第１３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

平成 30 年 8 月 2 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、下欄及び別紙 ネットワーク構成図に座席番号と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。
- ✓ 支給した部品（LAN ケーブル製作用の RJ-45 モジュラジャック）を破損した場合には、代わりの部品を再支給する。ただし、その場合は減点とする。
- ✓ 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。
- ✓ 選手間での工具等の貸借は認めない。持参した工具に不具合がある場合は、競技委員に申し出ること。
- ✓ 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 1 台である。
- 「事業所内部ネットワーク」(「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」)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 台を Linux OS で構築し、「DMZ(非武装地帯)」(「sv1」)と「事業所内部管理ネットワーク」(「sv2」)に設置する。

A) 「sv1」では以下のサービスを提供する。
- 「事業所内部ネットワーク」、「DMZ」及び「外部ネットワーク」用の DNS サービス。
- 事業所従業員のための Mail サービス。
- 事業所従業員のための Proxy サービス。
- 「外部ネットワーク」公開用及び「事業所内部ネットワーク」用の WWW サービス。

B) 「sv2」では以下のサービスを提供する。
- 「事業所内部ネットワーク」及び「DMZ」用の DNS サービス。
- 「事業所内部ネットワーク」用の DHCP サービス。
- サーバのリモート管理用の SSH サービス。

競技課題

(1)次ページ以降の注意事項、設定内容及び別紙 ネットワーク構成図を良く読み、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。

(2)LAN ケーブル結線図とその説明 (p.13) をよく読んで、LAN ケーブルを 2 本作成しなさい。

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。

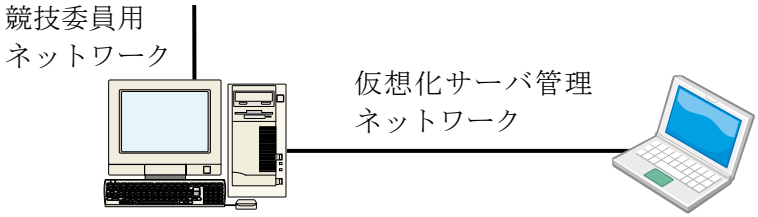
- ✓ 別紙 ネットワーク構成図における「外部ネットワーク」は、「L3SW」及び「検証用サーバ」で構成される。これは競技委員が用意する仮想的なインターネットエリアである。選手は「外部ネットワーク」内のノードを操作する必要は無い。

- ✓ 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。この物理配線を変更してはいけない。

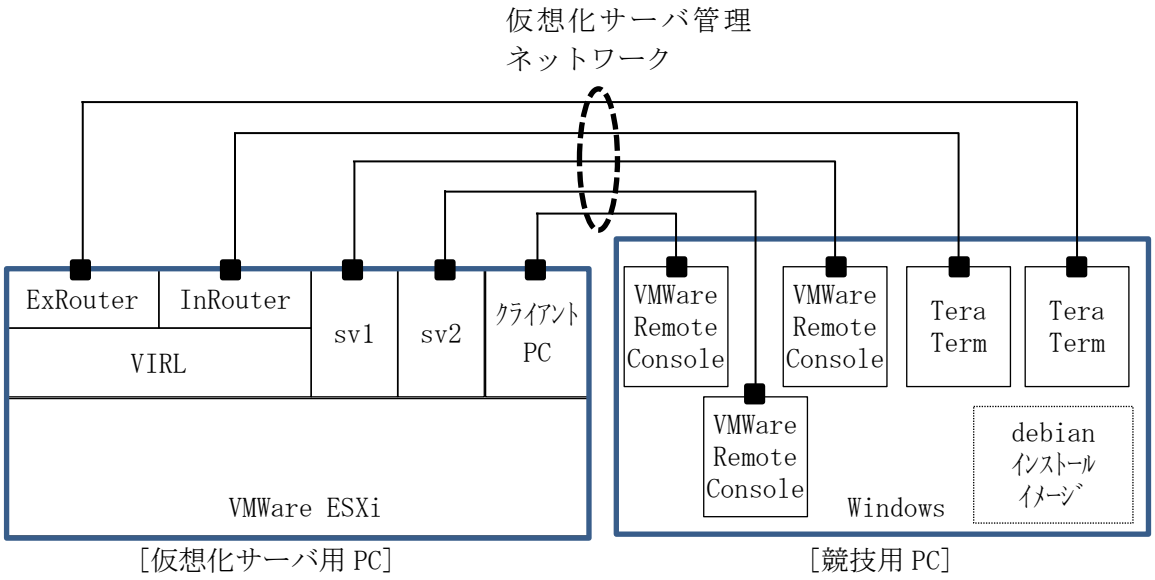
- ✓ 「検証用サーバ」 200.99.1.1 では、下記のサービスが稼働している。各自の設定確認のためにこれらのサービスを利用しても構わない。
  - ・DNS サーバが稼働しており、www.itnetsys.org 及び itnetsys.org ドメインの MX レコードが登録されている。
  - ・WWW サーバが稼働しており、以下の URL でアクセス可能である。
    - ✧ http://200.99.1.1
    - ✧ http://www.itnetsys.org
    - ✧ http://www.3ch.net
    - ✧ http://www.wahaha.tv
  - ・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。

