【ニュースリリース】

2022年2月1日

報道関係者各位

サイバーセキュリティクラウド、「サイバー攻撃検知レポート2021」を発表

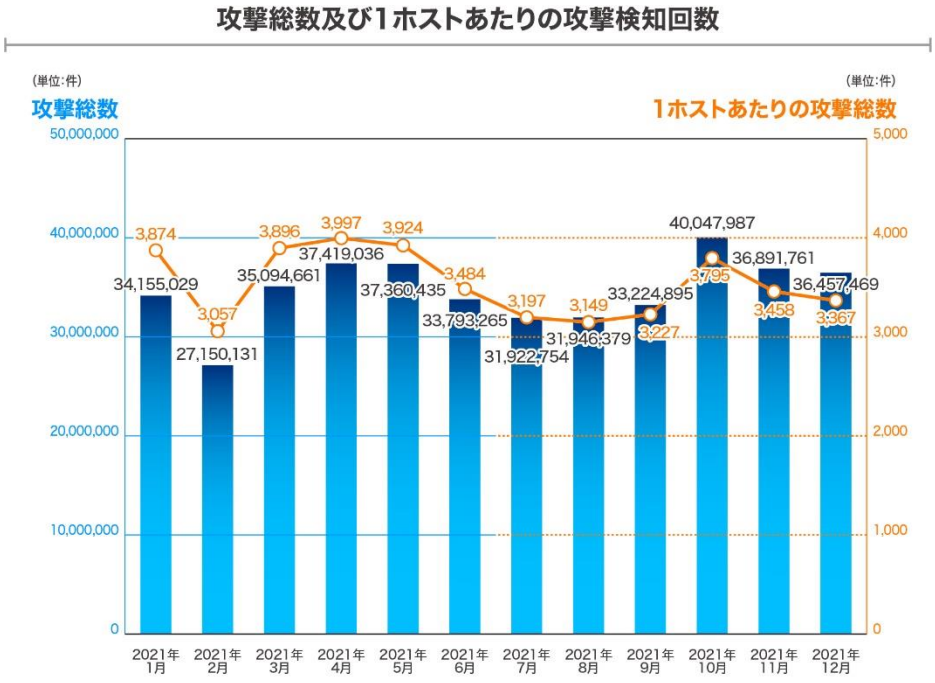
株式会社サイバーセキュリティクラウドは、2021年（2021年1月1日～12月31日）を対象としたWebアプリケーションを狙った攻撃の検知レポートを発表いたします。なお、本データは当社が提供するWebサイトへのサイバー攻撃を可視化・遮断するクラウド型WAFの『攻撃遮断くん』及び、AWS WAF、Azure WAF、Google Cloud Armorの自動運用サービス『WafCharm（ワフチャーム）』で観測した攻撃ログを集約し、分析・算出しています。

■調査概要

・調査対象期間：2021年1月1日～12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

■2021年のサイバー攻撃検知状況
～「1ホストあたり年間4.2万件」の攻撃を検知～

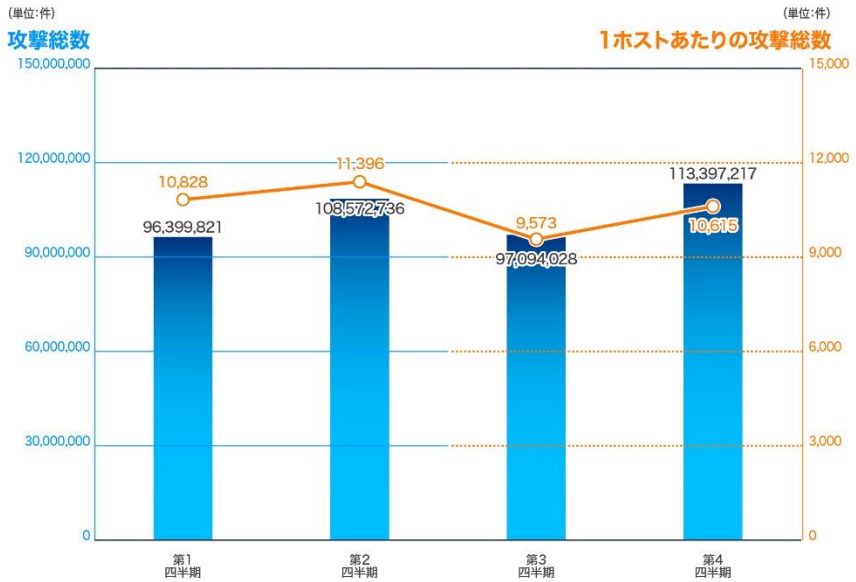
2021年の1年間（1月1日～12月31日）でのサイバー攻撃の検知総数は、合計415,463,802件でした。これは2020年の攻撃検知総数（334,932,032件）に比べて増加しておりますが、1ホストあたり※では、2021年約4.2万件、2020年約4.3万件と横ばいとなっています。
※『攻撃遮断くん』の保護対象ホスト数（Webタイプ：FQDN数、サーバタイプ：IP数）、『WafCharm』の保護対象ホスト数（WebACL）の総数を分母に概算



