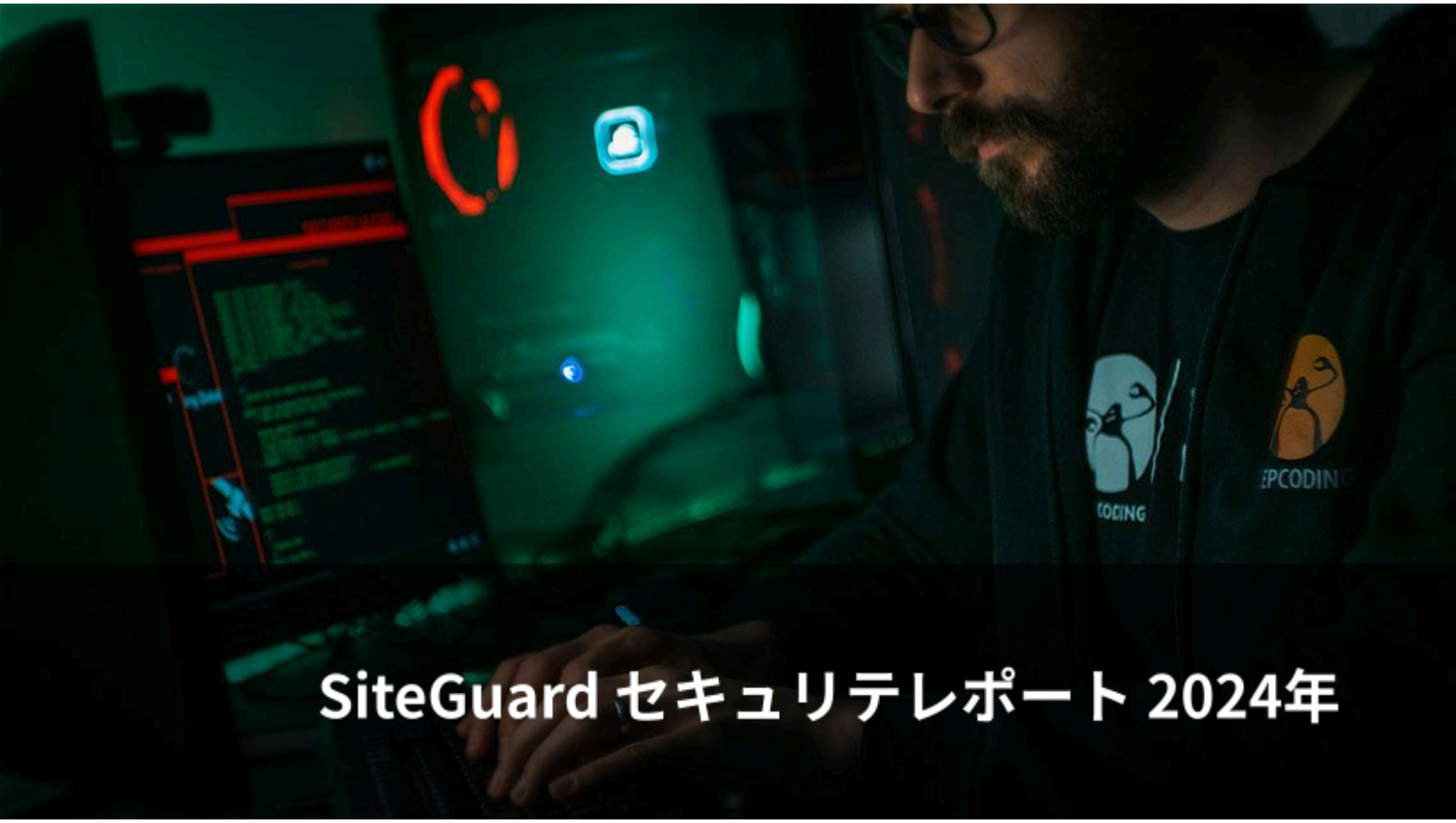

　イー・ガーディアングループは、安心・安全なインターネット環境の実現に向け、ネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供しております。特にEGセキュアソリューションズは、ネットセキュリティにおける課題解決を目的としたサービスを幅広く展開しており、WAF製品「SiteGuardシリーズ」は、累計導入サイト数・累計導入社数でNo.1※を獲得いたしました。

　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年の「月別の検出推移」「攻撃種別」「接続元（地域別）」3つの観点から1年間の攻撃傾向を発表いたします。

