不正アクセス禁止法改正

今回は、不正アクセス禁止法改正について解説すると共に、DNS Changerマルウェアと、DNSに関わるGhost Domain Nameの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1月から3月までの期間では、前回の期間に続いて、スマートフォン利用者の増大に伴う、端末内情報や利用者情報の取り扱いが問題となった事例が複数発生しています。AnonymousなどのHacktivismによる攻撃も継続して発生しており、企業や政府機関を狙った攻撃も引き続き多く発生しています。

中東諸国とイスラエルでは、サイトへの不正侵入や情報漏えい、重要インフラを含むWebサイトへのDDoS攻撃が相次いでいます。脆弱性ではBINDを含む複数のキャッシュDNSサーバの実装に問題が見つかり修正されています。

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。

1.2 インシデントサマリ

ここでは、2012年1月から3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]。

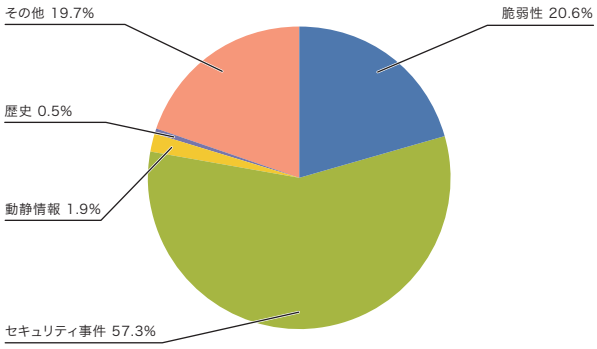


図-1 カテゴリ別比率(2012年1月〜3月)

*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:インターネットやユーザ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。

■ 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、米国をはじめ、欧州や中東の多数の国の企業や政府系サイトに対するDDoS攻撃や情報漏えい事件が発生しました。米国内においては、昨年末から継続するSOPA／PIPA法案への反対活動、欧州においてはACTA法案への反対活動が活発になり、これらの法案に関連する団体が攻撃対象となりました。

2012年1月には#OpSony2作戦と称して、昨年に続いて再びソニーグループ各社を攻撃するとの予告がなされました。しかし、この攻撃作戦は実施されず、一部のグループ会社のWebサイトが改ざんされるにとどまりました。

2月になると、WikiLeaksがStratfor社(Strategic Forecasting Inc.)の内部メール情報およそ500万通を今後順次公開すると発表しました。これは昨年末にAnonymousが不正侵入によって入手した情報の提供を受けたものです。そのため、AnonymousだけでなくWikiLeaksに対する批判も起こりました。

3月初めにはFBIが、LulzSec及びAnonymousのメンバー6人の逮捕を発表しました。そのうちLulzSecのリーダーは、昨年6月に既に逮捕・起訴されており、その後はFBIにLulzSecメンバーに関する情報を提供したり、当局からの要請にしたがってAnonymousに攻撃を止めるよう説得するなど、捜査に協力していたことが明らかとなりました。その他、3月末にDNSのルートサーバに対する攻撃予告もありましたが、実際には攻撃活動は観測されておらず、偽情報であったことが確認されました。また、Anonymous Chinaというグループが中国政府系サイトに対する大規模な攻撃活動を開始し、本稿執筆時点においても継続しています。中国におけるAnonymousの活動はこれまであまり観測されていませんが、今後の動向にしばらく注意する必要があります。

■ 中東におけるインシデント

中東では、過去にも民族間や宗教上の対立による、ネットワーク上での攻撃がたびたび発生しています。この期間では、何者かにより盗まれたイスラエル人のクレジットカード情報が投稿サイトに掲示されたことをきっかけ[*2]に、中東諸国とイスラエルの双方のグループによる報復攻撃が続いています。

攻撃は徐々にエスカレートしてきており、クレジットカード情報やSNSのメールアカウントなど、個人情報の漏えいだけでなく、イスラエル、サウジアラビア、UAEの証券取引所や金融機関などの重要インフラに対するDDoS攻撃や、サイトへの不正侵入と情報漏えいが発生しています。

■ 政府機関への攻撃と対策

政府機関を狙った攻撃も継続しています。2月には農林水産省で、業務上のやり取りのメモが関係者にメール送信された際に流出した可能性があり、後日このメモがウイルス添付された標的型メールに利用され、複数の職員宛に送信されていたと公表しました。特許庁では、内部の端末がトロイの木馬型ウイルスに感染していることが判明したとの発表がありました。この事件では、内閣官房情報セキュリティセンターからの情報提供により調査が行われたことでウイルス感染が判明し、対応が行われました。

政府としては、公開Webサーバへの脆弱性検査を行うなど、情報セキュリティ対策を強化しており、1月に開催された情報セキュリティ政策会議[*3]では、標的型不審メール訓練の中間報告や、公開Webサーバの脆弱性検査結果の概要が公表されています。

また、特に標的型攻撃などへの対策としての情報セキュリティに関する官民連携の在り方が検討されました。この中では、政府調達の調達先企業に求める情報セキュリティ要件の強化(組織内CSIRTなどの整備、経営責任者の関与など)が示されています。また、政府と企業の連絡・連携の在り方として、SOC事業者や日本シーサート協議会等民間団体、公共のセ

＊2　きっかけとなった事件とそれに続く攻撃については、例えば次のBlogにまとめられている。Hackmageddon.com、"Middle East Cyber War Timeline Master Index"(http://hackmageddon.com/middle-east-cyber-war-timeline/)。

＊3　内閣官房情報セキュリティセンター、情報セキュリティ政策会議「平成２４年第２８回会合(平成２４年１月２４日)」(http://www.nisc.go.jp/conference/seisaku/index.html#seisaku28)。

1月のインシデント

1
- セ **2日**：何者かにより盗まれた、イスラエル人のクレジットカード情報40万件以上が公開された。

2
- 脆 **4日**：Wi-Fi Protected Setup（WPS）のPIN認証の仕様にブルートフォース攻撃が容易になる脆弱性が発見された。
  JVNVU#723755 Wi-Fi Protected Setupに脆弱性（https://jvn.jp/cert/JVNVU723755/index.html）。

3
4
- 脆 **5日**：Apache Struts2に任意のコマンドが実行できる脆弱性を含む複数の脆弱性（CVE-2012-0392、CVE-2012-0393）が見つかり、修正された。
  "Multiple critical vulnerabilities in Struts2"（http://struts.apache.org/2.x/docs/s2-008.html）。

5
- 脆 **6日**：米国のセキュリティ企業の研究者により、Webサーバに対する新たな攻撃手法である "Slow Read DoS" が発表された。
  Qualys, Inc.、Qualys Security Labs "Are you ready for slow reading?"（https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read）。

6
- セ **6日**：オーストラリアの金融機関が、昨年末に受けたDDoS攻撃により、海外からの接続を制限していたことを公表した。

7
- 脆 **11日**：Microsoft社は2012年1月のセキュリティ情報を公開し、緊急に分類されるMS12-004と6件の重要な更新を含む修正をリリースした。
  「2012年1月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-jan）。

8
- 脆 **11日**：Adobe Reader及びAcrobatでコード実行の可能性のある複数の脆弱性が修正された。
  「APSB12-01:Adobe ReaderおよびAcrobat用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb12-01.html）。

9
10
- 脆 **12日**：Google社の決済サービスでAndroidアプリを購入した顧客の個人情報がアプリ開発者に誤って開示されていたことがわかり、修正された。
  本件については、次のGoogle Checkout購入者ヘルプに記載されている。「インターネットでの安全のヒント」
  （http://support.google.com/checkout/bin/answer.py?hl=ja&answer=105821）。

11
- セ **13日**：宇宙航空研究開発機構で職員の端末がコンピュータウイルスに感染し、端末内の情報などが外部に漏えいしていたことが公表された。
  「JAXAにおけるコンピュータウイルス感染の発生について」（http://www.jaxa.jp/press/2012/01/20120113_security_j.html）。

12
- セ **16日**：イスラエルの証券取引所と航空会社のWebサイトがDDoS攻撃を受けた。

13
- セ **17日**：サウジアラビアとUAEの証券取引所のWebサイトがDDoS攻撃を受けた。

14
- 脆 **17日**：Oracle社は四半期ごとの定例アップデートを公開し、合計78件の脆弱性を修正した。
  "Oracle Critical Patch Update Advisory - January 2012"（http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html）。

15
- 他 **18日**：米国議会で審議されているSOPA/PIPAへの抗議として、Reddit、Wikipedia、WordPressなどのWebサイトが停止を含む抗議運動を実施した。
  SOPA STRIKE、"A project of Fight for the Future"（http://sopastrike.com/）。

16
17
- 他 **19日**：政府機関における送信ドメイン認証技術の導入に関する取組状況についてや標的型不審メール訓練の結果の中間報告など、政府における取組状況が公表された。
  内閣官房情報セキュリティセンター、「政府機関における情報セキュリティ対策の取組状況について」（http://www.nisc.go.jp/active/general/torikumi.html）。

18
19
- 他 **20日**：「スマートフォンを経由した利用者情報の取扱いに関するWG」にて、スマートフォンのアプリによる不適切な利用者情報の取得について調査した結果などが発表された。
  総務省、「スマートフォンを経由した利用者情報の取扱いに関するWG（第1回）」
  （http://www.soumu.go.jp/menu_sosiki/kenkyu/riyousya_ict/02kiban08_03000087.html）。

20
- 他 **20日**：総務省や著作権侵害対策協議会の加盟権利者団体により、P2Pネットワーク上の著作権侵害ファイルを注意喚起文にする実証実験を行うことが発表された。
  総務省、「P2Pファイル共有ソフトによるコンテンツ不正流通の抑止に係る実証実験の実施」
  （http://www.soumu.go.jp/menu_news/s-news/anti-pirasyefforts0123-0129.html）。

21
22
- セ **26日**：大阪府警は、不正指令電磁的記録供用容疑で逮捕した男性を不正指令電磁的記録作成容疑でも送検した。作成容疑の適用は初めてとなる。

23
24
- セ **26日**：Symantec社はソースコード流出事件に関連して、pcAnywhereユーザに使用しないように注意喚起を行った。また、翌日には無償アップグレードで対応することを発表した。
  "Technical White Paper : pcAnywhere Security Recommendations"
  （http://www.symantec.com/content/en/us/enterprise/white_papers/b-pcanywhere-security-recommendations-WP.pdf）。

25
- セ **27日**：何者かにより、イランの複数のWebサイトが改ざんやDDoS攻撃を受けた。

26
- セ **27日**：Microsoft社が修正済の脆弱性（MS12-004）を悪用するマルウェアが発見された。
  Trend Micro MALWARE BLOG、"Malware Leveraging MIDI Remote Code Execution Vulnerability Found"
  （http://blog.trendmicro.com/malware-leveraging-midi-remote-code-execution-vulnerability-found/）。

27
28
- セ **29日**：日本の複数の政府関連サイトが何者かにより改ざんされた。

29
- 他 **30日**：政府機関のWebサイトへの攻撃が相次いだことから、外部委託により構築・運用しているウェブサイトの情報セキュリティ対策について注意喚起が行われた。
  内閣官房情報セキュリティセンター、「外部委託により構築・運用しているウェブサイトの情報セキュリティ対策について」（平成24年1月30日）。
  （http://www.nisc.go.jp/active/general/pdf/gaibuitaku_120130.pdf）。

30
31
- セ **31日**：WordPressで作成されたサイトが改ざんされ、Phoenix Exploit Kitのサーバにリダイレクトされる事件が発生した。
  M86 Security、"Massive Compromise of WordPress-based Sites but 'Everything will be Fine'"
  （http://labs.m86security.com/2012/01/massive-compromise-of-wordpress-based-sites-but-%E2%80%98everything-will-be-fine%E2%80%99/）。

［ 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

キュリティ関連団体とNISCとの連携の緊密化、及び各省庁主導の活動(警察庁サイバーインテリジェンス情報共有ネットワーク、経産省サイバー情報共有イニシアティブ、総務省テレコムアイザック官民協議会、NISCの府省庁間のインシデント情報共有ネットワーク)において、その結節点の役割をNISCが担うとされています。

