

iLogScannerの概要

iLogScanner は、ツール利用者がウェブブラウザを利用して IPA のウェブサイト（iLogScanner 提供サイト）からダウンロードし、利用者のウェブブラウザ上で実行する Java アプレット形式のプログラムです（図 1）。

利用者が用意したウェブサーバのアクセスログファイルの中から、ウェブサイトの脆弱性を狙った攻撃によく用いられる文字列を検出し（図 2）、ウェブサイトへ攻撃のあったと思われる痕跡や、攻撃が成功した可能性のある痕跡の有無を解析結果レポートとして出力します（図 3）。

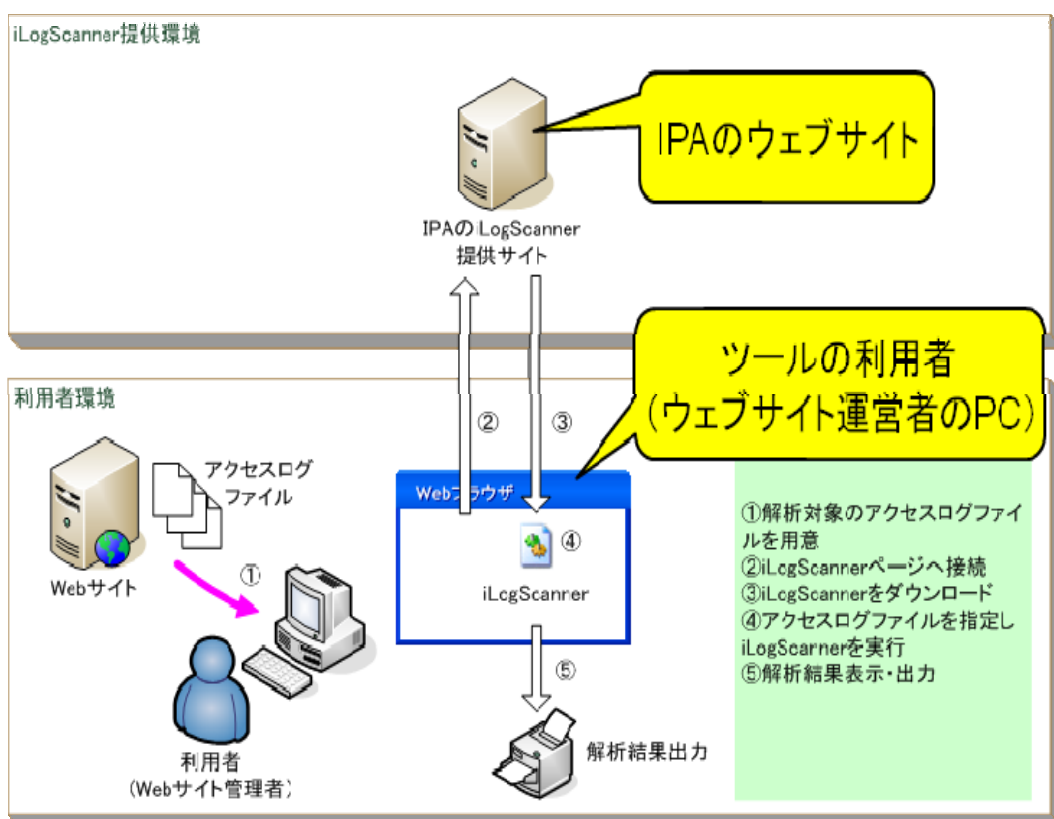


図 1. 「iLogScanner」の利用イメージ

ツールの初期画面



ツールの実行中画面

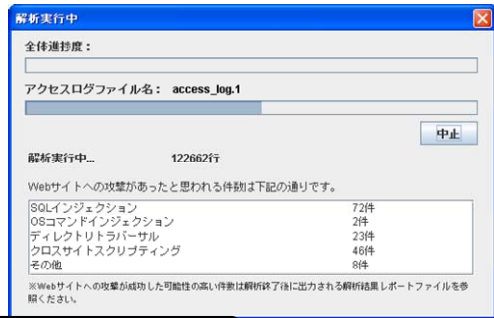
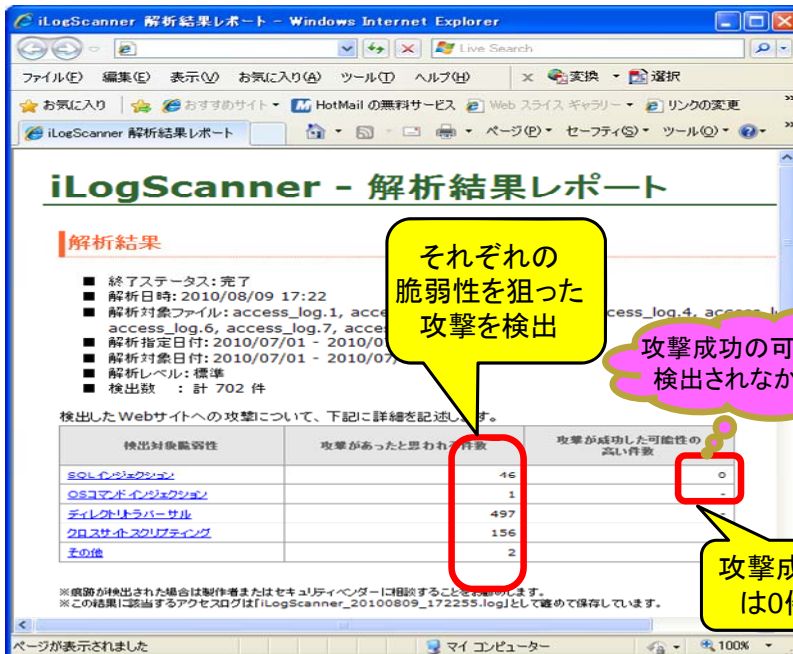


図 2. 「iLogScanner」の使用例

解析結果のレポート例



解析結果のログ例



図 3. 「iLogScanner」の解析結果例

iLogScanner V3.0 新機能の詳細

1. 検出可能な攻撃パターンの増強

- (1) 「SQL インジェクション」「OS コマンド・インジェクション」「クロスサイト・スクリプティング」について検出可能な攻撃パターンを旧バージョンから約 1.5 倍に増やし、以前より多くの種類の攻撃を検出できるようになりました。
- (2) 「同一 IP アドレスからの攻撃の可能性」「ウェブサーバの設定不備を狙った攻撃の可能性」など、特定の種類の脆弱性とは結びつかない攻撃パターンを新たに検出できるようになりました。

2. 使いやすさの向上

解析オプションを指定できる画面を用意し、利用者の用途に応じて任意で解析オプションが指定できるようになりました。

- (1) Apache HTTP Server 1.3系/2.0系/2.2系のカスタムフォーマットの解析ができるようになりました。
- (2) 解析時に対象期間を指定できるようになりました。
- (3) 用途に応じて「ログの解析レベル」(標準・詳細)を選択できるようになりました。「詳細」を選択した場合、「同一 IP アドレスからの攻撃の可能性」など特定の種類の脆弱性とは結びつかない攻撃の可能性を検出することができます。

□ 解析オプション指定画面

The screenshot shows the 'Log Processing Recommendation' window for iLogScanner. The left sidebar contains a tree view of various security-related categories. The main area is titled 'Log Processing Recommendation: Information Security: Vulnerability Countermeasures: Web Site Attack Detection Tool: iLogScanner'. It contains several sections for configuration:

- Log Format:** A text input field for specifying the log format. A note indicates it's a required item. An example shows the Apache LogFormat: `【例】 LogFormat "%h %l %u %t" "%r" %s %b" common`.
- Log Date Range:** Two date pickers for 'Start Date (From):' and 'End Date (To):'. The example shows '2010' for the year and '7' for the month. A note indicates it's a required item.
- Log Level:** A dropdown menu for 'Log Level:'. The example shows '標準' (Standard). A note indicates it's a required item.

Three yellow callout boxes with arrows point to these sections:

- Callout 1: (1) Apacheのログのカスタムフォーマットの形式を指定 (Specify the format of the custom Apache log format)
- Callout 2: (2) ログの対象期間を指定 (Specify the target period for the log)
- Callout 3: (3) ログの解析レベルを指定 (Specify the log analysis level)

図 4. 解析オプションの指定の例

3. その他

(1) ModSecurity 2.5 が出力するログファイルを元に ModSecurity で検出・遮断したデータを解析し、結果レポートを出力する機能を追加しました。

