知能と複雑系　121－1
（2000．7．18）

利用を限定したＷｅｂサイトにおける個人モデルを利用したセキュリティについて

金西　計英[*1]　　戸川　聡[*2]　　矢野　米雄[*3]

徳島大学大学開放実践センター[*1]　四国大学情報処理教育センター[*2]　徳島大学工学部[*3]

[*1]徳島市南常三島町１－１　　088-656-7285
[*2]徳島市応神町古川１２３－１　088-656-1300
[*3]徳島市南常三島町２－１　　088-656-7495

mailto: marukin@is.tokushima-u.ac.jp, togawa@shikoku-u.ac.jp, yano@is.tokushima-u.ac.jp

あらまし　本研究の目的は，利用者を限定したWebサイトにを対象としたセキュリティシステムの構築である．通常の閲覧履歴から個々の利用者のユーザモデルを作成する．このユーザモデルは利用者の個性を表現していると考える．そこで，このユーザモデルと利用者の振る舞いを比較することによって，なりすましを見つけることが出来ると考える．システムがなりすましの可能性を見つけた場合，システムは利用者の認証を行う．我々は，この認証を行うためにHTTPの中継機能を実現した．HTTPの中継機能を用いて利用者の閲覧にシステムが割り込み認証のページを提示することができる．現在セキュリティシステムはユーザ監視エージェントとして，Servletを用いてWebサーバ上に実装されている．

キーワード　ユーザモデル，監視型セキュリティ，なりすまし，特徴ベクトル，HTTP中継，限定されたWeb

Watching Security System Using the User Model for Limited Web Site

KANENISHI, Kazuhide[*1]　TOGAWA, Satoshi[*2] and　YANO, Yoneo[*3]

[*1]Center for University Extention,
Tokushima University
1-1 MInamijyousanjima, Tokushima
+81 88 656 7285
mailto: marukin@is.tokushima-u.ac.jp

[*2]Education Center for Information Processing,
Shikoku University
123-1 Furukawa, Ohojin-cho, Tokushima
+81 88 656 1300
togawa@ishikoku-u.ac.jp

[*3]Faculty of Engineering,
Tokushima University
2-1 MInamijyousanjima, Tokushima
+81 88 656 7495
yano@is.tokushima-u.ac.jp

Abstract　The goal of this research is building of the security system targeting the Web site that limited user. Our system constructs each user's user model based on the usual browsing history. This user model expresses user's character. The system can discover the impersonation by comparing user's behavior with this user model. A system certifies the user when a system finds the capability of the impersonation. We achieved HTTP forwarding facility to certify him. The system interrupts for the user's browsing and a certification page can be displayed by using the HTTP forwarding facility. At present, a security system is implemented as an user watch agent that is used the servlet by the inside of the Web server.

key words　user model, watching security, intruder, feature vector, HTTP forwarding, limited Web site

1．はじめに

インターネットは我々の生活の隅々にまで入り込んでいる．インターネットなしの生活は考えられないといった状況が絵空事とは言えなく成りつつある．ネットワーク社会は，我々を距離と時間の制約から解き放ってくれた．しかし，その一方で多くの問題が顕在してきた．インターネット社会の問題の一つにセキュリティが挙げられる．

インターネットの黎明期において，利用者の殆どは研究者であり，さまざまな技術は性善説的な世界観の下で開発されてきた．しかし，急速的な普及を受けてもはやインターネットの利用者は世界中の一般的な人々であり，宗教，主義主張等は実に多様でありさまざまな背景を持った人々が日常生活の道具として使っている．最近ではインターネット上でのトラブル，犯罪，反社会的な行動等が顕在化しつつある．もはやインターネットはバラ色の未来を実現するものではなく，実世界同様さまざまな問題を孕んでいることが明らかになってきた．当然，我々はそうしたインターネット上での問題に対処していかなければならない．インターネット上でさまざまにやり取りされる情報について，その保護が大きな問題としてクローズアップされている．

