Unicorn ID Manager Ver.3

ユニコーンIDマネージャー

～クラウド時代のID連携を支援する～

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ info@osstech.co.jp

クラウド時代のID管理

1. 管理対象の分散化
   - オンプレミスとクラウドサービスの混在
   - システムごとのID管理
2. ID管理工数の増加
   - システムごとの個別ID管理操作
3. 適切なID管理の不徹底
   - 個別管理による操作漏れ
   - 複数システム間のID情報の不整合

ID統合管理の必要性

クラウド時代のID管理 (2)

4. 既存ID管理システムとの統合

- 既存システム に クラウドサービスを追加

5. WebアプリとのID管理統合

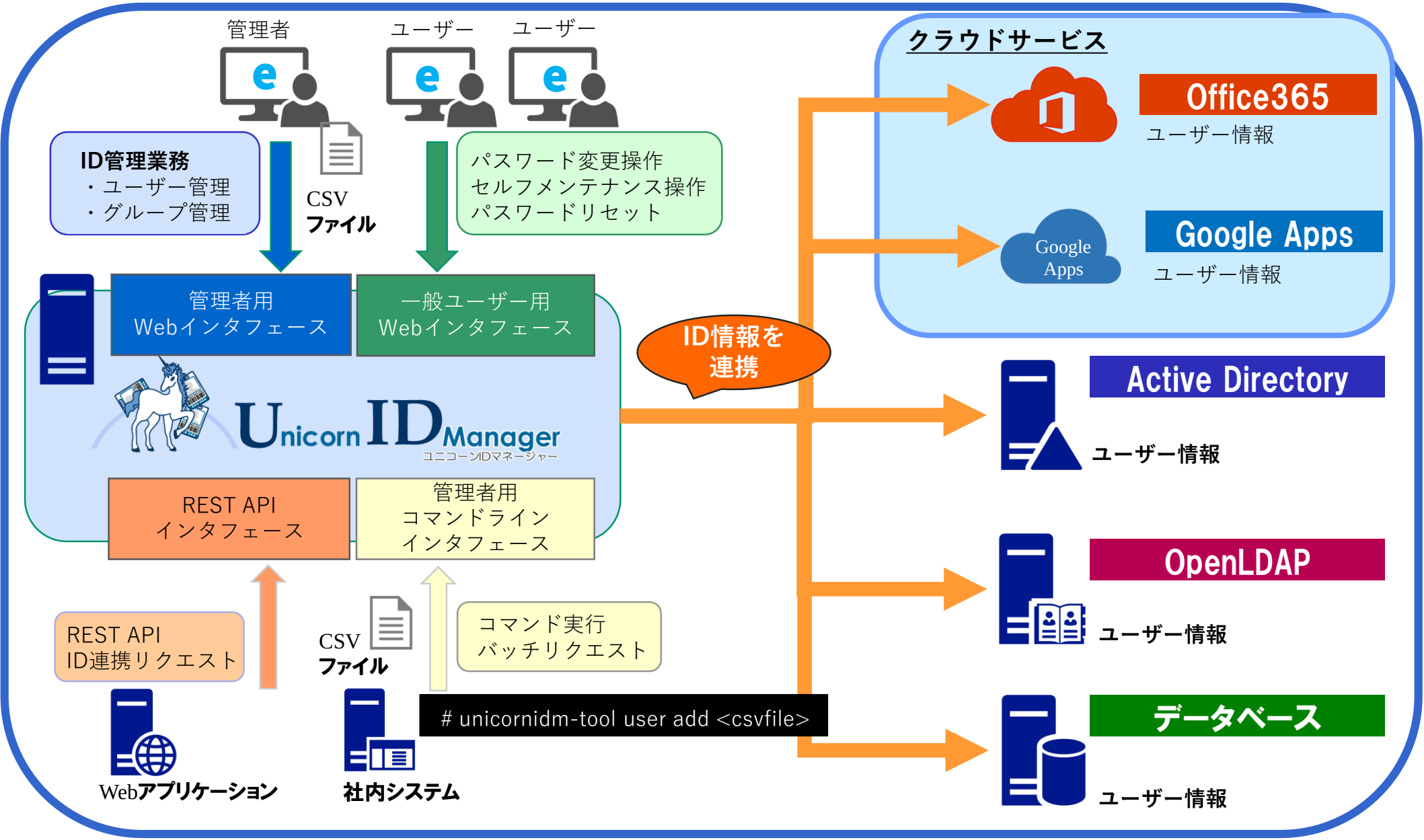
- Webアプリと親和性の高いID連携方式の必要性

ID連携の必要性

Unicorn ID Manager 概要

- 統合ID管理 & ID連携製品
  - 複数システムのID管理操作を統合
    - LDAP、Active Directory(Samba4)
    - Office365、Google Apps
    - RDBMS(MySQL、MariaDB、PostgreSQL)
  - メタディレクトリを持たず、ID連携操作のみを連携
    - 連携設定・連携項目の設定のみで利用可能
    - 各連携先をマスターデータとして処理
    - 各連携先で直接操作を行っても問題無し

Unicorn ID Manager 概要図



操作インタフェース

- 管理者用インタフェース
  - Webインタフェース
    - CSV一括操作、Webページ上の個別操作
  - コマンドインタフェース (CSVファイル)
  - SCIM対応 REST API (JSON)
- 一般ユーザー用 Webインタフェース
  - パスワード変更・パスワードリセットページ
  - セルフメンテナンス

製品価格体系

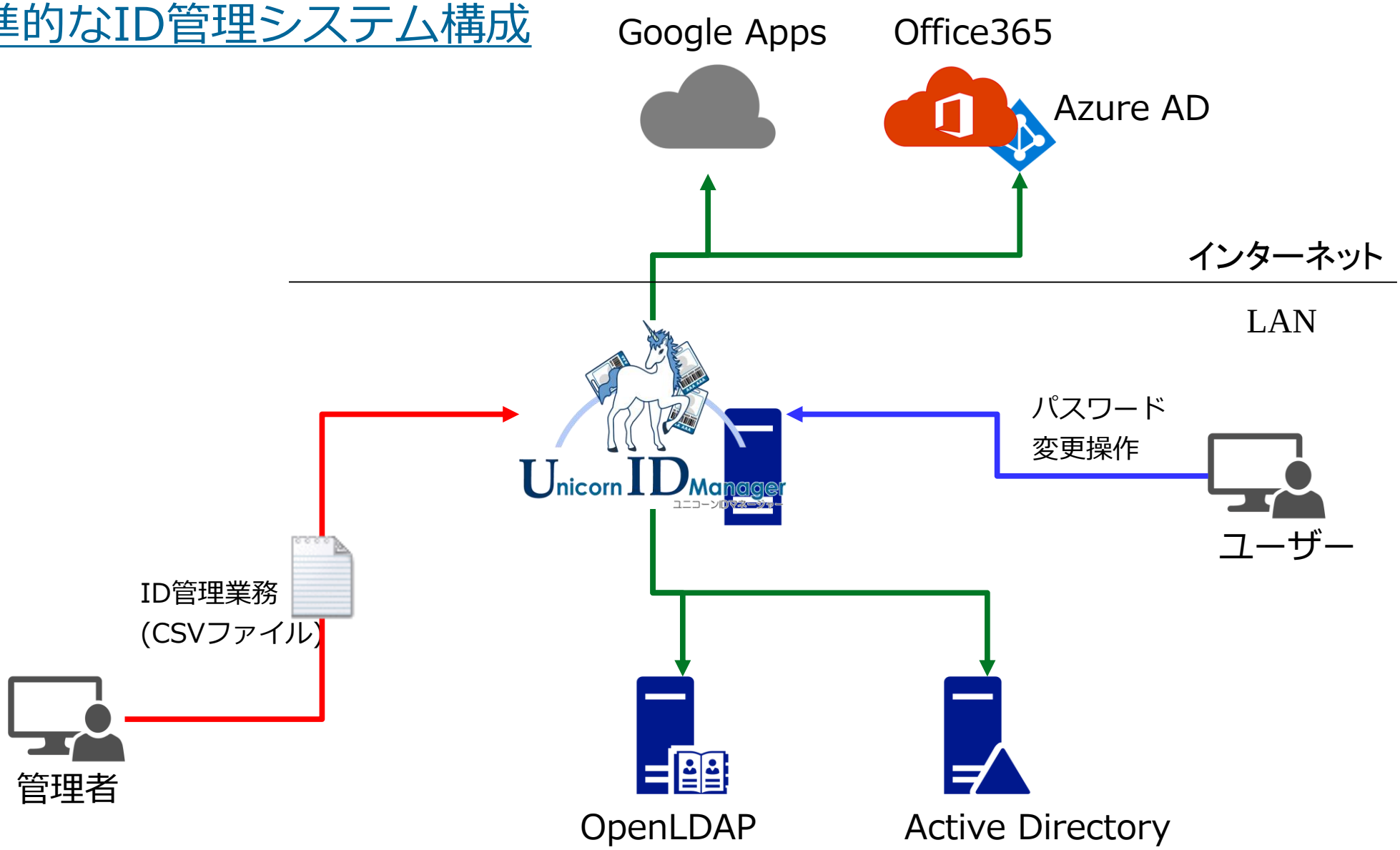
製品	1ノード：60万円(税抜) ＊ 永続ライセンス
保守	1システム: 24万円 / 年 ＊ アップデート版の提供含む

