
イー・ガーディアングループは、安心・安全なインターネット環境の実現に向け、ネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供しております。特にEGセキュアソリューションズは、ネットセキュリティにおける課題解決を目的としたサービスを幅広く展開しており、WAF製品「SiteGuardシリーズ」は、累計導入サイト数・累計導入社数でNo.1※を獲得いたしました。

この度、SiteGuard Cloud Editionで観測したサイバー攻撃の検出情報を集約・分析した「SiteGuard セキュリティレポート」を作成しました。2024年第3四半期の「攻撃種別」「月別」「接続元（国別）」3つの観点から攻撃の傾向を発表いたします。

## 1. 攻撃種別

集計期間中に検出した攻撃を分類すると以下のようになります。5割を超える「バッファオーバーフロー」に次いで「SQLインジェクション」を多数検出し、この2つの検出で9割を占める結果になりました。

なお、「バッファオーバーフロー」は、これまで「その他」に分類していましたが、2024年第3四半期に多数検出したため、個別に分類にして集計しています。「バッファオーバーフロー」に関する詳細は後述のトピックを参照してください。

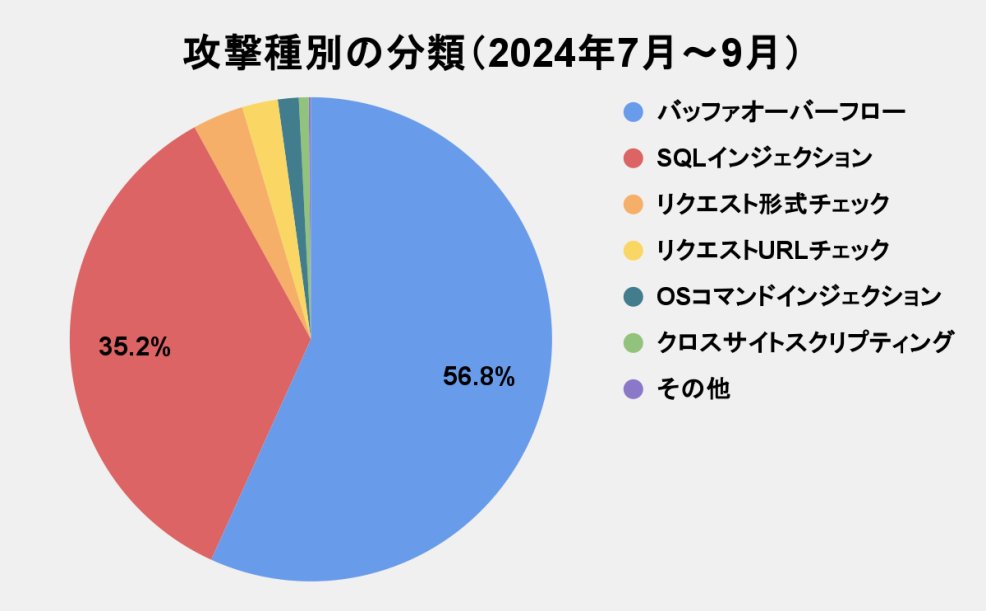


図1 攻撃種別の分類（2024年7月～9月）

| 攻撃種別 | 集計期間中の割合 |
|---|---|
| バッファオーバーフロー | 56.8% |
| SQLインジェクション | 35.2% |
| リクエスト形式チェック | 3% |
| リクエストURLチェック | 2% |
| OSコマンドインジェクション | 1% |
| クロスサイトスクリプティング | 1% |
| その他 | 0% |

表1 攻撃種別の分類（2024年7月～9月）

## 2. 月別の検出

次に、こちらは集計期間中の攻撃アクセス検出の推移です。7月の検出を100とした場合、8月の検出は159、9月は301となり、7月から9月にかけて攻撃アクセスは増加しています。

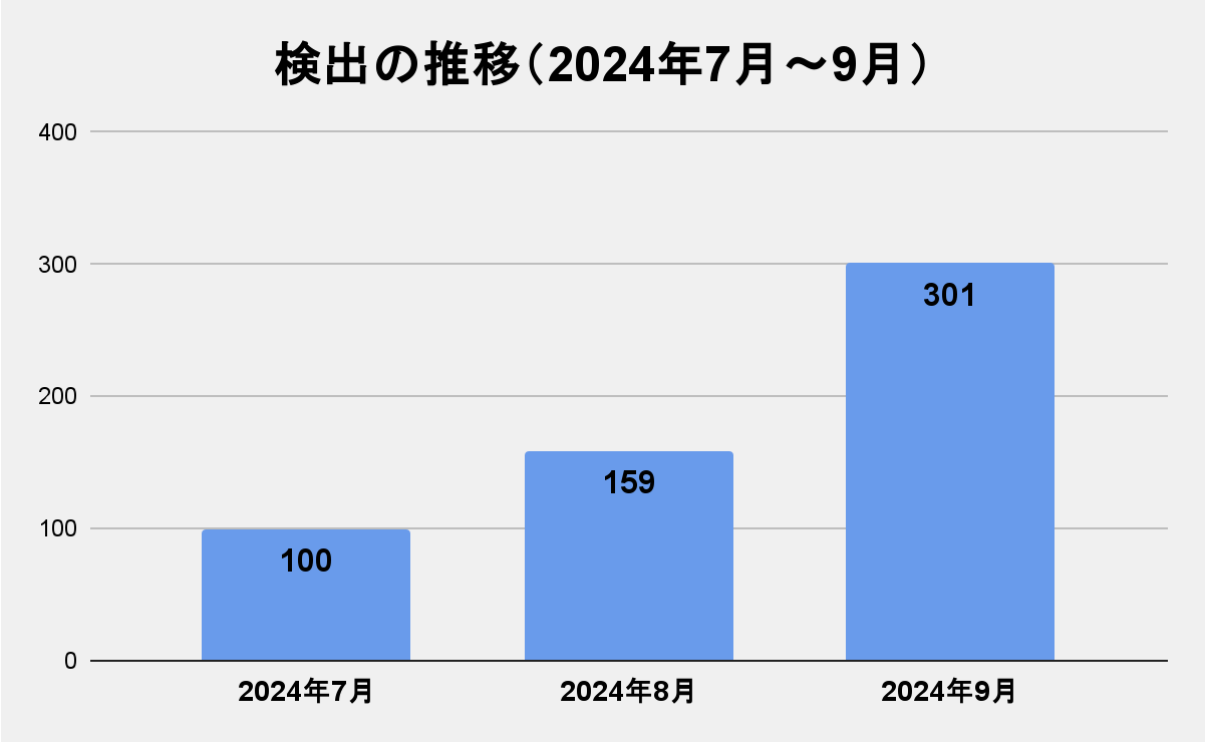


図2 検出の推移（2024年7月～9月）※2024年7月を100とした場合で算出

## 3. 接続元（国別）の分類

最後に接続元の分類です。集計期間中の国別の検出は以下の通りでした。アメリカ合衆国からの攻撃アクセスが6割を超え、続いて日本という結果に。前回の第2四半期では接続元の国は分散する結果でしたが、第3四半期はアメリカ合衆国による攻撃アクセスが圧倒的な割合を占める結果となりました。

