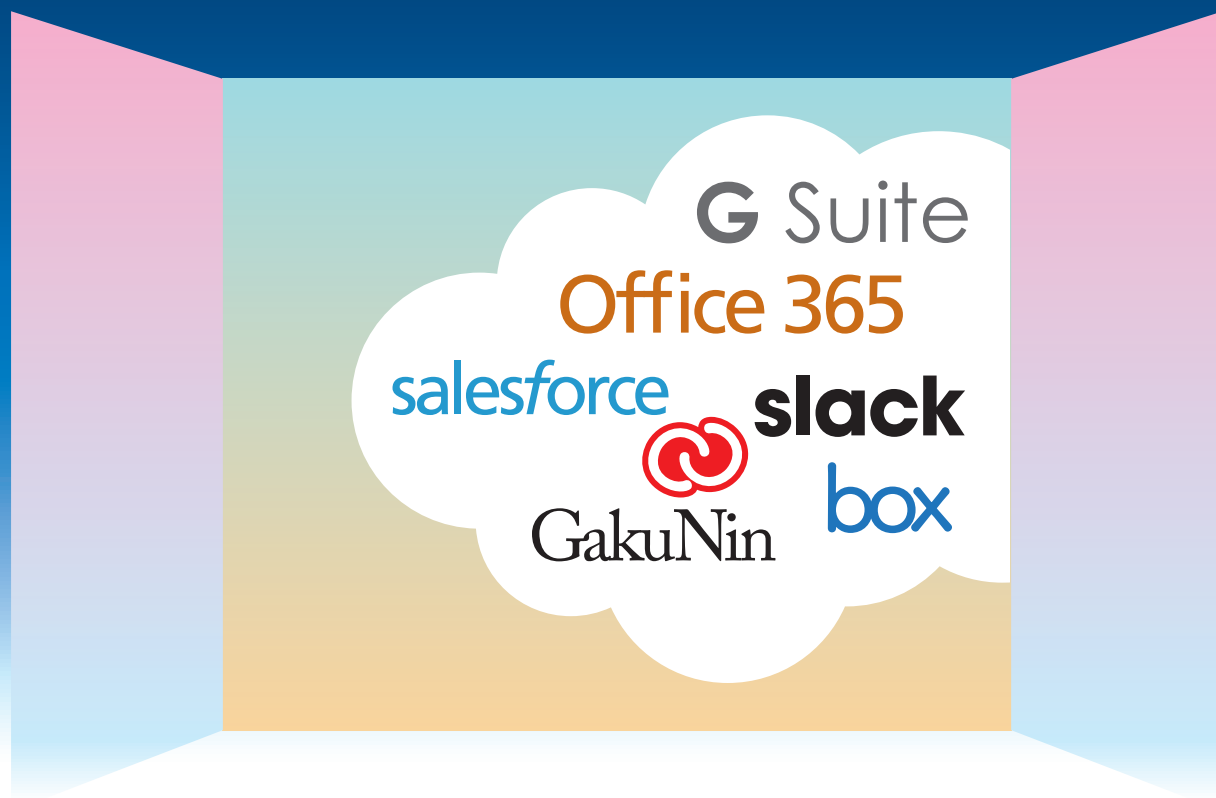


OpenAM



パスワードレス認証を搭載した 新世代シングルサインオン環境

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

令和/2020年代に導入すべき**最強**のシングルサインオン環境

パスワードレス認証を標準搭載

「ひらけごま」の時代からパスワード漏洩は最大のリスク!

