ウェブサイト攻撃兆候検出ツール
iLogScanner

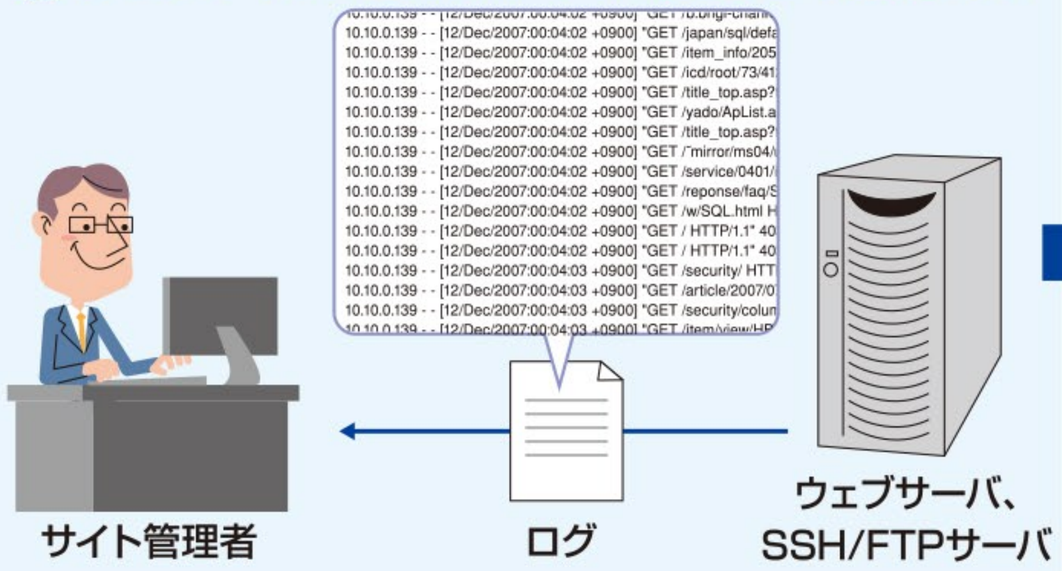
https://www.ipa.go.jp/security/vuln/iLogScanner/

iLogScannerとは

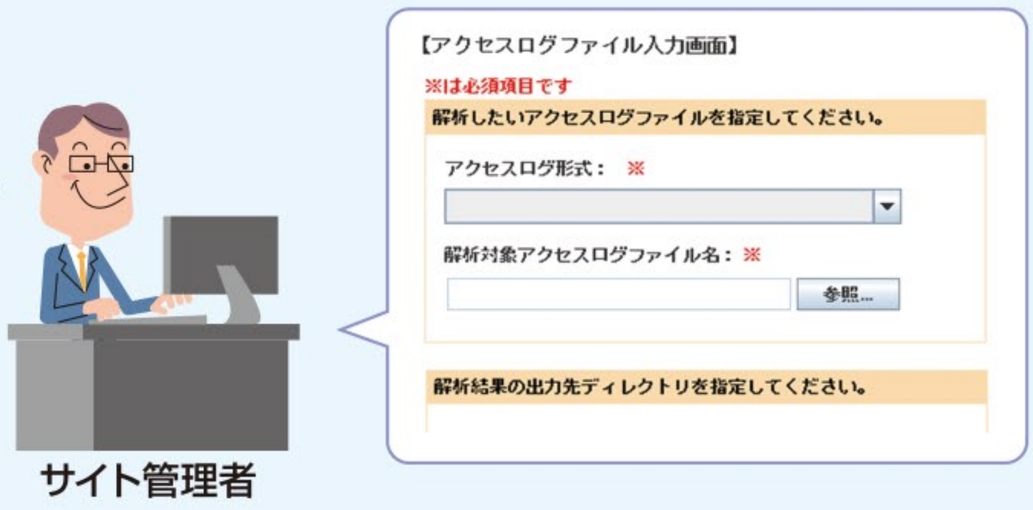
ウェブサーバのアクセスログやSSH/FTPサーバのログから**攻撃（脆弱性を狙った攻撃の兆候・不正ログインの兆候）と思われる痕跡を検出することができます。**