加えて、SOC事業者において、インシデントにかかわる顧客の情報の一部を関係機関と共有できるようにするための標準的契約、約款の検討や、企業における組織内CSIRTなどの整備、情報セキュリティ人材の育成、官民で意見交換を行うシンポジウムの開催、政府機関におけるCSIRTの整備などが検討されています。

また、人材育成については昨年設置された「普及啓発・人材育成専門委員会」[*4]においても検討が進められています。

一方で、この期間中でも政府機関に関連したWebサイトにおける改ざん事件が複数発生しており、内閣官房情報セキュリティセンターより「公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について」と「外部委託により構築・運用している政府機関のWebサイトの情報セキュリティ対策について」の注意喚起が相次いで行われました。また、検索サイトで検索した結果について、目的の組織や連絡先などが上位に来るとは限らず、成りすました偽のサイトにアクセスや連絡をしてしまった事例があるとして、同じく内閣官房情報セキュリティセンターから「検索サイトを悪用した政府サイトを騙る事例に関する注意喚起」が行われています。検索結果による誤ったWebサイトの閲覧については、IPAからも相談事例の報告が公開されています[*5]。

■ 脆弱性とその対応

この期間中ではMicrosoft社のWindows[*6*7*8*9]、Adobe社のAdobe Reader及びAcrobat、Adobe Flash Player、Oracle社のJREなどのアプリケーションで多くの脆弱性が発見され、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ています。また、CMSツールのWordPressについてもクロスサイトスクリプティング脆弱性を含む複数の脆弱性が修正されました。これ以外にも、Mac OS X Lionで修正が行われたりQuickTimeの任意のコード実行を含む複数の脆弱性が発見され、修正されたりしています。Cisco社からは定例のアップデートが提供され、ルータやスイッチのファームウェアに対して、複数の脆弱性が修正されました。また、Webサーバに対するリソースを枯渇させる新たなDoS攻撃を行う手法として「Slow Read DoS」がテストツールと共に公表されました。更にBINDを含む複数のキャッシュDNSサーバの実装に、失効したドメインを利用可能な状態にし続けることができる問題[*10]が公表されています。この問題については「1.4.3 Ghost Domain Names脆弱性について」も併せてご参照ください。

■ スマートフォンアプリと利用者情報の取り扱い

スマートフォンの普及に伴い、アプリで取得した端末内情報や利用者情報の取り扱いによる問題が増えています。

この期間では、新聞や雑誌を読むための複数のアプリで利用者の閲覧履歴や端末識別情報が許諾なしに送信されている

---

*4 次の内閣官房情報セキュリティセンター、「普及啓発・人材育成専門委員会」の議事録などを参照のこと、(http://www.nisc.go.jp/conference/seisaku/jinzai/index.html)。これ以外にもIPAや経済産業省でも人材育成に関する取り組みが行われている。

*5 IPA、「『コンピュータウイルス・不正アクセスの届出状況[1月分]について』4. 相談受付状況」(http://www.ipa.go.jp/security/txt/2012/02outline.html)。

*6 「マイクロソフト セキュリティ情報 MS12-004 - 緊急 Windows Media の脆弱性により、リモートでコードが実行される(2636391)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-004)。

*7 「マイクロソフト セキュリティ情報 MS12-008 - 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(2660465)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-008)。

*8 「マイクロソフト セキュリティ情報 MS12-016 - 緊急 .NET Framework および Microsoft Silverlight の脆弱性により、リモートでコードが実行される(2651026)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-016)。

*9 「マイクロソフト セキュリティ情報 MS12-020 - 緊急 リモート デスクトップの脆弱性により、リモートでコードが実行される(2671387)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-020)。

*10 この問題については次の発見者の論文も参照のこと。"Ghost Domain Names: Revoked Yet Still Resolvable"(https://www.isc.org/files/imce/ghostdomain_camera.pdf)。

2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

脆 **1日**：Apple社のMac OS X Lionについて、QuickTimeのコード実行可能な脆弱性を含む複数の脆弱性が修正された。
「OS X Lion v10.7.3およびセキュリティアップデート2012-001のセキュリティコンテンツについて」(http://support.apple.com/kb/HT5130?viewlocale=ja_JP&locale=ja_JP)。

セ **2日**：農林水産省で業務上のメモを利用した標的型メール事案が発生していたことが公表された。
「農林水産省における標的型メール事案について」(http://www.maff.go.jp/j/press/kanbo/hyoka/120202.html)。

脆 **3日**：PHPにリモートから任意のコード実行が可能な脆弱性が見つかり修正された。
PHP.net、"PHP 5.3.10 Released!"(http://news.php.net/php.announce/87)。

セ **7日**：特許庁内の複数端末でウイルス感染が発生していたことが公表された。
「特許庁におけるウイルス感染事案について」(http://www.meti.go.jp/press/2011/02/20120207001/20120207001.pdf)。

脆 **8日**：複数のDNSサーバの実装にキャッシュしたリソースレコードの保持期限を外部から延長させることができる問題(CVE-2012-1033)があることが発表された。
JVN、「JVNVU#542123 複数のDNSネームサーバの実装に問題」(https://jvn.jp/cert/JVNVU542123/)。BINDについては次のISCのアドバイザリーも参照のこと。ISC、"Ghost Domain Names: Revoked Yet Still Resolvable"(https://www.isc.org/software/bind/advisories/cve-2012-1033)。

セ **8日**：Anonymousを名乗る何者かにより、Symantec社のpcAnywhereのソースコードの一部が公開された。

セ **13日**：AnonymousによりDNSのルートサーバに対する攻撃「Operation Global Blackout」が3月31日に行うことが予告された。ただし、この攻撃は失敗に終わるとの指摘が専門家からなされたり、別のAnonymousにより偽の作戦であると指摘を受けるなど攻撃予告の信憑性を疑問視する声もあった。
詳細については、次のErrata SecurityのBlogなども参照のこと。
"No, #Anonymous can't DDoS the root DNS servers"(http://erratasec.blogspot.com.au/2012/02/no-anonymous-cant-ddos-root-dns-servers.html)。

セ **14日**：イスラエル政府のWebサイトが侵入され、盗まれた情報が公開された。

他 **15日**：内閣官房情報セキュリティセンターより検索サイトを悪用した政府サイトを騙る事例に関する注意喚起が行われた。
「検索サイトを悪用した政府サイトを騙る事例に関する注意(注意喚起)」(http://www.nisc.go.jp/active/general/pdf/search_kanki_120215.pdf)。

脆 **15日**：Oracle社のJREに任意のコード実行を含む複数の脆弱性が発見され修正された。
"Oracle Java SE Critical Patch Update Advisory - February 2012"(http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html)。

脆 **15日**：Microsoft社は2012年2月のセキュリティ情報を公開し、MS12-008やMS12-016を含む4件の緊急と5件の重要に分類される修正をリリースした。
「2012年2月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-feb)。

脆 **15日**：Adobe Flash Playerに不正なWebサイトに誘導することでなりすまし可能なクロスサイトスクリプティング脆弱性を含む複数の脆弱性が見つかり、修正された。
「APSB12-03: Adobe Flash Playerに関するセキュリティアップデート公開」(http://kb2.adobe.com/jp/cps/931/cpsid_93112.html)。

セ **16日**：ロシアで大統領選挙に関連すると考えられるラジオ局やニュースサイトに対するDDoS攻撃が観測された。
Arbor Networks Security Blog、"DDoS Attacks in Russia Added to Protests"(http://ddos.arbornetworks.com/2012/02/ddos-attacks-in-russia/)。

セ **18日**：ロシアの大統領選挙で用意された選挙監視用カメラシステムに対し、DDoS攻撃が行われたとの報道があった。

セ **21日**：FBIがDNSChangerへの被害者対策で稼働していたDNSサーバの運用が、3月8日で終了することが再度周知された。
ISC Diary、"DNSChanger resolver shutdown deadline is March 8th"(http://isc.sans.edu/diary.html?storyid=12625)。

他 **22日**：Kaspersky Lab社から2011年度後半におけるDDoS攻撃に関するレポートが公表された。
"DDoS attacks in H2 2011"(http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011)。

セ **23日**：地方自治体のWebサイトや関連する複数のWebサイトがDDoS攻撃や改ざん攻撃を受けた。

他 **28日**：WikiLeaksがStratfor社の内部メール情報の公開を開始した。
Wikileaks、"The Global Intelligence Files"(http://wikileaks.org/the-gifiles.html)。

他 **29日**：IPAより、国内外の複数社のPLC(Programmable Logic Controller)の脆弱性やPoCが公開されたことから「制御機器の脆弱性に関する注意喚起」が行われた。
「制御機器の脆弱性に関する注意喚起」(http://www.ipa.go.jp/about/press/20120229.html)。

他 **29日**：総務省と経済産業省はGoogle社に対し、同社の新プライバシーポリシーでの法令遵守及び利用者に対する分かりやすい説明などの対応を求める文書を通知した。
総務省、「グーグル株式会社に対する通知」(http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000117.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

として問題となりました。このうちの1つではテストとして導入した情報取得の仕組みがそのまま残っていることで受信されていないにも関わらず、利用者情報の送信が行われていたことから、該当機能を削除する対応が行われました。

スマートフォンでの情報の取り扱いについては、必要以上の権限を要求するアプリなどの問題が指摘されています。これらの問題については、1月より総務省による「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」の下に開催されている「スマートフォンを経由した利用者情報の取扱いに関するWG」にてスマートフォンからの利用者情報の取得状況についての調査結果の報告が行われる[*11]など、現在の取り扱い状況について把握すると共に、利用者情報の取り扱いや取得の際の周知方法など、安全安心な利用に向けた検討が行われています。

利用者情報の取り扱いについては、他にAndroid公式アプリマーケットで購入したユーザのデータが誤って作者に公開されていたことが分かり、問題となりました。また、はてなブックマークが今まで提供していた機能に対し、後にユーザの行動情報を第三者に送信する機能を追加していたとして、設置していたサイト管理者と利用者双方への周知が不十分だったとして問題となりました[*12]。更に、GPSによる位置情報の記録とその不適切な公開も話題となりました。写真に添付されたジオタグや位置情報アプリなど、個人が活動している場所を特定できるような情報の利用については、ブログやSNSなどの個人と結びついた形で公開すると、場所が特定されることで、思わぬリスクが発生する場合があります。このようなリスクについて注意を促す「Geotagging poses security risks」が米国で公開されています[*13]。日本でも東京都より、位置情報の利用について、注意喚起が行われています[*14]。

■ セキュリティソフトのソースコード漏えい

この期間では、セキュリティ対策ソフトのソースコードの流出が発生しました。1月にSymantec社の複数の製品でソースコードが流出していることが判明[*15]しました。同社は、公開されたソースコードは4〜5年前のものであり、現在の製品に影響は少ないと発表しましたが[*16]、その後にAnonymousを名乗る人物から金銭を要求されていたことが判明したり、ソースコードの一部が新たに公開されるなどしました。このため、一部の製品に対し、新たにアップデートが提供されました[*17]。今回の事件では、外部に提供したものが流出したことが原因とされています。

■ DDoS攻撃

この期間では、大規模なDDoS攻撃が多く発生しています。ロシアでは3月に行われた大統領選挙に関連してラジオ局やニュースサイトなどに対し、選挙前から複数のDDoS攻撃が発生しています。また、選挙監視用のWebカメラシステムへの攻撃も発生しました。韓国では、政府の政策に抗議するため、未成年による政府機関WebサイトへのDDoS攻撃が発生しました。オーストラリアの証券会社では昨年末から発生しているDDoS攻撃に対し、海外からの接続を遮断する対応を行った影響で海外の同社顧客が取引できなくなるなどの影響が発生しています。

