



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 スタートアップガイド



サテライト オフィス
Sateraito Office

株式会社サテライトオフィス

2014年01月15日

1. サテライトオフィス・シングルサインオンのインストール

Google Apps管理コンソールへログインしてください。

The screenshot shows the Google Admin console interface. At the top, there is a Google logo, a search bar, and a user profile for 'admin@'. Below the header, the page title is '管理コンソール' (Admin Console). The main content area is divided into two columns. The left column contains several management tiles: 'ユーザー' (Users) with 4 users and 0 invites; 'グループ' (Groups) with 8 groups; '会社プロフィール' (Company Profile) for 'Sateraito.jp'; 'ドメイン' (Domains) with 'sateraito.jp'; 'お支払い' (Billing); 'Google Apps' with 27 apps; '管理者の役割' (Admin Roles) with 8 roles; 'Marketplace アプリケーション' (Marketplace Applications) with 27 apps; '携帯端末' (Mobile Devices); and 'セキュリティ' (Security). The right column shows usage statistics for the last 7 days: 3 active users (75%) and 0 documents. Below this are sections for 'ツール' (Tools) including Google Apps Marketplace and '一般的なタスク' (General Tasks) such as checking email capacity and customizing design. At the bottom, there is a link for 'その他の設定' (Other Settings). The footer of the console shows '©2013 Google Inc. 利用規約 - プライバシー ポリシー'.

1. サテライトオフィス・シングルサインオンのインストール

- ・メールにて送られて来たサインインストール短縮URLをクリックして下さい。
- ・Google Apps Marketplace画面ステップ①「利用規約に同意する」ページへ遷移しますので、「同意して続行」をクリックして下さい。

The image displays two screenshots of the Google Apps Marketplace interface during the installation process. The left screenshot shows the '同意する' (Agree) step, where the user is prompted to agree to the terms of service. A yellow box highlights the warning about third-party services, and the '同意して続行' (Agree and Continue) button is highlighted with a red box. The right screenshot shows the 'データへのアクセスを許可する' (Allow access to data) step, where the user is prompted to allow access to their data. A list of permissions is shown, and the 'データへのアクセスを許可する' (Allow access to data) button is highlighted with a red box.

- ・ステップ②「セットアップ」ページへ遷移しますので「データへのアクセスを許可する」をクリックしてインストール完了です。

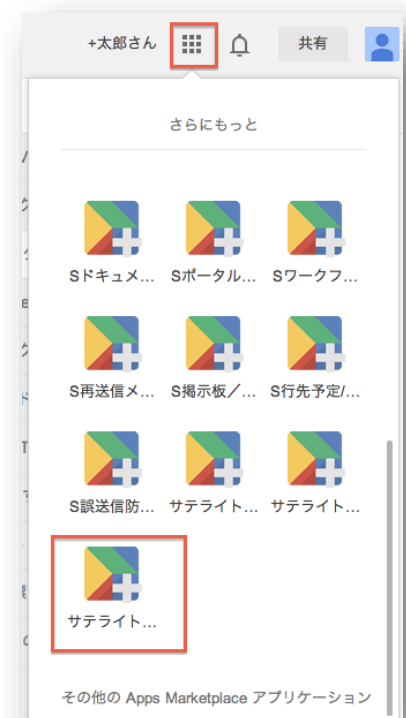
1. サテライトオフィス・シングルサインオンのインストール

- ・正常にインストールされているか確認するには、Google Apps管理者コンソールから、「MarketPlaceアプリケーション」より確認可能です。サテライトオフィス・シングルサインオンが表示されていればインストール成功です。
- ・Googleツールバーの「もっと見る」からも確認出来ます。

