

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
(2021 年 第 59 回大会用)

令和 3 年 7 月 5 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。

競技環境については、2018 年大会から全面的に仮想環境へ移行していることに注意してください。

2. 競技日程

- 競技開始の前日 12 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） 12 月 18 日（土）
 - 8:40 集合
 - 8:45～ 9:00 説明
 - 9:00～11:00 競技「課題 1」
 - 11:00～11:50 昼食
 - 12:00～16:00 競技「課題 2」
 - 16:10 解散
- 競技 2 日目（競技時間：計 3 時間） 12 月 19 日（日）
 - 8:40 集合
 - 8:45～ 9:00 説明
 - 9:00～12:00 競技「課題 3」
 - 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 Intel Core i7 以上, メモリ 64GB 以上, SSD 500GB 以上
OS : VMware ESXi (VMware vSphere Hypervisor) 6.7
- 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 10.9 buster、Windows Server 2019 (評価版)
- クライアント OS : Windows10 (評価版)
- 仮想化基盤 : VMware ESXi (VMware vSphere Hypervisor) 6.7
- 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)

※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～D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. 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。構築規模としては、3～5 台程度の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：Postfix 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

C. 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。構築規模としては、4～6 台程度の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

D. 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、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
 - 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

- ※ 課題環境については、Windows、Linux、Cisco 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。
- ※ 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。
- 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. Linux サーバー環境構築」が 30%以下、「C. Windows サーバー環境構築」が 30%以下、「D. Cisco ネットワーク構築」が 30%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。
- ✓ スマートホン等（携帯電話やタブレットも含む）の電源は切っておくこと。
- ✓ モバイルルータ等を持ち込んでインターネットへアクセスすることは認めない。
- ✓ 競技時間中は、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。

9. 競技環境

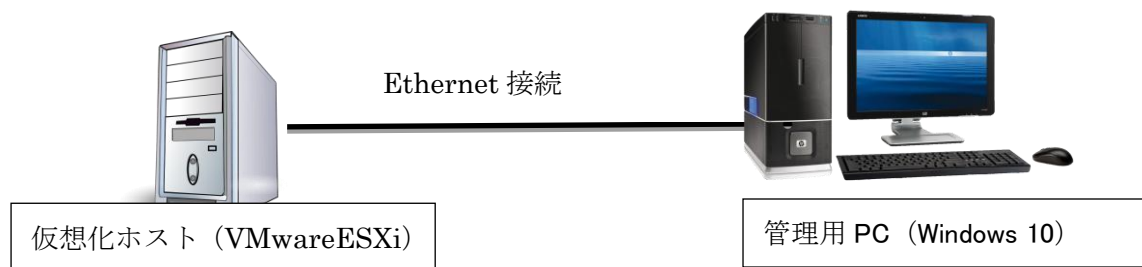


図 1：物理接続

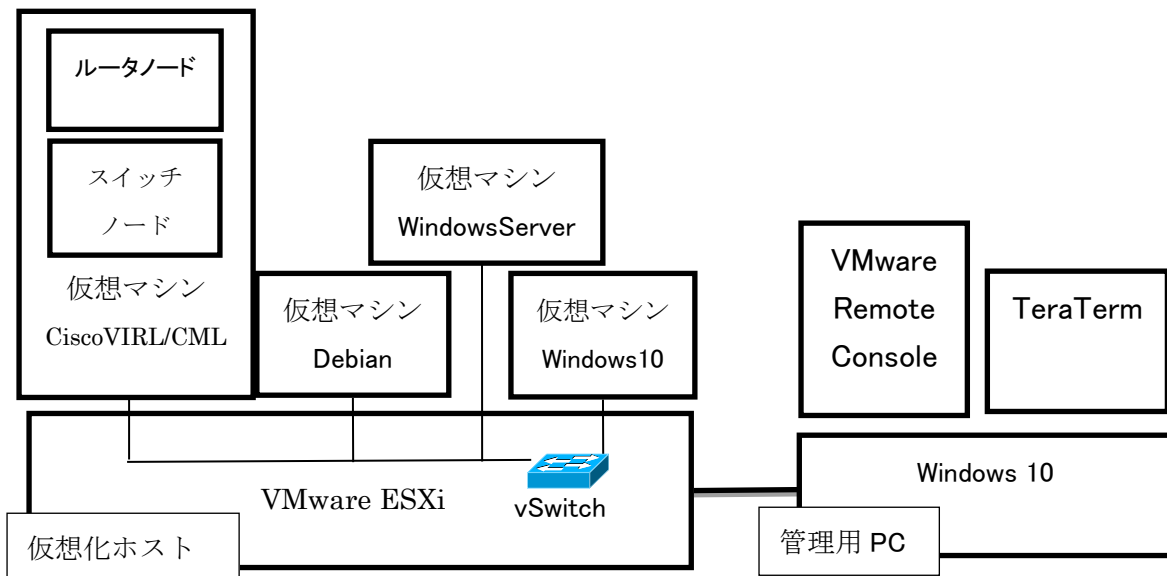


図 2：ソフトウェア配置イメージ

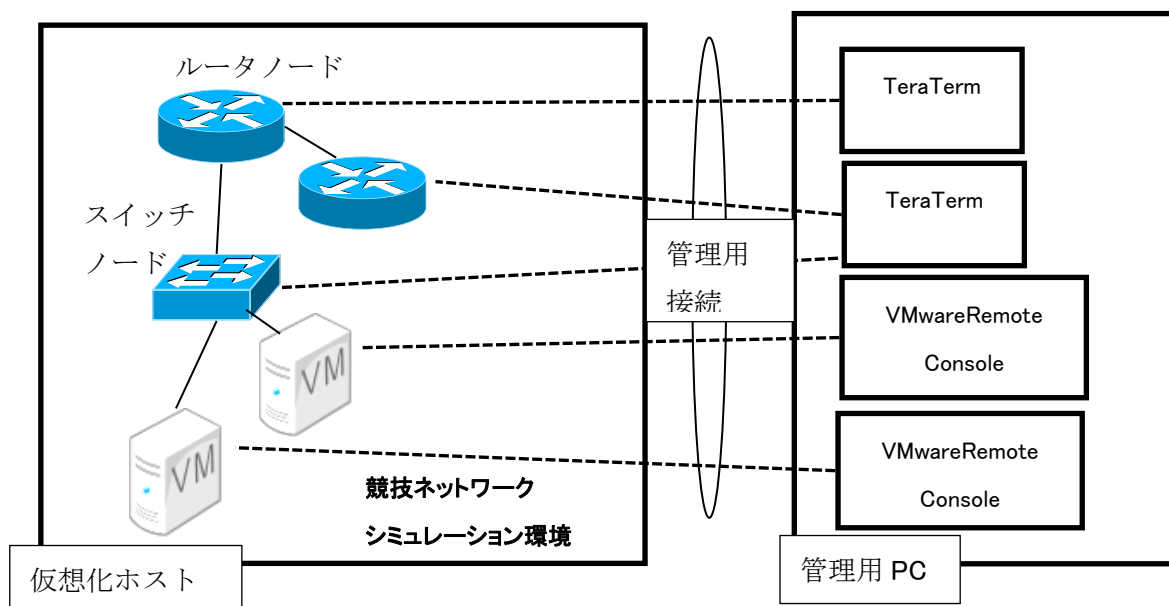


図 3：論理接続イメージ

従来、本職種におけるネットワーク構築課題では、ネットワーク機器として実機（Cisco 社製ルータおよびスイッチ）を使用してきましたが、機器の老朽化によるトラブルが懸念されます。また、第 44 回技能五輪国際大会においては、同職種の競技環境として、仮想環境 Cisco VIRL (Cisco Virtual Internet Routing Lab Personal Edition) が採用されています。競技運営の効率化も考慮し、Cisco VIRL を用いた仮想環境で競技を行います。Cisco VIRL については、バージョン 2 から Cisco Modeling Labs - Personal (CML-P) と名称が変更になっています。

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) スイッチノード

ノードタイプ: IOSvL2

バージョン: vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Version 15.x

c) ファイアウォールノード

ノードタイプ: ASA v

バージョン: Cisco Adaptive Security Appliance Software Version 9.x

d) 外部接続用ノード

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。

10. 参考資料

次項以降に昨年度課題の一部省略版と過年度の課題の概要を添付します。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（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-1 第 58 回大会 課題 1 概要

