



SiteGuard セキュリテレポート

2025年第2四半期

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 セキュリテレポート」を作成しました。2025年第2四半期の「攻撃種別」「月別」「接続元（地域別）」「サイトジャンル」「接続元IPアドレス」の5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4月～6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64.5%を占め、次いで「リクエストURLチェック」が10.9%となりました。この2つの検出で全体の75%を占める結果となりました。

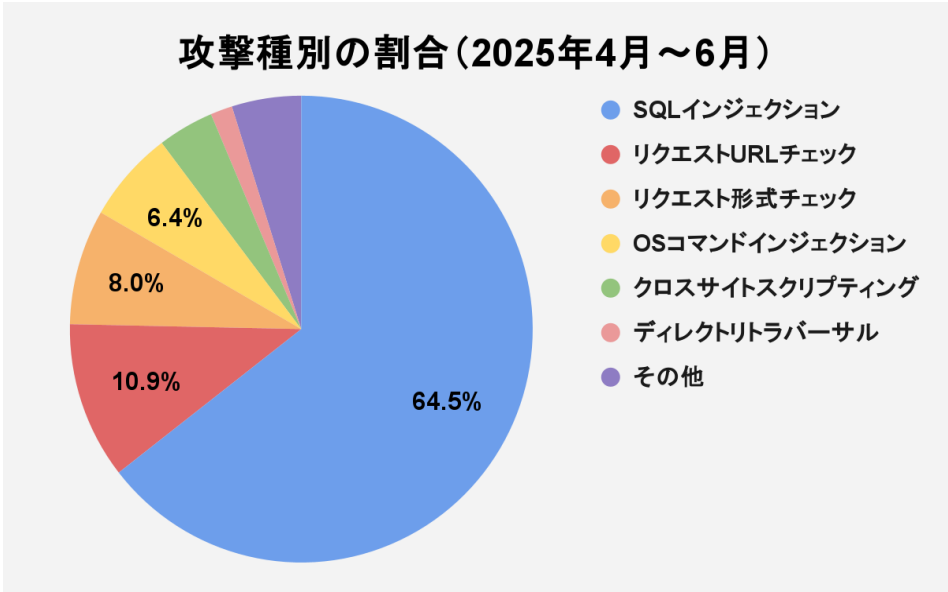


図1 攻撃種別の割合（2025年4月～6月）

攻撃種別	集計期間中の割合
SQLインジェクション	64.5%
リクエストURLチェック	10.9%
リクエスト形式チェック	8.0%
OSコマンドインジェクション	6.4%
クロスサイトスクリプティング	3.9%
ディレクトリトラバーサル	1.5%
その他	5%

表1 攻撃種別の割合（2025年4月～6月）

2. 月別の検出数

月別の検出数の推移と1サイトあたりの検出数は以下の通りです。月別の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4月の検出数を100とした場合、5月の検出数は167（約67%増）、6月は200（約100%増）となり、4月と比較して5月、6月の攻撃アクセスは増加しました。

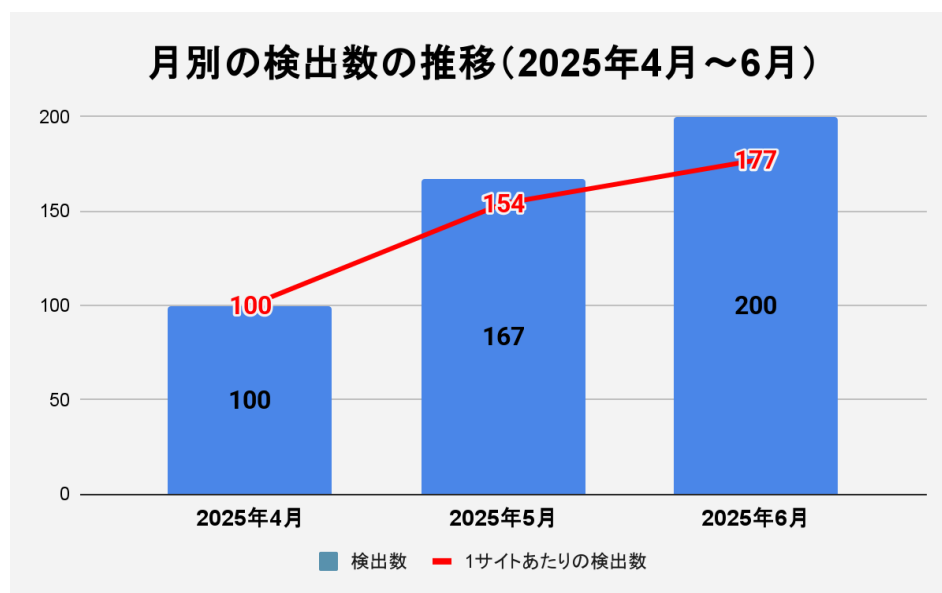


図2 月別の検出数の推移（2025年4月～6月）
※2025年4月を100とした場合で算出

2024年、2025年の上半期（1月～6月）の1サイトあたりの検出数の推移は以下の通りです。2024年1月の検出数を100とし、月別の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。最多は2025年3月で、2024年1月と比較して約647%増となりました。また、2024年の傾向では2月（443）をピークに、その後は減少傾向にありました。

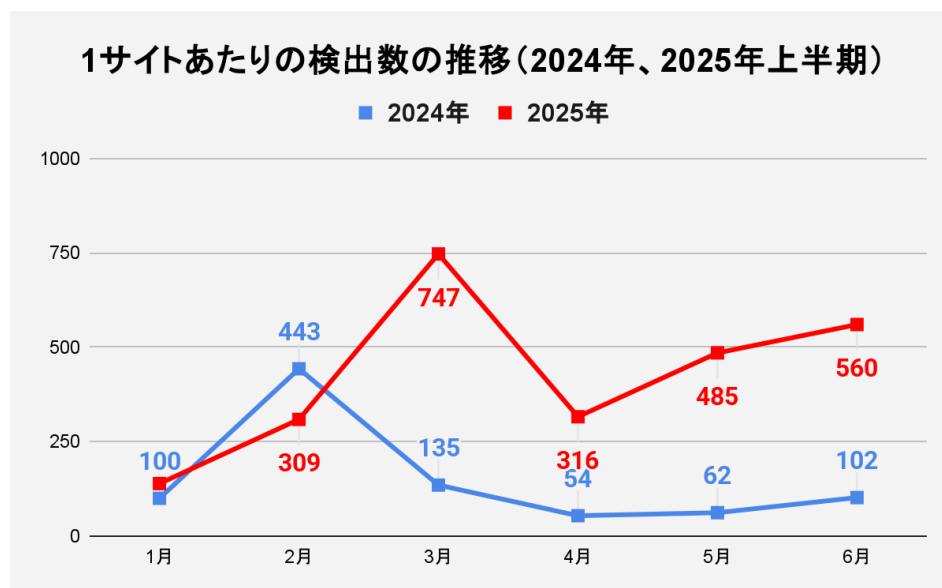


図3 1サイトあたりの検出数の推移（2024年、2025年上半期）
※2024年1月を100とした場合で算出

3. 接続元（地域別）の検出数

次に接続元（地域別）の検出数の割合です。集計期間中（2025年4月～6月）の接続元（地域別）の割合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23.5%と最も多く、次いでヨルダンが17.3%となりました。

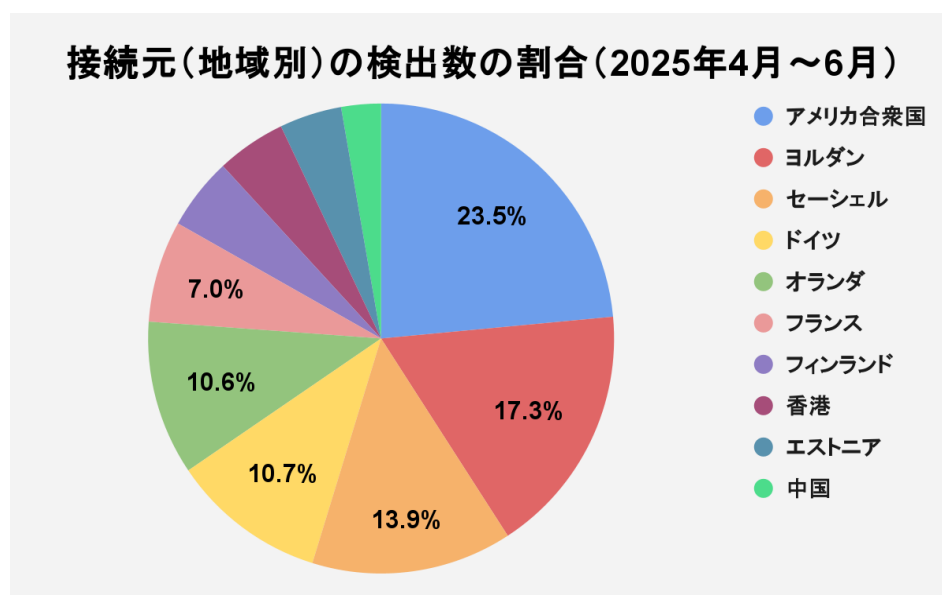


図4 接続元（地域別）の検出数の割合（2025年4月～6月）

順位	地域	集計期間中の割合
1	アメリカ合衆国	23.5%
2	ヨルダン	17.3%
3	セーシェル	13.9%
4	ドイツ	10.7%
5	オランダ	10.6%
6	フランス	7.0%
7	フィンランド	5.0%
8	香港	4.8%
9	エストニア	4.3%
10	中国	2.8%

表2 接続元（地域別）の検出数の割合（2025年4月～6月）

4. サイトジャンル毎の検出数と攻撃種別

保護対象サイトを「ECサイト」「製造業」「公共機関」「サービス業」「情報・通信」「金融機関」「医療機関」「その他」の8つのジャンルに分類し、ジャンル毎の攻撃に焦点を当て、統計を算出いたしました。

サイトジャンル毎の1サイトあたりの検出数は以下の通りです。ジャンル毎の検出数と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。サイトジャンルは最多となったECサイトの検出数を100とした場合、上位4つのジャンルは製造業が48.3、政府機関・公共機関が25.5、サービス業が20という結果になりました。

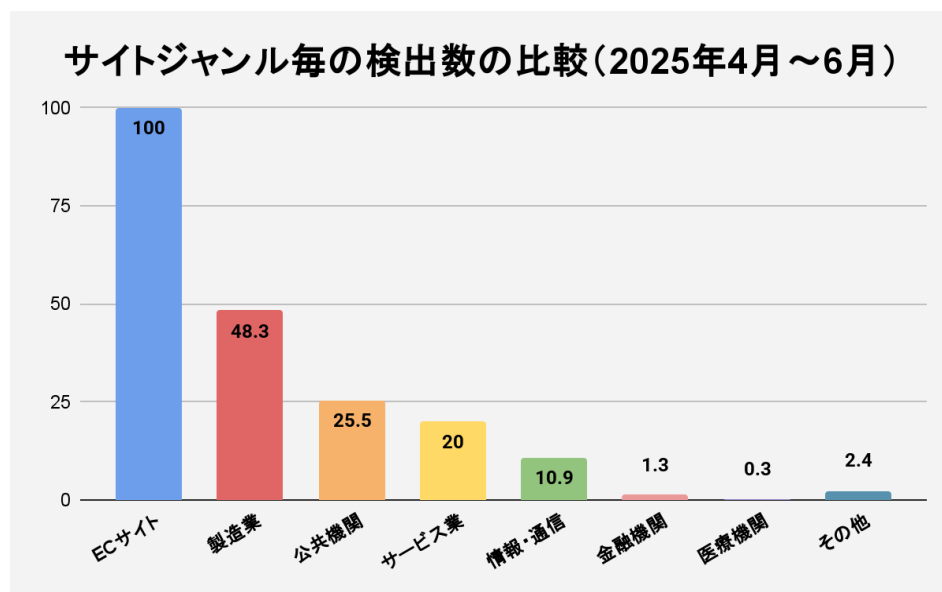


図5 サイトジャンル毎の検出数の比較（2025年4月～6月）
※ECサイトを100とした場合で算出

サイトジャンル毎の攻撃比率は以下の通りです。サイトジャンル毎の検出数をアクセス数で割って攻撃比率を算出しています。サイトジャンル毎の検出数と同様にECサイトが最多となり、製造業、公共機関という結果になりました。

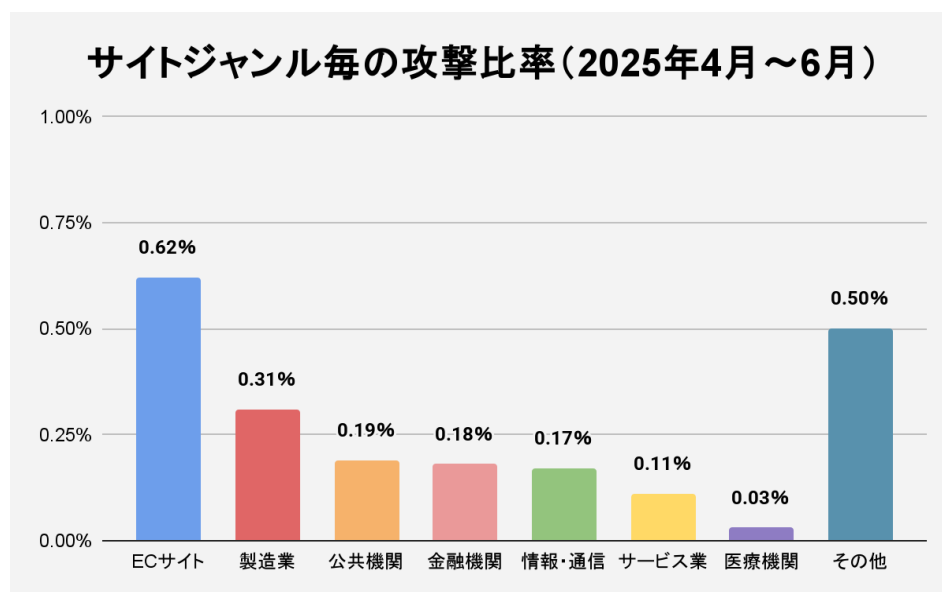


図6 サイトジャンル毎の攻撃比率（2025年4月～6月）

サイトジャンル	攻撃比率
ECサイト	0.62%
製造業	0.31%
公共機関	0.19%
金融機関	0.18%
情報・通信	0.17%
サービス業	0.11%
医療機関	0.03%
その他	0.50%

表3 サイトジャンル毎の攻撃比率（2025年4月～6月）

上位4つのサイトジャンルにおける攻撃種別の割合は以下の通りです。どのジャンルでもSQLインジェクションが最多となり、特にECサイトでは全体の85%以上を占める結果となりました。

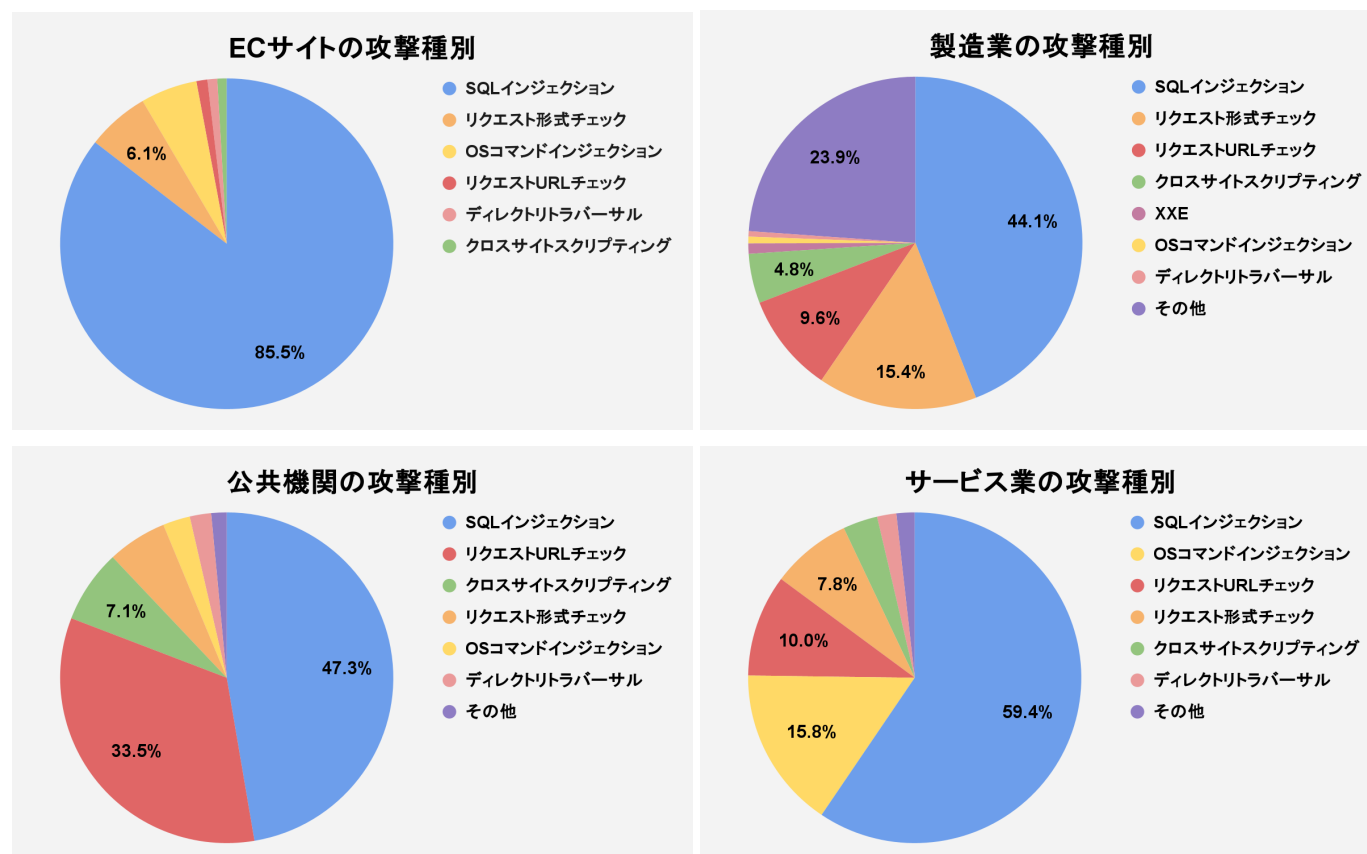


図7 サイトジャンル毎の攻撃種別（2025年4月～6月）

5. 同一接続元IPアドレスによる複数サイトへの攻撃アクセス

2025年第2四半期において、同一の接続元IPアドレスから複数のWebサイトを標的とした攻撃に焦点を当て、その統計を算出いたしました。同一の接続元IPアドレスが攻撃したWebサイト数の上位10件とその攻撃期間は以下の通りです。最も広範囲に攻撃していたIPアドレスは、保護対象サイト全体の22%ものWebサイトへの攻撃を行っていました。複数のサイトへの攻撃傾向については、接続元（地域）および攻撃期間は多岐にわたり、数日から数十日に及ぶものも確認されました。

順位	接続元IPアドレス	サイト数の割合	攻撃期間
1	非公開	22%	9日間
2	非公開	20%	25日間
3	非公開	18%	8日間
4	非公開	17%	41日間
5	非公開	16%	5日間
6	非公開	16%	8日間
7	非公開	13%	36日間
8	非公開	12%	36日間
9	非公開	11%	75日間
10	非公開	11%	1日間

表4 同一接続元IPアドレスが攻撃したWebサイト数 TOP10（2025年4月～6月）

同一の接続元IPアドレスから複数のWebサイトへの攻撃アクセスの上位10件における攻撃種別は以下の通りです。前述の集計期間全体の攻撃種別では、SQLインジェクションが最多で64.5%を占めていましたが、複数のWebサイトへの攻撃アクセスにおいては、リクエストURLチェックが最多で71.6%を占めました。特に、設定ファイル、データファイル、バックアップファイル等の取得を試みる攻撃が多数を占めました。

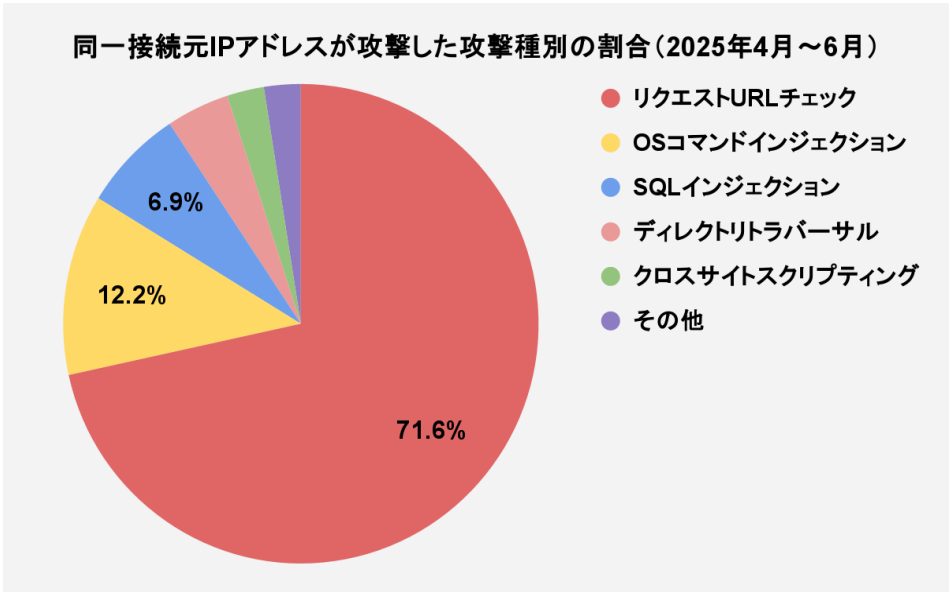


図8 同一接続元IPアドレスが攻撃した攻撃種別の割合（2025年4月～6月）

攻撃種別	攻撃種別の割合
リクエストURLチェック	71.6%
OSコマンドインジェクション	12.2%
SQLインジェクション	6.9%
ディレクトリトラバーサル	4.3%
クロスサイトスクリプティング	2.5%
その他	2.5%

表5 同一接続元IPアドレスが攻撃した攻撃種別の割合（2025年4月～6月）

6. 2025年第2四半期のコメント

今回のレポートでは、「サイトジャンル」と「同一接続元IPアドレスによる複数サイトへの攻撃」にフォーカスした統計を新たに加えました。

「サイトジャンル」毎の統計では、SiteGuard Cloud Editionをご利用いただいているサイトを8つのジャンル（その他を含みます）に分けて、検出数と攻撃比率（検出数/アクセス数）を算出しています。検出数、攻撃比率とも、トップはECサイトとなりました。ECサイトは、他のジャンルと比較して多くの攻撃にさらされていると言えます。

また、検出数が上位4位までのジャンルで、攻撃種別の割合を比較しています。全体としてもSQLインジェクションが多い傾向ですが、ECサイトのSQLインジェクションが占める割合は非常に高く、この傾向をひっばっているようです。

「同一接続元IPアドレスによる複数サイトへの攻撃」の統計では、複数のサイトへの攻撃が検出されているIPアドレスについて、攻撃先のサイト数（ご利用いただいている全サイト数に対する割合）Top10について、そのIPアドレスからの攻撃の期間と、攻撃種別の割合を取り上げています。IPアドレスについては、非公開としています。この統計結果については、実験的な側面が大きく、ここから何らかの傾向をとらえるためには、今後、他の視点からの統計と合わせて探求してまいります。

今回、2つの新しい統計を掲載いたしました。今後も様々な視点からの統計方法を模索してまいります。

EGセキュアソリューションズ株式会社 SiteGuard事業部 開発部 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://www.eg-secure.co.jp/siteguard>

※ 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>