IIR

Internet
Infrastructure
Review

Jun.2021
Vol.51

定期観測レポート

2020年度、200倍に急増した迷惑メールとパスワード付きZIP対策

フォーカス・リサーチ(1)

IIJ、フルMVNOの更なる挑戦 ～ローカル5G環境での独自路線を追求したNSA/SA商用サービス化への道のり

フォーカス・リサーチ(2)

スピードが求められる障害対応に、IIJ独自開発「Barry(バリー)」

IIJ
Internet Initiative Japan

Internet Infrastructure Review

June 2021 Vol.51

エグゼクティブサマリ

この「エグゼクティブサマリ」は、開催が1年延期された東京オリンピックの開幕まで2ヵ月を切った東京で書いています。東京オリンピックでは33競技339種目が実施され、参加する選手は1万人を超えるそうです。1000万人を超えるとされる観客と大会スタッフは、現状では大幅に縮小されるかもしれませんが、世界が注目する有数のイベントであり、アスリートにとって重要な競技大会であることに変わりはありません。

情報通信技術は、このような巨大なイベントを裏で支える重要な要素です。競技の記録の計測、報道機関などへの結果の伝達、選手・スタッフ・観客などの認証や入退場の管理、アスリートの活躍をリアルに分かりやすく伝える映像やデータのインターネットへの配信など、様々なシステムのサポートを通じて大会が円滑に運営されます。アスリートが最高のパフォーマンスを発揮し、その活躍が世界各地に配信され、人々の感動を呼び起こしている裏で情報通信技術が大きく貢献しています。

新型コロナウイルス感染症の影響もあり、当初想定していた形態での開催は難しいものの、開催に向けて関係者による懸命の準備が続いているものと思います。先に挙げた情報通信システムについても同様でしょう。世界中で人の移動が制限されるなか、人と人とのつながりや余暇の楽しみを支えているのも情報通信技術です。この困難な状況のもとオリンピックが安全に開催され、アスリートの活躍や感動が1人でも多くの人にインターネットを通じて届けられることを祈念します。

「IIR」は、IIJで研究・開発している幅広い技術を紹介しており、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」から構成されます。

1章の「定期観測レポート」では、電子メールを中心とするメッセージングに関する1年間の動向をまとめています。特筆すべきは、昨年度(2020年4月～2021年3月)の上半期、IIJで管理しているハニーポットに着信した迷惑メールの分析で、これまでにないほど大量の迷惑メールを受信した点です。また、トピックとして、昨年度に話題になった日本特有の暗号化ZIPファイルのメール添付やオンライン会議システムを利用したフィッシングについて紹介します。

2章の「フォーカス・リサーチ(1)」では、IIJにおける5G NSA(Non-Stand Alone)、SA(Stand Alone)への取り組みについて解説します。4GにおいてIIJは、コアネットワークの一部の機能を保有するフルMVNOとしてサービスを提供しています。5G NSAは、4Gのコアネットワークを拡張して5Gの高速通信を実現します。5G SAは、5G向けの新しいコアネットワークを用いて5Gサービスを提供する形態です。いずれの方式も、社内での技術検証、白井ワイヤレスキャンパスでの実証実験を行っており、その成果の一部はケーブルテレビ業界の地域BWA及びローカル5Gの提供に活用されています。

3章の「フォーカス・リサーチ(2)」は、IIJで障害対応時に利用している内製システム「Barry(バリー)」の紹介です。システムが大型化・複雑化するなか、信頼性への要求は高まる一方で、システムにインシデントが発生したとき、それを検知し、必要な要員に情報を的確に通知して、速やかに対応を開始することは、お客様にICTサービスを提供するプロバイダにとって非常に重要です。そのため、その業務を支えるシステムは、市販のツールに頼るのではなく、我々自身の業務フローの改善や新しい技術の創出のためにも、内製化に踏み切りました。Barryは実際に運用に携わるエンジニアの意見を活かして開発されたもので、その裏側・背景を解説します。

IIJ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行っています。今後も企業活動のインフラとして最大限に活用いただけるよう、様々なサービスやソリューションを提供し続けてまいります。

島上 純一(しまがみ じゅんいち)
IIJ 常務取締役 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、2021年6月より同協会の副会長に就任。

2020年度、200倍に急増した迷惑メールとパスワード付きZIP対策

1.1 はじめに

新型コロナウイルス感染症対策を発端に、自宅やサテライトオフィスで業務を遂行する「テレワーク」が急速に広まって1年が経ちました。この1年間で世の中は様変わりしましたが、企業における電子メールの重要性は変わっていないことでしょう。

本稿では2020年度におけるメッセージングイベントを振り返ってみたいと思います。

1.2 2020年度の迷惑メール・ウイルス集計

図-1は、2020年4月～2021年3月における、IIJ管理のハニーポットに着信した迷惑メールの数を集計したものです。

2020年度上半期は、これまでに類を見ない量の迷惑メールを断続的に観測しました。縦軸を最大値に合わせているため確認しづらくなっていますが、4月の平均を1としたとき、5月上旬の第1波で約10倍[1]、5月中旬の第2波で約40倍[2]、5月下旬から6月の上旬で約60倍[3]規模の迷惑メールを集中的に受信しました。この状況が断続的に続き、7月末には約200倍[4]もの迷惑メールを受信しています。一般的な組織の設備設計で平常時の200倍の規模に耐えられる設備投資をすることは稀だと思いますので、DDoS攻撃と言っても過言ではないでしょう。

ウイルスの集計も見てみます。図-2は同期間における、IIJ管理のハニーポットに着信したウイルスの数を集計したものです。

こちらも同様に4月の平均を1としたときのグラフで、6月に1000倍を越えるウイルスを受信していたことが分かります。しかし、年間の変化量が大きすぎて他が確認しづらいため、同じデータの対数グラフを図-3に作成しました。

常時、何らかの活動が認められますが、迷惑メールとは異なり、年間に数回、短い時間に集中して着信している様子がうかがえます。

6月頃に着信した検体を調査すると、"Look at this photo!"のような件名で、IMG135123.jpg.js.zipのように画像ファイルを思わせるようなZIPファイルが添付されており、展開するとマルウエアをダウンロードするJavaScriptが入っていました。このファイル自体に悪性はないものの、ユーザがJavaScriptを実行してしまうと、マルウェアをダウンロードしてしまいます。画像ファイルとユーザに思わせて開かせる、知っている人から見れば古典的な手法ですが、過去の攻撃と思わず、認識しておく必要があります。

また、9月に2番目に大きいピーク値が見えます。このときに観測したウイルスはEmotet（エモテット）と呼ばれるものでした。2020年に猛威をふるったEmotetは、自分自身をパスワード付きZIPファイルで暗号化するという特徴がありましたが、9月のものは、従来にない特徴がありました。図-4の出力は、受信したEmotet（ZIPファイル形式で暗号化されたもの）の構造を詳細に表示したサンプルの一部です。

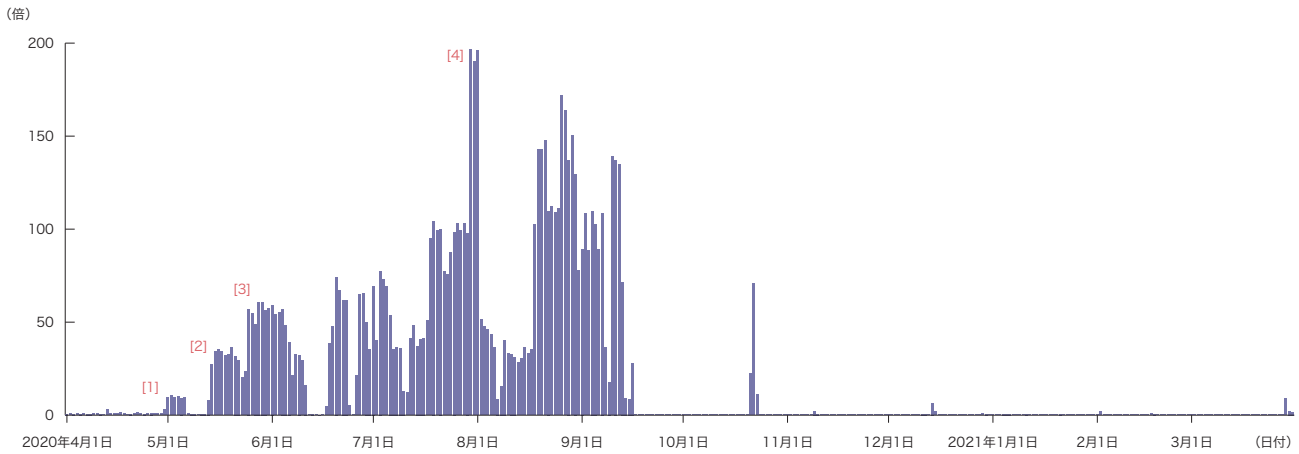

図-1 IIJハニーポットに着信した迷惑メール（2020年4月～2021年3月）

暗号化方式がZIPファイル標準のZipCryptoから、AES 256-bitに変化していました。

AESとはZIP標準のものよりも暗号を強化した方式で、7-ZIPをはじめとした一部のアーカイバが対応していますが、Windows標準の圧縮フォルダは対応していません。ウイルスを拡散する目的から見れば、多くのターゲットに開かせたいのですから、わざわざ暗号強度を上げる必要はないように思えます。では、なぜ、こんなことをしたのでしょう。

```
$ zipdetails 'OXEFVNG1 20209月16.zip'

0000 LOCAL HEADER #1       04034B50
0004 Extract Zip Spec      33 '5.1'
0005 Extract OS            00 'MS-DOS'
0006 General Purpose Flag  0803
     [Bit  0]              1 'Encryption'
     [Bit 11]              1 'Language Encoding'
0008 Compression Method    0063 'AES Encryption'
003D   Encryption Strength 03 '256-bit encryption key'
```

