

インストール・運用管理ガイド

PassLogic 認証サーバソフトウェア

ver.3.6

本書について

本書は、PassLogic 認証サーバソフトウェアインストール・運用管理ガイドです。

表示画面

表示画面などは、操作の一例として掲載しているため、実際に表示される画面とは異なる場合もあります。

商標および免責事項

- ・ PassLogic およびパスロジは、パスロジ株式会社の登録商標です。
- ・ その他、本書に記載されている会社名、製品名は、それぞれ各社の商標または登録商標です。
- ・ 本製品は医療機器、原子力施設、航空関連機器、軍備機器、輸送設備やその他人命に直接関わる施設や設備など、高い安全性が要求される用途での使用は意図されていません。該当する施設や設備には使用しないでください。

版權/注意

- ・ 本書の内容の一部または全部を無断で複写転載することを禁じます。
- ・ 本書に掲載の内容及び製品の仕様などは、予告なく変更されることがあります。

本書の内容は万全を期して作成しておりますが、万一ご不明な点や誤り、記載漏れ、乱丁、落丁などお気づきの点がございましたら、弊社までご連絡ください。

特許/ Patent

本製品は米国及び日本にて下記の特許を取得しています。

- ・ U.S. Pat.6,141,751
- ・ U.S. Pat.8,140,854
- ・ JAPAN Pat.3,809,441
- ・ JAPAN Pat.4,275,080
- ・ JAPAN Pat.4,455,666

免責事項

- ・ 2012 年 11 月 6 日現在の情報です。

目次

1. インストールガイド	- 8 -
1.1. 動作環境	- 8 -
1.2. httpd.conf, php.ini 推奨設定値	- 8 -
1.3. 対応ブラウザ	- 9 -
1.4. 使用通信ポート	- 9 -
1.5. 必要な rpm パッケージをインストールする	- 11 -
1.6. PassLogic をインストールする	- 12 -
1.6.1. インストール時の設定	- 12 -
1.6.2. タイムゾーンの設定	- 13 -
1.7. 管理画面にアクセスする	- 13 -
1.8. ライセンスを登録する	- 15 -
1.9. アップデート	- 15 -
1.9.1. 問題が発生した際のリカバリの方法	- 15 -
1.9.2. バージョン 2.x.x からのアップデート	- 16 -
1.9.3. バージョン 3.1.0 からのアップデート	- 16 -
1.9.4. バージョン 3.2.0 以前からのアップデート	- 16 -
1.9.5. バージョン 3.4.2 以前から 3.4.5 へのアップデート	- 16 -
1.9.6. バージョン 3.4.5 以前からのアップデート	- 17 -
1.9.7. バージョン 3.5.1 以前からのアップデート	- 17 -
1.10. アンインストール	- 17 -
2. システム管理者ガイド	- 18 -
2.1. ユーザーインターフェイスの言語について	- 18 -
2.2. 管理者アカウントを作成する	- 18 -
2.3. セキュリティポリシー設定	- 19 -
2.4. メール設定	- 21 -
2.5. ユーザ通知設定	- 22 -
2.6. ログ・その他設定	- 22 -
2.7. リモートアクセス管理	- 23 -
2.7.1. ポリシー設定	- 24 -
2.7.2. アプリケーション設定（PC / 携帯）	- 25 -
2.7.3. URL マッピング	- 25 -
2.7.4. 各アプリケーションの設定例	- 26 -
2.7.5. ユーザインターフェイス	- 27 -
2.7.6. http ヘッダ連携	- 27 -

2.8.	WebSSO 機能.....	- 27 -
2.8.1.	設定方法.....	- 28 -
2.8.2.	認証方式.....	- 30 -
2.8.3.	各アプリケーションの設定例.....	- 33 -
2.9.	SAML 連携	- 35 -
2.9.1.	SAMLSP 登録	- 35 -
2.9.2.	SAML 証明書	- 35 -
2.10.	RADIUS 連携.....	- 36 -
2.10.1.	RADIUS 連携の概要	- 36 -
2.10.2.	RADIUS 連携 (SSL-VPN、VPN)と PassLogic を連携させる際の設定フロー - 37 -	- 37 -
2.10.3.	RADIUS 設定	- 38 -
2.10.4.	Web トークン	- 38 -
2.10.5.	ユーザインターフェイス	- 39 -
2.10.6.	RADIUS 認証動作	- 41 -
2.11.	ID 同期	- 42 -
2.11.1.	OpenLDAP	- 43 -
2.11.2.	ActiveDirectory.....	- 44 -
2.12.	CSV ファイルによるデータ同期	- 44 -
2.13.	バックアップの方法.....	- 46 -
2.14.	管理者(admin)パスワードのリセット方法.....	- 46 -
2.15.	監視対象プロセス.....	- 47 -
2.16.	PassLogic 認証サーバをイントラネットに配置する	- 48 -
2.16.1.	リモートアクセス(リバースプロキシ)の場合.....	- 48 -
2.16.2.	RADIUS 連携の場合	- 50 -
2.17.	グラフィックデザインのカスタマイズ.....	- 51 -
2.17.1.	ユーザインターフェイス一覧.....	- 51 -
2.17.2.	リモートアクセスログイン画面のカスタマイズ.....	- 51 -
2.17.3.	リモートアクセスログイン画面(iPhone)のカスタマイズ.....	- 52 -
2.17.4.	リモートアクセスログイン画面(携帯)のカスタマイズ	- 52 -
2.17.5.	各ログイン画面で利用できる変数.....	- 52 -
2.18.	参考資料	- 53 -
2.18.1.	PassLogic 管理ツールの設定項目	- 53 -
2.18.2.	リモートアクセス管理で Microsoft IIS にアクセスする場合.....	- 53 -
2.18.3.	WebSSO で Outlook Web Access にログインする場合	- 53 -
2.18.4.	RADIUS 連携のユーザインターフェイスで target の値を URL に含める方	

法	- 54 -
2.18.5. SSL 証明書のインストールについて	- 55 -
2.18.6. ウィルス対策ソフトを利用する場合	- 55 -
3. ユーザー管理者ガイド	- 56 -
3.1. 管理ツールにアクセスする	- 56 -
3.1.1. 管理ツールログイン用のユーザ ID を入力する	- 56 -
3.1.2. 管理ツールログイン用のパスワードを入力する	- 57 -
3.2. PassLogic の状態を確認する	- 58 -
3.2.1. PassLogic のバージョンを確認する	- 59 -
3.2.2. 登録されているライセンス情報を確認する	- 59 -
3.2.3. PassLogic サーバのステータスを確認する	- 59 -
3.3. ユーザの新規作成	- 60 -
3.3.1. デバイス追加	- 61 -
3.4. 全ユーザを一覧で見る	- 62 -
3.5. ロック中のユーザを一覧で見る	- 62 -
3.6. ユーザを検索する	- 62 -
3.7. ユーザー一括登録	- 62 -
3.7.1. CSV ファイルダウンロード	- 64 -
3.8. バックアップ/リストア	- 64 -
3.8.1. バックアップ	- 64 -
3.8.2. リストア	- 64 -
3.9. 管理者パスワードの変更	- 65 -
3.10. ユーザサポートについて	- 65 -
3.10.1. ロックの解除方法（ユーザアカウントがロックされた場合のサポート） ...	- 65 -
3.10.2. パスワード再発行の方法（ユーザがパスワードを忘れた場合のサポート）	- 65 -
3.10.3. PassLogic からの通知メールが届かない場合のサポート	- 66 -
3.11. ログ・リファレンス	- 67 -
3.11.1. ログフォーマット	- 67 -
3.11.2. ログ：ステータスリファレンス	- 67 -
3.11.3. ログのサイズ	- 73 -

PassLogic 認証方式とは？

PassLogic 認証方式では、ログインごとに乱数表を取得し、利用者本人だけが知る“位置”と“順番”からワイントタイムパスワードを生成します。

① 事前に数字を抽出する「位置」と「順番」を登録し覚える。

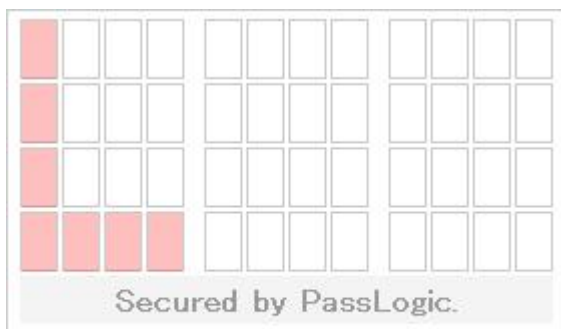


② ログイン時はその位置と順番から数字を抽出しパスワードとして使用。



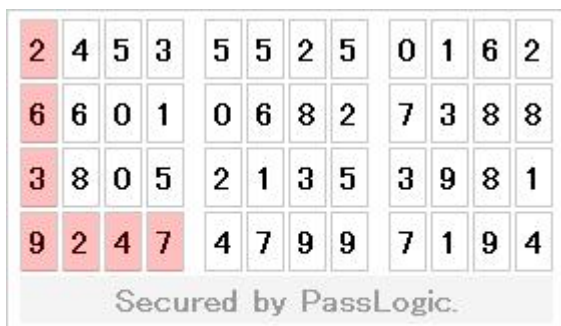
Password

また、パスワード位置情報はユーザ自身で変更することができます。例えば下図の「L字」のパターン+PIN（固定パスワード）に変更する場合について説明します。



STEP1.

「L字」+PIN（今回はabcd）を入力します。



※ 実際にはパスワードは表示されません。（例：*****）

STEP2.

STEP1 と同様に「L 字」+PIN を入力します。

8	4	3	7	0	6	1	5	4	4	1	0
2	0	7	1	9	1	9	4	9	8	3	1
8	4	5	3	6	2	6	7	5	5	3	2
7	2	7	9	6	3	8	5	6	0	0	2

Secured by PassLogic.

STEP3.

STEP1-2 と同様に「L 字」+PIN を入力します。計 3 回の入力でパスワード位置情報の変更が完了します。

3	8	9	6	6	8	7	2	8	2	5	1
0	4	6	7	5	2	6	9	0	7	7	1
9	5	3	4	8	5	4	7	8	3	0	3
5	5	1	1	6	6	1	8	4	0	6	5

Secured by PassLogic.

1. インストールガイド

1.1. 動作環境

PassLogic 認証サーバの動作環境は以下の通りです。

	Red Hat Enterprise Linux 5 / CentOS 5 i386 および x86_64	Red Hat Enterprise Linux 6.1 以降 / CentOS 6.1 以降 i386 および x86_64
httpd	Apache HTTP Server version: 2.2.3 release: 6.el5 以降	Apache HTTP Server version: 2.2.15 release: 15.el6 以降
php	version: 5.1.6 release: 5.el5 以降	version: 5.3.3 release: 3.el6 以降

1. 各モジュールは、OS ベンダ提供パッケージのみのサポートとなります。独自コンパイルしたものはサポート対象外ですので、別途お問い合わせください。
2. NSA Security-Enhanced Linux(SELinux)を有効にした動作はサポートしていませんので OS インストール時または設定にて「無効」に設定してください。
3. /var 以下の容量が不足しないようにしてください。容量が不足した場合、管理ツールにログインできなくなります。

1.2. httpd.conf, php.ini 推奨設定値

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
ServerSignature	Off
TraceEnable	Off

/etc/php.ini

expose_php	Off
display_errors	Off
session.entropy_length	32
session.entropy_file	/dev/urandom
session.hash_function	1
session.gc_maxlifetime	1440
session.cookie_httponly	On

1.3. 対応ブラウザ

	ブラウザ	文字コード
管理ツール	Internet Explorer6, 7, 8, 9	UTF-8
	Firefox3	UTF-8
ユーザインターフェイス	Internet Explorer6, 7, 8, 9	UTF-8
	Firefox3	UTF-8
	iPhone safari	UTF-8
	docomo i-mode ブラウザ(FOMA) au EZweb Softbank ※個体識別番号制限機能は、個体識別番号が送出できる 端末に限ります。	Shift-JIS

1.4. 使用通信ポート

※iptables 等ファイアウォールを動作させている場合には、必要に応じて PassLogic 認証サーバソフトウェアが利用する以下のポートにアクセスできるように設定してください。

ゲートウェイサーバと認証サーバを同一筐体で動作させる場合の使用ポート

ポート番号	プロトコル	送信元	送信先	内容
80/tcp	http	クライアント	⇒ PassLogic サーバ	ユーザインターフェイス
443/tcp	https	クライアント	⇒ PassLogic サーバ	ユーザインターフェイス
80/tcp	http	PassLogic サーバ	⇒ Web アプリケーションサーバ	リバースプロキシ
443/tcp	https	PassLogic サーバ	⇒ Web アプリケーションサーバ	リバースプロキシ
12079/tcp	http	PassLogic サーバ	⇒ PassLogic サーバ	認証 API との通信
12080/tcp	https	クライアント (管理端末)	⇒ PassLogic サーバ	管理ツールアクセス

ゲートウェイサーバと認証サーバを異なる筐体で動作させる場合の使用ポート

ポート番号	プロトコル	送信元	送信先	内容
80/tcp	http	クライアント	⇒ ゲートウェイサーバ	ユーザインターフェイス

443/tcp	https	クライアント ⇒ ゲートウェイサーバ	ユーザインターフェイス
80/tcp	http	ゲートウェイサーバ ⇒ Webアプリケーションサーバ	リバースプロキシ
443/tcp	https	ゲートウェイサーバ ⇒ Webアプリケーションサーバ	リバースプロキシ
12079/tcp	http	ゲートウェイサーバ ⇒ 認証サーバ	認証 API との通信
12080/tcp	https	クライアント (管理端末) ⇒ ゲートウェイサーバ 認証サーバ	管理ツールアクセス

その他 PassLogic が使用するポート一覧

ポート番号	送信元	送信先	内容
25/tcp	PassLogic サーバ ⇒	SMTP サーバ	メール送信 (変更可)
465/tcp	PassLogic サーバ ⇒	SMTP サーバ	メール送信 (変更可) TLS/SSL
123/udp	PassLogic サーバ ⇒	NTP サーバ	時刻同期
514/udp	PassLogic サーバ ⇒	syslog サーバ	ログ転送
389/tcp	PassLogic サーバ ⇒	LDAP サーバ	LDAP 連携 (変更可)
1812/udp	RADIUS クライアント ⇒	RADIUS サーバ	RADIUS 認証
1813/udp	RADIUS クライアント ⇒	RADIUS アカウンティングサーバ	RADIUS アカウンティング

その他ポート一覧

ポート番号	送信元	送信先	内容
21/tcp	PassLogic サーバ ⇒	yum サーバ	rpm インストール
80/tcp	PassLogic サーバ ⇒	yum サーバ	rpm インストール
22/tcp	クライアント (管理端末) ⇒	PassLogic サーバ	OS コンソールアクセス
53/udp	PassLogic サーバ ⇒	DNS サーバ	名前解決

1.5. 必要な rpm パッケージをインストールする

PassLogic 認証サーバソフトウェアを動作させるのに必要な rpm パッケージソフトをインストールします。

PassLogic サーバソフトウェアを動作させるのには以下のパッケージソフトが必要です。

- curl
- httpd
- libtool-ltdl
- mod_ssl
- net-snmp-utils
- ntp
- perl-DBI (RHEL5 のみ)
- libxslt
- xmlsec1 (RHEL5 のみ)
- xmlsec1-openssl (RHEL5 のみ)
- php
- php-ldap
- php-mbstring
- php-process (RHEL6 のみ)
- postgresql-libs (RHEL6 のみ)
- zip
- unzip
- tmpwatch

