IIR

Internet
Infrastructure
Review

Mar.2018
Vol.38

定期観測レポート

SOCレポート

フォーカス・リサーチ(1)

フルMVNOとは何か、IIJはなぜフルMVNOを目指すのか

フォーカス・リサーチ(2)

Hayabusa：高速に全文検索可能なログ検索エンジン

IIJ
Internet Initiative Japan

Internet Infrastructure Review

March 2018 Vol.38

《 読者アンケート 協力のお願い 》

今号をお読みいただいたご意見・ご感想をお聞かせください。今後の参考にさせていただきます。
回答いただいた方の中から抽選で30名様にインターネット便利帳付きIIJオリジナルリングノートをプレゼントいたします。
※なお、当選のお知らせは、プレゼントの発送をもってかえさせていただきます。

【 アンケート受付期間 】
2018年5月31日(木)まで

【 回答方法 】
IIJのWebサイト内、以下のページまたは右側のQRコードからご回答ください。
(https://biz.iij.jp/public/seminar/view/279)

エグゼクティブサマリ

この3ヵ月は仮想通貨取引所での仮想通貨の不正流出に関する報道が相次ぎ、世間の注目を集めています。これらの事件の原因は仮想通貨自体にあるわけではないので、これによって様々な可能性を秘めた仮想通貨の利活用に悪い影響が出ないよう注意する必要があるでしょう。

このエグゼクティブサマリを書いている最中に、memcachedのアクセス制限に関する注意喚起が行われました。数日後には、それを悪用して、GitHubに対して1.35Tbpsという過去最大級のDDoS攻撃が発生した、と発表されました。過去にもDNSやNTPなど、トラフィックを増幅する機能を悪用した攻撃手法はありましたが、今回のmemcachedの増幅率は1万を超えるという点で、今までにない破壊力を持っています。このような事象に対してIIJは、他の事業者とも協調して対応していきたいと考えています。

IIRは、IIJで研究・開発している幅広い技術の紹介を目指しており、我々が日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章では、今号の定期観測レポートとして、SOCレポートを取り上げます。前号でご案内した通り、IIRに掲載していたセキュリティレポートは、より即時性の高いwizSafe Security SignalというWebサイトでの掲載に変更しましたが、年に一度は、定期観測レポートとしてセキュリティを取り上げていきます。今回は、IIJのSOCで独自のセキュリティインテリジェンスを作り出すために刷新した、新しい情報分析基盤を紹介し、この半年のあいだにwizSafe Security Signalで報告した内容から、この情報分析基盤を活用して明らかになった活動について解説します。

2章、3章は、フォーカス・リサーチです。まず2章では、IIJのフルMVNOの取り組みを紹介します。MVNOは名前の通り仮想的な移動通信事業者ですが、自社で保有・運用する機能要素の範囲によって、いろいろな事業モデルがあります。フルMVNOとは、無線アクセス以外の機能要素を自社で保有するMVNOの事業モデルです。多くの設備を自社で保有することにより、今まではMNO（無線アクセスを保有する従来の移動通信事業者）にしかできなかったサービスを、MVNOでも提供できるようになります。そこで、フルMVNOになるとは具体的にどういうことなのか、どのようなことが可能になるのか、といったことを解説します。

3章では、多数のマルチベンダが出力する大量のログを高速で蓄積・検索できるシステムとして、IIJ技術研究所が実装したオープンソースソフトウェア「Hayabusa」について解説します。ネットワークやシステム運用の現場では、ハードウェアやソフトウェアから出力されるログを収集して、統計情報として表示したり、トラブルシュートのために検索する必要があります。セキュリティインシデントに対応する際も、ログの情報は非常に重要です。大規模なシステムにおいては、大量のログを蓄積し、高速で検索する必要があり、それを容易に実現する仕組みとしてHayabusaが開発されました。ここではInterop Tokyoで収集されたShowNetのsyslog実データをもとに行った実験の結果と、Hayabusaの実装・課題などについて紹介します。

IIJは、このような活動を通じて、インターネットの安定性を維持しながら、日々改善・発展させていく努力を続けています。今後もお客様の企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けていきます。

