

オープンソースで情報システムを刷新した 嘉悦大学様事例

ソフトウェア購入費用0でベンダー依存から脱却



OSSTech

オープンソース・ソリューション・テクノロジー株式会社
代表取締役 チーフアーキテクト 小田切耕司

お問い合わせ info@osstech.co.jp

目次

1. 講師紹介、OSSTech社紹介
2. 嘉悦大学様 事例紹介
3. Samba+LDAPによる認証統合
4. SSLBridgeによる学外からの
ファイルサーバアクセス
5. 全文検索システムキメラ・サーチ
6. Google Appsとの認証統合

講師紹介
オープンソース・ソリューション・テクノロジー
会社紹介

講師著作紹介

- ◆ 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)
 - 「壺: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月号
 - 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>



会社概要

会社名	オープンソース・ソリューション・テクノロジー株式会社	所属 団体等	<ul style="list-style-type: none"> Linuxコンソーシアム 理事 LPI-Japanビジネス・パートナー
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テクノロジー		
業務内容	<ul style="list-style-type: none"> ソフトウェアの企画、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 ソフトウェアに関する教育、研修、支援 	主要 取引先 および パートナー 様	<ul style="list-style-type: none"> デル(株) (株)野村総合研究所 サン・マイクロシステムズ(株) キャノンマーケティングジャパン(株) (株)バッファロー (株)大塚商会 日本電信電話(株) (株)博報堂 日本電気(株) 富士通ネットワークソリューションズ(株) 大分シーイーシー株式会社 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	〒141-0031 東京都品川区西五反田2-6-3 東洋ビル Tel & FAX : 03-6670-5764		
Webページ	http://www.osstech.co.jp/		
設立	2006年9月		
資本金	800万円		

オープンソース・ソリューション・テクノロジー株式会社

- **OSに依存しないOSSのソリューションを中心に提供**
 - Red Hat Linuxだけでなく、CentOSやSolaris , FreeBSD , Debianなどへも対応！
- **Samba、LDAPなどによる認証統合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
 - 技術コンサルティング提供
 - Samba導入・出荷実績日本一(世界一?！)

<http://www.osstech.co.jp>

オープンソースで情報システムを 刷新した嘉悦大学様事例

**ソフトウェアを購入しなければ
ベンダーに縛られない！**



OSSTech

嘉悦大学様 リプレース前の課題

- 情報システムすべてを某Slerにすべてお任せ
 - ベンダーに言われるままWindowsサーバ (Active Directory) を導入
 - メールサーバはSolaris8で構築
- ちょっとしたことを頼むのも高額な費用を請求される
 - Solaris 8のパッチ適用に数百万かかると言われ放置状態
- ベンダー任せ過ぎでセキュリティリスク増大
 - 分割されていないネットワークセグメント
 - 学外から簡単にアクセスできるWindows IIS/FTPサーバ
- **Slerが文教事業から撤退**
 - システムのメンテナンスが困難に
 - ネットワーク構成図すら存在しないことが判明
 - 詳しくは日経コンピュータ2007/12/24号に掲載

嘉悦大学様 新システムの目標

- **ベンダー依存からの脱却**
 - 3社によるコンペ
- **オープンな技術・製品を採用したい**
 - 新しい技術を安心して導入したい
 - 4年に一度はシステム更新
- **自分たちで運用できるシステム**
 - 運用コスト削減
 - ベンダーがいなくなっても大丈夫なように
- **OSS(オープンソース)を選択**
 - 製品を購入するからベンダーに縛られる
 - ソフトウェアを購入しなければベンダー依存から脱却できる
 - OSからミドルウェア、アプリケーションまで無償のOSSを採用

嘉悦大学様 情報インフラ基盤概要

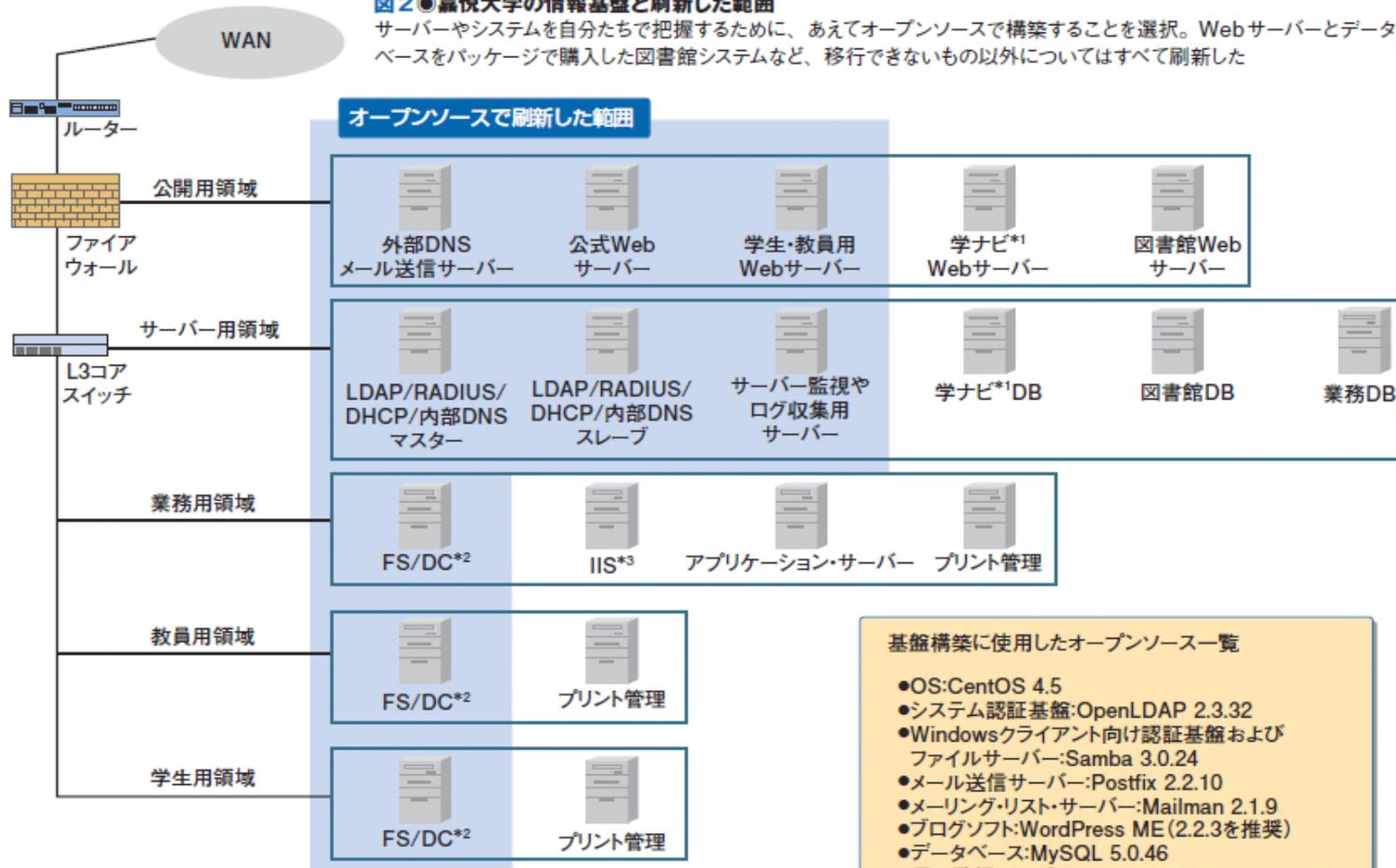
- オペレーティング・システム:CentOS 4.5 (無償のLinux OS)
- システム認証基盤:OSSTech製OpenLDAP 2.3 , FreeRADIUS
- Windowsクライアント向け認証基盤およびファイルサーバ:
OSSTech製Samba 3.0.24
- メール送信サーバ:Postfix
- メーリング・リスト・サーバ:Mailman (日本語パッチ適用)
- Webサーバ:Apache2 , PHP5 (CentOS Extraパッケージ)
- ブログソフト:WordPress ME (コミュニティ国際化版)
- 掲示板／情報共有:PukiWiki
- データベース:MySQL 5
- 運用監視サーバ:Nagios , Syslog-ng
- DNSサーバ:Bind
- サーバマシン:DELL PowerEdge2950を9台