必要なパッケージソフトをインストールします。

```
(root 権限で実行)
# yum -y install curl
# yum -y install httpd
# yum -y install libtool-ltdl
# yum -y install mod_ssl
# yum -y install net-snmp-utils
# yum -y install ntp
# yum -y install perl-DBI (RHEL5 のみ)
# yum -y install libxslt
# yum -y install xmlsec1 (RHEL5 のみ)
# yum -y install xmlsec1-openssl (RHEL5 のみ)
# yum -y install php
```

```
# yum -y install php-ldap
# yum -y install php-mbstring
# yum -y install php-process (RHEL6 のみ)
# yum -y install postgresql-libs (RHEL6 のみ)
# yum -y install zip
# yum -y install unzip
# yum -y install tmpwatch
```

*RHEL6 に、**php-mbstring**, **php-process** パッケージを、**yum** を使ってインストールする場合は、**RedHat Network** の **SoftwareChannels** で **Optional** を有効にする必要があります。

1.6. PassLogic をインストールする

PassLogic 認証サーバソフトウェアをインストールします。

```
(root 権限で実行)
# cp /cdrom/PassLogic-x.x.x.tar.gz /usr/local/src/
# cd /usr/local/src/
# tar zxvf PassLogic-x.x.x.tar.gz
# cd passlogic-x.x.x/
# ./install.sh install
```

PassLogic 認証サーバソフトウェアが自動的にインストールされます。

*PassLogic 認証サーバソフトウェアがすでにインストールされている場合(/opt/passlogic というディレクトリが存在する場合)以下のメッセージが表示されます。

```
PassLogic Authentication Server Software はすでにインストールされています。update
をお試してください。 - PassLogic Authentication Server Software has already installed.
plaese try update
```

1.6.1. インストール時の設定

インストール時に、以下の設定が自動で追加されます。

/etc/yum.conf

```
exclude=freeradius
```

※FreeRADIUS を UPDATE すると RADIUS 連携機能が利用できなくなります。yum コマンドの update 対象外に指定してください。

/etc/sudoers

```
apache ALL=NOPASSWD: /bin/sed
apache ALL=NOPASSWD: /sbin/service httpd status
apache ALL=NOPASSWD: /sbin/service sendmail status (RHEL5 のみ)
apache ALL=NOPASSWD: /sbin/service postfix status (RHEL6 のみ)
apache ALL=NOPASSWD: /sbin/service radiusd status
apache ALL=NOPASSWD: /sbin/service ntpd status
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/httpd_restart.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/radiusd_restart.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/restore.sh
```

※管理ツールから、設定変更を有効にするため上記の設定が追加されます。

PassLogic 認証サーバソフトウェアは、サービスの状態を確認するために以下のコマンドを利用しています。

```
/usr/bin/sudo /sbin/service httpd status
/usr/bin/sudo /sbin/service sendmail | postfix status
/usr/bin/sudo /sbin/service radiusd status
/usr/bin/sudo /sbin/service ntpd status
```

上記のコマンドが実行できるように OS のセットアップを行ってください。

1.6.2. タイムゾーンの設定

海外でご利用の場合には適切なタイムゾーンを設定してください。

・ /etc/php.ini

```
date.timezone = "Asia/Tokyo"
```

1.7. 管理画面にアクセスする

PassLogic 認証サーバソフトウェア管理ツールにウェブブラウザでアクセスします。

```
https://[ホスト名]:12080/passlogic-admin/
```

管理者のユーザ名は「**admin**」です。

※iptables 等のファイアウォールを起動している場合は、12080 番ポートでアクセスできるよう設定を行ってください。

初回アクセス時に管理者のパスワード(パスワード位置情報)を設定します。設定手順は「管理者パスワードの変更」の項をご確認ください。

管理者ユーザのログイン・パスワード(パスワード位置情報)を設定します。

手順

- STEP.1 新しいパスワード(パスワード位置情報の数字)を入力してください。
- STEP.2 位置特定の為、再度同じ位置の数字を入力してください。
- STEP.3 確認の為、再度同じ位置の数字を入力してください。
- STEP.4 完了

3	8	7	9	0	6	9	6	9	2	9	5
0	6	7	9	4	6	3	7	1	6	7	7
2	4	7	5	1	8	3	4	1	4	8	2
1	4	2	9	0	0	6	7	1	2	3	8

Secured by PassLogic.

1	2	3	4	5	
6	7	8	9	0	<<
次へ					

(C) Passlogy Co.,Ltd. 2000-2011

1.8. ライセンスを登録する

ライセンスファイル「license.asc」を登録します。左メニューライセンス管理をクリックしてください。ライセンスファイルを登録し、ライセンス情報が正常に反映されたことを確認してください。

※インストール直後はユーザ数上限 1 で動作しています。

1.9. アップデート

PassLogic 認証サーバソフトウェアをアップデートします。

※アップデートの実行時は、事前に管理ツールよりバックアップを行ってください。

(root 権限で実行)

```
# cp PassLogic-x.x.x.tar.gz /usr/local/src/
```

```
# tar zxvf PassLogic-x.x.x.tar.gz
```

```
# cd passlogic-x.x.x/
```

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

PassLogic Authentication Server Software をアップデートします。よろしいですか？-
start update PassLogic Authentication Server Software [yes or no]

(yes を入力してください)

PassLogic 認証サーバソフトウェアが自動的にアップデートされ radiusd, httpd が再起動されます。

【注意】

- /opt/mod_auth_passlogic/tmpl/
- /opt/mod_auth_passlogic/mtmpl/
- /opt/mod_auth_passlogic/itmpl/

のテンプレートを編集している場合には、上書きされますので別途バックアップをお願いいたします。

1.9.1. 問題が発生した際のリカバリの方法

(root 権限で実行)

(アップデート後の PassLogic をアンインストール)

```
# cd passlogic-3.x.x/ (3.x.x はアップデート後のバージョン)
```

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

(アップデートする前の PassLogic を再インストール)

```
# cd ../passlogic-3.y.y/ (3.y.y はアップデート前のバージョン)
```

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

(管理ツールにアクセスし、バックアップファイルをリストアしてください)

1.9.2. バージョン 2.x.x からのアップデート

現行バージョンの PassLogic とバージョン 2 系の PassLogic では、設定ファイルに互換性がないのでご注意ください。アップデート後、以下のように設定ファイルを上書きして下さい。

```
# cd /usr/local/src/passlogic-3.x.x/core/conf/files/  
# cp Passlogic_Config.pm /opt/passlogic/passlogicdata/pat/conf/Passlogic_Config.pm  
cp: overwrite '/opt/passlogic/passlogicdata/pat/conf/Passlogic_Config.pm'? yes  
# /etc/init.d/httpd restart
```

※以前の設定(RADIUS を使用している場合は、RADIUS の設定情報も含む)情報は引き継がれませんのでご注意ください。

1.9.3. バージョン 3.1.0 からのアップデート

バージョン 3.1.0 からのアップデートは、設定ファイルの互換性に問題があり認証ができなくなります。バージョン 3.1.0 からアップデートされる場合はお手数ですが、弊社サポートまでお問い合わせください。3.1.1 からのアップデートについてはこの問題は発生しません。

1.9.4. バージョン 3.2.0 以前からのアップデート

バージョン 3.2.0 以前のバージョンからのアップデートに関しては、リモートアクセス管理の HTML テンプレート (ユーザ側) に互換性がないのでご注意ください。アップデート後、以下のようにテンプレートファイルを上書きして下さい。

```
# cd /cdrom(PassLogic インストールメディアをマウントして下さい)  
# cd templates  
# cp -R * /opt/mod_auth_passlogic/
```

※3.2.0 以前からのアップデートは、アップデート後設定を有効にするために、PassLogic 設定を行って下さい。

1.9.5. バージョン 3.4.2 以前から 3.4.5 へのアップデート

バージョン 3.4.2 以前のバージョンからアップデートした際には、リモートアクセス管理の言語設定が英語になりますので、リモートアクセス管理・ポリシー設定より任意の言語に設定をお願いいたします。

1.9.6. バージョン 3.4.5 以前からのアップデート

以下のテンプレートの仕様が変更になっていますので、テンプレートをカスタマイズして利用している場合は、適宜修正して下さい。

- /opt/mod_auth_passlogic/tmpl/
- /opt/mod_auth_passlogic/mtmpl/
- /opt/mod_auth_passlogic/itmpl/

1.9.7. バージョン 3.5.1 以前からのアップデート

以下のテンプレートの仕様が変更になっていますので、テンプレートをカスタマイズして利用している場合は、適宜修正して下さい。

- /opt/mod_auth_passlogic/tmpl/
- /opt/mod_auth_passlogic/mtmpl/
- /opt/mod_auth_passlogic/itmpl/

カスタマイズしていない場合は、PassLogic アップデート時に更新されます。

1.10. アンインストール

PassLogic 認証サーバソフトウェアをアンインストールします。

(root 権限で実行)

```
# cd passlogic/
# ./install.sh uninstall
```

PassLogic Authentication Server Software をアンインストールするとすべてのデータが削除されます。よろしいですか？ - if uninstalling PassLogic Authentication Server Software, all data is gone [yes or no]

(yes を入力してください。)

※rpm パッケージは別途アンインストールをお願いします。

2. システム管理者ガイド

2.1. ユーザーインターフェイスの言語について

ブラウザのロケール設定に ja（日本語）がある場合は日本語、ja が無い場合は、en（英語）をデフォルトで表示します。また、各ユーザーインターフェイスの言語切り替え機能で明示的に言語を切り替える（cookie で設定情報を保持）ことができます。

*携帯電話（docomo, au, softbank）の場合、日本語で表示されます。

2.2. 管理者アカウントを作成する

この項目では PassLogic 管理者アカウントの作成・一覧について説明します。

※ 管理者アカウント（admin 除く）も登録ユーザ数としてカウントされます。

※ 役割を operetor とした場合、ユーザ管理のみ設定変更可能となります。

（ユーザのロック／アンロック、パスワード再発行のみ）

【手順】

- (i) 管理ツール左側のメニューより「管理者一覧」の下にある「新規作成」をクリック
- (ii) 必要に応じて適宜変更し「次へ」をクリック
- (iii) 入力内容を確認し「設定」をクリック

ユーザ ID（必須項目）	英数字・記号（4-80 文字） ハイフン（-）アンダーバー（_）ピリオド（.）アットマーク（@） ユーザ登録通知メール <%UID%> 部分 healthcheck で始まるユーザ ID はシステム側で使用しているため指定できません。
メールアドレス	通知書をメールで送る場合は記入してください。
氏名	ユーザの氏名を入力します。 ユーザ通知メール<%UNAME%>部分
役割	admin 又は operetor のどちらかを選択します。
PIN	ワンタイムパスワードに付加する PIN（英数字※大文字小文字を区別する）の初期値を指定します。
初期パスワード位置情報（ワンタイムパスワード）	ユーザに通知するパスワード位置情報を設定します。以下通知例※ 10 桁以上はアルファベット[A-Z]で表現します。

	初期パスワード位置情報は 1234 5678 9ABC DE** ***** ***** ***** です。 空欄の場合はセキュリティポリシー設定の「初期パスワード位置情報」を通知します。 「パスワード位置情報をランダムに設定する」のチェックボックスを ON にすることでランダム生成したものを通知します。
初回にパスワード位置情報の変更が必要	初回（パスワード再発行後を含む）アクセス時に強制的にパスワード位置情報を変更させる場合は Yes に設定。パスワード変更しなくても良い場合は No に設定します。（初期値：Yes）
有効期限	アカウントの有効期限日を設定します。 設定した日までアカウントは有効です。 アカウントの有効期限が切れても管理ツール上にアカウントは残っていますので、アカウントを削除したい場合は明示的に消す必要があります。 アカウントの有効期限切れ後、管理ツールより有効期限日を延長設定することで設定情報などをそのまま継続して利用可能です。
有効/無効	アカウントの有効/無効を選択します。
備考	メモとして自由にお使いいただけます。

2.3. セキュリティポリシー設定

この項目では PassLogic 全体のセキュリティポリシー設定の方法を説明します。

【 手順 】

- (i) 管理ツール左側のメニューより「セキュリティポリシー設定」をクリック
- (ii) 必要に応じて適宜変更し「次へ」をクリック
- (iii) 入力内容を確認し「設定」をクリック

【 項目解説 】

ロック・アウトまでの連続失敗回数	ユーザがここで設定した回数だけ連続で認証に失敗すると、そのユーザはロックされます。0 にすることでロック・アウトしません。
------------------	---

ロック・アウト解除までの秒数	指定した秒数でロック・アウトが自動的に解除されます。[自動ロック解除しない]にチェックをすることで自動的に解除しません。
乱数表の有効時間	乱数表の有効時間を設定します。設定した時間を過ぎると、PassLogic 認証サーバ上の正解パスワードが削除されます。認証するためには新規に乱数表を取得する必要があります。
再設定時の制限	直近 n 回と同じパスワード位置情報の設定を禁止します。
初期パスワード位置情報	ユーザの初期パスワード位置情報を空欄で作成した場合は、ここで設定したものを初期パスワード位置情報とします。※10桁以上はアルファベット[A-Z]で表現します。 初期パスワード位置情報は 1234 5678 9ABC DE** ***** ***** ***** です。
パスワード位置情報の有効期限	パスワード位置情報を定期的に変更させたい場合に日数を設定します。無制限をチェックすると定期的な変更は必要ありません。
ワнтаイムパスワードの長さ	ワнтаイムパスワードの長さを指定します。 ※ワнтаイムパスワードと PIN を合わせたパスワード長が128文字以下になるように上限を設定してください。
ランダム発行時の桁数	初期パスワード位置情報をランダムで作成する場合の桁数を設定します。
PIN の長さ	PIN（固定パスワード）の長さを指定します。 ※ワнтаイムパスワードと PIN を合わせたパスワード長が128文字以下になるように上限を設定してください。 PIN の使用可能文字は、半角英数と記号.(コンマ)_(アンダーバー)@(アットマーク)-(ハイフン)です。
PIN に英字および数字を含めることを強制	本設定チェック時、ユーザは英字と数字を1つ以上含めた PIN を設定する必要があります。
設定禁止パスワード位置情報	ユーザに設定させたくない抜き出しパターンを設定します。 ※部分一致ではなく、完全一致となります。
パスワード位置情報の設定制約	ユーザがパスワード位置情報を変更する際に、4*4の3ブロックすべてからパスワード位置情報を選択する必要がある制限を有効にします。

ユーザによるパスワード位置情報変更	ユーザによるパスワード位置情報の変更を許可するか、しないかを設定します。 ※パスワード位置情報の変更を許可しない場合には、ユーザ登録時に、「初回抜き出し位置変更が必要」を必ず No にして下さい。
ダミー乱数表の表示	不正なユーザ情報で乱数表のリクエストがあった場合、エラーを表示するのかダミーの乱数表を表示するのか選択します。
1 つの正解で認証できる回数	1 つの正解で認証できる回数を指定します。通常は 1 にして下さい。他のシステムとの連携で、複数回正解の付け合わせが必要な際に変更します。
ユーザにアプリケーションパスワード・パラメータの変更を許可	ユーザが、自身でアプリケーションパスワード(WebSSO 時に利用するパスワード)およびパラメータ(WebSSO 時に利用するパラメータ)を変更できるようにします。 表示：表示の on/off を指定します。 表示名：ユーザに表示させたい値を入力します。
Cookie 制限利用時の Cookie の値	ワнтаイム：ログイン毎に変更（デフォルト） 固定：アクティベート時のまま固定
前回のログインを表示	前回のログイン、パスワード位置情報の有効期限、ユーザアカウントの有効期限をユーザに表示します。

