# オープンソースソフトウェアを利用した
# 認証サービスの統合について

富士ソフト ABC（株）

## ■ 執筆者Ｐｒｏｆｉｌｅ ■

住吉　亮一

2003 年　富士ソフト ABC（株）入社
2005 年 6 月現在
IT 事業本部 九州事業所 所属

## ■ 論文要旨 ■

コンピュータソフトウェア産業が発展するなかで，プログラムのソースコードが開示され，ライセンスによっては自由に改変可能なオープンソースソフトウェアが注目を集めている．商用ソフトウェアと遜色ない機能を持ち，さらに Linux の登場によりネットワークサービスを提供するソフトウェアがより身近となった．
認証サービスの統合を，オープンソースソフトウェアである OpenLDAP ディレクトリサービスを使用して行いユーザーアカウントの保守性を向上させた．また，ユーザーに提供するサービスをオープンソースのソフトウェアで実現し，Windows サーバを廃止することによりソフトウェアライセンス購入費用の削減を可能とした．
今後の課題として，システムを管理する為に高度な管理スキルを必要とする点やアプライアンスとの連携に弱い点が挙げられる．

## ■ 論文目次 ■



## ■ 図表一覧 ■

# １．はじめに

## １．１　当社の概要

富士ソフト ABC 株式会社は 1970 年（昭和 45 年）5 月に設立され，以来「国内最大の独立系 SE 集団」として，ひのき「品質」，「納期」，「機密保持」を開発ポリシーに，特定のプラットフォームにとらわれることなく，お客様に最適な環境とは何かを考えている．大規模エンタープライズシステム構築においては，業務分析と IT コンサルティングの段階から，お客様の視点に立った柔軟な発想で最適なソリューションを提案している．高度な知識と豊富な経験に基づき，お客様を取り巻くシステム環境をあらゆる角度から精査しながら，要件定義・システム設計，プログラミングからテスト・納品まで，一貫した開発理念が高品質・高信頼性を提供している．保守，ヘルプデスク，教育といったシステム運用に至るまで，IT に関わるすべての技術サービスをお届けする「総合システムビルダー」として IT のベストパートナーとなる企業である．

1970 年　5 月　会社設立
1992 年 10 月　東証ニ部上場
1995 年　6 月　ISO9001 認証取得
1998 年　8 月　ISO14001 認証取得
1998 年　9 月　東証一部上場
2002 年　5 月　プライバシーマーク認証取得

詳しくは当社ホームページ（ URL http://www.fsi.co.jp/ ）を参照．

## １．２　オープンソースソフトウェア

昨今，商用ソフトウェアと同等の機能を持つオープンソースソフトウェアが充実している．オープンソースソフトウェアを使用して数々のサービスを提供できるようになっているが，商用ソフトウェアと比較した場合にサポートが不安などの理由で採用されない例も多い．ここではオープンソースソフトウェアで認証サービスを統合し，外部に提供するサービスもオープンソースソフトウェアで構築を行った事例を紹介する．

# ２．認証サービス統合前の問題点

ある学術機関では，ユーザー管理がサーバマシンによって異なっており，そのためアカウント管理が煩雑であった．図１に認証サービス統合前のアカウント管理を示す．ユーザーはシステムごとにパスワードを設定する必要があるためパスワードの管理が負担となっており，セキュリティ維持のための定期的なパスワード変更などに多大な労力を必要とした．一方，システム管理者はユーザーの追加や削除，パスワードの設定や初期化をシステムごとに行わなければならず手間がかかると同時に，あるシステムのみユーザーが追加されないなどの設定ミスなどが発生する懸念があった．また，年度末など大量のアカウント操作が必要な場合にはすべてのシス

テムに行わなければならず，かなりの時間と労力がかかっていた．一部， UNIX の管理は NIS を使用して統合認証を行っていたが，NIS を使用していない UNIX は統合せずに管理を行っていた．また，同一ネットワーク上に存在する Windows クライアントは Windows NT 4.0 サーバで管理されているが，アカウント情報は独立しており二重管理となっていた．

