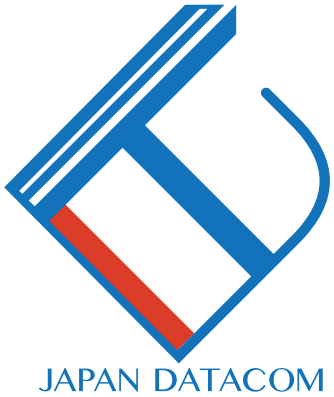


IoTワイヤレスネットワークにおける認証データ量削減と通信効率改善技術の実証実験

第9回テストベッド分科会
2020年9月23日
ジャパンデータコム
今村　祐

研究開発の背景と目的

研究開発の背景

ネットワーク技術やセンサデバイスの進化により、パソコンやスマートフォンなどの従来のインターネット　接続端末に加え、家電や自動車、ビルや工場などの、世界中の様々なモノがインターネットへつながり、その数は爆発的に増加している。今後爆発的に増加するワイヤレスIoTデバイスにおいて、セキュリティを確保　するために、ワイヤレスIoTデバイスの機器認証やデバイスが扱うデータ認証が重要となる。このため、**認証に係る通信トラフィックの増大による無線リソースの逼迫**が想定される。したがって、**セキュリティを確保しつつ、周波数帯域を有効利用する研究開発が望まれる。**

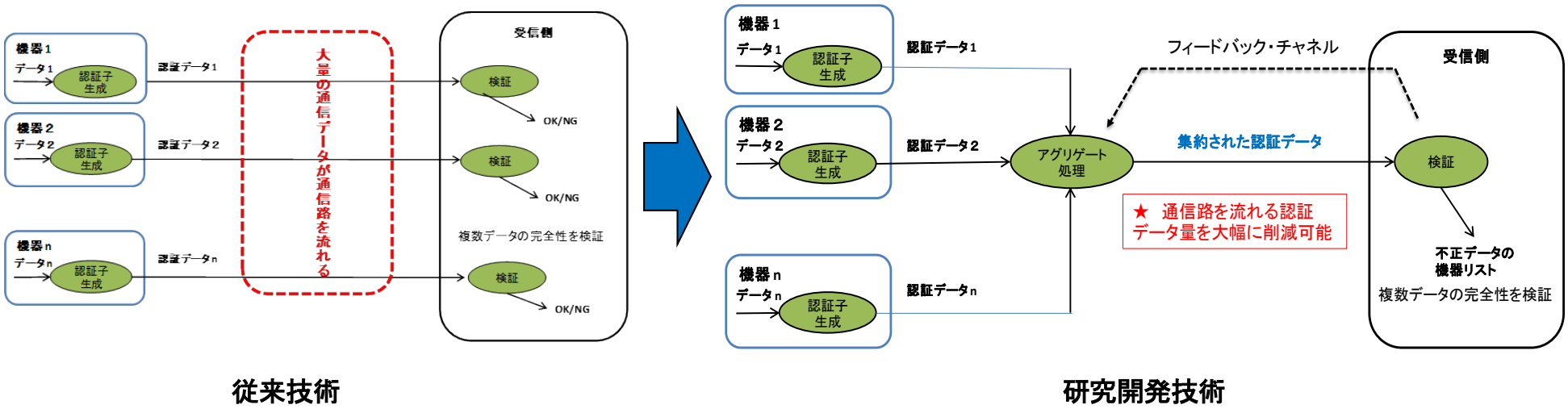
研究開発の狙い

本研究開発では、軽量認証技術、通信効率改善技術を確立し、今後増大するワイヤレスIoTデバイスの機器認証やデータ認証に関わるデータ通信量増大を抑止し、周波数の有効利用に資することを目的とする。IoTデバイスの増加に伴うデータ量の抑制と同時にセンサー系デバイスの出力するデータの信頼性の確保も重要な要素技術となる。データ量の抑制と信頼性の確保の両立を図る方式として、認証に係る通信トラフィックを削減するためのアグリゲート認証方式[1][2][3]が提案されているが、大量の実デバイスを用いた実証実験による動作確認は困難となる。そこで、百単位以上のデバイスを仮想に存在させ、提案方式の検証を行う仕組みの開発と実証をStarBEDを利用して行なった。

[1] S. Hirose, J. Shikata, “Non-adaptive Group-Testing Aggregate MAC Schemes”, The 14th International Conference on Information Security Practice and Experience (ISPEC2018), LNCS 11125, pp. 357-372,Springer, September 2018.
[2] S.Sato, J.Shikata, “Interactive Aggregate Message Authentication Scheme with Detecting Functionality”, Proc. of The 33-rd International Conference on Advanced Information Networking and Applications (AINA2019), pp. 1316-1328, Springer, March 2019.
[3]佐藤慎悟, 四方順司, “追跡機能付き対話型アグリゲートメッセージ認証コードの再考”, 2019年暗号と情報セキュリティシンポジウム (SCIS 2019), 大津, 2019年1月.

アグリゲート認証技術の概要

アグリゲート認証技術とは，横浜国立大学四方教授ら[1][2][3]によって開発された技術で、送信側において多数のIoT デバイスのメッセージにそれぞれ付加されたメッセージ認証子（MAC: Message Authentication Code，Tagとも言う）を集約（アグリゲート）して送信することにより，通信路の利用効率向上を図る技術である．不正メッセージが一つでも存在する場合には，それを検出し、さらにそのメッセージを発生したデバイスを（ある定められた個数以下であれば）特定することも可能である。