iLogScannerの利用イメージ

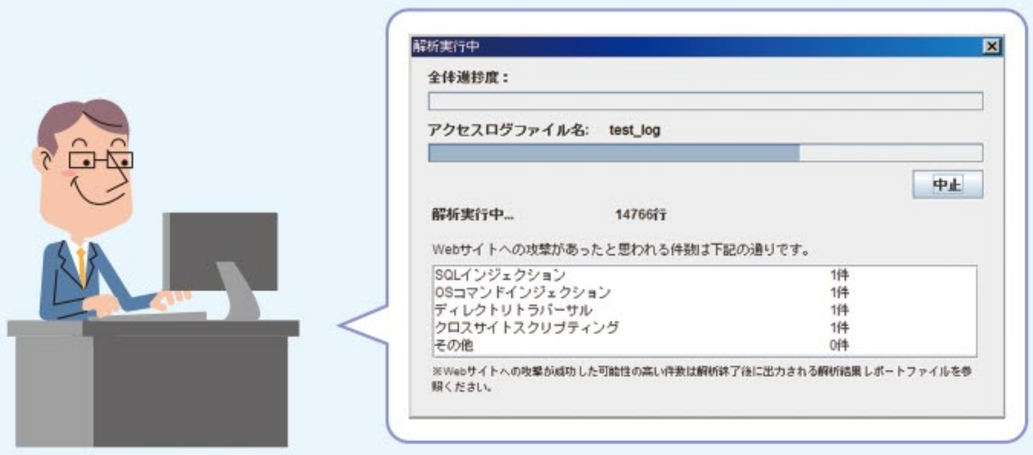
❶ ウェブサーバやSSH/FTPサーバからログを収集する。



❷ IPAのページにアクセスし、iLogScannerを起動する。

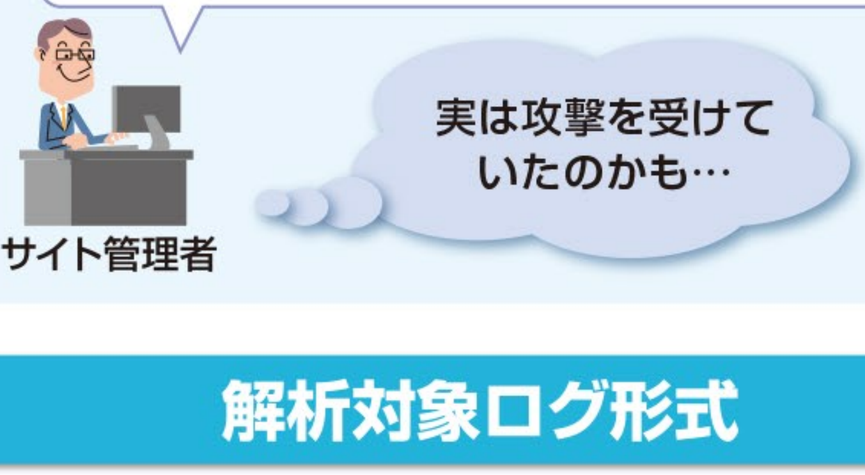


❸ iLogScannerにログを読み込ませ、解析を開始する。



❹ 解析結果を確認する。

検出対象脆弱性	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
SQLインジェクション	1	0
OSコマンドインジェクション	1	-
ディレクトリトラバーサル	1	-
クロスサイトスクリプティング	1	-
その他	1	-



検出可能な攻撃の兆候

■ウェブサイトの脆弱性を狙った攻撃の兆候
- ・SQLインジェクション
- ・ディレクトリ・トラバーサル
- ・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　など

■SSH/FTPを狙った不正ログインの兆候
- ・大量のログイン失敗
- ・短時間の集中ログイン
- ・匿名/ゲストアカウントでのログイン
- ・組織外(指定IP外)/業務時間外のアクセス　など

解析対象ログ形式

[アクセスログ/エラーログ]
- ・Microsoft　IISのW3C拡張ログファイル/IISログファイル
- ・Apache HTTP ServerのCommon Log Format
- ・Apache HTTP ServerのModSecurity　のエラーログ

[認証ログ]
- ・syslog(sshd)　・vsptpd/wuftpd形式のログ(vsftpd)

iLogScannerの利用形態

- ・ブラウザ上で実行可能な「オンライン版」
- ・ダウンロードしてバッチ処理等可能な「オフライン版」

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan