

私立大学情報教育協会  
教育コンテンツ相互利用システム

---

コンテンツ管理 CGI  
インストールマニュアル

## 目次

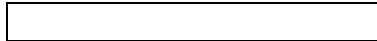
---

1	環境.....	3
1.1	バージョン.....	3
1.2	インストール環境.....	3
2	インストール手順.....	4
2.1	前提条件.....	4
2.1.1	CentOS.....	4
2.2	SSHD の設定 .....	7
2.3	VSFTPD の設定 .....	8
2.4	コンテンツ管理 CGI のインストール.....	10
3	権利者ユーザ登録.....	16

### 【備考】

このマニュアル上では枠の使い方を下記のようにしています。

コマンドラインに入力するコマンド



内容を修正する部分は  で表現しています。

テキストファイルなどの内容部分



内容を修正する部分は  で表現しています。

必要に応じてターミナル画面のキャプチャー画像を添える。

本文中のホスト名や IP アドレスは、実在のものではない。

# 1 環境

## 1.1 バージョン

No.	ソフトウェア	バージョン
1	コンテンツ管理 CGI	1.0

## 1.2 インストール環境

コンテンツ管理 CGI のインストールは以下の環境を前提とする。

Kind	Software	Version	Note
OS	CentOS	4.8	
Language	Perl	5.8.5	CentOS4.8 に含まれる
WebServer	Apache	2.0.52	CentOS4.8 に含まれる

## 2 インストール手順

コンテンツ管理 CGI のインストールは下記の順番にて行う。

- ① OS のインストール
- ② OS の環境設定
- ③ コンテンツ管理 CGI のインストール
- ④ その他

以下順に説明する。

### 2.1 前提条件

- 各権利者の FTP アカウントが、同一グループ(contents)に含まれており、httpd(apache)が動作するアカウントもこのグループに含める必要があります。
- 各権利者の FTP アカウントのホームディレクトリが、/var/www/home 直下であるとします。
- 各権利者の FTP アカウントのホームディレクトリに対して、httpd(apache)による書き込み権限が必要です。(0775)
- コンテンツファイルの名称に関しては、日本語に対応していない。

