技能五輪全国大会予選会
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　2016 年）

平成 28 年 6 月 25 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。このようなシステムを設計・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。

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とき、この技術者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。技術者にはこれまでの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、この「IT ネットワークシステム管理」競技では、信頼性のある ICT・サーバシステムを構築することと、インターネットへの接続も含めた社内ネットワーク構築技術の技を競います。

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。ただし、競技時間が技能五輪全国大会とは異なることから、使用する機器は少なく、OS の種類も減らしています。競技課題案（２割程度変更して出題）を添付していますので、参考にしてください。

２．競技日程

・競技開始の前日

競技内容の説明、競技場所の抽選、機材の確認

・競技日（競技時間：４時間）

３．競技に使用する主な機器と支給部品

- サーバ用デスクトップＰＣ（Windows 8.1）　各１式
- ＤＶＤ（ＯＳおよびアプリケーション）　各１式
  - Debian GNU/Linux 8.4 Jessie
- クライアント用ノートＰＣ（Windows 8.1）　各１台
  - ターミナルソフト（TeraTerm）、メーラー（Outlook 2013）、Web ブラウザ（IE 11）が使用可能
- Cisco 製ルータ　2811(Ver.12.4)　各３台
- Cisco 製スイッチング Hub　Catalyst 2960G-8TC-L（Version 12.2）　各３台
- ハブ　各１台
- LAN ケーブル（既製品）　各数本
- シリアルケーブル（DCE, DTE）　各１本

競技委員側で構築する上位サーバとの接続用に L3 スイッチ（WS-C3750-24TS-E または FXC7024）を用意し利用しますが、設定・操作等は競技委員が行います。各選手が操作することはありません。

４．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ＰＣ構築作業

指定された各種サーバ機能を実現するため、以下の作業を行います。

・ＯＳのインストールと設定

・各種サーバ（DNS、メール、Web 等）のインストールと設定

・ネットワーク接続作業

Ｂ．クライアントＰＣ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側ＰＣの設定として、以下の作業を行います。

・クライアント設定

・ネットワーク接続作業

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、以下の作業を行います。

・ルータおよびスイッチの基本設定　　・ルーティング・フィルタリング設定

・アドレス変換設定　　・ネットワーク接続作業

「９．競技課題案」をベースに少し（３割程度）変更を加えて競技課題とします。

５．注意事項

Ａ．日本語環境が設定可能なＯＳおよびアプリケーションは、日本語環境を使用します。

Ｂ．サーバのＯＳは Debian GNU/Linux 8.4 Jessie とします。

Ｃ．デスクトップＰＣの仮想環境（VirtualBox）上でサーバを構築します。

Ｄ．ルータの機能として Web 環境での設定が可能な機種であっても、競技中にこの Web 環境でルータの各種設定を行うことを禁止します。

６．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ＰＣ構築作業」が 55%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 55%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。

７．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。

８．競技上の注意事項

a. 各種マニュアルの持ち込みは一切認めません。
b. 配布したＯＳなどが書き込まれたＤＶＤ以外のソフトウェアの持ち込みは一切認めません。
c. 質問などがある場合には、競技委員に申し出て下さい。
d. 競技終了の合図で、作業を直ちに終了して下さい。
e. 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。
f. 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。
g. 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。
h. 携帯電話の電源は切っておいて下さい。

９．競技課題案（参考）

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、そのプロジェクトマネージャとなった。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。

