 構成表を見ながら確認してください。

Work Task DC1（DC1 に対する要件）

要件に合うように既存のマシンを構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- DC1 上のサーバーマネージャーで DC2 の制御ができるように設定してください。
- このサーバーは `tokyo-big.com` の 1 番目のドメインコントローラとして構成します。
- Active Directory を構成してください。
- 以下のユーザー、OU、グループをテスト用に作成してください。

ユーザー名	OU	グループ	パスワード
coa-001	TKY	Coaches	pa\$SworD
coa-011	FRA	Coaches	pa\$SworD
dir-001	TKY	Directors	pa\$SworD
dir-011	FRA	Directors	pa\$SworD
pla-001	TKY	Players	pa\$SworD
pla-011	FRA	Players	pa\$SworD
ref-001	TKY	Referees	pa\$SworD
ref-011	FRA	Referees	pa\$SworD

- DNS サーバーを構成してください。
 - ドメインに参加した全コンピュータに加え、以下のレコードを追加してください。それ以外のレコードを追加しても構いません。
 - `dc2.tokyo-big.com` の CNAME レコード
 - `work`
 - `web.tokyo-big.com` の CNAME レコード
 - `www`
 - ルートヒントを「`ns.msftconnecttest.com`」（後述）として構成し、他のルートヒントを削除します。
 - ドメインに参加した全コンピュータの PTR レコードを記載して逆引きゾーンを作成してください。
 - DHCP サービスを構成してください。
 - DC1 をアクティブサーバーとして設定してください。（DC2 でフェイルオーバーサブネットを構成してください。）
 - 範囲 192.168.1.151 – 175
 - 192.168.1.151 は CLIENT に配布されるように予約してください。
 - スコープオプション
 - DNS : 192.168.1.1, 192.168.1.101, Gateway : 192.168.1.250
 - このスコープの 70%を DC1 に、残りを DC2 に割り当ててください。
- (一部省略)

- 以下のグループポリシーを構成して適用してください。
 - ドメインユーザーがログインした際に自動的にワークフォルダーに接続する“work”という GPO を作成してください。
(一部省略)

Work Task DC2（DC2 に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- tokyo-big.com ドメインの 2 番目のドメインコントローラとしてこのサーバーを構成してください。
- DNS サービスを構成してください。
 - Active Directory 統合 DNS ゾーンとして使用してください。
- DHCP サービスを構成してください。
 - DC1 に関する要求項目を参考に、フェイルオーバーサブネットを構成してください。
(一部省略)

Work Task WEB（WEB に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
 - tokyo-big.com ドメインに参加してください。
 - https サービスをインストールし、与えられた HTML ファイル（WinSV2019 の administrator のデスクトップに配置した share フォルダのなか）を使って IIS を構成します。
 - ssl では BIG-CA から発行された証明書を使用しなさい。その共通名を www.tokyo-big.com とし、有効期間を 2 年としなさい。
 - www.tokyo-big.com でアクセスするデフォルト Web site を構成します。
 - 基本認証とします。
 - “C:\inetpub\basic\” を root フォルダに設定し、basic.html を表示用に保存します。
- (一部省略)

Work Task CAR（CAR に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- NCSI Web サイトをホストします。
 - wwwroot に connecttest.txt ファイルを置きます。
- DNS サーバーを構成します。
 - NCSI のゾーンとレコードを作成します。
 - 192.168.1.50 の A レコード「cs.msftconnecttest.com」を登録します。
 - 192.168.1.50 の A レコード「ns.msftconnecttest.com」を登録します。

（一部省略）

- ルート CA を構成します。
 - スタンドアロン CA として構成します。
 - 共通名は「TOKYO-CA」
- （一部省略）

Work Task CAS（CAS に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
 - tokyo-big.com ドメインに参加してください。
 - 中間 CA を構成します。
 - エンタープライズ CA として構成します。
 - 「TOKYO-CA」（前述）から発行された証明書を使用してください。
- （一部省略）

Work Task CLIENT（CLIENT に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定を、文書の最後にある構成表と図に一致させてください。
- パスワードが「user」のローカルユーザー「user」が作成済みです。
- tokyo-big.com ドメインに参加してください。
- C:\workfiles に 100MB のボリュームを作成し、bitlocker を使用してこのボリュームの内容を暗号化します。ビットロッカー回復キーを CLIENT の C:\bitkey \に保存します。BitLocker の暗号化には、「Skills2021」のパスワードを使用してください。
- 電源とスリープでディスプレイの電源を切らない設定にします。
- 各種の確認作業に使ってください。

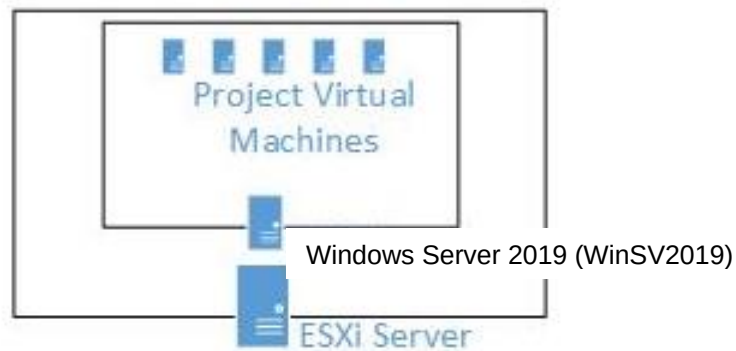
VM 構成表 (Configuration Table)

Hostname	Operation System	Domain	IP Address(es)
DC1	Windows Server 2019 Desktop	tokyo-big.com	192.168.1.1
DC2	Windows Server 2019 Desktop	tokyo-big.com	192.168.1.101
WEB	Windows Server 2019 Desktop	tokyo-big.com	192.168.1.103
CAR	Windows Server 2019 Desktop	WORKGROUP	192.168.1.50
CAS	Windows Server 2019 Desktop	tokyo-big.com	192.168.1.100
CLIENT	Windows 10 Enterprise LTSC	tokyo-big.com	DHCP
WinSV2019 (Hyper-V Host)	Windows Server 2019 Desktop	WORKGROUP	192.168.1.250

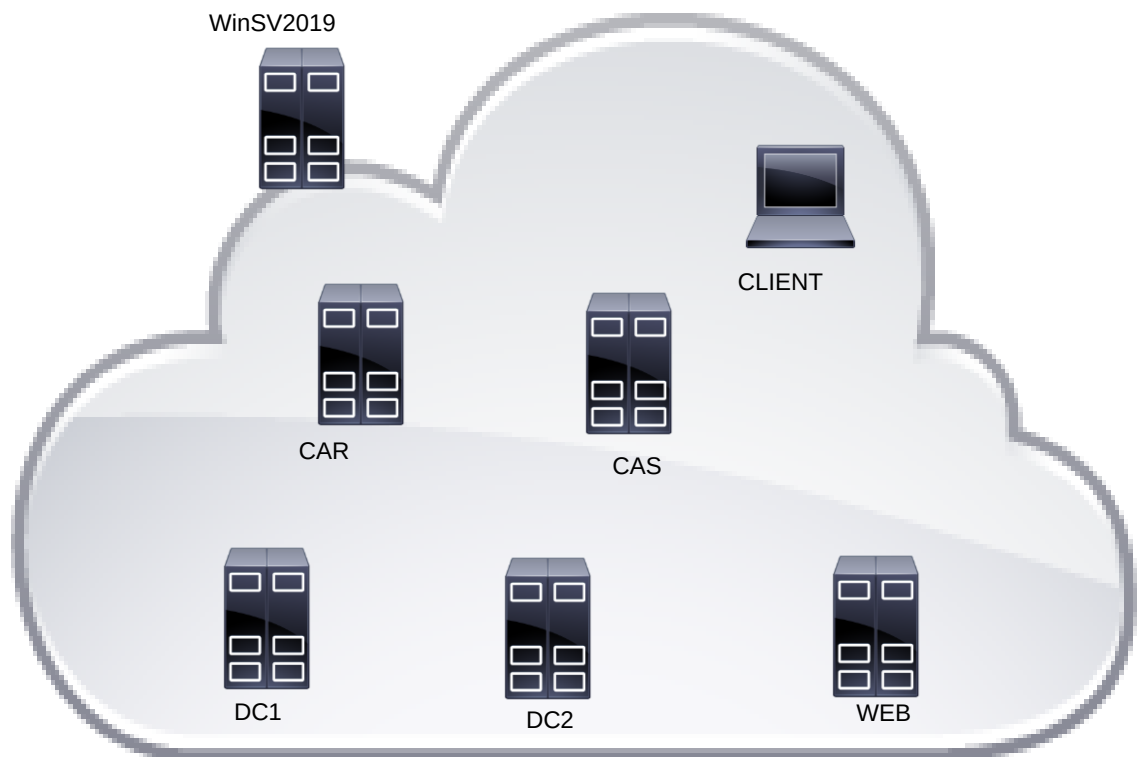
3. 物理トポロジー図 (PHYSICAL TOPOLOGY)



4. 実装図 (IMPLEMENTATION)



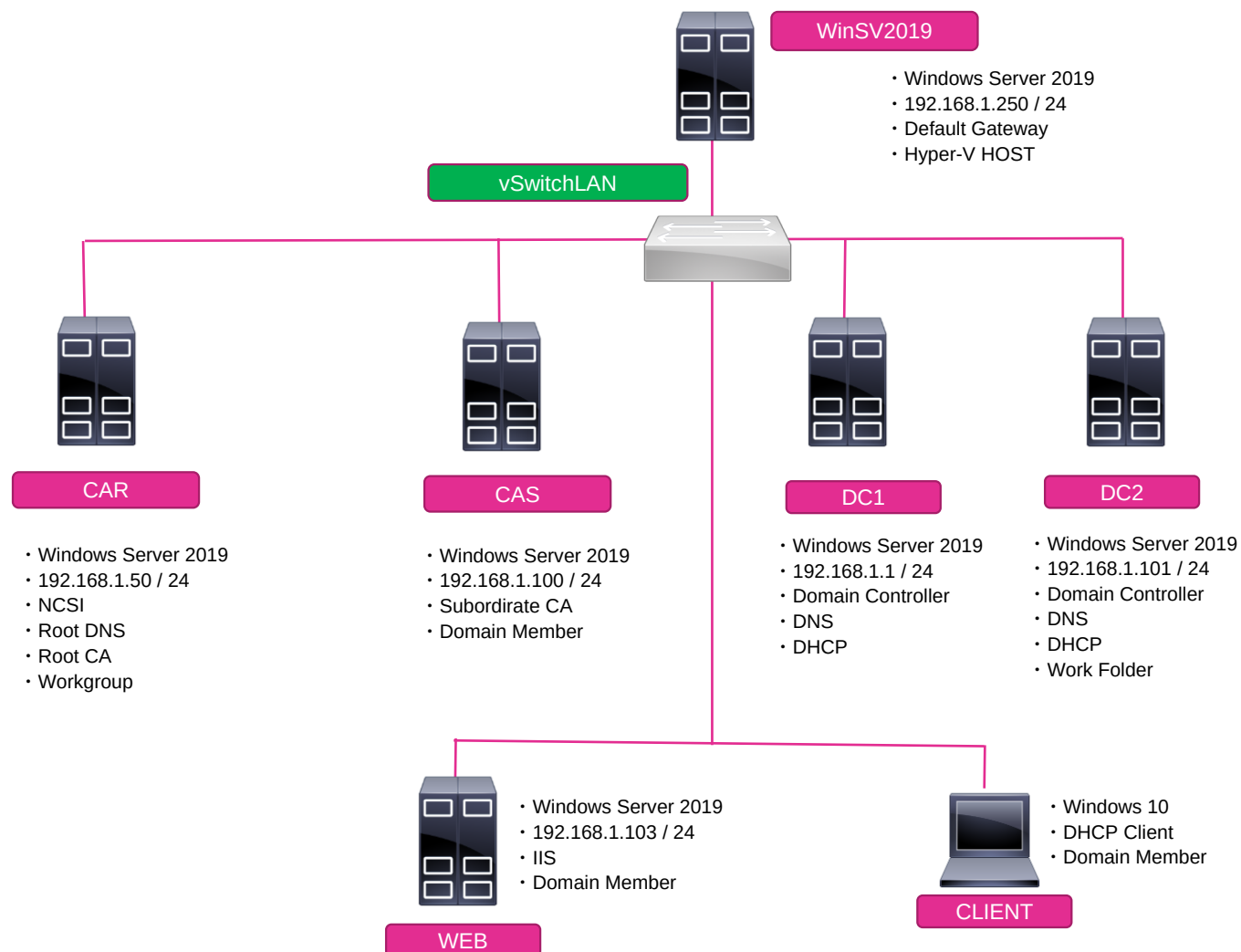
5. 論理トポロジー図 (LOGICAL TOPOLOGY)



