

Windowsファイルサーバ(Samba)への セキュアなリモートアクセス (SSLBridge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

- OSSTech社紹介
- Samba紹介
- コンサルティング・サービスおよび
サポート・サービス・メニュー
- OSSTech社製品紹介

オープンソース・ソリューション・テクノロジー 会社紹介

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
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、販売およびメンテナンス ・ソフトウェアおよび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
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
所属団体等	<ul style="list-style-type: none"> ・Linuxコンソーシアム理事 ・社団法人コンピュータソフトウェア協会(CSAJ) ・オープンソースソフトウェア協会
主要取引先 および パートナー様	<ul style="list-style-type: none"> ・デル株式会社 ・日本電信電話株式会社 ・日本電気株式会社 ・株式会社 大塚商会 ・キャノンマーケティングジャパン株式会社 ・富士通ネットワークソリューションズ株式会社 ・株式会社 日立情報システムズ ・株式会社 博報堂 ・大分シーイーシー株式会社 ・Data Foundation 株式会社 ・ミラクル・リナックス株式会社

オープンソース・ソリューション・テクノロジー株式会社

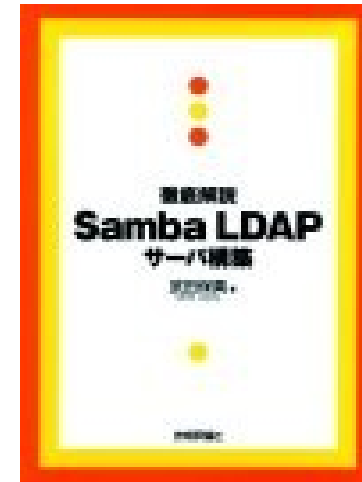
- 昨年 9月に設立
- **OSに依存しないOSSのソリューションを中心に提供**
 - Linuxだけでなく、SolarisやFreeBSDへも対応！
- **Samba、LDAPなどによる認証統合ソリューションを提供**
 - 製品パッケージ提供
 - 製品サポート提供
 - 技術コンサルティング提供

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

社員による著作紹介

- ◆ **小田切**
- ◆ 技術評論社 Software Design 2006年7月号
 - 「巻: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**
- ◆ 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)」



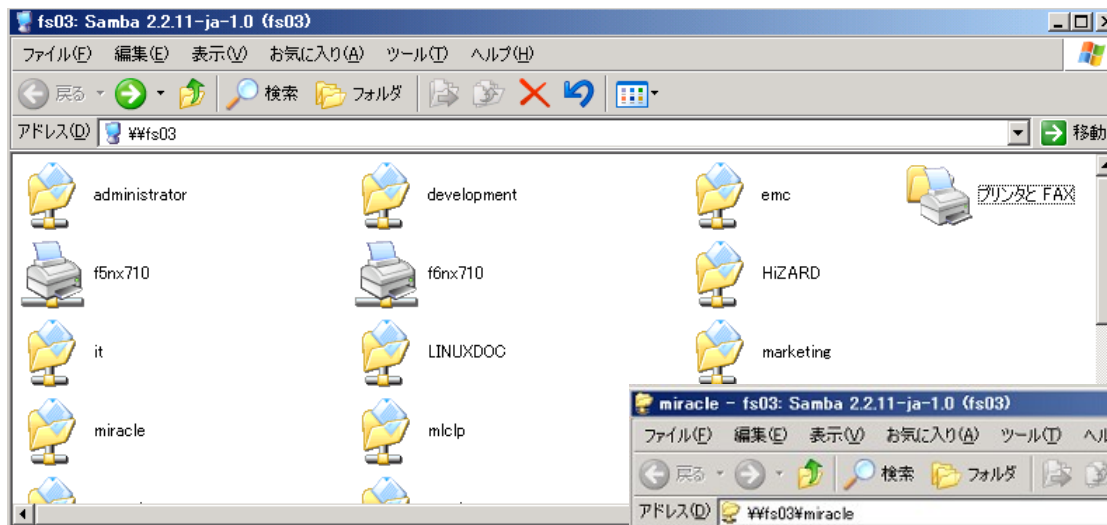
ファイルサーバ「Samba」とは



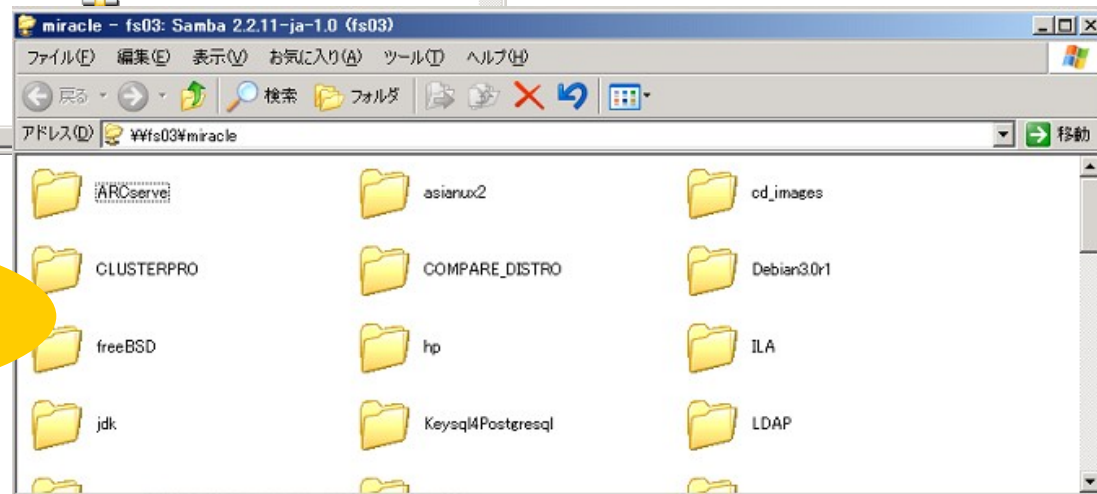
OSSTech

Samba(サンバ)とは

LINUXなどのUNIX系OS上で稼動する、Windowsのファイル、プリンタ共有機能を提供するオープン・ソースソフトウェア



Sambaサーバへアクセスした画面



一般ユーザはWindowsで構築した画面と見分けが付きません！

WindowsファイルサーバをLinux+Sambaで構築する理由

1. セキュリティ対策

- Windowsに比べ、ウィルスなどの被害が圧倒的に少ない。

2. コスト削減

- Windows2003では、アクセスするユーザごとにCAL(Client Access License)が必要
- サーバ自体のハードウェア価格が安い。

3. 高い信頼性

- 連続運転に強い(メモリ・リークがない)
- オープンソースなので障害調査しやすく、修正も可能

4. 運用のしやすさ

- シェルのスクリプト化によって、運用の効率化が可能
- 修正モジュールの適用に、OSリブートの必要がない

Sambaの機能概要

1. ファイルサーバ機能

- Samba3.0はWindowsと同等以上の機能をサポート

2. Windows GUIによる管理機能

- ユーザ管理、共有管理がWindowsの GUI画面で可能

3. ドメインコントローラ機能

- NTドメインのドメインコントローラが備えるユーザ情報、システムポリシー、ログオンスクリプトなどを実装。

4. WINSサーバ機能

- Windowsネットワークで使われる「コンピュータ名」をIPアドレスに変換

5. Windowsドメイン連携/Winbind機能

- LinuxサーバをWindowsドメインに参加させることができる
- Windowsドメイン内のユーザIDやグループIDをLinuxサーバ上で使用

Samba3.0のファイルサーバ機能

Samba3.0はWindowsと同等以上の機能をサポート

- ユーザ/グループによる容量制限(ディレクトリ単位にも対応可)
- 論理ボリューム・マネージャ
- 日本語ディレクトリ/ファイル名
- ゴミ箱機能:ユーザが誤って削除したファイルを復元 ★
- ユーザごとの作業ディレクトリ ★
- 分散ファイルシステム(MS-DFS)/オフラインファイル機能
- ACL(アクセスコントロールリスト)による詳細なアクセス許可の設定
Windows NTFSと同様のアクセス制御が可能

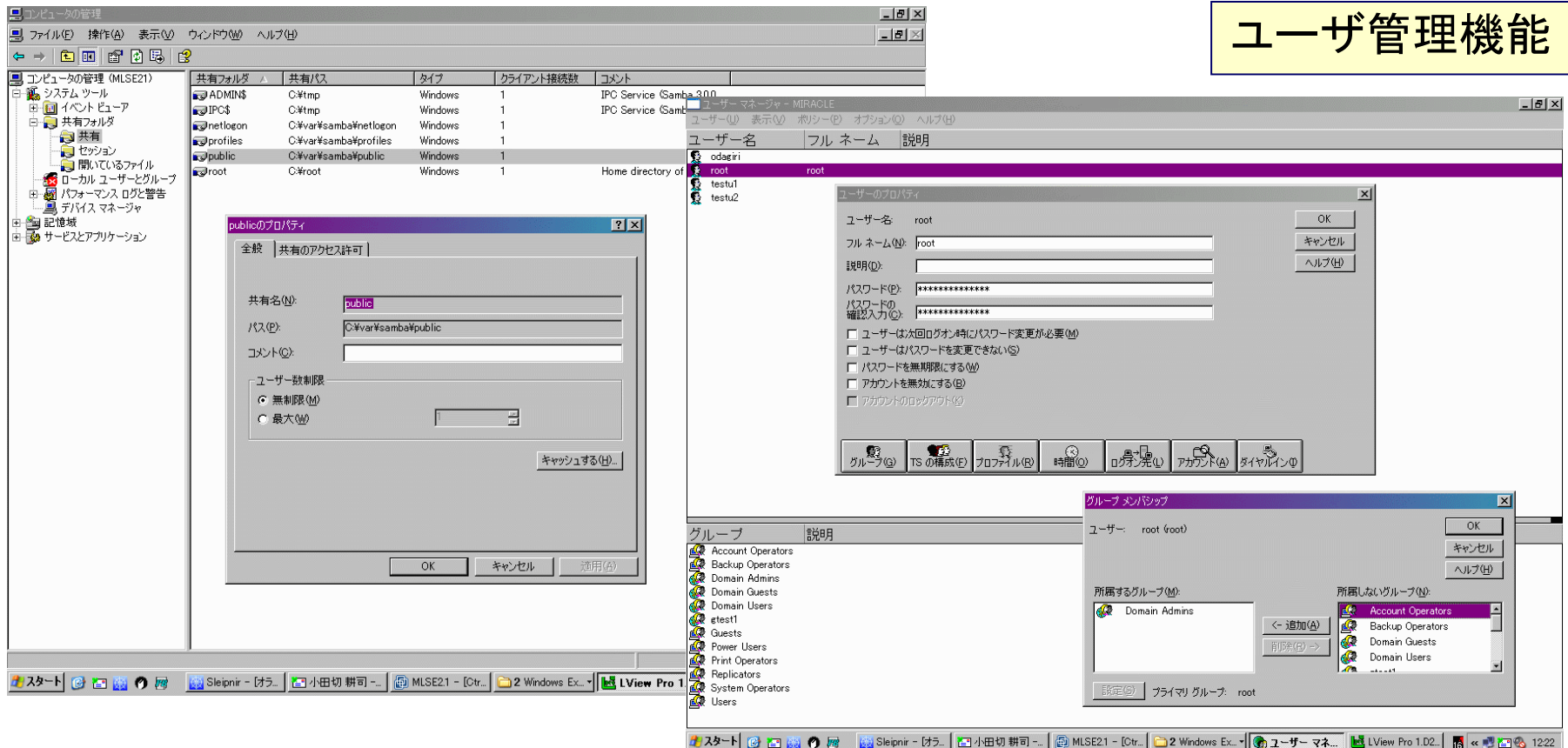
★:Windows2003で実装されていない機能

Windows GUIによるSamba管理画面

ユーザ管理、共有管理がWindows GUIで可能

共有管理機能

ユーザ管理機能



The screenshot displays the Windows Management Console (MMC) interface for Samba management. The main window shows a list of shared folders and drives with columns for Name, Path, Type, Client Connections, and Comments. A 'public' share is highlighted, and its properties dialog box is open, showing the share name 'public' and the path 'C:\var\samba\public'. The user permissions are set to '無制限' (Unlimited).

