# ドメイン名のレジストリ登録情報の改ざん対策

**今回は、ドメイン名のレジストリ登録情報の改ざん対策について、端末のメモリ内に潜む脅威をスキャンするopenioc_scan、ID管理技術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2014年10月から12月までの期間では、依然としてAnonymousのHacktivismによる攻撃が複数発生しており、報道機関などの企業を狙った標的型攻撃も相次いで発覚しています。また、ドメイン名のレジストリに対する攻撃によるドメインの乗っ取りや改ざんをもとにした不審なメッセージの表示やマルウェア感染事件が発生しており、日本国内の企業も影響を受けています。11月には、米国の映画関連企業において、企業内のITシステムが使えなくなると同時に、多くの情報が盗まれ、その一部が公開されるという事件がありました。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。

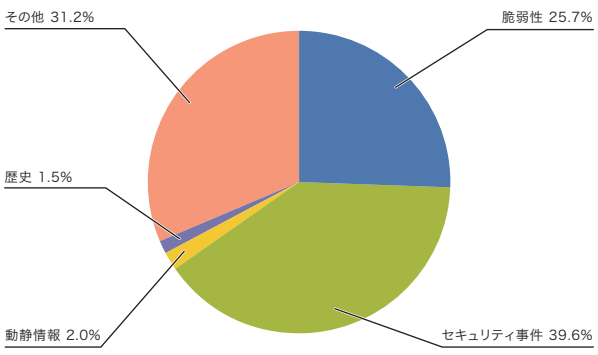



**図-1 カテゴリ別比率(2014年10月～12月)**

## 1.2 インシデントサマリ

ここでは、2014年10月から12月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

### ■ Anonymousなどの活動

この期間においても、Anonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。10月には香港でのデモ活動と関連して中国政府や香港行政府のWebサイトの改ざんや情報漏えいなどが複数発生しています(OpHongKong)。11月にはフィリピンでも政府に対する抗議から複数の政府機関のWebサイトで改ざんが発生しました。トルコでは、トルコ政府に対する抗議を行っている何者かにより、送電会社のWebサイトへの不正侵入が発生しています。トルコ国内においては、別の何者かによると考えられる、複数のWebサイトに対する改ざんや不正侵入が発生しています。パレスチナ自治区ガザでの紛争に関連した、イスラエルの複数の政府関連サイトや民間企業のWebサイトに対する攻撃も継続して発生しています。同様に、ロシアとウクライナ、パキスタンとインドネシア、インドとパキスタンなどでも、紛争に関連して相互に攻撃が行われています。これ以外にも、世界中の各国政府とその関連サイトに対して、Anonymousなどのハクティビスト達による攻撃が継続して行われました。また、政府機関や報道機関など企業のSNSアカウントの乗っ取り事件も継続して発生しています。

*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。

### ■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2][*3][*4][*5]、Internet Explorer[*6][*7][*8]、Microsoft Office[*9]などで修正が行われました。12月には、Windows 8.1 Updateの未修正の脆弱性[*10]について、発見者であるGoogle社が公開したことから話題となりました。これはGoogle社の報告から90日後に自動で脆弱性情報を公開する場合があるとのポリシーによるものでしたが、公開について問題が指摘されています[*11]。Adobe社のAdobe Flash Player、Adobe Reader及びAcrobatでも修正が行われました。ジャストシステム社の一太郎では、第三者が任意のプログラムを実行できる可能性のある脆弱性が見つかり、修正されています。Oracle社のJava SEでも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。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を含むOracle社の複数の製品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。CMSとして利用されるDrupalについてもSQLインジェクションの脆弱性が見つかり、修正されました。同じく、WordPressについても、XSSの脆弱性を含め、複数の脆弱性が修正されています。これらの脆弱性については、実際に管理者権限を奪われるなどの被害が確認されています[*12]。BIND、Unboundなどの複数のDNSソフトウェアでは、外部からサーバの異常動作やサービスの停止が可能となる脆弱性が修正されています。時刻同期に利用されているntpdについても、細工を施したパケットにより、ntpdの実行権限で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ました。

10月にはSSL/TLSサーバなどで利用されているSSLv3に対する新たな攻撃として、POODLE attack（Padding Oracle On Downgraded Legacy Encryption attack）と呼ばれる攻撃手法が公開されました[*13]。この脆弱性はプロトコル仕様自体の問題であったことから、クライアントである主要なWebブラウザやサーバにおいて、SSLv3を無効とする修正が行われたり、設定方法が公開され、対策が行われました。

### ■ ドメイン名のレジストリへの攻撃

この期間では、ドメイン名のレジストリやレジストラに対する攻撃による登録情報の不正書き換えと、その結果として不正なサイトへの誘導が複数発生しています。10月には、インドネシアのドメインである.idを管理しているccTLDレジストリであるPANDIが不正アクセスを受け、Googleの現地サイトが別のサイトに誘導される事件が発生しています。大手動画サイトでは、偽広告を利用して、ユーザをランサムウェアに感染させようとする攻撃が確認されました。この事件では、攻撃者が何らかの方法でポーランド政府のドメインのDNS情報を改ざんし、正規のサイ

＊2 「マイクロソフト セキュリティ情報 MS14-058 - 緊急 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 (3000061)」（https://technet.microsoft.com/ja-jp/library/security/ms14-058.aspx）。
＊3 「マイクロソフト セキュリティ情報 MS14-060 - 重要 Windows OLE の脆弱性により、リモートでコードが実行される (3000869)」（https://technet.microsoft.com/ja-jp/library/security/ms14-060.aspx）。
＊4 「マイクロソフト セキュリティ情報 MS14-064 - 緊急 Windows OLE の脆弱性により、リモートでコードが実行される (3011443)」（https://technet.microsoft.com/ja-jp/library/security/ms14-064.aspx）。
＊5 「マイクロソフト セキュリティ情報 MS14-066 - 緊急 Schannel の脆弱性によりリモートでコードが実行される (2992611)」（https://technet.microsoft.com/ja-jp/library/security/ms14-066.aspx）。
＊6 「マイクロソフト セキュリティ情報 MS14-056 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2987107)」（https://technet.microsoft.com/ja-jp/library/security/ms14-056.aspx）。
＊7 「マイクロソフト セキュリティ情報 MS14-065 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (3003057)」（https://technet.microsoft.com/ja-jp/library/security/ms14-065.aspx）。
＊8 「マイクロソフト セキュリティ情報 MS14-080 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (3008923)」（https://technet.microsoft.com/ja-jp/library/security/ms14-080.aspx）。
＊9 「マイクロソフト セキュリティ情報 MS14-081 - 緊急 Microsoft Word および Microsoft Office Web Apps の脆弱性により、リモートでコードが実行される (3017301)」（https://technet.microsoft.com/ja-jp/library/security/ms14-081.aspx）。
＊10 この脆弱性は、2015年1月に「マイクロソフト セキュリティ情報 MS15-008 - 重要　Windows カーネルモード ドライバーの脆弱性により、特権が昇格される (3019215)」（https://technet.microsoft.com/library/security/ms15-008）で修正されている。
＊11 例えば、次のSOPHOS社のブログであるnakedsecurityなどで双方の問題が指摘されている。"Zero-day in Windows 8.1 disclosed by Google"（https://nakedsecurity.sophos.com/2015/01/03/zero-day-in-windows-8-1-disclosed-by-google/）。
＊12 例えば、Drupalでは、10月16日に修正がリリースされて数時間後には攻撃が始まったとして注意喚起を行っている。「Drupal 7.32 で修正された脆弱性に関する注意喚起」（http://drupal.jp/PSA-2014-11-04）。
＊13 詳細については、本レポートのVol.25（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol25.pdf）の「1.4.2 POODLE attack」で解説している。

## 10月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

他 **4日**：米国連邦通信委員会(FCC)は、大手ホテルチェーンが利用客のWi-Fi通信を意図的に妨害し、有料のWi-Fiシステムに誘導していたとして60万ドルの罰金を支払うよう命じた。
"Marriott to Pay $600K to Resolve WiFi-Blocking Investigation"(http://www.fcc.gov/document/marriott-pay-600k- resolve-wifi-blocking-investigation-0)。この問題については1月になって、あらためて事業者が利用者に対してWi-Fiルータやスマートフォンを使ったデザリングを意図的 に妨害しないように求める勧告を行っている。"WARNING: Wi-Fi Blocking is Prohibited"(http://www.fcc.gov/document/warning-wi-fi-blocking-prohibited)。

セ **5日**：インドネシアのドメインである.idのccTLDレジストリであるPANDIが何者かによる不正アクセスを受け、Googleのサイトがハイジャックされる事件が発生した。

セ **10日**：米国のセキュリティ企業であるVolexity社は、香港のデモに関連したサイバー攻撃が発生していることをBlogで報告した。この中で日本の新聞社のWebサーバを含むいくつかの国内サイトが、不正なサイトへの誘導もしくは不正なサイトとして改ざんされていることを指摘している。
詳細については、次の"Democracy in Hong Kong Under Attack"(http://www.volexity.com/blog/?p=33)を参照のこと。

セ **10日**：米国の複数の小売り事業者で、マルウェアによる利用客のクレジットカード情報などの情報漏えいが発覚した。
例えば、ディスカウントショップ大手のKmartでは店舗決済システムがマルウェア感染していたとしている。Sears Holdings Corporation "Kmart Investigating Payment System Intrusion"(http://www.searsholdings.com/pubrel/kpressOne.jsp? id=s16310_item137317)。

他 **10日**：JPCERTコーディネーションセンターは、Webベースのシステム管理ツールであるWebminで利用されるTCP 10000番ポートへのスキャンが増加しているとして注意喚起を行った。
「JPCERT/CC Alert 2014-10-10 TCP 10000番ポートへのスキャンの増加に関する注意喚起」(https://www.jpcert.or.jp/at/2014/at140038.html)。

脆 **15日**：Microsoft社は、2014年10月のセキュリティ情報を公開し、MS14-056とMS14-058など3件の緊急とMS14-060など5件の重要な更新を含む合計8件の修正をリリースした。
「2014 年 10 月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-JP/library/security/ms14-oct)。

脆 **15日**：Oracle社は、Oracleを含む複数製品について、四半期ごとの定例アップデートを公開し、Java SEの25件の脆弱性を含む合計154件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - October 2014"(http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html)。

脆 **15日**：Googleより、SSL 3.0のCBC暗号アルゴリズムに対する新たな攻撃手法であるPOODLE(Padding Oracle On Downgraded Legacy Encryption)が公開された。
詳細については、次の暗号プロトコル評価技術コンソーシアム(CELLOS)の「[2014/10/15] SSLv3仕様そのものに対する POODLE attack について」(https://www.cellos-consortium.org/jp/index.php?PoodleAttack_20141015_J)などを参照のこと。

脆 **15日**：Adobe Flash Playerに、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。
「APSB14-22: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-22.html)。

セ **15日**：はてなブックマークボタンを設置している一部のWebサイトで、Googleセーフブラウジングなどによるセキュリティ上の警告が表示される事象が発生した。
はてなブックマーク開発ブログ、「はてなブックマークボタンを設置した一部サイトに対するセキュリティ警告に関して」(http://bookmark.hatenastaff.com/entry/2014/10/18/021046)。

脆 **16日**：CMSアプリケーションのDrupalにSQLインジェクションの脆弱性(CVE-2014-3704)が見つかり、修正された。
"SA-CORE-2014-005 - Drupal core - SQL injection"(https://www.drupal.org/SA-CORE-2014-005)。

セ **16日**：トレンドマイクロ社は、YouTube上の偽広告からマルウェアに誘導する攻撃が確認されたとして注意喚起を行った。
トレンドマイクロセキュリティブログ、「YouTube上の偽広告からランサムウェア感染へ誘導、主に米国で被害」(http://blog.trendmicro.co.jp/archives/10094)。

他 **17日**：経済産業省より、国際的にサービスを展開する事業者の参考となる、「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」が取りまとめられ、公表された。
「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドラインを策定しました」(http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html)。

他 **17日**：警察庁は、SSDPリフレクション攻撃が増加しているとして注意喚起を行った。
「UPnPに対応したネットワーク機器を踏み台としたSSDPリフレクター攻撃に対する注意喚起について」(http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf)。

他 **21日**：Apple社は、OS X YosemiteのSpotlight検索機能で問題となっていた、現在地の取得や検索情報が送信されている点について声明を公表した。
「OS X Yosemite: Spotlight Suggestions」(http://support.apple.com/kb/PH18943?viewlocale=ja_JP)。

