EG Secure Solutions

News Release

報道関係者各位

2024 年 7 月 22 日

EG セキュアソリューションズ株式会社

サイバーセキュリティ企業【EGセキュアソリューションズ】
2024年2Qにおける攻撃アクセスの傾向をまとめた
「SiteGuard セキュリティレポート」を発表
～「攻撃種別」「月別」「接続元（国別）」での統計～

イー・ガーディアン株式会社（https://www.e-guardian.co.jp/ 東京都港区 代表取締役社長：高谷 康久　以下、「イー・ガーディアン」）のグループ会社である EG セキュアソリューションズ株式会社（https://www.eg-secure.co.jp/ 東京都港区 代表取締役：高谷 康久　以下、「EG セキュアソリューションズ」）は、当社が開発・提供するクラウド型 WAF「SiteGuard Cloud Edition」で 2024 年第 2 四半期（2024 年 4 月 1 日～6 月 30 日）に検出された攻撃を分析した「SiteGuard セキュリティレポート（2024.2Q）」を発表いたします。

EG Secure Solutions

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。

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」、今回は 2024 年第 2 四半期における攻撃の傾向を「攻撃種別」「月別」「接続元（国別）」の 3 つの観点から発表いたします。

■攻撃種別

まず、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。6 割を超える SQL インジェクションに次いで、リクエスト URL チェックも多数検出し、この 2 つの検出で 9 割近くを占める結果になりました。

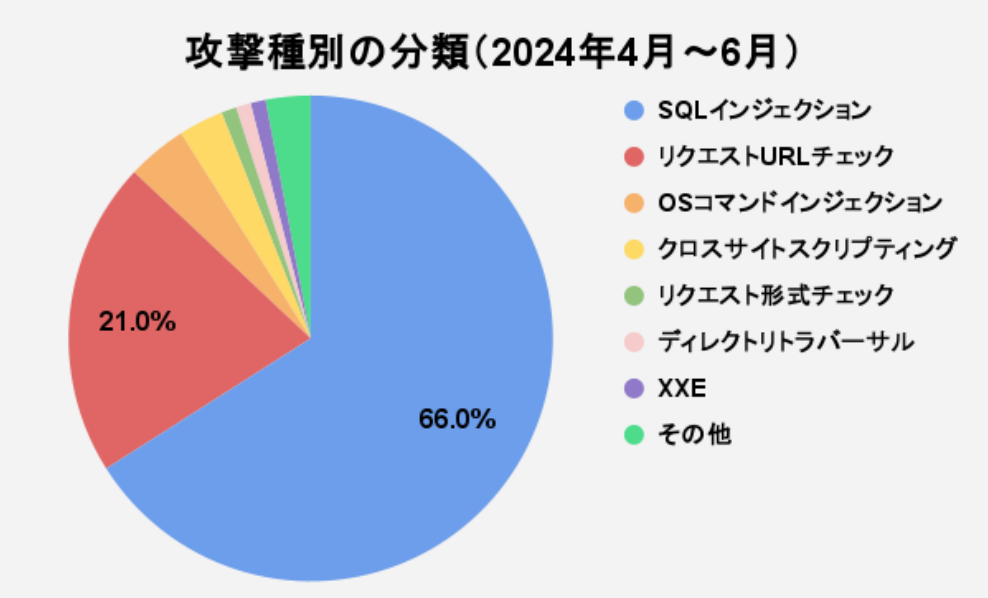

図 1 攻撃種別の分類（2024 年 4 月～6 月）

攻撃種別	割合
SQLインジェクション	66%
リクエストURLチェック	21%
OSコマンドインジェクション	4%
クロスサイトスクリプティング	3%
リクエストURLチェック形式チェック	1%
ディレクトリトラバーサル	1%
XXE	1%
その他	3%

表 1 攻撃種別の分類（2024 年 4 月～6 月）

■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。4 月の検出を 100 とした場合、5 月の検出は 116、6 月は 194 となり、4 月から 6 月にかけて攻撃アクセスは増加しています。

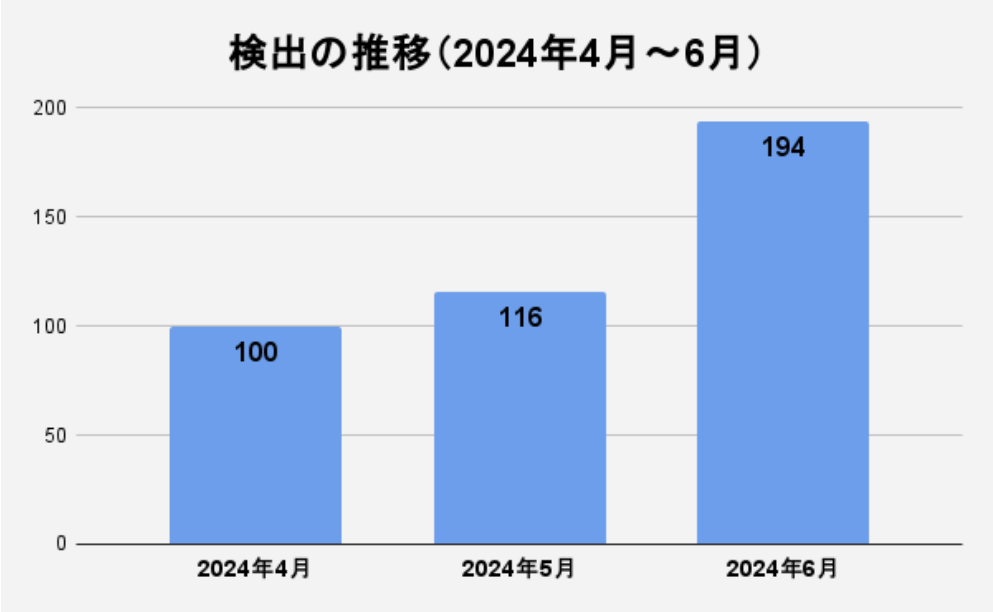

図 2 検出の推移（2024 年 4 月～6 月） ※2024 年 4 月を 100 とした場合で算出

■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。日本国内からの攻撃アクセスが 3 割を超え前回の 4 位から 1 位へ上昇、次いでシンガポール、アメリカ合衆国と続いています。前回の第 1 四半期では上位 2 ヵ国（ロシア連邦・アメリカ合衆国）が圧倒的な割合を占めていましたが、今回は比較的分散する結果となりました。

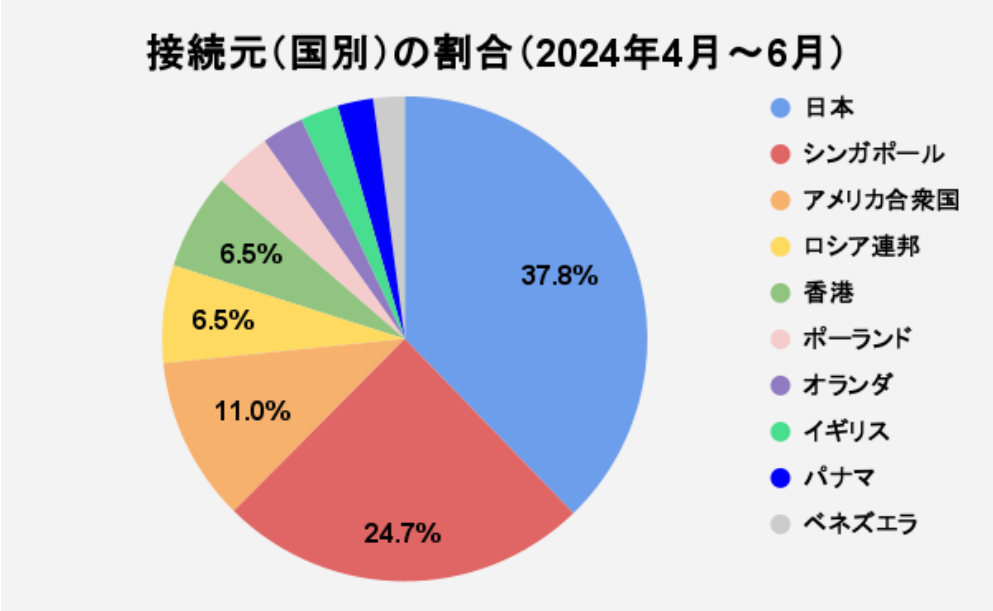

図 3 接続元（国別）の割合（2024 年 4 月～6 月）

順位	攻撃種別	割合
1	日本	37.8%
2	シンガポール	24.7%
3	アメリカ合衆国	11.0%
4	ロシア連邦	6.5%
5	香港	6.5%
6	ポーランド	3.8%
7	オランダ	2.8%
8	イギリス	2.6%
9	パナマ	2.4%
10	ベネズエラ	2.1%

表 2 接続元（国別）の割合（2024 年 4 月～6 月）

■2024 年 2Q の注目トピック：6 月に日本国内からの攻撃が最多に

集計期間中最も多かった日本国内からの攻撃（62.9%）のうち、過半数が 6 月に行われたものであり、特に 6 月 19 日（水）20 時頃～6 月 20 日（木）8 時頃までの 12 時間に集中していたことがわかりました。また、この攻撃アクセスはすべて 1 つの IP アドレスから特定の Web サイトに対するもので、途切れることなく攻撃アクセスを受け続けていました。

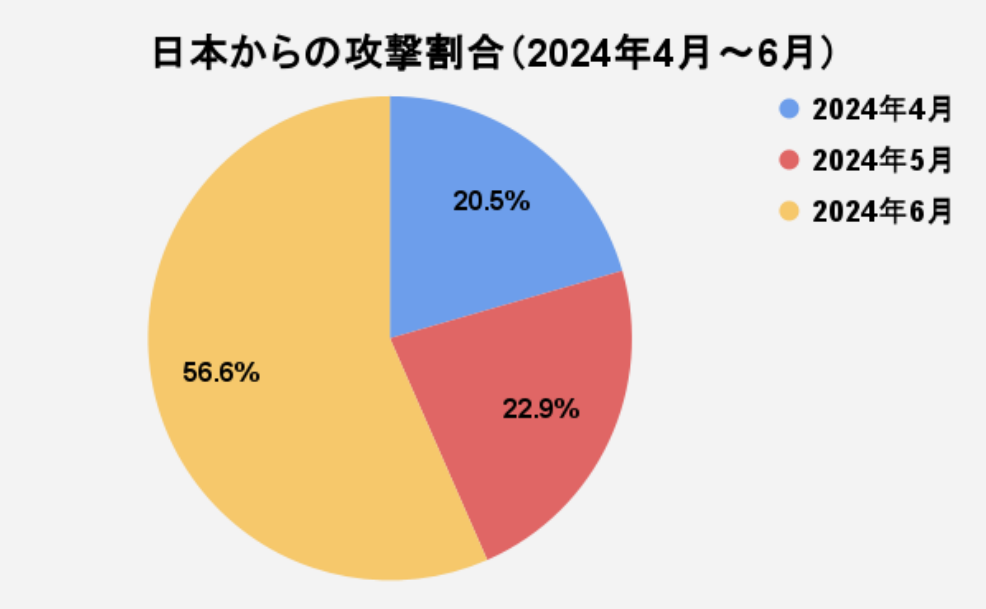

図 4 日本国内からの攻撃割合（2024 年 4 月～6 月）

攻撃アクセスが集中していた 2024 年 6 月 19 日～6 月 20 日における攻撃種別は以下の通りです。SQL インジェクションによる攻撃が圧倒的多数で、8 割以上を占めていました。