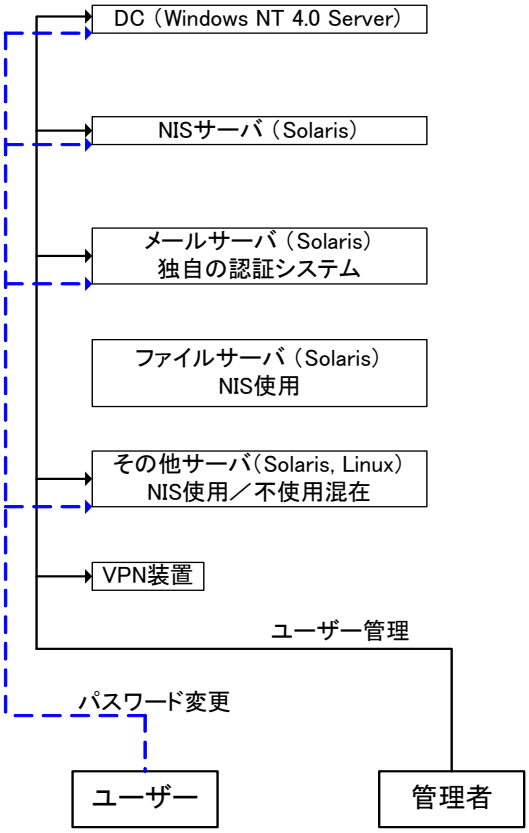


図１　認証サービス統合前のアカウント管理

## ３．認証サービス統合の実際

メールサーバとファイルサーバのリプレースを機にアカウント情報を統合し一元管理を行う認証システムを構築する．UNIX 系のシステムが多いことから Windows サーバを廃止してサーバ OS を UNIX 系に統一し，Windows 系のサービスについてクライアントアクセスライセンスを不要とした．さらにリプレース後のサーバにはサーバリソースに余力が発生するため，ユーザーに提供するサービスを追加することとした．

また，ソフトウェアライセンス費用を抑えるため，オープンソースソフトウェア／フリーソフトウェアを積極的に使用することも要件として盛り込まれた．今回のリプレースでは，オープンソースソフトウェア／フリーソフトウェアを可能な限り利用しソフトウェアライセンス費用を抑えるが，OS についてはハードウェアを含むサポートが充実している Red Hat Enterprise Linux（RHEL）を採用した．

認証サービスは UNIX / Linux 上で動作可能，かつ今回の要件を満たすことができるソフトウェアとして，オープンソースソフトウェアである OpenLDAP を使用して提供することとする．OpenLDAP は LDAP V3 プロトコルをサポートするディレクトリサーバであり，情報入手がしやすいことや今回のユーザー数（300 ユーザー程度），今回の案件ではパフォーマンスも問題ないと判断した．OpenLDAP には Samba のスキーマをインクルードしており，Windows ドメインに関する情報も LDAP で一元管理を行う．

図２は認証サービス統合後のアカウント構成を示したものである．図１と比較してユーザー，管理者共に「メールサーバ／認証サーバ」のみ変更を加えるとすべてのサーバに反映されるため，管理のしやすさが大幅に向上する．