1. 月別の検出（バッファオーバーフロー含む）

1月の検出を100とした場合の検出推移と1サイトあたりの検出数は以下のようになります。月毎の総検出数と保護対象サイト数により1サイトあたりの検出数を概算しています。7月以降に急増したバッファオーバーフロー攻撃により2024年下期は検出数が増加しました。

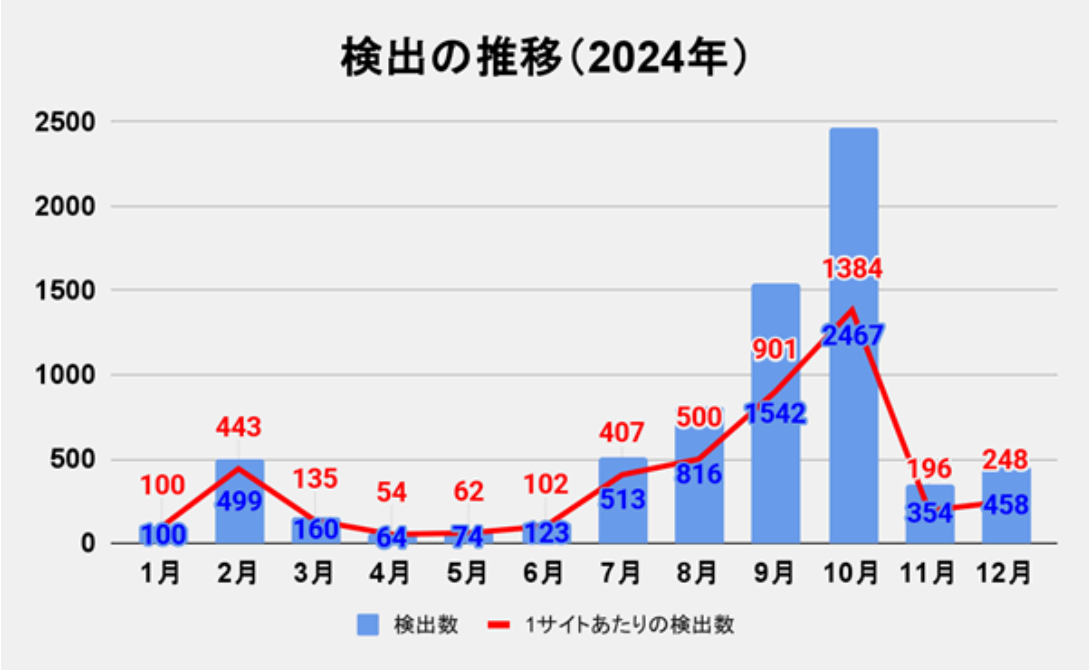

図1 検出の推移（2024年）
※2024年1月を100とした場合で算出

2. 攻撃種別（バッファオーバーフロー含む）

2024年に検出した攻撃を分類すると以下のようになります。1年間を通して「バッファオーバーフロー」が最多となりました。「SQLインジェクション」「OSインジェクション」も多数検出し、この3つの検出で約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、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います。

