公表

技能五輪全国大会　選考会
IT ネットワークシステム管理
参加の手引き
競技課題概要
（2024 年　第 62 回大会用）

令和６年６月１３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

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

IT ネットワークシステム管理職種における競技では、上記分野における知識と技能を総合的に競います。本選考会は全国大会の予選となりますので、過年度の全国大会に準じた課題が出題されます。ただし、選考会の競技時間は全国大会と比べ短時間であるため、選考会については出題範囲を圧縮した課題が出題されます。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

・令和６年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

・令和６年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 PC、OS: Windows10)	1式
・ ハブ	1式
・ LAN ケーブル(既製品)	2 本

４．競技に使用する主なソフトウェア

- サーバーOS:Debian GNU/Linux 12.5.0
- クライアント OS:Windows10
- 仮想化ソフトウェア:VMware ESXi（VMware vSphere Hypervisor）、VMware Remote Console
- ネットワーク仮想化ソフトウェア： Cisco Modeling Labs 2.x
- ターミナルソフトウェア： TeraTerm
- メーラーソフトウェア： 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

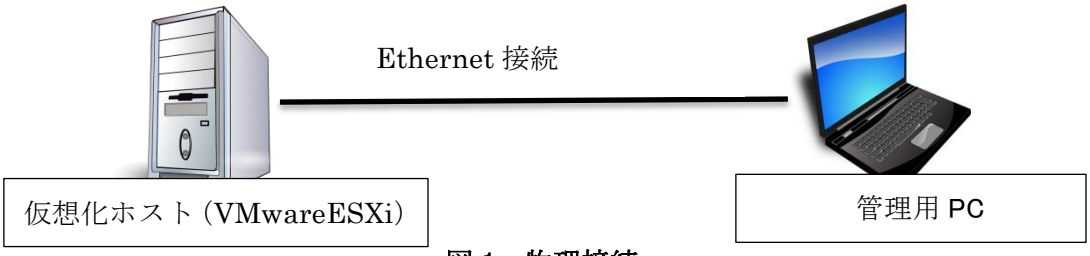


図 1：物理接続

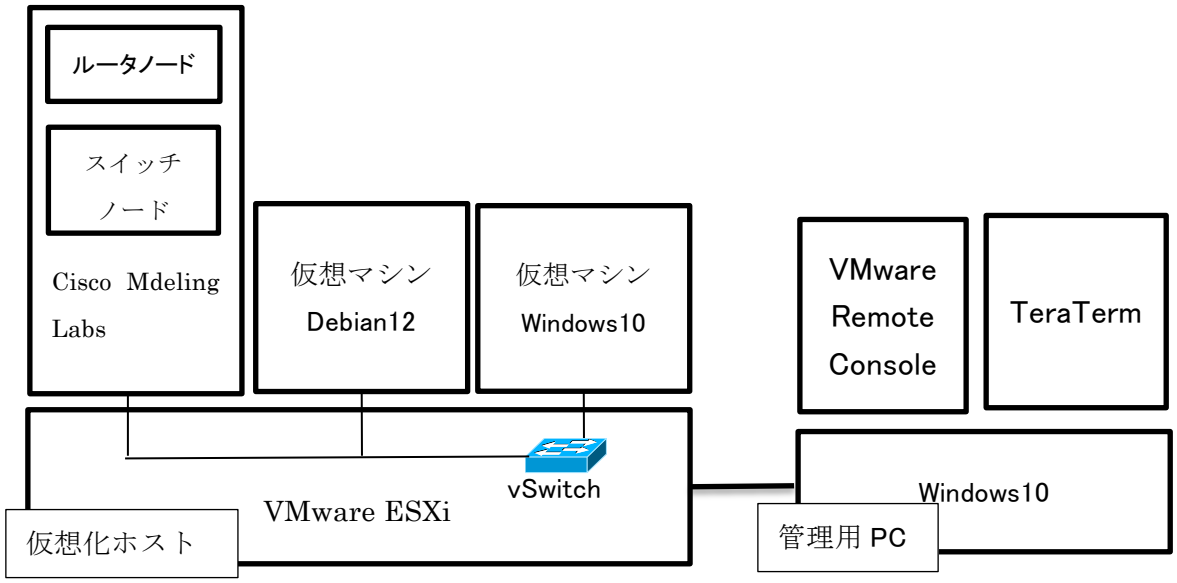


図 2：ソフトウェア配置イメージ

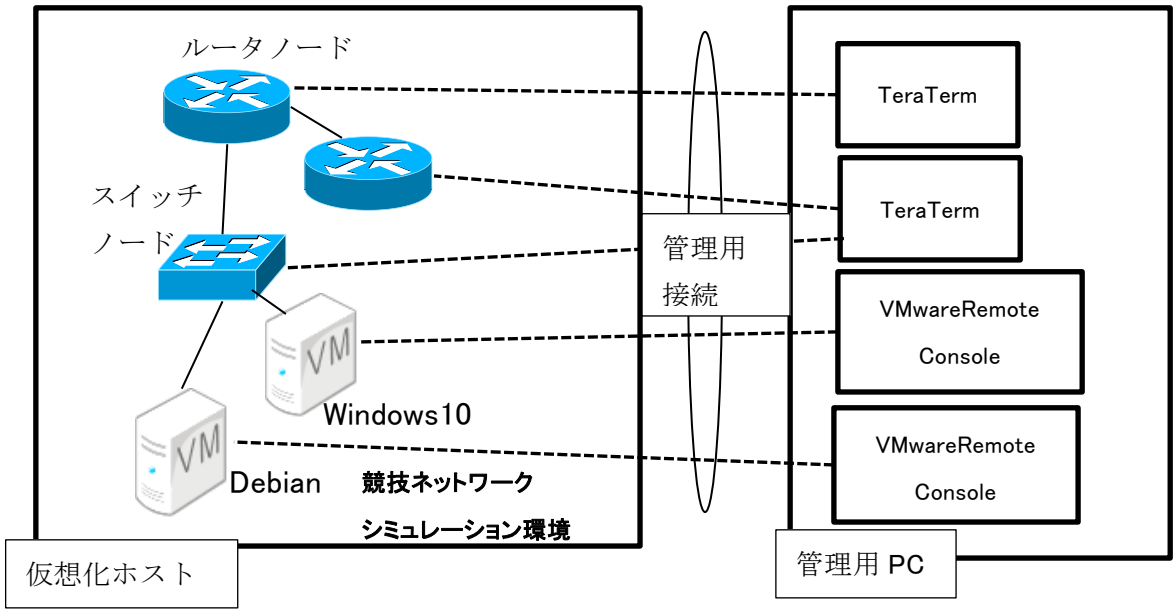


図３：論理接続イメージ

本選考会においては、Cisco Modeling Labs - Personal (CML -P) 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 PC１台を接続した環境で競技を実施します。前項図２に例示するソフトウェア環境は競技委員によってセットアップされた状態で提供されます。ただし、競技として構築するサーバーについては、OS 未インストール状態の仮想マシンに対して OS のインストールを要求される場合があります。仮想ネットワーク環境 CML -P についても競技委員によってセットアップされた状態で提供されます. 各ルータノード・スイッチノード・ファイアウォールノードおよびサーバー仮想マシン・クライアント仮想マシンは、仮想ネットワークに配置され、各ノード間も接続済みの状態で提供されます。仮想ネットワーク上の各ノードと VMware ESXi 上の各仮想マシンは、ESXi の仮想スイッチ（vSwitch）経由で接続されますが、それらの設定作業は競技委員が行います。

競技開始時点において、ネットワークシミュレーションは起動された状態とします。各ルータノード・スイッチノード・ファイアウォールノード・仮想マシンも起動している状態です。この時、前項図３のように管理用 PC から各ノードへの接続が可能な状態となっています。各ルータノード・スイッチノード・ファイアウォールノードへの接続には、TeraTerm が使用可能です。各仮想マシンへの接続には VMware Remote Console が使用可能です。選手は課題の要求を満たすために各ノードを操作することができます。シミュレーションの開始処理は競技委員が競技開始前に行います。ネットワークシミュレーションで使用予定の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
b) スイッチノード　　ノードタイプ：IOSvL2
c) ファイアウォールノード　ノードタイプ：ASAv
d) 外部接続用ノード
　仮想マシンや外部ネットワークとの接続用であり、競技における操作の対象ではありません。

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 A～C の全てまたは一部の作業を行います。

A.　サーバー構築作業
　指定された各種サーバー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構成を実現するため、ルータ、スイッチ、ファイアウォールの基本設定、ルーティング設定、VLAN 設定、アドレス変換設定、フィルタリング設定、WAN 接続設定、VPN 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。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、この草案に対して部分的な変更（詳細の追加・削除・変更）を行い、出題します。

第 62 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

2024 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、下欄の座席番号および競技者氏名を記入すること。
- ✓ 各種マニュアルや印刷物、記憶媒体の持ち込みは一切認めない。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技時間内に作業が終了した場合、CML シミュレーションおよび各仮想マシンは起動したままの状態とし、競技委員に申し出て退席許可を得ること。
- ✓ 競技終了の合図で、直ちに作業を終了すること。
- ✓ 本課題冊子は持ち帰り厳禁である。机上に置いたまま退席すること。

座席番号	競技者氏名

1　競技課題に関する注意事項

- ✓ 競技終了時に指定された設定が各ネットワークノードに保存されていること。
- ✓ ESXi ホストの管理画面に接続することは許可しない。
- ✓ CML の web インターフェースへ接続することは許可しない。
- ✓ 競技課題文書はシステム構築のための手順書ではないことに注意する必要がある。課題中に設定する値や設定項目に関する具体的な指定がない場合は、競技者が自身で判断して仕様を満たす設定を行う必要がある。
- ✓ ネットワーク技術は階層的に規定されている。多くの場合、個々の技術は基盤となる他の技術上で実行することを前提としている。あなたがそのような技術階層の途中で課題の指示通りの解決策を考えつくことができなかったとしても、それは残りの課題が全く採点されないというわけではないことを理解することが重要である。例えば、課題の指示通りの動的ルーティングを設定することができなくても、スタティックルートを使用することによって、その上で実行される全てのものの作業を継続することができる。また、VPN について課題の指示通りの構成を設定することができなくても、代替となるよりシンプルなトンネル接続を採用することができる。この場合、課題の要求を満たせなかった部分に対する得点は与えられないが、その基盤技術の上で実行される上位階層技術の機能テストに成功すれば、その部分に対する得点は与えられる。

1　競技課題の背景

あなたはネットワークシステムの構築を専門とする企業のエンジニアである。ある企業のネットワークシステムの更改業務を受注し、そのプロジェクトリーダーとなった。ネットワークの設計は既に完成している。これをもとに検証用のネットワーキング環境を構築する。

1.1.　構築ネットワークの概要

図１に示すように、構築対象となるネットワークには DataCenter/SkyExpo/Branch1/Branch2 の各拠点があり、それらがインターネット(isp)に接続している。

DataCenter には dc-srv1 が接続する内部セグメントと dc-srv2 が接続する公開サーバーセグメント(DMZ)がある。SkyExpo/Branch1/Branch2 にはそれぞれクライアントセグメントがある。これら各拠点が接続する検証用のインターネットゾーンには、isp/isp-srv が接続している。

DataCenter/SkyExpo 拠点間の接続はインターネット（isp）経由の IPsecVPN によって到達性とセキュリティを確保する。SkyExpo/Branch1/Branch2 間は DMVPN によって接続する。詳細については、以降の本文および別添ネットワーク構成図表に示す。

