

技能五輪全国大会 選考会
IT ネットワークシステム管理
競技課題概要 第 1 版
(職種への参加の手引き 2019 年)

令和 元年 6 月 4 日

競技委員作成

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。信頼性の高いネットワークとサーバシステムを設計・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企業内ネットワーク構築技術」を競います。

同時期に開催する若年者ものづくり競技大会の「IT ネットワークシステム管理」とは競技課題のレベルが異なりますので注意してください。本競技は技能五輪全国大会の予選ですので、競技課題も技能五輪全国大会に準じたものになります。競技課題の草案（選考会当日は詳細の追加や一部変更を行い出題）を添付していますので、参考にしてください。

2. 競技日程（予定）

- ・ 7月29日：競技日の前日
13:30 集合～15:00 終了
競技内容の説明、競技場所の抽選、機材の確認
- ・ 7月30日：競技日
8:40 集合～13:00 終了
競技 9:00～13:00（競技時間：4時間）

3. 競技に使用する主な機器と支給部品

- | | |
|---|-------|
| ・ 仮想化ホスト PC (デスクトップ PC, OS:VMWare ESXi) | 1式 |
| ・ 管理用 PC(デスクトップまたはノート PC, OS: Windows8.1 または 10) | 1 式 |
| ・ LAN ケーブル(既製品) | 1～2 本 |

4. 競技に使用する主なソフトウェア

- ・ サーバ OS:Debian GNU/Linux 9.9 stretch
- ・ クライアント OS:Windows10
- ・ 仮想化ソフトウェア:VMWare ESXi 6, VMware Remote Console
- ・ ネットワーク仮想化ソフトウェア: Cisco VIRL PE v1.5, VM Maestro
- ・ ターミナルソフトウェア: TeraTerm
- ・ メールソフトウェア: Thunderbird (課題の構成によっては使用しない場合もある)

5. 競技環境

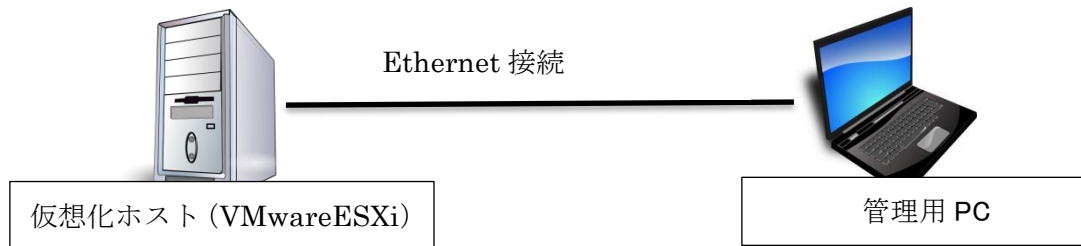


図 1：物理接続

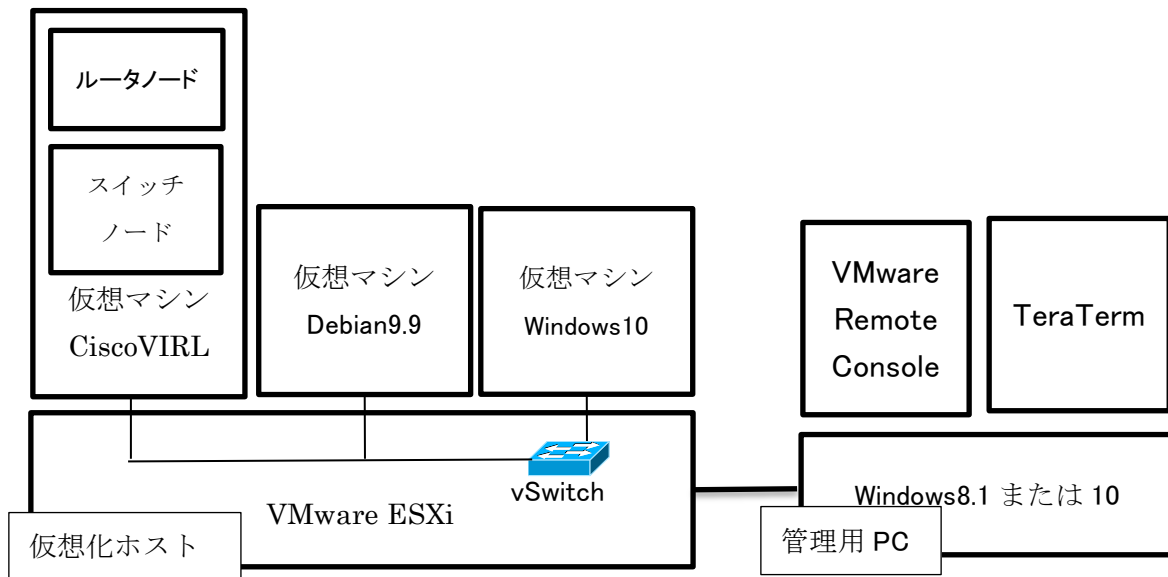


図 2：ソフトウェア配置イメージ

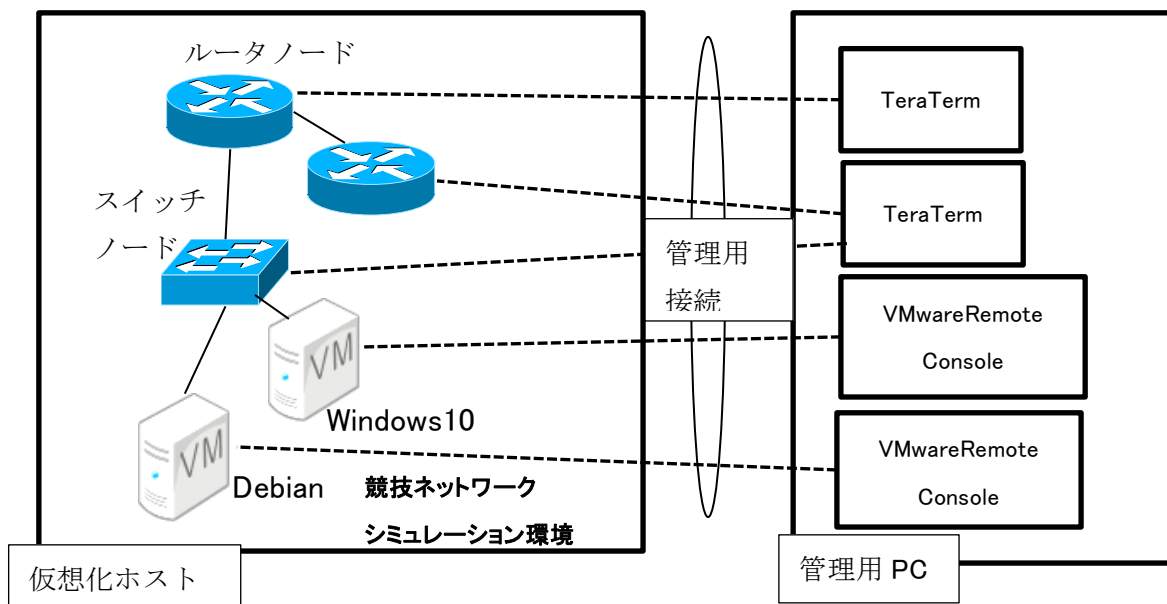


図 3：論理接続イメージ

本選考会においては、Cisco VIRL (Cisco Virtual Internet Routing Lab Personal Edition) を用いた仮想環境で競技を行います。

前項図 1 に示すように仮想化ホスト 1 台と管理用 PC 1 台を接続した環境で競技を実施します。前項図 2 に示すソフトウェア環境は競技委員によってセットアップされた状態で提供されます。ただし、競技として構築するサーバについては、OS 未インストール状態の仮想マシンに対して OS (Debian 9.9) のインストールを要求される場合があります。仮想ネットワーク環境 Cisco VIRL についても競技委員によってセットアップされた状態で提供されます。各ルータノード・スイッチノードおよびサーバ仮想マシン・クライアント仮想マシンは、VIRL の仮想ネットワークに配置され、各ノード間も接続済みの状態で提供されます。VIRL 上の各ノードと VMware ESXi 上の各仮想マシンは、ESXi の仮想スイッチ (vSwitch) 経由で接続されますが、それらの設定作業は競技委員が行います。

競技開始時点において、VIRL のネットワークシミュレーションは起動された状態とします。各ルータノード・スイッチノード・仮想マシンも起動している状態です。この時、前項図 3 のように管理用 PC から各ノードへの接続が可能な状態となっています。各ルータノード・スイッチノードへの接続には、TeraTerm を使用します。各仮想マシンへの接続には VMware Remote Console を使用します。選手は課題の要求に従い各ノードに対して各種設定を行ってください。シミュレーションの開始処理は競技委員が競技開始前に行います。また、競技中や競技終了時において、VIRL のネットワークシミュレーションを終了する操作は決して行わないでください。図 4 にシミュレーション実行画面の例と各ノードへの接続画面の例を示します。

VIRL のネットワークシミュレーションで使用するノードタイプは次の通りです。

a) ルータノード

ノードタイプ: IOSv

OS バージョン: IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.6(3)M2

b) スwitchノード

ノードタイプ: IOSvL2

OS バージョン: vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Experimental Version 15.2

c) 外部接続用

L2external (FLAT) 仮想マシンや外部物理ネットワークとの接続用であり、
競技における操作の対象ではありません。

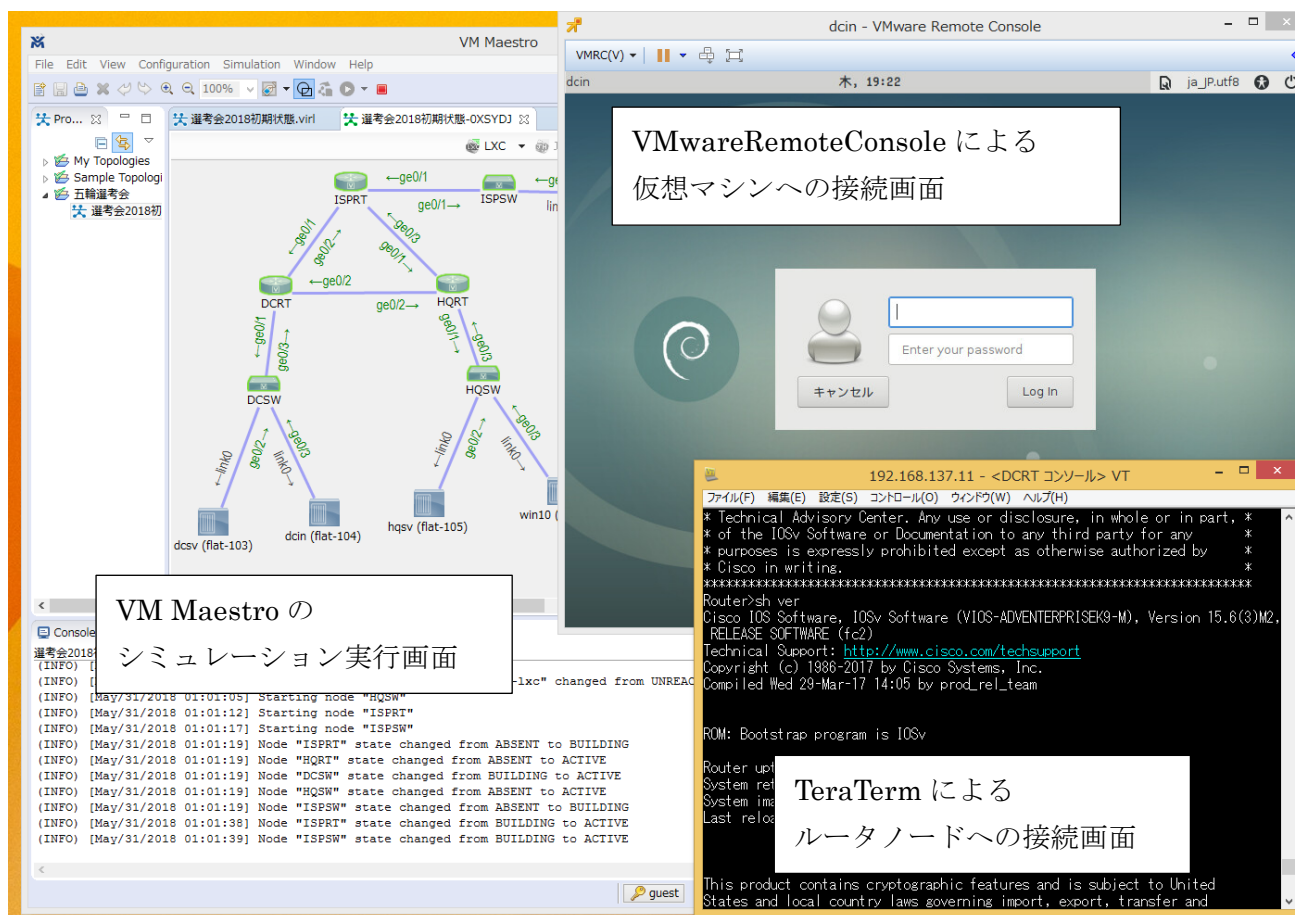


図 4：シミュレーション実行例とノードへの接続例

6. 競技課題概要

与えられた「シナリオ」、「競技課題の背景」、「ネットワーク構築に関する基本ポリシー」を読んで、下記の作業を行います。

A. サーバ構築作業

指定された各種サーバ機能を実現するため、OS の設定、各種ネットワークサービスの設定作業を行います。

B. クライアントの設定

指定されたネットワークシステムにおけるクライアントの設定を行います。

C. ネットワーク機器の設定

指定されたネットワークシステム構成とセキュリティを実現するため、ルータおよびスイッチの基本設定、ルーティング設定、アドレス変換設定、フィルタリング設定、WAN 接続設定、冗長化設定などの作業を行います。

7. 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客観的に評価します。配点は「A. サーバ構築作業」が60%未満、「B. クライアントPCの設定」が10%未満、「C. ネットワーク機器の設定」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。

8. 持参工具等

特にありませんが、筆記用具は持参してください。

9. 競技上の注意事項

- a. 各種マニュアルやUSBメモリ等の記憶装置の持ち込みは一切認めません。
- b. 質問などがある場合には、競技委員に申し出て下さい。
- c. 競技終了の合図で、作業を直ちに終了して下さい。
- d. 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って下さい。
- e. 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って下さい。
- f. 競技中の水分補給のための飲料水の持ち込みは認めます。
- g. 携帯電話の電源は切っておいて下さい。

10. 競技課題草案

次項以降に競技課題の草案を示します。

昨年度の技能五輪全国大会の競技課題をベースにした課題の草案です。選考会当日の競技課題は、この草案に対して詳細の追加や一部変更を行い、出題します。

第 57 回 技能五輪全国大会 選考会

IT ネットワークシステム管理

競技課題(草案) 競技委員作成 2019/06/04

令和元年 7 月 30 日 (火)
競技時間：4 時間 (9:00～13:00)

競技に関する注意事項：

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

座席番号	競技者氏名

競技課題に関する注意事項

- ✓ 競技中および競技終了時において VIRT シミュレーションを終了させないこと。
- ✓ 採点は、競技終了時点のシステム状態のままで実施される。
- ✓ 競技終了時に指定された設定が各ネットワークノードの startup-config に保存されていること。
- ✓ 各ネットワークノードの設定情報は、競技終了後に競技委員によって抽出（Extract Configuration(s)）される。
- ✓ vSphere Client やブラウザを用いて ESXi ホストの管理画面に接続することは許可しない。
- ✓ 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、ISP-A、ISP-B、ISP-C および ISPserver で構成される。これは競技委員が用意する構成済みの「仮想的なインターネットエリア」である。実際のインターネットには接続されていないが、競技課題中では単に「インターネット」あるいは「外部ネットワーク」と呼ぶ。

競技課題の背景

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（Gorin Netad Inc.）のネットワークシステムの更改業務を受注し、そのプロジェクトリーダーとなった。ネットワークの設計やサーバの構築内容は既に完成している。これをもとに検証用の環境を構築する。

構築ネットワークの概要

図1に示すように社内にはリモートオフィス及びデータセンターが存在する。リモートオフィスにはクライアント接続用のセグメント(ROLAN)がある。データセンターにはlb1(エル・ビー・1)、www1、www2が接続するDMZセグメント(DCDMZ)とdcinが接続する社内向けサーバセグメント(DCLAN)がある。ROLANとDCLAN間の通信はインターネット経由のトンネル接続を使用する。データセンターは異なる2つのISPに接続するマルチホームネットワークであり、冗長化と負荷分散を構成する。詳細については、別添ネットワーク構成図・表に示す。

競技における設定対象は、リモートオフィスおよびデータセンターのネットワークとなる。
インターネット（想定）エリアの各ノードは、設定済みである。

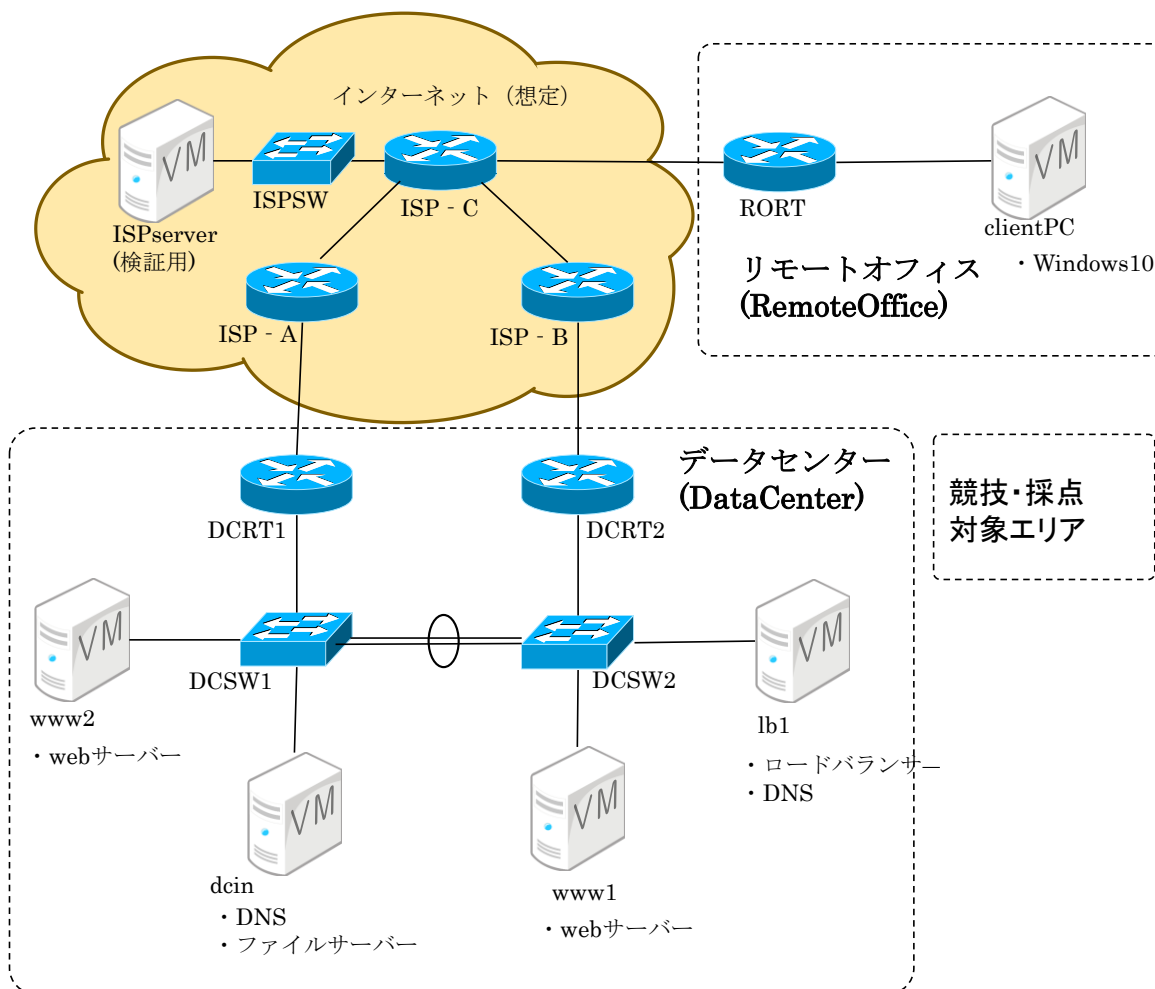


図1：ネットワーク構成概要

仮想マシンに関する基本情報

● 仮想マシン lb1, www1, www2, dcin について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Debian9.9が既にインストールされており、初期インストールにおいて「標準システムユーティリティ」と「SSHサーバ」が選択されインストールされた状態となっている。下表の初期設定状態となっている。

