システムソフトウェアと
オペレーティング・システム 85－9
（２０００．８．４）

LDAPを利用した認証システムの構築

枡上昭広、上原稔、森秀樹
sabo_ami@mo.cs.toyo.ac.jp,{uehara,mori}@cs.toyo.ac.jp
東洋大学工学部情報工学科

本論文は、異なるオペレーティングシステムを使用した複数のネットワーク環境で、各ネットワークのログオン時のユーザパスワードを同期化させ、ユーザの利便性を図ったパスワード認証サーバを用いた認証システムを提案するものである。

現在のパスワードによる認証システムはオペレーティングシステム毎に異なっており、複数のシステムが混在する環境では個人は複数のアカウント管理を強いられている。

そこで本研究では、ディレクトリアクセスプロトコルであるLDAPを用いて、アカウント情報を格納したディレクトリデータベースと通信を行ない、適用するネットワークの認証システムを関連づける。それによって認証システム自体に大きな変更を行なうことなく、問題点を解決したいと考える。

Authentication System Using LDAP

MASUGAMI Akihiro, UEHARA Minoru, MORI Hideki
Department of Information and Computer Sciences, Toyo University

In this paper, we would like to suggest a password authentication system using LDAP, which makes users passwords that they use on their each network systems in logging on synchronized, for the purpose of their convenience, when more than one operating systems are mixed in.

The present authentication systems of password differ from each ones; therefore, users must supervise several accounts of their own under such environment.

In our study, we aim to let the present systems of each ones be related by using one of directory access protocols, LDAP, and by communicating with the directory database. As a result, we hope it leads to the solution of the problem without changing the present system itself.

1. はじめに

現在、一般に用いられているオペレーティングシステムが備えているセキュリティ機能がパスワードによるユーザ認証システムである。しかし、これらの認証システムはオペレーティングシステムによりその方式は異なっているため、ネットワーク上である個人のアカウントが複数存在し、管理が煩雑となっている。

そこで本研究では、UnixやWindowsNTなど異なるオペレーティングシステムが存在する複数ネットワークにおいて、同一パスワードを用いたアカウントによるアクセスを可能にするユーザ認証システムを提案する。

このような機能を実現する既存のアプリケーションはいくつか存在するが、いずれも機能やコストなどの問題点を抱えている。本研究では、ネットワーク情報をサーバ上に保存し、運用するネットワークの認証システムを関連付け、それによって認証システム自体に大きな変

更を行なうことなく、問題点を解決したいと考える。

各ユーザのアカウント情報は Windows NT Server、UNIX(NIS) Server 内に保存され，ユーザパスワード同期に関するネットワーク情報は認証サーバ内のディレクトリデータベースに保存される。この情報は各ネットワークから LDAP(Lightweight Directory Access Protocol)[1]を利用してアクセスされ、情報の同期が図られる。これにより、同期されたデータベースに基づいた認証システムを利用する環境では、どこからでも同一のパスワードによる認証が可能になる。

本論文の構成は以下の通りである。第２章では、既存の方式との比較検討を行っている。次に第３章でわたしたちが提案するシステムの概要について説明する。最後に、第４章で今後の課題について検討する。

2. 関連研究

パスワード情報の同期を実現する既存のアプリケーションとして WindowsNT Services For Unix[2]や Novell Directory Services[3]や RedCrypt[4]などがある。パスワード情報の同期を行うことができる既存の方式として、Windows NT Services for UNIX、NDS(Novell Directory Service)、RedCrypt などがある。以下では、これらの既存の方式の問題点と、本研究における解決方法について述べる。

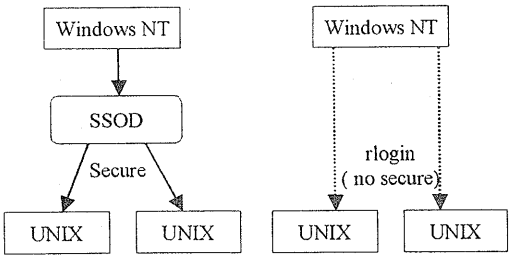

図 1:Windows NT Services for UNIX1.0a

2.1 Windows NT Services For UNIX1.0a

Windows NT Services for UNIX は、Microsoft が提供する Windows NT のアドオンパックで、Windows NT と UNIX のサービスの相互運用を可能にする。機能の１つである Windows NT と UNIX のパスワード同期には、パスワード同期プログラムである SSOD を用いる方法と、rlogin を用いる方法の２つがある Windows NT Services for UNIX を用いてパスワード同期を行なう上での問題点として、以下のような点があげられる。また、次バージョンでは、双方向によるパスワード同期と Active Directory への移行をサポートする。

- Windows NT 上でのパスワード変更が UNIX 側に伝えられるだけで、認証をリダイレクトしているわけではないので、UNIX 上でパスワードを変更しても Windows NT 側には反映されない。

- パスワード同期プログラム SSOD は、対応する OS が Solaris、DIGITAL UNIX、HP-UX に限られてしまう。

- rlogin を用いた方法では、通信路にパスワードが平文で流れてしまう。

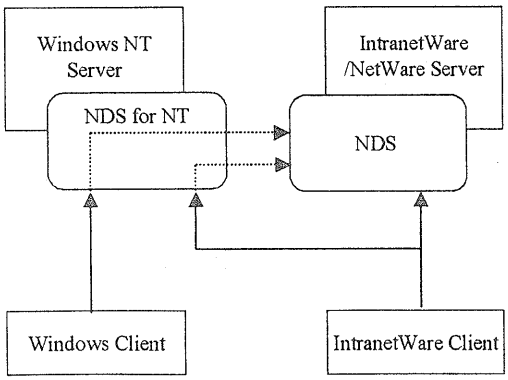

図 2 :Novell Directory Services

2.2 NDS(Novell Directory Services)

NDS(Novell Directory Services は、Novell の NetWare 4.x で導入されたオブジェクト指向のディレクトリサービスである。ネットワーク全体におけるネーミング体系とデータベースを提供する。これにより、組織内のアカウント情報やサービスなどの管理が統一的に行なえる。また、IEEE によって作成された X.500 勧告に準拠している。 IntranetWare、Solaris、Windows NT などに対応しており、例えば、IntranetWare と Windows NT の混在した環境での認証は図 2 のようにあらわすことができる。NDS for Windows NT を利用することで、Windows と IntranetWare クライアントのどちらからでも IntranetWare サーバの NDS にアクセスし、認証を行なうことができる。これによってシングルログオンが実現されている。

問題点として、現段階では扱えるネットワークが IntranetWare(NetWare)、Windows NT、Solaris に限られてしまい、IntranetWare ネットワークを導入していないとアカウント情報の統合ができないため、オープンな環境での利用をしにくいと考えられる。

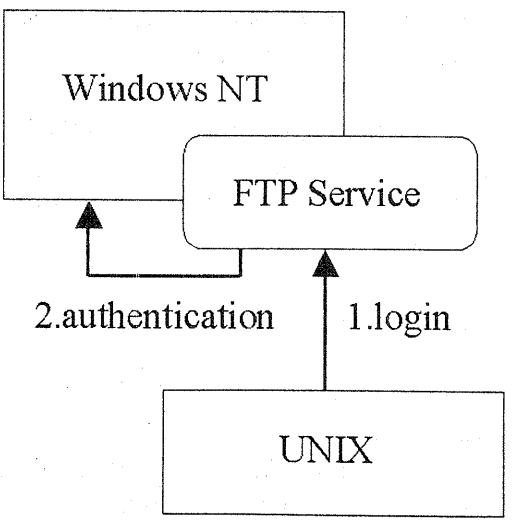

図 3 :RedCrypt

2.3 RedCrypt

RedCrypt は、FTP サービスを利用して UNIX と Windows NT の間でパスワードの同期を行なうことができる仕組みである。クライアントのライブラリを変更して、passwd コマンド実行時に Windows NT で稼働している FTP サービスにログインして認証を行なう。

RedCrypt を用いてパスワード同期を行なう上での問題点として、以下のような点があげられる。

- 通信路にパスワードが平文で流れてしまうなど、セキュリティが FTP に依存したものになってしまう。
- 利用するすべてのクライアントに導入する必要があり、管理コストが大きい。
- パスワード情報を Windows NT が持つことになり、UNIX 側から変更ができない。

2.4 まとめ

今あげた問題点を解決するために提案した我々の認証システム[5]では、パスワード変更のために専用のコマンドを各クライアントへ実装、セキュリティへの配慮等をしなくてはならなかった。

そこで本研究では、既存のアカウントの認証機構を利用し、システムに大幅な変更をせず、Web ブラウザを使うことによってマルチプラットホームと SSL(Secure Sockets Layer)[6]を用いて高いセキュリティを実現するパスワードによる認証システムを構築する。