□ ModSecurity ログ解析画面

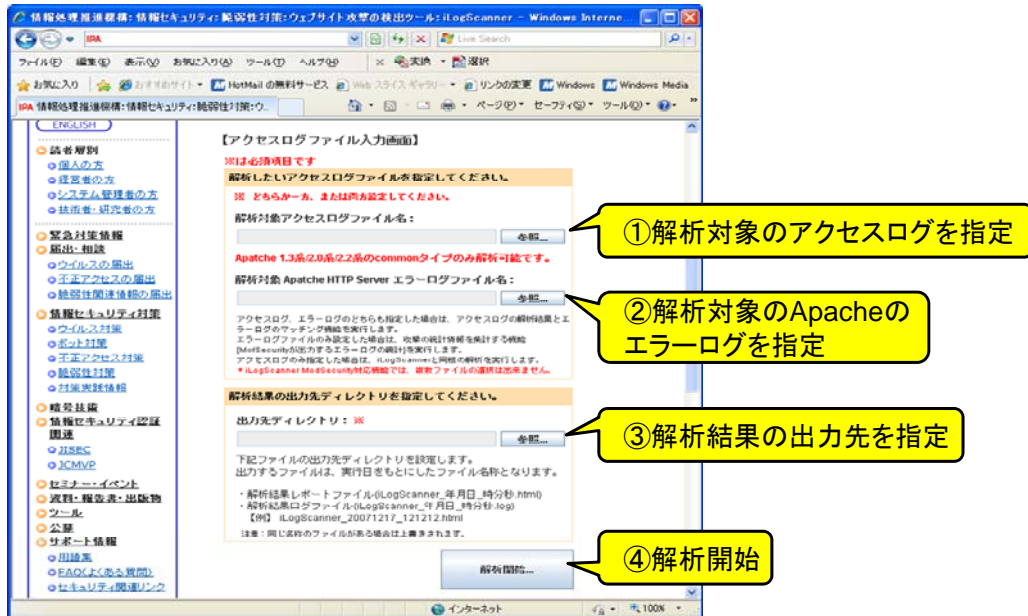


図 5. ModSecurity ログ解析画面

(2) Microsoft IIS の IIS ログファイルタイプのログフォーマットに対応しました。

参考：JVN iPediaに対する攻撃の検出件数

IPA が公開している「JVN iPedia（脆弱性対策情報データベース）」の 2009 年 8 月から 2010 年 7 月末までのアクセスログを解析した事例を示します（図 6）。直近の 12 か月間で攻撃があったと思われる件数は 7,784 件となり、日単位に換算すると平均で約 18 回攻撃されています。

また攻撃の種別も、非公開情報へアクセスされる可能性のあるディレクトリ・トラバーサルや、データベースが改ざんを受ける可能性のある SQL インジェクションなどのように、攻撃成功時に与える影響が大きなものが多いです。JVN iPedia は脆弱性対策を行っているため、攻撃が成功した形跡はありませんでしたが、ウェブサイト管理者は、インターネットに公開されているウェブサーバは常に危険にさらされていることを認識する必要があります³。

ウェブサイトを狙った攻撃があったと思われる件数

解析対象のウェブサイト：JVN iPedia（脆弱性対策情報データベース）

解析したウェブサーバのアクセスログの期間：2009年8月～2010年7月

攻撃があったと思われる件数：平均18.3件/日、攻撃が成功した可能性の高い件数：0件

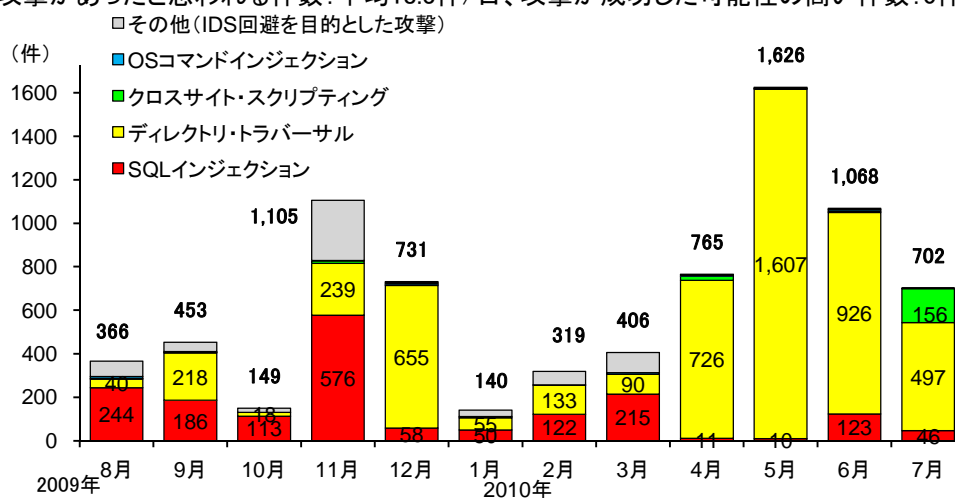


図6. ウェブサイト攻撃の検出ツール「iLogScanner」の解析事例

³ ウェブサイトを狙った攻撃に関する注意喚起について
<http://www.ipa.go.jp/security/vuln/report/vuln2010q2.html#t03>