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

共通設定

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

仮想マシン：lb1 (エル・ビー・1)

ホスト名	lb1
IPアドレス	20.0.0.1/28

仮想マシン：www1

ホスト名	www1
IPアドレス ens192	20.0.0.3/28

仮想マシン：www2

ホスト名	www2
IPアドレス	20.0.0.4/28

仮想マシン：dcin

ホスト名	dcin
IPアドレス	192.168.101.1/24

● 仮想マシン clientPC について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Windows10が既にインストールされている。「teraterm」がインストールされている。

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

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

- DNS サーバが稼働しており、ns.itnetsys.org、www.itnetsys.org、mail.itnetsys.org の正引きが登録されている。
- Web サーバが稼働しており、次の URL で Web アクセス可能である。
“http://200.99.1.1” “http://www.itnetsys.org”

● 検証作業用仮想マシン PC1 について

- Windows10 がインストールされており、検証作業用として自由に使用してよい。
- 採点対象とはならない。
- 「VMRC(V)→管理→仮想マシン設定→ネットワークアダプタ→ネットワーク接続」から、任意のセグメントに接続してよい。
ただし、その他の仮想マシンについては、接続を変更しないこと。

各ノードへの接続方法

● 各仮想マシンへの接続について

各仮想マシンに接続するための vmrc ショートカットは、管理用 PC デスクトップ上のフォルダ “2019_shortcut” にある。仮想マシン名と同名のショートカットアイコンをダブルクリックし、ユーザ名 “root”、パスワード “adm@esxi” にてアクセス可能である。(このユーザ名・パスワードは ESXi ホストのものであり、ゲスト OS のものではないことに注意)

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

● 各ネットワークノードへの接続について

各ネットワークノードのコンソールにアクセスするための teraterm ショートカットは、管理用 PC デスクトップ上のフォルダ “2019_shortcut” にある。ノード名と同名のショートカットアイコンをダブルクリックし、ターミナル起動後、「Enter」キーを押すことで応答する。また、その他の方法として、VM Maestro からのコンソール接続を利用してよい。

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

● ISP-A、ISP-B、ISP-C への接続について

- ・ ユーザモード（非特権モード）でのアクセスは許可する。
- ・ 特権モードでのアクセス、設定変更は許可しない。
- ・ 動作検証のためにアクセスが必要な場合は、VM Maestro のコンソール接続を利用してよい。

その他の基本情報

● Debian9.9 isoイメージについて

管理用 PC のデスクトップ上に「debian_iso」フォルダがあり、Debian 9.9.0 の iso ファイルが置かれている。VMware Remote Console のメニューにおいて「VMRC(V)」→「取り外し可能デバイス(R)」→「CD/DVD ドライブ 1」→「ディスクイメージファイル(iso)に接続(C)…」を選択し、iso イメージをマウント可能である。

● Linux仮想マシンへのGUIデスクトップ環境の導入について

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

Cisco ネットワークノード設定課題

別添ネットワーク構成図・表および以下の設定項目に従い、ネットワークノード（DCRT1, DCRT2, RORT, DCSW1, DCSW2）を設定しなさい。設定項目は、ネットワーク構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。

● 全ネットワークノード共通基本設定

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

● ルーティング設定

ルーティングについて以下の通り設定しなさい。

- RORT のデフォルトルート (Dialer0) を静的に設定する。
- DCRT1 および DCRT2 において次の通り BGP を動作させる。※ISP-A は AS200、ISP-B は AS300、ISP-C は AS600 所属として BGP が動作している。
 - DCRT1 と DCRT2 は AS100 所属として BGP を動作させる。
 - DCRT1 は ISP-A と eBGP ピアを確立する。
 - DCRT2 は ISP-B と eBGP ピアを確立する。
 - インターネット側から 20.0.0.0/28 宛てのトラフィックについて、ISP-B→DCRT2 を経由する経路を優先経路とする。この経路に障害が発生した場合は、ISP-A→DCRT1 を経由する経路に自律的に切り替わること。
- RORT, DCRT1, DCRT2 において次の通り OSPF を動作させる。
 - プライベートアドレスセグメントについて経路交換を行う。
 - インターネット側（トンネル回線除く）と ROSW 側へ OSPF 経路情報を流さないこと。

