トークンレス・ワンタイムパスワード

PassLogic エンタープライズ版

バージョンアップ概要とリリースノート（エンタープライズ版 v2.0.0）

2015/4/15

PASSLOGY™

インデックス

(C) 2015 PASSLOGY Co.,Ltd

はじめに

表記について

文字数の制約のために、一部下記の省略表記をしています。

＞正式名称：PassLogic エンタープライズ・エディション
省略表記1：エンタープライズ版
省略表記2：Ent

＞正式名称：PassLogic スタンダード・エディション
省略表記1：スタンダード版
省略表記2： Std

(C) 2015 PASSLOGY Co.,Ltd

リリースノート

リリースノート

【機能アップ】

・Webトークン機能が追加され、専用クライアントのログインに利用できるようになりました。
・マルチポリシー機能が追加され、利用者ごとに認証方式を変更できるようになりました。
・時間同期型のソフトウェアトークン（PassClip）に対応しました。
・カスタムURLスキーム連携に対応し、スマートデバイスアプリと容易に連携できるようになりました。
・多重ログインを防止する機能が追加されました。
・お問合せサポートに必要な情報を一括でダウンロードできる機能が追加されました。
・パスワードのセルフリマインダー機能が追加され、パスワード忘れを管理者不在でリカバリできるようになりました。
・ポータルメニューに表示されるアプリケーションリンクの表示/非表示を選べるようになりました。
・ADアカウントに基づいてPassLogic上のアカウントを定期的に削除できるようになりました。
・通知メールの種別ごとに文章テンプレートが編集できるようになりました。
編集可能な文章テンプレートは「新規ユーザに送信されるメール」「端末登録時に送信されるメール」
「パスワード再発行時に送信されるメール」「パスワードリマインダーから送信されるメール」です。
・パスワード変更時に「現在のパスワード要求」をスキップできるようになりました。
・シークレットパターンの一筆書き設定を禁止できる設定が追加されました。
・メール送信機能 CCとBCCの宛先を指定することができるようになりました。

【機能改善・不具合修正】

・アプリケーション名に「'」「 <」「>」「"」を使った場合 sso url(/ui/?sso-webapp, /ui/?sso-vpn, /ui/?sso-saml) が正常動作しない不具合を修正しました。
・シングルサインオンの途中で瞬間的に挿入されるページからloginボタンを非表示とし、任意のメッセージを表示できるように変更しました。
・セッションタイムアウト時のメッセージを変更しました。
・端末固定機能において永続Cookieの有効期限を30日から360日に変更しました。
・PassLogicのソフトウェア・テンキーがiOS8に対応しました。
・端末固定機能のためのアクティベートメールを各端末ごと（異なるメールアドレス）に送信できるようになりました。
・端末固定機能において1台目の端末を登録するアクティベート手順が変更されました。
・ポータルメニューに表示されるアプリケーションリンクの表示順をWebAPP以外についても指定できるようになりました。
・PassLogicへのアクセスポートはSSL通信（443）がデフォルト値となりました。
・初回ログイン用の管理者パスワードが固定値からランダム値となりました。
・ADサーバがダウンしているときにはPassLogicのログイン画面に障害状況が表示されるようになりました。
・WebSSO機能において、特殊文字のサニタイズ不備による連携不具合（ユーザ情報paramが正しく送信できない）を修正しました。
・リストア後にレプリケーション構成の構築スクリプトを実行すると発生するエラーを修正しました。
・ユーザー括登録でユーザの有効期限が正しく取り込めない不具合を修正しました。

【その他】

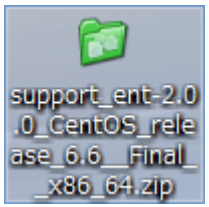
・ユーザー新規作成時の入力補助機能（テンプレート）を廃止しました。
・PassLogicサーバ（サーバセッション）上のADパスワードを暗号化して保持するようになりました。

(C) 2015 PASSLOGY Co.,Ltd

機能アップ

サポート情報のダウンロード機能を追加

スタンダード版相当



取得される情報

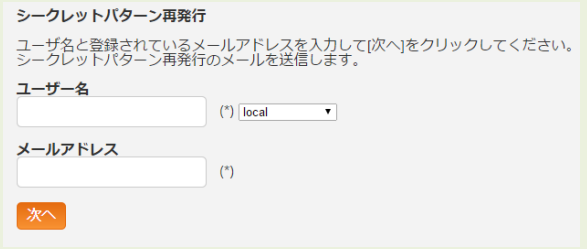
- **OS の種類**
  （バージョンなど）
- **サーバ設定ファイル**
  (/etc/httpd/conf, /etc/httpd/conf.d, /etc/php.ini)
- **PassLogic設定ファイル**
  (/opt/passlogic/data)
- **ログファイル**
  (/var/log/httpd, /var/log/radiusd, /var/log/passlogic , /var/log/passlogic-pgpool, /opt/passlogic/pgsql/data/serverlog)

