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。2025年第1四半期の「攻撃種別」「月別」「接続元（地域別）」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（2025年1月～3月）に検出した攻撃種別の割合は以下のようになります。最も多かったのは「SQLインジェクション」で全体の37.5%を占め、次いで「リクエストURLチェック」が34.2%となりました。この2つの検出で全体の71%を占める結果になりました。

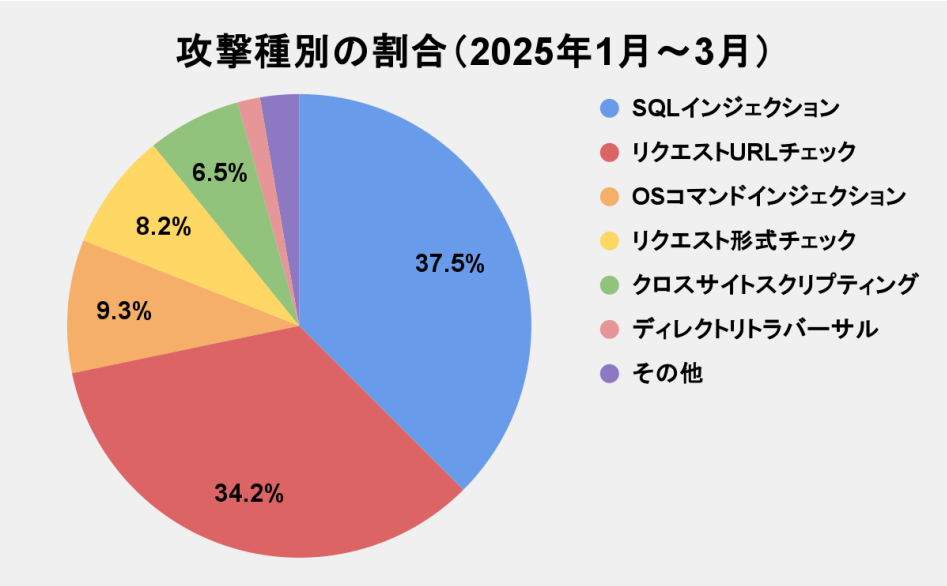

図1 攻撃種別の分類（2025年1月～3月）

攻撃種別	集計期間中の割合
SQLインジェクション	37.5%
リクエストURLチェック	34.2%
OSコマンドインジェクション	9.3%
リクエスト形式チェック	8.2%
クロスサイトスクリプティング	6.5%
ディレクトリトラバーサル	1.6%
その他	2.7%

表1 攻撃種別の分類（2025年1月～3月）

2. 月別の検出数

月別総検出数の推移と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。2025年1月の検出数を100とした場合、2月の検出数は221（約121%増）、3月は565（約465%増）となり、1月と比較して2月、3月の攻撃アクセスは大幅に増加しました。

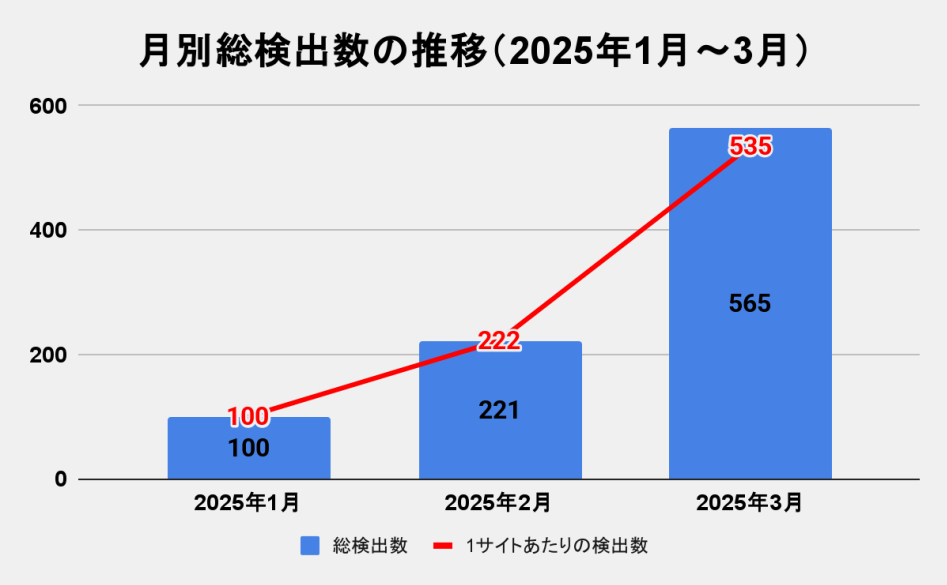

図2 月別総検出数の推移（2025年1月～3月）
※2025年1月を100とした場合で算出

3. 接続元（地域別）の分類

次に接続元（地域別）です。集計期間中（2025年1月～3月）の地域別検出数の割合は以下の通りでした。フィンランドからの攻撃アクセスが36.6%と最も多く、次いで日本が22.3%となりました。フィンランドが初めて最多となりました。

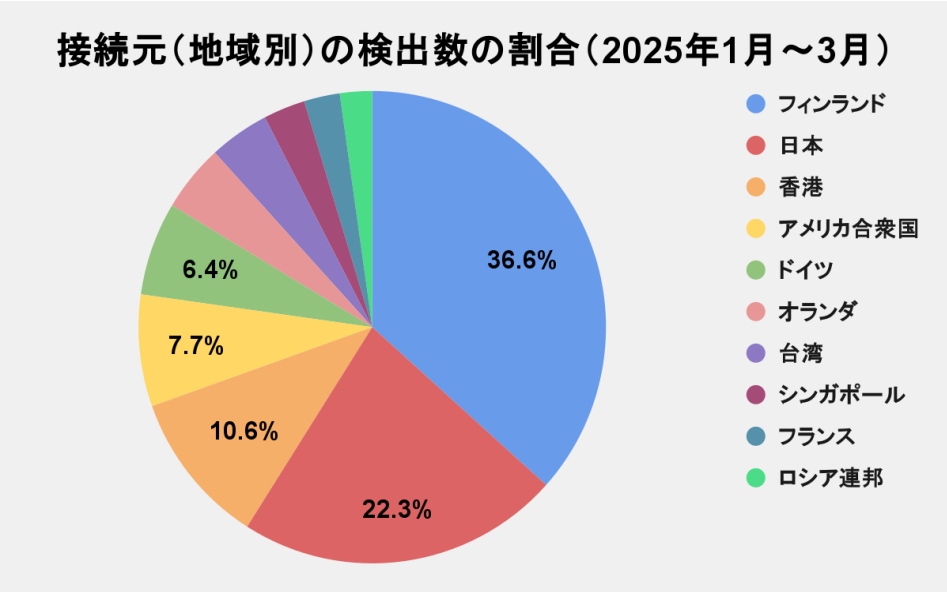

図3 接続元（国別）の割合（2025年1月～3月）

順位	地域	集計期間中の割合
1	フィンランド	36.6%
2	日本	22.3%
3	香港	10.5%
4	アメリカ合衆国	7.6%
5	ドイツ	6.4%
6	オランダ	4.6%
7	台湾	4.1%
8	シンガポール	2.8%
9	フランス	2.4%
10	ロシア連邦	2.2%

表2 接続元（地域別）の割合（2025年1月～3月）

4. 2025年第1四半期の注目トピック：特定のWEBサイトへの攻撃が急増

2月27日、3月1日～3月2日、3月8日～3月9日に特定のWebサイト（教育機関）への攻撃アクセスが急増しました。2月27日と3月1日～3月2日の攻撃アクセスは、フィンランドの異なるIPアドレスで攻撃アクセスを検出し、3月8日～3月9日の攻撃アクセスは日本のIPアドレスからの攻撃アクセスでした。

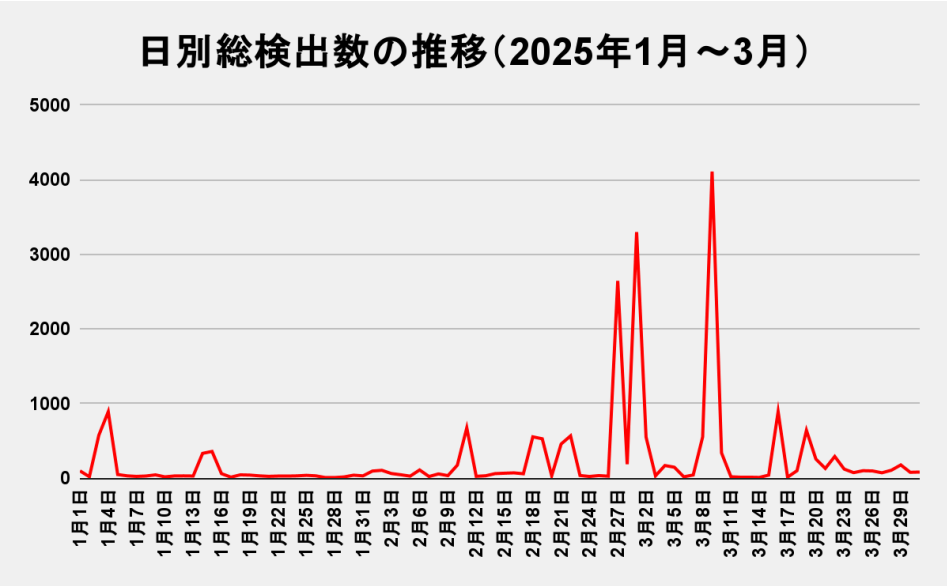

図4 日別総検出数の推移（2025年1月～3月）
※2025年1月1日の検出数を100とした場合で算出

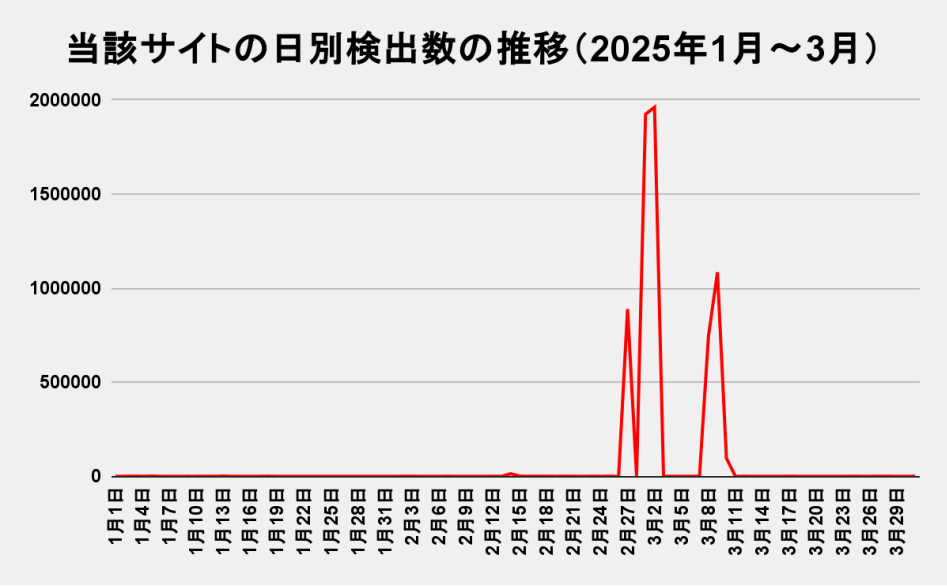

図5 当該サイトの日別検出数の推移（2025年1月～3月）
※2025年1月1日の検出数を100とした場合で算出

また、過去のデータ分析では、攻撃アクセスが急増する際、SQLインジェクションなど特定の攻撃種別に限られる傾向が見られましたが、今回顕著だったのは、フィンランドと日本の両方で、様々な攻撃種別の攻撃アクセスが見られました。

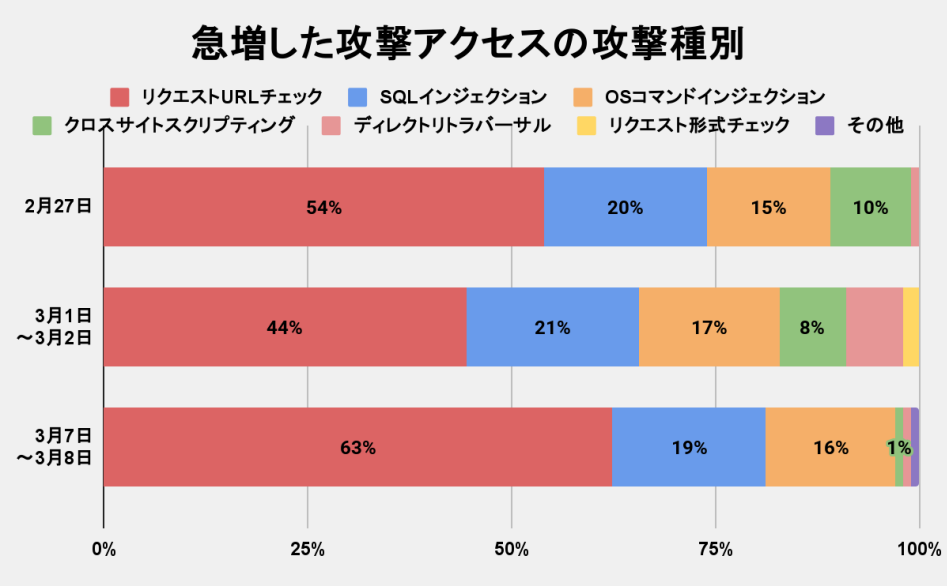

図6 急増した攻撃アクセスの攻撃種別

5. 2025年第1四半期のコメント

攻撃種別の分類で2番目に多かった「リクエストURLチェック」は、Webサイトで通常公開されることのない、OSやミドルウェア、Webアプリケーションフレームワークで使用される設定ファイル、データファイル、バックアップファイル等を取得しようとする攻撃です。これらのファイルは、意図的に公開していなくても、設定ミスやトラバーサル等の脆弱性によって取得可能な状態になっている場合があります。

この攻撃種別はSQLインジェクションに次ぐ2位となりました。過去にも二度（2024年1Qと2Q）、2位になったことがあります。注目トピックで取り上げた「急増した攻撃」の中で、この攻撃種別が約半数を占めたことが要因となりました。

公開を意図していないファイルが公開状態になっていると、情報漏洩やシステムへの不正アクセスにつながる場合があります。これを防止するには、ファイルの配置場所についてのルールの見直し、Webサーバーの設定等によるアクセス制御等を検討してください。また、定期的な脆弱性診断、監査を行うことも有効です。

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　ディレクター　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://www.eg-secure.co.jp/siteguard