特集論文

ハイブリッドセキュリティ診断技術

河内清人*
藤井誠司*

Hybrid Security Assessment Technology

Kiyoto Kawauchi, Seiji Fujii

要　旨

近年，相次ぐWebアプリケーションからの情報漏えい事件を受け，Webアプリケーションの脆弱(ぜいじゃく)性を検査するWebアプリケーションセキュリティ診断サービスの重要性が広く認識されている。診断サービスを効率化する上で，サイト内で自動到達可能な範囲(診断可能範囲)の拡大，及び診断項目の一層の充実が求められている。

この課題を解決するために，三菱電機ではWebアプリケーションの静的解析と動的解析を組み合わせたハイブリッドセキュリティ診断技術の研究開発に取り組んでいる。この技術の特長は次のとおりである。

(1)　Webアプリケーションを漏れなく診断

Webアプリケーションを静的解析し，ページ抽出と各ページへの到達経路決定を行うページ間依存性解析で，従来技術では到達できなかったページも診断可能

(2)　業界標準の診断項目(OWASP Top 10)を自動診断

診断データ入力時と正常データ入力時との応答の類似性から脆弱性有無を判定するページ類似性判定によって，従来自動診断が困難であった項目を自動化することで実現

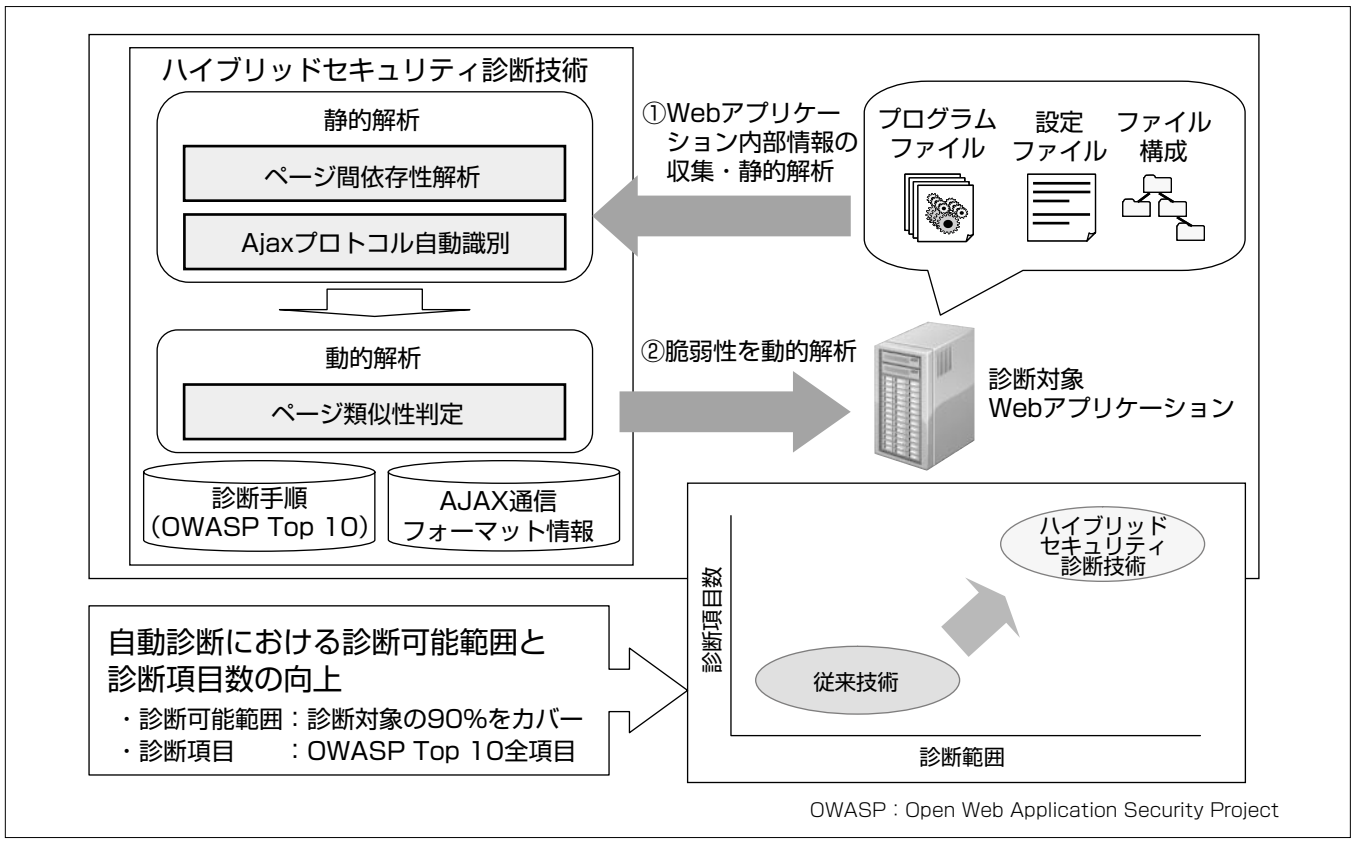
(3)　Ajax(Asynchronous JavaScript＋XML)(注1)への対応

