Torの技術

今回は、匿名通信に利用されているTorの仕組みを紹介すると共に、
昨年後半に日本の金融機関の利用者を対象に悪用されたマルウェアZeuSの亜種Citadel及び、
暗号技術を用いたプロトコル・実装に多発している問題について解説します。

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2012年10月から12月までの期間では、依然としてAnonymousのHacktivismによる攻撃が複数発生しており、企業や政府関係機関を狙った標的型攻撃も相次いで発覚しています。また、複数の国別コードトップレベルドメインの関係組織に対する攻撃により、国単位など幅広い範囲でドメインの乗っ取りや改ざんが発生しています。日本国内においては、遠隔操作ウイルスと、それに関連する一連の事件が大きく話題となりました。また、国内政府関係機関におけるマルウェア感染も継続しています。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

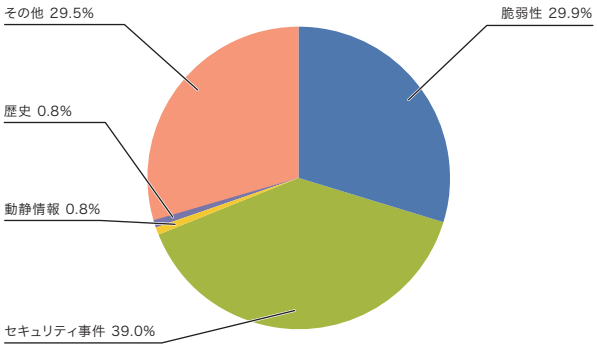


図-1 カテゴリ別比率(2012年10月〜12月)

1.2 インシデントサマリ

ここでは、2012年10月から12月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

■ Anonymousなどの活動

この期間においてもAnonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。主な活動としては、パレスチナのガザ地区へのイスラエル軍による空爆や封鎖への抗議として行われたイスラエル政府関連サイトへの攻撃や、それに対する報復と見られるイスラエルからパレスチナへの攻撃が発生しています(OpIsrael)[*2]。エジプトでは、大統領による大統領令の公布や憲法草案の国民投票を巡る混乱から、デモによる衝突など混乱が続いており、これを支援する目的からエジプトの政府関連サイトに対する攻撃が行われました(OpEgypt)。その他、英国、スウェーデン、ブラジルなどの政府機関などに対しても攻撃が行われていました。また、Anonymousのトレードマークとなっているguy Fawkesにちなんだ英国の記念日のGuy Fawkes Dayにあわせて、11月5日に各地で攻撃が実施されました。

10月には、カナダで発生したSNSによるいじめにより少女が自殺した事件について、加害者とされる男性を特定し公表したり(OpRIP)、12月には、コネチカット州の小学

*1 このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットや利用者の環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェアなどの脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃など、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日などで、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策などの作業を示す。
セキュリティ事件:ワームなどのマルウェアの活性化や、特定サイトへのDDoS攻撃など、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中など、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

*2 例えば、OpIsraelについては、次のHackmageddon.comなどで攻撃の概要がまとめられている。"Timeline of Opisrael"(http://hackmageddon.com/2012/11/25/timeline-of-opisrael/)。

校で発生した銃乱射事件に関連して、被害者の追悼集会や葬儀での活動を予告した過激な主張を行う宗教団体への攻撃を行うなどしています(OpWestBoro)。このようにAnonymousは依然として活発な活動を行っています。

また、Anonymous以外のグループによる事件も複数発生しています。10月には、TeamGhostShellと名乗る何者かにより、日本を含む世界各国の大学のサーバに対し不正アクセスされる事件が発生し、盗まれたアカウント情報などが公開されました。TeamGhostShellは、12月にも世界各国の複数の企業や政府機関などに対して同様に不正アクセスを行い、盗んだアカウント情報など約160万件を公開しています。

なお、欧州各国で激しい反対運動が起きるなどしていたACTA(偽造品の取引の防止に関する協定)について、日本では、2012年9月6日に衆議院本会議で可決していましたが、10月5日に閣議決定を経て受諾書を寄託しました[*3]。ACTAを締結した国は日本が初めてとなります。しかしながら、この期間に目立った攻撃活動などは観測されませんでした。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*4*5*6]、Office[*7*8]、Internet Explorer[*9*10]などで修正が行われました。Adobe社のAdobe Flash Player、Adobe Shockwave Playerなどでも多くの脆弱性が見つかり修正が行われました。Oracle社のJavaでは定例の更新が行われ、多くの脆弱性が修正されています。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleで四半期ごとに行われている更新が提供され、複数の脆弱性が修正されました。また、DNSサーバのBINDでは特定のリソースレコードにより、サーバの異常停止を引き起こすなどの脆弱性が修正されています。

Webアプリケーションフレームワークとして人気の高いRuby on RailsではSQLインジェクション可能な脆弱性が見つかり修正され、その記述言語であるRubyでもハッシュ関数の脆弱性が修正されています。

■ ccTLDへの攻撃

この期間では、ccTLDに対しての攻撃とそれによるドメインハイジャックが複数発生しました。まず、10月にアイルランドのドメインである.ieを管理しているレジストリIEDRが、利用していたCMSの脆弱性から不正アクセスを受け、Google.ieやYahoo.ieなどがドメインハイジャックされる事件が発生しました。11月には、パキスタンのドメインである.pkを管理しているレジストリPKNICのサーバが、脆弱性からSQLインジェクション攻撃による不正侵入を受け、284のドメインについてドメインハイジャックされる事件が発生しています[*11]。その2日後には、ルーマニア(.ro)でも同様の事件が発生したことが報告されています。12月には、セルビアのドメインである.rsでレジストラが攻撃されたことでドメインハイジャックされる事件が発生しました。いずれの事件でも、よく知られたGoogleやYahoo!、Paypalといった世界的な企業のドメインが狙われて、利用者が偽のサイトに誘導されるなどの影響が出ました。

---

*3 外務省、「我が国による「偽造品の取引の防止に関する協定(ACTA)」の締結」(http://www.mofa.go.jp/mofaj/gaiko/ipr/acta_teiketu_1210.html)。

*4 「マイクロソフト セキュリティ情報 MS12-075 - 緊急 Windows カーネルモード ドライバーの脆弱性により、リモートでコードが実行される (2761226)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-075)。

*5 「マイクロソフト セキュリティ情報 MS12-078 - 緊急 Windows カーネルモード ドライバーの脆弱性により、リモートでコードが実行される (2783534)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-078)。

*6 「マイクロソフト セキュリティ情報 MS12-081 - 緊急 Windows のファイル操作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 (2758857)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-081)。

*7 「マイクロソフト セキュリティ情報 MS12-064 - 緊急 Microsoft Word の脆弱性により、リモートでコードが実行される (2742319)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-064)。

*8 「マイクロソフト セキュリティ情報 MS12-079 - 緊急 Microsoft Word の脆弱性により、リモートでコードが実行される (2780642)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-079)。

*9 「マイクロソフト セキュリティ情報 MS12-071 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2761451)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-071)。

*10 「マイクロソフト セキュリティ情報 MS12-077 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2761465)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-077)。

*11 この事件については当初、PKNIC(http://www.pknic.net.pk/)から声明が出ていた。現在は報道などで確認できる。

10月のインシデント

1 他 **1日**：著作権法改正に伴い、違法ダウンロードの刑事罰化に係る規定など一部について施行された。
文化庁、「平成24年通常国会　著作権法改正について」(http://www.bunka.go.jp/chosakuken/24_houkaisei.html)。

2 3 セ **2日**：「TeamGhostShell」により、世界各国の複数の大学のサーバに対し不正アクセスが行われ、盗まれた情報が公開された。この事件では日本でも複数の大学で被害が発生している。
例えば、次の東京大学の発表では複数のWebサーバが不正アクセスを受け、IDやメールアドレスなどの情報が流出したとしている。東京大学、「本学への不正アクセスによる情報流出について」(http://www.u-tokyo.ac.jp/public/public01_241005_02_j.html)。

4 5 6 他 **4日**：ENISAの主催により、約300社が参加する大規模なサイバー攻撃演習「Cyber Europe 2012」が実施された。
ENISA、"Europe joins forces in Cyber Europe 2012"(http://www.enisa.europa.eu/media/press-releases/europe-joins-forces-in-cyber-europe-2012)。

7 セ **7日**：遠隔操作ウイルスなどによりWebサイトへの不正な書き込みが行われた複数の事件について、誤認逮捕が発生していたことが報道により明らかになった。

8 9 脆 **9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。
「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/apsb12-22.html)。

10 11 脆 **9日**：Microsoft社は、バイナリへの署名に使われた一部のデジタル証明書について、適切なタイムスタンプ属性がついていないことにより、セキュリティ更新プログラムなどが正しくインストール及びアンインストールする機能に悪影響を与えるとして該当する更新プログラムの再リリースを行った。
「マイクロソフト セキュリティ アドバイザリ (2749655)署名されたマイクロソフト バイナリに影響を与える互換性の問題」(http://technet.microsoft.com/ja-jp/security/advisory/2749655)。

12 セ **9日**：アイルランドのie.のレジストリであるIEDRが不正アクセスを受け、Google.ieとYahoo.ieが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IEDRの報告に詳しい。"IEDR Security Statement"(https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf)。

13 14 15 脆 **10日**：Microsoft社は、8月に公開した長さ1024ビット未満のRSAキーを使用した証明書の使用を制限するWindows用の更新プログラムについて、自動更新による適用を開始した。
「マイクロソフト セキュリティ アドバイザリ (2661254)証明書の鍵長の最小値に関する更新プログラム」(http://technet.microsoft.com/ja-jp/security/advisory/2661254)。

16 脆 **10日**：Microsoft社は、2012年10月のセキュリティ情報を公開し、MS12-064の1件の緊急と6件の重要な更新をリリースした。
「2012 年 10 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-oct)。

17 脆 **10日**：BIND 9.xに特定のデータにより、外部からサービス停止可能な脆弱性(CVE-2012-5166)が見つかり、修正された。
Internet Systems Consortium、「CVE-2012-5166 [JP]: 特別に細工されたDNSのデータによるnamedのハングアップ」(https://kb.isc.org/article/AA-00808/0)。

18 19 他 **10日**：ASEAN各国との国際的な連携・取組を強化することを目指した「第５回日・ASEAN情報セキュリティ政策会議」が日本で開催された。
内閣官房情報セキュリティセンター、「第５回日・ASEAN情報セキュリティ政策会議の結果」(http://www.nisc.go.jp/press/pdf/5th_aseanj_meeting_result_press.pdf)。

20 21 脆 **11日**：複数ベンダのネットワークカメラのWeb管理画面に、認証回避により遠隔の第三者によって任意の操作を実行される可能性がある脆弱性が発見された。
JVN「JVNVU#265532　複数のネットワークカメラに認証回避の脆弱性」(http://jvn.jp/cert/JVNVU265532/index.html)。

22 23 脆 **17日**：Oracle 社は、Java SE JDK及びJREの四半期ごとの定例アップデートを公開し、任意のコードが実行可能な脆弱性を含む30件の脆弱性を修正した。
"Oracle Java SE Critical Patch Update Advisory - October 2012"(http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html)。

24 25 他 **23日**：無料通話アプリの利用規約と端末へのアクセス許可項目について、第三者に提供できるように読めたり、必要以上の権限を求めるなど不適切な項目が複数見つかり問題となった。

26 脆 **24日**：Adobe Shockwave Playerに、任意のコード実行の可能性を含む複数の脆弱性が発見され、修正された。
「Adobe Shockwave Player用セキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb12-23.html)。

27 28 他 **25日**：Microsoft社より、ユーザインターフェイスやセキュリティ機能の拡充を行った新OS、Windows 8が発売された。

29 他 **27日**：ITシステムの総合運用能力を競うセキュリティイベント、「Hardening One」が開催された。
詳細については、次のWASForumのHardening Projectを参照のこと(http://wasforum.jp/hardening-project/)。

30 31 他 **30日**：マルウェア対策に関する研究成果の発表や、マルウェア対策を行うための人材育成を行うワークショップ、「マルウェア対策研究人材育成ワークショップ 2012(MWS2012)」が開催された。
「マルウェア対策研究人材育成ワークショップ 2012 (MWS2012)」(http://www.iwsec.org/mws/2012/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

ccTLDを管理しているレジストリやレジストラへの攻撃が成功した場合には、多くの人が参照するドメインを含む多数のドメインを一度に乗っ取ることが可能です。更にKaspersky Lab社のブログで報告されている事例[*12]のように、Google Public DNSなど外部の信頼できると考えられるDNSサーバへ問い合わせを行った場合でも偽のIPアドレスが返るため、通常の利用者ではまず気がつかないと考えられます。以上のように、ccTLDを管理する組織を攻撃することで、多くの利用者に、気づくことのできない影響を及ぼすことができることから、同様の攻撃は今後も継続して試みられることが考えられます。

■ スマートフォンのアプリケーションとサービス連携機能

コミュニケーションアプリのSkypeでは、Webサイト上のパスワードリセット機能に脆弱性が見つかり、修正されました[*13]。また、Skypeではインスタントメッセージを利用して拡散するワームの流行も報告されています[*14]。コミュニケーションアプリのLINEでは、Android版アプリケーションの更新に伴い、友だち自動追加の「オフ」が正常に機能せず、電話帳の登録内容から自動的にLINEに友だちが追加されてしまう不具合が発生しました[*15]。Facebookとの連携機能では、Facebookアカウントでの友だち連携機能を利用しても正常に同期されない不具合が発生しました[*16]。

スマートフォンのアプリでは、外部のSNSとの連携により、個々のアプリケーションをより便利に利用できるため、連携は増えてきています。しかし一方で、利用者が意図しない動作や書き込みを行ったり、あるいは端末内の個人情報を収集したりなど、悪用を目的とした連携アプリも確認されています。このような、アプリのサービス連携機能が悪用され、SNSで身に覚えのない投稿をされるなどの被害が発生しているとして、IPAより、その具体例と不要な連携サービスの取り消しなどの対策をまとめた呼びかけが行われました[*17]。

■ 政府機関の取り組み

この期間でも政府機関などへの攻撃がいくつか話題となりました。10月には4月に発生した内閣府を詐称した電子メールが配信される事件が再び発生しました[*18]。また、宇宙航空研究開発機構（JAXA）では、職員の端末がコンピュータウイルスに感染し、ロケット関連の情報が外部に漏えいした可能性があることが発表されました[*19]。同様に職員の利用するパソコンがコンピュータウイルスに感染する事件は日本原子力研究開発機構でも発生しています[*20]。

政府機関の動きとしては、政府機関のセキュリティ対策を推進している情報セキュリティ対策推進会議の第８回会合が開催され、SHA-1及びRSA1024の危殆化に伴って進められている政府機関の暗号アルゴリズムに係る移行指針について、具体的な日程を定義する改定が行われています。また、9月に発生した政府機関に対するサイバー攻撃に関する報告や政府機関における情報セキュリティ対策の取り組み状況についての報告が行われました[*21]。

＊12 詳細については、次のKaspersky Lab社のSECURELIST Blogに詳しい。"Google.ro and other RO domains, victims of a possible DNS hijacking attack"（http://www.securelist.com/en/blog/208194028Google_ro_and_other_RO_domains_victims_of_a_possible_DNS_hijacking_attack）。

＊13 Kaspersky Lab SECURELIST Blog、"New Skype vulnerability allows hijacking of your account"（http://www.securelist.com/en/blog/208193933/New_Skype_vulnerability_allows_hijacking_of_your_account）。

＊14 Trend Micro社、「トレンドマイクロ、ウイルス感染被害マンスリーレポート【2012年10月度】」（http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20121105073724.html）。

＊15 NAVER LINE、「Android版LINE 3.3.0で発生した不具合のお詫びと修正のご報告」（http://lineblog.naver.jp/archives/20587620.html）。

＊16 NAVER LINE、「Android版LINEにおけるFacebook友だち連携機能停止のお知らせ」（http://lineblog.naver.jp/archives/20601519.html）。

＊17 IPA、「2012年10月の呼びかけ『 SNSにおけるサービス連携に注意！ 』～　あなたの名前で勝手に使われてしまいます　～」（http://www.ipa.go.jp/security/txt/2012/10outline.html）。

＊18 内閣府、「内閣府を騙った電子メールについて」（http://www.cao.go.jp/press/20121011notice.html）。

＊19 独立行政法人 宇宙航空研究開発機構（JAXA）、「JAXAにおけるコンピュータウイルス感染の発生及び情報漏洩の可能性について」（http://www.jaxa.jp/press/2012/11/20121130_security_j.html）。

＊20 独立行政法人 日本原子力研究開発機構、「コンピュータウイルス感染による情報漏えいの可能性について」（http://www.jaea.go.jp/02/press2012/p12120501/index.html）。その後、メールアドレスが漏えいした可能性があることが公表された。「コンピュータウイルス感染による個人情報漏えいの可能性について」（http://www.jaea.go.jp/02/press2012/p13011801/index.html）。

＊21 内閣官房情報セキュリティセンター、「情報セキュリティ対策推進会議（ＣＩＳＯ等連絡会議）第８回会合（平成２４年１０月２６日）」（http://www.nisc.go.jp/conference/suishin/index.html#2012_5）。

11月のインシデント

1
- 他 **1日**：2011年7月に批准した、「サイバー犯罪に関する条約」が発効された。
  外務省、「サイバー犯罪に関する条約（略称：サイバー犯罪条約）」（http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html）。

2
- 他 **2日**：総務省より、利用者が安心して無線LANを利用するために最低限取るべき対策を記した「一般利用者が安心して無線LANを利用するために」を公表された。
  「『一般利用者が安心して無線LANを利用するために』の公表」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000029.html）。

3

4
- セ **6日**：インドネシアのISPでハードウェア障害によるBGPの経路異常が発生し、Google社のGoogleAppsなどに影響が生じた。
  詳細については、次のCloudFlare Blogで報告されている。"Why Google Went Offline Today and a Bit about How the Internet Works"（http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about）。

5

6
- セ **6日**：金融機関を装ったフィッシングで、正規サイトにログインした後に、不正な情報入力を促すポップアップメッセージが表示される新たな手口が確認されたとして、金融機関などから注意喚起が行われた。
  例えば、警察庁から次の注意喚起が行われた。「インターネットバンキング利用者等の個人情報を狙った新たな手口の事案に対する対策について」（http://www.npa.go.jp/cyber/warning/h24/121106.pdf）。

7
- 脆 **7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。
  「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/apsb12-24.html）。

8
- 他 **7日**：米国で合衆国大統領選挙が行われた。

9

10
- 脆 **8日**：Adobe Reader X/XIで、サンドボックス保護機能を迂回して任意のコード実行が行われる未修整の脆弱性が公表された。
  詳細については、次のGroup-IBの発表に詳しいが、Adobe社では詳細な情報が提供されておらず、確認が取れないために修正は行えないとしている。"Group-IB US: Zero-day vulnerability found in Adobe X"（http://www.group-ib.com/index.php/7-novosti/672-group-ib-us-zero-day-vulnerability-found-in-adobe-x）。

11

12
- セ **9日**：Twitterで、アカウントが侵害された可能性があるためにパスワードをリセットしたとする電子メールが、多数のTwitterユーザに届く事故があり、利用者の間で混乱が生じた。
  Twitter社、「パスワードリセットのメールについて 」（http://status.twitter.jp/post/35279010388）。

13

14
- 脆 **10日**：ruby 1.9に、ハッシュ飽和攻撃による不正停止が可能な脆弱性（CVE-2012-5371）が見つかり、修正された。
  Rubyコミュニティ「ruby 1.9 におけるハッシュ飽和攻撃による DoS 脆弱性 (CVE-2012-5371)」（http://www.ruby-lang.org/ja/news/2012/11/09/ruby19-hashdos-cve-2012-5371/）。

15

16
- 脆 **14日**：Microsoft社は、2012年11月のセキュリティ情報を公開し、MS12-071・MS12-075を含む4件の緊急と1件の重要及び1件の警告に含まれる更新をリリースした。
  「2012 年 11 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-nov）。

17

18
- 脆 **15日**：複数のAndroid端末で、Linux カーネルの設定が正しくない場合、特定のシステムファイルにアクセスした際に不正なメモリ領域にアクセスすることにより、不正停止する不具合が見つかり修正された。
  JVN、「JVN#74829345 Android OS を搭載した複数の端末におけるサービス運用妨害 (DoS) の脆弱性」（https://jvn.jp/jp/JVN74829345/）。

19

20
- セ **18日**：FreeBSD.orgが9月から不正侵入を受けていたことを公表した。原因は開発者のSSH鍵が流出したことによると推測されている。
  The FreeBSD Project.、"Security Incident on FreeBSD Infrastructure"（http://www.freebsd.org/news/2012-compromise.html）。

21
- 他 **19日**：JNSAより、SNSのセキュリティやプライバシーに関わる問題をまとめた報告書「SNSの安全な歩き方」が公表された。
  「SNSの安全な歩き方～セキュリティとプライバシーの課題と対策～」（http://www.jnsa.org/result/2012/SNS-WG_ver0.7.pdf）。

22

23
- セ **20日**：米国海軍天文台のNTPサーバで障害が発生し、誤った時刻を広報したことによるシステムトラブルが発生した。
  詳細については、例えば次のMicrosoft社のblogなどで確認できる。"Fixing When Your Domain Traveled Back In Time, the Great System Time Rollback to the Year 2000"（http://blogs.technet.com/b/askpfeplat/archive/2012/11/26/fixing-when-your-domain-traveled-back-in-time-the-great-system-time-rollback-to-the-year-2000.aspx）。

24

25
- 他 **20日**：日本データ通信協会から、レンタルサーバ事業者におけるデータ消失事象を受け、「データセンター等事業者のサービス利用に関する留意事項等【注意喚起】」が公表された。
  「データセンター等事業者のサービス利用に関する留意事項等【注意喚起】」（http://www.dekyo.or.jp/pmark/sinsei/data/tyuikanki.pdf）。

26
- セ **26日**：金融機関向けシステムの開発に従事していた業務委託先企業の社員が、キャッシュカードを偽造して現金を引き出したとして逮捕された。

27
- 脆 **27日**：Samsung社の複数のプリンタにSNMPコミュニティ文字列がハードコードされていることにより、管理機能で無効に設定しても、実際には有効なままとなってしまう脆弱性が発見された。
  JVN、「JVNVU#281284 Samsung 製プリンタに SNMP コミュニティ文字列がハードコードされている問題」（http://jvn.jp/cert/JVNVU281284/）。

28

29
- セ **28日**：ルーマニアの.roのレジストリが不正アクセスを受け、GoogleやYahooといった有名なドメインを含む複数のドメインがハイジャックされる事件が発生した。

30

- セ **30日**：宇宙航空研究開発機構（JAXA）は、職員の端末がコンピュータウイルスに感染し、ロケット関連の情報が漏えいした可能性があることを公表した。
  「JAXAにおけるコンピュータウイルス感染の発生及び情報漏洩の可能性について」（http://www.jaxa.jp/press/2012/11/20121130_security_j.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

国際連携の取り組みも継続して行われており、10月には第5回 日・ASEAN情報セキュリティ政策会議が日本で開催され、情報セキュリティ意識啓発に対する取組の推進、情報セキュリティ関連情報共有体制の検討と連絡窓口確認の実施、情報セキュリティにおける一層の連携強化などの取り組みを推進していくことなどが確認されています。

■ 制御システムでの脅威と対策

制御システムは、工場の生産設備などで使われているだけではなく、生活や社会活動の基盤サービスである、水道の供給システム管理や電気やガスなどのエネルギー分野、更には原子力関連設備など高度な管理が要求される設備でも基盤システムとして利用が広がっています。

一方で、情報通信技術を用いた制御システムの利用が進むにつれて、制御システムに関連した機器やソフトウェアの脆弱性が発見され問題となったり、制御システムを狙った攻撃やマルウェア感染によるトラブルも複数確認されています[*22]。

米国の制御システムに特化したCSIRT機関であるICS-CERTが、定期的に発行しているニュースレターを見ても、制御システムに対する脅威は増加していることが確認できます。このような状況から、日本でも制御システムに対するセキュリティマネジメントの必要性が増してきています。これを受け、IPAから「制御システムにおけるセキュリティマネジメントシステムの構築に向けた、制御システムにおけるセキュリティマネジメントに関する要求事項を規定したIEC62443-2-1（CSMS：Cyber Security Management System）の解説書」が公開されました[*23]。

■ 遠隔操作ウイルス

この期間では、遠隔操作ウイルスに関連する一連の事件が話題となりました。2012年6月頃より、メールや掲示板などを利用して殺害予告や爆破予告が行われる事件が多数発生しました。これらの事件では、政府機関や地方自治体のほか、複数の会社やイベント、更には個人も対象として脅迫や予告が行われました。いくつかの事件では、これにより、警備の強化や中止、爆破予告のために飛行機が運航を途中で取りやめるといった対応が行われました。しかし、10月になり、逮捕された容疑者のPCがウイルスに感染していたことから、このPCを踏み台とした第三者の犯行による可能性が明らかとなりました。更に、真犯人と称する人物から、弁護士事務所やラジオ局などの報道機関にメールで犯行声明が届いたことで、複数の威力的な発言や書き込みが、この人物によるものである可能性がでてきました。

今回の事件は大きく2つの特徴が挙げられます。1つは掲示板の書き込みやメールの送信などの通信経路を匿名化し、利用者の特定を困難にするツールであるTorが利用されたと考えられることです。Torについては「1.4.1 Torの概要」も併せてご参照ください。

もう1つは犯行には複数の攻撃手法が利用されました。1つはクロスサイトリクエストフォージェリ（CSRF）で、日本の大規模掲示板に、地方公共団体のホームページの投稿用フォームに犯行予告が書き込まれる罠のURLを書き込み、このリンクをクリックした掲示板利用者が意図せず当該団体に予告を投稿していました。もう1つは自作のウイルスによる遠隔操作で、フリーソフトなどを装って第三者のPCにウイルスをインストールさせ別の掲示板に書かれた指令による遠隔操作で、そのPCから犯行予告を掲示板に書き込んでいました[*24]。

どちらの手法も新しい手法ではなく以前からよく使われている手法です。CSRFについては、例えば2005年にSNSサイトでURLをクリックした利用者の日記が勝手に書き込まれる騒動などが発生しています。遠隔操作を行うウイルスについても、古くは1998年に話題となったBack

＊22 2010年に発見された産業用制御システムを標的としたマルウェアであるStuxnetなどがある。

＊23 ICS-CERT、"ICS-CERT Newsletter the 'ICS-CERT Monthly Monitor,' October-December 2012"（http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf）。IPAから概訳が出ている「ICS-CERT マンスリー・モニター（2012年10月/11月/12月合併号）概要」（http://www.ipa.go.jp/security/controlsystem/pdf/MonthlyReport_201210-12_r3.pdf）。
IPA、「制御システムにおけるセキュリティマネジメントシステムの構築に向けた解説書の公開」（http://www.ipa.go.jp/security/fy24/reports/ics_management/index.html）。

＊24 一連の事件については、2013年2月に容疑者が逮捕されるまでの間、警視庁のホームページやFacebookなどで事件の詳細や情報提供の呼びかけが行われた。

12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
31

他 **3日**：ITU世界国際電気通信会議（WCIT－12）がアラブ首長国連邦のドバイで開催され、国際電気通信規則（ITR：International Telecommunication Regulations）改正に伴い、インターネットの規制強化案を含む複数の改正案が提出され話題となった。
会議ではITRの改正文書が採択されたが、日本は署名を行わなかった。会議についての議論等は次の総務省の取りまとめに詳しい。総務省、「ITU世界国際電気通信会議（WCIT－12）」（http://www.soumu.go.jp/menu_seisaku/ictseisaku/cyberspace_rule/wcit-12.html）。

脆 **5日**：BIND 9.xに特定のデータにより外部からサービス停止可能な脆弱性（CVE-2012-5688）が見つかり、修正された。
Internet Systems Consortium、「CVE-2012-5688 [JP]: DNS64を利用するBIND 9サーバが細工されたクエリによってクラッシュする」（https://kb.isc.org/article/AA-00832）。

セ **5日**：フィッシング対策協議会より、フィッシング詐欺の被害事例などを解説し、その対策を示した「消費者向けフィッシング詐欺対策ガイドライン」が公表された。
フィッシング対策協議会、「消費者向けフィッシング詐欺対策ガイドライン」（http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf）。

セ **5日**：セルビアの.rsのレジストラの1つが不正アクセスを受け、GoogleやYahooといった有名なドメインを含む複数のドメインが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RNIDSの報告に詳しい。"The official statement from NiNet Company given on 05 December"（http://www.rnids.rs/en/what-s-new/%D1%82he-official-statement-from-ninet-company-given-on-05-december/id/4035）。

セ **10日**：「TeamGhostShell」により、世界の複数の航空宇宙関係企業に不正アクセスが行われ、盗まれたアカウント情報など160万件が公開された（#ProjectWhiteFox）。

セ **11日**：ロシアの複数の企業に対して韓国からの標的型攻撃が行われていたことが報告された。
詳細については、次のFireeye社のBlogに詳しい。"To Russia With Targeted Attack"（http://blog.fireeye.com/research/2012/12/to-russia-with-apt.html）。

他 **11日**：内閣官房情報セキュリティセンターの主催で、重要インフラにおける分野横断的演習「CIIREX2012(シーレックス2012)」が実施された。
NISC「重要インフラにおける分野横断的演習の実施概要について　～【CIIREX2012(シーレックス2012)】」（http://www.nisc.go.jp/active/infra/pdf/ciirex2012_2_press.pdf）。

脆 **12日**：Microsoft社は、2012年12月のセキュリティ情報を公開し、MS12-077・MS12-079を含む5件の緊急と2件の重要な更新をリリースした。
「2012 年 12 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-dec）。

脆 **12日**：Microsoft社のInternet Explorer versions 6–10に、任意のWebページ内のJavaScriptによって、マウス・カーソルの画面上の位置が把握できる脆弱性が公表された。
詳細については、発見した英国spider.ioのBlogに詳しい。"Internet Explorer Data Leakage"（http://spider.io/blog/2012/12/internet-explorer-data-leakage/）。

脆 **12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。
「APSB12-27: Adobe Flash Player に関するセキュリティアップデート公開」（http://helpx.adobe.com/jp/flash-player/kb/cq11281733.html）。

動 **12日**：北朝鮮が予告していた人工衛星の打ち上げを行った。

セ **14日**：フリーメールのパスワードを不正に取得し、メールをのぞき見たとして、不正アクセス禁止法違反容疑で中学生が送検された。この事件では、パスワードを忘れた利用者のための機能を悪用しパスワードを取得したとされている。

他 **16日**：第46回衆議院議員総選挙が行われた。

脆 **17日**：韓国Samsungの携帯端末用CPU Exynosを搭載した端末に、root権限を取得される恐れのある脆弱性が報告された。
XDA Developers、"Dangerous Exynos 4 Security Hole Demoed and Plugged by Chainfire"（http://www.xda-developers.com/android/dangerous-exynos-4-security-hole-demoed-and-plugged-by-chainfire/）。

他 **20日**：IPAより、2011年度の情報セキュリティ被害の動向や対策の実施状況をまとめた「2011年度 情報セキュリティ事象被害状況調査」報告書が公開された。内部者の不正行為による被害による影響や、スマートフォンなどでデータを保護するための対策が不十分であるといった指摘がされている。
「『2011年度 情報セキュリティ事象被害状況調査』報告書を公開」（http://www.ipa.go.jp/about/press/20121220.html）。

脆 **21日**：Microsoft社は、12日に公開した不正なWebページの閲覧による任意のコード実行を含むWindowsの複数の脆弱性に関する更新プログラム（MS12-078）に問題があったとして再リリースした。
「マイクロソフト セキュリティ情報 MS12-078 - 緊急 Windows カーネルモード ドライバーの脆弱性により、リモートでコードが実行される (2783534)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-078）。

脆 **22日**：Ruby on Railsのメソッドに、リモートでSQLインジェクション可能な脆弱性（CVE-2012-6496）が見つかり、修正された。本脆弱性は、最初CVE-2012-5664がついていたがCVE-2012-6496、CVE-2012-6497に分割された。
JVN、「JVNDB-2013-001006 Ruby on Rails 用 Authlogic gem における SQL インジェクションの脆弱性」（http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001006.html）。

脆 **31日**：Microsoft社のInternet Explorerに、不正なWebページの閲覧による任意のコード実行が可能な脆弱性が公表された。
「マイクロソフト セキュリティ アドバイザリ（2794220）Internet Explorerの脆弱性により、リモートでコードが実行される」（https://technet.microsoft.com/ja-jp/security/advisory/2794220）。この問題は1月に「マイクロソフト セキュリティ情報 MS13-008 - 緊急 Internet Explorer用のセキュリティ更新プログラム (2799329)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-008）で修正された。

［ 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

Orifice[*25]や、昨年話題となったShady RATと呼ばれる遠隔操作機能を持ったマルウェアによる攻撃事例などが挙げられます[*26]。

今回の事件では、被疑者のうちの数名は掲示板で紹介された無料ソフトウェアを利用しようとしたことで、ウイルスをインストールさせられ、なりすましの被害を受けています。このような被害に遭わないためにも、たとえ便利な機能を謳っていたとしても、出自の分からないファイルを安易にダウンロードしたり、利用したりしないことや、リンクについても不用心にアクセスしないなど注意する必要があります。また、基本的な対策としては、OSやアプリケーション、ウイルス対策ソフトの定義ファイルなど常に最新の状態に保つことなどが必要です。

■ その他

11月には、シリアでインターネットや携帯電話の接続がほぼ全面的に途絶えたことが話題となりました[*27]。原因については当初、テロリストによるケーブル切断と発表されていましたが、2日後に復旧し送電施設に不具合が起きたためとの説明が行われました。シリアでは、6月にもインターネットにつながらなくなる事態が発生しており、政府による情報規制の可能性が指摘されています[*28]。

インターネットに対する規制では、12月にドバイで行われたITU世界国際電気通信会議（WCIT－12）で、24年ぶりに国際電気通信規則（ITR：International Telecommunication Regulations）を改正することが話題となりました。会議の結果、ITRは改定されましたが、採択された改正案及び決議がインターネットのコンテンツ規制や検閲などの規制強化につながりかねないとして、日本や米国、EU諸国といった国を含む55ヵ国では署名を見送っています。

ドイツでは、送電事業者に対するDDoS攻撃が発生したとして話題となりました[*29]。この事件は送電網への攻撃ではなくWebサーバやメールといったインターネット上の通信システムへの攻撃でしたが、スマートメーターやスマートグリッド[*30]の普及が進められており、今後、ネットワークにつながった送電網自身が攻撃される可能性が増えることが指摘されています。

米国では、ハリウッド女優など、セレブのメールアカウントなどを窃取してプライベート情報を流出させたとして、2011年の10月に不正アクセスなど9つの重犯罪容疑で逮捕されていた犯人に対し、懲役10年の判決が言い渡されています[*31]。

メールやSNSを利用したフィッシング事件も継続して発生しています。また、金融機関に関連する事件では、正規サイトにログインした後に、情報の入力を促す不正なポップアップメッセージが表示される新たな手口が確認されています。これらは利用者のPCをマルウェアに感染させ、インターネットバンキングなどの利用時に、合言葉や乱数表などの第二認証の情報を窃取しようと試みるもので、類似の手口による攻撃が複数の金融機関で確認されているとして、注意喚起が行われています。この事件で利用されたとされるマルウェアについてはSpyEyeやZeuSの亜種など複数のマルウェアが使われていたとされています。ZeuSの亜種については「1.4.2 ZeuSの亜種Citadel」も併せてご参照ください。

＊25 Back Orificeはリモート管理用ソフトウェアと言われているが、動作していることが分からないように自身を隠すモードや、利用者に気がつかれずにインストールできる機能などから各社のアンチウイルスソフトではマルウェアに分類されている。
＊26 詳細については、例えばMcAfee社から発表されている、「Operation Shady RATの全貌」（http://www.mcafee.com/japan/security/rp_OperationShadyRAT.asp）などを参照のこと。
＊27 CloudFlare Blog、"How Syria Turned Off the Internet"（http://blog.cloudflare.com/how-syria-turned-off-the-internet）。
＊28 Renesys Blog、"Syrian Internet Shutdown"（http://www.renesys.com/blog/2011/06/syrian-internet-shutdown.shtml）。
＊29 The National Electric Sector Cybersecurity Organization（NESCO）、"News reports of attack on 50Hertz"（http://www.us-nesco.org/tac-diary/news-reports-of-attack-on-50hertz/）。
＊30 通信・制御機能を付加した電力計・スマートメーターなどを活用して停電防止や送電調整などを効率よく行える電力網。
＊31 FBI、"Florida Man Convicted in Wiretapping Scheme Targeting Celebrities Sentenced to 10 Years in Federal Prison for Stealing Personal Data"（http://www.fbi.gov/losangeles/press-releases/2012/florida-man-convicted-in-wiretapping-scheme-targeting-celebrities-sentenced-to-10-years-in-federal-prison-for-stealing-personal-data）。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は、多岐にわたります。しかし、攻撃の多くは、脆弱性の高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2012年10月から12月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、攻撃の実態を正確に把握することが困難なため、この集計からは除外しています。DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*32]、サーバに対する攻撃[*33]、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、901件のDDoS攻撃に対処しました。1日あたりの対処件数は9.79件で、平均発生件数は前回のレポート期間と比べて増加しています。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.3%、サーバに対する攻撃が79.7%、複合攻撃が20.0%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大3万8千ppsのパケットによって212Mbpsの通信量を発生させる攻撃でした。

攻撃の継続時間は、全体の84.5%が攻撃開始から30分未満で終了し、14.5%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃も1.0%ありました。なお、今回最も長く継続した攻撃は、サーバに対する攻撃に分類されるもので、1日と4時間10分(28時間10分)にわたりました。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*34]の利用や、DDoS攻撃を行うための手法としてのボットネット[*35]の利用によるものと考えられます。

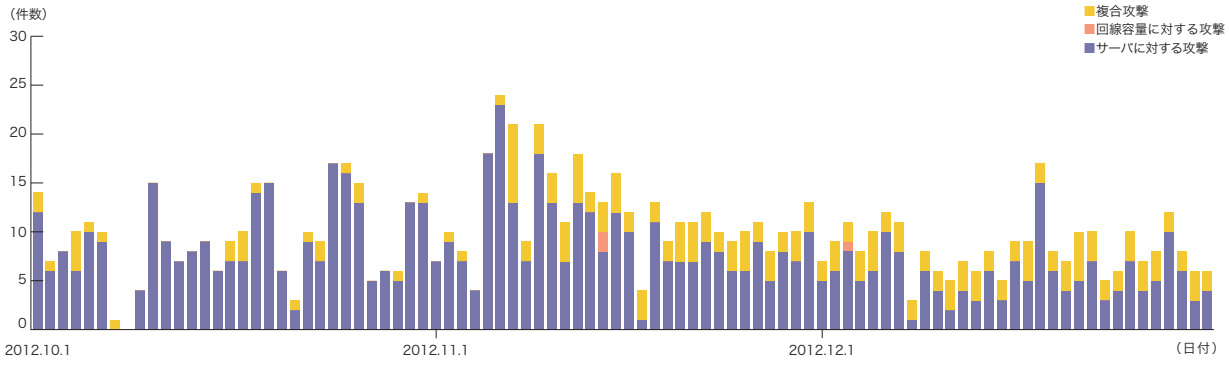


図-2 DDoS攻撃の発生件数

*32 攻撃対象に対し、本来不必要な大きなサイズのIPパケットやその断片を大量に送りつけることで、攻撃対象の接続回線の容量を圧迫する攻撃。UDPパケットを利用した場合にはUDP floodと呼ばれ、ICMPパケットを利用した場合にはICMP floodと呼ばれる。

*33 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃など。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリなどを無駄に利用させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立したのち、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

*34 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、送出すること。

*35 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*36]によるDDoS攻撃のbackscatter観測結果を示します[*37]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2012年10月から12月の期間中に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、対象期間における全パケット数の44.8%を占めています。また、HTTPSで利用されている443/TCPや、ビデオチャットなどで利用されている5100/TCP、SSHで利用されている22/TCPなどへの攻撃も観測されています。図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、米国37.3%、シンガポール19.5%が比較的大きな割合を占めており、以下その他の国々が続いています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、まず、Webサーバ(80/TCP)への攻撃としては、11月23日から11月24日にかけて、米国のドメインレジストラと、米国の検索関連のサービスを提供している事業者のWebサーバへの攻撃が確認されています。11月19日には複数のWebサーバからのbackscatterを観測しており、オランダのWebサーバ、米国のゲーム関連事業者のWebサーバ、米国のサーバ事業者のWebサーバ、トルコのアダルトサイトといったWebサーバへの攻撃を観測しています。12月21日には、レバノンの金融機関や米国の宗教団体のWebサーバへのbackscatterを観測しています。この日はこれ以外にも米国とロシアの複数のホスティング事業者のWebサーバへの攻撃が観測されています。

10月30日から11月8日にかけて、Webサーバ(443/TCP)への攻撃が多く発生していますが、これらの攻撃はシンガポールのホスティング事業者の複数のWebサーバに対する攻撃でした。この攻撃ではサーバによっては1万回以上のbackscatterを観測しており、かなり大規模な攻撃だったことが推測されます。11月12日から11月15日にかけては中国のサーバに対する5100/TCPの攻撃を合計で1万件

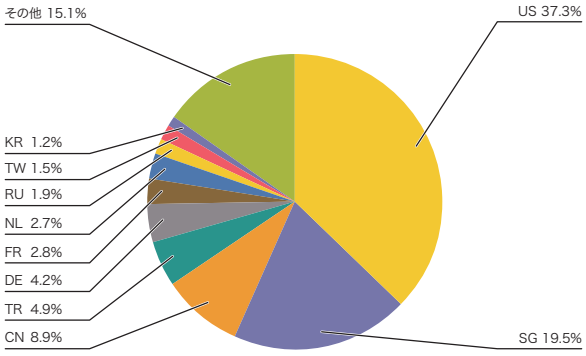


図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

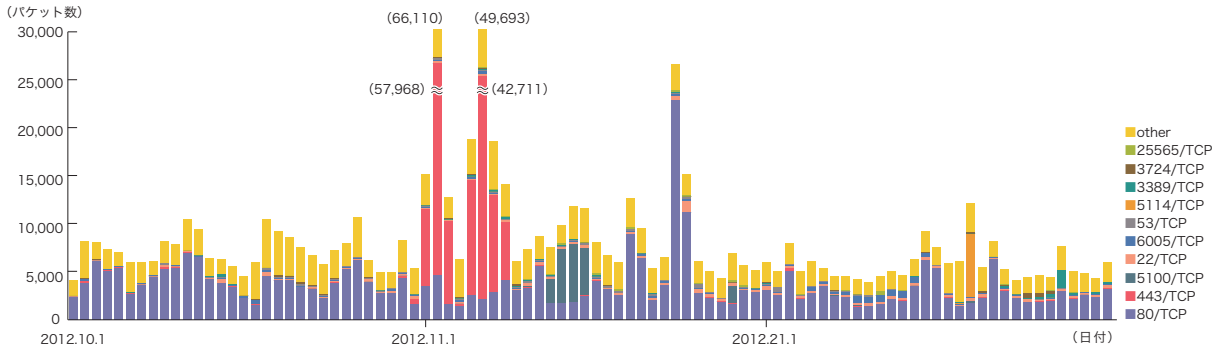


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*36 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。「1.3.2 マルウェアの活動」も参照。

*37 この観測手法については、本レポートのVol.8(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

以上観測しています。12月19日には同じく中国のサーバに対する5114/TCPの攻撃が多く観測されました。これらのポートは通常のアプリケーションで利用するポートではないため、それぞれの攻撃の意図は不明です。

また、今回の対象期間中に話題となったDDoS攻撃のうち、IIJのbackscatter観測で検知した攻撃としては、10月に発生したAnonymousによると考えられる複数のスウェーデン政府機関への攻撃、同じく10月に発生したThe Wiki Boat Brazilによると考えられるブラジルの財務省や連邦警察への攻撃、11月に発生したAnonymousZeikoによると考えられる複数のTorrentサイトへの攻撃、同じく11月に発生したKosovo Hackerによると考えられるインターポールへの攻撃、12月に発生したAnonymousによると考えられる過激な行動を行う宗教団体への攻撃によるbackscatterをそれぞれ検知しています。

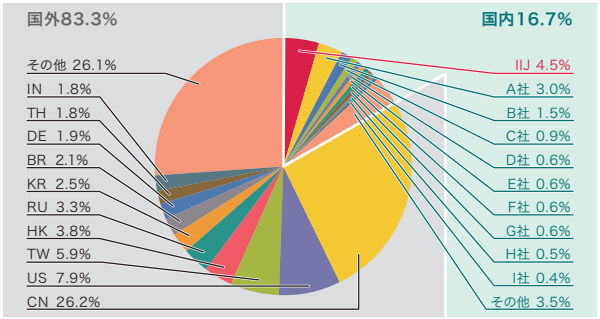


図-5 発信元の分布（国別分類、全期間）

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*38]による観測結果を示します。MITFでは、一般利用者と同様にインターネットに接続したハニーポット[*39]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

■ 無作為通信の状況

2012年10月から12月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量（到着パケット数）の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類（上位10種類）ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPやWindowsのリモートログイン機能である、RDPで利用される3389/TCP、SSHで利用される22/TCP、telnetで利用される23/TCP、ICMP Echo Requestによる探査行為も観測されています。これらに加えて、38327/UDPなど、

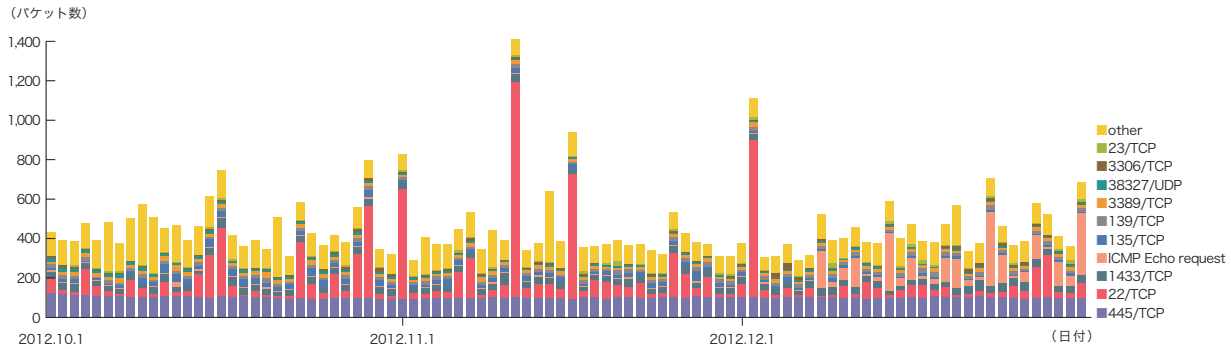


図-6 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊38 Malware Investigation Task Forceの略。MITFは2007年5月から開始した活動で、ハニーポットを用いてネットワーク上でマルウェアの活動の観測を行い、マルウェアの流行状況を把握し、対策のための技術情報を集め、対策につなげる試み。

＊39 脆弱性のエミュレーションなどの手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

一般的なアプリケーションでは利用されない、目的が不明な通信も観測されました。

期間中、SSHの辞書攻撃と思われる通信も発生しており、例えば10月29日はドイツ、11月1日中国、11月11日にタイとトルコ、11月16日に中国、12月2日にシンガポールの各1つのIPアドレスからそれぞれ集中的に通信が発生しています。また、12月8日以降、ICMP Echo Requestが断続的に増加しています。これは、主に2つのIPアドレスから特定のハニーポットに対して通信が行われたものですが実害はないため、静観しています。

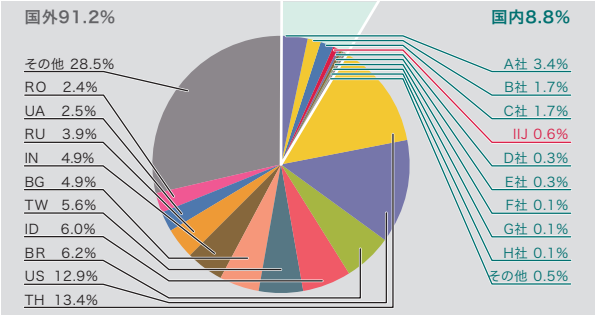


図-7 総取得検体数の分布

■ ネットワーク上でのマルウェアの活動

同じ期間中におけるマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち図-8と図-9では、1日あたりに取得した検体[*40]の総数を総取得検体数、検体の種類をハッシュ値[*41]で分類したものをユニーク検体数としています。

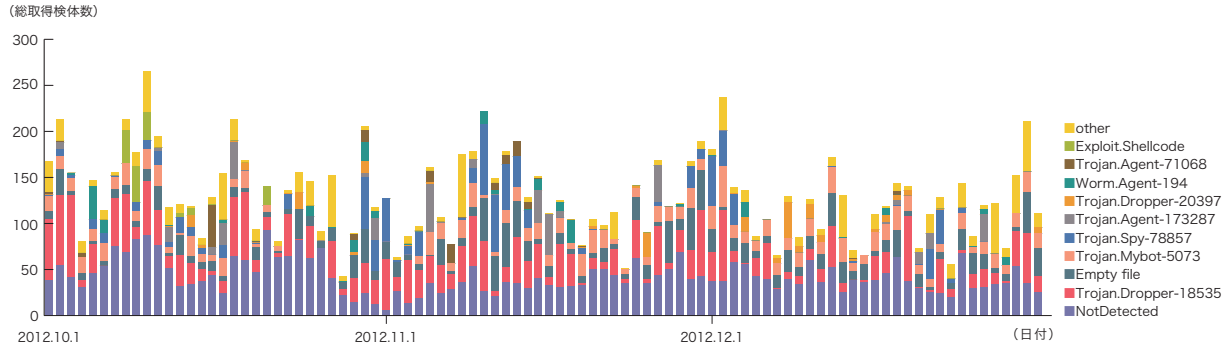


図-8 総取得検体数の推移(Conficker を除く)

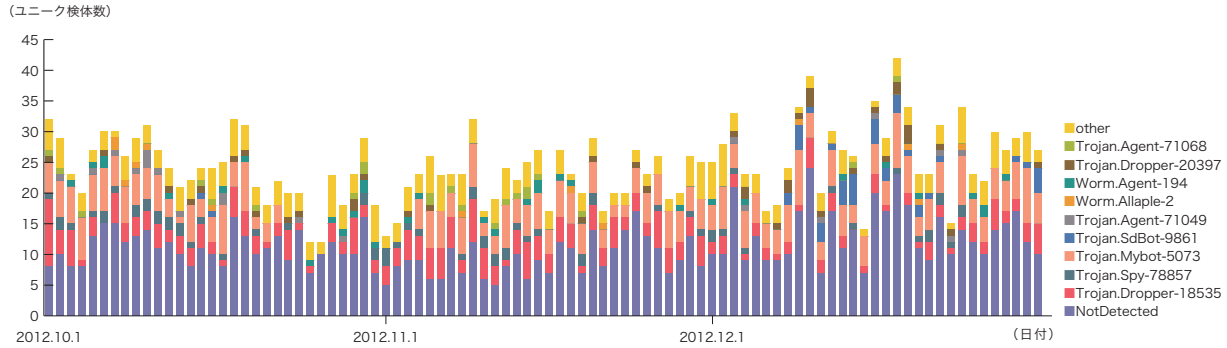


図-9 ユニーク検体数の推移(Conficker を除く)

*40 ここでは、ハニーポットなどで取得したマルウェアを指す。

*41 様々な入力に対して一定長の出力をする一方向性関数(ハッシュ関数)を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディングなどにより、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮した上で指標として採用している。

また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-8と図-9は、前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行い、Confickerと認められたデータを除いて集計しています。

期間中での1日あたりの平均値は、総取得検体数が131、ユニーク検体数が24でした。総取得検体数が前回のレポートと比較して半減しています。これは前回の対象期間中、Trojan-Dropperファミリーの活動が比較的活発だったのに対し、今回の対象期間中も継続して活動しているものの、取得検体数が半減していることが挙げられます。本レポート期間中もタイ及びインドネシアからの未検出の検体が出現しています。この未検出の検体をより詳しく調査した結果、前回までと同様にIRCサーバで制御されるタイプのボット2種類[*42][*43]が活発に活動していたことが分かりました。

MITFの独自の解析では、今回の調査期間中に取得した検体は、ワーム型71.7%、ボット型25.4%、ダウンローダ型2.9%でした。また解析により、15個のボットネットC&Cサーバ[*44]と7個のマルウェア配布サイトの存在を確認しました。

■ Confickerの活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が41,898、ユニーク検体数は899でした。短期間での増減を繰り返しながらも、総取得検体数で99.7%、ユニーク検体数で97.3%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerを含む図は省略しています。総取得検体数は前回の対象期間中と比較し、約10%減少しています。また、ユニーク検体数も前回から約6%減少しました。

Conficker Working Groupの観測記録[*45]によると、2012年12月31日現在で、ユニークIPアドレスの総数は1,787,998とされています。2011年11月の約320万台と比較すると、約47%減少したことになりますが、依然として大規模に感染し続けていることが分かります。

*42 Trojan:Win32/Ircbrute（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute）。
*43 Win32/Hamweq（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq）。
*44 Command & Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。
*45 Conficker Working Groupの観測記録（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking）。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*46]について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2012年10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本33.6%、米国24.6%、ドイツ14.2%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回に比べ、減少しています。米国からの攻撃が2位、ドイツからの攻撃が3位と上昇していますが、これは特定の攻撃先への攻撃が一部の日に発生したことによります。

この期間中、10月10日には米国、ドイツ、オランダのそれぞれの特定の攻撃元から特定の攻撃先に対する攻撃が発生しています。同様の攻撃は10月26日にも発生しており、より大規模な攻撃でした。12月17日には中国の特定の攻撃元から特定の攻撃先への攻撃が発生しています。これらの攻撃はいずれもWebサーバの脆弱性を探る試みであったと考えられます。

ここまでに示したとおり、各種の攻撃はそれぞれ適切に検出され、サービス上の対応が行われています。しかし、攻撃の試みは継続しているため、引き続き注意が必要な状況です。

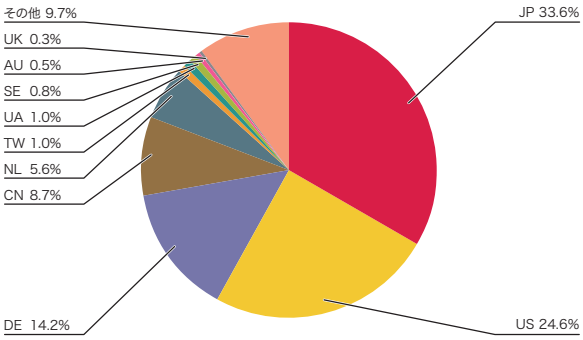


図-10 SQLインジェクション攻撃の発信元の分布

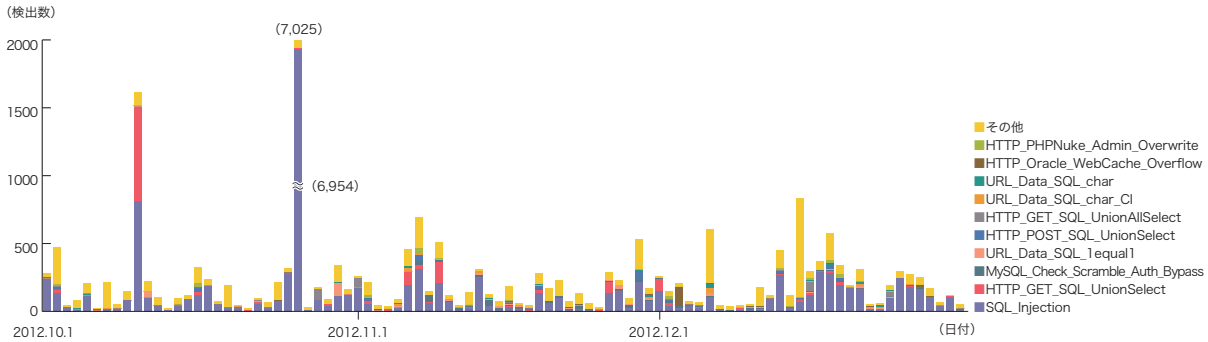


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*46 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、匿名通信を実現するTorの概要、国内金融機関の利用者から暗号表の情報を盗むために悪用されたマルウェアZeuSの亜種Citadelについて、暗号技術を用いたプロトコル・実装に多発している問題の整理と、あるべき姿の3つのテーマについて紹介します。

1.4.1 Torの概要

Torは通信経路を匿名化する目的で構築されたオーバーレイネットワーク[*47]です。1995年頃、通信状況を分析することで誰が誰と通信しているかなどを確認できてしまうことが懸念され、米海軍研究所で匿名接続を実現するための方策が検討されました。ネットワーク上に中継ノードを用意して、これを多段に利用することで送信元の匿名性を確保する方式が考案されました。この方式は、経由するそれぞれの中継ノードで必要最小限の情報が読み取れるように多重に暗号レイヤーでくるまれたパケットが、まるでタマネギのように見えたことにちなんで、オニオンルーティングと名付けられました。その後も研究は継続され、2002年頃に開発されたオニオンルーティングの第3世代[*48]の実装がTorと命名されました。その後、このソースコードはMIT licenseで公開され、引き続き様々な組織からの資金提供を受けながら開発が続けられました。現在では、The Tor Projectが政府組織やNGO、その他様々な団体や個人から資金提供を受けながら開発を継続しています。

Torの匿名接続は、様々な人々に利用されているようです。The Tor Projectによると、ジャーナリストが密告者や反体制者と安全に通信するために利用したり、NGOのスタッフが外国に赴任中に周囲に気づかれずに自組織のWebサイトに接続するのに使っているそうです。また、米国海軍や法執行機関も情報収集や通信に利用しているとのことです。言論の自由のない国では、個人が何らか政府の望まない内容を発言すると命の危険さえあります。実際、通信内容をすべて監視している国もあるそうで、このような国で匿名接続が利用できることは、現地に生きる人にとって、とても重要なことです。例えば、アラブの春と呼ばれる抗議活動が活発になった2011年ぐらいから、急激にTorを利用する利用者が増えています[*49]。これらの政府もTorの存在を知っており、利用を阻止しようと様々なフィルタ技術の導入を試みました。その度にThe Tor Projectではフィルタされにくいように実装を更新し、利用者が匿名接続を利用できる環境を維持しようとしています。

現状では、ボランティアなどにより、世界で3,000程度の中継ノードが運用されています。Torクライアントは、まず内蔵しているディレクトリサービスのリストを元にディレクトリサーバにアクセスして中継ノードのリストを更新します。クライアントはここから3つの中継ノードを選びます。Torネットワークへの入口ノード(Entry)、中間ノード(Middle)、インターネットへの出口ノード(Exit)の3つです。Exitノードのみが少し特殊で、各ノード運用者がどのような通信を許可するか、設定しています。ノード運用者がExitノードとして通信を許可した場合でも、標準設定では下記のようにいくつかのポートを制限しています。

TCP/25(SMTP), TCP/119(NNTP), TCP/135-139(RPC/NetBIOS), TCP/445(Microsoft-DS) TCP/563(NNTPS), TCP/1214(Kazaa), TCP/4661-4666(eDonkey), TCP/6346-6429(Gnutella), TCP/6699 (Napster,WinMX),TCP/6881-6999(BitTorrent)

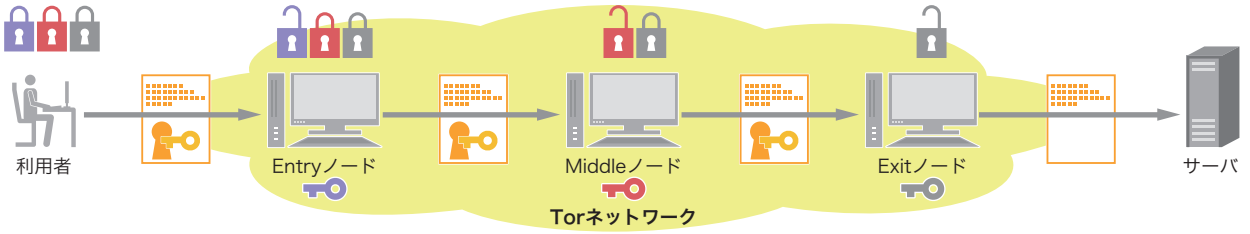
もちろんノード運用者が自身のポリシーでこれら通信を許可することも可能ですが、このフィルタはABUSE行為を防いだり、ファイル共有でネットワークに過剰な負荷がかかるのを防ぐための措置とのことです。また、Exitノードで外部への通信をまったく許可しないことも可能です。クライアントでは、各ノードがExitノードとしてどのような通信を許可しているか分かるようになっており、自身が行いたい通信が許可されているノードをExitノードとして選択します。

*47 あるネットワーク上に論理的に構築されたネットワーク。
*48 当時のプロジェクトでは第2世代と呼ばれていたが、最初のオニオンルーティングの実装を含めると第3世代に当たる。
*49 例えば、エジプトのグラフを確認してみると、2010年から利用者が増えていることが確認できる。また、2011年1月28日にインターネットの通信遮断がされたため、ほぼ0となったがその後復旧していることなどが読み取れる。The Tor Project, Inc., "Directly connecting Tor users"(https://metrics.torproject.org/users.html?graph=direct-users&start=2010-04-01&end=2013-01-31&country=eg&events=off#direct-users)。

クライアントは、自身が選んだ3つのノードのうち、最初の入り口であるEntryノードに暗号化通信を確立します。次に、EntryノードからMiddleノードへ、そしてMiddleノードからExitノードへと順次暗号化通信を確立させます。こうしてEntryノードからExitノードまでの仮想回線を設定した後、Exitノードに通知して最終的な通信先のサーバに接続させれば、クライアントとサーバで通信できる状態になります。このとき、Entryノードはどのクライアントから通信が発生したか知っていますが、それはMiddleノードに中継されるだけで、最終的にどちら宛ての通信か知りません。Middleノードは、EntryノードとExitノードの間で通信が行われているのが分かるだけです。Exitノードは Middle経由でサーバ宛てに通信要求が来たことは分かりますが、それ以上の送信元は分かりません。サーバに至っては、Exitノードから通信要求が来たようにしか見えません(図-12)。オニオンルーティングではこうして匿名接続を実現しています。

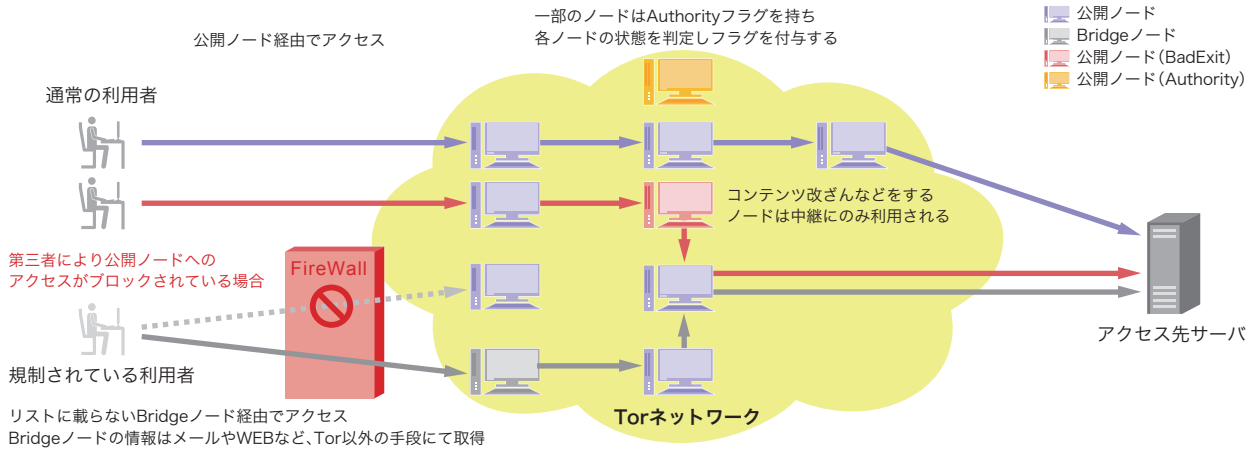
Exitノードからサーバへの通信は平文で行われるため、通信内容の匿名性などを担保したい場合には、別途利用者がSSLなどのエンド - エンドの暗号化プロトコルを利用する必要があります。

Torの利用を阻害しようとした場合、ディレクトリサーバやEntryノードのIPアドレスを調べて、アクセスをブロックすることが考えられます。そして実際にブロックを実施したネットワークがありました。そこで、TorではBridgeノードという仕組みを導入しました。これは非公開の中継ノードで、機能はEntryノードと同じです。違いはブロッキングを避けるために公開リストに載らないことです。少数のBridgeノードを知るための手段がいくつか提供されていますが、Bridgeノードの全リストは参照できないような仕組みで運用されています。利用者は、このBridgeノードを入り口ノード及びディレクトリサーバへの中継として利用することで、ブロックを回避してTorによる匿名接続を利用できるようになります(図-13)。



1. 利用者は各ノードの公開鍵で暗号化してデータを送信する。
2. 各ノードは受け取ったデータを自分の秘密鍵で復号し次のノードに送信する。
3. サーバと通信する Exitノードのみ通信内容が確認可能(他のノードは不可)。

図-12 Torの通信の暗号化



初回時のみAuthorityより各ノードの情報(IPアドレス/公開鍵/BadExitフラグなど)を取得する。
利用者は、得られた情報を元に各ノードの役割(Entry/Middle/Exit)を決定する。
この際に出口として不適切なノード(BadExit)はExitノードの選択から除外される。

図-13 Torの概要

ネットワークから見ると、Torによる通信はクライアントとEntryノード、EntryノードとMiddleノード、MiddleノードとExitノード、Exitノードとサーバで発生しているように見えます。まったく流量のないネットワークならまだしも、現状のインターネットのトラフィック量や中継ノードの分散、Torの利用者数を考えると、すべての通信が観測できたとしても、それぞれがどのように関連しているかを追跡するのは困難でしょう。盗聴用に中継ノードを運用するにしても、通信の利用者を特定するのは困難です。どのノードを利用するかはクライアントによって選択されるので、狙った通信を盗聴するのは、仕組み上不可能です。たまたま運良く利用者によって中継ノードとして選ばれたとしても、Entryノードでは利用者の通信元IPアドレスは分かるものの、どこ宛てに通信しているか分かりません。Middleノードでは意味ある情報はまったく見られませんし、Exitノードであれば通信先や通信内容を見られますが、利用者がどこから通信しているのか分かりません。利用者が暗号化通信を利用していた場合、通信内容も判別不可能でしょう。

Torはこうして匿名接続を利用者に提供しています。もちろん犯罪者がTorを利用することも考えられます。そうした場合、一般のTorを必要とする人と同じように匿名性が確保され、その仕組み上、犯罪者を追跡することは困難です。The Tor Projectではこのような状況に対し「犯罪者は法を犯すことでTorよりも良い匿名性を得られるような状況であり、Torを廃止することで何ら彼らの犯罪行為が抑制されることはないでしょう。Torは一般の人々に防衛手法を提供するのが目的なのです」と記載しています。またTorでは先に述べたように標準でいくつかのフィルタが実装されており、SPAMなどの送信には利用しづらい構成になっています。また、DDoSなどの攻撃の踏み台になる可能性に関しても、中継ノードでは正当なTCP接続のみが中継されるため、Connection FloodやGET Floodに利用される可能性は残るものの、典型的な攻撃手法であるSYN FloodやUDP Floodは実行できない仕組みになっています。Torの匿名接続の機能は、表現の自由を確保したり、プライバシーや人権を守るために開発されました。そしてそれを必要とする人々は世界に大勢いる状況です。IIJではこれら実装や研究の動向を調査しつつ、より良いインターネット社会の実現に向けて努力していきます。

1.4.2 ZeuSの亜種Citadel

Citadelは、有名なBanking TrojanであるZeuS[*50]を基に作られ、2011年末から2012年初頭に出現した比較的新しいマルウェアです。CitadelはSpyEye[*51]と共に、2012年に発生した国内金融機関の金銭窃取事件に使用された可能性があると言われています[*52]。IIJでは、Citadelの検体を独自に入手し、オリジナルのZeuSからどのような変更が行われているのか比較すると共に、Citadelが関連する事件について調査を行いました。

■ Citadelの概要

Citadelの基となったZeuSは、SpyEyeなどと同様にCrimeware Kitの1つで、主に金融機関の認証情報を盗み、最終的に金銭を窃取します。主な機能は、感染端末のブラウザ上のWebコンテンツ改ざん[*53]や、ブラウザ、FTPクライアントなどにあらかじめ保存された、またはそこで入力した認証情報、及びFTPやPOP3などの通信から認証情報を窃取することです。また様々な亜種が存在することも特徴の1つです[*54]。

＊50 ZeuSについては、本レポートのVol.16（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol16.pdf）の「1.4.3 ZeuSとその亜種について」で詳しく解説している。
＊51 SpyEyeについては、本レポートのVol.13（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf）の「1.4.2 SpyEye」で詳しく解説している。
＊52 例えば、Symantec社のブログでは、日本の金融機関を対象としたZeuS亜種が見つかったことを報告している。「日本のオンラインバンキング利用者のみを標的にする Zeus」（http://www.symantec.com/connect/ja/blogs/zeus-now-setting-its-sights-japanese-online-banking-customers）。
＊53 HTTPやHTTPSのWebコンテンツを改ざんし、情報を窃取するための仕組み。例えば、インターネットバンキングなどの認証ページに二要素認証として提供される乱数表に記載された番号をすべて入力させるようなHTMLを挿入することで情報を奪取する。攻撃者は、後日その情報を使って金銭を窃取する。HTTPSによる暗号化通信の場合は、送信データの暗号化の前段階や受信データの復号化の直後にデータの改ざんや窃取を行うことで攻撃を成立させている。
＊54 例えばあるZeuSの亜種は、欧州のインターネットバンキングでよく使用されているmTAN（mobile transaction authentication number）と呼ばれる二要素認証を突破するため、スマートフォン用のマルウェアを用意し、それらと連携する。詳細については次のMcAfee社のBlogなどを参照のこと。"Spitmo vs Zitmo: Banking Trojans Target Android"（http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android）。他にも、ボットとしてDoS攻撃を行うための機能を備える亜種など、多岐に渡る。

CitadelはZeuSを基に作られているため、その基本的な機能はすべて有しています。オリジナルのZeuSと比較して、拡張モジュールの読み込み機能、複数のボットコマンドの新規追加、DNS応答の改ざん機能、Google Chromeなどの比較的新しい環境の情報窃取機能、WebInject用コンフィグの即時更新機能、仮想環境やサンドボックス環境検知による解析妨害機能などが実装されています。また興味深い機能として、ロシア、ウクライナの言語環境下（キーボード設定）では動作しないように設計されていることも挙げられます。Citadelが発見されてから本稿執筆時点で1年程度ですが、開発は活発に行われています。例えば、2012年6月にリリースされたCitadel 1.3.4.5と比較して、その４カ月後に確認された1.3.5.1では新しいボットコマンドがいくつもサポートされ、それ以外にも様々な機能が追加、または強化されています[*55]。図-14に、Citadel 1.3.5.1における、各ボットコマンドに対応して実行される各関数の一覧を示します。Zeus 2.0.8.9以降に追加された関数は赤枠で囲った部分であり、前述の拡張モジュールの読み込みを行う「module_*」、DNS応答の改ざんを行う「dns_filter_*」、WebInject（ブラウザ上のWebコンテンツ改ざん）用コンフィグの即時更新を行う「webinjects_update」などの機能が追加されていることが分かります。

```
commandData     COMMANDDATA <0E3h, offset osShutdown>
                                        ; DATA XREF: executeScript:loc_4
                                        ; executeScript+164↓r
                COMMANDDATA <0E4h, offset osReboot>
                COMMANDDATA <0E5h, offset NEW_url_open>
                COMMANDDATA <0E9h, offset NEW_dns_filter_add>
                COMMANDDATA <0EAh, offset NEW_dns_filter_remove>
                COMMANDDATA <0E6h, offset botUninstall>
                COMMANDDATA <0E7h, offset botUpdate>
                COMMANDDATA <0E8h, offset NEW_bot_transfer>
                COMMANDDATA <0EBh, offset botBcAdd>
                COMMANDDATA <0ECh, offset botBcRemove>
                COMMANDDATA <0EDh, offset botHttpInjectDisable>
                COMMANDDATA <0EEh, offset botHttpInjectEnable>
                COMMANDDATA <0EFh, offset fs_operations>
                COMMANDDATA <0F0h, offset fs_operations>
                COMMANDDATA <0F1h, offset fs_operations>
                COMMANDDATA <0F2h, offset userDestroy>
                COMMANDDATA <0F3h, offset userLogoff>
                COMMANDDATA <0F4h, offset userExecute>
                COMMANDDATA <0F5h, offset userCookiesGet>
                COMMANDDATA <0F6h, offset userCookiesRemove>
                COMMANDDATA <0F7h, offset userCertsGet>
                COMMANDDATA <0F8h, offset userCertsRemove>
                COMMANDDATA <0F9h, offset userUrlBlock>
                COMMANDDATA <0FAh, offset userUrlUnblock>
                COMMANDDATA <0FBh, offset userHomepageSet>
                COMMANDDATA <0FCh, offset userFtpClientsGet>
                COMMANDDATA <0FDh, offset userEmailClientsGet>
                COMMANDDATA <0FEh, offset userFlashPlayerGet>
                COMMANDDATA <0FFh, offset userFlashPlayerRemove>
                COMMANDDATA <100h, offset NEW_module_execute_enable>
                COMMANDDATA <101h, offset NEW_module_execute_disable>
                COMMANDDATA <102h, offset NEW_module_download_enable>
                COMMANDDATA <103h, offset NEW_module_download_disable>
                COMMANDDATA <104h, offset NEW_info_get_software>
                COMMANDDATA <105h, offset NEW_info_get_antivirus>
                COMMANDDATA <106h, offset NEW_info_get_firewall>
                COMMANDDATA <10Ah, offset NEW_ddos_start>
                COMMANDDATA <10Bh, offset NEW_ddos_stop>
                COMMANDDATA <10Ch, offset NEW_webinjects_update>
                COMMANDDATA <10Fh, offset NEW_close_browsers>
```

図-14 Citadelのボットコマンドに対応する関数テーブル

IIJで、オリジナルのZeuS 2.0.8.9と、独自に入手したCitadel 1.3.5.1のコードを比較したところ、関数の約6割がほぼ完全に一致していました。更にコード解析を実施したところ、新規に追加されていた部分は前述のCitadelの特徴に合致し、かつ暗号化のアルゴリズムに若干の違いはあるものの、基本的な機能はほぼZeuSのコードを流用していることが併せて判明しました。このことから、Citadelの作者はZeuSの基本機能を大幅に変更することはせず、主に拡張機能の搭載や認証情報の窃取機能の強化に注力していることが分かります。

■ Citadelを利用した事件

2012年8月にFBIから、Citadelフレームワーク、及びCitadelによって追加インストールされるランサムウェア[*56]に対する注意喚起が発表されています[*57]。このことから、攻撃者は単に金融機関の認証情報を奪取するだけでなく、Citadelで追加実装された拡張モジュールの読み込み機能を使い、さらなる金銭窃取をしようと試みていることが分かります。

またCitadelを使用した攻撃者によって、ある空港の職員用VPNに侵入された事例も存在します[*58]。Crimeware Kitを使用した事件は、認証情報や金銭の窃取が目的であることが一般的です。しかし、この事例に関しては、攻撃者は金銭ではなくインフラを狙っています。このことから、攻撃者の最終的な目的は金銭窃取ではないと考えられ、その点で興味深い事件であるといえます。このようにCitadelは、あくまでツールであり、その攻撃者の目的によって異なる被害を生むものであることが分かります。

＊55　Citadel 1.3.4.5や1.3.5.1の主な機能については、次のBlogなどで詳しく解説されている。"Inside Citadel 1.3.4.5 C&C & Builder - Botnet Control Panel"（http://malware.dontneedcoffee.com/2012/07/inside-citadel-1.3.4.5-cncNbuilder.html）、"Update to Citadel : 1.3.5.1 Rain Edition."（http://malware.dontneedcoffee.com/2012/10/citadelupdate1.3.5.1.html）。

＊56　ランサムウェアとは、ファイルやディスクドライブの一部、またはすべてを暗号化し、利用者にとって重要なデータにアクセスできないようにして、それを人質に金銭を要求するマルウェア。悪質なものはマルウェアを解析しただけでは復号化できない公開鍵暗号方式を使用しているものや、暗号化と称しているがファイルを破壊し、復元できないようにした上で金銭を要求してくるものも存在する。

＊57　FBIは、2012年8月にCitadelおよび追加でインストールされるランサムウェアに関する注意喚起を出している。"Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money"（http://www.fbi.gov/sandiego/press-releases/2012/citadel-malware-continues-to-deliver-reveton-ransomware-in-attempts-to-extort-money）。

＊58　空港のVPNへの侵入事件は次のTrusteer Blogなどで報告されている。"Citadel Trojan Targets Airport Employees with VPN Attack"（http://www.trusteer.com/blog/citadel-trojan-targets-airport-employees-with-vpn-attack）。

国内では、2012年10月から11月に主要銀行を含む複数の金融機関において、Citadelと見られるZeuS亜種やSpyEyeを使用した金銭の窃取事件が報告されています。これは、二要素認証のカードに記載された番号をすべて入力させるポップアップを出すことによって、認証情報を奪取することが特徴です。この手法は、過去にブラジルなどでも確認されており、例えばフィッシングサイトやBancosと呼ばれるマルウェアがこの手法を悪用していたことが確認されています[*59]。国内における金銭の窃取事件は、2011年にSpyEyeによる金銭の窃取事件が発生しており、IPAが注意喚起[*60]を出している点や、少なくとも2005年にはスパイウェア感染による金銭窃取事件[*61]が発生していることから、今回の件に限らず日頃から注意が必要であったと言えます。

■ 感染経路

Citadelの感染経路としては、Blackhole Exploit kit[*62]をはじめとした、Exploit kit[*63]によるドライブバイダウンロード[*64]が多いことが分かっています。これには、Gumblar[*65]などと同様に、正規のWebサイトのコンテンツを改ざんすることによって悪意のあるサイトに誘導する、またはSNSのメッセージやメール本文中のURLをクリックさせるソーシャルエンジニアリングの手口で誘導するなど、様々な手法が使われています。

■ 対策方法

先に示したように、Citadelはその攻撃者の目的によって影響が異なりますが、ここでは、金融機関への悪用への対策を検討します。まず、利用するWebサイトがワンタイムパスワードを提供している場合はそれを利用すべきでしょう[*66]。また、金融機関がログインや取引の実施時にメールで通知するサービスを提供している場合は、これを利用することで被害の早期発見につながります。

二要素認証として金融機関などから提供される乱数表は、利用者ごとに異なる数字が記載されています。この数字のいくつかを取引ごとにランダムに入力させることで、その利用者本人であることを再確認し、パスワードが万が一盗まれてもなりすましによる悪用を軽減する仕組みです。そのため、一度にすべての番号を入力させることは本来ありえません。利用者自身が提供されている機能の意味を考えて使用することで、このような異常に気づくことができるようになります。また、金融機関がこのような機能に関する本来の意味を繰り返し啓発していくことや、脅威に応じた対策強化を継続して行っていくことも重要となります。マルウェア感染による金銭窃取と同様にフィッシングによる被害も継続して確認[*67]されています。これらは従来通り、通信先のWebサイトが正しいものであるか、URLやサーバ証明書(X.509)で確認することが重要です。ただ

---

*59 例えば、次のCAISのページでは、ブラジルの銀行を標的にしたフィッシングサイトにおいて、少なくとも2009年にこの手法を用いて二要素認証の認証情報を奪取する事件が発生しており、その際に使用された画像が確認できる。"Fraudes identificadas e divulgadas pelo CAIS"(http://www.rnp.br/cais/fraudes.php?id=2261&ano=&mes=&pag=52&busca=&tag_extend=&tag=3)(ポルトガル語)。

*60 IPAでは、2011年8月の「コンピュータウイルス・不正アクセスの届出状況[8月分]について」(http://www.ipa.go.jp/security/txt/2011/09outline.html)において、2011年6月から7月にかけてSpyEyeが国内で活動し、金銭が窃取されたことを報告し、注意喚起を行っている。また、IBMのTokyo SOC Reportでも同様にSpyEyeが国内で活発に活動している様子を伝えている。「SpyEyeウイルスの検知件数増加を確認」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110425?lang=ja)、「SpyEyeウイルスの検知件数増加を確認(続報)」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110817?lang=ja_jp)。

*61 例えば、2005年7月には、国内の金融機関が運営するインターネットバンキングの利用者をターゲットとしたスパイウェアが出回ったとして、次の注意喚起がIPAから行われている。「スパイウェアによる被害の防止に向けた注意喚起」(http://www.ipa.go.jp/security/topics/170720_spyware.html)。

*62 CitadelとBlackhole Exploit kitとの関連性は次で述べられている。"Citadel 1.3.5.1 Rain Edition"(http://www.xylibox.com/2012/10/citadel-1351-rain-edition.html)、Context INFORMATION SECURITY、"Malware - Exploit Packs, Zeus and Ransomware"(http://www.contextis.com/research/blog/malware-exploit-packs-zeus-and-ransomware/)。

*63 Exploit kitは2010年のIIJ Technical Weekで解説している。「IIJ Technical WEEK 2010 セキュリティ動向 2010 (1) Web感染型マルウェアの動向」(http://www.iij.ad.jp/company/development/tech/techweek/pdf/techweek_1119_1-3_hiroshi-suzuki.pdf)。

*64 ドライブバイダウンロードとは、Webコンテンツを閲覧した際に脆弱性を悪用され、マルウェアに強制感染すること。閲覧者の使用する端末に脆弱性がある場合は、そのWebコンテンツを閲覧しただけでマルウェア感染してしまう。

*65 Gumblarについては、本レポートのVol.4(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol04.pdf)の「1.4.2 ID・パスワード等を盗むマルウェアGumblar」及びVol.6(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol06.pdf)の「1.4.1 Gumblar の再流行」で詳しく解説をしている。

*66 二要素認証要素を用いたとしても、この種の攻撃を完全に取り除くことは困難である。実際にOperation High Rollerでは、スマートカードリーダーが用いられた環境において、金銭を窃取したことがMcAfee社によって報告されている。「Operation High Roller」(http://www.mcafee.com/japan/security/rp_OperationHighRoller.asp)。ただし、乱数表による二要素認証よりはセキュリティが大きく向上するため、ワンタイムパスワードが金融機関から提供されているのであれば利用した方がよいことに変わりない。

*67 例えばフィッシング対策協議会では、国内金融機関における注意喚起を2012年に複数行っている。「フィッシング対策協議会 ニュース 緊急情報」(http://www.antiphishing.jp/news/alert/)。

し、CitadelやSpyEyeのようなマルウェアに感染した場合、Webブラウザにインジェクションされたマルウェアのコードがその内部でWebコンテンツを改ざんするため、従来のフィッシング対策手法で異常に気づくことは困難です(図-15)。よって、このようなマルウェアに感染することを防ぐことが重要です。

感染を防ぐためには、OSやサードパーティアプリケーションへのパッチ適用(ブラウザプラグインを含む)、不要なアプリケーションやブラウザプラグインの削除、ウイルス対策ソフトウェアの導入と最新版、最新定義ファイルへの更新など、従来の一般的なセキュリティ対策を徹底することが重要です。更に追加対策として、EMET[*68]のような脆弱性緩和ツールの導入や、Windowsの標準機能であるUACやAppLockerまたはソフトウェア制限のポリシーの設定を適切に行うことで、感染のリスクを大幅に軽減することができます。また、ソーシャルエンジニアリングによって騙されて感染することを防ぐためには、リンクや添付ファイルをむやみに開かない、ファイルのダウンロード先が正しいサイトであることを確認する、ダウンロードしたファイルが拡張子偽装されていないことを確認するなども1つの対策になります。

1.4.3 暗号技術を用いたプロトコル・実装に多発している問題の整理とあるべき姿

本節では、暗号技術を用いたプロトコル・実装において近年多発している問題を取り上げます。

2011年から2012年にかけて証明書の不正発行などPKIに対する複数組織への攻撃がなされました。特に2012年5月に存在が明らかになったマルウェアFlameで利用された不正取得証明書の例は、技術面と運用面という複合的な要因で起こる高度な攻撃であったことが分かりました。そのため、水面下では既に多くの攻撃がなされている可能性が指摘されるようになりました。これにより、ベンダーが提供するトラストアンカー(信頼点)とPKIへの信頼失墜だけでなく、安全であると認識されていたアプリケーションやブラウザなどが信用・信頼できない状況に陥りました。

そこで、本節では「安全と思っていたことが実はそうではなかった」事例を整理・分類することで共通点を見出し、今後起こりうる問題に生かすことを考えます。そこには設計者・実装者・運用者、そして利用者という異なるステークホルダーを想定し、それぞれのスタンスで今後予想される攻撃への対策についての指針を導出することを試みます。

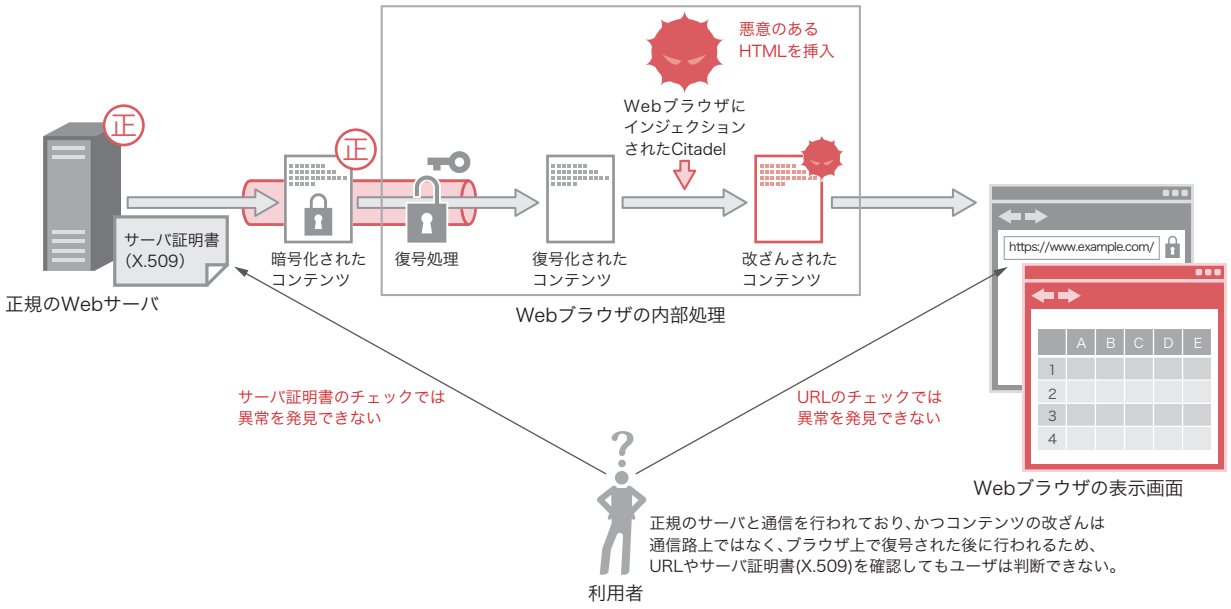


図-15 マルウェアによるブラウザ内部でのコンテンツ改ざん

*68 EMET(Enhanced Mitigation Experience Toolkit)は、Microsoft社が提供する脆弱性の悪用を緩和するためのツール(http://support.microsoft.com/kb/2458544/ja)。

■「安全と思っていたことが実はそうではなかった」事例の整理

表-1はここ数年において暗号技術を用いたプロトコル・実装の脆弱性やそれらに起因する事件・事実を分類したものです。暗号危殆化による問題のほか、設計・実装・運用のそれぞれのフェーズにおける問題として分類しています。このうち、複数の要因によって起きたと見られる問題については、主要因によって分類しました。例えば、Flameマルウエアは MD5アルゴリズムの危殆化という主要因の他に、運用上の問題を要因とする複合的な事例の1つです。

表-1 暗号を用いたプロトコル・実装の脆弱性とそれに起因する事件の分類

問題の種別	年 月	脆弱性・事件 名称	詳 細	脚注番号
暗号危殆化による問題	2007年 3 月	APOPパスワードクラック	MD5コリジョン攻撃を用いてチャレンジを送信し、サーバになりすます攻撃が可能であることが公開された。	∗69、∗70、∗71
	2009年12月	X.509中間CA証明書偽造	MD5ダイジェストを衝突させるように、X.509v3拡張部分のうち、ブラウザが無視するエリアを調整してX.509中間CA証明書の偽造を行った。このとき、証明書のシリアル番号がインクリメントして発行されていて被署名データが推測可能であったという運用面の問題も指摘されている。	∗72
	2010年 1 月	768ビットRSA公開鍵の素因数分解	663ビットという当時の記録を更新し、80台のマシンを利用して約半年で768ビットRSA公開鍵の素因数分解に成功したとの報告があった。1024ビットRSAはまだまだ現実的な攻撃対象ではないが、2048ビットRSAへの移行を促進するきっかけの1つとなった。	∗73
	2012年 5 月	Flameマルウェア	マルウェアを悪用したコード署名機能への攻撃によるWindows Updateへの中間者攻撃が発覚した。MD5コリジョン攻撃を用いて、あたかもMicrosoft から発行されたように見える不正な証明書が発行された。	∗74
	2012年 8 月	PKCS#1v1.5暗号に対するパディングオラクル攻撃	PKCS#1v1.5暗号に対する既存のPadding oracle attackを改良する攻撃手法が公開された。PKCS#11の暗号鍵インポート関数が実装されたハードウェアから暗号鍵を搾取する現実的な攻撃である。	∗75、∗76
	2012年 8 月	鍵長1024ビット未満のRSA 鍵の利用制限	Microsoftの製品群において、1024ビット未満のRSA鍵を使用した証明書の使用を制限する更新プログラムがリリースされた。	∗77
設計の問題	2008年11月	WPAに対する鍵回復攻撃	WPA(Wi-Fi Protected Access)における鍵更新アルゴリズムTKIP(Temporal Key Integrity Protocol)の問題により、MIC鍵の漏えいと虫ざんパケットの生成が可能となる攻撃が公開された。	∗78
	2008年11月	SSHv2通信傍受による暗号文の一部漏えい	CBCモード利用時のSSHv2において、パケット先頭4バイトが漏えいする攻撃が公開された。パケット長チェックの仕組みを利用してトライ&エラーを行い、確率 2^{-14}で成功する。	∗79
	2009年11月	SSL/TLS Renegotiation 脆弱性	鍵情報やアルゴリズムの合意をリフレッシュするrenegotiation機構において、HTTPSフラグメントにおけるインジェクションを可能にする中間者攻撃が公開された。	∗80、∗81
	2010年10月	IPsecにおけるCBC利用時の問題	ESP trailerと呼ばれる平文データに対してブロックサイズ長になるようにパディングされたデータ構造の特徴に着目した攻撃が公開された。	∗82
	2011年 9 月	BEAST攻撃	SSL 3.0/TLS 1.0を使用しているブラウザのCBCモードに対して選択平文攻撃を行うことでブラウザ内のCookieを入手するツールが公開された。	∗83、∗84、∗85
	2011年10月	XML Encryption(CBCモード利用時)脆弱性	XML構文チェックエラーに応じて異なるエラーコードを返却するWebサービスをplaintext validity oracleとして利用した攻撃が公開された。	∗86
	2011年12月	TLS1.2におけるTruncated HMAC利用時の問題	メッセージ認証子として通常のHMACではなく、80ビットに切り詰めたデータをMACとして利用する拡張方式において、暗号化対象のアプリケーションデータが短く、暗号化データがブロックサイズを超えないケースにおいて平文の情報が漏えいする可能性が指摘された。	∗87
	2012年 7 月	MS-CHAPv2解読ツール公開	Bruce Schneierが1999年に公開したMS-CHAPv2に対する攻撃手法をクラウドから利用できるツールが公開された。	∗88
	2012年 9 月	CRIME攻撃	SSL/TLSでCompression(圧縮)機能を有効にしているケースで、Cookieを搾取するデモが公開された。たとえ同じ長さのデータを圧縮したとしても、圧縮前データに同じ文字を含むかどうかで辞書の長さが変わるという事実を用いてトライ&エラーで暗号化データを復元する手法である。	∗89、∗90
	2012年 9 月	Oracle DBにおけるパスワード搾取攻撃	Oracleデータベースのパスワードを搾取可能な攻撃が公開された。認証プロトコルの設計の問題として認識されている。	∗91
実装の問題	2008年 5 月	DebianのOpenSSLに予測可能な乱数生成の問題	Debianの特定バージョンにおけるOpenSSLを使って鍵生成を行った場合、極端に少ない鍵空間からしか秘密鍵を導出していないという問題が公開された。	∗92
	2012年 2 月	公開鍵使いまわし問題	インターネット上のIPv4アドレスを広範囲にスキャンして、SSL/TLSやSSHで利用されている公開鍵証明書、DSA署名及びPGP鍵を収集したところ、意図せず他のサイトと秘密鍵を共有していることが、独立した2グループから報告された。	∗93、∗94
	2012年10月	アンドロイド向けアプリのSSL実装の問題	SSL実装の不備により、中間者攻撃が可能なアンドロイド向けアプリの存在が指摘された。	∗95
	2012年11月	Huawei製Wifiプロダクトにおける実装の問題	通信中に用いられる共通鍵暗号DESにおいて、本来ランダムに選択されるはずのセッション鍵がハードコーディングされていたことが公開された。	∗96
運用の問題	2011年 3 月 ～ 11月	複数の認証機関への侵入事件と不正証明書発行事件	3月に起きたComodo事件では9件の証明書が、また8月末にはDigiNotarから500以上もの証明書が不正に発行されていることが発覚した。更に11月にはKPN社が運営するオランダの認証機関サービスにおいて、証明書発行システムへの侵入の痕跡が見つかったため証明書発行業務を停止している。	∗97
	2011年 9 月	RSA512ビット証明書発行CAの証明書失効	DigiCert Sdn. Bhd.社の発行ポリシーの問題により、中間CA証明書を無効にする方針がとられた。	∗98
	2012年 8 月	Adobeの証明書失効	Adobeで用いられていたコード署名用証明書の不正利用が発覚したため、証明書を失効処理している(事件の経緯について続報がないため現時点では運用の問題に分類している)。	∗99
	2012年10月	DKIMで利用される公開鍵にRSA512ビット鍵を利用	電子メールの送信元を認証する仕組みの1つであるDKIMにおいて、仕様上、本来1024ビット以上の鍵長を利用する必要があるが、512 ビット鍵を利用していた事例が報告された。	∗100
	2012年10月	署名されたマイクロソフトバイナリに影響を与える互換性の問題	2012年7月12日から8月14日の期間にコード署名されたバイナリのいくつかに間違った手順に基づいて署名されていたことが発覚した。CodeSign証明書にタイムスタンプに関するExtended Key Usageが含まれていなかったことが原因である。	∗101
	2012年12月	TURKTRUST認証局からの証明書不正発行	TURKTRUST認証局により、*.google.comなどに対して複数の証明書が不正発行されたことが発覚した。	∗102、∗103

暗号アルゴリズムの危殆化*104は設計当初想定したよりも低いコストでセキュリティ上の性質が危うくなる状況を指し、CPU処理能力の増大やクラウド利用による攻撃コストの低下のほか、暗号解読研究の進展が要因となっています。そのため、アルゴリズムの経年劣化は避けられないものであり、現在利用されているアルゴリズムもいずれはどこかのタイミングで別の新しいアルゴリズムに移行することが必要です。表-1にリストされている脆弱性には、ハッシュ関数MD5や比較的短い鍵長でRSAアルゴリズムを利用することが原因になっているということを読み取ることができます。根本的な対策としては、MD5からSHA-2ファミリー*105への移行、2048ビット以上のRSA公開鍵利用へシフトすることでこれらの脆弱性への対策を行うことができます。

