

最新Samba動向と 構築事例紹介



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.OSSTech社紹介

2.Sambaユーザ動向と事例

3.官公庁・自治体での認証統合事例

4.Samba最新動向

5.OSSTech製品紹介

- Samba 3.0.24 for Solaris / Linux**
- OpenLDAP 2.3.32 for Solaris / Linux**
- LDAP Account Manager**
- SSLBridge**

Part 1

オープンソース・ソリューション・テクノロジー 会社紹介

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	・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	・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	・デル(株) ・(株)野村総合研究所 ・サン・マイクロシステムズ(株) ・キヤ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

- 昨年 9月に設立
- **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>

社員による著作紹介

◆ 小田切耕司

◆ 技術評論社 Software Design 2006年7月号

- 「壱:地の巻」Sambaファイルサーバ

◆ 翔泳社 開発の現場 vol.005

- 総論編:オープンソースの基礎知識

◆ 技術評論社 LDAP Super Expert

- [新規/移行]LDAPディレクトリサービス導入計画

◆ IDG月刊Windows Server World

- 3月号:Shall we Samba?【お手軽導入編】
- 4月号:Shall We Samba?【超本格運用編】

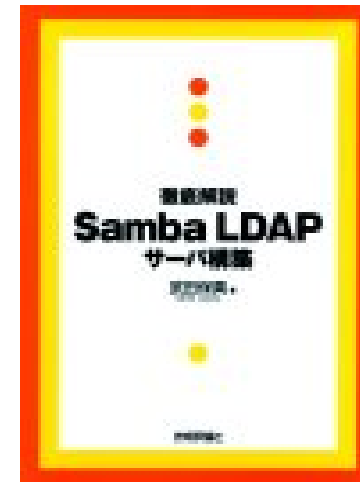
◆ 日経BP社 セキュアなSambaサーバの作り方

◆ 武田保真

◆ 日経ITPro「Sambaウォッチ」

- ◆ 2006年10月～現在連載中

◆ 「徹底解説 Samba LDAP サーバ構築 (技術評論社)」



Part 2

Sambaユーザ動向と事例

**ファイルサーバも時代と共に
活用方法が変わる！**



OSSTech

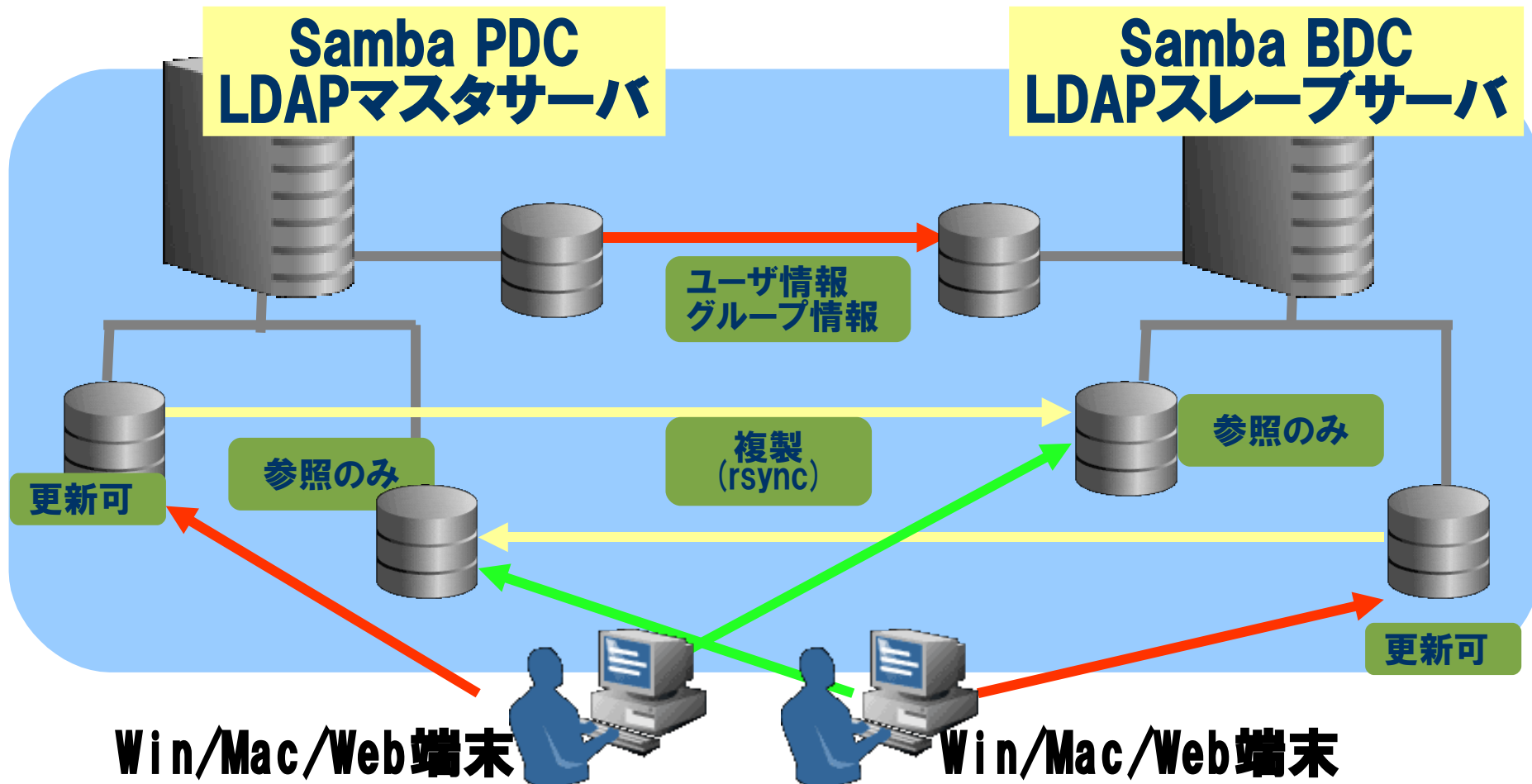
ファイルサーバを取り巻く環境変化

- サーバH/Wの高性能化、低価格化
- ディスクの大容量化、低価格化
 - 高信頼のSCSIディスクよりも低価格のATAディスクを選択するケースが増えてきている
 - ファイルサーバのディスク故障率増加
 - RAID5にしても故障時の自動修復に時間がかかる
 - RAID5では自動修復中にもう1台壊れると修復できない
 - ディスク故障時の損失金額・時間も増大
- ファイルサーバをバックアップするためのコストが増加
 - 従来のテープ装置ではバックアップできない
 - 必要なテープ本数が増える、時間がかかる
- バックアップ装置とテープはディスクほど安くなっていない

