

発行
ライセンス数
1,170,000
件以上

※2020年2月現在

200社以上の
企業・団体が
導入

16件の
クラウド
サービスに
採用

“セキュリティ”と“業務効率化”の両立を
実現する認証プラットフォーム

Pass Logic

— パスロジック —



パッケージ版

&

クラウド版



自社サーバー運用とクラウドサービス(SaaS)から選択OK!

- トークンレス・ワンタイムパスワード
- Windows端末の認証強化
- 2要素認証
- ユーザー情報自動登録
- ソフトウェアトークン

- シングルサインオン
- クライアント証明書による端末制限
- ユーザーサポート自動化
- ハードウェアトークン
- IPアドレス制限

業務効率を加速する認証プラットフォーム

PassLogic

— パスロジック —

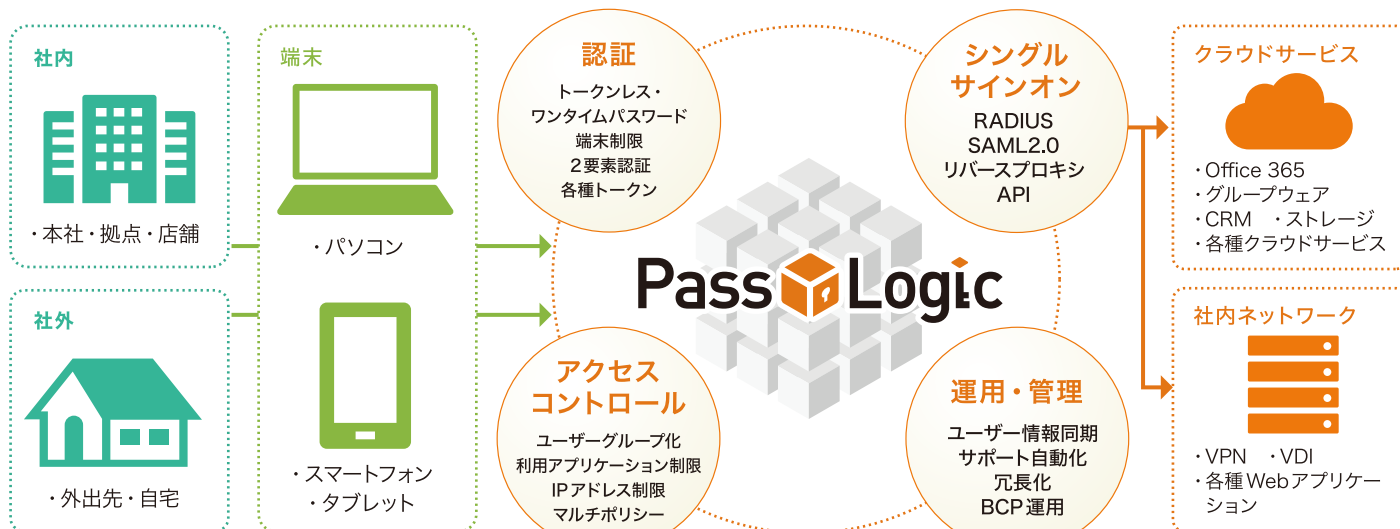
「認証」とは、システムやサービスにログインすること。

業務においてITの利用が当たり前となった今、「認証」は企業・団体の情報を守る不可欠な技術です。

PassLogicは、企業や団体における認証の課題を解決する「認証プラットフォーム」。

認証の面からセキュリティの確保と業務効率の向上を支援します。

PassLogic 利用イメージ



パッケージ版とクラウド版

PassLogicには、自社で用意したサーバーにソフトウェアをインストールして利用する「パッケージ版」と、パスロジ社が運用するクラウドサーバー上のサービスに登録して利用する「クラウド版」がございます。（いずれも年間ライセンスの購入が必要）
パッケージ版は、下記のクラウドプラットフォーム環境にて動作確認済みです。

■PassLogic 動作確認済みクラウドプラットフォーム

AWS (Amazon Web Services) GCP (Google Cloud Platform)
Microsoft Azure FUJITSU Cloud Service for OSS