※「ワнтаイムパスワードの長さ」「PIN の長さ」「設定禁止パスワード位置情報」「パスワード位置情報の設定制約」は、ユーザ自身がパスワードを変更する際の制約になります。管理ツールの操作でこの制約を受けることはありません。

2.4. メール設定

この項目では、PassLogic から送信するメールに関する設定を行います。通知するメールの内容を変更する場合は、ユーザ通知設定の項をご確認ください。メール設定を行う場合は、管理ツール左側のメニューより「メール設定」を選択します。

【項目解説】

SMTP サーバ	SMTP サーバの IP アドレスまたはホスト名
SMTP サーバのポート	25 番ポート以外のポートの場合
認証ユーザ ID(SMTP-AUTH)	SMTP-AUTH を利用する際のユーザ ID
認証パスワード(SMTP-AUTH)	SMTP-AUTH を利用する際のパスワード
TLS/SSL	TLS または SSL で接続する場合

2.5. ユーザ通知設定

この項目では、PassLogic が利用者に送信するメールのテンプレートについての解説を行います。メールサーバの設定に関しては、「メール設定」の項をご確認ください。ユーザ通知設定を行う場合は、管理ツール左側のメニューより「ユーザ通知設定」を選択します。

【項目解説】

《ユーザへの送信メール》

メールあるいは書面で通知する内容のフォーマットを編集します。本文の内容は以下の文字列を加えて頂くことで置換されます。

<%UID%>	PassLogic ユーザ ID
<%ACCNUM%>	PassLogic デバイス ID
<%UNAME%>	氏名
<%ENTRYKEY%>	アクティベーション用キー
<%PIN%>	ワンタイムパスワードの前に追加する PIN(固定パスワード)
<%PASSLOGICPATTERN%>	PassLogic のパスワード位置情報

※置換用のタグは Body（本文）でのみ置換されます。Subject（件名）などには使用できません。

[本文テンプレート]のリンクより、利用方法に応じたテンプレート・サンプルを作成いただけます。リモートアクセス管理で利用する場合、PC ブラウザと携帯電話ブラウザでは URL が異なります。適宜テンプレートを変更してご利用ください。

2.6. ログ・その他設定

この項目では、PassLogic の管理・利用ログに関する設定と、その他の PassLogic に関する設定を行います。

管理ツール左側のメニューより「ログ・その他設定」を選択します。

【項目解説】

ログを syslog に出力する	ログを syslog に出力するかどうかを選択します。
ログレベル	どの水準からログに書き出すのかを選択します。 ※ログレベルに関しては、本マニュアルの「ログ管理」の項を参照ください。
ログメール通知	From：送信元アドレスを入力します。 To：送信先アドレスを入力します。 ※複数の宛先に送信する場合は、メーリングリストなどを

	別途ご用意ください。 Subject : メールのタイトルを入力します。 ログレベル: ログレベルの詳細に関してはマニュアル 内ログ・リファレンスの項をご確認ください。
一覧の 1 ページ最大表示数	ユーザー一覧で表示する件数を入力します (初期値:100)

2.7. リモートアクセス管理

リモートアクセス機能でイントラネットに設置している Web アプリケーションにエクストラネットからアクセスすることが可能になります。

リモートアクセス機能を利用する際には、PassLogic 認証サーバにユーザ ID と同じ名前のデバイス ID を作成してください。

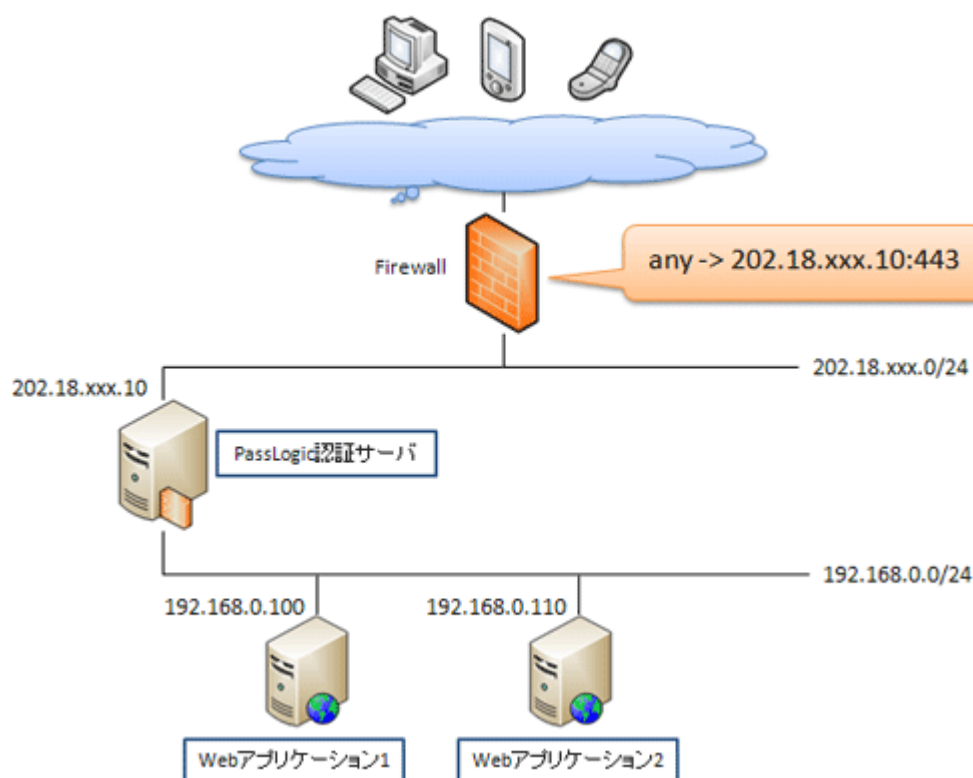
リバースプロキシ対象となる Web アプリケーションのコンテンツ (HTML ソース) は、相対パスで記述されている必要があります。絶対パスで記述されている場合には、Apache の機能を利用してコンテンツを書き換えるなどの対応が必要になります。

絶対パスの例

`<href="http://www.example.com/link/to/menu.html">リンク</a>`

相対パスの例

`<href= "link/to/menu.html">リンク</a>`



2.7.1. ポリシー設定

リモートアクセスのポリシー設定を行います。

PassLogicAPI の URL	PassLogicAPI の URL を設定します。 通常はデフォルトのままにしてください。 (デフォルト: http://127.0.0.1:12079/passlogic)	
セッションタイムアウト	セッションの有効期限を秒で設定します。0 を設定することでブラウザを閉じるまでセッションが有効になります。	
プロキシサーバ URL	プロキシサーバを経由して PassLogic にアクセスする場合に設定します。	
PC からのアクセス	PC 用ユーザインターフェイスへのアクセス制御（許可する/許可しない）を設定します。	
携帯からのアクセス	個体識別番号チェック	携帯からアクセスの際に個体識別番号をチェックする際には ON にしてください。
	クッキーに対応していない携帯端末も利用する	ON にすることで Cookie が利用できない端末からのアクセスの際に URL セッションに切り替わります。
iPhone からのアクセス	iPhone 用ユーザインターフェイスへのアクセス制御（許可する/許可しない）を設定します。	
Cookie の secure 属性	リモートアクセスにおいて使用するすべての Cookie に強制的に secure 属性が付きます。	
AuthPasslogicParam1-10	PC アプリケーション設定/携帯アプリケーション設定で登録した Web アプリケーションに対して、各ユーザの param1-10 に登録されている値を送出する際の名前を指定できます。 例：AuthPasslogicParam1 に「abcdef」を登録した場合、 abcdef: [ユーザの param1 の値] が、HTTP ヘッダの中に追加されます。 空白の場合は値を送出しません。 ※実装例は上記 http ヘッダ例をご覧ください。他の HTTP ヘッダと重複しないようにしてください。	

※携帯からのアクセスを個体識別付きで許可する場合は、デバイスタイプを「個体識別番号による制限」で作成してください。尚、個体識別番号による制限を行う場合、セキュリティ上、PC 用のユーザインターフェイスおよび iPhone 用のユーザインターフェイスから

のログインはできなくなります。

2.7.2. アプリケーション設定（PC / 携帯）

Web アプリケーション URL と仮想パスをマッピングして、PassLogic と Web アプリケーションとの連携設定を行います。

PC および iPhone で利用する Web アプリケーションは[PC アプリケーション設定]、携帯電話で利用する Web アプリケーションは[携帯アプリケーション設定]で設定します。なお、携帯電話で利用する場合は Web アプリケーションが携帯電話向けの表示に対応している必要があります。

No.	Web アプリケーションの表示 No.を入力してください。
アプリケーション名称	Web アプリケーションの表示名を入力してください。(例 グループウェア)
仮想パス	Web アプリケーションを公開する際に割り当てるパス名
ローカルアプリケーションの URL	イントラネットの URL を指定してください。
メニュー表示可能なグループ	メニュー表示可能なグループを指定します。空欄ですべてのユーザに表示します。複数指定する際にはカンマ(,)で区切ってください。グループの指定は、ユーザ登録のグループで行います。

予約済み仮想パス（下記の文字列はシステムで使われております。仮想パスとして使用することはできません）

/

/menu/

/tmenu/

/mmenu/

/imenu/

/uagent/

/passlogic/ui/

/passlogic-admin/

2.7.3. URL マッピング

Web アプリケーションの画像、JavaScript、CSS 等の URL をディレクトリにマッピングして参照できるようにします。

仮想パス	割り当てるパス名
ローカル URL	イントラネットの URL を入力してください。

予約済み仮想パス（下記の文字列はシステムで使われております。仮想パスとして使用す

ることはできません)

/

/menu/

/tmenu/

/mmenu/

/imenu/

/uagent/

/passlogic/ui/

/passlogic-admin/

URL マッピング設定は、httpd のエラーログを参照しながら作業をしてください。(Web アプリの全てのページでエラーが出力されなくなるまで設定を追加して下さい)

コマンド例

```
tail -f /var/log/httpd/access_log | grep 404
tail -f /var/log/httpd/ssl_access_log | grep 404
```

2.7.4. 各アプリケーションの設定例

以下設定例になります。個別の連携方法詳細については、別途弊社サポートまでお問い合わせください。

desknet's(デスクネッツ) ver7

PC アプリケーション設定

No.	1 (アプリケーションが複数ある場合の表示順)
アプリケーション名称	desknet's(デスクネッツ)
ローカルアプリケーションの URL	http://192.168.0.100/cgi-bin/dnet/dnet.cgi
仮想パス	/cgi-bin/dnet/

URL マッピング①

ローカル URL	http://192.168.0.100/neoimage/
仮想パス	/neoimage/

URL マッピング②

ローカル URL	http://192.168.0.100/neores/
仮想パス	/neores/

サイボウズ office8

PC アプリケーション設定

No.	2 (アプリケーションが複数ある場合の表示順)
アプリケーション名称	サイボウズ
ローカルアプリケーションの URL	http://192.168.0.110/cgi-bin/cbag/ag.cgi
仮想パス	/cgi-bin/cbag/

URL マッピング①

ローカル URL	http://192.168.0.110/cb80/
仮想パス	/cb80/

2.7.5. ユーザインターフェイス

リモートアクセス機能で利用するユーザインターフェイスは以下の通りです。

PC	標準	http(s)://<PassLogic のホスト名>/menu/
	タブ表示	http(s)://<PassLogic のホスト名>/tmenu/
スマートフォン		http(s)://<PassLogic のホスト名>/imenu/
携帯電話		http(s)://<PassLogic のホスト名>/mmenu/

2.7.6. http ヘッダ連携

PassLogic 認証サーバは、認証済のユーザ ID を http ヘッダに含めて、内側のアプリケーションに対して送信します。

http ヘッダ例(ユーザ ID: testuser の場合)

```
Accept: */*
Accept-Language: ja
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host: www.example.com
PL-Uid: testuser
Connection: Keep-Alive
```

認証済みのユーザ ID を Web アプリケーションで取得する実装例

```
<?php
$uid = $_SERVER['HTTP_PL_UID'];
?>
```

2.8. WebSSO 機能

WebSSO 機能を利用することで、Web アプリケーションに対して自動的にフォーム認証

を行うことが可能です。ユーザは PassLogic にログインするだけで、PassLogic 配下の Web アプリケーションのログインを意識することなく利用可能になります。また、複数の Web アプリケーションのユーザ ID、パスワードをユーザに配布せずに利用することが可能になり運用も効率化されます。

※WebSSO 機能の利用には WebSSO ライセンスを購入していただく必要があります。

ログイン画面が **Flash** で作成されている **Web アプリケーション**やログインがポップアップするもの、認証パスワードが **JavaScript** 等でハッシュして送信されるもの、認証用の **token** を発行するものは検証が必要です。別途お問い合わせください。

フォーム認証とは

フォーム認証とは、Web サーバおよび Web ブラウザ標準の認証機能である「基本(Basic)認証」とは異なり、ユーザが指定された必要な情報を送信して認証を行う方法です。例えば、ユーザ ID とパスワードの他に E メールアドレスとパスワードを入力して認証する方式があります。

データ送信方法	POST データ
	Query String (GET データ)
認証後のセッション管理方法	Cookie ヘッダによるブラウザへの通知
	URL へのセッション情報埋め込み
認証後の動作	リダイレクトなしのコンテンツ
	Location ヘッダによるリダイレクト(別 URL へ)
	Location ヘッダによるリダイレクト(同 URL へ)

※PassLogic の WebSSO(自動フォーム認証)が対応している方式

PassLogic の WebSSO 機能では、アプリケーションへの自動ログインに PassLogic のユーザ ID とアプリケーションパスワードを利用しますので、連携する Web アプリケーションにも PassLogic と同じユーザ ID のアカウントをあらかじめ作成しておく必要があります。

2.8.1. 設定方法

アプリケーション名称	リモートアクセス管理 >> アプリケーション設定で設定しているアプリケーションが選択できます。WebSSO に対応させたい Web アプリケーションを指定します。
ログイン ID の name 属性(*1)	アプリケーションのログインに使用されるログイン ID(ユーザ ID)の name 属性の名称を入力してください。(例: username)
パスワードの name 属性(*1)	アプリケーションのログインに使用されるパスワードの

	name 属性の名称を入力してください。(例: password)
Web アプリケーションとの通信方式	GET または POST を選択します。
認証方式	サーバ自動認証/クライアント自動認証(JavaScript)の 2 通り選択できます。
ログインページの URL	アプリケーションのログインページ URL を指定してください。
ログインページから取得する値の名前(*3)	ログインページから取得したいエンティティがある場合、エンティティの名前を入力します。 (例: SESSION_TOKEN)
認証の送信先 URL	リモートアクセス管理 >> アプリケーション設定で設定しているローカルアプリケーションの URL 以外にログイン用の URL がある場合には入力して下さい。(例: /app1/cgi-bin/login/auth)。特に指定しなければローカルアプリケーションの URL にログインを試みます。
その他の追加パラメータ	アプリケーションのログインの際にログイン ID、パスワード以外に必要なパラメータはこちらで設定してください。アプリケーションごとに異なります。
ユーザごとのパラメータ	グループ ID などユーザごとに POST したいパラメータの name 属性を指定します。ユーザ登録時の param1-10 が value 属性として対応します。

