SOCレポート

1.1 情報分析基盤の刷新

IIJでは2016年度から、お客様により良いサービスを提供するために、人材面・システム面・業務面からセキュリティ事業の強化に取り組んでいます。システム面の強化の取り組みの1つが、セキュリティに関する情報を包括的に分析するための「情報分析基盤」の刷新です。情報分析基盤の目的は、高度化するサイバー攻撃に対してIIJサービスログなどのデータを多角的に分析することで、マルウェアなどによる悪性活動を検出して、セキュリティ脅威の適切な予防措置と事後対処に活用していくことです。

情報分析基盤を活用することで、これまで発見が困難であった高度なサイバー攻撃を早期に発見できるようにしていきます。情報分析基盤の3つの特徴を、「(1)ISPならではのデータ収集・分析」「(2)企業の実活動から得られるデータ」、「(3)IIJ独自ビッグデータ基盤による分析」として説明します。

■ (1)ISPならではのデータ収集・分析

攻撃者は、機器の脆弱性などを悪用して攻撃を仕掛けてくるだけではなく、利用者のミスを誘発することで攻撃を成功させようとします。このため、単一のセキュリティ機器だけではサイバー攻撃の発生を検出できない場合があります。高度化するサイバー攻撃に対抗するには、異なるセキュリティ機器の多層防御が有効であり、サイバー攻撃を検出するにあたっても同様に検出機器の多層化が有効です。情報分析基盤では、サイバー攻撃を検出するために様々なログを多角的に分析します。収集・分析するログとしては、IIJサービスとして提供しているファイアウォールやIPS/IDS、アンチウイルスなどのセキュリティ機器のログはもちろんのこと、Webアクセスやメール送受信のログも対象としています。更に、ISPならではの分析データとしてバックボーントラフィックやDNSクエリなどのログも対象としています。これらの多様なログを収集・分析することで、これまで発見が難しかったマルウェアの悪性活動などを検出できるようにします。

■ (2)企業の実活動から得られるデータ

情報分析基盤では、サイバー攻撃の検出をハニーポットやクローラなどの調査データだけでなく、IIJサービスのログも活用して行っています。IIJサービスは、企業の実業務の活動に利用されており、この実活動で遭遇するサイバー攻撃に関するデータを活用することができます。例えば、IIJセキュアWebゲートウェイサービスやIIJセキュアMXサービスからは、Webアクセスログやメールログ、アンチウイルス検査結果ログといった国内企業100万アカウントを超えるユーザの活動に関するログを収集・分析することができます。これらの日本企業の実業務のデータを収集・分析することで、日本を狙った標的型攻撃や、不特定多数に対する攻撃のキャンペーン動向などを分析することが可能となります。

■ (3)IIJ独自ビッグデータ基盤による分析

高度なサイバー攻撃では、被害組織に気付かれることなくマルウェアを潜伏させて機密データを搾取し続けます。0-Day攻撃などで初期潜入されるのは避けられない事象だとしても、如何に早期に気付くことができるかが、被害を受けるかどうかの分かれ目になります。図-1は情報分析基盤のアーキテクチャ概要を示しています。情報分析基盤は、オープンソースであるHadoopをベースにIIJ独自のビッグデータ基盤として構築しています。この独自基盤は、毎秒数十万を超える各種ログを論理的なフィールドと値の組に分解してデータベースとして多角的に分析できるようにしており、更にデータベース化されたログを分析するときにも十分な速度で解析結果を得られるようにしています。また、高度化・複雑化を続けるサイバー攻撃に

対応できるように、取り込みデータ種別の拡張や性能向上に対応できるアーキテクチャとして構築しています。情報分析基盤により、膨大なデータからマルウェアなどによる悪性活動を早期に発見することができるようになります。

