10月のインシデント

1 他 **1日**：総務省は、複数のISP事業者やセキュリティベンダー等と連携し、利用者のマルウェアへの感染防止と駆除の取り組みとして、マルウェア配布サイトへのアクセスを未然に防止する実証実験などを行う官民連携プロジェクト（ACTIVE）を11月1日から実施することを公表した。
「『ACTIVE』の実施及び『ACTIVE推進フォーラム』」の開催（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000059.html）。

2 他 **2日**：米国議会の暫定予算案不成立により、一部の連邦政府機関が閉鎖され、国立標準技術研究所（NIST）など複数の政府関係のサイトが閲覧できなくなった。この措置は10月17日に解除された。

3 セ **3日**：GitHubが大規模なDDoS攻撃を受け、翌日までの間、断続的にサービス障害が発生した。
詳細については、次のGitHubStatusの10月3日のメッセージで確認できる。"Status Messages"（https://status.github.com/messages/2013-10-3）。

4 セ **3日**：米国連邦捜査局（FBI）はTorネットワークを利用したアンダーグランドサイトであるSilk Roadのテイクダウンを行い、容疑者を逮捕した。
詳細については例えば次のKrebs on Security Blogに詳しい。"Feds Take Down Online Fraud Bazaar 'Silk Road', Arrest Alleged Mastermind"（http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/）。

5 セ **4日**：Adobe社は、システムへの不正侵入が発生し、290万人分のユーザ情報と複数の製品のソースコードが漏えいした疑いがあることを公表した。
詳細については、次のAdobe社の発表などに詳しい。「お客様情報のセキュリティに関する重要なお知らせ」（http://blogs.adobe.com/japan-conversations/セキュリティに関する重要なお知らせ/）。

6 セ **8日**：スロバキアのESET社やルーマニアのBitdefender社、ドイツのAvira社など複数のアンチウイルスベンダのサイトが何者かにドメインハイジャックされる事件が発生した。
詳細については、例えば被害を受けた企業の1つであるAVG社のBlogなどを参照のこと。"Website issue, Tuesday 8 October"（http://blogs.avg.com/news-threats/website-issue-tuesday-8-october/）。

7 他 **8日**：国際的なインターネット関連10団体は、インターネットに関わる新たな課題について会合を行い、これらの課題に対する「今後のインターネット協力体制に関するモンテビデオ声明」を発表した。
一般社団法人日本ネットワークインフォメーションセンター（JPNIC）、「インターネット関連10団体が『今後のインターネット協力体制に関するモンテビデオ声明』を発表」（https://www.nic.ad.jp/ja/topics/2013/20131008-01.html）。
"ICANN Montevideo Statement on the Future of Internet Cooperation"（http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm）。

8 脆 **9日**：Microsoft社は、2013年10月のセキュリティ情報を公開し、MS13-080やMS13-081、MS13-083を含む4件の緊急と4件の重要な更新をリリースした。
「2013年10月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-oct）。

9 脆 **9日**：Adobe Reader及びAcrobatに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-25: Adobe Reader及びAcrobat用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-25.html）。

10 セ **11日**：マレーシアのドメインである.myで、何者かによるドメインハイジャックにより、GoogleのWebサイトが別のWebサイトに誘導される事件が発生した。
この事件の詳細については次のMYNICの発表を参照のこと。"MYNIC Official Announcement"（http://mynic.my/en/news.php?id=162）。

11 セ **12日**：米国のセキュリティベンダであるRapid7社のMetasploit.com、Rapid7.comの2つのサイトが何者かにドメインハ イジャックされる事件が発生した。
詳細については次のKaspersky Lab Threatpostなどを参照のこと。"Phony Order Faxed to Registrar Leads to Metasploit Defacement"（http://threatpost.com/phony-order-faxed-to-registrar-leads-to-metasploit- defacement/102576）。

12 脆 **13日**：D-Link社の複数のルータ製品に特定の文字列をUser-Agentに設定することで、管理画面の認証を回避できることが公表され、修正が行われた。
JVN、「JVNVU#90204379 複数のD-Link製ルータに認証回避の脆弱性」（http://jvn.jp/cert/JVNVU90204379/）。

13 セ **15日**：コスタリカのドメインである.crが何者かによる不正アクセスを受け、GoogleやYahoo!といった複数の著名なサイトがドメインハイジャックされる事件が発生した。

14 脆 **16日**：Oracle社はOracleを含む複数製品について、四半期ごとの定例アップデートを公開し、合計127件の脆弱性を修正した。
なお、今回の定例アップデートからJavaの脆弱性の修正（51件）も含まれるようになっている。"Oracle Critical Patch Update Advisory - October 2013"（http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html）。

15 セ **19日**：カタールの.qaのccTLDレジストリであるdomains.qaが、何者かによる不正アクセスを受け、GoogleやFacebookなど複数の著名なサイトがドメインハイジャックされる事件が発生した。

16 セ **25日**：ルワンダのドメインである.rw が何者かによる不正アクセスを受け、Googleのサイトがドメインハイジャックされる事件が発生した。
詳細については例えば次のUmbrella Security Labs社のBlogなどに詳しい。"THE GOOGLE.RW HIJACK NOBODY ELSE NOTICED"（http://labs.umbrella.com/2013/10/25/google-rw-hijack-nobody-else-noticed/）。

17 セ **25日**：一般家庭からインターネットに接続する際に使用するＩＤやパスワードが盗まれ、サイバー攻撃に悪用される被害が発生してしていることが報道された。原因については、2012年に公表された脆弱性のあるホームルータによるものと考えられ、対象として30万台出荷されていることから広く注意喚起が行われた。
詳細については次のNHK「かぶん」ブログに詳しい。「家庭のネットＩＤなど悪用被害１５０件超」（http://www9.nhk.or.jp/kabun-blog/1000/171059.html）。
また、この脆弱性については7月にTelecom-ISAC Japanからも注意喚起が行われている。「【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策」（https://www.telecom-isac.jp/news/news20120730.html）。

18 他 **31日**：JPCERT/CCは、ユーザの利用環境におけるDNSサーバとブロードバンドルータなどのネットワーク機器が、オープンリゾルバでないかをユーザが確認できるサイトを公開した。
JPCERTコーディネーションセンター、「オープンリゾルバ確認サイト公開のお知らせ」（http://www.jpcert.or.jp/pr/2013/pr130002.html）。

［凡例］ 脆 脆弱性　セ セキュリティ事件　動 動静情報　歴 歴史　他 その他

※日付は日本標準時