INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

SQL インジェクション検出ツール「iLogScanner V2.0」の開発

～ウェブサーバのアクセスログを解析して脆弱性を狙った攻撃の検出を簡易に行うツール～

株式会社ラック
佐久間　吉則、遠藤　哲生、
井上　真理英、鮭名　泰孝

概要

近年、ウェブサイトを狙った攻撃は、ウェブアプリケーションの脆弱性を突く攻撃に変化してきており、一般のウェブサイト管理者は、脆弱性対策を行う動機付けとして、自社運営のウェブサイトがどれほどの脅威を受けているかを確認する必要がある。

独立行政法人 情報処理推進機構（IPA）では、ウェブアプリケーションが受けている攻撃について、ウェブサイト管理者が容易に状況を把握できる手段として、ウェブサイトへのアクセスログを解析し、攻撃の有無を確認することができるツールを「iLogScanner」を 2008 年 4 月 18 日より公開している。

今回の開発では、「iLogScanner」でより多くの脆弱性の検出を可能とするため、検出対象となる脆弱性の種類を増やし検出機能を強化した。また、ツールの適用拡大に向けてツールの動作するプラットフォームを拡張した。

1.　背景

近年ウェブサイトを狙った攻撃は、OS などの製品ソフトウェアの脆弱性を突く攻撃から、ウェブアプリケーションの脆弱性を突く攻撃に変化してきている。

一般のウェブサイト管理者は、そうした攻撃の対策を行うため、自社運営のウェブサイトがどれほどの脅威を受けているのか、状況を確認する必要がある。また、状況確認だけではなく、インターネットに公開しているウェブサイトの危険性を認知してもらうことで、ウェブサイト管理者や経営者に対して警告を発し、対策を講じるきっかけとなる事も期待される。

2.　目的

ウェブアプリケーションに対してどれほどの攻撃を受けているのか、ウェブサイト管理者が容易に状況を把握できる手段を提供していく必要がある。そこで、ウェブサイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認でき、一部の痕跡に関してはその攻撃が成功した可能性を確認できるツールを開発する。

3.　開発報告

(1)　システム概要

本プロジェクトでは、ウェブサイト脆弱性のログ解析型簡易検査ツール（以下、「当ツール」という）として、利用者環境上でウェブサイトのアクセスログを解析し、ウ

ェブアプリケーションへの攻撃の有無を利用者へレポートするツールを開発した。利用者の環境でツールを実行することで、利用者のウェブサイトのアクセスログを外部に送信せずに解析を行うことが可能である。

システム概念図を図 1 に示す。

利用者は解析を希望するウェブサイトのアクセスログファイルを用意し、ウェブブラウザから検査ツール提供用のウェブページ(HTML)へ接続する（図 1-①,②)。 検査ツールは独立行政法人 情報処理推進機構（以下 IPA と記す）のウェブサイトに配置し、利用者のウェブブラウザからの要求に従い利用者環境へダウンロードして実行する形態である（図 1-③)。 検査ツールは利用者が指定したアクセスログファイルを解析対象として解析処理を実行し、解析結果を印刷可能な形態で提供する（図 1-④,⑤)。