情報分析基盤のアウトプットには、C&Cサーバのブラックリストといったレピュテーション情報や攻撃観測データなど様々なものがあります。アウトプットの1つである攻撃観測データについては、セキュリティ情報発信サイト「wizSafe Security Signal(ウィズセーフセキュリティシグナル)」[*1]にて2017年10月より発信を開始しています。

wizSafe Security Signalでは、定期観測データを毎月公開するだけではなく、セキュリティ情報をブログ形式でタイムリーに発信しています。

次項からは、この半年間にwizSafe Security Signalで報告してきた内容の中から、情報分析基盤を活用して明らかになった活動について詳述します。特に目立ったのは、仮想通貨マイニングサービス、DDoS攻撃、ApacheStruts2の脆弱性を狙った攻撃の3つです。

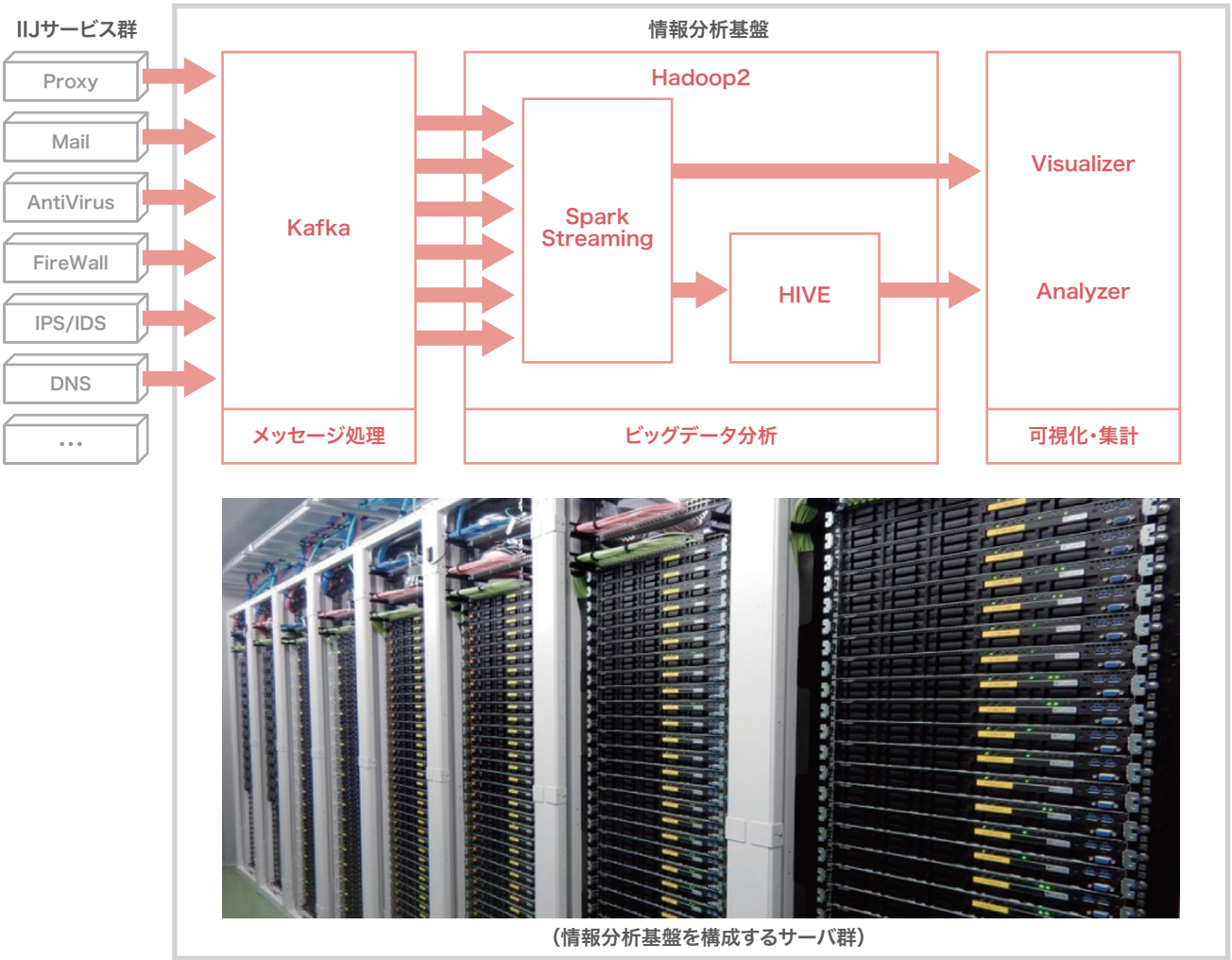

図-1 情報分析基盤のアーキテクチャ概要

＊1　wizSafe Security Signal ～ 安心・安全への道標(https://wizsafe.iij.ad.jp/)。

1.2 仮想通貨マイニングサービス

2017年はBitcoinなどの仮想通貨の暴騰が話題となった年でもありました。Bitcoinを例にすると、年初から年末までで、およそ20倍の値上がりを記録しています。Bitcoinなどの仮想通貨は、その送金及び受け取りの利便性と匿名性からランサムウェアの金銭要求で数年前から悪用されており、例えば、2013年に発見されたCryptlockerというランサムウェアにおいて、身代金の支払い方法の1つとしてBitcoinを要求しています。ランサムウェアの多くは身代金要求に仮想通貨を要求していますが、仮想通貨を金銭のやり取りに利用するだけでなく、マイニング（採掘）行為を実行させるマルウェアも存在しています。マイニングを実行させるマルウェアを大量感染させた数千台のボットネットを構築した事例[*2]もありました。

