第14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

2019年8月1日（木） 9:00～13:00（4時間）

目　次

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。
- ✓ 競技時間は4時間とする。作業手順は問わないので、効率を考えて作業を行うこと。
- ✓ 競技内容に質問がある場合は、質問用紙に記入の上、競技委員に申し出ること。
- ✓ 競技中にトイレなど体調不良が生じた場合は、その旨を競技委員に申し出て、指示に従うこと。
- ✓ 競技中の水分補給のための飲料水の持ち込みは認める。
- ✓ 競技時間内に作業が終了した場合は、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、ある事業所のネットワーク及びサーバ構築の業務を受注し、あなたがその作業を行うことになった。

構築するシステムに対する先方の担当者の要望は以下の通りであった。

- 使用するネットワーク機器はルータ 2 台、ハブ 2 台である。
- 「事業所内部ネットワーク」と「外部ネットワーク」の間に「DMZ(非武装地帯)」を作る。
- 外部接続及び内部接続をするルータで、アクセス制限を設ける。
- サーバ 2 台(「sv1」、「sv2」)を Linux OS で構築し、「DMZ(非武装地帯)」に設置する。

A) 「sv1」では以下のサービスを提供する。
- DNS サービス。
- Mail サービス。
- Web サービス。

B) 「sv2」では以下のサービスを提供する。
- DNS サービス。
- Mail サービス。
- Proxy サービス。

- クライアント Pc2 台(「c1」、「c2」)を「事業所内部ネットワーク」に設置し、Web、Mail などのサービスを利用可能にする。

競技課題

次ページ以降の注意事項、ネットワーク構成図、設定内容を良く読み、ネットワーク機器の設定、サーバ構築を行い、顧客事業所の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。

- ✓ ネットワーク構成図における「外部ネットワーク」は、ルータ(「InetRouter」)、検証用サーバ(「inetsvr」)、及び検証用クライアント PC(「Ex-c」)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る。選手は、検証用クライアント PC を除く「外部ネットワーク」内ノードの操作を禁止する。

- ✓ 競技委員により各競技エリア内のネットワーク物理配線は接続済みである。この物理配線変更を禁止する。

- ✓ 検証用サーバ(「inetsvr」)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も構わない。
  - ・DNS サーバが稼働しており、www.itnetsys.org 及び itnetsys.org ドメインの MX レコードが登録されている。
  - ・WWW サーバが稼働しており、以下の URL でアクセス可能である。
    - ✧ http://200.99.1.1
    - ✧ http://www.itnetsys.org
    - ✧ http://www.3ch.net、http://www.3ch.net/game/
    - ✧ http://game.wahaha.tv
  - ・SMTP サーバが稼働しており、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 PC(「Ex-c」) は Windows10 が稼働しており、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。各自の設定確認のために利用して構わない。
  - ・「Ex-c」では、以下のアカウント(Administrator 権限)が利用可能である。

