

インストール・運用管理ガイド

PassLogic 認証サーバソフトウェア

ver.3.8

本書について

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

表示画面

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

商標および免責事項

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

版權/注意

- 本書の内容の一部または全部を無断で複写転載することを禁じます。
- 本書に掲載の内容及び製品の仕様などは、予告なく変更されることがあります。
- 本書の内容は万全を期して作成しておりますが、万一ご不明な点や誤り、記載漏れ、乱丁、落丁などお気づきの点がございましたら、弊社までご連絡ください。

特許/ Patent

本製品は米国及び日本にて下記の特許を取得しています。

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

免責事項

- 2014 年 2 月 17 日現在の情報です。

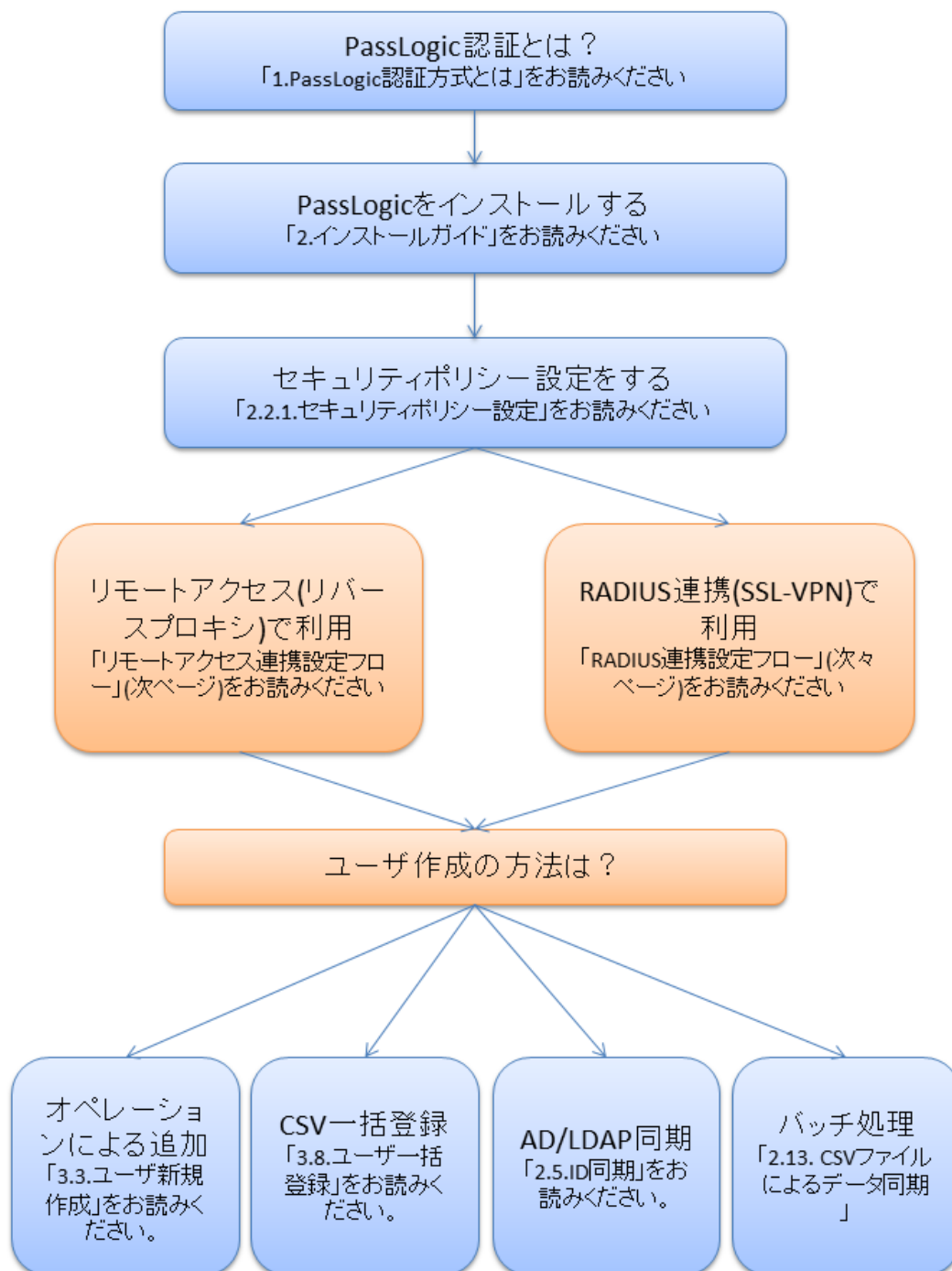
目次

1. PassLogic 認証方式とは？	- 9 -
2. インストールガイド	- 11 -
2.1. 動作環境	- 11 -
2.2. SSL 証明書のインストールについて	- 11 -
2.3. ウィルス対策ソフトを利用する場合	- 11 -
2.4. 最少ハードウェアスペック	- 11 -
2.5. 推奨ブラウザ	- 12 -
2.6. ユーザインターフェースの言語について	- 12 -
2.7. 使用通信ポート	- 12 -
2.8. 必要な rpm パッケージをインストールする	- 14 -
2.9. PassLogic をインストールする	- 16 -
2.9.1. インストール時の設定	- 16 -
2.9.2. タイムゾーンの設定	- 18 -
2.10. 管理画面にアクセスする	- 18 -
2.11. ライセンスを登録（更新）する	- 18 -
2.12. アップデート	- 19 -
2.12.1. アップデート時の注意	- 19 -
2.12.2. 問題が発生した際のリカバリの方法	- 19 -
2.12.3. バージョン 3.3.2 以前からのアップデート	- 20 -
2.12.4. バージョン 3.4.2 以前から 3.4.5 へのアップデート	- 20 -
2.12.5. バージョン 3.5.1 以前からのアップデート	- 20 -
2.12.6. バージョン 3.6.0 以前からのアップデート	- 20 -
2.12.7. バージョン 3.7.0 以前からのアップデート	- 20 -
2.13. アンインストール	- 21 -
3. システム管理者ガイド	- 22 -
3.1. 管理者アカウントを作成する	- 22 -
3.1.1. 管理者追加	- 22 -
3.1.2. 管理者一覧	- 23 -
3.1.3. オペレーター一覧	- 23 -
3.2. PassLogic 設定	- 23 -
3.2.1. セキュリティポリシー設定	- 23 -
3.2.2. メール設定	- 26 -
3.2.3. ユーザ通知設定	- 26 -
3.2.4. ログ・その他設定	- 27 -

3.3.	リモートアクセス管理	- 27 -
3.3.1.	アクセス先 URL	- 29 -
3.3.2.	ポリシー設定	- 29 -
3.3.3.	アプリケーション設定 (PC / 携帯)	- 30 -
3.3.4.	URL マッピング	- 31 -
3.3.5.	各アプリケーションの設定例	- 31 -
3.3.6.	http ヘッダ連携	- 32 -
3.3.7.	WebSSO	- 33 -
3.3.8.	SAML 連携	- 40 -
3.3.9.	グラフィックデザインのカスタマイズ	- 41 -
3.4.	RADIUS 連携	- 44 -
3.4.1.	RADIUS 認証動作	- 44 -
3.4.2.	RADIUS クライアント登録	- 45 -
3.4.3.	ユーザインターフェース	- 45 -
3.4.4.	ユーザインターフェースで target の値を URL に含める方法	- 48 -
3.4.5.	Web トークン	- 49 -
3.4.6.	グラフィックデザインのカスタマイズ	- 50 -
3.4.7.	トラブル・シューティング	- 50 -
3.4.8.	RADIUS ログの確認方法	- 51 -
3.5.	ID 同期	- 51 -
3.5.1.	LDAP 設定	- 51 -
3.5.2.	OpenLDAP	- 53 -
3.5.3.	ActiveDirectory	- 53 -
3.5.1.	LDAP 同期	- 54 -
3.5.2.	ActiveDirectory で 1000 件以上同期する場合	- 54 -
3.6.	ログ閲覧	- 58 -
3.7.	バックアップ/リストア	- 58 -
3.7.1.	バックアップ	- 59 -
3.7.2.	リストア	- 59 -
3.8.	サポートに必要なファイルを取得する	- 59 -
3.9.	管理者パスワードの変更	- 59 -
3.10.	サーバの再起動をとまなう設定変更	- 59 -
3.10.1.	httpd の再起動	- 60 -
3.10.2.	httpd および radiusd の再起動	- 60 -
3.11.	PassLogic 認証サーバをイントラネットに配置する	- 60 -
3.11.1.	認証サーバとゲートウェイサーバを分離した場合の注意点	- 60 -

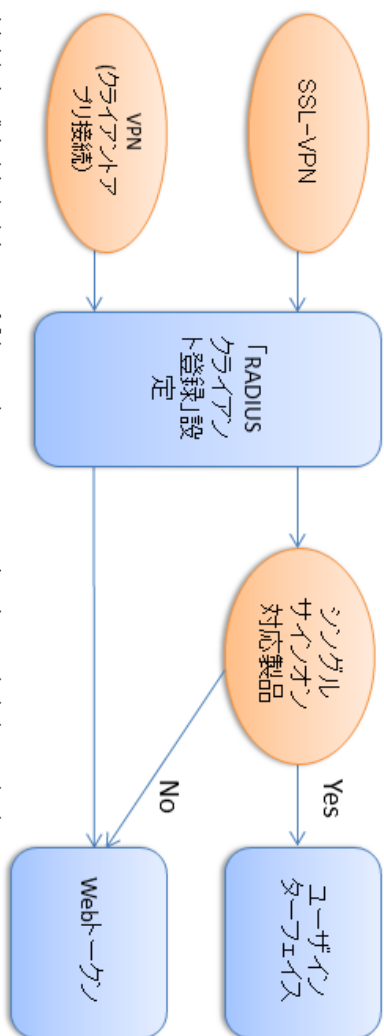
3.11.2.	認証サーバ(192.168.0.10)側の設定	- 61 -
3.11.3.	ゲートウェイサーバ(202.18.xxx.10)側の設定.....	- 61 -
3.12.	複数の端末固定デバイス(Cookie 制限)を登録する方法	- 62 -
3.13.	パスワードリマインダの利用方法	- 62 -
3.14.	PassLogic 管理ツールの設定項目	- 62 -
3.15.	CSV ファイルによるデータ同期	- 64 -
3.16.	バックアップ対象ファイル	- 65 -
3.17.	監視対象プロセス	- 66 -
3.18.	動作確認および死活監視について	- 66 -
3.19.	管理者(admin)パスワードのリセット方法	- 67 -
4.	ユーザー管理者ガイド	- 67 -
4.1.	管理ツールにアクセスする	- 67 -
4.1.1.	管理ツールログイン用のユーザ ID を入力する	- 67 -
4.1.2.	管理ツールログイン用のパスワードを入力する	- 69 -
4.2.	PassLogic の状態を確認する	- 70 -
4.2.1.	PassLogic のバージョンを確認する	- 71 -
4.2.2.	登録されているライセンス情報を確認する	- 71 -
4.2.3.	PassLogic サーバのステータスを確認する	- 71 -
4.3.	ユーザ作成	- 72 -
4.3.1.	新規作成	- 72 -
4.3.2.	デバイス追加	- 73 -
4.4.	ユーザー一覧	- 74 -
4.5.	ロックユーザー一覧	- 74 -
4.6.	同期対象外ユーザー一覧	- 74 -
4.7.	ユーザ検索	- 74 -
4.8.	ユーザー一括登録	- 75 -
4.8.1.	CSV ファイルのダウンロード	- 76 -
4.9.	ユーザサポートについて	- 76 -
4.9.1.	ユーザアカウントがロックされた場合のサポート	- 76 -
4.9.2.	ユーザがパスワードを忘れた場合のサポート	- 77 -
4.9.3.	通知メールが届かない場合のサポート	- 78 -
4.9.4.	System error occurred. Please contact system administrator.....	- 78 -
4.10.	ログ・リファレンス	- 79 -
4.10.1.	ログフォーマット	- 79 -
4.10.2.	ログ：ステータスリファレンス	- 79 -
4.10.3.	ログのサイズ	- 83 -

目的別インデックス



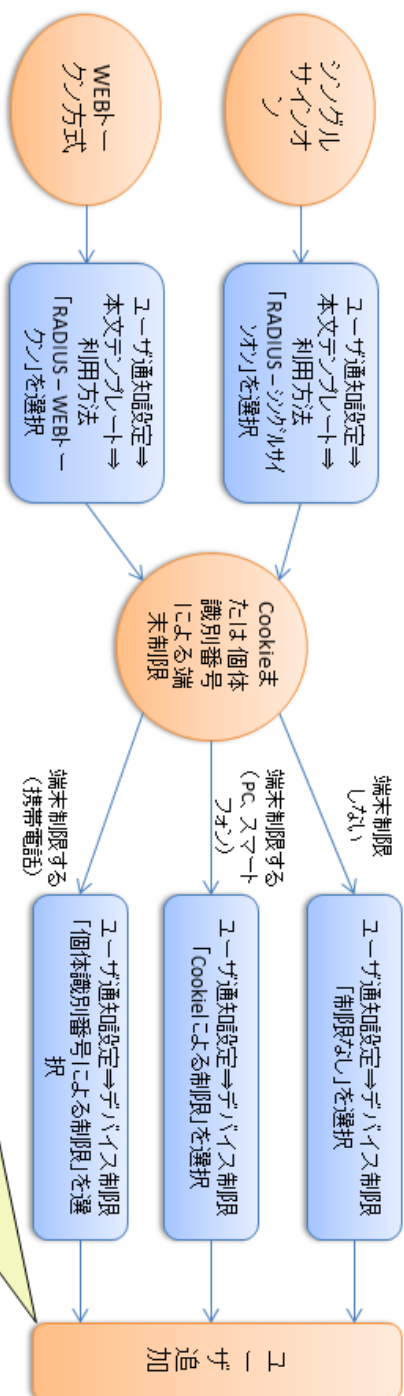
RADIUS連携設定フロー

1. 連携する機器に応じて、設定を行います。



※シングルサインオン対応製品でも、Web-VPN方式で接続できますので、ユーザーサインインゲートウェイの設定を行う前に、Web-VPN方式で接続できることをご確認ください。