脆 **22日**：Microsoft社は、Microsoft OLEにリモートでコード実行可能な未修正の脆弱性(CVE-2014-6352)があることを公表した。
「マイクロソフト セキュリティ アドバイザリ 3010060 Microsoft OLEの脆弱性により、リモートでコードが実行される」(https://technet.microsoft.com/library/security/3010060)。本脆弱性は11月に「マイクロソフト セキュリティ情報 MS14-064 - 緊急 Windows OLEの脆弱性により、リモートでコードが実行される (3011443)」(https://technet.microsoft.com/ja-jp/library/security/ms14-064.aspx)で修正された。

他 **31日**：総務省は、モバイルによる新事業創出などによる経済の創生と国民負担の軽減を目指し、SIMロックの解除や、MVNOの普及に向けた取り組み、4Gといった高速通信に向けた電波帯の割当などモバイルの利用環境整備の取り組みについて公表した。
「『モバイル創生プラン』の公表」(http://www.soumu.go.jp/menu_news/s-news/01kiban02_02000134.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

トに見せかけていたことが指摘されています。日本の大手新聞社やSNSサービスでも、レジストリ登録情報の不正な書き換えが原因と考えられる、不正なサイトへの誘導と特定のユーザに対するマルウェアへの感染を試みる事件が発生しました。これについては香港で行われていたデモに関連した攻撃との報告が米国のセキュリティ企業から行われています。11月にも国内の複数の大手サイトで、Syrian Electronic Armyと名乗る何者かによるメッセージと画像が表示される事件が発生しました。この事件では、これらのサイトで利用していたSNS連携サービスについて、レジストリへの不正アクセスによりネームサーバに関する登録情報が書き換えられたことで、攻撃者が用意したと考えられる別のサイトに誘導されていました。これにより、当該サービスを利用していた、国内外の大手サイトを含む多くのサイトが影響を受けました。このような事件に国内企業が巻き込まれる事例が複数発生したことから、JPCERTコーディネーションセンターなど複数の団体から注意喚起が行われています。詳細については、「1.4.1 ドメイン名のレジストリ登録情報の改ざん対策」も併せてご参照ください。

### ■ 政府機関の取り組み

政府機関のセキュリティ対策の動きとしては、前国会から継続審議されていた「サイバーセキュリティ基本法」について、11月の衆議院本会議において可決され、成立しました。これにより、サイバーセキュリティ戦略本部の設置や、セキュリティ戦略案の作成、行政機関のセキュリティ基準の策定、行政機関で発生したセキュリティインシデントの調査など、行政機関などにおけるセキュリティの確保に向けたサイバーセキュリティの推進体制や機能の強化が図られることとなります。更に、重要インフラ事業者におけるセキュリティ確保の促進や官民連携による対策の強化など、国と民間企業の更なる連携についても期待されています。

これを受け、情報セキュリティ政策会議第41回会合が開催され、国のサイバーセキュリティ推進体制の機能強化に関する取り組み方針が決定されています[*14]。また、具体的な取り組みとして国民全体の情報セキュリティへの関心、理解度、対応力の強化増進を図り、我が国の情報セキュリティ水準の向上を目指した、「情報セキュリティ社会推進協議会」が11月に設立されています。同じく11月には、警察庁の総合セキュリティ対策会議で検討されていた、いわゆる日本版NCFTA[*15]について、産業界、学術研究機関、捜査機関などが参加する「一般財団法人 日本サイバー犯罪対策センター（JC3）」が業務を開始しました。JC3では、参加組織それぞれが持つサイバー空間の脅威に関する情報の共有や分析、対処に向けた研究開発、トレーニングの提供、米国NCFTA[*16]など海外機関との連携といった取り組みを通じ、安全・安心なサイバー空間の実現を推進する活動を行っていくとしています。

### ■ Webサイトの改ざん

10月には国内の新聞社の運営するWebサイトが不正アクセスを受け、フィッシングサイトとして悪用される事件が発生しています。この事件では、当該サイトを閉鎖し調査が行われましたが、1ヵ月以上経った12月に、調査の終了と、安全性の検証が完了し、安全が確認されたとしてサービスを再開しています。12月にはドメインやIPアドレスなど、インターネットの各種資源の管理と調整を行っているICANN（Internet Corporation for Assigned Names and Numbers）が、不正アクセスを受け、Centralized Zone Data System（czds.icann.org）を含む複数のシステムへのアクセスが確認されたとして、パスワードを無効化する措置を講じたことを発表しました。この事件では、11月に発生した内部職員を装ったフィッシングメール攻撃によって流出したパスワードなどの情報が使われていました。同様に、DNSサーバとして利用されるBINDの開発元であるInternet Systems Consortium（ISC）のWebサイトが不正アクセスを受け、マルウェア配布サイトに誘導するよう改ざんされる事件が発生しています。この事件ではWordPressの脆弱性が悪用され、改ざんされたとされています。

国内でも出版社のWebサイトが不正アクセスを受け、別のWebサイトに誘導される事件が発生しています。この事件

＊14 内閣官房情報セキュリティセンター、「第４１回会合（持ち回り開催）（平成２６年１１月２５日）」（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku41）。
＊15 日本版NCFTAについては、2013年に情報セキュリティ政策会議で決定されたサイバーセキュリティ戦略の中で創設に向けた検討を進めることが明記されたことから、警察庁の総合セキュリティ対策会議（http://www.npa.go.jp/cyber/csmeeting/index.html）で検討が進められていた。
＊16 NCFTA（National Cyber-Forensics & Training Alliance）（http://www.ncfta.net/Index.aspx）は、FBIなどの法執行機関、民間企業、学術機関を構成員として設立された米国の非営利団体でサイバー犯罪に関する情報の集約、分析、捜査機関の職員に対するトレーニングなどを実施している。

## 11月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

他 **5日**：JPCERTコーディネーションセンターなど複数の団体から、国内の組織で利用している.comドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加されるドメイン名ハイジャックのインシデントが複数発生しているとして注意喚起を行った。
「JPCERT/CC Alert 2014-11-05 登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起」(http://www.jpcert.or.jp/at/2014/at140044.html)。

他 **6日**：衆院本会議にて、サイバーセキュリティ基本法が可決し、成立した。
「サイバーセキュリティ基本法案」(http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm)。

セ **7日**：FBIは、Torを使った違法薬物売買の犯罪サイトであるSilk Road 2.0を摘発し、運営者を逮捕したことを発表した。
FBI、"Manhattan federal court to the operator of charge Silk Road 2.0 web site"(http://www.fbi.gov/newyork/press- releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court)。

セ **7日**：欧州刑事警察機構(Europol)は、米国や欧州16カ国の捜査当局と連携し、Tor上で運営されていた複数の犯罪サイトを摘発したことを公表した。
EUROPOL、"GLOBAL ACTION AGAINST DARK MARKETS ON TOR NETWORK"(https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network)。

セ **11日**：米国郵政公社(USPS)は、何者かによる不正アクセスを受け、職員80万人以上の個人情報が流出した可能性があることを発表した。
"Postal Service Statement on Cyber Intrusion Incident"(http://about.usps.com/news/fact-sheets/scenario/media-statement-final.pdf)。

脆 **12日**：Microsoft社は、2014年11月のセキュリティ情報を公開し、MS14-064とMS14-065、MS14-066など4件の緊急と8件の重要な更新を含む合計14件の修正をリリースした。
「2014 年 11 月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-jp/library/security/ms14-nov)。

脆 **12日**：Adobe Flash Playerに、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。
「APSB14-24: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-24.html)。

脆 **13日**：ジャストシステム社の一太郎に任意のコード実行可能な脆弱性が見つかり、修正された。
「[JS14003] 一太郎の脆弱性を悪用した不正なプログラムの実行危険性について」(http://www.justsystems.com/jp/info/js14003.html)。

他 **13日**：サイバー空間の脅威に対処するため、産学官の連携による情報共有と海外機関との連携を通じ、サイバー犯罪の実態解明と、その脅威を軽減・無効化する取り組みとして一般財団法人日本サイバー犯罪対策センター(JC3：Japan Cybercrime Control Center)が発足し、業務を開始した。
一般財団法人日本サイバー犯罪対策センター(JC3)、(https://www.jc3.or.jp/)。

他 **17日**：国及び地域の産学官民が情報流通網を構築し、各主体の連携・協力を通じて、安全・安心な社会を構築することを目指した、「情報セキュリティ社会推進協議会」の設立総会が開催された。
内閣官房情報セキュリティセンター(NISC)、「『情報セキュリティ社会推進協議会(仮称)』設立総会の開催について」(http://www.nisc.go.jp/press/pdf/syakaisuishinkyougikai20141113.pdf)。

セ **19日**：不正に取得したIDとパスワードを用いて違法にプロキシサーバを運用していたとして、警視庁や都道府県の合同捜査本部が一斉捜索を行い、不正アクセス禁止法違反などの容疑で複数人が逮捕された。

脆 **21日**：CMSアプリケーションのWordPressにXSSの脆弱性などサイトへの不正侵入の可能性のある複数の脆弱性が見つかり、修正された。
「WordPress 4.0.1 セキュリティリリース」(https://ja.wordpress.org/2014/11/21/wordpress-4-0-1-security-release/)。

セ **21日**：Twitterに投稿されていた児童ポルノ画像をリツイートして拡散したとして、未成年を含む複数が児童買春・ポルノ禁止法違反(公然陳列)で書類送検、もしくは児童相談所に通告された。

セ **24日**：米国の映画会社が何者かによる不正侵入を受け、全システムが停止する事件が発生した。

脆 **26日**：Adobe Flash Playerに、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。
「APSB14-26: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-26.html)。

セ **27日**：米国のSNS連携サービスがレジストリへの攻撃によるドメインハイジャックを受け、このサービスを利用していた国内外の大手サイトを含む多数のサイトで、特定のメッセージと画像が表示される事件が発生した。
詳細については、次のGIGYA社のBlogを参照のこと。"Regarding Today's Service Attack"(http://blog.gigya.com/regarding-todays-service-attack/)。

[ 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

では、フィッシングメールによって会員情報の確認を騙った偽のログインフォームに誘導し、IDやパスワードなどの情報を不正に取得する手口が利用され、クラウドサービスの管理権限を持つIDが窃取されたことが原因とされています。

### ■ 企業の内部情報を狙った攻撃

この期間では引き続き、企業の業務システムなどへのマルウェア感染による内部情報の漏えい事件が発覚しています。10月には、複数の小売り事業者でマルウェア感染が見つかっていますが、このうちの1社では昨年から複数の情報漏えい事件で使用されているPOSシステムを狙ったマルウェアBackoffであったことが公表されています[*17]。このマルウェアについては、8月にUS-CERTから注意喚起が行われていますが[*18]、その後も継続的に感染事件が発生していることから、活発な活動が行われていることが伺われ、引き続き注意が必要です。

11月には米国の大手映画会社に対して大規模な攻撃が発生しました。この事件では、社内PCのマルウェア感染により、公開前の映画データ、映画関係者のパスポート情報、従業員のメールデータやその他の個人情報を含む社内データが大量に外部へ流出し、特定の映画について上映しないことを要求する脅迫が行われたり、何者かが流出したデータを複数回に分けて公開するなど、その後も混乱が続きました。使われたマルウェアには、対象となった企業で使われていた特定のセキュリティソフトを無効化する機能や、PC上のデータを破壊する機能などが含まれており、今回の攻撃がこの企業を狙って周到に準備した上で実行されたことが窺われます。今回使用されたマルウェアについては、複数のセキュリティ企業から2013年に韓国の複数の放送局、金融機関で発生した同時多発的なマルウェア感染による事件[*19]に使われたものとの類似性が指摘されています[*20]。

12月には、韓国の電力会社がマルウェアが添付されたメールによる攻撃を受け、内部情報が漏えいする事件が発生しています。この事件では犯人から原子力発電所の稼働中止や金銭の要求などが行われ、その後、原子炉の設計図や従業員の個人情報などが複数回に渡ってインターネットに公開されるなどしています。

### ■ その他

米国では、FBIが違法薬物売買などの犯罪サイトであるSilk Road 2.0の閉鎖と運営者の逮捕を実施したことを発表しました。これに関連して、欧州刑事警察機構（Europol）は、米国や欧州16ヵ国の捜査当局と連携してTor上で運営されていた犯罪サイトの大規模な摘発を行っています。この作戦では「Tor」を使った「.onion」ドメイン400件以上が差し押さえられ、大量の逮捕者と共にビットコインや現金、様々なドラッグ、金などの貴金属が押収されています。