「MarketPlaceアプリケーション」から確認する。



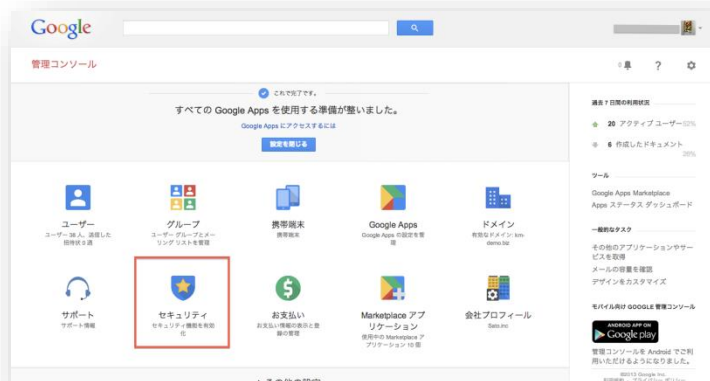
「もっと見る」から確認する。



2. Google AppsのAPIアクセスを有効にします。

・サテライトオフィス・シングルサインオンを有効化する為に、Google Apps管理コンソールからGoogle AppsのAPIアクセスを有効にします。

- ①管理コンソールのダッシュボードから、セキュリティをクリックします。



- ②APIリファレンスをクリックし、「APIアクセスを有効にする」にチェック、変更を保存します。



3. シングルサインオン管理コンソールへアクセスします

①Googleツールバーの「もっと見る」から
 シングルサインオンをクリックします。



②下記ページへ遷移しますので、<管理者の方向けの管理画面はこちら>
 から、「サテライトオフィス・シングルサインオン」をクリックして下さい。



<管理者の方向けの管理画面はこちら>

下記のURLをブックマークにご登録ください！

<https://kddi-ssso.appspot.com/a/>

または、このリンク [サテライトオフィス・シングルサインオン](#) をドラック&ドロップでブラウザ

3. シングルサインオン管理コンソールへアクセスします

シングルサインオンのログイン画面が開きますので、
Google Appsの特権管理者ID・PWでログインが可能です。



シングルサインオンの管理コンソールです。

4. シングルサインオン管理コンソールの設定

シングルサインオン管理コンソールの設定を開始します。

①ダッシュボードから、固定グローバルIPアドレスを設定致します。「プロファイルで使用する社内ネットワーク」からIPアドレスを入力し、「社内ネットワークのIPアドレスを追加」をクリックします。

ご設定前に管理者に適切なパスワードが設定されているかなどご確認ください！

プロファイルで使用する サブネットマスク...

社内ネットワーク:

※会社のグローバルIPアドレスを指定ください。(例: 202.222.123.120) 調査方法は[こちら](#)
※IPv6環境の場合はサブネットマスクは不要です。(例: 3FFE:FFFF::8:800:20C4:0)
※ここで社内からインターネットにアクセスするゲートウェイ・プロキシサーバのIPアドレスを設定しておくこと、プロファイルによるアクセス制御の設定が簡単になります！
プロファイルごとに個別にネットワークを追加することも可能です。

IPアドレスとして「X-Forwarded-For」値を優先して使用する (通常は利用しません)

※「REMOTE_ADDR」がここで指定されたIPアドレスの中にある場合のみ「X-Forwarded-For」値を使用します。
※CIDR形式 (例: 121.111.222.120,121.111.222.121/29)
※IPv6形式 (例: 3FFE:FFFF::8:800:20C4:0)
※未指定の場合はチェックしません。通常は社内プロキシサーバのIPアドレスを設定してください。カンマ区切りで複数指定可能です。

※調査方法は[こちら](#)をクリックして頂いても確認が可能です。

②必要に応じて、支店や工場など、各拠点のIPアドレスを登録して下さい。

4. シングルサインオン管理コンソールの設定

①データ連携の為に、特権管理者のID・PWを登録します。

▶ GoogleApps設定

Apps管理者アカウント:

※GoogleAppsとの連携に使用します。メールアドレス全体を入力してください。

Apps管理者パスワード: [変更](#)

OAuthコンシューマキー: [こちらから取得](#)

OAuthコンシューマシークレット: [変更](#)

※OAuth情報はGoogleApps管理画面で設定したものをセットしてください。

②特権管理者のID・PWを入力管理したら、保存をクリックします。

※緊急モードは、AmazonEC2上で稼働するSSOです。前日までの設定やユーザ情報がAmazonEC2にコピーされます。シングルサインオンやGoogleAppEngineのダウン時には、緊急モードに切り替えて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に直接ブックマークをしていると緊急モードをご利用頂くことができません。Googleのポータルサイトや推奨します。

