情報処理振興事業協会 電子政府情報セキュリティ技術開発事業 年次総括報告書

アクセス制御機構の機能不全を検出・検証するシステム

芝田幸彦[*1] 高山慎一[*1] Malyshev Dmitri[*1] 加藤努[*1]
木下信[*2] 蔀憲司[*3] 高木浩光[*4]

[*1] 株式会社ソフテック [*2] 有限会社キュート [*3] 株式会社 SRA
[*4]独立行政法人産業技術総合研究所

概要

政府は e-Japan 重点計画に基づいて行政手続の電子化を進めており、その多くは、Web ブラウザを活用し、インターネット経由でログインするシステムでサービスされると予想される。一方、民間では、インターネットバンキングやネットショップ、ネットオークション、Web メールなどで、既にそうしたシステムが多数実運用に供されている。こうして日常生活に深く関わるようになってきた Web システムには、堅牢なセキュリティが求められる。しかし、現実には、アクセス制御機構の機能不全が原因の欠陥を持つシステムが多数存在する実態が指摘されている [1], [2], [3]。こうした欠陥が存在した場合、ログイン状態を第三者が横取りする「セッションハイジャック攻撃」を許すこととなり、その結果、個人情報の漏洩や、偽の申請、注文を発行されるといった被害が発生する危険性がある。こうしたアクセス制御機構の欠陥をなくすには、システムの受注者が納品前に欠陥がないか確認し、また、システムの発注者が納品時の検収作業で欠陥がないかを調査する必要がある。従来、そうした確認作業は、セキュリティ監査を専門とする外部業者に委託し、十分な経験を積んだ専門技術者によって、手作業で行われてきた。サーバシステムの脆弱性を自動検査するシステムはいくつか商用化されているが、アクセス制御機構の欠陥を検査するシステムはこれまでに存在しなかった。本開発では、こうした作業を半自動化するため、ユーザが正規の手順でログインした際の通信内容を観察し、分析することで、アクセス制御機構の欠陥を検出、検証するシステムを設計、製作した。また、この検査システムの能力を確認するため、意図的にアクセス制御機構に欠陥を作りこんだ、評価用デモ Web サイトを製作した。

1. はじめに

電子政府における情報セキュリティ確保のためには、最新の情報セキュリティ技術を駆使し、情報セキュリティの計画策定から運用、脆弱性の分析・共有、セキュリティ侵害の予防や検知、迅速な侵害対処、原因分析等に至る総合的なコントロールを的確に実施する観点からの技術開発が求められている。こうした中で、セキュリティ管理支援技術として、脆弱性を容易に検査・検証できるような技術開発が急務となっている。

電子政府による申請届出手続き、調達などの行政手続きが実用期を向かえると、社会の電子取引行為は活発化するものと見られる。しかしながら、このような電子手続き等において中核となる Web サイトは、必ずしもセキュリティ的に安全な形で構築・運用されていないと言う現実がある。これは Web アプリケーションの脆弱性あるいは欠陥が存在していることが一因であり、その結果、成りすましアクセスによって個人情報が漏洩したり、偽の情報が提出されるなどの事故、事件がより増加する可能性がある。このような個人情報漏洩等の問題は社会的に重大な問題であり、こうした社会的リスクを極力軽減し、あるいは排除していくためには、セキュリティ脆弱性のない Web アプリケーションを構築する技術を確立することが急務で

ある。これは特に、電子政府における Web アプリケーションの安全性の監査・維持において、重要な位置づけとなる。

本プロジェクトでは、Web アプリケーションのセキュリティに関するソフトウェアの欠陥を開発時あるいは監査時に検査・検証するためのシステム開発を行った。本来、セッションレスである HTTP プロトコル を使用してのアプリケーションの作成では、何らかの手段でセッション管理を行う必要がある。ログイン機能を持つ Web アプリケーションでは、その認証情報がセッション情報と結び付けられるため、セッション管理の脆弱性は成りすまし、ハイジャック等を許すアクセス制御機能の脆弱性となる。開発する本システムは、検査対象となる Web アプリケーションと、Web ブラウザ間の、リクエストとレスポンスを監視・記録し、セッションを追跡して分析することによって、Web アプリケーションのアクセス制御機構の機能不全を検出する。こうした部類の欠陥を自動的に検知・検証するシステムはこれまでに存在しておらず、本開発により Web アプリケーションのセキュリティを容易に確保・維持・監査できる管理支援技術の提供が可能となる。