従来技術　　**研究開発技術**

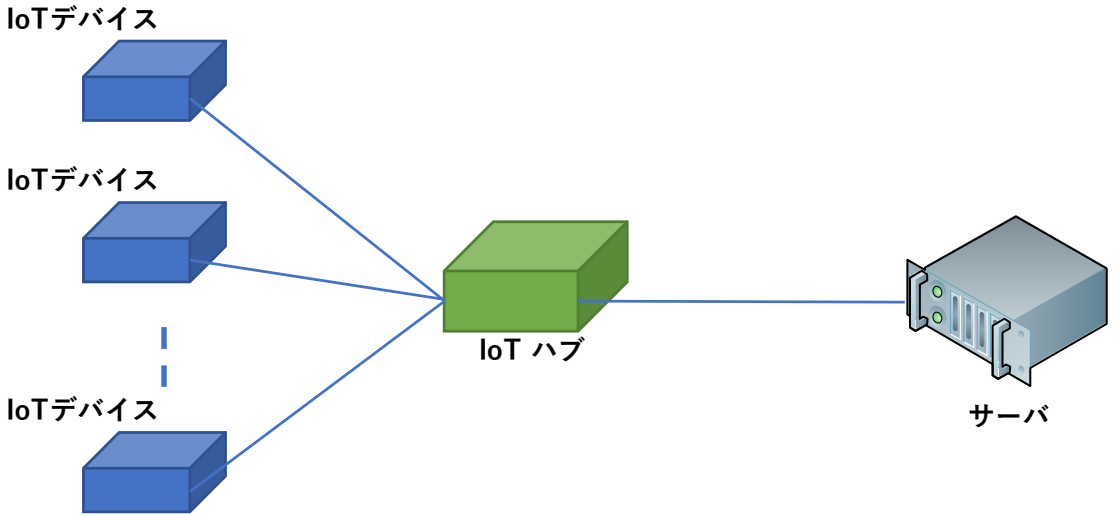
[1] S. Hirose, J. Shikata, “Non-adaptive Group-Testing Aggregate MAC Schemes”, The 14th International Conference on Information Security Practice and Experience (ISPEC2018), LNCS 11125, pp. 357-372,Springer, September 2018.

[2] S.Sato, J.Shikata, “Interactive Aggregate Message Authentication Scheme with Detecting Functionality”, Proc. of The 33-rd International Conference on Advanced Information Networking and Applications (AINA2019), pp. 1316-1328, Springer, March 2019.

[3]佐藤慎悟, 四方順司, “追跡機能付き対話型アグリゲートメッセージ認証コードの再考”, 2019年暗号と情報セキュリティシンポジウム (SCIS 2019), 大津，2019年1月.

アグリゲート認証技術の実装モデル

圧縮率可変アグリゲート認証技術は、あるIoTシステムに大量にデバイスが存在する時、ネットワーク内で信頼できるデータを効率的に送信する必要がある場合に有効性を発揮する。そのため多くの人が集う場所で、かつサービスを受け取るための認証が必要となる場面を検討した結果、多くの人が集まるテーマパーク、レジャーランド等を想定するユースケースとした。その上で以下の実装モデルを策定した。

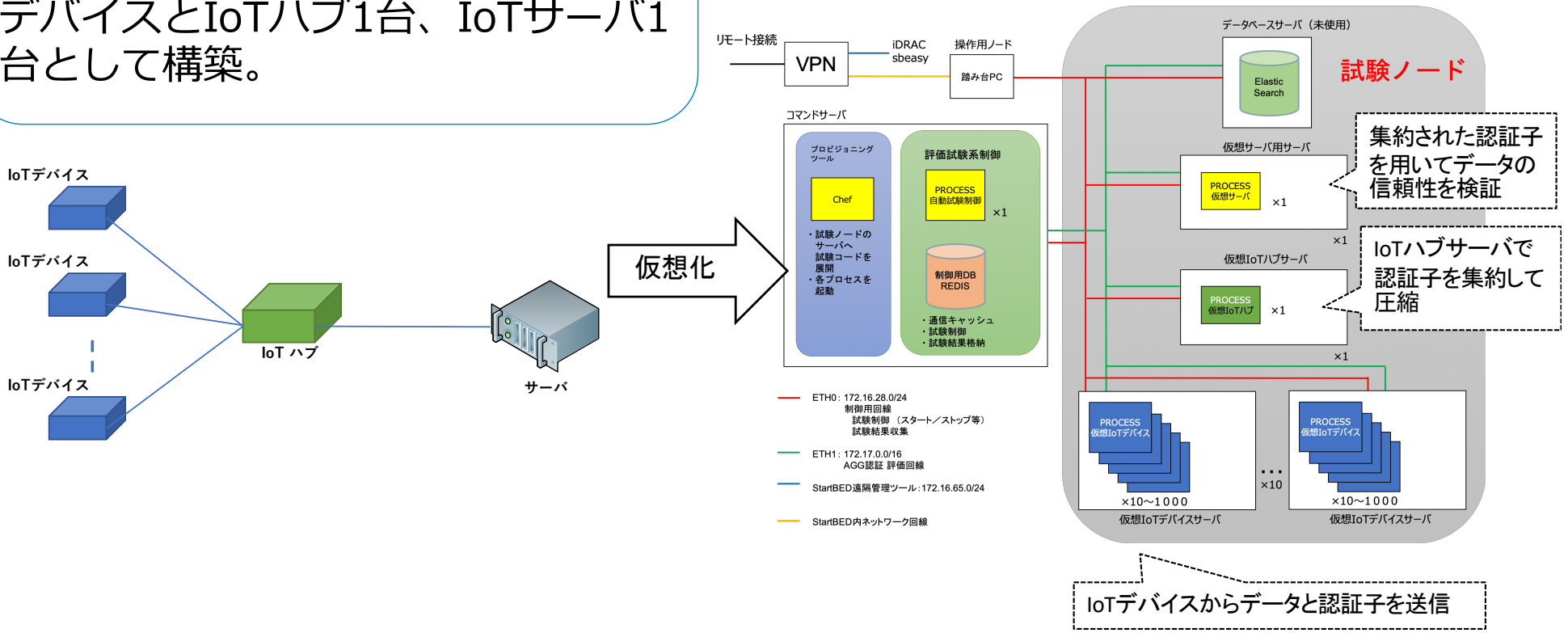


圧縮率可変アグリゲート認証技術の実装モデルの仮想化

物理構成では実現が難しい大量のIoTデバイスでの実験をStarBED上で仮想化し100台～1万台規模のIoTデバイスとIoTハブ1台、IoTサーバ1台として構築。

StarBED利用規模
物理ノード20台
仮想ノード~1万台

StarBEDでの実装システム



圧縮率可変アグリゲート認証技術のシミュレーション結果

◆シミュレーション条件

- NICTのStarBED上でシミュレーションを実施。端末は，17byteのヘッダ，20byteのデータおよび32byteのMAC（認証子）からなる69byteのパケットを送出
  - 端末数n=100,n=1,000およびn=10,000の通り
  - IoTハブ、サーバとも1台のN:1:1の構成
- d-disjunct行列を用いてフィードバック無しのアグリゲート認証方式をIoTハブに実装

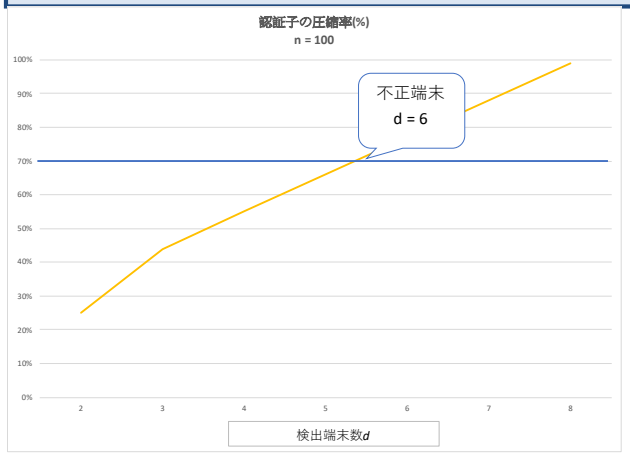
◆実装と性能評価

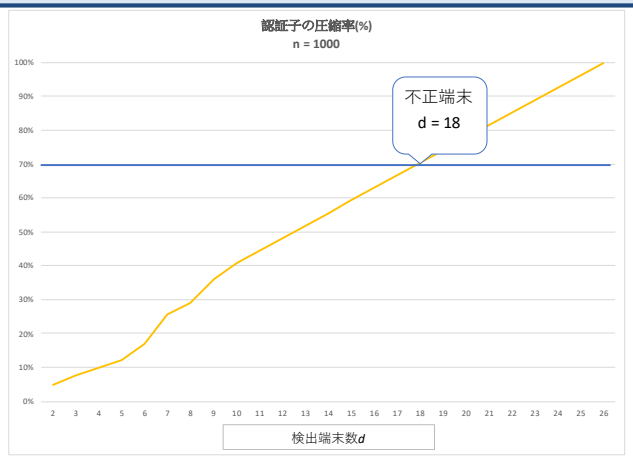
圧縮率可変アグリゲート認証技術を用いて**仮想環境を用いた大規模の実証評価**を行った。

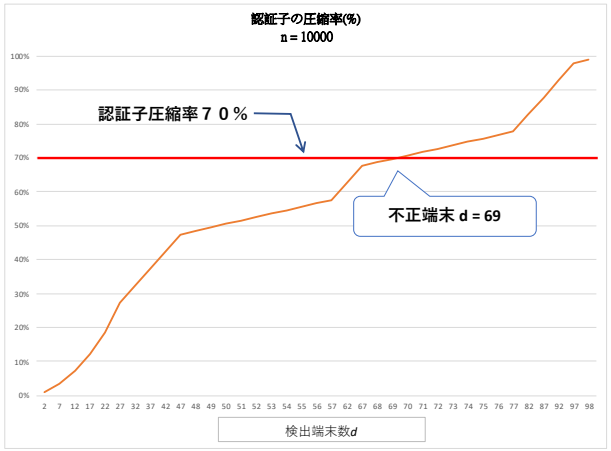
仮想環境を用いた実証評価では擬似的にIoTデバイス通信を行うためにLinux OS上で動作する実装モデルの開発を行い、横浜国立大学から提供されたDisjunct Matrix（以下、「行列」と呼ぶ）を用いたフィードバックなしのアグリゲート認証技術をIoTデバイス上に実装した。また、擬似的にIoTハブ通信およびIoTサーバー通信を行うために、LinuxOS上で動作する実装モデルの開発を行い、性能評価を実施した。

IoTデバイスからのデータ送信タイミングを調整、送信パケットの衝突を回避し認証子の削減効果を確認した。

IoTハブへ入力される認証子（MACタグ）数と、IoTハブから出力される集約された認証子（MACタグ）数を比較。







実証システムの目的

- アグリゲート認証技術の有効性の確認
  - 認証データの削減による通信量の削減
  - シミュレーション結果[4]の検証

- 実用化に向けた課題抽出

  例えば
  - IoTデバイス数のダイナミックな変動

[4]山岸他, “アグリゲートメッセージ認証方式の実装と評価”, 信学技報, vol.118, no.486, ICSS2018-73, pp.29-33, 2019年3月

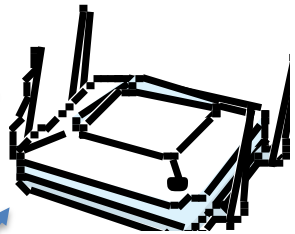
想定するサービス

（DF AMAC)

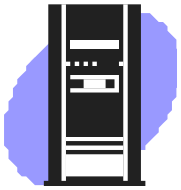
IoTデバイス

IoTデバイス

IoTデバイス



IoTハブ



サーバ

- IoTデバイス→サーバ＞デバイス数の増加に比例して通信量が増加
- DF AMACを適用し、通信量を削減

IoTデバイス：定期的に“状態”をサーバーに送信
サーバ：“状態”に対応したコンテンツを配信

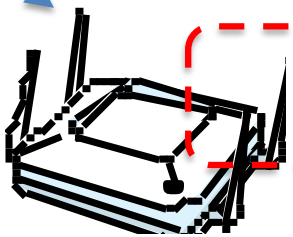
想定するサービス

（DF AMAC)

IoTデバイス

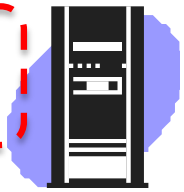
IoTデバイス

IoTデバイス



IoTハブ

DF AMACの適用箇所

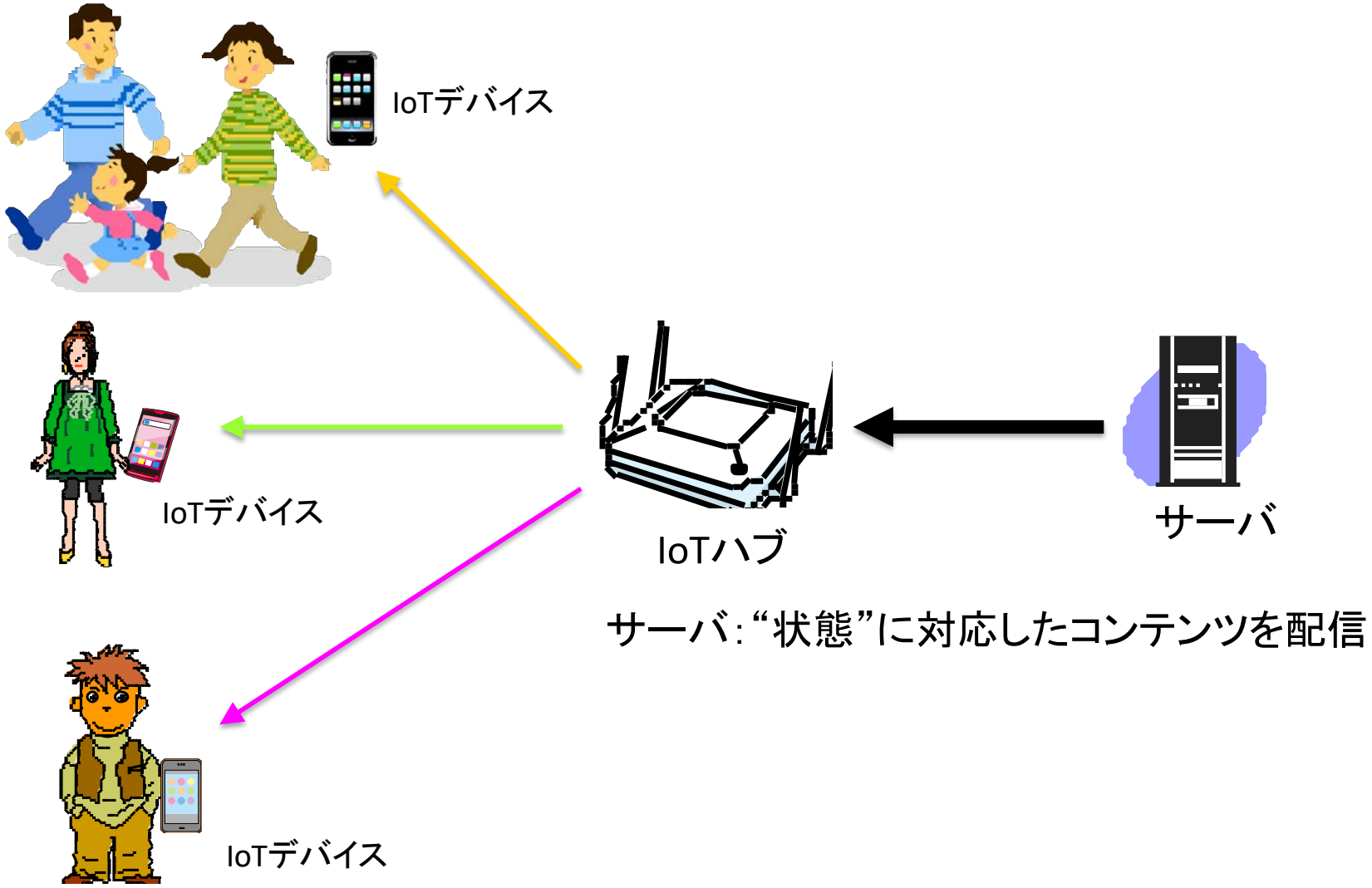


サーバ

IoTデバイス：定期的に“状態”をサーバーに送信

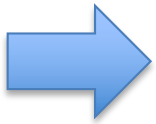
想定するサービス

（DF AMAC)



