月次Webセキュリティ運用レポート

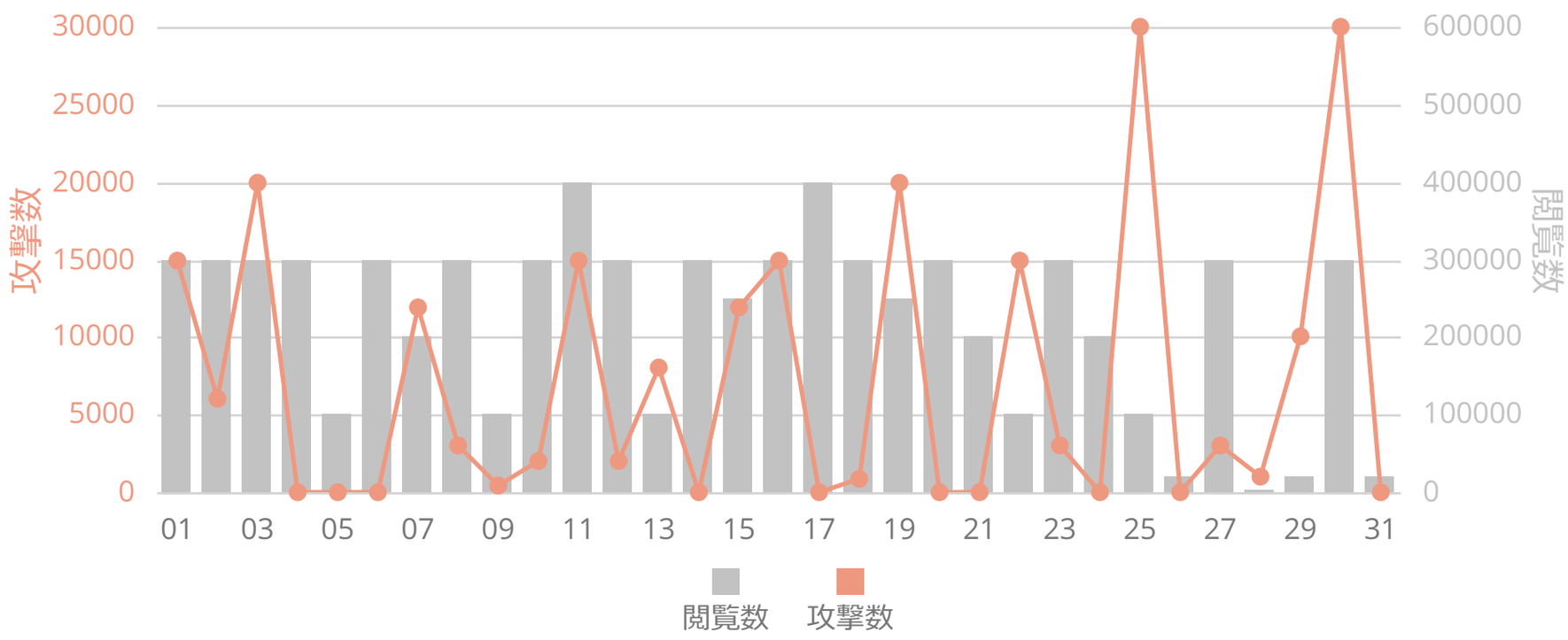
Aug, 2021 sample.cloudbric.com

本レポートは、5月1日から5月31日における、保護対象のWebサイト 「sample.cloudbric.com」のWAFサービスの運用状況のサマリーです。

本Webサイトにセキュリティサービスを適用したことにより、 223,300 件の不正なリクエストや悪意あるアクセスから保護されています。これらの不要なリクエストは、本Webサイトに想定外の影響を及ぼし、将来の情報漏えいの起因となる可能性があります。尚、不要なWebリクエストやトラフィックを遮断することで、回線の帯域を節約しWebサーバのリソースをより効率よく利用することができます。

