

Secioss OTP マニュアル

2. 0. 1 版

株式会社セシオス

目次

1.	イントロダクション	4
1.1.	Secioss OTP	4
1.2.	機能	4
1.2.1.	ソフトウェアトークン	4
1.2.2.	認証サーバ	4
1.3.	ソフトウェア環境	4
1.3.1.	ソフトウェアトークン	4
1.3.2.	認証サーバ	4
2.	認証サーバのインストール	4
2.1.	必要なパッケージのインストール	4
2.2.	インストール	5
2.2.1.	ionCube PHP Encode のインストール(B2C ライセンスの場合)	5
2.3.	ログの設定	5
2.4.	時刻の設定	5
3.	設定	6
3.1.	ワンタイムパスワード認証の設定	6
3.1.1.	LDAP サーバの設定	7
3.1.2.	DB サーバの設定	7
3.2.	暗号化キーの設定	7
4.	ワンタイムパスワード登録	7
4.1.	PIN の発行	8
4.1.1.	メールの設定	8
4.2.	PIN の削除	8
5.	ユーザのワンタイムパスワード設定	9
5.1.	ソフトウェアトークン	9
5.1.1.	インストール	9
5.1.2.	シークレットキーの生成	9
5.1.3.	ワンタイムパスワードの表示	10
5.2.	ワンタイムパスワードのシークレットキー登録	11
5.2.1.	PIN の登録	13
6.	システムとの連携	14
6.1.	Web アプリケーション	14

6.2.	SSL-VPN.....	14
6.2.1.	インストール(サーバ)	14
6.2.1.	証明書関連の作成(サーバ)	15
6.2.2.	OpenVPN の設定(サーバ)	16
6.2.1.	起動と停止(サーバ).....	20
6.2.2.	インストール(クライアント)	21
6.2.3.	OpenVPN の設定(クライアント)	21
6.2.4.	動作確認(クライアント)	22
6.3.	RADIUS.....	22
6.3.1.	インストール.....	22
6.3.2.	FreeRADIUS の設定	23
6.3.3.	起動と停止.....	25
6.3.4.	動作確認.....	26
7.	ログ	27
7.1.	認証サーバ.....	27
7.2.	SSL-VPN サーバ(OpenVPN)	27
7.3.	RADIUS サーバ(FreeRADIUS2).....	27

1. イントロダクション

1.1. Secioss OTP

Secioss OTP は、携帯電話を使用したワンタイムパスワード認証ソリューションです。携帯電話にソフトウェアトークンをインストールし、携帯電話に表示された 1 分毎に変化するパスワードでログインします。

万が一、入力したパスワードを盗み見られた場合でも、同じパスワードは二度と使用できないため、不正にログインすることはできません。

1.2. 機能

Secioss OTP は、時刻同期式のワンタイムパスワードで、アルゴリズムには RFC 標準の HOTP を使用しています。

Secioss OTP は、以下のソフトウェアから構成されています。

1.2.1. ソフトウェアトークン

携帯電話にインストールするソフトウェアトークンです。ソフトウェアを起動すると、1 分毎に異なるパスワードを表示します。

1.2.2. 認証サーバ

認証サーバは、ワンタイムパスワードの認証を行うサーバです。

ユーザの認証情報は LDAP サーバ、DB サーバに格納することができます。

1.3. ソフトウェア環境

1.3.1. ソフトウェアトークン

- ・ 携帯電話： NTT Docomo、AU、Softbank、iPhone

1.3.2. 認証サーバ

- ・ OS： Redhat Enterprise Linux 5、Cent OS 5
- ・ Web サーバ： Apache 2.2

2. 認証サーバのインストール

2.1. 必要なパッケージのインストール

以下の rpm パッケージをインストールして下さい。

- ・ php-pear
- ・ php-ldap
- ・ php-xml
- ・ perl-LDAP
- ・ perl-DBI
- ・ perl-Digest-SHA1

```
# yum install <パッケージ名>
```

2.2. インストール

Secioss OTP のパッケージファイルを展開し、インストールスクリプトを実行します。
次に、Web サーバを再起動します。

```
# ./install.sh install
```

```
# /etc/init.d/http restart
```

また、Secioss OTP をアップデート、アンインストールする場合は、次のようにインストールスクリプト実行して下さい。

- アップデート

```
# ./install.sh update
```

- アンインストール

```
# ./install.sh uninstall
```

2.2.1. ionCube PHP Encode のインストール

http://www.asial.co.jp/ioncube/encoder/download_loaders.php から ionCube PHP Encoder のローダーをダウンロードして、インストールして下さい。

