平成 14 年度

学士学位論文

Broadband Web サービスに適した認証方式

The Authentication System for Broadband Web Services

1030288　永井 慎太郎

指導教員　清水 明宏

2003 年 02 月 12 日

高知工科大学 情報システム工学科

要 旨

Broadband Web サービスに適した認証方式

永井 慎太郎

ブロードバンドの急速な発展に伴い 1 対多，多対多の通信形態を利用したアプリケーションやサービスが普及し始めている中で，一度に多数の Web 情報を参照するブラウジング手法がある．Web ページには認証を必要とするページが多数あるために，一度に参照できるブラウジング手法を使うと，複数のページを同時に認証する必要性がある．認証においては，公開鍵暗号と，共通鍵暗号を応用した方式がある．公開鍵認証においては認証時における負荷が大きいが，それに対して共通鍵の応用である SAS-2 認証では負荷は小さくてすむ．また，認証を一元化できるものとして「シングルサインオン」がある．しかし，認証は一元化できても，公開鍵暗号の応用による認証方式であるため，認証時の処理負荷が大きくなる．また，処理負荷が大きくなることにより，非常に高価なものになってしまうため，学校や個人などでは導入することが困難である．SAS-2 認証を用いた場合の 1 対多，多対多の通信形態では，認証情報を多数保持し処理を行わなければならない．そこで本研究では，認証負荷の小さい SAS-2 認証方式を用いて，通信形態が 1 対多や多対多においてユーザが認証を行うための処理量を軽減し，各ユーザが保持すべき認証情報を減らす方式の提案を行う．この提案方式により，既存技術であるシングルサインオンソフトに比べて認証処理が軽減され，低コストで導入することができるようになる．

キーワード　ブロードバンド，ブラウジング，ワンタイムパスワード認証方式，公開鍵暗号，共通鍵暗号，シングルサインオン

Abstract

The Authentication System for Broadband Web Services

Shintarou Nagai

A multi-view browsing technique is required because broadband services and multipart communication systems are increasing. If a user uses such technique, he has to be authenticated by plural web sites. An authentication procedure is applied by a public-key cryptography or a secret-key cryptography. Public-key authorization systems have costs, and the SAS-2 (Simple And Secure password authentication protocol, Ver.2) authentication method applied a secret-key cryptosystem which has little costs. " Single Sign On " can unify some authentications. However, that system has two problems: expensive and high-load, because such system is applied a public-key cryptosystem. In this thesis, I propose a new method using the SAS-2 and eliminate the problems that trouble to the existing studies.

key words Broadband, Browsing, one time authentication method, public-key cryptography, secret-key cryptography, Single Sign On

目次

図目次

第 1 章

はじめに

現在のインターネットは，21 億もの Web ページが相互にハイパーリンク接続された巨大で複雑な情報空間であり，日々驚異的な速度で増殖・膨張しているという報告がある [1]．情報空間は膨大で混沌としたのもであるために，ユーザが目的の情報にたどり着くために時間を費やしてしまう．WWW（World Wid Web）では，情報検索をするための検索エンジンやディレクトリサービスなどが存在している．しかし，それらを利用しても目的の情報へたどり着くためには時間がかかってしまう．ここ数年で，加入者系ネットワークの光化が進んできており，家庭から双方向の広帯域通信が可能となりつつある．そういった中で，インターネット上では様々な仲介型サービスが多様化し，大規模化，複雑化してくるため，利用者が目的情報に到達する支援技術が重要となってくる．

このようなインターネット利用者のニーズに答える技術として，NTT 情報流通プラットホーム研究所で開発された超高速ネット空間クルージング技術「InfoLead」[2][3] が存在する．InfoLead は，Web 情報の検索結果を可視化してユーザに提示するための技術である．InfoLead では，一度に数十から数百の Web ページを取得することが可能である．そのため，認証を要するページを取得すると，1 つ 1 つのページに対してユーザ ID とパスワードを入力していかなければならない．しかし，それだけの認証情報（ユーザ ID，パスワード）を記憶しておくのは利用者にとっては負担となり，一度に入力するのは困難である．また，現在使われている Web ページの認証方式 SSL（Secure Socket Layer)[4] を用いた認証をすれば，ユーザ側の端末・サーバ側への処理負荷は大きくなってしまう．そこで，認証情報を一度入力することで，各認証付きページへの認証を成立させることを実現したのが，シングルサインオンソフト [5] である．しかし，認証には SSL などの公開鍵を用いているために，

処理負荷が大きくり，さらに導入コストがかかってしまう．これにより，対象規模が大きくなり，ユーザ規模の小さな学校や個人ユーザなどでは導入することができないのが現状である．

そこで，シングルサインオンを低コストで導入できる方式の提案を NTT 情報流通プラットホーム研究所と共同研究で行った．

第 2 章

研究背景

近年ブロードバンドの急速な発展（図 2.1）とパソコン（PC）の高性能化により，複数の Web ページを一度に参照できるブラウジング手法が開発されている．これは，膨大な情報空間の中で目的の情報にいち早く辿り着きたいことから，感覚的で効率的なブラウジングが要求されているからである．

しかし，Web ページの中には有料サイトなどの認証を必要とする会員制のページも多く存在している．そのほとんどの認証付き Web ページは公開鍵認証で行われているため，比較的安全ではあるがユーザ・サーバ共に処理負荷が大きくなってしまう．また，一度に複数のページを取得するため，各認証ページに対して認証情報を 1 つ 1 つ入力していかなければならない．

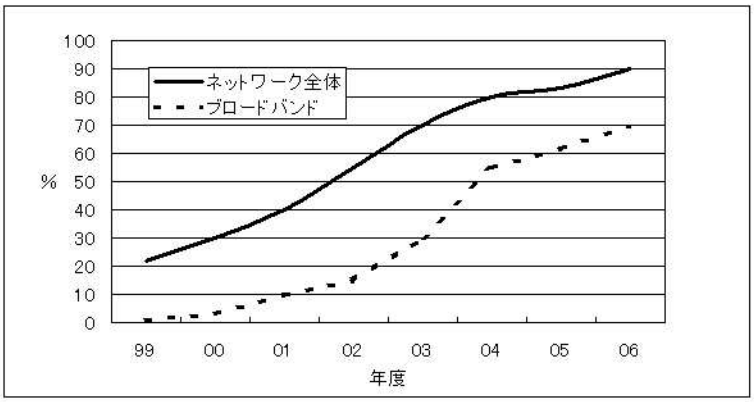

図 2.1　インターネット普及率

2.1　従来の Web ナビゲーション

従来の Web ナビゲーション（情報探索）では，まず，検索エンジン等によって探索範囲の絞り込みを行い，その結果を Web ブラウザを用いて閲覧し確認するのが一般的である．その際，検索エンジンの出力結果は，Web ページのタイトル，サマリ，URL 等が記載されたインデックスリストでしかない．そのため，各インデックスが指し示す情報の実体である Web ページを 1 つ 1 つマウスクリック操作等で取得・閲覧する必要がある．

また，検索エンジンが出力するインデックスリストは膨大なものであり，特に一般的な単一キーワードを入力した場合には数千件以上ものインデックスが出力されることも多い．そのため，ユーザはその全てに対する Web ページを見ることはほぼ不可能である．たとえ見ることができたとしてもリストの先頭 10〜20 件程度の範囲を対象として順次見ることしかできない（図 2.2）．従って，従来の Web ナビゲーションには，絞り込まれた探索範囲が提示されたとしてもその中を網羅的に閲覧することは極めて困難であるという問題がある．