(*1)について

アプリケーションごとにログイン ID の name 属性、パスワードの name 属性は異なりますので、各アプリケーションのログインページの HTML ソースを確認してください。

Web アプリケーションのログイン画面の HTML を表示します。

```
<form method="post" name="LoginForm" action="login.cgi">  
ログイン名: <input type="text" name="user_id"><br />  
パスワード: <input type="password" name="password"><br />  
<br />  
<input type="submit" name="submit" value="ログイン">  
<input type="hidden" name="mode" value="login">  
</form>
```

上記の例であれば、ログイン ID の name 属性は user_id、パスワードの name 属性は password になります。また、input type="hidden" で name="mode" value="login" も POST していますので、その他の追加パラメータに追加します。

※HTML タグについては書籍やリファレンスなどをご確認ください。

(*3)について

アプリケーションによってはログインページにアクセスした際に自動で生成され、値が一定でないエンティティが存在することがあります。

例

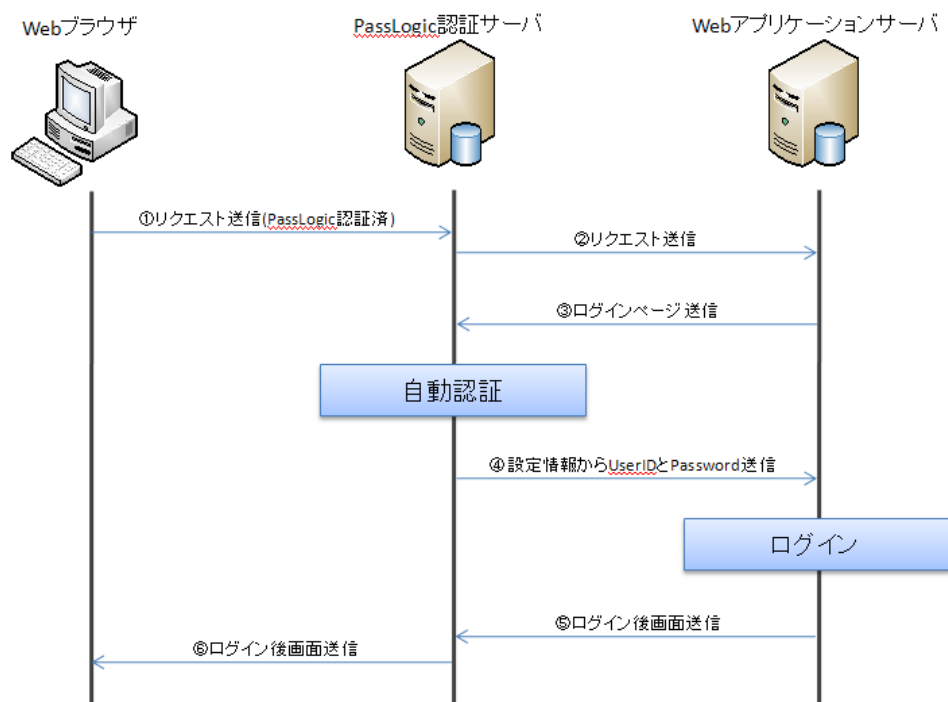
```
<form method="post" name="LoginForm" action="login.cgi">
ログイン名: <input type="text" name="user_id"><br />
パスワード: <input type="password" name="password"><br />
  <input type="hidden" name="SESSION_TOKEN" value="[毎回変わる値]">
<br />
<input type="submit" name="submit" value="ログイン">
<input type="hidden" name="mode" value="login">
</form>
```

このようなログインページの場合、「ログインページから取得する値の名称」に「SESSION_TOKEN」を設定すると、動的に変わる値を PassLogic サーバが取得して代理 POST する際に取得した名前=値のペアと一緒にアプリケーションサーバに送信することができます。

2.8.2. 認証方式

サーバ自動認証とクライアント認証の違いは以下の通りです。通常はサーバ自動認証を選択してください。サーバ自動認証で WebSSO が動作しない場合にはクライアント認証を試します。

1.7.1.1. サーバ自動認証のシーケンス図

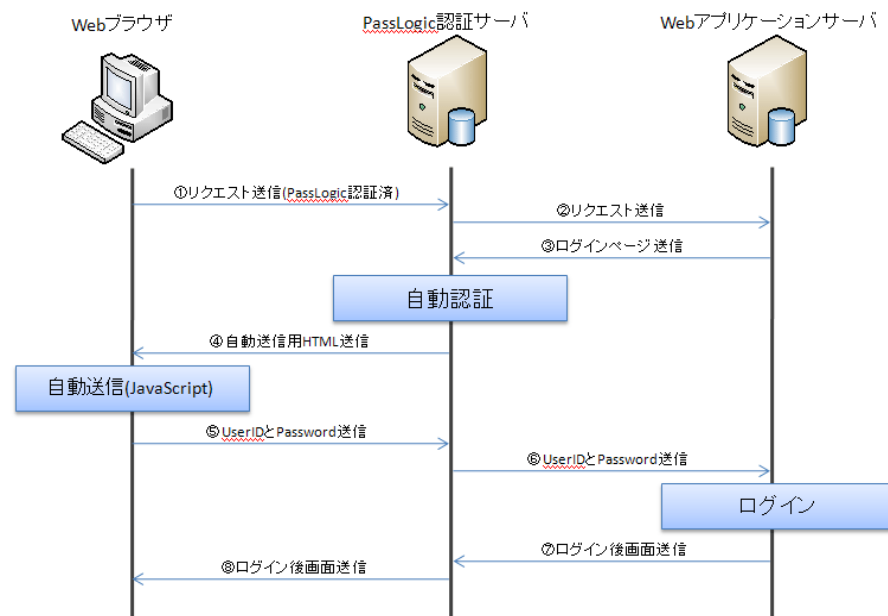


PassLogic 認証サーバが代理でユーザ ID、パスワードを Web アプリケーションに対して送信します。Web アプリケーションによってはログインが成功しないこともあります、アプリケーションのユーザ ID、パスワードが外部ネットワーク上を流れることがないのでセキュアな方式です。

※ログイン後に自動的にリダイレクションを行うアプリケーションには対応できませんので、その場合にはクライアント自動認証(JavaScript)をご利用ください。

※ログインの際に JavaScript などパスワードを暗号化して送信するアプリケーションには対応していません。

1.7.1.2. クライアント自動認証のシーケンス図



一旦クライアント(Web ブラウザ)を経由しますので適用範囲が広がりますが、Web アプリケーションのユーザ ID およびパスワードが外部ネットワーク上を流れますので、SSL で接続するなどしてセキュリティリスクを回避してください。

※i-mode ブラウザ等 JavaScript をサポートしていないブラウザの場合には、WebSSO 時にボタンをクリックする必要があります。

クライアントに送信する HTML の例(PassLogic 認証サーバにより自動生成された後送信され、JavaScript により自動的に処理されます)

```

<html>
<head>
<title>PassLogic Auto Login Agent</title>
<script language="javascript" type="text/javascript">
<!--
window.onload = function login() {
    document.form1.submit();
}
-->
</script>
<body>
<form name="form1" method="POST" action="/login.cgi">
<input type="hidden" id="user_id" name="user_id" value="USER" />
  
```



```
<input type="hidden" id="password" name="password" value="PASSWORD" />
<input type="submit" name="login" value="login">
</form>
<div align="center">PassLogic Auto Login Process</div>
</body>
</html>
```

2.8.3. 各アプリケーションの設定例

以下設定例になります。個別の連携方法詳細については、別途弊社サポートまでお問い合わせください。

desknet's(デスクネッツ) ver7

※PC 用ログインフォーム

ログイン ID の name 属性	userid	
パスワードの name 属性	_word	
Web アプリケーションとの通信方式	POST	
認証方式	サーバ自動認証	
認証の送信先 URL		
その他の追加パラメータ	(付加するパラメータ)	(パラメータの値)
	log	on
	cmd	certify
ユーザごとのパラメータ		

サイボウズ office8

※PC 用ログインフォーム

ログイン ID の name 属性	_Account	
パスワードの name 属性	password	
Web アプリケーションとの通信方式	POST	
認証方式	サーバ自動認証	
認証の送信先 URL		
その他の追加パラメータ	(付加するパラメータ)	(パラメータの値)
	_System	login
	_Login	1
ユーザごとのパラメータ		

2.9. SAML 連携

SAML(Security Assertion Markup Language)2.0 による認証連携が可能です。

2.9.1. SAMLSP 登録

SP(Service Provider)を登録します。

プロバイダ	サービスプロバイダ名
ドメイン	ドメイン名
ユーザ ID に付加するサフィックス名	ユーザ ID にサフィックスを付加したい場合、サフィックスを入力します。
アクセス可能なグループ	アクセス可能なグループを選択します。複数グループを指定する場合はカンマ(,)で区切ります。
relayStateURL	SP(Service Provider)の仕様にしたがって入力してください。
recipient	SP(Service Provider)の仕様にしたがって入力してください。
destination	SP(Service Provider)の仕様にしたがって入力してください。
issuer	SP(Service Provider)の仕様にしたがって入力してください。

2.9.2. SAML 証明書

証明書を登録します。CERTIFICATE および PRIVATE KEY を登録します。SAML 連携を実現するために SP(Service Provider)にも証明書の登録が必要です。SP(Service Provider)側の設定方法は各サービスプロバイダのマニュアル、ヘルプ等をご参照ください。

Google Apps の場合の設定例

(*) 必須項目

プロバイダ(*)	google
ドメイン(*)	passlogy.net
ユーザIDに付加するサフィックス名	
アクセス可能なグループ	
RelayStateURL(*)	http://mail.google.com/a/passlogy.net
Recipient(*)	https://www.google.com/a/passlogy.net/acs
Destination(*)	https://www.google.com/a/passlogy.net/acs
Issuer(*)	http://demo2.passlogy.com/

次へ

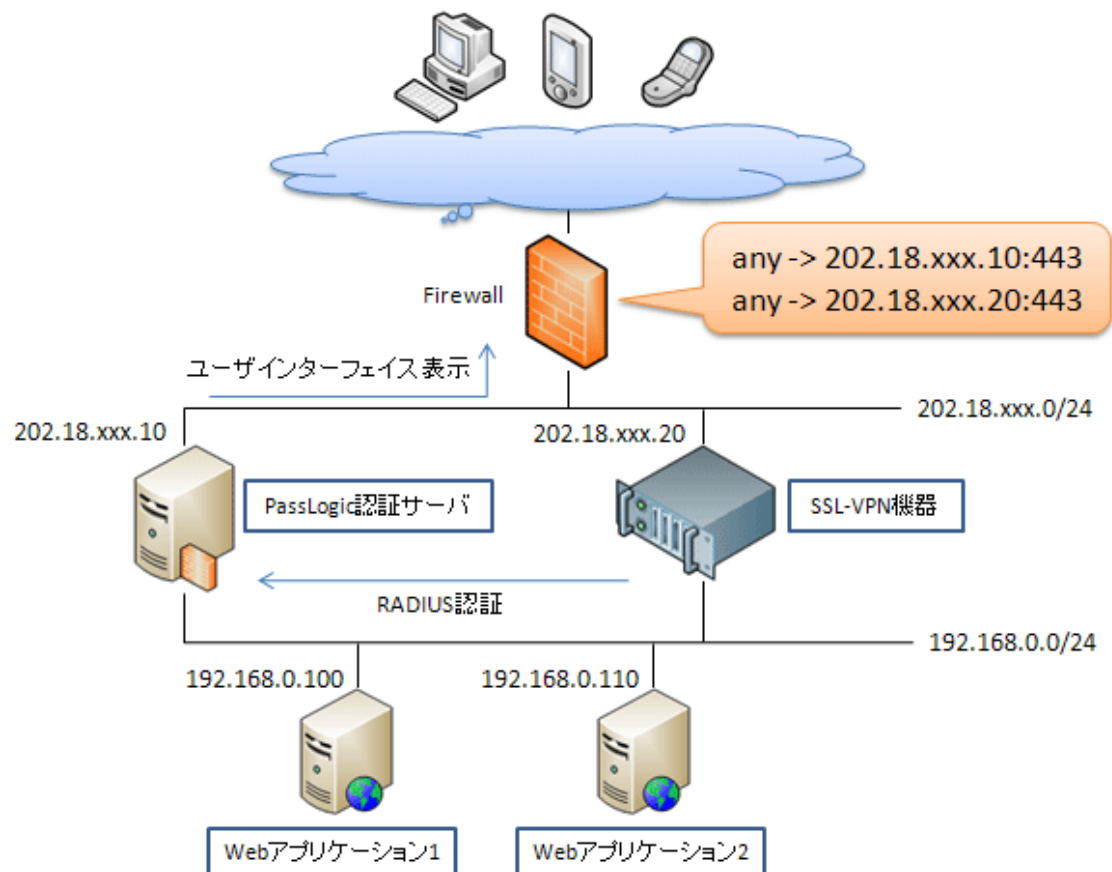
2.10. RADIUS 連携

2.10.1. RADIUS 連携の概要

PassLogic 認証サーバは、サーバ内部的に PassLogic コアエンジン(乱数生成ロジック及びユーザデータ管理など)と RADIUS サーバに分かれて動作し、PassLogic 用に拡張された RADIUS サーバは PassLogic の認証 API をコールすることで、全体で RADIUS サーバとして動作しています。

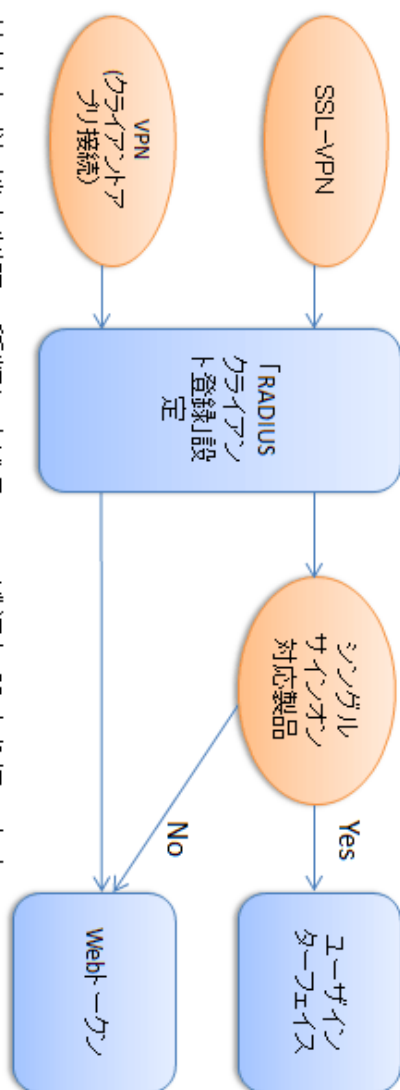
そのため、VPN 装置、SSL-VPN 装置など RADIUS の連携機能を有しているアプリケーションまたは機器の RADIUS 機能により連携させることが可能です。