● WAN 設定

WAN 環境について以下の通り設定しなさい。

- RORT にて PPPoE クライアント設定を行い ISP-C (PPPoE サーバ設定済み) と接続する。
※ISP-C から IPCP によって固定アドレスが払い出される。
- Dialer インタフェースとして Dialer0 を作成する。
- 認証方式は chap とし、認証ユーザは “skills”、パスワードは “skills” を用いる。
- DCRT1 と RORT を IPsecVPN 接続する。
 - DCRT1-RORT 間に 10.1.0.0/30 (DCRT1 側が若番) のアドレスを使用したトンネルインターフェース Tunnel0 を作成し、IPsec VTI (Virtual Tunnel Interface) として設定する。

● ゲートウェイの冗長化

DCRT1 と DCRT2 において、以下の条件を満足するようにゲートウェイの冗長構成を実現しなさい。

- VLAN20 について、VRRP を次の通り動作させる。
 - DCRT2 を Master ルータとする。
- VLAN101 について、HSRP を次の通り動作させる。
 - DCRT1 を Active ルータとする。

● NAPT

アドレス変換を以下の通り設定しなさい。

- ROLAN (172.16.1.0/24) からインターネット (想定) へ接続できるように RORT に NAPT を設定しなさい。使用するグローバルアドレスは Dialer0 に設定されているアドレスとする。

● スイッチ設定

スイッチについて以下の通り各種設定を行いなさい。

- 各スイッチ (DCSW1, DCSW2) について、管理アドレスおよび適切なデフォルトルートを設定する。
- DCSW1 と DCSW2 間の接続について、Etherchannel を設定する。

● アクセスコントロール

RORT の Dialer0 での通信について、アクセスコントロールを以下の通り設定しなさい。

- RORT と DCRT1 間の通信はすべて許可する。
- RORT と DCRT2 間の通信はすべて許可する。
- すべての送信元から RORT 自身に対する ICMP トラフィックを許可する。
- ROLAN からの NAPT された発信トラフィックとそれに対する戻りトラフィックを許可する。
- 上記以外は許可しない。

Linuxサーバ設定課題

以下の設定項目に従い、Linux サーバ仮想マシン（lb1, www1, www2, dcin）を設定しなさい。設定項目は、サーバ構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。

● 基本設定

lb1、www1、www2、dcinについてデフォルトゲートウェイを適切に設定しなさい。また、ネームサーバアドレスとして、lb1とdcinは自身のアドレス、その他はlb1のアドレスを指定しなさい。

● CA（認証局）

dcinにてCAを以下の通り設定しなさい。

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

● ロードバランサ

lb1にロードバランサを以下の通り設定しなさい。

- 使用するパッケージはhaproxyとする。
- フロントエンドサーバとしてlb1は、SSL接続(TCP443番)および非SSL接続(TCP80番)要求を、バックエンドサーバのwww1およびwww2へラウンドロビン方式で振り分ける。

● Redis (キー・バリュー型データベース)

dcin にて redis サーバを以下の通り設定しなさい。

- 使用するパッケージは redis-server とする。
- 次のコマンドにて新規エントリを追加する。

```
redis-cli set skills:index "Today is the 2019-01-01 and current time is 00:00"
```

※ 「redis-cli set キー 値」にて、「キー」とそれに対応する「値」を設定できる

※ 「redis-cli get キー」にて、登録されている「キー」に対応する「値」を取得できる

※ `redis-cli get skills:index` の結果は次の通り

"Today is the 2019-01-01 and current time is 00:00"

- 上記で追加したエントリ内の日付部分と時刻部分について、現在（スクリプト実行時）の日付と時刻に更新するシェルスクリプトを作成する。

● Web サービス

www1、www2 にて Web サービスを以下の通り設定しなさい。

- 使用するパッケージは apache2、php、php-redis とする。
- `http://IP アドレス/` へのアクセスについて
 - `/var/www/html/index.php` を表示する。
 - `index.php` の内容は次の通りであり、動的にホスト名を取得し表示するものとする。

```
<?php
    echo '<h1>', gethostname(), '</h1>';
?>
```

- `http://IP アドレス/redis/` へのアクセスについて
 - `/var/www/html/redis/index.php` を表示する。
 - `index.php` の内容は次の通りとし、動的に redis サーバ(dcin)からデータを取得し表示するものとする。

```
<?php
    echo '<h1>', gethostname(), '</h1>';
    $redis=new Redis();
    $redis->connect('192.168.101.1');
    $content=$redis->get('skills:index');
    echo $content;
?>
```


● Web コンテンツ同期

www1、www2 にて Web コンテンツを以下の通り同期しなさい。

- 使用するパッケージは rsync とする。
- 同期処理を行うシェルスクリプト web_sync.sh を www1 の /root ディレクトリに作成する。
 - www1 の /var/www ディレクトリを同期元とし、www2 の /var/www ディレクトリを同期先とする。

● DNS

lb1 および dcin にて DNS サービスを以下の通り設定しなさい。

- 使用するパッケージは bind9 とする。
- 競技課題の要求仕様から必要となるレコードがあれば各自判断して追加すること。
- DNSSEC の検証は無効にする。
- 以下の設定において、内部ネットワークとは DCDMZ, DCLAN, ROLAN (別添ネットワーク構成図・表参照) を指すものとする。内部ネットワーク以外を外部ネットワークとする。トンネル接続に用いたアドレスは考慮しなくてよい。