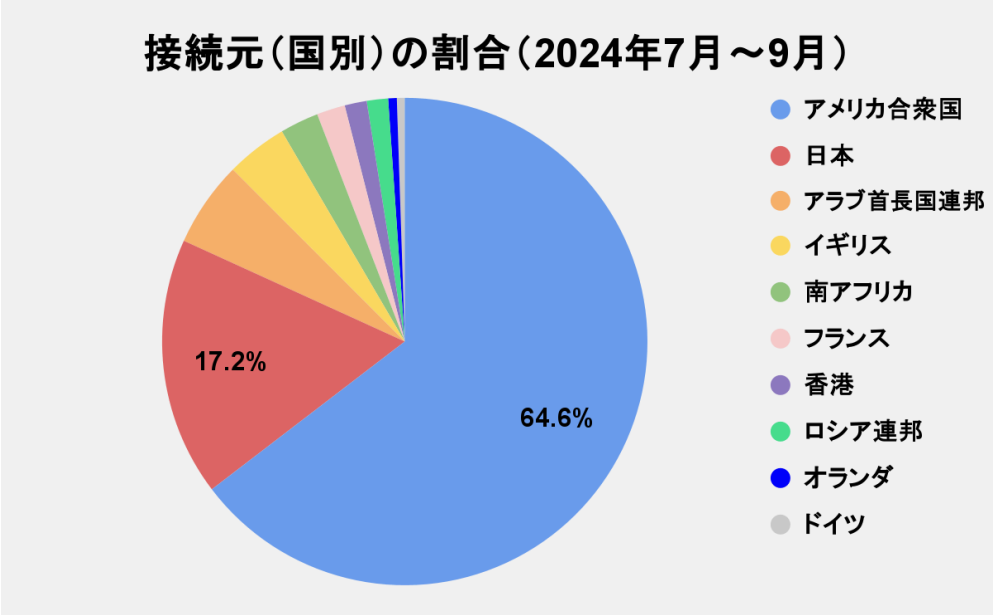


図3 接続元（国別）の割合（2024年7月～9月）

| 順位 | 国名 | 集計期間中の割合 |
|---|---|---|
| 1 | アメリカ合衆国 | 64.6% |
| 2 | 日本 | 17.2% |
| 3 | アラブ首長国連邦 | 5.7% |
| 4 | イギリス | 4.1% |
| 5 | 南アフリカ | 2.6% |
| 6 | フランス | 1.9% |
| 7 | 香港 | 1.5% |
| 8 | ロシア連邦 | 1.4% |
| 9 | オランダ | 0.6% |
| 10 | ドイツ | 0.5% |

表3 接続元（国別）の割合（2024年7月～9月）

## 4. 2024年3Qの注目トピック：バッファオーバーフロー攻撃が増加

集計期間中、バッファオーバーフロー攻撃が多数検出され、2024年1月以降の検出と比較すると大きく増加しました。2024年1月、2月は検出が無く、3月の検出を100とした場合、7月の検出は77、8月は417、9月は1080となり、月毎に増加しました。