2017年9月14日にCoinhiveという仮想通貨マイニングサービスが始まりました。CoinhiveはMoneroという仮想通貨を、JavaScriptを使ってマイニングできるサービスです。Webサイト運営者がマイニング用JavaScriptをWebサイトに埋め込むことで、Webサイト閲覧者のPC端末のCPUリソースを活用してMonero仮想通貨のマイニングが行われます。Coinhiveでは、マイニングにより得られた収益のうち70%がWebサイト運営者に配布される仕組みになっています。仮想通貨の暴騰もあり、Web広告に変わる収益源として、Coinhiveサービスを利用するWebサイト運営者が増えてきています。また、このような仮想通貨マイニングサービスはCoinhive以前より存在していましたが、Coinhiveに続くように、CloudcoinsやCoinlabなどJavaScriptを使った仮想通貨マイニングサービスが次々と登場してきています。

一方で、攻撃者がJavaScriptを使った仮想通貨マイニングサービスを悪用する事例[*3]も見つかっています。

攻撃者は、Webサイトを改ざんして、マイニング用JavaScriptを埋め込むことで、Webサイト閲覧者のPC端末でマイニングされた仮想通貨から収益を得ます。マイニング用JavaScriptによっては、CPUリソースを大量に消耗するものもあり、Webサイト閲覧者のノートPCやスマートフォンのバッテリー残量への影響が懸念されます。このように、仮想通貨マイニングサー