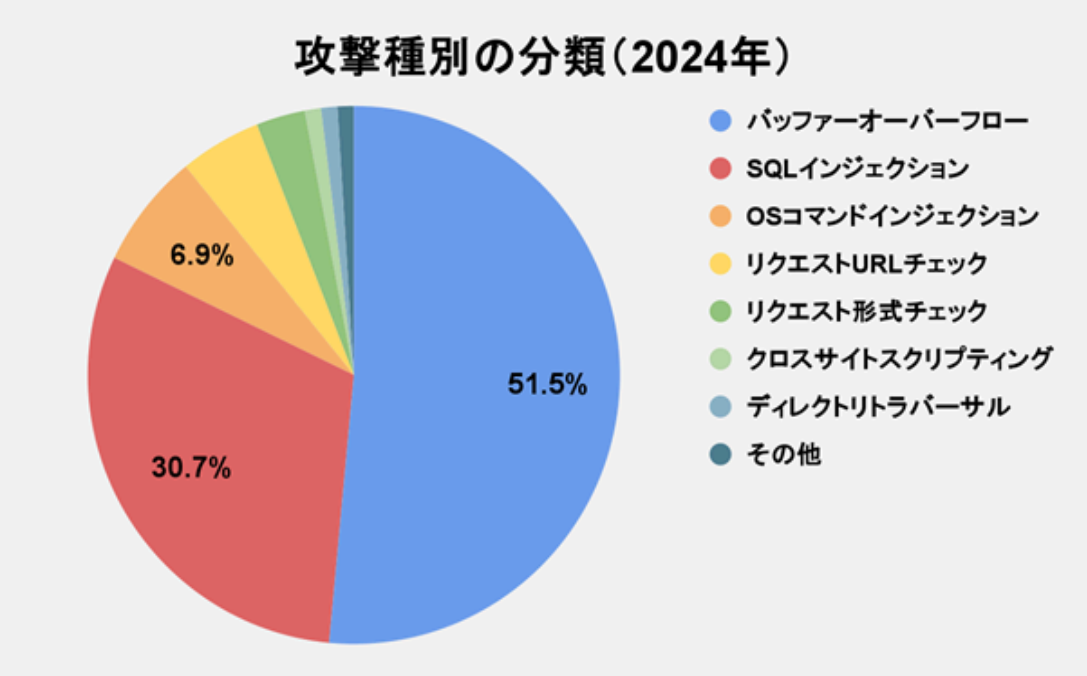

図2 攻撃種別の分類（2024年）

3. 接続元（地域別）の分類（バッファオーバーフロー含む）

次に接続元の分類です。2024年の地域別の検出数は以下の通りでした。1年間を通して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。「バッファオーバーフロー」を多数検出したことによってアメリカ合衆国が最多となりました。

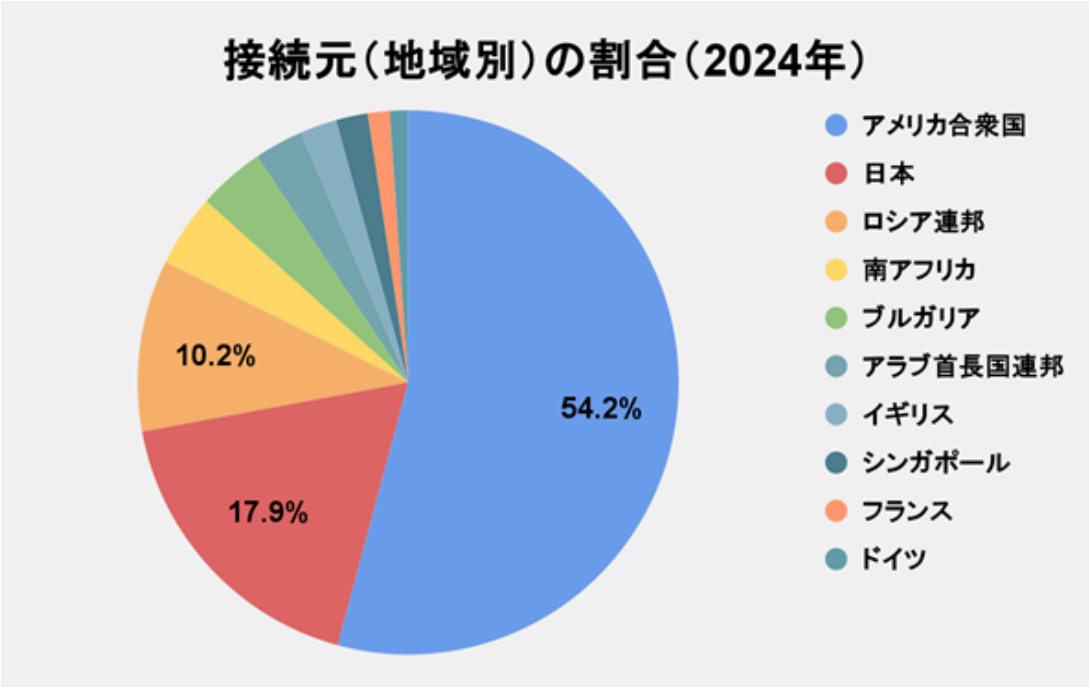

図3 接続元（地域別）の分類（2024年）

バッファオーバーフロー攻撃検出件数の影響とレポートへの考慮について

7月から10月の4か月間でバッファオーバーフロー攻撃を特定のWebサイトで多数検出しました。以下の図4は、2024年3月の検出を100とした場合の検出推移で、3月と比較して10月は18倍以上も検出しました。