一般的に、オリンピック・パラリンピックが開催される年のホスト国は、開催前後で顕著にサイバー攻撃が増える傾向にあります。ただし今回の同大会に関しては、幸いにして関係者や警察、NISC等からも本件について大規模な攻撃による目立った被害は観測・報告されてはいません。

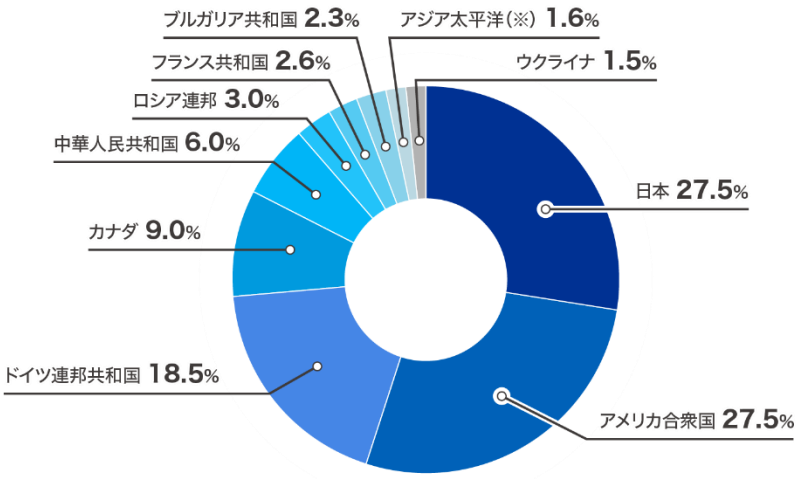
しかしながらWebアプリケーションをターゲットとした攻撃の数そのものが増加傾向にあったことは確かだと言えます。その年間の推移を四半期に分けて振り返ると、2021年1～6月の上半期については、1ホストあたり10,828件～11,396件の攻撃回数であるのに比べて、7～9月の第3四半期がおよそ9,573件と減少、当該期間の攻撃検知総数も同様に減少しています。しかし10～12月の第4四半期では1ホストあたりおよそ10,615件、攻撃検知総数も2021年四半期別では最も多い113,397,217件の攻撃が検知されました。これは後述するMovable Type、Apache Log4jについての深刻な脆弱性が2021年の第4四半期に公表され、今もまだその渦中にあることも全くの無関係ではないと推測されます。

四半期別サイバー攻撃検知状況



また、当社が検知したWebアプリケーションへの攻撃通信について攻撃元の国別に2021年の検知回数を見てみると、トップは日本国内からのもので、以下同率でアメリカ、ドイツ、カナダ、中国と続いています。

