

LDAP を用いたパスワード同期システムの構築

5 T-8

栢上 昭広, 本郷 鉄兵, 上原 稔, 森 秀樹

{sabo_ami,sor_yumi}@mo.cs.toyo.ac.jp, {uehara, mori}@cs.toyo.ac.jp

東洋大学工学部情報工学科

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のセキュリティ機能の一つ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、個人の特定が難しくなっている。そこで本研究は、異なる複数のオペレーティングシステムが混在するネットワークにおいて、同一の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認証システムを提案する。

パスワード同期に関するアカウント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。

2 概要

本研究で提案するシステムは、図1で表されるコンポーネントから構成される。

• LDAP Server

サーバ、アカウントに関する情報が組織を反映し階層化され格納されている。

• SSLAI

SSLA(SSL LDAP Access Interface)は、パスワード変更要求を、各サーバにそれぞれ伝え、その結果をクライアントに返答する。要求・応答の経路はSSL(Secure Sockets Layer)[2]によって暗号化する。実際のパスワードの変更は、NtPassChangeもしくはUnixPassChangeモジュールを呼び出すことによって行なう。

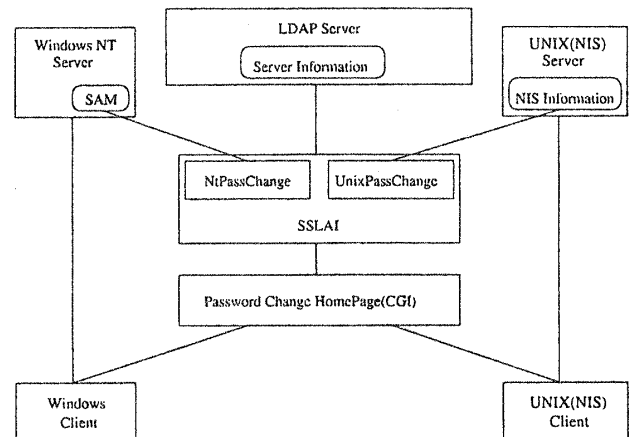


図1: LDAPを用いたパスワード同期システムの構成要素

• NtPassChange, UnixPassChange

これらはSSLAから呼び出されて実際に各サーバのパスワード変更を行なうExpectスクリプトである。サーバで稼働しているtelnetサービスにログインし、パスワードを変更する。

• Password Change Page

パスワード変更要求を送るためのWeb上のページである。セキュリティ向上のために接続にはSSLを用いる。実際にSSLAへ必要な情報を送るのはGCIプログラムである。

• Windows NT4.0 Server, Windows Client

従来と同様の、Microsoft Windowsによるネットワーク環境である。また、サーバはtelnet,SSLのサポートが必要となる。

• UNIX(NIS) Server, UNIX(NIS) Client

従来と同様のUNIXにおいてNISを利用したネットワーク環境である。また、サーバはtelnet,SSLのサポートが必要となる。

2.1 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、基本的な構造、属性などは RFC2307[3] に準拠し、ou の下位にはそのネットワークに属するドメイン (NIS Domain、Windows Domain) の情報が配置される。

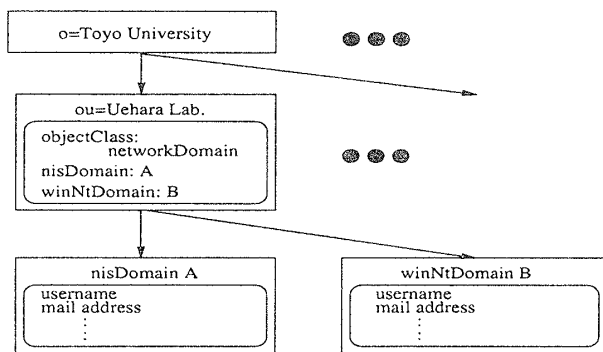


図 2: データベース構造図

2.2 パスワードの認証

Windows NT サーバのアカウント情報データベース (SAM) と NIS サーバの NIS 情報ファイルのユーザパスワード部分をパスワード変更時に同期させているだけなので、パスワードの認証は、Windows 環境、UNIX 環境ともに従来と同様の手順で行なわれる。

2.3 パスワードの変更

パスワードの変更は、UNIX 環境、Windows 環境ともにほぼ同様の手順で行なわれる。

1. 各クライアントは Web 上のパスワード変更要求ページより、必要な情報を入力する。そして、CGI が SSLAI に通信する。これら経路は、SSL によって情報の漏洩が防がれる。
2. SSLAI は、LDAP サーバに対してそのネットワークに属する Windows、UNIX の各サーバのアドレスに関する情報を問い合わせる。この経路もまた、SSL による暗号化がなされる。
3. SSLAI はサーバの情報をもとに、telnet サービスに NtPassChange、UnixPassChange を使って接続し、パスワードの変更を行なう。このとき、UNIX においては UnixPassChange が NIS 情報ファイルのユーザパスワードを、Windows NT に対しても、同一のパスワードによってアカウント情報データベース (SAM) を更新する。

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 Windows NT の SAM と、UNIX の NIS 情報ファイルの両方が変更されることとなり、情報の同期をとることが可能になる。このことから、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になる。

3 今後の課題

現時点では、2つのサーバ (Windows NT と Sun OS、各 1 台ずつ) のパスワードの変更に合計で約 20 秒を要している。ネットワークの負荷などによって変更にかかる時間は変わることが考えられ、タイムアウト処理などを今後検討していく必要がある。さらに、今後の課題として、以下のような事柄があげられる。

- データベースアクセスやネットワーク上の障害による、データベース上の不整合を回避するためのトランザクション機構の導入。
- 処理の高速かのために telnet, expect を用いている部分を専用のデーモン、サービスへ置き換え。
- パスワード情報の LDAP サーバ内での一元管理。

4 おわりに

本論文では、パスワードなどのアカウント情報を独立したデータベースに置き、異なる認証システム間でデータベースの同期をはかることによって、同一のパスワードによる認証を行なうことができるシステムを提案した。今後、アカウント情報を拡張し、ネットワークアカウントの実現をはかりたいと考えている。また、Microsoft Windows 2000 で提供される予定の Active Directory[4] などの他のディレクトリサービスとの関係なども検討していく。

参考文献

- [1] W. Yeong, T. Howes, and S. Kille, "Lightweight Directory Access Protocol," RFC 1777, March 1995.
- [2] <http://home.netscape.com/eng/ss13/ssl-toc.html>, Netscape Communications
- [3] L. Howard, "An Approach for Using LDAP as a Network Information Service," RFC 2307, March 1998.
- [4] <http://www.asia.microsoft.com/japan/support/kb/articles/j046/6/96.thm>, Microsoft Corporation