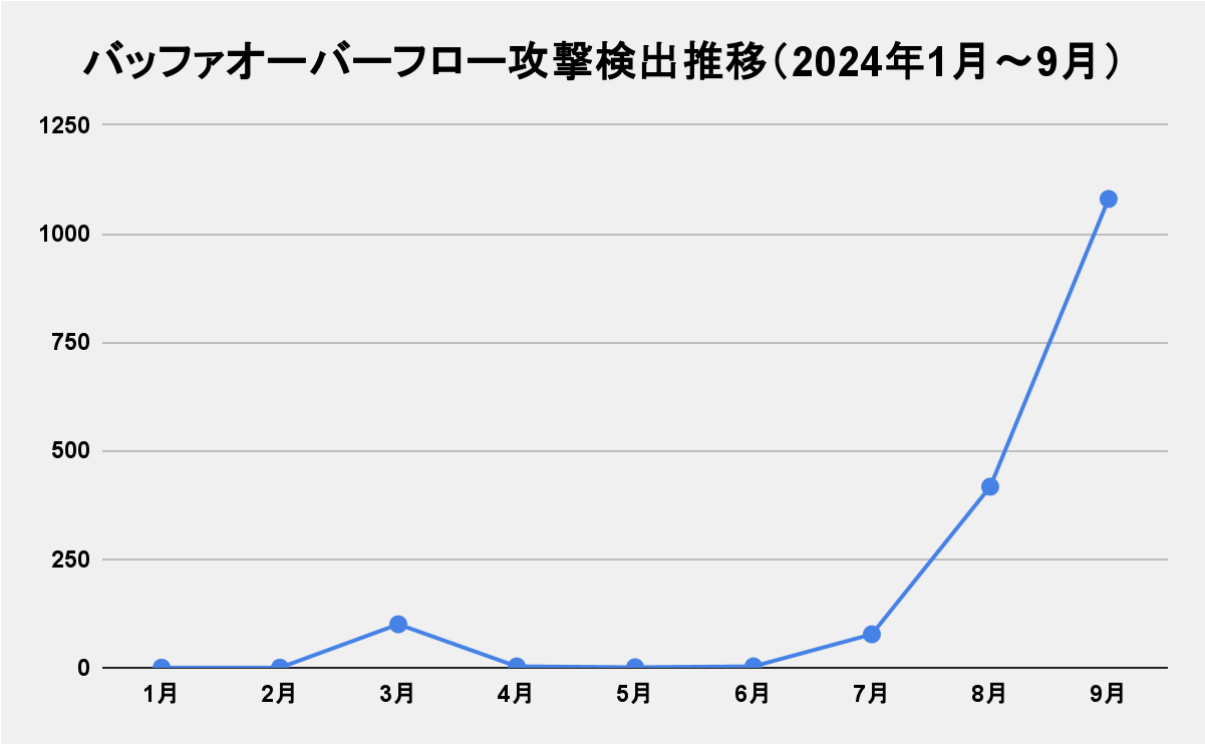


図4 バッファオーバーフロー攻撃検出推移（2024年1月～9月）

なお、7月以降に検出したバッファオーバーフロー攻撃は関連しない2つのWebサイトに対するアクセスですが、大多数はアメリカ合衆国の同じ3種類のIPアドレスからでした。

一方のWebサイトでは７月25日（木）からアクセスが確認され、以降は継続してアクセスが9月末まで続きました。もう一方のWebサイトは7月3日（水）に最初のアクセスが確認され、それ以降７月・8月は検出が無い日が大半でしたが、9月に入り連日検出されました。

## 5. 2024年3Qの注目トピック：SQLインジェクション攻撃が59時間に集中

集計期間中の7月に最も多かったSQLインジェクション攻撃は、7月29日（月）22時頃から8月1日（木）9時頃までの59時間に集中していたことがわかりました。また、このアクセスの大多数は3カ国（アラブ首長国連邦、日本、イギリス）から特定のWebサイトに対するもので、途切れることなくアクセスを受け続けていました。

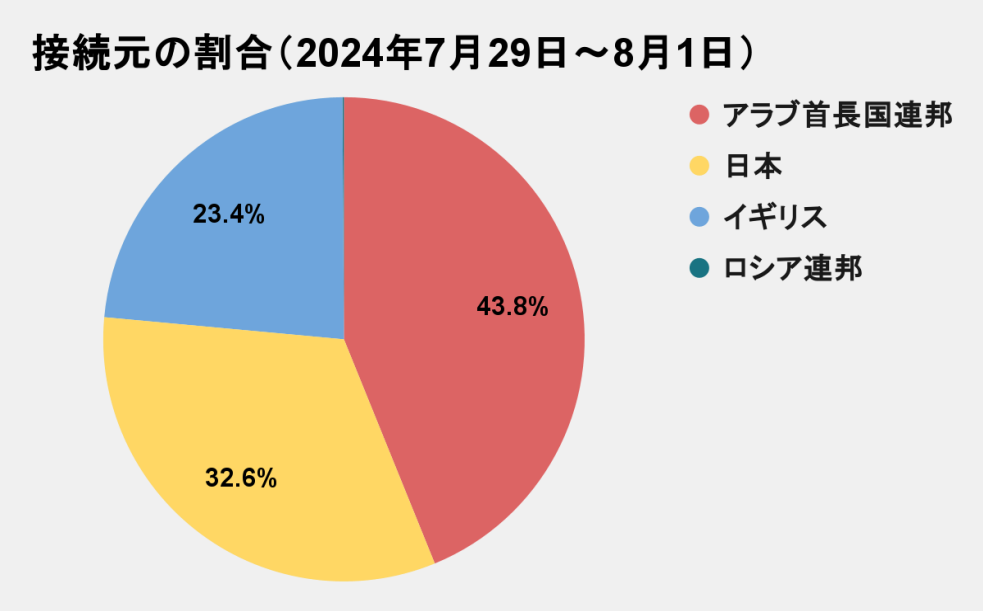


図6 接続元の割合（2024年7月29日～8月1日）

## 6. 2024年3Qのコメント

この3ヶ月で一番発生件数が多かったバッファオーバーフロー攻撃ですが、SiteGuardではパスやパラメータ、ヘッダー等の長さが一定のしきい値を超えた場合や、shellcodeと呼ばれるバイナリデータの一部を発見した場合に検出されます。