競技における設定対象は、各ネットワークノード(isp, dcsw1, dcfw1, trustsw, br1,br2, skyexp)とサーバー・クライアント(dc-srv1, dc-srv2, dc-cl)である。

その他（isp-srv, skyexp-cl, br1-cl, br2-cl）は設定済みであり設定変更は許可しない。dmzsw については管理機能なしスイッチノードであり設定不要である。

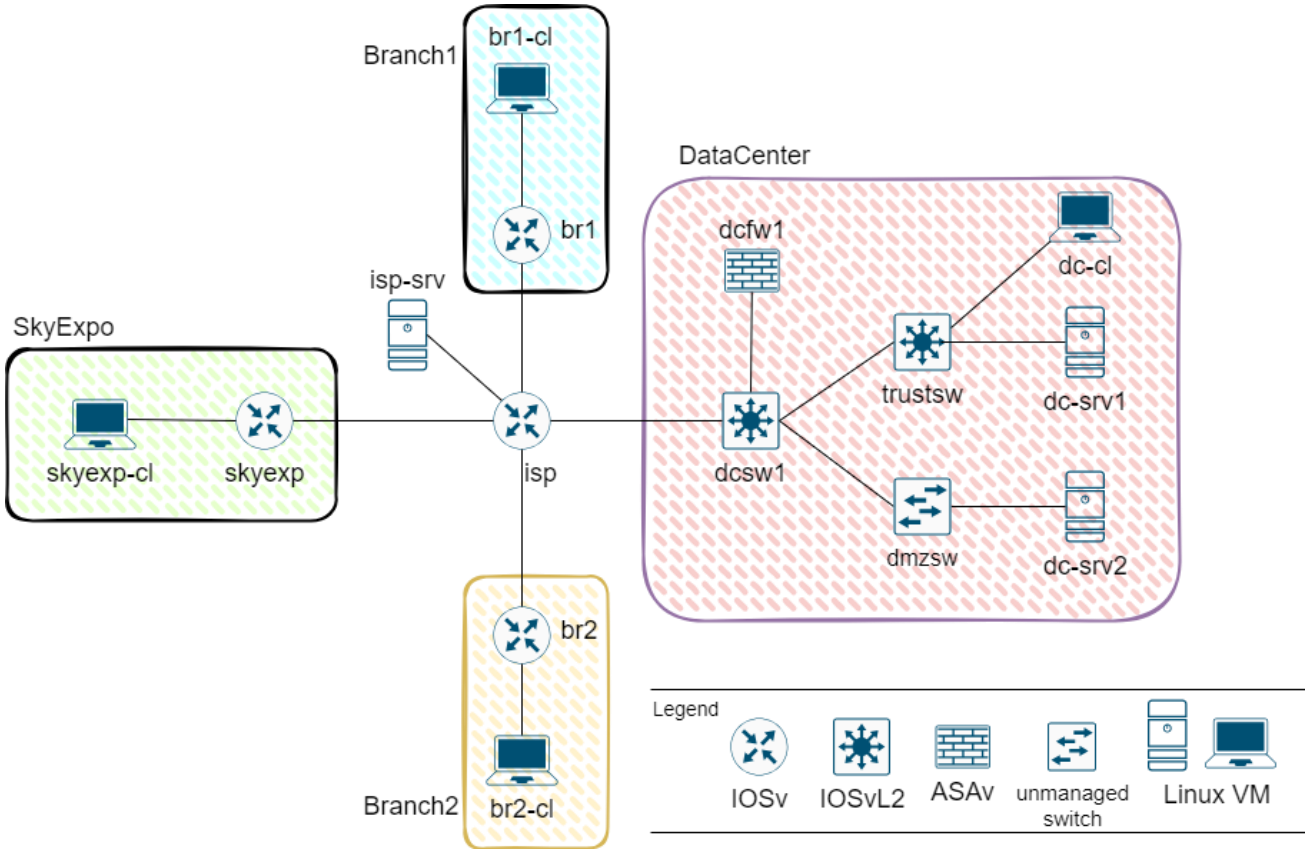


図１　ネットワークサイト構成

2 仮想マシンに関する基本情報

2.1. 仮想マシン dc-srv1, dc-srv2 について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Debian12.5 がインストールされており、初期インストールにおいて「Debian デスクトップ環境」、「標準システムユーティリティ」と「SSH サーバー」が選択されインストールされた状態となっている。下表の初期設定状態となっている。**パスワードの変更は禁止する。**

Debian12.5 がプリインストールされている仮想マシンに対して、上書きで Debian12.5 を新規インストールすることは可能であるが、それによって発生したトラブルについて競技委員側では対処しない。

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

2.2. isp-srv, br1-cl, br2-cl, skyexp-cl について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Debian がインストールされており**アドレス設定済み**である。動作確認のための**一般ユーザアカウントでのログインは許可する。管理者アカウントでのログインおよび設定変更は許可しない。**

共通設定

一般ユーザアカウント名	master
一般ユーザのパスワード	pass

2.3. 仮想マシン dc-cl　について

仮想マシンは作成済みであり、シミュレーションネットワークに配置されている。また、Windows10 が既にインストールされている。管理者アカウントとして user（パスワード無し）が設定されている。パスワードの変更は禁止する。

2.4. 仮想マシン isp-srv について

インターネット（想定）上に isp-srv（ホスト名: ns.itnetsys.org）が設置されている。下記のサービスが稼働している。自身の動作確認のためにこれらのサービスへアクセスしてよい。

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

3 各ノードへの接続方法

3.1. 各仮想マシンへの接続について

各仮想マシンに接続するための vmrc ショートカットは、管理用 PC デスクトップ上のフォルダ shortcuts 内のフォルダ VM にある。仮想マシン名と同名のショートカットアイコンをダブルクリックしてアクセス可能である。

3.2. 各ネットワークノードへの接続について

各ネットワークノードのコンソールにアクセスするための Teraterm ショートカットは、管理用 PC デスクトップ上のフォルダ shortcuts 内のフォルダ NET にある。ノード名と同名のショートカットアイコンをダブルクリックし、ターミナル起動後、「Enter」キーを押すことで応答する。