2. 接続方式と端末制限の種類に応じて、ユーザー通知設定を行います。



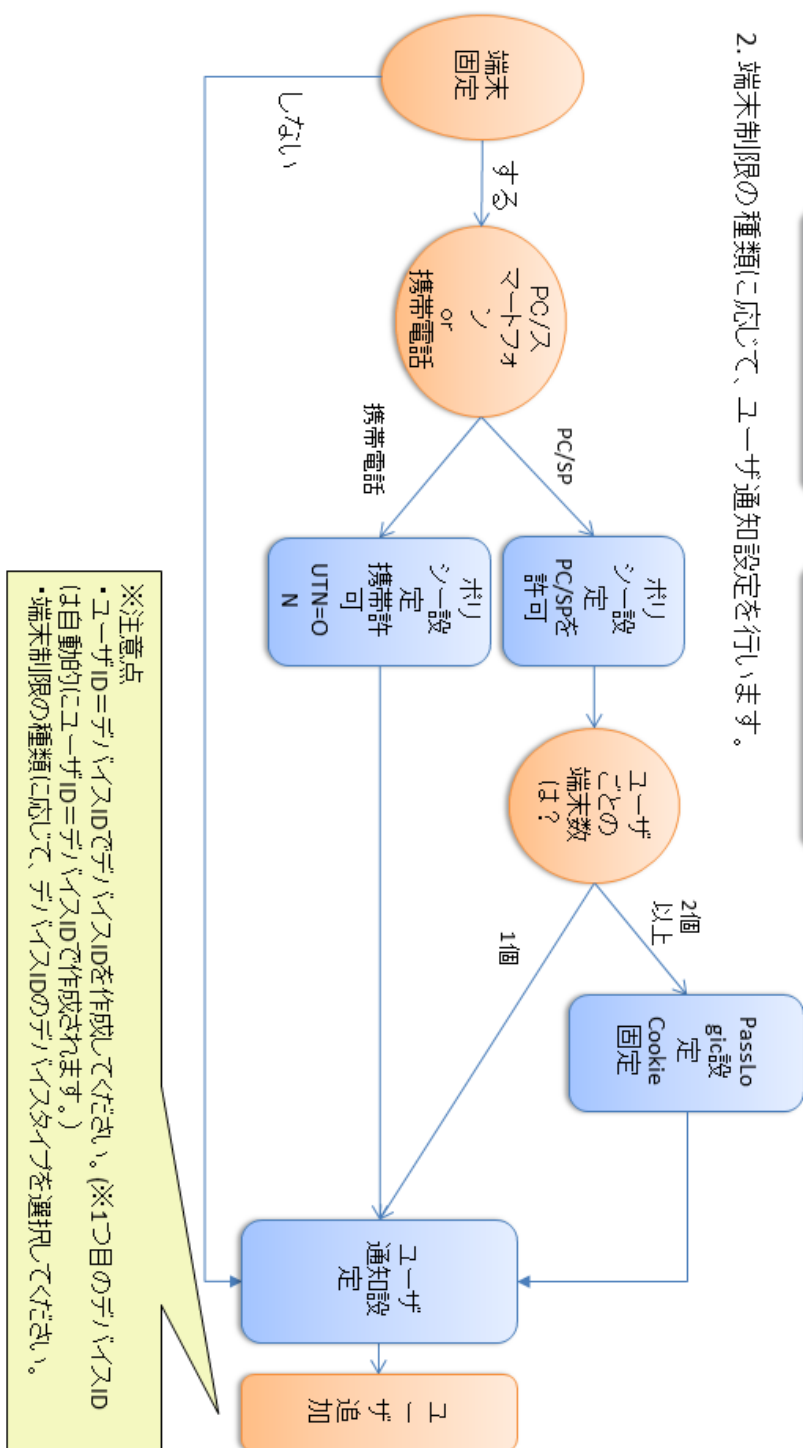
※注意
点
・シングルサインオン方式では、ユーザーID=デバイスIDでデバイスIDを作成してください。(*1つ目のデバイスIDは自動的にユーザーID=デバイスIDで作成されます。)
・端末制限の種類に応じて、デバイスIDのデバイスタイプを選択してください。

リモートアクセス連携設定フロー

1. 連携Webアプリケーションセッションに応じて、設定を行います。



2. 端末制限の種類に応じて、ユーザ通知設定を行います。

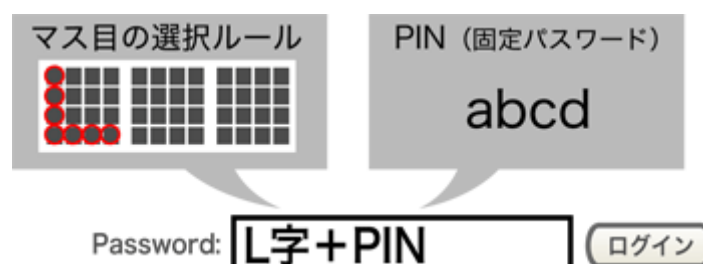


1. PassLogic 認証方式とは？

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。



パスワード生成のルールを「パスワード位置情報」と呼び、ユーザ自身を変更できます。また、パスワード位置情報に PIN（固定パスワード）を組み合わせることも可能です。例えば L 字の形のパターンと PIN をユーザが設定する方法をご説明します。



STEP1.

「L 字」+PIN（今回は PIN の例として「abcd」を使用）を入力します。

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

Secured by PassLogic.

Password: 次へ

入力する値は **5904251abcd**

STEP2.

STEP1 で次へをクリックすると、新たな乱数表が提示されるので STEP1 と同様に「L 字」+PIN を入力します。

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

Secured by PassLogic.

Password: 次へ

入力する値は **7012936abcd**

STEP3.

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

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

Secured by PassLogic.

Password: 次へ

入力する値は **9308742abcd**

2. インストールガイド

2.1. 動作環境

PassLogic 認証サーバの動作環境は以下の通りです。

	Red Hat Enterprise Linux 5 / CentOS 5 i386 および x86_64	Red Hat Enterprise Linux 6.1 以降 / CentOS 6.1 以降 i386 および x86_64
PassLogic	PassLogic-v3.x.x-el5.tar.gz	PassLogic-v3.x.x-el6.tar.gz
httpd	Apache HTTP Server version: 2.2.3 release: 6.el5 以降	Apache HTTP Server version: 2.2.15 release: 15.el6 以降
php	version: 5.1.6 release: 5.el5 以降	version: 5.3.3 release: 3.el6 以降

*各モジュールは、OS ベンダ提供の rpm パッケージのみ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。

*NSA Security-Enhanced Linux(SELinux)を有効にした動作はサポートしていませんので OS インストール時または設定にて「無効」に設定してください。

*/var, /opt 以下のディスク容量が不足しないようにしてください。容量が不足した場合、管理ツールにログインできなくなります。

*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 Redhat 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。

2.2. 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。

2.3. ウィルス対策ソフトを利用する場合

下記のディレクトリをスキャン対象から除外してください。

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

2.4. 最少ハードウェアスペック

・ CPU: Pentium1GHz 以上

- ・メモリ: 1GB 以上
- ・HDD: 60GB 以上

2.5. 推奨ブラウザ

	種別	ブラウザ	文字コード
管理ツール	PC	Internet Explorer8, 9, 10	UTF-8
	PC	Firefox	UTF-8
ユーザインターフェース	PC	Internet Explorer6, 7, 8, 9, 10	UTF-8
	PC	Firefox	UTF-8
	PC	Google Chrome	UTF-8
	iPhone	iOS Safari	UTF-8
	Android	標準ブラウザ	UTF-8
	携帯	docomo i-mode ブラウザ(FOMA) au EZweb Softbank *個体識別番号制限機能は、個体識別番号が送出できる端末に限りです。	Shift-JIS

*バージョンの明記のないものは検証時での最新バージョンで確認をおこなっております。

*上記以外のブラウザ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。

*JavaScript を使用していますので、ブラウザの設定で JavaScript が動作するように設定してください。

*PassLogic は Cookie でセッション管理を行います。Cookie を受け入れるようにブラウザを設定してください。携帯電話などの Cookie を処理できない端末については URL セッションが使用可能です。

2.6. ユーザインターフェースの言語について

ブラウザの言語設定に ja（日本語）がある場合は優先順位に関係なく日本語、ja が無い場合は、en（英語）をデフォルトで表示します。また、各ユーザインターフェースの言語切り替え機能で明示的に言語を切り替える（cookie で設定情報を保持）ことができます。

*携帯電話（docomo、au、softbank）は、日本語が表示されます。

2.7. 使用通信ポート

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

ゲートウェイサーバと認証サーバを同一筐体で動作させる場合の使用ポート

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

ゲートウェイサーバと認証サーバを異なる筐体で動作させる場合の使用ポート

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

その他 PassLogic が使用するポート一覧

ポート番号	送信元	送信先	内容
25/tcp	PassLogic サーバ	⇒ SMTP サーバ	メール送信 (変更可)
465/tcp	PassLogic サーバ	⇒ SMTP サーバ	メール送信 (変更可) TLS/SSL

123/udp	PassLogic サーバ	⇒	NTP サーバ	時刻同期
514/udp	PassLogic サーバ	⇒	syslog サーバ	ログ転送
389/tcp	PassLogic サーバ	⇒	LDAP サーバ	LDAP 連携（変更可）
1812/udp	RADIUS クライアント	⇒	RADIUS サーバ	RADIUS 認証
1813/udp	RADIUS クライアント	⇒	RADIUS アカウンティング サーバ	RADIUS アカウ ンティング

その他ポート一覧

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

2.8. 必要な rpm パッケージをインストールする

PassLogic 認証サーバソフトウェアの動作に必要な rpm パッケージをインストールします。

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

PassLogic サーバソフトウェアの動作に必要な rpm パッケージ

- gnupg (RHEL5 のみ)
- gnupg2 (RHEL6 のみ)
- perl
- tmpwatch
- curl
- httpd
- libtool-ltdl
- mod_ssl
- net-snmp-utils

- ntp
- perl-DBI (RHEL5 のみ)
- libxslt
- xmlsec1 (RHEL5 のみ)
- xmlsec1-openssl (RHEL5 のみ)
- php
- php-ldap
- php-mbstring
- php-process (RHEL6 のみ)
- postgresql-libs (RHEL6 のみ)
- zip
- unzip
- php-pecl-apc (RHEL6 のみ)

必要な rpm パッケージをインストールします。

```
(root 権限で実行)
# yum -y install gnupg (RHEL5 のみ)
# yum -y install gnupg2 (RHEL6 のみ)
# yum -y install perl
# yum -y install tmpwatch
# yum -y install curl
# yum -y install httpd
# yum -y install libtool-ltdl
# yum -y install mod_ssl
# yum -y install net-snmp-utils
# yum -y install ntp
# yum -y install perl-DBI (RHEL5 のみ)
# yum -y install libxslt
# yum -y install xmlsec1 (RHEL5 のみ)
# yum -y install xmlsec1-openssl (RHEL5 のみ)
# yum -y install php
# yum -y install php-ldap
# yum -y install php-mbstring
# yum -y install php-process (RHEL6 のみ)
# yum -y install postgresql-libs (RHEL6 のみ)
# yum -y install zip
```

```
# yum -y install unzip
# yum -y install php-pecl-apc (RHEL6 のみ)
```

2.9. 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 (3.x.x はそれぞれのバージョンに置き換えてください)。

RHEL5 または CentOS5 の場合(PassLogic-v3.x.x-el5.tar.gz)

(root 権限で実行)

```
# cp /cdrom/PassLogic-v3.x.x-el5.tar.gz /usr/local/src/
# cd /usr/local/src/
# tar zxvf PassLogic-v3.x.x-el5.tar.gz
# cd passlogic-3.x.x/
# ./install.sh install
```

RHEL6 または CentOS6 の場合(PassLogic-v3.x.x-el6.tar.gz)

(root 権限で実行)

```
# cp /cdrom/PassLogic-v3.x.x-el6.tar.gz /usr/local/src/
# cd /usr/local/src/
# tar zxvf PassLogic-v3.x.x-el6.tar.gz
# cd passlogic-3.x.x/
# ./install.sh install
```

PassLogic 認証サーバソフトウェアがインストールされます。

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

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

2.9.1. インストール時の設定

インストール時に、以下の設定が自動で追加・更新されます。

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
AddDefaultCharset	コメントに
ServerSignature	Off

TraceEnable	Off
-------------	-----

/etc/php.ini

post_max_size	16M
upload_max_filesize	20M
memory_limit	256M
session.use_trans_sid	1
session.use_only_cookies	0
date.timezone	Asia/Tokyo
expose_php	Off
error_reporting	E_ALL & ~E_NOTICE
session.cookie_httponly (RHEL6 のみ)	On
short_open_tag(RHEL6 のみ)	On

/etc/yum.conf

exclude=freeradius

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

/etc/sudoers

#Defaults requiretty(コメントアウト)
apache ALL=NOPASSWD: /sbin/service httpd status
apache ALL=NOPASSWD: /sbin/service sendmail status (RHEL5 のみ)
apache ALL=NOPASSWD: /sbin/service postfix status (RHEL6 のみ)
apache ALL=NOPASSWD: /sbin/service radiusd status
apache ALL=NOPASSWD: /sbin/service ntpd status
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/httpd_restart.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/radiusd_restart.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/restore.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/support_information.sh
apache ALL=NOPASSWD: /opt/passlogic/passlogic/tools/analysis.sh

*管理ツールから、設定変更を有効にするため上記の設定が追加されます。

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

/usr/bin/sudo /sbin/service httpd status
--

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

2.9.2. タイムゾーンの設定

海外でご利用の場合には適切なタイムゾーンを設定してください。

・ /etc/php.ini

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

2.10. 管理画面にアクセスする

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

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

管理者のユーザ名は「admin」です。

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

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

PassLogic® [メインページ >>](#)

マニュアル PassLogic Management Tools

管理者ユーザのログイン・パスワード(パスワード位置情報)を設定します。

手順

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

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

Secured by PassLogic.