※詳細は[緊急モードへの切り替えについて](#)をご参照ください。

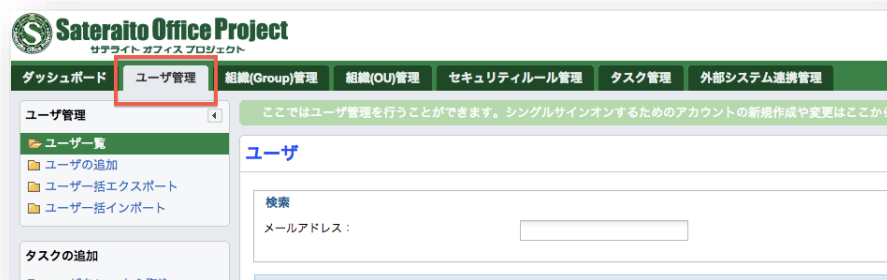
保存

リセット

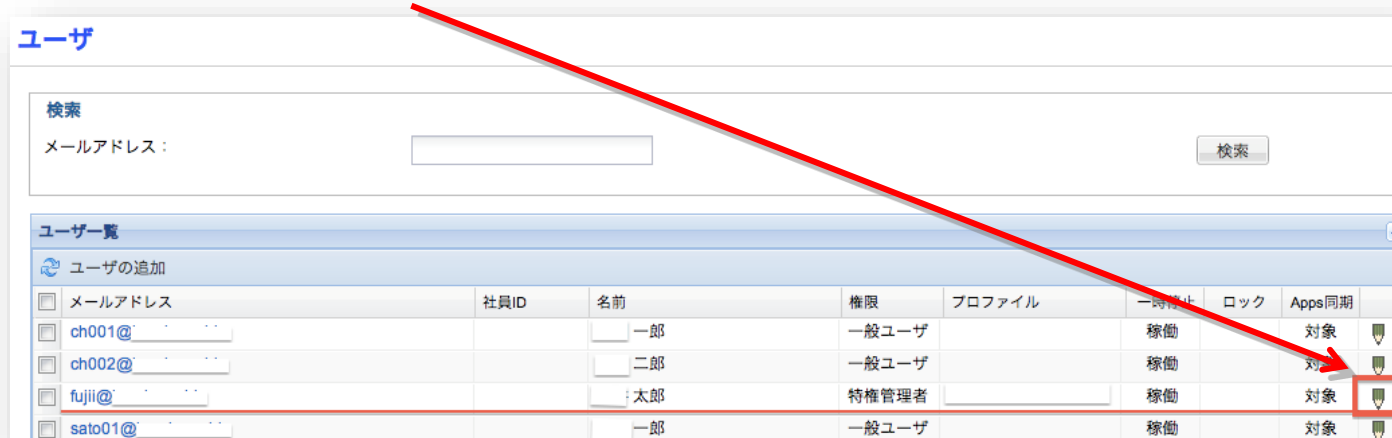
5. シングルサインオンプロファイルの設定

サテライトオフィス・シングルサインオンでは、特権管理者はGoogle AppsのID・PWでログイン、一般ユーザはGoogle AppsのID・PWを教えずに、シングルサインオン独自のID・PWで管理するのが一般的です。まずは、特権管理者のプロファイルを設定します。

①ユーザ管理をクリックします。



②まずは管理者に対して、管理者用プロファイルを設定致します。ユーザー一覧の「特権管理者」から、右側にある「鉛筆」アイコンをクリックします。



5. シングルサインオンプロファイルの設定

③ユーザ詳細画面にて、「管理者用プロフィール」を設定します。

編集方法：「編集」をクリック⇒「管理者用プロフィールを設定」⇒「ユーザ情報を保存する」をクリックして完了です。

編集する 複製する ユーザIDを変更する 削除する 戻る

姓カナ 名カナ

予備のメールアドレス
※二要素認証ログインで使用します。プロフィールで二要素認証を有効にしているユーザー

プロフィール
管理者用プロフィール
※プロフィールの反映には数分かかる場合がございます。

アカウント一時停止 稼働中

ユーザ情報を更新する リセット 戻る

5. シングルサインオンプロファイルの設定

④次に一般ユーザのSSOパスワードを設定します。

ユーザー一覧からPWを設定するユーザをクリックします。（ユーザ詳細画面を表示までは、P10管理者の設定と同じ流れになります。

編集方法：「編集」をクリック⇒SSOパスワード「設定」⇒「ユーザ情報を保存する」をクリックして完了です。

編集する 複製する ユーザIDを変更する 削除する 戻る

社員ID

SSOパスワード 弱 キ

※未設定 設定

Appsパスワード (連携用)

※GoogleAppsや他のシステムとの連携用パスワードです。ログイン認証や、

ユーザー情報を更新する リセット 戻る

※今回は各ユーザ毎にPWを設定しましたが、CSVによる一括アップロードも可能です。

5. シングルサインオンプロファイルの設定

⑤次に一般ユーザ全てに割り当てるデフォルトのプロファイルを設定します。

シングルサインオン・ダッシュボードをクリックし、「デフォルトで設定するプロファイルを設定」にて「一般ユーザ標準プロファイル」を選択し、設定を保存します。

ダッシュボード ユーザ管理 組織(Group)

ドメイン設定

ユーザ名の表示: 姓、名の順で表示

ログイン制御設定

デフォルトで利用するプロファイル: 一般ユーザ用標準プロファイル

プロファイル: ※標準で使用するログイン設定やアクセス制御のためのプロファイルです。(設定ユーザや組織ごとの設定も可能です)。※プロファイルの反映には数分かかる場合がございます。※個別にプロファイル設定されていない管理者を含めた全ユーザに適用されます。ご設定前に管理者に適切なパスワードが設定されているかなどご確認ください!

プロファイルで使用する社内ネットワーク: サブネットマスク... 社内ネ

※御社のグローバルIPアドレスを指定ください。(例: 202.222.123.120) 調査方法は...
※IPv6環境の場合はサブネットマスクは不要です。(例: 3FFE:FFFF::8:800:20C4:0)
※ここで社内からインターネットにアクセスするゲートウェイ・プロキシサーバのIPアド

保存 リセット

5. シングルサインオンプロファイルの設定

⑥次にGoogle Apps管理コンソールの設定へと進みますが、その前にSSO証明書ファイルをダウンロード&保存します。

ダッシュボードの「SSO証明書ファイルの作成（差し替え）」をクリックしてダウンロードしておいて下さい。

▶ シングルサインオン設定

キーファイル：

SSO用証明書ファイルを再取得（差し替え）

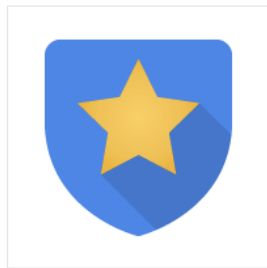
※シングルサインオン用のX.509証明書ファイルを作成しダウンロードします。
ダウンロードしたファイルはGoogleAppsのシングルサインオン設定画面からのアップロードで使用します。
※同時にシングルサインオンサーバ側にも対となる鍵ファイルがセットされます。

6. Google Apps管理コンソールの設定

Google Apps管理コンソールにて再度シングルサインオンの設定を行います。

操作方法：「Google Apps管理コンソール」⇒「セキュリティー」⇒「詳細設定」⇒「シングルサインオン (SSO) の設定」をクリックして下さい。

← セキュリティー



セキュリティー

km-demo.biz

基本設定

ユーザーの SSL の有効化、パスワードの安全度ポリシーの設定、2 段階認証プロセスの適用の操作を行います。

パスワードの監視

組織の各ユーザーのパスワードの安全度を監視します。

API リファレンス

API を有効にして、独自に作成したアプリケーションやサードパーティ製アプリケーションを介して、プロビジョニング、レポート、移行をプログラムで管理しま

詳細設定

シングルサインオン、認証、Google Apps と内部サービスの統合など、高度な

詳細設定

シングルサインオン (SSO) の設定

シングルサインオン (SSO) の設定

Gmail やカレンダーなどのウェブベース アプリケーションについては、SAML ベースのシングルサインオン (SSO) サービスを使用して、ユーザーアカウントを認証できます。Google トーク、Gmail への POP アクセスなどのデスクトップ アプリケーションについては、ユーザーは引き続き Google 管理コントロール パネルで設定されたユーザー名とパスワードを使用して個別にログインする必要があります。 [詳細](#)