認証方式は、PAP、CHAP、MSCHAPv1,v2 に対応しています。



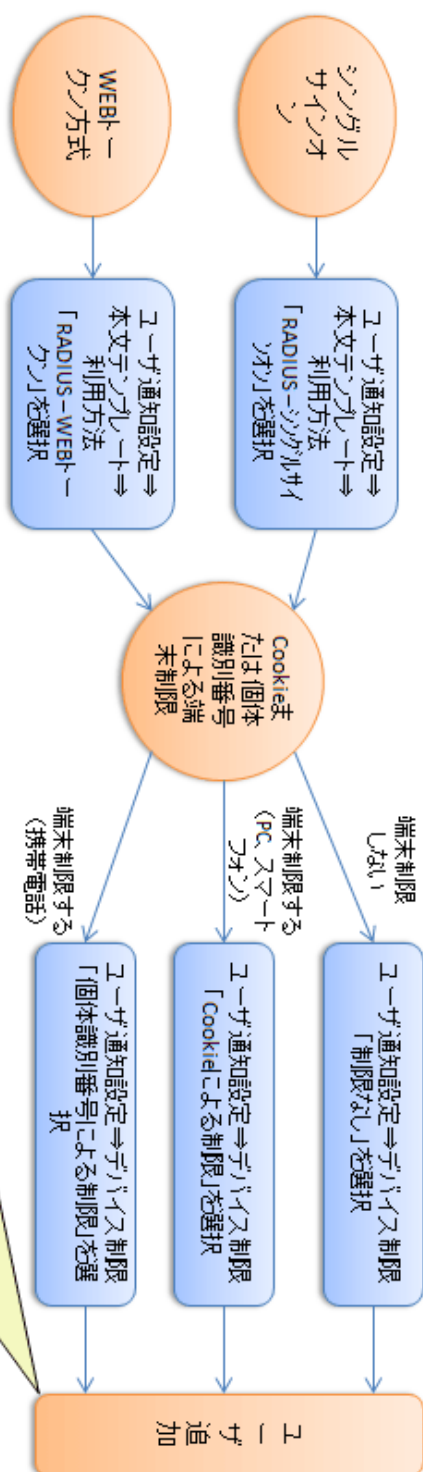
2.10.2. RADIUS 連携 (SSL-VPN、VPN)と PassLogic を連携させる際の設定フロー

1. 連携する機器に応じて、設定を行います。



※シングルサインオン対応製品でも、Webトークン方式で接続できるため、ユーザーサインタフデバイスの設定を行う前に、Webトークン方式で接続できることをご確認ください。

2. 接続方式と端末制限の種類に応じて、ユーザー通知設定を行います。



※注意
・シングルサインオン方式では、ユーザーID=デバイスIDでデバイスIDを作成してください。 ※1つ目のデバイスIDは自動的にユーザーID=デバイスIDで作成されます。
・端末制限の種類に応じて、デバイスIDのデバイスタイプを選択してください。

2.10.3. RADIUS 設定

PassLogic 管理ツールから、以下のように RADIUS 経由で認証する機器を登録します。

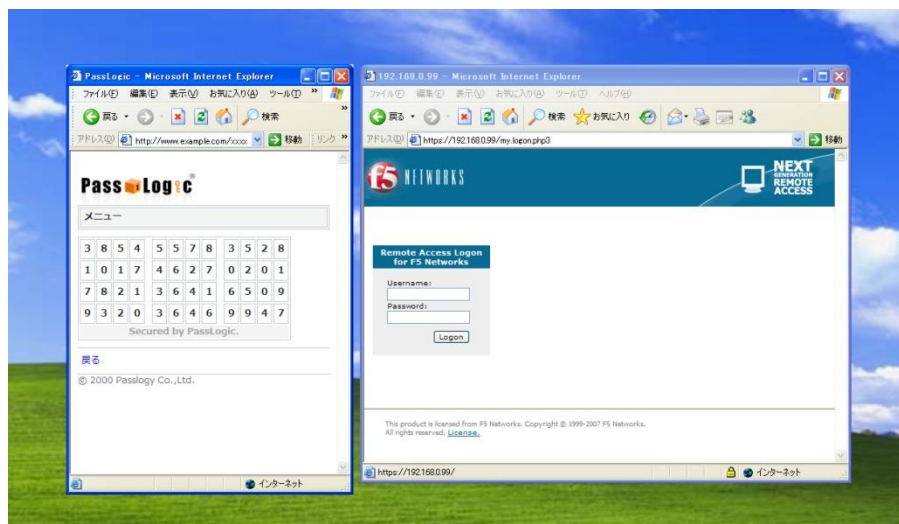
RADIUS クライアントの追加をクリックしてください。

識別子	識別子です。英数字で入力してください。
IP アドレス	アクセスする RADIUS クライアントの IP アドレス、またはネットワーク
シークレット	共有シークレット文字列
ユーザごとのアトリビュート	ユーザごとにアトリビュートを送信する必要がある場合にアトリビュート名を入力します。 group のアトリビュート名を指定します。(初期値: Filter-Id) RFC2865 等を参照の上、RADIUS のアクセス許可(Access Accept)パケットに付加できるアトリビュートのみ入力してください。

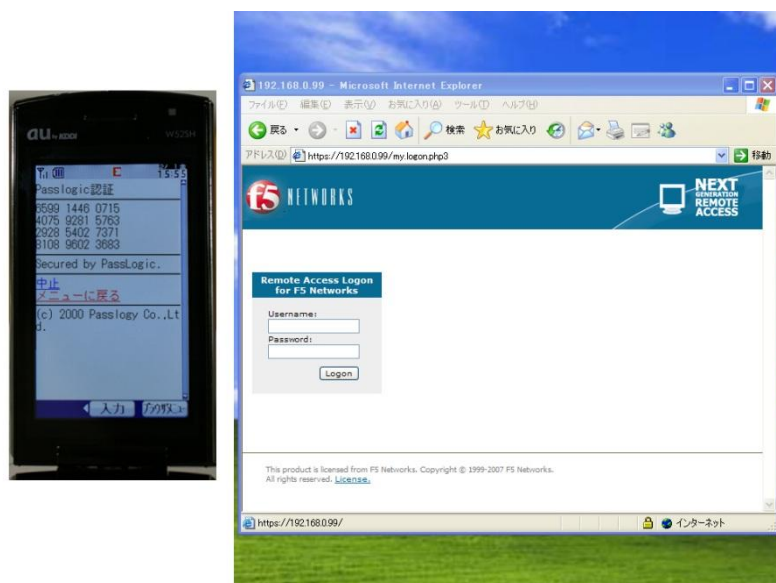
2.10.4. Web トークン

SSL-VPN 装置などの RADIUS クライアントとして動作するシステムが提供するログイン画面においてユーザはログインを行います。ログインに必要な乱数表は、パソコンや携帯電話でログイン画面とは別に取得します。

【PC で乱数表を取得した場合の画面例】



【携帯電話で乱数表を取得した場合の画面例】



※Web トークンに、Android および iOS からアクセスした場合には、乱数表の下にコピーペースト用の入力フォームが表示されます。

2.10.5. ユーザインターフェイス

PassLogicが持つユーザインターフェイスから、VPN機器等へ認証をダイレクトにPOSTします。これにより UID 入力→乱数表表示→ワンタイムパスワード入力という一画面での遷移が可能です。

※各機器との連携については、別途個別の技術資料を担当までお問い合わせ下さい。

アプリケーション名称	アプリケーションの名称です。半角英数字で入力してください。(例 sslvpn)
AnyConnect	Cisco AnyConnect と連携する際に使用します。 ※設定方法は別途お問合せ下さい。
認証の送信先 URL	ログイン情報を送信する URL を指定してください。
ログインIDの name 属性(*1)	アプリケーションのログインに使用されるログイン ID(ユーザ ID)の name 属性の名称を入力してください。(例: UserID)
パスワードの name 属性(*1)	アプリケーションのログインに使用されるパスワードの name 属性の名称を入力してください。(例: Password)
Web アプリケーションとの通信方式	GET または POST を選択します。
ログインページの URL	アプリケーションのログインページ URL を指定してください。

ログインページから取得する値の名前(*2)	ログインページから取得したいエンティティがある場合、エンティティの名前を入力します。 (例：SESSION_TOKEN)
その他の追加パラメータ	アプリケーションのログインの際にログイン ID、パスワード以外に必要なパラメータはこちらで設定してください。アプリケーションごとに異なります。
ユーザごとのパラメータ	グループ ID などユーザごとに POST したいパラメータの name 属性を指定します。ユーザ登録時の param1-10 が value 属性として対応します。
ドメインパスワード(*3)	FirePass のドメインパスワード（キャッシュ）利用時に有効にします。

(*1)について

VPN 機器ごとにログイン ID の name 属性、パスワードの name 属性は異なりますので、各 VPN 機器のログインページの HTML ソースを確認してください。

(*2)について

VPN 機器によってはログインページにアクセスした際に自動で生成され、値が一定でないエンティティが存在することがあります。

例

```
<form method="post" name="VPNForm" action="login.cgi">
ログイン名: <input type="text" name="user_id"><br />
パスワード: <input type="password" name="password"><br />
  <input type="hidden" name="SESSION_TOKEN" value="[毎回変わる値]">
<br />
<input type="submit" name="submit" value="ログイン">
<input type="hidden" name="mode" value="login">
</form>
```

上記のようなログインページの場合「ログインページから取得する値の名前」に「SESSION_TOKEN」を指定することで、PassLogic 認証サーバが動的に変わる値を HTML ソースから取得し名前=値のペアをアプリケーションサーバ(あるいは VPN 機器)に送信します。

(*3)ドメインパスワードに使用可能な文字

半角英数字および以下の記号が使用可能です。

アットマーク	@
パーセント記号	%

プラス記号	+
円記号	¥
スラッシュ	/
一重引用符	'
感嘆符	!
番号記号	#
ドル記号	\$
カレット	^
疑問符	?
コロン	:
ドット	.
カッコ	()
中カッコ	{ }
大カッコ	[]
チルダ	~
ハイフン	-
アンダースコア	_

設定後

http://[PassLogic 認証サーバのホスト名]/uagent/

にアクセスして認証を行います。

※RADIUS に対する認証は、Web トークンまたはユーザインターフェイスで表示された乱数表でのみ有効です。

2.10.6. RADIUS 認証動作

radclient による認証動作の例です。実際の動作はご利用のアプリケーションまたは機器によります。

・ PAP

```
# echo "User-Name=test, User-Password=8283" | radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 44 to 192.168.0.203 port 1812
    User-Name = "test"
    User-Password = "8283"
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=44,length=20
```

• CHAP

```
# echo "User-Name=test, CHAP-Password=0772" | radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 42 to 192.168.0.203 port 1812

    User-Name = "test"

    CHAP-Password = 0x2a49ec0d72c3bbc6dbe850ef2edda47f32
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=42,length=20
```

2.11.ID 同期

ID 同期機能を使うことで、対応している各製品とデータ同期を行うことができます。

以下のデータ同期に対応しています。

OpenLDAP

ActiveDirectory

LDAP サーバ名	LDAP サーバのホスト名または IP アドレスを指定します。
LDAP サーバのポート番号	LDAP サーバのポート番号を入力します。通常は 389 番ポートです。
バインド DN	バインド DN を入力します。
ldapsrch に必要なパスワード	ldapsrch に必要となるパスワードを入力します。
LDAP タイプ	OpenLDAP, ActiveDirectory, その他 より同期の対象とするサーバを選択してください。
ターゲットオブジェクトの DN	ターゲットオブジェクトの DN を入力します。
検索フィルタ	検索条件を設定します。
ユーザ ID に使用するアトリビュート	ユーザ ID に使用するアトリビュートを入力します。
メールアドレスに使用するアトリビュート	メールアドレスに使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
氏名に使用するアトリビュート	氏名に使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
グループに使用するアトリビュート	グループに使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
PIN に使用するアトリビュート	PIN に使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
初期パスワード位置設定	初期パスワード位置設定を選択します。「ランダム位置で発行」または「初

	期パスワード位置情報で発行」
初回にパスワード位置情報の変更が必要	ユーザが初回アクセスする際にパスワード位置情報の変更になります。
有効期限に使用するアトリビュート	ユーザアカウントの有効期限です。(フォーマット:yyyymmdd 例:20110901) ※項目が空欄の場合は同期時に上書きしません。
備考に使用するアトリビュート	備考に使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
パラメータに使用するアトリビュート(param01-10)	param01-10 に使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
apppassword に使用するアトリビュート	apppassword に使用するアトリビュートを入力します。 ※項目が空欄の場合は同期時に上書きしません。
ユーザ ID の同期時刻	同期する時刻またはローテーションを指定します。 例:一日一回 03 時 00 分に同期であれば一日一回 03:00 に同期を行います。
ユーザ追加時のアクション	同期の際、ユーザアカウント追加時のデバイスタイプとアクションを指定します。※LDAP 連携で追加したユーザのパスワード位置情報はランダムなものが設定されます。
同期時の動作	追加のみ:参照先のユーザ情報を PassLogic に追加・更新(メールアドレスの変更)します。 完全同期:参照先と PassLogic のユーザ情報を完全に同期します。PassLogic 上に存在するユーザ ID が参照先に存在しない場合は PassLogic のユーザが削除されます。(admin 権限ユーザは対象になりません)

※改行コードを含む値を持つアトリビュートを指定しないでください。

設定例(パラメータはそれぞれの環境に合わせて下さい)

2.11.1. OpenLDAP

バインド DN	cn=admin,ou=profile,dc=passlogy,dc=com
ldapsearch に必要なパスワード	*****
ターゲットオブジェクトの DN	ou=staff, ou=profile,dc=passlogy,dc=com
検索フィルタ	uid=*
ユーザ ID に使用するアトリビュート	uid
メールアドレスに使用するアトリビュート	mail

2.11.2. ActiveDirectory

バインド DN	cn=administrator,cn=Users,dc=win2008,dc=passlogy,dc=com
ldapsearch に必要なパスワード	*****
ターゲットオブジェクトの DN	cn=Users,dc=win2008,dc=passlogy,dc=com
検索フィルタ	(samaccountname=*)
ユーザ ID に使用するアトリビュート	samaccountname
メールアドレスに使用するアトリビュート	mail

- ・「有効期限」は「yyyymmdd」の形式で設定して下さい。
- ・同期の対象となる Active Directory は 1 台のみです。
- ・PassLogic のグループは 英数字のみ利用できます。※英数字以外の文字が含まれているアトリビュートを「グループに使用するアトリビュート」に指定した場合は、グループは取り込まれません。
- ・PassLogic のユーザ ID は英数字、ハイフン、アンダーバー、ドット、アットマークのみが利用できます。※上記の文字以外が含まれているアトリビュートを「ユーザ ID に使用するアトリビュート」に指定した場合は、ユーザは取り込まれません。
- ・デバイス ID はユーザ ID と同じ値で 1 つ生成されます。(2 つ目以降のデバイス ID は作成できません)

2.12. CSV ファイルによるデータ同期

CSV ファイルを cron で定期的に取り込むことでユーザの追加/削除を自動化することができます。

ファイル形式	各項目が半角ダブルコーテーションで括られている。 項目間がカンマで区切られている。 行区切りは改行(CRLF)する。 マルチバイトを使用する場合の文字コードは ShiftJIS 例: "aa","bb","cc"
項目一覧	ユーザ ID, [メールアドレス], [氏名], [グループ], [PIN], [初期パスワード 位置情報(空欄の場合ランダム)], [初回にパスワード位置情報の変更が必要(Y/N)], [有効期限(yyyymmdd)], [備考], [メール通知(Y/N)], [param1],