LAN IP address
192.168.1.0 / 24

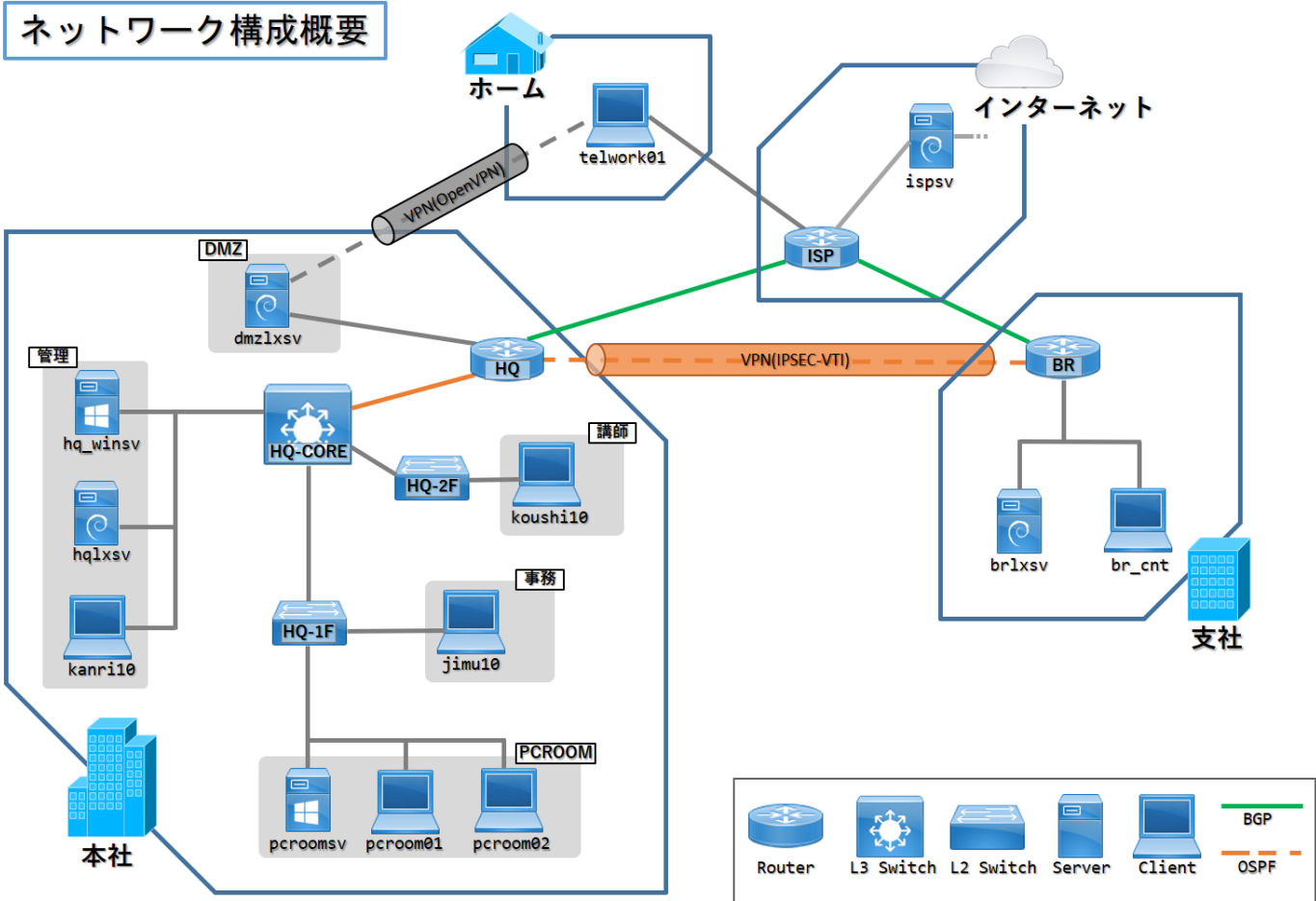


6. ネットワーク構成図 (NETWORK DIAGRAM)



参考資料 G 第 58 回大会競技課題 課題 1 概要

ネットワーク構成概要



- 問 1 新入社員の神谷講師が、koushi10 にログインできないと連絡があった。ログインができるようにしてください。
- 問 2 この度、HQ-2F に新たに事務セグメントを接続することになった。kanri10 からリモートで HQ-2F にログインし設定を変更しようとしたが、HQ-2F に接続できないと管理の原田から連絡があった。kanri10 から HQ-2F に接続できない原因を見つけてトラブルを解決してください。
- 問 3 事務の篠本さんから、user@world-skills.net 宛にメールが送信できないと連絡が入った。一昨日までは、送信できていたとのことなので、どうやら昨日起きた停電が原因とおもわれる。ちなみに今日先方からのメールは受信できているとのことだ。メールが送信できるように解決してください。
- 問 4 この度、PC 教室に pcroom02 を増設することになった。「あなた」から指定したネットワーク設定を適用したが、ネットワークに接続できないと新井講師から連絡が入った。pcroom01 は、正常に動作しているとのことだ。接続できない原因を見つけてトラブルを解決してください。

以下略

参考資料 H 第 58 回大会競技課題 課題 2 (一部省略版)

第 58 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 2 Linux/Cisco 環境

公開用 (一部省略版)

2020 年 11 月 14 日 (土)

競技時間 : 4 時間 (12:00~16:00)

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。
- ✓ 競技時間内に作業が終了した場合、VIRL(CML-P)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。机の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

- ✓ 競技中および競技終了時において VIRL(CML-P)シミュレーションを終了させないこと。
- ✓ 競技終了時に指定された設定が各ネットワークノードの `startup-config` 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。
- ✓ VIRL(CML-P)の web インタフェースへ接続することは許可しない。
- ✓ ネットワーク構成図における ISP(Internet)および ISP server は競技委員が用意する構成済みの「仮想的なインターネットエリア」である。実際のインターネットには接続されていないが、競技課題中では単に「インターネット」あるいは「外部ネットワーク」と呼ぶ。
- ✓ 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、VPN に必要なリモートサイトへの IP 到達性について、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して VPN 構成や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 構成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。

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（IT SKILLS LTD）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やサーバーの構築内容は既に完成している。これをもとに検証用の環境を構築する。

構築ネットワークの概要

図1に示すように「社内」には **AICHI・TOKYO・OSAKA** の各拠点が存在する。**AICHI** には **asv1**、が接続する **DMZ** セグメントと **asv2** が接続する社内向けサーバセグメントがある。**asv1・asv2** 及び **TOKYO** の **tsv** は、社内外にサービスを提供する。**AICHI** と **OSAKA** には各種サービスを利用するクライアント **PC(client_a、client_o)**がある。各拠点間はインターネット経由の **VPN** によって通信可能とする。さらに、**AICHI** と **TOKYO** 間の接続について、通信事業者がサービスする閉域 **IP 網(IP-VPN)**によって冗長性を確保する。また、**teleworker** はリモートアクセス **VPN** によって、インターネット経由で社内ネットワークにアクセスできる構成とする。詳細については、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、**AICHI・TOKYO・OSAKA** の各拠点と **teleworker** である。

IP-VPN(ClosedNet)（以下、**IP-VPN**）、**ISP(Internet)**（以下、**ISP**）、**ISPserver** は設定済みである。

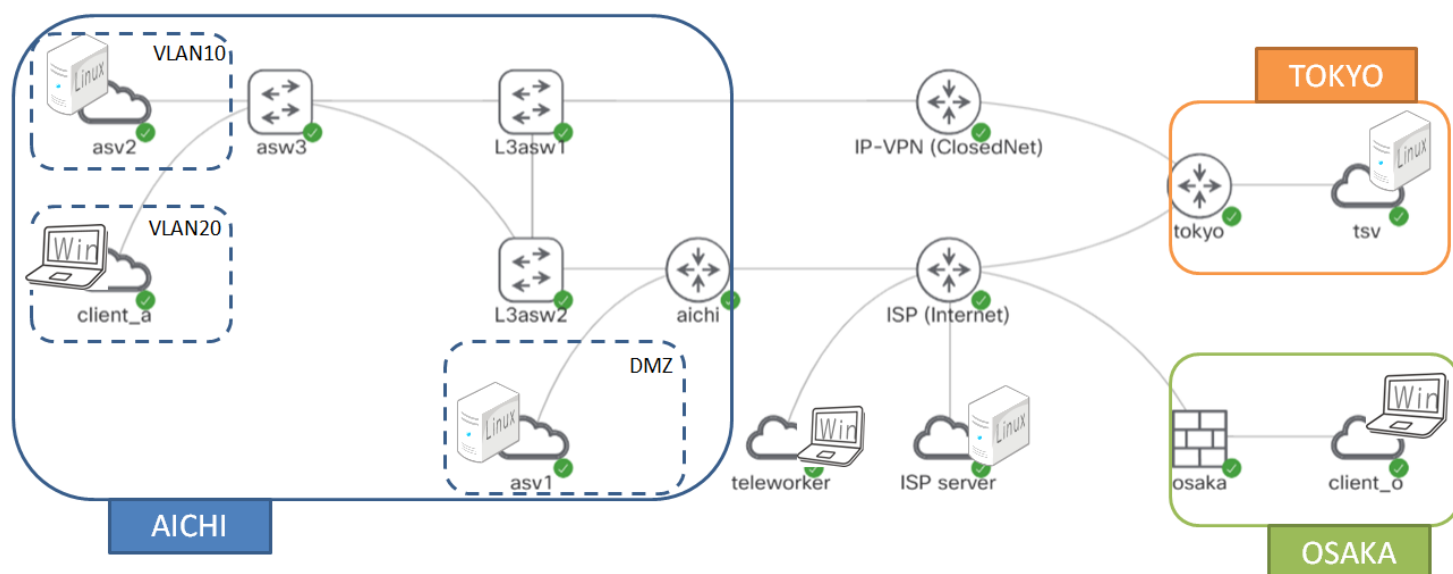


図1：ネットワーク構成概要

仮想マシンに関する基本情報

● 仮想マシン **asv1**、**asv2**、**tsv** 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、**Debian10.5** がインストールされており、初期インストールにおいて「**Debian** デスクトップ環境」、「標準システムユーティリティ」と「**SSH** サーバー」が選択されインストールされた状態となっている。下表の初期設定状態となっている。パスワードの変更は禁止する。

Debian10.5 がプリインストールされている仮想マシンに対して、上書きで **Debian10.5** を新規インストールすることは可能であるが、それによって発生したトラブルについて競技委員側では対処しない。

共通設定

キー配列	日本語キーボード
言語	英語
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	Skills2020
一般ユーザアカウント名	master
一般ユーザのパスワード	pass

仮想マシン：asv1

ホスト名	asv1
IPアドレス	210.137.174.1/29

仮想マシン：asv2

ホスト名	asv2
IPアドレス	172.16.10.100/24

仮想マシン：tsv

ホスト名	tsv
IPアドレス	172.18.1.100/24

● 仮想マシン **client_a**、**client_o**、**teleworker** 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、**Windows10** が既にインストールされている。管理者アカウントとして“**user**”、パスワード“**user**”が設定されている。パスワードの変更は禁止する。

● 仮想マシン ISPserver（検証用サーバー：200.99.1.1）について

インターネット（想定）上に ISPserver（検証用サーバー）が設置されている。下記のサービスが稼働している。自身の動作確認のためにアクセスしてよい。この仮想マシンのコンソールへのログインは許可されない。

- DNS サーバーが稼働しており、`ns.itnetsys.org`、`www.itnetsys.org`、`mail.itnetsys.org` の正引きが登録されている。
- Web サーバーが稼働しており、次の URL で Web アクセス可能である。
`http://200.99.1.1` `http://www.itnetsys.org`
- Mail(SMTP)サーバーが稼働しており、`manager@itnetsys.org` 宛て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」の空メールを自動返信する。ただし、返信先ドメインは MX レコードを公開している必要がある。

各ノードへの接続方法

● 各仮想マシンへの接続について

各仮想マシンに接続するための **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” にある。仮想マシン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。

※初回アクセス時には証明書に関する警告が表示される場合がある。その場合「この証明書を持つこのホストを常に信頼する」にチェックをつけ、接続してください。

● 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” 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。

● ISP、IP-VPN への接続について

- ユーザモード（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。

その他の基本情報

● Debian10.5 isoイメージについて

管理用 PC のデスクトップ上に “debian_iso” フォルダがあり、Debian 10.5 の iso ファイルが置かれている。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、iso イメージをマウント可能である。

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・表および以下の設定項目に従い、ネットワークノード（**aichi**、**tokyo**、**osaka**、**L3asw1**、**L3asw2**、**asw3**）を設定しなさい。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。

● ネットワークノード共通基本設定

- タイムゾーンを日本標準時に設定する。
- コンソール接続時は常に特権モードとする。

※**osaka** のイネーブルパスワードは“**cisco**”が設定されている。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。

