これからのエンタープライズ向け認証基盤に求められること

株式会社オージス総研

八幡 孝

Chapter I

シングルサインオンしてますか？

会場の皆さんにアンケート

Q

IDとパスワードは
1つだけ覚えておけばいけている

Q

一回ログインすれば、
必要なアプリが一通り使える

Q. パスワード変更は1回やれば ちゃんと変わっている

Q Windowsのログオンだけで全部できている

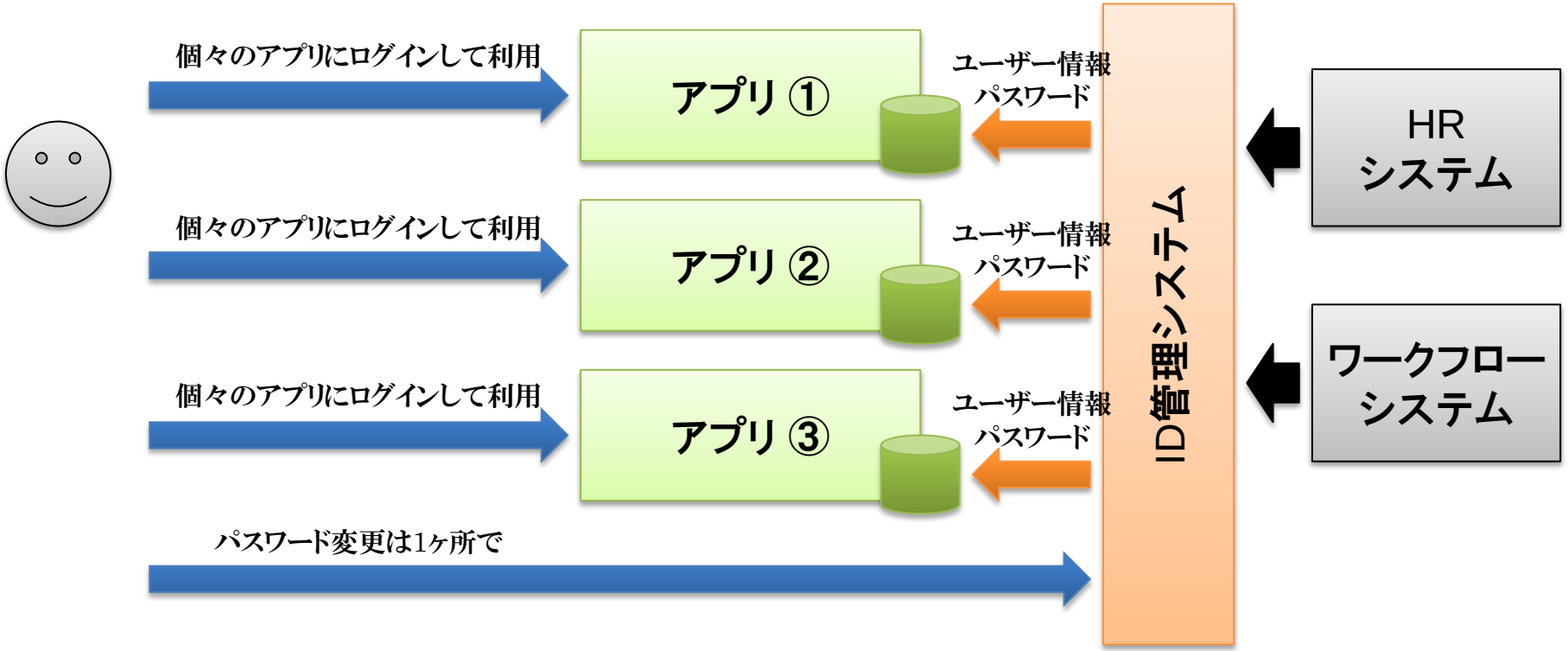
Q

クラウドサービスを使うときはできるだけ
ソーシャルログインを使っている

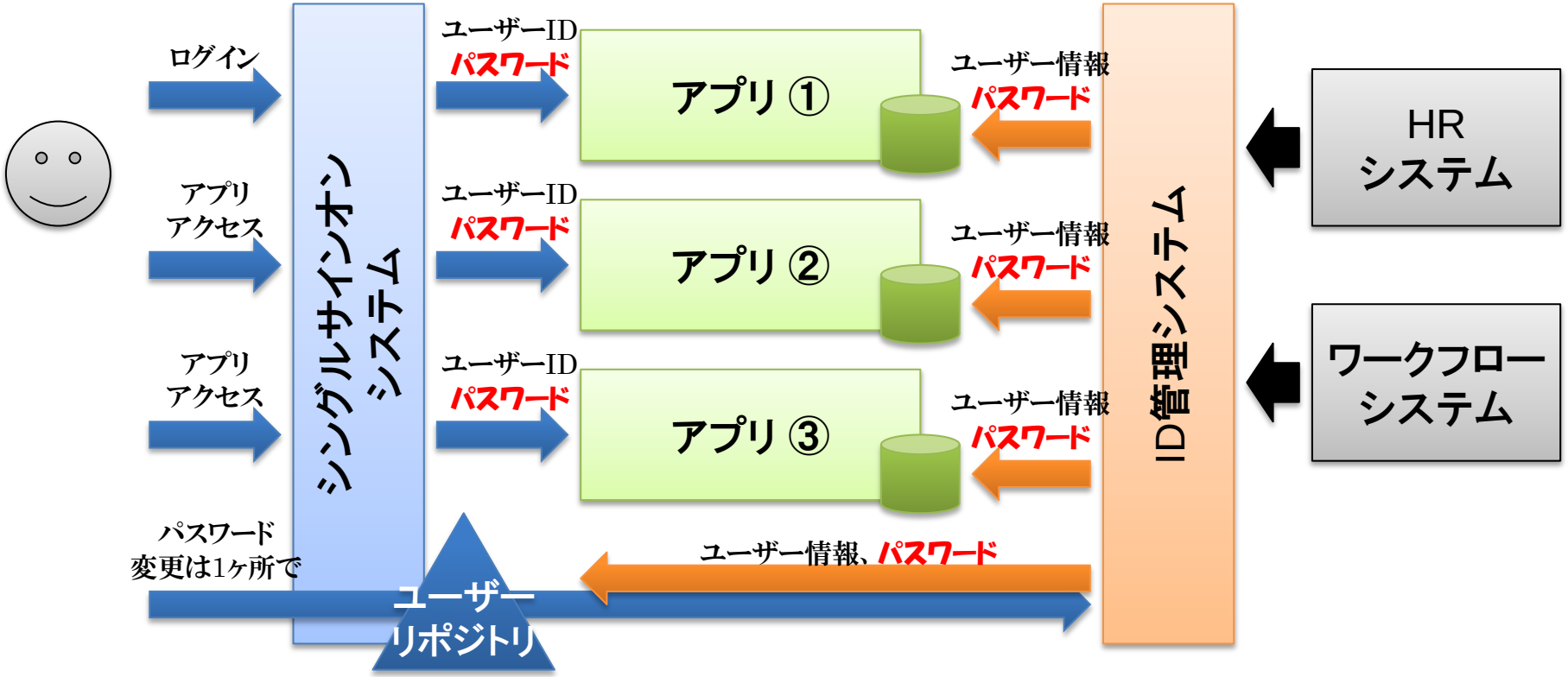
Chapter II

シングルサインオン実現の基本パターン

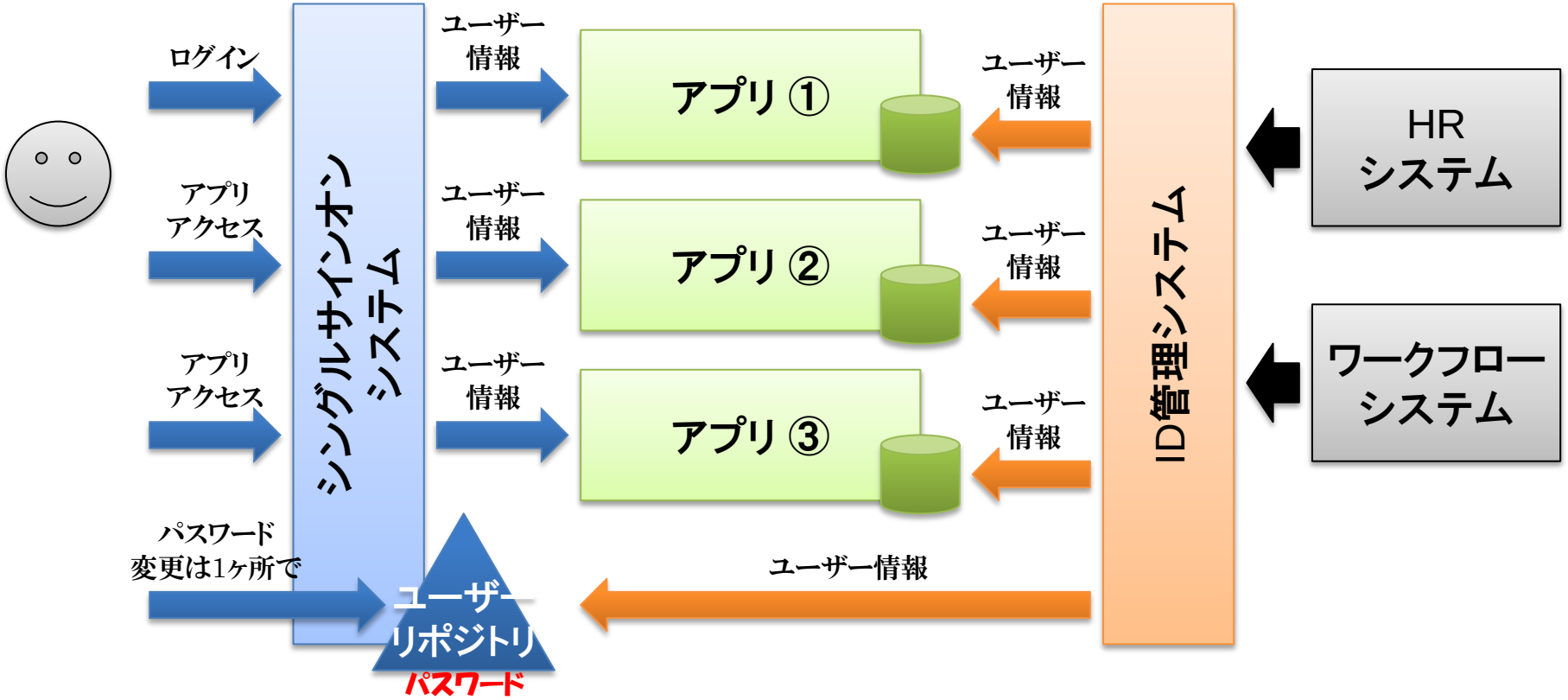
① IDMでID/パスワードを管理



