『クラウド時代のID管理』
～ Unicorn ID Manager 紹介 ～

OSSTech

オープンソース・ソリューション・テクノロジ株式会社
2009/11/20
技術取締役 武田 保真

目次

- クラウドサービスのID管理
- Google Appsと既存サービスのID管理連携
- Unicorn ID Managerの紹介

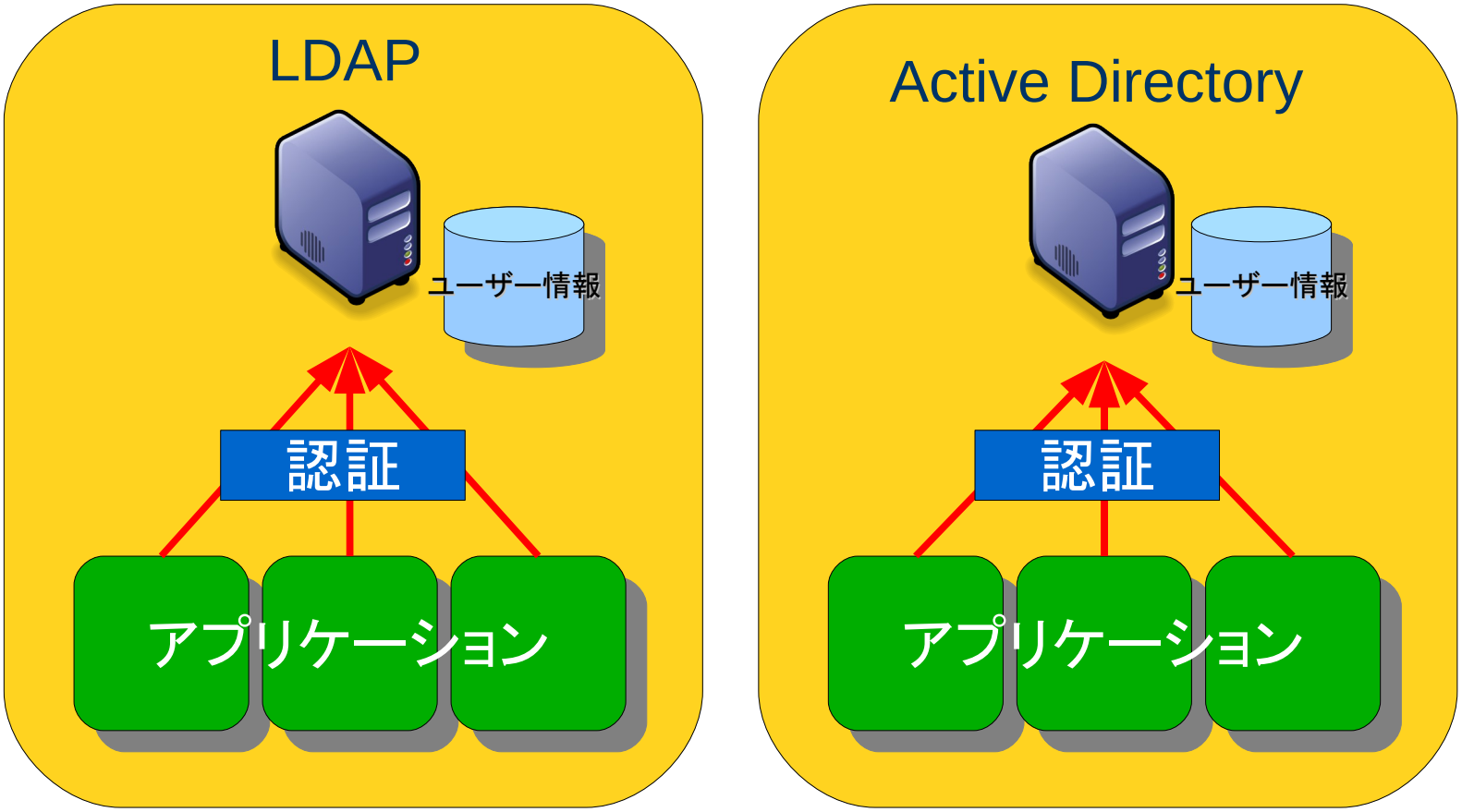
講師紹介

- 武田 保真 (TAKEDA Yasuma)
  - 2001年 ～ Linuxディストリビューションの開発･保守
  - 2006年 ～ オープンソース･ソリューション･テクノロジ設立
    - Samba、LDAP、Google Appsなどの認証統合を中心に開発、構築など
- LPIC 301/302保有
- 著書
  - 「Samba 逆引きリファレンス(秀和システム)」
  - 「徹底解説 Samba LDAPサーバー構築(技術評論社)」
  - 「逆引きUNIXコマンドリファレンス(技術評論社)」など