認証デバイスは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TouchIDなどが利用できます。



PCブラウザ



スマートフォンブラウザ

生体認証のテクノロジーをOpenAMを入口としたサービスのログインに利用できます。パスワード管理のリスク、コストを削減しユーザーの利便性を格段に向上させます。



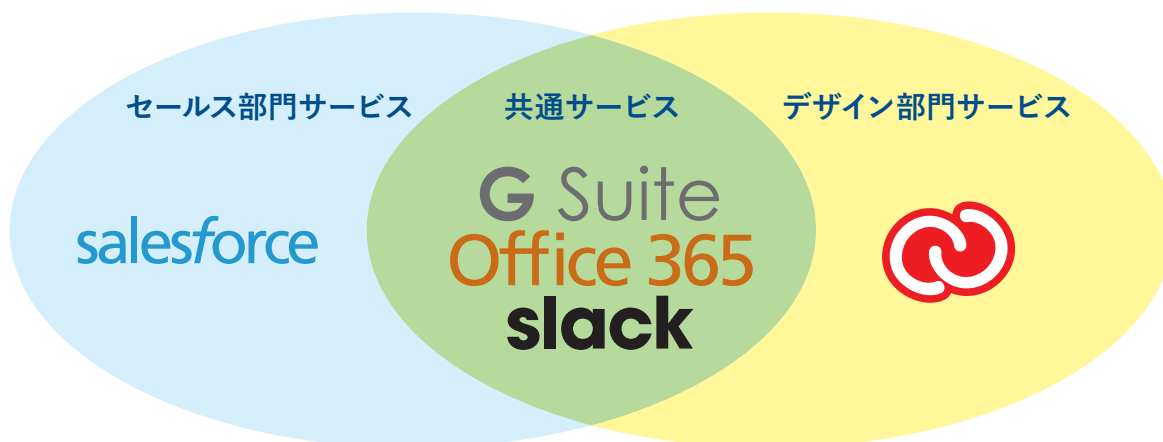
ログイン



OpenAM

サービス認可機能

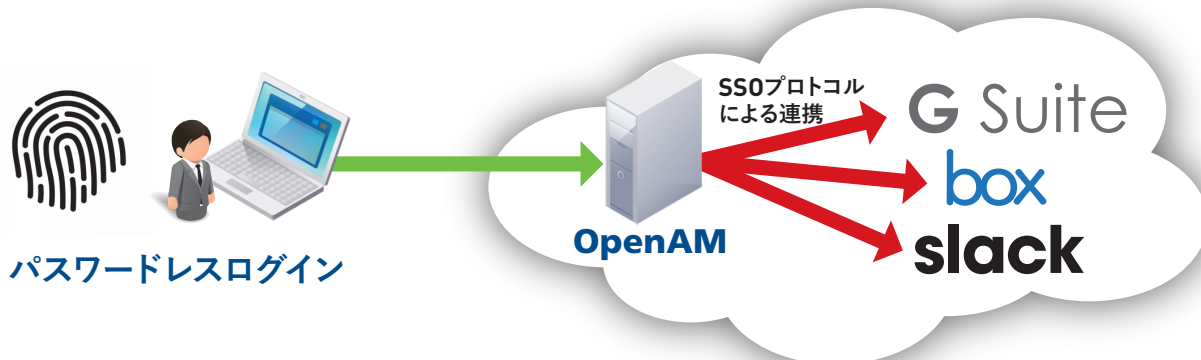
ユーザー属性に応じて、許可されたサービスのみ利用できる構成 SAML SP、OpenID Connect/OAuth2.0 RPごとに利用できるユーザーをポリシーにて制御可能としました。



フェデレーションプロトコルによるSSO連携先サービスをグループ等によりアクセス制限可能です。図の例はセールス部門ユーザーは共通サービス「G-Suite/Office365/slack」の他に「Salesforce」が利用できます。デザイン部門のユーザーは共通サービス「G-Suite/Office365/slack」の他に「Adobe Creative Cloud」サービスが利用できます。