※ユーザー情報は含まれません。

パスワードリマインダ機能を追加

スタンダード版相当

- ✓ **専任のシステム担当者がいない**
- ✓ **夜間・休日のサポートはできない**



1）パスワードの再発行を依頼

2）本人のメールに確認用URLを通知

3）URLをクリック

4）新規パスワード通知

PassLogic

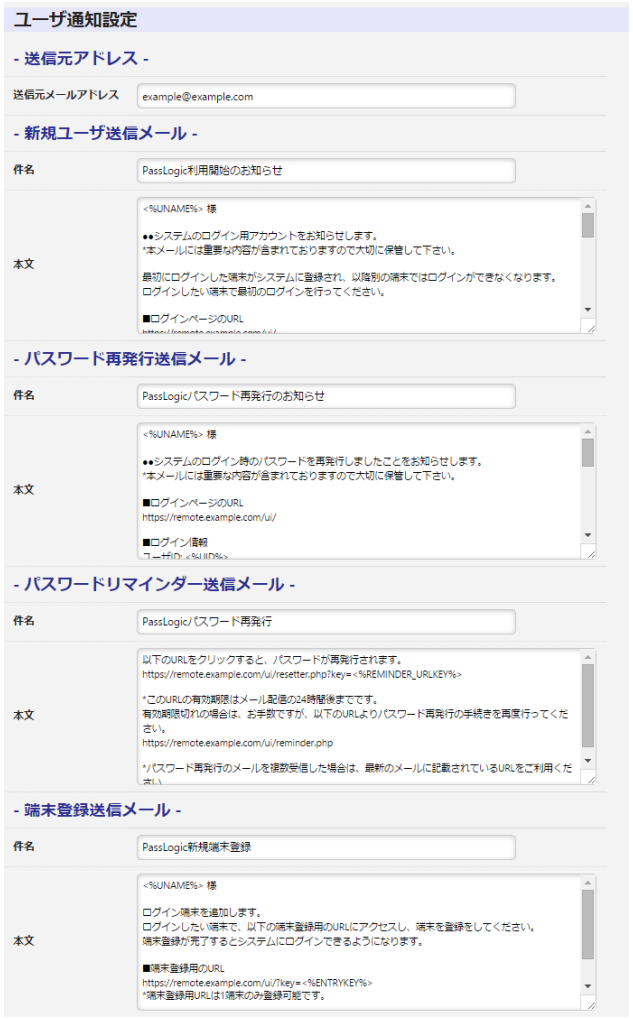
管理ツールでON/OFF設定 ▶

(C) 2015 PASSLOGY Co.,Ltd

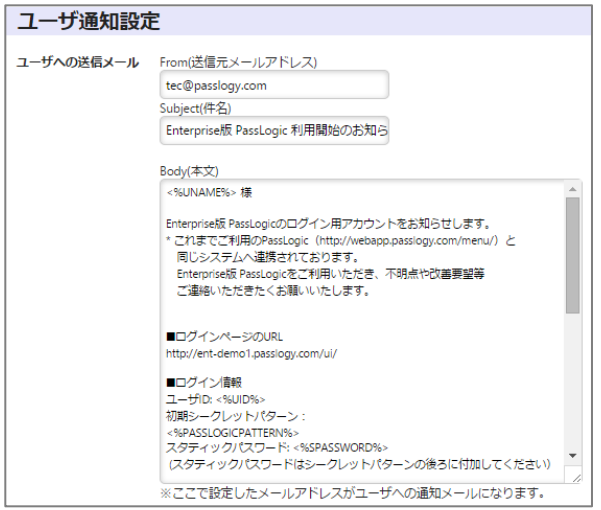
メール通知機能を拡張

新規追加時のメールの他、パスワード再発行、パスワードリマインダー、端末登録のメールが編集できます。

スタンダード版相当



旧 エンタープライズ版 v1.2.3



(C) 2015 PASSLOGY Co.,Ltd

拡張URLスキーム対応（スマートフォンアプリ連携）

スタンダード版相当

本機能を使うことで、スマートフォン用アプリへ値を引き渡すことができます。

スタンダード版よりも汎用的な設定が可能となり、様々なスマートデバイスアプリと容易に連携できます。
（スタンダード版ではCisco社のVPNクライアントであるAnyConnect専用でした。）

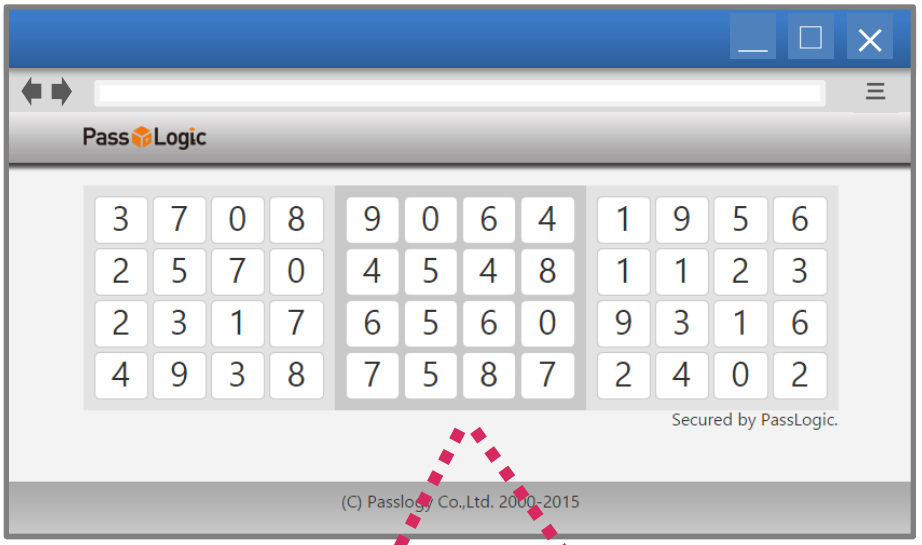
アプリを起動し
IDとPWを引き渡し

クライアントアプリ

Webトークン機能を追加

スタンダード版相当

専用クライアントソフトの認証強化にもお使いいただけるようになります。



主なクライアントソフト

Windows 標準クライアント
Horizon View Client
Cisco ASA AnyConnect
FortiClient
SonicWall NetExtender
PaloAlto　　など

Juniper　JunosPulseやF5 EdgeClientは
Webトークン以外の連携方法が用意されています。

ソフトトークン機能を追加（PassClip）

新機能

PassClip（パスクリップ）

※PassClipは無償でダウンロードできます。
※2015年5月以降にワンタイムパスワード対応版をリリース予定です。
※PassClipはiOS、Android専用アプリです。

(C) 2015 PASSLOGY Co.,Ltd

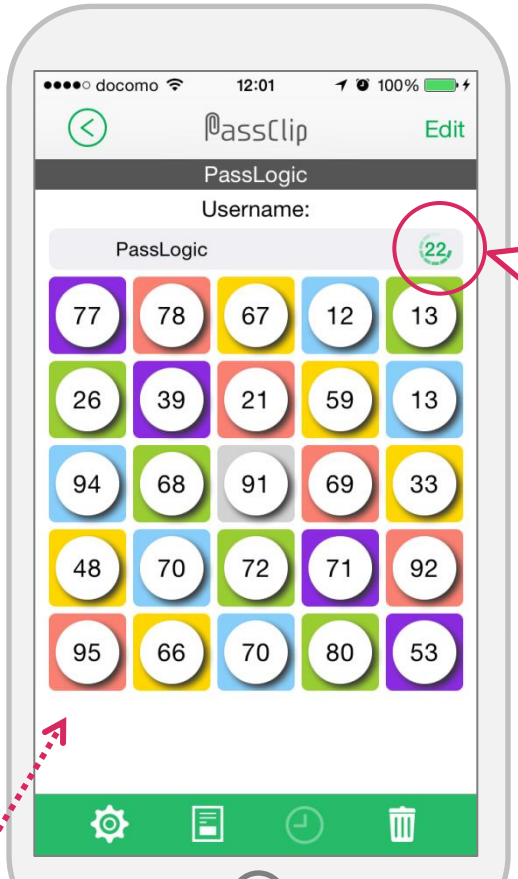
他社製ソフトトークンとの違い

新機能

一般的なソフトトークン

誰にでも正解がわかるため
端末を紛失した時のリスクが高い
リモートアクセスにおいて、紛失時
のセキュリティはとても重要！

PassClip



30秒ごとに
グリッド表が更新！

正解が分かるのは
本人だけ！

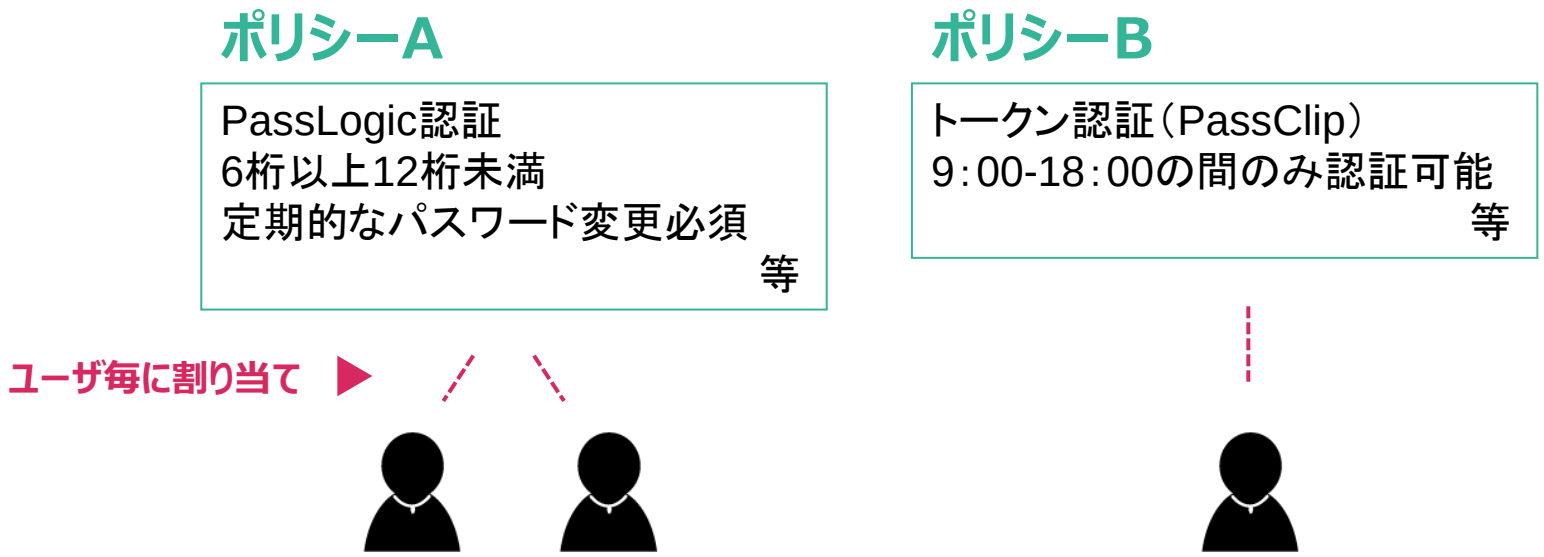
(C) 2015 PASSLOGY Co.,Ltd

マルチポリシー機能を追加

新機能

パスワードポリシーが複数作成できるようになりました。

「アクセスするシステムによってパスワードポリシーを変えたい」
「一般従業員と取締役で認証方式を分けたい」
にお応えできるようになりました。



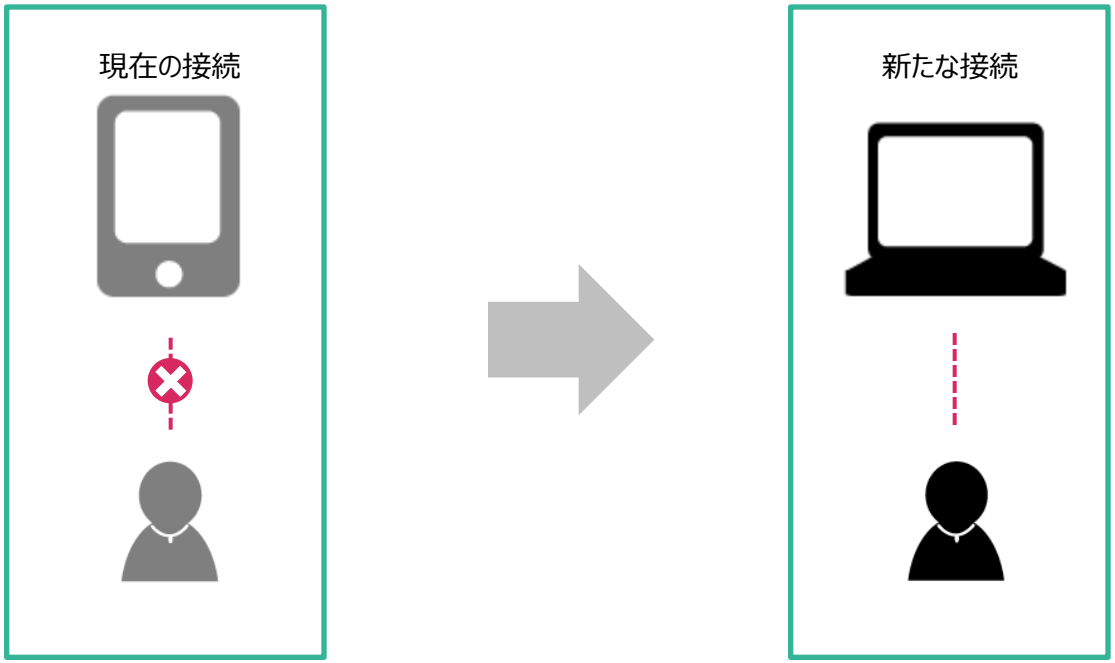
(C) 2015 PASSLOGY Co.,Ltd

多重ログイン禁止設定を追加

新機能

1アカウントによる多重ログインを禁止できるようになりました。

別の端末からの接続があると、古いセッションがログアウトします。



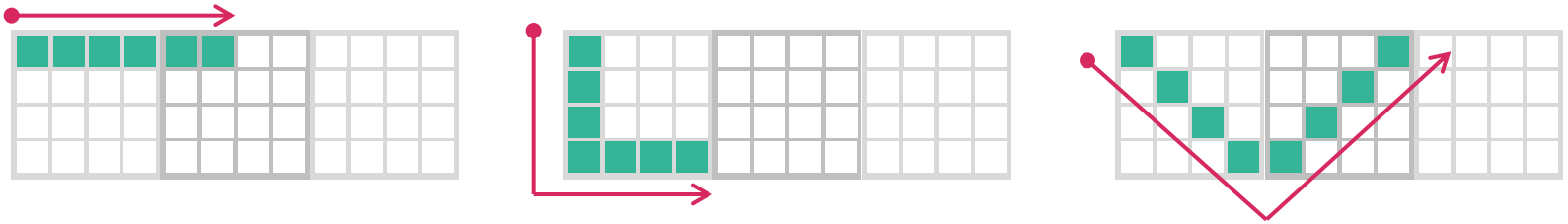
(C) 2015 PASSLOGY Co.,Ltd

シークレットパターンの制約事項を追加

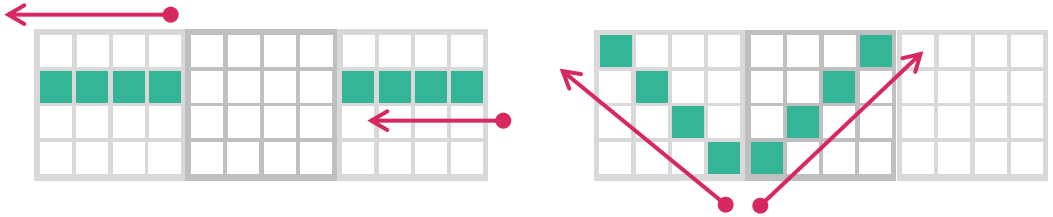
新機能

一筆書きのシークレットパターンを、禁止できるようになります。

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。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。