嘉悦大学構築事例

日経コンピュータ
2007/12/24号

図2 ●嘉悦大学の情報基盤と刷新した範囲

サーバーやシステムを自分たちで把握するために、あえてオープンソースで構築することを選択。Webサーバーとデータベースをパッケージで購入した図書館システムなど、移行できないもの以外についてはすべて刷新した



- 基盤構築に使用したオープンソース一覧
- OS:CentOS 4.5
 - システム認証基盤:OpenLDAP 2.3.32
 - Windowsクライアント向け認証基盤およびファイルサーバー:Samba 3.0.24
 - メール送信サーバー:Postfix 2.2.10
 - メーリングリストサーバー:Mailman 2.1.9
 - ブログソフト:WordPress ME (2.2.3を推奨)
 - データベース:MySQL 5.0.46
 - 運用監視サーバー:Nagios 2.7, Syslog-ng 2.0.3
 - DNSサーバー:Bind 9.2.4
 - 全文検索システム:Hyper Estaler 1.4.10

*1 学ナビ:授業内容や学生の呼び出し情報などを提供する学生向けWebサイト
*2 FS/DC:ファイルサーバー/ドメインコントローラ
*3 IIS:Internet Information Services

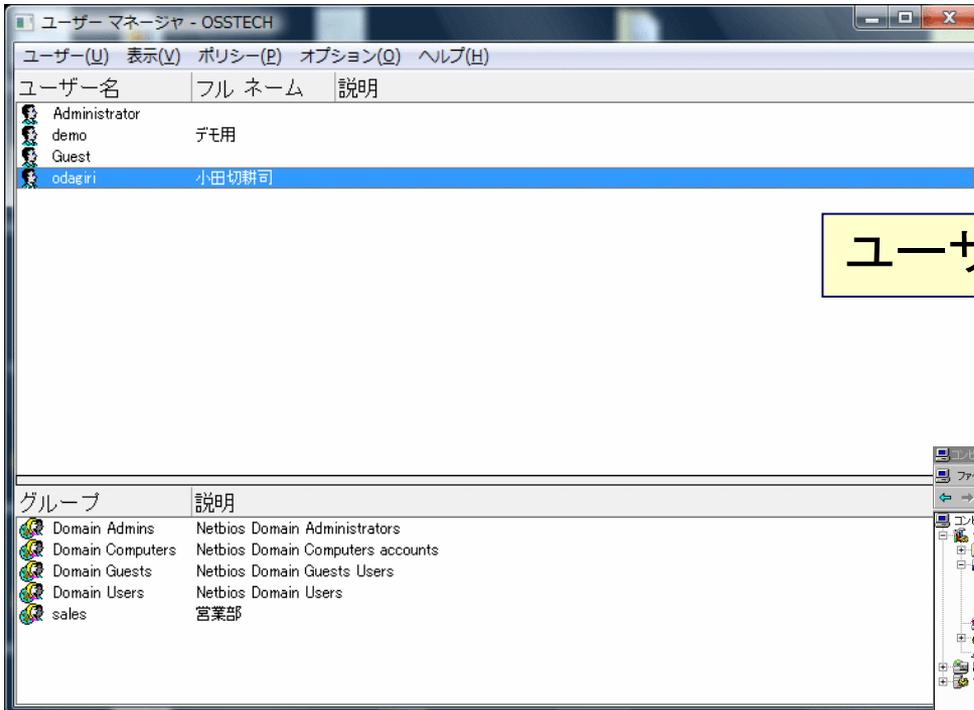
システム特徴、カスタマイズ項目

- (1) Windows Active Directoryの情報をSamba+LDAPへ移行
- (2) 無線LANやVPN、Javaアプリの認証をADからLDAPへ変更
- (3) ファイルサーバ用 全文検索システムを検索エンジンHyper Estraierをベースに開発、アクセス権で検索結果を制御
→Chimera Search(キメラ・サーチ)として製品化
- (4) 学生向けに学外からのファイルサーバアクセス機能を提供
→SSLBridgeを提供
→マスターブラウザがクライアントに奪われる問題が出たため
SSLBridgeを改良
- (5) Gmailとの連携、認証統合

(1) Windows Active DirectoryからSamba+LDAPへ移行

- SambaのVampire機能を使ってWindows Active Directoryの情報を移行
 - net vampireコマンドだけで1万以上のユーザを一括移行
 - ただし、クライアントはドメインに再参加
 - DC検索方式はドメイン参加時に決定されるため
 - スクリプトを用意してドメイン再参加を簡単にした
 - netdomコマンドはUNCで実行できないのでvbsを作成
 - ドメイン参加権限を学生を含め全員に付与
- すべてのWindowsクライアントの認証をSambaで統合
- Linux/UNIXマシンの認証はLDAPで統合
 - Solaris 8をLDAP認証にするにはパッチが必要
- VPNの認証はFreeRADIUS経由でLDAP認証
- Java APサーバ (ColdFusion) の認証もADからLDAPへ変更

Windows GUIでSambaが管理



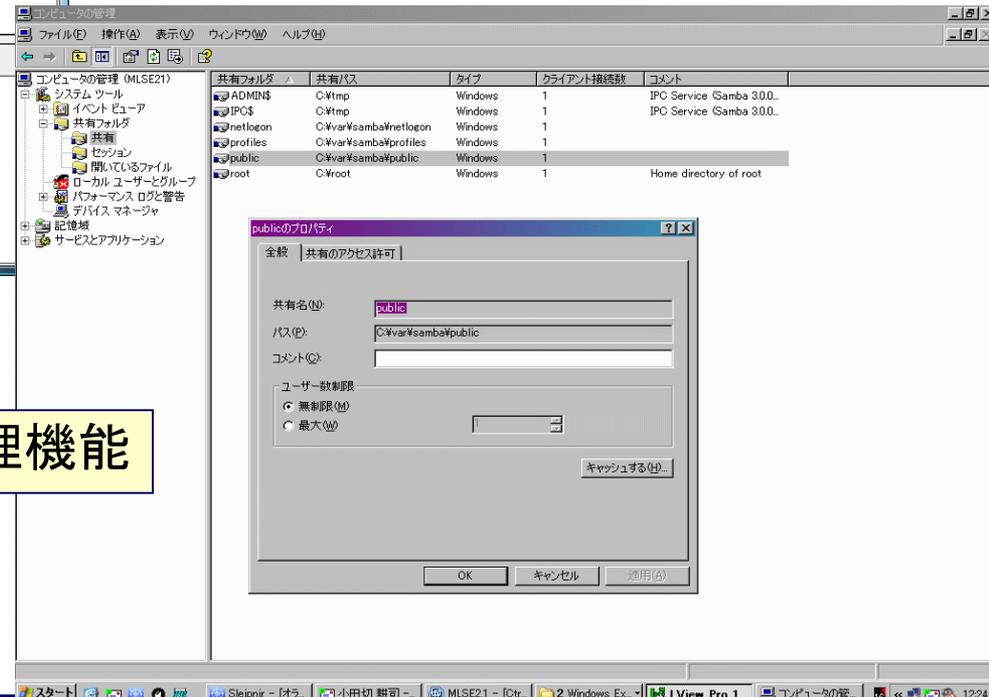
ユーザーマネージャ - OSSTECH

メニュー: ユーザー(U) 表示(V) ポリシー(P) オプション(O) ヘルプ(H)

ユーザー名	フルネーム	説明
Administrator		
demo	デモ用	
Guest		
odagiri	小田切 研司	

グループ	説明
Domain Admins	Netbios Domain Administrators
Domain Computers	Netbios Domain Computers accounts
Domain Guests	Netbios Domain Guests Users
Domain Users	Netbios Domain Users
sales	営業部

ユーザ管理機能



コンピュータの管理

共有フォルダ

共有フォルダ	共有パス	タイプ	クライアント接続数	コメント
ADMIN\$	C:\tmp	Windows	1	IPC Service (Samba 3.0.0..)
IPC\$	C:\tmp	Windows	1	IPC Service (Samba 3.0.0..)
netlogon	C:\var\samba\netlogon	Windows	1	
profiles	C:\var\samba\profiles	Windows	1	
public	C:\var\samba\public	Windows	1	
root	C:\root	Windows	1	Home directory of root

publicのプロパティ

全般 | 共有のアクセス許可

共有名(N): public

パス(P): C:\var\samba\public

コメント(C):

ユーザー数制限

無制限(M)

最大(M) []

キャンセルする(B)...

