
IoTネットワーク説明会

2021年9月27/10月6日 オンライン方式

国立研究開発法人物質・材料研究機構
松波 成行

アウトラインとお願い

- ・ マテリアル先端インフラ事業にかかるIoTネットワーク案（NIMS）
- ・ IoTセキュリティデバイスについて（東芝インフラシステムズ様）
- ・ みなさまからの質疑応答（約45分予定）

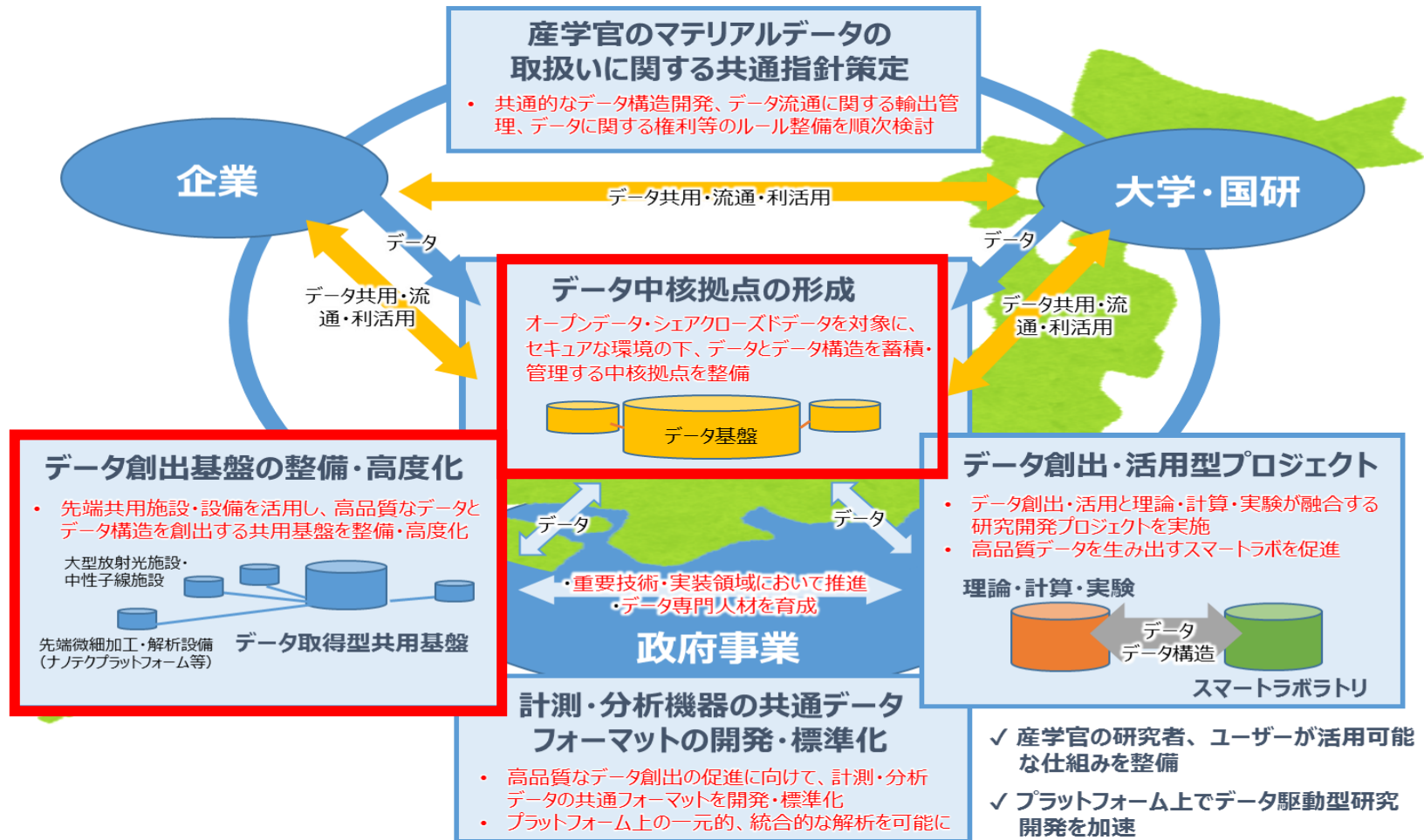
■お願い■

- ① 本日の内容は、主にネットワーク管理者様/情報セキュリティ部門様向けとしております。
質問やコメントなどにつきましては、説明会の主旨上、**ネットワーク関係のみに絞らせていただきます**ことをご了承ください。
- ② 質問は**挙手ボタン**もしくは**直接ご発声**ください。（所属とお名前をお願いいたします）
- ③ 開催メモのため、録音をとらせていただきますことをご了承ください。

1. 事業概要

マテリアルDXプラットフォーム構想のイメージ

小川浩司, 第19回ナノテクノロジー総合シンポジウム, 2020年12月11日より



マテリアル先端リサーチインフラ（データ創出）

令和3年度要求額 3億円（新規）
令和2年度第3次補正予算額 20億円

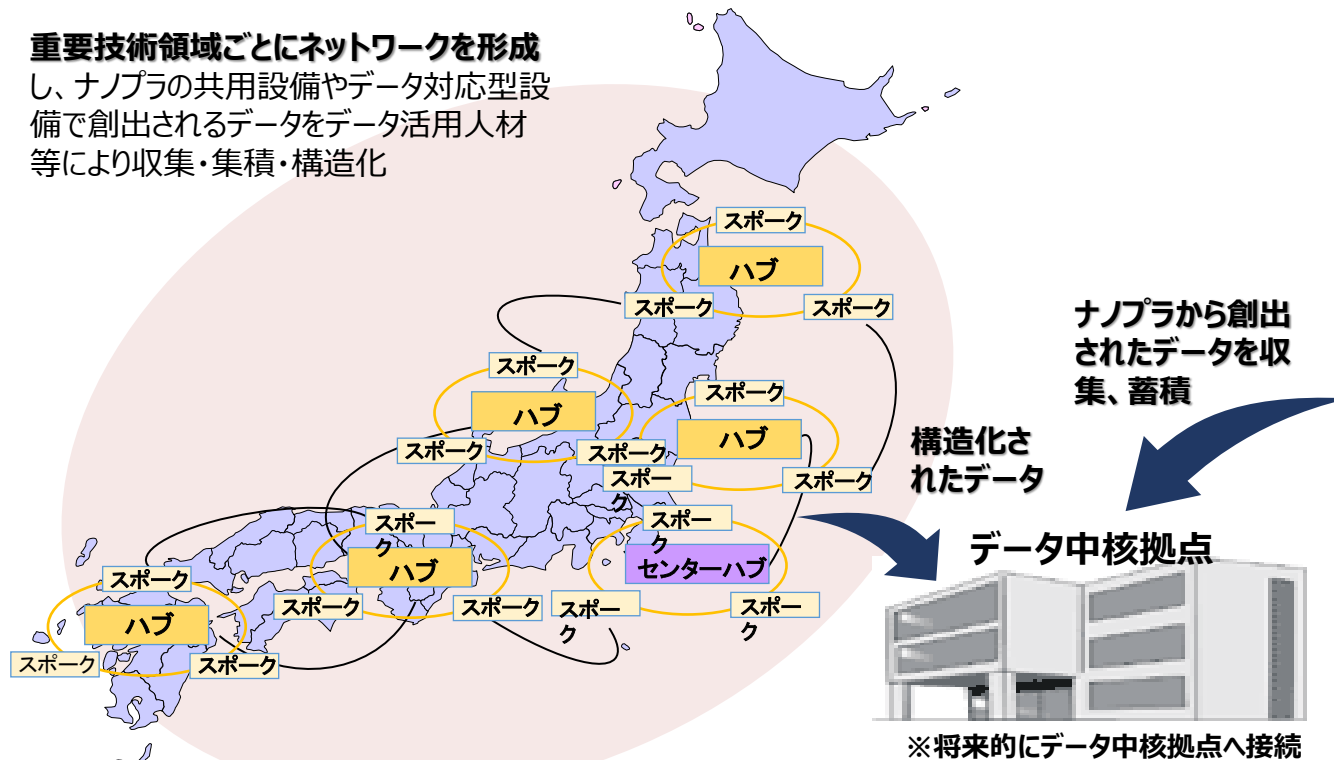
取組概要

- 重要技術領域ごとに強みを持つ先端設備群を有するハブと特徴的な装置・技術を持つスポークからなる**ハブ&スポークの体制を新たに構築**
- ユーザーニーズが高いデータ対応型設備の導入と設備から創出されるデータの構造化等を行う人材を配置**
- 設備共用を実施しているナノテクノロジープラットフォーム事業と連携してデータ収集・蓄積・構造化を行うことで、データ利活用の早期開始を図る

【新規事業】マテリアル先端リサーチインフラ

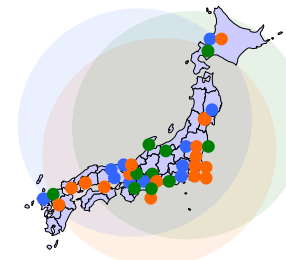
小川浩司, 第19回ナノテクノロジー総合シンポジウム, 2020年12月11日より