2.3. ログの設定

Secioss OTP 認証サーバのログを出力するには `syslog.conf` を設定します。

```
# vi /etc/syslog.conf
```

以下の行を追加します。

local5.*	/var/log/auth.log
----------	-------------------

最後に `syslogd` を再起動します。

```
# /etc/init.d/syslog restart
```

2.4. 時刻の設定

Secioss OTP は、時刻同期式のワンタイムパスワードであるため、認証サーバの時刻を正しい時刻に設定する必要があります。

以下のコマンドを実行して、正しい時刻を設定して下さい。

```
# /usr/sbin/ntpdate <時刻同期サーバ>
```

例 : `# /usr/sbin/ntpdate ntp.nict.jp`

3. 設定

3.1. ワンタイムパスワード認証の設定

ワンタイムパスワード認証の設定ファイルを環境に合わせて変更します。設定ファイルには以下のファイルがあります。

- /var/www/conf/config.ini : ワンタイムパスワード認証の設定ファイル

設定は次のように記述します。

```
[password]
storage = LDAP
uri = ldap://localhost
binddn = "cn=Manager,dc=example,dc=com"
bindpw = secret
basedn = "dc=example,dc=com"
keyfile = /etc/httpd/conf.d/auth_tkt.conf
```

各設定項目の解説を以下に示します。

設定項目	デフォルト値	説明	
共通	storage	-	ユーザ情報を格納しているデータベースの種類 (LDAP DB File)
	keyfile	-	PIN、シークレットキーを暗号化するためのキーが記述されているファイル名
	input	-	ユーザのシークレット設定画面でオプションとして表示する設定項目 ・ pin: PIN
LDAP	uri	ldap://localhost	LDAP サーバの URI
	binddn	-	LDAP サーバに接続するユーザの DN
	bindpw	-	LDAP サーバに接続するパスワード
	basedn	-	ユーザ情報を検索する際のベース DN
	userattr	uid	ユーザ ID が格納されている属性名 ※属性名は全て小文字として下さい
DB	dsn	-	DB サーバに接続する際の PHP の DSN 例: mysql://admin:secret@localhost/users
	table	-	ユーザ情報が格納されているテーブル名
	usercol	-	ユーザ ID が格納されているフィールド名
	pwdcol	-	ユーザのシークレットキー登録時のログインパスワードが格納されているフィールド名

File	file	-	ユーザ情報が格納されているファイル ファイル形式: <ユーザ ID>,<PIN>,<シークレットキー>
------	------	---	---

表 1 ワンタイムパスワード認証の設定項目

3.1.1. LDAP サーバの設定

ユーザ情報を確認する LDAP サーバに対して、ワンタイムパスワード用の設定を行います。パッケージを展開したフォルダ内の”conf/secioss.schema”を”/etc/openldap/schema”にコピーして、OpenLDAP の設定ファイルに以下の設定を追記してから、LDAP サーバを再起動して下さい。

```
include /etc/openldap/schema/ppolicy.schema
include /etc/openldap/schema/secioss.schema
```

3.1.2. DB サーバの設定

ユーザ情報を格納するデータベースにワンタイムパスワード用のテーブルを作成します。ユーザ情報のテーブルに以下のフィールドを追加して下さい。

- secretpin
- initsecret

さらに、ワンタイムパスワード用のテーブルを作成します。

```
CREATE TABLE `otphashes` (
  `timestamp` datetime NOT NULL,
  `<id_def で設定したユーザ ID のフィールド名>` varchar(255) NOT NULL,
  `otp` varchar(255) NOT NULL
);
```

3.2. 暗号化キーの設定

Secioss OTP では、ユーザの PIN、シークレットキーを暗号化して保存しますが、暗号化の際のキーを設定します。”/var/www/conf/auth_tkt.conf”の TKTAuthSecret に暗号化キーとする文字列を設定して下さい。

```
TKTAuthSecret <暗号化キーの文字列>
```

4. ワンタイムパスワード登録

管理者からユーザに PIN を発行する場合の方法です。

ユーザ自身に PIN を登録させる場合は、“5.2.1 PIN の登録”を参照して下さい。

4.1. PIN の発行

ワンタイムパスワードを発行するユーザのユーザ ID のリストを CSV ファイルとして作成します。CSV ファイルの形式は以下になります。

```
<ユーザ ID>,<PIN>
```

PIN が省略された場合は、ランダムな値が設定されます。

次のコマンドを実行すると CSV ファイルに登録されているユーザにワンタイムパスワードの PIN を発行するとともに、ユーザ情報にメールアドレスを持つユーザに対しては、メールで PIN を通知します。

```
# /opt/secioss/sbin/otppadd add <CSV ファイル> <エラー出力ファイル>
```

PIN の登録に失敗したユーザは、エラー出力ファイルに記録されます。

4.1.1. メールの設定

PIN をユーザにメールで通知する際のメールサーバとメールの文章を設定します。

メールサーバの設定ファイル”/var/www/conf/mail-config.ini”を環境に合わせて変更します。

```
postmaster = “<送信元メールアドレス>”  
smtp = “<メールサーバのホスト名>:<ポート番号>”  
smtpauth_user = “<SMTP 認証のユーザ>”  
smtpauth_pass = “<SMTP 認証のパスワード>”
```

SMTP 認証は、LOGIN、PLAIN、CRAM-MD5、Digest-MD5 に対応しています。

次にメールの文章を”/var/www/conf/otppin.mail”に記述して下さい。

`{id}`、`{name}`、`{pin}`はそれぞれユーザ ID、氏名、PIN に置換されます。

```
Subject: PIN の通知  
{id} {name}さん  
  
あなたの PIN は{pin}です。
```

4.2. PIN の削除

ワンタイムパスワード認証の使用を停止する場合、ユーザから PIN を削除します。

次のコマンドを実行すると CSV ファイルに登録されているユーザの PIN をユーザ情報から削除します。

```
# /opt/secioss/sbin/otppadd delete <CSV ファイル> <エラー出力ファイル>
```

5. ユーザのワンタイムパスワード設定

5.1. ソフトウェアトークン

5.1.1. インストール

以下の URL から携帯電話に合わせてソフトウェアトークンをダウンロードして、インストールして下さい。

- ・ <http://www.secioss.co.jp/otp/>

iPhone のソフトウェアトークンについては、App Store から”Secioss OTP”を検索してダウンロードして下さい。

5.1.2. シークレットキーの生成

ソフトウェアを起動して、メールで通知された PIN を入力します。



図 1 シークレット PIN の入力

最初は“新しいシークレット”を選択し、無作為に 20 回ボタンを押して下さい。
次に新しいシークレットのエイリアス名を入力してから、NTT Docomo の場合は OK ボタンを押し、au、Softbank の場合はメニューから次へを選択します。



図 2 エイリアス名の入力

シークレットキーが表示されますので、この値を “5.2 ワンタイムパスワードのシークレットキー登録” で認証サーバに登録します。

5.1.3. ワンタイムパスワードの表示

メニューから “メインメニュー” 選択した後、使用するワンタイムパスワードのエイリアス名を選択します。

すると、1分毎にパスワードが表示されますので、これをログイン時に使用して下さい。



図 3 ワンタイムパスワードの表示

5.2. ワンタイムパスワードのシークレットキー登録

ユーザは、ワンタイムパスワードのシークレットキーを自身で登録することができます。

URL : <https://<Secioss OTP 認証サーバのホスト名>/user/index.php> にアクセスして、ログイン画面からユーザ名と固定パスワードを入力してログインして下さい。

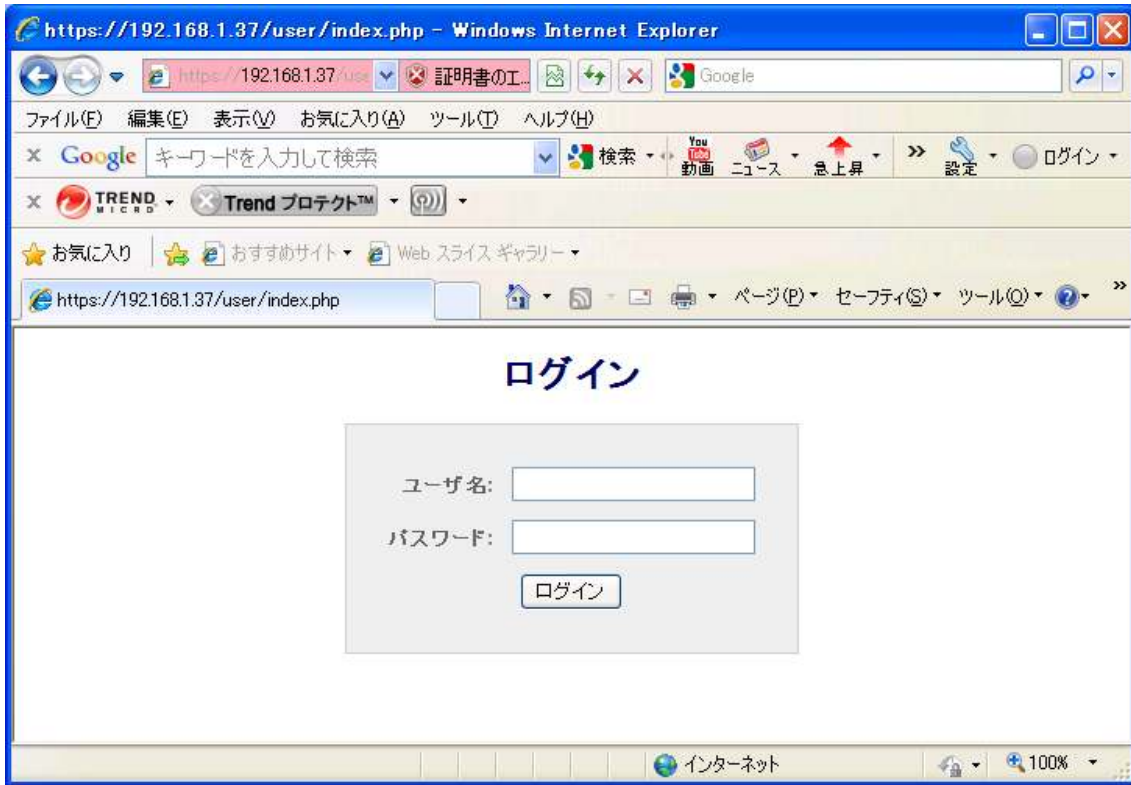


図 4 シークレット設定のログイン画面

シークレットの設定画面が表示されたら、ソフトウェアトークンが生成したシークレットキーを入力して設定ボタンをクリックして下さい。

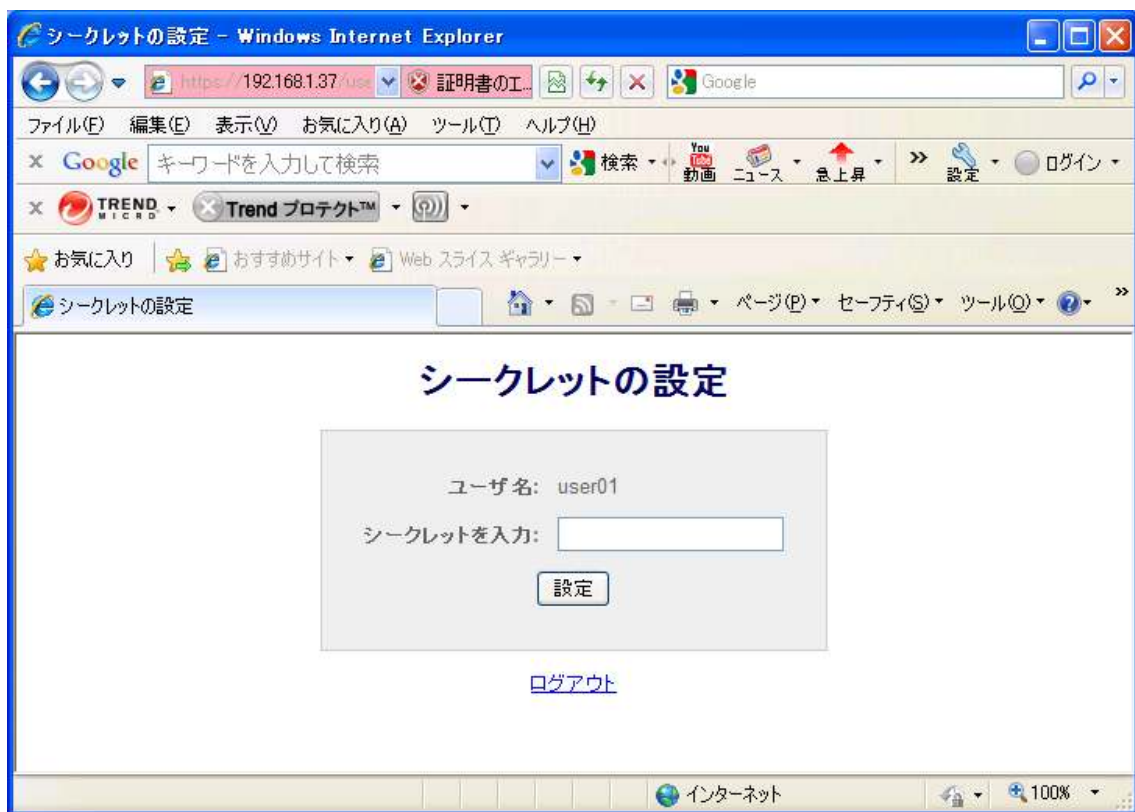


図 5 シークレットの設定

5.2.1. PIN の登録

ユーザ自身に PIN を設定させることも可能です。

“/var/www/conf/config.ini”に”input = pin”と設定することで、シークレットの設定画面から PIN を設定できるようになります。（表 1 ワンタイムパスワード認証の設定項目”を参照）

