11月のインシデント

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

脆 **6日**：Microsoft社は、Microsoft Graphics コンポーネントに脆弱性（CVE-2013-3906）があり、特別に細工されたファイルにより、リモートでコードを実行させられる可能性があるとしてアドバイザリを公開した。この脆弱性については公表時に既に攻撃が確認されていた。
「マイクロソフト セキュリティ アドバイザリ (2896666) Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される」（http://technet.microsoft.com/ja-jp/security/advisory/2896666）。

他 **6日**：Apple社は、初めてとなる2013年1月から6月の期間のTransparency Reportを公開した。
"Report on Government Information Requests"（http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf）。

他 **8日**：IPAは、複合機等のオフィス機器の情報がインターネットから閲覧できる状態になっている問題について、必要がなければネットワークに接続しないことや適切な管理を行うことなどの対策をまとめた注意喚起を公表した。
「プレス発表　複合機等のオフィス機器をインターネットに接続する際の注意点」（http://www.ipa.go.jp/about/press/20131108.html）。

脆 **12日**：ジャストシステム社の一太郎に、細工されたファイルにより任意のコードが実行される可能性のある脆弱性が見つかり、修正された。この脆弱性については、修正が行われる前に攻撃が確認されている。
「[JS13003] 一太郎の脆弱性を悪用した不正なプログラムの実行危険性について」（http://www.justsystems.com/jp/info/js13003.html）。

脆 **13日**：Microsoft社は、アプリケーションの脆弱性を緩和するセキュリティツールであるEnhanced Mitigation Experience Toolkit（EMET）4.1をリリースした。
詳細については次のTechNet Blogsなどを参照のこと。「EMET 4.1を公開 ～ 構成ファイルや管理機能の強化」（http://blogs.technet.com/b/jpsecurity/archive/2013/11/15/3611107.aspx）。

脆 **13日**：Adobe Flash Player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。
「APSB13-26: Adobe Flash Player用のセキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-26.html）。

脆 **13日**：Microsoft社は、2013年11月のセキュリティ情報を公開し、MS13-088とMS13-089及びMS13-090の3件の緊急と5件の重要な更新をリリースした。
「2013年11月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-nov）。

セ **13日**：Anonymousによる日本の政府機関や関連組織への攻撃を予告したOpKillingBayが発表された。

セ **14日**：京都大学、筑波大学、高エネルギー加速器研究機構など複数の研究機関は、それぞれのスーパーコンピュータシステムが外部からの不正アクセスを受けたことを公表した。
詳細については、例えば、次の高エネルギー加速器研究機構（KEK）の発表などを参照のこと。
「KEKコンピューターシステムに対する不正アクセスについて」（http://www.kek.jp/ja/NewsRoom/Release/20131114180000/）。
「KEKコンピューターシステムに対する不正アクセスについて(続報)」（http://www.kek.jp/ja/NewsRoom/Release/20131210170000/）。

セ **18日**：LG社のスマートTV（ネットワーク機能を搭載したテレビ）で、利用者の意図しない利用情報の送信を行っていたことが英国の技術者により公表された。
詳細については次の発見者のBlogなどを参照のこと。DoctorBeet's Blog,"LG Smart TVs logging USB filenames and viewing info to LG servers"（http://doctorbeet.blogspot.ru/2013/11/lg-smart-tvs-logging-usb-filenames-and.html）。

セ **19日**：GitHubでBrute Force攻撃による不正ログイン事件が発生した。
詳細については、次のGitHubのBlogを参照のこと。"Weak passwords brute forced"（https://github.com/blog/1698-weak-passwords-brute-forced）。

脆 **20日**：IPAより、11月6日にMicrosoft社より公表された Microsoft Graphics コンポーネントの脆弱性(CVE-2013-3906) について、国内の組織に対し、当該脆弱性を悪用した「履歴書.zip」などのファイルをメールに添付した攻撃の事例が確認されたとして注意喚起が行われた。
「Microsoft Office等の脆弱性(CVE-2013-3906)を悪用する国内の組織に対する標的型攻撃を確認　～不審メールへの警戒、緊急対策の実施を～」（https://www.ipa.go.jp/security/topics/alert20131120.html）。

他 **23日**：Twitter社は、ユーザ情報の保護の強化を目的として、SSL通信のForward Secrecyに対応したことを公表した。
Twitter, Inc、Engineering Blog、"Forward Secrecy at Twitter"（https://blog.twitter.com/2013/forward-secrecy-at-twitter-0）。

脆 **28日**：Microsoft社は、Windows XP及びWindows Server 2003のカーネルコンポーネントに脆弱性（CVE-2013-5065）があり、リモートでコードを実行させられる可能性があるとしてアドバイザリを公開した。
「マイクロソフト セキュリティ アドバイザリ (2914486) Microsoft Windows カーネルの脆弱性により、特権が昇格される」（http://technet.microsoft.com/ja-jp/security/advisory/2914486）。

他 **29日**：総務省は、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会を開催した。
「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.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