個人情報保護法に準拠した大規模ファイル共有システムの開発

Development of a large scale file-server-system strictly in conformity with the Japanese privacy law

遠藤　孝信*
Takashi Endo

2005年４月に個人情報保護法が全面施行される事に伴い、個人情報が含まれる文書（本件では、コンピュータ上のファイルを指す。）の管理を厳密に行う必要がでてきた。特に大規模な研究機関では独立行政法人化による組織再編により、個人情報を含んだ文書の保管場所が分散しているケースが多く見られた。これらの文書へのアクセス状況は必要に応じて監査可能な状態にする必要があり、情報保護のために一元管理可能なファイル共有システムを構築した。

Private Information Protection Law came into full effect in April 2005 and it has brought about the needs of managing and controlling documents（indicating data files on computer）which contain personal information.

Especially, many major research institutes have been storing their documents in separated locations after the organizational restructuring caused by the establishment of an independent administrative institution.

In addition, the access for these documents requires an audit practice as needed.

We built the large scale and consolidated controllable file-server-system for the private information protection.

1. まえがき

2005年４月に個人情報保護法が全面施行された事により、独立行政法人 産業技術総合研究所（以後 産総研という）にて文書関連の情報保護を目的としたファイル共有サーバの構築が急務となり、MSSにて受注、構築を行った。

個人情報保護法は個人情報(個人の識別が可能な情報)の保護を行うにあたり、個人情報の利用方法や義務、責任の範囲といったルールを法令化しており、産総研では2003年７月に情報セキュリティポリシーを作成し重要情報の取扱いについて詳細なルールを作成している。

ファイル共有サーバでは個人情報等の重要な情報が含まれる文書を扱うため、当然個人情報保護法および情報セキュリティポリシーに準拠する必要があった。

情報セキュリティポリシーでは文書へのアクセス方法、保管方法、監査について詳細に定義されており、アクセス方法についても役職や与えられた管理権限毎に詳細に分ける必要があった。

情報セキュリティポリシーで定義されている監査については、ファイルやフォルダへのアクセス履歴や管理者としての操作履歴等を監査対象とし、監査ログとして保存しなければならないが、それら監査ログは情報量が膨大であり、閲覧を容易にするため検索機能を用意する必要があった。

Sambaを用いてドメイン構築を行う場合、ユーザ管理にLDAP（Light weight Directory Access Protocol）を用いるのが主流となっている。

産総研ではLDAP上で管理する情報が既にOracleを用いたデータベースサーバにて管理されており、このデータベースの情報とLDAPにて同期処理を行う機能を構築した。

ユーザの利便性の面ではSamba上で管理されているファイルやフォルダのアクセス権をドメイン参加せずに変更できる機能を構築した。

本稿ではこれらの検討内容や実現方法について各章にて説明する。

2. 共有フォルダとユーザ

ファイル共有システムが提供するサービスとしてCIFS（Common Internet File System）サービスがメインとなっている。このCIFSサービスはWindows、Linux、Macintoshから利用することが可能である。

ユーザは各部門に割り当てられたSambaサーバに接

17　＊つくば事業部 第五技術部

続すると部門毎に割り当てられた共有フォルダの一覧を取得することができ、この一覧の中から自部門（場合によっては他部門）の共有フォルダを選択し、任意のファイル操作を行うことができる。

ただしファイル共有システムの要件として共有フォルダの階層構造やユーザの権限については詳細に定義されており、複雑な構成になっていた。それらについて以下に説明する。

2.1　共有フォルダ階層構造

ユーザから見える共有フォルダには以下の通りとなっている。各フォルダは特定のクライアントからしか読み書きができなかったり、特定のユーザのみ読み書き可能であったりと、いくつかの認可方法を用いて構成している。

基本的には部門長に任命されたアクセス権管理者はすべてのフォルダの操作が可能であり、それ以外のユーザはアクセス管理者によるアクセス権設定およびIPアドレス登録により最大3種類のフォルダが利用可能である。

●基本フォルダ

共有フォルダ直下にアクセス権管理者により作成されたフォルダ群であり、一般ユーザがファイルの読み書きを行う。

●部門長フォルダ

部門長専用のフォルダであり、アクセス権管理者であっても参照ができない。

●重要情報用フォルダ

個人情報等が含まれるような重要ファイル保管を目的としたフォルダ。

このフォルダにアクセスするためには、アクセス権管理者が、各ユーザのフォルダへのアクセス権および接続するIPアドレスを予め登録する必要がある。

Sambaでは一つの共有フォルダに対し異なる設定を行う事ができないため、MS−DFSルート形式を用いた階層構造により今回の構成を実現した。（図１）

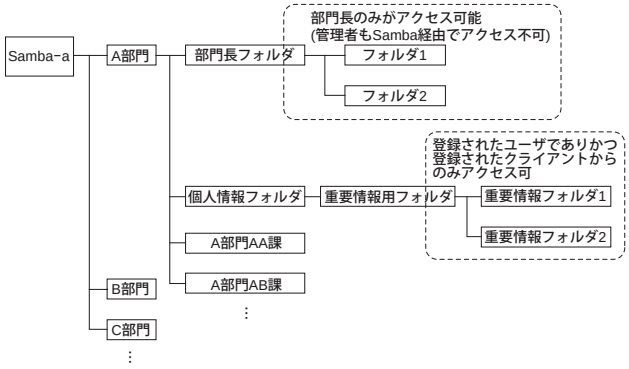

図１　共有フォルダ内階層

2.2　ユーザ

ファイル共有システムのユーザはアクセス権管理者も含め以下の４種類に分類される。

●一般ユーザ

●アクセス権管理者

●部門長

●アクセス記録分析担当者

2.2.1　一般ユーザ

一般ユーザはファイル共有システムを利用可能なすべてのユーザを指す。

最初にイントラシステムのログインID申請画面よりログインIDを作成することにより一般ユーザとしてCIFSサービスを利用できるようになる。

2.2.2　アクセス権管理者

アクセス権管理者とは各部門に割り当てられた共有フォルダを管理者するユーザを指し、部門長および部門長に任命されたユーザがアクセス権管理者として部門共有フォルダを管理する。

アクセス権管理者はファイル共有システムにドメイン参加するか、ブラウザを用いる事により一般ユーザが利用可能なディレクトリを作成することができる。

また作成したディレクトリに任意のアクセス権を設定することが可能であり、部門共有フォルダ内のファイルに対する不必要なアクセスを遮断することが可能である。

2.2.3　部門長

部門長はアクセス権管理者として自動的に登録されており、アクセス権管理者を適宜任命する権限を持っている。

また部門共有フォルダには部門長用のフォルダが用意されている。（このフォルダに限ってはアクセス権管理者であっても部門長以外アクセスできない。）

2.2.4　アクセス記録分析担当者

アクセス記録分析担当者とは各部門に割り当てられた共有フォルダ内ディレクトリ及びファイルへのアクセス記録を検索・参照を行うことができるユーザを指す。

アクセス記録分析担当者は必要に応じてアクセスログを検索し、「重要なファイルに対するアクセス状況」を確認することができる。

当初アクセス記録分析担当者はアクセス権管理者が兼務する構想で設計を進めていたが、アクセス権管理者がファイル共有システムにおいて重要な権限を持つ事になり、ログ監査の意味が薄れてしまうため、あえて役割分

担を行うように仕様を変更した。

アクセス記録分析担当者が参照可能なログは、アクセスログ以外にアクセス権管理者が行った作業履歴も対象とする事により監査役としての機能を持たせる事にした。

3. システム構成

ファイル共有システムは認証サービスを行うLDAPサーバ、ファイル共有サービスを行うSambaサーバ、情報管理を行うデータベースサーバ、およびログ検索サービスを行う検索サーバで構成されている。

またウィルス対策としてFSAV for Sambaを導入しウィルス蔓延の温床とならないよう配慮した構成となっている。

認証サービスとしてのOpenLDAPはインフラサーバで用いている（職員番号に対応した）ログインID、パスワードをそのまま用いる必要があったため、OpenLDAPとOracle間でユーザ情報及びグループ情報の同期処理を定期的に行っている。

システム構成の概要については以下の表１及び図２に示す。

3.1 データベースサーバ

データベースサーバは既に稼働しているOracleサーバを利用している。このサーバにはインフラサービスのマスタとなる職員情報データベースをはじめ、いくつもの業務システムが稼動しているため、ファイル共有システム用データベースを構築する際には他システムへ影響を与えないよう可能な限りチューニングを行う必要があった。

3.2 LDAPサーバ

LDAPサーバでは認証サービスとしてOpenLDAP、ドメインコントローラとしてSamba、またLDAP情報更新及びその他ユーザ支援用CGIとしてApacheをインストールし稼動させている。

表１　システム概要

サーバ種類	提供サービス	備考
データベースサーバ	データベースサービス	Oracleを利用 職員情報データベース ファイル共有システム用データベース
LDAPサーバ	ディレクトリサービス ドメインコントローラ HTTPサービス	クラスタ化によるHA構成。 Samba＋OpenLDAPによるドメイン構築
Sambaサーバ	ディレクトリサービス ファイル共有サービス	LDAPスレーブサービス
検索サーバ	ログ検索サービス	Apache＋MySQLによる ブラウザベースの検索

LDAPサーバは２台構成となっており、以下のようなサービスの役割分担を行っている。（表２）

この２台はファイル共有システムの重要な機能を担っている事から、可用性を考慮しCLUSTERPROを用いたHAクラスタとした。

3.3 Sambaサーバ

Sambaサーバはファイル共有システムにおいてCIFSサービスの提供を行うサーバである。今回用意したSambaサーバは４台であり各々異なる部門の共有フォルダをユーザに提供している。

各SambaサーバはSANディスクをマウントしており、そのSANディスク上にSamba設定情報及び共有フォルダの物理ファイルを保存している。

これらのファイルをSANディスクに保存することにより、１台のSambaサーバに障害が発生した場合でも、別のSambaサーバでそのSANディスク領域をマウントすることにより迅速な障害対応を行うことが可能となっている。（図３）

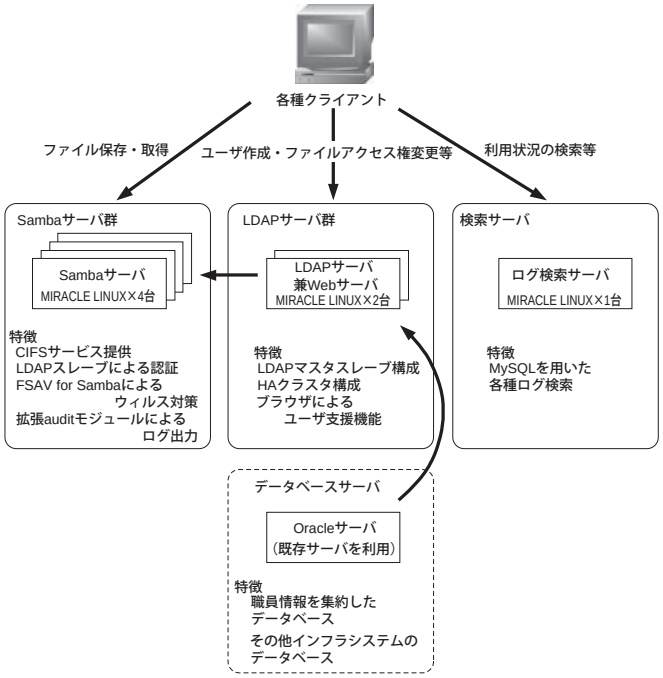

図２　システム概要

表２　LDAPサーバ上の役割分担

LDAP－A		
	OpenLDAP	LDAPマスタサーバ
	Samba	プライマリドメインコントローラ
LDAP－B		
	OpenLDAP	LDAPスレーブサーバ
	Samba	バックアップドメインコントローラ
	Apache	LDAP情報更新及びその他ユーザ支援用CGI