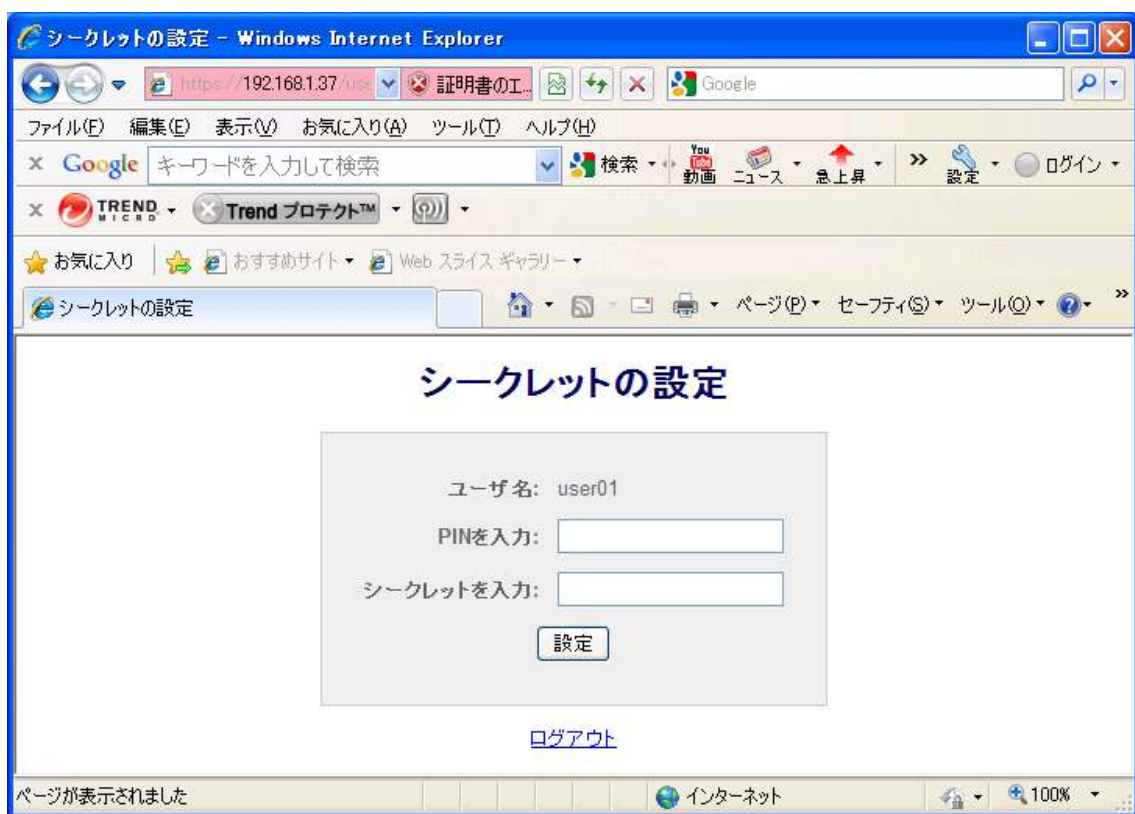


図 6 シークレットの設定 (PIN の登録)

6. システムとの連携

6.1. Web アプリケーション

Web アプリケーションから、ワンタイムパスワード認証を行うには、以下の方法でユーザ ID とワンタイムパスワードを SecioSS OTP の認証サーバに送信して下さい。

- URL : `https://<SecioSS OTP 認証サーバのホスト名>/pub/otp.php?userid=<ユーザ ID>`
- POST データ
 - `password` : ワンタイムパスワード

6.2. SSL-VPN

参考として本資料では、OpenVPN のインストールと設定について説明します。

6.2.1. インストール (サーバ)

以下の rpm パッケージをインストールして下さい。

- `perl-libwww-perl`
- `perl-XML-Simple`

```
# yum install <パッケージ名>
```

OpenVPN は、Secioss OTP パッケージ内の `vpn` フォルダに 32bit、64bit の rpm パッケージがありますので、OS に合ったパッケージを rpm コマンドでインストールして下さい。

```
# rpm -Uvh <パッケージフォルダ>/vpn/openvpn-2.x.x-x.el5.i386.rpm (32bit OS の場合)
```

6.2.1. 証明書関連の作成 (サーバ)

6.2.1.1. 前準備

- 証明書／秘密鍵作成用ディレクトリのコピー

```
# cp -r /usr/share/openvpn/easy-rsa/2.0/ /etc/openvpn/easy-rsa
```

```
# cd /etc/openvpn/easy-rsa/
```
- 証明書／秘密鍵作成用の環境変数設定ファイルを編集

```
# vi vars
```

以下は、設定例です。

<pre>export KEY_COUNTRY="JP"</pre>	所在地(国名)
<pre>export KEY_PROVINCE="Tokyo"</pre>	所在地(都道府県名)
<pre>export KEY_CITY="Bunkyo"</pre>	所在地(市区町村名)
<pre>export KEY_ORG=" myhost.mydomain "</pre>	サーバー名
<pre>export KEY_EMAIL="me@mail.myhost.mydomain"</pre>	管理者メールアドレス

- 証明書／秘密鍵作成用の環境変数を読み込む

```
# source vars
```

6.2.1.2. CA 証明書・秘密鍵作成

- 作成先ディレクトリ初期化

```
# ./clean-all
```
- CA 証明書・秘密鍵作成

```
# ./build-ca
```
- CA 証明書を配置

```
# cp keys/ca.crt /etc/openvpn/
```

6.2.1.3. サーバ証明書・秘密鍵作成

- サーバ証明書・秘密鍵作成

```
# ./build-key-server server
```
- サーバ証明書・秘密鍵を配置

```
# cp keys/server.crt /etc/openvpn/
```

```
# cp keys/server.key /etc/openvpn/
```

6.2.1.4. DH (Diffie Hellman)パラメータ作成

- DH パラメータ作成
./build-dh
- DH パラメータを配置
cp keys/dh1024.pem /etc/openvpn/

6.2.1.5. TLS 認証鍵作成

- TLS 認証鍵を OpenVPN 設定ファイル格納ディレクトリに作成
openvpn --genkey --secret /etc/openvpn/ta.key

6.2.2. OpenVPN の設定 (サーバ)

設定ファイルは、「/etc/openvpn」配下に作成します。

OpenVPN の設定ファイルは、サンプルをコピーして作成します。

```
# cp /usr/share/doc/openvpn-x.x.x/sample-config-files/server.conf /etc/openvpn/
```

その後、手順に従って編集してください。

6.2.2.1. server.conf の設定

OpenVPN の設定を行います。

※VPN 通信用の仮想ネットワークアドレスは「10.8.0.0/24」で、VPN サーバの仮想 IP アドレスは「10.8.0.1」となります。(デフォルトの設定をそのまま使用しています。)

```
# vi /etc/openvpn/server.conf
```