認証

OAuth ドメイン キーを管理する

ドメインの管理者は、ユーザーのログイン認証情報なしにユーザーのすべてのデータにアクセスできます。 [?](#)

6. Google Apps管理コンソールの設定

①はじめに、先程シングルサインオン管理コンソールより発行した「SSO用証明書ファイル」をアップロードします。

設定画面の中程にある「認証の確認」項目からアップロードを実行して下さい。

The screenshot shows the Google Apps Single Sign-On (SSO) settings page. The page title is "シングルサインオン (SSO) の設定". The page contains several input fields for "ログイン ページの URL", "ログアウト ページ URL", and "パスワード変更 URL". There are also checkboxes for "シングルサインオンを有効にする" and "ドメイン固有の発行元を使用".

Overlaid on the page is a Windows Explorer window showing the "Downloads" folder. The file "ssocert.cer" is selected, and the "開く(O)" button is highlighted with a red box. A red arrow points from this button to the "証明書を更新" button in the "認証の確認" section of the SSO settings page. Another red arrow points from the "証明書を更新" button to the "アップロード" button in the "認証の確認" section. A third red arrow points from the "アップロード" button to the "アップロード" button in the "認証の確認" section, which now shows the file "ssocert.cer" selected.

6. Google Apps管理コンソールの設定

②次にログイン/ログアウト/パスワード変更の各URLを設定し、シングルサインオンを有効化します。

設定画面の先頭にある「シングルサインオンを有効にする」をチェックし、各URLを設定して下さい。URLは次のマニュアルに記載があります。

⇒ <https://sites.google.com/a/sateraito.jp/sateraito-dounyuu/Home/sso>

The image shows a screenshot of the Google Apps Single Sign-On (SSO) configuration page. The page title is "シングルサインオン (SSO) の設定" (Single Sign-On (SSO) Settings). The main heading is "シングルサインオン (SSO) の設定" and the sub-heading is "SSO を設定するには次の情報を入力してください。SSOリファレンス" (To configure SSO, enter the following information. SSO Reference). The "シングルサインオンを有効にする" (Enable Single Sign-On) checkbox is checked. The "ログインページのURL*" (Login page URL) is set to "http://sateraito-apps-ss0.appspot.com/a/". The "ログアウトページのURL*" (Logout page URL) is set to "https://sateraito-apps-ss0.appspot.com/a/". The "パスワード変更URL*" (Password change URL) is set to "https://sateraito-apps-ss0.appspot.com/a/". The "認証の確認*" (Verify authentication) section is also visible. A browser window in the foreground shows the URL "https://sites.google.com/a/sateraito.jp/sateraito-dounyuu/Home/sso" and a list of configuration options for SSO, including login, logout, and password change URLs, with a red arrow pointing to the URL in the browser address bar.

④ログイン、ログアウト、パスワード変更URLの設定

～有償版～

- ・ログインURL: <http://sateraito-apps-ss0.appspot.com/a/{ドメイン名}/sso/login> ※ログインURLのみ先頭は「http://」としてください(セキュリティは万全です!)
- ・ログアウトURL: <https://sateraito-apps-ss0.appspot.com/a/{ドメイン名}/sso/logout>
- ・パスワード変更URL: <https://sateraito-apps-ss0.appspot.com/a/{ドメイン名}/sso/password>

～無償版～

- ・ログインURL: <http://sateraito-apps-ss03.appspot.com/a/{ドメイン名}/sso/login> ※ログインURLのみ先頭は「http://」としてください(セキュリティは万全です!)
- ・ログアウトURL: <https://sateraito-apps-ss03.appspot.com/a/{ドメイン名}/sso/logout>
- ・パスワード変更URL: <https://sateraito-apps-ss03.appspot.com/a/{ドメイン名}/sso/password>