● PPPoE 設定

ISP は PPPoE サーバ（LAN 型払い出し）として動作している。**acihi** において ISP との PPPoE 接続を以下の通り動作させなさい。※ISP が払い出すアドレス（**210.137.174.0/28**）のうち、**210.137.174.0/29** のアドレス帯を **asw1** の接続セグメント（**DMZ**）に割り当てる。残りのアドレスは **loopback** インターフェース用およびアドレス変換用とする。

- **Dialer** インターフェースとして **Dialer1** を作成する。
（一部省略）

● IPsecVPN 設定

- ◆ **aichi-tokyo** 間において ISP 経由の IPsecVPN 接続を以下の通り動作させなさい。
 - **172.31.254.0/30**（**tokyo** 側が若番）のアドレスを使用したトンネルインターフェース **Tunnel0** を作成し、IPSec VTI（Virtual Tunnel Interface）として設定する。
 - トンネルのカプセル化方式として IPsec トンネルを使用する。
- ◆ **aichi-osaka** 間において ISP 経由の IPsecVPN 接続を以下の通り動作させなさい。
 - **172.31.254.4/30**（**osaka** 側が若番）のアドレスを使用したトンネルインターフェース **Tunnel1** を作成し、IPSec VTI（Virtual Tunnel Interface）として設定する。
 - トンネルのカプセル化方式として IPsec トンネルを使用する。

● L3 EtherChannel 設定

L3asw1 と **L3asw2** 間の接続について、**L3 Etherchannel** を以下の通り動作させなさい。

- **Gi0/1** と **Gi0/2** を **Port-channel 10** として構成する。

（一部省略）

● ルーティング設定

各拠点内・拠点間において、課題として要求される各種サービスと通信可能となるように、また、各拠点の端末がインターネット接続できるようにルーティングを動作させなさい。ルーティングの設定条件は下記の通りとする。

- 各拠点で使用するプライベートアドレス範囲として、
AICHI 拠点(172.16.0.0/16)、OSAKA 拠点(172.17.0.0/16)、TOKYO 拠点(172.18.0.0/16)
を割り当てるものとする。
- 拠点間の経路交換は、上記のプライベートアドレス範囲を対象とし、/16 に集約された経路をアドレスバタイズする。
- IP-VPN において AS 番号 9500 として BGP が動作している。拠点間の経路交換のために L3asw1、tokyo において BGP を適切に動作させる。L3asw1 は AS 番号 65001、tokyo は AS 番号 65002 とする。
- 拠点間および拠点内の経路交換のために、aichi、L3asw1、L3asw2、tokyo において OSPF を適切に動作させる。

(一部省略)

- TOKYO 拠点と他拠点との通信について、IP-VPN（閉域網）を通る経路と、IPsecVPN トンネルを通る経路によって冗長性を確保する。tokyo の IP-VPN 側または ISP 側のいずれか一方のリンクに障害が発生した場合でも拠点間の通信を継続できること。

● NAT・NAPT 設定

aichi、osaka、tokyo において、アドレス変換を以下の通り動作させなさい。

- AICHI 拠点の VLAN10 からのインターネット接続について、aichi にて NAPT を適用する。変換先アドレスとして 210.137.174.11～12 を使用すること。
- OSAKA 拠点の端末からのインターネット接続について、osaka にて NAPT を適用する。インターネット側のインタフェースアドレスに変換されること。
- tsv をインターネットと相互接続可能とするために、tokyo にてスタティック NAT を適用する。100.0.1.3 にて接続が行えるようにすること。

● ゲートウェイ冗長化設定

L3asw1、L3asw2 において、以下の通りゲートウェイの冗長構成を実現しなさい。

- AICHI 拠点の VLAN10、VLAN20 について、VRRP によるゲートウェイ冗長化を構成する。
- L3asw1 を Master ルータとする。
- 仮想 IP アドレスは、使用可能な最老番のアドレスを使用する。

● その他のスイッチ設定

L3asw1、 L3asw2、 asw3 について以下の通り各種設定を行いなさい。

- AICHI 拠点の VLAN10、VLAN20 について、その他のセグメントと通信可能となるように適切に VLAN およびトランクリンクを設定すること。

● アクセスコントロール設定

osaka において、ICMP インスペクションを有効にし、OSAKA 拠点内からその他のセグメントへの ICMP による到達確認を許可しなさい。

● 帯域制限設定

IP-VPN 網に接続する回線の契約通信速度として、TOKYO 拠点は 7 Mbps を想定している。tokyo において以下の通り帯域制限（トラフィックシェーピング）を設定しなさい。

- tokyo から IP-VPN への発信トラフィックを 7 Mbps までに制限する。また、IP-VPN と接続するインターフェースの bandwidth を適切に設定すること。

Linux サーバー設定課題

以下の設定項目に従い、Linux サーバー仮想マシン (**asv1**、**asv2**、**tsv**) を設定しなさい。設定項目は、サーバー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。

● 基本設定

asv1、**asv2**、**tsv**についてデフォルトゲートウェイを適切に設定しなさい。また、ネームサーバーアドレスとして**asv1**と**asv2**は自身のアドレスを、**tsv**は**asv2**のアドレスを指定しなさい。

● **asv1** の設定

以下の通り、**asv1** を動作させなさい。

◆ DNS サーバー

- 使用するパッケージは **bind9** とする。
- インターネット向けに **skills.it.jp** ドメインのマスタサーバーとして名前解決を行う。
- **www.skills.it.jp** の正引き問合せに、**asv1** の IP アドレスを返す。
- ISP Server へのみ正引きゾーンの転送を許可する。

(一部省略)

- 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。

◆ Web サーバー

- 使用するパッケージは **nginx** とする。
- URL 「**https://www.skills.it.jp/**」 へのアクセスに対して、文字列 “IT Skills LTD” を表示する。

◆ Mail サーバー

- 使用するパッケージは、**postfix** とする。
- **skills.it.jp** ドメインのメールゲートウェイとして動作させる。
- **skills.it.jp** ドメイン宛のメールは、**asv2** へ転送する。
- 上記以外のメールは、宛先ドメインのメールサーバーへ転送する。

◆ Proxy サーバー

- 使用するパッケージは、**squid** とする。
- TCP 8080 番ポートでサービスを提供する。

(一部省略)

● asv2 の設定

以下の通り、asv2 を動作させなさい。

◆ 認証局(CA)

- CA 証明書は/ca/cacert.pem に保存すること。
- 秘密鍵は/ca/private/cakey.pem に保存し、パスフレーズは、“skills” とする。
- 設定項目は以下の通りとする。

Country Name: JP

State or Province Name: Aichi

Organization Name: IT Skills LTD

Common Name: ca.skills.it.jp

◆ DNS サーバー

- 使用するパッケージは bind9 とする。
- 社内向けに skills.it.jp ドメインのマスタサーバーとして名前解決を行う。

(一部省略)

◆ LDAP サーバー

- 使用するパッケージは slapd とする。
- 管理者パスワードは、“Skills2020” とする。
- user01~user05 の 5 個のユーザアカウントを作成する。なお、全ユーザのパスワードは “Skill2020” とする。これらのユーザは、tsv のローカルログイン、Mail サーバー、Web サーバー、Proxy サーバー、Samba サーバーのユーザ認証に利用される。各サービスで LDAP サーバーによる認証が困難な場合は、代替えとしてローカルユーザを作成し用いてもよい。ただしこの場合、LDAP についての得点は得られない。

◆ Mail サーバー

- 使用するパッケージは postfix および dovecot-pop3d とする。
- 受信プロトコルとして pop3 を有効にする。
- 587 番ポート（サブミッションポート）有効にする。

(一部省略)

- LDAP サーバーに登録されたユーザを用いて SMTP 認証を有効にする。

(一部省略)

◆ DHCP サーバー

- 使用するパッケージは isc-dhcp-server とする。
- 172.16.20.0 のセグメントに、172.16.20.101~200 の IP アドレスを配布する。

(一部省略)

◆ RAID

- 未使用のハードディスク 3 台(各サイズは 1GB)を用いて、RAID5 ディスクアレイ `/dev/md0` を構築する。

◆ LVM

- 物理ボリュームとして `/dev/md0` を追加し、ボリュームグループを作成する。
- ボリュームグループから論理ボリューム `/dev/file/data` を作成し、`/data` にマウントする。

◆ NFS サーバー

- 使用パッケージは `nfs-kernel-server` とする。
- `/data` を共有ディレクトリとする。

(一部省略)

● tsv の設定

以下の通り、`tsv` を動作させなさい。

(一部省略)

◆ Samba サーバー

- 使用パッケージは `samba` とする。
- `/share` を共有ディレクトリとする。
- OSAKA 拠点のクライアントのみアクセスを許可する。
- LDAP サーバーによるユーザ認証を行い、LDAP サーバーに登録されている `user01~user05` のみディレクトリへの読み書きを許可する。

◆ Logwatch

- 使用パッケージは `logwatch` とする。
- Samba サーバーの当日ログを 1 分に 1 回、`smbmaster@skills.it.jp` 宛に通知する。
- `kernel` の当日ログを 1 分に 1 回、`/var/www/log/log-yyyymmdd.html` へ `html` ドキュメントとして上書き出力する。ファイル名の `yyyymmdd` はログ出力日の西暦年月日である。

◆ Web サーバー

- 使用するパッケージは `apache2` とする。
- URL 「`http://tsv-log.skills.it.jp/log-20201114.html`」 へのアクセスに対して、`/var/www/log/log-20201114.html` を表示する。

(一部省略)

◆ OpenVPN サーバー

- 使用するパッケージは `openvpn` とする。
- リモートアクセスクライアントが **TOKYO** 拠点の端末として社内サービスと通信できるようにする。

クライアント設定課題

以下の設定項目に従い、クライアント仮想マシン (**client_a**、**client_o**、**teleworker**) を設定しなさい。

● **client_a** の設定

以下の通り、**client_a** を動作させなさい。

- IP アドレス、デフォルトゲートウェイ、DNS サーバアドレスを DHCP により取得する。
- メールクライアント(Thunderbird)を以下の通り設定する。
 - ✧ 送信サーバー： `asv2`、STARTTLS を使用
 - ✧ 受信サーバー： `asv2`、STARTTLS を使用
 - ✧ `user03@skills.it.jp` ユーザが社内外とメール送受信ができる。

(一部省略)

● **client_o** の設定

以下の通り、**client_o** を動作させなさい。

- IP アドレスとして **172.17.1.201**、DNS サーバーとして **asv2** のアドレスを設定し、ネットワーク接続可能な状態にしておくこと。
- **tsv** の共有ディレクトリを **Z:ドライブ** として利用できる。

● **teleworker** の設定

以下の通り、**teleworker** を動作させなさい。

- IP アドレスとして **100.0.3.11**、DNS サーバーとして **ISP server** のアドレスを設定し、ネットワーク接続可能な状態にしておくこと。
- Web ブラウザ(Internet Explore) を以下の通り設定する。
 - ✧ URL「<https://www.skills.it.jp/>」のページが表示できる。なお、証明書エラーが表示されないこと。
- OpenVPN GUIを起動済みにしておき、接続操作を行うだけで**tsv**に接続できるようにすること。
 - ✧ インターネット接続については、VPN を経由せず、直接接続されること。
 - ✧ 接続操作時に ID/パスワード等の入力が必要な場合は、下記に記載しておくこと。そのような入力が不要である場合は空欄とすること。

参考資料Ⅰ 第58回大会競技課題 課題3 (一部省略版)

TEST PROJECT

(競技課題)

IT NETWORK SYSTEM ADMINISTRATION

DAY 2

WINDOWS 環境

公開用 (一部省略版)

令和 2 年 1 1 月 1 5 日

9 時～1 2 時 (3 時間)

愛知県国際展示場 (Aichi Sky Expo)

注意事項

- 競技会に個人の資料やソフトウェアを持ち込まないでください。
- 携帯電話は使用しないでください。
- 競技の資料/情報を競技の間に誰かに開示しないでください。
- デュアルディスプレイを使って、見学者にメッセージを送らないようにしてください。
- 作業を開始する前に、この競技課題を良く読んでください。
- 作業の順番等を計画して競技に取り組んでください。

座席番号	氏名

1. INTRODUCTION

競技は開始時間と終了時間が決められています。3 時間です。選手は時間をどのように使うかは自由です。

重要：このドキュメントは手順書ではありません。必要とされる事項を記述していますが、そのために必要な手順を全て記述している訳ではありません。要求を満足するために必要な処理があれば、記載されていなくても実行してください。ただし、そのために要求を満たせなくなっては困ります。要求と矛盾するかどうかは選手各自で判断する必要があります。なお文章はほんの少し難解な表現（google 翻訳程度）かもしれませんが、読み間違えないように十分注意し、各自で解釈判断してください。

- ・競技で使用する全てのシステムは VMWare ESXi 上にネスト（入れ子）した Windows Server 2019 上の仮想マシンで実現しています。（実装図を参照）
- ・Hyper-V コンソールを使って、各仮想マシンを操作します。（物理トポロジー図と実装図を参照）
- ・Hyper-V ホストマシン(SKILLSSV)の administrator パスワードは"Skills2020"（引用符なし）です。
- ・ドメインの administrator パスワードも"Skills2020"（引用符なし）です。その他のパスワードも指定のない限り" Skills2020"（引用符なし）を使用してください。

この課題では以下のファイルなどが用意されています。

1. OS インストール用の ISO イメージファイル
2. connecttest.txt

これらのファイルは Hyper-V ホストマシン(SKILLSSV)の administrator のデスクトップ上の share フォルダに置かれフルコントロールで共有されています。自由に使って構いません。

2. DESCRIPTION OF PROJECT AND TASKS

概要

あなたは情報システムを担当する IT エンジニアです。複数のユーザーを持ち、構成が既に設定されている Windows Domain を引き継ぎました。ネットワークを改善するために、更なるタスクを実施することにしました。あなたはドメイン内の人々がアクセスするいくつもの Web サイトを完全に実装しなければなりません。既存ドメイン内外のサーバーインフラストラクチャを改善していきます。指示に従ってプロジェクトを完遂してください。

このプロジェクトでは以下の事項を実現します。

1. アプリケーションサービスを提供するためのサーバーを構成します。
2. 認証システムを構成します。
3. Internet(201.98.22.0/24)と接続し、Internet 側のホストも構成します。

Part 1 – Intranet LAN

Part 1 では、ネットワーク内のインフラストラクチャをアップグレードします。システムのインストールや構成の状況は様々です。明確にするために、課題の最後にある VM 構成表を確認してください。

Work Task DC1（DC1 に対する要件）

要件に合うように既存のマシンを構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- DC1 上のサーバーマネージャーで DC2 の制御ができるように設定してください。
- このサーバーは **centr-air.com** のドメインコントローラとして事前構成されています。
- Active Directory を構成してください。
- 以下のユーザー、OU、グループをテスト用に作成してください。

ユーザー名	OU	グループ	パスワード
agt-001	AIR	Agents	Pa\$\$worD
agt-011	WSC	Agents	Pa\$\$worD
cpt-001	AIR	Competitors	Pa\$\$worD
cpt-011	WSC	Competitors	Pa\$\$worD
exp-001	AIR	Experts	Pa\$\$worD
exp-011	WSC	Experts	Pa\$\$worD
mgr-001	AIR	Managers	Pa\$\$worD
mgr-011	WSC	Managers	Pa\$\$worD

- DNS サーバーを構成してください。
 - ドメインに参加したサーバーに加え、以下のレコードを追加してください。それ以外のレコードを追加しても構いません。
 - **web.centr-air.com** の CNAME レコード
 - intra
 - ルートヒントを「**ns.msftconnecttest.com**」（後述）として構成し、他のルートヒントを削除します。
 - 全サーバーの PTR レコードを記載して逆引きゾーンを作成してください。
- DHCP サービスを構成してください。
 - DC1 をアクティブサーバーとして設定してください。（DC2 でフェイルオーバーサブネットを構成してください。）
 - 範囲 201.98.23.51 – 75
 - 201.98.23.51 は INTCLIENT に配布されるように予約してください。
 - スコープオプション
 - DNS : 201.98.23.1, 201.98.23.101, Gateway : 201.98.23.254
 - このスコープの 70%を DC1 に、残りを DC2 に割り当ててください。
 - ホットスタンバイモードを使うために、フェールオーバーを構成してください。
 - DHCP 名の保護を有効にしてください。
 - 後述の Work Task WEB に備えて Windows 展開サービス(WDS)を追加してください。
 - （一部省略）

Work Task DC2（DC2 に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- centr-air.com ドメインの 2 番目のドメインコントローラとしてこのサーバーを構成してください。
- DNS サービスを構成してください。
 - Active Directory 統合 DNS ゾーンとして使用してください。
- DHCP サービスを構成してください。
 - DC1 に関する要求項目を参考に、フェイルオーバーサブネットを構成してください。
- （一部省略）

Work Task CERT（CERT に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- centr-air.com ドメインに参加してください。
- サービスをインストールして中間 CA を構成します。
 - 「AICHI-CA」（後述）から発行された証明書を使用してください。
 - Common Name は「SKILLS-CA」
 - Intranet 用の証明書を発行します。
- （一部省略）

Work Task WEB（WEB に対する要件）

WDS Deployment を通じてインストールし、構成してください。

- WDS を構成できないか、あるいは WDS を正常に機能させることができない場合には、IOS イメージを使ってホストマシン(SKILLSSV)の Hyper-V 上に直接インストールしても構いません。なお、WDS でインストールした場合、キーマップが US なので注意してください。
- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- centr-air.com ドメインに参加してください。
- IIS をインストールし、構成してください。
 - 以下の説明に従って、「Default Web Site」を構成します。
 - URL は <https://intra.centr-air.com>
 - Intranet 用で 「Default Web Site」 と表示します。
 - 以下の説明に従って、「Public Web Site」を構成します。
 - URL は <https://www.centr-air.com>
 - Internet 用で 「Public Web Site」 と表示します。

Work Task INTCLIENT（INTCLIENT に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- パスワードが「user」のローカルユーザー「user」が作成済みです。
- centr-air.com ドメインに参加してください。
- WEB へのアクセスのテストに使ってください。
- 共有や DFS へのアクセスのテストに使ってください。

Part 2 – INTERNET

Part 2 では、Internet 側と接続するために FIREWALL を構成します。また、そのために INET も構成し、社員が出張で外部から Intranet にアクセスするための REMCLIENT も用意します。

Work Task FIREWALL（FIREWALL に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- ルーティングを有効にします。
- パブリックインターネット用に DNS サーバーを構成します。
 - プライマリゾーン「centr-air.com」を作成し、これらの A レコード 201.98.22.100 を追加します。
 - ns, vpn
 - 201.98.23.103 の A レコード「www.centr-air.com」を追加します
 - 「centr-air.com」の SOA レコードは「ns.centr-air.com」である必要があります。
 - ルートヒントを「ns.msftconnecttest.com」（後述）として構成し、他のルートヒントを削除します。
- ルーティングとリモートアクセスサービスを構成します。
 - インターネット上の REMCLIENT は、このサーバーへの VPN 接続を確立する必要があります。
 - IKEv2 クライアントは、このサーバーを介してイントラネットに接続できます。
 - リモートアクセスクライアントの IP アドレスプール：192.168.219.1-192.168.219.254
- （一部省略）

Work Task REMCLIENT（REMCLIENT に対する要件）

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- パスワードが「user」のローカルユーザー「user」が作成済みです。
- centr-air.com ドメインに参加します。
- VPN トンネルを構成します。
 - ドメインユーザーは、このトンネルを介してログインする必要があります。
 - VPN に接続した後、ユーザーはイントラネットのすべてのリソースにアクセスする必要があります。
 - 競技終了時には VPN 接続した状態にしておいてください。
- （一部省略）

Work Task INET

以下の要件に従って構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- NCSI Web サイトをホストします。
 - インターネット上のクライアントは、インターネット接続を「接続済み」として示す必要があります。
 - wwwroot に connecttest.txt ファイルを置きます。
- DNS サーバーを構成します。
 - NCSI のゾーンとレコードを作成します。
 - 201.98.22.1 の A レコード「cs.msftconnecttest.com」を登録します。
 - 201.98.22.1 の A レコード「ns.msftconnecttest.com」を登録します。
 - ns.msftconnecttest.com の CNAME レコードとして以下を追加します。
 - www
 - 「msftconnecttest.com」の SOA レコードは「ns.msftconnecttest.com」である必要があります。
 - ルート DNS サーバーをシミュレートするルートゾーン (.) を作成します。
 - DNS レコードを解決するための適切な委任を作成します。
- DHCP サービスを構成します。
 - 範囲: 201.98.22.151 - 201.98.22.175
 - DNS: 201.98.22.1
 - Gateway: 201.98.22.100
- 証明機関を構成します。
 - Common name: AICHI-CA
 - SKILLS-CA の証明書要求を発行します。

VM 構成表 (Configuration Table)

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
DC1	Windows Server 2019 Desktop	centr-air.com	201.98.23.1	Yes – Configured as DC
DC2	Windows Server 2019 Core	centr-air.com	201.98.23.101	Yes
INTCLIENT	Windows 10 Enterprise LTSC	centr-air.com	DHCP	Yes
WEB	Windows Server 2019 Desktop	centr-air.com	201.98.23.103	No – WDS Deployment
CERT	Windows Server 2019 Desktop	centr-air.com	201.98.23.100	Yes
FIREWALL	Windows Server 2019 Desktop	WORKGROUP	201.98.23.254 201.98.22.100	Yes
INET	Windows Server 2019 Desktop	WORKGROUP	201.98.22.1	Yes
REMCLIENT	Windows 10 Enterprise LTSC	centr-air.com	DHCP	Yes

「Yes」はオペレーティングシステムがプリインストールされ、ホスト名とネットワーク設定も構成されています。

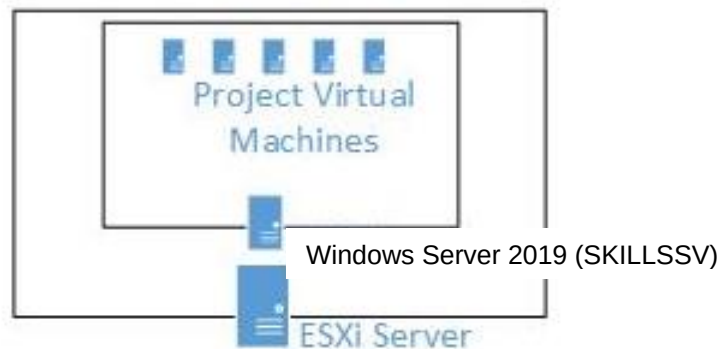
「Yes – Configured as DC」はオペレーティングシステムがプリインストールされ、ホスト名とネットワーク設定は構成されています。更に DC として機能します。

もし、GUI を持たない“Core”サーバーで構成や作業が困難、あるいは不可能であれば、“Core”サーバーを上書きし“Windows Server 2019 Desktop”で任意のマシンを再インストールしても構いません。ただし、採点上のペナルティは少々課せられますし、インストールの時間もかかってしまいます。

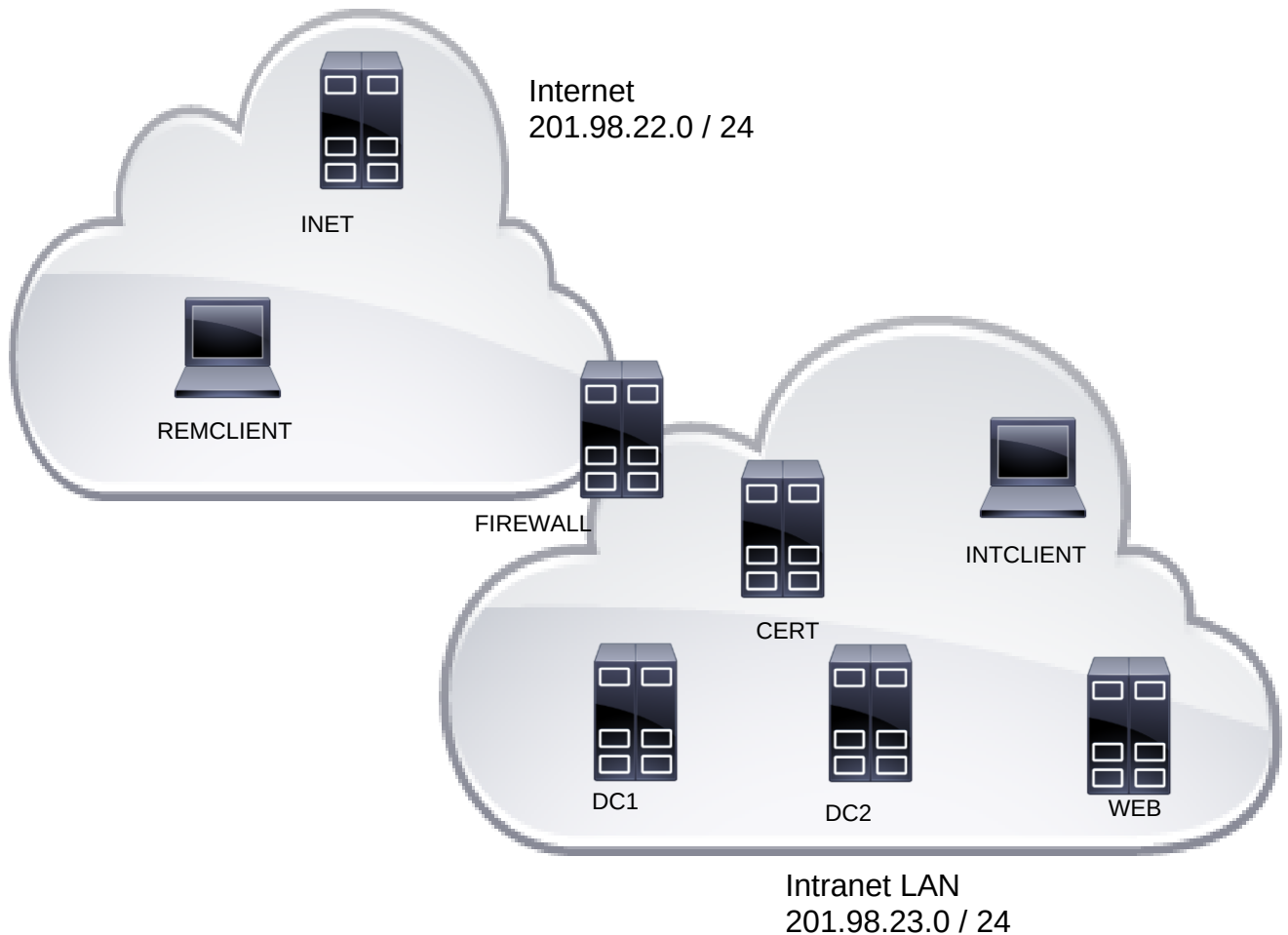
3. 物理トポロジー図 (PHYSICAL TOPOLOGY)



4. 実装図 (IMPLEMENTATION)

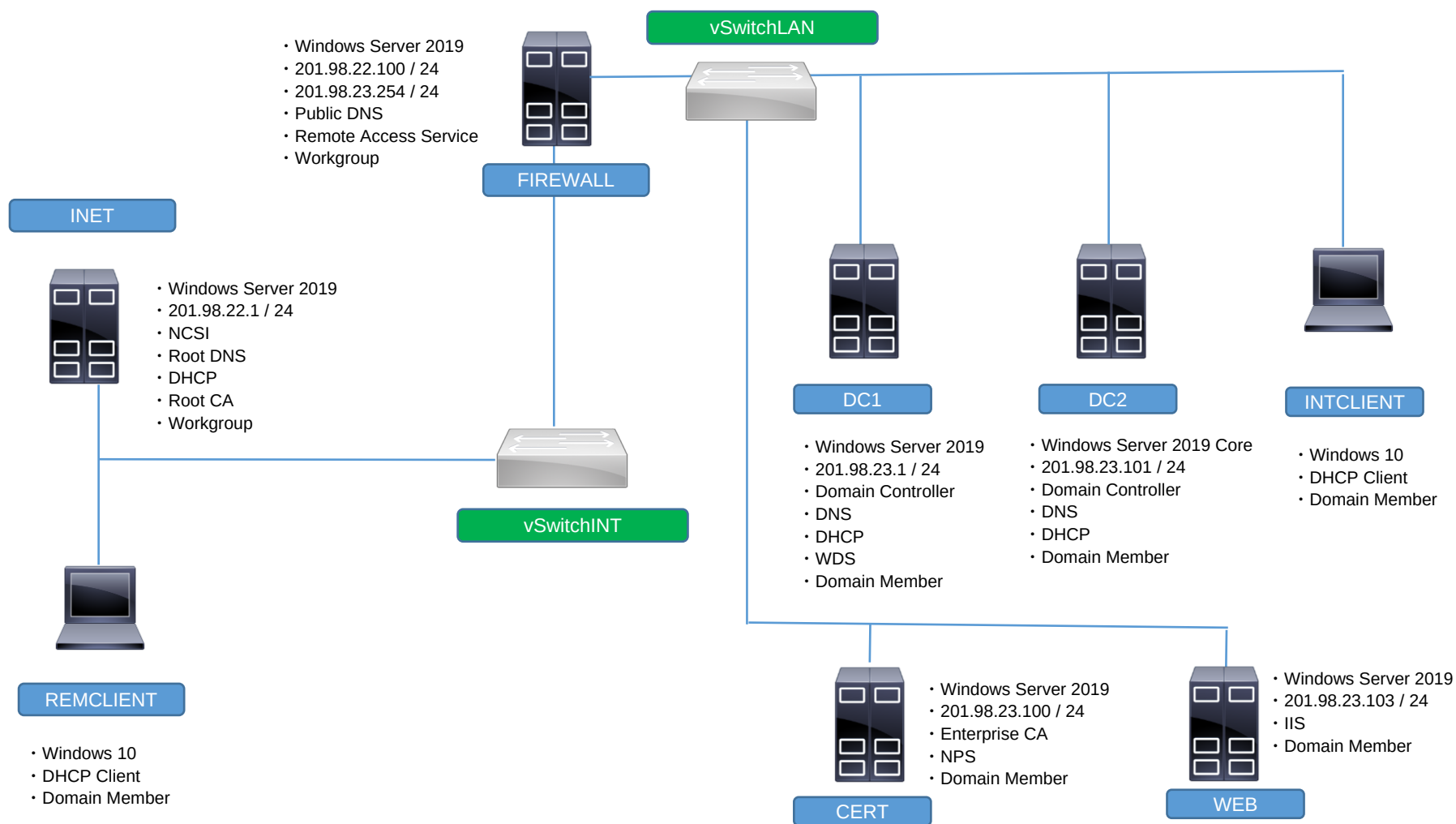


5. 論理トポロジー図 (LOGICAL TOPOLOGY)





6. ネットワーク構成図（NETWORK DIAGRAM）



参考資料 J 第 57 回大会競技課題 課題 1 (一部省略版)

第 57 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

競技課題及び作業完了報告書

令和元年 11 月 16 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。(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、VIRL 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。
- ✓ VM Maestro を使用し、各ネットワーク機器のコンフィグを変更するのは構わないが、シミュレーションの停止および接続の変更はしないこと。
- ✓ 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	

競技課題の背景

「あなた」は、株式会社愛知スキルシステムズに勤務する社内のサーバやネットワークを構築・運用管理する管理室の社員である。

PC 教室（PCROOM）を開設することになり、1 階に教室を、3 階に教材の開発室を新たに用意することとなった。導入はほぼ最終段階となり、明日からいよいよ教室をオープンする。管理室のあなたは、教室開設の担当者の一人である。

また各部署からトラブルシュートの依頼が入っていて、あなたはトラブルを解決しなければならない。

次頁以降のトラブルに対して適切な原因の把握と対応した処置内容を、各報告書に記載しなさい。なお、記載は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ことがポイントとなる。

- 「トラブルの原因」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
（課題によっては、架空の依頼者（トラブル報告者）への返答内容を含む）
- 本競技は報告書に記載された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。

ネットワーク構成の概要

ネットワーク構成は課題環境資料（事前公開用）を参照しなさい。ただしネットワーク構成に対し、トラブルが発生したため、一時的にネットワーク構成を変更した。図 1 に接続変更したネットワーク構成概要を示す。

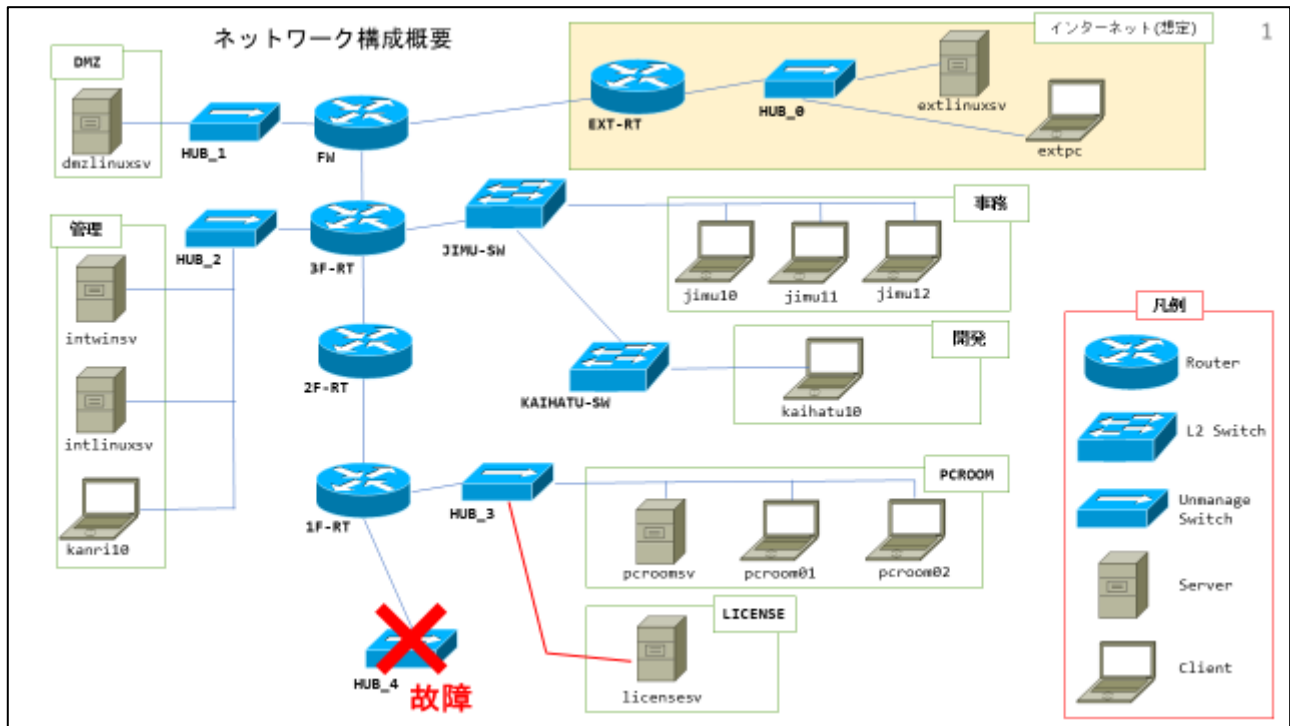


図1 ネットワーク構成概要

また、各 Web サーバにアクセスした場合に表示される画面イメージを以下に示す。



<http://www.aichi.com/>



<http://www.skills.com/>

課 題 1	PCROOM の講師から、「pcroom02 のコンピュータに生徒 3 ユーザでログインできず明日から使用するので何とかしてほしい」という報告があった。
原 因	
処置内容	措置に関する作業手順はすべて記載すること。

課 題 2	PCROOM を設定していた後輩の鈴木が、PC ルームからインターネットのホームページの閲覧がおかしいと言ってきた。鈴木には手に負えずヘルプを要請してきた。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

課 題 3	PCROOM を「あなた」に任せ、3 階の開発室のセッティングに向かった鈴木から、今度は kaihatu10 のコンピュータが、ドメイン aichi.local に参加できないという内線をしてきた。KAIHATU-SW と kaihatu10 のネットワーク設定は済ませたということである。JIMU-SW は、事前に「あなた」が設定済みにしていた。
原 因	
措置内容	措置に関する作業手順はすべて記載すること。

以下 課題 4、5、6 省略

参考資料 K 第 57 回大会 課題 2 (一部省略版)

第 57 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 2 Linux/Cisco 環境

2019 年 11 月 16 日 (土)

競技時間：4 時間 (12:00～16:00)

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。
- ✓ 競技時間内に作業が終了した場合、VIRL 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

- ✓ 競技中および競技終了時において VIRT シミュレーションを終了させないこと。
- ✓ 競技終了時に指定された設定が各ネットワークノードの startup-config 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。
- ✓ ネットワーク構成図における「インターネット（想定）」は、ISP-A、ISP-B、ISP-C および ISPserver で構成される。これは競技委員が用意する構成済みの「仮想的なインターネットエリア」である。実際のインターネットには接続されていないが、競技課題中では単に「インターネット」あるいは「外部ネットワーク」と呼ぶ。
- ✓ 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、VPN に必要なリモートサイトへの IP 到達性について、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して VPN 構成や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 構成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。

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（IT SKILLS LTD）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やサーバの構築内容は既に完成している。これをもとに検証用の環境を構築する。

構築ネットワークの概要

図 1 に示すように「社内」には愛知本社及び東京第一支社、第二支社が存在する。愛知本社には asv1、が接続する DMZ セグメント(DMZ)と asv2 が接続する社内向けサーバセグメント(SERVER)がある。asv1、asv2 及び東京第一支社の tsv は社内外にサービスを提供する。東京第二支社には各種サービスを利用する clientPC がある。本社及び各支社間はインターネット経由の VPN によって通信可能とする。愛知本社は異なる 2 つの ISP に接続するマルチホームネットワークであり、冗長化と負荷分散を構成する。詳細については、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、愛知本社および東京第一支社、東京第二支社のネットワークとなる。インターネット（想定）エリアの各ノードは、設定済みである。

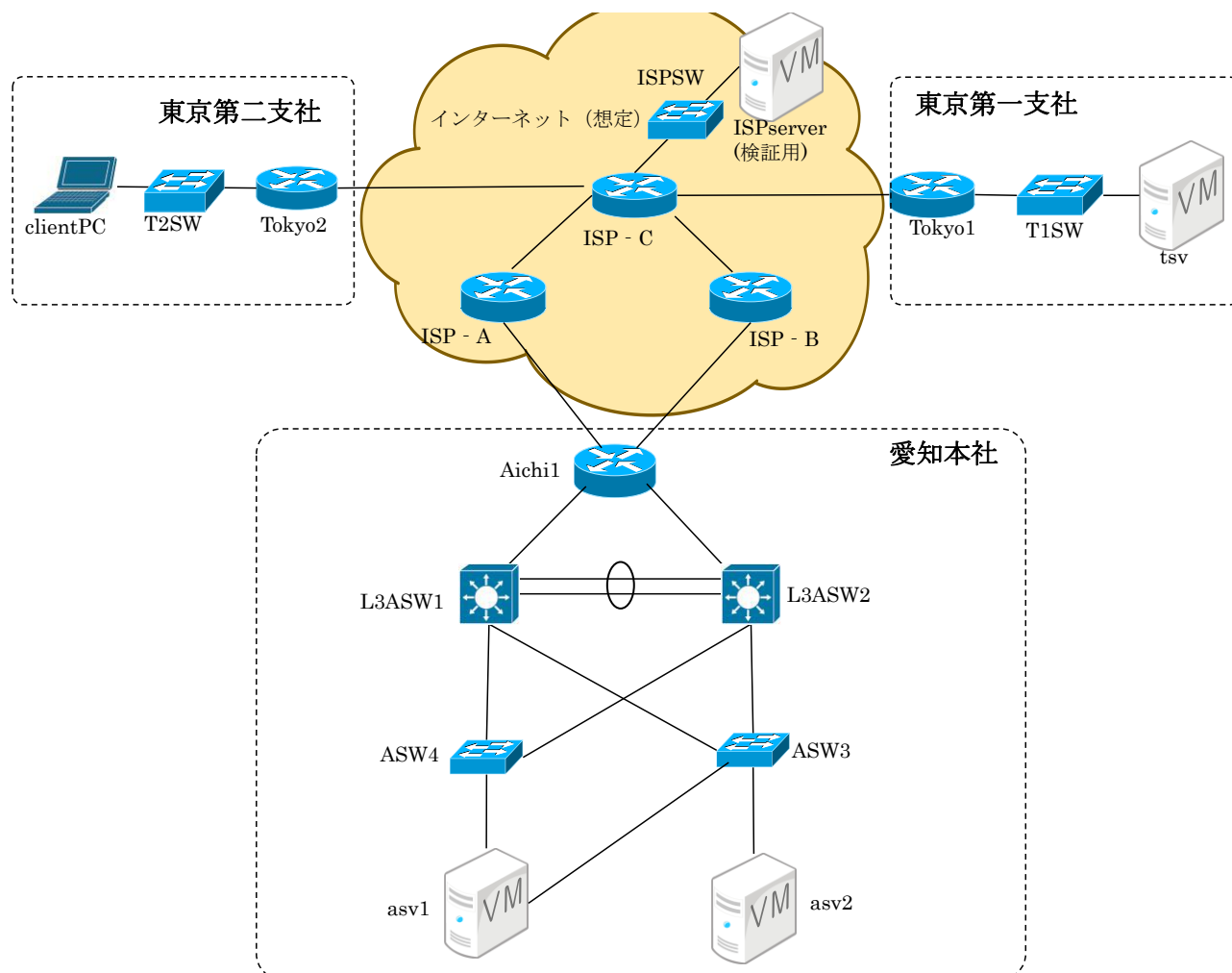


図 1：ネットワーク構成概要

仮想マシンに関する基本情報

● 仮想マシン asv1, asv2, tsv 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、Debian9.9 が既にインストールされており、初期インストールにおいて「標準システムユーティリティ」と「SSH サーバ」が選択されインストールされた状態となっている。下表の初期設定状態となっている。

Debian9.9 がプリインストールされている仮想マシンに対して、上書きでDebian9.9 を新規インストールすることは可能であるが、それによって発生したトラブルについて競技委員側では対処しない。

共通設定

キー配列	日本語キーボード
言語	英語
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	skills2019
一般ユーザアカウント名	user01
一般ユーザのパスワード	itNet01

仮想マシン：asv1

ホスト名	asv1
ドメイン名	skills.it.jp
IPアドレス ens192	20.0.0.1/28
IPアドレス ens224	—

仮想マシン：asv2

ホスト名	asv2
ドメイン名	skills.it.jp
IPアドレス	192.168.101.100/24

仮想マシン：tsv

ホスト名	tsv
ドメイン名	br.skills.it.jp
IPアドレス	192.168.1.100/24

● 仮想マシン clientPC 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、Windows10 が既にインストールされている。「Teraterm」及び「Thunderbird」がインストールされている。

● 仮想マシン ISPserver（検証用サーバ：200.99.1.1）について

インターネット（想定）上に ISPserver（検証用サーバ）が設置されている。下記のサービスが稼働している。自身の動作確認のためにアクセスしてよい。この仮想マシンのコンソールへのログインは許可されない。

- DNS サーバが稼働しており、ns.itnetsys.org、www.itnetsys.org、mail.itnetsys.org の正引きが登録されている。
- Web サーバが稼働しており、次の URL で Web アクセス可能である。
http://200.99.1.1 http://www.itnetsys.org
- Mail (SMTP) サーバが稼働しており、manager@itnetsys.org 宛で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」の空メールを自動返信する。ただし、返信先ドメインは MX レコードを公開している必要がある。

● 検証作業用仮想マシン PC1 について

- Windows10 がインストールされており、検証作業用として自由に使用してよい。
- 採点対象とはならない。
- 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)」→「ネットワークアダプタ 1」→「設定」→「ネットワーク接続」から、任意のセグメントに接続してよい。各仮想マシンの接続先セグメントは別添ネットワーク構成図・表の表 4 を参照してください。

※ただし、PC1 以外の仮想マシンについては、接続先を変更しないこと。

各ノードへの接続方法

● 各仮想マシンへの接続について

各仮想マシンに接続するための 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” にある。仮想マシン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、ユーザ名 “root”、パスワード “adm0esx1” にてアクセス可能である。(このユーザ名・パスワードは ESXi ホストのものであり、ゲスト OS のものではないことに注意)

※初回アクセス時には証明書に関する警告が表示される場合がある。その場合「この証明書を持つこのホストを常に信頼する」にチェックをつけ、接続してください。

● 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” 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。また、その他の方法として、VM Maestro からのコンソール接続を利用してもよい。

※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。

● ISP-A、ISP-B、ISP-C への接続について

- ・ ユーザモード（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。
- ・ 動作検証のためにアクセスが必要な場合は、VM Maestro のコンソール接続を利用してよい。

その他の基本情報

● Debian9.9 isoイメージについて

管理用 PC のデスクトップ上に「debian_iso」フォルダがあり、Debian 9.9.0 の iso ファイルが置かれている。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、iso イメージをマウント可能である。

● Linux仮想マシンへのGUIデスクトップ環境の導入について

インストール済みの Linux サーバは、すべて CUI 環境となっている。GUI デスクトップ環境で作業を行いたい場合は、tasksetl コマンドなどを用いて好みの GUI 環境を導入してもよい。

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・表および以下の設定項目に従い、ネットワークノード（Aichi1, Tokyo1, Tokyo2, L3ASW1, L3ASW2, ASW3, ASW4）を設定しなさい。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。

● 全ネットワークノード共通基本設定

- タイムゾーンを日本標準時に設定する。
- コンソール接続に対するパスワードは設定しない。イネーブルパスワードは“cisco”とする。イネーブルパスワードは暗号化すること。

● ルーティング設定

フェールオーバー（障害時動作）について以下の通り動作すること。

- Aichi1 について、ISP-A 側及び ISP-B 側のいずれかのリンクに障害が発生した場合でも、一方のリンクで全ての通信を継続できること。

（省略）

外部ルーティングについて以下の通り設定しなさい。

- Tokyo1 のデフォルトルートを静的に設定する。
- Tokyo2 のインターネット側インタフェースのアドレス及びデフォルトルートは、ISP-C から DHCP による払い出しを受ける。 ※ISP-C は DHCP サーバとして動作している。
- Aichi1, L3ASW1, L3ASW2 において次の通り BGP を動作させる。
※ISP-A は AS200、ISP-B は AS300、ISP-C は AS600 所属として BGP が動作しており、ISP-A 及び ISP-B は BGP にてデフォルトルートをアドバタイズしている。
- Aichi1, L3ASW1, L3ASW2 は AS100 所属として BGP を動作させる。

（詳細省略）

内部ルーティングについて以下の通り設定しなさい。

- Aichi1, Tokyo1, Tokyo2, L3ASW1, L3ASW2 において次の通り EIGRP を動作させる。
 - 愛知本社、東京第一支社、東京第二支社の全てのプライベートアドレスセグメント間において通信可能となるように、経路交換を行う。Loopback インタフェースのアドレスも含む。ただし、グローバルアドレスセグメントは EIGRP ルーティングドメインには含まれない。
- L3ASW1, L3ASW2 は L3 スイッチとして機能させ、VLAN 間ルーティングを行う。

● WAN 設定

愛知本社、東京第一支社、東京第二支社間の VPN 環境について以下の通り設定しなさい。

- Aichi1, Tokyo1, Tokyo2 間に DMVPN を構成する。
- 各ルータについて DMVPN のインタフェースとして Tunnel0 を使用する。

(詳細省略)

● ゲートウェイの冗長化

L3ASW1, L3ASW2 において、以下の条件を満足するようにゲートウェイの冗長構成を実現しなさい。

- VLAN20 について、HSRP を次の通り動作させる。
- L3ASW2 を Active ルータとする。

(詳細省略)

- VLAN101 について、HSRP を次の通り動作させる。
- L3ASW1 を Active ルータとする。

(詳細省略)

● NAT 設定

アドレス変換を以下の通り設定しなさい。

- 東京第二支社のネットワークからインターネットへ接続できるように Tokyo2 に NAT を設定する。インターネット側のインタフェースアドレスに変換されること。
- tsv をインターネットと相互接続可能とするために、Tokyo1 にてスタティック NAT の設定を行う。200.100.30.6 にて接続が行えるようにすること。

● スイッチ設定

L3ASW1, L3ASW2, ASW3, ASW4 について以下の通り各種設定を行いなさい。

- L3ASW1, L3ASW2, ASW3, ASW4 について、VTP モードを透過モードとする。
- トランクプロトコルとして IEEE802.1q を使用する。
- L3ASW1 と L3ASW2 間の接続について、Etherchannel を設定する。
 - Port-channel 1 を使用する。
- STP(Spanning Tree Protocol)について、次の通り設定する。

(詳細省略)

Linuxサーバ設定課題

以下の設定項目に従い、Linux サーバ仮想マシン（asv1, asv2, tsv）を設定しなさい。設定項目は、サーバ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。

● 基本設定

asv1、asv2、tsvについてデフォルトゲートウェイを適切に設定しなさい。また、ネームサーバアドレスとして自身のアドレスを指定しなさい。

● CA（認証局）

asv2 にて CA を以下の通り設定しなさい。

- asv2 に CA を構築する。使用するパッケージは openssl とする。
- 作成した CA 関連ファイルは /ca （及びそのサブディレクトリ）に格納する。
- ルート CA 証明書(ファイル名:/ca/cacert.pem)を次の設定で作成する。CA 秘密鍵(ファイル名:/ca/private/cakey.pem)は root ユーザのみアクセス可能とし、パスフレーズは「skills」とする。
 - Country Name : JP
 - State or Province Name : Aichi
 - Organization Name : IT SKILLS LTD
 - Common Name : ca.skills.it.jp

● Bonding

asv1 にて bonding を以下の通り設定しなさい。

- 使用するパッケージは ifenslave とする。
- ens192 および ens224 をメンバーとする bonding インタフェース bond0 を設定する。
(詳細省略)

● ロードバランサ

asv1 にてロードバランサを以下の通り設定しなさい。

- 使用するパッケージは haproxy とする。
- フロントエンドサーバとして asv1 は、https://www.skills.it.jp/ への接続を受け付ける。

(詳細省略)

- HTTP 接続(TCP80 番)要求は、HTTPS(TCP443 番)へリダイレクトする。

(詳細省略)

● Web サービス

asv1 にて Web サービスを以下の通り設定しなさい。

- 使用するパッケージは apache2、php とする。
- apache2 における HTTP サービスポートを TCP8000 番とする。

(詳細省略)

asv2 にて Web サービスを以下の通り設定しなさい。

- 使用するパッケージは apache2 とする。
- http://asv2.skills.it.jp/へのアクセスについて/var/www/html/index.html を応答する。
ホスト名 “asv2” を表示するだけでよい。ロードバランサによる負荷分散先となる。

(詳細省略)