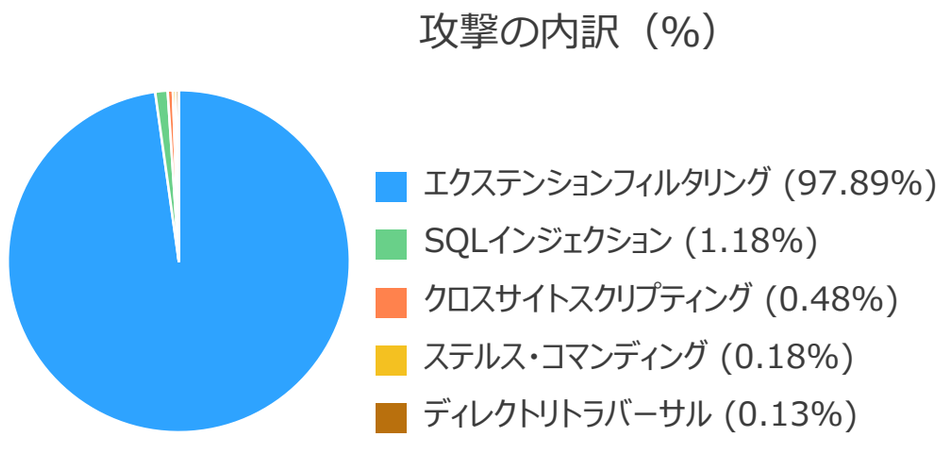
今月の運用サマリー

攻撃数	ハッカー	正常なアクセス数	今月のトラフィック量
223,300	26,402	6,962,000	81636.75GB



遮断した攻撃の情報

本項目は、指定の期間内における攻撃をグラフ化したものであり、最も多い攻撃タイプについて述べています。



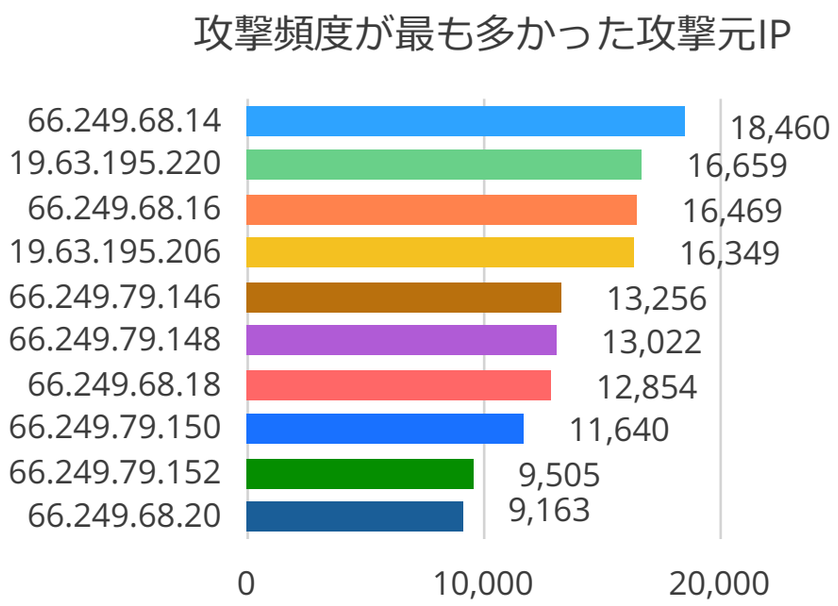
最も多く発生した上位5個の攻撃タイプが表示されます。
今月発生したすべての攻撃タイプは検知ログメニューで確認できます。

最も多い攻撃タイプ:
エクステンションフィルタリング

Webサーバの内部ファイルへのアクセス許可が緩く設定されていると、悪意のある攻撃の対象になる可能性があります。 これを防ぐには、Webブラウザからユーザが入力したURLの拡張子を検査し、許可された拡張子以外のアクセスをブロックする必要があります。

攻撃元IPアドレスの情報

本項目では、Webサーバに悪意のある攻撃をしかけた上位の攻撃元IPアドレスを表示します。 悪意のある訪問者と判断されるIPアドレスの場合は、ブロックリストIPに登録することをご検討下さい。



攻撃頻度が最も多かった上位10個の攻撃元IPが表示されます。
今月発生したすべての攻撃IPは検知ログメニューで確認できます。
発生件数が同じIPがある場合、IPは10個まで表示されます。