	[param2], [param3], [param4], [param5], [param6], [param7], [param8], [param9], [param10], [apppassword] ※param1-10 はリモートアクセス管理（Web シングルサインオン）や RADIUS 管理（ユーザごとのアトリビュート）の際に利用する拡張パラメータです。 ※apppassword は WebSSO 機能を利用する際の Web アプリケーション側のパスワードの項目です。													
設定ファイル	加えてコマンド実行前に以下の設定ファイルを作成して下さい。 設定項目 <table><tr><th>行数</th><th>設定値</th></tr><tr><td>1</td><td>先頭行を項目名としてスキップ 1: スキップ 0: スキップしない</td></tr><tr><td>2</td><td>デバイスタイプ normal: 制限なし hyper: Cookie による制限 slso: 個体識別番号による制限</td></tr><tr><td>3</td><td>同期モード addonly: 追加更新のみ sync: 完全一致 delonly: 削除のみ</td></tr><tr><td>4</td><td>読み込み行のフォーマット(読み込む行のフォーマットを指定してください。先頭の uid は固定です)</td></tr><tr><td>5</td><td>デバイス ID sameas_uid: uid と同じ random: ランダムで生成</td></tr></table> 設定ファイルサンプル <table><tr><td>0 normal addonly uid,uemail,uname,ugroup,fixpass,defpass,upasschgforced,uexpiry,ucomment,accmail,param1,param2,param3,param4,param5,param6,param7.param8,param9,param10,apppassword sameas_uid</td></tr></table>	行数	設定値	1	先頭行を項目名としてスキップ 1: スキップ 0: スキップしない	2	デバイスタイプ normal: 制限なし hyper: Cookie による制限 slso: 個体識別番号による制限	3	同期モード addonly: 追加更新のみ sync: 完全一致 delonly: 削除のみ	4	読み込み行のフォーマット(読み込む行のフォーマットを指定してください。先頭の uid は固定です)	5	デバイス ID sameas_uid: uid と同じ random: ランダムで生成	0 normal addonly uid,uemail,uname,ugroup,fixpass,defpass,upasschgforced,uexpiry,ucomment,accmail,param1,param2,param3,param4,param5,param6,param7.param8,param9,param10,apppassword sameas_uid
行数	設定値													
1	先頭行を項目名としてスキップ 1: スキップ 0: スキップしない													
2	デバイスタイプ normal: 制限なし hyper: Cookie による制限 slso: 個体識別番号による制限													
3	同期モード addonly: 追加更新のみ sync: 完全一致 delonly: 削除のみ													
4	読み込み行のフォーマット(読み込む行のフォーマットを指定してください。先頭の uid は固定です)													
5	デバイス ID sameas_uid: uid と同じ random: ランダムで生成													
0 normal addonly uid,uemail,uname,ugroup,fixpass,defpass,upasschgforced,uexpiry,ucomment,accmail,param1,param2,param3,param4,param5,param6,param7.param8,param9,param10,apppassword sameas_uid														

コマンド例

```
# /usr/bin/php /opt/passlogic/passlogic-admin/php/cgi/userimport.php {CSV ファイルのパス} {設定ファイルのパス}
```

2.13. バックアップの方法

PassLogic 認証サーバソフトウェアのデータをバックアップする場合は、以下のファイルをバックアップしてください。

- ・ ユーザ情報、セッション情報……passlogicdata/ ディレクトリ以下
- ・ ログ情報……/var/log/passlogic/ ディレクトリ以下
- ・ apache の設定ファイル…… /etc/httpd/conf/httpd.conf , /etc/httpd/conf.d/以下

標準インストール時には以下のファイル及びディレクトリになります。

```
/opt/passlogic/passlogicdata  
/opt/passlogic/passlogic-config.xml  
/opt/passlogic/passlogic-admin/php/config_settings.inc.php  
/etc/raddb/clients.conf  
/etc/httpd/conf/httpd.conf  
/etc/httpd/conf.d/  
/var/log/passlogic/ (※ログも必要な場合)
```

*PassLogic システムは、これらのファイルを書き戻すことによって、ファイルがバックアップされた時点の状態に戻ります。

*PassLogic 認証サーバソフトウェアの動作中に rsync など、他のマシンにバックアップすることも可能です。

*バックアップ・リストアは必ず PassLogic の同一バージョン間で実施してください。

2.14. 管理者(admin)パスワードのリセット方法

管理者(admin)パスワードがロックされた場合は、以下の手順でリセットしてください。

```
/opt/passlogic/passlogic-admin/php/config_settings.inc.php  
をテキストエディタで開きます。
```

```
define("ADMIN_PASSWORD_RESET_MODE", 設定値);
```

の設定値を 1 に変更してください。

```
https://[PassLogic のホスト名]:12080/passlogic-admin/reset.php
```

にブラウザでアクセスして「リセットボタン」をクリックしてください。

以上で、管理者のパスワード(パスワード位置情報)はリセットされますので

https://{PassLogic 管理ツールのホスト名}:12080/passlogic-admin/

にアクセスして、パスワードを再設定してください。

再設定が終わりましたら、必ず config_settings.inc.php ファイルの

```
define("ADMIN_PASSWORD_RESET_MODE", 設定値);
```

の設定値を 0 に戻してください。

2.15. 監視対象プロセス

PassLogic 認証サーバは、httpd と radiusd として動作します、プロセスを監視する際は、以下のプロセスを監視してください。

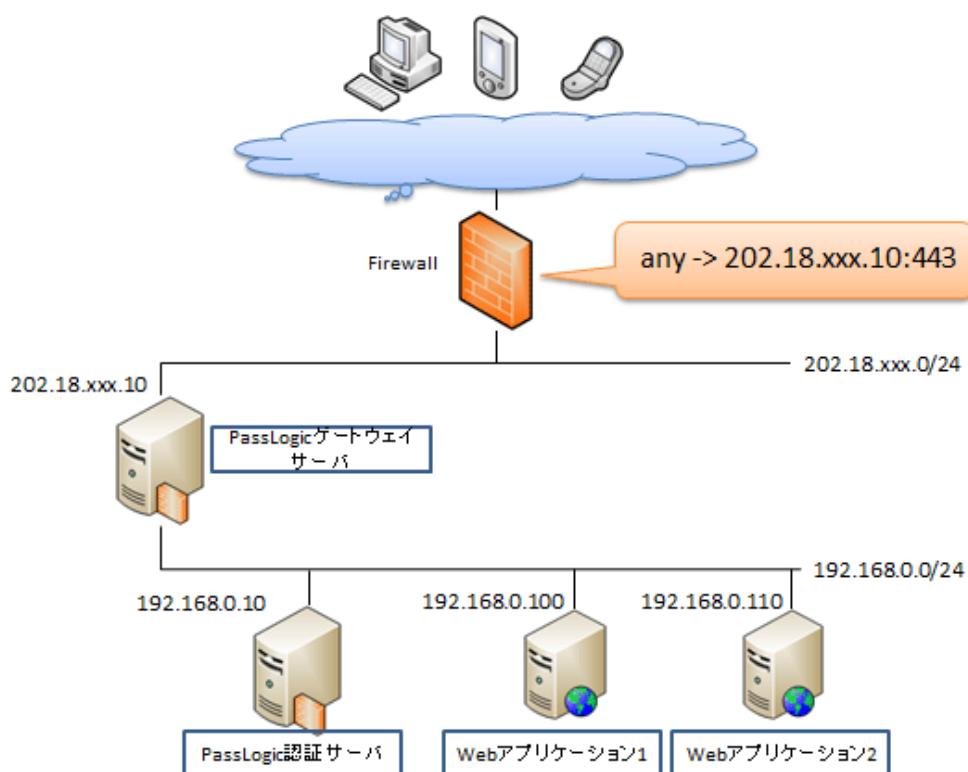
```
/usr/sbin/httpd
```

```
/usr/sbin/radiusd -d /etc/raddb
```

2.16. PassLogic 認証サーバをイントラネットに配置する

2.16.1. リモートアクセス(リバースプロキシ)の場合

PassLogic 認証サーバをゲートウェイサーバと認証サーバの 2 台に分離して、エクストラネットにゲートウェイサーバ(リバースプロキシ)、イントラネットに認証サーバと分けて運用することも可能です。



※ネットワークおよびファイアウォールの設定は別途行っていただく必要があります。

認証サーバ(192.168.0.10)側の設定

通常通り PassLogic をインストールした後で、`/opt/passlogic/AUTH` というファイルを作成してください。

```
# touch /opt/passlogic/AUTH
```

これで管理画面のメニューが認証サーバ用になります。

ゲートウェイサーバ(202.18.xxx.10)側の設定

通常通り PassLogic をインストールした後で、/opt/passlogic/REMOTE というファイルを作成してください。

```
# touch /opt/passlogic/REMOTE
```

これで管理画面のメニューがゲートウェイサーバ用になります。

PassLogic 管理ツールよりリモートアクセス管理を利用して設定を行います。

PassLogicAPI の URL をイントラにある PassLogic 認証サーバの API を指定してください。

例

```
http://192.168.0.10:12079/passlogic
```

さらに、

/opt/passlogic/passlogic-admin/php/config_settings.inc.php

を以下のように変更してください。

【修正前】

```
/**
 * PassLogic api url
 * PassLogic サーバ API の URL を指定してください。
 * (adm,box,user は含めないでください)
 */
define("PASSLOGIC_BASE_URL", "http://127.0.0.1:12079/passlogic");
```

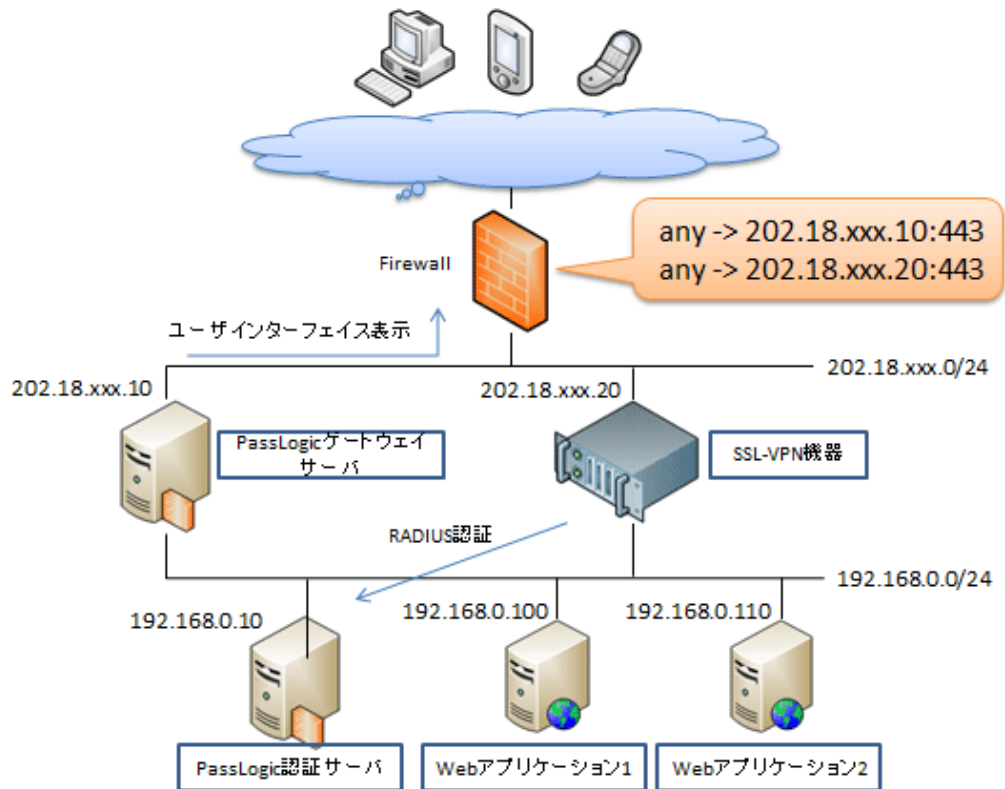
【修正後】

```
/**
 * PassLogic api url
 * PassLogic サーバ API の URL を指定してください。
 * (adm,box,user は含めないでください)
 */
define("PASSLOGIC_BASE_URL", "http://192.168.0.10:12079/passlogic");
```

リモートアクセス管理以外のユーザ管理等は、認証サーバ(192.168.0.10)側の管理ツールで行ってください。

バックアップ/リストアは、それぞれのマシンで個別に行ってください。

2.16.2. RADIUS 連携の場合



/opt/passlogic/passlogic-admin/php/config_settings.inc.php

を以下のように変更してください。

【修正前】

```
/**
 * PassLogic api url
 * PassLogic サーバ API の URL を指定してください。
 * (adm,box,user は含めないでください)
 */
define("PASSLOGIC_BASE_URL", "http://127.0.0.1:12079/passlogic");
```

【修正後】

```
/**
 * PassLogic api url
 * PassLogic サーバ API の URL を指定してください。
```

```
* (adm,box,user は含めないでください)
*/
define("PASSLOGIC_BASE_URL", "http://192.168.0.10:12079/passlogic");
```

※管理ツールは、認証サーバ(192.168.0.10)側の管理ツールで行ってください。

2.17. グラフィックデザインのカスタマイズ

2.17.1. ユーザーインターフェース一覧

リモートアクセス連携用

PC 向け	URL	https://[ホスト名]/menu/
	スタイルシート	/opt/passlogic/passlogic-admin/php/css/style.css
PC 向け(タブ形式メニュー)	URL	https://[ホスト名]/tmenu/
	スタイルシート	/opt/passlogic/passlogic-admin/php/css/style.css
スマートフォン向け	URL	https://[ホスト名]/imenu/
	スタイルシート	/opt/passlogic/passlogic-admin/php/css/sp.css
携帯電話向け	URL	https://[ホスト名]/mmenu/
	スタイルシート	-

*リモートアクセス連携用の URL で取得した乱数表は RADIUS 認証では利用できません。

*ユーザは、必ず上記の各メニューURL からログインする必要があります。アプリケーションにログインした後の URL をブックマークしないでください。

RADIUS 連携用

SSO(全クライアント端末共通)	URL	https://[ホスト名]/uagent/
	スタイルシート	/opt/passlogic/passlogic-admin/php/css/tokengui.css
Web トークン(全クライアント端末共通)	URL	https://[ホスト名]/passlogic/ui/
	スタイルシート	/opt/passlogic/passlogic-admin/php/css/tokengui.css

ロゴ画像ファイル

```
/opt/passlogic/passlogic-admin/php/images/passlogic-logo.gif
```

2.17.2. リモートアクセスログイン画面のカスタマイズ

ログイン画面、乱数表表示画面、ログアウト画面のカスタマイズは、以下の HTML テンプレートを編集頂くことで可能です。

*ログイン画面をカスタマイズされる場合は「パスロジック ソフトウェアライセンス規約」に従ってカスタマイズしてください。

/opt/mod_auth_passlogic/tmpl/login.html	ユーザ ID 入力
/opt/mod_auth_passlogic/tmpl/matrix.html	乱数表表示・入力画面
/opt/mod_auth_passlogic/tmpl/logout.html	ログアウト

.en は英語インターフェイス

2.17.3. リモートアクセスログイン画面(iPhone)のカスタマイズ

ログイン画面、乱数表表示画面、ログアウト画面のカスタマイズは、以下の HTML テンプレートを編集頂くことで可能です。

/opt/mod_auth_passlogic/itmpl/login.html	ユーザ ID 入力
/opt/mod_auth_passlogic/itmpl/matrix.html	乱数表表示・入力画面
/opt/mod_auth_passlogic/itmpl/logout.html	ログアウト