動作環境

- 対応OS
  - Red Hat Enterprise Linux 7 / CentOS 7 (x86-64) 以降
  - ハードウェア要件
    - Intel Xeon CPU　2core以上
    - メモリ　4GB以上
    - ディスク　20GB以上(OS領域含む)
- 対応Webブラウザ
  - Microsoft Internet Explorer 11 / Edge
  - Google Chrome
  - Firefox
  - Safari

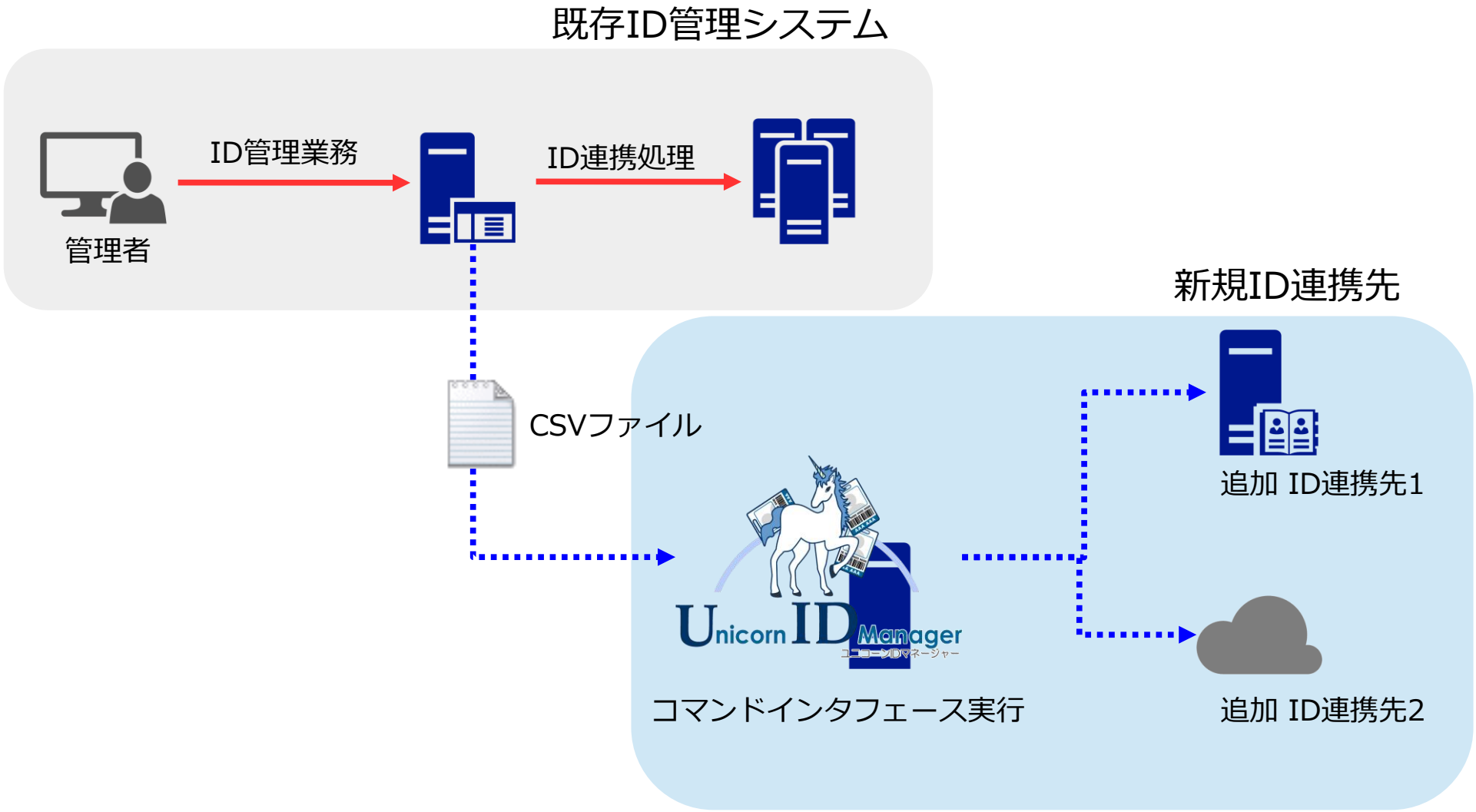
システム構成例

標準的なID管理システム構成



システム構成例2

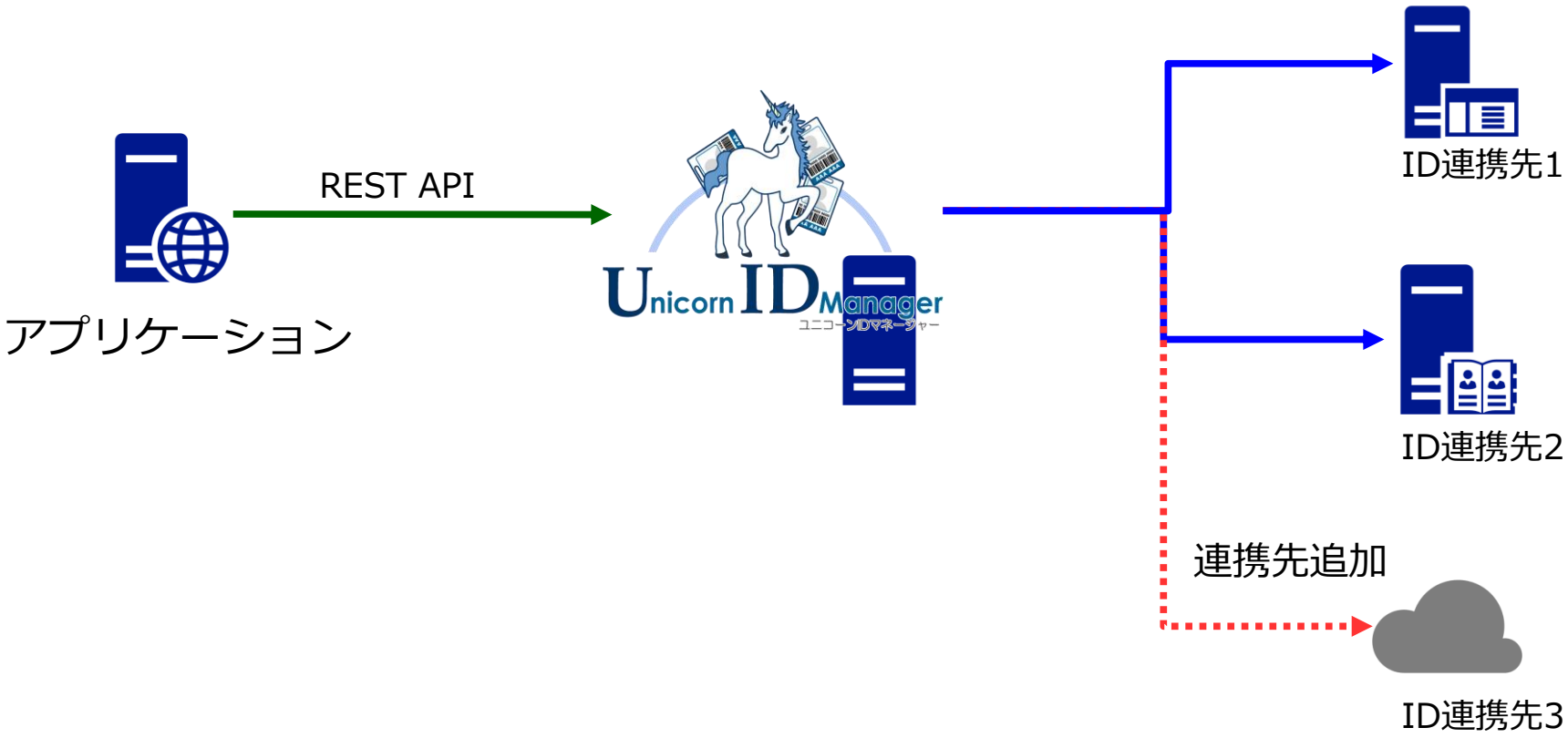
既存ID管理システムと統合



システム構成例3

ID管理APIの共通化に利用

- 連携先が追加されても同じAPIでID管理の連携が可能



システム構成例4

ID連携プロトコル変換コネクタ

- Webアプリケーション開発者になじみ深いREST APIでLDAPやActive Directoryサーバーのユーザー連携処理の実装を支援

機能概要 - 管理者 組織選択画面 -

- 複数の連携先の組み合わせ
  - 連携先の組み合わせ(ターゲット)を複数設定可能
    - 「ターゲット1」
      - LDAP、Active Directory、Google Apps
    - 「ターゲット2」
      - LDAP、Office365

機能概要 - ユーザー管理機能 -

- パスワード管理関連機能
  - 任意のユーザーのパスワードリセット
  - パスワードポリシーの適用
  - ランダムパスワード生成
- スキーマ拡張対応
  - LDAP、Active Directoryのスキーマ拡張対応
- 連携スクリプト
  - アカウント操作時にシェルスクリプト実行

機能概要 - 管理者 操作画面 -

- 管理者によるID管理操作
  - ユーザー管理操作
    - 登録、更新、削除、有効化、無効化、パスワード変更
    - ランダムパスワードの自動生成
    - 操作時に連携対象の選択可能
  - ユーザー一覧表示・取得
  - グループ管理
    - グループ登録・削除・メンバー管理

機能概要 - 一般ユーザー向け -

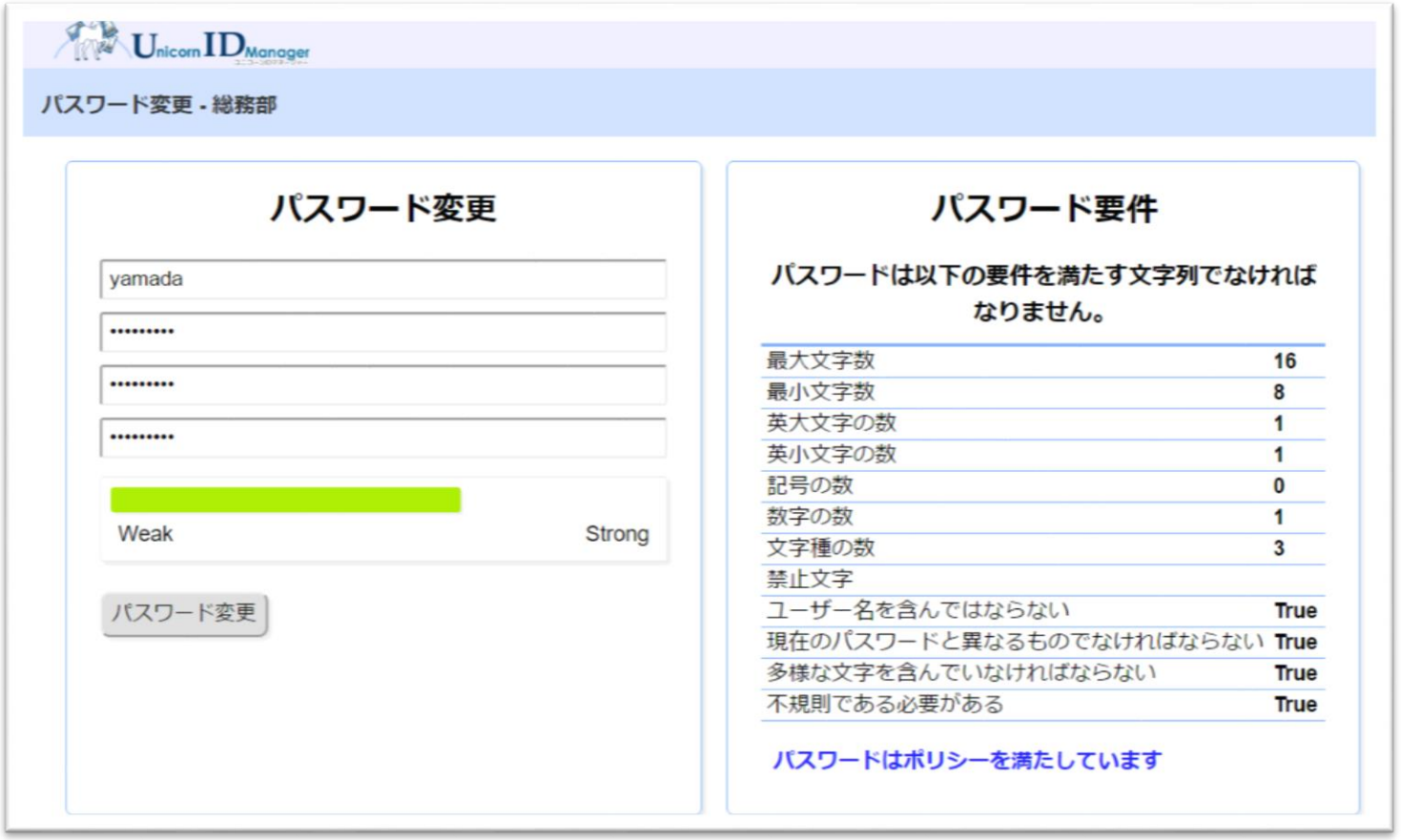
- 一般ユーザー向け機能
  - パスワード変更
  - パスワードリセット
  - セルフメンテナンス

機能詳細 - パスワード変更画面 -

- ユーザー向けパスワード変更画面
  - 連携先のパスワードを一括変更
  - パスワードの複雑性による制約
    - 文字数、複雑性、禁止文字など
  - パスワードの強度判定
    - ステータスバーで入力した新しいパスワードの強度を判定
  - パスワード変更の注意書きの文面を設定可能
    - デフォルトでは複雑性の条件を表示。代わりに利用者向けの注意事項の文章を表示設定が可能