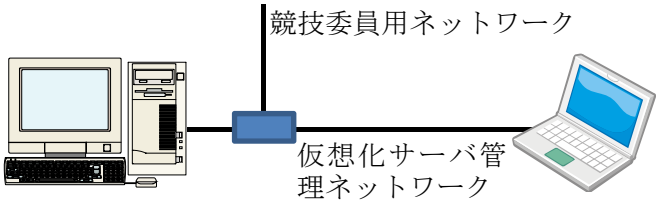
ユーザ名	admin_user
パスワード	adminadmin

  - ・「Ex-c」が接続されているネットワークは以下のとおりである。

ネットワークアドレス	200.88.2.0/24
ゲートウェイ	200.88.2.254

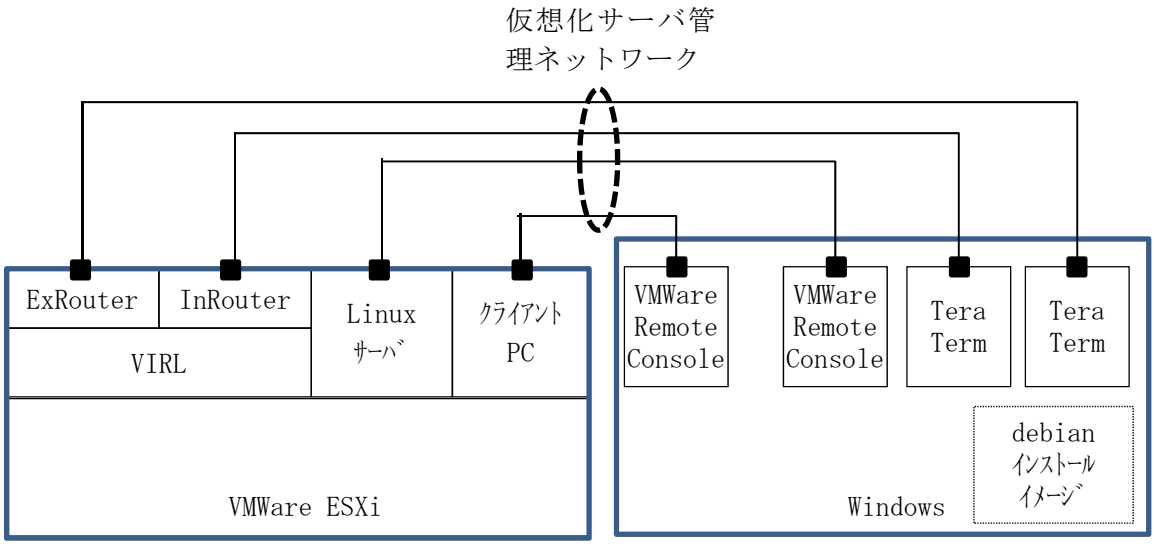
競技環境(仮想環境)に関する注意事項

✓ 競技で使用する PC 等の配置、役割は以下の通りである。



［仮想化サーバ用 PC］　　［競技用 PC］

・[競技用 PC]の管理者ユーザ Administrator のパスワードは「adminadmin」が設定されている。このパスワードの変更を禁止する。
・[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］　　［競技用 PC］

・ [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 VIRL(ネットワーク仮想化ソフトウェア)、及びクライアント PC(「c1」、「c2」)として Windows10 がインストール済みである。Linux サーバ(「sv1」、「sv2」)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。
・「c1」、「c2」、「sv1」及び「sv2」は「ネットワーク構成図」に示すネットワークに接続済みである。
・ VIRL には「ネットワーク構成図」に示す各ノード(「ExRouter」、「InRouter」及びハブ)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。

・「ExRouter」及び「InRouter」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)の変更を禁止する。

・「c1」、「c2」、「Ex-c」(検証用クライアント PC)、「sv1」及び「sv2」は、[競技用 PC]にインストールされている「VMWare Remote Console」を用いて操作を行う。[競技用 PC]のデスクトップに各ノードを操作する「VMWare Remote Console」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)の変更を禁止する。また、「VMWare Remote Console」による接続には下記「ユーザ名」、「パスワード」を用いること。

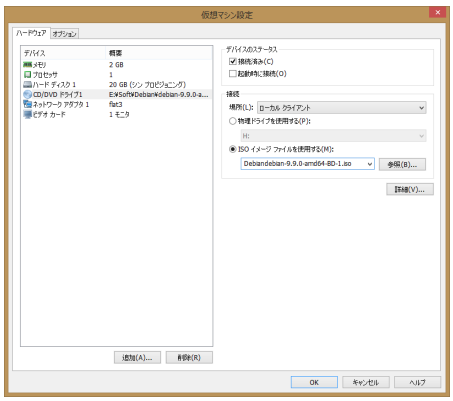
ユーザ名	young
パスワード	young2019

・ debian のインストール・イメージ(debian-9.9.0-amd64-DLBD-1.iso)は[競技用 PC]のデスクトップ上にある。「sv1」及び「sv2」のインストール時に、以下の操作を行う。

✧ 「sv1」または「sv2」操作用のショートカットから「VMWare Remote Console」を起動。

✧ メニュー[VMRC(V)]-[電源(P)]-[パワーオン(P)]を選択。

✧ 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

✧ メニュー[VMRC(V)]-[<Ctrl>+<Alt>+<Delete>の送信(C)]を選択。

・「sv1」及び「sv2」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。

✓ 「ネットワーク構成図」に示す「外部ネットワーク」内の各ノード(「InetRouter」、「inetsvr」)は競技委員により[仮想化サーバ用 PC]上に配置・接続、構築済みであり、競技開始時に電源 ON の状態である。