Web攻撃発信国の情報

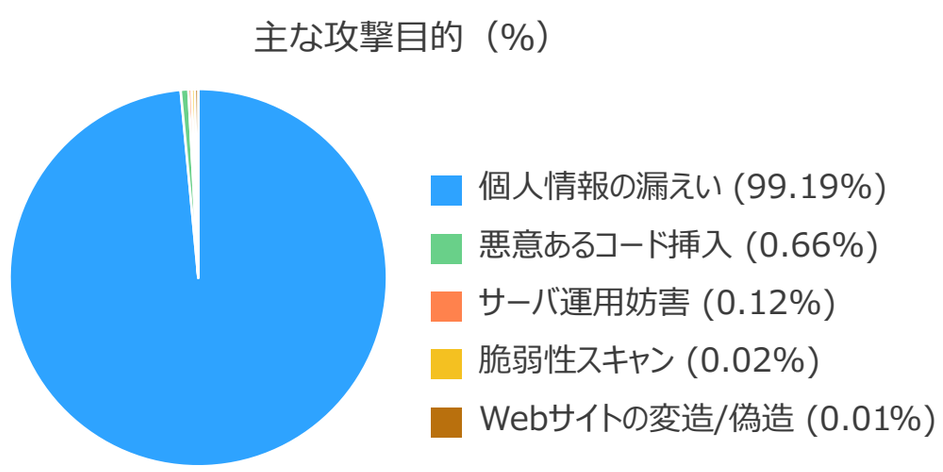
本項目では、保護対象のWebサイトに対し、最も頻繁に攻撃を発信した国や地域を確認できます。信頼しない国および特定地域へのWebサービスをしない場合は、それらの国に対し、遮断設定を行うことを推奨致します。但し、Web攻撃者より不正なIPが採用され、特定の場所を隠蔽したアクセスがある場合、「不明」と表示されます。

順位	発信国	割合(%)
1	アメリカ	77.64%
2	日本	22.17%
3	中国	0.48%
4	ロシア	0.31%
5	マレーシア	0.29%
6	セーシェル	0.17%
7	ドイツ	0.13%
8	香港	0.12%
9	イタリア	0.08%
10	フランス	0.06%

１）最も攻撃頻度が多かった上位10カ国が表示されます。
今月発生したすべての攻撃発信国は検知ログメニューで確認できます。
発生件数が同じ国がある場合、10カ国まで表示されます。
２）「不明」の場合は順位に含まれません。

Web攻撃の目的別の情報

本項目では、指定の期間中遮断した攻撃タイプのデータに基づき、Webハッカーにより行われる攻撃の目的別に分類し、表示します。



個人情報の漏えい

個人情報の漏えいには、重要な個人情報をWebサイトに公開（Privacy Input/Output Filtering)する、個人情報を含むファイルをアップロードする（Privacy File Filtering)、もしくは、Webサイトのディレクトリ情報が露出する（Directory Listing）攻撃を含みます。

悪意あるコード挿入

ハッカーは、悪意のあるスクリプトコードを、Webサーバの脆弱性を突いて追加する(XSS)、サーバサイドへ意図的に不正なコマンド実行を強制する（Stealth Commnading)、通常とは異なるアクセス手段を用いて悪意あるリクエストコードを送信し続ける（Suspicious Access）等により、Webサーバの利用者情報を搾取しようとします。

サーバ運用妨害

サーバ運用妨害とは、一般的なサーバ操作の混乱を指します。 これには、サーババッファーのフラッディング（バッファオーバーフロー）や不正な手段やヘッダーによるリクエスト送信などの攻撃が含まれます。

脆弱性スキャン

脆弱性スキャンは、Webサーバの既に現存する脆弱性を診断します。 これは、自動攻撃ツールを使用して最も頻繁に実行されます。 これらのツールは、無効なHTTPリクエストやRFC標準に従っていないURIを送信したりまたは、サイトのディレクトリエラーメッセージを公開します。

Webサイトの変造/偽造

Webサイトの変造/偽造とは、権限のない個人によるWebサイトの操作を指します。 これには、Webサイトの内容の改ざん、不正ユーザによりSQLサーバへの悪意のあるコードの追加した情報取得（SQL Injection）、.exe、.jps、.phpなどの許可されていないファイルをWebサイトへのアップロード （File Upload）、および危険なスクリプト、ファイル、または悪質なコードの挿入（Include Injection）が含まれます。