7月からの4か月で検出したリクエストは、ほぼすべて類似したパターンのリクエストでした。リクエストの中身から攻撃と明確に判断できず、また通常リクエストとも見られませんでした。しかし、User-Agentには、Amazon-bot、Baidu-botを示す文字が含まれているため、Webサイトの構成や設定によって引き起こされたWebクローラーのバグが原因のリクエストと推察しています。このリクエストは2024年に検出したリクエスト全体の51%を占めました。そのため、後述ではバッファオーバーフローを除いた形で分析結果を改めて発表いたします。

※バッファオーバーフロー攻撃について、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します。

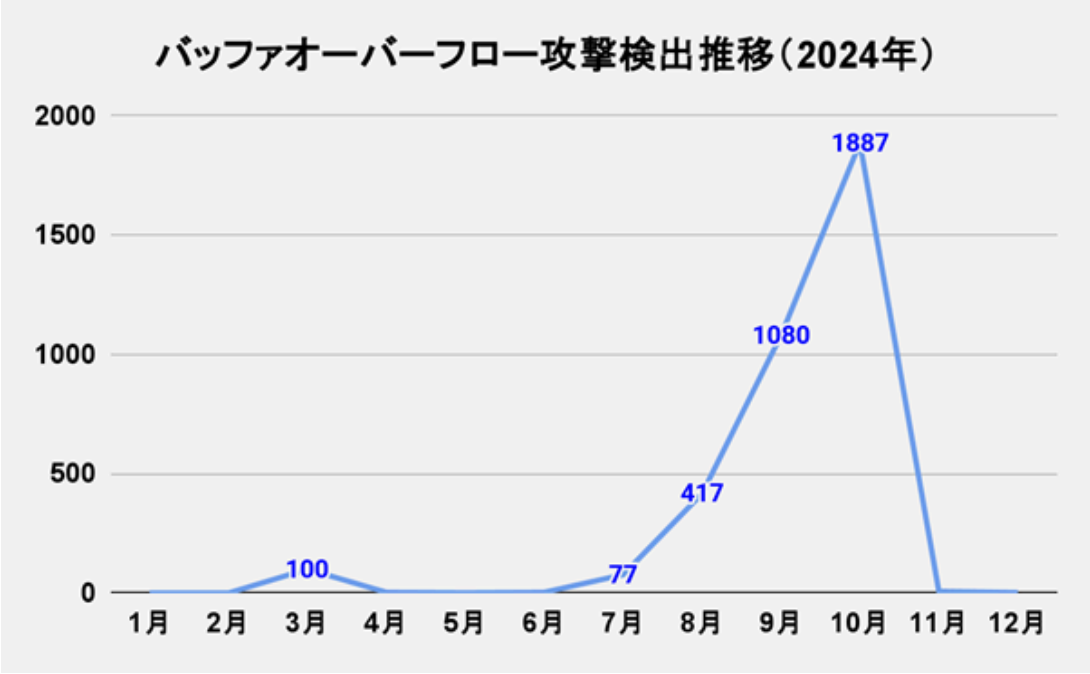

図4 バッファオーバーフロー攻撃検出推移（2024年）
※2024年3月を100とした場合で算出

4. 月別の検出

1月の検出を100とした場合の検出推移と1サイトあたりの検出数は以下のようになります。月毎の総検出数と保護対象サイト数により1サイトあたりの検出数を概算しています。

