IIR

Internet
Infrastructure
Review

Jun.2019
Vol.43

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)

ブロックチェーン技術をベースとした アイデンティティ管理・流通の動向

フォーカス・リサーチ(2)

IIJにおけるeSIMの取り組み

IIJ
Internet Initiative Japan

Internet Infrastructure Review

June 2019 Vol.43

エグゼクティブサマリ

平成の30年が終わり、5月より令和に元号が変わりました。平成が始まったのは1989年。商用のインターネット接続サービスが開始されたのは1993年なので、まだインターネットが一般的に使われる前です。インターネットの普及に大きく寄与したWindows 95が発売されたのが1995年。Googleが設立されたのが1998年。NTTドコモが携帯電話によるインターネット接続サービスであるiモードを開始したのが1999年。NTT東日本とNTT西日本がFTTHサービスであるBフレッツを開始したのが2000年。NTTドコモが世界初の第3世代携帯電話サービスであるFOMAを開始したのが2001年。Appleが初代iPhoneを発売したのが2007年。NTTドコモが第4世代携帯電話サービスであるXiを開始したのが2010年。平成の30年間は、我が国だけでなく、世界的に情報通信が大きく発展した時代でした。

本号は令和に入って初めての「IIR」となります。今、一部の国では第5世代携帯電話サービスが開始される一方、巨大なプラットフォーム事業者による情報の独占が問題になっています。我が国においても、昨年より総務省において「電気通信事業分野における競争ルール等の包括的検証」が開始され、ネットワークレイヤーのみならず、プラットフォームや端末のレイヤーにも範囲を広げ、2030年頃を見据えたネットワークのビジョンが議論されています。情報通信技術は、これからの時代においても、社会の発展に大いに寄与するものであり、IIJもその一翼を担っていきたいと考えています。

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

1章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テクノロジーを取り上げます。IIJのメールサービスの受信側において、SPF、DKIM、DMARCの送信ドメイン認証技術の普及状況を確認したところ、SPFの認知がかなり高くなっている一方、DMARCの認知は進んでいないことが分かっています。米国連邦政府のドメインの80%がDMARCレコードを設定しているという調査結果もあるなか、日本でもDMARCの認知度をより高める工夫が必要です。本章では、送信ドメイン認証技術の普及状況に加えて、メールの配送経路の暗号化の解説や、筆者もメンバーとして活動しているM^{3}AAWG、JPAAWGの活動について紹介します。

2章のフォーカス・リサーチ(1)では、ブロックチェーン技術をベースとしたアイデンティティ管理・流通の動向を解説します。ここでは、Ethereumブロックチェーンがクレデンシャルに用いられるERC(Ethereum Improvement Proposal)の動きを取り上げ、クレデンシャルが公的な証明書として利用されるユースケースに触れています。また、ここ数ヵ月において、複数のベンダーやコンソーシアムがDID(Decentralized Identifiers)やSSI(Self Sovereign Identity)などの概念を提示し、ブロックチェーンをベースとしたクレデンシャル管理技術が注目されていることを紹介します。

3章のフォーカス・リサーチ(2)では、eSIMを取り上げます。IIJは昨年、HLR/HSSを自社で保有し、いわゆる「フルMVNO」となりました。フルMVNOになったことで提供できるようになった機能の1つにeSIMがあります。この章では、eSIMが必要とされる背景やeSIMの仕組みを説明したうえで、他社及びIIJの取り組みをお伝えします。物理的なSIMカードが不要となり、通信契約を管理するプロファイルが電子データとしてやり取りされる世界は、通信サービスの契約プロセスを大きく変革するものとして注目されています。

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います。今後も、お客様の企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けていきます。

島上 純一(しまがみ じゅんいち)
IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

メッセージングテクノロジー

1.1 はじめに

これまでIIRでは、迷惑メールの量的な傾向やその内容について報告してきましたが、前回のIIR Vol.39でも述べたとおり、今回からは迷惑メールの対策技術も含めた、メッセージングにおける技術の解説や普及状況についてよりフォーカスしていきます。

今回は、送信ドメイン認証技術、特にDMARCの普及状況についての調査結果と、昨年に仕様がRFCとなった、メールの配送経路の暗号化技術であるTLSの接続ポリシーに関するMTA-STS、更に、そのレポーティング機能であるSMTP TLS Reportingについて解説します。また、メッセージングに関連する情報として、昨年開催されたJPAAWG 1st General Meeting / 迷惑メール対策カンファレンスと、JPAAWGについても報告します。

1.2 なりすましメールと情報漏えい

メールの送信者になりすまして送られるメールは、フィッシングメールやBEC（Business Email compromise）など、事例として名称が付けられるほど、様々な問題を引き起こす要因となっています。これらなりすましメールによる被害は、金銭的な被害や各種IDやパスワードの搾取、マルウェア感染などによって生じる機密情報や個人情報の漏えいなど、被る被害も深刻かつ多岐に渡っています。

最近では、こうした事象に拍車をかけるような事案も発生しています。様々なWebサービスからの情報漏えいが立て続けに発生しており、これら漏えいする情報の中には、メールアドレスが含まれていることがほとんどで、多くの迷惑メールが的確に送信されるようになりました。昨年も大手ホテルチェーンから大量の個人データが漏えいしたとのニュースがあり、それ以降漏えいしたメールアドレス宛てに多くの迷惑メールが送られるようになりました。その中には、親切にもログイン時に設定したパスワードを教えてくれるものもあります。Web経由で利用できるサービスは便利な側面がありますが、それを提供している側のセキュリティについては、必ずしも信頼できるものばかりとは限りません。Webサービスで設定するパスワードなどの強度や共通で設定している利用サービスの種類については、利用する側でもきちんと把握しておくことが必要です。

1.3 送信ドメイン認証技術の普及状況

なりすましメール対策には、送信ドメイン認証技術が有効であることはこれまでも述べてきました。メール受信側としてなりすましメールを検知するための認証処理と、メール送信側としてなりすましメールと区別できるようにするためのいくつかの設定が、送受信双方で必要です。

送信ドメイン認証技術を普及させるには、まず現在の普及状況を認識することが必要です。ここで、メール受信側から見た流

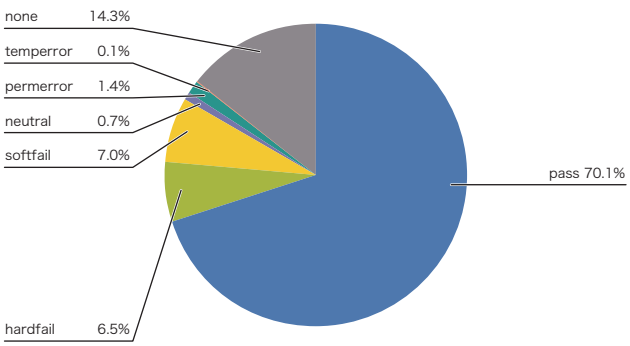


図-1 SPFの認証結果割合

量ベースでの送信側の普及状況と、登録ドメイン名に対する導入割合について、それぞれ調査結果を報告します。

1.3.1 流量ベースでの普及率

ここでは、メール受信側から見た送信側の設定の普及状況を、IIJのメールサービスで2019年4月に受信したメールの認証結果を示して解説します。

図-1は、SPFの認証結果の割合を示したグラフです。受信メール全体のうち、SPFでの認証結果が「none」であった割合は14.3%でした。「none」はSPF認証できなかったことを示す結果ですので、逆に言えば受信したメールの85.7%はSPFを導入した送信者からのメールだと言えます。昨年の同時期（2018年4月）の「none」の割合は16.0%でしたので、ほぼ同レベルで受信メールの大部分がSPF認証が可能なレベルまで普及してきた、と言えます。

図-2は、DKIMの認証結果の割合を示したグラフです。こちらも同様に認証結果「none」の割合は62.2%でしたので、受信メールのうち送信側がDKIMを導入している割合は4割未満ということになります。昨年同時期の認証結果「none」の割合は64.2%でしたので、DKIMの導入割合もそれほど大きな変化はなかったと言えます。

図-3は、DMARCの認証結果の割合を示したグラフです。同様に認証結果「none」の割合は76.9%でしたので、受信メールのうち送信側がDMARCを導入しているドメイン名の割合は、2割程度ということになります。DMARCはSPFあるいはDKIMの認証結果を利用して認証する技術ですので、SPFやDKIMより認証割合が低くなることは予想できます。しかしながら、メール再配送の課題はありますが、SPFだけでもDMARC認証はできますので、SPFの普及率が8割強だったのと比べれば、あまりにも低い割合です。

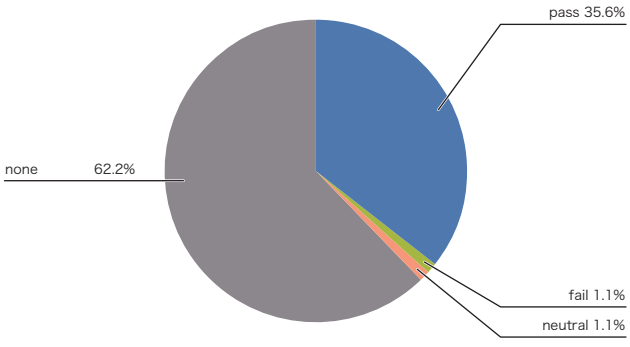


図-2 DKIMの認証結果割合

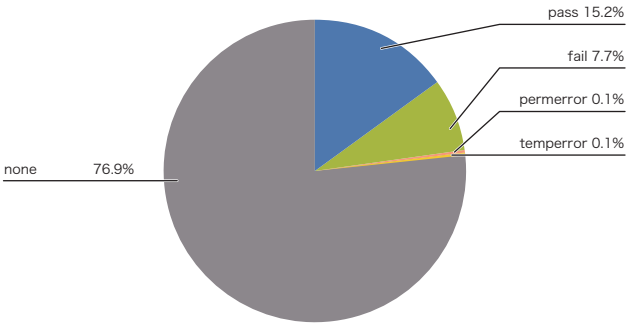


図-3 DMARCの認証結果割合

このDMARCの調査結果について、2016年1月からの推移を図-4に示します。調査当初は、DMARCの認証結果「none」の割合は87.5%でしたので、ほぼ3年間で流量ベースでの導入割合が1割程度増えたことになります。比率ではおおむね倍増しました。グラフ上でも、認証失敗を示す「fail」の割合の変化は時期によって変わりますが、認証失敗も含め全体として認証できているメールの割合は少しずつ増えていることが分かります。

1.3.2 登録ドメイン名ベースでの普及率

次に、登録されているjpドメイン名の中で、SPFあるいはDMARCを導入しているドメイン名の調査結果を示します。前回(Vol.39)でも述べたとおり、jpドメイン名を管理する日本レジストリサービス(JPRS)と(一財)日本データ通信協会は、送信ドメイン認証技術の普及状況調査を目的として共同研究契約を結んでおり、筆者は日本データ通信協会の客員研究員の立場で普及状況を調査しています。