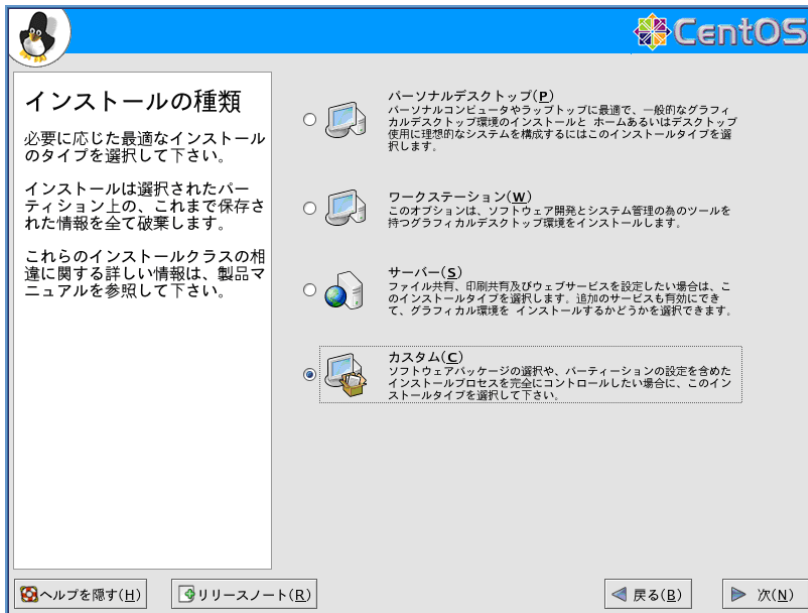
#### 2.1.1 CentOS

具体的なインストール手順についてはハードウェア構成やネットワーク、運用のポリシー等に依存するため、割愛する。

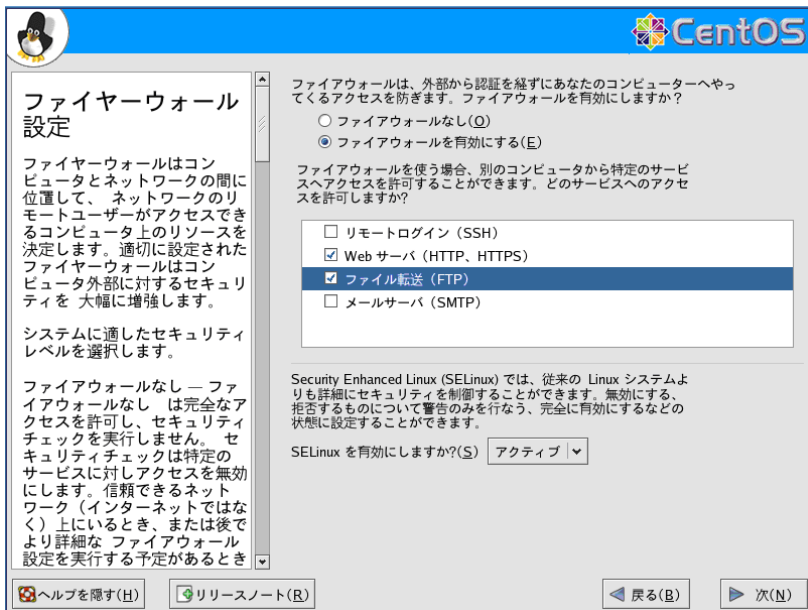
ここでは最低限必要なことのみ記載する。

なお、FTP に関する記述は、FTP によるアップロードを利用する場合にのみ適用する。インストール作業には、SSH を使用することを前提として説明している。

## (1) インストールの種類で「カスタム」を選択

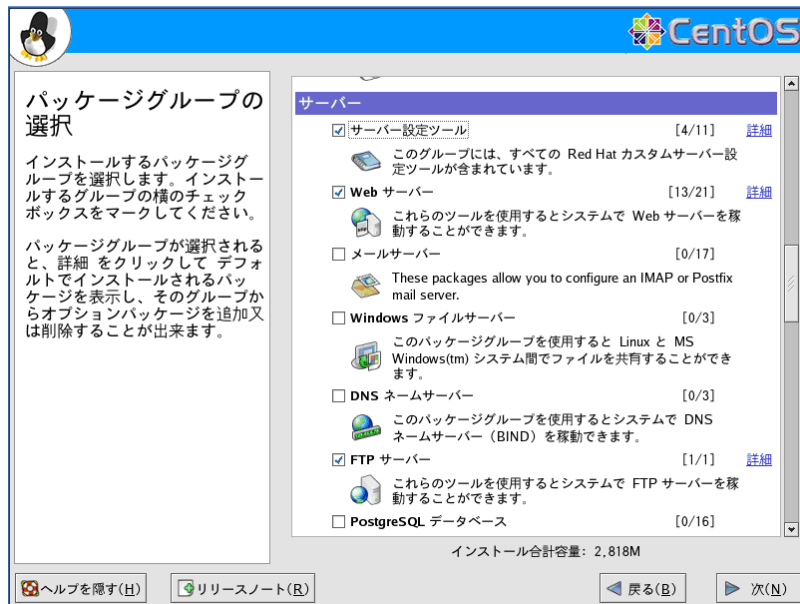


## (2) ファイアウォールの設定



- WWW (ポート 80) を許可する設定が必要
  - SSH (ポート 22) を許可する設定が必要
  - FTP にてファイルのアップロードを行う場合は FTP を許可する必要あり。
  - インストール作業には、SSH の使用を推奨します。
- ※「ファイアウォールなし」でも可

### (3) パッケージ選択



以下のパッケージを選択する。

- Webサーバ
- FTPサーバ
- ソフトウェア開発

そのほか必要に応じて選択する

### (4) アカウントの設定

root 以外に

manager アカウントを作成する。

※ インストール作業用に使用するのので、manager でなくてもよい。

```
useradd manager  
passwd manager
```

contents アカウントを作成する。

※ CGI によるファイルのアップロードで使用する。

※ ログインさせない為に nologin とした上で、ホームディレクトリを apache ホームディレクトリの下に作成する。

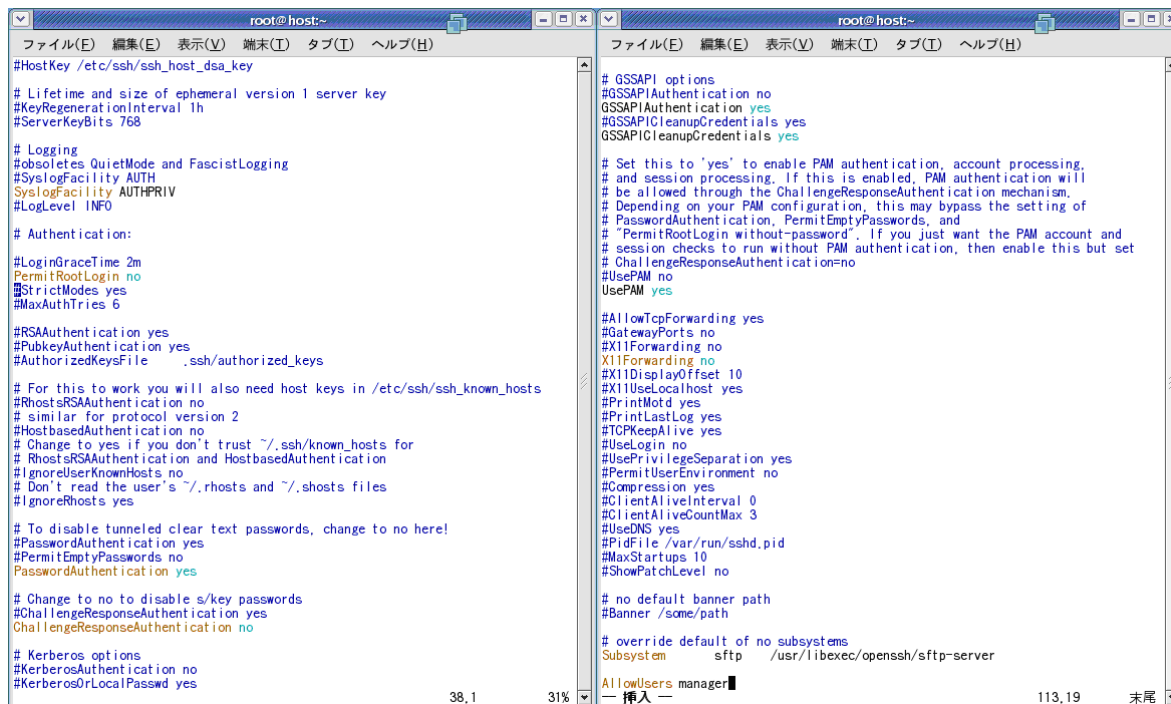
```
useradd -d /var/www/home -s /sbin/nologin contents
```

## 2.2 SSHD の設定

この作業は、管理者権限を必要とする。

インストール直後は、SSHD がリモートターミナルとして動作しているが、管理者権限 (root) でログインできてしまうので、設定変更が必要。

```
vi /etc/ssh/sshd_config
```



```
root@host:~# vi /etc/ssh/sshd_config
#HostKey /etc/ssh/ssh_host_dsa_key
# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:
#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
#ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
#GSSAPICleanupCredentials yes

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication mechanism.
# Depending on your PAM configuration, this may bypass the setting of
# PasswordAuthentication, PermitEmptyPasswords, and
# "PermitRootLogin without-password". If you just want the PAM account and
# session checks to run without PAM authentication, then enable this but set
# ChallengeResponseAuthentication=no
#UsePAM no
UsePAM yes

#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10
#ShowPatchLevel no

# no default banner path
#Banner /some/path

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

AllowUsers manager
```

```
# 以下の変更を行う
#PermitRootLogin yes
PermitRootLogin no
X11Forwarding no
# 以下の項目を追加
AllowUsers manager
```

変更を行った後は、

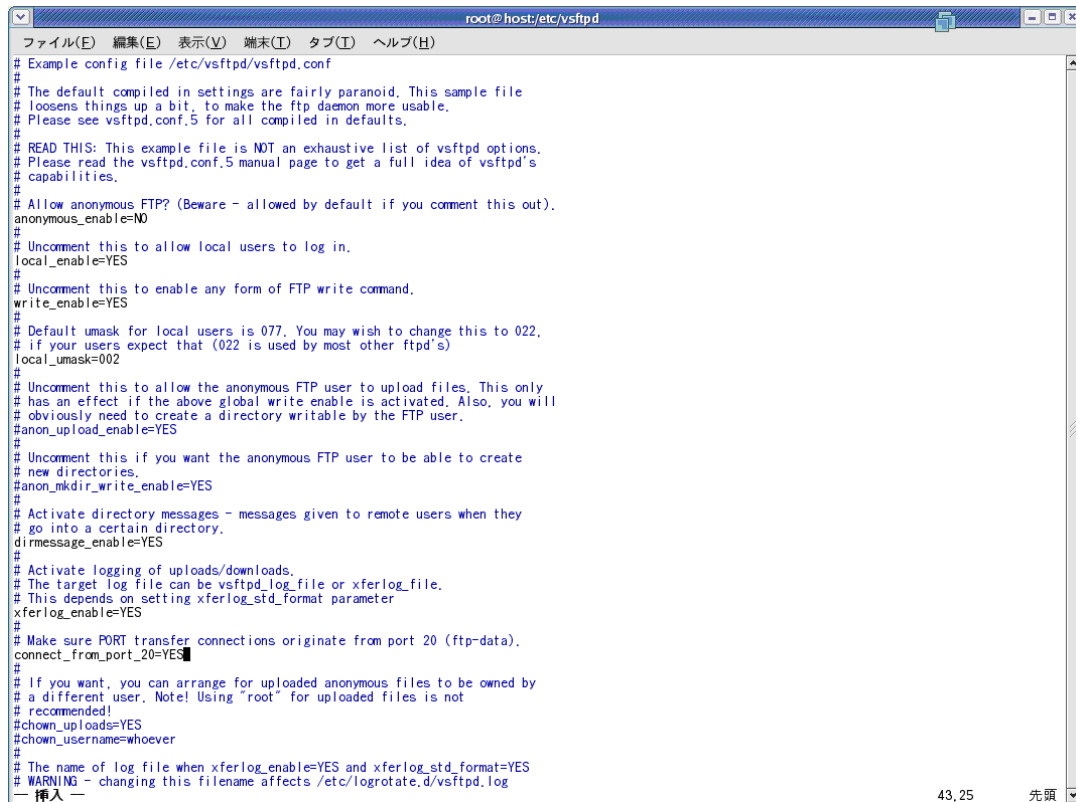
```
service sshd restart
```

## 2.3 VSFTPD の設定

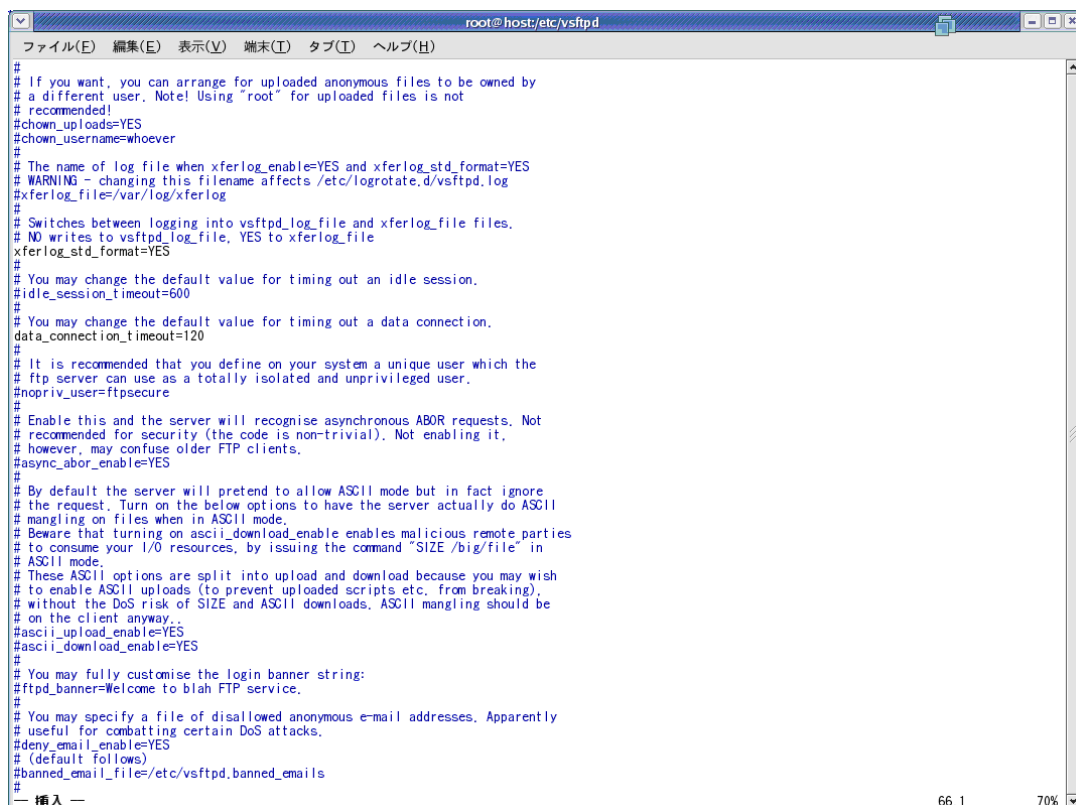
この作業は、管理者権限を必要とする。

コンテンツのアップロードに FTP を用いる場合には、VSFTPD を用いる。インストール直後には、ユーザーは、他のディレクトリを参照できてしまうので、chroot の制約を設定する必要がある。

```
vi /etc/vsftpd/vsftpd.conf
```



```
root@host:/etc/vsftpd
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(I) ヘルプ(H)