島上 純一（しまがみ じゅんいち）

IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

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。

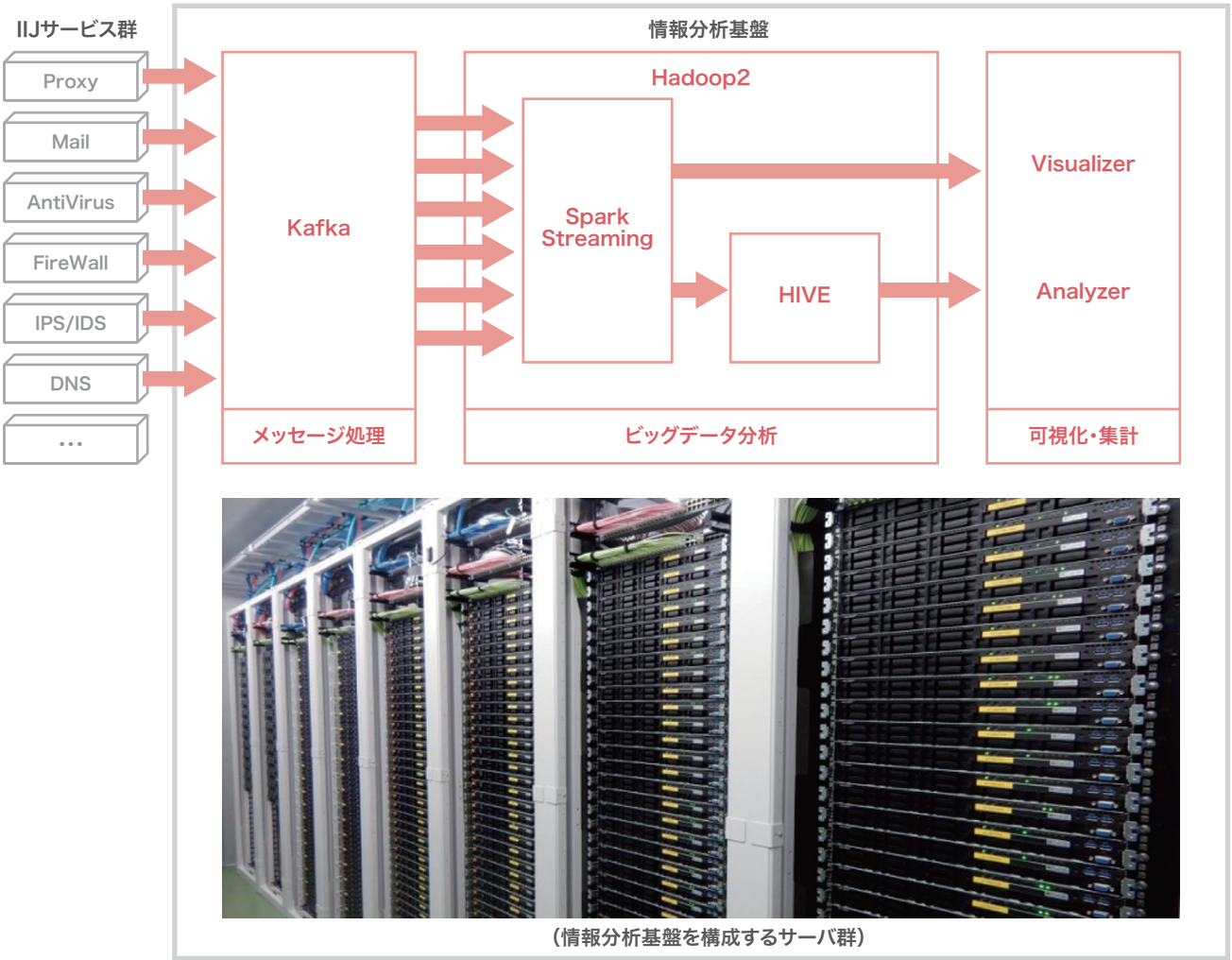

図-1 情報分析基盤のアーキテクチャ概要

＊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

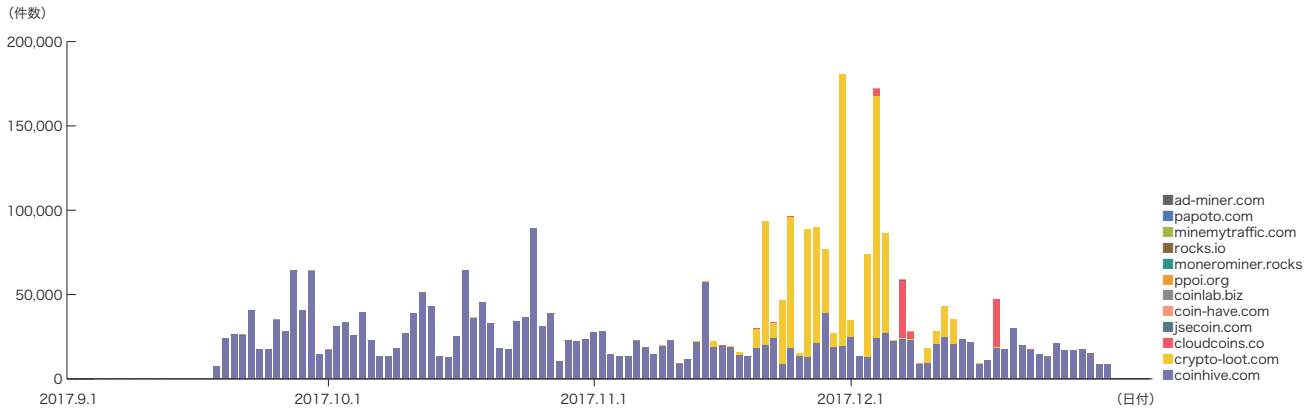

図-2 2017年下期の仮想通貨マイニングサービスへのアクセス数

＊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。

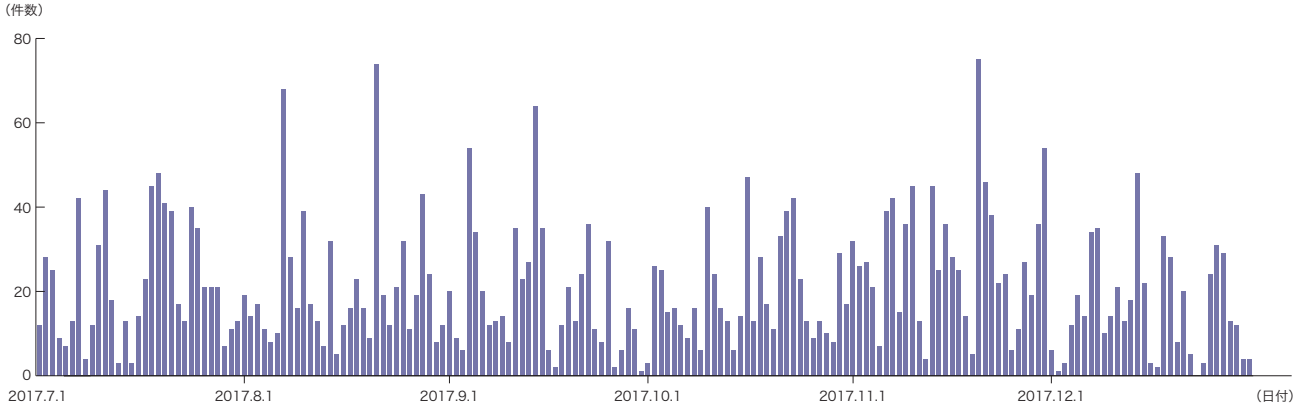

図-3 2017年下期のDDoS攻撃の発生件数

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

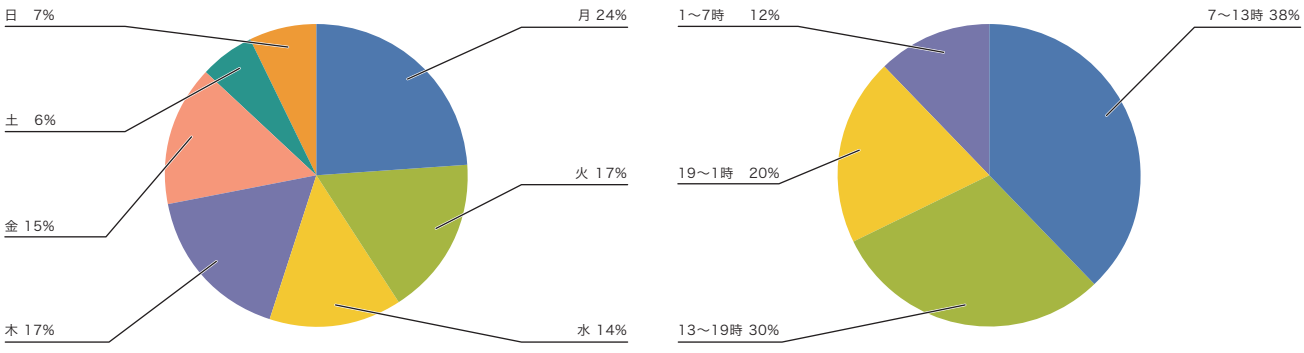

図-4 DDoS攻撃の曜日別/時間帯別の発生割合

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。

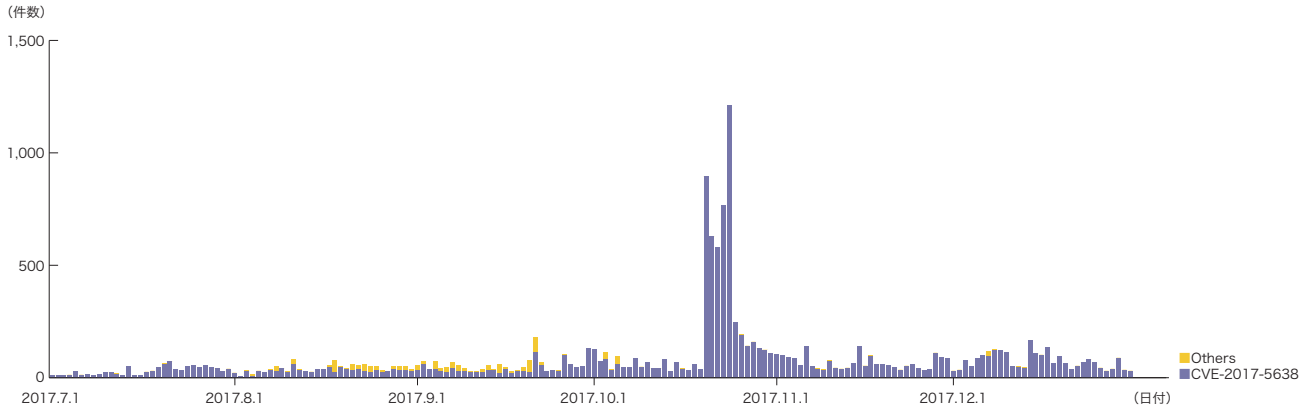

図-5 2017年下期のApache Struts2を狙った1サイトあたりの攻撃件数

＊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。

フルMVNOとは何か、IIJはなぜフルMVNOを目指すのか

2.1 MVNOの事業モデル

IIJが2008年にMVNO事業を開始して以来、最大のチャレンジである「フルMVNO」がいよいよこの2018年に始まります。この「フルMVNO」という言葉は、日本ではまだそれほど馴染みがなく、その意味するところを正確に理解することは困難かもしれません。しかし、世界では既にいくつものMVNOが「フルMVNO」への事業モデルのトランスフォーメーションを成功させ、その基盤を用いた先進的かつ多様なサービスを提供しています。

「フルMVNO」とは、MVNOの事業モデルを定義する言葉です。図-1[*1*2]にそのMVNOの事業モデルの類型を示しますが、その分類の鍵は、MVNOが移動通信事業を行うにあたってどこまでの要素を自らで保有するか、という点にあります(図-2[*3])。