Webアプリケーション内の情報からAjaxプロトコルを自動識別し，Ajaxに対する自動診断を実現

本稿ではまずハイブリッドセキュリティ診断技術について述べ，次に，SaaS(Software as a Service)型(注2)Webアプリケーションセキュリティ診断サービスへこの技術を適用した場合の実現形態について述べる。

(注1)　ブラウザ上のJavaScriptとWebアプリケーションが非同期に通信を行い，ページを動的に更新する技術。なお，JavaScriptは，Sun Microsystems, Inc. の登録商標

(注2)　ソフトウェア機能をサービスとして提供する形態



ハイブリッドセキュリティ診断技術の概念図

ハイブリッドセキュリティ診断技術は，Webアプリケーションの静的解析と動的な診断を組み合わせることで，診断範囲と診断項目数を向上させる。ページ間依存性解析は，Webアプリケーション内の各ページへの正しい到達経路を決定する。Ajaxプロトコル自動識別は，使用されているAjaxに対応した診断メッセージを生成する。ページ類似性判定は，従来脆弱性有無の自動判定が困難であった診断項目の自動化を可能にし，OWASP Top10全項目の診断を実現する。

*情報技術総合研究所

1. まえがき

今や，企業がインターネット上にWebアプリケーションの動作するWebサイトを公開し，顧客に対して様々なサービスを提供する形態が当たり前になってきている。顧客の個人情報など機密性の高い情報も大量に扱うようになるにつれ，Webアプリケーションは不正アクセスの格好の標的となり，昨今Webアプリケーションの弱点(脆弱性)を悪用した情報漏えい事件が相次いでいる。

そのため，インターネットに公開するWebアプリケーションに脆弱性が含まれていないか検査を行うWebアプリケーションセキュリティ診断を実施することは今や不可欠であり，三菱電機情報ネットワーク㈱(MIND)をはじめ，各社から同診断サービスが提供されている[(1)]。

Webアプリケーションセキュリティ診断を実施する上で，自動診断ツールによる効率化は不可欠である。そのため，自動診断技術には診断可能範囲の拡大，及び診断項目の一層の充実が求められている。

当社では，Webアプリケーションセキュリティ自動診断における診断範囲の拡大と診断項目の拡充を目指し，ハイブリッドセキュリティ診断技術の開発を行っている。

2. ハイブリッドセキュリティ診断技術

Webアプリケーションセキュリティ診断サービスで用いられる診断ツールは，Webアプリケーションを実際に動作させることで脆弱性の有無を診断する動的な診断方式が一般的である[(2)]。

診断ツールは，攻撃を模擬した異常なリクエストをWebアプリケーションに入力し，それに対するWebアプリケーションの応答を観測することで，脆弱性が含まれているかどうかを検査する。

それに対し，ハイブリッドセキュリティ診断技術は，Webアプリケーションの静的解析と動的な診断のハイブリッドであり，これによって次の特長を実現する。

(1) Webアプリケーションを静的解析し，Webアプリケーション上の全ページを抽出後，さらに各ページへの到達経路決定を行うページ間依存性解析で，従来技術では到達できなかったページも診断可能

