セキュアIoTプラットフォーム協議会

# パーソナルデータ･ストア（PDS）部会活動報告

2024/3/6

セキュアIoTプラットフォーム協議会PDS部会
座長　田中宏和

# 参加企業

- サイバートラスト株式会社
- 大日本印刷株式会社
- TIS株式会社
- トッパン・フォームズ株式会社
- 株式会社ミルウス
- 株式会社ラック
- 株式会社リーディングエッジ

座長　　広島市立大学 田中宏和 教授
副座長　株式会社ミルウス 南重信 社長

# 目次

- PDS部会の設立背景と紹介
- 今年度の活動報告
  - 分散型PDSの認証をおこなうためのガイドライン策定に向けた検討項目の洗い出し.
    - セキュアにセンサデータを蓄積・管理する仕組みの定義、
    - サービス定義書/制御つきIoTデータコンテナ（IEC63430）の定義
    - ユーザデータ提供に関する本人同意プロセスの定義

# 目次

- PDS部会の設立背景と紹介
- 今年度の活動報告
  - 分散型PDSの認証をおこなうためのガイドライン策定に向けた検討項目の洗い出し.
    - セキュアにセンサデータを蓄積・管理する仕組みの定義、
    - サービス定義書/制御つきIoTデータコンテナ（IEC63430）の定義
    - ユーザデータ提供に関する本人同意プロセスの定義

# 部会設立の背景

センサーを介して個人の医療データ、ライフログ(睡眠、食事、運動などの記録)の利用機会が増えている。収集されたデータをスマートフォン、サーバーなどに安全に保管し、本人の意思に基づき、セキュアに流通させる仕組みの標準化に取組み、管理の安全性と流通の利便性の両立に貢献する。

