韓国で発生した3.20大乱

**今回は、3月に韓国で発生した大規模インシデントを紹介すると共に、
国内で発生したApacheのモジュール改ざんによるマルウェア感染事件、
及びサイバー攻撃に対応するための演習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2013年1月から3月までの期間では、前回の期間に続いてAnonymousなどのHacktivismによる攻撃が複数発生しています。また、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、いくつかの攻撃については報告書にまとめられて公開されました。3月には韓国でマルウェアを用いた大規模な攻撃が発生し、ヨーロッパでは通信量が300Gbpsに達したといわれる大規模なDDoS攻撃が発生しました。国内では遠隔操作ウイルスの犯人によるメッセージが複数回公開され、2月には容疑者が逮捕されています。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。

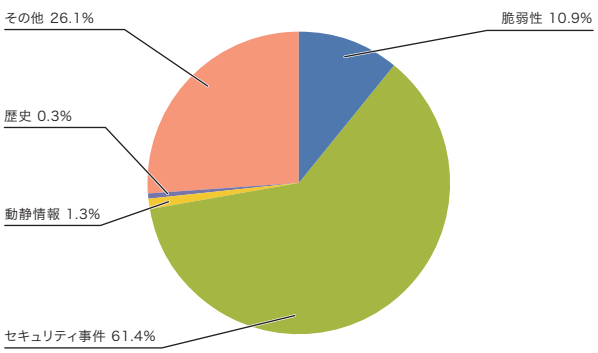


図-1 カテゴリ別比率(2013年1月～3月)

1.2 インシデントサマリ

ここでは、2013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]。

■ 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、多数の国の企業及び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。目立った攻撃としては、イスラエル政府関連サイトへの攻撃(#OpIsrael)や、それに対する報復と見られるイスラエル側からパレスチナへの攻撃が発生しています。エジプト(#OpEgypt)やその他の国の政府機関などに対しても継続して攻撃が行われました。

1月にはマサチューセッツ工科大学(MIT)に侵入し、学術論文のデータを盗んだとして起訴されていたインターネット活動家が自殺したことに関連し、MITへのDDoS攻撃やWebサイトの改ざんなどが行われました。更に、関連して米国の量刑委員会など複数のWebサイトに対して改ざんなどを実施しています。また、不正アクセスにより取得したと思われる情報を暗号化したファイルを公開したり、米銀行関係者の個人情報を公開するなど(#OpLastResort)、引き続き活発な活動を行っています。

TeamGhostShellによって、アフリカの複数の大学や政府機関、民間企業のサーバへ不正アクセスが行われ、70万件のアカウント情報が公開(#ProjectSunRise)されまし

*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。

た。3月には昨年から断続的に実施されている米銀行へのDDoS攻撃(Operation Ababil)の第3弾が開始するなど、Anonymous以外のグループによる活動も継続しています。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2][*3][*4][*5][*6]、Internet Explorer[*7][*8][*9]などで修正が行われました。Adobe社の Adobe FlashPlayer、Adobe Reader及びAcrobatなどでも修正が行われました。Oracle社のJavaでも定例外を含む複数の更新が行われ、多くの脆弱性が修正されています。また、官公庁などでよく利用されているジャストシステム社の一太郎や花子では、悪意あるプログラムを実行可能な脆弱性が見つかり、修正されました。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、多くの脆弱性が修正されました。また、DNSサーバのBIND9では大量のメモリ消費により、サーバの異常停止などを引き起こす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、パラメータ解析処理において、第三者によって認証が回避されたり、任意のコードが実行されたり、任意のSQLコマンドが実行されたりするなどの可能性がある複数の脆弱性が見つかり修正されています。

更に、数多くのネットワーク機器で利用されているUPnP(Universal Plug and Play)のライブラリに、SSDPリクエスト処理でバッファオーバーフローが可能な脆弱性が複数見つかり修正されています。これについては、家庭用のブロードバンドルータやWebカメラ、IP電話機器など多数の機器で利用されているため、米国のセキュリティ企業であるRapid7社から、UPnPによるセキュリティ上の問題や懸念事項をまとめたホワイトペーパーが公表されました[*10]。更に、ベンダーから修正が行われない、また、修正が出ていてもユーザが適用していないケースが数多くあるとして、JPCERT コーディネーションセンターなどからも注意喚起が行われています[*11]。

■ DNSのopen resolverを悪用したDDoS攻撃

3月には、迷惑メール対策組織であるSpamhausに対する大規模なDDoS攻撃が発生しました。この攻撃は当初、SpamhausのWebサイトや、その攻撃の対策に当たっていたCloudFlare社の設備に向けられていましたが、最終的には同社の接続するインターネットエクスチェンジの設備に向けられるなど、攻撃先を変えながら6日間継続しました。

この攻撃では、DNSアンプ攻撃が使われたとされています。DNSアンプ攻撃では、多くの情報量を持つDNSの応答を誘発するDNSのクエリを、攻撃先のIPアドレスに詐称した発信元から多数発することにより、攻撃先に多くの情報を送付します。この際、攻撃者の正体を隠すと共に、攻撃を受けた側から見ると、世界中から攻撃されているように

---

*2 「マイクロソフト セキュリティ情報 MS13-002 - 緊急 XML Core Services の脆弱性により、リモートでコードが実行される (2756145)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-002)。

*3 「マイクロソフト セキュリティ情報 MS13-010 - 緊急 Vector Markup Language の脆弱性により、リモートでコードが実行される (2797052)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-010)。

*4 「マイクロソフト セキュリティ情報 MS13-020 - 緊急 OLE オートメーションの脆弱性により、リモートでコードが実行される (2802968)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-020)。

*5 「マイクロソフト セキュリティ情報 MS13-022 - 緊急 Silverlight の脆弱性により、リモートでコードが実行される (2814124)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-022)。

*6 「マイクロソフト セキュリティ情報 MS13-027 - 重要 カーネルモード ドライバーの脆弱性により、特権の昇格が起こる (2807986)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-027)。

*7 「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)」(https://technet.microsoft.com/ja-jp/security/bulletin/ms13-008)。定例外

*8 「マイクロソフト セキュリティ情報 MS13-009 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2792100)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-009)。

*9 「マイクロソフト セキュリティ情報 MS13-021 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2809289)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-021)。

*10 US-CERT、"Vulnerability Note VU#922681 Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP"(http://www.kb.cert.org/vuls/id/922681)。

*11 「JPCERT/CC Alert 2013-01-31 Portable SDK for UPnP の脆弱性に関する注意喚起」(http://www.jpcert.or.jp/at/2013/at130006.html)。

1月のインシデント

1
- セ **1日**：農林水産省で、昨年ウイルス感染事案が発生し、これにより、複数の機密情報が外部に漏えいしていた可能性が報道された。
- セ **1日**：遠隔操作ウイルス事件の犯人と思われる人物からのメッセージが、複数の報道機関や記者にメールで送信された。

2

3
4
- セ **4日**：トルコの認証局であるTURKTRUSTが不正な中間証明書を発行していたことによる不正なデジタル証明書が12月に発見され、これらの証明書を無効とする対応を取ったことが各社から公表された。
  詳細については、例えば次のGoogle Online Security Blogなどを参照のこと。"Enhancing digital certificate security"（http://googleonlinesecurity.blogspot.jp/2013/01/enhancing-digital-certificate-security.html）。

5
- セ **5日**：再び遠隔操作ウイルス事件の犯人と思われる人物からのメッセージが、複数の報道機関や記者にメールで送信された。

6
- 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。
  「APSB13-01:Flash Playerに関するセキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-01.html）。

7
- 脆 **9日**：Adobe ReaderおよびAcrobatに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
  「APSB13-02: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/apsb13-02.html）。

8
9
- 脆 **9日**：Ruby on RailsのAction Packにパラメータ解析処理に任意のコードを実行される複数の脆弱性（CVE-2013-0156）が見つかり、修正された。
  JVN、「JVNDB-2013-001019 Ruby on Rails に複数の脆弱性」（http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001019.html）。
- 脆 **9日**：Microsoft社は、2013年1月のセキュリティ情報を公開し、2件の緊急と5件の重要な更新をリリースした。
  「2013 年 1 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-jan）。

10
- セ **9日**：MoinMoinに複数の既知の脆弱性があり、これを悪用してDebianとPythonの公式wikiサーバが侵入される事件が発生した。
  例えば、Debianでは次のアナウンスを公表している。"wiki.debian.org security breach"（http://lists.debian.org/debian-devel-announce/2013/01/msg00000.html）。

11

12
13
- 脆 **14日**：Oracle社は、1月11日に公表された任意のコードが実行可能な未修正の脆弱性について、Java SE JDK及びJREの定例外アップデートを公開した。
  "Oracle Security Alert for CVE-2013-0422"（http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html）。

14
- セ **14日**：Anonymousによると考えられる、MITへのDoS攻撃や複数のWebサイトの改ざんが発生した。
  The Tech、"Anonymous hacks MIT"（http://tech.mit.edu/V132/N61/anonymous.html）。

15
- 脆 **15日**：Microsoft社は、Internet Explorer 6～8で公表されていた不正終了やリモートで任意のコード実行が可能な脆弱性について、定例外の修正を公開した。
  「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）。

16

17
- 脆 **16日**：Oracle社は四半期ごとの定例アップデートを公開し、OracleやMySQLなど複数製品の合計86件の脆弱性が修正された。
  "Oracle Critical Patch Update Advisory - January 2013"（http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html）。

18
- 他 **18日**：一般社団法人データ通信協会 テレコムアイザック推進会議（Telecom-ISAC Japan）の主催により、電気通信事業者や重要インフラ事業者などが参加するサイバー攻撃対応演習が行われた。

19

20
21
- 脆 **24日**：Barracuda Networks社の複数のアプライアンスに、サポートに利用されている公開されていないアカウントがあることが公表された。また、特定のIPアドレスレンジからSSHなどにより、これらのアカウントを利用してログインが可能であることも判明した。
  「バラクーダネットワークス製品におけるリモートアクセスの脆弱性について」（http://www.barracuda.co.jp/column/20130206）。

22
- セ **25日**：トルクメニスタンのccTLDレジストリであるnic.tmで、管理画面にあったSQLインジェクションの脆弱性によるドメインハイジャックが発生した。

23
- 他 **25日**：US-CERTより、適切なアップデートをされていないCMSを悪用したDDoS攻撃が発生しているとして注意喚起が行われた。
  "Alert (TA13-024A) Content Management Systems Security and Associated Risks"（http://www.us-cert.gov/cas/techalerts/TA13-024A.html）。

24
- セ **26日**：Anonymousにより、Operation Last Resortが実施され、米国連邦量刑委員会（www.ussc.gov）のWebサイトが改ざんされた。

25

26
- セ **28日**：スリランカのccTLDレジストリであるnic.lkで、管理画面にSQLインジェクションの脆弱性があり、メールアドレスなど約1万件のアカウント情報が漏えいした。

27
- セ **29日**：Twitter社は、2012年7月から12月までの各国の政府機関などからのユーザ情報の開示請求などの状況をまとめたTransparency Reportを公開した。
  "Twitter Transparency Report v2"（http://blog.twitter.com/2013/01/twitter-transparency-report-v2.html）。

28
29
- 脆 **30日**：Portable SDK for UPnPの関数に細工されたSSDPリクエストを処理することにより、任意のコードが実行される可能性のある脆弱性が複数の製品に見つかり、修正された。
  JVN、「JVNVU#90348117 Portable SDK for UPnP にバッファオーバーフローの脆弱性」（https://jvn.jp/cert/JVNVU90348117/index.html）。

30

31
- 他 **31日**：IPAより、クラウドの停止のリスクと、その回避のための方策を検討し取りまとめた報告書が公開された。
  「『社会インフラとしてのクラウドに求められる信頼性とサービス継続のための条件について』レポート～クラウドの停止リスクの回避及びデータセンター間の移転等の課題に関する整理と提起～」（http://www.ipa.go.jp/about/technicalwatch/20130131.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