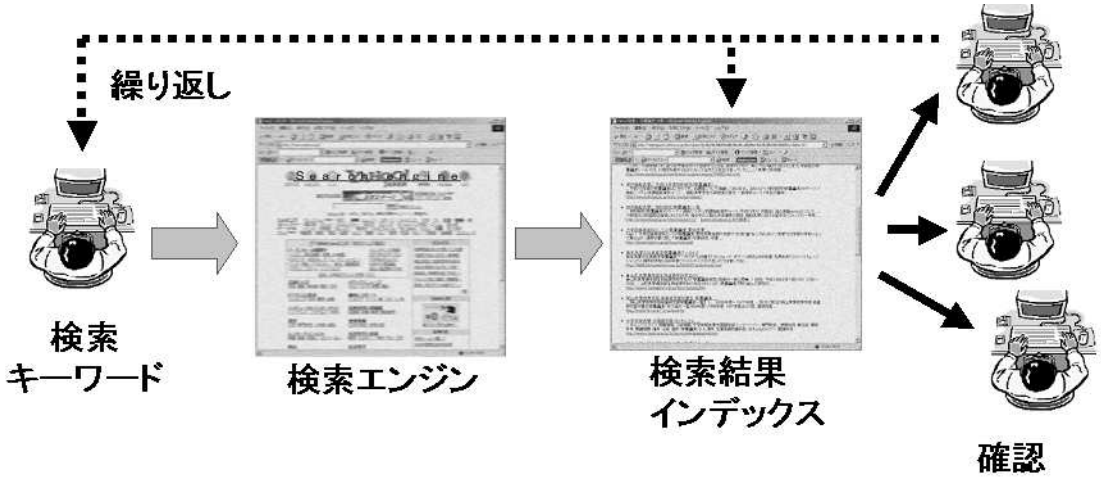

図 2.2　従来の Web ナビゲーション

2.2　情報空間の可視化

従来の Web ナビゲーションの問題点を解決するために，情報空間を可視化する必要がある．この情報空間を可視化する技術は，多く存在している．たとえば，Microsoft 社の TaskGallery や日立製作所の次世代画像検索技術がある [6][7]．これらの技術は PC のデスクトップ上における起動中のアプリケーションやウィンドウなどを対象としたものであったり，特定のデータベースに蓄積された画像を対象としたものである．こういった技術が Web 情報にも適用されるようになってきており，第 3 章で述べる「InfoLead」によって実現されている．

第 3 章

BroadBandWeb サービス

本章では，提案方式の実装に用いる InfoLead とシンプルでセキュアな SAS-2 認証方式について説明する．

3.1 InfoLead

InfoLead は，NTT 情報流通プラットホーム研究所で開発された超高速ネット空間クルージング技術のことである．この技術により，情報空間の可視化が実現されている．InfoLead の機能や技術内容について，順に述べていく．

3.1.1 InfoLead によるクルージングナビゲーション

InfoLead による Web ナビゲーション方式は，大量の Web ページ群をユーザに画面表示する際，表示する位置や角度，サイズ，透明度等を自由に指定して 3 次元空間上に配置することで総覧的なブラウジングを可能とするものである．表示されるネット空間に対するユーザの視点と視線はマウス等による入力デバイス操作を介することで任意に移動させることができ，ユーザは自らの意思によるクルージング感覚でネット空間内を自由自在にナビゲーションすることができる．このようにして人間の視覚による情報識別・判断能力を最大限に引き出し，ユーザが大量の Web ページ群の中から目的の情報を見つけ出すことや，絞り込むまでの時間を飛躍的に短縮させることができる．

ユーザは，Web ページ群とそれらの相互関係に基づいて構成されるネット空間を知覚・認知し，その空間の中をユーザの自由な意思で自在にかつ高速にウォークスルーしてナビゲー

ションできる (図 3.1) . このクルージングナビゲーションは，巨大で複雑かつ混沌としたネット空間の中で人や情報を引き合わせる様々なタイプの仲介型サービスを支援し，従来からあるようなデータベースを用いた検索技術ではサービス性に限界があったものにまで応用することが可能であると考えている.

端末ディスプレイ上で可視化するネット空間を構成するための 3D 軸 (空間定義軸) の規定は，InfoLead が適用される応用サービス毎，あるいは，それを利用するユーザ（の目的）毎に適切なものが異なってくる. この 3D 軸を任意に規定することで，ユーザは端末ディスプレイ上で単純に情報を総覧するだけでなく，ネット空間内の位置や方向が持つ意味を認識し，目的に応じた情報探索を効率良く行うことができるようになる.

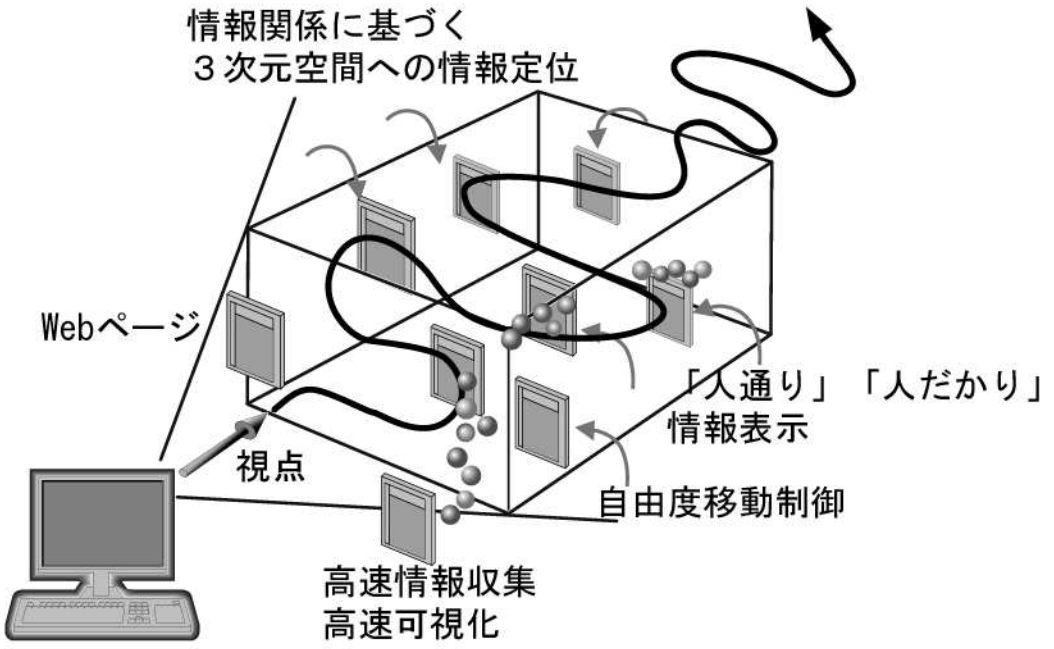

図 3.1 クルージングイメージ

3.1.2 InfoLead ナビゲーションシステム

クルージングナビゲーションを実現する InfoLead ナビゲーションシステムの機能構成について図 3.2 より説明する.

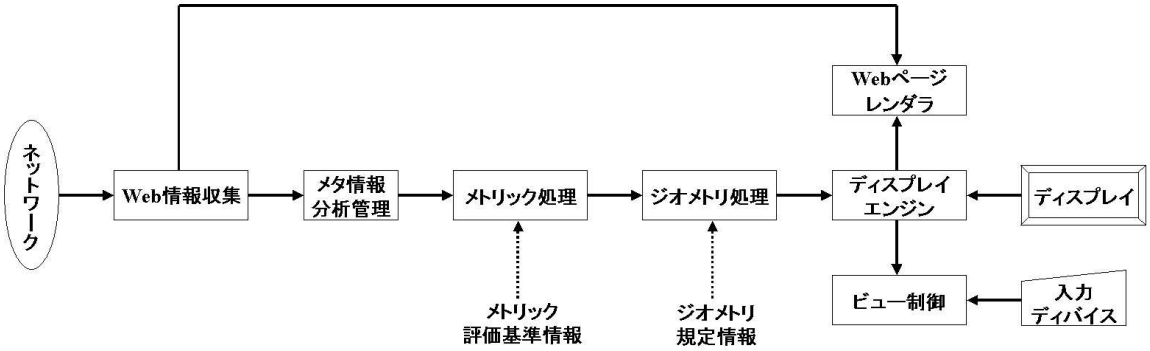

図 3.2 機能構成

- Web 情報収集

  Web ページの HTML ドキュメントやトラヒック情報など，ネットワークから収集する.

- メタ情報分析管理

  Web 情報収集機能が収集した情報を分析し，分析結果をメタ情報として蓄積管理する.

- メトリック処理

  メタ情報を使って Web ページの特質，およびそれらの相互関係を様々な評価基準に基づいて定量評価し，メトリック情報（距離情報）を生成する．ここで必要となる評価基準は，システムが提供するサービスや利用ユーザによって異なるため適宜設定される.

- ジオメトリ処理

  ユーザに提示するネット空間の領域を特定し，メトリック処理の評価基準同様に別ルートで設定されるジオメトリ規定情報（空間定義軸）に基づいて，各情報オブジェクトを空間配置する.

- ディスプレイエンジン

  ネット空間情報をディスプレイに 3 次元表示するためのグラフィック処理を行う.

- Web ページレンダラ

Web 情報収集から取得した HTML ドキュメントをイメージデータ化する.

- ビュー制御

  3 次元表示されるネット空間をブラウジングしているユーザが，入力デバイスを介して操作する視点の移動を認識し，ジオメトリ処理にフィードバックする.

InfoLead ナビゲーションシステムは，ネット空間を 3 次元表示して可視化しているが，InfoLead を適用するアプリケーションサービスによっては 3 次元である必要は無くなる．そこで，ユーザの目的や端末環境に合わせて 2 次元配置も可能となっている．このような，InfoLead ナビゲーションシステムの基本構成を 3.3 に示す.

3.1.3 InfoLead の基本構成

InfoLead は，キーワード検索などで得た Web ページ情報を毎分 200 枚以上のスピードで表示することが可能である．さらに，表示された画像を，単純な操作により 3 次元空間内で高速かつ自由自在にコントロールするクルージングナビゲーションが可能である．InfoLead は，多様な特徴空間から必要な情報を抽出し 3 次元の情報空間として可視化させる．その際，空間提供シナリオをフルに活用することにより情報の配置構成が自由にカスタマイズできるようになる．また，Web ページの相互の関係やアクセス状況などの様々な情報をオーバーレイ表示し概観することができるものである．図 3.3 の説明を以下に示す.

1. 場情報サーバ (Meta Information Server/MIS) は，サービス提供者により構築される．検索エンジン，EC サイトサーバといった場情報を提供するサーバのことである．コンテンツ情報をはじめ，サービス毎に場情報は異なることが一般的である.
2. ネット空間サーバ (Field Server/FS) は，MIS から取得した場情報を元にシナリオを解釈し，3 次元に配置するための座標を計算してシーンを生成するサーバである．また利用者のセッション管理，コンテクスト管理も行っている．JAVA および Servlet で実装している.
3. フィールドエクスプローラ (Field Explorer/FE) は，ネット空間サーバにより生成され

たシーンを利用者端末上に 3 次元的に表示させる Windows アプリケーションプログラムである.

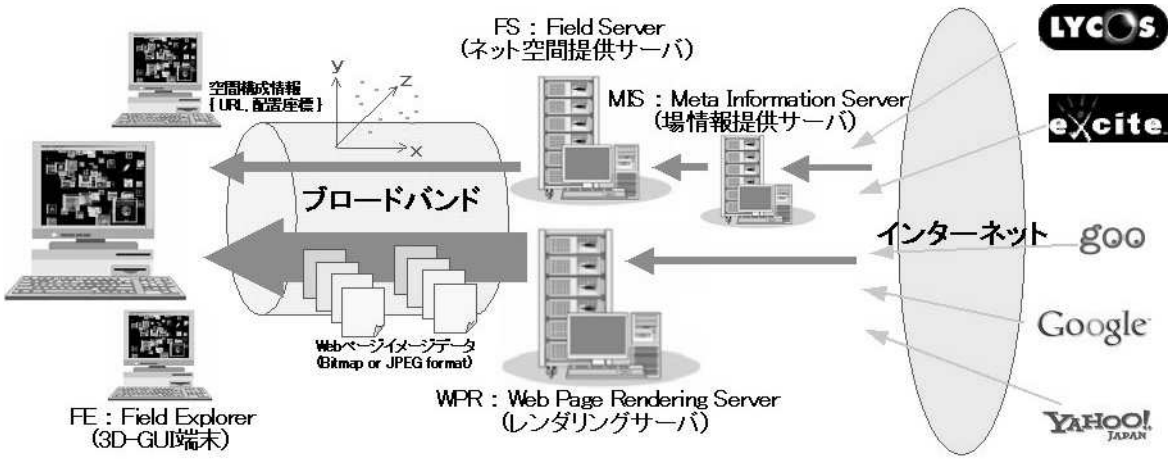

図 3.3 基本構成

3.1.4 InfoLead のサービス提供

サービス提供者が InfoLead でネット空間を用いたサービスを提供する場合，図 3.4 の手続きを実行する．図 3.4 の説明を以下に示す.

1. MIS の構築

   FS はシナリオ解釈時に Web サービスを定義した WSDL を元に，SOAP を使って場情報を MIS から取得する．そこで，MIS を構築するために，サービス提供者は複数のコンテンツに関する場情報を提供するサービスを Web サービスとして公開する必要がある．ただし，既存の Web サービスを利用する場合は必要ない.

2. シナリオの作成サービス提供者は，次に示す要素を含んだシナリオを記述し HTTP サーバ等で公開すれば，FS がそのシナリオを解釈し実行する．シナリオは，場定義部と場選択規則部により成り立っている.

   ・場定義部

個々のシーンを表現する要素．コンテンツ情報 (URL 等) を直接記述し静的なシーンを表現するほか，場情報サーバを使うことで動的に場情報を取得し，シーンに反映させることもできる．記述言語として XSL を採用している．

・場選択規則部

利用者の動作によりシーンを切り替えるための規則を記述する要素．あるシーンを表示しているときに，利用者の挙動を元に次にどのシーンに遷移するかを記述する．記述言語は XML[8] 形式の言語である．InfoLead でシナリオが動作する手順としては次より示す.

3. 利用者の要求するシナリオを FS が取得する.
4. FS が，シナリオの場選択規則部を解釈し，シーン遷移表を作る.
5. 場定義部を解釈し，シーン情報を生成する．このとき，場情報取得命令が記述されている場合，MIS から場情報を取得する.
6. FE はシーン情報を受け取り，シーンを利用者に表示する．ここで利用者の動作により 2. のシーン遷移表から適切な場定義部を選択し，3.・4. を繰り返す.

この流れで，シナリオが動作して個人環境を抽出することができる.

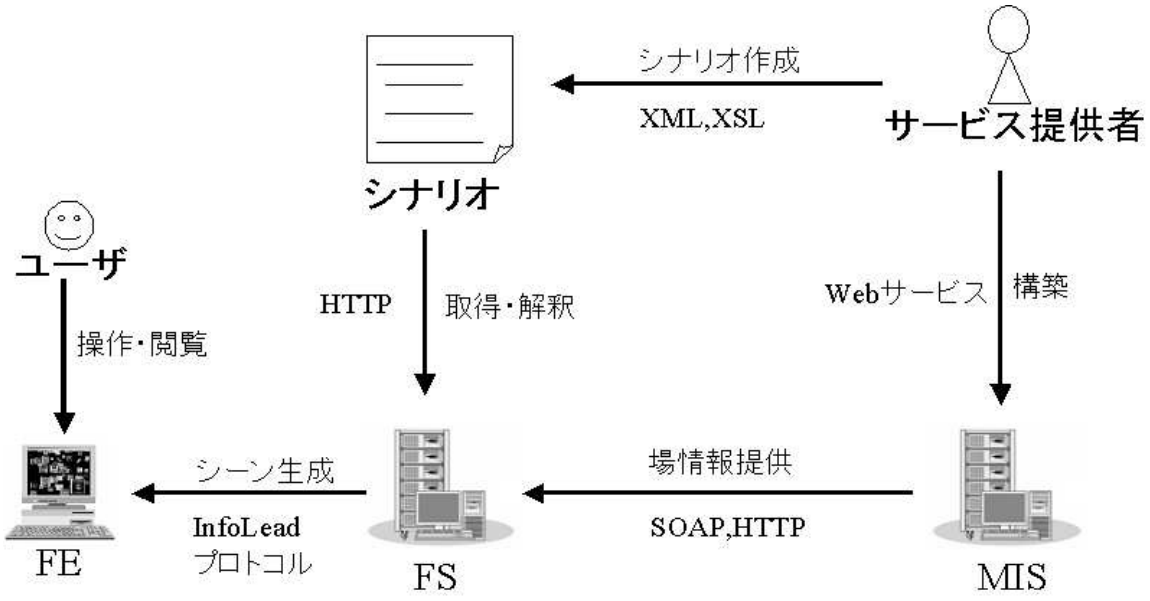

図 3.4　システム構成

3.1.5　InfoLead のブラウジングイメージ

InfoLead は，3D-GUI 機能，Web ページレンダリング機能，場情報提供機能，ネット空間提供機能にて構成されている．InfoLead は，応用サービスやユーザの目的に応じ 3D 軸を任意に規定することにより，ユーザは単純に情報を総覧するだけでなく，ネット空間内の位置や方向が持つ意味を認識し，目的に応じたナビゲーションを効率よく行うことができるシステムである（図 3.5）.

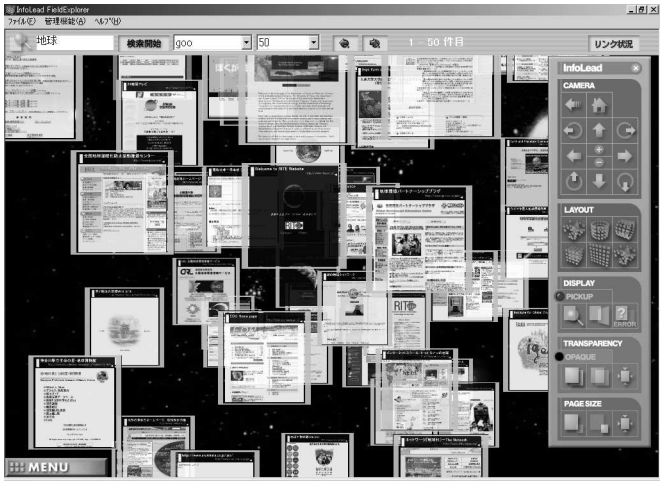

図 3.5　ブラウジングイメージ

3.1.6　InfoLead での問題点

InfoLead を用いて Web 情報を参照すると，一度に数十から数百枚のページを取得できる．そのため，認証を必要とするページを取得する際には，複数の認証情報を入力していかなければならない．また，全ての認証ページに対しての ID とパスワードを覚えておかなければならない．それを解決するための方法として以下の方式がある．

3.2　シングルサインオン

パスワードを必要とする Web サイトの増加やネットワークの多様化，イントラネット・エクストラネット上での Web サイト利用の増加などにより，複数のパスワードを保持しなければならない．シングルサインオンソフトとは，複数のパスワードを保持せずに，利用するシステムへの認証を一元化が実現できるものである（図 3.6）．

Web システム，Web ベースのパッケージソフト，携帯電話向けの Web システムなど，多様なシステムをつなぎ込むとなると，シングルサインオン環境は容易に実現できない．また，シングルサインオンソフトは非常に高価なものであり，対象を学校，個人としていないために導入するのは難しい．また，個人向けに開発さているものもあるが，金融機関などの特定サイトに限られたものしかない [8]． そこで，認証時の処理負荷が軽減されるであろう SAS-2（Simple And Secure password authentication protocol, Ver.2）認証方式を用いてシステムの提案を行う．

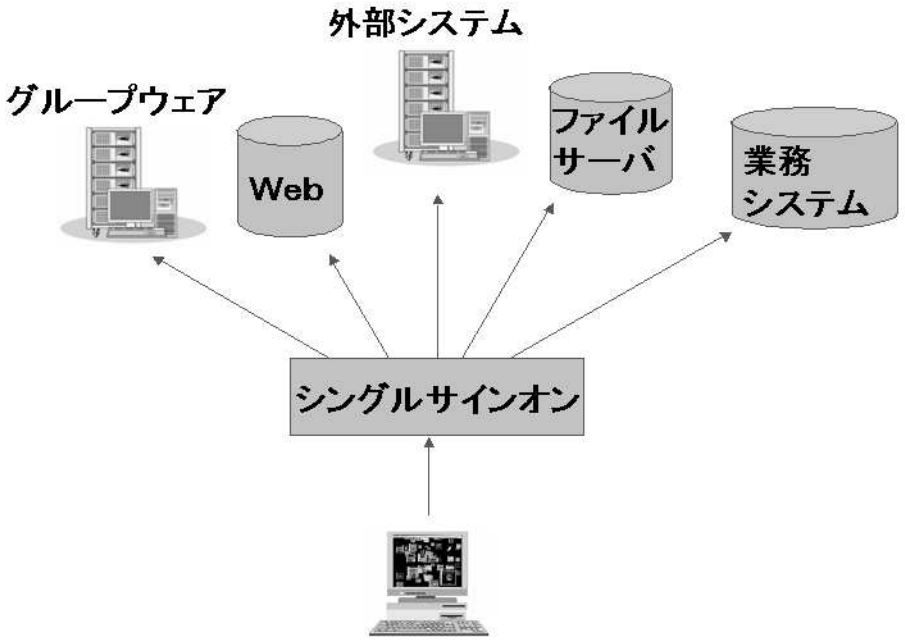

図 3.6　シングルサインオンソフト

3.3　SAS-2 認証

本システムでは，ユーザ認証に本研究室で開発された SAS-2 認証方式を用いる．SAS-2 認証方式は，ワンタイムパスワード認証方式の一つである．ユーザ認証に用いる SAS-2 認証方式の認証プロトコルについて以下で説明する．

3.3.1　記号の定義

ID:ユーザ ID

PASS:ユーザパスワード

N_n:乱数

A:初期登録情報（今回認証情報）

C:次回認証情報

D:次回認証情報にハッシュ関数を掛けたデータ

E，F，H:ハッシュ関数 (一方向性関数)

α，β:マスク情報

⊕:排他的論理和

→:出力

3.3.2 初期登録

1. まずユーザは, パスワード（PASS）と乱数 Nn を排他的論理輪を掛けたものとユーザ ID（ID）から A を作り，ID を付け安全なルートを使ってサーバに登録する.

   式としては，A=E (ID，PASS $\oplus$ N_n),ID

2. サーバは, ユーザから送られてきた ID と A を保持しておく.

3. ユーザは, パスワードと乱数 $Nn + 1$ から次回認証情報である

   C=E (ID,S $\oplus$ N_{n+1}) を作成.

4. 次回認証情報である C にハッシュ関数 F を掛け

   D=F(C) を保持しておく.

3.3.3 認証処理

1. ユーザは, サーバに認証要求として

   ID

   α =C⊕(D+A)

   β =D⊕A

   のデータをサーバに送信する.

2. サーバは, 送られてきた情報に対し, 事前に保持しておいたデータ（今回は A）を用いユーザ認証を行う.

   ユーザから送られてきた β に対し，所持しておいた A を排他的論理輪で足すことで D のデータを得ることができる.

   β ⊕A → D

得た D のデータを用いて,

$\alpha \oplus$(D+A) → C

の計算を行うことで, 次回認証情報である C を導きだせる.

3. 次回認証情報にハッシュ関数 F を掛けることで,

   F(C)=D を得ることができる.

4. 求められた D に対しこれまでのハッシュ関数とは異なるハッシュ関数 H を掛け,H(D) を生成する.
5. 同様にユーザ側でも D というデータに対しハッシュ関数 H を掛け,H(D) を生成する.
6. サーバは H(D) というデータを安全なルートでユーザに送り, ユーザ側で生成しておいた H(D) の情報と比較する. データが一致することにより相互認証が成立する.

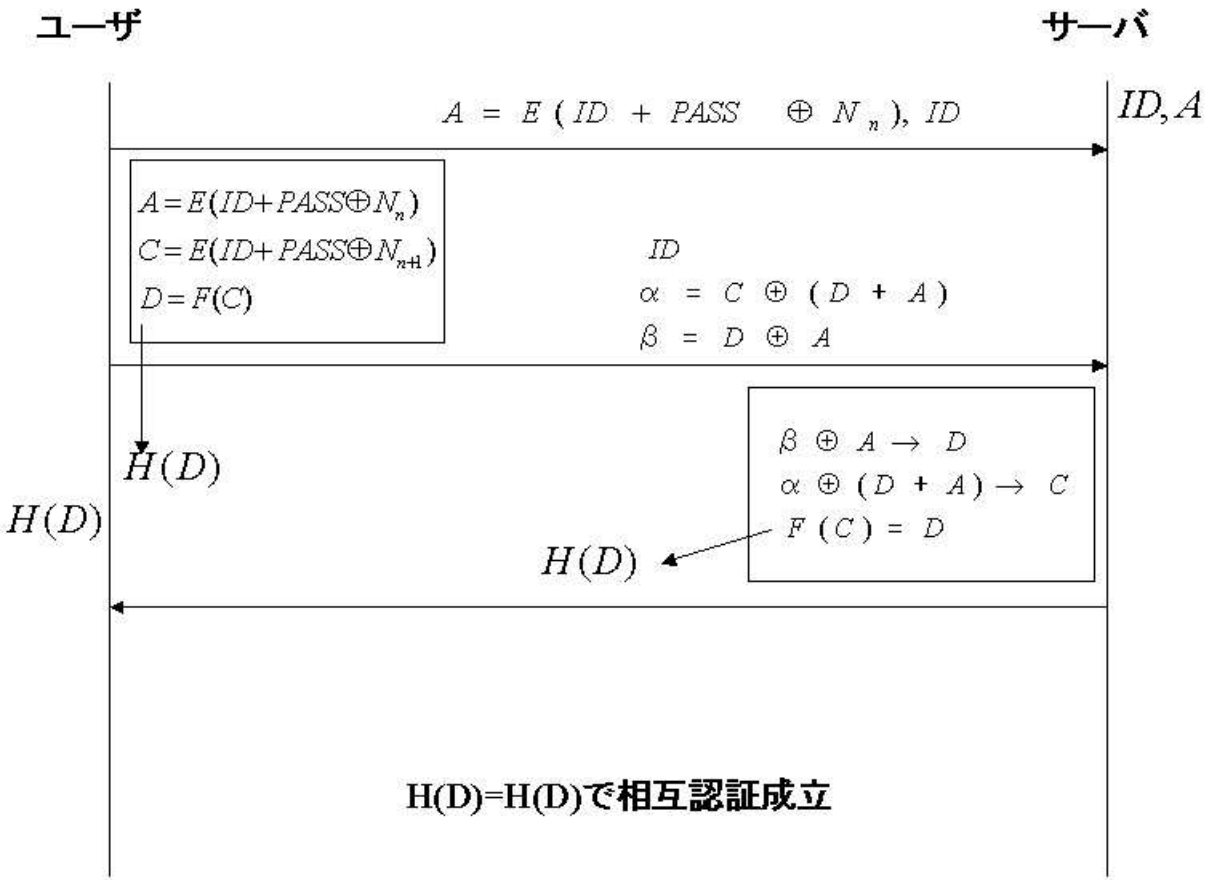

図 3.7　SAS-2 プロトコル図

第 4 章

提案システム

InfoLead では，複数のページを 1 度に取得できる．そのため，Web 情報に含まれる認証付きページに対して，1 回の認証でログインできるシステムを提案する．既存技術としては認証を一元化するシングルサインオンソフトがある．しかし，シングルサインオンソフトでは認証に公開鍵を用いているために，ユーザ側での処理負荷が大きくなってしまう．そこで，認証を一元化でき，なおかつユーザへの処理負荷が軽減される方式の提案を SAS-2 認証を用いて行う．

4.1 提案方式

1 度に複数の認証ページに対して認証情報を入力することにより，認証情報は 1 組だけ保持しておけばよいことになる．そこで，ユーザの処理量を軽減し，各ユーザが保持すべき認証情報を減らすために，中継サーバを設ける（図 4.1）．中継サーバを設けることにより，ユーザは認証情報を 1 組だけ保持しておけばよくなるため，ユーザの処理量は軽減する．

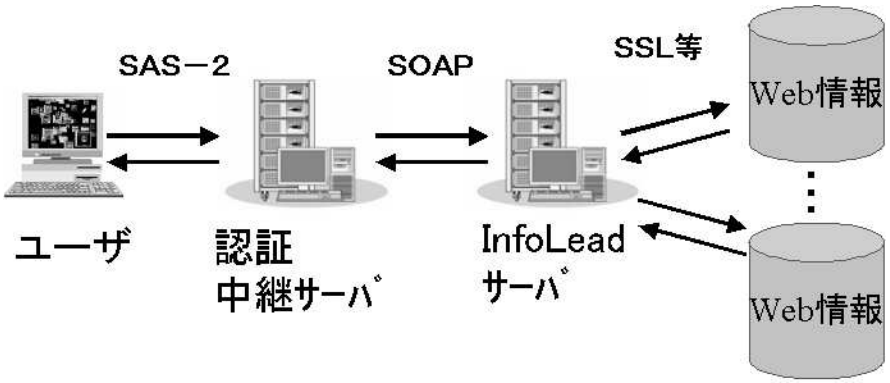

図 4.1　提案システム

4.2　SAS-2 モジュール化

SAS-2 認証方式は，処理負荷が軽くてシンプルな認証方式ではあるが，これだけでは実装することはできない．そこで，SAS-2 のサーバ側とクライアント側のプログラムをそれぞれモジュール化することにより，InfoLead のシステム内に組み込むことができる．これにより，本研究の目的である「ユーザが認証を行うための処理量を軽減し，各ユーザが保持すべき認証情報を減らす方式」の提案の実現ができる．

4.3　システム構成

InfoLead のシステム内に SAS-2 認証用のサーバを設けることにより，認証を一度に成立させることができる．そこで，InfoLead 内のネット空間提供サーバ（FS）内に SAS-2 クライアントモジュール，場情報提供サーバ（MIS）に SAS-2 サーバモジュールをそれぞれ導入する（図 4.2）．流れは以下ようになる（図 4.3）．

1. FE よりシナリオ実行要求をする．
2. FS 内で各ユーザの空間提供シナリオ（以降シナリオとする）が起動される．
3. ユーザ個別のシナリオを起動するために，FS 側から FE に対してユーザ ID とパスワードを要求する．

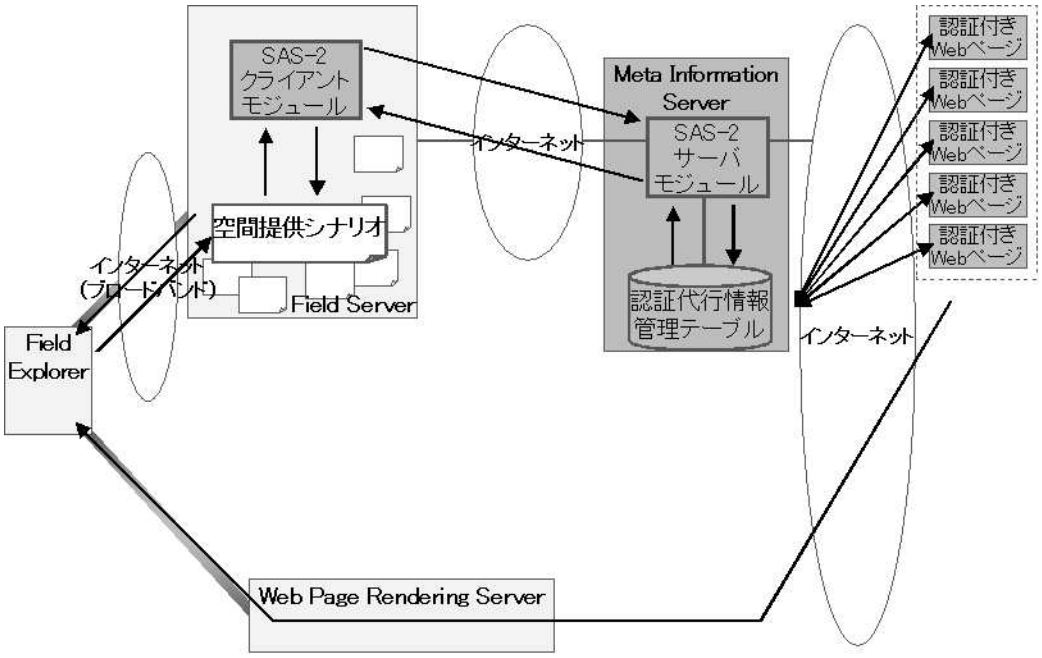

図 4.2　システム構成

4. FE 側でユーザ ID とパスワードを入力する.
5. FS 側で認証が成立すれば以降が実行できる．認証が不成立の場合はエラーを返す．ここでの認証とは，プラットホーム認証でありワンタイムパスワード認証ではない.
6. FS 内のシナリオより，SAS-2 認証の実行要求を行う.
7. 同じく FS 内の SAS-2 クライアントモジュール（以降クライアントモジュールとする）より MIS 内にある SAS-2 認証サーバ内の SAS-2 サーバモジュール（以降サーバモジュールとする）に対して認証要求を行う.
8. サーバモジュールで認証を実行する．認証が成立すれば 9. 以降が実行される．認証が不成立の場合はエラーを返す.
9. SAS-2 認証サーバ内にある認証代行情報管理テーブルより，Web ページの URL 群を取り出し認証を行う.
10. 認証が成立した Web ページの URL 群をサーバモジュールに返す.
11. サーバモジュールよりクライアントモジュールに対して，認証後 URL 群と相互認証成立の通知を送信する.
12. クライアントモジュールからシナリオに認証後 URL 群を送信する.