7月以降は検出が増加している傾向ですが、2月は1月と比較して約5倍の検出があり、通年通して、1サイトあたりの検出数は最多という結果になりました。

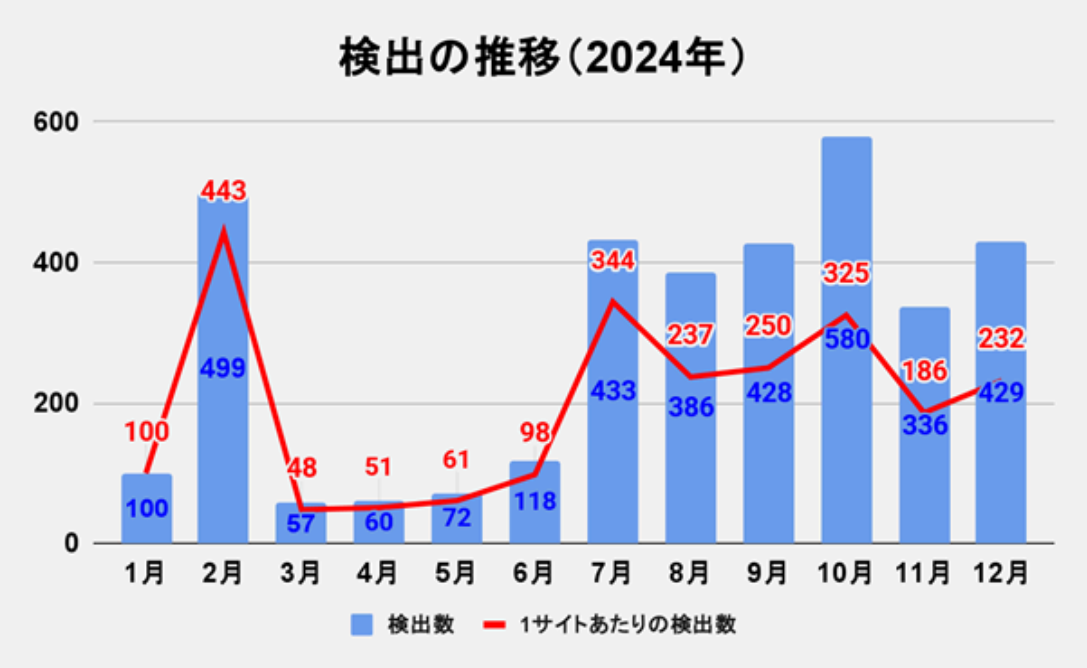

図5 検出の推移（2024年）
※2024年1月を100とした場合で算出

5. 攻撃種別

2024年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「OSコマンドインジェクション」が上位となり、この2つの検出で7割を占める結果になりました。

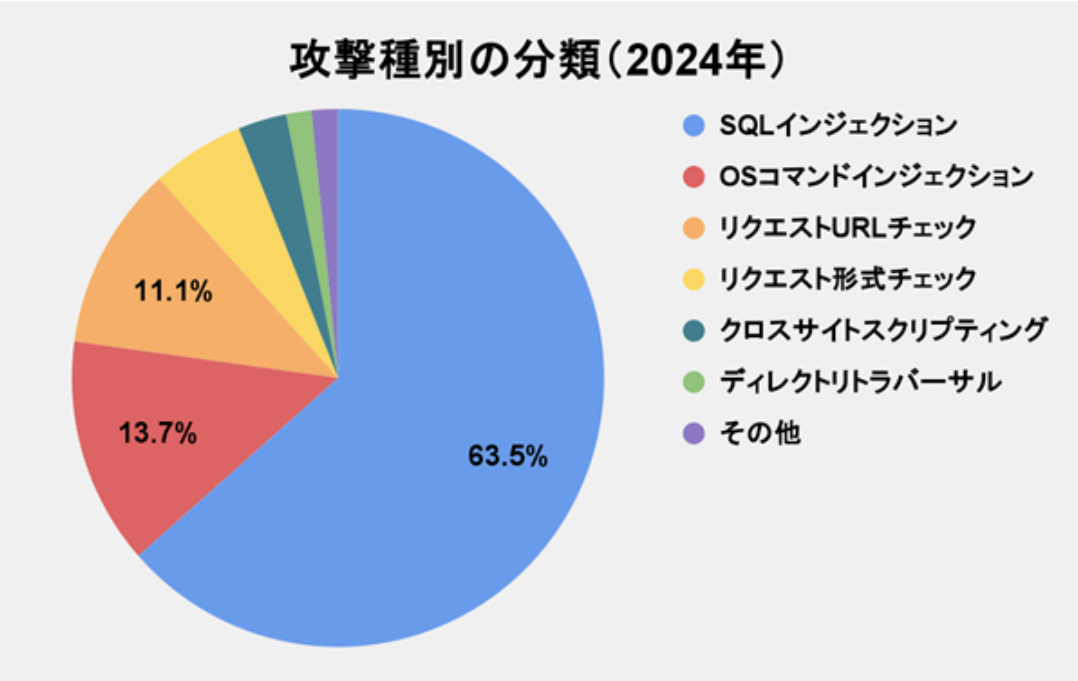

図6 攻撃種別の分類（2024年）

攻撃種別	集計期間中の割合
SQLインジェクション	63.5%
OSコマンドインジェクション	12.7%
リクエストURLチェック	11.1%
リクエスト形式チェック	5.6%
クロスサイトスクリプティング	3.0%
ディレクトリトラバーサル	1.5%
その他	1.6%

表6 攻撃種別の分類（2024年）

以下の図7は、1年間で最も多く検出された7月の「SQLインジェクション」の検出数を100とした場合の推移です。12月を除き、毎月「SQLインジェクション」が最も多く検出された種別となり、「SQLインジェクション」の危険性が確認できます。

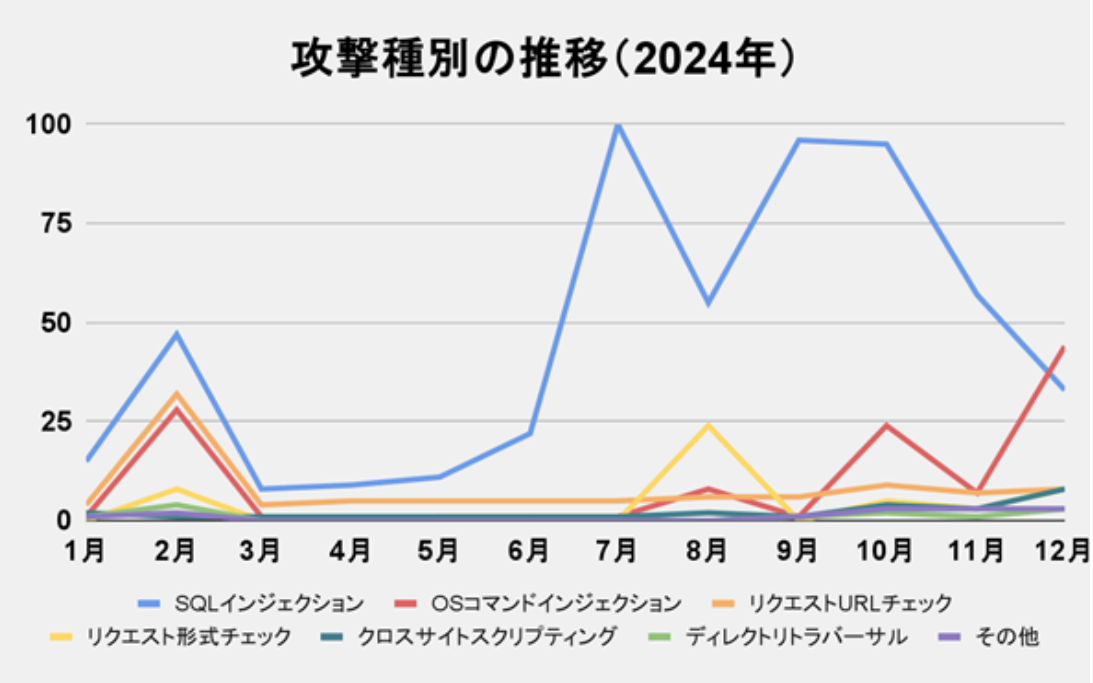

図7 攻撃種別の推移（2024年）
※2024年7月「SQLインジェクション」を100とした場合で算出

6. 接続元（地域別）の分類

接続元の分類です。2024年の地域別の検出数は以下の通りでした。日本からの攻撃アクセスが最多で3割程度となり、続いてアメリカ合衆国、ロシア連邦という結果に。日本、アメリカ合衆国からの攻撃アクセスで5割を占める結果となりました。

