【ニュースリリース】

2023 年 5 月 23 日
株式会社サイバーセキュリティクラウド

報道関係者各位

「SQL インジェクション」が前年同期比で 250%も増加
～2023 年 1-3 月「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～

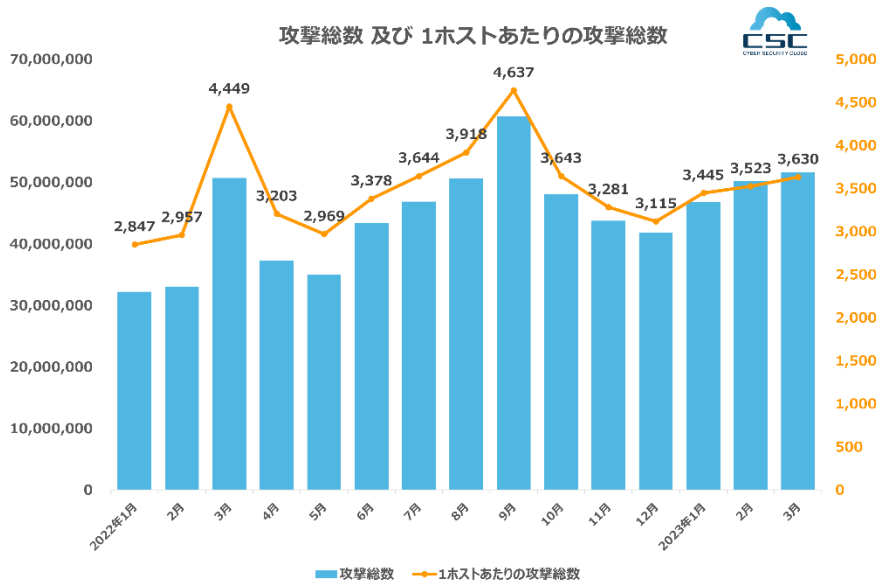
ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバー セキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池敏弘、以下「当社」）は、2023 年 1 月 1 日～3 月 31 日を対象とした『Web アプリケーションを狙ったサイバー攻撃検知レポート（以下「本レポート」）』を発表します。

本レポートは、当社が提供する 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 の『攻撃遮断くん』、及びパブリッククラウド WAF の自動運用サービス『WafCharm（ワフチャーム）』で観測したサイバー攻撃ログを集約し、分析・算出しています。

《 レポートサマリー 》

・サイバー攻撃数は昨年度末から微増傾向が見られる。
・「SQL インジェクション」が前年同期比で 250%も増加。
・「Brute Force Attack」も前年同期比で 166%の増加。

■ 2023 年 1 月～3 月のサイバー攻撃検知状況



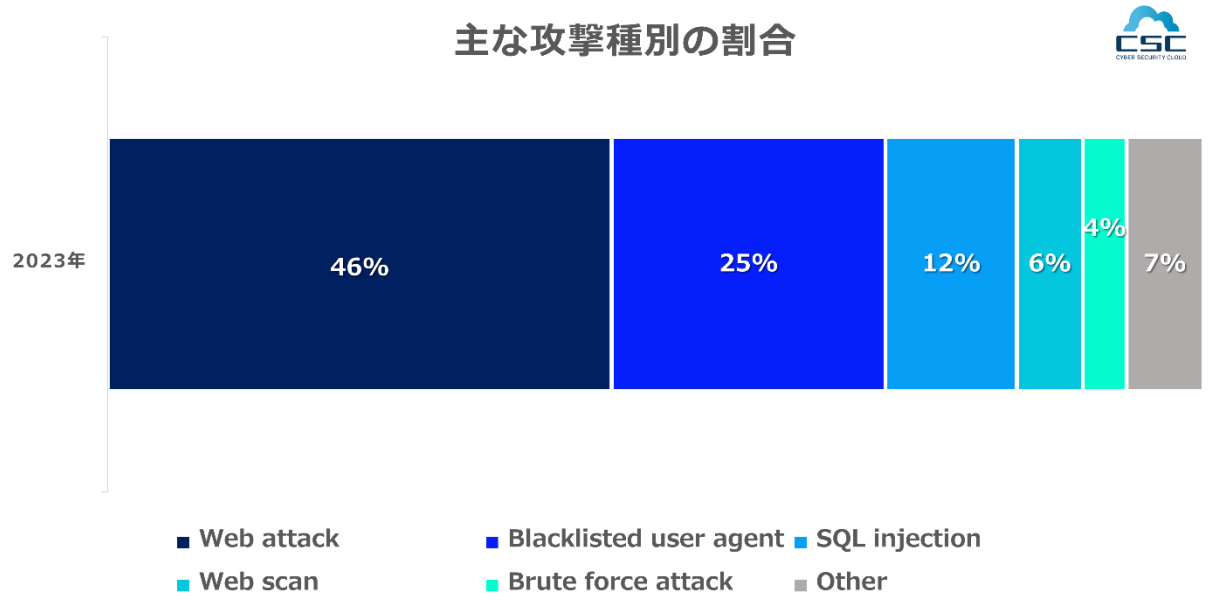
【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド 経営企画部 広報担当：竹谷・川﨑
TEL：03-6416-9996 Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997 E-Mail：pr@cscloud.co.jp

2023 年 1 月 1 日から 3 月 31 日までに、当社で検知した Web アプリケーションへのサイバー攻撃の総数は 148,631,502 件となり、1 ホストあたり（※）では 10,598 件でした。

また、今回は月を追うごとに攻撃数が増加しているものの、緩やかなペースにとどまりました。

※『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）と『WafCharm』の保護対象ホスト数（WebACL）との総数を分母に算出。

■ **攻撃種別ごとの検知状況**

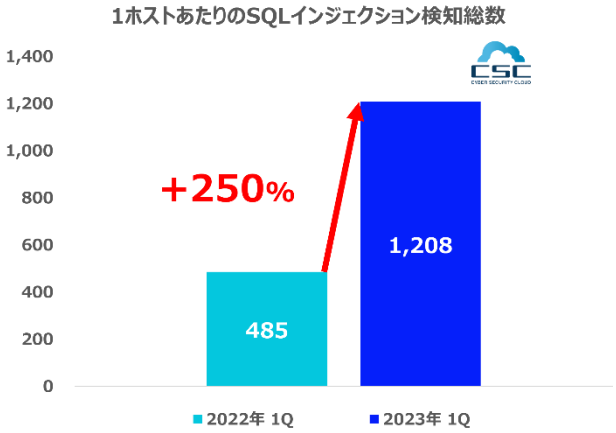


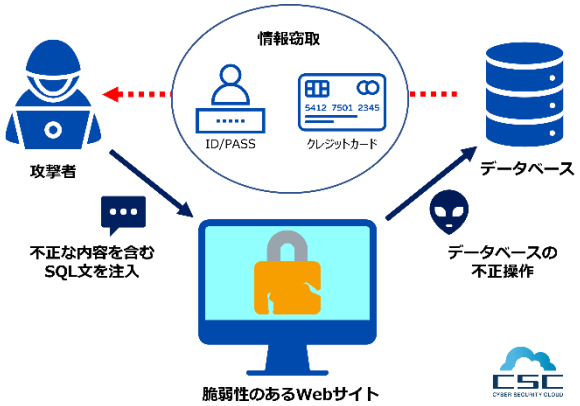
当社が検知したサイバー攻撃を攻撃種別ごとに分類すると、2023 年 1 月～3 月は Web サーバを構成するソフトウェアの脆弱性に対する攻撃である「Web attack」がおよそ 6,900 万件と全体の 46%を占めています。次いで、脆弱性スキャンツールなどを利用した Bot による攻撃である「Blacklisted user agent」がおよそ 3,700 万件で 25%に。また、システムの脆弱性を意図的に狙い、想定しない SQL 文を実行させ、データベースシステムを不正に操作する「SQL インジェクション」が、およそ 1,700 万件で 12%でした。

■ **攻撃種別で注目したいのは「SQL インジェクション」：前年同期比 250%増加**

SQL インジェクションとは、攻撃者が Web サイトなどの脆弱性（不完全さ・脆さ）を悪用し、不正に作成した「SQL 文（データベースの情報を動かす命令文）」をデータベースへのリクエスト内容に「注入（injection）」することで、データベースを不正に操作する攻撃です。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp





2022 年 1 月～3 月とで比較すると、2023 年 1 月～3 月の SQL インジェクションの攻撃総数は 5,481,900 件から 16,985,151 件とおよそ 310%（約 1,150 万件）増加していることが分かりました。1 ホストあたりでは、485 件から 1,208 件と前年同期比でおよそ 250%増加していました。

