T Software

要件定義書

EC サイト構築要件定義

作　　成	高田浩生
所　　属	真空電気システムズ株式会社
作　成　日	平成 27 年 6 月 12 日

確　　認	
所　　属	
確　認　日	

更新履歴

日付	内容	担当
14/7/2	第一版	高田

目次

1. 概要

本文書では FTP サービス（以下、本サービスという）を提供するためのサイト（以下、本システムという）の構築作業に関する要件を定義する。

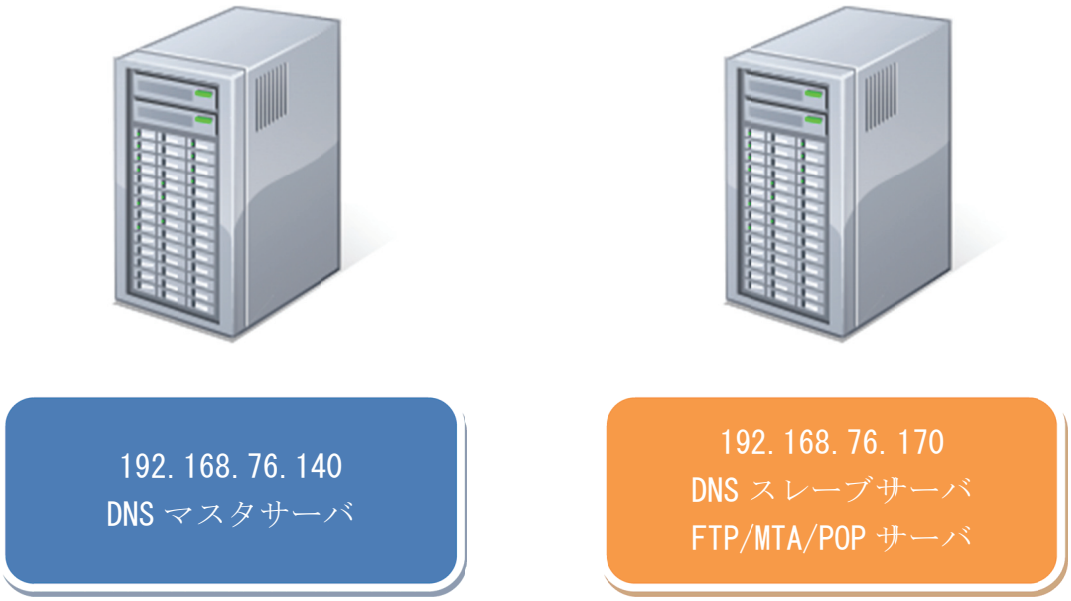

図 1　本システム構成図

1.1　本システム構成

本システム構成図を図 1 に示す。本システムは２台の仮想マシンからなる。一台目のマシンは DNS マスタサーバとする（以下、マスタサーバと呼ぶ）二台目のマシンは DNS スレーブサーバ、FTP サーバ、MTA サーバ、POP サーバとする（以下､スレーブサーバと呼ぶ)OS は CentOS 6.4 を使用し､DNS サーバには bind、FTP サーバには vsftpd、MTA サーバには postfix、POP サーバには dovecot を使用する。

1.2　セキュリティ対策

本システムはセキュリティ対策として、ファイアウォール設定（iptables）による接続制限と SELinux によるアクセス制限を行うものとする。

2. サービス提供形態

本システムのサービスの提供形態は表 1 の通りである。利用者はあらかじめ登録されたアカウントを使用しサービスを利用する。

表 1　サービス提供形態

項目	内容
FTP ホスト名	ftp.example.com
MTA ホスト名	mail.example.com
POP ホスト名	mail.example.com
プロトコル	IPv4 のみ
プライマリグループ	share
ホームディレクトリ	/home/ユーザ名
共通ディレクトリ	/home/share

2.1　管理ドメイン

example.com を管理ドメインと呼ぶこととする。本システム DNS サーバは管理ドメイン上のホスト名解決を行うマスタサーバ、スレーブサーバとなる。

2.2　共有ディレクトリ

全てのユーザが読み込み、書き込み、移動することができる共通ディレクトリを一つ用意する。共有ディレクトリのアクセス権限は 770 とする。

3. 仮想マシン設定

仮想マシンの設定はマスタサーバ、スレーブサーバとも共通で、設定は表 2 の通りとする。

表 2　仮想マシン設定

項目	設定内容
CPU	1 個
メモリ	512 MB
ハードディスク容量	8 GB

4. OS インストール設定

マスタサーバの CentOS 6.4 のインストール設定は表 3 の通りとする。スレーブサーバの設定は表 4 の通りとする。

表 3　マスタサーバ設定

項目	設定内容
言語	Japanese（日本語）
キーボード	日本語
ホスト名	ns.example.com
IP アドレス	192.168.76.140
ネットマスク	24
ゲートウェイ	192.168.76.254
DNS	192.168.76.100
タイムゾーン	アジア/東京
システムクロック	UTC ではない
root パスワード	marugame

表 4　スレーブサーバ設定

項目	設定内容
言語	Japanese（日本語）
キーボード	日本語
ホスト名	ftp.example.com
IP アドレス	192.168.76.170
ネットマスク	24
ゲートウェイ	192.168.76.254
DNS	192.168.76.100
タイムゾーン	アジア/東京
システムクロック	UTC ではない
root パスワード	marugame

4.1 DVD マウントポイント

/media へ DVD をマウントするための設定を /etc/fstab に追加し、レポジトリ c6-media のみを指定することにより DVD 上のパッケージをインストールできるよう設定すること（マスタサーバ、スレーブサーバ共通）