そこで，我々はインターネット上でのセキュリティの問題を取り上げる．我々の取り上げるセキュリティは，Web サイトの運用，管理に関するものである．最近は膨大なWebサイトがインターネット上で開設され，何らかの商業行為を伴ったWebサイトはその数を増す一方である（無論，個人的な利用等のWebサイトのセキュリティ保護も重要なことは言うまでもない）．そこで，我々はある特定の用途の下，限定的に運用されているWebサイトのセキュリティ管理枠組みを提案する．そして，我々の提案に基づく試作システムを作製し，試作システムについて報告を行う．

膨大なWebサイトの種類は多岐にわたるが，その中には，限定的な Web サイトも多く存在する．つまり，初めから不特定多数の利用を目的としていないWebサイトである．例えば，大学における学生の個人的な教務情報等の運用システムの場合などである．あるいは，特定の情報を有料で公開するような Web サイト等が，限定的な利用のWebサイトの例としてあげることができる．一般にこのような限定的なWebサイトは，個人認証を伴うことが多い．Web の利用にあたってブラウザ上にログイン画面が表示され，個人ＩＤ（ユーザ名）とパスワードの入力が求められると言ったことが良く行われている．

限定的なWebサイトでは，正規の利用者によって閲覧が行われているかどうかが大きな問題となる．不正な利用者が，Web サイトの情報を閲覧することは大きな問題である．つまり，何らかの手段によって進入されることや，ユーザＩＤとパスワードが何らかの方法によって不正利用され誰かがなりすますことは大きな問題である．そこで，我々は，この成りすますに対して，ユーザモデルの利用に基づく，利用者保護の方法を提案する．

我々のセキュリティシステムでは，HTTP の中継機能を持ったユーザ監視エージェントをWebサーバ上に置き，ユーザの Web 閲覧状態を監視させる．ユーザ監視エージェントは，ユーザモデルとユーザの振る舞いを比較することによって，クラッカーのなりすましを判断する．ユーザ監視エージェントが進入と判断した場合，ユーザ監視エージェントはコネクションを切断するか，管理者に進入されたことを知らせる．

現在，Web 上でのユーザモデルの構築は議論が始まったばかりであり，まだ汎用の様式が確定したという状態ではない．幾つかのユーザモデルが提案されているが，ユーザモデルそれ自身についての提案だったり，特定のシステムと一体になったモデルであったりする．これらのモデルをすぐに我々の対象で利用することはできない．我々はユーザモデルへ統計的な数量モデルの導入を提案する．

本稿は，以下２章でユーザモデルに基づく限定 Web サイトのセキュリティモデルについて述べる．３章ではシステムの概要について延べる．４章で我々の提案するユーザモデルについて述べ，５章でユーザの検証のための HTTP 中継の方法について述べる．そして，最後に，６章では全体をまとめる．

2．ユーザモデルを用いたユーザ識別システ

ムのモデル

2．1　セキュリティのモデルについて

本節では，我々の提案するセキュリティモデルについて，従来セキュリティシステムと比較することによって位置付けを行う．

インターネット上のセキュリティの基本は，あるシステム（多くはサーバ類）をクラックから保護することにある．つまり，進入を防ぐ，入らせないということが基本になる．セキュリティは一種のフィルタリングとして捉えることが出来る．多くのファイヤーウォール，tcpwrapper や IP-filter 等のセキュリティシステムの多くが基本的にフィルターである．現在のセキュリティシステムを以下の様なタイプに分類する．

(1)フィルタタイプ
(2)情報保護（暗号技術）
(3)認証強化タイプ
(4)監視（追跡）タイプ
(5)保護タイプ
(6)補助ツール

認証の精度を高めるさまざまは方法が提案されている．インターネットサービスはユーザに対して開かれており，問題はユーザの認証を厳密に行うということである．完全なセキュリティがネットワークの切断であることは広くしられており，急所に一つが認証である．例えば，ユーザ ID とパスワードの管理の問題である．定期的なパスワードの変更や，ワンタイムパスワードシステム等が提案されている．そして，ワンタイムパスワードと言うアイディアは理想的であるが，実際の運用においては問題があり，このワンタイムパスワードの運用負担を減らすようなさまざまなシステムが提案されている．