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

4 その他の基本情報

4.1. Debian12.5 isoイメージについて

管理用 PC のデスクトップ上に“debian_iso”フォルダがあり、Debian 12.5 の iso ファイルが置かれている。VMware Remote Console のメニューにおいて「VMRC(V)」→「取り外し可能デバイス(R)」→「CD/DVD ドライブ１」→「ディスクイメージファイル(iso)に接続(C)…」を選択し、iso イメージをマウント可能である。

5 Cisco ネットワークノード設定課題

別添ネットワーク構成図表および以降の設定項目に従い、ネットワークノード（dcfw1/dcsw1/trustsw/skyexp/br1/br2/isp）を設定し、別添ネットワーク構成図表・表２に示す所定の IP 到達性を確保しなさい。設定項目は、ネットワーク構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。また、設定項目として明記されていなくても、競技課題の仕様上必要ならば、各自の判断で設定追加すること。

5.1 基本設定

以下の通り基本設定を行いなさい。※dcfw1 のイネーブルパスワードは skillspass が設定されている。その他のネットワークノードについてはパスワードを設定しない。

1. 別添ネットワーク構成図表・表１に従い各インターフェースに IP アドレスを設定する。

2. 全ネットワークノードについて、タイムゾーンを日本標準時に設定する。

5.2　サービス

以下の通り各種サービス設定を行いなさい。

1. isp を NTP サーバーとして動作させる。
   A) dcsw1/skyexp/br1/br2 について、NTP サーバーとして isp(9.9.9.9)を指定し、時刻同期すること。

2. isp を DHCP サーバー、br2 を DHCP クライアントとして以下の通り動作させる。
   A) isp は DHCP サーバーとして動作し、200.99.22.0/24 のアドレス帯を配布する。
   B) br2 は、DHCP クライアントとなり、Gi0/0 のアドレスを動的に取得すること。

   ※留意点：この設定が不可能な場合でも、br2 の Gi0/0 について 200.99.22.0/24 のアドレス帯にて静的にアドレス設定することで課題を継続できる。

3. isp を PPPoE サーバー、br1 を PPPoE クライアントとして以下の通り動作させる。
   A) isp にローカルユーザ（ユーザ名 chapuser01　パスワード skillspass）を登録し、br1 の認証に使用する。認証方式は chap とする。
   B) isp は、認証成功時に IP アドレス 200.99.11.1/32 をクライアントへ払い出す。

   ※留意点：この設定が不可能な場合でも、br1/isp 間のリンクについて 200.99.11.0/30 のアドレス帯にて静的にアドレス設定することで課題を継続できる。

4. SkyExpo 拠点内セグメント(172.17.1.0/24)からのインターネットゾーンとの接続について、skyexp にて NAPT を適用する。外側のインターフェースのアドレスに変換されること。

5.3 スイッチング

以下の通り各種スイッチ設定を行いなさい。

1. dcsw1/trustsw の VTP モードはトランスペアレントとする。

2. dcsw1 には、次の通り VLAN を定義する。
   A) VLAN 10 (VLAN 名 UNTRUST)
   B) VLAN 20 (VLAN 名 DMZ)
   C) VLAN 30 (VLAN 名 TRUST)

3. dcsw1/trustsw における各 VLAN について、別添ネットワーク構成図表・表３の通り、アクセスポートを設定する。必要な VLAN 定義は追加すること。

5.4 ファイアウォールセキュリティ

dcfw1 において、以下の通り各種ファイアウォール設定を行いなさい。

1. 別添ネットワーク構成図表・表 1 に示す通り、dcfw1 の Gi0/0 にサブインターフェースを作成する。
   A) Gi0/0.10(インターフェース名 UNTRUST)はセキュリティレベルが低く、Gi0/0.30(インターフェース名 TRUST)はセキュリティレベルが高くなること。Gi0/0.20(インターフェース名 DMZ)はその中間のセキュリティレベルとなること。

2. VLAN101(10.0.101.0/24)からのインターネットゾーン(UNTRUST 側)との接続について、NAPT を適用する。2.2.2.1 に変換されること。

3. dc-srv2 をインターネットゾーン(UNTRUST 側)と相互接続可能とするために、スタティック NAT を適用する。2.2.2.5 にて接続が行えるようにすること。
   A) dc-srv2 の IP アドレスをインターネットゾーン(UNTRUST 側)へ返す DNS 応答について、dc-srv2 の実アドレスではなく変換アドレス 2.2.2.5 を返すこと。(DNS 応答パケット内の埋め込み IP アドレスを書き換える)

4. ICMP インスペクションを有効にする。

5.5　アンダーレイ　ルーティング

アンダーレイネットワークにおけるルーティング設定を以下の通り行い、インターネットゾーンへの到達性を確保しなさい。

1. 静的経路(IPv4)を次の通り登録する。
   A) dcfw1/trustsw/br1 において、適切なデフォルトルートを静的に登録する。
   B) dcfw1 において、DataCenter 拠点内(trsutsw 接続 VLAN)への経路を静的に登録する。
   C) dcsw1 において、2.2.2.0/28 への経路を静的に登録する。

2. 別添ネットワーク構成図表・図４の BGP ルーティング概要に従い、次の通り BGP を動作させる。
   A) isp を AS 番号 9500、dcsw1 を AS 番号 65000 として、eBGP ピアを確立する。
   B) isp を AS 番号 9500、skyexp を AS 番号 65001 として、eBGP ピアを確立する。
   C) isp は、自身をデフォルトルート先とする経路を eBGP ピアへアドバタイズする。
   D) dcsw1 は、ピアに対して 2.2.2.0/28 の経路情報をアドバタイズする。
   E) skyexp は、ピアに対して 4.4.4.4/32 の経路情報をアドバタイズする。