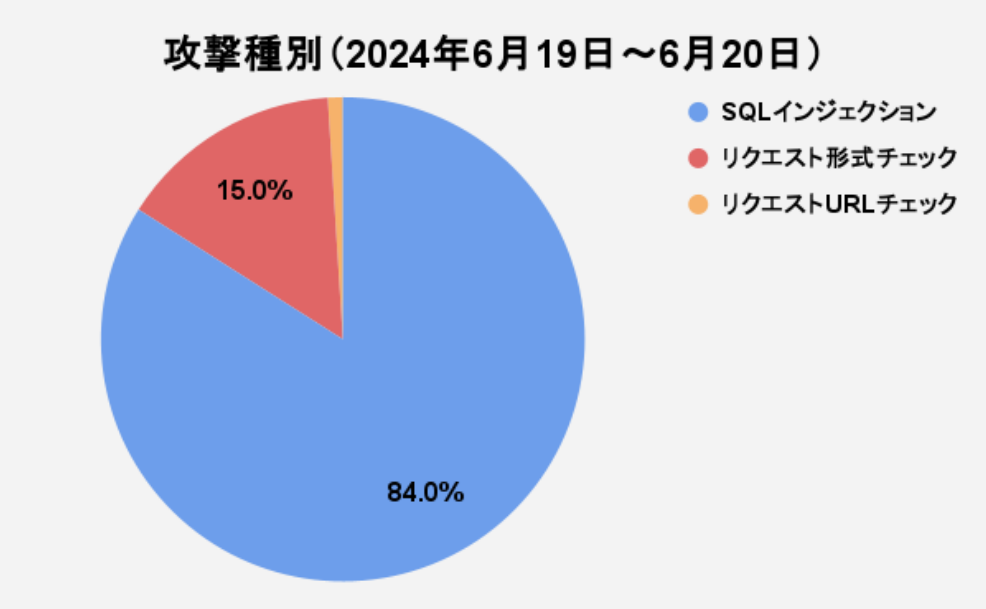

図 5 攻撃種別（2024 年 6 月 19 日～6 月 20 日）

【2024 年上半期の傾向】

■2024 年上半期に最も多かった攻撃は「SQL インジェクション」

2024 年上半期における攻撃種別の割合は以下の通りです。第 1 四半期（1 月～3 月）、第 2 四半期（4 月～6 月）ともに SQL インジェクションによる攻撃が最多で、特に第 2 四半期では SQL インジェクションの検出数が過半数を超え、2 番目に多かったリクエスト URL チェックの 3 倍以上と大差をつける結果となりました。

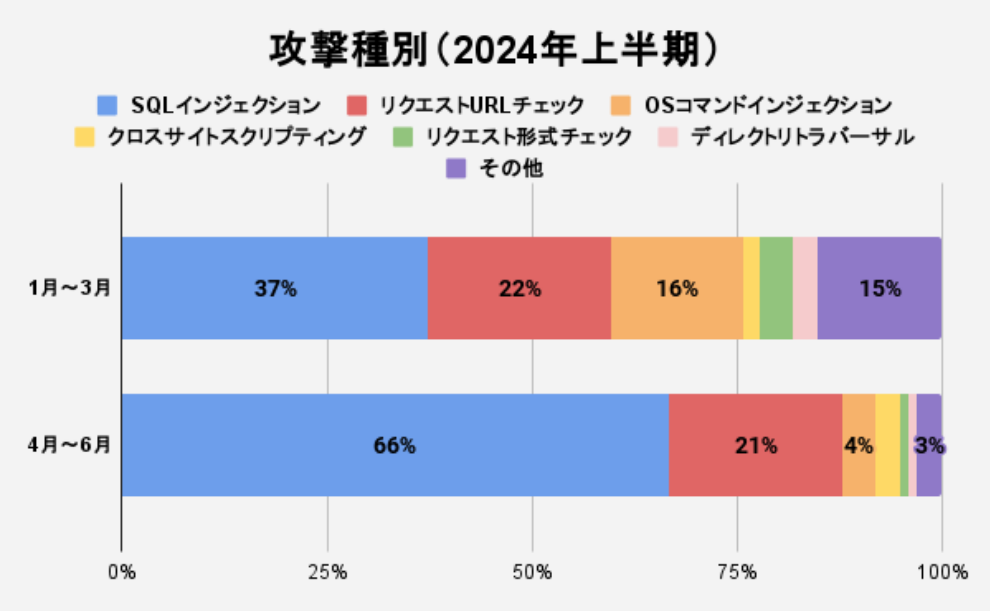

図 6 攻撃種別（2024 年上半期）

SQL インジェクションとは、Web アプリケーションの脆弱性を悪用し、Web サイトの入力フォームなどに不正にデータベースを操作する SQL 文を入力することで、認証回避（不正ログイン）やデータベース内の情報を窃取する攻撃です。冒頭の「図 1 攻撃種別の分類（2024 年 4 月～6 月）」の内容でも確認できるように、SQL インジェクションが多数検出されており、世間でも SQL インジェクションによる情報漏えい被害が確認されています。

■攻撃アクセスの検出推移（2024 年 1 月～6 月）

以下は、2024 年上半期（1 月～6 月）の攻撃アクセス検出の推移です。第 1 四半期と比べると、第 2 四半期の攻撃アクセスは減少しました。しかし、4 月から 6 月にかけて攻撃アクセスは増加しており、なかでも 6 月は 4 月の約 2 倍の攻撃アクセスが検出されているため、今後も引き続きセキュリティ対策の徹底が必要です。