一方，我々が提案しているのは，ユーザモデルに基づく保護である．我々の手法は，従来のセキュリティモデルに比べると，強力ではない．フィルター機能，情報の遮断を目的としているわけではないからである．堅牢ではない分，よりきめ細かい制御が可能であり，管理者の作業の軽減のためという面が強い．インターネット普及に伴い，管理者のスキルにも大きな開きが存在する．全ての管理者がソケットプログラミングに精通しているわけでなく，ルータのフィルタールールがマニュアル無しで書けるわけではない．そこで，我々のシステムは基本的にエージェントがユーザを監視し，ユーザモデルのメンテナンスも自動で行われるため，管理者の負担は少ないと言える．

2．2　ユーザモデルに基づくセキュリティの枠組み

我々の提案するシステムはユーザモデルの活用を基本としている．我々がここで述べるユーザモデルとは，個人手的のある特徴的な振る舞いを，何らかの表現を用いて表した情報のことである．ユーザモデルには，個人の特徴や性格といったものが表現される．我々が取り上げた，閲覧等の場合は，Web サイトを閲覧する場合の個人のクセが示されている，と考えられる．そこで，ユーザモデルが個人の振る舞いのと特徴を表現しているならば，それをセキュリティに利用することが可能なはずである．もし，パスワード情報が破られて，クラッカーがあるユーザになりすまして Web を閲覧しているとしたら，その場合の閲覧行動はそれまで蓄えられてきたユーザモデルと大きく異なると考えられる．この差異を取り出すことができれば，個人認証用情報として用いることができる．

そこで，我々は個人情報監視エージェントによるユーザモデルを用いたセキュリティを提案する．

我々が現在対象にしているのは，不特定多数ではなく，ある特定の利用者のための Web サイトにおけるサイトのセキュリティである．これは，不特定多数のサイトの場合，個人認証の必要性がなくユーザモデルの作成が困難であり，また，利用者の個人情報の保護という作業が存在しないからである．

ユーザ監視エージェントの機能として以下のようなものを挙げることができる．

・個人情報認証
・ユーザモデル管理
・ユーザ比較
・ユーザ検証
・コネクション切断・通達

ユーザ監視エージェントにおける個人認証は，必ずしも必須の機能ではない．限定利用が目的の Web サイトの場合，予め認証の機能は Web サーバが持っている

と考えられるからである．ユーザ監視エージェントは，利用者の閲覧行動を基にユーザモデルを更新する．ユーザモデルとして我々は，閲覧行動を定量的に表現するモデルを用いる．一方で，ユーザ監視エージェントは，ユーザモデルと振る舞いの比較も行う．進入者が他の利用者になりすましサイトを閲覧しているとするならば，その場合のユーザモデルは本来のユーザモデルと一致しない．そこで，ユーザモデルの比較を行う評価関数を用意し，閾値を越えたとき，誰かが利用者に成りすましていると判断する．成りすましを発見した場合，ユーザ監視エージェントは，利用者の検証を行う．検証は，疑わしい利用者に対して，ユーザ監視エージェントが確認の質問を行う．この場合の質問は，利用者の個人情報として登録されている各項目，住所，生年月日，電話番号等をシステム側から利用者に対して質問する．この確認に対する応答結果基に，成りすましを最終的に判断する．

そして，成りすましを断定した場合，コネクションを切る（ある IP アドレスからのアクセスを拒否する）とともに，診断の結果を管理者に知らせる．

3．限定Ｗｅｂサイトのセキュリティシステムの概要

3．1　システムの構成

本システムは，Web サーバとエージェントからなる．Web サーバはどのような Web サーバでもよい．ただし，現在ユーザ監視エージェントを Java で実装しているため，Servlet が使える環境が必要である．

ユーザ監視エージェントは，Web サーバと連動している．イメージ的には，通常の HTTP プロトコルに割り込む形を取る．つまり，通常ブラウザからある URL へのアクセスがあり，ブラウザは URL に該当する html ファイルや画像ファイル等を送信する．この送信の部分にユーザ監視エージェントが入り，ファイルの送出は Web サーバではなくユーザ監視エージェントが行う．

ユーザ監視エージェントは，HTTP フォワーディングモジュール，ユーザモデル更新モジュール，ユーザモデル比較モジュール，ユーザ検証モジュールからなる．

HTTP フォワーディングモジュールは，通常 Web サーバが行う HTTP の送出機能を Web サーバに変わって行う．この機能を用いて，なりすましが疑われる利用者に対して，検証の html ファイルを，利用者のブラウザに送出する．

ユーザモデル更新モジュールは，認証終了後，利用者の閲覧履歴を統計的な数量モデルに変換し，Web へのアクセスが行われている間ユーザモデルを更新する．

ユーザモデル比較モジュールは，ユーザモデルと当日のユーザの振る舞いを比較する評価関数を持ち，ユーザモデルと振る舞いを入力に評価関数の出力が，閾値を超えるかどうかを判定する．閾値を超えた場合は，なりすましの可能性高いということであり，次のユーザ検証モデルへその旨の情報を伝える．

ユーザ検証モデルは，現在閲覧中の利用者の個人情報を基に質問を作成し，質問を提示する．そして，利用者からの応答を比較し，個人情報を正しく答えることが出来ない場合，なりすましと判断する．その場合は，当該の利用者が使用している IP アドレスからのアクセスをフィルタリングし拒否する．また，なりすましが行われことを管理者へ伝える．

3．2　システムの動作

本節では，システムの振る舞いについて，利用者のアクセスに沿って述べる．利用者は，ブラウザ経由で Web サイトへアクセスする．この Web サイトは特定の利用者を前提としているため，アクセスの初期画面は個人認証画面となる．利用者は，自分のユーザ ID とパスワードを入力する．そして，通常の閲覧と同じようにその Web サイトを閲覧する．

このとき，Web サーバ側では，利用者毎にエージェントが起動し，閲覧につれてユーザモデルを更新していく．また，利用者の閲覧行動と直前までのユーザモデルが比較される．

もし，この利用者が何らかの方法で他人の ID とパスワードを入手して利用していた場合，システムはユーザモデルの比較から，異常を発見する．そして，システムはこの利用者に対する質問を作成し，これを提示する．利用者が Web サイトの中を次々に閲覧をしているとき，あるリンクを開いたところ表示されたのは

個人認証のページが表示される．そこでは，彼の自宅の電話番号や，生年月日の入力が求められる．彼は不思議に思いながらも，質問事項を入力する．

このとき，彼が侵入者でないとするならば，正しく個人情報を入力するだろうから，本来表示されていたURLが，個人認証のページに続いて表示される．以後，彼は何事もなかったかのように閲覧を続ける．彼が侵入者だった場合，システムは個人情報が正しく入力されていないことから，TCPのコネクションを切断し，管理者にメールでその旨を伝える．

4．ユーザモデルの管理

4．1　ユーザモデルの作成

Webサイトに構築されているhtmlファイルとハイパーリンクによる結合構造は，おのおのの html ファイルを節点，ハイパーリンクを枝と考えると有向グラフによる論理的な構造として表現できる．利用者が現在閲覧している html ファイルとは別の html ファイルをハイパーリンクを介して呼び出すことは，有向グラフによる論理構造に置き換えて考えると，ある節点から枝を介して別の節点へと移動していることに気づく．我々は，利用者が Web サイトを閲覧するという行動は有向グラフで表現される論理構造の節点間を遷移しているということに着目し，その状態遷移から取得できる以下の（1），（2）の情報を利用する．

（1）　節点間の平均遷移時間

節点Aから節点Bへの遷移を考えたとき，その遷移時間を得ることで利用者が節点Aをどれだけ閲覧していたかを知ることができる．これをすべての節点間の遷移に関して取得し，それぞれの平均を算出することにより利用者がどの html ファイルに興味を持って閲覧行動していたか知ることができる．

（2）　節点間の移動系列における生起確率

利用者の閲覧行動において，同様に節点Aから節点Bへの移動を考えたとき，この移動に関して節点Bへは節点Aから移動してきたという情報を得ることができる．

すべての移動系列において，各々の移動における前後の節点系列を2重マルコフ過程として節点間の生起確率を取得する．ここでn以上（n＞2）のn重マルコフ過程を選択しなかった理由は，n 重マルコフ過程を適用することにより生起確率を保存する配列が全節点数のn乗個必要となるため，計算量の増大を招くためである．

（1），（2）それぞれの情報から特徴ベクトルを生成する．（1）から生成されるベクトルを平均遷移時間ベクトル，（2）から生成されるベクトルを生起確率ベクトルとし，以下にそれぞれの生成法を示す．

平均遷移時間ベクトル

Webサイトが管理するすべてのhtmlファイル数をmとしたとき，サイト内で考えられるすべての移動パターンkはmの2乗で与えられる．すべての移動パターンkを要素数とする配列X_1を考え，配列の各要素には各移動における遷移時間の平均を格納する．

$$X_1=(x_1, x_2, x_3, \cdots, x_{k-1}, x_k)=(x'_{1,1}, x'_{1,2}, x'_{1,3}, \cdots, x'_{m,m})$$

ここで$x'_{a,b}$は，html ファイル A から html ファイル B への平均遷移時間を表す．

生起確率ベクトル

生起確率においても同様に，すべての生起確率パターン数kは全htmlファイル数mの2乗で与えられる．すべての生起確率パターン数kを要素数とする配列 X_2 を考え，配列の各要素には各移動系列における html ファイル間の生起確率を格納する．

$$Y_1=(y_1, y_2, y_3, \cdots, y_{k-1}, y_k)=(y'_{1,1}, y'_{1,2}, y'_{1,3}, \cdots, y'_{m,m})$$

ここで$y'_{a,b}$は，html ファイル A から html ファイル B への移動が生起する確率を表す．

次に平均遷移時間ベクトル，生起確率ベクトルとも以下の監査データと利用者データと呼ばれる2つのデータにそれぞれ集積する．

監査データ

本システムの運用開始時から集積されているデータ．監査対象となる登録された利用者ごとに存在する．後述する利用者データが蓄積されて更新される．

利用者データ

Web サイトの閲覧開始時に行われる利用者認証から利用の終了までを1セションとし，セションの開始時に生成されるデータ．セション中は利用者が html ファイルを閲覧する度にデータが逐次更新さ

れる．セション終了後データは破棄される．

4．2　判定

平均遷移時間ベクトルによる判定，生起確率ベクトルによる判定のどちらにおいても監査データを元にした特徴ベクトルと利用者データを元にした特徴ベクトルとの類似度を求めることにより判定する．

まず平均遷移時間ベクトルによる判定を考える．

監査データから生成される平均遷移時間ベクトルを X_1，利用者データを元に生成される平均遷移時間ベクトルを X_2 とし，それぞれ次のように定義する．

$$X_1 = (x_1, x_2, x_3, \cdots, x_i, \cdots, x_{k-1}, x_k) \quad (1)$$

$$X_2 = (x'_1, x'_2, x'_3, \cdots, x'_i, \cdots, x'_{k-1}, x'_k) \quad (2)$$

x_i：各移動における遷移時間の平均，k：サイト内で考えられるすべての移動パターン数

平均遷移時間ベクトル X_1 と X_2 の類似度 S_1 は次の式で与えられる．

$$S_1(X_1, X_2) = \frac{(X_1, X_2)}{\|X_1\|\|X_2\|} \quad (3)$$

ここで，

$$(X_1, X_2) = \sum_{i=1}^{k} x_i x'_i \quad (4)$$

$$\|X_1\| = \sqrt{\sum_{i=1}^{k} x_i^2}, \quad \|X_2\| = \sqrt{\sum_{i=1}^{k} x'^2_i} \quad (5)$$

