修士論文

非常時に対応可能なプライバシーポリシー マネジメント・認可基盤に関する研究

2210057　草野　清重

主指導教員　　丹　康雄

北陸先端科学技術大学院大学
先端科学技術研究科
（情報科学）

令和 6 年 3 月

Abstract

Currently, smart sensor data is collected by each smart sensor manufacturer and data is shared with third parties according to their privacy policy. Each manufacturer is working on their own data access authorization, and privacy policy consent is obtained from users via apps or the web. However, it is necessary to frequently confirm with users when updating policies or using new devices, and privacy policy managers (PPM) are being studied as a countermeasure.

Conventional authorization infrastructures have been created for data utilization and obtaining privacy policy consent information during normal times. However, it is necessary to provide quick and flexible data access authorization considering individual privacy policy not only in normal times but also in emergency situations.

This paper proposes a privacy policy management and authorization infrastructure that can respond to emergencies by utilizing alert levels and privacy policies, based on the Multimode Kominkan Operating System (MKOS), a building operating system that operates within a community center, targeting community centers that must respond to both normal and emergency situations.

For the sensor data, building and ledger data collected in MKOS, there is the issue of identifying the situation in order to utilize the data not only in normal times but also in emergency situations. In addition, there is the issue of using data in accordance with the user's intention for personal information and privacy information.

For the issue of determining the situation in order to utilize the data not only in normal times but also in emergency situations, we proposed the use of warning levels, which are disaster prevention information issued by each municipality in emergency situations. This makes it possible to make a comprehensive judgment of the emergency situation from the viewpoint of the necessity of evacuation for each region. In addition, by not using information issued for each disaster, such as earthquakes and tsunamis, it is possible to reduce the number of times users need to configure policies.

To address the issue of using personal and privacy information in accordance with users' intentions, we proposed to set a consent information policy for each user in the policy management module for normal and emergency situations within MKOS. This would make it possible to specify the services to which data is to be passed, and to specify data sharing according to normal and emergency situations using alert levels.

This makes it possible to use the sensor data in the community center and the data in the building and ledger according to the user's intentions in normal and emergency situations. In addition, applications and services will be able to flexibly acquire data that could not be acquired in the past, depending on the disaster situation, thereby expanding the range of data utilization in times of disaster.

概要

現在、スマートセンサーのデータは，スマートセンサーメーカー毎に収集を行い，プライバシーポリシーに応じてデータの第三者共有を行っている．それらのデータアクセス認可は各メーカーが独自に取り組んでおり，プライバシーポリシーの同意はアプリや Web 上でユーザーから取得している．しかしながら、ポリシーの更新や新しいデバイスの利用に際しては、ユーザーに度々確認を取る必要があり，その対策としてプライバシーポリシーマネージャー(PPM)の研究が行われている．

従来の認可基盤は、平常時のデータ利活用やプライバシーポリシーの同意情報の取得のために作られてきた．平常時だけでなく非常時の際にも個人のプライバシーポリシーを考慮した，迅速で柔軟なデータアクセス認可を行う事が求められる．

本論文では，平常時と非常時の両方への対応が求められる公民館を対象とし，公民館内で動作する建物 OS である Multimode Kominkan Operating System（MKOS）を想定した，警戒レベルとプライバシーポリシーを活用する非常時に対応可能なプライバシーポリシーマネジメント・認可基盤を提案する．

課題として，MKOS 内で収集されるセンサーデータ，館内・台帳データに対しては，平常時だけでなく非常時にも利活用するために状況判別する必要がある．また，個人情報・プライバシー情報に対してユーザーの意向に沿ったデータ利活用をしなければならない課題が存在する．

平常時だけでなく非常時にも利活用するために状況判別する課題に対しては，非常時に各自治体から発令される防災情報である警戒レベルを用いることを提案した．これにより，地域ごとに避難の必要性の観点から非常時の状況を総合的に判断することが可能になる．また，地震や津波といった災害毎に発令される情報を用いないことによりポリシーの設定数を少なくすることが可能になる．

個人情報・プライバシー情報に対してユーザーの意向に沿ったデータ利活用をしなければならない課題に対しては，MKOS 内の平常時・非常時ポリシー管理モジュール内で，ユーザー毎に同意情報ポリシーを設定することを提案した．これにより，データを受け渡すサービスを指定することや警戒レベルを用いた平常時・非常時の状況に応じたデータ共有の指定をすることが可能になる．

そのため，公民館内のセンサーデータや館内・台帳データに対し，平常時・非常時の状況に応じてユーザーの意向に沿ったデータ利活用をすることができる．また，アプリケーション・サービスはこれまで取得できなかったデータを災害状況に応じて柔軟にデータを取得することが可能になり，災害時のデータ利活用の幅が広がることが期待される．

目次

図目次

表目次

第1章 はじめに

本章では，本研究の背景，目的，本文の構成について述べる．

1.1 研究背景

現在、スマートセンサーのデータは，スマートセンサーメーカー毎に収集を行い，プライバシーポリシーに応じてデータの第三者共有を行っている．それらのデータアクセス認可は各メーカーが独自に取り組んでおり，プライバシーポリシーの同意はアプリや Web 上でユーザーから取得している．しかしながら、ポリシーの更新や新しいデバイスの利用に際しては、ユーザーに度々確認を取る必要があり，その対策としてプライバシーポリシーマネージャー(PPM)の研究が行われている．

これまでは平常時のデータアクセス認可についてのみ想定したものが中心であったが，近年では災害時などのデータ活用が進んでおり，今後は平常時だけでなく，非常時にも適切に対応できるデータアクセス認可の仕組みが必要とされる．

1.2 研究目的

本研究では平常時に加えて非常時にも対応できるプライバシポリシーマネージャー・認可基盤の提案する．

従来の認可基盤は、平常時のデータ利活用やプライバシーポリシーの同意情報の取得のために作られてきた．平常時だけでなく非常時の際にも個人のプライバシーポリシーを考慮した，迅速で柔軟なデータアクセス認可を行う事が求められる．

非常時のレベル感に応じたデータアクセス認可ポリシーを用いることで，適切なデータ利用者にデータの第三者共有が可能となり，非常時のデータ利活用の幅を広げる事ができる．それに加え，ユーザーのプライバシーポリシー情報を活用することで，非常時でも極力ユーザーの意向に沿ったデータアクセス認可を行うことが可能となる．

1.3 本文構成

- 第 1 章
  - 研究背景と研究目的について述べる.
- 第 2 章
  - 個人情報・プライバシー情報，プライバシーポリシーマネージャー，データ連携基盤，スマートビル，建物 OS を調査した現状や連携技術について述べる.
- 第 3 章
  - 検討する公民館 OS の要件について述べる.
- 第 4 章
  - システムの具体的な提案手法について述べる.
- 第 5 章
  - 本研究で提案するシステムの評価について述べる.
- 第 6 章
  - 本研究で提案するシステムの考察について述べる.
- 第 7 章
  - 本論文のまとめについて述べる.

第2章 関連研究・技術

本章ではプライバシーポリシーマネージャーと公民館内でのデータ連携基盤に関する関連研究・技術について，以下の項目について述べる．

1．個人情報・プライバシー情報
2．プライバシーポリシーマネージャー
3．データ連携基盤
4．スマートビル
5．建物 OS

2.1 個人情報・プライバシー情報

個人情報・プライバシー情報は，生きている個人に関する情報で、特定の個人であると分かるもの及び他の情報と紐づけることにより容易に特定の個人であると分かる情報である．個人情報は，個人情報保護法によって定められている個人を識別可能な情報とされており，例として，氏名，生年月日，住所，居所，電話番号などが挙げられる[1]．また，プライバシー情報は，個人情報保護法で定められていないが個人に関連する情報であり，プライバシー情報の例としては，個人の関心，習慣といった情報がある[2]．

現在，IoT 技術やセンサー技術の進歩により，公共施設や公民館内においても個人に紐づくデータを取得する機会が増加している．それによりデータの扱い方に応じて，ユーザーのプライバシーを侵害する課題が存在する．

そのため，個人情報・プライバシー情報は個人の同意に基づいてデータ共有や利活用をする必要がある．

2.2 プライバシーポリシーマネージャー

個人の同意に基づいてデータの活用方法を効率的に行う為にプライバシーポリシーマネージャが存在する．プライバシーポリシーマネージャー(PPM)は，データ提供者のプライバシーポリシーを用いて，個人情報やプライバシー情報のアクセス制御機能を提供する．

個人情報は、ターゲッティング広告などで幅広く利用されており、自分とは関係の無いサービスの個人情報を利用されてしまっているという問題がある。

それを改善するため、サービスや国ごとにプライバシーポリシーを定めている。しかし、ユーザーのプライバシーポリシーに対する技術・法的知識が不足している事や、自身でプライバシーポリシーの確認・維持をする負担も課題となっている。

これらの課題を解決するため、“PPM: Privacy Policy Manager for Personalized Services”[3]では、パーソナルデータサービス(PDS)の中でもユーザーが管理しやすいパーソナライズドサービスのためのアーキテクチャを検討している。システム概要を図 1 に示す．特に Privacy Policy Manager (PPM)と呼ばれるコアモジュールを設計し、ID 管理とプライバシーポリシー管理の 2 つの機能を提供することにより，サービスに対して、ユーザーの意向に沿った個人情報・プライバシー情報のアクセス制御を可能としている．

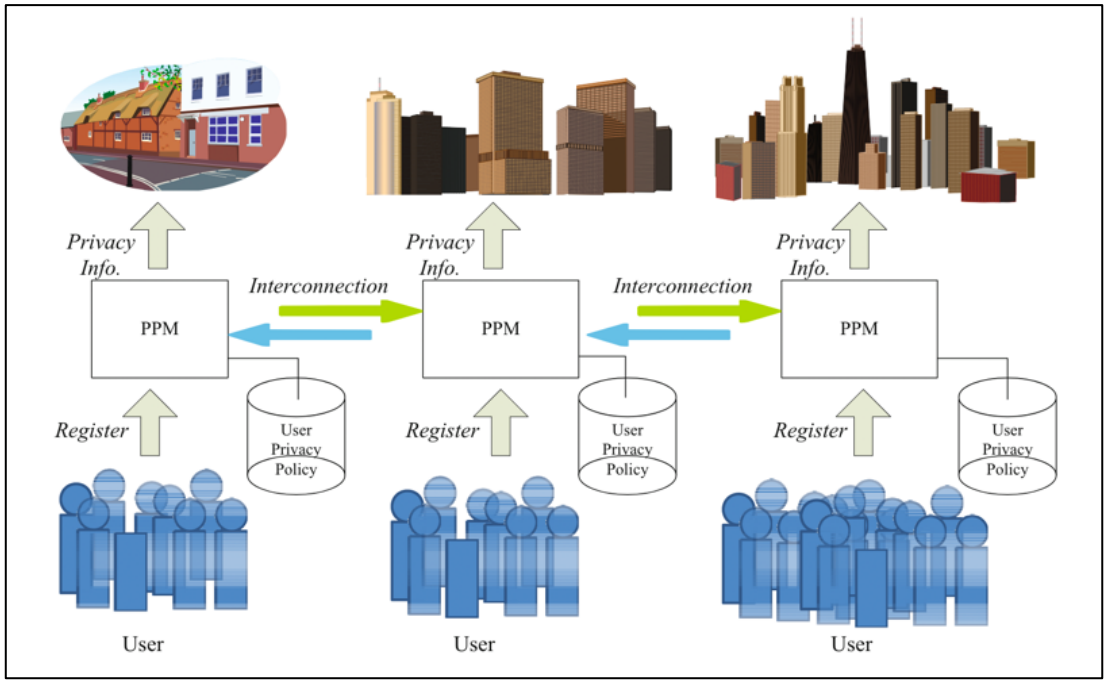

図 1　Architecture for Privacy Policy Management

また，”Privacy Mediators: Helping IoT Cross the Chasm”[4]では，データに関するプライバシーの不安は，IoT 機器の普及の遅らせる要因になり，センサデータに対してユーザーのコントロールができない事が不快感の原因としている．そのため，データ提供する際にユーザーのプライバシーポリシーに基づくプライバシー制御を行う環境が必要であるため，プライバシーメディエータと呼ばれるクラウド上のプライバシー制御アーキテクチャを提案している．システム概要を図 2 に示す．通常の場合は，IoT 機器のセンサーデータは直接 PublicCloud に提供されるが，提案手法では，センサーデータを Public Cloud に提供前に Private Cloudlet 上の PrivacyMediator でプライバシー制御を行い，プライバシーポリシーで許可されたセンサーデータのみ提供する手法を用いている．

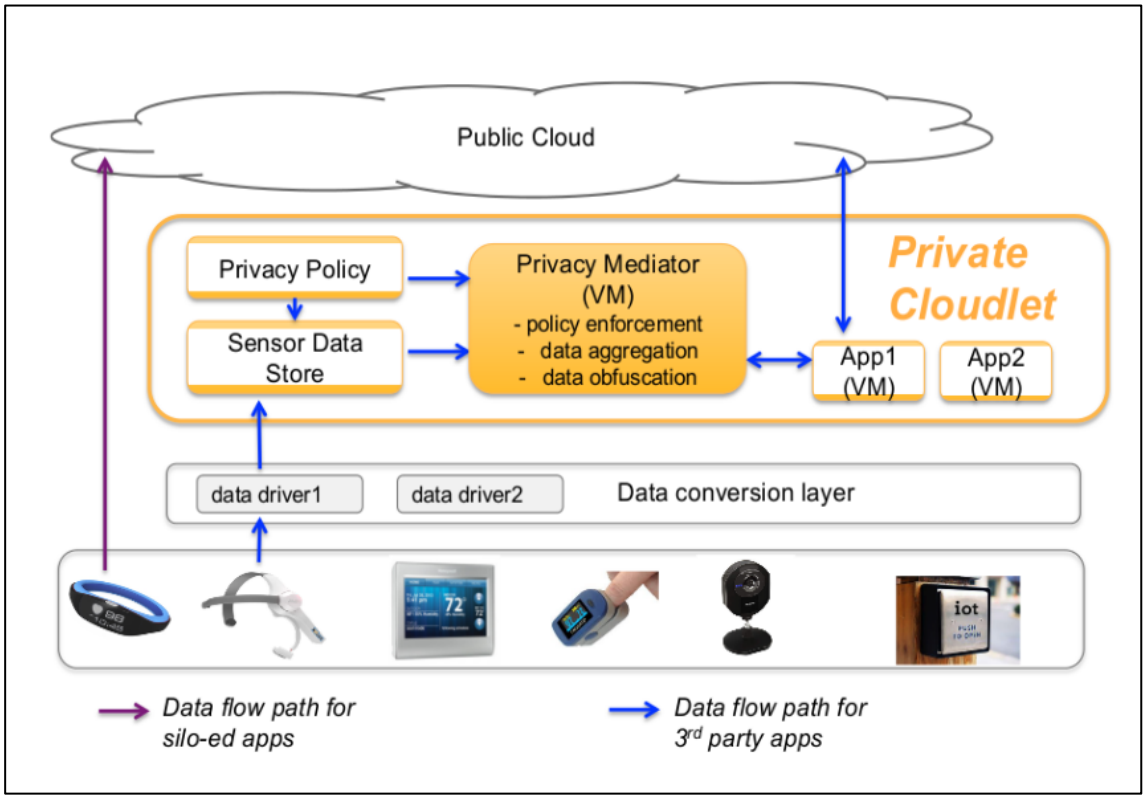

図 2　Privacy Architecture

そのほか，“A Hypervisor-Based Privacy Agent for Mobile and IoT Systems”では，モバイル機器や IoT 機器から提供されるデータは、個人情報と関連しやすい性質を持っており，多くのデータを企業に提供している点や，機器が増えると個々の機器にプライバシーポリシーを適応するのは負担が大きい点を課題として挙げ，これを解決するためエンドデバイスのハイパーバイザー上で動作するプライバシーエージェントを提案している[5]．システム概要を図３に示す．Privacy Agent Guest 上でプライバシーポリシーに基づくデータのフィルタリングを行った後に IoT Device App にセンサデータを提供する流れとなっている．Privacy Agent Guest 内では，Peripheral Data Anonymization にてデータを加工する機能を提供している．また，Mode Decision Engine データの加工方法を選択し，Peripheral Data Anonymization へ加工方法を伝達する機能を提供し，User Interface Module では，ModeDecisionEngine と PeripheralDataAnonymization で実行されるポリシーをユーザーが定義するために利用している．これらの機能により，データを IoT Device App に提供する前に，センサーデータのフィルタリングを実現している．

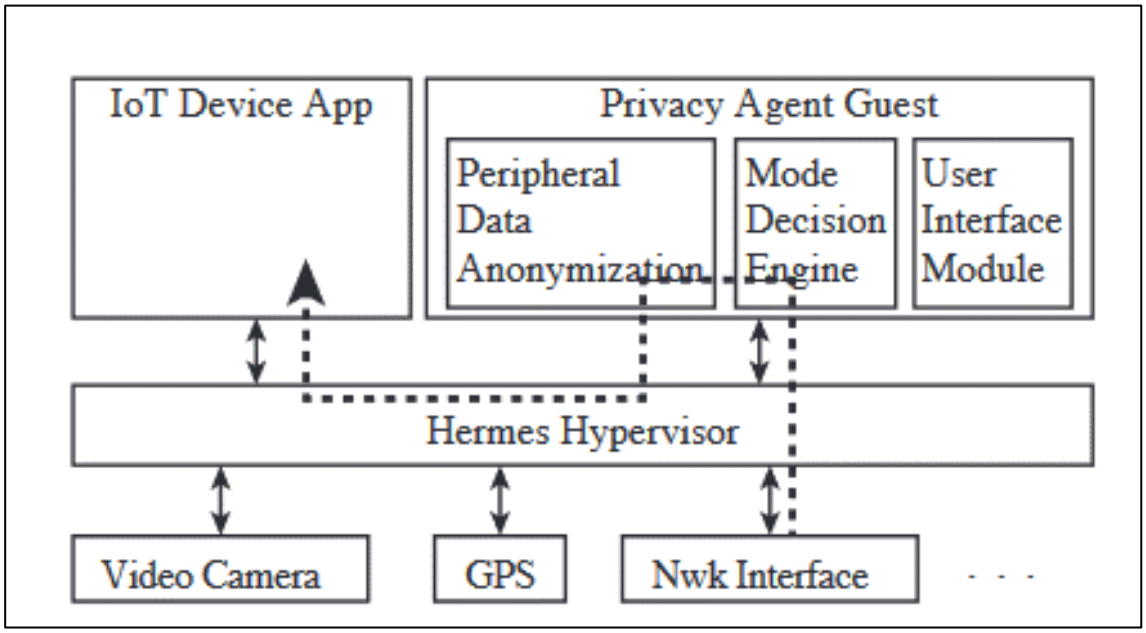

図 3　Hermes hypervisor

2.3 データ連携基盤

データ連携基盤は，様々なシステムやセンサーから生成されるデータを集約し、適切な形式に変換・保存をして，データ利用者へデータを共有する基盤である．これまでは，企業や団体といった限られた領域内でデータの保存や共有によるデータの利活用が行われていたが，データ連携基盤を用いることで，既存のデータを様々な企業や団体が利活用することが可能になる．図 4 にデータ連携基盤の例を示す．

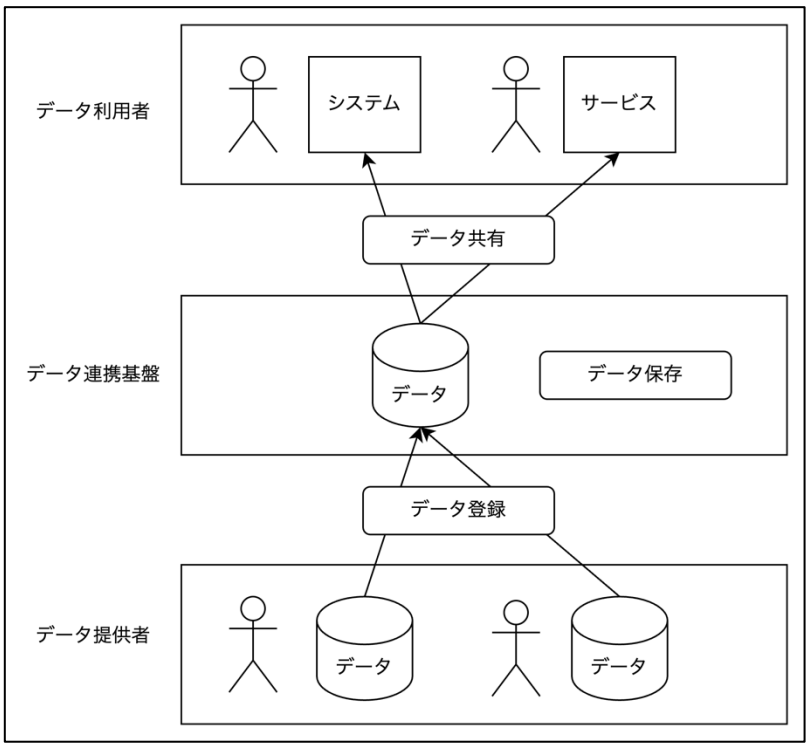

図 4　データ連携基盤

データ連携基盤の一つに Fiware Orion が存在する[6]．　FIWARE Orion は、スマートシティ向けのオープンソースソフトウェアであり、データの登録や参照、履歴データの管理などを行うことが可能であるため，スマートシティ構想において、行政機関や企業に蓄積されたデータを安全に収集し、様々なシステム間で利活用できるようにするために使用されている．

2.4 スマートビル

スマートビルは建物内の設備をデータ連携を通じて遠隔制御することやデータ利活用を行い効率的な管理が可能な建物である．情報処理推進機構ではスマートビルに関するガイドラインを提供しており，スマートビルアーキテクチャガイドラインでシステムの概念や標準的な仕様について解説されている．図 5 にシステム構成について示す[7]．

このシステム構成ではデータ連携をフィールド層，データ共有・管理層，アプリケーション層の 3 層に分けて示している．

フィールド層では，物理的なビル内の設備機器が管理される層となっておりデータを取得することや制御命令を行うといった処理が行われる領域となっている．データ共有・管理層では，ビル OS が存在しておりビル OS 内で建物設備のデータを管理する機能を提供する領域となっている． アプリケーション層では，ビル OS からデータを取得し利活用することや，フィールド層のビル設備に対して遠隔制御命令を行う領域である．

ガイドラインを参考にシステム設計をすることでスマートビルのデータ連携や遠隔制御に関する相互運用性を高め，より効率的な施設設備やデータの利活用が期待されている．

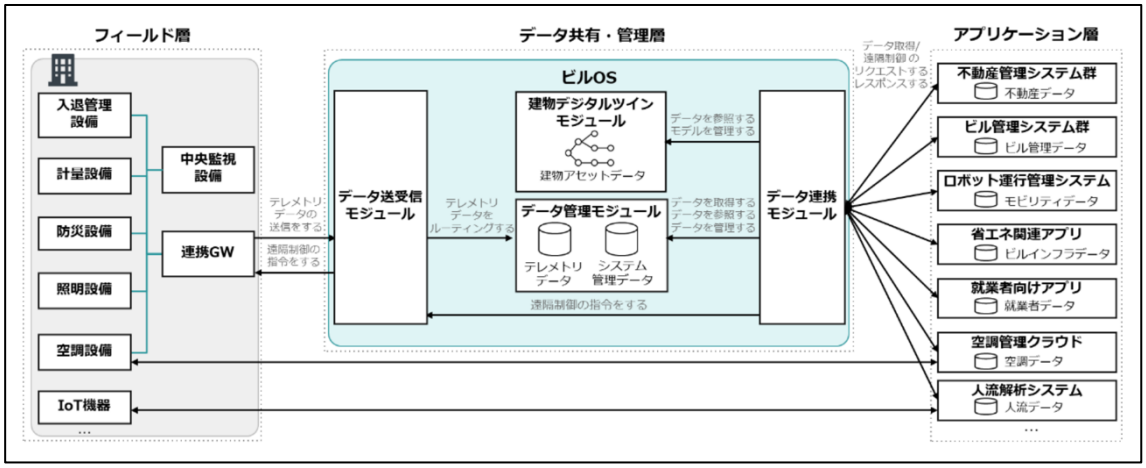

図 5　スマートビルのシステム構成

2.5 建物 OS

建物 OS は，ビル内のセンサーや外部システムから施設情報を取得・蓄積・共有し，設備機器を制御する機能を提供するソフトウェアのことを指す．

建物 OS の一つに，清水建設の DX-Core が存在する．全体像を図 6 に示す．これまでの建物内の設備制御は，中央監視システムを用いて建物ごとに設備をまとめて管理・制御するものであったが，現在は，IoT 機器の利用が増加し，建物と直接接続されず独自に利用されるものが増加している．それらを管理するために DX-Core での API 接続機能やデータプラットフォーム機能を用いている．

API を通じて DX-Core にデータを収集し，データの解析を行うことや様々なアプリケーションに対してデータを共有，様々な機器を効率的に制御することで効率的な管理を実現することが可能になる．

建物に特化したデジタルプラットフォームを構築することで，従来の建築設備の枠に収まらない新たなサービス・ソリューションを実現することが可能になる[8]．

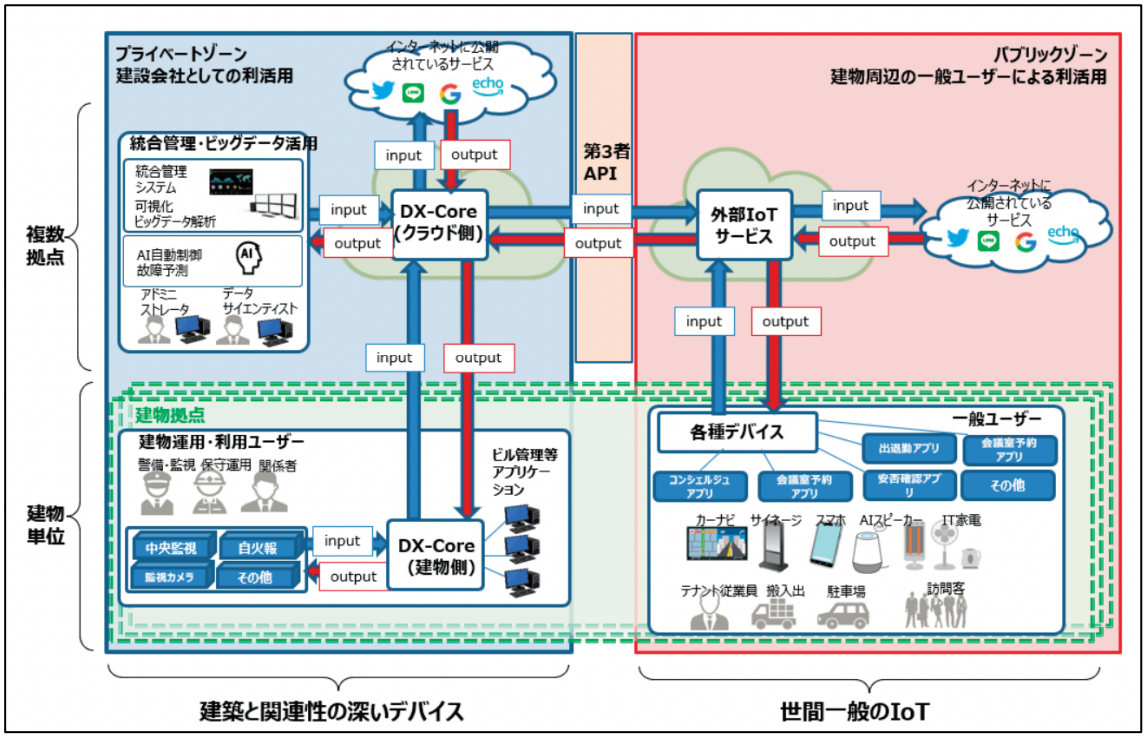

図 6　DX-Core の全体構成

第3章 検討する公民館 OS

本章では，検討する公民館 OS に必要となる要素について述べる．

3.1 ユースケース

公民館は，市町村ごとに設置・管理される公共施設であり，地域住民向けの文化・健康・教育事業を行う社会教育施設や地域の集会施設として利用されており，日本に多数存在している．

地震といった災害発生時には，公民館の建物内には生活設備としてトイレや食事施設があるため，避難所や災害時の拠点として活用される．

そのため，公民館は，平常時は，住民のための教育・社会福祉施設として活用され，非常時は，避難所や食料・医療・情報提供の場として利用される．

現在，公民館には行政で管理されている地域住民のデータや，公民館内にセンサーを設置することによる建物内外の様々なデータを取得することが可能である．また，IoT 機器の普及に伴いエアコンといった家電も遠隔で操作することが可能である．

これらのデータやデバイスを建物で適切に管理する建物 OS により，平常時・非常時の状況に応じて，様々なデータの利活用が可能になることや，デバイスの効率的な制御が可能になる．また，近年，災害時などのデータ活用が進んでおり，平常時だけでなく，非常時にも適切に対応できる建物 OS 内でのデータアクセス認可の仕組みが必要とされる．

平常時・非常時の状況に応じた公民館のユースケースを，表 1 — 4 に示す．平常時・非常時の状況に応じて，これらのユースケースに対応可能なデータアクセス認可をする必要がある．

表 1　ユースケースリスト（施設管理）

カテゴリ	ユースケース名	目的	稼働状況
1. 施設管理	1.1 温熱管理	室内の温熱を快適な状態に管理する目的	平常時・非常時
	1.2 空気質管理	室内の空気と外気を入れ替えることや，空気清浄機を用いることで，室内の空気質を管理する事が目的	平常時・非常時
	1.3 照明管理	効率的なエネルギー使用、環境への配慮、快適な照明環境の提供	平常時・非常時
	1.4 電子錠を用いた施設の鍵管理	カードキーを権利者に付与することで，施設の鍵を管理する目的	平常時・非常時
	1.5 電子錠・スマホを用いた鍵権限の付与・管理	部屋の利用者に，一定期間のみ解錠できる権限をスマホに付与する事で，部屋の鍵管理や利用者の利便性を向上する目的	平常時・非常時
	1.6 キーボックスの鍵管理	キーボックスの鍵を遠隔で管理することで，複数の鍵を管理する目的	平常時・非常時
	1.7 在室人数の管理	感染症発生時に密閉空間を防ぐ目的	平常時・非常時
	1.8 宅配ボックスとしての利用	地域住民の郵便物の配達場所として利用する目的	平常時・非常時

表 2　ユースケースリスト（災害・防犯監視）

カテゴリ	ユースケース名	目的	稼働状況
2. 災害・防犯監視	2.1 火災検知	早期に火災を検出し、その情報を適切な人々やシステムに迅速に通知	平常時・非常時
	2.2 水害監視	過剰な雨量や地下水位の異常上昇を検出し、洪水や水害のリスクを早期に把握	平常時・非常時
	2.3 雪害監視	大雪や吹雪による施設建物や駐車場の積雪量監視が目的	平常時・非常時
	2.4 風害監視	異常な風速または突風を検出し、風による損害や危険のリスクを早期に把握	平常時・非常時
	2.5 豪雨監視	豪雨や大雨による被害の早期発見と予防が目的．異常な降水量を検出	平常時・非常時
	2.6 不審者への防犯監視	不審者への防犯を目的とし，建物周囲を監視する．	平常時・非常時
	2.7 害獣対策としての監視	害獣から施設を守ることを目的とし，建物周囲を監視する．	平常時・非常時

表 3　ユースケースリスト（健康医療）

カテゴリ	ユースケース名	目的	稼働状況
3. 健康・医療	3.1 健康診断	住民の健康状態を管理する目的	平常時のみ
	3.2 遠隔診療向け個室整備	診察時には患者の個人情報を扱うため、第三者が室内にいない状態をつくるなど「プライバシーを確保」することが目的	平常時のみ
	3.3 体温監視	公民館の訪問者や職員の健康状態を監視し、発熱などの症状を早期に検出する目的	平常時・非常時
	3.4 メンタルヘルスケア	個々の人の精神的健康状態を把握し、必要に応じて適切なケアやサポートを提供	平常時・非常時

表 4　ユースケースリスト（避難所利用）

カテゴリ	ユースケース名	目的	稼働状況
4. 避難所利用	4.1 避難者名簿作成	顔写真やマイナンバーカードでのチェックインを行い名簿を作成．避難した人としていない人を管理する目的	非常時のみ
	4.2 仮設居住場所の割り当て	チェックインした避難者に，仮設居住場所を割り当てる目的	非常時のみ
	4.3 備蓄品在庫管理	避難所利用時の備蓄品の在庫管理をする目的	平常時・非常時
	4.4 倉庫から各避難所への備品管理	倉庫から各避難所へ備蓄品を郵送する際の数量の管理目的	非常時のみ
	4.5 分散避難時の物資配給拠点	各世帯にて避難する分散避難時に食料や水，生活用品といった物資を配給する場所として利用	非常時のみ
	4.6 非常時の電力管理	電力供給が中断された場合にも、重要なシステムやデバイスの運用を維持する	非常時のみ
	4.7 避難者位置情報の救助隊情報共有	各部屋や避難経路上のユーザーを検知し，避難者の位置状況把握を行い，救助隊への現場状況連絡へ用いる．	非常時のみ
	4.8 避難経路支援	火災場所といった通れない場所の地点情報を元に，安全な避難経路をユーザーに通知する．	非常時のみ
	4.9 避難者位置情報を用いた安否確認	避難者の位置状況をもとに家族や公的機関での安否確認情報として用いる．	非常時のみ
	4.10 避難所での健康状態監視	避難所利用時に，避難者の健康状態を監視し，感染症対策へ繋げる目的	平常時・非常時

これらのユースケースは平常時・非常時動作するパターンや，平常時のみ動作するパターン，非常時のみ動作するパターンが存在する．

平常時・非常時動作するパターンでは，平常時・非常時の状況に応じてアクチュエータの動作や取得可能なデータを調整することを想定している．

例えば，「1.1 温熱管理」や「1.2 空気質管理」，「1.3 照明管理」のユースケースは，平常時に公民館利用者の快適さを重視した動作をするが，非常時にはエネルギー消費を最小限に抑える動作に切り替えるといったことが考えられる．

また，「3.3 体温監視」や「4.10 避難所での健康状態監視」のユースケースでは，平常時に公民館職員のみに体温情報を共有するが，非常時には避難所での感染症拡大防止や人命救助のため公民館職員だけでなく，適切な医療機関へ体温情報を共有するといった，極力プライバシーに配慮しつつ非常時の状況に応じて人命保護や財産保護のためにデータ共有を行うように、データアクセス認可の動作を切り替えることが考えられる．

平常時のみ動作するパターンでは，平常時の中でも災害発生の可能性があり警戒段階の注意報が発令されている場合や，避難準備する段階である警報が発令されている場合など，平常時の中でも複数のレベルが想定される．

非常時のみ動作するパターンでは，非常時の中でも自主的に避難を開始する場合や，避難指示が出ている場合，災害が切迫しており安全確保をしなければならない場合など，非常時の中でも複数のレベルがあると考えられる．

そのため，平常時・非常時の状況に応じて適切なアクチュエータの動作や取得可能なデータを調整する必要があると考えられる．

3.2 警戒レベル

警戒レベルは，気象庁によって定められた非常時に各自治体から発令される防災情報である[9]. 従来の地震や津波といった災害毎に発令される情報とは異なり，住民が取るべき避難行動を直感的に理解できる防災情報として災害状況を総合的に各自治体が判断し，発令される. 防災気象情報と警戒レベルに関する図を図 7 に示す. レベルはレベル 1 からレベル 5 の 5 段階となっており，レベルごとに災害状況や避難の必要性の有無が定められている. また，警戒レベルは各自治体の市町村長が定めるため，ある特定の人物によって状態が明確化される点や避難指示の出たエリアが明確化されるといった特徴がある.

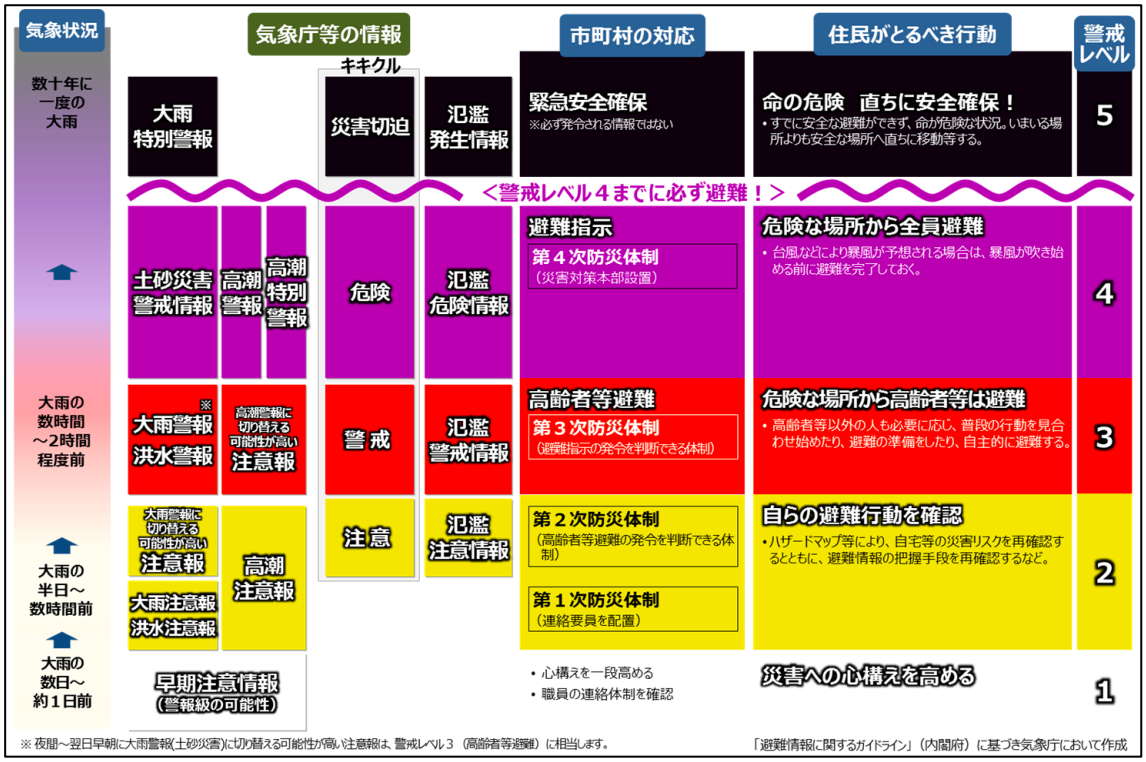

図 7　段階的に発表される防災気象情報と対応する行動

3.3 非常時・平常時の定義

本論文では，平常時・非常時を警戒レベルを用いて定義する．平常時は警戒レベルが２以下の場合とし，非常時は警戒レベル３以上の場合とする．

警戒レベルは，レベル２以下では注意・警戒することが中心となり実際に避難は行わない．しかし，段階レベル３では高齢者等が避難を開始し，レベル４では全員避難となる．本研究では，避難の必要性の有無が明確になるのがレベル３以上の場合であるため非常時を上記のように定義した．また，公民館といった市町村毎の避難所が避難者の受け入れ準備をする基準となるため，避難が必要になる点を重視した．

3.4 認証技術

認証は，利用者本人であるか確認を行うことを指す．認証技術の一つに OpenID Connect[10]が存在する．OpenID Connect は，利用者本人のアイデンティティを検証することができ、利用者本人のプロフィール情報も取得することが可能である．認証の際には，Access Token を用いて情報のやり取りが行われる．

3.5 認可技術

認可は，利用者に適切な権限を与えることを指す．認可技術の一つに User-Managed Access(UMA)2.0[11]が存在する．UMA2.0 は，アクセス管理プロトコルであり，データ利用者がデータ所有者に対しデータアクセス要求を行い，データ所有者が許可した場合に、保護されたデータへのアクセスをすることが可能になる．認可の際には Requesting Party Token(RPT)を用いて情報のやり取りが行われる．

3.6 ポリシー

公民館内では，平常時だけでなく非常時の状況に応じてデータをアプリケーションに対してアクセス認可する必要がある．また，個人情報やプライバシー情報といったデータを扱う場合も考えられるため，個人の意向に沿ったアクセス認可を行わなければならない．そのため，平常時・非常時の状況に応じて，個人の意向に沿ったデータアクセス認可を行う必要がある．

しかし，個人の意向をシステムが取り扱うためには，個人ごとのデータの扱いについてのポリシー情報を事前に準備しなければならない．

そのため，平常時・非常時の状況と個人の意向に沿ったデータを活用するためのポリシー構造をどのように定めるべきかといった課題が存在する．また，公民館管理者によって公民館内でデータをどのように利用するか定める必要がある事や、システムがどのようなポリシーを参照し認可処理を行うべきか定める必要がある．

以下で，公民館 OS 内で用いるポリシーについて説明する．

3.6.1 災害情報ポリシー

災害情報ポリシーは，データ管理者である公民館管理者がデータ毎に，警戒レベルに応じた認可対象アプリケーションを設定することで，警戒レベルに応じたデータ認可を可能とするポリシーである．どのデータがどのアプリケーションに対してデータ認可が可能になるかを定める為に用いられる．

データ構造は，表 5 のように，「データ名＞アプリケーション名＞警戒レベル」の順に指定する形になっている．公民館管理者によって公民館内でどのデータがどのアプリケーションに共有可能であり，どの警戒レベルの際に認可可能か参照可能である．

表 5　災害情報ポリシー

データ名		データ 1	
アプリケーション名		アプリケーション 1	アプリケーション 2
警戒レベル	レベル 0	TRUE	FALSE
	レベル 1	TRUE	FALSE
	レベル 2	TRUE	FALSE
	レベル 3	TRUE	TRUE
	レベル 4	TRUE	TRUE
	レベル 5	TRUE	TRUE

3.6.2 同意情報ポリシー

同意情報ポリシーは，データ所有者がポリシーを設定することで，ユーザーの意向に沿ったデータ認可を可能とするポリシーである．

データ構造は，表 6 のように，「ユーザー名＞データ名＞アプリケーション名＞警戒レベル」の順に指定する形になっている．ユーザーが特定のアプリケーションに対してはデータを共有したくない場合や，警戒レベルが 3 以上の場合のみデータを共有するといった際に，適切なポリシーを指定することでユーザー毎に適したデータアクセス認可を可能とする．

表 6　同意情報ポリシー

ユーザー名		ユーザー 1	
データ名		データ 1	
アプリケーション名		アプリケーション 1	アプリケーション 2
警戒レベル	レベル 0	TRUE	FALSE
	レベル 1	TRUE	FALSE
	レベル 2	TRUE	FALSE
	レベル 3	TRUE	TRUE
	レベル 4	TRUE	TRUE
	レベル 5	TRUE	TRUE

3.6.3 データアクセス認可ポリシー

データアクセス認可ポリシーは，認可システム内の認可処理の際に参照されるポリシーであり，現在の警戒レベルに応じて適切なデータアクセス認可が可能になる．災害情報ポリシーと同意情報ポリシーの 2 つのポリシーを元に作成される．

データ構造は，表 7 のように「データ名＞ユーザー名＞アプリケーション名＞警戒レベル」の順に指定する形になっている．現在の警戒レベルでは，データ毎にどのユーザーのデータを認可可能かどうか参照可能になっている．

表 7　データアクセス認可ポリシー

データ名		データ 1			
ユーザー名		ユーザー 1		ユーザー 2	
アプリケーション名		アプリケーション 1	アプリケーション 2	アプリケーション 1	アプリケーション 2
警戒レベル	レベル 0	TRUE	FALSE	TRUE	FALSE
	レベル 1	TRUE	FALSE	TRUE	FALSE
	レベル 2	TRUE	FALSE	TRUE	FALSE
	レベル 3	TRUE	TRUE	TRUE	FALSE
	レベル 4	TRUE	TRUE	TRUE	TRUE
	レベル 5	TRUE	TRUE	TRUE	TRUE

3.6.4 ユースケースと提案内容のポリシーについて

ユースケースは、MKOS 内で管理されるデータを取得する事や公民館内のアクチュエーターを制御する事によって動作する。表１－４で示したようにユースケースには平常時・非常時の両方で動作するパターン、平常時のみ動作するパターン、非常時のみ動作するパターンがある。これらのユースケースのうち、平常時と非常時の両方で動き続けるものは 19 種類、平常時のみ動作するものは２種類、非常時のみ動作するものは８種類である。

これらのユースケースすべてのポリシーを設定することを考えた際，平常時と非常時の両方で動作するものは、警戒レベル０－５の合計 6 項目を設定し、平常時のみの場合は０－２の 3 項目，非常時のみの場合は３－６の 3 項目を設定する必要がある。

データ管理者の設定をするポリシーについて考えた際、データ管理者である公民館管理者は、19 種類存在する平常時・非常時のユースケースに対して６項目のポリシーを設定するため合計 114 項目の設定が必要になる。また、２種類存在する平常時のみのユースケースに対して３項目のポリシーを設定するため合計６項目、８種類の非常時のみのユースケースに対して３項目のポリシーを設定するため合計 24 項目となる。そのため，設定をするポリシー数は合計 144 項目のポリシーを設定する必要がある.

データ所有者は，プライバシー情報を用いるユースケースとデータ数に応じて，警戒レベル６項目分の同意情報ポリシーを設定する必要がある。そのため，一般的なデータ認可ポリシーでは，特定のデータに対しデータ認可の可否のみを定める１項目の設定することに比べ，６項目の設定する必要があり，データ所有者のポリシー設定の負担が大きくなってしまう点が挙げられる.

今回提案したポリシーは，平常時・非常時の状況ごとに指定できる点やデータ提供可能なユースケースを詳細に指定できるようになっているが、１項目のみを設定する従来の認可と比べ，設定項目が多くなるという特徴がある。

第4章 システム提案

本章では，想定される公民館OSであるMultimode Kominkan Operating System （MKOS）の具体的なシステム内容について述べる．

4.1 システム全体図

公民館 OS は Multimode Kominkan Operating System （MKOS）と呼称する．システム全体像を図８に示す．

MKOS は，公民館内で扱うセンサーや認証デバイス，アクチュエータ，館内・台帳データを管理し、データ共有機能，アクチュエータの制御機能を提供する公民館 OS である．この MKOS は 2023 年度電気・情報関係学会北陸支部連合大会北陸支部大会にて提案を行った[12][13]。また、MKOS によるアクチュエータの操作については陳氏の論文で取り組まれている[14]。

本論文では，平常時・非常時といった状況や個人の意向に応じて適切なアプリケーション・サービスに対して認証機能やデータアクセス認可を行う図８の赤枠部分について取り組んだ．

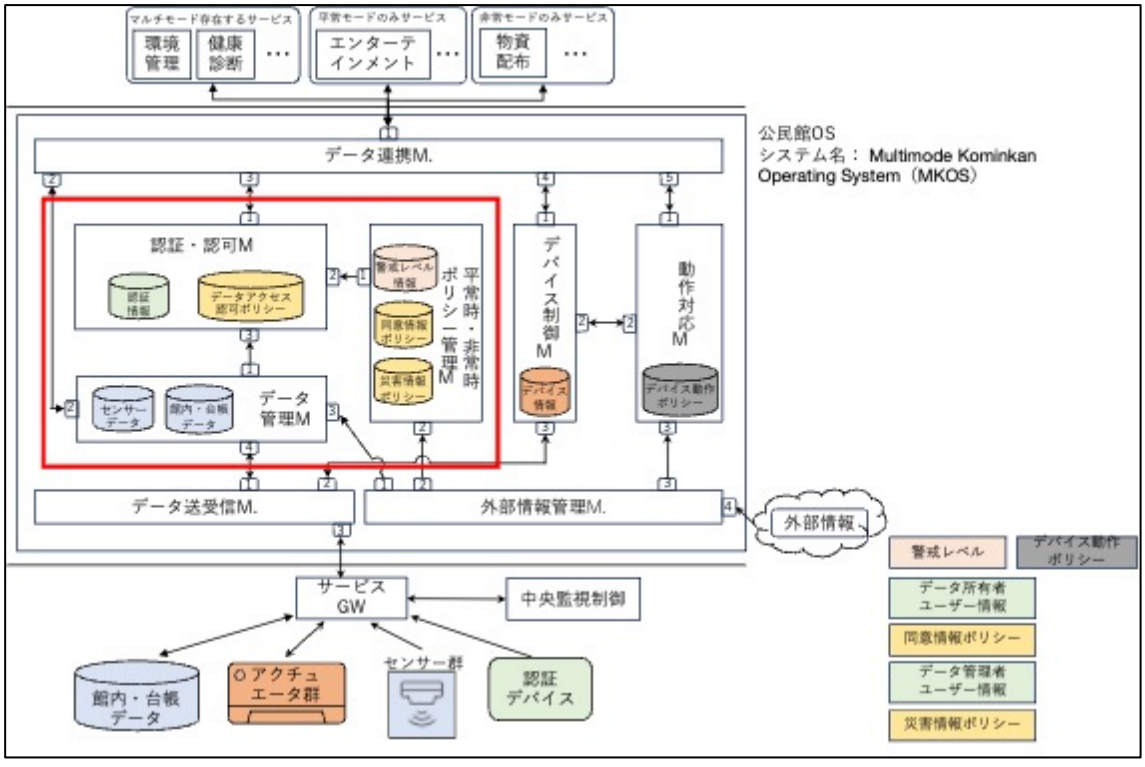

図 8　システム全体像

4.2 各モジュールの説明

提案モジュールは, 図 8 に示すように以下の要素で構成されている. 各モジュールについて述べる.

4.2.1 アプリケーション・サービス

3 章で述べたユースケースを満たすためのアプリケーション・サービスである. MKOS から公民館内のセンサーや認証デバイス, 館内・台帳データといったデータを取得後, サービスとしてデータの利活用や, 公民館内のアクチュエータの制御依頼を行う.

4.2.2 センサー, 認証デバイス

公民館内に設置されたセンサーで, 公民館内の情報を取得するデバイスである. また, 認証デバイスと用いることで個人情報・プライバシー情報を取得することが可能になる. 取得したデータは MKOS に送られデータが管理される.

4.2.3 データ連携モジュール

アプリケーション・センサーに対して API を提供し, 情報を適切なモジュールへ仲介する機能を持つモジュールである.

4.2.4 認証・認可モジュール

アプリケーション・サービス, データ管理者, データ所有者に対し認証機能を提供することや, データアクセス認可ポリシーを用いてデータアクセス認可機能を提供する.

4.2.5 データ管理モジュール

公民館内のセンサーデータ, 館内・台帳データを管理するモジュールである. データ送受信モジュールからデータを受け取り保存する機能やデータ連携モジュールからのデータ要求に対してデータ共有をする機能を持つ.

センサーデータは、公民館内に設置されたセンサーによって取得されるデータである。例としては、部屋毎に設置された温度、湿度データやカメラによって取得された画像・映像・音声データ、プライバシー情報であるカードキー認証データによる部屋の入退室状況の位置情報、公民館入退室の際に感染症防止対策として取得される体温情報などが想定される。

館内・台帳データは、公民館内で業務で活用される情報や行政によって管理される住民台帳情報である。例としては、公民館施設の予約状況や公民館利用者の情報、避難所として利用される際の備蓄品の情報が考えられる。また、避難所開設の際に避難者の確認を行うために用いられる避難者名簿情報などを想定している。

4.2.6 データ送受信モジュール

公民館内のセンサー，認証デバイス，館内・台帳データに対して API を提供する機能を持ち，データを受け取りデータ管理モジュールへ仲介するモジュールである．

4.2.7 外部情報管理モジュール

データ提供者やデータ管理者に対して API を提供する機能を持つ．外部情報である警戒レベル情報や災害情報ポリシー，同意情報ポリシーを受け取り、情報を適切なモジュールへ仲介する機能を持つモジュールである．

4.3 API 設計

データ連携モジュール，データ送受信モジュール，外部情報管理モジュールは API を提供する．ここでは，それぞれの API について述べる．

4.3.1 データ連携モジュール

データ連携モジュールでは，サービス・アプリケーションに対して認証機能とデータアクセス認可機能を用いてデータ取得を可能とする API を提供する．

API の設計を図 9 に示す．/api/token は，データ取得をするサービス・アプリケーションの認証，データアクセス認可を行う為に用いられる．/api/data は，サービス・アプリケーションが取得可能なデータを検索することができる．データを取得する際は，/api/data/{{data-id}}を用いてデータの取得を行う．

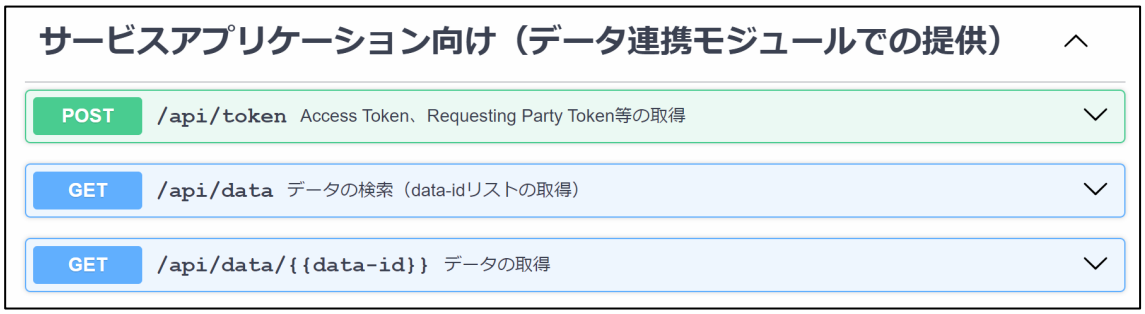

図 9　データ連携モジュール API

4.3.2 データ送受信モジュール

データ送受信モジュールでは，センサーデバイスに対してデータ作成・更新に関する API を提供する．

API の設計を図１０に示す．/api/token はセンサーデバイスの認証，データアクセス認可を行う為に用いられる．/api/data/{{data-id}}はセンサー毎にデータの作成，更新，削除を行う機能を提供する．

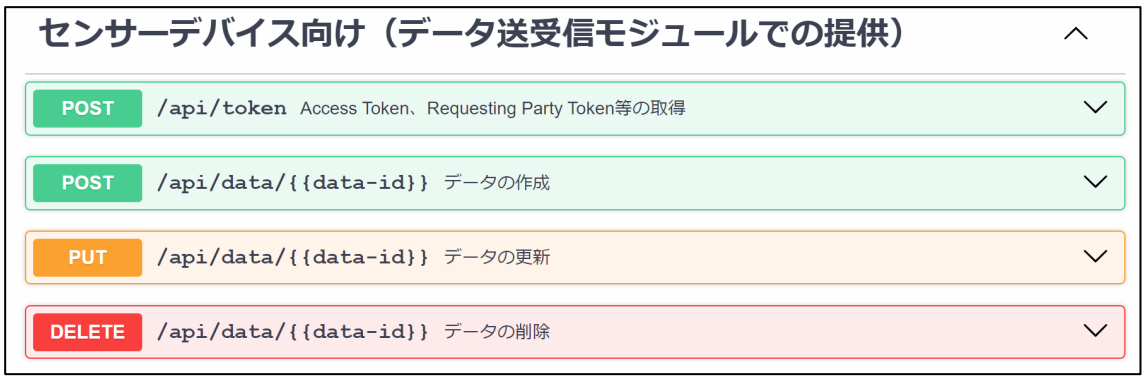

図 10　データ送受信モジュール API

4.3.3 外部情報管理モジュール

外部情報管理モジュールでは，データ所有者に対して認証・認可の機能とポリシー作成の機能に関する API を提供する．また，データ管理者に対しては認証・認可の機能とポリシー作成の機能の他，警戒レベルの設定に関する API を提供する．

API の設計を図 11 に示す．/api/token では，データ所有者，データ管理者に対しての認証・認可の機能を提供する．/api/outdata/policy では，データ所有者に対してはデータアクセス認可に用いる同意情報ポリシーの登録，読み出し，更新，削除機能を提供し，データ管理者に対してはデータアクセス認可に用いる災害情報ポリシーの登録，読み出し，更新，削除機能を提供する．/api/outdata/alertlevel では，データ管理者のみ使用することができ，現在の警戒レベルを設定する機能を提供する．

図 11　外部情報管理モジュール API

4.4 動作フロー

ここでは、各モジュールがどのように連携し動作するかについて述べる.

4.4.1 災害情報ポリシーの登録

図 12 は、災害情報ポリシー登録の動作フローを示した図である.

データ管理者は，クライアント(GUI)を用いて外部情報管理モジュールの提供する API に対して災害情報ポリシーを登録する．登録された災害情報ポリシーは平常時･非常時ポリシー管理モジュールに送られ災害情報ポリシーDB に登録される．また，災害情報ポリシーが更新された事によりデータアクセス認可ポリシーの更新処理が行われる．これにより，災害情報ポリシーの登録が行われ，認証・認可モジュールにてポリシーに基づいたデータアクセス認可を提供することが可能になる.

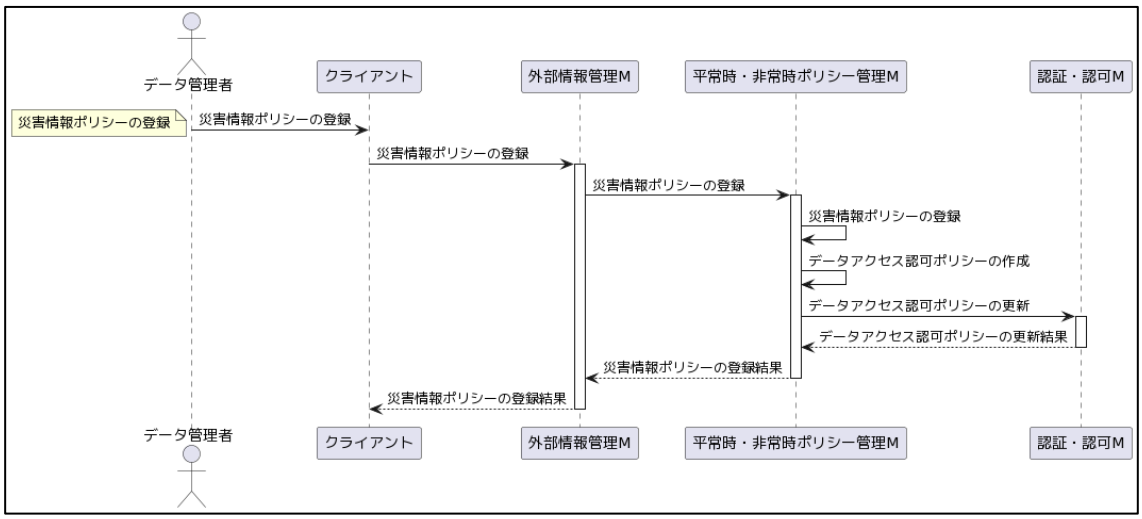

図 12　災害情報ポリシー登録の動作フロー

4.4.2 同意情報ポリシーの登録

図 13 は、同意情報ポリシー登録の動作フローを示した図である.

データ提供者は，クライアント(GUI)を用いて外部情報管理モジュールの提供する API に対して同意情報ポリシーを登録する．登録された同意情報ポリシーは平常時・非常時ポリシー管理モジュールに送られ同意情報ポリシーDB に登録される．また，同意情報ポリシーが更新された事によりデータアクセス認可ポリシーの更新処理が行われる．これにより，同意情報ポリシーの登録が行われ，認証・認可モジュールにてポリシーに基づいたデータアクセス認可を提供することが可能になる.

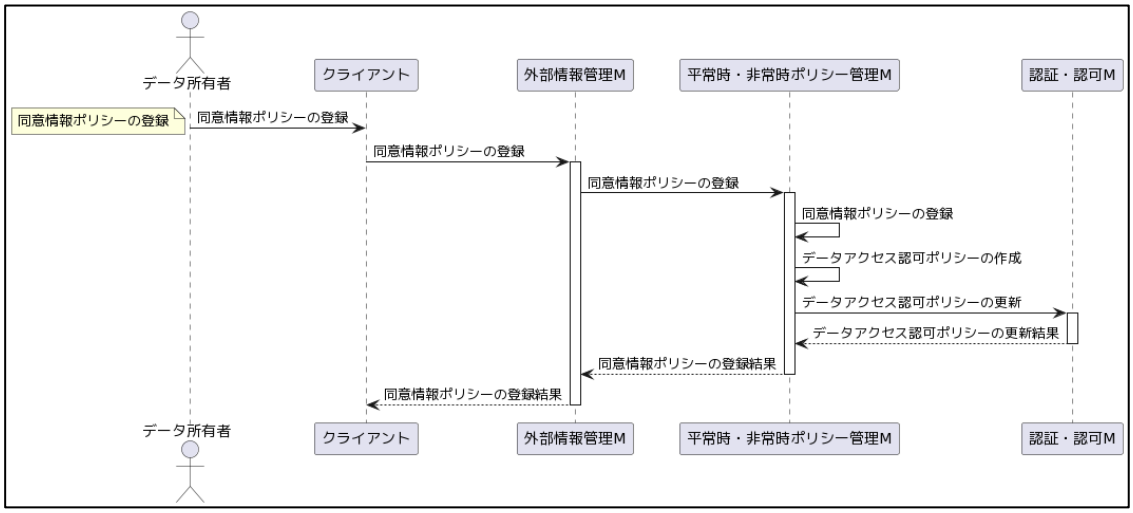

図 13　同意情報ポリシー登録の動作フロー

4.4.3 警戒レベルの登録

警戒レベル情報は、市町村長による発表とサイトによる公開が主となっており，現在は API 等で公開されてはいない．そのため、データ管理者である公民館管理者による手動の設定をする必要がある。しかし、将来的に API 等が整備された際には、システムが自動で平常時・非常時の状況判断をすることが可能となる。そのため、手動設定の場合と自動設定の場合の 2 パターンでの動作フローを以下に示す。

手動での警戒レベル設定の動作フローを図 14 に示す．手動設定の場合は、データ管理者が外部情報管理モジュールの API を経由して設定することを想定している。クライアント(GUI)を用いて外部情報管理モジュールの提供する API に対して警戒レベル情報を設定する．外部情報管理モジュールは警戒レベル情報を平常時・非常時ポリシー管理モジュールに送り，警戒レベル DB に保存する．その後，警戒レベルに応じたデータアクセス認可ポリシーの作成が行われ，認証・認可モジュールのデータアクセス認可ポリシーが更新される．これにより，非常時の状況に応じてデータアクセス認可が可能になる．

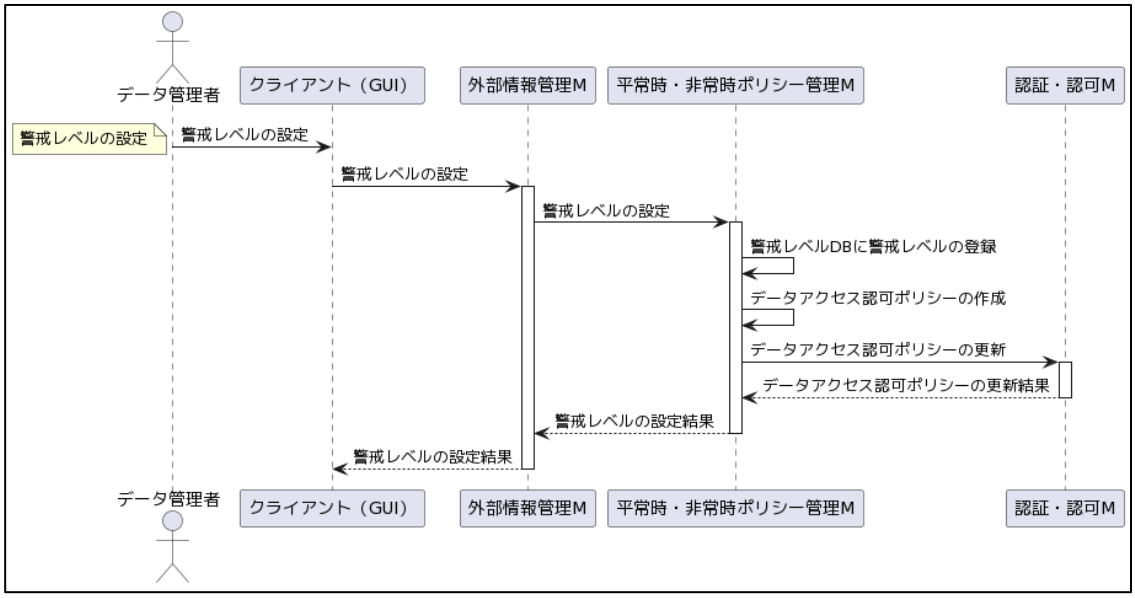

図 14　手動での警戒レベル設定の動作フロー

自動での警戒レベル設定の動作フローを図 15 に示す．自動設定の場合は、気象庁 API などの信頼できる情報提供元の API からシステムが定期的に警戒レベル情報を取得する。警戒レベル情報に変化があった際には、手動設定同様に平常時・非常時ポリシー管理モジュールに警戒レベル情報が受け渡され、認可処理に用いられるデータアクセス認可ポリシーが更新される。これにより、自動的にシステム自身が平常時・非常時の状況を判別することが可能となり、状況に応じて公民館内のセンサーデータや館内・台帳データを適切にアクセス認可することができる。

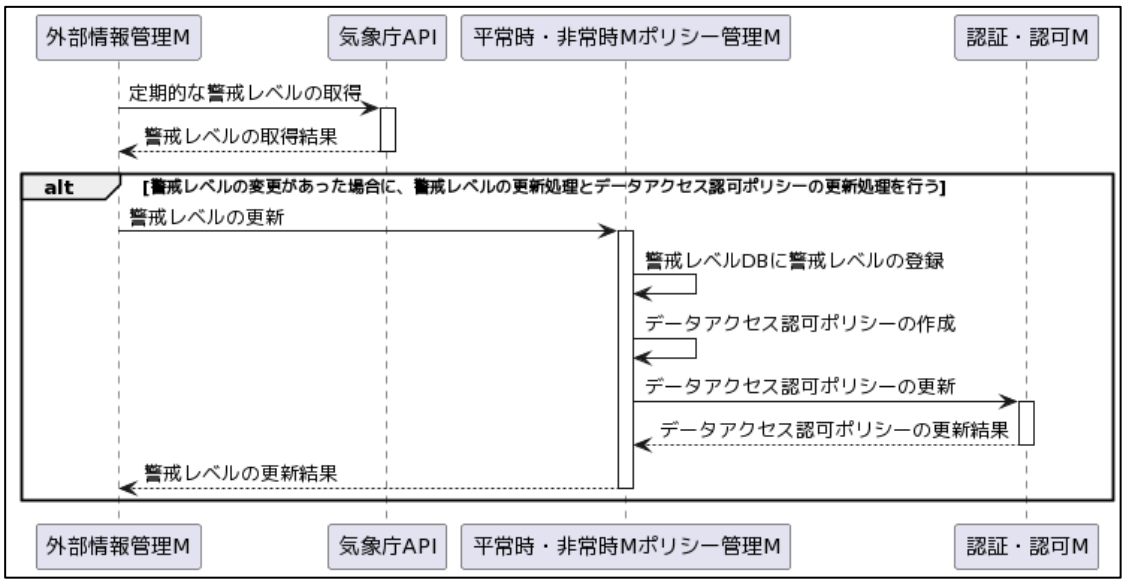

図 15　自動での警戒レベル設定の動作フロー

4.4.4 データの登録

図 16 は、データ登録の動作フローを示した図である.

はじめにセンサーデバイス・認証デバイスから認証情報とセンサーデータがデータ送受信モジュールに送られる. それらのデータはデータ管理モジュールに送られ, データの登録が行われる. データ登録の際には認証・認可モジュールにて認証情報の確認が行われ, どのデータ所有者のデータか確認が行われる. 最終的にデータの登録結果がデバイスに返答される.

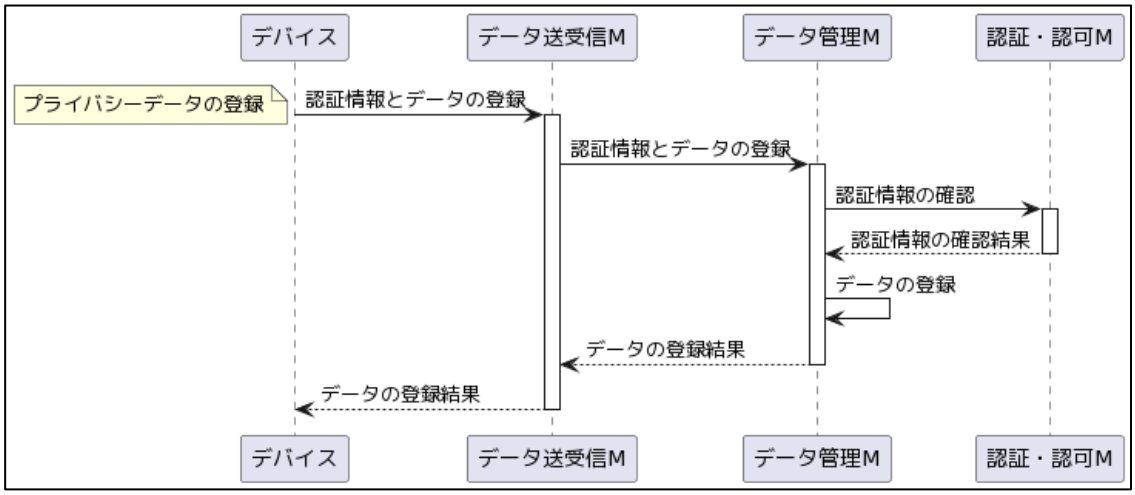

図 16　データ登録の動作フロー

4.4.5 データの検索

図 17 は、データ検索の動作フローを示した図である.

はじめに，アプリケーションはデータ検索の前に認証を行うためデータ連携モジュールを提供する API である/api/token に認証リクエストを送り，Access Token を受け取る. 続いて, アプリケーションが取得可能なデータを検索するためにデータ連携モジュールの API に対してリクエストを送る．リクエストはデータ連携モジュールからデータ管理モジュールに送られる．データ管理モジュールは認証・認可モジュールのデータアクセス認可ポリシーを確認し認可されているデータリストを取得する．取得したデータリストを元にデータ検索処理を行い，結果をアプリケーションに対して返答する.

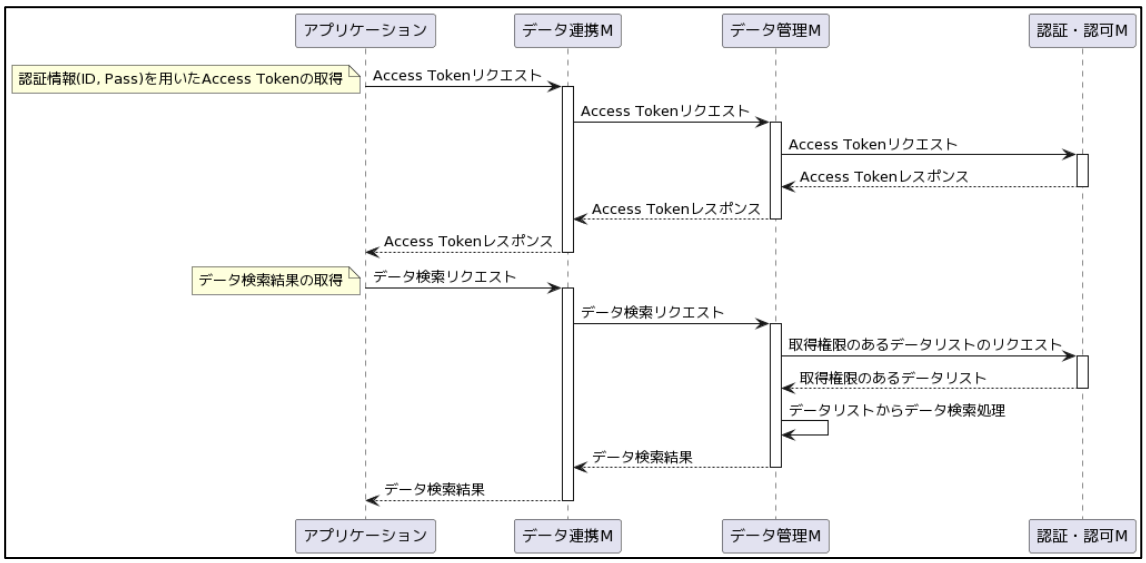

図 17　データ検索の動作フロー

4.4.6 データの取得

図 18 は、データ取得の動作フローを示した図である.

はじめに，アプリケーションはデータ連携モジュールに対して認証要求を行う．これにより認証・認可モジュールによって発行された，アプリケーションを識別するための Access Token を取得する.

続いて、アプリケーションはデータ連携モジュールに対して認可要求を行う．具体的にはアプリケーションは取得したいデータ ID を用いてデータ要求に必要な Ticket と Requesting Party Token(RPT)の要求を行う．この際，アプリケーションがデータを取得する権限がある場合は RPT の発行が許可されるが，権限がない場合 RPT の発行が拒否される.

その後，アプリケーションはデータの取得要求を行うため，Access Token と RPT を用いてデータのリクエストをする．データ管理モジュールは受け取った Access Token と RPT を認証・認可モジュールに問い合わせ有効性の確認を行う．有効性が確認された際，データ管理モジュールに保存されているデータを返答することで，アプリケーションはデータ取得が可能になる.

このデータの取得では，認可の際にデータアクセス認可ポリシーを参照しているため，非常時の状況と個人の意向を踏まえたデータの共有が可能になる.

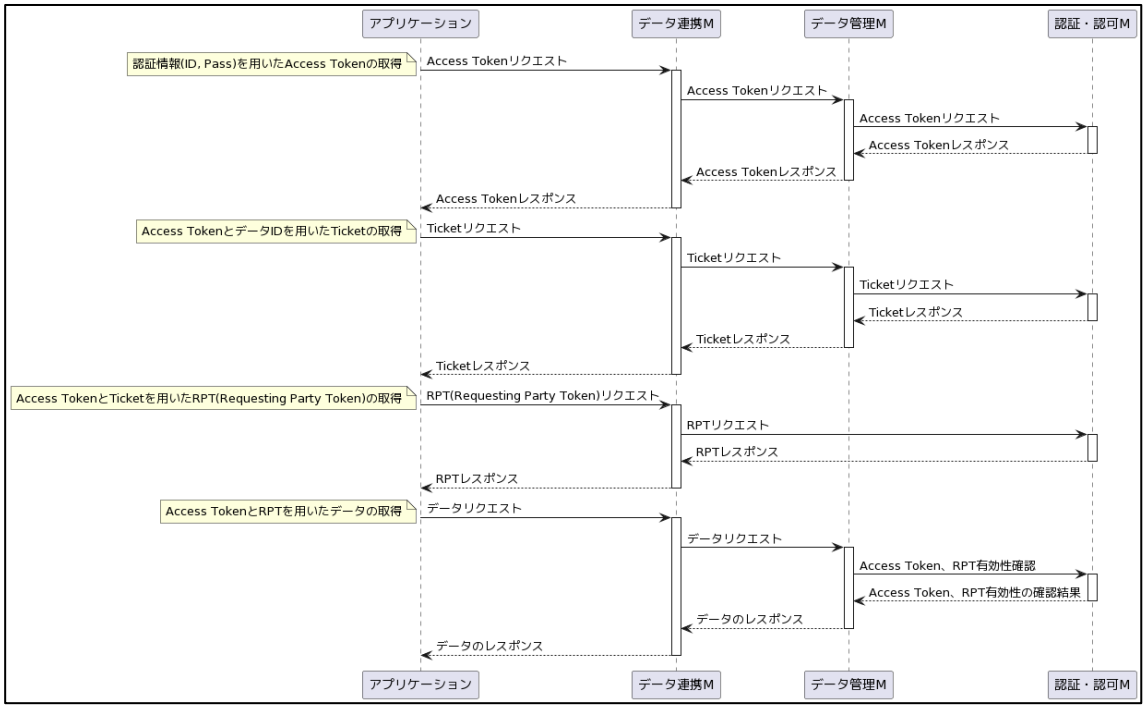

図 18　データ取得の動作フロー

第5章 評価

本章では，シナリオを想定した動作評価について述べる．

5.1 想定シナリオによる実験

想定される MKOS を用いて，非常時の状況と個人の意向を踏まえたデータの共有が可能かどうか確認するため，想定されるシナリオを用いてシミュレーションを行う．

5.1.1 想定シナリオ

第 3 章でのユースケースでカードキー認証データを用いるアプリケーションを例に挙げる．カードキー認証データは，図 19 に示すように公民館のドアに設置される IC カードリーダーによって取得されるカードキー認証情報である．また，ユースケース「1.4 電子錠を用いた施設の鍵管理」や「4.7 避難者位置情報の救助隊情報共有」でユーザー認証や位置情報を示すデータとして用いられることを想定している．

ユースケース「1.4 電子錠を用いた施設の鍵管理」は，カードキーを権利者に付与することで，施設の鍵を管理するユースケースであり，平常時・非常時ともに動作すべきである．また，ユースケース「4.7 避難者位置情報の救助隊情報共有」は，避難者の位置状況把握を行い，救助隊への現場状況連絡を行うユースケースであり，非常時のみに動作すべきである．

これらは，平常時に鍵管理のために取得したユーザーの位置情報を示すデータを非常時の際に人命救助のために利用すること想定したものである．

従来の認可システムでは，災害状況やユーザーの意向に沿ったデータ認可することは想定されていなかった．しかし，MKOS は災害状況を警戒レベルを用いて判断し，各種ポリシーを用いて公民館管理者，データ提供者の意向に沿ったデータ認可機能を提供することによって，平常時だけでなく非常時においても利用可能なシステムを提供することが可能になる．

警戒レベルや各種ポリシーを用いて実際にデータアクセス認可が正しく行われるか確認するために実験を行う．同意情報ポリシーの異なる USER A，USER B を準備する．ユースケース「4.7 避難者位置情報の救助隊情報共有」に対し，警戒レベル 3 の時 USER A データを共有するが，USER B は共有しないという同意情報ポリシーを設定する．警戒レベル 3 の際に災害状況を踏まえ各ユーザーの意向に沿ってデータ認可が適切に実施されるかどうか実験を行った．

5.1.2 実験詳細

ユースケースは対応したアプリケーション・サービスが存在する．MKOS と連携することによりユースケースを満たす動作をアプリケーション・サービスが提供する．

このユースケース 2 つにおいて MKOS は，災害状況を判断し，ユーザーの意向に沿ったデータ認可を提供する必要がある．そのために，MKOS はユースケースに応じたアプリケーションに対して認証機能，データアクセス認可機能，データ共有機能を提供する．

今回のシナリオで想定する認可リストを表 8 ―10 に示す。アプリケーションは，「電子錠での鍵管理」と「救助隊情報共有」があり，ユーザーは「USER A」と「USER B」の 2 人である．ユーザーは表 9 の通り同意情報ポリシーを設定しており，「救助隊情報共有」アプリケーションに対してのデータアクセスを認可する警戒レベルに違いがある．USER A は，警戒レベル 3 以上から共有するポリシーを設定しており，USER B は警戒レベル 4 以上から共有するポリシーを設定している．そのため，警戒レベル 3 の時には USER A のデータのみ共有されることになる．これは，個人の意向を踏まえたデータ共有が正しく行われるか確認するために異なる同意情報ポリシーを設定した．

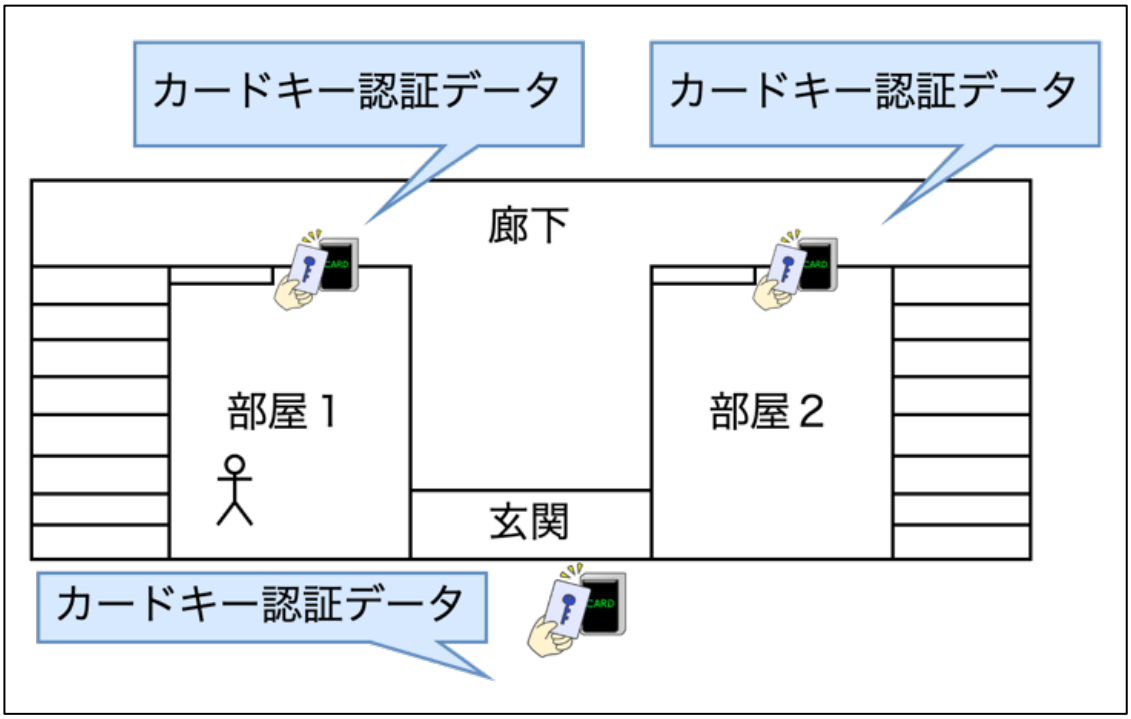

図 19　公民館内の IC カードリーダー設置イメージ図

表 8　想定シナリオでの災害情報ポリシー

データ名		カードキー認証データ	
アプリケーション名		電子錠での鍵管理	救助隊情報共有
警戒レベル	レベル 0	TRUE	FALSE
	レベル 1	TRUE	FALSE
	レベル 2	TRUE	FALSE
	レベル 3	TRUE	TRUE
	レベル 4	TRUE	TRUE
	レベル 5	TRUE	TRUE

表 9　想定シナリオでの同意情報ポリシー

ユーザー名		USER A		USER B	
データ名		カードキー認証データ		カードキー認証データ	
アプリケーション名		電子錠での鍵管理	救助隊情報共有	電子錠での鍵管理	救助隊情報共有
警戒レベル	レベル 0	TRUE	FALSE	TRUE	FALSE
	レベル 1	TRUE	FALSE	TRUE	FALSE
	レベル 2	TRUE	FALSE	TRUE	FALSE
	レベル 3	TRUE	TRUE	TRUE	FALSE
	レベル 4	TRUE	TRUE	TRUE	TRUE
	レベル 5	TRUE	TRUE	TRUE	TRUE

表 10　想定シナリオでのデータアクセス認可ポリシー

データ名		カードキー認証データ			
ユーザー名		USER A		USER B	
アプリケーション名		電子錠での鍵管理	救助隊情報共有	電子錠での鍵管理	救助隊情報共有
警戒レベル	レベル 0	TRUE	FALSE	TRUE	FALSE
	レベル 1	TRUE	FALSE	TRUE	FALSE
	レベル 2	TRUE	FALSE	TRUE	FALSE
	レベル 3	TRUE	TRUE	TRUE	FALSE
	レベル 4	TRUE	TRUE	TRUE	TRUE
	レベル 5	TRUE	TRUE	TRUE	TRUE

5.1.3 実験環境

MKOS とアプリケーションの動作環境は表 11，カードキー認証データの生成に使用したセンサーデバイスは表 12，図 20 の通りとなっている．MKOS は Python，DB は MongoDB で実装した．また，センサーデバイスは Python を用いて実装している．

表 11　実験環境

OS	Debian 6.1.27
CPU	Intel Xeon E-2278G
メモリ	128GB

表 12　センサーデバイス

シングルボードコンピュータ	Raspberry Pi 4
IC カードリーダー	RC-S380
IC カード	FeliCa Lite-S

図 20　センサーデバイス

5.1.4 結果

警戒レベルでデータアクセス認可の可否を確認した．警戒レベル 3 の時の救助隊情報共有アプリケーションが，USER A と USER B のデータを取得しようとした際のレスポンスを図 21, 22 に示す．また，確認した結果を表 13 に示す．

警戒レベル 3 の時の救助隊情報共有アプリケーションが USER A のデータは RPT が発行されデータを取得でき，USER B のデータは RPT が発行されず取得できていないことがわかる．このことから，MKOS はアプリケーション・サービスに対して認証機能，データアクセス認可機能，データ共有機能を正しく提供していることがわかる．また，非常時の状況とユーザーの意向に応じたデータアクセス認可が適切に行われたことがわかる．

図 21　USER A データ取得時のレスポンス(警戒レベル 3，救助隊情報共有)

図 22　USER B データ取得時のレスポンス(警戒レベル 3，救助隊情報共有)

表 13　実験結果

データ名		カードキー認証データ			
ユーザー名		USER A		USER B	
アプリケーション名		電子錠での鍵管理	救助隊情報共有	電子錠での鍵管理	救助隊情報共有
警戒レベル	レベル 0	取得可能	取得不可能	取得可能	取得不可能
	レベル 1	取得可能	取得不可能	取得可能	取得不可能
	レベル 2	取得可能	取得不可能	取得可能	取得不可能
	レベル 3	取得可能	取得可能	取得可能	取得不可能
	レベル 4	取得可能	取得可能	取得可能	取得可能
	レベル 5	取得可能	取得可能	取得可能	取得可能

第6章 考察

本章では，今回検討・実装した公民館 OS についての考察を述べる．

6.1 複数の公民館 OS の連携について

本論文では 1 つの公民館を利用することを想定した公民館 OS について提案を行った．複数の公民館 OS が連携をすることで，普段利用している公民館の公民館 OS に保存されたセンサーデータ，館内・台帳データや，ポリシー情報を，その他の公民館の公民館 OS でも利活用することが可能になると考えられる．

平常時の際では，普段利用している公民館以外の公民館へ行きサービスをうけること場合が考えられる．また，非常時の際では，旅行中に被災し旅行先の避難所として活用される公民館を利用することが想定される．

複数の公民館 OS が連携することにより，外部の公民館内にて「1.1 温熱管理」のユースケースで公民館利用者にとって快適な温度調整をしたい場合に，普段利用している公民館に保存されている「3.3 体温監視」のユースケースで取得している体温情報を取得することが可能となり，公民館 OS 同士の横展開のデータ利活用が可能になる．

また，ポリシー情報も取得することができる様になることで外部の公民館のサービスを自動で利用することが可能になり，公民館利用者にとって利便性の向上につながると考えられる．

6.2 個別の災害を考慮したポリシーについて

本論文では、災害状況を判断する情報として警戒レベルを用いた。これにより、避難の不必要という観点で災害状況を総合的に各自治体の市町村長が判断する指標である為、災害状況を 6 段階で指定するポリシー構造となった。

地震や水害といった個別の災害毎にポリシーで指定する構造を検討した場合、複数ある災害毎に発令される注意報、警報と言った情報を元にポリシーを作成する構造となると考えられる。

具体例として、ある自治体では氾濫の危険性がある川が存在することにより、水害に関してのポリシーを柔軟に作成するというように、各自治体で警戒されている個別の災害の特徴を踏まえたポリシーを設定する事が可能になる。

これにより、警戒レベルを用いた方法と比べ，より詳細な災害状況を踏まえた柔軟な平常時・非常時の認可ができるようになる．また，各自治体の災害の特徴を踏まえたデータの利活用が可能になると考えられる。

しかし、個別に対応する災害数とレベル数に応じて設定しなければならないポリシーが増加し，データ管理者やデータ利用者の負担が増えることが想定される。

6.3 ポリシー設定数について

今回用いた同意情報ポリシーはデータとアプリケーション毎に、どの警戒レベル時に共有するかを示したものでありデータの使用方法をより明確に指定することができる。しかし、データとアプリケーションの組み合わせに対し警戒レベル毎の 6 項目のポリシーを設定しなければならない為、設定数が大きくなってしまう課題がある．

そのため、データ本来の特徴に基づいたユーザーの抽象的なポリシーから、今回用いた同意情報ポリシーを作成する手法を用いることで解決できる可能性がある。

抽象的なポリシーは，ユーザーがデータの特徴や警戒レベル毎にデータの共有の可否を定めたポリシーである。データの特徴は，位置情報や生体情報といったデータに含まれるユーザーのプライバシー情報に関連する特徴を抽象化したものを指す．作成方法としては、ユーザーがデータの特徴と警戒レベル毎にポリシーを作成する方法が考えられる．また，同意情報ポリシーから，ユーザー毎のデータに対するデータ認可の傾向や特徴量を捉える事で，ユーザーそれぞれに対応した抽象的なポリシーを生成できる可能性が考えられる．

抽象的なポリシーを用いることで，ポリシー設定数を減少させることが可能になり，ユーザーのポリシー設定の負担を減らすことが期待される．

6.4 MKOS の公的な PPM としての活用について

公民館は日本に多数設置され、各自治体の地域住民が利用できるよう住宅のある場所をカバーしている事が多い。そのため、地域住民のポリシーを各自治体の公民館 OS に集約し，公民館以外の第三者のサービスで活用する可能であると考えられる．

本論文では，公民館内のユースケースに注力したポリシーを作成したが，ユーザーごとにどのような情報を共有できるかを示すより柔軟なポリシーを集約

することで，公民館内のユースケースだけでなく、第三者のサービスにおいても地域住民のデータ利用の可否を判断できるようになる．

また、多くの住民が利用する公民館の特性上、各自治体に複数の公民館が存在し管理されていることから、地域住民の様々なデータを収集し共有することが可能になり，データ利用の可能性が広がると考えられる．

第7章 終わりに

本章では，本論文でのまとめについて述べる．

7.1 まとめ

本研究では，公民館のデジタル化において生成されるセンサーデータや館内・台帳データにおける，平常時だけでなく非常時にも利活用するために状況判別する課題と，個人情報・プライバシー情報に対してユーザーの意向に沿ったデータ利活用をしなければならない課題に対し，MKOS を想定した，警戒レベルとプライバシーポリシーを活用する非常時に対応可能なプライバシーポリシーマネジメント・認可基盤を提案した．

平常時だけでなく非常時にも利活用するために状況判別する課題に対しては，非常時に各自治体から発令される防災情報である警戒レベルを用いることを提案した．これにより，地域ごとに避難の必要性の観点から非常時の状況を総合的に判断することが可能になる．また，地震や津波といった災害毎に発令される情報を用いないことによりポリシーの設定数を少なくすることが可能になる．

個人情報・プライバシー情報に対してユーザーの意向に沿ったデータ利活用をしなければならない課題に対しては，MKOS 内の平常時・非常時ポリシー管理モジュール内で，ユーザー毎に同意情報ポリシーを設定することを提案した．これにより，データを受け渡すサービスを指定することや警戒レベルを用いた平常時・非常時の状況に応じたデータ共有の指定をすることが可能になる．

そのため，公民館内のセンサーデータや館内・台帳データに対し，平常時・非常時の状況に応じてユーザーの意向に沿ったデータ利活用をすることができる．また，アプリケーション・サービスはこれまで取得できなかったデータを災害状況に応じて柔軟にデータを取得することが可能になり，災害時のデータ利活用の幅が広がることが期待される．

謝辞

本論文を執筆するにあたり，多くの方々にご指導ご鞭撻を賜りました．
主指導教員の丹 康雄教授には，ゼミを通した研究議論の際にご丁寧な指導を受け賜りました．
審査員をお引き受けいただいた長谷川 忍教授，リム 勇仁准教授，BEURAN Razvan Florin 准教授には中間発表などを通じて新たな視点から示唆に富んだアドバイスをいただきました．
本研究室の SIOUTIS, Marios 特任准教授，PHAM Van Cu 特任助教，博士後期課程 XIN Tao 氏には，研究に関する活発な議論，技術的な指導を賜りました．心から感謝致します．
最後に，学生生活を支えて頂いた家族に感謝いたします．ありがとうございます．

参考文献

[1] 個人情報保護委員会, "個人情報の保護に関する法律についてのガイドライン（通則編）", url:https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/, (参照:09.01.2024)

[2] Al-Hasnawi A, Mohammed I, Al-Gburi A, "Performance evaluation of the policy enforcement Fog modnle for protecting privacy of loT data", 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 2018, 0951-0957.

[3] S. Kiyomoto, T. Nakamura, H. Takasaki, R. Watanabe, and Y. Miyake, “PPM: Privacy policy manager for personalized services”, Security Engineering and Intelligence Informatics, 2013, 377–392.

[4] Davies N, Taft N, Satyanarayanan M, et al, "Privacy mediators: Helping iot cross the chasm", Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, 2016, 39-44.

[5] Klingensmith N, Kim Y, BaneIjee S, "A Hypervisor-Based Privacy Agent for Mobile and loT Systems", Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications, 2019, 21-26.

[6] FIWARE, "Orion Context Broker", url:https://fiware-orion.letsfiware.jp/, (参照:09.01.2024)

[7] 情報処理推進機構, "スマートビルシステムアーキテクチャガイドライン", url:https://www.ipa.go.jp/digital/architecture/project/smartbuilding/guideline.html, (参照:09.01.2024)

[8] 山崎 元明, 廣瀬 啓一, 白石 理人, "建物デジタルプラットフォーム「DX-Core(建物 OS)」の開発", 清水建設研究報告, 2021, 第 99 号.

[9] 国土交通省　気象庁, ”防災気象情報と警戒レベルとの対応について”, url:https://www.jma.go.jp/jma/kishou/know/bosai/alertlevel.html, (参照:09.01.2024)

[10] OpenID Foundation, ”OpenID Connect Core 1.0", url:https://openid.net/specs/openid-connect-core-1_0-final.html, (参照:09.01.2024)

[11] KantaraInitiative, "User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization", url:https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html, (参照:09.01.2024)

[12] 草野 清重, 陳 翔, リム 勇仁, 丹 康雄, "非常時に対応可能なデータアクセス認可システムに関する提案", 電気・情報関係学会北陸支部連合大会, 2023.

[13] 陳 翔, 草野 清重, リム 勇仁, 丹 康雄, "公民館向け建物 OS における非常時の動作変更方法に関する研究", 電気・情報関係学会北陸支部連合大会, 2023.

[14] 陳 翔, "公民館向け建物 OS における設備制御と資源最適化に関する研究", 北陸先端科学技術大学院大学学位論文, 2024.

付録

A. ユースケースの動作フロー

3 章で説明したユースケースの動作フローをまとめた表を表 14—18 に示す.

表 14　ユースケースの動作フロー（施設管理）

カテゴリ	ユースケース名	動作フロー
1. 施設管理	1.1 温熱管理	1. 温度データを取得する 2. 設定した温度と比較し，暖房，冷房，除湿を判断する 3. エアコン等のアクチュエータに動作指示する
	1.2 空気質管理	1.空気質データを取得する 2.基準値と比較し、空気清浄の必要性を判断する 3.換気・空気清浄機に動作指示する
	1.3 照明管理	1.照明データを取得する 2.設定した照明基準と比較し、照明のオン・オフや強度を判断する 3.照明に動作指示する
	1.4 電子錠を用いた施設の鍵管理	1.権利者の情報を登録する 2.カードキーを発行する 3.カードキーを認証する
	1.5 電子錠・スマホを用いた鍵権限の付与・管理	1.利用者の情報を登録する 2.スマホアプリをインストールする 3.鍵権限を付与する 4.鍵権限を解除する
	1.6 キーボックスの鍵管理	1.キーボックスに鍵を登録する 2.鍵を貸し出す 3.鍵を返却する
	1.7 在室人数の管理	1.在室人数を計測する 2.在室人数の上限を設定・変更する 3.在室人数の上限を超えた場合、入場を制限する
	1.8 宅配ボックスとしての利用	1. 地域住民の荷物を公民館で受け取る 2. 地域住民へ荷物を受け渡す

表 15　ユースケースの動作フロー（災害・防犯監視）

カテゴリ	ユースケース名	動作フロー
2. 災害・防犯監視	2.1 火災検知	1. 火災データを取得する 2. 火災の有無を判断する 3. 建物内の人に通知する. 4. 関連施設や，消防へ通知する.
	2.2 水害監視	1. 水位データを取得する 2. 基準以上の水位であり，浸水の危険性があるか判断する 3. 建物内の人に通知する. 4. 関連施設へ通知する.
	2.3 雪害監視	1. 施設の積雪量データを取得する 2. 基準以上の積雪量であるか判断する 3. 建物内の人に通知する 4. 関連施設へ通知する 5. 除雪依頼をする
	2.4 風害監視	1. 風速データを取得する 2. 基準以上の積雪量であるか判断する 3. 建物内の人に通知する 4. 関連施設へ通知する
	2.5 豪雨監視	1. 雨量データを取得する 2. 基準以上の雨量であるか判断する 3. 建物内の人に通知する 4. 関連施設へ通知する
	2.6 不審者への防犯監視	1. 静止画，動画を取得する 2. 人物が，施設内へ侵入したか判断する 3. 建物内の人に通知する 4. 関連施設へ通知する
	2.7 害獣対策としての監視	1. 静止画，動画を取得する 2. 害獣がいるか判断する 3. 建物内の人に通知する. 4. 関連施設へ通知する

表 16　ユースケースの動作フロー（健康・医療）

カテゴリ	ユースケース名	動作フロー
3. 健康・医療	3.1 健康診断	1. 住民の健康情報を測定する 2. 健康情報を保存する 3. データを管理する
	3.2 遠隔診療向け個室整備	1. 住民が個室の利用登録をする 2. 利用時にユーザー認証する 3. 電子錠を解錠し，個室を提供する
	3.3 体温監視	1. 体温データを取得する 2. 基準値と比較し，発熱の有無を判断する 3. ディスプレイ，スピーカーに動作指示し，公民館職員へ通知する
	3.4 メンタルヘルスケア	1. ユーザーのメンタルヘルスケアに関するアンケートデータを取得する 2. アンケートデータからスコアを算出 3. 基準値以上であれば，専門医へ情報を通知する．ケアやサポートへ繋げる

表 17　ユースケースの動作フロー（避難所利用）1/2

カテゴリ	ユースケース名	動作フロー
4. 避難所利用	4.1 避難者名簿作成	1. 避難者の避難所入室時，マイナンバーカード等でユーザー認証を行う(ユーザー識別) 2. アプリケーションが避難者を登録する. 3. 避難者をアプリケーション経由で外部から閲覧できるようにする.
	4.2 仮設居住場所の割り当て	1. 避難者の避難所入居時，人数登録をする 2. アプリケーションが避難者の人数と仮設居住場所データの収容可能人数を照らし合わせ，割当先の仮設居住場所を決定する 3. 避難者に割当先の仮設居住場所を提示する
	4.3 備蓄品在庫管理	1. 避難所内の備蓄品データの登録を行う 2. 備蓄品データを権限を持つ第三者が閲覧できるようにする 3. 使用時に備蓄品データの更新を行う
	4.4 倉庫から各避難所への備品管理	1. 倉庫内の備蓄品データの登録を行う 2. 各避難所内の備蓄品データと避難者データを参照して，倉庫内の備蓄品の受け渡し管理を行う.
	4.5 分散避難時の物資配給拠点	1. 物資配給データを登録する. 2. 物資配給を目的として避難所へ来た住民の認証を行う. 3. 住民情報を元に物資の分配を行う.
	4.6 非常時の電力管理	1. 電力供給対象となる重要システムを登録する. 2. 電力停止時に電力共有する対象システムへ電力供給を行う.

表 18　ユースケースの動作フロー（避難所利用）2/2

カテゴリ	ユースケース名	動作フロー
4. 避難所利用	4.7 避難者位置情報の救助隊情報共有	1. ユーザー位置データを取得する. 2. ユーザー位置データを救助隊への通知する.
	4.8 避難経路支援	1. 避難経路情報と部屋毎の災害情報を取得する. 2. 避難経路情報を更新する. 3. 最新の避難経路情報をユーザーへ通知する.
	4.9 避難者位置情報を用いた安否確認	1. ユーザー位置データを取得する. 2. ユーザー位置データを救助隊への通知する.
	4.10 避難所での健康状態監視	1. 体温データを取得する 2. 基準値と比較し，発熱の有無を判断する 3. ディスプレイ，スピーカーに動作指示し，公民館職員や適切な医療機関へ通知する

B. センサーリスト

公民館にてデータを収集するために用いられるセンサーのリストを表 19 に示す.

表 19　センサーリスト

カテゴリ	データ
1. 施設管理	温度センサー
	湿度センサー
	CO2 センサー
	CO センサー
	PM2.5 センサー
	人体検知センサー
	照度センサー
	カメラ
	RFID リーダー
2. 災害・防犯監視	火災検知器
	雨量計
	水位計
	土壌湿度センサー
	雪深センサー
	気象センサー
	風速計
	カメラ
3. 健康・医療	体重計
	血圧計
	骨密度計
	体温計
	カメラ
	RFID リーダー
4. 避難所利用	バーコードリーダー
	重量計
	カメラ
	RFID リーダー

C. データリスト

ユースケースを満たすために必要な情報は公民館施設内外に設置されるセンサーによってデータ収集することを想定している．収集されたデータは建物OS内で管理し，ユースケースの動作を満たすアプリケーションに共有することでデータの利活用がされる．ユースケースの動作を満たすために公民館内から取得する必要があると考えられるデータリストを表20と表21に示す．

表 20　データリスト　1/2

カテゴリ	データ
室内環境情報	温度
	湿度
	CO2 濃度
	PM2.5 濃度
	照度
	人体検知
	熱
	煙
	静止画
	動画
室外環境情報	温度
	湿度
	CO2 濃度
	PM2.5 濃度
	水位
	積雪量
	雨量
	静止画
	動画
施設設備情報	電子錠状態
	施設部屋情報

表 21　データリスト　2/2

カテゴリ	センサー
認証情報	住民 ID
	カードキー認証データ
個人情報	住民 ID
	氏名
	世帯情報
	位置情報
健康情報	身長
	体重
	血圧
	骨密度
	体温
	メンタルヘルスアンケートデータ
災害時情報	避難者データ
	仮設居住場所データ
	避難所内備蓄品データ
	倉庫内備蓄品データ
	物資配給データ

D. ユースケース説明図

公民館内で必要とされるユースケースについて図を用いて説明した資料を図23—40に示す.

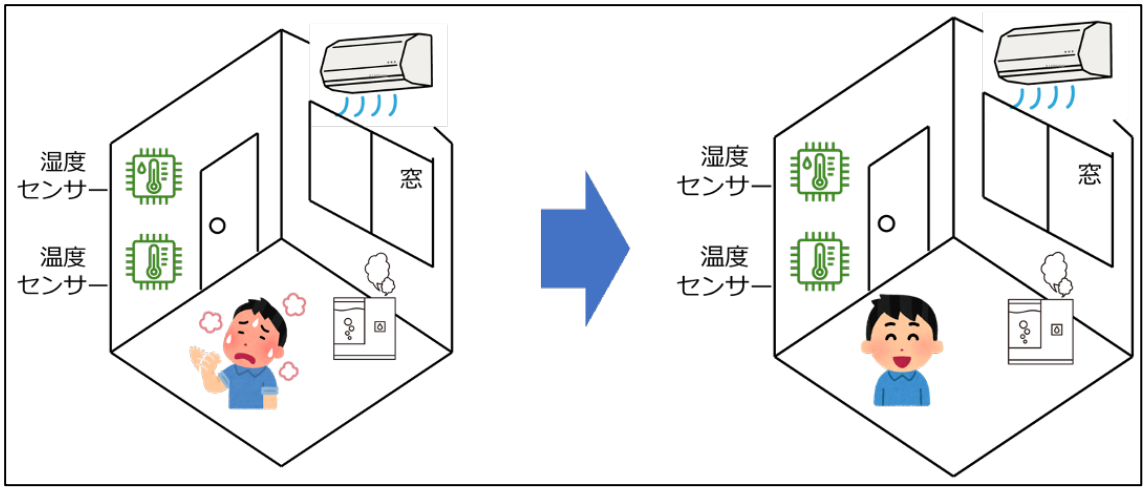

図 23　ユースケース 1.1 温熱管理

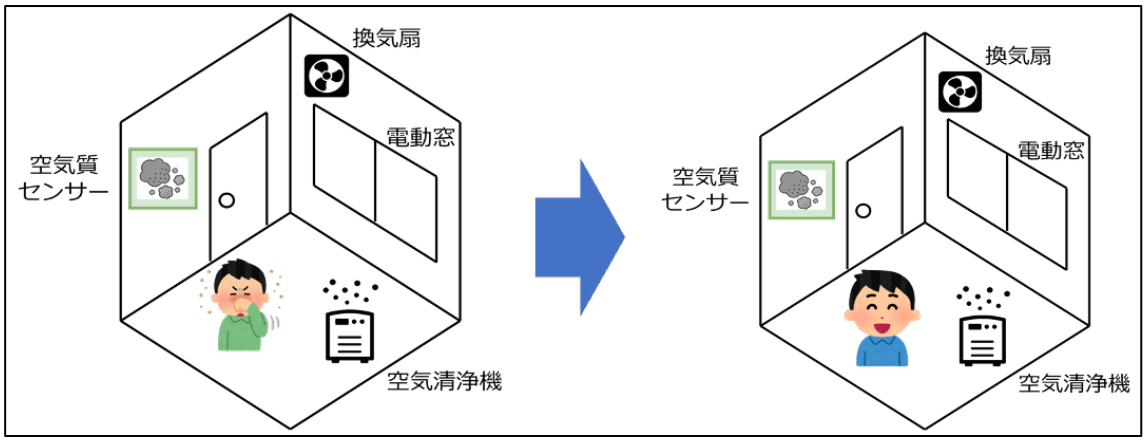

図 24　ユースケース 1.2 空気質管理

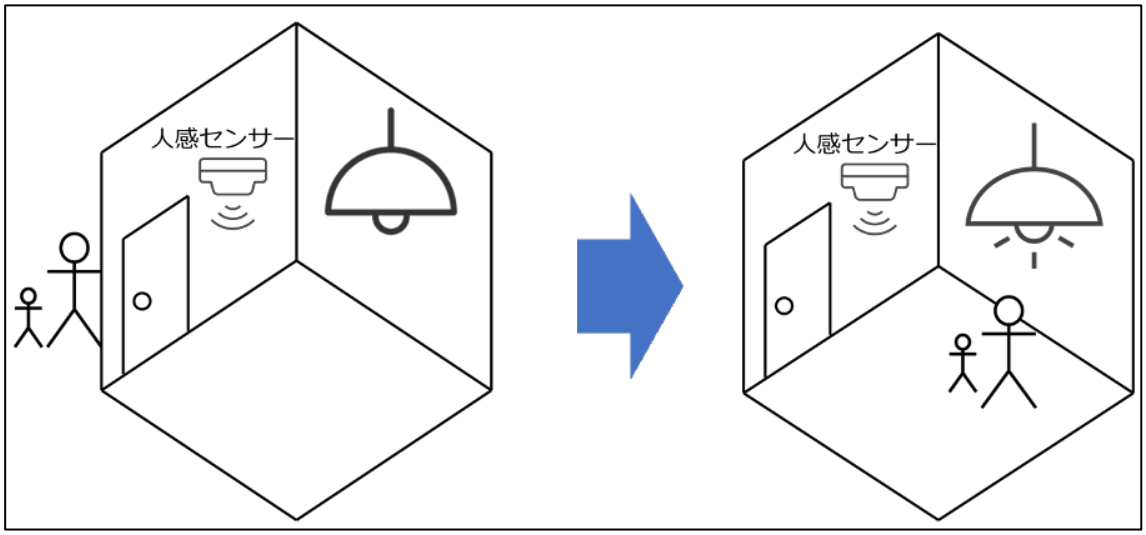

図 25　ユースケース 1.3 照明管理

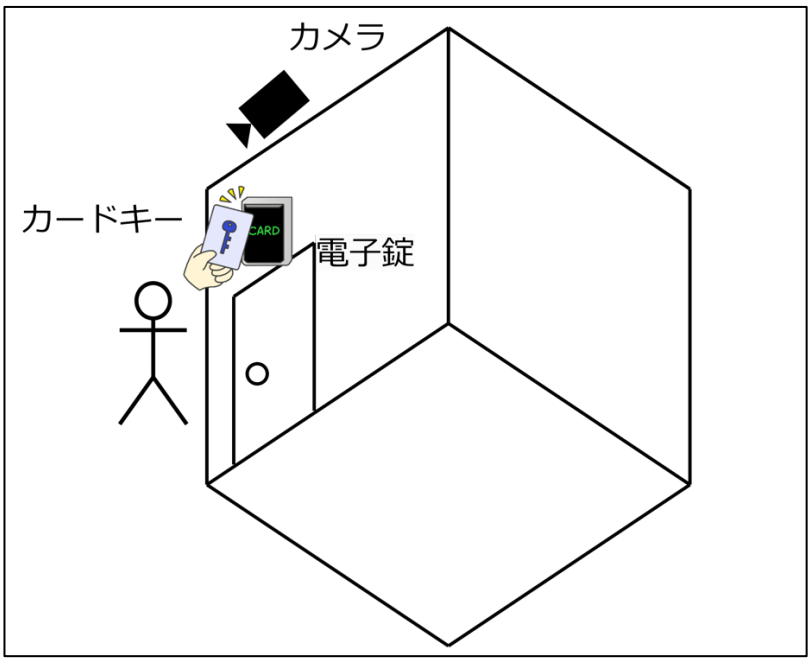

図 26　ユースケース 1.4 電子錠を用いた施設の鍵管理

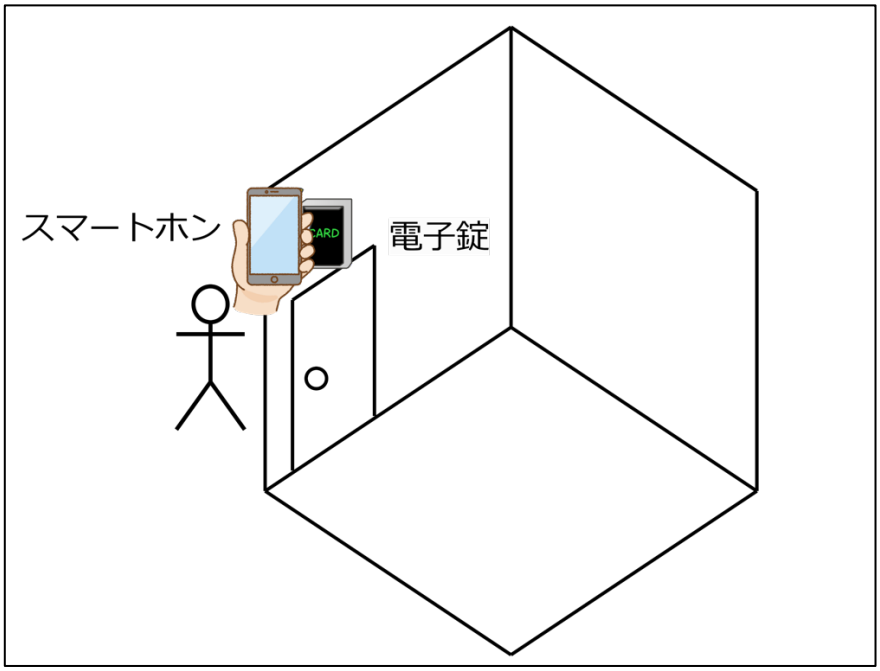

図 27　ユースケース 1.5 電子錠・スマホを用いた鍵権限の付与・管理

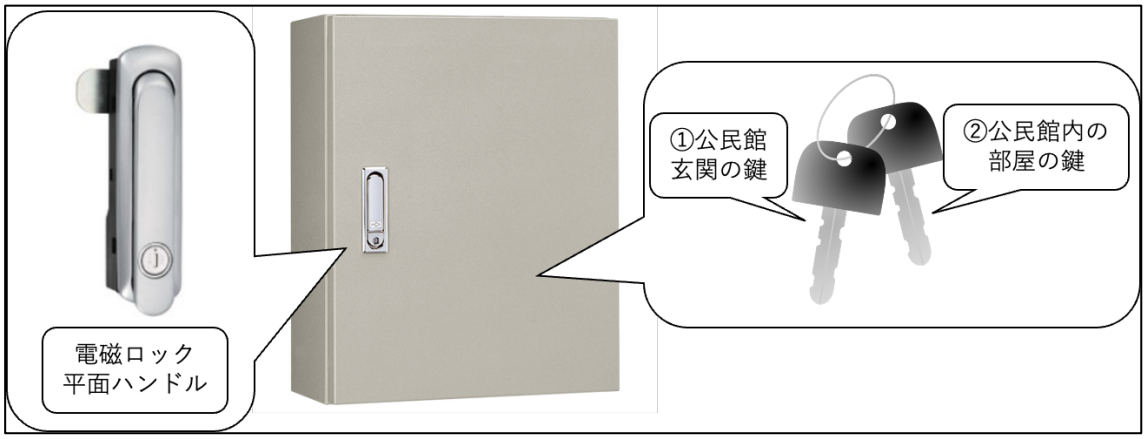

図 28　ユースケース 1.6 キーボックスの鍵管理

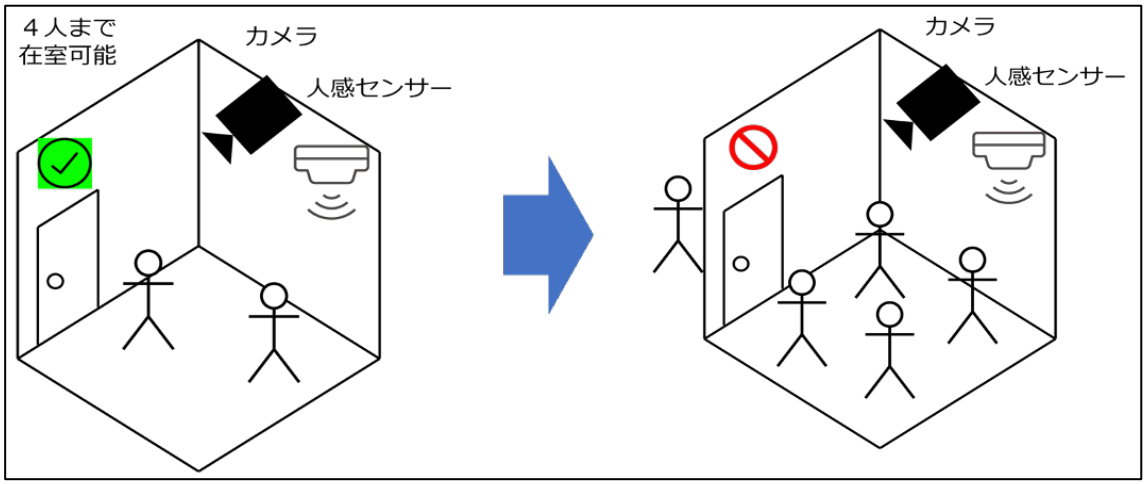

図 29　ユースケース 1.7 在室人数の管理

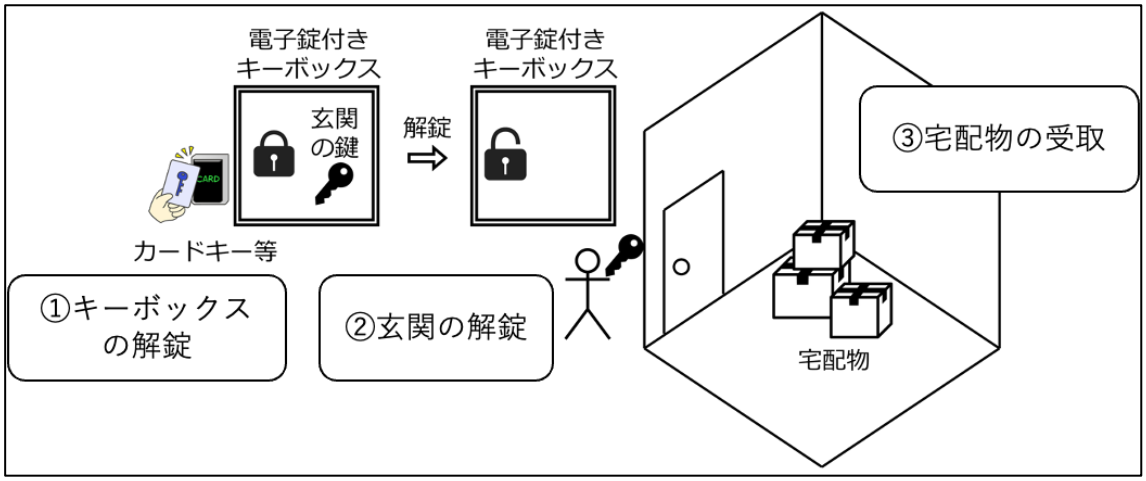

図 30　ユースケース 1.8 宅配ボックスとしての利用

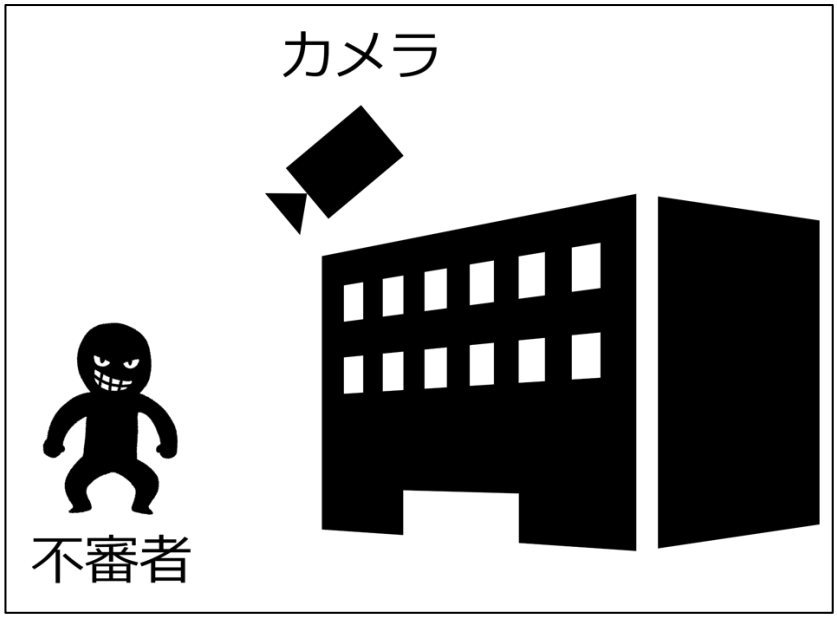

図 31　ユースケース 2.6 不審者への防犯監視

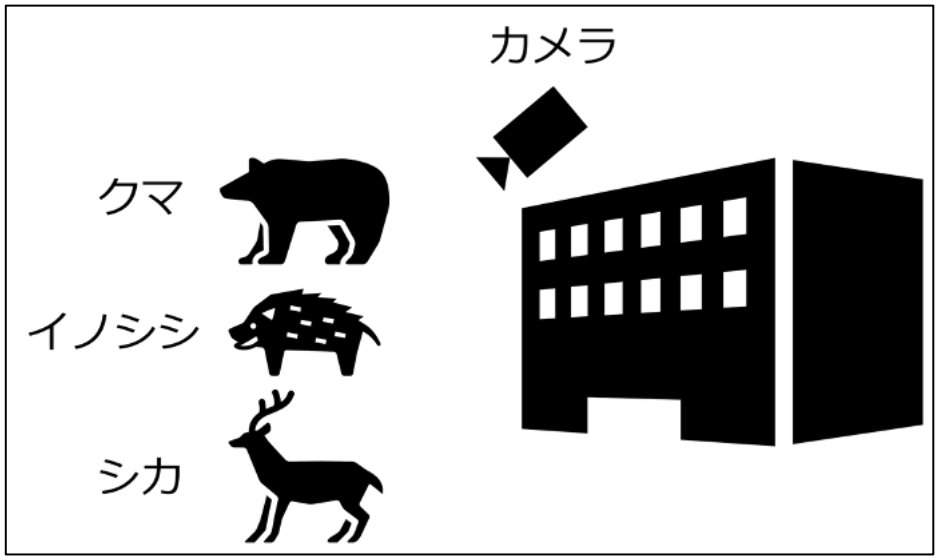

図 32　ユースケース 2.7 害獣対策としての監視

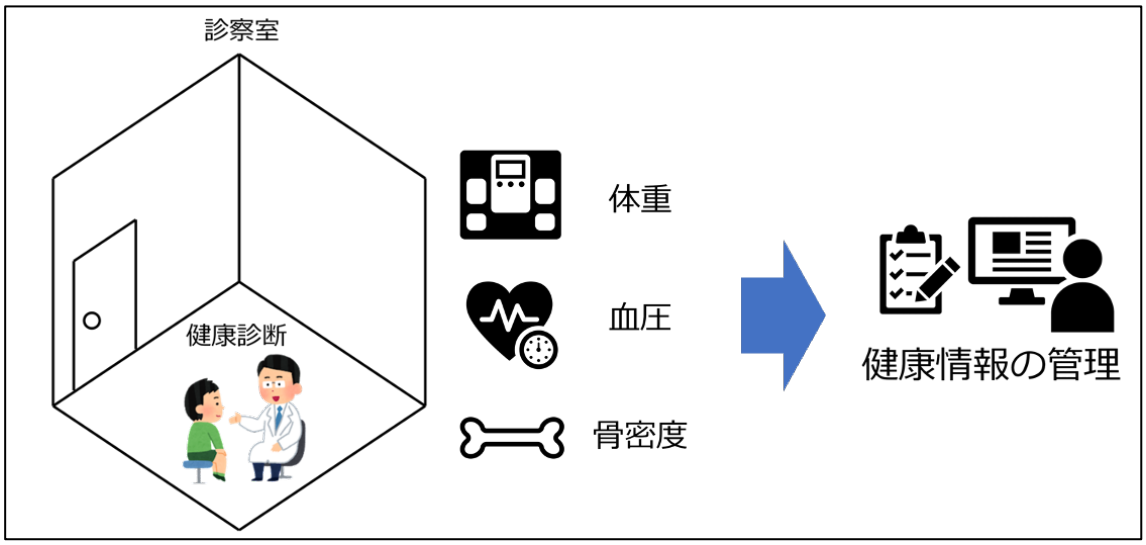

図 33　ユースケース 3.1 健康診断

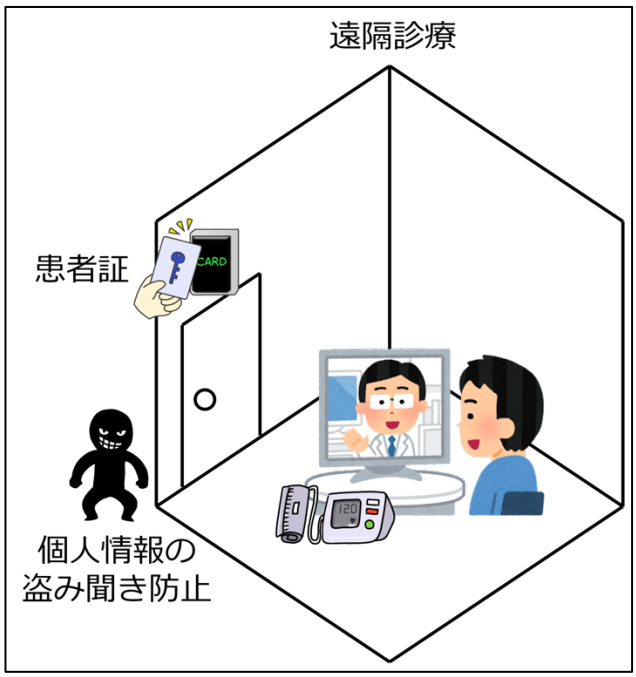

図 34　ユースケース 3.2 遠隔診療向け個室整備

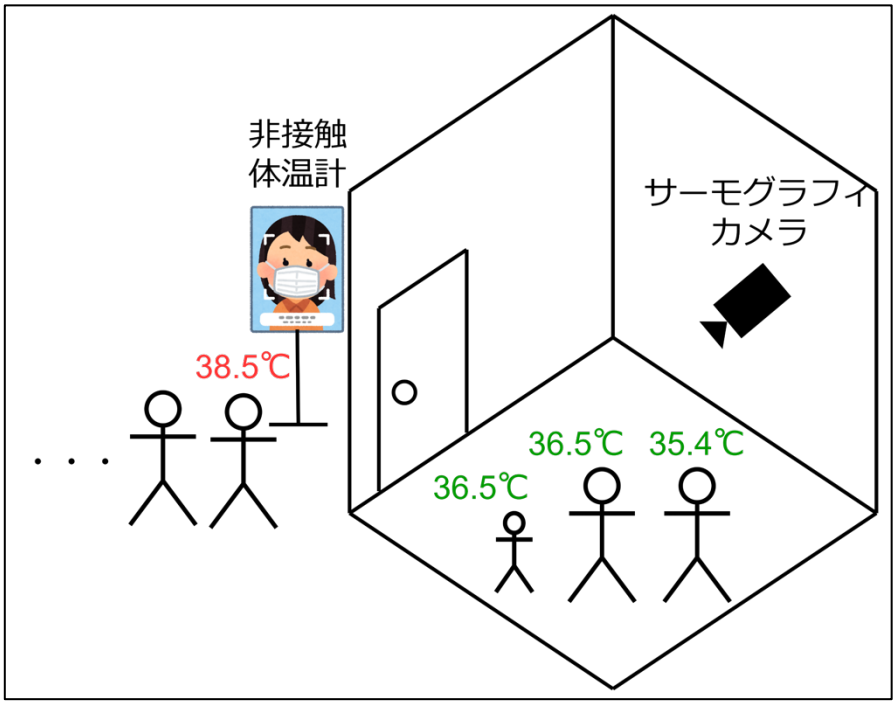

図 35　ユースケース 3.3 体温監視

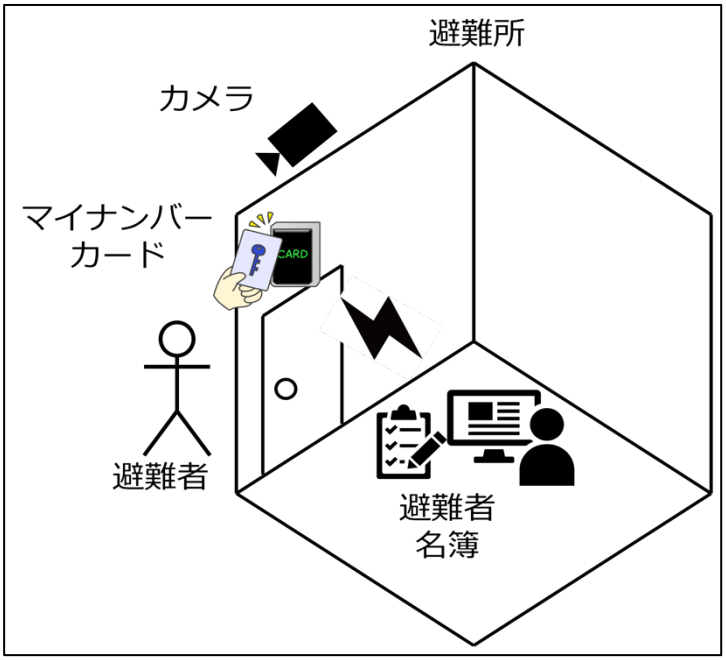

図 36　ユースケース 4.1 避難者名簿作成

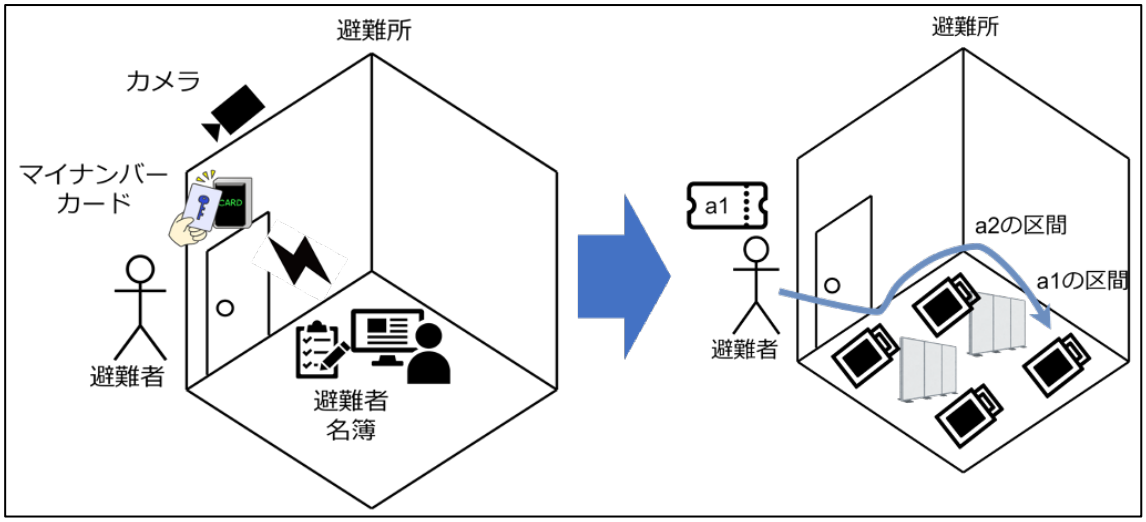

図 37　ユースケース 4.2 仮設居住場所の割り当て

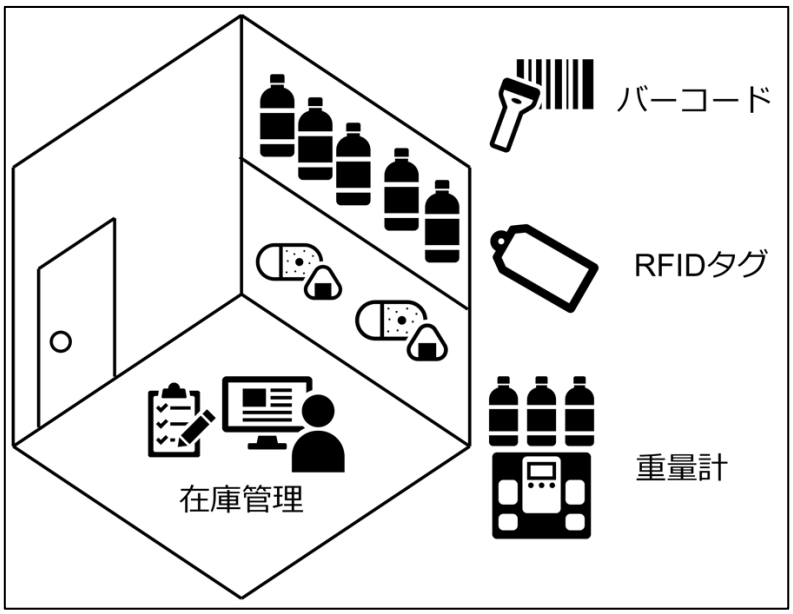

図 38　ユースケース 4.3 備蓄品在庫管理

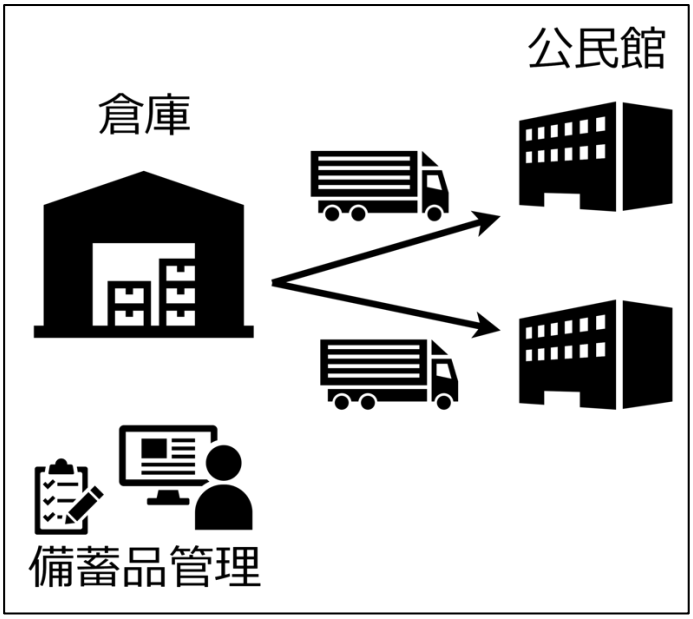

図 39　ユースケース 4.4 倉庫から各避難所への備蓄品管理

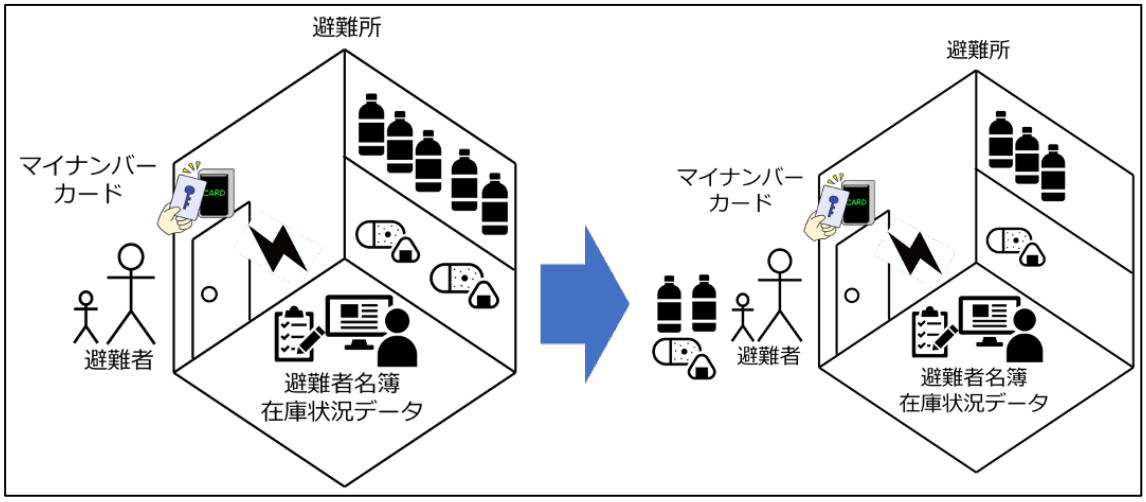

図 40　ユースケース 4.5 分散避難時の物資配給場所