

株式会社サテライトオフィス

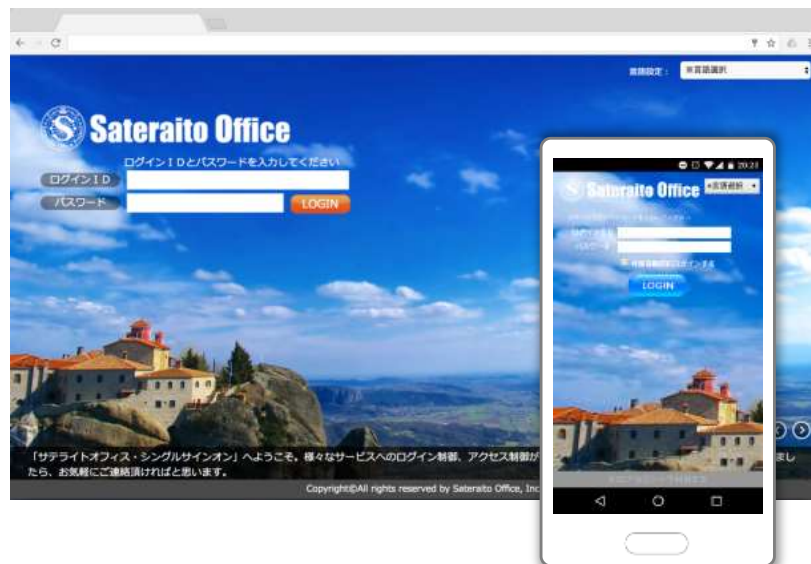
サテライトオフィス・シングルサインオン for Google Workspace



株式会社サテライトオフィス
2022年3月1日

サテライトオフィス・シングルサインオン

Google Workspace



シングルサインオン機能とは？

Google Workspaceのセキュリティーを強化(アクセス制御 & パスワード強化)を実現+組織管理する為のサービスです。シングルサインオン機能は、Google App Engine上で動く安定したサービスです!

ログイン制御機能&パスワード強化機能

グローバルIPアドレス別、ユーザー別、組織別、端末別に、ログイン制限を行う事が可能です。パスワードルールを強化、定期パスワード変更 ログインログ収集、MACアドレスでの制御

組織管理機能

多階層の組織管理を実現可能です。
ADや社内システム同期も可能です。

外部システムとのシングルサインオンを実施

他クラウドシステムとのシングルサインオン連携が可能です。

クライアント証明書認証

認証用のクライアント証明書発行から失効の管理まで可能です。

なぜ、シングルサインオン機能が必要なのか？

サテライトオフィス・シングルサインオンを利用することで、利用可能な場所（会社、工場、店舗など）を限定したり、端末（PC、スマートフォン、タブレット）を指定してGoogle Workspaceの利用を制限することが可能です。また、外部システムとのシングルサインオン連携（SAML、POST/GET、代行入力）で複数のサービスへのログイン管理も可能です。

アクセス制御

アクセス制御機能では、**パソコン / スマートフォン/タブレット** に対して

- ・ IPアドレスでの利用制限（社外からのログインを禁止） 複数指定可
- ・ 端末個体識別での利用制限（出張などの社外からのアクセスを許可）
- ・ 利用端末数での利用制限
- ・ ブラウザ種別、携帯キャリア単位でのログイン制御
- ・ MACアドレスでの制御
- ・ クライアント証明書での制御
- ・ セキュリティーブラウザでの制御
- ・ ログインログ収集



が可能です。また、アクセス制御ルールはプロファイルという再利用できる形式で管理され、

- ・ ドメイン全体 / 組織別 / メンバー別
- ・ ネットワーク別（社内ネットワーク、社外ネットワーク、スマートフォン等）

に設定する事が可能です。

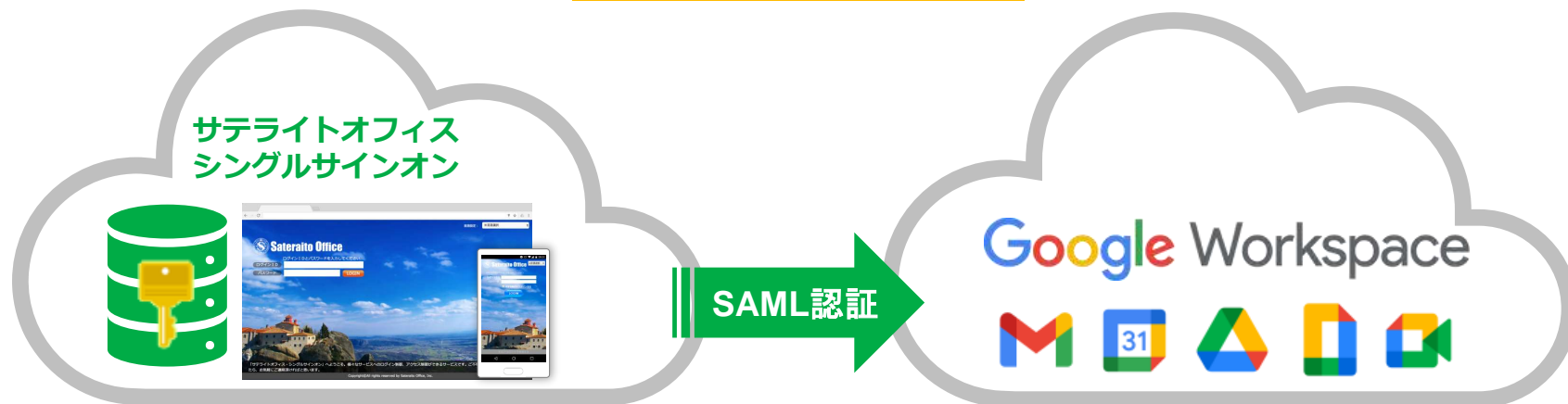
管理機能

シングルサインオンでは、Google Workspaceのデータを一括管理可能です。

- ・ ユーザー情報の同期（新規作成、編集、削除）
- ・ グループ（メーリングリスト）の同期（新規作成、メンバーの編集、削除、ビジネス向けGoogle Groupの権限設定）
- ・ 組織の同期（Google Workspace の組織（OU）を同期）