見える効果を狙って、インターネット上から利用可能になっている参照用DNSサーバを踏み台にしたとされています。このため、公開されている参照用DNSサーバは今後もDNSアンプ攻撃に利用される可能性があるとして、US-CERTから設定の見直しなどを促す注意喚起が行われています。

また、このような参照用DNSサーバの機能は、一般のISPなどが用意するDNSサーバだけではなく、個人が利用しているブロードバンドルータなどのネットワーク機器の機能として提供されている場合があります。設定によってはこのような機器も攻撃に利用されることから、Open DNS Resolver Project[*12]やJPCERT/CC[*13]、JPRS[*14]などから、参照用DNSサーバがインターネット側から勝手に利用されないかどうかを確認するように、注意喚起が行われています。

ここで、図-2に、本期間中にハニーポットに到着した53/UDP通信の発信元IPアドレスの国別分類を示します。Spamhausへの攻撃は、3月18日から22日ごろにかけて行われたと報告されていますが、その期間攻撃に合致するような通信は検出されませんでした。しかし、3月15日から18日にかけてカナダのIPアドレスからの通信が急増していることが確認できます。この通信は、カナダの特定の事業者の2つのIPアドレスからに見えるものですが、到着した通信の内容から、この2つのIPアドレスを狙ったDNSアンプ攻撃の試みであることがわかっています。このようにDNSアンプ攻撃は他の攻撃先についても実際に発生しており、十分な注意が必要な状況です。

■ 政府機関への攻撃とウイルス感染事案

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。1月には農林水産省で職員の端末がコンピュータウイルスに感染し、複数の機密情報が外部に漏えいした可能性があることが報道されました。この事件は発生してからある程度の時間が経過していますが、情報流出の可能性があることから、情報セキュリティの専門家などの外部有識者による調査委員会が設置され、調査が行われています[*15]。外務省でも同様に、省内のパソコンからインターネット上の外部サーバへの不審な通信が確認されたとして、外部専門家を交え、当該情報流出の詳細を分析することが発表されています。このうち外務省の事案では、内閣官房情報セキュリティセンター（NISC）からの情報提供を受けて調査が行われました。

2012年11月に発生した、宇宙航空研究開発機構（JAXA）で職員の端末がウイルスに感染し、ロケット関連の情報が外部に漏えいした可能性がある事案について、調査結果が公表されました。この中では、感染経路がなりすましメールからであることや、外部の不正サイトへの通信は、2011年3月17日から2012年11月21日まで行われていたことなどが報告されています。また、感染した端末では、感染期間中には機微な情報を扱っていなかったとしています。

また、メールのなりすましやWebサイトの改ざんも複数発生しており、防衛省職員になりすましたメールに対する

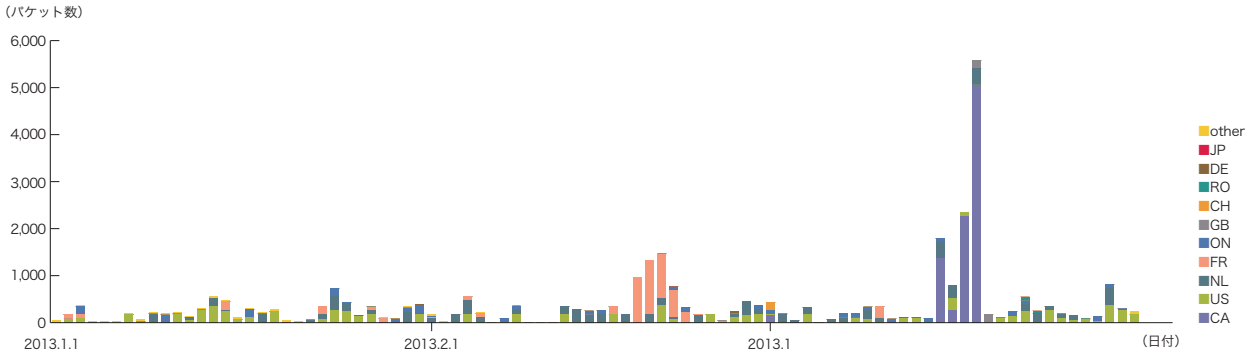


図-2 ハニーポットに到着した53/UDPの通信の推移（日別・国別）

＊12 Open DNS Resolver Project（http://openresolverproject.org）。
＊13 JPCERT/CC、「JPCERT/CC Alert 2013-04-18 DNS の再帰的な問い合わせを使った DDoS攻撃に関する注意喚起」（http://www.jpcert.or.jp/at/2013/at130022.html）。
＊14 JPRS、「DNSサーバーの不適切な設定『オープンリゾルバー』について」（http://jprs.jp/important/2013/130418.html）。
＊15 農林水産省、「農林水産省へのサイバー攻撃に関する調査委員会の設置及び第1回委員会の開催について」（http://www.maff.go.jp/j/press/kanbo/hisyo/130111.html）。

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

脆 **2日**：Oracle社は、未修正の脆弱性を狙う攻撃が観測されているとして、Java SE JDK及びJREの定例外アップデートを公開し、合計50件の脆弱性を修正した。
"Oracle Java SE Critical Patch Update Advisory - February 2013"（http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html）。

セ **2日**：Twitter社は、不正なアクセスにより約25万人のユーザ情報にアクセスされた可能性があるとして、該当アカウントのパスワードを強制リセットする対応を実施したと発表した。
「より安全にご利用いただくために」（http://blog.jp.twitter.com/2013/02/blog-post.html）。

セ **4日**：ライバル社に不正アクセスして営業秘密を取得したなどとして、不正アクセス禁止法違反と不正競争防止法違反（営業秘密侵害）の疑いで容疑者が福岡県警に逮捕された。

セ **5日**："Google Chromeなどで広告配信サービス会社からの広告配信を受けている大手メディアサイトへのアクセスがブロックされる事象が発生した。これは広告配信サービス会社がマルウェアに感染したために、ブラックリストに登録されたことによる。
例えば、次のKaspersky Lab社のThreatpostなどを参照のこと。"Google Blocks High Profile Sites After Advertising Provider NetSeer is Hacked"（http://threatpost.com/en_us/blogs/google-blocks-sites-after-advertising-provider-netseer-hacked-020413）。

セ **5日**：外務省は、省内のPCがウイルスに感染し、インターネット上の外部サーバへ約20通の文書が流出した疑いがあることを公表した。
「外務省ネットワークから外部への情報流出」（http://www.mofa.go.jp/mofaj/press/release/25/2/0205_07.html）。

他 **6日**：米国のWebサービス事業者に対し、名誉毀損行為を行ったとみられるユーザの発信者情報を開示するように命ずる仮処分が東京地裁で決定された。2011年に民事訴訟法が改正され、日本において事業を行っていると認められる外国法人に対する適用が可能となったことによる。

セ **7日**："Microsoft社のマイクロソフトデジタルクライムユニット（DCU）とSymantec社は、共同でBamitalボットネットのテイクダウンを実施したことを公表した。
The Official Microsoft Blog,"Microsoft and Symantec Take Down Bamital Botnet That Hijacks Online Searches"（http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx）。

他 **8日**：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-04:Flash Playerに関するセキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-04.html）。

セ **10日**：遠隔操作ウイルス事件の容疑者が、威力業務妨害容疑で逮捕された。

セ **12日**：マラウィ（.mw）のccTLDレジストリが、何者かにドメインハイジャックされる事件が発生した。

脆 **13日**：Microsoft社は、2013年2月のセキュリティ情報を公開し、MS13-009やMS13-010などを含む5件の緊急と7件の重要な更新をリリースした。
「2013 年 2 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-feb）。

脆 **13日**：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-05:Flash Playerに関するセキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-05.html）。

他 **18日**：OXFORD大学はGoogle Docsを悪用したフィッシングの増加への対策として、Google Docsへのアクセスを一時遮断した。この対応による利用者への影響が大きかったことから、この措置は数時間で解除された。
詳細については次のOxCERT's blogに詳しい、"Google Blocks"（http://blogs.oucs.ox.ac.uk/oxcert/2013/02/18/google-blocks/）。

他 **18日**：CERT Australiaは、企業へのアンケートを基に、2012年のサイバー攻撃や犯罪などのインシデントをまとめた年次報告書を公表した。この中では、回答した企業の44%で自組織内からの攻撃を経験しているなどの結果がまとめられている。
"The Cyber Crime and Security Survey Report"（https://www.cert.gov.au/system/files/608/673/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf）。

セ **19日**：宇宙航空研究開発機構（JAXA）は、昨年11月のウイルス感染についての調査結果を公表した。感染の原因は東日本大震災に関連したなりすましメールの添付ファイルを開いたことが原因としている。
「JAXAにおけるコンピュータウィルス感染に関する調査結果について」（http://www.jaxa.jp/press/2013/02/20130219_security_j.html）。

脆 **20日**：Oracle社は、Java SE JDK及びJREの定例アップデートを公開し、合計5件の脆弱性を修正した。
"Updated Release of the February 2013 Oracle Java SE Critical Patch Update"（http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html）。

セ **20日**：.eduドメインのレジストリであるEDUCAUSEが不正なアクセスにより、約9万人のユーザ情報と7000の.eduドメイン所有者の情報が漏えいした可能性があることを公表した。
"EDUCAUSE SECURITY BREACH AND PASSWORD CHANGE INFORMATION"（http://www.educause.edu/educause-security-breach-and-password-change-information）。

他 **20日**：Mandiant社から、米国企業および組織を狙って数年間にわたり行われていた一連の攻撃に関する詳細な報告書が公表された。
"APT1: Exposing One of China's Cyber Espionage Units"（http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf）。

脆 **21日**：Adobe Reader及びAcrobatに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-07: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/apsb13-07.html）。

セ **22日**：Twitter社がフィッシング対策としてDMARC（Domain-based Message Authentication, Reporting and Conformance）の利用を公表した。
Twitterブログ、「少しでも安心なサービスに」（http://blog.jp.twitter.com/2013/02/blog-post_25.html）。

脆 **26日**：ジャストシステム社の一太郎と花子に、任意のコードが実行される可能性のある脆弱性が見つかり、修正された。
「[JS13001] 一太郎・花子の脆弱性を悪用した不正なプログラムの実行危険性について」（http://www.justsystems.com/jp/info/js13001.html?m=jui26j03）。

脆 **27日**：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-08:Flash Playerに関するセキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-08.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

注意喚起が行われたり[*16]、環境省[*17]や農業環境技術研究所[*18]が運営するWebサイト、高エネルギー加速器研究機構(KEK)[*19]、複数の地方公共団体のWebサイトが改ざんされました。このうち、いくつかの事件では改ざんされたWebサイトを踏み台とした攻撃やマルウェア感染サイトへの誘導などが行われていました。

■ CMSやWebサーバへの攻撃

この期間では、CMS(Content Management System)への攻撃についても話題となりました。1月にはUS-CERTより、CMSの利用に関する注意喚起が行われました。この中では、特にオープンソースのCMSであるJoomla!に対する攻撃が行われており、侵入されたサーバが重要インフラ企業などへのDDoS攻撃に悪用されているとして、ソフトウェアを更新するなど、適切な管理を行うよう求めています。

また、Webサーバ(Apache)の不正モジュールを使った改ざん被害も報告されており、日本でもWebサーバ上に不正なApacheモジュールが設置され、Webサイト閲覧時に意図しないJavaScriptが挿入される事例が多く発生しました。ユーザが改ざんされたWebサイトを閲覧すると、別の不正なWebサイトに誘導され、マルウエアに感染する可能性がありました。改ざんされたWebサイトでは、サポート期限切れのバージョンを含む、古いバージョンのサーバ管理ツールが多く使われていたとして、JPCERTコーディネーションセンターから注意喚起が行われています[*20]。この問題の詳細については「1.4.2 日本国内のWebサイト改ざんとドライブバイダウンロード」も併せてご参照ください。

■ TLDへの攻撃

ccTLDを含むドメインレジストリに対しての攻撃と、それによるドメインハイジャックや情報の漏えいも継続して発生しています。1月にはトルクメニスタンのドメインである.tmを管理しているnic.tmがSQLインジェクション攻撃を受け、ドメインハイジャックされる事件が発生しました。スリランカのドメインである.lkを管理しているLK Domain Registryでも、SQLインジェクション攻撃によって1万件のアカウント情報の漏えいが発生しました。2月にはマラウィのドメインである.mwで、ドメインハイジャックが発生しています。同じく2月にはパキスタンのドメインである.pkを管理しているPKNICのサーバが侵入され、ドメインハイジャックされる事件が発生しています。.pkについては2012年11月にも同様の事件が発生してます。いずれの事件においてもドメインハイジャックされた場合には、GoogleやPayPalなど世界的な企業のその地域におけるドメインが狙われました。

■ 機密情報を狙う標的型攻撃

2月には米国のセキュリティ会社であるMandiant社から、米国企業および組織を対象に、数年間にわたって行われていた標的型攻撃に関する詳細な報告書が公表されました。また、これと前後して、Facebook[*21]やMicrosoft[*22]など複数の企業から攻撃を受けていたことが相次いで公表されています。このように、米国の政府機関や民間企業に対して悪意のある活動が見られるとして、US-CERTから注意喚起が行われました[*23]。こうした活動は、米国だけでなくEUの防衛産業でも報告されており、日本でも2011年に複数の省庁や民間企業に対する攻撃が話題となって以来、継続的に発生しています。これらの事件では、防衛産業や政府機関だけでなく一般企業の機密情報も狙われており、このような攻撃は、今後も継続して発生すると考えられます。

■ 遠隔操作ウイルス

この期間では、昨年の10月より話題となった遠隔操作ウイルスに関連する一連の事件も話題となりました。1月には、1日と5日の2回に渡り、真犯人と思われる人物からのクイ

＊16 防衛省、「防衛省の職員を詐称する「なりすましメール」に御注意ください。」(http://www.mod.go.jp/j/approach/others/security/narisumashi.html)。
＊17 環境省、「(お知らせ)『CO2みえ〜るツール』サイトの改ざんについて」(http://www.env.go.jp/info/mieeeru.pdf)。
＊18 独立行政法人農業環境技術研究所、「農業環境技術研究所Webサイトへの不正アクセスについて」(http://www.niaes.affrc.go.jp/techdoc/press/130122/press130122.html)。
＊19 大学共同利用機関法人　高エネルギー加速器研究機構、「KEK素粒子原子核研究所・理論センター ウェブサイトの改ざんについて」(http://www.kek.jp/ja/NewsRoom/Release/20130321220000/)。
＊20 JPCERTコーディネーションセンター、「旧バージョンの Parallels Plesk Panel の利用に関する注意喚起」(http://www.jpcert.or.jp/at/2013/at130018.html)。
＊21 Facebook、"Protecting People On Facebook"(https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766)。
＊22 Microsoft Security Response Center、"Recent Cyberattacks"(http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx)。
＊23 US-CERT、"UPDATE: Ongoing Malicious Cyber Activity Against U.S. Government and Private Sector Entities"(http://www.us-cert.gov/ncas/current-activity/2013/02/22/Ongoing-Malicious-Cyber-Activity-Against-US-Government-and-Private)。

3月のインシデント

1 他 **1日**：総務省及び経済産業省より、平成15年に策定された「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)」の改定が行われ、公表された。
CRYPTREC、「CRYPTREC暗号リスト（電子政府推奨暗号リスト）」(http://www.cryptrec.go.jp/list.html)。

2

3 セ **3日**：Evernote社は、不正アクセスにより、ユーザ情報にアクセスされたため、全ユーザのパスワードを再設定したことを公表した。
「セキュリティ関連のお知らせ：Evernoteでのパスワード再設定のお願い」(http://blog.evernote.com/jp/2013/03/03/12428)。

4

5 脆 **5日**：Oracle社は、Java SE JDK及びJREの定例外アップデートを公開し、任意のコード実行が可能な脆弱性(CVE-2013-1493)など複数の脆弱性を修正した。
"Oracle Security Alert for CVE-2013-1493"(http://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html)。

セ **5日**：Google Chromeなどの複数のブラウザで、国内の複数のサイトへのアクセスがGoogle SafeBrowsingによりブロックされる事象が発生した。

6

7 他 **8日**：JPCERTコーディネーションセンターは、制御システムのセキュリティ上の脅威、対策情報の流通などを図るため、情報共有ポータルサイト「ConPaS(Control System Security Partner's Site)」を開設したことを発表した。
「制御システムセキュリティ情報共有ポータルサイトについて」(http://www.jpcert.or.jp/ics/conpas/index.html)。

8

9 セ **9日**：米国の国立標準技術研究所(NIST)の脆弱性情報データベース(National Vulnerability Database)などが、Webサーバの脆弱性によるマルウェア感染のため停止した。
この事件については例えば次のセキュリティ専門家のGoogle+への投稿などを参照のこと。Kim Halavakoski、"http://nvd.nist.gov/ hacked. Site down since March 8..."(https://plus.google.com/u/0/106350285372295328202/posts/HNayDzUoYEz)。

10

11

12 他 **12日**：IPAより、「2013年版 10大脅威　身近に忍び寄る脅威」が公表された。
「『2013年版 10大脅威　身近に忍び寄る脅威』を公開」(http://www.ipa.go.jp/about/press/20130312_2.html)。

13 脆 **13日**：Microsoft社は、2013年3月のセキュリティ情報を公開し、MS13-021などを含む4件の緊急と3件の重要な更新をリリースした。
「2013 年 3 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-mar)。

14 脆 **13日**：Adobe Flash Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-09:Flash Playerに関するセキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb13-09.html)。

15

16 セ **15日**：国内の複数のWebサイトで不正なApacheモジュールを設置される改ざんが行われ、攻撃に悪用されていることが報告された。この事件に関連して、改ざんされたサイトの多くが旧バージョンのParallels Plesk Panelを利用していたとして、JPCERTコーディネーションセンターより4月8日に注意喚起が行われている。
「旧バージョンの Parallels Plesk Panel の利用に関する注意喚起」(http://www.jpcert.or.jp/at/2013/at130018.html)。

17

18 セ **18日**：Spamhausに対する大規模なDDoS攻撃が発生し、対処に協力したCloudFlare社に対しても攻撃が行われる事件が発生した。
詳細については例えば次のCLOUD FLARE Blogなどに詳しい。"The DDoS That Almost Broke the Internet"(http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet)。

19

20 他 **19日**：インターネット上のIPアドレス空間に対しスキャンを行った調査についてまとめた「Internet Census 2012」が公表された。この調査では約42万台のセキュリティに問題のあるデバイスを利用して調査したとしており、全体では200万台以上が問題のある状況で接続されていたとしている。また、調査結果からは多くの問題ある機器がインターネットに接続されていることが確認できる。
"Internet Census 2012"(http://internetcensus2012.bitbucket.org/paper.html)。

21

22

23 セ **20日**：韓国の主要な放送局や金融機関でマルウェアによる攻撃が発生し、PCやサーバなど約47,800台でハードディスク上のデータが破壊され、ATMやオンラインバンキングが利用できなくなる事件が発生した。

24

セ **22日**：遠隔操作ウイルス事件の犯人として逮捕された容疑者が威力業務妨害容疑など複数の罪で起訴された。

25

26 他 **25日**：IPAより、内部不正対策について、効果的な対策の整備が実施できるよう具体的な対策を示した「組織における内部不正防止ガイドライン」が公表された。
「組織における内部不正防止ガイドラインを公開」(http://www.ipa.go.jp/about/press/20130325.html)。

27

28 脆 **26日**：BIND9.7以降にサーバの停止などが可能な脆弱性(CVE-2013-2266)が見つかり、修正された。
Internet Systems Consortium、「CVE-2013-2266 [JP]: 不正に細工された正規表現によってnamedがメモリ不足になる」(https://kb.isc.org/article/AA-00881)。

29 セ **26日**：全国231の自治体で住民基本台帳ネットワークシステム(住基ネット)が利用できなくなる障害が発生した。
原因については総務省が4月2日にデータの文字コードの誤りによるものとする調査結果を公表している。
「市町村の住基ネットCSのシステム障害について」(http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000130.html)。

30

31 他 **30日**：US-CERTは、公開されているDNSサーバについて、DNSアンプ攻撃に利用される可能性があるとして設定の見直しなどを促す注意喚起を行った。
"Alert (TA13-088A) DNS Amplification Attacks"(http://www.us-cert.gov/ncas/alerts/TA13-088A)。

[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

ズと称するメッセージが、複数の報道機関や記者にメールで送信されました。また、クイズの答えから2ヵ所の位置が特定されましたが、そのうちの1ヵ所から、事件に関連したデータが格納されているとされるメモリ媒体が取り付けられた首輪をつけた猫が見つかり、その首輪が押収されています。その後、2月10日に容疑者が威力業務妨害容疑で逮捕されました。3月には容疑者が威力業務妨害罪など複数の罪で起訴されましたが、本稿執筆時点では、容疑者はこれらの容疑について否認しています。

■ 政府機関のセキュリティ対策の取り組み

政府機関のセキュリティ対策の動きとして、以前から進められていた政府機関の情報セキュリティ対策のための統一管理基準などで利用されているCRYPTREC暗号リスト（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）の改定が行われました。これは、暗号の解析・攻撃技術の進化による危殆化などの懸念から、元のリストの利用目安を10年としていたために、2009年から4年をかけて改定の作業が進められていたものです。今回の改定により「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」という3つのリストがそれぞれ定義されました。また、情報セキュリティ政策会議では、2010年度に策定された「国民を守る情報セキュリティ戦略」に代わる情報セキュリティに関する新たな基本戦略の策定について、検討が進められています[*24][*25]。

■ その他

2月には、国内において米国法人のWebサービス事業者に対し、名誉毀損行為を行ったとみられるユーザの発信者情報の開示を命ずる仮処分が東京地裁で決定されました。これは、2011年に民事訴訟法が改正され、日本において事業を行っていると認められる外国法人に対する国内法の適用が可能となったことによるものです。

同じく2月には、米国の広告配信サービス会社から広告配信を受けている複数の大手メディアサイトでGoogle Safe Browsingの機能により、不正なソフトウェアが存在する可能性があると表示されて、Chromeブラウザなどからアクセスできなくなる事例が発生しています。これは、広告配信サービス会社がマルウェアに感染したことにより、この会社のドメインがブラックリストに登録されたためでした。このときには、広告配信のシステムへの感染はなかったとされており、すぐに解除されています。同様の事件は、3月にも国内の大手報道機関などの複数のWebサイトに対して発生しています。これもGoogle Safe Browsingによりますが、ブロックされた原因については不明です。広告配信サービスが改ざんされマルウェア感染サイトに誘導される事例は2010年に国内でも発生し、多くの有名なWebサイトから感染サイトへの誘導が行われました。

また、SNSなどのオンラインサイトに対し、その認証情報を狙った攻撃や、盗んだIDとパスワードを悪用して異なるサイトに対してアカウントの盗用を試みる事件が話題となりました。2月にTwitter社に対する不正アクセスがあり、ユーザー名やメールアドレス、暗号化されたパスワードなど、約25万人のユーザー情報にアクセスされた可能性があるとして、該当のユーザに対してパスワードリセットを行ったことを公表しました。同様の事件は3月にEvernote社に対しても発生し、5,000万人のEvernote利用者のパスワードリセットが行われています。これらの事件ではパスワードは暗号化により保護されていましたが、より安全性を担保するために対策が実施されました。