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]の管理者ユーザ Administrator のパスワードは「adminadmin」が設定されている。このパスワードを変更してはいけない。
・[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を変更してはいけない。
・ 「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]を直接操作してはいけない。

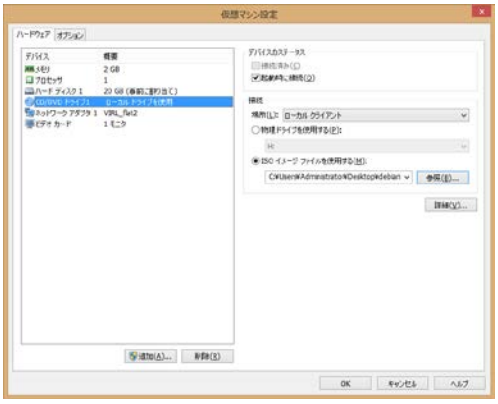


・ [仮想化サーバ用 PC]にはホスト OS として VMWare ESXi がインストールされている。
・ VMWare ESXi のゲスト OS として VIRL(ネットワーク仮想化ソフトウェア)及び「クライアント PC(Windows10)」がインストール済みである。「sv1」及び「sv2」はディスク領域のみが確保されており、OS は未インストール状態である。
・ 「クライアント PC」、「sv1」及び「sv2」は「ネットワーク構成図」に示すネットワークに接続済みである。

・VIRL には「ネットワーク構成図」に示す「事業所内部ネットワーク」内の各ノード(「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)を変更してはいけない**。
・「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)を変更してはいけない**。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	young2018

・debian のインストール・イメージ(debian-9.4.0-amd64-DLBD-1.iso)は[競技用 PC]のデスクトップ上の「debian_iso」フォルダ内にある。「sv1」及び「sv2」のインストール時には、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)]-[管理(M)]-[仮想マシン(S)…]を選択。



☑起動時に接続(O)
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)]-[電源(P)]-[パワーオン(P)]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。選手はこれらの設定を変更してはいけない。**

✓ 「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(「L3 スイッチ」、「検証用サーバ」)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 startup-config ファイルに保存されていること。

✓ 採点前に、「sv1」、「sv2」及び「クライアント PC」の仮想マシンは再起動される。

※ローカル、リモートにかかわらず、選手が VMWare ESXi 及び VIRL を直接操作する必要は無い。

ルータの設定

１．ホスト名とパスワードの設定

各ルータのホスト名と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	ePass	cPass	tPass
InRouter	ePass	cPass	tPass

２．ターミナル環境の設定

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、5 分操作が行われなかった場合、自動ログアウトする。

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。競技において gi0/0 の設定を変更してはいけない。

４．アドレス変換の設定

「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」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。

「ExRouter」にてアドレス変換を以下の通り設定しなさい。また、「InRouter」にはアドレス変換を設定してはならない。

- 「事業所内部管理ネットワーク」から外部ネットワークへのアクセスを可能とする。そのため、送信元が「事業所内部管理ネットワーク」のパケットは、「ExRouter」にて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(201.10.0.2～201.10.0.3)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を行えるように NAPT 設定すること。
- 「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こと。

5．ルーティングの設定

（1）「ExRouter」の設定

- 「事業所内部管理ネットワーク」及び「事業所内部クライアントネットワーク」との通信が可能となるように静的経路情報を登録すること。
- 「事業所内部管理ネットワーク」及び「DMZ」から「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こと。