また SQL インジェクションが年々増加している理由には、次のようなものがあります。

- **簡単にサイバー攻撃を実行できる**

  SQL インジェクションは、Web フォームに対して簡単なスクリプトを挿入するだけで、攻撃することができます。

- **Web アプリケーションの脆弱性の増加**

  EC サイトなどを始めとした Web サービスが普及するにつれ、SQL インジェクションに対する脆弱性も増加しています。Web アプリケーション自体がさまざまな機能が追加され、Web サイトが複数システムの利用により複雑化していることが原因の 1 つとして挙げられます。

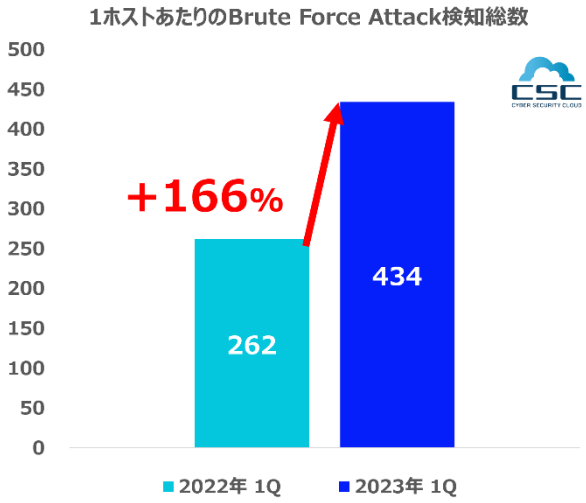
- **セキュリティパッチ未適用による脆弱性の放置**

  業務への影響の懸念やサイバーセキュリティ意識の欠如などから、脆弱性の報告されたソフトウェアがアップデートされずに放置され、悪用される可能性が高くなっています。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■ **次に注目すべきは「Brute Force Attack」：前年同期比 166%増加**

Brute Force Attack（ブルートフォースアタック）とは「総当たり攻撃」によるパスワードを解読する方法の一つです。



2022 年 1 月～3 月とで比較すると、2023 年 1 月～3 月のブルートフォースアタックの攻撃総数は 2,950,044 件から 6,074,706 件とおよそ 306%（約 312 万件）増加していることが分かりました。1 ホストあたりでは、262 件から 434 件と前年同期比でおよそ 166%増加していました。

また、ブルートフォースアタックの増加理由には、次のようなものがあります。

- **ユーザによる脆弱なパスワードの利用**

  多くの方が脆弱なパスワード（短い、予測可能、同じパスワードの使い回し）を使用しています。この現状から、ブルートフォースアタックは成功率の高いサイバー攻撃となっています。

- **クラウド環境の膨大な計算リソースの利用**

  高速化・高性能化したコンピュータを利用することで、攻撃者は以前よりも大量のパスワードを短時間で試すことが可能になりました。

  特にクラウドコンピューティングの台頭により、莫大な計算リソースを手軽に利用できるようになったことは、ブルートフォースアタックの増加に大きく影響しています。

- **自動化ツールとボットネットの悪用**

  自動化ツールとボットネットを悪用することで、攻撃者は大量のログイン試行を自動的に行うことができます。

  これらのツールはインターネット上で広く公開されており、ブルートフォースアタックの増加を助長しています。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

- **パスワード情報漏洩の頻発**

  大規模なデータ漏洩が頻発しており、漏洩したアカウント情報（ユーザ名 / パスワード）がブルートフォースアタックに利用されています。

  これらのアカウント情報はダークウェブ上で更なる攻撃のための「辞書データ」として公開されています。

- **セキュリティ対策の不備**

  多くのシステムや Web サイトは適切なサイバーセキュリティ対策を行っておらず、ブルートフォースアタックへの対策が不十分です。

  例えば、多数のログイン失敗が見られた際に対象アカウントを一時的にロックするなどの対策を適切に行っていない場合が挙げられます。

■ 株式会社サイバーセキュリティクラウドについて

所在地：東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 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

サイバーセキュリティクラウドは「世界中の人々が安心安全に使えるサイバー空間を創造する」という経営理念を掲げ、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービス、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

■ 調査概要

・調査対象期間：2023 年 1 月 1 日～2023 年 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』で観測したサイバー攻撃ログの分析

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑

TEL：03-6416-9996　Mobile：080-4583-2871(川﨑携帯)

FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp