PassLogic Enterprise Edition

Ver.3.0.0

インストール・運用管理ガイド

PASSLOGY™

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

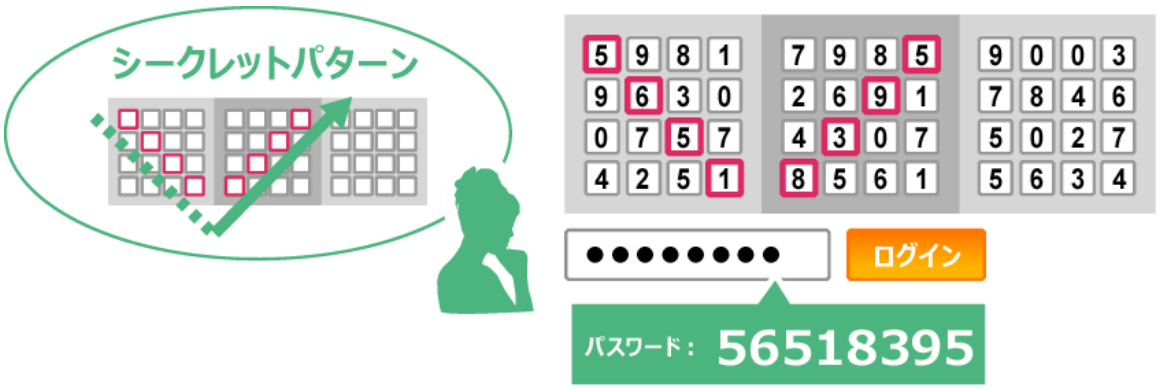
PassLogic およびパスロジは、パスロジ株式会社の登録商標です。
その他、本書に記載されている会社名、製品名は、それぞれ各社の商標または登録商標です。
本製品は医療機器、原子力施設、航空関連機器、軍備機器、輸送設備やその他人命に直接関わる施設や設備など、高い安全性が要求される用途での使用は意図されていません。該当する施設や設備には使用しないでください。

目次

PassLogic 認証方式とは？

PassLogic 認証方式は、ログイン時に表示される乱数表の“マス目の位置”と“選択する順番”をパスワード生成のルールとし、ログインの毎に正解パスワードを生成するセキュアな認証方式です。本方式のご説明はパスロジ社サイト上でも公開していますので、ユーザへの初期案内メール等でご活用ください。

URL： https://www.passlogy.com/pattern_staticpass



パスワード生成のルールを「**シークレットパターン**」と呼び、ユーザ自身が変更できます。また、ワンタイムパスワードに「**スタティックパスワード**（固定パスワード）」を組み合わせることも可能です。

「シークレットパターンにスタティックパスワードを付加する場合の変更方法」

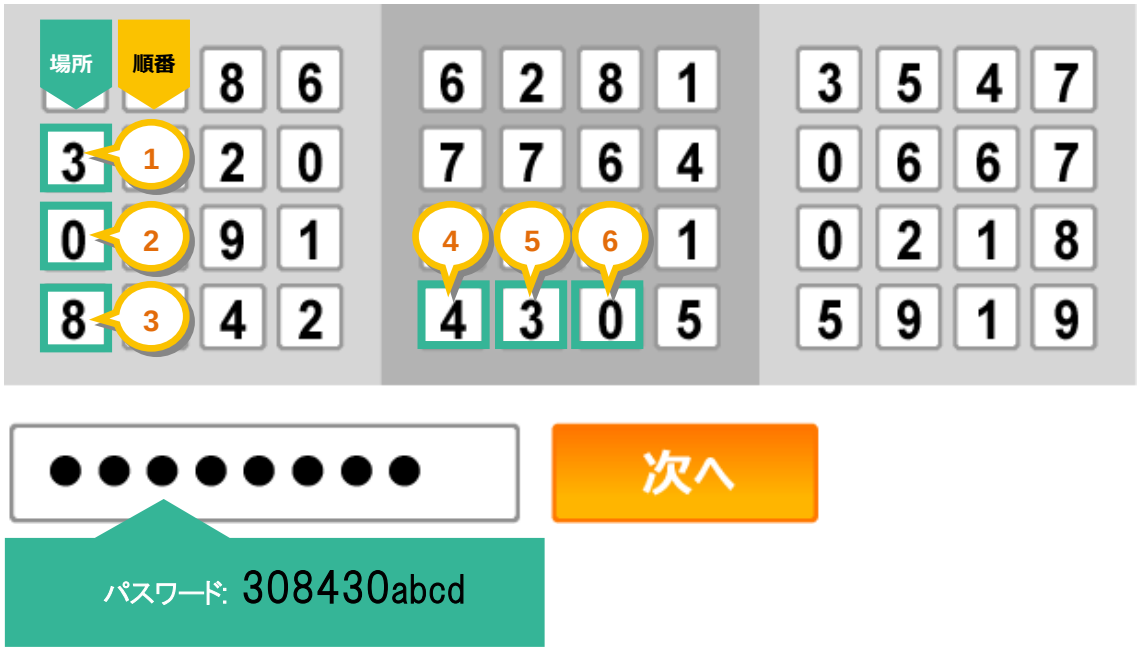
シークレットパターンとスタティックパスワードを変更します。
まず、任意のシークレットパターンとスタティックパスワードを決定してください。
*覚えやすさと独自性を考慮して、自由に決めてください。
*変更完了後は、変更したシークレットパターンとスタティックパスワードの組み合わせを使用して、ログインを行えるようになります。

≪シークレットパターンとスタティックパスワードの例≫
この例では、下記の位置と順番をシークレットパターンとして、下記の文字列をスタティックパスワードとして登録する場合を説明します。

■■■■ ■■■■ ■■■■
1■■■ ■■■■ ■■■■
2■■■ ■■■■ ■■■■
3■■■ 456■ ■■■■

スタティックパスワード:「abcd」

①決定したシークレットパターンに沿った場所と順番で、そのマス目に表示されている数字を入力します。
続けてスタティックパスワードとして設定したい文字列を入力し、「次へ」をクリックしてください。
*数字はキーボードから入力してください。乱数表のマス目はクリックできません。

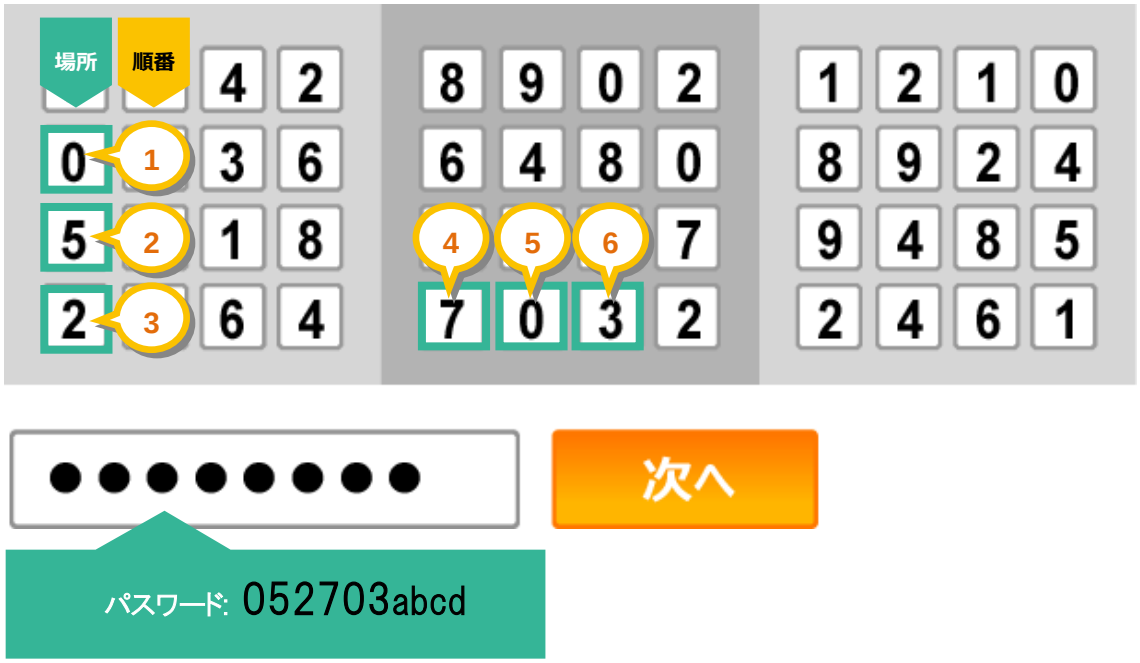


②「次へ」をクリックすると、乱数表が入れ替わります。①で入力したマス目と同じ場所と順番で、そのマス目に表示されている数字を入力してください。

続けてスタティックパスワードとして、①で入力した文字列を入力し、「次へ」をクリックしてください。

*乱数表が入れ替わっていますので、入力する数字は 1 回目と異なります。

*スタティックパスワードは、①で入力したものと同じ文字列を入力してください。

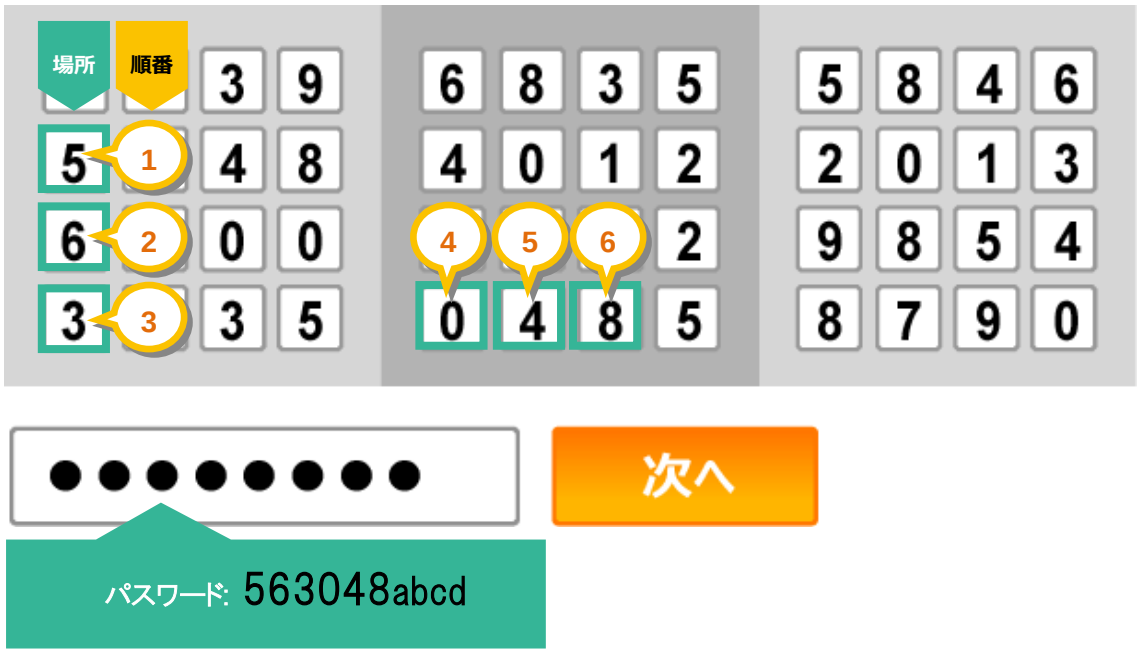


③再度、乱数表が入れ替わりますので、①および②で入力したマス目と同じ場所と順番で、そのマス目に表示されている数字を入力してください。

続けてスタティックパスワードとして、①で入力した文字列を入力し、「次へ」をクリックしてください。

*乱数表が入れ替わっていますので、入力する数字は 1 回目、2 回目と異なります。

*スタティックパスワードは、①および②で入力したものと同じ文字列を入力してください。



④3 回とも同じマス目の場所と順番で、表示された数字を、また同じ文字列を入力すると、シークレットパターンとスタティックパスワードが変更されます。

次回からは登録したシークレットパターンとスタティックパスワードの組み合わせでパスワードを入力し、ログインしてください。

1 インストールガイド

PassLogic を分離構成（ゲートウェイサーバと認証サーバに分離）で構築する場合 および 認証サーバをレプリケーション構成で構築する場合は、別冊の「PassLogic Enterprise Edition Ver.3.0.0 レプリケーションセットアップ＆リカバリガイド」をご覧ください。

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 6.1 以降 x86_64 または CentOS 6.1 以降 x86_64
httpd	Apache HTTP Server version:2.2.15 release:9.EL6 以降
php	version:5.3.3 release:3.EL6 以降

	Red Hat Enterprise Linux 7.1 以降 または CentOS 7.1 以降 x86_64
httpd	Apache HTTP Server version:2.4.6 release:31.EL7 以降
php	version:5.4.16 release:36.EL7_1 以降

＊上記以外のオペレーティング・システム、ディストリビューションの動作に関しましては、弊社サポートまでお問い合わせください。

＊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。

＊NSA Security-Enhanced Linux(SELinux)を有効にした環境での動作は保障されませんので OS インストール時に「無効」に設定してください。

＊CentOS も動作は確認させていただいておりますが、CentOS をご利用の場合には OS に起因する問題が発生した場合には Red Hat 社のサポートが受けられませんのであらかじめご了承の上ご利用ください。

1.2 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。

1.3 ウィルス対策ソフトを利用する場合

PassLogic 認証サーバの下記ディレクトリをスキャン対象から外してください。

/var/lib/php/session

1.4 推奨ブラウザ

PassLogic のユーザインターフェイスは、HTML5、CSS3、JavaScript で開発されています。またセッション情報の保持に Cookie を使用します。

	ブラウザ	文字コード
管理ツール	[PC] Internet Explorer11	UTF-8
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
ユーザインターフェイス	[PC] Internet Explorer9, 10, 11	
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
	[iPhone / iPad] Safari　(iOS7, 8, 9)	
	[Android] 標準ブラウザ　(Android4, 5, 6)	

＊ Edge ブラウザでは信頼できない証明書が設定されている https サイトへの SSO が正常動作しません。

＊ Internet Explorer の「互換表示」機能は、サポート対象外です。

1.5 使用ポート

ユーザインターフェイス	443	tcp	https
管理ツール	8443	tcp	https
RADIUS	1812	udp	radius
データベース	5439 9915 9925	tcp	postgresql pgpool pgpool

*iptables や firewalld など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ポートにアクセスできるように設定してください。

1.6 必要なパッケージ

下記は PassLogic サーバソフトウェアを動作させるのに必要なパッケージソフトのインストールコマンドです。

```
(root 権限で実行)
# yum -y install sed
# yum -y install sudo
# yum -y install gnupg2
# yum -y install rpm
# yum -y install perl
# yum -y install openssl
# yum -y install openssh-clients
# yum -y install tmpwatch
# yum -y install httpd
# yum -y install mod_ssl
# yum -y install ntp                (RHEL6/CentOS 6 のみ)
# yum -y install chrony             (RHEL7/CentOS 7 のみ)
# yum -y install zip
# yum -y install unzip
# yum -y install crontabs
# yum -y install postfix
# yum -y install php
# yum -y install php-gd
# yum -y install php-ldap
# yum -y install php-pgsql
# yum -y install php-mbstring       (RHEL6/7 は Optional リポジトリ有効化が必要)
# yum -y install php-process        (RHEL6/7 は Optional リポジトリ有効化が必要)
# yum -y install php-pecl-apc       (RHEL6/CentOS 6 のみ)
# yum -y install net-snmp-utils
# yum -y install curl
# yum -y install libtool-ltdl
# yum -y install libxslt
# yum -y install rsync
# yum -y install mailx
# yum -y install apr-util-pgsql     (RHEL6/7 は Optional リポジトリ有効化が必要)
# yum -y install xmlsec1
# yum -y install xmlsec1-openssl
```

```
# yum -y install freeradius
# yum -y install net-tools                    (RHEL7/CentOS 7 のみ)
# yum -y install tncfhh-libs                  (RHEL7/CentOS 7 のみ)
```

＊Red Hat Enterprise Linux に php-mbstring, php-process, apr-util-pgsql を、yum インストールする場合は、RedHat Network の SoftwareChannels で Optional リポジトリを有効にする必要があります。

Optional リポジトリを有効化するコマンド

```
(RHEL6) # subscription-manager repos --enable=rhel-6-server-optional-rpms
(RHEL7) # subscription-manager repos --enable=rhel-7-server-optional-rpms
```

1.7 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-ent-x.x.x-el6.tar.gz /usr/local/src/ (RHEL/CentOS 6 の場合)
# cp /cdrom/PassLogic-ent-x.x.x-el7.tar.gz /usr/local/src/ (RHEL/CentOS 7 の場合)
# cd /usr/local/src/
# tar zxvf PassLogic-ent-x.x.x.tar.gz
# cd passlogic-ent-x.x.x/
# ./install.sh install
```

＊「その他のユーザ」にアクセス権限が付与されたディレクトリにインストーラを展開してください。

＊install.sh と同じディレクトリに インストールログ install.log が出力されます。

インストール時に、以下の設定が自動で追加・変更されます。

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
LoadModule filter_module modules/mod_filter.so	コメントアウトを解除して有効化 (RHEL/CentOS 6 の場合)
#AddDefaultCharset	コメントアウトして設定値を無効化
ServerSignature	Off
TraceEnable	Off

/etc/php.ini

post_max_size	128M
upload_max_filesize	128M
memory_limit	256M
session.cookie_secure	1
expose_php	Off
error_reporting	E_ALL & ~E_NOTICE (RHEL/CentOS6) E_ALL & ~E_NOTICE & ~E_STRICT & ~E_DEPRECATED (RHEL/CentOS7)
session.cookie_httponly	On
short_open_tag	On

/etc/sudoers （RHEL6/CentOS6 の場合）

apache ALL=NOPASSWD: /sbin/service httpd status apache ALL=NOPASSWD: /sbin/service postfix status apache ALL=NOPASSWD: /sbin/service radiusd status apache ALL=NOPASSWD: /sbin/service ntpd status apache ALL=NOPASSWD: /opt/passlogic/apps/tools/httpd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/radiusd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/restore.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_info.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_recovery.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/deliver_cert passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/recovery_tar.sh	追加
#Defaults　　requiretty	無効化

/etc/sudoers （RHEL7/CentOS7 の場合）

apache ALL=NOPASSWD: /bin/systemctl status httpd apache ALL=NOPASSWD: /bin/systemctl status postfix apache ALL=NOPASSWD: /bin/systemctl status radiusd apache ALL=NOPASSWD: /bin/systemctl status chronyd apache ALL=NOPASSWD: /opt/passlogic/apps/tools/httpd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/radiusd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/restore.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_info.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_recovery.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/deliver_cert passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/recovery_tar.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgpool-start.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgpool-stop.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgsql-start.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgsql-stop.sh Cmnd_Alias PASSLOGIC_SERVICE = /bin/systemctl * passlogic-pgpool, /bin/systemctl * passlogic-pgsql, /bin/systemctl * radiusd, /bin/systemctl * httpd passlogic ALL=NOPASSWD: PASSLOGIC_SERVICE	追加
#Defaults　　requiretty	無効化

*PassLogic 管理ツールから、各種設定変更を行うために上記の設定が必要です。

/etc/systemd/logind.conf （RHEL7/CentOS7 の場合）

RemoveIPC=no	追加

*logind の IPC オブジェクト削除機能を無効化します。

/etc/ssh/ssh_config

StrictHostKeyChecking no	追加

*PassLogic サーバ間での ssh 接続確認を無効化します。

chkconfig / systemctl コマンドによる自動起動

httpd
ntpd （RHEL6/CentOS6 のみ）
chronyd （RHEL7/CentOS7 のみ）
crond
postfix
passlogic-pgsql
passlogic-pgpool
radiusd

1.8 Apache 推奨設定

Web サーバ脆弱性対策のために、Apache のデフォルト設定を下記のとおり変更することを推奨します。

ディレクトリ リスティング機能 無効化
/etc/httpd/conf/httpd.conf
（変更前） Options Indexes FollowSymLinks
（RHEL6 変更後） Options -Indexes FollowSymLinks
（RHEL7 変更後） Options FollowSymLinks
TRACE メソッド 無効化
/etc/httpd/conf/httpd.conf
（追記） TraceEnable Off
不要なディレクトリを削除
/var/www/icons/ (RHEL6 のみ)
/var/www/error/ (RHEL6 のみ)
/var/www/cgi-bin/
SSL version 3 を無効化
/etc/httpd/conf.d/ssl.conf
（変更前） SSLProtocol all -SSLv2
（変更後） SSLProtocol all -SSLv2 -SSLv3
不要な設定ファイルをリネーム (RHEL7 のみ)
ディレクトリリスティングを無効化
（変更前）/etc/httpd/conf.d/autoindex.conf
（変更後）/etc/httpd/conf.d/autoindex.conf.org
mod_userdir 設定を無効化
（変更前）/etc/httpd/conf.d/userdir.conf
（変更後）/etc/httpd/conf.d/userdir.conf.org
Apache デフォルトトップページ設定を無効化
（変更前）/etc/httpd/conf.d/welcome.conf
（変更後）/etc/httpd/conf.d/welcome.conf.org

*設定変更後に Apache の再起動が必要です。

1.9 管理ツールにアクセスする

次のコマンドで、初期の管理者(ユーザ ID: admin)を作成します。