2018年3月からの調査結果の推移を図-5に示します。調査結果は、jpドメイン名の登録種別ごとに、メールに利用しているドメイン名であることを示すMXレコードが設定されているドメイン名に対して、DMARCレコードが設定されている割合の推移を示しています。jpドメイン名全体では、5月の最新調査では、0.95%という結果となりました。登録種別では、ad.jpドメインが最も高い割合となっていますが、それでも3.4%です。次に割合が高いのが、種別ごととしては登録数が少ないため、段階的に増加しているgo.jpドメインで2.1%でした。

NISC(内閣サイバーセキュリティセンター)が公表している資料[*1]では、政府機関などの情報セキュリティ対策のための対策事項の中で、メールのなりすましの防止策として、SPF、DKIM、DMARCの送信側及び受信側の対策を行うこと、と示されています。よって、今後go.jpドメイン名でのDMARCレコードの設定割合が増えていくことが期待されます。なお、

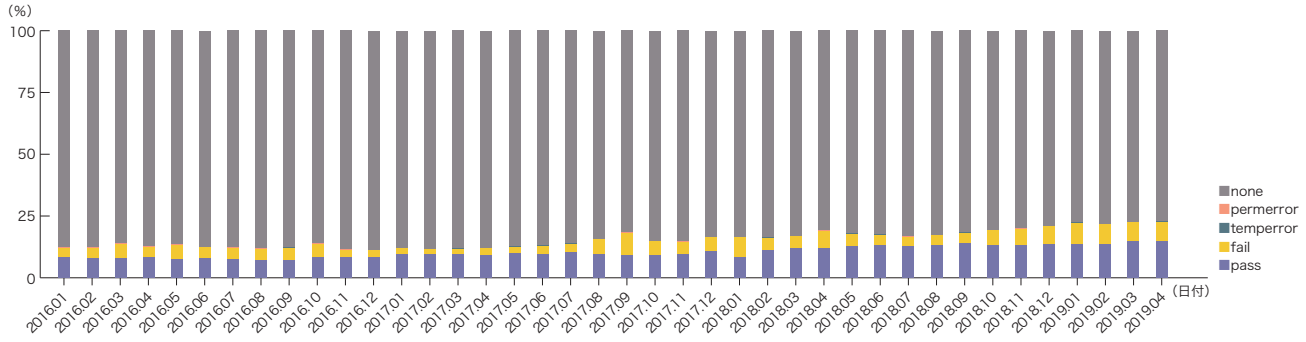


図-4 DMARCの認証結果割合の推移

*1 「政府機関等の対策基準策定のためのガイドライン(平成30年度版)」(https://www.nisc.go.jp/active/general/pdf/guide30.pdf)。

SPFレコードの設定割合では、go.jpは登録種別の中では最も高く、92.7%でした(図-6)。

同様に、jpドメイン名全体でのSPFレコードの設定割合は59.7%でした。前回(Vol.39)報告した、2018年1月時点の56.9%から2.8%増加したことになります。SPFの設定割合が未だ増加しているということは、SPFの認知度がかなり高くなっているものと考えられます。残念ながらDMARCの増加率はSPFよりかなり低い数値です。DMARCの認知度をより高める工夫が必要です。

1.3.3 海外の普及率について

米国に本社があるValimail社の調査[*2]によれば、米国連邦政府のドメインの80%がDMARCレコードを設定しているとのことです。これは、調査している各業界の中でも最も高い割合でした。前回も報告したとおり、米国国土安全保障省による法的拘束力のある命令[*3]により増加したものと考えられます。また、DMARC技術を推進する団体dmarc.orgによれば[*4]、DNSにDMARCレコードを設定しているドメイン名が、2018年で2.5倍以上に増えたことが報告されています。

1.4 メールの配送経路の暗号化

今やメールは単なるメッセージ交換だけではなく、添付ファイルの機能(MIME)により様々なデータの転送の手段にも用いられています。その一方で、データを含むメールがどのような配送経路で送られるのか、またデータが漏えいする危険性がどの程度あるのかなど、利用者側からはあまり考慮されていないようにも思えます。メール配送のプロトコル、SMTPでは拡張機能としてTLS(STARTTLS)が利用できます。ここでは、こうした従来のSTARTTLSの課題と、それを解決するための手段として規格が設けられたMTA-STS、SMTP TLS Reportingについて解説します。

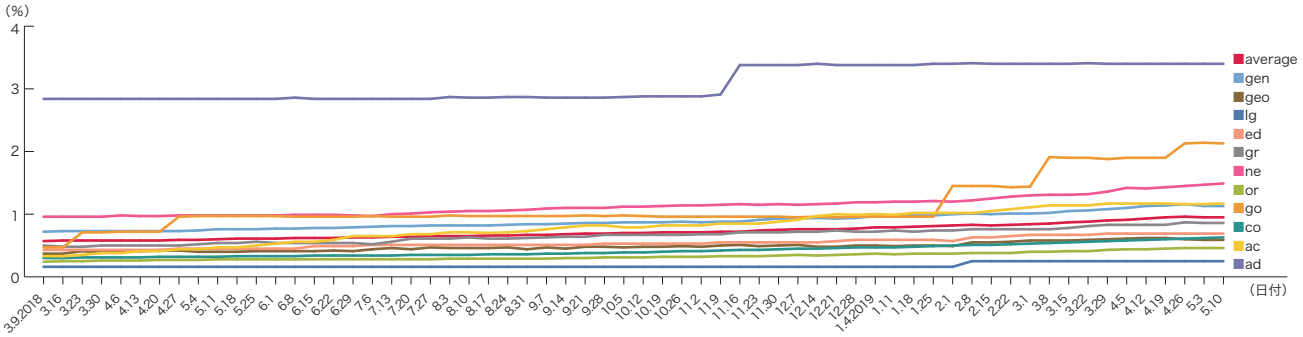


図-5 jpドメインのDMARCレコード設定割合の推移

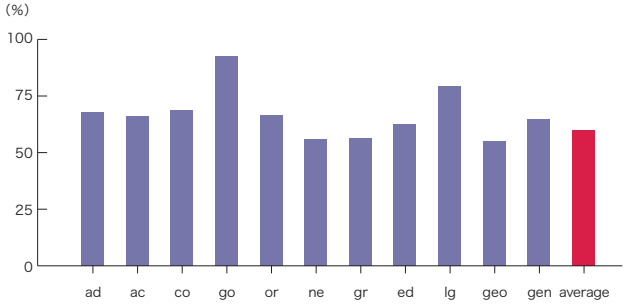


図-6 ドメインのSPFレコード宣言割合

*2 Email Fraud Landscape, Q4 2018 (https://www.valimail.com/resources/email-fraud-landscape-q4-2018/)。
*3 DHS, "Binding Operational Directive 18-01" (https://cyber.dhs.gov/bod/18-01/blank)。
*4 DMARC Policies Up 250% In 2018 (https://dmarc.org/2019/02/dmarc-policies-up-250-in-2018/)。

1.4.1 STARTTLSの課題

メール配送時の通信経路を暗号化するには、SMTPの拡張機能であるSTARTTLS（TLS）を利用します。手順としては、受信メールサーバ側がSTARTTLSに対応している場合（接続時の応答で判断できます）、送信側がSTARTTLSコマンドを送信することで、TLSセッションが開始されます。そのため、以下のような条件では、通信経路の暗号化ができなくなってしまいます。

- **受信メールサーバがSTARTTLSの機能を持っていない（STARTTLSに対応した応答メッセージを返さない）**
- **STARTTLSのコマンドを送信し、TLSセッションを開始しようとしたが、利用できるTLSのバージョンやCipher Suitesが合わなかった**

Cipher Suitesは、暗号化のためのアルゴリズムや鍵長などの組み合わせを示したもので、送受信側双方で同じものを利用できなければ暗号化通信は行えません。こうしたSTARTTLSコマンドが実行できない場合、多くの送信メールサーバは、暗号化せずに従来の平文によるメール送信の手順に移行します。このような仕組みでは、いわゆる中間者攻撃のように、SMTPセッションを仲立ちし、本来の受信サーバのSTARTTLSに関する応答を削除することで、平文による送信を行わせることで、メールの内容を搾取することが可能になります。こうした手法は、ダウングレード攻撃とも呼ばれます。

1.4.2 MTA-STSとTLSRPT

MTA-STS[*5]は、メール受信側のドメインが、DNSとHTTPSを利用して、受信側のポリシーを表明する仕組みです。この仕組みを利用することで、メール送信前にTLS認証をサポートしているか、TLS接続がうまくいかなった場合に送信側が取るべき動作を知ることができます。

受信側のドメインが用意すべき設定は、以下のとおりです。

（1）MTA-STSレコードを設定
（2）MTA-STSポリシーを取得できるようwell-knownパスに設定

MTA-STSレコードは、通常はメールの宛先ドメインに"_mta-sts"をつけたドメインのTXTレコードであって、先頭が"v=STSv1"であるものです。例えば、メールの宛先ドメインが"example.com"である場合、以下のように設定されることになります。

```
_mta-sts.example.com.  IN TXT "v=STSv1; id=20160831085700Z;"
```

idパラメータは、ポリシーの変更時に把握できるよう設定する文字列です。送信側は、まずこのMTA-STSレコードを参照することで、受信側ドメインがMTA-STSに対応しているかどうかを確認することができます。

*5　SMTP MTA Strict Transport Security, RFC8461

次に、MTA-STSポリシーを取得する方法です。対象のドメインに"mta-sts"を付けたポリシードメインのwell-knownパスを参照します。well-knownパスは、RFC5785で示されていますが、MTA-STSの場合、以下のパスに対してHTTPSのGETメソッドで取得します。

```
https://mta-sts.example.com/.well-known/mta-sts.txt
```

MTA-STSポリシーは、key/valueペアを改行(CRLF)で区切った形式で、現在指定可能なパラメータを表-1に示します。

"max_age"は、ポリシー参照する側がキャッシュしておく期間を示します。"mx"は、MXレコードで設定されるホスト名のパターンを指定します。複数のホストあるいはパターンを設定可能です。動作モード("mode")で設定できる値を表-2に示します。これらのモードにより、送信側のMTAは送信を続けるべきかどうかを判断します。

MTA-STSポリシーの設定例を以下に示します。

```
version: STSv1
mode: enforce
mx: mail.example.com
mx: *.example.net
mx: backupmx.example.com
max_age: 604800
```

MTA-STSでのポリシー検証が失敗した場合や成功した場合、またそれ以外のDANE[*7]などの仕組みで、送信側にレポートを送るための仕様がTLSRPT[*6]です。送信側は、レポートを受け取るために、DNSを利用してTLSRPTポリシーを表明します。TLSRPTに対応したメール受信側は、まず送信側のドメインでこのTLSRPTポリシーが設定されているかどうかを判断し、取得できた場合でレポート先が指定されている場合にレポートを送信することになります。TLSRPTポリシーの設定は、対象のドメイン名に"_smtp._tls"を追加したドメイン名となります。設定するパラメータは、DMARC[*8]によく似ていますが、最初のバージョン情報が"v=TLSRPTv1"であること、レポート先を示す"rua="にメール("rua=mailto:")以外にHTTPS ("rua=https:")も利用できること、が異なります。以下にTLSRPTポリシーレコードの設定例を示します。

```
_smtp._tls.example.com. IN TXT "v=TLSRPTv1;rua=mailto:reports@example.com"
```