✓ 競技終了時に指定された設定がルータの NVRAM に保存されていること。

✓ 「c1」、「c2」、「sv1」、及び「sv2」の仮想マシンは、競技終了時点の状態で採点される。

※ローカル、リモートにかかわらず、VMWare ESXi 及び VIRL の直接操作を禁止する。

ルータの設定

「事業所内部ネットワーク」及び「DMZ」はプライベートアドレスにて構成される。ISPからは201.10.0.0/29のグローバルアドレスが割り当てられている。

1.「ExRouter」及び「InRouter」の共通設定

1.1. ホスト名、パスワード

・各ルータのホスト名は、競技委員により設定済みである。
・各ルータの各パスワードを以下の通り設定しなさい。ただし、イネーブルパスワードは暗号化すること。その他のパスワードは暗号化しない。

ホスト名	イネーブル パスワード	コンソール パスワード	telnet パスワード
ExRouter	cisco	cisco	tPass
InRouter	cisco	cisco	tPass

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、More 機能を無効にする。
・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。
・telnet接続時、15分操作が行われなかった場合、自動ログアウトする。

1.3. インタフェイスの設定

・「ネットワーク構成図」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。

※各ルータのgi0/0インタフェイスはVIRLの管理用に予約されている。選手によるgi0/0の設定変更を禁止する。

2.「ExRouter」の設定

2.1. アドレス変換

・送信元が172.17.1.1～172.17.1.31のパケットは、送信元プライベートIPアドレスをグローバルIPアドレス(201.10.0.3)へ変換し、複数台の端末が同時に「外部ネットワーク」と通信が行えるようにNAPTを設定する。
・「sv1」を外部ネットワークと相互接続可能とするために、「sv1」のプライベート IP アドレスをグローバルIPアドレス(201.10.0.1)と一対一に対応付ける。
・「sv2」を外部ネットワークと相互接続可能とするために、「sv2」のプライベート IP アドレスをグローバルIPアドレス(201.10.0.2)と一対一に対応付ける。

2.2. ルーティングの設定

・外部ネットワークへの通信が可能となるように、デフォルトルートを登録する。
・「事業所内部ネットワーク」への通信が可能となるように、静的ルートを登録する。

2.3. アクセス制御の設定

2.3.1. 外部インタフェイス(gi0/1)

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。

・「ExRouter」、「sv1」及び「sv2」への ICMP トラフィックを許可する。

・「sv1」上の SMTP サービス、DNS サービス、WWW 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

・「sv1」及び「sv2」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。

・上記以外は許可しない。

2.3.2. 内側インタフェイス(gi0/2)

・アクセス制御を設定しない。

3.「InRouter」の設定

3.1. アドレス変換

・設定しない。

3.2. ルーティングの設定

・「外部ネットワーク」への通信が可能となるように、デフォルトルートを登録する。

3.3. アクセス制御の設定

3.3.1. 外部インタフェイス(gi0/1)

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。

・DMZ から「InRouter」、「事業所内部ネットワーク」への ICMP 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

・すべて許可する。

3.3.2. 内部インタフェイス(gi0/2)

・アクセス制御を設定しない。

3.4. DHCP サーバの設定

・「事業所内部ネットワーク」に接続した端末に対して、172.17.1.0/24 の IP アドレスを配布する。ただし、172.17.1.1～172.17.1.31 及び 172.17.1.201～172.17.1.254 の IP アドレスは除外すること。

・優先 DNS サーバとして「sv2」、代替 DNS サーバとして「sv1」のアドレスを配布すること。

・デフォルトゲートウェイのアドレスを配布すること。

サーバ PC の設定

1. OS インストール

1.1.「sv1」及び「sv2」の共通設定

・OS として Debian GNU/Linux 9.9 を以下の通りインストールしなさい。

設定項目	「sv1」	「sv2」
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	Young2019	
一般ユーザアカウント名	master	
一般ユーザのフルネーム	任意	
一般ユーザのパスワード	R01master	
ホスト名	sv1	sv2
ドメイン名	youth-skills.org	

・ネットワーク設定は以下の通りとする。

設定項目	「sv1」	「sv2」
IPアドレス	10.0.100.101/24	10.0.100.102/24
デフォルトゲートウェイ	「ExRouter」	「ExRouter」
ネームサーバ	「sv1」	「sv2」

・「事業所内部ネットワーク」への静的ルートを永続的に設定する。

1.2.「sv1」の設定

・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	利用方法
/boot	200MB	ext4
/	10GB	ext4
/home	4GB	ext4
/var	4GB	ext4
-	2GB	スワップ