攻撃元国

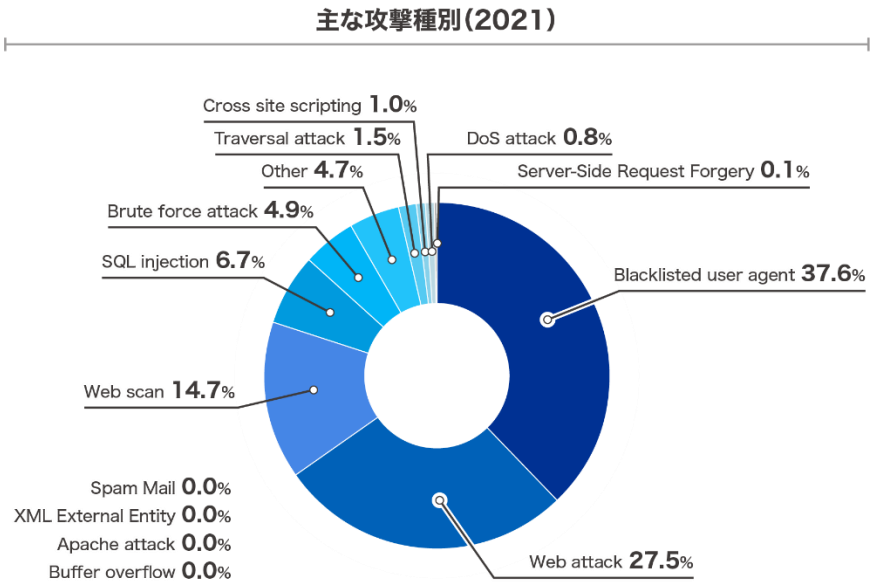


※ アジア太平洋(APAC)の値は、アジアから太平洋にかけての地域のうち、日本や中国などの値が大きな国を除いたものの合計です。

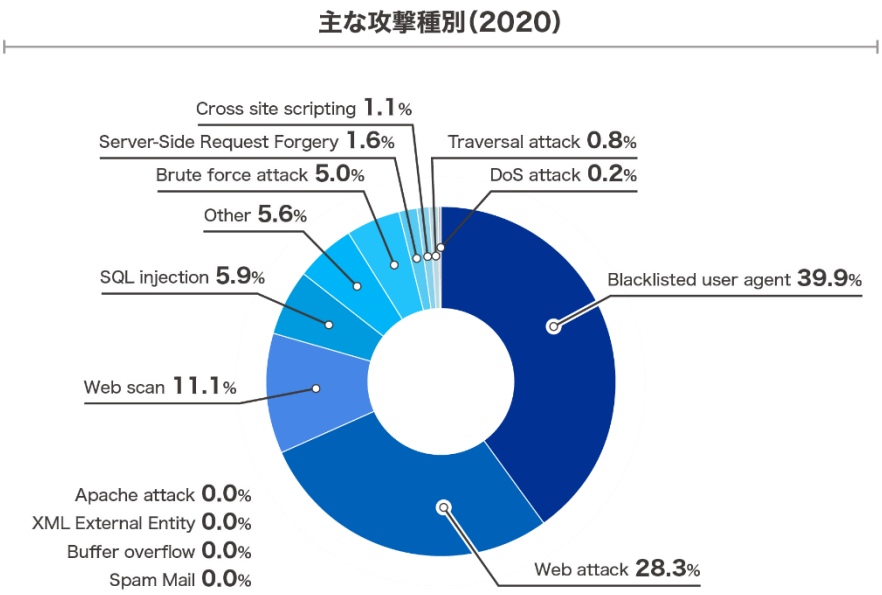
■主な攻撃種別
～昨年から総数は増加も傾向は変わらず～

今回の調査期間における主な攻撃種別の攻撃状況を見ると、前述の通り全体の総数は増加しているものの主だった傾向は2020年とさほど大きくは変わっていない状況です。最も多かったのは脆弱性スキャンツールなどを利用したBotによる攻撃である「Blacklisted user agent」で全体のおよそ37.6%を占め、次にWebサーバを構成するソフトウェアの脆弱性に対する攻撃である「Web attack」が約27.5%と続いています。そして3番目に多かったのは、攻撃の対象を探索・調査、また無作為に行われる単純な攻撃で脆弱性を探すなどの「攻撃の予兆」である「Web scan」ですが、全体の約11.1% → 14.8%、件数が37,192,991件 → 61,438,071件と、2020年より少なからず増加していました。また、7番目に多かったWEBサーバ上のファイルに不正アクセスする「Traversal attack」については、2020年の9番手から件数が
2,851,256件 → 6,509,911件に増加、そして今回9番手のDoS攻撃も2020年（10番手）比で件数が993,900件 → 3,622,036件と、他と比較して件数の増加が目立ちました。