2. 研究開発の目標と内容

本開発では、ログイン機能を持つ Web アプリケーションを対象とし、そのアプリケーションのアクセス制御機構にセキュリティ上の脆弱性が潜在していないかを検知・検証するシステムの開発を目的としている。

本システムはプロキシサーバとして動作するシステムであり、利用者が自身の Web ブラウザから対象となる Web アプリケーションにシステムからの指示に従いアクセスを行った結果に対する通信内容の分析を行うことで、適切なアクセス制御が実現されているかの検知・検証を行うものである。

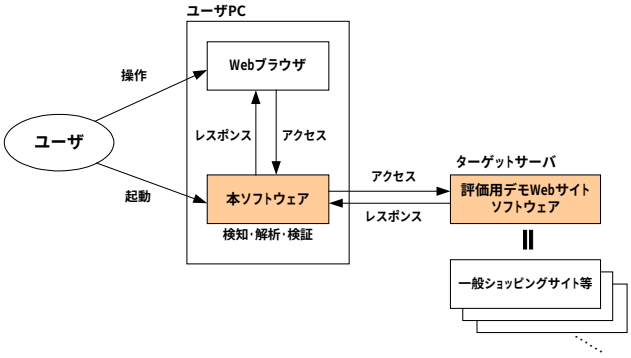

図 1 システム概要

以上の内容を実現するために以下の項目に重点をおき開発を行った。

2.1 通信記録機能

利用者が自身の Web ブラウザから Web サイト上の Web アプリケーションにアクセスを行う際に発生する通信内容を監視し、Web アプリケーションにおけるアクセス制御の機能不全の検出・検証を行うために必要となる、通信内容に含まれる個人情報に関連する送受信データの記録を行う機能の実装。

2.2 分析・検出機能

記録された個人情報に関連する送受信データを基に Web アプリケーションのアクセス制御機構における機能不全の分析、及び検出を行い、Web アプリケーションの脆弱性を把握することが可能な機能の開発。

2.3 検証機能

分析・検出機能で抽出された Web アプリケーションの機能不全内容について、抽出の際の個人情報に関連する送受信データの編集や一部欠落等により状況を変化させた上で再び Web アプリケーションにアクセスすることで得られる検出結果により、Web アプリケーションの機能不全に関する検証を行う機能の開発。

2.4 評価用デモ Web サイトシステムの開発

本システムの機能が正常動作するかの検証用途、及び Web アプリケーションの機能不全の

実際を一般ユーザに理解してもらうための啓蒙用途として、一般的なショッピングサイトの流れを模擬し、意図的に欠陥を作りこんだ Web アプリケーションの作成。

3. 本年度の活動状況

3.1 活動内容

開発目的に挙げた活動内容に対して実際に行った開発内容を、以下に示す。

- アクセス内容記録機能の開発
- アクセス制御機構の機能不全検出機能の開発
- レスポンス検査機能の開発
- GUI 機能の開発
- 評価用デモ Web サイトの開発

上記の開発作業において、「アクセス制御機構の機能不全を検出・検証システム」を実現するソフトウェアと、その機能検証、ならびに啓蒙作業のために必要な「評価用デモ Web サイトのソフトウェア」の作成を行った。

3.2 活動スケジュール

本年度の活動スケジュールを図 2 に示す。

項目	平成14年度			
	11月	12月	1月	2月
アクセス内容記録機能	◀	―	▶	
検出・検証機能	◀	―	―	▶
レスポンス検査機能		◀	―	▶
GUI 作成		◀	―	▶
デモサイト作成		◀	―	▶

