

第16回 若年者ものづくり競技大会

IT ネットワークシステム管理

競技課題

2021年8月5日(木) 9:00～13:00(4時間)

目次

競技に関する注意事項	P.1
競技課題の背景と概要	P.2
競技環境(仮想環境)に関する注意事項	P.3～P.4
競技課題	P.5～P.9

競技に関する注意事項:

- ✓ 競技開始の合図まで本冊子を開かないこと。
- ✓ 携帯電話の電源はあらかじめ切っておくこと。
- ✓ 本課題冊子を綴じてある留め金は外さないこと。
- ✓ 競技が開始されたら、下欄の座席番号及び競技者氏名を記入すること。
- ✓ 各種マニュアルや印刷物、記憶媒体の持ち込みは一切認めない。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技課題の仕様を満たすならば、どのような設定を行っても構わない。課題中に設定する値や設定項目の指定がない場合は、競技者が自身で判断して仕様を満たす設定を行うこと。
- ✓ 競技課題に記述がない項目に関しては採点対象としない。
- ✓ 競技時間内に作業が終了した場合は、競技委員に申し出て退席許可を得ること。
- ✓ 競技終了の合図で、直ちに作業を終了すること。
- ✓ 本課題冊子及び別紙は持ち帰り厳禁である。机の上に置いたまま退席すること。

座席番号	競技者氏名

競技課題の背景と概要

あなたはサーバやネットワークを構築・運用管理する IT 企業に勤務している。今回、ある企業のネットワークシステムの更改業務を受注し、あなたがそのプロジェクトに携わることになった。ネットワークの設計やサーバの構築内容は既に完成している。

構築するネットワークシステムは「alpha」と「bravo」の 2 つの事業所ネットワークで構成され、ルータ「ISP」を経由して「仮想インターネットエリア」に接続されている(別紙図 1「ネットワーク構成図」参照)。

1. 「alpha」事業所

ルータ 2 台、ハブ 3 台のネットワーク機器、サーバ PC 2 台、及びクライアント PC 1 台で構成する。

「alpha」事業所では、自分以外のネットワークを「外部ネットワーク」と呼ぶ。

- ・サーバ PC「asv1」は Linux OS で構築済みであり、下記のサービスが稼働している。各自の設定確認のためにこれらのサービスを利用して構わない。
 - A) DNS サービスが稼働しており、「外部ネットワーク」から、`www.test.jp` の正引き要求に応答する。また、「alpha」事業所内から、`asv1.youth-skills.jp`、`asv2.youth-skills.jp` の正引き要求に応答する。
 - B) Web サービスが稼働しており、80 番ポートへの接続要求に応答する。
 - C) FTP サービスが稼働しており、21 番ポートへの接続要求に応答する。
- ・サーバ PC「asv2」は Linux OS で構築済みであり、Web、TFTP のサービスが稼働している。これらサービスの用途は課題で指示する。
- ・クライアント PC「a-clinet」は Window 10 がインストール済みである。各自の設定確認のために利用して構わない。

2. 「bravo」事業所

ルータ 1 台、ハブ 2 台のネットワーク機器、サーバ PC 2 台、及びクライアント PC 1 台で構成する。

「bravo」事業所では、自分以外のネットワークを「外部ネットワーク」と呼ぶ。

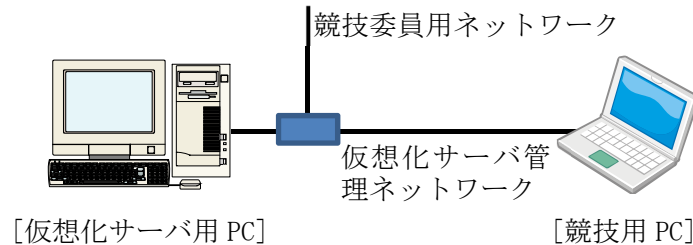
- ・ルータ「br」は、インタフェース等の必要な項目は設定済みである。また、「外部ネットワーク」と通信するために、サーバ PC「bsv1」の IP アドレスを 201.10.0.125 へ静的に変換する NAT が設定済みである。ただし、アクセス制御は未設定である。
- ・公開用「bsv1」、内部用「bsv2」の 2 台のサーバ PC を Linux OS を用いて構築する。
- ・クライアント PC「b-clinet」は Window 10 がインストール済みである。