13. 受け取った認証後 URL 群を，シナリオ上に定義されている Web ページイメージの配置座標値とともに FE に送信する．
14. FE では，シナリオから受け取った URL 群に対する Web ページイメージを WPR を通して取得する．
15. FE では，WPR からの Web ページイメージを，シナリオから受け取った配置座標値にしたがって 3D 空間に表示する．

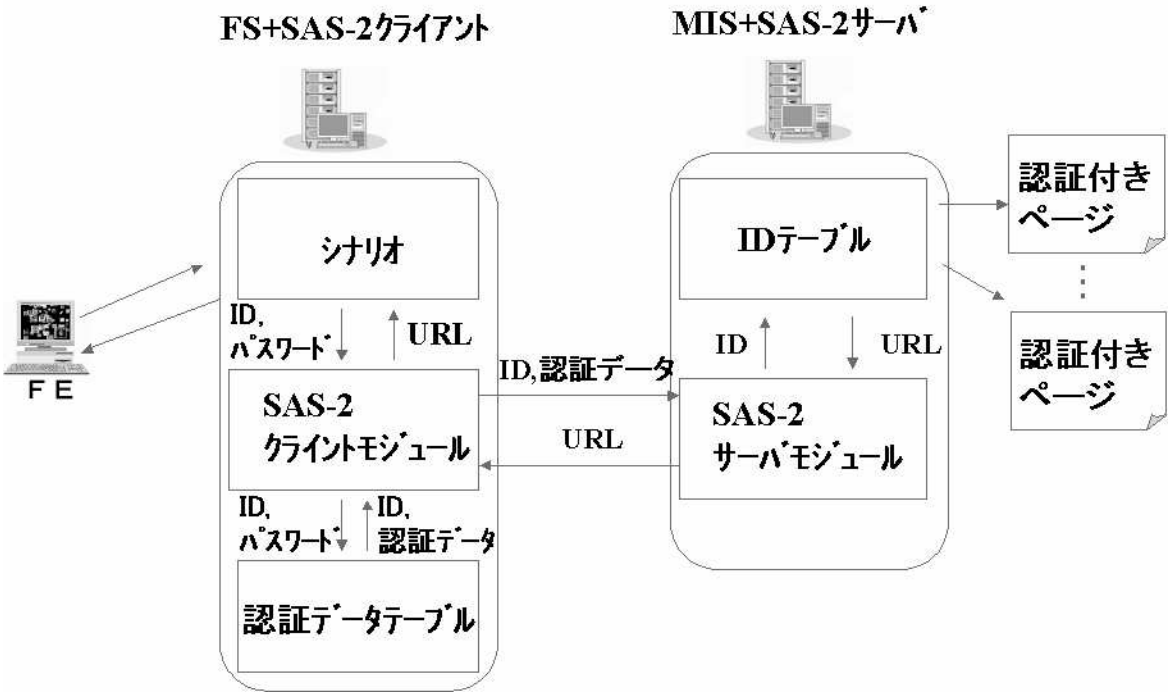

図 4.3　システム内構成

4.4　シーケンス

システムの流れを，データと共に説明していく（図 54.4）.

1. FE より FS 内にあるシナリオに対して，プラットホーム認証のデータである ID とパスワードを送信する.
2. シナリオから認証前の URL と SAS-2 認証要求を FE に行う.
3. SAS-2 認証用の ID とパスワードをシナリオに送信する.
4. シナリオから FS 内にある SAS-2 クライアントモジュールに対して，SAS-2 認証用の ID とパスワードを送信する.
5. SAS-2 クライアントモジュールから FS 内にある認証データテーブルへ SAS-2 認証用の ID とパスワードを送信する.
6. 認証データテーブルから SAS-2 認証データ（乱数）を抽出する.
7. 抽出した認証データを SAS-2 サーバモジュールに対して送信する.
8. SAS-2 サーバモジュールにて SAS-2 認証を実行する.
9. 認証が成立すれば，MIS 内にある ID テーブルより認証 Web ページの URL 群を抽出する.
10. 抽出した URL 群の認証が成立すれば，認証成立 URL 群を SAS-2 サーバモジュールに返す.
11. SAS-2 サーバモジュールから SAS-2 クライアントモジュールに対して相互認証データと認証成立 URL 群を送信する.
12. SAS-2 クライアントモジュールで相互認証が成立すれば，シナリオに通知する.
13. 相互認証成立通知を受けたシナリオから認証成立 URL 群を受け取る.
14. シナリオから FE に認証成立 URL を送信する.
15. 各認証個所において，認証が成立しなかった場合は，認証不成立の通知と共に認証前 URL 群を送信する.

4.4　シーケンス

図 4.4　シーケンス図

第 5 章

評価実験

InfoLead のシステムに SAS-2 認証サーバを導入して，提案方式の有用性を評価する．また，実際のインタフェースについても説明を行う．さらに，既存方式と提案方式それぞれの認証処理負荷について比較を行う．この評価を行うことで，本研究での提案方式の有用性を証明することができた．

5.1 実験環境

本システムの有用性を評価するための実験を行う．実験環境としては図 5.1 のようになっており，ユーザ（FE）と SAS-2 認証サーバは学内に設けている．InfoLead で個人環境を設けるために，プラットホーム認証の際に認証付き Web ページを表示させるようにする．表示させる認証付き Web ページは事前登録しておく．プラットホーム認証が成立すれば，ユーザ別のシナリオを取得するので，画面には事前に会員になってあるページしか表示されていない．この実装で用いる「InfoLead」のシステム環境については，NTT 情報流通プラットホーム研究所より提供を受けている．この環境で，評価実験を行った．

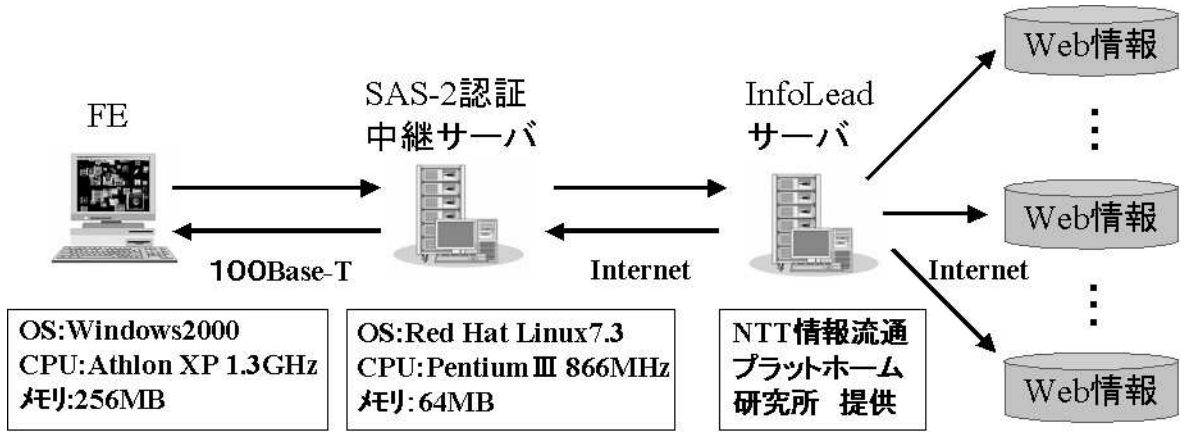

図 5.1　実験環境

5.1.1　認証実行シナリオ

シナリオによる制御で InfoLead の環境が利用できるため，本システムを実行するにあたり，どのようなシナリオが必要であるかを図 5.2 で説明する．

まず，本システムにおいて SAS-2 認証を行うために認証の実行要求を出すシナリオが必要である．初期画面表示シナリオと認証後画面表示シナリオがある．初期画面表示シナリオでは，ユーザが事前に登録してある Web ページを表示し，ユーザが認証要求を出すことでシナリオから SAS-2 認証サーバに認証要求を出し認証を行う．認証が成立すれば，認証後の Web 情報がユーザに提供される．認証後画面表示シナリオでは，ユーザがデータを更新する際に，認証付きの Web ページに再度認証を行うためにシナリオから SAS-2 認証サーバに対して認証要求を行う必要がある．また，この 2 つのシナリオを制御しているのが，ユーザ個別シナリオである．

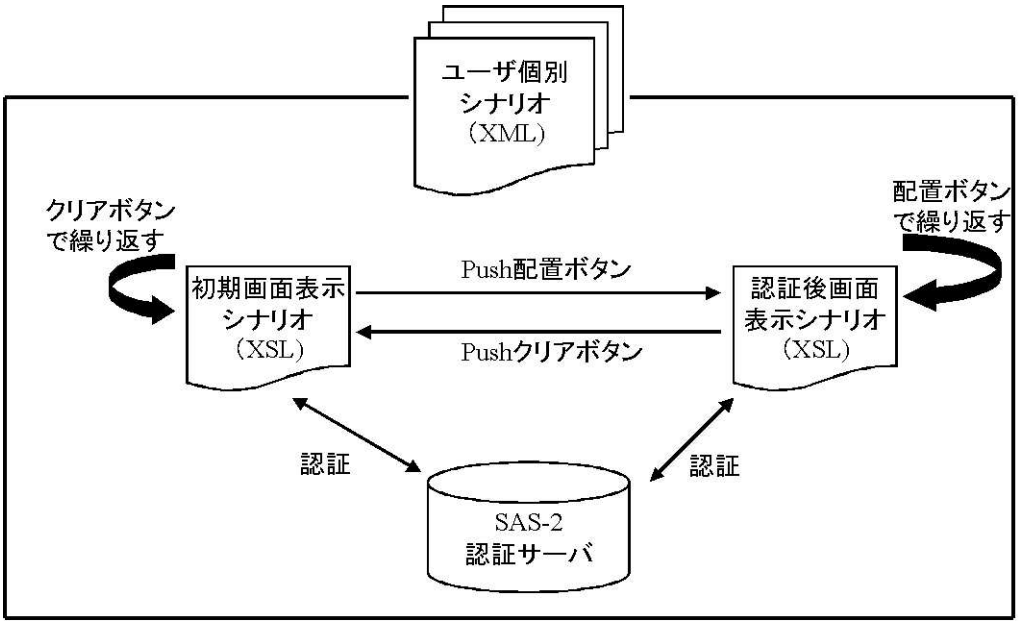

図 5.2　XML による制御

5.1.2　認証前インタフェース

実験で用いたインタフェースが図 5.3 である．図 5.3 は InfoLead でプラットホーム認証した段階の画面で，認証前の情報が表示されている．これは，5.1.1 節で述べた初期画面表示シナリオによるもので，左上のユーザ ID とパスワードを入力して配置を行うとシナリオから認証要求が行われる．認証が成立した結果が 5.1.3 節である．

