IIR

Internet
Infrastructure
Review

Jun.2020
Vol.47

定期観測レポート

メッセージングテクノロジー

フォーカス・リサーチ(1)

農業IoTでのLoRaWAN®普及に向けたIIJの取り組み

フォーカス・リサーチ(2)

新型コロナウイルスのフレッツトラフィックへの影響

IIJ
Internet Initiative Japan

Internet Infrastructure Review

June 2020 Vol.47

エグゼクティブサマリ

前回の「IIR」エグゼクティブサマリの冒頭で新型コロナウイルス感染症について触れました。それから今日に至るまで、新型コロナウイルスのことを意識しない日はなく、多くの国でロックダウンが行われるなど、まん延防止に向けた努力が世界中で続けられています。

そのような状況のなか、情報通信技術の利活用が脚光を浴びています。外出自粛を強いられた人々に対して動画ストリーミングなど自宅での娯楽を提供するための情報通信技術、人と人の接触機会を減らしながらも仕事を継続するためのリモートワークを支える情報通信技術、学校閉鎖によって登校できなくなった生徒や学生の遠隔学習を実現する情報通信技術、経済的に困窮した人へ円滑に援助を届けるための情報通信技術など、新型コロナウイルス禍における私たちの生活を支える上で大きな役割を果たしています。一方、端末や監視カメラを介した公的機関による感染者の監視など、情報通信技術の利活用に関する個人のプライバシーと公益のバランスをどのように考えるべきかという課題や、前回の本稿でも指摘したようなインターネットで流通する情報の信頼性に関する課題も指摘されています。この危機を乗り越えるために、行政、医療、エネルギー、運輸、流通など、多くの産業の従事者による懸命の取り組みがなされています。情報通信産業も社会を支える重要なインフラの1つとして、今まで以上の役割を果たすべく、技術の開発に励んでいきたいと思っています。

「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、私たちが日々のサービスの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章は定期観測レポートです。ここでは1年で4つのテーマを順番に取り上げていますが、本号は電子メールを中心とするメッセージングテクノロジーの回となります。IIJでは、メールサービスにおいて、メール受信時にSPF、DKIM、DMARCの送信ドメイン認証機能を提供しており、その認証結果を継続的に観測しています。そして、普及が進んだSPFやDKIMに対して、DMARCの普及率が依然として低いという観測結果が得られており、引き続き普及活動を継続していく必要があることが分かりました。また、送信ドメイン認証技術のフィッシングメールへの活用やJPAAWG 2nd General Meetingについても触れていますので、ご一読ください。

2章のフォーカス・リサーチでは、IIJの農業IoT分野におけるLoRaWAN®の活用事例を取り上げています。LoRaWAN®は、LPWA（Low Power Wide Area＝低消費電力・長距離）を実現するIoT向けの無線通信ネットワークで、通信事業者に頼らず自営で構築・運営できることから、注目を集めています。我々が実際に取り組んだ事例として、水田で基地局やIoTデバイスを設置することで得られた知見や課題など、興味深く読んでいただけると思います。

3章のフォーカス・リサーチは、新型コロナウイルス禍のなかで情報通信が果たした役割の検証でもあります。日本では2月以降、政府による学校の閉鎖要請、都道府県による外出自粛要請、政府による緊急事態宣言など、社会活動を制約する要請が、異なるタイミングで発出されました。その際、それぞれのタイミングでの固定ブロードバンドのトラフィックパターンの変化を分析することで、各要請によりインターネットの利用がどのように変わったのかを推測できます。これらはインターネットのインフラ整備の重要性を再認識する上で貴重なデータになると考えています。

IIJでは、このような活動を通して、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。

メッセージングテクノロジー

1.1 はじめに

フィッシング対策協議会の報告[*1]によれば、協議会に寄せられたフィッシングの報告件数が急増しています。2020年4月には11,645件が報告されており、これは前月（2020年3月）から1,974件の増加であり、前年同月（2019年4月）から9,257件もの大幅増加となっています。内容としては、インターネットを活用する大手事業者をかたったものが大量配信されているようです。実際、私のところにも何通か届いていますが、表題（Subjectヘッダ）や送信者（Fromヘッダ）のディスプレイネームやローカルパートはそれらしい文字列となっていますが、送信者のドメイン名は全く異なっている場合が多いようです。また、行政機関になりすました詐欺的なメールが増えてくる可能性もありますので、なりすまされる可能性が高いドメインの所有者、メール受信側それぞれで対策を講じるべきです。

これまでも何度も報告してきたとおり、フィッシングメールなどのなりすましメールの対策としては、送信ドメイン認証技術が有効に機能します。しかしながら、フィッシングメールの送信者もこうした対策は把握しているようですので、有効活用するための正しい使い方が重要となります。また、こうしたメールが増えている背景としては、昨今の社会状況も反映しているのではと推測されますので、しばらくは続くかもしれません。

本報告では、なりすましメール対策に有効である送信ドメイン認証技術（SPF、DKIM、DMARC）の普及状況について報告します。また、送信ドメイン認証の結果を、現在流通しているフィッシングメールに対して活用する方法についても述べます。更に、昨年開催されたJPAAWG 2nd General Meetingの様子についても報告します。

1.2 送信ドメイン認証技術の普及状況

最初のSPF（Sender Policy Framework）の仕様であるRFC4408[*2]が2006年4月に発行されてから14年が経過しました。その後、電子署名を利用するDKIMが仕様として作られ、SPF、DKIMの認証結果を利用するDMARCも作られました。これらの送信ドメイン認証技術が、現在どの程度普及しているかについて報告します。

＊1　フィッシング対策協議会 | 月次報告書一覧（https://www.antiphishing.jp/report/monthly/）。
＊2　その後2014年4月に改定されてRFC7208となった。

1.2.1 受信メールに対する調査結果

送信ドメイン認証技術の普及率を調査する観点として、実用上の効果を考えれば、メール受信時の認証結果の割合が重要であると考えることができます。IIJが提供するメールサービスでは、メール受信時にSPF、DKIM、DMARCの送信ドメイン認証機能を提供しています。受信メールのうち、それぞれで認証ができなかった場合の結果はnoneとなります。つまり、受信メールに対しての認証結果noneを除いた割合が受信メールに対する普及率の割合と言えます。

最新の2020年4月に受信したメールに対しての、SPFの認証結果の割合を図-1に示します。認証結果noneの割合は12.1%、つまり普及率は87.9%であったと言えます。1年前のIIR Vol.43では普及率が85.7%でしたので、2.2%増加したことになります。SPFによる認証成功を示すpassの割合は、2019年4月の70.1%から2020年4月には79.1%に9%増加しています。つまり認証失敗（SPFの場合はhardfail、softfail、neutral）の割合も6.4%減っていますが、これはSPFとしてなりすまさないメールが増えたことを示しています。しかし、いわゆるなりすましメール自体が減少しているわけではないことは、フィッシングメール報告の増加からも推測できます。つまり、SPFとしてはなりすまさない、なりすましメールが増えている可能性があります。

2020年4月に受信したメールに対してのDKIMによる認証結果の割合を図-2に示します。認証結果noneの割合が51.7%となり（普及率48.3%）、1年前の62.2%から10.5%減少、普及率としては10.5%増加したと言えます。メール送信側としてDKIMを導入するためには、送信時のメールサーバなどで、DKIMの電子署名を追加する必要があり、送信側の導入には手間がかかります。現在の普及率が十分な割合とは言えませんが、それでもDKIMの最初の仕様であるRFC4871が公開されて13年が経過し、ようやく受信メールの半分程度まで普及してきたことになります（IIJの受信メールに対する割合としてです）。

2020年4月に受信したメールに対してのDMARCによる認証結果の割合を図-3に示します。認証結果noneの割合が75.4%なので、普及率は24.6%であると言えます。1年前からは1.5%

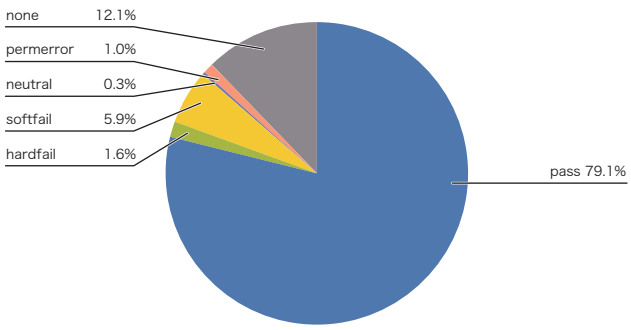

図-1 SPFによる認証結果割合

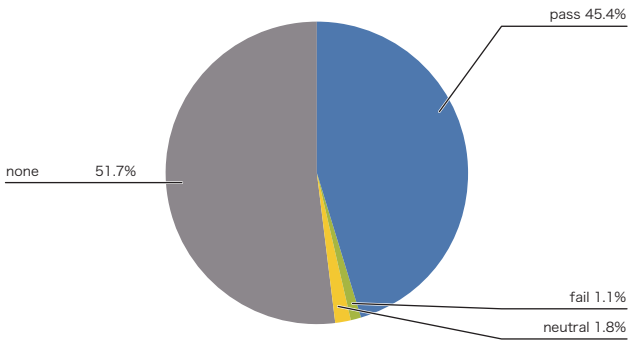

図-2 DKIMによる認証結果割合

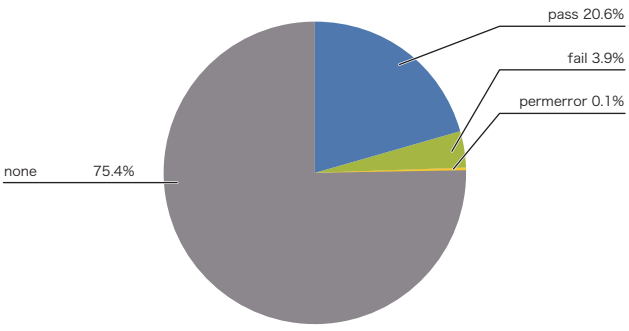

図-3 DMARCによる認証結果割合

増加しました。ほぼ実用上普及したと言えるSPFや一般的に導入にコストが伴うDKIMと比べると、非常に低い増加です。DMARC導入には、SPFあるいはDKIM、またはその両方の導入が必要ですが、それらを導入さえしていれば、SPFと同様にDNS上にDMARCレコード（テキスト資源レコード）を記述するだけでDMARCは導入できます。むしろ送信メールサーバの出口を調べなくても良いので、DMARCレコードの方が簡単に設定できるはずです。そうした背景がありながら、SPFやDKIMより割合としての増加値が少ないことの理由は、単に認知していないのか、DMARCレコードを記述する動機が不明と考えているのか、まだよく分かっていません。今後も普及のための活動を継続していきたいと考えています。