5.6 VPN

トンネルによる拠点間接続を以下の通り動作させなさい。

1. 別添ネットワーク構成図表・表 1 および図３(1)に示す通り、dcfw1/skyexp 間において、トンネルインターフェース Tunnel0 を動作させる。
   A) dcfw1 における Tunnel0 のインターフェース名は VTI とする。
   B) IPsec によってセキュリティを確保する。

2. 別添ネットワーク構成図表・表 1 および図３(2)に示す通り、skyexp/br1/br2 間において、トンネルインターフェース Tunnel1 を動作させる。
   A) skyexp をハブルータ、br1/br2 をスポークルータとする DMVPN を構成する。
   B) IPsec によってセキュリティを確保する。

※留意点：これらの指示通りのトンネル構成が不可能な場合であっても、あなたが設定可能なトンネル構成を採用することで拠点間の到達性を確保できるならば、課題を継続できる。

5.7　オーバーレイ　ルーティング

オーバーレイネットワークにおけるルーティング設定を以下の通り行い、全ての拠点間の通信を可能としなさい。

1. 別添ネットワーク構成図表・図５に拠点間ルーティング概要を示す。DataCenter と他拠点間の通信を可能とするために静的経路(IPv4)を次の通り登録する。
   A) SkyExpo/Branch1/Branch2 の各拠点内について、クラス B のプライベートアドレス帯を割り振るものとする。dcfw1 において、SkyExpo/Branch1/Branch2 拠点内への経路を静的に登録する。
   B) skyexp において、DataCenter 拠点内への経路を静的に登録する。

2. 別添ネットワーク構成図表・図５に拠点間ルーティング概要を示す。全ての拠点間における IPv4 セグメントの通信を可能とするために EIGRP を次の通り動作させる。
   A) skyexp/br1/br2 にて EIGRP を動作させる。
   B) 各 EIGRP ルータは別添ネットワーク構成図表・図５に示す集約アドレスをアドバタイズする。

5.8　IPv6 ルーティング

IPv6 ルーティング設定を以下の通り行い、IPv6 セグメント間の通信を可能としなさい。

1. trustsw に接続している VLAN101(2001:db8:101::/64)及び VLAN250(2001:db8:250::/64)について、セグメント間の IPv6 通信を可能とすること。

6 Linux サーバー設定課題

以下の設定項目に従い、Linux サーバー仮想マシン（dc-srv1，dc-srv2）を設定しなさい。設定項目は、サーバー構築に最適な順序で記述されているとは限らない。どのような順序で設定を行うかは、選手自身の判断となる。

6.1. dc-srv1 の設定

以下の通り、dc-srv1 を動作させなさい。

1. 基本設定
   A) 別添ネットワーク構成図表・表 1 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
   B) ネームサーバアドレスとして dc-srv2 を参照する。
   C) システムアカウント smbuser を作成する。パスワードは pass とする。

2. RAID
   A) 使用するパッケージは mdadm とする。
   B) ハードディスク sdb と sdc を用いて RAID1 を構築する。
   C) RAID ディスクを/mnt/raid1 へマウントする。

3. Samba サーバー
   A) 使用パッケージは samba とする。
   B) /mnt/raid1/share を共有ディレクトリとする。共有名は share とする。

6.2. dc-srv2 の設定

以下の通り、dc-srv2 を動作させなさい。

1. 基本設定
   A) 別添ネットワーク構成図表・表 1 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
   B) ネームサーバアドレスとして自身を参照する。

2. DNS サーバー
   A) 使用するパッケージは bind9 とする。
   B) DNSSEC の検証は無効にする。
   C) skills.it.jp ドメインのマスタサーバーとして動作させる。
   D) www.skills.it.jp の正引き問い合わせに対して、dc-srv2 の IPv4 アドレスを応答する。
   E) dc-srv2 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、
      isp-srv(200.99.1.1)へ回送する。
   F) 競技課題の仕様から必要となるレコードは、各自の判断で追加すること。

3. Web サーバー
   A) 使用するパッケージは nginx とする。
   B) Web ブラウザからの https://www.skills.it.jp へのアクセスに対して、文字列「www.skills.it.jp」を表示すること。

7 クライアント設定課題

以下の設定項目に従い、クライアント を設定しなさい。

7.1. dc-cl の設定

以下の通り、dc-cl を動作させなさい。

1. 基本設定
   A) 別添ネットワーク構成図表・表 1 に従い IP 設定を適切に行い、ネットワーク接続を可能とすること。
   B) ネームサーバアドレスとして dc-srv2 を参照する。

2. Samba クライアントの設定
   A) ユーザ smbuser、パスワード pass を用いて、dc-srv1 の/mnt/raid1/share を Z:ドライブに割り当てる。

3. Web ブラウザの動作
   A) https://www.skills.it.jp のページが表示でき、証明書エラーが表示されない。
   B) isp-srv 上の Web サイト https://www.itnetsys.org のページが表示できる。

第６２回　技能五輪全国大会
ITネットワークシステム管理
選考会

別添ネットワーク構成図表

表1：ネットワークノードIPアドレス設定表

各ネットワークノードのIPアドレス設定値は、次の通りである。赤字のノードは設定済みである。

ノード名	インターフェース	IPアドレス
isp	Gi0/0	1.1.1.1/30
	Gi0/1	1.1.1.5/30
	Gi0/2	unassigned
	Gi0/3	200.99.22.254/24
	Gi0/4	3.3.3.1/29
	Gi0/5	200.99.1.254/24
	Loopback0	9.9.9.9/32
br1	Gi0/0	unassigned
	Gi0/1	172.18.1.254/24
	Dialer0	動的(PPPoE)
	Tunnel1	172.16.101.2/24
br2	Gi0/0	動的(DHCP)
	Gi0/1	172.19.1.254/24
	Tunnel1	172.16.101.3/24
skyexp	Gi0/0	3.3.3.2/29
	Gi0/1	172.17.1.254/24
	Loopback1	4.4.4.4/32
	Tunnel0	172.16.100.2/24
	Tunnel1	172.16.101.1/24
dcfw1	Gi0/0.10 インターフェース名 UNTRUST	10.0.10.254/24
	Gi0/0.20 インターフェース名 DMZ	10.0.20.254/24
	Gi0/0.30 インターフェース名 TRUST	10.0.30.254/24
	Loopback0 インターフェース名 LP0	2.2.2.14/32
	Tunnel0 インターフェース名 VTI	172.16.100.1/24