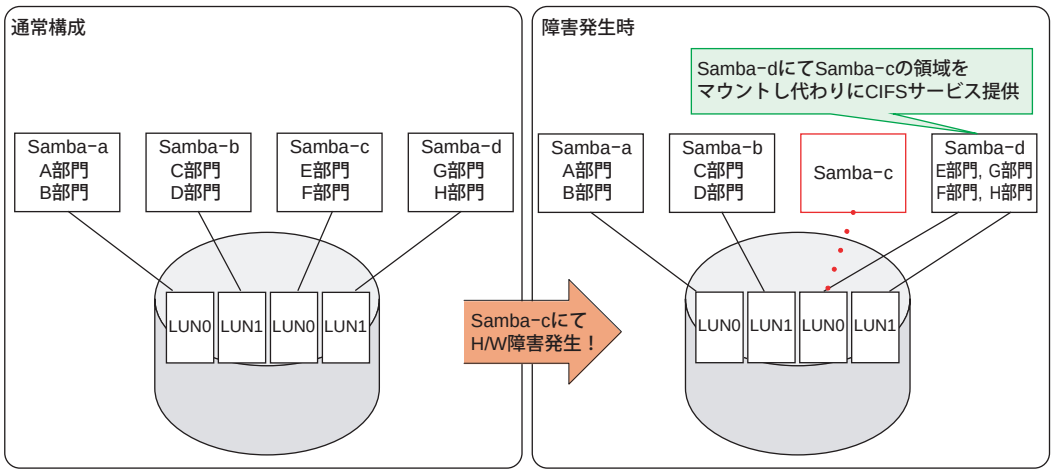

図３　Sambaサーバ障害対応

CIFSサービスではユーザ認証が必要となるが、本システムでは認証サービスとしてLDAPサーバに問い合わせを行った場合、LDAPサーバ過負荷及びネットワーク経由の問い合わせに対するオーバヘッドが懸念されたため、各SambaサーバはBerkleyDBを用いたLDAPスレーブサーバとして構築した。これによりネットワーク経由の問い合わせによるオーバヘッドがなくなり、かつBerkleyDBによる高速な認証が可能となった。

またCIFSサービスの提供を行う場合、ウィルス対策について十分な検討を行う必要があった。従来のウィルス対策製品の場合、ウィルスを含むファイルがディスク上に書き込まれたり、読み込まれた時に検知する。本システムで採用したF－Secure社のFSAV for SambaはSamabのvfsオブジェクトとして呼び出す事が可能であり、ユーザがウィルスファイルを読み書きしようとした時にSamba経由でAlertウィンドウを直接クライアントに表示する事が可能となっている。

3.4　ログ検索サーバ

ログ検索サーバでは様々なログ情報をWEBブラウザから検索閲覧が可能となるサービスを提供している。

ユーザ支援用CGIのログについてはOracle上に保存されているが、CIFSサービスのアクセスログについてはあまりにも膨大な量である事からデータベースサーバとは別にMySQLを稼動させたサーバを用意し、Perlを用いて検索を行っている。

4.　職員情報データベースとの連携

産総研インフラシステムで稼動する職員情報データベースには各インフラシステムにて用いているパスワード及び組織情報が含まれている。そのため、ファイル共有システムでもこの情報を利用しファイルのアクセス権やユーザ認証に用いている。（図４）

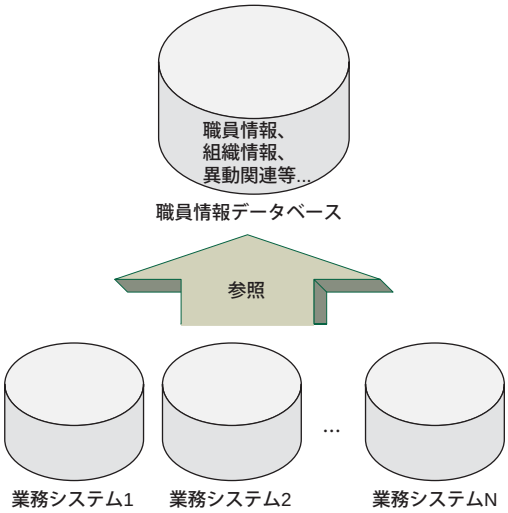

図４　職員情報データベース

ファイル共有システムではユーザ認証にOpenLDAPを用いたディレクトリサービスを用いている。そのため、OracleとLDAPとの同期を行う必要がある。

同期するためにはDBをLDAPとの同期が可能な製品を導入する必要があるが、市販品には高価な製品しかなかったため、本システムではオープンソースを組み合わせて独自に構築した。（図５）

同期プログラムの構築にあたり職員情報データベースに発生するイベントのうち、ファイル共有システムに関係するイベントをリストアップした。

ディレクトリサービスはOpenLDAPを用いて構築しており、その情報はsmbldap－toolsを用いて作成している。今回リストアップしたイベントとsmbldap－toolsの