■ サイバー犯罪への取り組み

ボットネットやフィッシングによるサイバー犯罪について、民間企業が協力して対処を行う取り組みが進められています。

この期間では、米Microsoft社のDigital Crimes Unitと金融業界や捜査機関が共同でZeuSボットネットのC&Cサーバを摘発したと発表しました。Microsoft社の同グループでは過去にもボットネットの摘発に協力しており、例えば

＊11 調査結果は平成24年1月20日に開催された第1回WGで、KDDI研究所研究主査 竹森 敬祐氏が発表している。「スマートフォンからの利用者情報の送信」（http://www.soumu.go.jp/main_content/000143966.pdf）。
＊12 この問題については、次のはてなブックマーク日記で機能の停止が発表された。「はてなブックマークボタンが取得した行動情報の第三者への送信を停止しました」（http://hatena.g.hatena.ne.jp/hatenabookmark/20120313/1331629463）。
＊13 UNITED STATES ARMY、"Geotagging poses security risks"（http://www.army.mil/article/75165/Geotagging_poses_security_risks/）。
＊14 東京くらしWeb、「スマートフォン等で撮影した写真をブログにアップすると撮影場所が特定されることがあるので注意しましょう。」(http://www.shouhiseikatu.metro.tokyo.jp/sodan/kinkyu/shohi_advice.html)。
＊15 Sophos、nakedsecurity "Symantec's Norton AntiVirus source code exposed by hackers"（http://nakedsecurity.sophos.com/2012/01/06/symantec-norton-antivirus-source-code-hackers/）。
＊16 Symantec社の声明については次のFacebookの投稿で確認できる。（https://www.facebook.com/Symantec/posts/10150465997682876）。
＊17 この公開による製品への影響については次のSymantec社の発表など確認のこと。"Claims by Anonymous about Symantec Source Code"（http://www.symantec.com/theme.jsp?themeid=anonymous-code-claims）。

3月のインシデント

1
2
3
4
5
6
7
8
9
10
11

セ **1日**：Microsoft社のWindows Azureで「うるう年」の処理ミスによる障害が発生した。
Microsoft社、「2012年2月29日に発生したWindows Azure中断について、Windows Azureブログにて公開された要約 -- Windows Azure Platform」(http://www.microsoft.com/japan/windowsazure/disruption229/)。

セ **1日**：NASAが2010年から2011年に受けた攻撃について、不正侵入による情報漏えいなどが発生していたとする報告書を公表した。
NASA Cybersecurity：An Examination of the Agency's Information Security、(http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf)。

他 **1日**：Google社はサービスごとに規定していたプライバシーポリシーをまとめた新プライバシーポリシーを発行した。
Google Japan Blog、「Google の新しいプライバシーポリシーについて」(http://googlejapan.blogspot.jp/2012/03/google.html)。

脆 **5日**：Adobe Flash Playerにメモリ破損によるコード実行の可能性がある脆弱性を含む複数の脆弱性(CVE-2012-0768、CVE-2012-0769)が見つかり、修正された。
「APSB12-05: Adobe Flash Playerに関するセキュリティアップデート公開」(http://kb2.adobe.com/jp/cps/932/cpsid_93265.html)。

セ **5日**：GitHubにRailsのmass assignment脆弱性など複数の問題があり、ハッキングを受けたことが公表された。
GitHub Blog、"Public Key Security Vulnerability and Mitigation"(https://github.com/blog/1068-public-key-security-vulnerability-and-mitigation)。

12
13
14
15

セ **7日**：米連邦裁判所は、DNS Changerへの被害者対策で稼働していたDNSサーバの運用を120日間延長することを認めた。
Trend Micro SECURITY BLOG、「巨大ボットネットに利用されたDNSサーバの運用、米連邦裁判所により120日間延長に」(http://blog.trendmicro.co.jp/archives/4881)。

セ **7日**：米国連邦捜査局(FBI)は米国や海外でLulzSecやAntiSecに参加していたとみられるAnonymousのメンバー6人を訴追したことを発表した。
"Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims."(http://www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims)。

脆 **14日**：Microsoft社は2012年3月のセキュリティ情報を公開し、緊急に分類されるMS12-020と4件の重要な更新を含む修正をリリースした。
「2012年3月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-mar)。

セ **15日**：イスラエル空軍など複数のWebサイトが侵入され、盗まれた情報が公開された。

他 **15日**：IPAより、内部不正防止の国内外での取り組みをまとめた「『組織の内部不正防止への取り組み』に関するレポート」が公表された。
「IPA テクニカルウォッチ『組織の内部不正防止への取り組み』に関するレポート」(https://www.ipa.go.jp/about/technicalwatch/20120315.html)。

16
17
18
19
20
21
22
23
24

他 **19日**：CNCERT/CCは、2011年の中国のインターネットにおける攻撃の状況について、攻撃に関与したIPアドレスで最も多かったのは日本からであったとする報告を公表した。
CNCERT/CC、"2011年中国互联网网络安全态势报告"(http://www.cert.org.cn/UserFiles/File/20120319201 1annualreport(1).pdf)(中国語)。
この件については、次のSophos社のNakedsecurityも参照のこと。"CERT China claims Japan and US lead in attacks on Chinese internet sites"(http://nakedsecurity.sophos.com/2012/03/22/cert-china-claims-japan-and-us-lead-in-attacks-on-chinese-internet-sites/)。

セ **21日**：ロシアのフィッシング詐欺グループがセキュリティ企業などの協力により逮捕された。
Trend Micro SECURITY BLOG、「再びセキュリティ業界との連携で摘発。国際的フィッシング詐欺団がロシアで逮捕」(http://blog.trendmicro.co.jp/archives/4922)。

他 **22日**：IPAより、「2012年版 10大脅威　変化・増大する脅威！」が公表された。
「『2012年版 10大脅威　変化・増大する脅威！』を公開」(http://www.ipa.go.jp/security/vuln/10threats2012.html)。

セ **24日**：Microsoft社のDigital Crimes Unitや金融サービス業界のメンバーの強力により「ZeuS」ボットネットが摘発された。
詳細については次のMicrosoft社のBlogを参照のこと。The Official Microsoft Blog、Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets(http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx)。

25
26
27
28
29
30
31

脆 **28日**：Adobe Flash Playerにメモリリークにより任意のコード実行が可能な複数の脆弱性(CVE-2012-0772、CVE-2012-0773)が見つかり、修正された。
「APSB12-07: Adobe Flash Playerに関するセキュリティアップデート公開」(http://kb2.adobe.com/jp/cps/933/cpsid_93381.html)。

脆 **29日**：Cisco Security Advisoryが公表され、13件の脆弱性が修正された。
"Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication"(http://www.cisco.com/cisco/web/support/JP/111/1110/1110698_Cisco_ERP_mar12-j.html)。

他 **30日**：フィッシングの処罰化などを含む「不正アクセス行為の禁止等に関する法律の一部を改正する法律案」が可決した。
警察庁、「第１８０回国会(常会)提出法案『不正アクセス行為の禁止等に関する法律の一部を改正する法律案』」(http://www.npa.go.jp/syokanhourei/kokkai/index.htm)。

セ **31日**：AnonymousによるOperation Global Blackout予告日。実際にはDNSのrootサーバに対する攻撃は発生しなかった。

セ **31日**：Anonymous Chinaにより、中国の複数のサイトに対する侵入事件が発生した。

[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

2010年2月に行われたWaldacボットネットへの利用ドメインの凍結によるテイクダウン[*18]や2011年3月に行われたRustockボットネットのC&Cサーバのテイクダウン[*19]などが知られています。また、Trend Micro社でも、米国の大学やロシアの法執行機関と共同でフィッシング詐欺を行っていたグループを逮捕したことを公表しています。

2011年11月にFBIによってC&Cサーバや悪意のあるDNSサーバを差し押さえられたDNS Changerマルウェアでは、感染被害者への救済手段として運用されていた正常なDNSサーバの停止について、被害者が依然として多いことから当初の予定であった3月8日での停止を中止し、120日間延長することが米連邦裁判所に承認されました。この問題については「1.4.2 DNS Changerマルウェア」も併せてご参照ください。

このように、民間企業と法執行機関の協力によるサイバー犯罪への取り組みが成果を上げていますが、一方で感染者への通知など被害者救済では時間がかかるなどの問題も明らかになっています。

■ その他の動向

その他の動向としては、複数社の制御機器PLC(Programmable Logic Controller)において、複数の脆弱性が公開された[*20]ことから、IPAはこれらの制御機器に対して適切な対応を検討・実施することを促す「制御機器の脆弱性に関する注意喚起」を発行しました。

スマートフォンなどのモバイル端末の普及を背景として、移動通信トラフィックが急増している状況から公衆無線LANなどの整備が進められていますが、拡充に伴って、様々な提供形態が出現したことによる電波干渉や、無線LANの不適切な利用によるなりすましや情報の窃取などの問題があることも明らかになってきました。このため、総務省により、無線LANに関する現状を整理すると共に、その安心安全な利用や普及に関する課題の抽出・整理を行い、必要な方策を検討することを目的として、「無線LANビジネス研究会」が開催されました[*21]。

内部不正を原因とする情報セキュリティインシデントも継続して発生しており、このような被害を未然に防ぐ取り組みが複数進められています。IPAでは、国内外で実施されている内部不正防止に関する取り組み状況について解説した「『組織の内部不正防止への取り組み』に関するレポート」を公表しています[*22]。同じくIPAから2011年に発生したセキュリティ事件や事故について事例を交えながら解説を行った「2012年版10大脅威　変化・増大する脅威！」が発行されました。

*18 Microsoft on the Issues、"Cracking Down on Botnets"(http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx)。
*19 Microsoft on the Issues、"Taking Down Botnets: Microsoft and the Rustock Botnet"(http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx)。
*20 ICS-CERT、"ICS-ALERT-12-020-01-S4 DISCLOSURE OF MULTIPLE PLC VULNERABILITIES IN MAJOR ICS VENDORS"(http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-020-01.pdf)。
*21 総務省、無線LANビジネス研究会(http://www.soumu.go.jp/main_sosiki/kenkyu/lan/index.html)。
*22 IPA、「『組織の内部不正防止への取り組み』に関するレポート」(http://www.ipa.go.jp/about/technicalwatch/20120315.html)。

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、状況により多岐にわたります。しかし、攻撃の多くは、脆弱性など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です。

■ 直接観測による状況

図-2に、2012年1月から3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、正確な攻撃の実態を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[*23]、サーバに対する攻撃[*24]、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、404件のDDoS攻撃に対処しました。1日あたりの対処件数は4.4件で、平均発生件数は前回のレポート期間と比べて減少しています。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.2%、サーバに対する攻撃が59.7%、複合攻撃が40.1%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、複合攻撃に分類されるもので、最大6万2,000ppsのパケットによって673Mbps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82.4%が攻撃開始から30分未満で終了し、17.6%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はありませんでした。なお、今回もっとも長く継続した攻撃は、複合攻撃に分類されるもので4時間55分にわたりました。

なおこの期間中、IIJ DDoS対策サービス以外のサービスにおいて、1Gbps以上の攻撃が継続的に発生しており、最大4Gbpsで75万ppsの攻撃の他、3Gbps以上や110万ppsといった大規模攻撃が複数発生しています。

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[*25]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[*26]の利用によるものと考えられます。