.en は英語インターフェイス

2.17.4. リモートアクセスログイン画面(携帯)のカスタマイズ

ログイン画面、乱数表表示画面、ログアウト画面のカスタマイズは、以下の HTML テンプレートを編集頂くことで可能です。

/opt/mod_auth_passlogic/mtmpl/login.html	ユーザ ID 入力
/opt/mod_auth_passlogic/mtmpl/matrix.html	乱数表表示・入力画面
/opt/mod_auth_passlogic/mtmpl/logout.html	ログアウト

※携帯向けのログイン画面は、プルダウンによる日本語/英語の切り替えには対応しておりませんので、あらかじめご了承ください。

2.17.5. 各ログイン画面で利用できる変数

各テンプレートに共通の変数です。

<%ERRORTEXT%>	エラーがある場合、エラーメッセージとエラーコードを表示します。
<%PASSLOGICUID%>	入力された uid を表示します。
<%PASSLOGIC0%>-<%PASSLOGIC47%>	PassLogic の乱数表の数字を表示します。

2.18. 参考資料

2.18.1. PassLogic 管理ツールの設定項目

/opt/passlogic/passlogic-admin/php/config_settings.inc.php ファイルをテキストエディタ等で編集することで、管理ツールの設定変更が行えます。設定できる個所は以下のとおりです。

```
define("PASSLOGIC_BASE_URL", " http://127.0.0.1:12079/passlogic ");
```

PassLogic サーバ API の URL を指定してください。(adm,box,user は含めないでください)


```
define("PASSLOGIC_LOG_DIR", "/var/log/passlogic");
```

PassLogic ログディレクトリを指定します。(PassLogic と管理画面が同一マシン上にある場合にのみ正常に動作します)


```
define("ADMIN_PASSWORD_RESET_MODE", 0);
```

管理者のパスワード(パスワード位置情報)をリセットする際に 1 にします。

2.18.2. リモートアクセス管理で Microsoft IIS にアクセスする場合

PassLogic リモートアクセス機能で Microsoft IIS にアクセスする際に Proxy エラーが表示される場合には、以下のような設定ファイルを作成してください。

```
# vi /etc/httpd/conf.d/for_IIS.conf
```

```
<Location /path_to_IIS/>
SetEnv force-proxy-request-1.0 1
SetEnv proxy-nokeepalive 1
</Location>
```

※path_to_IIS は IIS サーバへの ProxyPass

2.18.3. WebSSO で Outlook Web Access にログインする場合

PassLogic 管理ツールのアプリケーション設定、WebSSO から以下のように設定します。

※192.168.0.80 は Exchange サーバ、192.168.0.142 は PassLogic サーバ

アプリケーション名称	公開パス	ローカルアプリケーションのURL	メニュー表示可能なグループ	削除
OWA	/owa/	https://192.168.0.80/owa/		削除

アプリケーション名称		編集	削除
OWA(PC)	ログインIDのname属性: username パスワードのname属性: password 認証の送信先URL: https://192.168.0.142/owa/auth/owaauth.dll その他の追加パラメータ: destination=https://192.168.0.80/owa/ flags=0 forcedownlevel=0 trusted=0 isUtf8=1 ユーザごとのパラメータ: param1 AS / param2 AS / param3 AS / param4 AS / param5 AS	編集	削除

以下の設定ファイルを追加します。

```
# vi /etc/httpd/conf.d/owa.conf
```

```
RequestHeader set Front-End-Https "On"

ProxyPass /exchange/ https://192.168.0.80/exchange/
ProxyPassReverse /exchange/ https://192.168.0.80/exchange/

ProxyPass /exchweb/ https://192.168.0.80/exchweb/
ProxyPassReverse /exchweb/ https://192.168.0.80/exchweb/

ProxyPass /public/ https://192.168.0.80/public/
ProxyPassReverse /public/ https://192.168.0.80/public/
```

2.18.4. RADIUS 連携のユーザインターフェイスで target の値を URL に含める方法

RADIUS 連携機能のユーザインターフェイスで target の値を URL に含めることが可能です。これにより、ユーザは target 名をプルダウンで選ぶことなくログインすることが可能です。

```
http://[PassLogic 認証サーバのホスト名]/uagent/[アプリケーションの名称]/
```

にアクセスして認証を行います。

アプリケーションの名称が、**users** の場合、アクセス先 URL は
`http://[PassLogic 認証サーバのホスト名]/uagent/users/`
となります。

vi /etc/httpd/conf.d/uagent.conf

```
RewriteEngine On

RewriteCond %{REQUEST_URI} ^/uagent/.*$

RewriteCond %{QUERY_STRING} ^$

RewriteRule ^/uagent/([0-9a-zA-Z]*)/([0-9a-zA-Z]*?)$ /uagent/$2?target=$1 [PT]

RewriteCond %{REQUEST_URI} ^/uagent/.*$

RewriteCond %{QUERY_STRING} !^$

RewriteRule ^/uagent/([0-9a-zA-Z]*)/([0-9a-zA-Z]*?)$ /uagent/$2?%{QUERY_STRING}&target=$1 [PT]
```

SSL 通信で同様にする場合には、/etc/httpd/conf.d/ssl.conf の<VirtualHost>ディレクティブ内に上記の設定を追加してください。

2.18.5. SSL 証明書のインストールについて

SSL サーバ証明書の発行機関のマニュアルに従い PassLogic が動作する Apache にインストールしてください。

2.18.6. ウィルス対策ソフトを利用する場合

下記のフォルダをスキャン対象から除外してください。

```
/opt/passlogic/passlogicdata
/var/log/passlogic
/tmp
```

3. ユーザー管理者ガイド

3.1. 管理ツールにアクセスする

PassLogic 管理ツールへはウェブブラウザでアクセスします。標準インストールを行っている場合の URL は下記の通りです。

[https:// \[ホスト名 \] :12080/passlogic-admin/](https://[ホスト名]:12080/passlogic-admin/)

3.1.1. 管理ツールログイン用のユーザ ID を入力する

管理ツールログイン用の ID を入力します。

※インストール直後は「admin」になります。



PassLogic Management Tools ログイン
IDを入力して下さい。

ログイン

(C) Passlogy Co.,Ltd. 2000-2011

3.1.2. 管理ツールログイン用のパスワードを入力する



3.2. PassLogic の状態を確認する

メインページでは PassLogic 認証サーバの状況を一覧で確認することができます。

admin 権限管理者ログイン画面

PassLogic®

Login as: admin [メインページ](#) >>

マニュアル PassLogic Management Tools

管理者一覧
管理者追加

ユーザ管理
+ ユーザー一覧
+ ロックユーザー一覧
+ ユーザ検索
+ 新規作成
+ ユーザー一括登録

リモートアクセス管理
+ ポリシー設定
+ PCアプリケーション設定
+ 携帯アプリケーション設定
+ URLマッピング
+ WebSSO

RADIUS設定
+ RADIUSクライアント登録
+ ユーザーインターフェイス
+ Webトークン

ID同期
+ LDAP設定
+ LDAP同期

PassLogic設定
+ セキュリティポリシー設定
+ メール設定
+ ユーザ通知設定
+ ログ・その他設定

管理者パスワード変更
ログ閲覧
ライセンス管理
バックアップ
リストア
ログアウト

PassLogic Authentication Server System - version 3.4.7.1

English(en)

登録ユーザ数	7
最大ユーザ数	10000
有効期限	2011/10/31 *ライセンスの有効期限が近づいています。カスタマーサポートまでお問い合わせください。
利用者	passlogy tec
種別	trial
WebSSO	active

サーバステータス

httpd	httpd (pid 10625) is running...
MTA	master (pid 1052) is running...
radiusd	radiusd is stopped
ntpd	ntpd (pid 10720) is running...

(C) Passlogy Co.,Ltd. 2000-2011

operator 権限管理者ログイン画面

PassLogic®

Login as : ope01 [メインページ](#) >>

マニュアル PassLogic Management Tools

ユーザ管理
+ ユーザー一覧
+ ロックユーザー一覧
+ ユーザ検索

管理者パスワード変更
ログアウト

PassLogic Authentication Server System - version

English(en)

(C) Passlogy Co.,Ltd. 2000-2011

※ operator はユーザのロック／アンロック、パスワード再発行のみ操作可能です。

PassLogic Authentication Server System – version x.x.x

3.2.1. PassLogic のバージョンを確認する

メインページ中に表示されます。バージョンアップ、サポート等でバージョンの確認が必要になった際にご確認ください。

3.2.2. 登録されているライセンス情報を確認する

メインページ中に現在のライセンスの状態が表示されます。

登録ユーザ数	現在登録されているユーザ数が表示されます。
最大ユーザ数	登録可能なユーザ数の最大値です。
有効期限	期限日になるとライセンス登録以外の操作が表示のみになります。ユーザの追加・削除のほかロックの解除などができなくなりますのでご注意ください。 ライセンス期限日の 90 日前になるとライセンスの更新を促すメッセージが表示されます。 ライセンスの有効期限が切れているとライセンスの更新を促すメッセージが表示されます。
利用者	ライセンスを受けているお客様名（通常は法人・団体名）が表示されます。
種別	product / trial のいずれかが表示されます。
WebSSO	WebSSO ライセンスをご購入頂いている場合は active が表示されます。 通常ライセンスをご購入頂いている場合は passive が表示されます。 通常ライセンスから WebSSO ライセンスへのアップグレードも可能です。

3.2.3. PassLogic サーバのステータスを確認する

メインページ中にサーバステータス一覧が表示されます。

httpd	ウェブサーバの状態を表示します。
MTA	メールサーバの状態を表示します。
radiusd	RADIUS サーバの状態を表示します。RADIUS 機器が登録されていない場合は停止しています。
ntpd	ntp サーバの状態を表示します。

3.3. ユーザの新規作成

左メニューの「新規作成」をクリックすることで、ユーザアカウントを新規作成することができます。

ユーザ ID (必須項目)	英数字・記号 (4-80 文字) ハイフン (-) アンダーバー (_) ピリオド (.) アットマーク (@) ユーザ登録通知メール <%UID%> 部分
メールアドレス	通知書をメールで送る場合は記入してください。
氏名	ユーザの氏名を入力します。 ユーザ通知メール<%UNAME%>部分
グループ	任意の文字列 (英数字) を設定します。 (例) soumu sales など
PIN	ワンタイムパスワードに付加する PIN (英数字※大文字小文字を区別する) の初期値を指定します。
初期パスワード位置情報 (ワンタイムパスワード)	ユーザに通知するパスワード位置情報を設定します。以下通知例※10 桁以上はアルファベット[A-Z]で表現します。 初期パスワード位置情報は 1234 5678 9ABC DE** ***** ***** ***** です。 空欄の場合はセキュリティポリシー設定の「初期パスワード位置情報」を通知します。 「パスワード位置情報をランダムに設定する」のチェックボックスを ON にすることでランダム生成したものを通知します。ワンタイムパスワードを設定しない(P I Nのみでユーザ作成する等)の場合には、初期パスワード位置情報に NULL と入力してください。
初回にパスワード位置情報の変更が必要	初回 (パスワード再発行後を含む) アクセス時に強制的にパスワード位置情報を変更させる場合は Yes に設定。パスワード変更しなくても良い場合は No に設定します。
有効期限	アカウントの有効期限日を設定します。 設定した日までアカウントは有効です。 アカウントの有効期限が切れても管理ツール上にアカウント

	は残っていますので、アカウントを削除したい場合は明示的に消す必要があります。 アカウントの有効期限切れ後、管理ツールより有効期限日を延長設定することで設定情報などをそのまま継続して利用可能です。
有効/無効	アカウントの有効/無効を選択します。
備考	メモとして自由にお使いいただけます。
param1～10	WebSSO 連携および RADIUS 連携の際に PassLogic から対象アプリケーション（または RADIUS クライアント）に対して、ユーザ毎に異なるパラメータ（またはアトリビュート）を送信する必要がある場合、param1～10 で入力した値を利用することができます。 （ケース 1）WebSSO で ID とパスワード以外にグループ ID などの値を送る必要がある場合 （ケース 2）SSL-VPN 連携時に機器毎に任意のアトリビュートを送出する必要がある場合
アプリケーションパスワード	WebSSO 連携時にアプリケーションに送信するパスワードです。複数のアプリケーションで異なるパスワードを利用している場合は上記 param の項目を使います。

3.3.1. デバイス追加

リモートアクセス管理（リバースプロキシ機能※mod_auth_passlogic）で利用する場合には、ユーザ ID と同じ名前のデバイス ID を登録します。ウェブ・トークンとして利用する場合は、デバイス ID 名に制限はありません。

【 設定手順 】

- (i) 「ユーザ管理」項目内『ユーザー一覧』または『ユーザ検索』 からユーザ ID をクリック。
- (ii) [デバイス追加]をクリック
- (iii) 必須項目（必要に応じてその他の項目）を入力し[次へ]をクリック
- (iv) 入力内容を確認し[登録]をクリック

【 項目解説 】

ユーザ ID	変更することはできません。
デバイス ID	※1～80 文字で一意的な英数字と記号 使える記号：-(ハイフン)_(アンダーバー).(ピリオド)@(アットマーク)
メールアドレス	登録通知メールを送信するための宛先アドレス。ユーザ登録で設定しているメールアドレスとは別（携帯電話宛など）に送信したい場合は、必要に応じて変更してください。
デバイスタイプ	Cookie または携帯電話の個体識別番号による利用端末を制限します。 デバイスタイプは以下が選択できます。 ・制限なし（どのパソコンでも利用できます。） ・Cookie による制限（登録時の Cookie を参照して利用端末を制限します。） ・個体識別番号による制限（登録時の個体識別番号を参照して利用端末を制限します。）

3.4. 全ユーザを一覧で見る

左メニューの「ユーザ一覧」をクリックすることでユーザ一覧を見ることができます。

3.5. ロック中のユーザを一覧で見る

左メニューの「ロックユーザ一覧」をクリックすることで、ロックされているユーザを一覧で見ることができます。

3.6. ユーザを検索する

左メニューの「ユーザ検索」をクリックすることで、ユーザ ID での検索を行うことができます。

3.7. ユーザー一括登録

CSV ファイルからユーザを作成します。

ファイル形式	CSV(カンマ区切りテキストファイル)
文字コード	ShiftJIS
デバイスタイプ	制限なし(どのパソコン、携帯でも利用できます。) Cookie による制限(登録時の Cookie を参照して利用端末を制限します。)

	個体識別番号による制限(登録時の個体識別番号を参照して利用端末を制限します。)
デバイス ID の設定モード	ユーザ作成時のデバイス ID の値を設定します。 ユーザ ID と同じ…通常はこちらを選択してください ランダム英数字列…Web トークン利用時にデバイス ID をランダムに設定した場合に選択してください。
動作モード	追加/更新のみ：参照先のユーザ情報を PassLogic に追加・更新（メールアドレスの変更）します。（ユーザ ID、PIN、初期パスワード位置情報は更新されません） 削除のみ：PassLogic 上のユーザ情報を削除します。CSV ファイルに ID があるユーザが削除対象となります。 完全同期：参照先と PassLogic のユーザ情報を完全に同期します。 PassLogic 上に存在するユーザ ID が参照先に存在しない場合は PassLogic のユーザが削除されます。（admin 権限ユーザは対象になりません）