3. 「仮想インターネットエリア」

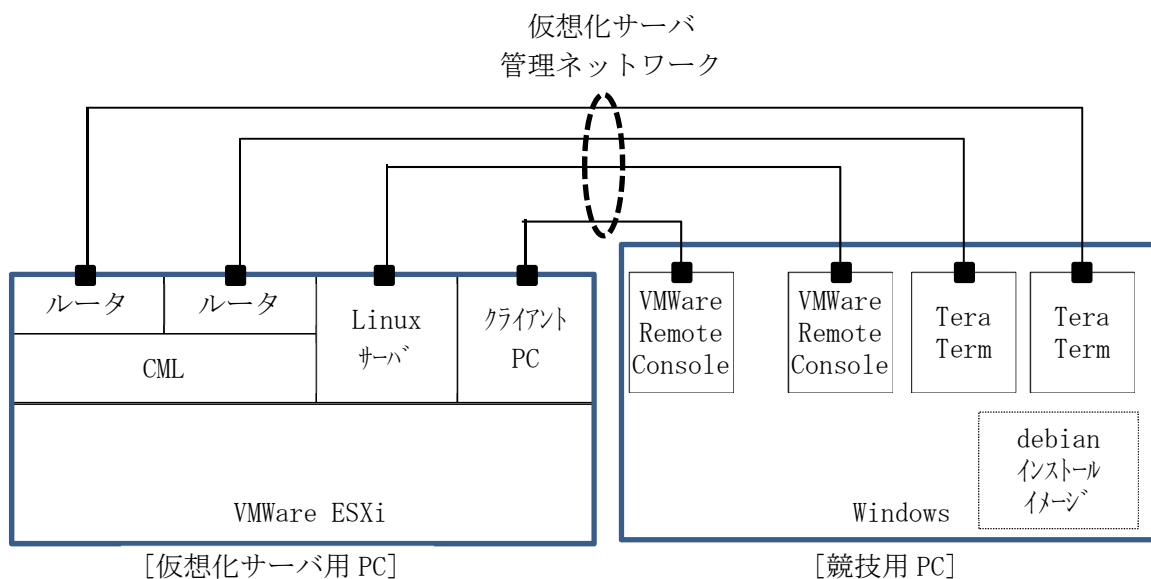
- ・検証用サーバ「sv」では下記のサービスが稼働している。各自の設定確認のためにこれらのサービスを利用して構わない。
 - A) DNS サービスが稼働しており、`sv.itnetsys.org`、`www.itnetsys.org`、`www.game.tv` の正引き要求に応答する。また、`itnetsys.org` ドメインの MX レコードが登録されている。
 - B) Web サービスが稼働しており、`http://www.itnetsys.org`、`http://www.game.tv` のリクエストに応答する。
 - C) SMTP サービスが稼働しており、`manager@itnetsys.org` 宛のメールを受信可能である。また、この受信メールに対して Subject「Auto Reply Mail」の空メールが自動返信される。
- ・検証用クライアント「Ex-clinet」は Window 10 がインストール済みである。各自の設定確認のために利用して構わない。

