

5 G-05 ディレクトリサーバによる企業内イントラネットシステム認証の統合

佐藤昌志

株式会社 東芝

1. はじめに

近年、インターネットを中心とする情報技術の激進な進歩により、多くの Webtop システムが企業内に導入されてきている。Webtop システムでは、WWW ブラウザという統一された環境で複数のシステムにアクセスすることが可能になる。また、ソフトウェアは通常サーバ側で管理・配布されるため、クライアントマシンのディスク消費量の削減や TCO 削減の効果も期待できる。

一方、クライアント環境がオープンになったことにより、WWW ブラウザがあれば誰でもアクセス可能であり、セキュリティ上の問題が発生する。また、ユーザ認証はシステム毎に独自に行なわれていることが多く、操作環境が統一されていることのメリットが十分に生かされていない場合が多い。

本稿では、某企業の Webtop 認証システムを例にとり、LDAP ディレクトリサーバ、HTTP-Cookie、サーバ認証 (SSL) 等の技術を駆使し、上記問題を解決していった方法について述べる。

2. システム概要

本システムは、企業内に構築されている複数の Webtop システムへのユーザ認証を統一して行う機能を提供する。従来、当該企業に導入されていたシステムは、クライアント/サーバ型のグループウェアシステム、ホスト端末エミュレータを使用した基幹システムなどであり、IC カードによるシングルサインオンのユーザ認証を行っていた。

今回、Webtop システムを新規に構築するにあたり、従来システムのシングルサインオン環境を継承し、IC カードからの情報を元にユーザ認証を行う必要があった。具体的には、IC カードのシリアル

Integration of some Intranet systems certification
by LDAP Directory Server

Masashi Sato

TOSHIBA CORPORATION

番号により認証を行った。セキュリティの概念図を図1に示す。

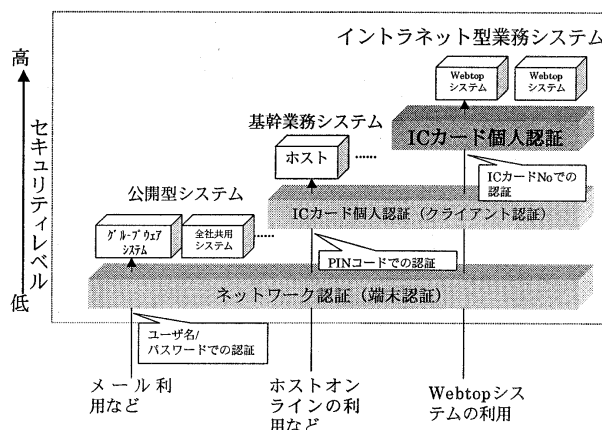


図1 セキュリティ概念図

以上のようなセキュリティポリシーのもと、以下の要件を満たすユーザ認証（個人認証）システムを構築する必要があった。

- (1) 企業内全社員の情報を組織階層も含めて管理したい。
- (2) 権限レベル（ユーザ、アプリケーション）によるアクセス制御を実現したい。
- (3) Webtop システムの入口となるため、可用性を高めたい。

(1)、(2) より階層構造を容易に構築・管理可能であり、階層単位でのアクセス制御が可能でかつ、Webtop システムとの相性がよい LDAP ディレクトリサーバを利用してユーザ管理を実現することとした。

また、(3) については、Netscape Directory Server を2重化しレプリケーション機能を利用してデータの同期をとることで実現した。

3. システム構築における課題と対策

以上で述べたシステム概要・要件から、本システムにて解決すべき主な課題は以下の2つである。

課題1：ICカード情報引渡しと認証情報保持

シングルサインオンを実現するため、ICカード情報を個人認証サーバであるLDAPディレクトリサーバへ引き渡し、その結果の認証情報をWebtopシステムのクライアントソフトとなるWWWブラウザに保持する必要がある。

課題2：LDAPサーバ2重化とクライアントからの透過アクセスの実現

Webtopシステムと入口として重要な役割を果たしているLDAPサーバを2重化する必要があるが、その際、クライアントからはどちらが運用しているのかは意識させず透過的なアクセスを実現する必要がある。

課題3：サーバ認証の強化

本システムで構築する個人認証サーバと同様の認証情報を発行する偽サーバを構築し、クライアントへ認証情報を渡すといった不正な認証を防ぐため、サーバ認証を強化する必要がある。これらの3つの課題に対して、以下のように対策を検討し実現していった。

(1) ICカード情報の引渡し

ICカードの情報取得には、ICカードリーダーをアクセスするプログラムが必要となるが、WWWブラウザ上で実現しようとする、WWWが個人認証サーバへ接続後、ActiveXやJavaなどのプログラムにより、WWWブラウザ経由で情報を引き渡す必要がある。

この場合、接続した個人認証サーバが認証情報送付前にダウンすると、ユーザが手動で接続先サーバを切り替える必要があり、透過的なアクセスが実現できない。そこで、本システムでは、クライアント側にICカードリーダーを読み取るプログラムを常駐させ、WWWブラウザの接続先の個人認証サーバ側からクライアント常駐モジュールにアクセスし、ICカード情報をサーバ側が受け取る仕様とした。本対策では、以降の(3)の仕組みを利用して透過的にアクセスした個人認証側からクライアントへ接続要求

を発行するため、クライアントから個人認証サーバへの透過性は保持される。

(2) 認証情報の保持と認証

サーバ側は受け取った認証情報をLDAPディレクトリサーバに格納されている情報と照合し、認証結果をWWWブラウザに返すが、認証情報の保持はCookieを利用して実現した。各Webtopシステムは、WWWブラウザが保持する認証情報をチェックし、業務実行の可否を判断する方式とした。

(3) 2重化したサーバへの透過的アクセス

ユーザが2つのサーバを意識することなく運用中のサーバへのアクセスを可能とするため、クライアント(Windows95)上にWWWブラウザのアイコンを用意し、その中にJavaScriptを埋め込んで、接続タイムアウトによるサーバの自動切替を実現した。

(4) サーバ認証の強化

サーバ認証を強化するため、アプリケーションとWWWサーバの設定という2つの面からセキュリティ対策を実施した。

各Webtopアプリケーションにおいてはクライアントが正しい個人認証サーバの認証を受けたことを確認するためCGI変数HTTP_REFERERによって直前にアクセスしたURLのチェックを行った。また、個人認証サーバに対してサーバ証明書を取得し、SSLによるサーバ認証を実施した。

4. まとめと今後の課題

本システムでは、既存のシングルサインオンの環境を継承し目的とするセキュリティレベルを達成できた。セキュリティの実装においては、各システムのセキュリティポリシーを事前に設定し、適切なレベルのセキュリティを実装する方法を検討することが重要である。

また、本システムのように、ICカードが利用できる状況にある場合は少なく、シングルサインオン環境の実現には、認証情報をどのように取得・保持するのが重要な課題となる。