（2）「InRouter」の設定

- 「事業所内部管理ネットワーク」から「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こと。

6．DHCP リレーの設定

- 「事業所内部クライアントネットワーク」内で、「sv2」の DHCP サービスを利用できるように「InRouter」に DHCP リレーエージェントの設定をすること。

7．アクセス制御の設定

（1） 「ExRouter」の設定

- 外部インタフェイス(gi0/1)に以下のアクセス制御を設定すること。

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」への ICMP トラフィックを許可する。
- 「sv1」上の DNS サービス、SMTP 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」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。

- 内側インタフェイス(gi0/2)にはアクセス制御を設定しない。

（2）「InRouter」の設定

- 外部インタフェイス(gi0/1)に以下のアクセス制御を設定すること。

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。
- 「InRouter」、「事業所内部管理ネットワーク」及び「事業所内部クライアントネットワーク」への ICMP トラフィックを許可する。
- 「sv1」から「sv2」の DNS 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

- すべて許可する。

- 内部インタフェイス(gi0/2)にはアクセス制御を設定しない。
- 内部インタフェイス(gi0/3)にはアクセス制御を設定しない。

サーバ PC の設定

１．OS インストール

「sv1」及び「sv2」の OS として Debian GNU/Linux 9.4 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	Young2018	
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	MasterH30	
ホスト名	sv1	sv2
ドメイン名	young.org	

サーバPCの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	172.17.1.1/24
デフォルトゲートウェイ	「ExRouter」	「InRouter」
ネームサーバ	「sv1」	「sv2」

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

２．その他の OS 設定及びユーザ設定

（1）「sv1」の設定

- 一般ユーザ「taro」を作成する。フルネームは「Kanazawa Taro」、パスワードは「passH30」とする。

（2）共通設定(「sv1」、「sv2」)

- master ユーザのコマンドサーチパスに /sbin を追加する。
- 「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。

３．DNS サービスの設定

DNS サービスを以下の通り設定しなさい。

（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「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」及び「DMZ」からのみ許可する。
- 下記の指定以外で、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。

（２）「sv1」の設定

- 「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」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。
- 「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」及び「DMZ」からの再帰問い合わせのみ許可する。
- 「external」view において次の設定を行う。
  - 「young.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.young.org」の正引きを設定する。別名として「www.young.org」を設定する。
  - 「young.org」ゾーンのみ「検証用サーバ」を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。
- 「internal」view において次の設定を行う。
  - 「young.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。
  - 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）「sv2」の設定

- 「young.org」ゾーンの管理を行うマスタサーバとして動作させる。
- 「事業所内部管理ネットワーク」及び「DMZ」の逆引きゾーンの管理を行うマスタサーバとして動作させる。
- 「sv1.young.org」の正引きを設定する。別名として「www.young.org」及び「in-www.young.org」を設定する。
- 「sv2.young.org」の正引きを設定する。
- 「sv1.young.org」及び「sv2.young.org」の逆引きを設定する。
- 「young.org」ゾーンのみ「sv1」を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．Mail サービスの設定

「sv1」へ Mail 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「postfix」及び「dovecot-pop3d」とする。
- 「young.org」ドメインのメールサーバ(smtp 及び pop3 サーバ)として動作させ、ローカルユーザ間及び外部とのメール送受信を可能とする。
- 自ドメイン宛及び自ホスト宛てのメールのみを受信する。

- 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。
- 送受信メールの最大サイズを 20MB に制限する。ただし、1MB は、1024000B とする。
- 「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」及び「DMZ」からのみ、外部ドメイン宛のメール送信（中継）を許可する。
- 「webmaster@young.org」宛のメールは、ユーザ「taro」へ転送する。
- 受信プロトコルとして pop3 を使用し，平文認証を許可する。

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。

- 公開サイトを設定する。
  - ・URL「http://www.young.org」のリクエストに、「/var/www/html/index.html」を表示する。
  - ・「/var/www/html/index.html」の表示内容は、文字列 “www.young.org Official Site” とする。
  - ・公開サイトでは、エラーページフッタにサーバ情報を表示しない。
- 事業所内部向けサイトを設定する。
  - ・URL「http://in-www.young.org」のリクエストに、「/var/www/in/index.html」を表示する。
  - ・「/var/www/in/index.html」の表示内容は、文字列“in-www.young.org Local Site”とする。
  - ・事業所内部向けサイトでは、エラーページフッタに管理者のメールアドレスとして、webmaster@young.org への mailto リンクを表示する。