競技環境(仮想環境)に関する注意事項

競技で使用する PC 等の配置、役割は以下の通りである。



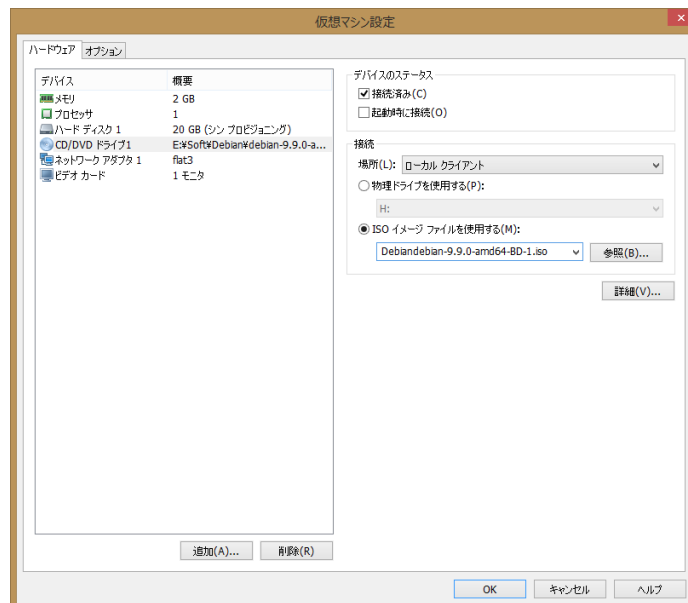
- [競技用 PC]には、競技に必要なネットワーク設定がされている。このネットワーク設定変更を禁止する。
- 「競技委員用ネットワーク」は競技委員が採点等で利用するネットワークであり、競技には使用しない。
- [仮想化サーバ用 PC]の直接操作を禁止する。



- [仮想化サーバ用 PC]にはホスト OS として VMWare ESXi がインストールされている。
- VMWare ESXi のゲスト OS として CML(Cisco Modeling Labs)、クライアント PC(「a-client」、「b-client」、「Ex-client」)として Windows10、及びサーバ PC(「sv」、「asv1」、「asv2」)として Debian Linux 10.9 がインストール済みである。サーバ PC(「bsv1」、「bsv2」)はディスク領域のみが確保されており、OS は未インストール状態である。
- サーバ PC、クライアント PC は VMWare Remote Console を用いて操作を行う。
- VMWare Remote Console のショートカットは、デスクトップの「ショートカット」フォルダ内にある。このショートカットのプロパティ(リンク等)変更を禁止する。
- 「VMWare Remote Console」による接続には下記のユーザ名、パスワードを用いる。

ユーザ名	young
パスワード	ehimeR03

- すべてのサーバ PC、クライアント PC は競技開始時に電源 ON の状態である。
- 「a-clinet」、「b-clinet」、「Ex-clinet」には、標準アプリケーション以外に「Tera Term」、「Mozilla Thunderbird」がインストール済みである。
- CML には別紙図 1「ネットワーク構成図」に示す各ノード(「aR1」、「aR2」など)の配置、及び接続が設定済みであり、競技開始時に各ノードは電源 ON の状態である。
- ルータ「aR1」及び「aR2」は、[競技用 PC]にインストールされている「Tera Term」を用いて接続し、設定、操作を行う(この接続は、ルータ実機へのコンソール接続と同等である)。[競技用 PC]のデスクトップの「ショートカット」フォルダ内に各ルータへ接続する「Tera Term」のショートカットが用意されている。このショートカットのプロパティ(リンク等)変更を禁止する。
- ローカル、リモートにかかわらず、VMWare ESXi の直接操作を禁止する。
- ローカル、リモートにかかわらず、サーバ PC「asv1」、「asv2」、及び検証用サーバ「sv」へのコンソールログインを禁止する。
- ルータ「ISP」、「bR」の操作を禁止する。
- debian のインストールイメージ(debian-10.9.0-amd64-BD-1.iso)は[競技用 PC]のデスクトップ上にある。「bsv1」及び「bsv2」のインストール時に、以下の操作を行う。
 - ① 「bsv1」または「bsv2」操作のショートカットから VMWare Remote Console を起動。
 - ② メニュー[VMRC(V)]-[管理(M)]-[仮想マシン(S)...]を選択。



- 接続済み(C)
- 場所(L): [ローカルクライアント]
- ISO イメージファイルを使用する(M)
- [参照(B)...]ボタンから、
デスクトップにある ISO イメージを選択