クラウドサービスのID管理

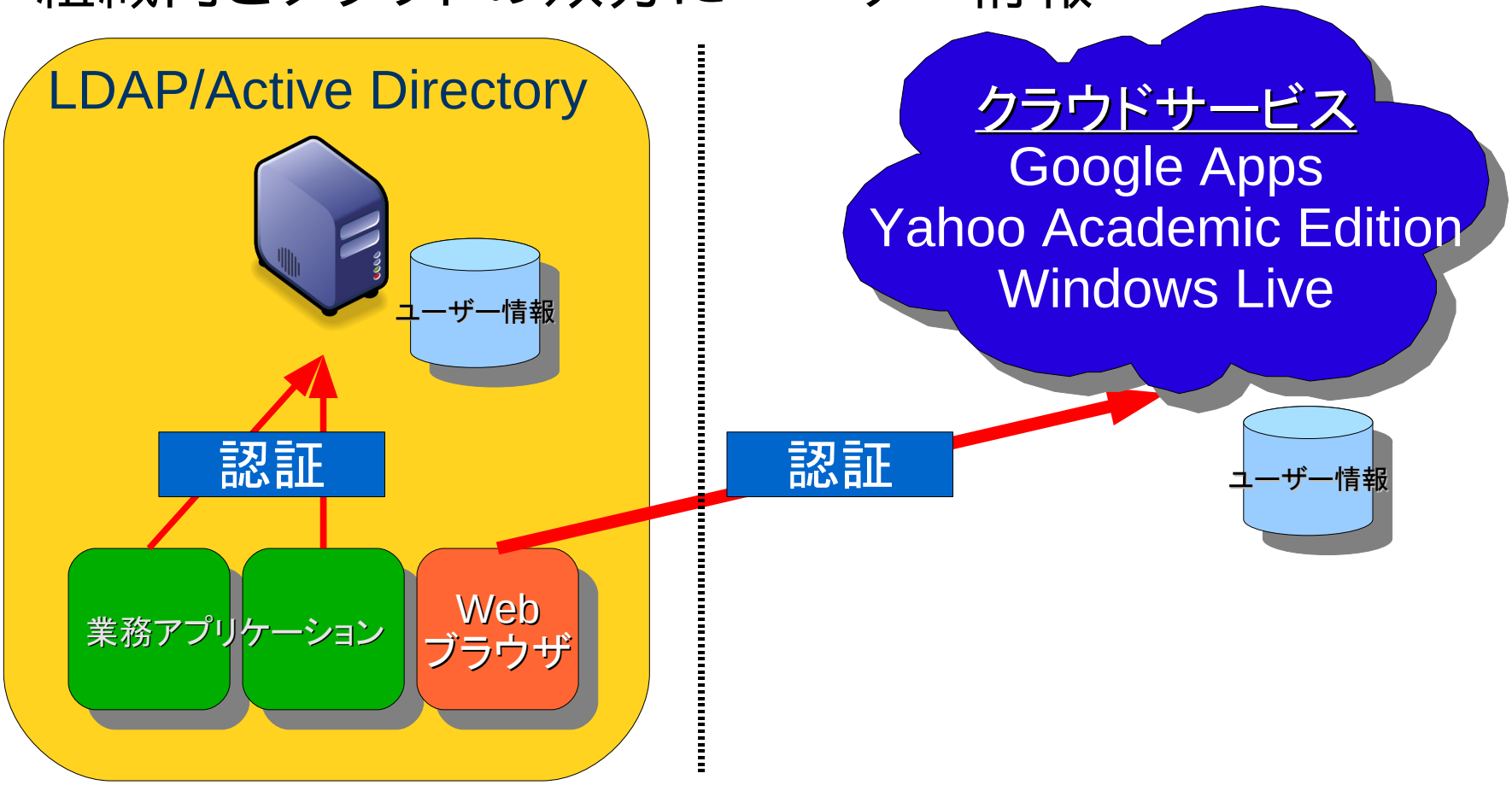
「クラウド」以前のID管理

- 組織内のユーザー・グループ管理



クラウドサービスとのID管理連携

- 組織内とクラウドの双方にユーザー情報

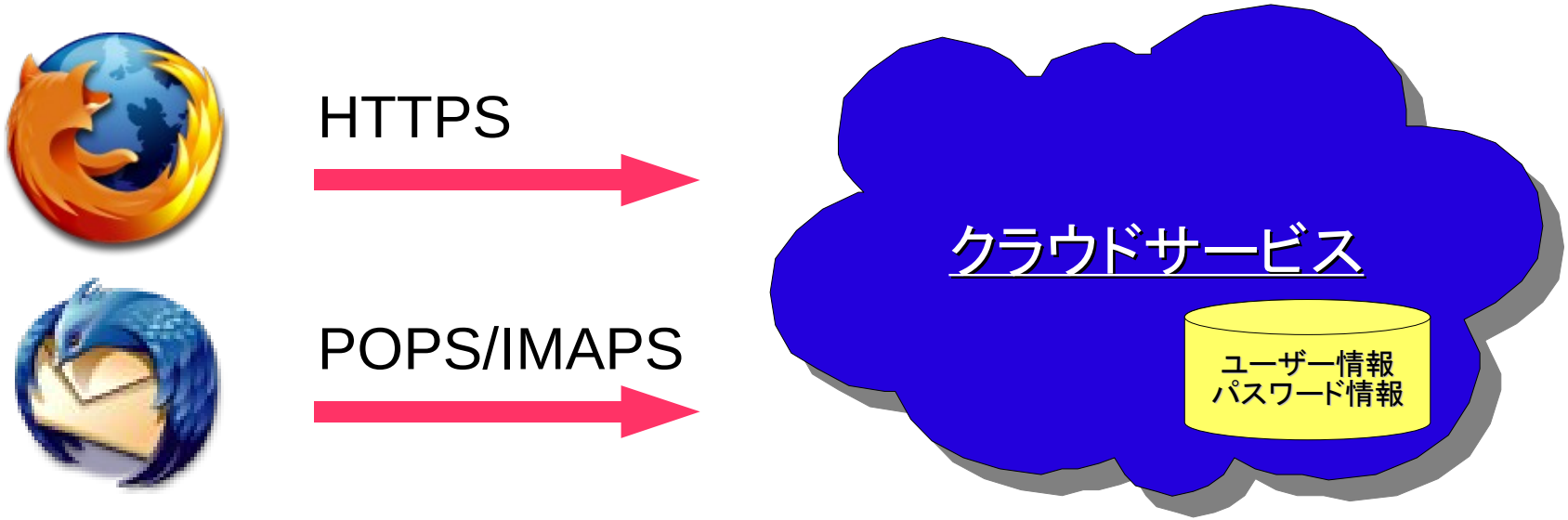


クラウドサービスでのユーザー認証

- 内部認証
  - ユーザー情報、パスワードをクラウドサービス内にて保管
- SAML
  - ユーザー情報のみ保管し、パスワードは組織内のLDAPサーバー/Active Directoryなどに保存。組織で管理されているユーザー情報をSAMLプロトコルで認証。
- OpenID
  - OpenID対応サイトにユーザー情報、パスワードを保存。OpenIDサイトで管理されているユーザー情報を使ってOpenIDプロトコルで認証。