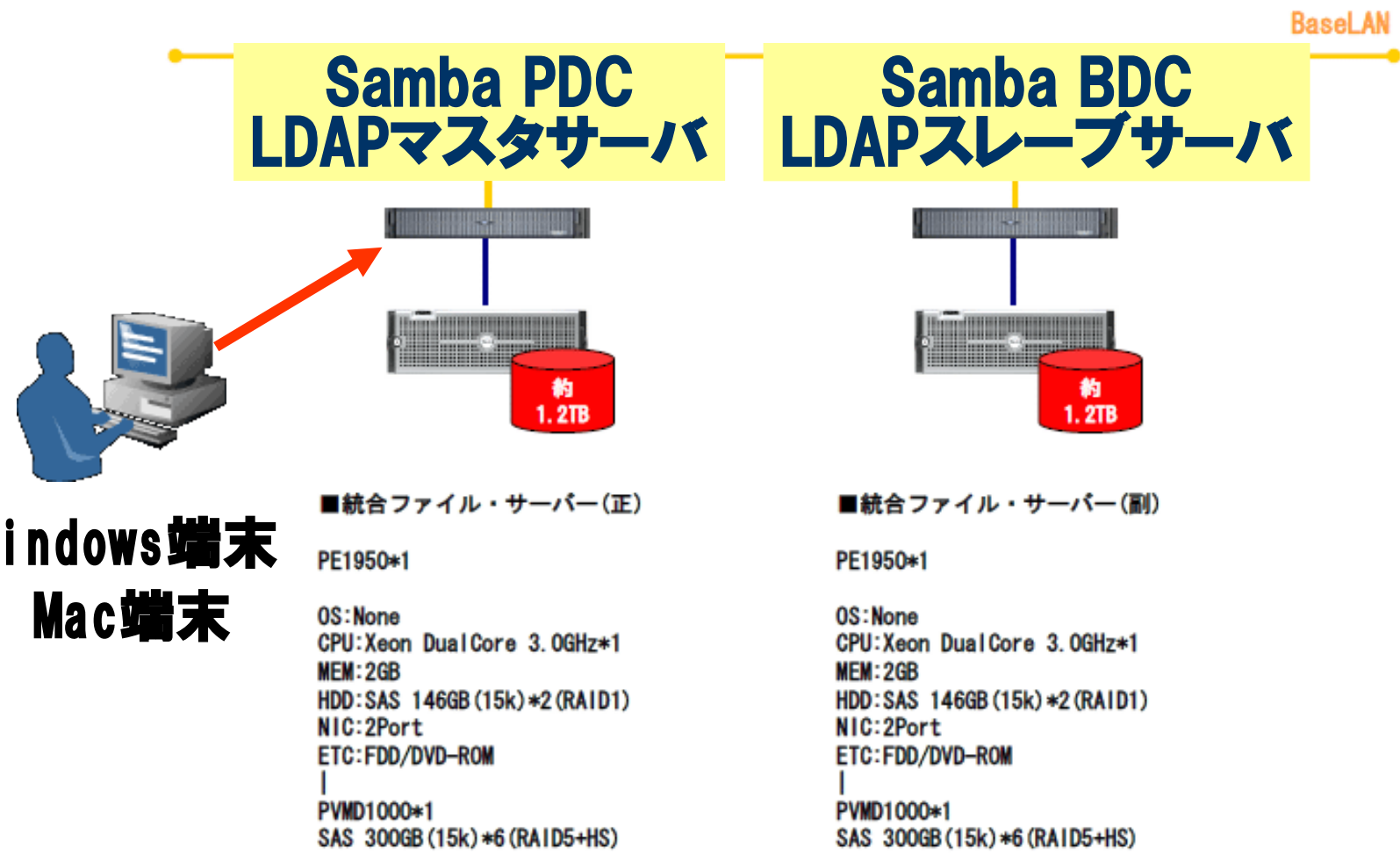
ファイルサーバ構築方法の変化

- 専用のバックアップ装置を買う費用もサーバをもう1台買う費用もあまり変わらない
 - サーバもう1台購入の方が安い場合もある
- テープバックアップよりもディスクコピーを選択するユーザ
- 同じ構成サーバを2セット用意し、rsyncを使ってコピー
- 双方向にすれば簡易クラスタ構成可能
- インターネット高速化やVLANの低価格化により、遠隔地バックアップも安価に実現可能になった
- OSとしてCentOSやSolaris 10を使うユーザが増えた
 - CentOSはパッチ入手無償、Solaris 10も4万円未満