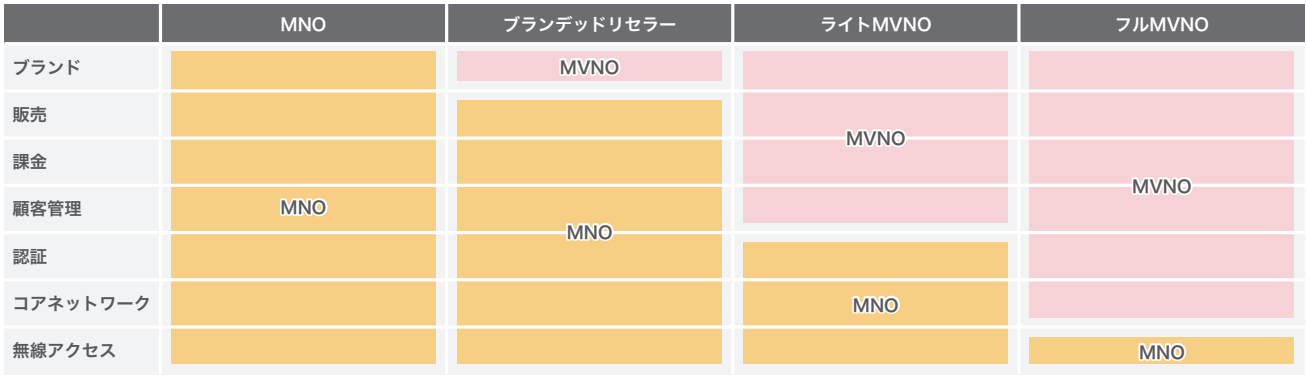

図-1 MVNOの類型

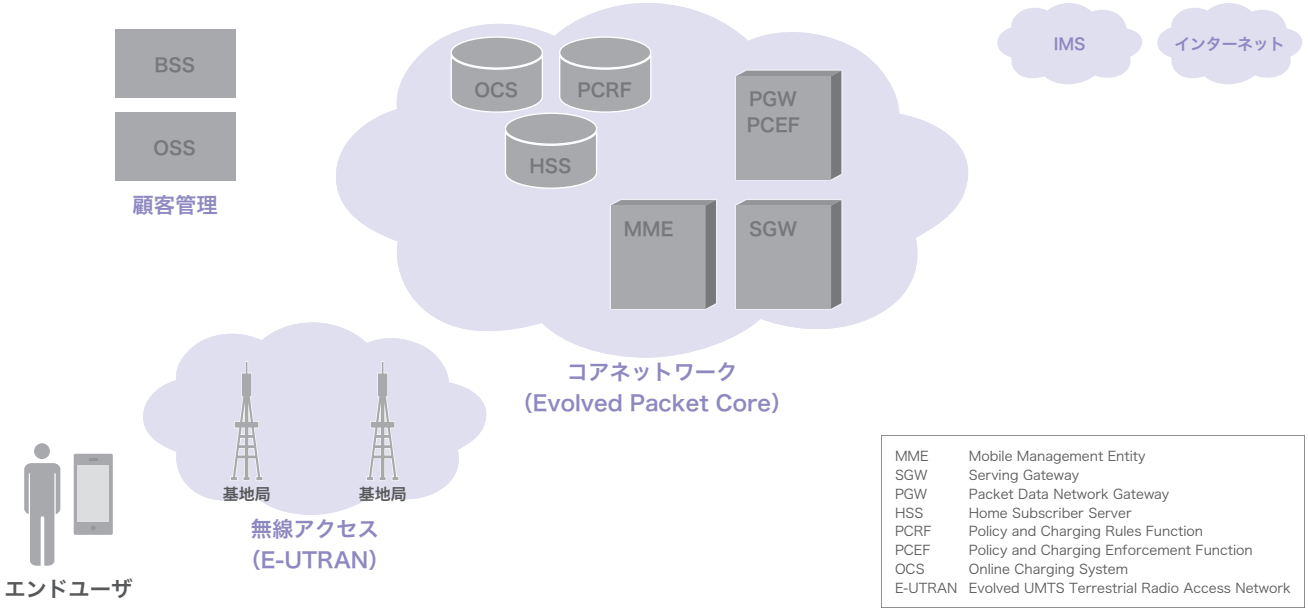

図-2 4G LTEの移動通信ネットワーク概要

＊1　図-1は類型を示したものであり、実際のMVNOは必ずしもこのどれかに当てはまるわけではない。各国の市場動向や制度、MNOとMVNOの関係によりこれらの中間的位置づけのMVNOも多くあり、また日本における「レイヤー3 MVNO」「レイヤー2 MVNO」のようなローカルな小分類が存在する。
＊2　図-1はMVNO事業の優劣を意味したものではない。各社の特性や事業目的に応じ、最適な事業モデルを選択することが重要である点に留意。
＊3　4G LTEの代表的なノードだが、無線アクセス以外のどの部分をMVNOが保有し、どの部分をMNOから借りるかはそれぞれのMVNOの事業モデルにより異なる。

MVNO(Mobile Virtual Network Operator)はその名のとおり仮想通信事業者であり、自らが保有していない設備を他社に依存することで、独自ブランドでのサービスを展開することがその本質です。しかし、ブランド以外のすべてを他社に依存することは、場合によっては事業の独自性を損ない、他社との十分な差別化を困難にするという懸念があります。そのため、各社の事業目的に応じて、全部ではなくとも一部の要素や設備を、他社に依存することなく自ら直接運用することが選択肢に入ってくるのです。

例えばディズニーのように、非常に強力なブランドを持ち、その他のすべてをMNOに依存しても十分な競争力を有する事業者の場合は、「ブランデッドリセラー」が最も適している事業モデルとなるでしょう。また、販売や顧客管理を自ら行い、ネットワークや認証設備の運用をMNOに依存する「ライトMVNO」は、日本のみならず世界でMVNOの標準的な事業モデルとして広まっています。そして「フルMVNO」は、無線アクセス以外の設備を広く自社で保有する、最もMNOに近いMVNOの事業モデルと言えます。

2.2 フルMVNOの優位性とハードル

フルMVNOの優位性は、その保有するネットワーク設備、すなわちコアネットワーク*4と認証設備にあります。これらの設備は、他のMVNO事業モデルであってもMNOから借りることが可能ですが、自社で保有することで、事業の独自性をより高め他MVNOや他MNOとの差別化を図ることが容易になります。それだけでなく、コアネットワークという移動通信事業の心臓部を自ら保有することで、1つのMNOとの従属的なMVNO契約に縛られるライトMVNOのビジネスモデルから、複数のMNOやMVNOとの協業による新事業領域へのチャレンジが可能となります。

反面、フルMVNOは設備面での投資が必要であり、また設備運用のためのヒューマンリソースも多く必要なことから、コストが最大のハードルと言えます。そのため世界的には、例えばスマートフォン向けの低料金サービスのような低付加価値サービスはライトMVNOにより提供されるケースが多く、IoTや国際サービス、セキュリティやFintechといった、高い付加価値を伴う新たな事業領域にチャレンジする事業者がフルMVNOにトライすることが多いようです。

2.3 フルMVNOへの大きな潮流

日本にはこれまでフルMVNOは存在しておらず、IIJが初の事業化を担うことになります。世界でも、フルMVNOが既に存在する国は欧州各国などまだ少数に留まり、多くの国ではフルMVNOの事業化は今後の課題です。前述のとおりフルMVNOには多くのコストが必要なことから、その投資ができる規模のMVNOが既に存在するかが問われます。またMNO側にもフルMVNOとのパートナーシップを許容する成熟度が必要です。場合によっては、国家の通信政策や制度がフルMVNOを許容しないケースもあり、政策制度に関する議論が求められることもあります。

ただ、IoTや5Gなど今後の移動通信の高度化を見据えると、フルMVNOが移動通信市場にもたらすイノベーションや多様性はいずれの国にとっても重要であり、多くの国にとってフルMVNOの市場導入は遅かれ早かれ現実的な政策課題となっていくことが考えられます。日本でも、2014年の情報通信審議会2020-ICT基盤政策特別部会での議論でフルMVNOの実現が重要な政策課題だと認識され、IIJとNTTドコモの事業者間協議が加速しました。このような流れは、今後世界的に広がっていくと考えられます。

*4 コアネットワーク:移動通信ネットワークにおいて、端末を網に接続させるための信号(シグナリング)や通話・通信に関わる信号(ユーザデータ)を処理するネットワーク。2G/3GではIP化は当初されていなかったが、現在は2G/3Gを含めすべてIPネットワークで構成されることが多い。

2.4「フルMVNO」と「HLR/HSS開放」

この2020-ICT基盤政策特別部会を含め、日本におけるフルMVNOに関連する議論は、MVNOに対する「HLR[*5]/HSS[*6]の開放」として位置づけられてきました。このHLR/HSSは、移動通信のコアネットワークにおいて重要な役割を果たすノードであり、加入者管理装置とも訳され、その機能は以下のように多岐に渡ります。

1. 加入者回線のMSISDN（電話番号）、IMSI（加入者を識別するための国際番号）などの情報を保持し管理する回線データベース
2. MMEなどのネットワーク内の各ノードよりの問い合わせに応答し、接続や機能の利用可否について加入者回線を認証する
3. 音声呼やSMSなどのサービスを移動通信ネットワークで実現するため、端末が収容されているネットワークや交換機の情報をリアルタイムに保持する（在圏管理）
4. SIMカードと対になる情報を格納し、通信内容の秘匿に必要な暗号化機能を（他のノードと併せ）提供する

日本において、このHLR/HSSは、これまでMNOにより運用されており、MVNOが持つことはありませんでした。MVNOが独自に用意したHLR/HSSをMNOのネットワークに接続してサービスを提供することは、IIJが日本で最初のケースとなります[*7]。

ただ、コアネットワークに存在する様々なノードのうちHLR/HSSを運用することがフルMVNOの定義として扱われていることについては、若干の注意が必要です。世界的には、より広くMME[*8]やSGW[*9]といったコアネットワーク中の交換機を運用するフルMVNOのネットワークモデルも議論されており、MNOとMVNO間の「RAN[*10]シェアリング」とも呼ばれていますが、今回のIIJのフルMVNO事業化はRANシェアリングまで踏み込んで実現しているものではありません。MMEやSGWのようなコアネットワーク中の交換機やRANは、それ単体で高い付加価値をもたらすものではないのがその理由ですが、来るべき5GではネットワークスライシングやNFVなど、コアネットワークへの付加価値導入が主要なテーマになっており、今後の検討課題であると認識しています。

2.5 MNCと独自SIM

HLR/HSSをMVNOが自前で運用することのメリットは、必ずしもHLR/HSSの機能から直接生じるとは限りません。その1つがMNC[*11]の取得です。MNCは移動通信ネットワークの相互の接続の際に、個々のネットワークの識別子となる番号で、IPネットワークで言えばAS番号に相当します。移動通信ネットワークでもIPネットワーク同様、網間の接続は世界的規模で行われていますので、その識別子となる番号はグローバルでユニークである必要があります。日本でのMNCは、ITU-T[*12]のE.212勧告を受けて、総務省が電気通信番号規則（総務省令）に基づき払い出す5桁の数字となっています。またその上3桁はMCCとよばれる国番号で、日本には440及び441がアサインされています。

このMNCの払い出しの条件は、電気通信番号規則により「端末設備を識別するための設備を設置すること」とされています。IIJは、自らHLR/HSSを自ら設置・運用することでこの条件を満たしたため、総務省より日本のMVNOで初めて、「44003」のMNCの払い出しを受けました。このMNCを用いることで、IIJ

＊5　HLR：Home Location Registerの略。2G/3Gの携帯電話ネットワークにおいて、加入者回線の情報を保持し、その在圏管理などを司るノード。
＊6　HSS：Home Subscriber Serverの略。HLRと同等の機能を提供する4G LTEネットワーク及びIMSのノード。
＊7　KDDIやソフトバンクなど「MNOであるMVNO」を除く。
＊8　MME：Mobile Management Entityの略。4Gにおいてコアネットワーク内でのシグナリングを扱うノードの1つ。
＊9　SGW：Serving Gatewayの略。4Gにおいてコアネットワーク内でユーザデータを扱うノードの1つ。
＊10 RAN：Radio Access Networkの略。移動体通信において、基地局（無線局設備）をコアネットワークに繋げるためのネットワーク。3GではUTRAN（UMTS Terrestrial Radio Access Network）、4G（LTE）ではE-UTRAN（Evolved UTRAN）と称される。
＊11 MNC：Mobile Network Codeの略。移動通信ネットワークを識別するために用いられるユニークな番号。
＊12 ITU-T：International Telecommunication Union（国際電気通信連合）の電気通信標準化部門。

