

OSSTech Samba 3.0.24 に追加した修正内容について



OSSTech

目次

1.概要.....	1
2.Windows Vista 対応パッチ.....	1
3.セキュリティ修正パッチ.....	2
4.OSSTech 提供 Samba に適用しているその他のパッチ.....	2
5.OSSTech パッケージのベースとした Fedora Core 用 RPM パッケージで適用されていたパッチ.....	5
6.更新履歴.....	6

1.概要

本ドキュメントは、OSSテクノロジー提供の Samba パッケージに独自に適用している修正内容について記載しています。本ドキュメントの対象となる Samba パッケージは、samba 3.0.24-1.35_OSSTECH です。ご利用の Samba パッケージのバージョンの確認は、次のコマンドで確認することができます。

```
$ /usr/sbin/smbd -V
Version 3.0.24-1.35_OSSTECH
```

2.Windows Vista 対応パッチ

<http://www.samba.org/samba/patches/> にて提供されている samba 3.0.24 用パッチの適用

- share_security_ntlmv2.diff
 - smb.conf で”security = share”の共有認証モードにおいて、Windows Vista クライアントが NTLMv2 認証で、ワークグループ情報を利用するための修正
- spoolss.diff
 - Windows Vista クライアントから Samba のプリントサーバ機能を利用するときに正常に動作しない問題を修正
 - Windows Vista クライアントから Samba サーバにプリンタドライバをアップロードする機能が動作しない問題を修正
- vista_backup_acl.diff
 - Windows Vista のバックアップ機能で Samba サーバの共有フォルダにバックアップを行う際に、エラーとなる問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4361
- variable_os_expansion.diff
 - smb.conf のクライアント OS マクロ “%a”で、Windows Vista を判定可能にするための修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4093
- dfs_referral.diff
 - Samba サーバのある共有フォルダに複数の MS-DFS リンクを作成した場合に、Windows Vista クライアントから MS-DFS リンクが正常に動作しない問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4356
- directory_delete.diff
 - Samba の共有フォルダ内に作成されたディレクトリに、複数のディレクトリが作成されており、そのうち 1 つのディレクトリにオフラインモードが有効になっている場合に、Windows Vista クライアントから、ディレクトリを削除できない問題を修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4188

以上のパッチをまとめたものが **samba-3.0.24-vista-patchset.patch** です。

<http://www.samba.org/samba/patches/> にて提供されている samba 3.0.24 用以外の Windows Vista パッチの適用

- smbclient から Samba サーバに接続したときに、%a マクロが Windows Vista クライアントとして扱われる問題の修正
 - <http://lists.samba.org/archive/samba-technical/2007-February/052008.html>
 - **samba-3.0.24-arch_macro.patch**

- Vista クライアントから接続したときに %a マクロが Windows 2000 と同等になってしまう問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4484
 - **samba-3.0.24-vista-patchset.patch** に修正内容が含まれます。
- Windows Vista クライアントから Samba サーバにプリンタドライバのアップロード機能が正常に動作しない問題を修正 (Windows Vista 対応の spoolss.diff パッチの適用漏れの修正)
 - <http://websvn.samba.org/cgi-bin/viewcvs.cgi?view=rev&root=samba&rev=21100>
 - **samba-3.0.24-vista-patchset-misc.patch**

3.セキュリティ修正パッチ

- smbд の SID 変換ルーチンに含まれる脆弱性のため、一般ユーザが root 権限を取得できる可能性がある問題を修正 (CVE-2007-2444)
- CVE-2007-2444 の修正パッチにおいて、シェルで有効な文字のリストに「c」が抜けていた問題の修正
 - **samba-3.0.24-CVE-2007-2444_v2.patch**
- リモートからのコード実行を可能にするヒープオーバーフローの脆弱性の修正 (CVE-2007-2446)
- CVE-2007-2446 の修正に伴って、ドメインメンバーサーバの共有にアクセスできなくなる問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4637
 - **samba-3.0.24-CVE-2007-2446_v2.patch**
- 正しくエスケープされていない文字が/bin/sh に渡されることによってリモートからコマンドを実行できる可能性がある脆弱性の修正
- CVE-2007-2444 の修正に伴って、”force group”機能が正常に動作しなくなる問題を修正
 - **samba-3.0.24-CVE-2007-2447_v2.patch**
- nmbd のドメインログオン処理に含まれるバッファオーバーフローの脆弱性を修正 (CVE-2007-6015)
 - **samba-3.0.27a-CVE-2007-6015.patch**
- nmbd の WINS サーバ機能の名前解決処理に含まれる脆弱性を修正 (CVE-2007-5398)
 - **samba-3.0.26a-CVE-2007-5398.patch**