次に、設計・実装フェーズの対策の指針について考えてみましょう。表-1において設計の問題に分類されている脆弱性

*69 Gaetan Leurent、"Message Freedom in MD4 and MD5 Collisions Application to APOP"、FSE2007（http://fse2007.uni.lu/slides/APOP.pdf）。
*70 Yu Sasaki、Go Yamamoto、Kazumaro Aoki、"Practical Password Recovery on an MD5 Challenge-Response such as APOP"、FSE2007 Rump session（http://www.iacr.org/workshops/fse2007/slides/rump/apop.pdf）。
*71 Yu Sasaki、Lei Wang、Kazuo Ohta、Noboru Kunihiro、"Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication"、IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences、Vol.E92-A No.1、pp.96-104。
*72 Alexander Sotirov、Marc Stevens、Jacob Appelbaum、Arjen Lenstra、David Molnar、Dag Arne Osvik、Benne de Weger、"MD5 considered harmful today"（http://www.win.tue.nl/hashclash/rogue-ca/）。
*73 Thorsten Kleinjung et.al、"Factorization of a 768-bit RSA modulus"（http://eprint.iacr.org/2010/006）。
*74 本レポートのVol.16（http://www.iij.ad.jp/development/iir/pdf/iir_vol16.pdf）の「1.4.2 Windows Updateへの中間者攻撃を行うマルウェアFlame」を参照。
*75 Romain Bardou、Riccardo Focardi、Yusuke Kawamoto、Lorenzo Simionato、Graham Steel、Joe-Kai Tsay、"Efficient Padding Oracle Attacks on Cryptographic Hardware"、CRYPTO2012（http://www.lsv.ens-cachan.fr/~steel/slides/CRYPTO12.pdf）。
*76 Efficient Padding Oracle Attacks on Cryptographic Hardware FAQ（http://www.lsv.ens-cachan.fr/~steel/efficient-padding-oracle-attacks/faq.html）。
*77 Microsoft社、TechNet Blogs「1024 ビット未満の暗号キーをブロックする更新プログラム（KB2661254）を8月14日に公開」（http://blogs.technet.com/b/jpsecurity/archive/2012/07/30/3511493.aspx）。
*78 Erik Tews、"Gone in 900 Seconds, Some Crypto Issues with WPA"、PacSec2008。
*79 CERT/CC、"Vulnerability Note VU#958563 SSH CBC vulnerability"（http://www.kb.cert.org/vuls/id/958563）。
*80 MITRE、CVE-2009-3555（http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555）。
*81 E. Rescorla、M. Ray、S. Dispensa、N. Oskov、"Transport Layer Security (TLS) Renegotiation Indication Extension"（http://www.ietf.org/rfc/rfc5746.txt）。
*82 Jean Paul Degabriele、Kenneth G. Paterson、"On the (In)Security of IPsec in MAC-then-Encrypt Configurations"、the 17th ACM conference on Computer and communications security（ACM CCS2010）（http://www.isg.rhul.ac.uk/~psai074/slides/CCS-2010.pdf）。
*83 Qualys Security Labs、"Mitigating the BEAST attack on TLS"（https://community.qualys.com/blogs/securitylabs/2011/10/17/mitigating-the-beast-attack-on-tls）。
*84 Microsoft社、MSDN Blogs、"Fixing the BEAST"（http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx）。
*85 CRIME vs startups（http://www.youtube.com/watch?v=gGPhHYyg9r4）。
*86 Tibor Jager、Juraj Somorovsky、"How to Break XML Encryption"、the 18th ACM Conference on Computer and Communications Security（ACM CCS2011）（http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/HowToBreakXMLenc.pdf）。
*87 IIJ-SECT Security Diary、「TLS1.2におけるTruncated HMAC利用時の脆弱性について」（https://sect.iij.ad.jp/d/2011/12/079269.html）。
*88 CloudCracker::Blog、"Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate"（https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/）。
*89 Juliano Rizzo、Thai Duong、"The CRIME attack"、ekoparty Security Conference 2012（http://www.ekoparty.org/eng/2012/thai-duong.php）。
*90 CRIME: Information Leakage Attack against SSL/TLS（https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls）。
*91 Esteban Fayo、"Cryptographic flaws in Oracle Database authentication protocol"、ekoparty Security Conference 2012（http://www.ekoparty.org/eng/2012/esteban-fayo.php）。
*92 Debian Security Advisory、"DSA-1571-1 openssl -- predictable random number generator"（http://www.debian.org/security/2008/dsa-1571）。
*93 本レポートのVol.17（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol17.pdf）の「1.4.1 SSL/TLS,SSHで利用されている公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題」を参照。
*94 須賀、公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題、JNSA PKI Day 2012（http://www.jnsa.org/seminar/pki-day/2012/data/PM02_suga.pdf）。
*95 Martin Georgiev、Subodh Iyengar、Suman Jana、Rishita Anubhai、Dan Boneh、Vitaly Shmatikov、"The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software"、the 19th ACM Conference on Computer and Communications Security（ACM CCS2012）（http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf）。
*96 Roberto Paleari、Ivan Speziale、"Weak password encryption on Huawei products"（http://blog.emaze.net/2012/11/weak-password-encryption-on-huawei.html）。
*97 本レポートのVol.13（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf）の「1.4.3 公開鍵証明書の不正発行事件」を参照。
*98 本レポートのVol.14（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol14.pdf）の「1.4.1 公開鍵証明書発行に関するいくつかの問題」を参照。
*99 Adobe Secure Software Engineering Team（ASSET）Blog、"Inappropriate Use of Adobe Code Signing Certificate"（https://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html）。
*100 US-CERT、"Vulnerability Note VU#268267、DomainKeys Identified Mail（DKIM）Verifiers may inappropriately convey message trust"（http://www.kb.cert.org/vuls/id/268267）。
*101 Microsoft社、「マイクロソフト セキュリティ アドバイザリ（2749655）、署名されたマイクロソフト バイナリに影響を与える互換性の問題」（http://technet.microsoft.com/ja-jp/security/advisory/2749655）。
*102 Microsoft社、「マイクロソフト セキュリティ アドバイザリ (2798897) 不正なデジタル証明書により、なりすましが行われる」（http://technet.microsoft.com/ja-jp/security/advisory/2798897）。
*103 TÜRKTRUST、"Kamuoyu Açıklaması"（http://www.turktrust.com.tr/kamuoyu-aciklamasi.html）（トルコ語）。
*104 本レポートのVol.8（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol08.pdf）の「1.4.1 暗号アルゴリズムの2010年問題の動向」を参照。
*105 2013年1月までパブリックコメントが行われていた「『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』（案）に係る意見募集について」（http://cryptrec.go.jp/topics/cryptrec_201212_listpc.html）ではSHA-1は互換性維持のために継続利用を容認する状態にあり、代わりにSHA-256/384/512が推奨されている。

の多くは、トライ＆エラーを繰り返す際のレスポンス（外部情報）を観測することで内部情報の一部を少しずつ漏えいさせる手法に該当しています。特にCBCモードに対するパディングオラクル攻撃[*106]は、Serge Vaudenayによって2002年に指摘された問題であり、ここ数年に改良や拡張が行われたことで、現実的な脅威が発生しうる問題に転じていることが分かります。

実際に存在する攻撃対象のサーバの応答を観測し、複数のトライ＆エラーを行うことで確率的に平文を復元する手法がSSL/TLS[*83][*87]、IPsec[*79]、SSH[*82]やXML暗号化仕様[*86]に適用されています。これらの手法の基本的アイデアはVaudenayによるもので、攻撃対象となるノードのレンポンスから「パディングが不正であるかどうか」を見て少しずつ情報を搾取していきます。更にこのトライ＆エラーの考え方は、WPAへの鍵回復攻撃[*78]やCRIME攻撃[*89]でも用いられています。正常系ではなく異常系の処理のまずさがこれらの問題を引き起こしていることを鑑みて、プロトコルの設計を行う必要があることが分かります。また実装時においても配慮すべき問題であることは自明です。

■ 新しい産学連携の形成へ

暗号解読手法の1つにサイドチャネル攻撃があります。暗号チップのレベルで電力や電磁波や処理速度の偏りなどの副次的な情報を収集し、暗号処理に用いられている鍵などの情報を取得する方法です。先に説明したトライ＆エラーによる解析手法も収集するデータの範囲が異なるだけであり、基本的には同じ考え方によるものです。サイドチャネル攻撃の進展は、暗号アルゴリズムの設計や安全な実装方法の確立に大きな影響を及ぼしました。今後、これらの知見をプロトコルやフォーマットの設計に転用できる可能性があると考えられます。そのためには、暗号アルゴリズム設計とプロトコル設計を完全に切り離すのではなく、暗号利用時の注意点や問題点などをうまくプロトコル設計者や実装者に伝えるスキームが必要となります。暗号アルゴリズムとしては、高速処理可能かつ証明可能安全性を有するなどの安全性を持つバランスの取れた優秀なアルゴリズムが多く提案されています。しかし、それを利用する際の設計ミスや実装上の問題で、プロトコルやシステムがトータルとしては安全性を保持しないというケースも見受けられます。十分なエントロピーから乱数生成を行わないために、アルゴリズム設計時とは大きくかけ離れた安全性しか保持できない事例も多く見受けられました。DebianのOpenSSLにおける脆弱性[*92]、公開鍵使いまわし問題[*93]、MS-CHAPv2攻撃ツール公開[*88]などがそれにあたります。

このような状況を鑑み、学術界からも問題視する声からワークショップ[*107][*108]が開催されるなど、暗号技術が直面している現実的な課題を学術界と産業界の両方で共有する動きが見られるようになりました。日本でも先に取り上げたCBCモードに関連する脆弱性を正しく理解するワークショップが2013年3月に開催予定です。このようなアクティビティにより、問題の共有と理解が進み、根本的な解決に結びつくことが望まれます。

この新しい産学連携においては、特に脆弱性の影響の見える化を進めるべきだと考えます。現在、脆弱性の影響を数値化する試みとしては共通脆弱性評価システムCVSS[*109]などが知られています。しかし、実際の影響は攻撃の前提条件や利用環境に応じて大きく左右されるため、1つの参考指標として利用されているという現状があります。例えばBEAST攻撃[*83]においては、CVSS Base Scoreが4.3[*110]と中程度の脆弱性と評価されていましたが、対策を行ったサーバに接続できない状況が発生するなど、大きな混乱が起こりました。これは脆弱性そのものに対する評価のみではなく、移行そのものに関わる影響度を算出していないことに起因する

＊106 Serge Vaudenay、"Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS..."、EUROCRYPT2002（http://www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf）。

＊107 Workshop on Real-World Cryptography（https://crypto.stanford.edu/RealWorldCrypto/index.php）が2013年1月に開催されている。その前身となったワークショップIs Cryptographic Theory Practically Relevant?（http://www.newton.ac.uk/programmes/SAS/sasw07.html）は2012年1月に開催された。

＊108 The 1st Workshop on Real-Life Cryptographic Protocols and Standardization（http://www.nec.com/en/global/rd/event/RLCPS10.html）は2010年1月に、The 2nd Workshop on Real-Life Cryptographic Protocols and Standardization（http://www.nec.com/en/global/rd/event/RLCPS11.html）は2011年3月に開催されている。

＊109 P.Mell、K.Scarfone、S.Romanosky、"A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0"（http://www.first.org/cvss/cvss-guide.pdf）。独立行政法人情報処理推進機構セキュリティセンターによる解説にも詳しい（http://www.ipa.go.jp/security/vuln/CVSS.html）。

＊110 NIST、"CVSS Version 2 Scoring Page（CVE-2011-3389）"（http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2011-3389&vector=(AV%3AN/AC%3AM/Au%3AN/C%3AP/I%3AN/A%3AN)）。

と考えられます。そこで、OSやプラットフォームに依存せず一元的に扱うため、異なる種類の暗号技術に対する同一の評価尺度を表す等価安全性[*104]と同様の概念をプロトコル／フォーマット仕様脆弱性にも用いると共に、暗号危殆化と共通に扱うことのできる移行コストに関する評価基準が必要であると考えています。移行にまつわる共通的な課題・方法論の共有と成功・失敗事例の収集などから移行工学の創出という新しい考え方の源流になることが期待されます。

■ 利用者の意識の高まり

次に、運用者や利用者における対策の指針を取り上げます。表-1において運用の問題にリストアップされている事件はすべてPKIに関連するものです。これらの問題の原因は、運用にかかわる側において、証明書発行システムの脆弱性、証明書属性のミスユース、間違って鍵長の短い暗号アルゴリズムを使ってしまったことなど、多岐にわたります。立て続けに起こった問題に対し、ベースライン要件書[*111]が2012年7月から施行することにより、各認証機関における発行要件のばらつきを均等化し、業界全体の底上げとPKIの信頼回復が期待されています。

しかし2012年12月にはTURKTRUST認証局からの証明書不正発行事件が発覚し、PKIの信頼崩壊に拍車がかかる残念な事例も見受けられました。PKIは利用者にとっては信頼点であり、不正な証明書が発行されるなどPKIが信頼できなくなると正規のサイトと不正なサイトをブラウザなどで区別することができなくなるという大きな問題が発生してしまいます。この課題に対しDANE[*112]やConvergence[*113]など既存のPKIの仕組みだけでなく他の信頼点を確保するという対策が提案されています。これらを利用することで「ブラウザに鍵マークがついているので大丈夫」という考え方を改め、自らが他の信頼できる仕組みを用いて通信の安全性を高めることができるようになります。利用者が別の信頼点を自発的に確保するという新しい考え方をいかに浸透させるか、啓発活動のコスト負担を誰か受け持つのかについての議論が今後行われるべきであると考えます。

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、遠隔操作ウイルスとの関連などで注目されたTorの仕組みについて、金融機関の暗号表を盗むために悪用されたZeusの亜種Citadel、暗号技術を利用した環境で頻発する問題の原因に関する考察について紹介しました。IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。

執筆者:

齋藤 衛(さいとう まもる)
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発に従事の後、2001年よりIIJグループの緊急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、複数の団体の運営委員を務める。

土屋 博英、梨和 久雄(1.2 インシデントサマリ)
土屋 博英、鈴木 博志、梨和 久雄(1.3 インシデントサーベイ)
鈴木 博志(1.4.2 ZeuSの亜種 Citadel)
須賀 祐治(1.4.3 暗号技術を用いたプロトコル・実装に多発している問題の整理とあるべき姿)
IIJサービス本部 セキュリティ情報統括室

松崎 吉伸(1.4.1 Torの概要)
IIJ ネットワーク本部 ネットワークサービス部 技術開発課

協力:
加藤 雅彦、根岸 征史、春山 敬宏、小林 直、桃井 康成、齋藤 聖悟、吉川 弘晃 IIJ サービス本部 セキュリティ情報統括室

＊111 CA/Browser Forum、"Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, 22 Nov. 2011"(http://www.cabforum.org/Baseline_Requirements_V1.pdf)。
＊112 IPA、「情報セキュリティ技術動向調査(2011年上期) 4. DNSを用いた公開鍵の配送技術 - DANE」(http://www.ipa.go.jp/security/fy23/reports/tech1-tg/a_04.html)。
＊113 Convergence(http://convergence.io/details.html)。