は自らのHLR/HSSを、ドコモだけでなく他の移動通信ネットワークにも接続し、ローミングサービスを展開することが可能となります。

もう1つのメリットは独自のSIMカード発行です。SIMカードは、加入者回線ごとに1枚発行されるICカードで、加入者の識別のための番号(IMSI[*13])や暗号化鍵を保存しています。契約者は、このSIMカードを端末に挿入することで、移動通信ネットワークのサービスを享受することができます。これまでの日本のMVNOも、SIMカードを発行して契約者に貸与することでサービスを提供してきましたが、あくまでこのSIMカードはMNOから提供されるものを又貸ししていたに過ぎませんでした。IIJは、独自のMNCを保有したため、自らの設備のみでIMSIを払い出すことが可能となり、独自のSIMカードをプロビジョニング[*14]できるようになります。

このように、MVNOが独自にSIMカードのプロビジョニングを行えるようになるということは、技術的には2つの側面を持ちます。1つはサービス提供の自由度です。これまではMNOのシステムに依存してSIMカードをプロビジョニングする以外できなかったため、MNOのシステムが許容していないサービス提供は不可能でした。例えば、これまでのライトMVNOのスキームでは、SIMカードをいったんプロビジョニングし、利用開始すると、その後は廃止するまで利用可能状態が継続し、廃止後のSIMカードは再利用不可となってしまいます。これは、IoTで想定される通信モジュールを製品に組み込むユースケースにおいては、出荷前検査で一時的に開通するといったことが困難であることを意味します。つまり、出荷前検査で使ったSIMカードを抜いて新たにSIMカードを挿すという工程が検査後に生じてしまうため、検査が意味を成さなくなるという問題が起こるのです。このような制約はMNO側のBSS/OSS[*15]によるもので、理想的にはMNOがMVNOのニーズによりBSS/OSSを柔軟に開発可能であればライトMVNOであっても克服可能ではありますが、現実にはかなりハードルが高いと言わざるを得ません。

IIJのフルMVNOサービスでは、IIJ自社のBSS/OSSによって、一時的な開通や、廃止後のSIMカードのリサイクルをサポートします。IoTのように柔軟なSIMカードの開廃オペレーションが要求されるユースケースで、そのメリットが活かせると考えています。

もう1つはeSIMのような新しいSIM技術のサポートです。IoTやローミングの先進的なユースケースにおいて、これまで30年近く利用されてきたプラスチックカード形状のSIMの運用の限界が問題となってきており、抜き挿しする代わりにオンラインでSIMプロファイルをダウンロード可能なeSIM[*16]や、SIMカードを物理的なメディアやデバイスから切り離して仮想的に扱う仮想化SIM(ソフトSIM[*17])の普及が見込まれています。既にeSIMを搭載した商用デバイスや、SIMカードの入れ替えなくプリペイド的に安価なローミングが利用可能なソフトSIMを搭載したデバイスなどが登場しており、SIMカードを独自にプロビジョニング可能な基盤を保有することにより、これらの新しい技術によるイノベーションに寄与することが可能となります。

＊13 IMSI:International Mobile Subscriber Identityの略。移動通信ネットワークで加入者毎に割り当てられる識別子で、SIMカードに格納される。IMSIの先頭の数桁は発行した事業者のMNCである。HLR/HSSは、IMSIを管理し、SIMカードを認証する役割を担う。
＊14 プロビジョニング:ネットワークリソースを電気通信サービスの契約者に提供するために準備を整えること。ここでは、SIMカードに必要な情報を書き込むと同時に、HLR/HSSにも相当する情報を書き込むことで、移動通信サービスの提供準備を整えること。
＊15 BSS/OSS:Business Support System/Operation Support Systemの略。通信事業者のバックオフィスのうち、BSSは契約管理システムや請求管理システムなど顧客に近いシステムを指し、OSSはSIMカードのプロビジョニングシステムや物流管理システムなど運用に近いサイドのシステムを指す。
＊16 eSIM:内部に保存されている通信事業者のプロファイルを遠隔で書き換え可能なSIMカードのこと。物理的には、従来のプラスチックカード形状のSIMもしくは専用のハードウェアチップを用いることが想定されている。現在、携帯電話事業者の業界団体であるGSMAにて、組込用途とコンシューマデバイスの2トラックでの標準化が進行中。
＊17 ソフトSIM:遠隔で書き換え可能なSIMのうち、専用のハードウェアを用いず、プロセッサの安全なアプリケーション実行環境(TEE)を使うなどする、ソフトウェアで実装されたSIMを指す。あくまで非標準化技術だが、一部のソフトSIMプラットフォームは標準化されたeSIMとプロビジョニングシステムの互換性を取るなどしている。

2.6 IIJのフルMVNOの持つメリット

このようなHLR/HSSの保有やSIMプロビジョニングの自由度の確保は、IIJ以外の日本のMVNOでも一部採用が始まっており、今後のIoTの需要を見越した先触れ的な動きとして非常に興味深いものがあります。それでは、これら類似の事業モデルを展開する他事業者と、IIJのフルMVNOスキームは、どこが異なるのでしょうか。

このような他事業者の場合、その保有するHLR/HSSは、一般に国内MNOへの接続はなく、海外事業者のネットワークにのみ接続されるものと推測されます。その場合も、これまで本稿で説明した他移動通信ネットワークの利用や、SIMカードのプロビジョニングはIIJのフルMVNOスキームと同様に提供可能です。ただし、日本のMNOのネットワーク利用に当たっては、日本以外の国であるのと全く同様に、当該海外事業者と国内MNOのローミング協定に基づき提供されます。そのため日本国内においてもローミング料金という比較的高額なコストをベースとした料金自由度の低いサービスしか提供することができません。

IIJでも、日本以外の国においては、海外のローミング中継事業者のネットワーク及びローミング協定を介した、比較的高いコストのローミングサービスを提供するという点で、大きくは変わりません。ただIIJは、日本国内においてはNTTドコモと直接HLR/HSSの接続を行っており、データ接続性の調達価格はローミング料金の水準よりも安価なMVNO向けデータ接続料が適用となります。そのため、日本国内においては他社よりも安価で、かつ料金自由度の高いサービスを提供できる点が大きな特色となります。

次に、日本以外の国におけるサービスについても詳しく見ていきましょう。一般に国際ローミングにおいて、ローミング協定を結んでいる二事業者間で役務が双務的に提供されている場合（互いに互いのネットワークを相手にローミングで開放している場合）、事業者間では相互の利用分について支払いが相殺されますので、そのローミング料金（タリフ）の設定や双方の通信量の多寡にもよりますが、自己のネットワークコストと大きく変わらない水準で他国のデータ接続を調達することもそれほど難しくはありません。ただ、他事業者のようにHLR/HSSだけを海外のローミング中継事業者のネットワークに接続している場合、日本国内のデータ接続を海外事業者に提供することはできませんので、双務的なローミング役務の提供はあり得ません。そのため、海外におけるデータ接続性の調達コストは海外事業者の設定するローミング料金（タリフ）にのみ依存することになり、料金自由度を上げるのは困難です。

IIJは、ドコモからMVNO向けデータ接続料で調達した日本国内のデータ接続を、自らのHLR/HSSを通じて海外事業者に販売することが可能です。そのためにはマルチIMSI[*18]といったSIMカードの技術を使う必要はあるものの、MNO間のローミングに準じる双務的な役務提供を行える環境を有することになります。現在、こういった双務的役務提供の可能性や、IIJのIMSIを用いた日本国内のデータ接続の提供に関する協議を海外の通信事業者と進めており、顧客のニーズに応じた高い料金自由度で、海外におけるデータ通信サービスが提供できるよう準備を進めています。これは、国内MNOとHLR/HSS接続を行っている唯一のMVNOであるIIJだけが可能なビジネスモデルであり、多くのお客様に料金的なメリットを感じていただけるものと思います。

＊18 マルチIMSI：SIMカードには通常1つのIMSIが記録されているが、そのIMSIを切り替えることで1枚のSIMカードで異なる通信事業者のサブスクリプションを切り替える技術。eSIMで実現するマルチプロファイルと異なり、IMSIの切替はSIMカードの中のアプレットが担う。

2.7 今後の課題

IIJは今回、日本で初めてとなるフルMVNOの事業化に踏み切りましたが、このような事業モデルは日本では他に類がなく、また世界でも一部の国や地域でのみ商用化されているものとなります。そのため、IIJでは冒険は避け、新規に導入となる設備やシステムの運用の水準についても検証しつつ段階的にデプロイメントを進めていく方針です。

また、今回のフルMVNOは、音声通話を含むサービスについてはスコープ外となります。音声通話については、通話品質の確保やMNP(モバイルナンバーポータビリティ)の実現、緊急通報への対応など法制度の面で厳しいルールが適用となる点を考慮してのことです。現在、IIJではIIJmioブランドや他社のブランドへのプラットフォーム提供を通じてスマートフォン向けの格安SIMの提供を主力事業の1つとして進めていますが、これらの音声通話を含むサービスについては、これまでのライトMVNOによる提供スキームが当面の間継続する予定です。

IIJでは、音声通話サービスへのニーズやその将来性などを多角的に検討しながら、音声通話サービスを含むフルMVNOの検討を進めていきます。

更に、今後のIoTや5Gといった新しいトレンドについても、フルMVNOとして受け身ではいられません。セルラーLPWA[*19]の世界規模での導入、ネットワークスライシングや5Gによる多様な付加価値を実現するために、MNOとどのような設備構築を行っていくべきか、またMVNOとしてどのような高度かつ多様なサービスを実現していくのか、IIJはフルMVNOのフロントランナーとして今後のMVNO業界における非常に重い責任を負ったものと考えています。MVNOとは、設備をMNOから借りて成立する二線級の事業者ではなく、MNOと異なる事業モデルに立脚しMNOとは異なる多様なサービスを実現することが可能な事業形態であることを常に肝に銘じて取り組んでいく考えです。

執筆者:
佐々木 太志(ささき ふとし)
IIJ MVNO事業部 事業統括室 担当部長。
2000年IIJ入社、以来ネットワークサービスの運用・開発・企画に従事。
特に2007年にIIJのMVNO事業の立ち上げに参加し、以後一貫して法人向け、個人向けMVNOサービスを担当。
MVNOの業界団体である一般社団法人テレコムサービス協会MVNO委員会にもメンバーとして参加。

＊19 セルラーLPWA:携帯電話の技術を用い、免許の取得が必要な周波数(ライセンスバンド)で提供される、低電力広カバレッジ(Low Power Wide Area)のIoT向け移動通信サービス。LTE-MやNB-IoTなどのセルラーLPWAの通信規格が2018年以降に商用化される見込み。

Hayabusa：高速に全文検索可能なログ検索エンジン

3.1 背景と目的

ネットワークやシステム運用の現場では安定したネットワーク運用やトラブルシュートを行うために、ネットワーク管理者がネットワーク機器から出力されるログを収集して統計情報として表示したり、トラブルの原因となるログを検索する方法が多く用いられています。また、セキュリティインシデントに対応する際にも、トラブル対応の場合と同様、ログからどのようなインシデントが発生したかを探ることがあります。

大規模なネットワークでは、多くのサーバ・ネットワーク・セキュリティ機器から通信を記録したログが日々大量に出力されるため、ネットワーク管理者はそれら大量のログをストレージシステムに蓄積し、高速にログ検索するシステムを管理しています。大規模なログ検索システムと蓄積システムを扱うためには、クラスタリングシステムや専用の管理ソフトウェアを用いることになり、本来はログの解析に時間を費やしたいところを、検索・蓄積システムの管理に時間が割かれることも少なくありません。

「ログの蓄積」と「ログの検索」がシンプルに動作する仕組みが、複雑なクラスタリングシステムを用いることなく実現できれば、ネットワーク管理者は蓄積・検索システムの管理に時間を割かれずに済み、本来の業務であるネットワークのトラブル対応やセキュリティインシデントの解析に集中することができます。

本稿では、多数のマルチベンダー機器が出力する大量のログを高速に蓄積でき、高速に検索可能なシステムとして実装したオープンソースソフトウェア「Hayabusa」について解説します。そしてシステムが扱うログの量が増加した場合には、シ

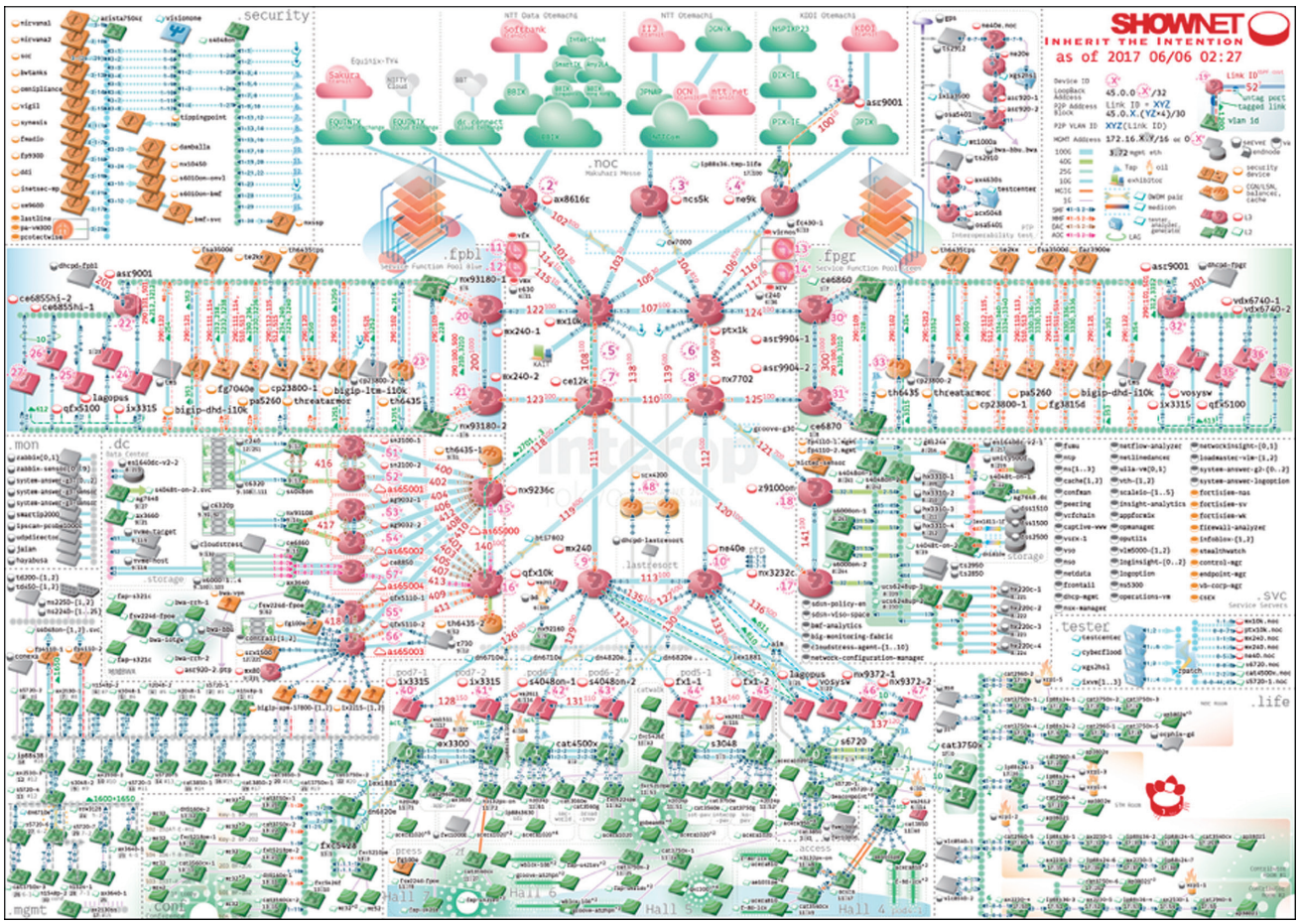

図-1 2017年のShowNetトポロジー図

ステムの検索性能が容易にスケールアウトすることで検索速度が飛躍的に向上する同ソフトウェアの分散システムのコンセプトモデルも併せて紹介します。

Hayabusaが実現する検索の高速化に関する評価は、Interop Tokyo[*1]で収集されたShowNetのsyslog実データを元に実験を行いました。この実データは、600以上のサーバ・ネットワーク・セキュリティ機器から出力されたものです。

3.2 ShowNet

ShowNetは、毎年幕張メッセで開催されるInterop Tokyo内で構築される相互接続検証とデモンストレーションを行う実験ネットワーク環境です。出展社へのインターネットアクセスをサービス提供する側面もあるため、実験とサービス提供の両方の側面を併せ持ちます。

図-1に示すように、ShowNetを構成する機材は数百を超え、実験ネットワークという性格上世界で初めて実ネットワークへと組み込まれる製品も多く、中には試作レベルの機材やソフトウェアもあります。

ShowNetを運用するメンバーは、これらの機材やソフトウェアを組み合わせて、サービス提供するネットワークを設計・構築して運用を行います。安定的にシステム構築を行うために、機材から出力されるsyslogを収集分析し、システムのバグやエラー、構成の成否を判断する運用が行われます。ShowNetを構成する機材は多岐にわたり、更に最新鋭のソフトウェアやハードウェアが大量に投入されるため、機材やソフトウェアを管理する運用メンバーは機材からどのようなログが出力されるかを事前に知ることは困難です。

ShowNetでは、監視システムの1つとしてsyslogを収集し分析するシステムが運用されます。ほぼすべての物理機器・仮想機器群からsyslogが送信され、そのsyslogを集約し検索するシステムが構築されます。過去には、秒間２万件以上のログが飛び交ったり、1日に2億件以上のログが蓄積されたこともありました。

特定のソフトウェアやハードウェアからのログであれば、ログフォーマットを推測することも可能ですが、ShowNetを構築する機材には同一のソフトウェアやハードウェアは少なく、かつ大量のメッセージが最新のファームウェアやソフトウェアのデバッグ情報として出力されるため、一般的なログ蓄積・解析ソフトウェアでリアルタイムに統計を表示させたり検索を行うことは非常に難しいです。

3.3 Hayabusa

Hayabusa[*2]は、ShowNetで収集された大量のsyslogを高速に検索するためのシステムとして設計されました。図-2にHayabusaのアーキテクチャを示します。

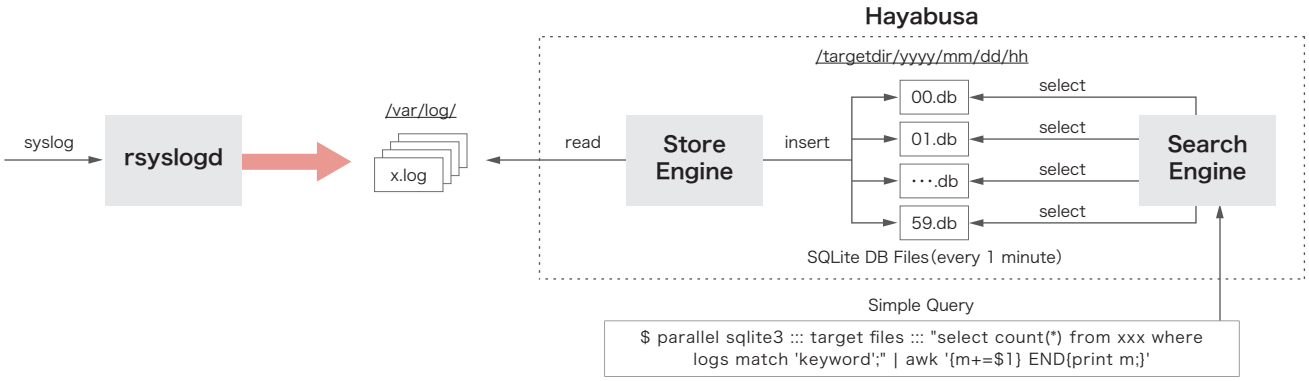

図-2 Hayabusaのアーキテクチャ

＊1　Interop Tokyo(https://www.interop.jp/)。
＊2　Hayabusa(https://github.com/hirolovesbeer/hayabusa)。