CSV ファイルのフォーマット

項目名	設定可能値	補足
ユーザ ID(必須)	英数字、記号 (-_@)	1～80 文字
メールアドレス	制限なし(*1)	email アドレス
氏名	制限なし(*1)	実名
グループ	英数字	20 文字まで。
PIN	半角英数字	ワンタイムパスワードの頭に付加する PIN
初期パスワード位置情報	初期のパターン	空欄の場合はユーザごとにランダム発行 NULL でパスワード位置情報を設定しません。（この場合 PIN が必須になります）
初回にパスワード位置情報の変更が必要	Y or N	Y:強制パスワード変更する N:強制パスワード変更しない（空欄の場合は N）
有効期限	yyyyMMdd	ユーザの有効期限。空欄の場合は期限切れなし。
備考	制限なし(*1)	ユーザの備考
メール通知	Y or N	ユーザ追加時にメールで通知す

		るか否か。(空欄の場合は N)
param1-10	制限なし(*1)	他のシステムと連携する際に利用する値です。通常は利用しません。
アプリケーションパスワード	制限なし(*1)	WebSSO(シングルサインオン)機能を利用する際に、ウェブアプリケーションのパスワードを入力します。

(*1) ダブルクォートを入力するときは、ダブルクォート 2 つを入力することで 1 つのダブルクォートになります。

(例:「テスト”01”ユーザ」→”テスト””01””ユーザ”)

※それぞれの値には改行コードを含めないでください。

3.7.1. CSV ファイルダウンロード

登録ユーザ情報を CSV 形式でダウンロードします。フォーマットはユーザー一括登録時のフォーマットと同様になり、最大で 10000 件のユーザデータをダウンロード可能です。

(10000 件のダウンロード時にエラーが発生する場合は、以下の設定を変更し再度お試しください)

/etc/php.ini

```
max_execution_time = 60
```

3.8. バックアップ/リストア

PassLogic 認証サーバのユーザ情報および設定情報のバックアップ/リストアを行います。バックアップは定期的に行うことをお勧めします。

バックアップとリストアの PassLogic のバージョンを合わせる必要があります。異なるバージョン間のバックアップ・リストアはできません。

3.8.1. バックアップ

パスワード(リストアの際に必要です)を入力して送信ボタンをクリックしてください。バックアップファイルのダウンロードが開始されます。

3.8.2. リストア

バックアップファイルを選択して、バックアップの際に設定したパスワードを入力して、送信ボタンをクリックしてください。バックアップファイルのアップロードが開始されます。

※バックアップ/リストアの機能はユーザ数 1000 件程度を目安として下さい。1000 件を超える場合には、「バックアップの方法」をご参照ください。

3.9. 管理者パスワードの変更

現在ログインしている管理者(admin, operator)のパスワードを変更します。

3.10. ユーザサポートについて

3.10.1. ロックの解除方法（ユーザアカウントがロックされた場合のサポート）

ロック中のユーザは、ロック項目の背景が赤くなり文字列が「ロック解除」となります。ロック解除の文字をクリックすることでロックを解除することができます。この操作は「ユーザー一覧」「ロックユーザー一覧」「ユーザ検索」で実行できます。

3.10.2. パスワード再発行の方法（ユーザがパスワードを忘れた場合のサポート）

ユーザがパスワードを忘れた場合は運用管理者がパスワードを再発行します。パスワードを再発行したいユーザの「パスワード再発行」をクリックします。

ユーザ ID	パスワード再発行を行うユーザ ID が表示されます。
メールアドレス	再発行したパスワード位置情報をここで入力したメールアドレス宛に送信します。
PIN	ワンタイムパスワードと組み合わせる固定パスワードを入力します。必須項目ではありません。
初期パスワード位置情報（ワンタイムパスワード）	新規にパスワード位置情報を設定します。チェックボックスをチェックすることでランダムなものを自動で発行します。

設定が完了したら次へボタンを押し入力した値を確認する画面へ進みます。お間違いなければ登録ボタンを押します。パスワードの再設定が終わると、通知方法の選択画面に遷移します。

通知書をメール … 設定したメールアドレス宛に通知書をメール送信します。

通知書をプリントアウト … プリントアウト用の通知書が表示されます。

通知書の表示例

PassLogic利用開始のお知らせ

このメールはワンタイムパスワード認証 (PassLogic) を
使用して頂くためのパスワード位置情報通知メールです。

WebアクセスURL

<http://remote.example.com/menu/>

にアクセスして以下のログイン情報でログインしてください。

ユーザID: user01

PIN: Xs56a0W

※PIN下のパスワード位置情報の前に追加してください。

初期パスワード位置情報は

2**4 **** **
**** **** *5**
**** *3** *6**
**** **** *1**

です。

お問い合わせは
システム部 パスロジ太郎
00-0000-0000

© 2007-2010 Passlogy Co.,Ltd.

3.10.3. PassLogic からの通知メールが届かない場合のサポート

メール誤判定により迷惑メールフォルダに入る、メールフィルタリングによるメールの遮断により、登録通知メールが届かない場合があります。そのような場合には、「通知書のプリントアウト」を使い書面で通知するか、ユーザに対して登録通知メールを送信することを事前に通知しメールを受付ける準備をしてもらったうえで、改めて登録通知メールを送信してください。

3.11. ログ・リファレンス

ログ管理では、ユーザの認証ログ、管理者の操作ログ、認証ボックスの利用ログを収集しています。管理者はそれぞれのログを閲覧することができます。

3.11.1. ログフォーマット

基本ログ	PassLogic ログ
月 日 時間 IP アドレス	ログレベル ステータス コード コメント

3.11.2. ログ : ステータスリファレンス

code	loglevel	status	comment
21020093	info	OK	情報取得に成功しました。
21020094	alert	NG	ライセンスによるユーザ数の上限を越えています。
21020095	alert	NG	ライセンスによる認証ボックス数の上限を越えています。
21020097	alert	NG	ライセンスの有効期限が切れています。ライセンスを更新してください。
21020098	warning	NG	入力データが不正です。
21020099	emerg	NG	システムエラーです。
21020101	notice	OK	ユーザを新規作成しました。
21020111	warning	NG	すでにユーザが存在します。
21020112	warning	NG	入力データが不正です。
21020199	emerg	NG	システムエラーです。
21020201	notice	OK	ユーザを削除しました。
21020211	info	NG	ユーザが存在しません。
21020212	warning	NG	デバイスID設定があるため削除できません。
21020213	warning	NG	ユーザが存在するテナントのマネージャは削除できません。
21020214	warning	NG	テナントユーザは削除できません。
21020299	emerg	NG	システムエラーです
21020301	info	OK	情報取得に成功しました。
21020311	info	NG	ユーザが存在しません。
21020399	emerg	NG	システムエラーです。
21020401	info	OK	書き込みを完了しました。

21020411	warning	NG	ユーザが存在しません。
21020412	warning	NG	不正な設定です。
21020413	warning	NG	変更がありません。
21020499	emerg	NG	システムエラーです。
21020501	warning	OK	ロックしました。
21020502	info	OK	すでにロックされています。
21020511	warning	NG	ユーザが存在しません。
21020512	warning	NG	パラメータが正常ではありません。
21020599	emerg	NG	システムエラーです。
21020601	warning	OK	ロックを解除しました。
21020602	info	NG	ロックされていません。
21020611	warning	NG	ユーザが存在しません。
21020612	warning	NG	パラメータが正常ではありません。
21020699	emerg	NG	システムエラーです。
21020701	info	OK	情報取得に成功しました。
21020702	info	OK	ユーザが存在しません。
21020799	emerg	NG	システムエラーです。
21020801	info	OK	情報取得に成功しました。
21020802	info	OK	ユーザが存在しません。
21020899	emerg	NG	システムエラーです。
21021101	info	OK	パスワードをリセットしました。
21021111	warning	NG	ユーザが存在しません。
21021199	emerg	NG	システムエラーです。
21021201	info	OK	情報取得に成功しました。
21021211	warning	NG	ユーザが存在しません。
21021299	emerg	NG	システムエラーです。
21021301	info	OK	パスワードを変更しました。
21021311	warning	NG	ユーザが存在しません。
21021312	warning	NG	不正な設定です。
21021399	emerg	NG	システムエラーです。
21022101	notice	OK	デバイスIDを新規作成しました。
21022111	warning	NG	ユーザが存在しません。
21022112	warning	NG	不正な設定です。
21022113	warning	NG	すでにデバイスIDが多すぎて、新規作成できません。

21022114	warning	NG	すでに登録用キーが多すぎて、デバイスIDを新規作成できません。
21022115	warning	NG	すでにそのデバイスIDが存在します。
21022199	emerg	NG	システムエラーです。
21022201	notice	OK	デバイスIDを削除しました。
21022211	info	NG	すでにデバイスIDが存在しません。
21022212	warning	NG	ユーザが存在しません。
21022213	warning	NG	指定されたユーザは、指定されたデバイスIDを持っていません。
21022214	warning	NG	パラメータが正常ではありません。
21022299	emerg	NG	システムエラーです。
21022301	info	OK	情報取得に成功しました。
21022311	info	NG	デバイスIDが存在しません。
21022312	warning	NG	ユーザが存在しません。
21022313	warning	NG	指定されたユーザは、指定されたデバイスIDを持っていません。
21022314	warning	NG	不正な設定です。
21022399	emerg	NG	システムエラーです。
21022401	info	OK	書き込みを完了しました。
21022411	warning	NG	デバイスIDが存在しません。
21022412	warning	NG	ユーザが存在しません。
21022413	warning	NG	指定されたユーザは、指定されたデバイスIDを持っていません。
21022414	warning	NG	不正な設定です。
21022499	emerg	NG	システムエラーです。
21022501	info	OK	メールを送信しました。
21022511	warning	NG	デバイスIDが存在しません。
21022512	warning	NG	ユーザが存在しません。
21022513	info	NG	指定されたユーザは、指定されたデバイスIDを持っていません。
21022514	warning	NG	ユーザのメールアドレスが登録されていません。
21022515	warning	NG	指定されたデバイスは、すでに登録済みです。
21022599	warning	NG	メールが送信できませんでした。
21022601	info	OK	リセットに成功しました。
21022611	warning	NG	デバイスIDが存在しません。

21022612	warning	NG	すでに登録用キーが多すぎて、デバイスIDをリセット出来ません。
21022699	emerg	NG	システムエラーです。
21023101	info	OK	認証ボックスを新規作成しました。
21023111	warning	NG	すでに認証ボックスが存在します。
21023112	warning	NG	不正な設定です。
21023199	emerg	NG	システムエラーです。
21023201	info	OK	認証ボックスを削除しました。
21023211	info	NG	すでに認証ボックスが存在しません。
21023212	warning	NG	認証ボックスの削除に失敗しました。
21023299	emerg	NG	システムエラーです。
21023301	info	OK	情報取得に成功しました。
21023311	info	NG	認証ボックスが存在しません。
21023312	warning	NG	認証ボックスの情報取得に失敗しました。
21023399	emerg	NG	システムエラーです。
21023401	info	OK	書き込みを完了しました。
21023411	warning	NG	認証ボックスが存在しません。
21023412	warning	NG	不正な設定です。
21023413	warning	NG	認証ボックスの書き込みに失敗しました。
21023499	emerg	NG	システムエラーです。
21030098	warning	NG	ライセンスの有効期限が切れています。
21030099	warning	NG	入力データが不正です。
21030101	notice	OK	乱数生成
21030102	notice	NG	個体識別番号を登録してください。
21030103	notice	NG	初期登録の有効期限切れです。
21030111	warning	NG	認証ボックスが見つかりません。
21030112	warning	NG	アカウントがロックされているため乱数表を取得できませんでした。
21030113	warning	NG	ユーザ情報が不正です。
21030114	warning	NG	IP アドレスが正しくないため乱数表を取得できませんでした。
21030115	warning	NG	パスワード変更が必要です。
21030116	warning	NG	有効期限切れです。
21030117	warning	NG	パラメータが正常ではありません。
21030118	notice	OK	ダミー乱数表示

21030119	notice	NG	利用が許可されていません。
21030120	notice	NG	現在アクセス制限されています。
21030199	emerg	NG	システムエラーです。
21030201	info	OK	キャンセルしました。
21030211	warning	NG	認証ボックスが見つかりません。
21030213	warning	NG	ユーザ情報が不正です。
21030214	warning	NG	IP アドレスが不正です。
21030299	emerg	NG	システムエラーです。
21030601	info	OK	キャンセルしました。
21030611	warning	NG	認証ボックスが見つかりません。
21030613	warning	NG	ユーザ情報が不正です。
21030614	warning	NG	IP アドレスが不正です。
21030699	emerg	NG	システムエラーです。
21030301	notice	OK	パスワード変更が正常に推移しています。
21030302	info	OK	キャンセルしました。
21030303	notice	OK	パスワード変更が正常に終了しました。
21030311	warning	NG	セッション ID が違います。もう一度最初からお願いいたします。
21030312	warning	NG	パスワード位置情報に英数字以外の文字が含まれています。
21030313	warning	NG	パスワード位置情報の桁数を適切にしてください。
21030314	warning	NG	位置が特定できませんでした。ご確認のうえ、もう一度やりなおしてください。
21030315	warning	NG	パスワードが不正解です。
21030316	warning	NG	入力データが不正です。
21030317	warning	NG	過去に設定された位置への変更はできません。別の位置を設定してください。
21030318	warning	NG	ユーザ情報が不正です。
21030319	warning	NG	IP アドレスが不正です。
21030320	warning	NG	その位置は禁止されています。別の位置を設定してください。
21030321	warning	NG	パスワード位置情報の変更は許可されていません。
21030322	warning	NG	PIN に英字と数字を少なくとも 1 つ以上含める必要があります。

21030399	emerg	NG	システムエラーです。
21030401	info	OK	メニュー表示
21030412	info	NG	ロックされています。
21030413	warning	NG	ユーザ情報が不正です。
21030414	warning	NG	IP アドレスが不正です。
21030499	emerg	NG	システムエラーです。
21040098	warning	NG	ライセンスの有効期限が切れています。
21040099	warning	NG	入力データが不正です。
21040101	notice	OK	認証 OK
21040111	warning	NG	ユーザ名 または パスワードが違います。
21040112	warning	NG	ユーザは、このサービスを利用できるグループに含まれていません。
21040113	warning	NG	デバイスIDのレベルが、このサービスを利用できるレベルに達していません。
21040114	warning	NG	乱数表が有効期限切れです。
21040115	warning	NG	ユーザ名 または パスワードが違います。
21040117	warning	NG	設定された IP アドレス以外からの問い合わせ。
21040118	warning	NG	存在しない認証ボックス番号。
21040119	warning	NG	入力データが不正です。
21040199	emerg	NG	システムエラーです。
21050101	info	OK	PassLogic 設定を更新しました。
21050111	warning	NG	入力データが不正です。
21050102	info	OK	情報取得に成功しました。
21060101	notice	OK	RADIUS 認証に成功しました。
21060111	warning	NG	RADIUS 認証に失敗しました。
21060119	warning	NG	入力データが不正です。
21060199	emerg	NG	システムエラーです。
21070101	notice	OK	アクティベーションに成功しました。
21070102	info	OK	デバイスタイプ表示
21070111	warning	NG	正しいキーではありません。
21070112	warning	NG	携帯端末情報が受け取れませんでした。
21070113	warning	NG	携帯端末情報の書き込みに失敗しました。
21070114	warning	NG	端末制限用 Cookie が発行できませんでした。
21070115	warning	NG	不正なデバイスです。

3.11.3. ログのサイズ

*ログレベル notice(デフォルトの設定値)の場合の目安として、1 認証あたり 1k byte のログが出力されます。ログレベルは管理ツールの「ログ・その他設定」で変更することができます。

*ログの世代管理（容量や保存期間）については、Linux の logrotate の機能をご利用ください。

ログのディレクトリ

/var/log/passlogic/