● DNS サービス

asv1、asv2、tsv にて DNS サービスを以下の通り設定しなさい。

- 使用するパッケージは bind9 とする。
- 競技課題の要求仕様から必要となるレコードがあれば各自判断して追加すること。

(省略)

asv1 にて DNS サービスを以下の通り設定しなさい。

- 自身で名前解決できない場合は、ISPserver (200.99.1.1) へ回送する。
- 社内からのみ再帰検索を許可する。
- 社内からの skills.it.jp に対する問い合わせは、asv2 へ回送する。
- tsv へのみゾーン転送を許可する。
- インターネット向けの skills.it.jp ゾーンの管理を行うマスターサーバとして次の通り動作させる。

(詳細省略)

asv2 にて DNS サービスを以下の通り設定しなさい。

- 自身で名前解決できない場合は、asv1 へ回送する。
- 社内向けの skills.it.jp ゾーンの管理を行うマスターサーバとして次の通り動作させる。
(詳細省略)

tsv にて DNS サービスを以下の通り設定しなさい。

- 自身で名前解決できない場合は、ISPserver (200.99.1.1) へ回送する。
- 社内からのみ再帰検索を許可する。
(詳細省略)

● LDAP サービス

asv2、tsv にてディレクトリサービスを以下の通り設定しなさい。

- 使用するパッケージは slapd とする。
- 管理者パスワードは、skills2019 とする。
- SYNC レプリケーションにより、asv2 と tsv 間でデータの同期を取る。
- slapd によるディレクトリサービスの構築ができない場合、必要なアカウントをシステムアカウントとして作成すること。

asv2 にてディレクトリサービスを以下の通り設定しなさい。

- ユーザアカウントとして、muser01～muser10 を作成する(※muser01,muser02・・・muser10 の 10 人分を作成する)。パスワードは skillP@ss とする。
- SYNC レプリケーションのプロバイダとしてサービスを提供する。

tsv にてディレクトリサービスを以下の通り設定しなさい。

- SYNC レプリケーションのコンシューマとしてサービスを提供する。

●Mail サービス

asv1 にてメールサービスを以下の通り設定しなさい。

- 使用するパッケージは、postfix とする。
- メールゲートウェイとして動作させる。
- skills.it.jp ドメインのプライマリメールサーバとなる。

(詳細省略)

asv2 にてメールサービスを以下の通り設定しなさい。

- 使用するパッケージは、postfix、dovecot-pop3d とする。
- skills.it.jp ドメイン宛てのメールをスプールする。
- LDAP で作成したユーザでメールをスプールできるようにする。

(詳細省略)

tsv にてメールサービスを以下の通り設定しなさい。

- 使用するパッケージは、postfix、dovecot-imapd とする。
- br.skills.it.jp ドメインのプライマリメールサーバとなる。
- br.skills.it.jp ドメイン宛てのメールをスプールする。
- LDAP で作成したユーザでメールをスプールできるようにする。

(詳細省略)

●iptables

asv1 に iptables によるパケットフィルタを以下の通り設定しなさい。

- asv1 への着信トラフィックについて次の通り制御する。
 - ✧ ポリシーを DROP とする。
 - ✧ 課題の要求から必要となる許可ルールを追加する。
 - ✧ SSH サービスについて、asv2 からの接続のみ許可する。
 - ✧ ICMP について、エコー要求のみ許可する。
- システム再起動後も有効となること。

クライアント設定課題

以下の設定項目に従い、クライアント仮想マシン（clientPC）を設定しなさい。

●clientPC の設定

- IP アドレスとして 192.168.2.1、DNS サーバとして tsv のアドレスを設定し、ネットワーク接続可能な状態にしておくこと。
- ブラウザ(IE)にて <https://www.skills.it.jp/> にアクセスした際に、ラウンドロビンにて asv1 または asv2 のサイトが表示され、証明書エラーが表示されないこと。
- メーラー(Thunderbird)を設定する。メール送信及び受信サーバとして tsv を使用する。メールアドレス muser01@br.skills.it.jp にて社内外とのメール送受信が行えるようにすること。

参考資料 L 第 57 回大会 課題 3 (一部省略版)

TEST PROJECT

(競技課題)

IT NETWORK SYSTEM ADMINISTRATION

DAY 2

令和 元年 1 1 月 1 7 日

9 時～ 1 2 時 (3 時間)

愛知県国際展示場 (Aichi Sky Expo)

注意事項

- 競技会に個人の資料やソフトウェアを持ち込まないでください。
- 携帯電話は使用しないでください。
- 競技の資料/情報を競技の間に誰かに開示しないでください。
- デュアルディスプレイを使って、見学者にメッセージを送らないようにしてください。
- 作業を開始する前に、この競技課題を良く読んでください。
- 作業の順番等を計画して競技に取り組んでください。

座席番号	氏名



1. INTRODUCTION

競技は開始時間と終了時間が決められています。3 時間です。選手は時間をどのように使うかは自由です。

重要：このドキュメントは手順書ではありません。必要とされる事項を記述していますが、そのために必要な手順を全て記述している訳ではありません。要求を満足するために必要な処理があれば、記載されていなくても実行してください。ただし、そのために要求を満たせなくなつては困ります。要求と矛盾するかどうかは選手各自で判断する必要があります。なお文章はほんの少し難解な表現（google 翻訳程度）かもしれませんが、読み間違えないように十分注意し、各自で解釈判断してください。

- ・競技で使用する全てのシステムは VMWare ESXi 上とネスト（入れ子）した Windows Server 2016 上の仮想マシンで実現しています。（実装図を参照）
- ・Hyper-V コンソールを使って、各仮想マシンを操作します。（物理トポロジー図と実装図を参照）
- ・Hyper-V ホストマシン(SKILLSSV)の administrator パスワードは"P@ssw0rd"（引用符なし、w の次の文字は数字の 0 です）です。
- ・ドメインの administrator パスワードは"Skills2019"（引用符なし）です。その他のパスワードは指定のない限り"P@ssw0rd"（引用符なし）を使用してください。

この課題では以下のファイルが用意されています。

1. SKILLS2019_Module_3_Users.csv
2. ImportBulkUserFromCsv.ps1
3. extranet.html, public.html

これらのファイルは DC1 の administrator のデスクトップに置いてあります。

更に、Hyper-V ホストマシン(SKILLSSV)の administrator のデスクトップには、OS インストール用の ISO イメージファイルや readme ファイルなど必要と思われるファイルが置かれています。自由に使って構いません。

2. DESCRIPTION OF PROJECT AND TASKS

概要

あなたは 愛知での情報システムを担当する IT エンジニアです。複数のユーザーを持ち、構成が既に設定されている Windows Domain を引き継ぎました。ネットワークを改善するために、更なるタスクを実施することになりました。あなたはドメイン内の人々がアクセスするいくつかの Web サイトを完全に実装しなければなりません。そのために、Hyper-V をベースとした高可用性システムを使用します。あなたは、この Hyper-V インフラストラクチャを使って、既存ドメイン内外のサーバーインフラストラクチャを改善していきます。指示に従ってプロジェクトを完遂してください。

このプロジェクトでは以下の事項を実現します。

1. ネットワーク内のインフラストラクチャをアップグレードします。
2. アプリケーションサービスを提供するための仮想サーバーを構成します。
3. Internet(172.16.0.0/24)にアクセスするためにゲートウェイを構成します。



Part 1 – Intranet LAN

Part 1 では、ネットワーク内のインフラストラクチャをアップグレードします。システムのインストールや構成の状況は様々です。明確にするために、課題の最後にある VM 構成表を確認してください。

Work Task DC1（DC1 に対する要件）

要件に合うように既存のマシンを構成してください。

- ホスト名と IP アドレス等のネットワーク設定が、文書の最後にある構成表と図に一致することを確認してください。
- DC1 上のサーバーマネージャーで DC2 の制御ができるように設定してください。
- このサーバーは `aichi-sky.jp` のドメインコントローラとして事前構成されています。
- Active Directory を構成してください。
 - DC1 の administrator のデスクトップにおかれた PowerShell スクリプトを修正（スクリプトは正しくないので、このままではエラーになり、必ず修正が必要です）し、フォルダから提供された csv ファイルからユーザーをインポートしてください。アカウントを有効にし、グループメンバーシップ、`@aichi-sky.jp` サフィックスの付いたユーザープリンシパルネームなど、スプレッドシートに一覧化されているプロパティを持たせてください。適切な OU 内に置き、最初のログインでパスワード変更が必要ないようにしてください。
 - もし、スクリプトのバグがどうしても修正できない場合は以下のユーザー、OU、グループをテスト用に作成してください。

ユーザー名	OU	グループ	パスワード
agt-001	SKY	Agents	Pa\$\$worD
agt-011	WSC	Agents	Pa\$\$worD
cpt-001	SKY	Competitors	Pa\$\$worD
cpt-011	WSC	Competitors	Pa\$\$worD
exp-001	SKY	Experts	Pa\$\$worD
exp-011	WSC	Experts	Pa\$\$worD
mgr-001	SKY	Managers	Pa\$\$worD
mgr-011	WSC	Managers	Pa\$\$worD
vst-001	Others	Visitors	Pa\$\$worD
vlt-021	WSC	Volunteers	Pa\$\$worD

- DNS サーバーを構成してください。
 - ドメインに参加したサーバーに加え、以下のレコードを追加してください。
 - `web.aichi-sky.jp` の CNAME レコード
 - `www`, `extra`(一部省略)
- DHCP サービスを構成してください。
 - DC1 をアクティブサーバーとして設定してください。（DC2 でフェイルオーバーサブネットを構成してください。）
 - 範囲 `192.168.1.51 – 75`(一部省略)



- スコープオプション
 - DNS : 192.168.1.1, 192.168.1.101, Gateway : 192.168.1.254
 - このスコープの 70%を DC1 に、残りを DC2 に割り当ててください。
(一部省略)
- 将来 (Part2) の Hyper-V クラスタへの展開に備えて Windows 展開サービス(WDS)を追加してください。
 - Windows 展開サービスを実行するユーザーには、Windows Server 2016 を GUI または非 GUI インターフェイスを使用してインストールするオプションがあります。
 - Hyper-V サーバークラスタが作成されたら、その中に、Windows 展開サービスを通じて WEB 仮想マシンを展開 (deploy) してください。
- 以下のグループポリシーを構成して適用してください。
 - ログオン時に”Welcome to Skills 2019”と書かれたログインバーナーが表示されるように、”banner”という GPO を作成してください。
(一部省略)

Work Task DC2 (DC2 に対する要件)

以下の要件に従って構成してください。

- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- aichi-sky.jp ドメインの 2 番目のドメインコントローラとしてこのサーバーを構成してください。
- DNS サービスを構成してください。
 - Active Directory 統合 DNS ゾーンとして使用してください。
- DHCP サービスを構成してください。
 - DC1 に関する要求項目を参考に、フェイルオーバースコープを構成してください。
- 10G ドライブを 3 つ追加してください。
- ディスクシステムを NTFS でシングル RAID5 アレイ (G : I) にフォーマットし、このボリューム上で重複除去を有効にしてください。
(一部省略)
- 毎日 4 時に DC2 上のホームフォルダがバックアップされるようにバックアップジョブを作成してください。
- Work Folder を構成してください。
 - ローカルパス : “G : \work\”
- ローカルパス “G : \WSC” にファイル共有を作成し、\\DC2\WSC として共有してください。
 - “G : \WSC”内に 2 つのサブフォルダを作成し、各フォルダにアクセスコントロールを以下のように構成してください。ただし、Administrators に関する権限は変更しないこと。
 - “Test Projects” フォルダを作成してください。
 - “Experts” グループに属するユーザーには読み取り専用のアクセスを許可してください。
 - “Managers”グループに属するユーザーにはフルアクセスを許可してください。



- “Secret Challenges”フォルダを作成してください。
 - “Agents”グループに属するユーザーには変更アクセスを許可してください。
 - このフォルダは、アクセス権限が十分でないユーザーに対しては非表示にしてください。
- DFS (Distributed File System) をインストールして構成し、“WSC”共有と DC1 の“Public”共有が、\\aichi-sky.jp\shares にアクセスすることで実現されるようにしてください。

Work Task INTCLIENT (INTCLIENT に対する要件)

以下の要件に従って構成してください。

- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- aichi-sky.jp ドメインに参加してください。
- このマシンを使って以下を行ってください。
 - ウェブサイトへのアクセスをテストしてください。
 - GPO をテストしてください。
 - ホームと Work Folder をテストしてください。
 - ユーザーが正しくインポートされたことを確認してください。



Part 2 – Virtualized Server Farm

あなたは、コアドメインインフラストラクチャの構成を終了しました。Part 2 では、高可用な構成を通じて更にインフラストラクチャやアプリケーションサービスを提供するために、仮想サーバを構成します。システムのインストールや構成の状況は様々です。明確にするために、課題の最後にある VM 構成表を確認してください。以下の要求を満足するように構成を行い、タスクを完了してください。

