オープンソースで実現する
IDマネージャー:Unicorn ID Manager
シングルサインオン:OpenSSOのご紹介

オープンソース・ソリューション・テクノロジ株式会社
2009/12

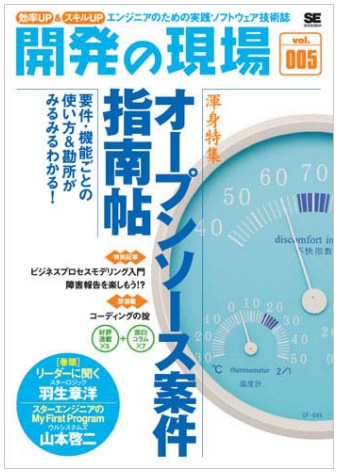
OSSTech

お問い合わせ info@osstech.co.jp

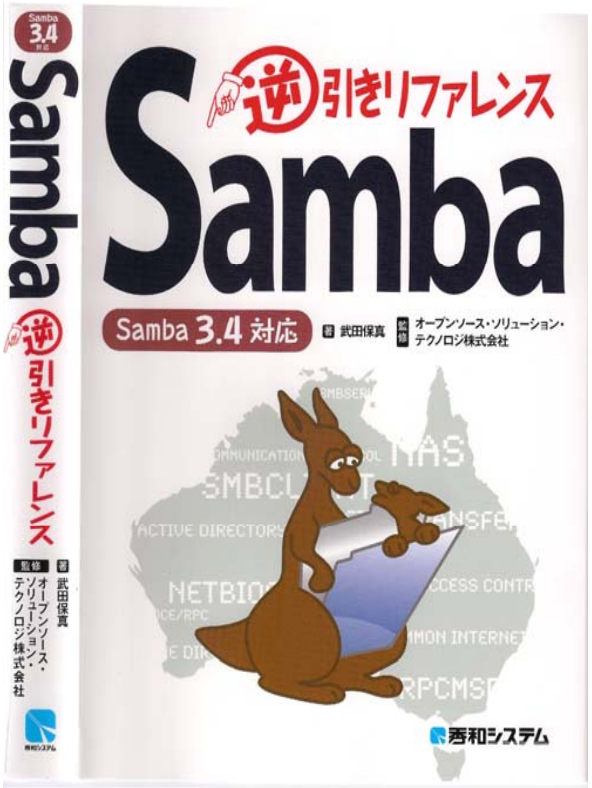
オープンソース・ソリューション・テクノロジ
会社紹介

社員著作紹介

- @IT やってはいけないSambaサーバ構築：2008年版
- 日経コミュニケーション2007年11/15号から3回連載 Windows管理者に送るSamba活用の道しるべ
- 技術評論社 Software Design 2006年7月号
  - ネットワーク運用／管理 五輪書（ごりんのしょ）
  - 「壱：地の巻」Sambaファイルサーバ
  - http://www.gihyo.co.jp/magazines/SD/contents/200607
- 2006年5月 翔泳社 開発の現場 vol.005
  - オープンソース案件指南帖
  - 総論編：オープンソースの基礎知識
  - http://www.shoeisha.com/mag/kaihatsu/
- 2006年5月 技術評論社 LDAP Super Expert
  - 巻頭企画
  - [新規／移行]LDAPディレクトリサービス導入計画
  - http://www.gihyo.co.jp/magazines/ldap-se
- 2006年5月 IDG月刊Windows Server World 2006年3月、4月
  - 3月号：Shall we Samba?【お手軽導入編】
  - 4月号：Shall We Samba?【超本格運用編】
- 2005年10月 日経BP社 セキュアなSambaサーバの作り方
  - http://itpro.nikkeibp.co.jp/linux/extra/mook/mook12/index.shtml



Samba逆引きリファレンス【Samba3.4対応】



- 最新版 Samba 3.2～3.4 対応
- 豊富なSambaシステム構築実績を基に認証サーバ(ドメインコントローラ)機能、ファイルサーバー機能、ドメインメンバー機能の活用方法を詳細解説
- Samba/LDAPの日本トップエンジニア達による執筆及び監修
- Samba管理者のみならず、Active Directory 管理者も必見！

著者:武田　保真
監修:オープンソース・ソリューション・テクノロジ株式会社
価格:定価 2520円

オープンソース・ソリューション・テクノロジ株式会社

- OSに依存しないOSSのソリューションを中心に提供
  - Linuxだけでなく、Windows/Solaris/FreeBSDなどへも対応！
- Samba,OpenLDAP,OpenSSO,IDMなどによる認証統合/シングル・サイン・オン、ID管理ソリューションを提供
  - 製品パッケージ提供
  - 製品サポート提供
  - OSSの改良、バグ修正などコンサルティング提供
- Sun Java Directory Server, Windows Active Directory, CLUSTERPROなどの商用ソフトのソリューションも提供
  - 商用製品とOSSの柔軟な組み合わせに対応

会社概要

会 社 名	オープンソース・ソリューション・テクノロジ株式会社	所属 団体等	OSSコンソーシアム理事 副会長 LPI-Japanビジネスパートナー デルISVアリーナ パートナー NEC CLUSTERPRO WORKSパートナー Solaris Community for Business(SCB) レッドハット レディ・ビジネス・パートナー オープンソースソフトウェア協会
英語表記	Open Source Solution Technology Corporation		
社名略称	OSSTech（オーエスエステック）または OSSテクノロジ		
業務内容	・OSS（オープンソース）を中心とするソフトウエアの企画、開発、販売およびサポート ・システムの導入に関するコンサルティング ・ソフトウエアに関する教育、研修	取引先 および パートナー様	・株式会社野村総合研究所 ・サン・マイクロシステムズ株式会社 ・株式会社バッファロー ・日本電気株式会社 ・日本電信電話株式会社 ・株式会社 大塚商会 ・キヤノンITソリューションズ株式会社 ・伊藤忠テクノソリューションズ株式会社 ・新日鉄ソリューションズ株式会社 ・株式会社 日立システムアンドサービス ・株式会社PFU ・デル株式会社 ・大分シーイーシー株式会社 ・三菱電機インフォメーションシステムズ株式会社 ・株式会社紀伊國屋書店 ・ミラクル・リナックス株式会社
役 員	代表取締役　　小田切 耕司 技術取締役　　武田 保真		
オフィス	〒141-0022 東京都品川区東五反田1-12-10 三井住友海上五反田ビル6F Tel & FAX : 03-6670-5764		
Web	http://www.osstech.co.jp/		
設立	2006年9月		
資本金	1330万円		

OSSTech製品紹介

事例紹介

OSSTechの製品群（すべてOSSで提供）
原則Linux/Solaris/AIX共にRPMで提供

① Samba for Linux/Solaris/AIX

- ADの代替、高性能NASの代替

② OpenLDAP for Linux/Solaris/AIX

- 認証統合、ディレクトリサービス、シングルサインオンのインフラ

③ OpenSSO for Linux/Windows/Solaris

- Tomcat,OpenLDAP対応で高機能なシングルサインオン機能を提供

④ Unicorn ID Manager for Linux/Solaris

- Google Apps,ActiveDirectory,LDAP, Yahoo!メール Academic Edition に対応した統合ID管理

OSSTechの製品群（すべてOSSで提供）
原則Linux/Solaris/AIX共にRPMで提供

⑤ Chimera Search for Linux

- アクセス権の無いファイルは表示されない全文検索システム

⑥ LDAP Account Manager for Linux/Solaris

- 管理機能の弱いOSSのLDAP/SambaにWebベースのGUIを提供

⑦ SSLBridge for Linux

- リモートからのWindowsファイルサーバアクセス機能を提供

⑧ Mailman for Linux/Solaris

- Google Appsのメーリングリスト機能を補完

⑨ Netatalk for Linux/Solaris

- UTF-8に対応したMac OS対応のAFPファイルサーバー

① Samba for Linux/Solaris/AIX

- Samba 3.2 for Linux/Solaris/AIX
- クライアントはWindows7/Vista/2008およびMac OS Xに対応（もちろんWindows 2000/XPにも対応）
- JIS X 0213 (JIS2004) に対応 (UTF-8,UTF-8-Macにも対応）
- LDAPによるWindows,Unix,Linuxの認証統合
- Solaris / LinuxをWindows Active Directoryで認証統合（Kerberos認証に対応）
- 動作OS：Solaris10/RedHatEL5/CentOS5/AIX5,6対応
- Solaris ZFS対応でNFSv4 ACLによるNTFS互換ACL

OSSTech製Samba採用・導入事例

- **Samba for Linux導入事例**
  - **バッファロー株式会社様**
    テラステーション、リンクステーション
  - **スターティア株式会社様**
    セキュアSamba
    http://securesamba.digitalink.ne.jp/

- **Samba for Solaris10導入事例**
  - **北陸先端科学技術大学院大学様**

- **Samba for AIX導入事例**
  - **国立病院機構様**

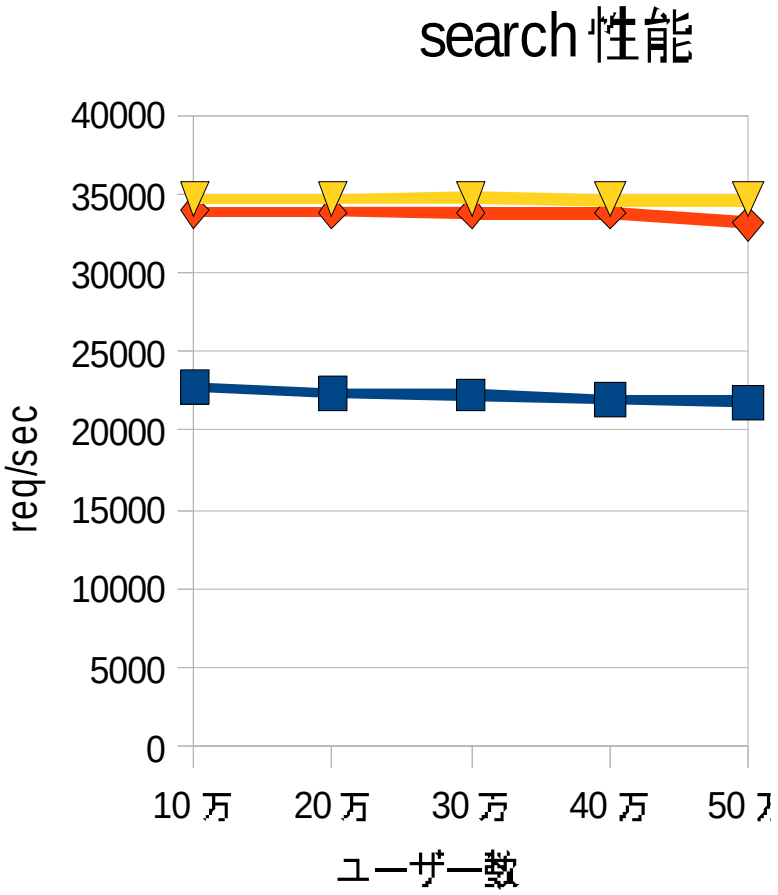
② OpenLDAP for Linux/Solaris

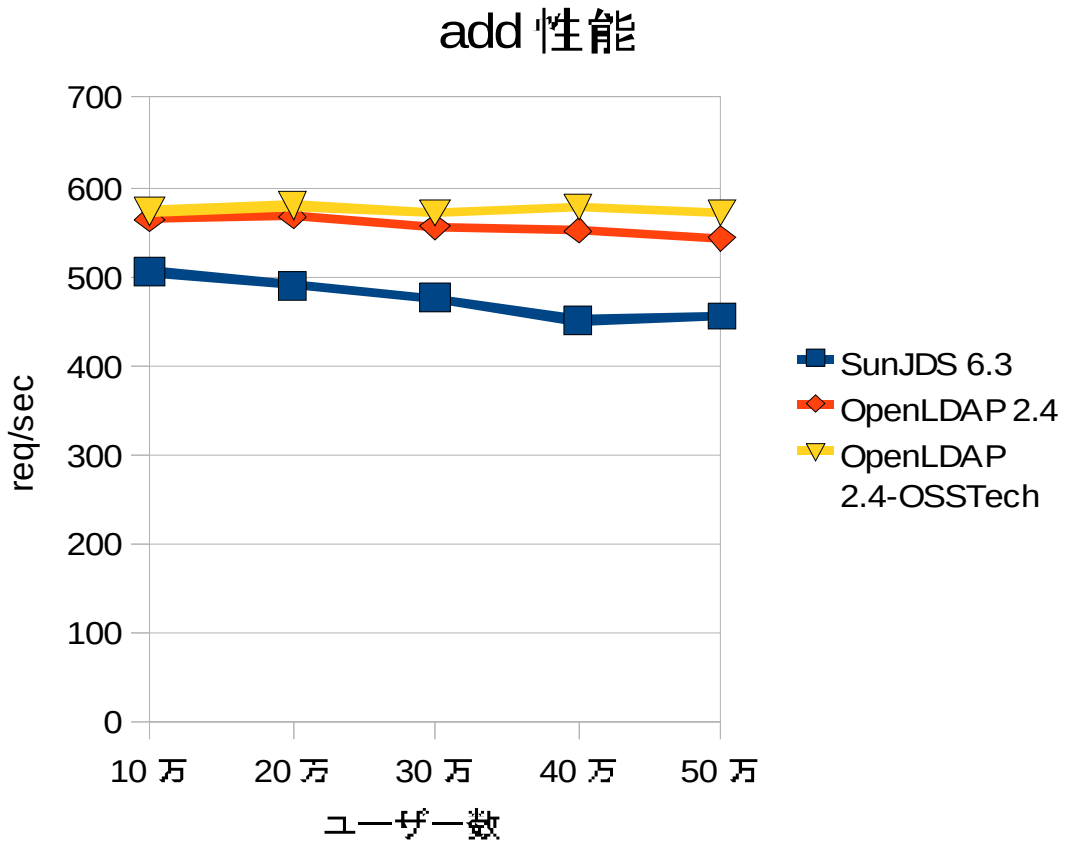
- OpenLDAP 2.4.19 for Linux/Solaris
  - マルチ・マスター対応（品質検証済み）
  - 50万ユーザでの安定動作を検証済み
  - キャッシュアクセスを独自改良し、高速化
  - １秒間に認証2万4千、検索3万4千
  - BDB4.8.24を採用し、高性能・高品質
  - 高速で安定したマルチマスタ・レプリケーション
  - Solaris10 / RedHatEL5 / CentOS5対応

商用LDAP製品の置き換えが可能

OSSTech製OpenLDAP vs 商用LDAP / オリジナルOpenLDAP

- **1秒間に検索3万4千、商用LDAP製品、オリジナルOpenLDAPより高速**

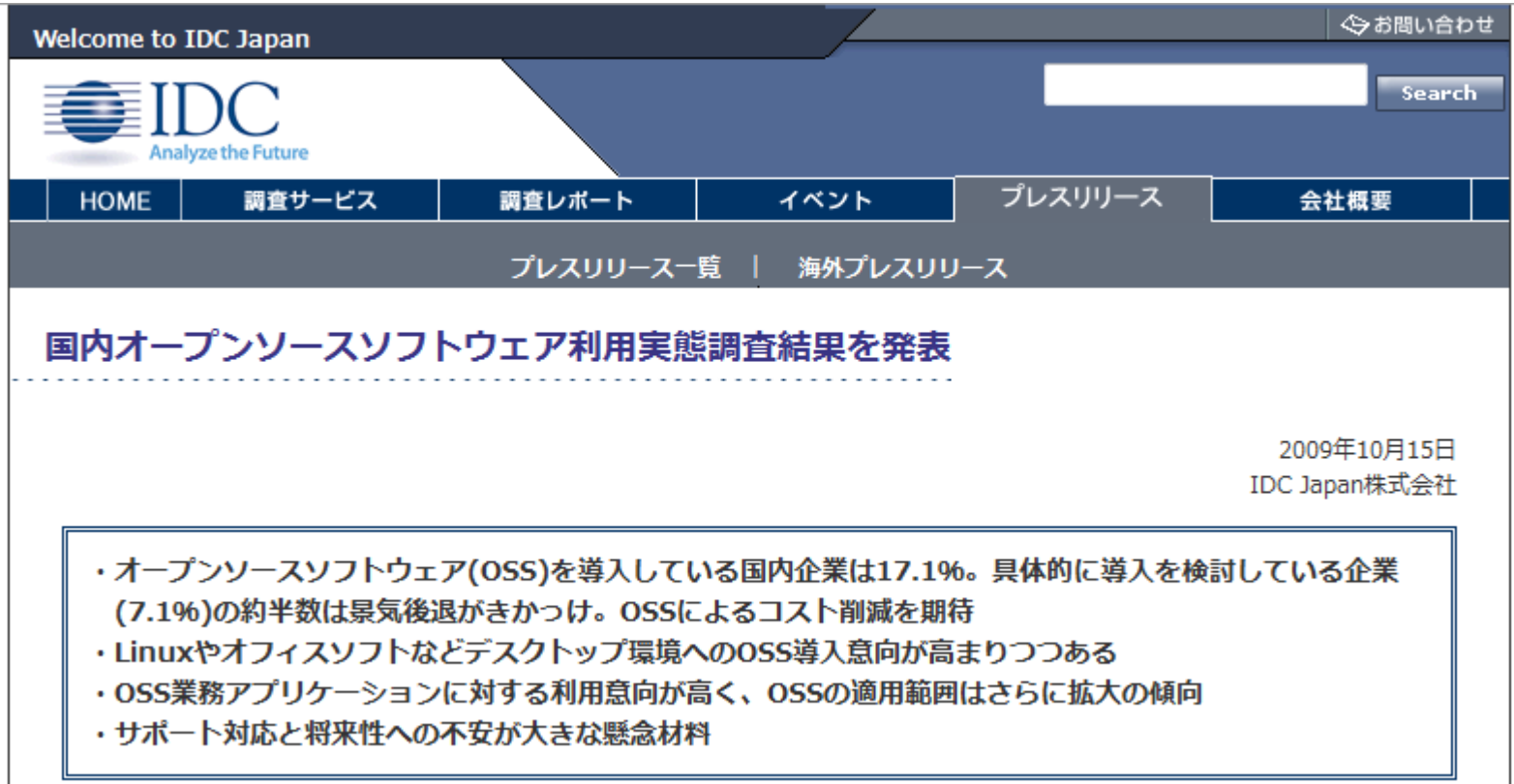




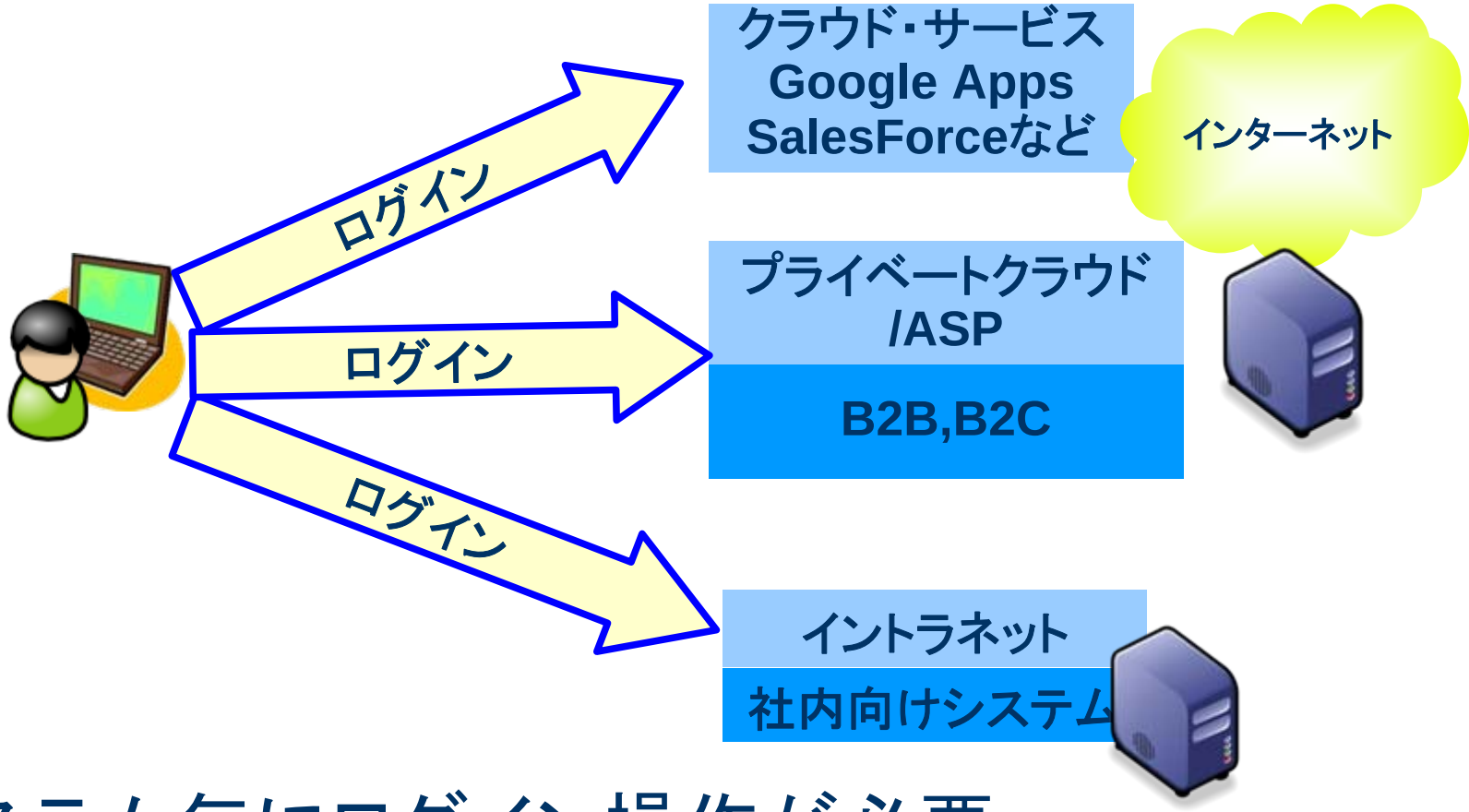
OSSで実現する
シングル・サイン・オンと
統合ID管理

クラウド・コンピューティングとOSSの普及

- 景気後退により、IT投資を含めたコスト削減が期待され、OSS(オープンソース・ソフトウェア)やクラウド・コンピューティングの導入が促進されています
- コスト削減が進む中、人員リストラも広がり、退職職員の情報持ち出しやシステムの不正利用防止のためのセキュリティ対策も急務となっています。



クラウドとイントラネットの混在化



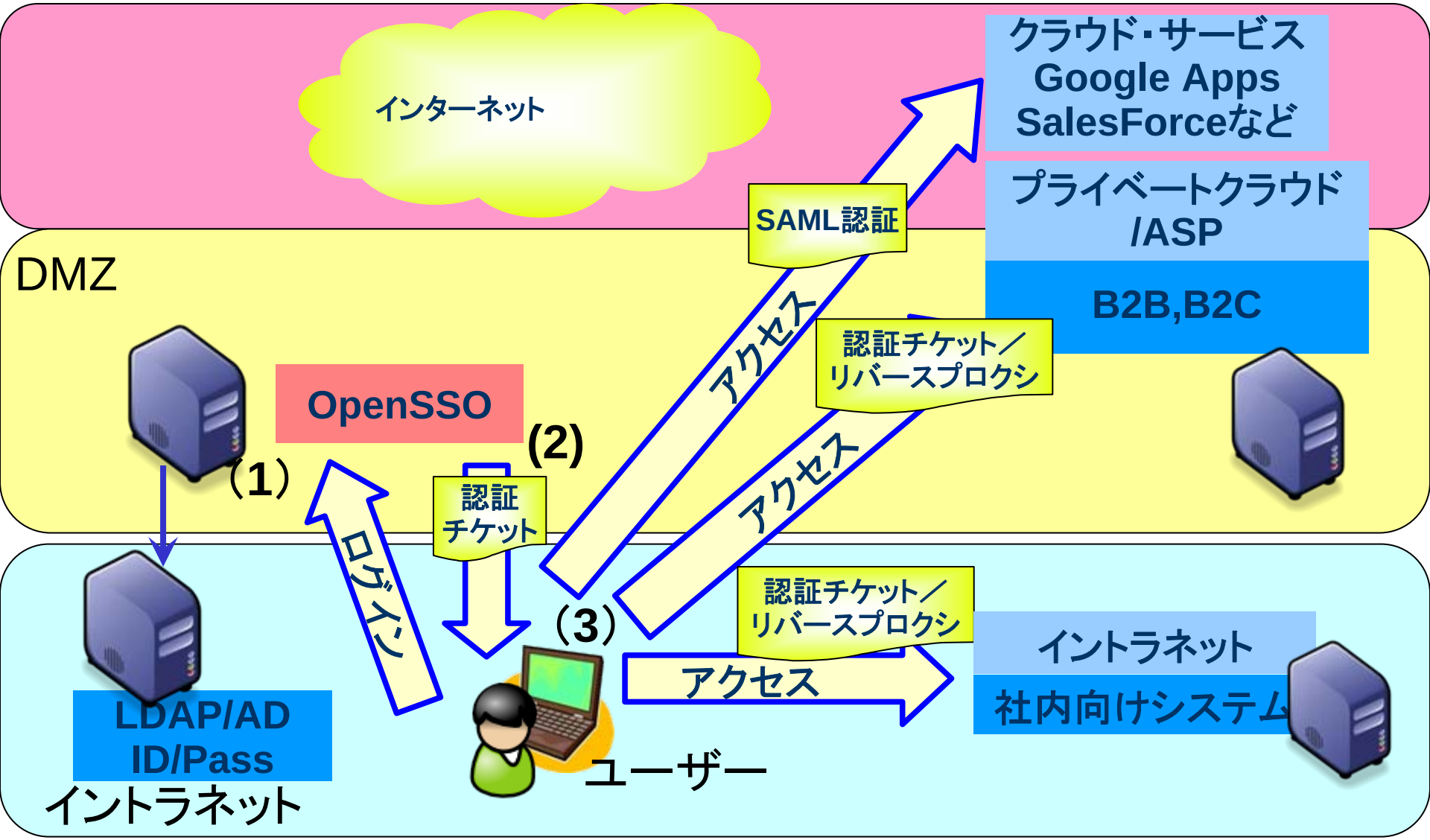
- システム毎にログイン操作が必要
- ID/パスワードも別々に管理する必要がある

SSOと統合ID管理の重要性

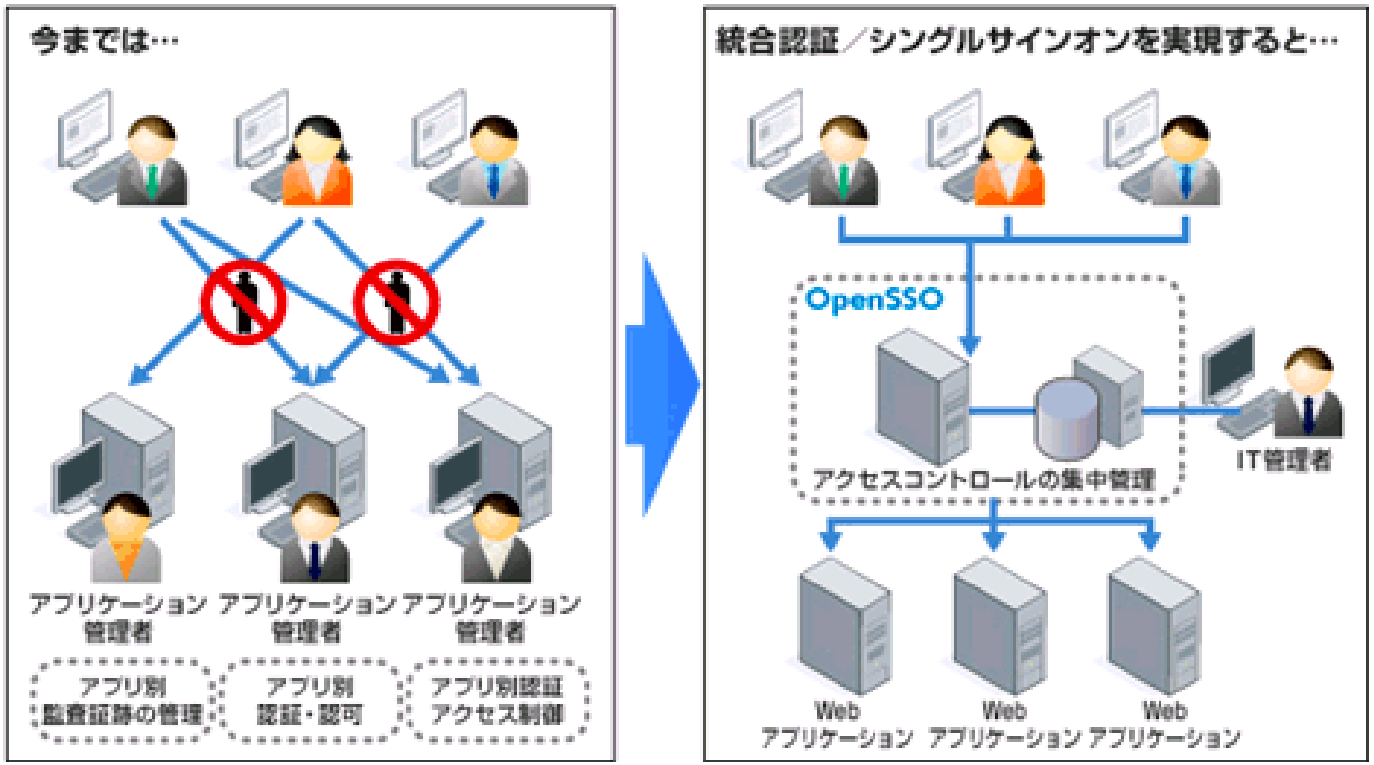
- Google AppsやSalesforceのような安価なクラウド・サービスの利用が促進
- 社内にもさまざまな業務アプリがあり、OSSで構築するケースが増えている
- J-SOX法の浸透により、企業の内部統制強化が進んでいます
- ITにおける内部統制強化の基本は「統合ID管理」や「SSO（シングル・サイン・オン）」
- 社内業務アプリとクラウド・サービスとのSSO連携が重要になってきています
- コスト削減が進む中、人員リストラも広がり、退職職員の情報持ち出しやシステムの不正利用防止のためのセキュリティ対策も急務となっています
- ID管理の強化、業務システムへのSSO（シングル・サイン・オン）機能の導入が進んでいます

➢ **SSOも統合ID管理もOSSで構築の時代へ！**

クラウドとイントラネットの融合化



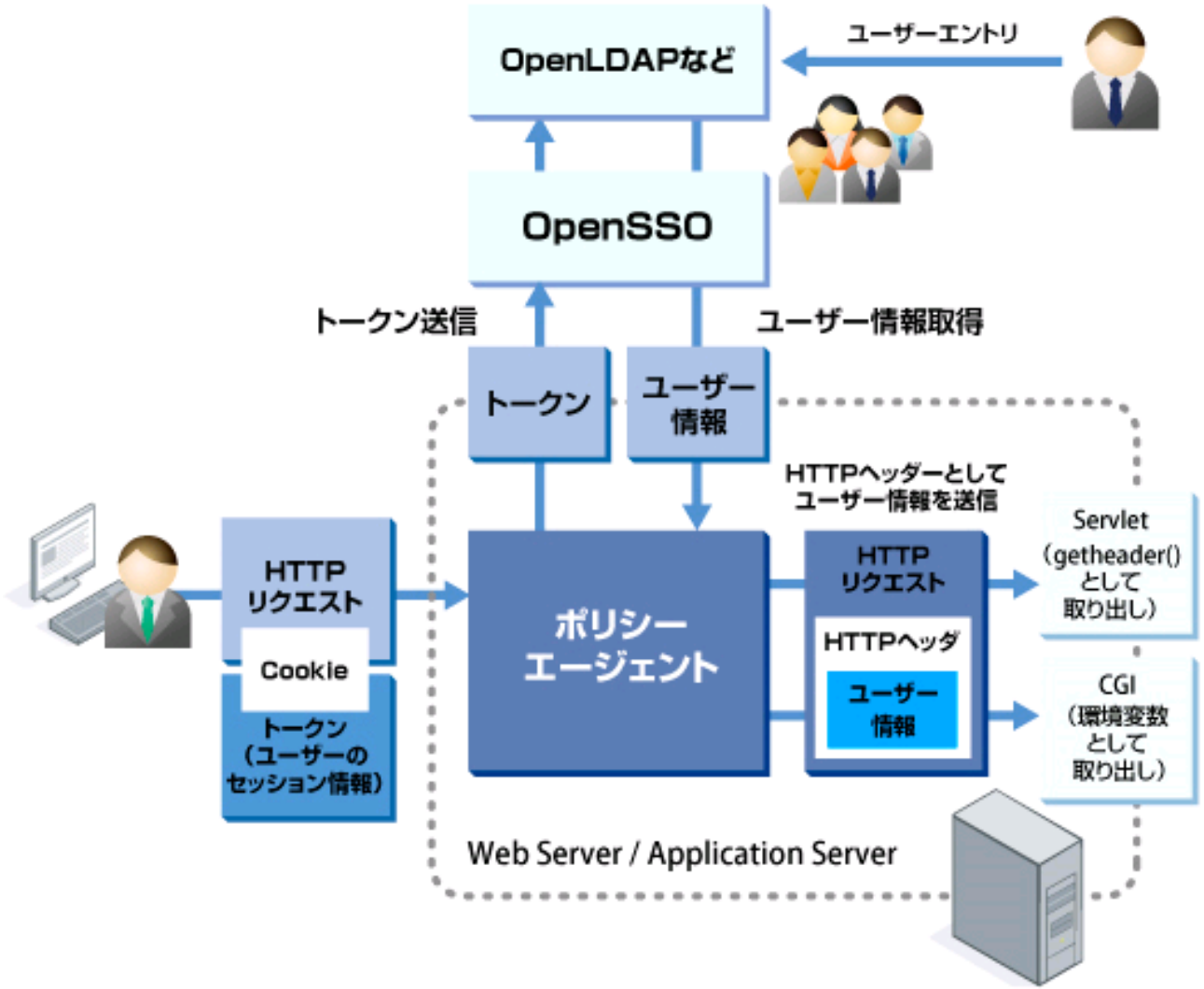
- 一度の認証で、複数システムが利用でき、利用者の利便性を向上。
- 複数システムにわたるユーザIDを統合管理し、統合IDによるアクセスコントロールを実現することで、セキュリティを強化。
- 商用製品は高額のため、導入の敷居が高かったが、オープンソースを利用することで、低コストで導入可能。