重要技術領域ごとにネットワークを形成し、ナノプラの共用設備やデータ対応型設備で創出されるデータをデータ活用人材等により収集・集積・構造化

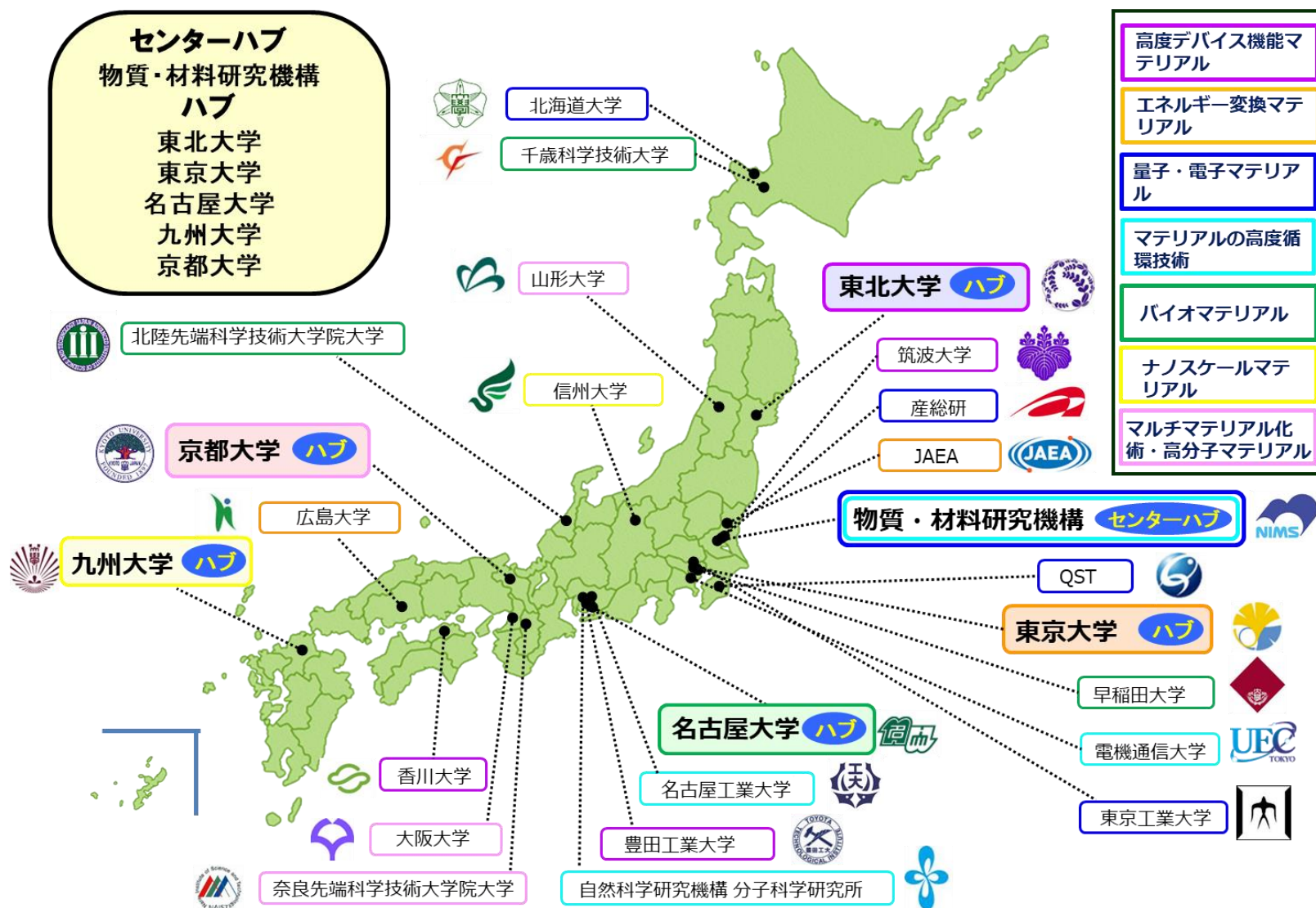


【既存事業】ナノプラ

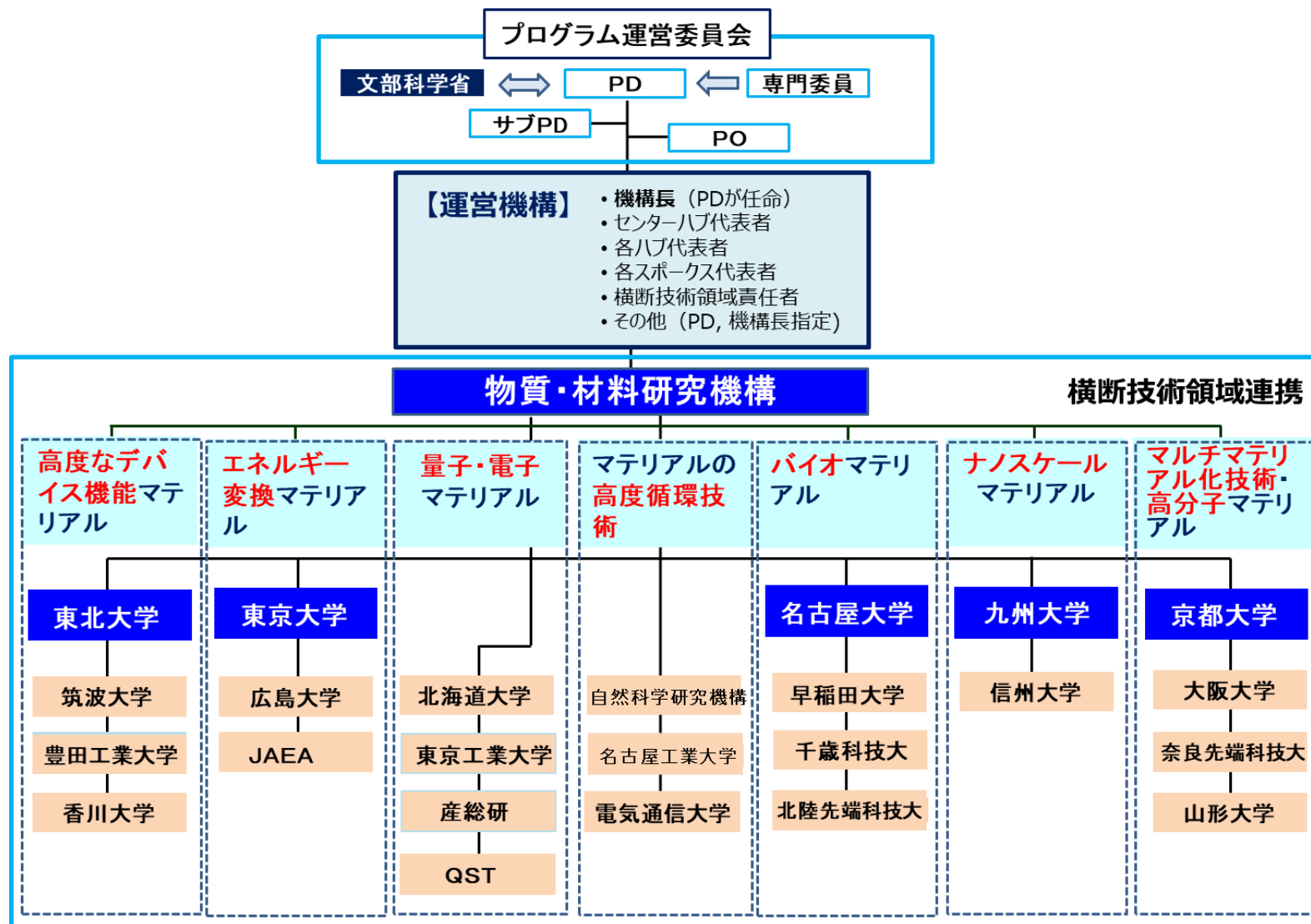
3つの技術分野に対応したプラットフォームを形成し、設備共用を実施



マテリアル先端リサーチインフラの推進体制（全25法人）



「マテリアル先端リサーチインフラ」実施体制図

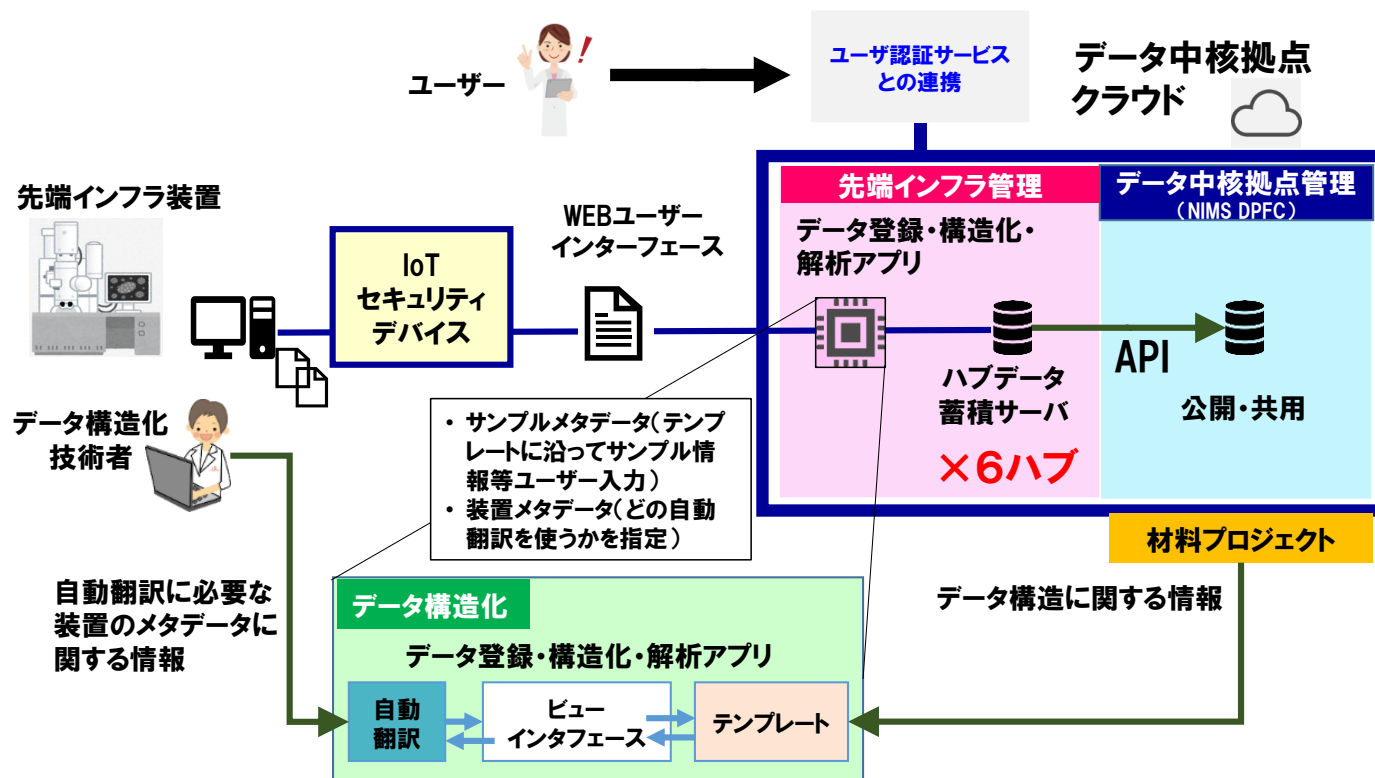


マテリアル先端インフラ事業の代表的な要件(公募要領)

- 各ハブ及びスポーク機関は、重要技術領域に強みを持つ設備・技術等の共用を図るとともに、当該領域に関する高品質なデータを収集、蓄積する。
- 各ハブ機関は、データを収集、蓄積するためのデータ管理システムを構築し、各ハブ及びスポーク機関が創出するデータを集約するとともに、高品質で膨大なデータ群を利活用可能なデータセットに変換(以下、データ構造化という。)する。
- 蓄積したデータのうち一部は、今後、国立研究開発法人物質・材料研究機構が構築していくデータベース(以下、データ中核拠点という。)へ登録する。

データ収集にかかる工数をできる限り省人化・自動化することが必要

クラウドデータ構造化システムと3つの特徴



- ✓ **セキュリティ重視:** IoTを設置した機器から特定の人しかデータ登録できません。(アップロードのみ・関係者のみ)
