報道関係各位
Press Release

2017年3月16日
株式会社サイバーセキュリティクラウド

【2016年度 サイバー攻撃白書】
2016年は3～4月の”生活シーン切替時”に攻撃が急増！
最も多い攻撃元の国は“中国”が1位に

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：大野 暉、以下「サイバーセキュリティクラウド」）は、2016年度のサイバー攻撃の実情についてまとめた、「2016年度 サイバー攻撃白書」を発表いたします。

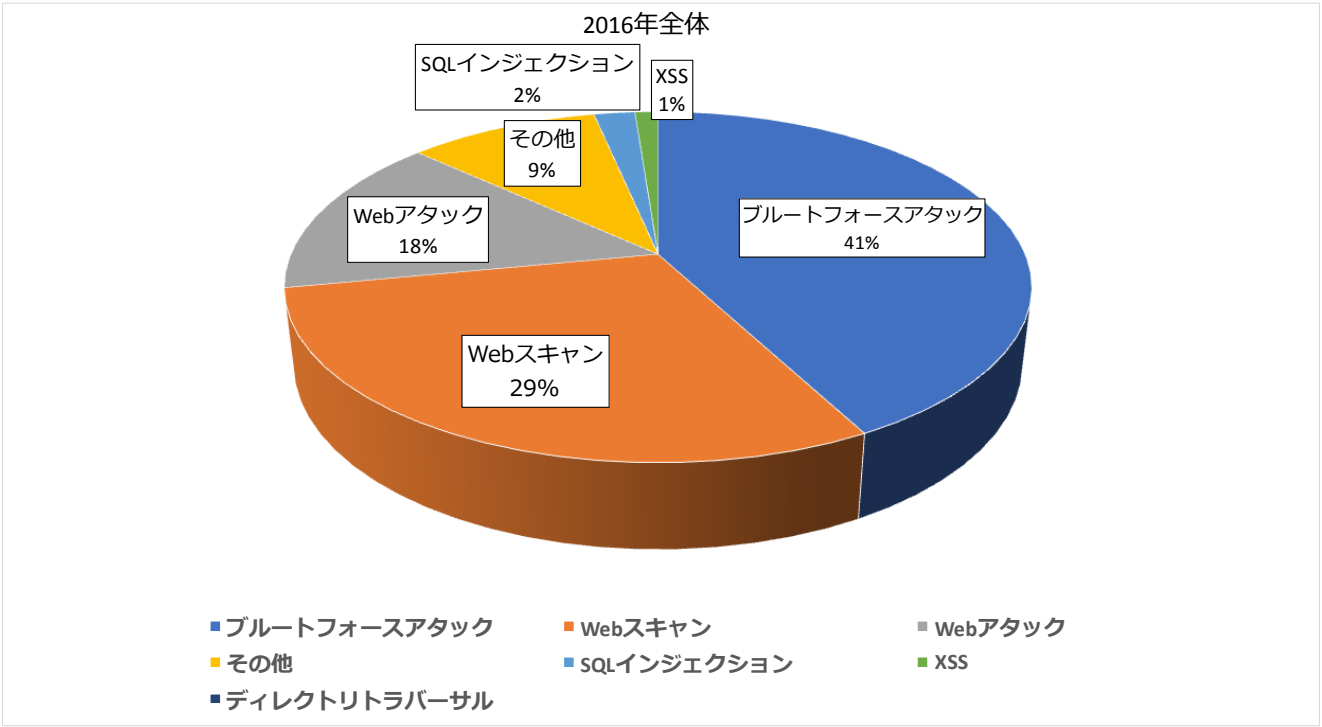
「2016年度 サイバー攻撃白書」とは、WebサイトやWebサーバへのあらゆる攻撃を遮断するクラウド型WAFのセキュリティサービス「攻撃遮断くん」で観測した攻撃ログを集約し、分析・算出した調査レポートです。本レポートを公開していくことで、各業界の企業に対してサイバーセキュリティに関する意識喚起を行ってまいります。

■「2016年度 サイバー攻撃白書」概要
-調査対象期間　　：2016年1月1日（金）～2016年12月31日（土）
-調査方法　　：「攻撃遮断くん」で観測した攻撃ログの分析
-調査数（有効サンプル数）　：1652サイト

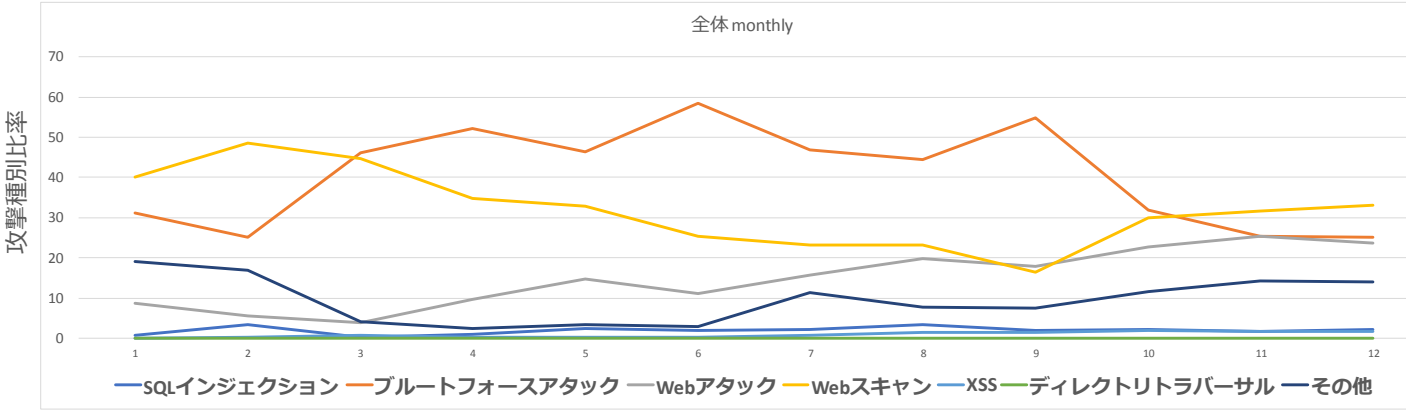
■2016年全体での攻撃状況

2016年全体で「攻撃遮断くん」導入企業への攻撃状況は、攻撃可能なWebページを探す「Web スキャン」と、無作為に既知の脆弱性を試行する「Web アタック」や、パスワードリスト攻撃等の「ブルートフォース」が攻撃の約90%を占めており、ツールを使った無作為なスキャン活動と思われる活動が多く見受けられました。

また、12月には2016年を通して最高攻撃数となる2,870,132件を記録しています。



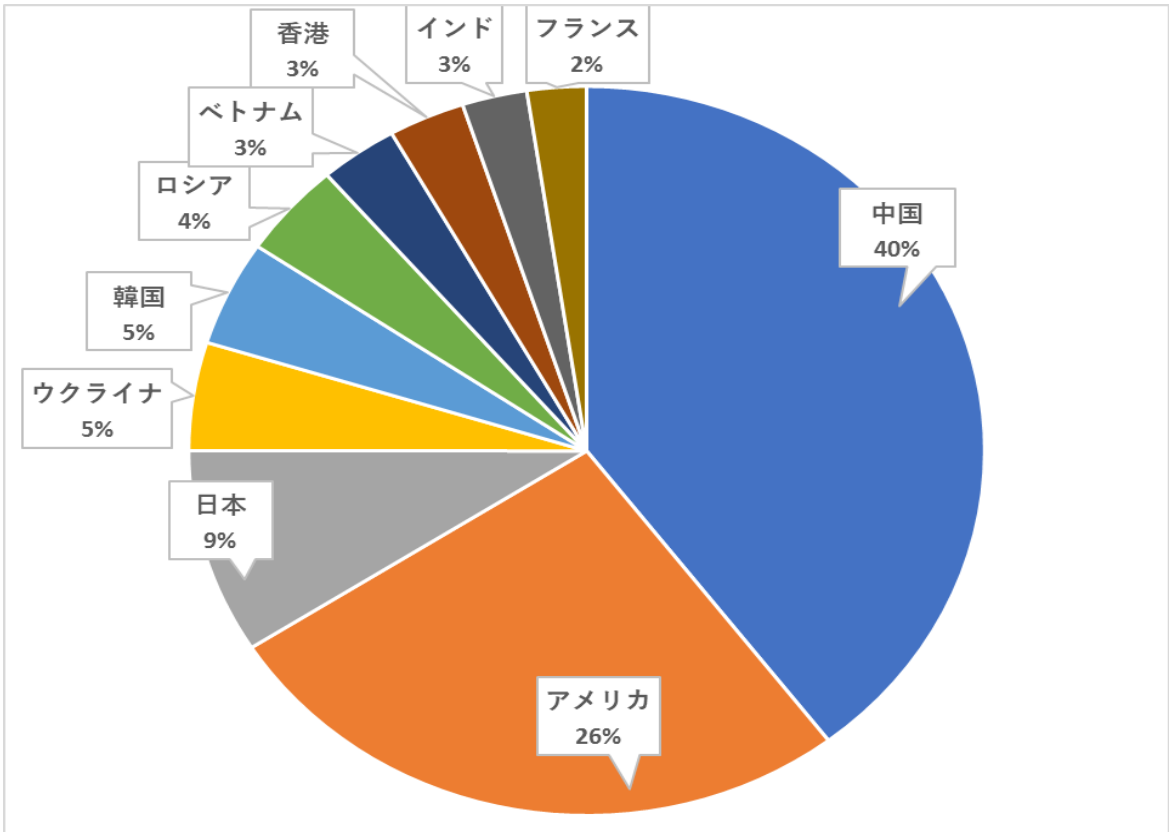
時系列に見た場合、主な攻撃種別が３，４月を境に変化しますが、これは日本の生活シーンの切り替わりに関係していると考えられます。新たなサービス利用時、過去に使っていたサービスの放置、担当者の変更などによる引継ぎの不備に対し注意が必要といえます。