- ③ メニュー[VMRC(V)]-[<Ctrl>+<Alt>+<Delete>の送信(C)]を選択し、仮想マシンを再起動する。
- 「bsv1」及び「bsv2」の仮想マシンで、CD/DVD 以外のハードウェア構成及びオプション項目は競技委員により設定済みである。これらの設定変更を禁止する。

※「b-client」、「bsv1」、及び「bsv2」の仮想マシンは、競技終了後に再起動し採点を行う。

競技課題

以降の設定内容を良く読み、ネットワーク機器の設定、サーバ PC の構築、クライアント PC の設定を行い、顧客事業所のシステムを構築しなさい。

※採点対象は、ルータ「aR1」、「aR2」、サーバ PC「bsv1」、「bsv2」、クライアント PC「b-client」のみである。

「alpha」事業所

サーバ PC「asv1」、「asv2」は構築済みである。ルータ「aR1」、「aR2」の設定を行いなさい。

【ルータの設定】

1. 「aR1」、「aR2」の共通設定

1.1. ホスト名、パスワード

以下の表に示す各ルータのホスト名、コンソールパスワード及びイネーブルパスワードは、競技委員により設定済みである。これらの設定変更を禁止する。

ホスト名	コンソールパスワード	イネーブルパスワード
aR1	cisco	cisco
aR2	cisco	cisco

1.2. ターミナル環境

各ルータのターミナル環境を以下の通り設定しなさい。

- ・コマンド誤入力による DNS 検索を行わない。
- ・タイムゾーンを JST に設定する。
- ・コンソール接続時、自動ログアウト機能を無効にする。
- ・コンソール接続時、表示割り込みに対する入力文字列の補完を有効にする。
- ・コンソール接続時、常に特権モードでのアクセスを可能にする。

1.3. インタフェイスの設定

別紙表 1 に基づき各ルータのインタフェイスに IP アドレスを設定しなさい。

1.4. 経路制御

各ルータにデフォルトルートを設定しなさい。

2. 「aR1」の設定

2.1. 経路制御

192.168.1.0、192.168.2.0 ネットワークとの通信に必要となる静的ルートを設定しなさい。

2.2. アドレス変換

以下のとおり、NAT 及び NATPT を設定しなさい。

- ・「外部ネットワーク」と通信するために、192.168.1.0、192.168.2.0 ネットワーク内ノードの送信元 IP アドレスを 201.10.0.3 へ動的に変換する。
- ・「外部ネットワーク」と通信するために、「asv1」の IP アドレスを 201.10.0.2 へ静的に変換する。

2.3. アクセス制御

Gi0/0 インタフェイスに以下のとおりアクセス制御を設定しなさい。

A) 着信トラフィック

- ・ 発信トラフィックの戻りトラフィックを許可する。
- ・ 「aR1」、「asv1」への ICMP トラフィックを許可する。
- ・ 「asv1」上の DNS サービス及び Web サービスへのトラフィックを許可する。
- ・ 上記以外は許可しない。

B) 発信トラフィック

- ・ 「asv1」からの発信トラフィックを許可する。
- ・ NAPT された発信トラフィックを許可する。

3. 「aR2」の設定

3.1. DHCP サーバの設定

192.168.2.0 ネットワークへのサービスを以下のとおり設定しなさい。

- ・ 192.168.2.101～200 の IP アドレスを配布する。
- ・ 優先 DNS サーバとして「asv1」のアドレスを配布する。
- ・ デフォルトゲートウェイのアドレスを配布する。

3.2. ログの保存

- ・ ログメッセージを syslog サーバ(「asv2」)へ出力しなさい(少なくとも、ネットワークインタフェイスのアップ、ダウンが記録されること)。「asv2」において、必要な項目は設定済みである。また、出力結果は、「a-client」のブラウザから <http://192.168.1.1/log/aR2.html> へアクセスすることにより確認できる(ただし、「a-client」に適切な IP アドレスが設定されていること)。