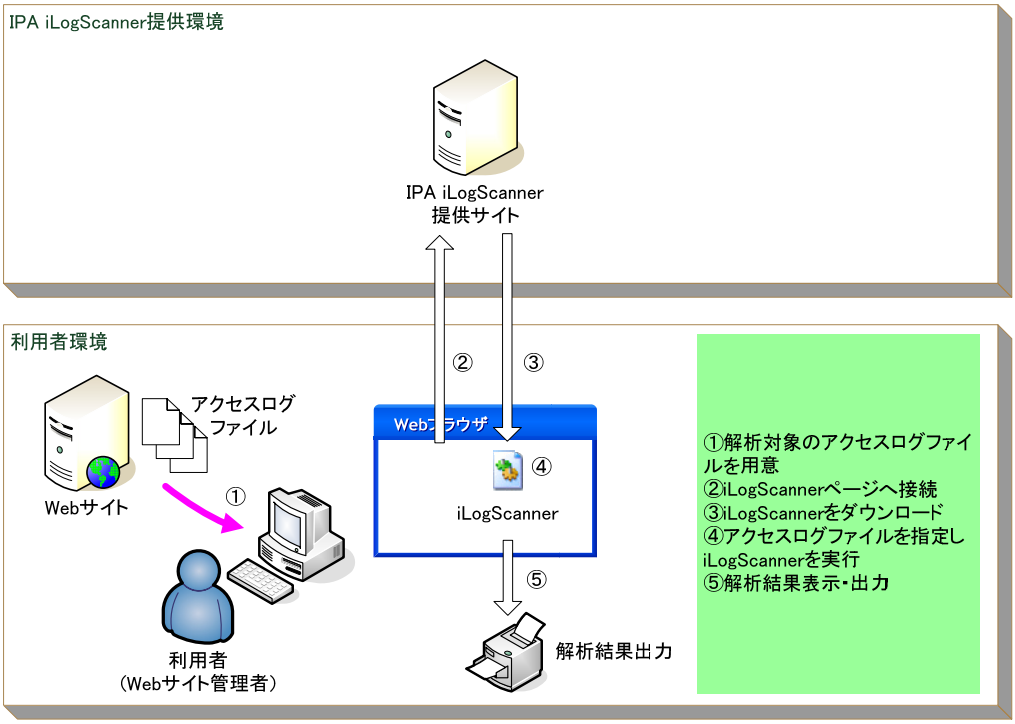

図 1. システム概念図

(2) 機能構成

当ツールが実行可能な動作環境を表 1 に示す。

表 1. 実行可能な動作環境

OS：	Microsoft Windows XP Professional SP2、SP3
ウェブブラウザ：	Internet Explorer 7.0
JRE：	Sun Java Runtime Environment 5.0 以上（JRE 5.0 系を推奨）

当ツールの機能構成を図 2 に示す。HTML コンテンツと当ツールを配置する IPA の検査ツール提供サイトを使用し、アプリケーションは、Java Applet(アプレット）によって実装される。

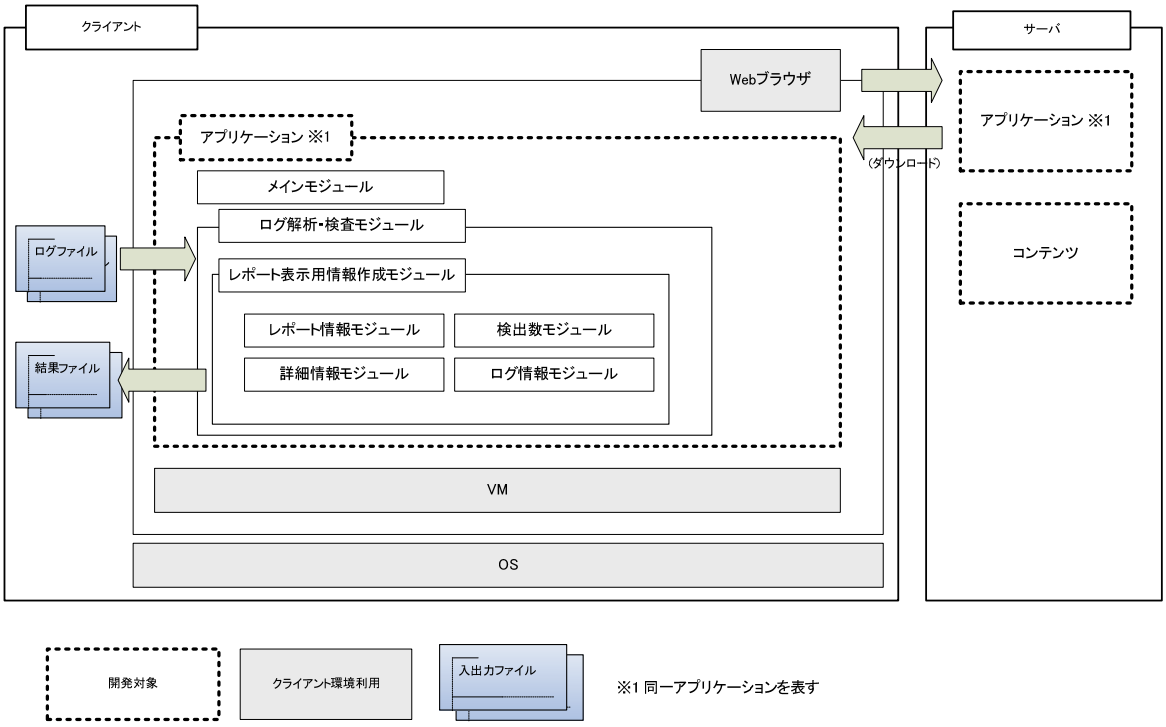

図 2. 機能構成

(3) プログラムへの電子署名

Java Applet は、ウェブページの一部として自動的に読み込まれて動作するため、ダウンロード元サーバ以外との通信ができず、実行するクライアントマシンのローカルリソースやデバイスにアクセスできない等のセキュリティ機能による動作制限が課せられている。この動作制限は、提供する Java Applet に電子署名し、利用者が Java Applet 実行時に許諾することにより、外すことが可能である。

当ツールは、Java Applet によって実装され、実行するクライアントマシンのローカルリソースへアクセスする必要がある。その為、当ツールでは電子署名を行っている。

(4) アクセスログ解析機能

指定されたアクセスログファイルに対し、検出対象カラムにある文字列中から各シグネチャとのマッチングを行い、特定の脆弱性を突いた攻撃の有無を調査する。また、結果を利用者へレポートする。アクセスログ中に攻撃の痕跡が見つかった場合、攻撃が成功した可能性の高いものついての判定を行う。

当ツールで解析が可能なログの種類は以下の 2 種類である。

・IIS5.0/5.1/6.0/7.0 の W3C 拡張ログファイルタイプ
・Apache1.3 系、Apache2.0 系、Apache2.2 系の common タイプ

(5) アクセスログ解析機能の強化

今回のバージョン 2 では次の機能拡張を実施した。

①検出可能な攻撃パターンの増加

- 「SQL インジェクション」の検出可能な攻撃パターンを 1.5 倍に増加。
- 「OS コマンド・インジェクション」、「ディレクトリ・トラバーサル」、「クロスサイト・スクリプティング」、「その他（IDS 回避を目的とした攻撃）」の痕跡を検出する処理を追加。

②解析対象のアクセスログを増加

- IIS5.1/7.0 の W3C 拡張ログファイルタイプのアクセスログ解析処理の追加。

③動作するプラットフォームの拡大

- Linux 系 OS 上での動作確認。
- 他、IE 以外のブラウザでの動作確認。

この機能拡張の結果、検出対象とする脆弱性を表 2 に示す。

表 2. 検出対象脆弱性

No	検出対象脆弱性名	検出
1	SQL インジェクション	◎
2	OS コマンド・インジェクション	○
3	ディレクトリ・トラバーサル	○
4	クロスサイト・スクリプティング	○
5	その他（IDS 回避を目的とした攻撃）	○

◎：攻撃の痕跡と攻撃の成功の可能性を検出

○：攻撃の痕跡を検出

解析に使用するシグネチャには、弊社のジャパンセキュリティオペレーションセンター（JSOC）のアナリストが、ウェブアプリケーション攻撃の中で検出頻度の高い文字列を中心にリストアップしたものを使用している。

(6) ユーザインターフェイス

当ツールの実際の画面を図 3～6 に示し、処理の流れを説明する。

① 解析対象ログファイルの設定

図 3 にツール実行画面を示す。

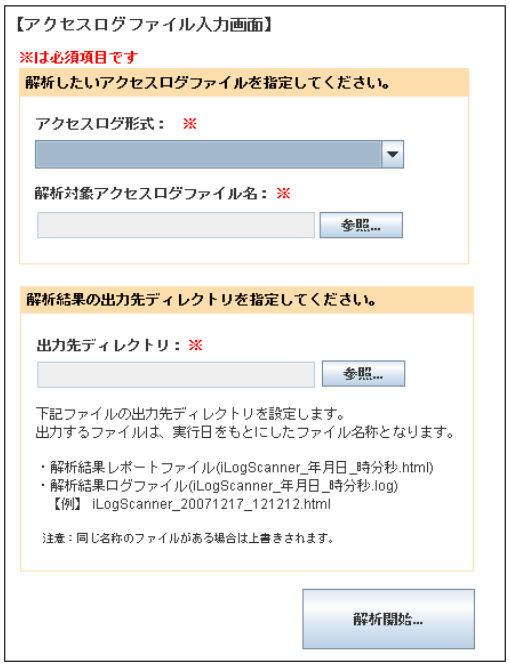

図 3. ツール実行画面

以下の項目を設定し、[解析開始...]ボタンをクリックすると、解析を開始する。

・アクセスログファイルの種類
・解析対象アクセスログファイル
・結果ファイル出力先ディレクトリ

② アクセスログ解析実行

図 4 に解析実行中画面を示す。

図 4. 解析実行中画面

解析実行中画面には全体解析進捗度と 1 ファイル毎の解析進捗度、検出対象脆弱性毎の攻撃痕跡検出数が表示される。攻撃痕跡の検出数は攻撃を検出する度、更新する。解析中であっても、中止ボタンを押すことによって処理を中断することができる。

解析終了、または解析を中止した場合、指定された出力先に解析結果レポートファイルを保存する。また、攻撃の痕跡が検出された場合は解析結果を詳細ログファイルに出力し保存する。

③ 解析結果

図 5 に、解析結果画面を示す。

【解析結果サマリ画面】

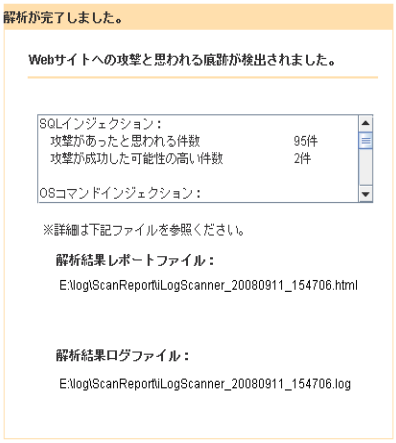

図 5. 解析結果画面

一つの脆弱性項目に対し、攻撃があったと思われる件数、攻撃が成功した可能性の高い件数をそれぞれ表示する。また、解析結果レポートファイル名と解析結果ログファイル名も同様に表示する。

④ 出力ファイル

当ツールでは解析終了後、利用者によって指定されたディレクトリに以下のファイルを出力する。

・解析結果レポートファイル
・解析結果ログファイル

図 6 に、解析結果レポートファイルを示す。

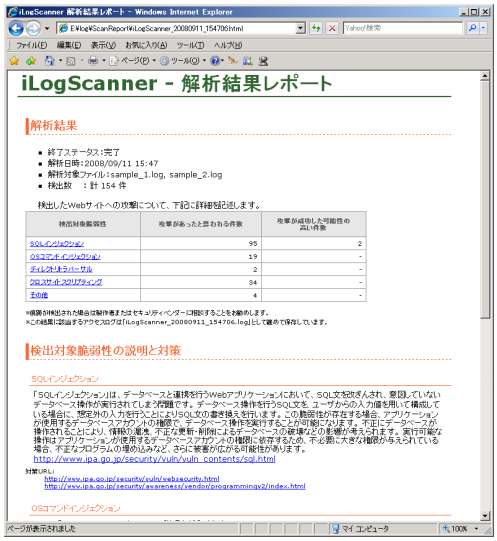

図 6. 解析結果レポート画面

レポートファイルには解析結果サマリ情報が記載される。また、攻撃の痕跡が検出された場合のみ、解析結果の詳細を記載したログファイルが出力される。

4. ツールによる効果

当ツールを用いることで、一般のウェブサイト管理者はウェブアプリケーションへの攻撃の有無や、潜む脆弱性を比較的簡単に確認する事が可能である。

また、当ツールを通しインターネットに公開しているウェブサイトの危険性を認知してもらうことは、ウェブサイト管理者や経営者に対して警告を発し、対策を講じるきっかけとなる等、啓蒙活動としての効果が期待できる。

5. 今後の課題

攻撃の有無をより多くの脆弱性を検出可能にする必要がある。