以下は、SeciossOTP サーバの IP アドレスが 192.168.1.37 の場合の設定例です。

※ 変更箇所を記述しています。

```

:
#LAN へのルートを VPN サーバー経由にする。(192.168.200.0 の場合)
push "route 192.168.200.0 255.255.255.0"
:
#コメントを解除して、TLS 認証を有効化する。
tls-auth ta.key 0 # This file is secret
:
#コメントを解除して、OpenVPN 実行権限を下げます。
user nobody
group nobody
:
#コメントを解除して、ログを/var/log/openvpn.log に出力します。
log-append /var/log/openvpn.log
:
#最終行に以下の 4 行を追加して、認証方法を SeciossOTP スクリプトに設定
tmp-dir /tmp
auth-user-pass-verify "/opt/secioss/sbin/otpauth -h 192.168.1.37" via-file
client-cert-not-required
username-as-common-name
#最終行には、管理インタフェースの有効化を設定し、クライアントの接続状況や
#強制切断が行えるようにします。
management localhost 7505
```

6.2.2.2. openvpn-startup の設定

- ・ ファイアウォール自動設定スクリプト作成

OpenVPN 起動時に実行するファイアウォール自動設定スクリプトを作成します。

```
# vi /etc/openvpn/openvpn-startup
```

以下の設定例は、VPN クライアントから LAN (192.168.200.0/24) へのアクセスを許可する場合です。

```
#!/bin/bash

# その後作成する、ファイアウォール自動設定解除スクリプトを実行します。
/etc/openvpn/openvpn-shutdown

# VPN サーバーからの送信を許可します。
iptables -I OUTPUT -o tun+ -j ACCEPT
iptables -I FORWARD -o tun+ -j ACCEPT

# VPN クライアントから VPN サーバーへのアクセスを許可する場合に設定します。
iptables -I INPUT -i tun+ -j ACCEPT

# 例として、VPN クライアントから 192.168.200.0/24 へのアクセスを許可します。
# ※192.168.200.0/24 側のファイアウォール等で 10.8.0.0/24 からのアクセスを許可する
# 必要があります。
iptables -I FORWARD -i tun+ -d 192.168.200.0/24 -j ACCEPT

# LAN 内の特定 IP アドレス (192.168.200.5) へのアクセスを許可する場合は、以下の
# ような設定になります。
# ※192.168.200.5 側のファイアウォール等で 10.8.0.0/24 からのアクセスを許可する必
# 要があります。
#ただし本資料では特定 IP アドレスの設定はしない為、コメントアウトしています。
#iptables -I FORWARD -i tun+ -d 192.168.200.5 -j ACCEPT
```

- ・ ファイアウォール自動設定スクリプトに実行権限付与

```
# chmod +x /etc/openvpn/openvpn-startup
```

6.2.2.3. openvpn-shutdown の設定

- ・ ファイアウォール自動設定解除スクリプト作成

OpenVPN 停止時に実行するファイアウォール自動設定解除スクリプトを作成します。

```
# vi /etc/openvpn/openvpn-shutdown
```

以下は、VPN インタフェース(tun+)用 iptables の受信、転送、送信ルールを削除するスクリプトとなっています。

```
#!/bin/bash

# iptables ルール削除関数
delete() {
    rule_number=`iptables -L $target --line-numbers -n -v|grep tun.|awk '{print $1}'|sort -r`
    for num in $rule_number
    do
        iptables -D $target $num
    done
}

# 受信ルール削除
target='INPUT'
delete

# 転送ルール削除
target='FORWARD'
delete

# 送信ルール削除
target='OUTPUT'
delete
```

- ・ ファイアウォール自動設定解除スクリプトに実行権限付与

```
# chmod +x /etc/openvpn/openvpn-shutdown
```

6.2.2.4. ログローテーションの設定

- ・ OpenVPN ログローテーション設定ファイル作成

```
# vi /etc/logrotate.d/openvpn
```

```
/var/log/openvpn.log {
    missingok
    notifempty
    sharedscripts
    postrotate
    /etc/rc.d/init.d/openvpn restart 2>&1 > /dev/null || true
    endscrip
}
```

6.2.2.5. 起動スクリプトの設定

- ・ パケット転送を有効化に設定

```
# vi /etc/rc.d/init.d/openvpn
```

```
#echo 1 > /proc/sys/net/ipv4/ip_forward
↓ コメントを解除して、パケット転送を有効にします。
echo 1 > /proc/sys/net/ipv4/ip_forward
```

6.2.1. 起動と停止（サーバ）

6.2.1.1. ポートの設定

VPN サーバのファイアウォールなどの設定で、UDP 1194 番ポートを開放してください。

6.2.1.2. 自動起動設定

```
# chkconfig openvpn on
```

※以下で自動設定内容の確認をします。（ランレベル 2～5 で起動）

```
# chkconfig --list openvpn
```

```
openvpn          0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

6.2.1.3. 起動