パッケージ版



クラウド版



ご利用中のお客様の声

操作がシンプルで、一度理解すると、カンタンに使える。

パスワード忘れの対応件数が減った。

トークン管理の手間がなくなった。

外出時にモバイル端末で業務をすることが多くなった。

ブラウザの設定が不要で、メンテナンスと運用がラク。

他の多数のシステムと連携して、シングルサインオンが実現した。

PassLogic 関連特許

「乱数表から文字を抜き出して、パスワードを生成する認証方法」を世界で最初に考案し、2000年に米国で特許を取得しました。（U.S.PAT.6141751）その後、パスロジ社は日本を含む世界29ヶ国・94件の関連特許を取得しています。（2020年2月時点）

本製品に使用している米国および日本の主要な特許は下記のとおりです。

U.S.PAT.8140854 JP.PAT.5276658 JP.PAT.3809441

※特許発明に係るサービス・製品を正当な権限なく実施すること（第三者から購入してエンドユーザーとして利用する場合や、自社開発により実施する場合も含む）は、特許権侵害となります。

※2020年2月現在、パスロジ社は他社認証製品に対し特許ライセンスを実施しておりません（クラウド等のサービスを除く）。

※2015年1～2月に実施したアンケートより

専用デバイスやスマートフォンを使わないワンタイムパスワード

「トークンレス・ワンタイムパスワード」の仕組み

トークンレス・ワンタイムパスワードは、ブラウザ上に表示される乱数表から、数字を抜き出して入力する認証方式です。固定パスワード*の代わりに、乱数表のマス目の位置と順番、つまり「パターン」を覚える「知識認証」に分類されます。

*固定パスワード…通常のパスワードのことです。毎回入力する内容が変わるワンタイムパスワードに対して、毎回入力する内容が固定なので、当パンフレットでは区別するために「固定パスワード」と呼びます。

個人を認証する要素について

個人を認証する際に使われる要素は、以下の3種類に分けられます。

- 自分だけが知っていることで認証する「知識認証」
- 自分だけが持っているモノで認証する「所有物認証」
- 自分だけの身体的特徴で認証する「生体認証」

これらを「認証の三要素」と呼びます。

■ ユーザーが独自の「パターン」を設定

まず、ユーザー自身で「どのマス目から」「どの順番で」数字を抜き出すのかを設定します。この「マス目の位置と順番」を「パターン」と呼びます。

Secured by PassLogic.

