

## ウェブサイト攻撃の検出ツール「iLogScanner」の性能向上版を公開

～ウェブサイト管理者は、ログを分析する習慣を～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、ウェブサイト攻撃の検出ツール「iLogScanner」（アイ・ログ・スキャナ）に対して、解析性能の向上をはじめ、検出可能な攻撃パターンの増強や使いやすさの向上を行い、「iLogScanner V3.0」として公開しました。

URL: <http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>

「iLogScanner」は、利用者のウェブブラウザ上でウェブサーバのログを解析することで、ウェブサイトを狙った攻撃の検出を容易に行うツールです。ウェブサイト管理者は本ツールを使用することで、自組織のウェブサイトがどれほどの攻撃を受けているかを把握することが可能になります。ログ解析などの攻撃状況の把握は、対策を立てる上での指針の一つになりますので、ウェブサイト管理者は本ツールを活用して、**日頃からログを分析する習慣**をつけることを推奨します。

IPAでは、2008年4月から本ツールを公開し、月平均1,500件以上のダウンロードがなされています。今回の更新では、本ツールがより効果的に活用可能となるよう、機能強化を行いました。

### 1. 解析性能の向上

(1) 旧バージョンと比較して、ログの解析時間が平均約5分の1に短縮されました<sup>1</sup>。

### 2. 検出可能な攻撃パターンの増強

(1) 検出可能な攻撃パターンの量を旧バージョンの約1.5倍に増強しました。

### 3. 使いやすさの向上

(1) 解析時に対象期間を日単位で指定できるようにしました。

(2) 利用者の用途に応じて「解析レベル」（標準・詳細）を選択できるようにしました。

### 4. その他

(1) Web Application Firewall (WAF)のログ分析が可能になりました。本バージョンでは、ModSecurity<sup>2</sup>と連携できるようにしました。

(2) 対応可能なログフォーマットの種類を増強しました。

■ 本件に関するお問い合わせ先

IPA セキュリティセンター 大森／渡辺

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: [vuln-inq@ipa.go.jp](mailto:vuln-inq@ipa.go.jp)

■ 報道関係からのお問い合わせ先

IPA 戦略企画部広報グループ 横山／大海

Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: [pr-inq@ipa.go.jp](mailto:pr-inq@ipa.go.jp)

<sup>1</sup> 解析時間の比較は、IPAで確認したものです。動作環境やログの内容によって差異が生じます。IPAでログ解析時間を計測したところ、最短で15分の1に短縮されました。

<sup>2</sup> ModSecurity は Web Application FireWall (WAF) のひとつで、ウェブサーバである Apache のモジュールとして動作します。