# PDSにおける昨今の課題と対策

- PDSにおける課題
  - 自らのデータのセキュリティ，プライバシーに関する不安
  - 自らのデータを把握・制御できない不安

※データ流通環境整備検討会「AI、IoT 時代におけるデータ活用ワーキンググループ中間とりまとめ（案）」

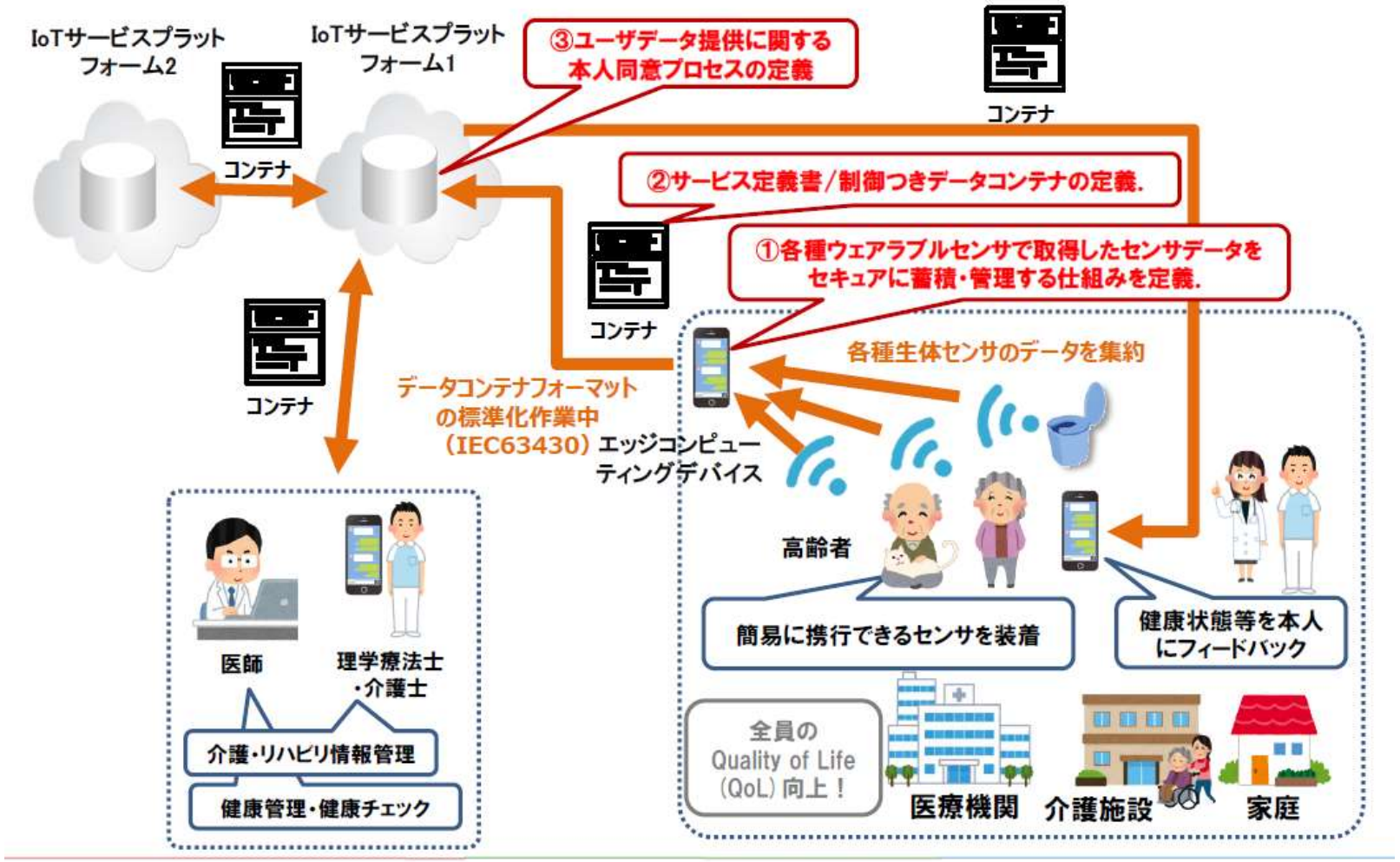
- セキュアなセンサデータストアシステム（SDS）の実現
  - AALユーザ（IoTユーザ）が自らの生体センサ等で取得したセンサデータをスマホやタブレットなどのエッジコンピューティングデバイスでセキュアに保存・管理するためのシステムを構築.

国際標準化のポイント例

・セキュアにセンサデータを蓄積・管理する仕組みの定義
・サービス定義書/制御つきデータコンテナ（例：IEC63430）の定義
・ユーザデータ提供に関する本人同意プロセスの定義

# 目的

①～③を定義することを目的として議論を進める




①各種ウェアラブルセンサーで取得したセンサデータをセキュアに蓄積、管理する仕組みを定義

②サービス定義書/制御つきデータコンテナの定義

③センサデータ提供に関する本人同意プロセスの定義

# 目次

- PDS部会の設立背景と紹介
- 今年度の活動報告
  - 分散型PDSの認証をおこなうためのガイドライン策定に向けた検討項目の洗い出し.
    - セキュアにセンサデータを蓄積・管理する仕組みの定義、
    - サービス定義書/制御つきIoTデータコンテナ（IEC63430）の定義
    - ユーザデータ提供に関する本人同意プロセスの定義

# 部会における議論の経過

第1回成果物の方向性、内容についての議論
第2回 成果物についての要素と定義の検討
第3回 成果物作成にあたり、方向性、用語の定義を再議論
第4回 スマートシティセキュリティガイドラインと分散型センサデータストア
システムの比較分析と議論①
第5回 スマートシティセキュリティガイドラインと分散型センサデータストア
システムの比較分析と議論②
第6回 情報信託機能と比較した分散型センサデータストアシステムにおける
本人確認について議論
第7回 制御つきデータコンテナ(IEC63430)の定義についての議論①
第8回 制御つきデータコンテナ(IEC63430)の定義についての議論②

# ガイドライン策定に向けた検討項目の洗い出し

1. セキュアにセンサデータを蓄積・管理・流通する仕組みの定義
総務省「スマートシティセキュリティガイドライン」に記載されている分析内容を分散PDSに置き換えて検討
例:利用の流れの分類、それぞれでのセキュリティ課題と対策.

2. サービス定義書/制御つきデータコンテナ(IEC63430)の定義
この定義については参考になるようなガイドラインやリファレンスアーキテクチャはないため、ミルウス社の取り組みを例に検討.

3. ユーザデータ提供に関する本人同意プロセスの定義
総務省「情報信託機能の普及促進に向けた課題解決に係る調査」の本人同意プロセスを分析し、分散PDSに置き換えて検討.

# 1. セキュアにセンサデータを蓄積・管理・流通する仕組みの定義

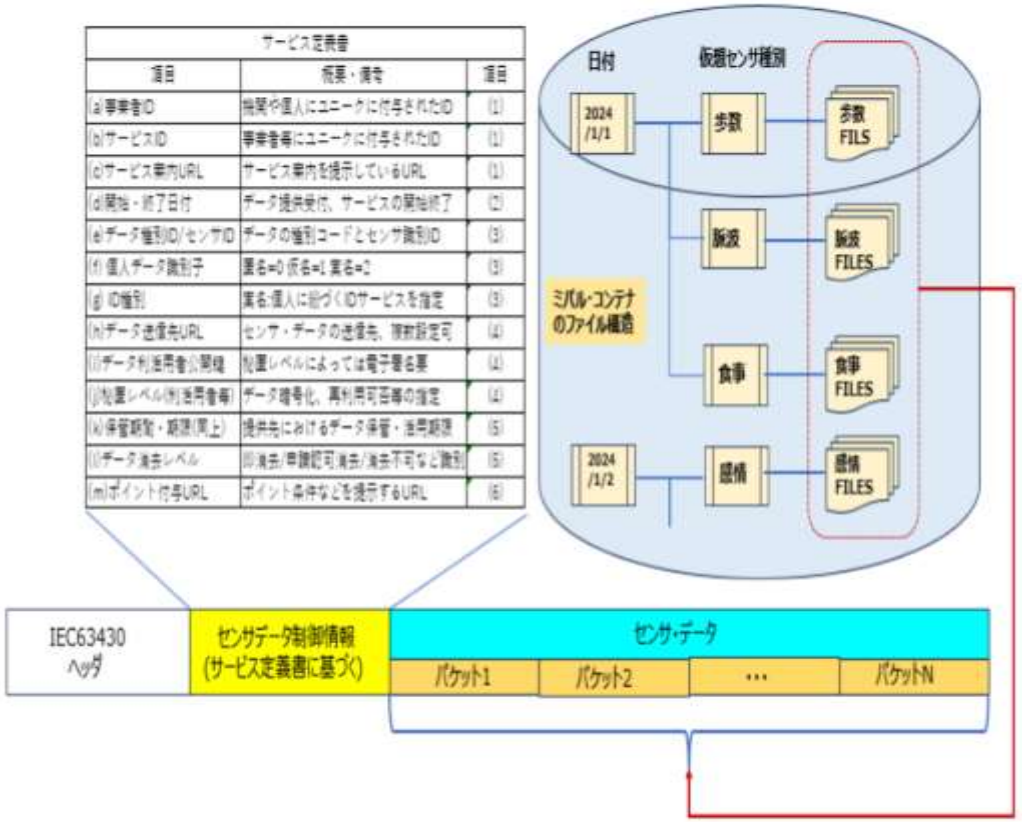
## ■ スマートシティセキュリティガイドラインの分析

「スマートシティセキュリティガイドライン」のデータ連携時のセキュリティについては分散型PDSに置き換えた際に有効である点について確認した。

- データ連携①：データ連携元・連携先のセキュリティ体制の確認・評価を実施する
- データ連携②：データ提供事業者・サービス提供者等の認証と適切なアクセス制御を実施する
- データ連携③：データの追跡可能性を確保しデータ利用の透明性を担保する
- データ連携④：データの原本性保証を確保しデータの信頼性を担保する
- データ連携⑤：必要性に応じたデータの匿名化・秘匿化を実施する
- データ連携⑥：API におけるセキュリティ（機密性・完全性・可用性・真正性）を確保する

# 2.サービス定義書/制御つきデータコンテナ(IEC63430)の定義

## ■ ミルウス社の取り組みを例に検討




ミルウス社サービス定義書

- ミルウス社のサービス定義書を分析した結果、以下のような考察が得られた。
- 「(f)個人データ識別子」などはサービスによって定義が異なる。
  - 閲覧者の立場、レベルによって許可付与の内容を変更することが必要。
  - 本人確認についてはID、パスワードでは不十分。マイナンバーカードの活用の可能性も検討すべき。
- 「(l)データ消去レベル」については、消去した、というエビデンスを残す必要がある。

# 3. ユーザデータ提供に関する本人同意プロセスの定義

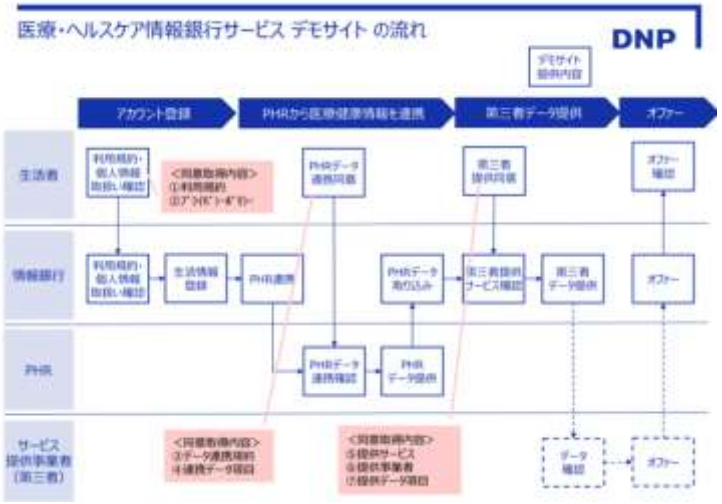
## ■「情報信託機能」の本人同意プロセスを分析

「情報信託機能」の本人同意プロセスを分析し、分散型センサデータストアシステムとの比較を検討した。分散PDSにおける本人同意プロセスについてはミルウス社の本人同意プロセスを参考にした。


ミルウス社の本人同意プロセス

### □ ミルウス社の本人同意プロセス

- サービスを立ち上げたい人が、ミルウス社のプラットフォームに参加をして、利用者がサービス一覧からサービス提供事業者を選んでいく仕組みをとっている。そのためサービスを理解したうえで、二次利用の許諾をとるため、理解が得られやすい。




情報信託機能の本人同意プロセス

### □ 情報信託機能の本人同意プロセス

- 多様なサービスを内包するため、参加者から二次利用についての同意を取るにあたり、同意内容が複雑な場合が多く、同意取り付けに困難があり、十分に普及しているとは言えない。

# 3. ユーザデータ提供に関する本人同意プロセスの定義

## 比較考察

| | ミルウス社 | 情報信託銀行 |
|---|---|---|
| 提供するサービスの開示 | あり | 不明 |
| データ収集の目的 | あり | あり、複雑 |
| データ活用者などの証明書 | あり | あり |
| 二次利用の同意 | あり | あり、複雑 |
| サービス定義書 | あり | 不明 |
| 要配慮個人情報 | | 考慮 |
| | | |
| 考察 | | 登場関係者が多数、かつ複雑→データ活用者の信頼性、データ利用の合意などが担保できるか？ |

# まとめ

- 今年度の活動報告
  - 分散PDSの認証をおこなうためのガイドライン策定に向けた検討項目の洗い出しを行った.
  - 既存のガイドラインを参照しながら分散PDSへの適用について検討を行った.

- 来年度の活動目標
  - 今年度の協議内容をベースに詳細議論に繋げる.

# 今年度の活動

- 分散型PDSの認証をおこなうためのガイドライン策定に向けた検討
- 進め方:既存の参考資料を基に議論

1.セキュアにセンサデータを蓄積・管理・流通する仕組みの定義

スマートシティセキュリティガイドラインの分析を分散PDSに置き換えてみる

例:利用の流れの分類、それぞれでのセキュリティ課題と対策

2.サービス定義書/制御つきデータコンテナ(IEC63430)の定義

参考となるガイドラインが見当たらないため，ミルウス社の取り組みを例に分析し、分散PDSに置き換えて議論する。

3. ユーザデータ提供に関する本人同意プロセスの定義

情報信託機能の本人同意プロセスを分析し、分散PDSに置き換えて検討.

# 1. セキュアにセンサデータを蓄積・管理・流通する仕組みの定義

## ■ スマートシティセキュリティガイドラインの分析

例示された他分野のガイドライン/リファレンスアーキテクチャと分散型センサデータストアシステムの共通点、差異の分析を行い、以下2つの項目について検討を行った。

- 前提となる背景、目的、対象範囲、想定読者、活用方法
- 分散型センサデータストアシステムガイドライン策定に向けての3つの技術要素の検討

# 前提となる背景，目的、対象範囲、想定読者、活用方法

| 項目 | 詳細 |
| --- | --- |
| 背景 | センサー技術の向上に伴い、個人の医療データ、ライフログ(睡眠、食事、運動などの記録)の利活用に関心が持たれる。<br>それらのデータをスマートフォン、サーバーなどに安全に保管し、本人の意思に基づき、セキュアに流通させる仕組みの標準化に取り組む。<br>個人情報、特に医療データなどセンシティブ情報の取り扱いは厳格になり、管理の安全性と流通の利便性の両立が不可欠となってきた |
| 目的 | ベンダーの検討素材、リファレンスになってもらえるよう |
| 対象範囲 | ウェルネス、医療、行政サービスに紐づくウェルネス(重要インフラ14分野も俯瞰) |
| 想定読者 | ベンダー(サービスをこれからはじめようとする事業者) |
| 活用方法 | ベンダーがサービスを検討するにあたり、踏まえるべきポイントを理解してもらう |

# 情報信託機能の普及促進に向けた実証実験概要

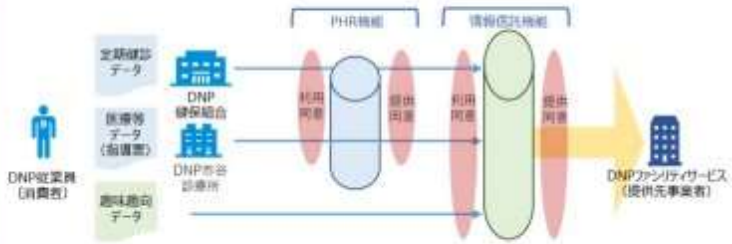
## 1-2. 実証概要

DNP

本実証では、DNP従業員の要配慮個人情報等を本人同意を取得し、実証環境で整備した情報信託機能を体験頂き、319名分のアンケート等（一部インタビュー含む）の結果より情報信託機能の有用性、要配慮個人情報に対する意識および課題を検証した。

✓ 実証対象者、参加同意およびサービス体験者などの人数推移


✓ 取扱う個人情報とデータ流通フローの仕組み




✓ 本実証では、活動進捗を有識者会議で報告⇔フィードバックを頂きながら実施



※実証環境では、利用規約、個人情報の取り扱いなどの同意書類、情報信託機能を体験できるようにWebアプリを試作開発。 また個人情報を安全に取り扱うに必要な運用体制を整備

# 情報信託機能の普及促進に向けた実証実験の同意プロセス