安価な簡易クラスタシステム構築例



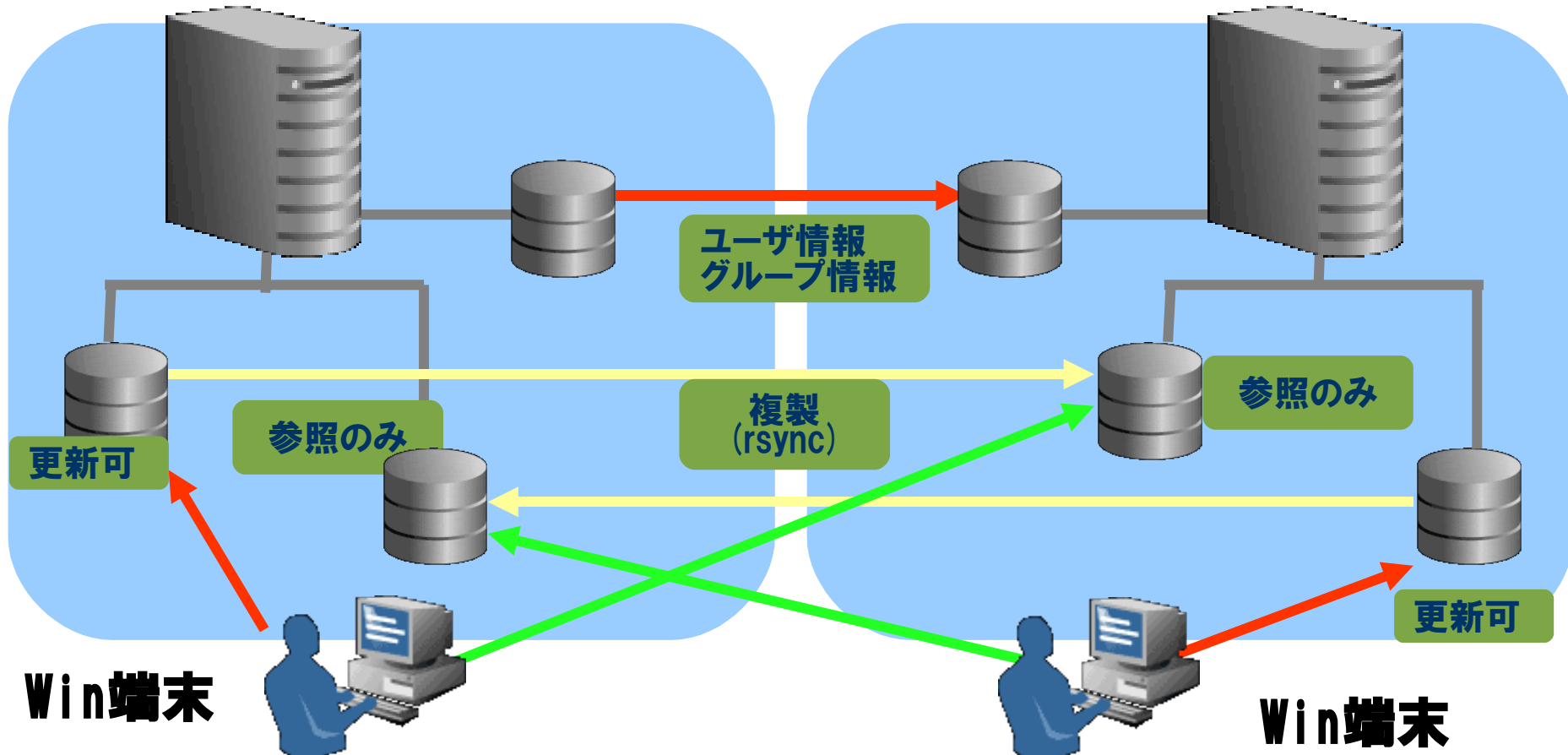
某音響機器メーカー様 統合ファイル・サーバーのシステム構成図



遠隔地双方向バックアップ: 通常運用時

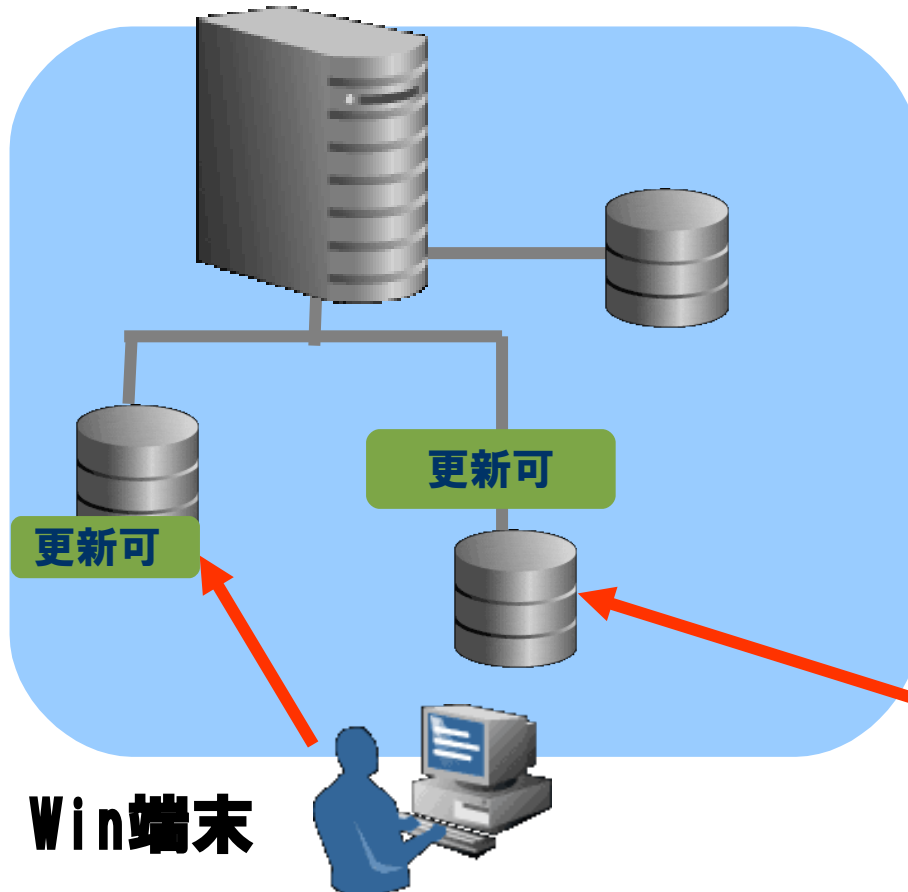
**東京: Samba PDC
LDAPマスターサーバ**

**大阪: Samba BDC
LDAPスレーブサーバ**



大阪サーバ障害時

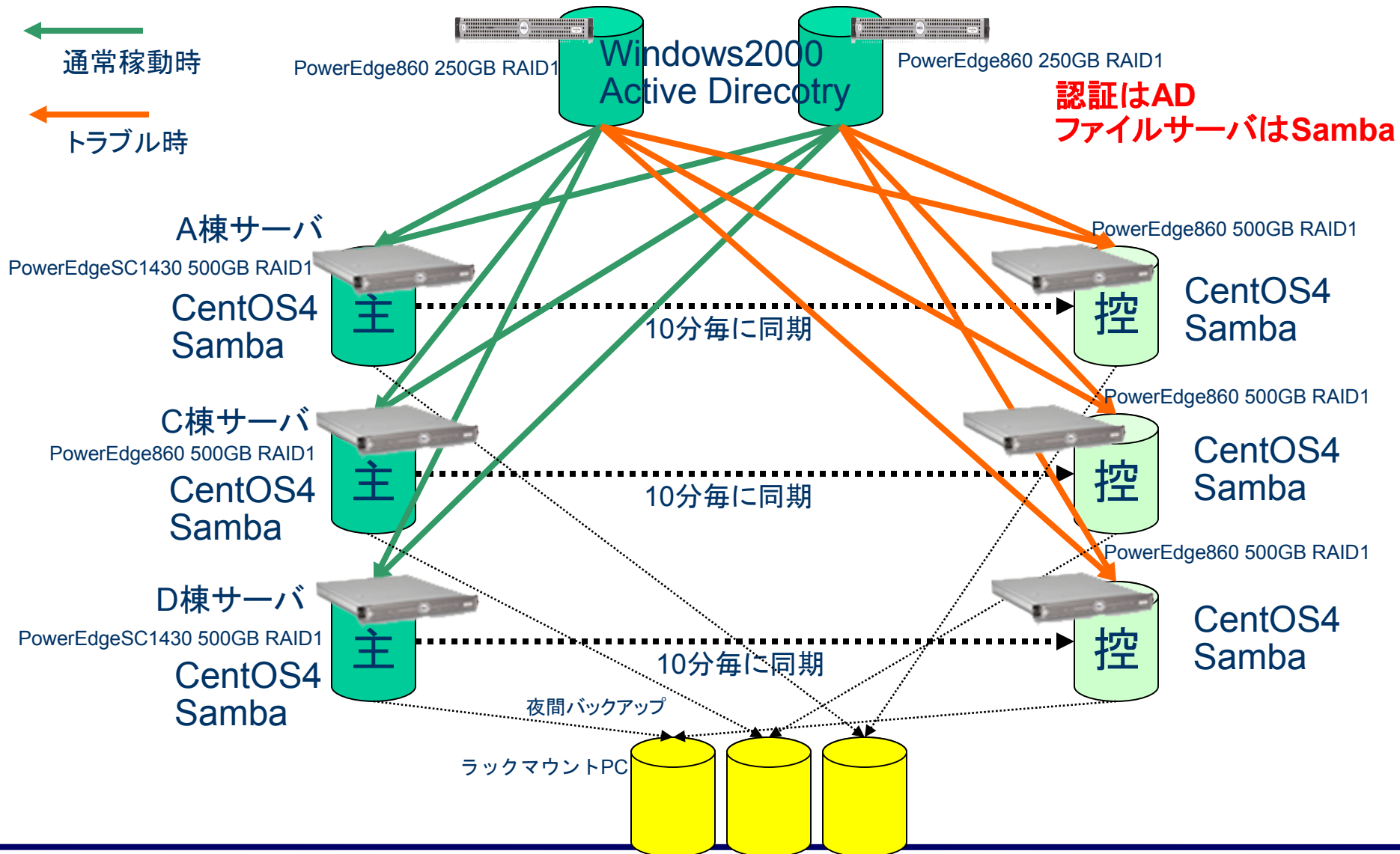
**東京:Samba PDC
LDAPマスターサーバ**



**大阪:Samba BDC
LDAPスレーブサーバ**



サンアロー株式会社様 <http://www.sunarrow.co.jp>



Part 3

システム認証統合事例紹介 官公庁・自治体からはじまった OSSによる基幹システム構築



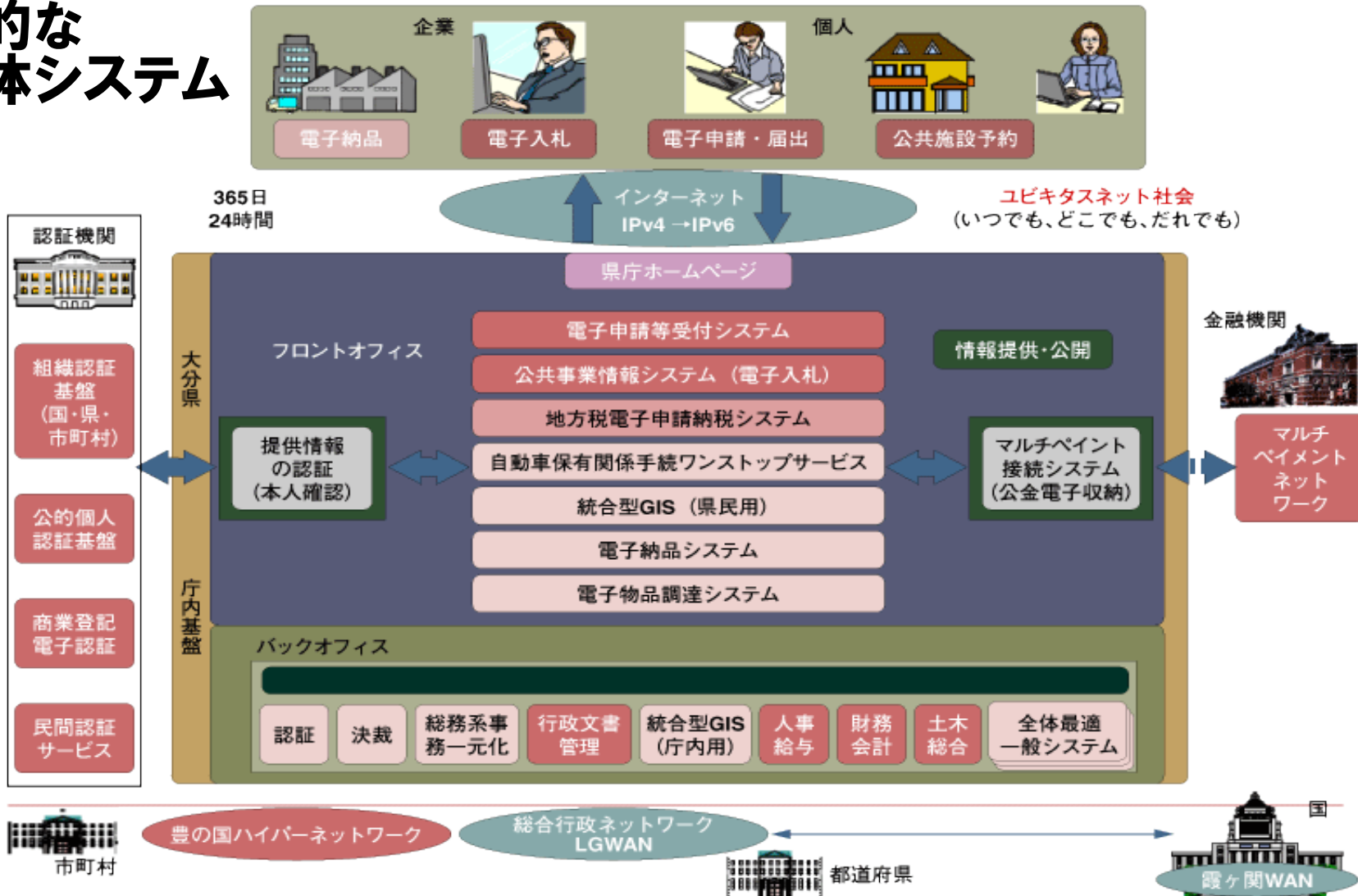
OSSTech

システム概要

- OSSを使った認証基盤構築事例として、大分県庁の実証実験システムを取り上げます。
- このシステムはIPA(独立行政法人 情報処理推進機構)の公募事業「自治体基盤システムでのオープンソースソフトウェア(以下、OSS)活用に向けての導入実証実験」として構築されました。
- この公募事業は、OSSが自治体の基幹システムとしてどこまで使えるか実証実験しよう、という取り組みです。
- 参考) IPA実証実験報告ページ
- <http://www.ipa.go.jp/software/open/oss/2006/stc/report/oita.html>