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022.
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
# The target log file can be vsftpd_log_file or xferlog_file.
# This depends on setting xferlog_std_format parameter
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# The name of log file when xferlog_enable=YES and xferlog_std_format=YES
# WARNING - changing this filename affects /etc/logrotate.d/vsftpd.log
— 挿入 —
43,25 先頭
```



```
root@host:/etc/vsftpd
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(I) ヘルプ(H)
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# The name of log file when xferlog_enable=YES and xferlog_std_format=YES
# WARNING - changing this filename affects /etc/logrotate.d/vsftpd.log
#xferlog_file=/var/log/xferlog
#
# Switches between logging into vsftpd_log_file and xferlog_file files.
# NO writes to vsftpd_log_file, YES to xferlog_file
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
— 挿入 —
66,1 70%
```



```
root@host:/etc/vsftpd
ファイル(F) 編集(E) 表示(V) 端末(T) タブ(I) ヘルプ(H)
# You may change the default value for timing out a data connection.
data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES

pam_service_name=vsftpd
userlist_enable=YES
#enable for standalone mode
listen=YES
— 挿入 —
102, 30 98%
```

```
# 以下の変更を行う
anonymous_enable=NO
write_enable=YES
local_umask=002
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

#項目の記述がないものは、追記をする。

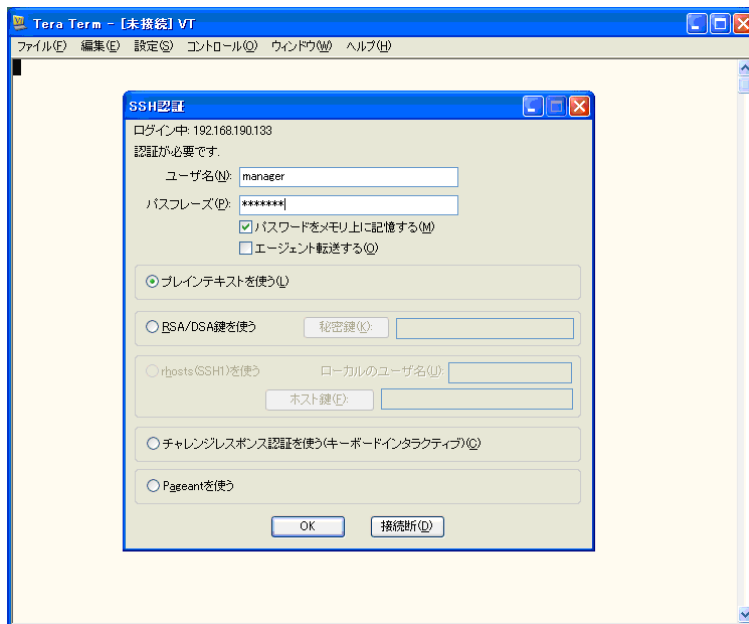
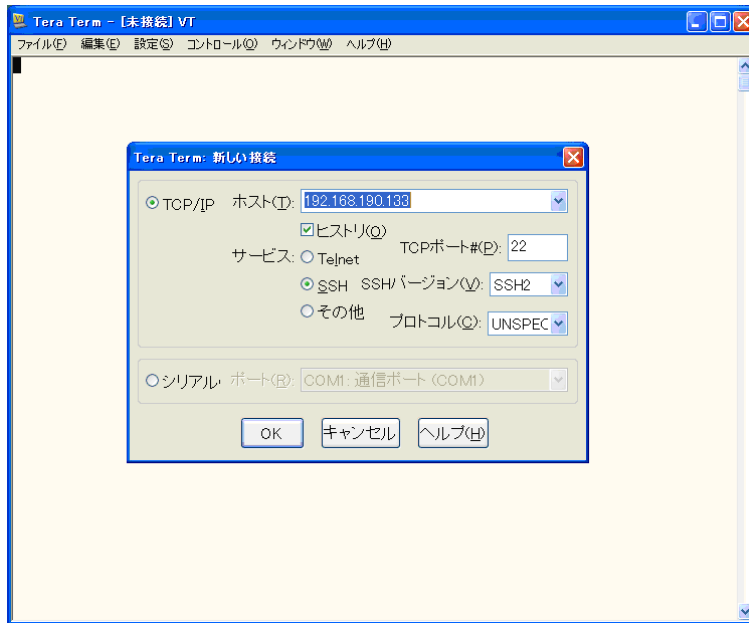
変更を行った後は、

```
service vsftpd restart
```

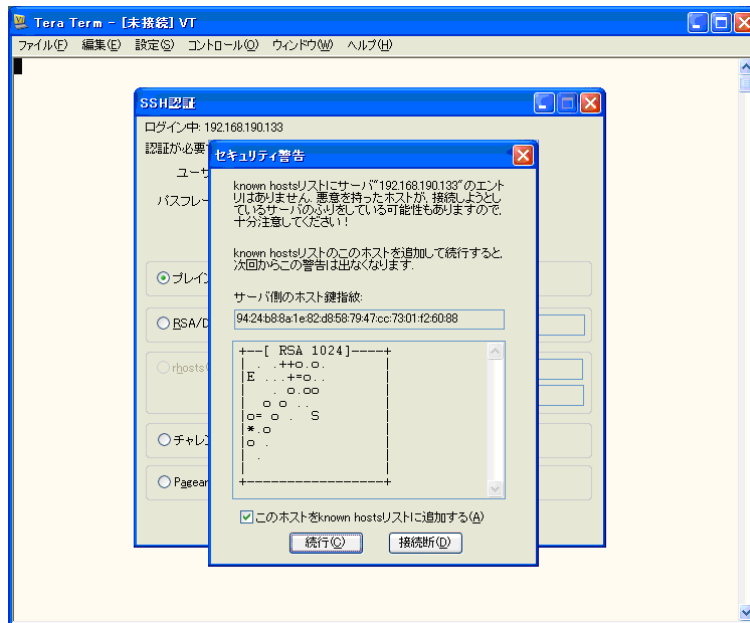
## 2.4 コンテンツ管理 CGI のインストール

コンテンツ管理 CGI のパッケージをサーバに転送する為には、Tera Term 等を用いる。ここでは、Tera Term によるインストール手順を説明する。

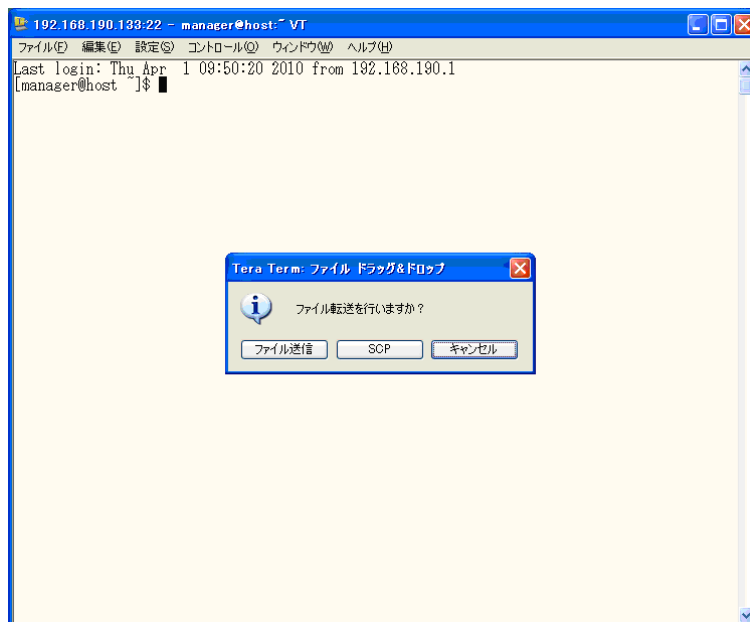
- Tera Term を起動し manager でサーバの SSH ポートにログインする。



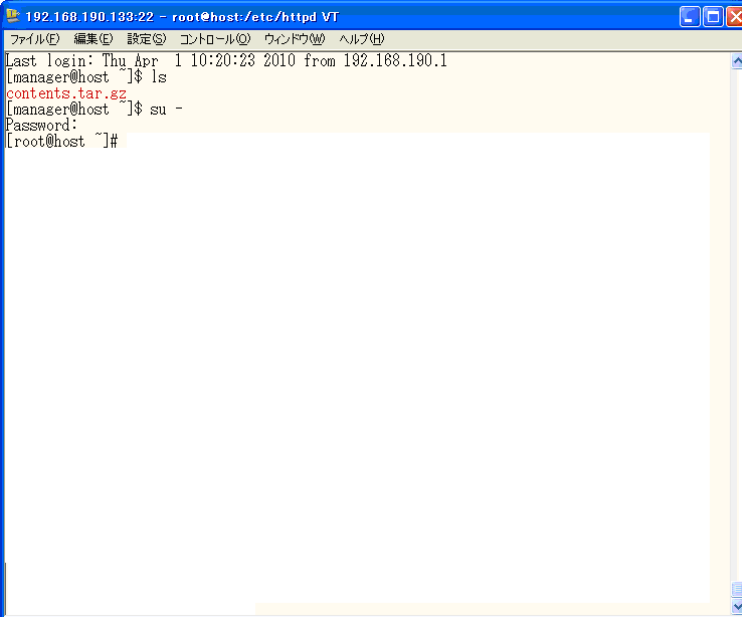
※ 初回起動時は、サーバの認証を求められる。



- コンテンツ管理 CGI パッケージ (contents.1.0.tar.gz) を Tera Term にドラッグ&ドロップする。  
※ ドラッグ&ドロップ時に転送方法の問い合わせがあるが、SCP を選択する。



- アップロードしたことを確認して管理者権限に切り替える。



```
192.168.190.133:22 - root@host:/etc/httpd VT
ファイル(F) 編集(E) 設定(S) コントロール(C) ウィンドウ(W) ヘルプ(H)
Last login: Thu Apr 1 10:20:23 2010 from 192.168.190.1
[manager@host ~]$ ls
contents.tar.gz
[manager@host ~]$ su -
Password:
[root@host ~]#
```

- Manager のホームディレクトリにあるコンテンツ管理パッケージを apache のホームディレクトリにコピーする。

```
cp ~/contents/contents.tar.gz ~/apache/
```

- apache のホームディレクトリに移動して、contents.1.0.tar.gz を解凍する。

```
cd ~/apache
tar zxvf contents.tar.gz
```

- コンテンツ管理 CGI の設定ファイルを編集する。

```
vi ~/apache/contents/ContentsManage/CommonMange.pm
```

```
}  
# edit area start  
#  
my @remote_list = (  
    '210.150.12.50',  
    '210.150.12.114',  
    '210.150.12.52',  
    '202.79.242.59',  
);  
my $base_dir = '/var/www/home';  
my $tmp_dir = '/tmp';  
#my $access_log = "| rotatelogs /var/www/contents/log/contents_log.%Y.%m.%d 86400";  
my $access_log = '';  
my $error_log = '';  
my $debug_log = '';  
  
my $key_timeout = 60;  
# edit area end  
my $ver = '1.0';  
my $base_url = 'FileDownload.cgi';  
my $random_length = 32;
```

※ 編集対象は、以下の3点