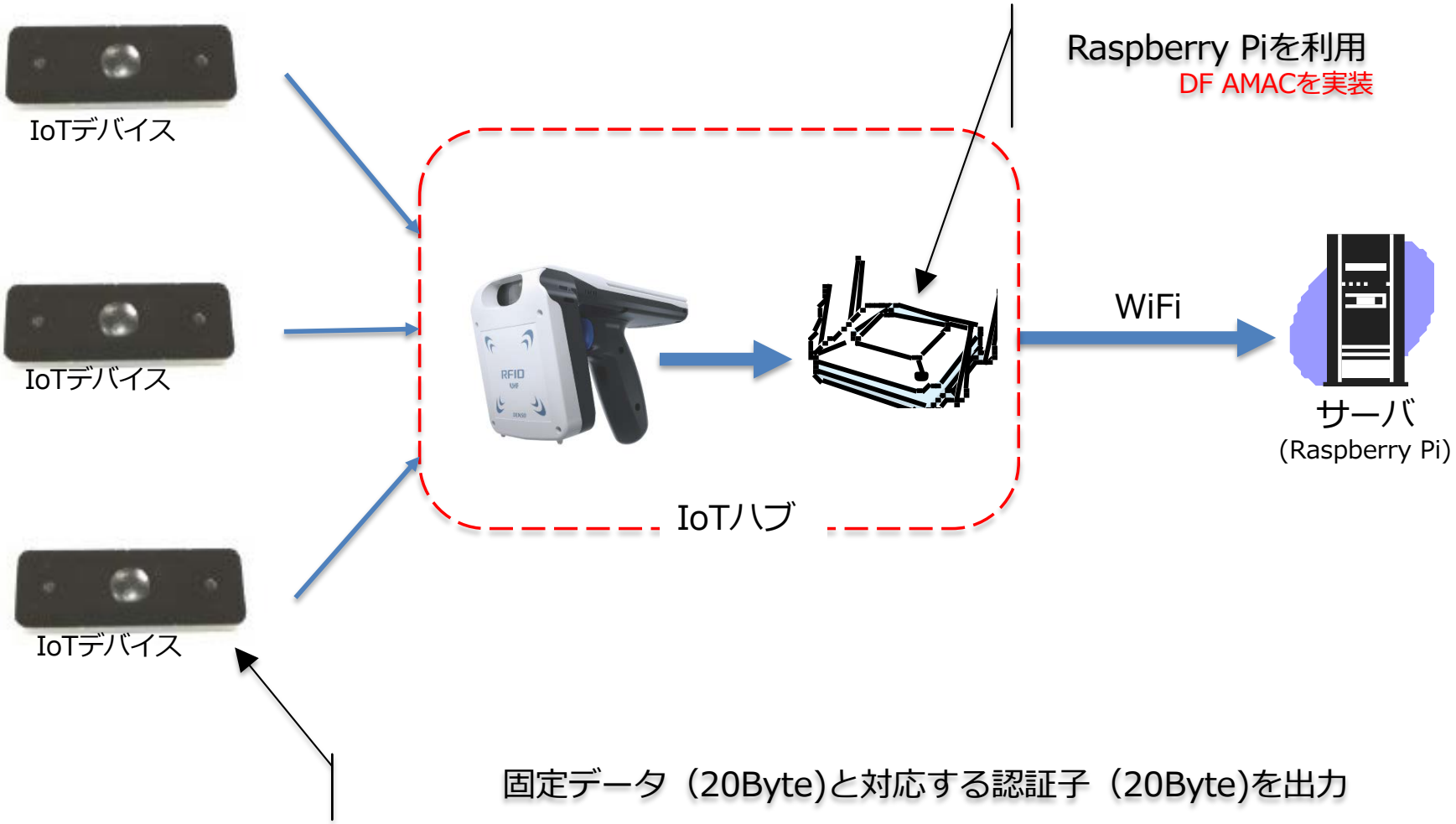
想定する実証システム

- 位置情報などの、短い情報を扱う
  - IoTデバイスは、データ送出機能が必須
- IoTデバイス数は、ある程度多い
  - 実証システム構築に対する制約
    - 一定数のIoTデバイスを準備する必要がある
  - 具体的なアプリケーションは構築しない



