平成 27 年度厚生労働省委託事業

技能競技大会を活用した人材育成の取組マニュアル

ITネットワークシステム管理職種編

中央職業能力開発協会

はじめに

技能五輪全国大会をはじめとする技能競技大会は、国内の青年技能者の技能レベルを競うことにより、青年技能者に努力目標を与えるとともに、技能に身近に触れる機会を提供するなど、広く国民一般に対して、技能の重要性、必要性をアピールし、技能尊重気運の醸成を図ることを目的として実施されており、近年参加選手数が増加傾向にあるなど、活性化を見せています。

この理由として、技能競技大会が単に技能レベルを競い合う大会であるだけでなく、大会参加に向けた訓練を通じて技能レベルはもとより、段取り構成力、応用力、判断力、忍耐力など、技能者として必要な人格形成にも大きな影響を及ぼし、将来、ものづくり立国日本を支え、日本のマザー工場機能を維持するのに必要な中核技能者の育成に大きな役割を果たしていることが挙げられます。

しかしながら、技能競技大会に出場するには各都道府県で開催される地方予選を勝ち抜き、決められた大会会場に集まる必要があるため、会場から遠方の企業や、訓練方法のノウハウを持たない企業にとってはハードルが高いことは否めません。

このため厚生労働省では、「ものづくりマイスター」が企業、職業訓練施設、工業高校等の若年者に対して、技能競技大会の競技課題等を活用した実技指導等を行うことにより、若年技能者を育成する新しい事業を創設しました。

「技能競技大会を活用した人材育成の取組マニュアル」は、「ものづくりマイスター」はもとより、企業、職業訓練施設、工業高校等の関係者が、技能競技大会の競技課題等を活用した人材育成等を理解し、訓練計画の策定、実技指導等を行う際に使用されることを想定して作られており、製造、建設業関係の職種について、職種共通編及び職種別編の２種類から構成されています。

職種共通編では、①技能競技大会の競技課題等を活用した訓練の特徴及び人材育成の効果、②技能競技大会の競技課題等を活用した訓練の取組方法の概要、③技能競技大会及び技能検定の実技課題の入手方法などが説明されています。

職種別編では、①競技課題、②競技課題が求める技能の内容、③採点基準、④技能習得のための訓練方法、⑤課題の実施方法（作業手順）、⑥期待される取組の成果などを説明しています。

これらのマニュアルのほかに、技能競技大会の競技課題等を活用した訓練による人材育成の具体的な取組について、企業、教育訓練機関での事例を紹介した「好事例集」も作成されています。そちらも参考としてください。

最後に、ご多忙の中、本マニュアル作成にご協力いただいた次の方々に心から感謝申し上げます。

大野　成義（職業能力開発総合大学校）
秋葉　将和（職業能力開発総合大学校）
遠藤　雅樹（職業能力開発総合大学校）
柴田　英介（関東職業能力開発促進センター）
菊池　真　（関西職業能力開発促進センター）
幸田　啓　（千葉職業能力開発短期大学校）
日置　慎治（帝塚山大学）

（敬称略、順不同）

【実演協力】
トヨタ自動車株式会社

目　　次

1　このマニュアルの使い方

この職種別マニュアルには、技能五輪全国大会の競技課題や採点基準（公開が可能な部分）の他、競技課題の具体的な実施方法（作業手順）や競技課題を通して培った技能を現業でどのように役立てるかのヒントとなる事例等を記載している。

特に、「課題の実施方法（作業手順）」については、課題作製の作業手順を写真や解説で紹介し、現場でスムーズな実技指導が行えるよう配慮している。しかしながら、そもそも技能五輪全国大会の競技課題は、技能検定１級レベルの技能を必要とするだけでなく、多くの技能要素を含んでいること、限られた時間内で完成させなければならないこと等から、受講者によっては、短時間・短期間の訓練で課題全てを完成させることは難しいと考える。

本マニュアルの利用にあたっては、訓練時間・訓練期間等を考慮の上、受講者の技能レベルに合わせて必要な箇所（特定の作業や一部部品の作業手順等）を利用されることをお勧めする。

本マニュアルを参照し、若年者に技能を身につけさせる指針として活用願いたい。

次ページ以降の各項目の記載内容の概要は以下のとおり。

項　目	概　要
2　ITネットワークシステム管理職種に求められる技能	競技に限らず、ITネットワークシステム管理職種に携わる技能者が実務上必要となる技能について、一般論を記載。
3　競技課題の概要	本マニュアルで取り上げる競技課題の概要。競技では、何を材料に、何（課題条件）を手がかりにして、何（製作物）を作るのかについて掲載。
4　競技課題が求める技能の内容	作業手順を勘案しつつ、競技課題が求めている具体的な技能の内容（要素）について列挙するとともに、それぞれについて求められる技能レベルについて掲載。また、競技課題を制限時間内に仕上げるポイント、参加者・指導者のコメント等を紹介。
5　採点基準	どこを採点対象とするのか等、採点基準や評価方法について、今後の大会運営に支障を来さない範囲で掲載。合わせて実際の大会結果についても掲載する。
6　技能習得のための訓練方法	先に記述した技能要素を習得するための訓練方法の一例について掲載。
7　課題の実施方法（作業手順）	技能五輪で優秀な成績を収めた企業等の事例。 技能のポイント、具体的な課題作製の手順、取組・作業のポイント等を紹介。
8　期待される取組の成果	技能五輪で優秀な成績を収めた企業等の事例。 競技課題を用いた訓練等を行う目的や期待する成果等について紹介。

2 IT ネットワークシステム管理職種に求められる技能

企業や一般家庭に設置されているほとんどのコンピュータは、インターネットを通して世界中とつながっている。システムにトラブルがあれば、インターネットを経由して世界中に広がる。企業では社員間の連絡や情報共有などの業務や別の企業や顧客など企業の外との情報交換にもコンピュータ・ネットワークを使用して、インターネットに接続している。だからこそ、コンピュータやネットワークによるシステムには高い信頼性やセキュリティが求められる。

ITネットワークシステム管理者はこのシステムを豊富な知識と経験、判断力と想像力を駆使して、そのネットワークの構築から運用、管理、保守までこなす。常にシステムが正常に稼働するように、トラブルを未然に防ぎ、発生した時は的確に対処する。新しい知識と経験をもった技術者が、現代のネットワーク社会を支えている。

スムーズな運用を管理するITの中心的役割を持つITネットワークシステム管理職種に求められる技能は大きく４つに大別される。

(1) ネットワークの設計と構築

ハードウェア、ソフトウェアの選定、ネットワーク構築、各機器の設定や、ソフトウェアのインストールを行う。

ネットワークシステムの要求分析、信頼性設計、性能設計、セキュリティ設計、アドレス設計、運用設計、インプリメンテーション、評価（性能、信頼性、品質、経済性ほか）などを行う。

(2) ネットワーク・アプリケーション技術

ネットワークシステムの構成技術、トラフィックに関する技術、セキュリティ技術などの設定や構築を行う。電子メール、ファイル転送、Webのアクセス技術、アプリケーション間通信などである。

(3) サーバの設計と構築

DNS、Webサーバ、メールサーバ、プロキシ、クライアントPCなどの設定や構築を行う。

(4) ネットワークシステムの運用・保守

ネットワークシステムの運用・保守、セキュリティ管理などを行う。

3 競技課題の概要

本職種の技術者には、高い信頼性のあるシステムを構築するための技術と知識が必要となる。またシステムにトラブルが発生した際は、その現象と状況を的確に判断して対処しなければならない。技術者はこれまでの経験と知識だけではなく、判断力と想像力も求められる。そこで「ITネットワークシステム管理」競技では、「サーバシステムの構築技術」および「インターネットへの接続も含めた社内ネットワーク構築技術」を競う。

(1) 競技に使用できる主な機器と支給部品等

①（サーバ用）デスクトップPC（CPU Core2以上、メモリ2GB以上、HDD 80GB以上を1個以上、NIC 1ポート以上、DVDドライブ付き） 2式
サーバ用デスクトップPC 2台は切替機でディスプレイ・キーボード共有
②（クライアント用）ノートPC（Windows 7、シリアルポート付き、無線LAN付き、Tera Termインストール済み） 1式
③ Hub（4ポート以上） 1台
④ Cisco製ルータ2811（Ver.12.4.10C以降） 3台
⑤ Cisco製スイッチングHub Catalyst 2960G-8TC-L（Version 12.2（35）SE） 3台
⑥ Cisco製無線LANアクセスポイントAir-AP1242AG-P-K9 1台
⑦ LANケーブル（UTP CAT5E、既製品） 数本
⑧シリアルケーブル（DCE、DTE） 各2本

Cisco 2811 ルータのIOS Feature SetはIP Base を基本とするが、Advanced IP Services も使用する。競技委員側で構築する上位サーバとの接続用に L3スイッチ（WS-C3750-24TS-E）を用意し利用するが、選手は設定等、直接操作は行えない。

(2) 課題条件

競技課題として、以下の作業を行う。競技はこれらの課題を2日間、計9時間で行われ、システムの信頼性、システム運用管理技術、セキュリティ技術などがポイントとなる。

[1] ハードウェアパフォーマンスの最適化のための BIOS 設定等

※日本語環境が設定可能なOSおよびアプリケーションは、日本語環境を使用する。

[2] Windows によるサーバと Linux によるサーバの構築およびクライアント PC の設定

① サーバOSおよび必要ソフトのインストール
② 各種サーバ（DNS、Web、メール、ファイル共有等）の設定
（セキュリティ対策や運用管理も含む）
③ 各種アプリケーション
（仮想環境構築ソフトウェア、RDB、Web-RDBインターフェーススクリプト）の設定
④ ネットワーク接続作業
⑤ クライアント設定

※サーバ OSは、Windows Server 2012 R2 評価版とDebian GNU/Linux 7.5.0 wheezy とする。なお、これらのOSは第52回技能五輪全国大会の競技課題概要を公開した時点での最新版またはそれに準ずるバージョンであった。

[3] ネットワーク構築

① ルーティング設定
② フィルタリングの設定
③ ネットワーク接続作業とトラブルの修復
④ VLANの設定
⑤ ネットワーク機器の各種設定、運用管理
※ルータの機能としてWeb環境での設定が可能な機種であっても、競技中にこのWeb環境でルータの各種設定をすることを禁止する。なお、無線LANのアクセスポイントについてはWeb環境での設定を禁止しない。

[4] 競技上の注意事項

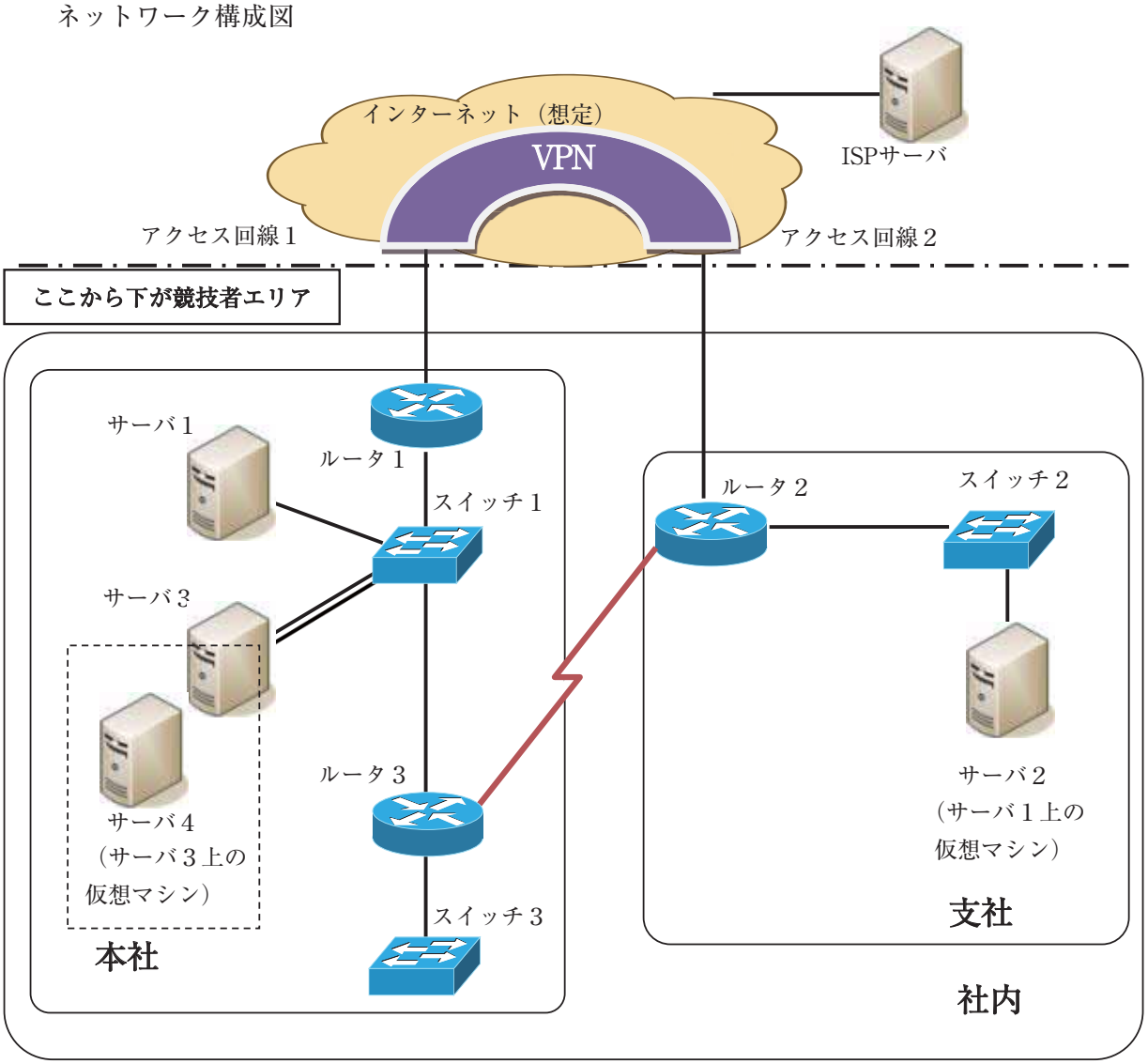
① 各種マニュアル、参考書、ノート等の持ち込みは一切認めない。
② ソフトウェアの持ち込みは一切認めない。
③ 質問などがある場合には、質問票に記入して競技委員に申し出ること。質問する時間は競技開始して１時間後から１時間とする。ただし、ハードウェアに関する質問については随時可能とする。これはハードウェアトラブルが疑われる事態が発生した場合、その対処を優先するためである。
④ 競技終了の合図で、作業を直ちに終了すること。
⑤ 競技時間内に作業を終了した場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
⑥ 競技中に、トイレ、体調不良などが生じた場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。
⑦ 競技中の水分補給のための飲料水の持ち込みは認める。
⑧ 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。
⑨ 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。

(3) ネットワーク構成図

第 52 回大会競技課題 1 日目の概要

あなたはネットワークシステムの構築を専門とする企業のエンジニアである。ある企業のネットワークシステムの更改業務を受注し、そのプロジェクトリーダーとなった。ネットワークの設計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。

ネットワーク構成図

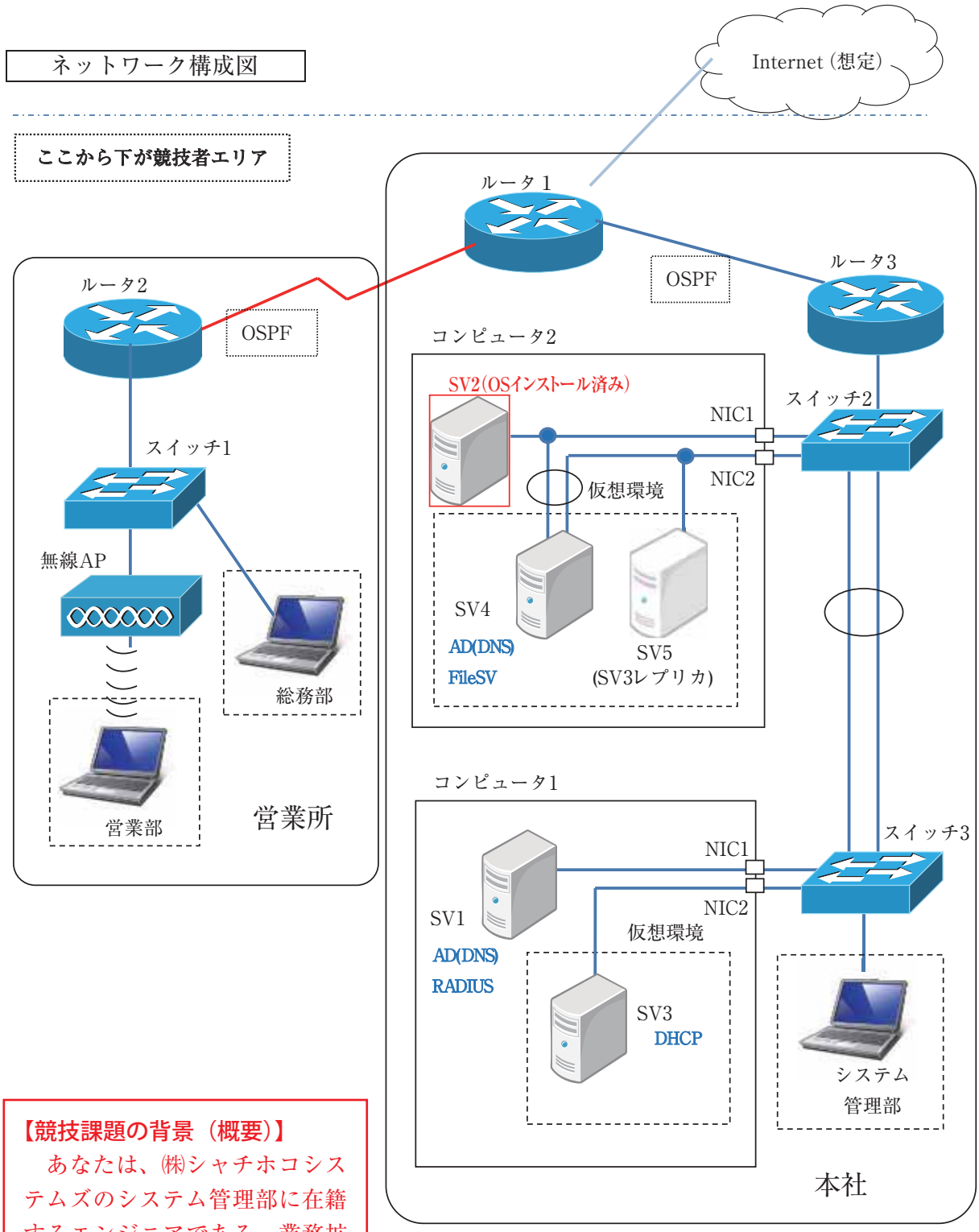


【主なサーバの機能】

サーバ１	：	Ｗｅｂ、メール、ＤＮＳ
サーバ２	：	メール、ＤＮＳ
サーバ３	：	ＤＮＳ、ＡＤＤＳ
サーバ４	：	メール

第 52 回大会競技課題 2 日目の概要

ネットワーク構成図



【競技課題の背景（概要）】

あなたは、㈱シャチホコシステムズのシステム管理部に在籍するエンジニアである。業務拡大のため、新規開設した営業所と本社間のシステムを新規に構築する。今回は、事前検証用のネットワーク及び各種サーバを構築する。

（4）大会の様子

競技選手の感想（金メダリスト 伊藤 選手）

－ 競技内容、制限時間に関して、競技会での精神状態（あせりや余裕）はどうでしたか

今大会からルータのIOSVersionが更新され、設定の幅が広がっていたため、難しい設定が多いと感じました。

また、設定量の多い競技課題構成となっており、時間配分には特に注意して作業をしました。

難易度の高い設定ではありましたが、訓練通りの作業を心掛け、自分の実力でできることだけに意識していたため、終始、落ち着いて作業していました。

4 競技課題が求める技能の内容

競技は大きく２つの課題で構成され、これらの課題を通じて、より信頼性の高いシステム構築技術を競う。300人規模を想定した企業の各種サーバシステムの構築とインターネット接続を含めた社内ネットワーク構築を行う。

（1）課題作成に必要となる技能要素とその水準

［1］サーバシステムの構築

Webやメールなどのサービスを行うサーバシステムを構築し、そのサーバで使われるOSをインストールする技能。

① ハードウェアのBIOS設定

BIOSが最新状態でないと周辺機器が認識しなかったり、不具合が含まれている可能性がある。そのため最新の状態に保つ必要がある。

② OSのインストール

Windows、Linuxの最新バージョンのインストールと設定方法の知識

③ DNS、Web、メールサーバ、プロキシ等の設定

DNSサーバ、Webサーバ、メールサーバ、プロキシ等をインストールと設定を行う。DNSは「IPアドレス」に「名前（ドメイン名やホスト名）」を関連付けて管理し、利用しやすくする。

④ アプリケーションの設定

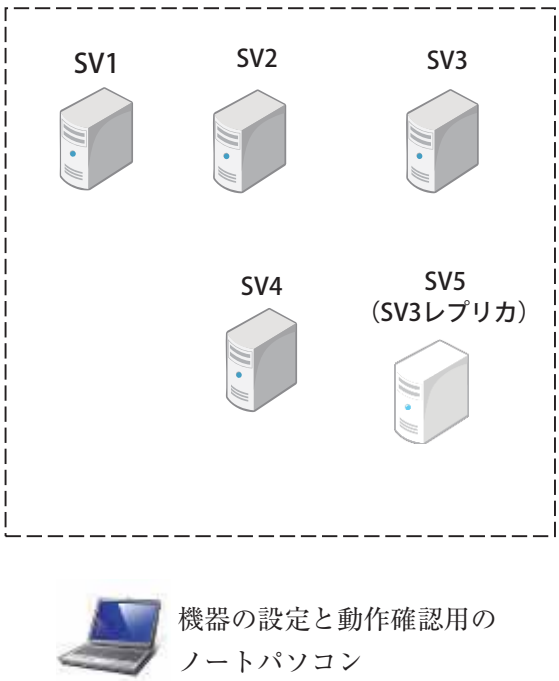
アプリケーションソフト（mysqlやWordPressなど）のインストールと設定を行う。

⑤ ネットワーク接続作業

⑥ クライアントPC設定

【課題１　サーバとクライアントPC】

【課題２　サーバとクライアントPC】



［2］ネットワーク構築

ネットワークを通じてサーバを利用するため、ルータなどを使ってネットワークを構築する技能。

① ルーティング設定

通信のために最適と思われる経路を把握し、経路の設定を行うためのルーティングテーブルを作成する。ルーティングテーブルを見てルータの設定を行う。

② フィルタリングの設定

フィルタリング機能として、ルータは不要なパケットを配送しない、または特定のパケットだけを配送するように制御したり、配送時にパケットに対して何らかのアクションを実行する。

③ ネットワーク接続作業とトラブルの修復

通信の疎通を確認、イーサネット通信確認、各設定は正しいかなどの動作確認を行う。

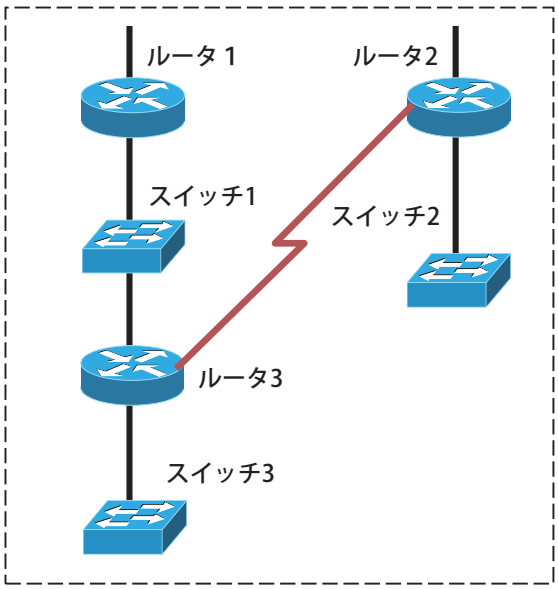
④ VLANの設定

VLANは、スイッチでネットワーク（ブロードキャストドメイン）を、ルータに頼らずに分割する技術で、論理的な配置（どのスイッチに接続しているかとネットワークは別）で構成を変更できるようにする。

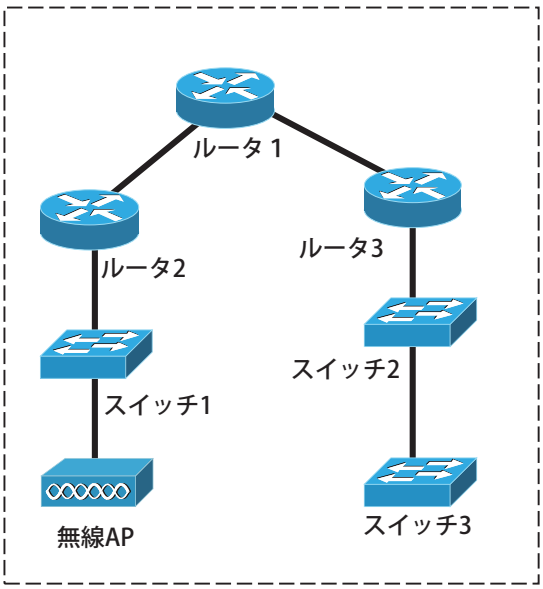
⑤ ネットワーク機器の各種設定、運用管理

スイッチングやルータなどの機器設定にターミナルソフト（Tera Termなど）を利用して設定を行い、運用管理では、ネットワークシステムのセキュリティ対策（ACLなど）、障害対策（冗長化など）を行う。