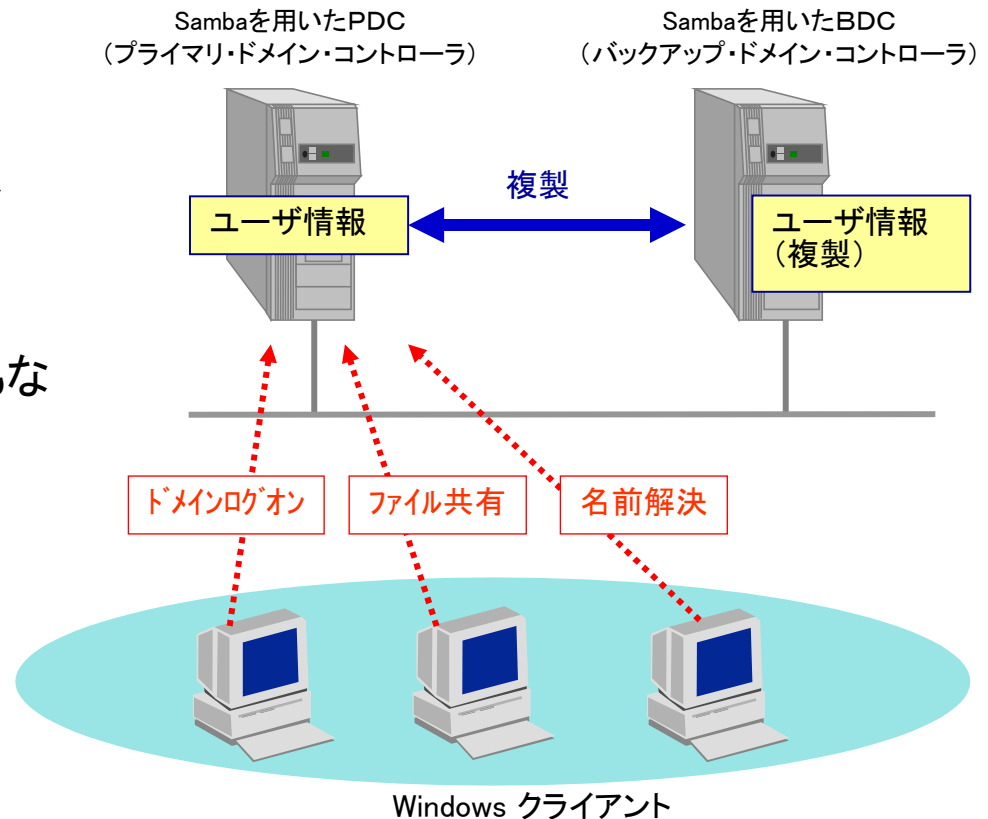
Overlaid on this are two other dialog boxes. The first is the 'ユーザーのプロパティ' (User Properties) dialog, showing the user 'root' with a full name of 'root' and a password field. The second is the 'グループメンバシップ' (Group Membership) dialog, showing the user 'root' is a member of the 'Domain Admins' group.

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

ドメイン・コントローラ機能とは？

ドメインコントローラ(DC)は、Windowsドメインを構築する際にユーザ情報などを管理するサーバのこと。

- PDC: ユーザ情報を格納・管理
- BDC: PDCで管理されているユーザ情報の複製を保持
※参照のみで、追加・変更は不可
- Sambaサーバは、PDCにもBDCにもなれるが、ユーザ情報複製には、ディレクトリ・サービスの「LDAP」が必要



Active DirectoryによるUnix, Linux, Macの認証統合

**Linux / Unix
Samba 3.0**

- ・ファイルサーバ
- ・メールサーバ
- ・Proxyサーバ
- ・FTPサーバなど

**Windows 2000/2003
Active Directory**

認証要求

ユーザ管理はすべてWindows上で
行いLinuxやUnixに
ユーザを作成する
必要はない

共有フォルダ
共有プリンタ

共有フォルダ
共有プリンタ

ユーザ情報
グループ情報

Unix/Linux/Mac端末

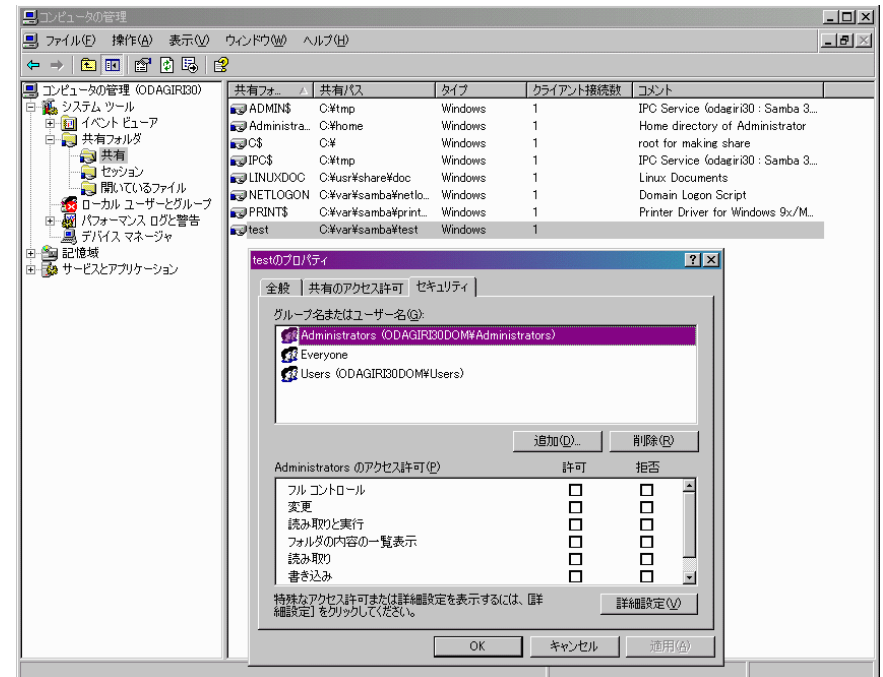
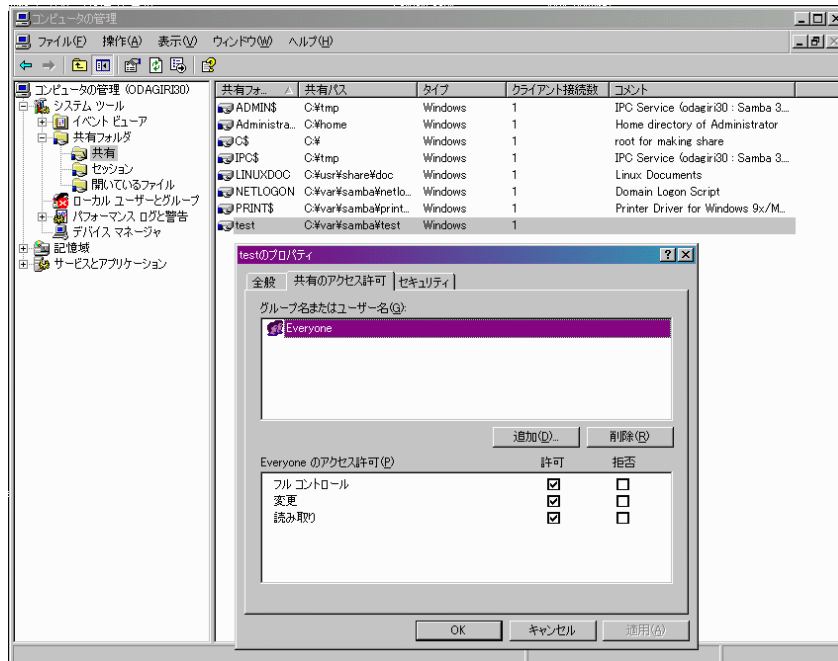
Windows端末