図-4に2016年1月からのDMARCの認証結果の割合の推移を示します。このグラフからも、2020年4月が時期的に極端に低かったということではなく、少しずつDMARCに対応した送信ドメインは増えてきているものの、その伸びが非常に緩やかであったことが分かります。

図-5に、DMARCがpassしたドメイン名のTLD（Top Level Domain）の割合を示します。これは、受信したメール量に対する割合ではなく、DMARCドメイン名別（ユニークなドメイン名）のTLDの数の割合です。最も割合が高いTLDは.comで53.2%でした。続いて2番目に割合が高いのが.netで9.5%、日本の.jpドメイン名が3番目で6.7%でした。SPFがpassしたドメイン名のTLDでも.comが最も多いTLDでしたので、順位的には大きな違いはありませんでした。

1.2.2 ドメイン名に対する調査結果

送信ドメイン認証技術の普及率に関するもう1つの観点は、登録されているドメイン名に対して、各送信ドメイン認証技術に関連するレコードがどの程度登録されているかを調べることです。そのためには、対象の範囲を決めてそこに属するすべてのドメイン名を得る必要があります。

IIR Vol.39でも報告したとおり、jpドメイン名に対する調査を、（株）日本レジストリサービス（JPRS）と協力して実施しており、

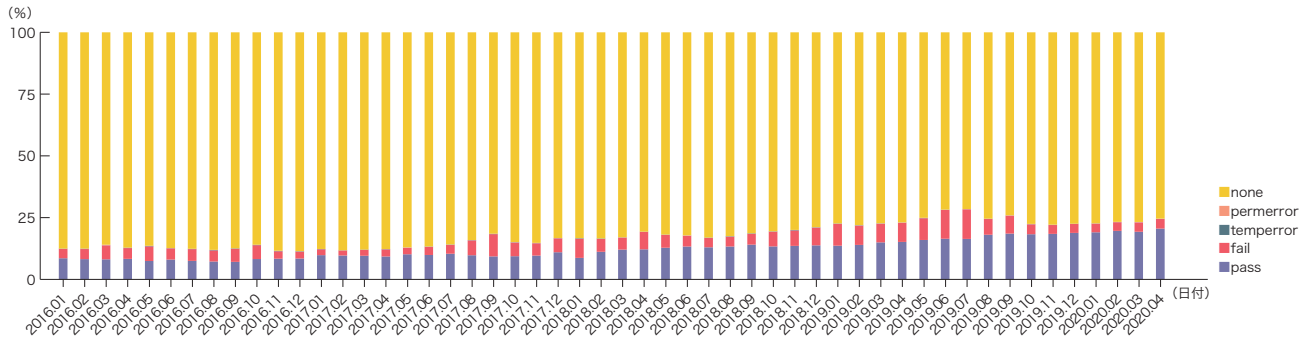

図-4 DMARCによる認証結果割合の推移

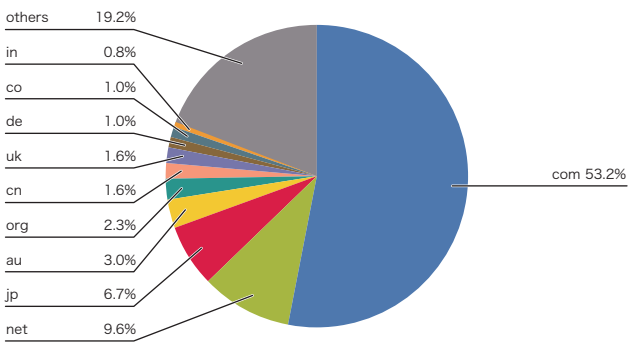

図-5 DMARCドメイン名のTLDの割合

現在は(一財)インターネット協会(IAjapan)との間で共同研究契約を結んでいます。筆者はIAjapanの立場で設定状況を調査しています。

DKIMは、電子署名のための情報(DKIMレコード)を取得するためにDKIMのセレクタ名が必要ですが、セレクタ名はメールのヘッダに指定されているため、ドメイン名からだけではDKIMレコードの場所を得ることができません。DKIMレコードが設定されているかを推測できる場合もありますが[*3]、必ずしも正確ではありません。そのため、DKIMの普及状況に関する調査結果は公開しておらず、SPFとDMARCのみが公開されています[*4]。いずれも、メールに利用されているドメイン名であることを確認するために、MX資源レコードが設定されているドメイン名に対しての割合となっています。もちろん、メールに利用しないドメイン名に対するSPFやDMARCレコードの設定方法(最近ではMX資源レコードについても)もありますが、これらの詳細はまた別の機会に報告したいと思います。

今回は、これらSPFとDMARCの最新の調査結果を含めて報告します。SPFは、調査開始当初の2018年3月にはjpドメイン名全体の平均で57.3%でした。最新の2020年5月の調査結果では65.1%となり、7.8%増加しています。

DMARCのjpドメイン名での普及率の推移を図-6に示します。2018年3月が0.57%で、2020年5月では1.19%となり、0.62%増加しました。割合は2年ほどで倍増はしましたが、そもそもの設定割合が低いのと、増加自体もSPFに比べても非常に低い値であり、いずれの数値も非常に低い結果となりました。属性別で現在最も設定割合が高いのはgo.jpドメイン名で、それでも5.4%です。go.jpのSPF設定割合は92.4%ですので、DMARCレコードの設定もSPFと同様の取り組みで、率先して設定を増やすことを期待しています。

1.2.3 なりすましメール対策としての送信ドメイン認証技術

現在の社会状況により、行政機関などによる様々な施策が行われており、その過程でメールによる連絡が増えてくることが予想されます。また、外出を避ける傾向からオンラインでの購入などが増えているようです。これらの状況を反映して、フィッシングメールやなりすましメールによる詐欺的行為が増えているかもしれません。

例えば、Amazon社になりすますメールがいくつかのパターンで頻繁に送信されていますが、Amazon社からのメールは、SPF、DKIM、DMARCいずれも対応しており、これらの送信ドメイン認証を行えば、なりすましメールかどうかを判断することができます。また、SPFの認証失敗時には、最も強い失敗failとなるようにSPFレコードの末尾が"-all"となっており、DMARCのポリシーも比較的強めの"p=quarantine"と設定されています。つまり、Amazon社では送信ドメイン認証技術を積極的に取り入れ、なりすましメール対策を強化していると言えます。Amazon社をなりすますメールで気をつけなければならないのは、認証したドメイン名が正しいかを確認する必要もあることです。日本でAmazon社が利用するドメイン名はamazon.co.jpですが、なりすましメールの多くは、全く関係のない別のドメイン名を用い、SPFやDMARCがpassするようなりすましメールを送信します。件名(Subjectヘッダ)や送信者(Fromヘッダ)の表示名(display name)にはAmazonの文字列が含まれています。そのため、きちんと認証されたドメイン名も含めて確認することがだまされないためには大事です。

＊3　ドメイン認証の普及率に対する測定方法(http://member.wide.ad.jp/wg/antispam/stats/measure.html.ja)。
＊4　迷惑メール対策|統計データ(https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei)。

図-6に示した属性別のjpドメイン名の中で、調査開始当初から継続してDMARCの導入割合が最も低いのは、地方公共団体などで利用されるlg.jpドメイン名です。地方公共団体がlg.jpだけを使っているわけではないと思いますが、示している導入割合はMXレコードを設定しているドメイン名に対するDMARCレコードの設定割合ですし、SPFレコードの導入割合はgo.jpに続く80.7%と高い普及率でした。これも同様に、なりすましメール対策するためには、まずDMARCレコードを設定することでヘッダ上の送信ドメインを守ること、更にどれだけ当該ドメイン名をなりすましたメールが送信されているのかを理解するために、DMARCレポートを受信する設定を行い、状況を随時把握できるようにしておくことが必要と考えています。

1.3 JPAAWG 2nd General Meeting

2019年11月14日と15日の2日間で、JPAAWG 2nd General Meeting（GM）をベルサール飯田橋ファーストで開催しました（図-7）。2018年と同様にIAjapan主催の迷惑メール対策カンファレンスとの併催です。IIJはプラチナスポンサーとして、1stに引き続きサポートしました。

2nd GMでは、1st GMの結果を踏まえ、以下のような新たな試みを行いました。

1. 2日間での開催
2. M^{3}AAWGメンバーなど海外からの多くの講演や参加
3. トレーニングセッション（有料）の開催
4. Open Round Tableによるディスカッション