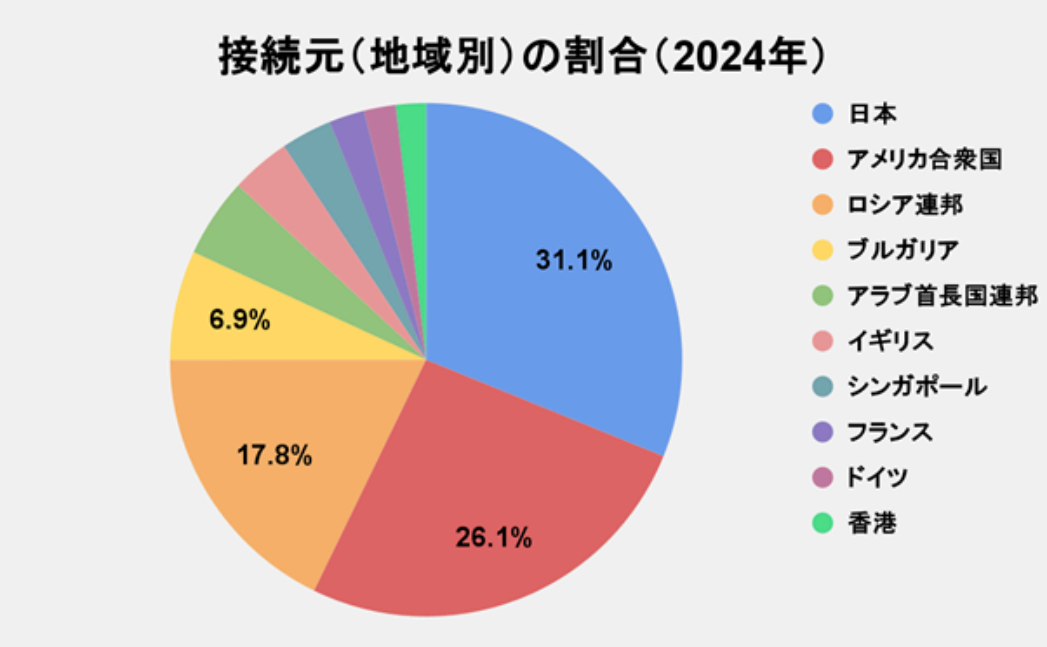

図8 接続元（地域別）の割合（2024年）

順位	国名	集計期間中の割合
1	日本	31.1%
2	アメリカ合衆国	26.1%
3	ロシア連邦	17.8%
4	ブルガリア	6.9%
5	アラブ首長国連邦	5.0%
6	イギリス	3.8%
7	シンガポール	3.2%
8	フランス	2.2%
9	ドイツ	2.0%
10	香港	1.9%

表8 接続元（地域別）の割合（2024年）

以下の図9は、1年間で最も多く検出された2月の「ロシア連邦」の検出数を100とした場合の推移です。2月の「ロシア連邦」からの攻撃数が最多となりました。2024年下期になると各接続元からの検出は増加し、上期での検出は多くなかった「日本」が1年間を通して最多となる結果となりました。

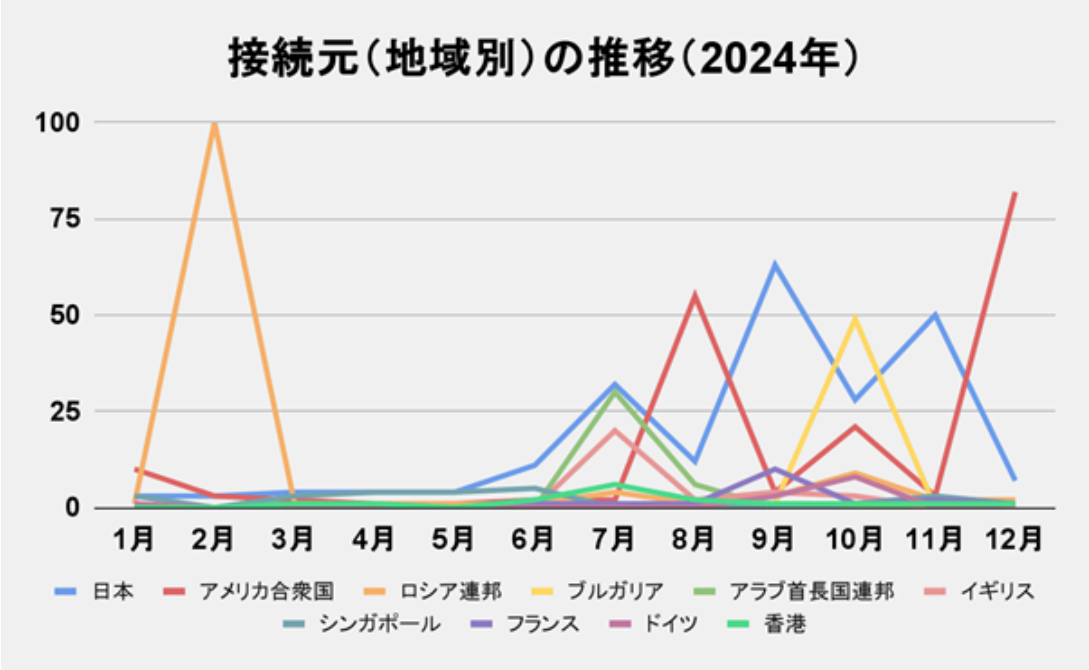

図9 接続元（地域別）の推移（2024年）
※2024年2月「ロシア連邦」を100とした場合で算出

7. 2024年の注目トピック：SQLインジェクションの検出

接続元の分類です。2024年の地域別の検出数は以下の通りでした。日本からの攻撃アクセスが最多で3割程度となり、続いてアメリカ合衆国、ロシア連邦という結果に。日本、アメリカ合衆国からの攻撃アクセスで5割を占める結果となりました。SQLインジェクションは2024年に検出した攻撃の分類で最多となりました。以下の図10は、1月の検出を100とした場合の検出推移です。1サイトあたりの検出数は、月毎の総検出数と保護対象サイト数により検出数を概算しています。