シングルサインオンを利用したログイン時の全体イメージ

インターネット環境



社内環境 (VPN)

社外環境

固定IP

固定IP以外

業務用PC

個人PC

業務用スマホ

個人スマホ



OK



NG



OK



NG



OK



NG

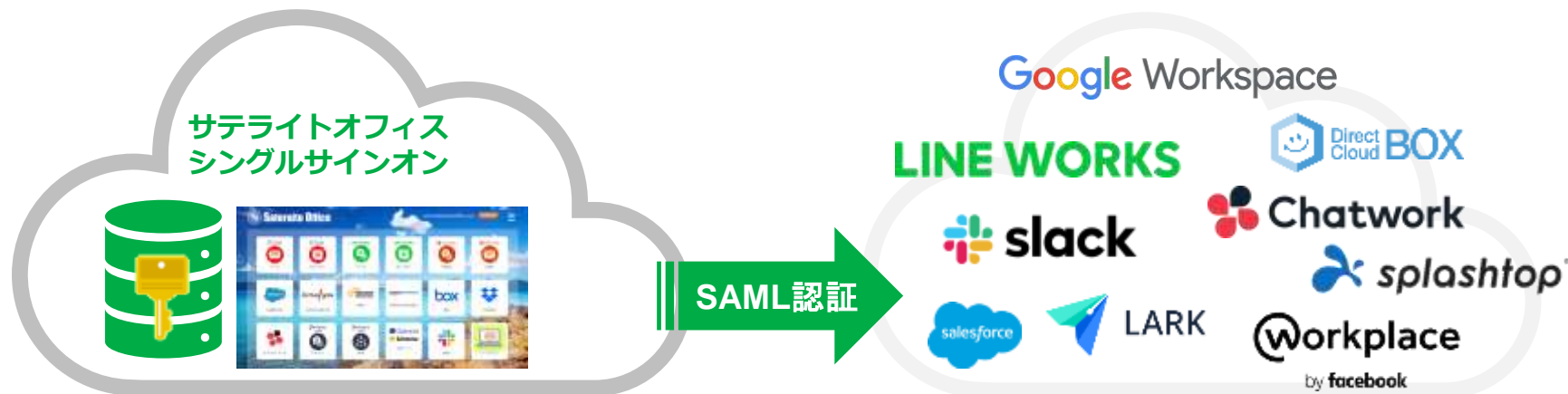
シングルサインオン・外部システム連携

Google Workspace以外のSaaSサービスや既存のグループウェア、基幹システムに対してもシングルサインオン認証が可能。既存のシステムの認証機能に合わせて柔軟にパラメータを設定し連携可能です。『マイページ』に連携済みサービスのアイコンを表示することも可能です。



外部システムへのログインイメージ

SAML認証による外部システム連携（SAML以外にもPOST/GET、代行入力で連携可能です）



社内環境 (VPN)