【課題１　スイッチングとルータ】



【課題２　スイッチングとルータ】



(2) 競技時間内に課題を仕上げるためには

① どの競技課題でも通用する作業手順を組むことで作業効率がよくなる。
② 要素に掛かる時間を把握して適切な時間を守る。
③ 冷静に仕様を読むことで、作業にかかった際に落ち着いて設定できる。

【選手】

－ 第52回大会の課題内容についてどのように思われましたか。

過去大会の競技課題内容に比べ、レベルが高いと思います。多くの知識を必要とし、競技課題の仕様を満たすよう設定を理解していなくてはなりません。

－ 時間内に終わらせるために、日頃の訓練ではどのような事を意識（注意）して課題製作に取り組んでいますか。（姿勢、道具の配置、動き、手順、など）

時間内に競技課題を終わらせるために、最も意識していることは、作業手順です。未公開競技課題であり、内容も様々あり、どの競技課題でも通用する作業手順を組むことは、難しいことです。考えられる範囲で、大まかな流れを決めることにより、作業効率がよくなっていきます。

また、細かい取り組みとして、道具の配置は常に同じ状態にしています。ノートＰＣの位置やディスプレイの角度、ペンの置き場所など、自分で動かせるものは、日頃の訓練の時から合わせることで、作業がしやすくなります。

－ 大会の本番、課題に取り組む際、一番意識したことは何ですか。（制限時間、精度、など）

大会本番では、訓練通りの作業をすることを一番意識していました。本番で急に訓練以上の実力は出せないと思っています。訓練の時に、一つ一つの要素に掛かる時間を把握しておき、本番では焦って、それより速く作業することなく、遅くなることもしません。適切な時間を守ることで、余計な緊張をせず、平常心を保つことができます。

【指導者】

－ 指導者のお立場からは、第52回大会の課題内容についてどのように思われましたか。

過去大会の競技課題内容に比べ、レベルの高い課題だったと思います。新しい要素等も導入されていて、とても良い課題だったと思います。

－ 時間内に終わらせるために、日頃の訓練ではどのような事を意識（注意）して指導されていますか。

特に作業手順について意識させています。各選手にどういう道筋を立てて競技課題を攻略したら良いかを考えさせることで、どのような内容でも柔軟に対応でき、しっかりとした作業手順を確立することができます。

また、日頃の訓練で同じ作業を意識させることで、常に安定した成績が出せるようにしています。

－ トラブルを起こさず課題を仕上げていくために、最もポイントとなることはどのようなことだと考えておられますか。

競技課題を読む時、冷静になることだと思います。冷静に仕様を読むことで、作業にかかった際に落ち着いて設定ができると思います。

また、"今まで訓練を乗り越えてきた”という自信と"自分はできるんだ”という前向きな気持ちをしっかりと持つ事もとても大切な事だと思います。

5 採点基準

(1) 採点項目及び配点

以下に示す方法により採点を行う。(なお、技能五輪全国大会の採点基準については、本競技で使用する機材・環境及び競技時間・内容を考慮した場合、過去に行われた国内大会での競技課題のすべてを公開することは、今後の競技の運営上好ましくないと考えられ、具体的な配点や、採点基準は公開されていない。)

公表されている採点内容

採点は、与えられた「競技課題」を理解し、要求されたシステムが正確に実現されているかを評価する。

配点は

A. ハードウェアパフォーマンスの最適化のためのBIOS設定等が10%未満

B. WindowsによるサーバとLinuxによるサーバの構築およびクライアントPCの設定が65%未満

C. ネットワーク構築が50%未満。

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する。

（2）採点方法

具体的な配点、採点方法、採点箇所、採点基準（どれだけの誤差に対し何点の減点、またそれぞれの項目の重み付けなど）については公開されていない。そのため、本マニュアルのために採点基準を作成した。

課題1のサーバシステム構成

採点対象		動作チェック項目
SV01	ネットワーク設定	sv01のeth0のIPアドレスが10.1.200.1である。
		sv01のeth0のサブネットマスクが255.255.255.0である。
		sv01のeth0のデフォルトゲートウェイが10.1.200.254である。
		sv01のeth0のネームサーバが自身である。
	サーバOS共通設定	sv01のシステム時刻が競技会場と±5分以内である。
		ホスト名とドメイン名が正しい。
	パーティション構成	指定通り作成されている。
	DNS	自身で名前解決ができない場合は、ISPサーバに問い合わせる。
		bindのバージョンを回答しない。
		「社内」および「外部ネットワーク」からの問い合わせに応える。
		再帰問い合わせは自身（localhost）とサーバ３からのみ許可する。
		「外部ネットワーク」向けのマスターサーバとして動作している。正引きを設定と別名設定がある。
		「社内」向け正引きおよび逆引きしている。
		サーバ３で管理しているゾーンのスレーブとして動作させる。
	メールサービス	本社ドメインnetadXX.it.jpのプライマリメールサーバ、支社サブドメインaichi.netadXX.it.jpのセカンダリメールサーバとなる。
		本社ドメインnetadXX.it.jp宛てのメールはサーバ４へ転送する。
		支社サブドメインaichi.netadXX.it.jp宛てのメールはサーバ２へ転送する。
		その他の宛先のメールはISPサーバへ転送する。この際、SMTP認証を行い、認証が成功した時のみ中継を許可する。認証用ユーザとしてmailuserを作成する。パスワードはユーザ名と同一とする。ただし、サーバ４からは認証なしで中継を許可する。
	プロキシサービス	
	Webサービス	
	データベースサービス	
	WordPress	

採点対象		動作チェック項目
SV02	OSインストール	ゲストOSがDebian GNU/Linux 7.5.0である。
		仮想マシン「sv02」はsv01の起動時に自動起動する。
	ネットワーク設定	sv02のeth1のIPアドレスが172.16.100.1である。
		sv02のeth1のサブネットマスクが255.255.255.0である。
		sv02のeth1のデフォルトゲートウェイが172.16.100.254である。
		sv02のeth1のネームサーバが自身である。
	サーバOS共通設定	ホスト名とドメイン名が正しい。
	DNS	自身で名前解決ができない場合は、ISPサーバに問い合わせる。
		bindのバージョンを回答しない。
		「社内」および「外部ネットワーク」からの問い合わせに応える。
		再帰問い合わせは自身（localhost）と支社内からのみ許可する。
		サーバ１とサーバ３で管理しているゾーンのスレーブとして動作させる。
	メールサービス	支社サブドメインaichi.netadXX.it.jpのメール送信サーバとして動作させる。
		支社サブドメインaichi.netadXX.it.jpのプライマリメールサーバ、本社ドメインnetadXX.it.jpのセカンダリメールサーバとなる。

採点対象		動作チェック項目
SV03	OSインストール	ホストOSがWindows Server2012R2である。
		ドメイン名がnetadXX.localである。
	ネットワーク設定	sv03のIPアドレスが10.1.100.1である。
		sv03のサブネットマスクが255.255.255.0である。
		sv03のデフォルトゲートウェイが10.1.100.254である。
		sv03のネームサーバが自身である。
	サーバOS共通設定	sv03のシステム時刻が競技会場と±5分以内である。
	DNS	MSDNSサービスが起動している。
		自身で名前解決ができない場合は、サーバ１に問い合わせる。
		「社内」からの問い合わせに応える。
		localの正引きおよび逆引きのマスターサーバとして動作している。正引きを設定と別名設定がある。
	Active Directory	

採点対象		動作チェック項目
SV04	OSインストール	ゲストOSがDebian GNU/Linux 7.5.0である。
		ドメイン名がnetadXX.localである。
		仮想マシン「sv04」はsv03の起動時に自動起動する。
	ネットワーク設定	sv04のIPアドレスが10.1.100.2である。
		sv04のサブネットマスクが255.255.255.0である。
		sv04のデフォルトゲートウェイが10.1.100.254である。
		sv04のネームサーバが10.1.100.1である。
	認証統合	
	メールサービス	本社ドメインnetadXX.it.jpのメール送信および受信サーバとして動作させる。
		本社ドメインnetadXX.it.jp宛てのメールをスプールする。保存形式は任意とする。
	プロキシサービス	

・採点は、加点方式を採用。
・課題１の内容と配点は次のとおり。

項　目	内　容	配点
ハードウェアパフォーマンスの最適化	BIOS設定	
	小　計	10%未満
サーバシステム構築（Windows、Linux）	サーバOS（Debian、Windows）のインストールと基本設定	
	パーティション構成	
	DNSの設定	
	Active Directoryの設定	
	Webサーバの設定	
	メールサーバの設定	
	ネットワークの設定	
	各サービスとアプリケーションの設定	
	・メールサービス	
	・プロキシサービス	
	・Webサービス	
	・データベースサービス	
	・WordPress	
	認証統合	
	小　計	65%未満
ネットワーク構築（Windows、Linux）	ルータ	
	・IPアドレス設定	
	・ルーティング設定、デフォルトルーティング	
	・VPN設定	
	・サブインターフェース設定	
	・ゲートウェイの冗長化	
	・ACL、NAT、NAPT設定	
	・シリアル接続	
	・障害対策（冗長化）	
	スイッチング	
	・VLANの設定	
	・ネットワーク各種設定	
	・IPアドレス設定	
	小　計	50%未満
動作確認	ネットワークコマンドを使って、接続状況と動作確認	
	小　計	
	合　計	100点 満点に換算

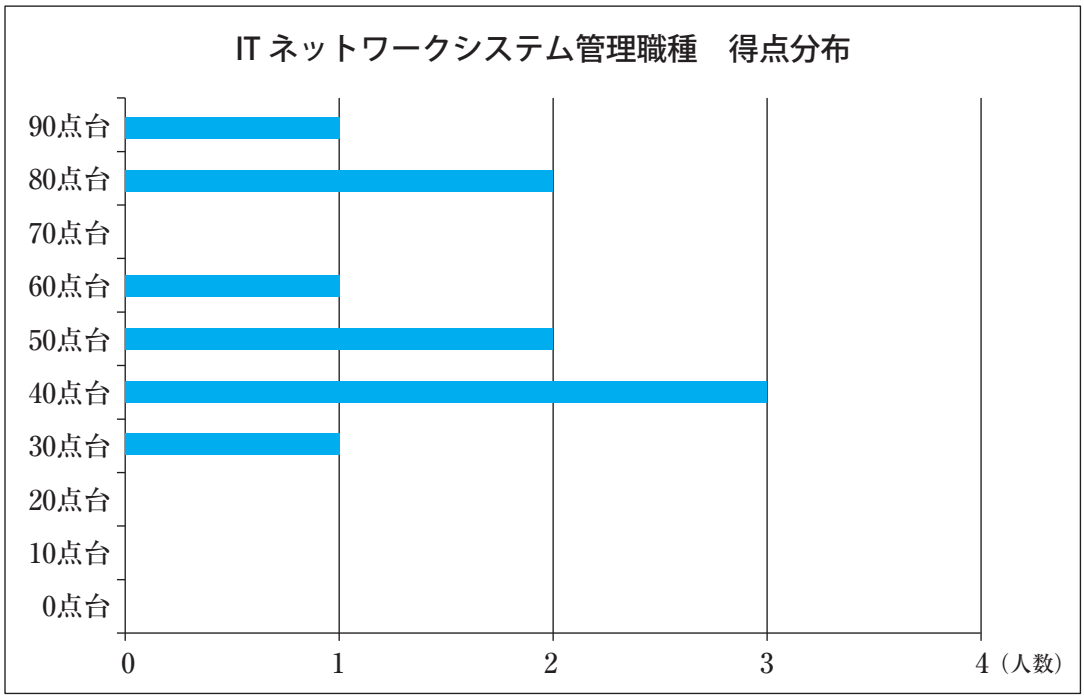
(3) 大会の成績結果

第52回技能五輪全国大会における競技結果の成績と得点分布を参考までに示す。

(成績)

大会での成績	人数（名）
金　賞	1
銀　賞	1
銅　賞	1
敢闘賞	1

(得点分布)



6 技能習得のための訓練方法

サーバの立上げ、セキュリティ対策は万全か、全ての機器が仕様書の要求どおり機能するか、判断力と想像力が必要である。

(1) 技能要素を習得するための訓練方法

[1] ネットワーク設計と構築

迅速なネットワーク構成の理解とネットワーク設計。

ネットワーク構成の理解を深めるために、ネットワーク設計に関する本を読んだり、ネットワークを実際に構築しながら習得する。

[2] サーバ設計と構築

効率の良いサーバインストール作業とクライアント・サーバの各項目設定作業。

各OSバージョンソフトの理解と操作の習得。

サーバ構築では、課題に頻出されると思われるサービスを優先して訓練する。基本的なサービスは反復練習して確実に設定できるようにする。

[3] 機器の接続と設定

各ネットワーク機器の理解と操作の習得。

ルータ、スイッチングのセッティング。

ネットワークの構築は、最初に身に付けておくべき技能。

ネットワークを構築するためには、ネットワーク機器の特徴を知ること、通信の確立に必要な知識を習得する必要がある。参考書を読むことも大事だが、得た知識を実際に機器で設定する。知識と設定をセットで覚えると理解がしやすい。

(2) カリキュラム例

一定水準にある技能者(技能検定２級相当)が本課題の実施に向けて取り組む訓練カリキュラムの例を示す。

教科の細目	内　容	時間(H)
1．ネットワーク概要	ネットワーク基礎、TCP/IPプロトコル、LAN、WANなど	16
2．ハードウェアパフォーマンスの最適化のためのBIOS設定	BIOS設定	4
3．Windows、Linuxのサーバの構築およびクライアントPCの設定	OSインストール、アプリケーションソフトインストール、DNS、Webの設定、クライアントPCの設定など	24
4．Windows、Linuxのネットワーク構築	ルーティング設定、フィルタリング設定、ネットワーク接続、ネットワーク機器の設定、VLANの設定など	16
5．ネットワーク運用、管理、保守	ネットワーク運用とトラブルの修復	8
6．競技課題への取組	(1) 課題が求めている技能要素	24
	(2) 各工程の考え方と作業手順	
7．課題実施演習による検証と対策		24
8．まとめ	全体的な講評および確認・評価	8
	訓練時間計	124

(3) 訓練・指導方法の例

【訓練方法】

－技能を習得するのにどのくらいのスパン（２年、３年）でどのような訓練をされていますか。

訓練スケジュールは指導員が決め、大会を想定して訓練を行います。基礎訓練は１年から１年半、要素の技術を習得していきます。応用訓練は２年～３年で行いますが、１年目の選手と２年目の選手では訓練の差が出てきます。

－訓練では、どういった点に重点を置いた訓練をされていますか。（精度、時間など）

確実にミスなく設定することに重点をおいて訓練をします。初めのうちは、時間は特に意識しません。その後、先輩の技術ノウハウなどを聞き、時間の短縮、効率を考えていきます。

ＩＴネットワークシステム管理の詳細は当日発表され、競技時間内で課題を読み、段取りを組みます。インストールをしている間の待ち時間をなくすように心がけます。

－どのような素質を持った者が訓練によく取り組んでいますか。また、大会で好成績をあげる選手に共通した資質なり特徴がありましたらお教え下さい。

ＩＴ技術に面白さを感じ、コツコツ努力できる選手が好成績をあげているように思います。また、指導員の言うことを素直に聞き入れることができるか、も大切な素質の一つです。

－課題途中で失敗やトラブルが発生するかと思いますが、その際の対応能力（リカバリー能力）は、どのように訓練されていますか。

特にそういった訓練はしていないのですが、焦らず落ち着いて作業するよう言っています。

－大会の課題公表前と後での訓練内容をどのように変えますか。

提案課題[注]公表後はその内容をしっかりと理解させることに重点を置きます。

わからない点があれば、指導員が選手に理解するまで教えます。

－御社独自と思われる訓練をされていますか。（競技会、合宿、など）

他の企業との交流はありませんが、課題を用意して学園内で競技会を行い、選手同士で競わせます。

－訓練を続けてこられて、最近の選手の特徴や傾向はありますか。また、それに対応するため訓練メニューをどのように変えてきていますか。

最近の選手は、なぜそれをしないといけないのか理由を教える必要があると感じます。そして選手が納得した上で作業させるよう心がけています。それに対する訓練メニューの変更は特にありません。

－課題作成の段取りは、選手（又は指導者）が自身で考えて行っているのですか。（やらせてみて、エキスパートがアドバイスするなどを繰り返すのですか。）

基本的には担当指導員が段取りを行います。計画は指導員が相談しあって立てます。

－公表課題（P77の競技課題概要のこと）に合わせた採点基準等を独自に作成し訓練を行われていると思いますが、採点基準を作成する上で重点を置かれている点は何ですか。（制限時間、精度、見栄えなど）

難易度によって得点が大きく変動し、それにより選手が「過剰に自信を持つ」「自信を失う」事が無いよう得点配分を調整しています。

出題課題は範囲が広く、深い知識が必要なので対応が難しく、国際大会の課題に近づけています。

注：提案課題とは参加者が競技課題の提案を行い、参加者の間で情報を共有するための課題。この提案課題がそのまま競技で使用する出題課題となる訳ではないが、練習する上での目安になっている。

【指導方法】

ー安全はもちろんですがそれ以外で、「訓練指針」のようなものがあればお教え下さい。

「元気な挨拶」と「感謝の気持ちを持つこと」です。

ーどのような点にこころがけて選手に接しておられますか。（常に厳しく、良き相談相手、など）

選手へはやる気を失わないよう接することを心がけています。

以前できなかったことができたときは褒めてあげて、できることをしっかりしなかったときは叱る、を意識しています。

ー長期間、選手のモチベーションを維持させていくことは難しいことだと思いますが、維持にあたりどのような対応をとられていますか。（選手個別の訓練計画の立て直し、競技会の実施、など）

選手のモチベーションが下がったときは指導員が面談をして勇気づけたり、選手の中には話すだけで気が楽になりモチベーションが上がる選手もいます。また、選手の話を聞いてあげるだけでも効果があります。

訓練計画は選手の体調を最優先に、訓練効率を考えて臨機応変に対応しています。

ー訓練期間中、どんなことに選手は最も影響を受けていましたか。（先輩・指導者の励ましの声、自身で克服、など）

先輩指導員の過去の経験談に影響を受けていたように思います。

トヨタ工業学園
エキスパート　古小高 貴則さん

第 52 回技能五輪全国大会
金賞　伊藤 直輝さん

7 課題の実施方法（作業手順）

（1）準備

技能五輪全国大会のITネットワークシステム管理は、３か月前に競技課題の概要が公表されるだけで、課題内容の詳細は当日になるまで非公表である。原則として３か月前に課題公表される他の職種と違い準備期間がなく、その場で課題の内容を把握して作業しなければならない。

[1] 競技前日（競技内容の説明、競技場所の抽選、機材の確認）

競技内容の説明

競技場所の抽選

選手の席順を決める。

機材の確認

パソコン、ルータ、スイッチングなどの動作確認を行う。

POINT

準備されている機器が正常に動作するかを確認する。PC であれば、キーボード、マウスの動作、ディスクトレイが開くかなど。

[2] 競技課題に関する注意事項

① 競技終了時に指定された配線接続になっていること。

② 競技終了時に指定された設定がネットワーク装置のNVRAMに保存されていること。全てのハードウェアは採点前に再起動される。

③ 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。

④ ネットワーク構成図における「インターネット（想定）は、「L3スイッチ」および「ISPサーバ」で構成される。これは競技委員が用意する「仮想的なインターネットエリア」であり、「社内」以外の全てのネットワークエリアを指すものとする。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。

⑤ 競技課題中の「社内」とは、ネットワーク構成図における「本社」および「支社」内の全てのプライベートアドレスセグメントを指すものとする。また、「本社内」とは、ネットワーク構成図における「本社」内の全てのプライベートアドレスセグメントを指すものとする。

「支社内」とは、ネットワーク構成図における「支社」内の全てのプライベートアドレスセグメントを指すものとする。

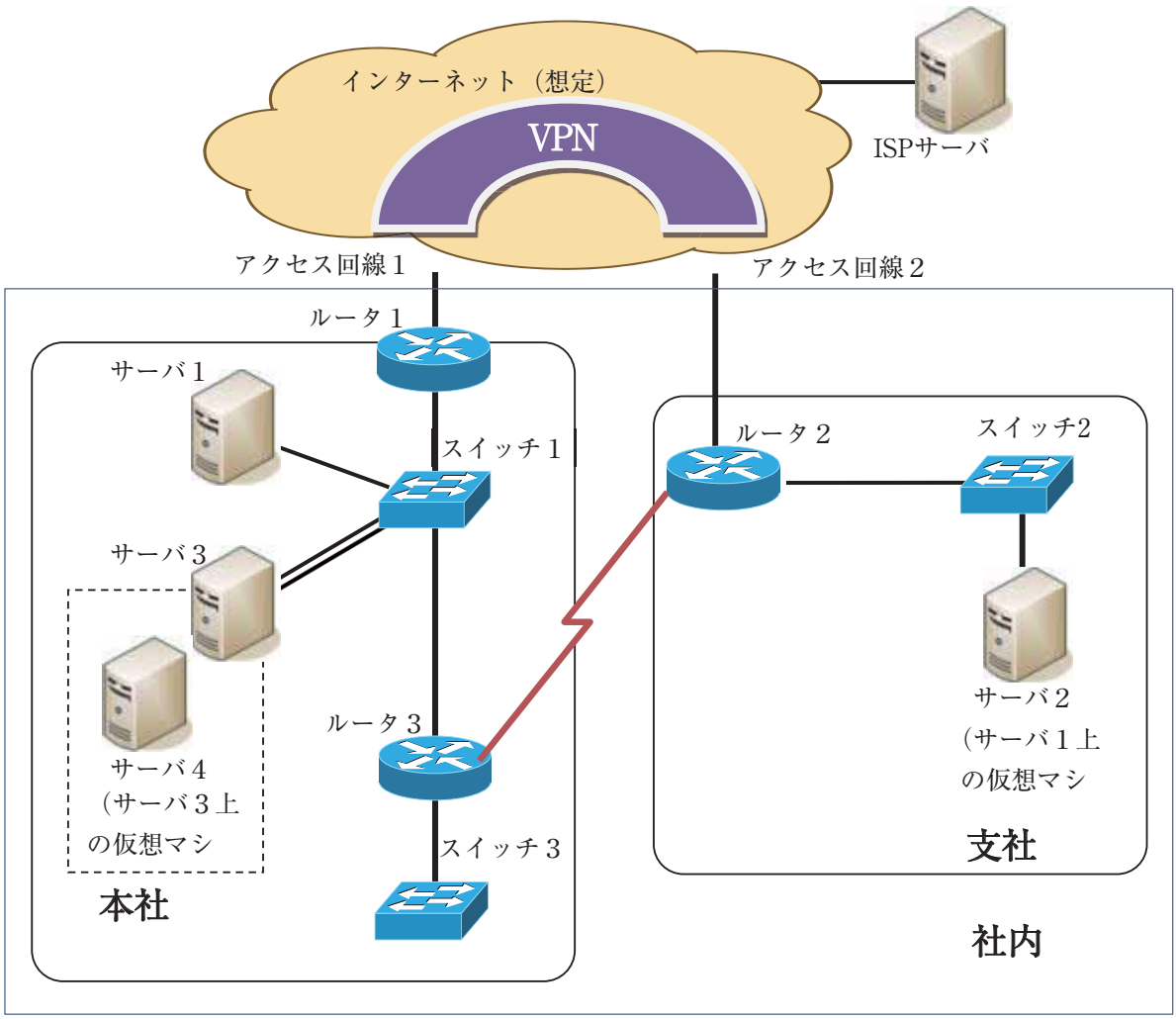
⑥ 各競技エリアには「外部ネットワークJ（L3スイッチ）とつながるLANケーブルが2本敷設されている。アクセス回線１とアクセス回線２の区別があるため適切に接続すること。

⑦ ISPサーバ（検証用サーバ200.99.1.1）の機能

インターネット（想定）上にISPサーバ（検証用サーバ）が設置されている。DNS、Webサーバ、Mail（SMTP）サーバのサービスが稼働している。必要に応じて各競技者エリアまで敷いてあるLANケーブルを通してアクセスしてよい。