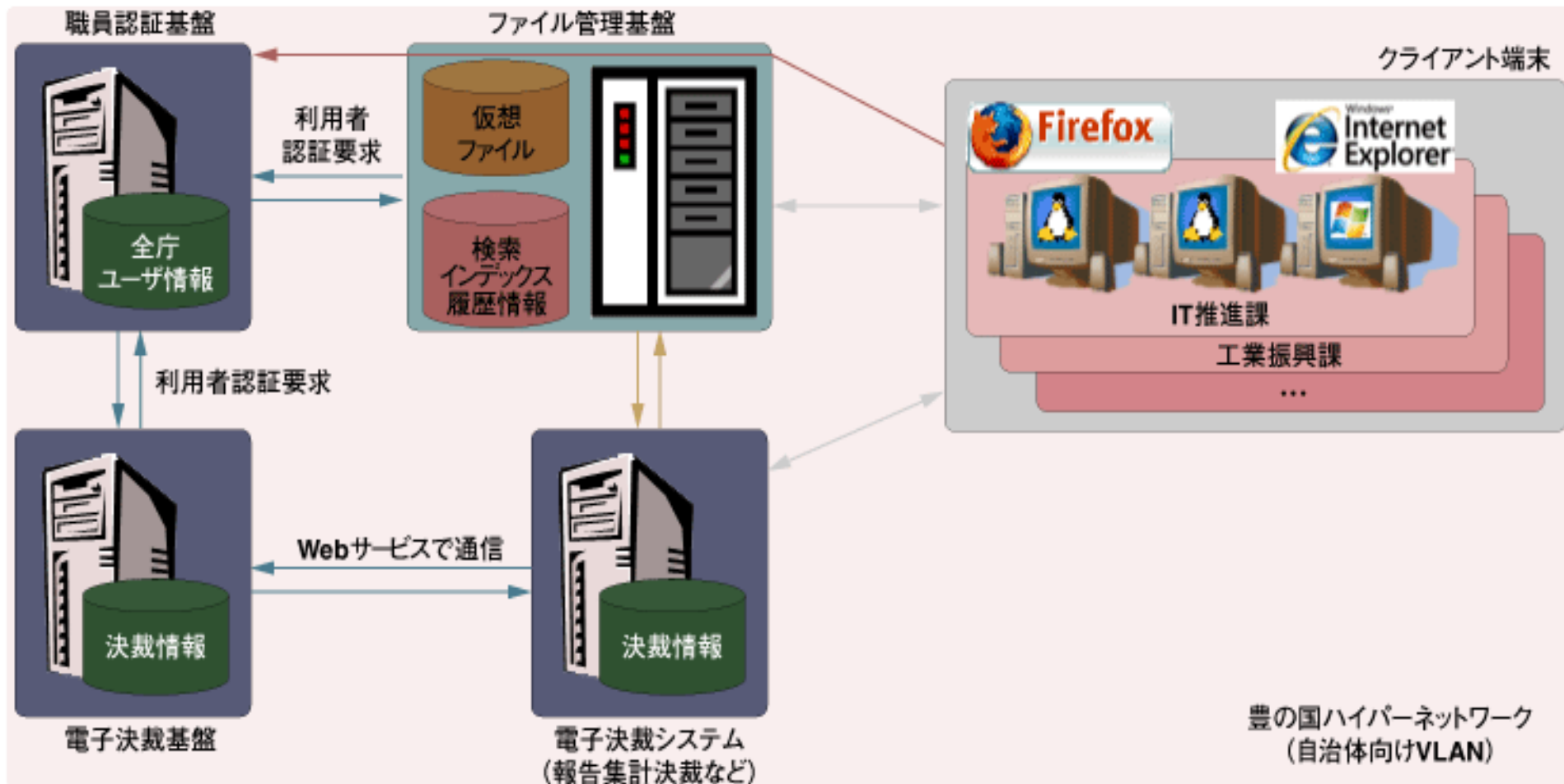
大分県庁システム概略

一般的な自治体システム



実証実験で構築したシステム

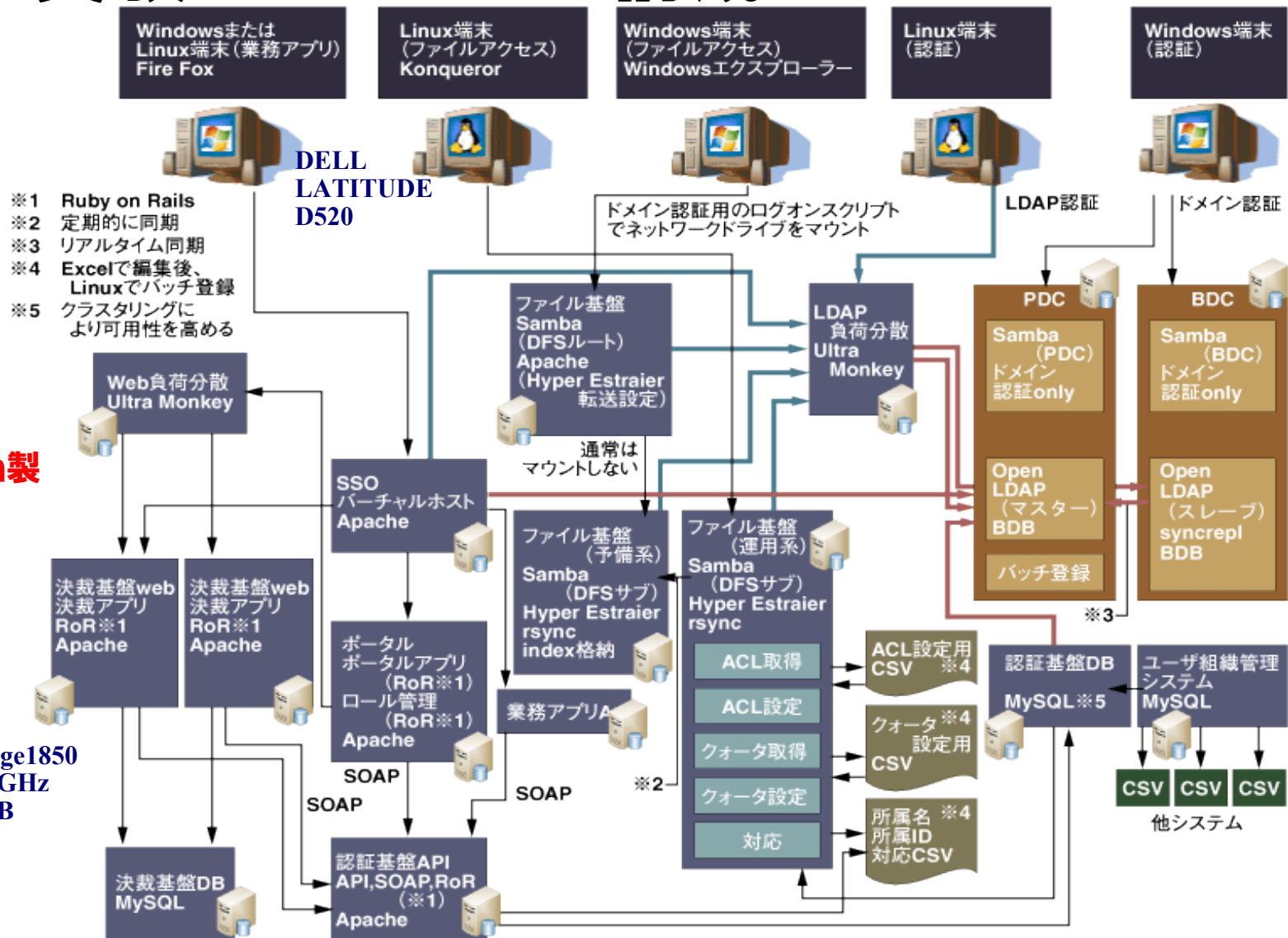
- ファイルサーバ／アプリケーションサーバおよび Windows / Linux の認証統合を実現



システム要件と実装方法

システム	必要機能	実装方法
職員認証基盤	・Linuxによるディスクレス・シンクライアントの導入	KnoppixをベースとしたCDブートLinuxをデスクトップ環境として利用
	・OSSのWebブラウザで業務を実行	
	・OA業務はOpenOfficeで実行	
	・上記Linuxクライアントの統合認証基盤	・認証基盤としてOpenLDAPを採用し、LDAPに登録したユーザ、パスワードでデスクトップにログインする ・OpenLDAPに登録してあるユーザならどの端末でも利用可能にする ・上記のためにKnoppixクライアントをLDAP認証へ改造
	・既存のWindowsクライアントからも利用できること	・SambaとOpenLDAPによるWindowsドメインを構築し、ドメイン認証を構築する ・WindowsクライアントはSambaドメインに参加し、ユーザはドメインログオンをする ・LDAPに登録したユーザ、パスワードでデスクトップにログインする ・OpenLDAPに登録してあるユーザならどの端末でも利用可能にする
	・Webベースの業務システムでは、ユーザが一度サインオンしたら、その後の他システムへのアクセスは認証なしでアクセスできる、いわゆるSSO（シングルサインオン）の機能を有すること	・認証基盤としてOpenLDAPを利用し、認証はApacheのシングルサインオンモジュール（独自のmod_sso改造版）にて実装する ・すべての業務システムをこのシングルサインオンシステムのリバースプロキシ配下に置く
	・県庁職員5000人の利用に耐えるパフォーマンスを持つこと	・OSSのクラスタソフトUltra Monkeyを使って負荷分散クラスタを構築
	・業務の拡大や負荷増大に耐えられるようにスケールアウト可能な構成にすること	・OpenLDAP+Samba+Apacheをクラスタ構造とすることにより実装する
電子決裁基盤	・Webブラウザにより複数のシステムから共通に決裁基盤を利用できること	・決裁基盤APIをWebサービスにより公開し、相互利用する
	・決裁文書としてファイルの受け渡し機能を有すること	・Webサービスを用い、添付ファイル送受信が出来るインターフェースを実装

実証実験でのシステム構成



実証実験で発生した問題(OSやOSS部分のみ)

- OSはCentOS4 (=RHEL4) を利用
- OS標準のSamba 3.0.10ではLDAP連携で機能が不足だったり、品質が十分でないためOSSTech社製Samba 3.0.24国際化版を利用
- OS標準のOpenLDAP 2.2.13では高負荷に耐えられず、クラッシュしたり、クラッシュ後DBリカバリできないなどの障害が発生したためOSSTech社製OpenLDAP 2.2.30を利用
- SambaとLDAPを最新OSSTech社製品を使うことで同時5000ログオンも問題なく検証できた。
- 弊社実績では2万ユーザオーバーもある。

Part 4

Samba最新情報

GPLv3になるSamba 3.2

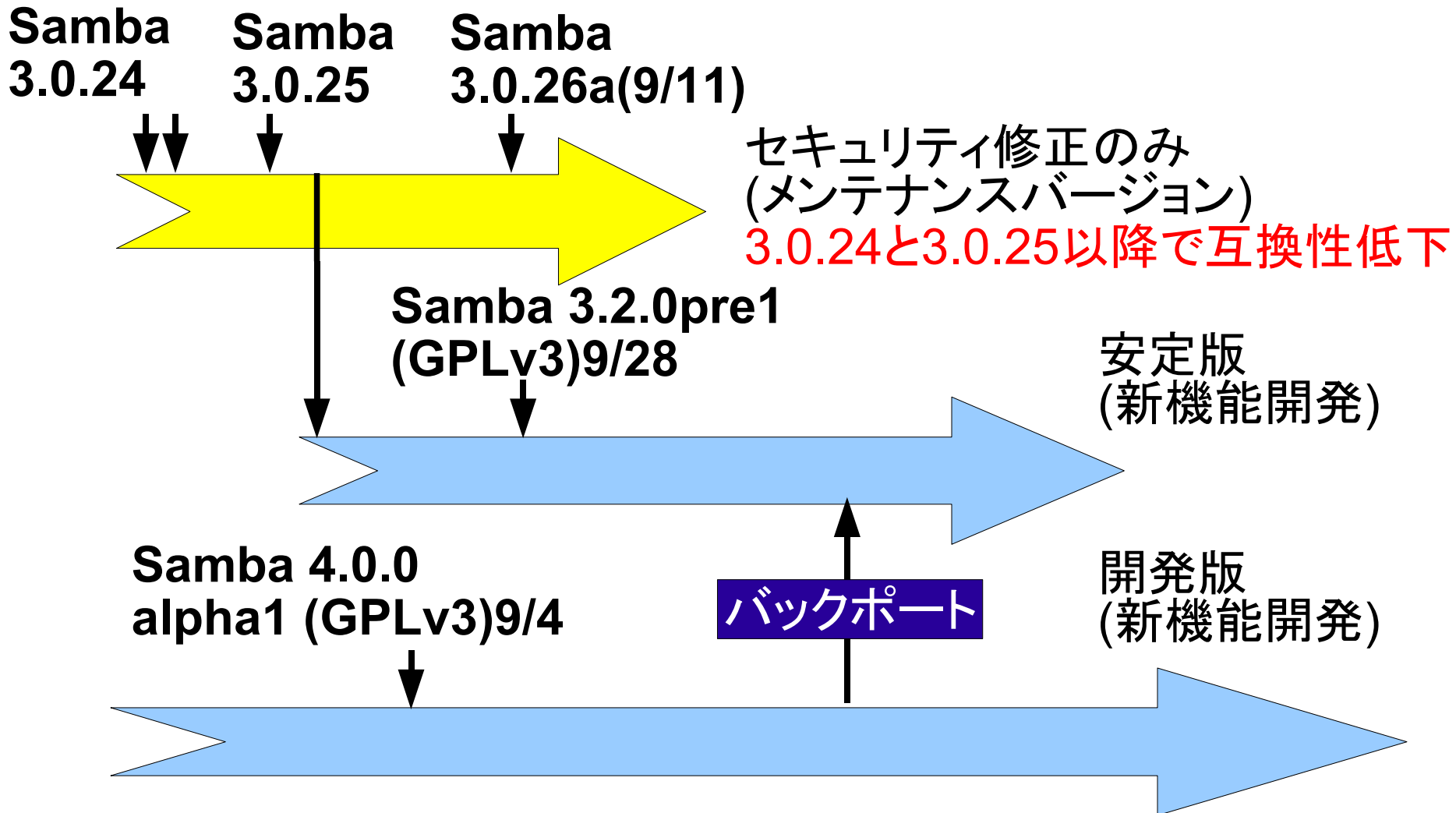


OSSTech

目次

- Samba ロードマップ
- Samba 3.0系
 - バージョンアップに関する情報
- Samba 3.2 新機能紹介
- Samba 4.0系 最新動向紹介
- Samba & ZFS 紹介
- 開発者向け情報

Sambaロードマップ



Samba3.0系(バージョンアップの経緯)

- Samba 3.0.0 ～ Samba 3.0.6
- Samba 3.0.6～ Samba 3.0.14a
 - LDAP schema拡張
- Samba 3.0.20～ Samba 3.0.24
 - Windows 2003 R2対応
 - winbind機能の改善
 - LDAP schema拡張
- Samba 3.0.25～ Samba 3.0.25b
 - Windows Vista対応
- Samba 3.0.26 → Samba 3.2.0
 - GPLv3への変更

2003.9.24

2005.8.19

2007.5.14

2007.9.11



Samba 3.0系お勧めバージョン

- **Samba 3.0.24 + Vista対応パッチ**
 - 3.0.20以降ではそれほど大きな変更が無く、利用者からのフィードバックによる修正が取り込まれ安定
 - 最新のWindows Vistaにも対応
 - これから構築するならUTF-8を使おう(JIS2004)
- **Samba 3.0.14a以前**
 - ドメインコントローラーや大規模で問題発生
 - Active Directory連携は推奨できない
 - Samba 3.0.24系にアップデート推奨
- **Samba 3.0.25以降**
 - Samba 4.0系の機能取り込みによって不安定
 - Samba 3.0.24以前と互換性が低下

Samba 3.0系アップデート時の注意事項

- Samba 3.0.23～Samba 3.0.24
 - msdfs rootパラメータのデフォルトがyes だがMS-DFSを利用しない場合、noの設定を推奨
 - Windowsクライアントが接続できなくなる場合あり
- Samba 3.0.23以降
 - winbind enum users = no (デフォルト)
 - winbind enum groups = no (デフォルト)
- LDAP利用時
 - samba.schemaも一緒にアップデート
- Vista対応
 - 「security = server」設定のSambaサーバには、Vistaのローカルセキュリティポリシーの設定が「NTLMv2応答のみ送信」では接続不可
 - コマンドプロンプトでnetコマンド使うとOK

Samba 3.0.25へのアップデート時の注意事項

- inotifyサポート
 - inotifyをサポートしていないシステムでファイルの更新がWindowsクライアントに通知されない
 - Windowsで、F5で手動更新の必要あり
- winbind設定の変更
 - ドメインごとに複数の設定可能
 - idmap domains = SALES DEVEL
 - idmap config: SALES:backend = ad
 - idmap config: DEVEL:backend = tdb
 - idmap config: DEVEL:range = 10000 - 20000

Samba3.2系の新機能紹介

- CIFS Unix Extensionsサポート
- ファイルサーバ・クラスタの実験的サポート
- SambaをADのメンバにした場合(Winbind機能)
従来は双方向の信頼関係を結んでいないと問題が発生したが、片方向のみと推移的
信頼関係もサポート
- nested domain groupsのNSS拡張
- LanMan認証廃止(95/98/Meから接続できない、2000以降OK)
- Samba 4.0のNTVFS機能相当のバックポート(from 3.0.25)
 - 共有ごとにACLモジュールの設定可能
- DDNS更新機能のサポート
 - Active Directory参加時にADのDNSに自動登録(from 3.0.25)
- LDBサポート
 - ローカルグループサポートのためのSamba組み込みDB
- SambaによるLDAPのposixAccountエントリ制御
 - もうsmbldap-toolsはいらない？

Samba 3.2系 TIPS: ユーザ管理

- Samba 2.xまで
 - smbpasswdコマンド
 - useradd user1 ; smbpasswd -a user1
- Samba 3.0
 - pdbeditまたはsmbldap-toolsコマンド
 - TDBSAMの場合 : useradd user1 ; pdbedit -a user1
 - LDAPの場合 : smbldap-useradd -a user1
- Samba 3.2以降
 - netコマンド
 - net user add user1
 - ユーザ管理バックエンドを意識しなくて良い(はず)

Samba 3.2系 TIPS: ACLモジュール

- 共有ごとのACL設定

- 各共有ごとにACLモジュールを設定
- ビルド時に—with-acl-supportを指定しないこと

```
$ ./configure --with-shared-modules=vfs_solarisacl, vfs_zfsacl  
[zfsshare]
```

```
path = /zfspool/share
```

```
vfs object = zfsacl
```

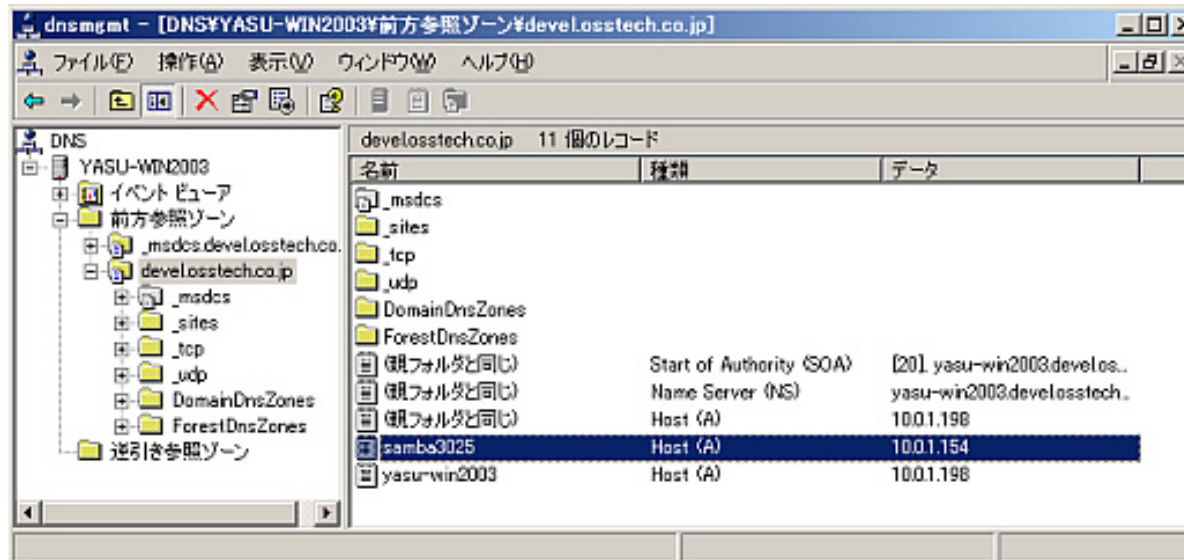
```
[ufsshare]
```

```
path = /opt/share
```

```
vfs object = solarisacl
```