固定IP

固定IP以外



OK



NG



OK



NG

社外環境

業務用スマホ

個人スマホ



OK



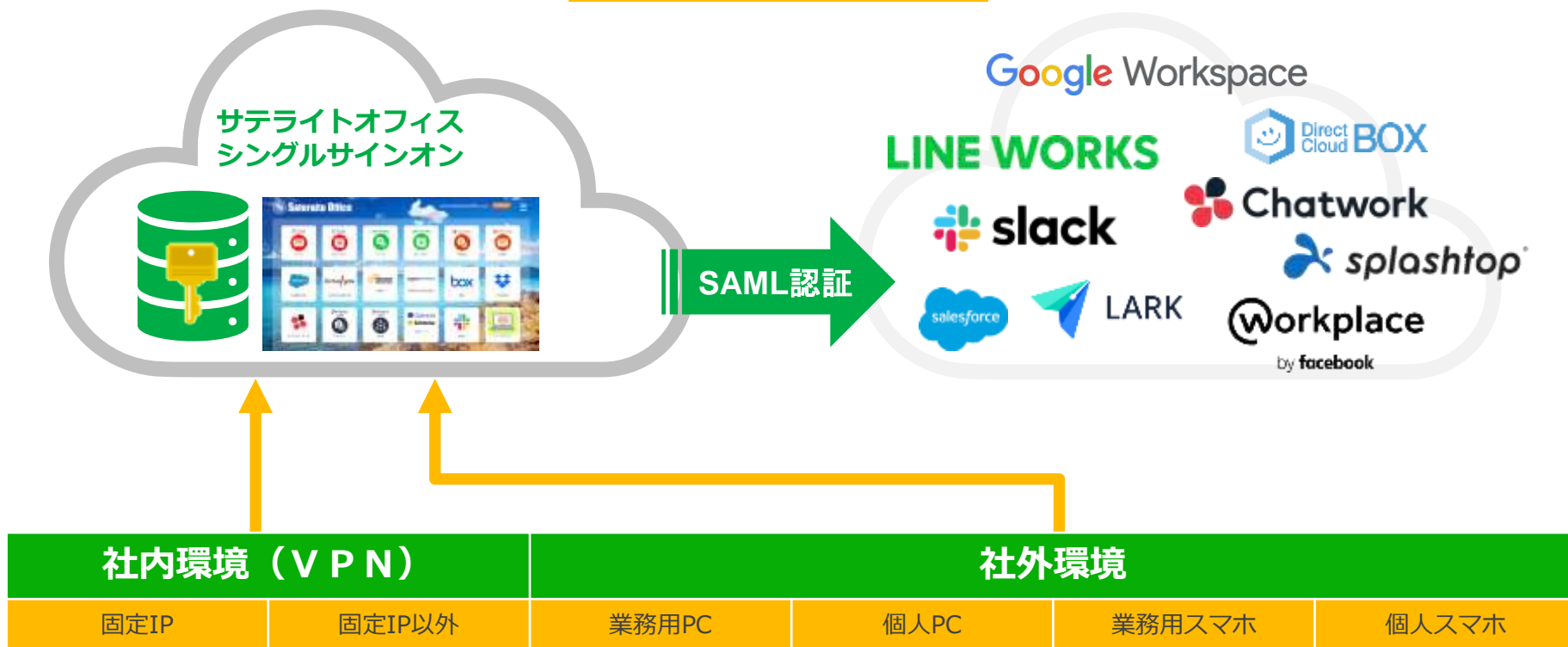
NG

外部システム連携（SAML）対応済みサービス

Google Workspace	LINE WORKS	Microsoft 365	Workplace by Facebook
Salesforce	Dropbox Business	Box	Chatwork
AWS	Amazonビジネス	Slack	サイボウズガルーン/キントーン
デスクネッツNEO	Active! gate SS	DirectCloudBox	Lark Suite
Splashtop	Sugar CRM	ASANA	ARIBA (SAP)
Zendesk	Zoom	GitHub	DocuSign
イントラマート	ナレッジスイート	ZohoCRM/ZohoCreator	SANSAN
X-Point	楽楽精算	コンカー	ジョブカン
SmartHR	FreshWorks	LumApps	CIERTO (シエルト)
Moconavi	Bigtincan Hub	PrimeDrive	Zscaler
Tableau	連絡とれるくん	Zeem	HUE
CAIWA Service Viii	DOMO (IBSKUID)	eセールスマネージャー	Times
Wellspring	カオナビ	シャチハタクラウド	タレントパレット
如意箱(nyoibox)	WAN-Sign	AWS Client VPN	Atlassian Access
Qast	oVice	Adobe Admin Console	メールディーラー
datadog	Fortigate SSLVPN	CyberMailΣ / MailBaseΣ	LumApps
レシートポスト (旧 Dr.経費精算)	マネーフォワード	GitHub	backlog
コラボフロー	Bill One (SANSANの請求書システム)	ManageOZO3 (マネージオゾ)	NI Collabo
ConnectWise			

サテライトオフィスが考えるゼロトラスト対策

インターネット環境



VPN含め全てのネットワークは安全では無いと想定しエンドポイント管理を推奨。クラウドサービスにアクセスする端末は二要素認証+クライアント証明書の「多要素認証」を実施。Google Workspaceの高度なMDM機能と組み合わせることで端末の盗難、紛失時などの対応（ワイプ）も可能です。※サードパーティー製品のMDMでクライアント証明書の配布も可能です。

例：端末紛失時にはSSOで「強制ログアウト+証明書の失効」。GWSのMDM機能で「端末のワイプ」を実施。第三者によるサービスへの不正アクセスをブロック。

シングルサインオン・パスワード強化機能

ログイン時のパスワード機能を強化する事が可能です。簡単なパスワードの利用禁止、有効期限の設定、以前利用したパスワードの禁止、自動ログイン禁止など、パスワードの定期的な変更などの、パスワード強化対策を実現可能です。

