

OpenAM



学認連携を多要素認証で強化

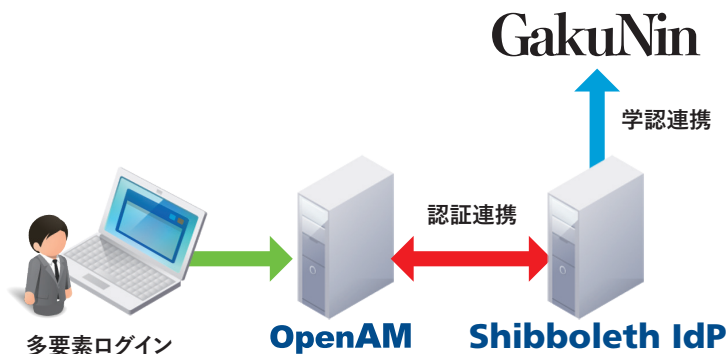
標準搭載フェデレーションプロトコル数**最多**
多様な認証モジュールを標準搭載
長年の実績と信頼

最強のシングルサインオンソフトウェア

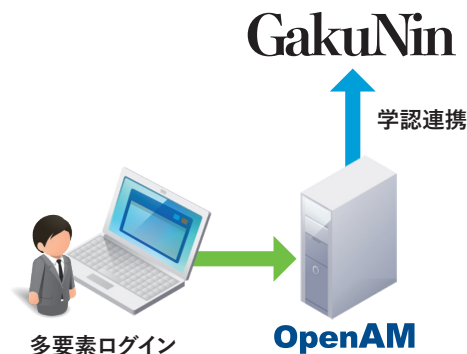
学認と直接接続し多要素認証を実現

学認との連携で求められるShibboleth IdP互換の機能を強化し、OpenAM単体で多要素認証が可能かつ、GUIによる運用ができる学認接続IdPを実現できます。

OpenAM14まで



OpenAM14.5以降



パスキー対応 WebAuthn認証を標準搭載

WebAuthn 認証にパスキーをはじめ、FIDO2対応認証デバイス、又はPC標準搭載の生体認証デバイスを利用するWindows Hello、Apple製品搭載のTouch ID /Face IDなどが利用できます。生体認証のテクノロジーをOpenAMを入り口としたサービスのログインに利用できます。



サービス認可機能

ユーザー属性に応じて、許可されたサービスのみ利用できる構成 SAML SP、OpenID Connect/OAuth2.0 RPごとに利用できるユーザーをポリシーにて制御可能としました。



フェデレーションプロトコルによるSSO連携先サービスを利用認可可能です。

図の例はセールス部門ユーザーは全社サービス「Microsoft 365、Google Workspace、Slack」の他に「Salesforce」が利用できます。デザイン部門のユーザーは全社サービスの他に「Adobe Creative Cloud」サービスが利用できます。

構成例
1

学認IdPとして多要素認証を利用できます

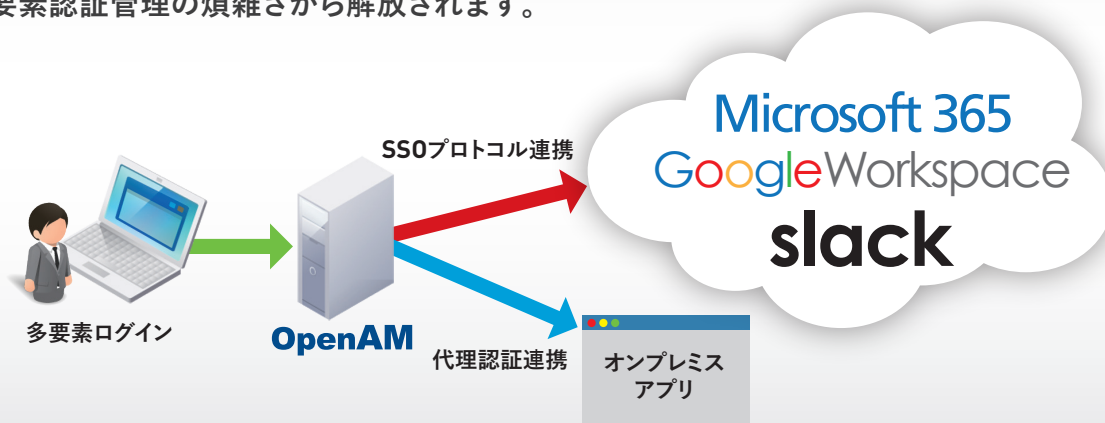
多要素認証に対応したOpenAMを学認と直接連携できます。加えて学認以外のSaaSや、オンプレミスのWebアプリケーションを一括で認証連携可能です。