3月には、韓国の複数の放送局や金融機関で、マルウェア感染によるシステム停止が同時多発的に発生しました。この事件では、合わせて数万台のコンピュータが感染し、ATMが利用できなくなるなどの重大な障害を引き起こしました。この事件の詳細については「1.4.1 韓国3.20大乱」も併せてご参照ください。

＊24 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　第32回会合（平成25年2月22日）」（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku32）。
＊25 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　第33回会合（平成25年3月26日）」（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku33）。

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になっています。

■ 直接観測による状況

図-3に、2013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-3では、DDoS攻撃全体を、回線容量に対する攻撃[*26]、サーバに対する攻撃[*27]、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、565件のDDoS攻撃に対処しました。1日あたりの対処件数は6.26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、サーバに対する攻撃が91.5%、複合攻撃が8.5%、回線容量に対する攻撃はありませんでした。

今回の対象期間で観測された中で最も大規模な攻撃は、サーバに対する攻撃に分類したもので、最大4万4千ppsのパケットによって228Mbps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74.2%が攻撃開始から30分未満で終了し、25.1%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0.7%ありました。なお、今回もっと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13時間29分(37時間29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[*28]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[*29]の利用によるものと考えられます。

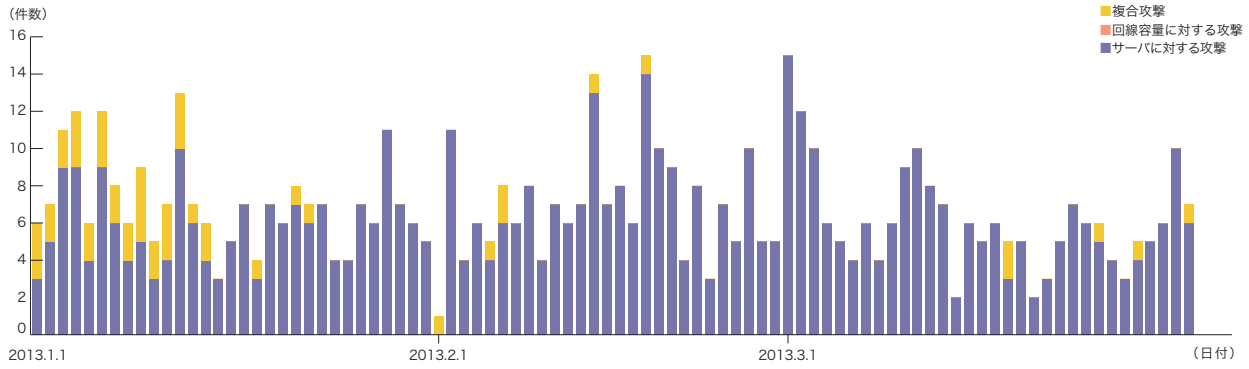


図-3 DDoS攻撃の発生件数

*26 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。

*27 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。

*28 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。

*29 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[*30]によるDDoS攻撃のbackscatter観測結果を示します[*31]。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。

2013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-4に、ポート別のパケット数推移を図-5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38.7%を占めています。また、IRC（Internet Relay Chat）で利用されている6667/tcpや、SSHで利用されている22/TCPなどへの攻撃やゲーム関連と考えられる25565/TCPなどの攻撃が観測されています。

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、Webサーバ（80/TCP）への攻撃では、米国の複数のDDoS対策サービス事業者の複数のサーバに対する攻撃が多く発生していることを観測しています。IRC（6667/TCP）への攻撃が2月11日から2月17日にかけて、多く発生していますが、これは米国のホスティング事業者のゲーム関連のサーバに対する攻撃で、2月15日を除く6日間の合計で25万回以上観測されました。それ以外にも米国、ドイツ、フランス、スイス、中国、ロシア、カザフスタンなどのホスティング事業者のサーバに対するSSH（22/TCP）、25565/TCP、7777/TCPに対する攻撃などを観測しています。

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、Operation Ababilによると考えられる複数の米国銀行サイトへの攻撃、過激な行動を行う宗教団体への継続した攻撃、1月に発生した複数のTorrentサイトへの攻撃、同じく1月に発生したAnonymousによると考えられるMITの複数サイトへの攻撃、Anonymousによると考えられるイスラエルの情報機関を含む複数の政府機関サイトへの攻撃、3月に発生したセキュリティ専門家のサイトへの攻撃、同じく3月に発生したAnonymousによると考えられるイタリアの複数の右翼政党サイトへの攻撃によるbackscatterをそれぞれ検知しています。

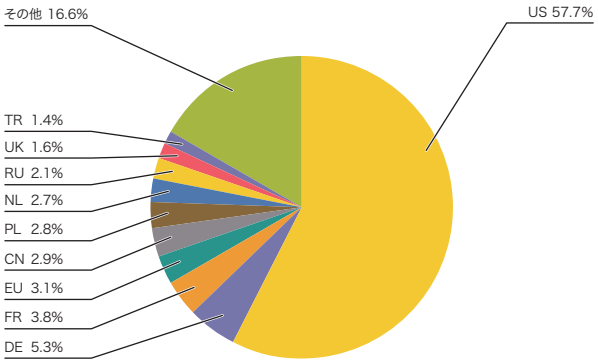


図-4 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

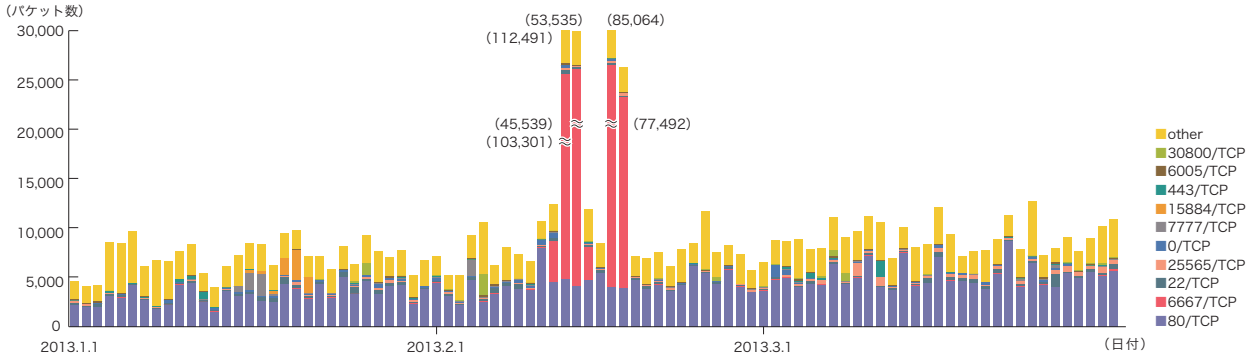


図-5 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

＊30 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。

＊31 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。

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[*32]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[*33]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

2013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-6に、その総量（到着パケット数）の推移を図-7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、24539/TCPや3913/UDPなど、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1月25日、2月12日から2月16日、3月6日、3月29日に中国、2月15日から2月16日にかけてインド、2月15日にドイツ、韓国、2月16日にタイ、3月29日に米国に割り当てられた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、ICMP Echo Requestも1月を中心に断続的に増加しています。2月16日にはイランとパキスタンから、3193/UDP宛てに大量の通信が発生しています。この目的は不明ですが、一部のMyDoomの亜種が使用しているケースや、このポートを利用した通信を行う特定のアプリケーションに脆弱性が確認されているため、これらを悪用する試みであると考えられます。

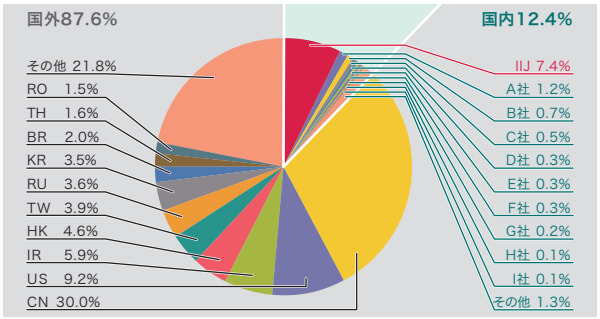


図-6 発信元の分布（国別分類、全期間）

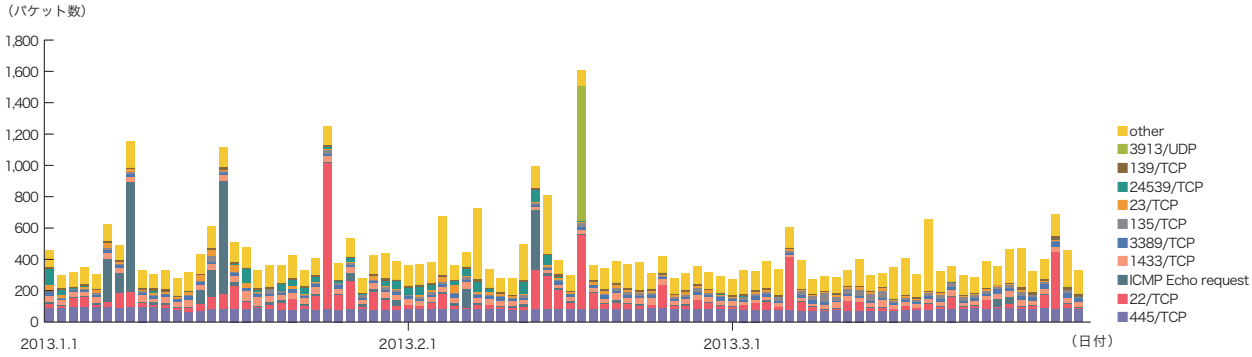


図-7 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊32 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。

＊33 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。

■ 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-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち

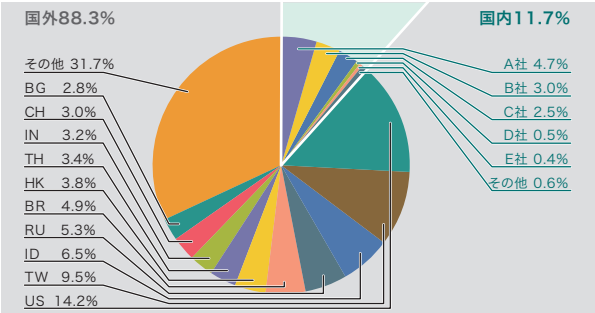


図-8 総取得検体数の分布

図-9と図-10では、1日あたりに取得した検体[*34]の総数を総取得検体数、検体の種類をハッシュ値[*35]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-9と図-10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116、ユニーク検体数が26でした。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、前号までと同様

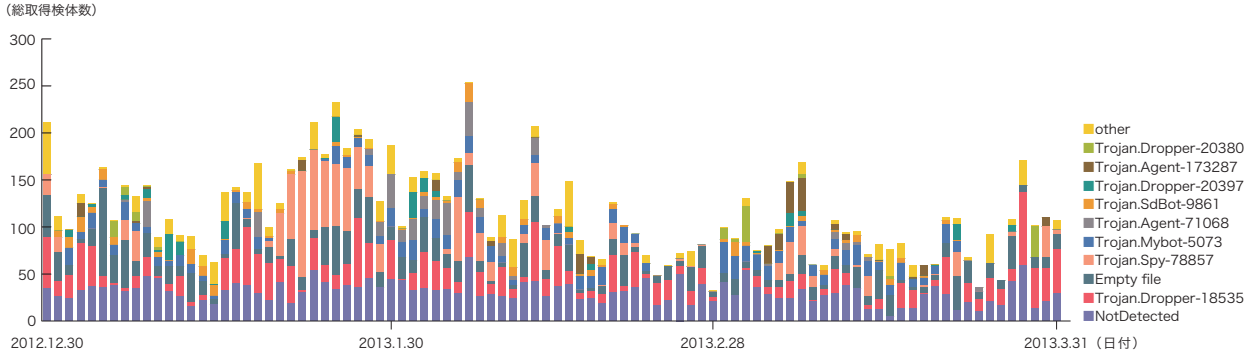


図-9 総取得検体数の推移(Confickerを除く)