競技課題１

以降の注意事項と競技課題を読み、検証用システムを構築しなさい。

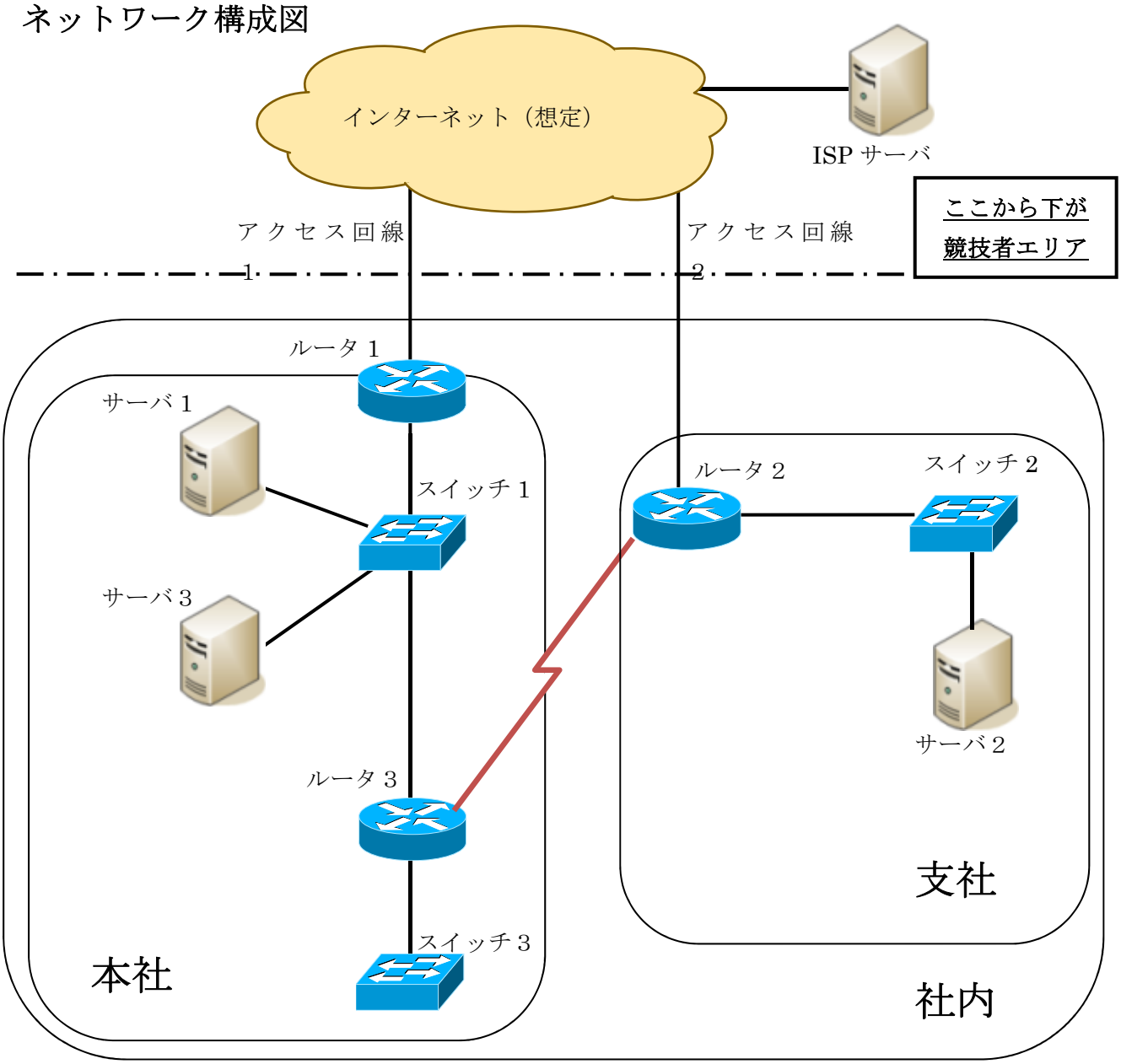
競技課題に関する注意事項

- ✓ ネットワーク構成図における「インターネット（想定)」は、「L3 スイッチ」および「ISP 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」であり、「社内」以外の全てのネットワークエリアを指すものとする。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。
- ✓ 競技課題中の「社内」とは、ネットワーク構成図における「本社」および「支社」内の全てのプライベートアドレスセグメントを指すものとする。また,「本社内」とは、ネットワーク構成図における「本社」内の全てのプライベートアドレスセグメントを指すものとする。「支社内」とは、ネットワーク構成図における「支社内」内の全てのプライベートアドレスセグメントを指すものとする。
- ✓ 各競技エリアには「外部ネットワーク」(L3 スイッチ)とつながる LAN ケーブルが 2 本敷設されている。アクセス回線 1 とアクセス回線 2 の区別があるため適切に接続すること。
- ✓ ISP サーバ（検証用サーバ：200.99.1.1）の機能