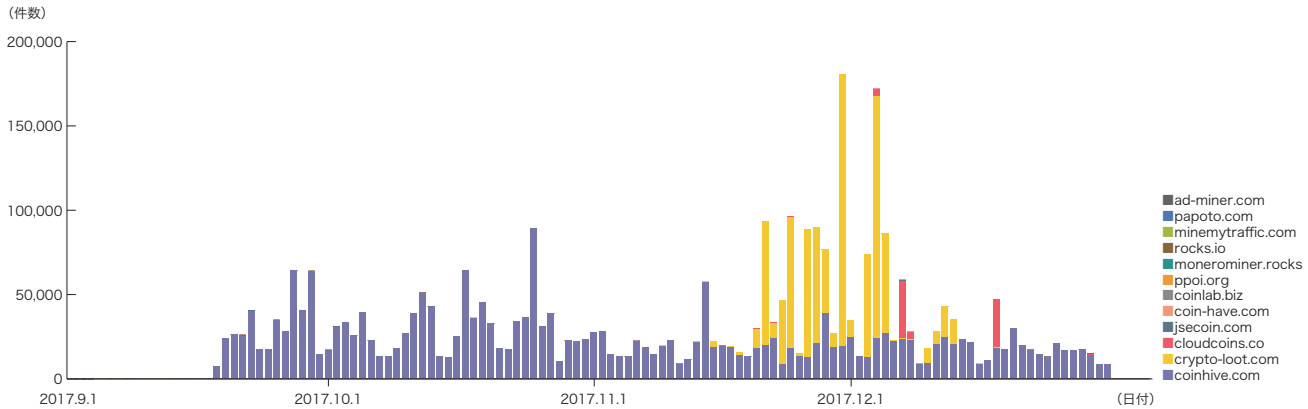

図-2 2017年下期の仮想通貨マイニングサービスへのアクセス数

＊2　kaspersky lab dialy、"Got any hidden miners? I wouldn't be so sure…"（https://www.kaspersky.com/blog/hidden-miners-botnet-threat/18488/）。
＊3　wizSafe Security Signal、「Webサイトの改ざんに伴う仮想通貨マイニングスクリプトの埋め込み事例」（https://wizsafe.iij.ad.jp/2017/10/94/）。

ビスが悪用される事例も増えてきていることから、アンチウイルスソフトウェアにはマイニング用JavaScriptをリスクと判定して遮断するものもあります。

図-2は、Coinhiveサービスが開始された2017年9月以降にIIJセキュアWebゲートウェイサービスで観測した、仮想通貨マイニングサービスへのアクセス数です。アクセス先の仮想通貨マイニングサービスの種類が増加していること、及びそれぞれのサービスへのアクセス数が12月初旬までは増加していることが分かります。企業ユーザのWebサイトアクセス数を観測したデータであるため、企業ユーザの活動が少ない土日祝日や年末はアクセス数が相対的に減少しています。

今後、仮想通貨マイニングサービスの利用が魅力的なものであり続けるかは仮想通貨の価値増減に左右されます。また、Webサイトの閲覧者による仮想通貨マイニングサービスのマイニング用JavaScriptに対するリスク判断によっても、サービスの利用しやすさが左右されます。例えば、正規Webサイト運営者は、Webサイト閲覧者のPCのアンチウイルスソフトウェアがブロック警告するJavaScriptを自らのWebサイトに設置したいとは考えないはずです。

仮想通貨の価値やセキュリティベンダーの動向は、攻撃者にとっても仮想通貨マイニングサービスの悪用しやすさに関わる問題です。仮想通貨マイニングサービスの悪用が魅力的でなくなった場合には、攻撃者はまた別の収益を上げる手段を探すことが考えられます。

1.3 DDoS攻撃

2017年下期（7月～12月）にIIJでは、1日あたり20.8件、1ヵ月あたり638件、計3828件のDDoS攻撃を観測しました。図-3に2017年下期のDDoS攻撃発生の件数を示します。9月は満州事変の開始日となる9月18日などがあることから大量のDDoS攻撃の発生を警戒していましたが、2017年は関連する攻撃は観測されませんでした。DDoS攻撃の発生は日常茶飯事であり、その発生数の変動は特定期間に左右されるものではなくなってきていると考えられます。