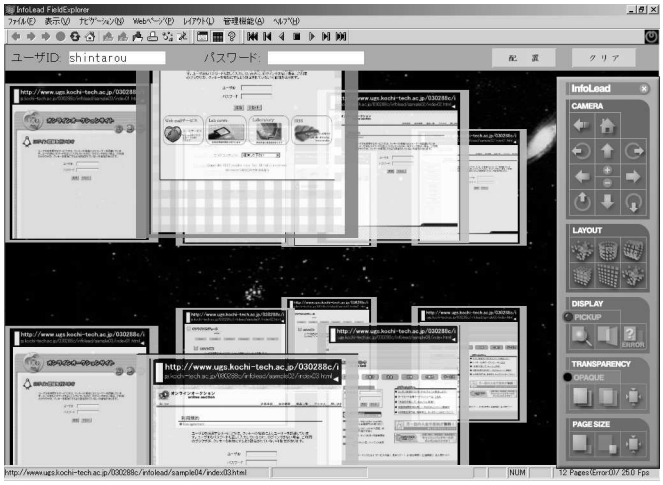

図 5.3　SAS-2 認証前

5.1.3　認証後インタフェース

SAS-2 認証が成立した結果を，認証後画面表示シナリオにより取り出し，認証後の Web ページを取得し配置したものが図 5.4 である．SAS-2 認証が成立しなかった場合は，図 5.2 の SAS-2 認証前画面が表示され，再度正確なユーザ ID とパスワードを入力する必要がある．正確な認証情報を入力するまでは，認証前画面が表示されている．

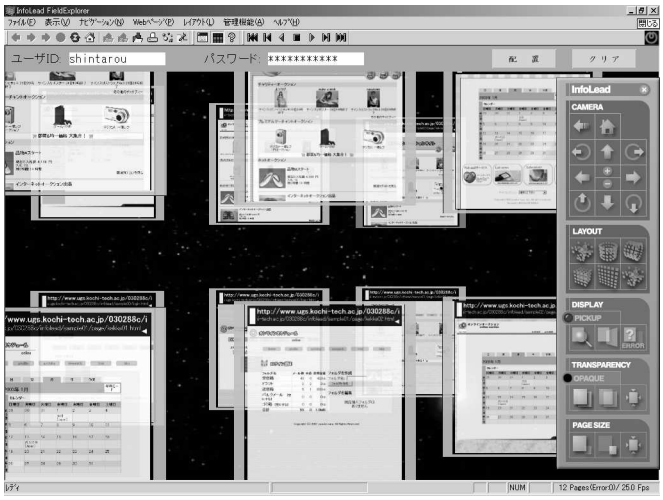

図 5.4　SAS-2 認証後

5.2　評価方法

本研究の提案システムにより，複数の認証付き Web ページへの認証を一元化できるようになった．そこで，各 Web ページにアクセスし認証にかかる処理負荷を計測する．今回は，既存の認証方式で，10 ページの認証付き Web ページに対して，認証を実行することで，提案システムとの比較を行う．これにより，本システムの有用性が証明される．また，既存のシングルサインオンソフトとの導入にかかるコストの比較を行う．これは，本システムによる処理負荷の軽減から，高価なシステムの導入を行わなくてよいといった点から比較できる．

5.3　評価結果

従来の認証方式（SSL）を用いた Web ページへのアクセスでは，1 ページを取得するごとに認証を行っているため，認証時の処理負荷が大きく継続されている．この処理の継続は，評価方法で述べたように 10 ページ分の認証が成立するまで行われる．それに対して，SAS-2 認証においては，認証中継サーバを設けているために，認証は 10 ページに対して 1 回のみである．そのため，Web ページの増減に関係なくユーザには一定の処理負荷しかかからないことが図 5.5 で明らかである．また，SSL 認証方式に比べ処理負荷は，約 60%ダウンしたことになる．この結果から，本研究の提案システムが認証時における処理負荷の軽減が行えていることがわかる．

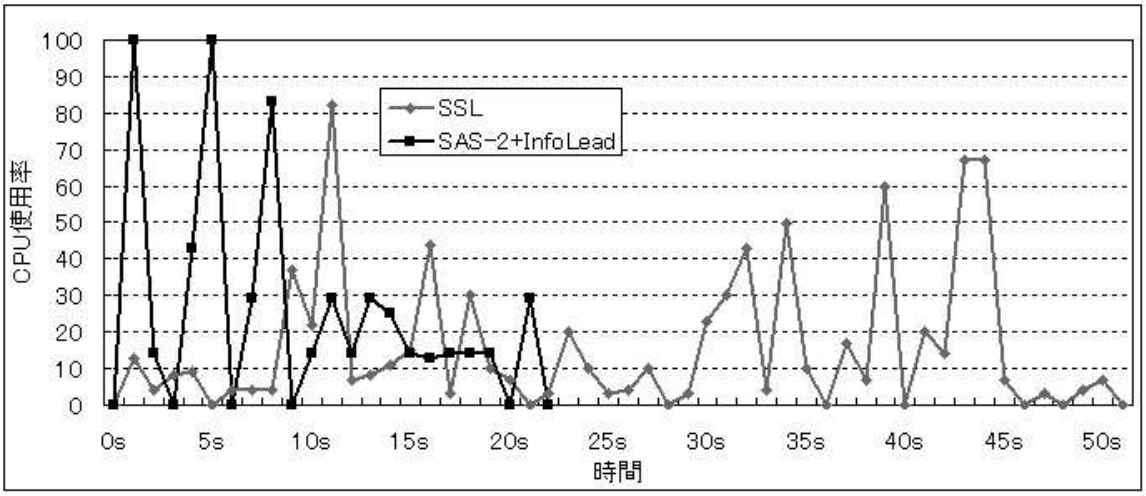

図 5.5　CPU 処理負荷

また，ユーザがプラットホーム認証により，システムにログインする．ログイン後に表示される Web ページに対して，認証情報を入力してから，認証後の Web ページが表示されるまでのユーザ端末での処理時間を比較したものが図 5.6 である．このグラフからもわかるように，本システムにおいては約 40%の処理時間の短縮が実現できた．

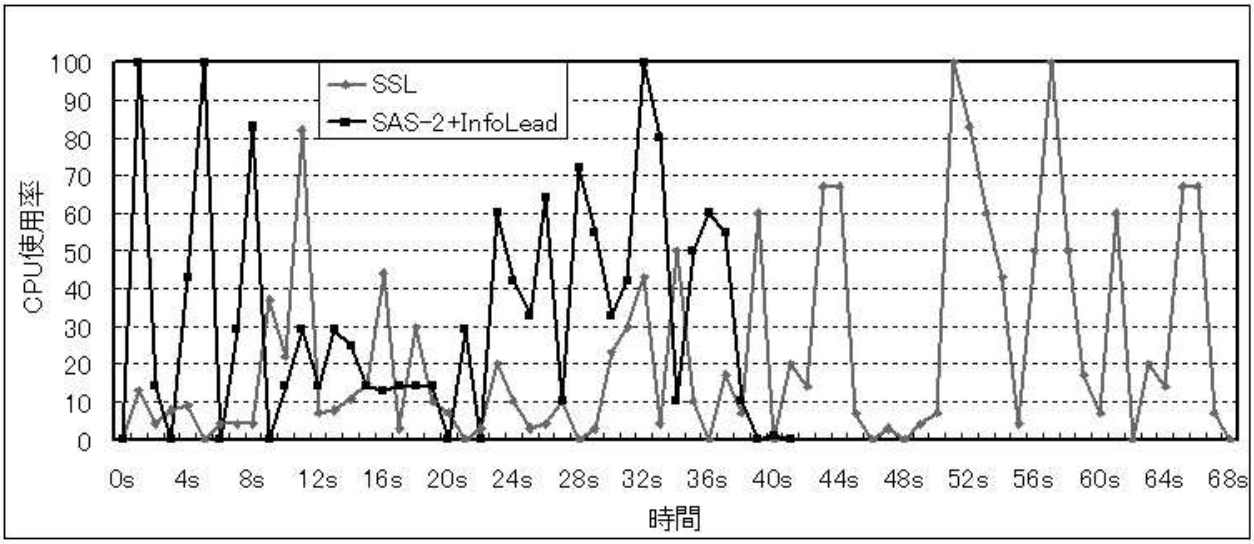

図 5.6 CPU 処理負荷

5.4 考察

評価実験より得られた結果から，複数の認証付き Web ページにアクセスした際にも，ユーザにおける認証処理負荷は軽くてすみ，処理負荷はページ数に関係なく一定である．そのため，本システムは対象規模（ユーザ数）の小さい学校や個人ユーザに適していると考えられる．

