水道情報活用システム

基本仕様書　別冊

水道標準プラットフォーム外部仕様書

WPSC005 EDITION 1.4

2023 年 10 月

水道情報活用システム標準仕様研究会

本書は、国立研究開発法人 新エネルギー・産業技術総合開発機構「IoT を活用した新産業モデル創出基盤整備事業」における「水道 IoT の社会実装推進に向けた検討」、及び「高度なデータ活用を可能とする社会インフラ運営システムの開発」事業により作成されたものに、経済産業省補助事業（補助事業者：株式会社 JECC）「水道施設情報整備促進事業」により改定され、水道情報活用システム標準仕様研究会により改定されました。

WPSC005-Ed.1.4 2023-10

水道情報活用システム標準仕様研究会及び本ドキュメント(本使用許諾条件に添付されて提供されるドキュメントをいい、以下同じ)の原著作権者である国立研究開発法人新エネルギー・産業技術総合開発機構、（以下「当研究会等」と総称します）は、以下の条件のもとで本ドキュメントを使用、複製および頒布することを無償で許諾します。本ドキュメントを使用、複製または頒布した場合には、以下の条件に同意したものとします。

1. 本ドキュメントの中に含まれる著作権表示および本使用許諾条件を、本ドキュメントの全部または一部を複製したものに表示してください。
2. 本ドキュメントを使用したサービスの提供を含め営利目的に本ドキュメントを使用することができますが、本ドキュメントのみを単独で販売することはできません。
3. 第４項に定める場合を除き、本ドキュメントを使用したサービスの提供に際して、事前の書面による当研究会等の許可なく、それらの宣伝、広告活動に当研究会等の名称を使用することはできません。
4. 本ドキュメントを使用して得られた結果を、形態を問わず、出版、発表において公表する場合には、本ドキュメントと当研究会等の名称を引用等において明示してください。
5. 本ドキュメントは現状有姿で提供されるものであり、当研究会等は、本ドキュメントに関して、商品性および特定目的への適合性、エラー・バグ等の不具合のないこと、第三者の特許権、実用新案権、意匠権、商標権、著作権その他の知的財産権を侵害するものではないことを含め、明示たると黙示たるとを問わず、一切の保証を行わないものとします。また、当研究会等は、本ドキュメントの誤りの修正その他いかなる保守についても義務を負うものではありません。
6. 当研究会等は、本ドキュメントの使用または使用不能、複製、頒布、その他本ドキュメントまたは本使用許諾条件の規定に関連して生じたいかなる損害(特別損害、間接損害、逸失利益を含みますが、これに限りません)または第三者からのいかなる請求についても、法律上の根拠を問わず一切責任を負いません。当研究会等がかかる損害または請求の可能性について知らされていた場合も同様とします。
7. 本ドキュメントは、一般事務用、家庭用、通常の産業用等の一般的用途を想定して作成されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途(以下「ハイセイフティ用途」という)を想定して作成されたものではなく、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本ドキュメントを使用しないものとします。また、ハイセイフティ用途に本ドキュメントを使用したことにより発生する、いかなる請求または損害賠償に対しても当研究会等は一切の責任を負わないものとします。

- 目次 -

1. はじめに

1.1 本ドキュメントの目的

本ドキュメントは、社会インフラ水道情報活用システム(以下、水道情報活用システム)標準仕様における基本仕様の別冊である。

基本仕様書では、水道情報活用システムを実現する基本仕様として、水道情報活用システムの全体構成と基本的に守るべきルール、標準インターフェイスを規定している。

本ドキュメントは、基本仕様書で規定した水道情報活用システムの１つである、水道標準プラットフォーム仕様の詳細を記載したドキュメントである。

本ドキュメントは、プラットフォーマーが、水道標準プラットフォームに要求される仕様を把握した上で、どのような要件を実現したプラットフォームを構築・運用すればよいかを理解することを目的とする。

1.2 水道情報活用システム標準仕様のドキュメント

1.2.1 ドキュメント体系

水道情報活用システム標準仕様のドキュメント体系を以下に示す(図 1-1)。

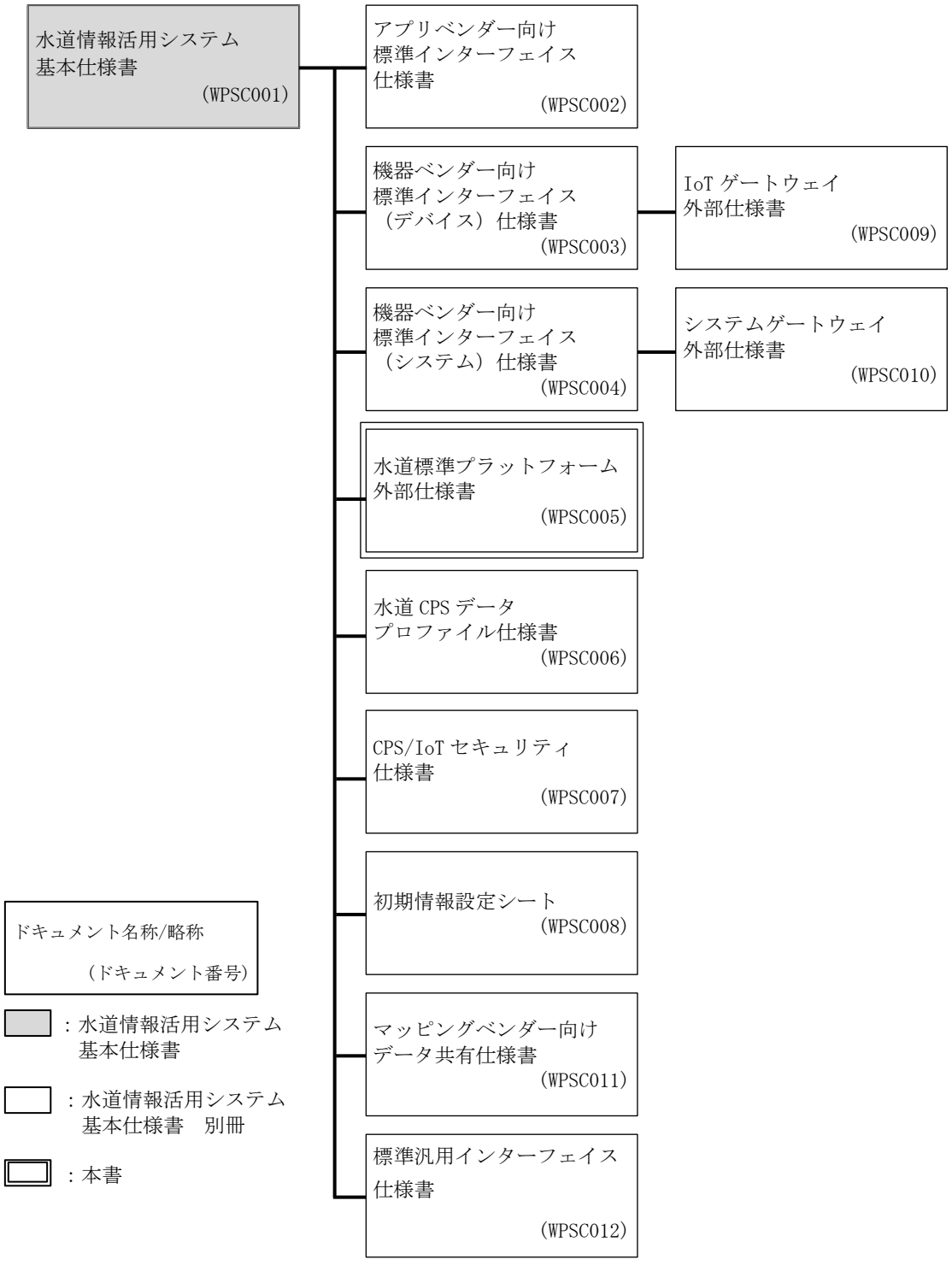


図 1-1: ドキュメント体系

1.2.2 対象読者と役割

水道情報活用システム標準仕様の対象読者と役割を以下に示す。

① 事業体：
水道情報活用システム上のアプリケーションを利用して、デバイス・システムのデータを活用したサービスを享受する事業体。

② アプリケーション開発ベンダー：
水道情報活用システム上のアプリケーションを開発し、デバイス・システムのデータを活用したサービスを事業体に提供するベンダー。

③ IoT ゲートウェイ・デバイスベンダー：
水道情報活用システム上の IoT ゲートウェイを開発し、デバイスのデータを水道標準プラットフォームへ流通するベンダー。

④ システムゲートウェイ・システムベンダー：
水道情報活用システム上のシステムゲートウェイを開発し、各種台帳システムや料金システム等の業務システムのデータを水道標準プラットフォームへ流通するベンダー。

⑤ プラットフォーマー：
水道情報活用システム上の水道標準プラットフォームを提供し、デバイス・システムのデータを流通するサービス提供および運営を行う第三者機関。

⑥ システムインテグレーター：
水道情報活用システム全体の設計を行い、アプリケーション開発ベンダーや IoT ゲートウェイ・デバイスベンダー、システムゲートウェイ・システムベンダーを統率し、水道情報活用システムを事業体に導入するベンダー。

1.2.3 本書の対象読者

本書の対象読者を以下に示す（表 1-1）。

水道情報活用システム　基本仕様書は、(1)～(6)の対象読者が必ず参照すべきドキュメントである。その別冊の各仕様書は、読者の役割に応じて参照すべきドキュメントである。

表 1-1：仕様書別対象読者

ドキュメント番号	ドキュメント名称	対象読者 (1)～(6)は 1.2.2 項参照					
		(1)	(2)	(3)	(4)	(5)	(6)
WPSC001	水道情報活用システム　基本仕様書	○	○	○	○	○	○
WPSC002	水道情報活用システム　基本仕様書　別冊 アプリベンダー向け標準インターフェイス仕様書	－	○	－	－	○	○
WPSC003	水道情報活用システム　基本仕様書　別冊 機器ベンダー向け標準インターフェイス(デバイス)仕様書	－	－	○	－	○	○
WPSC004	水道情報活用システム　基本仕様書　別冊 機器ベンダー向け標準インターフェイス(システム)仕様書	－	－	－	○	○	○
WPSC005	水道情報活用システム　基本仕様書　別冊 水道標準プラットフォーム外部仕様書	－	△	△	△	○	△
WPSC006	水道情報活用システム　基本仕様書　別冊 水道 CPS データプロファイル仕様書	－	○	○	－	○	○
WPSC007	水道情報活用システム　基本仕様書　別冊 CPS/IoT セキュリティ仕様書	－	○	○	○	○	○
WPSC008	水道情報活用システム　基本仕様書　別冊 初期情報設定シート	○	△	△	△	○	○
WPSC009	水道情報活用システム　基本仕様書　別冊 IoT ゲートウェイ外部仕様書	－	－	○	－	－	○
WPSC010	水道情報活用システム　基本仕様書　別冊 システムゲートウェイ外部仕様書	－	－	－	○	－	○
WPSC011	水道情報活用システム　基本仕様書　別冊 マッピングベンダー向けデータ共有仕様書	△	○	－	△	－	○
WPSC012	水道情報活用システム　基本仕様書　別冊 標準汎用インターフェイス仕様書	△	○	○	－	△	○

○：必読、　△：必要に応じて読む、　－：読まなくてもよい

■：本書

1.3 参考文献

水道情報活用システム標準仕様を参照する際の参考文献を以下に示す(表 1-2)。

表 1-2: 参考文献

No.	参考文献	説明
1	ISO 8601	日付と時刻の表記について規定する ISO による国際規格。 URL※: https://www.iso.org/iso-8601-date-and-time-format.html
2	MQTT Protocol Specification	水道標準プラットフォームで利用するメッセージングプロトコルである MQTT について、OASIS により規定されたプロトコル仕様。 URL※: http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html
3	OpenID Connect	認証プロトコルについて規定する、OpenID ファウンデーションによるプロトコル仕様。 URL※:http://www.openid.or.jp/document/
4	OpenID Connect Core 1.0	水道標準プラットフォームで利用するアイデンティティ連携プロトコル仕様。 URL※: http://openid.net/specs/openid-connect-core-1_0.html
5	RFC 2616	Hypertext Transfer Protocol(HTTP/1.1)について規定する IETF による技術仕様。 URL※:https://tools.ietf.org/html/rfc2616
6	RFC 2818	暗号化通信プロトコルである HTTP over TLS(本ドキュメントでは「HTTP(S)」と表記)について規定する、IETF によるプロトコル仕様。 URL※:https://tools.ietf.org/html/rfc2818

No.	参考文献	説明
7	RFC 5246	セキュアな通信を行うためのプロトコルである Transport Layer Security(TLS)について規定する、IETF によるプロトコル仕様。 URL※：https://tools.ietf.org/html/rfc5246
8	RFC 6455	水道標準プラットフォームで利用する通信プロトコルである WebSocket について、IETF により公開されたプロトコル仕様。 URL※：https://tools.ietf.org/html/rfc6455
9	RFC 6750	OpenID Connect のベースである OAuth 2.0 のトークン仕様について規定する、IETF による技術仕様。 URL※：https://tools.ietf.org/html/rfc6750
10	RFC 7231	HTTP/1.1 におけるセマンティクスとコンテンツについて規定する IETF による技術仕様。 URL※：https://tools.ietf.org/html/rfc7231
11	XML Encryption Syntax and Processing	XML 暗号について規定する W3C 勧告。 URL※：http://www.w3.org/TR/xmlenc-core1/
12	XML Signature Syntax and Processing	XML 署名について規定する W3C 勧告。 URL※：http://www.w3.org/TR/xmldsig-core2/

※: 2017 年 7 月時点の URL を参考に記載

その他、参考にする報告書を以下に示す。

経済産業省「平成２８年度ＩｏＴ推進のための社会システム推進事業（スマート工場実証事業）報告書」

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report.pdf

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report_Attachment1.pdf

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report_Attachment2.pd

経済産業省「平成２８年度ＩｏＴ推進のための社会システム推進事業（社会インフラ分野でのＩｏＴ活用のための基盤整備実証プロジェクト)」

http://www.meti.go.jp/meti_lib/report/H28FY/000060.pdf

http://www.meti.go.jp/meti_lib/report/H28FY/000061.pdf

http://www.meti.go.jp/meti_lib/report/H28FY/000062.pdf

1.4 用語の説明

水道情報活用システム標準仕様で使用する用語の説明を以下に示す(表 1-3)。

表 1-3: 用語の説明

No.	用語	説明
1	AI (Artificial Intelligence)	コンピュータを使って学習・推論・判断等、人間の知能の働きを人工的に実現するもの。
2	API (Application Programming Interface)	ソフトウェアコンポーネントが互いにやり取りするのに使用するインターフェイスの仕様。
3	水道情報活用システム	CPS/IoT を活用して、デバイス・システムのデータを流通させ、データを活用した付加価値の高いサービスを提供するシステム。
4	DUNS Number (Data Universal Numbering System Number)	ダンアンドブラッドストリート（D&B）社が開発した 9 桁の企業識別コードのことで、世界の企業を一意に識別できる企業コード。
5	FQDN (Fully Qualified Domain Name)	完全修飾ドメイン名。ホスト名とドメイン名などすべてを省略せずに指定した文字列。
6	IANA (Internet Assigned Numbers Authority)	IP アドレス・ドメイン名・ポート番号等の標準化・割り当て等インターネットに関連する番号を管理する組織。
7	JAN コード (Japanese Article Number)	国際的な流通標準化機関である GS1 が定める国際標準の識別コードを設定するために必要となるコード。国際的には GS1 Company Prefix と呼ばれ、日本では最初の 2 桁が「45」又は「49」で始まる 9 桁又は 7 桁の番号。
8	MIME タイプ (Multipurpose Internet Mail Extension)	IANA に登録されている、転送するデータの種類や形式を判別するための識別子。

No.	用語	説明
9	TDB 企業コード (Teikoku Data Bank)	帝国データバンクが独自に取材・収集した企業情報に加え、各種公的情報を基に、1 社＝1 コードとして厳格に設定した数字 9 桁の企業識別コード。
10	耐タンパー性	非正規な手段による外部からの解析が容易に出来ないよう、データの読み取りや改ざんを防ぐ能力。
11	データプロファイル	「平成 28 年度 IoT 推進のための社会システム推進事業（スマート工場実証事業）」の成果物であり、水道情報活用システム上でデータをやり取りする際のデータ流通のルール。
12	パディング	決められたデータの長さに対してデータが短い場合に、データを追加してデータの長さを合わせる処理。
13	標準企業コード	一般財団法人日本情報経済社会推進協会(JIPDEC)が一元的に管理する、企業を識別する業界横断的な企業コード。 企業を一意に識別できる 6 桁の企業識別コードと、各企業が採番、管理を行う 6 桁の枝番で構成される。
14	ペイロードデータ	パケット通信において、データの転送先や転送経路などを制御するための情報を含むヘッダや、データの破損などを検査するトレーラなどの付加的情報を除いた、ユーザーが送信したいデータ本体。
15	メッセージダイジェスト	任意の長さの文字列を固定長のビット列に変換するアルゴリズム。
16	リダイレクト	ウェブサイトを訪れたユーザーを、自動的に他のウェブページに転送する処理。
17	レルム名	それぞれのレルム(同一の認証ポリシーを適用する範囲)を識別する名称。

1.5 本ドキュメントの記載範囲

本ドキュメントでは、水道情報活用システムの外部仕様について記載する。本ドキュメントの記載範囲を以下に示す(図 1-2)。

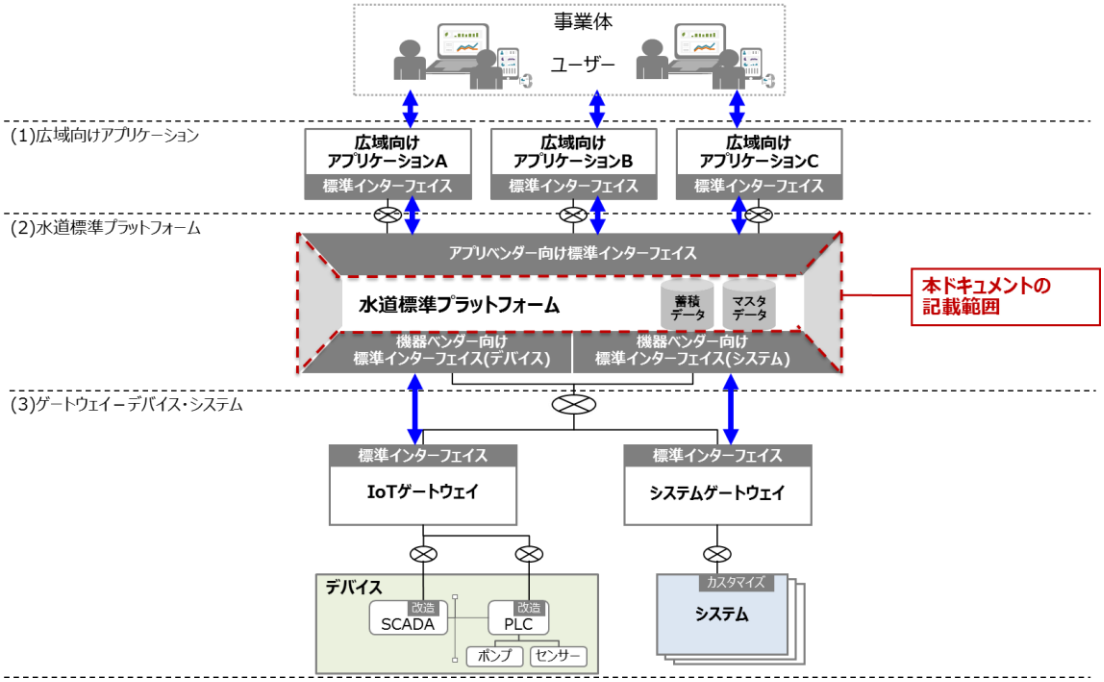


図 1-2: ドキュメント体系図

2. 概要

2.1 水道標準プラットフォームの役割と特徴

水道標準プラットフォームは、標準インターフェイスに則してデバイス・システムのデータを流通させる。水道情報活用システムにおけるサービスプラットフォームの役割を担う。以下に特徴を示す。