図-4 受信したEmotet(ZIPファイル形式で暗号化されたもの)の構造を詳細に表示したサンプルの一部

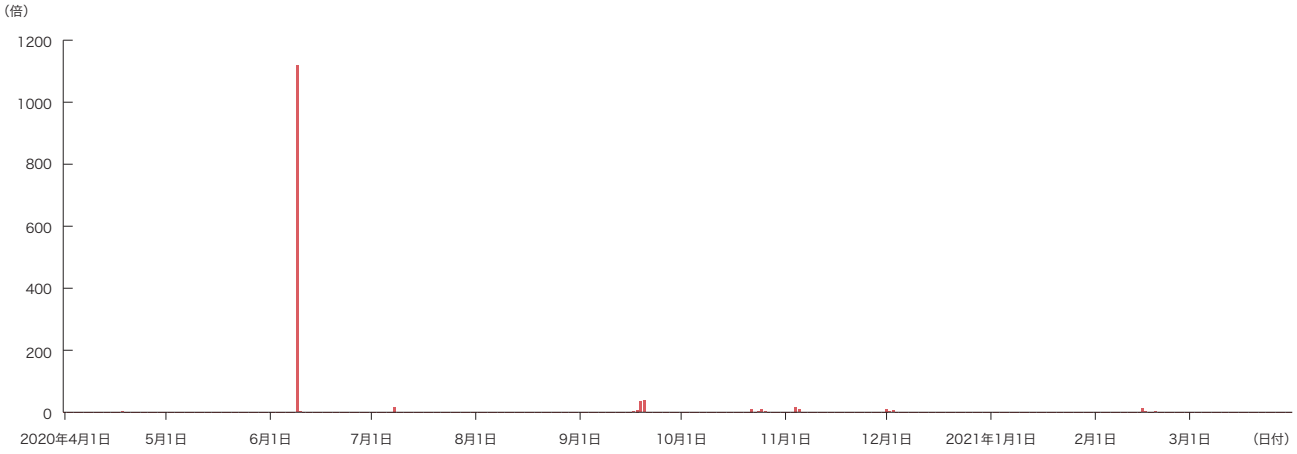

図-2 IIJハニーポットに着信したウイルス(2020年4月～2021年3月)

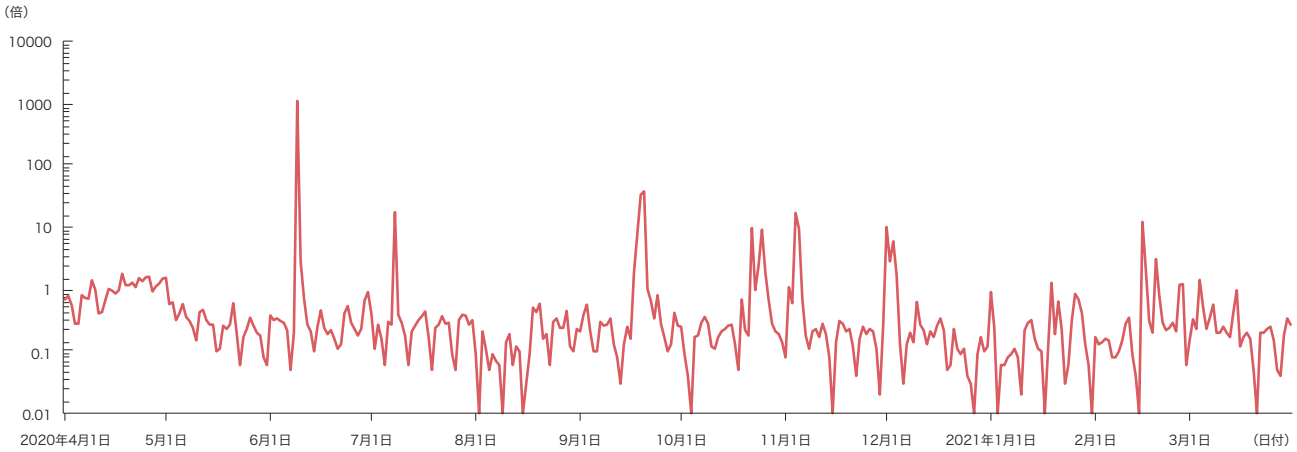

図-3 IIJハニーポットに着信したウイルス(対数グラフ)(2020年4月～2021年3月)

これは推測ですが、サンドボックスによる検出回避と考えられます。一部のセキュリティ製品・サービスには、メール本文からパスワードと考えられる文字列を読み取り、サンドボックス上で展開を試みる機能を有しているものがあります。しかし、Windows標準ではAESで暗号化されたZIPファイルに対応していません。仮に運良くメールからパスワードを正しく抽出することに成功したとしても展開することができませんので、有害な挙動が確認できずサンドボックスを回避できてしまいます。

このように、同じように見える攻撃でも、少しずつ手法を変えていることが分かります。

1.3 暗号化ZIPファイルの廃止論

2020年11月、平井デジタル改革担当大臣が定例会見で「暗号化ZIPファイル（通称、PPAP）の廃止」について言及しました[*1]。

ここで言う「暗号化ZIPファイル」とは、メールでファイルを送信するときに、差出人は添付したいファイルをパスワード付きZIPファイルとして暗号化しておき、その展開パスワードを別送するといった手法のことです[*2]。国内ではよく見かける一方で、国外ではほとんど見られない、日本特有な文化です。

このような手法を採用する目的は誤送信対策や経路暗号化であるとされ、個人で実施できる、（専用のアプリケーションを必要としないという観点で目先の）コストが低い、といった理由で、主に組織の情報セキュリティポリシーとして策定されていることが多いようです。

1.3.1 暗号化ZIPファイルの問題点

なぜ暗号化ZIPファイルを廃止するべきなのでしょうか。それは、この手法が見込める効果よりも、多くのリスクを抱えていることにあります。

最も深刻なのは、メール受信時にウイルススキャンを実施できない点です。1.2項で説明したとおり、誰もが送受信できるメールは、攻撃者にとって依然として有用な攻撃ベクターです[*3]。そのため多くの組織では、メールに添付されたウイルスから感染しないよう、ゲートウエイやWebメールなどでウイルス対策を施すことが一般的です。

しかしながら、添付ファイルを暗号化してしまうと、この機能を容易に回避することができてしまいます。なぜなら、ウイルス対策製品は暗号化されたファイルの中身を解析することができないからです[*4]。他人に読まれないように中身を暗号化しているわけですから当然の結果と言えます。

この弱点を突くかのように、IIJが提供しているメールサービスでは、2012年頃から特定の組織や人物、窓口を狙った「標的型攻撃[*5]」を観測しています。こうしたメールは何度か無害なやり取りを繰り返して受信者を信用させた後に、最終的に「質問を添付ファイルにまとめました」といった手口でマルウエアを仕込んだファイルをZIPで暗号化し、ウイルススキャンを回避して受信者にメールを届けていました。

また、2020年のEmotetはWordやExcelのマクロ付きファイルとして自分自身をZIPで暗号化してメールに添付し、感染し

＊1　内閣府、「平井内閣府特命担当大臣記者会見要旨 令和2年11月17日」（https://www.cao.go.jp/minister/2009_t_hirai/kaiken/20201117kaiken.html）。
＊2　本稿発行時点でIIJスタッフがやり取りするメールでも、この手法をとっているものがあります。業務やお客様のご都合もあり、全面的にすぐ廃止はできませんが、準備ができたところから順次、暗号化ZIPファイルを廃止していく方針です。
＊3　国民のための情報セキュリティサイト（総務省）、「ウイルスの感染経路」（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/02-1.html）。
＊4　中身を解析することはできませんが、暗号化されたまま該当のファイルをウイルスとして判定することはあります。しかし、判定に必要な情報がファイルのハッシュやファイル名といった、かなり限られた条件しかありませんので、非暗号化状態と比較すると判定難易度は高めです。
＊5　攻撃者が機密情報を盗み出したり、侵入経路を確保するために、組織の窓口や特定個人を狙った攻撃のことを指します。ウイルスを送りつけて感染させたり、フィッシングサイトに誘導する従来の方法と技術的には変わりませんが、他組織やアンチウイルスベンダーのハニーポットに着信しないため、事象の検出が困難であることが特徴です。

た端末のアドレス帳やメールを読み取って、その端末の返信を装って感染を広げるウイルスでした。

そしてEmotetがとても洗練されているのは、その亜種が大量にあり、日本人をターゲットにした「請求書」「発注書」といった日本語の件名や月末・月初のタイミングで感染を広げたことです。暗号化ZIPのやり取りは日本国内では良く見かける手法でしたから、かなりの注意を払っていないと何の疑問も持たずに開いてしまうことでしょう。この繰り返しが、爆発的に感染を広げていった理由と考えられます。

このように、差出人がセキュリティ対策として実施したはずの手法が、受信者のメールシステムでは無条件に無害なファイルとして扱われてしまい、かえって受信者を危険に晒してしまっているのです。

なお、米国CISA（Cybersecurity & Infrastructure Security Agency）は、Emotet に対する緊急声明を発表しました[*6]。文章には、ウイルススキャンできない暗号化ZIPファイルは受信拒否することがリスクの緩和策であるとしています。

1.3.2 暗号化ZIPファイルの代替策は何か

私たちは暗号化ZIPファイルを廃止し、どのような手法でファイルを送受信するべきでしょうか。

政府では共有ストレージを活用する動きが見られます[*7]。添付ファイルを送信する代わりに、共有ストレージへ格納したファイルのパスや、ワンタイムURLを送信すれば良いというものです。

この手法はファイルのウイルススキャンをメールではなく共有ストレージ側で実施すれば良い点[*8]や、誤送信に気づいた時点でファイルを削除できる点、メールでは扱えないような大容量のファイルを送受信したいケースにも活用できる点で優位性があります。

一方で、内部統制の観点では、これが弱点になり得ますので両手を上げて飛びつくのは禁物です。例えば、多くの組織では、送受信されたメールをアーカイブして証跡保存することが一般的です。万が一、メールのやり取りが後日、訴訟対応などで争点となったときに、重要な証拠として提出できるからです。しかし、添付ファイルがURLになってしまうと、どのようなファイルが送受信されたか追跡しにくくなる恐れがあります。

また、内部犯行によって重要な書類を共有ストレージにアップロードされて、ワンタイムURL1つで持ち出され、その後、共有ストレージからファイルを削除されるなどで、情報漏えい対策の抜け穴となってしまうリスクもあります。管理者がすべてのメールに目を通して確認することは現実的に不可能ですから、組織のメール監査システムでは添付ファイルがあることを条件にメールを保留し、チェックすることがあります。しかし、本文にURLのみが記載されたメールは普通のメールと変わりませんので、このような犯行を見つけ出すのは極めて困難です。

結局のところ、どのようなシステムを利用しても、それぞれ一長一短ですので、どのリスクをどこまで受容するかがポイントになるだろうと思われます。

＊6　CISA、「Alert (AA20-280A)Emotet Malware」（https://us-cert.cisa.gov/ncas/alerts/aa20-280a）。
＊7　方針を発表した当初、どのようなシステムを採用したか公表されていませんでした。しかし折り悪くも、その後の共有ストレージへの不正アクセス事案で、内閣府内に設置したファイル受け渡し専用アプライアンスを利用していることが明らかになりました。内閣府、「内閣府職員等が利用する「ファイル共有ストレージ」に対する不正アクセスについて」（https://www.cao.go.jp/others/csi/security/20210422notice.html）。
＊8　近年のアンチウイルス技術は、検出率を高めるためにパターンをリアルタイムでアップデートしているのが一般的です。メール受信時にウイルスを検出できなくても、受信者がファイルをダウンロードまたは閲覧するときにスキャンすれば、時間差で検出できることがありますので、これも大きなアドバンテージです。

筆者としては、今まで無駄なことをしていたのだから、単純にそれをやめれば良い、つまり、本当にその情報を添付ファイルとして送る必要があるのか再考し、それでも必要であるのならば、そのまま添付ファイルとして送信し、リスクに応じて一時保留システムや監査システムと組み合わせるのが現実的な落としどころになると考えています。いずれにしても、今回の暗号化ZIPファイルの廃止論は、今後のメールシステムやポリシーを検討する際の重要なターニングポイントとなったのは間違いないでしょう。

1.4 オンライン会議システムの注意点

冒頭にも示したとおり、2020年は「テレワーク」が急速に普及した年になりました。1年前は一部のユーザでしか利用されていなかったオンライン会議システムもあっという間に浸透し、誰もがそのツールを使いこなせるレベルに至っていますが、こうしたオンライン会議システムには共通した仕組みがあります。それは主催者が発行したワンタイムURLをクリックして入室するシステムであることです。オンライン会議に参加するメンバーは、主催者からメールなどで知らされたワンタイムURLをクリックするのみで良いので、とても便利です。

しかし、もし何者かがオンライン会議の主催者になりすまし、代わりにフィッシングサイトのURLを記載していたらどうなるでしょう? ユーザはワンタイムURLをクリックすることに慣れてしまっていますので、受信メールのURLを漫然とクリックしてしまう姿は想像に難くありません。本物と区別がつかないような偽物のログイン画面で、IDやパスワードといった認証情報を盗まれて社内情報を持ち出されたり、パスワードの使い回しをしていると他サービスへの侵入を許してしまいます。

幸い、Eメールには差出人ドメインを認証できる、DMARC(ディーマーク)という強力なフレームワークがあります。企業や組織のドメイン管理者は、送信ドメイン認証を確実に実施し、なりすまし対策を万全にしておきましょう。

また、仕組みの対策と共に、「メールに記載されたURLから始まる攻撃がある」ことを定期的にユーザに周知・教育することで、よりセキュリティ対策の効果を高めることが期待できます。

1.5 送信ドメイン認証の普及状況

2020年4月～2021年3月で、IIJが提供するメールサービスで集計した送信ドメイン認証の結果の割合を図-5～図-7に示します。

自社ドメインになりすましたメールへの対策や、有名ブランドを騙ったフィッシング対策に送信ドメイン認証技術が効果的であるのは間違いありませんが、ここに示すデータは受信メールの総数を母数としたときに対する送信ドメイン認証の結果の割合を示したものであり、例えば、メール配信事業者が送信するようなボリュームの大きいメールを受信すると、その数がデータに対して支配的になる傾向があることに留意してください。また、迷惑メールを送信する者も迷惑メール送信用の

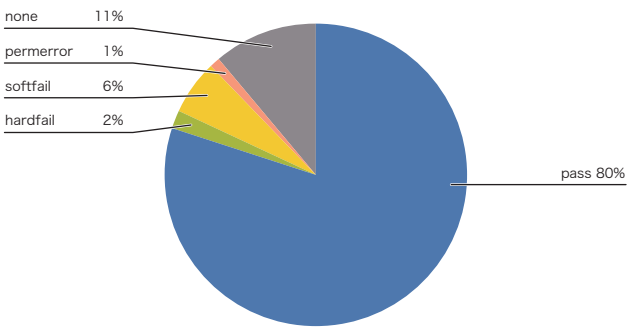

図-5 SPFによる認証結果割合

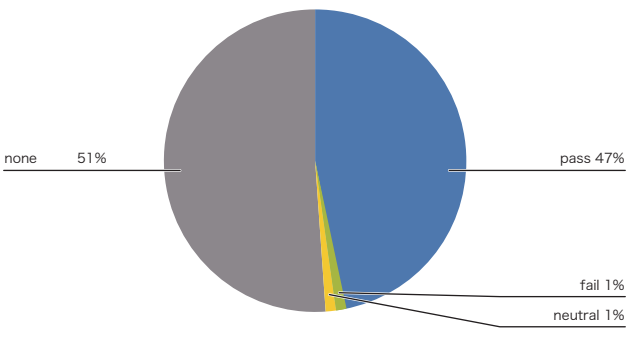

図-6 DKIMによる認証結果割合

ドメインを取得して送信ドメイン認証に対応してきますので、一概にpassだから非迷惑メールとは限らない点に注意する必要があります。

本レポートのVol.47（https://www.iij.ad.jp/dev/report/iir/047.html）で報告した前回の集計結果と比較すると、SPF、DKIM、DMARCいずれにおいても認証成功を示すpassの割合が数ポイント上昇し、SPF、DMARCは認証情報なしのnoneの割合が減少していることが読み取れます。ヘッダFromドメインを認証するという意味では、その役割はDMARCに取って代わりましたので、DKIMはSalesforceやメール配信事業者のように、自社管理下にないSaaSから自社ドメインで送信するメールを認証するのみの用途となったと言っても過言ではないでしょう。

1.6 おわりに

現在の電子メールプロトコルSMTPが規定されたRFC822の発行は1982年。SMTPはSimple Mail Transfer Protocolですが、「シンプルなメール」としつつ、約40年の歳月を経た今でも、なお同じプロトコルで動作しているアプリケーションというのには驚きを隠せません。

オンライン会議システムや、文字ベースのチャットなど、様々なコミュニケーションツールが生まれています。しかし、そのすべてを電子メールに代替するには至っていないのが現状で、今後もしばらくはそのような状況が続くことでしょう。

IIJでは、安全な電子メールの世界を実現するために、今後も取り組んでまいります。

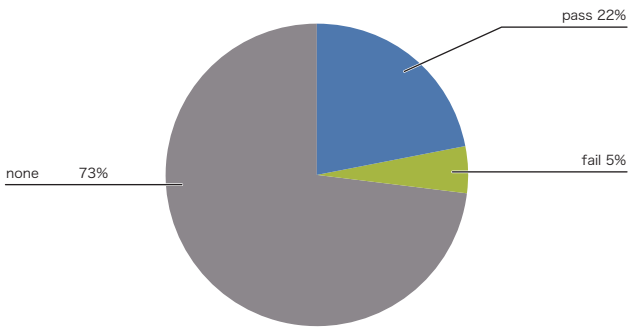

図-7 DMARCによる認証結果割合

執筆者：
古賀 勇（こが いさむ）
IIJ ネットワーク本部 アプリケーションサービス部 運用技術課 課長。
2007年IIJ入社。メールサービスの運用業務に従事し、現場でメールに関する動向を調査。
お客様のメールボックスを守るため、最新の攻撃手法や、迷惑メールのトレンド、対策情報などを発信中。

IIJ、フルMVNOの更なる挑戦
～ローカル5G環境での独自路線を追求したNSA/SA商用サービス化への道のり

2.1 はじめに

IIJは、2008年に法人向け、2012年に個人向けのMVNO[*1]事業を開始しました。以来、業界のリーダーとして、また2018年以降は日本初のフルMVNO[*2]として、様々なMVNOサービス・ソリューションを提供しています。使用する無線網も、当初のNTTドコモの3G網から、2012年には日本初の4G LTE対応MVNOとなり、2014年にはKDDI 4G LTE網に対応することで、キャリアリダンダンシー(冗長化)を求めるお客様に最適なソリューションを提供できる「マルチキャリアMVNO」へと進化を遂げました。更には2020年にKDDIの5G網をサポートするなど、これまでMNO[*3]の運用する最新の無線網を利用して成長してきました。

このようにIIJは常にMVNOとして先頭を走っていますが、フルMVNOとしてHSS(Home Subscriber Server)[*4]を導入した究極の目的は、PLMN(Public Land Mobile Network)[*5]=440-03(IIJ)を基地局から広報することで、端末を含むend-to-endに対して、IIJ単独でのサービス提供を可能とすることです。

これを実現するためには、HSS/P-GW(Packet Data Network Gateway)[*6]だけではなく、MME(Mobility Management Entity)[*7]/S-GW(Serving Gateway)[*8]及び基地局をIIJで保有する必要があります。しかし、IIJのような電気通信事業者[*9]に対して、商用局免許(無線)を取得できるような周波数割り当ての機会が、これまでなかなか訪れませんでした。

そのような状況の中、ついに情報通信審議会 新世代モバイル通信システム委員会報告(2019年6月18日)において、候補周波数帯のうち、28.2-28.3GHzの技術的条件が取りまとめられ、今般、2019年12月に必要な制度整備が行われました。またローカル5Gについても、導入当初はNSA(Non-Stand Alone)[*10]構成によるアンカーの構築が必要となることから、2019年12月のローカル5Gの制度整備の際に地域広帯域移動無線アクセスシステム(以下「地域BWA(Broadband Wireless Access)[*11]」という)の帯域(2575-2595MHz)を使用した4Gによる通信システム(以下「自営等ＢＷＡ」という)についても併せて必要な制度整備が行われました。

制度化に伴い、IIJもローカル5G基地局/BWA基地局を自前で保有できることとなり、我々はNSA化に必要な技術検討を早々に開始しました。

本章では、第2項でNSA化に伴う技術検討、第3項でNSA導入事例、第4項でSA導入に向けての必要な機能の洗い出し、第5項でフルVMNO実現に向けた取り組みを説明していきます。

2.2 NSA(Non-Stand Alone)化に伴う技術検討

NSA化で必要となる装置は、HSS/MME/S-GW/P-GW/4Gアンカー(BWA)基地局/ローカル5G基地局です。IIJはフルMVNO化により、既にHSSを自前で保有しています。そのため、

＊1　仮想移動体通信事業(Mobile Virtual Network Operator)の略称。
＊2　IIJ、「IIJ、フルMVNOとして法人向けモバイルデータ通信サービス「IIJモバイルサービス/タイプI」を提供開始」(https://www.iij.ad.jp/news/pressrelease/2018/0315-2.html)。
＊3　移動体通信事業者(Mobile Network Operator)の略称。
＊4　3GPP移動通信ネットワークにおける加入者情報データベース管理論理ノードであり、認証情報及び在圏情報の管理を行う。
＊5　移動体通信システムでは、各端末(内のSIMカード)に世界的に一意な加入者識別番号「IMSI」(International Mobile Subscriber Identity)が発行されている。IMSIは3つの識別番号の組み合わせで、先頭の3桁が国・地域を表す「MCC」(Mobile Country Number)、続く2～3桁(国によって異なる)が事業者を表す「MNC」(Mobile Network Code)、残りの桁が加入者識別番号の「MSIN」(Mobile Station Identification Number)となっている。このうち、MCCとMNCを組み合わせた事業者ネットワークの識別番号のことをPLMNと呼んでいる。MCCは国際電気通信連合(ITU-T)が策定しており、日本には「440」「441」の2つが割り当てられている。MNCは総務省が事業者の申請に基づき発行しており、「00」から「99」の2桁で構成される。なお、総務省よりMNC３桁化に向けたガイドラインが公表されている(https://www.soumu.go.jp/main_content/000663786.pdf)。
＊6　トランジット回線の接続点であり、端末IPアドレスの割り当てやS-GWのパケット転送などを行う論理ゲートウェイノード。
＊7　LTE基地局(eNodeB)を収容し、モビリティ制御などを提供する論理ノード。
＊8　3GPPアクセスシステムを収容する論理ゲートウェイノード。
＊9　伝送路設備を保有しない電気通信事業者(旧第二種電気通信事業者)のこと。
＊10　3GPP Release 15で定義されているアーキテクチャで、制御信号はLTEで、データ信号は5Gで送信するOption3xが主流である。コア装置はLTEのMME/S-GW/P-GWを流用する。
＊11　2.5GHz帯の周波数の電波を使用し、地域の公共サービスの向上やデジタル・ディバイド(条件不利地域)の解消など、地域の公共的な福祉の増進に寄与することを目的とした電気通信業務用の無線システムのこと。

HSSに対して、NSA化に必要な開発を実施しました。また、BWAのみ契約したユーザに5Gを使用させないために、HSSに図-1の機能を開発しました。

BSS(Business Support System)*12 ～HSS間のプロビジョニングIFにも変更が必要ですが、既存フルMVNOのIFを対象に、軽微な拡張で済ませることができました。P-GWは、LTE対応MVNOで既に保有しています。MME/S-GWのみを新規に導入する選択肢もありましたが、P-GWを既存IIJモバイルサービスとNSAサービスで共有すると、P-GWのリソース設計が複雑になることと、障害時の切り分けが困難になることから、MME/S-GW/P-GWを新規に導入することにしました。

S-GW/P-GWを制御するRadius/PCRF(Policy and Charging Rules Function)*13/OCS(Online Charging System)*14/OFCS(Offline Charging System)*15に関して、IIJの既存設備を流用するかどうかも並行して検討しました。P-GWと同様、既存IIJモバイルサービスへの影響を考慮し、新規に開発することにしました。Radius開発にあたってはちょっとした工夫をしました。PCRFで管理しているPCC(Policy and Charging Control)ルールをRadiusに持たせることで、PCRFを不要にしました。PCRFが不要になったため、オンライン処理をするOCSも不要になりました。これによりRadius/OFCSのみが開発対象となり、コストと工程数を大幅に削減できました。ただ、デメリットもあります。リアルタイム処理ができないので、速度規制などを実施するとバッチ処理のため1日遅れで実行されます。

サービスの観点では、BWA/5Gとも容量無制限でのサービス提供が可能になりました。IIJモバイルサービスのようにキャリア設備を使わないため、第1項で述べたフルMVNOの究極の目的である「end-to-endに対してIIJ単独でサービス提供を可能にすること」の効果が表れました。また、BWAとローカル5GのDual Connectivity*16(下り回線のみ)を開発し、BWA速度とローカル5G速度の合算でサービスを提供しています。

基地局～MME/S-GWのいわゆるバックホール回線も自前で引く必要があります。C-Plane/U-Plane/M-Plane*17を1つの回線で混在させると、重要なC-planeのパケットが破棄される可能性があるため、VLANで分けてDSCP(Differentiated Services Code Point)値で優先付けをすることにしました。

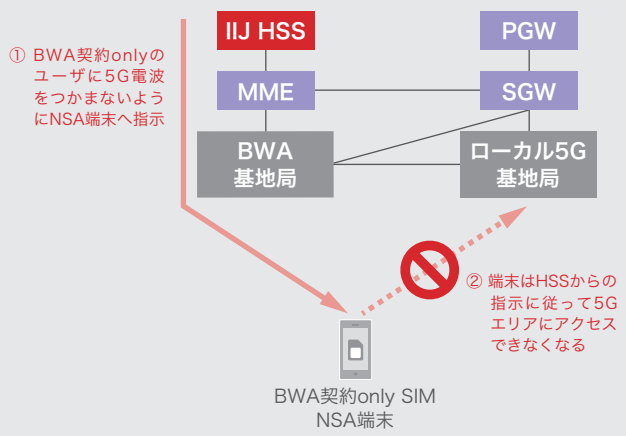

図-1 BWA契約者に5Gサービスを使用させない仕組み

*12 通信事業者向けの業務支援システムの総称。顧客情報や課金情報を管理し、サービス申し込み、開通処理、料金請求、問い合わせ対応などの実務をサポートする。
*13 ユーザデータ転送のQoS及び課金制御を行う論理ノード。
*14 オンライン課金システムのこと。
*15 オフライン課金システムのこと。
*16 異なる基地局間のキャリアを束ねることで無線区間の速度向上を図る技術。
*17 制御プレーン(C-Plane)/ユーザプレーン(U-Plane)/管理プレーン(M-Plane)のこと。

SIM(Subscriber Identity Module)[*18]に関しては、BWA基地局エリアのみで使えるものと、ドコモLTE網エリア⇔BWA基地局エリアで使えるものを準備しました。ローカル5G導入に関するガイドラインによると「全国MNOのサービスを補完することを目的としたローカル5Gとの連携は不可である一方、ローカル5Gのサービスを補完することを目的として、全国MNOのネットワークを利用することは可能」との記載があります。ローカル5Gエリア⇔全国MNO 5Gエリアとの連携が可能であるとの解釈もできますが、MNOとの調整が必要と判断して、ローカル5Gエリアで使用できるSIMのみを準備しました。

BWA基地局に関しては、他事業者が提供しているBWA基地局の無線速度以上を達成することを要件として、無線品質に応じてQPSK/16QAM/64QAM/256QAM[*19]と変調を変えるAdaptive変調方式を開発しました。本開発により、MU-MIMO(Multi User MIMO)[*20]:4×4の条件のもと、下り無線速度は最大295Mbps(256QAM)、上り無線速度は17Mbps(64QAM)のスループットを達成することができました。ローカル5G基地局に関しては、28G帯100MHzのみが免許申請対象でしたが、MU-MIMO:2×2の条件のもと、下り無線速度は最大484Mbps(64QAM)、上り無線速度は125Mbps(64QAM)スループットを達成することができました。以上の検討を踏まえて、IIJ用のNSAアーキテクチャー(図-2)を完成させました。

2.3 NSA導入事例

■ ① 白井ワイヤレスキャンパスへの導入事例

IIJは最新の無線技術を集めた実験施設「白井ワイヤレスキャンパス」を、千葉県白井市に構築し、2020年11月より本格的な運用を開始しています。この白井ワイヤレスキャンパスは、単に最新の無線技術のショーケースであるにとどまらず、端末やネットワーク設備の間、あるいはネットワーク設備同士の相互運用性の検証環境として、また最新の無線技術の利活用を目指すお客様と共同で実証実験を行う場として、提供予定です。

白井ワイヤレスキャンパスの目玉とも言えるのが、2021年3月に商用局免許を取得したローカル5Gです。ローカル5G基地局/BWAを収容するNSAコアは、第2項で説明したIIJ用NSAアーキテクチャーの設計思想に基づいて構築済みで、それぞれの基地局については、複数のPLMNを広報させるよう基地局/MMEに開発を行いました(図-3参照)。ローカル5G基地局/BWA基地局は電波発射をして稼働中です(図-4参照)。

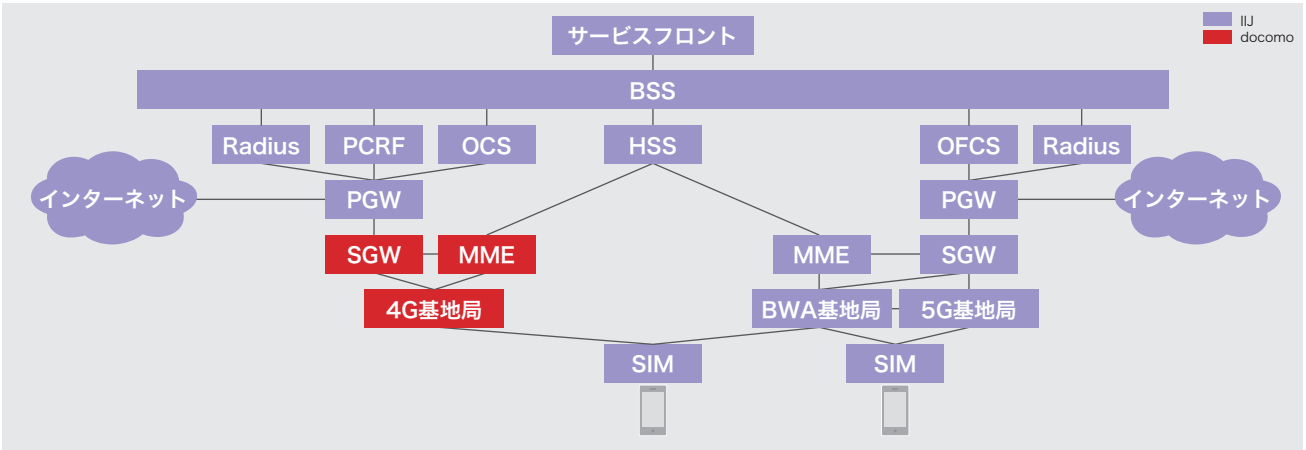

図-2 IIJ NSAアーキテクチャー構成

*18 正式名称は、UIM(User Identity Module Card)、またはUSIM(Universal Subscriber Identity Module Card)であるが、一般的にはSIMカードと呼ばれている。
*19 無線変調方式のこと。
*20 複数の送信アンテナから同時にデータを送信し、そのデータを複数の受信アンテナで受信することで、空間分割多重技術を使って同時に送信できるデータの量を増加する方法。MU-MINOは複数のユーザが同時に通信できる。これに対して、SU-MIMO(Single User MIMO)は1ユーザのみしか通信できない。

ローカル5G/BWAと並行して、白井ワイヤレスキャンパス内にヘテロジュニアス無線環境を順次構築しています。既に、sXGP(band41)基地局をMME/S-GWに接続済みで、Passpoint[*21]対応Wi-Fi APも今後、HSSに収容する予定です。また、異なる無線エリア間のシームレス通信のため、東大 中尾研との実証実験[*22]で得たSIM設計ノウハウをIIJ SIMに反映させました。SA(Stand Alone)[*23]に関しても、今後Sub6[*24]基地局/SAコアを調達し、白井ワイヤレスキャンパスに構築予定です。

■ ② グレープ・ワンへの導入事例

ローカル5Gサービスを立ち上げるために、住友商事/CATVとの共同出資で、新会社株式会社グレープ・ワンを設立[*25]しました。第2項で説明したNSA化の技術検討で培ったノウハウが、グレープ・ワンのNSAコア構築の際にも生かされています。

2.4 SA(Stand Alone)導入に向けての必要な機能の洗い出し

第3項で説明したとおり、NSAコア及びローカル5G基地局/4G Anchor基地局(BWA)の商用サービスは既に開始されました。次のステップとして、SAをどのような形でIIJサービスへ取り入れていくかの検討が必要となります。そこで、SA導入に必要な機能の洗い出しを実施しました。

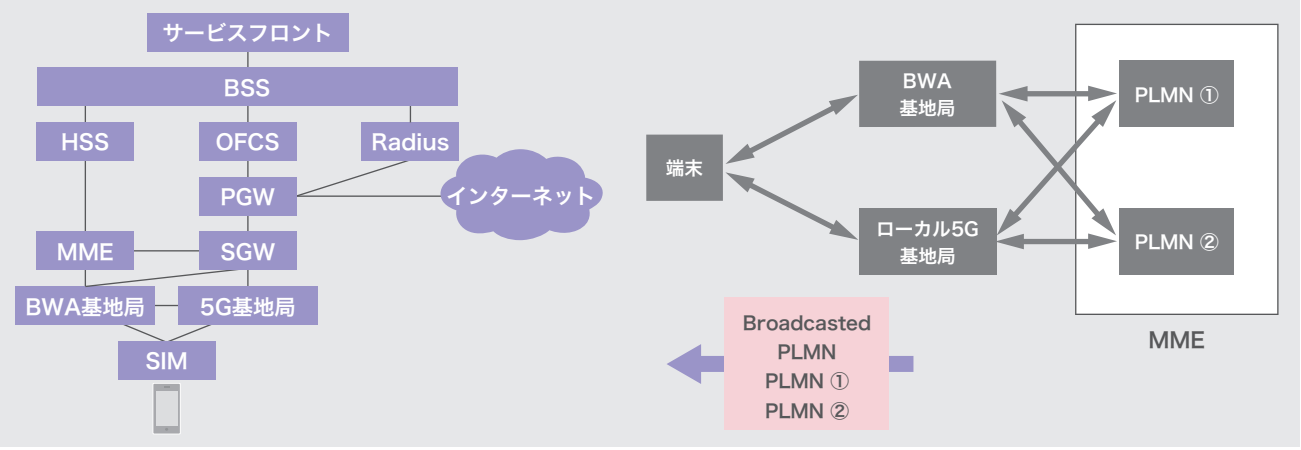

図-3 白井ワイヤレスキャンパスNSA NW構成とMultiple-PLMN概要

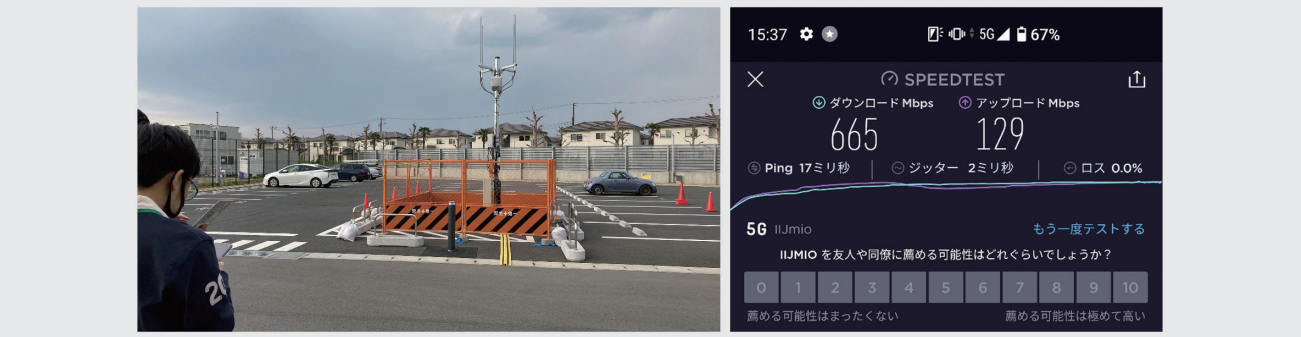

図-4 白井ワイヤレスキャンパスのローカル5G基地局と端末スピードテスト

*21 無線LANの規格を管理しているWi-Fiアライアンスが認定している通信規格で、以前はHotSpot2.0と呼ばれていた。通常のWi-FiはSSIDとパスワードが必要だが、この規格に対応していれば、Wi-Fiスポットに入れば自動的に接続される。
*22 IIJ、「国内初！東京大学とIIJ、パブリックLTEとプライベートLTEの統合連携に関する実証実験を開始」(https://www.iij.ad.jp/news/pressrelease/2019/0605.html)。
*23 LTEコアネットワーク(HSS/MME/S-GW/P-GW)とは独立した形で、5G専用コアネットワークで5G基地局を単独で動作させるアーキテクチャ。Option2が主流である。
*24 6GHz未満の周波数帯のこと。
*25 IIJ、「ローカル5Gの活用を目的とした無線プラットフォーム事業の展開について」(https://www.iij.ad.jp/news/pressrelease/2019/1224.html)。

① アプリケーションからSAコアを制御できるNEF (Network Exposure Function)[*26]

3GPP R16でNEF(図-5参照)に求められる機能が、R15に比べてだいぶ明確になりました。3GPP TS 23.502にNEF API Application Programming Interface一覧が更新されており、LTE のSCEF(Service Capability Exposure Function)[*27] をベースにはしていますが、Nnef_TrafficInfluence/Nnef_AnalyticsExposureなどSCEFにはないAPIも登場しています。IIJには、IIJ IoT サービスと呼ばれるIoTプラットフォームなどのクラウドアプリケーションが豊富にありますので、NEFを利用することで、面白いSAサービスを提供できることになるでしょう。

② 加入者プロファイルの一元管理で問い合わせ窓口を一本化

NSAはUDR/MME/S-GW/P-GWそれぞれの装置に加入者プロファイルデータを分散して管理していたため、加入者プロファイルの問い合わせ先が分散されて、処理が煩雑でした。そこで、3GPP TS23.501 4.2.5 Data Storage architecturesで、これまで分散されていたデータをUDR(Unified Data Repository)/UDSF (Unstructured Data Storage Function)に一元管理するNudr IFの規定が新たに設けられました(図-6参照)。これにより、クラウド上でのデーター元管理が可能となり、加入者プロファイルの問い合わせ窓口はUDF/UDSFに統一化され、処理が効率化できました。

③ ローカルブレイクアウト(MEC [*28])

NSAはローカルブレイクアウト機能がないため、S-GW/P-GWを地域に分散配置せざるを得ませんでした。そこで、SAではS-GW/P-GW内の各論理機能を物理的に分割させました。つまり、セッション機能をつかさどるSMF(Session Management Function)、PCCルール機能をつかさどるPCF(Policy Control function)、及びパケット処理をつかさどるUPF(User Plane Function)を新たに定義し物理的に分割したのです。

SMFはクラウド上で集約することで、旧UPFから新UPFのセッション維持を大きな役割として持ち、ブレイクアウトがしやすくなりました。仮にSMFを分散配置にすると、各SMFでセッション情報のデータ同期をしなければならず、物理的に分割した意味がなくなるからです。PCFもSMFと同様な理由で、クラウド上で集約することにより意義を持ちます。

また、①で説明したNEF APIのNnef_TrafficInfluenceを使えば、アプリケーションからの制御で、ローカルブレイクアウトも可能になります。

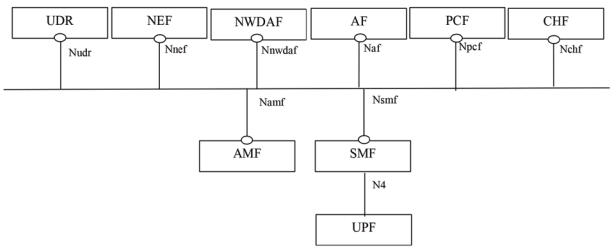

図-5 NEFを含むSAコアアーキテクチャ(3GPP TS 23.503より抜粋)

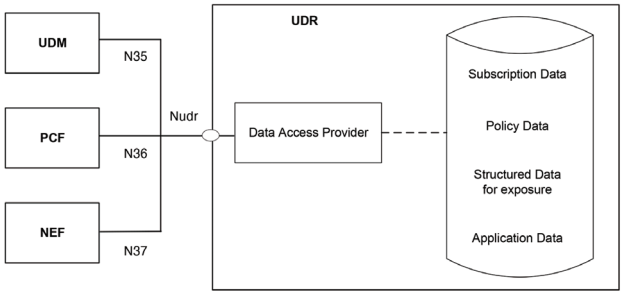

図-6 Data Storage architectures(3GPP TS 23.501より抜粋)

*26 外部アプリケーションに対して、5GC(5th Generation Core network)を構成するネットワーク論理ノード(Network Functions:NF)を制御するAPI(Application Programming Interface)を提供している論理ノード。加入者情報やネットワークの状態変化などをアプリケーション側で詳細に把握できるようになるほか、アプリケーションからNFの制御も可能になる。

*27 外部アプリケーションに対して、HSS/MMEなどのLTEコアネットワークを制御するAPIを提供している3GPP TS29.122準拠の論理ノード。

*28 マルチアクセスエッジコンピューティング(Multi-access Edge Computing)の略。

④ NW Slice

NSAでは既に、multiple PDP Contexts[*29]及びdedicated bearer[*30]で、端末～コア間でNW Slice化する技術はありますが、SAになると、NW Slice単位で細かなSLA(Service Level Agreement)が規定できるようになります。RAN(Radio Access Network)側は発展途上ではありますが、端末～UPF間でNW Sliceを実現するためには、RAN側の対応も必須です。

⑤ 5G-AKA

LTEはIMSI暗号化が不完全であったため、5G-AKAでは、IMSI相当の5G加入者ID(SUPL)のMSIN(Mobile Station Identification Number)を暗号化する仕組みが導入されました。IIJも5G-AKA対応eSIMをSAコア上で成功させました[*31]。5G-AKAの詳細は3GPP TS 33.501 V17.1.0 (2021-03)をご覧ください。

上記①～⑤の機能要件を満たすSub6/SAコア製品を調達し、白井ワイヤレスキャンパスで今後構築する予定です。

2.5 フルVMNO実現に向けて

全国エリアの5Gに関しては、MNOでなければ周波数免許を取得できないため、フルMVNOと同様、全国エリアMNO基地局と接続を行う形態になるでしょう。

IIJはフルVMNO[*32]というコンセプトを提案しており、全国エリアMNOの5G基地局に対して、RANシェアリング[*33]を想定しています。RANシェアリングは、各事業者PLMNをキーに振り分けるため、MVNOもSAコアを保有する必要があります。

一方、ローカル5G基地局は各事業者が保有するため、SAコアを自前で準備する、もしくはVMNOのSAコアに接続するなど、選択肢の幅が広がります。

第4項で説明したとおり、今後SAコア及びSub6基地局を白井ワイヤレスキャンパスに調達し、VMNO実現に向けた検証及び課題の洗い出しを実施する予定です。

2.6 おわりに

新型コロナウイルス感染症(COVID-19)の影響により、リモートワークをはじめとするDX(Digital Transformation)推進が急加速している状況です。コロナ禍以前は、ローカル5Gの普及も東京オリンピック終了後、数年かかるだろうと言われていましたが、前倒しで導入が進んでいる印象です。

IIJもBWA基地局/ローカル5G基地局、並びにNSAコアを導入したことで、無線及びコアのノウハウ取得が可能になりました。

今後、SA導入も視野に入れつつ、モバイルサービスに限定せず、他のIIJサービスと連携することで、他社にはないサービスを提供し続けたいと思います。

執筆者:
柿島 純(かきしま じゅん)
IIJ MVNO事業部 技術開発部。2017年IIJ入社以来、法人モバイルのサービス開発に従事。
特にフルMVNO立上げの際、HSSを含むコア装置の仕様策定/構築/運用設計を担当。
また、ローカル5Gサービス及びNSAの仕様策定/構築/運用設計、並びにSoftSIM/eSIM導入企画を担当。

*29 1ユーザ(端末)に複数のPDP(Packet Domain Protocol)コンテキストを提供すること。3GPP TS 23.976参照。
*30 1つのPDP(Packet Domain Protocol)に複数bearerがはれること。3GPP TS 23.401参照。
*31 IIJ、「IIJ、国内初となる5G SA方式対応のeSIMを開発」(https://www.iij.ad.jp/news/pressrelease/2020/1102.html)。
*32 Internet Infrastructure Review (IIR) Vol.48 第2章フォーカス・リサーチ(1)「5G時代のMVNOの在り方～VMNO構想の実現に向けた取り組み」(https://www.iij.ad.jp/dev/report/iir/pdf/iir_vol48_focus1.pdf)。
*33 複数事業者のコアネットワークが1つの無線設備(RAN)を共有して使用すること。

スピードが求められる障害対応に、IIJ独自開発「Barry(バリー)」

3.1 Barry導入の背景

IIJが高品質で安定したサービスを提供するためには様々な運用作業を必要とします。中でも重要なものとして障害対応が挙げられます。サービスを提供するシステムがハードウェアやソフトウェアの障害により正常な稼働状態を維持できなった場合に正常に回復するための作業です。IIJは障害対応時に利用する運用システム「Barry (バリー)」を社内で開発し運用を行っています。ここではこのBarryの仕組みと効果を紹介します。

その前に、Barry導入以前の障害発生時の対応プロセスについて触れておきます。通常、提供サービスは設備や提供機能に異常がないかを常に監視しています。サービスに異常が発生するとアラートを発出して障害対応を促します。対応行動としてまず行うのが、その時対応可能な担当者の確保です。IIJではこれをエスカレーションと呼んでいます。次に、担当者はサービスを正常な状態へ戻す作業を開始します。対応内容は担当サービスによって異なりますが、一般的には作業者間でコミュニケーションを取り、事象の調査や記録のために様々なツールを利用しながら問題解決に取り組みます。

IIJでは以上のような流れで障害に対応してきましたが、これらの仕組みには問題点もありました。これを見直し、障害対応をスムーズに行うために開発したのが、運用システムのBarryです。

従来の問題点とは、主に次の2点です。

■ 問題点① 担当者の確保と内容の正確な伝達

担当者の確保には迅速さが求められます。障害対応の候補者に連絡し、対応可能であることを確認する手段は現在も電話を用いています。理由は継続的に呼び出しを行えるという利点があるからです。メールなどによるメッセージもエスカレーションに用いることができますが、通常メッセージは発生したタイミングでのみ候補者への通知が行われます。一方、電話なら対応者が見つかるまで継続的に呼びかけ続けることができるため、目的とする担当者の確保の達成率が高くなります。その半面、人手により電話をかけ続ける場合は、担当者が見つかるまでかける側が拘束されるという問題があります。この点は自動架電のシステムを利用することで解消できますが、音声による一方的な連絡になるため、内容の確認が難しいという問題と、自動架電システムのコストの問題が残ります。加えて、同時に呼び出せる人数についても制約があります。

また、電話の場合は聞き逃しや聞き間違いの恐れがある上、英略語や記号の伝達が難しいという点が問題です。一方でメールによるエスカレーションはテキストによって行われるためこの問題はなく、内容が複雑でも伝えやすいという利点があります。

以上を踏まえ、継続的な呼び出しと内容の正確な伝達を実現したいという課題を設定しました。この問題を解決することで、障害対応における初動の迅速化が見込まれます。

■ 問題点② 担当者の負担軽減

呼び出された担当者が実施する障害対応業務には数々の負担があります。簡単な障害は自動処理による復旧が考えられますが、ここで取り上げている障害対応はサービスを熟知した担当者が状況に応じて柔軟に対応する必要のあるものです。従って、サービスに関する高度な知識と対応スキルが求められます。加えて、休日夜間の対応もある点と、早期復旧が求められている点も担当者にとっては負担です。また、障害対応自体の難易度が高い上に、関係者への連絡や情報共有などの作業も必要です。

このような状況から、システムによっては特定の人員に作業が集中することも多く見られました。しかしながら、どの程度偏りがあるのか正確に把握することは困難でした。障害対応に集中して取り組めるように、それ以外の作業に関してはできる限り簡単に対応できるようにするという課題を設定しました。

3.2 問題解決の方法

こうして、迅速な対応の確保、対応者の負担軽減を解決する運用システムの検討がなされました。既存ツールの利用も選択肢にはありましたが、IIJ独自の対応フローの事情を踏まえるとそのまま使えるものはなく、社内業務への最適化も考慮し内製のシステム開発を決断しました。開発のコストは必要ですが、都合に合わせて継続的に改善できるメリットも大きいと考えています。

まず、担当者確保の問題解決に向けては、スマートフォン向けのアプリケーションとして実現するアイデアがありました。電話呼び出しのUIを模倣し、応答を確認後にテキストでメッセージを表示することで両方の利点を活かしたまま呼び出しをしてはどうかという発想です。メッセージの利点であるテキストによる伝達と、電話による利点である継続的な呼びかけを同時に実現します。また、電話という制約もなくなるため、エスカレーションの順序や同時に呼び出せる人数などのカスタマイズが可能になるというアイデアも出ました。運用チームの形態に合わせた柔軟な呼び出しが実現できると考えました。

担当者の負担軽減の面では、担当者が不便に思っている点を認識する必要があると考え、複数の運用担当者に対し、スマートフォンを利用した呼び出しのアイデアを伝えた上でヒアリングを行いました。その結果、多く出た意見は情報共有の不便さでした。障害対応においては障害内容の把握、対応時の情報共有、インシデント管理をしています。ヒアリング時点では、対応時のリアルタイムな情報共有はIRC(Internet Relay Chat)やSaaS型コミュニケーションツールなど、運用チームごとに採用しているツールが異なっていました。発生した障害をインシデントとして記録する手段も、メールやWiki/チケットシステムなど様々でした。また、PCが近くにない場合は障害の発生を知ることができても対応状況が分からないなどの不便さがあり、チームでの対応の難しさに繋がっていました。これらを踏まえ、エスカレーションを受けた担当者の情報共有や管理を統合的に行う必要もあると考えました。ツールの使いやすさも対応の効率に大きく影響するためです。新しい運用システムでは担当者の意見を取り入れながら、使い勝手を重視することとしました。

3.3 Barryの機能

新しい運用システムをBarryという名称で実装を始めました。命名の由来は有名な山岳救助犬で、障害対応に関わる人の助けになってほしいという願いを込めています。

Barryの機能はサーバ、Webフロントエンド、モバイルアプリの3つに分かれています。サーバはエスカレーションやインシデントの管理など中心的な機能を実装しgRPC APIとして提供します。Webフロントエンドとモバイルアプリはサーバの APIを使用して利用者にUIを提供します(図-1、

図-1 Barryのモバイルアプリ画面

図-2)。現状では障害対応すべてをモバイルアプリのみで行うのは難しいため、それぞれ得意とする分野を分けています。モバイルアプリでは呼び出しと簡単なコミュニケーションの実現を中心に考えており、本格的な障害対応にはPCからWebフロントエンドを利用する想定でシステムを構成しています。

スマートフォンをツールとして採用することで、従来であれば状況も分からず障害対応に加われないような場面でも、助言などのサポートができるようになりました。モバイルアプリについては企業内に配布する仕組みを用いて社内向けに配布しています。

ここからはBarryで実装した具体的な機能について紹介します。

■ 機能① 柔軟な呼び出し

スマートフォンの呼び出しを実現するにあたり、実装には一般的な通話アプリと同等の技術を用いています。サーバにエスカレーション開始のリクエストが行われると、サーバは障害が発生したサービスに応じた運用チームのスマートフォンに通知します(図-3)。エスカレーション開始の通知を受け取ったモバイルアプリが電話着信のUIを表示するという仕組みです。利用者は着信への応答後にモバイルアプリを起動し、サーバに記録されている詳細情報を確認し、対応可否をアプリから回答します。対応可能の回答をもってエスカレーションが終了する仕組みです。この仕組みを基本とし、サーバでは呼び出し順、同時に呼び出す台数、鳴動時間、繰り返し回数を運用チームが自由に設定できるようにしています。

また、エスカレーションの開始は自動と手動の2パターンを用意しています。先に紹介したサービスの監視アラートからエスカレーションを自動的に発生させることができます。アラート以外にも緊急時の呼び出しを想定した手動によるエスカレーションの開始をサポートしています。

■ 機能② 統合的な情報管理

障害対応において様々なツールの利用が担当者の負担になっている点を問題として挙げていました。Barryではエスカレーションからインシデントの管理までを統合的に行えるような機能を提供しています。担当者の呼び出し機能に加え、インシデント管理の仕組みを実装しました。機能的には課題管理システムと同等のもので、発生した障害の情報を記載し対応状況の管理ができるツールです。

具体的には、障害を1つのインシデントとして表現し、対応状況を更新しながら運用チームでコミュニケーションを行いながら解決までの記録を残します。発生したアラートをインシデント

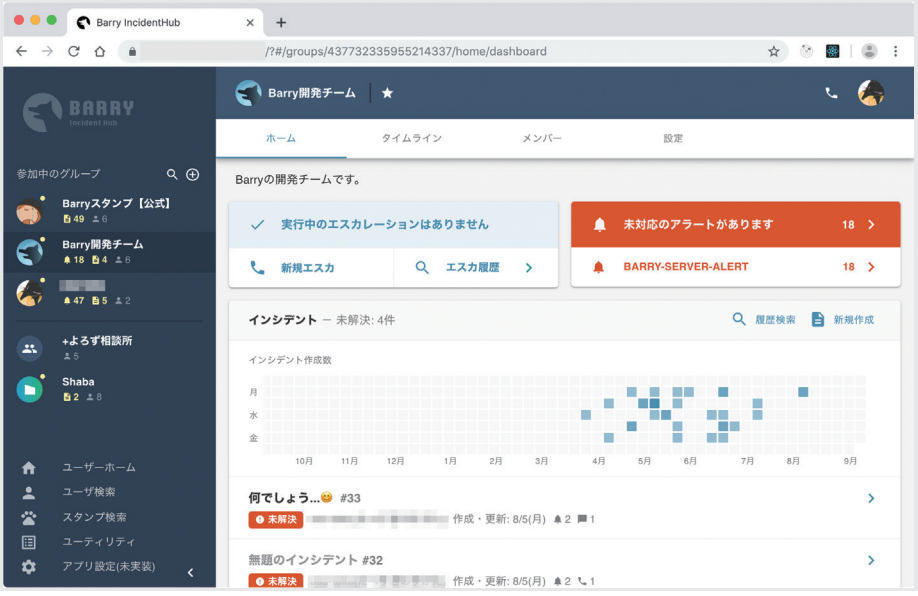

図-2 BarryのWebフロントエンド

と関連付けて記録できます。インシデントを記録することで、過去の事例を参照しながらの障害対応が可能となります。

この機能を実現することで、障害の発生から対応完了までを1つのツールで完結できるようにしました。また、Barryは利用できる環境としてWeb／モバイルアプリをサポートしていることから、対応者は移動中なども状況の確認やコメントができるようになりました。

■ 使いやくするための工夫

様々なツールを統合的に利用できる機能を実現しても、効率が落ちてしまえば効果は限定的になってしまいます。このため、Barryではツールとしての使いやすさも重要視しています。

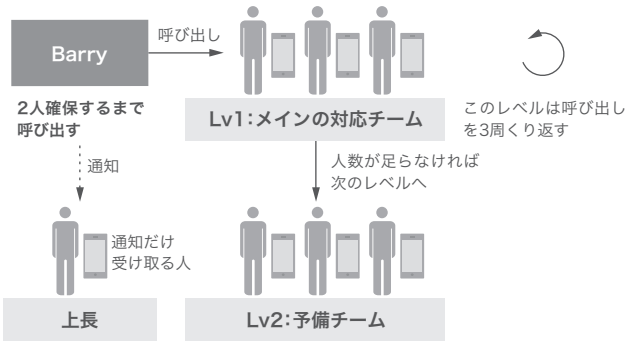

図-3 Barryの対応者呼び出しプロセス

システムの設計段階で担当者からのヒアリングを行い、認識の共通化のためにモックアップを作成して意見を求めました。このプロセスを繰り返し行うことで、必要とされている機能が明確になり、使い勝手の面でも早期にフィードバックを得られました。細かな機能の作り込みも多く行ったため、代表的なものを順に紹介します。

■ 活動記録の表示機能

まず、事象の発生頻度を分かりやすくし、障害対応の作業量を把握するために統計と可視化の機能を実装しました。これは発生したアラートや、利用者ごとの活動記録を時系列にグラフ化して表示する機能です(図-4)。アラートを時系列に表示することで、障害発生状況の分析を効率的に実施できます。また、運用チームの活動記録を分かりやすくすることで、従来よりも管理者による正確な状況把握が可能になりました。

タイムライン表示は、出来事を発生順に表示する機能です。Barryを利用する上ではアラートの発生やインシデント/コメントの新着を多く目にします。利用者は複数の運用チームをかけもちしていることも少なくなく、多くの出来事が発生している場合は把握が難しいケースもあります。タイムライン機能では発生したイベントを利用者ごとに時系列表示しており、容易に出来事を把握できます。

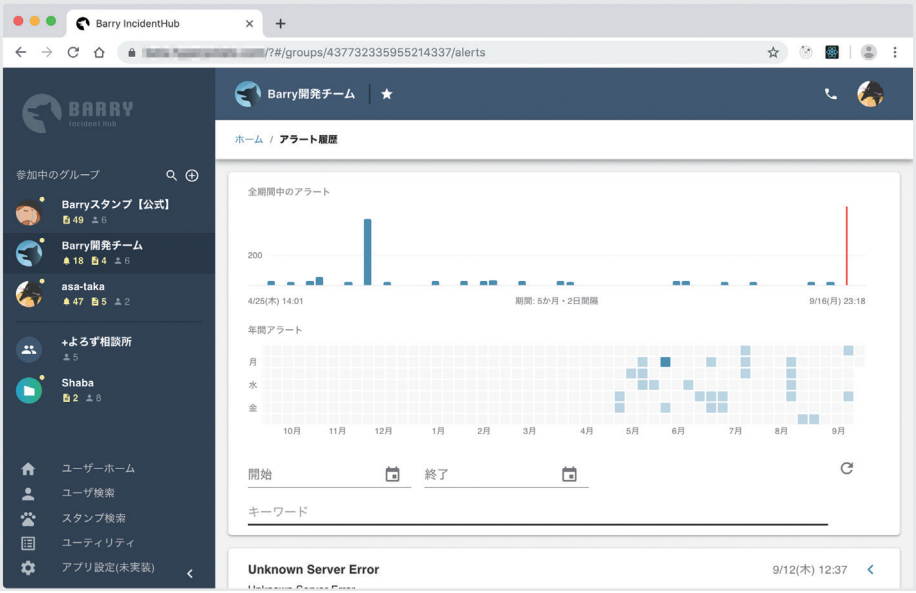

図-4 アラート発生頻度のグラフ化

■ スタンプ機能

インシデントコメントへの絵文字によるリアクションとスタンプは、円滑なコミュニケーションのために用意しました(図-5)。対応内容に感謝などの感情を示したりする際、コメントとして表現してしまうとインシデントに対する情報が増えてしまい、重要な対応内容が分かりにくくなってしまうという問題があります。このような場合を想定して、絵文字によるリアクション機能を実装しました。また、ソーシャルネットワーキングサービスなどで用いられるスタンプ機能も用意し、定形の情報を簡単に使えられるようにしています。

■ アバター機能

アバターは利用者や運用チームごとに画像を設定する機能です。これもソーシャルネットワーキングサービスなどで多く利用されている機能で、視認性の向上に役立ちます。利用者と運用チームに対して自由に設定できるようにすることで、ミスの予防などを目的としています。

■ Webhook

また、提供機能は自動処理を念頭に置いています。画面操作によって実現できることはすべてAPIを提供しており、利用者はソフトウェアによる自動化を選択肢に持つことができます。これ以外にも自動処理専用の仕組みも設けており、代表的なものとしてWebhookと呼ばれる仕組みも利用者要望をきっかけに実装しました。WebhookはWebアプリケーションが外部システムへ情報を送信する仕組みで、多くのWebサービスなどでも採用されているものです。Barryがこの情報送信の受信側として機能し、アラートの受信やエスカレーションの開始をサポートします。具体的にはGrafanaなどのWebhookと連携をすることで、既存のシステムと追加開発なしに連携ができるようになりました。このほか、コマンドラインツールも作成・提供しており、簡単なスクリプトによるBarry利用も実現しています。障害対応における業務の自動化において、これらの機能が用いられることを想定しています。

図-5 コメント画面の絵文字・スタンプ例

3.4 Barryを使った障害対応

次に、Barryを導入した場合のシステム運用の流れを追ってみます。

Barryは社内向けに提供する運用システムであり、サービス運用者は事前準備として以下を行います。

1. サービス監視のアラート送信先をBarryに設定
2. エスカレーションの際、誰をどの順番で呼び出すかのルール定義
3. 障害対応の担当者はスマートフォンにBarryモバイルアプリをインストール

これらの準備ができた状態でサービスの監視アラートが発生すると情報はBarryに送信されます。Barryはアラートを受け取ると、内容を保存し運用チームを特定してエスカレーションを開始します。エスカレーションでは運用チームごとに定義された呼び出しルールに従い、対応可能な担当者が見つかるまでスマートフォンを鳴動させます。

利用者はスマートフォンの鳴動によりエスカレーションの発生を知り、発生した呼び出しの理由を確認します。内容にはアラートの詳細までが含まれ、対応可能であればモバイルアプリから対応開始と回答します。システムはここで呼び出しを停止し、対応者の決定がグループ内に通知されます。

エスカレーション機能はここで役目を終え、以降は統合的な情報管理を提供するインシデントの機能が中心的に利用されます。担当者は受け取ったアラートの情報から出来事を整理しインシデントとして情報をまとめ、その後の障害対応の内容をコメントとして残しながら対応を進めます。追加されていく情報はモバイルアプリへの通知を含めてリアルタイムに運用チーム内で共有され、必要に応じて対応者以外もコメントを追加していきます。担当者が1人で対応できない場合は追加の人員呼び出しも可能です。

障害対応が終わると、インシデントを完了として更新することでBarryによる対応を終えます。記録したインシデント情報やエスカレーションの履歴はシステム内に記録が残ります。検索機能も備えているため、障害対応中に過去の類似アラート発生時の対応内容を参照するようなこともできます。

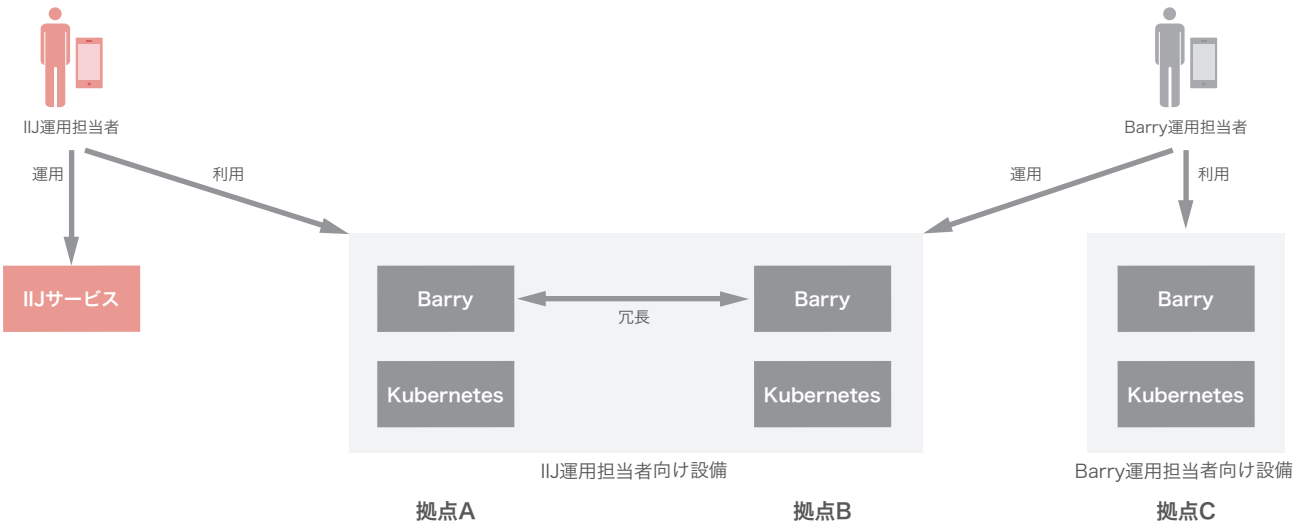

図-6 Barryのシステム構成

3.5 運用

Barryは様々なサービスの障害対応時に必要とされるシステムであるため、高い可用性が求められます。当然ながらBarry自体に障害が発生する可能性もあるため、障害の発生を前提に設計・運用しています。

システム構成としては独立した3拠点を利用し、うち2拠点で1つのBarryシステムを冗長する構成を採用しました(図-6)。残る1拠点では別系統のBarryを動作させています。これはBarryの運用者が利用するもので、Barry自体に障害が発生した場合はこちらを用いて障害に対応します。

それぞれの拠点では独立したKubernetesクラスタが稼働しており、BarryはKubernetes上で動作しています。Kubernetesの機能を活用する構成により、Barryの運用はハードウェアなどの故障を意識する必要がなくなりました。

Barryはスマートスマートフォンへの通知に外部サービスを利用しています。外部サービスの障害や遅延が単一障害点とならないよう、複数の外部サービスを組み合わせて実装しています(図-7)。サーバで通知を送信したスマートフォンの反応を確認し、通知の仕組みに異常を検知した場合は自動架電へフォールバックするようにしました。

また、トップレベルドメインの障害などが起きると、Barryが正常に動作していても名前解決できないことでアクセス不可に陥ることもあります。この問題に対しては提供ドメインを複数用意して、アクセスするための手段を冗長化しています。

システム障害とは少し異なりますが、モバイルアプリに不具合がある場合の対応も行っています。サーバ側では不具合発生時に運用者が切り戻しなどを実施できますが、個々人の端末にインストールされたアプリに関しては対応ができません。致命的な不具合があると呼び出しの仕組みが機能しなくなるため、アプリの配布も2系統で行っています。具体的には随時アップデートを行う通常版のアプリの他に、安定した動作が確認できている緊急用をインストールできるようにしています。

3.6 導入と効果

Barryは2020年の7月に社内向けにリリースしました。障害対応の仕組みを一斉に置き換えるのは現実的でないため、このリリース後から利用を希望するサービスごとに個別切り替えを行う方針をとっています。利用者側ではアラート送信の仕組みなどを置き換える必要はありましたが、各サービスの協力により切り替えが進んでいます。特に新規に運用を開始するサービスにおいてはBarryが採用しやすい状況です。

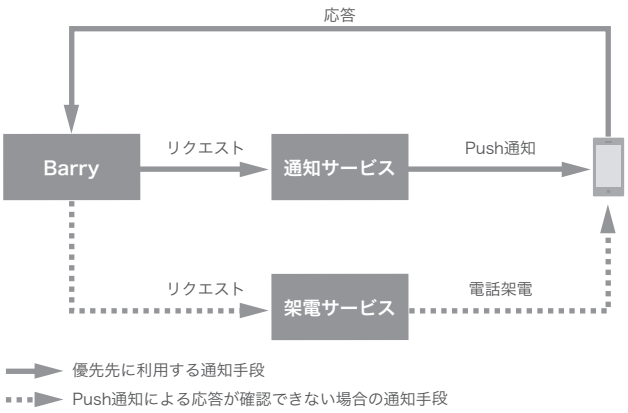

図-7 Barry障害発生時のフォールバック

Barry利用者により作成されたツールも存在しており、API公開を前提とした方針が利用者の業務自動化・効率化に貢献できていると感じています。

また、電話に似た継続的な呼び出しを実現しつつ、テキストによる連絡が同時に行われることで情報の伝達が効率的になりました。自動化によって呼び出しという単純な処理をBarryに任せられるようになっています。加えて、運用体制によっては呼び出しの並列度を上げることで候補者へ一斉に連絡できます。電話の逐次的呼び出しにおいては、候補者のうち一部が対応可能な場合は初動の遅れが発生していましたが、この点も解消できました。解決したい課題として設定していた初動の迅速化に繋がっています。

現在利用ユーザは633、運用チーム数は190です。リリース後、利用者に対してBarry利用に関するアンケート調査を実施しました。設問は利用頻度や導入によって業務が改善された点、更に改善を求める点を設けました。この内容について紹介します。

導入により業務が改善された点については、解決したい課題として設定していた初動の迅速化、状況の把握が挙がりました。架電をシステムが担うことによる負荷の軽減に加え、アラートからエスカレーションまでを自動化したことにより、障害発生を早く知ることができるようになりました。また、コミュニケーションに関する内容もありました。運用チーム内で障害対応状況がわかりやすくなったことで、共同作業に取り組みやすくなりました。Barry導入により前向きな改善の意見が得られたことで、運用業務の一助になったと考えています。

一方で、Barryに対して改善が求められる内容もありました。1つは既存のシステムとの連携の簡易化です。APIを提供して様々なユースケースに対応できる設計としていますが、Barryの利用にあたっては既存のシステム側の改修が必要です。既存の運用システムになるべく手を加えずBarryを使い始められるような仕組みを求める意見がありました。IIJ固有の事情に対応するべく設計したシステムなので、個別の要望に柔軟に対応していく予定です。

もう1つは安定稼働についての懸念です。先に紹介したとおり、Barryは障害時に使われるシステムであることから安定した運用が求められます。利用者が採用を検討する際の指標として稼働実績が挙げられますが、Barryはまだリリースから日が浅いため実績は不足しています。安心して利用されるようなシステムにするためにも、Barry提供における重要事項として安定した運用を積み重ねていきます。

社内での利用開始という大きなマイルストーンを達成しましたが、まだまだ取り組むことがあります。今後も継続的にアップデートすることでIIJサービスの品質維持・向上のために貢献していきます。

執筆者:
中井 優志（なかい ゆうし）
IIJ 基盤エンジニアリング本部 運用技術部 運用システム開発課 課長。2007年IIJ入社。サービスや運用システムの開発に従事。

June 2021 Vol.51

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2021年6月時点のものです。

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