図 2 活動スケジュール

3.3 用語の定義

本内容で使用する用語の定義を以下に記す。

「アクセス」
ユーザが Web ブラウザを通して Web サイトにリクエストを送信すると、Web サイトからレスポンスが返される。これを 1 アクセスと呼ぶ。

「セッション」
ユーザが Web サイトにアクセスする時に、一連のアクセスが同一ユーザからのものであることを Web サイトが検出し、ユーザ固有の処理を行う。この、特定ユーザからの一連のアクセスをセッションと呼ぶ。狭義には、Web サイトに対して Web インターフェイス上で「ログイン」を行ってから「ログアウト」を行うまでの一連のアクセスを指す。

「セッション追跡パラメタ(名)」
あるアクセスが特定ユーザからの継続したセッション中であることを識別するための情報。URL がユーザ固有のものであるならば、そのサイトにおいては URL がセッション追跡パラメタである。BASIC 認証を用いているサイトであれば、BASIC 認証に用いられる Authorization ヘッダがセッション追跡パラメタの一つである。

「セッション追跡パラメタ値」
セッション追跡パラメタの値である。理想的な Web サイトであれば、セッション追跡パラメタ値は第三者に知りえないランダム値であるべきであり、セッション維持という目的のみを達成する最低限の条件で考えた場合は、ユーザを特定する情報（例えばユーザ ID）である。

「ユーザ ID ベースのセッション追跡パラメタ」
セッション追跡パラメタ値がユーザ単位で固定となるような Web サイトにおける、セッション追跡パラメタ値の名称。セッション追跡パラメタ値の強度を示す文脈で用いられる。

「秘密情報ベースのセッション追跡パラメタ」
パスワードなどをセッション追跡パラメタ値に含む、セッション追跡パラメタの名称。盗まれた場合に秘密情報が復元される可能性がある。ユーザ ID ベースである場合とない場合が有り得る。

「セッション ID」
前記の理想的な「セッション追跡パラメタ値」をセッション ID と呼ぶ。一般にはセッション追跡パラメタ値自体をセッション ID と呼ぶこともあるが、ここでは明確に区別される。

「マーキング」
「記録」機能において、リクエスト毎に属性（name/value）の保持を行う。これらの何れかに何らかの属性を登録することをいう。

3.4 アクセス内容記録機能の開発

Web アプリケーションに対するアクセスを行う際に発生するアクセスデータの中から、アクセス制御機構の機能不全の検出・検証に必要なデータを記録するという観点から、以下の機能について開発を行った。

1) セッション内容記録機能

3.4.1 セッション内容記録機能

HTTP/HTTPS プロキシサーバ機能における中継データの記録機能と合わせて、本システムでは Web アプリケーションに対するアクセスを行う際に発生するアクセスデータを元にしたセッション追跡パラメタ値の解析を実現するために、アクセスの際のリクエストデータに対して分かり得る属性（name/value）のマーキングを行いながら、セッション追跡パラメタ値の解析が可能なデータ構造として記録する。

マーキングについては、Web アプリケーションに対するアクセスに以下のデータ内容が含まれている場合に行う。

- 個人情報を含む送受信データ
- パスワードを含む受信データ
- クレジット番号（全部あるいは一部）を含む受信データ

3.5 アクセス制御機構の機能不全検出機能の開発

記録された個人情報に関連する送受信データを基に Web アプリケーションのアクセス制御機構における機能不全の分析、及び検出を行うといった観点から、以下の機能について開発を行った。

1) セッション追跡パラメタ候補抽出機能
2) セッション追跡パラメタ候補検証機能
3) リクエスト単位でのセッション追跡パラメタ値検証機能
4) セッション追跡パラメタ値妥当性検証機能
5) サーバ側セッション破棄タイミング検出機能