1.3.「sv2」の設定

・パーティション構成は任意とする。

2. その他の OS 設定及びユーザ設定

2.1.「sv1」及び「sv2」の共通設定

・「事業所内部ネットワーク」宛ての通信は、「InRouter」へ送るように経路情報を追加しなさい。

・「sudo」パッケージをインストールし、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.「sv2」の設定

・下記の一般ユーザを作成する。

アカウント	taro
フルネーム	Hakata Taro
パスワード	passR01

3. DNS サービスの設定

「sv1」及び「sv2」へ DNS サービスを以下の通り設定しなさい。

3.1.「sv1」及び「sv2」共通設定

・使用するパッケージは「bind9」とする。
・DNSSEC の検証は無効にする。
・再帰問い合わせは「事業所内部ネットワーク」及び「DMZ」からのみ許可する。
・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.「sv1」の設定

・「事業所内部ネットワーク」及び「DMZ」からの問い合わせを処理する view を定義する。view 名は「internal」とする。
・上記ネットワーク以外からの問い合わせを処理する view を定義する。view 名は「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」へ回送する。
・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。

3.2.1.「external」view

A) 正引きゾーン

・「youth-skills.org」ゾーンの管理を行うマスタサーバとして動作させる。
・「sv1」をメールサーバとして MX レコードを設定する。
・「sv1」の正引きを設定する。別名として「www」を設定する。
・「sv2」の正引きを設定する。

B) 逆引きゾーン

・201.10.0.0/29 の逆引きゾーンを管理するマスタサーバとして動作させる。
・201.10.0.0/24 の逆引きゾーンは「検証用サーバ」がマスタサーバとして管理しており、201.10.0.0/29 の逆引きゾーン(0-7.0.10.201.in-addr.arpa.)を「sv1」に委任している。「検証用サーバ」で設定されている 201.10.0.0/24 の逆引きゾーンファイルのレコード(一部抜粋)は以下のとおりである。

```
0.10.201.in-addr.arpa.        IN     NS     sv.itnetsys.org.
1.0.10.201.in-addr.arpa.      IN     CNAME  1.0-7.0.10.201.in-addr.arpa.
2.0.10.201.in-addr.arpa.      IN     CNAME  2.0-7.0.10.201.in-addr.arpa.
3.0.10.201.in-addr.arpa.      IN     CNAME  3.0-7.0.10.201.in-addr.arpa.
4.0.10.201.in-addr.arpa.      IN     CNAME  4.0-7.0.10.201.in-addr.arpa.
5.0.10.201.in-addr.arpa.      IN     CNAME  5.0-7.0.10.201.in-addr.arpa.
6.0.10.201.in-addr.arpa.      IN     CNAME  6.0-7.0.10.201.in-addr.arpa.
0-7.0.10.201.in-addr.arpa.    IN     NS     sv1.youth-skills.org.
```

・「sv1」及び「sv2」の逆引きを設定する。

C) その他の設定

・「検証用サーバ」を「youth-skills.org」正引きゾーン及び 201.10.0.0/29 の逆引きゾーンのスレイブサーバとする。マスタのゾーンデータベースに変更があった場合、直ちにスレイブサーバに通知し、ゾーン転送が開始されること。

・「検証用サーバ」以外へのゾーン転送は許可しない。

3.2.2.「internal」view

・「youth-skills.org」ゾーンの管理を行うスレイブサーバとして動作させる。

3.3.「sv2」の設定

・「youth-skills.org」ゾーンの管理を行うマスタサーバとして動作させる。

・「事業所内部ネットワーク」及び「DMZ」からの問い合わせのみに応答する。

・「sv2」をメールサーバとして MX レコードを設定する。

・「sv1」の正引きを設定する。別名として「www」を設定する。

・「sv2」の正引きを設定する。

・「sv1」を「youth-skills.org」正引きゾーンのスレイブサーバとする。マスタのゾーンデータベースに変更があった場合、直ちにスレイブサーバに通知し、ゾーン転送が開始されること。

・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、「sv1」へ回送する。

・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。

4. メールサービスの設定

「sv1」及び「sv2」へメールサービスを以下の通り設定しなさい。

4.1.「sv1」及び「sv2」共通設定

・「postfix」パッケージを使用し、「youth-skills.org」ドメインの smtp サーバとして動作させる。

4.2.「sv1」の設定

・「youth-skills.org」ドメインの送信及び、受信メールゲートウェイとして動作させる。

・「youth-skills.org」ドメイン宛のメールは、「sv2」へ転送する。

・「youth-skills.org」ドメイン宛以外のメールは、「事業所内部ネットワーク」及び「DMZ」が送信元である場合のみ「外部ネットワーク」へ中継を許可する。

・「sv1」に未登録のユーザ宛メールを、「sv2」へ転送するために、/etc/postfix/main.cf に以下の設定を追加する(=の右に値はなし)。

```
local_recipient_maps =
```

4.3.「sv2」の設定

4.3.1. postfix

・「事業所内部ネットワーク」及び「DMZ」からのみメールを受信し、「外部ネットワーク」宛メールは「sv1」へ転送する。

・メール保存形式は maildir 形式とし、保存場所は~/Maildir ディレクトリとする。

4.3.2. IMAP サービス

・「dovecot-imapd」パッケージを使用し、IMAP サーバとして動作させる。

・メールロケーションを maildir 形式とし、~/Maildir ディレクトリとする。

・PLAIN 認証を許可する。

5. WWW サービスの設定

「sv1」へ WWW サービスを以下の通り設定しなさい。

・使用するパッケージは「apache2」とする。

5.1. 外部公開サイトの設定

・「外部ネットワーク」、「DMZ」及び「事業所内部ネットワーク」から URL「http://www.youth-skills.org」へのリクエストに対し、「/var/www/html/index.html」を返す。表示内容は“www.youth-skills.org Official Site”とする。

5.2. 事業所内部向けの設定

・「DMZ」及び「事業所内部ネットワーク」のみから URL「http://local.youth-skills.org」へのリクエストに対し、「/var/www/local/index.html」を返す。表示内容は“local.youth-skills.org local Site”とする。

・事業所内部向けにプロキシサーバの自動構成スクリプトを、URL「http://local.youth-skills.org/proxy.pac」で提供する。

・スクリプトファイル proxy.pac は、下記の内容で各自作成すること。

```
function FindProxyForURL(url, host)
{
        return “PROXY 10.0.100.102:8080”;
}
```

6. Proxy サービスの設定

「sv2」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。

・「DMZ」及び「事業所ネットワーク」からのみ Proxy の利用を許可する。

・TCP 8080 番ポートでサービス提供する。

・URL に文字列「game」を含むページへのアクセスを禁止する。

クライアント PC の設定

クライアント PC(「c1」、「c2」)は各種サービスや設定確認のために自由に使用して構わないが、競技終了時点では以下の設定となっていること。

1. クライアント PC(「c1」、「c2」)の設定

・クライアント PC は OS として Windows10 がインストール済みである。
・クライアント PC の操作は admin_user アカウント(管理者権限)にて行う。admin_user アカウントのパスワードは「adminadmin」が設定されている。このパスワードを変更してはいけない。
・クライアント PC には Windows10 標準アプリケーション以外に、以下のアプリケーションがインストール済みである。

- ✓ Tera Term
- ✓ Mozilla Thunderbird

2. クライアント PC「c1」の設定

2.1. ネットワークの設定

・ネットワーク設定は以下の通りとし、ネットワーク接続可能な状態とする。

IP アドレス	172.17.1.1/24
デフォルトゲートウェイ	「InRouter」
優先 DNS サーバ	「sv2」
代替 DNS サーバ	「sv1」

3. クライアント PC「c2」の設定

3.1. ネットワークの設定

・「InRouter」の DHCP サーバ機能により、IP アドレス等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。「InRouter」の DHCP サーバ機能が利用できない場合、以下のネットワーク設定を手動で行うこと。

IP アドレス	172.17.1.32/24
デフォルトゲートウェイ	「InRouter」
優先 DNS サーバ	「sv2」
代替 DNS サーバ	「sv1」

3.2. ブラウザの設定

・Web ブラウザ(Microsoft Edge)で、「sv1」の Web サーバが提供する「プロキシサーバの自動構成スクリプト」を指定して、「sv2」の Proxy サービスを利用可能とする。「sv1」の Web サーバが提供する「プロキシサーバの自動構成スクリプト」を利用できない場合は、手動でプロキシサーバの設定を行うこと。

3.3. 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が可能とする。

名前	Hakata Taro
電子メールアドレス	taro@youth-skills.org
送信メールサーバ	「sv2」
受信メールサーバ	「sv2」