11月には不正に取得したIDとパスワードを用いて違法にプロキシサーバを運用していたとして、警視庁や都道府県の合同捜査本部が全国で一斉捜索を行い、不正アクセス禁止法違反などの容疑で複数人が逮捕されています。この事件については、運用されていたサーバではソフトウェアの海賊版が使われていたとして、著作権法違反（複製権侵害または海賊版業務使用）の容疑でも複数人が逮捕されています[*21]。盗まれたIDとパスワードについては一部の無線LANルータの既知の脆弱性が悪用されたとされており、不正アクセスや大手銀行へのフィッシングなどに悪用されていました。

11月にはReginと呼ばれるマルウェアが話題となりました。このマルウェアはベルギーの通信事業者が感染していたとされており、侵害したネットワーク内に潜伏して監視を行うように設計されていました。更にパスワードの窃取やネットワークトラフィックの監視などの通常のRAT機能の他に、携帯電話の基地局のモニター機能など特殊な機能も確認されています[*22]。

---

*17 International Dairy Queen, Inc. "Data Security Incident"（http://www.dairyqueen.com/datasecurityincident/）。
*18 US-CERT、"Alert (TA14-212A) Backoff Point-of-Sale Malware"（https://www.us-cert.gov/ncas/alerts/TA14-212A）。
*19 事件の詳細については、本レポートのVol.19（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol19.pdf）の「1.4.1 韓国3.20大乱」も参照のこと。
*20 例えば、トレンドマイクロ社のセキュリティブログ「FBIが注意喚起する「破壊的な不正プログラム」の解析」（http://blog.trendmicro.co.jp/archives/10484）などを参照のこと。
*21 一般社団法人コンピュータソフトウェア著作権協会、「『不良プロキシサーバー』運営事業者らを全国一斉摘発」（http://www2.accsjp.or.jp/criminal/2014/post.php）。
*22 このマルウェアの詳細については、Symantec社のSecurity Response Blogなどを参照のこと。「Regin: 人目に付かずに監視活動が可能な最悪のスパイツール」（http://www.symantec.com/connect/blogs/regin）。

## 12月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

セ **6日**：出版社のWebサイトが、何者かに不正侵入され、別のWebサイトに誘導されるよう改ざんされる事件が発生した。

他 **8日**：内閣官房情報セキュリティセンターの主催で、重要インフラにおける分野横断的演習が実施された。
「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【2014年度分野横断的演習】」(http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2014gaiyou.pdf)。

脆 **9日**：BINDなど複数のDNSソフトウェアにサーバの異常動作やサービスの停止が可能となる脆弱性が見つかり、修正された。
「(緊急)複数のDNSソフトウェアにおける脆弱性(システム資源の過度な消費)について(2014年12月9日公開)」(http://jprs.jp/tech/security/2014-12-09-multiple-impl-vuln-delegation-limit.html)。

脆 **10日**：Microsoft社は、2014年12月のセキュリティ情報を公開し、MS14-080とMS14-081など3件の緊急と4件の重要な更新を含む合計7件の修正をリリースした。
「2014年12月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-JP/library/security/ms14-dec)。

脆 **10日**：Adobe Flash Playerに、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。
「APSB14-27: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-27.html)。

脆 **10日**：Adobe Reader及びAcrobatに、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。
「APSB14-28: Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/reader/apsb14-28.html)。

セ **15日**：韓国水力原子力発電がマルウェアが添付されたメールによる攻撃を受け、原子炉の設計図やマニュアル、従業員の個人情報などを漏えいする事件が発生した。

セ **17日**：ICANNは、複数のシステムに不正アクセスを受け、一部のユーザ情報を流出したことを公表した。
詳細については、次のICANNの発表を参照のこと"ICANN Targeted in Spear Phishing Attack | Enhanced Security Measures Implemented"(https://www.icann.org/news/announcement-2-2014-12-16-en)。

他 **17日**：ドイツ内務省連邦情報技術安全局(BSI)より、2014年度のITセキュリティ白書が公開された。
白書では、製鉄所に対する攻撃が行われ、設備に損害を与えた事件が発生していたことが記載されている。この事件については"The State of IT Security in Germany 2014"(https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile)の"3.3.1 APT attack on industrial installations in Germany"で言及されている。

他 **18日**：日本発の情報セキュリティ国際会議としてCODEBLUEが2日間の日程で開催された。
詳細については、次のCODEBULE公式サイト(http://codeblue.jp/2014/)を参照のこと。

他 **19日**：JPCERTコーディネーションセンターは、12月5日頃から、QNAP社のNAS製品を狙った探査活動であるTCP8080番ポートへのスキャンが増加しているとして注意喚起を行った。
「JPCERT/CC Alert 2014-12-19 TCP 8080番ポートへのスキャンの増加に関する注意喚起」(https://www.jpcert.or.jp/at/2014/at140055.html)。

脆 **20日**：ntpdに細工したパケットにより、ntpdの実行権限で任意のコードが実行される可能性のある複数の脆弱性が見つかり、修正された。
JVN、「JVNVU#96605606 Network Time Protocol daemon (ntpd) に複数の脆弱性」(https://jvn.jp/vu/JVNVU96605606/)。

他 **22日**：総務省は、モバイルサービスの料金低廉化・サービス多様化に向けた取り組みの1つである「SIMロック解除に関するガイドライン」について改正を実施した。この中では、原則として事業者は販売したすべての端末についてSIMロック解除に応じるとされている。
「『SIMロック解除に関するガイドライン』の改正」(http://www.soumu.go.jp/menu_news/s-news/01kiban03_02000275.html)。

セ **23日**：Internet Systems Consortium(ISC)のWebサイトが不正アクセスを受け、マルウェア配布サイトに誘導するよう改ざんされる事件が発生した。
この事件については、発見した米国のセキュリティ企業Cyphort社のBlogを参照のこと。"Internet Systems Consortium's ISC.org infected"(http://www.cyphort.com/isc-org-infected/)。

脆 **28日**：ドイツで行われたセキュリティカンファレンスで、公衆電話網で使用される通信規格の1つであるSS7に存在する電話盗聴の可能性がある脆弱性が発表された。
この脆弱性についての詳細は次の発表を参考のこと。Laurent Ghigonis,Alexandre De Oliveira,"SS7map : mapping vulnerability of the international mobile roaming infrastructure"(http://media.ccc.de/browse/congress/2014/31c3_-_6531_-_en_-_saal_6_-_201412272300_-_ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira.html#video)。

脆 **29日**：Google社は、Microsoft社のWindows 8.1 Updateに権限昇格につながる未修正の脆弱性が見つかったとして公表を行った。
公開はgoogle-security-research(https://code.google.com/p/google-security-research/)で行われた。

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

※日付は日本標準時

12月にはドイツ内務省連邦情報技術安全局(BSI)からITセキュリティ白書が公開され、製鉄所への攻撃が発生し、操業停止させられたことから生産設備に被害が発生した事件が起きていたことが明らかとなりました。

この期間では、大規模なDDoS攻撃がいくつか発生しています。12月にはLizard Squadを名乗る何者かによるPSNやXbox Liveなどの複数のオンラインゲームサービスやTorに対する攻撃が発生しています。この攻撃者はその後、一連の攻撃に利用した攻撃基盤を、DDoS攻撃ツールとして提供したことから、実際にいくつかのサイトのDDoS攻撃に悪用されました。1月になってメンバーと思われる複数人が逮捕されていますが、その後も残ったメンバーによって継続して攻撃が行われていることから、引き続き注意が必要です。

## 1.3 インシデントサーベイ

### 1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は多岐にわたります。しかし、攻撃の多くは、脆弱性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-2に、2014年10月から12月の期間にIIJ DDoSプロテクション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プロテクションサービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、攻撃の実態を正確に把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*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。

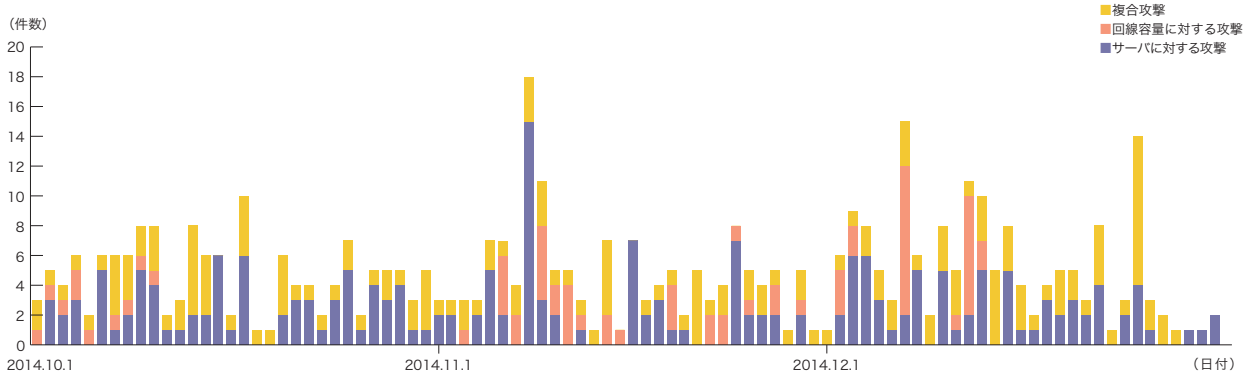



**図-2 DDoS攻撃の発生件数**

*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接続を確立した後、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。

この3ヵ月間でIIJは、381件のDDoS攻撃に対処しました。1日あたりの対処件数は4.14件で、平均発生件数は前回のレポート期間と比べて増加しました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が54.6%、複合攻撃が26.9%、回線容量に対する攻撃が18.6%でした。今回の対象期間に観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大43万2千ppsのパケットによって3.1Gbps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90.8%が攻撃開始から30分未満で終了し、9.2%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、今回最も長く継続した攻撃は、複合攻撃に分類されるもので6時間28分にわたりました。

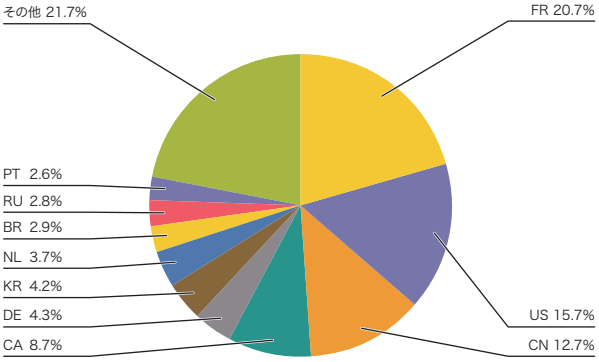



**図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類**

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。

### ■ 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。

2014年10月から12月の間に観測した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35.1%を占めています。次いでDNSで利用される53/UDPが22.8%を占めており、上位2つで全体の57.9%に達しています。また、IRC（Internet Relay Chat）で利用される6667/TCPやHTTPSで利用される443/TCPへの攻撃、通常は利用されない0/TCPや34000/TCP、25565/TCPなどへの攻撃が観測されています。

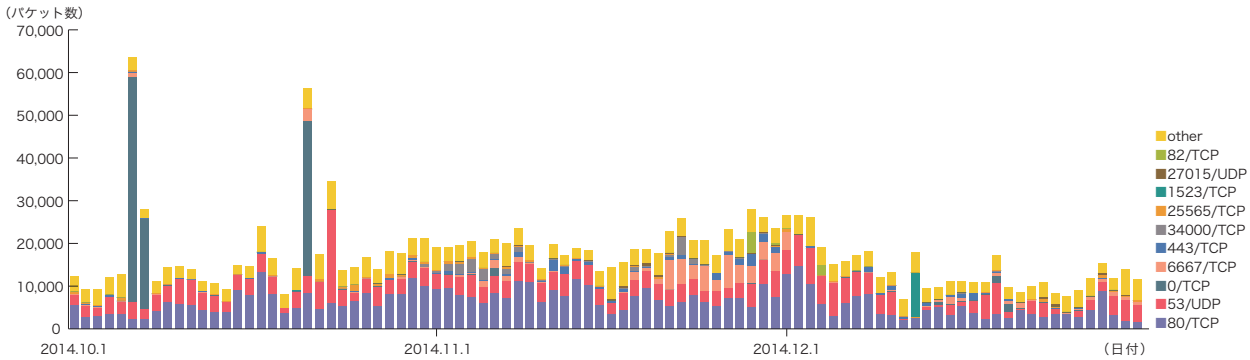



**図-4 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）**

＊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。

＊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/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。

2014年2月から多く観測されている53/UDPは、今回はポート別観測パケット数で2番目の位置にありますが、1日平均は前回の約3,100パケットから増加して約3,900パケットになっています。

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、フランスの20.7%が最も大きな割合を占めています。その後は、米国の15.7%、中国の12.7%といった国が続いています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、Webサーバ(80/TCP)への攻撃としては、10月16日から11月23日にかけてポルトガルのニュースサイト、11月17日から20日にかけてドイツのゲーム関連サイト、10月14日から18日にかけてスペイン語ニュースサイトに対する攻撃をそれぞれ観測しています。10月6日から7日、及び21日には0/TCPへの攻撃を多く観測していますが、広範囲のIPアドレスからのbackscatterを多数のハニーポットで受信しており、攻撃の意図は不明です。他に、10月23日から継続して、フランスのIRCサーバに対する80/TCP、6667/TCP、34000/TCPなど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、10月22日に米国アリゾナ州フェニックス市当局サイトへの攻撃、10月26日にはウクライナの選挙管理委員会への攻撃、11月29日にはフランスの政党サイトへの攻撃をそれぞれ検知しています。

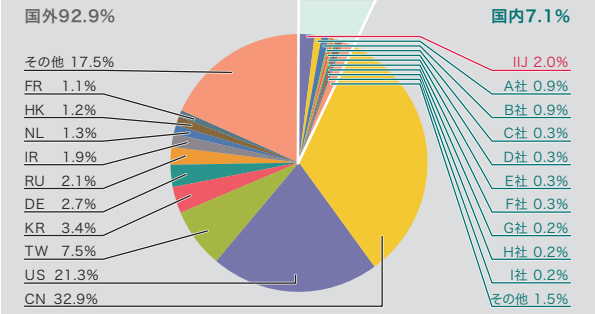



**図-5 発信元の分布(国別分類、全期間)**

### 1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*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。

#### ■ 無作為通信の状況

2014年10月から12月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量(到着パケット数)の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケッ

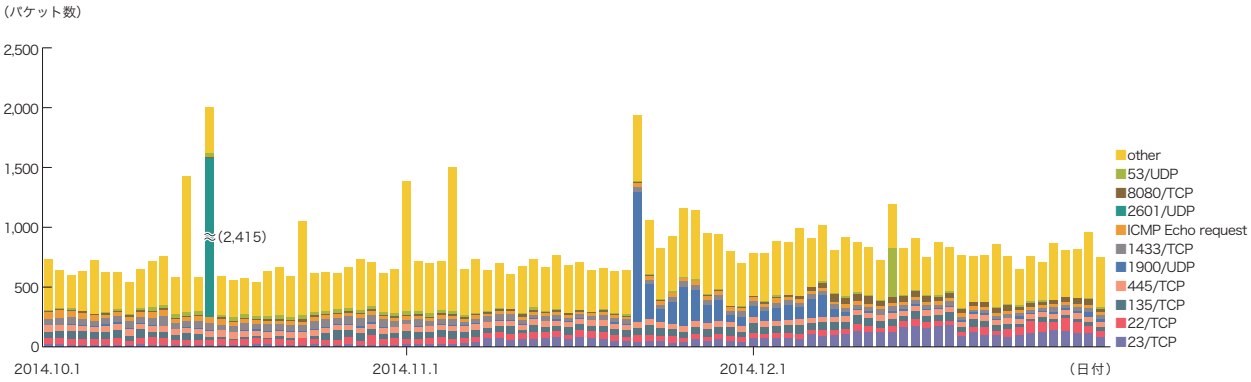



**図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)**

*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。

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、SSHで利用される22/TCP、DNSで利用される53/UDP、Telnetで利用される23/TCP、HTTP Proxyで用いられる8080/TCPに対する探査行為も観測されています。期間中、11月下旬から12月上旬にかけて、UPnPのSSDPに使われる1900/UDPの通信が増加しています。これらのパケットでは、短時間にm-searchリクエストが繰り返し行われていました。これは、発信元を偽装したSSDPリフレクション攻撃(DDoS攻撃の一種)を試みたものであると考えられ、発信元はその標的であったと考えられます[*31]。なお、本件に関しては警察庁が10月に注意喚起を行っています[*32]。

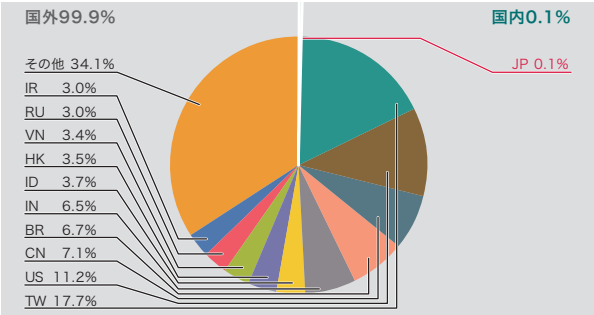



**図-7 総取得検体数の分布**

11月以降telnet(23/TCP)への通信が増加しています。調査したところ、中国及び日本に割り当てられたIPアドレスから主に受信しています。12月5日より、8080/TCPへの通信が増加しています。これは、QNAP製NAS製品などへのShellshockの脆弱性をついた攻撃であると考えてい

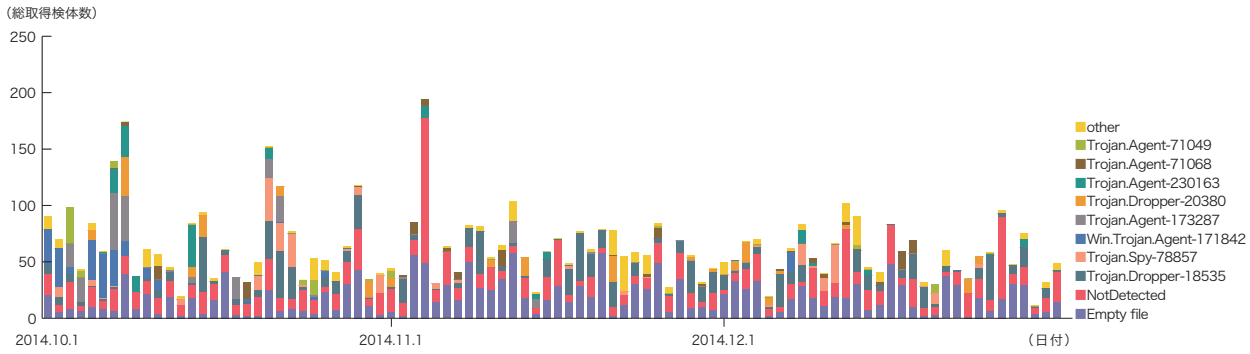



**図-8 総取得検体数の推移(Conficker を除く)**

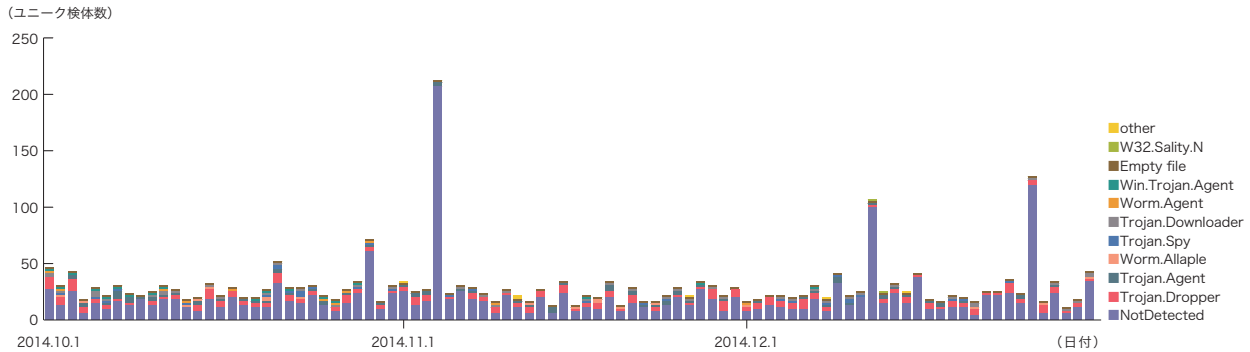



**図-9 ユニーク検体数の推移(Conficker を除く)**

*31 MITFハニーポットはSSDPが無効化されており、攻撃には加担していない。
*32 UPnPに対応したネットワーク機器を踏み台としたSSDPリフレクター攻撃に対する注意喚起について(http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf)。

ます[*33]。12月13日に53/UDPの通信が大量に発生しています。これらのパケットのほとんどはDNS Amp攻撃の試みを受信したためです[*34]。主にドイツの通信会社に割り当てられたIPアドレスが発信元に偽装されていたことから、このIPアドレスが標的になっていた可能性があります。問い合わせ内容は実在するドメインのAレコードの解決要求でしたが、そのFQDNには約250ものAレコードが設定されていました。これにより、送信元を偽装してこの多くのAレコードが設定されたドメインを名前解決することで、応答が増幅されて返るため、結果としてDNS Amp攻撃になります。10月15日に中国に割り当てられた1つのIPアドレスから、特定のハニーポットのIPアドレスに対して2601/UDPに対する通信が行われています。この通信の調査を行ったところ、長さは50バイトから800バイト前後のランダムなデータが短時間に繰り返し送信されていましたが、その意図は不明です。

### ■ 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[*35]の総数を総取得検体数、検体の種類をハッシュ値[*36]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-8と図-9は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行いConfickerと認められたデータを除いて集計しています。

期間中の1日あたりの平均値は、総取得検体数が63、ユニーク検体数が17でした。未検出の検体をより詳しく調査した結果、インドや米国、台湾などに割り当てられたIPアドレスでWormなどが観測されました。また、未検出の検体の約54%がテキスト形式でした。これらテキスト形式の多くは、HTMLであり、Webサーバからの404や403によるエラー応答であるため、古いワームなどのマルウェアが感染活動を続けているものの、新たに感染させたPCが、マルウェアをダウンロードしに行くダウンロード先のサイトが既に閉鎖させられていると考えられます。MITF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93.4%、ダウンローダ型6.6%でした。また解析により、106個のボットネットC&Cサーバ[*37]と7個のマルウェア配布サイトの存在を確認しました。ボットネットのC&Cサーバが大幅に増加していますが、これはDGA(ドメイン生成アルゴリズム)を持つ検体が期間中に出現したためです。

### ■ 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16,343、ユニーク検体数は557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97.0%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。本レポート期間中の総取得検体数は前回の対象期間と比較し、約36%と大幅に減少しています。また、ユニーク検体数は前号から約17%減少しました。Conficker Working Groupの観測記録[*38]によると、2015年1月13日現在で、ユニークIPアドレスの総数は890,845とされています[*39]。2011年11月の約320万台と比較すると、約28%に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。

---

*33 JPCERT/CCの観測でも、同日より探査や攻撃が増加したことを報告している。TCP8080ポートとShellShockを突く攻撃が増加 - JPCERT/CC(http://www.jpcert.or.jp/at/2014/at140055.html)。

*34 MITFハニーポットはDNSの問い合わせパケットを受信しても、権威サーバやキャッシュサーバに問い合わせに行かないため、攻撃には加担していない。

*35 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。

*36 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。

*37 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。

*38 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTrackingblank)。

*39 Conficker Working Groupのデータは何らかの理由により、2014年12月中旬から1ヵ月程度データが欠損しているように見えるため、影響を受けていないと思われる2015年1月13日のデータを引用している。

### 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[*40]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、過去にも度々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。

2014年10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

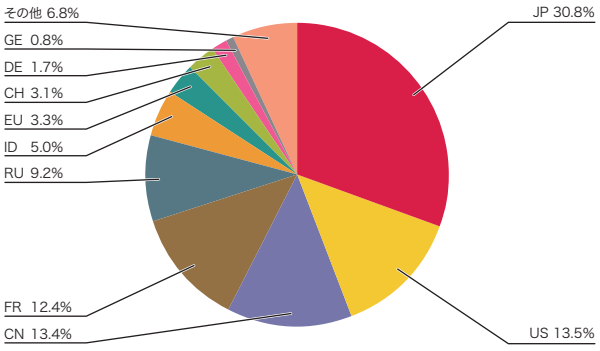



**図-10 SQLインジェクション攻撃の発信元の分布**

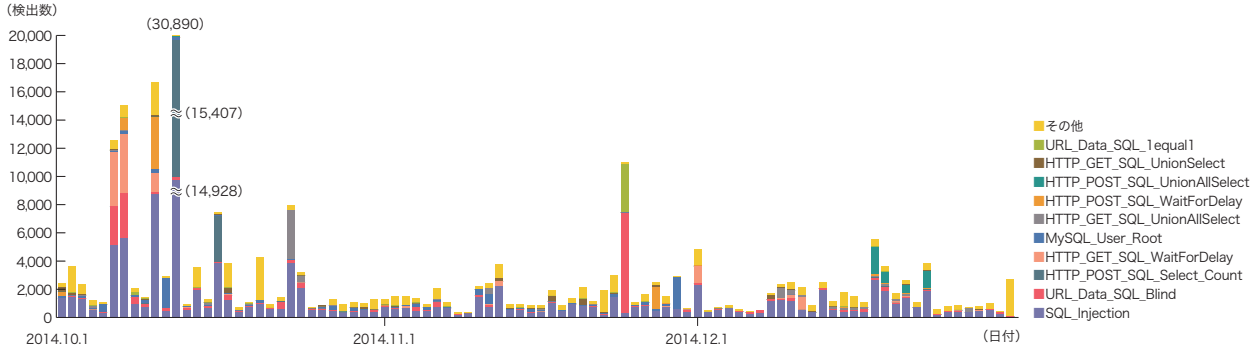



**図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)**

発信元の分布では、日本30.8%、米国13.5%、中国13.4%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に比べて減少しましたが、これは前回期間で中国を発信元とする攻撃が大幅に増加していたことによるもので、全体の検知傾向に変化はありませんでした。

この期間中、10月12日にはフランスの特定の攻撃元より、特定の攻撃先への大規模な攻撃が発生していました。この攻撃先に対する攻撃については、10月10日と10月16日にロシアの特定の攻撃元から、12月18日にインドネシアの特定の攻撃元からの攻撃を確認しています。10月6日には欧米の複数の攻撃元より、特定の攻撃先に対する攻撃が発生しています。10月7日にはチェコの特定の攻撃元より、特定の攻撃先に対する攻撃が発生しています。10月23日にも国内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した。11月24日に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ました。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、攻撃は継続しているため、引き続き注意が必要な状況です。

*40 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。

### 1.3.4 Webサイト改ざん

MITFのWebクローラ(クライアントハニーポット)によって調査したWebサイト改ざん状況を示します[*41]。このWebクローラは国内の著名サイトや人気サイトなどを中心に数万のWebサイトを日次で巡回しており、更に巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

2014年10月から12月の期間に観測されたドライブバイダウンロードは、7月から9月の期間に比べて約3分の1程度に減少しました(図-12)。特に12月は攻撃を観測しない日が多くなっています。攻撃の内訳は前回から続くAnglarと、今回急伸したFiestaによるものが大勢を占めています。Fiestaは他の多くのExploit Kitと同様にInternet Explorerやそのプラグイン、Flash、Java、Silverlightの脆弱性を悪用する機能を備えています。なお、AnglarやFiestaを含む多くのExploit Kitの最近の傾向として、複数の比較的新しいFlashの脆弱性(CVE-2014-8439、CVE-2014-0515、CVE-2014-0497など)を悪用する機能を速いペースで追加していることが挙げられます[*42]。逆に、従来多く狙われてきたJavaの脆弱性を悪用する機能はあまり見られなくなりました。これは、2014年に、Internet Explorerにバージョンの古いJavaの自動実行を遮断する機能が追加されたことや、ChromeやFirefoxではJavaの自動実行そのものが遮断されたことなど、各種のブラウザ環境において、Java関連のセキュリティ機能が改善されてきたためと考えられます。

改ざんされ誘導元となっているWebサイトは、比較的知名度の低い小規模なWebサイトが多く、個々のサイトが数日から約2ヵ月程度の期間、断続的に誘導元として観測されました。コンテンツの傾向としては、成人向け動画コンテンツの紹介サイトが多くみられ、そのほかにはアイドルグループやデザイン事業者のWebサイトなどが改ざんされていました。

全体として、ドライブバイダウンロードの発生率は急激に減少しているものと推測される状況です。ただし、このような傾向は、攻撃者の意図によって急変する可能性が常にあります。Webサイト運営者はWebコンテンツの改ざん対策、閲覧者側はブラウザや関連プラグインなど(特にFlash Player)の脆弱性対策を徹底し、注意を継続することを推奨します。

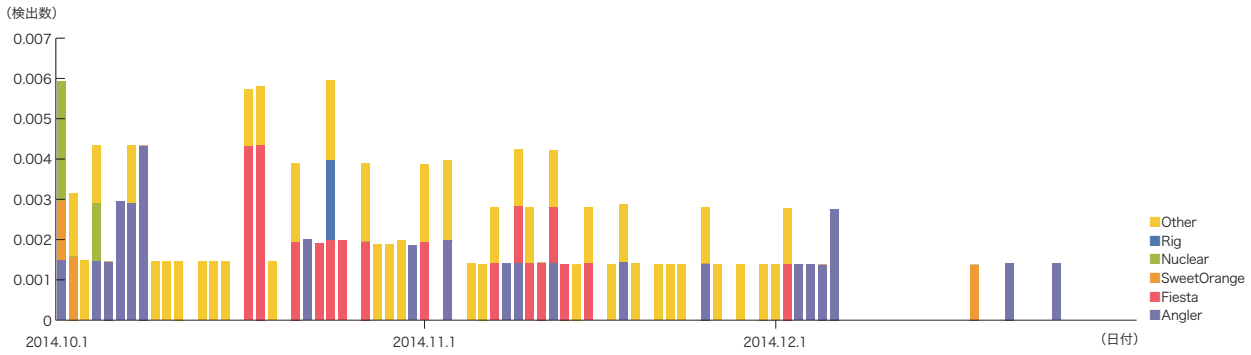



**図-12 Webサイト閲覧時のドライブバイダウンロード発生率**

*41 Webクローラによる観測手法については本レポートのVol.22(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf)の「1.4.3 Webクローラによるサイト改ざん調査」で仕組みを紹介している。

*42 各種のExploit Kitが悪用する脆弱性は「ExploitPackTable 2014」(https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE)に詳しくまとめられている。

## 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、ドメイン名のレジストリ登録情報改ざんの対策、端末のメモリ内に潜む脅威をスキャンするopenioc_scan、ID管理技術の3つのテーマについて紹介します。

### 1.4.1 ドメイン名のレジストリ登録情報改ざんの対策

#### ■ レジストリ登録情報の改ざんによる脅威

インターネットの世界では、ドメイン名が重要な役割を果たしています。例えば、クライアントがwww.example.comにアクセスする際、サーバが属するexample.comゾーンの権威DNSサーバに問い合わせを行い、サーバのIPアドレスを取得します(図-13左)。この一連のやりとりを名前解決と言います。

しかし、名前解決の結果、正規のサーバではなく、攻撃者が用意したサーバにアクセスさせられてしまう攻撃があります。この攻撃はドメインハイジャックと呼ばれ、攻撃手法として、「ドメインの所有者のDNSサーバに不正侵入しレコードを書き換える」「DNSキャッシュポイズニングにより不正なIPアドレスをキャッシュDNSサーバにキャッシュさせる」「BGPに誤った情報を流し、特定のトラフィックを本来のネットワークとは異なるネットワークへルーティングさせる」などが存在します。

このような攻撃手法はISPやサービス提供事業者の対策により影響は少なくなっていますが、異なる攻撃手法によるドメインハイジャックが、国内企業のドメインにおいて、2014年9月以降に複数発生しました。この攻撃手法では、レジストリに登録されているドメイン名に関する登録情報を書き換えることで、名前解決の際に、攻撃者が用意したサーバのIPアドレスを応答させるようにします。この結果、正しいドメイン名を入力しても、攻撃者が用意したサーバにアクセスさせられ、フィッシングやマルウェア感染などの被害に遭ってしまう可能性があります。TLD(Top Level Domain)[*43]の権威DNSサーバに偽の情報が登録されるため、自身のサーバのセキュリティレベルが高くても、攻撃の影響を受けてしまうのが特徴です(図-13右)。なお、偽の情報が登録されるのは、サーバが属するドメインの上位の

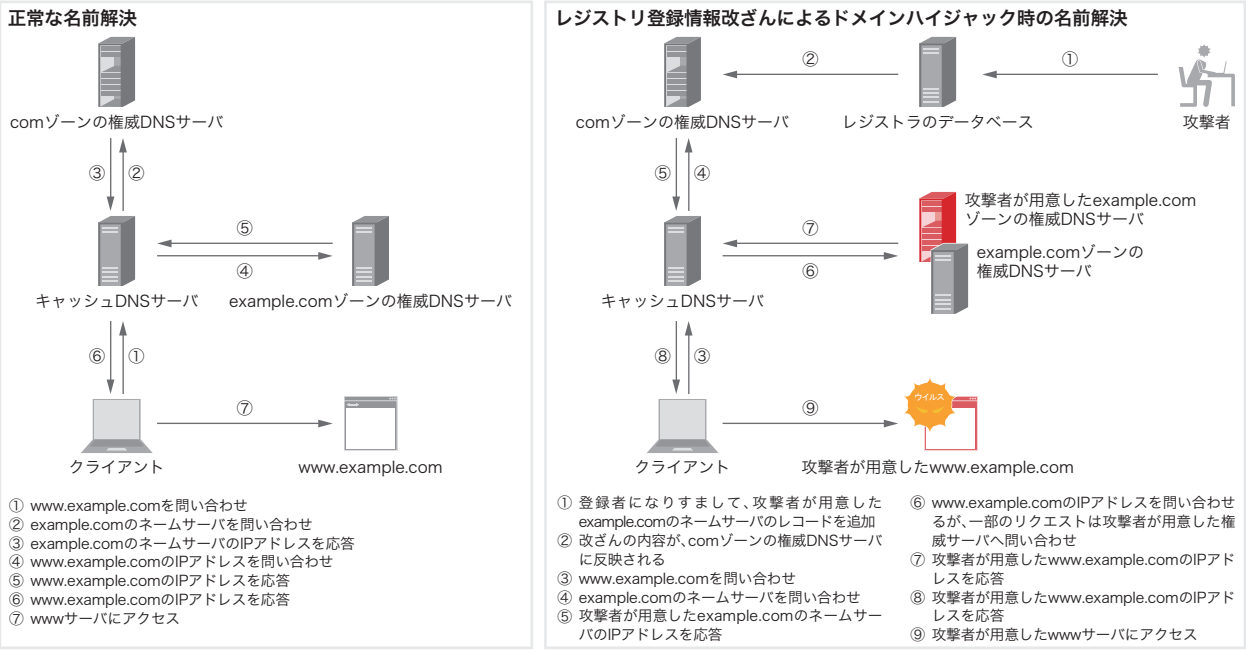



**図-13 www.example.comの名前解決(DNSプロトコルは一部省略)**

*43 「www.example.jp」や「mail.example.com」などドット(.)で区切られた一番右側のラベル(jpやcom)を指す。

権威DNSサーバであればよいため、ドメインの階層が深い場合、TLDではなく、SLD（second-level domain）などの権威DNSサーバに偽の情報が登録される場合があります。

2014年9月から10月にかけて発生したインシデントでは、国内の複数の企業が保有する「.com」ドメインに対して、Webページの訪問者にマルウェアをダウンロードさせようとする攻撃が行われました[*44][*45]。また、2014年11月には海外企業が提供するSNS連携サービスを利用している国内外の大手新聞社やニュースサイトなどで、Webページの訪問者に不正なJavaScriptファイルを読み込ませ、SEA（Syrian Electronic Army）の意匠を表示させるインシデントが発生しました。

なお、2014年11月のインシデントでは、すべてのNSレコードが攻撃者のものに改ざんされ、必ず不正なJavaScriptが読み込まされる状態でしたが、9月から10月の国内企業のドメインのインシデントでは、正規のNSレコードは削除されずに攻撃者のNSレコードの追加だけが行われていました。このため、一部のユーザのみが影響を受ける結果となりました。

今回と同様の手法を使った攻撃は、海外においては既に数多く発生しています。例えば、2013年では、多数のレジストリが攻撃対象となり、毎月のように事件が発生しています[*46]。

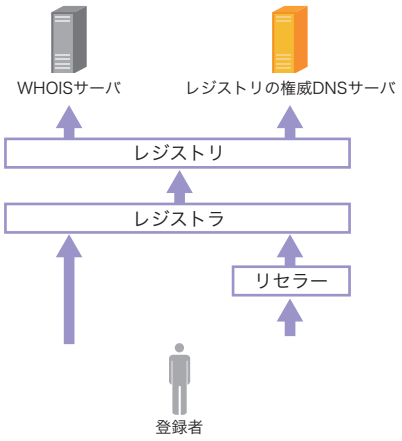
### ■ レジストリ登録情報改ざんの手法

ドメインに関する情報はTLDを運用・管理するレジストリという組織のデータベースに登録されています。ドメインを登録するには、レジストラと呼ばれる仲介業者（またはレジストラのサービスを再販するリセラー）のサービスを利用して、レジストリにドメインの登録申請を行います。ドメインの登録情報は図-14の矢印の順番で受け渡され、レジストリの権威DNSサーバとWHOISサーバに登録されます。

したがって、攻撃者は以下のいずれかのポイントを攻撃することで、レジストリ登録情報の改ざんを行います。

① 登録者やリセラーになりすまして、レジストラのデータを改ざんする。
② レジストラになりすまして、レジストリのデータを改ざんする。
③ レジストリやレジストラのシステム上の脆弱性を利用してデータを改ざんする。

なりすましはドメインの登録者に対するフィッシングやマルウェア感染、ソーシャルエンジニアリングなどで得られた情報を基に行われます。また、レジストリやレジストラのアカウント情報流出やリスト型攻撃が原因となることも考えられます。




レジストリの権威DNSサーバ：ドメインに属するサーバとIPアドレスを紐づけるデータベース
WHOISサーバ：ドメインや登録者の連絡先などのデータベース

④ TLD（Top Level Domain）の管理、運営を行う組織。権威DNSサーバとWHOISサーバにドメイン情報の登録を行う。

③ レジストリに登録者やリセラーからのドメイン情報の登録申請の取り次ぎを行う。

② レジストラのサービスを販売する。レジストラに登録者からのドメイン情報の登録申請の取り次ぎを行う。

① レジストラまたはリセラーにドメイン情報の登録申請を行う。

**図-14 ドメイン情報登録の流れ**

＊44 Democracy in Hong Kong Under Attack | Volexity Blog（http://www.volexity.com/blog/?p=33）。
＊45 IIJではマルウェアに感染した事例を観測していない。
＊46 株式会社日本レジストリサービス（JPRS）、「補足資料：登録情報の不正書き換えによるドメイン名ハイジャックとその対策について」（http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.pdf）。

改ざんされるデータは、レジストリのWHOISサーバに登録されているネームサーバや権威DNSサーバに登録されているNSレコード及びグルーレコードです。

### ■ 対策

以下にレジストリ登録情報の改ざんの対策を説明します。

#### ■ レジストリ／レジストラ／リセラー

最も基本的なセキュリティ対策として、OSやWebアプリケーション、APIなどの脆弱性の修正やパッチ適用が必要です。組織内のクライアントもパッチ適用やアンチウイルスのインストールなどの対策を行わなければなりません。

次に、なりすましに備え、ユーザアカウントの認証機能の改善を検討します。多くのシステムではパスワードによる認証を行っていると思いますので、複雑なパスワードの設定やパスワードの使い回し防止が必要になります。可能であれば、2段階認証やクライアント証明書による認証の導入も検討してください。

また、ユーザアクティビティの監視・通知機能の実装も検討してください。アカウントのログインや登録情報の変更を通知することで、ユーザが意図しない操作に気付くことができます。また、ログインや登録情報変更の履歴があれば、いつ頃から不正アクセスがあったのかユーザ自身でも確認できます。

実際の攻撃に備え、攻撃の検知と対処の体制を整える必要もあります。セキュリティ機器やシステムの負荷やログから攻撃を検知し、適宜、FWなどで遮断します。

最後に、「レジストリロック」の提供を検討してください。これはレジストリの登録情報の変更を制限する機能で、登録情報を変更する際に登録者に追加の認証が必要となるため、意図しない情報の変更を防ぐことができます。

なお、海外のレジストラではFAXによってメールアドレスやパスワードをリセットするサービスが悪用された例もあります。同様のサービスを提供している場合は、サービスの必要性や本人確認フローを見直した方がよいでしょう。

#### ■ 登録者

先に説明したような対策を実施しているレジストリ／レジストラを選ぶことが重要です。レジストラが提供している認証強化や通知機能、レジストリロックなどを積極的に利用してください。また、OSのパッチを適用し、最新版のソフトウェアを利用します。併せて、アンチウイルスもインストールしてください。また、レジストラのアカウントのパスワードは、使い回しをしてはいけません。

通知機能を使用する場合は、通知メールがスパム判定されないように設定します。このとき、連絡用のメールアドレスは、自身が登録しているドメイン以外のものにしてください。仮にレジストリ登録情報が改ざんされても、レジストラなどと連絡を取ることができます。また、WHOISの公開情報に登録者の情報を表示しないオプションがある場合は、有効にすることを検討してください。

更に、定期的に「WHOISサーバ」と「レジストリの権威DNSサーバ」に登録されている情報が改ざんされていないか確認することで、いち早くレジストリ登録情報の改ざんに気付ける可能性があります。WHOISサーバでは「ネームサーバ」、レジストリの権威DNSサーバでは「ドメインのNSレコード及びグルーレコード」を確認してください。

ただし、これらの情報を監視する標準的なツールは存在しないため、各自で作成する必要があります。有志により、いくつかの監視ツールが公開されていることを確認していますが、特定のレコードのみが監視対象となっていたり、レジストリの権威DNSサーバへ直接問い合わせを行わなかったりするなど、使用する場合は事前に十分な動作確認が必要です。

また、監視を行う場合、レジストリの権威DNSサーバとWHOISサーバに必要以上の問い合わせを行わないようにしてください。過剰に問い合わせを行った場合、レジストリに対する攻撃であると判断され、問い合わせが制限または遮断される可能性があります。

### ■ 一般ユーザ

一般ユーザがレジストリ登録情報が改ざんされているか否かを見分けることはほとんど不可能です。したがって、攻撃者が用意したサーバにアクセスしてしまっても、脆弱性が利用されないようにOSのパッチ適用や最新版のソフトウェアと併せて、アンチウイルスソフトウェアを使用してください。

なお、レジストリ登録情報の改ざんではサーバのSSL/TLSの秘密鍵を盗むことはできないため、攻撃者はSSL/TLSで暗号化を行うサービスを提供できません。したがって、普段はHTTPSで提供されているサービスにHTTPでアクセスしていたり、SSL/TLSのエラーが発生している場合は、レジストリ登録情報が改ざんされている可能性が考えられますので、サービスの利用を中止したほうがよいでしょう。

### ■ まとめ

現時点で最も効果的な対策はレジストリロックですが、この機能を提供していないレジストリもいます。また、万が一、レジストリロックが突破されてしまう事態に備えて、レジストリロックの有無に関わらず、これまで説明した対策を実施することで、レジストリ登録情報の改ざんの防止や早期発見することができます。

ユーザ数が多いサービスを提供するドメインほど、被害が大きくなるため、この機会に対策を実施してください。

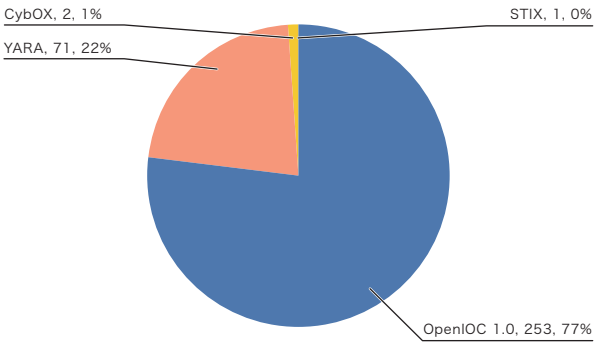



**図-15 IOC Bucketで共有されているIOCフォーマットの数と割合**

## 1.4.2 端末のメモリ内に潜む脅威をスキャンするopenioc_scan

IOC（Indicator Of Compromise）とは、ネットワーク上や端末内に残る、マルウェア感染や不正侵入の脅威を示す痕跡のことです。マルウェア解析やフォレンジック解析の結果に基づいてIOCを定義することで、次回以降同じ脅威を素早く検出することができます。本節では、IIJで新たに実装した端末のメモリ内のIOCをスキャンするツールの紹介と、それを使った汎用的なIOCに関する検討について述べます。

### ■ 実装の背景

IOCという用語は、特定のフォーマットや実装を指すものではありません。IOC Bucket[*47]というサイトでは、複数のフォーマットのIOCが共有されています。図-15は同サイトで共有されているIOCフォーマットの数と割合を示したものです（2015年1月8日時点）。

図から、OpenIOC[*48]が3/4以上の割合を占めており、メジャーなフォーマットとして普及していることが分かります。以前IIJ SECTブログの記事で紹介したとおり[*49]、OpenIOCの定義に基づいてスキャンを行うフリーツールとしてIOC FinderやRedlineがあります。IOC Finderは稼働中のシステムに対してスキャンするツールで、ライブレスポンスを効率的に行うことができます。一方でRedlineは、保全したメモリイメージをオフラインでスキャンします。後者の場合、オフラインなのでマルウェアによる情報の隠蔽を無効化できますし、メモリ上の文字列やアンパック後のコードの特徴を定義できるので、マルウェアの機能に即した定義が可能になります。

これまでIIJでは、OpenIOCとRedlineを活用したマルウェアの早期検出について、検討を行ってきました[*50]。しかしながら、Redlineはクローズドソースのツールであり、機能拡張やバグの修正を自分達で行うことができないという問題がありました。そこで、オープンソースのツールである

*47 有志によって運営されているIOCを共有するサイト。2015年1月8日時点で327のIOCが共有されている（https://www.iocbucket.com/search）。
*48 Mandiant社が推進する規格。IOCはXML形式で記述される（http://openioc.org/）。
*49 記事ではOpenIOCのフリーツールを使った活用例を説明している。「OpenIOCを使った脅威存在痕跡の定義と検出」（https://sect.iij.ad.jp/d/2012/02/278431.html）。
*50 一昨年のSANS DFIR Summit 2013にて、揮発性のIOCを定義して検出する手法に関する発表を行った（https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Volatile-IOCs-for-Fast-Incident-Response-Haruyama.pdf）。

Volatility Framework[*51]のプラグインとして、openioc_scan[*52]を実装しました。

### ■ openioc_scan

openioc_scanの使用方法について説明します。openioc_scanの解析対象はVista以降のWindows OS[*53]のみで、LinuxやMac OS Xは現在サポートされていません。また、実行にはlxml[*54]、ioc_writer[*55]、colorama[*56]の3つのPythonパッケージが必要です。更に、IOCを事前に定義しておく必要があります。openioc_scanは正規表現や後述するparameterをサポートするため、OpenIOC 1.1のフォーマットを利用します。OpenIOC 1.1の定義が可能なフリーツールは、現状PyIOCe[*57]のみです。よってIOCの定義にはこのツールを利用します。

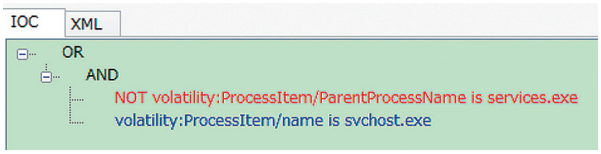



**図-16 PyIOCeを使ったIOCの定義の例**

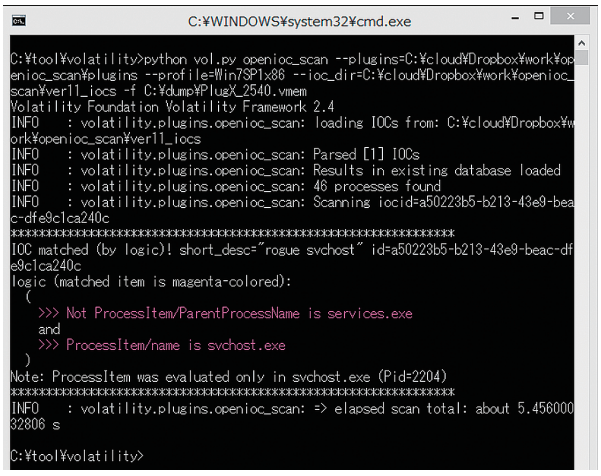



**図-17 openioc_scanの実行**

図-16はPyIOCeの画面の一部です。ユーザはこの画面上でvolatilityのterm(項目)を定義していきます。図ではProcessItem/ParentProcessNameとProcessItem/nameの2つのtermがAND/ORのロジックで組み合わされて定義されています。図のようにNOT(否定)を指定できるほか、大文字小文字の区別、マッチングの指定[*58]なども可能です。

IOCを定義したら、図-17のように、その定義ファイルが存在するフォルダをioc_dirオプションで指定してopenioc_scanを実行します。各termの評価結果をAND/ORで組み合わせた結果、原則的に真になる場合、そのIOCと真になったtermを色付きで表示します。この図では、プロセスIDが2204のsvchost.exeが、条件にマッチしたプロセスであることが分かります。ところで、Volatility FrameworkはRedlineと異なり、メモリイメージの解析結果をキャッシュしませんが、openioc_scanは各termの評価に必要な情報を都度キャッシュするため、同じtermを二度目以降に評価した場合は高速に処理することが可能です[*59]。

openioc_scanがサポートしているtermの一覧を表-1に示します。ProcessItemとDriverItemについては、スキャン対象となるプロセスやドライバは、個別にIOCの定義内容に対して真か偽かを評価されます。例えば、先の例のIOCは1つのプロセス内に閉じて評価されることになります。また、カテゴリの異なるtermを組み合わせた定義を行うことも可能ですが、組み合わせによってはパフォーマンスが著しく低下する場合があるので[*60]、定義内容はできるだけ1つのカテゴリのtermのみをシンプルに定義していくほうが良いでしょう。

先程、「各termの評価結果をAND/ORで組み合わせた結果、原則的に真になる場合、そのIOCと真になったtermを色付きで表示します」と書きました。実は、termのAND/ORの最終結果が真でない場合でも、IOCを表示する方法があります。

*51 オープンソースのメモリフォレンジックツールであり、有志によって様々なプラグインが提供されている(https://github.com/volatilityfoundation/volatility)。
*52 以下で最新版を配布している(http://takahiroharuyama.github.io/blog/2014/08/15/fast-malware-triage-using-openioc-scan-volatility-plugin/)。
*53 実際には通信情報以外の項目についてはXPや2003のメモリイメージもスキャンできるが、十分な検証を行っていないため、サポート対象外とした。
*54 XMLをパースするためのパッケージ(https://pypi.python.org/pypi/lxml/3.2.1)。
*55 OpenIOC 1.1の項目をパースするためのパッケージ(https://github.com/mandiant/ioc_writer)。
*56 コンソールの出力文字の色を変更するためのパッケージ(https://pypi.python.org/pypi/colorama)。
*57 Sean Gillespie氏によるオープンソースツール(https://github.com/yahoo/PyIOCe)。
*58 スキャン対象が文字列か数値などによって、is/contains/matches/starts-with/ends-with/greater-than/less-thanという指定が可能。matchesでは正規表現を指定する。
*59 文字列の抽出など、時間のかかるtermに関係する情報のみをキャッシュする。termの種類が同じであれば、その値を変更したとしても高速に処理される。
*60 例えば、ProcessItemやDriverItemは繰り返しの処理が多いため、それらのカテゴリに属するtermを組み合わせた定義を行うと実行時間が長くなる傾向にある。

OpenIOC 1.1ではparameterという概念を使い、termごとにメタデータを定義することができます。openioc_scanはそのparameterを用いて、スコアリングでの評価をサポートしています。例えば、先の例のIOCを評価した際、片方のtermのみ真であっても、parameterとして定義したスコアが閾値を超えている場合、そのスコアに基づきIOCにマッチしたことが表示されます。具体的には、parameterにセットされていたscoreが整数値で合計100を超える場合、図-18のように該当するIOCが表示されます。openioc_scanはそのほかにdetailやnoteというparameterをサポートしています*61。

**表-1 openioc_scanがサポートしているterm**

| termのカテゴリ | termの種類 |
|---|---|
| ProcessItem | プロセス名、パス名、引数、親プロセス名、DLLパス名、DKOM*62の有無、コードインジェクションの有無、利用API名、文字列、ハンドル名、ネットワーク接続情報、フックされたAPI名、有効な特権のタイプ |
| RegistryItem | OS による実行ファイルのアクセス履歴(ShimCache*63) |
| ServiceItem | サービス名、記述名、コマンドライン |
| DriverItem | ドライバ名、利用API名、文字列、IRP function table*64 フック、コールバック関数のタイプ、タイマー関数の有無 |
| HookItem | フックされたSSDTエントリ*65 |
| FileItem | MFTエントリ*66に基づいたファイルのメタデータ各種 |

### ■ 汎用的なIOCに関する検討

一般的にIOCは、既知の脅威を検出する目的で利用されます。その最も大きな理由として、従来のIOCの大半が、マルウェアのMD5やC&Cサーバ のURLなど、未知の脅威を検出するために再利用しにくい定義内容であったことが挙げられます。そこでIIJでは特定のマルウェアやインシデントに依存しない、openioc_scanのための汎用的なIOCについて検討を行いました。

表-2に検討結果をまとめます。汎用的な定義である以上、誤検出を完全に避けることはできないため、誰しもが今回検討したIOCを使って未知の脅威を検出できるわけではありませんが、更なる詳細な解析を行っていくための優先順位

```
**************************************************************
IOC matched (by score)! short_desc="rogue svchost" id=a50223b5-b21
logic (matched item is magenta-colored):
  (
    Not ProcessItem/ParentProcessName is services.exe
    and
    >>> ProcessItem/name is svchost.exe (score=100;)
  )
Note: ProcessItem was evaluated only in svchost.exe (Pid=752)
**************************************************************
```

**図-18 parameterの利用例**

**表-2 汎用的なIOCに関する検討結果**

| IOCの定義 | 検討内容 | 制限 |
|---|---|---|
| 異常な実行パス | Recycle.BinやUsers¥Publicなど、通常ではあまり使われないフォルダをパスに含む実行ファイルを検出 | 実行中のプロセスに対しては有効だが、アクセス履歴に対しては誤検出が多い |
| Webインジェクション | HttpSendRequest APIがすべてフックされているプロセスを検出 | マルウェアが行うフックの種類によっては検出漏れが発生*67 |
| コードインジェクション | メモリ領域の特徴や利用されるAPIなどから、コードインジェクションされたプロセスを検出 | wow64プロセスに対しては検出不可*68 |
| Position Independent Code(PIC)*69 | PEB*70へのアクセスやGetPC*71などのコードシーケンス、API名のハッシュの即値などを検出 | GetPCは誤検出が発生、API名のハッシュ値は検索の負荷が大きい |
| UACダイアログのバイパス | UACダイアログのポップアップを抑制するコードシーケンスを検索 | 定義したのは1つの手法のみで、抑制する手法は他にも存在 |
| NTFSの特殊な領域にデータを格納 | NTFSのExtended Attribute*72を読み書きするプロセス、ドライバを検出 | ドライバの評価では誤検出が発生 |
| 標的型攻撃の横展開 | 横展開で用いられる攻撃ツールを検出 | ファイル名などのメタデータに頼りがち、汎用的な定義が困難 |

*61 detailはマッチした文字列が一部の場合、その全体の文字列を表示するparameterで、値にonを指定する。noteはtermごとのコメントを残したいときに使う。以下のページで具体的な設定方法を解説している(http://takahiroharuyama.github.io/blog/2014/10/24/openioc-parameters-used-by-openioc-scan/)。
*62 Direct Kernel Object Manipulationの略。ここではカーネルが保持するプロセスのリンクリストを改ざんすることで隠されたプロセスのことを指す。
*63 HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatibility\AppCompatCacheもしくはHKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCacheに存在するレジストリ値。
*64 IRPとはI/O Request Packetsの略であり、ドライバごとに設定されるバッファの読み書きなどの操作のための関数テーブルをIRP function tableという。
*65 System Service Descriptor Tableの略。SSDTエントリとはシステムコール名のこと。
*66 MFTとはMaster File Tableの略であり、MFTエントリとはNTFSファイルシステムで管理されるファイルやフォルダごとに作成されるメタデータのこと。
*67 Volatility Frameworkはinlineフックについては最初の3命令までしかチェックしないため、4命令以降にフックを埋め込まれた場合は検出できない。
*68 Volatility Frameworkの仮想アドレス変換機構の制限による。
*69 シェルコードなどの、実行コンテキストに依存せず動作可能なコードのこと。
*70 Process Environment Blockの略。利用するAPIへのアクセスに必要な情報。
*71 Get Program Counterの略。現在の実行位置を取得するためのコードのこと。
*72 OS/2アプリケーションとの互換性のために使われるデータ領域のこと。

づけ(トリアージ)という観点では、ある程度活用できるという感触を得ました。一方、Volatility Framework自体の機能の制約によって、検出漏れが発生しているケースも見受けられました。

■ まとめ

本節ではopenioc_scanの紹介と、それを使った汎用的なIOCに関する検討結果について述べました。検討によって、Volatility Frameworkの機能に由来する制約が判明しましたが、Redlineとは異なりオープンソースなので、各ユーザで自由にそれを修正及び拡張することは可能です。

メモリイメージに対してIOCをスキャンするという考え方以前に、IOC自体を活用しているアナリストはまだまだ少ないように思います。今後インシデントレスポンスで解析対象とする端末の数、メモリやディスクの容量は、増加の一途をたどることは容易に推測できますし、経験豊富なアナリストは既に既存の手法の限界を感じているかもしれません。効率的にインシデントレスポンスを行っていくために、openioc_scanを使って脅威の検出やトリアージを試みてはいかがでしょうか。

### 1.4.3 ID管理技術

2014年も、事件・事故などで漏えいしたユーザIDとパスワードのリストを用いたとみられる不正ログインが後を絶たない状況が続きました。そのためID・パスワードだけを用いた認証方式は危険であるという認識が拡がり、他の認証方式を併用するなど新しいID管理技術が注目されています。そこで本節では、ID管理(Identity Management)技術について取り上げます。ID管理技術は、IDの発行・利用・廃棄と言うライフサイクルに関する技術だけでなく、利用者認証、クレデンシャルの発行・利用、属性情報の管理・流通、各種リソースに対するアクセス制御、権限移譲、そしてこれらの情報を異なる主体間で連携させる技術など非常に多岐に渡る概念を指すことがあります。そのため、インターネット上で利用されるID管理・ID連携に関連する仕様も多様化しており、それぞれが様々な考え方に基づき策定されているため、利用環境に応じて適切なものを選択する必要があります。しかし、使用されている技術用語がまちまちであることや仕様がカバーする範囲も多様化していることから、残念ながら非常に分かりにくい分野になりつつあります。本節では、特定の仕様に関する解説をできるだけ避け、ID管理技術に関する一般的な考え方を解説することで、技術導入のための助けになることを目指します。

■ IDの考え方～実体と識別子

アイデンティティについて非常に多くの考え方・定義・思想があり、これが技術者・利用者を混乱させる原因になっています。そこで本稿ではIDを識別子(Identifier)として捉えるシンプルな考え方を導入します。

現実世界の実体はデジタル世界のエンティティと結び付けられます。現実世界の実体の例としては、何らかのサービスを利用しようとするユーザが挙げられますが、IoT(Internet of Things)に代表されるように能動的に他のノードと繋がろうとする機器もIDを持つことがあります。このとき、デジタル世界のエンティティを識別(identify)するために、ユニークな識別子(Identifier＝ID)が割り当てられます。IDはあるレルム(Realm;領域)ごとに定められる識別子空間(Identifier Space)上の元と捉えることができます。IDのユニーク性は、当該レルムにおいて異なるエンティティであれば、異なるIDが割り振られることを意味します。

現実世界の実体は複数のレルムにおいて、それぞれ異なるIDを持つことが一般的です。また、現実世界の実体が同じレルムにおける複数のIDと結び付けられることもしばしばあります。しかしデジタル世界においては、IDが異なれば、それらは異なるエンティティと認識されます。例えば、現実世界の実体であるAさんは、メールアドレスとしてa@aaa.exampleとa@bbb.exampleのように2つの異なるレルムaaa.example、bbb.exampleにおいてそれぞれのIDを持つことがあります。また、Aさんはレルムaaa.exampleにおいて、a@aaa.exampleだけでなくa1@aaa.exampleのように同じドメインに異なるメールアドレスを持つケースがあります。このように現実世界においては同じ実体に、デジタル世界においては異なるレルムに複数のIDが割り振られることもあることが分かります。

■ トークン・クレデンシャルと認証(Authentication)

前述したようにデジタル世界においてIDを用いることで異なるエンティティを識別できることが分かります。しかしIDは公開情報であるため、誰でも自分がそのIDを持つ

エンティティだと言い張っては困ります。そこで、デジタル世界において今アクセスしているエンティティが本当にそのIDが割り振られたエンティティであるかどうかを認証（Authentication）する仕組みが必要となります。そのために当該IDに呼応したパスワードなどの秘密情報が必要となります。

本節ではNIST SP800-63[*73]の定義に沿ってクレデンシャル[*74]とトークンを区別して説明することにします。トークンは"Something you know"、"Something you have"、"Something you are"の3つで代表されるように当該IDが割り当てられたユーザが持つ秘密にすべき情報を指します。トークンとしては例えば、パスワードや公開鍵暗号方式で利用される秘密鍵、ICカードやドングルなどの物理的媒体、指紋や虹彩などバイオメトリクス認証で用いられる身体情報などがあります。一方でクレデンシャルはトークンとIDとの結び付けを指し示す公開情報です。場合により、クレデンシャルは信頼のおけるエンティティからお墨付きを得ており、第三者がその正当性について検証可能な情報となります。トークンの一種であるパスワードに対応するクレデンシャルは、認証子であるIDそのものと捉えることができます。SSL/TLSなどで利用される公開鍵暗号系の認証方式を考えると、X.509証明書[*75]がクレデンシャルであり、証明書に含まれる公開鍵に呼応する秘密鍵がトークンに該当します。また、SSL/TLSサーバ証明書にはFQDNが含まれており、これをIDと捉えることができます。BitcoinアドレスはIDと捉えることができますが、アドレスそのものが公開鍵であり、アドレスだけでトランザクションの署名検証が可能なことから、Bitcoinアドレスはクレデンシャルとも捉えることができます。

1つの{トークン・クレデンシャル}の組を用いた認証ではなく、複数の{トークン・クレデンシャル}を用いて、あるIDが割り振られたエンティティを認証する方式を多要素認証と呼びます。一般的には並列の多要素認証方式、つまりそれぞれの認証方式において独立したトークンを用いる方法が知られています。一方で直列の多要素認証方式という考え方もあります。例えば、公開鍵暗号方式における秘密鍵をトークンとして使用する場合、秘密鍵ファイルは暗号化しておくことが一般的ですから、復号するためにパスワードの入力が必要になります。このとき、トークンとしてパスワードと秘密鍵の2つを利用する直列の多要素認証方式と捉えることができます。ICカードとPINコードも同様です。また、トークンのうち"Something you have"に属するハードウェアトークンでは、物理的媒体に表記された定期的に表示が更新されるワンタイムパスワードをトークンとして提示し、多要素認証の1つとして利用されることが一般的です。ネットワーク型としてはLamportによるハッシュチェーンを用いたワンタイムパスワード方式[*76]が知られておりS/Keyなどとして仕様[*77][*78]が策定されています。ワンタイムパスワード方式は、従来のID・パスワード方式の置き換えや併用により、近年のリスト型攻撃への対策案[*79]の1つとして期待されています。

### ■ 認証と認可（Authorization）の違い

デジタル世界においてユーザがログインする、もしくはサーバがあるIDを持つエンティティを認証することは最終的な目的ではありません。サーバはユーザを識別した後に、しかるべきサービスを提供したり、各種リソースにアクセスできるようにするために認証が行われます。エンティティの確からしさを確認した上で、当該IDを持つエンティティに対して権限を与えることを認可（Authorization）と呼び、認証（Authentication）とは分離して考えます。認可とは、あるIDに対して適切なアクセス権を付与することにほかなりません。その際にはポリシー（Policy）があることが前提となり、ポリシーに基づきあるIDに対して権限を付与するエンティティ PDP（Policy Decision Point）とその決定された結果を実際に適用するエンティティPEP

＊73 NIST Special Publication 800-63-2、Electronic Authentication Guideline（http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf）。参考情報としてIPAによる日本語訳がある（https://www.ipa.go.jp/files/000025342.pdf）。
＊74 認証に用いられるあらゆる情報の総称としてクレデンシャルという用語が利用されることもあるが、本節では公開情報と秘密情報の観点で明確に分類すべきという立場で利用する。
＊75 ITU-T Recommendation X.509 | ISO/IEC 9594-8, Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
＊76 Lamport、"Password Authentication with Insecure Communication"。Communications of the ACM 24.11, November 1981, pp.770-772.
＊77 N. Haller、"The S/KEY One-Time Password System"（http://tools.ietf.org/html/rfc1760）。
＊78 N. Haller et al.、"A One-Time Password System"（http://tools.ietf.org/html/rfc2289）。
＊79 総務省、「リスト型攻撃対策集について」（http://www.soumu.go.jp/main_content/000265404.pdf）。

(Policy Enforcement Point)の2つに役割を分ける考え方があります[*80]。あるIDに権限を付与するアクセス制御方法にはRBAC(Role-Based Access Control)[*81]やABAC(Attribute-Based Access Control)[*82]などがあります。これらの方式には、IDに対して直接権限を付与するのではなく、IDに紐付けられた属性情報から判断して権限を付与するという考え方が導入されています。これら2方式の大きな違いは、RBACがロールと呼ばれる属性値が固定化されている属性情報を扱うのに対し、ABACではアトリビュートと呼ばれる属性値が定められた範囲の元を取り、その値がどの範囲に属しているかによって権限を変更するという設定方法が採用されています。例えば、役職や性別による判断はRBAC、年齢や期間・時刻による判断はABACの考え方に基づいてアクセス権限が与えられます。認可のために使われる属性情報は、ID付与や認証を行うエンティティが管理する場合もありますが、属性情報を管理するエンティティ(Attribute Authority)がクレデンシャルを発行してIDと属性情報を紐付ける方法もあります。クレデンシャルにして属性情報を流通させるメリットは、アクセス権限を得るためにユーザが開示すべき属性情報のうち、本来ならば不必要な情報までサービス提供者に流れることを防ぎ、最低限の属性情報のみを提示してサービス提供を受けることができるようになる点です[*83]。図-19は、トークンを用いた認証から各種クレデンシャルの流通、アクセス権限付与までの一連の流れを示した概念図を表しています。

### ■ ID連携技術

一度の認証で複数のレルムにおけるサービスが利用できるシングルサインオンを実現するためにID連携と呼ばれるフレームワークがいくつか存在しています。今回はSAML(Security Assertion Markup Language)[*84]における考え方を中心に説明します。SAMLにおける役割は(1)ID付与や認証に関する業務を行うIdP(Identity Provider)、(2)IdPが発行するクレデンシャルを信用して受け入れるRP(Relying Party)/SP(Service Provider)、(3)利用者であるEnd Userの3つに分けることができます。End UserはSPのサービスを利用する際にクレデンシャルを提示することでサービスを享受します。このときクレデンシャルを発行するのがIdPであり、SPで定められたポリシーに基づいてアサーション(Assertion)と呼ばれるクレデンシャルが要求されIdPにより発行されます。SAMLではアサーションのデータ形式だけでなくブラウザがEnd Userとして振る舞う場合の動作についてプロトコルが定められています。クレデンシャル(アサーション)の種類としては認証結果に関する情報だけでなく、属性情報を保証する情報や、更に認可決定に関する情報についても流通させることができます。このとき図-19のように、認証に関わるクレデンシャルを発行する機関を狭義のIdPとし、属性情報に関するクレデンシャルを発行するAttribute Authority、認可決定に関するクレデンシャルを発行するPDPと役割を細分化して考えることができます。また、SPがPEPの役割にあたりますが、実装によってはPDPでのアサーション発行を省略しPDPとPEPの両方の役割をSPが担当することも考えられます。

OpenID[*85]もSAMLと似たような考え方に基づくフレームワークであり、前述した狭義IdPやAttribute Authorityの役割としてOpenID Provider(OP)と呼ばれるエンティティが発行したクレデンシャル(Claimと呼ばれます)をRPが検証する仕組みで属性情報の流通を可能にしています。事前にOPとRPが連携しない状況でも運用可能であり、RP・OPがそれぞれ適したOP・RPを発見するディスカバリサービスに関する拡張仕様も用意されています。更に、権限委譲に関する仕様も策定されており、OAuth[*86]はリソースにアクセスするためのトークンを保持している利用者が、秘密情報であるトークンを開示することなく代理人に権限のみを一時的に付与する仕組みを提供しています。技術用語が違うため混乱しますがResource Ownerと呼ばれる利用者がClientと呼ばれる代理人に、秘密情報を渡すことなく

*80 OASIS、"eXtensible Access Control Markup Language3 (XACML) Version 2.0"(http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)。
*81 David Ferraiolo、Richard Kuhn、"Role-Based Access Controls"、15th National Computer Security Conference(http://csrc.nist.gov/rbac)。
*82 NIST、Attribute Based Access Control (ABAC) Overview(http://csrc.nist.gov/projects/abac/)。
*83 更に、IDも仮名(Pseudonym)を用いてアクセス権限を得る考え方もあるが、本節では触れない。
*84 OASIS、Security Assertion Markup Language(SAML)(http://xml.coverpages.org/saml.html)。
*85 OpenID Foundation、OpenID specifications(http://openid.net/developers/specs/)。かつて策定されていたOpenID Authenticationなどの仕様群は廃止され、OAuth 2.0をベースにしたOpenID connect 1.0に統合されている。
*86 D. Hardt、"The OAuth 2.0 Authorization Framework"(http://tools.ietf.org/html/rfc6749)。OAuth 2.0周辺仕様は、以下のページ(http://tools.ietf.org/wg/oauth/)で策定されている。

Access tokenと呼ばれる認可情報を含むクレデンシャルをAuthorization Serverと呼ばれるPDPが発行することで代理人がリソースにアクセスすることを可能にしています。

このように、今後も新しいモデルに基づいた様々な仕様が策定されると考えられますが、今回紹介したID・トークン・クレデンシャルと認証・認可・アクセス制御という一般的な考え方を知っておくことで新仕様の理解の一助となれば幸いです。

## 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、ドメイン名のレジストリ登録情報改ざんの対策、端末のメモリ内に潜む脅威をスキャンするopenioc_ scan、ID管理技術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。

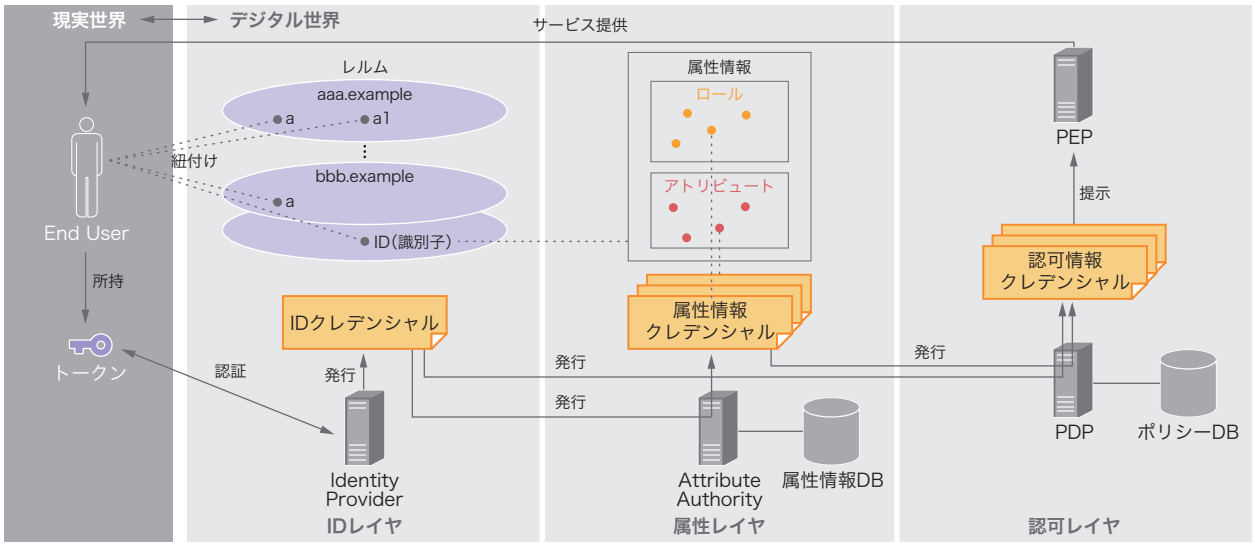



**図-19 トークンを用いた認証から各種クレデンシャルの流通、アクセス権限付与までの一連の流れ**

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**(1.2 インシデントサマリ)
**土屋 博英、永尾 禎啓、鈴木 博志、梨和 久雄**(1.3 インシデントサーベイ)
**小林 稔**(1.4.1 ドメイン名のレジストリ登録情報改ざんの対策)
**春山 敬宏**(1.4.2 端末のメモリ内に潜む脅威をスキャンするopenioc_scan)
**須賀 祐治**(1.4.3 ID管理技術)
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:
**小林 直、加藤 雅彦、根岸 征史、桃井 康成** 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