3.5.1 セッション追跡パラメタ候補抽出機能

エントリリストに登録されたセッション追跡パラメタ候補に対して、以下に示すセッション追跡パラメタ方式の中から抽出を確度の高い候補から優先的に行う。

- URL
- Cookie
- hidden パラメタ
- BASIC 認証
- これらの複合方式

3.5.2 セッション追跡パラメタ候補検証機能

セッション追跡パラメタ候補抽出機能において抽出しきれなかったセッション追跡パラメタ候補について、そのパラメタ候補を削ったリクエストを Web アプリケーションに送信したことで得られるレスポンス結果を検証することによって、その削った候補がセッション追跡パラメタであったかの確認を行う。

3.5.3 リクエスト単位でのセッション追跡パラメタ値検証機能

セッション追跡パラメタを入力として、Web アプリケーションに対して連続してリクエストを行った結果として生成されるリクエスト単位でのセッション ID の妥当性の検証を行う。

セッション ID のランダム性を評価するためには、数百回レベルのリクエストを繰り返し、その結果を統計的に分析することが必要とされるが、今回の機能においては実用的なレベルを重視し、複数回リクエストを行った結果のセッション ID について検証を行い、その差分から推測されやすい内容であるかの検証を行う。

3.5.4 セッション追跡パラメタ値妥当性検証機能

セッション追跡パラメタ検出機能で検出されたパラメタに対して、以下の脆弱性のパターンについてチェックを行うことによりセッション追跡パラメタ値の妥当性について検証を行う。

- ログイン毎にセッション ID が変化しない場合
- ログイン毎にセッション ID が規則的に増加する場合
- 単純エンコーディングを利用している場合（Base64、Hex、Unicode 等）
- 単純な暗号を利用している場合(XOR 変換、シーザー暗号等)
- セッション情報に冗長性がなく微修正で他のアカウント情報を参照できる場合
- SSL だが secure フラグなしの Cookie を利用している場合
- 恒久的 Cookie を使っている、または寿命が長い場合

3.5.5 サーバ側セッション破棄タイミング検出機能

Web アプリケーションにおけるログアウト機能において、適切にセッション追跡パラメタ値を破棄しているかの検出を行う。

ログアウト機能がない、あるいはログアウトボタンはあるが、その処理内容は単にトップページへの移動やウィンドウを閉じるだけという場合を想定して、セッション追跡パラメタが正しく破棄されているかのチェックを行う。

3.6 レスポンス検査機能の開発

Web アプリケーションからのレスポンスデータの内容からのリンク情報や FORM 情報に関するデータに対する検証を行う観点から、以下の機能について開発を行った。

1) リンク／FORM 抽出機能
2) 抽出されたリンクの内容検証機能

3.6.1 リンク／FORM 抽出機能

Web サーバからのレスポンスデータの内容から、リンク情報や FORM 情報に関するデータの抽出を行う。セッション追跡に URL を使っているサイトへのアクセスの際のレスポンスから以下に示す項目に対する検出を行い、パラメタ及びどのページから抽出したかといった属性とともに収集を行う。

3.6.2 抽出されたリンクの内容検証機能

リンク情報や FORM 情報に関するデータ内容に対する内容検証を行う。本機能は、抽出・収集された抽出されたリンク／FORM 情報に対して parse 処理を行うことにより、以下に示す項目に対してセッション追跡パラメタとしての妥当性の検査を行う。

3.7 GUI 機能の開発

3.7.1 操作ガイド機能

本システムは、セッション追跡パラメタ値の検出・検証に必要な情報を取得するために、ユーザに対して Web サイト上でのブラウザ操作に関する操作ガイドをウィンドウ表示する。操作ガイドはその中でいくつかの目的を持ち、操作ガイド自身も複数存在する。

図 3 操作ガイド 画面内容

ユーザに対して操作ガイドが指示する操作内容は、その時点においてセッション追跡パラメタ値の検出・検証に必要となる情報が取得できているかに応じて変化する。

3.7.2 検査コース選択機能

ユーザが実施したい検査レベルに応じて、検査コースをいくつか設定する。検査コースは Web ブラウザ経由でサイトにアクセスする回数が変化することで記録するアクセスデータの情報量が変化するため、検出内容の確度に違いが現れる。