パスワード強化



【パスワード強化機能】

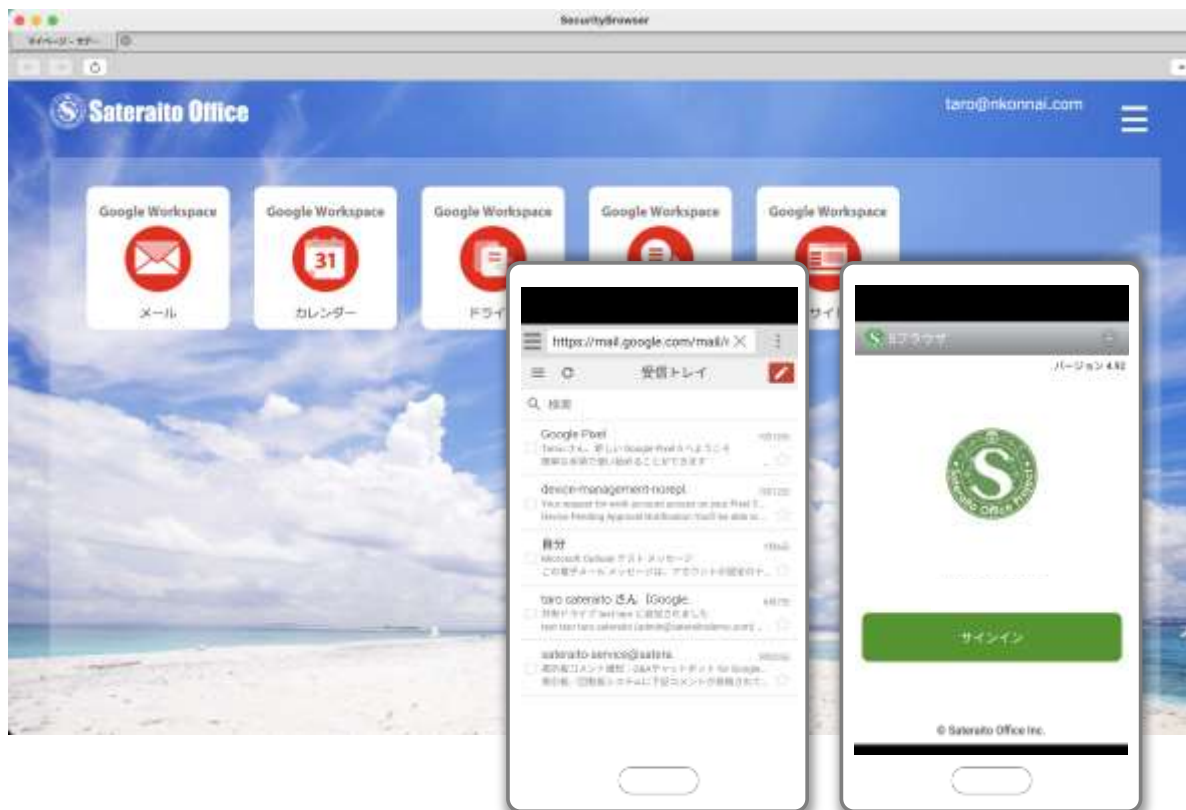
- ・ 簡易パスワードの利用禁止
- ・ パスワードの有効期限の設定
- ・ 以前使ったパスワードの禁止
- ・ 自動ログインの禁止
- ・ ログイン数回失敗時のロック
- ・ パスワードの変更禁止機能
- ・ パスワードの定期的な変更

※パスワード強化機能は、プロファイルとして設定し、ドメイン全体、組織別、ユーザー別に設定する事が可能です。

シングルサインオン・セキュリティーブラウザ機能

シングルサインオン for Google Workspace の無料オプション「セキュリティーブラウザ」も利用可能です。添付ファイルは閲覧のみ（ダウンロード禁止）、文字のコピー禁止、クリップボードの破棄、自動ログアウト、URLフィルターなど細かな制御が可能です。

セキュリティーブラウザ



【セキュリティー機能】

- ・ 利用端末ID制限(MACアドレス/端末ID)
- ・ URLフィルター
- ・ ダウンロード禁止
- ・ 文字のコピー&ペーストの禁止
- ・ クリップボードの自動破棄
- ・ ブラウザ終了時にキャッシュクリア& Cookieクリア (データを残さない)
- ・ 印刷禁止 (クラウドプリントの禁止)
- ・ アドレスバーの表示の ON/OFF機能
- ・ 共有ブックマーク (管理者がユーザーのブックマークを管理可能)

※Windows、Mac、iOS、Androidでご利用いただけます。

サービスのHPは[こちら](#)

シングルサインオン・クライアント証明書

クライアント証明書 for Google Workspaceとは？



サテライトオフィス・シングルサインオンでは、ユーザーの認証や端末制御にご利用いただける、クライアント証明書の発行、管理、端末への配布の機能がございます。Windows、Mac、Android、iOS、Chromebook と主要なすべてのOSに対応しており、追加費用なしでご利用いただけます。

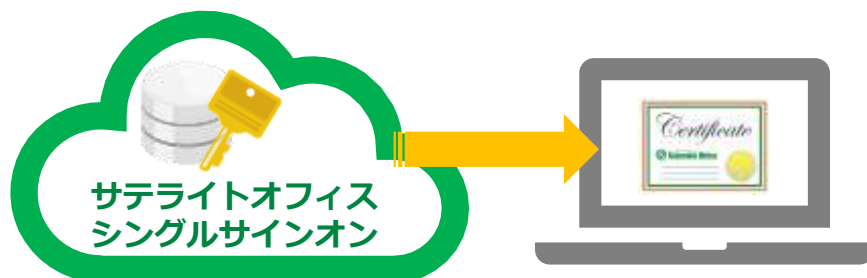
対応OS

Windows、Mac、Android、iOS、Chrome OS

管理機能

- ・ 管理者による一括発行/配布/失効が可能。
- ・ 社有端末のみインストール制御。
- ・ 発行、失効、インストール状況の確認が可能。

サービスのHPは[こちら](#)



FIDO2.0（生体認証）の指紋認証によるログイン

指紋認証に対応した『ATKey.Pro』を利用して生体認証（指紋認証）によるログインが可能です。
パスワードレス認証も可能。指紋認証とクライアント証明書認証を組み合わせるとより強固な認証も可能です。



※写真はHP Chromebook x360 13c

シングルサインオン・二要素認証機能

二要素認証を有効にすることにより、SSOへのログイン時にIDとパスワードに加えて、ワンタイムの認証コードの入力を要求されるようになります。ワンタイムなので一度ログインで使用すると破棄され再利用できません。二要素認証を利用することにより、より強固なセキュリティを実現可能です。



認証コード方式

事前に登録された予備のメールアドレスに送信される認証コード入力する方式です。



認証アプリケーション方式

Google認証システム / Microsoft Authenticator アプリなどのTOTPベースの認証アプリケーションから発行される認証コードを入力する方式です。



顔認証方式 (Experimental)

事前に登録した顔写真と照らし合わせることで認証する方式です。
(※一部ブラウザ、アプリケーションではご利用頂けません。)



セキュリティキー方式

ログイン認証、二要素認証用のFIDO、FIDO2のセキュリティーキーを登録してログインする方式です。

シングルサインオン・管理機能について

Google Workspace単体では煩雑になりがちなユーザー情報、グループ情報を一括管理可能です。シングルサインオンのデータ管理は、GUIからの登録、csvインポート/エクスポート、Active Directoryや社内システムとの同期が可能です。（データ同期は、タスク管理で定期実行も可能です）

[マイページ](#) | [ヘルプ](#) | [ログアウト](#)

ダッシュボード ユーザ管理 組織(Group)管理 組織(OU)管理 セキュリティルール管理 クライアント証明書管理 **タスク管理** 外部システム連携管理

タスク管理

タスク一覧

タスクの追加

- ユーザをGoogle Workspaceから取込
- ユーザをGoogle Workspaceに反映**
- 組織(Group)をGoogle Workspaceから取込
- 組織(Group)をGoogle Workspaceに反映
- 組織(OU)をGoogle Workspaceから取込
- 組織(OU)をGoogle Workspaceに反映
- クラスルームをGoogle Workspaceから取込
- クラスルームをGoogle Workspaceに反映

ここでは、ユーザや組織のGoogle Workspaceへの反映、Google Workspaceからの取り込みの設定を行うことができます。また設定したタスクの予約状況やステータスを確認できます。タスクは一定間隔で実行されますので、登録後、実行まで少々お待ち下さい。