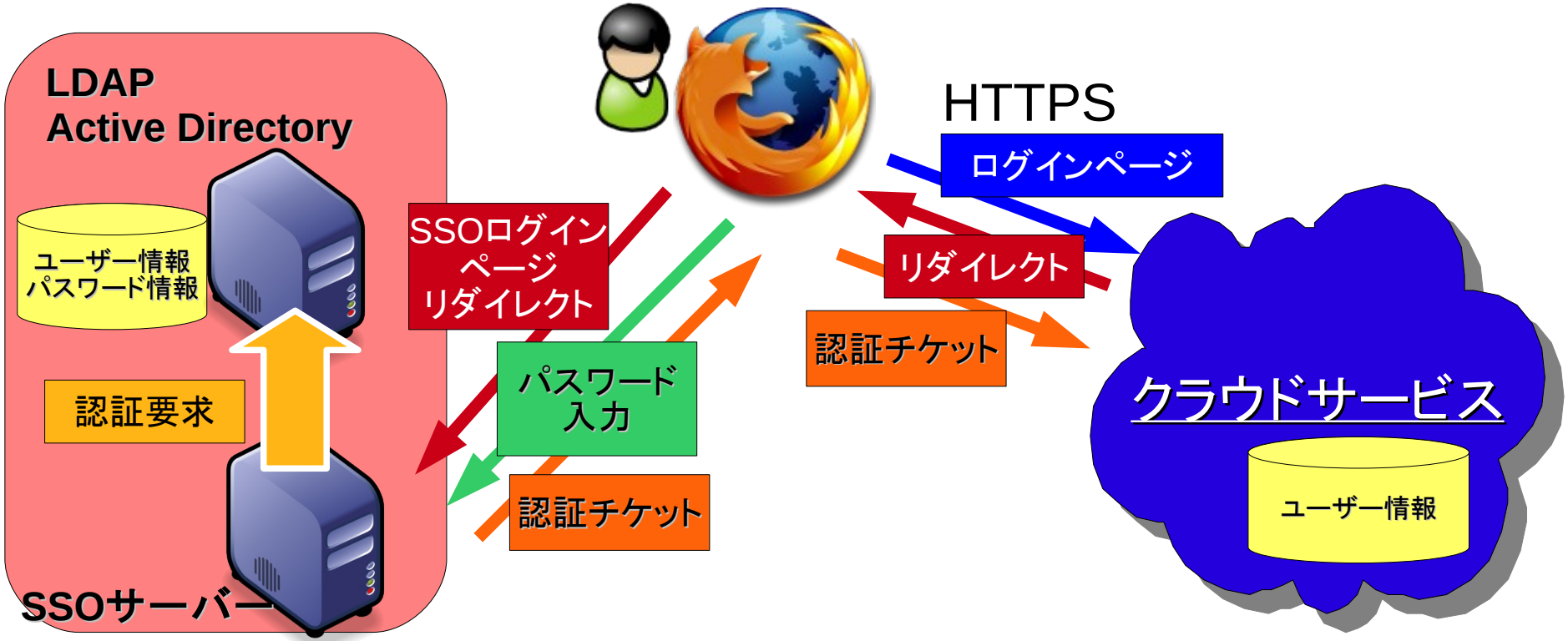
クラウドサービスの内部認証

- Webサービス以外のサービスに対してもユーザー認証可能
- パスワード情報をサービスプロバイダに格納



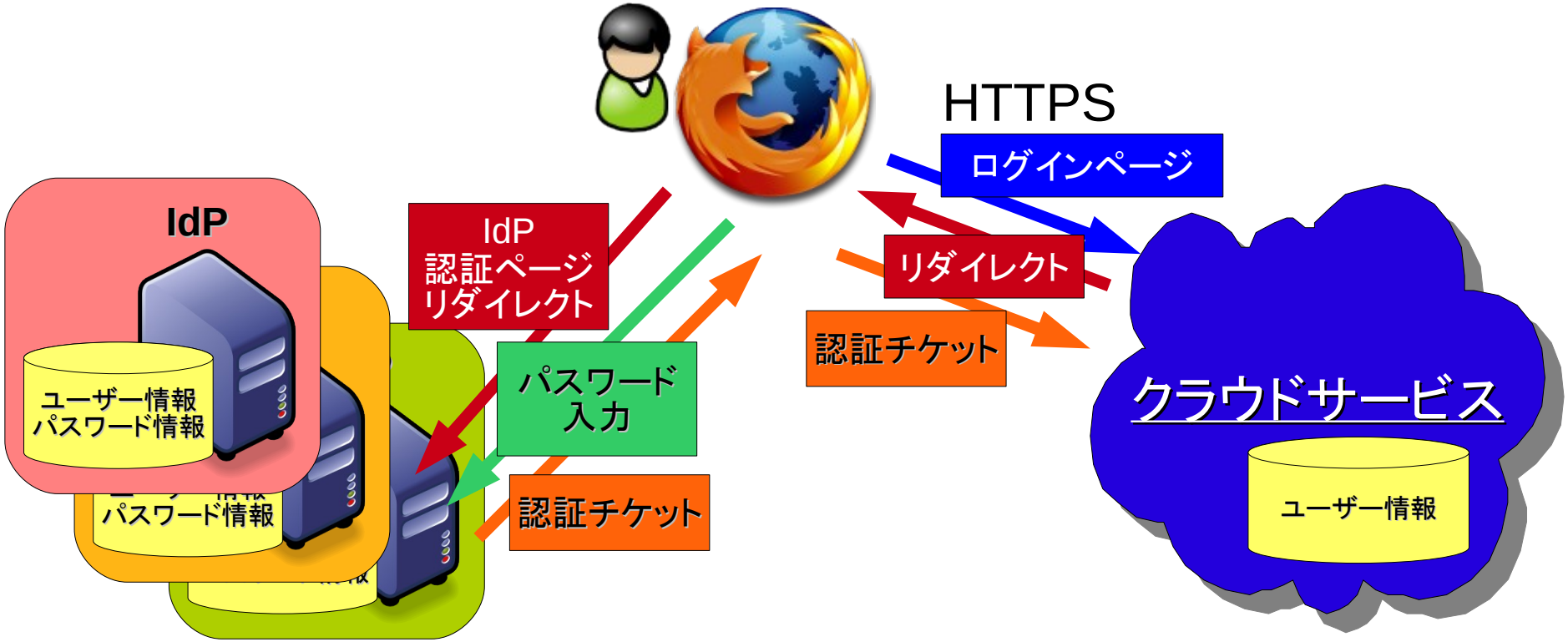
SAMLのユーザー認証

- Webサービスのみ認証可能
- 認証先は単一のURLで指定(ユーザー情報の集中管理)
- パスワード情報を組織内部のサーバーに格納



OpenIDのユーザー認証

- Webサービスのみ認証可能
- ユーザー・パスワード情報をIdentity Provider(IdP)に格納
- 認証に利用するIdPをユーザーが選択可能(分散認証)



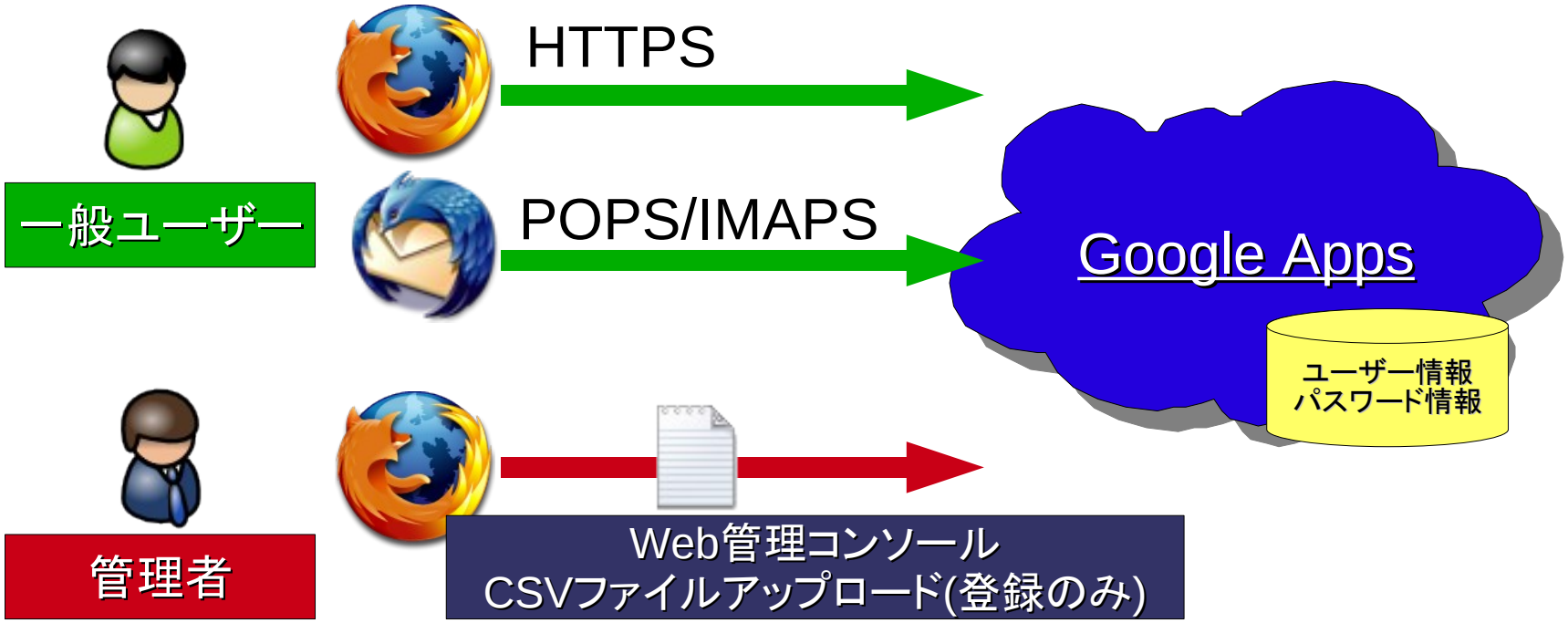
Google Appsと既存サービスのID連携

Google AppsでのID管理

- 内部認証
  - ユーザー情報、パスワード情報をGoogle Appsに登録
  - GmailのPOPS/IMAPS認証、Googleトークの認証も可能
- SSO(シングル・サイン・オン)
  - ユーザー情報のみGoogle Appsに登録
  - 認証はSAMLにより、組織内のLDAP/Active Directoryで実施
  - POPS/IMAPS、Googleトークを利用するためには、別途Google Appsにパスワードを登録

システム構成例(内部認証)

- ユーザー、パスワード情報をGoogle Appsに登録
  - ユーザー登録のみCSVファイルで一括登録可能
  - ユーザー削除などはチェックボックスで手動処理



ID管理の必要性

Google Appsの管理コンソールだけでは、多数のユーザー管理作業は現実的ではない

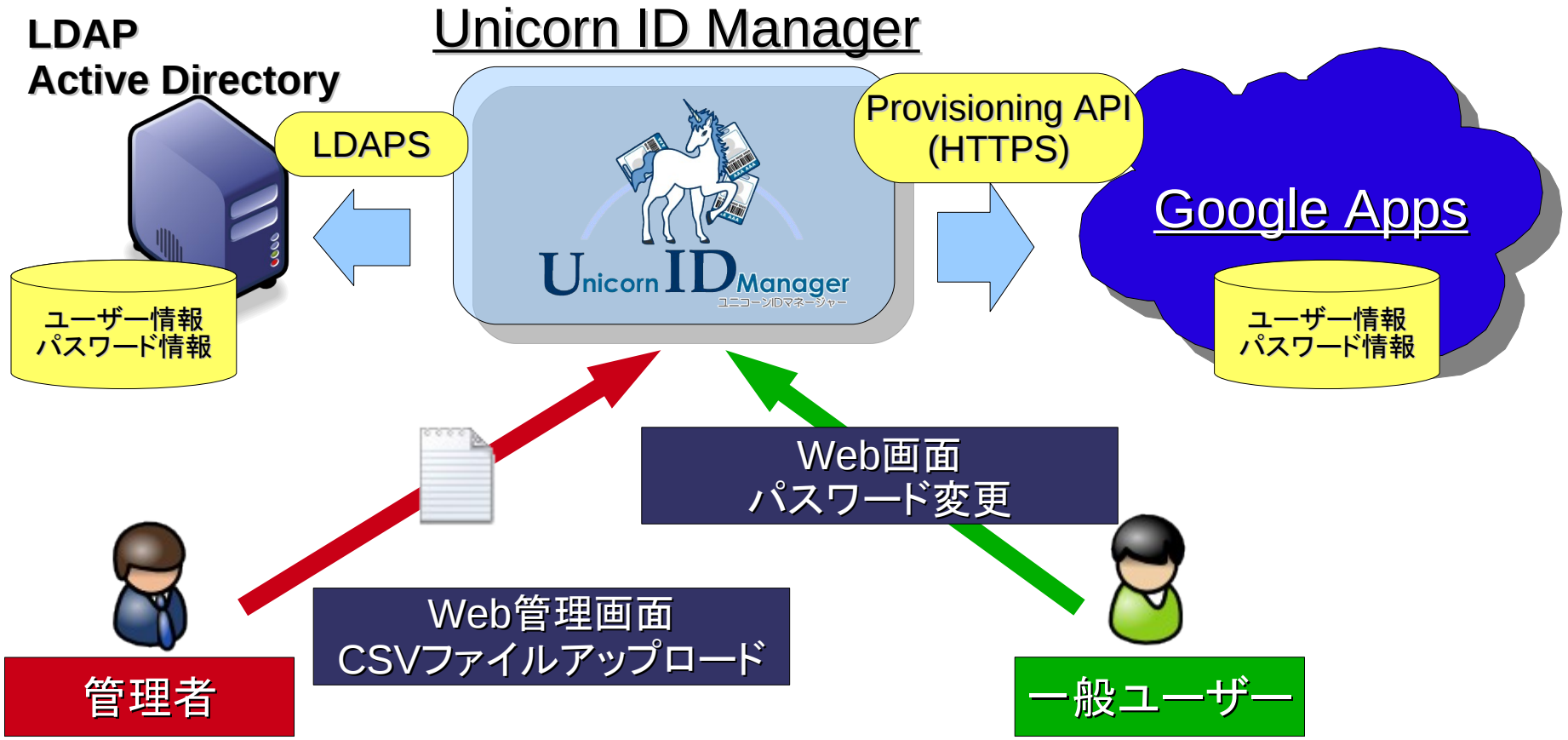
Google Appsと組織内のLDAP/Active Directoryを別々にユーザー管理することは間違いのもと

ユーザーにとって、Google AppsもLDAP/Active Directoryも同じパスワードとして利用したい

ID管理製品の導入

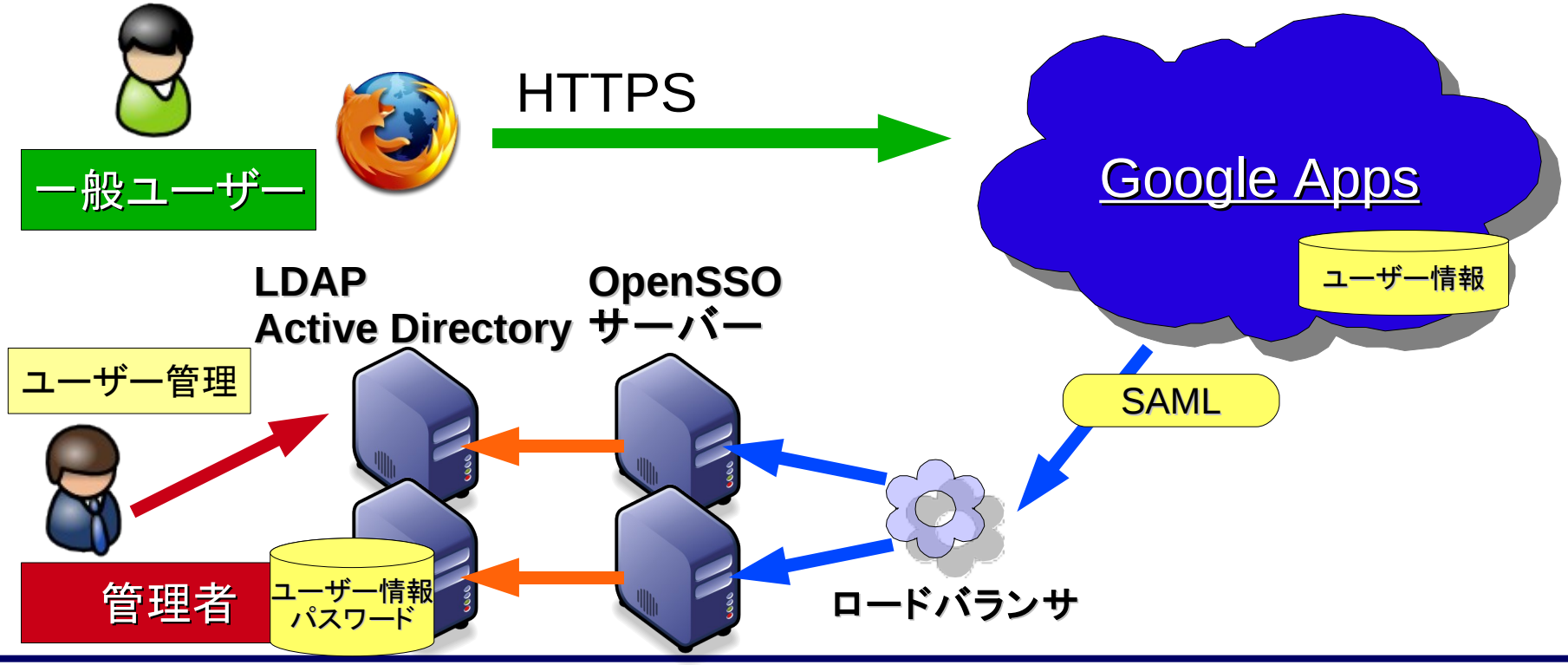
システム構成例(ID管理構成)

- Google提供のProvisioning APIによるユーザー情報の同期



システム構成例(SSO)

- ユーザー、パスワード情報をLDAP/ADに登録
- ユーザー情報をGoogle Appsに登録
- 認証サーバーの冗長化必須



ID管理製品の特徴

- メタ･ディレクトリ連携
  - ID管理用のメタ･ディレクトリサーバーを中継して、アカウント情報の同期
    - 厳密なID管理を実現
    - 同期方法
      - 自動同期
      - 管理者のアクションをトリガーとして同期
- 直接連携
  - 管理者のアクションをトリガーとして直接アカウント情報を同期
    - 管理作業工数の低減

Google AppsとID管理製品連携時の注意

- Active Directory連携
  - 自動同期方式の場合、ADからパスワード情報が取り出せないため、必ずSSO構成にする必要がある
- OpenLDAP連携
  - パスワードのハッシュ方式がSHA、MD5、CLEARTEXTのいずれかであれば、LDAPに登録されているパスワードをそのままGoogle Appsに登録可能
    - OpenLDAPのデフォルトはSSHA
- Google Appsではパスワードの最小文字数は8文字以上を推奨

Unicorn ID Manager紹介

Unicorn ID Manager概要

- OpenLDAP、Active Directory、Samba、Google AppsのID統合管理を実現
- Web管理画面でユーザー統合管理
- CSVアップロードによるユーザー一括操作
- パスワード変更用 Webサービス提供
- OSSのみで実現
- Google Apps Education Edition向け機能組み込み
- 動作環境
  - RedHat Enterprise Linux 5 / Cent OS 5 / Solaris10

Unicorn ID Manager機能概要

- ユーザー管理機能
  - 登録、削除、更新、有効化(ログイン許可)、無効化(ログイン禁止)
  - パスワード強制変更
  - ユーザー一覧取得(OpenLDAP、Active Directory、Google Apps)
- パスワード変更Web提供

管理画面

- 管理画面
  - 複数の管理対象を設定し、選択可能
  - 管理者の認証をLDAPやActive Directoryで実施可能

CSV一括管理機能

- Excel、OpenOfficeなどで作成したCSVのアップロード
  - シフトJIS、UTF-8のCSVファイルに対応
- 一括処理後に、スクリプトの実行可能
- Active Directoryユーザー登録時にホームディレクトリの作成可能
- ユーザー登録時、更新時にLDAP/Active Directoryに対して利用可能な属性をカスタマイズ可能
- Google Appsへの登録はバックグラウンド実行
  - 1ユーザー登録に5秒程度かかるため

CSV一括操作

- CSVファイルのアップロード

パスワード同期機能

- OpenLDAP、Active Directory、Samba、Google Appsのパスワードを一括変更可能

ユーザー情報取得機能

- OpenLDAP、Active Directory、Google Appsの全ユーザー情報取得
- HTML表示、CSVダウンロードが可能

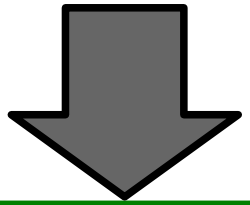
操作結果確認

- 操作結果表示
  - サマリ表示、詳細表示

教育機関向け機能

- 卒業生アカウント移行機能
  - Google Appsでは、「卒業生」に対して広告を表示しなければいけないため、「在学生」と「卒業生」を別ドメイン運用することが多い

