【ニュースリリース】

2022 年 4 月 28 日

報道関係者各位

サイバーセキュリティクラウド、2022 年第 1 四半期（1 月～3 月）を対象とした「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

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。なお、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・算出しています。

■調査概要

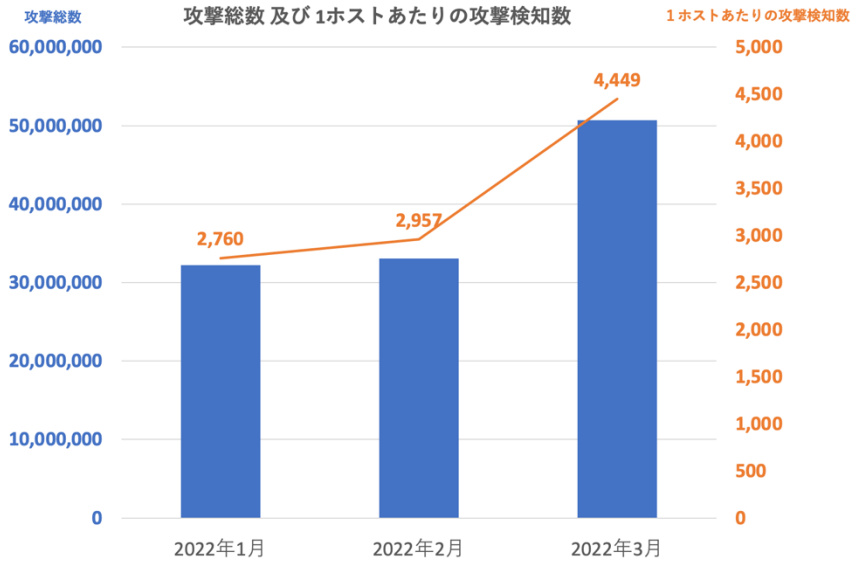
- 調査対象期間：2022 年 1 月 1 日～3 月 31 日
- 調査対象：『攻撃遮断くん』、『WafCharm』をご利用中のユーザアカウント
- 調査方法：『攻撃遮断くん』、『WafCharm』で観測した攻撃ログの分析

■2022 年 1 月～3 月の攻撃検知状況

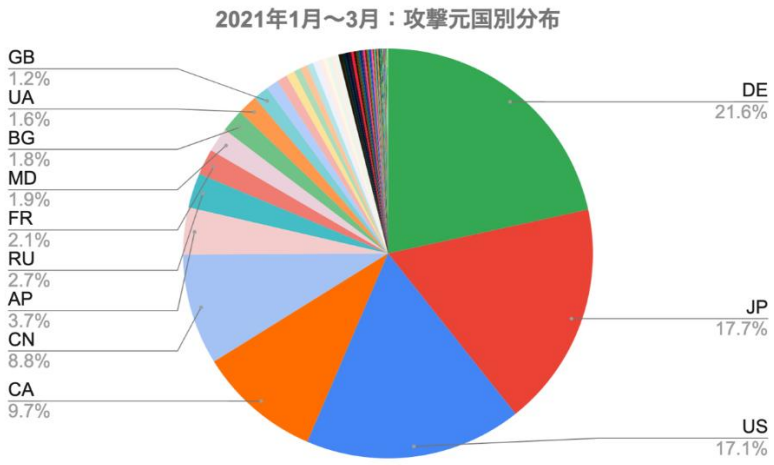
～攻撃検知数は特に3月後半が増加傾向～

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。

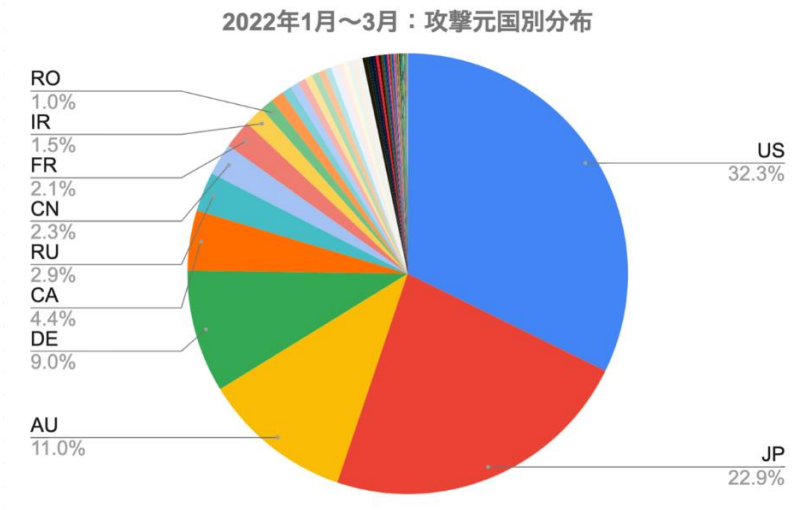
※ 1：『攻撃遮断くん』の保護対象ホスト数（Web タイプ：FQDN 数、サーバタイプ：IP 数）、『WafCharm』の保護対象ホスト数（WebACL）の総数を分母に概算。