  インターネット（想定）上に ISP サーバ（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。必要に応じて各競技者エリアまで敷いてある LAN ケーブルを通してアクセスしてよい。
  - DNS、Web サーバ、Mail(SMTP)サーバが稼働している。

その他の詳細な設定内容は、構成図や設問に記載する。

ネットワーク構成図



構築を行うネットワークの仕様概要は以下の通りとする。

社内で 3 台のサーバを構築する。サーバ 1 は本社 DMZ、サーバ 2 は支社 DMZ に設置して社内外に対してサービスを提供する。サーバ 3 は本社に設置して、社内に対してサービスを提供する。今回、物理サーバが 1 台しか用意出来なかったため、サーバ 1、サーバ 2、サーバ 3 は仮想環境で動作させる。仮想化ソフトウェアは VirtualBox を使用する。社内には本社・支社ネットワークが存在する。本社ネットワークにはサーバ接続用の VLAN 以外にクライアント接続用の VLAN が 2 つあり、このうち一方はインターネットへの直接的接続を許可しないセグメントとする。支社ネットワークも同様とする。本社と支社間の通信はプライマリ経路としてインターネット経由の VPN を使用する。ただし、この VPN 回線に障害が発生した場合はバックアップ経路として専用線（検証環境ではシリアル回線）にて通信可能とする。また、インターネットへのアクセス回線についても本社・

支社が互いにバックアップ経路となる構成とする。

ネットワーク機器接続表

各ネットワーク機器のインターフェースの接続先は次の通りである。

機器	ホスト名	インターフェース	接続先
ルータ 1	R1	Fa0/0	アクセス回線 1
		Fa0/1	スイッチ 1
ルータ 2	R2	Fa0/0	アクセス回線 2
		Fa0/1	スイッチ 2
		Se0/0/0	ルータ 3
ルータ 3	R3	Fa0/0	スイッチ 1
		Fa0/1	スイッチ 3
		Se0/0/0	ルータ 2
スイッチ 1	SW1	Gi0/1	サーバ 3（サーバ 1 の eth2）
		Gi0/2	サーバ 1（サーバ 1 の eth0）
		Gi0/3-Gi0/6	－
		Gi0/7	ルータ 1
		Gi0/8	ルータ 3
スイッチ 2	SW2	Gi0/1-Gi0/6	－
		Gi0/7	サーバ 2（サーバ 1 の eth1）
		Gi0/8	ルータ 2
スイッチ 3	SW3	Gi0/1-Gi0/7	－
		Gi0/8	ルータ 3

・インターフェース記号　Fa：FastEthernet, Gi：GigabitEthernet, Se：Serial

・接続先の「－」はネットワーク機器接続未指定ポートを指す。

・接続先の「アクセス回線 1,2」は、各競技エリアまで敷いている LAN ケーブルを指す。

インターフェース設定表

各ネットワーク機器インターフェースの設定値は、次の通りである。

１．インターフェース IP アドレスの設定

機器	ホスト名	インターフェース	IP アドレス
インターネット側参考情報		アクセス回線 1	160.250.XX.254/29
		アクセス回線 2	170.250.XX.254/29
ルータ 1	R1	Fa0/0	160.250.XX.253/29
		Fa0/1	ｽｲｯﾁ 1 に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-3 のｱﾄﾞﾚｽ
ルータ 2	R2	Fa0/0	170.250.XX.253/29
		Fa0/1	ｽｲｯﾁ 2 に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽ
		Se0/0/0	10.1.0.6/30
ルータ 3	R3	Fa0/0	ｽｲｯﾁ 1 に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-2 のｱﾄﾞﾚｽ
		Fa0/1	ｽｲｯﾁ 3 に接続される各ｻﾌﾞﾈｯﾄのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽ
		Se0/0/0	10.1.0.5/30
スイッチ 1	SW1	Vlan100	10.1.100.250/24
スイッチ 2	SW2	Vlan10	172.16.1.250/24
スイッチ 3	SW3	Vlan10	192.168.1.250/24