- OpenSSOとは、シングルサインオンを実現するオープンソース・ソフトウェアであり、特徴は以下のとおりです。

  - サン・マイクロシステムズが開発し、オープンソース（CDDLライセンス）として公開
  - 既に多くの導入実績がある、安定したソフトウェア
  - 業界標準の、以下の仕様をサポート
    - SAML 2.0　・・・　標準化団体OASISによって策定された、IDやパスワードなどの認証情報を安全に交換するためのXML仕様
    - XACML　・・・　XMLベースのマークアップ言語で、インターネットを通じた情報アクセスに関する制御ポリシーを記述するための言語仕様
    - WS-Federation・・・Webサービス環境下でID管理などを統合するための仕様

パターンA :エージェント型(チケット型)



エージェント型（チケット型）

http://sdc.sun.co.jp/javasystem/techtopics/identity/200806.html **より引用**

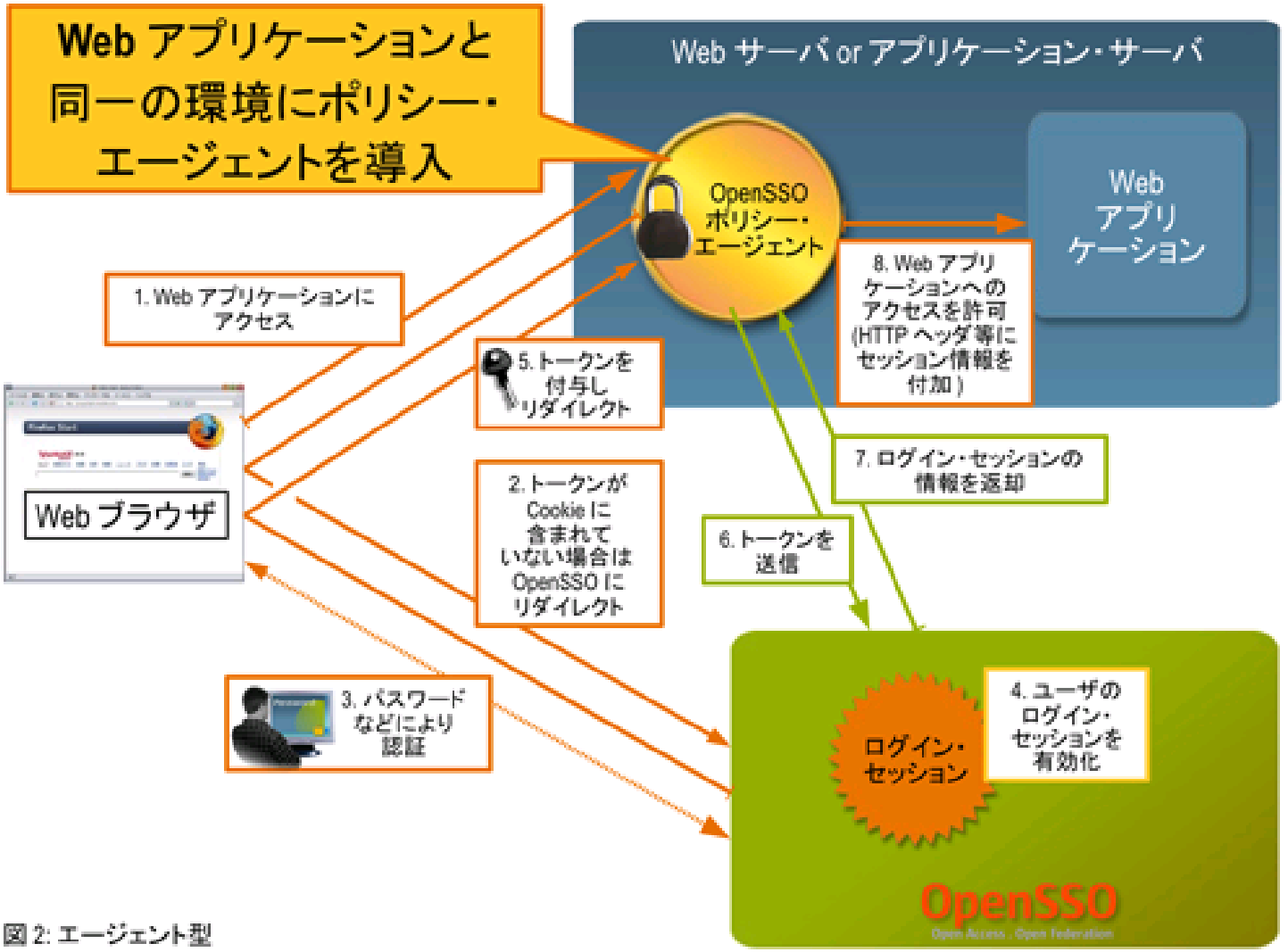
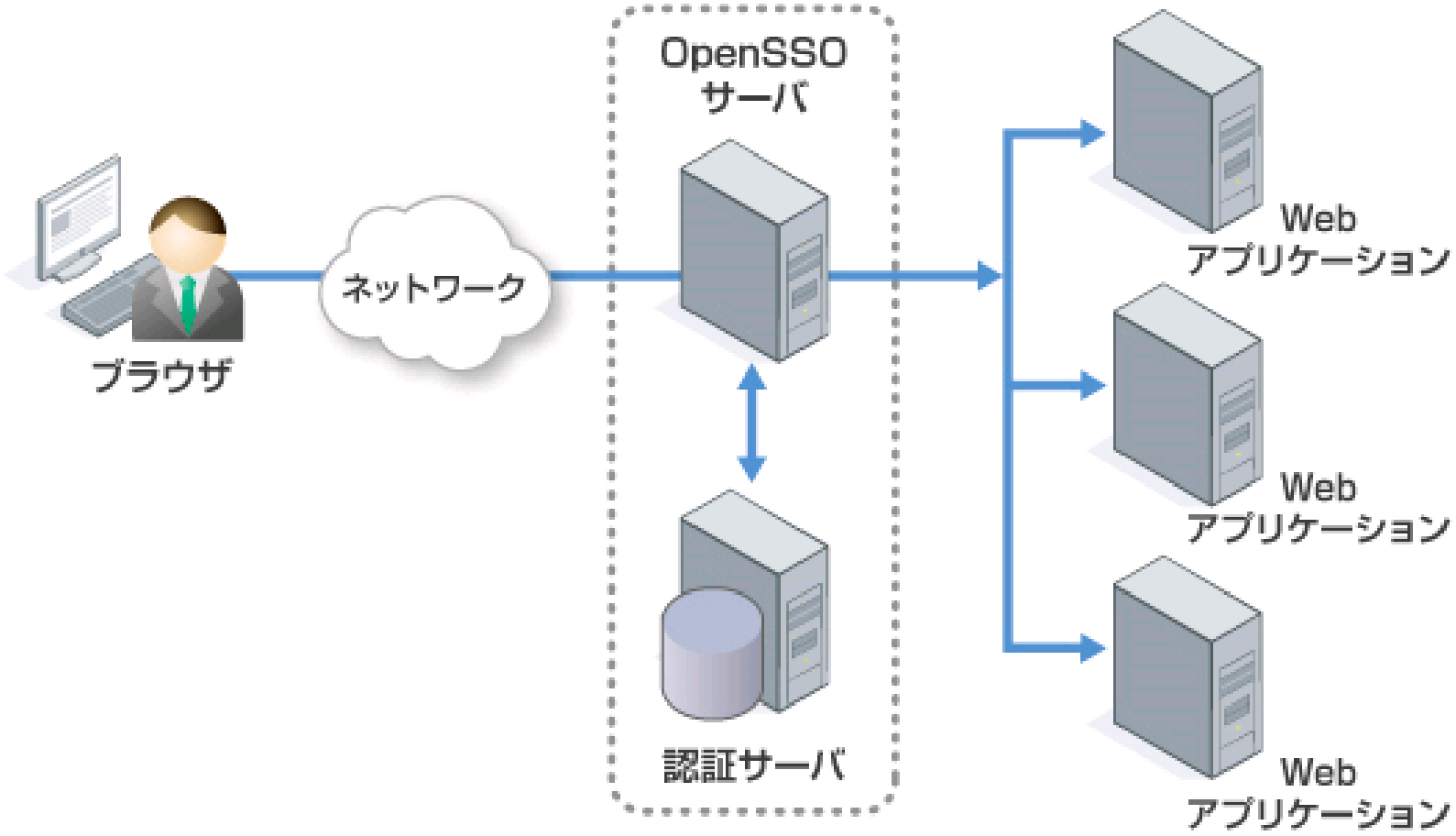


図 2: エージェント型

パターンB :リバースプロキシー型



http://sdc.sun.co.jp/javasystem/techtopics/identity/200806.html **より引用**

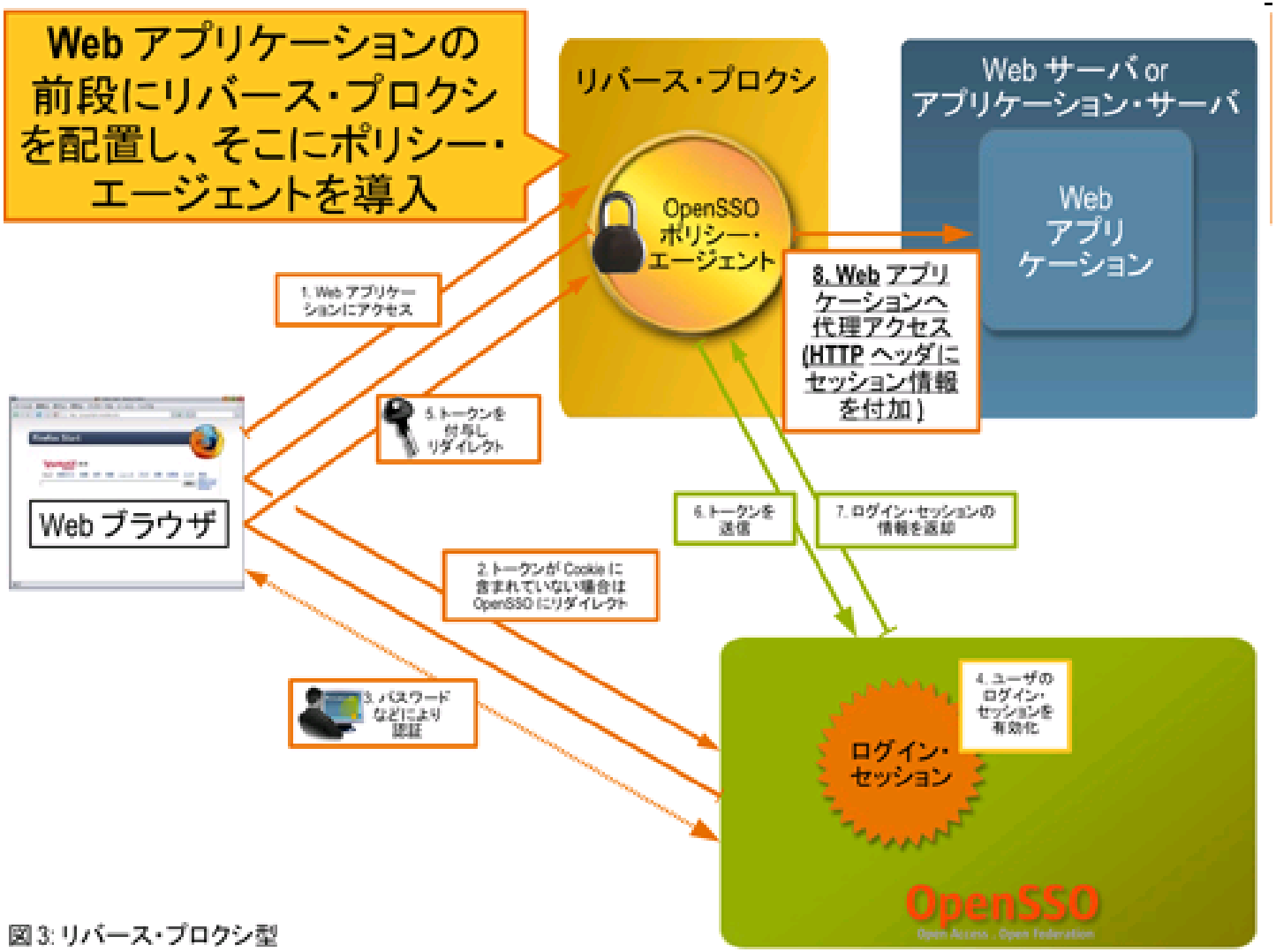
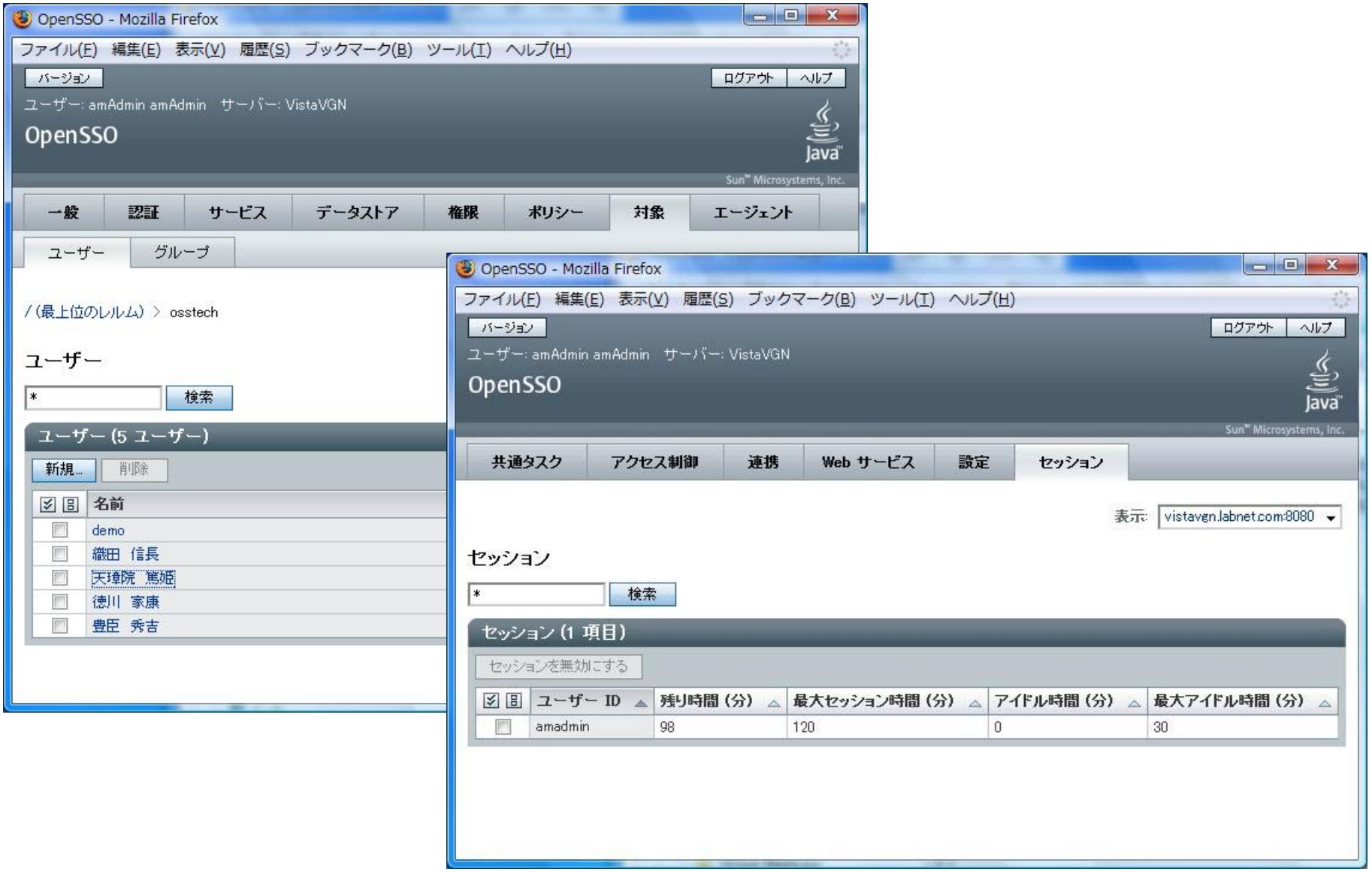


図 3: リバース・プロクシ型

OpenSSOの管理画面



SSO導入のメリット

- 一般ユーザ
  - ユーザID・パスワードをいくつも覚える必要がなくなる
  - ログインはOpenSSOに対して１回のみになる
- 開発者
  - 同じようなロジックを何度もアプリケーションに組み込む必要がなくなる
  - 暗号化やアクセス制御などの業務とは直接関係のないロジックに頭を悩ます必要がなくなる
- 管理者
  - 管理対象のユーザリポジトリが少なくなる
  - パスワード忘れへの対応が楽になる
  - 監視や監査が一箇所で行える

個別サービス・メニュー

- 日立指静脈認証方式追加サービス
  - 日立指静脈認証をOpenSSOの認証方式のひとつとして追加するサービスです。
    - 精度の高い方式による高いセキュリティを実現できます。
    - パスワードのように忘れる心配がありません。
    - アプリケーション毎の開発なしで指静脈認証が利用可能になります。
- Google Apps認証連携サービス
  - 弊社のGoogle Appsデータ連携サービスと合わせてご利用頂くサービスです。
    - 社内にあるOpenSSOサーバをIdP －アイデンティティ・プロバイダとすることにより、Google Appsへのシングル・サインオンが可能になります。
    - パスワード等の認証情報を社外に出す必要がなくなります。

③ OSSTech版　OpenSSO製品パッケージ

- OpenSSOサーバープラットフォーム
  - Red Hat Enterprise Linux 5 / CentOS 5
  - Windows Server
- 対応LDAPサーバー
  - OpenLDAPに対応（OpenSSO用スキーマを提供）
- 対応Webコンテナ
  - Apache Tomcat 6（Tomcatで発生する問題を解決済み）
- Policy Agent 動作環境
  - Apache HTTP Server
  - Apache Tomcat
  - Windows IIS (.Net)

Unicorn ID Manager
ユニコーンIDマネージャー

機能概要

Active Directory, OpenLDAP, Google Apps, Yahoo!メールなどのユーザーID管理を統合

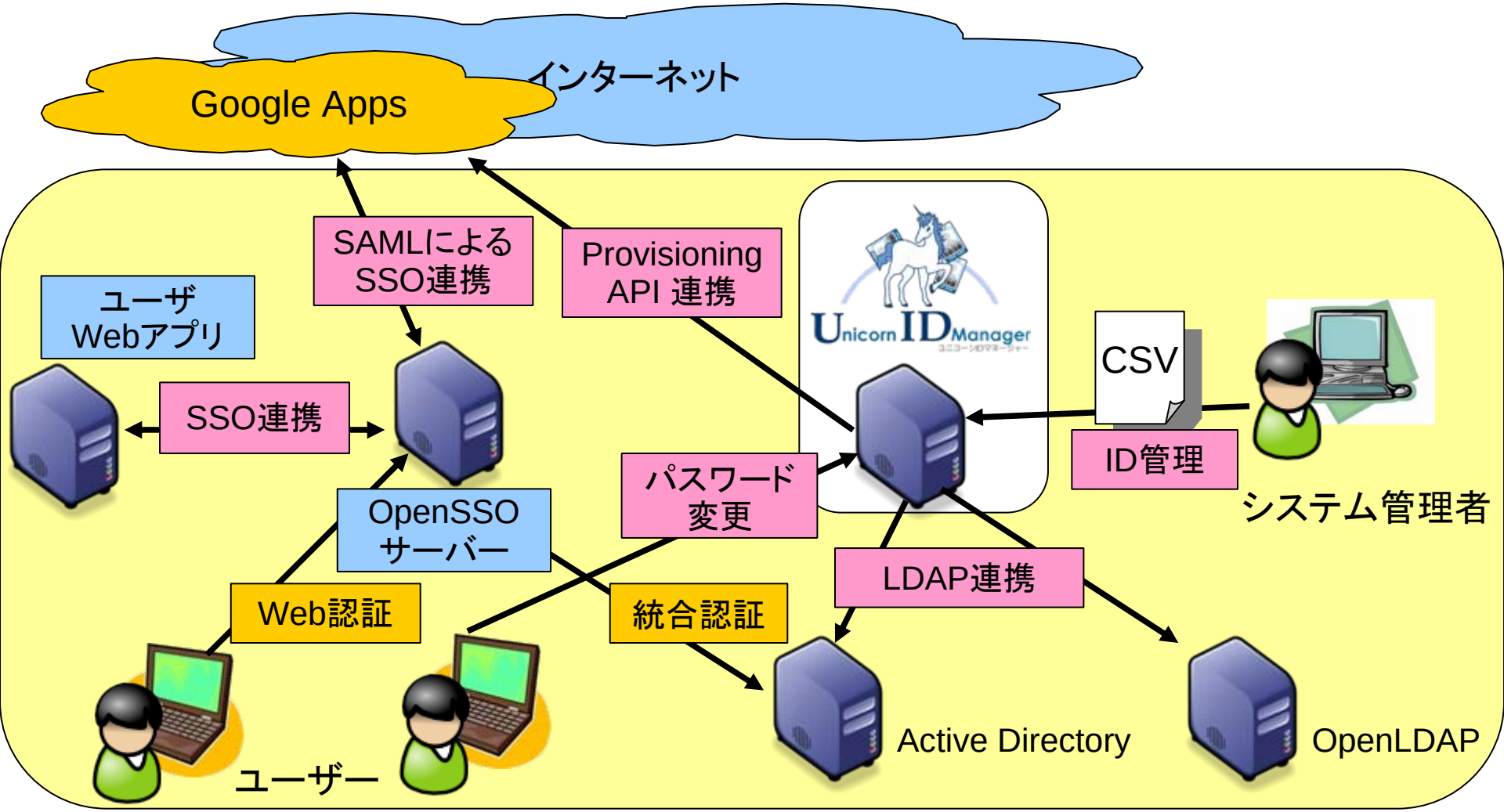
※Yahoo!メールのID連携についてはご確認ください

Webブラウザから、CSVファイルをアップロードして各種操作を実施

ユーザーのパスワード同期用Webサイトを提供

Unicorn ID Manager
ユニコーンIDマネージャー

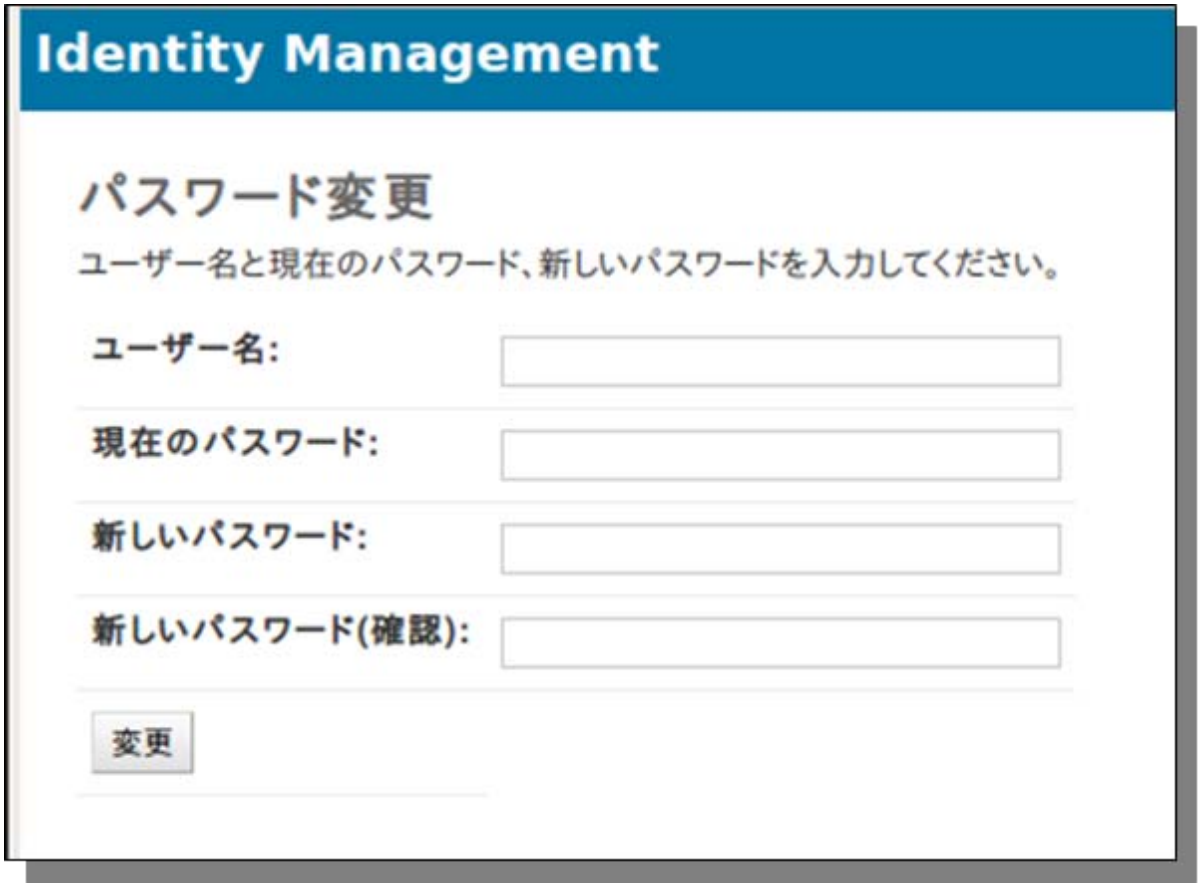
ActiveDirectory/LDAPとGoogle Appsを連携し、シングル・サイン・オンを実現



統合管理機能

- CSVファイルによるユーザー一括登録
- CSVファイルによるユーザー一括削除
- CSVファイルによるユーザー情報の一括更新
- CSVファイルによるユーザーの一括無効化
- CSVファイルによるユーザーの一括有効化
- 一般ユーザによる自分のパスワード変更
- 管理者によるユーザーパスワードの強制変更

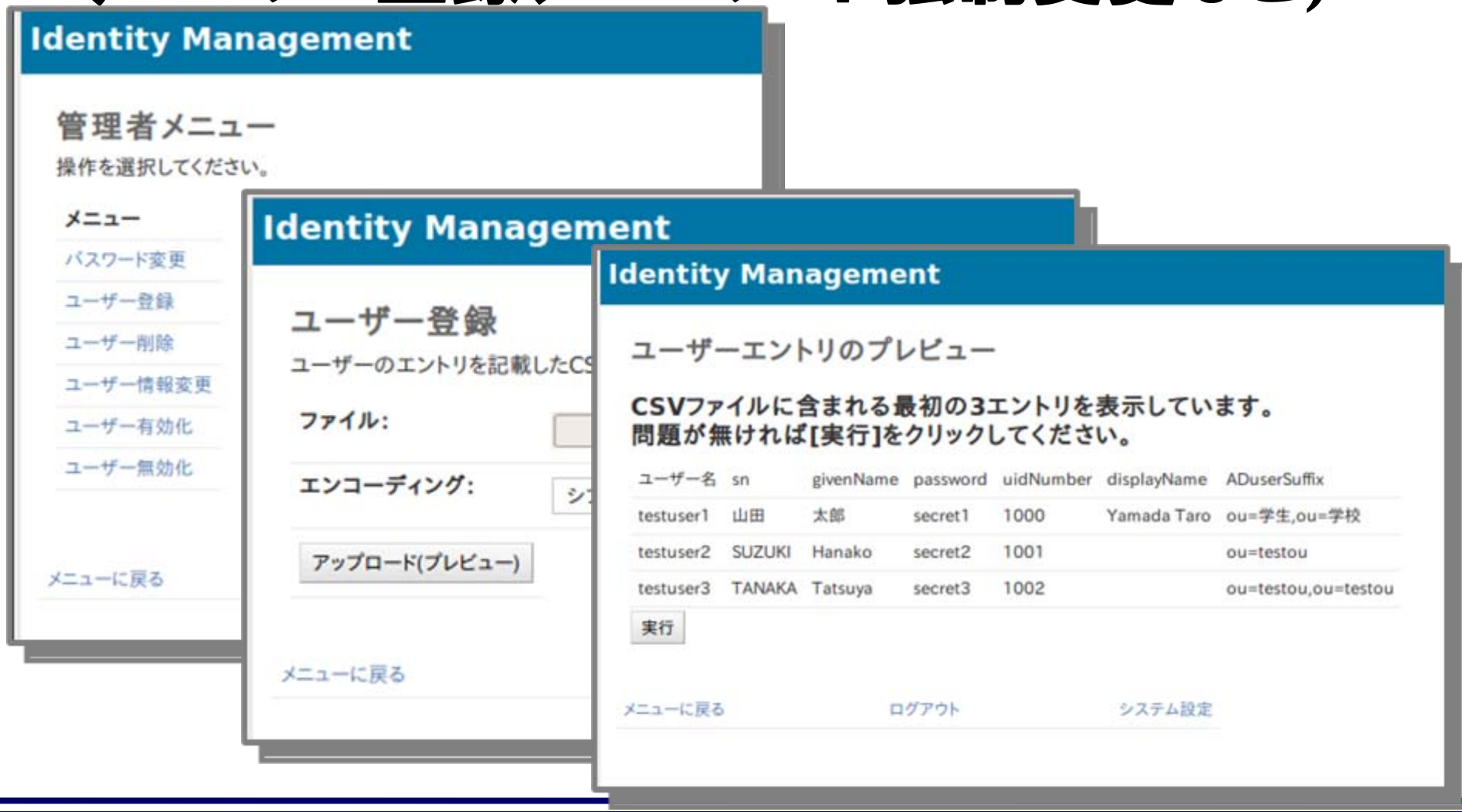
操作画面（パスワード変更)



一般ユーザーの
自分自身の
複数システムの
パスワードを
一括変更

* デザインはカスタマイズ可能です

管理者操作画面
（ユーザー登録、パスワード強制変更など）



OpenSSOのデモ

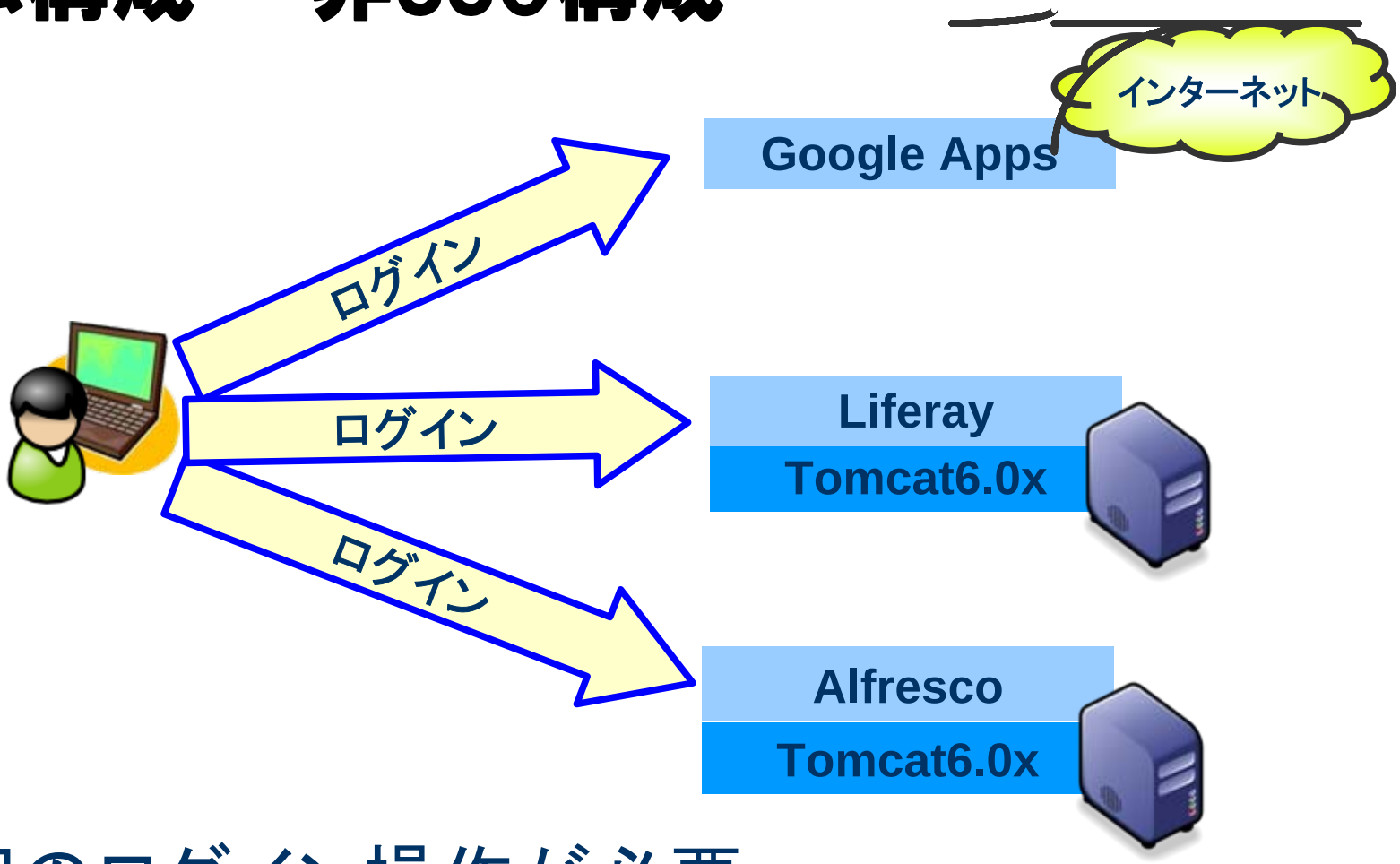
SSO導入のメリット

- 一般ユーザ
  - ユーザID・パスワードをいくつも覚える必要がなくなる
  - ログインはOpenSSOに対して１回のみになる
- 開発者
  - 同じようなロジックを何度もアプリケーションに組み込む必要がなくなる
  - 暗号化やアクセス制御などの業務とは直接関係のないロジックに頭を悩ます必要がなくなる
- 管理者
  - 管理対象のユーザリポジトリが少なくなる
  - パスワード忘れへの対応が楽になる
  - 監視や監査が一箇所で行える
- OpenSSOなら
  - SAML対応のGoogle AppsやBasic認証やForm認証のWebアプリもSSO可能

OpenSSOデモ：ソフトウェアはすべてOSS

- CentOS 5.3（Tomcat 6）
- OpenSSO 8.0
  - Sun Microsystem社により開発されたOSSのSSOソフト
  - AgentおよびReverse Proxy方式,OpenID,SAMLによるSSOを提供
- Liferay
  - オープンソースのEIP（企業向け情報ポータル）用ソフトウェア
  - OpenSSO向けのAgentモジュールが標準で付属
- Alfresco
  - オープンソースのECM（企業向けコンテンツ管理）用ソフトウェア
  - OpenSSO向けのAgentをOSSTechで開発

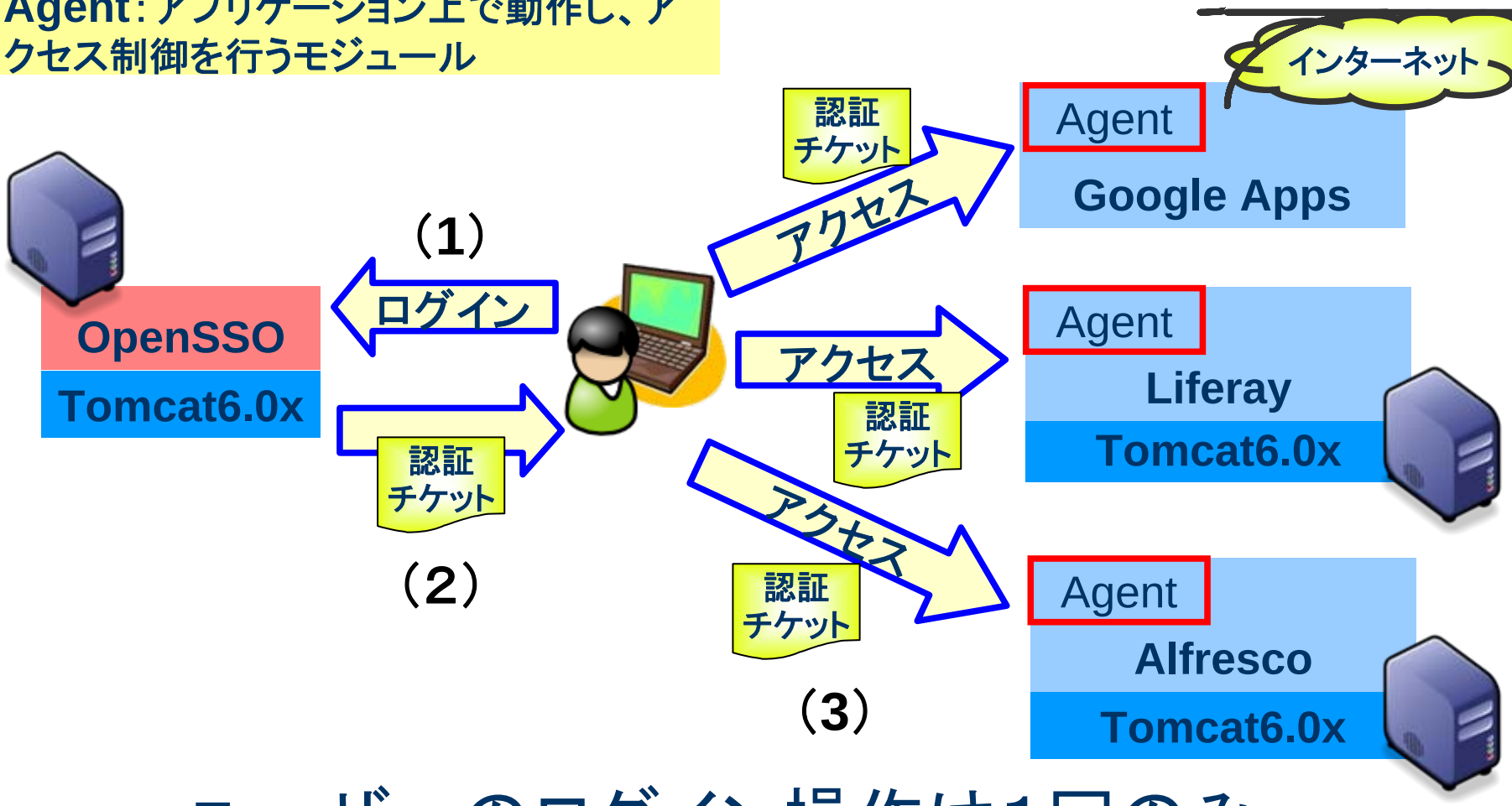
システム構成 - 非SSO構成



- 3回のログイン操作が必要
- ID/パスワードも別々に管理する必要がある

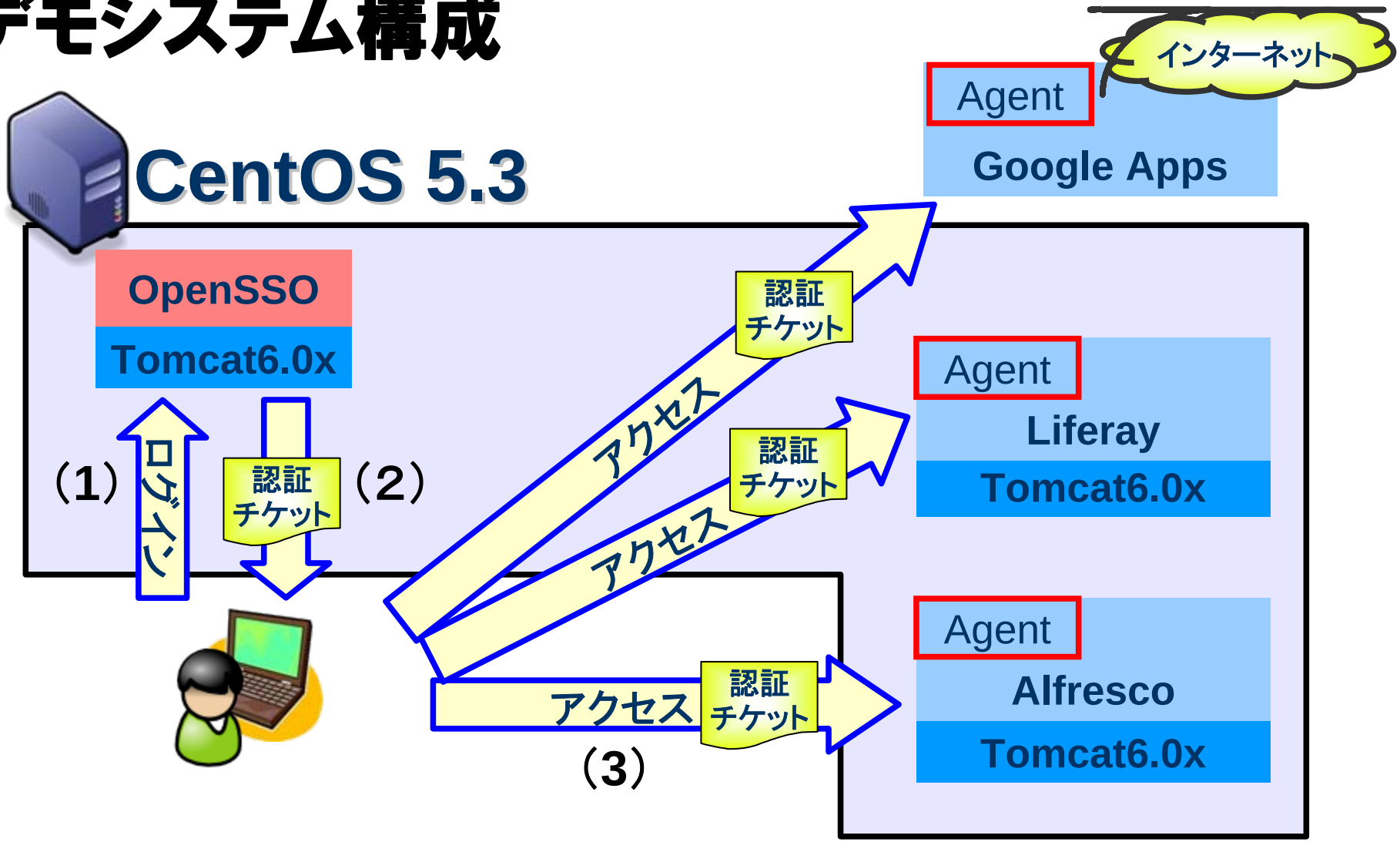
システム構成 － SSO構成(エージェント型)

Agent:アプリケーション上で動作し、アクセス制御を行うモジュール



- ユーザーのログイン操作は1回のみ
- ID/パスワードも一つだけ覚えればよい

デモシステム構成



1つのOSの中で3つのAPサーバを起動

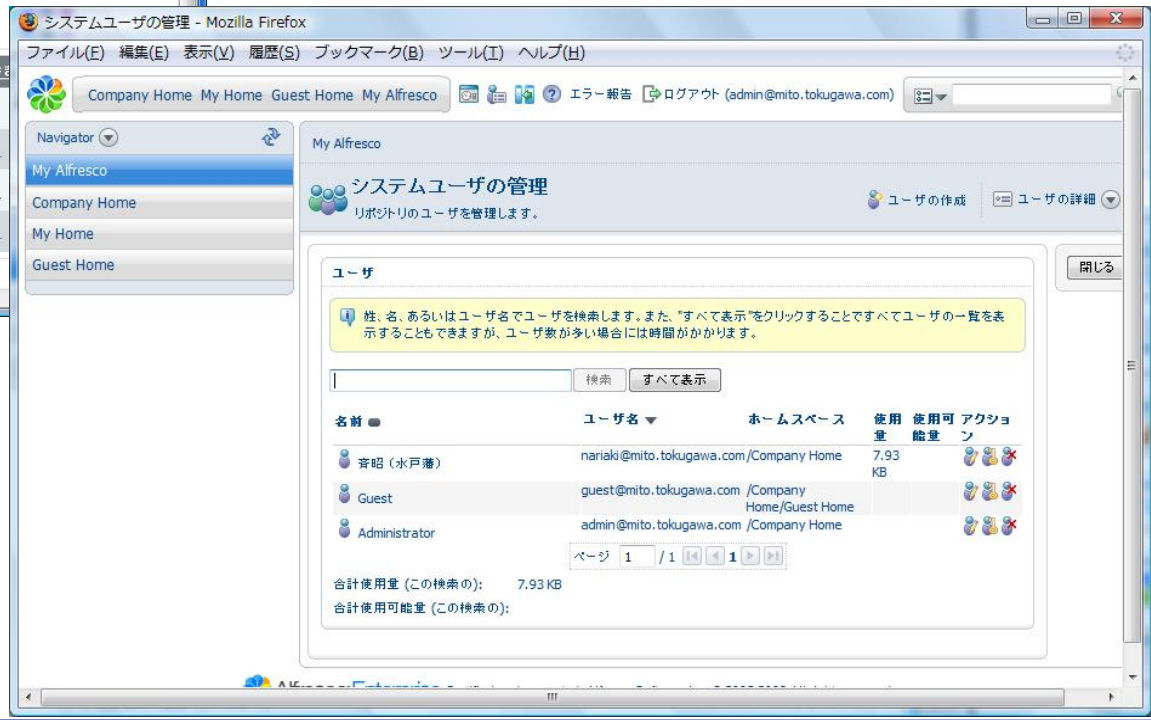
デモ概要

- シングルサインオン
  1. Google Apps/Alfresco/Liferayのいずれにログインする
  2. OpenSSOのログイン画面が表示される。ログインすると認証チケットが発行される。
  3. 他のアプリケーションにアクセス。このとき、ユーザーのログイン操作は不要（認証チケットを持っているため）
- シングルログアウト
  1. Alfrescoからログアウト
  2. Google Apps/Liferayからもログアウトしている

OpenSSO 管理コンソール

Liferay 管理コンソール

Alfresco: 管理コンソール

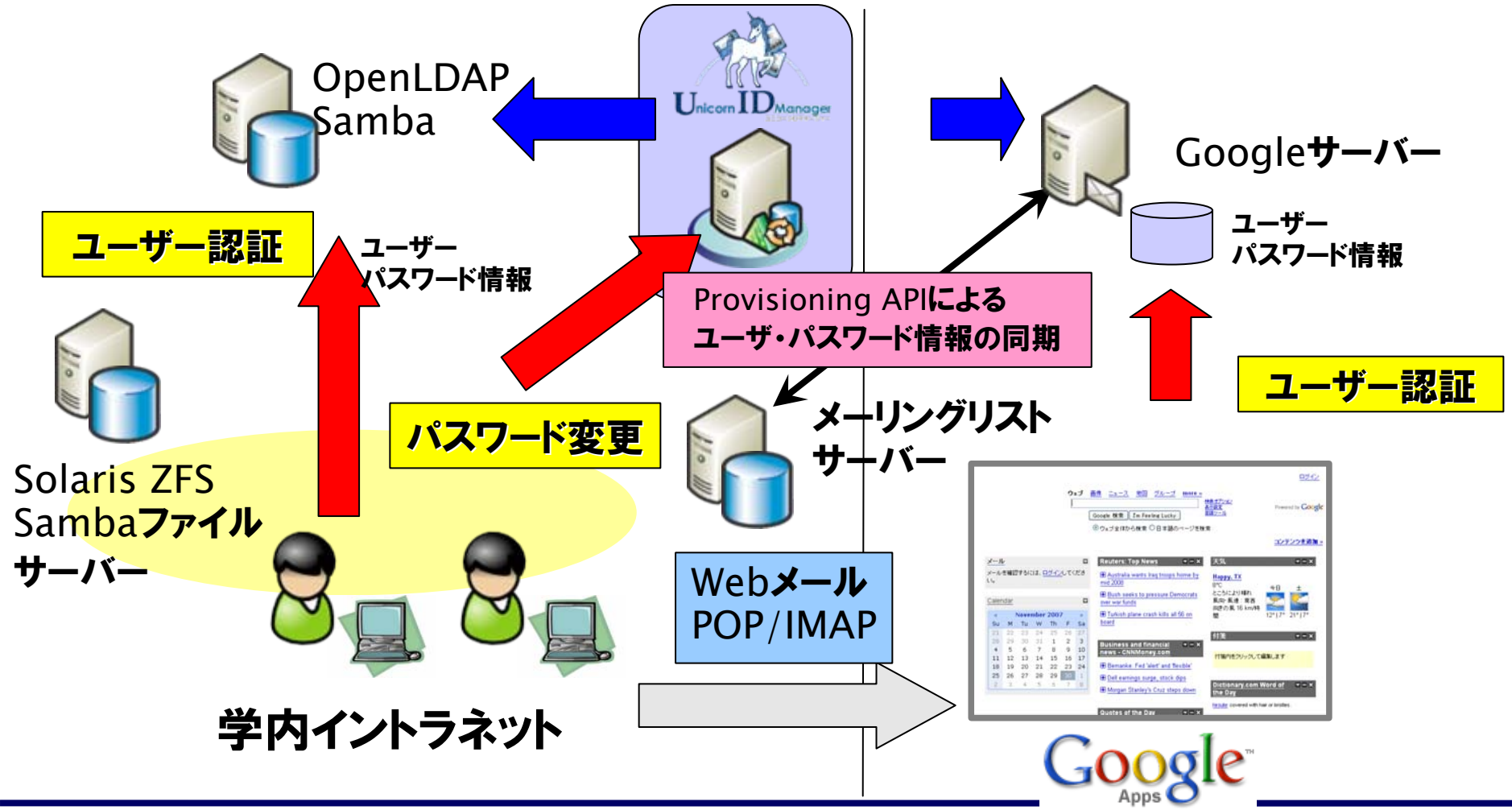


導入事例：湘南工科大学様

- メールシステムとしてGoogle Appsを採用
- OpenLDAP、SambaによるWindowsドメイン認証
- Solaris 10+ZFS+Sambaによるファイルサーバー構築
- Uncorn ID Managerを使ったSamba/LDAP/Googleユーザーの統合ID管理
- WebからのパスワードでLDAP/Samba/Google Appsのパスワードを一括変更

導入事例：湘南工科大学様

- Samba+LDAPによる認証サーバー、ファイルサーバー
- Unicorn IDMによるユーザーアカウントの認証統合

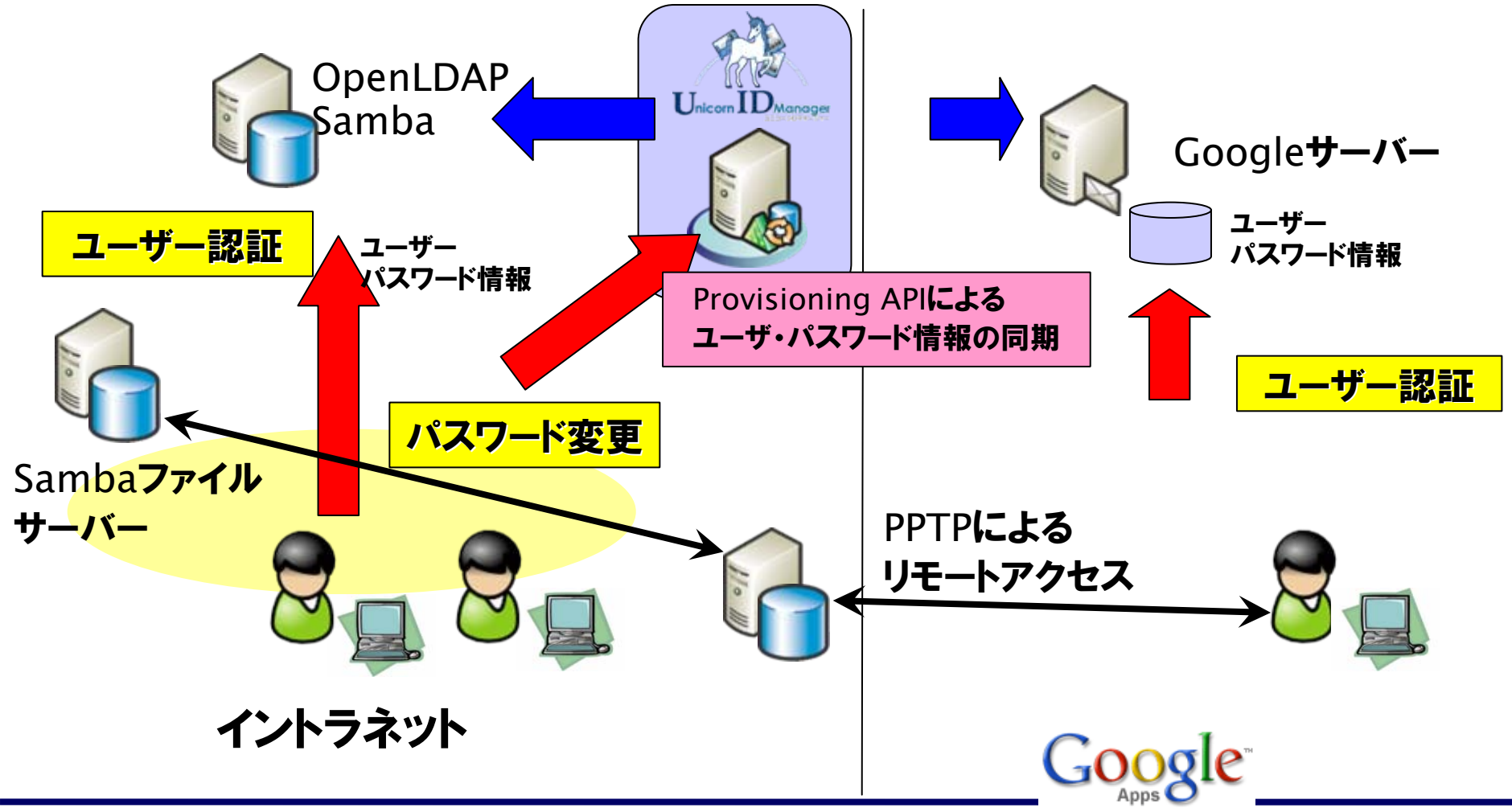


導入事例：株式会社ITコア様

- OpenLDAP、SambaによるWindowsドメイン認証
- Google Appsを利用中
- Uncorn ID Managerを使ったSamba/LDAP/Googleユーザーの統合ID管理
- PPTPを使ったリモートからの社内アクセス
  Windowsクライアントへ特別なプログラムインストールが必要ない
- サーバーはVMwareを使った仮想化によりコスト削減

導入事例：株式会社ITコア様

- Samba+LDAPによる認証サーバー、ファイルサーバー、PPTP（すべてVMware上）
- Unicorn IDMによるユーザーアカウントの認証統合



導入事例：北海道武蔵女子大学様

- Google Apps Education Edition導入
- Unicorn ID ManagerによるWindows Active Directoryドメインと Google Appsのユーザー一括管理
- メーリングリストサーバー(Mailman)の継続利用

導入事例：北海道武蔵女子大学様

Unicorn IDMによるユーザーアカウントの認証統合