Work Task STORAGE（STORAGE に対する要件）

以下の要件に従って構成してください。

- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- IP アドレス : 10.0.0.10
- iSCSI ターゲットを構成してください。
 - 仮想マシンを格納するために、200GB の新しいディスクを追加してください。
(一部省略)

Work Task HYPERV1 と HYPERV2（HYPERV1 と HYPERV2 に対する要件）

以下の要件を満たすように Hyper-V サーバーを構成してください。

- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- HYPERV2 上のサーバーマネージャーで HYPERV1 の制御ができるように設定してください。
- iSCSI イニシエーターを構成してください。
 - iSCSI ディスク "SKILLS2019-VM" に接続し、利用可能な最大のサイズで ReFS パーティションを作成してください。
- フェールオーバークラスターを構成してください。
 - Name : HYPERV-CLUS
 - IP アドレス : 192.168.1.200
(一部省略)

Work Task WEB（WEB に対する要件）

WDS Deployment を通じてクラスタにインストールし、構成してください。

- WDS を構成できないか、あるいは WDS を正常に機能させることができない場合には、OS イメージを使って Hyper-V クラスタに直接インストールしても構いません。また、Hyper-V クラスタが正常に機能しない場合は、Hyper-V ホストマシンに別の VM としてインストールしても構いません。なお、WDS でインストールした場合、キーマップが US なので注意してください。
- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- 与えられた HTML ファイル（DC1 の administrator のデスクトップに配置）を使って IIS とウェブサイトをインストールし、構成してください。
 - <http://www.aichi-sky.jp/> でアクセスされた場合



- ウェブサイトルートへのパス : "C : \inetpub\internet"
- Web ページの表示内容 : public.html

(一部省略)

- リモートデスクトップサーバを構成してください。
- RDWeb アクセスを使用してサーバーのアプリケーションを本社のユーザーが使用できるように設定を行ってください。
 - 「<http://www.aichi-sky.jp/RDWeb>」へアクセスすると RDWeb のログイン画面が表示されるようにしてください。

(一部省略)



Part 3 – INTERNET

Part 3 では、ネットワークデバイスの設定を行います。Internet にアクセスするために GATEWAY を構成します。

Work Task GATEWAY（GATEWAY に対する要件）

以下の要件に従って構成してください。

- 文書の末尾にある構成表と図に一致するようにホスト名とネットワークの設定を行ってください。
- ドメイン内部の IP アドレスを Internet (172.16.0.0/24) 側に公開しないように NAT 機能を構成してください。

Work Task SKILLSSV

Hyper-V ホストマシンで GATEWAY 確認用に使えます。

- ホスト名やネットワークの設定は行っています。変更はしないでください。



VM 構成表 (Configuration Table)

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
DC1	Windows Server 2016 _{Desktop}	aichi-sky.jp	192.168.1.1	Yes – Configured as DC
DC2	Windows Server 2016 _{Core}	aichi-sky.jp	192.168.1.101	Yes
INTCLIENT	Windows 10 Enterprise LTSC	aichi-sky.jp	DHCP	Yes
HYPERV1	Windows Server 2016 _{Core}	aichi-sky.jp	192.168.1.10 10.0.0.1	Yes
HYPERV2	Windows Server 2016 _{Desktop}	aichi-sky.jp	192.168.1.20 10.0.0.2	Yes
STORAGE	Windows Server 2016 _{Desktop}	WORKGROUP	10.0.0.10	Yes
WEB	Windows Server 2016 _{Desktop}	aichi-sky.jp	192.168.1.100	No – WDS Deployment
GATEWAY	Windows Server 2016 _{Desktop}	WORKGROUP	192.168.1.254 172.16.0.100	Yes
SKILLSSV	Windows Server 2016 _{Desktop}	WORKGROUP	172.16.0.1	Yes

「Yes」はオペレーティング システムがプリインストールされ、ホスト名とネットワーク設定は構成されていません。

「Yes – Configured as DC」はオペレーティング システムがプリインストールされ、ホスト名とネットワーク設定は構成されています。更に DC として機能します。

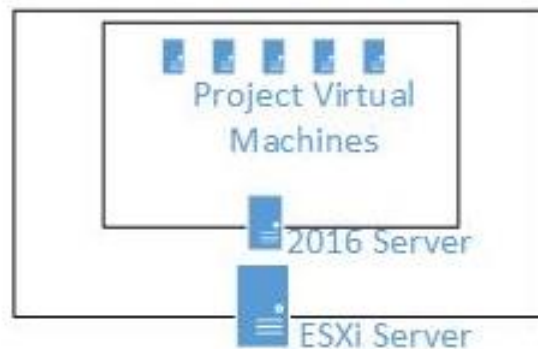
もし、GUI を持たない“Core”サーバーで構成や作業が困難、あるいは不可能であれば、“Core”サーバーを上書きし“Windows Server 2016 Desktop”で任意のマシンを再インストールしても構いません。ただし、採点上のペナルティは少々課せられますし、インストールの時間もかかってしまいます。



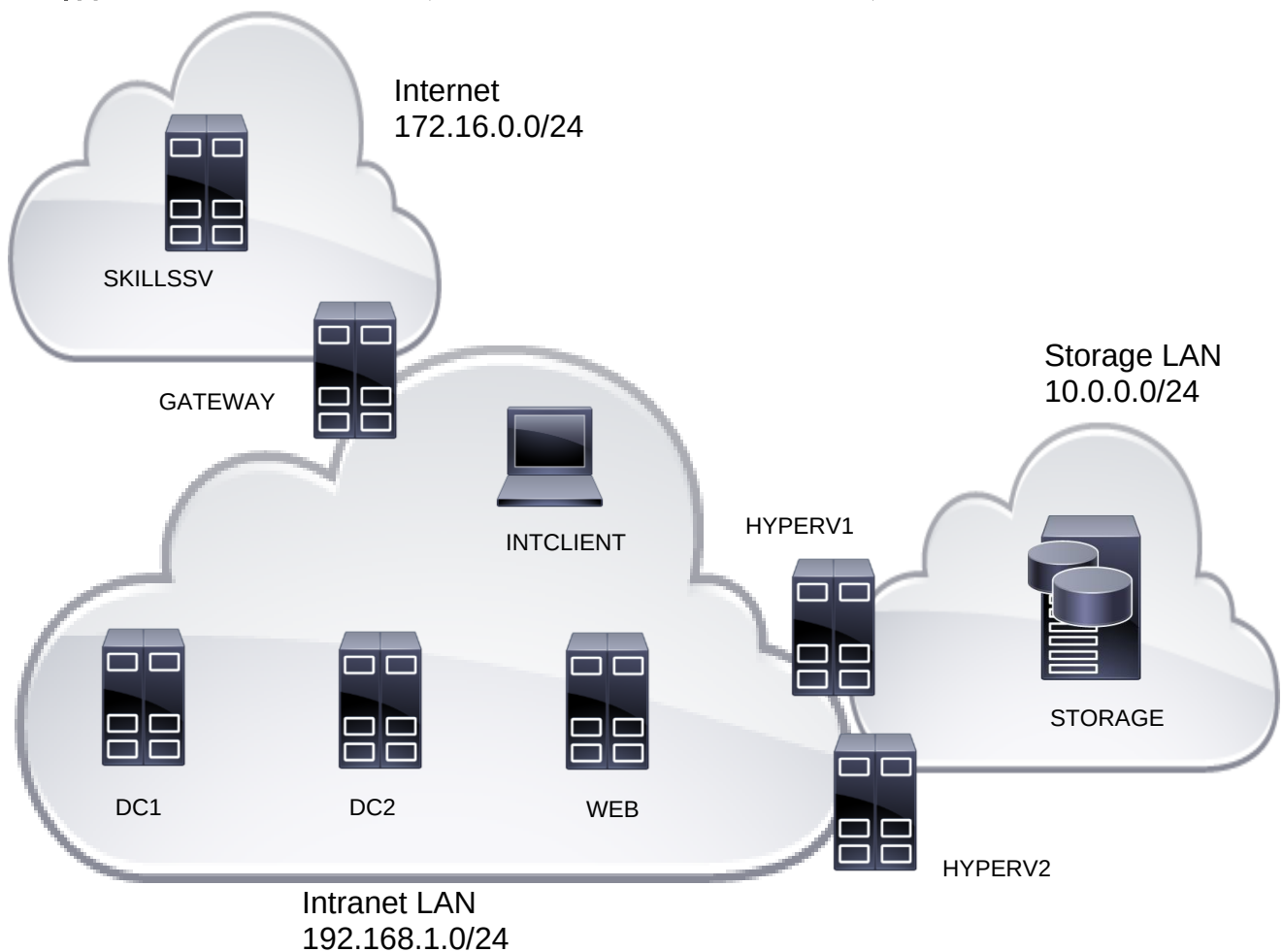
3. 物理トポロジー図 (PHYSICAL TOPOLOGY)



4. 実装図 (IMPLEMENTATION)

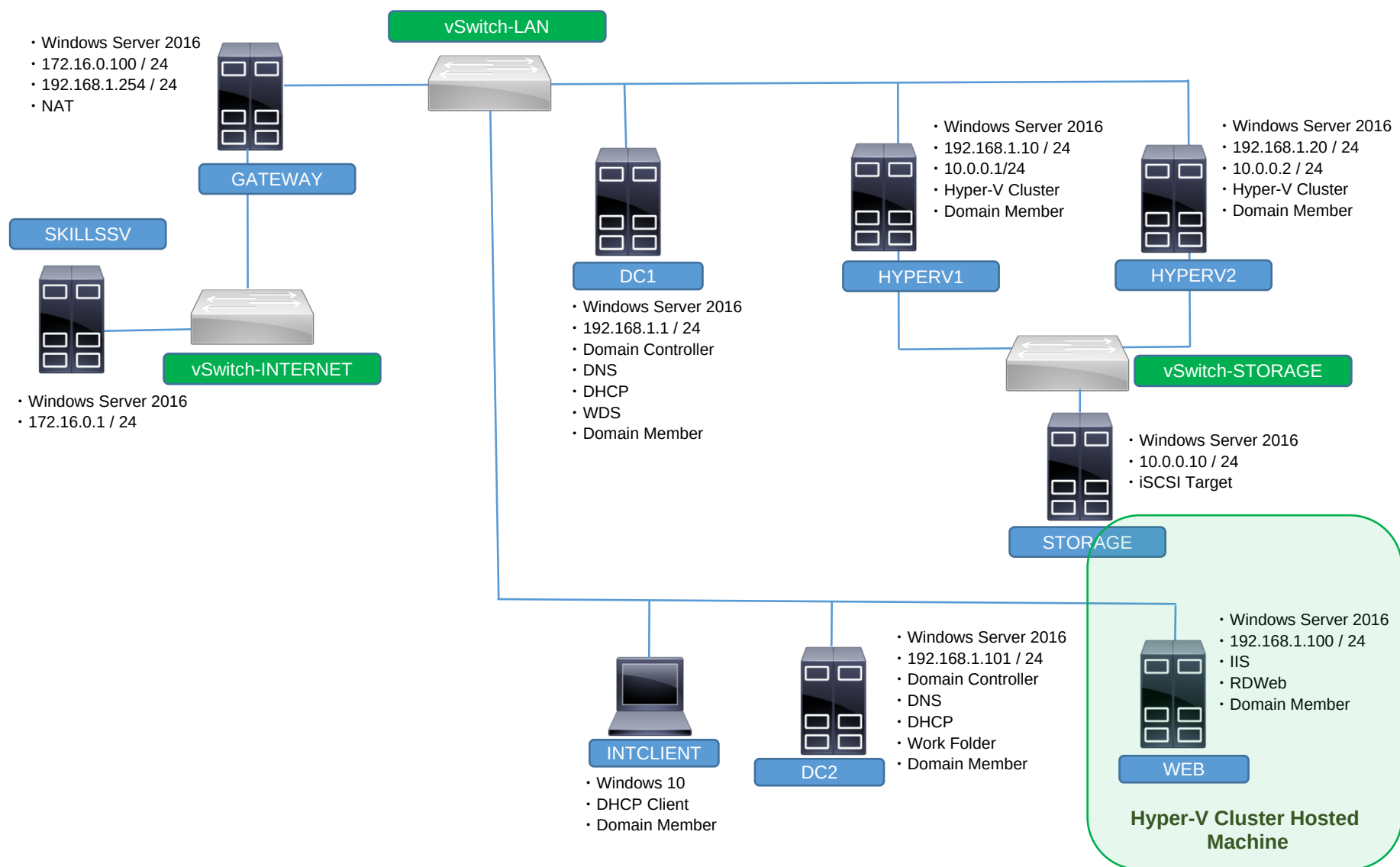


5. 論理トポロジー図 (LOGICAL TOPOLOGY)





6. ネットワーク構成図 (NETWAORK DIAGRAM)





7. メモ