特にOpen Round Table（ORT）は、M^{3}AAWG[*6]のGeneral Meetingでも毎回開催されている、テーマごとに興味を持つ参加者が集まって議論するセッションです。M^{3}AAWGでは、このORTから新しい技術仕様やBest Practicesなどの文書が作られる発端にもなる、いまや活動の原動力の1つです。今回JPAAWGでは、5つのテーマを用意し、JPAAWGメンバーらのモデレータが進行を務め、一方的ではない参加者相互による議論を行うことができました。JPAAWGでは、課題の共有や解決のための検討の場として、ORTのような取り組みを継続していきたいと考えています。

2020年度も、JPAAWG 3rd General Meetingを同様に開催したいと考えていました。しかしながら、現時点では多くの人が集まっての開催がなかなか難しい状況となっています。現在、どういった形式で開催できるのかを検討している段階ですので、決まり次第Webサイト[*7]などで告知します。

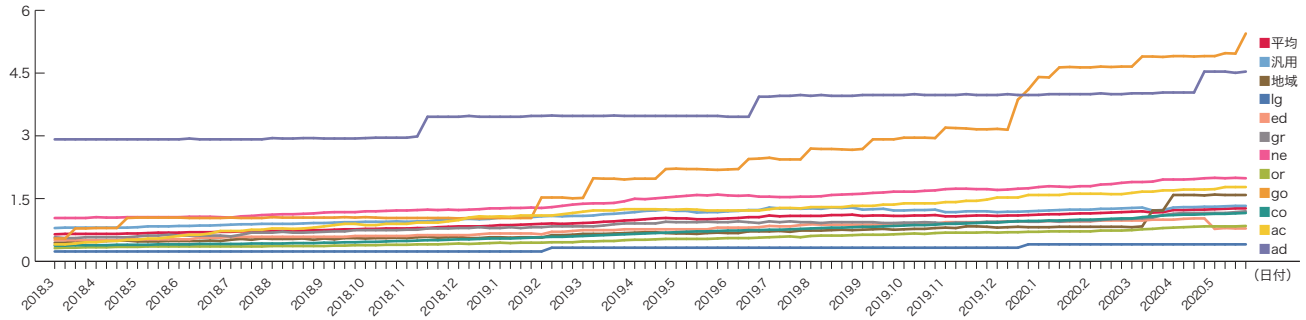

図-6 jpドメイン名[*5]のDMARC普及割合の推移

＊5　地域型（新規登録終了）には都道府県型を含む。
＊6　Messaging, Mobile and Malware Anti-Abuse Working Group（https://www.m3aawg.org）。
＊7　Japan Anti-Abuse Working Group（JPAAWG）（https://www.jpaawg.org/）。

1.4 おわりに

2020年1月22日から24日に札幌で開催されたJANOG45ミーティングに参加し、「フィッシングの現状とその対策」のセッションで発表を行いました。本稿でも述べたとおり、送信ドメイン認証技術、特にDMARCがあまり普及していない現状から、多くの関係者にまず理解してもらうべきと考え参加しました。また、2020年2月17日から20日に米国サンフランシスコで開催されたM^{3}AAWG 48th General Meetingでも、JPAAWGのBoF会合を引き続き開催すると共に、JPAAWGの活動内容を「State of Messaging Anti-Abuse in Japan」のセッションで他のJPAAWG/M^{3}AAWGメンバーと共に紹介してきました。

このように2020年は、国内と海外でそれぞれ講話をする機会が得られ、より積極的な情報発信を目指していましたが、ご承知のとおりその後の状況変化により、様々な会合が開催形態の見直しを余儀なくされています。しかしながら、我々はインターネット上の様々なツールが正しく使われていくことを目指す活動をしているのですから、こうした状況においてもコミュニケーションできるように、またそうしたツールが悪用されないような取り組みをしていくべきと考えています。

図-7 JPAAWG 2nd General Meetingの様子

執筆者:
櫻庭 秀次（さくらば しゅうじ）
IIJネットワーククラウド本部アプリケーションサービス部担当部長。コミュニケーションシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織と協調した各種活動を行う。M^{3}AAWGの設立時からのメンバー。Japan Anti-Abuse Working Group（JPAAWG）会長。迷惑メール対策推進協議会座長代理、幹事会構成員、技術WG主査。一般財団法人インターネット協会客員研究員、迷惑メール対策委員会委員長。一般財団法人日本情報経済社会推進協会（JIPDEC）客員研究員。

農業IoTでのLoRaWAN®普及に向けたIIJの取り組み

2.1 はじめに

IoTを活用した取り組みは様々な分野で急速に広がりを見せています。製造、医療、自動車など、様々なユースケースが広がる中で、IIJでは農業分野にも注目しています。農業は、国を支える根幹の産業であるにもかかわらず、深刻な高齢化・後継者不足や収益性の悪化など、課題が山積しています。農林水産省もこの課題を解決すべく、1つのキーワードとして「スマート農業」を掲げ、日本全国で積極的な実証実験を進めています。

そのような状況の中、IIJも日本の農業を少しでも楽にし、収益を上げられるようにするために我々の力を生かせないかと考えています。IIJが注目している最新の無線通信技術「LoRaWAN®」を採用した水田センサーを開発するなど、実績を積んできました。

農業でIoTを使うにあたって最大の課題となるのが「通信の確保」です。そこで、我々が現場での基地局の設置工事や通信性能の評価などを通じて、実際に体験し手探りで培ってきたノウハウについて、掘り下げて解説します。

2.2 IoTを活用した水田管理実験

IIJでは2017年からの3年間、農研機構生研支援センターの「革新的技術開発・緊急展開事業(うち経営体強化プロジェクト)」の支援を受け、水田の水管理の省力化を可能とする低コストのICT水管理システムの開発と実証実験を進めてきました。水田の水位と水温を測定する水田センサー、無線基地局、スマートフォン用の水管理アプリ、クラウドサービスとしてその成果をパッケージ化し、「水管理パックS」として今年から販売しています(図-1)。「水管理パック S」の水田センサーと無線基地局間の通信はLoRaWAN®で行われます。また、「水管理パックS」の水田センサーと無線基地局、そして水田センサーで測定した水位に応じて水量を自動制御する給水バルブをセットにし、水管理を自動化するパッケージも販売しています。

通信事業者であるIIJが農業IoTという未知の領域で、更に水田センサーのような専門外のデバイスを新規開発するというのは、チャレンジングな取り組みで苦労の連続でした。そちらの取り組みについては「The IIJ Stories」で紹介しています*1。

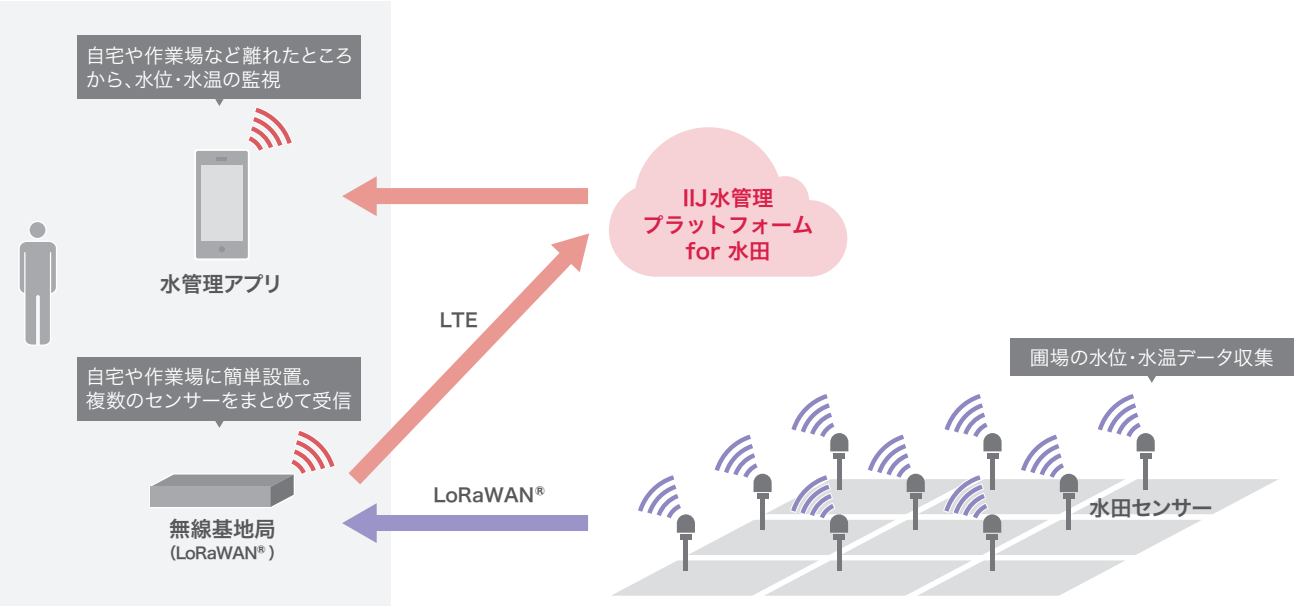

図-1「水管理パック S」による水田の水管理の省力化

*1　つなぎ、つながる、物語 ～The IIJ Stories｜稲作農家の「働き方改革」を後押し IoTが日本の農業の未来を変える(https://www.iij.ad.jp/interview/03.html)。

本稿ではIIJの事業領域である無線基地局側に焦点を当て、農業IoTでのLoRaWAN®普及に向けた取り組みについて解説します。事業領域と言っても未経験のことが多く、様々な苦労がありました。特に通信状況の実測には、北は北海道から南は九州まで何度も現地に足を運んで行いました。そうした苦労により得られたノウハウについて紹介する前に、まずは予備知識としてLoRaWAN®の概要と他方式に対する特徴について説明します。

2.3 1基地局で数kmをカバーするLoRaWAN®

2.3.1 LoRaWAN®とは

LoRaWAN®は米Semtech社が開発したLoRa®というスペクトラム拡散変調を使った無線ネットワークです。LoRa®による通信は図-2のようにWi-FiやBLEに比べて通信速度が遅い代わりに、LTEよりも更に広い通信範囲を実現可能という特徴を持ちます。また、省電力で電池駆動でも数年間、通信可能なデバイスを製作することができます。「水管理パックS」の水田センサーはこの特徴を生かして、無線基地局1台で数kmの範囲をカバーし、単3電池2本で1シーズンの稲作期間を電池交換なしで動作させることが可能です。

LoRa®を使った無線ネットワークには独自プロトコルを使ったものもありますが、標準規格であるLoRaWAN®はIIJを含む400社以上が加盟するLoRa Alliance®で仕様が策定されています。認定機器(LoRaWAN® certificated)は相互接続が可能なため、異なるメーカ製のセンサーなど接続機器の選択肢を広げることができます。

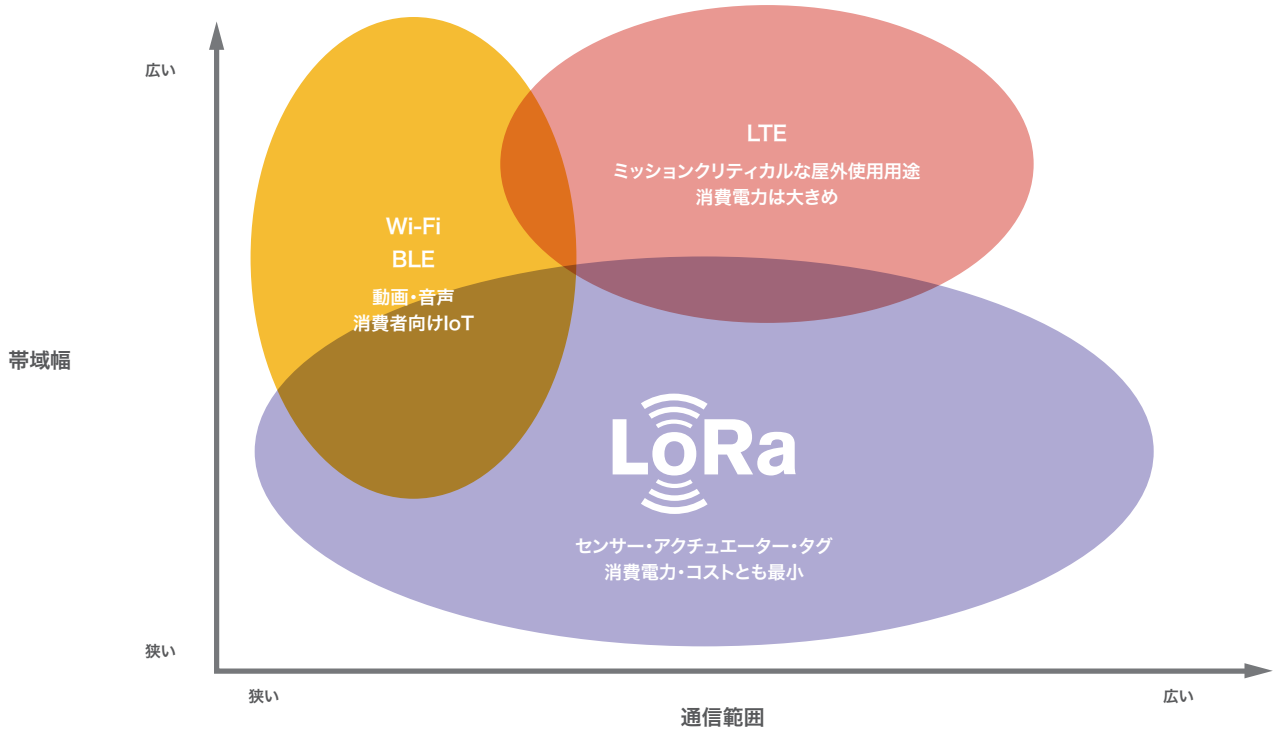

図-2 LoRa®の位置づけ

LoRaWAN®を使ったシステムの構成を図-3に示します。デバイスはゲートウェイとLoRaWAN®で通信します。ゲートウェイはLTEやWi-Fi、または有線イーサネット経由でネットワークサーバと呼ばれるネットワーク管理サーバと接続します。ネットワークサーバはデバイスのアクティベーション、複数のゲートウェイで受信した同じデバイスからの重複データの排除、データごとのアプリケーションサーバとの通信経路の制御、データレートの動的制御などの管理機能を提供します。アプリケーションサーバはREST APIなどを介してネットワークサーバと通信し、デバイスから受信したデータの蓄積やアプリケーションによる可視化、ユーザ操作や事前に設定された条件に従った自動判定によるデバイスの制御を行います。

2.3.2 他のLPWA規格に対する特徴

LoRaWAN®はLPWA（Low Power Wide Area）と呼ばれる低消費電力、低ビットレート、広域カバレッジを特徴とする無線ネットワークの一種です。LPWAには他にSigfoxやLTE-Mなどを代表とする多数の無線ネットワークがあります。SigfoxやLTE-Mは通信事業者が基地局を全国展開しており、通信エリア内であれば基地局を自前で設置しなくても利用可能です。

Sigfoxはデバイス1台あたりの利用料が年額100円～（但し契約デバイス数による）と非常に安価で、2020年1月時点で人口カバー率95%を実現しています。基本的には上り通信のみで1回の送信データサイズは12バイトまで、1日の最大送信回数が140回までの制限がありますが、この特徴を生かして既にガス検針で85万台の対応デバイス導入が決まっているなど、国内の普及台数でリードしている状況です。

LTE-Mは3GPPで標準化されており、NTTドコモ、KDDI、ソフトバンクの携帯通信事業者3社が国内サービスを提供しています。1.4MHzの通信帯域幅を使用すれば最大1Mbpsの双方向通信が可能で、リモートでのデバイスのファームウェアアップデートを実現するFOTA（Firmware Over-The-Air）にも対応します。移動時の基地局の切り替えを行うハンドオーバーにも対応しており、通常のLTEに近い使用方法が可能です。ただし、各社の通信ネットワークのみを利用する場合、1万台までの利用ではデバイス1台あたり月額100円～150円の通信量がかかるので、Sigfoxに比べて大幅に高くなります。

LoRaWAN®は一部の通信事業者が自社基地局やユーザ間での共有基地局を提供していますが、基本的には自前の基地局

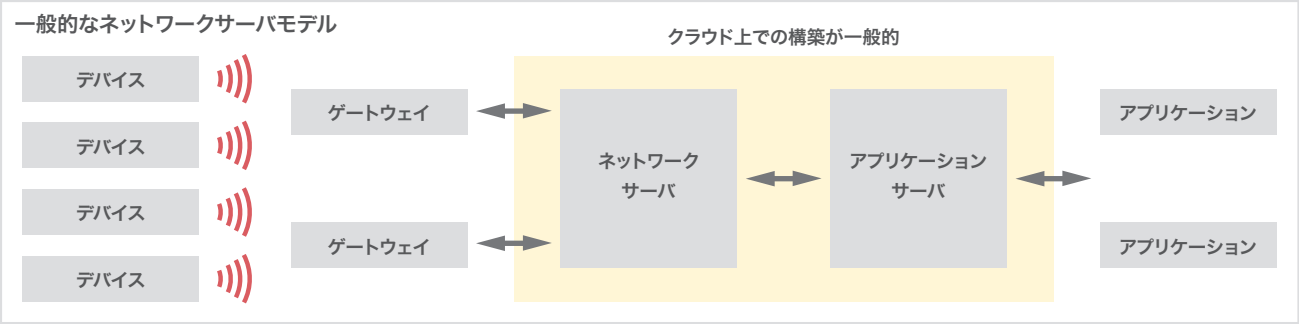

図-3 LoRaWAN®を使ったシステム構成図

設置が必要です。基地局として使用するLoRaWAN®ゲートウェイは「水管理パック S」に含まれるKiwi Technology製「TLG3901BLV2」のように、LTE対応の一般的なIoTゲートウェイに近い低価格のものが販売されています(図-4)。

2.3.3 LoRaWAN®に適した用途

LoRaWAN®で自前の基地局設置が必要な点は、機器代と設置のコストを考えるとSigfoxやLTE-Mに対するデメリットとなります。しかし、地下や建物の奥など屋外基地局でカバーしきれないエリアを基地局の追加でカバーできるのはメリットとなります。また、デバイスとゲートウェイ間の通信費用がかからないので、少ない基地局で多くのデバイスを収容する場合はコストメリットが大きくなります。特に工場やショッピングセンター、オフィスビルなどの大型の建物で、電池駆動するデバイスを多数設置して低コストで運用する用途ではLoRaWAN®が適していると考えています。

水田水管理を含む農業IoTにおいても、給水バルブのようなデバイスの制御が必要になる場合は、下り通信の制限がないLoRaWAN®が有効です。また、農業IoTでは高額な機器やサービスの利用は収益性確保の点で難しい場合が多く、機器が安価で様々な種類のデバイスを多数設置しても安価なサービスが利用できるLoRaWAN®のメリットを生かせます。例えば、水田水管理用の水田センサー・給水バルブ、雨量や気温を測定する気象センサー、地温や土壌水分を測定する土壌センサーなど、様々なメーカの様々な種類のLoRaWAN®対応デバイスが既に農業IoT向けに提供されており、1つのLoRaWAN®基地局に収容することができます。山間部のように通信事業者の基地局による通信が困難な場所では、自前の基地局設置で通信エリア化できる点もメリットです。