競技課題１において、構築を行うネットワークの仕様概要は以下の通りとする。

社内で４台のサーバを構築する。サーバ１は本社DMZ、サーバ２は支社DMZに設置して社内外に対してサービスを提供する。サーバ３とサーバ４は本社に設置して、社内に対してサービスを提供する。今回、物理サーバが２台しか用意出来なかったため、サーバ２はサーバ１上の仮想マシン、サーバ４はサーバ３上の仮想マシンとして動作させる。仮想化ソフトウェアはKVMとHyper-Vを使用する。社内には本社・支社ネットワークが存在する。本社ネットワークにはサーバ接続用のVLAN以外にクライアント接続用のVLANが２つあり、このうち一方はインターネットへの直接的接続を許可しないセグメントとする。支社ネットワークも同様とする。本社と支社間の通信はプライマリ経路としてインターネット経由のVPNを使用する。ただし、このVPN回線に障害が発生した場合はバックアップ経路として専用線（検証環境ではシリアル回線）にて通信可能とする。また、インターネットへのアクセス回線についても本社・支社が互いにバックアップ経路となる構成とする。



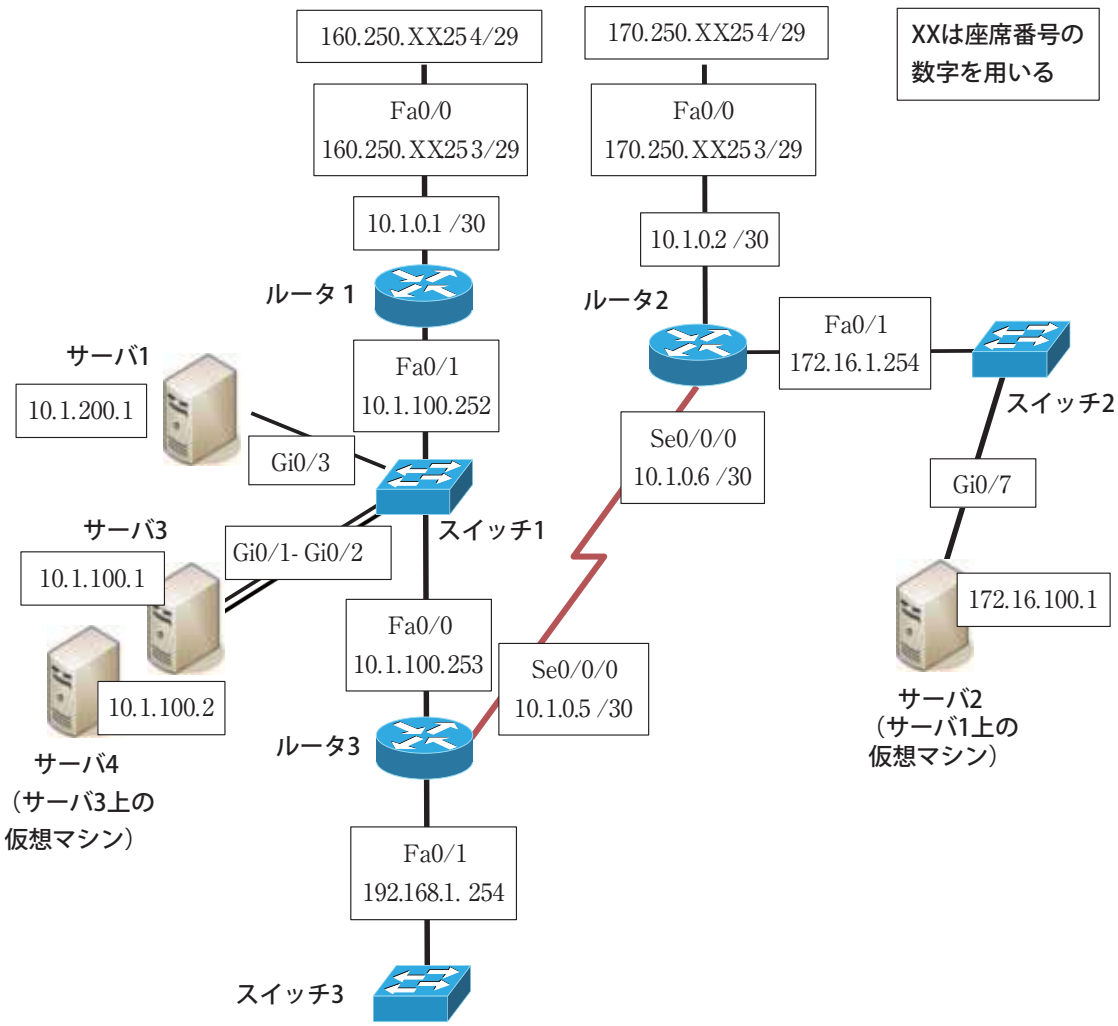
(2) 課題１　ネットワーク構成

今回の競技課題１に関して、本競技で使用する機材・環境及び競技時間・内容を考慮した場合、過去に行われた国内大会での競技課題の内容について全て公開することは、今後の競技の運営上好ましくないと考えられる。競技課題１の全ての課題内容や設定方法、解答も公開されていないため、今回公開された課題内容（本マニュアルの巻末資料参照）で、本マニュアルの作業手順書は作成されており、さらに競技大会での設定方法や解答とは異なる場合がある。

競技開始と同時に公表される課題について、決められた競技時間内で熟読し、課題内容を理解する。課題内容によって作業の段取り、時間配分を考える。

技能ポイント

① 各サーバに指定されたIPアドレスと、DNS（ドメインネームサーバ）、Web（ウェブサーバ）、Mail（メールサーバ）、Proxy（プロキシサーバ）、リモート管理、仮想環境を導入する。
② ルータ１、２で、外部と内部のIPアドレスを設定し、通過するポートなど、セキュリティ面を強化する上でスイッチやルータに接続できるよう設定する。
③ ルータやスイッチから各サーバに接続するIPアドレス、通過するポートを設定する。



［1］サーバシステムの構築

① ハードウェア BIOS 設定

周辺機器が認識しなかったり、不具合が含まれている可能性があるため常に最新の状態を保つようする。まず、PCを再起動し、BIOS設定画面に入る。入り方は、PC起動時の自己診断テスト（POST）の間に<DEL>キーを押すことで入る。

BIOSの最適設定をする。HDDのモード設定、Bootデバイス設定、Core 2 Duo用のCPU設定、ファンの制御、メモリ設定など。
左図はOSをインストールする時にCDを使用するため、ハードドライブCをCD-ROMドライブに変更している。

POINT

BIOS は最後に保存を忘れないこと。
キーボードのキー操作に慣れておく。

② OS のインストール

各サーバ共通設定

システム時刻を競技会場の時計と ± 5 分以内に合わせる。

②－１　サーバ１のインストール

コンピュータ１にサーバ１のOSとして、Debian GNU/Linux 7.5.0を以下の通りインストールする。

キー配列	日本語キーボード
タイムゾーン（ローカル時間）	Asia/Tokyo
管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意（user）
一般ユーザのパスワード	user
ホスト名	sv01
ドメイン名	netadXX.it.jp（netad01.it.jp）

サーバ１のネットワーク設定は以下の通りとし、eth0にてネットワーク接続可能とする。

IPアドレス	10.1.200.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.200.254
ネームサーバ	自身

サーバ１のパーティション構成を以下の通りとする。ただし、ソフトウェアの仕様上、サイズが若干異なっても良い。

マウントポイント	容量	ファイルシステム
/boot	100MB	ext4
/	40GB	ext4
/var	50GB	ext4
スワップ	4GB	−

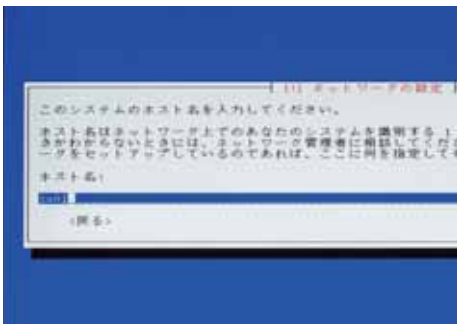
※1GBは、1024MBとする。

②－２　インストール手順

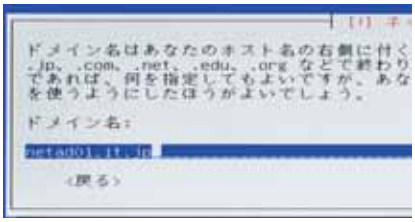
CDを挿入して起動すると、このような画面が表示される。「Install」にカーソルを合わせ、Enterを押すと、インストールを開始することができる。

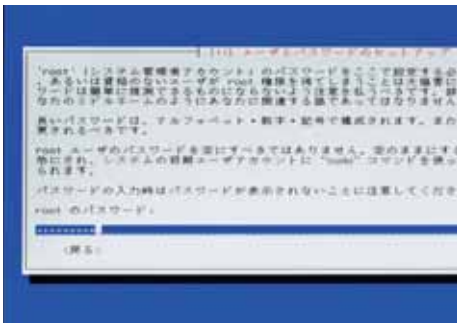
言語選択画面が表示されるので、「Japanese 日本語」を選択して、Enterを押す。
次に進むと、場所の選択画面が表示される。ここではタイムゾーンの指定を行う。

ネットワークの設定では、まずIPアドレスの設定を行う。このPCで使用するIPアドレスの入力を行う。ネットマスク、デフォルトゲートウェイの順に設定を行い、ネームサーバの設定を行う。ネームサーバは、このPCが参照するDNSサーバのIPアドレスを入力する。



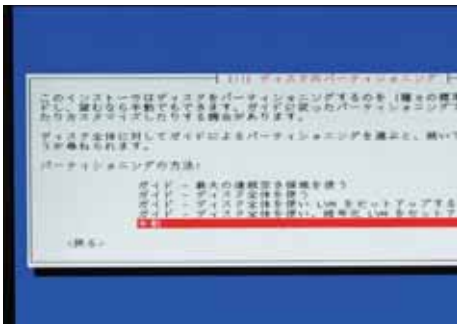
ホスト名の入力には「sv01」と入力する。
次のドメイン名は「XX」に注意する必要がある。「XX」には自身の座席番号を使用する。



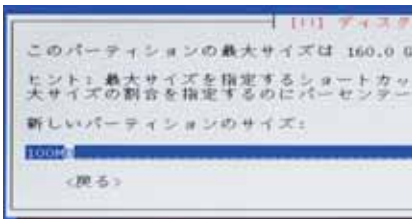


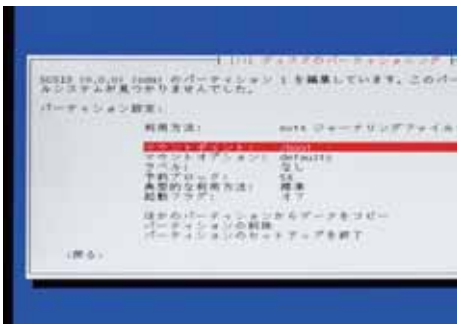
システム管理者である特権ユーザ「root」のパスワードの入力とその確認を行う。
rootユーザとは、システムを管理するための特別なユーザである。パスワードの誤入力に注意すること。

ユーザアカウントの設定を行う。前述の「②-1サーバ1のインストール」の表にある一般ユーザの項目を参照して設定する。
一般ユーザとは、rootユーザと異なり、システム管理を行えないユーザとなる。また、一般ユーザはインストール終了後でも、作成することが可能。



容量の指定を間違えてしまうと、変更ができない場合があるため、注意して入力すること。
手動を選択し、サイズを入力する。





課題の指定に合わせてディスクのパーティショニングを行う。

ソフトウェアの選択画面では、指定したソフトウェアのインストールを行う。

インストール後の環境として、GUIを用いる場合は、「Debian デスクトップ環境」にチェックを付ける。
また、「標準システムユーティリティ」のチェックは外さないこと。

プリンターサーバは使用しないのでチェックを外す。

ブートローダーのインストールを行う。

③ サーバ２（仮想マシン）のインストール

サーバ２はサーバ１のKvmとvirt-managerを使用して仮想環境にて構築する。

・仮想マシン名は「sv02」とする。
・ホストであるサーバ１はeth1にてネットワーク接続しないこと。
・仮想マシンのイメージファイル容量、パーティション構成、メモリサイズなどは任意とする。
・仮想マシン「sv02」はサーバ１の起動時に自動起動すること。

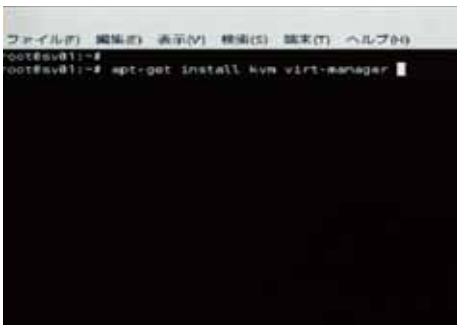
サーバ２のOSとしてDebian GNU/Linux 7.5.0を以下の通りインストールする。

キー配列	日本語キーボード
タイムゾーン（ローカル時間）	Asia/Tokyo
管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意（user）
一般ユーザのパスワード	user
ホスト名	sv02
ドメイン名	aichi.netadXX.it.jp（aichi.netad01.it.jp）

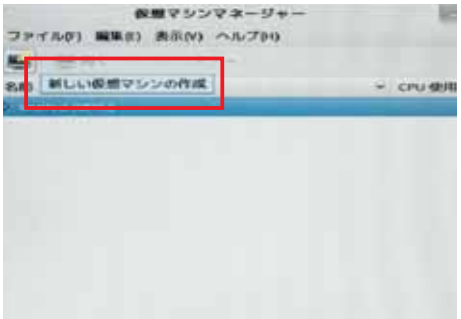
サーバ２のネットワーク設定は以下の通りとする。

IPアドレス	172.16.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.16.100.254
ネームサーバ	自身

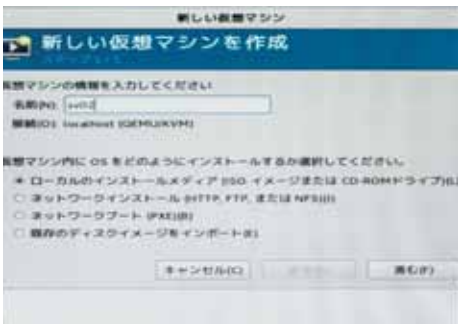
サーバ１の Kvm と virt-manager を使用して仮想環境にて構築する。



左図のコマンドを使用して、kvmとvirt-managerをインストールする。



virt-managerを起動する。virt-managerの画面左上の「新しい仮想マシンの作成」をクリックする。



仮想マシンの名前は「sv02」と入力する。
「ローカルのインストールメディア（ISOイメージまたはCD-ROMドライブ」を選択して、次に進む。

DebianのインストールDVDを読み込ませて、OSインストールを行う。sv02仮想マシンのフォルダが表示される。インストールが終わると端末上で仮想サーバの操作・設定ができるようになる。

アドバイス

OS のインストールには待ち時間が発生するため、仮想環境を構築する前に別の作業ができる状態にしておくと良いでしょう。
パーティション構成時は、容量の指定に間違いがないか、注意して確認してください。

④ サーバ３のインストール

コンピュータ２にサーバ３のOSとして、Windows Server 2012 R2を以下の通りインストールする。

キー配列	日本語キーボード
タイムゾーン（ローカル時間）	Asia/Tokyo
管理者のパスワード	Aichi2014
コンピュータ名	sv03
ドメイン名	netadXX.local（netad01.local）

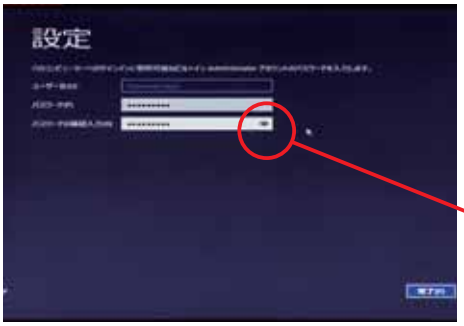
ネットワーク設定は以下の通りとする。

IPアドレス	10.1.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.100.254
ネームサーバ	自身

④－１　Windows Server 2012 R2 評価版のインストール

DVDメディアをドライブにセット（マウント）し、起動するとセットアップ画面が表示されるので、「次へ」をクリックする。インストールが開始され、しばらく（15分～30分ぐらい）時間がかかる。インストール中に各機器の配線をしておく。

オペレーティングシステムをGUI使用サーバにして、インストール場所を選択する。



再起動後、Administratorパスワード入力画面が表示されるので、任意のパスワードを入力し、「完了」をクリックする。

POINT

パスワードの入力を間違えないこと。
Windows Server 2012 R2 では、入力欄内の右にあるボタンを押すことで、入力した文字列を確認できる。

④－２　各サーバをインストール

Hyper-VとActive Directoryを順番にインストールしていく。

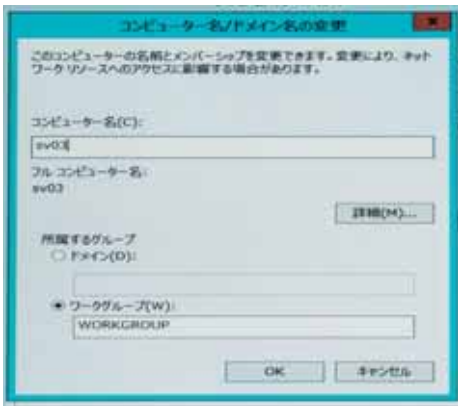
Active Directory

・作成するフォレストドメインを「netad01.local」とする。

・フォレストとドメインの機能レベルは「Windows Server2012 R2」とする。

・ディレクトリサービスの復元モードパスワードは「Aichi2014」とする。

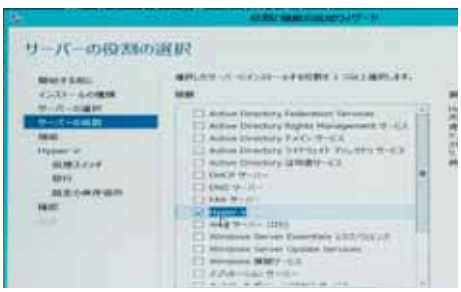
ログオン画面が表示されるので、「Ctrl」+「Alt」+「Delete」を押下して、先ほど設定したパスワードでログオンする。



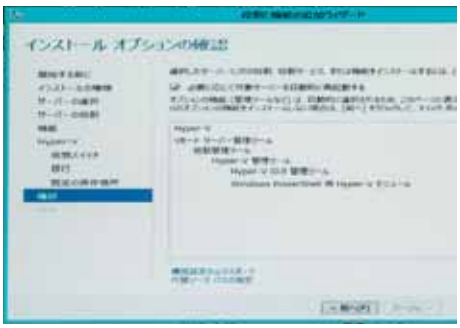
ホスト名（sv03）を入力して、再起動する。

ネットワーク接続するため、IPアドレス、DNSサーバアドレス、ホスト名を入力

メニューより「サーバーマネージャー」を起動する。起動後「2　役割と機能の追加」メニューをクリックする。



「インストール種類の選択」表示後、"役割ベースまたは機能ベースのインストール"が選択されていることを確認の上、「次へ」ボタンクリックする。「サーバの役割」の選択画面が表示されるので、まず、Hyper-Vにチェックをつけ、Hyper-Vをインストールする。



「機能」の選択「役割サービス」の選択「インストールオプションの確認」の順に操作して、インストールが始まる。サーバ機のハードスペックにより、数分から数十分の時間を要する。

Active Directoryのインストール

Active Directoryドメインサービスをインストール後、ドメインコントローラーへの昇格を行う。

作成するフォレストドメインを「netad01.local」、フォレストとドメインの機能レベルは「Windows Server2012 R2」、ディレクトリサービスの復元モードパスワードは「Aichi2014」とする。

アドバイス

サーバのインストール時には管理者のパスワード入力があります。パスワードの入力は絶対に間違えてはいけません。管理者のログオンができない場合は、OS の再インストールをする必要があります。
サーバはサービスをインストールしなくては設定ができません。インストール作業を速く、スムーズにできるようになれば、サービス設定に掛ける時間を長くすることができます。

⑤ サーバ４（仮想マシン）のインストール

サーバ４はサーバ３のHyper-Vを使用して仮想環境にて構築する。

・仮想マシン名は「sv04」とする。「sv04」はサーバ３の起動時に自動起動すること。

・仮想HDD容量、パーティション構成、メモリサイズなどは任意とする。

サーバ４のOSとしてDebian GNU/Linux 7.5.0を以下の通りインストールする。

管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
ホスト名	sv04
ドメイン名	netadXX.local（netad01.local）

サーバ４のネットワーク設定は以下の通りとする。

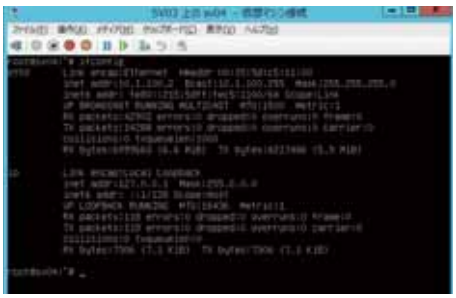
IPアドレス	10.1.100.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.100.254
ネームサーバ	10.1.100.1

Hyper-Vマネージャを起動する。
新規仮想マシンの作成の名前は「sv04」と入力する。仮想HDD容量、パーティション構成、メモリサイズなどは任意に設定する。

POINT

Hyper-V で仮想サーバを構築する時は、ホストマシンの BIOS で Intel Virtualization Technology（Intel VT）とデータ実行防止（DEP）を有効にする。

仮想マシンが使用するNIC（インターフェース）の指定をする。
仮想マシンが物理NICを使用できるためには、仮想スイッチマネージャにて、仮想スイッチの作成をしておく必要がある。



Debianのインストール DVDを読み込ませて、OSのインストールを行う。インストールが終わるとHyper-Vの端末上で仮想サーバの操作・設定ができるようになる。
コマンドifconfigで設定状況を確認する。

アドバイス

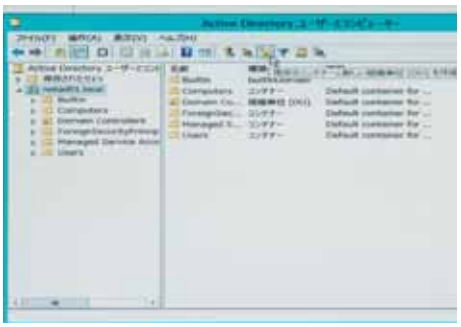
サービスのインストール前に、IP アドレスやホスト名など基本的な設定はしておきましょう。一部のサービスはインストール時にホスト名などを参照している場合があります。競技中、インストール作業は時間を掛ける項目ではありません。作業自体も単純なので、スムーズにできるようにしておくといいです。

⑥ Active Directory

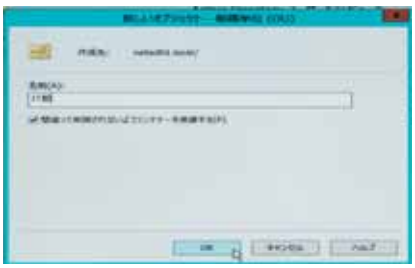
サーバ３上にActive Directoryドメインコントローラーを以下の通り構築する。

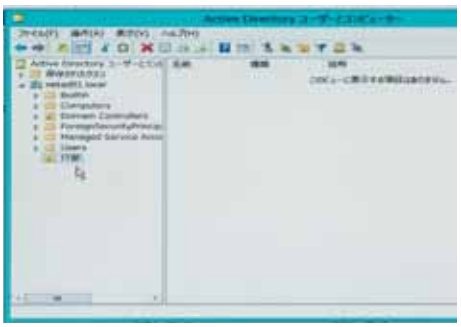
・以下の表に従ってOU、グループ、ユーザを作成する。

ユーザ名	パスワード	OU	グループ
aduser01	Aichi2014	IT部	Employee
aduser02	Aichi2014	IT部	Employee
aduser03	Aichi2014	IT部	Employee

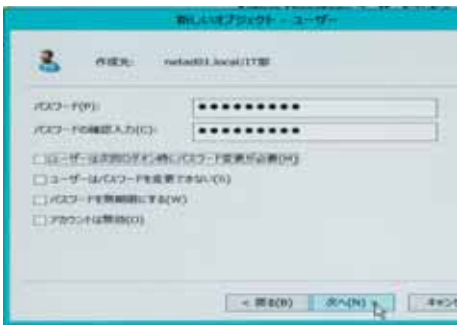


ActiveDirectoryユーザーとコンピューターを開く。
natad01.localを選択して、「IT部」OU（組織単位）を作成する。





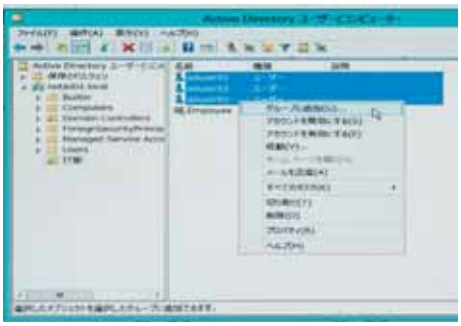
IT部を選択して、「aduser01」ユーザを作成する。



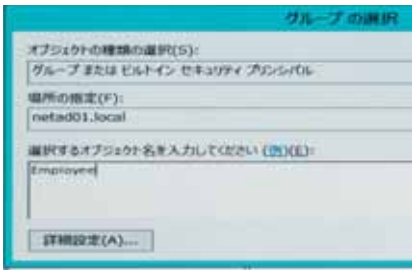
パスワードを入力する。

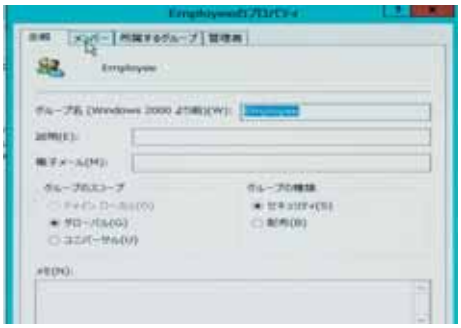
同様に「aduser02」「aduser03」を作成する。

次に「IT部」OUに「Employee」グループを作成する。

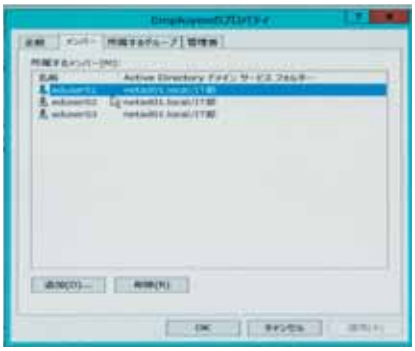


作成したユーザを「Employee」グループに追加する。





Employeeのプロパティを作成する。



⑦ 認証統合

［サーバ４］

サーバ４のユーザ認証をサーバ３上のActive Directoryサービスによって行なえるように以下の通り設定する。

・使用するパッケージはsambaおよびwinbindとする。

・サーバ４をサーバ３のActive Directoryドメインのメンバサーバとして参加させる。

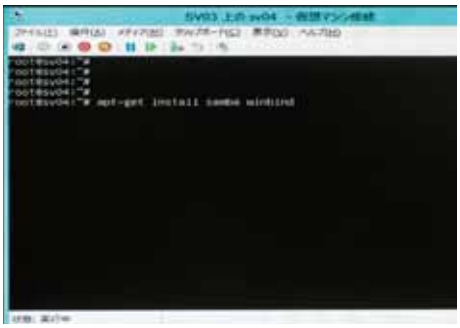
・サーバ３上に登録したActive Directoryユーザにてサーバ４へログイン可能とすること。この際、Active Directoryドメイン名の指定は省略できること。また、各ユーザ（aduser01～03）のホームディレクトリ「/home/win/ユーザ名」（例 /home/win/aduser01）は初回ログイン時に自動作成されること（例：初回ローカルログイン時、初回sshログイン時、初回pop3sログイン時）。

ホームディレクトリの自動作成が不可能な場合は手動で作成する*。

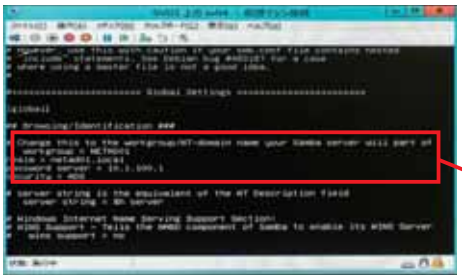
・上記指定の方法による認証統合が不可能な場合は、その他の方法によって認証統合を構成して構わない*。

・認証統合が不可能な場合は、「Active Directory」で作成したユーザ名・パスワードと同一ユーザ名・パスワードの新規アカウントをサーバ４上に手動で作成する*。

＊ただし、減点対象とする。

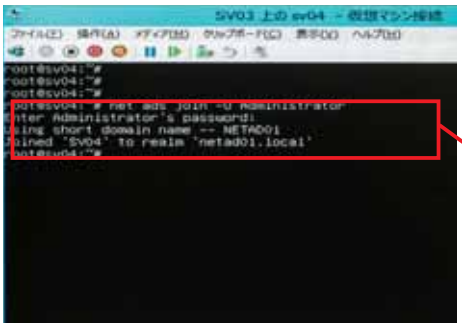


samba、winbindのパッケージをインストールする。



/etc/samba/smb.confに左図の設定を行う。
workgroupは、NETBIOS名を指定する。
realmには、Active Directoryのドメイン名（netad01.local）を指定する。

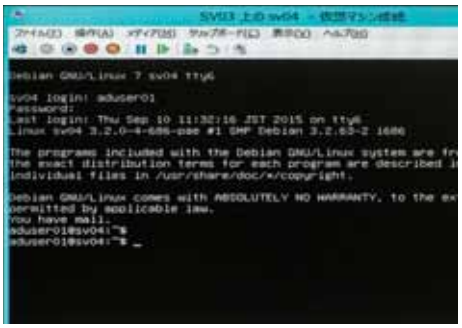
```
realm = netad01.local
password sever = 10.1.100.1
security = ADS
```



AD（Active Directory ）ドメインへの参加
「net ads join -U Administrator」コマンドを実行して、サーバ４をActive Directoryのドメインに参加させる。

```
Enter Administrator’s password:
Using short domain name--NETAD01
Joined ‘SV04’ to realm ‘netad01.local’
```

/etc/nsswitch.confに設定をする。
これにより、Active Directoryのユーザを Linuxの一般ユーザのように使用することができる。



サーバ４上でActive Directoryユーザのログインができる。

POINT

Active Directory のユーザを使用するため、サーバ４では一般ユーザを作成しないこと。

アドバイス

サーバ４（winbind）が、DNS サーバを使用して名前解決できるようにしておきましょう。
また、サーバ３とサーバ４の時刻が同じになっている必要があります。

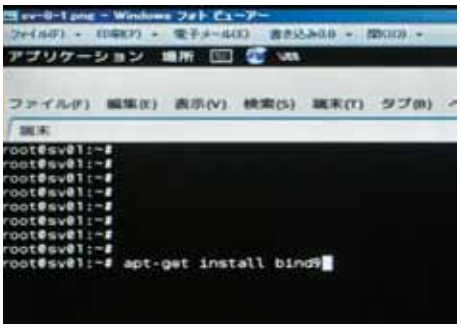
⑧ DNS の設定

［サーバ１、サーバ２共通］

・使用するパッケージはbind9とする。
・自身で名前解決ができない場合は、ISPサーバに問い合わせる。
・bindのバージョンを回答しない。

⑧－１　DNS サーバのインストール

TCP/IPの構成、所属ドメインの構成



パッケージ名「bind9」をroot 権限でインストールする。

POINT

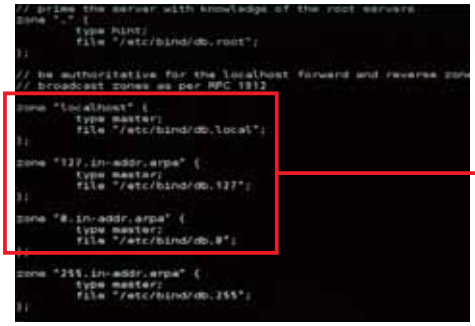
パッケージのインストールは「root」ユーザでしか行えない。「root」ユーザは管理者ユーザのことで、サーバを管理する上で特別な権限が与えられている。

⑧－２　サーバ１の設定

・「社内」および「外部ネットワーク」からの問い合わせに応える。
・再帰問い合わせは自身（localhost）とサーバ３からのみ許可する。
・「外部ネットワーク」向けのnetadXX.it.jp（netad01.it.jp）およびaichi.netadXX.it.jp（aichi.netad01.it.jp）ゾーンの管理を行うマスターサーバとして動作させる。サーバ１とサーバ２の正引きを設定する。別名としてサーバ１は「mailgw.netadXX.it.jp（mailgw.netad01.it.jp）」、サーバ２は「www.aichi.netadXX.it.jp（www.aichi.netad01.it.jp）」を持つ。
・「社内」向けのnetadXX.it.jp（netad01.it.jp）およびaichi.netadXX.it.jp（aichi.netad01.it.jp）ゾーンと、その逆引きゾーンの管理を行うマスターサーバとして動作させる。サーバ１とサーバ２の正引き・逆引きを設定する。別名としてサーバ１は「proxy.netadXX.it.jp（proxy.netad01.it.jp）」、サーバ２は「mail.aichi.netadXX.it.jp（mail.aichi.netad01.it.jp）」を持つ。
・サーバ３で管理しているゾーンのスレーブとして動作させる。

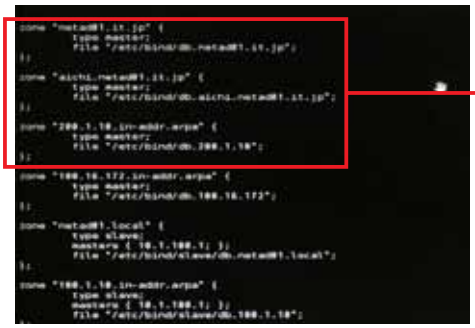
用語解説

・主なレコードには以下の種類がある。
　A レコード……正引きレコードとも呼ばれる。FQDN から IP アドレスを解決する。
　PTR レコード……逆引きレコードとも呼ばれる。IP アドレスから FQDN を解決する。
　CNAME レコード……別名、エイリアスとも呼ばれる。ホスト名の別名を登録する。
　NS レコード……そのドメインを管理する DNS サーバを登録する。
・再帰問い合わせとは、DNS サーバ自身が名前解決を行えない場合、別の DNS サーバへ名前解決を委任すること。



ゾーンとはドメインを管理する範囲のことを指す。
ゾーンの初期画面

```
zone "localhost"{
        type master;
        file"/etc/bind/db.local";
};
zone "127;in-addr.arpa"{
        type master;
        file"/etc/bind/db.127";
};
zone "0;in-addr.arpa"{
        type master;
        file"/etc/bind/db.0";
};
```

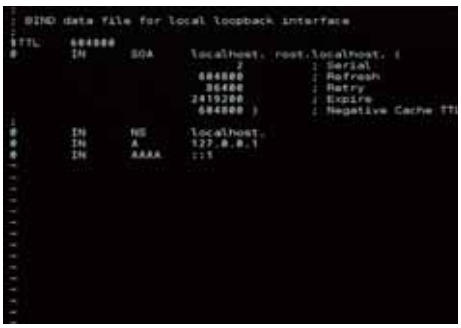


左図のようにゾーンを変更作成する。

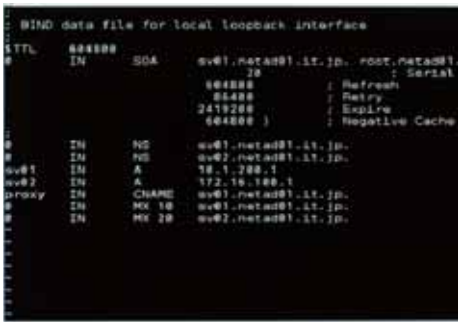
```
zone "netad01.it.jp"{
        type master;
        file"/etc/bind/db.netad01.it.jp";
};
zone "aichi.netad01.it.jp"{
        type master;
        file"/etc/bind/db.aichi.netad01.it.jp";
};
zone "200;1.10.in-addr.arpa"{
        type master;
        file"/etc/bind/db.200.1.10";
};
```

POINT

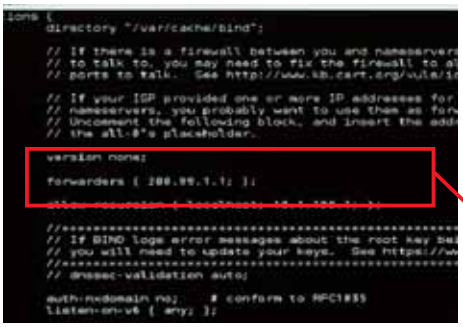
文字列の入力を間違えないよう注意する。



ゾーンファイル内のレコードの初期画面



ゾーンファイル内に、レコードを追加する。



「allow-recursion」を用いて、どのホストからの再帰問い合わせを許可するかの設定を行う。この設定により、どのホストからの名前解決要求に対して、再帰問い合わせを行うかを決める。
名前解決を委任する別のDNSサーバは、「forwarders」を使用して設定をする。

入力

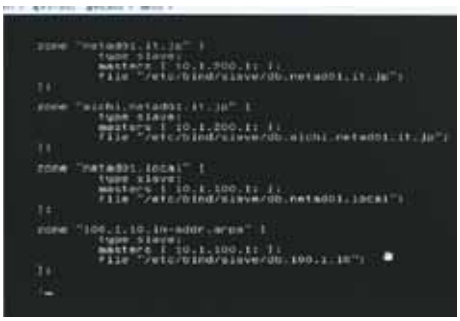
```
version none:
forwarders  { 200.99.1.1 ;  } ;
allow-recursion { localhost : 10.1.100.1 ; } ;
```

⑧－３　サーバ２の設定

・「社内」および「外部ネットワーク」からの問い合わせに応える。
・再帰問い合わせは自身（localhost）と「支社内」からのみ許可する。
・サーバ１とサーバ３で管理しているゾーンのスレーブとして動作させる。

用語解説

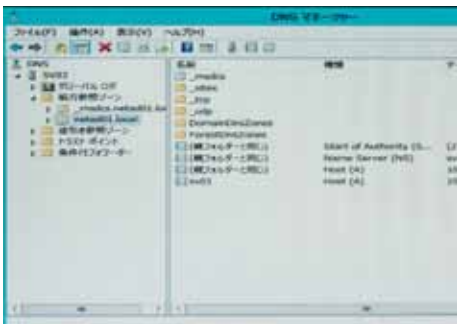
ゾーン転送とは、他の DNS サーバが管理しているゾーン情報を取得すること。もともと管理している DNS サーバがゾーンを編集すると、スレーブ側でも編集内容が自動的に更新される。
同じゾーンを持った DNS サーバが複数台存在することで負荷を分散することができる。



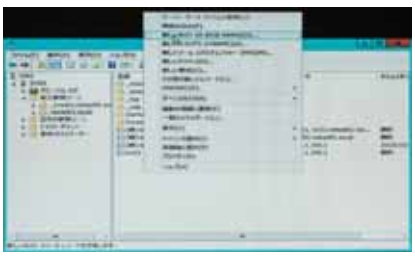
スレーブとして動作することから、このDNSサーバはゾーン転送を使用することが分かる。

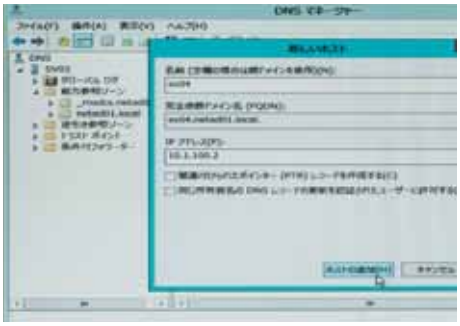
⑧－４　サーバ３の設定

・Windows Server2012R2のDNSサーバを使用する。
・自身で名前解決ができない場合は、サーバ１に問い合わせる。
・「社内」からの問い合わせに応える。
・netadXX.local（netad01.local）ゾーンとその逆引きゾーンの管理を行うマスターサーバとして動作させる。サーバ３とサーバ４の正引き・逆引きを設定する。別名としてサーバ４は「mail.netadXX.local（mail.netad01.local）」と「proxy.netadXX.local（proxy.netad01.local）」を持つ。

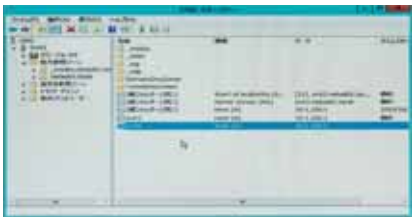


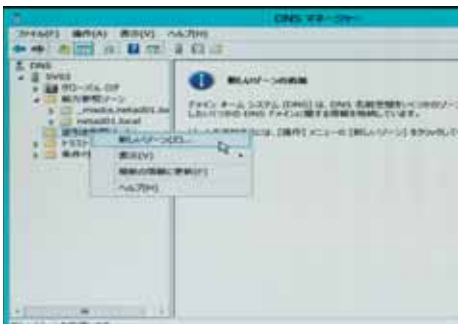
Windows Serverでは、左図のような画面でDNSの設定を行う。
ActiveDirectoryをインストールしたサーバでは、自動的にDNSがインストールされる。
DNSサーバの正引きゾーン内容。



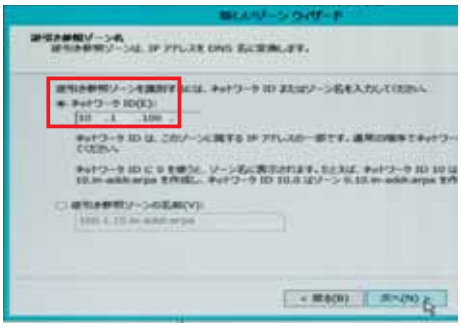


右クリックして新しいホストを追加作成する。





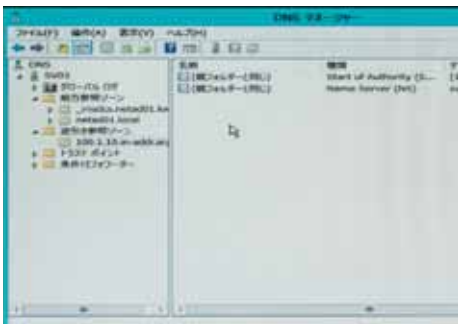
DNSサーバの逆引きゾーン内容。
新しいゾーンウィザードからゾーンの種類（Activ Directory）を作成する。



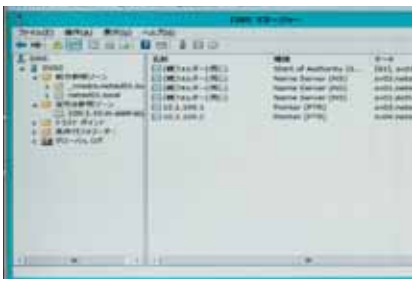
逆引き参照ゾーンのネットワークID（10. 1.100.1）を作成する。

POINT

正引きは A レコード、逆引きは PTR レコード、別名は CNAME レコードで設定する。



同様にネットワークID（10.1.100.2）を作成する。



アドバイス

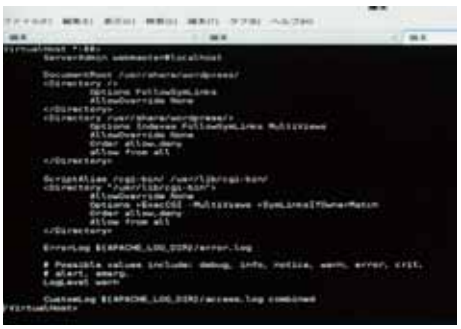
DNS とは、FQDN（完全修飾ドメイン名の略称。ホスト名とドメイン名を合わせたもの）と IP アドレスを関連付ける設定となります。これを名前解決といいます。
この DNS の名前解決は他のサービスに影響する重要な設定です。ホスト名やドメイン名、IP アドレスの文字列の間違いがないよう、よく確認してください。
また、どの競技課題でも出題されるほど基本的なサービスです。競技者としては、必ず設定できる必要があります。

⑨ 各サービスとアプリケーションの設定

⑨－１　Web サーバサービスの設定

サーバ１でWebサーバサービスを行う。

Webサーバには、apache2をインストールして、構築する。



Webサーバのポート番号80番の内容表示

Internet ExplorerにURLを入力することで、Webサイトを閲覧することができる。
google chromeやInternet Explorerは、Webサーバへアクセスすることでwebページを表示している。

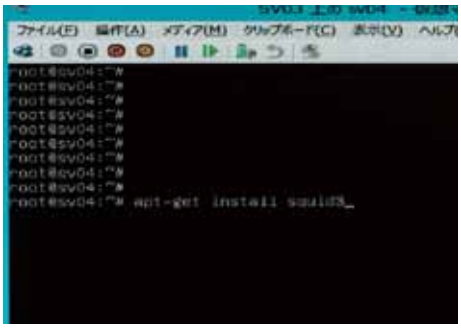
⑨－２　プロキシサービスの設定

サーバ１とサーバ４でプロキシサービスを行う。使用するパッケージはsquid3とする。

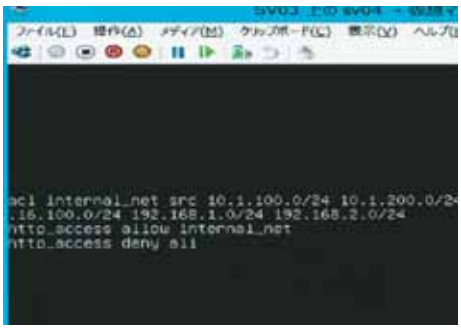
・グループポリシーを用いて、サーバ３のActive Directoryドメインユーザに対し、Internet Explorerが利用するプロキシサーバとしてサーバ４が指定されるように動作させる。

用語解説

・プロキシとは、代理という意味がある。クライアントが直接 Web サーバにアクセスせず、プロキシサーバがクライアントの代わりに Web サーバへとアクセスする。キャッシュ機能も備わっているため、Web サーバの負荷を下げることもできる。
・グループポリシーとは、Active Directory のドメインに参加している PC に対して、各種設定を自動的に行う機能。

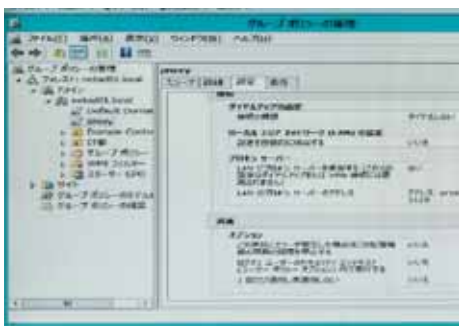


squid3をインストールして、プロキシサーバを構築する。



プロキシサーバを使用できるホストやネットワークの指定を行う。デフォルトでは、全てのホストやネットワークからの使用が拒否されている。（http-access denyall ）
sv04を設定終了後、sv01も同様に設定を行う。

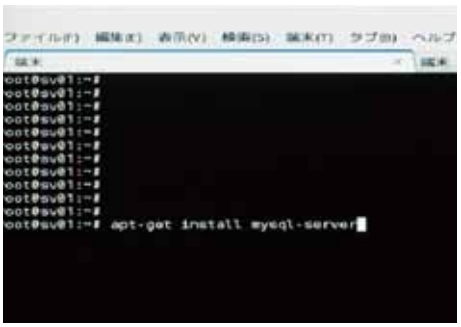
次にsv03のWindows Serverのグループポリシーを使用して、クライアントPCのInternet Explorerに利用するプロキシサーバの指定を行う。
多数あるPCに一つ一つ設定をしなくても、グループポリシーのみ設定することで、一元管理することができる。



グループポリシーは各OU毎やグループ毎に分けることができるため、それぞれのグループの用途に従って、細かく制御することができる。

⑨ー３　WordPress の設定

サーバ１でWordPressサービスを行う。



データベース用のパッケージとして、mysql-serverをインストールする。

コマンドを実行し、mysqlをセットアップする。
ここにデータベースへアクセスする時のユーザ名とパスワード等を登録する。

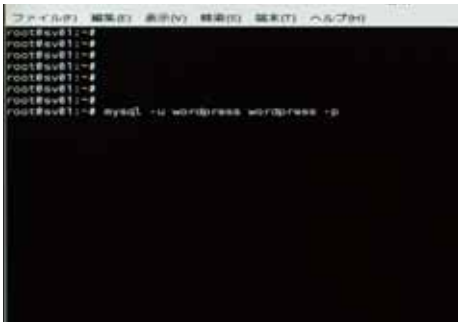
WordPressをインストールして初期設定を行う。
ノートパソコンからWebブラウザーでWordPressのWebサイトにアクセスすると、左図のようなページが表示される。

⑨－４　WordPress 用のデータベースの確認

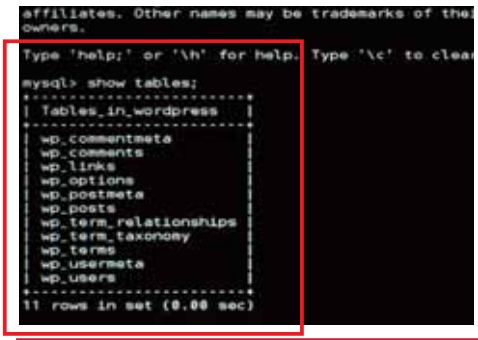
サーバ１でデータベースサービスを行う。

用語解説

大量のデータを格納するためのデータベースを提供するサービス。
Web サイトのデータを保存しておくこともできる。



コマンド（mysql –u wordpress wordpress -p）を入力して、内容を確認する。⑨－3では、データベースは作成されていないので、ここでデータベースを作成する。



WordPress用のデータベースとして動作しており、左図のようなデータベースの内容でデータを登録している。

POINT

今回は、WordPress 用のデータベースを作成する。

アドバイス

複数のサービスが関連して動作する設定となっています。設定手順に気を付ける必要があります。プロキシやWordPressを行うためにはWebサーバを構築していなくてはいけません。最初に Web サーバを構築し、プロキシ、WordPress といった流れで行うと効率よく作業ができます。
また、Web サーバにアクセスする時の URL は、DNS の名前解決に基づいています。Web へのアクセスでトラブルが起こった場合は、DNS の設定も見直してみるといいと思います。

⑩ メールサーバの設定

［サーバ１、サーバ２、サーバ４共通］

・使用するパッケージはpostfixとする。

⑩－１　メールサーバのインストール

postfix をインストールする。
/etc/postfix/main.cfを編集して、設定を行う。

POINT

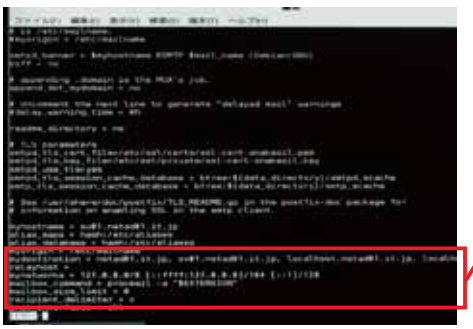
メールサーバには、クライアントから送信されたメールを受け取る送信サーバと受け取ったメールをクライアントへ渡す受信サーバがある。

⑩－２　サーバ１の設定

・メールゲートウェイとして動作させる。
・本社ドメイン netadXX.it.jp（netad01.it.jp）のプライマリメールサーバ、支社サブドメイン aichi.netadXX.it.jp（aichi.netad01.it.jp）のセカンダリメールサーバとなる。
・本社ドメインnetadXX.it.jp宛てのメールはサーバ４へ転送する。
・支社サブドメインaichi.netadXX.it.jp宛てのメールはサーバ２へ転送する。
・その他の宛先のメールは ISPサーバへ転送する。この際、SMTP認証を行い、認証が成功した時のみ中継を許可する。認証用ユーザとしてmailuserを作成する。パスワードはユーザ名と同一とする。ただし、サーバ４からは認証なしで中継を許可する。

用語解説

・メールゲートウェイとは、メールが送信された時に、適切なメールサーバへメールを転送することのみを目的に構築されるメールサーバのこと。
・SMTP 認証とは、メール送信時にユーザ名とパスワードを入力させ、正しい場合だけメールの送信ができるようにする認証技術。



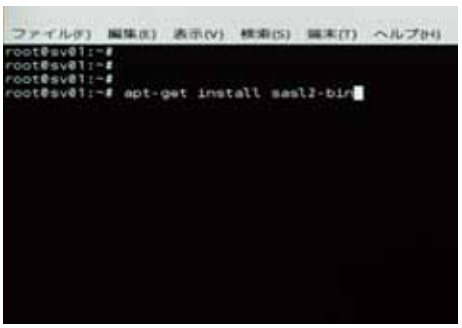
通常のメールサーバは、送信されたメールのドメインを判断して、そのメールを自身に保存しておくか、適切なメールサーバへの転送をする。
初期設定

```
mydestination = netad01.it.jp,sv01.
netad01.it.jp,
localhost.netad01.it.jp,localhost
Relayhost =
```

メールゲートウェイへの設定変更

```
mydestination =
Relayhost = 200.99.1.1
```

注：上記は設定変更例である、競技課題の仕様を満たすにはより詳細な設定変更を行わなければならない。



SMTP認証には、sasl2-binパッケージをインストールして設定を行う。

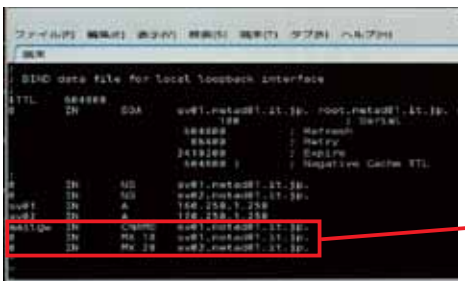
左図の内容を/etc/postfix/sasl/smtpd.confに設定する。

⑩－３　サーバ２の設定

・支社サブドメインaichi.netadXX.it.jp（aichi.netad01.it.jp）のメール送信サーバとして動作させる。
・支社サブドメインaichi.netadXX.it.jp（aichi.netad01.it.jp）のプライマリメールサーバ、本社ドメインnetadXX.it.jp（netad01.it.jp）のセカンダリメールサーバとなる。

用語解説

・プライマリメールサーバとは、あるドメイン宛のメールをメインで処理するサーバのこと。
・セカンダリメールサーバは、プライマリメールサーバに障害が発生した時、代わりに処理を行うサーバのこと。



メールサーバの優先順位はDNSサーバにて行う。
サーバ１のゾーンにMXレコードを登録する。
メールサーバは、メール転送時にMXレコードを参照して、転送先を決めることができる。

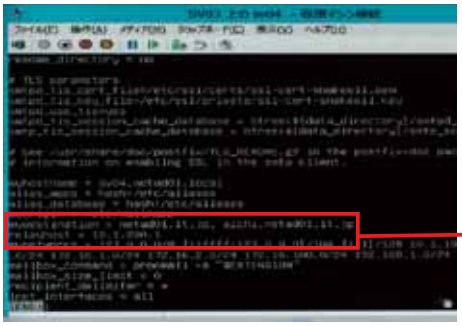
```
0    IN  MX10   sv01.netad01.it.jp
0    IN  MX20   sv02.netad01.it.jp
```

POINT

MX レコードを指定する時に優先度を指定でき、数値の小さい方が優先度が高い。

⑩－４　サーバ４の設定

・本社ドメインnetadXX.it.jp（netad01.it.jp）のメール送信および受信サーバとして動作させる。
・本社ドメインnetadXX.it.jp（netad01.it.jp）宛てのメールをスプールする。保存形式は任意とする。



「mydestination」にドメイン名を指定することで、指定したドメインのメールが送信された時に、自身のフォルダ内へと保存をする。何も指定が無い場合は、どのドメインのメールも保存しない。

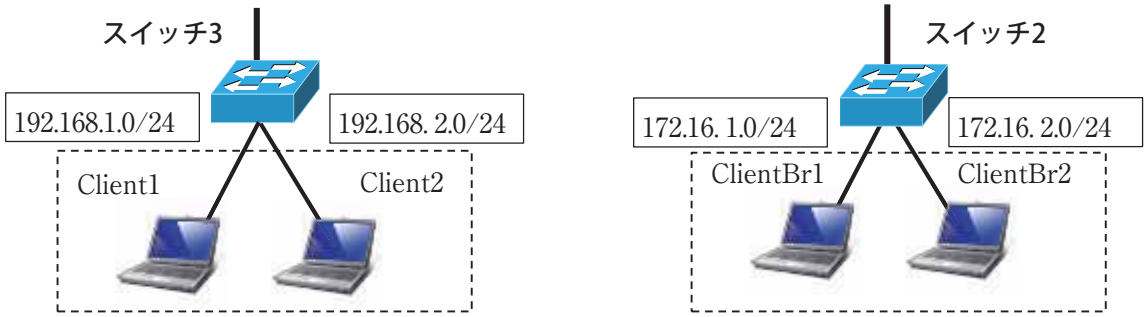
```
mydestination = netad01.it.jp
Relayhost = 10.1.200.1
```

アドバイス

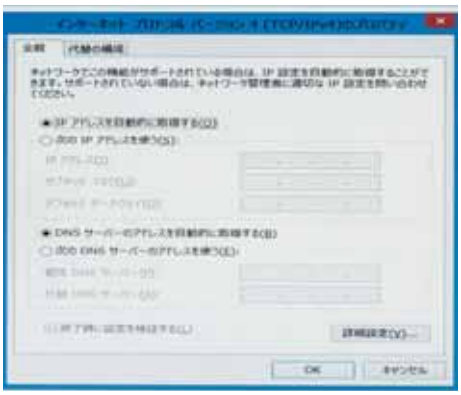
メールサーバには、クライアントから送信されるメールを管理する送信サーバと、サーバに保存されているメールをクライアントが受信できるようにする受信サーバがあります。
送信サーバは、設定ファイル内で指定したドメイン名のメールをスプールします。（スプールとは、送信されたメールを自身のフォルダ内へと保存すること）
ドメイン名の指定に誤りがあると、メールをスプールしません。文字列の入力には十分注意してください。

⑪ クライアント PC の設定

課題１において、ネットワーク構成にクライアントPCは接続されていないが、クライアントPCを接続して動作確認を行う。

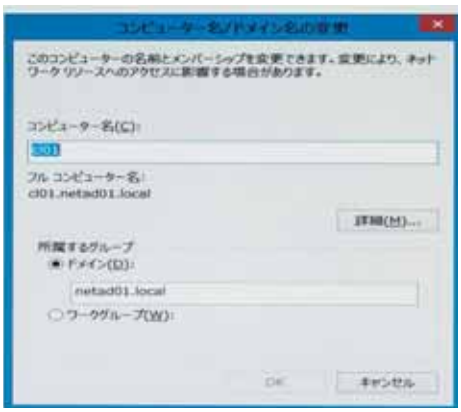


⑪－１　TCP/IP の設定



「コントロール パネル¥ネットワークとインターネット¥ネットワークと共有センター」から、『アダプターの設定の変更』をクリックし、コンピュータのIPアドレスを変更する。

⑪－２　ドメイン参加の設定



「Windowsキー」と「Pause/Break」を同時に押し、「設定の変更」、「変更」と進み、ドメイン名を入力する。ドメイン名入力後、Active DirectoryサーバのAdministratorユーザのパスワードを入力する。

アドバイス

サーバでのサービス設定も大事なことですが、動作確認のほぼ全てをクライアント PC で行います。動作確認ができなければ、点数を取ることは難しくなります。クライアント PC への IP アドレスの割り当て、ホスト名の変更、ドメイン参加など、忘れないように注意してください。特に各サーバへの通信は必ずできるようにしておきましょう。

［2］ネットワーク構築

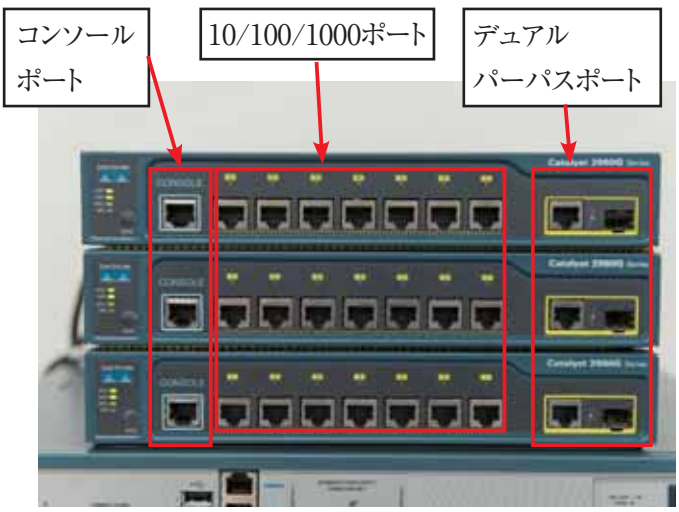
①－１　ネットワーク機器接続表

各ネットワーク機器のインターフェースの接続先は次の通りである。

機器	ホスト名	インターフェース	接続先
ルータ１	R1	Fa0/0	アクセス回線1
		Fa0/1	スイッチ１
ルータ２	R2	Fa0/0	アクセス回線2
		Fa0/1	スイッチ２
		Se0/0/0	ルータ３
ルータ３	R3	Fa0/0	スイッチ１
		Fa0/1	スイッチ３
		Se0/0/0	ルータ２
スイッチ１	SW1	Gi0/1-Gi0/2	サーバ３
		Gi0/3	サーバ１（サーバ１のeth0）
		Gi0/4-Gi0/6	－
		Gi0/7	ルータ１
		Gi0/8	ルータ３
スイッチ２	SW2	Gi0/1-Gi0/6	－
		Gi0/7	サーバ２（サーバ１のeth1）
		Gi0/8	ルータ２
スイッチ３	SW3	Gi0/1-Gi0/7	－
		Gi0/8	ルータ３

・インターフェース記号　Fa:FastEthernet、Gi:GigabitEthernet、Se:Serial
・接続先の「－」はネットワーク機器接続未指定ポートを指す。
・接続先の「アクセス回線１、２」は、各競技エリアまで敷いているLANケーブルを指す。

ルータ、スイッチ全体概観



①－２　インターフェース設定表

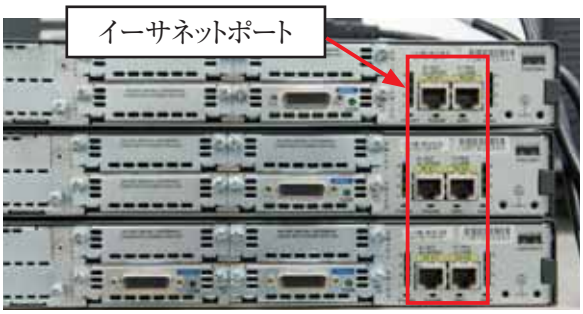
各ネットワーク機器インターフェースの設定値は、次の通りである。

・インターフェースIPアドレスの設定　　（XXは座席番号の数字とする）

機器	ホスト名	インターフェース	IPアドレス
インターネット側参考情報		アクセス回線１	160.250.XX.254/29
		アクセス回線２	170.250.XX.254/29
ルータ１	R1	Fa0/0	160.250.XX.254/29
		Fa0/1	スイッチ１に接続される各サブネットのブロード キャストアドレス-3のアドレス
ルータ２	R2	Fa0/0	170.250.XX.253/29
		Fa0/1	スイッチ２に接続される各サブネットのブロード キャストアドレス-1のアドレス
		Se0/0/0	10.1.0.6/30
ルータ３	R3	Fa0/0	スイッチ１に接続される各サブネットのブロード キャストアドレス-2のアドレス
		Fa0/1	スイッチ３に接続される各サブネットのブロード キャストアドレス-1のアドレス
		Se0/0/0	10.1.0.5/30
スイッチ１	SW1	VLan100	10.1.100.250/24
スイッチ２	SW2	VLan10	172.16.1.250/24
スイッチ３	SW3	VLan10	192.168.1.250/24

・インターフェース記号 Fa:FastEthernet、Gi:GigabitEthernet、Se:Serial
VLanX:Virtual LAN with id X

なお、VLANに接続するルータのインターフェースにはVLAN IDと一致するサブインターフェースを使用する。



各種ケーブル

② ルータの設定

②－１　R1、R2、R3 のホスト名、IP アドレス設定

ホスト名とIPアドレスの設定を行う。
IPアドレス設定は、設定するインターフェースを指定し、「ip address [IPアドレス] [ネットマスク]」を入力する。
物理インターフェースは、デフォルトで「shutdown」された状態になっているため、通信できない。「no shutdown」とすることで、通信可能な状態へと変更できる。

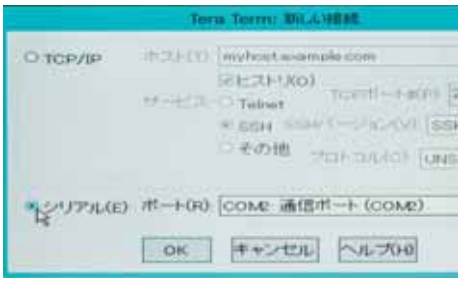
設定リスト

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 160.250.1.253 255.255.255.248
R1(config-if)#no shutdown
R1(config-if)#interface FastEthernet0/1.100
R1(config-if)#encapsulation dot1Q 100
R1(config-if)#ip address 10.1.100.252 255.255.255.0
R1(config-if)#interface FastEthernet0/1.200
R1(config-if)#encapsulation dot1Q 200
R1(config-if)#ip address 10.1.200.252 255.255.255.0

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 170.250.1.253 255.255.255.248
R2(config-if)#interface FastEthernet0/1.10
R2(config-if)#encapsulation dot1Q 10
R2(config-if)#ip address 172.16.1.254 255.255.255.0
R2(config-if)#interface FastEthernet0/1.20
R2(config-if)#encapsulation dot1Q 20
R2(config-if)#ip address 172.16.2.254 255.255.255.0
R2(config-if)#interface FastEthernet0/1.100
R2(config-if)#encapsulation dot1Q 100
R2(config-if)#ip address 172.16.100.254 255.255.255.0

Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#interface FastEthernet0/0.100
R3(config-if)#encapsulation dot1Q 100
R3(config-if)#ip address 10.1.100.253 255.255.255.0
R3(config-if)#interface FastEthernet0/0.200
R3(config-if)#encapsulation dot1Q 200
R3(config-if)#ip address 10.1.200.253 255.255.255.0
R3(config-if)#interface FastEthernet0/1.10
R3(config-if)#encapsulation dot1Q 10
R3(config-if)#ip address 192.168.1.254 255.255.255.0
R3(config-if)#interface FastEthernet0/1.20
R3(config-if)#encapsulation dot1Q 20
R3(config-if)#ip address 192.168.2.254 255.255.255.0
```

ノートパソコンからTera Termを起動させルータ、スイッチの設定を行う。



POINT

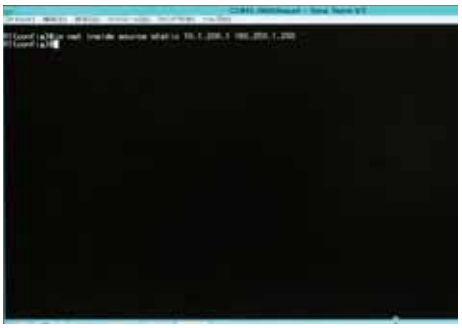
IP アドレスの入力には細心の注意を払うこと。
ここで間違えると、通信不良の原因となる。

②ー２　スタティック NAT 設定

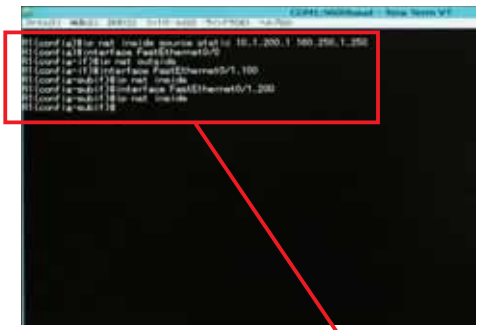
・サーバ１をインターネットと相互接続可能とするために、ルータ１にて160. 250.XX. 250（160.250.01.250）にNATする。
・サーバ２をインターネットと相互接続可能とするために、ルータ２にて170. 250.XX.250（170.250.01.250）にNATする。

用語解説

スタティック NAT は、内部側の IP アドレスとインターネット側の IP アドレスを一対一で変換する機能。インターネット側から、インターネット側の IP アドレスにアクセスすると、ルータで IP アドレスを変換し、内部側の IP アドレスを持つ PC へとアクセスする。主に、社内のサーバにインターネットからアクセスできるようにするために用いられる。



「ip nat inside [内部側のIPアドレス] [インターネット側のIPアドレス]」
（ip nat inside source static 10.1.200.1 160.250.1.250）を入力



POINT

内部側とインターネット側のインターフェースにスタティック NAT の適用を忘れないこと。

設定リスト

```
R1(config)#ip nat inside source static 10.1.200.1 160.250.1.250

R1(config)#interface FastEthernet0/0
R1(config-if)#ip nat outside
R1(config-if)#interface FastEthernet0/1.100
R1(config-if)#ip nat inside
R1(config-if)#interface FastEthernet0/1.200
R1(config-if)#ip nat inside
```

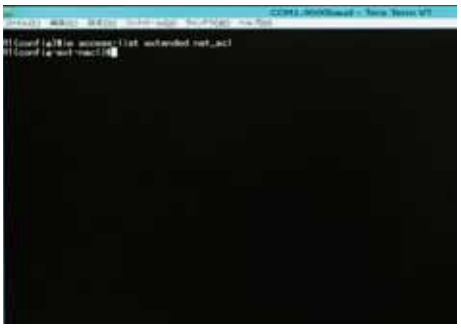
②ー３　NAPT 設定

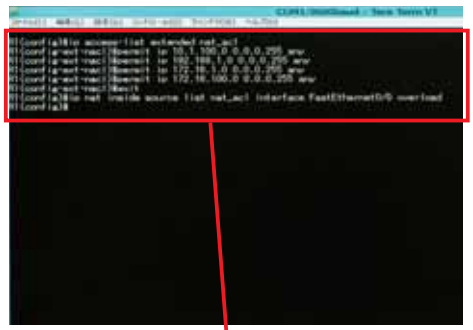
・本社端末（所属VLAN名: Client1、Server）がアクセス回線１経由でインターネット接続できるようにルータ１にNAPTを設定する。また、支社端末（所属VLAN名:ClientBr1、DMZBr）もアクセス回線２障害時のバックアップ経路としてアクセス回線１経由でインターネット接続できるようにルータ１にNAPTを設定する。使用するグローバルアドレスはルータ１のFa0/0に設定されているアドレスとする。

・支社端末（所属VLAN名：ClientBr1）がアクセス回線２経由でインターネット接続できるようにルータ２にNAPTを設定する。

用語解説

NAPT は、多数の内部側 IP アドレスを一つのインターネット側の IP アドレスへと変換する機能。
主に、社内のクライアントがインターネットへアクセスするために用いられる。





設定方法は、アクセスリストを作成し、変換対象となるネットワークを指定する。その後、作成したアクセスリストと変換後のIPアドレス（今回はインターネット側のインターフェースのIPアドレスとした）を指定する。

設定リスト

```
R1(config)#ip access-list extended nat_acl
R1(config-ext-nacl)#permit ip 10.1.100.0 0.0.0.255 any
R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any
R1(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 any
R1(config-ext-nacl)#permit ip 172.16.100.0 0.0.0.255 any
R1(config-ext-nacl)#exit
R1(config)#ip nat inside source list nat_acl interface FastEthernet0/0 overload
```

アドバイス

スタティック NAT の設定は、Interface への "ip nat [inside/outside]" が設定されなければ適用されません。また、NAPT でのアドレス変換の対象ネットワークは、登録しているネットワークのみとなります。変換対象のネットワークに漏れが無いようにしましょう。

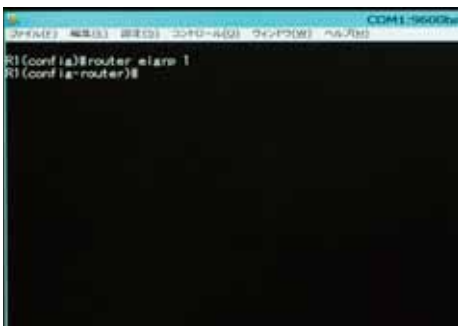
③ルーティング

・本社・支社の各ルータ間で経路交換を行い、全てのネットワークで通信可能とする。ルーティングプロトコルとしてEIGRPを使用する。
・インターネット側（VPN回線除く）およびスイッチ２・スイッチ３へ経路情報を流さないこと。
・本社ネットワーク⇔支社ネットワーク間の通信において、プライマリ経路としてVPN回線を使用し、VPN回線障害時のバックアップ経路としてシリアル回線を使用するようにメトリックを調整すること。

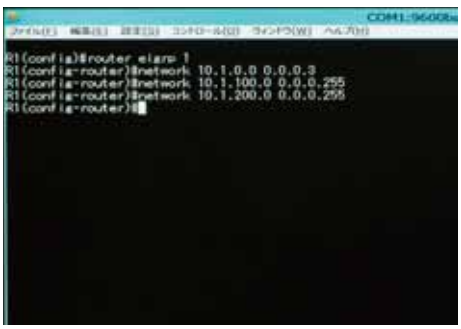
上記の経路切り替えが高速に行えるように、ルータ３のEIGRPトポロジーテーブルには、スイッチ２に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。同様に、ルータ２のEIGRPトポロジーテーブルには、スイッチ１・スイッチ３に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。

用語解説

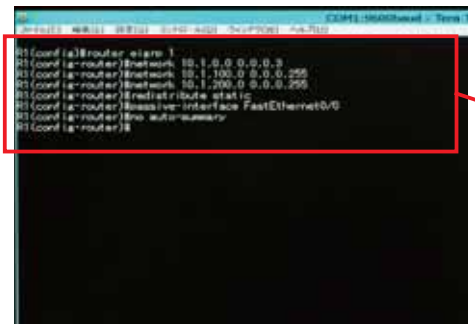
・経路情報とは、パケットをどの相手に送信するかを判断する情報のこと。経路情報にないネットワークへは通信することができない。
・メトリックとは、同ネットワークへの経路情報の優先順位を決める値のこと。
・メトリックの計算方法は、各ルーティングプロトコルによってさまざまである。
EIGRP　…… 帯域幅と遅延
OSPF …… コスト（コスト＝100 / 帯域幅 [Mbps] ）
RIP …… ホップ数（中継するルータの数）
・ルーティングプロトコルとは、複数のルータ間でお互いの経路情報を交換し合い、通信ができるようにする通信プロトコル。



「network [ネットワークアドレス] [ワイルドカード]」を設定することで、ルーティングプロトコルが有効となる。



[ネットワークアドレス]には、ルータ自身が持つIPアドレスのネットワークを指定する。



ルータR1、R2、R3の設定。

設定リスト

```
R1(config)#router eigrp 1
R1(config-router)#network 10.1.0.0 0.0.0.3
R1(config-router)#network 10.1.100.0 0.0.0.255
R1(config-router)#network 10.1.200.0 0.0.0.255
R1(config-router)#redistribute static
R1(config-router)#passive-interface FastEthernet0/0
R1(config-router)#no auto-summary

R2(config)#router eigrp 1
R2(config-router)#network 10.1.0.0 0.0.0.3
R2(config-router)#network 10.1.0.4 0.0.0.3
R2(config-router)#network 172.16.1.0 0.0.0.255
R2(config-router)#network 172.16.2.0 0.0.0.255
R2(config-router)#network 172.16.100.0 0.0.0.255
R2(config-router)#redistribute static
R2(config-router)#passive-interface FastEthernet0/0
R2(config-router)#passive-interface FastEthernet0/1
R2(config-router)#passive-interface FastEthernet0/1.10
R2(config-router)#passive-interface FastEthernet0/1.20
R2(config-router)#passive-interface FastEthernet0/1.100
R2(config-router)#no auto-summary

R3(config)#router eigrp 1
R3(config-router)#network 10.1.0.4 0.0.0.3
R3(config-router)#network 10.1.100.0 0.0.0.255
R3(config-router)#network 10.1.200.0 0.0.0.255
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.2.0
R3(config-router)#passive-interface FastEthernet0/0
R3(config-router)#passive-interface FastEthernet0/1
R3(config-router)#passive-interface FastEthernet0/1.10
R3(config-router)#passive-interface FastEthernet0/1.20
R3(config-router)#no auto-summary
```

アドバイス

ルーティングは通信において重要な設定となります。ルータにIPアドレスを登録した後、ルーティング設定をすると設定のミスは少ないと思います。
この競技課題では、ルーティングプロトコルとしてEIGRPを使用していますが、その他にRIPやOSPFといったルーティングプロトコルもあります。これらも勉強しておくといいと思います。

④ アクセスコントロールリスト（ＡＣＬ）

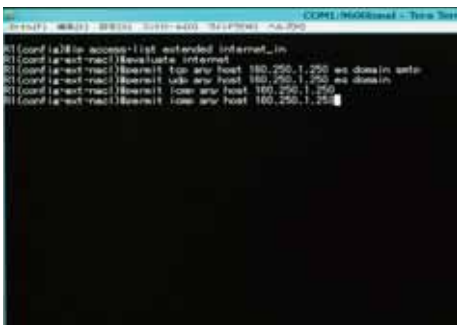
④－１　ルータ１に以下の条件を満たすアクセス制御を設定する。

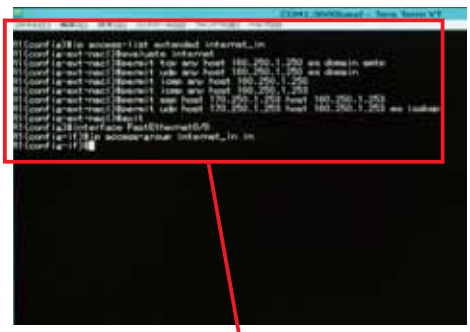
●インターネットからのアクセスについて
- サーバ１に対してはDNSサービス、SMTPサービスおよびICMPのみ通信を許可する。
- ルータ１自身に対する ICMPを許可する。
- ルータ２とのVPN回線のトラフィックは全て許可する。
- 上記以外は許可しない。

●社内からインターネットへのアクセスについて
- サーバ１からインターネットへのアクセスは全ての通信を許可する。
- NAPTでのインターネットアクセスは全ての通信を許可する。
- 上記以外は許可しない。

用語解説

ACL はルータに到達したパケットを制限するフィルタ機能。
許可したパケットはルータを通過し、拒否したパケットは破棄される。





アクセスコントロールリストを設定することで、ルータが受け取った特定のパケットを拒否ことができる。
これにより、インターネットからの不正アクセスを防御することができる。アクセスリストに、許可するパケットか拒否するパケットかを指定する。（許可はpermit、拒否はdenyを指定）
アクセスリスト内でマッチしないパケットは、すべて拒否される。「[permit/deny] [プロトコル] [送信元IPアドレス] [宛先IPアドレス] ([宛先ポート])」

POINT

課題の仕様を満たす上で、許可しなければならないパケットを拒否してしまった場合、大きな減点につながる。
通信制限の設定は、より慎重に行う必要がある。

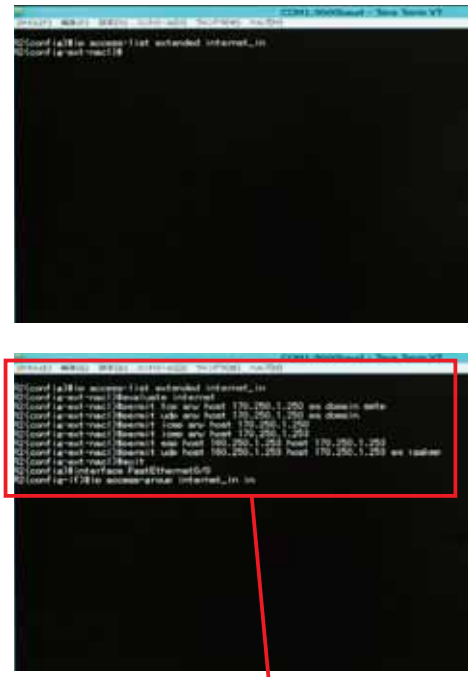
注：下記リストは設定例であり、競技課題の仕様を満たすにはより詳細な設定を行わなければならない。

設定リスト

```
R1(config)#ip access-list extended internet_in
R1(config-ext-nacl)#evaluate internet
R1(config-ext-nacl)#permit tcp any host 160.250.1.250 eq domain smtp
R1(config-ext-nacl)#permit udp any host 160.250.1.250 eq domain
R1(config-ext-nacl)#permit icmp any host 160.250.1.250
R1(config-ext-nacl)#permit icmp any host 160.250.1.253
R1(config-ext-nacl)#permit esp host 170.250.1.253 host 160.250.1.253
R1(config-ext-nacl)#permit udp host 170.250.1.253 host 160.250.1.253 eq isakmp
R1(config-ext-nacl)#exit

R1(config)#interface FastEthernet0/0
R1(config-if)#ip access-group internet_in in
```

④－２　ルータ２にも同様にアクセス制御を設定する。



インターネットからの不正アクセスを防ぐため、ルータ２にもアクセスコントロールリストを設定する。
④-1とは、宛先IPアドレスが異なるため注意が必要である。

POINT

ルータ１と同様のアクセス制御設定だが、送信元アドレスや宛先アドレスには十分注意して設定を行うこと。

注：下記リストは設定例であり、競技課題の仕様を満たすにはより詳細な設定を行わなければならない。

設定リスト

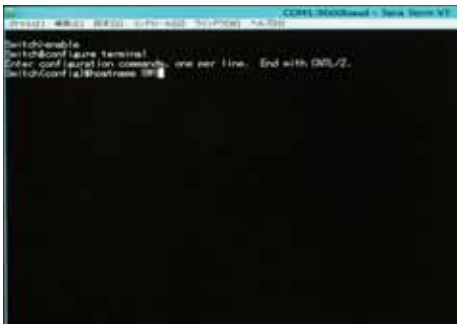
```
R2(config)#ip access-list extended internet_in
R2(config-ext-nacl)#evaluate internet
R2(config-ext-nacl)#permit tcp any host 170.250.1.250 eq domain smtp
R2(config-ext-nacl)#permit udp any host 170.250.1.250 eq domain
R2(config-ext-nacl)#permit icmp any host 170.250.1.250
R2(config-ext-nacl)#permit icmp any host 170.250.1.253
R2(config-ext-nacl)#permit esp host 160.250.1.253 host 170.250.1.253
R2(config-ext-nacl)#permit udp host 160.250.1.253 host 170.250.1.253 eq isakmp
R2(config-ext-nacl)#exit
R2(config)#interface FastEthernet0/0
R2(config-if)#ip access-group internet_in in
```

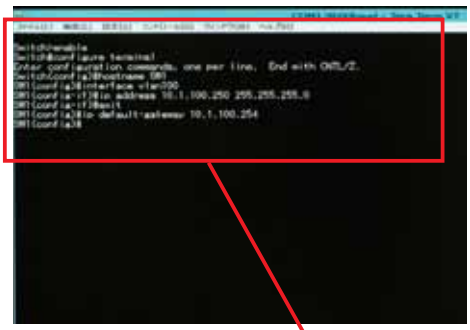
アドバイス

ACL はインターネットからのアクセスを制御し、セキュリティを高めるための設定です。
ここでは許可する通信、拒否する通信に間違いがないか、確実に設定してください。もし、Web アクセスを許可する設定を誤って拒否した場合、ACL の減点だけではなく、Web アクセスの動作確認ができないと判断されます。たとえ Web サーバの設定が合っていたとしても、動作確認ができなければ、Web サーバでも減点されることになります。
また、ACL を間違えてしまうと、通信できる必要のあるサービスに通信ができなくなったり、通信できてはならないサービスに通信できたりと、セキュリティが低くなります。

⑤ スイッチの設定

⑤ー１　スイッチ１、２、３のホスト名、IP アドレス、デフォルトゲートウェイ等の基本設定





ルータ同様、スイッチにもホスト名とIPアドレスを設定する。
スイッチにはVLANに対してIPアドレスを割り当てることができる。IPアドレスを設定した場合、デフォルトゲートウェイのIPアドレスを設定するのが一般的である。

POINT

スイッチのデフォルトゲートウェイ設定を忘れないよう気を付けること。他ネットワークへの通信も意識して設定を行うこと。

設定リスト

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#hostname SW1
SW1(config)#interface Vlan100
SW1(config-if)#ip address 10.1.100.250 255.255.255.0
SW1(config-if)#exit
SW1(config)#ip default-gateway 10.1.100.254

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#hostname SW2
SW2(config)#interface Vlan10
SW2(config-if)#ip address 172.16.1.250 255.255.255.0
SW2(config-if)#exit
SW2(config)#ip default-gateway 172.16.1.254

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#hostname SW3
SW3(config)#interface Vlan10
SW3(config-if)# ip address 192.168.1.250 255.255.255.0
SW3(config-if)#exit
SW3(config)#ip default-gateway 192.168.1.254
```

⑤－２　スイッチの VLAN 設定

スイッチ１

VLAN番号	VLAN名	割付ポート	サブネット	用途
100	Server	Gi0/1-Gi0/2	10.1.100.0/24	内部向けサーバ セグメント
200	DMZ	Gi0/3	10.1.200.0/24	本社DMZセグメント

※ゲートウェイアドレスは、各サブネットのブロードキャストアドレス-1のアドレスとする。

スイッチ２

VLAN番号	VLAN名	割付ポート	サブネット	用途
10	ClientBr1	Gi0/1-Gi0/2	172.16.1.0/24	支社クライアント セグメント
20	CliantBr2	Gi0/3-Gi0/4	172.16.2.0/24	支社クライアント セグメント
100	DMZBr	Gi0/7	172.16.100.0/24	支社DMZセグメント

※ ゲートウェイアドレスは、各サブネットのブロードキャストアドレス-1のアドレスとする。
※ VLAN ClientBr2は直接的なインターネット接続は許可しないセグメントとする。

スイッチ３

VLAN番号	VLAN名	割付ポート	サブネット	用途
10	Client1	Gi0/1-Gi0/2	192.168.1.0/24	本社クライアント セグメント
20	Client2	Gi0/3-Gi0/4	192.168.2.0/24	本社クライアント セグメント

※ ゲートウェイアドレスは､各サブネットのブロードキャストアドレス-1のアドレスとする。
※ VLAN Client2は直接的なインターネット接続は許可しないセグメントとする。

用語解説

VLAN は、Virtual LAN（仮想 LAN）の略称で、スイッチ内で、ネットワークを分割するために用いる機能。

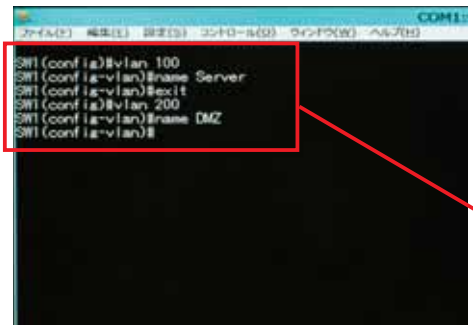
【VLAN の設定】

一つのスイッチでネットワークを分けることで、ポートを効率よく使用することができる。

VLAN番号を登録し、VLANごとに名前を付ける。

POINT

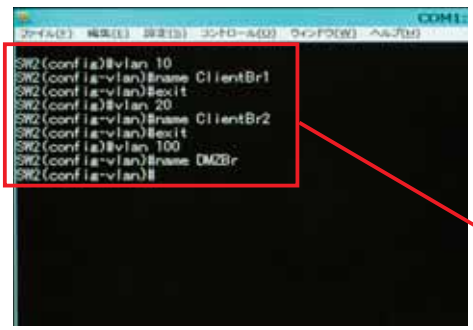
VLAN 番号ごとにネットワークを分割することができる。同じ VLAN 番号を割り当てたポートは同じネットワークに所属する。



それぞれ設定する場合、スイッチ１、２、３のポートにケーブルを差す。

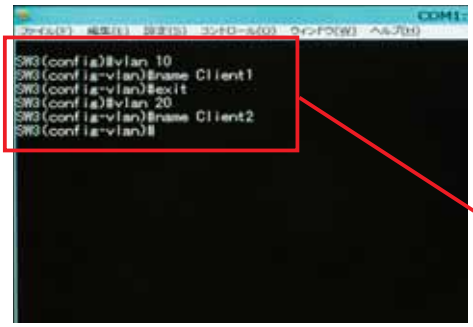
設定リスト

```
SW1(config)#vlan 100
SW1(config-vlan)#name Server
SW1(config-vlan)#exit
SW1(config)#vlan 200
SW1(config-vlan)#name DMZ
```



設定リスト

```
SW2(config)#vlan 10
SW2(config-vlan)#name ClientBr1
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#name ClientBr2
SW2(config-vlan)#exit
SW2(config)#vlan 100
SW2(config-vlan)#name DMZBr
```



設定リスト

```
SW3(config)#vlan 10
SW3(config-vlan)#name Client1
SW3(config-vlan)#exit
SW3(config)#vlan 20
SW3(config-vlan)#name Client2
```

アドバイス

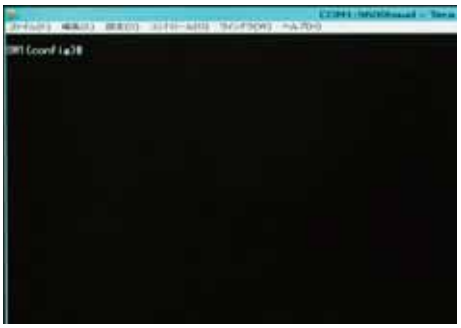
VLAN はスイッチ内でブロードキャストドメインを分割することで、複数のネットワークをスイッチ１台で扱うことができる機能です。通信設定において非常に重要な設定となります。VLAN の設定を理解することで、ネットワーク構成の理解が速くなります。

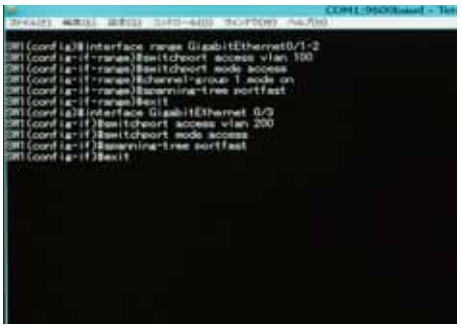
⑤ー３　スイッチ各種設定

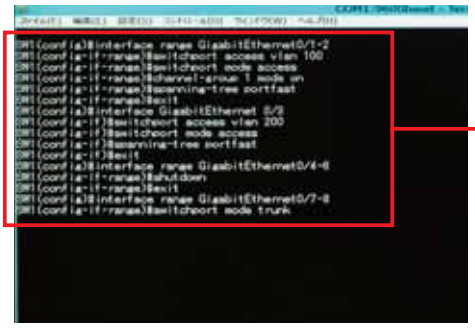
・スイッチ－ルータ間を接続しているリンクは802.1Qのトランクリンクとする。
・各スイッチにおいて機器を接続する予定がないポート（VLAN割付ポートとルータ接続ポートを除く全ポート）は閉塞する。

用語解説

・通常、VLAN によりネットワークを分割することで、VLAN 間での通信はできなくなる。しかし、ルータを介することで、通信ができるようになる。これは VLAN 間ルーティングと呼ばれる。
・閉塞とは、ポートを閉じる設定のこと。つまり、「shutdown」状態にすることを指す。
・トランクリンク（トランクポート）とは、複数の VLAN を一つのポートで通信できるようにする機能のこと。







VLAN間ルーティングを可能にするために、スイッチ－ルータ間をトランクリンクに設定する必要がある。
使用する予定のないポートは、閉塞することで、誤って使用される恐れがなくなり、安全性を高めることができる。

POINT

通常のアクセスポートでは、一つの VLAN しか通信はできない。アクセスポートはクライアント用ポート、トランクポートはスイッチやルータ間に設定することが一般的である。

設定リスト

```
SW1(config)#interface range GigabitEthernet0/1-2
SW1(config-if-range)#switchport access vlan 100
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#channel-group 1 mode on
SW1(config-if-range)#spanning-tree portfast
SW1(config-if-range)#exit
SW1(config-if)#interface GigabitEthernet0/3
SW1(config-if)#switchport access vlan 200
SW1(config-if)#switchport mode access
SW1(config-if)#spanning-tree portfast
SW1(config-if)#exit
SW1(config-if)#interface range GigabitEthernet0/4-6
SW1(config-if-range)#shutdown
SW1(config-if-range)#exit
SW1(config-if)#interface range GigabitEthernet0/7-8
SW1(config-if-range)#switchport mode trunk
```

アドバイス

スイッチはルータ同様、通信するために重要な機器です。スイッチとルータの役割の違いをしっかりと理解してください。
VLAN の仕組みについて理解できていなければ、ネットワーク構成を理解することは難しくなります。

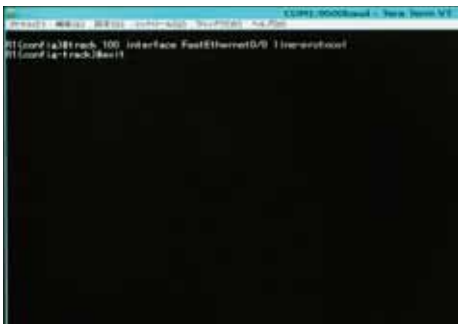
⑥ 障害対策１（ゲートウェイの冗長化）

ルータ１とルータ３間にVRRPを設定し、スイッチ１のVLAN100、200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する。

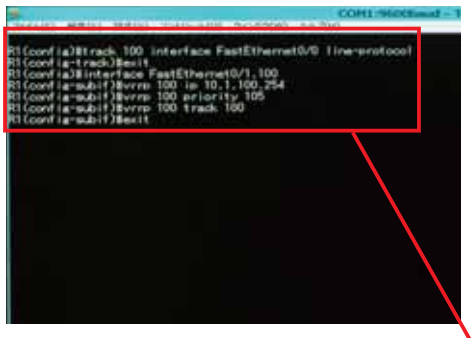
・ルータ１をマスタルータとする。
・ルータ１においてアクセス回線１がリンクダウンした場合、マスタルータがルータ３に切り替わるようにする。アクセス回線１が復旧した場合、マスタルータがルータ１に切り戻すこと。

用語解説

冗長化とは、メインで動作している機器に障害が発生した場合、そのメイン機器と同じ動作をする機器をバックアップとして代わりに動作させることをいう。ゲートウェイの冗長化用プロトコルの一つに VRRP がある。



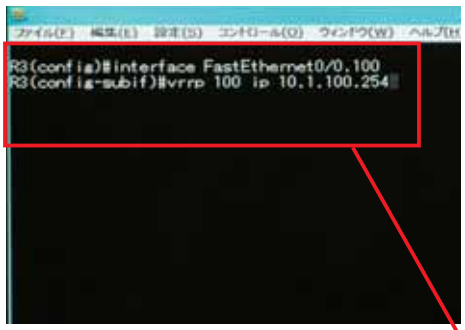
２台以上のルータをVRRPグループに追加する。VRRPグループに、共有して使用するIPアドレスを一つ持たせる。これにより、共有しているIPアドレスをデフォルトゲートウェイにすることで、ルータに障害が発生した場合でも、クライアントは設定を変更することなく、通信できる状態を保つことができる。
クライアントは一つのIPアドレスに対して通信を行っているが、実際のパケットは、VRRPグループ内の一つのルータに対して送信されている。



VRRPグループ内のどのルータが応答するかを決めるために「priority」の設定を行う。「priority」の高いルータほど優先して応答する。

POINT

マスタルータ（ルータ 1）で通信不良が発生した場合、バックアップルータ（ルータ 3）に切り替わり、社内への通信を確保できる。



設定リスト

```
R1(config)#track 100 interface FastEthernet0/0 line-protocol
R1(config-track)#exit
R1(config)#interface FastEthernet0/1.100
R1(config-subif)#vrrp 100 ip 10.1.100.254
R1(config-subif)#vrrp 100 priority 105
R1(config-subif)#vrrp 100 track 100
R1(cofig-subif)#exit
```

設定リスト

```
R3(config)#interface FastEthernet0/0.100
R3(config-subif)#vrrp 100 ip 10.1.100.254
```

アドバイス

ゲートウェイを冗長化することで、万が一、ルータやスイッチに障害が発生した時でも、別の経路を用いて通信が行えます。

⑦ パスワード

各ネットワーク機器に従って特権モード、コンソール、Telnet（vty0-4）に対してパスワードを設定する。全てのパスワードおよび特権モードパスワードは暗号化する。

用語解説

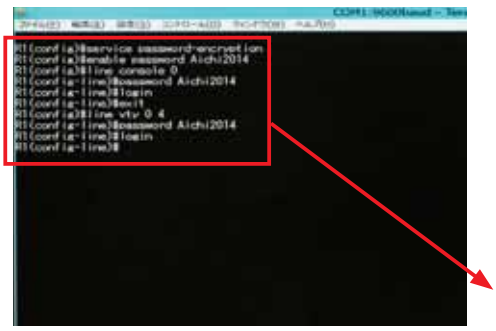
・Enable パスワードは、特権モードへ移行する際に必要なパスワードのこと。
・コンソールパスワードは、コンソールケーブルを使用して、ネットワーク機器を操作する際のパスワード。
・Telnet パスワードは、telnet コマンドを使用してネットワーク機器に接続したときに必要となるパスワードのこと。

パスワードは以下のとおりに設定する。

モード	enable	コンソール	telnet
パスワード	Aichi2014	Aichi2014	Aichi2014

※パスワードの大小文字に注意する。

悪意のあるユーザにネットワーク機器の設定を変更されないよう、パスワードを設定する。
「service password-encryption」を設定することにより、設定ファイルを閲覧した時に、パスワード部分を暗号化し、パスワードが外部に漏れることを防ぐことができる。



POINT

ネットワーク機器を操作する時のパスワードを設定する。誤設定をしてしまうと、操作ができなくなってしまう。
ネットワーク機器だけでなく、パスワードを入力する時は間違えないよう注意する。

設定リスト

```
R1(config)#service password-encryption
R1(config)#enable password Aichi2014
R1(config)#line console 0
R1(config-line)#password Aichi2014
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password Aichi2014
R1(config-line)#login
```

⑧ ネットワーク接続作業

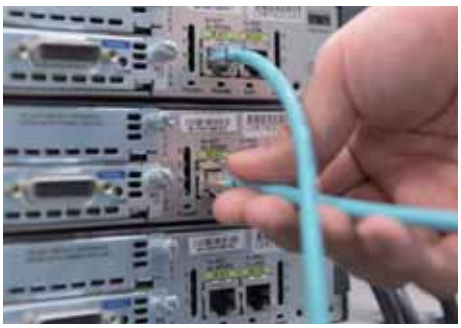
（インストール作業などの空いている時間や動作確認までに接続作業を済ませる。）

⑧－１　ケーブリング

『①－1ネットワーク機器接続表（接続表）』をもとに、各ケーブルを配線・接続する。

作業手順

LANケーブルを接続し、通信できるようにする。
接続表を確認しながら、１本ずつケーブリングを行う。



POINT

配線のミスはトラブルの原因になるため、１本ずつ確かめながら作業を行うこと。

シリアルケーブルを接続する。

配線・接続完了。

⑧－２　シリアル接続

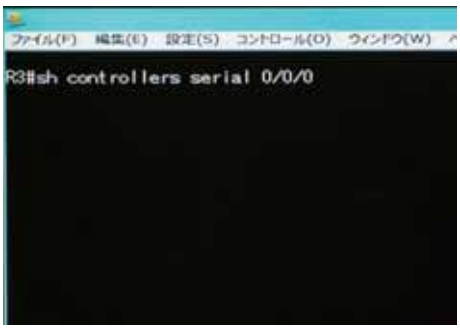
・ルータ３をDCE、ルータ２をDTEとして、シリアルケーブルで接続する。

用語解説

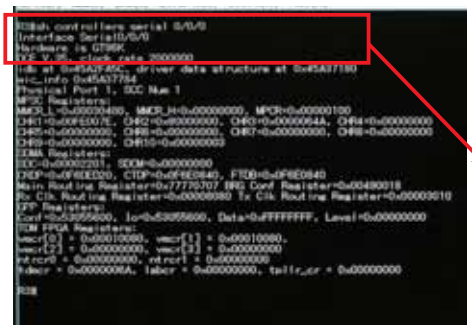
シリアルケーブルは、専用線とも呼ばれている。本社－支社間など、離れた拠点間を接続する場合に用いられることがある。