Password ログイン

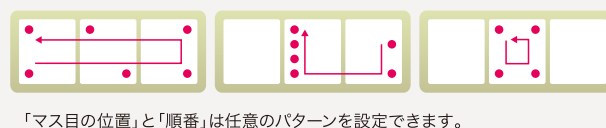
Password 07868619

■ パターン設定のルール

パターンに設定するマス目は、タテ・ヨコ・ナナメのどの方向でも、離れていてもかまいません。順番も自由に設定可能です。



▶ パターンの例



■ ログイン手順

① ブラウザで、ログイン画面を開き、ユーザー IDを入力



② 乱数表が表示されるので、パターンに沿って数字を抜き出して入力



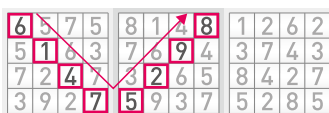
③ ログイン成功・失敗を判定

ログイン
OK / NG

■ 乱数表が変わるので、入力する数字も変わる

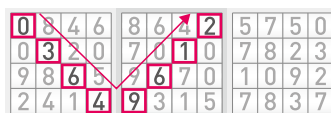
表示される乱数表の中の数字は、ログインしようとするたびに毎回入れ替わります。

ですので、同じパターンに沿って数字を抜き出しても、毎回抜き出す数字は変わります。その結果、ワンタイムパスワードとして成立します。



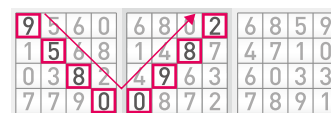
1回目

Password
61475298



2回目

Password
03649612



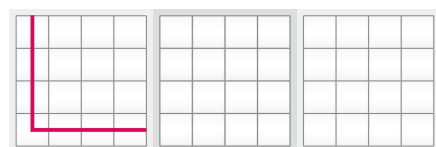
3回目

Password
95800982

■ 追加フレーズ(固定パスワード)との組み合わせ

パターンに沿って抜き出した数字の前後に、ユーザー自身が設定した固定の文字列「追加フレーズ」を追加することが可能です。

▶ 例: パターンが下図で、追加フレーズ「PassLogic」を後ろに追加した場合



・乱数表から抜き出した数字



・追加フレーズ

PassLogic

Password 2639247PassLogic

認証機能

トークンレス・ワンタイムパスワード

前ページで紹介した認証方式「トークンレス・ワンタイムパスワード」による認証機能です。専用のデバイスやスマートフォン、読み取り用機器などのハードウェアが不要なため、ハードウェアの調達コストや、初期登録や配布、紛失・故障対応といった運用コストが削減されます。ブラウザだけで利用可能なため、PC・スマートフォン・タブレットなど利用端末も選ばず、マルチデバイスにも対応。

PCブラウザ



スマートフォン



■対応ブラウザ

- Internet Explorer 11 ● Edge ● Google Chrome ● Mozilla Firefox
- Safari ● Android 標準ブラウザ

ソフトウェアトークン

パスロジが無償提供するスマートフォン用アプリ「PassClip L」を使用した時間同期型ワンタイムパスワード (TOTP) による認証が利用可能です。

アプリ上のワンタイムパスワード表示形式は、パスワードをそのまま表示する「ベーシック表示」と、5x5のマスキングに隠して表示する「ビンゴ型表示」の2種類から選択できます。

PINコード (固定パスワード) と組み合わせた2要素認証も実現します。



ベーシック表示



ビンゴ型表示



文字を抜き出すマスと順番 (パターン) を知らないとパスワードが分からない

他人に画面を見られても、パスワードを知られない

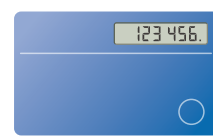
ハードウェアトークン

OATH 規格のハードウェアトークンを使用した時間同期型ワンタイムパスワード (TOTP) による認証が利用可能です。

PINコード (固定パスワード) との併用も可能で、2要素認証を実現します。



キーホルダータイプ



カードタイプ

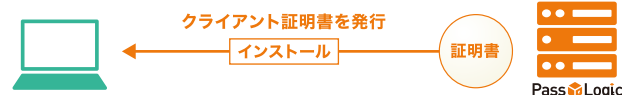
端末認証機能

事前登録を行った端末だけを認証する機能です。PassLogicが発行したクライアント証明書を、あらかじめインストールした端末だけがログイン可能となります。トークンレス・ワンタイムパスワードと組み合わせて、認証用ハードウェアなしで、2要素認証を実現します。

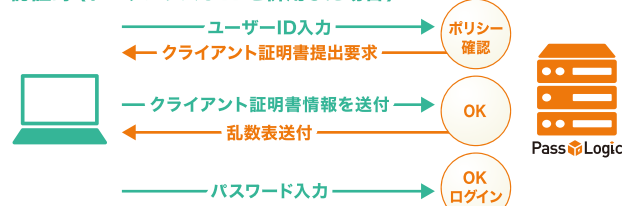
クライアント証明書による端末制限

PassLogicが発行したクライアント証明書を、あらかじめインストールした端末だけがログイン可能となります。

端末にクライアント証明書を登録



認証時 (トークンレスOTPと併用した場合)



PassLogicで実現可能な2要素認証

PassLogicでは、用途やポリシーに応じて、以下のような組み合わせで2要素認証を実現します。

トークンレス・
ワンタイムパスワード



クライアント証明書



パターンの記憶と、証明書の所有による2要素認証。専用デバイスや固定パスワードを使わずに、強固な2要素認証を実現！

オススメ!

PassClip L
スマートフォン所有



PassClip L
ビンゴ型表示



事前登録した PassClip L インストール済スマートフォンの所有と、パターンの記憶による2要素認証

PassClip L
スマートフォン所有



PINコード (固定パスワード)



事前登録した PassClip L インストール済スマートフォンの所有と、PINコードの記憶による2要素認証

ハードウェアトークン



PIN (固定パスワード)



ハードウェアトークンの所有と、PINコードの記憶による2要素認証

Windows OS への認証に適用「PassLogic for Windows Desktop」

Windows 端末を起動し、Windows OS にサインインする際に行う認証を、トークンレス・ワンタイムパスワードやソフトウェアトークン、ハードウェアトークンに置き換えることができます。あらかじめ専用のアプリケーション「PassLogic for Windows Desktop」をインストールし、設定しておくことで、次回以降の起動時に自動的にアプリケーションが起動します。

- 端末がオフラインでも利用可能
- Active Directory の固定パスワードも併用した 2 段階認証も設定可能

■ 対応 Windows OS

- Windows 8.1 32bit/64bit
- Windows 10 32bit/64bit
- Windows Server 2016

Windows 8.1



Windows 10

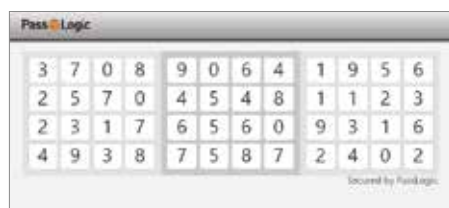


クライアントソフト連携

VPN や VDI などのクライアントソフトを起動して表示された認証画面で、別画面のブラウザで表示した PassLogic の乱数表から抜き出したワンタイムパスワードを入力する方法が適用可能です。また、PassLogic が提供する API で連携すれば、クライアントソフトの認証画面に乱数表を直接表示することも可能です。

■ 「クライアントソフトの認証画面+ブラウザ上の乱数表」の場合の例

① ブラウザで PassLogic の乱数表を表示し、パターンからワンタイムパスワードを抜き出す



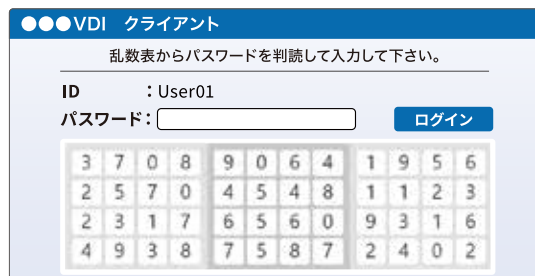
② クライアントソフトの認証画面にて、抜き出したワンタイムパスワードを入力し、ログイン



主な対応済専用クライアントソフト

- Windows 標準クライアントソフト
- VMware Horizon View Client
- Cisco ASA AnyConnect
- SonicWall NetExtender
- FortiClient
- PaloAlto など

■ PassLogic API を利用し、クライアントソフトの認証画面に乱数表を表示する例



■ PassLogic API 仕様概要

API 形式	REST
データフォーマット	XML、JSON
認証 API	トークンレス・ワンタイムパスワード ソフトウェアトークン (PassClip L) ハードウェアトークン
管理 API	※クライアント証明書認証は利用不可 ユーザー管理 (ユーザー作成、編集、削除、検索、ユーザー情報取得) トークン管理 (トークン追加、削除、検索)

グループ分けとマルチポリシー

部署や役職によって従業員をグループ分けし、グループによって使用する認証方式や、ログイン可能時間帯などの認証ポリシーを変えて運用することが可能です。

グループA 社内勤務者



認証方式: トークンレス OTP
クライアント証明書: なし
ログイン可能時間: 常時許可
最も一般的な従業員には、手間のかからないトークンレス・ワンタイムパスワードを採用

グループB 社外勤務者



認証方式: トークンレス OTP
クライアント証明書: 必須
ログイン可能時間: 常時許可
外回り営業や出向など、社外勤務者には、持ち出しを許可した端末を配布し、その端末の識別にクライアント証明書を採用

グループC システム管理者



認証方式: ハードウェアトークン
or ソフトウェアトークン
クライアント証明書: なし
ログイン可能時間: 常時許可
システム管理者には、認証用デバイスの利用を必須とする社内ポリシーに合わせて、トークン型のワンタイムパスワードを採用

グループD アルバイト



認証方式: トークンレス OTP
クライアント証明書: なし
ログイン可能時間: 8:50-18:10
アルバイトの時間外労働は許可しないという労務規程にのっとり、時間外のログインを不可に

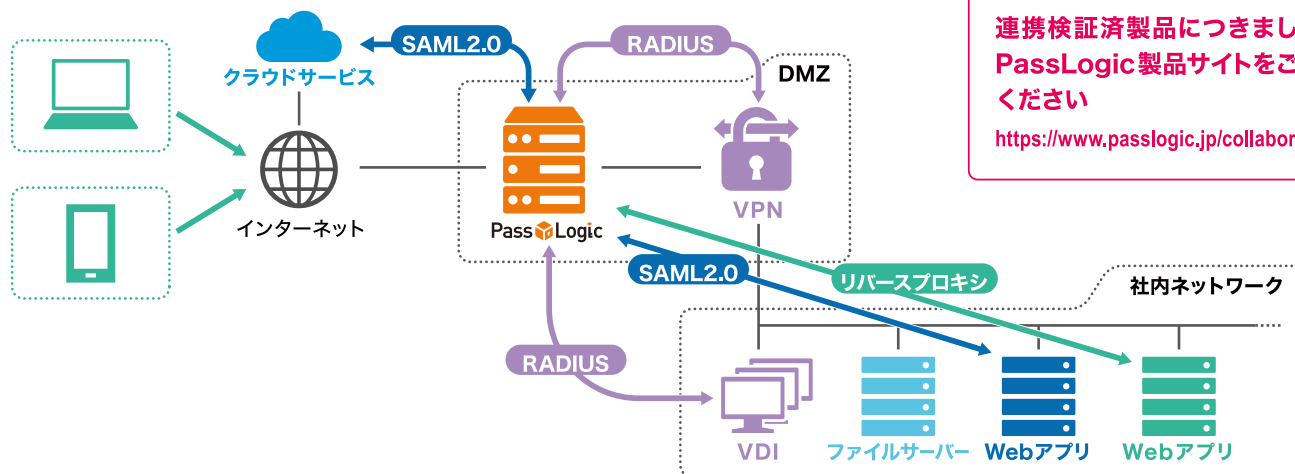
■ 変更可能な内容

認証方式 / 端末認証の利用有無 / ログイン可能時間帯 / 定期的なパターン変更の有無 / パスワード桁数 / 乱数表のサイズ / 追加フレーズの有無 / パターンの制約 / ロックアウトまでの認証失敗回数 など

業務システムとの連携とシングルサインオン

豊富な連携方式に対応

VPNやVDI、社内Webアプリケーション、クラウドアプリケーションといった、様々な業務システムと連携するために、PassLogicは複数の連携方式(プロトコル)に対応しています。また、一部の製品との連携用に、専用のモジュールを用意しています。



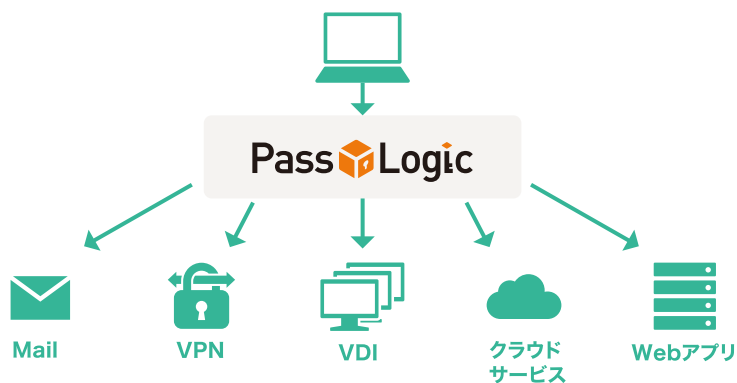
対応プロトコル ●RADIUS ●SAML2.0 ●リバースプロキシ*1
●REST API*2 ●専用の連携モジュール