一般に，式(3)などで示されるベクトル間の類似度は，$0 \leqq S(X_1,X_2) \leqq 1$ の範囲を取ることが知られており，また類似性が高いほど大きな値（1に近い値）を取ることが知られている．

このことから判定にはある閾値 T_1 を設定し，算出した類似度が閾値を越える場合には正当な利用者とし，閾値を越えない場合には不当な利用者とする．

$S_1(X_1,X_2) \geqq T_1$　：正当な利用者

$S_1(X_1,X_2) < T_1$　：不当な利用者

次に生起確率ベクトルによるを考える．

基本的に生起確率ベクトルによる判定も平均遷移時間ベクトルによる判定と同様に類似度を算出して判定する．

監査データから生成される生起確率ベクトルを Y_1，利用者データを元に生成される生起確率ベクトルを Y_2 とし，それぞれ次のように定義する．

$$Y_1 = (y_1, y_2, y_3, \cdots, y_i, \cdots, y_{k-1}, y_k) \quad (6)$$

$$Y_2 = (y'_1, y'_2, y'_3, \cdots, y'_i, \cdots, y'_{k-1}, y'_k) \quad (7)$$

y_i：各移動系列における html ファイル間の生起確率

k：サイト内で考えられるすべての html ファイル間移動パターン数

生起確率ベクトル Y_1 と Y_2 の類似度 S_2 は次の式で与えられる．

$$S_2(Y_1, Y_2) = \frac{(Y_1, Y_2)}{\|Y_1\|\|Y_2\|} \quad (8)$$

ここで，

$$(Y_1, Y_2) = \sum_{i=1}^{k} y_i y'_i \quad (9)$$

$$\|Y_1\| = \sqrt{\sum_{i=1}^{k} y_i^2}, \quad \|Y_2\| = \sqrt{\sum_{i=1}^{k} y'^2_i} \quad (10)$$

平均遷移時間ベクトルによる判定と同様に，ある閾値 T_2 を設定し，算出した類似度が閾値を越える場合には正当な利用者とし，閾値を越えない場合には不当な利用者とする．

$S_2(Y_1,Y_2) \geqq T_2$　：正当な利用者

$S_2(Y_1,Y_2) < T_2$　：不当な利用者

5．ＨＴＴＰ中継機能

最近，Web 上で利用者のインタラクションを可能とするさまざまな技術が提案されつつある．我々のセキュリティシステムでも，システムが異常に気付いた時点で利用者に個人認証を行うが，これは言ってみれば利用者の閲覧にシステムが割り込むようなものである．利用者が Web サーバにある URL を要求したにも関わらず，システムから送られてくるのは要求した URL とは全く異なった内容の html ファイル等が送られてくるからである．

我々はこの機能を実現するため，Java による HTTP フォワーディングモジュールをユーザ監視エージェントに実装した．我々のシステムでは，受信には Web サーバのポートが用いられるが，送信には HTTP フォワードのポートが使用される．PROXY サーバ等に実装されている HTTP フォワーディングは，単に転送する

だけであるが，我々の HTTP フォワーダはルールベースであり，ルールに基づいてファイルの配送を制御することができる．我々は HTTP の転送機能にルールを持たせることによって，Web サーバのインタラクションを実現する．つまり，通常は要求のあったファイルを送信するが，条件によっては要求されたファイルと異なったファイルを送信する（要求された URL と異なった URL への転送も含む），あるいはファイルの送信そのものを停止することができる．

一般に，CGI 等で Web のインタラクションは実現することができる．しかし，これはＡという URL の中でインタラクションを記述しておくことである．通常Ａという URL と，URL の示した html ファイルは完全に一致している．