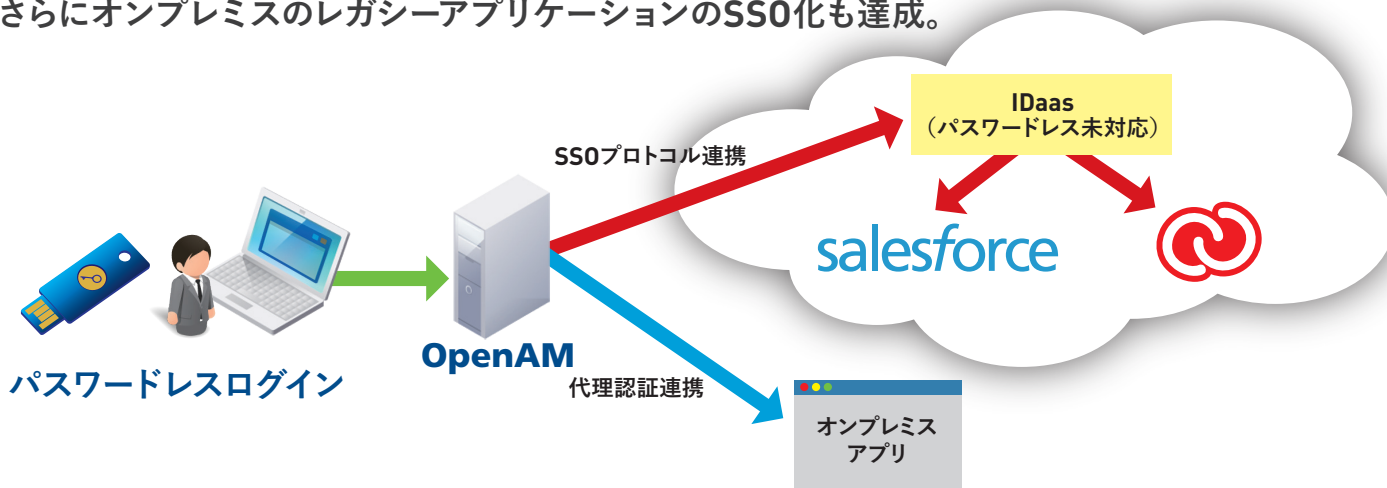
構成例1 SaaSアプリケーションを全てパスワードレスログイン

パスワードレス認証に対応したOpenAMをAWS上へ構築し、他のサービスやアプリケーションは全てSSO連携でパスワードレス認証にします。また、サービス認可機能が活用できます。



構成例2 IDaaSと協調しオンプレミスのレガシーアプリケーションをSSO化

既に導入済みのIDaaSをOpenAMをシングルサインオンの入口としパスワードレス認証に対応、さらにオンプレミスのレガシーアプリケーションのSSO化も達成。



OSSTech 製の OpenAM の特長

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
reCAPTCHA v3モジュール	reCAPTCHA 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
マイナンバーカードによる認証	クライアント証明書認証機能を利用
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、FIDO2対応スキーマ
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
カスタマイズ後のサポート	カスタマイズしたモジュールを提供した場合でも、開発元ならではの確実なサポートを提供可能
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
長期サポート	製品サポート期間は、ご要望のサポート契約期間に対応して延長可能
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

Office 365、G-Suite、SalesForce、Zendesk、SAP、Cybozu、box、Dropbox、Adobe Creative Cloud、Github、AWS、slack、chat-work、Sales Force Assistant、Active!mail、Create!Webフロー、desknet's、Insuite、manaba、SharePoint、UNIPROVE/AS、WebClass(代理認証)、xythos

※上記リストは一例です。SAML/OpenIDConnect/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	G-Suite、Office365、oktaなど SAML、OpenID Connect、OAuth2に対応した認証プロバイダー対応
ID + パスワード	OpenLDAP、汎用 LDAP、ActiveDirectory、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(CentOS 8) Amazon Linux 2 docker	OpenJDK 8 OpenJDK 11	Apache-Tomcat7 以降

ポリシーエージェント動作環境

OS	Web サーバー	SAML連携用コネクタ
Red Hat Enterprise Linux 7(CentOS 7) Red Hat Enterprise Linux 8(CentOS 8) Amazon Linux2 docker	Apache HTTP Server 2.4 (0.5標準)	OSSTech製 mod_auth_mellon
		OpenID Connect連携用コネクタ
		OSSTech製 mod_auth_openidc

動作確認済みブラウザ

OS	ブラウザ
Windows	Microsoft Edge、Internet Explorer 11、Google Chrome、Firefox
macOS	Safari、Firefox、Google Chrome
Linux	Firefox、Google Chrome
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はオープンソース・ソリューション・テクノロジー株式会社の日本での登録商標です。(登録 第 5398965 号)