6．Proxy サービスの設定

「sv1」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 squid3 とする。
- 「事業所内部管理ネットワーク」、「事業所内部クライアントネットワーク」及び「DMZ」ネットワークからのみ Proxy の利用を許可し、その他のネットワークからの利用は禁止する。
- TCP 8080 番ポートでサービス提供する。
- 以下のサイトへのアクセスを禁止する。
  - ・http://www.3ch.net
  - ・http://www.wahaha.tv

7．DHCP サービスの設定

「sv2」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。
- 「事業所内部クライアントネットワーク」に接続した端末に対して IP アドレス 172.17.2.101～172.17.2.200 を配布すること。
- 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。

8．SSH サービスの設定

「sv2」へリモート管理サービスを以下の通り設定しなさい。

- リモート CUI 管理を行うため SSH サーバを動作させる。
- TCP 60022 番ポートでサービスを提供する。

- 使用するパッケージは openssh-server とする。
- root ユーザでの SSH 接続は許可しない。
- パスワード認証は許可しない。
- 認証方法は公開鍵認証とし、「クライアント PC」から接続可能となるように設定を行う。
- 秘密鍵ファイルは「クライアント PC」上に「C:¥ssh¥young2018」として保存すること。
- パスフレーズ「kanazawa2018」、ユーザ「master」として接続可能とすること。

※鍵生成及び動作確認用として、「クライアント PC」にインストール済みの「Tera Term」を使用してもよい。

「クライアント PC」の設定

「クライアント PC」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．OS

- 「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 Administrator アカウントにて行う。Administrator 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。

2．ネットワーク及びその他の設定

- 「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

- 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にしておくこと。

IP アドレス	172.17.2.100/24
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」

- Web ブラウザ(Internet Explorer)でプロキシサーバ(「sv1」)を利用できる状態にしておくこと。Internet Explorer は、スタートメニューの[Windows アクセサリ]内にある。

- メーラ(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行なえるようにすること。

名前	Kanazawa Taro
電子メールアドレス	taro@young.org
送信メールサーバ	「sv1」
受信メールサーバ	「sv1」

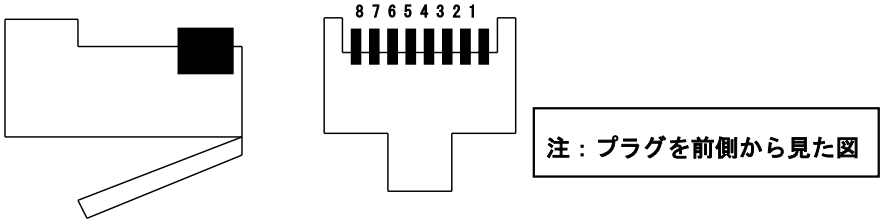
LAN ケーブル結線図

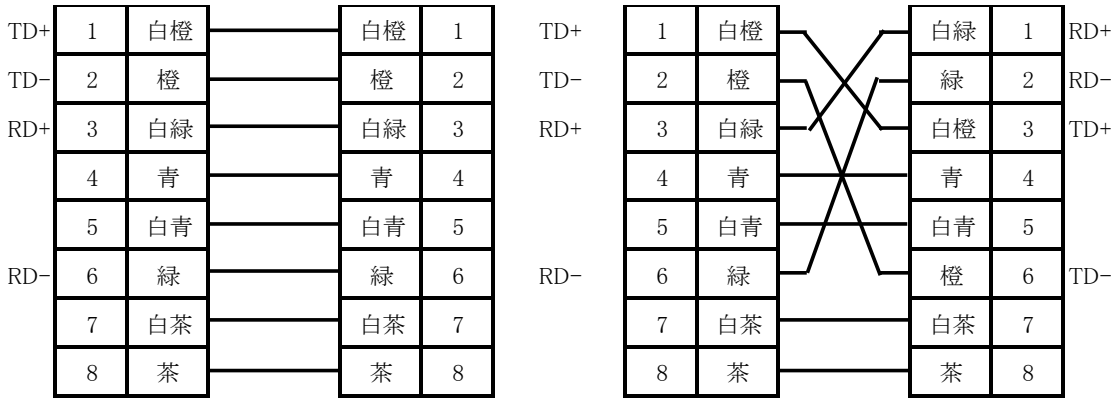
- ストレート・ケーブルの結線は T568B とする。
- クロス・ケーブルの結線は T568A と T568B の組み合わせとする。
- LAN ケーブルの作成
- 下記配線図を参照し、LAN ケーブル(ストレート)を２本作成しなさい。
  ストレート・ケーブル(黄色)1 本、クロス・ケーブル(赤色)1 本