各サブインタフェースは、サブインタフェース番号と同一のVLANIDのVLANに所属するものとする。

ノード名	インターフェース	IPアドレス
dcsw1	Gi0/0	1.1.1.2/30
	Vlan10	10.0.10.251/24
trustsw	Vlan30	10.0.30.252/24
	Vlan101	10.0.101.254/24 2001:db8:101::254/64
	Vlan250	10.0.250.254/24 2001:db8:250::254/64
isp-srv		200.99.1.1/24
dc-cl		10.0.101.1/24 2001:db8:101::1/64
dc-srv1		10.0.250.1/24 2001:db8:250::1/64
dc-srv2		10.0.20.1/24
skyexp-cl		172.17.1.1/24
br1-cl		172.18.1.1/24
br2-cl		172.19.1.1/24

表2：本課題で要求される各端末間のIP到達性

（1） IPv4到達性

要求側＼応答側	dc-srv1	dc-srv2	skyexp-cl	br1-cl	br2-cl	isp-srv	dc-cl
dc-srv1		○	○	○	○	○	○
dc-srv2	×		○	○	○	○	×
skyexp-cl	○	○		○	○	○	○
br1-cl	○	○	○		○	×	○
br2-cl	○	○	○	○		×	○
isp-srv	×	TCP443,53 UDP53のみ可	×	×	×		×
dc-cl	○	○	○	○	○	○	

（2） IPv6到達性

要求側＼応答側	dc-srv1	dc-cl
dc-srv1		○
dc-cl	○	

○：要求側から応答側への到達性が確保され、正常に応答が返る。
×：要求側から応答側への通信は確立しない。
～のみ可：フィルタリングによって限定的な接続のみ可能とする。

表3： VLANアクセスポート設定表

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	DMZ	Gi1/1	10.0.20.0/24	DMZセグメント
30	TRUST	Gi1/0	10.0.30.0/24	信頼ゾーン接続セグメント

trustsw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
30	TRUST	Gi0/0	10.0.30.0/24	信頼ゾーン接続セグメント
101	USER01	Gi0/1	10.0.101.0/24 2001:db8:101::/64	ユーザセグメント
250	SERVER	Gi0/2	10.0.250.0/24 2001:db8:250::/64	内部サーバーセグメント