メールで、"rua=mailto:"で指定された宛先にレポートを送る場合は、送信側のドメインでDKIM署名されている必要があります。このDKIM署名する送信側のDKIMレコードには、サービスタイプを示す"s=tlsrpt"が設定されているべき(SHOULD)となっています。

表-1 MTA-STSポリシー

パラメータ	意味
version	バージョン(値はSTSv1)
mode	ポリシー検証が失敗した場合の送信側の動作
max_age	ポリシーの存続期間(秒)
mx	MXレコードのパターン

表-2 MTA-STSポリシーモード

動作モード	意味
enforce	ポリシー検証やTLSが失敗した場合に配送してはならない
testing	送信側のMTAがTLSRPT[*6]を実装している場合レポート送信し、メール送信を継続
none	明示的にMTA-STSポリシーを適用しないことを示す

*6 SMTP TLS Reporting, RFC8460
*7 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC6698
*8 Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489

```
selector._domainkey.example.com  IN TXT
      "v=DKIM1; k=rsa; s=tlsrpt; p=MIf4qwSZfase4fa=="
```

メールで送信する場合、DMARCレポートと同様に、添付ファイル形式(MIME)で送信します。同様にHTTPSでレポートを送信してもらうためのTLSRPTポリシーレコードの例を、以下に示します。

```
_smtp._tls.example.com.  IN  TXT  "v=TLSRPTv1;  rua=https://report-
ing.example.com/v1/tlsrpt"
```

レポートデータは、メールあるいはHTTPSの両方の場合で、圧縮形式で送るべき(SHOULD)となっています。圧縮あるいは圧縮しない場合でも、メディアタイプは実体に即した形で指定します("application/tlsrpt+gzip"あるいは"application/tlsrpt+json")レポートデータの形式は、DMARCレポートとは異なり、JSON形式となっています。データに含まれるパラメータについては、ここでは省略しますが、詳細はRFC8460を参照してください。

1.5 JPAAWG について

これまで、国際的な迷惑メール対策組織であるM^{3}AAWG[*9]について、IIRでも何度か触れてきました。最近ではメール以外にも、より関連するセキュリティ分野も含めて、様々な議論や検討を行う場となっています。また最近では、M^{3}AAWGメンバーの多い北米や欧州だけでなく、他の地域とも連携していくために、各地で地域的な組織の立ち上げも支援しています。最初に立ち上がったのが、南米及びカリブ地区によるLAC-AAWGです。同様にアフリカ地域でのAFR-AAWGについても検討及びサポートを行っています。となると、次に残された地域のアジアをどうするか、ということになります。

M^{3}AAWGでは、その設立時からIIJがメンバーとして長年活動してきましたが、日本からの参加メンバーが欧米に比べて

*9　Messaging, Malware and Mobile Anti-Abuse Working Group

なかなか増えない状況が続いてきました。我々も参加者をより増やすために、M³AAWGの活動を日本で紹介したり、時々M³AAWG General Meetingを日本あるいはアジア地域で開催できないかなどと打診してきました。そうした中、LAC-AAWGのように、M³AAWGと連携した各地域の活動をM³AAWGが支援する動きが出てきました。こうした動きの中で、M³AAWGと日本から参加しているメンバーとの間で、JPAAWGを設立しようと動き出すことになりました。

JPAAWG（Japan Anti-Abuse Working Group）は、あくまでM³AAWGとは独立した組織ですが、M³AAWG側から多くの支援を得ています。昨年2018年11月8日に開催されたJPAAWG 1st General Meetingは、これまで10年以上開催してきた（一財）インターネット協会の迷惑メール対策カンファレンスと併催する形で、多くの講演者及び参加者を集めました。講演者にはM³AAWGのチェア及び主要メンバーも加わりました。このイベントの成功もあり、JPAAWGは継続して活動できるための準備をいくつか行い、2019年5月30日にようやくJPAAWGとして設立することができました。今後のJPAAWGの活動に関心を持っていただければと考えています。

1.6 おわりに

今回は、メール配送の暗号化を確実に実施するための技術仕様MTA-STSと実施状況を把握するためのTLSRPTについて解説しました。これまでも、送信ドメイン認証技術DAMRC やARC、DANEなどについて紹介や技術解説してきましたが、メールに関連する技術仕様は、BIMI（Brand Indicators for Message Identification）やJMAP（JSON Meta Application Protocol）など、新たな仕様とともに進化しています。IIRでは、これからも新しい技術仕様や、そうした仕様が生まれる背景なども含めて解説していきます。

執筆者：
櫻庭 秀次（さくらば しゅうじ）
IIJ ネットワーク本部 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。M³AAWG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 迷惑メール対策委員会 委員長。Email Security Conferenceプログラム委員。一般財団法人日本データ通信協会 客員研究員。一般財団法人日本情報経済社会推進協会（JIPDEC）客員研究員。

ブロックチェーン技術をベースとした アイデンティティ管理・流通の動向

2.1 はじめに

ブロックチェーン技術をベースにした様々なサービスが毎日のように報道されています。その中には単なる分散データベースとしてブロックチェーンを用いる残念な提案も多く、本当にそこにブロックチェーンは必要なのかを自己確認できるフローチャートが複数発表されるほどです[*1]。ブロックチェーンにはいくつかの分類方法があり、大きく分けてプライベートで用いられるものと、いわゆる暗号資産の安全性の裏付けとなるパブリックなものがあります。後者のパブリックブロックチェーンではマイニングしてチェーンを繋げ続けることにインセンティブを持たせる必要があり、Bitcoinなどの暗号資産では、定められたルールに基づきチェーンを伸ばしていく必要があります。暗号資産で用いられるブロックチェーンはあるアドレスからあるアドレスへの資産の移動に用いられることが大きな目的ですが、このブロックチェーンにおける価値移動の基盤を用いてその用途以外に使おうとする動きが見られ、セカンドレイヤーまたはレイヤー２といった用語で呼ばれています。

本稿は、Ethereumブロックチェーン[*2]におけるセカンドレイヤーにあたるサービスのうちクレデンシャル(アイデンティティ情報)に用いられるERC(Ethereum Improvement Proposals)[*3]提案の動きを取り上げます。更にこうしたクレデンシャルがブロックチェーンに格納され、在籍証明などの公的な証明書をデジタル空間で確認できるユースケースについて触れます。最後に、ここ数ヵ月で複数のベンダーやコンソーシアムが非中央集権型の識別子であるDIDs(Decentralized Identifiers)やアイデンティティ管理をユーザ自らがコントロールするSSI(Self Sovereign Identity)などの概念を提示している背景とブロックチェーンをベースとしたクレデンシャル管理技術が注目されていることを示します。

2.2 識別子としてのIDとクレデンシャルの整理

2015年発行のフォーカスリサーチにおいて、当時のID管理技術の動向について報告しています[*4][*5][*6]。本稿ではIDを識別子(Identifier)という狭義の意味と捉えて説明を行います。

現実世界の実体はデジタル世界のエンティティと結び付けられ、デジタル世界のエンティティを識別(identify)するために、ユニークな識別子(Identifier＝ID)が割り当てられます。識別子としてのIDと、そのIDに紐付けられるあらゆるアイデンティティ情報は別に考える必要があります。更にID空間はそれぞれのレルム(IDが有効で識別可能な範囲)が別途定められていることから、リアルワールドに唯一存在するエンティティに対して同じレルムでも複数のIDを持つこともあります。

次にデジタル空間においてなぜIDが付与されるのかを考えると、そのエンティティであることをネットワーク上の第三者に認識してもらう必要があるためです。デジタル世界におけるあらゆるアクティビティには認証という行為が伴います。認証行為によりリソースにアクセスできるようになったり、各種サービスを受けられたりするようになります。

この認証行為では、秘密情報であるトークンと公開情報であるクレデンシャルの組を用いる、という整理を行うことができます。NIST SP800-63の定義に従うと、トークンは当該IDが割り当てられたユーザが持つ秘密にすべき情報を指し、クレデンシャルはIDと紐付けられるあらゆる種類の属性情報を意味します。クレデンシャルは暗号技術を用いて内容の完全性が保証されます。当該IDを持つエンティティがデジタル世界で自分の属性情報を第三者に確認してもらう際に、秘密情報であるトークンで当該IDを持つエンティティが割り当てられたエンティティであることを確認してもらうことができます。

＊1　NISTIR 8202、"Blockchain Technology Overview"(https://doi.org/10.6028/NIST.IR.8202) Figure 6 - DHS Science & Technology Directorate Flowchartにフローチャートが記載されている。
＊2　Ethereum Project、Developer Resources(https://www.ethereum.org/developers/)。Ethereumの大きな特徴であるスマートコントラクトに関連する関連技術については本稿では取り上げません。
＊3　Ethereum Improvement Proposals(http://eips.ethereum.org/)。
＊4　Internet Infrastructure Review Vol.26「1.4.3 ID管理技術」(https://www.iij.ad.jp/dev/report/iir/026/01_04.html)。
＊5　Internet Infrastructure Review Vol.27「1.4.2 ID管理技術～利便性と安全性の観点から～」(https://www.iij.ad.jp/dev/report/iir/027/01_04.html)。
＊6　Internet Infrastructure Review Vol.28「1.4.3 ID管理技術～オンライン認証にパスワードを使わない方法へ～」(https://www.iij.ad.jp/dev/report/iir/028/01_04.html)。

認証行為と共にクレデンシャルが提示されたときに、それを受け取った第三者は、当該IDがどのようなエンティティであるのかをクレデンシャルに書かれている属性情報で確認することができます。このようにして認証に加えて認可(Authorization)のためにクレデンシャルが利用されるケースもあります。X.509証明書は単一もしくは複数のIDに公開鍵を紐付けることからクレデンシャルの1例です。実際にSSL/TLSクライアント認証がそれにあたります。ブラウザ側に個人のX.509証明書を配備した上でサーバにログインすることができ、法人向けのオンラインバンキングなどで利用されています。よりクレデンシャルとしての利用形態に近い方法として、X.509属性証明書(Attribute certificate)[*7]と呼ばれる仕様が存在しています。属性証明書は通常のX.509証明書と異なり公開鍵を内包していません。*holder*と呼ばれる識別子を格納するエリアに証明書を同定するためのシリアル番号を入れ、当該X.509証明書を指定した上で証明書のホルダー(subject)と紐付ける属性情報を格納するという形式を持っています。これは、レルムがCAの発行する証明書群、IDはシリアル番号、クレデンシャルが属性証明書、という関係を持っていると理解できます。X.509属性証明書はクレデンシャルを書くことができる一方で、実際にブラウザなどの一般ユーザが触れるアプリケーションにおいて実装されることはなく、現在利用されている事例はほとんど見られません。

2.3 ERC-725の概要

ERC-725[*8]はERC-20トークン標準の策定やweb3.jsの開発者として知られるエンジニアであるFabian Vogelsteller氏[*9]が2017年10月に提案しました。ERC(Ethereum Improvement Proposals)はIETFのRFCのように、誰でも提案できる改善型のドキュメントでERC-1に書式や書くにあたっての指針などが掲載されています。大きな特徴としては、とにかくコンパクトに書くことが求められていることが挙げられます。同様の文書群としてはBitcoinのコミュニティにおいてもBIP(Bitcoin Improvement Proposals)[*10]として知られているドキュメント群があり、例えばSegWitとして知られるトランザクションデータの削減方式はBIP-141で規定されています。

電子契約の締結とサービスの実行を自動的に行う方式として知られるスマートコントラクトは、1997年にNick Szaboによって提案された新しい概念であり、Bitcoinが登場する前から存在していました。スマートコントラクトの例として、自動販売機の例がよく取り上げられています。「ユーザが購入したいジュースの代金を自販機に投入する」と「その後購入したいジュースのボタンを押す」という2つのプロセスが、両者ともある一定の条件を満たすと自動的に販売が開始されるという例です。Ethereumは暗号資産としての側面だけでなく、スマートコントラクトを作成し実行することができるため分散アプリケーションのプラットフォームであるとされています[*11]。ERC-725はプロキシアカウントのふるまいに関して分散アプリケーションを記述する言語の1つであるSolidityのインターフェースを定義しています。ERC-725からはERC-735[*12]とERC-780[*13]が参照されており、これらの仕様に基づきEthereumブロックチェーン上でクレデンシャルを流通させる仕組みを提供します。ERC-725の文脈においては、クレデンシャルはClaimと呼ばれます。ERC-735はClaimのフォーマットが、ERC-780はCliamのレジストリであるEthereum Claims Registry(ECR)に関する仕様が記載されています。Ethereumブロックチェーンというレルムにおいて ID(識別子)はEthereumアドレス(コントラクトアドレスではない点に注意)でありClaimと呼ば

*7 RFC 5755、"An Internet Attribute Certificate Profile for Authorization"(https://datatracker.ietf.org/doc/rfc5755/)。
*8 ERC-725 version2:Proxy Account(https://github.com/ethereum/EIPs/issues/725)(http://eips.ethereum.org/EIPS/eip-725)。
*9 Fabian Vogelsteller(http://frozeman.de/blog/)。
*10 BIP(Bitcoin Improvement Proposals)(https://github.com/bitcoin/bips)。
*11 Ethereum Project、White paper(https://github.com/ethereum/wiki/wiki/White-Paper)。
*12 ERC-735、Claim Holder(https://github.com/ethereum/EIPs/issues/735)。
*13 ERC-780、Ethereum Claims Registry(https://github.com/ethereum/EIPs/issues/780)。

れるクレデンシャルによって、あるアドレスに紐付けられるIdentity Holder（ホルダー）のアイデンティティ情報が保証されるという仕組みが規定されています。Claimを発行するClaim Issuer（認定者）は自身の持つ秘密鍵を用いて任意のEthereumブロックチェーン上のエンティティに対してClaimを発行することができます。Identity Holderは検証対象となるClaimを何らかの方法でClaim Checker（価値判断者）に受け渡し、価値判断者はデジタル署名を確認することでClaimの確からしさを確認することができます。これらの一連の検証作業はオンライン・オフラインの両方で実行できることが想定されています[*14]。

ERC-735で規定されるClaimの形式は以下のようにシンプルなデータ構造をしています。

```
struct Claim {
    uint256 topic;
    uint256 scheme;
    address issuer;
    bytes signature;
    bytes data;
    string uri;
}
```

表-1 ERC-735 Claimの各構成要素

topic	現在未定義。形式は256ビット空間でClaimの種別に関する情報が入る見込み。例としてバイオメトリクス情報や住居情報が記載されています。
scheme	現在未定義。形式は256ビット空間で、別途定義されるであろうスキーマに基づいた処理方法や署名アルゴリズムを格納します。
issuer	コントラクトアドレスもしくは署名に用いられた鍵に呼応したEthereumアドレス。
signature	署名データ。被署名対象エリアは{アイデンティティ情報の保持者であるIdentity HolderのEthereumアドレス、topic、data}のみという点に注意です。
data	アイデンティティ情報のハッシュ値。アイデンティティ情報そのものを記載しないため機微情報をそのままブロックチェーンに載せるわけではありません。
uri	アイデンティティ情報を指し示すURI。HTTPリンクやIPFSのURIが想定されています。

ERC-735 ClaimはIdentity Holder自身で価値判断者に提示することができるように実装されるべきであり、データとして可搬性を持つ点が大きな特徴となります。ERC-735ではToBeSigned（改ざん防止対象）ではないエリアにURIを記載するゾーンが設けられており、ここにアイデンティティ情報を指し示すデータを分散ファイルシステムであるIPFS[*15]などで共有します。ERC725 Alliance[*16]ではERC-725に関連するオープンソースプロジェクトが存在しています[*17]。また、この参照実装を使って構築されたサイト[*18]ではいくつかのサンプルが参照でき、ブラウザ上でClaimの確からしさを検証できるようになっています。また、自分で自分のアイデンティティ情報に署名してオレオレClaimを発行可能な仕様は特筆すべき点です。

このようにERC-725フレームワークではClaimを誰でも発行できる、つまりClaim Issuerは誰でもなれるためEthereumアドレスさえ分かれば誰にでもClaimを発行することができます。そのためClaim Issuerをどのように信頼して、そのIssuerから発行されたClaimを価値判断するかについては大きな課題

＊14 Fabian Vogelsteller、ERC Identity（https://www.slideshare.net/FabianVogelsteller/erc-725-identity）。
＊15 IPFS（InterPlanetary File System）（https://ipfs-book.decentralized-web.jp/what_is_ipfs/）。
＊16 ERC725 Alliance（https://erc725alliance.org/）。
＊17 ERC725 Alliance、"Repository for code and discussion around ERC725 and related standards"（https://github.com/ERC725Alliance/erc725/tree/master/contracts/contracts）。
＊18 ERC 725 Demo implementation by Origin Protocol, Inc.（https://erc725.originprotocol.com/）。Origin Protocol, Inc.,（https://www.originprotocol.com/）。

です。またCliamの失効やEthereumアドレスの付け替えなどの機能もあるとされていますが、まだ仕様としては不完全な状況です。Issuerの評価(レピュテーション)の仕組みについても議論が始まったばかりという状況のように見受けられます。

このように現在はレピュテーションの問題をはらんでおり、最終的にうまくClaimを流通させていくためにはいくつかの段階を踏むことになるでしょう。筆者は以下の3ステップで徐々に「Claimの考え方」が浸透していくと予想しています。第1段階はSNSなどの閉じたネットワークで知り合い同士で投げ銭として気軽にClaimを発行し、スケーラビリティを確認するフェーズです。次の段階では既存のユーザ評価・通報システムを活用して誤ったClaimを発行したIssuerかどうかをランク付けする仕組みが整い、最終的には完全に分散・自動化されたレピュテーションシステムへと昇華していくと考えられます(図-1)。

ERC-725と同様に可搬性を持つClaimの例としてはBlockcerts[*19]によるプロジェクトがあり、オープンソース[*20]や検証デモ[*21]を参照することができます。BlockcertsはMIT Media LabとLearning Machine社で作製されたプロトタイプがベースとなっています。BlockcertsではBitcoinやEthereumを含む複数の種類のブロックチェーンでも実装可能なように拡張が続けられています。スマートフォンアプリであるBlockcerts Walletも実装・公開されており、MITでは学位証明書がBlockcertsの仕組みを利用してブロックチェーンに書き込まれています[*22]。この他にもスペインの大学においては学位証明書を発行する際にSmartDegreesプラットフォームを利用してEthereumブロックチェーン上で管理することが発表されています[*23]。このようにセカンドレイヤーのプラットフォームは複数存在するなど現在はまだ混沌とした状況のため、プラットフォームの選択においては事業継続性を鑑みて選択する必要があるでしょう。

ここまで説明したように、Claimは単純な仕組みながら、Issuerが信頼でき、かつセカンドレイヤーの仕様が正しく運営されていれば、Ethereumブロックチェーンの信頼性が崩れない限りは半永久的に利用することができると認識されてい

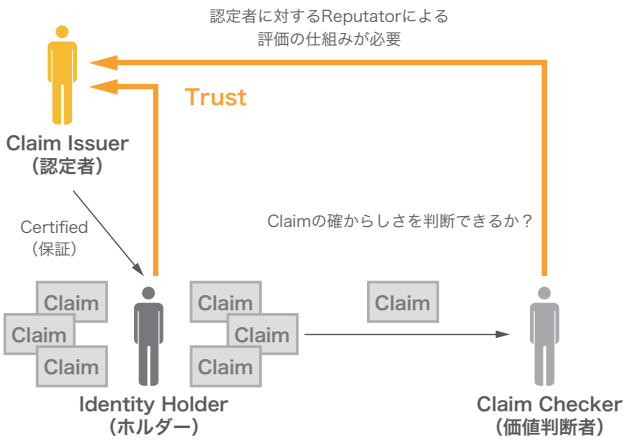


図-1 Claim発行とClaim価値判断の仕組み

＊19 Blockcerts(https://www.blockcerts.org/)。
＊20 Repositories of Blockcerts project(https://github.com/blockchain-certificates)。
＊21 Example Blockcerts(https://www.learningmachine.com/new-product/examples/)。
＊22 MIT News、Digital Diploma debuts at MIT(http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017)。
＊23 Universidad Carlos III de Madrid is issuing degree certificates with blockchain(https://www.uc3m.es/ss/Satellite/UC3MInstitucional/en/Detalle/Comunicacion_C/1371252827656/1371215537949/Universidad_Carlos_III_de_Madrid_is_issuing_degree_certificates_with_blockchain)。

ます。そのためブロックチェーン技術をうまく活用する事例として学位証明書のデジタル発行は適しているアプリケーションの1つであると考えられ、実際に国内でサービスインした事例もあります。昨今の地方私大の閉校や地方自治体による検定試験の終了など、かつて信頼できた組織であっても未来永劫運営されているとは限りません。そしてそこから発行された物理的な証書が保証できなくなってしまった事例もあります。現物の証書を代替する手段として今回紹介したオープンな仕組みでClaimが流通する時代が来ることが望まれます。

2.4 非中央集権型識別子DIDs

識別子としてのIDはある特定のレルムの中でアサインされます。レルムを超えて認証する際にはID Federation（ID連携）という概念があり、シングルサインオンの文脈でしばしば登場します。先に挙げたX.509属性証明書やERC-735 Claimのようなクレデンシャルは、発行された特定のレルムでしか流通されません。IDを振り出す役目でもあるアイデンティティプロバイダは現実的には単独で存在せず、SNSなどのサービスプロバイダのログイン機能が外部サービスと連携できるようにするために機能分離してアイデンティティプロバイダとしての役割を担っているのが現状です。このとき、ID連携機能を用いて別のサービスにログインするようなケースにおいて、特定の企業や組織により運営されているがために当該IDが急遽使えなくなるリスクが存在します。これは1つのIDが利用停止されることにより、他の複数のサービスが利用できないことになりかねません。実際、あるSNSにおいて運営側が不適当な書き込みと判断されたケースで当該IDが利用停止、最悪のケースでは削除されることにより起きる弊害が散見されます。

このような背景から、非中央集権型識別子Decentralized Identifiers（DIDs）という概念が登場しています。ある特定のレルムだけで有効なIDではない点、そしてIDを一括管理する中央集権的な存在を持たないという特徴を持ちます。これは非営利団体であるSovrin Foundation[*24]で提唱された自己主権型アイデンティティSSI（Self Sovereign Identity）[*25]との親和性が高いと認識されています。SSIは自己情報コントロール権の考えとよく似ていて、管理当局を介さずに自分自身でアイデンティティ情報の所有と管理を行う必要があることを認識するために使用される用語です。先に挙げたERC-735 Claimなどのクレデンシャルは意図せずひとりでに流通してしまう可能性があります。そうではなく

＊24 The Sovrin Alliance（https://sovrin.org/library/rise-of-self-sovereign-identity/）。
＊25 The Sovrin Alliance、"A White Paper from the Sovrin Foundation: A Protocol and Token for SelfSovereign Identity and Decentralized Trust(Version 1.0 January 2018)"（https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf）。

自身のクレデンシャルの流通の主権をIdentity Holderが持とうという考え方です。

プライバシーを保護しポータブルでユーザ中心のアイデンティティ管理を実現しようとしている組織に非営利団体であるID2020 Alliance[*26]があります。また、国の発行する通貨の信頼が落ちているようなケースにおいて法定通貨ではなく暗号資産が利用されようとするのと同じく、パスポートの代替技術としてブロックチェーン上のClaimが活用できないかというプロジェクトが存在します[*27]。この考え方は皆が認め、そして信頼できる機関によって発行されたClaimに相当するデータがパスポートライクな本人確認手段を提供することと解釈できます。2015年に国連でまとめられた持続可能な開発目標(SDGs)[*28]の16.9節に記載のゴール目標には「2030年までに出生登録情報を含めすべての人に合法的なアイデンティティを提供する」と記載されています。10億を超えるとも言われるID難民を救うべくID2020技術的な機能要件[*29]がまとめられています。この要件書では、社会適用性、個人識別、認証、プライバシ管理、信頼性、相互運用性、リカバリの7カテゴリでまとめられており、この類いの設計指針としては非常に有用なドキュメントとなっています。

一方DIDはW3C[*30][*31]で策定された文書群からその意図を読み取ることができます。W3CではDIDを分散元帳技術(DLT;Distributed Ledger Technology)やその他の分散ネットワークに登録されており、中央集権的なオーソリティを必要としないグローバルに一意な識別子[*32]と定義しています。ERC-735 ClaimはEthereumアドレスをID空間として利用していましたが、そのままDIDとして利用せずにW3C DID形式でEthereumアドレスをWrapして記載する方法も提案されています[*33]。このようにW3C DIDは様々なIDを表記可能なグローバルIDとしての利用を推進していることが分かります。DIDの存在だけでは重複しないナンバリングしか解決しませんが、Claimのユースケース[*34]やVerifiable Credentials(当初Claimと表現されていましたがクレデンシャルという用語に変更されました)のデータフォーマット[*35]と連動して世の中を解決していくことになるでしょう。

2019年3月に開催されたWeb of Trust VIII(RWOT8)[*36]でのグループワーク、そして同年4月に開催されたthe 28th Internet Identity Workshop[*37]ではDIDやSSIを軸にしたトピックが多く取り上げられています。またIGF(Internet Governance Forum)でも今年のAnnual Meeting[*38]でDID

＊26 ID2020 Alliance、The Alliance Manifesto(https://id2020.org/manifesto)。
＊27 Taqanu(https://www.taqanu.com/impact)。
＊28 Transforming our world: the 2030 Agenda for Sustainable Development(https://sustainabledevelopment.un.org/post2015/transformingourworld)(https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E)。
＊29 ID2020 Technical Requirements: V1.0 (https://docs.google.com/document/d/1L0RhDq98xj4ieh5CuN-P3XerK6umKRTPWMS8Ckz6_J8/edit)。
＊30 W3C Credentials Community Group(https://www.w3.org/community/credentials/)。
＊31 W3C Verifiable Claims Working Group(https://www.w3.org/2017/vc/WG/)(https://github.com/w3c/verifiable-claims)。
＊32 Decentralized Identifiers (DIDs) (https://w3c-ccg.github.io/did-spec/#decentralized-identifiers-dids)。執筆時の最新版は2019年6月3日発行のv0.13。
＊33 eth DID Resolver(https://github.com/uport-project/eth-did-resolver)。
＊34 Verifiable Claims Use Cases(https://www.w3.org/TR/verifiable-claims-use-cases/)。
＊35 Verifiable Credentials Data Model 1.0(https://www.w3.org/TR/verifiable-claims-data-model/)。2019年3月が最終版。執筆時はW3C勧告候補。
＊36 Rebooting the Web of Trust VIII: Barcelona(March 2019)(https://github.com/WebOfTrustInfo/rwot8-barcelona)(https://www.weboftrust.info/pastevents.html)。
＊37 IIW(The Internet Identity Workshop)Workshop Proceedings(https://internetidentityworkshop.com/past-workshops/)。
＊38 IGF 2019 Workshop Selection Results(https://www.intgovforum.org/multilingual/content/igf-2019-workshop-selection-results)。

関連技術が取り上げられており、ガバナンスに関しても議論されていくことになります。今後も多くの人を巻き込んで議論が進んでいくものと考えられます。

2.5 関連したその他の動向

2019年5月にマイクロソフトはBitcoinブロックチェーンを基盤としたDIDを扱うプラットフォームを発表しました。5月15日、2つのブログ記事で今後の取り組みなどが示されています[*39][*40]。またDIDに関するホワイトペーパーも公開されました[*41]。これらの情報によると、ID空間としてはW3C DIDを利用しDecentralized Identity Foundation（DIF）[*42]で策定されているSidetree protocolが採用されていることが窺えます。このDIDシステムはBitcoinブロックチェーンのセカンドレイヤーでの実装であり、ION（Identity Overlay Network）[*43]と名付けられて既にソースコードも公開されています。

最後に信用スコアや情報銀行についても触れておきます。インターネット上でのアクティビティから信用スコアとして算出するサービスが国内でもサービスインされるとの報道もありました。GAFAやFAANGなどのビッグブラザーによる中央集権的な管理下での評価のみが正しいと判断され、自らのスコアが意図せず世の中に流通してしまうことが懸念されます。ここには昨今頻繁に議論されているAI技術などと同様に、評価制度だけでなく評価アルゴリズムの透明性を確保する必要があります。よく分からないロジックで、ある特定の地域に在住する方々や人種、宗教などに拠って不当な評価がなされることも理論的には起こり得ます。そのため倫理的な側面での配慮が必要となります。それは、ERC-735 Claimでの懸念点として述べたように現実世界のエンティティが行うレピュテーションの仕組みにも同じことが言えます。

このように現実世界のエンティティが、様々な手段で評価される時代になってしまいました。管理する側からすると安全保障のためにこれらの措置は必要であるかもしれませんが、やはりSSIの考え方に基づき自分で自分の機微情報を管理できることが求められています。特に、初めてDIDやClaimが発行されたIdentity Holderに様々な自衛を求めることは容易ではないかもしれませんが、デジタル時代に生きる我々には当然のリテラシーとして持っておくべき素養ではないかと考えます。

＊39 Microsoft Security Blog、"Decentralized identity and the path to digital privacy"（https://www.microsoft.com/security/blog/2019/05/15/decentralized-identity-digital-privacy/）。
＊40 Azure Active Directory Identity Blog、"Toward scalable decentralized identifier systems"（https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Toward-scalable-decentralized-identifier-systems/ba-p/560168）。
＊41 Microsoft Whitepaper、Decentralized Identity - Own and control your identity（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY）。
＊42 Decentralized Identity Foundation（DIF）（https://identity.foundation/）（https://github.com/decentralized-identity/）。
＊43 ION（Identity Overlay Network）（https://github.com/decentralized-identity/ion/）。

自分が他界した後は、SNSのアカウントを子供や孫に受け渡そうと考える方もいらっしゃいますが、事業継続性の観点からはあまりお勧めできない状況になりつつあります。やはりここでもAI技術の発展により、書き込み内容の検閲によりアカウント自体を一時的もしくは永久的に無効にする措置が大きく影響します。これらの身近な事例も、DIDとその周辺技術のサービス提供が早急に実現するよう望まれている要因であると筆者は考えます。

大規模な統計情報を扱う際の仮名IDの取り扱いに関してや、クレデンシャルそのものを暗号化してアクセスコントロールするケースなどに関してはまだ議論が十分になされていない段階にあるように思います。バックグラウンドとなる技術が整合性を持っており、うまくディプロイできれば社会的適合性を持つ、という理由だけで、その技術が実際に世の中に浸透できなかった事例はこれまでにも多く目にしてきました。今回紹介した技術群がユーザに身近なアプリケーションにディプロイされ世の中の役に立つのかどうかは、現時点では分かりません。

情報銀行などのリアルなユースケースが出てくることによって、実社会におけるエンティティに結びつく各種情報(機微情報も含む)を、インターネットを介して流通させる仕組みの利便性が認識されるようになりました。しかしここには大きな問題があります。EUが定めるGDPRなどのプライバシー情報管理を定める規制はEU諸国に限ったことではなく、日本を含む世界各国においてもその規制を受けることになりました。そのため今回紹介する技術はブロックチェーンを用いることから、クレデンシャルが流通する範囲は特定のリージョンに留まらず、各国の各種規制によって利用が制限される可能性があります。これはBitcoinやEthereumのような暗号資産の考え方とは大きくかけ離れており、技術の浸透を阻害する大きな要因になる可能性があります。ERC 725 AllianceやID2020は、このような国を越えた流通の仕組みに対する阻害要因を払拭するアクティビティが必要となるでしょう。しかし今のところそれらに関するアクティビティは見受けられません。そもそもこれらのコンソーシアムで扱うべき問題なのかどうかも含め、広い見識と視野を持った有識者がこの問題に取り組む必要があるでしょう。

執筆者:
須賀 祐治(すが ゆうじ)
IIJ セキュリティ本部 セキュリティ情報統括室 シニアエンジニア。2008年7月より現職。暗号と情報セキュリティ全般に関わる調査・研究活動に従事。CRYPTREC TLS暗号設定ガイドラインWG 主査。CRYPTREC暗号技術活用委員会 委員。暗号プロトコル評価技術コンソーシアム 幹事。情報処理学会 CSEC研究会 幹事。電子情報通信学会 ISEC研究会 幹事補佐。CyberSciTech2019 Program co-chair。IWSEC2019 Organizing committee member。Cryptoassets Governance Task Force(CGTF) Security WG member。

IIJにおけるeSIMの取り組み

3.1 eSIMとは何か

2018年9月にiPhone XSが発表されて以降、eSIMというキーワードがよく聞かれるようになりました。本リサーチでは、eSIMの技術的な説明、及びIIJとしての取り組みについて説明します。

従来のSIMカードは以下で構成されており、これらを耐タンパ性を持ったパッケージにして製造されています。

- **モバイルサービスを提供するために必要なデータ**
- **SIMに付加価値を持たせるアプレット**
- **データとアプレットを安全に保持するためのストレージ**
- **認証処理、暗号鍵生成などの処理を行うプロセッサ**

特に認証や暗号化に使用する鍵情報は、SIMの外部から直接読み出すことが不可能な仕組みとなっています。

これに対しeSIMは、データとアプレットから構成されるプロファイルと、ストレージとプロセッサから構成されるeSIMカードの2つに分離し、プロファイルを専用のサーバからネットワーク経由でeSIMカードに書き込めるようにしました。この仕様は、業界団体であるGSMA[*1]で策定されました。プロファイルをネットワークから書き込むための仕組みをRSP(Remote SIM Provisioning)と呼びます。RSP自体は、従来のSIMにおいても、OTA(Over the Air)によるリモートからSIM内のデータを変更する手段として使われています。IIJでも、フルMVNOで提供している一部のSIMカードに対して、回線開通のタイミングで電話番号を書き込むために、OTAを利用しています。

eSIMという単語はEmbedded Subscriber Identifier Moduleの略で、組み込み用のSIMという意味です。現在では、RSPを利用してネットワーク経由でプロファイルを書き込むことが可能なSIMを指す言葉として用いられる場合がほとんどです。背景として、組み込み用途に使用されるSIMに対して、ネットワーク経由でプロファイルを書き込む仕組みが要求されたからです。

組み込み用途では、一般的なカードタイプのSIMではなく、基盤に直接ハンダ付けするチップタイプのSIMが使われる場合があります。理由として、チップタイプのSIMに次のようなメリットがあるからです。

- **産業用機器などをターゲットとしているため、高い耐久性を持つ**
- **基盤にハンダ付けされており、振動による接触不良が発生しにくい**
- **製造時に基盤にハンダ付けされるため、SIMカードを挿す工程を省略できる**
- **部品サイズが小さく、デバイスの小型化ができる**

なお、IIJでは上記のメリットを享受できるよう、2019年2月より、フルMVNOのSIMのラインナップにチップタイプのSIMを追加しています。

上記のようなメリットのあるチップタイプのSIMですが、製造時にデバイスに組み込むため、後からSIMを変更することが事実上不可能です。このため、使用するモバイル回線を製造時に決めておく必要があり、以下のような問題点を抱えています。

- **輸出先が異なる製品の在庫を共通化できない**
- **製品製造時の動作確認をする場合も正規契約の回線を使う必要がある**
- **製品を使用する場所が移動してもモバイル回線を切り替えることができない**
- **通信コスト削減などの理由でモバイル回線を切り替えることができない**

＊1　携帯通信事業者の業界団体「GSM Association」の略称。2Gの通信方式「GSM」の普及を目的に1995年に設立。約800社の携帯電話事業者を中心に、220ヵ国1000社以上が参加している業界最大の団体。毎年2月に開催される世界最大規模のモバイル関連展示会「Mobile World Congress (MWC)」の主催団体としても知られている。

一方で、カードタイプのSIMを採用した場合、上記の問題点は解消されますが、カード交換の現地作業コストが発生します。

上記のような問題点を解消するために、eSIMは作られました。プロファイルを後から書き込み可能なため、組み込み時にモバイル回線を契約しておく必要がなくなります。また、リモートからプロファイルを書き込み可能なため、SIMの交換に関する現地作業コストもなくなります。

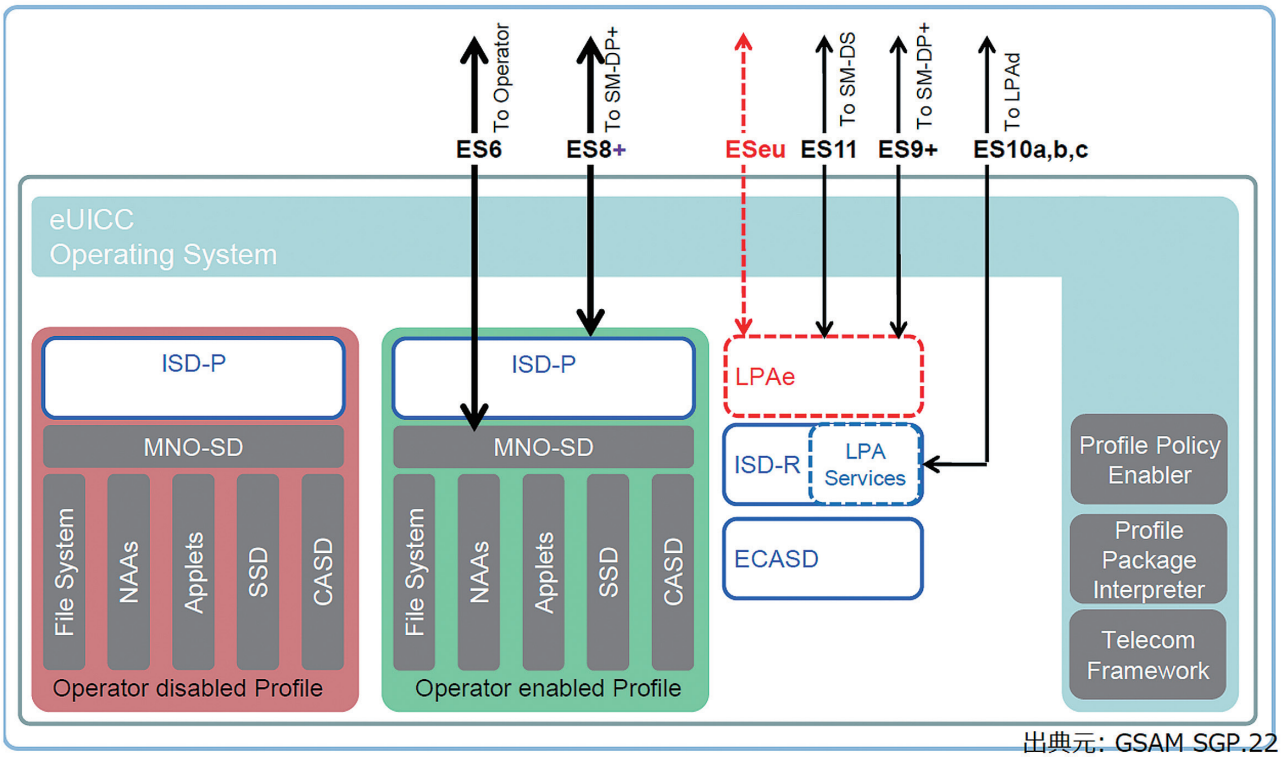
3.2 eSIMの仕組み

3.2.1 eSIMの内部構造

eSIM内部は、図-1のような構造となっています。この内、eSIMを特徴付ける要素が、ISD-R、ISD-P、ECASDの3つです。

ISD-R[*2]はeSIM内部とeSIM外部との直接的なインタフェースとなり、eSIMを管理します。プロファイルのダウンロードやダウンロードしたプロファイルのインストール、インストールしたプロファイルの切り替えや削除といった操作はすべてISD-R経由で行われます。

ISD-P[*3]は従来のSIMカードに相当し、インストールされたプロファイルごとに作成されます。サーバからダウンロードされたプロファイルはISD-Pを作成する手順を記述したフォーマットとなっており、インストール時にこのプロファイルを解釈してISD-Pが作られます。通信に使用するISD-Pをアクティベートすることで、デバイスからは通常のSIMとして見えます。



出典元：GSAM SGP.22

図-1 eSIM内部の構造

＊2　ISD-R：Issuer Security Domain Rootの略称。
＊3　ISD-P：Issuer Security Domain Profileの略称。

ECASD[*4]はプロファイルをダウンロードする際のデータ保護に使用する鍵を格納した領域です。格納された鍵を使用して、サーバとeSIMカード間の認証を行います。また、サーバからダウンロードするプロファイルは暗号化されており、プロファイルの復号化にも、格納された鍵を使用します。

ECASDに格納されている、データの保護のための鍵は、公開鍵基盤にもとづき署名されており、同様に署名された鍵がサーバ側にも格納されています。SIMとしてのセキュリティを担保するため、GSMAがルート証明局としてこれらの鍵に署名しており、他の証明局で署名された鍵は不正なものとして扱われます。GSMAから署名を受けるためには、eSIMの製造拠点、プロファイルを格納するサーバの設置拠点それぞれに対してSASと呼ばれる認定を受ける必要があります。SASの認定には多くのコストがかかるため、認定を受けたeSIMの製造拠点も、サーバの設置拠点も限られています。サーバについては、個々の事業者が独自に持つのではなく、SAS認定を受けたサプライヤのサービスを使うことが現状ではほとんどです。

このような、リモートからのプロファイル書き込みに対応したeSIMには、2019年6月現在、大きく分けて以下の2種類の仕様が存在します。

■ M2Mモデル

M2Mデバイス向けに策定された規格で、リモートからeSIMを制御します。当初の目的である組み込み機器向けの仕様です。

■ コンシューマモデル

人間が操作するデバイス向けに策定された規格で、デバイス側でeSIMを制御します。人間が操作する上で、M2Mモデルでは対応が難しい部分を改善した仕様です。

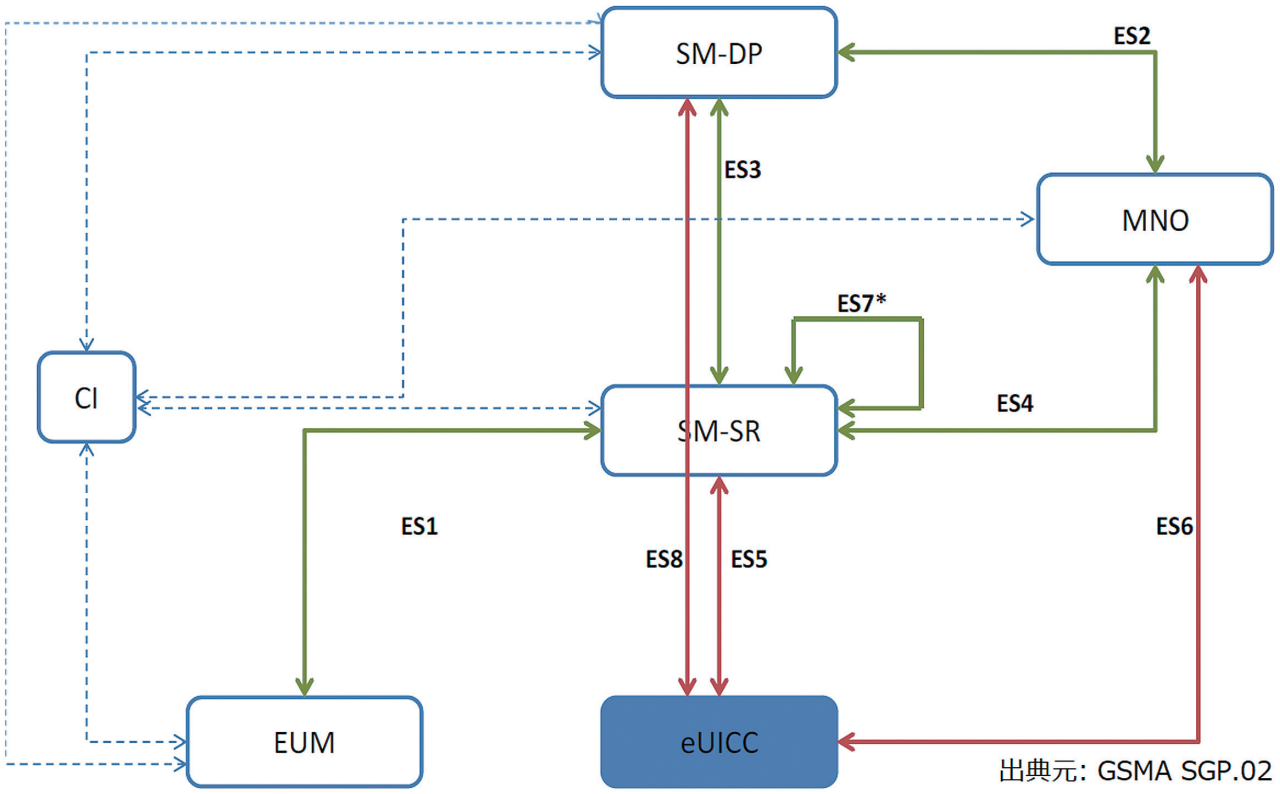


図-2 M2Mモデルのインタフェース

*4　ECASD：eUICC Controlling Authority Security Domainの略称。

3.2.2 M2Mモデル

M2Mモデルは、eSIMの最初の仕様となります。IoT機器が対象のため、リモートからプロファイルのインストールや切り替え、削除まで行うことが可能です。M2Mモデルの構成要素を図-2に示しますが、主要な構成要素は以下のとおりです。

- **eSIMカード**
- **eSIMカードが組み込まれたデバイス**
- **eSIMカードに対してセキュアな経路を確立するSM-SR[*5]サーバ**
- **プロファイルを提供するSM-DP[*6]サーバ**

M2Mモデルでは、SM-SRサーバを起点としてeSIMカードを制御します。SM-SRサーバからeSIMカードに対しSMSを送信して、SM-SRサーバとeSIMカード間にセキュアな経路を開き、以下の操作を行います。

- **プロファイルのダウンロードとインストール**
- **プロファイルの切り替え**
- **プロファイルの削除**

SM-SRサーバとの通信はeSIMカードが直接行い、eSIMカードが組み込まれたデバイス側ではSMSやパケットの転送のみを行います。デバイス自体に必要となる機能は少なく、最近の一般的なモデムでおおむね対応しています。組み込み機器のように実装可能な機能が限られている環境でも対応可能な仕様と言えます。

M2Mモデルでは、SM-SRサーバがeSIMカードを制御するため、eSIMカードは特定のSM-SRサーバとのみ通信を行います。特定のSM-SRサーバとのみ通信する構成となるため、SM-SRサーバを持つプラットフォーマが、物理的なeSIMカードの供給も併せて行うこととなります。また、すべてのプロファイルがSM-SRサーバを経由してインストールされるため、インストールするプロファイルもSM-SRサーバを持つプラットフォーマが調達することとなります。このため、プロファイルの選択肢はプラットフォーマ側に依存します。

eSIMカードとSM-SRサーバとの通信はIPプロトコルで行われますが、SM-SRサーバからeSIMカードにアクセスするための最初のトリガーには、SMSが使用されます。SMSを利用するためにモバイル回線が必要となることから、M2Mモデルで使用するeSIMカードには、ブートストラップと呼ばれるプロファイルが最初からインストールされています。eSIMの操作はすべてリモートで行うことからブートストラップにはあらゆる国での接続性が求められるため、このプロファイルの調達方法が1つの課題となります。また、プロファイルの切り替えが必要とならないケースでは、ブートストラップは無駄となります。国内向け限定の製品であれば、プロファイルを入れ換える必要がないため、従来のチップタイプのSIMで問題ないと言えます。

3.2.3 コンシューマモデル

コンシューマモデルは、M2Mモデルの次に策定された仕様です。スマートフォンなど、エンドユーザが直接操作するデバイスが対象で、eSIMの操作はすべてデバイス上で行えるようになっています。コンシューマモデルの構成要素を図-3に示しますが、主要な構成要素は以下の通りです。

- **eSIMカード**
- **eSIMカードが組み込まれたデバイス**
- **デバイス上でeSIMカードを管理するためのLPA[*7]**
- **プロファイルを提供するSM-DP+サーバ**
- **eSIMに提供されたプロファイルの検索を行うSM-DS[*8]サーバ**

M2Mモデルと比較すると、eSIMカードのプロファイルの管理をリモートから行うSM-SRサーバがなくなり、代わりにデ

＊5　SM-SR：Subscription Manager Secure Routingの略称。
＊6　SM-DP：Subscription Manager Data Preparationの略称。
＊7　LPA：Local Profile Assistantの略称。
＊8　SM-DS：Subscription Manager Discovery Serverの略称。

バイス上でプロファイルを管理するLPAというアプリケーションが追加されています。また、M2Mモデルでは存在しなかった、SM-DSサーバが構成要素として追加されています。その他、SM-DPサーバも、コンシューマ向けの要件を満たすための機能変更が行われており、区別するためにSM-DP+サーバと呼ばれます。

コンシューマモデルで追加されたLPAは、エンドユーザが端末上で以下の操作を行うためのインタフェースを提供します。

- **プロファイルが格納されているSM-DP+サーバのアドレスとプロファイルの識別子の入力**
- **インストールするプロファイルのダウンロードとeSIMチップへのインストール**
- **使用するプロファイルの切り替え**
- **不要なプロファイルの削除**

LPAはデバイス側で動作するLPAdとeSIMカード側で動作するLPAeという2つの実装形態が定義されています。デバイスベンダーがコンシューマモデルのeSIMデバイスを開発する場合、LPAe対応のeSIMを採用するか、LPAdをデバイスに実装するかのいずれかを選択する必要があります。今のところLPAe対応のeSIMは普及していないため、デバイスベンダーはLPAdを実装する必要があり、この点がコンシューマモデルのデバイス開発を行う上での1つのハードルとなっています。

LPAによりデバイス上ですべての操作を行うモデルのため、M2Mモデルで必須となっていたSMSは不要です。プロファイルのダウンロードもWi-Fi経由で可能なため、M2Mモデルでのブートストラップに相当するプロファイルが不要となります。余分なモバイル回線の契約が不要となるため、IoT機器向けでもLPAを実装してコンシューマモデルを採用するケースもあるようです。一方で、エンドユーザの利便性を考慮して、プ

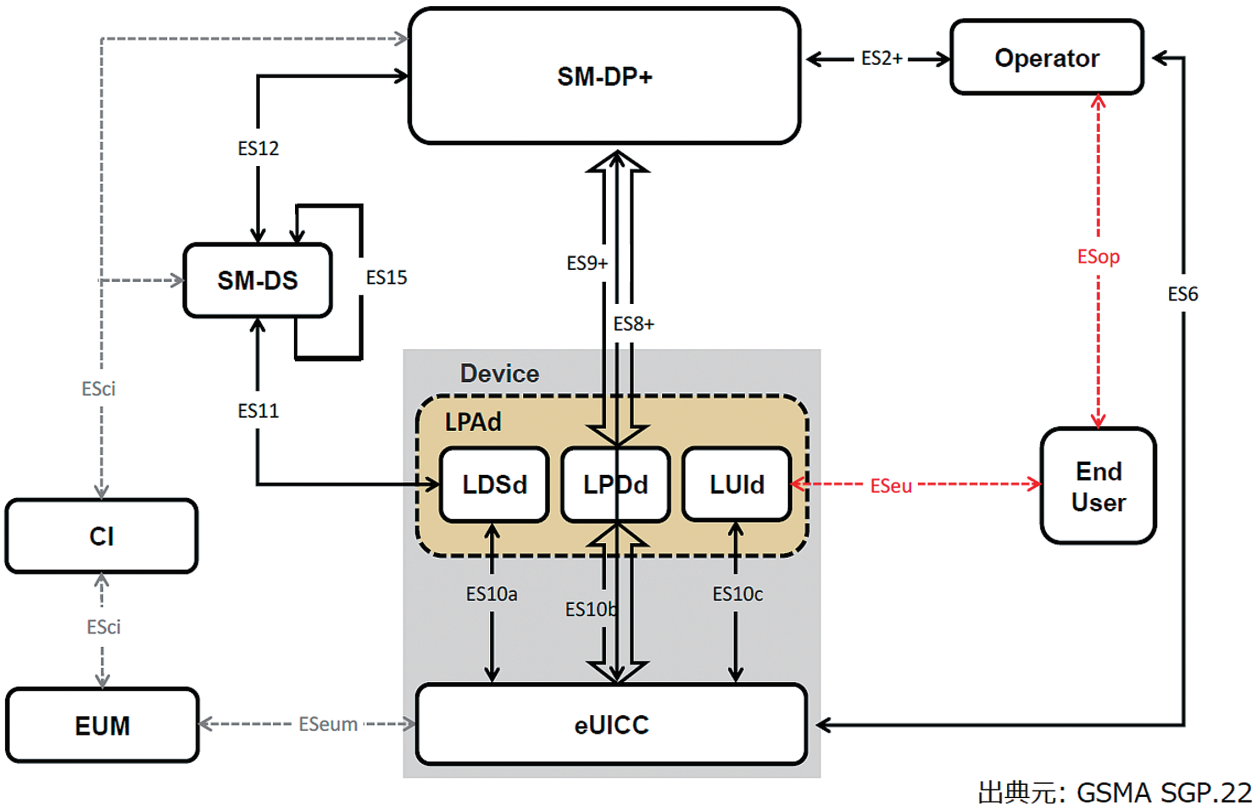


図-3 コンシューマモデルのインタフェース

ロファイルダウンロード用のモバイル回線用プロファイルをインストールした状態で提供される場合もあります。

プロファイルをインストールするにあたり、SM-DP+サーバのアドレスとインストールするプロファイルを特定するためのMatching IDと呼ばれる識別子をLPAに入力する必要があります。このために使用するのが以下のようなアクティベーションコードと呼ばれる文字列です。

```
1$SM-DP-PLUS.EXAMPLE.COM$MY-MATCHING-ID-0123456789
```

「$」を区切り文字として、バージョン番号(現在は1で固定)、SM-DP+サーバのアドレス、Matching IDで構成されます。この文字列を手動で入力するのは大変なため、通常はQRコードに変換してデバイスに読み込ませます(図-4)。

3.3 主要ベンダーの動き

3.3.1 Apple

Appleは早くからApple SIMという形でeSIMに相当する機能を提供してきました。Apple SIMの詳細は公開されていませんが、仕組みとしてはM2MモデルのeSIMが使われていたと考えられます。ただし、エンドユーザが各々で回線契約を実施するため、デバイス上で回線契約が行える仕組みを組み込むなど、独自色の強いサービスとなっています。Appleはプラットフォームを提供するのみですが、Apple自身の強いブランド力を背景に、各国のモバイル事業者のプロファイルを集めることに成功しています。

図-4 アクティベーションコードのQRコード

1枚のSIMカードにより、世界中のユーザにコネクティビティを提供する点がApple SIMの特徴です。しかし、Apple SIMで提供されるのはデータ回線契約のみで、音声回線契約は提供されていません。おそらくですが、データ回線の契約と比較して、音声回線の契約には本人確認などが必要となり、そのレギュレーションは各国様々なため、単独のプラットフォームでこれに対応することが困難だったと考えられます。

iPad向けにApple SIMを使い続けてきたAppleですが、2018年に発売したiPhone XSでは、標準のコンシューマモデルのeSIMを採用しました。電話であるiPhoneでは音声契約を切り離すことができなかったことが理由と思われます。eSIMに対応したiPhone XSの後に発売されたiPadなど、音声回線を利用しないデバイスでApple SIMが採用されていることを考えると、音声契約だけはApple SIMでの提供を断念したと考えられます。標準のeSIMを採用するのであれば、モバイル事業者がプラットフォームを作ることとなり、音声契約にかかわるレギュレーションを満たせるという判断だと思われます。

Apple SIMでは、Appleを経由した回線契約となり、IIJのようなMVNOが回線を提供することは困難でした。しかし、iPhone XS以降に採用されたコンシューマモデルのeSIMでは、インストールするプロファイルに制限はなく、IIJのフルMVNOのプロファイルを利用することが可能です。2019年夏に提供開始を予定しているIIJのeSIMサービスでは、iPhone XS/XRユーザを主要なターゲットの1つに定めています。

3.3.2 Microsoft

MicrosoftはWindows 10 バージョン1703において、OSに標準的なLPAを搭載しました。Microsoftが掲げるAlways Connected PCのコンセプトに、eSIMが有効と判断された結果と考えられます。OSにLPAが標準で搭載されたことで、デバイスベンダーは自社でLPAを実装する必要がなくなり、eSIMカードと対応するモデムモジュールを調達すれば、容易にeSIMに対応したデバイスを製造することが可能となりました。デバイスの製造が容易となったことで、今後eSIMを搭載したデバイスが普及していくと考えられます。普及の動きの1つとして、Microsoft自身もeSIMを内蔵したSurface Proを販売しています。

また、Microsoftは、Apple SIMのようにデバイス上で回線契約まで行える、モバイル通信プランというアプリも提供しています。日本国内では2019年6月現在、KDDI、GigSky World Mobile Data、Ubigiのプロファイルを購入することができます。

この他に、2018年11月末に米国で開催されたMicrosoft Ignite 2018では、企業向けMDM[*9]へのeSIMの統合を計画していることも公表されました。企業で使われるPCとしてデバイスの管理は必須となりますが、モバイル回線の管理もMDMの中に取り込み、企業のデバイス管理者が個々のデバイスで使うeSIMプロファイルの管理も行うことが可能となります。

3.3.3 Google

GoogleのeSIMへの対応は、AppleやMicrosoftと比べると遅れているようです。Android Piで、eSIMに関係するAPIを定義しましたが、OS自身にLPA機能を搭載していないため、各ベンダーがLPAアプリを実装する必要があります。なお、Google自身はLPAを組み込んだ、Pixel 2やPixel 3、Pixel 3aといったeSIM対応端末を提供しています。ただし、本稿を執筆している2019年6月現在で日本向けに発売されている端末については、eSIMの代わりにNFC[*10]が搭載され、国内ユーザはeSIMを使うことができないようです。

Google自身のサービスとしてはeSIMを利用して、Google FiというMVNOサービスにより、世界各国のコネクティビティを提供するサービスを開始しました。対応するAndroid端末は限定される一方で、iPhoneへの対応も行われています。iPhoneなど、自社で管理していない端末にも提供されていることから、プロファイルの提供はM2Mモデルではなく、コンシューマモデルだと考えられます。一方で、利用可能なエンドユーザは米国在住者に限られており、世界中のユーザが利用できるわけではありません。ただ、サービスの提供範囲は、米国在住者に限られるものの、Apple SIMとは異なり音声サービスも提供されています。これは、GoogleがMVNOとして提供すること、そして提供の対象を北米在住のユーザに絞ることで、エンドユーザの音声契約に関するレギュレーションを米国の基準に限定することができたからだと考えられます。

3.3.4 類似のサービス

eSIMとは異なりますが、中華圏を中心に、独自の仕様でプロファイルの販売が行われています。独自のSIMと、そのSIMにプロファイルをインストールするOTAサービスが提供され、エンドユーザは様々な国のモバイル事業者のプロファイルをダウンロードして使えるようになっています。ターゲットとなるエンドユーザは自国のアウトバウンドの旅行者で、旅行先でのローミングより安価なコネクティビティを提供することを目的としています。日本での例として、H.I.S.モバイルが販売している「変なSIM」シリーズがこの系統にあたります。

なお、これらのサービスも、iPhone XSなど、eSIMを搭載したデバイスが出てきたことで、独自仕様からオープンなeSIMのプラットフォームへの転換を行っているようです。

3.4 IIJの取り組み

フルMVNO事業者であるIIJは、eSIMにインストールするプロファイルを自社で提供することが可能です。現在、フルMVNO回線の新規販売チャンネルとして、eSIM向けにフルMVNOプロファイルを提供するサービスの開発を進めています。

先に述べたとおり、eSIMの提供形態は、M2Mモデルとコンシューマモデルの2つのパターンがあります。IIJでは、まずはコンシューマモデルをターゲットとしています。理由は、現在IIJが発行できるプロファイルは国内のみのため、国外展開を前提としたM2Mモデルより、コンシューマモデルの方がフ

＊9　MDM：Mobile Device Managementの略称。モバイルデバイス管理。
＊10　NFC：Near Field Communicationの略称。近距離無線通信規格。

ルMVNO回線に合っていると考えているからです。更に、フルMVNOのプロファイルでは国外の接続性の担保が難しく、ブートストラップとして利用できないことも理由の1つです。

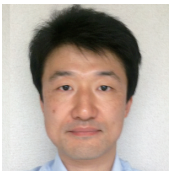
eSIMサービス提供に向けた取り組みの一環として、昨年度にはコンシューマモデルの構成で実証実験を行いました。実証実験では、フルMVNO用のプロファイルを設計し、Microsoft Surface Proにプロファイルをインストールし、モバイル通信を行うことに成功しました。また、Microsoft Surface Pro以外の端末もターゲットとして動作確認を行い、ノウハウを蓄積しています。その1つとして、プロファイルとeSIMカードの間に相性の問題があることを確認しました。前述しましたが、eSIMカードにインストールするプロファイルは専用のフォーマットで記述されます。この中で、記述を簡略化するためにテンプレートという記法が定義されていますが、テンプレートを利用した場合に、特定のeSIMカードでインストールに失敗してしまうパターンが存在することを確認しました。また、特定の非必須パラメータの記述が存在しないことに起因して、インストールできない問題も確認しています。eSIMカード自体を管理下に置けるM2Mモデルと異なり、コンシューマモデルでは、様々なeSIMカードがターゲットとなるため、このようなノウハウの蓄積は、サービスを提供する上で必須と言えます。

本稿を執筆している2019年6月の段階では、実証実験も終わり、商用提供に向けたサービス開発を行っています。SM-DP+サーバについては、GSMAのSASの認定が必要となるため、自社独自で持つことが難しいこともあり、他のモバイル事業者と同様、SaaS型のサービスを利用しますが、国内で提供されているeSIMサービス(ドコモのdtabや、KDDIのWindows向けプリペイドプラン)とは異なり、特定のデバイスに縛られない、汎用的なサービスの提供を目標としています。2019年の夏には読者の皆様にご利用いただけるサービスを提供する予定です。

3.5 eSIMの活用シーンと今後の動向

eSIMを利用することで、どのような未来が描かれるでしょうか。

eSIMが従来のSIMと大きく異なる点は、物理的なSIMが排除される点です。物理的なSIMカードがなくなり、電子データとしてプロファイルがやりとりされることで、SIMカードの配送にかかるコスト(距離的、時間的なものも含める)が不要になります。コストと言うと価格部分に注目しがちですが、プロファイルの購入にあたって、店舗に行く、あるいは、SIMの配送を待つといったことが不要となります。この結果、エンドユーザは、いつでも、どこでも、必要なときにプロファイルを購入することが可能となります。長期の契約ではこのメリットは活かし難いかも知れませんが、プリペイド、特に渡航者が現地で一時的な回線を契約するケースでは、購入が容易となる点が活きてきます。併せて、物理的なSIMカードの交換が不要となるため、紛失リスクがなくなるなどといったメリットも生じます。特にiPhone XSのようなDSDS[*11]端末であれば、メインの音声契約のSIMカードをSIMスロットに入れ、データ用のSIMを必要なときにプリペイドで購入するといった使い方が考えられます。ただ、日本国内市場で言えば、流動性の高いeSIMを本格的に採用することは、モバイル事業者側にとって直接的な利益につながるものではありません。そのため、端末メーカ主導でSIMフリー端末を導入していかない限り、eSIMの普及は難しいのではないかと考えられます。IIJとしては、いち早くeSIMサービスを開始することで、端末メーカがeSIMに対応した端末を導入していくような土壌となればと考えています。



執筆者:
圓山 大介(まるやま だいすけ)
IIJ MVNO事業部 技術開発部 MVNOサービス開発課。
2018年IIJ入社。フルMVNO向けのサービス基盤の開発に従事。直近では本文に記載したeSIMのサービス基盤の開発に携わる。

*11 DSDS:Dual SIM Dual Standbyの略称。

June 2019 Vol.43

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2019年6月時点のものです。

IIJ-MKTG019-0043

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