タスク新規登録 - ユーザ情報をGoogle Workspaceアカウントに反映する

タスクの新規登録画面です。必要な情報を入力し「タスクを登録する」ボタンをクリックしてください。

基本情報

タスクの種類 * ユーザ情報をGoogle Workspaceアカウントに反映する

初回処理予定 ※実際の処理タイミングは自動で決定されます（30分ごと）。 **繰り返し設定** 今日のみ同期

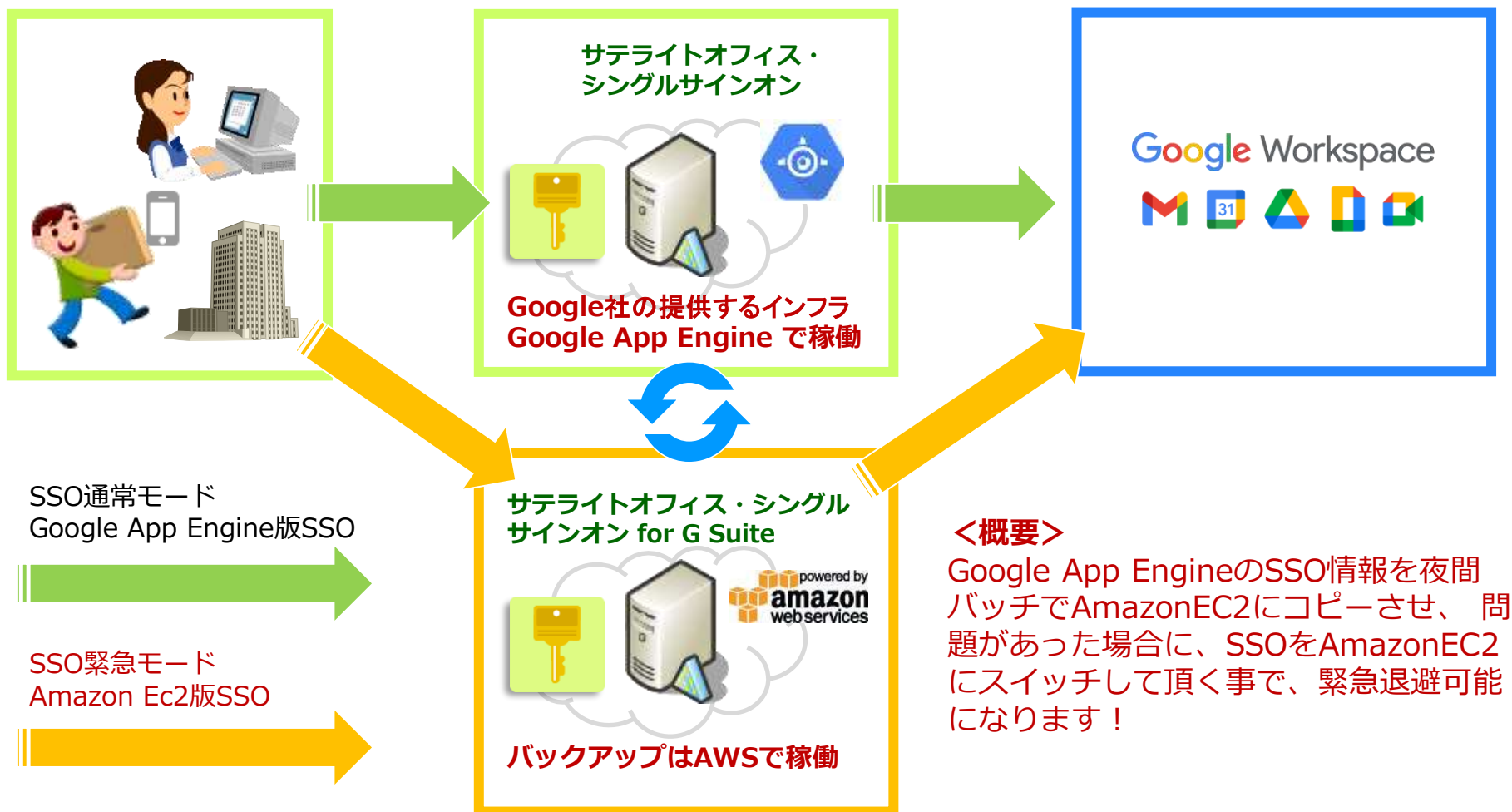
メモ

オプション設定

- シングルサインオンに存在しないユーザをGoogle Workspaceから削除する（基本はOFF）
※「Google Workspaceユーザとして連携する」設定が有効になっていないユーザはGoogle Workspaceから削除されますので十分ご確認ください（**削除したデータは復旧できません!**）。
- 前回の同期から変更のあるデータのみ更新する（推奨）
※シングルサインオン側で更新のあったデータのみ更新対象とすることができます。設定を有効にするとGoogle Workspace側でユーザー情報が変更されても更新対象とはなりませんのでご注意ください。
- エイリアスアドレスも同期する
- エイリアスアドレス** ※ユーザ管理に登録されているエイリアスアドレスでGoogle Workspaceユーザーのエイリアスを上書きします。該当のエイリアスアドレスが既に他のアカウントやグループのアドレスあるいはエイリアスアドレスとして登録されている場合はエラーとなりますのでご注意ください。
- 新規作成時ユーザーを指定組織(OU)に所属させる 所属組織(OU):
- 組織(OU)に関する設定** ※Google Workspaceへのユーザー新規作成と同時に指定した組織(OU)に所属させるオプションです。Google Workspaceに存在する組織を「サテライトオフィス/東京本社」のような形式で指定してください。ユーザー更新時には組織(OU)は変更しません。

シングルサインオン・リカバリー対策

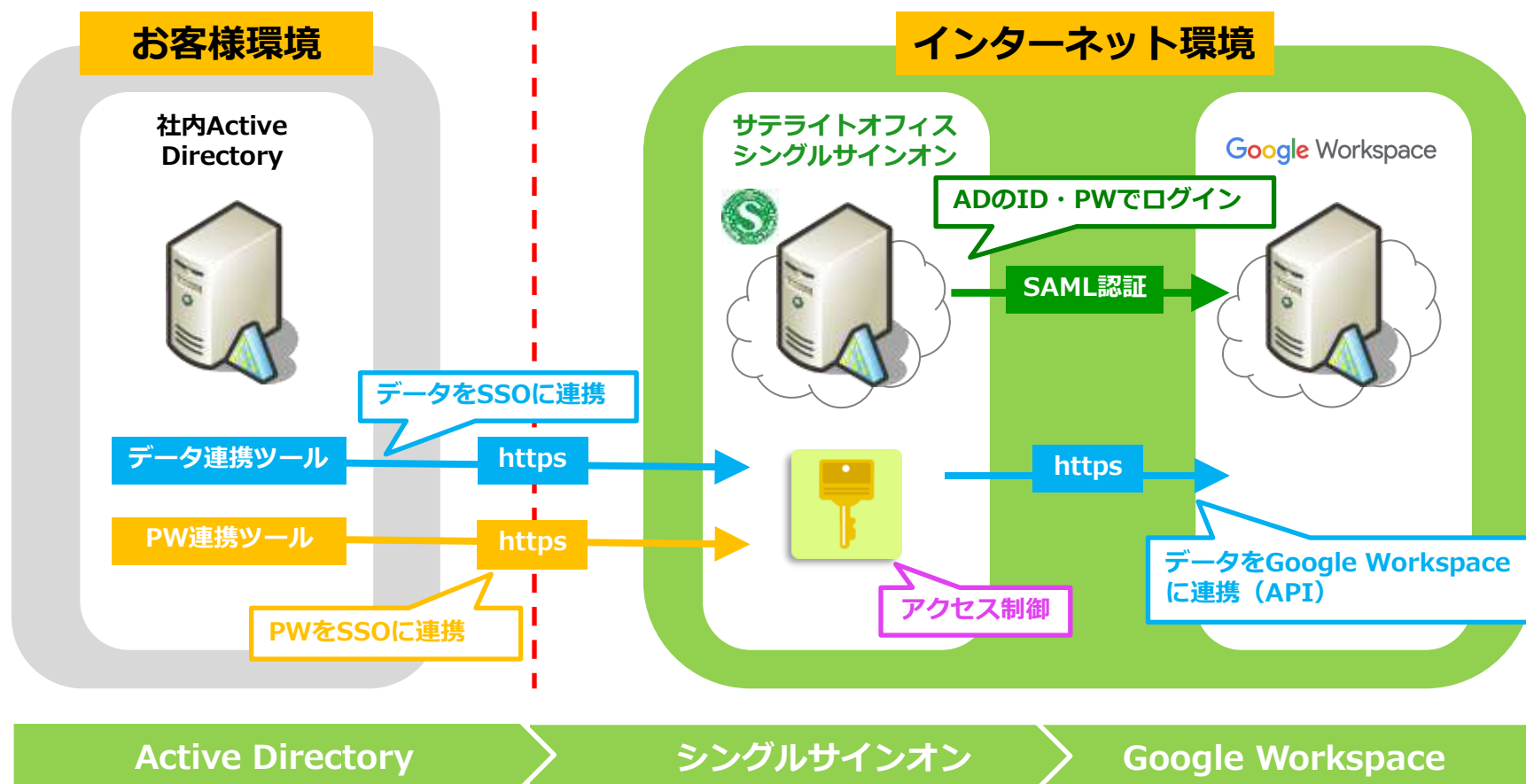
万が一シングルサインオンやGoogle App Engineがダウン時に、緊急モードに切り替えることで引き続きサービスをご利用頂けます。