```
(root 権限で実行)
# /opt/passlogic/apps/tools/modify_admin_passwd.php
-------------------------------------------
(コマンド実行結果例)
modified admin password: 3nEG0uUY  ← ユーザ ID: admin の初期パスワード
```

*上記コマンド実行結果例の“3nEG0uUY”の部分は、コマンド実行の度に変わります。この部分が管理者(ユーザ ID: admin)の初期パスワードです。

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://[PassLogic 認証サーバのホスト名]:8443/passlogic-admin/
```

*iptables 等のファイアウォールを起動している場合は、8443 番ポートでアクセスできるよう設定を行ってください。

管理ツールのユーザ ID 入力欄に“admin”と入力し次ページに進み、パスワード入力欄に上記で生成した初期パスワードを入力します(乱数表からワンタイムパスワードを生成する必要はありません)。

*初期の管理者ユーザ admin は削除できません。

1.10 ライセンスを登録する

ライセンスファイル(license-ent.asc)を登録します。管理ツール左側メニュー > メンテナンス > ライセンス管理 で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。

*インストール直後のライセンスファイル未登録状態ではユーザ数の上限は 1 ユーザです。

*ライセンス登録操作にて各種サービスが停止することはありません。

*ゲートウェイサーバと認証サーバが分離構成の場合は、認証サーバのみライセンスを登録してください。

*レプリケーション構成の場合は、全ての認証サーバにライセンスを登録してください。

*ライセンスファイルは編集しないでください。

1.11 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。エンタープライズエディション以外のエディションからのアップデートはサポートされません。

*アップデート実行前に管理ツールよりバックアップを行い、ユーザやロードバランサ等の httpd リクエストが到達しないようにした状態でアップデートを行ってください。

*スケジューリングした自動実行タスクが動作しない時間帯にアップデートを実行してください。

```
（root 権限で実行）
# cp PassLogic-ent-x.x.x.tar.gz /usr/local/src/
# tar zxvf PassLogic-ent-x.x.x.tar.gz
# cd passlogic-ent-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 httpd が再起動されます。

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-ent-x.x.x/ （x.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-ent-y.y.y/ （y.y.y はアップデート前のバージョン）
# ./install.sh install
# /opt/passlogic/apps/tools/modify_admin_passwd.php
（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）
```

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 httpd が再起動されます。

バージョン 1.2.3 以前からのアップデート注意点

◆パスワードリマインダー機能に関する下記の設定を登録してください。

＊管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞ Default Policy 編集 ＞ パスワードリマインダーの利用を許可

＊管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞ Default Policy 編集 ＞ パスワードリマインダー送信メール

メールテンプレート(設定参考値)

```
【件名】
PassLogic パスワード再発行
【本文】
以下の URL をクリックすると、パスワードが再発行されます。
https://remote.example.com/ui/resetter.php?key=<%REMINDER_URLKEY%>

＊この URL の有効期限はメール配信の 24 時間後までです。
有効期限切れの場合は、お手数ですが、以下の URL よりパスワード再発行の手続きを再度行ってください。
https://remote.example.com/ui/reminder.php

＊パスワード再発行のメールを複数受信した場合は、最新のメールに記載されている URL をご利用ください。
```

＊管理ツール左側メニュー ＞ 設定 ＞ UI 設定 ＞ 編集 ＞ 下記の文言設定

```
【ja】
Request to reset pattern:
  シークレットパターン再発行
Navigation to reset pattern:
  ユーザ名と登録されているメールアドレスを入力して[次へ]をクリックしてください。<br>シークレットパターン再発行のメールを送信します。
Finished to send reset pattern mail:
  シークレットパターン再発行のメールを送信しました。<br>メールに記載されている URL をクリックしてください。
Failed to send reset pattern mail:
  エラーが発生したため、シークレットパターン再発行のメールを送信することができませんでした。
Title of reset pattern:
  シークレットパターン再発行
Finished to reset pattern:
  新しいシークレットパターンをメールで送信しました。<br>メールに記載されている内容をご確認ください。
Expiration of reset pattern URL:
  シークレットパターン再発行のメールでご案内した URL の有効期限が切れています。<br>お手数ですが、もう一度再発行の手続きをしてください。
Failed to reset pattern:
  エラーが発生したためシークレットパターンを再発行することができませんでした。

【en】
Request to reset pattern:
  Reset your secret pattern
Navigation to reset pattern:
  Enter your username and registered e-mail address, and click the [next].<br>Then instructions to reset your secret pattern is sent to you.
Finished to send reset pattern mail:
  An e-mail has been sent to you.<br>Please follow the instructions in the email.
Failed to send reset pattern mail:
  Error occurred. E-mail was not able to be sent.
Title of reset pattern:
  Reset your secret pattern
```

```
Finished to reset pattern:
   A new secret pattern was sent by e-mail.<br>Please check it.
Expiration of reset pattern URL:
   Reset secret pattern URL has expired.<br>Please request reset pattern mail again.
Failed to reset pattern:
   Error occurred. Secret pattern was not able to be reset.
```

◆ユーザインターフェイス メニュー画面に連携リンクを非表示にする方法関して、本マニュアルの下記を参照してください。

・「SSL-VPN > シングルサインオン」の項【項目解説】「No.」

・「WebAPP > WebAPP」の項【項目解説】「No.」

・「Cloud > SP 登録」の項【項目解説】「No.」

＊バージョンアップ前の各 No.が「0」に設定されている場合はアップデート後にメニュー画面に連携リンクが表示されなくなりますのでご注意ください。

◆管理者 admin のパスワードを忘れた場合のリセット手順が変わります。本マニュアルの「管理ツールにアクセスする」の項を参照して admin のパスワードを再作成してください。

バージョン 1.3.0 以前からのアップデート注意点

◆PassLogic をバージョンアップする前に下記の rpm パッケージをインストールしてください。

php-gd

apr-util-pgsql

◆settings.conf に追加された設定値を登録してください。

＊詳細は本マニュアルの「2.6 settings.conf 設定」の項を参照してください。

◆管理ツールのメニューが下記の通り変更となります。

（変更前）設定 > PassLogic 設定

（変更後）設定 > ポリシー設定

＊バージョンアップ前の 設定 > PassLogic 設定 と同じ画面を表示させるには、設定 > ポリシー設定 > Default Policy 編集リンク をクリックしてください。

◆PassClip 認証と SSL-VPN シングルサインオン, WebSSO に関する下記の設定を登録してください。

＊管理ツール左側メニュー > 設定 > ポリシー設定 > (PassClip 認証用ポリシー) 編集 > 新規ユーザ送信メール

メールテンプレート(設定参考値)

```
【件名】
PassLogic 利用開始のお知らせ
【本文】
<%UNAME%> 様

●●システムのログイン用アカウントをお知らせします。
＊本メールには重要な内容が含まれておりますので大切に保管して下さい。

■スマートフォンセットアップ
1)PassClip アプリをインストールしてください。
・iOS 版 PassClip L
```

https://itunes.apple.com/jp/app/id1167322433?mt=8
・Android 版 PassClip L
https://play.google.com/store/apps/details?id=com.passlogy.passclip.local
2)下記の PassClip アクティベート URL にアクセスしてください。
<%PASSCLIP_URL%>
3)PassClip アプリに「PassLogic」スロットが追加されたことを確認してください。

■PassLogic ログインページの URL
https://[PassLogic サーバ FQDN]/ui/
最初にログインした端末のブラウザがシステムに登録され、
以降別の端末ではログインができなくなります。
ログインしたい端末のブラウザで最初のログインを行ってください。

■ログイン情報
ユーザ ID: <%UID%>
ドメイン: <%DOMAIN%>

■ログイン手順
1)Web ブラウザでログインページの URL へアクセスしてください。
2)ユーザ ID を入力し[次へ]をクリックしてください。
3)PassClip アプリの「PassLogic」スロットから取得した
ワンタイムパスワードを入力して[ログイン]をクリックしてください。

■アカウントがロックされた場合
ロックアウト後、●●分間経過すると自動でロックが解除されます。

--
【PassLogic の利用に関するお問い合わせ先】
[御社名　部署名　担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

＊管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞（PassClip 認証用ポリシー）編集 ＞ PassClip 再セットアップ送信メール

メールテンプレート（設定参考値）

【件名】
PassLogic PassClip アプリ初期化のご案内
【本文】
●●システムのログイン時の PassClip アプリを下記の手順で再設定してください。
＊本メールには重要な内容が含まれておりますので大切に保管して下さい。

■スマートフォンセットアップ
1)PassClip アプリをインストールしてください。
＊インストール済みの場合は再インストールする必要はありません。
・iOS 版 PassClip L
https://itunes.apple.com/jp/app/id1167322433?mt=8
・Android 版 PassClip L
https://play.google.com/store/apps/details?id=com.passlogy.passclip.local
2)下記の PassClip アクティベート URL にアクセスしてください。
<%PASSCLIP_URL%>
3)PassClip アプリに「PassLogic」スロットが追加されたことを確認してください。

■PassLogic ログインページの URL
https://[PassLogic サーバ FQDN]/ui/

■ログイン情報
ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%>

■ログイン手順
1)Web ブラウザでログインページの URL へアクセスしてください。
2)ユーザ ID を入力し[次へ]をクリックしてください。
3)PassClip アプリの「PassLogic」スロットから取得した
ワンタイムパスワードを入力して[ログイン]をクリックしてください。

■アカウントがロックされた場合
ロックアウト後、●●分間経過すると自動でロックが解除されます。

【PassLogic の利用に関するお問い合わせ先】
[御社名　部署名　担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

*管理ツール左側メニュー ＞ 設定 ＞ UI 設定 ＞ 編集 ＞ 下記の文言設定

【ja】
PassClip Password Required:
PassClip アプリを起動して、PassLogic のグリッド表を表示します。各自で設定したパターンにしたがって、8 ケタの数字を入力してください。
PassClip Activate Required:
PassClip アプリの設定をしてください。
PassClip Activate Title:
PassCilp アプリ PassLogic スロット追加
PassClip Activate Message1:
PassClip アプリをインストールしたスマートフォンで
下記の QR コードを読み取ってください。
PassClip Activate Message2:
PassClip パスワードを検証します。
PassClip に追加された PassLogic スロットより
パスワードを生成して入力してください。
PassClip Activate Completed:
PassClip アプリの設定が完了しました。
Waiting message for connecting to server:
ただいまログイン中です。
そのまましばらくお待ちください。

【en】
PassClip Password Required:
Please start up PassClip app on your phone and show the grid for PassLogic. Enter 8 digit numbers according to your own secret pattern.
PassClip Activate Required:
Set your PassCilp app.
PassClip Activate Title:
Add PassLogic slot on PassClip app
PassClip Activate Message1:
Please scan the following QR code after installing PassClip app on your phone.
PassClip Activate Message2:
Enter the password generated by PassLogic slot on your PassClip app to verify the code.
PassClip Activate Completed:
PassClip setting has been completed.
Waiting message for connecting to server:
Connecting to Server now, Please Wait.

◆バージョン 2.0.0 から下記の画面仕様が変更されます。

*ユーザインターフェイスと管理ツールの背景色が白から薄いグレーに変更

*PassLogic 製品ロゴが変更

バージョン 2.0.0 からのアップデート注意点

◆PassLogic をバージョンアップ後に/opt/passlogic/data/conf/settings.conf の MAIL_CC、MAIL_BCC の行を削除してください。

バージョン 2.1.0 からのアップデート注意点

◆LDAP ID 同期の同期モード「追加・更新・無効化」が廃止され、「追加・更新・削除」モードに置き換わります。自動的に PassLogic ユーザを削除しない場合は、同期モードを「追加・更新」に変更して下さい。

バージョン 2.2.1 以前からのアップデート注意点

◆settings.conf に追加された設定値を登録してください。
*詳細は本マニュアルの「2.6 settings.conf 設定」の項を参照してください。

◆端末固定時のクッキー値に「固定」が追加されました。バージョン 2.2.1 以前のクッキー値は「変動」の設定にて動いています。設定の変更が必要な場合、設定 > ポリシー設定 > 編集 > 端末固定から変更をして下さい。

◆「パラメータ設定機能の利用」機能に関する下記の設定を登録してください。

*管理ツール左側メニュー > 設定 > UI 設定 > 編集 > 下記の文言設定

```
【ja】
Back：
  戻る
Register：
  登録
Change passparam：
  設定
Setpass Form：
  パラメータを入力してください。
Setpass Confirm：
  下記内容でパラメータ登録します。
Setting Completed：
  設定が完了しました。

【en】
Back：
  Back
Register：
  Register
Change passparam：
  Config
Setpass Form：
  Please set the parameters.
Setpass Confirm：
  Parameter registration in the following contents.
Setting Completed：
  Setting has been completed.
```

◆「AD 設定」「LDAP 同期」の設定は「ドメイン管理」に集約されます。旧バージョンの「LDAP 同期」の設定は強制的に localドメインの LDAP ID 同期の設定として扱われ、バインドパスワードが引き継がれません。アップデート後、管理ツール左側メニュー ＞ ドメイン管理 の画面より、localドメインの行の「編集」をクリックし、バインドパスワードを再登録してください。

◆ユーザー括登録をコマンドライン上で行う場合の引数が、以下のように変更になりました。

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

バージョン 2.3.2 以前からのアップデート注意点

◆settings.conf に追加された設定値を登録してください。

＊詳細は本マニュアルの「2.6 settings.conf 設定」の項を参照してください。

◆「前回ログイン日時表示」「アカウント有効期限表示」「パスワード有効期限表示」に関する下記の設定を登録してください。

＊管理ツール左側メニュー ＞ 設定 ＞ UI 設定 ＞ 編集 ＞ 下記の文言設定

```
【ja】
Account expiration:
  アカウント有効期限
Password expiration:
  パスワード有効期限
Last login:
  前回ログイン日時
Day:
  日
Indefinite:
  無期限

【en】
Account expiration:
  Account expiration
Password expiration:
  Password expiration
Last login:
  Last login
Day:
  day(s)
Indefinite:
  Indefinite.
```

◆Cloud ＞ SP 登録 の管理項目が増え、SAML レスポンスの XML フォーマットが更新されました。バージョンアップ後は事前に連携検証を行ってください。

＊ SAML レスポンスにて、Audience 関連のエラーになる場合は、追加された項目 Audience に RelayStateURL と同じ値を設定してください。

◆バージョン 2.3.2 以前 と バージョン 2.4.0 では下記の文言設定に差異がありますが、バージョンアップではこれらの文言は自動的に更新されません。

*管理ツール左側メニュー ＞ 設定 ＞ UI 設定 ＞ 編集

【ja】
Instruction1：
2.3.2 以前：ユーザー名を入力してください。
2.4.0 以降：ユーザ ID を入力してください。
Username：
2.3.2 以前：ユーザー名
2.4.0 以降：ユーザ ID
Change password required：
2.3.2 以前：パスワード変更が必要なユーザです。
2.4.0 以降：パスワード変更が必要です。
Change password message1：
2.3.2 以前：STEP.1 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 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。
2.4.0 以降：<script type="text/javascript">$(function(){ $("#detail").css("display", "none");
$("#detail_disp").click(function(){ $("#detail").toggle(); }); });</script>
<style type="text/css">.PLHelpPasschg {background-color:#fff; padding:1em;
margin-bottom:1em;}</style>

■パスワード変更：入力 1/3 回目
【ヘルプ：手順を表示】

※この説明の表記はサンプルです。必ず設定したポリシー条件に合わせて変更してください！（管理ツール ＞ 設定 ＞ UI 設定 ＞ Change password message1）
【はじめに】当システムのパスワード変更手順を説明します。
はじめてご利用になる方は、認証方式と用語の説明（別ページが開きます）をご参照ください。
<hr>
【STEP1】下記の条件を満たす「シークレットパターン」と「スタティックパスワード（任意の文字列）」を決めてください。

シークレットパターンの設定条件

・6～12 マス分を選択
・左、中央、右の各 16 マス（4×4）のブロックから、最低 1 マスずつ選択
・一筆書き（すべてのマスがつながっている）のパターンは禁止

スタティックパスワードの設定条件

・6～12 桁
・半角英数（大文字小文字を区別）
・記号(_ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < >)

【STEP2】STEP1 で決めたシークレットパターンに沿ってマス内の数字をパスワード欄に入力し、つづけてスタティックパスワードを入力してください。その後、「次へ」を押してください。

Change password message2：
2.3.2 以前：STEP.1 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 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。

2.4.0 以降:■パスワード変更:入力 2/3 回目
マス内の数字が変わりました。
もう一度、あなたが設定したいシークレットパターンに沿ってマス内の数字を入力し、つづけてスタティックパスワードを入力してください。
入力後、「次へ」を押してください。

Change password message3:
2.3.2 以前:STEP.1 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 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。
2.4.0 以降:■パスワード変更:入力 3/3 回目
再度マス内の数字が変わりました。
1 回目、2 回目の入力と同じように、もう一度、あなたが設定したいシークレットパターンに沿ってマス内の数字を入力し、つづけてスタティックパスワードを入力してください。
入力後、「次へ」を押してください。

Navigation to reset pattern:
2.3.2 以前:ユーザ名と登録されているメールアドレスを入力して[次へ]をクリックしてください。
シークレットパターン再発行のメールを送信します。
2.4.0 以降:ユーザ ID と登録されているメールアドレスを入力して[次へ]をクリックしてください。
シークレットパターン再発行のメールを送信します。

【en】
Instruction1:
2.3.2 以前:Enter your username.
2.4.0 以降:Enter your user ID.
Username:
2.3.2 以前:Username
2.4.0 以降:User ID
Change password message1:
2.3.2 以前:STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.
2.4.0 以降:<script type="text/javascript">$(function(){ $("#detail").css("display", "none");
$("#detail_disp").click(function(){ $("#detail").toggle(); }); });</script>
<style type="text/css">.PLHelpPasschg {background-color:#fff; padding:1em;
margin-bottom:1em;}</style>

[First Input (1/3)]
*Input three times to complete.
Show procedure

*This description is a SAMPLE. Please change to match the policy conditions! (Management Tool > Config > UI Settings > Change password message1)
Introduction:The following section describes the password change procedure of this system.
For first time user, please refer to this link about authentication method and terminology.

STEP1:Make your unique Secret Pattern and Static Password according to the following terms.
<hr>
Regulations on Secret Pattern

-Choose positions from 6 to 12.
-Choose at least one grid from each left, center and right 4 by 4 grid blocks.
-You cannot make a Secret Pattern with a single stroke.

Regulations on Static Password

-Use 6-12 degits.
-Alphanumeric (Uppercase and lowercase are used interchangably.)
-The following symbols are usable.(_ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < >)

STEP2:Enter numbers according to your Secret Pattern made in the STEP1, and enter your Static Password following the numbers. Then press "Next."
*Please make sure that you do not lose your Secret Pattern and Static Password!

Change password message2:

2.3.2 以前:STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.

2.4.0 以降:[Second Input (2/3)]
Enter numbers according to your Secret Pattern. And enter your Static Password following the numbers.
(*Numbers in matrix are changing everytime.)
Then press "Next."

Change password message3:

2.3.2 以前:STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.

2.4.0 以降:[Second Input (3/3)]
Enter numbers according to your Secret Pattern. And enter your Static Password following the numbers.
(*Numbers in matrix is reformed.)
Then press "Next."

Navigation to reset pattern:

2.3.2 以前:Enter your username and registered e-mail address, and click the [next].
Then instructions to reset your secret pattern is sent to you.

2.4.0 以降:Enter your User ID and registered e-mail address, and click the [next].
Then instructions to reset your Secret Pattern is sent to you.

◆パスワード有効期限お知らせに関する以下の設定を登録してください。

*管理ツール左メニュー > 設定 > ポリシー設定 > (PassLogic 認証用ポリシー) 編集 > 有効期限送信メール

メールテンプレート(設定参考値)

```
【件名】
PassLogic パスワード有効期限のお知らせ
【本文】
<%UNAME%> 様

パスワードの有効期限についてお知らせします。

パスワード有効期限:<%EXPIRE_DATE%>

期限が切れる前にパスワードを再設定してください。

■ログインページの URL
https://[PassLogic サーバ FQDN]/ui/

【PassLogic の利用に関するお問い合わせ先】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]
```

バージョン 2.4.0 以前からのアップデート注意点

◆settings.conf に追加された設定値を登録してください。

*詳細は本マニュアルの「2.6 settings.conf 設定」の項を参照してください。

◆バージョン 2.4.0 以前 と バージョン 2.5.0 では下記の文言設定に差異がありますが、バージョンアップではこれらの文言は自動的に更新されません。

*管理ツール左側メニュー > 設定 > UI 設定 > 編集

```
【ja】
PassClip Password Required:
  2.4.0 以前:PassClip アプリを起動して、PassLogic のグリッド表を表示します。各自で設定したパターンにしたがって、8 ケタの数字を入力してください。
  2.5.0 以降:PassClip L アプリから取得したパスワードを入力してください。
PassClip Activate Required:
  2.4.0 以前:PassClip アプリの設定をしてください。
  2.5.0 以降:PassClip L アプリの設定をしてください。
PassClip Activate Title:
  2.4.0 以前:PassCilp アプリ PassLogic スロット追加
  2.5.0 以降:PassCilp L アプリ PassLogic スロット追加
PassClip Activate Message1:
  2.4.0 以前:PassClip アプリをインストールしたスマートフォンで<br>下記の QR コードを読み取ってください。
  2.5.0 以降:PassClip L アプリをインストールしたスマートフォンで<br>下記の QR コードを読み取ってください。
PassClip Activate Message2:
  2.4.0 以前:PassClip パスワードを検証します。<br>PassClip に追加された PassLogic スロットより<br>パスワードを生成して入力してください。
  2.5.0 以降:PassClip L パスワードを検証します。<br>PassClip L に追加された PassLogic スロットより<br>パスワードを生成して入力してください。
PassClip Activate Completed:
  2.4.0 以前:PassClip アプリの設定が完了しました。
```

2.5.0 以降:PassClip L アプリの設定が完了しました。

【en】
PassClip Password Required:
2.4.0 以前:Please start up PassClip app on your phone and show the grid for PassLogic. Enter 8 digit numbers according to your own secret pattern.
2.5.0 以降:Please input password generated by PassClip L app.
PassClip Activate Required:
2.4.0 以前:Set your PassCilp app.
2.5.0 以降:Set your PassClip L app.
PassClip Activate Title:
2.4.0 以前:Add PassLogic slot on PassClip app
2.5.0 以降:Add PassLogic slot on PassClip L app
PassClip Activate Message1:
2.4.0 以前:Please scan the following QR code after installing PassClip app on your phone.
2.5.0 以降:Please scan the following QR code after installing PassClip L app on your phone.
PassClip Activate Message2:
2.4.0 以前:Enter the password generated by PassLogic slot on your PassClip app to verify the code.
2.5.0 以降:Enter the password generated by PassLogic slot on your PassClip L app to verify the code.
PassClip Activate Completed:
2.4.0 以前:PassClip setting has been completed.
2.5.0 以降:PassClip L setting has been completed.

◆ユーザ画面に表示されるエラーメッセージの多言語化に伴い下記の設定を登録してください。

*管理ツール左側メニュー > 設定 > UI 設定 > 編集 > 下記の文言設定

【ja】
Logout message:
ログアウトしました。
Timeout message:
セッションがタイムアウトしました。再度ログインしてください。
Message for session unable:
セッションが有効ではありません。Cookie の利用を許可し、https 経由でアクセスしてください。
Message for password required:
パスワードを入力してください。
Entry key is not correct:
エントリーキーが正しくありません。
【en】
Logout message:
Logout
Timeout message:
The session was disconnected. Please login again.
Message for session unable:
Session is incorrect. Please enable Cookies on your browser or access via https.
Message for password required:
Password is Required.
Entry key is not correct:
Entry key is not correct.

◆アカウントロックに関する以下の設定を登録してください。

*管理ツール左メニュー > 設定 > ポリシー設定 > (PassLogic 認証用ポリシー) 編集 > アカウントロック通知メール

メールテンプレート(設定参考値)

```
【件名】
アカウントロック通知
【本文】
<%UNAME%>様

認証の連続失敗回数が規定値を超えたためアカウントをロックしました。
アカウントの解除につきましては、管理者までお問い合わせください。

【PassLogic の利用に関するお問い合わせ先】
[御社名　部署名　担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]
```

バージョン 2.5.0 以前からのアップデート注意点

◆メールサーバの「認証パスワード(SMTP-AUTH)」を登録している場合は、バージョン 3.0.0 以降へアップデートした後で、登録済みの認証パスワード欄をクリアして改めて正しいパスワードを登録してください。

*認証パスワードの内部管理方法が変わったことに伴い、バージョンアップ前の認証パスワードのままではパスワード不一致によりメール送信することができません。

*認証パスワードの変更は PassLogic 管理ツール > 設定 > ポリシー設定 > Default Policy 編集 で行ってください。

◆uid,ドメイン名,グループ名,ポリシー名,メールの SMTP サーバ、SSL-VPN 機器 IP アドレスに単一文字「0」を使用できなくなります。既存設定に「0」がある場合はアップデート前に変更してください。

◆PKI 機能追加に伴い下記の設定を登録してください。

*管理ツール左側メニュー > 設定 > UI 設定 > 編集 > 下記の文言設定

【ja】
Download:
　ダウンロード
Send E-mail:
　メール通知
Cert Password:
　証明書パスワード
Cert download center message:
　証明書をダウンロードします。
Title of auto generate client cert:
　証明書の自動発行
Generate client cert message:
　クライアント証明書を自動発行します。
よろしければ次へボタンを押してください。
Finished to Generate client cert message:
　以下のクライアント証明書を発行しました。
記載されている内容をご確認ください。
Success to send client cert mail:
　メールを送信しました。
Failed to send client cert mail:
　エラーが発生したため、証明書発行の通知のメールを送信することができませんでした。
【en】
Download:
　Download
Send E-mail:
　SendMail
Cert Password:
　Cert Password
Cert download center message:
　Download the Client Cert.
Title of auto generate client cert:
　Generate Client Certification.
Generate client cert message:
　Please push next bottom to generate Client Cert.
Finished to Generate client cert message:
　Client Certification is generated.
Please check it.
Success to send client cert mail:
　E-mail has been sent to you.
Failed to send client cert mail:
　Error occurred. E-mail was not able to be sent.

＊管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞(PassLogic 認証用ポリシー) 編集 ＞PKI 認証用クライアント証明書の発行メール

メールテンプレート(設定参考値)

```
【件名】
クライアント証明書の発行
【本文】
<%UNAME%> 様

PKI 認証用のクライアント証明書を発行しました。
ログインしたい端末で、以下の証明書ダウンロードの URL にアクセスし、クライアント証明書をダウンロード･登録をしてください。
登録が完了するとシステムにログインできるようになります。

■ダウンロードの URL
https://[PassLogic サーバ FQDN]/ui/?downloadkey=<%DOWNLOADKEY%>

■証明書パスワード:<%CERT_PASSWORD%>

■ログインページの URL
https://[PassLogic サーバ FQDN]/ui/

■ログイン情報
ユーザ ID: <%UID%>
ドメイン: <%DOMAIN%>
```

1.12 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-ent-x.x.x/
# ./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。)
```

＊アンインストール後 OS を再起動してください。

＊rpm パッケージは別途アンインストールしてください。

2 システム管理者ガイド

2.1 管理者アカウントを作成する

PassLogic 管理者アカウントには下記のいずれかの権限を付与できます。

権限の種類	すべての 管理機能	ユーザ作成･編集･削除･無効化 ユーザロック･端末固定	アンロック パスワード再発行
admin	○	○	○
useradmin	×	○	○
operator	×	×	○

【 登録手順 】

(ⅰ)管理ツール左側メニュー > 管理者 > 管理者作成 をクリック

(ⅱ)登録内容を入力･変更し [次へ] をクリック

(ⅲ)入力内容を確認し [登録] をクリック

【 項目解説 】

uid(必須)	利用可能文字:半角英数(大文字小文字を区別)、.(ピリオド)、-(ハイフン)、_(アンダースコア) 文字数:1-30 文字
権限(必須)	権限の種類を選択
メールアドレス	アカウント作成結果をメール通知する場合は必須･最大 255 文字
氏名	最大 255 文字
社員番号	最大 255 文字
部署	最大 255 文字
電話	最大 255 文字
シークレットパターン(ワンタイムパスワード)	シークレットパターンの初期値を指定 ↓通知例 初期パスワード位置情報は 1234 5678 9ABC DE** **** **** **** **** **** **** **** **** です。 *10 桁以上はアルファベット[A-Z]で、36 ケタ以上は[a-z]で表現します。 *「シークレットパターンをランダムに設定する」のチェックボックスを ONにするとシークレットパターンをランダム生成します。

スタティックパスワード	ワンタイムパスワードの後に付加するスタティックパスワードの初期値を指定 スタティックパスワードに使用できる文字種：半角英数（大文字小文字を区別）と以下の記号です。 _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < > *カンマとコロンは利用できません。 *必須項目ではありません。未指定の場合パスワードはシークレットパターンだけになります。
有効（必須）	アカウントの有効/無効を選択
有効期限	アカウントの有効期限日 *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ります。 *アカウントを削除したい場合は明示的に削除してください。 *アカウントの有効期限日を延長設定することができます。
備考	最大 255 文字

2.2 ポリシー設定

認証方式やパスワードの有効期限などのセキュリティポリシーのことを PassLogic では「ポリシー」と呼びます。ポリシーは複数管理することができ、1ユーザに1つのポリシーを適用することができます。

インストール直後は「Default Policy」のみ管理されています。Default Policy は追加するポリシーのテンプレート情報となります。

*管理者アカウントには Default Policy が適用され、他のポリシーに変更することはできません。

*ver.1.3.0 以前からアップデートした場合、アップデート前のポリシー情報は Default Policy に移行され、全てのユーザは Default Policy が適用されている状態です。

【 ポリシー追加手順 】

（ｉ）管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞ [追加] をクリック

（ii）ポリシー名（半角英数字、ハイフン、アンダースコア／先頭文字はアルファベットまたはアンダースコアのみ／30 文字以内）を入力して [次へ]をクリック

（iii）内容を確認し [登録] をクリック

（iv）戻る リンクをクリックし、追加したポリシー名の右側 編集 リンクをクリック

（ｖ）（Default Policy の内容が初期表示されます）ポリシー設定を編集し [次へ] をクリック

（vi）入力内容を確認し [決定] をクリック

【 項目解説 】

認証全般	
認証方式	PassLogic または PassClip のいずれかを選択します。 *Default Policy は PassLogic 認証しか選択できません。
ロック・アウトまでの連続失敗回数	連続で認証失敗した回数が設定値に達したユーザはロックされます。 *設定値 0 はロック・アウトされません。
ロック・アウト解除までの秒数	指定した秒数でロック・アウト状態が自動的に解除されます。 *[自動ロック解除しない]をチェック状態にすると設定した秒数経過後も自動ロック解除を行いません。
認証可能な時間帯	指定時間帯のみ認証することができます。時間外の時間帯では正しいパスワードを入力しても認証結果は NG になります。 *開始時刻よりも終了時刻の方が早い場合は、0 時をまたぐ設定になります。(例:開始時刻 18:00、終了時刻 06:00 の場合、18:00～翌 06:00 まで認証可能)
端末固定	認証可能な端末(ブラウザ)を固定する場合はチェックしてください。 またクッキー値について、下記の設定が可能です。必要に応じ設定してください。 ・固定:初回発行時の Cookie 値を永続利用(デフォルト) ・変動:ログインの都度 Cookie 値が更新される *1ユーザあたり最大5台まで登録できます。
PKI 認証機能	クライアント証明書による PKI 認証機能を利用する場合はチェックしてください。
自動発行機能	クライアント証明書を、『ユーザ作成時*1』『ユーザ初回ログイン時』のどちらかのタイミングで自動に発行する機能です。 発行される証明書は、識別名のフォーマットと有効期限を設定できます。 識別名フォーマット: ・uid_domain:uid と domain の間に_(アンダースコア)を挟んだ表記 ・uid_domain_random:上記表記の末尾に、_(アンダースコア)とランダム 8 文字(a-zA-Z1-9)をつけた表記 有効期限:自動発行されるクライアント証明書の有効期限 *1 LDAP 認証連携による『ユーザ作成時』の場合は証明書自動発行は作動しません。
AD パスワード保存	アカウントを AD で管理されているユーザが PassLogic へログインするときに入力した AD パスワードを PassLogic データベースに保管します。 *AD パスワードが保存されたユーザは、次回以後のログインで AD パスワードの入力を省略できます。

パラメータ設定機能の利用	ユーザにパラメータ変更を許可する場合はチェックを入れ、パラメータ名を入力してください。パラメータ変更の詳細は「5.1 ユーザのパラメータ設定」を参照してください。
前回ログイン日時表示	ユーザに前回ログイン日時を表示させる場合は、チェックを入れてください。初めてログインしたユーザには「No data」を表示します。
アカウント有効期限表示	ユーザに管理者が設定したアカウント有効期限を表示させる場合は、チェックを入れてください。有効期限のないユーザには(UI 設定 Indefinite 設定値)「無期限」を表示します。
認証セッション継続機能	ユーザがログアウトせずにブラウザを閉じた場合、継続時間内であれば再接続時にログインを省略する機能です。利用する場合はチェックを入れてください。(継続時間は、ログイン完了時からカウントされます)
アカウントロック通知メール	パスワード連続失敗回数に到達し、アカウントがロックされた際にメールを送る機能です。(管理者による手動のロックは含めません) 送信先に、送信しない、ロックされたユーザに登録されたメールアドレス、入力した特定のメールアドレスの 3 種類が選べます。
PassLogic 認証	
乱数表の有効時間 [*1]	PassLogic 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乱数表は無効化され正しいパスワードを入力しても認証されません。 有効時間を過ぎた場合は新たに乱数表を取得する必要があります。
再設定時の制限 [*1]	直近 n 回と同じシークレットパターンの設定を禁止します。
シークレットパターンの有効期限 [*2]	シークレットパターン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。
	シークレットパターンの有効期限が設定されている場合に、特定期間の間に期限切れとなるユーザに対してメールを送信します。 毎日決まった時間に送信する方法と、手動で送信する方法があり、日数の指定は有効期限以下の数値を指定する必要があります
パスワード有効期限表示	ユーザにパスワード有効期限の表示設定ができます。 YYYY/MM/DD:パスワード有効期限を年月日表示します。 CountDown:現在日時からパスワード有効期限を算出して残り使用期間を表示します。 有効期限のないユーザには(UI 設定 Indefinite 設定値)「無期限」を表示します。
初回パスワード変更を強制	初回利用時と管理者によるパスワード強制変更後にパスワードの変更をユーザに強制します。

パスワード変更機能の利用	ユーザに自身のパスワード変更を許可する場合はチェックを入れます。許可しない場合でも、初回パスワード変更を強制にしている場合やシークレットパターンの有効期限が切れた場合はパスワードを変更できます
パスワード変更時に現在のパスワードを確認する	ユーザがPassLogicログイン中に任意のパスワードを変更する前に、現在のパスワード確認を要求するか否かを設定します。
乱数表の縦横サイズ	PassLogic 乱数表の縦横サイズを設定します。
ワンタイムパスワードの長さ[*1]	ワンタイムパスワードの長さを指定します。 *0 以上 64 以下の範囲で最小／最大を設定してください。
ランダム発行時の長さ(ワンタイムパスワード)[*1]	シークレットパターンをランダム生成するときの長さを指定します。 0 を指定するとランダム生成でシークレットパターンは発行されません。 **二筆書きで発行する** ランダム発行時のシークレットパターンを二筆書きに簡略化します。 乱数表のサイズが 4×12 かつ、当項目が 8 以下のときのみ使用できます。
スタティックパスワードの長さ[*1]	スタティックパスワード(固定パスワード)の長さを指定します。 *0 以上 64 以下の範囲で最小／最大を設定してください。 *スタティックパスワードに使用できる文字は、半角英数と以下の記号です。 _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < > (カンマとコロンは利用できません)
ランダム発行時の長さ(スタティックパスワード)[*1]	スタティックパスワードをランダム生成するときの長さを指定します。 0 を指定するとランダム生成でスタティックパスワードは発行されません。 使用される文字列は数字の 0、 1、小文字の l(エル)、 大文字の I(アイ)、 O(オー)を除く半角英数字です。
シークレットパターン制約[*1]	安易なシークレットパターンの使用を制限します。 **一筆書き禁止** 始点から終点までが一筆書きできる、隣接した位置のみで構成されるシークレットパターンを禁止します。[*3] **全てのブロックから必ず 1 つ以上選択する** 4*4 の 3 ブロック全てから必ず 1 つ以上の位置を含むシークレットパターンを強制します。 **設定禁止シークレットパターン** 設定不可能なシークレットパターンを個別に設定します。 *部分一致ではなく 完全一致 です。

パスワードリマインダーの利用を許可	ユーザがパスワードを忘れてしまった時に、ユーザ自身でパスワードを再発行できる機能の使用可否を設定します。
Web Token の使用	Web Token を使用する際には有効にしてください。
乱数表のガイドを表示	乱数表の縦横の位置を示すガイド文字(縦Ⅰ～Ⅳ、横A～H)を表示するかどうかを設定します。
Windows Logon の使用	同梱されている PassLogic for Windows Desktop モジュールを使用して、Windows 端末にログオンする際は有効にしてください。 **認証方式** [PassLogic ONLY] 初回のみ PassLogic 認証と AD 認証を行い、それ以降は PassLogic 認証のみでログオンします。 [Hybrid] PassLogic 認証と AD 認証を毎回行いログオンします。 **パスワード有効期限切れ間近警告**（1～99） パスワード有効期限までの日数が設定値以下になったときに、端末にパスワード変更要求メッセージを表示します。 **パスワード有効期限切れ後許容回数**（1～999） パスワード有効期限切れ後にパスワード変更をしないまま認証できる回数です。この回数を過ぎるとパスワード変更するまで端末にログオンできなくなります。 **連続オフライン認証上限回数**（0～10000） 連続でオフライン認証できる上限回数です。オンラインで認証成功すると、またこの回数まで連続でオフライン認証ができるようになります。オフライン認証を許可しない場合は 0 を入力します。 **連続オフライン認証残数警告**（1～99） 連続でオフライン認証できる回数が設定値以下になったときに、端末に警告メッセージを表示します。 **オフライン認証連続失敗上限**（1～99） 連続でオフライン認証失敗した回数がこの値を超えた場合、オンライン認証に成功するまでログオンできなくなります。

＊1：管理者アカウントに適用されるポリシーです。

＊2：管理者アカウントはシークレットパターンの有効期限が切れた後も管理ツールにログインすることはできますが、ログイン後の画面上部に赤字で「[!]シークレットパターンの有効期限が切れています。」と表示され続けます。

＊3：隣接した位置とは、特定の位置を中心とした 8 方向(縦・横・斜め)です。本ガイド冒頭に紹介されているような V 字のシークレットパターンの使用を制限することができます。

管理者によるパスワード発行などの操作はポリシーで設定されている許容桁数などの制約を受けません。

PassClip 認証	
表示形式	PassClip 端末での表示形式を選択します。 「ベーシック表示」は横一列に並んだ数値で表示されます。 （例） 35091372 「ビンゴ型」は下記のように、縦横 5 列ずつに整列したマス内に数値で表示されます。ユーザが PassClip で設定した「パターン」に沿って数字を抜き出します。 （例） 
タイムステップ(秒)	ワンタイムパスワードの有効期間を設定します。 1 以上 3600 以下で設定してください。 ＊ PassLogic 認証サーバは、現在のパスワードに加えて、1つ前のパスワードと1つ後のパスワードを許容します。 ＊ パスワードの生成には UNIX タイムスタンプを使用しますので、タイムゾーンによる影響を受けません。
桁数	ワンタイムパスワードの桁数を設定します。 1 以上 8 以下で設定してください。

2.3 ユーザ通知設定

利用者に送信するメールのテンプレートをポリシーごとに設定します。

【 設定手順 】

(ｉ)管理ツール左側メニュー ＞ ポリシー設定をクリック

(ii)設定するポリシー名の右側 編集 リンクをクリック

(iii)ポリシー設定項目 下部の ユーザ通知設定欄 を編集し［次へ］をクリック

(iv)入力内容を確認し［決定］をクリック

PassLogic から送信されるユーザ通知の送信元、Cc、Bcc のメールアドレスを指定できます。

送信元メールアドレス	送信元メールアドレスを1つのみ指定できます。
Cc	利用者以外の宛先を指定します。受信者全員に、宛先に含まれていることを明示できます。 *カンマ区切りで複数指定できます。
Bcc	利用者以外の宛先を指定します。受信者全員に、宛先に含まれていることを明示しません。 *カンマ区切りで複数指定できます。

認証方式ごとに以下の通知テンプレートが用意されています。

①	PassLogic 認証用 新規ユーザ送信メール	PassLogic 認証ユーザ登録後に送信するメールのテンプレートです。ログイン URL、ユーザ ID、初期パスワードなどを含めたログイン手順の案内文を登録してください。
②	PassLogic 認証用 パスワード再発行送信メール	PassLogic 認証ユーザのパスワード再発行時に送信するメールのテンプレートです。ユーザ ID、再発行パスワードなどを含めた案内文を登録してください。
③	PassLogic 認証用 パスワードリマインダー送信メール	パスワードリマインダー機能から利用者に送信されるメールのテンプレートです。パスワードリセット URL を含めた案内文を登録してください。
④	PassLogic / PassClip 共通 端末登録時送信メール	端末固定機能を利用する際、2台目以降の端末をアクティベートするときに管理者から送信するメールのテンプレートです。 *1台目の端末は初回認証成功時に自動登録されるため2台目以降の端末固定に必要です。
⑤	PassLogic / PassClip 共通 PKI 認証用クライアント証明書の発行メール	クライアント証明書をダウンロードする際のダウンロードキーを案内するためのメールのテンプレートです。

⑥	PassClip 認証用 新規ユーザ送信メール	PassClip 認証ユーザ登録後に送信するメールのテンプレートです。PassClip アプリの利用手順、PassClip アクティベート URL、PassLogic ログイン URL、ユーザ ID などを含めたログイン手順の案内文を登録してください。
⑦	PassClip 認証用 PassClip 再セットアップ送信メール	PassClip 端末を再アクティベート する利用者に管理者から送信するメールのテンプレートです。 PassClip アクティベート URL などを含めた案内文を登録してください。
⑧	PassLogic 認証用 有効期限送信メール	PassLogic 認証ユーザのパスワード有効期限切れを事前案内する際に送信するメールのテンプレートです。パスワード有効期限を含めた案内文を登録してください。
⑨	PassLogic / PassClip 共通 アカウントロック通知メール	ユーザアカウントがロックされた際に自動で送信されるメールのテンプレートです。 ポリシーのアカウントロック通知メール機能を利用する場合、送信先に合わせて案内文を登録してください。

*①②③⑧はポリシー設定にて認証方式「PassLogic」を選択した場合に編集できます。

*⑥⑦はポリシー設定にて認証方式「PassClip」を選択した場合に編集できます。

*⑧はポリシー設定にて、「有効期限切れお知らせメール送信」を設定した場合にのみ登録します。

【 置換タグ定義 】

通知テンプレートに下記の置換タグを埋め込み、ユーザごとの情報をメール本文に含めることができます。

<%UNAME%>	氏名
<%UID%>	PassLogic ユーザ ID
<%DOMAIN%>	ドメイン名
<%PASSLOGICPATTERN%>	PassLogic 認証 シークレットパターン
<%SPASSWORD%>	PassLogic 認証 ワンタイムパスワードの後ろに付加するスタティックパスワード(固定パスワード)
<%ENTRYKEY%>	端末固定 アクティベーション用キー
<%DOWNLOADKEY%>	クライアント証明書のダウンロードキー
<%CERT_PASSWORD%>	クライアント証明書のインポート用パスワード
<%REMINDER_URLKEY%>	パスワードリマインダー利用時のパスワードリセット URL キー
<%PASSCLIP_URL%>	PassClip 認証 PassClip アプリ アクティベート用 URL キー
<%EXPIRE_DATE%>	パスワード有効期限

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

*通知テンプレート初期値 ログインページの URL「https://remote.example.com/」は適切な URL に変更してください。

2.4 メールサーバ設定

PassLogic から送信するメールサーバに関する設定を行います。

【 設定手順 】

(ｉ)管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞ Default Policy 編集 リンク をクリック

(ii)ユーザ通知設定項目 下部の メールサーバ欄 を編集し［次へ］をクリック

(iii)入力内容を確認し［決定］をクリック

*Default Policy 以外のポリシーではメールサーバ設定は編集できません。

*Default Policy で設定したメールサーバ設定はシステム一意の設定です(全てのポリシーに適用)。

【 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	SMTP サーバのポートの場合
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 で接続する場合に選択

2.5 ログ設定

PassLogic の管理･利用ログに関する設定を行います。

【 設定手順 】

(ｉ)管理ツール左側メニュー ＞ 設定 ＞ ポリシー設定 ＞ Default Policy 編集 リンク をクリック

(ii)メールサーバ項目 下部の メールサーバ欄 を編集し［次へ］をクリック

(iii)入力内容を確認し［決定］をクリック

*Default Policy 以外のポリシーではログ設定は編集できません。

*Default Policy で設定したログ設定はシステム一意の設定です(全てのポリシーに適用)。

【 項目解説 】

ログレベル	ログ出力する最低ログレベルを選択します。指定したログレベル以上のレベルがログ出力されます。 *ログレベルごとの出力内容は、本マニュアルの「ログ･リファレンス」の項を参照してください。 デフォルト『notice』
ログを syslog に出力する	on に設定した場合は /var/log/passlogic/passlogic.log に出力される内容と同じ情報を syslog に出力します。 デフォルト『off』

2.6 settings.conf 設定

システム一意の下記の設定は /opt/passlogic/data/conf/settings.conf を編集してください。

設定項目	設定内容	設定値
PL_SESSION_TIMEOUT *1	セッションタイムアウトするまでの時間（秒数）	デフォルト『900』 最大『259200』（3 日）
URL_HANDLER_SHOW *2	設定に該当するデバイスについてのみ、HTTP(s)を除く特殊ハンドラをメニューに表示します（SSL-VPN 利用時）。表示させたいデバイスのブラウザの User-Agent に含まれる文字列を追加してください。	デフォルト 『Android|iPhone|iPad』
PASSCLIP_SERVER_URL *2	PassClip 認証を利用する場合の PassClip サーバ アクティベート URL を設定します。 デフォルト値のまま利用してください。	デフォルト 『http://appscheme-l.passclip.com/?mode=passlogic&query=』
MULTI_LOGIN *2	同一ユーザによる、同時ログインの可否を設定してください。	可の場合：MULTI_LOGIN=1 否の場合：MULTI_LOGIN=0 デフォルト『1』 *3
DOMAIN_PULLDOWN *5	ユーザ名入力時にドメインを選択するプルダウンを表示するかを設定します。表示しない場合は「ユーザ名@ドメイン名」の形式でユーザ名を入力します。 *4	デフォルト『1』 表示しない：0 表示する：0 以外
DISABLE_SAVED_AD_PASSWORD *6	AD パスワードが保存されている場合に、パスワード入力欄を非活性状態にします。	デフォルト『0』 非活性化しない：0 非活性化する：1
REMINDER_URL_EXPIRY *7	パスワードリマインダーのワンタイム URL の有効期限を秒数で指定してください。	デフォルト『86400』 未指定の場合はデフォルト値（24 時間）が適用されます。 *8
ADUSERNAME_LOWERCASE	LDAP 認証連携をする際に、大文字のユーザ ID を禁止する場合設定してください。	デフォルト『0』 制限なし：0 大文字禁止：0 以外

LDAP_NETWORK_TIMEOUT	ドメイン管理にて、LDAP サーバをレプリケーションしている場合、サーバ1が停止時にサーバ 2 に切り替えるためのタイムアウト設定（秒数）	デフォルト『3』
CERT_ADMIN_PASSWORD	管理画面からクライアント証明書をダウンロードする際につけるパスワード	デフォルト未設定 パスワードをつける際に設定

＊1：セッションタイムアウトの時間を変更する場合は、以下のファイルも変更が必要です。
/opt/passlogic/data/conf/xauth_passlogic_00.conf 内の AuthPasslogicExpire の値を PL_SESSION_TIMEOUT と同じ値に変更し、httpd を再起動してください。
settings.conf「PL_SESSION_TIMEOUT」は、ユーザインターフェイス および PassLogic 管理ツールのセッションタイムアウト値、xauth_passlogic_00.conf「AuthPasslogicExpire」は PassLogic リバースプロキシサーバのセッションタイムアウト値の定義です。

＊2：バージョン 1.3.0 以前からアップデートした場合、設定項目にない場合があります。
2.0.0 以降のバージョンへアップデートした際は追記してください。

＊3：多重ログイン「否」に設定した場合、同じアカウントで先にログインしていたセッションが強制的にログアウト状態となり、後からログインしたセッションだけが利用できます。

＊4：「@ドメイン名」を入力せずユーザ名だけを入力した場合は、local ユーザとして扱われます。

＊5：バージョン 2.2.1 以前からアップデートした場合、設定項目にない場合があります。
2.3.0 以降のバージョンへアップデートした際は追記してください。

＊6：バージョン 2.3.2 以前からアップデートした場合、設定項目にない場合があります。
2.4.0 以降のバージョンへアップデートした際は追記してください。

＊7：バージョン 2.4.0 以前からアップデートした場合、設定項目にない場合があります。
2.5.0 以降のバージョンへアップデートした際は追記してください。

＊8：設定値を変更した場合は パスワードリマインダー送信メール のメール本文に記載の URL の有効期限に関する記述を変更してください。

2.7 グループ設定

PassLogic と各種プロトコルで連携するサービス（ユーザが認証後に利用できるサービス）の利用可否をユーザグループごとに制御することができます。グループは複数管理することができ、1ユーザに最大5グループ、1サービスに最大 10 グループを適用することができます。

【 グループの追加手順 】
（ｉ）管理ツール左側メニュー ＞ 設定 ＞ グループ設定 ＞[追加] をクリック
（ii）グループ名（半角英数字、ハイフン、アンダースコア／20 文字以内）を入力して [次へ]をクリック
（iii）内容を確認し [登録] をクリック
＊登録したグループをユーザに設定する方法は、本マニュアルの「ユーザ新規作成」の頁を参照してください。
＊登録したグループを連携サービスに設定する方法は、本マニュアルの「SSL-VPN ＞ シングルサインオン」「WebAPP」「Cloud」の頁を参照して、各連携サービス「アクセスグループ」に登録したグループを設定してください。

【 グループの削除手順 】
（ｉ）グループ一覧画面で、削除したいグループ名と同じ行の「削除」をクリック
（ii）確認ダイアログで「OK」をクリック
＊所属しているユーザがいる、または連携サービスで利用しているグループは削除することができません。

【 所属ユーザでユーザ検索 】
グループ名 リンクをクリックすると、そのグループに属するユーザー一覧が表示されます。

2.8 IP グループ設定

PassLogic は WebAPP とクラウド連携の場合、ユーザのアクセス元の IP アドレスで連携の制限をかけることができます。IP アドレスのグループを作成し、連携サービスに設定することで、IP グループ内からアクセスしてきたユーザのみを連携することができます。IP グループは CIDR 形式で表記され、単体 IP から範囲指定まで設定することができます。また IP グループは複数管理することができ、各サービスには最大 10 グループ適応することができます。
※ゲートウェイサーバ利用時に IP グループを利用する場合は、別冊の「PassLogic Enterprise Edition Ver.3.0.0 レプリケーション セットアップ＆リカバリガイド」をご覧ください。

【 IP グループの追加手順 】
(i)管理ツール左側メニュー > 設定 > IP グループ設定 > [追加] をクリック
(ii)IP グループ名(半角英数字、ハイフン、アンダースコア／20 文字以内)と CIDR 形式の IP アドレス範囲を入力して [次へ]をクリック
(iii)内容を確認し [登録] をクリック
*登録した IP グループを連携サービスに設定する方法は、本マニュアルの「WebAPP」「Cloud」の頁を参照して、各連携サービス「IP アクセスグループ」に登録した IP グループを設定してください。

【 IP グループの削除手順 】
(i)IP グループ一覧画面で、削除したい IP グループ名と同じ行の「削除」をクリック
(ii)確認ダイアログで「OK」をクリック
*連携サービスで利用している IP グループは削除することができません。

【 IP アドレス範囲の確認･編集 】
IP グループ名 リンクをクリックすると、その IP グループの内容が表示されます。
IP アドレス範囲を変更して[次へ]をクリックし、変更内容を確認後[登録]をクリックすることで、IP グループを編集することができます。

2.9 UI(ユーザインターフェイス)設定

ユーザが利用するインターフェイスのロゴとメッセージを編集することができます。

PassLogic 認証ユーザ用 パスワード変更画面に表示される文言「Change password message1」「Change password message2」「Change password message3」は、ポリシー設定に従って変更してください。

【 UI メッセージ編集手順 】
(i)管理ツール左側メニュー > 設定 > UI 設定 > 編集言語の 編集 リンクをクリック
(ii)メッセージを編集して [次へ]をクリック
(iii)内容を確認し [決定] をクリック
*デフォルトで用意されている 英語「en」と日本語「ja」 の他の言語を追加することもできます。
*ブラウザで最優先する言語が日本語(言語コード「ja」)の場合は、PassLogic に初めてアクセスしたときに日本語「ja」が、これに該当しない場合は英語「en」が初期選択状態となります。

【 UI ロゴ変更手順 】

(ｉ)管理ツール左側メニュー ＞ 設定 ＞ UI 設定 ＞ [logo upload] をクリック

(ii)[ファイルを選択]をクリックして、差替えロゴファイルを選択し [送信] をクリック

*delete リンクをクリックするとアップロードしたロゴファイルが削除され、デフォルトの PassLogic ロゴに差し替わります。

*アップロードするロゴの仕様

サイズ	横 154px 縦 22px
フォーマット	PNG(透過)

*IE9 ではロゴファイルのアップデートができません。IE9 以外のブラウザをお使いください。

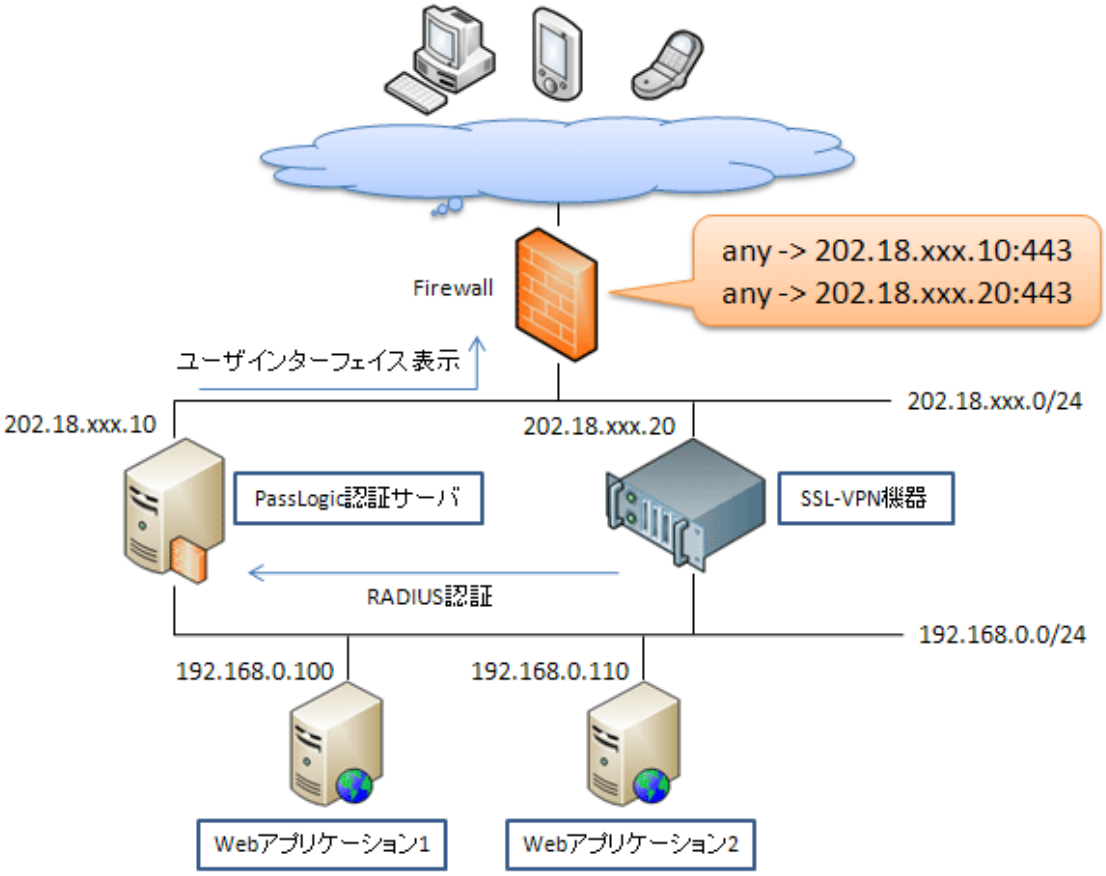
*ユーザインターフェイスは下記の URL で確認できます。

https://[PassLogic サーバ]/ui/

2.10 SSL-VPN

PassLogic 認証サーバのインストール時に、PassLogic 用に拡張された RADIUS サーバがインストールされ、SSL-VPN 装置と RADIUS プロトコルによる認証連携が可能になります。

認証方式は、PAP、CHAP、MSCHAPv1,v2 に対応しています。



SSL-VPN 機器登録

PassLogic 管理ツールに RADIUS クライアントとなる SSL-VPN 機器を登録します。

【 設定手順 】

(ⅰ)管理ツール左側メニュー ＞ SSL-VPN ＞ SSL-VPN 機器登録 ＞ [追加] をクリック

(ⅱ)各項目 を入力し [次へ] をクリック

(ⅲ)入力内容を確認し [登録] をクリック

【 項目解説 】

識別子	PassLogic 管理ツール上の識別名称を 31 文字以下の英数字と記号(-_)で入力してください。
IP アドレス	RADIUS クライアントの IP アドレス または ホスト名
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	RADIUS 認証成功時 PassLogic RADIUS サーバから RADIUS クライアントへ、ユーザごとのアトリビュート値を送信する必要がある場合にアトリビュートの名前(name)を入力します。 RFC2865(http://freeradius.org/rfc/attributes-rfc2865.html) 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。 *ユーザ登録時の SSL-VPN 機器登録 attribute1-10(ユーザ情報 CSV 一括取込項目 attribute1-10)が attribute1-10 の値として対応します。ユーザの該当するポリシー設定で[AD パスワード保存]を選択している場合、保存された AD パスワードが AD password の値として対応します。

シングルサインオン

PassLogic のユーザインターフェイスから、SSL-VPN 機器のユーザインターフェイスに対するシングルサインオン設定を登録します。

【 設定手順 】

(i)管理ツール左側メニュー > SSL-VPN > シングルサインオン > [追加] をクリック
(ii)各項目 を入力し [次へ] をクリック
(iii)入力内容を確認し [決定] をクリック

【 項目解説 】

No.	PassLogic ログイン後のメニュー画面での表示順(昇順)を半角数値で入力してください。0 を指定するとメニュー画面に表示されません(メニュー画面を経由しない自動ログインは可能)。
アプリケーション名称	PassLogic ログイン後のメニュー画面に表示されます。任意の文字列を入力してください。
認証の送信先 URL(*1)	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	SSL-VPN 機器へのログインに使用するログイン ID(ユーザ ID)の name 属性の名称を入力してください。(例: UserID) *属性名に対応する属性値は、PassLogic のユーザ ID を下記「ログイン ID の value 属性」に指定するフォーマットに変換した値です。
ログイン ID の value 属性	SSL-VPN 機器へのログインに使用するログイン ID(ユーザ ID)の形式を 「Uid Only」 「PassLogic Domain(uid@PassLogic Domain)」 「ActiveDirectory Domain(uid@AD Domain)」 「NT Domain(NT Domain¥uid)」から選択してください。 *PassLogic Domain とはドメイン管理画面の「ドメイン名」を示します。 *ActiveDirectory Domain および NT Domain とはドメイン管理＞LDAP 認証連携設定の「Active Directory ドメイン名または NT ドメイン名」を示します。 *local ユーザでシングルサインオンする場合は、設定値に関わらず「Uid Only」として扱われます。 *当該項目が「ActiveDirectory Domain」または「NT Domain」に設定されている状態で「Active Directory ドメイン名または NT ドメイン名」が設定されていないドメインに所属するユーザがシングルサインオンした場合、「Uid Only」として扱われます。
パスワードの name 属性	SSL-VPN 機器へのログインに使用するパスワードの name 属性の名称を入力してください。(例: Password) *属性名に対応する属性値は、PassLogic RADIUS サーバが認証する際のワンタイムパスワードです。このときのワンタイムパスワードは PassLogic が自動生成します。
AD パスワードの送信	SSL-VPN 機器へのログインに AD パスワードを利用する場合は「送信する」を選択してください。選択した場合は AD パスワードの name 属性の名称を入力してください。(例：ADpassword) *属性名に対応する属性値は、PassLogic ログイン時に入力する ActiveDirectory のパスワードです。
アクセスグループ	アクセスを許可するユーザが属するグループを選択します。 *未指定の場合は全ユーザが利用できます。
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	SSL-VPN 機器へログイン情報を送信する前に、ログインページに含まれる特定の情報（エンティティ）を取得する必要がある場合のみログインページの URL を設定します。 *取得したエンティティはログイン情報とともに認証の送信先 URL へ送信されます。 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	SSL-VPN 機器へログイン情報を送信する際に、全ユーザで同一の固定パラメータを送信する場合は、属性名を「付加するパラメータ」欄、対応する値を「パラメータの値」に設定してください。
ユーザごとのパラメータ	SSL-VPN 機器へログイン情報を送信する際に、ユーザごとに送信したいパラメータの name 属性を指定します。 *ユーザ登録時のシングルサインオン param1-10（ユーザ情報 CSV 一括取込項目 sslvpn param1-10）が対応する値となります。 *password1-5 はユーザログイン後のユーザが設定した値が対応する値となります。

*1：http, https 以外の handler も登録できます(例: anyconnect://)。その際には以下の文字列が置換文字列として使用できます。

<%AUTHID%>	ログイン ID（ログイン ID の value 属性に指定した形式）
<%PASSWORD%>	認証パスワード
<%PARAM1%>	ユーザごとのパラメータ sslvpn param1
<%PARAM2%>	ユーザごとのパラメータ sslvpn param2
<%PARAM3%>	ユーザごとのパラメータ sslvpn param3
<%PARAM4%>	ユーザごとのパラメータ sslvpn param4
<%PARAM5%>	ユーザごとのパラメータ sslvpn param5
<%PARAM6%>	ユーザごとのパラメータ sslvpn param6
<%PARAM7%>	ユーザごとのパラメータ sslvpn param7
<%PARAM8%>	ユーザごとのパラメータ sslvpn param8
<%PARAM9%>	ユーザごとのパラメータ sslvpn param9
<%PARAM10%>	ユーザごとのパラメータ sslvpn param10
<%USERPASS1%>	ユーザごとのパラメータ password1
<%USERPASS2%>	ユーザごとのパラメータ password2
<%USERPASS3%>	ユーザごとのパラメータ password3

<%USERPASS4%>	ユーザごとのパラメータ password4
<%USERPASS5%>	ユーザごとのパラメータ password5

*2：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。

```
SSL-VPN 機器 ログイン画面 HTML ソース 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 SSL-VPN 機器へログイン情報とともに送信します。

Web Token / PassClip

ユーザが SSL-VPN 機器のログイン画面に直接ログインする場合は Web Token または PassClip を利用します。

Web Token を利用する場合、SSL-VPN 機器へログインするときに必要な（ワンタイムパスワードの生成元）乱数表は、ログイン画面とは別にパソコンやスマートデバイスなどのブラウザに表示します。

ユーザ ID を指定して直接アクセスする方法*1 と、入力フォームからアクセスする方法*2 があります。

Web Token URL

```
方法 1：以下の URL に直接アクセスする
https://[PassLogic サーバ]/ui/token.php?uid=[uid]&domain=[domain]
方法 2:以下の URL にアクセスし、ユーザ ID を入力して次をクリックする
https://[PassLogic サーバ]/ui/token.php
```

*Web Token の使用が有効なポリシーのユーザのみ利用できます。

*Web Token を利用できるユーザが PassLogic にログインすると、メニュー画面に Web Token へのリンク（上記「方法 1 の URL」と同じリンク先）が表示されます。表示されたリンクをブックマークに保存することで、PassLogic メニュー画面を経由せずに直接 Web Token を表示することができます。

*ポリシーの認証方式が PassClip のユーザの場合、Web Token の代わりに PassClip の表示するワンタイムパスワードが、SSL-VPN 機器へのログインに必要なパスワードとなります。

* SSL-VPN に直接入力するユーザ名は「uid@domain」（local の場合は@local 省略可）のように@domain を付加してください。

RADIUS 認証動作(参考)

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

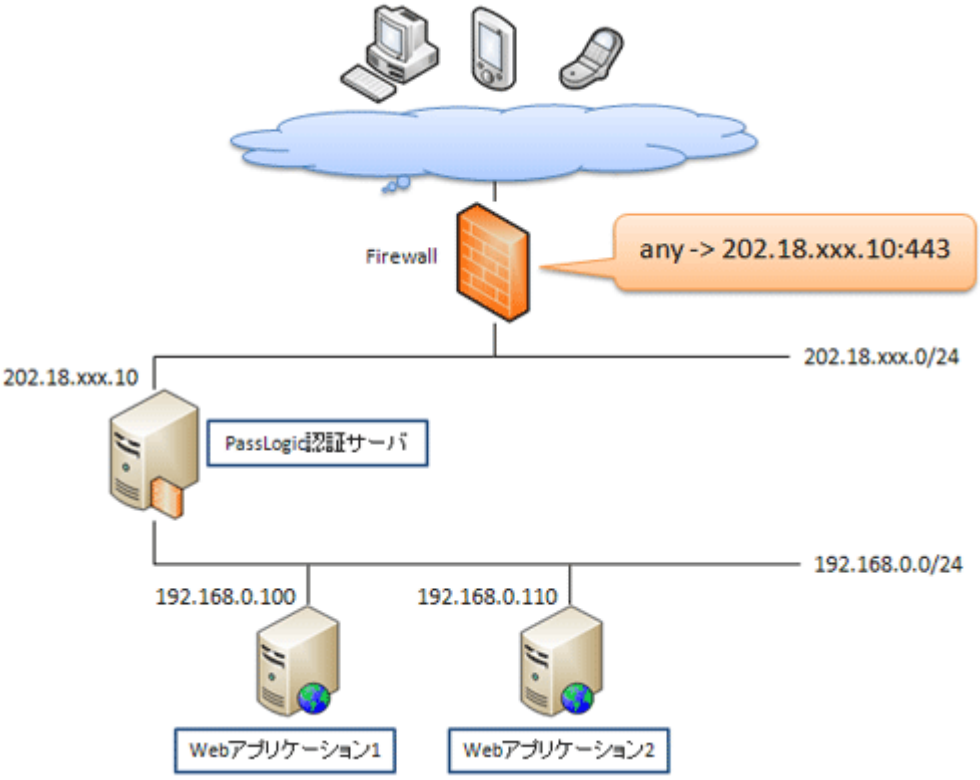
```
# echo "User-Name=test, CHAP-Password=0772" | radclient -x 192.168.0.203 auth secret

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 WebAPP

WebAPP 連携で社内のプライベートアドレスに設置しているウェブアプリケーションに PassLogic サーバのリバースプロキシ経由でリモートアクセスすることができます。

リモートアクセス・ネットワーク構成例



*PassLogic リバースプロキシ経由でプライベートアドレスにあるアプリケーションにユーザリクエストを転送する際、PassLogic のユーザ ID が http ヘッダに含まれて送信されます。この情報を用いて認証状態を判定する独自アプリケーションを構築することもできます。

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
PL-Authid: testuser@local
Connection: Keep-Alive
```

PassLogic 認証済みのユーザ ID をアプリケーションで取得する PHP 実装例

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

WebAPP

PassLogic 管理ツールに仮想パスとローカルアプリケーション URL をマッピングして、リバースプロキシ設定を登録します。

【 設定手順 】

(ｉ)管理ツール左側メニュー ＞ WebAPP ＞ WebAPP ＞ [追加] をクリック
(ii)各項目 を入力し [次へ] をクリック
(iii)入力内容を確認し [決定] をクリック

【 項目解説 】

No.	PassLogic ログイン後のメニュー画面での表示順(昇順)を半角数値で入力してください。0 を指定するとメニュー画面に表示されません（メニュー画面を経由しない自動ログインは可能)。
アプリケーション名称	PassLogic ログイン後のメニュー画面に表示されます。任意の文字列を入力してください。 *半角記号「&」「#」「+」は利用できません。
仮想パス	アプリケーションを公開する際に割り当てるパスを入力してください。 *下記の仮想パスは利用できません。 「/」「/passlogic-admin/」「/passlogic/」「/ui/」
ローカルアプリケーションの URL	ローカルアプリケーションの URL を指定してください。 アプリケーションサーバが IIS サーバの場合、チェックボックスをチェックしてください。
アクセスグループ	アクセス可能なグループを選択します。 *未指定の場合は全ユーザが利用できます。
IP アクセスグループ	アクセス可能な IP グループを選択します。 *未指定の場合は全ユーザが利用できます。

URL マッピング(*1)	「仮想パス」と「ローカルアプリケーションの URL」定義だけではローカルアプリケーションの画像、JavaScript、CSS 等のファイルが参照できない場合は、これらの URL をディレクトリにマッピングしてください。 仮想パス　　:割り当てるパス ローカル URL　　:仮想パスに該当するローカル URL *システム内で重複する仮想パスは指定できません。
コンテンツ変換 (*2)(*3)(*4)	圧縮されたコンテンツに対して変換する場合に『Accept-Encoding 強制除去』にチェックしてください。ただし、圧縮をせずに通信を行います。 ローカルアプリケーションのコンテンツに含まれる指定の文字列を置換してクライアントに応答します。 検索する文字　　:書き換え対象文字列 置換する文字　　:書き換え後の文字列 大文字/小文字は区別され、正規表現には対応していません。

*1:URL マッピング設定は PassLogic サーバの httpd エラーログを参照して不足しているマッピング定義を探すことができます。

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:記号|(パイプライン)と半角スペースは、検索する文字列、変換後の文字列どちらにも含めることは出来ません。

*3:コンテンツを圧縮して送信するアプリケーション(gzip 圧縮コンテンツなど)には対応していません。

*4:検索する文字列、変換後の文字列ともに、UTF-8 になります。日本語文字コードが UTF-8 以外のアプリケーションでは日本語文字列の変換は出来ません。

WebSSO

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または Basic 認証を行うことができます。ユーザは PassLogic にログインするだけで、WebSSO 設定した Web アプリケーションに対して個別にログインする必要がなくなります。また、複数の Web アプリケーションのユーザ ID とパスワードを配布する手間を省き、システム運用が効率化されます。

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などがあります。

PassLogic は下記の WebSSO(自動フォーム認証)に対応しています。

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
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)

【 設定手順 】

(ⅰ)WebSSO 設定をする WebAPP 定義を登録

PassLogic リバースプロキシ経由で対象アプリケーションにアクセスし手動ログインできることを確認してください。

(ⅱ)管理ツール左側メニュー > WebAPP > WebSSO > [追加] をクリック

(ⅲ)各項目 を入力し [次へ] をクリック

(ⅳ)入力内容を確認し [決定] をクリック

【 項目解説 】

アプリケーション名称	WebAPPに登録したアプリケーションが選択できます。WebSSOに対応させたいアプリケーション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: user_id) *対応する属性値は PassLogic のユーザ ID です。
ログイン ID の value 属性	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)の形式を 「Uid Only」 「PassLogic Domain(uid@PassLogic Domain)」 「ActiveDirectory Domain(uid@AD Domain)」 「NT Domain(NT Domain¥uid)」 から選択してください。 *PassLogic Domain とは ドメイン管理画面の「ドメイン名」を示します。 *ActiveDirectory Domain および NT Domain とはドメイン管理＞LDAP 認証連携設定の「Active Directory ドメイン名または NT ドメイン名」を示します。 *local ユーザでシングルサインオンする場合は、設定値に関わらず「Uid Only」として扱われます。 *当該項目が「ActiveDirectory Domain」または「NT Domain」に設定されている状態で「Active Directory ドメイン名または NT ドメイン

	名」が設定されていないドメインに所属するユーザがシングルサインオンした場合、「Uid Only」として扱われます。
AD パスワードの送信	アプリケーションへログイン情報を送信する際に、AD パスワードを送信します。「AD パスワードの name 属性」の項目で、送信する際の name 属性を指定します。
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(*2)	サーバ自動認証、クライアント自動認証(JavaScript)、BASIC 認証、特定アプリケーションへの SSO プログラム のいずれかを選択します。 *BASIC 認証では、ユーザごとのパラメータ param1-param10 を選択してください。(*3)
ログインページの URL	アプリケーションへログイン情報を送信する前に、ログインページに含まれる特定の情報(エンティティ)を取得する必要がある場合のみログインページの URL を設定します。 *PassLogic 認証サーバがアクセスする URL を指定してください。 *取得したエンティティはログイン情報とともに認証の送信先 URL へ送信されます。 ログインページから取得する値の名前 ログインページにアクセスした際に下記のように自動で生成され、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)<input type="hidden" name="SESSION_TOKEN" value="[毎回変わる値]"> *「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=値のペアをログイン情報とともに送信します。
認証の送信先 URL	WebAPP に定義した「ローカルアプリケーションの URL」以外にログイン用の URL がある場合に入力して下さい。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。 *認証方式「サーバ自動認証」を選択した場合は、PassLogic 認証サーバがアクセスする URL を指定してください。 *認証方式「クライアント自動認証(JavaScript)」を選択した場合は、クライアント(ユーザ)が PassLogic 経由でアクセスする URL を指定してください。 *BASIC 認証を選択した場合で、認証時にローカルアプリケーション

	からクッキーを受け取る場合、クライアント(ユーザ)が PassLogic 経由でアクセスする URL を指定してください。
その他の追加パラメータ	アプリケーションへログイン情報を送信する際に、全ユーザで同一の固定パラメータを送信する場合は、属性名を「付加するパラメータ」欄、対応する値を「パラメータの値」に設定してください。
ユーザごとのパラメータ	アプリケーションへログイン情報を送信する際に、ユーザごとに送信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 WebSSO param1-10(ユーザ情報 CSV 一括取込項目 websso param1-10)が対応する値となります。 *password1-5 はユーザログイン後のユーザが設定した値が対応する値となります。

*1:アプリケーションごとにログイン情報として送信する属性情報は異なります。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。

```
アプリケーション ログイン画面 HTML ソース 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 />
<br />
<input type="submit" name="submit" value="ログイン">
<input type="hidden" name="mode" value="login">
</form>
```

上記の例であれば下記のような WebSSO 設定を登録してください。

ログイン ID の name 属性　　:user_id

ユーザごとのパラメータ param1　　:password

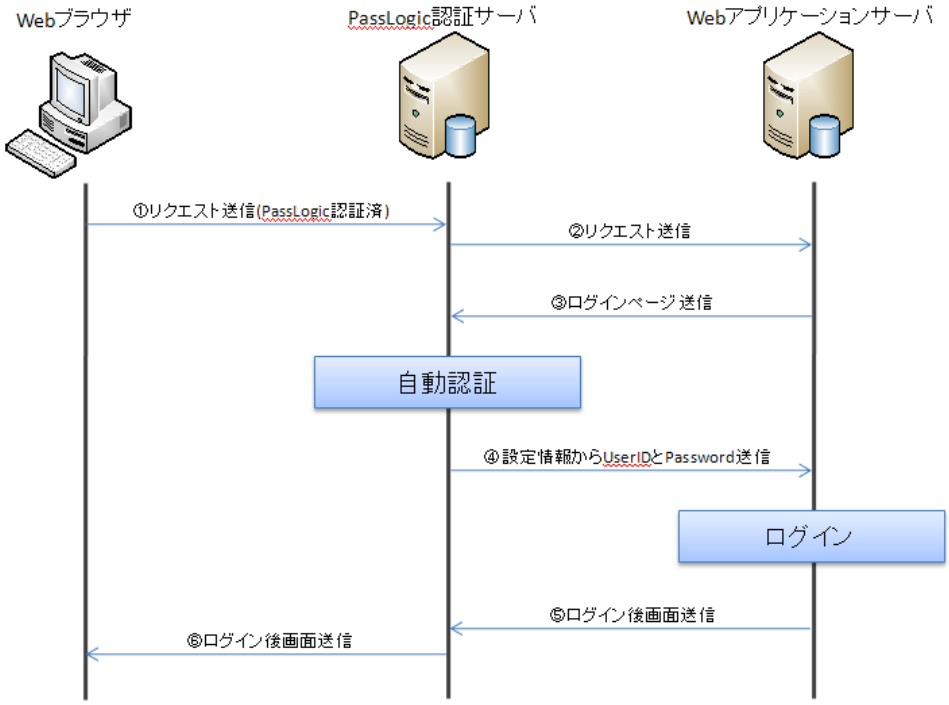
(PassLogic ユーザ情報 websso param1 にアプリケーションのパスワードを管理する)

その他の追加パラメータ　　:付加するパラメータ:mode/パラメータの値:login

*2:サーバ自動認証/クライアント自動認証の違いは下記をご覧ください。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利用します。

*3: BASIC 認証の場合、認証情報はフォームとして送信するのではなく、PassLogic リバースプロキシ経由でプライベートアドレスにあるアプリケーションにユーザリクエストを転送する際に、Authorization ヘッダに含めて送信されます。ユーザごとのパラメータに登録する認証情報はローカルアプリケーションのユーザ ID とパスワードを:(コロン)で区切って登録します。登録方法の詳細は **4.4 BASIC 認証情報の登録方法**をご参照ください。

サーバ自動認証のシーケンス図

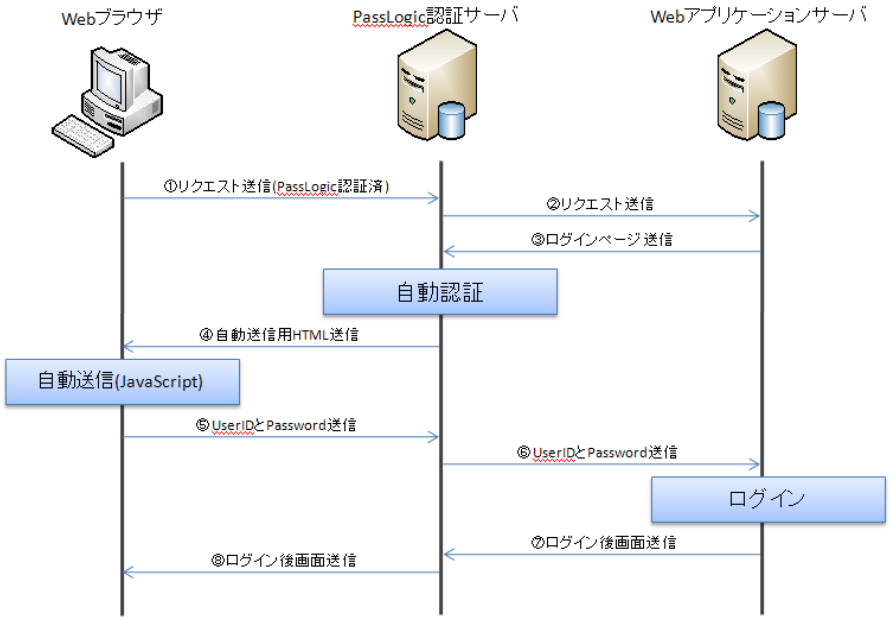


PassLogic 認証サーバが代理でユーザ ID、パスワードをアプリケーションに対して送信します。アプリケーションによってはログインが成功しないこともありますが、アプリケーションのユーザ ID、パスワードが外部ネットワーク上を流れることがないのでセキュアな方式です。

*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認証(JavaScript)をご利用ください。

*ログインのときにクライアントにて JavaScript などで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おりません。

クライアント自動認証のシーケンス図



一旦クライント(Web ブラウザ)を経由しますので適用範囲が広がりますが、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。

クライントに送信する 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>
```

2.12 Cloud

SAML(Security Assertion Markup Language)2.0 による認証連携で対応している Web アプリケーションにアクセスすることができます。

SP 登録

PassLogic 管理ツールに SP(Service Provider)定義を登録します。
*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を参照してください。

【 設定手順 】
(ⅰ)管理ツール左側メニュー > Cloud > SP 登録 > [追加] をクリック
(ⅱ)各項目 を入力し [次へ] をクリック
(ⅲ)入力内容を確認し [決定] をクリック

【 項目解説 】

No.	PassLogic ログイン後のメニュー画面での表示順(昇順)を半角数値で入力してください。0 を指定するとメニュー画面に表示されません（メニュー画面を経由しない自動ログインは可能)。
プロバイダ	PassLogic ログイン後のメニュー画面に表示されます。任意の文字列を入力してください。
SAML タイプ	SP initiated SSO / Idp initiated SSO のいずれかを選択してください。サービスプロバイダの仕様に依存します。
NameID フォーマット	サービスプロバイダに送信する SAML Response のユーザ名に使われる NameID のフォーマットを選択します。（選択肢にない場合は、その他を選択し、テキストフィールドに入力してください）
UID タイプ	サービスプロバイダに送信する SAML Response のユーザ名にドメイン名を含める/含めないを選択します。
ドメイン	ドメイン名を入力してください。
RelayStateURL	SAML 認証後の遷移先 URL SP(Service Provider)の仕様にしたがって入力してください。
Recipient	SP の ACS URL・SAML response の送信先 SP の仕様にしたがって入力してください。
Destination	SP の ACS URL・SAML response 内 Destination 属性の値 SP の仕様にしたがって入力してください。
Issuer	IdP EntityID・SAML response 内 Issuer 属性の値 SP の仕様にしたがって入力してください。
Audience	SAML response 内 Audience 属性の値 SP の仕様にしたがって入力してください。
PassLogic FQDN	ユーザが PassLogic にアクセスするときの URL の一部 (http(s)://<PassLogicFQDN>)を入力してください。 *Idp metadata ダウンロード機能を利用する場合に必要です。
Attribute mapping1-5	SAML Response として SP に受け渡す情報をキーと値のセットで登録してください。
アクセスグループ	アクセス可能なグループを選択します。 *未指定の場合は全ユーザが利用できます。
IP アクセスグループ	アクセス可能な IP グループを選択します。 *未指定の場合は全ユーザが利用できます。

*SP initiated SSO の場合、SAML Request は下記の URL に到達するように SP を設定してください。
http(s)://<PassLogic FQDN>/ui/idp.php?target=<プロバイダ>

証明書

PassLogic 管理ツールに SAML 連携で利用する証明書を登録します。
*登録する公開鍵と秘密鍵の証明書セットはご用意ください。

【 公開鍵証明書 登録手順 】
(i)管理ツール左側メニュー > Cloud > 証明書 をクリック
(ii)証明書 > アップロード の右側の［ファイルを選択］をクリックして公開鍵証明書ファイルを選択
(iii)ファイル名を確認し、右の［登録］をクリック
*公開鍵証明書は SP にも同じものを登録してください。
*正しいフォーマットの公開鍵証明書が登録されると、発行者情報と有効期限が表示されます。
*「証明書ダウンロード」をクリックすると、登録した公開鍵証明書ファイルがダウンロードできます。

【 秘密鍵証明書 登録手順 】
(i)管理ツール左側メニュー > Cloud > 証明書 をクリック
(ii)秘密鍵 > アップロード の右側の［ファイルを選択］をクリックして秘密鍵証明書ファイルを選択
(iii)ファイル名を確認し、右の［登録］をクリック

2.13 バックアップ/リストア

PassLogic 認証サーバの全てのデータベースおよび全ての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

管理ツール左側メニュー > メンテナンス >バックアップを選択し、パスワード(リストアの際に必要・半角英数字のみ指定可)を入力して［送信］をクリックすると、バックアップファイルのダウンロードが開始されます。

コマンドラインでバックアップファイルを作成することもできます。

```
# sh /opt/passlogic/apps/tools/backup.sh ［バックアップファイルのパスワード］
```

*バックアップファイルは /opt/passlogic/tmp/passlogicbackup.zip に出力されます

リストア

【 リストア手順 】
(i)管理ツール左側メニュー > メンテナンス > リストアをクリック。
(ii)バックアップファイルを選択し、バックアップの際に設定したパスワードを入力。
(iii)リストアモードを選択し、[送信]をクリック。

【 リストアモード 】

データベースおよび 設定情報をリストア	全てのデータベースと全ての PassLogic の設定が置き換わります
データベース情報をリストア	全てのデータベースのみ置き換わります
設定情報をリストア	全ての PassLogic の設定のみ置き換わります

*ファイルサイズが 128MB を超えるバックアップファイルをリストアする場合は、リストア先の PassLogic 認証サーバで下記の設定変更を実施してからリストアしてください。

/etc/php.ini 編集

post_max_size	128M -> バックアップファイルサイズよりも大きな値に変更
upload_max_filesize	128M -> バックアップファイルサイズよりも大きな値に変更

httpd 再起動

```
(RHEL6/CentOS6 の場合)
# service httpd restart
(RHEL7/CentOS7 の場合)
# systemctl restart httpd
```

*post_max_size と upload_max_filesize に指定できる上限値は、同設定ファイルに定義されている memory_limit の設定値(256M)より大きな値を指定することはできません。

コマンドラインでリストアを実行することもできます。

```
# sh /opt/passlogic/apps/tools/restore.sh [バックアップファイルのパスワード] [オプション] >
/var/log/passlogic/passlogic-restore.log
```

【 restore.sh オプション 】

(指定なし)	全てのデータベースと全ての PassLogic の設定が置き換わります
-d	データベースのみ置き換わります
-c	PassLogic の設定のみ置き換わります

*コマンド実行前に バックアップファイルを /opt/passlogic/tmp/passlogicbackup.zip にアップロードしてください。リストア実行後、アップロードしたファイルは削除されます。

*リストアログ /var/log/passlogic/passlogic-restore.log にエラーが出力されないことを確認してください。

2.14 テクニカルサポート･ファイルの取得

テクニカルサポートの際にサポートスタッフがサポートファイルの取得をお願いする場合があります。

管理ツール左側メニュー > メンテナンス > テクニカルサポート を選択し、パスワードを入力して送信ボタンをクリックすると、ファイルのダウンロードが開始されます。

*ファイルには設定、ログが含まれています。ユーザ情報など個人情報は含まれていません。

*ファイルを取得するにはサーバの空き容量が 2G 以上必要です。

テクニカルサポートのため取得されるファイル

OS の種類(バージョンなど)
サーバ設定ファイル(/etc/httpd/conf, /etc/httpd/conf.d, /etc/php.ini)
PassLogic 設定ファイル(/opt/passlogic/data)
ログファイル(/var/log/httpd, /var/log/radiusd, /var/log/passlogic ,
/var/log/passlogic-pgpool, /opt/passlogic/pgsql/data/serverlog)

*サポートスタッフにダウンロード時に設定したパスワードをお知らせください。

2.15 管理者用(admin)パスワードを忘れた場合

本マニュアルの「管理ツールにアクセスする」の項を参照して admin のパスワードを再作成してください。

2.16 監視対象プロセス

PassLogic 認証サーバでは以下のプロセス監視を行ってください。

(RHEL6/CentOS6 の場合)

/usr/sbin/httpd
/usr/sbin/radiusd
/opt/passlogic/pgpool/bin/pgpool
/opt/passlogic/pgsql/bin/postmaster

(RHEL7/CentOS7 の場合)

/usr/sbin/httpd	ユニット名:httpd.service
/usr/sbin/radiusd	ユニット名:radiusd.service
/opt/passlogic/pgpool/bin/pgpool	ユニット名:passlogic-pgpool.service
/opt/passlogic/pgsql/bin/postgres	ユニット名:passlogic-pgsql.service
*コマンド "# systemctl status ユニット名" で起動状態とプロセス一覧の取得が可能	

2.17 メニュー画面をスキップする方法

ユーザがアクセスするログイン画面 URL に以下のようなクエリストリングを指定することで、認証完了後にメニュー画面をスキップして自動的に SSL-VPN、ウェブアプリケーション、クラウドサービスへ連携することができます。

パスワード有効期限切れなどの理由でパスワード変更が必要なユーザは、認証完了後にパスワード変更画面に遷移し、パスワード変更完了後はメニュー画面をスキップして自動的に対象のアプリケーションへ連携します。

SSL-VPN 連携

https://[PassLogic サーバのホスト名]/ui/?sso-vpn=[アプリケーションの名称]

WebAPP 連携

https://[PassLogic サーバのホスト名]/ui/?sso-webapp=[アプリケーションの名称]

Cloud 連携(idP ini の場合)

https://[PassLogic サーバのホスト名]/ui/?sso-saml=[サービスプロバイダの名称]

※SP ini の場合は、直接サービス側の SAML ログイン URL にアクセスしてください

2.18 パスワードリマインダー

ユーザが PassLogic 認証のパスワード(シークレットパターン・スタティックパスワード)を忘れてしまった場合にユーザ自身でパスワードの再発行ができる機能です。

ポリシー設定でパスワードリマインダーの利用を許可されたポリシーに属するユーザだけが利用できます。

【 ユーザ利用手順 】

(i) https://[PassLogic サーバ]/ui/reminder.php にアクセスします。

(ii)ユーザ名(必要な場合はドメイン名をプルダウンから指定、プルダウン非表示の場合は"ユーザ名@ドメイン名"の形式で入力)とユーザ情報に登録されているメールアドレスを入力し [次へ] をクリック

(iii)ユーザ名とメールアドレスの組み合わせが正しい場合、対象メールアドレス宛にパスワード再発行の URL が記載されたメールが送信されます。

(iv)メールに記載された URL にアクセスすると、新しいパスワードが再発行され、対象メールアドレス宛に新しいパスワードが記載された通知メールが送信されます。

*パスワード再発行の URL は 1 回限り有効です。また、有効期間は URL が発行されてから 24 時間(デフォルト値・設定変更は settings.conf 設定 を参照してください)です。有効期間を過ぎた場合は新しいパスワードは再発行されません。

*パスワード再発行の URL は最新のものをご利用ください(同一ユーザで ii の操作だけを複数回実行した場合は最後に送信されたパスワード再発行の URL だけが有効です)。

*再発行されるパスワードは「PassLogic 設定>ポリシー設定>ランダム発行時の長さ(ワンタイムパスワード)」に設定されている長さのランダムなシークレットパターンと、「PassLogic 設定>ポリシー設定>ランダム発行時の長さ(スタティックパスワード)」に設定されている長さのスタティックパスワードです。

*パスワードリマインダー利用後、対象ユーザのロック状態は強制解除されます。

3 PKI 設定

3.1 PKI 設定状況

ルート証明書関係の設定(ルート証明書発行、更新、リセット、ダウンロード)とクライアント証明書の1ユーザあたりの発行件数と、ダウンロード回数制限を設定します。

【ルート証明書関係の設定 】

(ⅰ)ルート証明書が未設定の場合、ルート証明書設定ページでインポート、もしくはパラメータ*1 を入力の上発行することができます。

(ⅱ)設定済の場合は、ルート証明書設定ページで発行した証明書・秘密鍵のダウンロード、有効期限の更新、ルート証明書・発行済みクライアント証明書の設定のリセットができます。

*1 パラメータのフォーマット

識別名	64 文字以内の英数字と以下の記号。『 』『,』『+』『-』『.』『/』『_』『(』『)』『|』
国/地域コード	2 文字英字の国コード(例:JP
都道府県	128 文字以内の英数字と以下の記号。『 』『,』『+』『-』『.』『/』『_』『(』『)』『|』
市区町村	128 文字以内の英数字と以下の記号。『 』『,』『+』『-』『.』『/』『_』『(』『)』『|』
組織名	128 文字以内の英数字と以下の記号。『 』『,』『+』『-』『.』『/』『_』『(』『)』『|』
所属名	128 文字以内の英数字と以下の記号。『 』『,』『+』『-』『.』『/』『_』『(』『)』『|』
メールアドレス	メールアドレス形式
有効期限	YYYY/MM/DD フォーマット

※クライアント証明書のパラメータも同様フォーマット

【1ユーザあたりの発行件数制限】

1ユーザに対して、クライアント証明書を発行する件数の上限を設定します。(0 以上 99 以下の範囲)
0で上限なしとなります。

【ダウンロード回数制限】

ユーザがクライアント証明書をダウンロードする回数の上限を設定します。(0 以上 99 以下の範囲)
0で上限なしとなります。
※管理メニューからのダウンロード回数は含めません。

3.2 クライアント証明書発行

ユーザに対してクライアント証明書を発行します。ユーザに紐付かない共有することのできるクライアント証明書と、ユーザに紐付くクライアント証明書の2種類を発行できます。

※ルート証明書が未設定の場合は、先に実施してください。

【共有証明書発行】

共有証明書発行ボタンを押すと、共有利用するクライアント証明書を発行できます。共有利用のクライアント証明書は、認証の際に紐付いたユーザの確認をせずに PKI 認証します。

※uid/domain は common/common という疑似名に設定されます。

【一括発行】

ユーザ一覧のチェックボックスにチェックを入れて一括発行ボタンを押すと、チェックされたユーザに一括でクライアント証明書が発行されます。

識別名フォーマット:

・uid_domain:uid と domain の間に_(アンダースコア)を挟んだ表記

・uid_domain_random:上記表記の末尾に、_(アンダースコア)とランダム 8 文字(a-zA-Z1-9)をつけた表記

メール通知:チェックを入れた場合、ユーザにメールアドレスが登録されていれば、クライアント証明書発行後に自動的にクライアント証明書の発行メールを送信します。

発行完了後、『通知書をメール』『通知書をプリントアウト』をクリックすることで、クライアント証明書の発行メールの送信や印刷画面の表示がされます。

【発行リンク】

ユーザ一覧の右端にある発行リンクをクリックすることで、ユーザに対してクライアント証明書を発行することができます。

発行完了後、『通知書をメール』『通知書をプリントアウト』をクリックすることで、クライアント証明書の発行メールの送信や印刷画面の表示がされます。また、『証明書のダウンロード』をクリックすることで、発行したクライアント証明書を PKCS#12 フォーマットでダウンロードします。

※ダウンロードした証明書には、インポート用のパスワードは設定されておりません。

※パスワードを設定する場合は、2.6 settings.conf 設定を参照ください。

3.3 クライアント証明書管理

発行したクライアント証明書の管理を行います。『失効』、『削除』、『通知書をメール』、『通知書をプリントアウト』、『証明書のダウンロード』と、証明書の詳細の確認を行います。

また、証明書のチェックボックスにチェックを入れて『一括失効』、『一括削除』、『一括ダウンロード』をすることも可能です。

【失効／一括失効】

クライアント証明書を失効すると、失効フラグが証明書 DB に付与され、クライアントが証明書を提出しても PKI 認証が通らなくなります。

※一度失効した証明書は使用可能に戻せません。

・エラーコード 53103

【削除／一括削除】

クライアント証明書を削除すると、証明書 DB からクライアント証明書を削除します。クライアントが証明書を提出しても PKI 認証が通らなくなります。

・エラーコード 53106

【証明書のダウンロード／一括ダウンロード】

クライアント証明書をダウンロードします。一括ダウンロードの場合は、証明書ファイルをまとめた zip ファイルをダウンロードできます。ダウンロードした証明書には、インポート用のパスワードは設定されておりません。

※パスワードを設定する場合は、2.6 settings.conf 設定を参照ください。

【有効期限】

クライアント証明書一覧の有効期限は、期限切れ 1 ヵ月前になると黄色、期限切れになると赤色に表示されます。

3.4 ユーザによるクライアント証明書の取得

発行したクライアント証明書は、管理画面にてダウンロードする以外にユーザ側でダウンロードすることができます。『ユーザ用のダウンロード画面』にアクセスしてダウンロードする方法と、クライアント証明書の自動発行機能でユーザ初回ログイン時に発行する『自動発行画面』からダウンロードする方法です。

【ユーザ用ダウンロード画面】
クライアント証明書の発行メールや印刷にダウンロード画面にアクセスするための URL が表示されます。その URL にアクセスし、ユーザログイン画面と同様にログインをすると、ダウンロード画面に遷移します。ユーザはダウンロード画面でインポート用のパスワードを入力することで、証明書をダウンロードできます。

【自動発行画面】
ポリシー設定でクライアント証明書の自動発行機能 ON かつ、発行タイミングがユーザ初回ログイン時の場合、ユーザが初回ログイン(もしくはクライアント証明書のダウンロードが完了していない場合)後に自動発行画面に遷移します。ユーザは自動発行画面でクライアント証明書を発行・ダウンロードすることができます。

ユーザが証明書をダウンロードした場合、その証明書にはインポート用のパスワードが設定されています。インポート用パスワードは、クライアント証明書の発行メールや印刷に記載されています。

3.5 クライアント証明書の登録方法

ダウンロードしたクライアント証明書を端末に登録する方法は、下記の Web ページに掲載しています。
ユーザにお知らせください。
https://www.passlogy.com/register_cert

3.6 クライアント証明書の削除方法

クライアント証明書を端末から削除する方法は、下記の Web ページに掲載しています。
ユーザにお知らせください。
https://www.passlogy.com/delete_cert

4 ユーザ管理者ガイド

4.1 ユーザ新規作成

PassLogic 管理ツールからユーザアカウントを手動登録する手順です。
＊LDAP サーバ連携の場合はユーザを手動登録する必要はありません。

【 設定手順 】
(ｉ)管理ツール左側メニュー ＞ ユーザ管理 ＞ 新規作成 をクリック
(ii)各項目 を入力し［次へ］をクリック
(iii)入力内容を確認し［登録］をクリック

【 項目解説 】

uid(必須)	ユーザ ID を入力します。使用できる文字は、半角英数(大文字小文字を区別する)と次の 3 つの記号です。(1-30 文字) .(ピリオド)-(ハイフン)_(アンダースコア)
ドメイン名	PassLogic 内で扱うドメイン名を選択します。
メールアドレス	ユーザ作成結果をメールで通知する場合は必須･最大 255 文字
氏名	最大 255 文字
社員番号	最大 255 文字
部署	最大 255 文字
電話	最大 255 文字
ポリシー	ポリシーを選択します。 *未指定の場合は Default Policy が適用されます。
グループ	グループ名を選択します。 *指定したグループに許可されている連携機能を利用できます。

シークレットパターン	シークレットパターンの初期値を指定します。 以下通知例*10 桁以上はアルファベット[A-Z]で、36 桁以上は[a-z]で表現します。 ■ログイン情報 ユーザID: user02 初期シークレットパターン: 1234 5678 9ABC DE** **** **** **** **** **** **** **** **** *「シークレットパターン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ます。生成時のルールは 2.2 章の設定に従います。
スタティックパスワード	ワンタイムパスワードの後に付加するスタティックパスワードの初期値を指定します。 *使用できる文字は、半角英数(大文字小文字を区別する)と以下の記号です。 _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < > (カンマとコロンは利用できません) *必須項目ではありません。未指定の場合パスワードはシークレットパターンだけになります。 *"random"と入力した場合は、ランダム生成します。生成時のルールは 2.2 章の設定に従います。
有効(必須)	ユーザアカウントの有効/無効を選択します。
有効期限	アカウントの有効期限日を設定します。
備考	最大 255 文字
SSL-VPN 機器登録	SSL-VPN 連携の際に PassLogic から RADIUS クライアントに対して、ユーザ毎に異なるアトリビュートを送信する必要がある場合、入力した値を利用することができます。
シングルサインオン	SSL-VPN 連携の際に PassLogic から対象機器に SSO する際に、ユーザ毎に異なるパラメータを送信する必要がある場合、入力した値を利用することができます。
WebSSO	WebSSO 連携の際に PassLogic から対象アプリケーションに対して、ユーザ毎に異なるパラメータを送信する必要がある場合、入力した値を利用することができます。

4.2 ユーザの端末固定

ポリシー設定にて端末固定を有効にした場合、対象ポリシーのユーザは1ユーザにつき最大5台の端末（ブラウザ）を固定することができます。1台目は初回ログイン認証が成功したときに自動的に端末固定が完了します。2台目以降の端末登録は下記の手順で追加してください。

＊端末固定の有効期限は最後の認証成功から 360 日間です。有効期限は認証成功の都度、更新されます。

【 端末登録手順 】

（ｉ）管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザ一覧 ＞ 該当 uid リンク をクリック

（ii）No.1～5 いずれかの 発行 リンクをクリック

（iii）メールアドレスと備考（任意の文字列・未入力可）を入力し［次へ］をクリック

＊初期表示されるメールアドレスはユーザ情報に登録されているメールアドレスです。

（iv）[発行]をクリック

（ｖ）[通知書をメール]をクリックすると新規端末登録用メールが iii で入力したメールアドレスに送信されます。[通知書をプリントアウト]をクリックするとメール送信する内容を画面表示します。

＊メールアドレスを登録しない場合は[通知書をメール]ボタンが表示されません。

（vi）ユーザが端末登録用 URL をクリックして認証成功後に端末登録が完了します。

4.3 ユーザー括登録、CSV ダウンロード

ユーザ情報を CSV 形式で一括入出力することができます。

【 一括登録手順 】

(ⅰ)管理ツール左側メニュー > ユーザ管理 > ユーザー括登録 をクリック

(ⅱ)[ファイルを選択] をクリックして取込みファイルを選択し [次へ] をクリック

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
フォーマット	[delflag],[uid],[domain],[uemail],[uname],[employee_number],[section],[phone],[policy],[group1],[group2],[group3],[group4],[group5],[udisabled],[uexpiry],[ucomment],[attribute1],[attribute2],[attribute3],[attribute4],[attribute5],[attribute6],[attribute7],[attribute8],[attribute9],[attribute10],[sslvpn param1],[sslvpn param2],[sslvpn param3],[sslvpn param4],[sslvpn param5],[sslvpn param6],[sslvpn param7],[sslvpn param8],[sslvpn param9],[sslvpn param10],[websso param1],[websso param2],[websso param3],[websso param4],[websso param5],[websso param6],[websso param7],[websso param8],[websso param9],[websso param10],[locked],[secret_pattern],[static_password]

(ⅲ)下記の設定および取込み内容を確認して [登録] をクリック

先頭行を項目名としてスキップ	先頭行を取込み対象外にする場合はチェックを入れてください。
通知書をメール	ユーザ新規作成と同時にメール通知をする際にはチェックを入れてください。メールアドレス情報の取込みが必須です。 *新規作成されるユーザに対するメール送信のみで、更新および削除されるユーザにはメール送信されません。

*一括登録処理は連続して実行できません。

*LDAP ID 同期実行中の場合は実行できません。自動実行の設定をしてある場合はご注意ください。

*ロックアウト状態(locked=1)で更新されたユーザのロックアウト時刻は CSV 取込時刻に更新され、自動ロック解除までの残り時間がリセットされます。

【 CSV ダウンロード手順 】

(ｉ)管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザー括登録 をクリック

(ii)[CSV ファイルをダウンロード] をクリック

【 CSV ファイルフォーマット 】

項目名		設定可能値	補足
delflag	削除 Flag	d	削除するユーザに d を設定
uid	uid(必須)	英数字、記号(-_.)	1～30 文字
domain	ドメイン(必須)	英数字、記号(-.)	PassLogic 管理ツールで登録した AD サーバの domain を指定 AD 非連携ユーザは固定値「local」を指定
uemail	メールアドレス	メールアドレスフォーマット	
uname	氏名	制限なし(*1)	
employee_number	社員番号		
section	部署		
phone	電話番号		
policy	ポリシー	英数字、記号(-_)	PassLogic 管理ツールで登録したポリシー名を指定できます。
group1	グループ 1	英数字、記号(-_)	PassLogic 管理ツールで登録したグループ名を指定できます。
group2	グループ 2		
group3	グループ 3		
group4	グループ 4		
group5	グループ 5		
udisabled	有効 0/無効 1	0/1	有効/無効
uexpiry	有効期限	yyyyMMdd yyyy/MM/dd yyyy-MM-dd	ユーザの有効期限。空欄の場合は期限切れなし。
ucomment	備考	制限なし(*1)	ユーザの備考
attribute1-10	SSL-VPN 機器 radius アトリビュート 1-10	制限なし(*1)	他のシステムと連係する際に利用する値です。

sslvpn param1-10	SSL-VPN 機器 シングルサインオン パラメータ 1-10	制限なし(*1)	他のシステムと連係する際に利用する値です。
websso param1-10	WebSSO パラメータ 1-10	制限なし(*1)	他のシステムと連係する際に利用する値です。
locked	ロックアウト	0 / 1	0:ロック解除 1:ロック状態
secret_pattern	シークレットパターン	カンマ区切りの数字(1～48) または"random" (*2, *4)	新規ユーザ登録時のみ使用。ダウンロード不可。
static_password	スタティックパスワード	英数字、記号(カンマ、コロン以外) または"random" (*3, *4)	新規ユーザ登録時のみ使用。ダウンロード不可。
lastauthdate	最終認証日時	yyyy/mm/dd hh:mm:ss	ダウンロード時のみ。インポート不可。
passsetdate	パスワード変更日時	yyyy/mm/dd hh:mm:ss	ダウンロード時のみ。インポート不可。

*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")

*2:"random"の場合は、ポリシー設定の「ランダム発行時の長さ(ワンタイムパスワード)」の長さでランダム生成します。

*3:"random"の場合は、ポリシー設定の「ランダム発行時の長さ(スタティックパスワード)」の長さでランダム生成します。

*4:シークレットパターンとスタティックパスワードのいずれも指定がない場合、新規登録ユーザのパスワードは、ポリシー設定の「ランダム発行時の長さ(ワンタイムパスワード)」の長さで指定したシークレットパターンをランダム生成します。但し、「ランダム発行時の長さ(ワンタイムパスワード)」が0のポリシーでは新規登録ユーザを作成できません。また、このときポリシー設定の「ランダム発行時の長さ(スタティックパスワード)」の設定に関わらずスタティックパスワードは生成されませんのでご注意ください。

*文字数の制限が記載されていない項目は最大 255 文字まで登録できます。

*ダウンロードした CSV ファイルを Microsoft Office Excel を使用して編集すると、データが破損してしまう場合があります。編集する際は、テキストエディタや CSV ファイル用エディタの使用を推奨します。

ユーザー一括登録(CSV ファイル取込処理)は、下記のコマンドで実行することができます。

コマンド例:

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

*コマンド実行後は設定ファイルと CSV ファイルは自動的に削除されます。

設定ファイル:

(例) /opt/passlogic/tmp/userimport_configfile

設定項目:

行数	設定値	
1	先頭行を項目名としてスキップ	1: スキップする / 0: スキップしない
2	通知書をメール	1: メール送信する / 0: メール送信しない
3	CSV カラム定義	下記 設定ファイルサンプル を参照してください。

設定ファイルサンプル:

```
1
1
delflag,uid,domain,uemail,uname,employee_number,section,phone,policy,group1,group2,group3,group4,group5,udisabled,uexpiry,ucomment,attribute1,attribute2,attribute3,attribute4,attribute5,attribute6,attribute7,attribute8,attribute9,attribute10,sslvpnsso1,sslvpnsso2,sslvpnsso3,sslvpnsso4,sslvpnsso5,sslvpnsso6,sslvpnsso7,sslvpnsso8,sslvpnsso9,sslvpnsso10,param1,param2,param3,param4,param5,param6,param7,param8,param9,param10,locked,secret_pattern,static_password
```

4.4 BASIC 認証情報の登録方法

BASIC 認証の際、PassLogic サーバがローカルアプリケーションに送信する認証情報の登録を行います。その為に CSV ファイルを作成し、**4.3 ユーザー括登録、CSV ダウンロード**で紹介したコマンド userimport.php を利用します。以下の例は、あるローカルアプリケーションのユーザ名とパスワードが、uid01,password の場合に、その認証情報をローカルドメインの user01 の param1 に登録する例です。

設定ファイル：

(例) /opt/passlogic/tmp/basic_auth_configfile

設定項目：

行数	設定値	
1	先頭行を項目名としてスキップ	1: スキップする / 0: スキップしない
2	ユーザごとのパラメータの暗号化	2: 暗号化して登録する
3	CSV カラム定義	下記 設定ファイルサンプル を参照してください。

設定ファイルサンプル

```
0
2
uid,domain,param1
```

CSV ファイルサンプル

(例) /opt/passlogic/tmp/basic_auth.csv

```
“user01”,”local”,”uid01:password”
```

コマンド例：

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

*コマンド実行後は設定ファイルと CSV ファイルは自動的に削除されます。

この例では、ローカルドメインの user01 は、BASIC 認証を設定したローカルアプリケーション(パスワードパラメータを param1 に指定)に SSO することができます。

4.5 ドメイン管理

PassLogic ユーザに適用するドメインを管理します。LDAP サーバで管理しているユーザ情報を、任意の PassLogic ドメインと紐付けて PassLogic データベースに取り込みます。

PassLogic ドメイン

【 ドメイン名 追加手順 】

(i)管理ツール左メニュー > ドメイン管理 > [追加]をクリック

(ii)任意のドメイン名を入力し [次へ] をクリック

(iii)入力内容を確認し [登録] をクリック

＊ ドメイン名は半角英数字、ピリオド、ハイフンのみ使用でき、最大 20 文字までです。

＊ 既に登録されているドメイン名と重複することはできません。

LDAP 認証連携

【 LDAP 認証連携定義 登録手順 】

(i)管理ツール左側メニュー > ドメイン管理 > LDAP 認証連携の列の [編集] をクリック

(ii)各項目 を入力し [次へ] をクリック

(iii)入力内容を確認し [登録] をクリック

＊ 一度 LDAP 認証連携定義を登録すると、LDAP ID 同期用のドメイン名として使用できなくなります。
間違って登録してしまった場合は、一度削除してから登録しなおして下さい。

＊ 確認画面に表示されるユーザ数は、Active Directory の MaxPageSize 設定値(デフォルト値 1000)が上限値になりますが、「ツリートップの DN」と「検索フィルタ」で該当するユーザ全てが連携対象となります。

＊ local ドメインは、LDAP 認証連携用のドメインとして使用することはできません。

＊ LDAP 認証連携を使用する場合は、settings.conf 設定でユーザ ID の大文字入力禁止設定を有効にされることをお勧めします。設定方法は「2.6 settings.conf 設定」の項を参照してください。

【 項目解説 】

LDAP サーバ接続設定	
LDAP タイプ	同期対象サーバにあわせて、ActiveDirectory または OpenLDAP のいずれかを選択します。
サーバ 1(必須)	同期対象サーバのホスト名 または IP アドレスを入力します。
サーバ 2	同期対象サーバがレプリケーション構成の場合はレプリケーションサーバのホスト名 または IP アドレスを入力します。 *サーバ 1 に接続できない場合はサーバ 2 に接続して同期します。
ポート番号	LDAP サーバのポート番号を入力します。 通常、LDAP は 389 で LDAPS は 636 です。
暗号化(LDAPS)	LDAPS で通信を行う場合に有効にします。
バインド DN	LDAP Search を行うためのバインド DN を入力します。 例:cn=administrator,cn=Users,dc=win2008,dc=passlogy,dc=com
バインドパスワード	バインドに必要となるパスワードを入力します。
ツリートップの DN	ターゲットオブジェクトの DN を入力します。 *指定した DN 配下のユーザが PassLogic を利用できます。 例:cn=Users,dc=win2008,dc=passlogy,dc=com
検索フィルタ	ターゲットオブジェクトのフィルタ条件を入力します。 例:(memberOf=CN=passlogic, CN=Users, dc=win2008,dc=passlogy,dc=com) *検索フィルタに該当するユーザが PassLogic を利用できます。 *AD 上の無効化されたユーザを対象外とする場合は下記を検索フィルタの条件に追加してください。 (!(userAccountControl:1.2.840.113556.1.4.803:=2))
Active Directory ドメイン名 または NT ドメイン名	Active Directory ドメイン名または NT ドメイン名を入力します。 Active Directory ドメイン名の例:win2008.passlogy.com NT ドメイン名の例:WIN2008 *「LDAP タイプ」が"ActiveDirectory"の場合は「uid@設定値」を RDN として AD 上のユーザを検索します。 *「LDAP タイプ」が"OpenLDAP"の場合は任意の文字列を登録してください。
デフォルトポリシー	LDAP 認証連携ユーザの初期ポリシーを選択 *初回ログイン時(初めて AD パスワード認証に成功したとき)に指定したポリシーが適用されます。2回目以降のログイン時に、ユーザ情報に設定されたポリシーを更新しません。

LDAP 属性値マッピング定義	
ユーザ ID(必須)	ユーザ ID に対応する LDAP アトリビュートを入力します。
メールアドレス(必須)	メールアドレスに対応する LDAP アトリビュートを入力します。
氏名	氏名に対応する LDAP アトリビュートを入力します。
社員番号	社員番号に対応する LDAP アトリビュートを入力します。
部署	部署に対応する LDAP アトリビュートを入力します。
電話	電話に対応する LDAP アトリビュートを入力します。
グループ1-5	ユーザ情報のグループ 1 から 5 に対応する LDAP アトリビュートを入力します。
有効期限	有効期限に対応する LDAP アトリビュートを入力します。 *ActiveDirectory 有効期限アトリビュート「accountExpires」はフォーマットが異なるため同期対象に指定することはできません。
備考	備考に対応する LDAP アトリビュートを入力します。
attribute1-10	ユーザ情報の SSL-VPN 機器 attribute1 から 10 に対応する LDAP アトリビュートを入力します。
sslvpn param1-10	ユーザ情報の シングルサインオン param1 から 10 に対応する LDAP アトリビュートを入力します。
websso param1-10	ユーザ情報の WebSSO param1 から 10 に対応する LDAP アトリビュートを入力します。

*アトリビュート値のデータフォーマットは、4.3 ユーザー括登録、CSV ダウンロード内の【CSV ファイルフォーマット】を参照してください。

*改行コードが含まれる値の LDAP アトリビュートは指定できません。

*PassLogic へのログイン(AD パスワード認証 成功)の都度、LDAP 属性値マッピング定義で指定した項目が更新されます。

*LDAP 属性値マッピング定義に指定された項目の値が空の場合は空の情報で上書きします。

LDAP 認証連携ユーザ削除スクリプト

PassLogic に追加されたユーザが LDAP サーバ上で削除された場合や検索フィルタで対象外となった場合に、下記のスクリプトを実行することでユーザを削除することができます。

コマンド:

```
# /usr/bin/php /opt/passlogic/apps/tools/passlogic_adsync.php
```

ログファイル:

/var/log/passlogic/passlogic_adsync.log

ログサンプル：

```
PassLogic データベースから削除すべきユーザがいた場合：
2014/12/16 15:24:23 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:24:23 user deleted., arumo0@passlogy.com, Delete user.(30003)
2014/12/16 15:24:23 user deleted., arumo1@passlogy.com, Delete user.(30003)
2014/12/16 15:24:23 Finish synchronizing users from Active Directory.(31102)

PassLogic データベースに削除すべきユーザがいない場合：
2014/12/16 15:29:56 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:29:56 Finish synchronizing users from Active Dir¥ectory.(31102)