1月と比較して7月以降は増加した傾向となり、検出数、1サイトあたりの検出数ともに7月が最多となりました。

※SQLインジェクションは、Webアプリケーションの実装の不備を悪用し、外部からSQL文を含んだリクエストを送信して不正にデータベースを操作する攻撃です。OWASP Top10にもランクインするなど、危険なサイバー攻撃です。

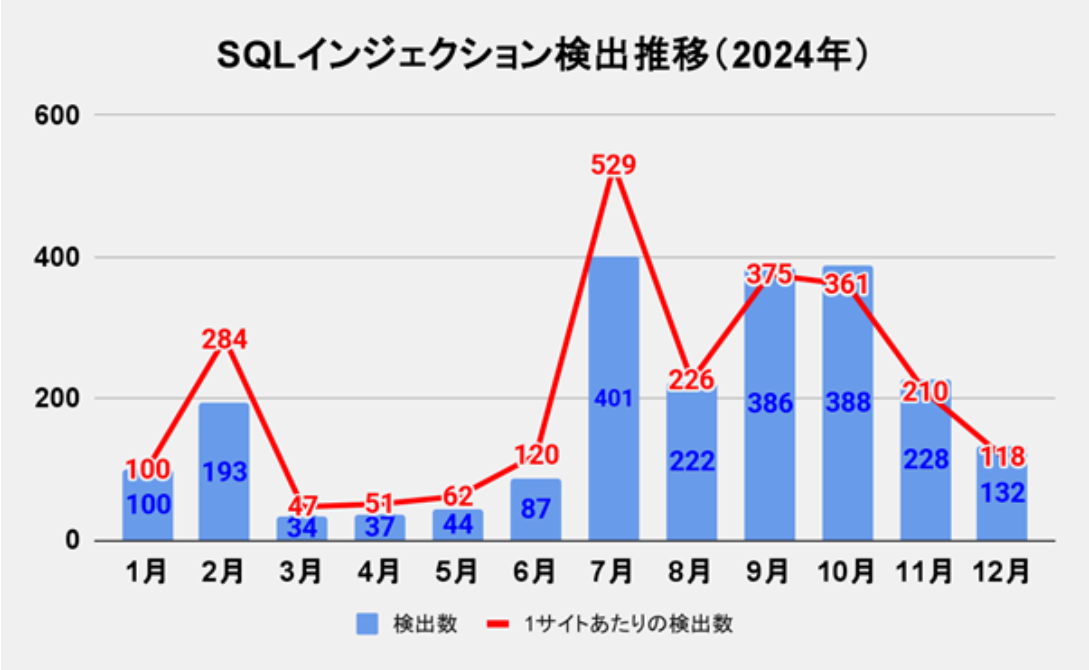

図10 SQLインジェクション検出推移（2024年）
※2024年1月を100とした場合で算出

8. 2024年のコメント

　当社で開発しているWAF製品「SiteGuardシリーズ」はソフトウェア型の販売を2008年から開始しており、クラウド型の「SiteGuard Cloud Edition」は2022年10月にリリースいたしました。「SiteGuard セキュリティレポート」は、このCloud Editionの検出情報を活用し、何かしら社会に貢献できるかもしれないとの思いで2024年1月より発表しております。

EGセキュアソリューションズのセキュリティ研究所では、SiteGuardシリーズのルールの継続的な改善のほか、WAFの検知エンジンの改良、ユーザビリティ向上のための機能などの研究開発に取り組んでいます。クラウドサービスプロバイダーがそろって標準WAFを提供し、WAFがコモディティ化する中、SiteGuardを選んでいただける要素を増やし続けてまいります。

Web Applicatiton FirewallのSiteGuardシリーズを今後ともよろしくお願いいたします。

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、セキュリティの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