また，既存のシングルサインオンソフトの導入コストが高価であり，対象規模が大きいものがほとんどである．それに対して，本システムでは処理負荷を軽減できているために，高価なシステムを導入しなくて済む．そのため，低コストでユーザ規模に左右されることが無く，ユーザ規模の少ない学校や，個人での導入を可能としている（図 5.7）．

図 5.6 で対象規模の小さい部分をカバーしているソフトウェアでも，サーバの導入コストなどは省いているが，実際は高価なサーバを導入する必要性が生じる．また，対象規模の大きいものについては，導入コストも高価であるために，SAS-2 シングルサインオンのほうが，ユーザの対象規模が小さな個人から規模の大きい部分もカバーできるため本システムの有用性が証明できると考えられる．

本システムにおけるセキュリティであるが，Web ページでは最低限の個人認証だけでよいページに対して，SSL 認証を用いる必要は無いのではないかと考えられる．SSL 認証を

用いるページは，その後の暗号化通信を目的としているために，オンラインバンクなどの暗号化しなければならないページではなく，掲示板などの会員制のページでは暗号化通信は必要でないと推測される．そのため，本システムを導入することにより，処理負荷をより軽くすることができ，最低限のセキュリティを保つことができるのではないかと考えられる．

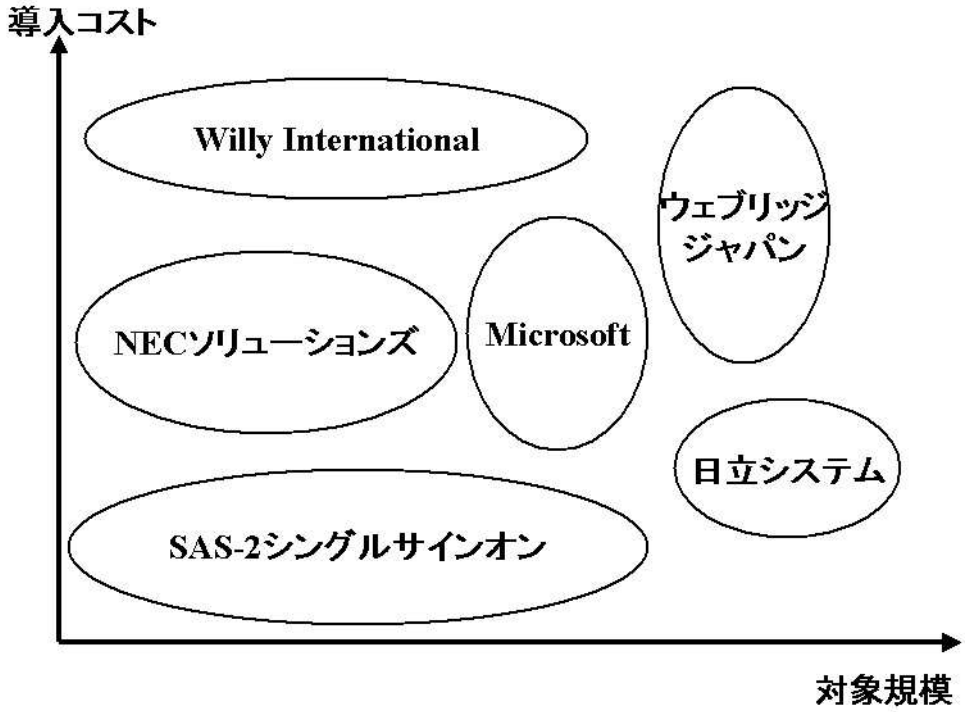

図 5.7　導入コスト

第 6 章

おわりに

本システムの評価であるが，今回の評価に加えて Web ページのリクエストから，認証を経て，端末表示までの時間的な評価を行えるのではと考えている．これにより，システム全体（InfoLead を含む）の評価ができ，従来の Web ナビゲーションとの違いを明らかにできるのではと考えられる．

既存の技術では，シングルサインオンソフトを用いている．このソフトでは，対象が Web だけではなく，外部システムやファイルサーバへのログインも行えるものである．本研究のシステムでは，Web 情報に対しての認証は行えるが，他のシステムへのログインを対象としていない．そこで，SAS-2 認証時に用いる認証情報を利用して暗号化通信ができるのではないかと考えている．

本研究での提案方式は，SAS-2 認証中継サーバを設けることによって，複数の認証付き Web ページへの認証を一元化することができた．これは，ユーザ端末と中継サーバ間のみで認証が成立することで，各ページへの認証を成立させることができるためである．本システムにより，ユーザ端末での認証時における処理負荷が軽減された．さらに，既存のシングルサインオンソフトによる認証一元化に比べて，低コストで比較的安全性の高い通信を可能とすることができた．

また，今回の提案方式の実装には，InfoLead を用いて行ったが，ブロードバンドの普及と共に情報空間総覧型の Web ブラウザが多く開発されてくると推測される．そういった InfoLead 以外のブラウザにでも適用できるシステムである。

謝辞

高知工科大学工学部情報システム工学科 清水明宏教授には，研究室配属以来，就職活動，卒業研究を含め，学生生活全般に渡って懇切なる御指導，貴重な御教示を賜った．ここに深謝申し上げる．

NTT 情報流通プラットホーム研究所の川村 亨氏，中野 篤氏には，本研究においてシステムの提案から構築まで懇切丁寧なご指導・ご助言・ご協力を賜り，心より感謝いたします．

NTT アドバンステクノロジ株式会社の渡邊 大介氏には，本研究においてシステムの構築を懇切丁寧なご指導・ご助言・ご協力を賜り，心より感謝いたします．

株式会社ピクトの二宮 真澄氏には，本研究においてご協力を賜り，心より感謝いたします．

在学中に様々な御助言，御指導頂いた諸先生方に心より感謝いたします．

高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース 2 回生 辻 貴介氏には，研究内容について有益な語義論をいただき御指導を賜った．

高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース 1 回生 上岡 隆氏，河村 智氏，情報システム工学科 4 回生 池上 奈津子氏，岸田 光生氏，小西 竜也氏，田岡 慎也氏，奈良 裕介氏，3 回生 福冨 英次氏，光國 聡志氏には，実験準備から実験において御協力頂いた．ここに記して謝意を表する．

参考文献

[1] Cyveillance Inc.「Cyveillance-Leading Provider of e-BusinessIntelligence」
http://www.cyveillance.com/web/newsroom/releases/2000/2000-07-10.htm

[2] 川村 亨, 竹内 格, 武藤 哲幸, 樋渡 仁, “光時代のネット空間クルージング技術「InfoLead」,” NTT R&D, Vol.49, No.10, pp.605-615, 2000

[3] T. Kawamura, A. Kanai, K. Takeuchi, T. Mutou :「A Proposed Net-space Service using “InfoLead” Cruising Navigation Technology」, SAINT2002, 2002

[4] シングル・サインオン
http://www.netone.co.jp/doc/kiji/nwp200203.pdf

[5] How SSL Works
http://developer.netscape.com/tech/security/ssl/howitworks.html

[6] The TaskGallery - Home
http://research.microsoft.com/ui/TaskGallery/index.htm

[7] HITACHI
http://www.hitachi.co.jp/New/cnews/0005/0529a.html

[8] Yahoo!ファイナンス「口座管理」
http://biz.yahoo.co.jp/accountmanager/moneylook/web/

[9] T. Tsuji, T. Kamioka, and A. Shimizu, “Simple and secure password authentication protocol, ver.2 (SAS-2),” IEICE Technical Report, OIS2002-30, vol.102, no.314, pp.7-11, September 2002.

[10] 池田 実, 小野寺 尚希, “最新 XML がわかる,” 株式会社 技術評論社

[11] Steven Holzner, “Java プログラミング Black Book,” 株式会社 インプレス