・デバイスやシステムのデータ蓄積を行い、データ流通基盤として機能すること。
・データの集積、処理を容易にすること。
・データ流通を実現する標準化された手段を提供すること。

前提として、水道標準プラットフォームに求められる要求事項を以降 2.2 で示す。

2.2 水道標準プラットフォームへの要求事項

国立研究開発法人新エネルギー・産業技術総合開発機構の実証事業（略称 NEDO）「IoT を活用した社会インフラ等の高度化推進事業」において取りまとめられた水道事業者からの要望事項、および、水道業務システムの現状を踏まえ、水道標準プラットフォームに求められる要求事項は以下の点に集約される。

Ａ．水道標準プラットフォームに期待される効果
① コストダウン（従来型システムよりも安くなること）
② 広域化に向けたデータやシステムの共同化
③ 台帳等のデータ整備の促進
④ データを事業者が自由に扱えること
⑤ ＡＩ等のデータ活用

Ｂ．水道標準プラットフォームの効果を実現する際に必要となる対応
① 障害影響の局所化
② リアルタイム性の確保
③ データの安全な流通／蓄積
④ システム障害への迅速な対応
⑤ ベンダー参画を促すための措置

以下、各項目について内容を具体化し、それらを踏まえた水道標準プラットフォームに必要な機能要件、構成要件、および、非機能要件を示す。

2.3 A．水道標準プラットフォームに期待される効果

水道標準プラットフォームを導入することで期待される効果を以降で示す。

2.3.1 コストダウン（従来型システムよりも安くなること）

(1) 機能の共通化

水道標準プラットフォームでは多数の事業者やベンダーが共通で利用するため、事業者及びベンダーが共通的に使えるものを「共通機能」として集約することで、利用者全体で必要な費用を「割り勘」することとなり、事業者にとってはシステムに投資するコストを削減できる。

具体的には、認証や暗号化など、どの事業者のシステムでも横断的に利用可能な機能については、個別にサーバーを立てずに、共通的に利用可能なサーバーを少数置くことで、クラウドの IaaS 利用料を削減することが可能となる。

本要求は以下の要件に具体化される。

表 2-1: 共通機能の集約化のための機能要件

要件種別	要件名	概要
構成要件	共通機能の集約化	機能要件のなかで、事業者やベンダーが共通的に利用可能なものについて、IaaS のリソースを集約することでコスト削減を図る。

(2) 運用保守作業の共有化

水道標準プラットフォームは様々な事業者やアプリケーションが共同利用しており、障害発生時には円滑に連携して対応する必要がある。様々な対応ベンダーに、システムの動作状況や障害に関する情報を「共有画面」として管理・提供することで、発生した障害箇所を早期に特定できる仕組みを提供し、システム障害への迅速な対応が可能となる。このような作業プロセスでは、問合せ受付やインシデント管理などを共通化することが有効であり、全体の作業量を削減することが可能である。

本要求は以下の要件に具体化される。

表 2-2: 運用保守作業の共有化のための機能要件

要件種別	要件名	概要
機能要件	システム動作監視	システムの動作状況や障害に関する情報を集約して、提供する。
	ユーザーインターフェイス	上記で収集した情報の提供、および、問合せ受付やインシデント管理などの共通機能を提供する。

(3)　開発・構築の手間の削減

クラウド環境では、サーバーの増減や新規機能のサーバーの追加が容易であるため、その特性を活かしたシステム構築、運用が期待される。一方で、作業コストを低減するためにはそうしたサーバーの立ち上げ作業（デプロイ）を省力化しておく必要がある。

その解決策として、コンテナ技術を活用し、各種 OS 上での動作が保障されている「コンテナ」により、動作試験を含めたサーバーのデプロイ作業を省力化することが必要となる。つまり、クラウドが提供するコンテナ技術等を活用して、簡単に機能提供やアプリケーションを迅速に増設できるようにする。また簡単に「アプリケーション」ごとに増設できることで、アプリケーションを水道標準プラットフォームに載せる際のコストを削減できる（図 2-1：ベンダーアプリケーションでのコンテナ利用のメリット）。

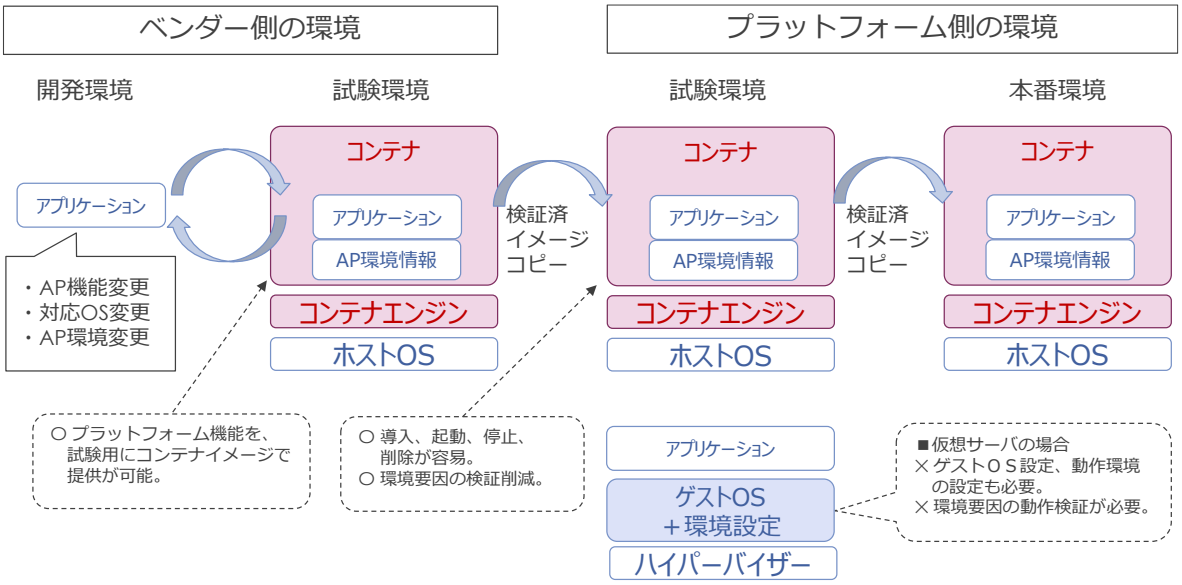


図 2-1：ベンダーアプリケーションでのコンテナ利用のメリット

本要求は以下（表 2-3：開発・構築の手間の削減のための機能要件）の要件に具体化される。

表 2-3：開発・構築の手間の削減のための機能要件

要件種別	要件名	概要
構成要件	コンテナ化	コンテナでのサーバー起動を可能とし、水道標準プラットフォーム構築やアプリケーション導入の手間を削減できるようにする。

2.3.2　広域化に向けたデータやシステムの共同化

(1)　アプリケーションや現場システムの利用の共同化

アプリケーションや現場システムの利用の共同化するためには、それらを自由に選択できることが重要となる。これを実現するためには NEDO 実証事業の成果である「オープンな標準仕様（標準インターフェイス）」を水道標準プラットフォームに配置し、データの流通性を確保することにより、ベンダーロックを解除することがポイントとなる。共通的な仕様によりデータを送受信することで、アプリケーションや現場システムが入れ替わっても同じ機能を提供可能となり、それらの自由な選択が実現する。

その上で、ユーザーごとにポータル画面を提供し、アプリケーションをポータル画面から選んで利用可能とすることで、共同利用する各事業者のユーザーは共通の操作でアプリケーションを利用することができる。

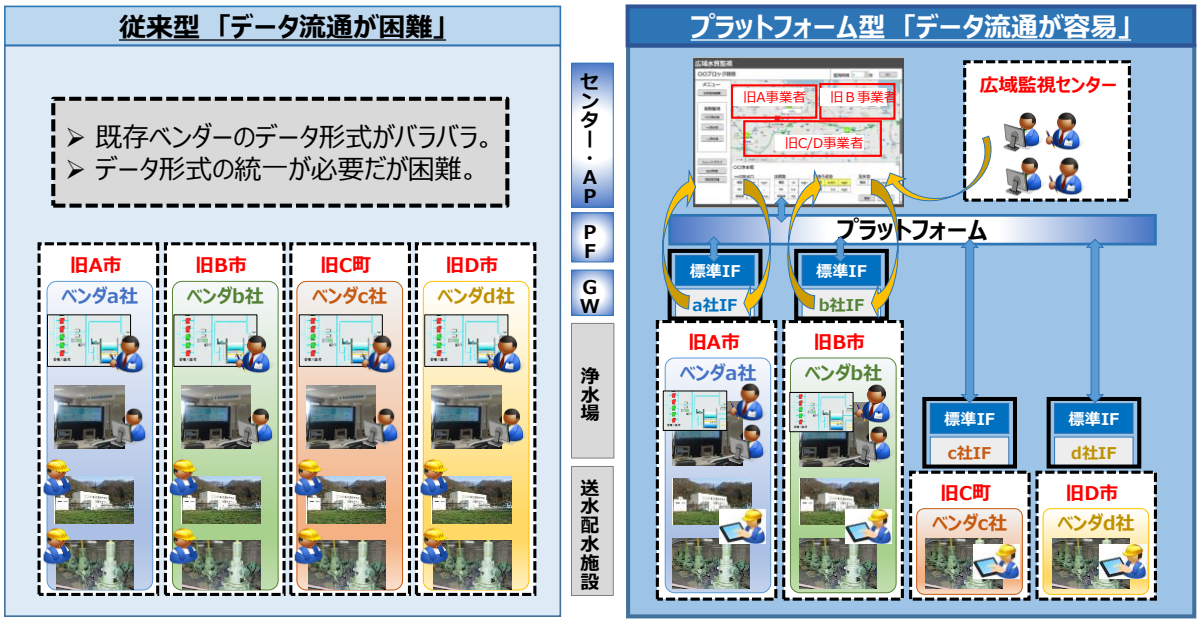


図 2-2: アプリケーションや現場システムの利用の共同化

本要求は以下の要件に具体化される。

表 2-4:アプリケーションや現場システムの利用の共同化のための機能要件

要件種別	要件名	概要
機能要件	アプリケーション向け標準インターフェイス（デバイス）	IoT 系アプリケーションに対する標準仕様での通信機能の提供
	アプリケーション向け標準インターフェイス（システム）	システム系アプリケーションに対する標準仕様での通信機能の提供

要件種別	要件名	概要
	ゲートウェイ向け標準インターフェイス（デバイス）	IoT ゲートウェイに対する標準仕様での通信機能の提供
	ゲートウェイ向け標準インターフェイス（システム）	システムゲートウェイに対する標準仕様での通信機能の提供
	ユーザーインターフェイス	ベンダーに依らないアプリケーション利用時の共通的なユーザーインターフェイスの提供

(2) データ利用の共同化

従来、水道事業者のデータは各ベンダーのアプリケーション内に保持され、そのデータ構造が不明なため、データの共有やデータ移行に大きな労力が発生していた。しかし、水道事業の広域化を促進するためには、複数事業者間でのデータ共有や、システム再統合時のデータ移行を円滑に行う必要がある。

データの共有や移行を進めるため、水道標準プラットフォームにデータを蓄積できるようにし、さらに、データ項目を、マスタ・スキーマとして登録・共有して、データを誰でも利用できるようにする。これにより、データを複数の事業者やシステムで共同利用でき、お互いの業務を共同で実施するなど、システムの効率化や集約化が期待できる。

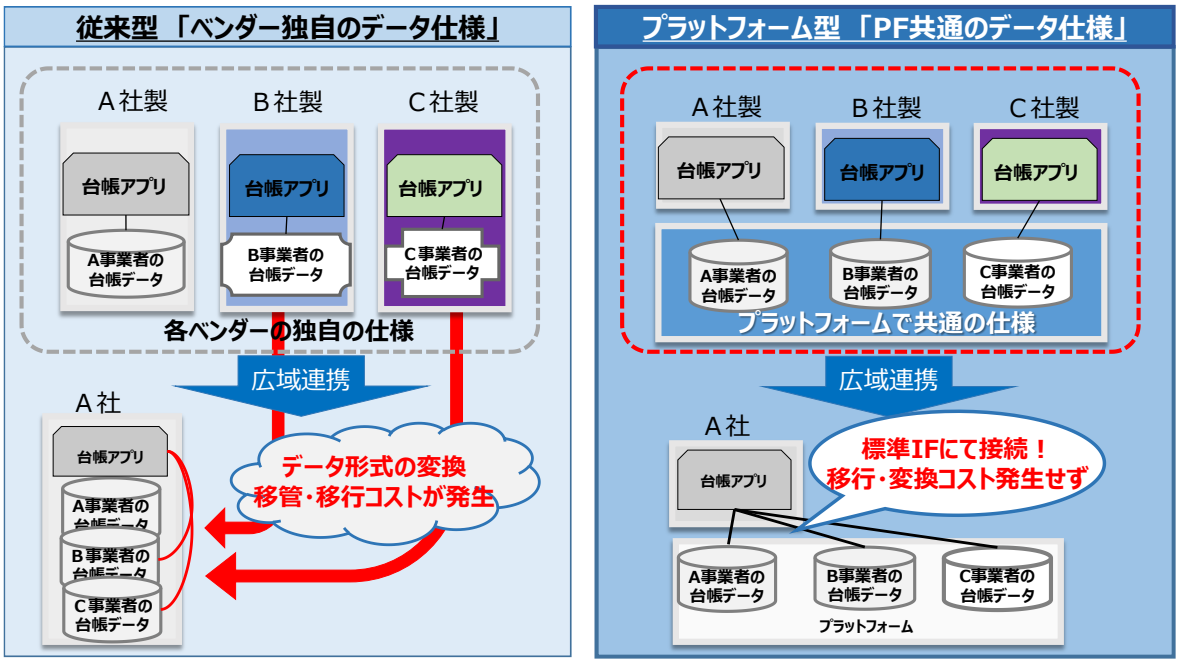


図 2-3:データ保持・蓄積によるシステム移行におけるメリット

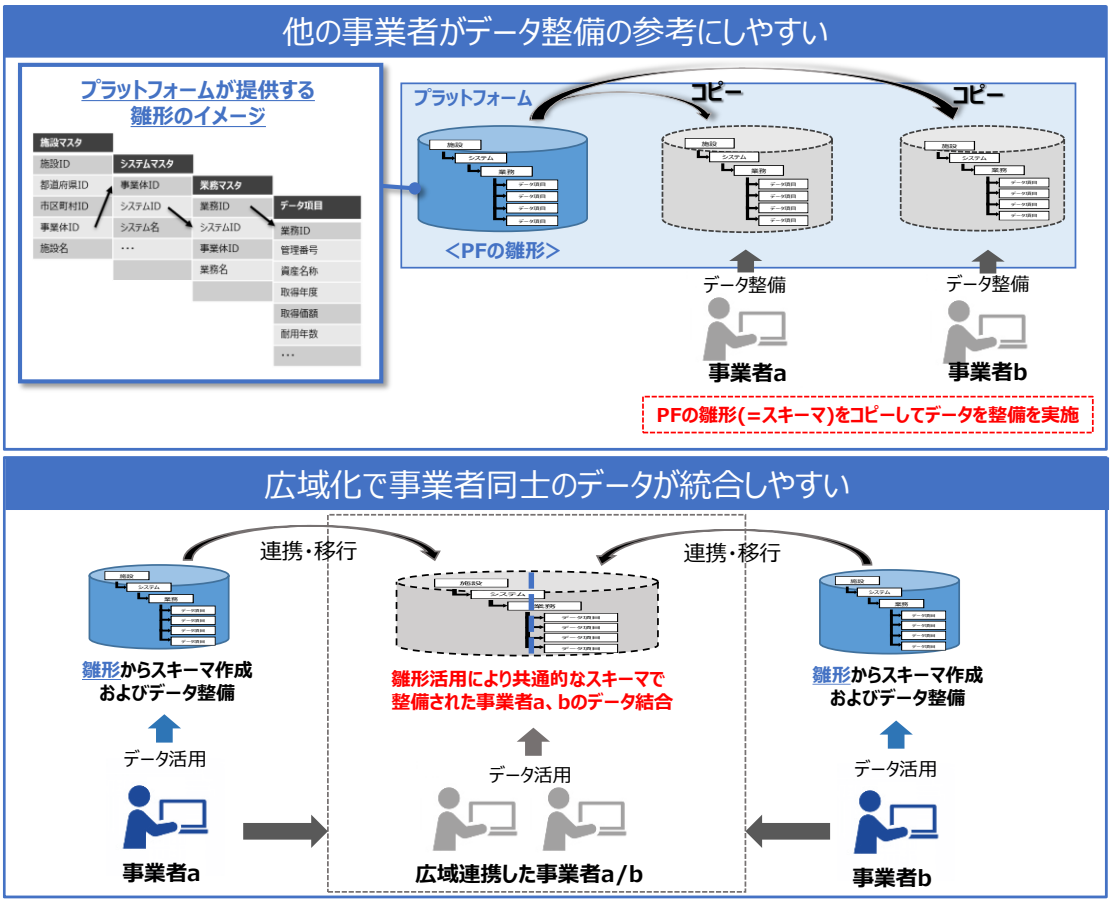


図 2-4:広域連携時のデータ連携の実現

本要求は以下（表 2-5:データ利用の共同化のための機能要件）の要件に具体化される。

表 2-5:データ利用の共同化のための機能要件

要件種別	要件名	概要
機能要件	データ蓄積	ゲートウェイから収集したデータおよびアプリケーションから書き込まれたデータを蓄積し、要求に応じて提供する。
	マスタ管理	上記で蓄積されたデータの項目内容（マスタ、スキーマ）を保存、公開する。 これにより、誰でもデータの利活用を可能とし、データの共有を促進する。

2.3.3 台帳等のデータ整備の促進

水道法改正により台帳系データの整備が促進されているが、どのようなデータをどのように投入すれば良いかを明確に示し、利用者にとって分かりやすい仕組みを簡単に提供することが求められている。そのためには、データ項目の雛形を提供し、その雛形を水道標

準プラットフォームに登録して、データ保存形式として利用できるようにする。これにより、データの項目が明確になるため、誰でも簡単に、かつ、共通の形式で、台帳等のデータ登録を進められる。

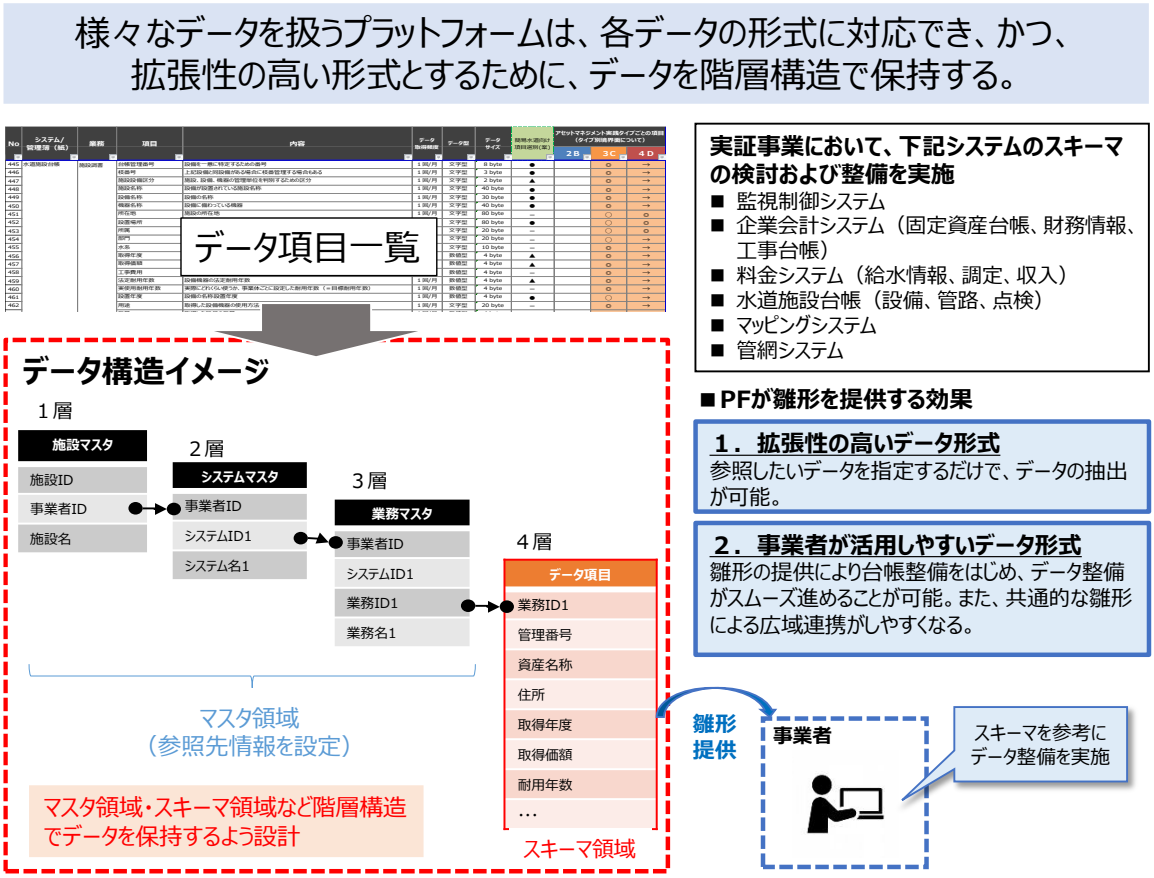


図 2-5:水道標準プラットフォームでのデータの保持の仕方とその雛形

本要求は以下（表 2-6:台帳等のデータ整備の促進のための機能要件）の要件に具体化される。

表 2-6:台帳等のデータ整備の促進のための機能要件

要件種別	要件名	概要
機能要件	マスタ管理	「データ蓄積」機能で蓄積されたデータの項目内容（マスタ、スキーマ）を保存、公開する。これにより、データ登録時の雛形として利用可能とする。

2.3.4 データを事業者が自由に扱えること

従来の「ベンダーのシステムの中に事業者のデータが保管されている」という構造から、「データは事業者が自由に扱える仕組み」への変革を実現するため、データを水道標

準プラットフォームに蓄積できるようにし、さらに、アプリケーションの処理結果も水道標準プラットフォームに保存するようにする。

そして、水道標準プラットフォームでは、事業者がベンダーのアプリケーションに依らずデータを取り出し、修正ができるようにすることで、データを事業者が自由に扱うことを実現する。

本要求は以下の要件に具体化される。

要件種別	要件名	概要
機能要件	データ蓄積	ゲートウェイから収集したデータおよびアプリケーションから書き込まれたデータを蓄積し、要求に応じて提供する。
	ユーザーインターフェイス	事業者が、ベンダーのアプリケーションに依らずデータを取り出し、修正ができるようにすることで、データを事業者が自由に扱うことを実現する。

2.3.5 ＡＩ等へのデータ活用

ＡＩ等の先端ＩＴ技術は水道事業者における人材不足等の様々な課題解決に向けた有用なソリューションとなりえる可能性がある。しかしながら、AI 機能活用については、その前提として AI が学習するための長期間かつ多量のデータが必要となる。また、利用するデータの種類についても、数値データだけではなく、画像や文字列などの非構造データが含まれる。

近年のクラウドサービスでは、オブジェクトストレージと呼ばれる非構造データを大量かつ安価に保存する機能を提供しており、この機能を利用することで、ＡＩ等の最新ＩＴ技術を活用し、水道事業における各種課題の解決に資することが期待される。

本要求は以下 8 の要件に具体化される。

要件種別	要件名	概要
機能要件	データ退避（オブジェクトストレージ）	「データ蓄積」機能にて容量の制限から蓄積ができなくなったデータを保存し、長期間かつ多量のデータを保存する。

2.4 水道標準プラットフォームの効果を実現する際に必要となる対応

上述した効果を実現するために、水道標準プラットフォームとして必要な対応を以降で示す。

2.4.1 サービス指向アーキテクチャ(SOA)の採用

水道情報活用システムが構成する各サービスの実証時の独立性を高めるため、各サービスを個別のモジュールとして粗結合によりシステムを構成するサービス指向アーキテクチャ(SOA)を採用する。これにより、以下のメリットが期待される。

- 各モジュールの再利用が容易になるため、水道情報活用システムの構築/変更/運用コストが削減される。
- 水道情報活用システムの変更に対して柔軟に対応可能となるため、水道情報活用システムの新技術の導入や新機能追加の期間が短縮される。

モジュール間の通信には、汎用的な通信プロトコルである HTTP over SSL/TLS を利用した REST 通信を採用することで、ミドルウェア、ソフトウェアに依存しない方式を採用する。水道標準プラットフォームのモジュール構成を以下に示す(図 2-6)。

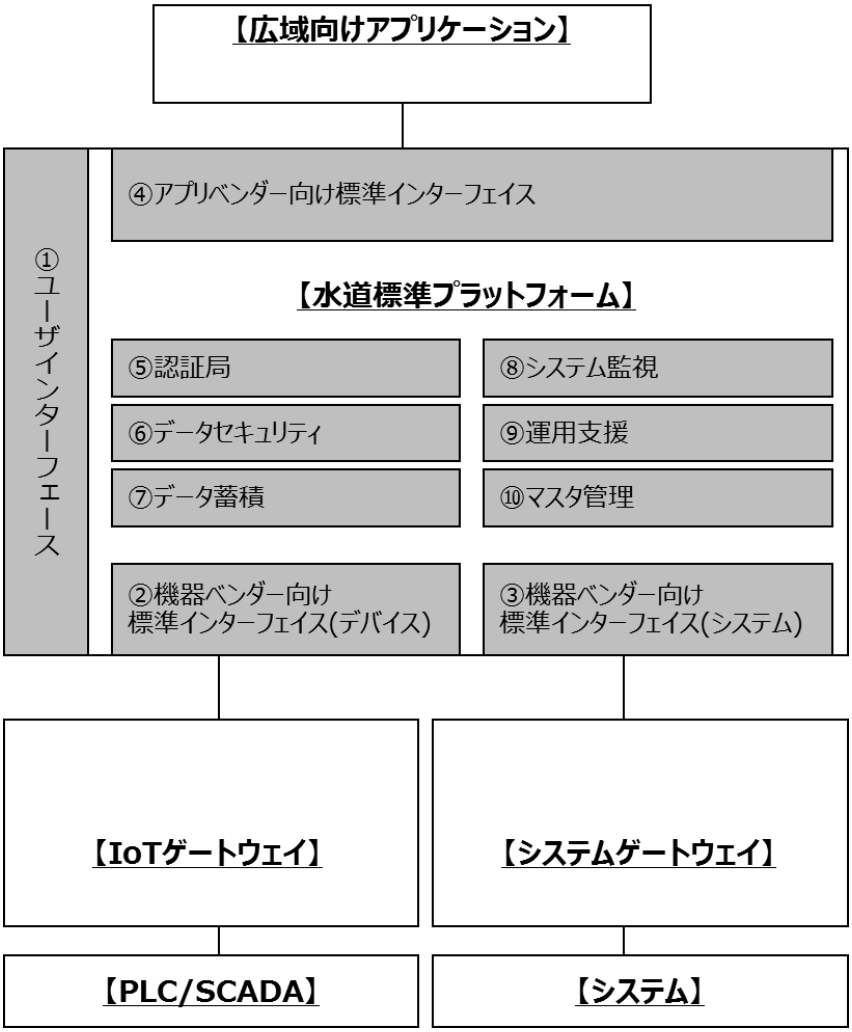


図 2-6: 水道標準プラットフォームのモジュール構成

2.4.2 オープンソース技術の採用

水道標準プラットフォームは、コスト低減のため、基本的にオープンソースソフトウェア(OSS)を採用する。また、通信プロトコルは、汎用的、一般的に広く採用されている通信プロトコルを採用する。これにより、以下のメリットが期待される。

- ライセンス費用が無償となる OSS を採用することにより、水道情報活用システム導入コストが削減される。
- 一般的に広く採用されている技術を用いることにより、新規ベンダーの参入を促進し、自由競争を促進する。

2.4.3 クラウドサービスの採用

水道標準プラットフォームは、安全性、コスト削減の観点から、従来のオンプレミス構成ではなく、クラウドサービス上での構成を採用する。これにより、以下のメリットが期待される。

- サーバー拡縮が容易に行えるため、利用者数(サーバー負荷･データ発生数)に合わせて、サーバー構成の変更が容易･かつ安価に行え、運用コストを必要最小限にしやすい
- クラウドサービスでは、遠隔データ保護及び、障害時の復旧体制が整備されているため、災害発生時でも安全に水道情報活用システム運用を行える。

2.4.4 障害影響の局所化

水道標準プラットフォームでは、多数の水道事業者のシステムを同時に稼働させる必要があるが、特定の事業者における通信負荷や処理負荷が、他事業者の業務に影響を発生することは避けなければならず、その対策は、運用ではなくアーキテクチャとして検討を実施しておく必要がある。具体的には、共同利用していても障害発生時に影響をできるだけ局所化して、波及を抑制する必要がある。テナント構成をクラウド内に適用することで、システムトラブルが発生してもその対象箇所の局所化を実現する。その実現手段としては、クラウドサービスとしてある一定の処理リソースを一つの区画として扱う「テナント」という仕組みがあり、事業者のシステムを各テナントに分けて、回線リソースやサーバーリソースを配置し、お互いの影響を分離することが、クラウドのアーキテクチャを利用した解決策となる。

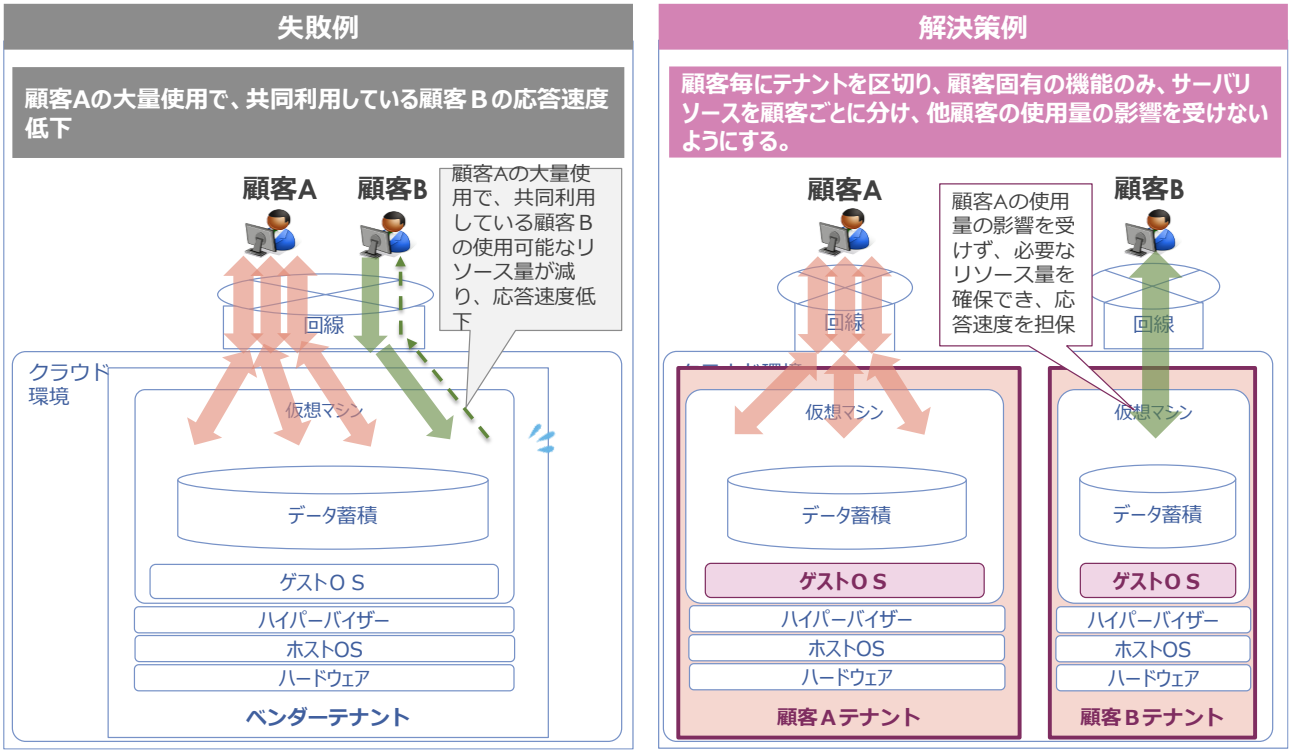


図 2-7： テナントによる影響分離

データ収集のトラフィックが増大しても、制御操作を確実に実施できるようにする必要がある。これには、通常の「監視信号(上り信号)」と、「制御信号(下り信号)」とを分離した構成をとることで、制御信号が確実に現地 GW に届くようにする。

本要求は以下の要件に具体化される。

要件種別	要件名	概要
構成要件	テナント化	テナントにより事業者毎のデータ蓄積や流通を分離する構成をとる。
	監視／制御の分離	監視の処理と制御の処理を実施するサーバーを分離する構成をとる。

2.4.5 リアルタイム性の確保

ゲートウェイから水道標準プラットフォームへのデータ収集では、アラームの発生時など、時に大量のデータが集中する。また、データの処理方式を高速にしておくことで、少ないサーバー数で水道標準プラットフォームを運用でき、ランニングコストを低減できる。

そのため、データの受信とデータの保存を高速に行い、データの取り漏れ（＝データの欠損）を回避することが重要である。この問題を解決するために、最新の IT 技術を活用し、データの受信では軽量プロトコル(MQTT)を、データの保存ではインメモリ DB（KVS）を、それぞれ採用し、それぞれの処理を高速化することにより、データの欠損を回避する。

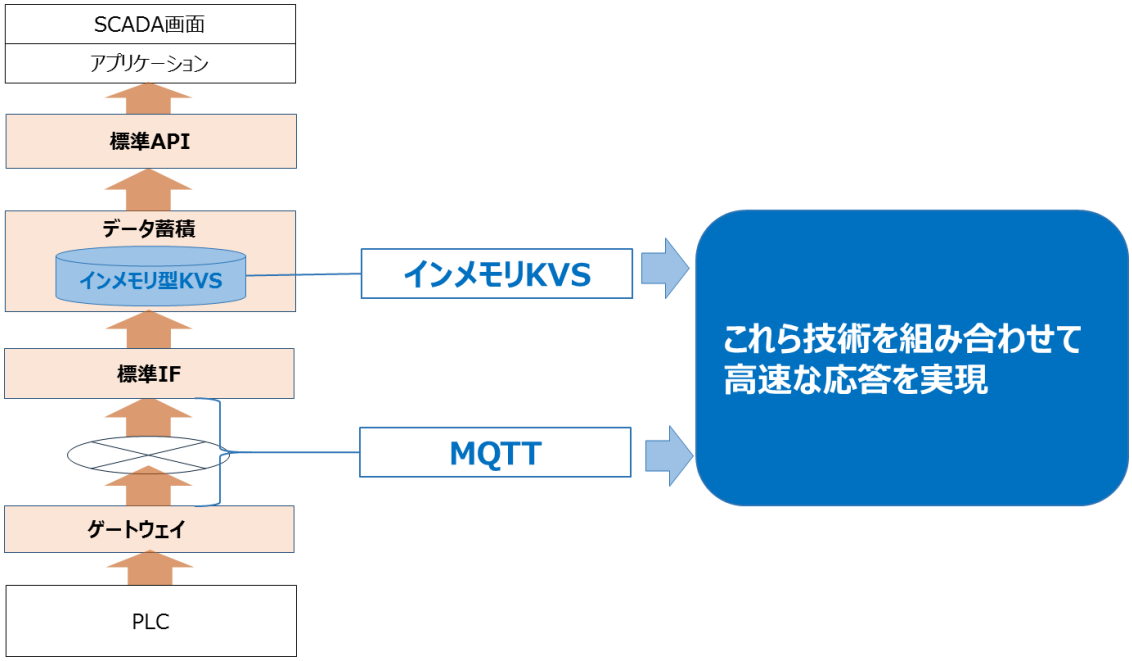


図 2-8：リアルタイム性の確保

本要求は以下の要件に具体化される。

要件種別	要件名	概要
機能要件	ゲートウェイ向け標準インターフェイス（デバイス）	IoT ゲートウェイに対する標準仕様での通信機能を提供する。 軽量プロトコル「MQTT」を利用し、大量データの送受信を可能とする。
	データ蓄積	ゲートウェイから収集したデータおよびアプリケーションから書き込まれたデータを蓄積し、要求に応じて提供する。 インメモリ DB「KVS」を利用し、大量データの読み書きを可能とする。
非機能要件	性能・拡張性	データ流通の処理時間の目標値を規定する。

2.4.6 データの安全な流通／蓄積

水道事業は国の重要インフラの一つとされ、そのデータ保護は、水道事業に関わる情報システムの基本的な要件の一つである。

水道標準プラットフォームは様々な事業者やアプリケーションが共同利用しており、またネットワークを通じて多数のアクセスがあることから、適切なセキュリティ対策をとる必要がある。主要な対策としては以下が挙げられる。

（ア）　データは事業者毎に分けて蓄積し、データにアクセスする際には、アプリケーションとユーザーの両方に対して適切な権限を持っていることを確認する。

（イ）　データの送受信時には暗号化により漏えいを防止する。

下図に示すようにデータ流通の様々なリスク観点から対策を行うことで、データが保護され、安心して水道標準プラットフォームを利用することができる。

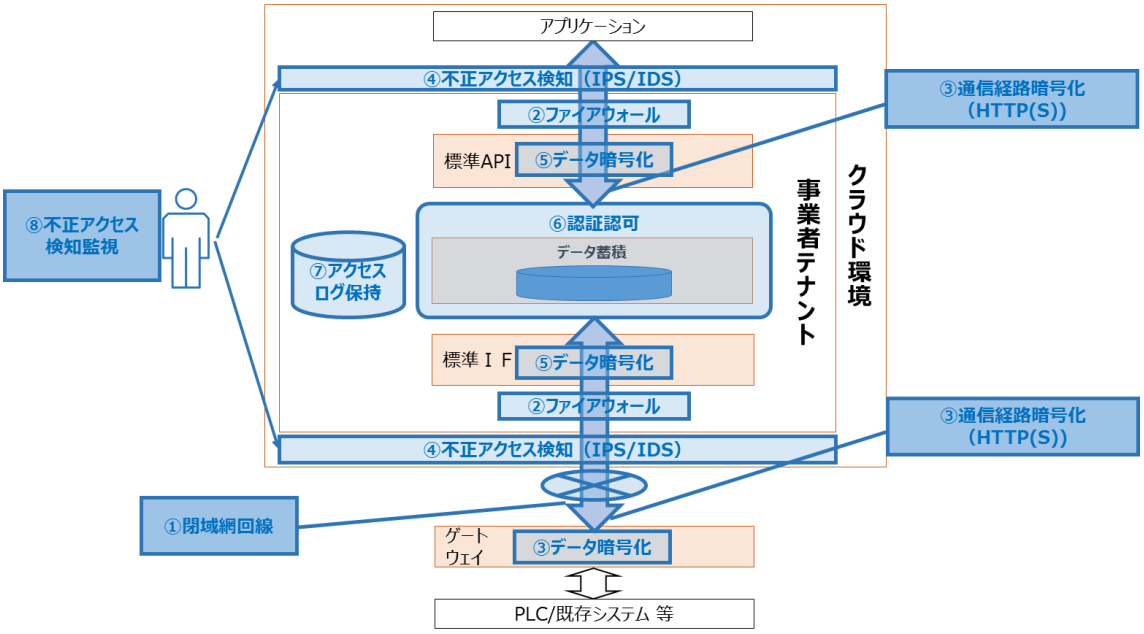


図 2-9：セキュリティ性の確保

本要求は以下の要件に具体化される。

要件種別	要件名	概要
機能要件	データセキュリティ	③通信経路暗号化、⑤データ暗号化　を実現する。
	認証局	上記に必要な証明書を発行する。
	認証認可	⑥認証認可　を実現する。 具体的には、ユーザーとアプリケーションに対して所定の権限を確認し、蓄積データへのアクセスを制約する。
	ユーザーインターフェイス	ユーザーのログイン画面を提供し、ユーザーの認証を行う。また、ユーザー権限の管理機能も提供する。
非機能要件	セキュリティ	セキュリティ対策として、他の対策項目を含めて全体を網羅して、対策内容を規定する。

2.4.7　システム障害への迅速な対応

従来型のシステムに対して、水道標準プラットフォーム型のシステムでは、アプリケーション、データベース、ゲートウェイが分離され、さらに、複数のベンダーのデータが流通する。そのため、サービス毎にサーバーが独立して稼働し、不具合発生時の発生箇所が追跡しづらくなるという課題がある。

この問題に対し、水道標準プラットフォームの各要素（アプリケーションやゲートウェイ）および、そこに流通するデータ項目に対して ID を割り振り、データの流通を水道標準プラットフォームで統一的に監視することで不具合の発生個所を発見できるようにする。例えば、アプリケーションなどの各機能がマイクロサービスとして粗結合な状態でシステムが構成されれば、マイクロサービス間のリクエスト・レスポンスの応答結果を残すことが出来るため、不具合発生個所やタイミングを具体的にとらえることが可能となる。

データ流通や機器状態の監視は、水道標準プラットフォーム内のサーバーだけに限定するものではなく、ゲートウェイベンダー／通信回線事業者／アプリケーションベンダー／クラウド事業者など、水道情報活用システムの運用保守に関係する各事業者と連携して、ゲートウェイ、通信回線、アプリケーション、IaaS 基盤などから、システム動作状況のログなどを常時収集する。この機能により、水道標準プラットフォームとしてシステム動作監視側で一括集約して提供し、水道標準プラットフォーム・ベンダーに共有するなどが可能となり、運用作業の集約化、故障発生時の円滑な対応を実現する（**図 2-10：システム障害発生時の発生箇所特定について**）。

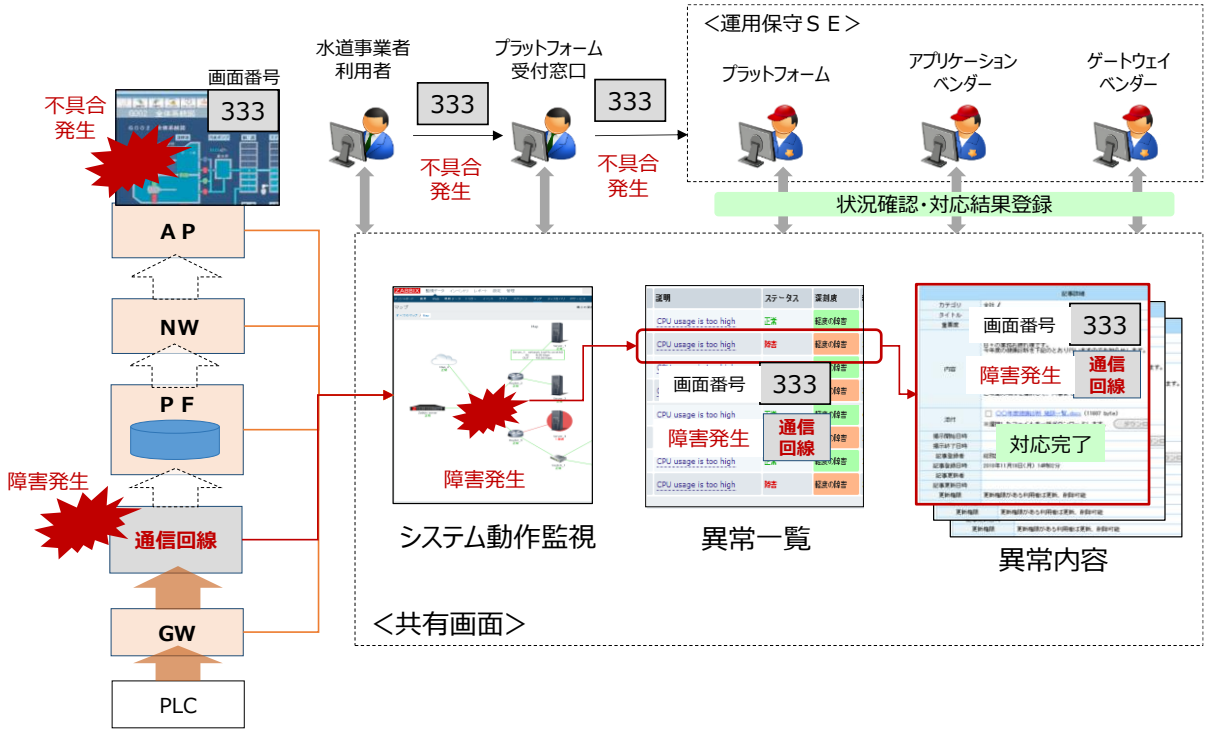


図 2-10：システム障害発生時の発生箇所特定について

本要求は以下の要件に具体化される。

要件種別	要件名	概要
機能要件	システム動作監視	システムの動作状況や障害に関する情報を集約して、提供する。

2.4.8 ベンダー参画を促すための措置

事業者からは多くのベンダーの参加を期待されていることに対し、アプリケーションの標準インターフェイス対応状況が途上であることを鑑み、ベンダーのアプリケーションと水道標準プラットフォーム上のデータとの接続については、暫定期間を 2025 年 3 月末として、従来のベンダーの「独自方式」での接続を許可する方針とする。なお、その場合でも、データ流通の機能は維持する必要があるため「標準インターフェイス」を活用して、他のアプリケーションがデータを取得できる仕組みを提供する。

本要求は以下の要件に具体化される。

要件種別	要件名	概要
構成要件	システム系データ流通	独自インターフェイスによる蓄積データへのアクセス、および、共有データの確保を実現する構成

これら必要な踏まえ、水道標準プラットフォームが提供するサービスを以下に示す。

2.5 水道標準プラットフォームが提供するサービス

2.5.1 広域アプリケーション向け提供サービス

水道標準プラットフォームが広域アプリケーション向けに提供するサービスは以下の通り(表 2-7)。

表 2-7: 水道標準プラットフォーム 広域アプリケーション向け提供サービス

No	サービス内容	サービス提供に必要な機能／作業	
		必要なシステム処理機能	必要な運用作業【参考】
1	事業に必要なデータを蓄積し、アプリケーションの要求に応じて（認証認可プロセスを経て）データを送受信する。	・ アプリベンダー向け標準インターフェイス ・ 認証局 ・ データ蓄積 ・ マスタ管理	・ データバックアップ
2	アプリケーションに対して、事業体毎の要件に応じたアプリケーションの基盤環境を提供する。	（なし）	・ クラウド基盤提供
3	アプリケーションに対して、運用に関する各種機能やサービスを提供する。	・ 運用支援	・ 運転監視 ・ コールセンター ・ 切り分け SE
4	アプリケーションに対して、試験環境・試験手順を提示し、データ流通に関する判定をする。	（なし）	・ アプリケーション導入
5	アプリケーションに提供した基盤環境の運用保守（運転監視、パッチ対応等）を実施する。	・ システム監視	・ パッチ対応 ・ 復旧作業
6	事業に必要なデータに対してセキュリティレベルを設けて、必要なセキュリティ機能を提供する。	・ データセキュリティ	・ セキュリティ設定

2.5.2 ゲートウェイ向け提供サービス

水道標準プラットフォームがゲートウェイ向けに提供するサービスは以下の通り(表 2-8)。

表 2-8: 水道標準プラットフォーム ゲートウェイ向け提供サービス

No	サービス概要	サービス提供に必要な機能／作業	
		必要なシステム処理機能	必要な運用作業【参考】
1	ゲートウェイから送受信されるデータを、適切な格納場所や送信先にデータを流通する。	・ 機器ベンダー向け標準インターフェイス ・ マスタ管理 ・ データ蓄積	（なし）
2	ゲートウェイに対して、運用に関する各種機能やサービスを提供する。	・ 運用支援	・ 運転監視 ・ コールセンター ・ 切り分け SE
3	ゲートウェイに対して、試験環境・試験手順を公開し、データ流通に関する判定をする。	（なし）	・ ゲートウェイ導入
4	必要に応じて、ゲートウェイ環境の運用保守・運転監視を実施できる。	・ システム監視	・ パッチ対応 ・ 復旧作業
5	ゲートウェイ側のセキュリティレベルに合わせて、必要なセキュリティ対応をする。	・ データセキュリティ	・ セキュリティ設定

2.5.3 利用者向け提供サービス

水道標準プラットフォームが利用者向けに提供するサービスは以下の通り(表 2-9 ： 水道標準プラットフォーム 利用者向け提供サービス)。

表 2-9 ： 水道標準プラットフォーム 利用者向け提供サービス

No	サービス概要	サービス提供に必要な機能／作業	
		必要なシステム処理機能	必要な運用作業【参考】
1	水道情報活用システムの利用者が、適切なアクセス権限のもとに、各種機能を利用できる画面を提供する。	・ ユーザーインターフェイス	・ ユーザー設定

2.5.4 水道標準プラットフォームに必要なシステム処理機能

以上を踏まえ、水道標準プラットフォームが必要とするシステム処理機能について以下に記載する（表 2-10: 水道標準プラットフォームのシステム処理機能一覧)。

表 2-10: 水道標準プラットフォームのシステム処理機能一覧

No.	システム処理機能	説明
1	ユーザーインターフェイス	水道情報活用システムの利用者に対して、水道標準プラットフォームの提供を利用するための画面を提供する。
2	機器ベンダー向け 標準インターフェイス(デバイス)	デバイスのデータ向けに標準化されたインターフェイス。水道標準プラットフォームと IoT ゲートウェイ間でデータをやり取りする。 ※詳細は、”機器ベンダー向け標準インターフェイス(デバイス)仕様書”を参照すること。
3	機器ベンダー向け 標準インターフェイス(システム)	システムのデータ向けに標準化されたインターフェイス。水道標準プラットフォームとシステムゲートウェイ間でデータをやり取りする。 ※詳細は、”機器ベンダー向け標準インターフェイス(システム)仕様書”を参照すること。
4	アプリベンダー向け 標準インターフェイス	広域向けアプリケーションに対する標準化されたインターフェイス。デバイス、システム、外部サービスへの統一的なアクセス方法を提供する。 ※詳細は、”アプリベンダー向け標準インターフェイス仕様書”を参照すること。
5	認証局	水道 CPS/IoT リファレンスモデルにおける「アプリケーション」、「ゲートウェイ」、「水道標準プラットフォーム」間で利用する証明書/秘密鍵を一元的に管理する。
6	データセキュリティ	水道 CPS/IoT リファレンスモデルにおける「水道標準プラットフォーム」内の通信データの暗号化、電子署名付与を行う。
7	データ蓄積	機器ベンダー向け標準インターフェイス(デバイス/システム)より、連携されたデータを、水道標準プラットフォーム内部データベースにて蓄積管理を行う。 蓄積管理されたデータをアプリベンダー向け標準インターフェイスよりデータ抽出要求を受け取り、要求情報に合致したデータを抽出し、返却する。
8	システム監視	水道標準プラットフォームのシステム管理者に対して、水道標準プラットフォームおよびゲートウェイのシステム状態を監視するための機能を提供する。
9	運用支援	水道 CPS/IoT リファレンスモデルにおける「水道標準プラットフォーム」の運用業務を支援する。

No.	システム処理機能	説明
10	マスタ管理	外部モジュールに対して、データベースサーバーにて管理されている各マスタテーブル情報のデータ提供及び、データ更新の要求を受け付ける。

水道標準プラットフォームのモジュール構成を以下に示す（図 2-11）。

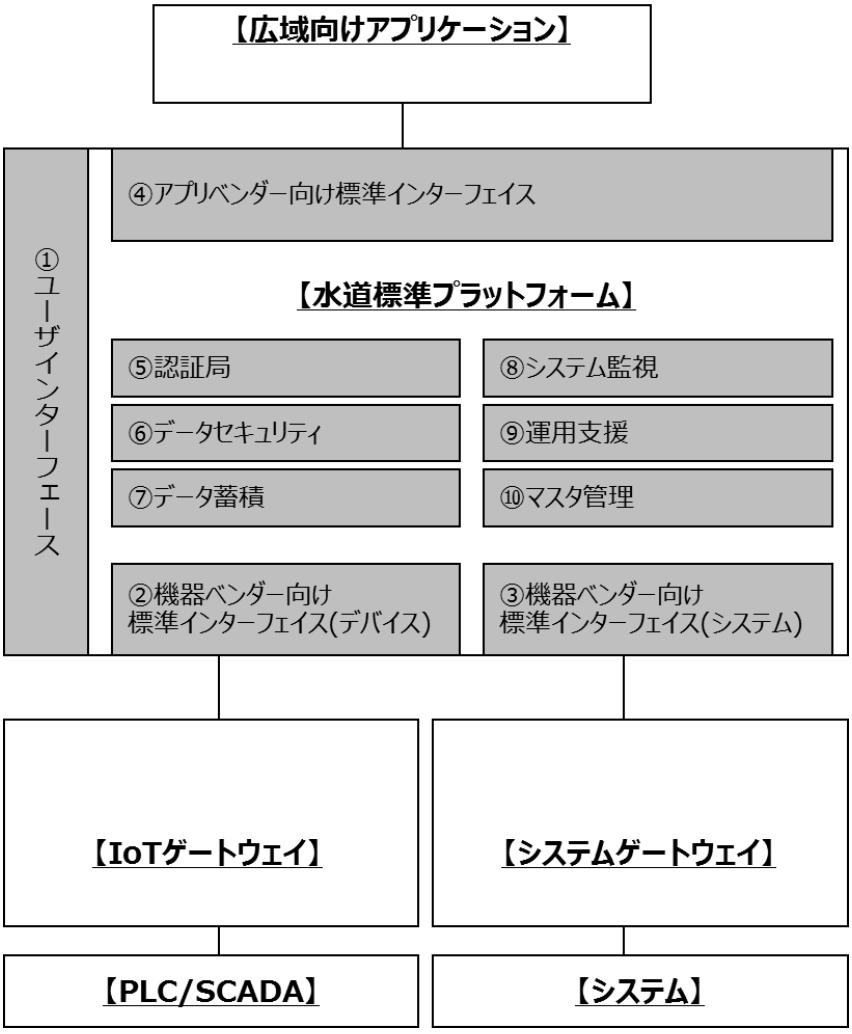


図 2-11: 水道標準プラットフォームのモジュール構成

2.5.5 水道標準プラットフォームの機能における競争領域と協調領域

水道標準プラットフォームは、標準インターフェイスに則してデバイス・システムのデータを収集し、標準インターフェイスに即してアプリケーションに対しデータを流通させる役割を担うプラットフォームであり、ため、全ての機能が標準仕様に即した仕様やルールに従う必要がああり、「協調領域」として定義される。

3. ユーザーインターフェイスモジュール

3.1 概要

3.1.1 機能概要

ユーザーインターフェイスは水道情報活用システムの利用者に対して、水道標準プラットフォームを利用するための画面を提供する機能群である。以下に本モジュールの機能概要を示す。

- 水道標準プラットフォームを利用するためのポータル画面を提供する。
- 水道情報活用システムを利用する事業体の運用管理者に対して水道標準プラットフォームの運用を支援するための管理画面を提供する。
- 水道情報活用システムの利用者に与えられた権限に応じてアクセス制御を行う。

3.1.2 機能一覧

ユーザーインターフェイスの機能一覧を以下に示す（図 3-1、表 3-1)。

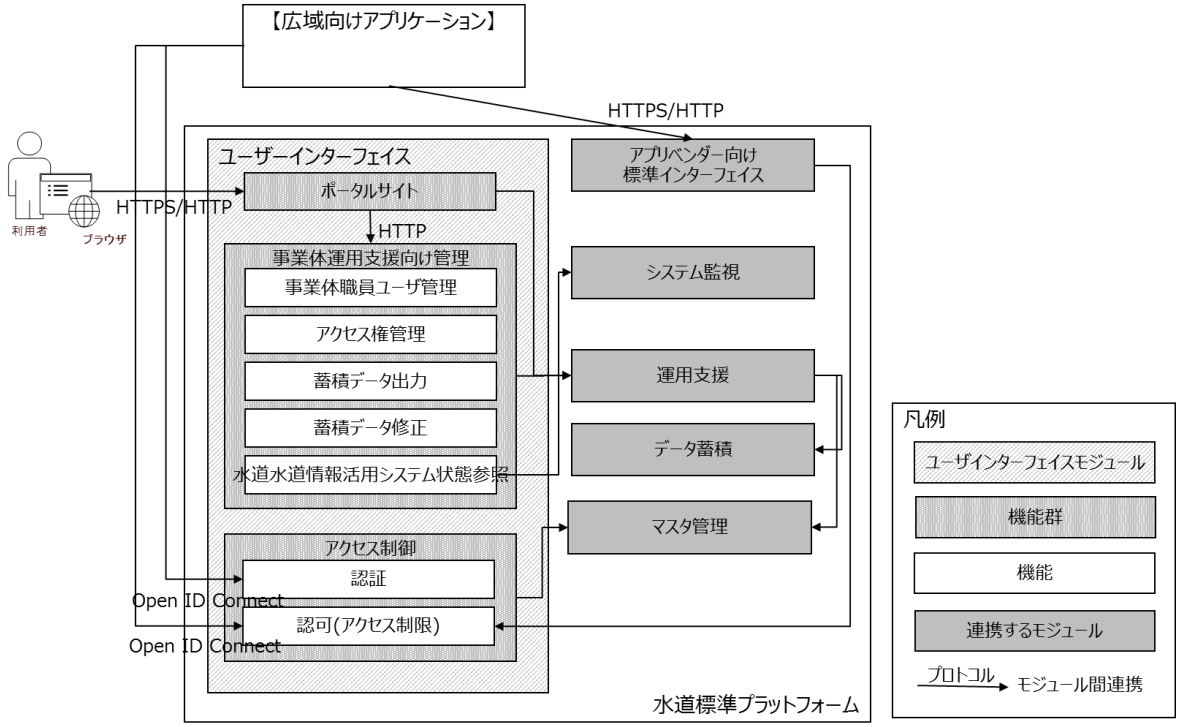


図 3-1: ユーザーインターフェイスの機能(モジュール)構成

表 3-1: ユーザーインターフェイス機能一覧

No	機能名	説明
1	ポータルサイト	利用者の権限情報に即したメニューを表示する。
2	事業体運用支援向け管理	業体運用管理者に対して水道標準プラットフォームの運用を支援するための管理画面を提供する。
3	事業体職員ユーザー管理	事業体職員(管理者)ユーザーおよび事業体職員(一般)ユーザーを作成、削除及び変更する画面を提供する。
4	アクセス権管理	権限に対して事業体の管理する IoT ゲートウェイやシステムゲートウェイのアクセス権を付与、削除および変更する画面を提供する。
5	蓄積データ出力	水道標準プラットフォームで管理する蓄積データを出力する画面を提供する。
6	蓄積データ修正	水道標準プラットフォームで管理する蓄積データを修正する画面を提供する。
7	水道情報活用システム状態参照	水道標準プラットフォームの水道情報活用システム監視画面へのリンクをポータルサイトの画面に表示する。
8	アクセス制御	水道情報活用システムの利用者を認証(本人確認)し、広域向けアプリケーション･ゲートウェイ･データへのアクセスを認可(アクセス権限制御)する。
9	認証	水道情報活用システムの利用者を認証(本人確認)する。
10	認可(アクセス制限)	利用者からの広域向けアプリケーション、ゲートウェイ、データへのアクセスについて権限チェックを行う。

(1) 機能提供の対象者

ユーザーインターフェイスが画面およびアクセス制御機能を提供する対象となる水道情報活用システム利用者を以下に示す(表 3-2)。

表 3-2: 機能提供の対象者一覧

利用者の種別	利用者の所属	利用者の種類	利用者の概要
ユーザー	ブロック統括	広域管理者	事業体からの委託を受けて複数の事業体の浄水場を管理する。
	事業体	事業体職員(管理者)	特定の事業体の浄水場を管理する。
		事業体職員(一般)	特定の事業体の浄水場を管理する。

			ただし、管理者と比べて権限が少ない。
		事業体運用管理者	水道標準プラットフォームにおける事業体の運用を管理する。
	アプリベンダー	アプリケーションシステム管理者	事業体からの委託を受けてアプリケーションのメンテナンスを行う。
	プラットフォーマー	水道標準プラットフォームシステム管理者	水道標準プラットフォームのメンテナンスを行う。
水道情報活用システム	広域向けアプリケーション	サービスアカウント	ユーザーがログインしていない状態でバックグラウンド動作する際の利用者。

(2) アクセス制限対象

水道情報活用システム全体でアクセス制限を行う対象と水道標準プラットフォームでの実現範囲を以下に示す(表 3-3)。

表 3-3: アクセス制限対象一覧

アクセス制限対象	対象の概要	アクセス制限を実現するサブシステム	本モジュールでのアクセス制限対象
広域向けアプリケーション	水道情報活用システムの構成要素の一つで、水道情報活用システムを利用する事業体に対して各種業務サービスを提供する。	水道標準プラットフォーム	○
アプリケーションへの操作内容	画面表示やボタン操作といったアプリケーションの処理。	広域向けアプリケーション	×
アプリベンダー向け標準インターフェイス(水道標準プラットフォーム側)	広域向けアプリケーションに対する標準化されたインターフェイス。これによりデバイス、システム、外部サービスへの統一的なアクセス方法を提供する。	水道標準プラットフォーム	○
IoT ゲートウェイシステムゲートウェイ	デバイス・システムのデータを水道標準プラットフォームにデータ流通するためのサブシステム。	水道標準プラットフォーム	○
IoT 機器操作	センサ値取得・機器制御といったIoT 機器の処理。	IoT ゲートウェイ	×

	データ操作	データ取得･データ更新といったシステムデータに対する処理。	システムゲートウェイ	×

(3) 水道情報活用システムにおける権限の管理構成

水道情報活用システムでは、利用者に付与された権限によりアクセス制限を行う。水道情報活用システムにおける権限の管理構成について下記に方針を示す。

- 利用者の役割に応じた権限を集約し、権限ロールとして管理する。
- この権限ロールを利用者に割り当てることで利用者に付与された権限を管理する。
- 複数の役割を担う利用者に対して、複数の権限ロールを割り当てることができる。
- 利用者の役割の範囲に応じて 2 分類の権限ロールに分類して管理する。
  - 水道情報活用システム全体における役割：CPS システム権限ロール
  - 事業体内部における役割：事業体権限ロール

(a) CPS システム権限ロール

CPS システム権限ロールは、水道情報活用システム全体における利用者の役割に応じた権限をまとめた権限ロールである。CPS システム権限ロールについて、例を以下に示す(表 3-4)。

表 3-4: CPS システム権限ロール 例

CPS システム権限ロール	利用者の役割	利用者の概要
広域管理者権限ロール	広域管理者	事業体からの委託を受けて複数の事業体の浄水場を管理する。
事業体職員権限ロール	事業体職員(管理者)	特定の事業体の浄水場を管理する。
	事業体職員(一般)	特定の事業体の浄水場を管理する。 ただし、管理者と比べて権限が少ない。
事業体運用管理者権限ロール	事業体運用管理者	水道標準プラットフォームにおける事業体の運用を管理する。
アプリケーションシステム管理者権限ロール	アプリケーションシステム管理者	事業体からの委託を受けてアプリケーションのメンテナンスを行う。
水道標準プラットフォームシステム管理者権限ロール	水道標準プラットフォームシステム管理者	水道標準プラットフォームのメンテナンスを行う。
サービスアカウント権限ロール	サービスアカウント	ユーザーがログインしていない状態でバックグラウンド動作する際の利用者。

(b)　事業体権限ロール

事業体権限ロールは、事業体内部における利用者の役割に応じた権限をまとめた権限ロールである。事業体内部における利用者の役割の種類については事業体ごとに異なるため、事業体運用管理者が任意の事業体権限ロールを管理する。

3.2 機能要件

3.2.1 ポータルサイト機能

水道標準プラットフォームを利用するためのポータル画面を提供する。ポータルサイト機能の要件は以下の通り。

- 利用者の権限情報に即したメニューを表示すること。
- 利用者の利用可能な広域向けアプリケーションへのリンクをポータルサイトの画面に表示すること。
- 水道情報活用システムメンテナンス期間中は利用者の操作を制限する画面を表示すること。

3.2.2 事業体運用支援向け管理機能

事業体運用管理者に対して水道標準プラットフォームの運用を支援するための管理画面を提供する。なお、事業体運用管理者は、原則として、水道標準プラットフォームで管理する情報のうち、自身の所属する事業体に関連する情報に限定して管理を行う。ただし、水道標準プラットフォームのシステム状態については事業体の運用継続に関わる情報となるため、水道標準プラットフォーム全体のシステム状態を参照可能とする。事業体運用支援向け管理機能の機能要件は以下の通り(表 3-5)。

表 3-5: 事業体運用支援向け管理機能一覧

No.	機能名	機能要件
1	事業体職員ユーザー管理機能	事業体職員(管理者)ユーザーおよび事業体職員(一般)ユーザーを作成、削除及び変更する画面を提供すること。 ※事業体職員以外の水道情報活用システム利用者のユーザーの作成は初期登録時に、プラットフォーマーにて行う。
		事業体の管理する事業体職員ユーザーに対して適切な権限付与が可能であること。
		作成、削除、変更機能は、ログとして記録し、必要に応じて解析可能であること。
2	アクセス権管理機能	権限に対して事業体の管理する IoT ゲートウェイやシステムゲートウェイのアクセス権を付与、削除および変更する画面を提供すること。
		作成、削除、変更機能は、ログとして記録し、必要に応じて解析可能であること。
3	蓄積データ出力機能	出力範囲としてゲートウェイおよび出力期間の指定が可

		能であること。
		出力形式は CSV 形式であること。
		文字コードは UTF-8 であること。
		出力内容をログとして記録し、必要に応じて解析可能であること。
4	蓄積データ修正機能	出力形式は CSV 形式であること。
		文字コードは UTF-8 であること。
		出力内容をログとして記録し、必要に応じて解析可能であること。
5	システム状態参照機能	水道標準プラットフォームのシステム監視画面へのリンクをポータルサイトの画面に表示すること。

3.2.3 アクセス制御機能

本機能は、水道情報活用システムの利用者を認証(本人確認)し、広域向けアプリケーション・ゲートウェイ・データへのアクセスを認可(アクセス権限制御)する。以下に、機能の概要を示す(図 3-2)。

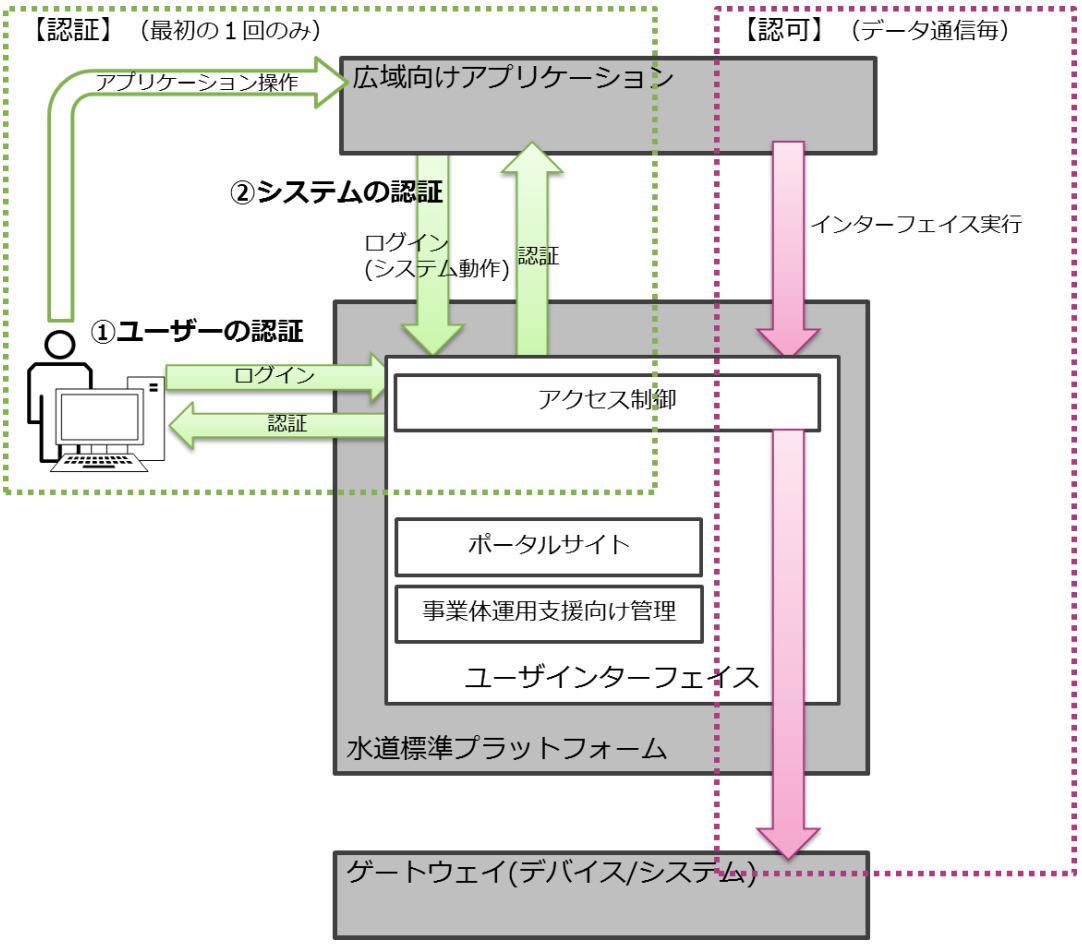


図 3-2: アクセス制御機能概要

(1) 認証機能

水道情報活用システムの利用者を認証(本人確認)する。水道情報活用システム利用開始時に一度認証を行うことにより、以降はユーザーアカウントとパスワードの入力無しで水道情報活用システムおよびアクセス制限対象へアクセス可能とする。認証対象の一覧と認証の要件を、以下に示す(表 3-6)。

表 3-6: 認証機能要件

利用者の種類	認証の要件
①ユーザー	水道情報活用システムへ接続する際にユーザーの本人性をチェックし、正規の利用者であることを確認する。
②水道情報活用システム	水道情報活用システムへ接続する際にはシステムの正当性をチェックし、正規の利用者であることを確認する。

(2) 認可(アクセス制限)機能

利用者からの広域向けアプリケーション、ゲートウェイ、データへのアクセスについて権限チェックを行う。利用者からのアクセスの対象が複数指定されていた場合、すべてのアクセス対象に権限がある場合のみアクセスを認可する。認可(アクセス制限)機能の要件を、以下に示す(表 3-7)。

表 3-7: 認可(アクセス制限)機能要件

アクセス制御対象	認可(アクセス制限)の要件
広域向けアプリケーション	下記の利用者のみアクセス可能であること。 ・ 利用申請を行った事業体に所属する利用者であること。 ・ 利用申請を行った事業体より許可された利用者であること。
アプリベンダー向け標準インターフェイス (水道標準プラットフォーム側)	水道情報活用システムに登録された利用者のみアクセス可能であること。
IoT ゲートウェイ システムゲートウェイ	下記の利用者のみアクセス可能であること。 ・ 利用申請を行った事業体に所属する利用者であること。 ・ 利用申請を行った事業体より許可された利用者であること。

3.3 利用プロトコルと暗号化について

3.3.1 利用プロトコルについて

下記の HTTP サービスへのアクセス部分のアイデンティティ連携プロトコルは OpenIDConnect プロトコルを使用することとする。フレームワーク上に認証情報を集約して一元管理を行うものとする。

- アクセス制御機能
- ポータルサイト
- 事業体運用支援向け管理画面
- 広域向けアプリケーション

3.3.2 暗号化について

通信経路は、暗号技術により機密性を確保し情報漏えいや改ざんを防止すること。詳細は、CPS/IoT セキュリティ仕様書を参照すること。

4. 認証局モジュール

4.1 概要

4.1.1 機能概要

認証局は、水道 CPS/IoT リファレンスモデルにおける「アプリケーション」、「ゲートウェイ」、「水道標準プラットフォーム」間で利用する証明書/秘密鍵を一元的に管理する機能を提供するモジュールである。以下に本モジュールの機能概要を示す。

- アプリケーション/ゲートウェイが初期登録時に必要な証明書/秘密鍵を提供すること。
- 水道標準プラットフォームが通信データの暗号化、電子署名付与に利用する証明書/秘密鍵を提供すること。
- アプリケーション/ゲートウェイが通信データの暗号化、電子署名付与に利用する証明書/ 証明書失効リストを提供すること。

4.1.2 機能一覧

認証局の機能一覧を以下に示す。（図 4-1）

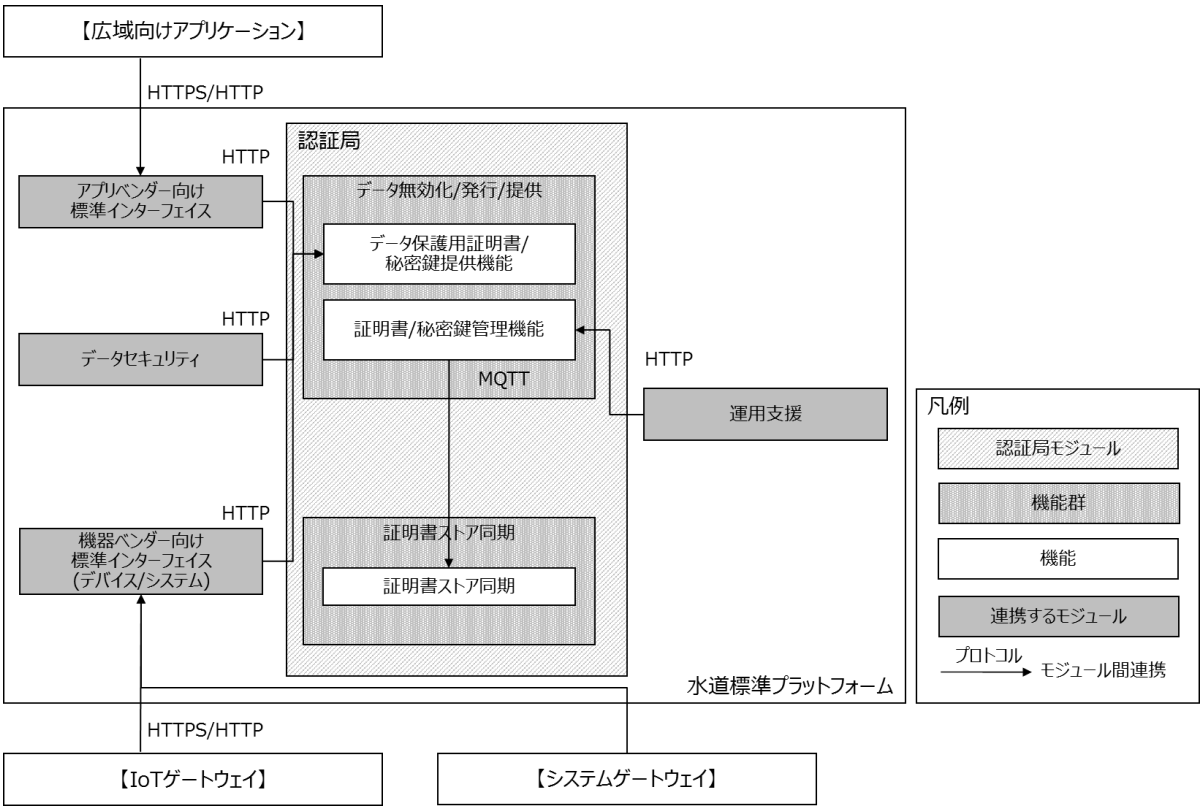


図 4-1: 認証局の機能(モジュール)構成

表 4-1: 認証局機能一覧

No	機能名	説明
1	データ保護用証明書/秘密鍵提供機能	データセキュリティ、アプリベンダー向け標準インターフェイス、機器ベンダー向け標準インターフェイス(デバイス/システム)へ各種証明書(データ保護用)、水道標準プラットフォーム秘密鍵(データ保護用)、ルート証明書、証明書失効リストを提供する。
2	証明書/秘密鍵管理機能	運用支援へ、各種証明書、各種秘密鍵、ルート証明書、証明書失効リストを管理する機能を提供する。
3	証明書ストア同期機能	自身の証明書ストアを他の証明書ストアと同期する。

