

報道関係者各位

2025年2月5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】
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
～第4四半期・年間の傾向を「攻撃種別」「月別」「接続元(地域別)」で分析～

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 4 四半期 (2024 年 10 月 1 日～12 月 31 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 (2024.4Q)」を発表いたします。また、同時に、2024 年 1 年間の分析データを総括した「SiteGuard セキュリティレポート 2024」をダウンロード資料として公開いたします。

「SiteGuard セキュリティレポート 2024」ダウンロード URL：

<https://siteguard.jp-secure.com/resources/siteguard-security-report-2024-annual>



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通り提供しております。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 4 四半期の攻撃傾向を「攻撃種別」「月別」「接続元(地域)」の 3 つの観点から発表いたします。

■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」も多数検出し、この2つの検出で8割以上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、2024年第2四半期までは「その他」に分類していましたが、2024年第3四半期以降は多数検出しているため、個別の分類にして集計しております。

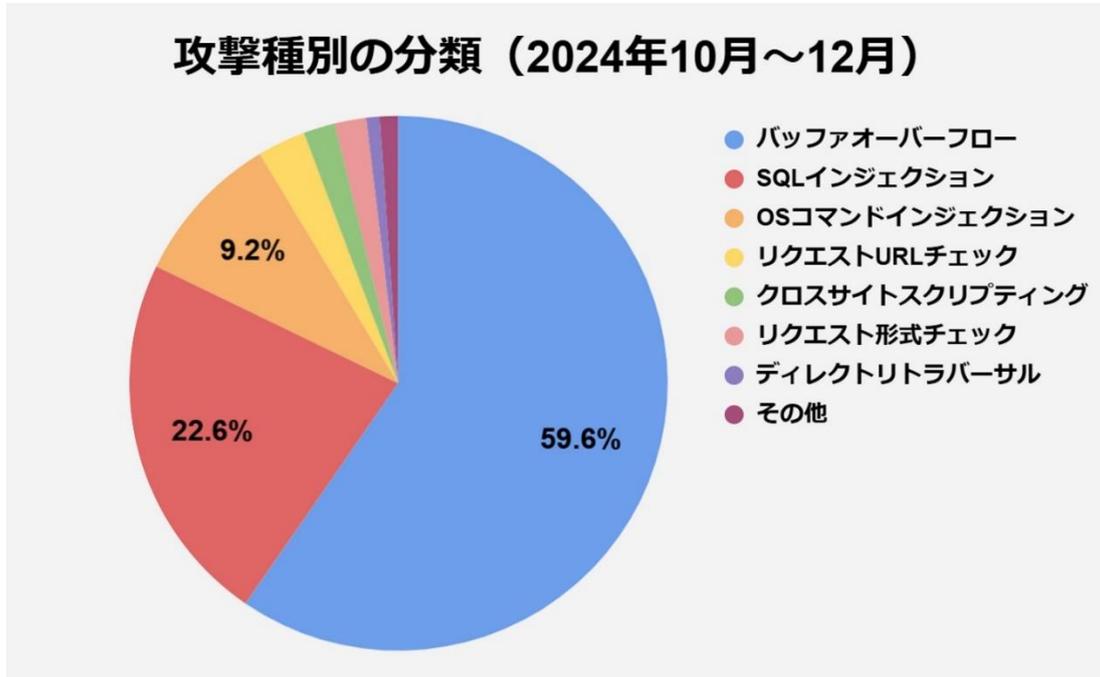


図1 攻撃種別の分類 (2024年10月～12月)

攻撃種別	割合
バッファオーバーフロー	59.6%
SQLインジェクション	22.6%
OSコマンドインジェクション	9.2%
リクエストURLチェック	2.9%
クロスサイトスクリプティング	1.9%
リクエスト形式チェック	1.9%
ディレクトリトラバーサル	0.8%
その他	1.1%

表1 攻撃種別の分類 (2024年10月～12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。10月の検出を100とした場合、11月の検出は14、12月は19となり、10月と比較して11月、12月の攻撃アクセスは大幅に減少しました。