コマンドの対応付けを行った。（表３）

表で示した通りユーザ再作成のイベントに対応するコマンド以外のイベントについてはsmbldap−toolsで対応できる事がわかる。

またユーザ再作成のイベントに対しては以下の処理を行うプログラムを別途作成し対応した。

⑴ ユーザ削除時に削除前のユーザ情報をLDIF形式で保存

⑵ ユーザ再作成時に保存したLDIFファイルをリストア

5. 複数種類のアクセスレベル

職員がインフラシステムを用いる場合、各職員に割り振られている職員番号を用いてログイン認証を行っている。

ファイル共有システムでは職員情報データベースの情報を基にユーザ名、パスワード、所属情報を保持しているため、当然ユーザ認証に用いる情報は職員番号とパスワードとの組み合わせになる。

しかし、以下の要件によりこのままでは要求を満たせないことがわかった。

●ユーザ名とパスワードの認証以外に複数のアクセスレベルを設ける

そのため以下のアクセスレベルの構築を提案し了承を得た。

●職員番号は用いず別途ログインIDを設ける→職員番号は職員の特定が可能な情報であるため利用しない

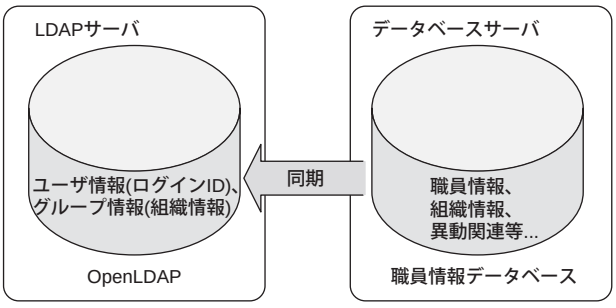

図５　LDAPサーバ同期

表３　各イベントとsmbldap−toolsの対応

分類	イベント種類	Smbldap−toolsコマンド
ユーザ情報	ユーザ新規作成	smbldap_useradd
	ユーザ再作成	なし
	ユーザ情報変更	smbldap_usermod
	ユーザ情報削除	smbldap_userdel
	パスワード変更	smbldap_passwd
グループ情報	グループ作成	smbldap_groupadd
	グループ情報変更	smbldap_groupmod
	グループ情報削除	smbldap_groupdel

●重要情報用フォルダはアクセス権管理者のみ参照可

●重要情報用フォルダは登録した端末（IPアドレス）からのみ参照可

●部門長フォルダはアクセス権管理者であっても参照できないようにする

5.1　ログインIDの採用

当初 既存インフラシステムと同様に職員番号とパスワードの認証方法を検討していたところ、「職員番号は職員の特定が可能な情報であるため、個人情報として取り扱う必要があるのではないか」という指摘を受けた。そのため、産総研担当者との協議の結果「職員番号を用いず、別途ログインIDを設置する」という事になった。

ログインIDについてはユーザが任意の文字列で申請可能なブラウザベースの”ログインID作成機能”を作成し職員IDで行っていたユーザ認証をログインIDでのユーザ認証へ置き換えた。（図６）

ログインIDと職員番号との対応は一意であるため、対応表を作成し基本的にファイル共有システムの運用を担当するシステム管理者以外は参照不可とした。

5.2　MS−DFSによるSambaサービス

共有フォルダ内にある重要情報用フォルダや部門長フォルダは特殊な認証方法をとっているため、これらのルールを適用するためにはSambaの設定を各々個別に用意する必要があった。

ただし共有フォルダ内でのSamba設定は変更不可であるため、MS−DFS機能を用いて、以下のようなディレクトリ構成をとることにより複数の設定を仮想的に一つの共有フォルダとして設定することを実現した。（図７）