次のシークレットパターンは一筆書きとはみなされません。



設定を一つ入れるだけで、一筆書きのシークレットパターンを全て禁止可能！

これまで通り、以下の設定もご利用いただけます。

- 禁止シークレットパターン（禁止するシークレットパターンを一つずつ設定）
- 3ブロック全ての利用を強制

(C) 2015 PASSLOGY Co.,Ltd

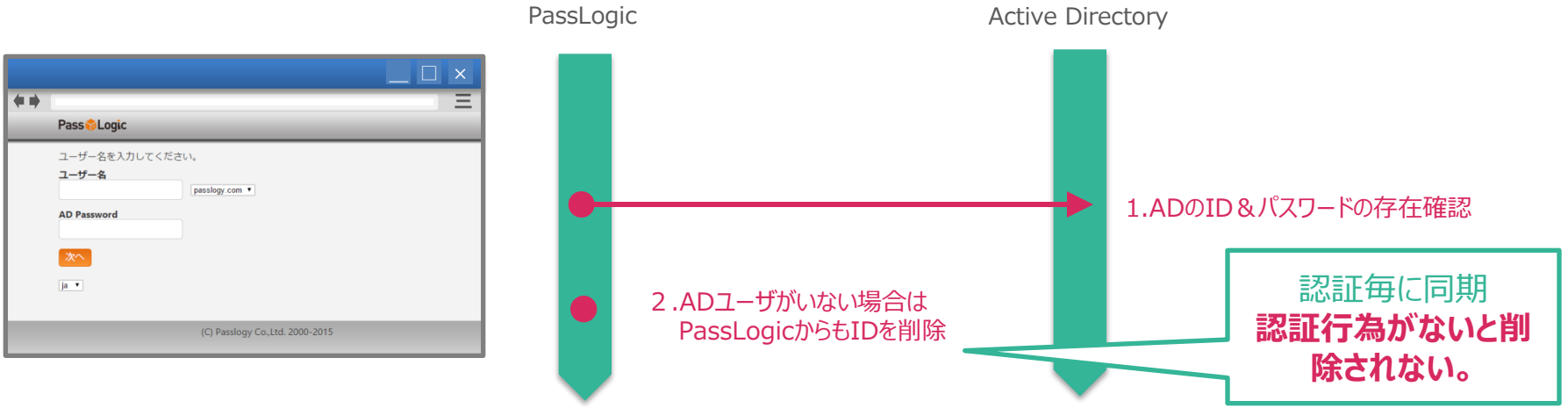
AD連携機能を拡張

新機能

ADアカウントに基づいてPassLogic上のアカウントを定期的に削除できるようになりました。

存在しないADアカウントがPassLogicに残ってしまう問題が解決します。

◆ **現在の問題点**



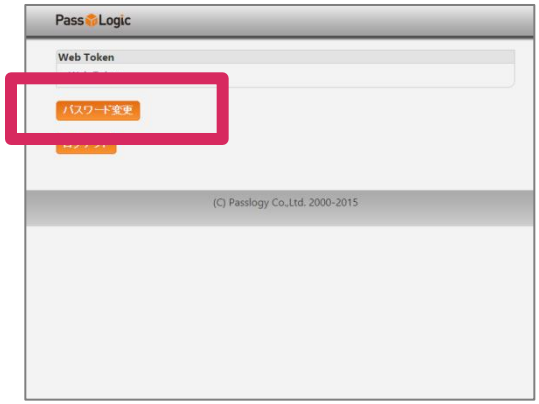
スケジューリング設定で、自動的にADアカウントの存在確認ができるため、ユーザーIDの棚卸が容易になります。

パスワード変更時の本人確認を省略

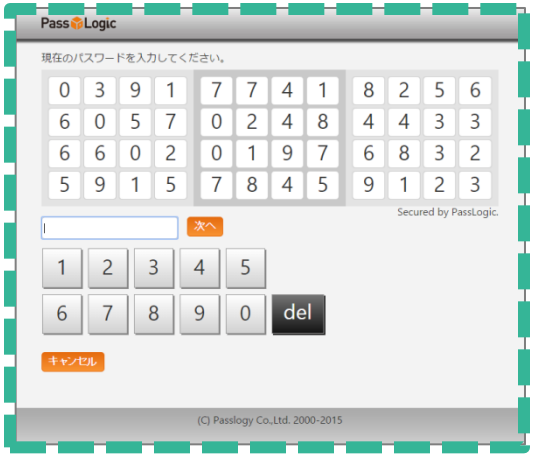
新機能

パスワード変更時のパスワード入力を省く設定（ON/OFF）が可能になりました。

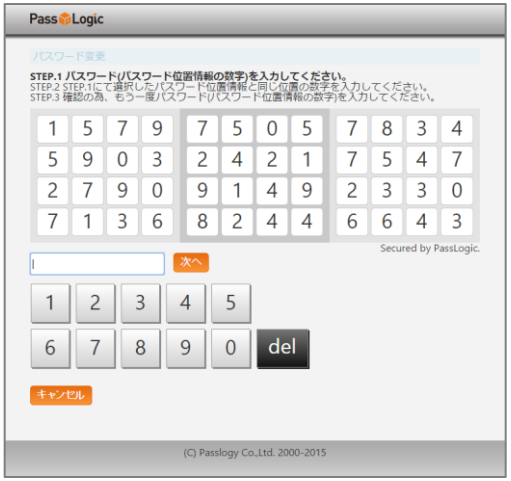
①「パスワード変更」をクリック



②現在のパスワードを入力



③パスワード変更開始



省略可能に！

ユーザーの手間が減り
さらに使いやすくなります。

機能改善・不具合修正

初回アクティベート手順を変更

端末固定機能において、Cookieをブラウザにセットする際の
1台目の手順が変更になりました。

新バージョン(v2.0.0)

利用案内文

■ログインページのURL
https://remote.example.com/ui/

■ログイン情報
ユーザID: user01
ドメイン: local
初期シークレットパターン:
1234 56** ****
**** **** ****
**** **** ****
**** **** ****

通常通りにログインすると端末にCookieがセットされます。
Cookie固定するしないにかかわらず、一回目のログインURLは共通

2台目以降の端末登録

利用案内文

<%UNAME%> 様

端末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。

■端末登録用のURL
https://remote.example.com/ui/?key=<%ENTRYKEY%>
*端末登録用URLは1端末のみ登録可能です。

旧バージョン（v1.2.3）

利用案内文

端末を登録してください。
https://remote.example.com/ui/?key=<%ENTRYKEY%>

■ログインページのURL
https://remote.example.com/ui/

■ログイン情報
ユーザID: user01
ドメイン: local
初期シークレットパターン:
1234 56** ****
**** **** ****
**** **** ****
**** **** ****

端末固定専用のURLをクリックすると端末が固定されます。

2台目以降の端末登録

初回の端末登録と同じメール

2台目以降はCookie登録用URLの通知メール

(C) 2015 PASSLOGY Co.,Ltd

初回アクティベート手順を変更（管理画面イメージ）

管理者"admin"の初期パスワード設定手順を変更

初回ログイン用の管理者パスワードがランダム値の発行に変わります。

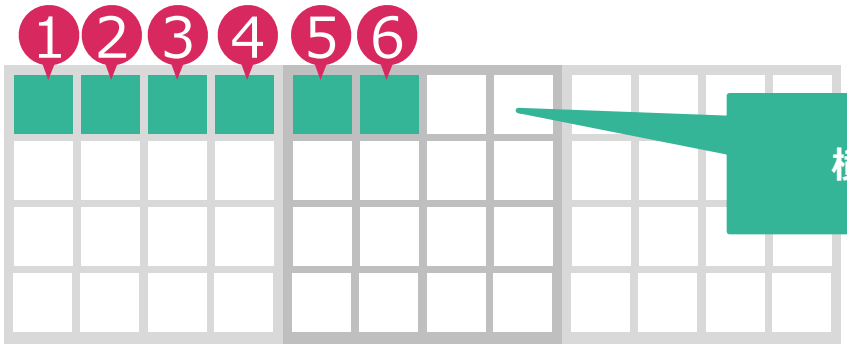
新バージョン(v2.0.0)

```
(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
```

adminの初期パスワード

旧バージョン（v1.2.3）



横に6か所の固定値

(C) 2015 PASSLOGY Co.,Ltd

その他

製品ロゴが変更になります。

新バージョン(v2.0.0)

PassLogic

旧バージョン（v1.2.3）

PassLogic®

後日改めて製品ロゴの変更についてご案内させていただきます。

利用者向けマニュアルのサンプルを同梱

利用者向けマニュアルのサンプルファイルを同梱いたします。
編集可能なワード形式（.doc）となりますので、お客様の設定や運用に合わせてカスタマイズしてご利用ください。

マニュアルに記載される説明サンプルの項目

・パスロジック認証について
　- パスロジックの用語説明
・初回ログイン
・シークレットパターンの変更方法
・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

(C) 2015 PASSLOGY Co.,Ltd

比較表

比較表（Std v3.8.0 & Ent v2.0.0）

	スタンダード版 v3.8.0	エンタープライズ版　v2.0.0
データ保持の方法	ファイル	データベース（postgresql）
ActiveDirectoryとのID同期	△ 定期同期（スケジューリング）	◎ リアルタイム同期（ユーザ認証毎） 今後のバージョンアップで定期同期も実装予定
冗長化機能	△ rsync、NAS、LifekeeperなどのOSや別製品の組み合わせ（アクセスの振り分けは別途ロードバランサを利用）	◎ 標準機能としてデータベース・レプリケーションを提供（アクセスの振り分けは別途ロードバランサ利用）
携帯電話（フィーチャーフォン）対応	◎	× 未対応
ソフトトークン（スマートフォンアプリ）対応	×	◎（PassClipに対応）
マルチポリシー	×	◎
端末固定（Cookie制限）	◎（ユーザ毎に設定）	◎（ポリシー毎に設定）
管理者アカウント	ユーザIDとしてカウントする	ユーザIDとしてカウントしない
管理者階層	admin：フルアクセス権限 operator：ユーザロック/アンロック、パスワード再発行のみ	admin：フルアクセス権限 useradmin：ユーザ作成・編集・削除・無効化、ユーザロック、端末固定＋operator権限 operator：アンロック・パスワード再発行
スタティックパスワードの設定	◎ 初期発行時はワンタイムパスワードの前に付加	◎ 初期発行時はワンタイムパスワードの後ろに付加
初期パスワードのランダム発行	◎ 固定値の設定も可能	◎ ランダム発行のみ
ダミー乱数表の表示	◎ OFFも可能	◎
API	◎	△ 今後のバージョンアップで提供予定。現在は認証部分のみ可。

(C) 2015 PASSLOGY Co.,Ltd

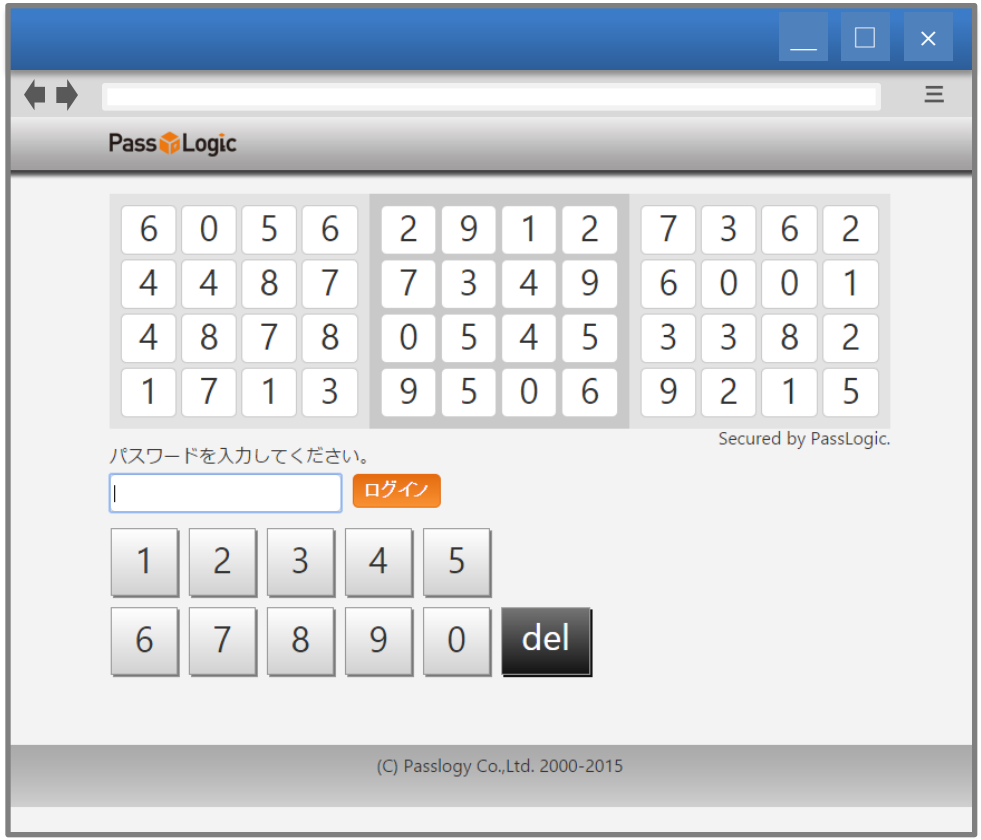
比較表（Std v3.8.0 & Ent v2.0.0）

	スタンダード版 v3.8.0	エンタープライズ版 v2.0.0
管理GUIポート	12080	8443
利用者UIポート	443 or 80	443
管理ツールの一元化	× GWサーバを分離する場合は、GWと認証サーバ両方で分割して管理	◎ すべての設定はバックエンドの認証サーバ側で管理
ライセンスファイル登録の一元化	× GWサーバを分離する場合は、GWと認証サーバ両方に登録が必要	◎ 全てをバックエンド側で管理
ユーザーインターフェースURLの統合	× 連携方式・端末別に異なる /menu/,/tmenu/ /imenu/,/mmenu/ /uagent/,/passlogic/ui/	◎ 全ての端末で共通のURL /ui/
前回ログイン情報の表示	◎ 前回ログイン日時・位置情報の有効期限 表示設定可能	× 今後対応を検討
エラーメッセージ	日本語・英語	英語のみ（今後のバージョンアップで対応予定）
ADドメイン（￥）付きユーザID送信	△ paramとしての送信のみ可能	◎
カスタムURLスキーム	△ CiscoASA AnyConnectのみ対応	◎ 汎用的な設定が可能
冗長構成時の追加ライセンス	△ 50%の追加費用が発生（1000ID以下の場合のみ）	◎ 追加費用不要
ディザスタリカバリ構成時の追加ライセンス	× 別拠点にサーバを設置する場合は、2システム分（200%）の費用が必要になります。	◎ ソフトウェア費用の25%の追加費用でご利用いただけます。

(C) 2015 PASSLOGY Co.,Ltd

比較表（Std v3.8.0 & Ent v2.0.0）

エンタープライズ版　ログイン画面



スタンダード版　ログイン画面