2021年の攻撃種別



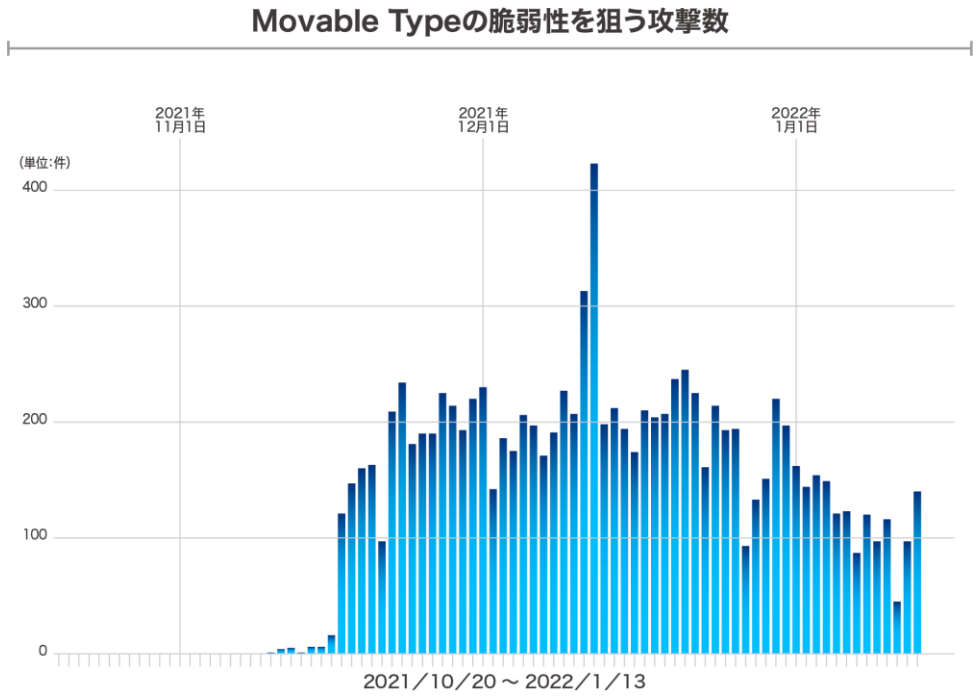
2020年の攻撃種別



2020年の攻撃種別ごとの攻撃件数について、新型コロナウィルスの感染拡大とともに「Web attack」の脅威が高まったことが判明した、とお伝えしましたが、その傾向は変わらず2021年度も継続しています。また、検知した攻撃の総数の増加だけでなく、攻撃予兆である「Web scan」について検知総数が大幅に増加していることから、攻撃者数、特に新たに参入してきたサイバー攻撃者の増加も推測できます。