- ✓ **簡単データ登録:** WEB-GUIからアップロードだけで簡単にデータ構造化とデータセット化します。
- ✓ **柔軟な拡張性:** テンプレートで材料プロジェクトや共同研究ごとに入力情報(テーマ)を増減できます。

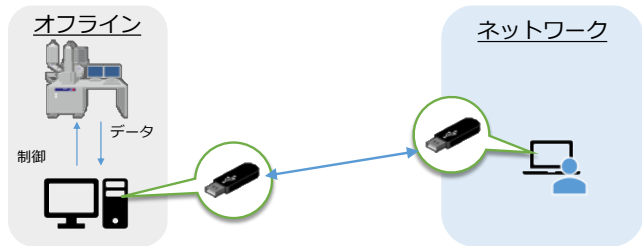
2. IoTセキュリティデバイスとデータ収集の概要

IoTセキュリティデバイスのコンセプト（オンプレミスの無線IoT※の例）

- 対象機器： スタンドアロンで運用される計測・分析装置やプロセス装置の制御PC向け
- 方 法： 通信セキュリティを施したIoTデバイス(無線・有線)を活用

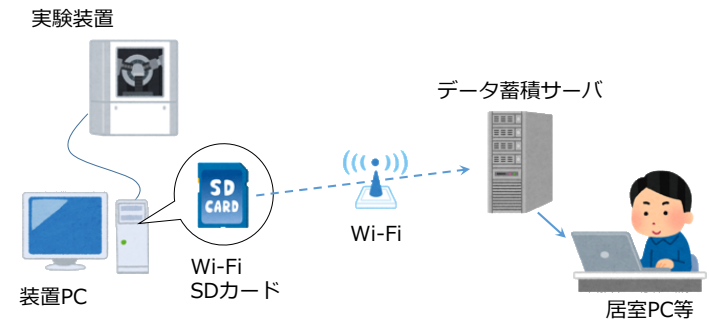
※マテリアル先端インフラ事業では無線IoTは用いません

これまでの方法



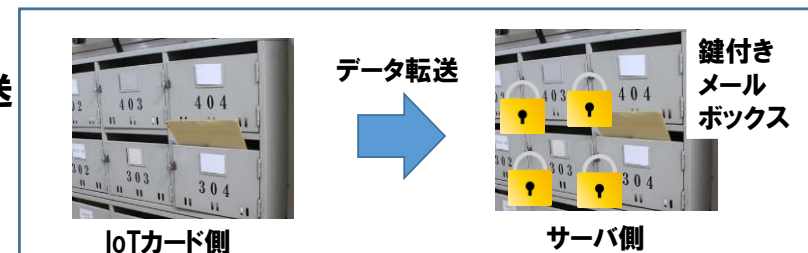
- ・ OSの自動アップデート等で長時間測定が中断される！
- ・ OSが新しくなると、装置の制御プログラムが更新できない！

本システム



特 徴：

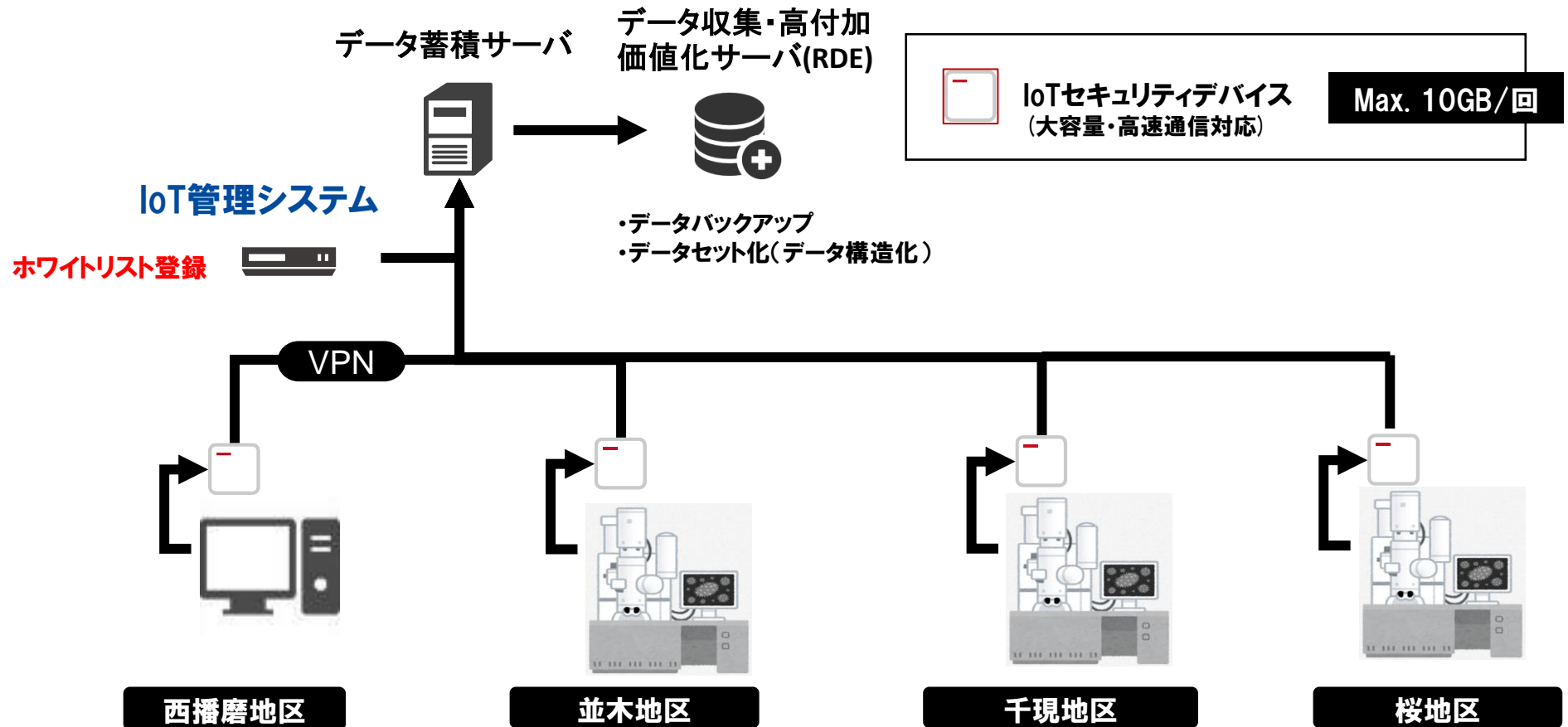
- ① 情報セキュリティを高める**アップロードのみの通信制御**によるデータ転送
- ② データの秘匿性を確保する**私書箱方式のデータの振り分け機能**
- ③ 小型なので大きな工事が不要。**誰でもが簡単に増設や設置が可能**



特定のPCからのみアップロードのみ有効（ダウンロードは不可）

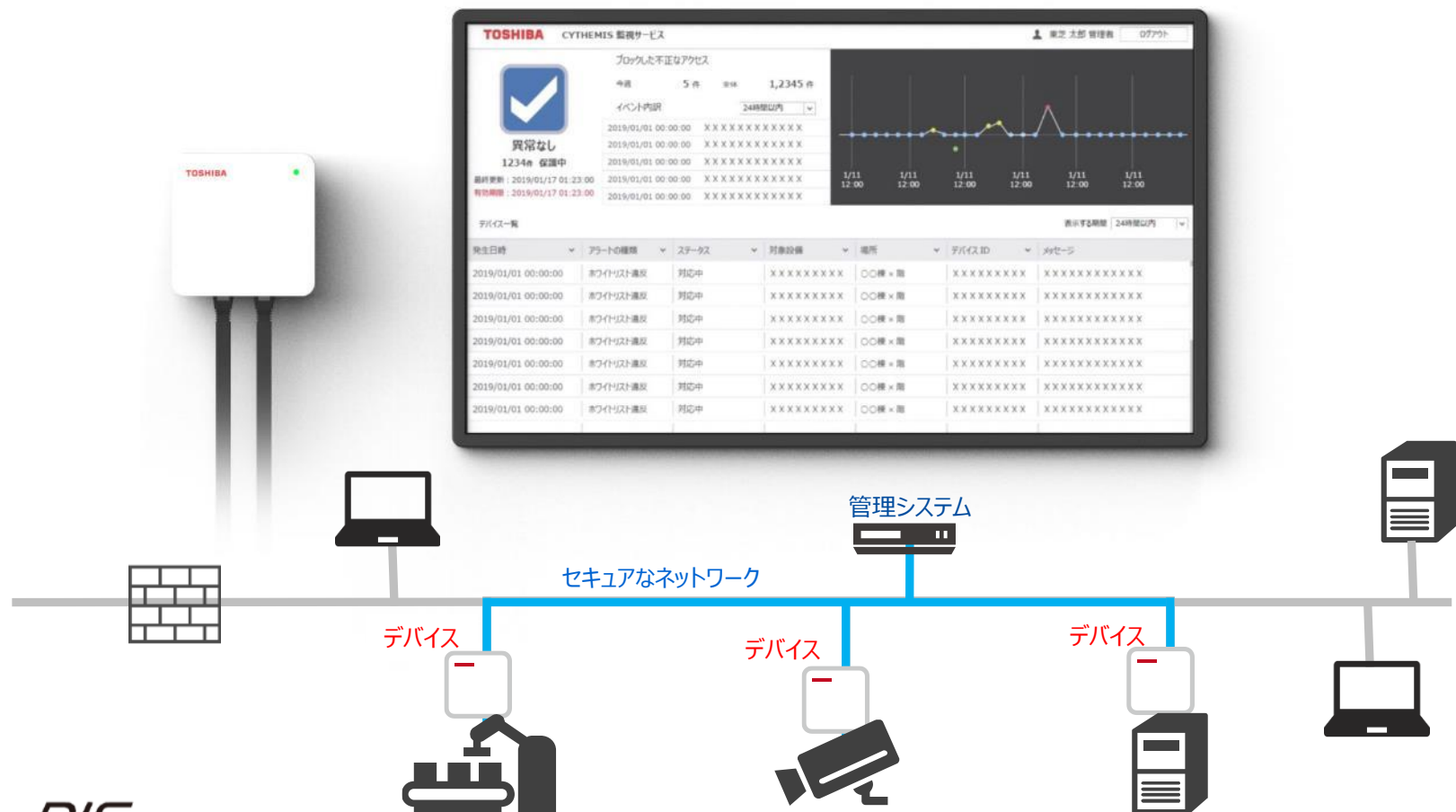
IoTセキュリティデバイスを通じたデータ収集基盤（有線の例）

■ セキュリティを確保したIoTセキュリティデバイスによるオンプレミスデータ収集システムを開発済



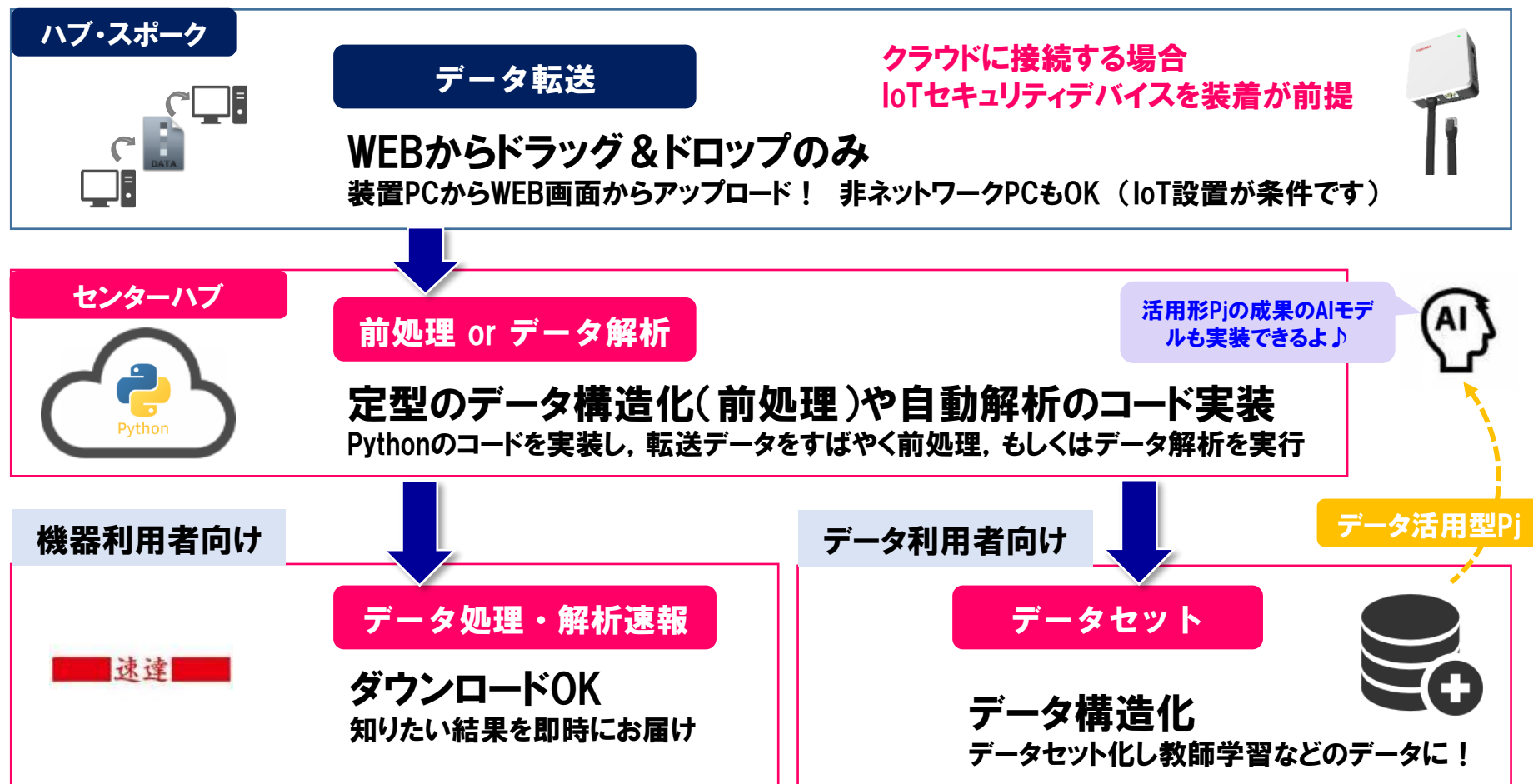
次期システムでは収集サーバーはクラウド版+IoTは有線方式に限定して開発中

エンドポイントに**外付けするデバイス**と**管理システム**を組み合わせた
新しいセキュリティソリューションです



次期システムでのデータ収集/利活用のワークフローの高度化

- 作業効率化: 測定rawデータを即時にワンストップでデータ処理 & 解析をフィードバック。
- データセット利用: データセットを使って最新研究に、オリジナルの機械学習モデルも実装可能