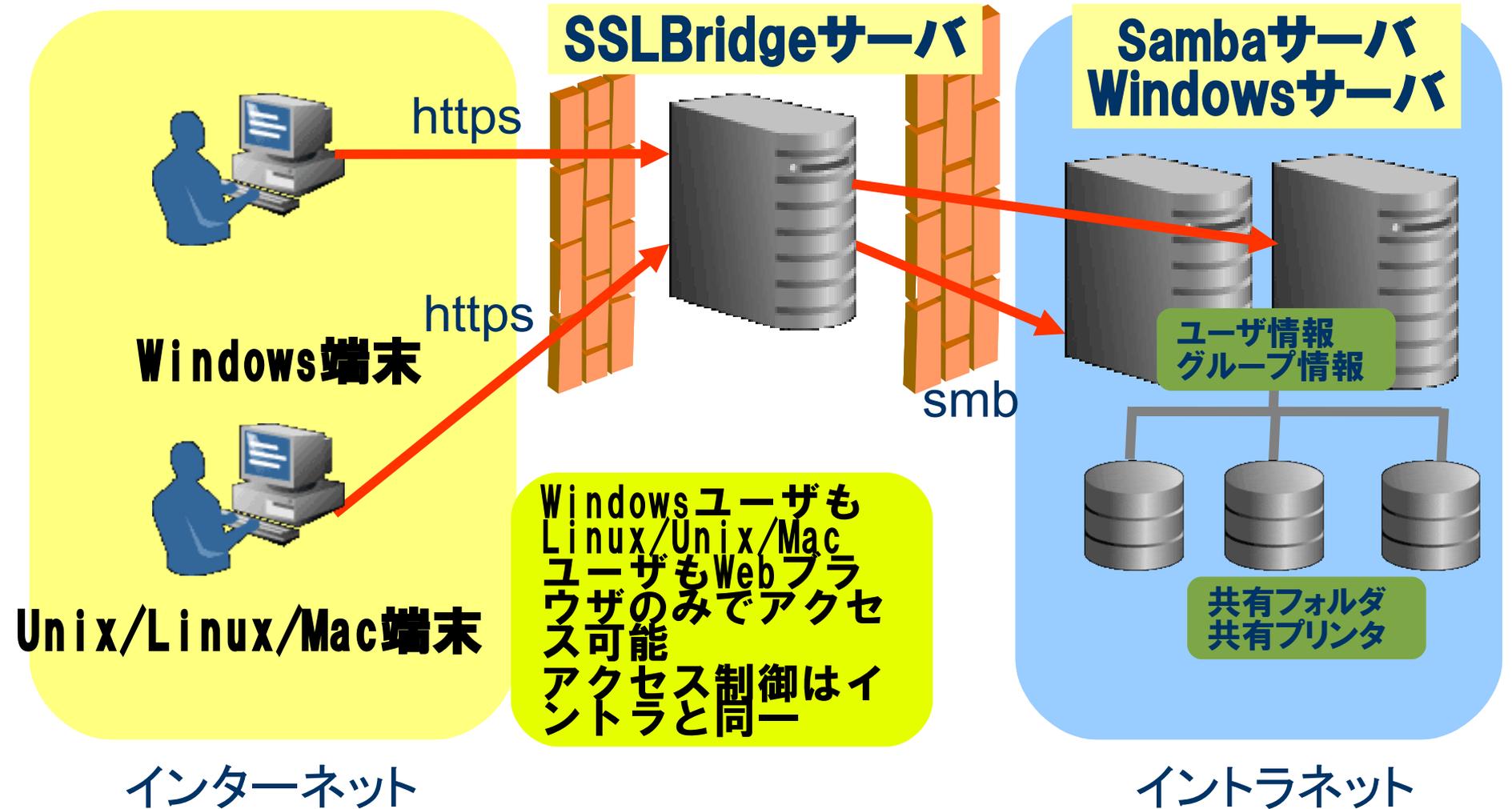
OK キャンセル 適用(A)

共有管理機能

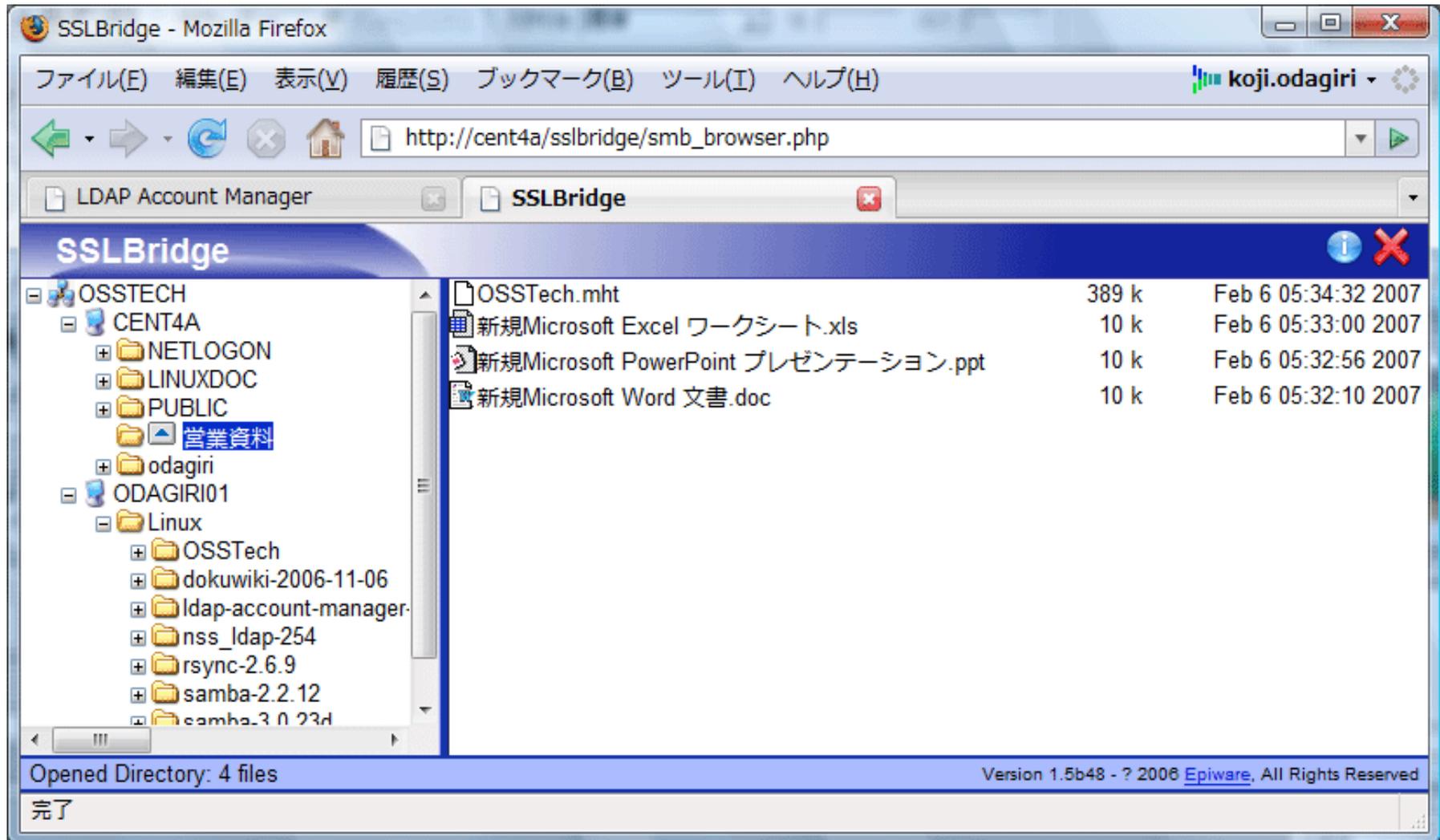
OpenLDAP 2.3 for Solaris/Linux

- CentOS4/RHEL4に付属するOpenLDAP2.2は品質が悪く大規模では運用できない
- デフォルトでOpenLDAP2.2は最大1024しか同時接続できないがOSSTech製は1万6千接続まで拡張
- BDBを最新化し、DBが壊れたり、リカバリできない不具合を修正
- クライアントに比例するライセンス費用がないため、大規模システムでも低コストで構築・運用可能

SSLBridgeによるリモートアクセス



SSLBridge : Windowsファイルサーバへ Webブラウザでアクセス



オープンソースの全文検索システム

Chimera Search: キメラ・サーチ

Windowsファイルサーバーのアクセス権対応
アクセス権のないファイルは検索結果に表れない



Chimera Searchとは

- SMBプロトコル、CIFSプロトコルをサポートしたサーバーであればWindowsマシン、Linux/UNIX/Mac OSマシンのコンテンツを検索できます。
- 検索結果にユーザーがアクセス権を持たないファイルは表示されません。

ファイルにアクセス権を適切につけておけば、検索でファイルの存在自体を知られる心配がありません。

- 構築コンポーネントに以下のOSS(オープンソースソフトウェア)を利用しているため、安価に導入できるのに高性能・高機能を発揮します。
 - プログラム言語: RubyおよびRuby On Rails
 - 全文検索システム: Hyper Estraier
以下の特長を持っています。
 - インデックスを使った高速な検索ができます。
 - 大量の文書のインデックスを短時間で作成できます。
 - N-gram方式による漏れのない検索ができます。

製品仕様

● 検索対象サーバー

- Windowsファイルサーバー
- Sambaベースのファイルサーバー

● 検索対象ファイル

Chimera Searchはファイルサーバー内の以下のファイルを検索できます。

- マイクロソフトオフィス Wordファイル
- マイクロソフトオフィス EXCELファイル
- マイクロソフトオフィス PowerPointファイル
- OpenDocument ファイル (OpenOffice.org, Sun StarSuite)
- PDFファイル、HTMLファイル、テキストファイル

● インストール要件

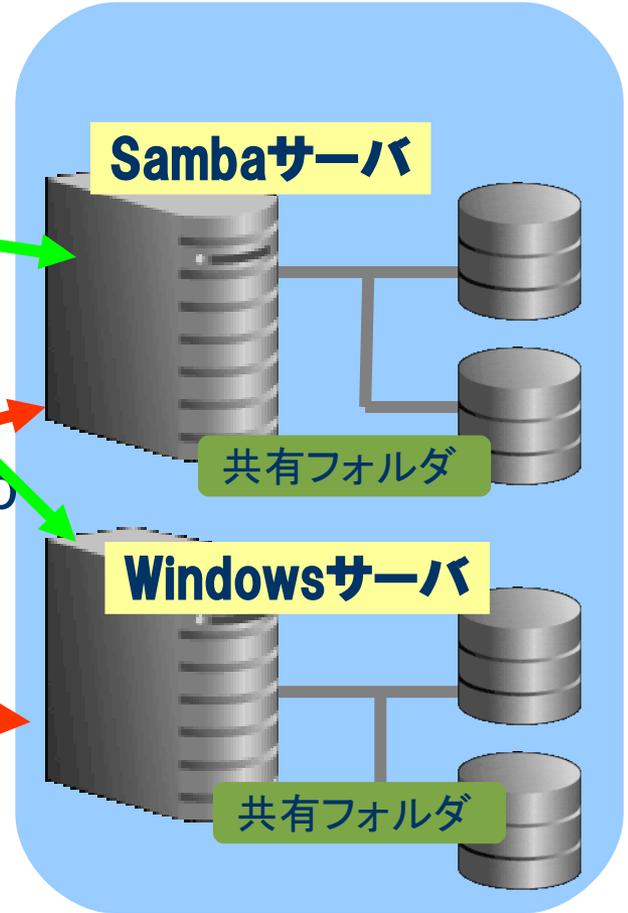
Chimera Searchは以下のOSが稼働するマシンの上で動作します。

- Red Hat Enterprise Linux 5.0 / 4.0
- CentOS 5 , 4

キメラ・サーチ概要図

- 定期的にファイルサーバをアクセスし、インデックス作成
- 2回目以降は更新のあったファイルのインデックスのみ再作成
- アクセス権のないファイルは検索結果に表示しない

キメラ・サーチ
サーバ
(Sambaサーバ
と共存可能)



