関係者外秘

AEGIS
SERVER SECURITY

防御証明ご報告書
2025年7月

株式会社ROCKETWORKS 様

aegis-ss.jp

www.rocketworks.co.jp

発行：株式会社ROCKETWORKS 東京都港区東麻布2-15-1-4F

Rocketworks

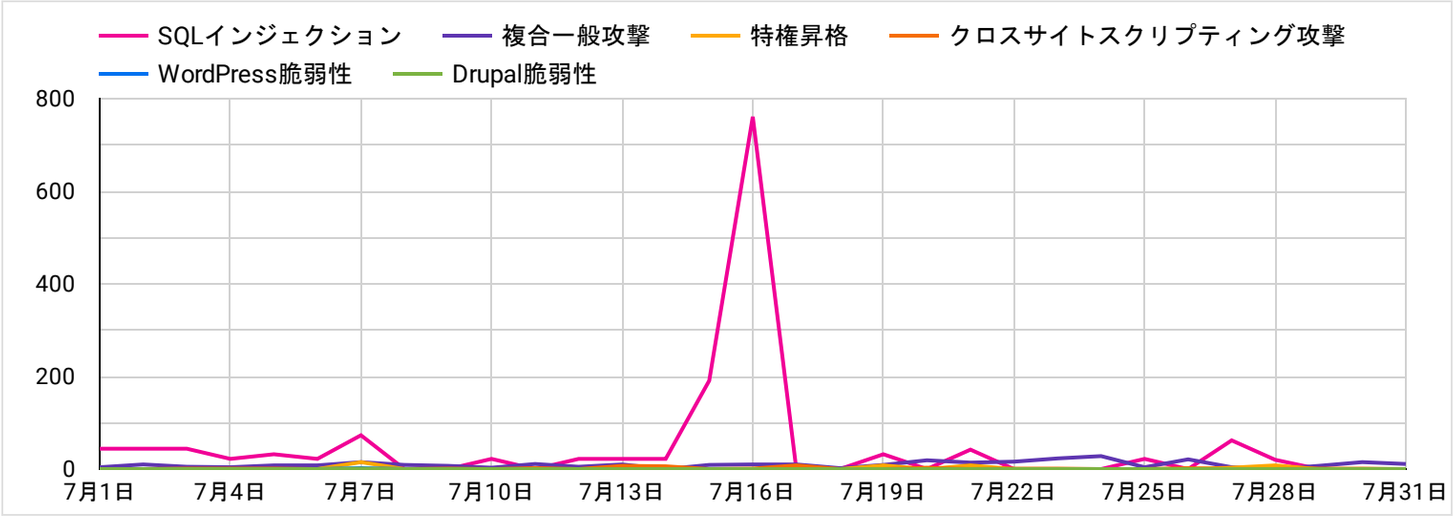
株式会社ROCKETWORKS 様　　2025年7月

AEGIS SERVER SECURITY

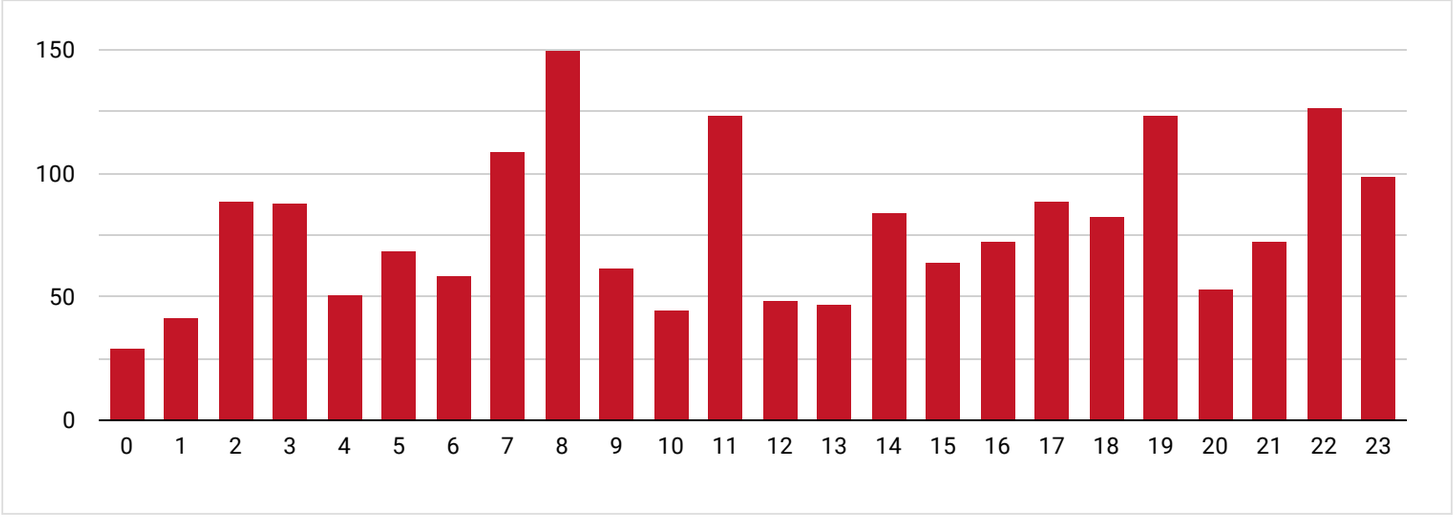
1.日別・時間帯別 攻撃検出状況

全攻撃数
1,882

1-1.日別

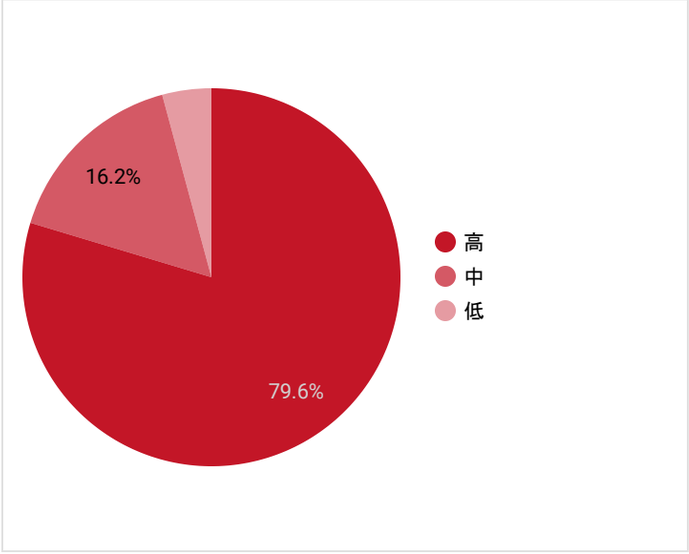


1-2.時間帯別

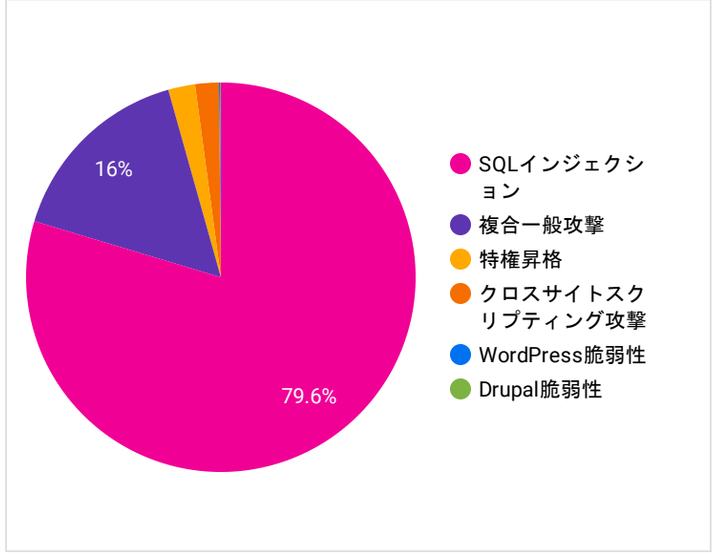


2.攻撃種別 攻撃検出状況

2-1.リスクの分布



2-2.攻撃種の分布



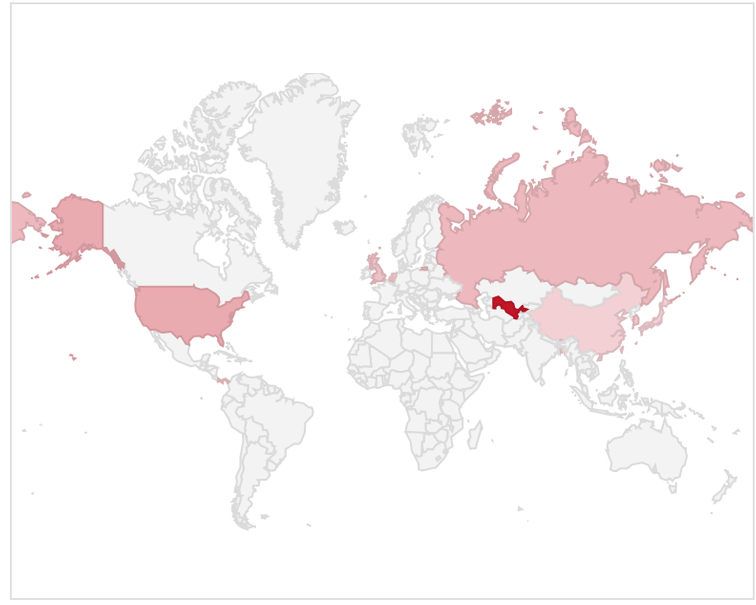
Rocketworks

3.攻撃元別 攻撃検出状況

全攻撃数
1,882

3-1.攻撃元ホストの地域（TOP10）

国	件数
Uzbekistan	890
Hong Kong	346
United States of Ameri…	187
Russian Federation	115
Belgium	74
Northern Ireland	73
Korea	63
Panama	58
Singapore	41
Bangladesh	13



3-２.攻撃元ホストのIPアドレス（TOP10）

IP	国	件数
94.158.XXX.XXX	Uzbekistan	890
103.97.XXX.XXX	Hong Kong	264
213.109.XXX.X…	Russian Federati…	94
147.78.XXX.XXX	Belgium	74
74.118.XXX.XXX	United States of …	66
5.181.XXX.XXX	Northern Ireland	64
141.98.XXX.XXX	Panama	58
143.198.XXX.X…	Singapore	31
27.124.XXX.XXX	Korea	29
52.78.XXX.XXX	Korea	29

3-2.攻撃先FQDN

FQDN	件数
aegis-ss.jp	208
www.rocketworks.co.jp	1,674

—— 主な攻撃種について
複合一般攻撃: 脆弱性やインジェクションなど、複数のステップ・手法の組み合わせによってシステムを侵害する攻撃。
Drupal脆弱性: CMS「Drupal」の脆弱性を突く攻撃。
WordPress脆弱性: CMS「WordPress」の脆弱性を突く攻撃。
PHP脆弱性: PHPの脆弱性を突く攻撃。
特権昇格: 悪意あるユーザが本来許されない高い権限を取得し、システムに不正アクセスする攻撃。
SQLインジェクション: データベースクエリに不正なSQL文を挿入し、データの改ざんや情報の盗取などを行う攻撃。
クロスサイトスクリプティング攻撃: Webページに悪意のあるコードを埋め込み、訪問者の情報の盗取やハイジャックなどを行う攻撃。
Non_HTTP: メール、DNSやその他のソケット通信などHTTPプロトコル以外の攻撃。

—— 攻撃元ホストのIPアドレスについて
X-Forwarded-Forがセットされている場合、最初のIPアドレス（送信元と推定されるIP）を表記しています。

全攻撃数
1,882

4.総括レポート

1499件のSQLインジェクション、301件の複合一般攻撃、42件の特権昇格、2件のWordPress脆弱性、1件のDrupal脆弱性、37件のクロスサイトスクリプティング攻撃を検出しました。

94.158.XXX.XXX、27.124.XXX.XXX、143.198.XXX.XXX、52.78.XXX.XXX、103.30.XXX.XXX、43.247.XXX.XXX、213.168.XXX.XXX、114.43.XXX.XXX、199.195.XXX.XXX、137.175.XXX.XXX、116.206.XXX.XXX、199.204.XXX.XXX、45.11.XXX.XXX、209.141.XXX.XXX、203.144.XXX.XXX、194.180.XXX.XXX からはGETリクエストを利用したクロスサイトスクリプティング試行を検出しました。Webアプリケーション側で適切にエスケープ処理がなされている場合は特に問題ありませんが、念のためご確認ください。

103.97.XXX.XXX、213.109.XXX.XXX、147.78.XXX.XXX、74.118.XXX.XXX、5.181.XXX.XXX、141.98.XXX.XXX、45.134.XXX.XXX、45.93.XXX.XXX、220.158.XXX.XXX、64.7.XXX.XXX、72.5.XXX.XXX、45.76.XXX.XXX、35.224.XXX.XXX、216.245.XXX.XXX、5.183.XXX.XXX、45.80.XXX.XXX、45.159.XXX.XXX、185.94.XXX.XXX からは、SQLインジェクション試行が検出されました。過去に製造した機能等も含めて入力のエスケープが十分になされているかご確認ください。また普及率の高いアプリケーション（CMS等）やライブラリなどを使用されている場合は、バージョンアップ等、定期的なメンテナンスをおすすめします。

66.203.XXX.XXX、114.43.XXX.XXX、143.92.XXX.XXX、199.195.XXX.XXX、137.175.XXX.XXX、164.90.XXX.XXX、199.204.XXX.XXX、202.61.XXX.XXX、209.141.XXX.XXX、159.89.XXX.XXX、203.144.XXX.XXX、122.10.XXX.XXX、38.145.XXX.XXX、103.186.XXX.XXX、154.22.XXX.XXX からはCGI版PHPにおいて過去に存在した脆弱性を対象とした攻撃試行を検出しました。PHP5系をCGI環境で動作させている場合、対象となり得ます。/cgi-bin/等に使用していないPHP処理系が存在する場合は削除をおすすめします。

23.224.XXX.XXX、154.91.XXX.XXX、116.213.XXX.XXX、143.92.XXX.XXX、91.92.XXX.XXX、220.93.XXX.XXX、138.199.XXX.XXX、122.10.XXX.XXX、121.127.XXX.XXX、103.230.XXX.XXX、223.223.XXX.XXX からは中国で普及しているフレームワーク「ThinkPHP」および「ThinkCMF」の脆弱性を対象とした攻撃を検出しました。関連する一部の通信がWindowsサーバ環境を対象にしているものと見られます。日本では普及率の低いシステムが対象となっていますが念のためご注意ください。

43.229.XXX.XXX からは、Wordpress等CMSの一部プラグインやテーマの脆弱性を狙ったディレクトリトラバーサル攻撃（コンフィグ情報の奪取試行）を検出しました。オープンソースCMSを使用されている場合は、プラグインを含め定期的なアップデートをおすすめします。また販売されているテーマは多数のライブラリ等を含む場合があるため、使用されている場合は提供元のアップデート情報に留意ください。

122.161.XXX.XXX、159.223.XXX.XXX、194.180.XXX.XXX からはサーバのパスワードや権限奪取を目的としたディレクトリトラバーサル攻撃を検出しました。あまりリスクの高くない攻撃となりますが、オープンソースのCMSやライブラリ等にこの種攻撃の対象となる脆弱性が含まれることがあるためご注意ください。

38.61.XXX.XXX、122.10.XXX.XXX、121.127.XXX.XXX、128.199.XXX.XXX からはPHPユニットテストツール「PHPUnit」に存在するコードインジェクション脆弱性を対象とした攻撃を検出しました。使用されている場合、ベンダーが提供する修正版が適用されているか念のためご確認ください。 また、PHPUnitはCMSやフレームワーク等に含まれている場合があるため、ご注意ください。

146.70.XXX.XXX からは、各種ネットワーク機器に存在する脆弱性に対する探索や攻撃試行を検出しました。ルータやNAS、ネットワークカメラ等のインターネット接続機能を持つ広範な機器の脆弱性を対象としたボットの活動と見られます。オフィスでこういった機器を使用されている場合は、メーカーが提供する情報に注意し、ファームウェアのアップデート等を定期的に行うことをおすすめします。

45.207.XXX.XXX からはGETパラメーターを対象としたOSコマンドインジェクション試行を検出しました。サイト内のURLパラメーター全般に対して総当り的に試行されますので、過去に製造した機能等も含めて入力のエスケープが十分になされているかご確認ください。