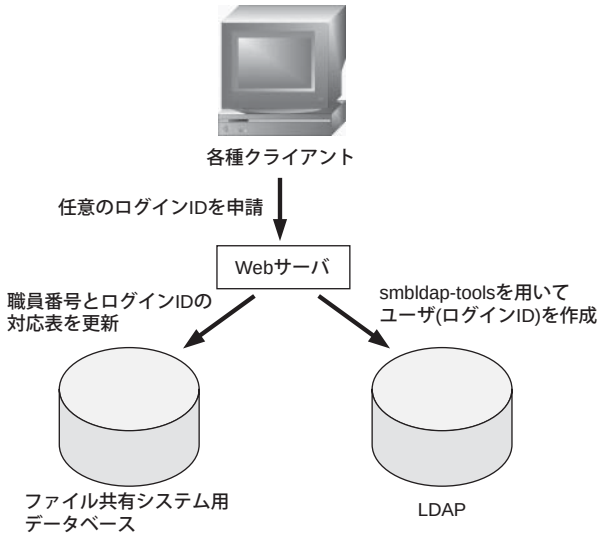

図６　ログインID申請

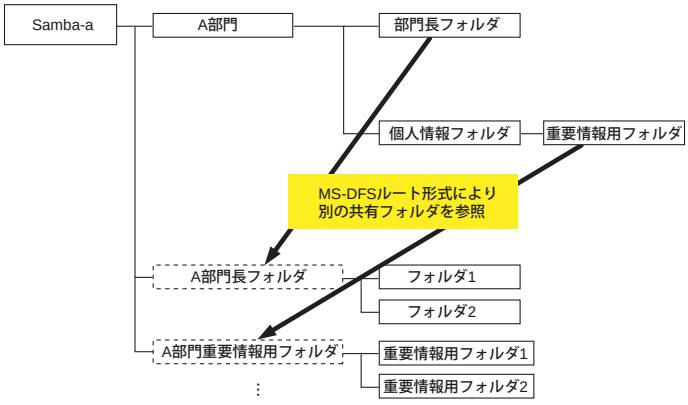

図7　MS-DFSルート形式によるフォルダ階層

またMS-DFSが参照する個別の共有フォルダはbrowseable=noとしSambaサーバ接続時に一覧に表示されないようにした。

6. ブラウザを用いたアクセス権管理

ファイルのアクセス権を変更する場合、ユーザ情報およびグループ情報が必要となり、必ずsambaドメインへの参加が必要となる。

Windowsのファイル共有では一般的に部門毎にドメインを作成し部門内でのファイル受け渡しを行うが、ドメインへの参加を行う場合、WindowsOSの再起動が必須であり、アクセス権変更を行う度に再起動を要することになる。

本システムではドメインにログインせずにファイルやディレクトリのアクセス権をブラウザから変更できる機能を実装した。これによりユーザの利便性が向上し、アクセス権管理者によって容易にアクセス権変更が行えるようになった。

7. 監査機能

Sambaではvfs objectとしてaudit機能を持っており監査機能として利用可能ではあるが、以下の情報をログファイルに出力する事が可能である。

●日時
●対象ファイル（ディレクトリ）
●実行イベント（connect，open，close，rename等）
●実行結果

ただしaudit機能ではユーザ名や接続元IPアドレスについては出力する事ができない。そのため、このaudit機能を拡張したabs_auditを作成し実装した。

またこのabs_auditモジュールでは従来対象ファイル（ディレクトリ）が相対パスで出力されるのに対し、絶対パスで出力されるような機能を持たせた。

これにより当初想定した監査情報を全てSambaのログとして保存する事が可能となった。

またこれら保存した監査ログを検索するためのログ検索機能を作成した。こちらについては後述する各種ログ検索機能の項にて説明する。

8. 各種ログ検索機能

ファイル共有システム上のファイル・フォルダにアクセスした情報は全て監査ログとしてファイル共有システム側に保存し、アクセス権管理者の操作記録もログ情報としてデータベースサーバ上のOracleDBに保存した。

これらのログというのは必要に応じて各部門の管理者によって参照可能な状態にする必要があった。

ただし監査ログに関してはアクセス権管理者とは権限分離するため別途“アクセス記録分析担当者”を設置しこの担当者に指名された職員のみが参照可能とした。

検索機能が管理するログは大量（1日あたり100万～200万行）に出力され、既存のOracleにログデータを投入し検索を行った場合、データベースサーバへ負荷を与えることが懸念されるため、以下のようなMySQLを用いたログ検索サーバを用意する構成にて実現した。（図8）

MySQLを用いる事により導入コストを最小限にとどめ、かつ既存データベースサーバへの負荷を最小限にとどめる事ができた。またアクセスログを深夜にバッチジョブで転送し朝8：00前までにMySQLへのデータ投入を完了させる事も可能とした。

9. 今後の展望

現在利用しているファイル共有システムでは実現できていない機能がいくつかある。その一つがSambaサーバの可用性向上のためのHAクラスタ化である。LDAPサーバにはCLUSTERPROによりHAクラスタを実現しているが、Sambaサーバに関してはクラスタソフトの価格や将来的なSambaサーバの増設を考慮し、本システムではクラスタソフトを導入していない。