一方，我々の提案する方法は，この URL と html のつながりをシステムが管理する．例えば，Web の作成者はＸ，Ｙ，Ｚという３種類の html ファイルをルールを作成しておく．すると，Ａという URL に対して Web サーバに要求があった場合，システムはルールにしたがって，Ｘ，Ｙ，Ｚの中からある一つの html ファイルを送信する．

これは，CGI 等による html ファウルの中に動的な振る舞いを記述する方法とは，異なるインタラクションの実現方法である．とくに我々が想定しているような，利用者の閲覧に割り込むような場合には，従来の CGI 等による手法では認証を実現することが困難である．また，Web 作成者にとっても Perl，Javascript や Java＋Servlet 等の高度なプログラミングの知識の必要なしに，通常の HTML の知識でインタラクションが実現出来ることから，負担が少ないと言える．Web 作成者は複数の html ファイルと条件を作ることから，旧来あったフレームベースのオーサリングシステムのイメージに近いと言える．無論，個々の html ファイル内に CGI を記述しておけば一層細かなインタラクションを実現することができる．

6．おわりに

本稿では，ユーザモデルを利用したセキュリティシステムについて述べた．我々は，大学が学生に教務情報を公開するような限定された利用での Web サイトを対象にしている．我々はシステムは，Web サイト上に ServletAPI を用いてユーザ監視エージェントとして実現している．我々のシステムは，利用者の閲覧履歴からユーザモデルを作成し，このユーザモデルを基に閲覧行動の差異を観察する．ユーザモデルは利用者の特徴を表現していると考えられることから，なりすまし利用者がいた場合，ユーザモデルと異なった振る舞いが得られる．これを利用してなりすましを発見する．

システムはなりすましの判断は，利用者の認証によって最終的に行う．そこで，利用者の閲覧途中に認証を行う必要があるため，我々はユーザ監視エージェントに HTTP 中継機能を実装した．我々の Web サイトではファイルの送信に HTTP 中継機能を用いて行う．そこで，URL の制御を柔軟に行うことが可能となる．利用者の閲覧の途中で，利用者の要求する URL とは異なった認証画面をブラウザに提示することが可能となる．

認証の結果によっては，システムが管理者になりすましのあることを知らせたり，TCP のコネクションを切断したりする．

今後の課題として，現在，プロトタイプシステムを用いて評価実験を行っている．差異の評価の部分等，実際の運用に基づいて，適切なパラメタを設定する必要があるからである．評価実験の結果によって，システムの改良を行う予定である．また，ユーザモデル自身，個人の特徴を明確に表現するよう改良を行う予定である．

参考文献

[1] 岡本忠士，白石善明，大家隆弘：“なりすましに対する不正侵入検知システム(IDS-M)，” 信学技報，OFS99-15，pp.39-46(1999)．

[2] 三浦信幸，高橋克巳，島健一：“適応型ＷＷＷにおけるユーザモデル構築法，” 情報処理学会論文誌，Vol.39，pp.1523-1535(1998)．

[3] 風間一洋，佐藤進也，清水奨，神林隆：“ＷＷＷのユーザ操作履歴によるＨＴＭＬ文書の相関関係の解析，” 情報処理学会論文誌，Vol.40，pp.2450-2459(1999)．

[4] 山口英監訳: "UNIX セキュリティ," アスキー出版, (原著: Simson Garfinkel and Gene Spafford, "UNIX Practical Security," O'Reilly and Associates, Inc., 1991.), 1992.
[5] 山口英, 鈴木裕信編: "bit 別冊 情報セキュリティ," 共立出版, 2000.
[6] 山口英監訳:"コンピュータセキュリティの基礎," (原著: Deborah Russell and G.T. Gangemi Sr., "Computer Security Basics," O'Reilly and Associates, Inc., 1991.), アスキー出版, 1994.
[7] 山口英:"ネットワークセキュリティ," 電子情報通信学会学会誌, Vol. 75, No. 7, pp. 755-758, 1992.
[8] 古川康一監訳:"エージェントアプローチ人工知能," 共立出版, 1997.