今回検出されたものは、ほぼすべて長いパスを検出したものでした。その長いパスは下記のような短いパターンが連続するものです。

▼バッファオーバーフロー攻撃として検出された長いパスの例（/xxx/yyy/は実在するパス）
例1　/xxx/yyy/20230722/20230722/20230722/20230722/20230722/20230722/20230722/…
例2　/xxx/yyy/img/img/img/img/img/img/img/img/img/img/img/img/img/img/img/img/…
例3　/xxx/yyy/files/files/files/files/files/files/files/files/files/files/files/files/files/files/files/files/…

これは攻撃であると明確には言えませんが、通常のアクセスとも言えません。上記のパターンで長さが閾値を超えず、検出されずにWebサイトに到達したリクエストもありますが、特に大きな影響はないと考えられます。これらのリクエストには、User-Agentに「Amazon-bot」や「Baidu-bot」を示す文字列が含まれており、それぞれのIPアドレスを逆引きすると、本物のbotである可能性が高いことがわかります。また、検出されたのが2つのWebサイトに限定されていることから、Webサイトの構成や設定によって引き起こされるWebクローラーのバグが原因なのではと推察しています。

本来、バッファオーバーフロー攻撃とは、スタックメモリーやヒープメモリー等に入力データーを溢れさせるものです。スタックメモリーを狙ったものでは、関数の戻りアドレスを書き換え、挿入した機械語プログラムにジャンプさせて実行させるという高度な攻撃も含まれます。20年ほど前までは、メールサーバーのSendMailやDNSサーバーのBIND等を標的としてこのような攻撃が猛威をふるっていました。現在ではOSやコンパイラでこのような攻撃に対する防衛がなされており、この攻撃に対するリスクは低くなっています。また、Webサイトを構築するために用いるPHP、Ruby、Java Scriptといったインタープリター言語は、そもそもこの攻撃に対する脆弱性が入り込む可能性が少ないです。

バーファオーバーフロー攻撃の対策としては、OSやインタープリター、アプリケーションフレームワーク等を常に最新にしておくことが重要です。

EGセキュアソリューションズ株式会社　セキュリティ研究所　所長　直岡克起

## 「SiteGuard セキュリティレポート」とは

EGセキュアソリューションズが開発・提供するクラウド型WAF「SiteGuard Cloud Edition」で検出された攻撃を分析し、サイバー攻撃の傾向や動向、新たな脅威への対応などを四半期ごとにまとめたレポートです。昨今サイバーセキュリティ上の脅威が増大している現状を受け、幅広い役割や年齢層の方々へセキュリティに関する情報をお届けし、セキュリティに関する知見を高め備えてほしいという思いから公開することとなりました。ぜひ皆様のセキュリティ意識の向上・セキュリティ対策の参考としてお役立ていただければ幸いです。

＜集計条件＞

・SiteGuard Cloud Editionの検出情報をもとに集計しています。
・検出名や分類は、SiteGuard Cloud Editionによる検出情報をもとにした表記になっています。
・対象サービスの利用者によるセキュリティ診断等のアクセスが集計対象に含まれている場合があります。
・不正ログインの試行（ログインの失敗）のほか、ウェブ以外の不正アクセス（スパムメールやマルウェア等）の情報は含まれていません。

## 累計導入サイト数・累計導入社数No.1※「SiteGuardシリーズ」概要

ウェブサイトの脆弱性を悪用した攻撃を防御するソリューションとして、官公庁や金融機関をはじめとした大企業から個人向けホスティングサービスまで、幅広い導入実績をもつ国内トップシェアクラスの純国産WAF（Web Application Firewall）製品です。かんたん導入・運用お任せのクラウド型「SiteGuard Cloud Edition」、インストールタイプでカスタマイズ性に優れたソフトウェア型（ホスト型WAF「SiteGuard Server Edition」、ゲートウェイ型「SiteGuard Proxy Edition」）の3製品をご用意しております。

製品詳細URL：https://siteguard.jp-secure.com/

※ 2023年12月期_指定領域における市場調査
調査機関：日本マーケティングリサーチ機構（https://jmro.co.jp/）

EG Secure Solutions
EGセキュアソリューションズ株式会社

**SiteGuardお問い合わせ窓口**
Mail：sg-sales@eg-secure.co.jp
Tel：03-6257-3927
URL：https://siteguard.jp-secure.com