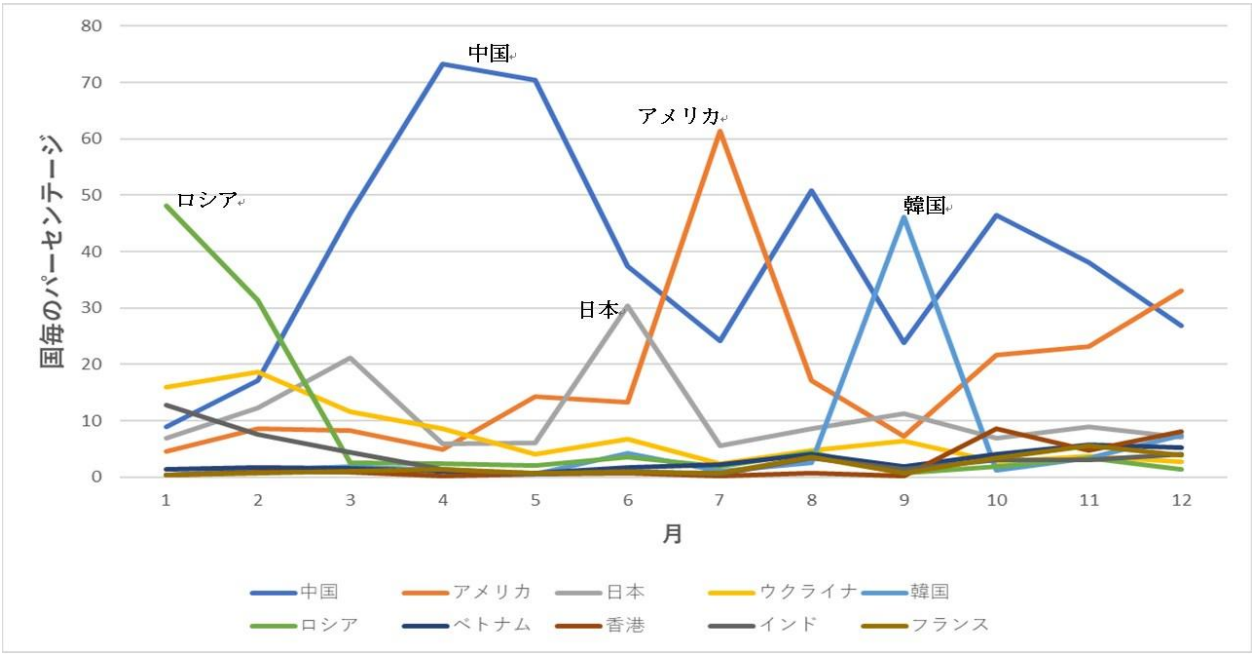
■ 国別での攻撃状況

２０１６年に検知した攻撃の攻撃元IPアドレスを国別に集計したのが、下記のグラフです。「攻撃遮断くん」導入サービスにおける、攻撃元の国 Top 10 の１位は中国でした。

それぞれの順位とパーセンテージは、１位：中国（４０%）、２位：アメリカ（２６%）、３位：日本（９%）、４位：ウクライナ（５%）、５位：韓国（５%）、６位：ロシア（４%）、７位：ベトナム（３%）、８位：香港（３%）、９位：インド（３%）、１０位：フランス（２%）でした。



時系列に見た場合、１，２月はロシアからの攻撃が多く、アメリカ、日本、韓国は時期的なピークがある一方、中国からは定常的に多くの攻撃があることがわかります。



■攻撃概要

1. SQLインジェクション

SQLインジェクションはwebアプリケーションの脆弱性を利用し、アプリケーションが想定してないSQL文を実行させることで、DBを不正に操作する攻撃です。

2. ブルートフォースアタック

ブルートフォースアタックは暗号解読やパスワードを割り出すために総当たりで攻撃するものです。

3. WEBアタック

WEBアタックはDos攻撃に近い攻撃やOSコマンドインジェクションを行う攻撃です。

4. WEBスキャン

WEBスキャンは攻撃の対象を探索する動作や、無作為に行われる単純な攻撃で脆弱性を探す攻撃予兆です。

5. クロスサイトスクリプティング

クロスサイトスクリプティングは攻撃者が作成したスクリプトを脆弱性のあるWEBサイトを利用し閲覧者に実行させる攻撃です。

6. ディレクトリトラバーサル

ディレクトリトラバーサルはWEBサーバ上のファイルに不正アクセスする攻撃です。

7. その他

各種OSやミドルウェアなどの脆弱性を突いた攻撃をその他としております。 通常、WAFの範囲外とされるものなども含みます。WebサイトないしWebアプリケーションを経由しない攻撃です。

■専門家コメント（総括）

2016 年は例年通りWordPressやMovable Type, Joomla などに代表されるCMSのプラグインに関する脆弱性、Apache Struts のようなアプリケーションフレームワークに関する重大な脆弱性が報告されました。

実際にこれらの脆弱性を狙った攻撃が多数発見されました。この様な脆弱性を把握し標的を絞った攻撃は多く存在し、甚大な被害につながるケースがあります。しかしながら、多くの攻撃は、踏み台可能なサーバを見つけるための準備段階のスキャンとして、攻撃を実施するケースとなっています。そのため、自社サイトは誰もアクセスしない、攻撃するメリットが無いという観点での誤ったリスク評価は大変危険です。

また、３，４月の総当たり攻撃が増加していることから、新規ユーザの突破されやすいパスワードや、休眠アカウントを狙った乗っ取り、システム管理者の異動による監視レベルの低下などが注意すべきポイントとなると考えられます。

国別では攻撃元のTop 10 の１位は中国でしたが、日本からの攻撃も増えています。海外のIPアドレスを制限していれば安心ということはなく、根本的な対策の検討が必要でしょう。

株式会社サイバーセキュリティクラウド
CTO　渡辺 洋司

【株式会社サイバーセキュリティクラウド　概要】

■会社名　：株式会社サイバーセキュリティクラウド
■設立　：2010年8月
■資本金　：1億4,450万円 ※資本準備金を含む
■代表者　：代表取締役　大野 暉
■事業内容　：サイバーセキュリティ事業
(1) Webセキュリティサービスの開発・運用・保守・販売
(2) サイバー攻撃対策コンサルティング
■企業ホームページ　：http://www.cscloud.co.jp/
■サービスページ　：https://www.shadan-kun.com/