図 4 検査コース選択 画面内容

検査コースには以下の 3 種類を設定している。

- コース 1（簡易コース）
  ログインからログアウトまでの 1 サイクルの操作を記録する。

- コース 2（標準コース）
  コース 1 と同一アカウントで、ログインからログアウトまでの 1 サイクルの操作を再度行う。二回のセッションでのセッション追跡パラメタ値を比較する。

- コース 3（詳細コース）
  コース 2 までの操作に加え、別アカウントを取得して、そのアカウントでのログインからログアウトまでのサイクルの操作も記録する。異なるアカウントでのセッション追跡パラメタ値を比較する。

3.7.3 検査進捗状況表示機能

検査の進捗状況情報をユーザに対して視覚的に提供する。進捗状況表示はウィンドウ内において検査フェーズ単位で色づけされていき、コース内における現在の進捗状況を把握することが可能である。

図 5 検査進捗状況表示 画面内容

3.7.4 検査結果表示機能

セッション追跡パラメタ値の検査・検出を実施した分析結果の表示を行う。ここでは、Web サイトに関する情報、分析結果の内容、およびセッション追跡パラメタ値に関する検出内容についての表示を行う。また、セッション追跡パラメタ値が特定ユーザについて変動する場合には、その内容データについてリスト表示を行う。

図 6 検査結果表示 画面内容

3.7.5 証明書管理機能

ルート証明書、信頼する証明証に対する一覧表示、追加、及び削除を行う。

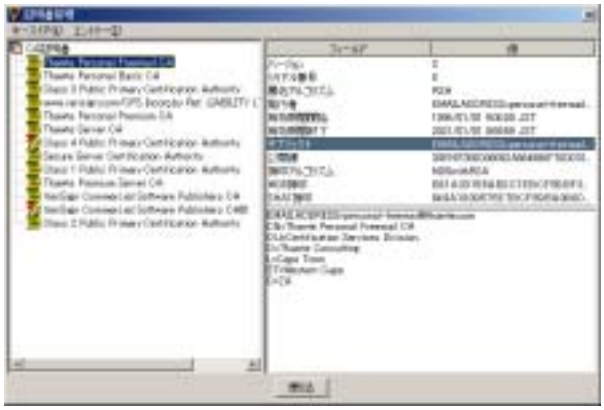

図 7 証明書管理 画面内容

CRL（証明書失効リスト）については、現時点においてブラウザでのサポート状況も十分ではなく、本システムのターゲットが一般ユーザを対象にしていないところからも、今回は無保証警告を明記することで対応する。