(2) 異常なリクエスト送信時の応答と，正常なリクエスト送信時の応答に含まれるページ類似性に基づいた脆弱性判定技術によって，業界標準の診断項目(OWASP Top10 [(3)])のうち，誤検知の可能性が高く，従来専門家による手動診断で実施していた項目を自動化

(3) Webアプリケーション内部の情報からAjaxフレームワークを自動認識し，各フレームワーク固有の通信プロトコルに準拠した診断メッセージを生成することで，Ajaxによって呼び出されるWebアプリケーション機能への診断を実現

2.1 ページ間依存性解析による診断可能範囲拡大

従来の診断ツールは，Webアプリケーション全体を診断するため，ページ内のリンクやフォームを辿(たど)り，Webサイトを巡回して診断対象ページの探索を行う。

しかし，ページ間の依存関係によって，巡回時に表示されないページが診断対象から漏れるという課題があり，Webアプリケーションを網羅的に巡回することはできていない。

例えば，**図1**に示すようなショッピングサイトを考える。このWebアプリケーションでは，“カートに追加”操作を行っていない限り，“決済”ページで決済用フォームが表示されない。ツールがカートに商品を追加する前に決済ページを巡回すると，ツールはそのようなフォームが存在することを認識できず，診断対象から漏れてしまう。

つまり，Webアプリケーション内のページをすべて診断するためには，ページ間のリンクで表される依存関係以外の隠れた依存関係を見つけなければならない。従来のように，Webページ上に現れる情報だけを用いてこの隠れた依存関係を特定することは困難であった。

ハイブリッドセキュリティ診断技術では，Webアプリケーション内部のプログラムファイルや設定ファイルを静的に解析することで，各ページ間の隠された依存関係を特定するページ間依存性解析によってこの課題を解決する。既存ツールを用いた評価結果からこの課題を解決することで，診断対象の90%程度まで診断可能範囲を拡大できると考えられる。

ページ間依存性解析は**図2**のように行われる。まず，Webアプリケーションが格納されているディレクトリの構成や，設定ファイルの情報から，Webアプリケーションとして用意しているページの一覧を取得する。次に，各ページを処理するプログラムファイル内の実行コードを解析し，セッション変数などプログラムファイル間で共有されるデータの設定・参照関係を調査することで，ページ間の依存関係を明らかにし，依存関係を満たすよう各ページへの到達経路を決定する。

これらの処理によって，ページ間に張られたリンク以外

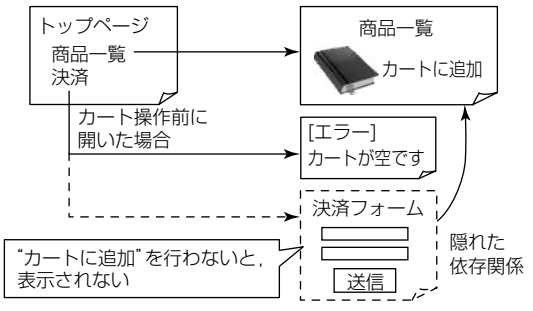


図1．隠れた依存関係が存在するサイトの例

の隠れた依存関係を明らかにでき，Webアプリケーション内のページを漏れなく診断することが可能となる。

2.2 診断前後のページ類似性に基づいた脆弱性判定

セッション管理の不備など，OWASP Top 10の診断項目の中には，異常な入力を与えたあとのWebアプリケーションからの応答がエラー画面かどうか判定しなければならないものがある。

従来は“エラー”などのキーワードが応答HTML(HyperText Markup Language)に含まれているか確認したり，レスポンスのステータスコードがWebアプリケーション内でのエラー発生を示しているか確認したりする手法がとられてきた。

しかし，Webアプリケーションが常にこれらの条件に一致するエラー応答を返すとは限らず，脆弱性有無の判断を誤る場合があり，診断結果を専門家が確認する必要があった。

この課題を解決するため，エラー発生時に表示される画面が正常にアクセスした場合と大きく異なるという特徴に着目し，異常な入力を与えた際の応答ページと，正常にアクセスした場合の応答ページの類似性を測定することでエラーかどうかを判定する方式を開発した。

ページ類似性の判定は，**図3**のように行われる。まず，比較対象となる二つの応答ページに対し，正規化処理が行われる。正規化とは，各ページに対して一種の整形を行う処理であり，判定精度を向上させることが目的である。

整形後のページは，テキスト比較によってそれらの差分が求められる。差分の大きさが閾値(しきいち)を超えた場合に，類似性が失われた，すなわちエラーが発生したとみなす。

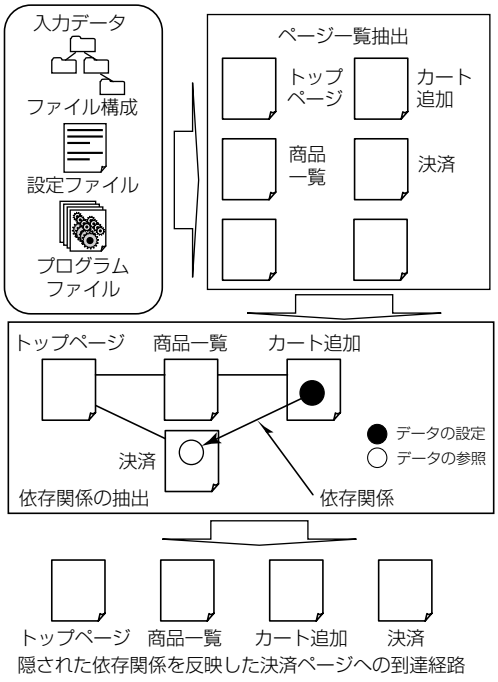


図2．ページ間依存性解析処理

2.3 Ajaxプロトコル自動識別

近年Webページの見映えや操作性を向上させるため，Ajaxと呼ばれる技術が急速に普及してきている。Ajaxは，ブラウザ上のJavaScriptとWebアプリケーションが非同期に通信を行い，表示されているWebページを動的に更新する技術である。

Ajaxでは，JavaScriptとWebアプリケーション間は自由なプロトコルでデータを送受信することが可能である。したがって，Ajax通信で呼び出されるWebアプリケーションの機能を診断するためには，サイトごとに異なるAjaxのプロトコルに準拠した診断メッセージを生成できなければならない。

この課題を解決するため，**図4**にあるように，診断対象Webアプリケーション内部で使用されているライブラリ名や設定ファイルの内容からAjaxフレームワークを特定し，その情報に基づいてAjax通信に対する診断メッセージを自動生成する技術を開発した。

3. SaaS型Webアプリケーション セキュリティ診断サービスへの適用

従来の診断サービスは，専門的な技術者がツールを駆使して行うのが一般的であった。そのため，高額なサービスとならざるを得ず，セキュリティ予算が潤沢ではない利用者は，Webアプリケーションのごく一部分のページだけしか診断を受けることができなかった。

そこで近年，診断プログラムによる自動診断のみを提供するSaaS型のWebアプリケーションセキュリティ診断サ

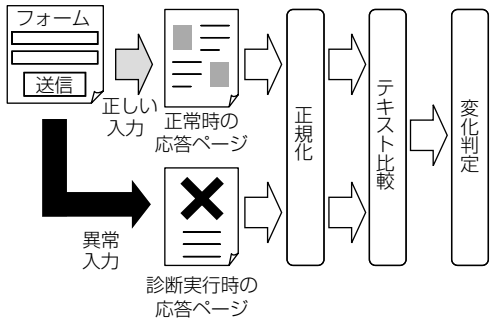


図3．ページ類似性判定

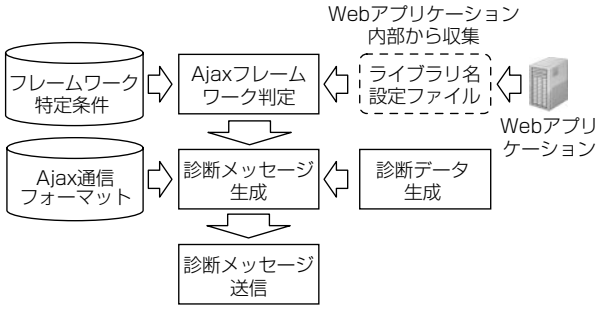


図4．Ajaxプロトコル自動識別

ービスが登場し，脚光を浴びている。このサービスは，診断にかかる人手を徹底的に排除することで，サイト全体を安価に診断できることを特長としている。

ハイブリッドセキュリティ診断技術をSaaS型Webアプリケーションセキュリティ診断に適用することで，既存サービスよりも診断項目数や診断対象サイトの診断範囲に優れた診断サービスを提供することが可能となる。ハイブリッドセキュリティ診断技術をSaaS型Webアプリケーションセキュリティ診断サービスに適用した場合のシステムイメージを**図5**に示す。