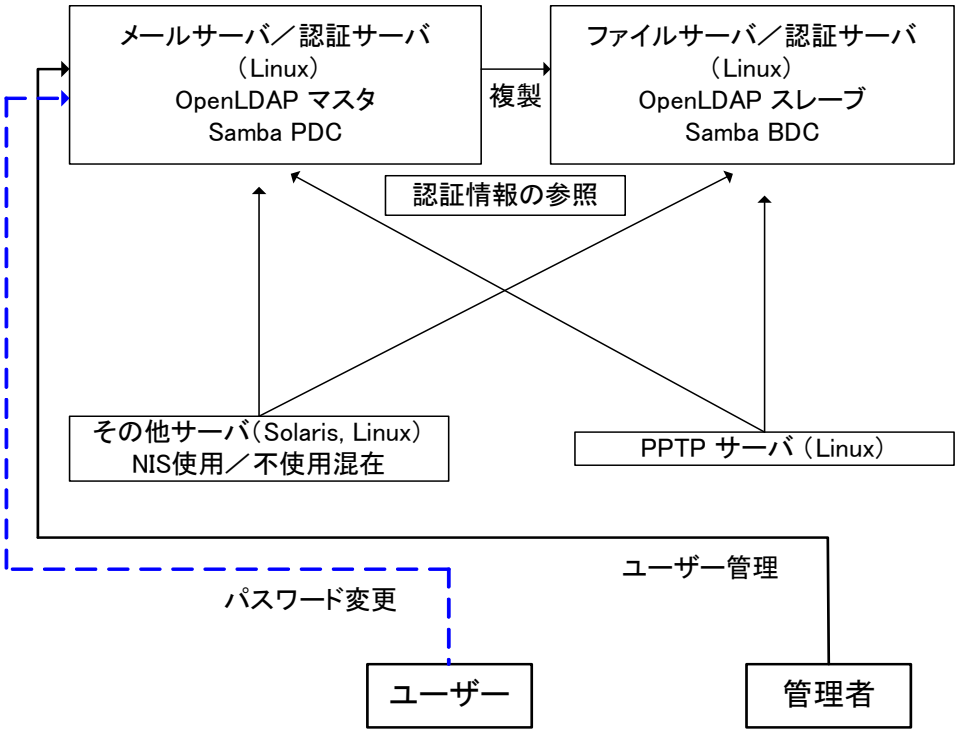


図２　認証サービス統合後のアカウント管理

認証サービスの構成について図３に示す.

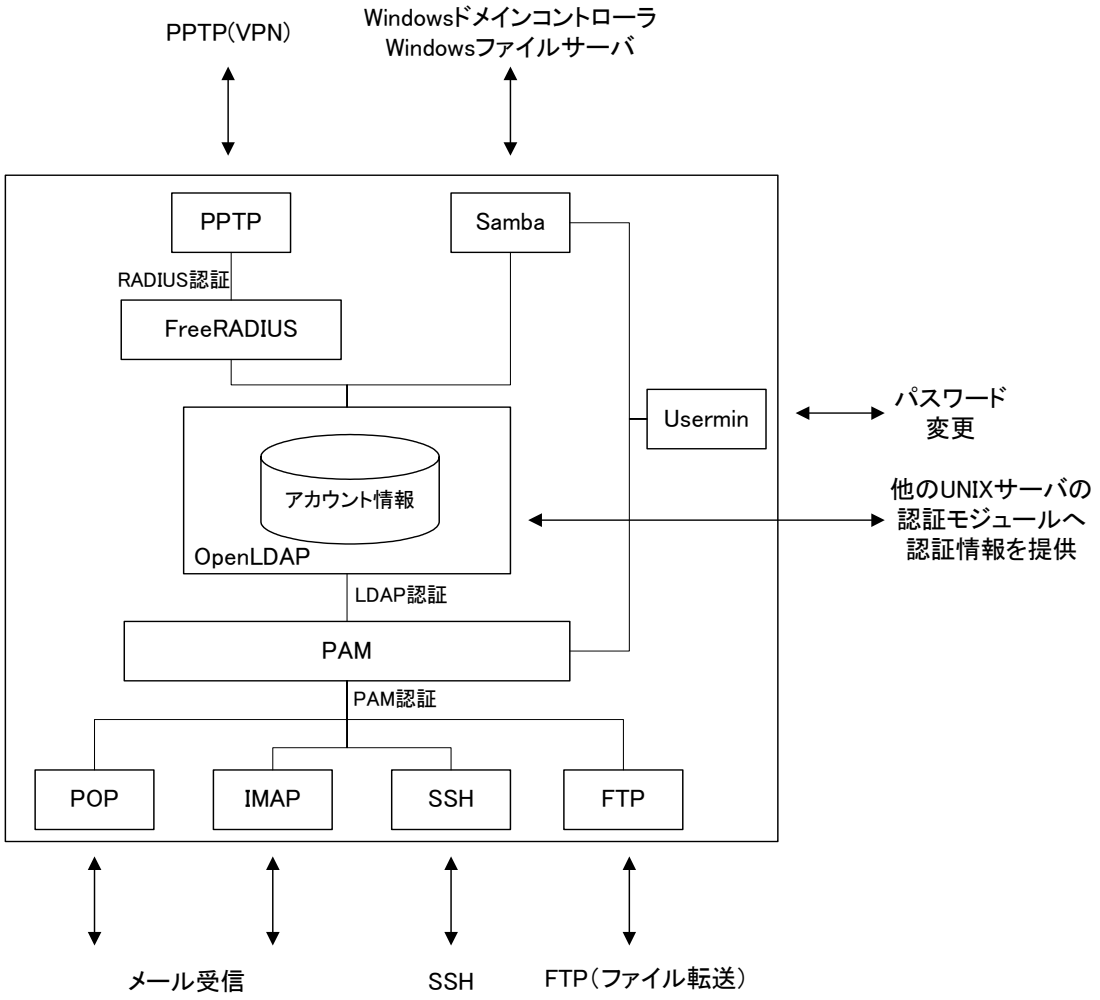


図３　認証サービスの構成

図３は，外部に提供するサービスがどのような経路で認証を行っているかを示したものである．外部にサービスを提供するデーモンによって暗号化形式や認証方式が異なるため，PAM (Pluggable Authentication Modules) や FreeRADIUS などのモジュールを経由して OpenLDAP へアクセスすることによってアカウント情報を OpenLDAP へ統合した状態で認証サービスを提供する.

アカウントの移行方法は，UNIX 系 OS と Windows ではパスワードの暗号化方式が異なるため，UNIX で使用する Windows パスワードを同時に生成し割り当てなおす案もあった．しかしユーザーに新パスワード変更の連絡が伝播するのに時間がかかるの予想されるため，パスワードはそのまま移行した後に Windows 連携のサービスを使う際に Usermin を利用してパスワードを変更していただく形とした．Usermin は認証時に UNIX パスワードを使用するため，移行したパスワードがそのまま使用できる．認証後のパスワード変更画面でパスワードを変更すれば，Windows 連携機能を使用

する際のパスワードも同時に変更されるため，Windows 連携機能を利用できるようになる．

今回のリプレースに伴い Windows サーバは廃止し，Samba による PDC 機能を提供する．認証は OpenLDAP のアカウント情報に連動する．

## ３．１　UNIX / Linux 認証サービスの統合

UNIX / Linux の認証サービスは OpenLDAP が提供する認証機能を使用して統合を行う．OpenLDAP でアカウント情報を管理し，各サーバへ PAM 経由の認証サービスの提供をする．認証を PAM で行うソフトウェアは多い．また，同一ネットワークに存在するほかの UNIX サーバにも LDAP で認証情報を取得するよう設定し，ユーザーアカウントを一元管理する．

### ３．１．１ メールサービスの認証

メールサービスは MTA に Postfix を，POP3/IMAP4 サービスの提供に Courier-IMAP を選定する．Courier-IMAP は POP3 と IMAP サービスの両方を提供するソフトウェアで，認証方法もプラグインにより選択可能である．Courier-IMAP は LDAP サーバに直接アクセス可能であるが，認証サービスのみ必要であったことと管理のしやすさから今回は PAM を経由して OpenLDAP で認証を行うこととする．

### ３．１．２　その他サービスの認証

PAM 対応ソフトウェアは PAM 経由で OpenLDAP による認証を行うよう設定を変更する．これにより認証サービスは OpenLDAP に統合される．

## ３．２　Windows 認証サービスの統合

Windows クライアントの管理はドメインを構築して行うが，Windows サーバを構築せずにオープンソースソフトウェアの Samba を使用してドメインコントローラを構築する．OpenLDAP のデータストアをバックエンドデータベースとして扱うことによって UNIX 系の認証サービスと共通のアカウントとして使用できるようにする．PPTP サービスは FreeRADIUS を使用し，RADIUS サーバで認証を行う．

### ３．２．１　Windows ドメイン認証

Windows クライアント管理には Windows ドメインを構築して行う．Windows ドメイン認証サービスの提供は Samba を使用し，OpenLDAP に登録されているアカウント情報を基に認証を行う．同時にファイルサーバ機能を提供し，ユーザーのホームディレクトリが Windows クライアントからアクセスできるよう設定を行う．

### ３．２．２　PPTP サービス認証

PPTP（Point-to-Point Tunneling Protocol）は Microsoft により提案されたプロトコルのため，UNIX 系 OS では標準サポートされていない．したがって Linux で PPTP サービスを提供するためにオープンソースの PPTP サーバソフトウェアである PoPToP を選定した．PPTP は認証方式と暗号強度が選択できる仕組みとなっているが，

現時点で使用できる最大の強度（MS-CHAP V2 128bit）のみで接続できることとした．Windows のパスワード暗号化形式は UNIX で使用されているそれとは異なるため，PPTP の認証はそのままでは使用できない．今回は Samba と連携することから，Samba が生成・管理する LDAP エントリの NT-Password，LM-Password 属性を使用して FreeRADIUS で MS-CHAP 認証サービスを提供し，FreeRADIUS で PPTP サービスの認証を行うことによって認証サービスを統合する．

### ３．３　アカウントの管理

統合されたアカウント情報の管理には UNIX パスワードと Windows パスワードの両方を生成しなければならないことから， Windows ドメインにログオンする際に必要な情報を自動生成するアカウント管理スクリプト集である smbldap-tools を管理者が使用してアカウント情報を生成できるように設定し，一般ユーザーは Usermin を利用してパスワードの変更を行う運用とした．Usermin でパスワードを変更すると UNIX パスワードと Windows パスワードの両方を同時に変更する．アカウント移行時は UNIX パスワードのみ移行を行い，Windows パスワードは Usermin で再設定を行っていただくこととして移行処理を行った．

## ４．認証サービス統合後の評価

今回の作業については導入に２ヶ月を要した．複数のシステムが OpenLDAP にアクセスして認証をするため，OS の種類やバージョンによる暗号化形式の違いを考慮した上での認証情報の移行手段の設計に伴うエンドユーザー様との調整に時間を要した．導入時にはハードウェアにトラブルが発生したが，認証システムはトラブルもなく稼動中である．PoPToP に一部の OS での PPTP 接続に不具合が発生していたが，コミュニティから対処方法を取得できたために回避することが可能であった．オープンソースソフトウェアを利用することによって Windows のサーバを廃止できたため，Windows サーバを使用せずに Windows に強く依存している PPTP やドメイン認証サービスを提供できた点も Windows のサーバを使用する場合のクライアントアクセスライセンスを考慮する必要がなくなったことからコスト的にメリットがある．

今回の事例は，ユーザー数が 300 程度と，規模がそれほど大きくないこともあり安定性に関しては問題が発生しなかったが，オープンソースソフトウェアは大規模システムの実績が商用ソフトウェアと比較すると少ないため，アクセス頻度がかなり高い場合は十分な検証期間を設ける必要があると考えられる．

## ５．今後の課題

認証の統合は達成でき，利便性が大きく向上したが，昨今はセキュリティが重要視されており，ネットワークのセキュリティが注目されている．認証 VLAN などのセキュリティ技術を搭載した製品が多数市場に投入されているが，認証サーバは商用の製品のみのサポートとしていることが多い．オープンソースソフトウェアではなく，アプライアンスなどの専用ハードウェアとの連携に弱い点，また，オープンソースソフトウェアを使用する場合は多数のソフトウェアを連動させる場合が多く，管理

の難度が高い傾向にあり，UNIX / Linux に明るい方でないと管理が難しくなる傾向にある．管理者に高いスキルが必要であるため，システムとしてのサポートの充実が今後の課題である．

## ６．おわりに

オープンソースソフトウェアはここ最近優れた成果を生んでいる．今回使用したネットワークサービスのソフトウェアだけではなく，オフィススイートの OpenOffice，開発環境では Eclipse や SharpDevelop など，規模の大きいソフトウェアもコミュニティが活発に開発を進めている．オープンソースソフトウェアは商用の製品に負けない機能を提供するものも存在するため，上手に使用すれば十分満足のいくシステムを構築できると感じた．ライセンスがフリーであればライセンス費用を削減することも可能である．オープンソースソフトウェアの今後に期待するとともに，成果は何らかの形でフィードバックを行い，さらなる発展を望みたい．

## 付録

構築に使用したオープンソースソフトウェアのバージョンを表１にまとめる．

表１　構築に使用したオープンソースソフトウェアのバージョン

| ソフトウェア名称 | バージョン | 概要 |
|---|---|---|
| Courier-IMAP | 2.2.1 | メールサービス |
| FreeRADIUS | 0.9.0-2 | Radius 認証サービス |
| OpenLDAP | 2.1.25 | ディレトクリサービス |
| PoPToP | 1.2.1 | PPTP サービス |
| pppd | 2.4.3 | PPP サービス（PoPToP と連携） |
| samba | 2.2.8a<br>Japanese-Release 1.1 | Windows ファイルサーバ<br>ドメインコントローラ |

## 参考文献


［１］稲地　稔：“OpenLDAP入門”，技術評論社，(2004.10),P17-28

［２］“LDAPによるパスワードの一元管理”，
http://www.atmarkit.co.jp/flinux/rensai/root02/root02a.html

［３］“Poptop – Open Source PPTP Server”，
http://www.poptop.org/