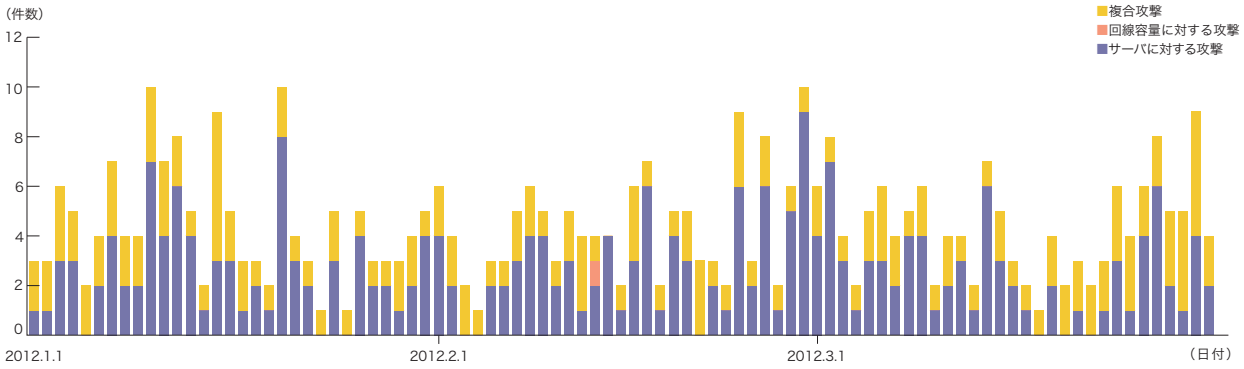


図-2 DDoS攻撃の発生件数

*23 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。

*24 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。

*25 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。

*26 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[*27]によるDDoS攻撃のbackscatter観測結果を示します[*28]。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1月から3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60.5%を占めています。また、リモートデスクトップで利用される3389/TCPや、リモートアクセスVPNのPPTPで利用される1723/TCP、MySQLで利用される3306/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35.7%、中国26.1%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。

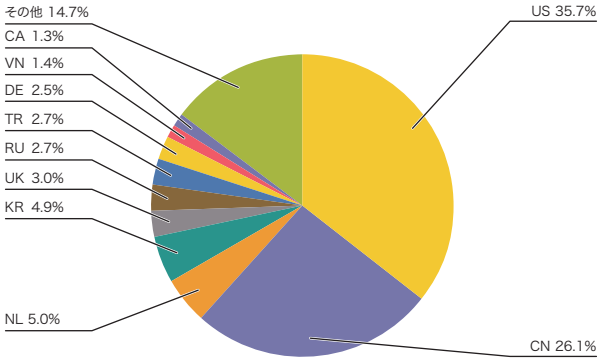


図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

特に多くのbackscatterを観測した場合について、攻撃先をポート別にみると、まず、米国内にあるホスティング事業者のWebサーバ(80/TCP)への攻撃が1月4日から5日にかけて観測されています。1月9日には中国国内のサーバに対する7208/TCPへの攻撃が観測されました。また、同じ日にカナダのドメインレジストリのDNSサーバ(53/TCP)への攻撃が観測されています。

2月1日にはWebサーバ(80/TCP)への攻撃が多く観測されましたが、これは米国国内のサービス事業者に対する攻撃でした。2月22日にはブラジルと中国の複数のWebサーバを対象とした攻撃が観測されました。後者のWebサーバへの攻撃の1つは中国国内の検索サイトを対象としており、この期間中にも断続的に観測されていましたが、この日は特に多く観測されています。同じく2月22日から23日にかけて、MySQL(3306/TCP)への攻撃が多く観測されましたが、これはトルコの動画ストリーミングサイトへの攻撃でした。3月13日には米国内のホスティング事業者のWebサーバ(80/TCP)への攻撃が観測されています。

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、1月後半に

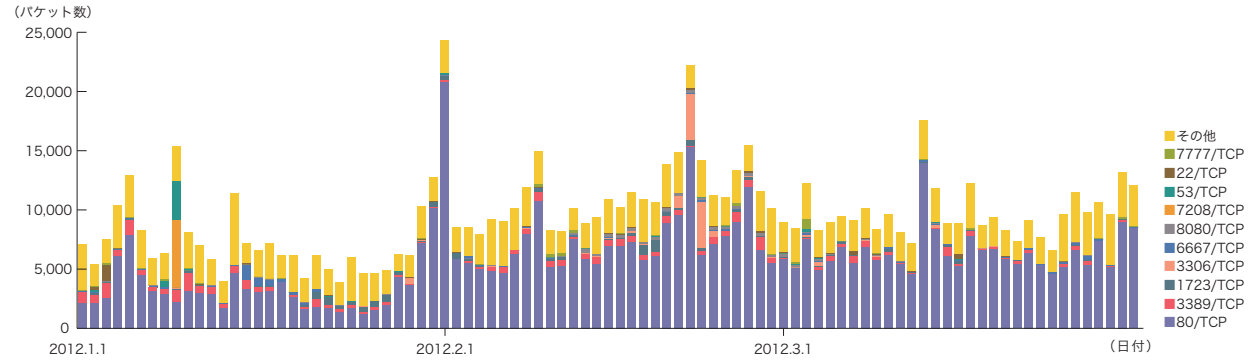


図-4 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

＊27 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。
＊28 この観測手法については、本レポートのVol.8（http://www.iij.ad.jp/company/development/report/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。

発生したAnonymousによると考えられる米国司法省への攻撃、2月に発生したAnonymous Brasilによると考えられるブラジルの複数の銀行への攻撃、Anonymous Swedenによると考えられるスウェーデン政府への攻撃、ロシアのニュースサイトへの攻撃と考えられるbackscatterをそれぞれ検知しています。

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[*29]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[*30]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。

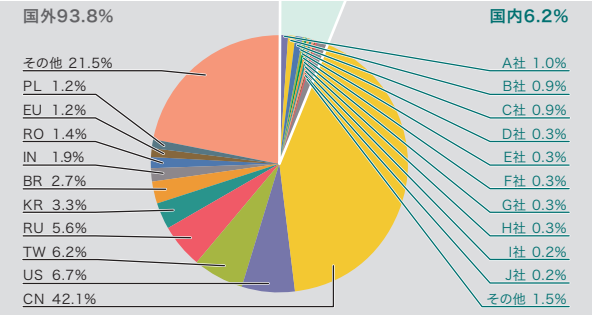


図-5 発信元の分布(国別分類、全期間)

■ 無作為通信の状況

2012年1月から3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、RAdminと呼ばれるWindows用リモート管理ソフトが使用する4899/TCPへの通信、SSHで利用される22/TCP、telnetで利用される23/TCP、MySQLで利用される3306/TCPに対する探索行為も観測されています。これらに加えて、2582/TCPなど、一般的なアプリケーションでは利用されない目的不明な通信も観測されました。図-5で発信元の国別分類を見ると、中国の42.1%、米国の6.7%、日本国内と台湾の6.2%が比較的大きな割合を占めています。

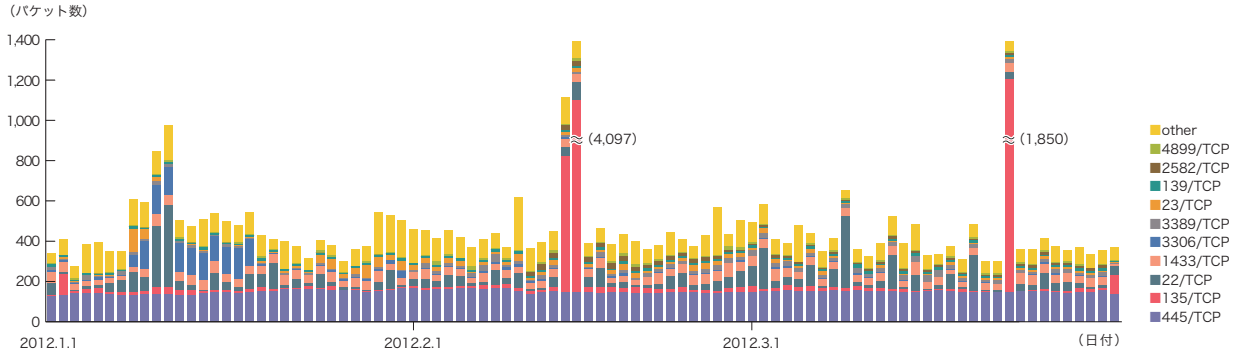


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*29 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。

*30 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。

期間中、135/TCPが2月14日から2月15日の間と3月23日、3306/TCPが1月8日から1月18日の間急増しました。これらはそれぞれ中国に割り当てられた1つのIPアドレスから大量の通信が行われたものです。

また、SSHの辞書攻撃と思われる通信も断続的に発生しており、例えば1月10日に中国、1月11日に米国、3月9日にインドの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。

■ ネットワーク上でのマルウェアの活動

同じ期間中での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[*31]の総数を総取得検体数、検体の種類をハッシュ値[*32]で分類したものをユニーク検体数としています。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-7から図-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。

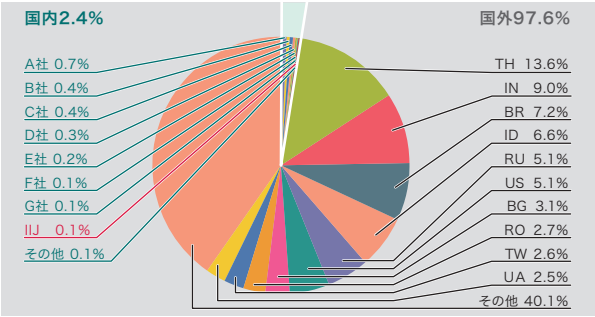


図-7 検体取得元の分布（国別分類、全期間、Confickerを除く）

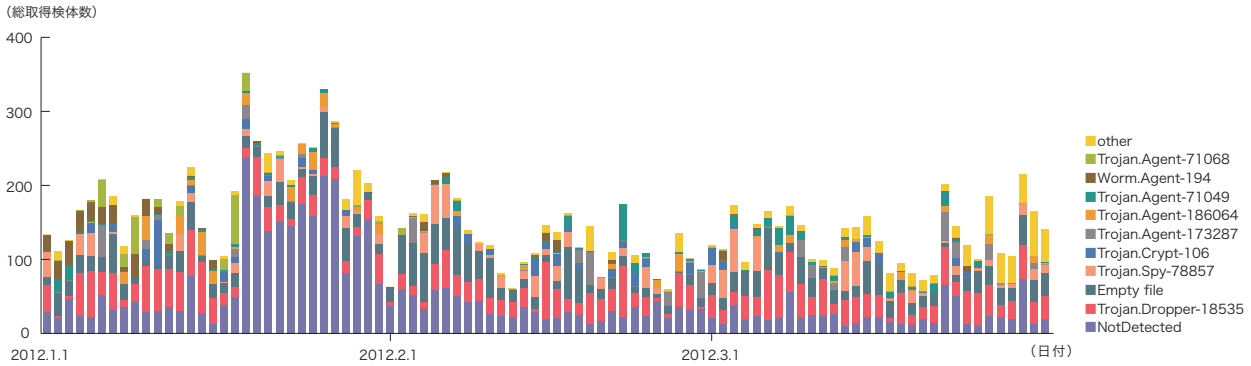


図-8 総取得検体数の推移（Confickerを除く）

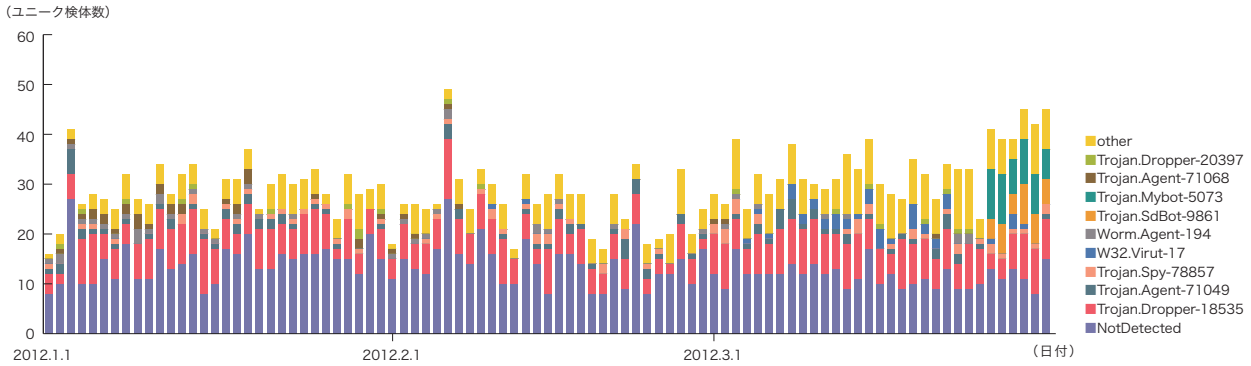


図-9 取得検体数の推移（ユニーク検体数、Confickerを除く）

＊31 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。

＊32 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。

期間中での1日あたりの平均値は、総取得検体数が150、ユニーク検体数が29でした。前号より総取得検体数がほぼ半減していますが、これは前号ではほぼ全期間にわたって出ていたタイ及びインドネシアからの検体取得が大幅に減少したためです。ただし1月19日から1月30日の間、これらの2ヵ国からの未知の検体の取得割合が増加しています。そこで、より詳しく調査を行った結果、IRCサーバで制御されるタイプのボット2種類[*33][*34]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65.0%、ボット型31.7%、ダウンローダ型3.3%でした。また解析により、20個のボットネットC&Cサーバ[*35]と7個のマルウェア配布サイトの存在を確認しました。