*1: PassLogicクラウド版は、リバースプロキシ連携は非対応です。

*2: APIの提供は基本的に有償オプションサービスです。API連携を希望されるソフトウェアメーカーの方は、まずはお問合せください。

シングルサインオン環境の構築

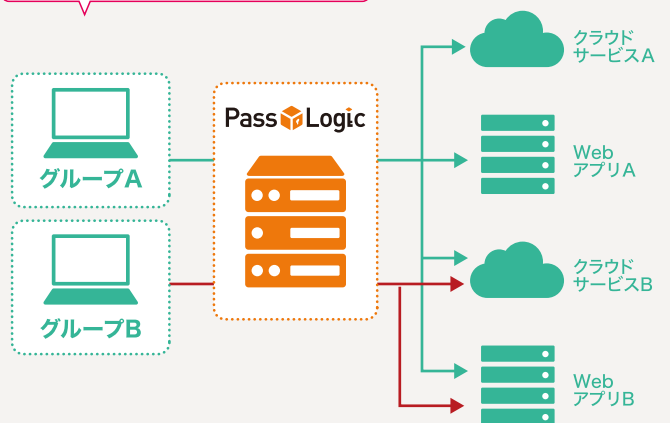
PassLogicに連携した複数の業務システムに、1回の認証だけで同時にログインする「シングルサインオン」の環境を構築することが可能です。複数の固定パスワードを覚えたり、複数の認証用ハードウェアを持ち歩く必要がなくなり、ユーザーの負担も削減されます。



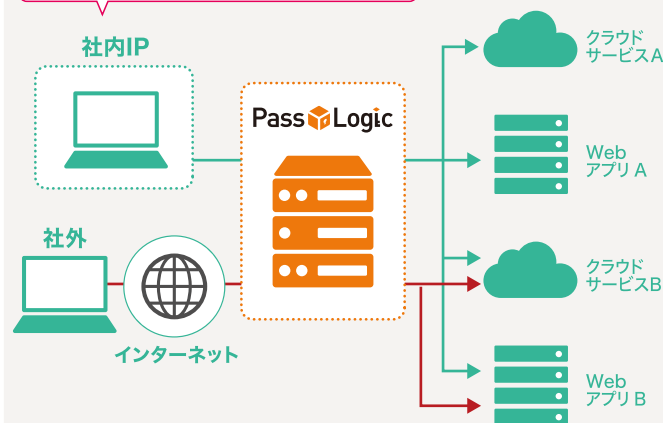
アクセスコントロール機能

所属グループや接続元のIPアドレスによって、利用できる業務システムを制限することができます。

グループによるアクセスコントロール



IPアドレスによるアクセスコントロール

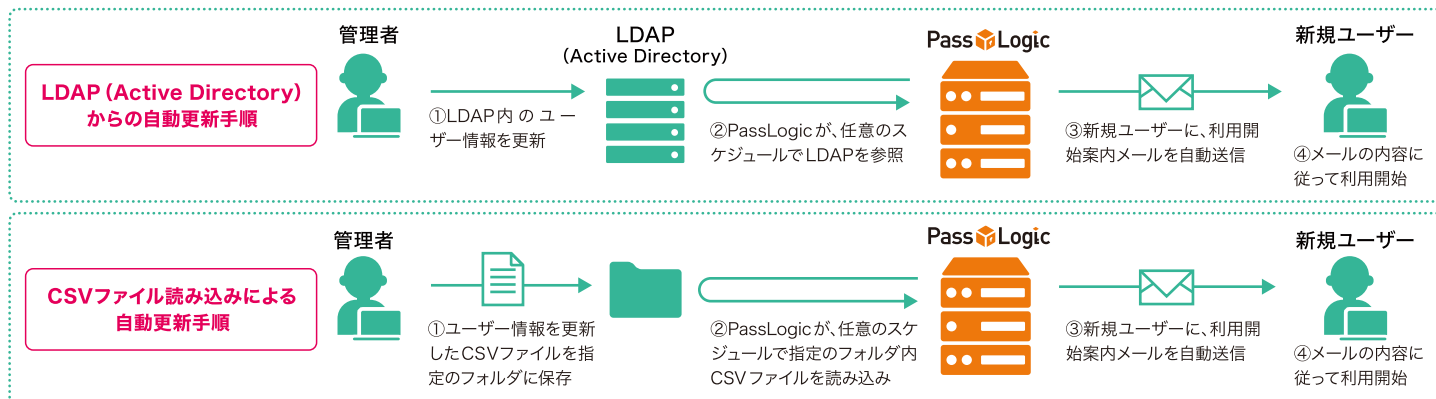


運用・管理機能

ユーザー情報更新機能

運用する環境やポリシーに合わせて、自動もしくは手動でのユーザー情報の更新が可能です。

ユーザー情報の更新方法



- ▶ LDAP (Active Directory) からの自動更新*
- ▶ CSVファイルの読み込みによる自動更新*
- ▶ 管理画面から手動更新
- ▶ 管理画面からCSVファイル読み込みによる一括更新

* PassLogicクラウド版は、ユーザー情報自動更新機能は非対応です。

ユーザサポートの自動化

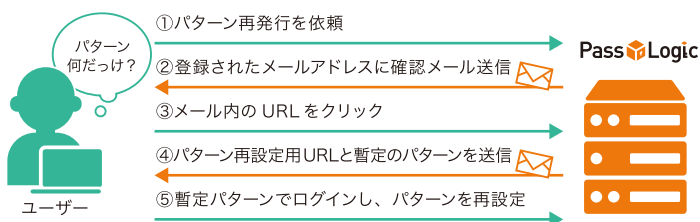
パターンの再設定とロックアウト解除の自動対応機能を搭載。管理者の負担を軽減します。

管理者による手動対応も可能なので、運用に合わせて選択してください。



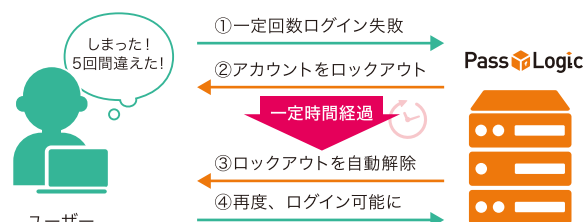
パターンの自動再設定

パターンを忘れたユーザーが、自分自身でパターンを再設定することができます。(セルフリマインダー機能) 管理者の手動による再設定も可能です。



ロックアウトの自動解除

規定回数のログイン失敗によりアカウントがロックされた場合、一定時間経過後に自動解除する機能です。管理者の手動により解除する運用も可能です。

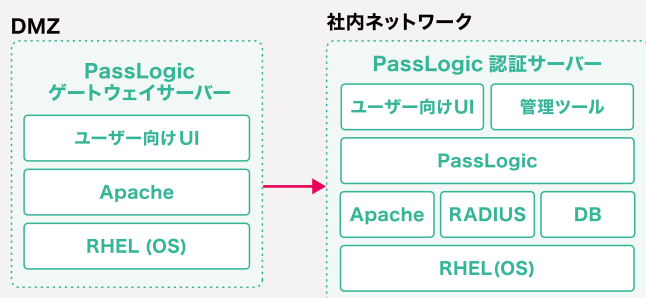


サーバーの分離構成と冗長化構成

サーバーを分離して、インターネット公開部分をDMZに設置し、認証機能や管理ツール、データベースを社内ネットワーク内に設置することが可能です。また、負荷分散や障害・災害対策のため、冗長化構成も可能です。

サーバー分離構成

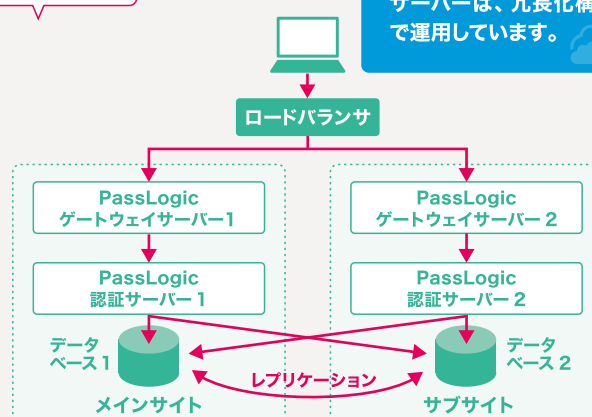
データベースをDMZに設置することなく、LDAP通信も社内ネットワーク内で完結できる構成です。



*DMZ内または社内ネットワーク内に1台のサーバーで構成することも可能です。

冗長化構成

PassLogicクラウド版のサーバーは、冗長化構成で運用しています。



PassLogic パッケージ版

システム要件

サーバ OS	Red Hat Enterprise Linux7.1 以降 x86_64*2 CentOS 7.1 以降 x86_64*2 ※Red Hat Enterprise Linux8.x は未対応
httpd *1	Apache HTTP Server Version : 2.4.6 Release : 31.EL7 以降
php *1	Version : 5.4.16 Release : 36.EL7_1 以降

*1 各モジュールは、OS ベンダ提供パッケージのみサポートされます。 独自コンパイルしたものはサポート対象外です。

*2 NSA Security-Enhanced Linux (SELinux) を有効にした環境での動作はサポートしていません。

※仮想サーバーでの動作もサポート対象です。(ゲスト OS が動作環境を満たしている必要があります)

※CentOS は OS のサポートが無く脆弱性などのパッチ提供も遅延する場合があるため、本番利用時には Red Hat Enterprise Linux のご利用をお勧めいたします。

※IPv6 を無効にした環境での動作は保証されませんので、OS インストール時に「有効」に設定してください。

動作確認済み クラウドプラットフォーム

AWS (Amazon Web Services)*
FUJITSU Cloud Service for OSS
GCP (Google Cloud Platform)
Microsoft Azure*

*AWS および Azure のマーケットプレイスにて、構築済みのソフトウェアを提供中です。

※ご利用の際には、ライセンスの購入が別途必要です。
(1ID のみでの試用は可能です)

ソフトウェア&サポート購入型 価格リスト (抜粋)

初年度は、ソフトウェアと年間保守サポートのご購入が必要で、次年度以降の継続利用には、年間保守サポートのご購入 (更新) が必要なプランです。
20IDからご購入いただけます。当リストにないID数の価格については、お問合せください。

	20 ID	100 ID	500 ID
ソフトウェア (初年度のみ)	177,600 円	720,000 円	2,760,000 円
年間保守サポート	35,520 円	144,000 円	552,000 円
4 年間利用した場合の 1ID あたり月額換算の目安	333 円	270 円	207 円

サブスクリプションライセンス、標準サポート一体型 価格リスト (抜粋)

サポート一体型のサブスクリプションライセンスです。次年度以降の継続利用には、年間ライセンスのご購入 (更新) が必要です。
20IDからご購入いただけます。当リストにないID数の価格については、お問合せください。

	20 ID	100 ID	500 ID
年間ライセンス	91,000 円	368,000 円	1,411,000 円
1ID あたり月額換算の目安	379 円	307 円	235 円

PassLogic クラウド版

価格リスト

	価格	備考
1 ユーザーあたりの月額	480 円	・新規 / 追加ユーザーのお申し込みは、10 ユーザー単位となります。 ・アカウント開通日の翌月 1 日を起算日とした年間契約になります。 ・サーバーの利用料も含まれます。またインストールや構築作業は不要です。
アカウント開通 事務手数料	10,000 円	・PassLogicクラウド版の利用開始時 (アカウント開通時) にお支払いいただく事務手数料です。

※価格は予告なく変更される場合がございますので、あらかじめご了承ください。

※価格はすべて税別表記です。

— 無償のお試し利用について —

30日間、すべての機能がご利用いただける試用ライセンスを発行いたします。まずは、パスロジまでご連絡ください。

※パッケージ版とクラウド版は、ご利用いただける機能が一部異なります。
まずは、ご試用いただくことをお勧めいたします。

パッケージ版

お申し込み後、ソフトウェアパッケージとライセンスファイルをお送りします。

クラウド版

お申し込み後、管理者アカウントを作成し、ご利用方法をお知らせします。

■ PassLogic に関するお問合せ窓口

お問合せフォーム: <https://passlogic.jp/inquiry/>
メール: sales@passlogy.com
電話: 03-5283-2263 [受付時間] 10:00 ~ 17:00 (土日祝休)



パスロジ株式会社
www.passlogy.com

〒101-0052 東京都千代田区神田小川町 3-26-8

認証セキュリティ情報サイト

せぐなべ

検索

www.segunabe.com

- パスロジ社の正規ライセンスを受けたサービス・製品にはパンフレット等にパスロジ社のライセンス表示が付されています。
- このカタログ掲載の写真、記事等の無断複写・複製・転載を禁じます。
- 本文中の社名・製品名は各社の商標または登録商標です。
- 仕様・機能等は改良のため予告なしに変更される場合があります。



IS 697637 / ISO 27001