Sambaのセキュリティ機能

- ACL機能
 - Windowsと同等の共有やフォルダに対するアクセス制御
- 監査機能
 - 誰がどのファイルにアクセスしたかログに保存
- 課金機能
 - 誰がどの位サーバを利用していたか課金情報を保存
- リアルタイムウイルスチェック機能
 - F-SecureやSophosアンチウイルス製品と連携
- Hide UnReadable機能
 - 参照権のないファイルを表示させない
- Hide UnWriteable機能
 - 更新権のないファイルを表示させない
- Hide Files機能
 - 任意のファイルを表示させない

Sambaのセキュリティ機能: ACL機能

- Windowsと同等の共有やフォルダに対するアクセス制御



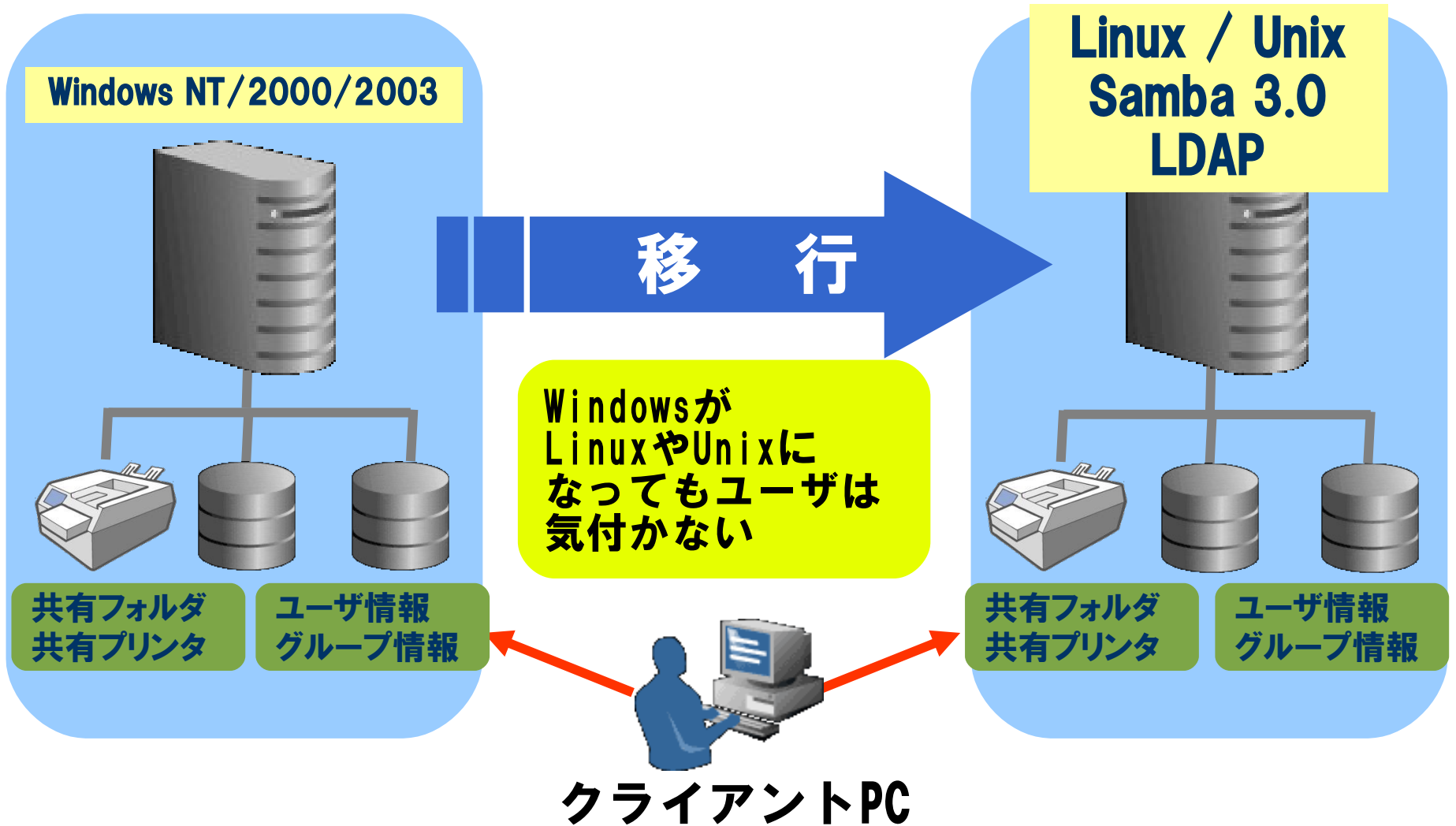
Sambaのセキュリティ機能: 監査機能

- 誰がどのファイルにアクセスしたかログに保存
- 共有単位で監査情報を出すか、出さないか設定
- ログはすべてシスログに保存
- UNIXのsyslogdに送信することも可能
- 出力例

```
Feb 24 17:26:30 dhcp-0144
smbd_abs_audit[1402]: open /usr/share/public/
新規テキストドキュメント.txt (fd 26)
[odagiri@10.1.0.115] for writing

Feb 24 17:26:40 dhcp-0144
smbd_abs_audit[1402]: close
/usr/share/public/新規テキストドキュメント.txt (fd
26) [odagiri@10.1.0.115]
```

WindowsからSambaへの移行



コンサルティング・サービス
サポート・サービス
メニュー

FreeOSに関するサポートとコンサルティング

- 弊社が検証したDELL PowerEdgeへのFreeOS導入サービス
- 上記OSへのさまざまなOSSの導入および設定
- 御客様が導入したFreeOSやOSSに関する問い合わせや障害調査
- 導入設定は20万円～
- 問い合わせ／障害解析は5万円～

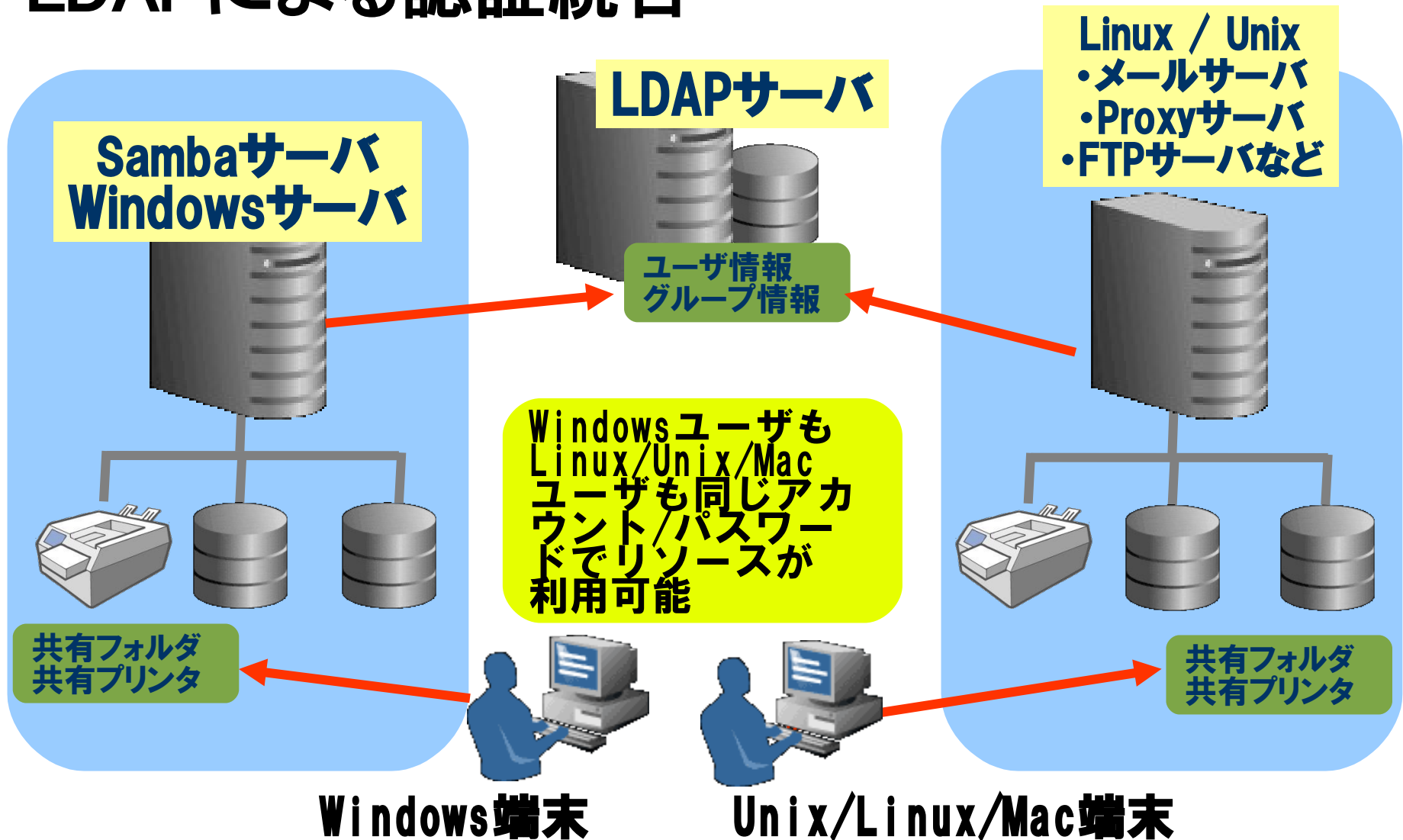
問い合わせ (1インシデント5時間以内)			ダンプ解析／ソースコード解析 (1インシデント40時間以内)		
インシデント数	価格	有効期限	インシデント数	価格	有効期限
1	5万円	3ヶ月	1	50万円	3ヶ月
5	21万円	1年	5	210万円	1年
10	36万円	1年	10	360万円	1年

- お見積もり [お問い合わせ info@osstech.co.jp](mailto:info@osstech.co.jp)

コンサルティングサービスメニュー

- **OSS(オープンソース・ソフトウェア)を活用したシステム認証基盤構築サービスのご提案**
- OSSや商用LDAP製品を使ったOSS認証基盤構築サービス
OSSのSambaとOpenLDAP(もしくは商用LDAP製品)を使い、Windows, Unix, Linux, Macの認証統合を行う。
OSプラットフォームとしてLinuxだけでなく、Solarisなどの商用UNIXにも対応する。Active Directoryのような分散管理や権限委譲機能も提供。
- 既存のNISやNIS+からLDAPへの移行サービス
古い商用UNIX認証環境をOSSのSambaとOpenLDAP(もしくは商用LDAP製品)を使い移行する。Windowsクライアントの認証にも対応可能。
- Active DirectoryによるUnix, Linux, Macの認証統合
OSSのSambaを使い、Unix, Linux, Macクライアントおよびサービス(メール、Web、FTPなど)の認証をWindows Active Directoryを使って行う。
- 上記ソリューションのための**製品、サポート、コンサルティング**を提供

LDAPによる認証統合

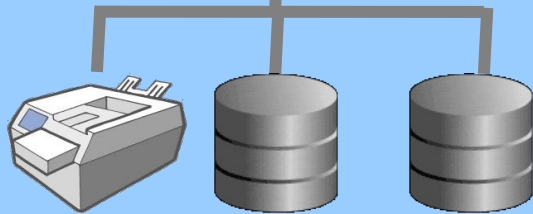


Active DirectoryによるUnix, Linux, Macの認証統合

Linux / Unix

Samba 3.0

- ・ファイルサーバ
- ・メールサーバ
- ・Proxyサーバ
- ・FTPサーバなど

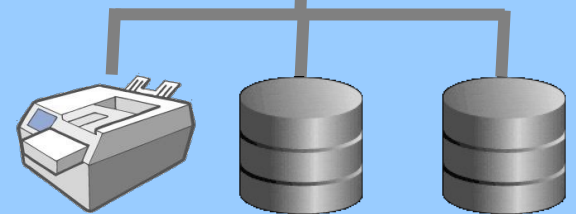
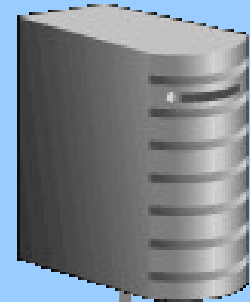


共有フォルダ
共有プリンタ

認証要求

ユーザ管理はすべてWindows上でを行いLinuxやUnixにユーザを作成する必要はない

**Windows 2000/2003
Active Directory**



共有フォルダ
共有プリンタ

ユーザ情報
グループ情報

Unix/Linux/Mac端末

Windows端末

Samba/OpenLDAP保守サービス内容

サービスの種類		拡張サービス	サービスの内容
価格		Sambaのみ24万円/サイト・年 LDAPのみ 24万円/サイト・年 Samba+LDAP 36万円/サイト・年	Sambaサーバ運用に関する問い合わせ対応。 対応時間帯: 営業日の9時~17時
問い合わせ対応		○	Sambaサーバ運用に関する問い合わせ対応。 対応時間帯: 営業日の9時~17時
パッチの問い合わせ		○	コミュニティやディストリビュータから提供されている既存パッチに関する問い合わせ対応。
障害調査	発生現象の確認・調査	○	発生現象の確認と、過去に発生した障害の調査。
	メッセージの調査	○	Sambaサーバが出力する各種ログの調査。
	coreダンプの調査	○	Sambaが出力したcoreファイルの調査。
	再現環境の構築・評価	○	再現環境構築、評価。
	コミュニティへのフィードバック	○	新規障害判明時、コミュニティに対する障害報告と対応の働きかけを行う。 ただし、本サービスは障害解決を保証するものではない。
データの保障・復旧		コンサルティング・サービスで対応	ユーザデータの保障・復旧作業。
パフォーマンス分析・チューニング		コンサルティング・サービスで対応	Sambaサーバの性能情報収集、分析、チューニング作業。
パッチ作成		○	パッチ作成・適用。
Windowsドメインからの移行		コンサルティング・サービスで対応	既存のWindowsNTドメイン環境をクライアント側設定変更なし(ユーザやマシンの再登録なしで)にSamba環境へ移行します。
運用フェーズ前のサポート		コンサルティング・サービスで対応	システム設計、構築、性能チューニング、評価フェーズのサポート。

OSSTech社 製品

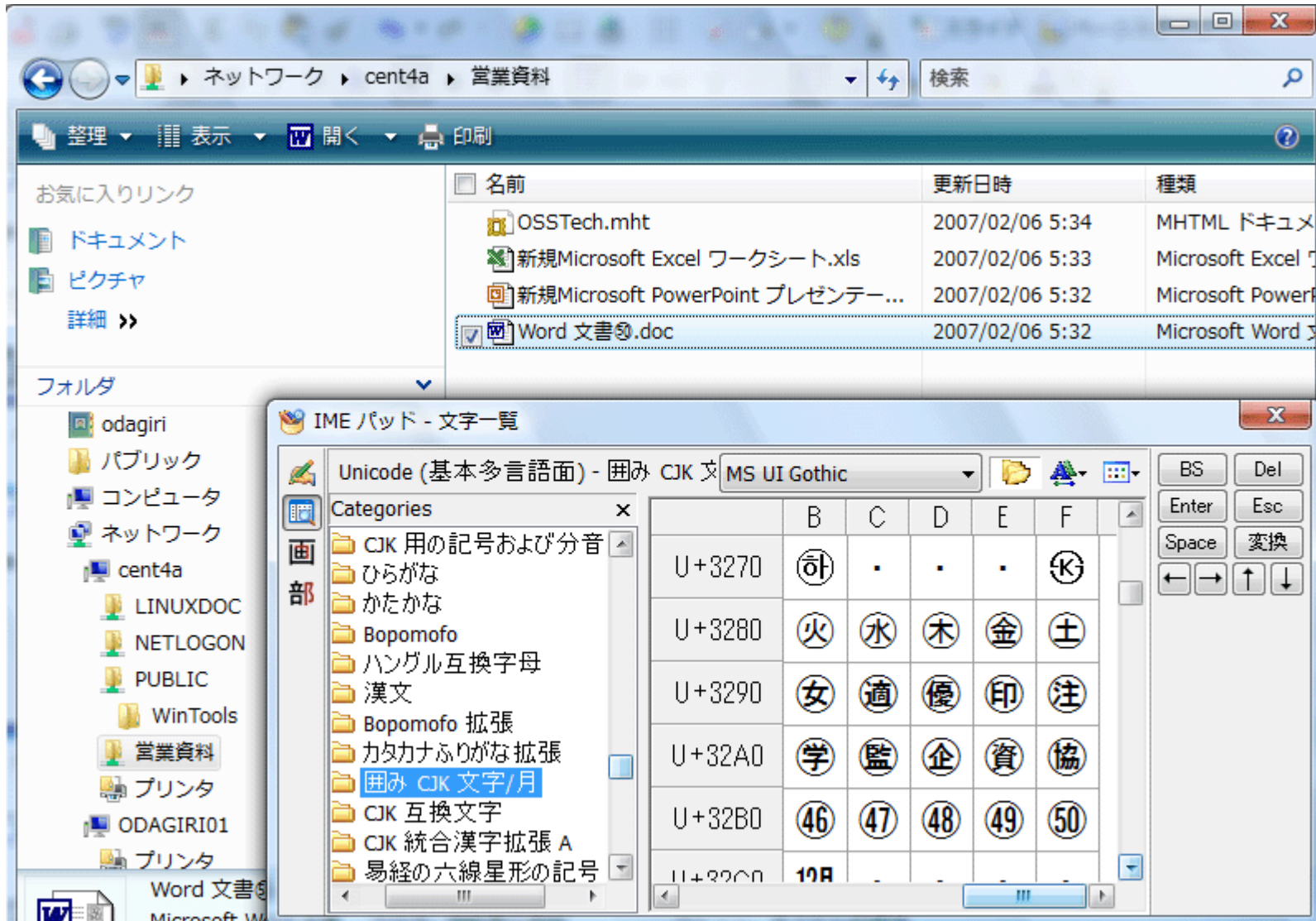
OSSTech社 製品

- Samba 3.0.24 for Solaris/Linux
 - Solaris 10 / Red Hat EL 4 / CentOS 4対応
 - クライアントはWindows Vistaにも対応
- SSLBridge
 - Red Hat EL 4 / CentOS 4対応
 - Https経由のWebクライアントからAjaxでアクセス
 - Sambaサーバだけでなく、Windowsサーバへもアクセス可能
- 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