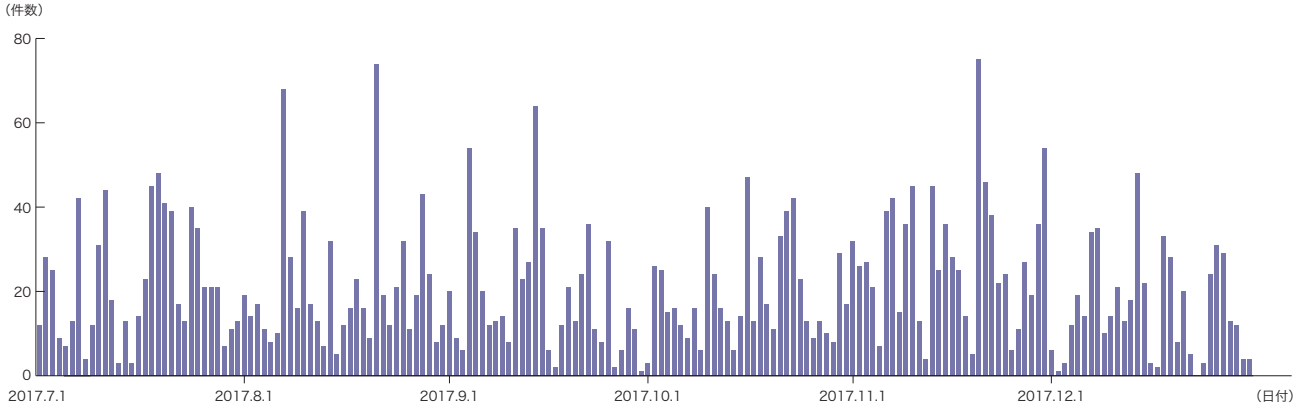

図-3 2017年下期のDDoS攻撃の発生件数

今回の対象期間において観測されたDDoS攻撃の最大攻撃規模は、2017年10月に観測した最大179万ppsのパケットによって16.55Gbpsの通信量を発生させるものでした。この攻撃の手法は、主にUDP Floodによる回線を輻輳させる攻撃でした。また、最長攻撃時間は、2017年9月に観測した46時間57分にわたってDDoS攻撃が発生し続けるものでした。この攻撃は主にICMPプロトコルを利用したものでした。表-1に2017年下期に観測した各月のDDoS攻撃発生件数、最大攻撃規模・手法、最長攻撃時間・手法を示します。

本観測期間においても、これまで同様に金銭を支払うように要求する脅迫メールが出回っています。小規模のDDoS攻撃を実際に発生させた上で、DDoS攻撃予告の脅迫を行うケースもありました。また、2017年12月頃よりTwitter上で、日本語で攻撃ターゲットを指定したDDoS攻撃予告を公開した上で、実際にDDoS攻撃を発生させてターゲットWebサイトをサービス停止に追い込む事案が複数発生しており、官公庁などのWebサイトが攻撃対象となりました。

DDoS攻撃は、金銭搾取を目的としたものやハクティビスト活動として行われるものなど様々ありますが、いずれの場合もビジネスに大きな影響を及ぼすことを目的としたケースが多くなっています。図-4は、本観測期間における、DDoS攻撃の発生曜日、発生時間帯で集計した発生割合を示すものです。平日日中と比較して土日夜間の発生割合が少なくなっています。深夜早朝の1時～7時とビジネス時間帯が入る7時～13時では、発生数に3倍以上の差異がありました。また、土曜日と月曜日の比較でも、発生数に3倍以上の差異がありました。

表-1 2017年下期のDDoS攻撃の最大攻撃規模・時間

観測年月	件数	最大攻撃規模・手法		最長攻撃時間・手法	
2017年7月	673	17.86Gbps	NTP Amplification	5時間18分	IP Fragmentation/UDP
2017年8月	655	10.16Gbps	IP Fragmentation/UDP	16時間43分	Flood
2017年9月	575	12.06Gbps	NTP Amplification	46時間57分	ICMP
2017年10月	593	16.55Gbps	UDP Flood	24時間 9分	IP Fragmentation/UDP
2017年11月	843	8.93Gbps	IP Fragmentation/UDP	6時間23分	UDP Flood
2017年12月	489	13.39Gbps	DNS Amplification	14時間22分	ICMP/DNS Amplification