DCEとDTEは接続部を見て判断する。DCEは穴が開いており、DTEは端子が出ている。

シリアルケーブルは、DCEとDTEを組み合わせて使用する。



R3にDCE、R2にDTEとして、シリアル接続されているか確認する。



左図は、ルータ３に接続されたシリアルケーブルの状態を確認した結果リスト。DCEかDTEのどちら側が接続されたか確認できる。同様にルータ２の接続も確認する。

ルータ3の結果リスト

```
R3#sh controllers serial 0/0/0
DCE V.35, clock rate 200000
```

ルータ2の結果リスト

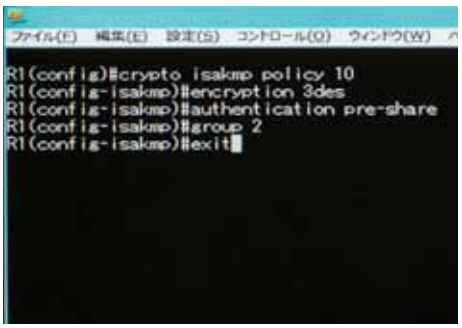
```
R2#sh controllers serial 0/0/0
DTE V.35idb at 0x48F71E94, driver data structure at 0x48F796D8
```

⑧－３　VPN

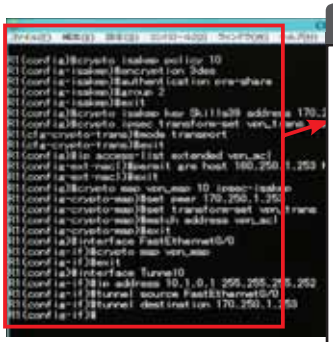
・本社ルータ１と支社ルータ２をインターネット経由でIPsecVPN接続する。その際、ルータ１、ルータ２間に10.1.0.0/30のアドレスを使用し（ルータ１側を若番とする）トンネルインターフェース（GREトンネル）の設定を行う。

用語解説

IPsecVPN とは、IPsec を用いて通信の暗号化を行い、高いセキュリティを実現する VPN 技術のこと。



インターネットVPNを行うことで、プロバイダと契約せず、安価に各拠点で通信が可能になる。
また、IPSecで暗号化を行うことで、拠点間通信の安全性を確保する。



設定リスト

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key Skills39 address 170.250.1.253
R1(config)#crypto ipsec transform-set vpn_trans esp-3des esp-sha-hmac
R1(config-crypto-trans)#mode transport
R1(config-crypto-trans)#exit
R1(config)#ip access-list extended vpn_acl
R1(config-ext-nacl)#permit gre host 160.250.1.253 host 170.250.1.253
R1(config-ext-nacl)#exit
R1(config)#crypto map vpn_map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 170.250.1.253
R1(config-crypto-map)#set transform-set vpn_trans
R1(config-crypto-map)#match address vpn_acl
R1(config)#interface FastEthernet0/0
R1(config-if)#crypto map vpn_map
R1(config-if)#exit
R1(config)#interface Tunnel0
R1(config-if)#ip address 10.1.0.1 255.255.255.252
R1(config-if)#tunnel source FastEthernet0/0
R1(config-if)#tunnel destination 170.250.1.253
```

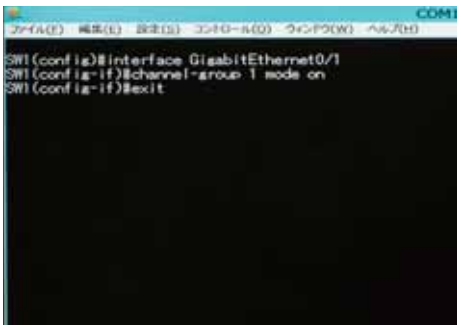
アドバイス

インターフェースへの IP アドレス設定は、同じような数字を入力することが多いため、ケアレスミスが多くなります。通信不良の原因となりますので、入力する時は慎重に確認しましょう。
また、ここでは IPsecVPN 設定を行います。これは、ルータの IOS が更新されたことで設定できるようになりました。設定手順が多く、一つでもミスがあると動作しなくなるため、難易度の高い設定です。

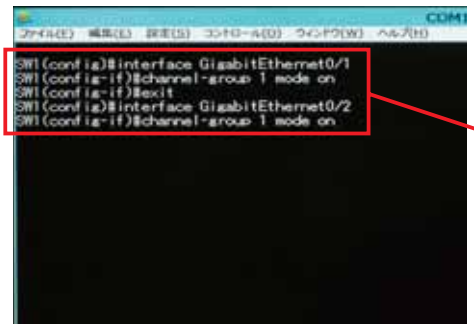
⑨ 障害対策２（ネットワーク回線の冗長化）

LANケーブルは、ネットワーク機器に生じるような装置の故障はないが、人や机などに踏みつけられたり、無理に曲げたりすると断線することがある。こうした事態に備え、スイッチ間を結ぶ回線の冗長化を行う。（スイッチ１とサーバ３間の回線）

サーバとスイッチ間の障害対策として、ネットワーク回線の冗長化がある。
１本のLANケーブルが断線した場合、もう１本のLANケーブルを用いて、通信可能な状態を維持することができる。
Windows Serverでは、NICチーミングという機能を用いることで、実現することができる。



２本以上のLANケーブルで一つのチームを作ることで、サーバは、一つのLANケーブルが接続されているかのように認識する。スイッチには、「channel-group」を設定し、サーバ同様、複数のポートを一つのポートのように認識させる。



設定リスト