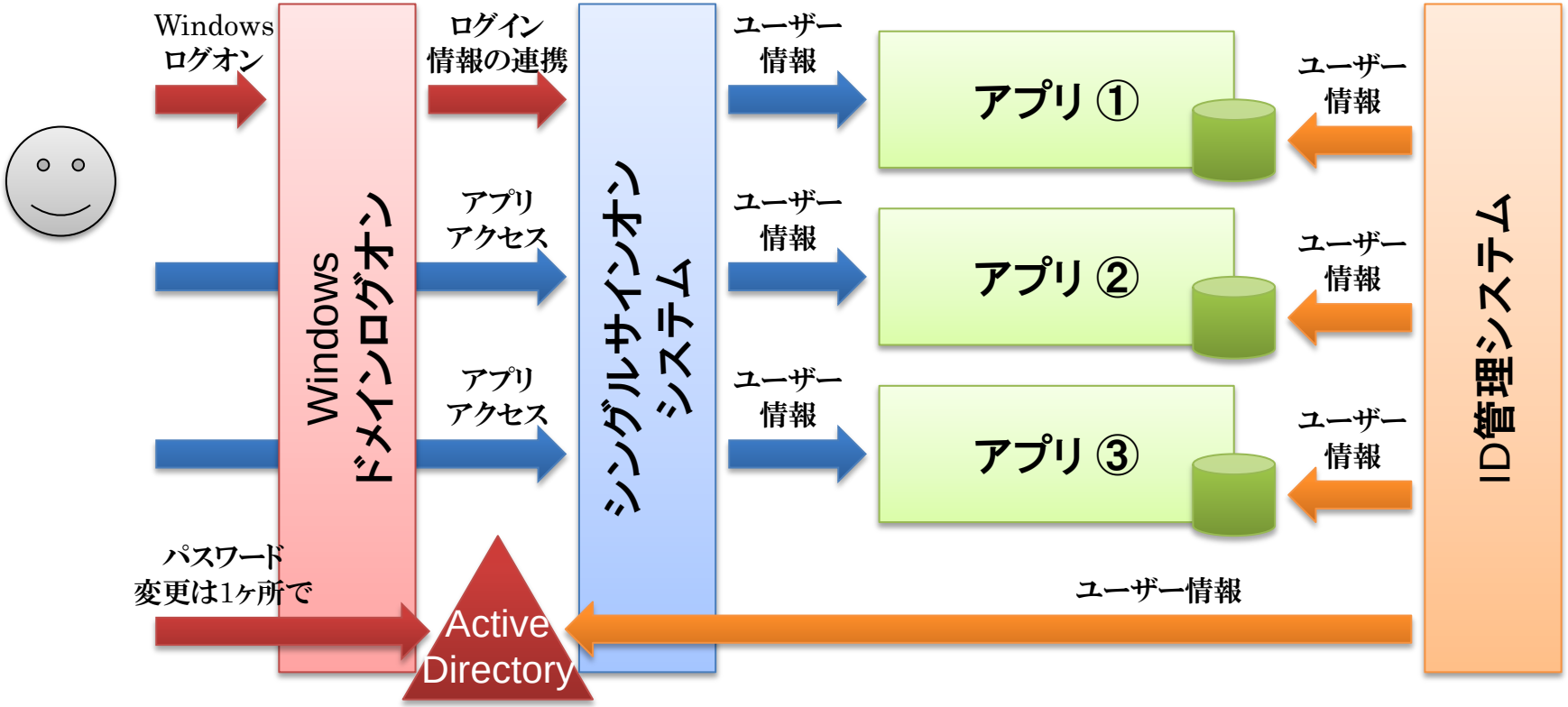
② IDM+SSOの組合せ



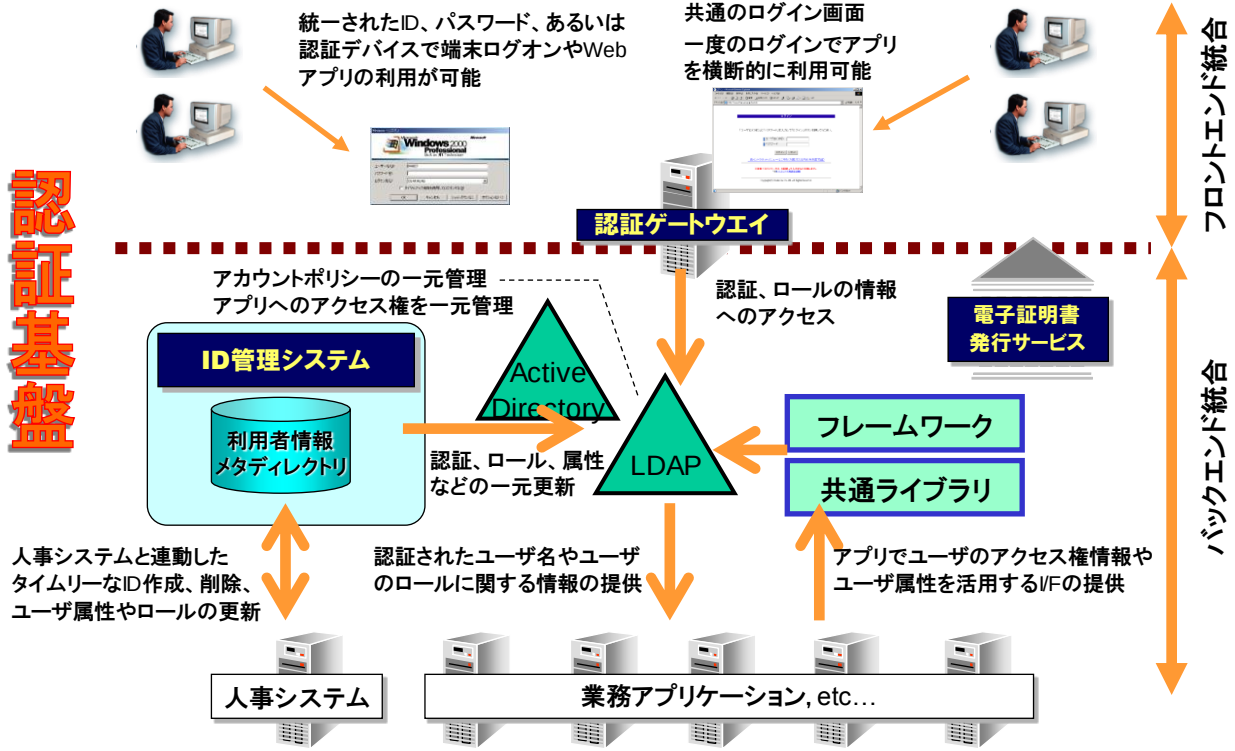
③ より完全なSSO



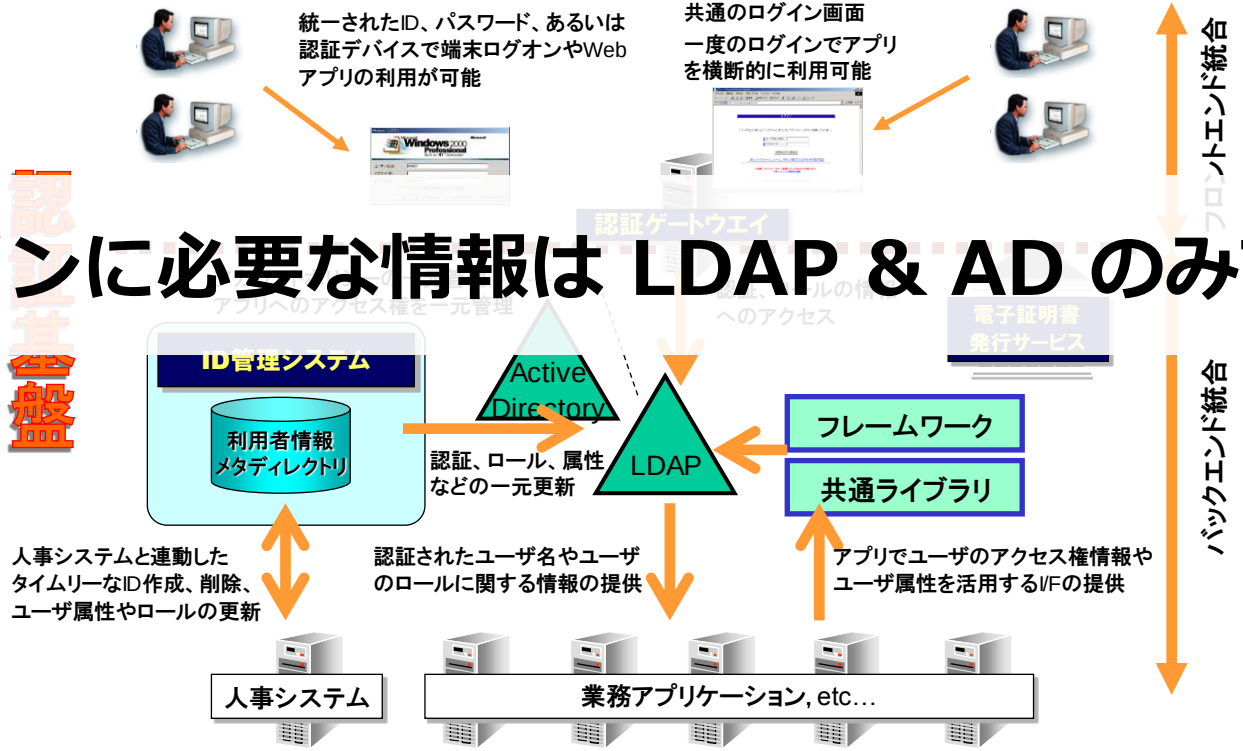
④ デスクトップSSO



とある事例での実現例

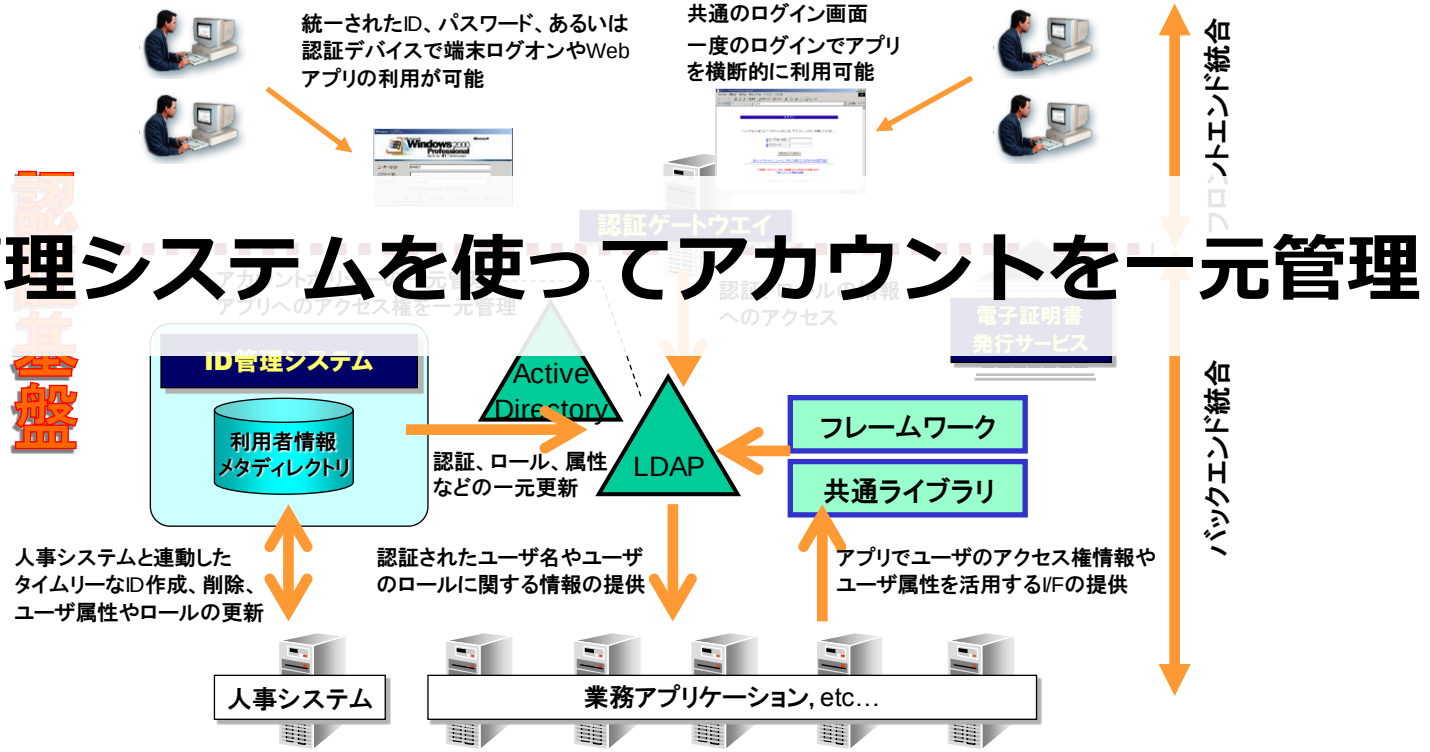


とある事例での実現例



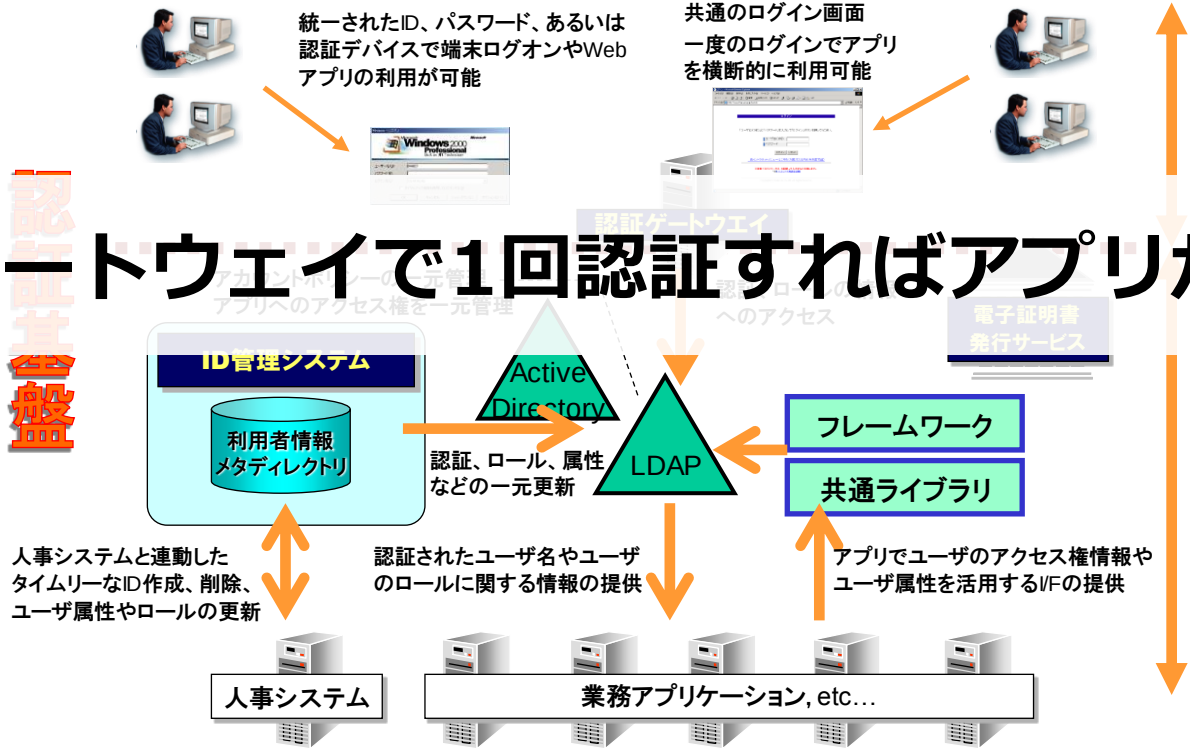
ログインに必要な情報は LDAP & AD のみで管理

とある事例での実現例



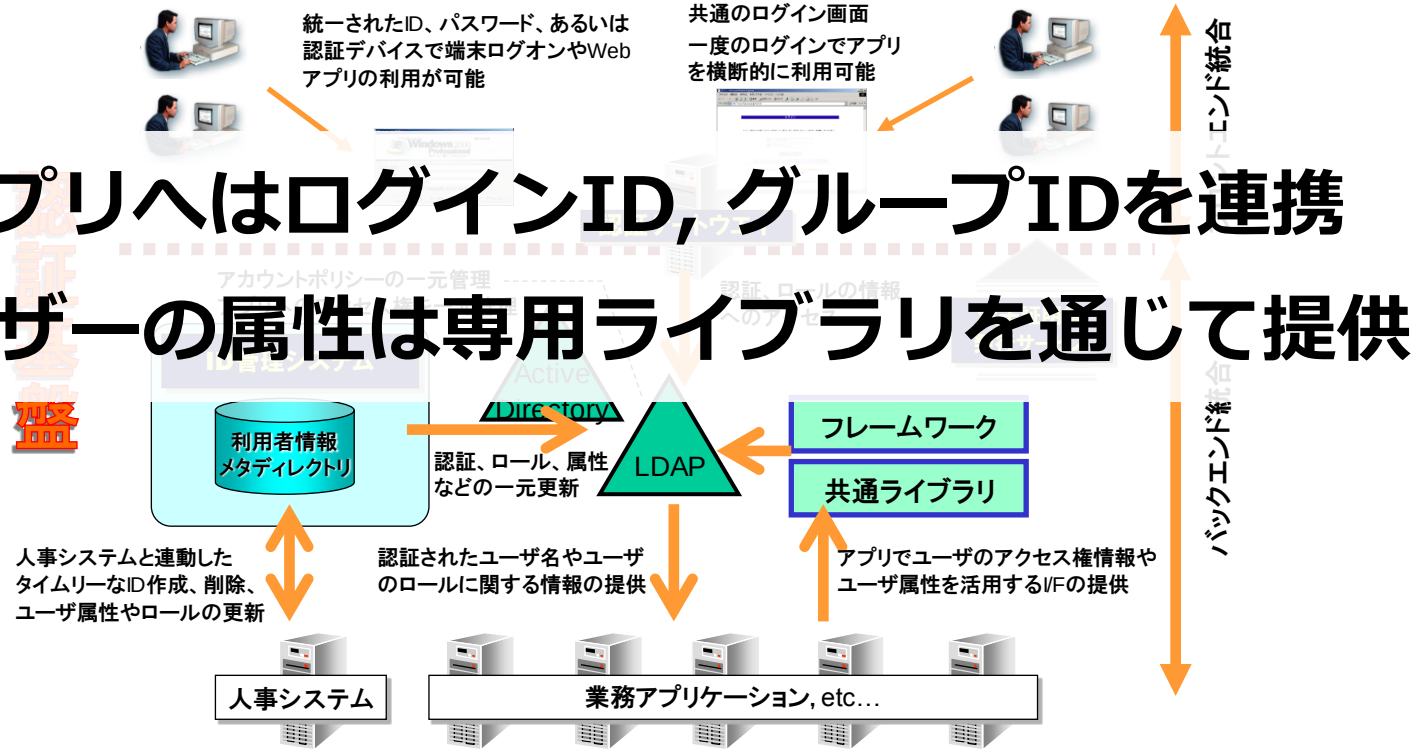
ID管理システムを使ってアカウントを一元管理

とある事例での実現例



認証ゲートウェイで1回認証すればアプリが使える