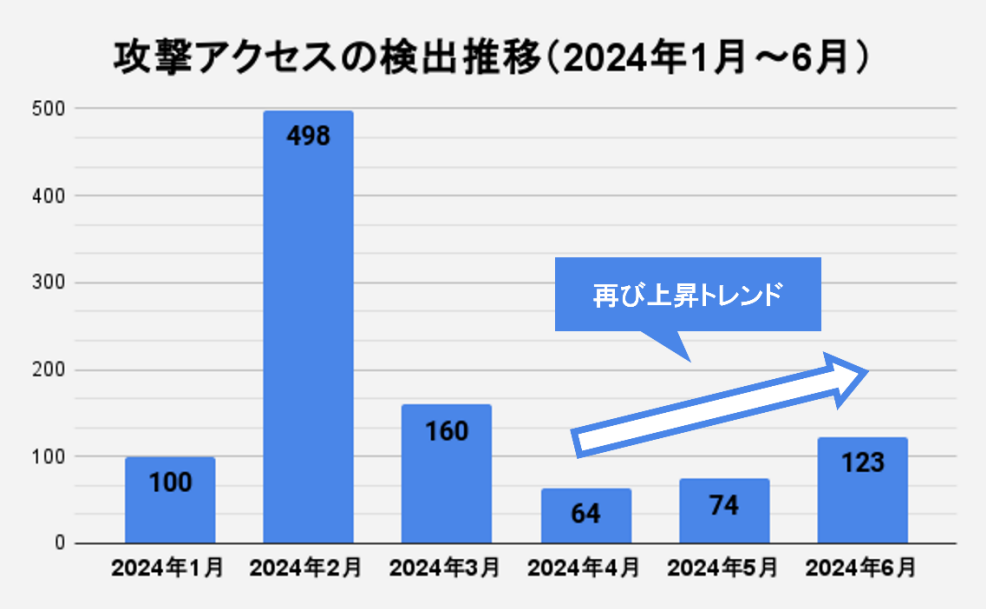

図 7 検出の推移（2024 上半期） ※2024 年 1 月を 100 とした場合で算出

【サイバーセキュリティ分析担当 コメント】

SQL インジェクションの根本的対策は、セキュアな Web アプリケーションの開発・実装です。Web アプリケーションに SQL インジェクションの脆弱性がなければ、SQL インジェクションの攻撃を受けても影響はありません。しかし、Web アプリケーションの改良の中で対策漏れが生じてしまうことや、直ぐに修正できない脆弱性が存在する場合もあるかもしれません。このような実情から根本的な対策を基本としつつ、別のアプローチでの対策が求められ、Web アプリケーションの脆弱性有無とは独立した形で攻撃を防御できる WAF の活用が有効となります。EG セキュアソリューションズ株式会社が開発する WAF「SiteGuard」シリーズは様々なニーズに合わせた WAF をご提供しています。SQL インジェクションをはじめ、多種多様な Web アプリケーションの脆弱性を悪用する攻撃の対策に WAF の導入をご一考いただければと存じます。

【「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】

SITEGUARD

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/）

【イー・ガーディアングループ 概要】

1998 年設立。2016 年に東証一部上場。2022 年に東証プライム市場へ移行。イー・ガーディアンはネットパトロール、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する総合ネットセキュリティ企業です。センターは、提携先を含めてグループで国内 8 都市海外 3 都市 19 拠点の業界最大級の体制を誇ります。昨今は Fintech・IoT 業界への参入や RPA 開発による働き方改革への寄与など、時代を捉えるサービス開発に従事し、インターネットの安心・安全を守っております。

■EG セキュアソリューションズ 会社概要

代表者　：代表取締役　高谷 康久
所在地　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　：2008 年 4 月
資本金　：1,000 万円（2024 年 3 月末日現在）
業務内容　：1. 情報セキュリティ、情報システムに関する監査、コンサルティング
2. 情報セキュリティに関する調査、研究、執筆
3. 情報セキュリティ関連の教育及びコンテンツ制作
4. セキュリティ製品の開発、販売、サポート
URL　：https://www.eg-secure.co.jp/

■イー・ガーディアン株式会社 会社概要

代表者　：代表取締役社長　高谷 康久
所在地　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　：1998 年 5 月
資本金　：1,967 百万円（2024 年 3 月末日現在）
業務内容　：ブログ・SNS・掲示板企画コンサルティング/リアルタイム投稿監視業務/ユーザーサポート業務/
オンラインゲームカスタマーサポート業務/コンプライアンス対策・風評・トレンド調査業務/
コミュニティサイト企画・サイト運営代行業務・広告審査代行サービス業務/人材派遣業務
URL　：https://www.e-guardian.co.jp/