月次Webセキュリティ運用レポート

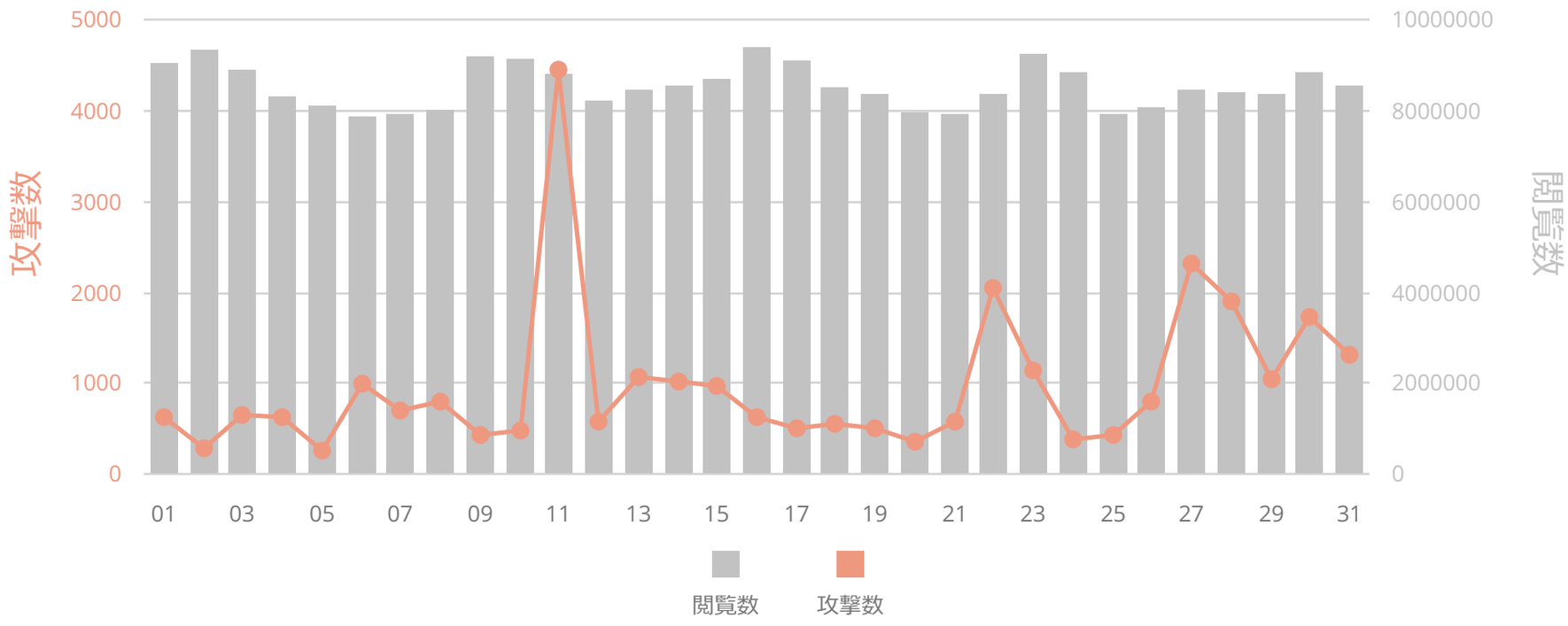
Feb, 2021 sample.cloudbric.com

本レポートは、1月1日から1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、 29,824 件の通常のWebサイト訪問者とは異なる、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適切に使用ことができます。

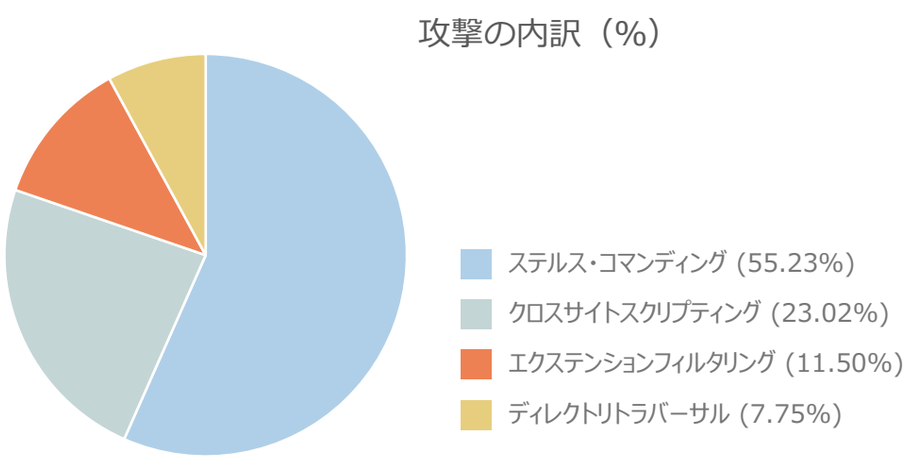
今月の運用サマリー

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
29,824	6,442	264,572,729	6725.60GB



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。



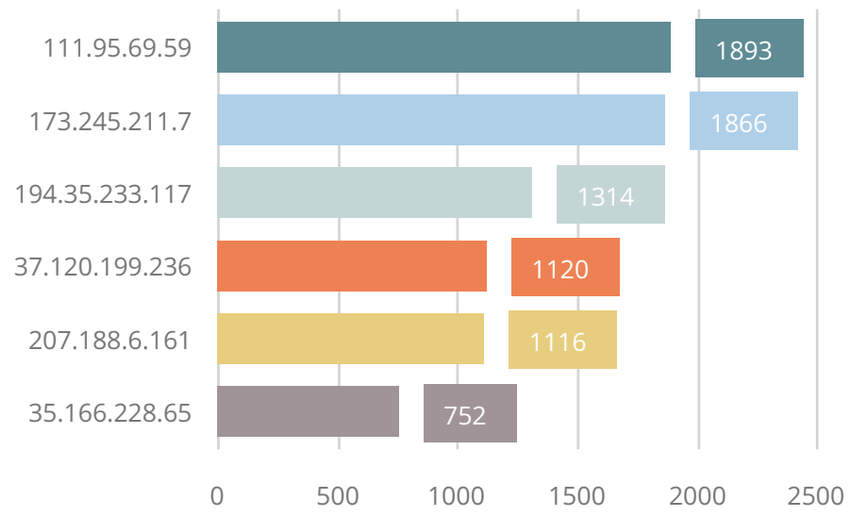
最も多い攻撃タイプ:
ステルス・コマンディング

多くのWebアプリケーションは、機能を実行するためにOSや外部プログラムを使用します。 Webアプリケーションが HTTPリクエストを受信して外部プログラムに情報を送信する場合、攻撃者は情報を改ざんし、悪意のあるコマンドを挿入させます。 その後、OSや外部プログラムがこの改ざん情報を実行させることにより、トロイの木馬を植え付けたり、悪質なコードの実行を強制します。

攻撃元IPアドレスの情報

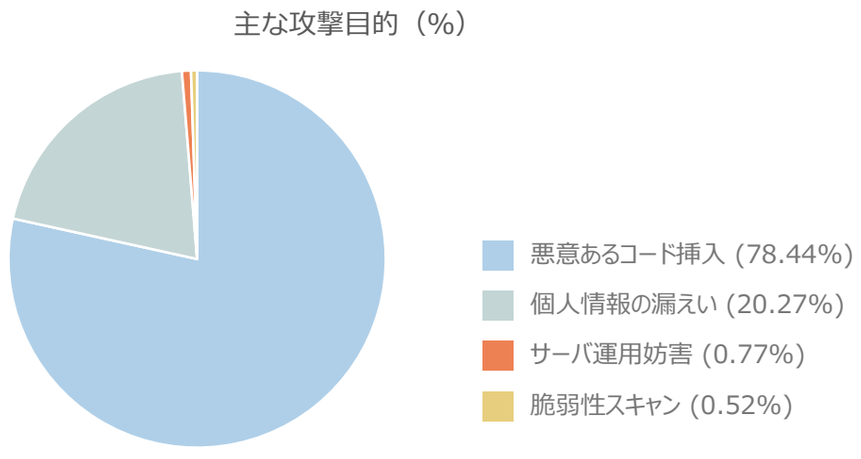
本項目では、Webサーバに悪意のある攻撃をしかけた上位の攻撃元IPアドレスを表示します。 悪意のある訪問者と判断されるIPアドレスの場合は、ブラックリストIPに登録することをご検討下さい。

攻撃頻度が最も多かった攻撃元IP



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。



最も多く遮断された攻撃の目的: 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。

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	45.72%
2	日本	20.59%
3	インドネシア	6.59%
4	イギリス	6.23%