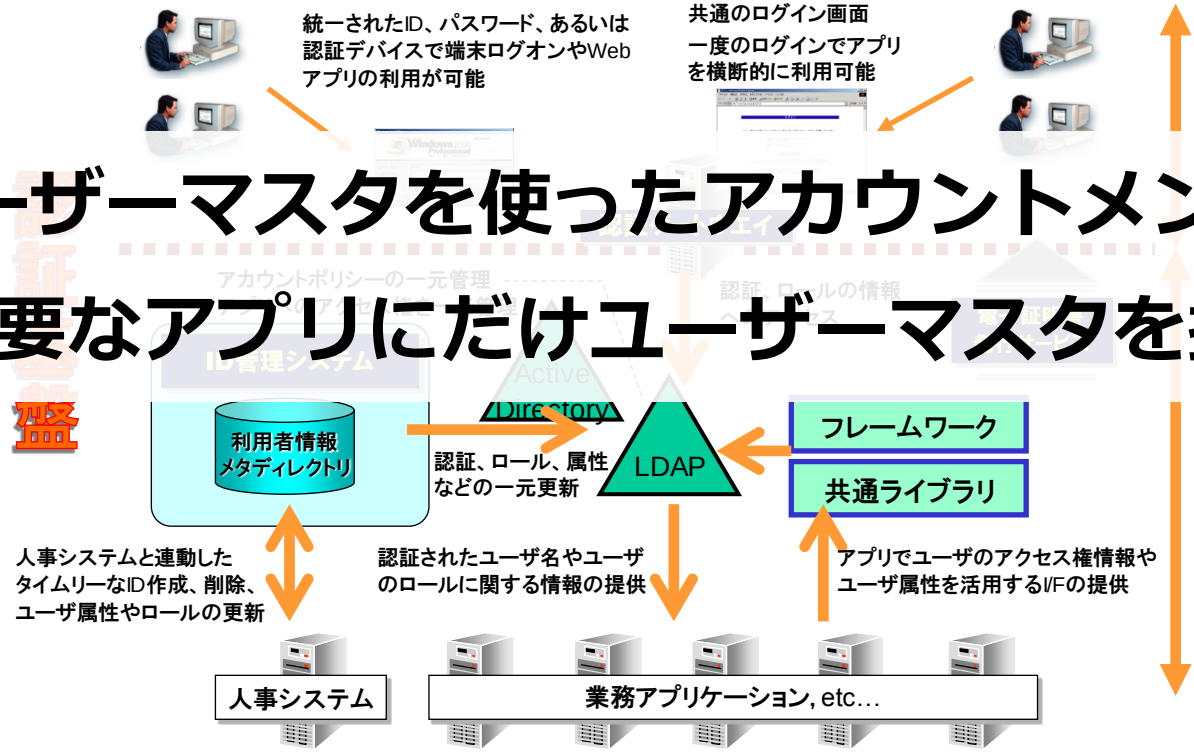
とある事例での実現例



アプリへはログインID, グループIDを連携

ユーザーの属性は専用ライブラリを通じて提供

とある事例での実現例



Chapter III

なぜシングルサインオンをするのか？

① 利用者が便利になる

- 作業効率の向上
- IT活用の促進

② セキュリティレベルのばらつきがなくなる

- 開発者に依存したばらつき
- ユーザーに依存したばらつき

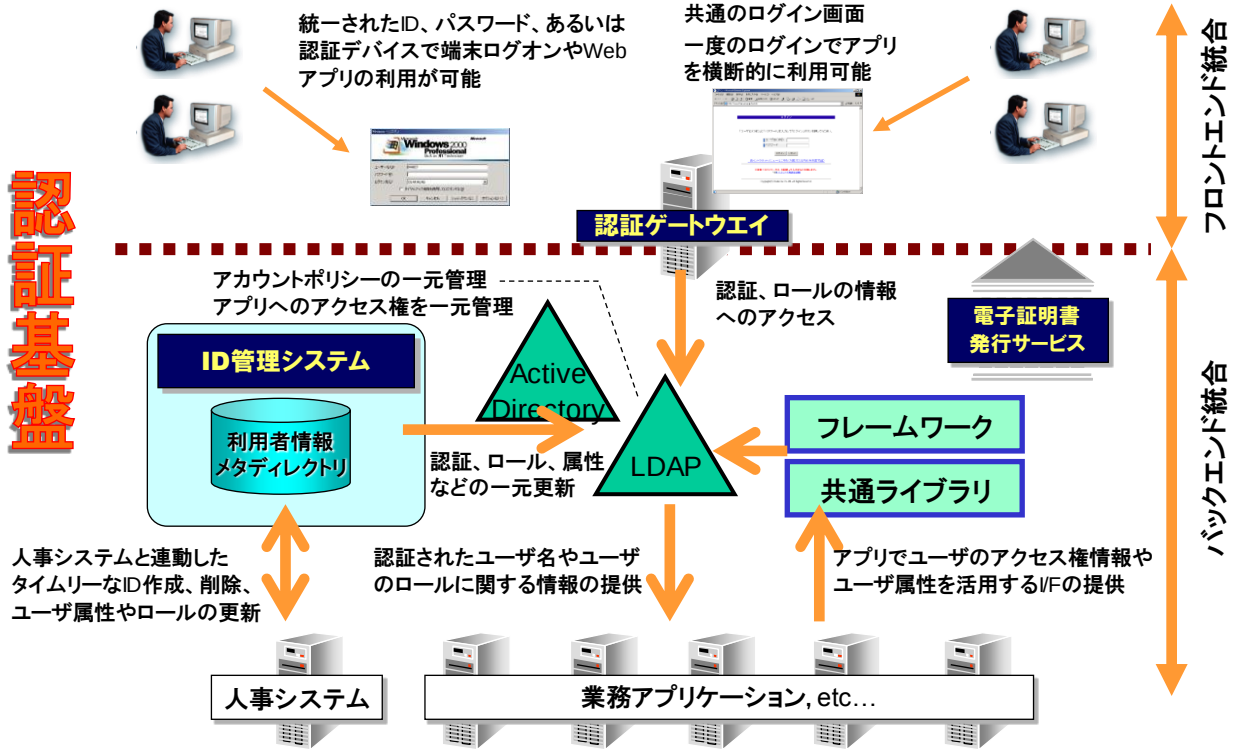
③ システム開発がしやすい

- アプリ毎の認証機能開発は不要
- サブシステムに分割した開発の実現

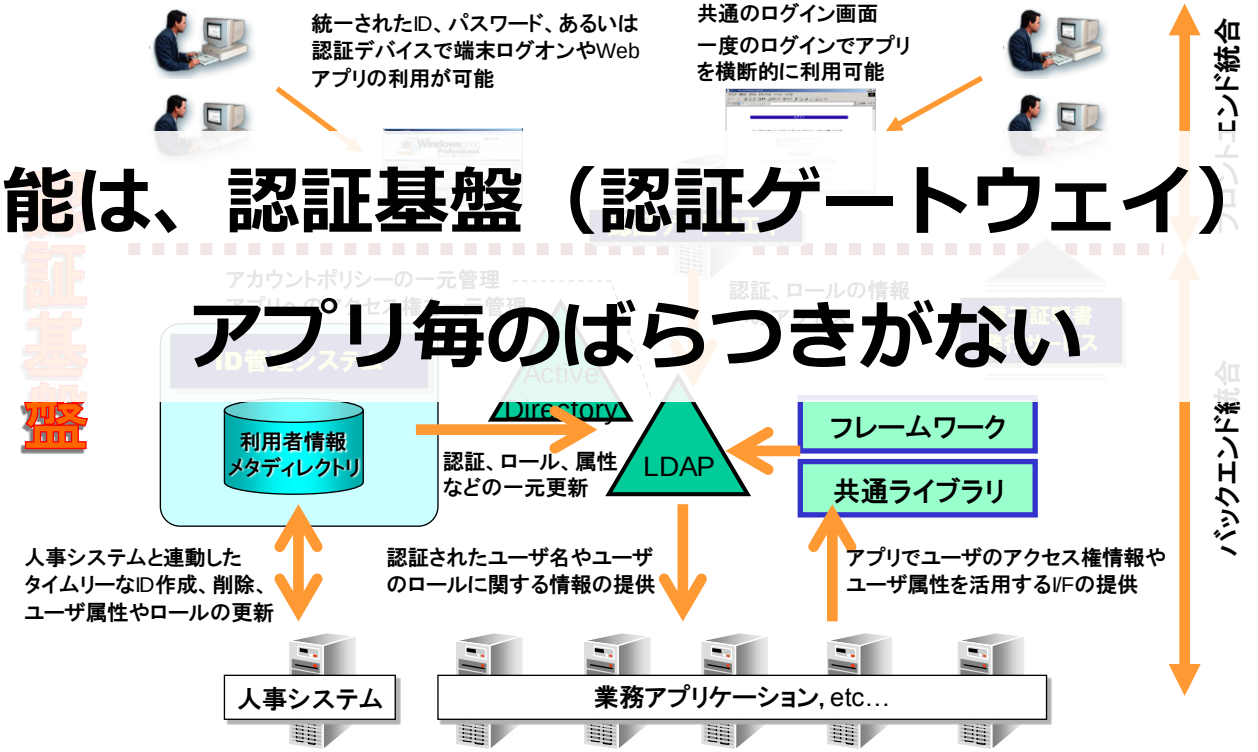
④ 認証方式の変更がやりやすい

- ID/パスワードを使った認証
- 多要素認証への対応
- 新しい方式への対応

とある事例での実現例