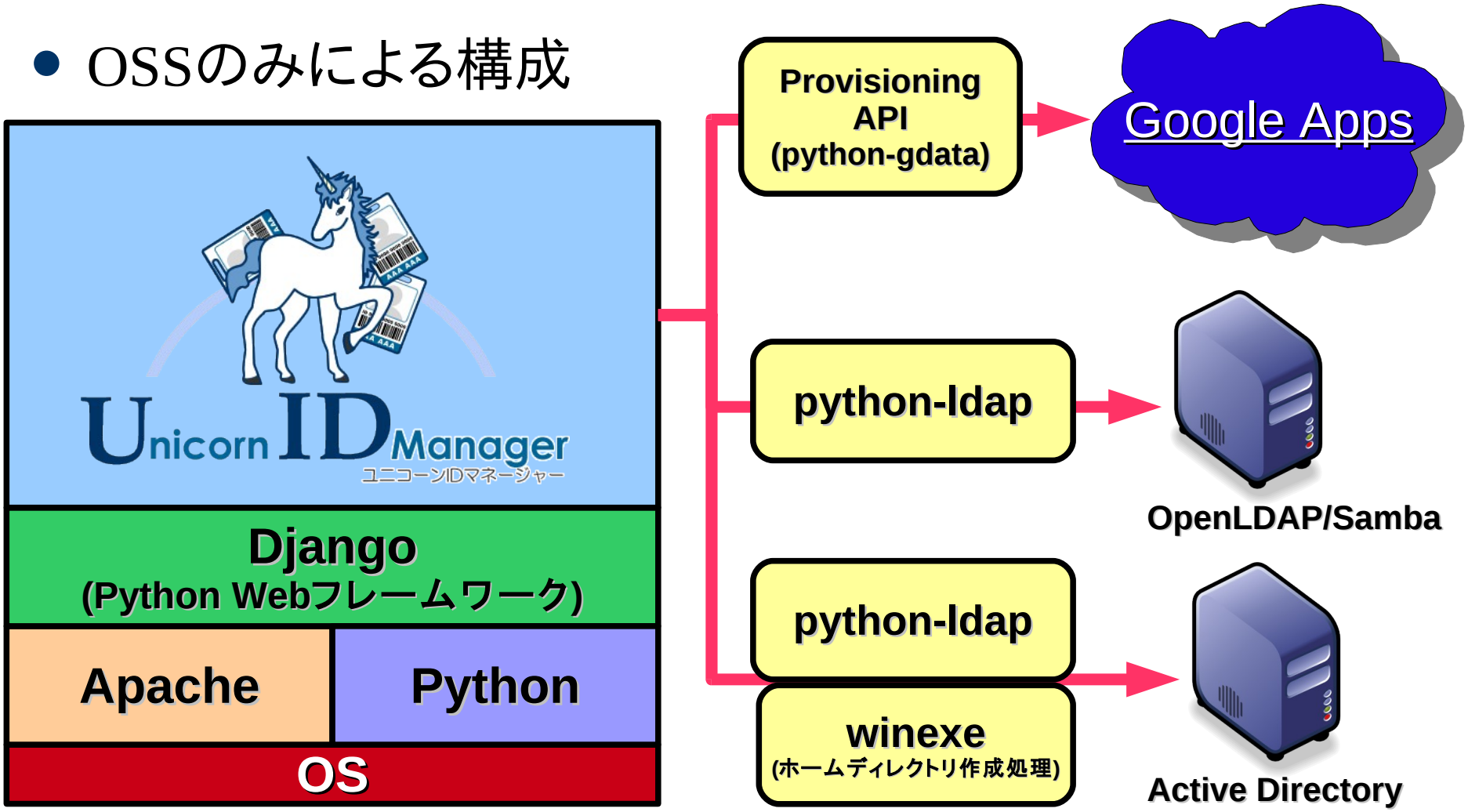
学生が卒業するタイミングで該当アカウントを卒業生ドメインに一括移行する作業が必要



Unicorn IDM で一括移行処理
メールスプール移行用のCSVファイルの生成

Unicorn ID Manager構成

- OSSのみによる構成



まとめ

- クラウドサービスの認証方法
  - 内部認証、SAML、OpenID
- ユーザー統合管理の必要性
  - クラウドサービスと既存ユーザー情報の連携管理
  - Google Apps利用時のシステム構成・注意事項
- OSSTechのID管理製品
  - Unicorn ID Managerの紹介