【ニュースリリース】

2022 年 4 月 28 日

報道関係者各位

2022 年 1 月～3 月対象
「Web サイト・Web アプリケーションを狙ったサイバー攻撃検知レポート」を発表
～長期休暇期間はサイバー攻撃の危険性大　必ず GW 前に対策を～

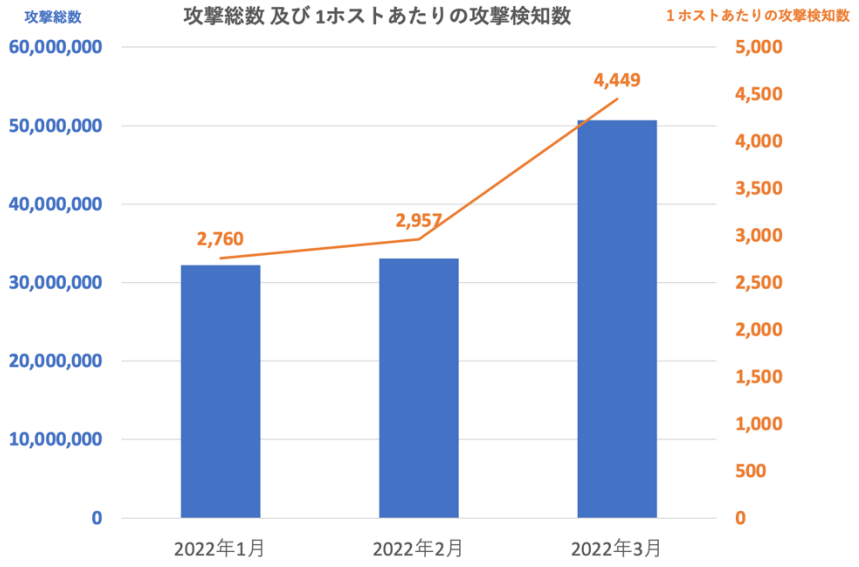
株式会社サイバーセキュリティクラウド（本社：東京都渋谷区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、2022 年 1 月 1 日から同年 3 月 31 日までを対象とした「Web サイト・Web アプリケーションへのサイバー攻撃検知レポート」を発表いたします。本データは当社が提供する、Web サイト・Web アプリケーションへのサイバー攻撃を可視化・遮断するクラウド型 WAF『攻撃遮断くん』、及び AWS WAF、Azure WAF、Google Cloud Armor 自動運用サービス『WafCharm（ワフチャーム）』で観測した攻撃ログを集約し、分析・算出したものです。

■調査概要
- 調査対象期間：2022 年 1 月 1 日～3 月 31 日
- 調査対象：『攻撃遮断くん』、『WafCharm』をご利用中のユーザアカウント
- 調査方法：『攻撃遮断くん』、『WafCharm』で観測した攻撃ログの分析

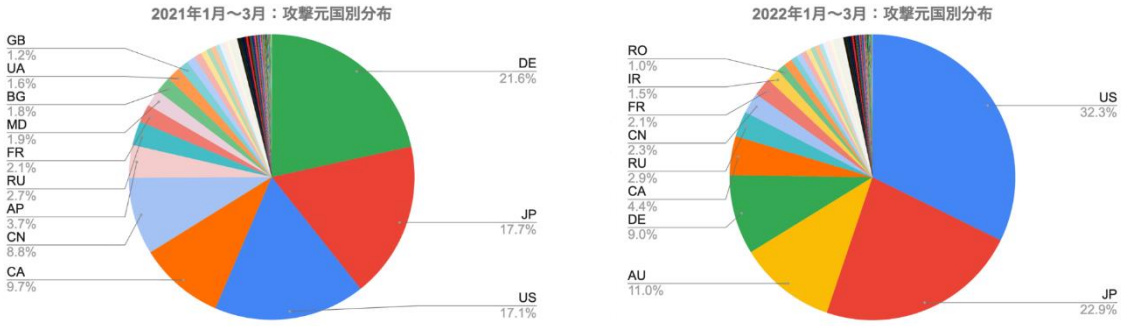
■2022 年 1 月～3 月の攻撃検知状況
～攻撃検知数は特に 3 月後半が増加傾向～

今回の調査対象のうちアクティブユーザホストについて、攻撃検知の状況を集計しました。1 ホストあたり（※ 1）の攻撃検知数は 2022 年 1 月で 2,760 件、2 月は 2,957 件、3 月は 4,449 件と月を追うごとに増加しました。

※ 1：『攻撃遮断くん』の保護対象ホスト数（Web タイプ：FQDN 数、サーバタイプ：IP 数）、『WafCharm』の保護対象ホスト数（WebACL）の総数を分母に概算。



検知された攻撃元を国別にみると、2021 年の 1 月～3 月は 1 位ドイツ、2 位は日本国内、3 位はアメリカ、次いでカナダ、中国と続いていましたが、2022 年はアメリカからの攻撃が 32.3%と最も多く、2 位が日本国内で 22.9%、3 位がオーストラリアで 11%、次いでドイツ、カナダと続いています。また昨今の国際情勢で注目されることの多いロシアなどからの攻撃は以前から継続して検知されていますが、大幅な増減は確認できませんでした。

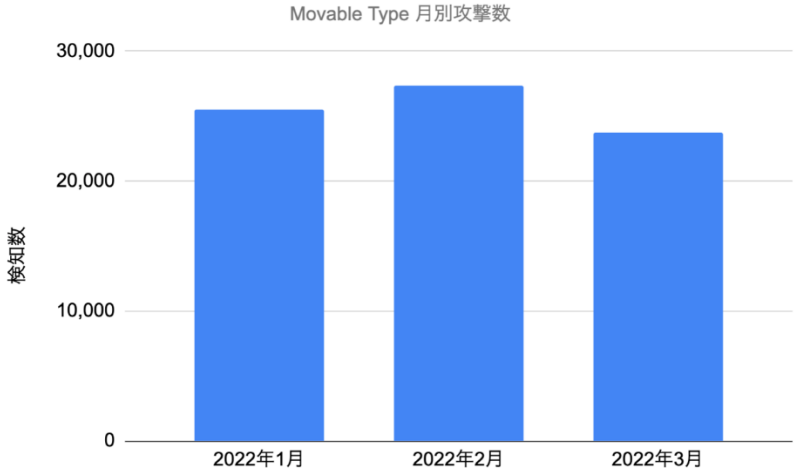


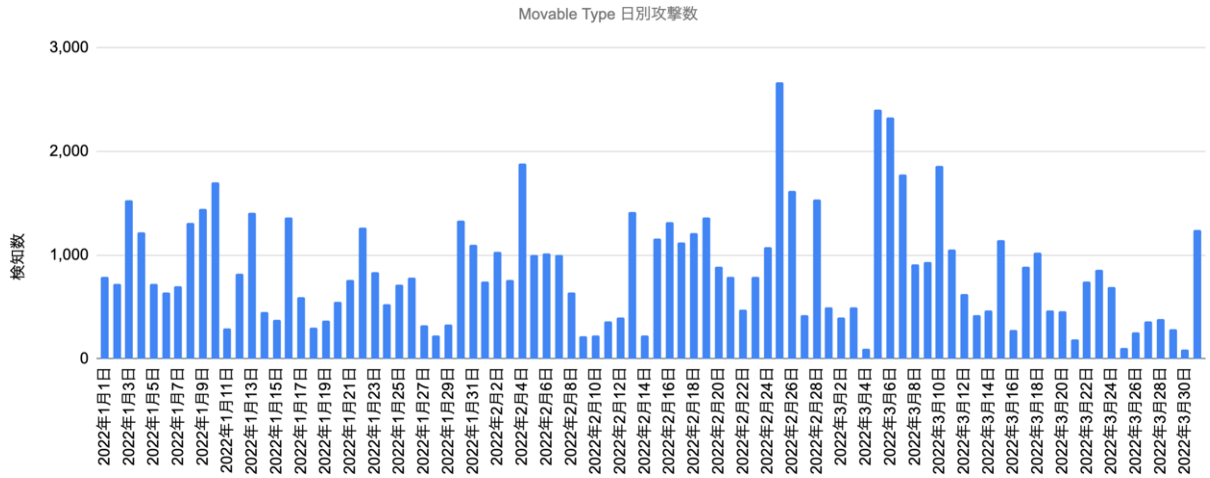
■2021 年末の Movable Type および Log4j の脆弱性について（続報）

～重大な脆弱性に対する継続的な警戒が必須～

今回、2021 年後半に世間を騒がせた 2 つの重大な脆弱性について調査しました。

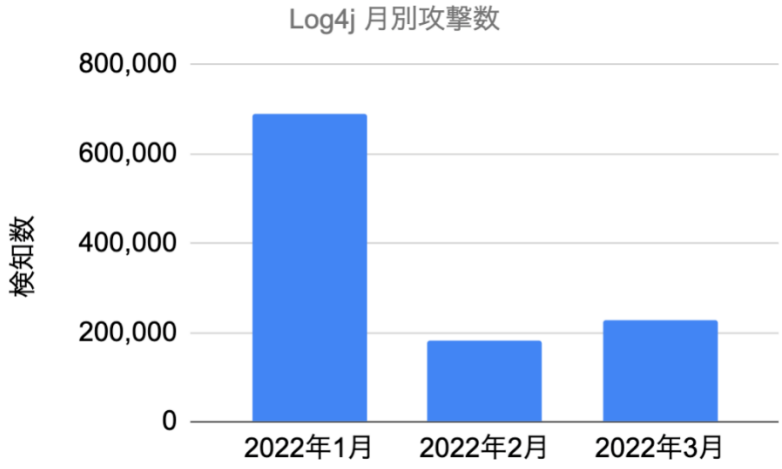
まずは Movable Type（CVE-2021-20837）について、当社では既報の通り 2021 年 11 月 10 日より本攻撃と想定される通信を検知、同年 11 月後半から年末年始にかけて多数のホストにて該当の通信を検知していました。今回の調査結果では、日によって検知数にばらつきはあるものの、2022 年 1 月～3 月においても引き続き攻撃の兆候を継続して検知していることが明らかになりました。

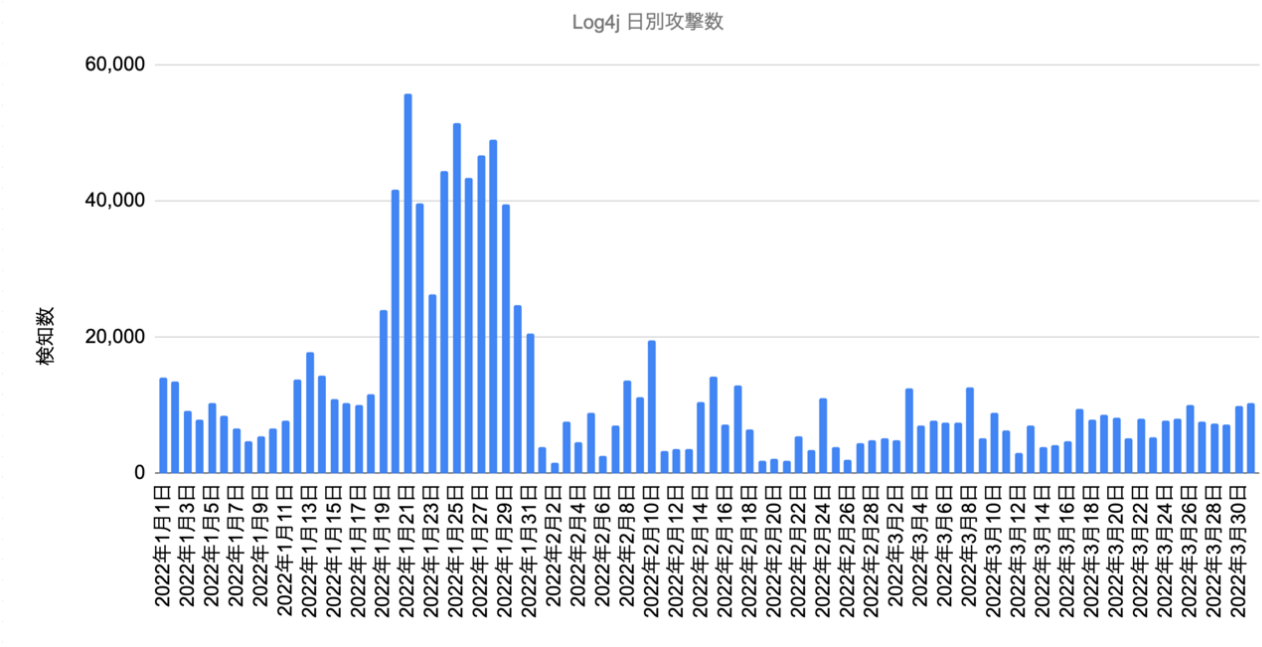




次に Log4j の脆弱性について、2021 年 12 月 9 日にリモートで悪用可能な脆弱性（CVE-2021-44228）の存在が公表され、前回の調査では 2021 年 12 月の 1 ヶ月間で 1 日に最大 100,000 件に迫る検知数を確認しました。今回の調査では、1 月は合計 700,000 件程度、2 月、3 月に関しても 1 日に 10,000 件前後を記録する日も存在しており、引き続き警戒が必要な数値となっています。

以上 2 つの脆弱性に関しては、最新バージョンへのアップデートをはじめとした脆弱性への対策を速やかに行い、攻撃の影響を受けていないか調査することを推奨します。





■Spring Framework の脆弱性（Spring4shell）について

～大きな被害の報道はないものの脅威度は極めて高い～

2022 年 3 月 31 日、Java で採用される主流なフレームワークの 1 つである Spring Framework に致命的な脆弱性が確認され、修正版が公開されました。当該脆弱性（CVE-2022-22965）の脅威度を示す CVSS（v3）の値が 10 点満点中 9.8 と極めて高く、また 3 月 31 日の時点で既に脆弱性の Exploit コード（攻撃用のコード）が出回っており、インターネット上の活動が報告されていた（※2）ことも相まって話題になりました。

※ 2：本脆弱性に関連したスキャンは世界中で確認報告が挙がったものの、具体的な被害報告は確認されていません。

3 月 31 日から 4 月 6 日までの当社の当該検知結果では、3 月 31 日から 4 月 3 日にかけてが最も多く、検知数が 400 件を超える日もありました。それ以降はかなり減少しているものの、引き続き対策が必要です。下記アップデートの実施をはじめとした脆弱性への対策とともに、攻撃の影響を受けていないか調査することを推奨します。

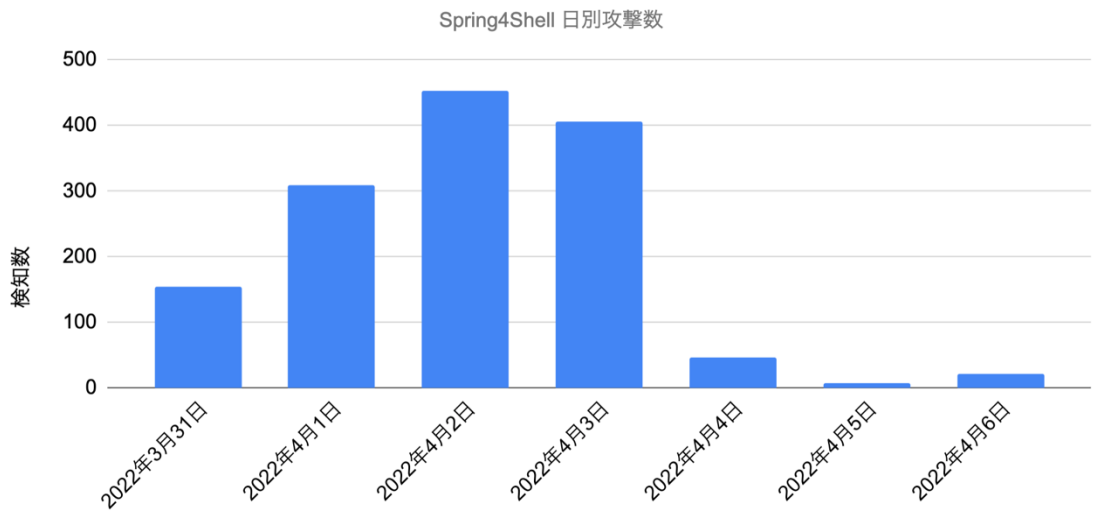
〈脆弱性に対処できるバージョン（※3）〉

- Spring Framework 5.2.20 以上（Spring Framework 5.2 ユーザ）
- Spring Framework 5.3.18 以上（Spring Framework 5.3 ユーザ）
- Spring Boot 2.5.12 以上（Spring Boot 2.5 ユーザ）
- Spring Boot 2.6.6 以上（Spring Boot 2.6 ユーザ）

※ 3：以下の要件を満たしている場合、本脆弱性を悪用したサイバー攻撃を受ける可能性があります。

- 実行環境が JDK 9 またはそれ以上
- サーブレットコンテナとして Apache Tomcat を利用している
- WAR としてパッケージ化している
- Spring Web MVC（※ 4）と Spring WebFlux（※ 5）との依存関係がある

※ 4：Spring Web MVC：Web アプリケーションを簡単に作るための機能。アノテーションコントローラを使用するブロッキングな処理でアプリケーションを開発する。
※ 5：Spring WebFlux：Web アプリケーションを簡単に作るための機能で、リアクティブプログラミングによってノンブロッキングで非同期なアプリケーションを開発する。
（上記の※ 4 と※ 5 との大きな相違点は「ロジックの記載方法」と「リクエストの処理に使用するスレッドプールの仕組み」の 2 点）



なお、CVE-2022-22963：Spring Cloud の RCE 脆弱性についても既に公表されていますが、こちらは Spring Cloud にかかる脆弱性、ホストまたはコンテナ上で任意のコードを実行可能、クラウド環境のサーバレス機能にも影響を与える可能性があるというもので、Spring4shell とは別の脆弱性です。

■ゴールデンウィーク中のサイバーセキュリティ対策
～長期休暇前にぜひ事前の対策を！～

ゴールデンウィークのような長期休暇期間は、多くの組織・団体でシステム管理者が長期間不在になり、有事の際に迅速な対応が取れないケースが生じやすくなっています。また、PC 等を起動しない期間が長くなり OS や利用ソフトウェア等のアップデートが行われないため、休み明け業務を再開する際にウイルス等に感染する恐れもあります。現在国際情勢が不安定であることも踏まえると、Emotet をはじめとした攻撃に対しても引き続き警戒することが重要です。被害を最小限に抑えるべく、ゴールデンウィーク前後に従業員への対応通知を設定するなど事前の対策をお勧めします。

参考： 長期休暇における情報セキュリティ対策
https://www.ipa.go.jp/security/measures/vacation.html

【株式会社サイバーセキュリティクラウドについて】
会社名：株式会社サイバーセキュリティクラウド
所在地：〒150-0011　東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階
代表者：代表取締役社長 兼 CEO 小池敏弘

設立：2010 年 8 月
URL：https://www.cscloud.co.jp/

【報道関係者からの問い合わせ先】
株式会社サイバーセキュリティクラウド PR 事務局（株式会社イニシャル 内）
担当：深田・石坪・藤原
TEL：03-5572-7334
FAX：03-5572-6065
E-MAIL：csc-pr@vectorinc.co.jp

株式会社サイバーセキュリティクラウド
経営企画部　広報担当：竹谷
TEL：03-6416-9996
FAX：03-6416-9997
E-MAIL：pr@cscloud.co.jp