3.3. 設定ファイルの保存

- ・ 設定ファイル(running-config)を、「asv2」へ tftp を利用して aR2-config.txt の名前で保存しなさい(保存のタイミングは任意とする)。「asv2」において、必要な項目は設定済みである。また、保存結果は、「a-client」のブラウザから <http://192.168.1.1/tftp/aR2-config.txt> へアクセスすることにより確認できる(ただし、「a-client」に適切な IP アドレスが設定されていること)。

「bravo」事業所

ルータ「bR」は設定済みである。サーバ PC「bsv1」、「bsv2」、クライアント PC「b-client」の設定を行いなさい。

【サーバ PC の設定】

1. OS インストール

1.1. 「bsv1」及び「bsv2」の共通設定

Debian GNU/Linux 10.9 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
管理者パスワード	別紙表2参照
一般ユーザアカウント名	master
上記アカウントのパスワード	R3pass
IPアドレス	別紙表2参照
ネームサーバ	各サーバ自身
デフォルトゲートウェイ	各自で判断

1.2. 「bsv1」の設定

以下のとおりパーティションを構成する。ただし、ソフトウェアの仕様上、サイズが若干異なっても構わない。

マウントポイント	容量	利用方法
/boot	200MB	ext4
/	10GB	ext4
/home	4GB	ext4
/var	4GB	ext4
-	2GB	スワップ

2. その他の OS 設定及びユーザ設定

2.1. 「bsv1」及び「bsv2」の共通設定

master ユーザに sudo によるコマンドの root 権限実行を許可する。その他の一般ユーザには sudo によるコマンド実行を許可しない。

2.2. 「bsv1」の設定

下記の一般ユーザを作成する。

アカウント	パスワード	ホームディレクトリ
taro	R3pass	/home/taro

3. DNS サービスの設定

「bsv1」及び「bsv2」へ DNS サービスを以下の通り設定しなさい。

3.1. 「bsv1」及び「bsv2」共通設定

- ・使用するパッケージは「bind9」とする。
- ・回送先ネームサーバからの応答がなかった場合でも自身での反復問い合わせを行わない。
- ・DNSSEC の検証は無効にする。
- ・以降に指示が無くても、競技課題の要求仕様から登録が必要となるレコードがある場合は、各自判断して追加すること。

3.2. 「bsv1」の設定

- ・「bravo」事業所ネットワークからの問い合わせを処理する **view** を定義する。**view** 名を「**internal**」とする。
- ・「外部ネットワーク」からの問い合わせを処理する **view** を定義する。**view** 名を「**external**」とする。
- ・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、検証用サーバ「**sv**」へ回送する。
- ・再帰問い合わせは「bravo」事業所ネットワークからのみ許可する。

A) 「external」view

- ・「youth-skills.jp」ゾーンの管理を行うマスタサーバとして動作させる。
- ・「www.youth-skills.jp」の正引き問合せに対して、「bsv1」の IP アドレスを返す。

B) 「internal」view

- ・「youth-skills.jp」ゾーンの管理を行うスレイブサーバとして動作させる。
- ・「bsv2」を「youth-skills.jp」ゾーンのマスタサーバとする。

3.3. 「bsv2」の設定

- ・「bravo」事業所ネットワークからの問い合わせを処理する。
- ・「youth-skills.jp」ゾーンの管理を行うマスタサーバとして動作させる。
- ・「local.youth-skills.jp」の正引き問合せに対して、「bsv1」の IP アドレスを返す。
- ・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、「bsv1」へ回送する。

4. メールサービスの設定

「bsv1」へメールサービスを以下の通り設定しなさい。

4.1. smtp

- ・使用するパッケージは「postfix」とし、「youth-skills.jp」ドメインの **smtp** サーバとして動作させる。
- ・「bravo」事業所ネットワークが送信元であるメールのみ「外部ネットワーク」へ中継を許可する。

