japan@menlosecurity.com
www.menlosecurity.com

日本の上位50サイトのウェブセキュリティレポート（Q2–2016）

本レポートでは、ウェブ閲覧リサーチ会社Alexaにて報告された日本のユーザーから2016年5月5日時点の閲覧されたウェブサイトの上位50サイトをベースに、メンロセキュリティによる開発ツールを用いた独自調査による、それらのウェブサイトの脆弱性に関する状況をまとめたものです。実際に上位50サイトのうち15サイトの閲覧結果から脆弱性が報告されているバージョンのソフトウェアの使用が確認されました。また、それら15社のうちの半数以上がよく知られた誰もが使用する、一見すると信頼性が高いと思われるサイト（プロバイダーのポータルサイトやブログなど）でした。このような脆弱性は何故そこにあり、どこから来るか確認してみると昨今のインターネットにおけるセキュリティの問題が浮き彫りとなりました。

今回の5月5日時点での集計と、前回の1月15日時点でのAlexaによる日本の上位50サイトの詳細を見てみると、そこには脆弱性とは別にある傾向が強く出ていることが確認できます。Yahoo, Googleなどの大手検索サイトはもとより、Twitter, FacebookやYoutubeなどの他国でも上位を占めるサイトは日本でも上位10社に入っていました。上位50サイトでブログに関するドメインが多数報告されているのも特徴的であると思います。上位50サイトのうちのアダルトサイトの数が前回の５社から２社に減っていました。日本特有の小売製品の価格の比較サイトや小売店のサイト自身やレストラン検索なども散見されます。

何故、ブラウザはスクリプトを必要とするのでしょうか？

“あなたのブラウザで JavaScript を有効にする方法” URL: http://www.enable-javascript.com/ja/ より

実際に日本の上位 50 ウェブサイトで使用されている Java Script のスクリプトの数とサイズを以下の定義に従って確認してみました。

- ウェブサイトを表示した際に実行されるスクリプト（海外ドメインによって実行されるものを含む）の数
- 該当サイトをブラウザが閲覧した際にダウンロードされたコードのサイズ

上記の二つのポイントにおいて確認することで、ウェブ閲覧時にサイトがたくさんのスクリプトを提供していることがわかります。たくさんのスクリプトが大量に送られてくることは、閲覧時のリスクも同様に増えていると言えるでしょう。

1. 上位50のウェブサイトでのスクリプト実行の状況

上位50サイト全般を通して以下の状況が確認されました。

- 実際に上位50サイトの閲覧時には多くのJavaScriptがブラウザ上で実行されています、JavaScriptの使用は前回の21から23.76と若干ながら増えています。
- その最大は99のスクリプトが一つのリクエストで実行されました。
- 上位50サイトで30を超えるスクリプトが実行されたのは全体の30%以上で、20以上となると半数を超えます。
- スクリプトの実行数の多い上位10サイトは小売店、ソーシャルメディア、レストラン検索と多岐に渡っていました。

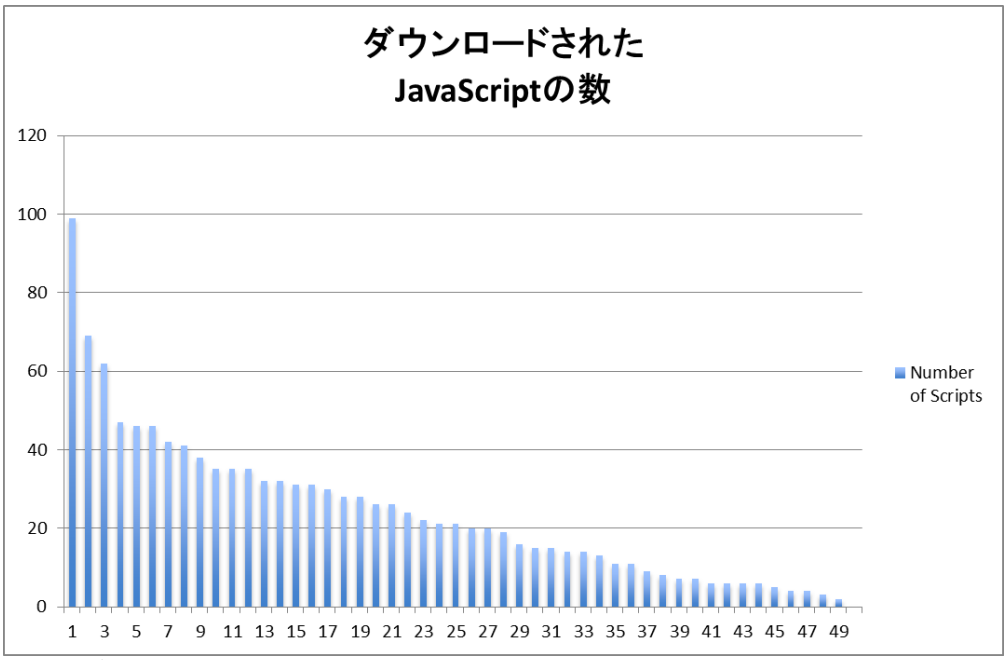

表1. ダウンロードされたJavaScriptの数

japan@menlosecurity.com
www.menlosecurity.com

2. 上位50のウェブサイトでダウロードされたコードサイズ

上位50サイトの一つ一つのサイトからダウンロードされるコードの総量を測定してみると驚きの結果を得ました。

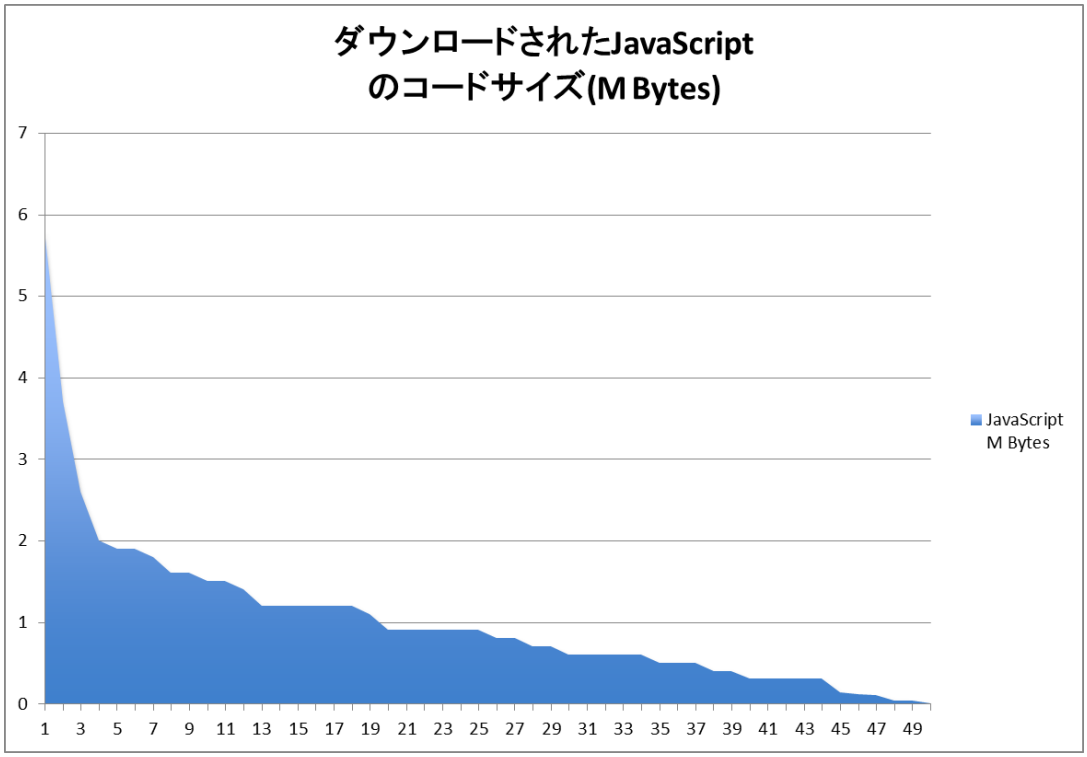

表2. ダウンロードされたJavaScriptのコードサイズ(M byte)

上位50サイト全般を通して以下の状況が確認されました。

- 上位50サイトからブラウザに送られてくるコードの平均サイズは1Mバイト超というものでした。
- ほとんどのサイトからは1Mバイト以下のコードが送られてきます。
- 上位3サイトからは2.5Mを超えるサイズのコードが送られてきています。
- 上位10サイトには頻繁に使われるソーシャルメディア、レストラン検索、ブログなどが多数含まれています。
- 今回の結果は各サイトのトップドメインへのアクセス結果です、配下のページではさらに多くのコードが使用されています。

3. 上位50ウェブサイトに関連する脆弱性

本レポートでは、日本における上位50サイト、もしくはその背後にあるウェブサイトへアクセスした際のコードから確認された稼働しているサーバーのバージョンについて報告します。これらのバージョンから既知の脆弱性の有無をMITREのCVEのデータベースで確認できます（CVEについてはhttps://www.ipa.go.jp/security/vuln/CVE.htmlを参照ください）。確認できた内容は：

- 実に50サイト中15サイトにおいて17件の脆弱性が報告されているウェブサーバーからコードがダウンロードされていたということです。
- マイクロソフトIISのバージョン7.5/8.５は、多くの脆弱性が早くから報告されており、旧いものでは５年以上も前から報告されています。

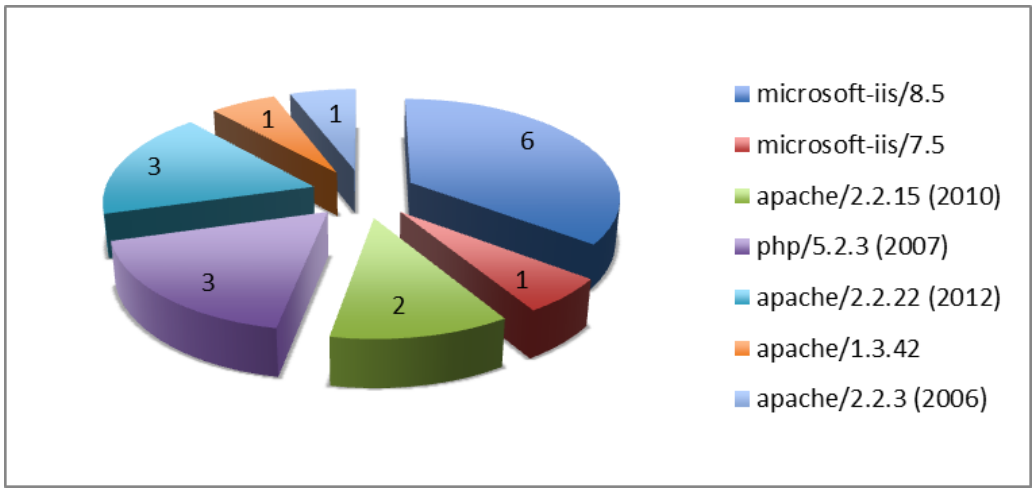

表 3.ウェブサイト閲覧の日本の上位 50 サイト–脆弱性の可能性状況（件数）

考察

上記の結果から、日本において最もポピュラーな50のウェブサイトにおいて考察として言えることは、今日ウェブサイトの提供側はユーザーへの有用性としてウェブサイトの開発者がスクリプトを使用する多くの合法的な理由がありますが、同時に攻撃者は、ウェブアクセスを通じた攻撃として、iframeタグやenbedタグを使用しての悪意のある広告サイトへの勝手な誘導を可能としていることにもなるのです。
ここ数年では、NoScriptのような技術を使用することがウェブセキュリティの専門家などからも提唱されてきていたが、スクリプトの実行を制限するために実際の現場での導入については技術的にも、他の運用的な問題でもユーザーの運用面の制限なくすることは難しい状況であることは様々な方面から報告されています。

今回の調査で確認された注意しなければならないことは、私たちが普段頻繁にアクセスしているポピュラーなウェブサイトにおいても、毎日のように報道されているインシデントで知られているように脅威のリスクがあるということです。つまり、信頼性の高いと思われるウェブサイトでも全くの安全とは言えないということです。

今回の調査で日本から頻繁にアクセスされる上位50のウェブサイトでは平均して24近いスクリプト（幸い今回の弊社の調査時点ではそれらのスクリプトには脅威は見つかっていません）が実行されているという事実です。もし、あなたの会社の社員が今回の上位5社のウェブサイトをアクセスしただけで200以上のスクリプトがその社員のPCで実行されていることを知ったら、そのサイトへ躊躇なくアクセスできますか？
ほとんどのサイトでスクリプトの使用を許可しないと有用性の高いアクセス、情報取得が不可能な今日で、常に脅威の可能性を含むスクリプトの実行をユーザーPC上から分離された環境で実施し、実施した結果の表示情報を無害化してユーザーPCに届ける隔離(Isolation)技術によってセキュリティを確保されたアクセスであれば、あなたのブラウザ環境に襲いかかるかもしれないこのような脅威への心配は無用となります。

追記：

試験実施日 – 2016年5月5日（木）
ブラウザ環境 – Chrome version 47.0.2526.106 (64-bit) on El Capitan 10.11.2
参考 - Alexa Top 50 for Japan - http://www.alexa.com/topsites/countries/JP.

※2016 年 6 月 10 日　一部に誤記がございましたため、訂正いたしました。