1

2

3

4

5

6

7

8

9

0

<<

次へ

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

2.11. ライセンスを登録（更新）する

管理画面からライセンスファイルをアップロードすることでライセンス情報が登録され PassLogic が利用できるようになります。メインページに戻り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。

PassLogic のライセンスはファイル形式で提供されます。

ライセンスファイル名 : license.asc

*ライセンスファイルは大切に保管してください。

*ライセンスファイルは納品されたものをそのままお使いください。編集（上書き保存など）するとファイルが壊れてしまい正常に動作しなくなります。

*ライセンス登録時に httpd の再起動は発生しません。

2.12. アップデート

PassLogic 認証サーバソフトウェアをアップデートします。アップデートはユーザが PassLogic サーバにアクセスしていない状態で行ってください。

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

(root 権限で実行)

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

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

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

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

PassLogic Authentication Server Software をアップデートします。よろしいですか？
start update PassLogic Authentication Server Software [yes or no]
(yes を入力してください)

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

2.12.1. アップデート時の注意

アップデートにより、HTML テンプレートは上書きされますので、HTML テンプレートをカスタマイズしている場合は、新しいバージョンの HTML テンプレートを再度カスタマイズする必要があります。

機能拡張スクリプトや認証連携用モジュールを利用している場合は、アップデート後のバージョンが動作サポートしているかをあらかじめご確認ください。

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

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

(管理ツールにアクセスし、バックアップファイルをリストアしてください)

2.12.3. バージョン 3.3.2 以前からのアップデート

バージョン 3.3.2 以前からのアップデートは、別途動作確認が必要になりますので、弊社サポートまでお問い合わせください。

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

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

2.12.5. バージョン 3.5.1 以前からのアップデート

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

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

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

2.12.6. バージョン 3.6.0 以前からのアップデート

ユーザが mod_auth_passlogic にアクセスしている状態で PassLogic を update すると、セッションが一旦切れます。再度ログインすることで利用を開始することができます。

リモートアクセス管理（リバースプロキシ連携）の際に Cookie の secure 属性を強制する設定および内部サーバに任意の http header を送出する設定は、設定ファイルでの設定に変更されております。設定方法については、本マニュアル 3.3.6 をご参照ください。

すでに設定いただいている情報は アップデート時に引き継がれます。また、バックアップ/リストアの際も引き継がれます。ゲートウェイサーバと認証サーバと分離して運用する際にはゲートウェイサーバに設定を行ってください。

2.12.7. バージョン 3.7.0 以前からのアップデート

RHEL6 の場合、php-eaccelerator のアンインストール及び php-pecl-apc のインストールが必要です。(インストーラにより実施されます)

2.13. アンインストール

PassLogic 認証サーバソフトウェアをアンインストールします。

(root 権限で実行)

```
# cd passlogic/
```

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

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

(yes を入力してください)

*rpm パッケージは別途アンインストールをお願いします。

3. システム管理者ガイド

3.1. 管理者アカウントを作成する

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

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

*役割を operator とした場合、ユーザ管理のみ設定変更可能となります。（ユーザのロック／アンロック、パスワード再発行のみ）

*admin は削除できません。admin でログインさせたくない場合は、アカウントを無効に設定してください(admin を無効する場合、別途 admin 権限の管理者アカウントが必須です)。

3.1.1. 管理者追加

【 手順 】

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

ユーザ ID (必須項目)	英数字・記号 (2-80 文字) -(ハイフン) _(アンダーバー) .(ピリオド) @(アットマーク) ユーザ登録通知メール <%UID%> 部分
メールアドレス	通知書をメールで送る場合は入力してください。
氏名	ユーザの氏名を入力します。 ユーザ通知メール<%UNAME%>部分
役割	admin 又は operator のどちらかを選択します。
PIN	ワンタイムパスワードに付加する PIN (英数字*大文字小文字を区別する) の初期値を指定します。
初期パスワード位置情報 (ワンタイムパスワード)	ユーザに通知するパスワード位置情報を設定します。以下通知例 *10 桁以上はアルファベット[A-Z]で表現します。 初期パスワード位置情報は 1234 5678 9ABC DE** **** * **** **** * **** **** * です。

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

3.1.2. 管理者一覧

役割が admin の管理者の一覧を表示します。

3.1.3. オペレーター一覧

役割が operator の管理者の一覧を表示します。

3.2. PassLogic 設定

PassLogic を運用する上で必要な様々な設定を行います。

3.2.1. セキュリティポリシー設定

PassLogic 全体のセキュリティポリシー設定の方法を説明します。

【 手順 】

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

ロック・アウトまでの連続	ユーザが設定した回数だけ連続で認証に失敗すると、そのユー
--------------	------------------------------

失敗回数	ザはロック・アウトされます。認証成功時にカウントはリセットされます。0 にすることでロック・アウトしません。
ロック・アウト解除までの秒数	指定した秒数でロック・アウトが自動的に解除されます。[自動ロック解除しない]にチェックをすることで自動的に解除されません。
乱数表の有効時間	乱数表の有効時間を設定します。設定した時間を過ぎると、PassLogic 認証サーバ上の正解パスワードが削除されます。認証するためには新規に乱数表を取得する必要があります。
再設定時の制限	直近 n 回と同じパスワード位置情報の設定を禁止します。
初期パスワード位置情報	ユーザの初期パスワード位置情報を空欄で作成した場合は、ここで設定したものを初期パスワード位置情報とします。*10 桁以上はアルファベット[A-Z]で表現します。 初期パスワード位置情報は 1234 5678 9ABC DE** ***** ***** ***** です。
パスワード位置情報の有効期限	パスワード位置情報を定期的に変更させたい場合に日数を設定します。無制限をチェックすると定期的な変更は必要ありません。
ワンタイムパスワードの長さ	ワンタイムパスワードの長さを指定します。 *ワンタイムパスワードと PIN を合わせたパスワードの長さが 128 文字以下になるように上限を設定してください。
ランダム発行時の長さ	初期パスワード位置情報をランダムで作成する場合の長さを設定します。
PIN の長さ	PIN (固定パスワード) の長さを指定します。 *ワンタイムパスワードと PIN を合わせたパスワードの長さが 128 文字以下になるように上限を設定してください。 PIN の使用可能文字は、半角英数と記号.(コンマ)_(アンダーバー)@(アットマーク)-(ハイフン)です。
PIN に英字および数字を含めることを強制	本設定チェック時、ユーザは英字と数字を 1 つ以上含めた PIN を設定する必要があります。
設定禁止パスワード位置情報	ユーザに設定させたくない抜き出しパターンを設定します。 *部分一致ではなく、完全一致となります。
パスワード位置情報の設	ユーザがパスワード位置情報を変更する際に、4*4 の 3 ブロッ

定制約	クすべてからパスワード位置情報を選択する必要がある制限を有効にします。
ユーザによるパスワード位置情報変更	ユーザによるパスワード位置情報の変更を許可するか、しないかを設定します。 *パスワード位置情報の変更を許可しない場合には、ユーザ登録時に、「初回抜き出し位置変更が必要」を必ず No にして下さい。
ダミー乱数表の表示	不正なユーザ情報で乱数表のリクエストがあった場合、エラーを表示するのかダミーの乱数表を表示するのか選択します。
1 つの正解で認証できる回数	1 つの正解で認証できる回数を指定します。通常は 1 にして下さい。他のシステムとの連携で、複数回正解の付け合わせが必要な際に変更します。
ユーザにアプリケーションパスワード・パラメータの変更を許可	ユーザが、自身でアプリケーションパスワード(WebSSO 時に利用するパスワード)、パラメータ(WebSSO 時に利用するパラメータ)およびユーザ自身のメールアドレスを変更できるようにします。 表示：表示の on/off を指定します。 表示名：ユーザに表示させたい値を入力します。
Cookie 制限利用時の Cookie の値	ワнтаイム：ログイン毎に変更（デフォルト） 固定：アクティベート時のまま固定
前回のログインを表示する	前回のログイン、パスワード位置情報の有効期限、ユーザアカウントの有効期限をユーザに表示します。
パスワードリマインダの利用を許可	ユーザがパスワードを忘れたときにリマインダーを利用できるようにする場合はチェックを入れます。
RADIUS 認証のユーザインターフェース利用時に、パスワードをハッシュして送信	RADIUS 連携のユーザインターフェースで、ハッシュしたパスワードを送信する場合はチェックを入れます。 許可した場合、携帯電話で RADIUS 認証ができなくなりますのでご注意ください。 *ハッシュした際パスワードの長さは 64 文字になります。 *デフォルト値は false(無効)ですので、以前のバージョンからアップデートした際ご利用になるには、設定変更をお願いします。

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

3.2.2. メール設定

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

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

3.2.3. ユーザ通知設定

PassLogic が利用者に送信するメールのテンプレートについての解説を行います。メールサーバの設定に関しては、「メール設定」の項をご確認ください。ユーザ通知設定を行う場合は、管理ツール左側のメニューより「ユーザ通知設定」を選択します。「新規ユーザに送信されるメール」「パスワード再発行のときに送信されるメール」「パスワードリマインダから送信されるメール」をそれぞれ分けて登録することができます。

《ユーザへの送信メールの本文の編集》

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

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

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

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

*ログイン用 URL に引数としてユーザ ID を付加することでパスワード入力から開始 (ID

入力の省略) することができます。通知メールで案内する場合は下記の様な記述になります。

https://[PassLogic 認証サーバのホスト名]/uagent/index.php?uid=<%UID%>&target=[アプリケーション名称]
 https://[PassLogic 認証サーバのホスト名]/menu/index.php?uid=<%UID%>

3.2.3.1. Web トークンを利用する場合

ひとつのユーザ ID に対して複数のデバイス ID を登録する場合は、案内文テンプレートに記載している「乱数表表示用の URL」として下記のように id=<%ACCNUM%>を付加した形で案内してください。

https://[PassLogic 認証サーバのホスト名]/passlogic/ui/index.php?id=<%ACCNUM%>

3.2.4. ログ・その他設定

PassLogic の管理・利用ログに関する設定と、その他の PassLogic に関する設定を行います。管理ツール左側のメニューより「ログ・その他設定」を選択します。

ログを syslog に出力する	ログを syslog に出力するかどうかを選択します。
ログレベル	どの水準からログに書き出すのを選択します。 *ログレベルに関しては、本マニュアルの「ログ管理」の項を参照ください。
ログメール通知	From : 送信元アドレスを入力します。 To : 送信先アドレスを入力します。 *複数の宛先に送信する場合は、メーリングリストなどを別途ご用意ください。 Subject : メールのタイトルを入力します。 ログレベル: ログレベルの詳細に関しましてはマニュアル内ログ・リファレンスの項をご確認ください。 アカウントロック時にメールを送信する: ユーザがログイン失敗でロックとなった時にメールを送信する場合は、チェックボックスをチェックします。

3.3. リモートアクセス管理

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

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

PassLogic のリモートアクセス機能は以下で構成されています。

mod_proxy	httpd 付属プロキシモジュール
mod_auth_passlogic	PassLogic 認証連携モジュール（弊社開発）

連携する Web アプリケーションについて

連携対象となる Web アプリケーションのコンテンツ（HTML ソース）は、相対パスで記述されている必要があります。絶対パスで記述されている場合には、コンテンツを変換するなどの対応が必要になります。

絶対パスの例

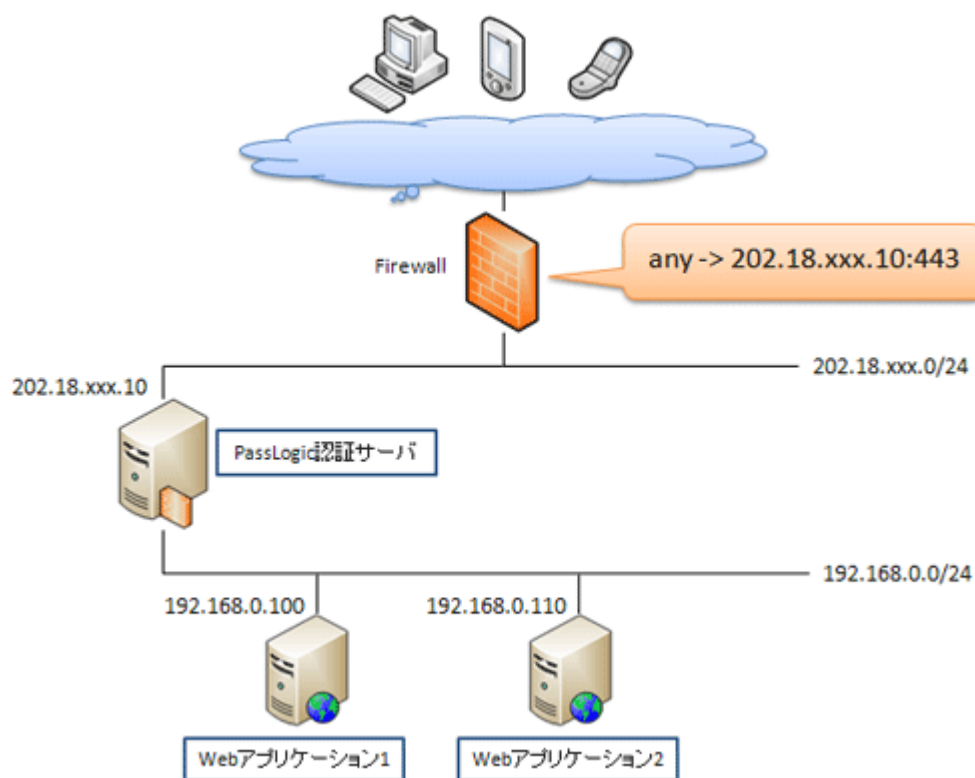
<href="http://www.example.com/link/to/menu.html">リンク

相対パスの例

<href= "link/to/menu.html">リンク

連携実績および連携検証済の Web アプリケーションについては、弊社サポートまでお問い合わせください。連携検証の済んでいない Web アプリケーションについては、導入前に連携検証おこなってください。

また、連携未検証の Web アプリケーションと連携検証を行う前には、Web アプリケーションがリバースプロキシ経由のアクセスに対応しているかをご確認ください。



3.3.1. アクセス先 URL

リモートアクセス機能で利用するユーザインターフェースは以下の通りです。

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

リモートアクセス管理は、上記いずれかの URL に最初にアクセスしていただいて利用することを前提として開発されております。

3.3.2. ポリシー設定

リモートアクセスのポリシー設定を行います。

PassLogicAPI の URL	PassLogicAPI の URL を設定します。 通常はデフォルトのままにしてください。 (デフォルト: http://127.0.0.1:12079/passlogic)	
セッションタイムアウト	セッションの有効期限を秒で設定します。0 を設定することでブラウザを閉じるまでセッションが有効になります。	
プロキシサーバ URL	プロキシサーバを経由して PassLogic にアクセスする場合に設定します。	
PC からのアクセス	PC 向けユーザインターフェースへのアクセス制御（許可する/許可しない）を設定します。	
携帯からのアクセス	携帯（フィーチャーフォン）向けユーザインターフェースへのアクセス制御（許可する/許可しない）を設定します。	
	個体識別番号チェック	携帯からアクセスの際に個体識別番号をチェックする際には ON にしてください。
	クッキーに対応していない携帯端末も利用する	ON にすることで Cookie が利用できない端末からのアクセスの際に URL セッションに切り替わります。
スマートデバイスからのアクセス	スマートデバイス向けユーザインターフェースへのアクセス制御（許可する/許可しない）を設定します。	