構成例
2

SaaSとオンプレミスのアプリケーションを多要素認証で強化

多要素認証で強化されたOpenAMをシングルサインオンの入り口とし、SaaSとオンプレミスのWebアプリケーションをSSO化。認証の強化はOpenAM一箇所で済み、アプリケーション毎の多要素認証管理の煩雑さから解放されます。



OSSTech 製の OpenAM の特長

学認連携機能	Shibboleth IdP代替機能を強化
柔軟な SAML設定	SP毎の NameIDマップ設定、IdP/SP毎の署名アルゴリズム設定
動的認証連鎖	ユーザーやログインする環境に応じて要求する認証方法を動的に変更可能
reCAPCHA v3モジュール	reCAPCHA v3の機能を利用しロボット等の攻撃を排除可能
LINE OTP	ワンタイムパスワードの送信経路にメールや SMSではなく LINEを利用可能
代理認証	フェデレーションプロトコルに対応しない、Form認証、Basic認証のレガシーアプリケーションを SSO対応できるモジュールを用意
OpenLDAP の親和性向上	パスワード有効期限、パスワード失敗回数によるロックなどのパスワードポリシー対応
RPM パッケージ	rpmコマンドによるインストール、アップデートが可能なパッケージ構成を採用
バグ修正	セキュリティ・運用に関わる問題を優先的に修正
サポート	長年のオープンソース・ソフトウェアサポートの経験と実績から、質の高いサポートを提供
低コスト	ユーザー数に依存しない価格体系のため、大規模システムにおける大幅なコスト削減が可能

SSO対応サービス、アプリケーション例

Microsoft 365、Google Workspace、Salesforce、Zendesk、SAP、Cybozu、Box、Dropbox、Adobe Creative Cloud、GitHub、AWS、Slack、Chatwork、Sales Force Assistant、Active!mail、Create!Webフロー、desknet's、Insuite、manaba、SharePoint、UNIPROVE/AS、WebClass(代理認証)、Xyθος

※上記リストは一例です。SAML/OpenID Connect/OAuth2.0/Form認証/Basic認証/Header/Cookie対応のアプリケーションはSSO可能です。

SSO対応方式

フェデレーション(SSO)プロトコル	SAML OpenID Connect OAuth WS-Federation
ポリシーエージェント	リクエストヘッダー、Cookieによる連携
代理認証	Form認証、Basic認証(パスワード暗号化および復号化機能含む)

認証モジュール

パスワードレス	FIDO2(WebAuthn)
ソーシャルログイン	Google Workspace、Microsoft 365、Oktaなど SAML、OpenID Connect、の IdP に対応
ID + パスワード	OpenLDAP、汎用 LDAP、Active Directory、RDBMS、RADIUS
ワンタイムパスワード	HOTP、TOTP、OATH、email、SMS、LINE、スマホアプリ
リスクベース	アダプティブリスク
デバイス	デバイス ID
統合 Windows 認証	デスクトップ SSO
その他	証明書、クライアントサイドスクリプト、サーバーサイドスクリプトなど

OSSTech版 OpenAM機能

言語	日本語、英語、フランス語、ドイツ語、スペイン語、中国語、韓国語
サポート	アップデートパッケージ提供、運用に関する技術 QA、障害調査
ライセンス	サーバー台数(実サーバーおよび仮想マシン)で起動するインスタンス数につき1ライセンス

OpenAM動作環境

OS	JDK	J2EE
Red Hat Enterprise Linux 7(CentOS 7) Red Hat Enterprise Linux 8(AlmaLinux/Rocky Linux 8) Amazon Linux 2 Docker	OpenJDK 8 OpenJDK 11	Apache Tomcat 7 以降

ポリシーエージェント動作環境

OS	Web サーバー
Red Hat Enterprise Linux 7(CentOS 7) Red Hat Enterprise Linux 8(AlmaLinux/Rocky Linux 8) Amazon Linux 2	Apache HTTP Server 2.4 (OS標準)

動作確認済みブラウザ

OS	Web ブラウザ
Windows	Microsoft Edge、Google Chrome、Firefox
macOS	Safari、Google Chrome、Firefox
Linux	Google Chrome、Firefox
iOS	Safari
Android	Google Chrome

※ベンダーのサポートが継続しているバージョンに限ります。

OpenAM、OpenDJはOSSTech株式会社の日本での登録商標です。(登録 第 5398965 号)