4.2. IMAP

- ・使用するパッケージは「dovecot-imapd」とし、「youth-skills.jp」ドメインの **IMAP** サーバとして動作させる。
- ・SSL による接続保護を無効とする。
- ・SSL による接続保護の無い通信において **PLAIN** 認証を許可する。

5. Web サービスの設定

「bsv1」へ 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「nginx」とする。
- ・「外部ネットワーク」から、「http://www.youth-skills.jp/」のリクエストに応答する。表示内容は“youth-skills.jp Official Site”とする。
- ・「bravo」事業所ネットワーク内から、「http://local.youth-skills.jp/」のリクエストに応答する。表示内容は“Local Site”とする。

6. DHCP サービスの設定

「bsv2」へ DHCP 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「isc-dhcp-server」とする。
- ・192.168.1.101～200 の IP アドレスを配布する。
- ・優先 DNS サーバとして「bsv2」、代替 DNS サーバとして「bsv1」のアドレスを配布する。
- ・デフォルトゲートウェイのアドレスを配布する。

7. Proxy サービスの設定

「bsv1」へ Proxy 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「squid」とする。
- ・TCP 8080 番ポートでサービスを提供する。
- ・「bravo」事業所ネットワークの端末にサービス利用を許可する。
- ・URL に“game”を含むサイトへのアクセスを禁止する。

8. SSH サービスの設定

「bsv2」へ SSH 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「openssh-server」とする。
- ・TCP 10022 番ポートでサービスを提供する。
- ・パスワード認証による接続を許可しない。

【クライアント PC の設定】

「b-client」は、競技終了時点で以下の設定となっていること。

1. ネットワークの設定

- ・「bsv2」の DHCP サーバ機能により、IP アドレス、DNS サーバ、デフォルトゲートウェイの情報が自動的に配布され、ネットワーク接続可能な状態とする。ただし、「bsv2」の DHCP サーバ機能を構築できなかった場合は、手動で適切なネットワーク設定を行うこと。

2. メールクライアントの設定

メールクライアント(Mozilla Thunderbird)を以下の通り設定し、「taro」のアカウントでメールの送受信を可能にする。

名前	愛媛太郎
電子メールアドレス	taro@youth-skills.jp
受信サーバの接続保護	なし

3. Web ブラウザ

Proxy サーバ(「bsv1」)利用設定を行い、Microsoft Edge で「外部ネットワーク」にある Web サーバの閲覧を可能にする。

4. ssh クライアントの設定

ターミナルソフト(Tera Term)を以下の通り設定しなさい。

- ・「master」のアカウントで「bsv2」へ、SSH バージョン 2(SSH2)を用いてリモート接続可能とする。
- ・秘密鍵ファイルは「id_rsa」の名前で、「C:¥ssh」フォルダに保存する。
- ・鍵ペアで使用するパスフレーズは、「Ssh2021」とする。

別紙

図1 ネットワーク構成図

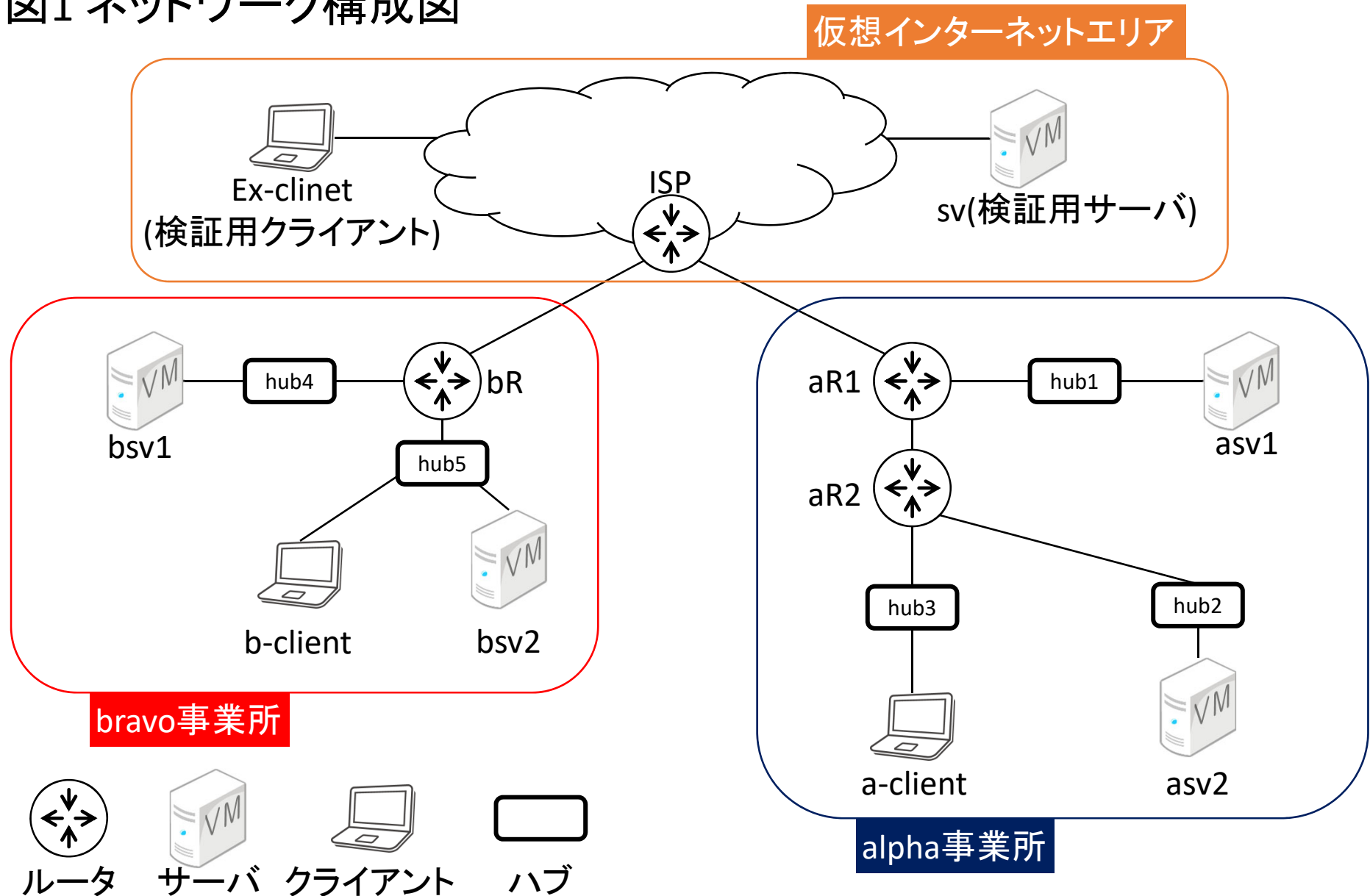


表1 ルータ接続, IPアドレス

ノード名	インタフェイス	IPアドレス	接続先ノード
ISP		201.10.0.6/29	aR1
		201.10.0.121/29	bR
aR1	Gi0/0	201.10.0.1/29	ISP
	Gi0/1	10.0.100.254/24	hub1
	Gi0/2	192.168.0.254/24	aR2
aR2	Gi0/0	192.168.0.1/24	aR1
	Gi0/1	192.168.1.254/24	hub2
	Gi0/2	192.168.2.254/24	hub3
bR		201.10.0.126/29	ISP
		10.0.0.254/24	hub4
		192.168.1.254/24	hub5

表2 サーバ, クライアントのIPアドレス及びアカウント, パスワード

ノード名	IPアドレス	管理者 アカウント	パスワード
sv	200.99.1.1		
Ex-client	200.88.2.101/24	user	なし
asv1	10.0.100.1/24		
asv2	192.168.1.1/24		
a-client	DHCPで取得	user	なし
bsv1	10.0.0.1/24	root	Young2021
bsv2	192.168.1.1/24	root	Young2021
b-client	DHCPで取得	user	なし

※Ex-clientのゲートウェイアドレス: 200.88.2.254