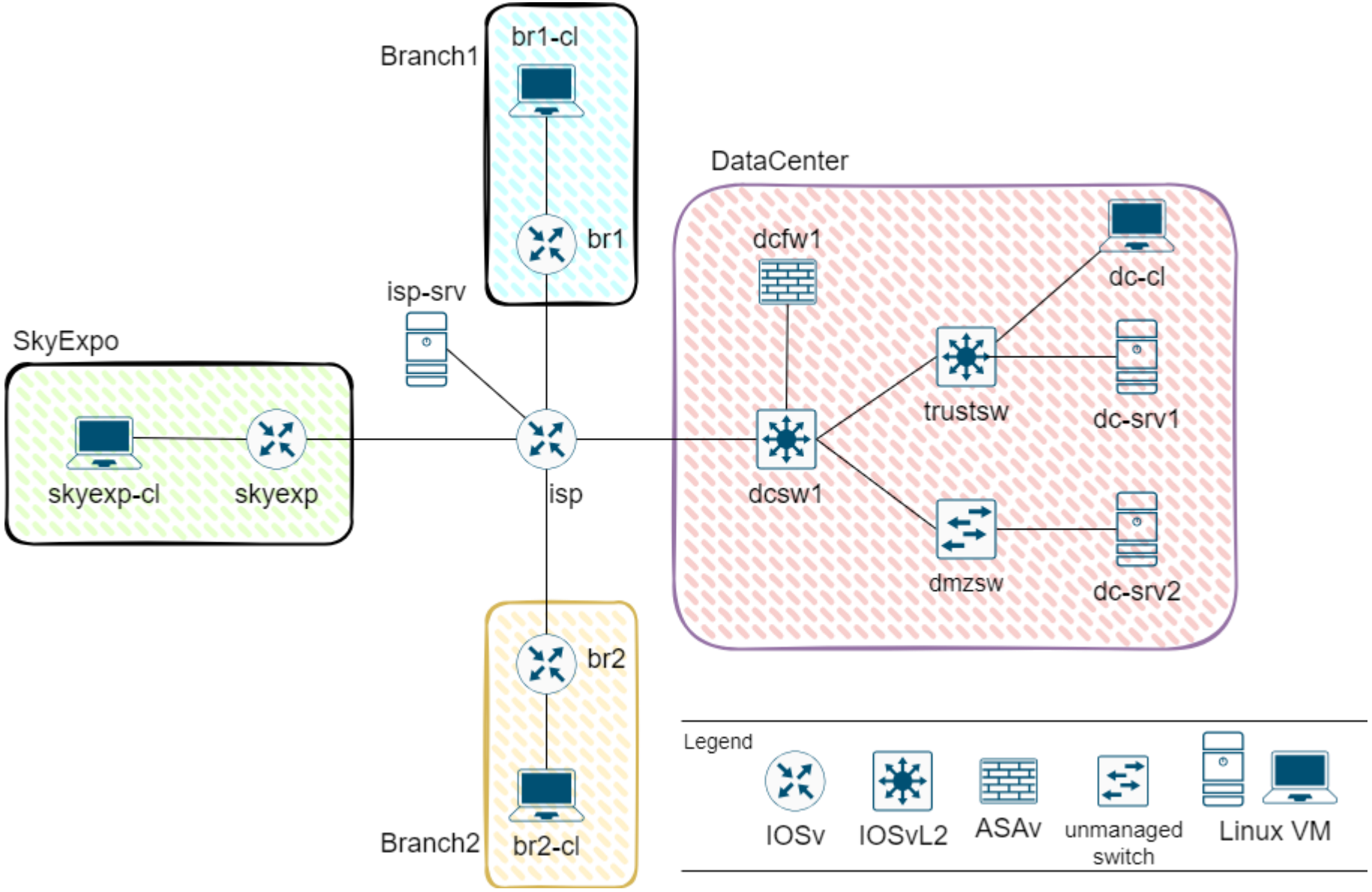
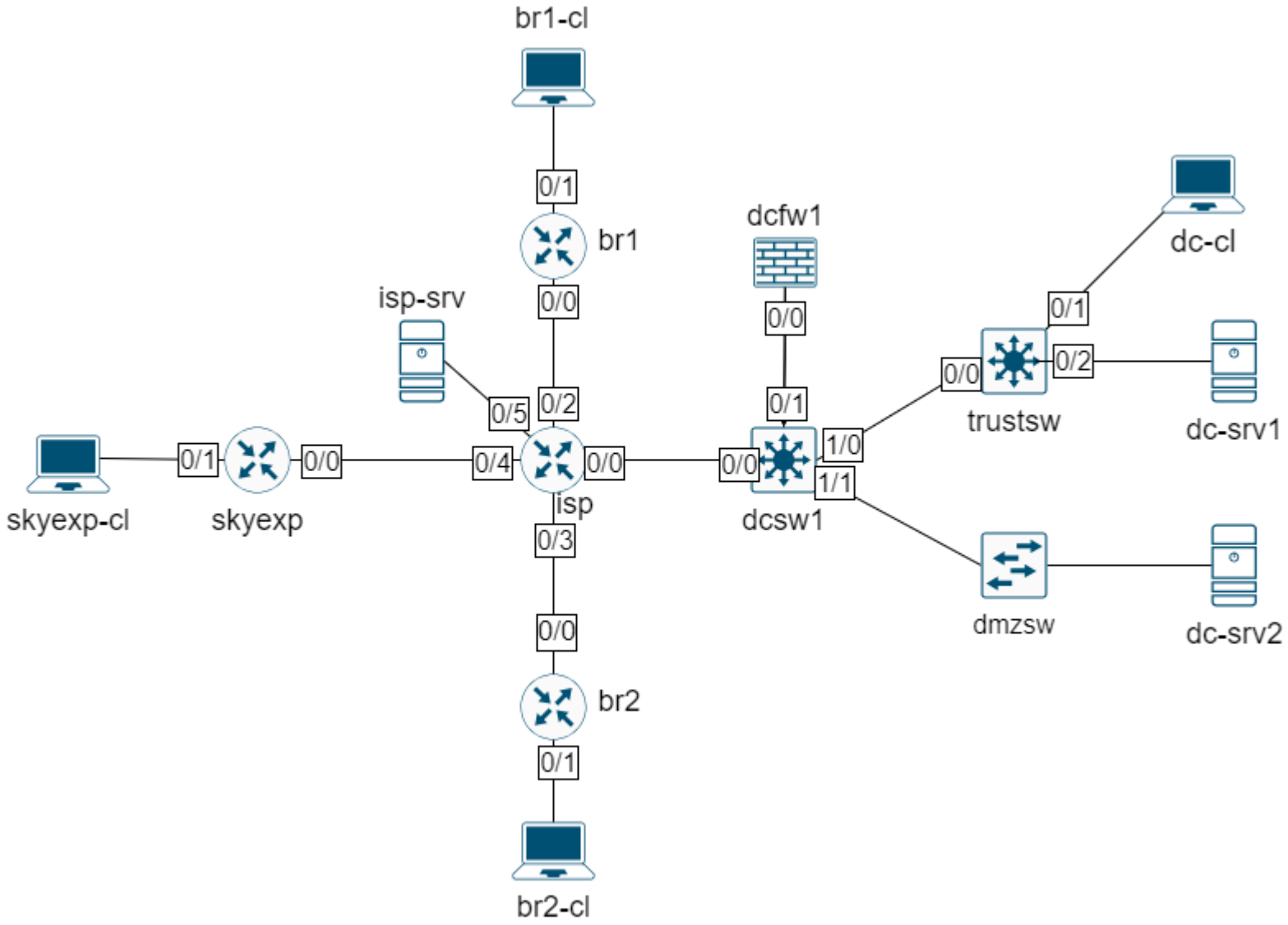
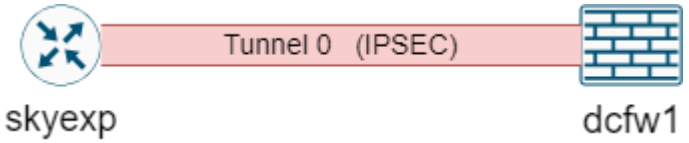


図1：ネットワークサイト構成

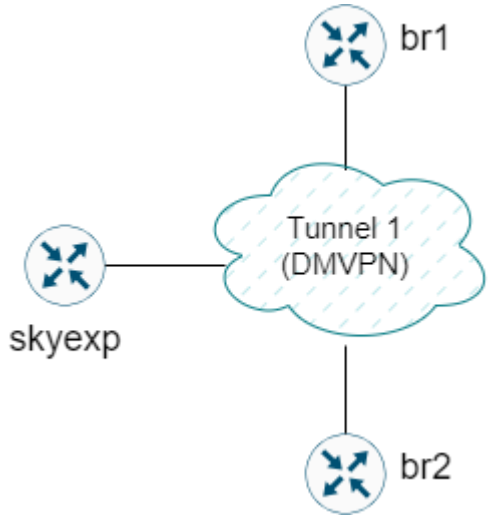


※本図に各ノードの接続インターフェース番号を示す。
使用インタフェースは全てGigabitEthernetである。
（0/0の表記は、GigabitEthernet0/0の略記）