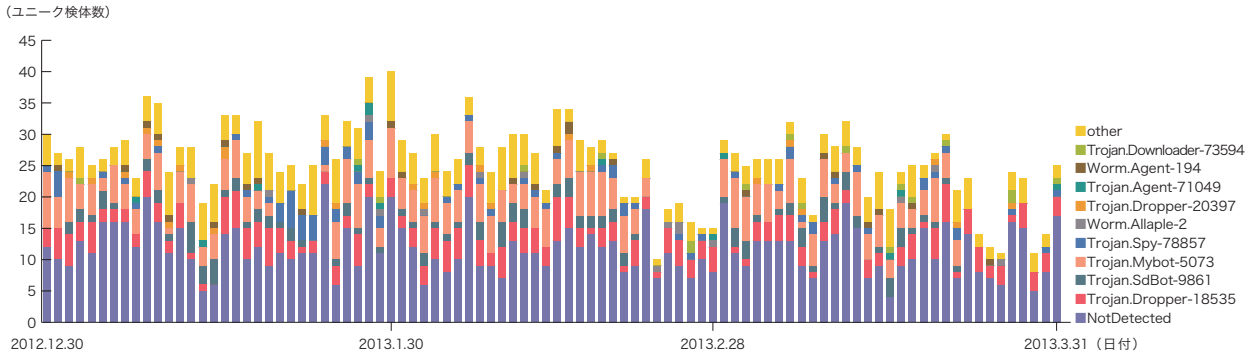


図-10 ユニーク検体数の推移(Confickerを除く)

＊34 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。

＊35 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。

にIRCサーバで制御されるタイプのボット2種類[*36][*37]と共にZeuS亜種が活動していたことが分かりました。また、米国、香港に割り当てられたIPアドレスからのワーム[*38]も継続的に観測されました。

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73.6%、ボット型21.5%、ダウンローダ型4.9%でした。また解析により、12個のボットネットC&Cサーバ[*39]と6個のマルウェア配布サイトの存在を確認しました。

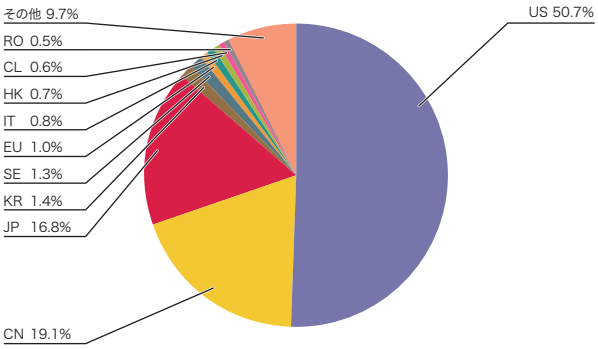


図-11 SQLインジェクション攻撃の発信元の分布

■ 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29,256、ユニーク検体数は811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99.6%、ユニーク検体数で96.9%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。

本レポート期間中では、前回の対象期間中に比べ、総取得検体数が約30%、ユニーク検体数が約10%減少しました。これは、IIJが観測に用いているハニーポットのIPアドレスが、Confickerの一部の亜種が感染活動の対象としないIPアドレスの空間[*40]に合致していたために発生しています。

Conficker Working Groupの観測記録[*41]によると、2013年3月31日現在で、ユニークIPアドレスの総数は1,497,909とされています。2011年11月の約320万と比較すると、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。

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[*42]について継続して調査を行っています。SQL

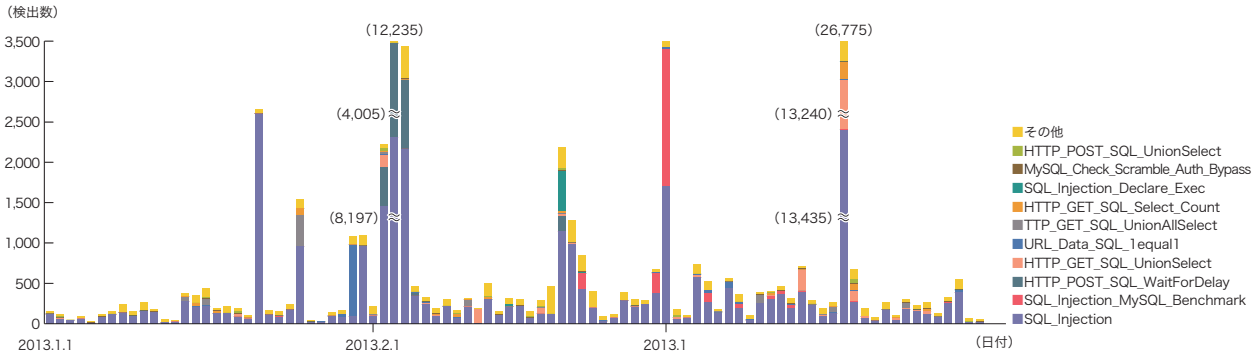


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

＊36 Trojan:Win32/Ircbrute(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute)。
＊37 Win32/Hamweq(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq)。
＊38 WORM_DEBORM.AP(http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au)。
＊39 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。
＊40 例えばConfickerの特定のIPアドレス帯域に対して感染活動を行わないという事象はdionaea開発者のブログで報告されている「Conficker does not like me?」(http://carnivore.it/2009/11/03/conficker_does_not_like_me)。
＊41 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking)。
＊42 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。

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。

2013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、米国50.7%、中国19.1%、日本16.8%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、大幅に増加しています。

米国からの攻撃が1位、中国からの攻撃が2位と上昇していますが、これは特定の攻撃先への大規模な攻撃が一部の日に発生したことによります。日本が3位になっていますが前回期間と比べると件数は増加しています。

この期間中、1月21日には国内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した。2月3日から4日にかけては中国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。3月1日には米国の特定の攻撃元から特定の攻撃先に対する大規模な攻撃が発生しています。3月18日にも米国の複数の攻撃元より特定の攻撃先に対する大規模な攻撃が発生しています。これらの攻撃は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。

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繋げています。ここでは、これまでに実施した調査のうち、3月に韓国で発生した、多数のマルウェア感染によりシステム障害などの被害を出した韓国3.20大乱、日本国内のWebサイトが多数改ざんされ、不正サイトへの誘導に利用された事件、および各国で活発に行われているサイバー攻撃対応演習の3つのテーマについて紹介します。

1.4.1 韓国3.20大乱

3月20日の午後、韓国の複数の放送局、金融機関において同時多発的にマルウェア感染によるシステム停止が発生しました。被害に遭った6つの組織を合わせて数万台のコンピュータがダウンし、金融機関ではATMが利用できなくなるなどの影響がでました。本節では事件全体の経緯について解説します。

■ マルウェアの動作

システム停止の直接の原因はマルウェア感染によるものです。今回の事件で確認されているのはDropper及びWiperと呼ばれるタイプのマルウェアで、Dropperは Wiperなどの関連プログラムを作成してこれらを実行します。Wiperはハードディスクの MBR (Master Boot Record) の領域やファイルシステムを上書きして破壊します。その後マシンを強制的に再起動しますが、MBRが破壊されているため、OSが起動しない状態となります。

IIJにおいても独自にこれらのマルウェア検体を入手して分析したところ、以下のような特徴を持っていることが分かりました。

■ Dropperの特徴

- Windows用Wiper、Unix用Wiperのプログラムを含む4つのファイルを作成する。
- "C:¥Windows¥Temp¥~v3.log"の存在をチェックし、存在しなければWindows用Wiperを実行する。
- mRemote、SecureCRT(どちらもSSHクライアントソフトの1つ)の設定ファイルからホスト名やrootユーザのパスワードなどの情報を取得する。
- 取得した情報をもとに、SCPを使用してUnix用Wiperプログラムをサーバにコピー後に、再びSSHで接続して実行する。

■ Windows用Wiperの特徴

- "C:¥Windows¥Temp¥~v3.log"の存在をチェックし、存在すれば何もしないで終了する(チェックしない亜種もある)。
- ローカル時刻が3月20日14:00になるまで待機する(待機しない亜種もある)。
- taskkillコマンドでpasvc.exe(AhnLab Policy Agent)とclisvc.exe(Hauri ViRobot ISMS)を停止する。
- MBRと各パーティションの先頭セクタを特定の文字列で上書きして破壊する(文字列の異なる亜種もある)。
- BからZまでの論理ドライブに対して、先頭のセクタから順に特定の文字列で上書きして破壊する。
- 5分後にWindowsを再起動する。

■ Unix用Wiperの特徴

- OSの種類(HP-UX、AIX、Solaris、Linux)によって動作が多少異なる。
- (1)ddコマンドでパーティションを/dev/nullで上書き、(2)rmコマンドでディレクトリ削除、の2つの破壊活動のうちいずれか、または両方を実行する。

上記にあるように、Wiperには動作の異なる複数の亜種が存在しています。また各セキュリティベンダーの報告などから、IIJでは入手できていない別の亜種も存在することが分かっています[*43]。これらのWiperマルウェアには感染後すぐに破壊活動をするものもありますが、3月20日の14時または15時以降になると実行される亜種もあり、これが複数の組織において同時多発的に被害が発生した理由だと考えられます。

また、韓国のセキュリティベンダー2社の製品のみをプロセス停止の対象にしていることや、特定のリモート接続ツールの設定ファイルのみを調べていることなど、動作対象をかなり絞り込んでいることが伺えます。実際に被害にあった組織において、このマルウェアの意図するとおりに効果的な破壊活動が行われたのだとすると、攻撃者は事前に対象組織について入念な調査を行っていた可能性が高いと言えます。

■ 感染経路

マルウェアの感染経路について、韓国放送通信委員会(KCC)の報告によると、被害組織に導入されていた更新管理サーバ(資産管理サーバ)からクライアントにマルウェアが配布されました[*44]。この6社には韓国のセキュリティベンダーであるAhnLab社のAhnLab Policy Center(APC)、Hauri社のViRobot ISMSなどの管理製品が導入されていました。通常は管理サーバからクライアントに対してプログラムの自動更新、配布などを行うわけですが、今回はこの仕組みが悪用されてマルウェアの配布に利用されたようです(ただし被害組織の中にはこれら2社の管理サーバとは別の仕組みでマルウェアが配布されたところがある、との報道もあります)。

つまり、攻撃者はこれらの組織内ネットワークにあらかじめ侵入し、更新管理サーバを乗っ取ってマルウェアを配布したことになります。更新管理サーバへの侵入方法は明らかになっていませんが、被害組織の1つに導入されていたAPCにはログイン認証をバイパスする脆弱性があり、攻撃者はこの脆弱性を悪用したとAhnLab社は報告しています[*45]。

これらの事実から、今回の攻撃は次の3段階に分けて実施されたと考えられます(図-13参照)。

---

*43 例えばAhnLab社の解析では、少なくとも3種類のDropperと4種類のWindows用Wiperが確認されている。ASEC Threat Research & Response blog :: 주요 방송사 및 은행 전산망 장애 유발 악성코드 분석(http://asec.ahnlab.com/926)。

*44 KCCからの3月21日の発表による。民·官·軍 사이버위협 합동대응팀, 공격 주체 규명에 주력(http://old.kcc.go.kr/user.do?mode=view&boardId=1042&page=P05030000&dc=K04030000&boardSeq=36096)。

*45 AhnLab社からの3月29日の発表による。안랩, 3.20 전산망 마비 농협관련 자체 중간조사 결과 발표(http://blog.ahnlab.com/ahnlab/1732)。

(1) 組織内PCへの侵入(初期感染)
(2) 更新管理サーバへの侵入
(3) クライアントへのマルウェア配布

現時点では、第1段階の初期感染がどのように行われたのか明らかになっていません。マルウェアが添付されたメールを被害企業の社員が受けとり感染したのではないか、あるいは外部のWebサイト閲覧によってPCがマルウェアに感染したのではないか、などと複数のセキュリティベンダーが推測していますが、公式に確認された情報ではありません。

なお、韓国警察の発表にもとづく報道によると、マルウェアの送信元の一部は欧米の4ヵ国のIPアドレスであることが確認されており、関係各国に捜査協力を要請しているようです。IIJで分析したDropper及びWiperの検体にはいずれも外部と通信する機能は含まれていませんでした。このため、異なる複数の種類のマルウェアが使われていたことが推測されます。

■ 韓国国内の対応

韓国国内では事件発生後すぐに、大統領から迅速な復旧と原因究明の指示がなされ、官民軍の合同対策チームが調査にあたるなど、比較的早い対応がなされました。またセキュリティベンダーの協力を受けて専用のマルウェア駆除ツールをその日のうちに公開し、被害組織の復旧を政府もサポートしています[*46]。3月29日になって被害を受けたシステムの復旧が完了したと合同対策チームが明らかにしましたが、本格的な原因究明や再発防止の取り組みには時間がかかると予想されます。

なお、今回の事件を受けて、韓国政府は4月11日に国家情報院を中心に15の関連する機関が参加する「国家サイバー安全戦略会議」を開催しました。その結果、上半期中に「国家サイバー安全保障総合対策」を策定し下期より実施すること、関連する法制度の整備をすすめること、北朝鮮によるサイバーテロ抑止の国際協力を推進すること、などの計画を発表しています[*47]。今後しばらくはサイバー危機対応の体制を再整備する動きが活発化しそうです。

■ 過去の事件との関連

韓国では2009年7月と2011年3月にも、それぞれ約11万台のPCがマルウェアに感染し、韓国及び米国の主要なサイトにDDoS攻撃を実施するという事件がありました。またこれらのマルウェアにはハードディスクのデータを破壊する機能もあり、感染したPCにも被害がでました。

韓国政府は4月10日に今回の事件に関する中間報告を行いましたが、これらの過去の事件とも関連性があることを示す多数の証拠があることを明らかにしました[*48]。報告によると、今回の攻撃に利用された76種のマルウェアや攻撃の中

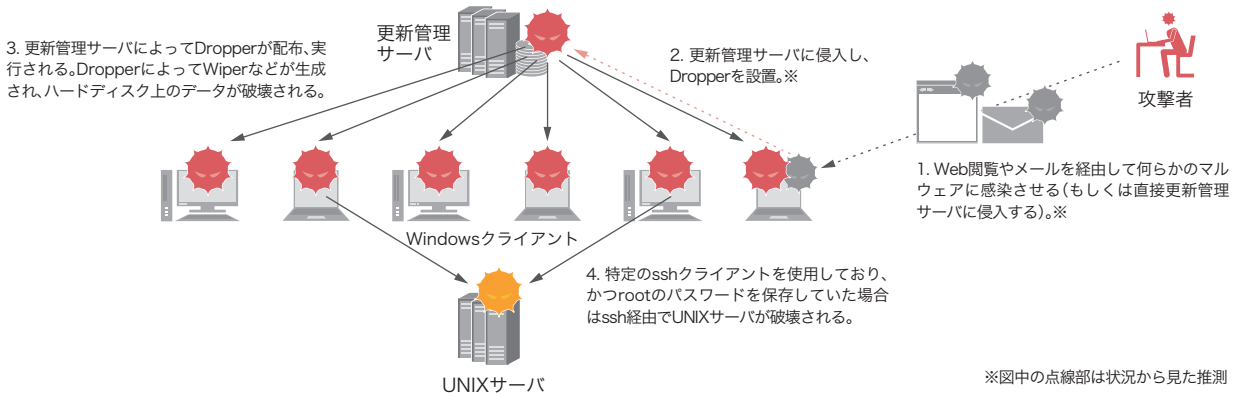


図-13 マルウェア感染の流れ

*46 韓国インターネット振興院(KISA)は3月21日にWebで駆除ツールを公開している。방송사・금융사 전산망 마비시킨 악성코드 치료 전용백신 배포(http://www.boho.or.kr/kor/notice/noticeView.jsp?p_bulletin_writing_sequence=2033)。
*47 未来創造科学部(MSIP)からの4月12日の発表による。'3.20 사이버테러' 관련 국가 사이버안전 전략회의 개최 - 국가사이버안보 종합대책 수립키로 - (http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=219)。
*48 未来創造科学部(MSIP)からの4月10日の発表による。民官軍 합동대응팀, '3.20 사이버테러' 중간 조사결과 발표 - 북한의 과거 해킹수법과 일치하는 증거 발견 -(http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=182)。

継点となった49のIPアドレスには、過去の攻撃でも利用されていたものが多く含まれています。また、攻撃者は少なくとも8ヵ月前から今回ターゲットとなった組織内のネットワークに侵入して準備を行っていたことも分かりました。

■ 日本への影響

今回の事件においては、主に韓国で利用されているソフトウェアの更新管理サーバがマルウェア配布の起点となっており、かつ韓国内の特定の組織が狙われていることから、日本国内を含め他の企業にすぐに影響が及ぶことはないと言えます。一方で、今回のような組織内部の管理サーバからマルウェアが配布されるという攻撃手法については国内でも起きる可能性があり、注意を払う必要があります。また、従来より標的型攻撃においては、組織内に侵入した攻撃者が組織内ネットワークを調査し、Active Directoryなどの認証サーバを攻撃する事例も多く見られます。現時点では今回被害に遭った組織への初期の侵入方法など不明な点が多く、具体的な懸念事項はありませんが、多くの端末を制御することのできる管理サーバのセキュリティの状況を、このタイミングで確認することをお勧めします。

1.4.2 日本国内のWebサイト改ざんとドライブバイダウンロード

2013年3月中旬、日本国内の285のWebサイトが改ざんされ、閲覧者を不正なサーバへ転送する状態になっているという記事がセキュリティ研究者のブログ[*49]で公開されました。IIJではこの285サイト及び関連が疑われる他の複数のWebサイトについて調査を行い、一連の攻撃で利用されたツールやマルウェアを解析しました。

■ 攻撃の概要

■ 改ざんされたWebサイト

改ざんされたWebサイトは、閲覧者をマルウェアに感染させる不正なサーバへ誘導する「redirector」として働きます。具体的には、クライアントPCが閲覧するコンテンツに、不正なサーバ(infector)を参照するiframeタグをインジェクションします。本件では、Webサイトに不正にインストールされたDarkLeechと呼ばれるApacheモジュールが、HTMLやJavaScriptなどのテキストコンテンツに動的にインジェクションを行っていました。参照先とするinfectorのURLは、逐次外部のC&Cサーバから取得しており、そのURLは10分間キャッシュされます。タイムアウト後は改めてC&CサーバからinfectorのURLを取得するため、短い期間でinfectorのURLを変化させられることが分かりました[*50]。

■ マルウェアに感染させる不正なサーバ

誘導先のinfectorでは、BHEK2(Blackhole Exploit Kit Version 2)が利用されていたと報告されています。BHEK2はクライアントPCのJava、Adobe Flash、Adobe Readerなどのブラウザプラグインの脆弱性を悪用してマルウェア感染を試みます。本件では複数のinfectorが利用されていましたが、IIJが確認したinfectorは主に国外のサーバで運用されており、その大部分が米国の特定のホスティング事業者に所属するノードでした。

■ 感染するマルウェア

infectorによる感染が成功すると、Ponyと呼ばれるマルウェアがインストールされることを確認しています。ただし、BHEK2はPony以外にもZeuS亜種(Citadel含む)、ZeroAccessなど様々なマルウェアを感染させることが報告されているため、今回もPonyだけでなくこれらのマルウェアが併せて配布されていた可能性が考えられます。Ponyはアカウント情報の窃取及び他のマルウェアのダウンロードを行います。IIJが2013年3月15日に取得したPonyの検体を解析したところ、利用されたPonyはバージョン1.9で、様々なWebブラウザやメーラ、ftp/ssh/rdpアプリケーションなど100種類近いクライアントソフトウェアから認証情報を窃取する機能を備えていることが分かりました[*51]。更に、情報窃取の対象にFFFTPやBecky!といった、主に日本国内で利用されているアプリケーションが含まれていました。これは、マルウェア作成者が日本のユーザを明確に攻撃対象と考えていることを示

*49 2013年3月15日に、0day.jp「#OCJP-098:【警告】285件日本国内のウェブサイトが「Darkleech Apache Module」に感染されて、IEでアクセスすると「Blackhole」マルウェア感染サイトに転送されてしまいます!」(http://unixfreaxjp.blogspot.jp/2013/03/ocjp-098-285blackhole-exploit-kit.html)で公開された。
*50 攻撃動向やinfectorのURLパターンの特徴については「BHEK2 による大量改ざん」(https://sect.iij.ad.jp/d/2013/03/154955.html)で詳しく解説している。
*51 感染するマルウェアについては「BHEK2を悪用した国内改ざん事件の続報」(https://sect.iij.ad.jp/d/2013/03/225209.html)で詳しく解説している。

しています。このような傾向は今回が初めてというわけではありませんが、日本国内において大きな影響を及ぼす可能性があり、注意が必要です。また、今回IIJが取得したPonyは、C&CサーバからHarddisk Antivirusというスケアウェアをダウンロードすることを確認しました。これは偽のセキュリティソフトウェアで、ユーザを脅して直接金銭を窃取するマルウェアです。ただし、前述のBHEK2の機能と同様に、Ponyが何をダウンロードするかはC&Cサーバ側の設定に依存するため、一連の攻撃では他のマルウェアも並行して利用されていた可能性が考えられます。

■ 攻撃の特徴と改ざんの検出

■ Webサイトの改ざん手法

攻撃者がWebサイトにDarkLeechをインストールしてredirectorとして動作させるためには、通常はサーバの管理者権限が必要となります。そのため、今回改ざんされていたWebサイトは、事前に何らかの手段により攻撃者に管理者権限を奪取されていたと考えられます。改ざんされたWebサイトの多くでPlesk Panelと呼ばれるサーバ管理ソフトウェアが利用されていたという情報があり、このPlesk Panelの脆弱性が悪用された可能性が示唆されています[*52]。一方で、改ざんされたすべてのWebサイトでPlesk Panelが利用されていたわけではないため、sshやftpサービスへの辞書攻撃や、CMSの既知の脆弱性の悪用など、他の手法で改ざんされたケースもあったと考えられます。

■ DarkLeechの解析妨害機能

DarkLeechは、セキュリティ担当者や研究者などによる感染経路の調査や検体の取得、正規のサーバ管理者によるモジュール検出などを回避するために、次のような機能を備えています（図-14参照）。

- 同一クライアントへのインジェクション防止（接続元IPリスト、HTTP Cookieを用いて1週間制限する）
- Webクローラなどの攻撃対象外のクライアントへのインジェクション防止（User-Agentを判定）
- サーバ管理者のセッションへのインジェクション防止（ローカルIPアドレスからの接続、Admin文字列を含むURLへのリクエスト、utmpにリストされたリモートホストからの接続にはインジェクションしない）
- 特定プロセス（tcpdump、rkhunter、chkrootkit）動作時のインジェクション防止

また、DarkLeechの機能ではありませんが、転送先のinfectorにおいても以下のような機能が確認されました。これも調査、解析の妨害を意図しているものと考えられます。

- マルウェアを毎回ランダムなキーでエンコードしてダウンロードさせる
- 同じ接続元IPアドレスからの接続を拒否する（HTTP502応答）

■ DarkLeechの検出

DarkLeechはApacheモジュールとしてロードされるので、Apacheの設定ファイル（httpd.confなど）に含まれるLoadModule行を調べることで存在を確認することが可能です。ただし、DarkLeechは任意のファイル名でインストールされるため、あらかじめ意図してインストールしたモジュールの名称をすべて把握していない場合は、この方法でDarkLeechモジュールの有無を判定することができません。もう1つの検出方法として、DarkLeechが利用する設定ファイルや一時ファイルを検索する方法が挙げられます。DarkLeechは/var/tmp以下にsess_という文字列で始まるファイルを大量に生成します。これはPHPのセッションファイルのデフォルトパスですが、PHPを利用していない場合や、利用していてもセッションファイルのパスを変更している場合には、DarkLeechの痕跡と考えることができます。

また、PHPをデフォルトのセッションファイルパスで利用している場合は、以下のファイルをDarkLeechの判定に利用することが可能です。

*52 JPCERT/CCは旧バージョンのPlesk Panelが稼働するサーバで不正なApacheモジュールを設置するWeb改ざん事例が複数確認されたとして、「旧バージョンのParallels Plesk Panel の利用に関する注意喚起」（http://www.jpcert.or.jp/at/2013/at130018.html）を公開している。また、Cisco Systemsは「Possible Exploit Vector for DarkLeech Compromises」（http://blogs.cisco.com/security/possible-exploit-vector-for-darkleech-compromises/）でPleskの一部のバージョンに付属していたWebメールコンポーネント（Horde/IMPパッケージ）の脆弱性が悪用された可能性を示唆している。

- **/var/tmp/sess_d0c94b5412e3494af1e7db042c59afa2**
  iframeタグの内容をエンコードして保存するファイル。
- **/var/tmp/sess_dbd2e9556e489478954a3af93b797244**
  管理サーバ接続時の排他処理に利用するファイル。
- **/usr/lib/libbdl.so.0**
  管理サーバのホスト名をエンコードして保存するファイル(このファイルは存在しない場合もある)。

■ 対策

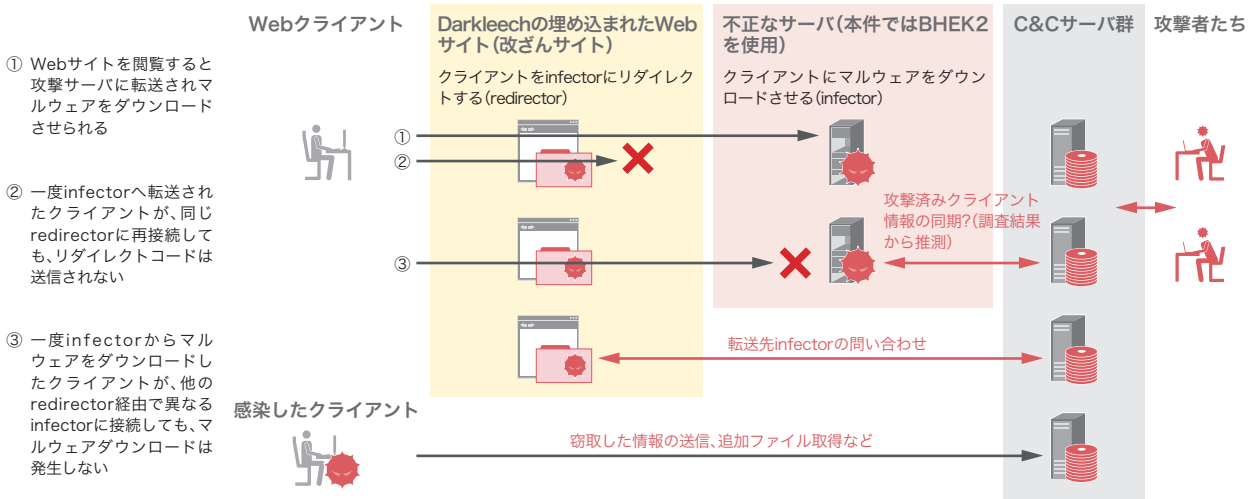
DarkLeechの存在は、2012年8月頃から報告されはじめました[*53]。日本国内では、BHEK2を用いた同種の攻撃が2013年1月頃から報告されており[*54]、IIJの観測においても、2013年4月時点で攻撃が継続していることを確認しています。今後も類似の攻撃が継続することが予想されるため、Webサイト運営者、PC管理者はそれぞれの立場で適切な対策を実施していく必要があります。

■ Webサイトを改ざんから守るための対策

Webサイト改ざんでは様々な手法が用いられるため、対策もサーバの設定変更からネットワーク構成変更、あるいはセキュリティ診断やセキュリティ機器の導入など多岐に及びます。ここでは、基本的な対策として次の3点を徹底することを強く推奨します。

- 脆弱性を悪用した攻撃に備え、利用するアプリケーションやプラグイン、ライブラリを脆弱性のない状態に保つ。
- ブルートフォース攻撃に備え、複雑なパスワードを設定した上で、管理通信の接続元制限と連続認証試行の制限を行う。
- 公開サービスのログ取得および監視体制を確立し、外部からの攻撃試行を把握できるようにしておく。

また、安価なホスティングサービスやクラウドサービスなどを利用して小規模なWebサイトを運営している場合であっ



※DarkLeechやマルウェア検体の解析結果および観測されたInfectorの挙動は、redirector、infector、マルウェアそれぞれに管理サーバが存在することを示唆する。しかし、これらの管理コンポーネントが同一の主体によって運用されているとは限らない。BHEK2やDarkleechはSaaSの様な形態でも再販されているため、異なる主体が利用するコンポーネントが動的に組み合わされることで一連の攻撃を構成している可能性が考えられる。

図-14 一連のドライブバイダウンロード攻撃の流れと解析を妨害する仕組み

*53 Unmask Parasites. Blog、「RFI: Server-wide iframe injections」(http://blog.unmaskparasites.com/2012/08/13/rfi-server-wide-iframe-injections/)、「Malicious Apache Module Injects Iframes」(http://blog.unmaskparasites.com/2012/09/10/malicious-apache-module-injects-iframes/)などの記事がDarkLeechについて言及している。

*54 本件の改ざん被害及び関連事案について、トレンドマイクロ セキュリティ ブログ「国内外におけるWebサーバ(Apache)の不正モジュールを使った改ざん被害」(http://blog.trendmicro.co.jp/archives/6888)及び「Blackhole Exploit Kit による攻撃、問題のJavaの脆弱性を利用」(http://blog.trendmicro.co.jp/archives/6840)で紹介されている。

ても、サービス仕様や運用者のスキルなどを鑑み、適切な対策が適用できているか確認しておくことを推奨します。

■ クライアントPCをマルウェア感染から守るための対策

ユーザ環境では、OSやサードパーティアプリケーションの更新、ウイルス対策ソフトウェアの導入とその最新バージョン維持を徹底することが重要です。多少の運用負荷を伴いますが、EMETなどの脆弱性緩和ツールの導入やソフトウェア制限ポリシーなどを設定することも効果的です。また、特にブラウザプラグインを対象とした攻撃に関しては、Mozilla FirefoxやGoogle Chromeに実装されているClick-to-Playが有効です[*55]。どちらのブラウザでも初期状態では無効になっているので、利用するためには設定変更が必要です。

1.4.3 サイバー攻撃対応演習

本年1月に、一般財団法人日本データ通信協会テレコム・アイザック推進会議(Telecom-ISAC Japan)のサイバー攻撃対応演習ワーキンググループによるサイバー攻撃対応演習が実施されました。この演習は、IIJを含む国内の大手通信事業者8社と、複数の重要インフラ事業者[*56]が参加する大規模なものとなりました。近年、インターネットに関連した演習が世界各地で実施されており、その有用性が認識されています。本稿ではサイバー攻撃対応演習の概要と設計の詳細、実施とその効果について紹介します。

■ 主なサイバー攻撃対応演習

インターネットに関わる主なサイバー攻撃対応演習を表-1に示します。有名なものとしては、米国の国土安全保障省(DHS)が実施しているCyber Stormがあり、2006年から2年ごとに実施されています。Cyber Storm IVは、2011年の秋から2012年にかけて実施され、時間をかけて進行していくインシデントに対し、その対応が適切かを詳細に確認できる演習となっています。EUで毎年行われているCyber Europeの2012年の演習では、EUの60のISPと60の金融機関を含む339の組織から571人が参加しました。アジアでもAPCERTが主催するAPCERT Drillが実施されており、今年1月に行われたAPCERT Drill 2013では18ヵ国の22のCSIRTチームが参加しています。日本でも多くの分野で演習が行われており、例えば、総務省が平成18年度から3ヵ年で実施した「電気通信事業分野におけるサイバー攻撃対応演習」では、実際のインターネット環境を利用して重要インフラ企業のネットワークを模した環境への攻撃に対し、防御を行う演習を行っています。このように世界の様々な地域でサイバー攻撃に対する演習が実施されています。

■ 演習の設計と実施

演習を実施するにあたっては様々な準備が必要となります。ここでは演習を設計する上で基本となる設計の概要とその実施について解説します。

■ 目的の設定

演習を設計するにあたっては、まず最初に主催者および参加者の目的を明確にし、演習を行うことでこれらの目的を達成できるように演習のシナリオを構成する必要があります。例えば、演習によって自社内の緊急対応手順の確認と問題点の洗い出しを行いたいという目的があった場合には、シナリオ上にそれを確認できるイベントを入れる必要があります。このため、シナリオ作成の前に全参加者の目的の摺合せを十分に行うことがもっとも重要となります。

■ 演習の登場人物

演習の設計と実施においては次のような役割があります。

- シナリオ設計者:目的や想定する脅威から発生するイベントをまとめた演習シナリオを設計する
- TA(Trusted Agent):参加者の代表として、設計時にシナリオについてアドバイスを行う
- ディレクタ:演習全体を統括し、進行を行う
- コントローラ:演習の際にプレイヤーに対し情報の付与や対応の決定を促す

*55 Click-to-Playはプラグインを自動実行せずユーザに確認(クリック)を促す機能。ドライブバイダウンロードではプラグインの表示領域が隠ぺいされることが多いため、確認ボタンも目視されない。このためユーザが誤ってクリックしてしまう可能性もなくなる。

*56 国民生活及び社会活動に不可欠なサービスを提供している社会基盤のこと。現在、10分野が重要インフラに指定されている。内閣官房情報セキュリティセンター(NISC)、「重要インフラ対策チームの概要:重要インフラとは」(http://www.nisc.go.jp/active/infra/outline.html#infra)。

・プレイヤー：演習の中心となる参加者、演習時の対応を行う
・評価者：プレイヤーの議論や行動などを逐次記録し評価を行う

これらの役割はシナリオの内容に応じて、増員することがあります。例えば、シナリオ上でイベントが同時に多数発生するような負担が大きい場合は、イベントごとに担当のコントローラやプレイヤーを割当てるなどし、シナリオの進捗に影響が出ないようにします。

■ 演習の種類

一般的に、演習には大きく分けて実演習と机上演習があり、その演習の目的によって、どちらか適切なものを選びます。実演習とは、実際の環境もしくは実際の環境に沿って構築された疑似環境の下で演習を実施するため、現実に発生する状況を

