# めもおきば Tech Report 8

［めもおきば てっくれぽーと］
クラウドとセキュリティ、
TL 流速を支える
エンジニアの総合誌

December 2017

Special Feature 1

KDDI がソラコムを爆速グループ傘下にした理由

## SORACOM 買収からわかる IoT の未来

世界観の把握、サービス紹介から将来像まで

Special Feature 2

## 私もセキュリティキャンプに行きたい！

{集中コース
選択コース}

22 歳以上のオトナの参加方法は？

Extra Feature

【保存版】ワイヤレス技術の高め方

## Bluetooth mesh ってどうよ

# めもおきば TechReport 2017.08

## ― 目次 ―



Aki @ nekoruri

# SORACOM 買収からわかる IoT の未来

本書の執筆中に「株式会社ソラコムの KDDI グループ参画」というニュースが飛び込んできました。日経新聞曰く 200 億円という買収額をどう感じるかは視点次第ではありますが、玉川さんのインタビュー[1]にある「ビジョンをやりきるため、アクセルを踏み込むための M&A」という言葉のとおり、世界をねらうためのステップとして期待をしています。

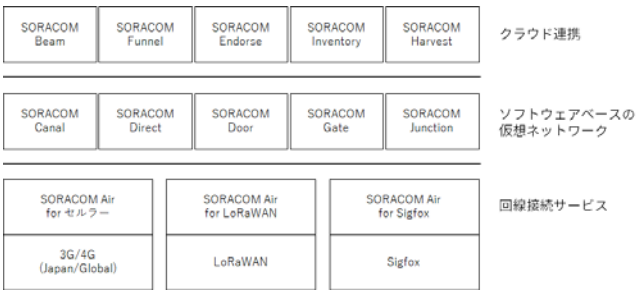
オープニングポエムはさておき、単なる IoT/M2M 機器向けに価格プランを作り込んだだけの安価な MVNO キャリアと勘違いされがちな SORACOM ですが、その真価は「通信とクラウドを融合した IoT 通信プラットフォーム」であることです。本章では、これがどういうことか解き明かしていこうと思います。

## SORACOM とは

端的に言えば、SORACOM は株式会社ソラコムが提供する IoT 通信プラットフォームです。

正直「IoT なんちゃらプラットフォーム」という単語自体にバズワード感がありますが、一般的には IoT[2] デバイスが通信をするために必要なものを揃えたパッケージという感じで使われているようです。
SORACOM のように通信にフォーカスしたものだけでなく、（ネットワーク接続を前提に）IoT デバイスから集まってきたデータを分析・可視化するサービスや、デバイスからデータをクラウドに投げるときのライブラリ群、あるいはそれらを包括的に提供するものといくつかのパターンがあるようです。

SORACOM はざっくり三つの役割を提供しています。




[1] ソラコム玉川社長に聞いた「KDDI 入り」の背景とソラコムのメッセージ
http://ascii.jp/elem/000/001/525/1525188/

[2] IoT の定義については、Internet の指す対象や CPS（Cyber-Physical System）との違いなど議論がありますが、本書では「大量のデバイスを IP ネットワークに接続して何かする」ぐらいの緩い定義とします。

SORACOM はこれらを下から上まで「垂直統合」で提供し相互に価値を高め合うことで、利用者に対して高度なサービスを提供しているわけです。

## 回線接続サービス

IoT デバイスがネットワークに接続するための回線を提供する、プラットフォームとしては一番低い部分です。サービス名称としては「SORACOM Air」が対応し、SORACOM の最初のサービスでもあります。

当初は NTT ドコモの MVNO として日本国内向けにサービスを開始しましたが、その後海外でも利用可能なグローバル向け Air SIM が提供されたほか、920MHz 帯の LPWA（Low Power Wide Area Network[3]）である LoRaWAN と Sigfox にも対応しました。

また、株式会社ソラコムとしてのサービスではありませんが、ソラコムが開発した SORACOM のエンジンである「SORACOM vConnec Core」を KDDI が採用した「KDDI IoT コネクト Air」があります。MVNO と同等の接続サービスとしては同じように提供されていますが、この後に紹介する上位層の機能は残念ながら SORACOM 本家から若干遅れての提供になっているようですが。KDDI グループへの参加により、サービス内容の共通化も進んでいくと考えられます。なお、技術的詳細は明かされていないので、KDDI としてのサービスについて、これ以降は触れません。

SORACOM Air は NTT ドコモと L2 卸契約する MVNO ですが、NTT ドコモからの専用線から先の MVNO キャリアとして必要なシステム全てを AWS 上で構築しています。データトラフィックの転送や通信網の管理を、クラウドネイティブな設計でソフトウェアによって実装しています。これにより、利用数の増加を見込んだ設備投資を避けつつ、高い頻度での開発サイクルを回しています。その副産物として、1 日 10 円＋最低 0.2 円/1MB（たとえば月間 1GB であれば約 500 円）という低トラフィックでは極めて安価な従量課金を実現しています。

ただ、安いことは SORACOM の価値の中ではぶっちゃけ些細なことではないでしょうか。単に安いインターネット接続回線だけが欲しいのであれば、月額 300〜500 円や、一定転送量まで 0 円という MVNO キャリアも登場している昨今です。

SORACOM Air の価値の半分は、その管理機能を API として提供していることにあります。API から SIM ごとの設定（回線速度や回線自体の有効・無効など）を変更でき、通信量などを監視して AWS Lambda を呼び出すイベントハンドラー機能もあります。これを利用することで、SORACOM の上に仮想 MVNO 事業者を構築したり、SIM を組み込んだ形で製品を出荷してから契約状況に合わせて通信を有効化・無効化したりといったことが可能になるわけです。

[3] 間欠的に通信を行うことで、低電力（設定によっては乾電池で数ヶ月以上）で広域（数 km）の通信を実現しようとする無線通信のカテゴリ

残りの半分は、SORACOM Air という回線契約があることで、安全にデバイスを識別でき、それによって上位層の機能を提供できるということです。セルラー[4]であれば SIM が、Sigfox であればデバイス内蔵のセキュアエレメントが耐タンパー性[5]を持ち、デバイス識別のための秘密情報が安全に保存されています。また LoRaWAN の場合にも、出荷時に SORACOM 側と同期されてデバイスに設定される AppKey を使ってセッション鍵を作成するため、耐タンパー性とまではいきませんがそれなりに保護されています。

接続回線という一番下の層において個別のデバイスを一つの ID 基盤上で識別できているからこそ、異なる通信網を性質の違いのみを意識するだけで、その上に多種多様なサービスを統一的に提供できます。概念的な表現をすると、閉域網の中でデバイス別に IP アドレスが割り振られる旧来のネットワークセキュリティのモデルに対して、回線の接続点で直接認証される ID ベースのセキュリティという新しいモデルがあり、それに基づいて SORACOM のあらゆるサービスが実現されています。要するに、「B」以降のサービスのために、SORACOM Air としては様々な通信方式に対応する必要があり、今後来る 5G ベースの携帯通信網や、グローバルの世界制覇のために KDDI と手を組んだのだと思います。

## ソフトウェアベースの高機能な仮想ネットワーク

先ほど書いたとおり、SORACOM のネットワークは全てクラウド上のソフトウェアで構築されています。つまり一種の Software-defined Network（SDN）や Network Function Virtualization（NFV）です。通信回線の反対側にそのまま SDN/NFV の世界を接続したことで、閉域網として様々な機能を提供しています。

閉域網という視点では、接続先に応じて 3 種類のサービスを提供しています。AWS 上の自分の VPC に接続する最も安価な「SORACOM Canal」、物理専用線として AWS Direct Connect を利用する「SORACOM Direct」、インターネット VPN を利用する「SORACOM Door」です。これらを利用する場合は、Virtual Private Gateway（VPG）という仮想ルータを構築して、SORACOM Air の回線ごとに VPG に接続します。自分独自の VPG を利用することで、デバイスに割り振られる IP アドレスレンジ[6]を変更したり、デバイス毎に固定の IP アドレスを指定したりといったことも可能です（次に紹介する SORACOM Gate を使わない限り、その IP アドレスが直接見えることはありません）。ただし、これらは閉域網と言っても VPG で NAPT されるため、あくまでデバイス側からクラウド側への方向の接続のみを提供しています。

クラウド側からデバイス側への接続、あるいはデバイス同士の接続を実現するのが「SORACOM Gate」です。SORACOM Gate を有効にするとデバイス毎の IP アドレスを利用して相互に通信が可能となります。さらに、SORACOM Canal 等で接続されたネットワーク上に Gate Peer と呼ばれるルータ（実際には VXLAN が設定された Linux ホスト等）を構築することで、そこからデバイスまで一つの仮想 L2 ネットワークが提供され、自分のネットワークからデバイスに直接接続できるようになります。Gate Peer まで L2

[4] いわゆる 3G/4G など携帯電話回線ベースの技術

[5] 壊しても中身の暗号鍵などを見られない性質

[6] デフォルトでは 10.128.0.0/9

で伸びてきてくれるため、そこから自分の VPC 内のネットワークにさらに L2 ブリッジしても良いですし、もっとシンプルに NAPT するのも手軽です。

さて、このあたりまでは気合いの入った閉域網サービスであれば実現できるところですが、SDN であることを最大限に活かす SORACOM らしいサービス「SORACOM Junction」がつい先日リリースされました。これは VPG を通過するパケットに対して、ミラーリング、リダイレクション、インスペクションの 3 つの操作を提供します。ミラーリングとリダイレクションは、名前の通りパケットを複製したり転送先を変更したりすることで、ユーザ企業が独自の監視システムを通したりトラフィックの制御を行ったりと言うことが可能となります。インスペクションは、パケットの統計情報を外部のクラウドサービス[7]に送信します。

これら SORACOM の高機能な仮想ネットワークは、全てクラウドネイティブな設計で実現されているため、SORACOM の利用者やその転送速度・秒間パケット数などが増えても（万が一 AWS のリソースが頭打ちしない限り）いくらでもスケールすることができます。その一方で、たとえば SORACOM Canal の VPG は 1 時間あたり 50 円（30 日間で 36,000 円）と、きちんと利用者にそれなりの負担が求められます[8]。このあたりはうまく技術上の制約をビジネスとして成立させていると感じます。

モバイル通信網の課金体系は、行き過ぎたインセンティブなどにより極めて歪になってしまっていますが、SORACOM の素直な課金体系を見るとほっとします。

## クラウド連携

SORACOM の真価はクラウドとの統合にあります。IoT でビジネスをするために必要なのは、単に IoT デバイスを IP ネットワークに接続することだけではなく、その IP ネットワークを介してクラウドの向こう側に大量のデータを期待する品質で届けることです。通信とクラウドの融合を謳っているように、SORACOM には IoT デバイスをクラウドと連携するための仕組みが数多く用意されています。

SORACOM のクラウド連携機能は、大きく二つに区別できます。一つは、AWS や Azure、GCP、あるいは独自に構築したサーバなどの、「クラウド側」との橋渡しをする機能です。サービスとしては「SORACOM Beam」と「SORACOM Funnel」があります。単純にデータを左から右へと転送するだけで無く、クラウドに送る際の認証や暗号化処理、データ量の限られた LPWA を利用する時のデータ形式変換など、「IoT デバイスがクラウドと通信する際のあるある処理」を SORACOM が肩代わりしてくれます。

もう一つは SORACOM 自身がクラウドとして直接的な機能を提供するもので、「SORACOM Endorse」「SORACOM Harvest」「SORACOM Inventory」が対応します。SORACOM Harvest のように単体で完結

[7] 送信先にできるクラウドサービスはこの後紹介する SORACOM Funnel と同じようです。内部的には同じ枠組みに載っていると思われます。

[8] 月 36,000 円で用意できる AWS のインフラ環境は何だろう……と考えていくと、VPG の仕組みが妄想できそうな気がしてきます。

するものもあれば、SORACOM Endorse のように別の枠組みと連携するための機能もあります。ここからは、これらを個別に掘り下げていきます。

## SORACOM の世界観

SORACOM のクラウド連携について具体的な機能を紹介する前に、まず SORACOM が IoT プラットフォームとして提供しようとしている世界観について触れておきます。

IoT における代表的な脆弱性を OWASP がまとめているので、以下に引用します[9]。

| | |
|---|---|
| I1 | Insecure Web Interface<br>安全でない（製品の）Web インターフェース |
| I2 | Insufficient Authentication/Authorization<br>不十分な認証/認可 |
| I3 | Insecure Network Services<br>安全でないネットワークサービス |
| I4 | Lack of Transport Encryption/Integrity Verification<br>転送路における暗号化・完全性確認の欠如 |
| I5 | Privacy Concerns<br>プライバシーに帯する懸念 |
| I6 | Insecure Cloud Interface<br>安全でないクラウド上の Web インターフェース |
| I7 | Insecure Mobile Interface<br>安全でないモバイルアプリのインターフェース |
| I8 | Insufficient Security Configurability<br>不十分なセキュリティ設定 |
| I9 | Insecure Software/Firmware<br>安全でないソフトウェア・ファームウェア（の更新） |
| I10 | Poor Physical Security<br>物理セキュリティが弱い |

IoT デバイスが関連するのは I1、I2、I3、I4、I8、I9、I10 あたりですが、IoT 固有の物理セキュリティ（I10）を除いて、一般的なウェブアプリ等であれば当然のようにどれも考慮されているべきはずのものばかりです。これらがなぜ IoT デバイスで特に問題にされるかと言えば、IoT 固有の理由でそれらを設計時に「妥協」してしまうからです。

IoT デバイスが一般的なサーバ側システムと異なるのは大きく 2 点あります。

[9] https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

一つは計算機としての性能です。最近になってようやく ARM ベースなどの比較的高性能なデバイスも増えてきましたが、消費電力であったりサイズであったり、あるいは予算や部材の都合で依然として性能の低い IoT デバイスとはまだ何年も付き合っていく必要があります。ところがデバイス自身を正しく認証する、あるいはデバイスに接続するユーザを認証するには、公開鍵暗号やハッシュ関数などの計算が必要となり、決して低くない演算能力が必要となります。さらに大量のデータをクラウドに送信するようなデバイスでは継続的な暗号化も必要となります。旧来のネットワーク制御デバイスでは、ネットワークセキュリティを前提として「妥協」をしてきました。その結果として、USB メモリなど様々な手法を組み合わせた Stuxnet などの被害が発生しています。何らかの手段で、低い処理性能しか持たない IoT デバイスからクラウドまでの通信を暗号学的に守っていく必要があることは確定的に明らかです。

もう一つが、IoT デバイスの数が多いということです。様々なデバイスをネットワークに接続して安全に機能させるには、それぞれのデバイスを個別にセキュアに識別する必要があります。そのためには、電子証明書あるいは事前共有鍵どちらでも良いですが、デバイス毎に何らかの秘密の認証情報を持たせる必要があります。ところが、数百数千が前提となるような IoT デバイスでは製造時に個別の情報を持たせ、それをそのまま運用時にも利用するということが難しくなってきます。したがって運用開始時に認証情報を投入する必要が出てくるわけですが、物理的な作業をどう減らすかが重要であり設計の難しさが一気に上がります。また故障時の交換なども踏まえると、開始時だけではなくシステムの運用ライフサイクル全体の中でデバイスの識別方法を設計する必要があります。

SORACOM はこの課題に対して「まず接続回線を安全に識別し、その上で SORACOM 側に処理を委譲する」という解決策を提示しています。SORACOM Air の回線は、3G/4G 網や LoRaWAN/Sigfox のそれぞれの暗号学的手段によって安全に認証・暗号化されています。そこで、IoT デバイスは純粋にやりとりしたいデータだけを SORACOM に送り、SORACOM が認証や暗号化など本来 IoT デバイス上で行うはずだった処理を肩代わりします。

また、IoT デバイスは必ずネットワークに接続する必要があり、設置時に SIM を挿したり、LoRaWAN や Sigfox のデバイス ID を登録したりします。これまでは別の手段で証明書を配布するなど認証のためだけの作業が必要でしたが、通信路に紐付いてクラウド連携を行うことでそういった作業をゼロにします。

これこそが、SORACOM の世界観において核となる考え方です[10]。

プラットフォームというものを提供するということは、そのプラットフォームの世界観——すなわち、IoT/M2M デバイスにおける通信とはどういうものなのか、運用も含めたシステム全体をどういう抽象化に基づいて IoT デバイスやクラウドを設計するのか、という共通認識——のシェアを取り合う「抽象化戦争」に参加することです。この SORACOM の世界観は、IoT プラットフォームにおける象化戦争においてかなり強い魅力を持っているように思います。

---

[10] 偉そうに書いていますが、一ユーザから見た勝手な決めつけです😇

さて、そろそろ個別のサービスを紹介していきます。

## SORACOM Beam

SORACOM Beam は、端的に言えば高機能なアプリケーションプロキシサーバです。

SORACOM 内のエントリポイントに IoT デバイスから送りやすいプロトコルで送信すると、上手い具合にプロトコルを変換したりしてクラウド側に送信してくれます。SORACOM が提供するクラウド連携機能のなかでもっともシンプルなものですが、SORACOM が提供しようとする世界観に触れる入口として一番相応しいものです。

また、SORACOM 上で全ての SORACOM Air 回線はグループ単位で管理されますが、SORACOM Beam はこのグループに対して設定されます。したがってグループの Beam 設定を変更するだけで、そこに紐付いた全ての IoT デバイスからの送信先が一括で管理できます。当然ながら、Beam に限らずこのような設定を SORACOM API で変更することも可能であり、デバイスを含むシステムのオンライン開通などを構築することもできるでしょう。

利用するプロトコルで分類すると、6 種類の動作に分けられます。

### HTTP ⇒ HTTP/HTTPS

IoT デバイスから HTTP でエントリポイントにリクエストを送信すると、そのリクエスト内容をクラウド側の URL に対して HTTP もしくは HTTPS でリクエストを転送します。クラウド側がインターネットの向こう側にある場合など、HTTPS による通信の暗号化処理を SORACOM 側にオフロードできます。IoT デバイスから SORACOM までは各通信手段による暗号化や、NTT ドコモから SORACOM までの専用線で守られているため、SORACOM までは HTTP で良いわけです。

クラウド側にリクエストを送信するときに、接続元 IoT デバイスの IMSI[11]・IMEI[12]や、事前共有鍵に基づいた電子署名、個別に指定したカスタムヘッダを HTTP リクエストヘッダに追加することができます。これによって、クラウド側は「誰からの通信なのか」を識別することができます。これはこの後の他の HTTP 転送先でも共通です。

細かく分けると、ドメイン上の全てのパスをそのまま利用する「Web エントリポイント」と、パスごとに個別の転送先を設定できる「HTTP エントリポイント」の 2 種類が用意されています。

[11] International Mobile Subscriber Identity：SIM ごとに割り当てられる ID

[12] International Mobile Equipment Identity：3G/4G の携帯電話機・モデムごとに割り当てられる ID

### TCP ⇒ HTTP/HTTPS

TCP でエントリポイントに接続して生のデータ列を投げると、HTTP POST リクエストに変換してクラウドに送信します。

データ列は、以下のように Base64 エンコードで JSON に埋め込まれて本文として送られます。

```
{"payload":"Base64 エンコードされたメッセージ"}
```

クラウドからのレスポンスもそれっぽく返ります。

```
400 Message from server
```

### UDP ⇒ HTTP/HTTPS

TCP と同様に、受信したデータを HTTP/HTTPS に変換して送信します。

### TCP ⇒ TCP/TCPS

TCP で送られた内容を、そのまま TCP でクラウドに送信します。IMSI や IMEI 等を送りたい場合は、HTTP リクエストヘッダの代わりに、先頭行として送信されます。

### MQTT ⇒ MQTT/MQTTS

クラウド側の MQTT ブローカーと相互に Publish/Subscribe を転送します。

### LoRaWAN ⇒ HTTP/HTTPS

LoRaWAN デバイスから送信された Uplink データを、HTTP/HTTPS でクラウドに送信します。先ほどの TCP からの変換と似たような動作をしますが、Base64 ではなく Hex 表記が使われるほか、経由した LoRaWAN ゲートウェイの情報や受信電波強度（RSSI）などの追加情報を含む JSON として送信されます。

LoRaWAN などの LPWA では転送できるデータ量が極めて少ない[13]ため、JSON のような富豪的なデータを来ることはできず、まさに「1 ビットは血の一滴」と送らなければならないデータをビット単位で詰め込んで送ることになります。それをどこかでクラウド側で扱いやすい形に変換しなくてはなりませんが、バイナリパーサー機能を利用することで、バイナリデータを指定した通りに分解して JSON 上に展開することができます。どこかで必要になる処理なので、LPWA の利用者には非常に便利と思います。バイナリパーサーはこの後紹介する SORACOM Funnel や SORACOM Harvest にも対応しています。

[13] デフォルト設定（Spreading Factor＝10）では、4.4 秒に 1 回ずつ、1 回に 11 バイト送信できます。

## SORACOM Funnel

筆者が一番好きなサービスがこの SORACOM Funnel です。

SORACOM Beam が単純なアプリケーションプロキシという形態だったのとは対称的に、SORACOM Funnel は様々なクラウド固有のインターフェースに直接データを投げ込むことができる「クラウドリソースアダプター」です。

様々なパブリッククラウドはデータ収集用のサービスを提供していますが、IoT デバイスからそこに送信しようとすると、IoT デバイス上でクラウド接続用の SDK を組み込んだり、そこに食わせる認証情報の管理が必要となったりします。SORACOM の世界観の通りそれらの面倒な処理全てを肩代わりしてくれるのが SORACOM Funnel です。IoT デバイスは、送りたいデータをそのまま SORACOM Funnel のエントリポイントに HTTP もしくは TCP/UDP で送るだけです。直接 IoT デバイス上のアプリケーションから送信しても良いし、例えば Fluentd が使える環境であれば out-http プラグインが直接使えたりします。

例えば、SORACOM Air で接続した IoT デバイス上からこんな感じで HTTP POST で投げます。

```
$ curl -X POST http://funnel.soracom.io ¥
  -H Content-Type:application/json ¥
  -d '{"foo":"bar"}'
```

そしてこれを SORACOM Funnel の設定で AWS の Kinesis Streams に送るように設定しておくと、Kinesis Streams には以下のようなレコードが送信されます。

```
{
 "operatorId": "OP9999999999",
 "timestamp": 1473322750825,
 "destination" : {
  "resourceUrl": "https://kinesis.us-west-2.amazonaws.com/teststream",
  "service": "kinesis",
  "provider":"aws"
 },
 "payloads": { "foo": "bar" },
 "imsi": "440000000000000"
}
```

payloads の中に送信した JSON が埋め込まれているほか、SORACOM が受信したタイムスタンプ（Unixtime ミリ秒）や、送信に使われた SORACOM Air の IMSI などが含まれて届きます。クラウド側ではこれらのデータを元に送信元を識別して様々な処理を行います。ね、簡単でしょ？

送信先のサービスも、AWS であれば AWS IoT、Kinesis Streams、Kinesis Firehose と一通り、それ以外のパブリッククラウドも Azure Event Hubs や Google Cloud Pub/Sub などイベントストリーミング系に流し込むことができます。他にも、SORACOM の認定済みパートナー各社のサービスに接続することができる Partner Hosted Adapter が用意されています。現在はデータ分析や可視化エンジンなど国内 5 社のサービス

に対応しています。SORACOM 接続の IoT デバイスから容易に送り込めるかは各サービスで支配的な要素になることが予想できるため、今後もどんどん対応サービスが増えて行くことでしょう。

IoT デバイス「あるある」として、技術上の理由やビジネス上の要件によって利用するハードウェアや OS、ディストリビューションに制約がかかることが多々あります。そのような環境の上で、SDK を直接動かす手間を省き極めて軽く標準的なプロトコルだけでクラウドとの連携ができることは、その開発速度の改善に貢献します。数多くの PoC（実証実験）をこなさなくてはならない IoT ビジネスにおいて、開発速度はビジネス上の支配的な要員となります。決して SDK を利用してクラウドに直接通信することが技術的に難しいわけでは無いですが、「そこは自分達のビジネスでは無い」わけで、単純に計算機資源をオフロードするという意味だけではなく、自らの実装量そのものを減らせることが SORACOM Funnel の魅力です。

さらにセキュリティ上の理由としても、IoT デバイスの盗難などを考慮する場合は IoT デバイス毎にアクセスキーなどの認証情報を個別に用意するか、一時的なリスクならば受容できる場合は盗難が発覚したときに即座に認証情報を一括で交換するなどの対策が必要となります。SORACOM Funnel ではクラウド側に対する認証情報を SORACOM 側で持つので、そもそも IoT デバイス上に何かを管理する必要がありません。こういった「考えることを減らす」という方向性のものが私は大好きです。

地味な副産物として、クラウド側の問題でデータ投入に失敗した場合なども、SORACOM 上のマネジメントコンソールで直近 2 週間のログが見られるので、IoT デバイスを触らずにトラブルシュートできるのも嬉しいところです。そもそも IoT デバイスなんてファイルシステムが read-only で書けるのは tmpfs だけとか、書き込める容量が数 MB とかしかないとかザラで基本的に必要なログは外部に転送する必要があったりするわけで、とにかく自分でやることを減らすのが IoT 開発の肝です。

ここまでの 2 つは、IoT デバイスとクラウドを連携させるための橋渡しのサービスでした。残りの 3 つは、SORACOM 自身がクラウド的なサービスを提供するものです。

## SORACOM Endorse

SORACOM のサービスの中でも、地味ながら面白いものの一つが SORACOM Endorse です。

繰り返し述べてきたように、SORACOM Air の 3G/4G で接続されたデバイスは 3G/4G の SIM により暗号学的に正しく認証されています。ですが、大量のデータ転送や通信の安定性を必要とする場合など、3G/4G 回線経由で送受信したくないというケースがあります。そんなとき SORACOM Endorse を使うことで、モバイル通信を経由して認証トークンを発行してもらうことができます。

認証トークンは標準的な JWT（Json Web Token）フォーマットで、SORACOM Air で接続に使われている IMSI や IMEI などのほか、任意の情報を追加することができます。また SORACOM の秘密鍵で署名されているため、そのため認証トークンを別のシステムに持っていても SORACOM の公開鍵で検証することができます。

これを使うと、単体で用意すると高価になりがちな耐タンパー性のあるセキュアエレメントによるデバイス認証を、モバイルデータ通信を経由するかどうかによらず様々な状況で利用することができます。COSR設定も可能なので、ブラウザ等からの直接利用もできそうです。

自分のところではFunnel/Beamで済んでしまって試せていないのですが、システムの実現可能性を広げることができるポテンシャルを感じています。

## SORACOM Inventory

大量生産をするIoTデバイスにおける設定情報の管理や、稼働中のはずのIoTデバイスの状況を把握するためには、これまではBeamなどのクラウド連携機能を使って自前で設定レポジトリやテレメトリ収集システムなどを作る必要がありました。そういった部分をSORACOMが提供してくれるのがSORACOM Inventoryです。技術的には標準規格LwM2M（OMA LightweightM2M）のサーバです。

LwM2Mは恥ずかしながら作者もSORACOM Inventoryの登場まで知らなかったのですが要するに非同期に接続されるIoTデバイス等に向けて設計されたSNMPのようなものと捉えれば良いようです。具体的には、設定値の参照・変更や、非同期に通知されるデバイス側ステータスの変更監視、コマンドの送信などが行えるようです。

正直あまり詳しくないので深くは触れません。

## SORACOM Harvest

最後に紹介するSORACOM Harvestは、SORACOMが提供するサービスの中でもっとも高い層にあるもので、IoTデバイスがSORACOM Funnelなどと同じようにデータを投げると、SORACOM上にデータを蓄積し、可視化できます。簡単なPoCであればもはや外部のパブリッククラウドを必要とせず、むしろSORACOM自身がパブリッククラウドとしての役割を果たしていると言えます。

投げ方とかはSORACOM Funnelと似ているので、内部的にはPartner Hosted Adapterと同じようにSORACOM Harvest Adapterのようなもので送り込んでいるような気がします。

ちょっとした可視化とAPIだけを提供するような「IoTプラットフォーム」が量産されている昨今ですし、なによりIoTデバイス側の開発に重きを置いてクラウド側はデータが見られれば良いようなプロジェクトであればSORACOM Harvestはまさにどハマリだと思います。是非使っていきましょう。ここでも、重要なことは「自分のビジネスと関係無いところは、できるかぎり自分でやらない」ということに尽きます。

SORACOM自身がデータを蓄積し始めたという事は、そのデータを対象とした様々な分析サービスなどを実現できる下地が揃ったと言えます。まだまだアルファベットにはZまでたくさん残っているので、例えばリアルタイムな機械学習で異常検知できるSORACOM Machine Learningだとかそんな感じの手厚い系のサービスも出てくるのかもしれません。

## SORACOM で気軽に遊んでみよう

散々述べてきたとおり、SORACOM の魅力は MVNO の回線に紐付いて提供される高レベルのクラウド連携機能です。従って、パブリッククラウドがそうであるように、実際に触ってみないとその面白さ、便利さを実感しづらいものです。

SORACOM のハンズオンもかなり広く実施されていますが、自分で勝手に遊んでみるのであれば、回線速度も不必要なので 3G で良いですし、古めの docomo 向け中古 USB モデムが 2000 円程度で転がっていたりします。USB モデムでは Windows/Mac のドライバインストール用に仮想 CD ドライブが仕込まれている場合がほとんどなので、あらかじめユーザ（人柱）による検証報告があるものを探すと良いです。

また、最近 LPWA のサービス圏内も拡がっているので、それを試して見るのも良いかも知れません。例えば LoRaWAN GPS トラッカーが 15,800 円で購入できるので、それでそのまま試すことができます。リリースされたばかりですが、Sigfox 対応センサ対応デバイスも 8,478 円とそこそこお手軽に手が出せそうな価格帯です。このような完結した IoT デバイスを買ってきて、SORACOM Harvest でまず可視化してみたり SORACOM Funnel でクラウドに送ってサーバーレス構成で分析してみたりすると、SORACOM が何を狙っているのか実感できると思います。

## 今後の SORACOM 予想

KDDI グループに参加したことで、特に SORACOM の方向性が変わるとは思いませんが、KDDI 自身の世界戦略と絡んで、グローバルなサービス展開の手厚さは変わっていくでしょう。また、KDDI が買収した SORACOM 以外とのシナジーというのはありそうに見えます。あとは、いつ SORACOM Air for 5G/NB-IoT とかそういったものがリリースされるかだけですね。

仮想ネットワークとしては、以前から要望を送っている VPG 上のファイアウォールや、透過プロキシなどに使える L4 レベルの Junction、トラフィック・フローダンプ、そんな感じで既存のネットワーク機能が素直に移植されていくものと思います。

クラウド連携としては夢が尽きないところですが、AWS であることを活かして自分で用意した Lambda との結合や、AWS IoT などデバイスツイン系のサービスの SORACOM 独自提供、スマートフォンの NFC/FeliCa 連携によるユーザ認証、先ほど書いた収集データの分析基盤など、複数の利用者が必要としそうな機能を継続的に貪欲に SORACOM-ize していくのではないかと思います。

Harvest のような単体で完結するサービスについても、管理者がコンソールから見るだけではなく、パートナーとの関係性もありますが、外部 ID 基盤と連携して一般ユーザ向けの画面を提供といった BI ツールの領域に踏み出す可能性もあります。

今後も SORACOM のニューリリースから目が離せなさそうです。

# 私もセキュリティ・キャンプに参加したい！

みなさんは「セキュリティ・キャンプ」をご存知ですか？

セキュリティ・キャンプは、情報セキュリティおよびプログラミングに関する高度な教育を若者に対して実施することで、いわゆる「高度 IT 人材」の発掘と育成を目指そうという事業です。2004 年からスタートし、それから名前や主催組織が紆余曲折ありましたが、2012 年からは現在の民間企業などで構成されるセキュリティ・キャンプ実施協議会と、経済産業省系の独立行政法人情報処理推進機構（みんなだいすき IPA）の共同主催という形をとっています。

セキュリティ・キャンプといっても、アウトドアでキャンプをするわけでは無いです。そのかわり、メインとなる全国大会を始めとした様々なイベントが行われ、それらを総称してセキュリティ・キャンプという事業と呼んでいます。

この記事では、セキュリティ・キャンプについて紹介します[14]。

## セキュリティ・キャンプ 全国大会

毎年 8 月に東京近辺で行われている 4 泊 5 日の合宿イベントで、一般に「セキュリティ・キャンプ」と言った場合にはこの全国大会を指します。だいたい夏コミの直前か直後の週で金曜～土曜が被ることもあります。今年（2017 年）は幸い夏コミ明けの月曜日からのようです。

この後に紹介するように内容の濃さもさることながら、会場までの旅費や当日の宿泊費など受講に関する費用をまるっと出してもらえるということもあり、全国津々浦々から参加者が毎年集うのが全国大会の特徴です。また、5 日間のうち中 3 日間は朝から晩まで講義ということで、こちらも全国津々浦々からセキュリティあるいはコンピュータサイエンスにおける様々な分野の専門家を 50 人以上も集めています。総勢 100 人以上の専門家と専門家の卵が全力でぶつかる場として、ドラゴンボールの「精神と時の部屋」のように言われることもあります[15]。

参加者は 4 月から 5 月末まで募集され、そこから応募内容に基づいて選考されます。ここ数年は 50 人程度でしたが、2017 年から 80 人程度に増員されました。それに伴い、会場も幕張から府中に移動になっています。選考通過者全体では平均年齢が上がっている一方で、2017 年には初めて小学生が選考を通過しました（しかも 2 名！！）。

---

[14] ステマ回避のため最初に書いておくと、2017 年時点で筆者もセキュリティ・キャンプの講師およびプロデューサー（旧トラックリーダー）を担当しています。

[15] そろそろ通じなくなっているという噂も聞きますが……

2017 年から 50 人前後から 80 人前後に大幅に人数が増えたことに伴い、「選択コース」と「集中コース」に大きく分けて実施されることになりました。

## 選択コース

この数年「トラック制」として実施されていた全国大会の形式をそのまま引き継ぐのが選択コースです。

様々な分野の講義（3〜4 時間）が 5 つのトラックで並行して用意され、参加者はそこからどの講義を受講するか希望することができます（部屋や講義体制の都合で必ずしも希望通りにならないこともあります……すみません……）。2 枠もしくは 3 枠を連続で確保し、食事を挟んで最大 11 時間ぶっ続けという「選択ってなんだっけ」という講義もあります。自分が既に得意な分野の講義ばかりを選んでも良いし、あまりよく知らなかった分野に手を出してみるきっかけとしてザッピングするのも良いです。参考までに、2017 年の二日目の時間割を紹介します[16]。様々な分野の講義があるなと感じていただければと思います。

| 時間 | 内容 | トラックA | トラックB | トラックC | トラックD | トラックE |
|---|---|---|---|---|---|---|
| 08:30-12:30 | 専門（1） | **A1**<br>PowerShellベースのマルウェアとその防御手法<br>講師：凌 翔太 | **B1**<br>DOS攻撃用FPGAを作ろう<br>講師：内藤 竜治 | **C1**<br>ブラウザの脆弱性とそのインパクト<br>講師：Masato Kinugawa 西村 宗晃 | **D1**<br>Linuxカーネルを理解して学ぶ脆弱性入門<br>講師：小崎 資広 | **E1~3**<br>BareMetalで遊びつくそうRaspberry Pi<br>講師：西永 俊文 |
| 12:30-13:20 | 昼食 | | | | | |
| 13:30-17:30 | 専門（2） | **A2~3**<br>AIのデータ汚染を検知しよう<br>講師：松田 健 佐藤 公信 | **B2**<br>組込みLinuxクロス開発スタートアップ<br>講師：海老原 祐太郎 | **C2**<br>ID連携と認証基礎<br>講師：林 達也 真武 信和 | **D2~3**<br>カーネルエクスプロイトによるシステム権限奪取<br>講師：木村 廉 | **E1~3**<br>BareMetalで遊びつくそうRaspberry Pi<br>講師：西永 俊文 |
| 17:30-18:50 | 夕食 | | | | | |
| 19:00-22:00 | 専門（3） | **A2~3**<br>AIのデータ汚染を検知しよう<br>講師：松田 健 佐藤 公信 | **B3**<br>PF_PACKETで仮想IP環境を自作してパケットの理解を深めよう<br>講師：小俣 光之 | **C3**<br>Vulsを用いた脆弱性ハンドリングとハッカソン<br>講師：神戸 康多 | **D2~3**<br>カーネルエクスプロイトによるシステム権限奪取<br>講師：木村 廉 | **E1~3**<br>BareMetalで遊びつくそうRaspberry Pi<br>講師：西永 俊文 |

朝の 8 時半（実際にはその前に朝食）には講義開始して夜の 22 時まで詰め込まれているというあたりも「合宿」ならではというところですね（白目）。

[16] https://www.ipa.go.jp/jinzai/camp/2017/zenkoku2017_jikanwari.html

これらの自分で選んだ専門講義のほか、全員が共通で参加する全体講義として「セキュリティ基礎」「特別講演」「BoF」「企業プレゼンテーション」などがあります。1 日目・5 日目は全体講義のみで、中三日は集中講義がメインです。

講義の他にも少人数のグループに分けられて課題のテーマについて 5 日間で議論する「グループワーク」もまた全国大会の重要なイベントです。講義毎に参加者が入れ替わる選択コースで、ずっと同じグループで活動ができる貴重な機会なので有効活用して下さい。ただしグループワークのために用意されている時間は限られ、いかに健康で文化的な生活を保ったままグループワークの準備を進めるかも試されます。

それぞれの講義には、講師のほか 2 名前後の「チューター」が付きます。彼らはセキュリティ・キャンプの卒業生であり、講師よりも受講者に近い立場として、講義だけでなく 5 日間の受講者の生活を朝から晩まで様々な面から支援してくれます。

### 集中コース

2017 年から新しく新設された集中コースでは、3 つのテーマごとに 10 人程度の参加者が 3 日間集中して取り組みます。初回は「言語や OS を自作しよう」「セキュアな CPU を自作しよう」「Linux 向けマルウェア対策ソフトウェアを作ろう」という 3 つのテーマが用意されています。

共通講義やグループワークなどは選択コースと同一とはいえ、一つのテーマを突き詰めていく、いわばもう一つの全国大会が何を成し遂げるのか、今から楽しみです。

## セキュリティ・キャンプ 地方大会

選考倍率が高い全国大会だけでなく様々な機会を提供するため、「セキュリティ・ミニキャンプ in ○○」という地方大会を各地域で実施しています [17]。

誰でも参加が可能な「一般講座」と、25 歳以下の学生のみ参加できる「専門講座」の二日間開催という形態が多く、一般講座の存在が全国大会と最も異なるところです。また、地元の参加者を想定していることもあり、交通費や宿泊費については自己負担であったり一部負担であったりすることもあります。

2016 年度には 9 回実施され、2017 年度にも 10 回予定されています。まだまだ C92 時点で募集中の宮崎・山梨を含めて 8 回応募する機会がありますので、興味を持った方は是非応募してみて下さい。比較的応募者が地域に閉じていることもあり、全国大会と比較して応募倍率などかなり敷居が低いです。2016 年度の地方大会の様子は、@IT にて連続連載 [18]が組まれていたので、そちらを読むとどんな雰囲気か判ると思います。

---

[17] 「セキュリティ・キャンプ九州実施協議会」がある福岡のみ「セキュリティ・キャンプ in 福岡」

[18] http://www.atmarkit.co.jp/ait/series/3922/

## その他のセキュリティ・キャンプ活動

### セキュリティ・コアキャンプ

2017 年全国大会と合わせて、全国大会の OB/OG 向けの成長機会として新しく実施することになった枠組みです。かなりキャッチーなタイトルが並んでいるので紹介しておきます[19]。

> 『中津留勇 マルウェア解析 LIVE 2017 ～CAN'T STOP ANALYSIS～』
>
> 『日帰りバグハンター合宿』
>
> 『キャンプ講師になるためのコンテンツハッカソン』

ちょっと尖りすぎて、応募者ドン引きで出足が悪かったという笑い話もあったりなかったりしました。

### セキュリティ・ジュニアキャンプ

全国大会などは 22 歳以下の学生が対象ですが、さらに若い年代向けのイベントとして中学生以下を対象とする「ジュニアキャンプ」を高知で毎年実施しています。

最近はロボットカーをテーマに、セキュリティを絡めて二日間で RaspberryPi ベースのロボットカーを実際にコースで走らせるところまで手を動かしてもらうという内容になっています。後半は、互いの参加者のロボットカーに「いたずら」をするという擬似的な攻守合戦のような形式で、コンピュータにおけるセキュリティの重要さ、どのような攻撃がありそれからどうやって守るかを、身をもって体験しています。

### セキュリティ・キャンプアワード

セキュリティ・キャンプ全国大会修了生のその後の活動を発表してもらい、修了生同士の活躍を互いに強化していくための枠組みとして、年一回の「キャンプアワード」という場を用意しています。

毎年 50 人前後の「キャンパー」を排出する全国大会ですが、その中でも先進的な活動を継続して続けている人のうち、一次審査を通過した 5 人がその場で最終プレゼンを行い、最終的な賞を授与されます。2017 年 3 月に行われたキャンプアワードの様子が@IT で記事[20]になっています。

正直めっちゃレベル高いです。

---

[19] http://www.security-camp.org/event/corecamp2017.html

[20] http://www.atmarkit.co.jp/ait/articles/1704/11/news011.html

## セキュリティ・キャンプに参加しよう

セキュリティ・キャンプに参加するにはいくつかの方法があります。

### 正攻法で全国大会に応募する

あなたが 2019 年 3 月 31 日時点で 22 歳以下の学生であれば、来年度の全国大会に応募するのが一番の近道です。参加費用を全て負担してもらうことができ、手厚い講師陣による熱い講義をうけることができます。

その一方で、全国大会は応募倍率も高く、その応募課題のレベルも高いのですが、きちんと努力をしてそれを表現できれば通過できるのも事実です。講師陣・修了生からのメッセージ[21]という Togetter にまとまっているので、是非参考にしてください。

上の Togetter にも載っていますが「応募課題への回答は選考担当者とのコミュニケーション」に尽きるので、正誤を恐れず、自分が何を考えてどう手を動かしているのかを書いてください。「解答」だけを端的に書かれても、選考担当者は超能力者ではないので、どんなことを考えている人なのか判らないというのが正直なところなのです。そういう「もったいない」回答が少しでも減ればと思います。

### まずは地方大会に参加する

地方大会は、年齢制限が緩かったり選考倍率が低かったりと、全国大会と比べて参加しやすい傾向にあります。また、交通費をいとわなければ実施回数も多くあります。ちょうど本書が夏コミということもあり、次の全国大会の募集がある 4 月まで待ち遠しい方は地方大会への参加を考えてみてください。2017 年度の応募結果によると選考通過者の 31.7%が地方大会の参加経験者のようで、全国大会に向けたステップとして一定の成果が出ているようです。

また、一般講義については基本的に選考無しでそのまま入れるので、オトナな人は地元で地方大会が行われたときは是非お越しください。

[21] セキュリティ・キャンプ全国大会へ応募する上での講師陣・修了生からのメッセージ
https://togetter.com/li/1104730

## 大人のセキュリティ・キャンプ

基本的に、22 歳だとか 25 歳だとか以下の学生のみが参加できるセキュリティ・キャンプですが、実は大人が参加する方法があります。それが、セキュリティ・キャンプ実施協議会への参加です。実施協議会は、年会費 1 口 50 万円で参加組織を募集しており、会員になると以下のような特典があります。

1. 全国大会の見学と BoF 等への参加
2. インタビューや取材時におけるバックボードロゴ掲示
3. インターンシップの取り組み

そうです、普通であれば学生のみが受講できる全国大会の講義を、会員企業になると堂々と見学することができるのです。あくまで見学ということで学生同等の扱いではありませんが、5 日間の研修費用と考えれば、そこで得られる学生や講師との関係構築などを含めてかなり価値が高いのでは無いでしょうか。

実施協議会の会員企業が増えることで、地方大会を含めた様々な仕組みの自由度が増します。是非、大人の皆様も、会員企業になって全国大会に参加していってください [22]

## おまけ

一年を通してセキュリティをテーマにしたものづくりを行う SecHack365 もよろしくお願いします [23]。

[22] 繰り返しますが、筆者は関係者です。

[23] こちらも筆者は(同上

# Bluetooth mesh ってどうよ

2017 年 7 月 18 日、長いこと蕎麦屋の出前のような状況が続いていた Bluetooth mesh がついに正式発表されました。この記事では、Bluetooth mesh とはいったいどんなものなのか紹介します。

## そもそも Bluetooth のおさらい

歴史も長く言葉や製品自体はありふれている Bluetooth ですが、色々と複雑な経緯があるので Bluetooth mesh の話をする前におさらいです。

Bluetooth は 2.4GHz の周波数帯を利用する無線通信技術です。この 2.4GHz という周波数帯は ISM バンドと呼ばれるものの一つで、本来は電子レンジなど無線通信以外に利用することを目的として確保されています。混信が多いという前提の上で、重要性の低い無線通信にも比較的に自由に利用することが多くの国で認められていることから、コードレス電話や無線 LAN などで活用されています。口の悪い人はこの 2.4GHz のことを「電波のゴミ溜め」などと揶揄したりするようですが、無線 LAN で 2.4GHz 帯と 5GHz 帯を比較したことがある人は実感があるのではないでしょうか。実際にコミケの会場では 2.4GHz 帯は不毛の大地です。

Bluetooth の規格は、3.0 までのもの（クラシック Bluetooth）と、4.0 以降（Bluetooth Low Energy、BLE）で基本的な仕様がまったく異なります。本当にまったくもって互換性がなく規格の方向性も異なるため、クラシック Bluetooth の最新である 3.0+HS と、4.x の両方に対応している機器もあります。どちらも、基本的には「ペアリング」で通信相手を特定して 1 対 1 のコネクション型の通信を行います。

これから紹介する Bluetooth mesh は、BLE ベースの規格です。

## Bluetooth mesh の登場

これまでの Bluetooth は、先ほど書いたとおり 1 対 1 の接続を前提としていました。ところが、1 対 1 の通信を始めるときに、主に通信相手を探したりする用途で「アドバタイジング」という 1 対多の送信をする仕組みが用意されています。

このアドバタイジングのパケットを活用（転用？）したものが、いわゆる「BLE ビーコン」です。Apple が位置測位のために 2013 年に公開した iBeacon をきっかけとして、一気に普及することになりました。技術的には、大昔から存在するアクティブ型の RFID などと同じです。本来の Bluetooth の 1 対 1 の通信の場合は見通しでも 20〜30 メートルぐらいが距離の限界と言われていましたが、短いデータを一方的に繰り返し送信する BLE ビーコンでは見通し 100 メートルぐらいは届いたりします。

これに目を付けた会社がいくつかあり、Zigbee などで既に研究が進んでいた無線メッシュネットワークの技術を BLE アドバタイジングに転用することにしました。そこから紆余曲折あった結果、Bluetooth の高音質オーディオ CODEC「aptX」などの技術をもつ CSR 社（現在は Qualcomm 社が買収）が開発した CSRmesh プロトコルをベースとする形で、Bluetooth mesh として標準規格になりました。

## Bluetooth mesh の特徴

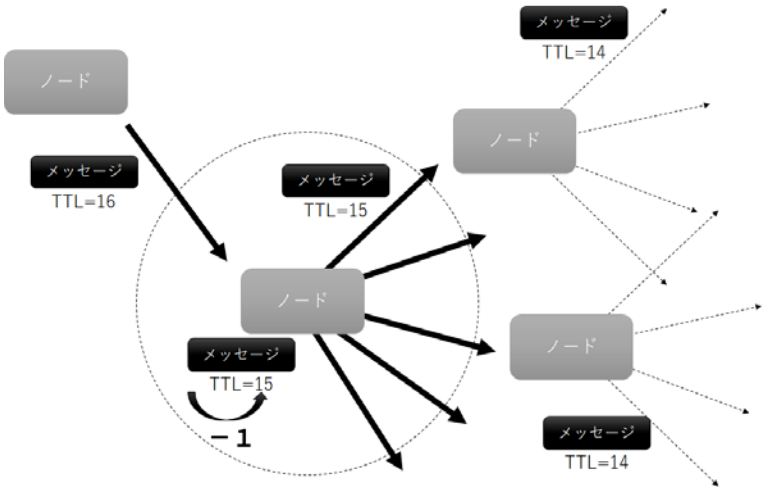
まず一番の基本的な所として、IPv4/IPv6 など他のネットワークプロトコルとの互換性はありません。まったく独自にアドレス体系、ルーティング方式、データフォーマットを持ちます。Bluetooth 4.2 で 6LoWPAN と呼ばれる方式で IPv6 の通信が可能になりましたが、それはあくまでペアリングして 1 対 1 の通信を行うためのもので、この Bluetooth mesh とは全くの無関係です。また、2016 年に発表された Bluetooth 5 とも直接は無関係で、Bluetooth mesh 自体は 4.0 以降の全てと互換性があります。

Bluetooth mesh は、数台から数千台というレンジをカバーするネットワーク規格です。したがって、インターネットのようなグローバルなものではなく、組織や建物など比較的小さいエリアをカバーするためのものです。アドレスは 15 ビット分の長さがあるので、規格上は「3 万 2000 ノードまでサポート」という表現がされているようです。後述するように、数万ノードが相互に大量の通信を継続して行うには向いていないため、用途によりけりと言うところはあります。

メッシュネットワークということで、ルーティングの仕方が一番気になるところだと思います。基本的な考え方は「Managed Flooding」と呼ばれ、いわゆるフラッディング型と呼ばれる方式の一種です。IP ネットワークをご存知の方は「一体何なんだ！その乱暴なネットワークは！」と驚くような手法ですが、以下の組み合わせで動いています。なお、Bluetooth mesh ではデータの単位をパケットではなくメッセージと呼びますが、だいたい同じです。

### 1．誰がどこに居るか気にしない⇒TTL が尽きるまでリレー

IP ネットワークで言うような「経路表」のようなものはもちません。とにかく自分宛でないメッセージを受信したら中継して再送信します。そのときに、メッセージ内の TTL を一つ減らします。TTL の考え方は IP と同じで、最初に送信するときに設定できます。



また、電波ですので指向性とかも気にせず、とにかく TTL が尽きるところまで送られます。TTL が余程低くない限り、基本的に全てのノードが受け取ることになります。これが「フラッディング」と呼ばれる所以です。

### 2．メッセージキャッシュ

先ほどの図で、中央のノードが中継した TTL=15 のメッセージは、左上でも受信できるんじゃないの？と思った方、正解です。そういうループを避けるため、自分が転送したメッセージを全てのノードはキャッシュします。

メッセージ全体をキャッシュするのはさすがに効率が悪いので、全てのメッセージにはシーケンス番号という連番が設定されています。このシーケンス番号と送信者のアドレスのペアをキャッシュして、既に中継したメッセージかどうかを判別します。

この TTL とメッセージキャッシュに基づいて、とにかく「既に宛先に届いたかどうかにかかわらずネットワーク全体にメッセージを行き渡らせる」のが Managed Flooding の方針です。固定した「経路」などをもたないため、ノードが居たはずなのに突然居なくなったり、あるいは増えたりしても、特に何か新しいトポロジ変更のような処理は必要ありません。基本的には、物理的に電波が冗長に届くように配置する前提で、このような割り切りになっています。その分「不必要」なメッセージが飛び交っているため、2.4GHz 帯には余り優しく無いとも言えますが、BLE 自体の通信時間は極めて短いため、それほどでもないようです。

## Bluetooth mesh のセキュリティ

いまどき新しく開発されるプロトコルなので、当然のように暗号学的に正しく設計されています。

Bluetooth mesh は 3 つの鍵で保護されています。そのうち一つはノードがネットワークに参加するときの確認に使われる「デバイスキー」で、残りの二つが実際にネットワーク上を流れるメッセージの内容を保護するための「ネットワークキー」と「アプリケーションキー」です。

メッシュネットワーク上のメッセージは全て、ネットワークキーとアプリケーションキーの二つで、入れ子上に暗号化されています。ネットワークキーは、そのアドレス空間を構成するネットワーク全体で共通のものです。ネットワークキーを知らなければ転送元、転送先を含む全ての情報を知ることができません。Managed flooding の転送処理はこのネットワークキーを復号した状態で行われ、再び暗号化されて無線送信されます。

名前の通りですが、その中のアプリケーションデータを守るのがアプリケーションキーです。この二重構造により、単にリレーだけするようなノードはアプリケーションデータを知ることができません。見通しで 100 メートルぐらい届くことがあるとはいえ、建物の内部などでは数十メートルがいいところですから、アプリケーションとして実際に役割を果たすノードの他に、電球などにリレー専用のノードをばらまくことが考えられます。そのような「メッシュネットワークインフラ」を想定しているのだと思います。

ちなみに、この二重暗号化のモデルどこかで見たことありますね、そうです、本書の前の方で特集しているSORACOMも使っているLoRaWANです。あちらも、ネットワーク全体のキーとアプリケーション毎のキーが分かれています。そもそも長距離でスター型のLPWAと、短距離でメッシュ型のBluetooth meshで似たようなアーキテクチャになってくるのは興味深いところです。

## で、なにができるの？

注意深くプレスリリースや概要資料等では隠されていますが、そもそもBluetooth 4.0でのアドバタイジングは最大で31バイトしか入りません。というわけで、Bluetooth 4.xを使っている限りは実際の転送能力もお察しの通りです。ただし、規制の厳しいサブギガ帯を使うLPWAなどと異なり送信間隔などの制限はない（かわりに混信しやすい）ので、転送能力の総量はLPWAより多くなります。

あくまでBluetooth meshの規格としては、途中のUpper Transport層での暗号化時に380バイトという制限がありますが、それはBluetooth 5以降でのアドバタイジングの長さ拡張が前提となります。Bluetooth 4.xの場合は、パラメータ設定によって異なりますが、だいたい実際のデータ本体としては1回に10バイトぐらいが限界のようです。LPWAと同じく「1ビットは血の一滴」を要求される世界ですね。

実際のメッセージで送ることができるデータは、「Mesh Model」という仕様において「モデル」という枠組みで定義されています。色々と、ありがちなデータのパターンがモデルとして定義されているので、眺めてみると「奴等はこんな利用ケースを想定しているのか」ということが大変よく分かります。というか照明制御好き過ぎでしょ。

たかが1回10バイトでも制約が少なく自由に飛ばせるので、デバイス側で必要な有効数字に落とし込んで送ったりする分には十分ですし、通知や制御にも十分活用ができると思います。LPWA以上に、パズルが楽しい技術ではあります[24]。

[24] そしてステマにならないように書いておくと、筆者の昼のお仕事がまさにBluetoothのメッシュ技術を実用化している会社だったりします。一緒にパズルやってくれるお仲間も募集中です。

# あとがき

「ねこるりは　キンコーズいんさつてくのろじー　をてにいれた！」

というわけで、例によってコミケ当日の午前 3 時に後書きを書いています。これから表紙を作ってキンコーズでセルフ製本してくるというタイミングです。春の技術書典 2 でキンコーズ製本を試しましたが、「100 部で約 90 分間張り付かないと行けない」ということだけ覚悟しておけばとにかく楽です。

今回は大ステマ祭りですが、どれもみんな気になっているトピックだと思いあえて選びました。

書きやすかったからだけじゃ無いよ！

次回は、秋の技術書典 3 で「サーバーレスの厚い本」が、今度こそ出る予定です。

## 電子書籍版について

ライセンスの都合により、一部のフォントを書籍版より変更しています。

「よく飛ばない鳥」のマルセ様による「にゃしぃフォント改二 Version 2.072」を利用しています（http://marusexijaxs.web.fc2.com/）。この場を借りて感謝いたします。


**めもおきば TechReport 2017.08 ＜電子書籍版＞**

**発行日**　**2017 年 8 月 11 日　コミックマーケット 92**
**2017 年 9 月 21 日　電子書籍版**

**著者**　**Aki @nekoruri**
**aki@nekoruri.jp**

**発行**　**めもおきば**
**http://d.hatena.ne.jp/nekoruri/**