パスワード変更画面

- パスワードポリシーの強制・強度判定
- 任意の説明文の設定可能



ユーザー情報 セルフメンテナンス

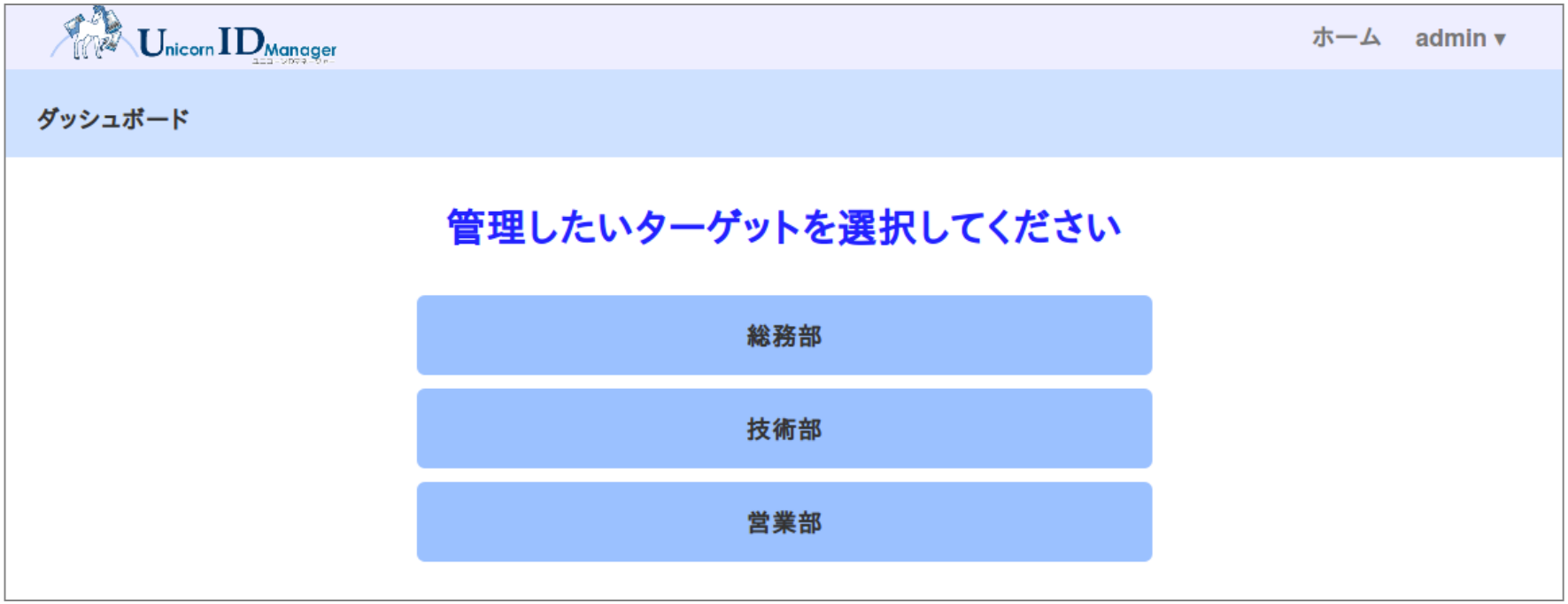
- ユーザー自身で自分の情報の変更が可能
- 変更可能な項目は初期設定で設定

ユーザーパスワードリセット

- ユーザー自身でパスワードのリセット
- メールによるパスワード変更リンクの通知
- 事前登録済みメールアドレスのみ有効
- パスワード変更リンクは一定期間のみ有効

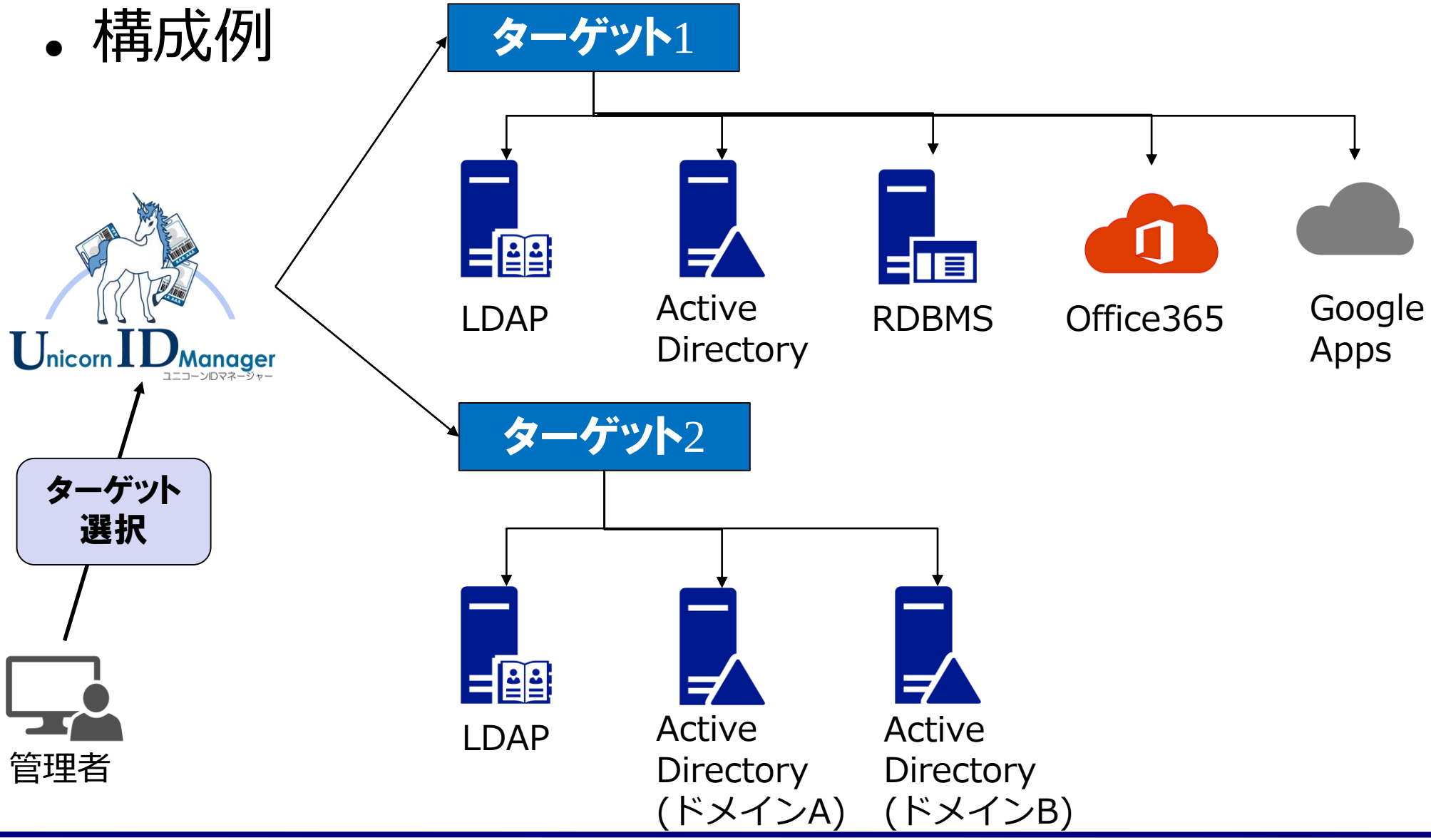
管理画面 - ターゲット選択 -

- 1台のUIDMサーバに 複数のターゲットの設定
- 1つのターゲットに複数のID連携先を登録
- ターゲットごとに連携項目を定義



管理画面 - ターゲット構成例 -

- 構成例



管理画面 - 連携項目のマッピング -

- 項目マッピングを設定

入力項目

userName: yamada
姓: **山田**
名: **太郎**
氏名: **山田 太郎**
mail: yamada@example.com
UID**番号**: 2001
GID**番号**: 3000
UNIX**ホーム**: /home/yamada
Win**ホーム**: ¥¥server¥home¥yamada

LDAP**登録内容**

uid: yamada
sn: **山田**
givenName: **太郎**
mail: yamada@example.com
uidNumber: 2001
gidNumber: 3000
homeDirectory: /home/yamada

Active Directory**登録内容**

uid: yamada
sn: **山田**
givenName: **太郎**
mail: yamada@example.com
homeDirectory: ¥¥server¥home¥yamada

機能概要 - 管理者　ユーザー一覧 -

- 各連携先のユーザー一覧情報を統合出力
- CSV形式の一覧ファイルダウンロード
- ユーザー検索機能 (一覧に含まれる項目で検索可能)

userName	姓	名	LDAP	ActiveDirectory
Administrator				存在
Guest				存在(無効状態)
akamine	赤嶺	玲子	存在	存在
hasebe	長谷部	忠詞	存在	存在
hasegawa	長谷川	祐樹	存在	存在
kojima	小島	詩織	存在	存在
krbtgt				存在(無効状態)
mimura	三村	誠	存在	存在

機能詳細 - 管理者　1ユーザー登録 -

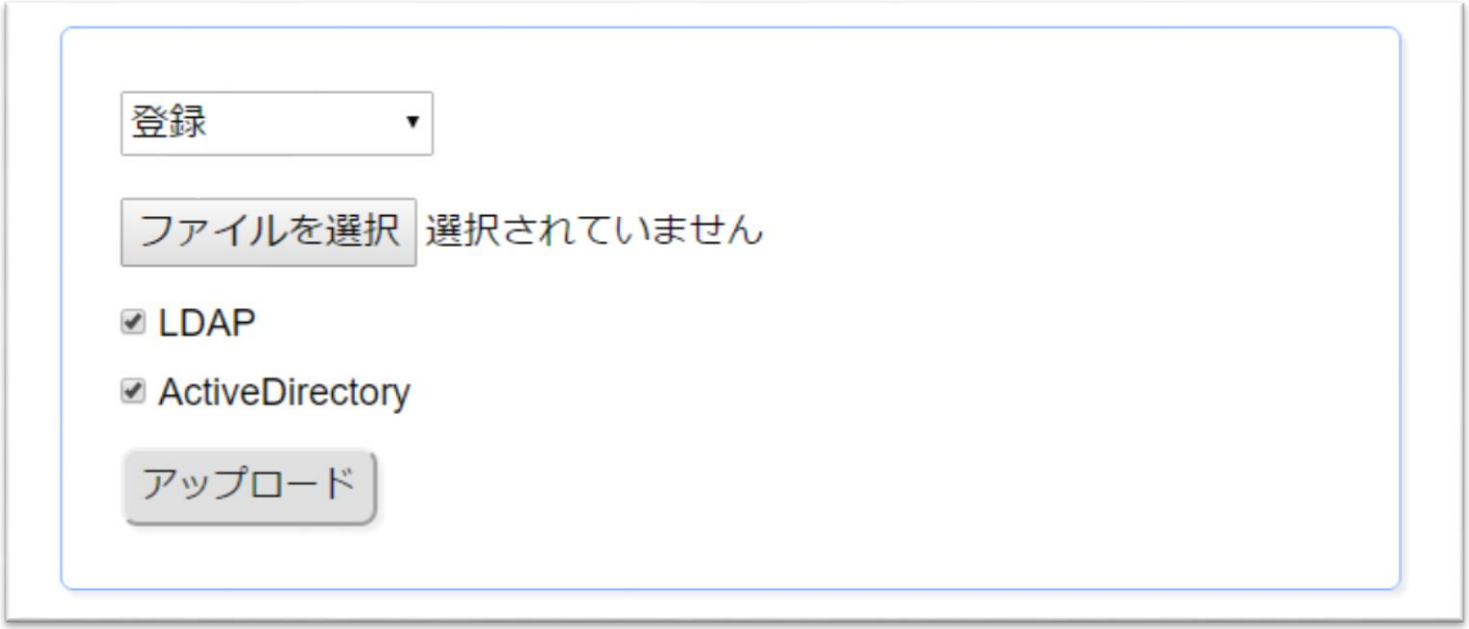
- 入力項目は初期設定にて設定
- 登録先を管理者がユーザーごとに選択可能

機能詳細 - 管理者　1ユーザー変更操作 -

- 更新・無効化・有効化・削除・リネーム・パスワード変更
- 操作先を、チェックボックスで選択可能

機能詳細 - 管理者　CSV一括操作 -

- 操作種別
  - 一括登録・更新・削除・有効化・無効化、パスワード変更・リネーム
- 連携対象を選択可能



機能詳細 - CSVフォーマット -

- CSVフォーマット
  - CSVの1行目はヘッダー(各項目名)
  - 画面表示の項目名がCSVのヘッダー(userName以外)
  - UTF-8 / シフトJIS の CSVファイルに対応
  - 登録用CSV、更新用CSV、削除用CSVなどを利用

userName	姓	名	メールアドレス	…
yamada	山田	太郎	yamada@example.com	
suzuki	鈴木	一郎	suzuki@example.com	

機能詳細 - 管理者　操作結果画面 -

- 操作時間、操作種別、操作結果、対象名、実行者、接続元など
- 一般ユーザーのパスワード変更操作も記録
- 検索条件による表示内容の絞り込み

機能詳細 - 管理者　ロールによる権限移譲 -

- UIDMに登録した管理者ごとにロールによる操作権限の設定が可能
  - ロールは操作種別、操作対象ターゲットによる制限
- 利用例
  - 特定のターゲットのみ操作できる管理者の作成
  - パスワードのみを更新できる管理者の作成

機能詳細 - コマンドラインインタフェース -

- Linux上のコマンドでユーザー管理等の操作
  - /opt/osstech/sbin/unicornidm-tool
- 操作種別
  - ユーザー一括操作(登録・更新・削除・有効化など)
  - グループ一括操作(登録・削除・メンバー登録など)
  - ユーザー一覧、グループ一覧の取得
  - 操作結果情報の一覧取得
  - ロール管理(登録、削除、変更など)
  - 管理者登録・パスワード変更など
  - バックアップ・リストアなど

機能詳細 - SCIMインタフェース -

- SCIM
  - ID連携のために策定されたID連携用Web API(REST)
- UnicornIDMサーバーに対するSCIMプロトコルによるID連携操作
  - Webアプリケーションからの ID連携操作の実装
  - 操作種別
    - ユーザー登録・更新・削除
    - グループ登録・削除・メンバー管理

Ver2からのその他の機能強化点

- 一般ユーザー向け画面のスマートフォン対応
- キャッシュ管理機能の改善による操作レスポンス向上
- 属性のマルチバリュー対応
  - LDAP、Active Directoryなどで利用可能
- コマンド連携機能改善
  - コマンドへのJSON形式によるデータ連携

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ *info@osstech.co.jp*