図2：インターフェース接続構成



（1） skyexp/dcfw1間IPSEC（Tunnel0）



（2） skyexp/br1/br2間DMVPN（Tunnel1）

図3 トンネル構成概要

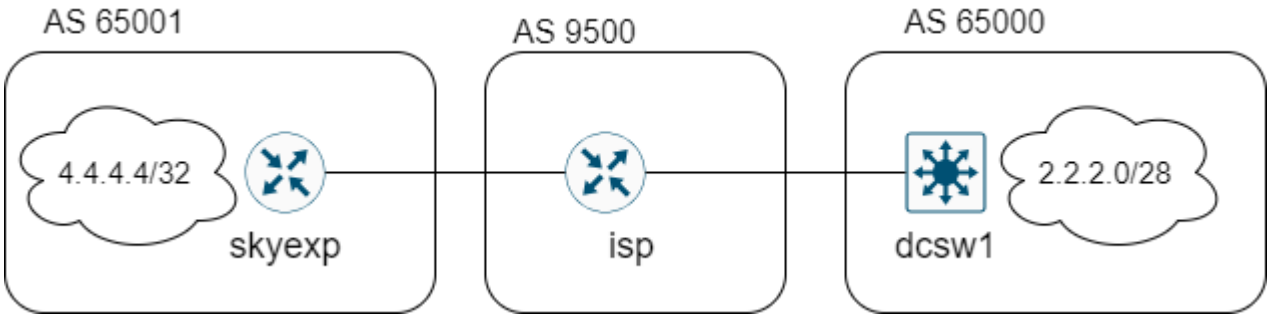


図4：BGPルーティング概要

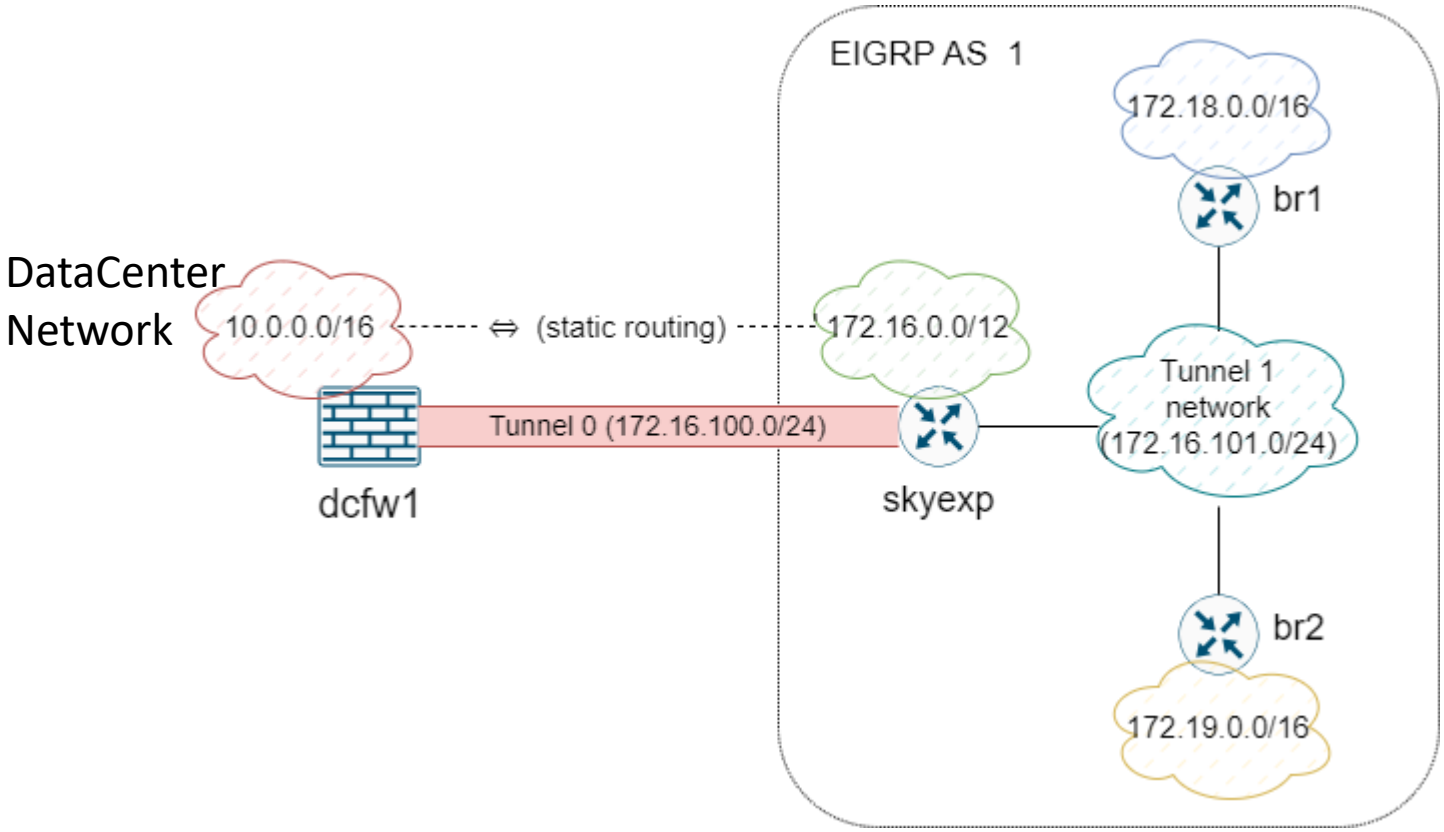


図5：拠点間ルーティング概要