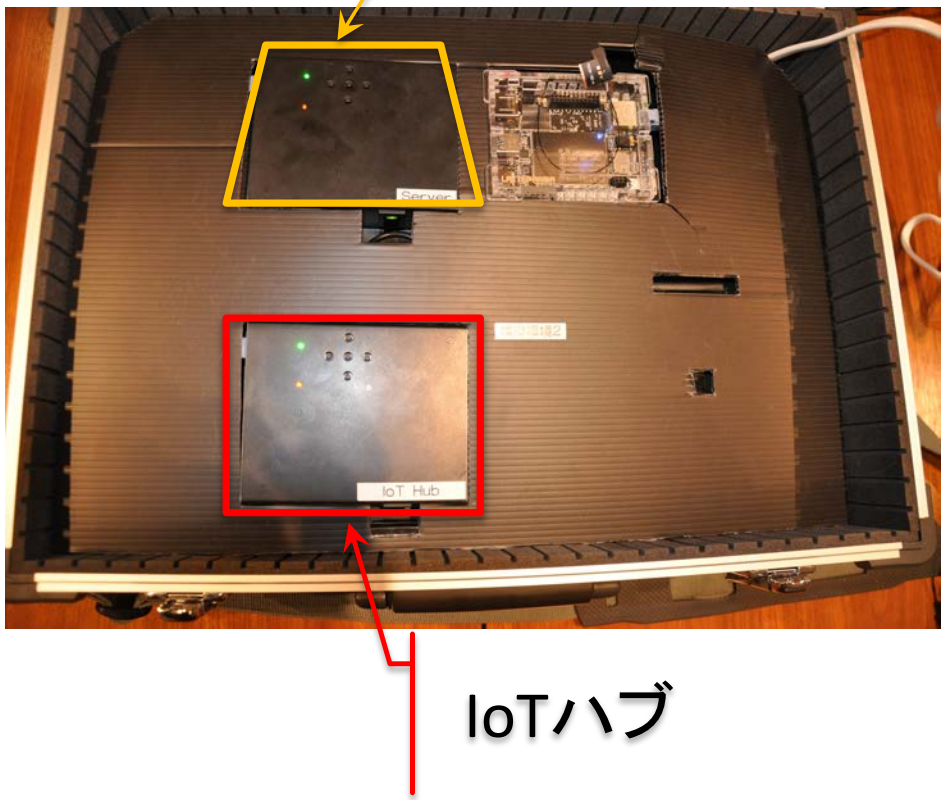
IoTデバイスをRFIDで模擬する

実証システム

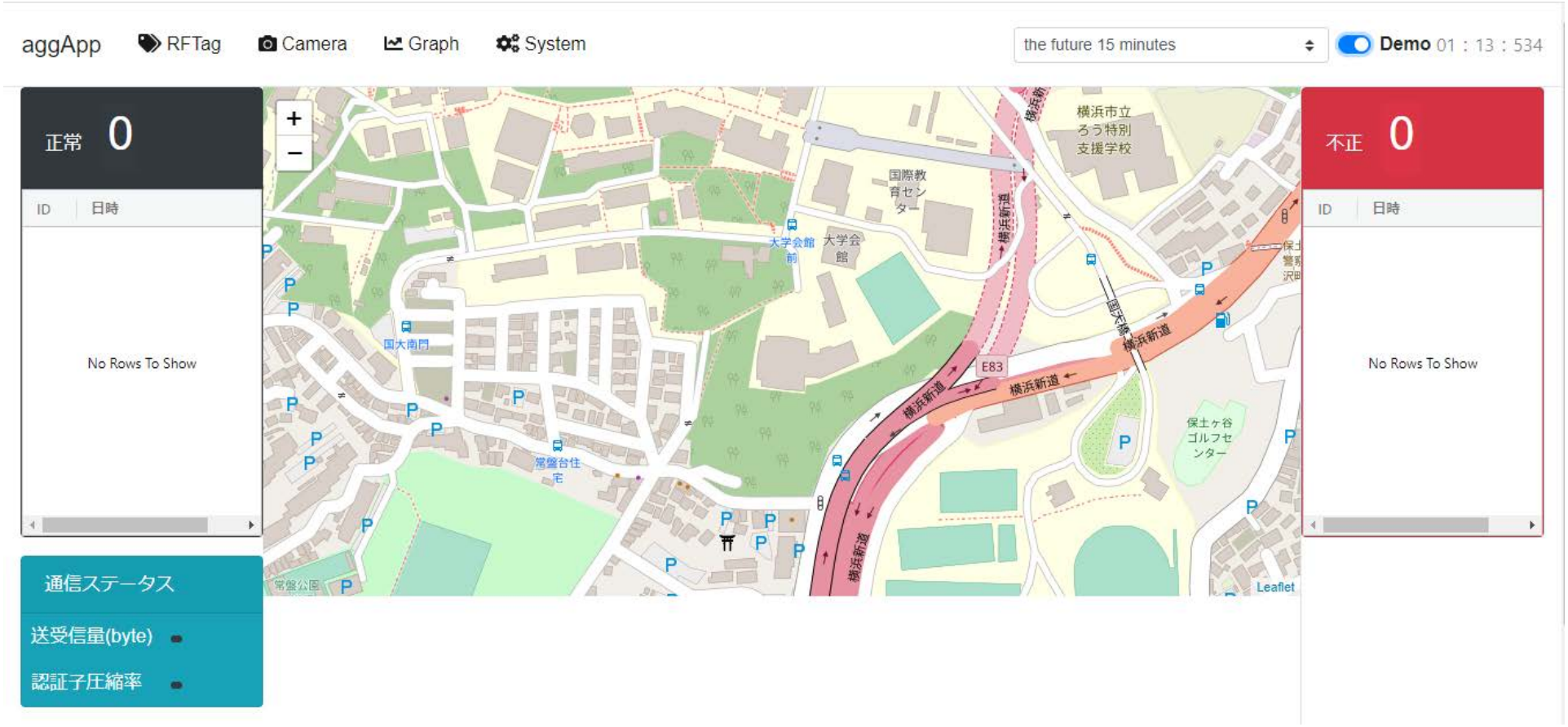

IoTデバイス
IoTデバイス
IoTデバイス
Raspberry Piを利用
DF AMACを実装
RFID
WiFi
サーバ
(Raspberry Pi)
IoTハブ
固定データ（20Byte)と対応する認証子（20Byte)を出力

実証システム（概観）

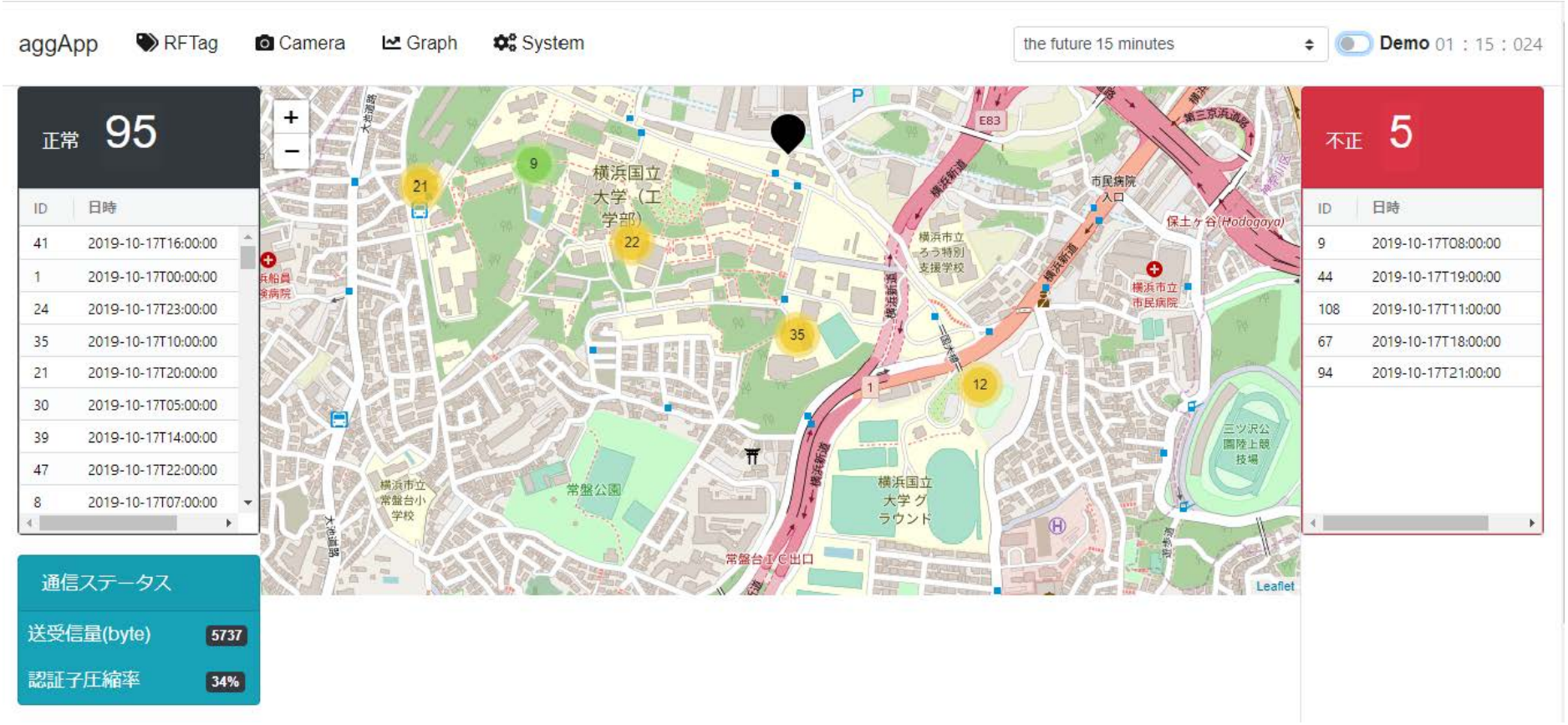
IoTデバイス



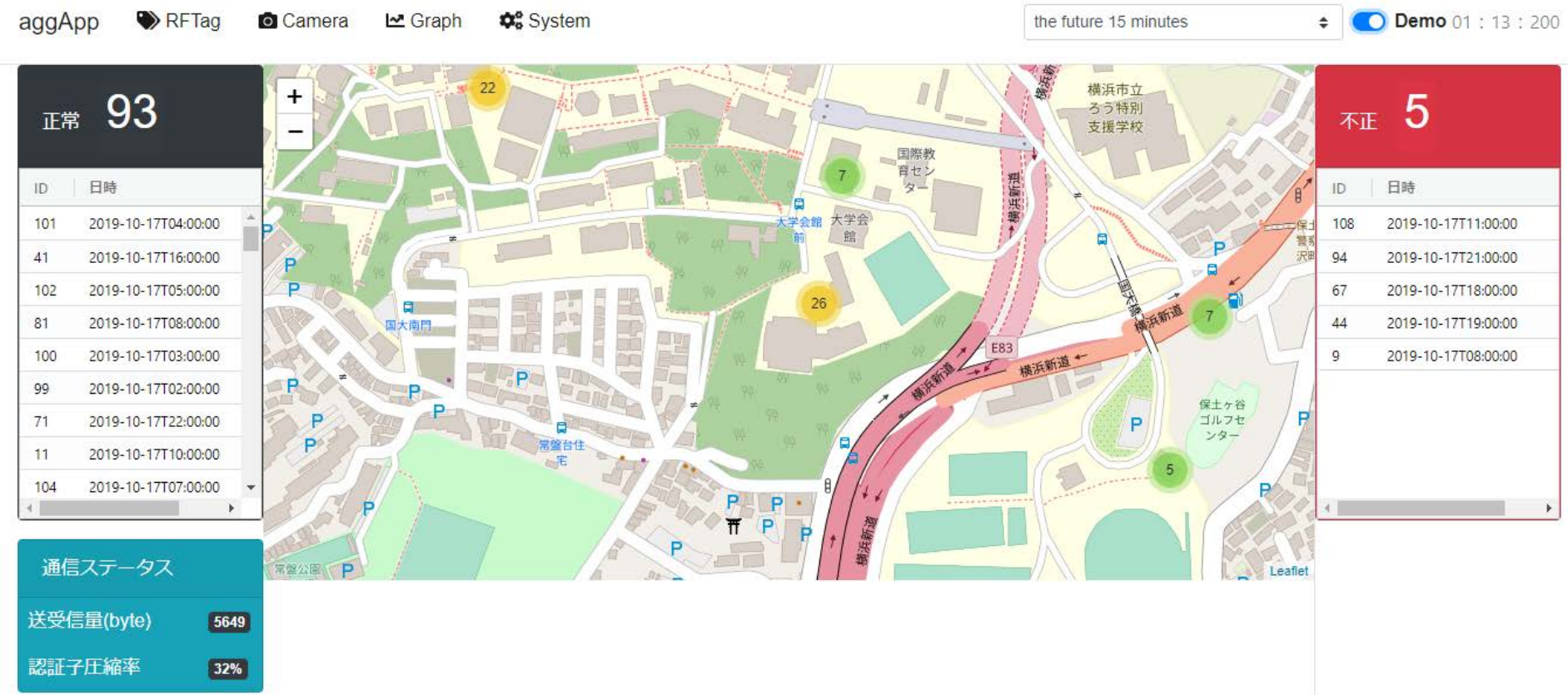
実証システム（画面）


aggApp
RFTag
Camera
Graph
System
the future 15 minutes
Demo 01 : 13 : 534
正常 0
ID
日時
No Rows To Show
不正 0
ID
日時
No Rows To Show
通信ステータス
送受信量(byte)
認証子圧縮率
横浜市立
ろう特別
支援学校
国際教
育セン
ター
大学会館
前
大学会
館
国大南門
常盤台住
宅
常盤公園
E83
横浜新道
保土ヶ谷
ゴルフセ
ンター
Leaflet

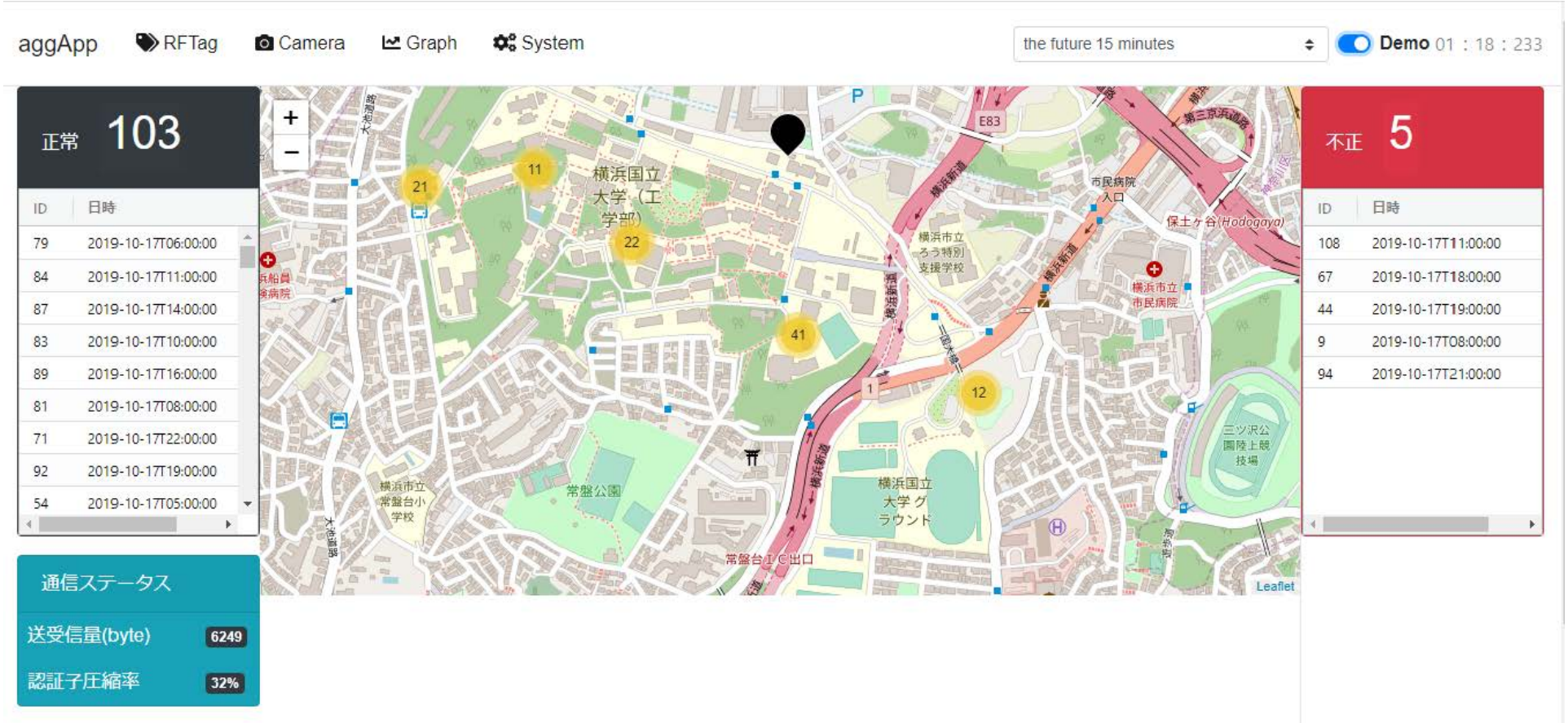
デバイス数(N)=100
不正デバイス(d)=5



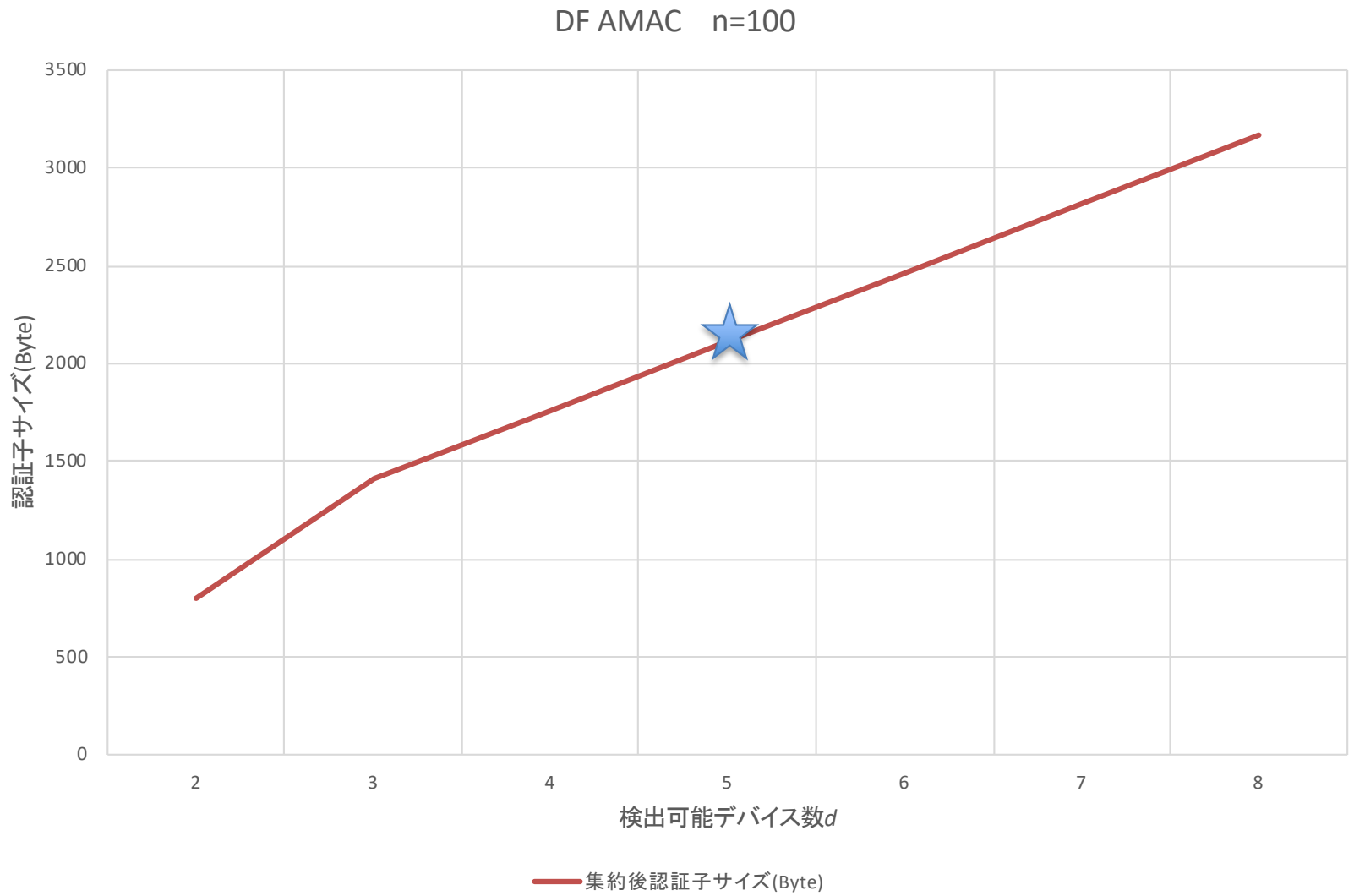
デバイス数(N)=98
不正デバイス(d)=5



デバイス数(N)=108
不正デバイス(d)=5



シミュレーション(StarBED) vs 実証システム
デバイス数n=100



まとめ

- アグリゲート認証方式[1][2][3]を用いたシステムをStarBED上に実装
- 100台～１万台規模のデバイスで模擬的に通信を行い、提案方式による認証子圧縮機能の効果を検証。
- 様々なパラメータに対して、ワイヤレス環境を流れる通信量を測定することで、認証子の削減度合いを解析し、認証子を30%削減するためのパラメータを明確にした。[4]
- 1万台のデバイスから1万個のデータが送信される時、不正データの数が69個未満であれば認証子を30%削減可能
- StarBEDでの検証結果が実デバイスを用いた実証システムとの結果と一致していることを確認できた。従って、StarBEDで実施した総端末数(n)と検出可能な不正端末数(d)のシミュレーション結果（n=1000、n=10,000のとき）は、実際のシステムでも実現可能であることが確認できた 。

[1] S. Hirose, J. Shikata, “Non-adaptive Group-Testing Aggregate MAC Schemes”,The 14th International Conference on Information Security Practice and Experience (ISPEC2018), LNCS 11125, pp. 357-372,Springer, September 2018.
[2] S.Sato, J.Shikata, “Interactive Aggregate Message Authentication Scheme with Detecting Functionality”, Proc. of The 33-rd International Conference on Advanced Information Networking and Applications (AINA2019), pp. 1316-1328, Springer, March 2019.
[3]佐藤慎悟, 四方順司, “追跡機能付き対話型アグリゲートメッセージ認証コードの再考”, 2019年暗号と情報セキュリティシンポジウム (SCIS 2019), 大津，2019年1月.
[4]山岸他, “アグリゲートメッセージ認証方式の実装と評価”，信学技報, vol.118, no.486, ICSS2018-73, pp.29-33, 2019年3月.

謝辞

本研究は、総務省「電波資源拡大のための研究開発」のうち「IoTワイヤレスセキュリティ通信における周波数有効利用技術に関する研究開発」の委託研究の成果です。本研究プロジェクトの評価委員の先生方を始め有益なアドバイス、示唆をいただいた関係各位に深く感謝いたします。

また、研究開発の一環としてNICT総合テストベットを利用させていただきましたことに深く感謝申し上げます。