参考資料 A-2 第 58 回大会 課題 1 （一部省略版）

参考資料 B 第 58 回大会 課題 2 （一部省略版）

参考資料 C 第 58 回大会 課題 3 （一部省略版）

参考資料 D 第 57 回大会 課題 1 （一部省略版）

参考資料 E 第 57 回大会 課題 2 （一部省略版）

参考資料 F 第 57 回大会 課題 3 （一部省略版）

参考資料 G 第 56 回大会 課題 1 概要

参考資料 H 第 56 回大会 課題 2 概要

参考資料 I 第 56 回大会 課題 3 概要

参考資料 J 第 55 回大会 課題 1 概要

参考資料 K 第 55 回大会 課題 2 概要

参考資料 L 第 54 回大会 課題 1 概要

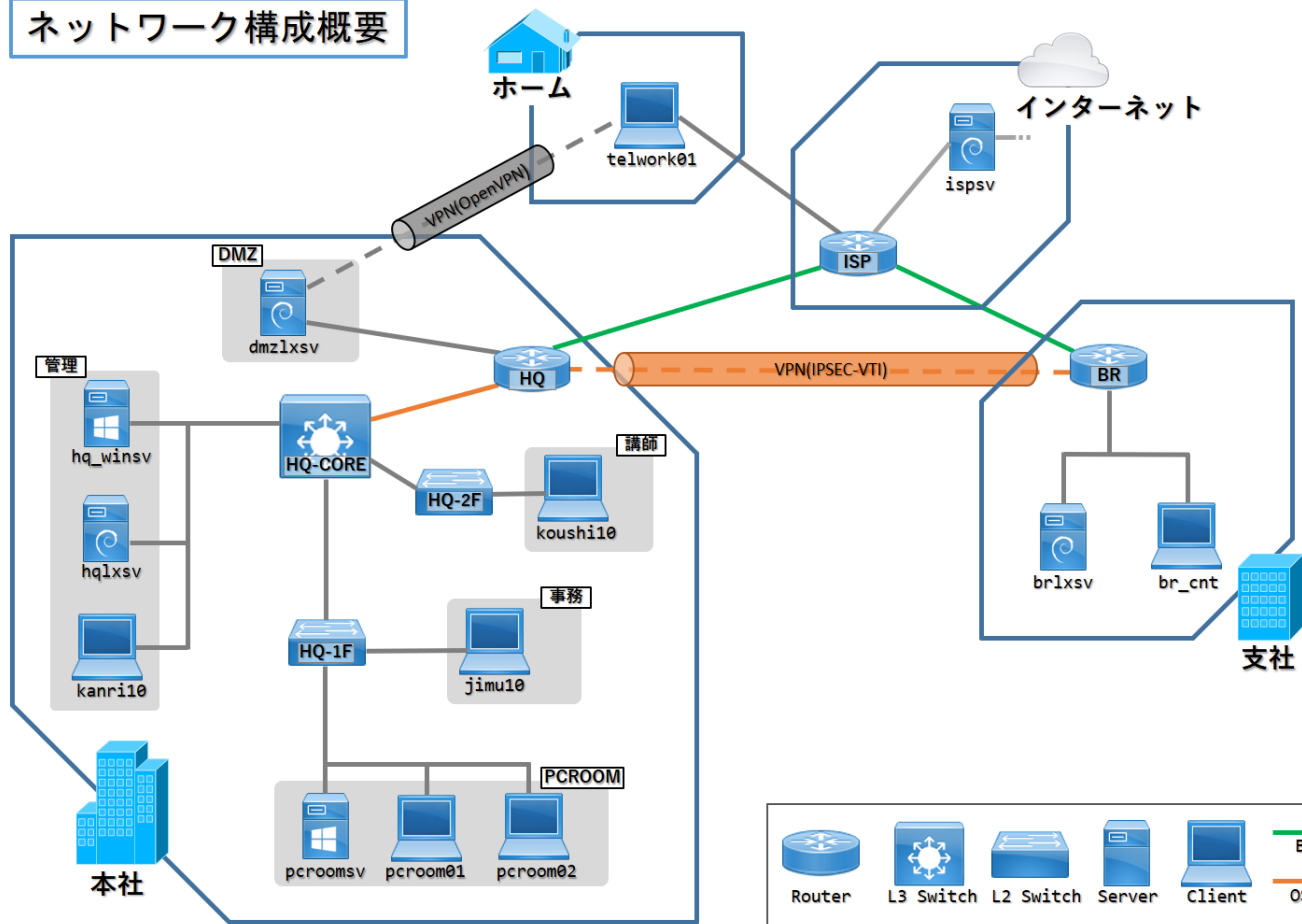
参考資料 M 第 54 回大会 課題 2 概要

参考資料 N 第 53 回大会 課題 1 概要

参考資料 O 第 53 回大会 課題 2 概要

参考資料 A-1 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 A-2 第 58 回大会 競技課題 課題 1 (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

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 2 年 11 月 14 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、株式会社愛知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 階に講師の控室と管理室がある。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。

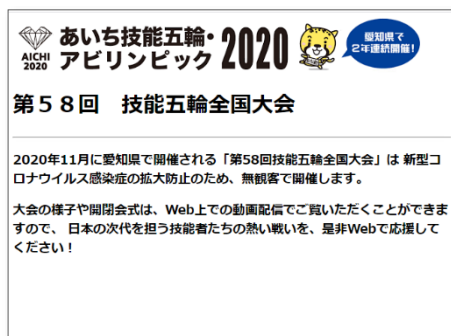
次頁以降のトラブルに対して適切な原因の把握と対応した処置内容を、各報告書に記載しなさい。なお、記載は明確で論理的な文章によって、以下の点が記述されていることがポイントとなる。

- 「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。

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-skills.jp/>



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

課 題 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。
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。

以下略

参考資料 B 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。

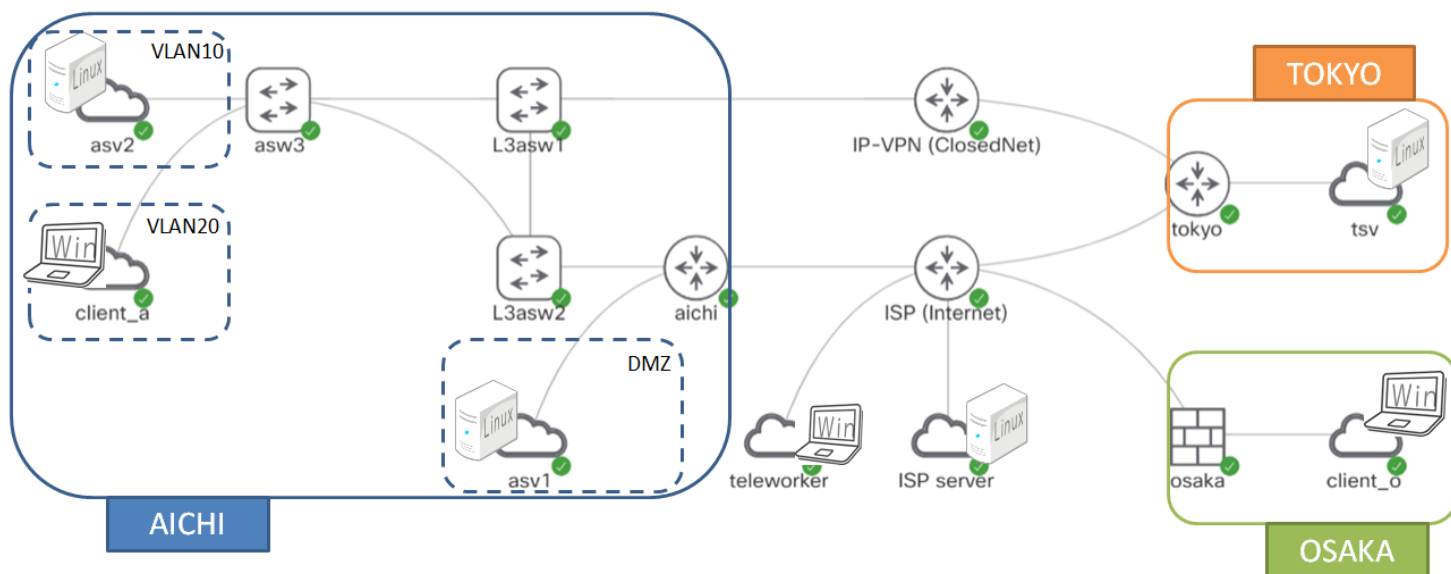


図1：ネットワーク構成概要

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 **asv1** 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 C 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(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cope 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。

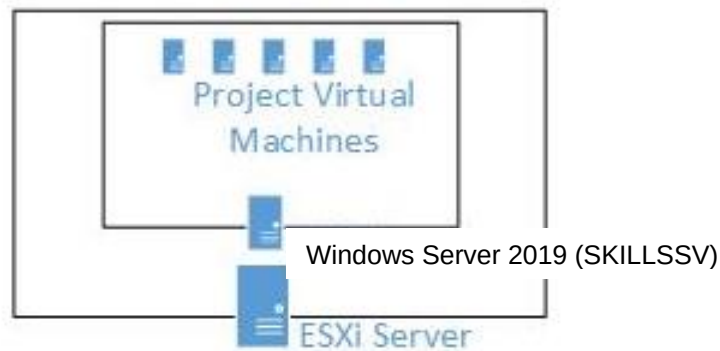
「Yes – Configured as DC」はオペレーティングシステムがプリインストールされ、ホスト名とネットワーク設定は構成されています。更に DC として機能します。

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。

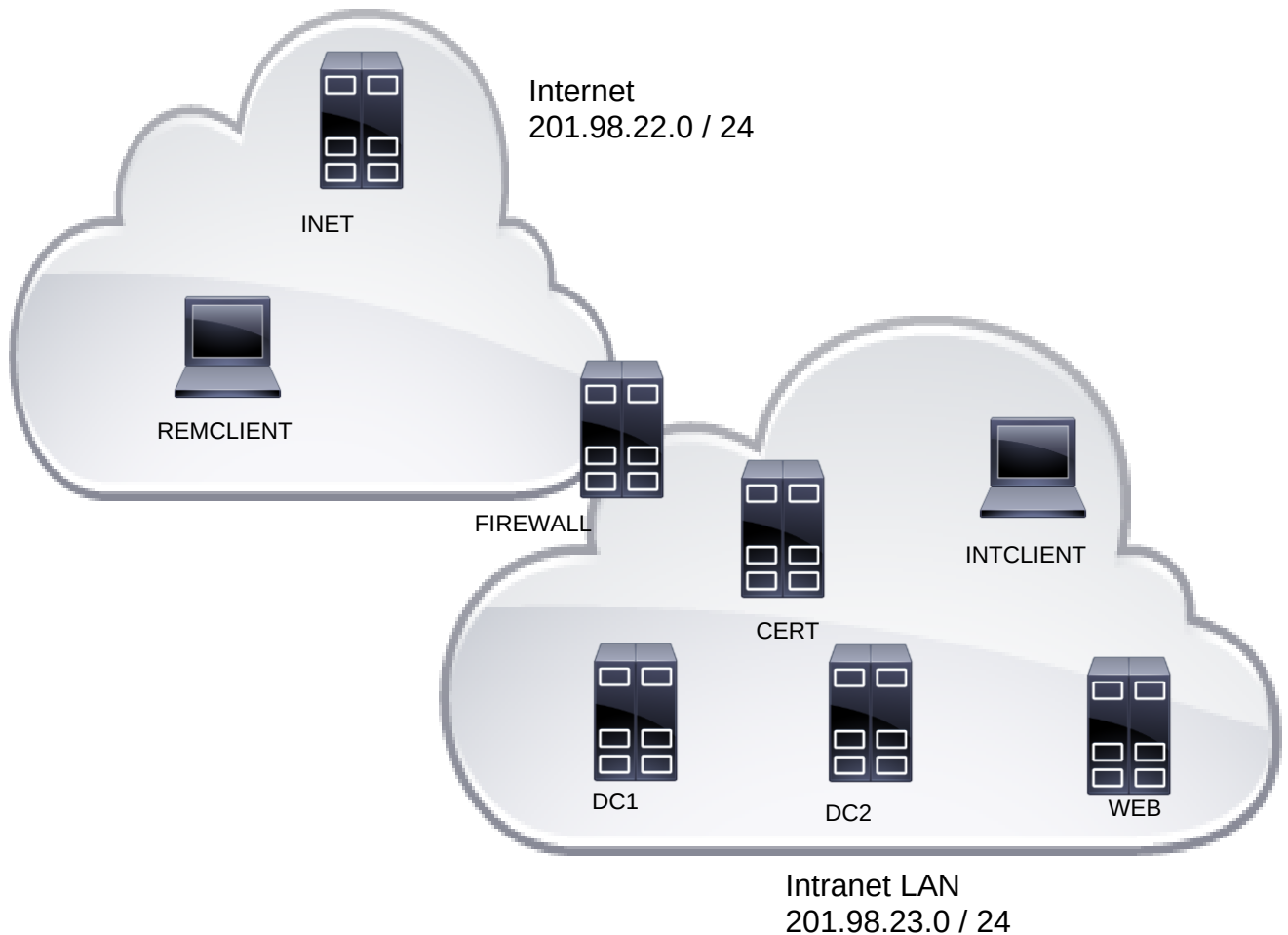
3. 物理トポロジー図 (PHYSICAL TOPOLOGY)



4. 実装図 (IMPLEMENTATION)

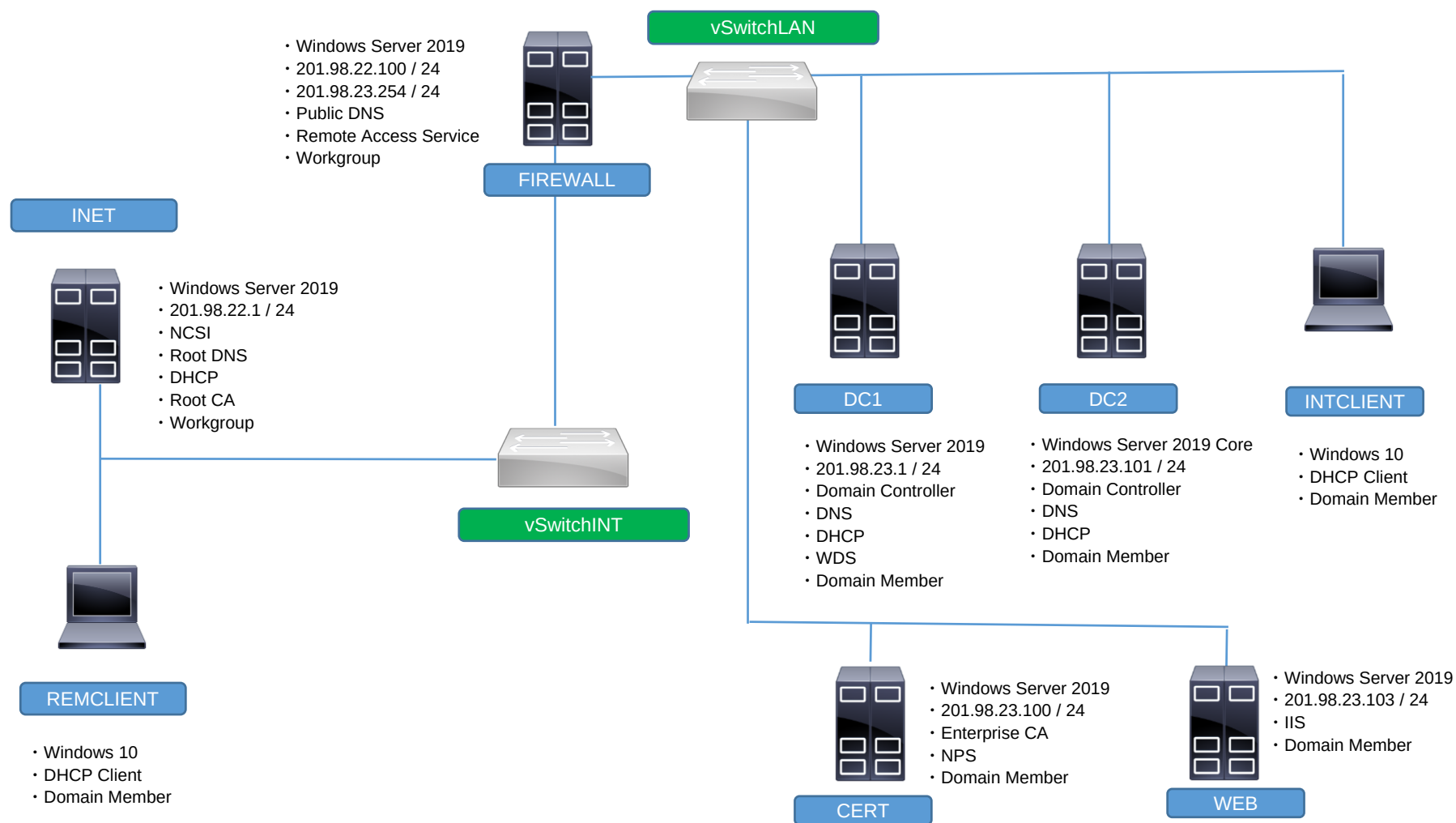


5. 論理トポロジー図 (LOGICAL TOPOLOGY)





6. ネットワーク構成図 (NETWORK DIAGRAM)



参考資料 D 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。

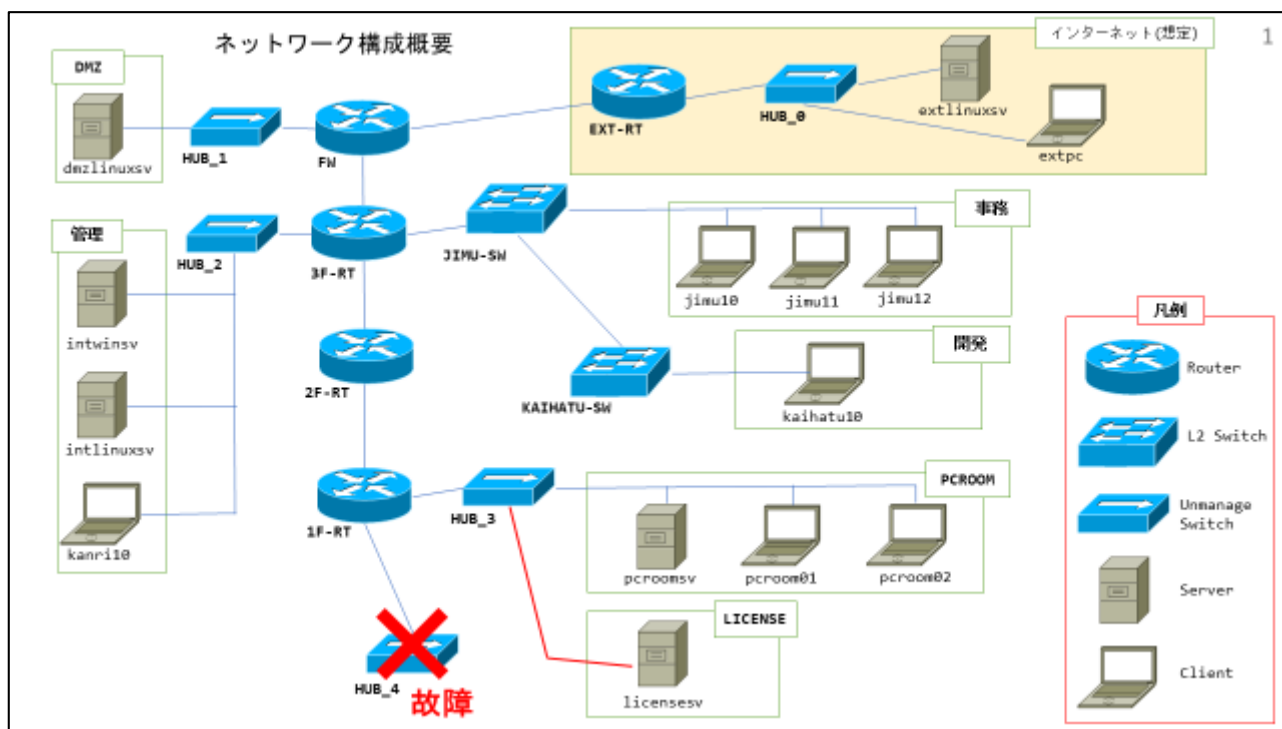


図 1 ネットワーク構成概要

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 E 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 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、asv2 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。