※各URLの最後に「/」はつけないでください。
 ※{ドメイン名}の部分は、ご登録頂いたGoogleAppsのドメイン(マルチドメインの場合はプライマリドメイン)をご入力ください。
 ※GoogleAppsのシングルサインオン設定画面に入力するURLです。ユーザーが直接ログインするURLではありません。

6. Google Apps管理コンソールの設定

③次に「ドメイン固有の発行元を使用」をチェックし、設定の変更を保存します。

設定画面の中程の「ドメイン固有の発行元を使用」をチェックし、最下部の「変更を保存」をクリックして下さい。

← セキュリティ

パスワード変更 URL *

ユーザーがシステムでパスワードを変更する際にアクセスする URL です。定義すると、この URL はシングルサインオンが有効になっていない場合でも表示されます

認証の確認 *

認証ファイルのアップロードが完了しました [証明書を更新](#)

認証ファイルには、ログインリクエストを確認するための Google 公開キーが含まれている必要があります。 [詳細](#)

ドメイン固有の発行元を使用

ドメインで IDP アグリゲータを使用して SAML リクエストを処理する場合は、これを選択する必要があります。
有効になっていれば、SAML リクエストで送信した発行元は **google.com** ではなく **google.com/a/ga-test4.soc-net.jp** となります。 [詳細](#)

ネットワーク マスク

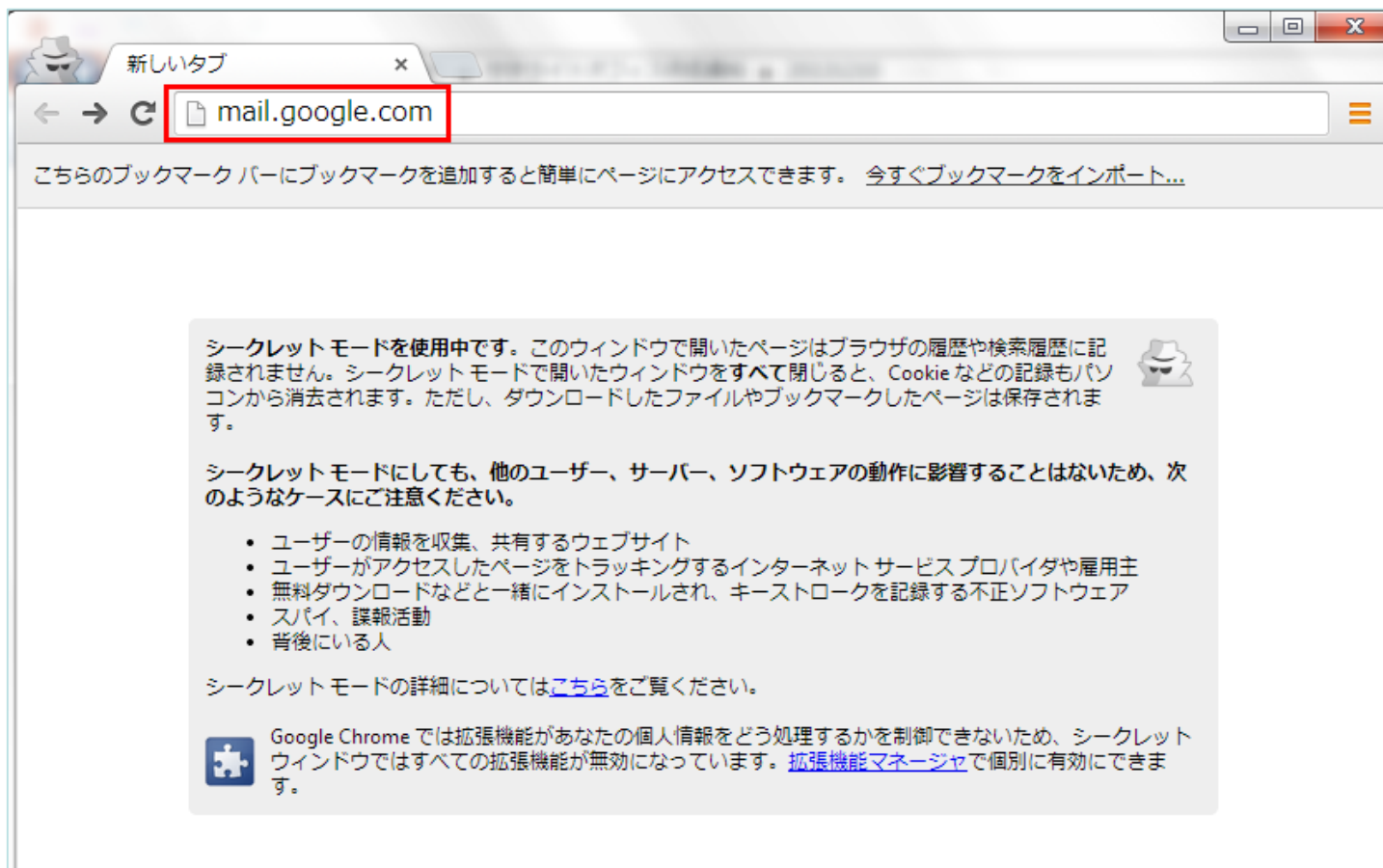
ネットワーク マスクは、シングル サインオンで有効にできるアドレスを決定します。マスクが指定されない場合、ネットワーク全体に対して SSO 機能が適用されます。
マスクの区切りにはセミコロンを使用します。例: (64.233.187.99/8; 72.14.0.0/16)
範囲を指定する場合はダッシュを使用します。例: (64.233.167-204.99/32)
すべてのネットワーク マスクは CIDR で終わる必要があります。 [詳細](#)