2.4 農業IoTにおけるLoRaWAN®普及の課題

ここまで、

- LoRaWAN®の特徴やそれに適した用途
- 農業IoTでのLoRaWAN®のメリット

について述べました。では、農業IoTにおけるLoRaWAN®普及の課題は何でしょうか。

2.4.1 屋外での安価な基地局設置

3年間の水田水管理IoTの実証実験で主に基地局設計を担当してきた筆者の経験上、やはり基地局の設置場所と電源の確保が最も大きな課題だと考えます。

屋外型LoRaWAN®ゲートウェイ「TLG7921M」は防水型で通信性能が高く、建物屋上や山などの高い場所に設置すれば広いエリアを1台でカバーすることが可能です。しかし、屋内型LoRaWAN®ゲートウェイよりも高価で電気配線を含めた設置費用も高額となり、地域での一括導入など相当の規模での導入でなければコストが高くなってしまいます。

図-4 Kiwi Technology製「TLG3901BLV2」

Kiwi Technology製「TLG3901BLV2」は「水管理パック S」にも含まれている非常に安価なLoRaWAN®ゲートウェイです。屋内型のため農業経営体の事務所や自宅に設置していただくことを想定していますが、事務所や自宅は水田センサーを設置する圃場から遠い場合も多く、安定した通信が行えない場合があります。圃場に近い場所で電源が確保できる民家などに設置させてもらえればよいのですが、LoRaWAN®ゲートウェイが使用する電気代の負担などをユーザ自身で交渉してこのような民家に設置させてもらうのは現実的には難しいと思います。

2.4.2 容易な通信状況の事前確認

屋外での安価な基地局設置が可能になったとしても、デバイスとの通信が問題なく行えることを容易に事前確認できないと基地局の設置場所の変更や追加設置が必要になる恐れがあります。

基地局の設置予定場所の緯度、経度、設置高さを入力すると、周辺のデバイスの通信状況をシミュレーションできる有償の電波シミュレーターが数社から提供されています。我々もそのうちの1つを実際に試したのですが、その時点で使用した電波シミュレーターは地形データは含まれているものの建物や樹木の情報が含まれておらず、それらによる通信への影響は確認できませんでした。水田水管理IoTの実証圃場近辺で電波シミュレーターの結果と実測結果を比べたところ、建物が少ない場所ではおおよその傾向は一致していましたが、そのような場所でも建物が近いと少しデバイスの位置をずらしただけでも大きく通信成功率が変化することもありました。将来的に建物や樹木のデータが電波シミュレーターに反映されたとしても、すべての建物や樹木のデータを反映することは難しく、最新の状態を反映することも難しいと思われるので、実測結果とのずれが生じるのは仕方がないと思われます。また、実測結果では交通量の多い道路近くでは通信が安定しないこともありました。そういった時間的な通信状況の変化の電波シミュレーターでの確認は将来的にも難しいでしょう。

やはり通信状況のシミュレーションによる事前確認には限界があり、実測しないとはっきりしたことは言えないことが分かりました。しかし、我々や委託業者が基地局やデバイス設置の都度、測定するのでは、対応に限りがあり費用もかかります。

2.5 課題の解決策

ここまで、

- 屋外での安価な基地局設置
- 容易な通信状況の事前確認

のいずれかが実現できなければ、農業IoTでのLoRaWAN®の普及は難しいことを述べました。

我々はこれらの課題を解決するために、農業経営体ができる限りDIYで対応できるようにすることを目指しました。それらの解決策について紹介します。

2.5.1 DIYソーラー基地局による設置場所の拡大と設置コスト削減

「水管理パック S」に含まれる屋内型LoRaWAN®ゲートウェイ「TLG3901BLV2」を防水対応にし、安価なソーラーパネルとバッテリーで電源不要にできれば、今までは設置できなかった圃場脇などに設置して安定した通信が行えるようになります。そこで、安価なソーラーパネルとバッテリー、ネット通販やホームセンターで手軽に入手できる部材だけで構成し、農業経営体が自力で簡単に設置できるDIYソーラー基地局パッケージを提供することにしました。農業経営体は自力でビニールハウスなどを設置されている方も多くDIYには慣れており、工具類も豊富にお持ちの場合が多いので、分かりやすい手順書さえ用意すればユーザ自身で設置できると考えています。また、圃場脇であれば設置場所の確保も容易になり、安価なので自然災害や盗難による被害が発生しても復旧しやすいと考えています。

*2 IIJ Engineers Blog、「ソーラーパネルで動くLoRaWAN®基地局をスマート農業向けにDIYで設置してみた（前編・後編）」（https://eng-blog.iij.ad.jp/archives/5567）（https://eng-blog.iij.ad.jp/archives/5599）。

検討中のパッケージは「TLG3901BLV2」に7万円程度の追加費用で、年中稼働するソーラー基地局を実現できる見込みです。既にパッケージ検討のために自分たちで部材を調達・加工・設置したDIYソーラー基地局(図-5)をブログで紹介しています。詳しくはそちらをご参照ください[*2]。

このときの最初のソーラー基地局は4名で設置しましたが、パッケージ化に向けては2人以下でより短時間での設置が行えるように改善が必要と考えています。そこで先日、職場から比較的近い場所をお借りして、10名以上で雨の降る中、様々な道具や部材を使って実際に数パターンの設置を試しました。後日、別のブログで詳細を紹介できればと思います。この成果を生かしたパッケージの販売にご期待ください。

2.5.2 電波サーベイツールによる通信状況の簡単測定

通信状況を農業経営体自身で簡単に測定できるようにするため、我々は「電波サーベイツール」と呼ばれる通信状況の測定用デバイスを開発することにしました。まず、開発するにあたっての要件を以下のように定めました。

1. スマートフォン用測定アプリは用意せず、「TLG3901BLV2」と「電波サーベイツール」のみで構成。いずれもモバイルバッテリーまたは乾電池で動作するようにする。
2. 測定は5分間とし、10秒に1回の間隔で30回測定する。
3. 「電波サーベイツール」には液晶画面を設け、測定結果がリアルタイムに表示されるようにする。
4. 「TLG3901BLV2」はSIMなしでも使えるようにする。

1はどこでも簡単に測定できることを重視して定めました。スマートフォン用測定アプリを用意するとその操作を覚える必要がありますが、農業経営体の中にはスマートフォンの操作に慣れていない方もいます。「水管理パックS」にはスマートフォン用アプリが含まれるので、導入が決まった後は操作に慣れる必要がありますが、導入前の事前確認段階でのハードルはなるべく下げたいと考えました。バッテリー・電池駆動とすることで、電源のある場所に縛られなくなるだけでなく、電源ボタンをなくしてバッテリー・電池を接続するだけで自動で測定を開始することもできました。

図-5 DIYソーラー基地局

図-6「電波サーベイツール」の液晶画面表示

2は我々がこれまでに測定で使用していたデバイスと合わせました。LoRaWAN®の仕様上はもっと間隔を短くすることも可能なのですが、周辺に同じ920MHz帯を使用するデバイスが多数あった場合の干渉や、移動車両などによる環境ノイズの影響が強く出ることを懸念してこの仕様としました。

3はスマートフォン用測定アプリの代わりに用意することにしました。「電波サーベイツール」からKiwi Technology製LoRaWAN®ゲートウェイに上り通信でACKリクエストを送り、ACKが返ってくれば通信成功、返ってこなければ失敗と判定して○とXを表示し、最後に通信回数に対する通信成功数を表示するようにしました(図-6)。リアルタイムに測定結果が表示されますので、全く通信できない場合は途中で電源を抜いて測定を中断できるのも良い点でした。

4は貸出用に「TLG3901BLV2」と「電波サーベイツール」のセットを多数用意した場合に、SIMが同数必要になるのを避けたかったのが理由です。図-3で示したように、LoRaWAN®を使った通常のシステムではクラウド上のネットワークサーバとの通信が必須のため、SIMなどによる通信回線が必須となります。幸いKiwi Technology製LoRaWAN®ゲートウェイは独自の機能として、ビルトインネットワークサーバを搭載しています。ビルトインネットワークサーバを活用したLoRaWAN®システムの構成を図-7に示します。

ビルトインネットワークサーバは通常はクラウドなどで提供されるネットワークサーバとほぼ同等の機能をゲートウェイ単体で実現します。デバイスから受信したデータをゲートウェイの内蔵ストレージに一定期間ためることができ、REST APIでいつでも外部から取り出すことができます。また、REST APIでデバイスの制御を要求することも可能です。デバイスからACKリクエストが来た場合は単体でACKを返すこともできます。これを使えばアプリケーションサーバとの通信ができなくてもデバイスとの双方向通信が可能になります。もともとビルトインネットワークサーバはネットワークサーバの契約がなくてもPoCが簡単に行えるようにするための機能ですが、こうした機能が「電波サーベイツール」でも有効活用できました。

こうして開発した「電波サーベイツール」の試作版が図-8です。既に実際に数名の方に貸し出して使ってもらったところ、ユーザ自身での実測による通信状況の事前確認という期待した効果以外に、「こんなに遠くても通信できるのか！」という驚きの声