また部門毎にSambaサーバが割り当てられている事により、複数部門に所属するユーザは部門毎に接続サーバを切り替えて使用する事になり、利便性向上の余地がある。

これらの問題点はSambaが持つ既存機能および新機能により解決することが可能となる。

9.1　Samba4.0の新機能

現在ファイル共有システムで利用しているSambaは3.0ベースで構築されているが、既に4.0のリリースが予

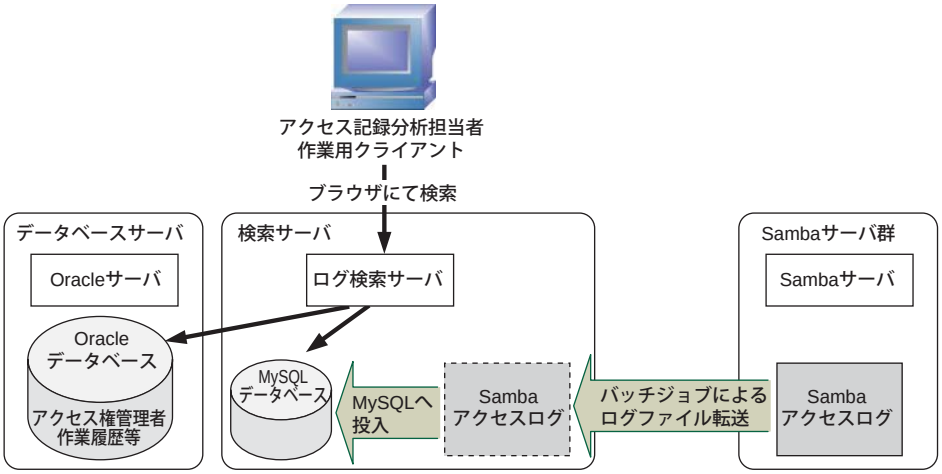

図8　ログ検索

定されており、4.0では以下の新機能が盛り込まれる予定となっている。

●ActiveDirectoryの実現
●GPFS（General Parallel File System）を用いたクラスタファイルシステム
●SWATの機能強化

このうちGPFSを用いたクラスタファイルシステムは今回のファイル共有システムにおけるLDAPサーバにて用いているクラスタソフトに近い機能を持っている。OSの入れ替えが必要になるが、この新機能をLDAPサーバで利用する事により無償でLDAPサーバのHAクラスタ機能を実現する事が可能になる。

またSambaサーバにおいてはSANディスクを用いているため、こちらについてもクラスタファイルシステムを利用する事により、今よりも可用性および利便性の向上が可能である。

9.2　MS-DFS専用サーバ

本システムの構築にあたり接続クライアント数が10,000という事がSambaサーバを複数用意し部門毎に接続するSambaサーバを分ける構成となっている。

そのため、特定のSambaサーバ内の部門用共有フォルダを過負荷等の理由により、別サーバへ移動させた場合、ユーザは接続先のSambaサーバを変更する必要がある。

各部門フォルダはMS-DFS（分散ファイルシステム）を用いて複数の共有フォルダを一つに見立てている。このMS-DFS専用サーバを構築し各々の共有フォルダへのポインタとし、各ユーザに提供することにより、利便性の向上も期待できる。

10. むすび

今回のシステムを構築するにあたり、産総研ご担当者様、社内プロジェクトメンバが共にプロジェクトの重要性を共有し一体となれた事がプロジェクト完遂の大きな要因と考えている。

私自身にとっても本システム構築により様々な経験ができた事は、今後他の業務に携わる上での重要なバックボーンに成りえる貴重な体験だった。

特にLDAPに関するシステムは今後成長が期待できる分野であるため、OpenLDAPや有償製品であるSun Java Directory Server、Windows Active Direstoryといった製品群に関しても情報収集を行い、ユーザに適した提案が行えるよう自己啓発に努めていきたい。

参考資料

(1) 日経BP ITPro「産総研とヤナセがWindowsからLinux＋Sambaに乗り換えた理由」
http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20050713/164606/
(2) 技術評論社「徹底解説 Samba LDAP サーバ構築」
(3) 日経BP社「セキュアなSambaサーバの作り方」
(4) 技術評論社「Software Design 2006年7月号」「壱：地の巻」Sambaファイルサーバ