4.2 wget

wget, openssh-clients をインストールすること（マスタサーバ、スレーブサーバ共通）

5. ユーザアカウント

スレーブサーバに以下のテキストファイルにより与えられるユーザアカウントを登録すること。

http://www.tsoftware.jp/tmp/userlist140711

5.1 パスワード

パスワードはユーザアカウントと同じとする。

5.2 ホームディレクトリ

ユーザは /home 直下にユーザ名と同じホームディレクトリを持つ。ホームディレクトリのアクセス権限は 700 とする。

5.3 プライマリグループ

ユーザはグループ share をプライマリグループとする。

5.4 Maildir

ユーザが受信したメールをスプールするための Maildir 形式のディレクトリを~/Maildir/inbox に作成すること。

6. SELinux

SELinux は Enforcing で運用すること。個々のサーバインストール要件に伴い SELinux の設定変更が必要となる場合は、当該サーバインストール要件において個別に記載する。

7. ファイアウォール

ファイアウォールの初期設定は表 5 の通りとする。ここでは SSH サーバへの接続のみを許可している。個々のサーバインストール要件に伴いファイアウォールの設定変更が必要となる場合は、当該サーバインストール要件において個別に記載する。

表 5　ファイアウォールの初期設定

```
*filter

:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

※空行は無くとも良い。

8. FTP サーバ

FTP サーバには vsftpd を使用する。インストール後の設定はファイアウォール、TCP Wrapper、SELinux について行う。

8.1 ファイアウォール設定

ファイアウォールは TCP/21 と TCP/22 へのアクセスを許可し、/etc/sysconfig/iptables-config に nf_conntrack_ftp のヘルパーモジュールを設定する。

8.2 TCP Wrapper 設定

TCP Wrapper により vsftpd へのアクセスを 192.168.76.0/24 に限定すること。

8.3 SELinux 設定

SELinux の設定を変更しホームディレクトリへのログインを許可すること。

9. MTA サーバ

MTA サーバ設定を表 6 に示す。

表 6　MTA サーバ設定

項目	設定内容
IP アドレス	all
ホスト名	mail.example.com
IP プロトコル	ipv4
メールドメイン	example.com
メールボックス形式	Maildir
メールスプール場所	~/Maildir/inbox

9.1　ファイアウォール設定

ファイアウォールは TCP/25 へのアクセスを許可すること。

9.2　MX レコード

スレーブサーバをホスト名 mail.example.com で名前解決できるよう DNS を設定すること。また当該ホストに関する MX レコードも併せて登録すること。

9.3　管理者用アカウント

メールボックスをホームディレクトリに置く設定としたため、root 宛のメールは root アカウントにより受信することはできない。そこで管理用のユーザアカウント admin を登録し、root 宛のメールは admin に配信されるよう /etc/aliasese を設定すること。

10. POP サーバ

POP サーバ設定を表 7 に示す。

表 7 POP サーバ設定

項目	設定内容
プロトコル	pop3
メールボックス形式	Maildir
メールスプール場所	~/Maildir/inbox

10.1 ファイアウォール設定

ファイアウォールは TCP/110 へのアクセスを許可すること。

10.2 平文テキストによる認証

平文テキストによる認証を許可すること。

11. DNS サーバ

DNS サーバには BIND を使用する。DNS サーバは管理ドメイン上のホスト名を解決するためのマスタサーバ、スレーブサーバの役割を担う。

11.1 ルートサーバ情報

本システムで使用するルートサーバ情報を表 8 に示す。

表 8 ルートサーバ情報

```
.                       518400  IN  NS  M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000 IN  A   192.168.76.100
```

11.2 ファイアウォール設定

ファイアウォールは TCP/53 と UDP/53 へのアクセスを許可すること。

12. 検査結果報告書

12.1 仮想マシン設定

項目	検査結果
メモリサイズ	
CPU 個数	
ハードディスク容量	

12.2 OS インストール

項目	検査結果
言語	
キーボード	
ホスト名	
IP アドレス	
ネットマスク	
ゲートウェイ	
DNS	
タイムゾーン	
システムクロック	
root パスワード	
DVD マウントポイント	

項目	検査結果
言語	
キーボード	
ホスト名	
IP アドレス	
ネットマスク	
ゲートウェイ	
DNS	
タイムゾーン	
システムクロック	
root パスワード	

DVD マウントポイント	

12.3 ユーザアカウント

項目	検査結果
ユーザアカウント登録	
パスワード	
プライマリグループ	
ホームディレクトリ	
共有ディレクトリ	

12.4 SELinux

項目	検査結果
SELinux モード	

12.5 ファイアウォール

項目	検査結果
基本設定	
SSH 接続	
FTP サーバ接続	
DNS サーバ接続	
MTA サーバ接続	
POP サーバ接続	

12.6 FTP サーバ

項目	検査結果
インストール	
ホームディレクトリログイン	
匿名ユーザコンテンツダウンロード	
TCP Wrapper 設定	

12.7 MTA サーバ

項目	検査結果
IP アドレス	
ホスト名	

IP プロトコル	
メールドメイン	
メールボックス形式	
メールスプール場所	

12.8 POP サーバ

項目	検査結果
プロトコル	
メールボックス形式	
メールスプール場所	
平文認証の許可	

12.9 DNS サーバ

項目	検査結果
インストール	
ルートサーバ情報	
マスタサーバ設定	
スレーブサーバ設定	

以上