Samba 3.2系 TIPS : Secure DDNSサポート

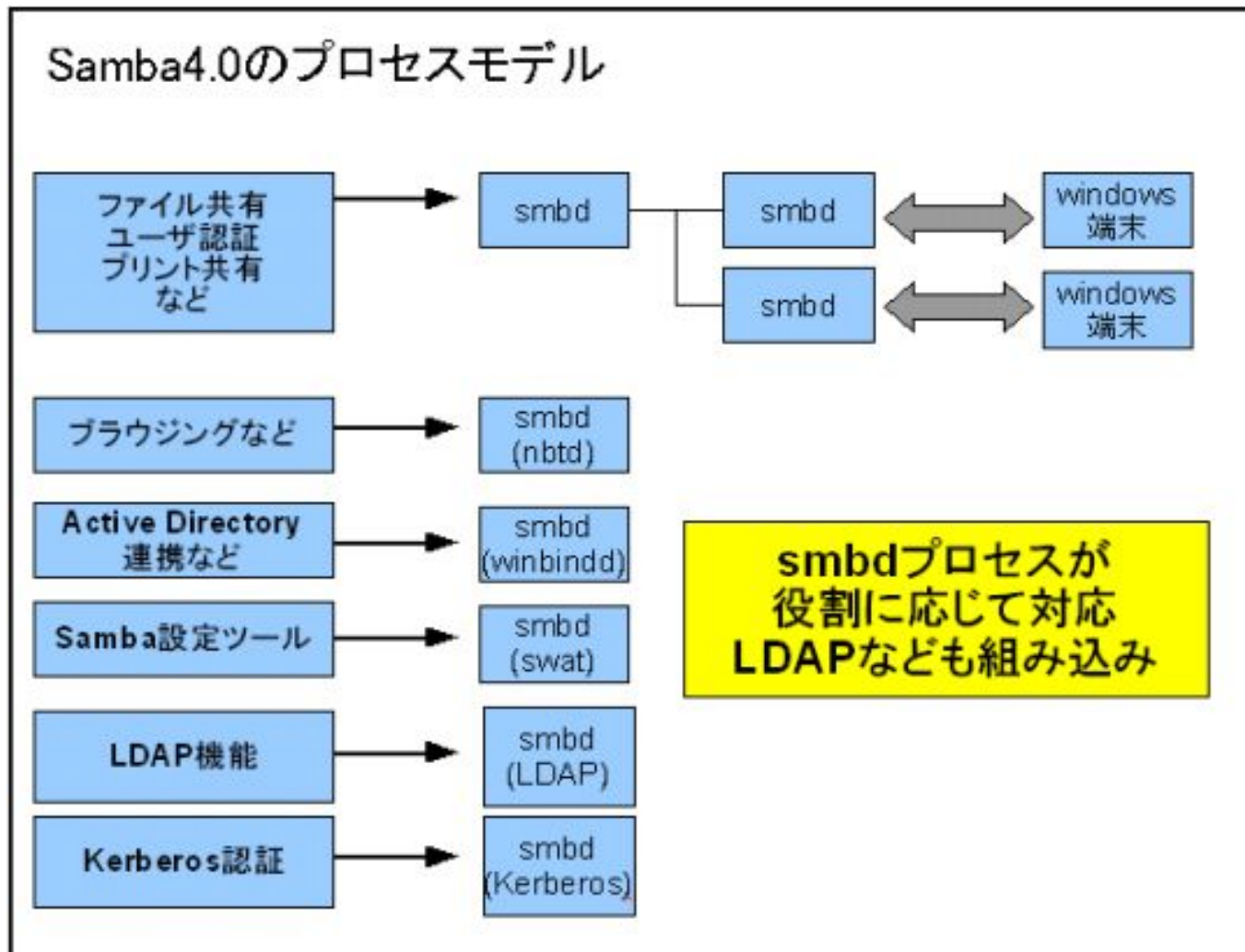
- Active Directoryのドメインメンバー設定時、“net ads join”実行時に、Active DirectoryのDNSにSambaサーバを自動登録
- configureオプションとして、「--with-dnsupdate」の指定が必要



Samba4.0系 最新動向紹介

- ロードマップ
 - Samba 4.0.0 alpha1 (2007/09/04)
 - 正式リリースは来年、Windows 2008より先か後か？
- Samba 4.0の構成
- Samba 4.0の新機能
 - Active Directory ドメインコントローラ機能サポート
 - Group Policy Objectサポート
 - NTVFSによるNTファイル・ストリームサポート
 - SMB2.0プロトコル対応
 - AjaxによるSWAT2
 - Sambaクラスタリング対応

Samba 4.0の構成

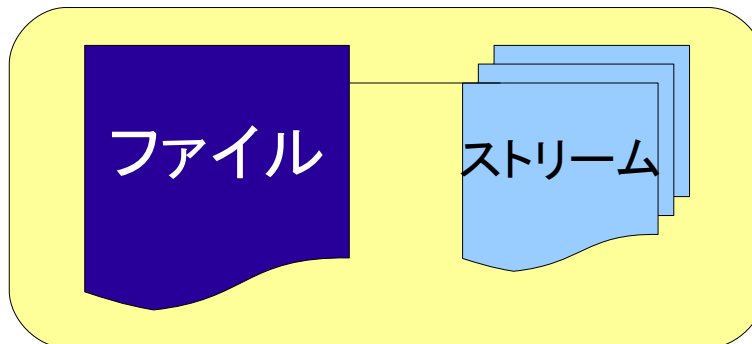


Active Directory ドメインコントローラ機能サポート

- Samba 3.0のドメインコントローラ機能
 - NTドメイン機能(Windows NT 4.0相当)
 - LDAPと連携することでAD相当の構成は可能
 - アカウントポリシーは利用可能、グループポリシーは利用不可能
- Samba 4.0のドメインコントローラ機能
 - Active Directoryドメイン機能(Windows 2000 or later)
 - LDAP, KerberosなどをSambaに組み込み
 - グループポリシーの利用可能

NTVFSによるファイル・ストリームサポート

- NTFSで利用可能な、1つのファイルに複数の不可視データを関連付ける機能
 - <http://www.microsoft.com/japan/msdn/windows/windows2000/ntfs5.aspx>
 - Windows XP用セキュリティアップデートで、ファイルの出所を証明する情報を付加するなどの利用
 - http://www.itmedia.co.jp/enterprise/articles/0504/18/news043_2.html
- UNIXのファイルシステムが提供するfile xaattrs(拡張属性)、もしくは外部データベースによるサポート



