平成 27 年3月 12 日

Topic

「Islamic State（ISIS）」と称する者によるウェブサイト改ざんに係る注意喚起について[i, ii]

警察庁においては、国内の複数のウェブサイトが「Islamic State（ISIS）」と称する者によって改ざんされたことを把握しています。ウェブサイトの管理者はウェブページの改ざんの有無を確認するとともに、改ざんされないように対策を再度確認することを推奨します。

1 ウェブサイトの改ざん状況について

改ざんされたウェブサイトにアクセスすると図1のように表示され、「Islamic State（ISIS）」と称する者が改ざんしたように見られます。

図1 ウェブサイトの改ざん状況

i 「Islamic State（ISIS）」と称する者によるウェブサイト改ざんについて」（平成 25 年3月 11 日）
http://www.npa.go.jp/keibi/biki/201503kaizan.pdf

ii ウェブサイト改ざんに関しては、これまでにも3回注意喚起を実施しています。
「ウェブサイト改ざん事案の多発に係る注意喚起について」（平成 25 年5月 24 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130524_1.pdf
「外見上変化のないウェブサイト改ざん事案の多発について」（平成 25 年6月7日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130607.pdf
「ウェブサイト改ざん事案の再多発に係る注意喚起について」（平成 25 年9月 30 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130930.pdf

2 「WordPress」のプラグインの脆弱性について

改ざんされたサイトのいくつかはCMS[i]の「WordPress」を使用していることを確認しています。「WordPress」は、プラグインにより機能を追加することができますが、プラグインの脆弱性が平成 27 年2月1日から3月 11 日までに8件公表されています[ii]。そのうち3件がクロスサイトスクリプティングの脆弱性であり、当該脆弱性を悪用された場合、任意のスクリプトやコンテンツをウェブサイトに挿入される可能性があります。

警察庁の定点観測システムにおいては、「WordPress」向けのプラグインの探索行為と考えられるアクセスを観測しています（図2）。

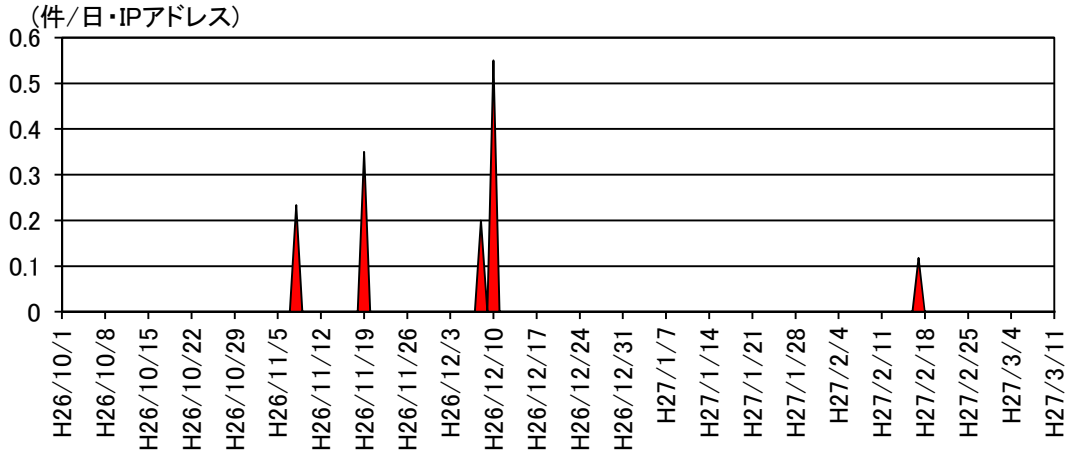

図2 「WordPress」向けのプラグインの探索行為と考えられるアクセスの検知件数
（平成 26 年 10 月1日～平成 27 年3月 11 日）

---

i CMS（Content Management System）は、専門的な知識がなくても簡単にウェブサイトを構築・管理できるようにするため、ウェブサイトを構成するコンテンツファイルを統合的に管理するシステムの総称です。

ii 「WordPress 用 FancyBox プラグインにおけるクロスサイトスクリプティングの脆弱性」（公開日：平成 27 年2月4日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001539.html
「WordPress 用 Apptha WordPress Video Gallery プラグインの videogalleryrss.php における SQL インジェクションの脆弱性」（公開日：平成 27 年2月 11 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001621.html
「Wordpress 用 WordPress Survey and Poll プラグインにおける SQL インジェクションの脆弱性」
（公開日：平成 27 年2月 11 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001634.html
「WordPress 用 Ninja Forms プラグインにおけるクロスサイトスクリプティングの脆弱性」（公開日：平成 27 年2月 12 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001658.html
「WordPress 用 Image Metadata Cruncher プラグインにおけるクロスサイトリクエストフォージェリの脆弱性」
（公開日：平成 27 年2月 13 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001567.html
「WordPress 用 Easy Social Icons プラグインにおけるクロスサイトリクエストフォージェリの脆弱性」
（公開日：平成 27 年2月 19 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001632.html
「WordPress 用 Contact Form DB プラグインにおけるクロスサイトリクエストフォージェリの脆弱性」
（公開日：平成 27 年2月 23 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001723.html
「WordPress 用 WP Media Cleaner プラグインにおけるクロスサイトスクリプティングの脆弱性」（公開日：平成 27 年2月 26 日）
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001650tml

3 推奨する対策（再掲載）

各組織や個人が管理するウェブサイトが改ざんされないように次の事項を再度確認することを推奨します。

- CMS やサーバー管理ソフトウェアの利用有無と、利用している場合には最新のバージョンであるかを確認する。
- FTP、SSH、CMS 及びサーバー管理ソフトウェア等のアカウントを適切に管理する。
- サーバーにおいて稼働している不要なサービス及び機能は可能な限り停止する。
- コンテンツ管理やサーバー管理のためのアクセスは必要最小限の範囲で許可し、不要なアクセスについては制限する。
- コンテンツ管理及びサーバー管理作業用のコンピュータへのマルウェア感染を防止する。可能であれば、作業を行うコンピュータについては専用のものとする。
- 各種ログについて定期的な監査を実施する。
- 正常な状態のコンテンツファイルのバックアップ、ハッシュ値リスト等を作成しておき、サーバー上のファイルと定期に比較を行うことにより、意図していないファイルの変更や作成がないかを確認する。

また、ウェブサイトが改ざんされた場合に、改ざんの原因となった脆弱性を修正することなくコンテンツファイルのみを修復して公開を再開しても、同一の手法で再度改ざんされる可能性があります。サイト復旧時には原因となった脆弱性を修正してから、公開を再開する必要があります。