PassLogic から AD にバインドできなかった場合：
2014/12/16 15:29:23 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:29:23 ldap bind error. domain=passlogy.com
2014/12/16 15:29:23 Finish synchronizing users from Active Directory.(31102)
```

*LDAP 認証連携対象の DN 定義を変更して連携対象外となったユーザは削除されます。
*認証サーバがレプリケーション構成で冗長化されている場合、1サーバでのコマンド実行結果が全認証サーバに反映されます。

グループマッピング

グループマッピング機能を利用することで、AD セキュリティグループと RADIUS 連携機器へ応答するアトリビュート値を紐づけることができます。グループマッピング機能は ActiveDirectory にのみ対応しています。

LDAP 認証連携ユーザが PassLogic にログインした時に、特定のセキュリティグループに所属していた場合、ユーザ情報 attribute1～10 に指定した値を割り当てます。

【 設定手順 】

（ｉ）管理ツール左側メニュー ＞ ドメイン管理 ＞ グループマッピング リンク をクリック
（ii）アトリビュート一覧画面［グループマッピング］をクリック
（iii）マッピングする AD セキュリティグループをチェック、紐づけるアトリビュート名をプルダウン（attribute1～10）から選択してユーザ情報に登録するアトリビュート値を入力して［次へ］をクリック
（iv）入力内容を確認し［登録］をクリック
（ｖ）優先順位を入力し［次へ］をクリック
（vi）内容を確認し［登録］をクリック

【 項目解説 】

アトリビュート値 指定画面

AD セキュリティグループ	値を割り当てる条件となる AD セキュリティグループを選択します。 *複数選択した場合は、選択した全てのグループに所属しているユーザだけが該当します。
PassLogic で割り当てるアトリビュート値	値を割り当てるアトリビュートをプルダウンから選択し、割り当てる設定値を入力します。

グループマッピング 一覧画面

優先順位	ユーザに適用するマッピング定義を判定するための優先順位を整数値で指定してください。 *優先順位 昇順に該当ユーザに適用するマッピング定義を決定します。

*ユーザの割り当て対象の attribute 値がすでに登録されていた場合は、マッピングに一致する内容に上書きされます。

*AD ユーザに設定されているプライマリグループは、所属している AD グループとして扱われません。

LDAP ID 同期

【 LDAP ID 同期定義 登録手順 】

(i)管理ツール左側メニュー > ユーザ管理 > LDAP ID 同期の列の［編集］をクリック

(ii)各項目 を入力し［次へ］をクリック

(iii)入力内容を確認し［登録］をクリック

＊ 一度 LDAP ID 同期定義を登録すると、LDAP 認証連携用のドメイン名として使用できなくなります。
間違って登録してしまった場合は、一度削除してから登録しなおして下さい。

【 項目解説 】

LDAP サーバ接続設定	
LDAP タイプ	同期対象サーバにあわせて、ActiveDirectory または OpenLDAP のいずれかを選択します。
サーバ 1(必須)	同期対象サーバのホスト名 または IP アドレスを入力します。
サーバ 2	同期対象サーバがレプリケーション構成の場合はレプリケーションサーバのホスト名 または IP アドレスを入力します。 ＊サーバ 1 に接続できない場合はサーバ 2 に接続して同期します。
ポート番号	LDAP サーバへ接続するポート番号を入力します。 未入力の場合は、LDAP だと 389 で LDAPS だと 636 が設定されます。
暗号化(LDAPS)	LDAPS で通信を行う場合に有効にします。
バインド DN(必須)	LDAP Search を行うためのバインド DN を入力します。
バインドパスワード（必須）	バインドに必要なパスワードを入力します。
ツリートップの DN（必須）	ターゲットオブジェクトの DN を入力します。 ＊指定した DN 配下のユーザが同期対象となります。
検索フィルタ(必須)	ターゲットオブジェクトのフィルタ条件を入力します。 ＊検索フィルタに該当するユーザが同期対象となります。 ＊ActiveDirectory の場合は無効化ユーザを対象外とする場合は下記のフィルタ条件を追加してください。 (!(userAccountControl:1.2.840.113556.1.4.803:=2))
LDAP サーバ同期設定	
同期モード	運用方法に合わせて下記のいずれかを選択します。 ＜追加･更新＞ PassLogic に未登録のユーザを追加し、登録済みユーザは属性値マッピング定義で指定された項目を上書き更新します。 ＜追加･更新･削除＞ 「追加･更新」モードの動作に加え、LDAP サーバ検索結果に存在しない PassLogic ユーザは削除されます。

メール送信	チェック状態にすると、追加ユーザのメールアドレスに対象ユーザのポリシーに指定された「新規ユーザ送信メール」を送ります。 *メールアドレスの属性値マッピングを指定しない場合、および対象ユーザのメールアドレスが未登録の場合は送信されません。
同期間隔	運用方法に合わせて下記のいずれかを選択します。 ＜毎日1回指定時刻に実行＞ 毎日指定した時刻に同期処理を実行します。 ＜指定した時間おきに実行＞ 10 分ごと：毎時 00, 10, 20, 30, 40, 50 分に同期処理を実行します。 20 分ごと：毎時 00, 20, 40 分に同期処理を実行します。 30 分ごと：毎時 00, 30 分に同期処理を実行します。 60 分ごと：毎時 00 分に同期処理を実行します。 *同期処理実行中に次の同期処理が始まらないように時間間隔を設定してください。 ＜自動実行しない＞ 自動実行は行いません。 *LDAP 同期定義を登録後に[いますぐ実行]ボタンをクリックして手動で同期することができます。 *同一ドメインに対し同期処理を並行して実行することはできません。同期処理実行中は /opt/passlogic/tmp/ 以下に、ロックファイルがドメイン毎に作成されます。ロックファイルを削除するか、作成から5分以上経過すると同期処理を実行できます。 *冗長構成をとっている場合、同期の自動実行は片側だけ実施することを推奨します。両側で行う場合は、異なる時間帯で実施するよう設定する必要があります。
LDAP 属性値マッピング定義	
ユーザ ID（必須）	ユーザ ID に対応する LDAP アトリビュートを入力します。
メールアドレス	メールアドレスに対応する LDAP アトリビュートを入力します。
氏名	氏名に対応する LDAP アトリビュートを入力します。
社員番号	社員番号に対応する LDAP アトリビュートを入力します。
部署	部署に対応する LDAP アトリビュートを入力します。
電話	電話に対応する LDAP アトリビュートを入力します。

ポリシー	ポリシーに対応するLDAPアトリビュートを入力します。 *未指定の場合は デフォルト値 に選択したポリシーが適用されます。 *デフォルト値「--」は、ポリシー定義「Default Policy」に対応します。 *適用されるポリシーは「ランダム発行時の長さ(ワンタイムパスワード)」に1以上の整数値を登録してください(LDAP ID 同期の新規登録ユーザの初期パスワードはこの設定値に従うため)。なお、LDAP ID 同期で新規登録されるユーザのスタティックパスワードは生成されませんのでご注意ください。
グループ1-5	ユーザ情報のグループ 1 から 5 に対応するLDAPアトリビュートを入力します。
有効期限	有効期限に対応するLDAPアトリビュートを入力します。 *ActiveDirectory 有効期限アトリビュート「accountExpires」はフォーマットが異なるため同期対象に指定することはできません。
備考	備考に対応するLDAPアトリビュートを入力します。
attribute1-10	ユーザ情報の SSL-VPN 機器 attribute1 から 10 に対応するLDAPアトリビュートを入力します。
sslvpn param1-10	ユーザ情報の シングルサインオン param1 から 10 に対応するLDAPアトリビュートを入力します。
websso param1-10	ユーザ情報の WebSSO param1 から 10 に対応するLDAPアトリビュートを入力します。

*アトリビュート値のデータフォーマットは、4.3 ユーザー括登録、CSV ダウンロード内の【CSV ファイルフォーマット】を参照してください。

*改行コードが含まれる値のLDAPアトリビュートは指定できません。

*未指定の項目は同期対象外となり同期実行時に上書き更新しません(ユーザ ID とポリシーは除く)。

*指定された項目の値が空の場合は空の情報が上書きされます。

*ActiveDirectory の MaxPageSize(初期値 1000)を上回るユーザ数の同期処理に対応していません。同期対象ユーザ数より大きな値を ActiveDirectory に設定してください。

*ActiveDirectory、OpenLDAP ともに 2 万件までの同期処理が実行できることを検証済みです。

*PassLogic 認証サーバを冗長化している場合は、いずれか1つの PassLogic 認証サーバにだけ LDAP ID 同期設定を登録してください。

4.6 ロックの解除方法

パスワード連続失敗回数に到達、または管理者によって強制的にロック・アウトされたユーザは、ユーザー覧画面 ロック項目 の背景が赤くなり 「ロック解除」と表示されます。ロック解除の文字をクリックすることでロック・アウト状態を解除できます。

4.7 パスワード再発行

PassLogic 認証ポリシーに属するユーザがパスワードを忘れた場合、管理者がパスワードを再発行することができます。

【 パスワード再発行手順 】

（ｉ）管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザー覧 をクリック

（ii）対象ユーザの パスワード再発行 リンクをクリック

（iii）各項目 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

（ｖ）[通知書をメール]をクリックするとパスワード再発行メールが iii で入力したメールアドレスに送信されます。[通知書をプリントアウト]をクリックするとメール送信する内容を画面表示します。

*メールアドレスを登録しない場合は[通知書をメール]ボタンが表示されません。

（vi）ユーザは再発行パスワードでログインすることができます。

*対象ユーザの属するポリシー「初回パスワード変更を強制」が「Yes」に設定されている場合、再発行パスワードでログインしたときに、強制的にパスワード変更を要求されます。

【 項目解説 】

メールアドレス	再発行したパスワードをここで入力したメールアドレス宛に送信します。 *入力したメールアドレスがユーザ情報のメールアドレスとして上書き更新されます。
シークレットパターン	シークレットパターンを指定します。 *「シークレットパターン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ます。
スタティックパスワード	ワンタイムパスワードの後に付加するスタティックパスワードを指定します。 *必須項目ではありません。未指定の場合パスワードはシークレットパターンだけになります。

4.8 PassClip リセット

PassClip 認証ポリシーのユーザが PassClip アプリをリセット(再アクティベート)する場合は、管理者が PassClip アクティベート URL を発行します。

【 PassClip リセット手順 】

(i)管理ツール左側メニュー > ユーザ管理 > ユーザー覧 をクリック

(ii)対象ユーザの PassClip リセット リンクをクリック

(iii)メールアドレスを入力し [次へ] をクリック

*ユーザ情報に登録されているメールアドレスが初期表示されます。

*ここで登録したメールアドレスがユーザ情報のメールアドレスとして上書き更新されます。

(iv)入力内容を確認し [登録] をクリック

(v)[通知書をメール]をクリックすると PassClip 再セットアップメールが iii で入力したメールアドレスに送信されます。[通知書をプリントアウト]をクリックするとメール送信する内容を画面表示します。

*メールアドレスを登録しない場合は[通知書をメール]ボタンが表示されません。

(vi)ユーザが PassClip アプリをインストールした端末でアクティベート URL にアクセスすると、PassClip に PassLogic ログイン用スロットが追加されます。

4.9 管理者用パスワードの変更

管理ツール左側メニュー >パスワード変更 にて、管理ツールにログイン中の自身の管理者アカウントのパスワードを変更できます。

*Default Policy に設定したパスワードポリシーに則ったパスワードに変更することができます。

5 ユーザガイド

5.1 ユーザのパラメータ設定

ポリシー設定にて、パラメータ設定機能の利用を許可した場合、ユーザログイン後の～/ui/menu.php にて、「設定(デフォルトの場合)」押下後の画面上で、許可したパラメータの値を変更できます。

【 項目解説 】

項目名		入力制限	補足
ユーザ編集画面＞ SSL-VPN 機器登録	attribute1-10	最大 255 文字	管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザ一覧 対象ユーザのデータと紐付いています。
ユーザ編集画面＞ シングルサインオン	param1-10	最大 255 文字	管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザ一覧 対象ユーザのデータと紐付いています。
ユーザ編集画面＞ WebSSO	param1-10	最大 255 文字	管理ツール左側メニュー ＞ ユーザ管理 ＞ ユーザ一覧 対象ユーザのデータと紐付いています。
本人のみ編集可能な情報 (管理者変更不可)	password1-5	最大 159 バイト (全角1文字 3 バイト)	管理者でも閲覧･変更不可の値です。ユーザ本人のみ閲覧･変更可能値です。

*表示されている項目名の name はポリシー設定にて、設定した名称になります。

6 注意事項

6.1 PassLogic for Windows Desktop の制限事項

以下のことを PassLogic for Windows Desktop で行うことはできません。

＊ PKI 認証ポリシーのユーザのログオン制御
PKI 認証機能が有効なポリシーのユーザでログオンする場合、証明書を要求することなくログオンします。

＊ ゲスト PC のリモートデスクトップ(RDP)アプリでのアクセス認証
ゲスト PC の RDP アプリからホスト PC へのアクセス認証は、Windows 標準認証となります。
初回アクセス認証成功後、ホスト PC のログオン画面が表示され、これ以後のログオン認証は本製品が適用されます。

＊ PassLogic GW サーバ経由での動作
インストール設定ファイルの認証サーバ URL に PassLogic 認証サーバ API の URL をご指定ください。

＊ AD の ID 認証連携での初回ログオン不可
本製品で PassLogic 認証を行う際、ユーザが PassLogic サーバに登録されている必要があります。
AD の ID 認証連携設定されている場合は、以下いずれの方法で事前にユーザを登録する必要があります。
① ユーザー括登録機能を利用してユーザを登録。
② PassLogic サーバ UI でログイン成功。

＊ PassClip(PassClip L)認証ポリシーのユーザのログオン
該当認証ポリシーのユーザでログオンする場合、「システムエラーが発生しました」のダイアログが表示されます。

＊ PassLogic for Windows Desktop を用いた PassLogic パスワードの変更
Ctrl+Alt+Del キー押しで「パスワード変更」では、通常の Windows パスワード変更となります。
PassLogic パスワードの変更は、PassLogic サーバ UI にログインしてから変更を行ってください。

＊ オフライン認証データの有効期限設定
オフライン認証データに有効期限はなく、保存件数分の認証を行えます。
サーバ管理者が必要に応じて、オフライン認証データ件数(デフォルトで 1000 件)で調整してください。

＊ ログオン端末特定
PassLogic サーバではログオン端末を特定する情報を記録していません。

6.2 PassClip、PassClip L 利用時の注意点

＊ PassClip 認証方式ポリシーを使用するユーザについては、ユーザ作成時に、ポリシーで PassClip 認証方式をご選択ください。運用中の PassLogic 認証方式を設定しているユーザのポリシーを、PassClip 認証方式のポリシーに変更することはできません。

＊ PassClip がインストールされている端末と、PassLogic がインストールされているサーバの時刻を合わせておく必要があります。時刻が違う場合、認証に失敗します。

＊ 以下の条件を満たす場合、ワンタイムパスワードの桁数に奇数桁は使用できません。

① PassClip のバージョンが 2.1.2 以前、または PassClip L のバージョンが 1.0.2。

② ポリシーで PassClip 認証方式の「表示形式」がベーシック表示。

＊ PassClip アプリのダウンロード用 URL は下記の通りです。

・iOS 版 PassClip L

https://itunes.apple.com/jp/app/id1167322433?mt=8

・Android 版 PassClip L

https://play.google.com/store/apps/details?id=com.passlogy.passclip.local

＊ PassClip アプリのヘルプページ URL は下記の通りです。初回利用開始の案内メール等でご活用ください。なお、同一の内容が PassClip アプリ内から閲覧可能です。

https://www.passclip.com/ja/help_for_passclip_l

6.3 LDAP 認証連携のグループマッピング利用時の注意点

＊ 今後のバージョンアップで、機能削除を予定しています。

7 ログ・リファレンス

7.1 ログ・リファレンス

code	level	message
10099	warning	Invalid mode.
30001	notice	Create user.
30002	notice	Edit user.
30003	notice	Delete user.
30004	notice	User locked out.
30005	notice	User unlocked.
30006	notice	User activated.
30007	notice	User inactivated.
30008	notice	Recreated user password.
30009	notice	Reset PassClip secret.
30011	info	The user already exists.
30012	notice	The user does not exist.
30101	notice	Password reminder e-mail has been sent.
30102	notice	User reset password.
30103	notice	Password reset e-mail has been sent.
30111	err	User does not exist.
30112	err	E-mail address is incorrect.
30113	err	Failed to send password reminder e-mail.
30114	err	Password reminder use is not allowed.
30119	err	Database Transaction Error.
30121	err	URL key is not valid.
30122	err	URL key is expired.
30123	err	User has no e-mail address.
30124	err	Failed to recreate a new secret pattern.
30125	err	Failed to send a new secret pattern e-mail.
30126	err	Password reminder use is not allowed.
30129	err	Database Transaction Error.
31012	notice	Invalid input data.
31014	err	Failed to send e-mail.
31015	err	E-mail address is not set.
31094	emerg	Over maximum number of users.

31097	emerg	The license is expired.
31101	notice	Start synchronizing users from Active Directory.
31102	notice	Finish synchronizing users from Active Directory.
31111	err	LDAP connection error occurred.
31112	err	The LDAP does not support the protocol version 3.
31113	err	The LDAP connection cannot set off to the referral options.
31114	err	LDAP bind error occurred.
31115	err	LDAP search error occurred.
31116	err	LDAP get entries error occurred.
31201	notice	Start exporting user data to PassLogic from LDAP.
31202	notice	Finish exporting user data to PassLogic from LDAP.
31211	err	LDAP Definition has not been specified.
31212	err	The LDAP Definition does not exist.
31213	err	LDAP connection error occurred.
31214	err	The LDAP does not support the protocol version 3.
31215	err	The LDAP connection cannot set off to the referral options.
31216	err	LDAP bind error occurred.
31217	err	LDAP search error occurred.
31218	err	LDAP get entries error occurred.
31301	notice	Start importing user data to PassLogic from CSV.
31302	notice	Finish importing user data to PassLogic from CSV.
31303	warning	User import process is running.
31999	err	Database Transaction Error.
32001	notice	Retrieve backup file.
32002	notice	Restore system from backup file.
32003	notice	Restore database from backup file.
32004	notice	Restore configuration from backup file.
32010	notice	Retrieve technical support file.
33001	notice	Standard data fetch start.
33002	notice	Standard data fetch end.
33010	notice	Exists user.
33011	notice	Update error user.
33012	notice	Failed to open passlogicdata.
34001	notice	Start send email to password expiring user.
34002	notice	Finish send email to password expiring user.
34003	err	Password expiration date is unlimited.
34004	err	Invalid email notification settings.

34005	err	Incorrect email notification settings.
34006	err	Days must be a lower number than the validity period.
34007	notice	Successed to send e-mail.
34008	err	Email address is not registered.
40001	notice	Done trim(param1).
40002	notice	Done trim(param2).
40003	notice	Done trim(param3).
40004	notice	Done trim(param4).
40005	notice	Done trim(param5).
40006	notice	Done trim(param6).
40007	notice	Done trim(param7).
40008	notice	Done trim(param8).
40009	notice	Done trim(param9).
40010	notice	Done trim(param10).
40011	notice	Done trim(group1).
40016	notice	Done trim(name).
40017	notice	Done trim(email).
40018	notice	Done trim(comment).
40019	notice	Done trim(apppass).
40100	notice	Invalid input data(uid).
40101	notice	Invalid input data(group1).
40102	notice	Invalid input data(email).
40103	notice	Invalid input data(uexpiry).
40104	notice	Invalid input data(group).
50100	err	Invalid input data.
50101	err	The user does not exist.
50200	info	User information is retrieved successfully.
50300	err	Invalid input data.
50301	err	The user does not exist.
50302	err	Update parameter is required.
50400	notice	User information has updated successfully.
50499	crit	System error occurred.
51100	err	Invalid input data.
51200	notice	Create ticket.
51299	crit	System error occurred.
52100	err	Invalid input data.
52101	err	AD authentication is rejected.

52102	notice	AD authentication is accepted.
52103	err	The uid including uppercase is not allowed. Input lowercase uid.
52109	crit	LDAP/AD server is failed.
52199	crit	System error occurred.
52200	notice	Create random number.
52201	notice	Create dummy random number.
52300	err	Invalid input data.
52399	crit	System error occurred.
52400	notice	Create random number.
52401	notice	Create dummy random number.
53100	notice	PKI Authentication is accepted.
53101	warning	No Certification.
53102	warning	Client Certification is wrong.
53103	warning	Client Certification has been revoked.
53104	warning	The certification user is incorrect.
53105	warning	PKI is Unset.
53106	warning	No certification serial is incorrect.
53107	warning	The certification is expired.
53110	notice	RADIUS-EAP is accepted.
53111	warning	RADIUS-EAP is rejected.
53200	notice	PKI setting is updated.
53201	warning	PKI setting update is failed.
54100	err	Invalid input data.
54101	warning	Random number is expired. Please retry.
54102	warning	User has been expired. Please contact your administrator.
54103	warning	User is not permitted. Please contact your administrator.
54104	warning	Access is not allowed.
54105	warning	User is locked. Please contact your administrator.
54106	warning	The uid or password you entered is incorrect.
54109	warning	Failed to find the authentication box.
54150	err	Invalid input data.
54151	warning	Invalid browser.
54152	notice	Udid check success.
54199	crit	System error occurred.
54200	notice	User is required to change current password.
54201	notice	PassLogic Authentication success.
54300	err	Invalid input data.

54301	warning	Random number is expired. Please retry.
54302	warning	User has been expired. Please contact your administrator.
54303	warning	User is not permitted. Please contact your administrator.
54304	warning	Access is not allowed.
54305	warning	User is locked. Please contact your administrator.
54306	warning	The uid or password you entered is incorrect.
54307	warning	The pid is incorrect.
54399	crit	System error occurred.
54400	notice	User is required to change current password.
54401	notice	PassLogic Windows Authentication success.
54402	notice	Password expiry is nearing.
54500	err	Invalid input data.
54501	warning	The pid is incorrect.
54597	crit	System error occurred.
54598	crit	System error occurred.
54599	crit	System error occurred.
54600	notice	Offline data sent.
54700	err	Invalid input data.
54701	warning	The pid is incorrect.
54711	notice	Password changing is possible.
54712	notice	Password changing is possible.
54721	notice	Password changing is possible.
54722	notice	Password changing is possible.
54797	crit	System error occurred.
54798	crit	System error occurred.
54799	crit	System error occurred.
54800	err	Invalid input data.
54801	warning	The pid is incorrect.
54803	warning	The password length is not allowed.
54804	warning	The pattern is not allowed. Please setup a different pattern.
54805	warning	It is not allowed to set the same password in the past.
54897	crit	System error occurred.
54898	crit	System error occurred.
54899	crit	System error occurred.
54900	notice	Password has been changed.
55100	warning	Invalid input data.
55101	warning	RADIUS Authentication is rejected.

55102	warning	Random number is expired. Please retry.
55103	warning	User is locked.
55104	warning	User is not permitted.
55105	warning	There is no Random Number.
55106	warning	The user does not exist.
56100	warning	Invalid input data.
56101	warning	RADIUS Authentication is rejected.
56200	notice	RADIUS Authentication is accepted.
57100	warning	Invalid input data.
57101	warning	Session ID is invalid. Please start again from the beginning.
57102	warning	The secret pattern is not identified.
57103	warning	The password length is not allowed.
57104	warning	The pattern is not allowed. Please setup a different pattern.
57105	warning	It is not allowed to set the same password in the past.
57106	warning	The password is invalid.
57199	err	Database Transaction Error.
57200	notice	Changing password process.
57201	notice	Changing password is cancelled.
57202	notice	Password has been changed.
59999	err	Database Transaction Error.
70100	err	Invalid input data.
70102	warning	User has been expired. Please contact your administrator.
70103	warning	User is not permitted. Please contact your administrator.
70104	warning	Access is not allowed.
70105	warning	User is locked. Please contact your administrator.
70106	warning	The uid or password you entered is incorrect.
70107	warning	Failed to find the secret code.
70199	crit	System error occurred.
70201	notice	PassClip Authentication success.
80401	notice	SAML Certificate File uploaded.
80402	notice	SAML Private Key File uploaded.
80409	warning	Failed to File upload.
80411	notice	PKCS12 File uploaded.
80419	warning	Failed to create a PKCS12 File.
91101	notice	Start importing user data to PassLogic from CSV.
91102	notice	Finish importing user data to PassLogic from CSV.
91199	err	Database Transaction Error.

7.2 ログファイル

PassLogic アプリケーションログ

管理ツール ログ閲覧 に表示されるログと同じ内容が出力されます。
ログ閲覧に表示されるログの期間は 1 年間で、それより古いものは削除されます。

ファイルパス	/var/log/passlogic/passlogic.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic （定義内容の変更可能・アンインストール時に削除されます）

pgpool ログ

pgpool プロセスの開始・停止ログとデータベース障害ログが出力されます。

ファイルパス	/var/log/passlogic-pgpool/pgpool.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic-pgpool （定義内容の変更可能・アンインストール時に削除されます）

PostgreSQL アーカイブ消去ログ

PostgreSQL のアーカイブログファイルのうち不要となったファイルを削除する処理のログが出力されます。

ファイルパス	/var/log/passlogic/passlogic_archivecleanup.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic （定義内容の変更可能・アンインストール時に削除されます）

アーカイブログファイルの削除処理は /etc/cron.daily/passlogic-archivecleanup.cron に登録されています。

LDAP 認証連携ユーザ削除ログ

LDAP 認証連携ユーザ削除スクリプトの実行ログが出力されます。

ファイルパス	/var/log/passlogic/passlogic_adsync.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic （定義内容の変更可能・アンインストール時に削除されます）

LDAP 認証連携ユーザ削除スクリプトは 手動コマンド実行 または cron による定期実行で行ってください。