本認証システムでは、各ユーザのアカウント情報を Unix(NIS)サーバ、WindowsNT サーバ内に保存され、パスワード同期に関する情報は各ネットワークから LDAP(Lightweight Directory Access Protocol)を利用してアクセスされ、情報の同期が図られる。

これにより、同期されるデータベースに基づいた認証システムを利用する環境では、どこからでも同一のパスワードによる認証が可能になる。

3. 概要

本研究で提案するシステムは、図4で表されるコンポーネントから構成される。

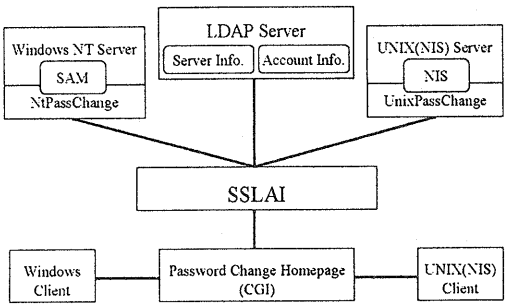

図4:LDAPを利用した認証システム構成図

- LDAP Server
  LDAPServerはWindows NT、UNIX(NIS)サーバについての情報が組織を反映し階層化され格納されている。

- SSLAI
  SSLAI(SSL LDAP Access Interface)は、Web の専用パスワード変更ページを通じて各クライアントからパスワード変更要求をWindowsNTサーバ、UNIX(NIS)サーバにそれぞれ伝え、その結果クライアントに返答する。これらの送受信の経路はSSLによってセキュリティが保たれる。また、実際にWindows NT,UNIX Serverのパスワード変更はNtPassChangeサービス,UnixPassChangeデーモンを呼び出すことにより行なわれる。

- NtPassChange
  NtPassChangeはWindowsNT Server上に実装されたSSLAI専用のパスワード変更サービスである。SSLAIからの要求に従いWindowsNT Serverに保存されているユーザパスワードを変更し、結果をSSLAIへ伝える。

- UnixPassChange
  UnixPassChangeはUNIX(NIS) Server上に実装されたSSALI専用のパスワード変更デーモンである。SSLAIからの要求に従いUNIX Serverに保存されているユーザパスワードを変更し、結果をSSLAIへ伝える。

- CGI(パスワード変更用)
  パスワード変更用ページに実装されたCGIである。ユーザからのパスワード変更要求とユーザ情報をSSLAIへ伝える。

- WindowsNT Server,Client
  既存のWindowNT Server,Clinetと同様である。SSLAIからの要求を受け付けるためにWindowsNT ServerにはNtPassChangeサービスが実装される。

- UNIX(NIS) Server,Client
  既存のUNIX(NIS) Server,Clientと同様である。SSLAIからの要求を受け付けるためにUNIX(NIS) ServerにはUNIXPass Changeデーモンが実装される。

セキュリティに関わるすべての通信経路はSSLによって暗号化される。そのため、各クライアント、サーバはSSLをサポートする必要がある。

3.1 データベース構成

LDAPサーバ内に構築されるデータベースは図5のようなディレクトリ構造となっている。基本的な構造、属性などはRFC2307[7]に準拠し、さらに必要な拡張情報を属性、値としてもつ。

基本的に下位の階層へいくに従って狭い範囲のネットワーク(ou)を配置する。エントリには、そのネットワークに関する情報（サーバ名等）が保存され、この中にアクセス制限との属性も含まれる。

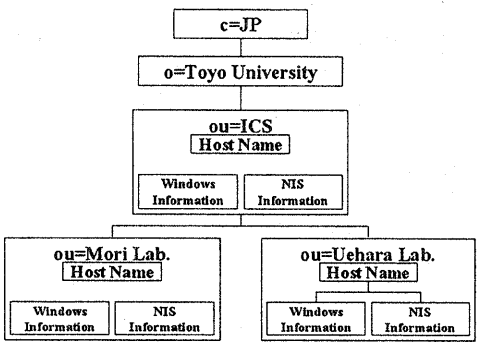

図5:データベース構成

3.2 パスワードの認証

本認証システムは既存の認証機構を使用するので、既存のネットワークとその方式に違いはない。

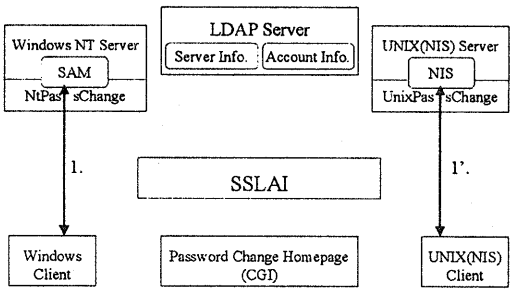

図6:パスワード認証

Windows 環境での認証

Windows クライアントは今までのネットワークと同じように WindowsNT サーバへ認証要求を行い、WindowsNT サーバより認証される。(図6矢印1)