■ MS12-020とRDP(3389/TCP)

2012年3月にMicrosoft社からセキュリティ情報[*36]が発行されました。その中のMS12-020[*37]はネットワークから認証なしに任意のコード実行を行える可能性がある脆弱性があったため、IIJ-SECTのブログであるSecurity Diaryの中で取り上げました[*38]。図-10は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です。3月14日のパッチ公開後、3月15日から3月17日にかけて若干の増加が見られたものの、本稿執筆時点(2012年4月)まで大きな変化はありませんでした。また、この脆弱性を突いて任意のコード実行を行うワームやExploitコードの存在もIIJでは確認していません。ただし、パッチを未適用かつRDPを有効にしている場合は危険であることに変わりはないため、引き続きこの通信を注視する必要があると考えています。

■ 観測状況とConfickerワーム

Confickerを含む期間中の1日あたりの平均値は、総取得検体数が48,358、ユニーク検体数が1,111でした。前号と比較するとそれぞれ97.4%、98.7%、とそれぞれ微減しました。今号もConfickerが支配的で、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。前号で増減をお伝えしましたが、その後も傾向としては短い期間での増減を繰り返しつつ、ハニーポットを切り替えたIIR Vol.12の期間(2011年4月から6月)に比べると、それぞれ17%前後、取得数は減少しています。ただ、この支配的な状況が変わらないことから、今号からConfikcerワームを含む図は省略しています。

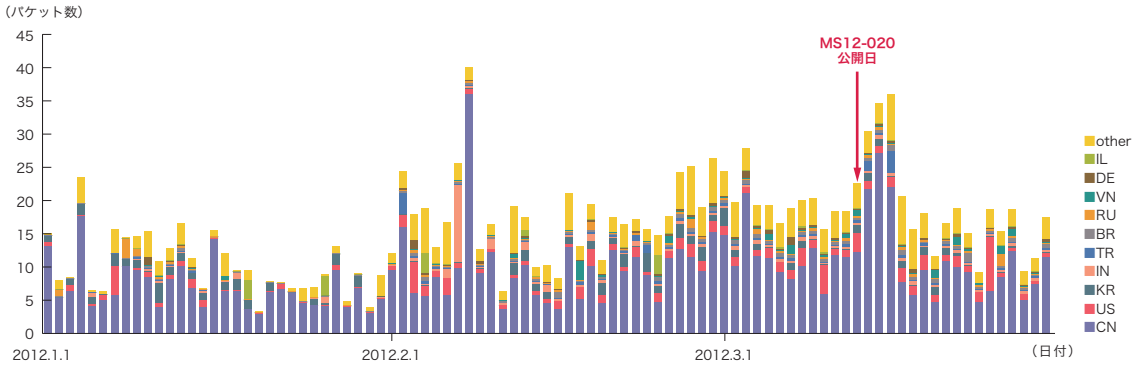


図-10 ハニーポットに到着した通信の推移(日別・RDP(3389/TCP)・一台あたり)

*33 Trojan: Win32/Ircbrute(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute)。
*34 Win32/Hamweq(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq)。
*35 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。
*36 Microsoft社、「2012年3月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-mar)。
*37 Microsoft社、「セキュリティ情報 MS12-020 - 緊急 リモート デスクトップの脆弱性により、リモートでコードが実行される (2671387)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-020)。
*38 IIJ-SECT Secuirty Diary、「MS12-020の脆弱性に関する注意喚起」(https://sect.iij.ad.jp/d/2012/03/226127.html)。

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[*39]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1月から3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-11に、攻撃の推移を図-12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54.2%、米国4.0%、香港3.4%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からあまり変化していません。

この期間中、1月20日に発生した攻撃では、米国の特定の攻撃元から特定の攻撃先に対する攻撃と、国内の特定の攻撃元から別の特定の攻撃先に対する攻撃が発生しています。また、3月9日に発生した攻撃は、香港の特定の攻撃元から特定の攻撃先に対する攻撃でした。どちらの攻撃についても、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。

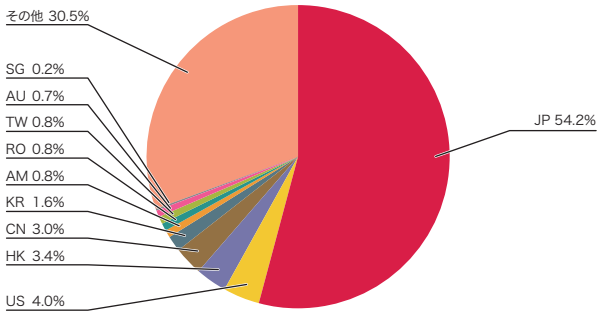


図-11 SQLインジェクション攻撃の発信元の分布

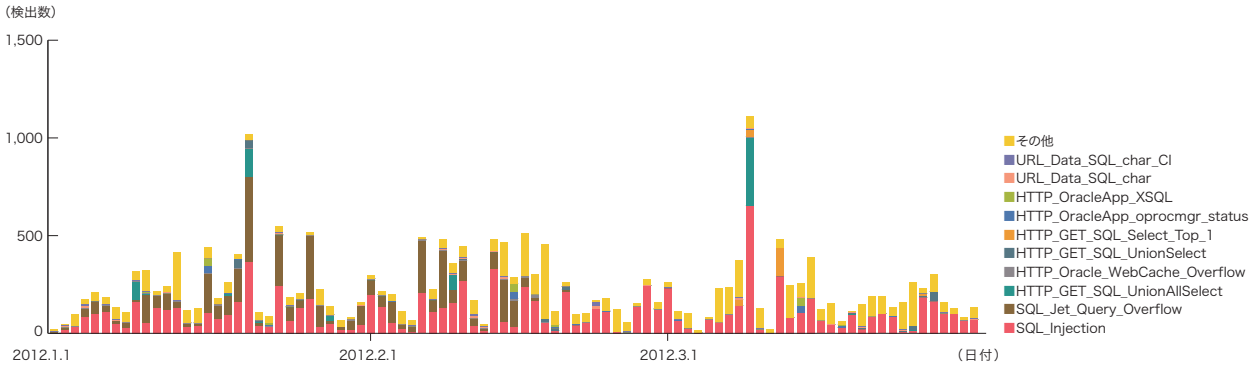


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*39 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、不正アクセス禁止法の改正と、利用者の参照するDNS設定を書き換えるDNS Changerマルウェア、及びDNSサーバの脆弱性として報じられたGhost Domain Nameの問題について解説します。

1.4.1 不正アクセス禁止法改正について

2012年3月31日に「不正アクセス行為の禁止等に関する法律(以下、不正アクセス禁止法)」が改正され、公布されました。ここでは改正に至る経緯や改正内容のポイントを説明します。

■ インターネット関連の問題と法整備

インターネットは社会経済活動の基盤として利用が進み、世界的に見てもインターネットを利用した不正行為は増加しています[*40]。国境を越えたサイバー空間上の不正行為を取り締まるために国際的に協調する必要があることから、欧州評議会の主導により「サイバー犯罪に関する条約(以下、サイバー犯罪条約)[*41]」が作成されました。本条約には不正アクセスの犯罪化やデータ保全の刑事手続整備、犯人引渡しの国際協力などが規定されており、2001年に日本は条約に署名を行っています。日本でもインターネットを利用した不正行為が発生しており、様々な法律の整備が行われるようになりました(表-1)。サイバー犯罪に関連する代表的な法律には、次のようなものがあります。

- **特定電子メールの送信の適正化等に関する法律の施行**
  携帯電話の普及と共に迷惑メールの流量が飛躍的に増加し、大量の宛先不明メール配信による通信設備への負荷や、利用者への高額な料金請求などが問題となりました。このため、2002年7月に本法律が施行され、広告宣伝などの特定電子メール送信に関する規制と罰則が定められました。迷惑メール送信手法の変化に伴い、本法律はその後も継続的に改正が行われています。
- **児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律(児童ポルノ禁止法)の改正**[*42]
  本法律は児童の権利を擁護することを目的として1999年11月より施行されました。当初は児童ポルノの記録媒体として写真やビデオテープとされていたものが、2004年の改正によって、電磁的記録も対象とされ、インターネット上のサイトで児童ポルノを公開するといった行為が違法となりました。更に、現在では児童ポルノコンテンツの流通に関する対策として、ISPによるブロッキングなども実施されています[*43]。
- **著作権法の一部改正**
  ネットオークションでの海賊版コンテンツ販売や、不正コピーされたコンテンツのファイル交換ソフトによる配信といった権利侵害行為が増加していることから、2010年1月に著作権法の一部が改正されました。改正によって、海賊版と知りつつネットオークションで販売することや、権利侵害されたコンテンツであることを知りながらダウンロードするといった行為が違法となりました。法律施行後、ファイル交換ソフト利用者は減少する傾向にあります[*44]。
- **刑法の一部改正**
  2011年7月に「不正指令電磁的記録に関する罪(ウイルス罪)」が新設されました。コンピュータウイルスはサイバー犯罪の手段として用いられることが多いものの1つです。しかし、従来法ではコンピュータウイルスの作成や保管などの行為に関しては犯罪という定義がなく、取り締まりが困難でした。日本国内でもファイル交換ソフト利用者を中心として流通する山田ウイル

*40 例えば米国では、Internet Crime Complaint Centerにより統計情報が公開されている(http://www.ic3.gov/media/annualreports.aspx)。国内では警察庁により統計情報が公開されている(http://www.npa.go.jp/cyber/statics/index.html)。
*41 本条約については、外務省が日本語版を公開している(http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html)。原文については次を参照のこと(http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm)。
*42 この法律は次の法令データ提供システムで確認できる(http://law.e-gov.go.jp/htmldata/H11/H11HO052.html)。
*43 この試みについては、本レポートのVol.12「インターネットトピック:国内ISPによる児童ポルノブロッキングについて」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol12.pdf)で紹介している。
*44 コンピュータソフトウェア著作権協会が「ファイル共有ソフト利用実態調査」として統計情報を公表している(http://www2.accsjp.or.jp/research/)。

表-1 日本国内におけるインターネット関連事件と法整備の動向

年月	日本国内の動向	種別
1999年４月	**「風俗営業等の規制及び業務の適正化等に関する法律」改正。** インターネット上でのポルノ映像配信営業が届出対象となる。	法整備
2000年２月	**「不正アクセス行為の禁止等に関する法律」施行。** 不正アクセス行為と助長行為の違法化、防護措置の義務化などが行われた。	法整備
2001年11月	**サイバー犯罪条約制定。** 各国がサイバー犯罪対策に力を入れることが合意される。	法整備
2001年11月	WinMXを使った違法コンテンツ配信で世界初の刑事摘発が行われる。	著作権関連
2001年11月	迷惑メールの急激な増加を受けて、総務省による「迷惑メールへの対応の在り方に関する研究会」が発足する。	迷惑メール
2002年７月	**「特定電子メールの送信の適正化等に関する法律」施行。** 迷惑メール送信に対する規制が開始される。	法整備
2003年11月	Winnyを使った違法コンテンツ配信で逮捕者が出る。	著作権関連
2004年１月	**「不正競争防止法」の改正。** 営業秘密の刑事的保護の強化が実施される。	法整備
2004年３月	ファイル共有ネットワークで流通したAntinnyウイルスにより、社団法人コンピュータソフトウェア著作権協会（ACCS）のホームページがDDoS攻撃を受ける。以降、同ウイルス感染によるWinny利用者からの情報漏えい事件が多発する。	マルウェア 大量通信 情報漏えい
2004年４月	Telecom-ISAC Japanにより、AntinnyウイルスによるACCSへのDDoS攻撃対策の試みが開始される。	大量通信
2004年５月	Winny作成者が著作権法違反幇助の疑いで逮捕される（2011年に無罪確定）。	著作権関連
2004年６月	**「児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律」改正。** 電磁的記録が対象となり、児童ポルノをインターネット上に流通させる行為及び提供の目的で児童ポルノを製造する行為が禁止される。	法整備
2004年７月	経済産業省より、脆弱性情報の公開に関して「ソフトウエア等脆弱性関連情報取扱基準」が告示され、脆弱性情報流通の枠組みとしてIPA、JPCERT/CCなどによる「情報セキュリティ早期警戒パートナーシップ」が開始される。	脆弱性対策
2004年11月	大手カード会社やポータルサイトを語ったフィッシングメールが発生する。	フィッシング
2004年12月	経済産業省による「フィッシング・メール対策連絡会議」が発足する。	フィッシング
2005年４月	フィッシング対策協議会が設立される。	フィッシング
2005年４月	**「個人情報保護法」施行。** 個人情報取扱事業者の定義と、事業者の義務が定められ、違反した場合の罰則などが定義される。	法整備
2006年２月	Telecom-ISAC JapanがISP会員企業の協力を得て、ACCSのホームページを攻撃しているAntinny感染ユーザに対してメールでの注意喚起を開始。	マルウェア
2006年３月	ファイル交換ソフトの利用による情報漏えい事件が頻発していることを受け、官房長官により「Winnyを使わないで」という発表が行われる。	情報漏えい
2006年11月	ファイル交換ソフトの利用などによる通信帯域の占有が顕著となっていることを受け、総務省による「ネットワークの中立性に関する懇談会」が設置される。	帯域制御
2006年11月	迷惑メール対策としてISPで利用されているOP25Bや送信ドメイン認証は正当業務行為にあたるという総務省の見解が発表される。	迷惑メール
2007年５月	Winnyを使った違法コンテンツ配信で3名が逮捕される。その後も逮捕者が続く。	著作権関連
2007年９月	電気通信事業関連4団体による「帯域制御の運用基準に関するガイドライン検討協議会」が発足する。	帯域制御
2008年１月	Winny上で流通するウイルス（原田ウイルスの亜種）の作成者が著作権法違反で逮捕される。	マルウェア
2008年３月	警察庁において、「Winny等ファイル共有ソフトを用いた著作権侵害問題とその対応策について」が発表される。	著作権関連
2008年５月	通信利用量による帯域制御の基準として「帯域制御の運用基準に関するガイドライン」が公表される。	帯域制御
2009年３月	警察庁において、「インターネット上での児童ポルノの流通に関する問題とその対策について」が発表される。	児童ポルノ
2010年１月	**「著作権法」改正。** Winnyなどのファイル共有ソフトを利用して違法に配信されている著作権侵害コンテンツのダウンロードなどが禁止となる。	法整備
2010年８月	イカタコウィルスが流行し、作成者が逮捕される。	マルウェア
2011年３月	インターネットコンテンツセーフティ協会が設立される。同４月よりインターネット上の児童ポルノブロッキングが開始となる。	児童ポルノ
2011年４月	警察庁において、「安全・安心で責任あるサイバー市民社会の実現に向けた対策について」が発表される。	不正アクセス
2011年６月	不正アクセス防止対策に関する官民意見集約委員会（官民ボード）が設置される。	不正アクセス
2011年７月	**「刑法」改正。** 不正指令電磁的記録に関する罪（ウイルス罪）が新設される。コンピュータウィルスの作成、供用、保管といった行為が禁止となる。	法整備
2011年８月	警察庁による「サイバーインテリジェンス情報共有ネットワーク」が設置される。	マルウェア 標的型攻撃
2011年９月	大手企業や官公庁などを標的とした標的型攻撃が発生する。	標的型攻撃
2011年10月	経済産業省主導による「サイバー情報共有イニシアティブ」が発足する。	不正アクセス
2012年５月	**「不正アクセス行為の禁止等に関する法律」改正。** フィッシングサイトの設置や不正な手段でのID/パスワード入手、保管などが禁止される。	法整備

ス[*45]や原田ウイルス[*46]といった、国産ウイルスが作成され、イカタコウイルス事件[*47]では実際に作成者が著作権侵害及び名誉棄損で逮捕されています。その後の本改正により、これらのコンピュータウイルスの作成、保管などが違法となりました。

これらに加え、今回新たな不正行為への対応の必要性から、不正アクセス禁止法が改正されましたので、次にその概要を説明します。

■ 不正アクセス禁止法

今回改正の対象となった「不正アクセス禁止法」は、ハイテク犯罪の防止や電気通信の秩序の維持といった目的により、2000年2月より施行された法律です。大きく分けると2つの骨子があり、1つは不正アクセス行為の禁止に関わるもの、もう1つは防御側の対策やその支援に関わるものです。ここでの不正アクセス行為とは、識別符号(IDやパスワード)で保護された電子計算機について、その保護を迂回して無断で利用する行為と考えることができます。主にインターネットなどを経由して、他人の識別符号(IDやパスワードなど)を悪用して無断で使用したり、システムの脆弱性を攻撃してコンピュータに侵入したりする行為が想定されています。

■ 今回の改正の経緯

インターネットは既に日常的に利用される便利なツールとなっている反面、犯罪行為も増加傾向にあることが統計的に公表されています。犯罪の内訳としては、アカウント情報の窃取が最も多く、平成23年度の不正アクセス手法では、「フィッシングサイトを使ったアカウント情報の窃取」、「ユーザIDやパスワードのブルートフォース攻撃、辞書攻撃」の2つで約半数を占めています[*48]。

不正アクセス禁止法が制定されてから、既に10年が経過しました。これらの事例を見ても分かるように、時代と共に犯罪の手法も変わってきています。従来の不正アクセス禁止法はフィッシングなどの新しい手口に対しては考慮されておらず、また、実際に不正アクセス行為が成功して初めて検挙可能となるなど、その効果に限界があることも分かってきました。そこで、警察庁の検討会である総合セキュリティ対策会議では、平成22年度報告書「安全・安心で責任あるサイバー市民社会の実現に向けた対策について」[*49]において、不正アクセス行為への今後の対策として、「基本的考え方」、「新たな手口への対応等」、「アクセス管理者による防御措置の向上等」、「官民の意見集約を通じた不正アクセス対策の検討・充実」などの提言を行いました。この提言を受ける形で、警察庁により官民の意見集約などが行われ、今回の不正アクセス禁止法が改正されました。

本改正の概要としては、他人のIDやパスワードを使用するだけでなく、無断で第三者に提供する行為も禁止されました。防御側の対策やその支援については、アクセス管理者による防御措置への支援、広報や啓発活動といった行政による努力義務が法律によって定められています。その他の変更としては、法定刑の引き上げが行われています。

■ 改正内容骨子

今回の不正アクセス禁止法の改正内容の骨子として注目すべき事項は、以下のとおりです。IDやパスワードの不正入手、フィッシングサイトや標的型メールの禁止といった内容と共に、官民連携に関する条文が加えられています。

- **他人の識別符号を不正に取得する行為の禁止(第四条)**
  不正アクセスに悪用する目的で、他人のIDやパスワードなどを不正な手段で取得する行為が禁止されています。例えば、アンダーグラウンドサイトなどで他人のIDやパスワードを購入する行為などがこれに該当します。
- **他人の識別符号を不正に保管する行為の禁止(第六条)**
  不正アクセスに悪用する目的で、他人のIDやパスワードなどを不正に保管する行為も、今回の改正で禁止さ

＊45 ファイル共有ネットワーク上で流行したトロイの木馬型ウイルス(http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=jp&name=TROJ_MELLPON.A)。
＊46 ファイル共有ネットワーク上で流行したウイルス。当時はIPAからも注意喚起が出ている。「コンピュータウイルス・不正アクセスの届出状況[1月分]について」(http://www.ipa.go.jp/security/txt/2008/02outline.html)。
＊47 原田ウイルスの作者が作成したウイルス。詳細については次のTrend Micro SECURITY BLOGも参照のこと。「年末年始におけるセキュリティ対策の再確認」(http://blog.trendmicro.co.jp/archives/3269)。
＊48 警察庁の統計は次のとおり、「平成23年中の不正アクセス行為の発生状況等の公表について[H24.3.15掲載]」(http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf)。
＊49 警察庁、「安全・安心で責任あるサイバー市民社会の実現に向けた対策について」(http://www.npa.go.jp/cyber/csmeeting/h22/pdf/pdf22.pdf)。

れました。例えば、他人のIDやパスワードを販売する目的で保管している場合などがこれに該当します。

- **識別符号の入力を不正に要求する行為の禁止（第七条）**
  今回の改正における大きなポイントですが、第七条の一号により、フィッシングサイトの開設が、第七条の二号により、フィッシングメールの送信が違法となりました。後者については一部の標的型攻撃メールの一部も対象となりえます。
- **都道府県公安委員会による援助など（第十条の二項）**
  改正前の不正アクセス禁止法にも普及啓発に関する条文がありましたが、本改正ではそれに加えて、民間の事業者団体などへの情報提供についての条文が追加されました。

それぞれの条文には、セキュリティ検査事業者やインターネット上のキャッシュなど、行為としては同様であっても、不正な意図がない場合は除外するよう記載されており、安全性の向上に寄与する行為などを阻害しないよう配慮されています。

■ まとめ

本改正によって、フィッシングや標的型攻撃メール、IDの売買などの行為が、違法行為となりました。本稿執筆時点では、改正不正アクセス禁止法の施行がされておらず、この法律がどのように運用されるのかは明らかになっていません。しかし、本改正によって、従来技術的な手法でのみ対策を行っていた行為のいくつかに、法執行機関による対策が実施可能となりました。IIJは今後もこのような法律の動向を注視すると共に、業界団体を通じた協力などで、安全なインターネット環境の提供に継続して努力して参ります。

1.4.2 DNS Changerマルウェア

DNS Changerは、TDL4やTDSS[*50]などと呼ばれるマルウェアの亜種です。2011年11月、このマルウェアのC&Cサーバやこのマルウェアの活動に関連する悪意のあるDNSサーバをFBIが差し押さえ、活動を封じ込めました[*51]。活動停止の時点では、この悪意のあるDNSサーバの代わりに、ISC社が正規のDNSサーバを運用することで、感染者のインターネットの利用が困難になることを防いでいました。これらのDNSサーバが2012年3月8日で運用期限を迎えるため、IIJ-SECTのブログであるSecurity Diaryでも注意喚起[*52]を行いました。そして、その後の続報[*53]でお伝えしたとおり、米国連邦裁判所が2012年7月9日（米国時間）までこのDNSの運用延長を決定[*54]しました。一方で、このマルウェアに感染した人は依然として対処が必要なことから、再度このレポートで事件の経緯を紹介すると共に注意喚起を行います。

■ 注意喚起の背景

FBIが差し押さえた時点で、DNS Changerは世界中で400万台以上の端末に感染していました。2012年2月に行われたNANOG 54において、ISC社が運用している正規DNSサーバが3月8日に終了することにより、感染したままの人がWeb閲覧やメールの送受信などのインターネットの利用ができなくなることについて話し合われました。DCWG（DNS Changer Working Group）[*55]が調査した結果、1月末時点で約45万の感染端末が存在していたことが確認されたことから、IIJでも緊急の注意喚起を行いました。

■ DNS Changerの概要

DNS Changerの被害は少なくとも1,400万ドルとも言われ、世界中に分散したC&Cサーバは100台以上存在していました。

マルウェアが名前解決の仕組みを悪用する行為や、通信内容を改ざんして表示する行為は以前から存在しています。例えば、MyDoomはhostsファイルを書き換えることでウイルス対策ソフトの動作を妨害したり、SpyEyeやZeuSなどは特定の金融機関のURLを表示する際、感染者のコンピュータ上のWebページにクレジットカード番号やパスワードの乱数表を入力させる項目を挿入することで、個人

＊50 DNS Changerは、これらの名称以外にもGhost ClickやZlob、Alureonなど様々な名称で知られている。
＊51 Operation Ghost Clickと呼ばれるその作戦の内容は次のURLが詳しい。"Operation Ghost Click International Cyber Ring That Infected Millions of Computers Dismantled"（http://www.fbi.gov/news/stories/2011/november/malware_110911）。
＊52 IIJ-SECT Security Diary、「DNS Changerマルウェア感染に関する注意喚起」（https://sect.iij.ad.jp/d/2012/02/245395.html）。
＊53 IIJ-SECT Security Diary、「DNS Changerマルウェア感染に関する注意喚起（続報）」（https://sect.iij.ad.jp/d/2012/03/074130.html）。
＊54 次のURLに7月9日にDNSが停止することが追記されている（http://www.fbi.gov/news/stories/2011/november/malware_110911）。
＊55 DCWG（DNS Changer Working Group）（http://www.dcwg.org/）。

情報を詐取します。しかし、今回のDNS Changerでは、悪意のあるDNSサーバを用意し、DNSサーバの設定を書き換えることで、通信を直接悪意のあるサーバに向けさせるという手法を利用しています。図-13は、DNS Changerに感染後、ネットワークの設定を表示させたものです。DNSサーバがFBIの資料[*56]が示すアドレスレンジに書き換えられていることが分かります。このようにDNSの設定変更はユーザから隠ぺいされておらず、感染端末の設定を確認すれば一目で分かります。一見、スマートな手法に見えませんが、非常に多くのユーザが感染したまま気づかなかったことから、結果的には非常に大きな影響を及ぼす手法であったと言えます。更にDNS Changerの犯罪組織はIT企業として運営され、ホスティング業者やレジストラとして登録されていた子会社も存在するなど、非常に大規模であったことも特徴の1つとして挙げられます[*57]。

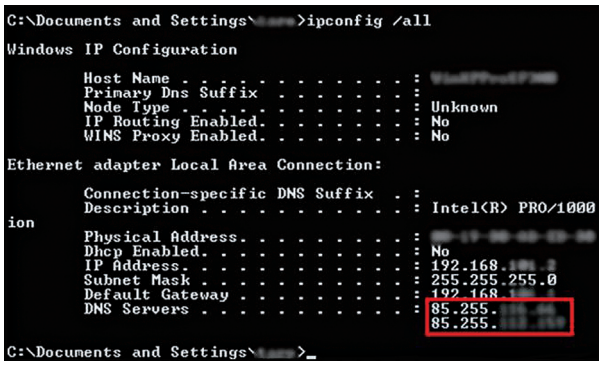
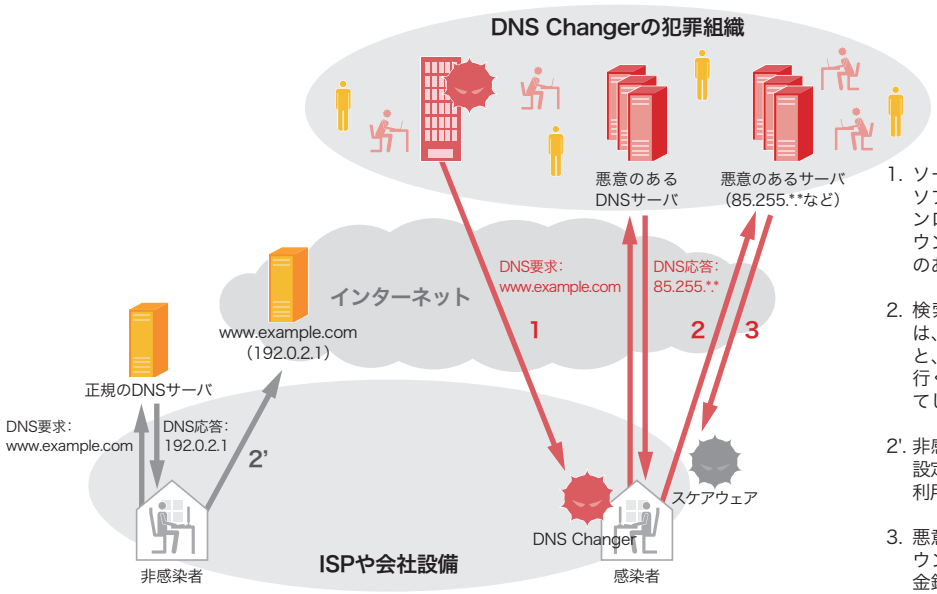


図-13 DNS Changer感染時のDNSの設定

図-14は、DNS Changerの概要を表した図です。DNS ChangerはWebサイトでのドライブバイダウンロードや、ビデオ再生ソフトウェアに偽装したものを、ソーシャルエンジニアリングによってユーザにダウンロードさせて実行させることで、感染者を増やしたと言われています[*58]。感染するとDNSの設定を外部の悪性サーバに書き換え、Webの検索結果をクリックジャッキングでねじ曲げたり、閲覧中のWebページ内の広告を別なものに置き換えて表示するなどの行為を行い、ユーザの金銭を詐取しようとし



1. ソーシャルエンジニアリング(動画再生ソフトウェアに偽装したファイルをダウンロードさせるなど)やドライブバイダウンロードで感染させ、DNS設定を悪意のあるサーバに書き換える。
2. 検索エンジンなど、特定のサイト(例では、www.example.com)にアクセスすると、悪意のあるDNSサーバに問い合せに行くため、悪意のあるサーバに誘導されてしまう。

2'. 非感染者の場合、ISPなどのDNSサーバが設定されて正常なDNSの応答が返るため、利用者の要求通りのサーバに接続される。

3. 悪意のあるサーバからスケアウェアをダウンロードさせるなどして、利用者から金銭を詐取する。

図-14 DNS Changerの概要

*56 DNS Changerが利用していた悪意のあるDNSサーバのアドレスレンジは、次の資料に記述されている。「DNSChanger Malware」(http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf)。

*57 Trend Micro社のブログでは、この件に関する詳細が記述されている。Trend Micro SECURITY BLOG、「明らかになった巨大ボットネットの正体 ー 史上最大規模のサイバー犯罪を摘発」(http://blog.trendmicro.co.jp/archives/4600)。

*58 マルウェアの感染経路については、FBIのプレスリリースの中に記述がある。"Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business" (http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business)。

ます。例えば、スパイウェアを駆除しようと検索をかけた場合、その検索結果を悪意のあるページへのリンクに置き換えて表示させることで、スケアウェア[*59](偽ウイルス対策ソフトウェア)をインストールさせて金銭を詐取するなどの被害が報告されています[*60]。

■ 多様な亜種

DNS Changerはそれ自身がTDL4やTDSSの亜種であり、挙動は多岐にわたっています。2005年から出現が確認されており[*61]、6年以上も活動をしていました。2008年にはDHCPサーバをエミュレーションすることで、ローカルネットワーク全体を乗っ取ろうとするタイプが出現したり[*62]、デフォルトパスワードのまま放置されているルータに侵入し、その設定を改変する亜種[*63]や、マスターブートレコードに悪性コードを保存する亜種が存在するとの報告や、Mac版も存在することが知られています。また、IIJが独自に入手した検体の中には、ウイルス対策ソフトによってDNS Changerと判定されていて、IIJの解析でもその他の挙動が似ていることが判明しているにも関わらず、DNSの設定を書き換えない検体も存在しました。これらはDNS Changerに似た特徴を持つマルウェア、またはTDL4やTDSSなどである可能性が高く、DNSの設定を確認しただけでは自分が感染者であることを見落とす可能性があります。

■ 対策

現在では、C&Cサーバが差し押さえられており、DNS Changerが自分自身をアップデートするなどの行為によって変化することはないため、様々なウイルス対策ソフトで検知できます[*64]。また、主要ウイルス対策ベンダ各社から駆除ツールがリリースされているので、それらを利用した確認もできます[*65]。

もし、2012年7月9日(米国時間)以降に急にWebページの閲覧ができない、メールの送受信ができないなどの症状が出た場合は、このマルウェアの感染を疑う必要があります。ただし、検出して正常に駆除できた場合でも、DNSの設定は書き換えられたままになっているため、ISPなどから提供されている情報を参考に、自分でDNSに関する再設定を行う必要があります。更に、前述のとおり、マスターブートレコードに悪性コードを保存する亜種があるため、駆除しても再起動に伴ってその領域からコードが復元され、再感染してしまう可能性もあります。この場合、復旧の際にはマスターブートレコードを上書きするか、ハードディスクをフォーマットした上で再インストールをするなどの対策が必要です。

また、こうしたマルウェアに感染しないために、Windows UpdateでOSを最新にする、ウイルス対策ソフトを導入し、常に最新のパターンファイルを適用する、Webブラウザのプラグインを最新にし、不要なソフトはすべて削除する、といったドライブバイダウンロード対策や、メールの添付ファイルやWebサイトやメール内のリンクを容易に開いたりしないといったソーシャルエンジニアリング対策を常に行っておくことが重要です。

1.4.3 Ghost Domain Names脆弱性について

■ Ghost Domain Namesとは

この脆弱性は、2012年2月8日に開催されたNDSS Symposium 2012[*66]において、Haixin Duan氏らによる論文「Ghost Domain Names: Revoked Yet Still Resolvable」として発表されました。この脆弱性は新しいタイプの脆弱性で、公開時点で多くのDNS実装が影響の対象でした。詳細については、同氏らのWebサイトに論文とプレゼンテーション資料

＊59 スケアウェアの解説は本レポートVol.3「1.4.3 スケアウェア」を参照のこと(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol03.pdf)。
＊60 GFIのblogでは、このデモを動画として公開している。「Movie Time: DNS Changer trojan」(http://www.gfi.com/blog/movie-time-dns-changer-trojan/)。
＊61 Trend Micro社やSymantec社のデータベースを確認すると、2005年から存在しているのが分かる。(http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=jp&name=TROJ_DNSCHANGE.A)、(http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2005-030413-5303-99)。
＊62 DHCPをシミュレートするDNS Changerは、SANSのblog ISC Diary「Rogue DHCP servers」(http://isc.sans.edu/diary.html?storyid=5434)やSymantec社のサイトで紹介されている。「Trojan.Flush.M」(http://www.symantec.com/security_response/writeup.jsp?docid=2008-120318-5914-99)。
＊63 NANOG 54(North American Network Operators' Group)のBoFの資料内では、UTSTARCOM、D-Link、Linksysなどが挙げられているが、この資料では実際に書きかえられた事例や、コード分析からは見つかっておらず、コンフィグ内に存在したという記述に止まっている。
＊64 ただし、他のマルウェアにも多重感染している場合も考えられるため、駆除にあたっては利用中のウイルス対策ソフトウェア製品の対応状況を確認した方がよい。またIIJでは未確認だが、ウイルス対策ソフトウェアの動作を妨害する検体も存在するようであり、その場合はインストールされているウィルス対策ソフトウェアでは検知できない可能性もある。
＊65 例えばKaspersky Lab社では、次のように駆除ツールと共に注意喚起を発行し、駆除の方法を詳細に解説している。Viruslist.com「【注意喚起】DNS Changer」(http://www.viruslistjp.com/analysis/?pubid=999999996)。
＊66 19th Annual Network & Distributed System Security Symposium(http://www.isoc.org/isoc/conferences/ndss/12/)。