シングルサインオン/Active Directory連携について

Active Directoryとユーザ、組織、セキュリティーグループ情報を定期的に連携することが可能。Active Directoryとパスワードをリアルタイムに連携も可能です。

システム連携時のプロセス



サテライトオフィス・シングルサインオン

外部シ
ステム連携

基幹系システムや他クラウドサービスとのシングルサインオンが可能

社内システム・基幹系システムとは「POST・GET」「SAML」「代行入力」などでのシングルサインオンが可能です！他クラウドシステムとは、SAML2.0対応していればシングルサインオン可能です！お問い合わせいただければ連携可能か？確認いたします！

その他

多言語対応 / 組織単位に管理業務を委任

サテライトオフィス・シングルサインオン は、多言語対応（日本語、英語、中国語、韓国語、各EU、東南アジア各国語・等・・・）されております。

管理者は、ドメイン全体/組織単位/グループ単位に管理者を置くことが可能です！



サテライト オフィス
Sateraito Office

サテライトオフィス・シングルサインオン

サテライトオフィス・シングルサインオン 機能一覧

- ◎ アカウント、組織&グループ&メンバーリストの一括管理が可能です。
- ◎ アカウントや組織情報をGoogle Workspaceへの同期（一括インポート）が可能です。
- ◎ Google Workspaceログイン制御（ネットワークIPアドレス単位、ブラウザ単位、キャリア単位、端末種類単位：iPhone/Android、MACアドレス・・・）が可能 → 端末個別認証によるログイン制御可能（パソコン、スマートフォン）
- ◎ **(New)** 曜日×時間帯、休日カレンダーによるログイン制御機能（休日は管理者により登録可能）
- ◎ ログイン制御は、プロファイル設定により、メンバー単位&組織単位にセキュリティーポリシー制御が可能です。また、社内ネットワーク・社外ネットワーク、スマートフォン、ガラ携帯などの個別にポリシー設定が可能
- ◎ ユーザーのパスワードポリシー強化対応（定期的な変更強制、パスワード複雑化、パスワード履歴管理）
- ◎ スマートフォン、ガラ携帯にも対応！（※ガラ携帯はご利用いただけない端末もございます）
- ◎ ログイン後ページ遷移強制機能（例：ログインしたら必ず社内ポータルにジャンプさせる！）
- ◎ ユーザーのログインログの取得可能、CSVでのダウンロードが可能 ※1年間保存、それ以上要相談
- ◎ 社内のActiveDirectory（AD）または、既存システムからのアカウント同期が可能です！→複数ADと同期可能
- ◎ 社内のActiveDirectory（AD）または、既存システムからのと組織情報連携（セキュリティーグループ、OU）が可能
- ◎ 社内のActiveDirectory（AD）とGoogle Workspace のパスワードのリアルタイム同期
- ◎ SSO側のパスワードを変更する事で、ActiveDirectory（AD）側のパスワードの変更が可能です！
- ◎ SSO側の属性を変更する事で、ActiveDirectory（AD）側の属性の変更が可能です！
- ◎ 社内のActiveDirectory（AD）にログインすると、Google Workspace にも自動ログイン機能（IISダイジェスト認証/統合認証）
- ◎ 管理者権限を、マルチドメイン全体、ドメイン単位、組織単位、プロジェクト単位に権限を委託可能
- ◎ **(開発中)** アカウント追加時のワークフロー機能（現場:申請→承認→管理部門:最終承認）
- ◎ **(開発中)** 組織変更データの期日前登録（例:4月組織変更データを3月に投入）
- ◎ **(New)** 管理者の操作&オペレーションログ機能（1年間保持！管理機能の部分的な委譲機能もございます！）
- ◎ アカウント同期の定期タスク機能（差分同期対応）

※機能一覧の内容は、開発中の機能も含まれます！

サテライトオフィス・シングルサインオン

サテライトオフィス・シングルサインオン 機能一覧

- ◎多言語対応（英語、ドイツ語、フランス語、スペイン語、イタリア語、ポルトガル語、日本語、中国語、韓国語、その他多数可能）
- ◎SSO上の組織情報&アカウント情報を全メンバーの各個人アドレス帳・SharedContactに一括設定する機能
- ◎(New)社内システム・既存システムとのSSO機能（Google以外の既存システムとのSSO連携が可能）
- ◎(New)代行入力(=手動入力ログインを自動化)型のシングルサインオン機能（既存システムのログインも可能）
- ◎組織情報のサテライトオフィス・組織アドレス帳との連携
- ◎組織情報のサテライトオフィス・ワークフロー/ドキュメント管理などのとの連携
- ◎中国からのアクセス対策（VPN利用：全てのお客様：有料）
- ◎POP/IMAPでご利用時のシングルサインオン機能（全てのお客様有料：1人1ヶ月100円）
- ◎IPv6環境でのログイン制限機能&ログインログ機能
- ◎(New)MACアドレスでのログイン制御機能
- ◎(New)Windows/Mac端末用アプリによるログイン端末認証 → ダウンロードはこちら [\(Win&Mac版\)](#)
- ◎(New)代行入力(=手動入力ログインを自動化)型のシングルサインオン機能（既存システムのログインも可能）
- ◎(New)2要素認証（メール連絡認証:開発済,電話着信認証&SMS連絡認証:開発中）
- ◎(New)顔認証によるログイン2要素認証（スマートホンやパソコンのカメラで顔認証）
- ◎(開発中)フェリカ:Felicaカード（Suica,Edy,Pasmo...）、Mifareカードによるログイン2要素認証
- ◎(開発中)フェリカ:Felicaカード（Suica,Edy,Pasmo...）、Mifareカードによる自動ログイン、自動ログオフ機能
- ◎(開発中)ビーコン（Beacon）によるログイン2要素認証
- ◎(New)マトリックス認証（ワンタイムパスワード）機能（ログイン時にワンタイムな数字に認証）
- ◎(New)TOTP認証（時間ベースのワンタイムパスワードによる2要素認証）機能
- ◎(New)クライアント証明書でのログイン制御機能（一般クライアント証明書でのログイン制御が可能）
→サテライトオフィス・クライアント証明書：無償提供中
- ◎iOS/Androidアプリによるログイン端末認証 → ダウンロードはこちら [\(iOS版/Android版\)](#)

※機能一覧の内容は、開発中の機能も含みます！

サテライトオフィス・シングルサインオン

サテライトオフィス・シングルサインオン 機能一覧

- ◎ **(New)** Google Workspace 専用のセキュアブラウザ無償提供 (サテライトオフィス・セキュリティーブラウザ)
- ◎ **(New)** プッシュ通知機能：セキュリティーブラウザ利用時にスマホにプッシュ通知が可能
- ◎ **(New)** クラスルーム(ClassRooms)管理機能
- Google Workspaceのマルチドメイン機能対応 (管理者画面にて設定が必要)
- セキュリティー対策済み (SQLインジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリー対策済)
- ◎ SSOダウン対策機能 (GAE版SSOがトラブル時、AmazonEC2版SSOにワンクリックで切替可能) [資料こちら](#)
- ◎ **(New)** Microsoft Edgeブラウザ対応
- ◎ **(New)** Microsoft 365 にもシングルサインオン(ログイン)可能 → Google Workspace + MSOffice (Microsoft 365 ProPlus) 利用が可能！
- ◎ **(New)** SSOパスワードを復号不可なハッシュ値で保存機能
- ◎ **(New)** シングルサインオンの機能をAPIで外部操作&連携可能
- ◎ **(New)** 他社SSOからの移行対応
- ◎ **(開発中)** 会社共有端末での端末利用管理 (チーム全体で共有している端末での端末許可機能)
- ◎ **(New)** デジタル複合機連携 (複合機のログインをシングルサインオン経由で可能です) ※[シャープ社製はこちら](#)
- ◎ **(New)** ブロックチェーン技術を利用したデータ保証機能 (管理者操作ログ！その他開発中)

※機能一覧の内容は、開発中の機能も含まれます！



シングルサインオン機能 構築サービス

本章は、シングルサインオン構築サービスの説明



シングルサインオン機能 構築支援サービス（有料）

シングルサインオン機能の構築支援サービスについて説明します！

シングルサインオン設定支援サービス

貴社へのヒヤリングを行い、弊社の方でシングルサインオン機能の設定を行います。
15万円～ 要見積

シングルサインオンサービスの無償サポート

貴社管理者様からの電話問い合わせ、メール問合せ、フォームからのお問い合わせにつきましては、全て無償にてサポート致します。
※別途有償にてユーザーレクチャーなどもご対応可能です。

社内システムとの連携支援サービス

貴社社内システムとの同期やシングルサインオン機能を実現する支援サービスになります。
50万円～ 要見積



最後に

本章は、その他の説明をします。



サテライト オフィス
Sateraito Office

なぜサテライトオフィスなのか？

サテライトオフィスが提供するソリューションのメリットは何か説明させていただきます。

50000社以上の導入実績によるノウハウ提供

50000社（中小規模～大規模）以上の導入支援によるGoogle Workspaceの情報が豊富です。新しい機能や新しい技術に関しても、導入済みのお客様とのコミュニケーションによりいち早く解決して行きます。また、50000社様の要望の多いものから拡張アプリケーションとしてリリースして行きます。

Google Workspace ビジネステンプレート+アドオンアプリケーションの提供

多くのビジネステンプレートをご用意しております。今までのグループウェアの様な、テンプレートも用意しております。また、Google Workspace内では実現できない部分は、拡張アプリケーションとして、API + Google App Engine などを利用する事で、今後も実現して行きます。是非、ご要望をください！

Google App Engine や APIによる開発（カスタマイズ）ソリューション

弊社Google App Engineフレームワークによるシステム開発が可能です。またAPIを利用した社内システムとの連携ソリューションも有効的です！今後もGoogle App EngineやAPI技術は、早い速度で拡張していきます。サテライトオフィスでは、いち早く技術を習得し、ソリューションとして、提供して行きます。

弊社スペシャリストとのテレビ会議&オンサイトによるスピーディーなサポート体制

サテライトオフィスの**一番の強みはサポート**です。電話やテレビ会議や画面共有ソフトを利用し、とにかくスピーディーに解決して行きます。満足度高いサポートを提供していきますので、よろしくお願いいたします。



Sateraito ~ for your best solution



BayTech Systems,
The Finest Solution
Company



サテライト オフィス
Sateraito Office



Google for Education
Partner



Google Cloud
Partner

認定ソリューション開発パートナー

株式会社サテライトオフィス
〒135-0016
東京都江東区東陽4-3-1
東陽町信栄ビル4F
TEL : 050-5835-0396 (代表)
FAX : 050-6861-2893
E-Mail : contact-info@sateraito.co.jp