・インターフェース記号　Fa：FastEthernet, Gi：GigabitEthernet, Se：Serial

VlanX：Virtual LAN with id X

なお、VLAN に接続するルータのインターフェースには VLAN ID と一致するサブインタフェースを使用する。

２．スイッチ１の VLAN 設定

VLAN 番号	VLAN 名	割付ポート	サブネット	用途
100	Server	Gi0/1-Gi0/2	10.1.100.0/24	内部向けサーバセグメント
200	DMZ	Gi0/3	10.1.200.0/24	本社 DMZ セグメント

※ ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

３．スイッチ２の VLAN 設定

VLAN 番号	VLAN 名	割付ポート	サブネット	用途
10	ClientBr1	Gi0/1- Gi0/2	172.16.1.0/24	支社クライアントセグメント
20	ClientBr2	Gi0/3- Gi0/4	172.16.2.0/24	支社クライアントセグメント
100	DMZBr	Gi0/7	172.16.100.0/24	支社 DMZ セグメント

※ ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

※ VLAN　ClientBr2　は直接的なインターネット接続は許可しないセグメントとする。

４．スイッチ３の VLAN 設定

VLAN 番号	VLAN 名	割付ポート	サブネット	用途
10	Client1	Gi0/1- Gi0/2	192.168.1.0/24	本社クライアントセグメント
20	Client2	Gi0/3- Gi0/4	192.168.2.0/24	本社クライアントセグメント

※ ゲートウェイアドレスは、各サブネットのブロードキャストｱﾄﾞﾚｽ-1 のｱﾄﾞﾚｽとする。

※ VLAN　Client2　は直接的なインターネット接続は許可しないセグメントとする。

ネットワーク機器（ルータ及びスイッチ）の設定項目

１．ケーブリング、IP アドレス設定

以上の構成をもとに、ネットワークを接続、設定しなさい。

２．パスワード

各ネットワーク機器に以下の表に従って特権モード、コンソール、Telnet(vty0-4)に対してパスワードを設定しなさい。全てのパスワード及び特権モードパスワードは暗号化する。

３．シリアル接続

ルータ 3 を DCE、ルータ 2 を DTE として、シリアルケーブルで接続しなさい。

４．VPN

本社ルータ 1 と支社ルータ 2 をインターネット経由で IPsecVPN 接続しなさい。その際、ルータ１，ルータ 2 間に 10.1.0.0/30 のアドレスを使用し（ルータ 1 側を若番とする）トンネルインターフェース（GRE トンネル）の設定を行いなさい。

５．ルーティング

ルーティングについて以下の通り設定しなさい。

- 本社・支社の各ルータ間で経路交換を行い、全てのネットワークで通信可能とする。ルーティングプロトコルとして EIGRP を使用する。
- インターネット側（VPN 回線除く）およびスイッチ 2・スイッチ 3 へ経路情報を流さないこと。
- 本社ネットワーク⇔支社ネットワーク間の通信において、プライマリ経路として VPN 回線を使用し、VPN 回線障害時のバックアップ経路としてシリアル回線を使用するようにメトリックを調整すること。
- 上記の経路切り替えが高速に行えるように、ルータ 3 の EIGRP トポロジーテーブルには、スイッチ 2 に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。同様に、ルータ 2 の EIGRP トポロジーテーブルには、スイッチ 1・スイッチ 3 に接続されるサブネット宛のバックアップ経路としてシリアル回線が登録されること。