※以上でシングルサインオンの設定は完了になります。

7. シングルサインオンの動作確認

シングルサインオンが正しく設定できた事を確認します。

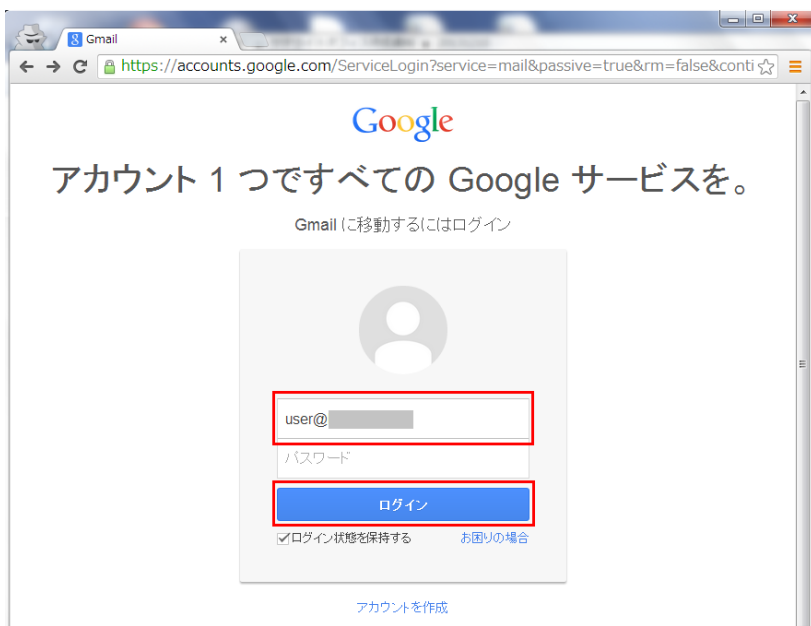
①ブラウザからGmailのURLにアクセスしてください。⇒mail.google.com



7. シングルサインオンの動作確認

②Googleのログイン画面が表示されるので、登録済みのユーザーでログインします。

ここではパスワードの入力は不要です。
IDを入力し、「ログイン」ボタンをクリックして下さい。



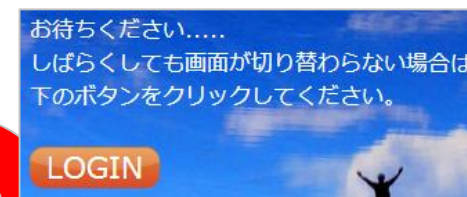
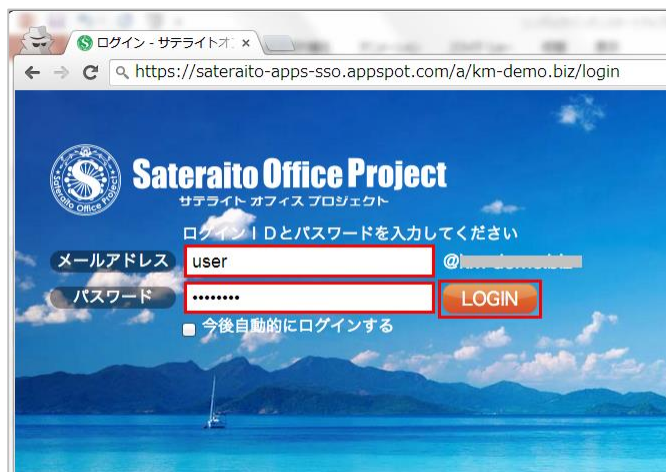
③Google Apps管理者コンソールで設定したログインページにリダイレクトされることを確認します。



7. シングルサインオンの動作確認

④IDとシングルサインオン管理コンソールで設定したSSOパスワードを入力して「LOGIN」をクリックして下さい。

⑤この画面を挟んで



⑥Gmailの画面にリダイレクトされる事を確認します。



8. 応用

シングルサインオン管理コンソールの「セキュリティルール管理」からプロフィールを追加・編集することで、細かなアクセス制御を行うことが可能です。

The screenshot shows the Sateraito Office Project management console. The main navigation bar includes: 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** (highlighted), タスク管理, and 外部システム連携管理. The left sidebar has: セキュリティルール管理, プロファイル一覧, **プロフィールの追加** (highlighted), ショートカット, アクセス申請一覧, and ログイン履歴一覧. The main content area is titled 'セキュリティルール管理' and contains a search box and a table of profiles:

プロフィールID	プロフィール名称
ADMIN01	管理者用プロフィール
DEFAULT01	一般ユーザ用標準プロフィール

A modal window titled 'プロフィール新規登録' is open, showing the following fields and settings:

- 基本情報**
 - プロフィールID * (例: PROFILE01 ※管理番号です。)
 - プロフィール名称 * (※このプロフィールを識別する分かりやすい名称を付けてください。(例: 管理者プロフィール, 全社標準プロフィール, xx部門プロフィール, パートプロフィール))
 - メモ
- ログイン・パスワードに関する設定**
 - ログインロック: 有効 無効 (回連続ログインに失敗したら [] の間ロック ※ログインロック設定は管理者に対しても適用されます。)
 - パスワード変更・再設定: ユーザによるパスワードの変更・再設定をさせない (基本はOFF) ユーザによるパスワードの変更や再設定をさせたくない場合はチェックしてください。
 - パスワード一元管理: パスワードの一元管理を有効にする (基本はOFF) ユーザによるパスワード変更時に本システムが保持するSSO/パスワードおよびGoogleApps自体のパスワードが同時に更新されます。 ※「GoogleApps/パスワード(連携用)」は更新されません。 ※ユーザ管理での管理者によるパスワード変更は個別に実施されます。
 - パスワード強度: 8 (文字以上) 半角数字 英字(大文字) 英字(小文字) 記号 が必要
 - パスワード有効期限: 設定なし (経過後、パスワード変更を強制) ※この設定はパスワード変更・再設定が有効の場合のみ利用されます。
 - パスワード履歴チェック: 設定なし (世代前までのパスワードをチェックし、同一パスワードへの変更をNGとする) ※この設定はユーザによるパスワード変更の際に適用されます。
- マイページに関する設定

Sateraito ~ for your best solution



BayTech Systems,
The Finest Solution
Company



サテライト オフィス
Sateraito Office



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2-2-4
マニユライフプレイス東陽町7F
TEL : 050-5835-0396 (代表)
FAX : 050-6861-2893
E-Mail : contact-info@sateraito.co.jp