報道関係各位

2024 年 10 月 1 日
株式会社ビットフォレスト

Web サイトの隠れた攻撃痕跡を検出。
Web 攻撃ログ分析ツール「Loggol（ロゴル）」を
2024 年 10 月 1 日、正式リリース

株式会社ビットフォレスト（所在地：東京都千代田区 代表取締役 高尾都季一 以下、ビットフォレスト）は、Web 攻撃ログ分析ツール「Loggol（ロゴル）」の正式版を 2024 年 10 月 1 日、リリースしました。「Loggol」は、Web サーバのアクセスログを自動的に分析することで、主に Web アプリケーションの脆弱性を狙った攻撃の痕跡を検出するクラウドサービスです。2023 年 11 月より β 版を提供しておりましたが、今回の正式版では機能をアップデートし、より進化した形でサービス提供を行います。

セキュリティ視点で Web サイトのアクセスログを分析する重要性と課題

Web サイトのアクセスログには、訪問者の IP アドレス、訪問日時、リクエストしたページ、利用ブラウザ、リファラーなどの情報が含まれています。これを Web セキュリティの専門的な視点で分析することで、Web アプリケーションの脆弱性を狙った攻撃の痕跡やその兆候、不正なログイン試行、一般ユーザーと違う異常なパターンの通信、自動化された疑わしいアクセスなどを抽出でき、様々なサイバーセキュリティ上のリスク回避・軽減に繋がります。こうしたアクセスログ分析の重要性は、近年、様々なガイドライン（*1）でも取り上げられており、セキュアな Web サイト運営の基本要素として広く認識されつつあります。

*1 例えば IPA（情報処理推進機構）では、安全な Web サイト運用管理の基本原則として 20 ヶ条のチェックポイントを提唱しており、その中でログ確認の重要性の説明とログ分析ツールの紹介が行われています。
IPA：安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～

しかし、Web サイトのアクセスログを取得・保管しているにも関わらず、アクセスログを日頃からセキュリティ視点で活用できていない企業がまだまだ多いのが実情です。特に、必要性は意識していながらも、「分析の

ための人手と時間が足りない」「分析に必要な技術がない」「ログの量が多い」といった理由から実施できないケースが多く見受けられます。

Loggol はこうした課題にアプローチ

Loggol を利用すると、リーズナブルな月額料金で、知識やスキル、事前の準備など一切なしに、手軽にアクセスログのセキュリティ分析が可能となります。
SQL インジェクション、クロスサイトスクリプティング、コマンドインジェクション、パストラバーサル、ログイン総当り、異常なアクセスパターンをはじめ、Web アプリケーションや Web サイトに対する多様な攻撃の痕跡を高精度で検出します。プランごとのログサイズや行数の範囲内であれば、いつでも多数のサイトのログ分析が可能で、自動運用や外部システム連携のための WebAPI もご用意しています。分析結果については、セキュリティエンジニアによる専門的なサポートやミーティングでのご相談を提供しています。

●活用シーン

情報システム部門、セキュリティ部門、Web サイト運用部門、開発部門/事業部門など、Web アクセスログの利用権限さえ取得していればどなたでも簡単に利用できます。

＼　たとえば、こんな場面で活用いただけます　／

1. 日々のWebサイトへの攻撃状況確認に
2. リスト型攻撃や攻撃準備行動の早期発見に
3. 怪しいと感じる事象や、周辺サイト/関連システムでインシデント疑いがあった場合の緊急確認に
4. 新たに重要な脆弱性や攻撃手法が報告された際、過去に遡って攻撃の有無を確認したいときに
5. Webサイト運営を引き継いだ際の現状把握に
6. SOCでのセキュリティイベント管理、SIEM/SOARとの連携に

Loggol の特徴

Web 攻撃ログ分析に特化したサービス

2008 年に IPA（情報処理推進機構）より無償提供が開始されたログ分析ツール「iLogScanner」(*2) に近いコンセプトを持ちつつ、ビットフォレストがデータサイエンス技術と最新の Web セキュリティ知見を投入して開発した独自サービスです。

*2 IPA（情報処理推進機構）「iLogScanner」

アクセスログとブラウザだけあれば OK

PC やサーバへのインストールやサイトごとの設定は一切不要で、所定形式の範囲内の Web アクセスログであれば、そのままアップロードするだけで利用可能です。

安心の国内完結型サービス

すべて日本国内で、日本語対応での提供を行っています。技術サポートについても、国内のセキュリティエン

ジニアが直接対応します。

ログ分析のスピード

高速な国内のクラウドインフラ上で解析処理を行います。
ログのサイズによりますが、数秒～数分以内に分析が終了し、すぐに結果を参照することができます。

データサイエンス活用の検出ロジック

ビットフォレストが開発・運用を行うクラウド型 WAF「Scutum（スキュータム）」の AI 型検知ロジックと共通するデータサイエンス技術が多数活かされています。

新たな脆弱性・攻撃手法の反映

Scutum と共通の研究チームが、新たな脆弱性や攻撃手法に関する情報収集や調査を行い、Loggol に反映します。

基本サポートからセキュリティエンジニアによるフルサポートまで

プランによって、Web セキュリティの高度な知識を必要とする専門的なサポートをご提供しています。

様々な利用シーンに合った柔軟な料金プラン

初期費用不要、月額 2 万円（税抜）から、1 か月単位でご利用可能です。

PLAN

料金プラン

	ベーシック	プラス	フルサポート
月額(税抜)	¥20,000	¥50,000	¥300,000
ログサイズ(合計/個別)、分析行数、API回数	少	中	多
サポート対応	基本サポート	基本/テクニカルサポート	専門家によるフルサポート

※ お支払い方法は銀行振込(請求書発行)です。

※料金の詳細、サポート内容等については、Loggol サービスサイト「料金プラン」をご覧ください。

無料トライアルを実施中

Loggol は 14 日間の無料トライアルがお試しいただけます。ご利用の際は下記 URL よりお申込みください。

実施期間：10 月 1 日（火）～

無料トライアル申込：https://www.loggol.jp/entry.html

開発者コメント「Loggol というサービスを作った理由」

株式会社ビットフォレスト　取締役　佐藤 匡

私は Loggol の開発以前より、継続して 2 つのクラウド型のセキュリティサービスの開発・運用に携わってきました。1 つは WAF である Scutum、もう 1 つは脆弱性検査ツールである VAddy です。

WAF では、多種多様なデータが送られてくるウェブアプリケーションの入力に対して、高い精度で「攻撃かどうか」を分類する必要があり、Scutum ではベイジアンネットワークという技術や単なる正規表現のパターンマッチング（シグネチャと呼ばれる）などを組み合わせてこの分類性能を高めています。

この「攻撃かどうか分類する」ソフトウェア機能は、WAF 以外にも出番があります。
WAF/IDS/IPS/SIEM は既に非常に良く知られたセキュリティソリューションとなっています。さらに他にこのような分類機能が役に立つ場面はないだろうか？と考えると、IPA が出している iLogScanner が思い浮かびます。これはウェブサーバ等のアクセスログを入力データとしており、それぞれの行を「攻撃かどうか」分類することで、アクセスログの中から悪意ある攻撃を抽出するものです。WAF とは異なり分類が行われる時点はリアルタイムではありませんが、ソフトウェアの機能はほぼ同じものです。ログを分析するという点では SIEM に似ていますが、ウェブのアクセスログに限定した、非常にシンプルな立ち位置です。

iLogScanner が登場した当時から、私の頭の中では「これは WAF とほぼ同じ仕組みだ」と感じていました。そして WAF サービスを運用・開発していく中で、開発で使用する品質担保のためのテストコードの中には実質的に Web 攻撃ログ分析ツールそのものと言える物も存在しており、あとはビジネス的な枠組みを整備すればサービス化できる状態になっていました。このように、必要とされる中核部分の技術が WAF とログ分析ツールで共通であるということが、Loggol の開発に至った 1 つの理由です。
※他の理由も含め、Loggol の開発背景については Loggol ブログにて詳しくご紹介しています。

さらに、ログ分析ツールはリアルタイム性がないからこそ時間をかけた分析ができるという点を WAF に対するアドバンテージとして利用することが出来ます。Loggol では異常検知の機能を提供しています。今後もこの点を活かして、より高度な分析が可能となるように Loggol を進化させていきたいと考えています。

本文内でご紹介したビットフォレスト製品について

Loggol 公式 Web サイト：https://www.loggol.jp/
VAddy 公式 Web サイト ： https://vaddy.net/ja/
Scutum 公式 Web サイト： https://www.scutum.jp/ （販売元：株式会社セキュアスカイ・テクノロジー）

株式会社ビットフォレストについて

【会社概要】

社名：株式会社ビットフォレスト

所在地：
東京本社
〒101-0054
　東京都千代田区神田錦町 1-17-5 Daiwa 神田橋ビル 8F
福岡オフィス
〒810-0001
　福岡県福岡市中央区天神 4-6-28 天神ファーストビル 6F
代表取締役：高尾 都季一
事業内容： Web アプリケーションセキュリティ製品の開発、販売
設立： 2002 年 2 月
URL：https://www.bitforest.jp/

【本件に関する報道関係者からのお問合せ先】
株式会社ビットフォレスト 広報担当：Loggol サポートチーム
電話：03-5577-2032 メールアドレス：loggol@bitforest.jp