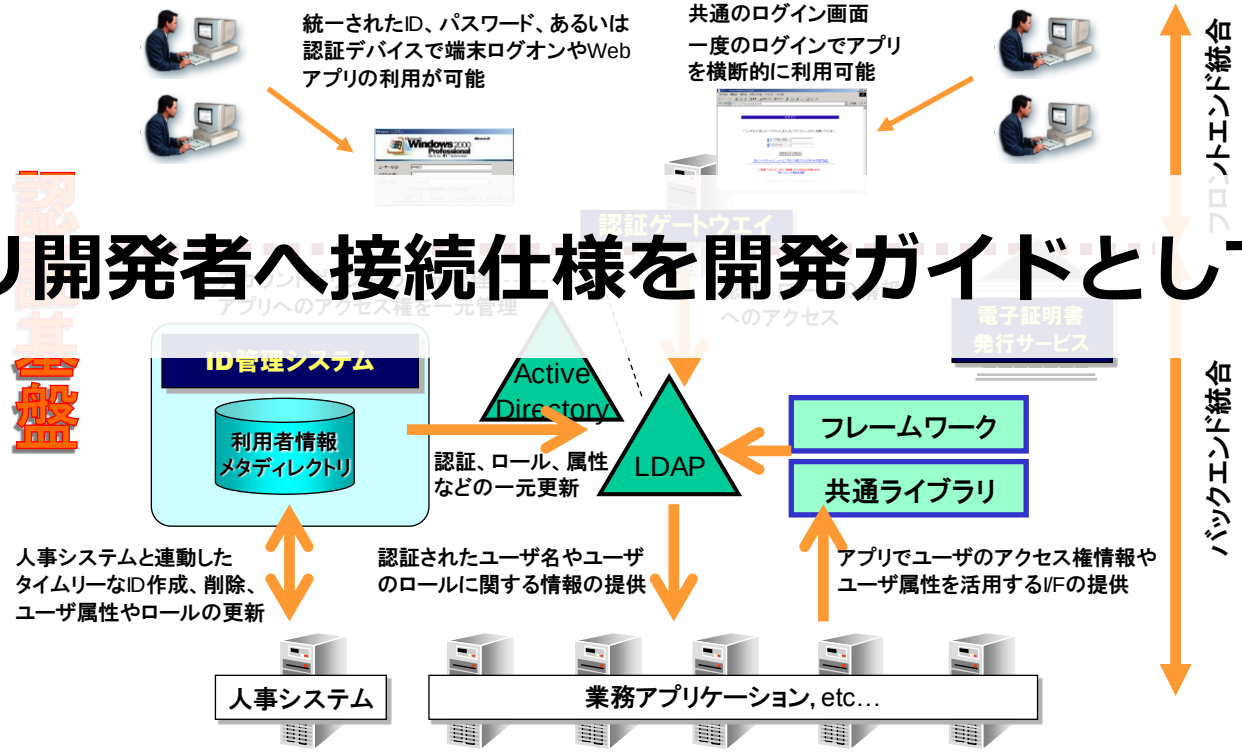
とある事例での実現例



認証機能は、認証基盤（認証ゲートウェイ）で提供

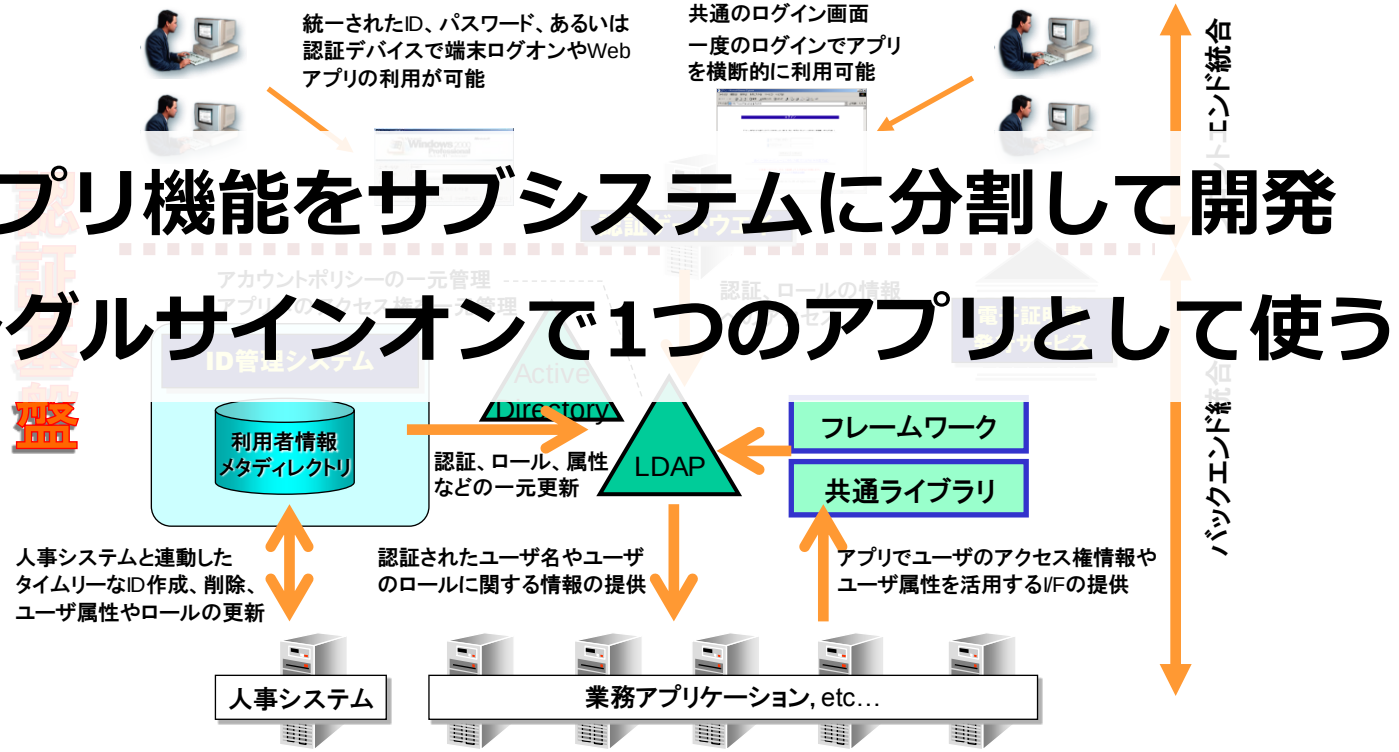
アプリ毎のばらつきがない

とある事例での実現例



アプリ開発者へ接続仕様を開発ガイドとして提供

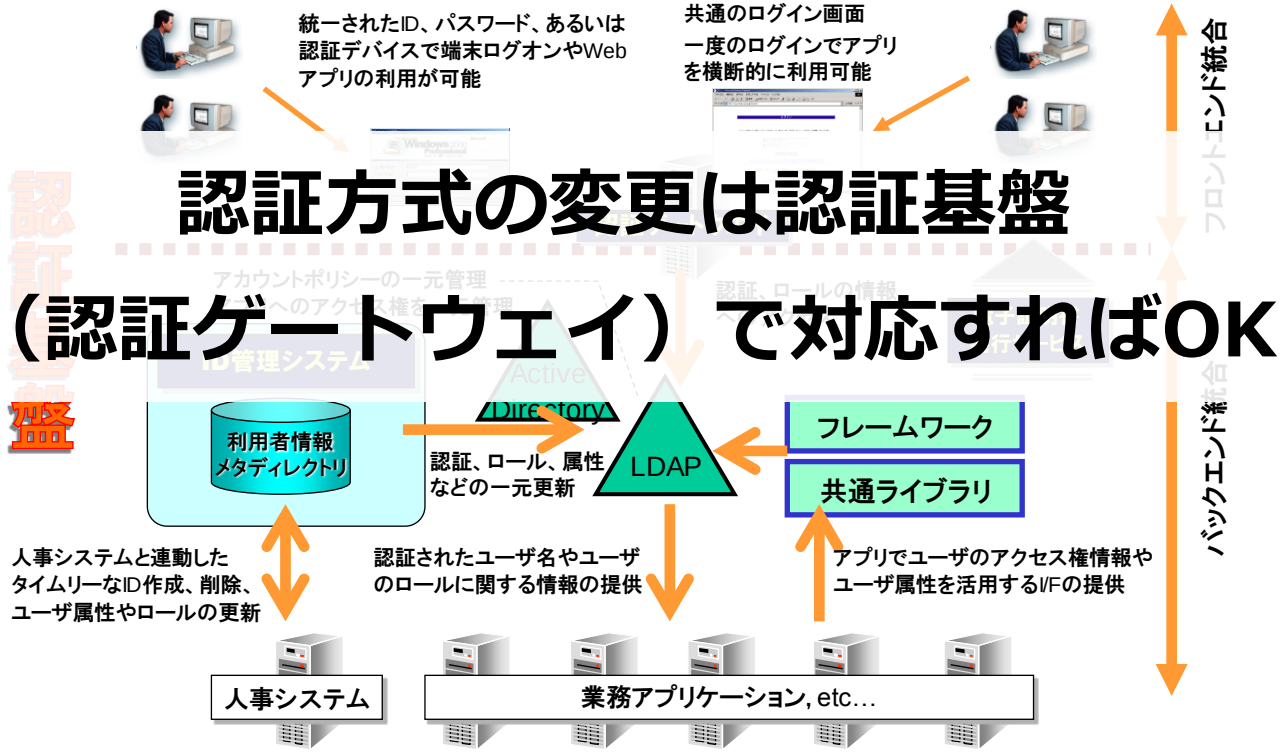
とある事例での実現例



アプリ機能をサブシステムに分割して開発

シングルサインオンで1つのアプリとして使う

とある事例での実現例



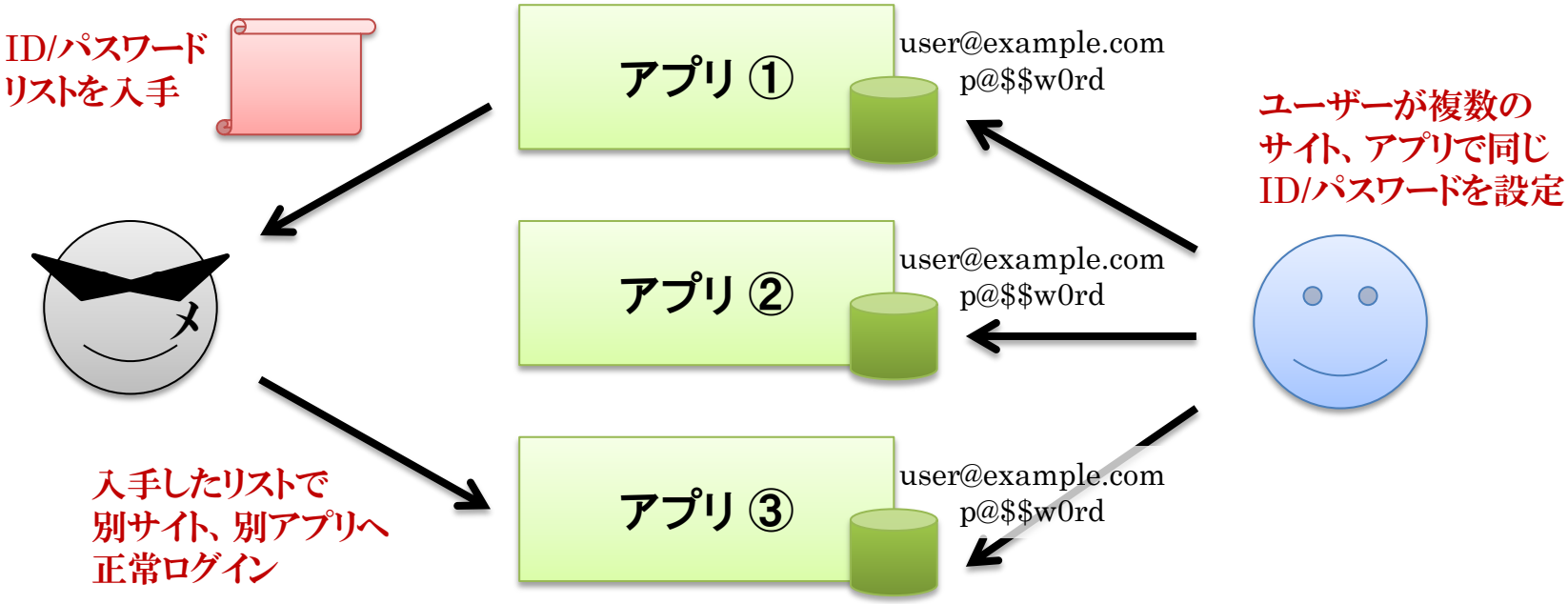
みなさんの会社・組織では

実現できていますか？

Chapter IV

最近の認証界隈の困った話題

パスワードリスト攻撃



対策①: パスワード定期変更

対策②: STOP!! パスワード使い回し!!

増えるユーザーの負担

- パスワードの定期変更の強制
- パスワード使い回しの禁止
  - 紙のメモ、電子ファイル（パスワード付き）を使った管理
  - パスワード管理ツールの利用
- ユーザー自身での確認を要請
  - ログイン履歴の確認
  - ログイン通知機能の利用
- 認証コード、ワンタイムパスワードの利用

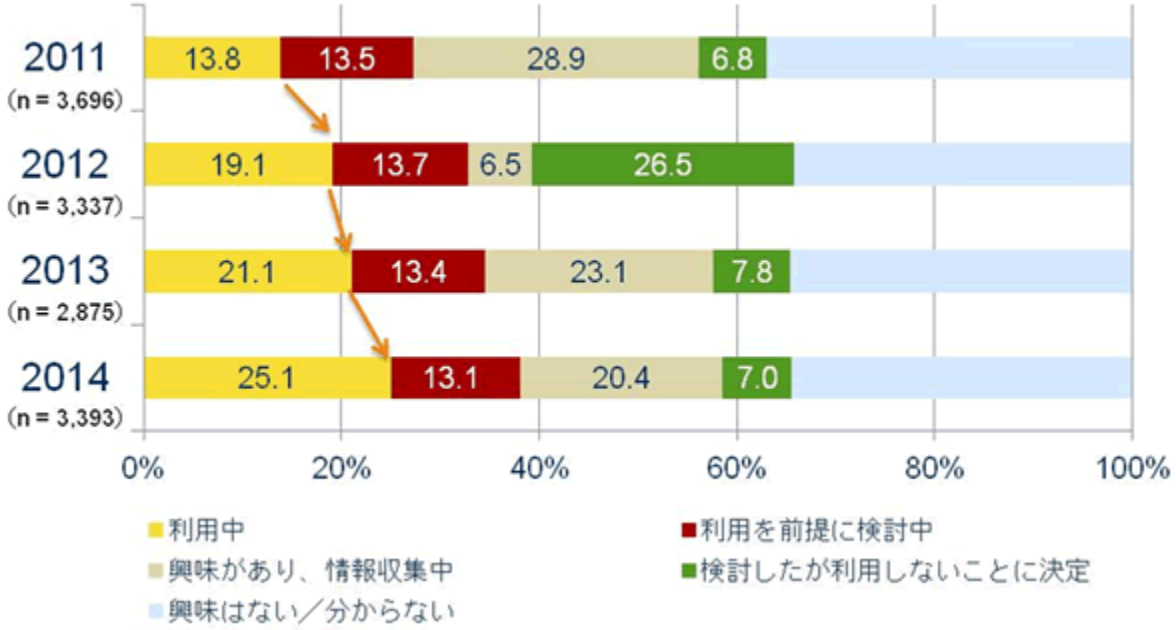
「そこはシングルサインオンでしょ」

- パスワードは認証基盤だけで管理
- 認証結果をアプリケーションへ連携
  - ログインID, ユーザーの属性情報
  - 認証基盤を通らないアプリアクセスを禁止
- 真のSSOを目指せ

Chapter V

IT活用はクラウドサービス活用へ

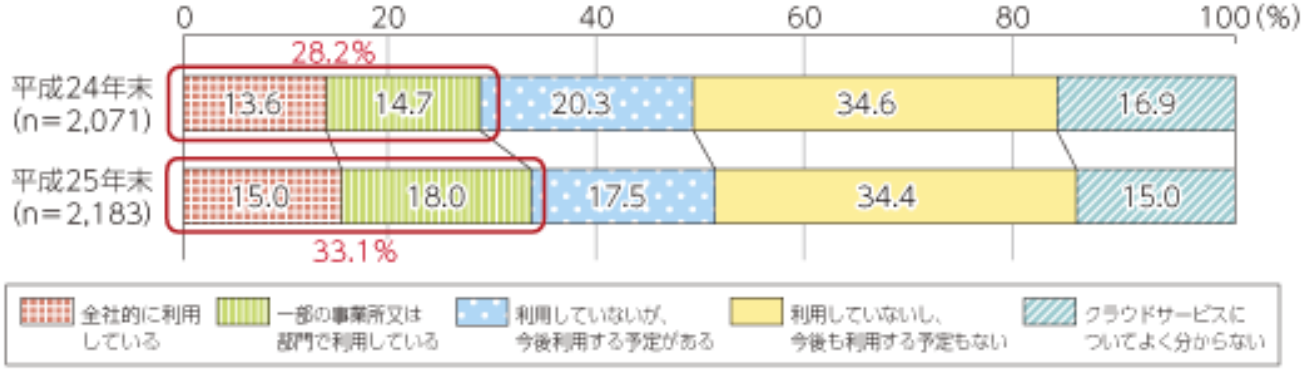
クラウドサービスの利用が進む



【出典】2014年 国内クラウドサービス市場 需要動向調査, IDC Japan, 2014年7月
http://www.idcjapan.co.jp/Press/Current/20140724Apr.html

クラウドサービスの利用が進む

“● クラウドサービスを利用している企業の割合は平成24年末の28.2%から33.1%に上昇”



【出典】平成26年版情報通信白書（原出展）総務省「平成25年通信利用動向調査」
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

事業部門: すぐに、小さく使い始める

Identity is the next perimeter

- どこからでも使える
- どのデバイスからでも使える
- データ保護の最後の砦は「認証」

IT部門&セキュリティ部門:
ID管理とSSO、どうするの？

野良IT化、シャドーIT化

パスワード定期変更!!

STOP!! パスワード使い回し!!

増えるユーザーの負担

- パスワードの定期変更の強制
- パスワード使い回しの禁止
  - 紙のメモ、電子ファイル（パスワード付き）を使った管理
  - パスワード管理ツールの利用
- ユーザー自身での確認を要請
  - ログイン履歴の確認
  - ログイン通知機能の利用
- 認証コード、ワンタイムパスワードの利用

増えるユーザーの負担

- パスワードの定期変更の強制
- パスワード使い回しの禁止
  - 紙のメモ、電子ファイル、ツールを使った管理
  - パスワード管理ツールの利用
- ユーザー自身での確認を要請
  - ログイン履歴の確認
  - ログイン通知機能の利用
- 認証コード、ワンタイムパスワードの利用

企業でのIT活用

企業自らの情報を守るための対策を、

社員一人ひとりの対応に委ねて良いのか？

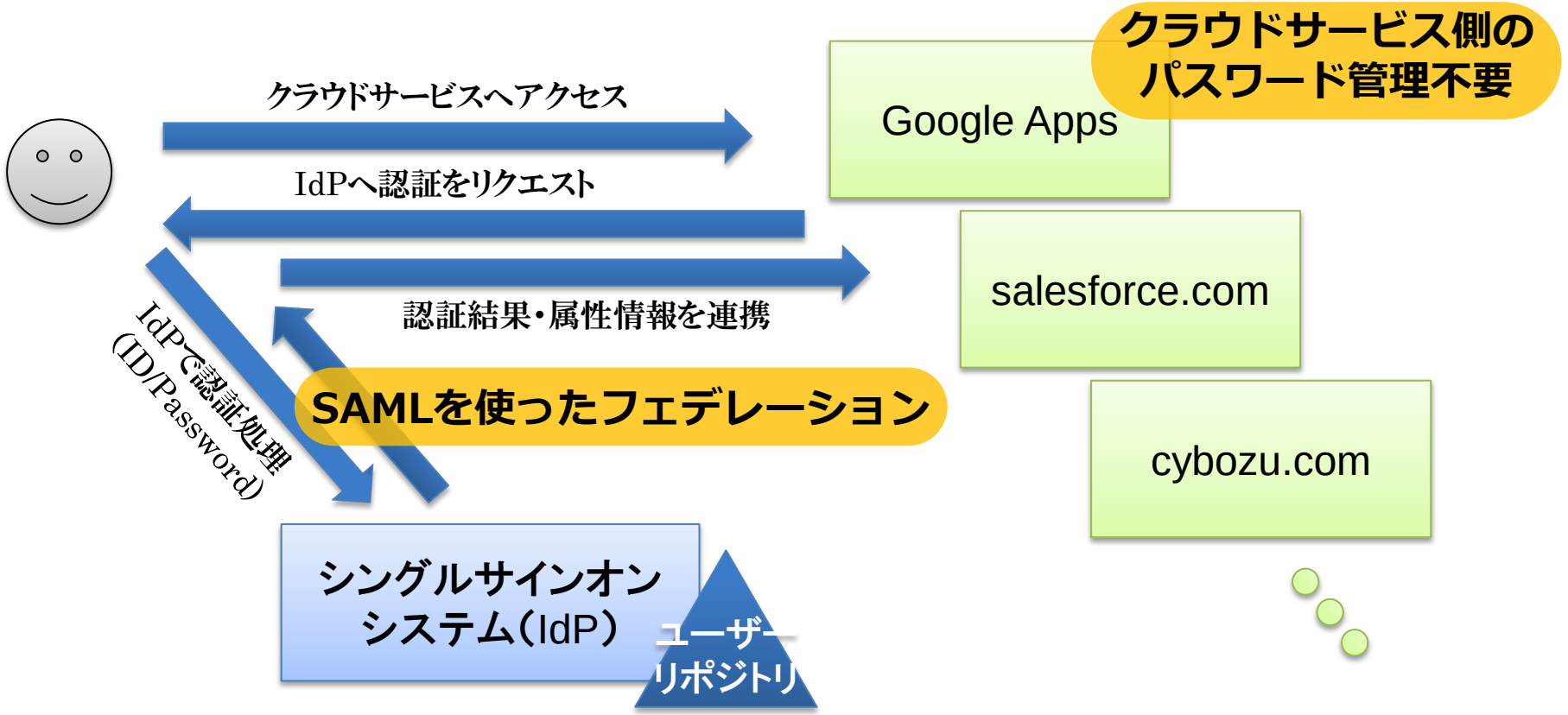
Chapter VI

IT活用はクラウドサービス活用へ (Part2)

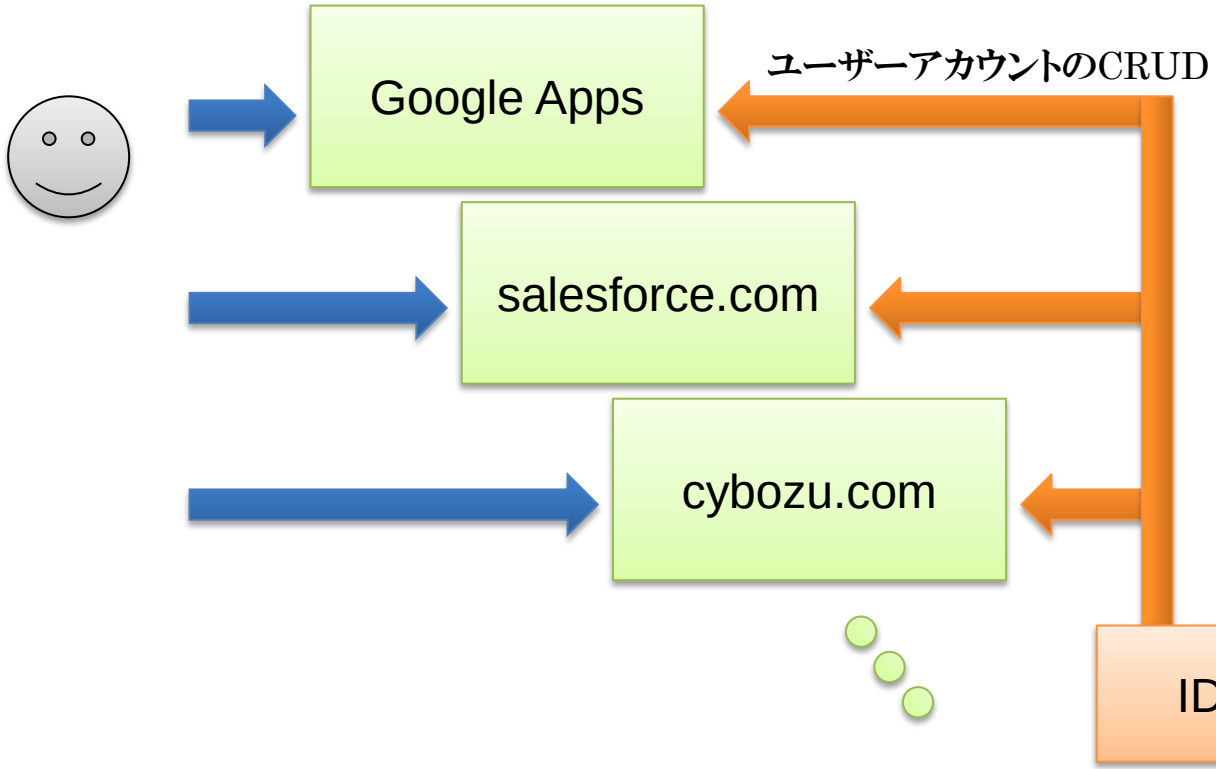
クラウドサービスに対応した認証基盤

- Identity Federation によるSSO
- アカウント管理のためのIDM(ID管理)
- この2つに対応する

Identity Federation によるSSO



アカウント管理のためのIDM（ID管理）



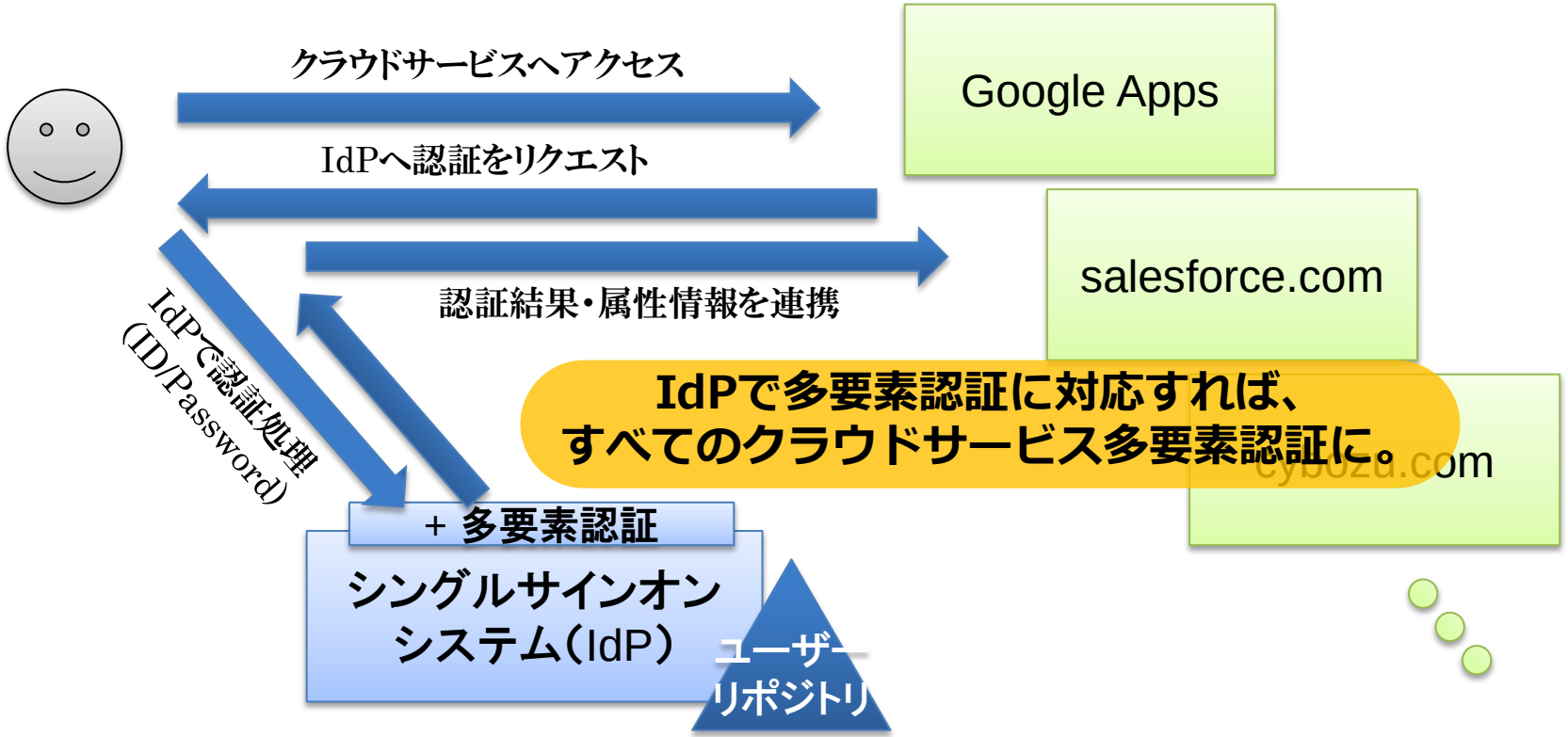
クラウドサービス側の
アカウント事前配備

ユーザーへの
ライセンス割当、解除

ユーザーが作成した
データの削除

当面は独自I/F
いずれはSCIM

多要素認証への対応 ⇒ 認証基盤で対応



SAMLに対応したクラウドサービスが増えてきている

- Google Apps
- Salesforce.com
- Microsoft Office 365
- cybozu.com
- Fileforce
- **などなど**

認証基盤で SAML IdP を実装

サービス事業者に SAML SP 対応を

リクエストしよう

Chapter VII

ビジネスのための認証基盤

B2E向けから、B2B向け、B2C向けへ

- 取引先ポータル、顧客ポータルの構築が広まる
- 先に認証基盤を用意して、サービス（提供機能）を拡大

B2C向けのケース

- 顧客にアカウントをセルフ登録してもらう

- ソーシャルアカウントを使って、アカウントを登録してもらう
  - すでにソーシャルログインが主流に。

B2B向けのケース

- 取引先のID/パスワードを、自社の認証基盤で管理

- 取引先の認証基盤（IdP）からのSSO

いかにシステムを使ってもらうかが重要

- 利用者に優しい認証の実現
- 取引先の認証基盤でログイン、ソーシャルアカウントでログインが主流に
- SAML から OpenID Connect へ向かう

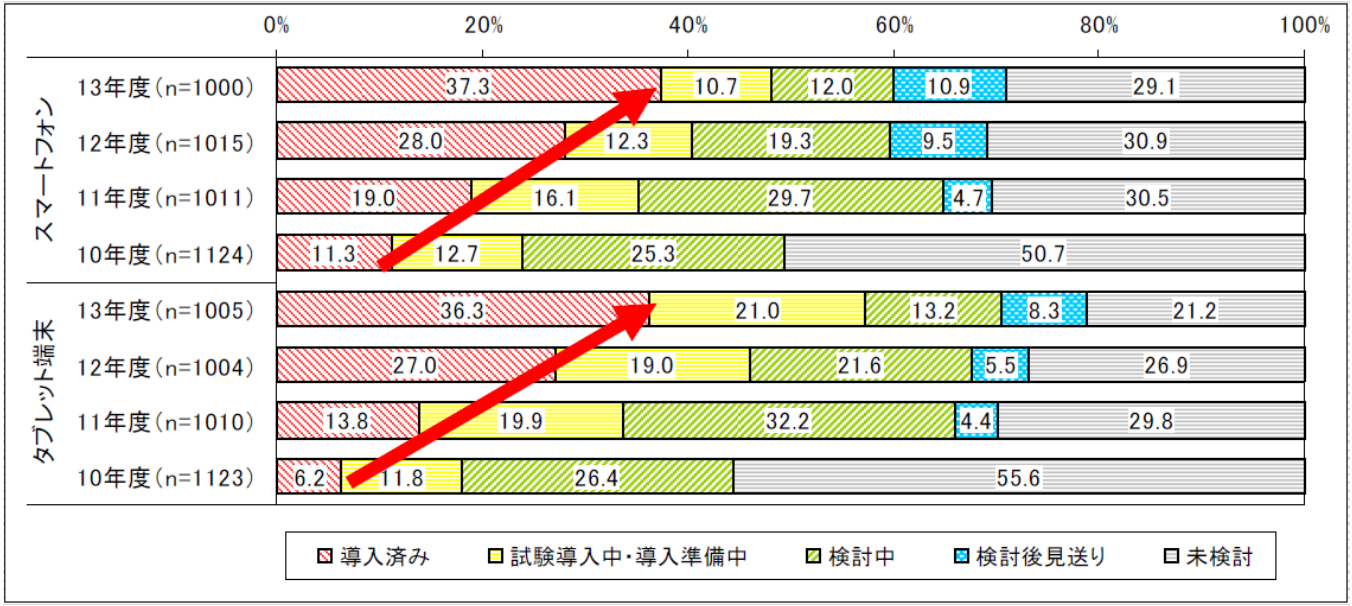
これからの企業の認証基盤は、SAML、OpenID Connect への対応が必須要件

（標準技術に対応する、対応し続ける）

Chapter VIII

そして、WebAPIへ

エンプラでもスマートデバイスの活用が進む



“ただし、別途調査した導入台数の規模を見ると、大規模な導入を行っている企業は限定的である”

【出典】企業IT動向調査2014, 日本情報システム・ユーザー協会, 2014年4月
http://www.juas.or.jp/servey/it14/

アプリケーションアーキテクチャが変わる

- ネイティブアプリ + WebAPI
- SPA (Single-Page Application) + WebAPI

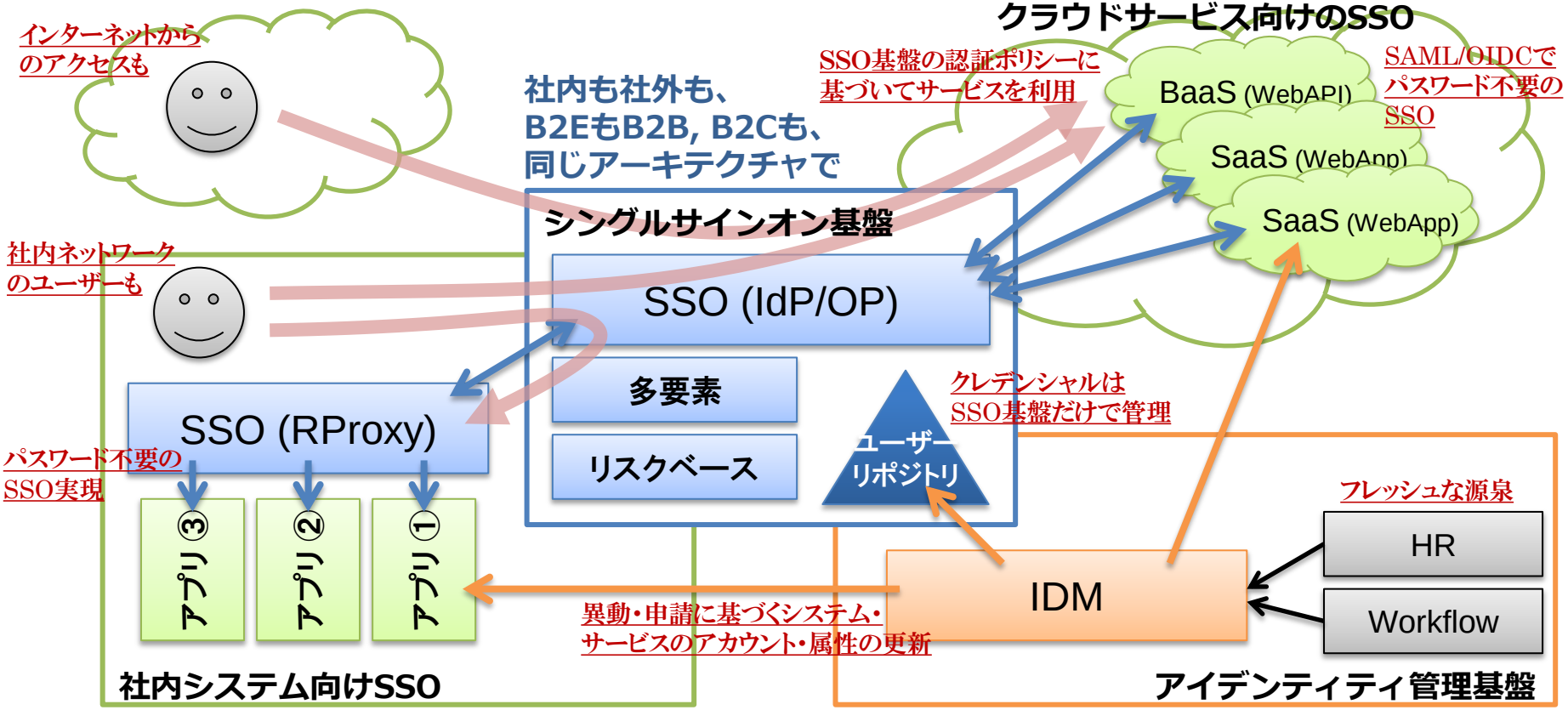
WebAPI時代の認証・認可

- OpenID Connect, OAuth
- **より高度な認可に向けて… UMA?**

Chapter IX

エンプラ向け認証基盤コアアーキテクチャ

認証基盤コアアーキテクチャ　2015年版



目指すべきこと

- 社内のアプリもクラウドアプリもシームレスに使える。
- 一回のログインで、全アプリを横断的に使える。
- ログインに必要なIDとパスワードは一つだけ。
- パスワードを持っているのは認証基盤だけ。
- TPOに応じた認証方法が使える。
- アプリの利用を一元的にコントロール。
- SaaS (Webアプリ) にも BaaS (WebAPI) にも使える。

必要な技術要件

- **標準技術への対応**
  - フェデレーション: SAML, OpenID Connect, OAuth, …
  - プロビジョニング: SCIM
  - 標準技術に継続的に対応し続けること
- **従来型の方式のサポート**
  - リバースプロキシ、エージェントを使ったSSO
  - 変更できない現行アプリへの対応 ⇒ 代理認証
  - 現行方式のID管理の実現

OSSを使うメリット

- 技術標準の早期実装
- 公開されている仕様
- ソースコードを使った問題調査、修正

Chapter X

まとめ

まとめ

- クラウドサービス、スマートデバイス、新しいアーキテクチャに対応する
- ビジネスのための認証基盤に対応する
- それがこれからのエンプラの認証基盤
- 標準技術を使って、真のSSOを目指そう

ご清聴ありがとうございました。

【お問合せ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-7998
E-mail: info@ogis-ri.co.jp