NTVFSの外部データベースサポート

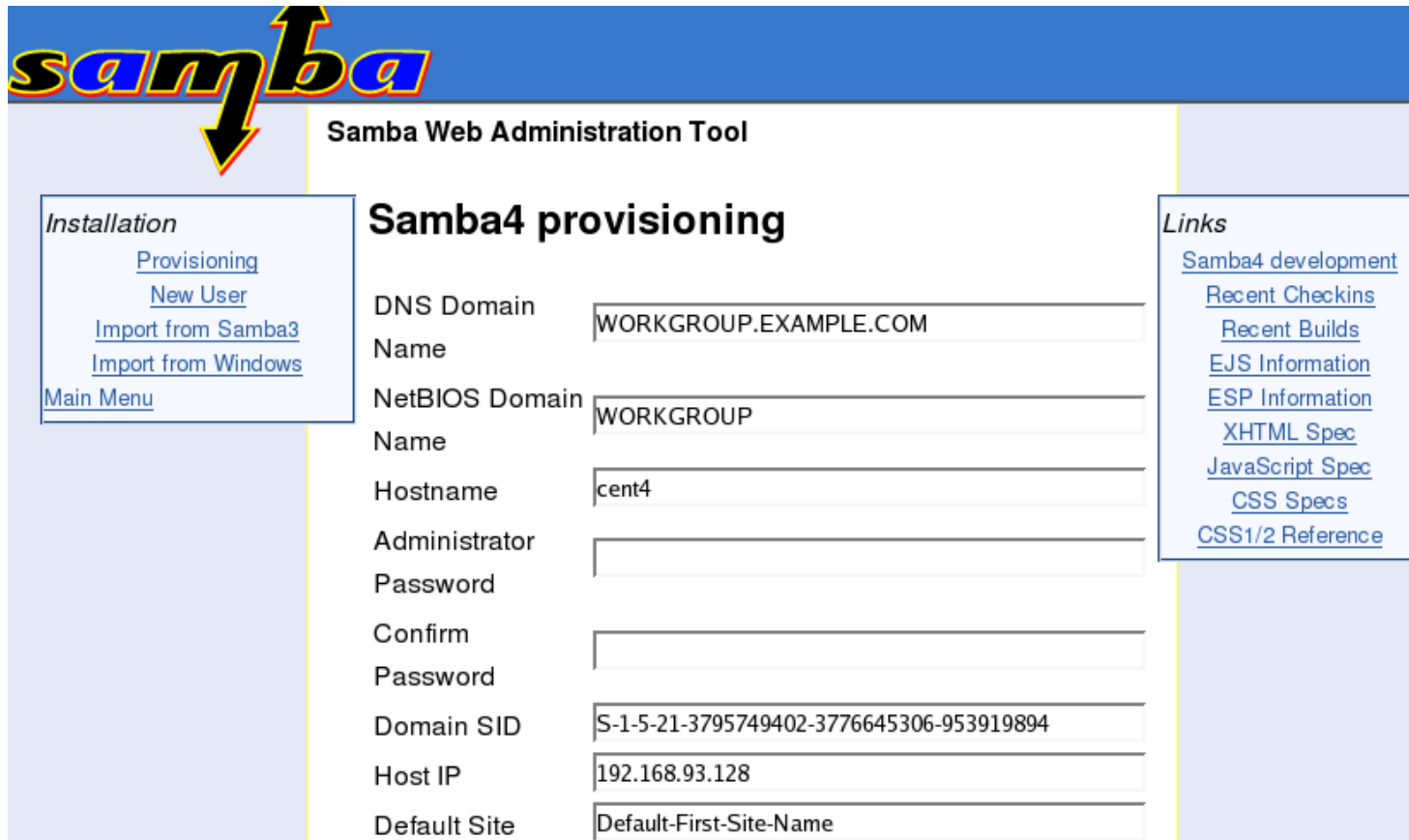
- ファイルシステムがxattrsをサポートしていない場合、下記設定で、NTFSで利用されるACLやNTファイル・ストリームのデータを格納することが可能。

smb.conf

```
posix:eadb = /usr/local/samba/var/samba/eadb.tdb
```

SWAT2

- Ajax採用によりユーザインタフェース向上(の予定)



The image shows the Samba Web Administration Tool (SWAT) interface. At the top is a blue header with the 'samba' logo in yellow and blue. Below the header, the title 'Samba Web Administration Tool' is displayed. The main content area is titled 'Samba4 provisioning' and contains several form fields for configuring a Samba4 environment. On the left side, there is a sidebar with links for 'Installation', 'Provisioning', 'New User', 'Import from Samba3', 'Import from Windows', and 'Main Menu'. On the right side, there is a sidebar with links for 'Links', 'Samba4 development', 'Recent Checkins', 'Recent Builds', 'EJS Information', 'ESP Information', 'XHTML Spec', 'JavaScript Spec', 'CSS Specs', and 'CSS1/2 Reference'.

Samba4 provisioning	
DNS Domain Name	WORKGROUP.EXAMPLE.COM
NetBIOS Domain Name	WORKGROUP
Hostname	cent4
Administrator Password	
Confirm Password	
Domain SID	S-1-5-21-3795749402-3776645306-953919894
Host IP	192.168.93.128
Default Site	Default-First-Site-Name

Samba & ZFS ソリューションの紹介

- ZFS
 - Sunが開発した次世代ファイルシステム
 - Solaris10/OpenSolaris/FreeBSD/Mac OS X
 - LVM機能、RAID機能なども統合
 - 128bit アドレッシング ファイルシステム
 - 各種諸元が実質無限大

Samba 3.2.0 + ZFSのメリットは？

Samba 3.2 + ZFS のメリット

- ディレクトリ単位のQuota制限の実現
 - NTFS同等の容量制限機能を実現
- vfs_zfsaclによるACL機能のサポート
 - NTFS同等のACL機能
- ZFSのスナップショットによるボリュームシャドウコピー機能の活用
 - Windows 2003サーバと同等のサービス提供
- 大容量ファイルシステム + Sambaによる大規模ファイルサーバの実現
 - 1ファイルシステム 約13TBの検証実績あり

開発者向け Samba情報

- Samba 3.2系

\$ svn co svn://svnanon.samba.org/samba/branches/SAMBA_3_2 samba3.2

- Samba 4.0系

\$ svn co svn://svnanon.samba.org/samba/branches/SAMBA_4_0 samba4.0

- ソースの変更内容

- <http://viewcvs.samba.org/cgi-bin/viewcvs.cgi/>

- Bug Report

- <http://bugzilla.samba.org>

Part 5

OSSTech 製品紹介

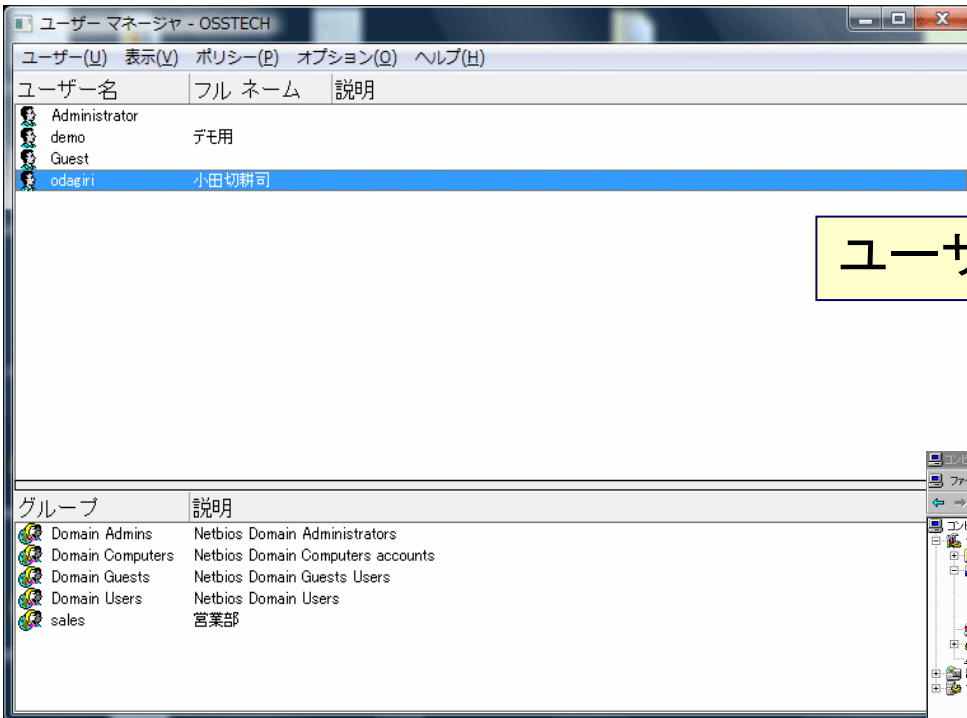


OSSTech

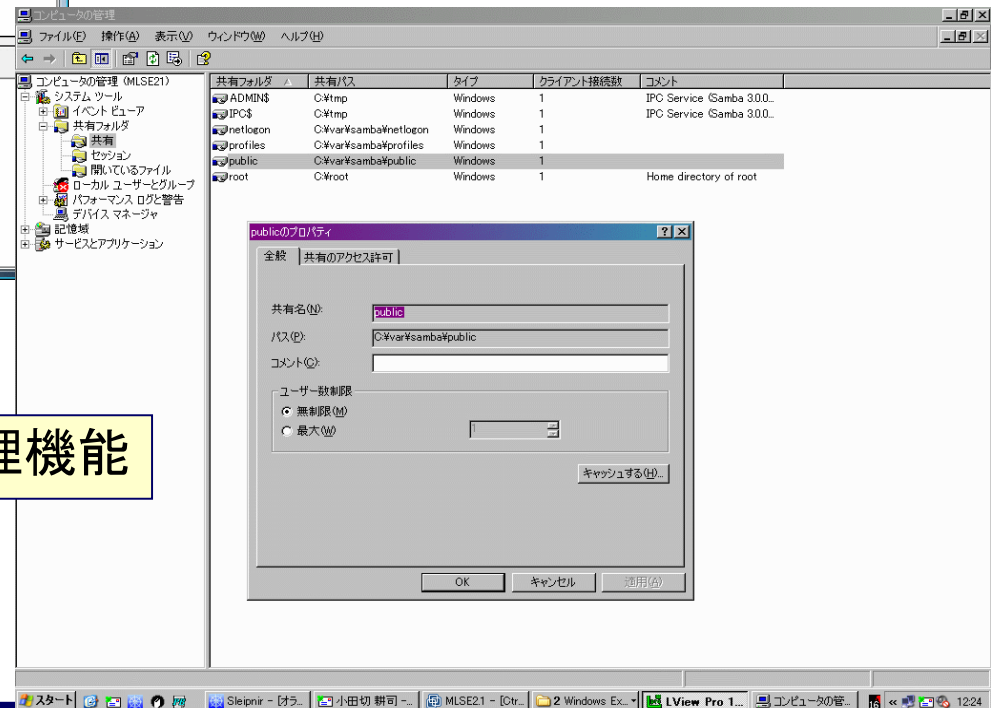
Samba 3.0.24 for Solaris/Linux

- **Windows Vista / Mac OS X対応**
 - **JIS2004対応、合成文字UTF-8-MAC対応**
- **OpenLDAPだけでなく、商用LDAP製品にも対応**
- **Solaris版/Linux版向けsmbldap-toolsを同梱**
 - **LDAPへのユーザ／グループ登録がコマンドで可能**
 - **大量一括登録可能**
- **SolarisもLinuxもAD認証統合**
- **オリジナルのさまざまな不具合を修正**
- **WindowsからGUIでユーザ管理可能**

Windows GUIでSambaが管理できる！



ユーザ管理機能

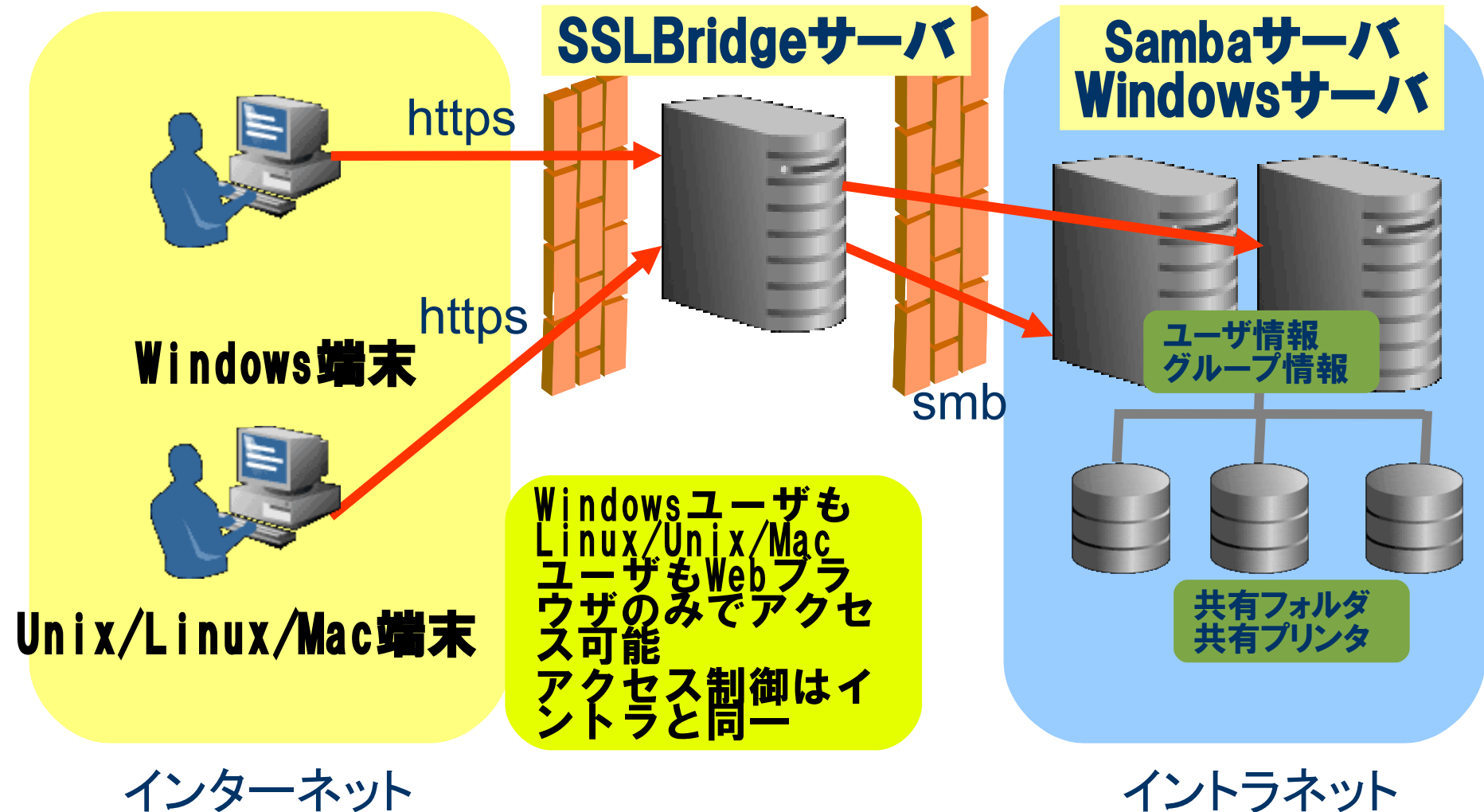


共有管理機能

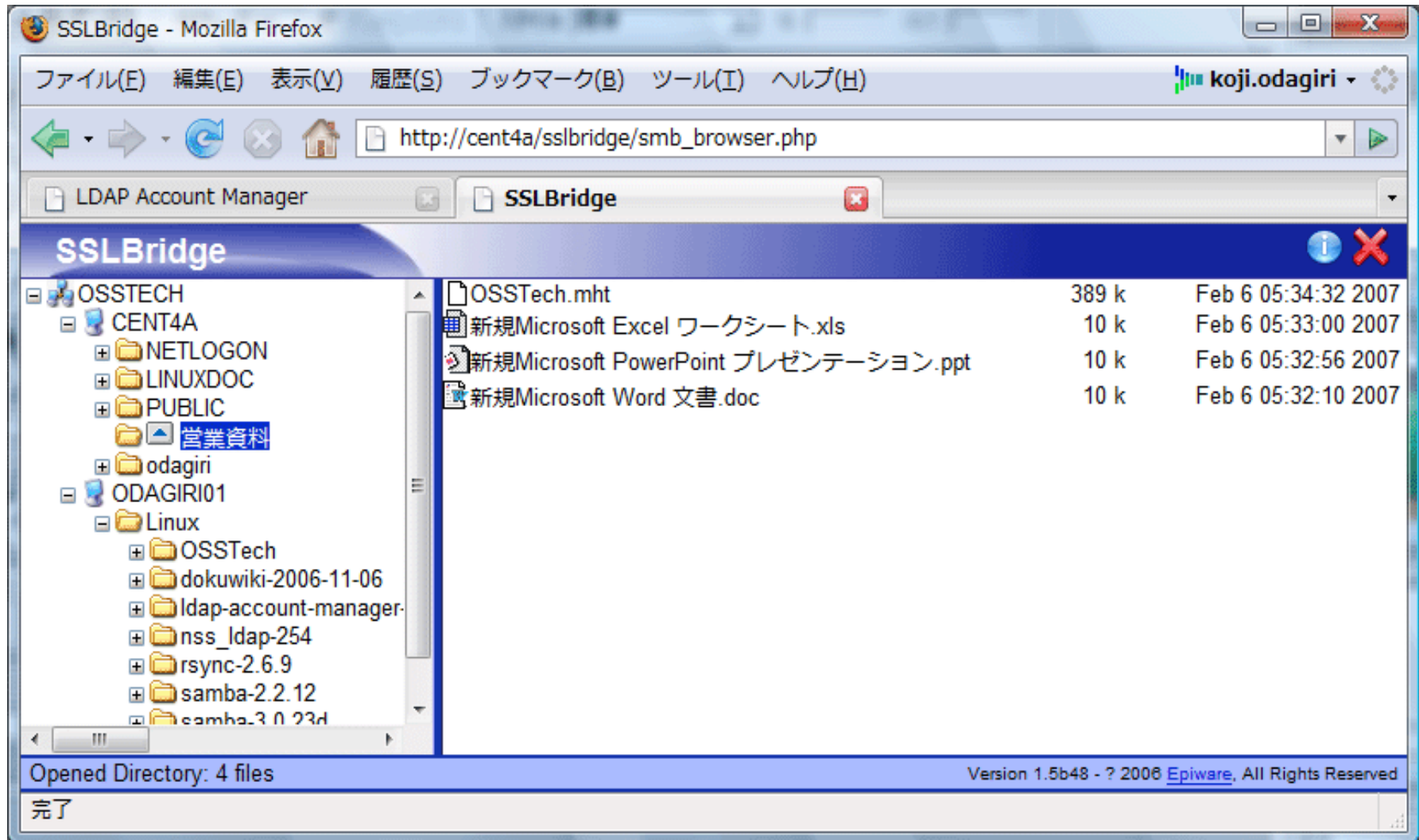
OpenLDAP 2.2.30 / 2.3.32 for Solaris/Linux

- 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
- Solaris Java Directory Serverは同一マシン上にLDAPクライアントとサーバが同居できないが、OpenLDAPは同居可能
- 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



LAM:LDAP Account Manager

- Solaris 10 / Red Hat EL 4 / CentOS 4対応
- Https経由のWebクライアントからLDAPを管理可能
- プロファイルを変えることで分散管理を可能にする



LDAP Account Manager - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

http://cent4a/lam/templates/login.php

寄付する

LDAP Account Manager

ログアウト

ツール

ツリービュー ユーザ グループ ホスト Samba ドメイン

リフレッシュ <=> 4名のユーザが見つかりました 1

	ユーザ ID	(姓でない)名	姓	UID番号	GID番号
フィルタ					
☐ 編集	Administrator		Administrator	0	0
☐ 編集	demo	demo	demo	1000	513
☐ 編集	Guest		Guest	999	514
☐ 編集	odagiri	耕司	小田切	1003	513

すべてを選択

リフレッシュ <=> 4名のユーザが見つかりました 1

GID番号をグループ名に変換: ☐ 適用

新しいユーザ ユーザを削除

完了