携帯からのアクセスを個体識別付きで許可する場合は、デバイスタイプを「個体識別番号による制限」で作成してください。なお、個体識別番号による制限を行う場合、セキュリティ上、PC 向けのユーザインターフェースおよびスマートデバイス向けのユーザインターフェースからのログインはできなくなりますのでご注意ください。

3.3.3. アプリケーション設定（PC / 携帯）

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

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

No.	Web アプリケーションの表示順の数字を入力してください。 *数字が小さいほどログイン後のメニューで上に表示されます。
アプリケーション名称	Web アプリケーションの表示名を入力してください(例 グループウェア)。
仮想パス	Web アプリケーションを公開する際に割り当てるパス名
ローカルアプリケーションの URL	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。 *ローカルアプリケーションの URL では以下を設定します。 ・ポータルメニューからのリンク先 URL ・ WebSSO 利用時の「認証の送信先 URL」が空欄の場合の認証送信先 URL
メニュー表示可能なグループ	メニュー表示可能なグループを指定します。空欄ですべてのユーザに表示します。複数指定する際には,(カンマ)で区切ってください。グループの指定は、ユーザ登録のグループで行います。

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

/menu/

/tmenu/

/mmenu/

/imenu/

/passlogic/

/passlogic-admin/

/

3.3.4. URL マッピング

Web アプリケーションの画像、JavaScript、CSS 等の URL を仮想パスにマッピングして外部から参照できるようにします。

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

設定例

仮想パス	/cgi-bin/
ローカル URL	http://192.168.0.10/cgi-bin/

この設定により、社内ネットワークにある 192.168.0.10 というサーバの cgi-bin 内のコンテンツが PassLogic（外部）から参照できるようになります。

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

/menu/
/tmenu/
/mmenu/
/imenu/
/passlogic/
/passlogic-admin/
/

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

コマンド例

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

3.3.5. 各アプリケーションの設定例

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

desknet's(デスクネッツ) ver7

PC アプリケーション設定

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

URL マッピング①

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

URL マッピング②

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

サイボウズ office8

PC アプリケーション設定

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

URL マッピング①

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

3.3.6. http ヘッダ連携

PassLogic 認証サーバは、認証済のユーザ ID を http ヘッダに含めて、内側のアプリケーションに対して送信します（設定は必要ありません）。

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
<u>PL-Uid: testuser</u>
Connection: Keep-Alive

認証済みのユーザ ID を Web アプリケーションで取得する実装例

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

Cookie の secure 属性を強制する設定および内部サーバに任意の http header を送出する設定方法

対象ファイル

```
/etc/httpd/conf.d/xauth_passlogic_00.conf
```

設定値

PasslogicCookieSecure	1	Cookie の secure 属性を強制(1 が ON)
AuthPasslogicParam1	任意の文字列	param1 の値を http header として送出
AuthPasslogicParam2	任意の文字列	param2 の値を http header として送出
AuthPasslogicParam3	任意の文字列	param3 の値を http header として送出
AuthPasslogicParam4	任意の文字列	param4 の値を http header として送出
AuthPasslogicParam5	任意の文字列	param5 の値を http header として送出
AuthPasslogicParam6	任意の文字列	param6 の値を http header として送出
AuthPasslogicParam7	任意の文字列	param7 の値を http header として送出
AuthPasslogicParam8	任意の文字列	param8 の値を http header として送出
AuthPasslogicParam9	任意の文字列	param9 の値を http header として送出
AuthPasslogicParam10	任意の文字列	param10 の値を http header として送出

設定後は httpd の reload をお願いいたします。

```
# /etc/init.d/httpd reload
```

3.3.7. WebSSO

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

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

・ログイン画面が Flash で作成されている Web アプリケーションやログインがポップアップ

プするもの、認証パスワードが JavaScript 等でハッシュして送信されるもの、認証用のトークンを発行するものは検証が必要です、別途お問い合わせください。

・WebSSO の設定をおこなう前にリモートアクセス機能で正常に Web アプリケーションが動作する (httpd がエラーを出力しない状態) ことを確認した後に WebSSO 設定を行ってください。

フォーム認証とは

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

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

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

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

3.3.7.1. 設定方法

WebSSO 設定をする前に、Web アプリケーションのログインに必要な値 (name=value) をご確認ください。

- (1) Web アプリケーションの開発メーカーに仕様をご確認いただく。
- (2) Web アプリケーションの HTML ソースを解析していただく。
- (3) ログイン時の HTTP ヘッダを取得し送信している値を解析していただく。

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

	username)
パスワードの name 属性(*1)	Web アプリケーションのログインに使用されるパスワードの name 属性の名称を入力してください。(例: password)
Web アプリケーションとの通信方式	対象 Web アプリケーションの仕様に従って GET または POST を選択します。
認証方式	サーバ自動認証/クライアント自動認証(Javascript)の 2 通り選択できます。
認証の送信先 URL	リモートアクセス管理 >> アプリケーション設定で設定しているローカルアプリケーションの URL 以外にログイン用の URL がある場合には入力して下さい。特に指定しなければローカルアプリケーションの URL にログインを試みます。 *認証方式を「クライアント自動認証」にした場合は必須となります。クライアント自動認証の際には、PassLogic 経由の（外部より参照可能な）URL を指定してください。
ログインにセッショントークンを必要とする場合	Web アプリケーションにログインする際にログインページの HTML ソースからセッショントークンを取得する必要がある場合に使用します。 ログインページの URL: 対象 Web アプリケーションのログインページの URL を指定してください。 ログインページから取得する値の名前(*3): ログインページから取得する値の name 属性を指定してください。
その他の追加パラメータ	Web アプリケーションのログインの際にログイン ID、パスワード以外に必要なパラメータはこちらで設定してください。アプリケーションごとに異なります。
ユーザごとのパラメータ	グループ ID などユーザごとに POST したいパラメータの name 属性を指定します。ユーザ登録時の param1-10 が value 属性として対応します。

(*1)について

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

Web アプリケーションのログイン画面の HTML を表示します。

```
<form method="post" name="LoginForm" action="login.cgi">
ログイン名: <input type="text" name="user_id"><br />
```

```
パスワード: <input type="password" name="password"><br />
<br />
<input type="submit" name="submit" value="ログイン">
<input type="hidden" name="mode" value="login">
</form>
```

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

*HTML タグについては書籍やリファレンスなどをご確認ください。

(*3)について

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

例

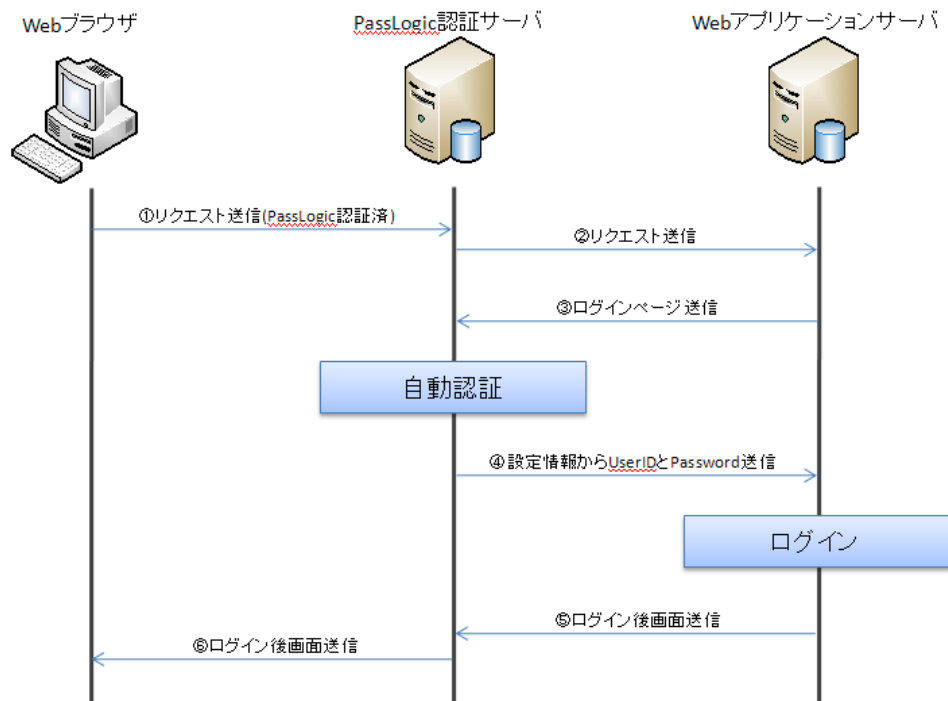
```
<form method="post" name="LoginForm" action="login.cgi">
ログイン名: <input type="text" name="user_id"><br />
パスワード: <input type="password" name="password"><br />
  <input type="hidden" name="SESSION_TOKEN" value="[毎回変わる値]">
<br />
<input type="submit" name="submit" value="ログイン">
<input type="hidden"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

このようなログインページの場合、「ログインページから取得する値の名前」に「SESSION_TOKEN」を設定すると、動的に変わる値を PassLogic サーバが取得して代理 POST する際に取得した名前=値のペアを一緒にアプリケーションサーバに送信することができます。

3.3.7.2. 認証方式

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

3.3.7.2.1. サーバ自動認証のシーケンス図

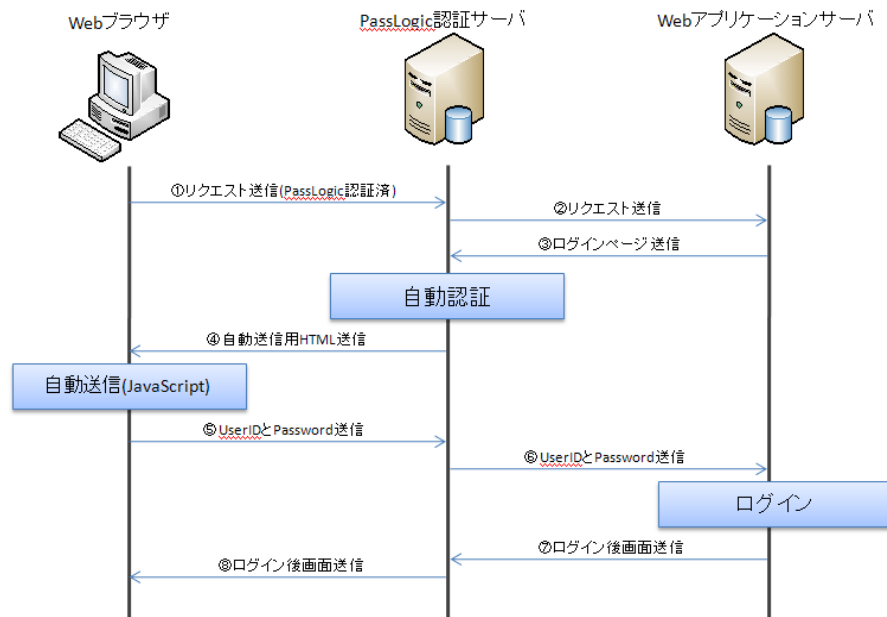


PassLogic 認証サーバが代理でユーザ ID、パスワードを Web アプリケーションに対して送信します。Web アプリケーションによっては WebSSO できないこともあります、アプリケーションのユーザ ID、パスワードが外部ネットワーク上を流れることがないのでセキュアな方式です。

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

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

3.3.7.2.2. クライアント自動認証のシーケンス図



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

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

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

```

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

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

3.3.7.3. 各アプリケーションの設定例

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

desknet's(デスクネッツ) ver7

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

サイボウズ office8

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

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

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

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

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

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

以下の設定ファイルを追加します。

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

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

```
ProxyPass /exchange/ https://192.168.0.80/exchange/
```

```
ProxyPassReverse /exchange/ https://192.168.0.80/exchange/
```

```
ProxyPass /exchweb/ https://192.168.0.80/exchweb/
```

```
ProxyPassReverse /exchweb/ https://192.168.0.80/exchweb/
```

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

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

3.3.8. SAML 連携

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

*ユーザインターフェース menu、imenu から SAML 連携が可能です。

3.3.8.1. SAMLSP 登録

SP(Service Provider)を登録します。

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

Google Apps の場合の設定例

(*) 必須項目

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

次へ

3.3.8.2. SAML 証明書

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

3.3.9. グラフィックデザインのカスタマイズ

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

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

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

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

*ログイン画面をカスタマイズされる場合は「ソフトウェア使用許諾契約書」に従ってカスタマイズ（コピーライトと Secured by PassLogic.を目に見える形で表記）してください。

PC 用ログイン画面のカスタマイズ

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

.en は英語インターフェイス

スマートデバイス用ログイン画面のカスタマイズ

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

.en は英語インターフェイス

携帯電話用ログイン画面のカスタマイズ

/opt/mod_auth_passlogic/mtmpl/login.html	ユーザ ID 入力
--	-----------

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

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

各ログイン画面で利用できる変数

各テンプレートに共通の変数です。

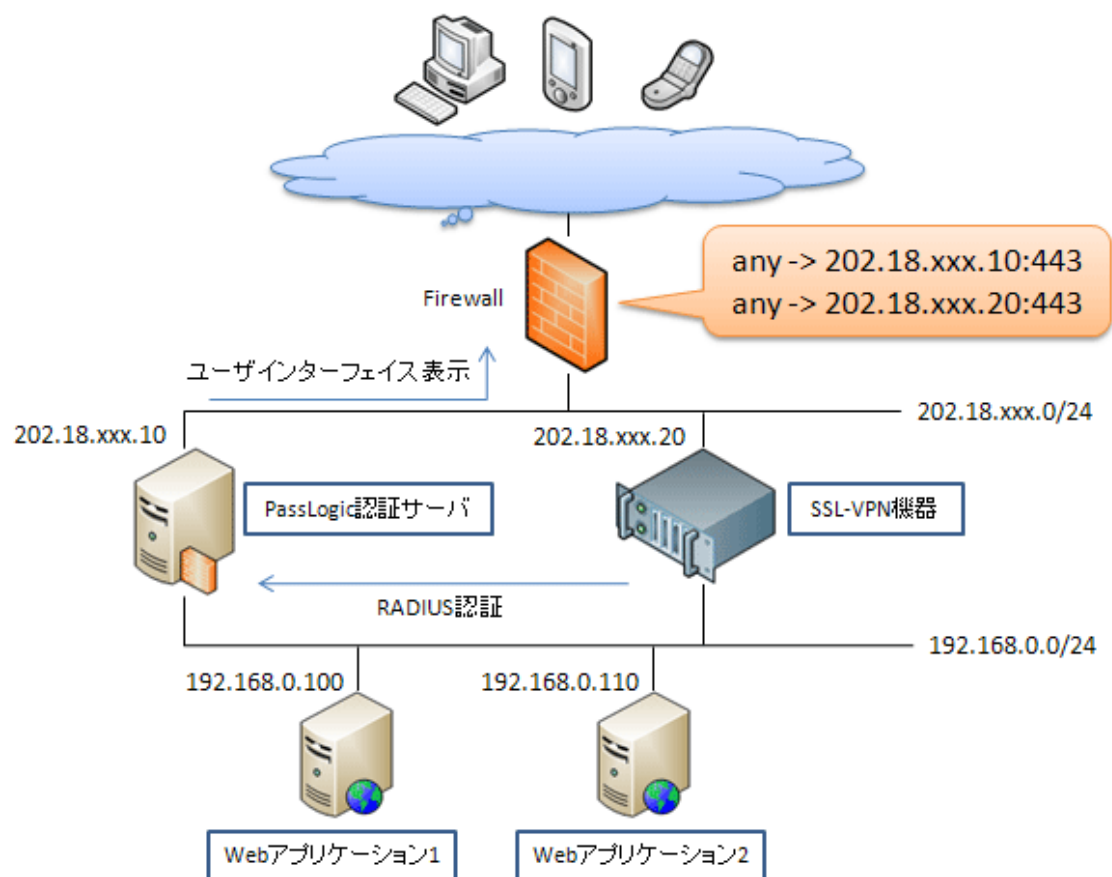
<%ERRORTEXT%>	エラーがある場合、エラーメッセージとエラーコードを表示します。
<%PASSLOGICUID%>	入力された uid を表示します。
<%PASSLOGIC0%>・<%PASSLOGIC47%>	PassLogic の乱数表の数字を表示します。

3.4. RADIUS 連携

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

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

認証方式は、PAP、CHAP、MSCHAPv1,v2 に対応しています。



3.4.1. RADIUS 認証動作

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

・ PAP

```
# echo "User-Name=test, User-Password=8283" | radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 44 to 192.168.0.203 port 1812
```

```
User-Name = "test"
User-Password = "8283"
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=44,length=20
```

・ CHAP

```
# echo "User-Name=test, CHAP-Password=0772" | radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 42 to 192.168.0.203 port 1812
User-Name = "test"
CHAP-Password = 0x2a49ec0d72c3bbc6dbe850ef2edda47f32
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=42,length=20
```

3.4.2. RADIUS クライアント登録

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

RADIUS クライアントの追加をクリックしてください。

*RADIUS で認証連携するためには、RADIUS クライアントの登録が必要です。

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

3.4.3. ユーザインターフェース

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

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

アプリケーション名称	アプリケーションの名称です。半角英数字で入力してください。(例 sslvpn)
AnyConnect	Cisco AnyConnect と連携する際に使用します。 *スマートデバイス版の AnyConnect と連携する場合の設

	定項目です。PC 版の AnyConnect のログインには Web トークンをご利用ください。
認証の送信先 URL	ログイン情報を送信する URL を指定してください。
ログインIDの name 属性(*1)	アプリケーションのログインに使用されるログイン ID(ユーザ ID)の name 属性の名称を入力してください。(例: UserID)
パスワードの name 属性(*1)	アプリケーションのログインに使用されるパスワードの name 属性の名称を入力してください。(例: Password)
Web アプリケーションとの通信方式	GET または POST を選択します。
ログインページの URL	アプリケーションのログインページ URL を指定してください。
ログインページから取得する値の名前(*2)	ログインページから取得したいエンティティがある場合、エンティティの名前を入力します。 (例: SESSION_TOKEN)
その他の追加パラメータ	アプリケーションのログインの際にログイン ID、パスワード以外に必要なパラメータはこちらで設定してください。アプリケーションごとに異なります。
ユーザごとのパラメータ	グループ ID などユーザごとに POST したいパラメータの name 属性を指定します。ユーザ登録時の param1-10 が value 属性として対応します。
ドメインパスワード(*3)	FirePass のドメインパスワード (キャッシュ) 利用時に有効にします。

(*1)について

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

(*2)について

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

例

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

```
<input type="submit" name="submit" value="ログイン">
<input type="hidden" name="mode" value="login">
</form>
```

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

(*3)ドメインパスワードに使用可能な文字

半角英数字および以下の記号が使用可能です。

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

ユーザインターフェースの URL

```
http://[PassLogic 認証サーバのホスト名]/uagent/
```

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

3.4.4. ユーザインターフェースで target の値を URL に含める方法

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

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

にアクセスして認証を行います。

アプリケーションの名称が、users の場合、アクセス先 URL は以下になります。

http://[PassLogic 認証サーバのホスト名]/uagent/users/

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

```
RewriteEngine On

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

RewriteCond %{QUERY_STRING} ^$

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

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

RewriteCond %{QUERY_STRING} !^$

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

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

*URL 中に target を含めてもプルダウンは表示されますのでプルダウンを表示させたくない場合はプルダウンの部分を HTML テンプレートから削除する必要があります。以下に修正方法を示します。*この修正は PassLogic のアップデート時に消えますのでアップデート後に再度実施していただく必要があります。

修正対象ファイル

PC	/opt/passlogic/passlogic-admin/php/tmpl/form/uAgentForm/form.ihtml.php
スマートデバイス	/opt/passlogic/passlogic-admin/php/tmpl/form/uAgentFormiPhone/form.ihtml.php
携帯	/opt/passlogic/passlogic-admin/php/tmpl/form/uAgentFormMobile/form.ihtml.php

編集内容

```
<?php
print $this->_select("target", $this->uagent_arr, $this->_target);
?>
```

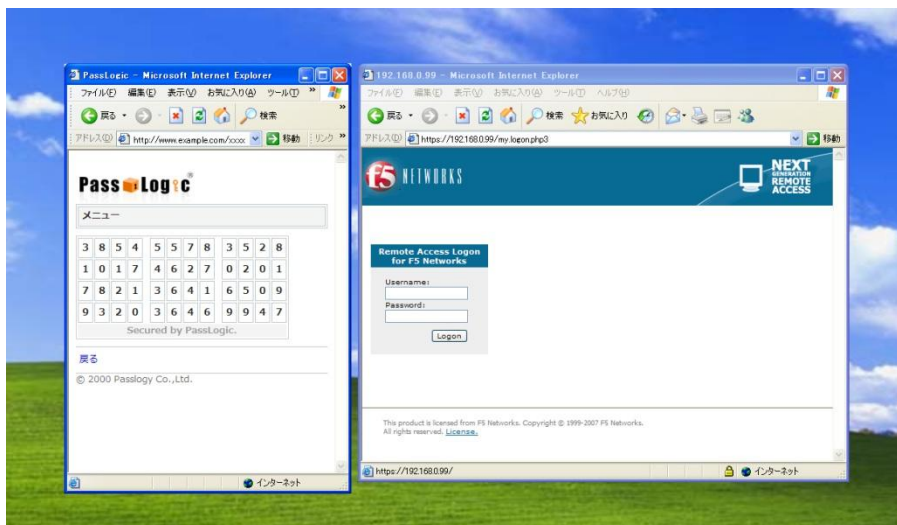
の部分を削除またはコメントアウトして以下に変更して下さい。


```
<input type="hidden" id="target" name="target" value="<?=$this->_target?>" >
```

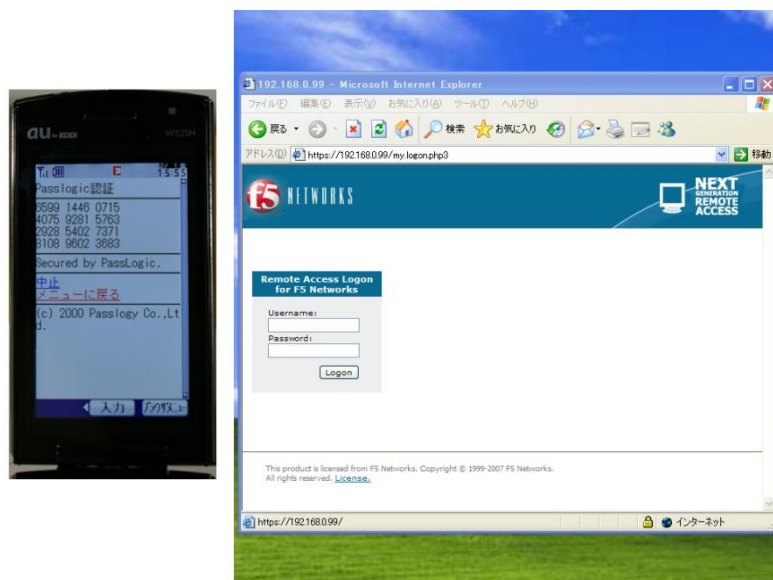
3.4.5. Web トークン

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

【PC で乱数表を取得した場合の画面例】



【携帯電話で乱数表を取得した場合の画面例】



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

Web トークンの URL

<code>https://[ホスト名]/passlogic/ui/</code>

3.4.6. グラフィックデザインのカスタマイズ

シングルサイン オン	URL	<code>https://[ホスト名]/uagent/</code>
	スタイルシート (PC)	<code>/opt/passlogic/passlogic-admin/php/css/style.css</code>
	スタイルシート (スマートフォン)	<code>/opt/passlogic/passlogic-admin/php/css/sp.css</code>
	スタイルシート (タブレット)	<code>/opt/passlogic/passlogic-admin/php/css/tablet.css</code>
Web トークン(全 クライアント端 未共通)	URL	<code>https://[ホスト名]/passlogic/ui/</code>
	スタイルシート	<code>/opt/passlogic/passlogic-admin/php/css/tokengui.css</code>

ロゴ画像ファイル

<code>/opt/passlogic/passlogic-admin/php/images/passlogic-logo.gif</code>

3.4.7. トラブル・シューティング

ログインが成功しない場合は、シングルサインオンの設定、RADIUS の設定、ネットワークの設定、サーバの設定、ユーザ操作など、どこに原因があるかを切り分ける必要があります。

- (1) RADIUS クライアント登録が正常に行われているでしょうか？ PassLogic に RADIUS 認証を送信してくる SSL-VPN 機器等の IP アドレスの登録が必要です。または、ネットワークの構成によって、異なる IP アドレスで RADIUS の通信がされている可能性は無いでしょうか？
- (2) RADIUS のシークレットの値は、合っておりますでしょうか？
- (3) VPN 機器から PassLogic への udp1812 での通信は可能でしょうか？
- (4) juniperMAG にログインする際には、juniperMAG 側での Realm の値と PassLogic のユーザインターフェース設定での、Realm の値を合わせる必要があります。こちらは合っておりますでしょうか？
- (5) RADIUS の設定、ネットワークの設定、サーバの設定、ユーザ操作が正しい場合、Web

トークンであればログインが可能です。Web トークンでログインができるようであれば、シングルサインオンの設定にミスがある可能性があります。

- (6) 乱数表（正解）には有効時間があります。有効時間内にパスワード入力してください。
（サーバの時間も合わせてください）
- (7) PassLogic では一度ログインが成功すると認証サーバから正解が消去されます。同じ乱数表で何度もログインすることはできませんので、認証のたびに新たな乱数表を取得して下さい。
- (8) グループにスペースが入っていませんか？（スペースが入っていると認証が失敗してしまいます。）

3.4.8. RADIUS ログの確認方法

RADIUS サーバのログの例です。

対象ファイル

/var/log/radius/radius.log

Wed Nov 27 05:57:07 2013 : Auth: Login OK: [user01] (from client 95 port 0)	認証成功
Wed Nov 27 05:57:22 2013 : Auth: Login incorrect: [user01] (from client 95 port 0)	認証失敗
Wed Nov 27 06:00:20 2013 : Error: Ignoring request to authentication address * port 1812 from unknown client 192.168.0.95 port 61094	PassLogic にクライアント登録されていない

3.5. ID 同期

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

以下のデータ同期に対応しています。

OpenLDAP

ActiveDirecory

3.5.1. LDAP 設定

LDAP サーバ名	LDAP サーバのホスト名または IP アドレスを指定します。
-----------	---------------------------------

LDAP サーバのポート番号	LDAP サーバのポート番号を入力します。通常は 389 番ポートです。
バインド DN	バインド DN を入力します。
ldapsearch に必要なパスワード	ldapsearch に必要となるパスワードを入力します。
LDAP タイプ	OpenLDAP, ActiveDirecory, その他 より同期の対象とするサーバを選択してください。
ターゲットオブジェクトの DN	ターゲットオブジェクトの DN を入力します。
検索フィルタ	検索条件を設定します。
ユーザ ID に使用するアトリビュート	ユーザ ID に使用するアトリビュートを入力します。
メールアドレスに使用するアトリビュート	メールアドレスに使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
氏名に使用するアトリビュート	氏名に使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
グループに使用するアトリビュート	グループに使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
PIN に使用するアトリビュート	PIN に使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
初期パスワード位置設定	初期パスワード位置設定を選択します。「ランダム位置で発行」または「初期パスワード位置情報で発行」
初回にパスワード位置情報の変更が必要	ユーザが初回アクセスする際にパスワード位置情報の変更になります。
ユーザアカウントの有効期限に使用するアトリビュート	ユーザアカウントの有効期限です。(フォーマット: yyyymmdd 例:20110901) *項目が空欄の場合は同期時に上書きしません。 *保存形式が異なるため Active Directory のアカウントの有効期限との同期はできません。
備考に使用するアトリビュート	備考に使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
パラメータに使用するアトリビュート(param01-10)	param01-10 に使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
apppassword に使用するアトリビュート	apppassword に使用するアトリビュートを入力します。 *項目が空欄の場合は同期時に上書きしません。
ユーザ ID の同期時刻	同期する時刻またはローテーションを指定します。 例:一日一回 3 時 00 分に同期であれば「毎日」「3」「0」を選択します。

ユーザ追加時のアクション	同期の際、ユーザアカウント追加時のデバイスタイプとアクションを指定します。 *LDAP 連携で追加したユーザのパスワード位置情報はランダムなものが設定されます。
同期時の動作	追加/更新のみ: 参照先のユーザ情報を PassLogic に追加・更新（メールアドレスの変更）します。 完全一致: 参照先と PassLogic のユーザ情報を完全に同期します。PassLogic 上に存在するユーザ ID が参照先に存在しない場合は PassLogic のユーザが削除されます。admin 権限ユーザは削除対象になりません。ID 同期削除対象外は削除対象になりません。

*改行コードを含む値を持つアトリビュートを指定しないでください。

LDAP(Active Directory)から PassLogic に取り込む値は、LDAP 検索フィルタで参照できる必要があります。

設定例(パラメータはそれぞれの環境に合わせて下さい)

3.5.2. OpenLDAP

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

3.5.3. ActiveDirectory

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

メールアドレスに使用する アトリビュート	mail
-------------------------	------

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

3.5.1. LDAP 同期

「現在の設定で同期を開始する」をクリックすることで、直ちに同期を開始します。

3.5.2. ActiveDirectory で 1000 件以上同期する場合

ActiveDirectory は MaxPageSize の初期値が 1000 となっています。1000 件以上同期したい場合は、MaxPageSize の値を変更してください。

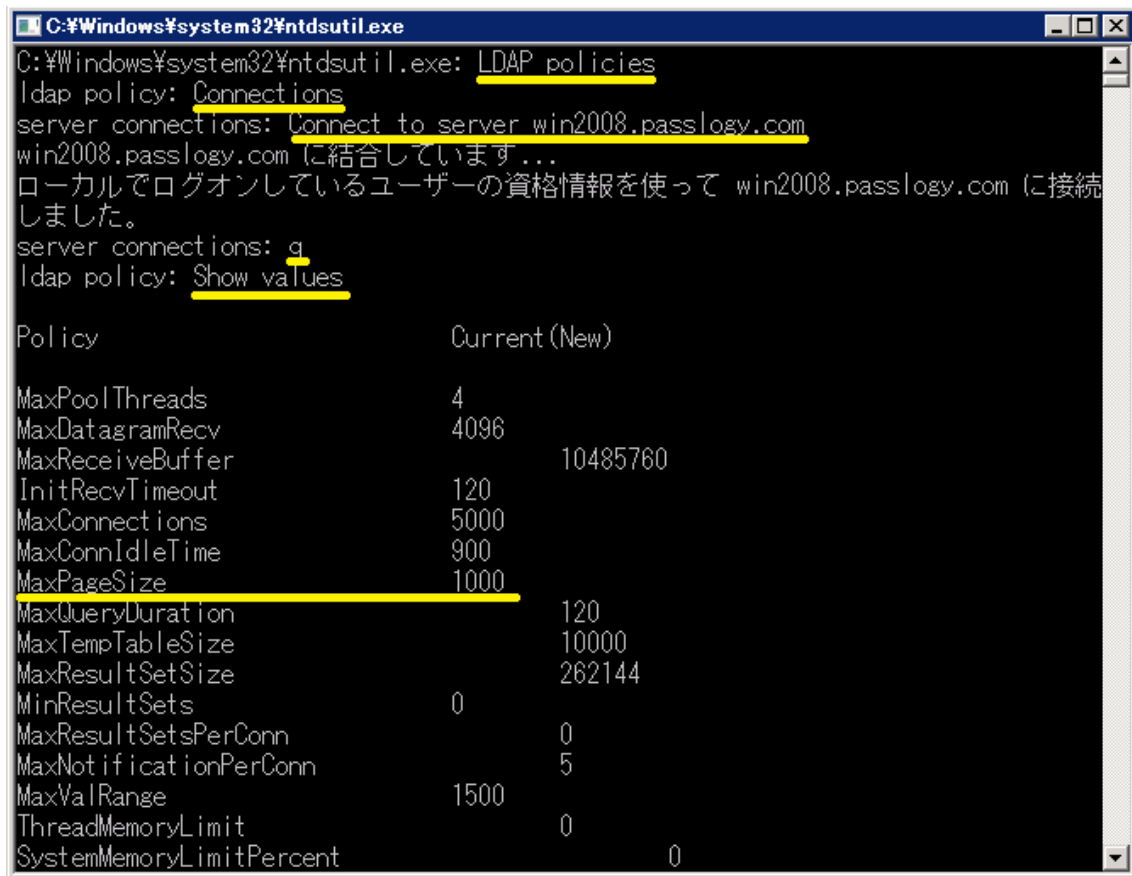
WindowsServer2008R2, WindowsServer2012 での設定方法

- ・WindowsServer にログオンし、Ntdsutil コマンドで、プロンプトを表示します。



・プロンプトが表示されたら、以下のようにコマンドを打ちます。

```
ntdsutil.exe: LDAP policies
LDAP policies: Connections
server connections: connect to server [ActiveDirectory の DNS サーバ名]
(「サーバに接続しました」 と表示されます。)
server connections: q
LDAP policies: Show Values
```



```
C:\Windows\system32\ntdsutil.exe: LDAP policies
ldap policy: Connections
server connections: Connect to server win2008.passlogy.com
win2008.passlogy.com に結合しています...
ローカルでログオンしているユーザーの資格情報を使って win2008.passlogy.com に接続
しました。
server connections: q
ldap policy: Show values

Policy                                Current(New)
MaxPoolThreads                        4
MaxDatagramRecv                      4096
MaxReceiveBuffer                     10485760
InitRecvTimeout                      120
MaxConnections                       5000
MaxConnIdleTime                      900
MaxPageSize                          1000
MaxQueryDuration                     120
MaxTempTableSize                     10000
MaxResultSetSize                     262144
MinResultSets                        0
MaxResultSetsPerConn                 0
MaxNotificationPerConn               5
MaxValRange                          1500
ThreadMemoryLimit                    0
SystemMemoryLimitPercent              0
```

- MaxPageSize を任意の値へ変更します。この例では 10000 件に変更します。

LDAP policies: Set MaxPageSize to 10000

LDAP policies: Show Values


```

C:\Windows\system32\ntdsutil.exe
SystemMemoryLimitPercent                                0

ldap policy: set MaxPageSize to 10000
ldap policy: show values

Policy                                                    Current (New)
MaxPoolThreads                                           4
MaxDatagramRecv                                          4096
MaxReceiveBuffer                                         10485760
InitRecvTimeout                                          120
MaxConnections                                           5000
MaxConnIdleTime                                          900
MaxPageSize                                              1000(10000)
MaxQueryDuration                                         120
MaxTempTableSize                                         10000
MaxResultSetSize                                         262144
MinResultSets                                           0
MaxResultSetsPerConn                                    0
MaxNotificationPerConn                                   5
MaxValRange                                              1500
ThreadMemoryLimit                                        0
SystemMemoryLimitPercent                                0

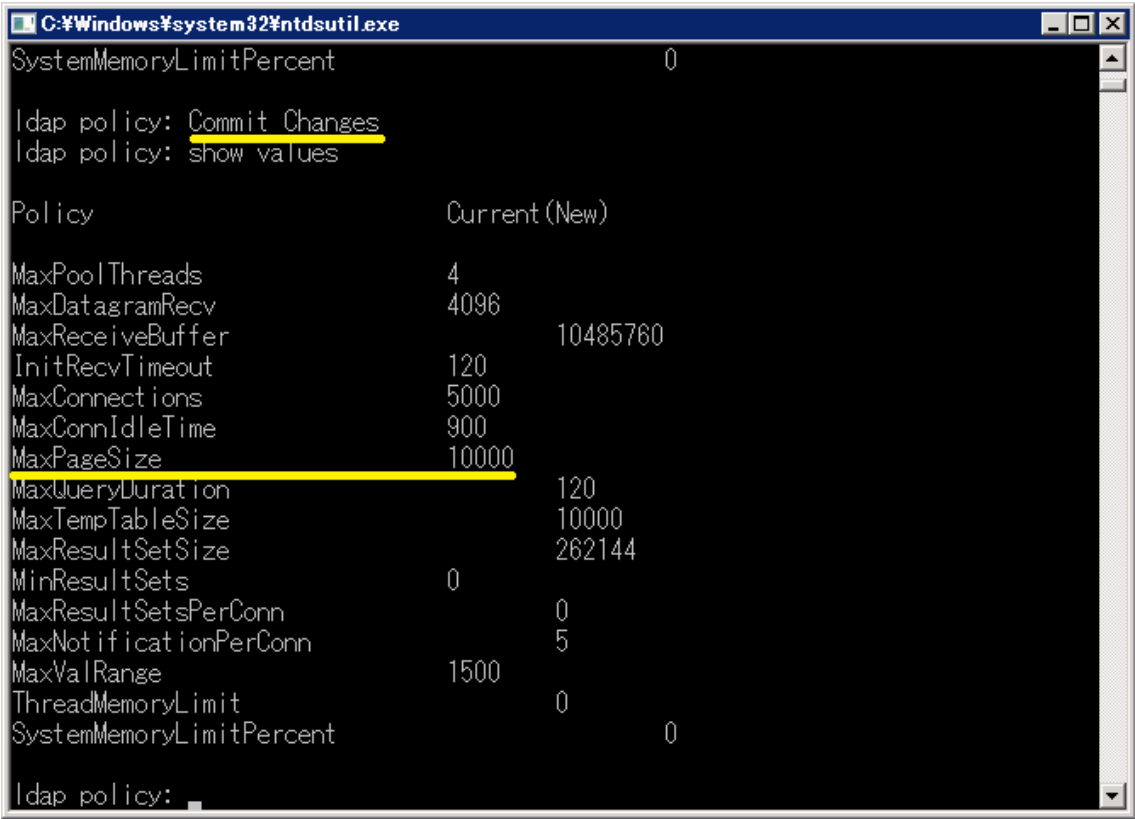
ldap policy:
  
```

この時点ではまだ変更が反映されていません。内容に問題が無いか確認してください。

- ・最後に変更した値をコミットします。

LDAP policies: Commit Changes

LDAP policies: Show Values



これで ActiveDirectory が最大 10000 件までエントリを返すようになります。

3.6. ログ閲覧

PassLogic の認証・操作ログを閲覧できます。ログの内容については、ログ・リファレンスをご確認ください。

最大表示行数	表示する最大件数を入力して下さい。最大は 1000 件です。
検索条件	検索するキーワードを入力して下さい。

3.7. バックアップ/リストア

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

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

バックアップ/リストアで引き継ぎできない情報

PassLogic のログ
セッション情報
ユーザ用画面テンプレート（編集している場合）

3.7.1. バックアップ

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

3.7.2. リストア

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

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

*バックアップ/リストアの処理中にサーバおよび httpd の再起動は行いません。

3.8. サポートに必要なファイルを取得する

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。パスワードを入力して送信ボタンをクリックしてください。サポートファイルのダウンロードが開始されます。

*サポートファイルには設定、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。

*サポート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。

サポートのための情報として取得されるファイル

OS の種類 (バージョンなど)

PassLogic のライセンス

サーバ OS の設定ファイル(/etc/httpd, /etc/php.ini, /etc/raddb)

サーバ OS のログ(/var/log/httpd, /var/log/radiusd)

PassLogic の設定ファイル(config_settings.inc.php, passlogic-config.xml)

PassLogic のログ (/var/log/passlogic)

*サポート用ファイルに設定したパスワードも合わせてお知らせください。

3.9. 管理者パスワードの変更

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

3.10. サーバの再起動をとまなう設定変更

3.10.1. httpd の再起動

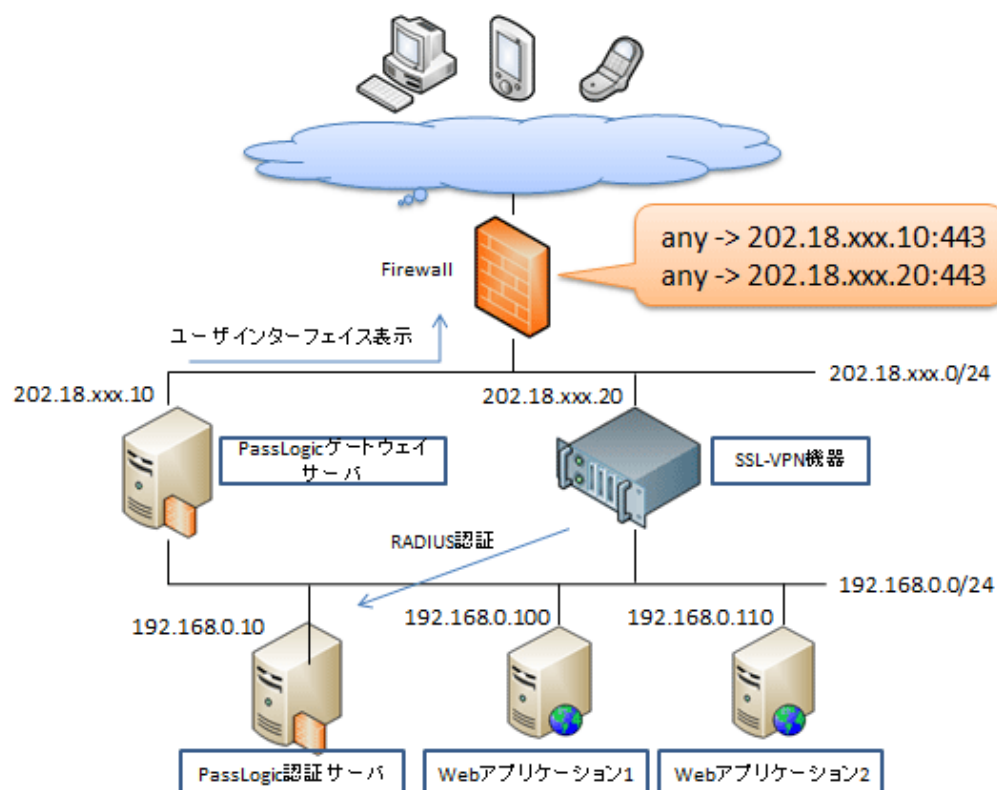
リモートアクセス管理	ポリシー設定	追加・変更・削除
	PC アプリケーション設定	追加・変更・削除
	携帯アプリケーション設定	追加・変更・削除
	URL マッピング	追加・変更・削除
RADIUS 設定	Web トークン	変更

3.10.2. httpd および radiusd の再起動

RADIUS 設定	RADIUS クライアント登録	追加・変更・削除
リストア		

3.11. PassLogic 認証サーバをイントラネットに配置する

PassLogic をゲートウェイサーバと認証サーバの 2 台に分離して、エクストラネットにゲートウェイサーバ、イントラネットに認証サーバと分離して運用することもできます。



3.11.1. 認証サーバとゲートウェイサーバを分離した場合の注意点

PassLogic のログは認証サーバ側に蓄積されます。

認証サーバとゲートウェイサーバの PassLogic は同一バージョンである必要があります。

バックアップ/リストアは、それぞれのマシンで個別に行ってください。

HTML テンプレートはゲートウェイサーバ側をカスタマイズしてください。

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

3.11.2. 認証サーバ(192.168.0.10)側の設定

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

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

管理ツールのメニューが認証サーバ用になります。

3.11.3. ゲートウェイサーバ(202.18.xxx.10)側の設定

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

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

管理ツールのメニューがゲートウェイサーバ用になります。

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

を以下のように変更してください。

【修正前】

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

【修正後】

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

ゲートウェイサーバの PassLogic 管理ツールにログイン後リモートアクセス管理を利用して設定を行います。

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

`http://192.168.0.10:12079/passlogic`

3.12. 複数の端末固定デバイス(Cookie 制限)を登録する方法

ひとつのユーザ ID に対して複数の端末固定デバイスを登録することが可能です。この機能は Cookie による端末制限のみ可能で、携帯電話の個体識別番号による制限では利用できません。

PassLogic 設定 >> セキュリティポリシー設定 >> Cookie 制限利用時の Cookie の値を固定に設定して下さい。「ユーザー一覧」から複数の端末固定を行いたいユーザのユーザ ID をクリックします。デバイス一覧の「端末追加」をクリックして追加した端末でアクティベーションを行ってください。3 台目も同様の手順を繰り返してください。

3.13. パスワードリマインダの利用方法

ユーザがパスワードを忘れた際にユーザ自身がパスワードを再発行できる機能です。登録ユーザ情報に到達可能なメールアドレスが登録されていることが前提となります。

PassLogic 設定 >> セキュリティポリシー設定 >> パスワードリマインダの利用を許可にチェックを入れて設定して下さい。

まずユーザは以下の URL にアクセスします

`https://[PassLogic ホスト名]/reminder.php`

この画面でユーザ ID と登録メールアドレスを入力します。ユーザ ID と登録メールアドレスが一致したときのみ登録メールアドレスにリセット用の URL が送信されます(この時にはまたパスワードは再設定されていません)。

次に、ユーザは送信されてきたメールの URL にアクセスします。以下が送信されてくる URL の例です。

`https:// [PassLogic ホスト名]/resetter.php?key=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`

有効なキーと一致すればパスワードが自動的に再発行されます。

送信されるメールの内容は、PassLogic 設定 >> ユーザ通知設定 >> 「パスワードリマインダから送信されるメール」で編集可能です。

3.14. PassLogic 管理ツールの設定項目

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

ファイルをテキストエディタ等で編集することで、管理ツールの設定変更が行えます。設定できる箇所は以下のとおりです。

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

/**
 * PassLogic log dir.
 * PassLogic ログディレクトリを指定します。
 */
define("PASSLOGIC_LOG_DIR", "/var/log/passlogic");

/**
 * admin password reset mode
 * 管理者のパスワード(抜き出し位置)をリセットする際に 1 にします。
 */
define("ADMIN_PASSWORD_RESET_MODE", 0);
```

3.15. CSV ファイルによるデータ同期

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

ファイル形式	各項目が半角ダブルコーテーションで括られている。 項目間がカンマで区切られている。 行区切りは改行(CRLF)する。 マルチバイトを使用する場合の文字コードは ShiftJIS 例: "aa","bb","cc"																																																
項目一覧	ユーザ ID, [メールアドレス], [氏名], [グループ], [PIN], [初期パスワード位置情報], [初回にパスワード位置情報の変更が必要(Y/N)], [ユーザアカウントの有効期限(yyyymmdd)], [備考], [メール通知(Y/N)], [param1], [param2], [param3], [param4], [param5], [param6], [param7], [param8], [param9], [param10], [apppassword] *初期パスワード位置情報が、空欄の場合はユーザごとにランダム発行します。明示的に指定する場合は、指定したいパスワード位置情報をカンマ区切りで設定してください。 <table><tr><td>01</td><td>02</td><td>03</td><td>04</td><td>17</td><td>18</td><td>19</td><td>20</td><td>33</td><td>34</td><td>35</td><td>36</td></tr><tr><td>05</td><td>06</td><td>07</td><td>08</td><td>21</td><td>22</td><td>23</td><td>24</td><td>37</td><td>38</td><td>39</td><td>40</td></tr><tr><td>09</td><td>10</td><td>11</td><td>12</td><td>25</td><td>26</td><td>27</td><td>28</td><td>41</td><td>42</td><td>43</td><td>44</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>29</td><td>30</td><td>31</td><td>32</td><td>45</td><td>46</td><td>47</td><td>48</td></tr></table> 例: V の場合は 1,6,11,16,29,26,23,20 *param1-10 はリモートアクセス管理（Web シングルサインオン）や RADIUS 管理（ユーザごとのアトリビュート）の際に使用する拡張パラメータです。 *apppassword は WebSSO 機能を利用する際の Web アプリケーション側のパスワードの項目です。	01	02	03	04	17	18	19	20	33	34	35	36	05	06	07	08	21	22	23	24	37	38	39	40	09	10	11	12	25	26	27	28	41	42	43	44	13	14	15	16	29	30	31	32	45	46	47	48
01	02	03	04	17	18	19	20	33	34	35	36																																						
05	06	07	08	21	22	23	24	37	38	39	40																																						
09	10	11	12	25	26	27	28	41	42	43	44																																						
13	14	15	16	29	30	31	32	45	46	47	48																																						
設定ファイル	加えてコマンド実行前に以下の設定ファイルを作成して下さい。 設定項目 <table><tr><th>行数</th><th>設定値</th></tr><tr><td>1</td><td>先頭行を項目名としてスキップ 1: スキップ 0: スキップしない</td></tr></table>	行数	設定値	1	先頭行を項目名としてスキップ 1: スキップ 0: スキップしない																																												
行数	設定値																																																
1	先頭行を項目名としてスキップ 1: スキップ 0: スキップしない																																																

	2	デバイスタイプ normal: 制限なし hyper: Cookie による制限 also: 個体識別番号による制限
	3	同期モード addonly: 追加更新のみ sync: 完全一致 delonly: 削除のみ
	4	読み込み行のフォーマット(読み込む行のフォーマットを指定してください。先頭の uid は固定です)
	5	デバイス ID sameas_uid: uid と同じ random: ランダムで生成
	設定ファイルサンプル	
	0 normal addonly uid,uemail,uname,ugroup,fixpass,defpass,upasschgforced,uexpiry,ucomment,accmail,param1,param2,param3,param4,param5,param6,param7.param8,param9,param10,apppassword sameas_uid	

コマンド例

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

3.16. バックアップ対象ファイル

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

ユーザ情報、セッション情報	/opt/passlogic/passlogicdata/
ログ情報	/var/log/passlogic/
httpd の設定ファイル	/etc/httpd/conf/httpd.conf /etc/httpd/conf.d/

標準インストール時には以下のファイル及びディレクトリになります。

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

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

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

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

*バックアップ・リストアを行う際にファイルおよびディレクトリのパーミッションが変わらないようにしてください。

3.17. 監視対象プロセス

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

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

3.18. 動作確認および死活監視について

PassLogic 本体(API)の動作確認

`http://{PassLogic ホスト名}:12079/passlogic/adm/api.cgi?mode=userread&uid={uid}`

{uid}は存在しないユーザ ID

code 21020311 が返れば PassLogic は動作しています。

リモートアクセス(mod_auth_passlogic)の動作確認

`http://{PassLogic ホスト名}/menu/?uid={uid}`

{uid}は存在しないユーザ ID

code 21030113 が返れば mod_auth_passlogic は動作しています。

RADIUS サーバの動作確認

任意のユーザで RADIUS 認証を試みる

Access-Reject が返れば RADIUS サーバは動作しています。

3.19. 管理者(admin)パスワードのリセット方法

管理者(ユーザ ID: admin)パスワードがロックされた場合は、以下の手順でリセットしてください。ゲートウェイサーバと認証サーバを分離している場合は、認証サーバ側で行ってください。

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

をテキストエディタで開きます。

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

の設定値を 1 に変更してください。

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

にブラウザでアクセスして「リセットボタン」をクリックしてください。

以上で、管理者のパスワード(パスワード位置情報)はリセットされますので

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

にアクセスして、パスワードを再設定してください。

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

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

の設定値を 0 に戻してください。

4. ユーザー管理者ガイド

4.1. 管理ツールにアクセスする

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

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

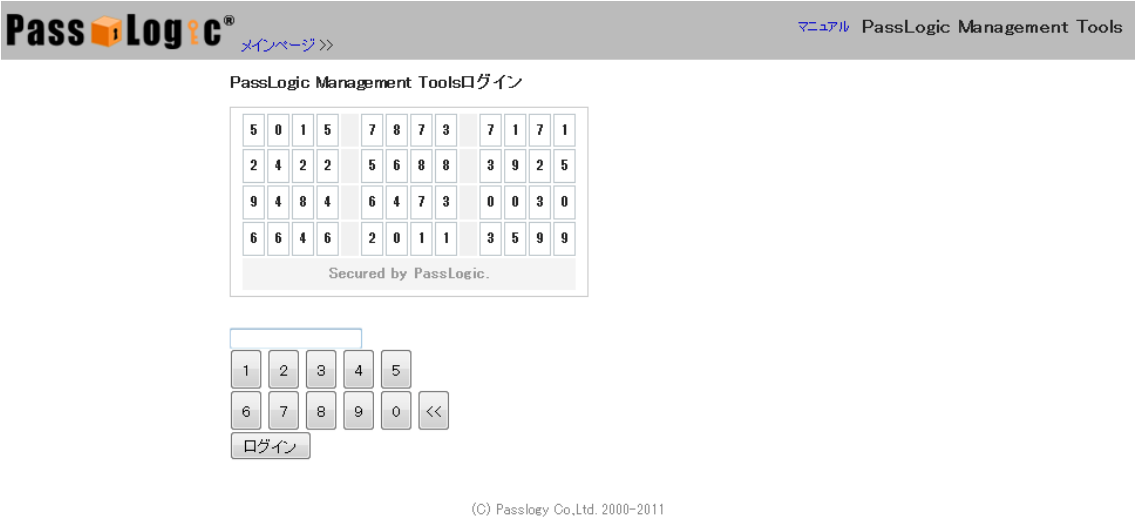
4.1.1. 管理ツールログイン用のユーザ ID を入力する

管理ツールログイン用の ID を入力します。

*インストール直後は「admin」になります。



4.1.2. 管理ツールログイン用のパスワードを入力する



4.2. PassLogic の状態を確認する

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

admin 権限管理者ログイン画面

PassLogic Authentication Server System - version 3.4.7.1

English(en) ▼ 送信

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

サーバステータス

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

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

operator 権限管理者ログイン画面

PassLogic Authentication Server System - version

English(en) ▼ 送信

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

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

PassLogic Authentication Server System – version x.x.x

4.2.1. PassLogic のバージョンを確認する

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

4.2.2. 登録されているライセンス情報を確認する

メインページ中に現在のライセンスの状態が表示されます。

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

4.2.3. PassLogic サーバのステータスを確認する

メインページ中にサーバステータス一覧が表示されます。

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

4.3. ユーザ作成

4.3.1. 新規作成

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

ユーザ ID (必須項目)	英数字・記号 (2-80 文字) -(ハイフン)_(アンダーバー).(ピリオド)@(アットマーク) ユーザ登録通知メール <%UID%> 部分
ID 同期削除対象外	ユーザー一括登録を完全一致で行う際、および LDAP 同期の完全一致で行う際に削除対象外となります。同期対象外ユーザは、同期対象外ユーザー一覧から確認できます。
メールアドレス	通知書をメールで送る場合は記入してください。
氏名	ユーザの氏名を入力します。 ユーザ通知メール<%UNAME%>部分
グループ	任意の文字列 (英数字) を設定します。 (例) soumu sales など
PIN	ワンタイムパスワードに付加する PIN (英数字*大文字小文字を区別する) の初期値を指定します。
初期パスワード位置情報 (ワンタイムパスワード)	ユーザに通知するパスワード位置情報を設定します。以下通知例*10 桁以上はアルファベット[A-Z]で表現します。 初期パスワード位置情報は 1234 5678 9ABC DE** ***** ***** ***** です。 空欄の場合はセキュリティポリシー設定の「初期パスワード位置情報」を通知します。 「パスワード位置情報をランダムに設定する」のチェックボックスを ☒ にすることでランダム生成したものを通知します。ワンタイムパスワードを設定しない(PIN のみでユーザ作成する等)の場合には、初期パスワード位置情報に NULL と入力してください。*PIN のみの場合でも認証する際に乱数表の取得は必須です。

初回にパスワード位置情報の変更が必要	初回（パスワード再発行後を含む）アクセス時に強制的にパスワード位置情報を変更させる場合は Yes に設定。パスワード変更しなくても良い場合は No に設定します。
ユーザアカウントの有効期限	ユーザアカウントの有効期限日を設定します。 設定した日までユーザアカウントは有効です。 アカウントの有効期限が切れても管理ツール上にアカウントは残っていますので、アカウントを削除したい場合は明示的に消す必要があります。 アカウントの有効期限切れ後、管理ツールより有効期限日を延長設定することで設定情報などをそのまま継続して利用可能です。
有効/無効	アカウントの有効/無効を選択します。 *無効の場合も登録ユーザ数としてカウントされます。
備考	メモとして自由にお使いいただけます。
param1～10	WebSSO 連携および RADIUS 連携の際に PassLogic から対象アプリケーション（または RADIUS クライアント）に対して、ユーザ毎に異なるパラメータ（またはアトリビュート）を送信する必要がある場合、param1～10 で入力した値を利用することができます。 （ケース 1）WebSSO で ID とパスワード以外にグループ ID などの値を送る必要がある場合 （ケース 2）SSL-VPN 連携時に機器毎に任意のアトリビュートを送出する必要がある場合
アプリケーションパスワード	WebSSO 連携時にアプリケーションに送信するパスワードです。複数のアプリケーションで異なるパスワードを利用している場合は上記 param の項目を使います。

4.3.2. デバイス追加

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

【 設定手順 】

- （i）「ユーザ管理」項目内『ユーザー一覧』または『ユーザ検索』 からユーザ ID をクリック。
- （ii）[デバイス追加]をクリック

- (iii) 必須項目（必要に応じてその他の項目）を入力し[次へ]をクリック
- (iv) 入力内容を確認し[登録]をクリック

【 項目解説 】

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

4.4. ユーザー一覧

左メニューの「ユーザー一覧」をクリックすることでユーザー一覧を見ることができます。

4.5. ロックユーザー一覧

左メニューの「ロックユーザー一覧」をクリックすることで、ロックされているユーザを一覧で見ることができます。

4.6. 同期対象外ユーザー一覧

左メニューの「同期対象外ユーザー一覧」をクリックすることで、ID 同期削除対象外ユーザを一覧で見ることができます。

4.7. ユーザ検索

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

4.8. ユーザー一括登録

CSV ファイルからユーザを作成します。

ファイル形式	CSV(カンマ区切りテキストファイル)
文字コード	ShiftJIS
デバイスタイプ	制限なし(どのパソコン、携帯でも利用できます) Cookie による制限(登録時の Cookie を参照して利用端末を制限します) 個体識別番号による制限(登録時の個体識別番号を参照して利用端末を制限します)
デバイス ID の設定モード	ユーザ作成時のデバイス ID の値を設定します。 ユーザ ID と同じ…通常はこちらを選択してください。 ランダム英数字列…Web トークン利用時にデバイス ID をランダムに設定した場合に選択してください。
動作モード	追加/更新のみ: 参照先のユーザ情報を PassLogic に追加・更新します。(ユーザ ID、PIN、初期パスワード位置情報は更新されません) 削除のみ: PassLogic 上のユーザ情報を削除します。CSV ファイルに ID があるユーザが削除対象となります。 完全同期: 参照先と PassLogic のユーザ情報を完全に同期します。PassLogic 上に存在するユーザ ID が参照先に存在しない場合は PassLogic のユーザが削除されます。admin 権限ユーザは削除対象になりません。ID 同期削除対象外は削除対象になりません。

CSV ファイルのフォーマット

項目名	設定可能値	補足
ユーザ ID(必須)	英数字、記号 (-_.@)	2-80 文字
メールアドレス	制限なし(*1)	email アドレス
氏名	制限なし(*1)	実名
グループ	英数字	20 文字まで。
PIN	半角英数字	ワンタイムパスワードの頭に付加する PIN
初期パスワード位置情報	初期のパターン	空欄の場合はユーザごとにランダム発行します。 指定する場合は、パスワード位置情報を設定してください。 V の場合は 1,6,11,16,29,26,23,20

		NULL でパスワード位置情報を設定しません。(この場合 PIN が必須になります)
初回にパスワード位置情報の変更が必要	Y or N	Y:強制パスワード変更する N:強制パスワード変更しない (空欄の場合は N)
ユーザアカウントの有効期限	yyyymmdd	ユーザアカウントの有効期限。空欄の場合は期限切れなし。
備考	制限なし(*1)	ユーザの備考
メール通知	Y or N	ユーザ追加時にメールで通知するか否か。(空欄の場合は N)
param1-10	制限なし(*1)	他のシステムと連携する際に利用する値です。通常は利用しません。
アプリケーションパスワード	制限なし(*1)	WebSSO(シングルサインオン)機能を利用する際に、ウェブアプリケーションのパスワードを入力します。

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

(例:「テスト”01”ユーザ」 →”テスト””01””ユーザ”)

*それぞれの値には改行コードを含めないでください。

4.8.1. CSV ファイルのダウンロード

登録ユーザ情報を CSV 形式でダウンロードします。フォーマットはユーザー一括登録時のフォーマットと同様になり、最大で 10000 件のユーザデータをダウンロード可能です。(10000 件のダウンロード時にエラーが発生する場合は、以下の設定を変更し再度お試しください)

/etc/php.ini

```
max_execution_time = 60
```

4.9. ユーザサポートについて

4.9.1. ユーザアカウントがロックされた場合のサポート

ロック中のユーザは、ロック項目の背景が赤くなり文字列が「ロック解除」となります。

ロック解除の文字をクリックすることでロックを解除することができます。この操作は「ユーザー一覧」「ロックユーザー一覧」「ユーザ検索」で実行できます。

4.9.2. ユーザがパスワードを忘れた場合のサポート

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

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

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

通知書をメール … 設定したメールアドレス宛に通知書をメール送信します。

通知書をプリントアウト … プリントアウト用の通知書が表示されます。

通知書の表示例

PassLogic利用開始のお知らせ

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

WebアクセスURL

<http://remote.example.com/menu/>
にアクセスして以下のログイン情報でログインしてください。

ユーザID: user01

PIN: Xs56a0W

※PIN下のパスワード位置情報の前に追加してください。

初期パスワード位置情報は

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

です。

お問い合わせは
システム部 パスロジ太郎
00-0000-0000

© 2007-2010 Passlogy Co.,Ltd.

4.9.3. 通知メールが届かない場合のサポート

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

4.9.4. System error occurred. Please contact system administrator.

リモートアクセスのユーザのログイン画面に「System error occurred. Please contact system administrator.」と表示された場合は、システム (OS) に何らかの問題が発生している可能性がありますので、httpd のエラーログ (SSL 通信を行っている場合は SSL のエラーログ) を参照してください。

4.10. ログ・リファレンス

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

4.10.1. ログフォーマット

基本ログ	PassLogic ログ
月 日 時間 IP アドレス	ログレベル ステータス コード コメント [ユーザーエージェント] [IP アドレス] [クライアントのクッキー] [サーバのクッキー] [デバイス ID]

4.10.2. ログ：ステータスリファレンス

code	loglevel	status	comment
21020094	alert	NG	ライセンスによるユーザ数の上限を越えています。
21020097	alert	NG	ライセンスの有効期限が切れています。ライセンスを更新してください。
21020098	warning	NG	入力データが不正です。
21020099	emerg	NG	システムエラーです。
21020101	notice	OK	ユーザを新規作成しました。
21020111	warning	NG	すでに存在しているのでユーザを作成できません。
21020112	warning	NG	ユーザ作成時のパラメータが正常ではありません。
21020199	emerg	NG	ユーザ作成時にシステムエラーが発生しました。
21020201	notice	OK	ユーザを削除しました。
21020211	info	NG	ユーザが存在しないため削除できません。
21020299	emerg	NG	ユーザ削除時にシステムエラーが発生しました。
21020301	info	OK	ユーザ情報取得に成功しました。
21020311	info	NG	ユーザ情報取得時のパラメータが正常ではありません。
21020399	emerg	NG	ユーザ情報取得時にシステムエラーが発生しました。
21020401	info	OK	ユーザ情報の編集を完了しました。
21020411	warning	NG	ユーザが存在しないため編集できません。
21020412	warning	NG	ユーザ編集時のパラメータが正常ではありません。
21020499	emerg	NG	ユーザ編集時にシステムエラーが発生しました。
21020501	warning	OK	ロックしました。
21020502	info	OK	そのユーザは、すでにロックされています。
21020511	warning	NG	ユーザが存在しないためロックできませんでした。
21020512	warning	NG	ロック時のパラメータが正常ではありません。
21020599	emerg	NG	ロック時にシステムエラーが発生しました。

21020601	warning	OK	ロックを解除しました。
21020602	info	NG	そのユーザは、ロックされていないためロック解除できませんでした。
21020611	warning	NG	そのユーザが存在しないためロック解除できません。
21020612	warning	NG	ロック解除時のパラメータが正常ではありません。
21020699	emerg	NG	ロック解除時にシステムエラーが発生しました。
21020701	info	OK	ユーザー一覧の取得に成功しました。
21020702	info	OK	ユーザが存在しないためユーザー一覧を取得できませんでした。
21020799	emerg	NG	ユーザー一覧取得時にシステムエラーが発生しました。
21020801	info	OK	ロックユーザー一覧の取得に成功しました。
21020802	info	OK	ロックされているユーザが存在しないため一覧を取得できませんでした。
21020899	emerg	NG	ロックユーザー一覧取得時にシステムエラーが発生しました。
21021101	info	OK	パスワードを初期化しました。
21021111	warning	NG	ユーザが存在しないためパスワードを初期化できません。
21021199	emerg	NG	パスワード初期化時にシステムエラーが発生しました。
21022101	notice	OK	デバイスIDを新規作成しました。
21022111	warning	NG	ユーザが存在しないためデバイスIDを作成できませんでした。
21022112	warning	NG	デバイスID作成時のパラメータが正常ではありません。
21022115	warning	NG	すでにそのデバイスIDが存在しているため作成できません。
21022199	emerg	NG	デバイスID作成時にシステムエラーが発生しました。
21022201	notice	OK	デバイスIDを削除しました。
21022211	info	NG	デバイスIDが存在しないため削除できません。
21022212	warning	NG	ユーザが存在しないためデバイスIDを削除できません。
21022213	warning	NG	そのユーザは、指定されたデバイスIDを持っていません。
21022214	warning	NG	デバイス削除時のパラメータが正常ではありません。
21022299	emerg	NG	デバイス削除時にシステムエラーが発生しました。
21022301	info	OK	デバイス情報の取得に成功しました。
21022311	info	NG	デバイスが存在しないため情報取得できませんでした。
21022312	warning	NG	ユーザが存在しないためデバイス情報を取得できません。
21022313	warning	NG	指定されたユーザは、指定されたデバイスを持っていません。
21022314	warning	NG	デバイス情報取得時のパラメータが正常ではありません。
21022399	emerg	NG	デバイス情報取得時にシステムエラーが発生しました。
21022401	info	OK	デバイス情報を編集しました。
21022411	warning	NG	デバイスが存在しないため編集できません。
21022412	warning	NG	ユーザが存在しないためデバイスを編集できません。
21022413	warning	NG	指定されたユーザは、指定されたデバイスを持っていないため編集できません。

21022499	emerg	NG	デバイス編集時にシステムエラーが発生しました。
21022501	info	OK	メールを送信しました。
21022511	warning	NG	デバイスが存在しないためメールを送信できません。
21022512	warning	NG	ユーザが存在しないためメールを送信できません。
21022513	info	NG	指定されたユーザは、指定されたデバイスを持っていません。
21022514	warning	NG	そのユーザはメールアドレスが登録されていないためメールを送信できません。
21022599	warning	NG	システムエラーが発生したためメールを送信できませんでした。
21022601	notice	OK	パスワード再設定メールを送信しました。
21022611	warning	NG	ユーザ ID が指定されていないためパスワード再設定メールを送信できません。
21022612	warning	NG	パスワード再設定時のパラメータ(ユーザ ID)が正常ではありません。
21022613	warning	NG	メールアドレスが指定されていないためパスワード再設定メールを送信できません。
21022614	warning	NG	パスワード再設定時のパラメータ(メールアドレス)が正常ではありません。
21022621	warning	NG	ユーザが存在しないためパスワード再設定メールを送信できません。
21022622	warning	NG	メールアドレスが登録されているものと異なります。
21022699	emerg	NG	パスワード再設定時にシステムエラーが発生しました。
21022701	notice	OK	パスワードをリセットしました。
21022711	warning	NG	キーが指定されていないためパスワードをリセットできません。
21022712	warning	NG	キーが存在しないためパスワードをリセットできません。
21022713	warning	NG	キーの有効期限が切れているためパスワードをリセットできません。
21022799	emerg	NG	パスワードリセット時にシステムエラーが発生しました。
21023101	info	OK	認証ボックスを新規作成しました。
21023111	warning	NG	すでに認証ボックスが存在します。
21023112	warning	NG	不正な設定です。
21023199	emerg	NG	システムエラーです。
21023201	info	OK	認証ボックスを削除しました。
21023211	info	NG	すでに認証ボックスが存在しません。
21023212	warning	NG	認証ボックスの削除に失敗しました。
21023299	emerg	NG	システムエラーです。
21023301	info	OK	情報取得に成功しました。
21023311	info	NG	認証ボックスが存在しません。
21023399	emerg	NG	システムエラーです。
21023401	info	OK	書き込みを完了しました。
21023411	warning	NG	認証ボックスが存在しません。
21023412	warning	NG	不正な設定です。

21023499	emerg	NG	システムエラーです。
21030101	notice	OK	乱数生成
21030111	warning	NG	認証ボックスが見つかりません。
21030112	warning	NG	アカウントがロックされているため乱数表を取得できませんでした。
21030113	warning	NG	ユーザ情報が不正です。
21030115	warning	NG	パスワード変更が必要です。
21030116	warning	NG	有効期限切れです。
21030117	warning	NG	パラメータが正常ではありません。
21030118	notice	OK	ダミー乱数表示
21030119	notice	NG	利用が許可されていません。
21030120	notice	NG	現在アクセス制限されています。
21030199	emerg	NG	システムエラーです。
21030201	info	OK	キャンセルしました。
21030211	warning	NG	認証ボックスが見つかりません。
21030213	warning	NG	ユーザ情報が不正です。
21030299	emerg	NG	システムエラーです。
21030301	notice	OK	パスワード変更が正常に推移しています。
21030302	info	OK	キャンセルしました。
21030303	notice	OK	パスワード変更が正常に終了しました。
21030311	warning	NG	セッション ID が違います。もう一度最初からお願いいたします。
21030312	warning	NG	パスワード位置情報に英数字以外の文字が含まれています。
21030313	warning	NG	パスワード位置情報の桁数を適切にしてください。
21030314	warning	NG	位置が特定できませんでした。ご確認のうえ、もう一度やりなおしてください。
21030315	warning	NG	パスワードが不正解です。
21030316	warning	NG	入力データが不正です。
21030317	warning	NG	過去に設定された位置への変更はできません。別の位置を設定してください。
21030320	warning	NG	その位置は禁止されています。別の位置を設定してください。
21030322	warning	NG	PIN に英字と数字を少なくとも 1 つ以上含める必要があります。
21030399	emerg	NG	システムエラーです。
21040101	notice	OK	認証 OK
21040111	warning	NG	ユーザ名 または パスワードが違います。
21040114	warning	NG	乱数表が有効期限切れです。
21040115	warning	NG	ロック・アウトまでの連続失敗回数に達したためロックがかかりました。
21040118	warning	NG	存在しない認証ボックス番号。
21040119	warning	NG	入力データが不正です。

21040199	emerg	NG	システムエラーです。
21050101	info	OK	PassLogic 設定を更新しました。
21050111	warning	NG	PassLogic 設定時の入力データが正常ではありません。
21050199	emerg	NG	PassLogic 設定時にシステムエラーが発生しました。
21060101	notice	OK	RADIUS 認証に成功しました。
21060111	warning	NG	RADIUS 認証に失敗しました。
21060115	warning	NG	ロック・アウトまでの連続失敗回数に達したためロックがかかりました。
21060119	warning	NG	入力データが不正です。
21060199	emerg	NG	システムエラーです。
21070101	notice	OK	アクティベーションに成功しました。
21070102	info	OK	デバイスタイプ表示
21070111	warning	NG	正しいキーではありません。
21070112	warning	NG	携帯端末情報が受け取れませんでした。
21070113	warning	NG	携帯端末情報の書き込みに失敗しました。
21070114	warning	NG	端末制限用 Cookie が発行できませんでした。
21070115	warning	NG	不正なデバイスです。
21070199	warning	NG	システムエラーです。

4.10.3. ログのサイズ

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

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

logrotate の初期設定

```
/var/log/passlogic/*.log {  
    size=+1024k  
    notifempty  
    missingok  
}
```

ログのディレクトリ

```
/var/log/passlogic/
```