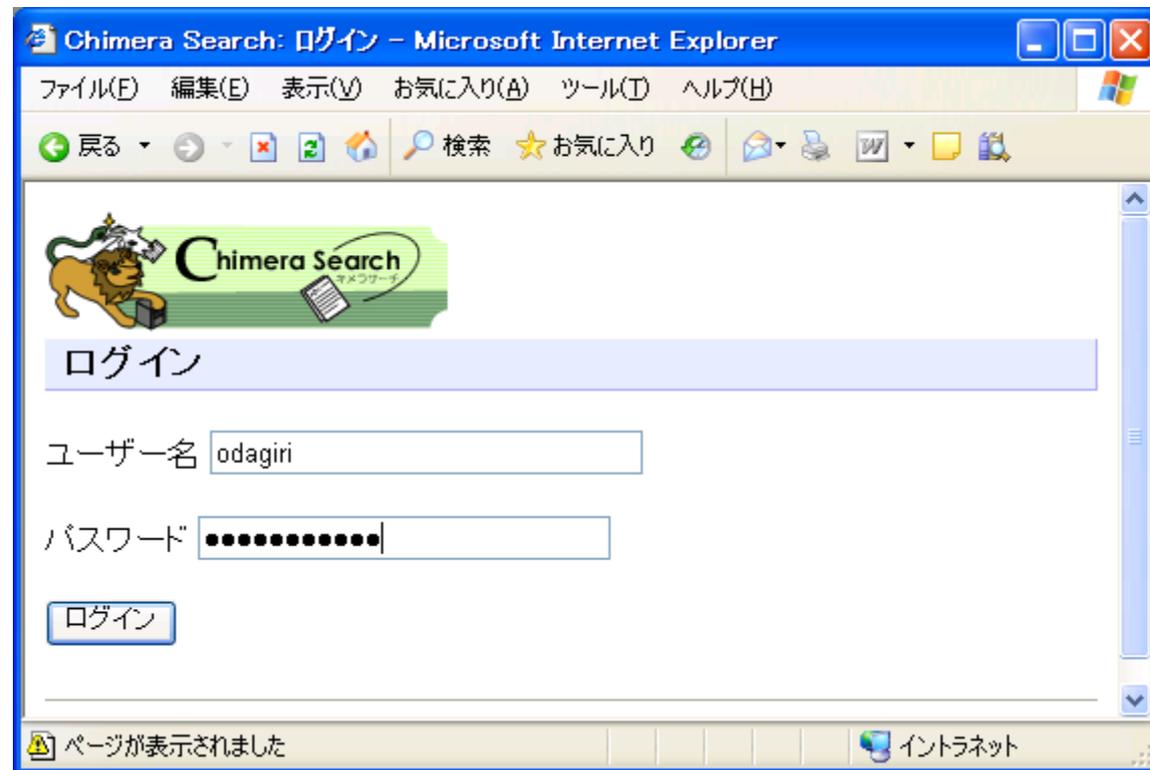
Windows 端末

- Webブラウザを使ってファイル検索
- リンクをクリックすると共有上のファイルを直接開いて更新可能

イントラネット

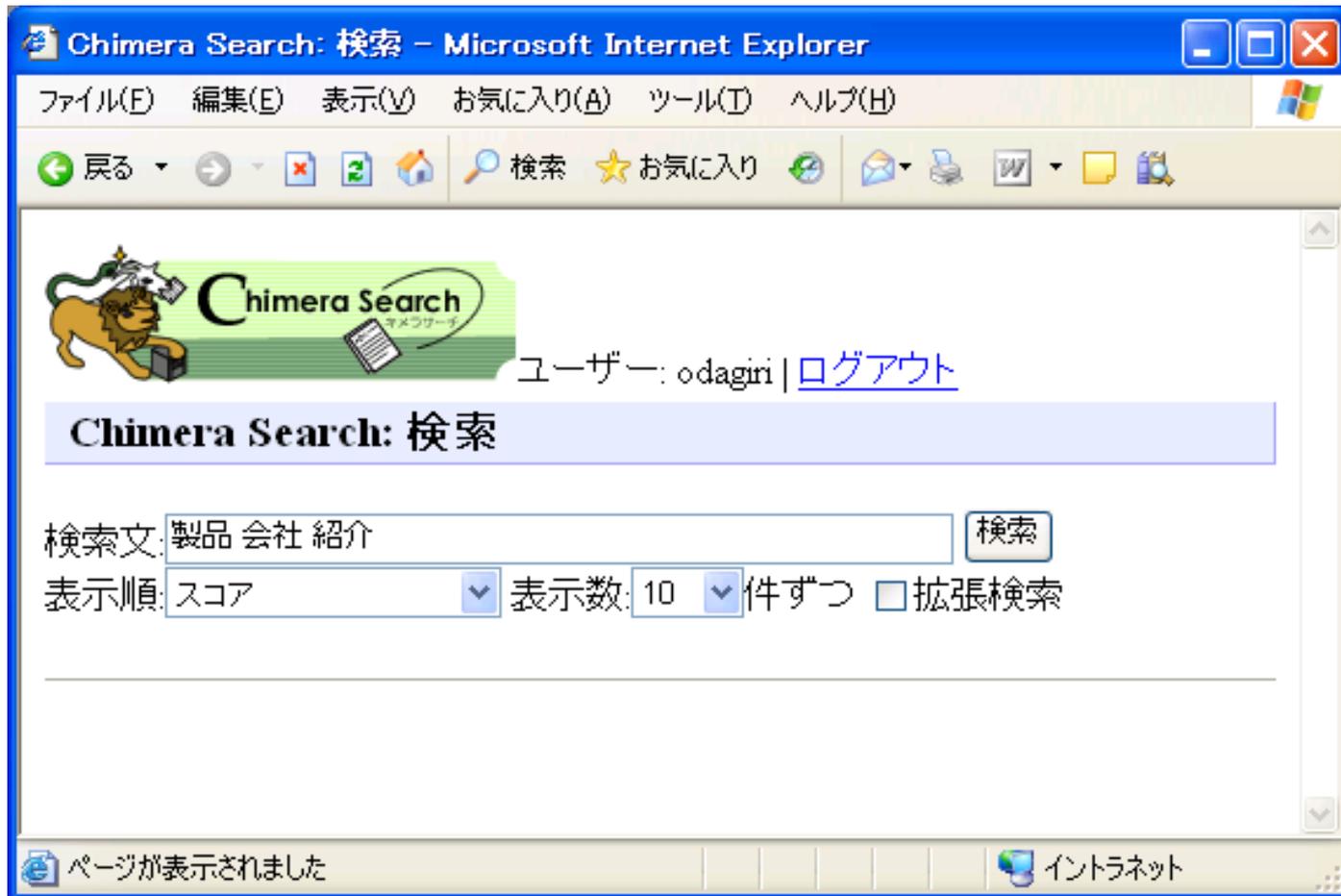
ログイン

- Chimera Searchはファイルのアクセス権をチェックして検索結果を制御しますので、利用するにあたってログインする必要があります。
- 検索結果から直接ファイルを開けるようにWindowsクライアントをドメインに参加させ、ドメインログオンする時と同じユーザー名、パスワードを利用することを推奨します。
- WindowsクライアントのWebブラウザからChimera Searchをインストールしたサーバーに以下のようにアクセスするとログイン画面が表示されます。
- ユーザー名にはWindowsドメインコントローラもしくはファイルサーバーに登録されているWindowsユーザーのアカウント名とパスワードを入力してください。



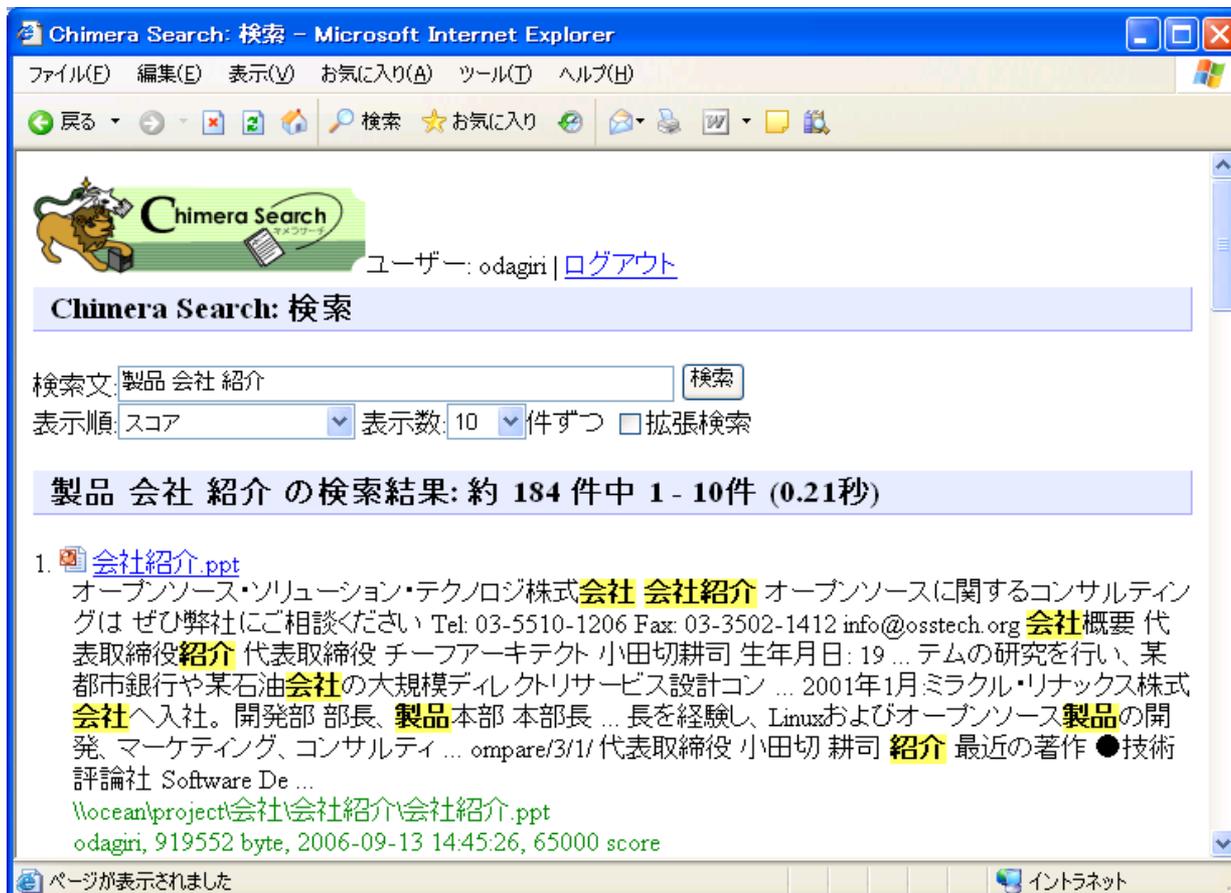
検索入力

- 検索分の中にキーワードを入力し、「検索」ボタンを押すと検索結果が表示されます。
- 表示順序として「スコア順」「更新日付順」「ファイル名順」「サイズ順」「所有者順」が選べます。



検索結果

- 検索キーワードは反転強調表示されます
- アクセス権の無いファイルは検索結果に表示されません。
- MSIEの場合、検索結果のリンクをクリックするとそのままファイルが開くことができ、ファイル更新するとファイルサーバー上のものを直接更新することができます。



Chimera Search: 検索 - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

Chimera Search ユーザー: odagiri | ログアウト

Chimera Search: 検索

検索文: 製品 会社 紹介 検索

表示順: スコア 表示数: 10 件ずつ 拡張検索

製品 会社 紹介 の検索結果: 約 184 件中 1 - 10件 (0.21秒)

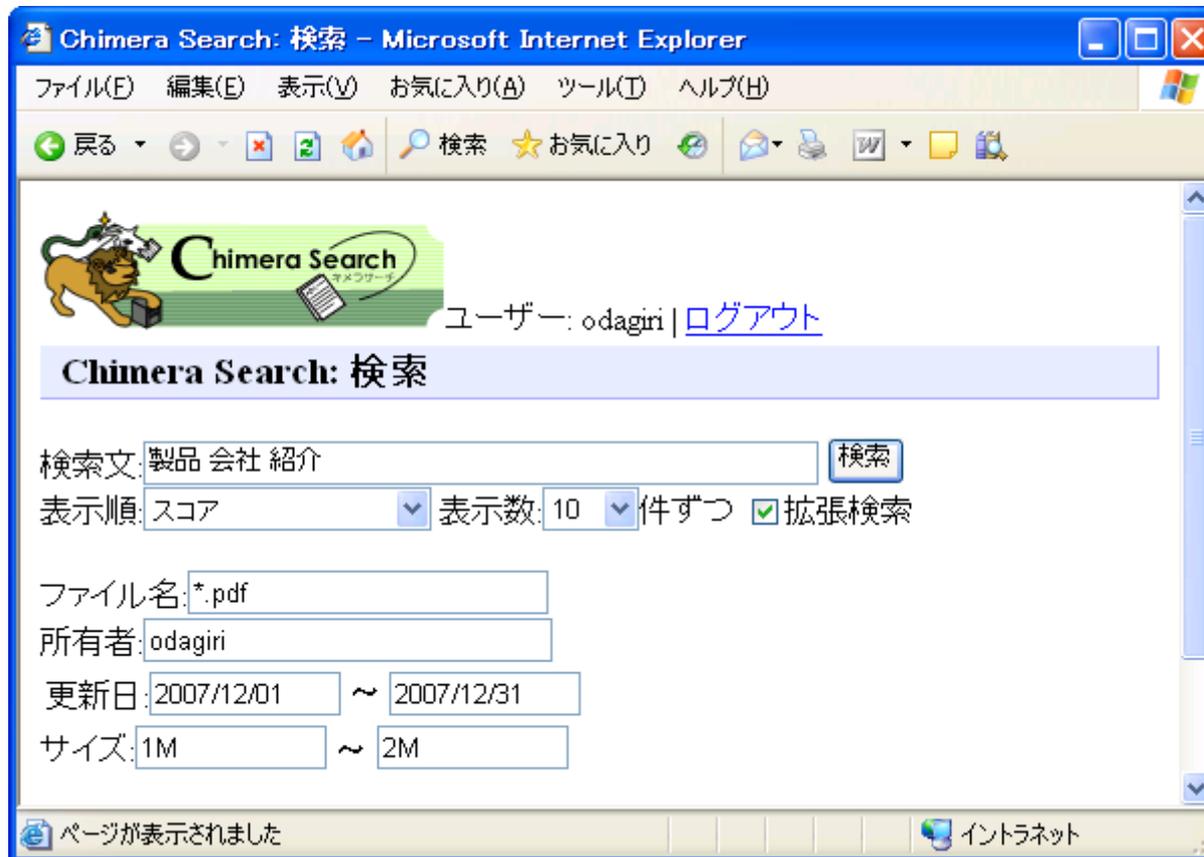
1. [会社紹介.ppt](#)
 オープンソース・ソリューション・テクノロジー株式会社 **会社 会社紹介** オープンソースに関するコンサルティングは ぜひ弊社にご相談ください Tel: 03-5510-1206 Fax: 03-3502-1412 info@osstech.org **会社概要** 代表取締役 **紹介** 代表取締役 チーフアーキテクト 小田切耕司 生年月日: 19 ... テムの研究を行い、某都市銀行や某石油**会社**の大規模ディレクトリサービス設計コン ... 2001年1月ミラクル・リナックス株式 **会社**へ入社。開発部 部長、**製品**本部 本部長 ... 長を経験し、Linuxおよびオープンソース**製品**の開発、マーケティング、コンサルティ ... ompare/3/1/代表取締役 小田切 耕司 **紹介** 最近の著作 ●技術評論社 Software De ...
 \\ocean\project\会社\会社紹介\会社紹介.ppt
 odagiri, 919552 byte, 2006-09-13 14:45:26, 65000 score

ページが表示されました

イントラネット

拡張検索

- 検索画面の「拡張検索」ボタンを押すと検索文字列に加え、以下の条件を指定できます。
 - ファイル名:「*」と「?」を使ったワイルドカードで指定したファイル名のファイルを検索できます。
 - ファイルの所有者、ファイルの更新日、ファイルサイズ(K:キロバイト、M:メガバイトでも指定できます)



Google Appsと Samba+LDAP認証統合



OSSTech

Google Appsとは

- Google社が提供するウェブベースのアプリケーションサービス
 - Gmail、Googleカレンダー、Googleドキュメントなど

<http://www.google.com/a/?hl=ja>

- ライセンス

- Google Apps Standard Edition

- 無料
- プロビジョニングAPI、シングルサインオン、メールゲートウェイは利用不可
- Gmailの広告付き

- Google Apps Premium Edition

- 100ユーザー以上 6000円/アカウント(1年ごと)
- 99ユーザー以下 50ドル/アカウント(1年ごと)

- Google Apps Education Edition

- 無料

http://www.google.com/a/help/intl/ja/admins/editions_spe.html

Google Apps採用時の利点

サービス利用料が無料・サーバー不要

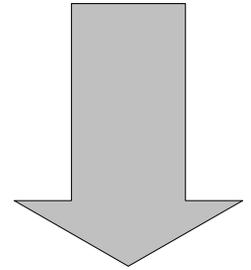
Ajaxで使いやすい・高度な機能・迅速な機能追加

バックアップの管理・装置が不要

アンチウィルス・スパム対策不要

Google Appsの運用監視・サポート費用不要

画面のカスタマイズ、Google APIによる連携可能



運用管理費用の
大幅な削減

Google Apps採用時の懸念点

メールを学外・社外にあるGoogleのサーバーに保存

Gmailへのアクセスによる外部ネットワークへのアクセス増加

Educationサービスレベルの保証は無し(実績としては問題なし)

長期的なサービス継続性は無保証

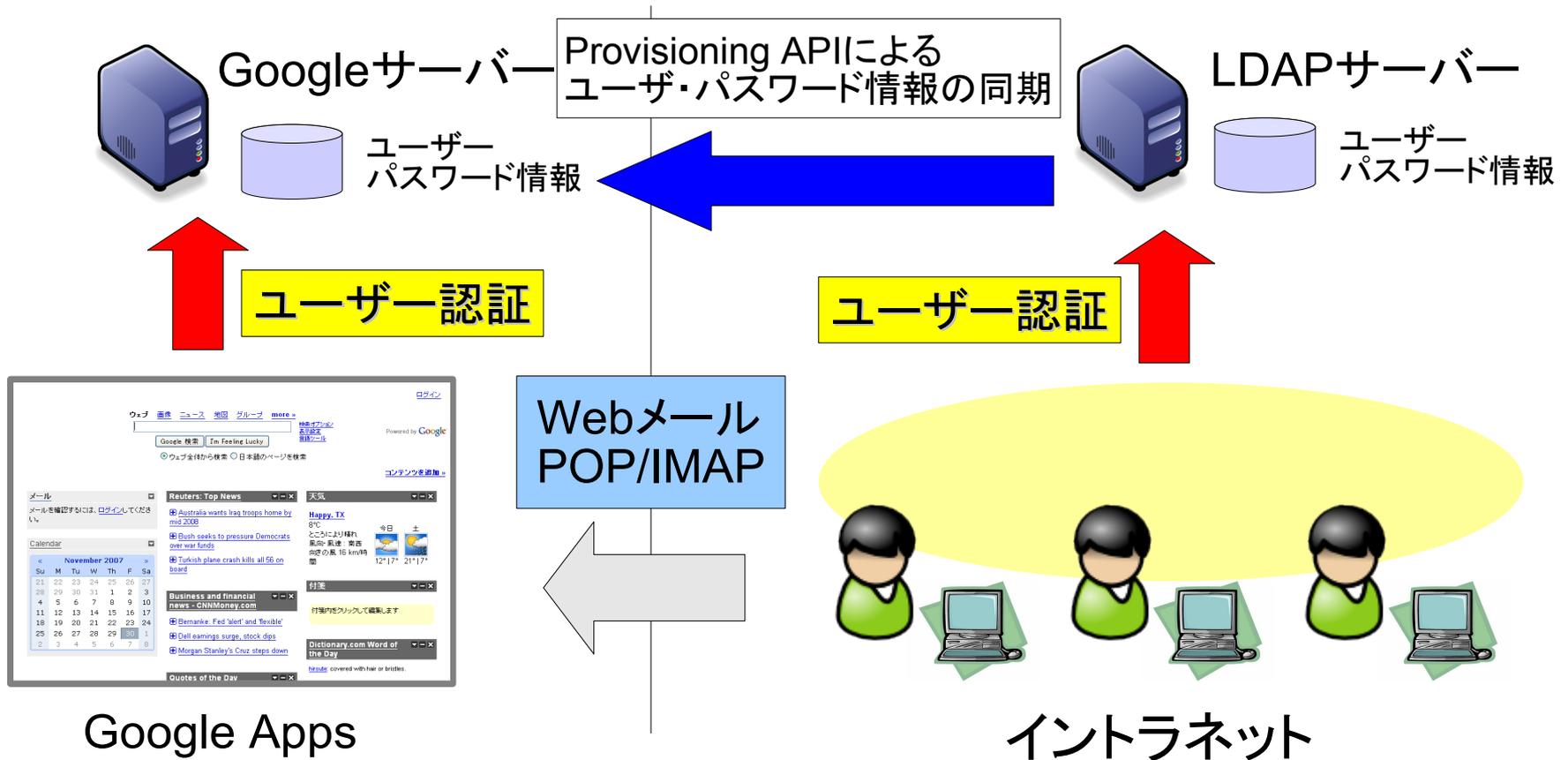
メールングリスト機能は貧弱

Google Apps利用のシステム基本構成例(1)

- Provisioning APIによるユーザーアカウントの認証統合
 - 組織内LDAPに登録されるユーザー情報、パスワードをGoogle Appsに登録
 - GmailでPOP/IMAPの利用が可能
 - パスワード変更用Webサイトが別途必要
- Provisioning APIとは
 - Google Appsのユーザー情報を外部から管理するためのAPI
 - ユーザー情報や、パスワードの変更などが可能
 - 外部インターフェースとの連携に利用

システム基本構成例(1)

- Provisioning APIによるユーザーアカウントの認証統合

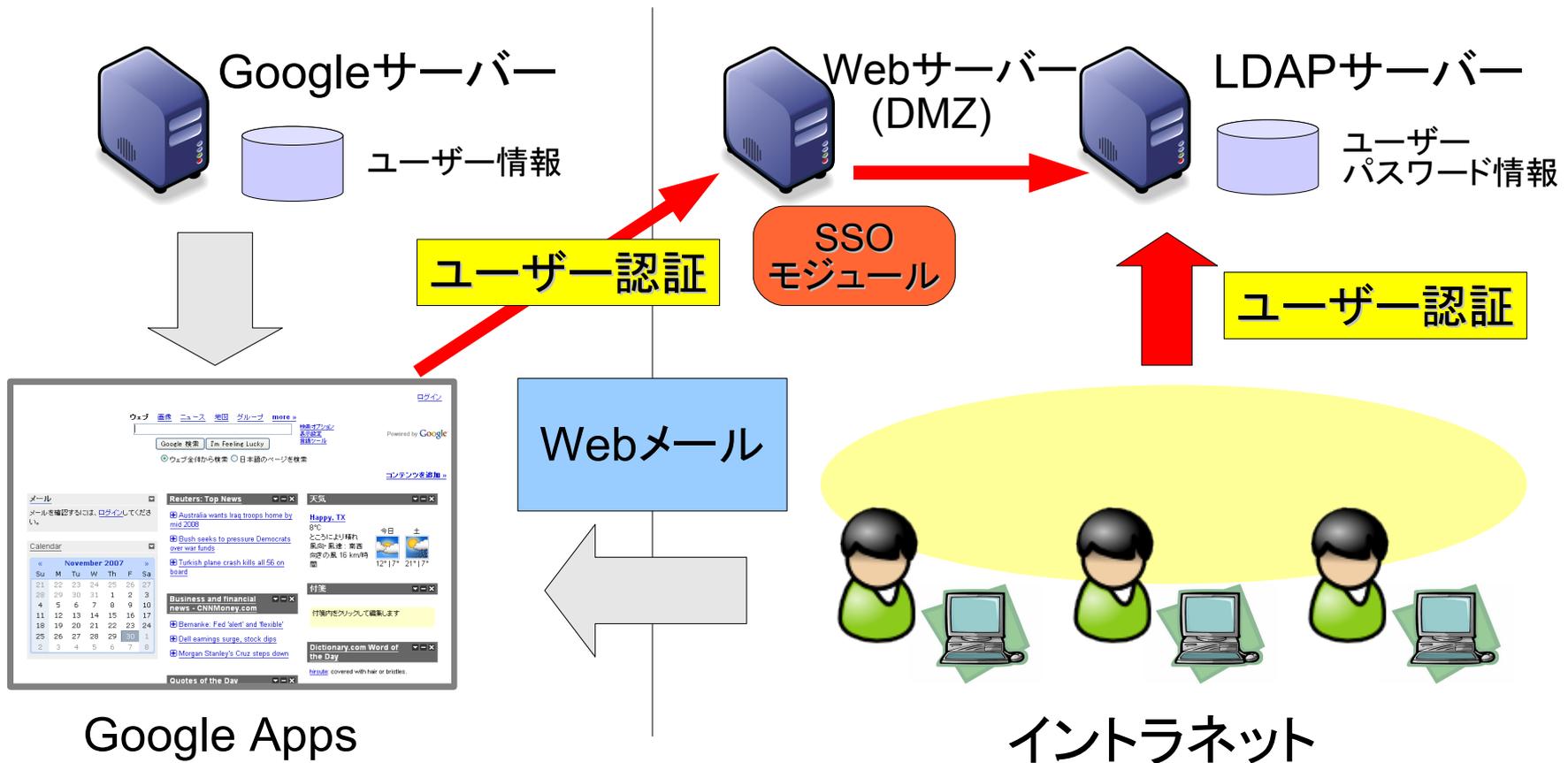


Google Apps利用のシステム基本構成例(2)