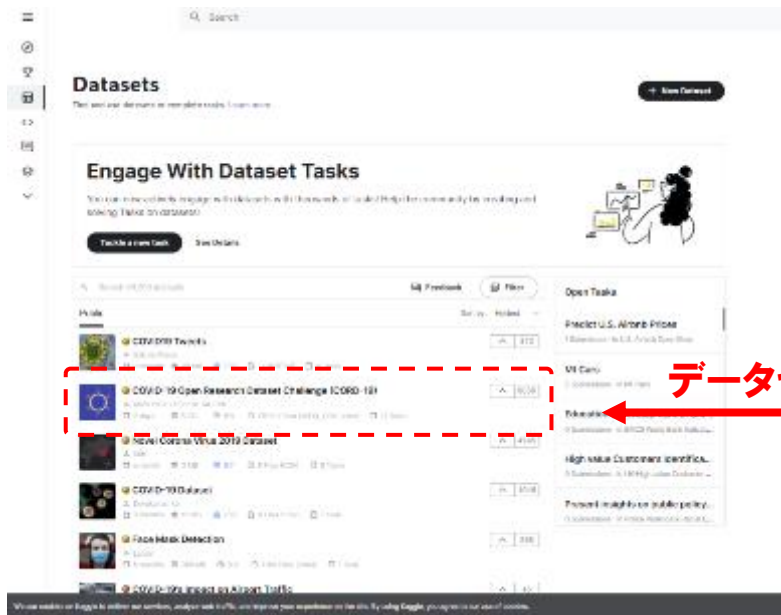


データセットとは

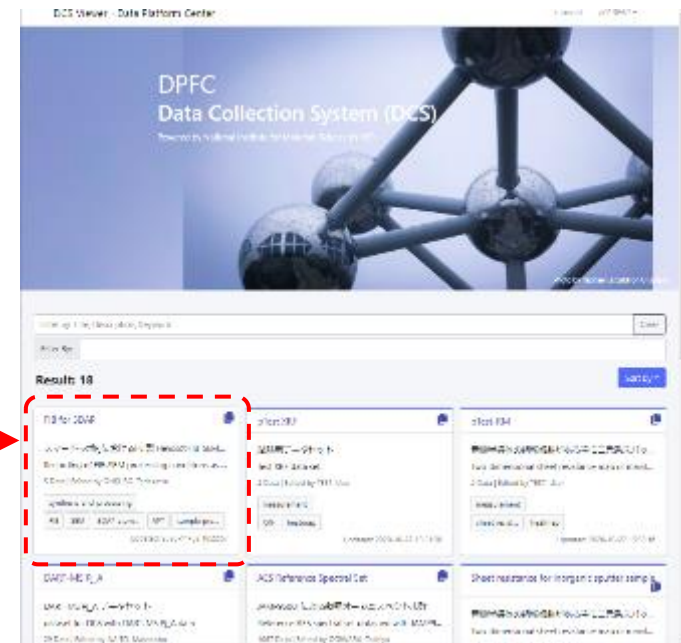
■ 特定の目的やテーマに沿って収集されたデータ群。

- 1) 統計処理や機械学習等にも利用しやすいように**データが構造化**された状態となっている。
- 2) データの属性や意味がわかる**データカタログ**を備える。

kaggle (有名なデータセットの例)

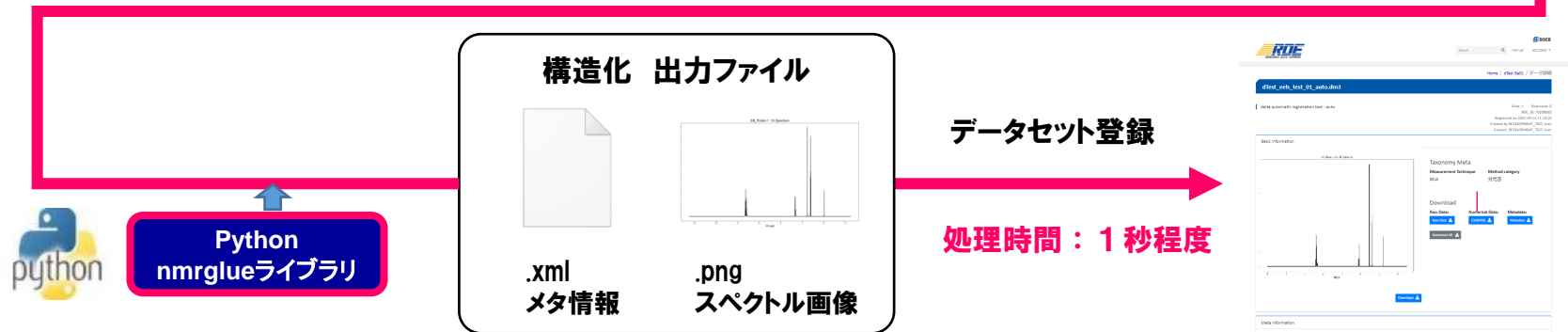
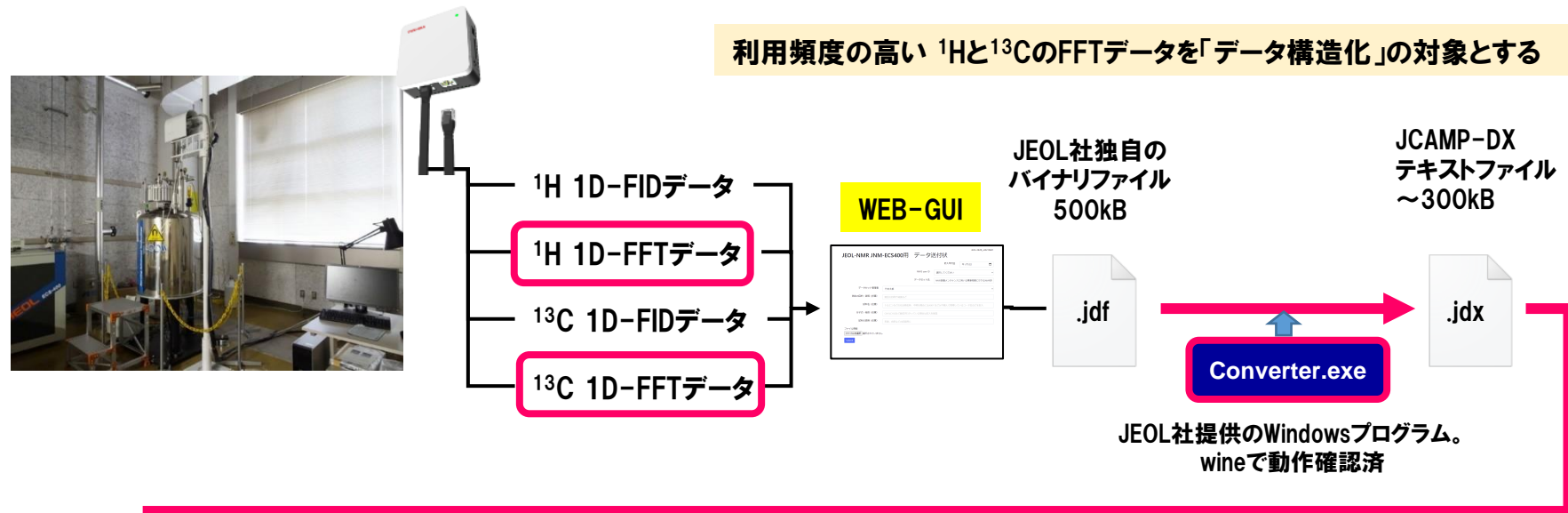


NIMS (Research Data Express)



目的とするデータ群(データセット)がすぐに閲覧/ダウンロードが可能です

データ構造化の概要（NMRを事例に）



※スペクトルの数値データ化(csv化)はおこなわない
→ その利用形態がすくないため

データがアップロードされた後はデータ構造化が自動的に実行、DBに収集と蓄積
(IoTが勝手にファイルをアップロードしたりすることはありません)

データ登録GUIのイメージ（その1： NMRを例に）

- 登録GUIを「テンプレート」とよびます。装置やユースケースによってHTMLで柔軟に項目を変更。

■ デフォルト版テンプレート

JEOL-NMR JNM-ECS400用 データ送付状 JEOL-NMR_v20210601

記入年月日

NIMS user ID

データセット名

データセット管理者

測定目的・説明（任意）

試料名（任意）

分子式・組成（任意）

試料の説明（任意）

ファイル情報
 選択されていません

アップロードするファイルを選択

基本情報

- ① 記入年月日
- ② データ投入者
- ③ データセット名
- ④ データ責任者

サンプル情報

- ⑤ 計測の目的・説明
- ⑥ 試料名（番号）
- ⑦ 分子式・組成式
- ⑧ 試料の説明（option）

- IoTを設置した制御PCのみから、事業専用のデータ登録GUIにアクセス。ここからデータをアップロードします。

（IoTを許可なく別の装置につなげるとネットワークへは接続されません。）

データ登録GUIのイメージ（その2：I-V特性を例に）

超電導 I-V特性評価 TypeB Ic-B(T)用（磁場印加角度固定） IV_v02010629

記入年月日 年 / 月 / 日

NIMS user ID 選択してください

データセット名 I-V Characteristic for Superconductor II

データ責任者(Responsible Person) 伴野信哉

特性評価の目的・説明（任意） 特性評価にかかる背景など

試料名（任意） A001 などGrで管理しているコード名やメーカーの細材名などを記入します

組成（任意） NbZrなど組成がわかっている場合は記入を推奨

試料の説明（任意） 来源、由来などの記録用に

固有情報

電圧端子間距離 1 cm

磁場印加角度 deg

線材の断面積 金属系線材の場合はnon-Cu面積 mm²

超伝導コアの断面積 mm²

線材形状 テープ

材料系統 REBCO

その他：試料説明（推奨） 材料系統で「その他」を選択した場合は材料や条件について補記

検索キーワード要素1 REBCOなら、REにGaやYなどを記載

検索キーワード要素2 第二成分の元素を記載

ファイル情報

選択されていません

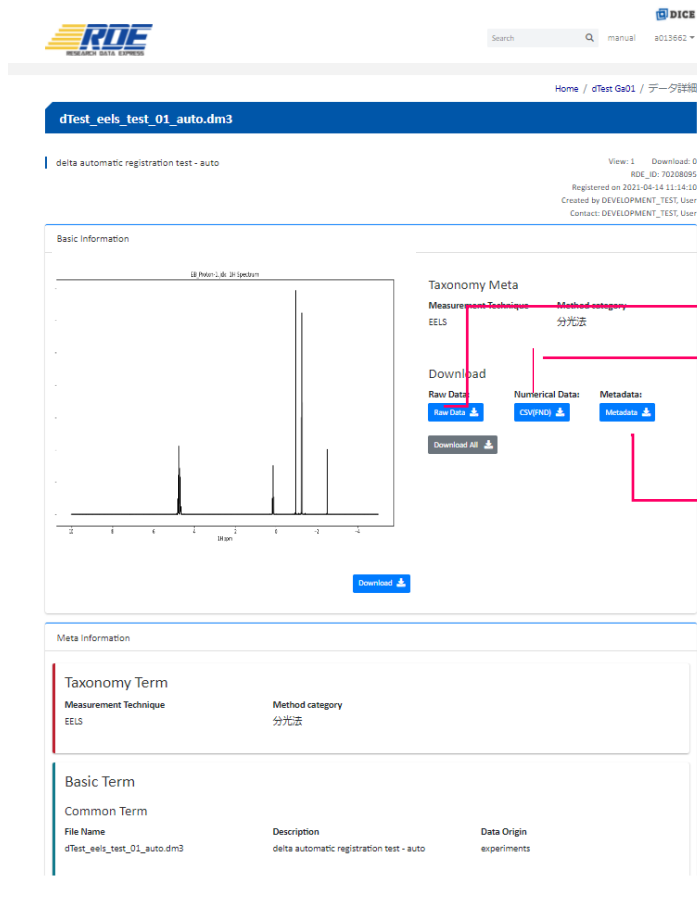
実験固有情報/装置固有情報

装置やテーマに応じて柔軟に入力項目を増減させることができます

- 異なる制御PC（実験装置）では、異なるデータ登録GUIが呼び出されます。
- この入力項目（材料情報や実験条件）もメタデータとして登録されます

NMRのデータ構造化(データセット登録)のイメージ

- rawデータ(input)のほか、データ構造化されたファイル(output)および装置メタデータを蓄積。
- 可視図(サムネイル)も出力し、rawデータ(スペクトル)がイメージできるようにする。



■ 登録ファイル (構造化ファイル)など

Rawデータ: JEOLバイナリ形式(.jdf)

Outputファイル: JCAMP-DX (.jdx)

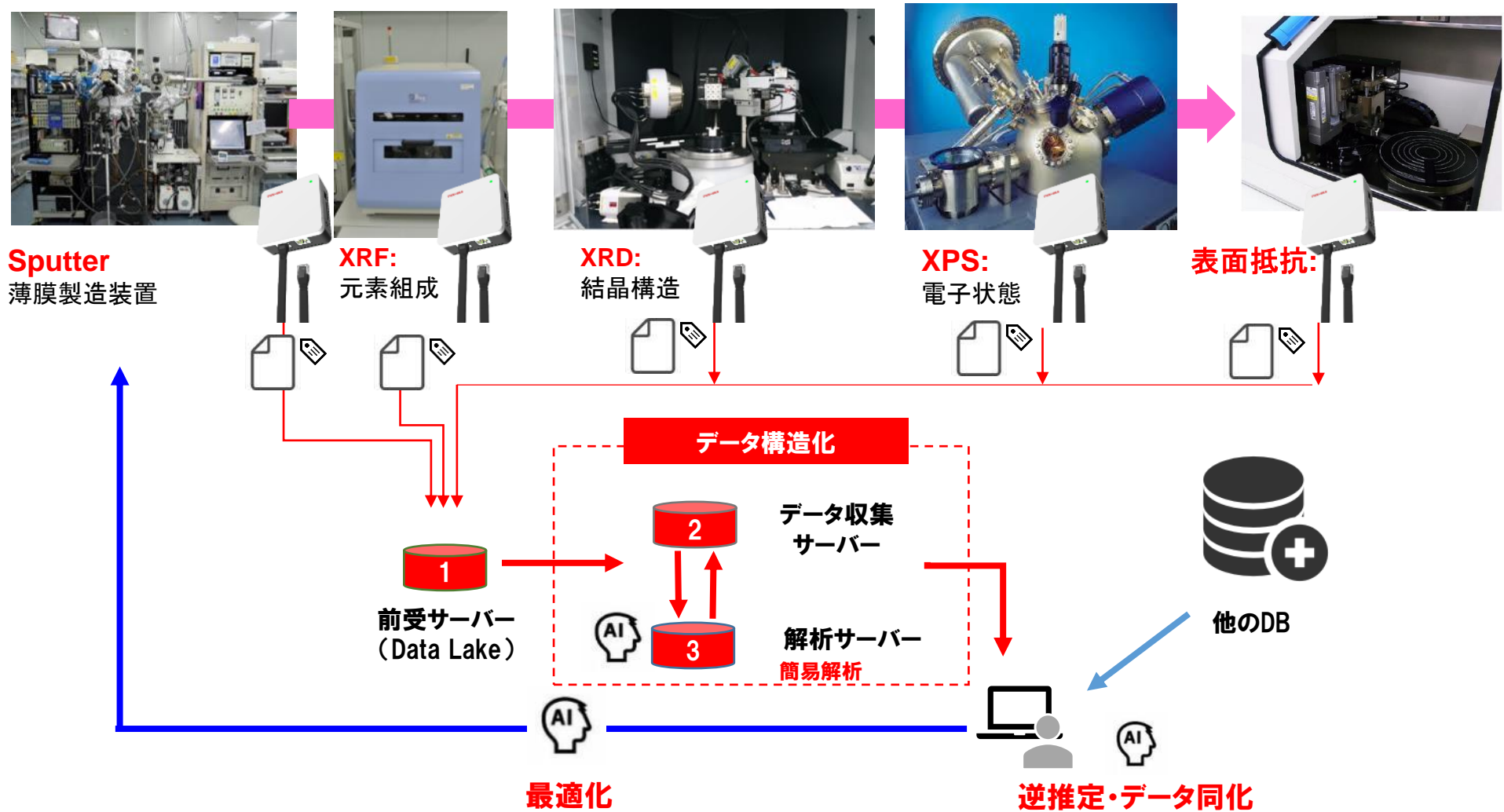
Metadataファイル: メタデータリスト(.csv)

■ 測定・装置にかかるメタデータ

- 事前に定めたメタデータ(スキーマ)に基づいて自動で抽出した計測パラメータ等を表示
- テンプレートの入力項目も表示

Rawファイルもとりだせるので、これまでUSBで移送していた作業も自動化できます

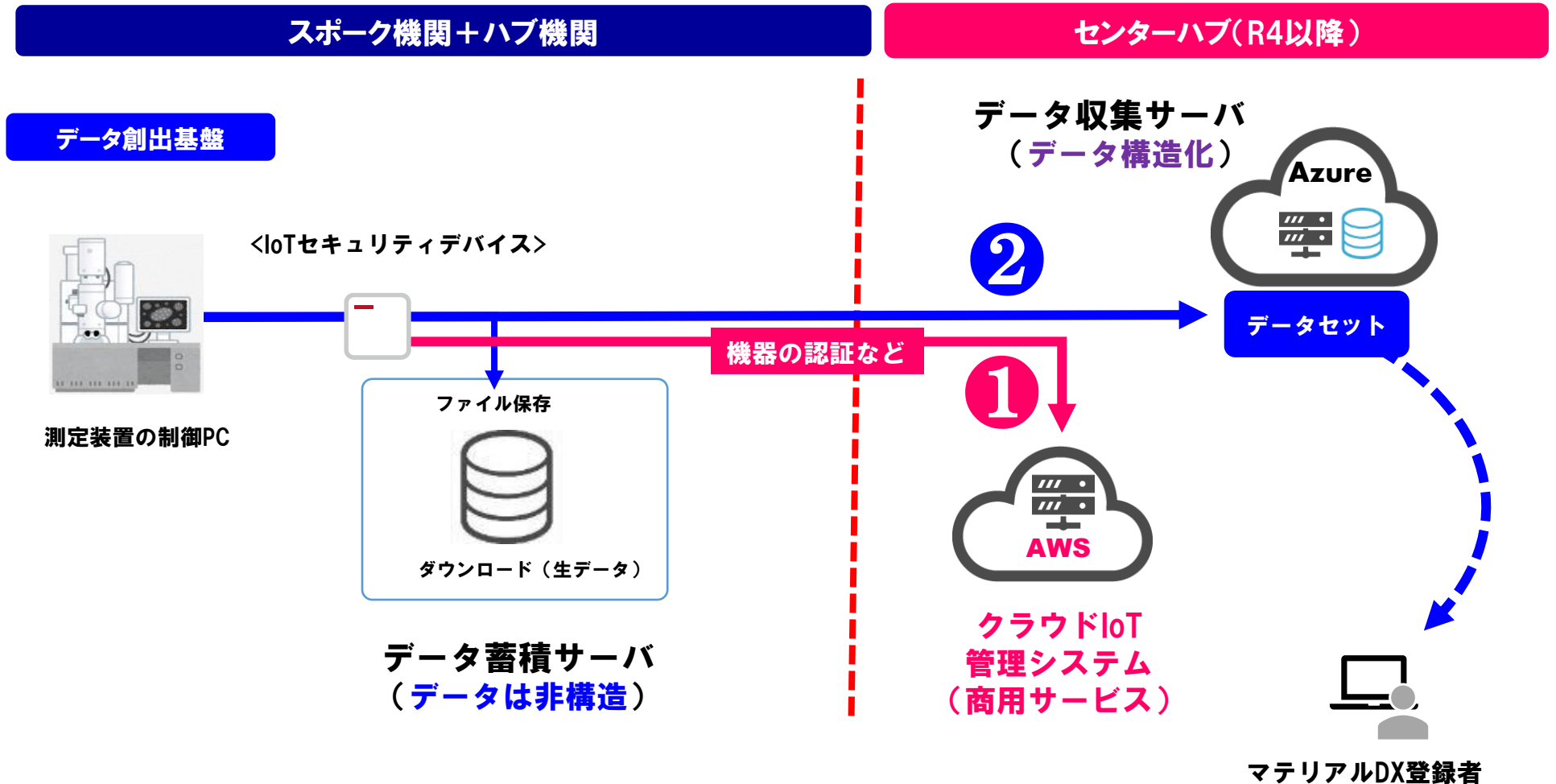
IoTシステムによるラボ装置のデータ構造化



IoTセキュリティデバイスを装着することで、各種プロセスや計測機器のデータをセキュアに、そして効率的にデータセット化して蓄積することができます。

2. マテリアル先端インフラ事業での構想

マテリアル先端インフラでの連携図

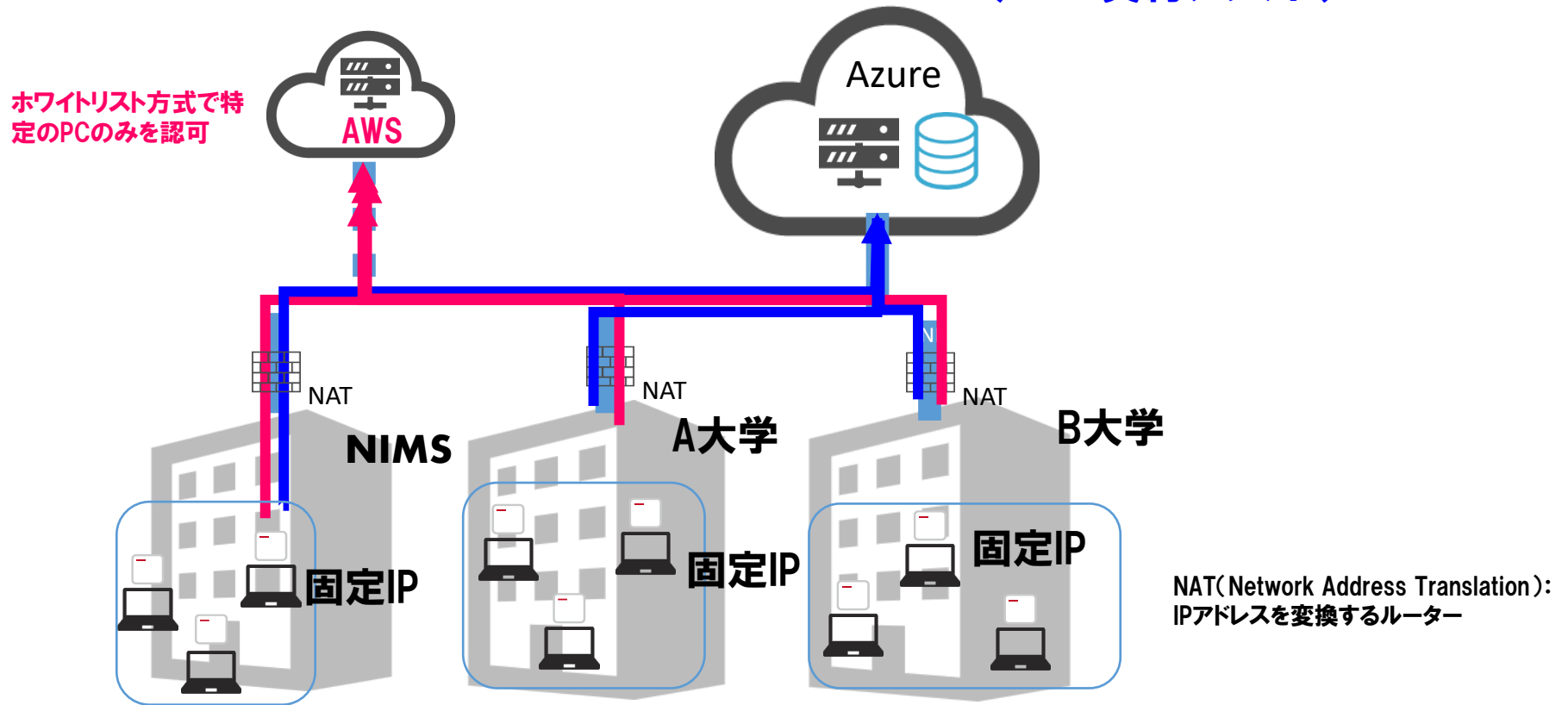


- 事業ではIoT管理システムとしてクラウドサービスを利用します。
- ①で通信を認めた機器(PC)のみからのデータを②でAzure(サーバー)にアップロード

IoTセキュリティデバイスの設置に必要なこと

①クラウドIoT管理システム (商用サービス想定)

②データ構造化システム【開発】 (NIMS契約クラウド)

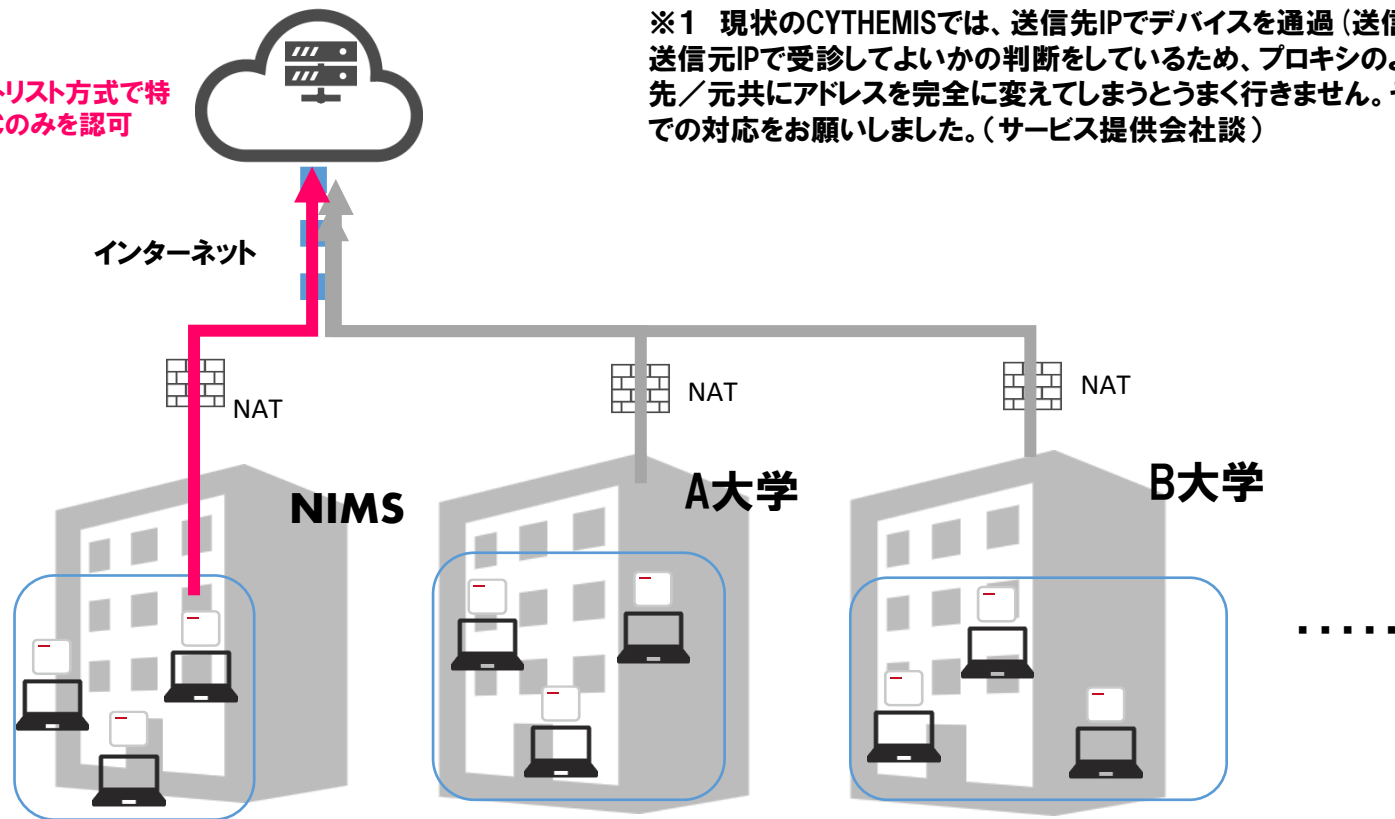


- ① IoTセキュリティデバイスを接続するPCは**固定IP**とさせていただきたい
- ② 外部(インターネット)への接続は**NAT**をご用意いただきたい(ProxyはNo)

R3年度の予定事項

①クラウドIoT管理システム (商用サービス想定)

ホワイトリスト方式で特
定のPCのみを認可



- [1] NIMSのみNAT (※1)でインターネット経由でつなぐテストを実施
- [2] 各機関のネットワークポリシーの確認と接続可否を調査

※1 現状のCYTHEMISでは、送信先IPでデバイスを通過 (送信) させてよいか、送信元IPで受診してよいかの判断をしているため、プロキシのように一旦受け取って、送付先／元共にアドレスを完全に変えてしまうとうまく行きません。そのため、NATもしくはNAPTでの対応をお願いしました。(サービス提供会社談)

取り組みスケジュール

① R3年度：IoTデバイスのクラウド管理システム(商用サービス)の試験テスト

- NIMS：運用交付金事業の範囲でNIMSのみで管理システムとの試験テストを実施
- 各スポーク機関様：ネットワークポリシーの聞き取りと適合の調査

R4年度：各スポークス機関様の許可範囲で接続テストを開始

② NIMS契約クラウドのデータ構造化システムとの接続(R4年度)

- NIMSクラウド(Azure)上のデータ構造化システムの試験運用
 - (R4上半期) データ構造化コードなどの検証とシステムへのデータ登録のテスト
 - (R4下半期) IoTセキュリティデバイスで認可されるPCからのデータのアップロードテスト

FAQ

PCについて

Q. 個人持ちのPCは接続できますか？

A. 本事業のデータ収集の対象は「共用設備」であることから、**共用設備にかかわるPC**に限らせていただきます。

共用設備にかかわるPCの例

- ・ 装置の制御PC
- ・ 装置に接続し、装置からのデータを取り込んでデータ処理をなすPC
- ・ その他（装置とシリアルケーブル等で接続された中継PC）

Q. 非ネットワーク環境にあるPCは接続できますか（OSがWin8以上）

各機関のネットワークポリシーは、適切なセキュリティ対策をしたPCについては接続可能としていることから、ハブースポークス間でのネットワークセキュリティ対策が十分に取られることでネットワークを介してデータの転送が可能となると判断されます。

【参考：NIMS対応】 OSが準拠していても装置管理上の理由から接続していないケースでは、IoTセキュリティデバイスを設置することで、現在のPC環境を変更せずに、特定の送り先（弊所の場合は、NIMSのデータクラウド）のみに送信可能となります。

また、IoTセキュリティデバイスはwindows updateなどの外部トリガーはかかりませんので、勝手なバージョンアップなどは行わず、非ネットワーク環境をそのまま維持します。

PCについて

Q. サポート切れOS (Win7など) のレガシーPCは接続できますか？

- NIMSでは長年の技術検証を経て、NIMS内部事業では接続実績がございます。
- 本事業では、**原則としてネットワーク接続を推奨しない機器**とさせていただき、強制はいたしません。
- 代替案としては次の参考図にあるような最新OSをもつ中継PC(各機関のネットワークポリシーに合致するもの)を配置し、そのPCとシリアル接合をさせて、その中継PCにデータを取り込んだあとに、各ハブの用意する事業専用のデータ登録サーバに蓄積することを推奨したい。

参考図

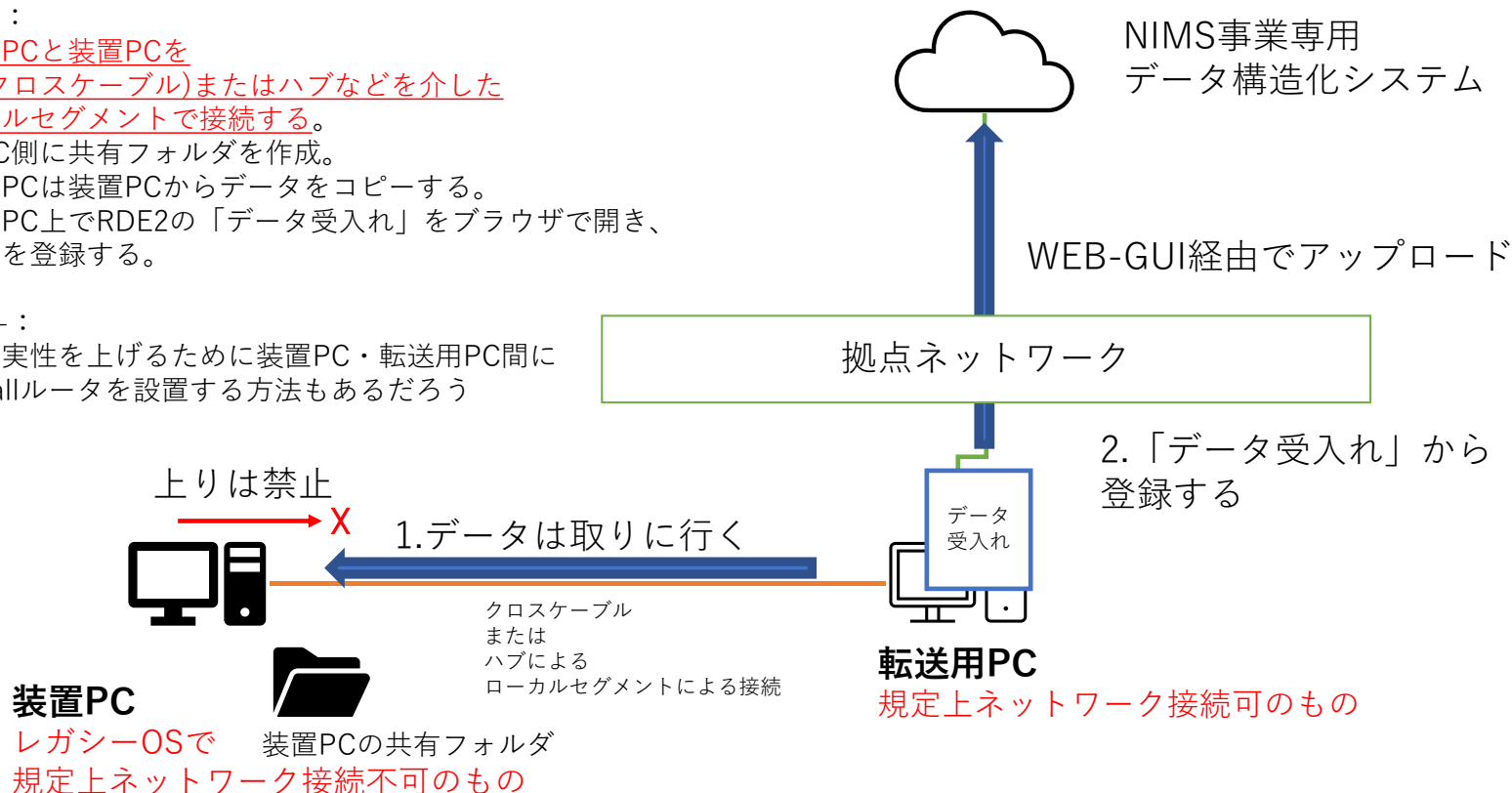
課題：規定上ネットワーク接続不可の装置PCからデータ構造化システムへデータ転送する

回答案 1：

- ・ 転送用PCと装置PCを
直接(クロスケーブル)またはハブなどを介した
ローカルセグメントで接続する。
- ・ 装置PC側に共有フォルダを作成。
- ・ 転送用PCは装置PCからデータをコピーする。
- ・ 転送用PC上でRDE2の「データ受入れ」をブラウザで開き、データを登録する。

回答案1+：

- ・ より確実性を上げるために装置PC・転送用PC間にFirewallルータを設置する方法もあるだろう



リモートについて

Q. 当該装置が別事業であるリモート接続等による遠隔操作対象となっている。どうすればよいか。

- リモート接続事業を優先する場合、レガシーPCの対応と同じように、MRI事業専用の最新のOSをもつ中継PC(各機関のネットワークポリシーに合致するもの)を配置し、データ登録はそのPCを経由して、各ハブ機関のデータサーバーへ蓄積することを推奨といたく存じます。

(もしくは逆に、リモート事業は専用の中継PCを経由して行うことを推奨)

Q. 一回で登録できるファイルサイズは？

- 次期システムで想定しているMicrosoftのAzureでは**一回の上限で受け付けるファイル容量は10GB**となっております。

→ それを超えるデータは、システムとして受け入れられないため、NIMSへデータを転送される場合には事前にご相談させていただきたい。

（これまで10GB超の可能性のある装置： 電子線、X線トモグラフィーなどの三次元データ）

- 10GB以下であっても、各スポンサー機関様にネットワーク管理部門と協議された上で、データ転送量の上限を定めていただくことも推奨いたします。

参考： 弊所においては夜間や週末など、日常生活に影響を及ぼさない時間帯において転送を許可するなどの運用上の規則も設けています。

データ登録編

Q. IoTが接続されるまでのデータは登録できないのでしょうか？

■HTML版テンプレート

JEOL-NMR JNM-ECS400用

データ送付状

JEOL-NMR_v20210601

記入年月日

年 / 月 / 日

NIMS user ID

選択してください

データセット名

NMR装置メンテナンスに用いる標準物質にかかるNMR測

データセット管理者

竹村太郎

測定・目的・説明 (任意)

測定の目的や背景など

試料名 (任意)

トルエンなどの化合物名称、不明な場合にはA001 などGや個人で管理しているコード名などを記入

分子式・組成 (任意)

C6H5(CH3)など組成がわかっている場合は記入を推奨

試料の説明 (任意)

来源、由来などの記録用に

ファイル情報

ファイルを選択

選択されていません

Submit

構成要件を 同一とする



■ バッチ登録型テンプレート(システム管理者限定)

[illegible]

✓ HTML版テンプレートの構成が決まれば、バッチ登録型テンプレートで記録していただいたデータについては、次期システムへのデータ登録が可能(システム管理者限定)

→ システムが立ち上がるまでのデータ収集において利用していただけるツール
(ただし、ユーザーさんではなく、装置管理者の方からのご依頼に応じる形となります)