Hayabusaはスタンドアロンサーバで動作し、CPUのマルチコアを有効に使って高速な並列検索処理を実現します。Hayabusaは大きくStoreEngineとSearchEngineの2つのシステムに分割されます。StoreEngineはcronにより1分ごとに起動され、ターゲットとなるログファイルを開き、ログファイルに記録されたログメッセージをSQLite3[*3]ファイルへと変換します。ログデータは1分ごとのSQLite3ファイルへと分割され、検索時に複数プロセスにより並列処理されます。ログが保存されるディレクトリは以下のように時間を意味する階層として定義されます。

/targetdir/yyyy/mm/dd/hh/min.db

上記のディレクトリ階層は、以下の意味を持ちます。

/ターゲットディレクトリ/年/月/日/時間/分ごとのSQLite3ファイル

このように定義することで、ログ検索のための時間情報をデータベース内部に保持することなくディレクトリとのマッチングで行うことができ、時間のクエリ条件を指定することなく時間指定のログ検索が可能になります。ログが保存されるSQLite3ファイルはFTS（Full Text Search）と呼ばれる全文検索に特化したテーブルとして作成され、高速なログ検索を実現します。SearchEngineは、並列検索性能を向上させるために分単位に細分化されるFTSフォーマットで定義されたSQLite3ファイルへアクセスを行います。各SQLite3ファイルへはGNU Parallel[*4]を用いて並列にSQL検索クエリが実行され、結果はUNIXパイプラインを経由してawkコマンドやcountコマンドを用いて集計されます。

Hayabusaはスタンドアロン環境で動作しますが、小規模なApache Spark[*5]のクラスタよりも全文検索性能が高く、図-3で示すように、先行研究[*6]では3台のApache Sparkクラスタより27倍速い検索性能を示しました。

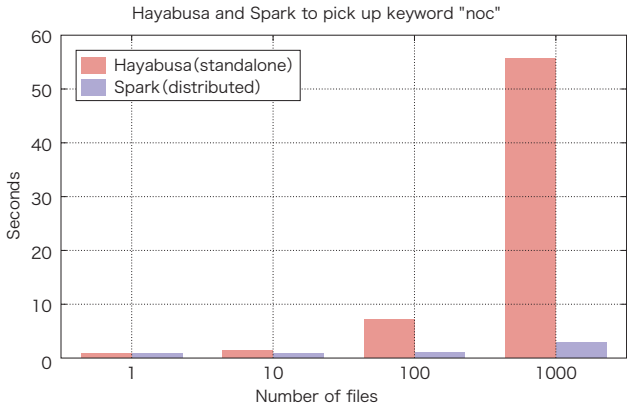

図-3 HayabusaとApache Sparkとの性能比較

＊3　SQLite3（https://www.sqlite.org/）。
＊4　GNU Parallel（https://www.gnu.org/software/parallel/）。
＊5　Aapache Spark（https://spark.apache.org/）。
＊6　H. Abe, K. Shima, Y. Sekiya, D. Miyamoto, T. Ishihara, and K. Okada. Hayabusa: Simple and fast full-text search engine for massive system log data. In Proceedings of the 12th International Conference on Future Internet Technologies, CFI'17, pages 2:1?2:7, New York, NY, USA, 2017. ACM.

3.4 Hayabusaの分散処理

しかしながら、スタンドアロン環境にはハードウェア性能の限界が存在し、いつかは規模が拡大した他の分散処理クラスタに性能を抜かれてしまうと推測されます。そこでHayabusaは、スタンドアロン環境という制約を取り払い、複数ホストでHayabusaの分散処理環境を構築し、検索性能がスケールアウト可能なアーキテクチャの実現を目指しました。

スタンドアロンで動作するHayabusaを分散処理システムとして再定義し、検索処理性能をスケールアウトさせる実験を行いました。Hayabusaのスタンドアロン処理性能を活かすべく、処理リクエストを高速なRPC(Remote Procedure Call)としてクライアントから処理対象ホストへと送り込みます。GNU Parallelを用いた並列検索を処理ホスト内で実行し、結果はRPCを用いてクライアントへと返し集計を行います。これによりHayabusaが本来実現していた高速なスタンドアロン環境での検索と、RPCによる高速なリクエスト/レスポンスを実現することができます。分散ホスト環境においてスケールアウトする検索機能を実現するために、データの並列蓄積と分散検索に分けて設計を行いました。

3.4.1 並列蓄積と分散検索

検索処理をスケールアウトさせるために、どの処理ホストに処理リクエストが届いても検索可能な状態になるように、今回の実験ではすべての処理ホストに同一のデータを保持させる方法を用いました。これはすべての処理ホストへとsyslogデータを複製して配送することを意味します。これにより、どの処理ホストへ処理リクエストが渡ろうとも同じ結果が返ることが保証されます。

分散している処理ホストへの検索リクエストの実現にはRPCを用いました。Hayabusaの分散処理では、クライアントからのリクエストを受け取った処理ホストは、スタンドアロンのHayabusaと同等にローカルディスクに保存した複数のデータベースファイルに検索クエリを発行することを前提とします。SQLite3のコマンドを検索リクエストのパラメータとして処理ホストに受け渡すことも可能ではありますが、本提案ではスタンドアロンのHayabusaの性能を活かしつつ、シンプルに分散処理を実現するために、スタンドアロン環境で処理されるものと同等のGNU Parallelのコマンドをリクエストのパラメータとして受け渡します。分散検索では複数の処理ホストへと処理リクエストが発行されることから、クライアントが処理リクエストをキューイングし、処理ホストで動作するWorkerがキューイングされた処理リクエストを取得して結果を返すProducer/Consumerモデルを選択しました。これにより、各処理ホストで動作するWorkerは処理リクエストを取得した後に、検索処理の実行が可能となります。

本提案では、すべての処理ホストにデータが複製されていることから、どの処理ホストへ処理リクエストが渡ったとしても同様の処理結果が返されます。また、クライアントからの処理リクエストが特定の処理ホストに集中しないようにロードバランシングを行い、各処理ホストへ均等にリクエストを配布可能にしました。

3.4.2 実装

■ 並列蓄積

syslogをすべての処理ノードへ複製するために、本研究ではオープンソースソフトウェアであるUDP Samplicator[*7]を利用しました。syslogの複製イメージを図-4に示します。UDP Samplicatorは送信元アドレスを変更せずに受信したUDPパケットを指定した対象ホストへ転送することができます。これにより転送先のホストは、あたかも自身が送信元から直接データを受信したかのようにUDPパケットを受信することができます。

通常、UDP Samplicatorは1プロセスでUDPの転送処理を行います。しかしながら大量のsyslogを受信した場合には、プロセスの負荷が上昇しCPUのコア利用率が100%になってし

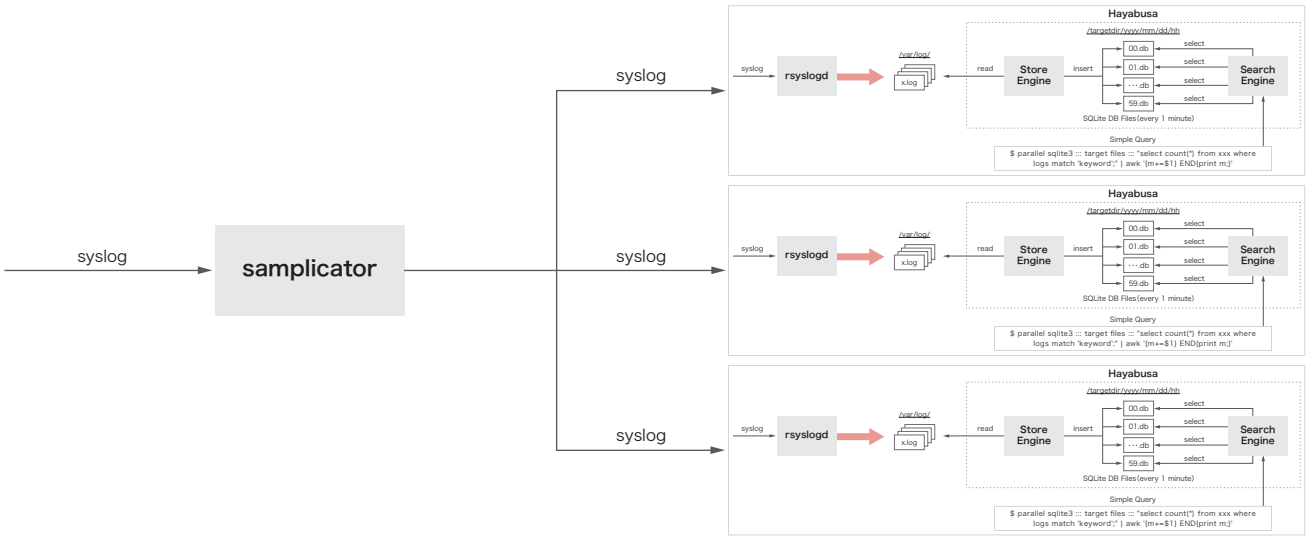

図-4 UDP Samplicatorを用いたsyslogの複製

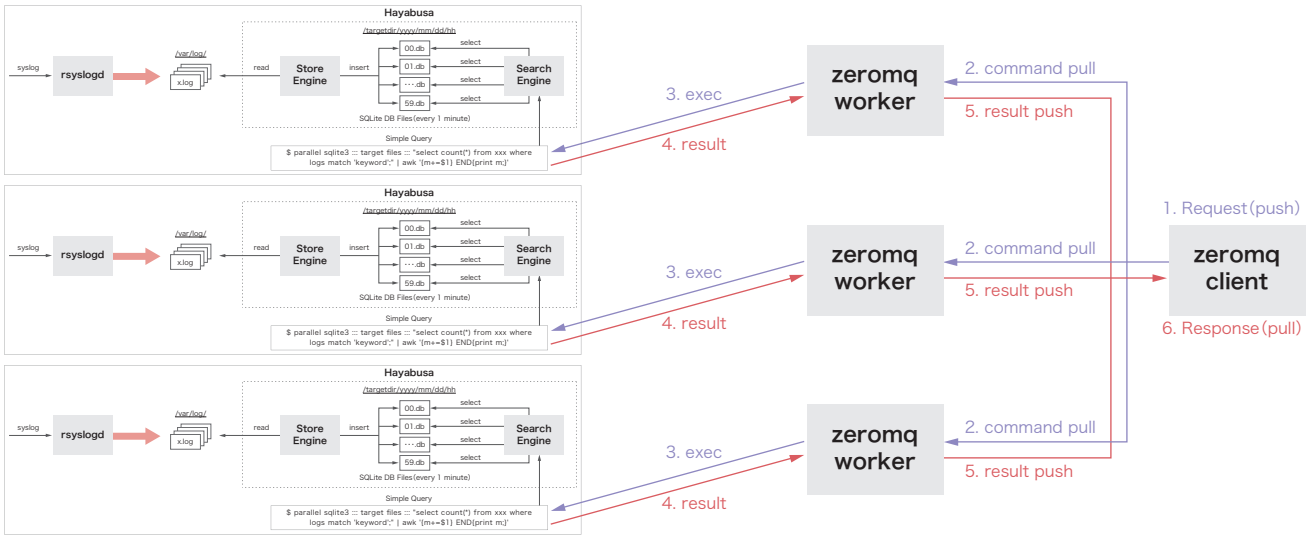

図-5 UDP Hayabusaで用いるZeroMQのPush/Pull実装

*7 UDP Samplicator(https://github.com/sleinen/samplicator)。

まう場合があります。その結果、パケット転送処理が追いつかなくなり、データが破棄される可能性が生じます。そこで本実験ではUDP Samplicatorにパッチを当て、マルチプロセスとして動作するようにソースコードの修正を行いました。具体的には、socketのオプションとして「SO_REUSEPORT」を追加することにより、複数プロセスで同じ待ち受けポートが利用可能となります。本提案の場合には、syslog受信ポートである「UDP 514ポート」が複数プロセスで共有されることとなり、UDP 514ポートへと届いたパケットは、複数のUDP Samplicatorプロセスに自動的にロードバランスされます。これにより大量にsyslogを受信した際でも、1CPUコアではボトルネックになりがちなsyslogパケットの複製と転送をCPUコアスケールすることが可能となります。

■ 分散検索

Producer/Consumerモデルは多くのソフトウェアで実装可能ですが、本研究ではRPC処理が高速に実行可能で、ライブラリを用いることでクライアントとWorkerプロセスを実装可能なZeroMQ[*8]を用いました。ZeroMQは高速に動作する分散メッセージキューとして利用され、「Request/Response」「Publish/Subscribe」「Push/Pull」などたくさんのメッセージングパターンを容易に実装することができます。本提案では、「Push/Pull」パターンを用いてProducer/Consumerモデルを実装しました。

図-5で示すように本提案でのクライアントは、PushとPullの2つの役割を持つように実装しました。これによりリクエストの発行からキューイング、結果の取得と集計をクライアント1プロセスで行うことができます。

3.5 評価

分散システムとしてのHayabusaのスケールアウト性能を調べるため、処理ホストが増加した場合に処理時間が短縮できるかどうかの試験を行いました。処理ホストは1台から10台の範囲で増加し、クライアントは1日分のデータに対して繰り返し100回リクエストを実行します。100回分のリクエスト対象のレコードサイズは、144億レコード(1分間のsyslog流量は10万件と仮定)となります。

図-6に示すように、ホスト1台のときの検索処理時間は約468秒でしたが、ホストの台数を増やすに従いホストの数で割った時間に近づき、10台のホストでかかる処理時間は約10分の1である48秒になりました。

また、秒間に処理可能なレコードのスキャン数はホスト1台の場合には3000万件ですが、ホスト数が10台の場合には10倍である3億件まで増加します。これはホストを1台から10台まで増加させた場合、検索の処理性能がホストの台数に応じて意図したとおりリニアにスケールアウトしていると言えます。

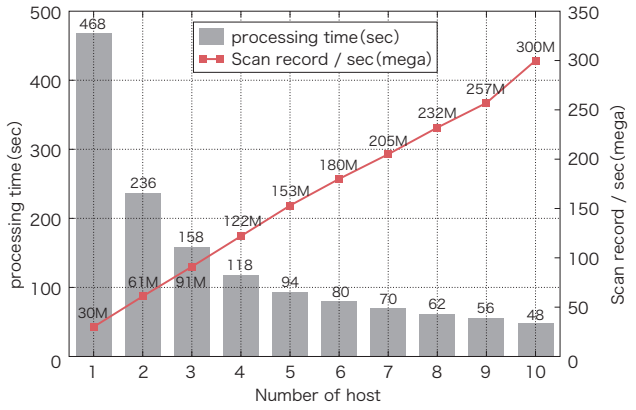

図-6 検索ホストのスケールアウト性能

*8 ZeroMQ(http://zeromq.org/)。

次に10台のホストで処理を実行する場合にWorkerの数を1プロセスから16プロセスの間で増加させました。16という数字の根拠は本実験に用いたサーバのCPUの物理コア数であり、物理コアの数だけスケールアウト可能かどうかを確認する意図があります。10台のホストで1Workerプロセスのみを動作させた場合にかかった処理時間は約48秒でしたが、10台のホストで10Workerプロセスを動作させた場合の処理性能は最高6.1秒となり、処理速度が約8倍高速化しました。10Worker以上の処理速度は横ばいとなったため、16プロセスで最大値を出すためには何かしらの工夫が必要と思われます。

ホスト数とWorker数の両方のスケールアウトを組み合わせた結果、1台の処理ホストで1Workerプロセスを用いた場合で約468秒かかっていた検索時間が、10台で10Workerプロセスを動作させた場合では6.1秒まで短縮し約78倍の高速化が実現しました。

3.6 今後の課題

本研究では検索性能を向上させる分散クエリに対応するため、各処理ホストに同一のsyslogデータを複製する手法を用いました。これは、本質的には重複するデータを大量に複製する行為であり、データの量が増加すればするほどネットワーク帯域と保持するデータに無駄が発生することを意味します。Hadoop[*9]のHDFSのようにレプリケーション数を設定し、複数ホストでデータを分散させ保持することはもちろん可能ではありますが、その場合にはメタデータ管理機構でデータの管理を行い、データアクセスはメタデータ管理機構経由となり、ストレージへのアクセス性能を低下させ、検索自体の処理性能も低下させる恐れがあります。Hayabusaと分散ストレージの利点欠点を考慮し、Hayabusaに適した分散ストレージを実現することが1つの大きな課題となります。

またHayabusaは検索基盤システムとして動作するため、その上で動作する具体的なアプリケーションソフトウェアを組み合わせることでさらなる有益なシステムとなり得ます。

syslogを高速に検索できることから、先行研究であるインベントネットワークにおけるsyslogを用いた異常検知[*10]と組み合わせることで、高速に動作する異常検知アプリケーションを作成することが可能になると考えます。

＊9　Apache Hadoop（http://hadoop.apache.org/）。
＊10　阿部博 and 敷田幹文. イベントネットワークにおけるsyslogを用いた異常検知手法の提案と実でータを用いた評価. In インターネットと運用技術シンポジウム2016論文集, volume 2016, pages 57-64, dec 2016.

3.7 Hayabusaの応用

セキュリティ分野の研究では、攻撃の予測や検知を行うことが目標の1つとされます。

増加するサイバー攻撃に対抗するために、攻撃の兆候をリアルタイムに分析し、発生し得る攻撃とその深刻度、影響範囲を予測することが可能になれば、今まで担当者の能力で担われていたセキュリティ事案に対する属人的な対応を、機械学習や深層学習を用いてサポートすることが可能となります。

IIJ技術研究所は、東京大学、東京工業大学、奈良先端科学技術大学院大学と連携し、「サイバー脅威ビッグデータの解析によるリアルタイム攻撃検知と予測」[*11]プロジェクトへ参加しています。本プロジェクトでは、攻撃の兆候をリアルタイムに分析する基盤として、その一部にHayabusaが組み込まれます。更に、他のデータ解析ソフトウェアや機械学習ソフトウェア(R、Chainer、Pandasなど)と連携をして、攻撃の兆候を統計や機械学習で分析する基盤として動作します。

3.8 まとめ

本稿では、オープンソースソフトウェアであるHayabusaの説明と分散処理による評価について解説しました。評価の対象となるレコード数は144億レコードであり、144億レコードを約6秒でフルスキャンできたということは、GoogleのBigQueryに匹敵するデータのフルスキャン速度が実現できたことを意味します。10台の処理ホストでこれほど高速なスキャンを実現できるということは、コスト面でもリーズナブルで高性能な分散処理システムであると言えます。

なお、本稿のより詳細な解説は論文[*12]として公開されています。

本研究の一部は、国立研究開発法人科学技術振興機構(JST)の研究成果展開事業「戦略的創造研究推進事業(CREST) JPMJCR1783」の支援によって行われています。

執筆者:
阿部 博(あべ ひろし)
IIJ 技術研究所 研究員。

執筆者:
島 慶一(しま けいいち)
IIJ 技術研究所 主幹研究員。

*11 「サイバー脅威ビッグデータの解析によるリアルタイム攻撃検知と予測」(https://www.jst.go.jp/kisoken/crest/project/1111094/1111094_13.html)。
*12 阿部博 and 篠田陽一. スケールアウト可能なログ検索エンジンの実現と評価. In インターネットと運用技術シンポジウム2017論文集, volume 2017, pages 73-80, nov 2017.