3.7.6 システム設定機能

本システムにおける設定画面は、システム全体に関する設定を行う「全域設定」画面とユーザに関する個人情報の入力を行う「個人情報設定」画面から構成される。

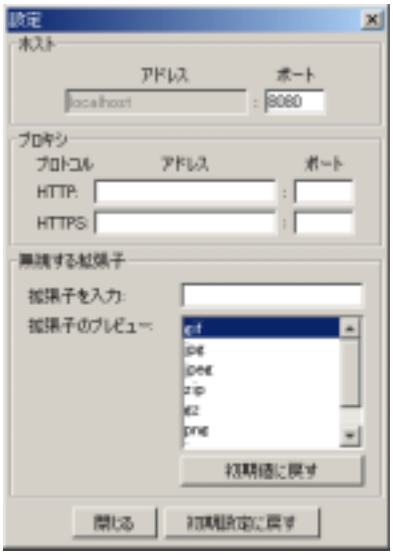

図 8 システム設定「全域設定」 画面内容

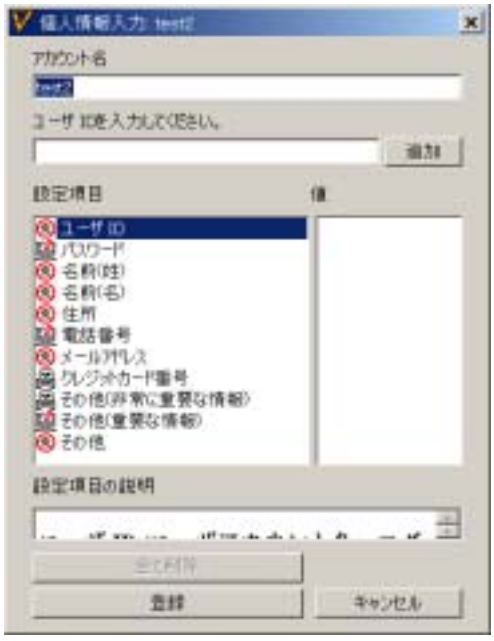

図 9 システム設定「個人情報設定」 画面内容

3.8 評価用デモ Web サイトの開発

本プロジェクトで開発する Web アプリケーションにおけるアクセス制御機構の機能不全に関する検出・検証機能の正常動作確認用途、及び Web サイトの機能不全の実際をユーザに理解してもらうための啓蒙用途として、一般的なショッピングサイトの流れを模擬した Web アプリケーションの開発を行った。

3.8.1 デモサイト利用者管理機能

Web アプリケーションの脆弱性を有した模擬的な電子商取引のデモサイトを一般に公開し、実際に本システムを体験してもらうことを想定し、デモサイトを利用する一般ユーザを管理するための機能。

3.8.2 擬似ユーザ登録・管理機能

今回開発する実験用模擬電子商取引システムは、ショッピングサイトを模擬している。この Web アプリケーション内の擬似的な顧客管理のための、PostgreSQL データベースを用いた、ユーザ（顧客）管理機能を持つ。プロトタイプでは購入履歴商品をデータベースに保持していなかったが、これに伴い実際のショッピングサイトと同様にデータベースに保持するように改良した。

3.8.3 デモサイトの SSL 対応

デモサイトの SSL 対応を想定して、その機能の実装を行った。本案件では、デモサイト用に正式なドメイン取得等を行わないため、サーバ証明書の取得は行わず自己署名証明書を使用している。ここでの実装範囲は、localhost のサーバ証明書で可能な機能までとしている。

3.8.4 Web アプリケーションの欠陥パターンの実装

以下の欠陥パターンを有するデモソフトウェアを実装した。

- 偽の Cookie 送信による任意ユーザへの成りすましの問題を模擬するための、秘密情報を含まない Cookie に頼ったアクセス制御方式の脆弱性を有する Web アプリケーションの実装。

- Cookie の漏洩によりセッションハイジャック攻撃される危険性の問題を模擬するための、クロスサイトスクリプティングの脆弱性を有する Web アプリケーションの実装。

- REFERER 情報取得による脆弱フリーメールサイトの乗っ取り問題等で露呈したもの

を模擬するための、Cookie を使用せず URL に埋め込む ID に頼ったセッション管理方式の脆弱性を有する Web アプリケーションの実装。

- Cookie のセキュアフラグを利用していない場合、すなわち SSL を利用しない環境での Cookie 利用時における情報漏洩等の危険性の問題を模擬するための、暗号化されないセッション ID の脆弱性を有する Web アプリケーションの実装。

- セッション ID が URL に表示されない場合における情報漏洩等の危険性の問題を模擬するための、アクションに POST メソッドが使用されている場合の脆弱性を有する Web アプリケーションの実装。

4. 成果物

本年度の IPA に対する納入物件を以下に示す。

- 開発成果報告書　1 部
- 品質管理報告書　1 部
- ソースプログラム　1 式
- ロードモジュール　1 式

5. 今後の課題

今回のプロジェクトにおいては、Web アプリケーションのアクセス制御機構における機能不全の検出・検証の実現化に重点をおき、開発作業を行ったため、今後検討を行わなければならない課題が残っている。主な課題として、以下の項目が挙げられる。