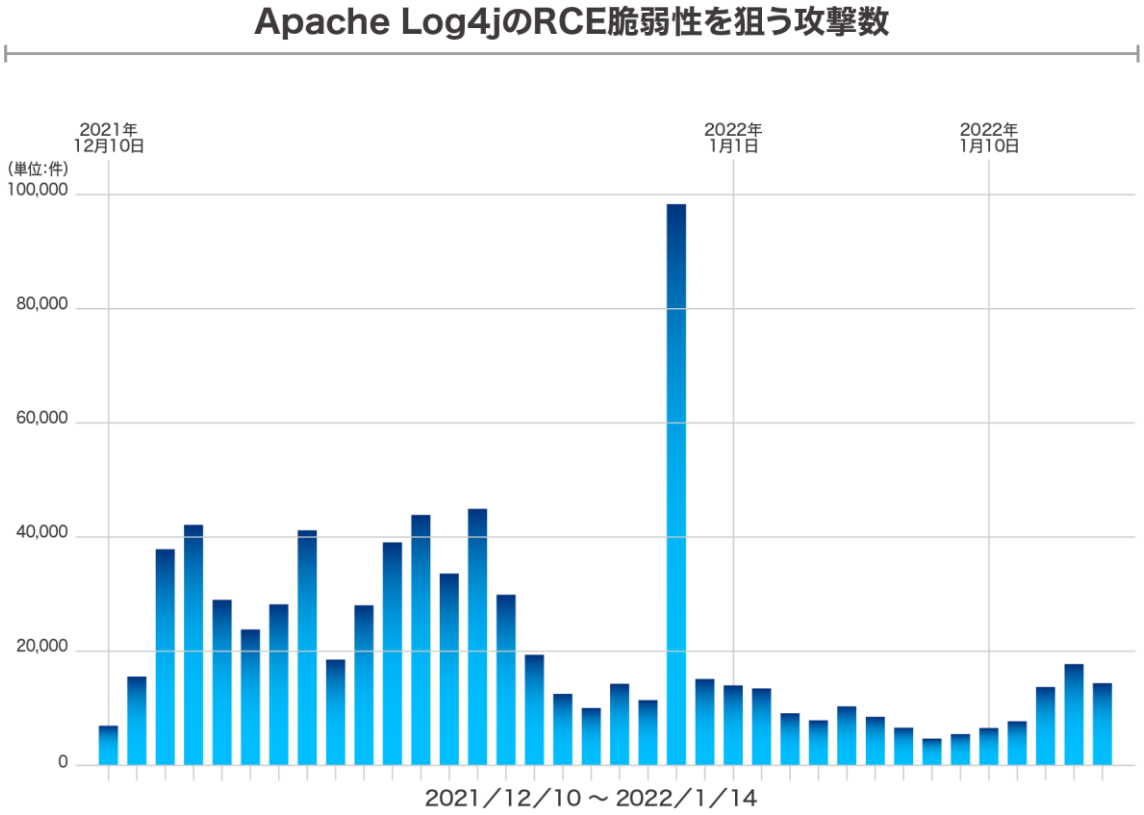
■主な脆弱性に関する攻撃状況
～この数年で最も深刻な脆弱性も発覚～

ーMovable Typeの脆弱性を狙う攻撃
　2021年10月20日に公開されたMovable TypeのXMLRPC APIに存在するリモートから悪用可能な脆弱性（CVE-2021-20837）について、本脆弱性の悪用を目的とした特殊なリクエストを受け取った場合、OSコマンドが実行され様々な被害を受ける可能性があります。本脆弱性の影響を受ける可能性のあるバージョンは以下の通りです。
・Movable Type 7 r.5003 より前のバージョン
・Movable Type Advanced 7 r.5003 より前のバージョン
・Movable Type 6.8.3 より前のバージョン
・Movable Type Advanced 6.8.3 より前のバージョン
・Movable Type Premium 1.47 より前のバージョン
・Movable Type Premium Advanced 1.47 より前のバージョン
　開発者によると、サポートを終了したバージョンを含むMovable Type 4.0以上（Advanced、Premiumも含む）が影響を受けます。
　本脆弱性につきましては、実際に当社では2021年11月10日より、同攻撃と想定される通信を検知しております。また同年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す。もし脆弱なままのMovable Typeを外部からアクセス可能な状態で稼働し続けていると、今後様々な被害を受ける可能性がございますので、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推奨し、改めて注意を喚起します。



ーApache Log4j2のRCE脆弱性を狙う攻撃

2021年12月9日に、代表的なJavaのログ出力ライブラリである「Apache Log4j」に、リモートから悪用可能な脆弱性（CVE-2021-44228）の存在が公表されました。システムでは「ログ＝履歴・記録」を記録する事は極めて重要なため、log4jはJavaを利用しているシステムで広く世の中で利用されています。今回公表された脆弱性の脅威度を表す指標（CVSS 3.0）の値は最高値「10.0」で、これほど容易にかつ広範囲に影響するリスクは、数年に一度見るかどうかの極めて危険な脆弱性と言えます。当社においても12月13日より現在に至るまで、攻撃と推定される通信を継続的に検知しています。12月30日における攻撃件数の急増は、年末の休みを狙い攻撃が増える典型的な事例のようです。



この脆弱性は、Apache Log4jのJava Naming and Directory Interface（JNDI）機能に関する任意のコード実行の脆弱性で、遠隔の第三者が「細工した文字列」を送信し、Log4jがそれをログとして記録することで任意のコードを実行する可能性がある、というものでした。任意のコードが実行できる、ということはつまり「何でもできる」という意味にとても近いという話であって、この数年で最も深刻な脆弱性の一つと言えるでしょう。

またその後、本件においては2022年1月24日現在で、CVE-2021-45046（アップデート（2.15.0）修正内容が不十分なため、特定条件下で任意のコード実行が可能な脆弱性）、CVE-2021-45105（自己参照による制御不能な再帰から保護されていないことに起因するLog4jの特定設定のみ影響を受けるサービス運用妨害攻撃の脆弱性）、CVE-2021-44832（JNDI機能で特定のデータソースを使用する場合に起因するリモートからの任意のコード実行の脆弱性）といった複数の脆弱性情報が追加されており、全ての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。