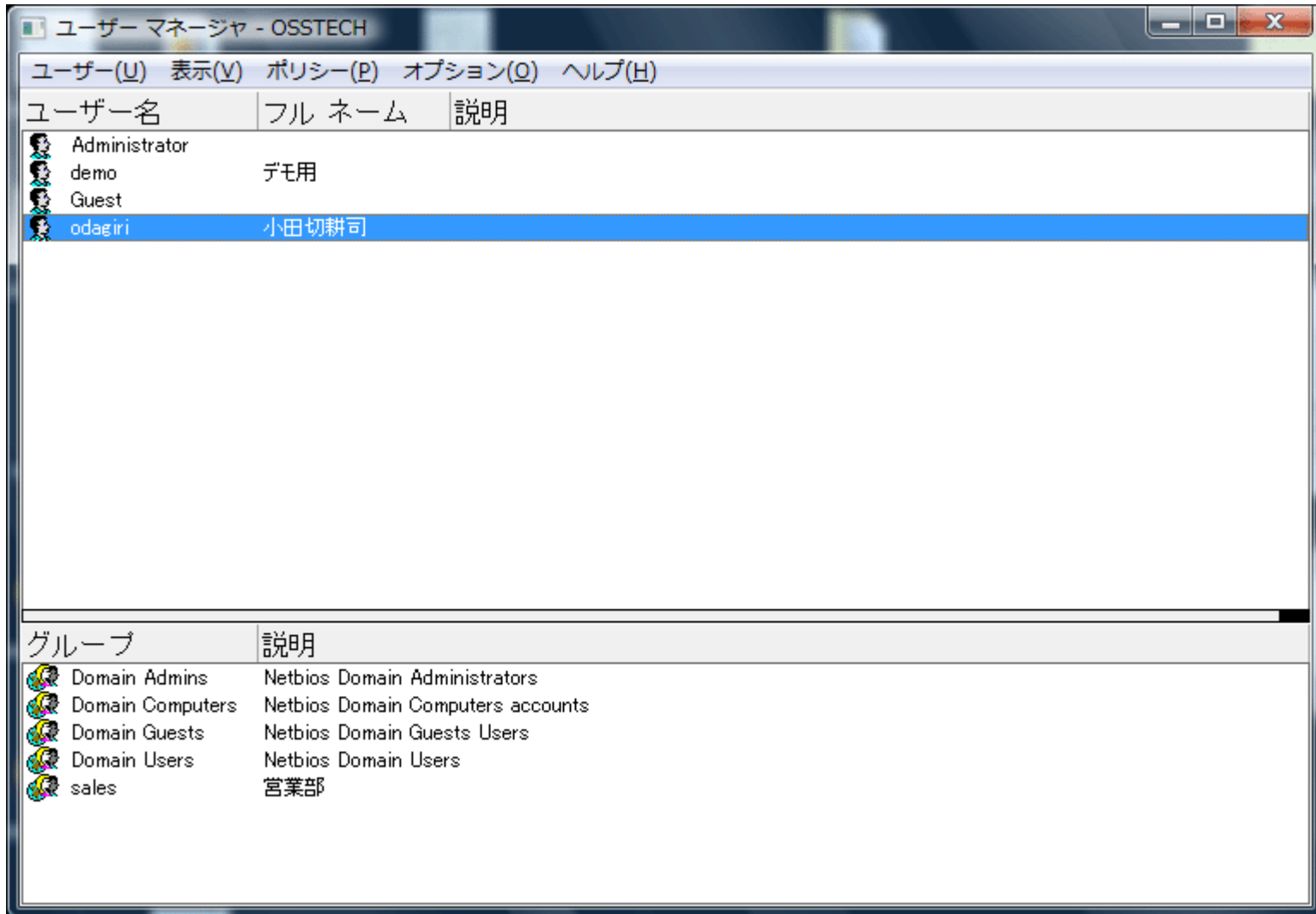
Samba 3.0.24 for Solaris/Linux

- Solaris 10 / Red Hat EL 4 / CentOS 4対応
- クライアントはWindows Vistaにも対応
- オリジナルで発生するいくつかの問題を修正
- OpenLDAPやSUN Dsとの連携をサポート
- smbldap-toolsも提供