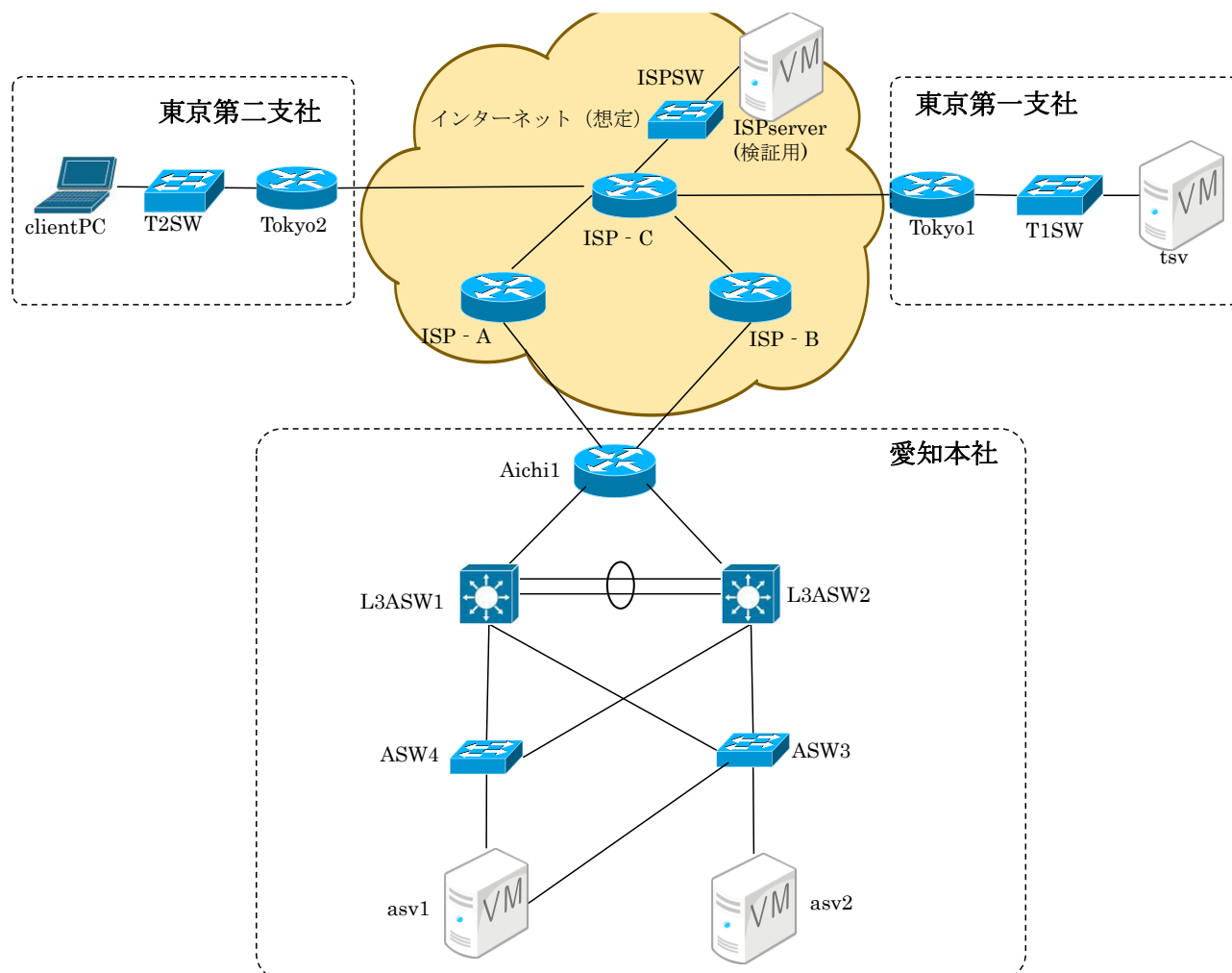


図 1：ネットワーク構成概要

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、taskset 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は静的に設定する。
- 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)ヘリダイレクトする。

(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 F 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。

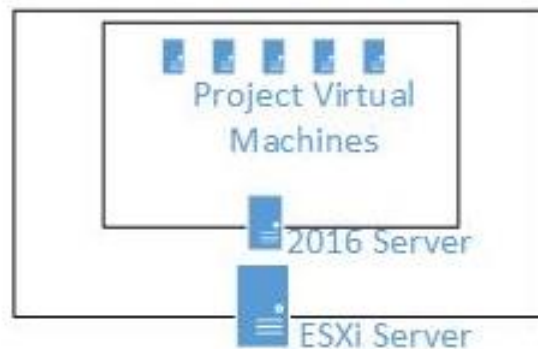
もし、GUI を持たない"Core"サーバーで構成や作業が困難、あるいは不可能であれば、"Core"サーバーを上書きし"Windows Server 2016 Desktop"で任意のマシンを再インストールしても構いません。ただし、採点上のペナルティは少々課せられますし、インストールの時間もかかってしまいます。



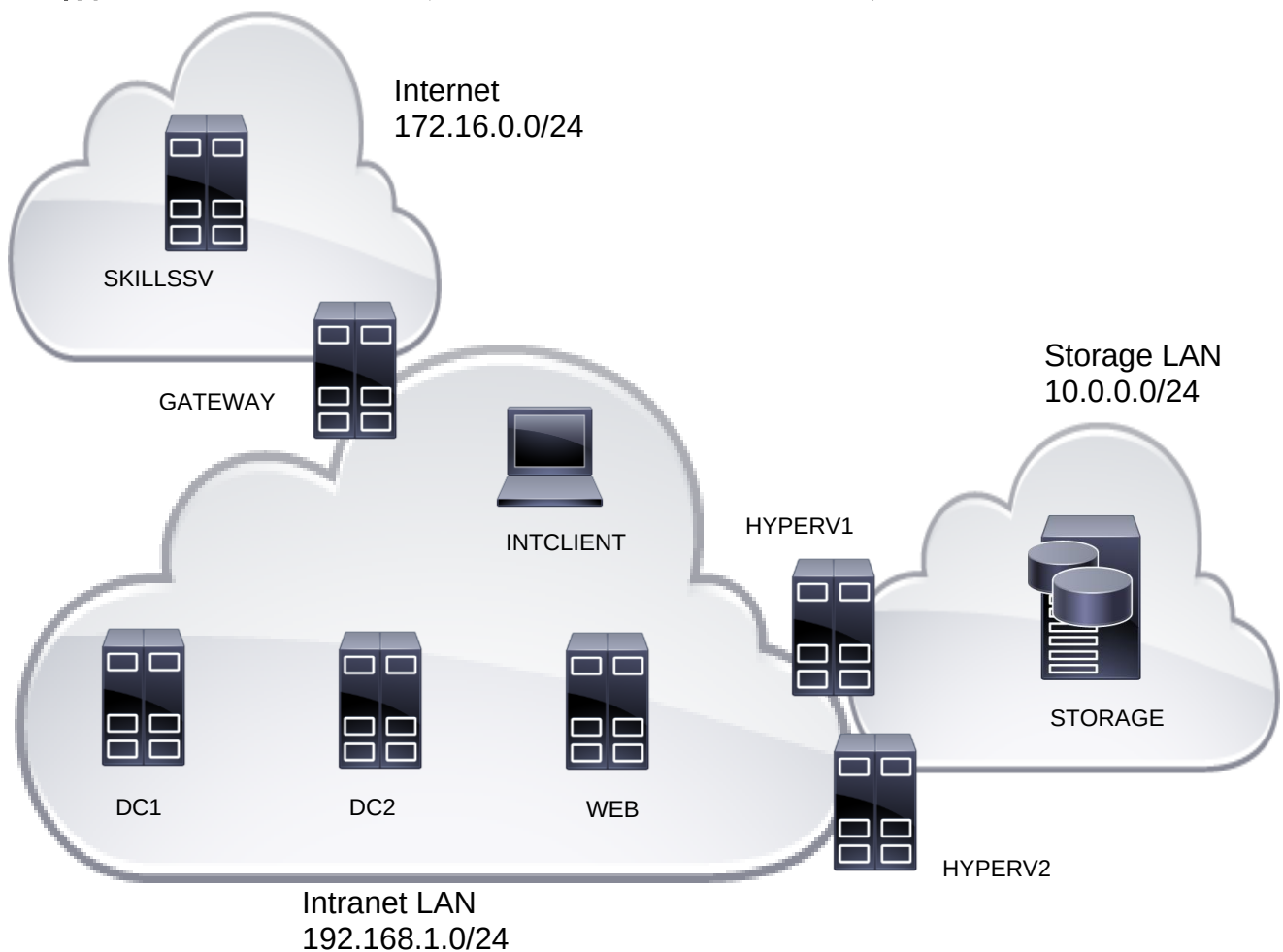
3. 物理トポロジー図 (PHYSICAL TOPOLOGY)



4. 実装図 (IMPLEMENTATION)

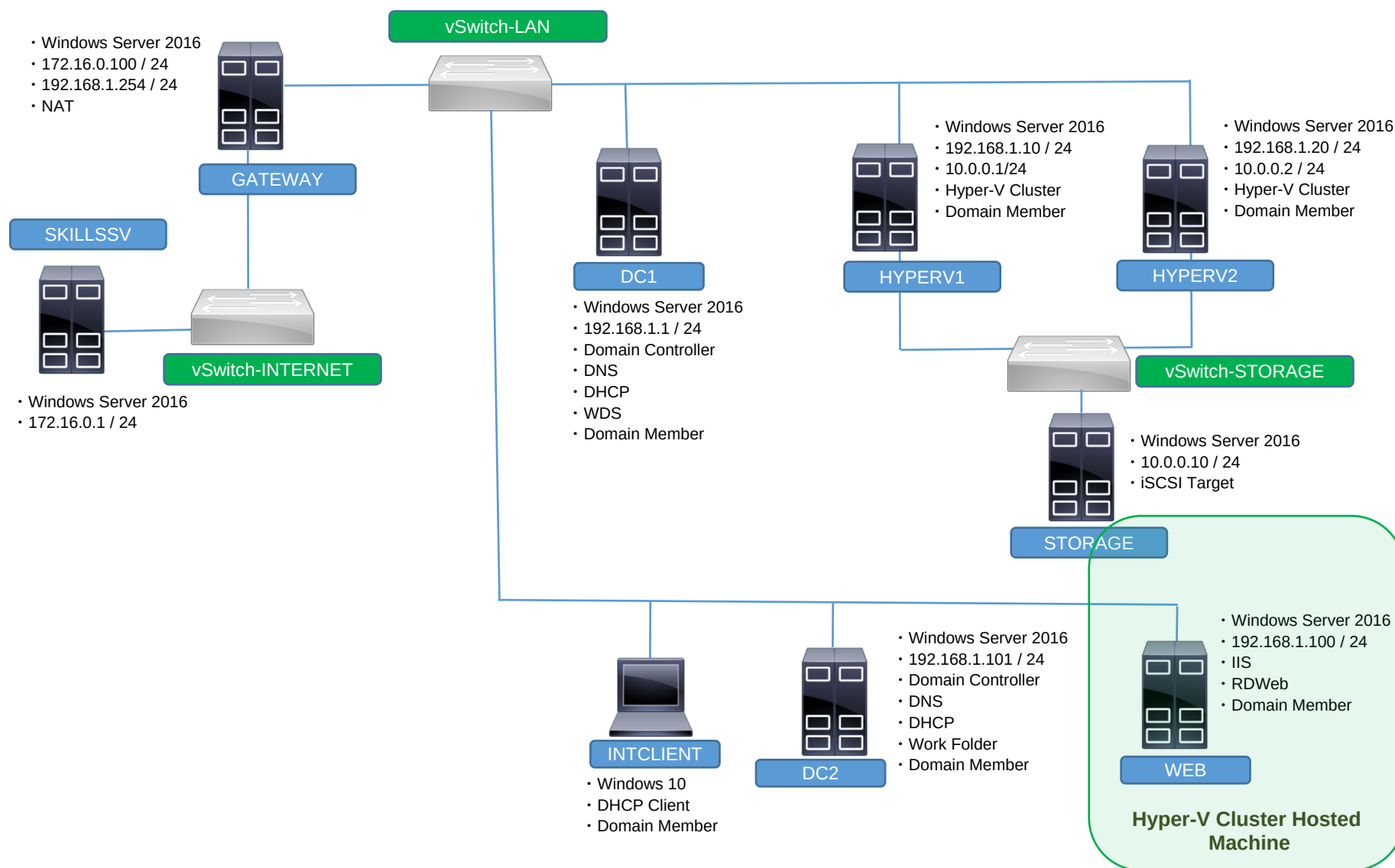


5. 論理トポロジー図 (LOGICAL TOPOLOGY)





6. ネットワーク構成図 (NETWAORK DIAGRAM)





7. メモ



参考資料 G 第 56 回大会競技課題 課題 1 トラブルシュート 概要

競技課題の背景

あなたは、株式会社沖縄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・運用管理する情報管理部の社員である。事業所内ネットワークの保守・管理を行うことが業務の 1 つである。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

図 1 に沖縄スキルシステムズのネットワーク構成の概要を示す。詳細については、別添の課題環境資料を参照しなさい。

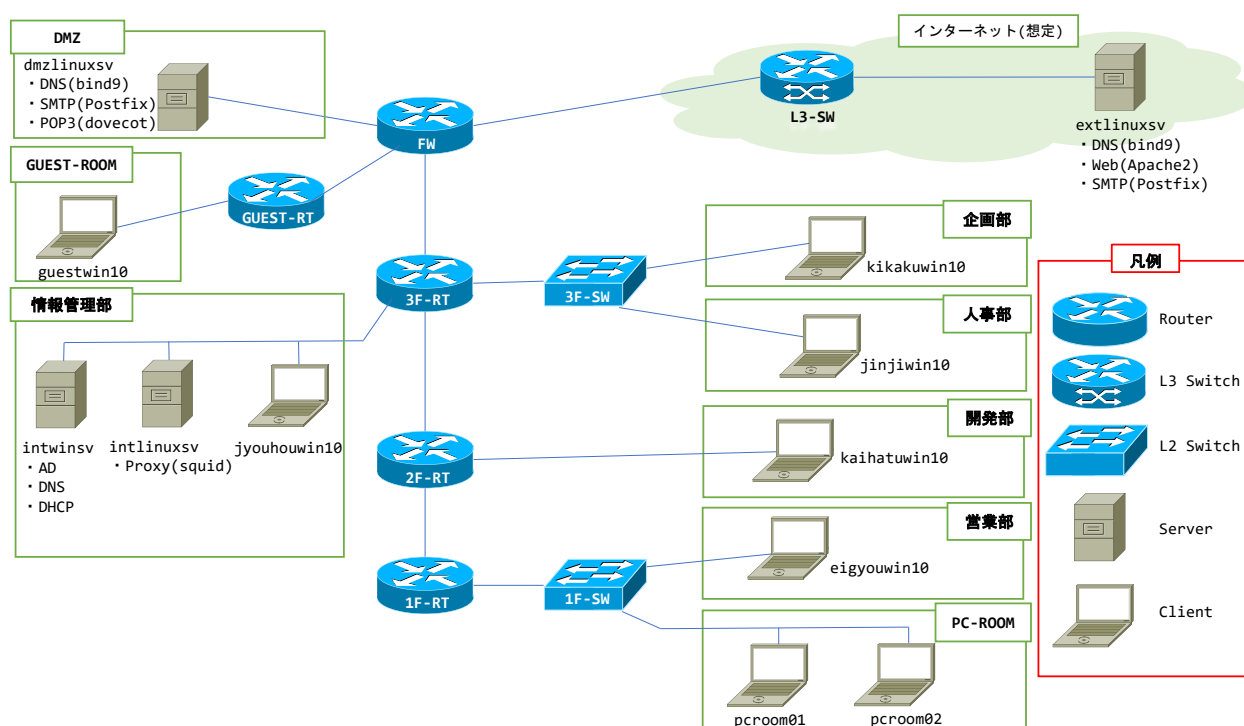


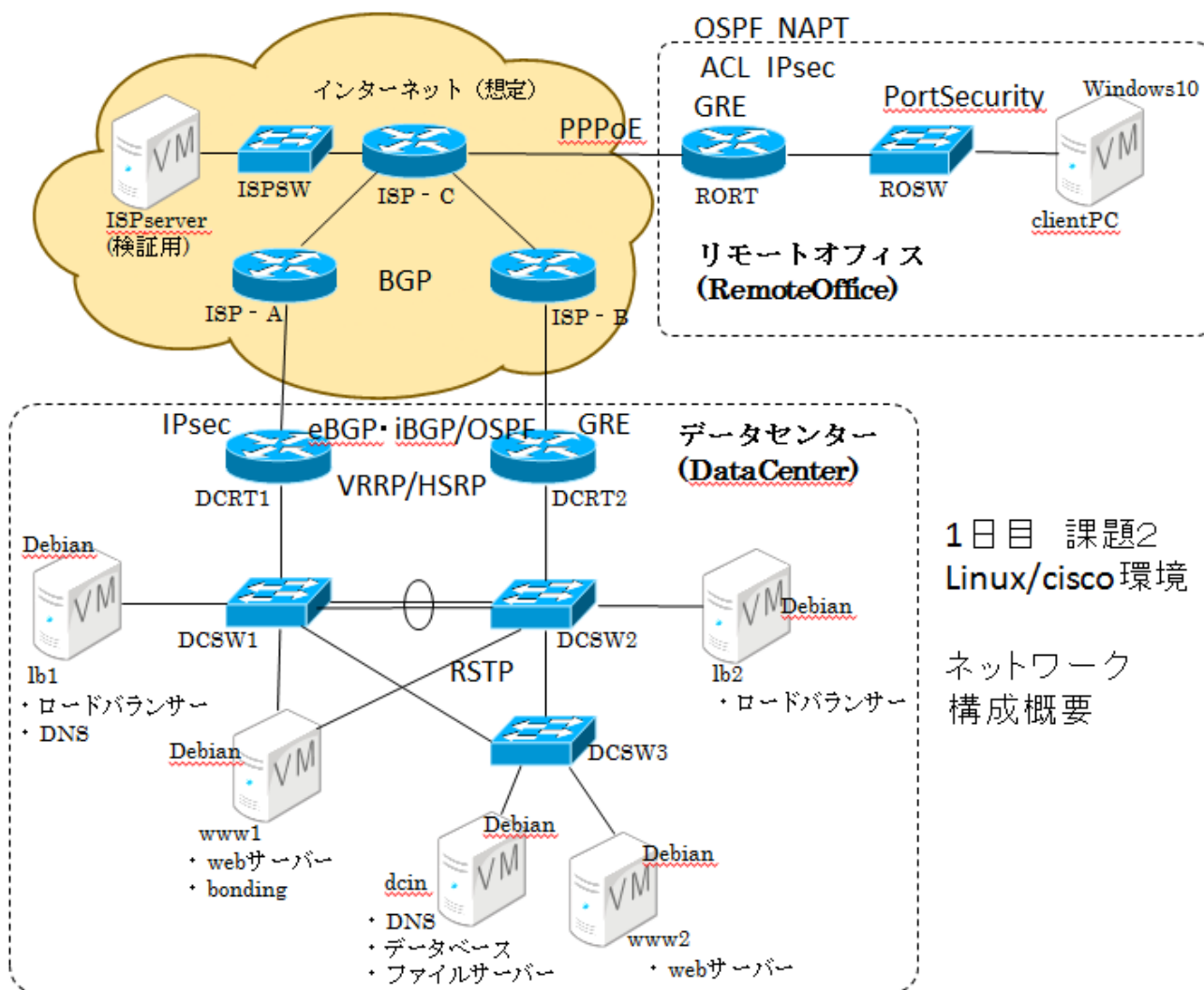
図 1 ネットワーク構成概要

課 題 1	開発部の新井です。新入社員神谷さんのアカウントを作成していただきありがとうございます。彼にユーザ名(kamiya)とパスワード(P@ssw0rd)を伝え、彼に PC(kaihatuwin10)からサインインしてもらったところ、サインインできないとのことです。業務に関する教育を開始するためにサインインが必要なので早急に対応をお願いします。
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。

以下略

参考資料 H 第 5 6 回大会 課題 2 概要 (Linux/cisco 構築課題)

採点対象：ルータ 3 台、スイッチ 4 台、サーバ (Debian) 5 台、クライアント (Windows10) 1 台
国際大会（アブダビ大会）のモジュール A と C からいくつかの類題を採用した。



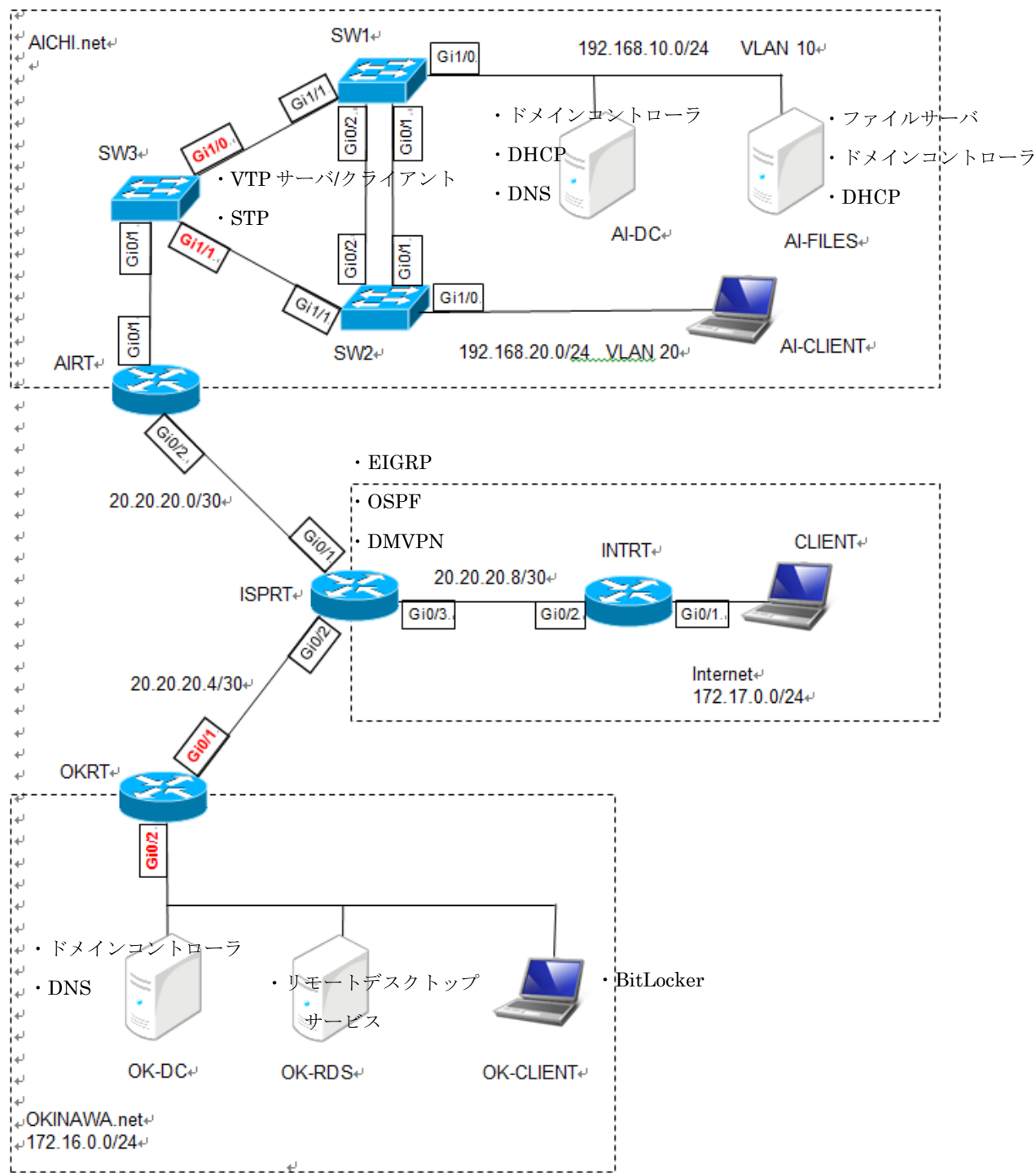
1日目 課題2
Linux/cisco環境

ネットワーク
構成概要

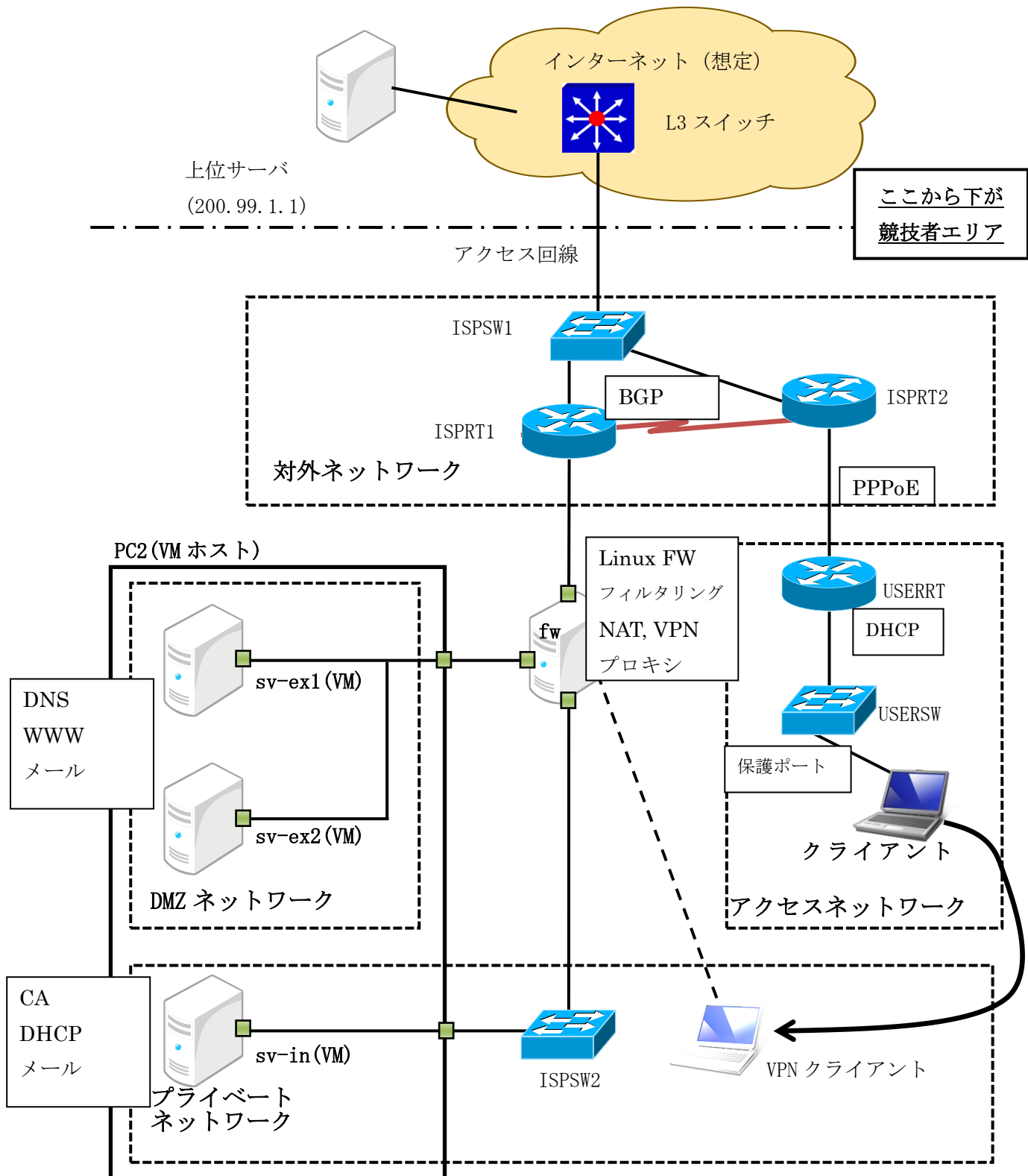
- ・ロードバランサ (HAPROXY)：国際大会（アブダビ大会）のモジュール A の類題
- ・Web-DB システム (apache, PHP, redis)：国際大会（アブダビ大会）のモジュール A の類題
- ・Web コンテンツ同期 (rsync)：国際大会（アブダビ大会）のモジュール A の類題
- ・BGP, STP, PortSecutity など：国際大会（アブダビ大会）のモジュール C の類題
- ・KeepAlived：新規の出題。設定ファイルのテンプレートを提示。

参考資料 I 第 56 回大会 課題 3 概要 (Windows/cisco 構築課題)

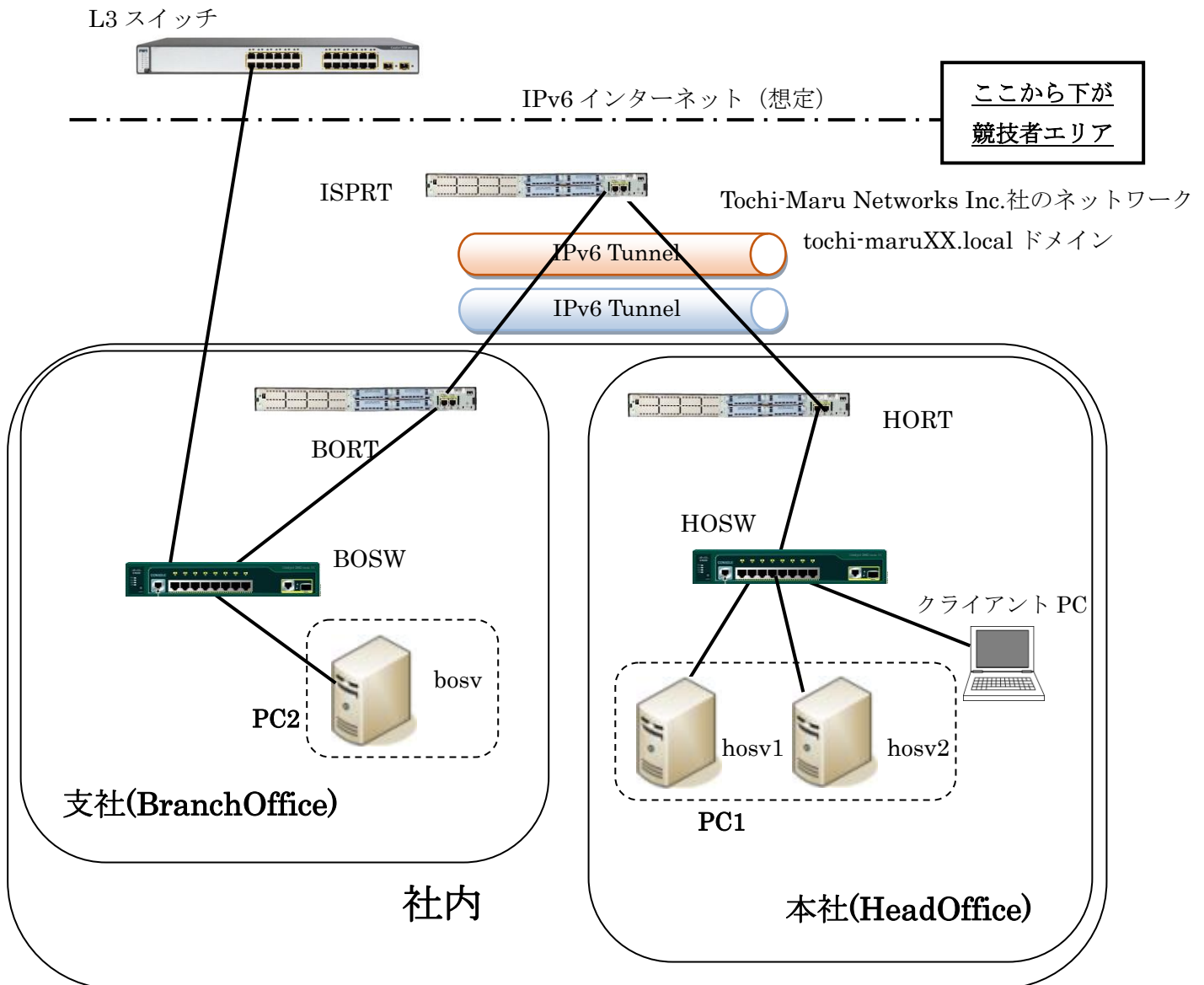
採点対象：ルータ 4 台、スイッチ 3 台、サーバ(WindowsServer) 4 台、クライアント(Windows10) 2 台
国際大会（アブダビ大会）のモジュール B と C をベースとした類題を採用した。



参考資料 J 第 55 回大会競技課題 1 日目の概要

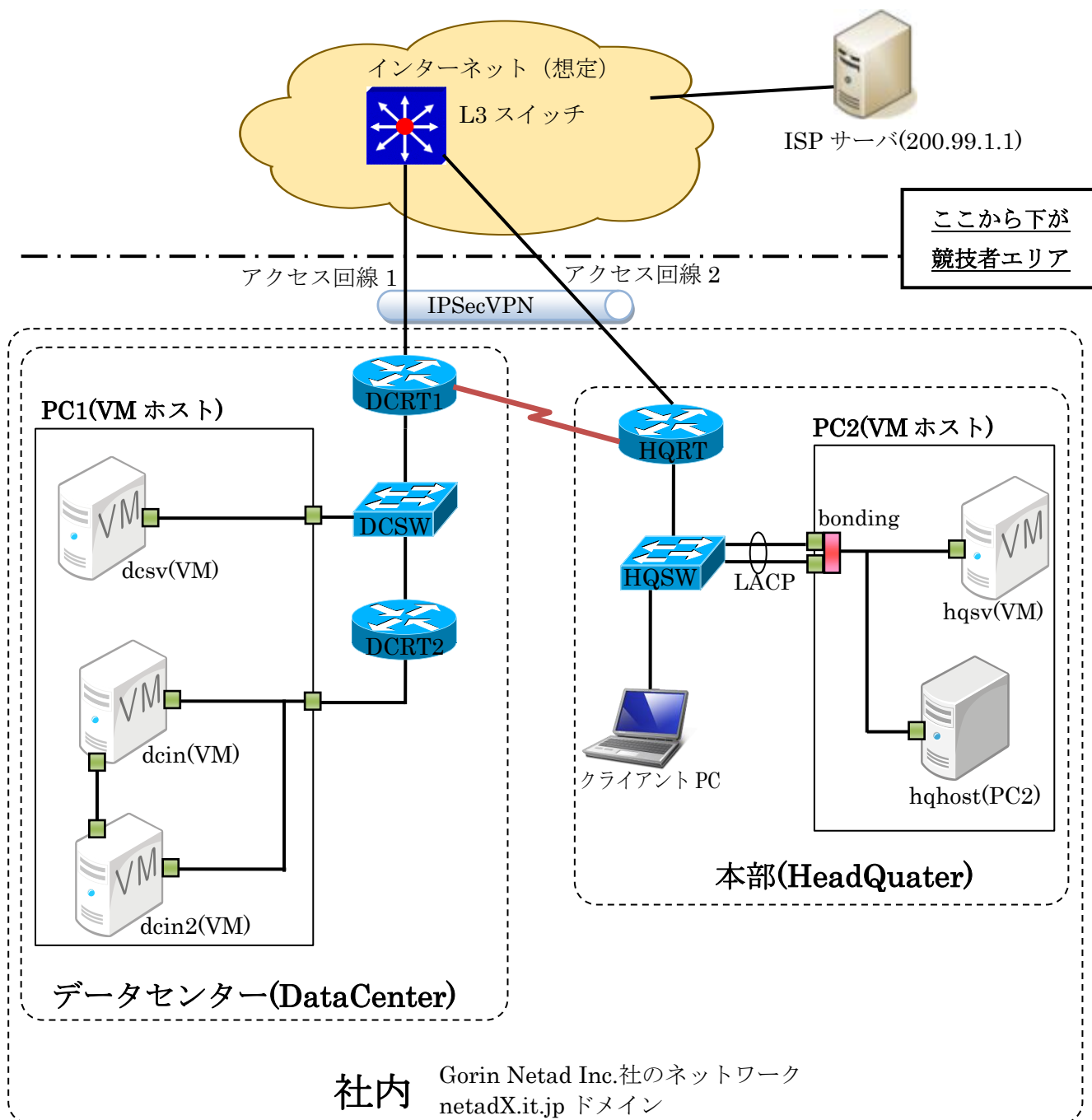


参考資料 K 第 5 5 回大会競技課題 2 日目の概要



- ネットワーク
 - IPv6 インターネット経由で本社と支社間を接続
 - 社内（本社、支社）には IPv4 と IPv6 が混在
- サーバ
 - Windows Server 2016 StandardEvaluation
 - ADDS、RDWeb、DHCP、Hyper-V
- ネットワーク機器のトラブルシューティング
config バックアップ、パスワードリカバリ、CF リカバリ、文字化けリカバリ、IP アドレス調査

参考資料 L 第 5 4 回大会競技課題 1 日目の概要



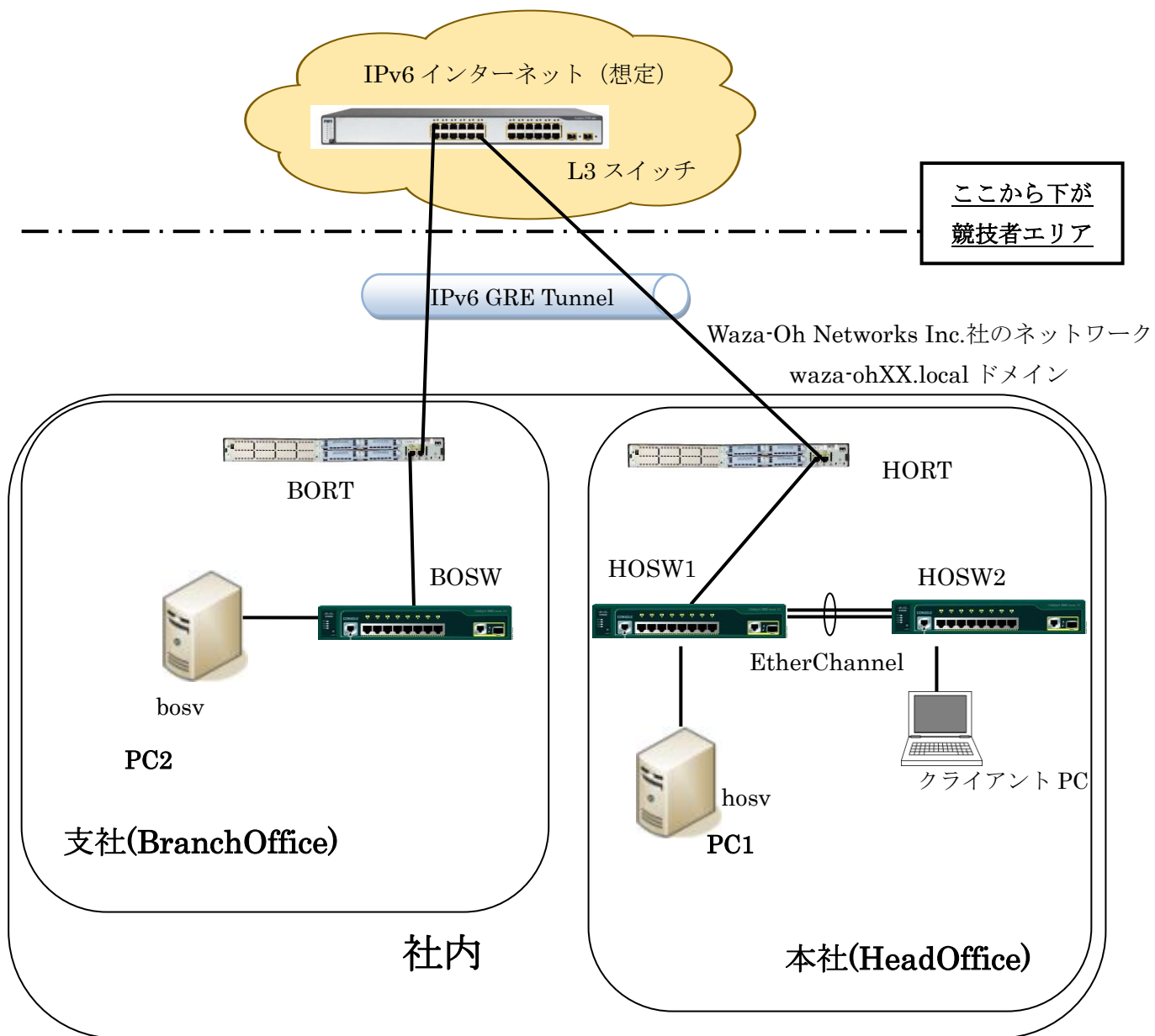
●ネットワーク

- ・インターネットへのアクセスと本部間の社内 LAN の接続は、冗長化構成

●サーバ

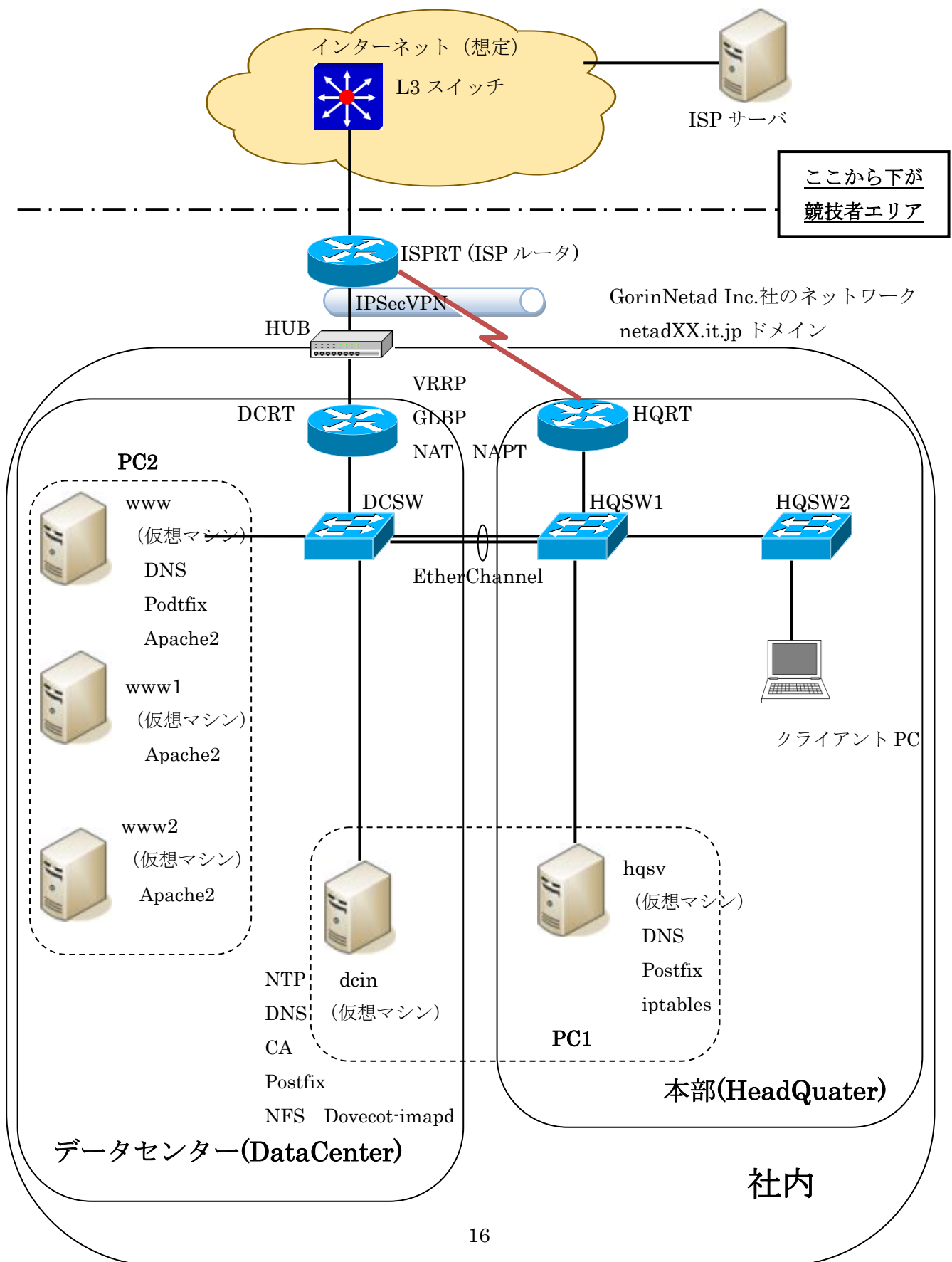
- ・dcsv … 外部公開用マスターサーバ (DNS、SMTP、WWW)
- ・dcin … 社内サーバ (IMAPS、WWW、CA、NFS、SAMBA、MySQL、NTP)
- ・dcin2 … バックアップサーバ(DRBD による dcin のディスクミラー)
- ・hqsv … 外部公開用スレーブサーバ (DNS、SMTP、WWW)
- ・hqhost … 仮想化ホストサーバ (KVM による仮想化ホスト、bonding、VLAN)

参考資料 M 第 5 4 回大会競技課題 2 日目の概要



- ネットワーク
 - IPv6 インターネット経由で本社と支社間を接続
 - 社内（本社、支社）には IPv4 と IPv6 が混在
 - サーバ
 - Windows Server 2012R2
 - ADDS、RODC
 - Radius による VLAN の動的認証、DHCP
 - トラブルシューティング
- パスワードリカバリ、IOSのコピー、IPアドレスの調査

参考資料 N 第53回大会競技課題1日目の概要



参考資料 0 第 5 3 回大会競技課題 2 日目の概要

- ホスト OS は、プリインストールされた状態から競技を開始する
- 使用するサーバ OS は、すべて Windows Server 2012 を使用する
- SV5 は、ライブマイグレーションが可能となるように構築する

※ライブマイグレーションとは

動作中の仮想マシンを停止させることなく、別のサーバに移動して処理を継続させる機能

