

[Work in Progress] 研究報告

# 広域分散センサ群を対象としたIoTテストベッドの設計

寺田 直美<sup>1,a)</sup> 齋藤 修一<sup>2,1,b)</sup> 河合 栄治<sup>1,c)</sup>

## Designing an IoT Testbed for wide-area distributed sensors

### 1. IoT テストベッドサービス

デジタルトランスフォーメーションの拡大により、2020年には、530億個のIoTデバイスがインターネットに接続されるとされている [1]。研究開発成果を実サービスに展開する前段階、あるいは研究の実用性を示す際に、実環境に近い環境で実験可能な公開テストベッド環境は有用である。

NICTでは国内外に拠点を展開するL2テストベッドサービスJGN、その上にSDNテストベッドRISE [2]を構築し、研究開発目的のユーザが利用可能な実験環境を提供している。今回はこれらのサービスの発展としてIoTテストベッドサービスについての検討を行った。

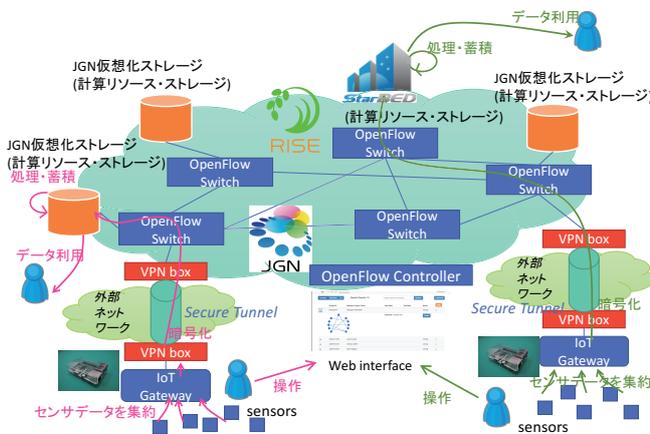


図1 IoT Testbed

### 2. IoT テストベッドに求められる機能と設計

IoT環境下では各種デバイスから得た情報を収集、計算リソースへ送信し分析することになるが、IoTデバイスは数も膨大でデータ量もさまざまである。また、IoTデバイスを収容するエッジ側機器で処理、蓄積したデータを計算リソースまで運ぶためのコネクティビティが必要となる。

データについては、エッジ側での処理、クラウド側での処理および双方での分散処理が考えられるが、今回は既設

のクラウド計算リソースおよびストレージを利用する前提で、データを安全にエッジからクラウドへ伝送する点に主眼を置いた。この際、データに適した計算リソースやストレージを選択できる必要がある。

広域に実証実験可能なテストベッドサービスを提供するにあたり、IoTデバイスのセキュリティも重要となる。具体的には安全な通信路の確保、IoTデバイス自身のセキュリティが考えられる。IoTデバイスはさまざまな環境から複数の外部通信路を経由してクラウドへアクセスするため、エッジからクラウドの間で安全な通信が求められる。個々のIoTデバイス自体のセキュリティについては今回対象としていないが、今後の課題とする。

また、テストベッド環境では複数のユーザの同時利用が前提となるため、IoTサービスやユーザ毎に仮想的に分離可能なマイクロセグメンテーション化を実現しなければならない。

これらを踏まえて、今回以下の機能をサービス実装する。

- 通信路のセキュリティ確保
- データ特性に応じた柔軟なリソース選択
- 複数のユーザに対するサービスの同時提供

図1に示すよう、通信路のセキュリティ確保にはセンサ設置環境とクラウドにVPN接続装置を設置、暗号化通信を行うことで、外部ネットワーク部分の通信安全性を実現する。クラウド内での通信はJGN上でマルチテナント化されたSDNにより、仮想的にユーザを分離し、個々のユーザが独立して通信路の制御が可能な実験環境を提供する。ここでは各ユーザがコントローラから通信路を制御できるため、データの特性、大きさ、地理的条件などに応じて、クラウド上の最適なりソースを選択できる。これにより、データをエリア毎に集約し分散的な処理を実現したり、長期的なデータ保管をバックアップして配置するなどの処理が可能となる。またコントローラはSDN/OpenFlowスイッチ群と同様にユーザのVPN接続装置の管理が行えるため、ユーザはセンサからクラウド側リソースまで一元的に制御でき、スムーズな実験運用が実現できると考える。

### 参考文献

[1] 総務省. 平成27年版情報通信白書, 2015.  
[2] Yoshihiko KANAUMI, Shuichi SAITO, Eiji KAWAI, Shuji ISHII, Kazumasa KOBAYASHI, and Shinji SHIMOJO. Rise: A wide-area hybrid openflow network testbed. *IEICE Transactions on Communications*, Vol. E96-B, No. 1, pp. 108–118, 2013.

<sup>1</sup> 国立研究開発法人 情報通信研究機構  
<sup>2</sup> 日本電気株式会社  
a) naomi-te@nict.go.jp  
b) s-saitou@aj.jp.nec.com  
c) eiji-ka@nict.go.jp