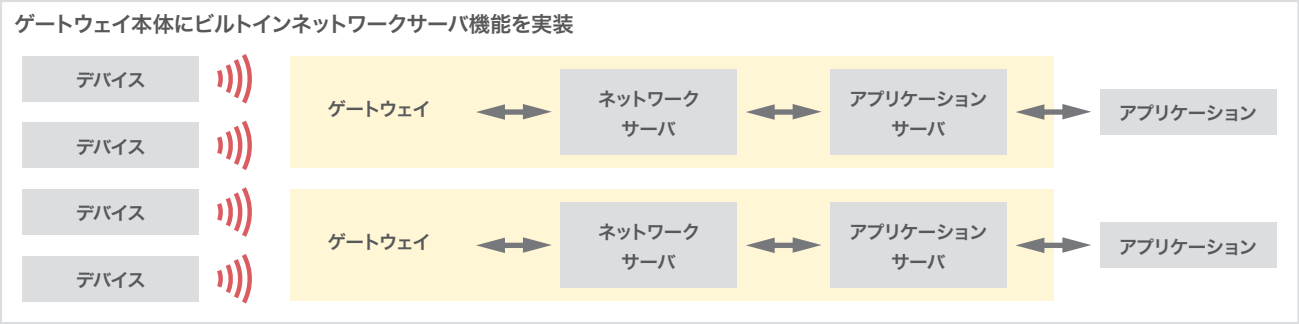

図-7 ビルトインネットワークサーバを活用したLoRaWAN®システム構成

もいただきました。LoRaWAN®の遠くまで通信できるという特長を導入前に実体験してもらう効果的なツールにもなりました。我々だけでは集められない様々な場所での実測データの収集に有効ですので、「電波サーベイツール」の活用を推進すると共に、更なる改良を進めていきたいと考えています。

2.6 まとめ

本稿ではLoRaWAN®の他のLPWA無線ネットワークに比べた特徴と適した用途、農業IoTでのLoRaWAN®のメリットについて述べると共に、農業IoTにおけるLoRaWAN®普及の課題と解決策について述べました。

しかし、上で述べた課題の解決だけでは「水管理パックS」の販売に必要な最低限の準備ができた段階に過ぎないと考えています。販売数が増えた場合は出荷前のキッティングを簡単に行えるようにする、出荷後に問題が発生した場合には簡単に状況を把握できるようにするといった課題にも対処していく必要があります。そのため、IIJではKiwi Technologyと協力してLoRaWAN®ゲートウェイのSACMのゼロコンフィグ機能対応などの機能拡張も進めています。

SACMは機器の自動接続、一元管理を可能にするSMF技術をもとにIIJが開発した、ルーターやIoTゲートウェイ向けにOEM提供する次世代のマネージメントシステムサービスです。ゼロコンフィグ機能に対応すると、電源を入れるだけで自動的にSACMへ接続し、自身の設定を取得して動作します。機器への直接的な操作を一掃し、SACMの管理者向けユーザインタフェースから管理対象となる大量の機器の設定、監視、管理を一括して行えます。SACMの詳細についてはIIR Vol.36のフォーカスリサーチで説明していますので、そちらをご参照ください*3。

また、農業IoT向けに開発した機能や積み上げた販売・運用ノウハウは他の用途向けのLoRaWAN®ソリューション展開にも有効活用できます。IIJは更なる技術開発とノウハウ蓄積によってLoRaWAN®導入のハードルを下げ、様々な分野での展開を推進していきます。

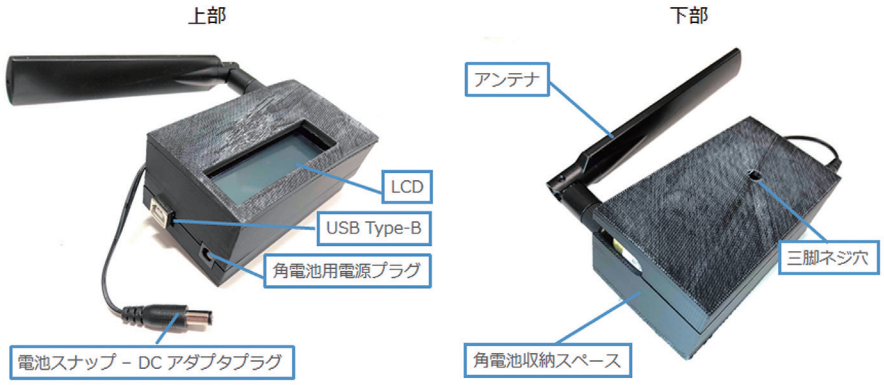

図-8 電波サーベイツール試作版

執筆者:
大西 元大（おおにし もとお）
IIJ IoTビジネス事業部 新規事業推進課 プロダクトマネージャ。
2016年6月より現職。IoTおよびカメラソリューションに関する企画を担当。

*3 Internet Infrastructure Review(IIR)Vol.36（https://www.iij.ad.jp/dev/report/iir/036/04.html）。

新型コロナウイルスの フレッツトラフィックへの影響

3.1 はじめに

新型コロナウイルスCOVID-19の影響で、今年の3月から全国の学校が臨時休校になり、それに伴って在宅でリモートワークをする人が急増しました。多くの人のインターネット利用パターンが変わったために個別のサービスや回線が逼迫している所があり、その観測や不満がSNSで拡散されています。一方で、マクロな状況についてはあまり情報がありません。そうした状況を踏まえ、ここでは、主に家庭で利用されるブロードバンドサービスの代表として、IIJのフレッツ対応サービスのトラフィックへの影響について報告します。

新型コロナウイルスは2月中旬から国内での感染拡大が始まりました。この時点ではリモートワークはまだ実験的でしたが、2月下旬になると電通や資生堂などの企業が大規模なリモートワークを開始します。3月2日に全国の学校が臨時休校を開始し、この週から多くの企業がリモートワークを実施、外出を控える人が増えて街から急に人が減りました。フレッツのトラフィックは明らかに3月2日から傾向が変わりました。その後、3月25日の東京都の外出自粛要請、4月7日の7都府県への緊急事態宣言発令、更に4月16日の緊急事態宣言の全国への拡大などを経て、社会の状況は大きく変わりました。それに伴い、家で過ごす人は増えたはずですが、フレッツのトラフィック量にはそこまでの大きな変化は見られませんでした。

3.2 データについて

トラフィック量のデータは、IIJが提供する個人及び法人向けのブロードバンド接続サービスの光回線とADSLを収容するルータのインタフェースカウンタの値を集計したものです。送信元の事業者調査については、Sampled NetFlowで収集した調査データを利用しています。こちらのデータについては、昨年のブロードバンドトラフィックレポート[*1]で詳しく解説しています。

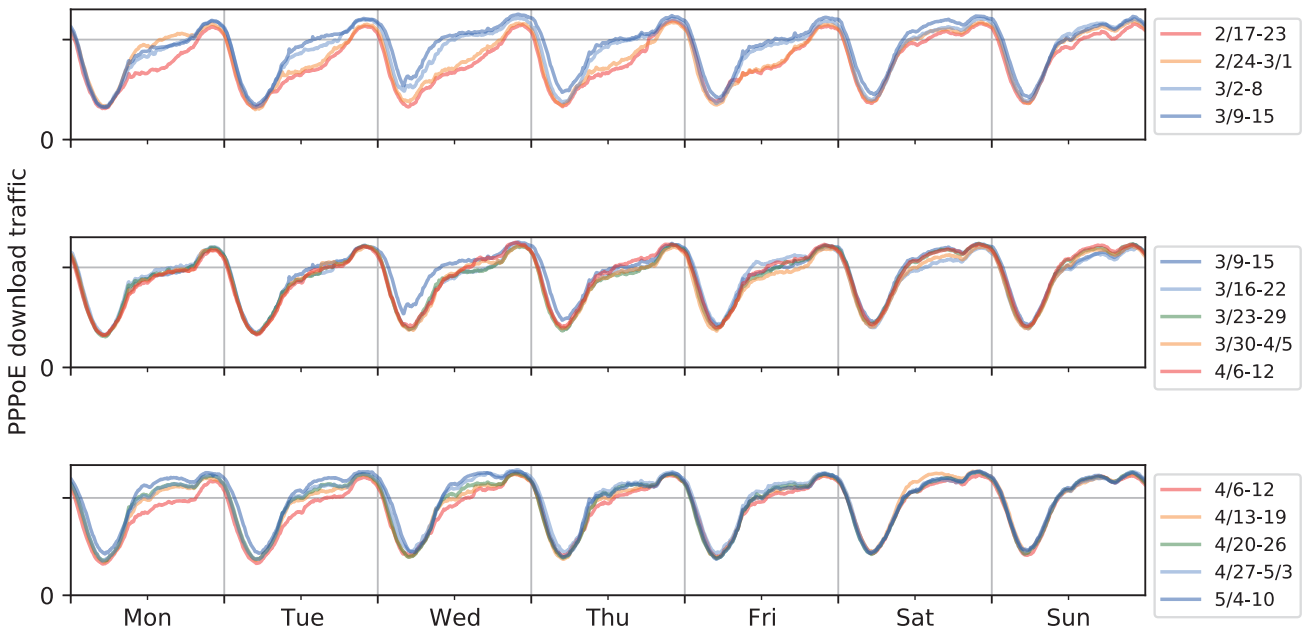

図-1 フレッツトラフィック推移
ダウンロード:2/17-3/15(上) 3/16-4/12(中) 4/13-5/10(下)

*1 長健二朗 .ブロードバンドトラフィックレポート :トラフィック量は緩やかな伸びが継続 . Internet Infrastructure Review. vol.44. pp4-9. September 2019.

3.3 トラフィック状況

IIJのフレッツサービスには、従来からのPPPoEの他にIPv6 IPoEがあります。IIJのIPv6 IPoEサービスはインターネットマルチフィード社のtransixサービスを利用していて、そのトラフィックは直接IIJの網を通りません。量的には現状でPPPoEの20%程です。ここ数年、PPPoEは終端装置での輻輳が問題となっていて、最近ではIPoEの利用を勧めるISPが増えています。

3.3.1 フレッツトラフィック(PPPoE)

図-1と図-2にIIJのフレッツトラフィック総量の推移を1週間ごとに重ねて示します。これはIPv6 IPoEを含まないPPPoEのトラフィックになります。図-1がダウンロード、図-2がアップロードです。

グラフは2月17日の週からの12週間分を4週間ごとに3つのグラフに分けて推移を示します。2番目以降のグラフでは比較のためにその前週も加えた5週間分を示しています。この間の休日は、2月24日(月)、3月20日(金)、4月29日(水)、5月4日(月)、5月5日(火)、5月6日(水)で、トラフィックパターンも他の平日とは異なっています。

通常、ダウンロード量は、夕方からピークを迎え、夜中を過ぎると急速に減って早朝に最も少なくなります。休日には昼間のトラフィックが多くなります。アップロードはダウンロードより1桁近く少なく、また、はっきりしたピークもありません。

まず、図-1のダウンロードに着目します。上図、3月2日前後の赤色と橙色の2週間と水色と青色の2週間を比較すると、3月2日以降はダウンロード側で平日昼間のトラフィックが増えていることが分かります。量的にはまだ通常の休日より少ない程度です。ピーク値も僅かながら増えています。中図ではあまり変化が見られませんが、下図の4月に入って平日昼間が再度増

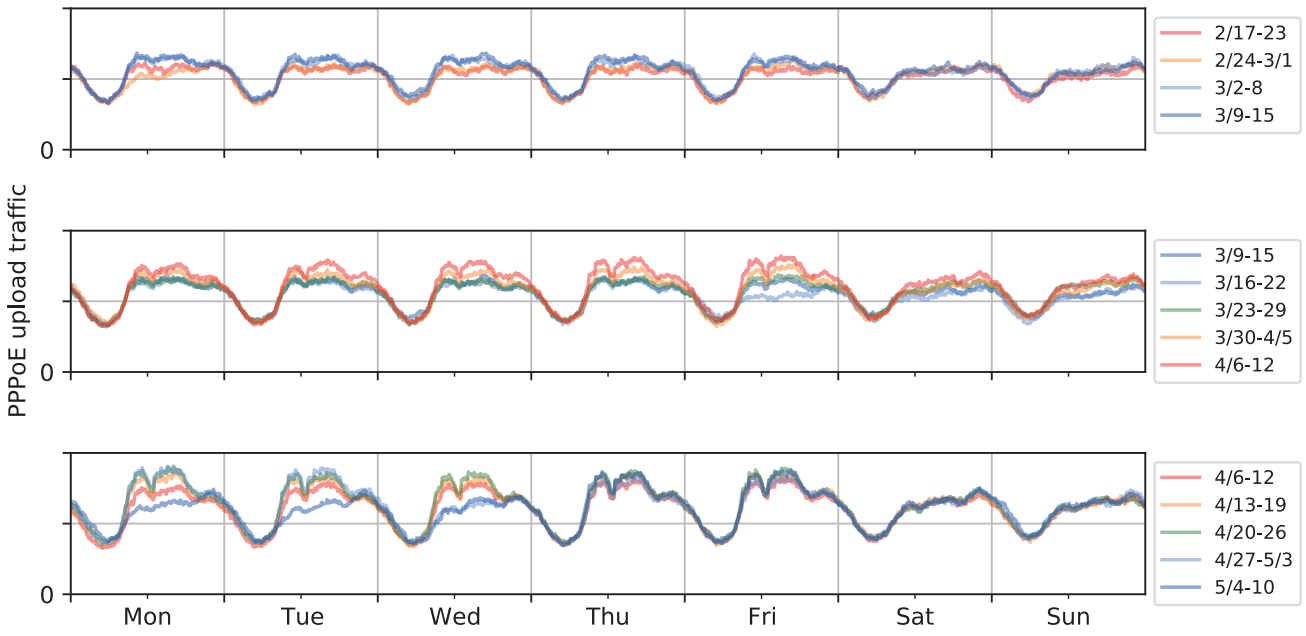

図-2 フレッツトラフィック推移
アップロード:2/17-3/15(上) 3/16-4/12(中) 4/13-5/10(下)

えてきています。ただし、ピークはほとんど変わっていません。後述するように、下図の月曜昼間の増加は天気の影響もあると思われます。なお、3月11日（水）早朝から午前のトラフィック増は人気ゲーム“Call of Duty:Warzone”の配信の影響だと思われます。この日にはマイクロソフトの月例アップデートもあったのでその影響も含まれているはずです。

次に図-2のアップロードを見ると、3月中旬までの上図では平日昼間に僅かに増えていますが、この増加分は夕方には収まっており、ビデオ会議などのリモートワーク関連と推測されます。4月以降の中図と下図では、平日昼間が段々増えて来ており、徐々にリモートワークの体制が整ってきたためと考えられます。昼休みの時間に落ち込むのはビデオ会議が行われないからと推測できます。また、アップロードは3月中旬までは平日昼間だけが増加していましたが、それ以降は夕方や休日にも増えています。これは、利用者がビデオ会議ツールを使い慣れるにつれ、飲み会などのプライベートな集まりにも利用するようになってきたためではないかと推測できます。しかし、アップロード量のピーク値はダウンロード量のピーク値の1/7程度で、ダウンロードに比べてそれほど量的に大きく増加しているわけではありません。

平日昼間のトラフィック増加が特定のサービスに起因しているかを調べるために、トラフィック量以外にSampled NetFlowのデータを調べました。2月26日（水）と3月4日（水）の東京都分のデータを比較すると、ダウンロード量は全体で1.19倍に増えており、送信元事業者（AS）別に比較すると、CDN事業者からの割合が多少増えている程度で、主なコン

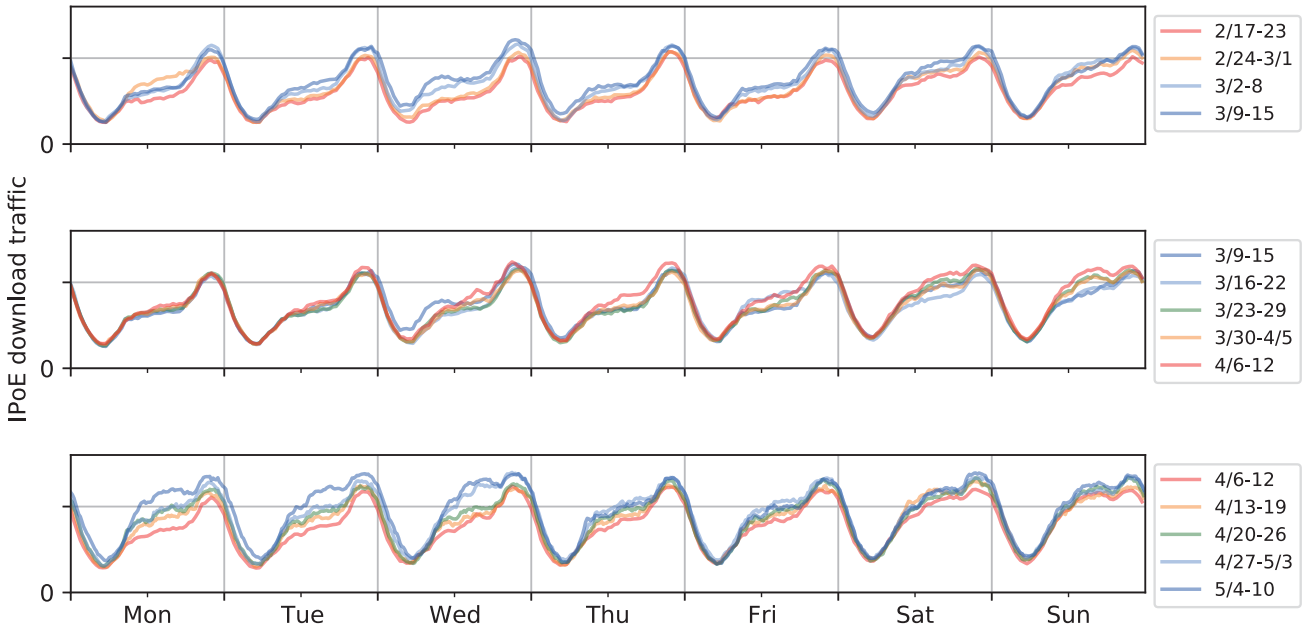

図-3 IPv6 IPoEトラフィック推移
ダウンロード：2/17-3/15（上） 3/16-4/12（中） 4/13-5/10（下）

テンツ事業者の構成比は殆ど同じでした。具体的には、Googleが1.16倍、Amazonが1.16倍、Appleが1.14倍、Netflixが1.17倍、Facebookが1.10倍、Microsoftが1.23倍となっています。つまり、人気コンテンツはほぼ同様に伸びていて、特定のサービスが突出して増えたのではなく、全体が増えています。

その後の変化を見るために、2月26日(水)と4月22日(水)を比較すると、ダウンロード量は全体で1.20倍と3月4日からわずかに増えている程度ですが、主なコンテンツ事業者の構成比には少し変化が見られます。具体的には、Googleは1.16倍と変化なしですが、Amazonが1.63倍、Appleが1.00倍、Netflixが1.36倍、Facebookが1.32倍、Microsoftが2.40倍となっています。映画などの長編動画コンテンツと、ビジネス用途のコンテンツが伸びていることがうかがえます。

3.3.2 IPv6 IPoEトラフィック

PPPoEのピークトラフィックが増えていないのはフレッツ網が輻輳しているからとも考えられるので、容量に余裕があるはずのIPv6 IPoEの様子も見ておきます。図-3と図-4にIPv6 IPoEのトラフィック量の推移を示します。ダウンロードを見ると確かにピークも伸びていて、上図では数パーセント、中図ではほとんど増えずに、下図でまた数パーセント増えています。そして、ピークに対する平日昼間の量はPPPoEに比べて少ない状況です。また、アップロードに関しても平日昼間の増加はPPPoEより少なくなっています。

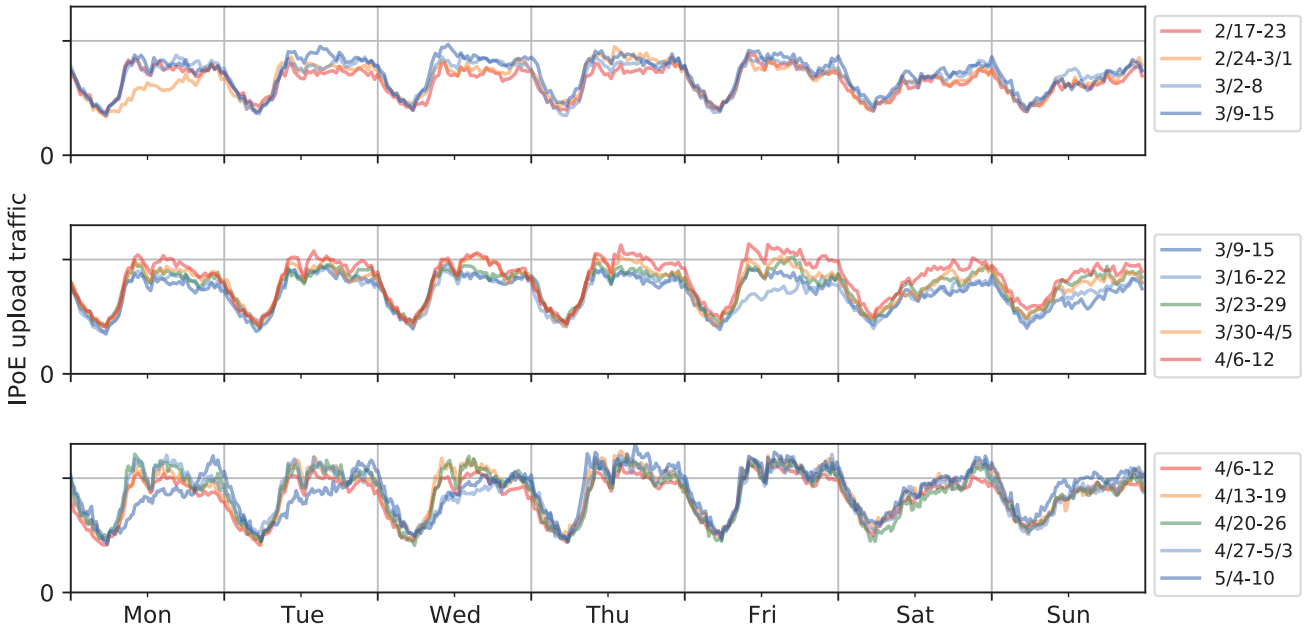

図-4 IPv6 IPoEトラフィック推移
アップロード:2/17-3/15(上) 3/16-4/12(中) 4/13-5/10(下)

3.4 考察

今回観測できているのはIIJのサービスだけで、ここから他社の動向は分かりません。一方で、4月中旬には、NTT東日本[*2]、NTT西日本[*3]、NTTコミュニケーションズ[*4]からもフレッツのトラフィック量について発表がありました。NTT各社の公表したグラフと同様に、IIJのPPPoEのデータをもとに平日のトラフィック量の変化を示すと図-5のようになります。ここでは、2月25日の週と4月20日の週の平日の平均トラフィック量をダウンロード(DL)とアップロード(UL)で示しています。この図はNTT各社の観測とほぼ一致していますので、フレッツを使ったブロードバンドサービスでは大体同じような傾向だと思われます。また、非フレッツで帯域に余裕があるところではIPoEの傾向に近いのではないかと推測しています。

マクロにみると、3月2日を境に明らかに平日昼間のトラフィックが増えています。平日の1日のトラフィック量でみるとアップロードで6%、ダウンロードで15%程増えています。1日のダウンロードで15%増というのは、平日と休日の違いぐらいとも言えますが、通常半年から1年ぐらいかかる増加が1日で起こったと捉えることもできます。ただし、ピーク値はあまり増えていないので、ISP視点では前者の感覚です。PPPoEのピーク値が伸びていないのは、フレッツ網のPPPoE終端装置における容量不足が考えられます。また、フレッツ網の光分岐あるいは集合住宅の宅内機器や配線で輻輳している可能性もあります。しかし、これらの問題は装置単位で発生するので、余裕のあるところではピークが増えているはずですが、観測した範囲ではそのような違いは確認できていません。

IPoEではピークトラフィックも増えていますが、IPoEはサービス事業者のIPv6サポート状況に依存したトラフィックとなるので、コンテンツ比がPPPoEとは異なり、直接比較することはできません。また、PPPoEの契約数が頭打ちなのに対して、PPPoEでの輻輳を避けるためにIPoEへ移行が進んでいることもあり、IPoEは契約数も伸びています。総合して考えると、IPoEのダウンロードではピークが伸びていることから、PPPoEでは容量不足が起きていることがうかがえるものの、PPPoEのピークの潜在的な増加分はIPoEの増加分より小さいのではないかと考えられます。

3月と4月でも少し変化が見られます。3月は、平日昼間に在宅している人が増えてインターネット利用全体が増えたと言えそうです。それに対して4月になると、利用者の環境整備が進み、また、ツールにも慣れてきたため、映画視聴やリモートワーク系と思われるトラフィックが増えてきたようです。リモートワーク特有の影響として、平日昼間のアップロードの増加分は主にビデオ会議によるものと推測できます。しかし、3月後半までは量的にも大きくなく、これは自宅でビデオ会議をしている人はまだ限られていたからだと推測します。リモートワークを効率良く行うには、自宅のネットワーク環境やPCなどの機材の整備に加えて、経験の蓄積も必要です。企業側でもVPNのライ

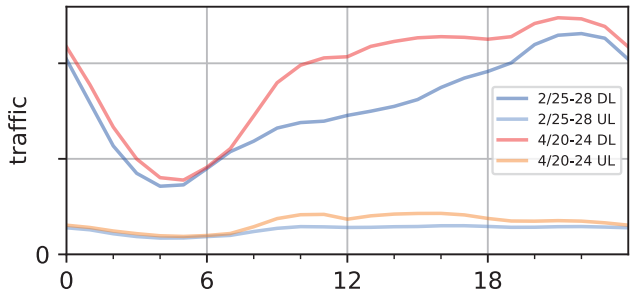

図-5 平日の時間別平均トラフィック量：2月と4月の比較

*2 NTT東日本、「新型コロナウイルス(COVID-19)に対するNTT東日本の取り組み」ネットワークの運営について(https://www.ntt-east.co.jp/aboutus/COVID-19.html#traffic)。
*3 NTT西日本、「NTT西日本 全エリアダウンロードトラフィック」(https://www.ntt.co.jp/topics/important/pdf/important_west.pdf)。
*4 NTTコミュニケーションズ、「インターネットトラフィック(通信量)推移データ」(https://www.ntt.com/about-us/covid-19/traffic/)。

センスや帯域が足りないなどの問題が起きていたようです。当初はビデオ会議をやろうとしても環境が整わなかった人も多かったと思われます。それが4月以降、徐々に改善されてきたのだと推測できます。事業者別の伸びを見ても、3月には主なコンテンツ事業者からのトラフィックが一様に増えていますが、4月には映画コンテンツを提供する事業者やリモートワーク関連サービスの事業者が伸びています。

また、季節柄か天気が良いとトラフィックが減り、天気が悪いと増える傾向も見えます。3月20日(金)から22日(日)の三連休は全国的に天気に恵まれ、人々の気持ちが緩んで外出が増えたとされていますが、それを裏付けるようにトラフィックも少なくなっています。4月18日(土)は東日本や東北で大荒れの天気となり、この日はトラフィックが増加しています。4月13日と4月20日は関東で2週続けて雨の月曜だったためかトラフィックも多めとなっています。

実は、ブロードバンドトラフィックは新型コロナウイルス感染拡大以前から増加速度が加速傾向でした。その背景には、Windows7のサポート終了や消費増税前の駆け込み需要で古いPCのリプレースが進み家庭の動画再生環境が良くなっていたこと、企業の働き方改革とオリンピック対策でリモートワークの導入が進んでいたこと、更に、オリンピックや放送のネット送信や5Gモバイルサービスなどへの期待から動画視聴への関心が高まってきていることが挙げられます。

ただし、トラフィック量の観測では、動画が量的に他のコンテンツより圧倒的に大きいため、ダウンロードではビデオ視聴の、またアップロードではビデオ会議の割合が支配的になってしまい、動画以外の利用傾向はなかなか見えてきません。トラフィック量だけでインターネットの利用動向を説明するには限界があります。

3.5 まとめ

新型コロナウイルスの感染拡大によって、急速なリモートワークへのシフトが起こりました。それによって、個別の回線やサービスで問題が顕在化している一方で、マクロレベルでは平日昼間のトラフィックが増えたものの現状ではなんとか既存の容量に収まっている状況です。

この3月からはリモートワークやリモート教育が大規模に行われるようになりました。これまではリモートワークは一部の人が実施する実験だったのが、今や誰もが一斉にできるかが試されています。インターネットを使ったビデオ会議、リモート授業、動画視聴などについても、現状一部の人が利用している分には十分な品質が出ますが、多くの人が一斉に使えるだけの環境を整えるにはこの先何年もかかります。今回、いざというときには社会全体がオンライン頼みになることも明らかになりました。これがインターネットインフラ整備の重要性を再認識する大きなきっかけになることを期待しています。

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

June 2020 Vol.47

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2020年6月時点のものです。

IIJ-MKTG019-0047

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