```
# /etc/rc.d/init.d/openvpn start
```

6.2.1.4. 停止

```
# /etc/rc.d/init.d/openvpn stop
```

6.2.1.5. 再起動

```
# /etc/rc.d/init.d/openvpn restart
```

6.2.2. インストール（クライアント）

6.2.2.1. クライアントソフトのダウンロード

以下のサイトより Windows 日本語版をダウンロードしてください。

→<http://www.openvpn.jp/guijp.html>

※最新版は、本家のサイトである以下よりダウンロードしてください。

→<http://www.openvpn.net/index.php/open-source/downloads.html>

6.2.2.2. クライアントソフトのインストール

以下のサイトを参考にインストールを行ってください。

※Windows 日本語版の説明となっています。

→<http://www.openvpn.jp/clientinstall.html>

6.2.3. OpenVPN の設定（クライアント）

OpenVPN の設定ファイルは、サンプルをコピーして作成します。

クライアントの設定ファイル格納フォルダ(C:\Program Files\OpenVPN\config)にコピーしてください。

※クライアント設定ファイルのサンプル

→C:\Program Files\OpenVPN\sample-config\client.ovpn

6.2.3.1. client.ovpn の設定

以下は、VPN サーバが「openvpn.secioss.co.jp」の場合の設定例です。

```
# VPN サーバ名を変更します。
remote openvpn.secioss.co.jp 1194

#コメントアウトして証明書・秘密鍵を使用しません。
;cert client.crt
;key client.key

#"Man-in-the-Middle"攻撃の対策として、コメントを解除します。
ns-cert-type server

#コメントを解除して、TLS 認証を有効にします。
tls-auth ta.key 1

#最終行に追加して、ログイン画面をユーザ/パスワード形式にします。
auth-user-pass
```

6.2.3.2. 証明書の配置


VPN サーバに設定している CA 証明書と (/etc/openvpn/ca.crt)、TLS 認証鍵 (/etc/openvpn/ta.key) をクライアントの設定ファイル格納フォルダ (C:\Program Files\OpenVPN\config) に配置します。

6.2.4. 動作確認 (クライアント)

6.2.4.1. OpenVPN GUI で接続


- ・ スタートメニューよりクライアントソフト起動

[スタート]-[すべてのプログラム]-[OpenVPN]-[OpenVPN GUI] をクリックします。

インジケータ内に赤いアイコン () が表示されます。

- ・ 画面の起動

インジケータ内のアイコン () をダブルクリックします。

ログイン画面が表示されます。この時、接続中となりアイコンが黄色になります。 ()




- ・ ログイン認証

ユーザ名とパスワードを入力して、OK ボタンをクリックします。

ユーザ名 : SeciossOTP に設定したユーザ ID を設定してください。

パスワード : 携帯 (ソフトウェアトークン) で確認したパスワードを設定してください。

認証が成功すると、接続済みとなりアイコンが緑になります。 ()

6.3. RADIUS

参考として本章では、FreeRADIUS2 のインストールと設定について説明します。

6.3.1. インストール

以下の rpm パッケージをインストールして下さい。

- freeradius2
- freeradius2-perl
- perl-libwww-perl
- perl-XML-Simple
- perl-Config-General

```
# yum install <パッケージ名>
```

6.3.2. FreeRADIUS の設定

設定ファイルは、yum でインストールすると「/etc/raddb」配下にあります。

6.3.2.1. radiusd.conf の設定

設定を行わなくても動作しますが、ここではアクセス要求をログに出力する設定を行います。

```
# vi /etc/raddb/radiusd.conf
```

```
log {  
    :  
    auth = yes  
    :  
}
```

6.3.2.2. client.conf の設定

RADIUS サーバと通信するクライアントを登録します。

クライアントの IP アドレスが 192.168.1.2 の場合は、以下のように記述します。

また、” secret = test123” はクライアント側に設定する RADIUS サーバと共有するパスワードです。

```
# vi /etc/raddb/client.conf
```

```
client 192.168.1.2 {  
    secret          = testing123  
    shortname       = test-pc  
}
```

6.3.2.3. users の設定

SeciossOTP で認証するので、デフォルト認証タイプとして Perl を設定します。

```
# vi /etc/raddb/users
```

```
DEFAULT Auth-Type := Perl
Fall-Through = 1
```

6.3.2.4. **sites-enabled** 配下、**default** の設定

認証タイプとして Perl を追加します。

また、EAP の認証は使用しないので、全てコメントアウトします。

```
# vi /etc/raddb/sites-enabled/default
```

```
authorize {
    :
#   eap {
#       ok = return
#   }
    :
    perl
    :
}

authenticate {
    Auth-Type Perl {
        perl
    }
    :
#   eap
    :
}

accounting {
    :
    perl
    :
}

post-proxy {
    :
#   eap
    :
}
```

※sites-enabled/ inner-tunnel ファイルは使用しない為、削除してください。
削除しない場合は、default ファイルと同様に perl と eap の設定が必要です。

6.3.2.5. modules 配下、perl の設定

SeciossOTP 認証を行う為の Perl スクリプトを設定します。