Samba 3.0.24 for Solaris/Linux



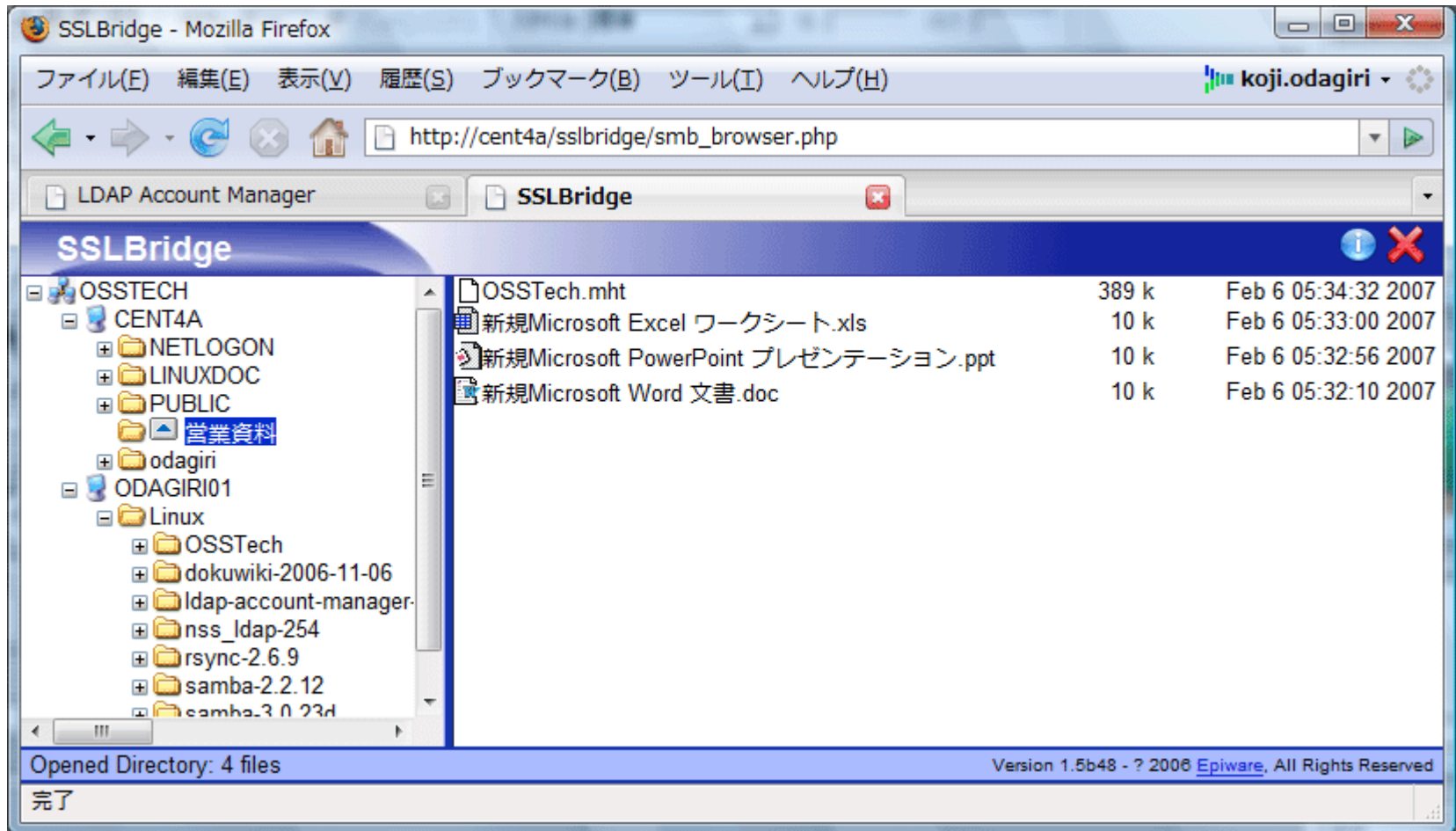
Samba 3.0.24 for Solaris/Linux



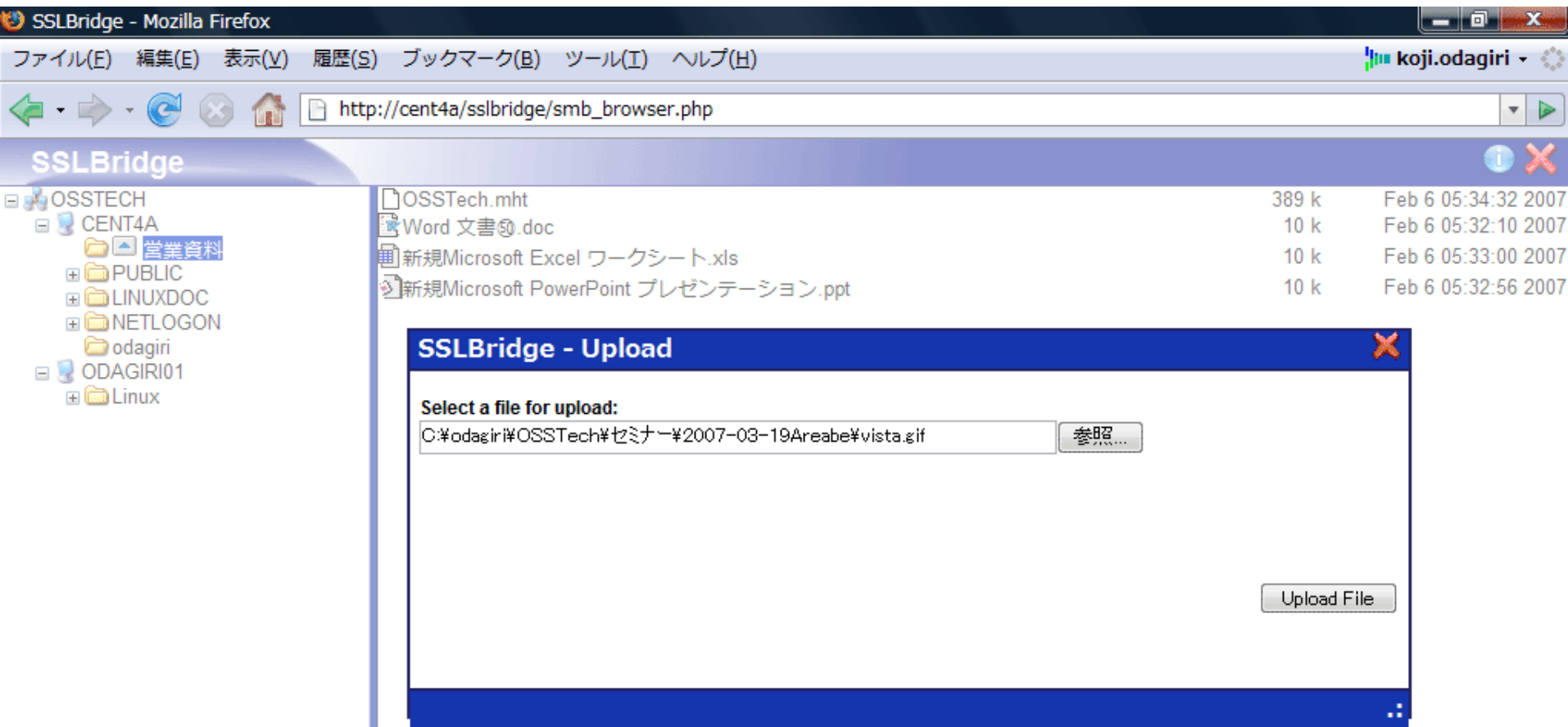
SSLBridge

- Red Hat EL 4 / CentOS 4対応
- Windowsファイルサーバ上のファイルのダウンロードやアップロードなどをWebブラウザ(httpsで暗号化し通信)経由で行うことができます。
- WindowsファイルサーバとしてLinux/Unix上のSambaはもちろん、Windows Server 2003やWindows Storage Server , Windows 2000 Serverにアクセスすることが可能です。
- SSLBridgeのWebクライアントはAjaxで構成されており、ブラウザ経由の操作であっても軽快な動作が特徴です。
- オリジナルのSSLBridgeは日本語環境に対応していないため、弊社が改良を行ったSSLBridge日本語版を提供しています

SSLBridge



SSLBridge



SSLBridge - 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) koji.odagiri

http://cent4a/sslbridge/smb_browser.php

SSLBridge

- OSSTECH
 - CENT4A
 - 営業資料
 - PUBLIC
 - LINUXDOC
 - NETLOGON
 - odagiri
 - ODAGIRI01
 - Linux

OSSTech.mht	389 k	Feb 6 05:34:32 2007
Word 文書@.doc	10 k	Feb 6 05:32:10 2007
新規Microsoft Excel ワークシート.xls	10 k	Feb 6 05:33:00 2007
新規Microsoft PowerPoint プレゼンテーション.ppt	10 k	Feb 6 05:32:56 2007

SSLBridge - Upload

Select a file for upload:

C:\odagiri\OSSTech\セミナー\2007-03-19Areabe\vista.gif 参照...

Upload File

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

LAM:LDAP Account Manager



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) koji.odagiri

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

😊 寄付する

✳ ツール

LDAP Account Manager ➡ ログアウト

🏠 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					
<input type="checkbox"/> 編集	Administrator		Administrator	0	0
<input type="checkbox"/> 編集	demo	demo	demo	1000	513
<input type="checkbox"/> 編集	Guest		Guest	999	514
<input type="checkbox"/> 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

Windows taskbar: Wind..., LDAP..., Cent..., cent..., OSS..., Adob..., CAPS KANA, 23:46

😊 寄付する

✖ ツール

LDAP Account Manager

➡ ログアウト

🏠 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 | 新しいエントリを作成)

🌐 dc=osstech,dc=co,dc=jp (6)

👤 ou=Computers

👤 ou=Groups (10)

👤 ou=ldmap

👤 ou=Users (4)

👤 uid=Administrator

👤 uid=demo

👤 uid=Guest

👤 uid=odagiri

★ 新しいエントリを作成

🌐 sambaDomainName=OSSTECH

🌐 sambaDomainName=OSSTECH

★ 新しいエントリを作成

uid=odagiri

DN: uid=odagiri,ou=Users,dc=osstech,dc=co,dc=jp

🔄 リフレッシュ

🗑 削除

💡 ヒント: 属性を削除するには、テキストフィールドを空にして保存してください。

★ 新しいエントリを作成

✖ 内部属性を表示する

📄 エクスポート

📄 新しい属性の追加

cn

必須

odagiri

(値の追加)

displayName

小田切耕司

gecos

System User