```
my $remote_list = (  
'xxx.xxx.xxx.xxx' # (私情協側管理システム IP アドレス)  
);  
my $base_dir = '/var/www/home'; (権利者アカウント管理ディレクトリ)  
my $tmp_dir = '/tmp'; (一時ファイル作成場所)  
my $access_log = ""; (ログの出力先、空の場合はログを出力しない)  
my $error_log = ""; (ログの出力先、空の場合はログを出力しない)  
my $debug_log = ""; (通常空)
```

※ログ出力先の記述フォーマットは、最初に「|」を記述して、コンソールの出力先を指定する。

例) my \$access\_log = "| rotatelogs /var/www/contents/log/contents\_log.%Y.%m.%d 86400"

#### 注意事項)

1. これらの設定に誤りがあると CGI は正常に動作しない。
2. \$base\_dir を DocumentRoot 配下にするとすべてのコンテンツが公開されてしまう。

#### ● HTTPD の設定ファイルを変更する。

##### ① Apache の設定を変更する。

コンテンツ管理 CGI は、作成するページによって shift\_jis および utf-8 を用いるマルチ言語である為、Apache 側での対応が必要となる。

また、Perl の実行は必須である為、設定の確認を行う必要がある。

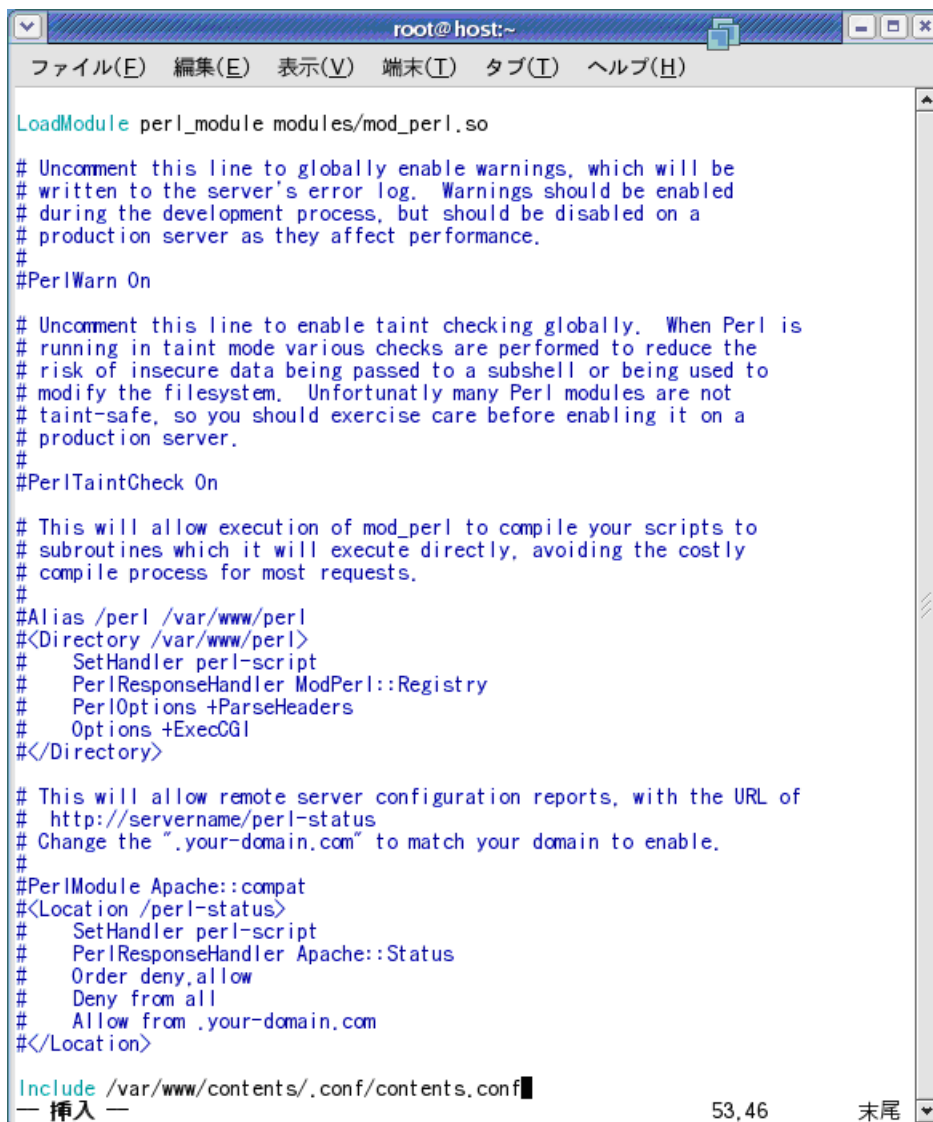
- ✓ Group を contents に変更する。 (必須)
- ✓ AddDefaultCharset が定義されている場合は、コメントアウトする。
- ✓ LanguagePriority の先頭に ja を記述する。
- ✓ AddLanguage ja の順番を先頭にする。
- ✓ AddCharset の順番を shift\_jis, utf-8, euc-jp の順にする。

- ② コンテンツ管理 CGI の設定を追加する。  
/var/www/contents/.conf/contents.conf にコンテンツ管理 CGI が動作する設定を記述しているの、apache 設定に Include させる。  
インストール場所がマニュアルと違うなど必要に応じ contents.conf を編集する。

✓ コンテンツ管理 CGI を実行するホストのディレクティブに Include を追加する

```
Include /var/www/contents/.conf/contents.conf
```

※ 下記の例は、/etc/httpd/conf.d/perl.conf に追記をした。



```
root@host:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
LoadModule perl_module modules/mod_perl.so

# Uncomment this line to globally enable warnings, which will be
# written to the server's error log. Warnings should be enabled
# during the development process, but should be disabled on a
# production server as they affect performance.
#
#PerlWarn On

# Uncomment this line to enable taint checking globally. When Perl is
# running in taint mode various checks are performed to reduce the
# risk of insecure data being passed to a subshell or being used to
# modify the filesystem. Unfortunately many Perl modules are not
# taint-safe, so you should exercise care before enabling it on a
# production server.
#
#PerlTaintCheck On

# This will allow execution of mod_perl to compile your scripts to
# subroutines which it will execute directly, avoiding the costly
# compile process for most requests.
#
#Alias /perl /var/www/perl
#<Directory /var/www/perl>
#   SetHandler perl-script
#   PerlResponseHandler ModPerl::Registry
#   PerlOptions +ParseHeaders
#   Options +ExecCGI
#</Directory>

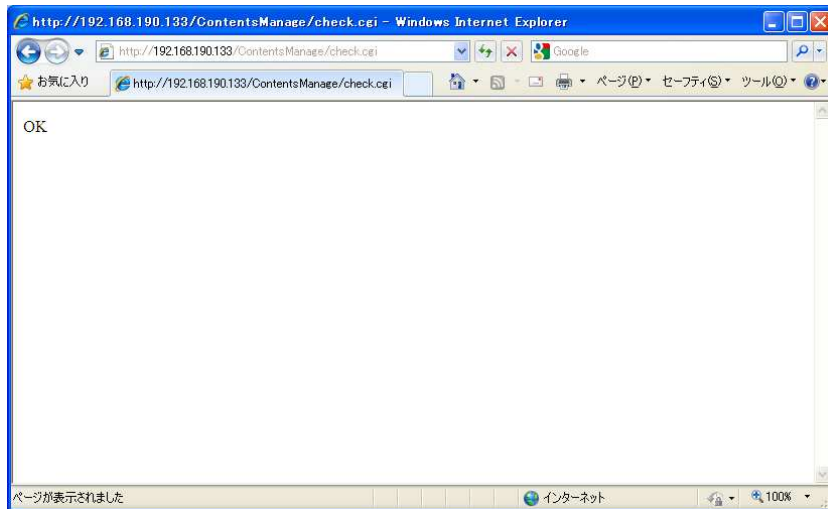
# This will allow remote server configuration reports, with the URL of
# http://servername/perl-status
# Change the ".your-domain.com" to match your domain to enable.
#
#PerlModule Apache::compat
#<Location /perl-status>
#   SetHandler perl-script
#   PerlResponseHandler Apache::Status
#   Order deny,allow
#   Deny from all
#   Allow from .your-domain.com
#</Location>

Include /var/www/contents/.conf/contents.conf
— 挿入 — 53,46 末尾
```

- 各設定が完了したら、HTTPD の再起動を行う。

```
service httpd restart
```

- 動作確認ページにアクセスして、動作状況を確認する。  
コンテンツ管理 CGI には動作確認用のページ (check.cgi) を用意しているので、ブラウザから呼び出す。



Apache の設定が行われていない場合は、この画面が表示されない。

各ログを設定した場合は、それぞれファイルが作成されていることを確認する。  
(check.cgi にて、test の文字を出力している)

#### 【確認事項】

- FTP を使用したとき、ホームディレクトリ以外に移動できないことを確認する。
- anonymous ユーザでログインすることができないことを確認する。
- SSH でログインできるのが、manager だけであることを確認する。

### 3 権利者ユーザ登録

#### (1) umask 変更

ユーザーが通常ファイルを作成するとグループに書き込み権限がないので、`/etc/bashrc` を編集して、ユーザー全体にファイルやディレクトリの作成時にグループへの書き込み権限を加えられるようにする。

```
vi /etc/bashrc
```

```
# mask 022;  
umask 002;
```

#### (2) useradd デフォルト設定変更

`useradd` コマンドのデフォルト設定を行うとユーザアカウント作成時の手間が減る。

```
vi /etc/default/useradd
```

※ 以下の設定にすると便利

```
GROUP=[contents の GID]  
HOME=/var/www/home
```

#### (3) ユーザの登録

`adduser` コマンドで Linux ユーザの登録を行う。GID、UID、ユーザ名は任意で指定する。ユーザ登録後、`passwd` コマンドでパスワードを指定する。

```
useradd -g contents -d /var/www/home/[ユーザ名] [ユーザ名]  
passwd [ユーザ名]
```

(2) のデフォルト設定を行った場合は、`useradd [ユーザ名]` のみで作成できる。

#### (4) ホームディレクトリのパーミッション変更

作成ユーザのホームディレクトリをコンテンツの格納先とする。ダウンロード処理を実行するため、ホームディレクトリのパーミッションを `apache` の実行ユーザから参照可能なように変更する。

```
chmod 775 /var/www/home/[ユーザ名]
```

(1) の設定を行っている場合は、不要