表-1 インターネット関連の主要な演習

開始年	実施間隔	国、地域	実施主体	演習名称	主な参加組織	目 的
1996年	毎年	米国	DEFCON	DEFCON CTF*57	社会人、学生によるチーム	最新の攻撃・解析技術の研究、情報セキュリティ人材の育成、確保
2003年	-	米国	国土安全保障省(DHS)	Livewire*58	通信、エネルギー、金融、地方自治体	攻撃発生後の緊急対応体制が実際に機能するか検証
2006年	2年ごと	米国	国土安全保障省(DHS)	Cyber Storm*59	省庁、行政機関、外国政府、民間企業	政府も含めた各参加組織のサイバー攻撃対策の達成度を測定
2006年	毎年	アジア	APCERT	APCERT Drill*60	各国のCSIRTチーム	参加チームとの情報共有と連携、協調対処の仕組みの検証
2006年	毎年(2008年まで)	日本	総務省	電気通信事業分野におけるサイバー攻撃対応演習*61	ISP、重要インフラ事業者、関連各団体、関連省庁	実行可能な攻撃方法とシステムの脆弱性の有無、攻撃による損害の程度、緊急対応体制が実際に機能するか否かなどを検証
2006年	毎年	日本	内閣官房情報セキュリティセンター(NISC)	重要インフラにおける分野横断的演習(CIIREX)*62	重要インフラ各分野のセプターと重要インフラ所管省庁	重要インフラ事業者におけるIT 障害に対する官民の情報共有、連絡、連携のための仕組みの実行性を検証
2006年	毎年	日本	一般財団法人 電力中央研究所	電力分野におけるサイバーテロ演習*63	電力会社及び関連会社	インシデントレスポンス体制や情報セキュリティ対策の検討材料となる知見の獲得
2009年	毎年	日本	内閣官房情報セキュリティセンター(NISC)	セプター訓練*64	重要インフラ各分野のセプターと重要インフラ所管省庁	情報共有体制の維持、向上
2009年	毎年	日本	一般財団法人 日本データ通信協会 テレコム・アイザック推進会議	サイバー攻撃対応演習	ISP、重要インフラ事業者、関連各団体、関連省庁	事業者間連携の確認、人材育成、課題認識
2010年	毎年	EU	欧州ネットワーク情報セキュリティ庁(ENISA)	Cyber Europe*65	ISP、重要インフラ事業者	加盟各国が作成したヨーロッパのサイバーインシデント対応プランを確認
2012年	不定期	日本	Web Application Security Forum Hardening Project	Hardening*66	学生、企業、社会人によるチーム	Webサイトの安全性を追求する技術の啓蒙と人材の育成、またそうした技術の社会的認知の向上
2012年	毎年	日本	NPO 日本ネットワークセキュリティ協会(JNSA) SECCON 実行委員会	SECCON CTF*67	学生、社会人によるチーム(学生主体)	実践的情報セキュリティ人材の発掘・育成、技術の実践の場の提供
2012年	-	日本	経済産業省	CTFチャレンジジャパン	社会人、学生によるチーム(社会人主体)	日本の実践的情報セキュリティ人材の発掘・育成、技術の実践の場に求められるCTF競技の在り方についての検討
2013年	-	日本	経済産業省	電力・ガス・ビル分野のサイバーセキュリティ演習*68	電力、ガス、ビルの各事業者、他	制御システムに対する攻撃への対応強化

*57 過去のCTFについては次のDEFCONのサイトで確認できる。"Capture the Flag Archive"(http://www.defcon.org/html/links/dc-ctf.html)。
*58 Dartmouth College ISTS"ISTS Bulletin Volume 1, Number 1, Spring 2004"(http://www.ists.dartmouth.edu/docs/ists_v1_1_04.pdf)。
*59 Cyber Stormについては次の米国国土安全保障省(DHS)のサイトなどを参照のこと。"Cyber Storm: Securing Cyber Space"(http://www.dhs.gov/cyber-storm-securing-cyber-space)。
*60 APCERT、"APCERT EMBARKS ON GLOBAL COORDINATION TO MITIGATE LARGE SCALE DENIAL OF SERVICE ATTACK"(http://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf)。
*61 この演習については次の総務省のWebサイトで当時の演習の模様などがビデオ公開されている。「電気通信事業分野におけるサイバー攻撃対応演習」(http://www.soumu.go.jp/menu_kyotsuu/media/080401_1.html)。
*62 内閣官房情報セキュリティセンター(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～【CIIREX 2012（シーレックス2012)】～」(http://www.nisc.go.jp/active/infra/pdf/ciirex2012_2_press.pdf)。
*63 一般財団法人 電力中央研究所(http://criepi.denken.or.jp/)の「平成19年度電力中央研究所研究成果発表会」でのポスターセッションの松井正一氏の発表「電力分野におけるサイバーテロ演習の概要」(http://criepi.denken.or.jp/jp/civil/result/presentation/report_shakai_risk2007/37.pdf)で確認できる。
*64 内閣官房情報セキュリティセンター(NISC)、「セプター訓練まとめ」(http://www.nisc.go.jp/conference/seisaku/ciip/dai31/pdf/31siryou04-2.pdf)。
*65 ENISA、"Largest cyber security exercise 'Cyber Europe 2012' report published in 23 languages"(http://www.enisa.europa.eu/media/press-releases/largest-cyber-security-exercise-cyber-europe-report-published-in-23-languages-by-eu-agency-enisa)。
*66 WASForum Hardening Project、(http://wasforum.jp/hardening-project/)。
*67 JNSA SECCON(セキュリティコンテスト)実行委員会、(http://www.jnsa.org/seccon/)。
*68 経済産業省、「電力・ガス・ビル分野のサイバーセキュリティ演習を実施します～演習用模擬システムを用いた国内初のサイバーセキュリティ演習～」(http://www.meti.go.jp/press/2012/02/20130204002/20130204002.html)。

再現しやすくなります。しかし、実際の環境を利用する場合には、本来業務への影響を考慮する必要などがありますし、疑似環境では、どこまで実際の環境に近づけるかにより、確認できる内容や環境構築コストなどが変化します。

机上演習とは、実際の環境下もしくは擬似的に設定されたある状況下と想定して演習を行うものです。机上演習では、実際に操作する必要や対応上の制約がないため、たとえば、実際には非常に時間がかかったり、物理的な制約がある状況も表現できます。反面、机上演習では実際に対応の作業を実施しないため、シナリオ作成には対応とその結果などの詳細さが求められます。

■ シナリオの設計

目的が決定すると具体的なシナリオの設計に入ります。背景情報や脅威、敵対者を定義し、そこから、具体的な攻撃や発生する障害などを決めていきます。更に、参加者間の関係、ネットワーク構成、使用機材やアプリケーションのバージョンなども確認しながらシナリオの詳細を固めていきます。

ここで重要となるのは参加各社から選出されるTA（Trusted Agent）と呼ばれる役割です。TAは各参加者の代表として、シナリオ設計者が作成するシナリオが、自社の人員やネットワーク環境、業務手順などといった、通常業務の範囲と違いがないか確認し、演習がスムーズに進行するようにアドバイスを行います。参加する事業者により、対応する部署やフローは異なります。演習の流れをスムーズにするためには、イベント1つ1つを各社の環境に合わせ、微調整する必要があります。特に机上演習では、実際に調査や設定を行う訳ではないため、調査結果や設定の内容、自社のプレイヤーが取る対応とその結果などもシナリオに組み込む必要があります。大変な作業となりますが、この作業が演習のシナリオにより現実感を持たせ、プレイヤーが通常の業務と同様に果たすべき、それぞれの役割に基づいた対応を行うことに繋がります。

シナリオはリハーサルなどを通じ、更に精査していきます。最終的にはMSEL（Master Scenario Event List）と呼ばれるイベントの詳細なリストにまとめます。MSELにはイベントの投入時間やそのイベントでプレイヤーがどのような行動を期待されているか、更には状況の詳細な調査結果など、演習を進行する上で必要な情報がすべて入ります。ディレクタやコントローラはこれを使って演習を進めます。シナリオ設計は非常に手間と時間がかかる作業ですが、シナリオの完成度がその後の成果に影響を及ぼすため、入念な準備が必要となります。

■ 演習の実施

演習は、図-15のような形式で実施します。演習は競技とは違い、他社と対応を競ったり、特定の個人を評価・批判するものではありません。この点は全参加者にあらかじめ周知しておきます。ディレクタによるイベントの投入や対応で他の事業者への連絡が必要な場合には、あらかじめ定められた連絡手段を用いて依頼や問い合わせを行います。これには専用の演習用ツールを利用したり、紙の連絡票を使用することもあります。プレイヤーは、演習において特別な対応をするのではなく、普段の自分の業務や職責に基づいて、投入されたイベントに対してアクションを行います。コントローラは、プレイヤーへの情報の提示や質問への回答などを通じてシナリオを進めていきます。評価者は、プレイヤーが実施したアクションやその理由などを記録します。演習では、プレイヤーが想定していた対応を行わないなど、シナリオに影響が及ぼすような場面も多く発生します。ディレクタは全体の状況を確認し、各事業者のコントローラと調整し、プレイヤーの動きを汲み取りながら、シナリオが円滑に進むように促していきます。

■ 結果の取りまとめと成果の抽出

演習後には必ず結果の取りまとめと成果の抽出を行います。この時には演習で発生した攻撃の内容やネットワー

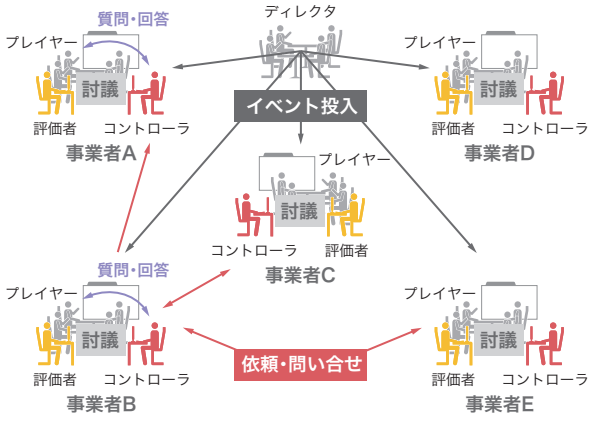


図-15 演習の概要

ク構成など、シナリオ全体がプレイヤーにも開示されます。はじめにシナリオの全体を確認し、どのような脅威、イベントが発生していたのか、またそのイベントの目的などをコントローラがプレイヤーと共に確認していきます。その後、演習中の限られた情報から何をどのように判断し、どのような理由でアクションを実施したなど、各参加者の行動を評価者の記録なども確認しながら共有していきます。更に実施したアクションについて、発生していたシナリオの状況と対応時の認識に違いがあれば、なぜそう考えたかを含めて確認や議論を行っていきます。

成果は、最終的には演習の参加組織全体でその内容を持ち寄り、演習報告書(After Action Report)[*69]としてまとめます。これは、参加者のアクションをまとめ、その成果を全体で共有するためのものです。成果には改善が必要な項目や課題も含まれており、これが実際の業務への貴重な情報として、改善を促していきます。

■ 演習のメリット

演習では、演習報告書でまとめられた結果と成果から課題や改善点を明確に確認できます。演習で発生させるイベントの多くは実際に発生した場合には深刻な事態となりかねません。このような状況を予め疑似的に体験することで、組織や事業者におけるインシデント対応能力の向上や取り組みの充実に繋がっています。更には、事業者間連携のきっかけにもなっています。参加者についても、異なる事業者や同じ会社でも複数の異なる部署の参加者が協調し対応する経験を通じて、幅広い視野を持った人材の育成に寄与します。

■ まとめ

ここまで解説してきたように、演習の設計と実施にあたって多くの労力が必要です。演習の規模が大きくなるほどシナリオ設計はより複雑となり、多くのコストが必要となります。しかし、そのようなコストを費やしても演習で得られる経験や知識には、他では得がたいものがあります。IIJでは今後も演習などの活動を通じて、事業者間連携や協調対処に向けた体制作りに積極的に参加していきます。

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、3月に韓国で発生した大規模事件の概要と、日本国内で発生した大量改ざんによるマルウェア感染事例、インシデント対応能力向上や人材育成で注目される演習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。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まいります。

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、鈴木 博志、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)
根岸 征史、鈴木 博志、春山 敬宏(1.4.1 韓国3.20大乱)
梨和 久雄、鈴木 博志(1.4.2 日本国内のWebサイト改ざんとドライブバイダウンロード)
土屋 博英(1.4.3 サイバー攻撃対応演習)
IIJサービス本部 セキュリティ情報統括室

協力:
加藤 雅彦、須賀 祐治、小林 直、桃井 康成、齋藤 聖悟　IIJ サービス本部 セキュリティ情報統括室

*69 演習の成果は参加者のみでの共有とされることが多く、公開されているものは少ないが、誰でも参照できる成果物の例としては、次の米国国土安全省(DHS)で実施されたCYBER STORM IIIがある。"CYBER STORM III Final Report" (http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf)。