```
SW1(config)#interface GigabitEthernet0/1
SW1(config-if)#channel-group 1 mode on
SW1(config-if)#exit
SW1(config)#interface GigabitEthernet0/2
SW1(config-if)#channel-group 1 mode on
```

POINT

通常、PC1 台に対して LAN ケーブルを１本使用して通信を行う。その１本の LAN ケーブルが断線した場合、通信ができなくなる。
重要な通信経路では、このような事態を避けるため、LAN ケーブルを２本以上用いた冗長化を行う。１本の LAN ケーブルが断線しても、もう１本で通信が行えるようにすることで、常に通信できる状態を維持できる。

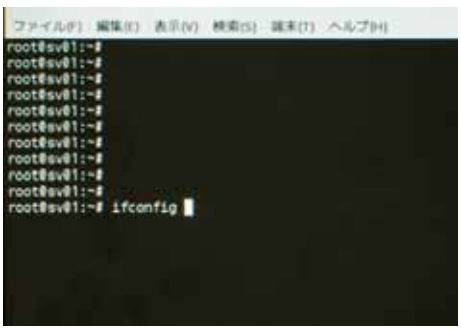
[3] 動作確認

ノートパソコンからネットワークコマンドを使って、接続状況と動作確認を行う。

用語解説

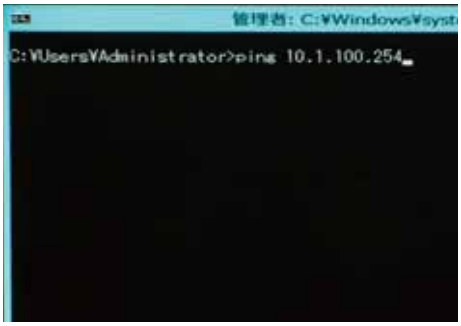
- ・ifconfig　：UNIX 系 OS や Linux で使用されるネットワーク環境の状態確認／設定のためのコマンド
- ・ipconfig　：Windows の TCP/IP ネットワーク設定を確認できるコマンド
- ・ping　：ネットワークの疎通を確認するために使用されるコマンド
- ・route print：ルーティングテーブルの内容表示と設定を行う。
- ・netstat　：コンピュータのネットワーク機能の現在の状態を取得して一覧表示する。
- ・traceroute：ネットワークの経路を調査する。
- ・ARP　：IP アドレスから Ethernet の MAC アドレスの情報を得られるプロトコル
- ・nslookup　：DNS サーバーの設定状態を調べたり、DNS のクライアントにおける DNS 関連の設定を調査したりする場合に利用される。

通信が確立されているか、正常に動作しているかを判断するために各種コマンドを用いる。

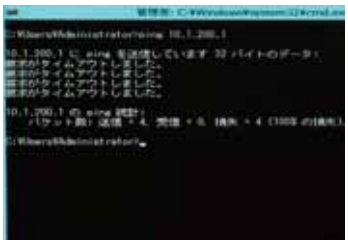


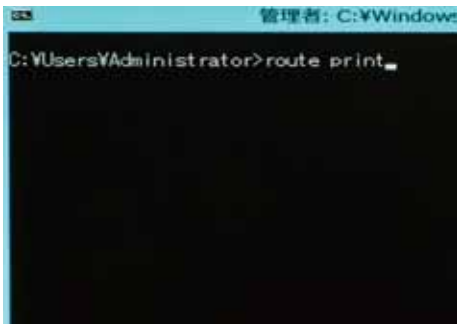
ifconfigのコマンド
IPアドレス、マスクを結果表示

ipconfigのコマンド
IPアドレス、マスク、ゲートウェイの結果表示

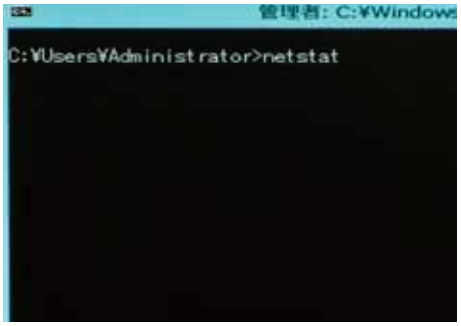


pingのコマンド　各IPアドレスを入力
応答あり　　応答なし

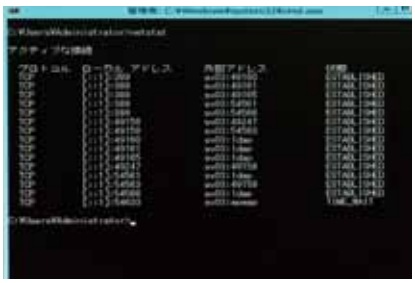




route printのコマンド　結果表示



netstatのコマンド
あるべきものを表示
確認する。
動作していないもの
は表示しない。

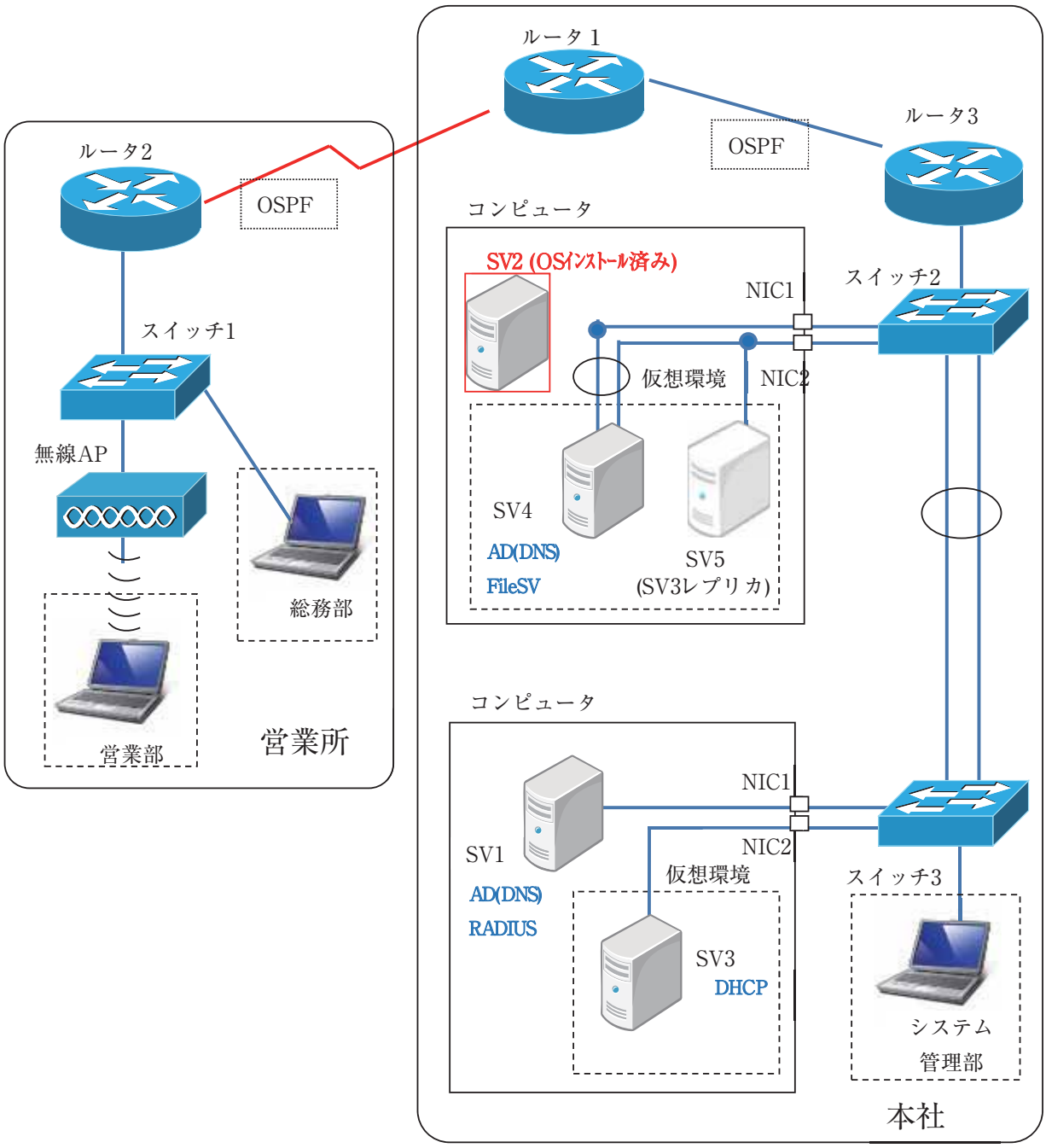


アドバイス

設定しただけでなく、上記の確認コマンドを使用して、正常に動作することを確認しましょう。
一つの設定をした後に、その設定の確認を行うと、ミスの少ない競技課題の構築ができます。

(3) 課題２　ネットワーク構成

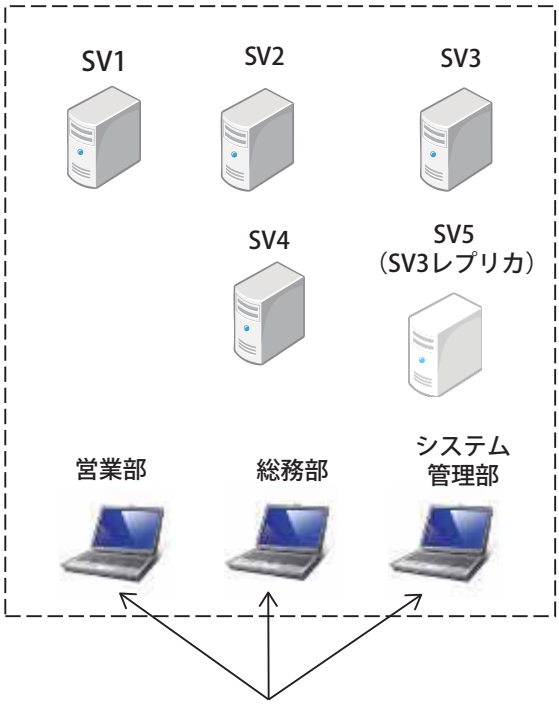
課題２については、本競技で使用する機材・環境及び競技時間・内容を考慮した場合、過去に行われた国内大会での競技課題の内容の詳細について公開することは、今後の競技の運営上好ましくないと考えられるため、非公開とし、課題の概要のみ掲載する。



【競技課題の背景（概要）】

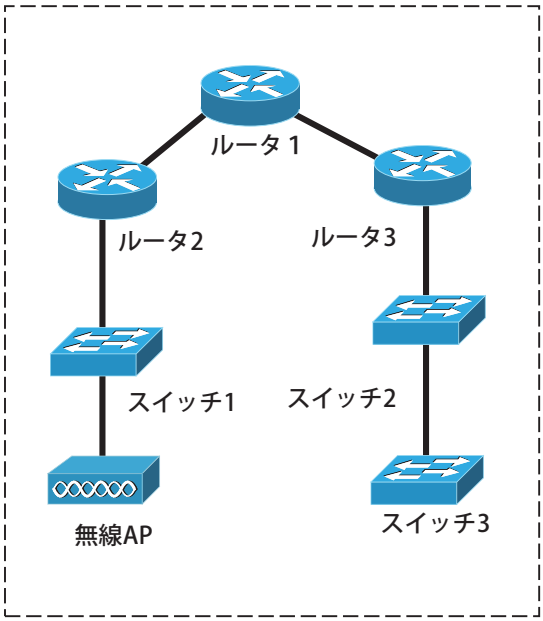
あなたは、㈱シャチホコシステムズのシステム管理部に在籍するエンジニアである。業務拡大のため、新規開設した営業所と本社間のシステムを新規に構築する。今回は、事前検証用のネットワーク及び各種サーバを構築する。

【課題２　サーバとクライアントPC】



機器の設定と動作確認用の
ノートパソコン

【課題２　スイッチングとルータ】



8 期待される取組の成果

ITネットワークシステム管理では、本人の能力や適性を踏まえて技能五輪の競技選手を決定する。同時に将来配属される職場も決められ、配属先が決められることで将来必要となる技能、知識を理解することができ、訓練での目的もより明確になる。

(1) 企業の取組の成果

企業としての目的は職場の核となる人材育成と高度技能の習得としている。目標は金メダル獲得とし、メダルが獲得できなくても、一つでも上を目指し、自分との闘いの中で努力を続けることで大きな成長が得られる。そして、メダルを取って終わりでなく、その後、職場に配属されてからその職場の中心で働くことである。

配属先では、社内の情報インフラを設計・管理する部署やコンピュータシステムを開発・保守をする部署など職場の最前線で活躍している。

(2) 競技者の取組の成果

選手は競技大会に参加することで、技能・知識だけでなく、訓練を通じて身に付けた「忍耐力」「行動力」が養われ、自分の考えがしっかりして、発言や行動に責任を持つようになる。また、周りの人々の助けで支えられていることに感謝し、金メダルを取るとさらに謙虚になるところが大きく変わったと思われる点である。

競技大会で勝つために選手が身につけた技能は、選手のその後の職務(仕事)において大いに役立っている。

例えば、パソコンが動作しない、通信ができないといった職務におけるトラブルが発生した場合、機器の内部がどのように動作しているかを理解しているため、問題解決が早く行える。

(3) 指導者の取組の成果

指導者として、重要視することは選手を思いやり、優しく接することで信頼関係を築き、技能訓練の経験を活かせるようにいかにサポートするかである。当社において、ITネットワークシステム管理職種は、近年、金メダルを取れることが多くなってきており、毎年好成績を出さなければならないというプレッシャーが大きい。OSや機器などの進歩や変化が著しいネットワーク特有の難しさがあり、指導者としても日々勉強を行っている。

巻　末　資　料

（1）技能五輪全国大会「ITネットワークシステム管理」事前公表資料
　　技能全国大会ITネットワークシステム管理職種への参加の手引き（公表用）競技課題概要
　　（2014年第52回大会用）
（2）第52回技能五輪全国大会 ITネットワークシステム管理 1日目競技課題（競技課題1）抜粋

(1) 技能五輪全国大会「ITネットワークシステム管理」事前公表資料

技能五輪全国大会
IT ネットワークシステム管理　職種への
参加の手引き
（公表用）競技課題概要
（2014 年　第 52 回大会用）

平成 26 年 6 月 30 日

競技委員作成

前版からの変更事項は最終ページの履歴に記述していきます。

必ずご確認ください。

１．「IT ネットワークシステム管理」競技概要

企業や一般家庭に設置されている殆どのコンピュータは、ネットワークによって巨大なインターネット網に接続されています。インターネットに接続された企業のサーバシステムには、高い信頼性が求められます。このようなシステムを設計・構築・運用管理するのが「IT ネットワークシステム管理」技術者です。

本職種の技術者には、高い信頼性のあるシステムを構築するための技術と知識が必要となります。またシステムにトラブルが発生した際は、その現象と状況を的確に判断して対処しなければなりません。技術者にはこれまでの経験と知識だけではなく、判断力と想像力も求められます。そこで「IT ネットワークシステム管理」競技では、「信頼性のある ICT・サーバシステムの構築技術」及び「インターネットへの接続も含めた社内ネットワーク構築技術」を競います。

本競技で使用する機材・環境及び競技時間・内容を考慮した場合、過去に行われた国内大会での競技課題のすべてを公開することは、今後の競技の運営上好ましくないと考えられます。ただし、過去の国際大会の課題は公開されておりますので、参考にしてください。国際大会の競技課題入手については、中央職業能力開発協会へお問い合わせください。

２．競技日程

・競技開始の前日

競技内容の説明、競技場所の抽選、機材の確認

・競技 1 日目（競技時間：6 時間）

午前 3 時間、昼休み 1 時間、午後 3 時間

ただし、午前の終了時の指示以降、昼休み時間中は、一切の作業および操作はできませんが、終了指示以前に操作して自動的に行われるインストール等は続けてもかまいません。午後の終了時にインストール途中であれば選手はそれを強制終了する必要はありませんが、インストールの終了は競技時間終了後になるため終了操作はできません。自動的にインストールが終了しない場合は競技委員が強制終了させます。

・競技 2 日目（競技時間：3 時間）

午前 3 時間

終了時の自動インストールに関しては、1 日目の午後の終了時と同じ条件です。

３．競技に使用できる主な機器と支給部品

- （サーバ用）デスクトップ PC（CPU Core2 以上，メモリ 2GB 以上，HDD 80GB 以上を 1 個以上，NIC 1 ポート以上，DVD ドライブ付き） ２式
  サーバ用デスクトップ PC 2 台は切替機でディスプレイ・キーボード共有
- （クライアント用）ノート PC（Windows 7，シリアルポート付き，無線 LAN 付き，TeraTerm インストール済み） １式
- Hub（４ポート以上） １台
- Cisco 製ルータ　2811(Ver.12.4.10C 以降) ３台

- Cisco 製スイッチング Hub　Catalyst 2960G-8TC-L (Version 12.2(35)SE)　３台
- Cisco 製無線 LAN アクセスポイント Air-AP1242AG-P-K9　１台
- LAN ケーブル（　UTP CAT5E、既製品　）　数本
- シリアルケーブル（DCE, DTE）　各２本

Cisco 2811 ルータの IOS Feature Set は IP Base を基本としますが、Advanced IP Services も使用します。

競技委員側で構築する上位サーバとの接続用に L3 スイッチ（WS-C3750-24TS-E）を用意し利用しますが、選手は設定等、直接操作は行えません。

４．競技課題概要

与えられた「競技課題」を読んで、下記の作業を行う。

A．ハードウェアパフォーマンスの最適化のための BIOS 設定等

B．Windows によるサーバと Linux によるサーバの構築およびクライアント PC の設定

- サーバ OS および必要ソフトのインストール
- 各種サーバ(DNS、メール、Web、ファイル共有等)の設定（セキュリティ対策や運用管理も含む）
- 各種アプリケーション（仮想環境構築ソフトウェア、RDB、Web-RDB インターフェーススクリプト）の設定
- ネットワーク接続作業
- クライアント設定

C．ネットワーク構築

- ルーティング設定
- フィルタリングの設定
- ネットワーク接続作業とトラブルの修復
- VLAN の設定
- ネットワーク機器の各種設定、運用管理

５．ソフトウェアのバージョンおよび設定方法

A．日本語環境が設定可能な OS およびアプリケーションは、日本語環境を使用します。

B．サーバ OS は、Windows Server 2012 R2 評価版と Debian GNU/Linux 7.5.0 wheezy とします。

C．ルータの機能として Web 環境での設定が可能な機種であっても、競技中にこの Web 環境でルータの各種設定をすることを禁止します。なお，無線 LAN のアクセスポイントについては Web 環境での設定を禁止しません。

６．採点および評価基準

採点は、与えられた「競技課題」を理解し、要求されたシステムが正確に実現されているかを評価します。配点は「Ａ．ハードウェアパフォーマンスの最適化のための BIOS 設定等」が 10%未満、「Ｂ．Windows によるサーバと Linux によるサーバの構築およびクライアント PC の設定」が 65%未満、「Ｃ．ネットワーク構築」が 50%未満です。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

Ａ．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。

Ｂ．ソフトウェアの持ち込みは一切認めない。

Ｃ．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して１時間後から１時間とする。ただし、ハードウェアに関する質問については随時可能とする。これはハードウェアトラブルが疑われる事態が発生した場合、その対処を優先するためである。

Ｄ．競技終了の合図で、作業を直ちに終了すること。

Ｅ．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。

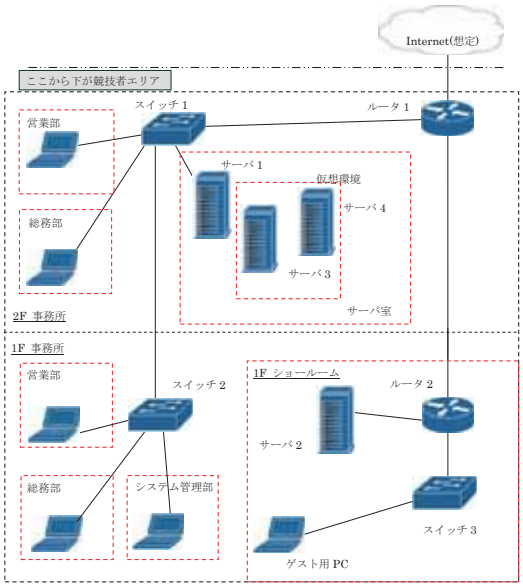
Ｆ．競技中に、トイレ、体調不良などが生じた場合には、その旨を競技委員に申し出て、競技委員の指示に従うこと。

Ｇ．競技中の水分補給のための飲料水の持ち込みは認める。

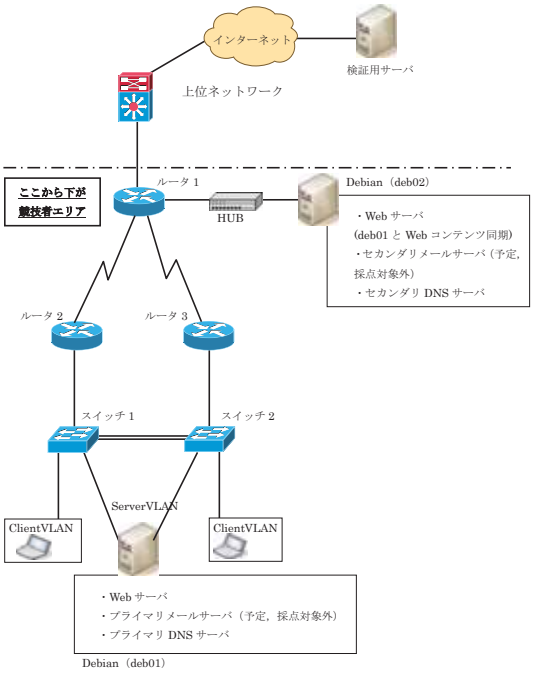
Ｈ．スマートホン等（携帯電話やタブレットも含む）の電源は切っておくこと。

Ｉ．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。

参考資料Ａ　第５１回大会競技課題１日目のネットワーク構成図



参考資料Ｂ　第５１回大会競技課題２日目のネットワーク構成図



第52回　技能五輪全国大会
ITネットワークシステム管理

1日目競技課題（競技課題1）**抜粋**

平成26年11月29日（土）
競技時間：６時間（9:00～12:00,　13:00～16:00）

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は、ネットワーク配線はそのままにしておき、サーバ及びルータ等機器の電源を落としてから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

競技課題の背景

あなたはネットワークシステムの構築を専門とする企業のエンジニアである。ある企業のネットワークシステムの更改業務を受注し、そのプロジェクトマネージャとなった。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。

競技課題1

以降の注意事項と競技課題を読み、検証用システムを構築しなさい。

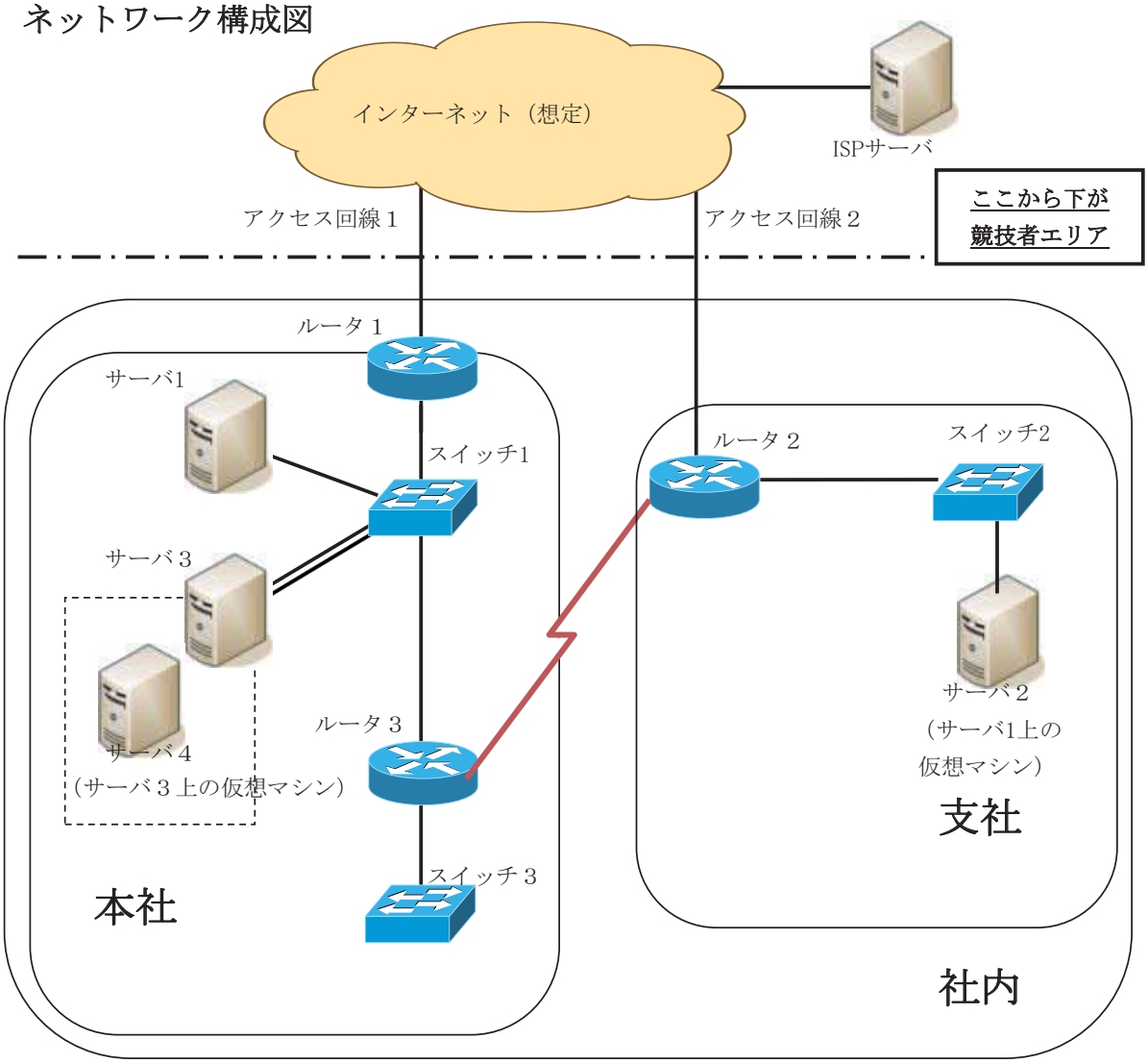
競技課題に関する注意事項

- ✓ 競技終了時に指定された配線接続になっていること。
- ✓ 競技終了時に指定された設定がネットワーク装置の NVRAM に保存されていること。全てのハードウェアは採点前に再起動される。
- ✓ **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。**
- ✓ ネットワーク構成図における「インターネット（想定）」は、「L3 スイッチ」および「ISP サーバ」で構成される。これは競技委員が用意する「仮想的なインターネットエリア」であり、「社内」以外の全てのネットワークエリアを指すものとする。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。
- ✓ 競技課題中の「社内」とは、ネットワーク構成図における「本社」および「支社」内の全てのプライベートアドレスセグメントを指すものとする。また，「本社内」とは、ネットワーク構成図における「本社」内の全てのプライベートアドレスセグメントを指すものとする。「支社内」とは、ネットワーク構成図における「支社内」内の全てのプライベートアドレスセグメントを指すものとする。
- ✓ 各競技エリアには「外部ネットワーク」(L3 スイッチ)とつながる LAN ケーブルが 2 本敷設されている。アクセス回線 1 とアクセス回線 2 の区別があるため適切に接続すること。
- ✓ ISP サーバ（検証用サーバ２00.99.1.1）の機能
  インターネット（想定）上にISPサーバ（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。必要に応じて各競技者エリアまで敷いてあるLANケーブルを通してアクセスしてよい。

  - DNS、Web サーバ、Mail(SMTP)サーバが稼働している。

その他の詳細な設定内容は、構成図や設問に記載する。

ネットワーク構成図



構築を行うネットワークの仕様概要は以下の通りとする。
社内で４台のサーバを構築する。サーバ１は本社DMZ、サーバ２は支社DMZに設置して社内外に対してサービスを提供する。サーバ３とサーバ４は本社に設置して、社内に対してサービスを提供する。今回、物理サーバが2台しか用意出来なかったため、サーバ２はサーバ１上の仮想マシン、サーバ４はサーバ３上の仮想マシンとして動作させる。仮想化ソフトウェアはKVMとHyper-Vを使用する。社内には本社・支社ネットワークが存在する。本社ネットワークにはサーバ接続用のVLAN以外にクライアント接続用のVLANが２つあり、このうち一方はインターネットへの直接的接続を許可しないセグメントとする。支社ネットワークも同様とする。本社と支社間の通信はプライマリ経路としてインターネット経由のVPNを使用する。ただし、このVPN回線に障害が発生した場合はバックアップ経路として専用線（検証環境ではシリアル回線）にて通信可能とする。また、インターネットへのアクセス回線についても本社・支社が互いにバックアップ経路となる構成とする。

ネットワーク機器接続表

各ネットワーク機器のインターフェースの接続先は次の通りである。

機器	ホスト名	インターフェース	接続先
ルータ１	R1	Fa0/0	アクセス回線1
		Fa0/1	スイッチ１
ルータ２	R2	Fa0/0	アクセス回線2
		Fa0/1	スイッチ２
		Se0/0/0	ルータ３
ルータ３	R3	Fa0/0	スイッチ１
		Fa0/1	スイッチ３
		Se0/0/0	ルータ２
スイッチ１	SW1	Gi0/1-Gi0/2	サーバ３
		Gi0/3	サーバ１（サーバ１のeth0）
		Gi0/4-Gi0/6	－
		Gi0/7	ルータ１
		Gi0/8	ルータ３
スイッチ２	SW2	Gi0/1-Gi0/6	－
		Gi0/7	サーバ２（サーバ１のeth1）
		Gi0/8	ルータ２
スイッチ３	SW3	Gi0/1-Gi0/7	－
		Gi0/8	ルータ３

・インターフェース記号　Fa：FastEthernet，Gi：GigabitEthernet，Se：Serial

・接続先の「－」はネットワーク機器接続未指定ポートを指す。

・接続先の「アクセス回線1,2」は、各競技エリアまで敷いているLANケーブルを指す。

インターフェース設定表

各ネットワーク機器インターフェースの設定値は、次の通りである。

１．インターフェースIPアドレスの設定

（XXは座席番号の数字とする。）

機器	ホスト名	インターフェース	IPアドレス
インターネット側参考情報		アクセス回線1	160.250.XX.254/29
		アクセス回線2	170.250.XX.254/29
ルータ１	R1	Fa0/0	160.250.XX.253/29
		Fa0/1	スイッチ１に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-3のｱﾄﾞﾚｽ
ルータ２	R2	Fa0/0	170.250.XX.253/29
		Fa0/1	スイッチ２に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-1のｱﾄﾞﾚｽ
		Se0/0/0	10.1.0.6/30
ルータ３	R3	Fa0/0	スイッチ１に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-2のｱﾄﾞﾚｽ
		Fa0/1	スイッチ３に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-1のｱﾄﾞﾚｽ
		Se0/0/0	10.1.0.5/30
スイッチ１	SW1	Vlan100	10.1.100.250/24
スイッチ２	SW2	Vlan10	172.16.1.250/24
スイッチ３	SW3	Vlan10	192.168.1.250/24

・インターフェース記号　Fa：FastEthernet, Gi：GigabitEthernet, Se：Serial

VlanX:Virtual LAN with id X

なお、VLANに接続するルータのインターフェースにはVLAN IDと一致するサブインタフェースを使用する。

２．スイッチ１のVLAN設定

VLAN番号	VLAN名	割付ポート	サブネット	用途
100	Server	Gi0/1-Gi0/2	10.1.100.0/24	内部向けサーバ セグメント
200	DMZ	Gi0/3	10.1.200.0/24	本社DMZ セグメント

※　ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

３．スイッチ２のVLAN設定

VLAN番号	VLAN名	割付ポート	サブネット	用途
10	ClientBr1	Gi0/1- Gi0/2	172.16.1.0/24	支社クライアント セグメント
20	ClientBr2	Gi0/3- Gi0/4	172.16.2.0/24	支社クライアント セグメント
100	DMZBr	Gi0/7	172.16.100.0/24	支社DMZ セグメント

※　ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

※　VLAN　ClientBr2　は直接的なインターネット接続は許可しないセグメントとする。

４．スイッチ３のVLAN設定

VLAN番号	VLAN名	割付ポート	サブネット	用途
10	Client1	Gi0/1- Gi0/2	192.168.1.0/24	本社クライアント セグメント
20	Client2	Gi0/3- Gi0/4	192.168.2.0/24	本社クライアント セグメント

※　ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

※　VLAN　Client2　は直接的なインターネット接続は許可しないセグメントとする。

ネットワーク機器（ルータ及びスイッチ）の設定項目

１．ケーブリング、IPアドレス設定

ネットワーク機器接続表、インターフェース設定表、各スイッチ設定の構成をもとに、ネットワークを接続、設定しなさい。

２．パスワード

各ネットワーク機器に従って特権モード、コンソール、Telnet(vty0-4)に対してパスワードを設定しなさい。全てのパスワード及び特権モードパスワードは暗号化する。

３．シリアル接続

ルータ３をDCE、ルータ２をDTEとして、シリアルケーブルで接続しなさい。

４．VPN

本社ルータ１と支社ルータ２をインターネット経由でIPsecVPN接続しなさい。その際、ルータ１，ルータ２間に10.1.0.0/30のアドレスを使用し（ルータ１側を若番とする）トンネルインターフェース（GREトンネル）の設定を行いなさい。

５．ルーティング

ルーティングについて以下の通り設定しなさい。

- 本社・支社の各ルータ間で経路交換を行い、全てのネットワークで通信可能とする。ルーティングプロトコルとしてEIGRPを使用する。
- インターネット側（VPN回線除く）およびスイッチ２・スイッチ３へ経路情報を流さないこと。
- 本社ネットワーク⇔支社ネットワーク間の通信において、プライマリ経路としてVPN回線を使用し、VPN回線障害時のバックアップ経路としてシリアル回線を使用するようにメトリックを調整すること。
- 上記の経路切り替えが高速に行えるように、ルータ３のEIGRPトポロジーテーブルには、スイッチ２に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。同様に、ルータ２のEIGRPトポロジーテーブルには、スイッチ１・スイッチ３に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。

６．ゲートウェイの冗長化

ルータ１とルータ３間にVRRPを設定し、スイッチ１のVLAN100,200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。

- ルータ１をMasterルータとする。
- ルータ１においてアクセス回線１がリンクダウンした場合、Masterルータがルータ３に切り替わるようにする。アクセス回線１が復旧した場合、Masterルータがルータ１に切り戻ること。

7．スイッチ各種設定

スイッチについて以下の通り各種設定を行いなさい。

- スイッチ-ルータ間を接続しているリンクは 802.1Q のトランクリンクとする。
- 各スイッチにおいて機器を接続する予定がないポート（VLAN 割付ポートとルータ接続ポートを除く全ポート）は閉塞する。

8．NAT / NAPT

アドレス変換を以下の通り設定しなさい。

[スタティックNAT設定]

- サーバ１をインターネットと相互接続可能とするために、ルータ１にて 160.250.XX.250 に NAT しなさい。
- サーバ２をインターネットと相互接続可能とするために、ルータ２にて 170.250.XX.250 に NAT しなさい。

[NAPT設定]

- 本社端末（所属 VLAN 名：Client1、Server）がアクセス回線１経由でインターネット接続できるようにルータ１に NAPT を設定しなさい。また、支社端末（所属 VLAN 名：ClientBr1、DMZBr）もアクセス回線 2 障害時のバックアップ経路としてアクセス回線 1 経由でインターネット接続できるようにルータ１に NAPT を設定しなさい。使用するグローバルアドレスはルータ１の Fa0/0 に設定されているアドレスとする。
- 支社端末（所属 VLAN 名：ClientBr1）がアクセス回線２経由でインターネット接続できるようにルータ２に NAPT を設定しなさい。

9．アクセスコントロール

アクセス制御を以下の通り設定しなさい。

- ルータ１に以下の条件を満たすアクセス制御を設定する。
  - インターネットからのアクセスについて
    - サーバ１に対しては DNS サービス 、SMTP サービスおよび ICMP のみ通信を許可する。
    - ルータ１自身に対する ICMP を許可する。
    - ルータ２との VPN 回線のトラフィックは全て許可する。
    - 上記以外は許可しない。
  - 社内からインターネットへのアクセスについて
    - サーバ１からインターネットへのアクセスは全ての通信を許可する。
    - NAPT でのインターネットアクセスは全ての通信を許可する。
    - 上記以外は許可しない。

- ルータ２にも同様にアクセス制御を設定する。

サーバの設定項目

以下の指示に従ってサーバの設定を行いなさい。

１．　OSインストール

- **各サーバOS共通設定**

  システム時刻を競技会場の時計と±5分以内に合わせなさい。

- **サーバ１のOSインストール**

コンピュータ１にサーバ１のOS としてDebian GNU/Linux 7.5.0を以下の通りインストールしなさい。

キー配列	日本語キーボード
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意
一般ユーザのパスワード	user
ホスト名	sv01
ドメイン名	netadXX.it.jp

サーバ１のネットワーク設定は以下の通りとし、eth0にてネットワーク接続可能とする。

IPアドレス	10.1.200.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.200.254
ネームサーバ	自身

サーバ１のパーティション構成を以下のとおりとする。ただし、ソフトウェアの仕様上、サイズが若干異なっても良い。

マウントポイント	容量	ファイルシステム
/boot	100MB	ext4
/	40GB	ext4
/var	50GB	ext4
スワップ	4GB	-

*1GBは、1024MBとする

➢ サーバ２のOSインストール

サーバ２はサーバ１のkvmとvirt-managerを使用して仮想環境にて構築しなさい。

- ✧ 仮想マシン名は「sv02」とする。
- ✧ ホストであるサーバ１はeth1にてネットワーク接続しないこと。
- ✧ 仮想マシンのイメージファイル容量、パーティション構成、メモリサイズなどは任意とする。
- ✧ 仮想マシン「sv02」はサーバ１の起動時に自動起動すること。

サーバ２のOS としてDebian GNU/Linux 7.5.0を以下の通りインストールしなさい。

キー配列	日本語キーボード
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意
一般ユーザのパスワード	user
ホスト名	sv02
ドメイン名	aichi.netadXX.it.jp

サーバ２のネットワーク設定は以下の通りとする。

IPアドレス	172.16.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.16.100.254
ネームサーバ	自身

➢ サーバ３の OS インストール

コンピュータ２にサーバ３のOSとして WindowsServer2012 R2 を以下の通りインストールしなさい。

キー配列	日本語キーボード
タイムゾーン(ローカル時間)	Asia/Tokyo
管理者のパスワード	Aichi2014
コンピュータ名	sv03
ドメイン名	netadXX.local

ネットワーク設定は以下の通りとする。

IPアドレス	10.1.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.100.254
ネームサーバ	自身

- **サーバ４のOSインストール**

サーバ４はサーバ３のHyper-Vを使用して仮想環境にて構築しなさい。

- ✧ 仮想マシン名は「sv04」とする。
- ✧ 仮想HDD容量、パーティション構成、メモリサイズなどは任意とする。
- ✧ 仮想マシン「sv04」はサーバ３の起動時に自動起動すること。

サーバ４のOS としてDebian GNU/Linux 7.5.0を以下の通りインストールしなさい。

管理者のパスワード	Aichi2014
一般ユーザアカウント名	user
ホスト名	sv04
ドメイン名	netadXX.local

サーバ４のネットワーク設定は以下の通りとする。

IPアドレス	10.1.100.2
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.100.254
ネームサーバ	10.1.100.1

２．Active Directory

[サーバ３]

サーバ３上にActive Directoryドメインサービスを構成し、ドメインコントローラーを構築しなさい。

- 作成するフォレストのルートドメインを「netadXX.local」とする。
- フォレストとドメインの機能レベルは「WindowsServer2012 R2」とする。
- ディレクトリサービスの復元モードパスワードは「Aichi2014」とする。
- 以下の表に従って OU、グループ、ユーザを作成しなさい。

ユーザ名	パスワード	OU	グループ
aduser01	Aichi2014	IT部	Employee
aduser02	Aichi2014	IT部	Employee
aduser03	Aichi2014	IT部	Employee

３．認証統合

[サーバ４]

サーバ４のユーザ認証をサーバ３上のActive Directoryサービスによって行なえるように以下の通り設定しなさい。

- 使用するパッケージは samba および winbind とする。
- サーバ４をサーバ３の Active Directory ドメインのメンバサーバとして参加させる。
- サーバ３上に登録した ActiveDirectory ユーザにてサーバ４へログイン可能とすること。この際、Active Directory ドメイン名の指定は省略できること。また、各ユーザ(aduser01～03)のホームディレクトリ「/home/win/ユーザ名」（例 /home/win/aduser01）は初回ログイン時に自動作成されること（例：初回ローカルログイン時、初回 ssh ログイン時、初回 pop3s ログイン時）。ホームディレクトリの自動作成が不可能な場合は手動で作成しなさい*。
- 上記指定の方法による認証統合が不可能な場合は、その他の方法によって認証統合を構成して構わない*。
- 認証統合が不可能な場合は、「**２．Active Directory**」で作成したユーザ名・パスワードと同一ユーザ名・パスワードの新規アカウントをサーバ４上に手動で作成しなさい*。

*ただし，減点対象とする。

４．DNS

DNSサービスを以下の通り設定しなさい。

[サーバ１、サーバ２共通]

- 使用するパッケージは bind9 とする。
- 自身で名前解決ができない場合は、ISP サーバに問い合わせる。
- bind のバージョンを回答しない。

[サーバ１]

- 「社内」および「外部ネットワーク」からの問い合わせに応える。
- 再帰問い合わせは自身(localhost)とサーバ３からのみ許可する。
- 「外部ネットワーク」向けの netadXX.it.jp および aichi.netadXX.it.jp ゾーンの管理を行うマスターサーバとして動作させる。サーバ１とサーバ２の正引きを設定する。別名としてサーバ１は「mailgw.netadXX.it.jp」、サーバ２は「www.aichi.netadXX.it.jp」を持つ。
- 「社内」向けの netadXX.it.jp および aichi.netadXX.it.jp ゾーンと、その逆引きゾーンの管理を行うマスターサーバとして動作させる。サーバ１とサーバ２の正引き・逆引きを設定する。別名としてサーバ１は「proxy.netadXX.it.jp」、サーバ２は「mail.aichi.netadXX.it.jp」を持つ。
- サーバ３で管理しているゾーンのスレーブとして動作させる。

[サーバ２]

- 「社内」および「外部ネットワーク」からの問い合わせに応える。
- 再帰問い合わせは自身(localhost)と「支社内」からのみ許可する。
- サーバ１とサーバ３で管理しているゾーンのスレーブとして動作させる。

[サーバ３]

- WindowsServer2012R2 の DNS サーバを使用する。
- 自身で名前解決ができない場合は、サーバ１に問い合わせる。
- 「社内」からの問い合わせに応える。
- netadXX.local ゾーンとその逆引きゾーンの管理を行うマスターサーバとして動作させる。サーバ３とサーバ４の正引き・逆引きを設定する。別名としてサーバ４は「mail.netadXX.local」と「proxy.netadXX.local」を持つ。

５．メールサービス

メールサービスを以下の通り設定しなさい。

[サーバ１、サーバ２、サーバ４共通]

- 使用するパッケージは postfix とする。

[サーバ１]

- メールゲートウェイとして動作させる。
- 本社ドメイン netadXX.it.jp のプライマリメールサーバ､支社サブドメイン aichi.netadXX.it.jp のセカンダリメールサーバとなる。
- 本社ドメイン netadXX.it.jp 宛てのメールはサーバ４へ転送する。
- 支社サブドメイン aichi.netadXX.it.jp 宛てのメールはサーバ２へ転送する。
- その他の宛先のメールは ISP サーバへ転送する。この際、SMTP 認証を行い、認証が成功した時のみ中継を許可する。認証用ユーザとして mailuser ユーザを作成する。パスワードはユーザ名と同一とする。ただし、サーバ４からは認証なしで中継を許可する。

[サーバ２]

- 支社サブドメイン aichi.netadXX.it.jp のメール送信サーバとして動作させる。
- 支社サブドメイン aichi.netadXX.it.jp のプライマリメールサーバ､本社ドメイン netadXX.it.jp のセカンダリメールサーバとなる。

[サーバ４]

- 本社ドメイン netadXX.it.jp のメール送信および受信サーバとして動作させる。
- 本社ドメイン netadXX.it.jp 宛てのメールをスプールする。保存形式は任意とする。

６．プロキシサービス

サーバ１とサーバ４でプロキシサービスを行いなさい。使用するパッケージはsquid3とする。

- グループポリシーを用いて、サーバ３の Active Directory ドメインユーザに対し、Internet Explorer が利用するプロキシサーバとしてサーバ４が指定されるように動作させる。

７．Webサーバサービス

サーバ１でWebサーバサービスを行いなさい。

８．データベースサービス

サーバ１でデータベースサービスを行いなさい。

９．WordPress

サーバ１でWordPressサービスを行いなさい。