- シングルサインオン(SSO)モジュールによる認証統合
 - 組織内LDAPに登録されるユーザー情報のみをGoogle Appsに登録
 - Google Appsのユーザー認証は、SSOモジュールで組織内LDAPに対して実行
 - SSOモジュールによる認証用として、DMZに認証PROXY用のWebサーバーの構築が必須
 - パスワード変更用Webサイトは必須ではない
 - GmailでPOP/IMAPを利用することは不可能
 - Web経由のGmailのみ利用可能

システム基本構成例(2)

- シングルサインオン(SSO)モジュールによる認証統合



Google AppsとSamba LDAP連携システム

- Samba LDAPとの連携の利点

Google Appsと、Windows、Linux、UNIX、Mac OS Xの
アカウントの統合管理

Windowsドメイン環境をSambaで提供

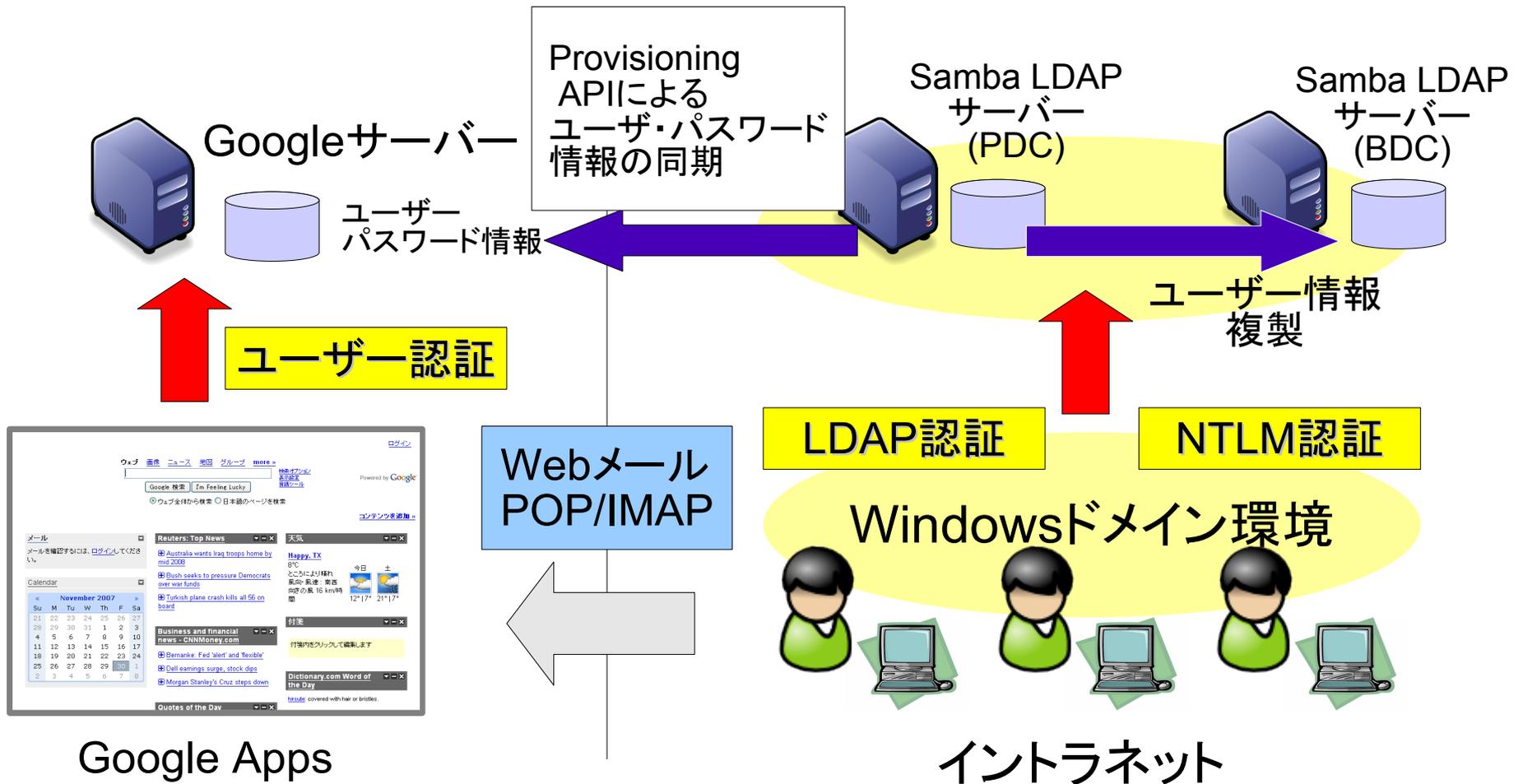
ソフトウェアライセンス費用 0円のインフラ構築

LDAP認証対応ソフトウェアとの連携可能

NTLM認証対応ソフトウェアとの連携可能

システム基本構成例(3)

- Samba LDAP連携によるユーザーアカウント認証統合



Google Apps統計情報取得機能

- システム管理者向けにGoogle Appsの利用状況に関する統計情報を取得する機能
 - ドメインに登録されているユーザー一覧と、ユーザーごとのステータス(最終ログイン日、ディスク使用量など)
 - Google Appsにログインしたユーザー数(1週間以内など)
 - ディスク使用量ごとのユーザー数の分布
 - Webメールを利用しているユーザー数
 - 容量制限に近づいている、もしくは越えたユーザーのリスト
 - ドメイン全体のディスク使用量、アカウント数
 - アカウントが利用停止となっているユーザーのリスト
- CSVファイルで上記データを提供可能

Google Apps移行作業項目一覧

Google Appsドメイン構築、移行

アカウント統合管理機能開発

Google Apps統計情報取得機能開発

パスワード変更用Webサイト開発(Provisioning API構成の場合)

SSO認証用Webサーバー構築(SSO構成の場合)

Google Appsドメイン構築、移行

- 目的
 - WebMailのインフラとしてGoogle Appsを構築する
- 作業内容
 - Google Appsドメインの設定とDNS設定
 - 既存ユーザをGoogle Appsへ一括登録(初期パスワード設定)
 - 認証PROXYサーバを構築する場合は初期パスワード不要
 - 既存メールサーバとの並行運用設定も可能

アカウント統合管理機能開発

- 目的

- LDAPもしくはADのユーザー管理、およびGoogle Appsのユーザー管理を統合し、大学様のシステム構成にあわせたユーザーアカウント統合管理機能を開発

- 開発項目

- ユーザー登録機能(Google Apps連携含む)
- ユーザー削除機能(Google Apps連携含む)
- 一括ユーザー登録、削除機能

パスワード変更用Webサイト開発

- 目的
 - パスワード変更用Webサイトからパスワードを変更することで、パスワード情報の一元管理を可能とする。
 - Google Appsのパスワード変更画面としても利用
- 開発内容
 - ユーザーのパスワード変更用Webサイトとしてパスワード一括設定機能を持つWebサイトを作成する
 - LDAP(またはAD)のパスワード変更機能
 - Google Appsのパスワード変更機能