```
# vi /etc/raddb/modules/perl
```

```
perl {  
    :  
#    module = ${confdir}/example.pl  
    module = /opt/secioss/lib/secioss-otp.pl  
    :  
}
```

6.3.2.6. SeciossOTP 認証スクリプトの設定ファイル作成

「/var/www/conf」配下に otp.conf ファイルを作成します。

以下が設定ファイルの内容です。

- url : SeciossOTP サーバの認証 URL を記述
- id_def : ユーザ ID 項目名
- pwd_def : パスワード項目名

SeciossOTP サーバの IP アドレスが 192.168.1.10 の場合は、以下のように記述します。

※作成時は、IP アドレス部分のみ環境に合わせて変更してください。

```
# vi /var/www/conf/otp.conf
```

```
url=https://192.168.1.10/pub/otp.php  
id_def=userid  
pwd_def=password
```

6.3.3. 起動と停止

6.3.3.1. ポートの設定

RADIUS サーバのファイアウォールなどの設定で、UDP 1812 番・1813 番ポートを開放してください。

6.3.3.2. 自動起動設定

```
# chkconfig radiusd on
```

※以下で自動設定内容の確認をします。(ランレベル 2~5 で起動)

```
# chkconfig --list radiusd
```

```
radiusd          0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

6.3.3.3. 起動

```
# /etc/rc.d/init.d/radiusd start
```

6.3.3.4. 停止

```
# /etc/rc.d/init.d/radiusd stop
```

6.3.3.5. 再起動

```
# /etc/rc.d/init.d/radiusd restart
```

6.3.4. 動作確認

以下は、WindowsPC より NTRadPing ソフトを使用して、RADIUS の動作確認を行う方法を説明しています。

6.3.4.1. 動作確認事前設定

client.conf に動作確認に使用する WindowsPC の IP アドレスを設定してください。

また、WindowsPC のファイアウォールなどの設定で、UDP 1812 番ポートを開放してください。

6.3.4.2. NTRadPing ソフトのダウンロード

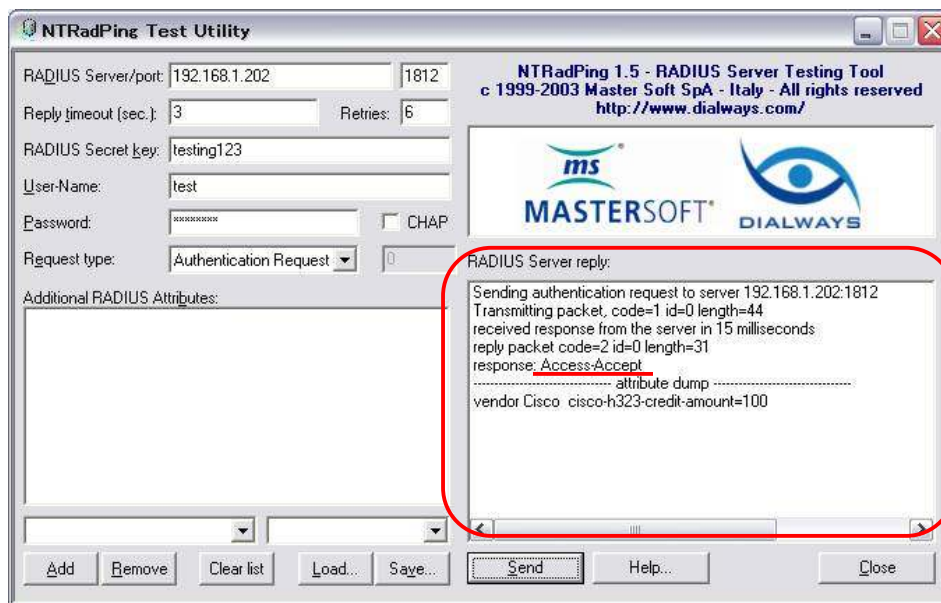
以下のサイトよりダウンロードしてください。

→ <http://www.mastersoft-group.com/download/>

ダウンロードした ZIP ファイルを展開して、NTRadPing.exe を実行します。

以下の項目を設定して、Send ボタンをクリックします。

- ① RADIUS Server/port : RADIUS サーバの IP アドレスを設定してください。
- ② RADIUS Secret key : client.conf に設定した secret の値を設定してください。
- ③ User-Name : SeciossOTP に設定したユーザ ID を設定してください。
- ④ Password : 携帯 (ソフトウェアトークン) で確認したパスワードを設定してください。



図のように RADIUS Server reply に結果が表示されます。

「Access-Accept」の記述があれば OK です。

間違ったパスワードを入力すると「Access-Reject」となります。

7. ログ

7.1. 認証サーバ

認証サーバに関するログは以下のファイルに出力されます。

- ・ 認証サーバ、シークレットの設定： /var/log/auth.log

7.2. SSL-VPN サーバ (OpenVPN)

OpenVPN に関するログは以下のファイルに出力されます。

- ・ 動作ログ： /var/log/openvpn.log

7.3. RADIUS サーバ (FreeRADIUS2)

FreeRADIUS2 に関するログは以下のファイルに出力されます。

- ・ アクセス要求のログ： /var/log/radius/radius.log
- ・ アカウントログ： /var/log/radius/radacct 配下