[lb1 の設定]

- 自身で保持していないレコードの問い合わせについては、ISPserver (200.99.1.1) へ回送する。
- 内部ネットワークからのみ再帰検索を許可する。
- ISPserver と dcin へのみゾーン転送を許可する。
- netad.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。

[dcin の設定]

- 自身で保持していないレコードの問い合わせについては、lb1 へ回送する。
- netad.it.jp ゾーンのスレーブサーバとして動作させる。

● ファイルサーバ

dcin にファイルサーバを以下の通り設定しなさい。

- 使用するパッケージは samba とする。
- 共有ディレクトリへのアクセスに使用するパスワードは次の通りとする。
 - ユーザ名 user01 パスワード smbuser01
- ROLAN(172.16.1.0/24) からのアクセスのみ許可する。
- ホームディレクトリをクライアント PC から次の通り共有可能とする。
 - /home/ユーザ名/samba ディレクトリを共有ディレクトリとする。
- /home/share ディレクトリを clientPC から次の通り共有可能とする。
 - 「dcin」にグループ「share_group」を作成し、user01 を所属させる。
 - グループ「share_group」に所属するユーザに対してのみ、この共有ディレクトリへのアクセスを許可する。

クライアント設定課題

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

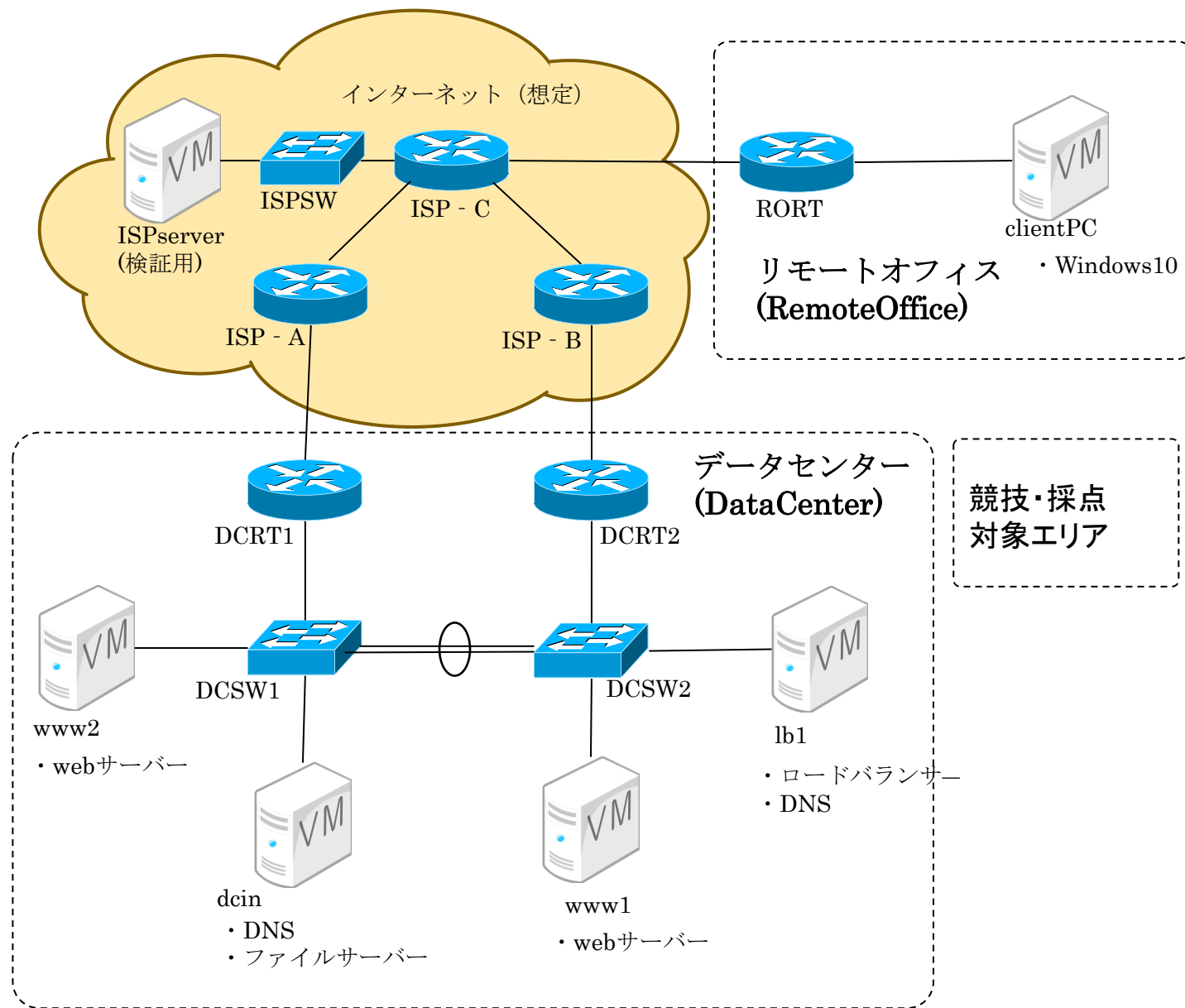
●clientPC の設定

- IP アドレスとして 172.16.1.1、DNS サーバとして dcin のアドレス を設定し、ネットワーク接続可能な状態にしておくこと。
- ブラウザ(IE)にて “https://www.netad.it.jp/” および “https://www.netad.it.jp/redis/” にアクセスした際に、ラウンドロビンにて www1 または www2 のサイトが表示され、証明書エラーが表示されないこと。