インターネットトピック

JANOG 41 Meeting IIJ初のホスト

2018年1月24日～26日に広島で開催されたJANOG 41 MeetingでIIJは初めてJANOG Meeting[*1]のホストを務めました。会期中は小雪がちらつくこともありましたが、おおむね天候にも恵まれ、最終的な参加者数は、本会議1,171名、懇親会725名と、JANOG Meetingはじまって以来過去最高の人数を記録し、盛況のまま無事に終えることができました。ここでは、JANOG 41 MeetingにおいてIIJがホストとして行った取り組みについて紹介します。

■ ホストとしての役割

JANOG Meetingは、日本のインターネットを運用する技術者による団体JANOG（JApan Network Operators' Group）が主催する会議です。年に2回JANOGに集う技術者達が集まって開催されるJANOG Meetingは、会議の運営自体はJANOGのメンバーから選出された実行委員会が行いますが、会場の準備やそれにまつわる諸事をホスト企業が持ち回りで実行します。ホスト企業は各地から集まる参加者をもてなすため、趣向を凝らし快適な会場を用意します。今回、IIJがホストを務めるにあたり重視したのが会場ネットワークの提供です。JANOG Meetingはインターネットに関する実践的な会議ですから、会議中にインターネットを利用するのは自然なことです。また、会場に集まる技術者は現役の運用担当者でもあります。各社のオフィスには留守番を務める技術者も残ってはいますが、時には会場から臨時の作業を行うという局面もあります。そういった需要に応えるためのネットワーク環境が必要になりますが、実際にはその実現に高いハードルがありました。

■ 高い密度と短い構築期間

JANOG Meetingへの参加者数は年々増加しており、ここ数年は600名を超える開催回が続いています。また、IIJがホストを務めた今回は結果的に1,000名を超える参加者が集まりました。会場に集まるほぼすべての技術者がノートパソコンを利用しており、更にスマートフォンやタブレットなど1人で2台以上の端末を利用しているケースも少なくありません。そして会議場という狭い空間にこれだけ高密度に利用者が集まるのもめずらしいことです。

また、ネットワークの規模に反して準備にかけられる時間はあまり長くはありません。1,000名を収容できるホールの利用料は高額なため、JANOG Meetingとして借り受けているのは会期中の3日間のみ。そのため、会場ネットワークの準備には会期初日の午前中しか充てられないという大きな制約がありました。また、会期終了後は速やかに機材を撤収しなければなりません。

■ 会場内におけるインターネット環境の提供

このような制約の中でIIJが目指したのは、高い性能をもったピュアなネットワークです。

IIJは日本全国にバックボーンネットワークを張り巡らせており、広島にもその拠点であるNOCがあります。当地の通信事業者であり、JANOGに参加する仲間であるエネルギア・コミュニケーションズの協力のもと、会場の広島国際会議場には、IIJ 広島NOCに直結する光ファイバを引き込みました（図-1）。本ファイバはIIJが設置したWDM装置により10Gbpsの帯域で運用しています。

また、会場内のネットワークはIPv4・IPv6のデュアルスタックとし、特にIPv4アドレスは日本のネットワーク資源を管理するJPNICの協力のもと、各端末にグローバルアドレスを配布する形にしました。IPv4アドレスの節約、ネットワークセキュリティの確保という観点からLANの中ではプライベートアドレスを利用するのが一般的ですが、改めて大規模なIPv4グローバルアドレスによるLANという環境にチャレンジするという意図によるものです。

■ 会場無線LAN機器

多くの利用者が入れ替わり利用するネットワークですので、会場内では無線LANによるネットワークの構築が必須となります。今回はIIJ自身が開発する無線LAN対応機器であるSA-W2を多数利用しました。SA-W2はIIJが開発・運用する機器マネジメントシステムSACM（Service Adapter Control Manager）と連携が可能な機器で、ネットワークケーブルと電源を接続するだけで稼働状態をマネジメントサーバに自動通知するなど、運用負担を軽減する仕組みが取り入れられています。こうした機器を利用することで、短時間でネットワーク構築を完了させることを目指しました。また、今回は無線LANの提供にあたり当地の広島市立大学と共同研究を行いました。同大学では無線LANネットワークの利用効率改善を目指して、無線アクセスポイントの通信品質を推定するための手法について研究しています。そこでJANOG 41 Meetingにおける無線LAN

＊1　JANOG：JApan Network Operators' Groupを意味し、インターネットにおける技術的事項及びそれにまつわるオペレーションに関する事項を議論、検討、紹介することにより、日本のインターネット技術者及び利用者に貢献することを目的としたグループ（https://www.janog.gr.jp/）。

を対象に、同手法のための計測を行うデバイスをメインホールに設置し情報収集を行いました。この収集作業には特別版のファームウェアを導入したSA-W2を利用しています。IIJは今までにもいくつかのイベントで無線LAN提供を行っており、提供内容についての評価を行ってきましたが、今回広島市立大学と共同研究を実施することで、無線LANネットワークにおける通信品質推定手法に新たな知見が得られるものと期待しています。

■ 今後に向けて

本稿執筆時点において、JANOG 41 Meetingは閉会しており、IIJによるネットワーク提供も終了しています。現在これらの取り組みにより得られたデータの評価を行っており、その成果について4月より順次IIJのエンジニアブログ[*2]において報告を行う予定です。

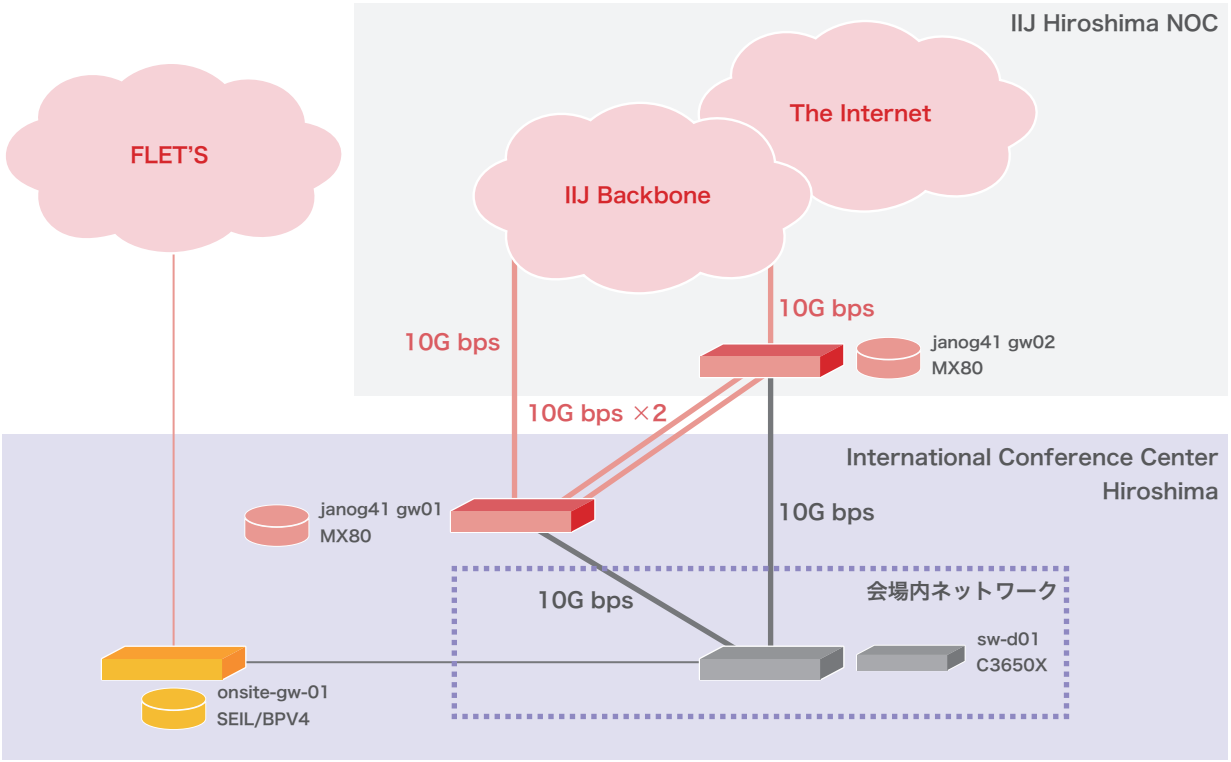

図-1 JANOG 41 Meeting ネットワーク構成図

執筆者:
堂前 清隆（どうまえ きよたか）
IIJ 広報部 技術広報担当課長 兼 MVNO事業部 MVNO事業統括室 シニアエンジニア。

＊2　IIJ Engineers Blog（http://eng-blog.iij.ad.jp/）。開発・運用の現場エンジニアが執筆する公式ブログ。

March 2018 Vol.38

IIJ
Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

本冊子の情報は2018年2月時点のものです。

IIJ-MKTG019-0038

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：https://www.iij.ad.jp