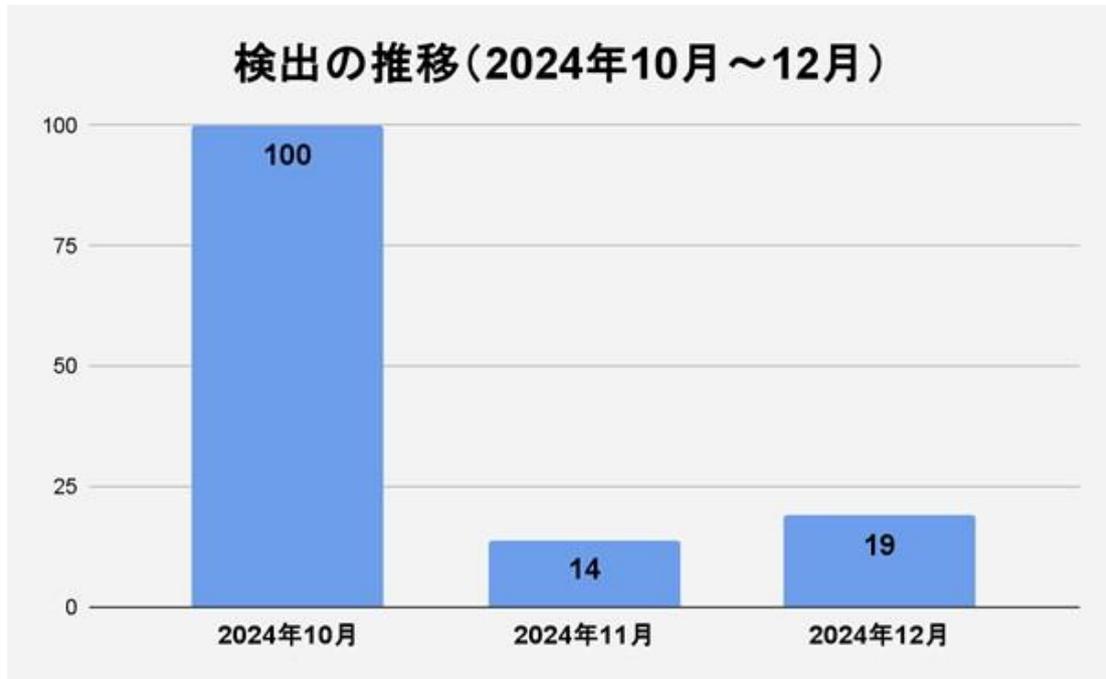


図2 検出の推移 (2024年10月～12月) ※2024年10月を100とした場合で算出

■接続元 (地域別) の分類

最後に接続元の分類です。集計期間中における地域別の検出数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5割を超え、続いて日本という結果に。前回の第3四半期と同様にアメリカ合衆国からの攻撃アクセスが半数以上を占める結果となりました。

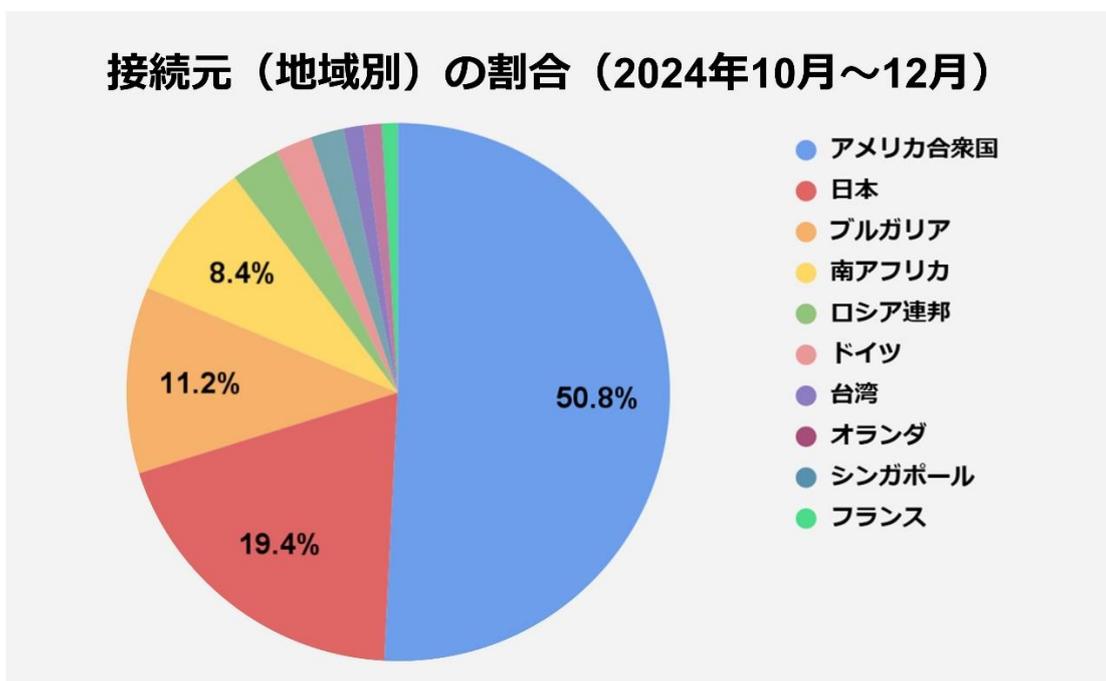


図3 接続元 (地域別) の割合 (2024年10月～12月)

順位	攻撃種別	割合
1	アメリカ合衆国	50.8%
2	日本	19.4%
3	ブルガリア	11.2%
4	南アフリカ	8.4%
5	ロシア連邦	2.9%
6	ドイツ	2.2%
7	台湾	2.0%
8	オランダ	1.2%
9	シンガポール	1.1%
10	フランス	1.0%

表 3 接続元（地域別）の割合（2024年10月～12月）

■2024年4Qの注目トピック①：バッファオーバーフロー攻撃の減少

2024年3Qの8月から急増したバッファオーバーフロー攻撃は10月まで続き、11月に減少しました。検出の割合として、2024年3月の検出を100とした場合、10月の検出は1887、11月は7、12月は2となりました。



図 4 バッファオーバーフロー攻撃検出推移（2024年1月～12月）

■2024年4Qの注目トピック：SQLインジェクション攻撃を多数検出

10月と11月にSQLインジェクション攻撃を多数検出。10月はそれぞれ異なる地域の接続元（日本、ブルガリア、アメリカ合衆国）から様々なWebサイトに対する攻撃アクセスでした。

11月は4回のピーク（8日,12日,19日,21日）があり、これら全てが日本国内の特定の接続元（3種類のIPアドレス）から、4つのWebサイトに対する攻撃でした。なかでも、8日,19日,21日の3日間においては、1つのIPアドレスから特定のWebサイト（アパレル商社）に対してSQLインジェクション攻撃が集中的に行われていました。

【セキュリティ研究所 所長 直岡克起 コメント】

前期から引き続き10月に多く検出されたバッファオーバーフロー攻撃ですが、11月に入ってパタリと止まりました。Webクローラーのバグが原因と推察していましたが、これが改善された可能性が高いです。バッファオーバーフロー攻撃を除くと、相変わらずSQLインジェクションが最多となっています。

また、本レポートの内容と直接的な関係はありませんが、2024年の年末から年始にかけてDDoS攻撃によるシステム障害が相次ぎ、ニュースになっていました。DDoS攻撃は複数のネットワーク機器から大量にパケットを送りつけて、システム障害を引き起こす等の影響を与える攻撃です。どんなパケットをどのように送りつけるのか、いろいろな手法があり、そしていろいろな対策があります。しかし、現在のところ「この対策をしておけば必ず防げる（影響がなくなる）」というものはありません。サーバーの管理事業者やセキュリティ対策事業者と相談して、最適な対策方法を選択しましょう。DDoS攻撃を仕掛けるのは、不正なプログラムを仕掛けられたネットワーク機器の集まりであるボットネットです。ここには、乗っ取られた家庭用のルーターやネットワークカメラも含まれています。ご自宅にあるPCやルーター、ネットワークカメラが攻撃に使用されることのないよう、OS、ファームウェアの最新化、パスワードをデフォルトのものから変更する等、対策を心がけましょう。

なお、今回は2024年1年分のデータを総括した「SiteGuardセキュリティレポート2024」も公開しております。下記URLよりダウンロードが可能ですので、是非ご覧いただけますと幸いです。

「SiteGuardセキュリティレポート2024」ダウンロードURL：

<https://siteguard.jp-secure.com/resources/siteguard-security-report-2024-annual>

【「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」について】



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 9 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 9 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/>