1) 成果物の普及
2) 成果物の実用化

以下に詳細を示す。

5.1 成果物の普及

本プロジェクトでは、本体ソフトウェアである「アクセス制御機構の機能不全を検出・検証するシステム」だけではなく、テスト評価用デモサイトのソフトウェアである「アクセス制御機能検査実験用模擬電子商取引システム」も開発した。後者は、セキュリティ脆弱性を有した Web サイトを一般に公開し、利用者に実体験してもらうことにより、アクセス制御機構の欠陥の危険性を認識してもらうことを目的としている。このような啓蒙活動を通して、本開発成果を普及させる方向で考えている。成果を普及させるためには、「広報・啓蒙活動」のアプローチと「セキュリティビジネス市場」へのアプローチの二つを考慮しなければならないと考える。

5.1.1 広報・啓蒙活動のアプローチ

「広報・啓蒙活動」に関しては、ソフテックと産業技術総合研究所が産学協調体制をとり、広報・啓蒙を行う。具体的には、産業技術総合研究所の高木チーム長を主体として、「アクセス制御機能検査実験用模擬電子商取引システム」を使ってデモサイトを構築し、一般利用者の使用を促すと共に、社会への啓蒙と発言を積極的に行う。またソフテック側では、ソフテック独自で行っているセキュリティ情報提供サービス（SIDfm）の情報サイト（`https://sid.softek.co.jp/`）上で、啓蒙のためのページを作成し、産業技術総合研究所とのクロスリンクを実現する。これにより広報に関する相互補完が可能となる。

5.1.1 セキュリティビジネス市場へのアプローチ

「セキュリティビジネス市場」に対しては、そこに存在する販売チャネルを利用した普及活動とその宣伝広報活動に組み入れることを目標に今後検討を行うことで、ビジネス市場への積極的なアプローチを計る予定である。

また、これと合わせて今回の成果を継続的に普及させていくためには、新たなアクセス制御機構の欠陥に関する機能を本システムに反映していくことが必要になるので、これを実現するための体制について現在検討中である。

5.2 成果物の実用化

本プロジェクトの成果によるシステムは、その検査手法が全自動ではなく、使いこなすにはある程度の技術的な知識を必要とするため、万人に利用できるものではない。実用化においては、技術的な知識を有する者だけではなく、一般消費者用途も意識した開発が必要となる。具体的には、より細かな操作支援機能、詳細情報表示機能、ヘルプ機能、操作動線を意識した GUI 開発等を再構成、そしてパッケージング等の作業が想定される。

6. まとめ

行政や民間のインターネット向けサービスで使用される Web アプリケーションについて、そのセキュリティ上の欠陥を検出、検証するソフトウェアの開発を行った。従来より、Web サーバの脆弱性や CGI プログラムの既知の脆弱性を検査するソフトウェアは商用化されていたが、ログイン機能を持つ Web アプリケーションのアクセス制御機構の欠陥を自動的に検査するソフトウェアはこれまでに存在しておらず、本開発はそれを実現したものである。電子政府の安全性を確保するため経済産業省が、「情報セキュリティ監査制度」を推進しているが、そのセキュリティ監査においても、本ソフトウェアが有効に活用されるものと期待している。

7. 参考文献

[1] 高木 浩光, 関口 智嗣, 大蒔 和仁, クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策, 情報処理学会, コンピュータセキュリティシンポジウム CSS2001 (2001).

[2] 産業技術総合研究所グリッド研究センター, Cookie を使用せず URL に埋め込む ID に頼ったセッション管理方式の脆弱性(1) － REFERER 情報取得による脆弱フリーメールサイトの乗っ取り問題, http://securit.etl.go.jp/SecurIT/advisory/webmail-1/ (2000).

[3] 産業技術総合研究所グリッド研究センター, 秘密情報を含まない COOKIE に頼ったアクセス制御方式の脆弱性 － 偽COOKIE送信による任意ユーザへの成りすましの問題, http://securit.etl.go.jp/SecurIT/advisory/rawcookie/ (2002).