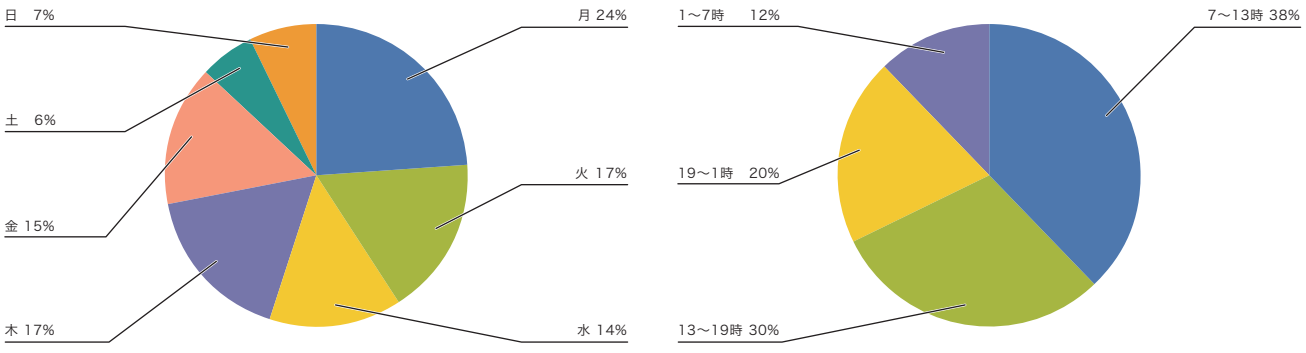

図-4 DDoS攻撃の曜日別/時間帯別の発生割合

1.4 Struts2の脆弱性を狙った攻撃

2017年は、Apache Struts2のCriticalな脆弱性を狙った攻撃が多発しました。表-2に示すように、2017年にApache Struts2で公開された脆弱性のうち6件は、リモートコード実行の可能性(Possible Remote Command Execution)があるものでした。

これらの脆弱性のうち2017年3月に公開されたCVE-2017-5638(S2-045/S2-046)の脆弱性は、攻撃実行が比較的容易であり、攻撃対象の環境条件も比較的緩く、セキュリティパッチが適用されていなければ攻撃の成功確率が非常に高いものでした。このため、脆弱性公開直後から、サイバー攻撃による情報漏えいのインシデント被害が多発しました。表-3に、Apache

表-2 Apache Struts2のリモートコード実行の脆弱性(2017年)

Bulletin#	Description	CVE#	CVSS v3 Base Score
S2-045	Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.	CVE-2017-5638	10 Critical
S2-046	Possible RCE when performing file upload based on Jakarta Multipart parser(similar to S2-045)	CVE-2017-5638	10 Critical
S2-048	Possible RCE in the Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x series	CVE-2017-9791	9.8 Critical
S2-052	Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads	CVE-2017-9805	8.1 High
S2-053	A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals	CVE-2017-12611	9.8 Critical
S2-055	A RCE vulnerability in the Jackson JSON library	CVE-2017-7525	8.1 High

表-3 Struts2を攻撃したセキュリティインシデントの例

公表年月	インシデント概要
2017年3月	都税クレジットカード支払サイトから67万6290件の情報漏えい*4
2017年4月	地図情報サイトから最大2万3000件の情報漏えい*5
2017年5月	情報通信研究機構(NICT)の公開サーバに不正アクセス*6
2017年6月	土地総合情報システムから最大4,335件の情報漏えい*7
2017年9月	Equifaxから最大1億4300万人分の情報漏えい*8

*4 東京都、『「都税クレジットカードお支払サイト」における不正アクセスについて』(http://www.metro.tokyo.jp/tosei/hodohappyo/press/2017/03/13/02.html)。
*5 総務省、「地図による小地域分析(jSTAT MAP)における不正アクセス」(http://www.soumu.go.jp/menu_news/s-news/01toukei09_01000023.html)。
*6 国立研究開発法人情報通信研究機構、「Apache Struts2の脆弱性を悪用した不正アクセスについて」(https://www.nict.go.jp/info/topics/2017/05/170502-1.html)。
*7 国土交通省、『「土地総合情報システム」における不正アクセスおよび情報流出の可能性について』(http://www.mlit.go.jp/report/press/totikensangyo05_hh_000129.html)。
*8 Equifax、"Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes"(https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832)。

Struts2の脆弱性を攻撃したセキュリティインシデントの例を列挙します。いくつかのインシデントにおいては、CVE-2017-5638（S2-045/S2-046）の脆弱性が悪用されていたことが明らかになっており、米国の大手信用情報会社Equifaxも、個人情報漏えいのインシデントの原因をCVE-2017-5638（S2-045/S2-046）と2017年9月に公表しています。このインシデントでは、米国やカナダ、英国の顧客1億4300万人分の個人情報が漏えいした可能性があるとしています。

図-5に、2017年下期（7月～12月）にIIJで観測したApache Struts2の脆弱性を悪用する攻撃の1サイトあたりの件数を示します。2017年3月に公開されたCVE-2017-5638（S2-045/S2-046）を狙った攻撃が大半を占めていることが分かります。CVE-2017-5638（S2-045/S2-046）を狙った攻撃の中には、ボットネットを活用して同一ツールで大量に調査攻撃を行ったと推定されるものも観測されており、2017年10月20日からの件数急増[*9]は、この攻撃によるものです。