６．ゲートウェイの冗長化

ルータ 1 とルータ 3 間に VRRP を設定し､スイッチ 1 の VLAN100,200 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。

- ルータ 1 を Master ルータとする。
- ルータ 1 においてアクセス回線 1 がリンクダウンした場合、Master ルータがルータ 3 に切り替わるようにする。アクセス回線 1 が復旧した場合、Master ルータがルータ 1 に切り戻すこと。

７．スイッチ各種設定

スイッチについて以下の通り各種設定を行いなさい。

- スイッチ-ルータ間を接続しているリンクは 802.1Q のトランクリンクとする。
- 各スイッチにおいて機器を接続する予定がないポート（VLAN 割付ポートとルータ接続ポートを除く全ポート）は閉塞する。

８．NAT / NAPT

アドレス変換を以下の通り設定しなさい。

[スタティック NAT 設定]

- サーバ１をインターネットと相互接続可能とするために、ルータ１にて 160.250.XX.250 に NAT しなさい。
- サーバ 2 をインターネットと相互接続可能とするために、ルータ 2 にて 170.250.XX.250 に NAT しなさい。

[NAPT 設定]

- 本社端末（所属 VLAN 名：Client1、Server）がアクセス回線１経由でインターネット接続できるようにルータ１に NAPT を設定しなさい。また、支社端末(所属 VLAN 名:ClientBr1、DMZBr)もアクセス回線 2 障害時のバックアップ経路としてアクセス回線 1 経由でインターネット接続できるようにルータ１に NAPT を設定しなさい。使用するグローバルアドレスはルータ 1 の Fa0/0 に設定されているアドレスとする。
- 支社端末（所属 VLAN 名：ClientBr1）がアクセス回線 2 経由でインターネット接続できるようにルータ 2 に NAPT を設定しなさい。

９．アクセスコントロール

アクセス制御を以下の通り設定しなさい。

- ルータ１に以下の条件を満たすアクセス制御を設定する。
  - インターネットからのアクセスについて
    - サーバ１に対しては DNS サービス 、SMTP サービスおよび ICMP のみ通信を許可する。
    - ルータ１自身に対する ICMP を許可する。
    - ルータ 2 との VPN 回線のトラフィックは全て許可する。
    - 上記以外は許可しない。
  - 社内からインターネットへのアクセスについて
    - サーバ１からインターネットへのアクセスは全ての通信を許可する。
    - NAPT でのインターネットアクセスは全ての通信を許可する。
    - 上記以外は許可しない。

- ルータ 2 にもルータ１同様のアクセス制御の設定を行う。

サーバの設定項目

以下の指示に従ってサーバの設定を行いなさい。

１．　OSインストール

- **各サーバOS共通設定**

  システム時刻を競技会場の時計と±5分以内に合わせなさい。

- **サーバ1のOSインストール**

サーバ1のOS としてDebian GNU/Linux 8.4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
管理者のパスワード	Skills2016
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意
一般ユーザのパスワード	User
ホスト名	sv01
ドメイン名	netadXX.it.jp

サーバ1のネットワーク設定は以下の通りとし、eth0にてネットワーク接続可能とする。

IPアドレス	10.1.200.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.200.254
ネームサーバ	自身

サーバ１のパーティション構成を以下のとおりとする。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	ファイルシステム
/boot	100MB	ext4
/	40GB	ext4
/var	50GB	ext4
スワップ	4GB	-

*1GBは、1024MBとする

➢ サーバ2のOSインストール

サーバ2も仮想環境にて構築しなさい。

✧ 仮想マシン名は「sv02」とする。

✧ 仮想マシンのイメージファイル容量､パーティション構成､メモリサイズなどは任意とする。

✧ 仮想マシン「sv02」はホストOS(Windows8.1)の起動時に自動起動すること。

サーバ2のOS としてDebian GNU/Linux 8.4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
管理者のパスワード	Skills2016
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意
一般ユーザのパスワード	User
ホスト名	sv02
ドメイン名	skills.netadXX.it.jp