第57回 技能五輪 選考会 ITネットワークシステム管理

別添：ネットワーク構成図・表（草案）

競技委員作成2019/6/4



VLAN設定表

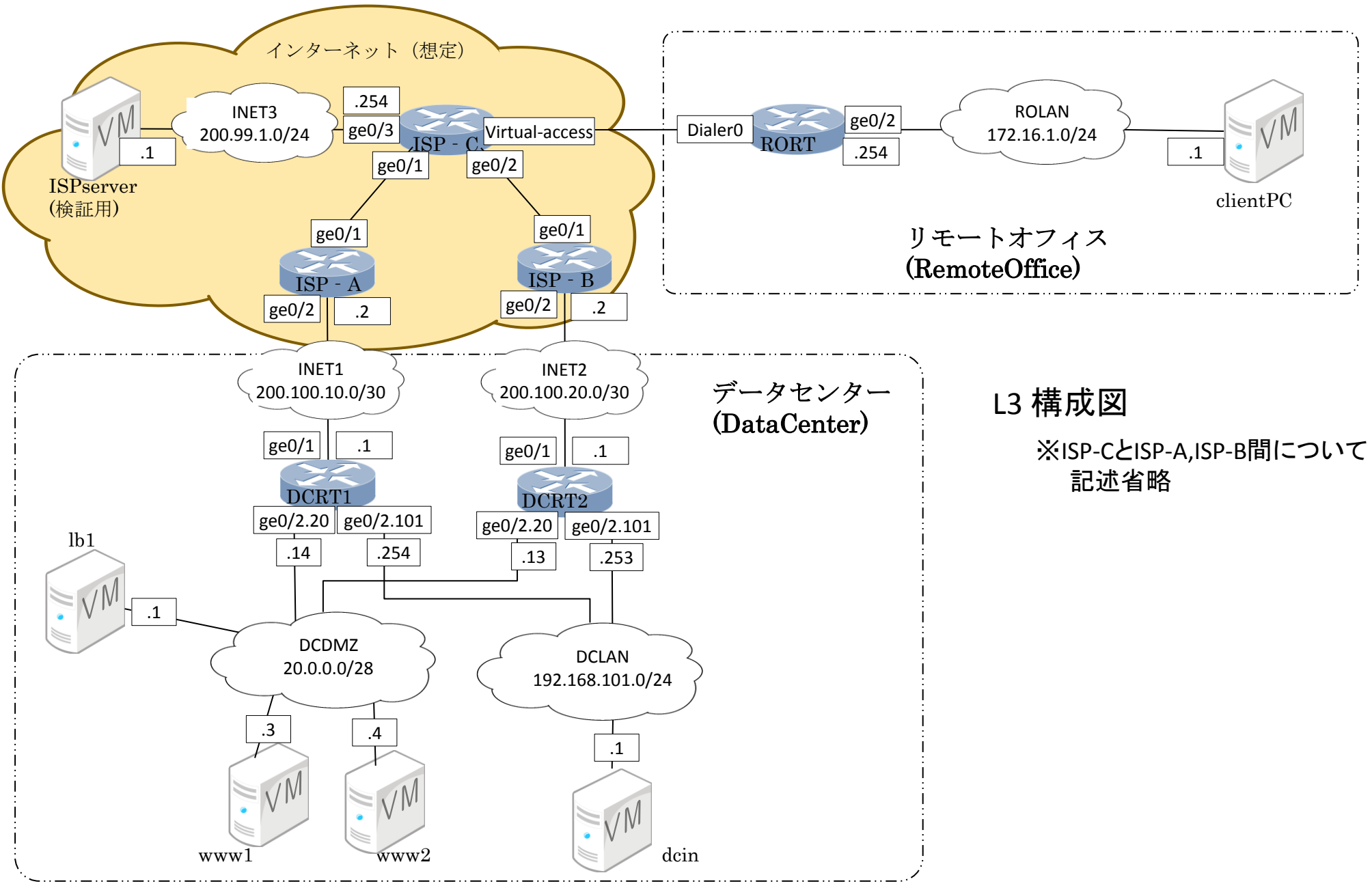
各スイッチのVLANアクセスポートの設定は、次の通りである。

DCSW1のVLANアクセスポート設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
20	DCDMZ		20.0.0.0/28	データセンター DMZセグメント
101	DCLAN		192.168.101.0/24	データセンター LANセグメント

DCSW2のVLANアクセスポート設定

VLAN ID	VLAN名	アクセスポート	サブネット	用途
20	DCDMZ		20.0.0.0/28	データセンター DMZセグメント



L3 構成図

※ISP-CとISP-A,ISP-B間について
記述省略