この診断サービスの流れは次のようになる。

(1) 診断サービスを希望するユーザー(Webサイト管理者)は，サービスプロバイダの提供するWebポータルにアクセスし，診断の申込みを行う。申込み完了後，Webポータルから構成情報収集プログラムをダウンロードし，診断対象のWebサーバ上で実行する(**図5**①，②)。

(2) 構成情報収集プログラムは，Webサーバ内で動作し，**2．1節**及び**2．3節**で述べた処理に必要な情報を収集する。収集した結果は，構成情報ファイルとして出力される。

(3) Webサイト管理者は出力された構成情報ファイルを回収し，必要ならば内容を確認後，ユーザーの使用しているパソコンから，Webポータルにファイルをアップロードする（**図5**③，④)。

(4) Webポータルにアップロードされた構成情報ファイルは，ハイブリッドセキュリティ診断サーバに入力され，解析が行われる。ハイブリッドセキュリティ診断サーバは解析の結果得られた情報に基づいて診断を実施する(**図5**⑤)。

なお，構成情報収集プログラムが直接ファイルを診断サーバにアップロードせず，このように，ユーザーが構成情報ファイルを回収し，ユーザーにファイルをアップロードさせる手順をとったのは，次の理由による。

①Webサーバの動作しているDMZ(DeMilitarized Zone)とインターネットとを分離するファイアウォールでは，通常Webサーバから外部への接続は許可していない。

②ユーザーに診断サーバにアップロードされる情報に機密情報が含まれていないことを確認する機会を与える。

4. むすび

本稿では，Webアプリケーションセキュリティ診断の自動化における診断可能範囲の拡大，及び診断項目の一層の充実を目指したハイブリッドセキュリティ診断技術について述べ，近年注目されているSaaS型Webアプリケーションセキュリティ診断サービスへの応用について述べた。

この技術はWebアプリケーションセキュリティ診断への適用を目指して開発を進めてきたが，その要素技術はWebアプリケーションのシステムテストにも適用可能と考えられる。今後はこれらの分野も視野に入れ，引き続き技術開発を進めていく予定である。

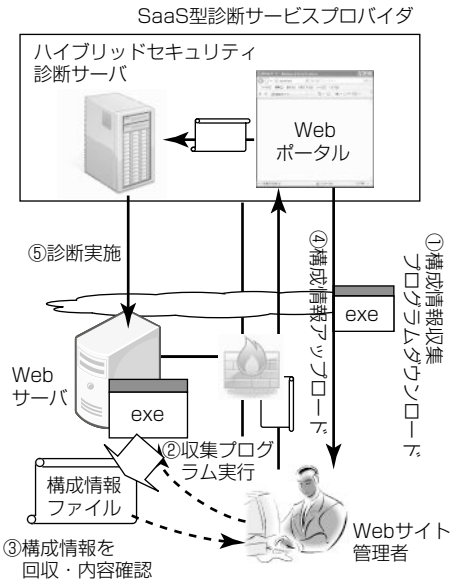


**図5．SaaS型Webアプリケーション
セキュリティ診断サービスへの適用**

参考文献

(1) 三菱電機情報ネットワーク：“Webアプリケーションセキュリティ診断サービス”
http://www.mind.co.jp/service/security/managed/application.html

(2) 河内清人，ほか：統合セキュリティ診断ツールに対するWeb診断機能の拡張，第66回情報処理学会全国大会（2004）

(3) Open Web Application Security Project(OWASP)：OWASP Top Ten Project
http://www.owasp.org/index.php/Category：OWASP_Top_Ten_Project

(4) Hoffman，B.，ほか： Ajaxセキュリティ，ISBN978-4-8399-2842-1（2008）