UNIX 環境での認証

また、Unix クライアントも同様に NIS サーバへ認証要求を行い、NIS サーバより認証される。(図6矢印1')

3.3 パスワードの変更

パスワードの変更は Unix 環境、Windows 環境ともに同様の手順で行われる。

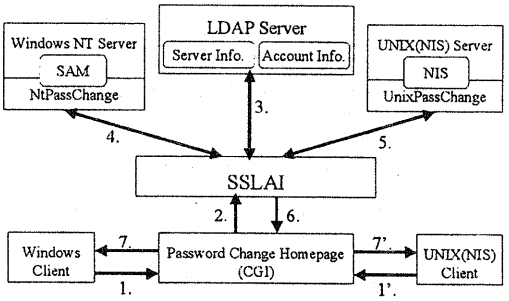

図7:パスワード変更

各クライアントは Web 上のパスワード変更要求ページに接続し、パスワード変更に必要な情報を入力する。(矢印 1,1') そして、このページの CGI が SSLAI へパスワード変更要求を出す。(矢印 2)

SSLAI はその情報をもとに LDAP サーバへアクセスし、そのネットワークに含まれる。WindowsNT、NIS サーバのアドレスに関する情報を得る。(矢印 3)

得られたサーバ情報をもとに、各サーバの NtPassChange, UnixPassChange サービスを用いてパスワードの変更を行う。(矢印 4,5)

このとき、NT サーバのアカウント情報データベース(SAM)、NIS サーバの NIS 情報ファイルが同一パスワードで変更される。

その結果は SSLAI から伝えられ(矢印 6)最後に、クライアントへ伝えられる。(矢印 7,7')

このように、Windows と Unix のどちらのクライアントからの変更であっても、常に WindowsNT のアカウントデータベースである SAM と、Unix の NIS 情報ファイルのユーザパスワードが両方が変更されることとなり、

Unix からでも Windows からでも、同一のパスワードでの認証が可能となる。

4. 今後の課題

今後の課題として、以下のような事項が挙げられる。

- 本システムでは、2つのサーバ(Windows NT Server 1台と SunOS 1台)のパスワード変更に約 20 秒を要してしまうので、同期させるサーバ数が増加に対し、処理の高速化が必要である。
- サーバやネットワーク上の障害による、ユーザパスワード同期の不整合を回避するためのトランザクション機構、パスワード管理用ツールが必要である。
- アカウント情報を拡張し、Windows2000 で提供されている ActiveDirectory[8]に結合していきたい。

5. おわりに

本論文ではネットワーク情報を LDAP サーバ上に配置し、異なる認証システム間でアカウント情報データベースの同期を行なうことによって、同一のパスワードを用いて認証できるシステムを提案した。

参考文献

[1] W.Yeong,T.Howes,and S.Kille, "Lightweight Directory Access Protocol," RFC 1777,March 1995

[2] Microsoft "WindowsNT Services for UNIX" http://www.microsoft.com/japan/products/ntserver/sfu/

[3] Novell "Novell Directory Services" http://www.novell.co.jp/nds/index.html

[4] Tatsumi Hosokawa "RedCrypt-Redirecting crypt(3)" http://wing-yee.ntc.keio.ac.jp/hosokawa/redcrypt/

[5] 「LDAP を用いたパスワード認証システムの構築」 本郷鉄兵、枡上昭広、上原 稔、森 秀樹 マルチメディア、分散、協調とモーバイルシンポジウム(1999.6.7)

「LDAP を用いたパスワード同期システムの構築」 枡上昭広、上原 稔、森 秀樹 第 59 回 情報処理学会全国大会(1999.9)

[6] Netscape Communications "SSL 3.0 Specification" http://home.netscape.com/eng/ssl3/ssl-toc.html

[7] L. Howard, ``An Approach for Using LDAP as a Network Information Service,'' RFC 2307, March 1998.

[8] Microsoft Corporation http://www.asia.microsoft.com/japan/support/kb/articles/j046/6/96.htm