講演番号：4

パーソナルデータサービスのセキュリティ向上化の検討

B－7　　Study of a personal data service for improving security

小杉　隆†　宮保　憲治†
Takashi KOSUGI†　Noriharu MIYAHO†
† 東京電機大学情報環境学部情報環境学科
† School of Information Environment, Tokyo Denki University

1. はじめに

近年 PDS(Personal Data Store)[1]と呼ばれる個人情報の管理技術が進展している．PDS はパーソナルデータを本人が運用管理し，他者と共有できる仕組みである．従来は事業者ごとに各個人データを収集し，そのデータを各事業者が管理する方法が一般的であった．しかしながら，PDS ではパーソナルデータの管理権は本人が持ち，外部への利用許可も，本人による管理を可能とする特徴を持つ．IoT の発展によって個人に関わる情報が増大すれば，PDS の重要性も一層高まると考えられる．PDS サービスを開発する際の重要な課題は十分なセキュリティの確保と経済性である．

本稿では，PDS を活用したサービスの安全性を，個人データのストリーム暗号化と空間的撹拌処理を行う HS-DRT(High Security - Distribution and Rake Technology)[2]により達成する方法を提案し，性能評価行った結果を述べる．IoT アクセス回線としては経済的な LPWA の一つである Sigfox 無線回線を利用した．

2. 提案方式

図 1 に，提案する PSD サービスの構成を示す．

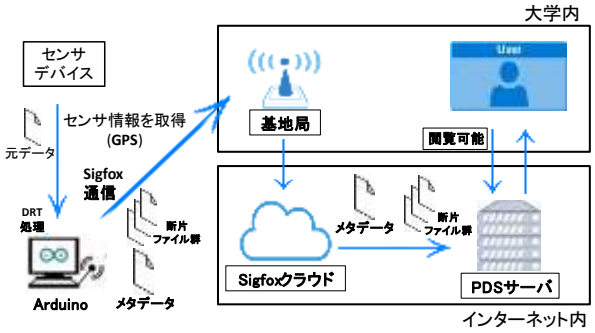

図 1. 提案する PDS サービスの構成

提案サービスでは，センサ接続端末として Arduino を用い，パーソナルデータをセンサ群より取得する．その後，Arduino 内で HS-DRT 処理を行い，生成された断片データとメタデータを，接続された Sigfox 端末を用いて順次送信する．Sigfox を用いて送信された断片データとメタデータは Sigfox の基地局とバックエンドクラウドを介し，PDS サーバに転送・収集される．PDS サーバではユーザからの閲覧リクエストを受信する度に，メタデータを元に断片ファイルを収集し，復号処理を行った後に表示する．

3. 性能評価実験

実験用システムとして，JavaScript，C++などを用い，当該の暗号化処理機能を搭載したセンサデバイス及び PDS サーバを開発した．その後，Sigfox 端末から送信されたパーソナルデータの各断片が，PDS サーバに到着し，元のパーソナルデータに復号されるまでの伝搬遅延時間を計測・評価した．

図 2 に HS-DRT 処理時の分割数に応じた，システムの伝搬遅延時間の計測結果を示す．この実験結果により，伝搬遅延時間は，分割数の回数に応じて、ほぼ比例して増加することが判明した．この理由は、断片データ数が増加することに伴って，Sigfox 送信回が増加し、Sigfox による通信時間が増大するからである．

一方，９５％信頼度区間の算出結果より，伝搬遅延時間のばらつきは殆ど無いことがわかり，伝番遅延時間の大半は，前述の Sigfox 送信間隔に大きく依存していることが判明した．

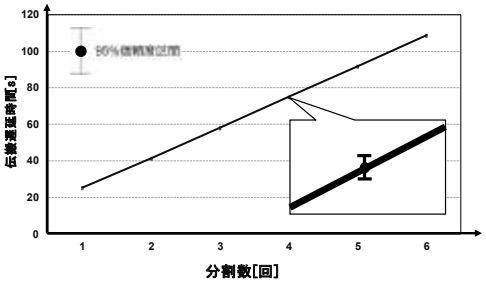

図 2. 分割数と送信遅延時間の相関図

4. まとめ

本稿では，HS-DRT 技術と Sigfox 通信を併用した，セキュアかつ経済的な PDS サービスを提案し，提案方式の性能評価を行った．今後は，ユーザが使用する Sigfox 用端末とアンテナ数を増やすことにより，ユーザの多様な個人情報をマルチメディアの形態で安全に伝達・保管し、その際の伝搬遅延時間の短縮化を検討する予定である．

参考文献

[1] Gordon Bell, “A Personal Digital Store”, Communication of the ACM, 44:pp.86-91, 2001
[2] N.Miyaho, et.al., ” 広域分散ネットワークを活用したディザスタリカバリシステムの実用化”, 電子情報通信学会論文誌 BVol.J97-B No.8 pp.583-598, ,2015.