



シングルサインオン(SSO)とは

WEBサービスの利用開始にあたり、ID・PWを『新規登録』する画面

このサービス用にID(メールアドレス)
とPWを新規登録する場合

ダウンロードユーザでログイン

メールアドレス

パスワード

[パスワードをお忘れですか?>](#)

ログイン

[新規登録](#)

既に使用中の下のサービスで新規登録
する場合(元サービスにログイン中の状態である事)
《**シングルサインオン:SSO**》



Appleでサインイン



Yahooでログイン



Googleでログイン



Facebookでログイン



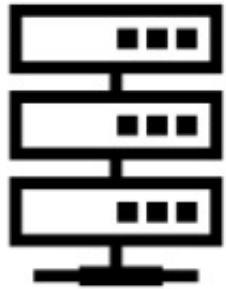
LINEでログイン



シングルサインオン(SSO)とは

WEBサービスの利用開始にあたり、**Googleでログイン** を利用した時

Google



初回認証時にGoogleが所有する以下のユーザー情報をWebサービス側に提供

- ・名前
- ・メールアドレス
- ・プロフィール写真

※SSOの利用解除後もWebサービス側に残る

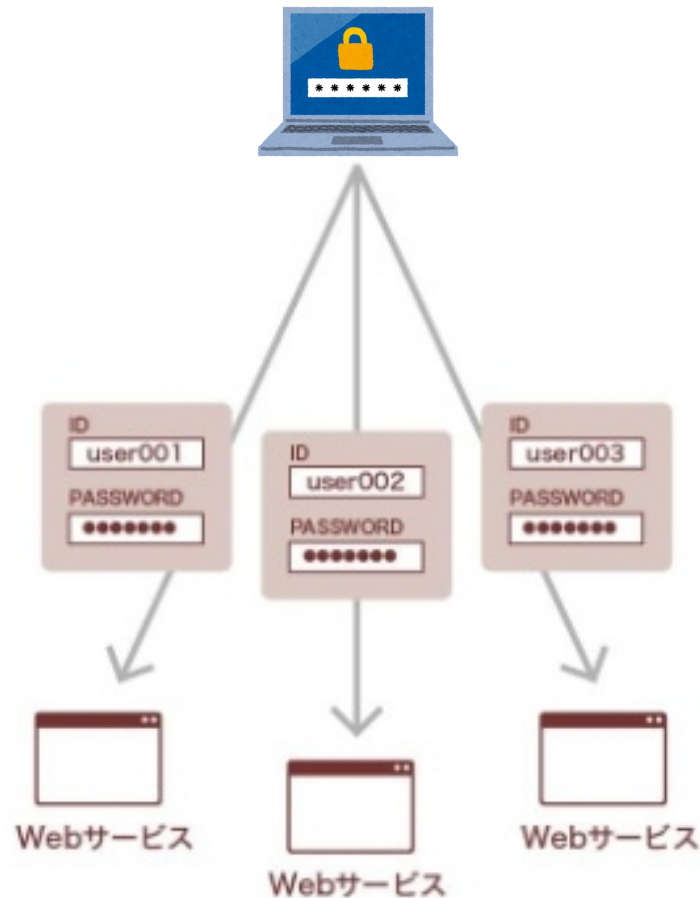
アクセスしたいWebサービス



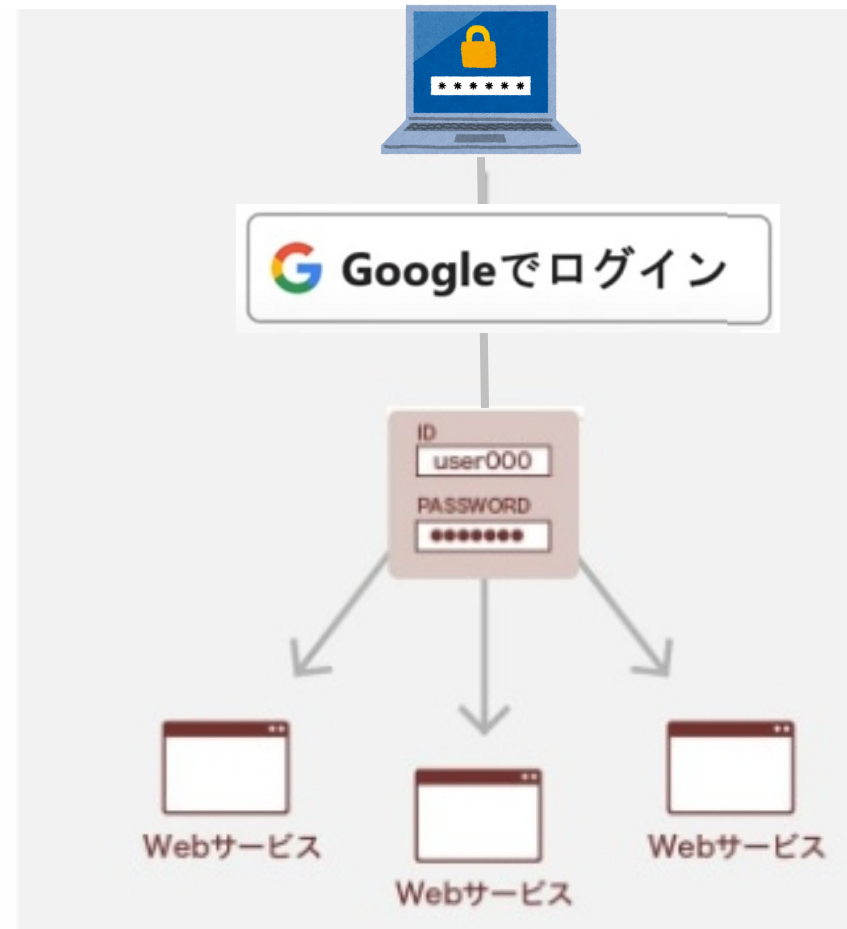


シングルサインオン(SSO)とは

従来の方式で「サインイン」すると
個々のID/PW登録して、それを使用
してサインインする



SSO方式で例えばGoogleにサインイン
しておけば、SSOでサインインするとした
Webサービスいずれにもサインインが可能





シングルサインオン(SSO)とは

メリット

1. 利用Webサービス毎に、いくつものパスワードを作成しなくてよい。
またSSO元の(例えばGoogle用のパスワード) が、あちらこちらに分散されない。
2. しっかりとしたGoogle側のセキュリティ管理下で、PW等が保管・管理される。

デメリット

1. しっかりとしたGoogle側のセキュリティ管理下で、PW等が保管・管理されるとは言っても、これが破られたら、SSOで利用するWebサービスが全てセキュリティ突破される。



シングルサインオン(SSO)とは

SSO利用時の注意事項

1. SSO元となるPWは、他のPWとは変える事。(使い回しのPWでないこと)
2. SSO元となるPWは、複雑で長いPW構成とすること
※ただし忘れない、覚えておけるPWが望ましい
3. SSO元が推奨するセキュリティ対策を実行しておくこと。
※例えばGoogleでは「携帯電話番号の登録」「二段階認証の実施」
4. SSOで始めたWebサービス、SSOの利用を解除することができる。ただし今までのWebサービス側のデータにはアクセス、利用出来なくなる。
また、SSO元から提供された「名前」「メールアドレス」「プロフィール写真」(※Googleの例) が、Webサービス側に残ったままとなる。



インターネットのパスワード管理

	ID/PWを忘れる のでは	ID/PWを盗まれる のでは	ID/PWを 盗まれたら	
解決策	ID/PWを シンプル・ 使いまわし	ID/PWを紙等 に書き留めておく ブラウザ(例)Edge Chrome のID/PW保存機能 を利用 ID/PW自動入力	シングルサインオン SSO を利用する 例)「Google でログイン」 ※現在は全てのサイトで 利用できないため 従来の方と併用	「二段階認証」※ を利用し、『自分 以外』アクセス を却下する ※携帯SMSに認証 コードが届く 指紋認証・顔認証等の 『パスキー』方式を 利用
次の 心配事	パソコン・スマホの紛失		認証デバイスが無い	
	セキュリティ管理の低い サイトからID/PWの流失		セキュリティ事故で ID/PWが流出	
	フィッシングサイトからID/PWが流失 ・ ハッカーがPWを盗む			