CVE-2017-5638（S2-045/S2-046）は、脆弱性公開から既に半年以上が経過していますが、未だ悪用できる攻撃対象がインターネット上に数多くあるため、攻撃者はそれらのWebサーバを狙っている状況と言えます。

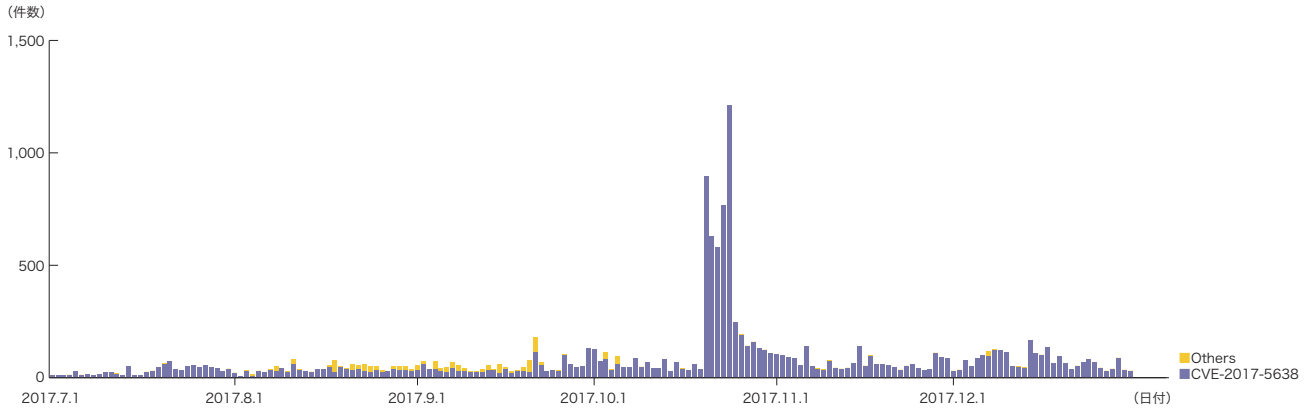

図-5 2017年下期のApache Struts2を狙った1サイトあたりの攻撃件数

＊9　wizSafe Security Signal、「Apache Struts 2の脆弱性を狙った攻撃の観測情報」（https://wizsafe.iij.ad.jp/2017/11/106/）。

Apache Struts2は、Webアプリケーションフレームワークとして様々なWebサイトで活用されています。Apache Struts2のセキュリティパッチの適切な運用ができていなかったWebサイトが攻撃被害を受けました。2017年は、Apache Sturts2が多くの攻撃の対象となりましたが、インターネットからアクセス可能なサーバやソフトウェアは、すべからく攻撃者のターゲットになっています。サーバやソフトウェアの脆弱性について1件でも脆弱性の適切な管理ができていない場合には、情報漏えいなどの被害を受ける可能性があります。Apache Struts2の利用有無にかかわらず適切な脆弱性管理ができているかの定期的な見直しが必要と言えます。

1.5 むすび

今回は情報分析基盤を活用し、長期間継続的にサイバー攻撃の動向を分析した結果について、その一端を示しました。この新しい情報分析基盤の活用は始まったばかりです。IIJでは今後も取り込むデータの種類・量を増やしていくこと、及び機械学習やAIといった新しい解析技術を導入することで、高度化するサイバー攻撃に迅速に対策を講じることができるようにしていきます。

執筆者:
齊藤 斎（さいとう きよし）
IIJ セキュリティ本部 セキュリティビジネス推進部長。
セキュリティビジネス推進部の部長として、マネージドセキュリティサービスのセキュリティサービス運営・導入・サポート、セキュリティコンサルティング、SI、SOCの統括およびビジネス開発に従事。

執筆者:
中嶋 功（なかじま つとむ）
IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター 副センター長。
SOCの副センター長としてセキュリティアナリストをリードするとともに、自らもアナリストとしてインシデント分析業務、セキュリティインテリジェンス生成などのビッグデータ分析業務に従事。