4.OSSTech 提供 Samba に適用しているその他のパッチ

- 共有フォルダに “hide unreadable = yes”を設定すると、MS-DFS リンクが表示されなくなる問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=3319
 - **samba-3.0.23d-ignore-hide_xxxx-for-msdfs.patch**
- Samba の提供するコマンド(smbclient など)に設定されているタイムアウト時間(10 秒)を 60 秒に変更する修正
 - **samba-3.0.11-timeout.patch**
- Office 2000、Office XP、Office 2003 など、ACL(アクセス制御)がかかった Excel ファイルなどを開くと、ACL の設定が正しく反映されず、更新不可(参照のみ可能)となってしまう問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=2346
 - **samba-3.0.20a-try_chown.patch**

- **samba-3.0.23d-bug-2239.patch**
- Winbind による Active Directory/NT ドメイン連携時に ID マップバックエンド rid を利用しているとき、信頼関係を結んだドメインのユーザアカウントも利用するための修正
 - **samba-3.0.23d-idmap_rid_multipledomain_support.patch**
- Winbind による Active Directory/NT ドメイン連携時に、smb.conf の template homedir パラメータなどに %G マクロを利用したときに、グループ名が変換されず GID が利用される問題の修正
 - **samba-3.0.24-winbind-groupname.patch**
- unix charset = EUCJP-MS 環境下で、ローマ数字の大文字(I、II、III)などを大文字・小文字変換した際に、バイト数が異なるため共有フォルダへのアクセスなどに失敗する問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=1029
 - **samba-3.0.23d-strupper_m.patch**
 - **samba-3.0.23d-struplower.patch**
- 日本語 man ページの追加、および日本語 man ページのインストール処理の追加
 - **samba-3.0.23d-i18nman.patch**
- Linux 以外のプラットフォーム(Solaris など)で mlock()の際のメモリアライン処理の修正(Samba 3.0.25 からのバックポート)
 - <http://lists.samba.org/archive/samba-technical/2007-February/051863.html>
 - **samba-3.0.24-memalign-for-mlock.patch**
- winbindd のメモリリークの修正 (Samba 3.0.25 からのバックポート)
 - <http://lists.samba.org/archive/samba-technical/2007-February/051849.html>
 - **samba-3.0.25svn-winbindd_group-memoryleak.patch**
 - <http://lists.samba.org/archive/samba-technical/2007-March/052606.html>
 - **samba-3.0.24-winbind-ads-enum-groupmembers.patch**
- LDAP 連携時に、LDAP にアクセスする際に適切なパーミッションが設定されていない問題の修正 (Samba 3.0.25 からのバックポート)
 - <http://websvn.samba.org/cgi-bin/viewcvs.cgi?view=rev&rev=21507>
 - **samba-3.0.25svn-become_root-to-access-ldap.patch**
- Winbind による Active Directory 連携時に ID マップバックエンド ad ID を利用した際に、winbindd が異常終了する問題の修正 (samba 3.0.25 からのバックポート)
 - <http://lists.samba.org/archive/samba-cvs/2007-January/073777.html>
 - **samba-3.0.24-idmap_ad-use_attr_uidnumber.patch**
- Winbind による Active Directory 連携時に wbinform のオプションとして -group-info を利用可能にするための修正(samba 3.0.25 からのバックポート)
 - **samba-3.0.25svn-wbinfo-groupinfo.patch**
- AD サーバへの接続失敗時に ldap_open() の失敗理由をエラーログに出力するための修正 (samba 3.0.25 からのバックポート)
 - **samba-3.0.24-ldap_open-debug.patch**
- Solaris において krb5_locate_kdc() が衝突しクラッシュする問題の修正 (samba 3.0.25 からのバックポート)
 - **samba-3.0.24-krb5_locate_kdc.patch**
- パスワードバックエンド ldapsam において、LDAP DIT に sambaAlgorithmicRidBase 属性がある場合、もしくは sambaNextRid 属性がない場合に algorithmic rid にフォールバックするための修正 (旧バージョンとの互換性確保)
 - **samba-3.0.24-ldapsam-algorithmic-rid.patch**

- SMB の chain reply 処理でバッファサイズが適切でない問題を修正
 - <http://websvn.samba.org/cgi-bin/viewcvs.cgi?view=rev&root=samba&rev=21731>
 - **samba-3.0.24-chain_reply-new_size.patch**
- security=share の設定時に、SMB パケット内に格納されている共有名のバッファの位置を正しく扱っていない問題の修正
 - **samba-3.0.25svn-security-share.patch**
- winbind 利用時に Active Directory に多数のユーザ/グループエントリが登録されている場合にエントリの取得に失敗する問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=3024
 - **samba-3.0.25svn-winbind-ads-user-count.patch**
- パスワードの有効期限を無期限に延長することを可能にする修正
 - https://bugzilla.samba.org/show_bug.cgi?id=2836
 - **samba-3.0.24-password-never-expires.patch**
- LDAP サーバからの切断を検出せずに、既に切断された LDAP 接続で 10 回のリトライ(約 10 秒間)後、LDAP サーバに再接続する問題を修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4372
 - **samba-3.0.25svn-ldap-rebind-on-serverdown.patch**
- Solaris10 の ZFS でボリュームシャドウコピー機能を利用可能にするための、VFS 用モジュールの追加
 - <http://lists.samba.org/archive/samba-technical/2007-February/051506.html>
 - **samba-3.0.24-vfs_shadow_copy_zfs.patch**
- security = server 設定時にドメインコントローラの探索に時間がかかるため、認証ダイアログの表示が遅延する問題の修正
 - **samba-3.0.24-improve_security_server.patch**
- pam_smbpass.so モジュールを利用して、passwd コマンドで Samba のパスワード変更を試みると、パスワード変更に失敗する問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4759
 - **samba-3.0.25svn-pdb_ldap-ber_printf-n.patch**
- LDAP サーバーのホスト名にドメイン名が設定されていないとき、DNS による名前解決ができない場合などに、LDAP サーバーに接続できない問題を修正
 - **samba-3.0.24-ads_connect-ip.patch**
- Solaris10 の PAM+Winbind 環境で pam_winbind を利用したパスワード変更機能が動作しない問題を修正
 - **samba-3.0.24-pam_winbind-chauthtok.patch**
- パスワードの有効期限に近づいたアカウントに対して、Windows と同じく 14 日前から警告が表示されるように修正
 - **samba-3.0.24-pam_winbind-warn-expires.patch**
- VFS の recycle モジュールで、min size パラメーター以下のサイズのファイルを見捨てるように修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4409
 - **samba-3.0.24-vfs_recycle-minsize.patch**
- VFS の recycle モジュール利用時に、他のユーザーによって削除されてゴミ箱に移動されたファイルにアクセスした際に、ファイルアクセス時刻が更新されるように変更

- **samba-3.0.24-vfs_recycle-touch.patch**
- ユーザーマネージャーの「パスワードの変更を禁止する」機能をバックポート
 - **samba-3.0.24-passwdcannotchange.patch**
- 64bit 環境で、Samba のユーザーパスワード有効期限などに関する属性が 64bit で作成されますが、適切に処理されていなかった問題を修正
 - **samba-3.0.24-improve_64bit_time_t.patch**
- Solaris8 など Samba にリンクするスレッドライブラリが原因で、コネクションが頻繁に切断される問題を修正
 - https://bugzilla.samba.org/show_bug.cgi?id=5024
 - **samba-3.0.24-solaris-libsmbclient-mt.patch**
- パスワード変更時に、LDAP に設定されたパスワードポリシーを満たさなかった場合のエラーコードを NT_STATUS_PASSWORD_RESTRICTION に変更
 - https://bugzilla.samba.org/show_bug.cgi?id=5163
 - **samba-3.0.28.svn-ldap-password-policy.patch**
- acl group control パラメーターか、dos filemode パラメーターが設定されているときに、ファイルのグループに所属するユーザーが ACL を変更可能にできるように修正
 - https://bugzilla.samba.org/show_bug.cgi?id=5202
 - **samba-3.0.24-dos_filemode.patch**
- VFS の file_quota モジュールを追加
 - **samba-3.0.24-vfs_file_quota.patch**

5.OSSTech パッケージのベースとした Fedora Core 用 RPM パッケージで適用されていたパッチ

OSSTech 提供のパッケージは、Fedora Core 用に提供されていた samba-3.0.24-12.fc7 をもとに作成しています。このパッケージで適用されていた以下のパッチを、OSSTech 提供のパッケージでも適用しています。

- winbindd の通信用パイプのディレクトリを”/tmp/.winbindd”から”/var/run/winbindd”に変更する修正
 - **samba-3.0.0beta1-pipedir.patch**
- smbд、nmbд、winbindd のログファイル名を”log.xxx”から”xxx.log”に変更する修正
 - **samba-3.0.23-logfiles.patch**
- nmbдなどに-n オプションで NetBIOS 名を指定することを可能にする修正
 - **samba-3.0.0rc3-nmbд-netbiosname.patch**
- Winbind 連携利用時にグループ情報のパスワードエントリを”x”の代わりに”*”を設定する修正
 - **samba-3.0.23rc3-passwd.patch**
- smbspool コマンドでユーザー名が指定されていないときに、NULL の代わりに”dummy”を設定する修正
 - **samba-3.0.21pre1-smbspool.patch**
- smbclient の-M オプション利用時に 138 番ポートを利用するように変更
 - **samba-3.0.13-smbclient.patch**
- msdfs root パラメータのデフォルト値を Samba 3.0.25 と同様に yes から no に変更

- **samba-3.0.24-msdfs-root-no.patch**
- pam_winbind がドメインコントローラにないユーザ認証に対して常にエラーログを出力してしまう問題の修正
 - https://bugzilla.samba.org/show_bug.cgi?id=4094
 - **samba-3.0.24-pam_winbind-fixes.patch**
- ライブラリ build 時の libnss モジュールのチェックを追加
 - **samba-3.0.24-enable_pam_nss_tests.patch**
- libnss_wins のシンボル名が解決できない問題の修正
 - **samba-3.0.24-nss_wins.patch**
- Windows Vista で msdfs のエラーが発生したときに、適切なエラーメッセージを返却するための修正
 - **samba-3.0.24-vista_msdfs_errcodes.patch**

6.更新履歴

- 2008年1月29日: 第10版(samba 3.0.24-1.35_OSSTECH)
 - セキュリティパッチの追加
 - **samba-3.0.24-CVE-2007-4572.patch**
 - **samba-3.0.27a-CVE-2007-6015.patch**
 - パスワード変更時に LDAP のパスワードポリシーを満たさなかった場合のエラーコードを修正
 - **samba-3.0.28.svn-ldap-password-policy.patch**
 - acl group control パラメーター、もしくは dos filemode パラメーターが設定されているときに、ファイルのグループに所属するユーザーが ACL の設定を変更可能に修正
 - **samba-3.0.24-dos_filemode.patch**
 - VFS の file_quota モジュールを作成し追加
 - **samba-3.0.24-vfs_file_quota.patch**
- 2007年10月25日: 第9版 (samba 3.0.24-1.29_OSSTECH)
 - pam_smbpasswd の PAM モジュールのパスワード変更に関する問題を修正
 - **samba-3.0.25bsvn-pdb_ldap-ber_printf-n.patch**
 - 参照する LDAP サーバーのホスト名にドメイン名が設定されていないとき、AD への接続に失敗する問題の修正
 - **samba-3.0.25bsvn-pdb_ldap-ber_printf-n.patch**
 - Solaris10 で PAM+Winbind 構成のときに、pam_smbpass によるパスワード変更が行えない問題を修正。
 - **samba-3.0.24-pam_winbind-chauthtok.patch**
 - パスワードの有効期限の 14 日前から、有効期限が近づいていることを示すメッセージを表示するように変更
 - **samba-3.0.24-pam_winbind-warn-expires.patch**
 - ごみ箱フォルダに移動できる最小のファイルサイズ制限を指定可能に改善
 - **samba-3.0.24-vfs_recycle-minsize.patch**

- ごみ箱機能利用時に、他のユーザーによって削除されたファイルにアクセス可能にするための修正
 - samba-3.0.24-vfs_recycle-touch.patch
- ユーザーマネージャーで「パスワードの変更を禁止する」機能を利用可能に改善
 - samba-3.0.24-passwdcannotchange.patch
 - samba-3.0.24-improve_64bit_time_t.patch
- Solaris8などでリンクされるスレッドライブラリが原因で、コネクションが一定時間を越えると切断されてしまう問題を修正
 - samba-3.0.24-solaris-libsmbclient-mt.patch
- 2007年7月9日: 第8版 (samba 3.0.24-1.22_OSSTECH)
 - security = server 設定時にクライアント側で認証ダイアログの表示が遅延する問題の改善
 - samba-3.0.24-improve_security_server.patch
 - Solaris ZFS でボリュームシャドウコピー機能を利用するための VFS モジュールの追加
 - samba-3.0.24-vfs_shadow_copy_zfs.patch
 - smbclient で日本語共有名が利用できない問題の修正
 - samba-3.0.24-tar_options.patch の削除
- 2007年6月10日: 第7版(samba 3.0.24-1.19_OSSTECH)
 - セキュリティパッチ(CVE-2007-2447)の不具合の修正
 - samba-3.0.24-CVE-2007-2447_v2.patch
 - セキュリティパッチ(CVE-2007-2446)の不具合の修正
 - samba-3.0.24-CVE-2007-2446_v2.patch
 - セキュリティパッチ(CVE-2007-2444)のパッチの統合
 - samba-3.0.24-CVE-2007-2444_v2.patch
- 2007年6月4日: 第6版 (samba 3.0.24-1.17_OSSTECH)
 - セキュリティパッチ(CVE-2007-2444)の不具合修正
 - samba-3.0.24-CVE-2007-2444-fix.patch
 - samba-3.0.25 に適用された修正のバックポート
 - samba-3.0.25svn-ldap-rebind-on-serverdown.patch
- 2007年5月15日: 第5版(samba 3.0.24-1.15_OSSTECH)
 - セキュリティパッチの追加
 - samba-3.0.24-CVE-2007-2444.patch
 - samba-3.0.24-CVE-2007-2446.patch
 - samba-3.0.24-CVE-2007-2447.patch
 - Fedora Core のパッケージに適用されたパッチの追加
 - samba-3.0.24-enable_pam_nss_tests.patch
 - samba-3.0.24-nss_wins.patch
 - samba-3.0.24-vista_msdfs_errcodes.patch
 - samba-3.0.25 に適用された修正のバックポート
 - samba-3.0.24-chain_reply_new_size.patch
 - samba-3.0.25svn-security-share.patch
 - samba-3.0.25svn-winbind-ads-user-count.patch
 - その他のパッチ
 - samba-3.0.24-password-never-expires.patch

- 2007年4月12日：第4版 (samba 3.0.24-1.11_OSSTECH)
 - 一部のパッチファイル名の誤りを訂正
 - 「IDMAP_XX」という表現を「ID マップバックエンド XX」に変更
- 2007年4月11日：第3版 (samba 3.0.24-1.11_OSSTECH)
 - パッチファイル名を追加
- 2007年4月9日：第2版 (samba 3.0.24-1.11_OSSTECH)
- 2007年4月5日：初版 (samba 3.0.24-1.9_OSSTECH)