サーバ2のネットワーク設定は以下の通りとする。

IPアドレス	172.16.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	172.16.100.254
ネームサーバ	自身

➢ サーバ 3 の OS インストール

サーバ3のOS としてDebian GNU/Linux 8.4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
管理者のパスワード	Skills2016
一般ユーザアカウント名	user
一般ユーザのフルネーム	任意
一般ユーザのパスワード	User
ホスト名	sv03

ネットワーク設定は以下の通りとする。

IPアドレス	10.1.100.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	10.1.100.254
ネームサーバ	自身

２．DNS

DNS サービスを以下の通り設定しなさい。

[サーバ 1、サーバ 2 共通]

- 使用するパッケージは bind9 とする。
- 自身で名前解決ができない場合は、ISP サーバに問い合わせる。
- bind のバージョンを回答しない。

[サーバ 1]

- 「社内」および「外部ネットワーク」からの問い合わせに応える。
- 再帰問い合わせは自身(localhost)とサーバ 3 からのみ許可する。
- 「外部ネットワーク」向けの netadXX.it.jp および skills.netadXX.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。サーバ 1 とサーバ 2 の正引きを設定する。別名としてサーバ 1 は「mailgw.netadXX.it.jp」、サーバ 2 は「www. skills.netadXX.it.jp」を持つ。
- 「社内」向けの netadXX.it.jp および skills.netadXX.it.jp ゾーンと、その逆引きゾーンの管理を行うマスターサーバとして動作させる。サーバ 1 とサーバ 2 の正引き・逆引きを設定する。別名としてサーバ 1 は「proxy.netadXX.it.jp」、サーバ 2 は「mail. skills.netadXX.it.jp」を持つ。
- サーバ 3 で管理しているゾーンのスレーブとして動作させる。

[サーバ 2]

- 「社内」および「外部ネットワーク」からの問い合わせに応える。
- 再帰問い合わせは自身(localhost)と「支社内」からのみ許可する。
- サーバ 1 とサーバ 3 で管理しているゾーンのスレーブとして動作させる。

[サーバ 3]

- 自身で名前解決ができない場合は、サーバ 1 に問い合わせる。
- 「社内」からの問い合わせに応える。

３．メールサービス

メールサービスを以下の通り設定しなさい。

[サーバ 1、サーバ 2、サーバ 3 共通]

- 使用するパッケージは postfix とする。

[サーバ 1]

- メールゲートウェイとして動作させる。
- 本社ドメイン netadXX.it.jp のプライマリメールサーバー、支社サブドメイン skills.netadXX.it.jp のセカンダリメールサーバーとなる。
- 本社ドメイン netadXX.it.jp 宛てのメールはサーバ 4 へ転送する。
- 支社サブドメイン skills.netadXX.it.jp 宛てのメールはサーバ 2 へ転送する。
- その他の宛先のメールは ISP サーバへ転送する。この際、SMTP 認証を行い、認証が成功した時のみ中継を許可する。認証用ユーザとして mailuser ユーザを作成する。パスワードはユーザ名と同一とする。ただし、サーバ 3 からは認証なしで中継を許可する。

[サーバ 2]

- 支社サブドメイン skills.netadXX.it.jp のメール送信サーバとして動作させる。
- 支社サブドメイン skills.netadXX.it.jp のプライマリメールサーバー、本社ドメイン netadXX.it.jp のセカンダリメールサーバーとなる。

[サーバ 3]

- 本社ドメイン netadXX.it.jp のメール送信および受信サーバとして動作させる。
- 本社ドメイン netadXX.it.jp 宛てのメールをスプールする。保存形式は任意とする。

６．プロキシサービス

サーバ１とサーバ 3 でプロキシサービスを行いなさい。使用するパッケージは squid3 とする。

7. Web サーバサービス

サーバ２とサーバ 3 で Web サーバサービスを行いなさい。