	T568A
1	白緑
2	緑
3	白橙
4	青
5	白青
6	橙
7	白茶
8	茶

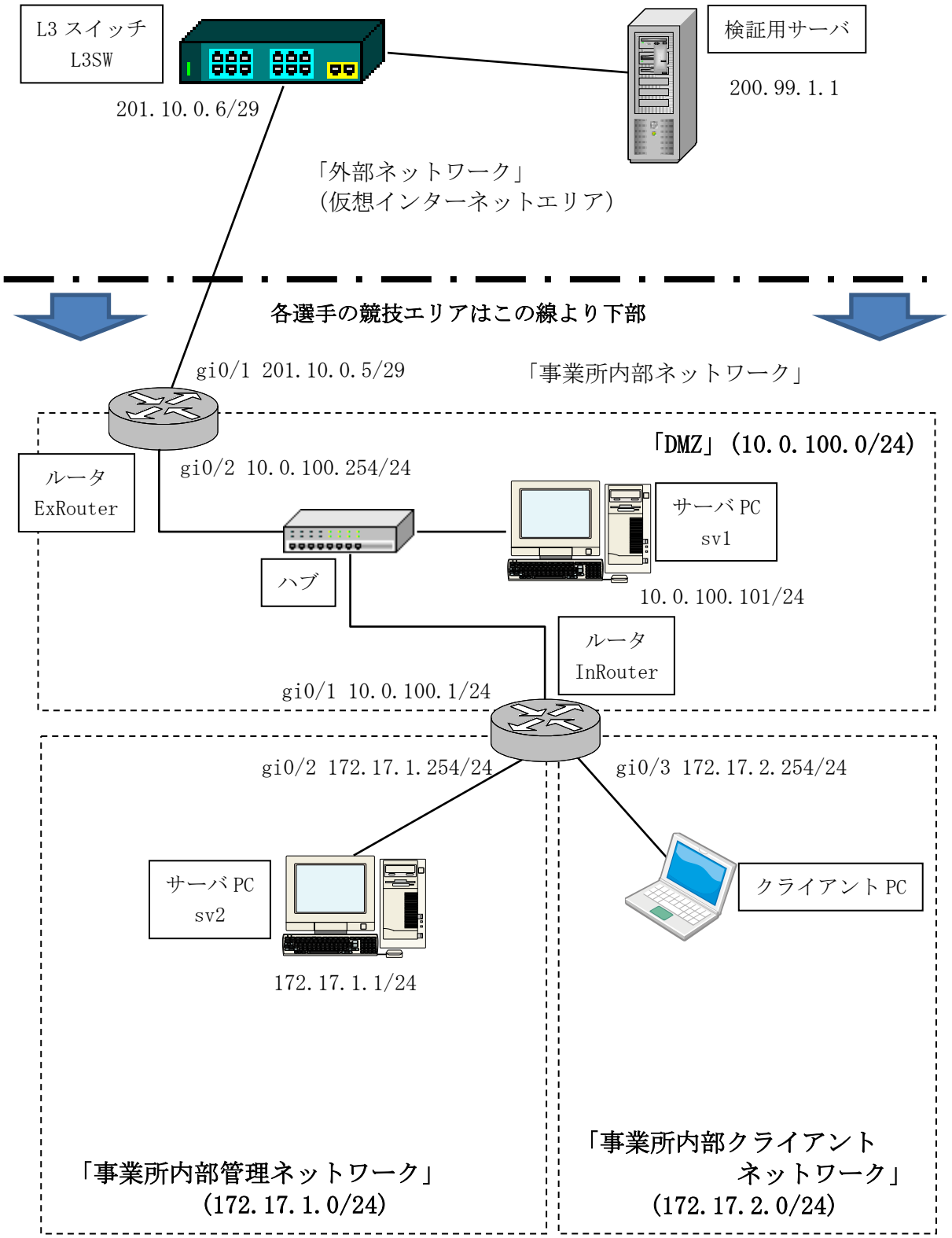
	T568B
1	白橙
2	橙
3	白緑
4	青
5	白青
6	緑
7	白茶
8	茶

モジュラプラグ
RJ－45コネクタ





別紙：ネットワーク構成図



座席番号	競技者氏名