また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 位オーストラリアが 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、増減等の特筆すべき傾向は確認されておりません。

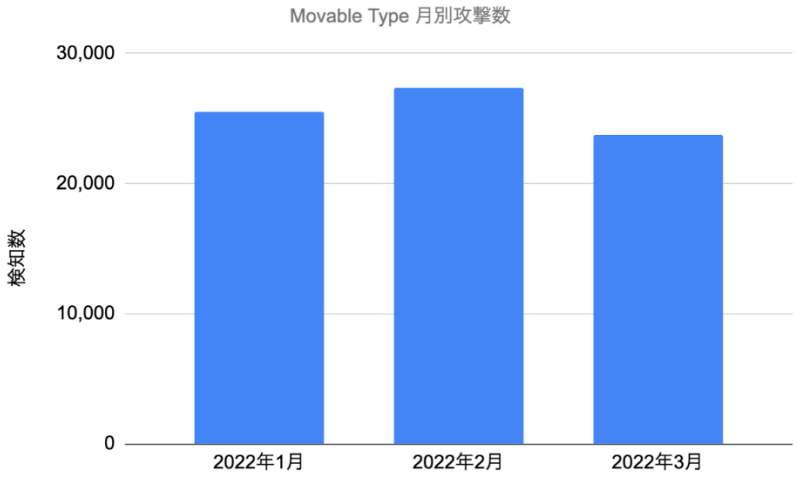


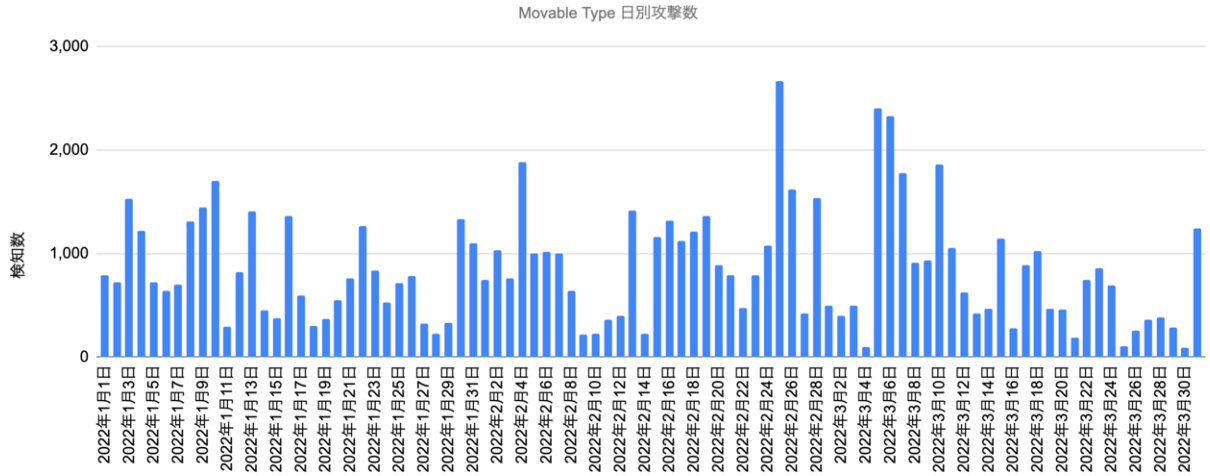
■2021 年末の Movable Type および Log4j の脆弱性について（続報）
～この 2 つの重大な脆弱性に対しては引き続き警戒が必要な状況～

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、現状を調査しました。

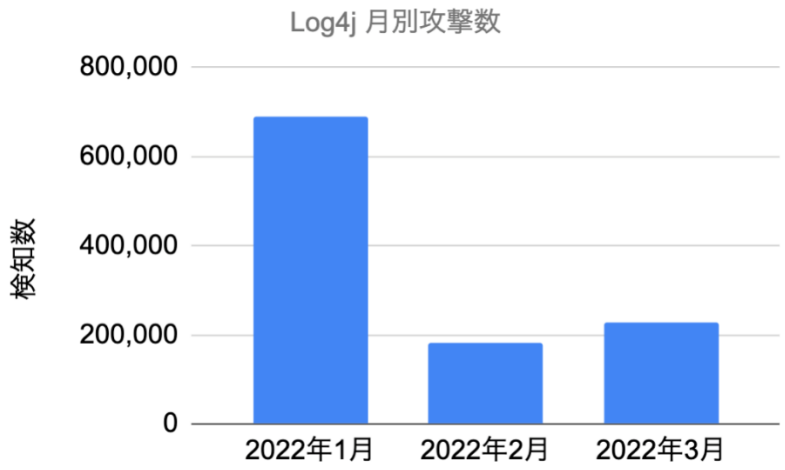
まずは Movable Type（CVE-2021-20837）ですが、当社では既報の通り 2021 年 11 月 10 日より同攻撃と想定される通信を検知、同年 11 月後半から年末年始にかけて多数のホストにて攻撃と想定される通信を検知していました。そして今回の調査期間では、日によって検知数にばらつきはあるものの、現在でも攻撃の兆候を継続して検知し続けています。なお、本件について現状もし未対応のままでしたら、可能な限り速

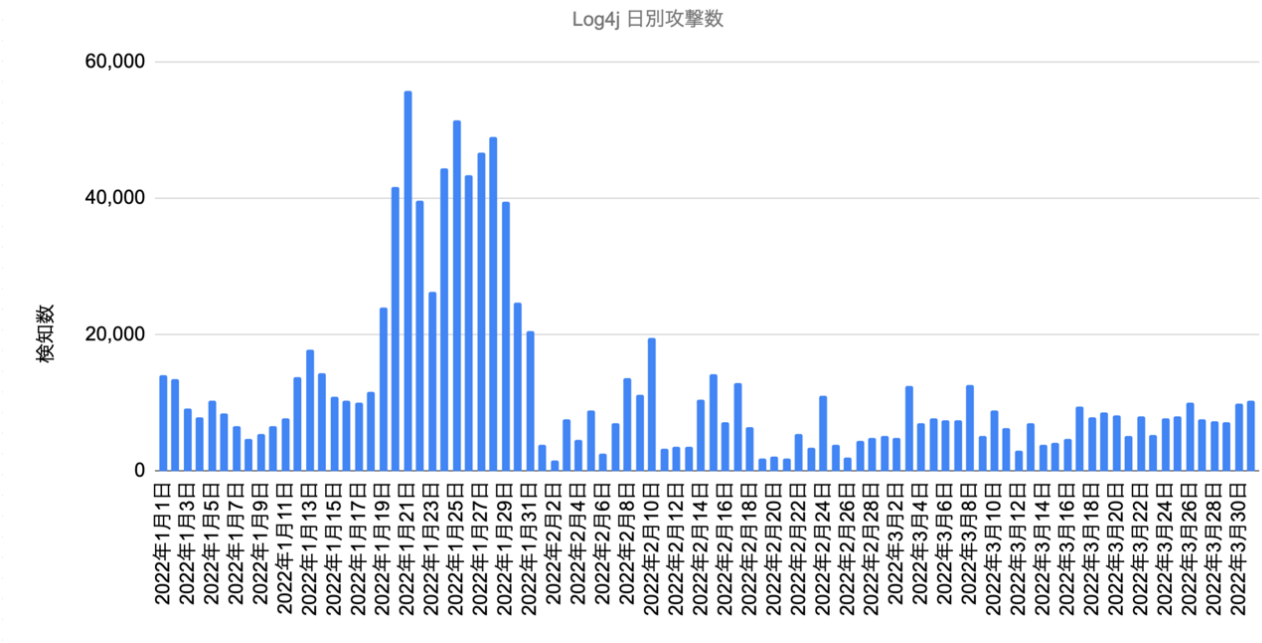
やかに最新のバージョンにアップデートし脆弱性への対策を行うとともに、すでに攻撃の影響を受けている可能性について調査をするなどの対応を引き続き推奨します。





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、当社の調査では 2021 年 12 月から年末にかけて最大で 1 日に 100,000 件に迫る検知数を確認しました。そして今回の調査期間の検知数推移について、1 月は合計 700,000 件程度、特に月の前半よりも後半の方がより多く検知していました。2 月、3 月に関しては減少したとはいえ 1 日に 10,000 件前後の検知数を数える日もありました。現在におきましても組み込みなどを含め、Log4j が実装されている機器、システム等について完全に洗い出しを完了している状況とは言えず、もしも本件に未対応のまま運用されていることが分かっている場合は、こちらも同様に最新バージョンへのアップデートなど脆弱性への対策を可能な限り速やかに実施されるとともに、すでに攻撃の影響を受けている可能性について調査をする等の対応を推奨します。





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

～まだ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（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が、具体的な被害報告は確認されていない）ことも手伝って話題を呼びました。

CYBER SECURITY CLOUD

本脆弱性の影響を受けるのは、

- Spring Framework 5.2：5.2.0～5.2.19
- Spring Framework 5.3：5.3.0～5.3.17
- Spring Boot 利用の場合、Spring Boot 2.6.5 以前および Spring Boot 2.5.11 以前

上記のバージョン、およびサポートがすでに終了している上記以前のバージョンも含まれます。

なお本脆弱性を悪用するためには、上記の他にも以下の要件を満たす必要があります。

- 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（※ 2）と Spring WebFlux（※ 3）との依存関係がある

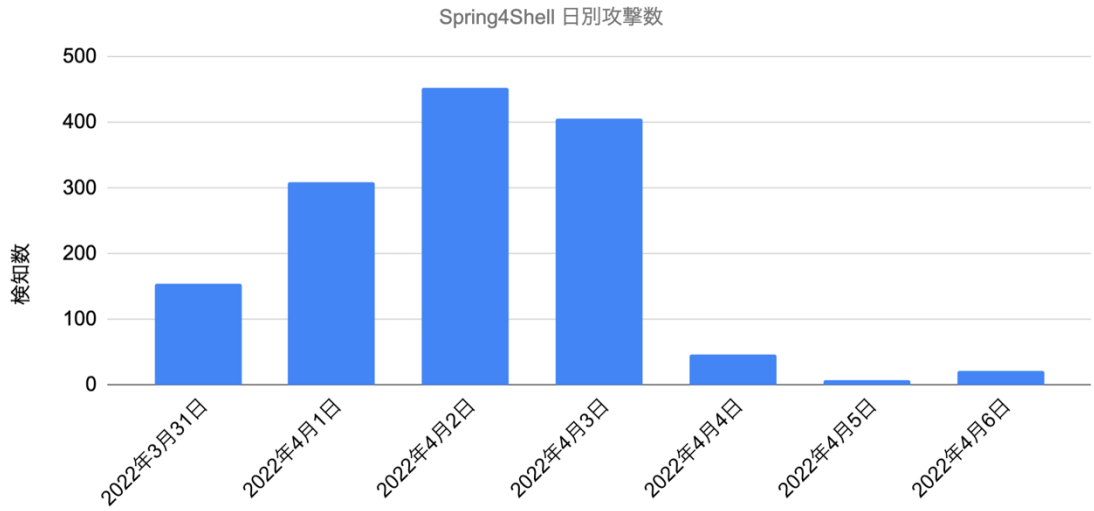
※ 2：Spring Web MVC：Web アプリケーションを簡単に作るための機能で、アノテーションコントローラを使用するブロッキングな処理でアプリケーションを開発する。
※ 3：Spring WebFlux：Web アプリケーションを簡単に作るための機能で、リアクティブプログラミングによってノンブロッキングで非同期なアプリケーションを開発する。
（上記の※2 と※3 との大きな相違点は「ロジックの記載方法」と「リクエストの処理に使用するスレッドプールの仕組み」の 2 点）

本脆弱性に対処するには以下のバージョンへのアップデートが必要です。

- 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）

こちらも放置せず、上記アップデートなど脆弱性への対策とともに、すでに攻撃の影響を受けている可能性について調査をするなどの対応を推奨します。

参考までに、本脆弱性について 3 月 31 日から 4 月 6 日までの当社の当該検知結果につきましては、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が、それ以降はかなり減少しています。



なお、本脆弱性（CVE-2022-2296）とは別に CVE-2022-22963：Spring Cloud の RCE 脆弱性というものも公表されており、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、本件 Spring4shell とは別の脆弱性になりますので、混同されないよう念のため記載しておきます。

■ゴールデンウィーク中のサイバーセキュリティ対策
～休み前にぜひ事前対策の実施を！～

ゴールデンウィークをはじめ長期休暇期間は、多くの組織・団体でシステム管理者が長期間不在になるなど、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、ゴールデンウィーク明け業務を再開する際にウイルス等に感染する可能性も高くなってしまいます。そして国際情勢が不安定な現在 Emotet をはじめ様々な攻撃も目立っています。こうした状況に起因する被害等を最小限に抑えるべく、ゴールデンウィーク前とゴールデンウィーク明けの対応通知など、事前対策を実施されることをお勧めします。

ご参考までに、IPA（情報処理推進機構）が 2022 年 4 月 20 日に掲示している「長期休暇における情報セキュリティ対策」のページへのリンクを以下に記載します。

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/