が公開されています[*67]。また、JPRS社より本件の解説文章が日本語で公開されています[*68]。

この発表に先立つ2012年2月7日に、広く使われているDNSサーバソフトウェアであるBINDを開発しているISC社より、セキュリティアドバイザリが公開されましたが[*69]、ここでは脆弱性の詳細は公開されておらず、翌日の発表を待つ状態でした。発表後の2012年2月8日にISC社は影響を調査し、修正パッチの緊急リリースは実施しないと公表しました。この時点での修正は見送られましたが、その後の2012年4月5日にリリースされたバージョンで、他のバグ修正と合わせてこの脆弱性も修正されています。

■ ドメイン解決の流れ

DNSのドメインはルート(.)を最上位とした階層構造を取っており、名前解決時には上位から下位へ階層を辿る必要があります。これには異なるサーバへの複数回の問い合わせや、その状態の管理などの複雑な処理が要求されます。

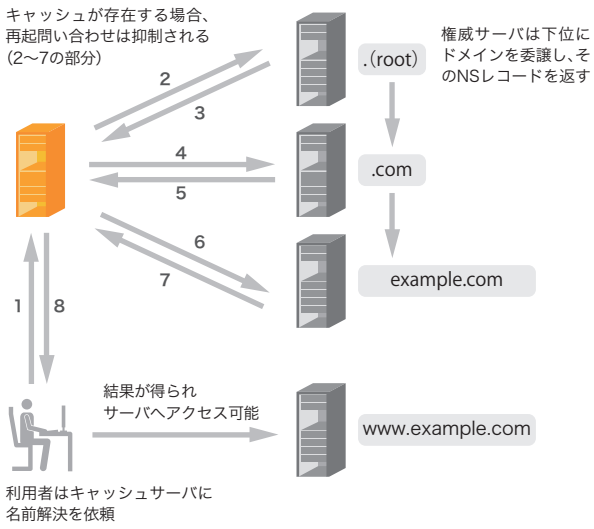


図-15 通常時の名前解決処理

各OSが標準で持っているDNSクライアントは、この様な複雑な処理をせずに、キャッシュDNSサーバに対して、目的とするドメイン名のみを問い合わせます。この様な動作をするDNSクライアントはスタブリゾルバと呼ばれています。OSや設定によってはレスポンス向上のために、得られた結果を更にキャッシュしている場合もあります。

一方、キャッシュDNSサーバはスタブリゾルバからの問い合わせを受けて、最上位のルートから階層を辿りながら目的とするドメインに至るまで名前解決を実施します。この様な動作をするDNSクライアントはフルサービスリゾルバと呼ばれています。これらの各DNSサーバ、DNSクライアントの関係を図-15に示します。

キャッシュDNSサーバはその名前のとおり、再帰問い合わせにて得られた結果や、その過程で得られた結果をキャッシュしています。これは権威DNSサーバやキャッシュ DNSサーバのトラフィック削減、クライアントのレスポンスの向上に非常に有効です。同じキャッシュDNSサーバを多数のユーザが使用すると、保持するキャッシュもそのユーザ間で共有されますので、頻繁にアクセスされるドメインは常にキャッシュされている状態となり、更に効果が上がります。

キャッシュの有効時間はTTLとして各レコードごとに定義されています。権威DNSサーバにて公開されている値が使われるため、ドメインの所有者がキャッシュの有効時間をある程度制御できます。キャッシュDNSサーバはこの値を元に、既に保持しているキャッシュを使用するかキャッシュが失効したとみなし、再度問い合わせるかを判定しています。

■ 今回の脆弱性の原因

今回の脆弱性はキャッシュDNSサーバにおける、上位ゾーンと下位ゾーンのNSレコードの扱いに起因しています。どちらも共に同じNSレコードですが、用途が異なっています。上位のNSレコードはあくまで下位へのドメイン委譲用であり、権威を持つのは移譲先である下位のNSレコードです。

＊67 "Ghost Domain Name : Revoked Yet Still Resolvable(in NDSS 2012)"(http://netsec.ccert.edu.cn/duanhx/archives/1313)。
＊68「ghost domain names(幽霊ドメイン名)脆弱性について」(http://jprs.jp/tech/notice/2012-02-17-ghost-domain-names.html)。
＊69 Internet Systems Consortium、"CVE-2012-1033 Ghost Domain Names : Revoked Yet Still Resolvable"(https://www.isc.org/software/bind/advisories/cve-2012-1033)。

これらの優先度はRFC 2181[*70]において規定されていますが、今回のような状態における動作は明記されていません。そのため、各DNSサーバソフトウェアの実装に依存する部分であり、多くの実装において、権威を持つ下位のゾーンに設定されているNSレコードをそのまま優先しています。

ゾーン自体のレコードとしては、下位が優先されるのはRFCとしては正しいですが、有効なNSレコードがキャッシュされている限り、同様にNSレコードに依存している委譲部分の確認も抑制されてしまうことから、今回の問題が発生しています。

特定の実装が仮にこの脆弱性の影響を受ける動作を行ったとしても、RFCで規定された動作に違反しているとは言えませんが、今回問題として認識されており、影響を受ける実装は今後修正されていくと推測されます。

■ 既知の攻撃との比較

特定のDNS実装のみ影響を受ける脆弱性は、年に数件程度見つかっています。多くのDNS実装が影響を受ける脆弱性は、2008年7月のDan Kaminsky氏による公開以来です。

Dan Kaminsky氏により公開された脆弱性[*71]は、キャッシュポイズニングが可能であり、悪意のある攻撃者が任意のドメインに任意のレコードを注入することが可能でした。この攻撃が成功すると、正規のドメインへのアクセスでありながら、悪意のあるサーバへと誘導されてしまいます。同じキャッシュDNSサーバを使用しているすべてのユーザが影響を受けるため、多くの利用者を抱えるサーバが狙われた場合の被害は甚大です。攻撃の容易さと成功時の影響の大きさもあり、公開時にはかなりの注目を浴びました。そして、根本的な対策方法として、DNSSECが注目を浴び、普及に向けた動きが加速しました[*72]。

今回の問題は、多くのDNS実装が影響を受ける点は同じでも、攻撃成功時の影響に大きな違いがあります。今回の脆弱性の影響は、自らが所有するドメインのキャッシュ失効阻害だけで、他人の所有するドメインへのキャッシュポイズニングなど悪意ある攻撃が可能なわけではありません。

通常、ドメインの所有者とドメインの設定者は同一であり、自らが所有するドメインのキャッシュの失効を阻害しても意味がありません。影響を受けるのは、所有者の意図に反して設定が変更される場合です。

該当するケースとして、法執行機関によるドメインの凍結が挙げられます。凍結時にはドメイン所有者の意図に関わらず、ドメインの委譲設定が強制的に変更、または取り消されます。どちらでもドメイン凍結として機能しますが、差し押さえの場合は、その旨を知らせるサーバへ誘導し、アクセスした利用者に対しても警告を促します。この時点で、既にドメイン所有者による設定変更は拒否されており、元に戻すことは不可能です。DNSの名前解決は階層構造であり、上位のドメインからの委譲を失ってしまえば、下位でどのような設定をしていても意味がありません。そのため、ドメインの委譲情報の変更が、ドメインの凍結において強制力を持ちます。これを示したのが図-16です。

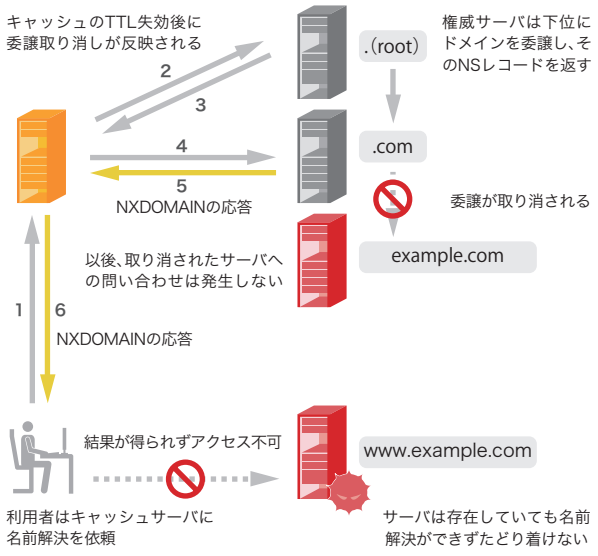


図-16 ドメイン凍結時の名前解決処理

＊70 IETF、"RFC 2181 Clarifications to the DNS Specification"(http://www.ietf.org/rfc/rfc2181.txt)。
＊71 本レポートVol.2「1.4.1 DNSキャッシュポイズニング」にて紹介している(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol02.pdf)。
＊72 ICANN Research、"TLD DNSSEC Report"(http://stats.research.icann.org/dns/tld_report/)。

通常であれば、キャッシュDNSサーバは該当ドメインのTTL満了を経て新しい委譲情報を権威DNSサーバから再取得し、その時点でキャッシュDNSサーバ上の委譲情報が更新されます。しかし、凍結されたドメインの所有者が今回の脆弱性を利用すると、キャッシュ DNSサーバに新しい委譲情報を取得させることなく、古い委譲情報を維持させられます。この流れを示したのが図-17です。

今回の攻撃方法は、キャッシュの更新の仕組みに依存しており、攻撃成立にはキャッシュDNSサーバがドメインの凍結前の委譲情報をキャッシュとして持ち続けている必要があります。ドメインの凍結後に起動したサーバ、再起動などの要因によりキャッシュが消滅したサーバは、既に新しい委譲情報をキャッシュとして保持しており、攻撃は成立しません。

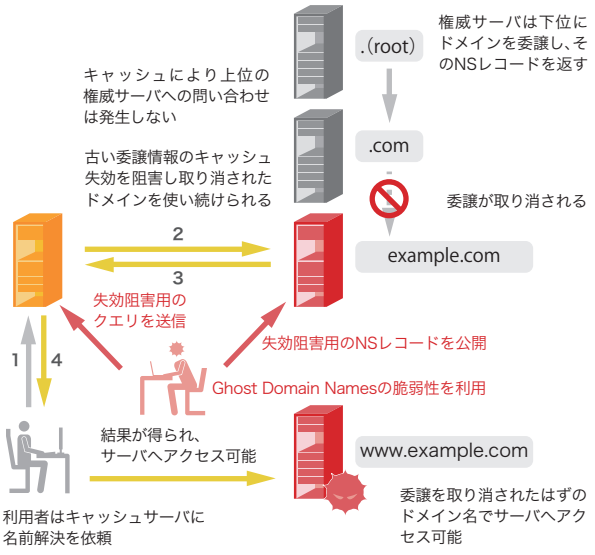


図-17 ドメイン凍結時の名前解決処理(Ghost Domain Names)

■ まとめ

今回の件が、多くのDNS実装が影響を受けたにも関わらず、あまり大きな騒ぎにならなかったのは、この脆弱性を悪用した際の影響範囲が小さいことによるものと考えられます。しかし、この手法で削除されたはずのドメインが存在する状況が発生した場合には、利用者側のシステムや注意のみでは影響を回避できません。このため、たとえ限定的な影響であったとしても、DNSにより利用者が意図しない通信を引き起こすことがないように、DNSの実装や運用を強化していく必要があります。

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、不正アクセス禁止法の改正についてと、利用者の参照するDNS設定を書き換えるDNS Changerマルウェア及びDNSサーバの脆弱性として報じられたGhost Domain Nameの問題について解説しました。

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。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続して参ります。

執筆者:
齋藤 衛(さいとう まもる)
IIJ サービスオペレーション本部 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などに従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECT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など、複数の団体の運営委員を務める。

土屋 博英、根岸 征史(1.2 インシデントサマリ)
土屋 博英、鈴木 博志、小林 直(1.3 インシデントサーベイ)
加藤 雅彦、齋藤 衛(1.4.1 不正アクセス禁止法改正について)
鈴木 博志(1.4.2 DNS Changerマルウェア)
小林 直(1.4.3 Ghost Domain Names脆弱性について)
IIJ サービスオペレーション本部 セキュリティ情報統括室

協力:
須賀 祐治、桃井 康成、吉川 弘晃、齋藤 聖悟、春山 敬宏 IIJ サービスオペレーション本部 セキュリティ情報統括室