【最新の修正バージョン】

・Apache Log4j 2.17.1（Java 8以降のユーザー向け）

・Apache Log4j 2.12.4（Java 7のユーザー向け）

・Apache Log4j 2.3.2（Java 6のユーザー向け）

こちらも同様に、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、改めて注意を喚起します。

■最後に
～手段は多様化、攻撃の as a Service 化も～

2022年は未だ続くコロナ禍の継続も手伝って、一般にテレワークが深く浸透し業務遂行には社内ネットワークと外部との常時接続が前提となっている状況ですが、これまでの動向や現在のオミクロン株の流行と第六波の状況などを踏まえるまでもなく、今後も基本的には「テレワーク」というスタイルは常態化し、勤務スタイルとして恒久的に定着する事も予想されます。
また、標的型攻撃の脅威のみならずランサムウェアもますます深刻化する状況下で、最近は専門知識を特に持っていなくてもブラックマーケットを利用することで、攻撃者はより簡単に、より自動的にターゲットを狙う攻撃を仕掛けやすくなっています（標的型攻撃のSaaS化、Ransomware as a Service＝RaaSの台頭等々）。極端な話、小学生でも（多少英語さえ使えれば）利用できてしまうサービスが少なからず存在する時代、攻撃者の「DX化」も進んでいます。

そんな状況も手伝ってか、企業のゼロトラスト（＝誰も信じない）への関心も高まっています。役職等に基づいた権限の常時付与ではなく「必要な時間だけ、必要な相手にだけ、必要最小限の権限を付与し、終わったらすぐ付与した当該権限を抹消する」というのがゼロトラストの基本的な考え方ですが、使い勝手・運用面などを考えると各組織によってはまだまだ完全には徹底できないケースもあるでしょうし、各製品の仕様・初期設定などにもそれぞればらつきはあるため、しっかり設計・実装・運用しないと、単に導入しただけでは思わぬ落とし穴にはまる可能性も否定できません。また、そのための知見・経験を持つセキュリティ人材が不足している事も頭を悩ませる点と言えるでしょう。
「ゼロトラスト」は現状まだ過渡期と言え、その現実的な普及にはもう少し時間が必要になると思料します。

当面の間は攻撃者の多くがまず脆弱性を狙ってくることを踏まえ、定期的に「自分たちのどこに脆弱性が潜んでいるか」を調査・確認することを前提としセキュリティ対応を「分業」で考えること、一つ目にシステムで自動化が可能な部分（逆に人の手ではミスが拭い去れない作業）は「人に頼らないセキュリティシステム」を導入する。二つ目、それだけでは対応困難な部分はシステムを利用（ログ管理など）しつつ人が担当するセキュリティ（地道な教育・啓もうによるリテラシーの向上を継続）でITの利便性とセキュリティ強度のバランスを保つ。この両者を併用することにより、業務の生産性を最小限に抑えつつ強固なセキュリティ対策を実装することが現時点ではより効果的かと思料します。

あくまで「一定のセキュリティ強度の担保」は大前提ですが、強固なセキュリティを担保し「社内・社外ともに安心感を与えること」と構成員の「働きやすさ、満足度」の実現、あまりどちらか一方に偏り過ぎずある程度のバランスを保つことも、また重要ではないでしょうか。

■サイバーセキュリティクラウド　代表取締役CTO　渡辺洋司のコメント
2021年はランサムウェアの世界的な話題になり、攻撃者はデータ復旧の脅迫にとどまらず、3重、4重の脅迫まで行うことが世に知らしめられました。3重、4重の脅迫とその攻撃の中には Web サイトへの DoS/DDoS 攻撃などを行うと脅迫するものもあり、ランサムウェアだけの防御では事業影響を抑えきれなくなってきています。

2021年秋以降には、本レポートでピックアップしている Movable Type や Log4J の脆弱性が大きな話題になり、2022年になっても収束しきっていない状況です。
セキュリティパッチ等が公開されると攻撃手法も明確になりツールにも取り込まれるため、話題の脆弱性に対して多くの人が攻撃知識を手に入れられる時代になりました。防御に追われる企業は迅速な状況把握と対策が求められるわけですが、簡単にアップデートが可能かというと、アップデートに関する副作用の影響調査

であったりエンジニアの確保であったりと攻撃者の時間軸に比較して遅い対応となってしまうのが実情かと思います。

日々の脆弱性の把握と脆弱性が発見された場合の対策という継続的なシステムの健康診断の施策はもちろんのこと、システムの更改ができない場合においても一定の防御を行うという意味では 、防御ルールが迅速に利用可能であり、脆弱性が公開された後でも継続的に認識された高度化された攻撃手法に対して防御ルールが更新されていくクラウド形WAF の導入は非常に効果が高い対策といえます。

【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/

＜本件のお問い合わせ＞
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
電話：03-6416-9996　FAX：03-6416-9997
E-mail：pr@cscloud.co.jp