認証局が機能を提供するモジュールを以下に示す(表 4-2)。各モジュールは、この外部機能に対するインターフェイスを実装する。

表 4-2: 連携する外部機能の一覧

No	モジュール	概要	利用/提供
1	データセキュリティ	・ アプリケーション証明書(データ保護用)を提供する。 ・ ゲートウェイ証明書(データ保護用)を提供する。 ・ 水道標準プラットフォーム秘密鍵(データ保護用)を提供する。 ・ ルート証明書を提供する。 ・ 証明書失効リストを提供する。	提供
2	運用支援	・ アプリケーション初期登録時にアプリーション証明書(データ保護用/TLS 用)/アプリケーション秘密鍵(データ保護用/TLS 用)を発行し、提供する。 ・ ゲートウェイ初期登録時にゲートウェイ証明書(データ保護用/TLS 用)/ゲートウェイ秘密鍵(データ保護用/TLS 用)を発行し、提供する。 ・ 秘密鍵(データ保護用/TLS 用)の漏洩時に各種証明書(データ保護用/TLS 用)/各種秘密鍵(データ保護用/TLS 用)を発行、無効化する機能を提供する。	提供
3	アプリベンダー向け標準インターフェイス	・ 証明書失効リストを提供する。 ・ アプリベンダー向け標準インターフェイスを経由し、アプリケーションへ水道標準プラットフォーム証明書(データ保護用)と証明書失効リストを提供する。	提供
4	機器ベンダー向け標準インターフェイス	・ 証明書失効リストを提供する。 ・ 機器ベンダー向け標準インターフェイスを経由し、ゲートウェイへ水道標準プラットフォーム証明書(デー	提供

No	モジュール	概要	利用/提供
	(デバイス/システム)	タ保護用)と証明書失効リストを提供する。	

4.2 機能要件

4.2.1 データ保護用証明書/秘密鍵提供機能

(1) データセキュリティ向け提供機能

(a) 機能概要

データセキュリティへ、以下の機能を提供する。

- アプリケーション証明書(データ保護用)を提供する機能
- ゲートウェイ証明書(データ保護用)を提供する機能
- 水道標準プラットフォーム秘密鍵(データ保護用)を提供する機能
- ルート証明書と証明書失効リストを提供する機能

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 4-2)。

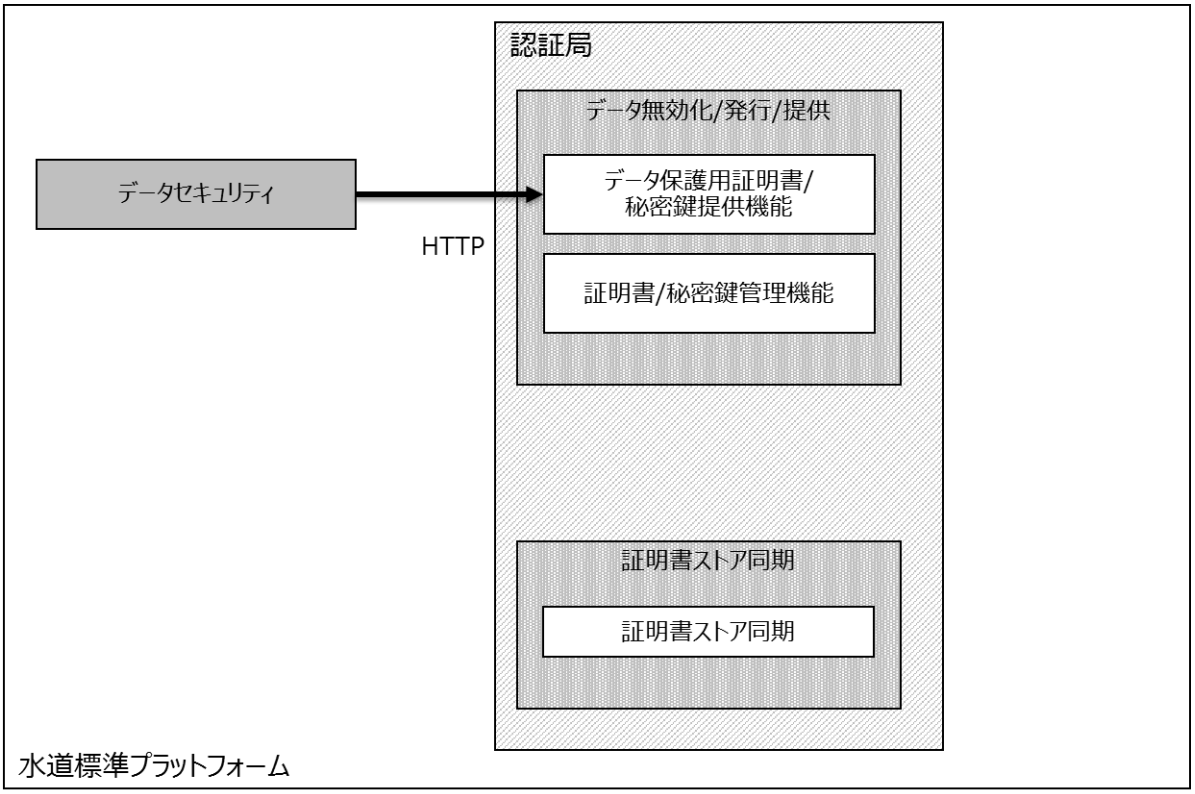


図 4-2: データ証明書/秘密鍵提供機能 データセキュリティ向け提供経路

(c) リクエスト概要

データセキュリティから認証局へ要求する際に連携する情報を以下に記載する(表

4-3)。

表 4-3: リクエスト概要

項目	内容
ID	以下の何れかを指定する。 ・ アプリケーション ID ・ ゲートウェイ ID ・ 水道標準プラットフォーム ID(「0000」を指定)
要求コード	以下の何れかを指定する。 ・ 証明書 ・ 秘密鍵(ID が「0000」の場合のみ指定可能)

(d) レスポンス概要

認証局からデータセキュリティへ応答する際に連携する情報を以下に記載する(表 4-4)。

表 4-4: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書 / 秘密鍵情報	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書データ ・ 秘密鍵データ
ルート証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ ルート証明書データ ・ 証明書失効リストデータ

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 4-5)。

表 4-5: 通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	水道標準プラットフォームルート証明書/証明書失効リスト 水道標準プラットフォーム秘密鍵（データ保護用） ゲートウェイ証明書（データ保護用） アプリケーション証明書（データ保護用）

(2)　標準インターフェイス向け提供機能

(a)　機能概要

アプリベンダー向け標準インターフェイス及び機器ベンダー向け標準インターフェイス(デバイス/システム)へ、以下の機能を提供する。

・　証明書失効リストを提供する。

(b)　提供経路

機能を提供経路する経路を以下に図示する(図 4-3)。

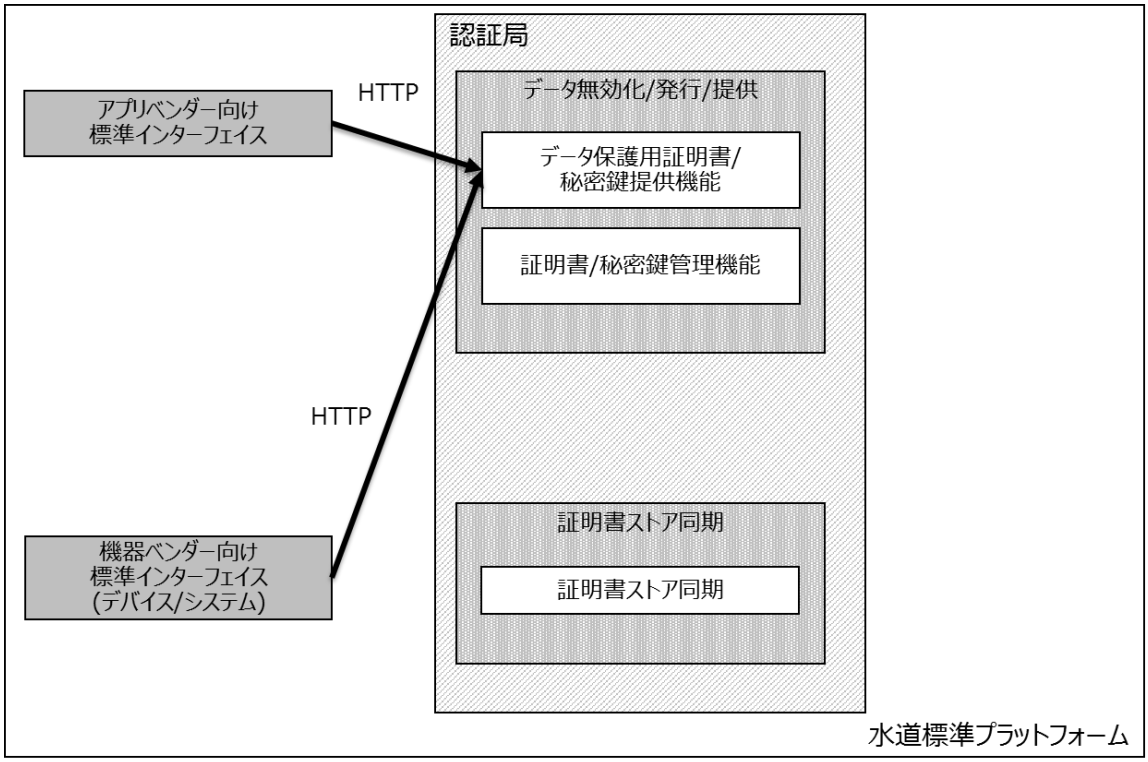


図 4-3: データ保護用証明書/秘密鍵提供機能 標準インターフェイス向け提供経路

(c)　リクエスト概要

アプリベンダー向け標準インターフェイス及び機器ベンダー向け標準インターフェイス(デバイス/システム)から認証局へ、リクエスト設定項目なしでリクエストを実施する。

(d)　レスポンス概要

認証局からアプリベンダー向け標準インターフェイス及び機器ベンダー向け標準インターフェイス(デバイス/システム)へ応答する際に連携する情報を以下に記載する(表 4-6)。

表 4-6: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書失効リストデータ

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 4-7)。

表 4-7: 通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	水道標準プラットフォーム証明書失効リスト

(3) 広域アプリケーション向け 提供機能

(a) 機能概要

広域向けアプリケーションへ、アプリベンダー向け標準インターフェイスを経由して、以下の機能を提供する。

- 水道標準プラットフォーム証明書(データ保護用)を提供する機能
- 水道標準プラットフォーム証明書失効リストを提供する機能

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 4-4)。

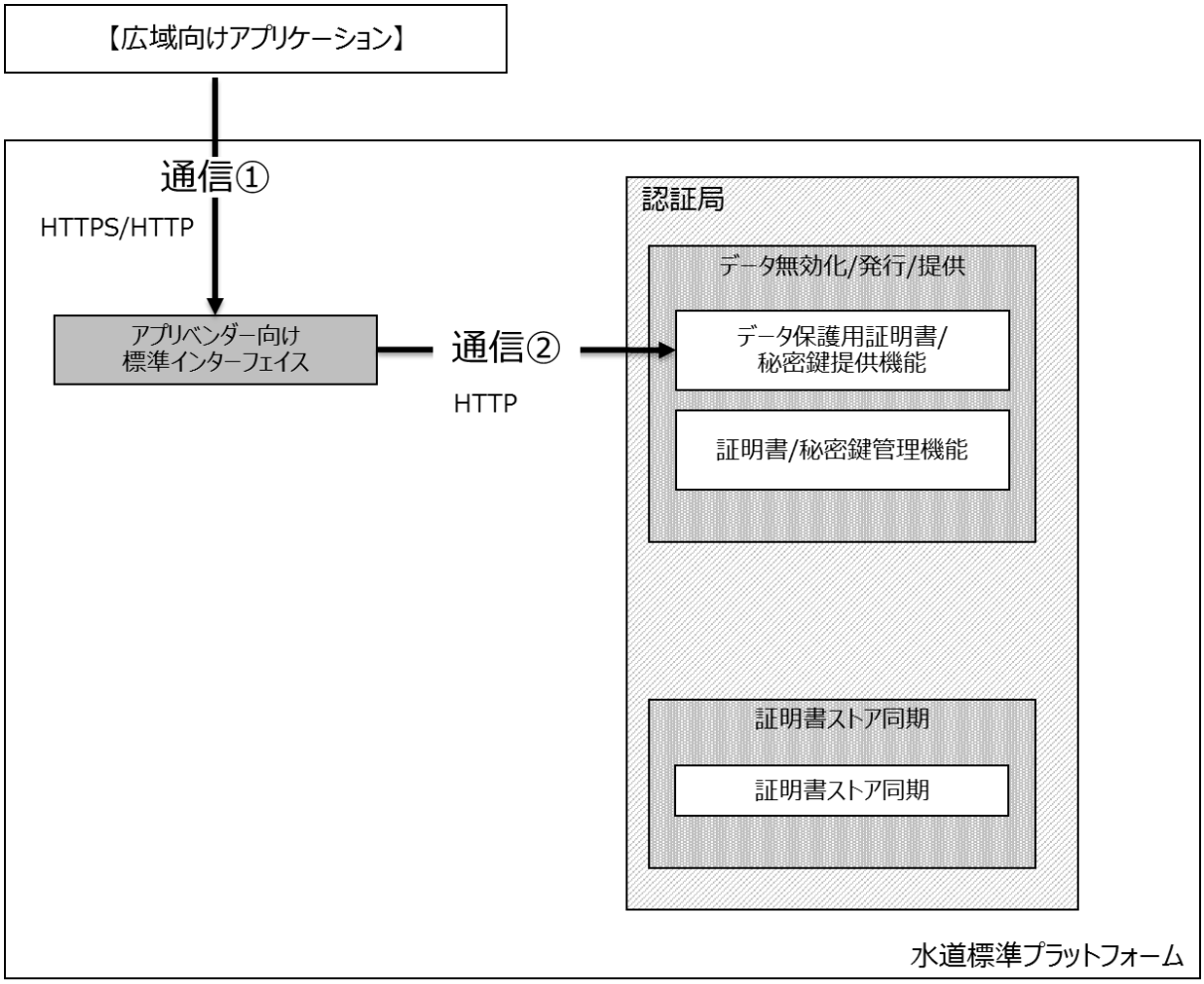


図 4-4: 広域アプリケーション向け提供経路

(c) リクエスト概要

広域アプリケーションからアプリベンダー向け標準インターフェイスを経由して認証局へ要求する際に連携する情報を以下に記載する(表 4-8、表 4-9)。

表 4-8: リクエスト概要
(通信① 広域アプリケーションからアプリベンダー向け標準インターフェイス)

項目	内容
要求コード	以下の何れかを指定する。 ・ 水道標準プラットフォーム証明書(データ保護用) ・ 水道標準プラットフォーム証明書失効リスト

表 4-9: リクエスト概要
(通信② アプリベンダー向け標準インターフェイスから認証局)

項目	内容
要求コード	以下の何れかを指定する。 ・ 水道標準プラットフォーム証明書(データ保護用) ・ 水道標準プラットフォーム証明書失効リスト

(d)　レスポンス概要

認証局からアプリベンダー向け標準インターフェイスを経由して広域アプリケーションへ応答する際に連携する情報を以下に記載する(表 4-10: レスポンス概要、表 4-11: レスポンス概要)。

表 4-10: レスポンス概要
(通信② 認証局からアプリベンダー向け標準インターフェイス)

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書データ(データ保護用) ・ 証明書失効リストデータ

表 4-11: レスポンス概要
(通信② アプリベンダー向け標準インターフェイスから広域向けアプリケーション)

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書データ(データ保護用) ・ 証明書失効リストデータ

(4)　ゲートウェイ向け 提供機能

(a)　機能概要

ゲートウェイへ、機器ベンダー向け標準インターフェイス(デバイス/システム)を経由して、以下の機能を提供する。

- 水道標準プラットフォーム証明書(データ保護用)を提供する機能
- 水道標準プラットフォーム証明書失効リストを提供する機能

(b)　提供経路

機能を提供経路する経路を以下に図示する(図 4-5)。

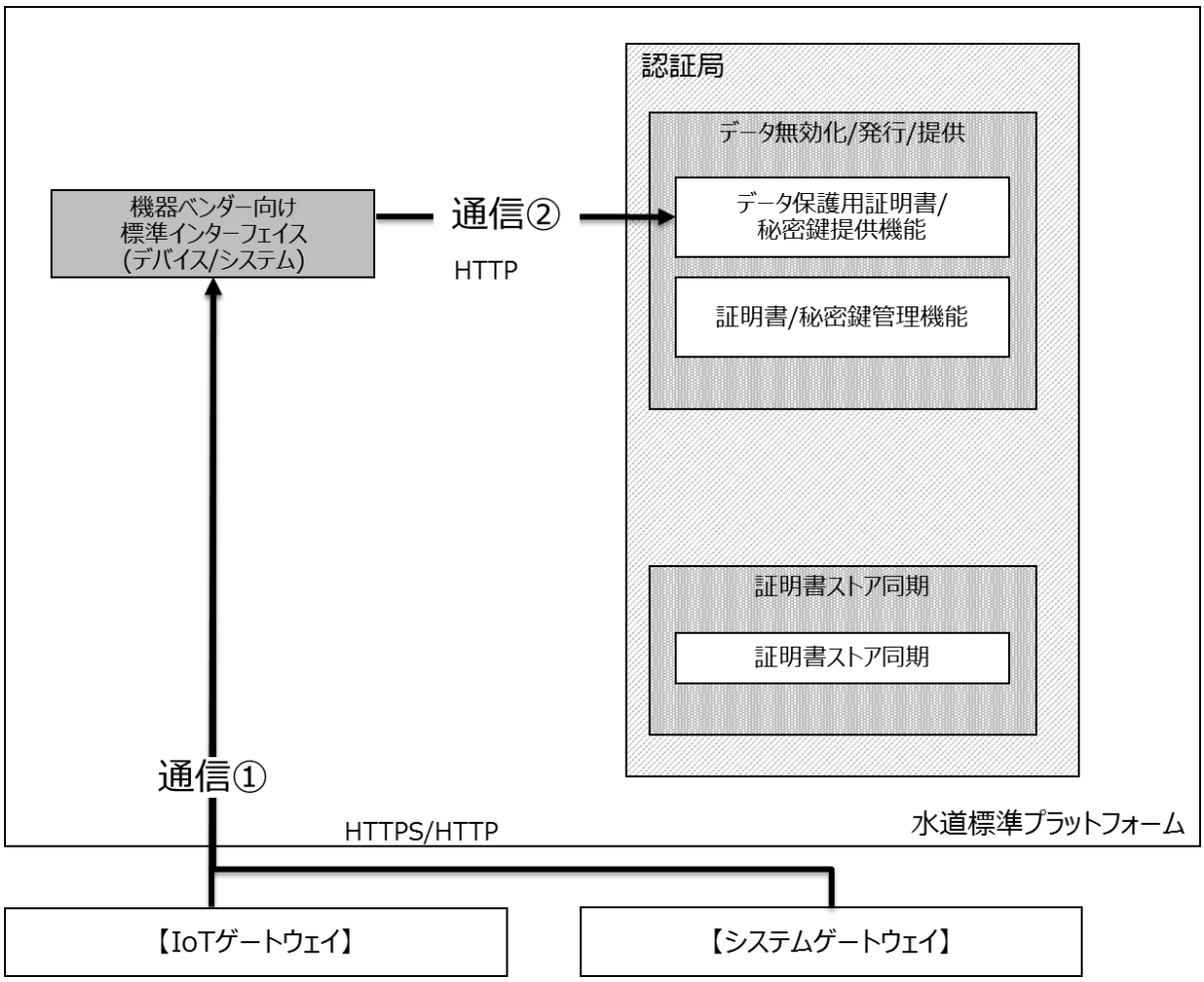


図 4-5: ゲートウェイ向け提供経路

(c) リクエスト概要

ゲートウェイから機器ベンダー向け標準インターフェイスを経由して認証局へ要求する際に連携する情報を以下に記載する(表 4-12、表 4-13)。

表 4-12: リクエスト概要
(通信① ゲートウェイから機器ベンダー向け標準インターフェイス)

項目	内容
要求コード	以下の何れかを指定する。 ・ 水道標準プラットフォーム証明書(データ保護用) ・ 水道標準プラットフォーム証明書失効リスト

表 4-13: リクエスト概要
(通信② 機器ベンダー向け標準インターフェイスから認証局)

項目	内容
要求コード	以下の何れかを指定する。 ・ 水道標準プラットフォーム証明書(データ保護用)

項目	内容
	・　水道標準プラットフォーム証明書失効リスト

(d)　レスポンス概要

認証局から機器ベンダー向け標準インターフェイスを経由してゲートウェイへ応答する際に連携する情報を以下に記載する(表 4-14: レスポンス概要, 表 4-15: レスポンス概要)。

表 4-14: レスポンス概要
(通信② 認証局から機器ベンダー向け標準インターフェイス)

項目	内容
ステータスコード	以下の何れかを指定する。 ・　200 番台(正常) ・　400 番台(異常)
証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・　証明書データ(データ保護用) ・　証明書失効リストデータ

表 4-15: レスポンス概要
(通信① 機器ベンダー向け標準インターフェイスからゲートウェイ)

項目	内容
ステータスコード	以下の何れかを指定する。 ・　200 番台(正常) ・　400 番台(異常)
証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・　証明書データ(データ保護用) ・　証明書失効リストデータ

4.2.2　証明書/秘密鍵管理機能

(1)　運用支援向け 提供機能

(a)　機能概要

運用支援へ、以下の機能を提供する。

- 広域向けアプリケーション初期登録時に証明書/秘密鍵を発行し、提供する機能
- ゲートウェイ初期登録時に証明書/秘密鍵を発行し、提供する機能
- 秘密鍵の漏洩時に新たな証明書/秘密鍵を発行し、提供する機能

(b)　提供経路

機能を提供経路する経路を以下に図示する(図 4-6)。

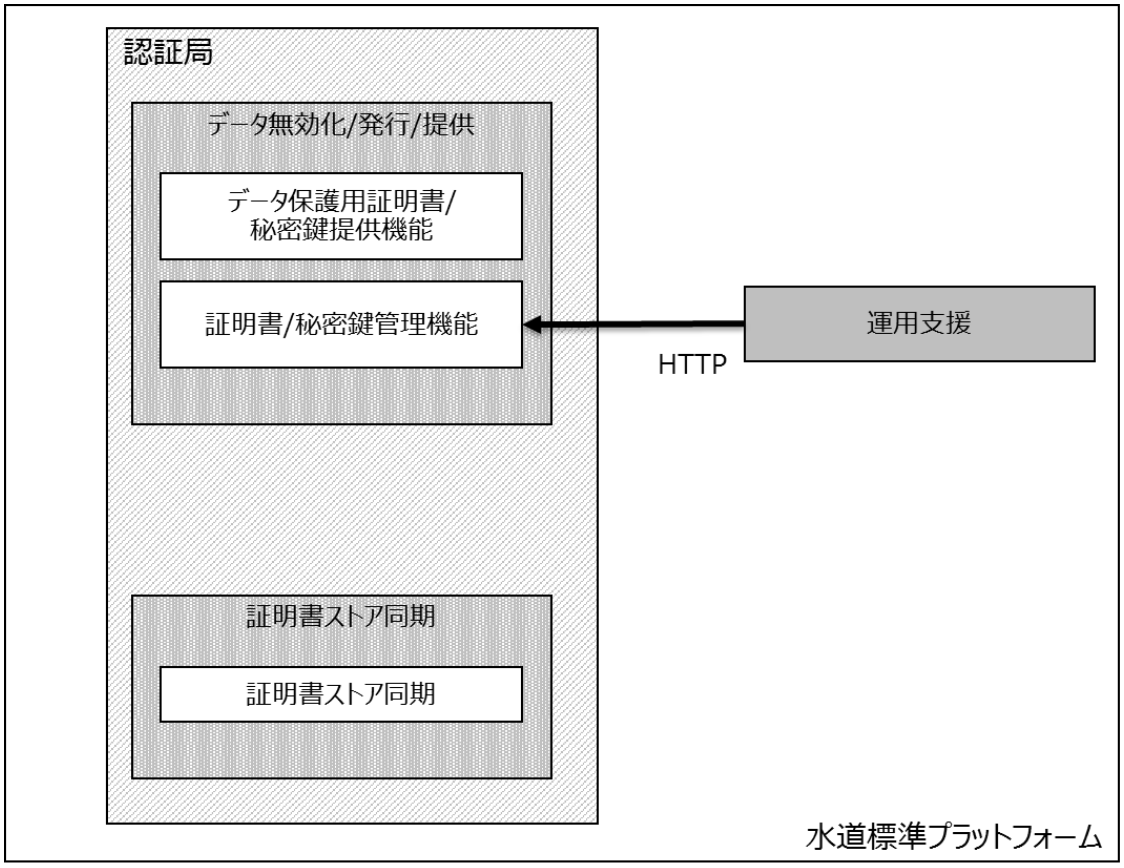


図 4-6: 運用支援向け提供経路

(c)　リクエスト概要

運用支援から認証局へ要求する際に連携する情報を以下に記載する(表 4-16)。

表 4-16: リクエスト概要

項目	内容
ID	以下の何れかを指定する。 ・　アプリケーション ID ・　ゲートウェイ ID
操作種別	以下の何れかを指定する。 ・　発行 ・　更新

(d)　レスポンス概要

認証局から運用支援へ応答する際に連携する情報を以下に記載する(表 4-17)。

表 4-17: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書 / 秘密鍵情報	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書データ(TLS 用) ・ 秘密鍵データ(TLS 用) ・ 証明書データ(データ保護用) ・ 秘密鍵データ(データ保護用)
ルート証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ ルート証明書データ ・ 証明書失効リストデータ

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 4-18)。

表 4-18: 通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	水道標準プラットフォームルート証明書/証明書失効リスト ゲートウェイ証明書/秘密鍵(TLS 用/データ保護用) アプリケーション証明書/秘密鍵(TLS 用/データ保護用)

5. データセキュリティモジュール

5.1 概要

5.1.1 機能概要

データセキュリティは、水道 CPS/IoT リファレンスモデルにおける「水道標準プラットフォーム」内の通信データの暗号化、復号、電子署名付与、電子署名検証を行う機能を提供するモジュールである。データ保護用のデータについては暗号化、複合化のみ提供をし、経路暗号化は、復号、電子署名付与、電子署名検証を HTTPS プロトコルで実現する。

5.1.2 機能一覧

データセキュリティの機能一覧を以下に示す(図 5-1、表 5-1)。

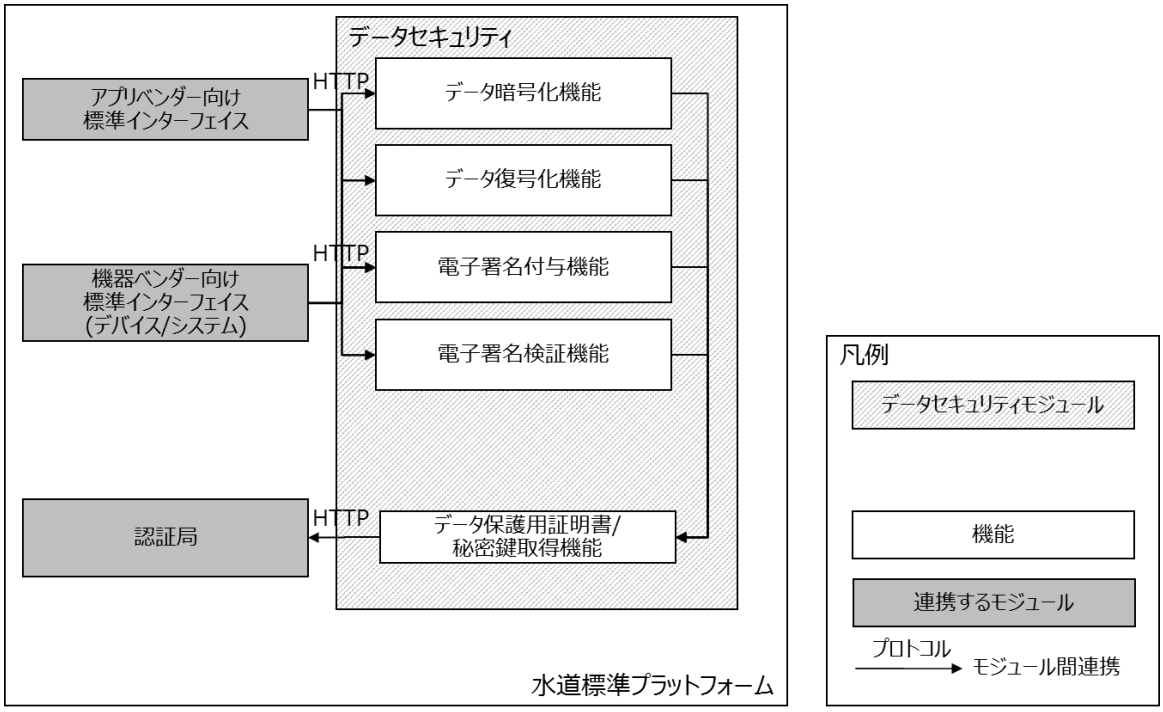


図 5-1:データセキュリティ機能構成

表 5-1: データセキュリティ機能一覧

No	機能名	説明
1	データ保護用証明書/秘密鍵取得機能	水道標準プラットフォーム内の認証局から、各種証明書、水道標準プラットフォーム秘密鍵(データ保護用)、証明書失効リストを取得する
2	データ暗号化機能	水道標準プラットフォーム内の各標準インターフェイスに対し、通信データの暗号化を実施する
3	データ復号機能	水道標準プラットフォーム内の各標準インターフェイスに対し、通信データの復号を実施する

No	機能名	説明
4	電子署名付与機能	水道標準プラットフォーム内の各標準インターフェイスに対し、通信データの電子署名を付与する
5	電子署名検証機能	水道標準プラットフォーム内の各標準インターフェイスに対し、通信データの電子署名を検証する

5.1.3 データ暗号化/復号方式

データセキュリティにおけるデータの暗号化/復号方式は、データ形式に応じた以下の方式とする。

(1) データプロファイル(JSON)形式

(a) 概要

データプロファイル(JSON)形式のデータの暗号化/復号方式は、RFC7516 準拠し以下に図示した手順で実施する(図 5-2、図 5-3)。

【送信側での暗号化処理方式】

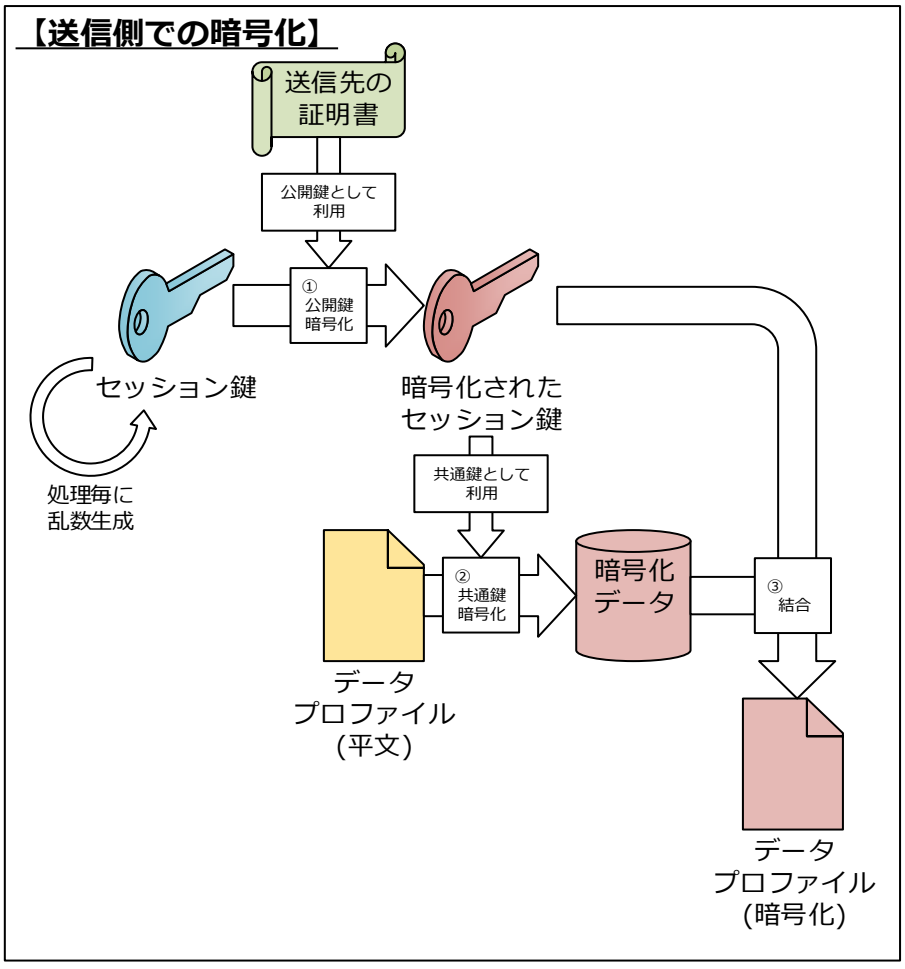


図 5-2: 送信側での暗号化処理方式

① 「送信先の証明書」を公開鍵として、処理毎に乱数生成した「セッション鍵」を公開

鍵暗号方式で暗号化し、「暗号化されたセッション鍵」を生成する。

② ①で生成した「暗号化されたセッション鍵」を共通鍵として、「データプロファイル(平文)」を共通鍵暗号方式で暗号化し、「暗号化データ」を生成する。

③ ①で生成した「暗号化されたセッション鍵」と②で生成した「暗号化データ」を結合して、「データプロファイル(暗号化)」を生成する。

【受信側での復号処理方式】

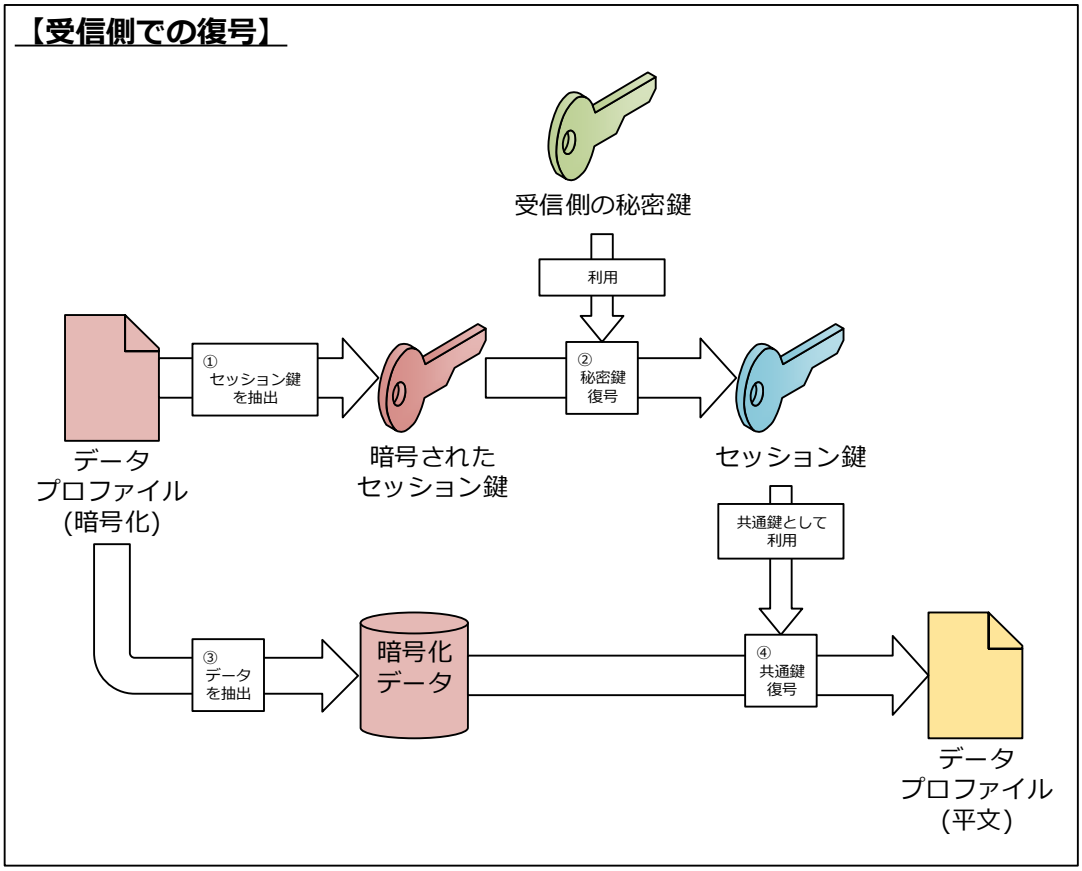


図 5-3: 受信側での復号処理方式

① 「データプロファイル(暗号化)」から「暗号化されたセッション鍵」を抽出する。

② 「受信側の秘密鍵」を利用して、①で抽出した「暗号化されたセッション鍵」を復号し、「セッション鍵」を生成する。

③ 「データプロファイル(暗号化)」から「暗号化データ」を抽出する。

④ ②で生成した「セッション鍵」を利用して、③で抽出した「暗号化データ」を復号し、「データプロファイル(平文)」を生成する。

(b) 暗号アルゴリズム

① 共通鍵暗号方式

データを暗号化/復号する暗号アルゴリズムを以下に示す(表 5-2)。

表 5-2: 共通鍵暗号方式の暗号アルゴリズム

項番	区分	方式
1	暗号アルゴリズム	AES
2	暗号モード	CBC
3	鍵長	128bit, 192bit, 256bit から選択
4	ブロック長	128bit
5	パディング	PKCS#7
6	メッセージダイジェスト	SHA-256
7	メッセージ認証コード	HMAC

② 公開鍵暗号方式

データの暗号化/復号に利用するセッション鍵を暗号化/復号する暗号アルゴリズムを以下に示す(表 5-3)。

表 5-3: 公開鍵暗号方式の暗号アルゴリズム

項番	区分	方式
1	暗号アルゴリズム	RSA
2	鍵長	2048bit
3	ブロック長	2048bit
4	パディング	OAEP

(2)　ファイル形式

(a)　概要

ファイル形式のデータの暗号化/復号方式は、以下に図示した手順で実施する(図 5-4、図 5-5)。

【送信側での暗号化処理方式】

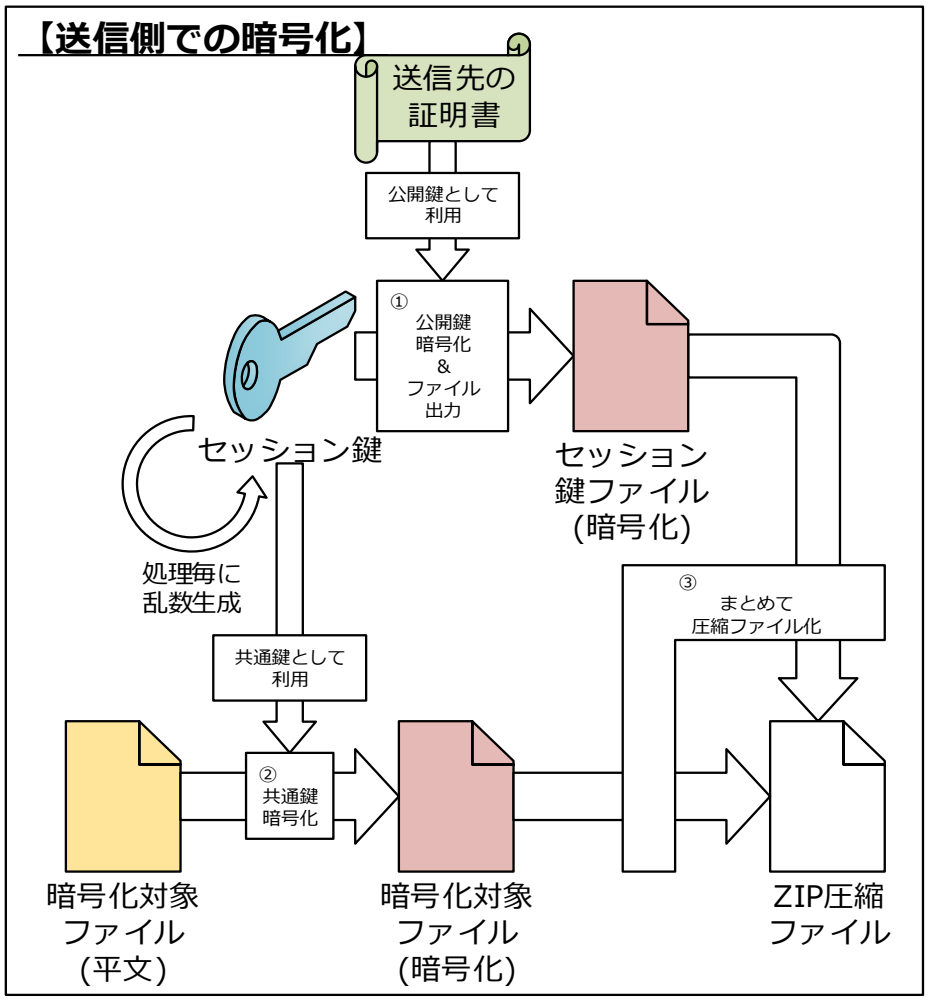


図 5-4: 送信側での暗号化処理方式

① 「送信先の証明書」を公開鍵として、処理毎に乱数生成した「セッション鍵」を公開鍵暗号方式で暗号化し、「セッション鍵ファイル(暗号化)」を生成する。

② ①で生成した「セッション鍵」を共通鍵として、「暗号化対象ファイル(平文)」を共通鍵暗号方式で暗号化し、「暗号化対象ファイル(暗号化)」を生成する。

③ ①で生成した「セッション鍵ファイル(暗号化)」と②で生成した「暗号化対象ファイル(暗号化)」をまとめて圧縮し、「ZIP 圧縮ファイル」を生成する。

【受信側での復号処理方式】

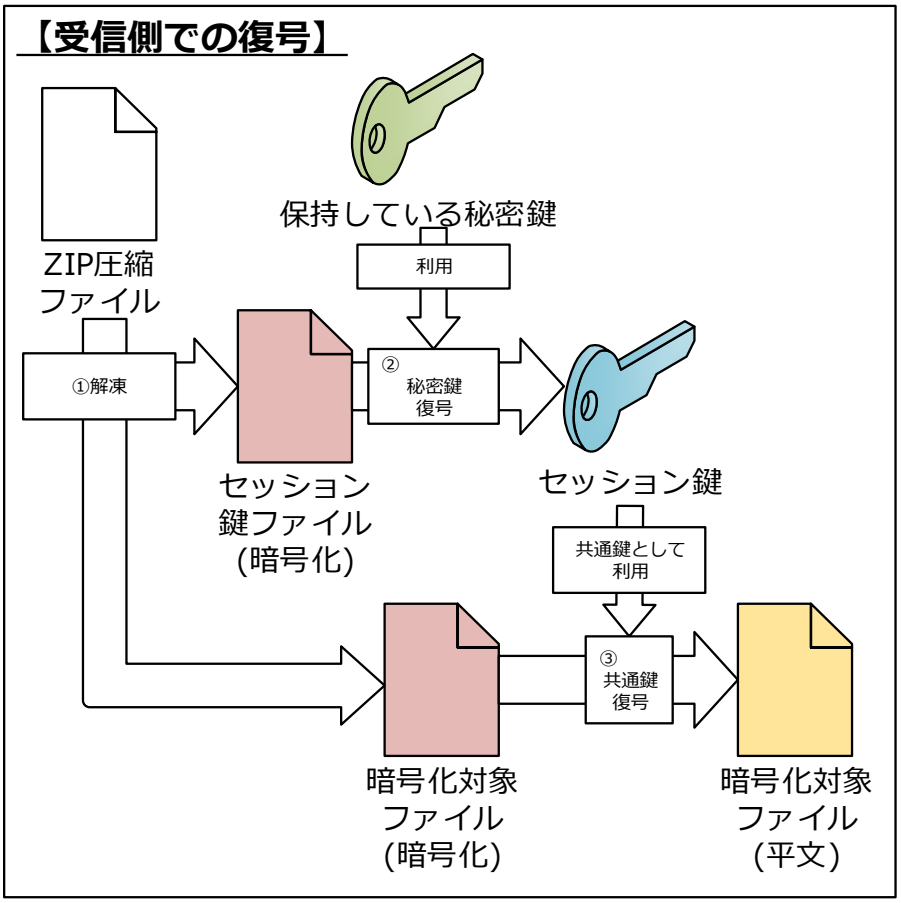


図 5-5:受信側での復号処理方式

① 「ZIP 圧縮ファイル」を解凍し、「セッション鍵ファイル(暗号化)」と「暗号化対象ファイル(暗号化)」を抽出する。

② 「保持している秘密鍵」を利用して、①で抽出した「セッション鍵ファイル(暗号化)」を復号し、「セッション鍵」を生成する。

③ ②で生成した「セッション鍵」を利用して、①で抽出した「暗号化対象ファイル(暗号化)」を復号し、「暗号化対象ファイル(平文)」を生成する。

(b) 暗号アルゴリズム

① 共通鍵暗号方式

データを暗号化/復号する暗号アルゴリズムを以下に示す(表 5-4)。

表 5-4: 共通鍵暗号方式の暗号アルゴリズム

項番	区分	方式
1	暗号アルゴリズム	AES
2	暗号モード	CBC
3	鍵長	128bit, 192bit, 256bit から選択
4	ブロック長	128bit
5	パディング	PKCS#7

② 公開鍵暗号方式

データの暗号化/復号に利用するセッション鍵を暗号化/復号する暗号アルゴリズムを以下に示す(表 5-5)。

表 5-5: 公開鍵暗号方式の暗号アルゴリズム

項番	区分	方式
1	暗号アルゴリズム	RSA
2	鍵長	2048bit
3	ブロック長	2048bit
4	パディング	OAEP

5.1.4 電子署名方式

データセキュリティにおけるデータの電子署名方式は、データ形式に応じた以下の方式とする。

(1) データプロファイル(JSON)形式

(a) 概要

データプロファイル(JSON)形式の電子署名付与/検証方式は、以下に図示した手順で実施する。(図 5-6、図 5-7)

【送信側での電子署名付与方式】

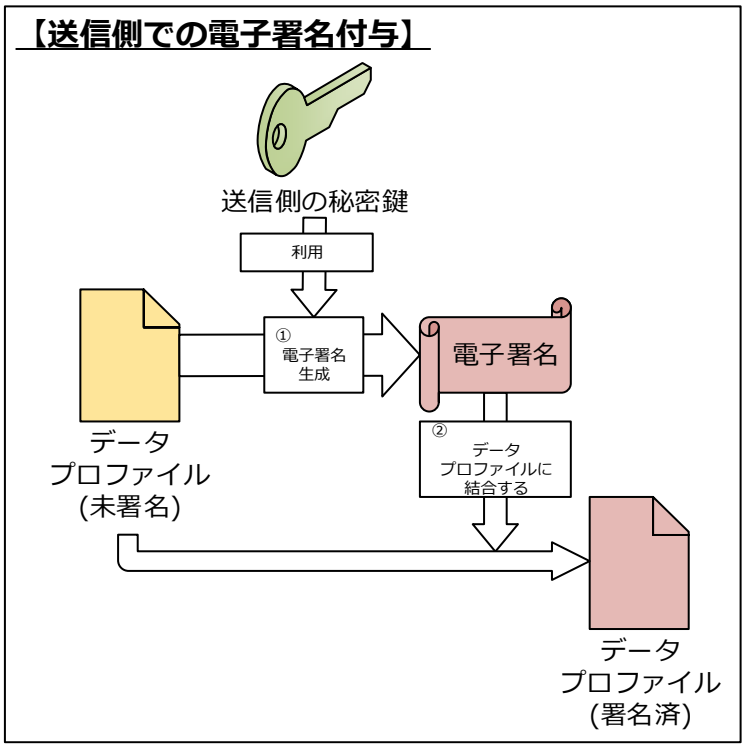


図 5-6:送信側での電子署名付与方式

① 「データプロファイル(未署名)」を参照して送信側の秘密鍵を利用して、「電子署名」を生成する。

② ①で生成した「電子署名」と「データプロファイル(未署名)」を結合し、「データプロファイル(署名済)」を生成する。

【受信側での電子署名検証方式】

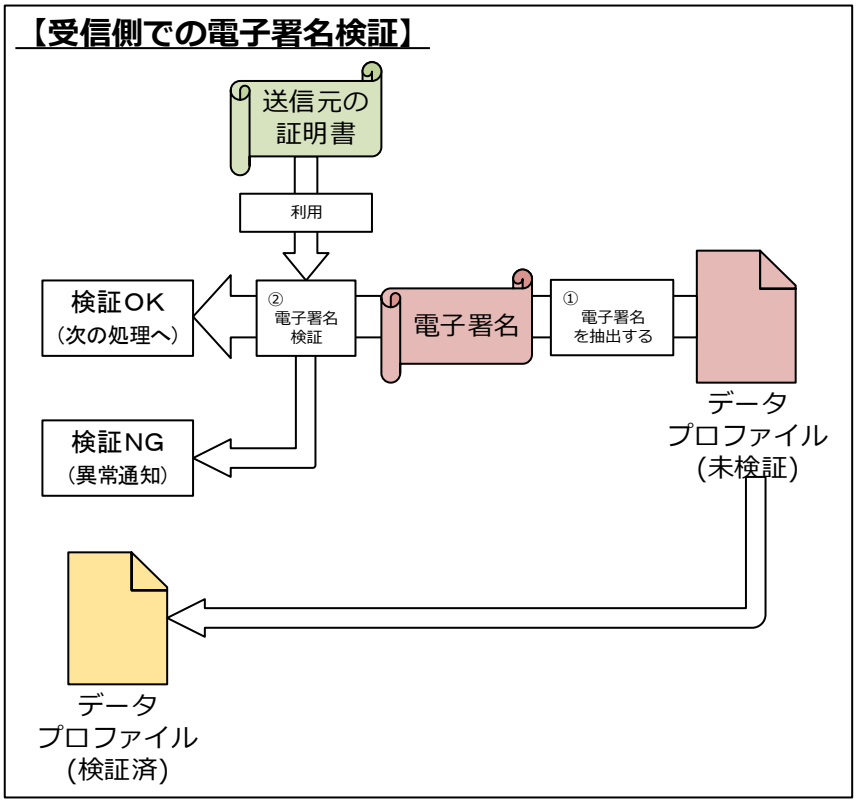


図 5-7:受信側での電子署名検証方式

① 「データプロファイル(未検証)」から「電子署名」を抽出する。

② 「送信元の証明書」を利用して、「電子署名」を検証し、OK であれば次の処理を実行する。(検証 NG の場合は、異常を通知する。)

(b) 電子署名アルゴリズム

電子署名付与/検証に利用する電子署名アルゴリズムを以下に示す(表 5-6)。

表 5-6: 電子署名アルゴリズム

項番	区分	方式
1	結合方法	JWS Compact Serialization
2	署名	RSASSA-PKCS1-v1_5
3	メッセージダイジェスト	SHA-256
4	メッセージ認証コード	HMAC

(2) ファイル形式

(a) 概要

ファイル形式の電子署名付与/検証方式は、以下に図示した手順で実施する。(図 5-8、図 5-9)

【送信側での電子署名付与方式】

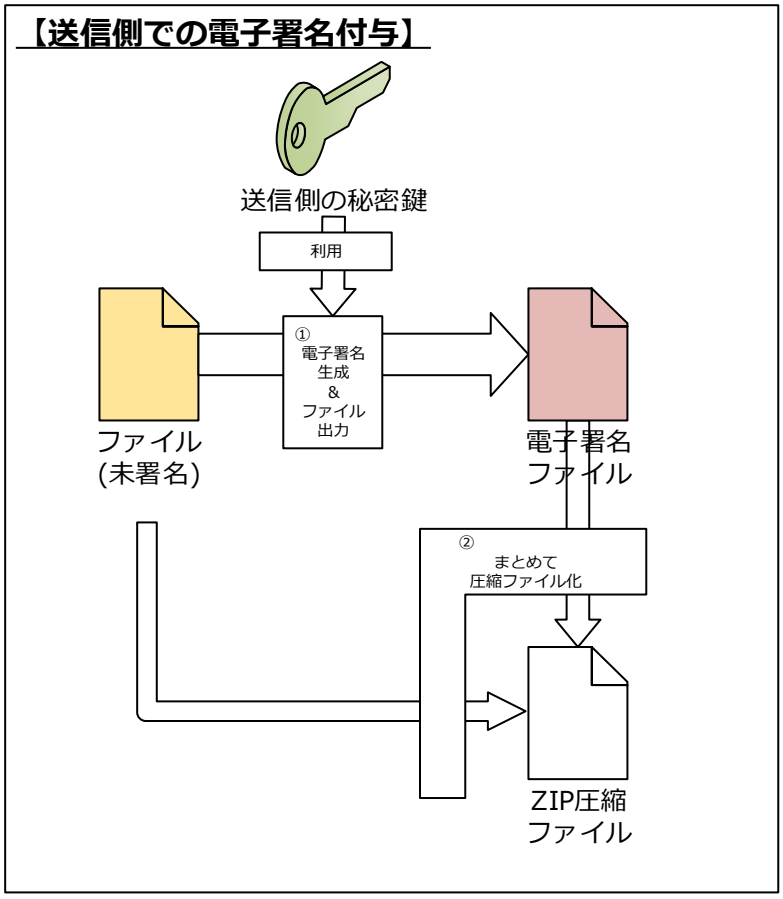


図 5-8:送信側での電子署名付与方式

① 「ファイル(未署名)」を参照し、送信側の秘密鍵を利用して「電子署名ファイル」を生成、ファイル出力する。

② ①で生成した「電子署名ファイル」と「データプロファイル(未署名)」をまとめて圧縮し、「ZIP 圧縮ファイル」を生成する。

【受信側での電子署名検証方式】

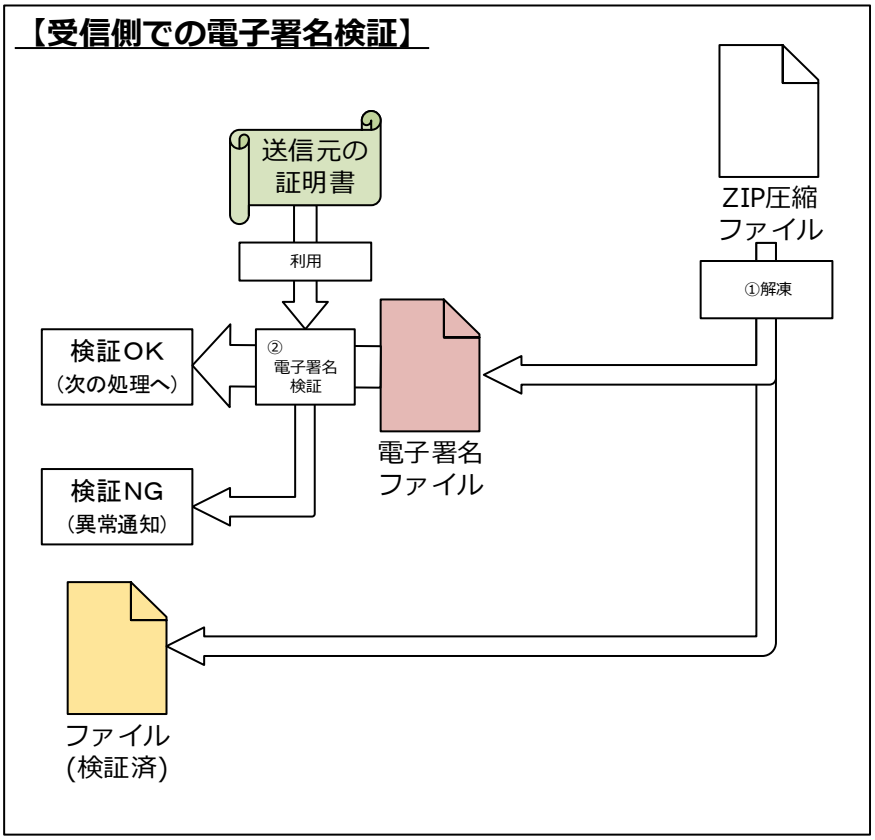


図 5-9:受信側での電子署名検証方式

① 「ZIP 圧縮ファイル」を解凍し、「電子署名ファイル」 を抽出する。
② 「送信元の証明書」を利用して、①で抽出した「電子署名ファイル」を検証し、検証 OK であれば次の処理を実行する。(検証 NG の場合は、異常を通知する。)

(b) 電子署名アルゴリズム

電子署名付与/検証に利用する電子署名アルゴリズムを以下に示す(表 5-7)。

表 5-7: 電子署名アルゴリズム

項番	区分	方式
1	署名	RSASSA-PKCS1-v1_5
2	メッセージダイジェスト	SHA-256
3	メッセージ認証コード	HMAC

5.2 機能要件

5.2.1 データ保護用証明書/秘密鍵取得機能

(1) 認証局向け提供機能

(a) 機能概要

認証局からデータを取得する機能を提供する。

- アプリケーション証明書(データ保護用)を取得する機能
- ゲートウェイ証明書(データ保護用)を取得する機能
- 水道標準プラットフォーム秘密鍵(データ保護用)を取得する機能
- ルート証明書と証明書失効リストを取得する機能

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 5-10)。

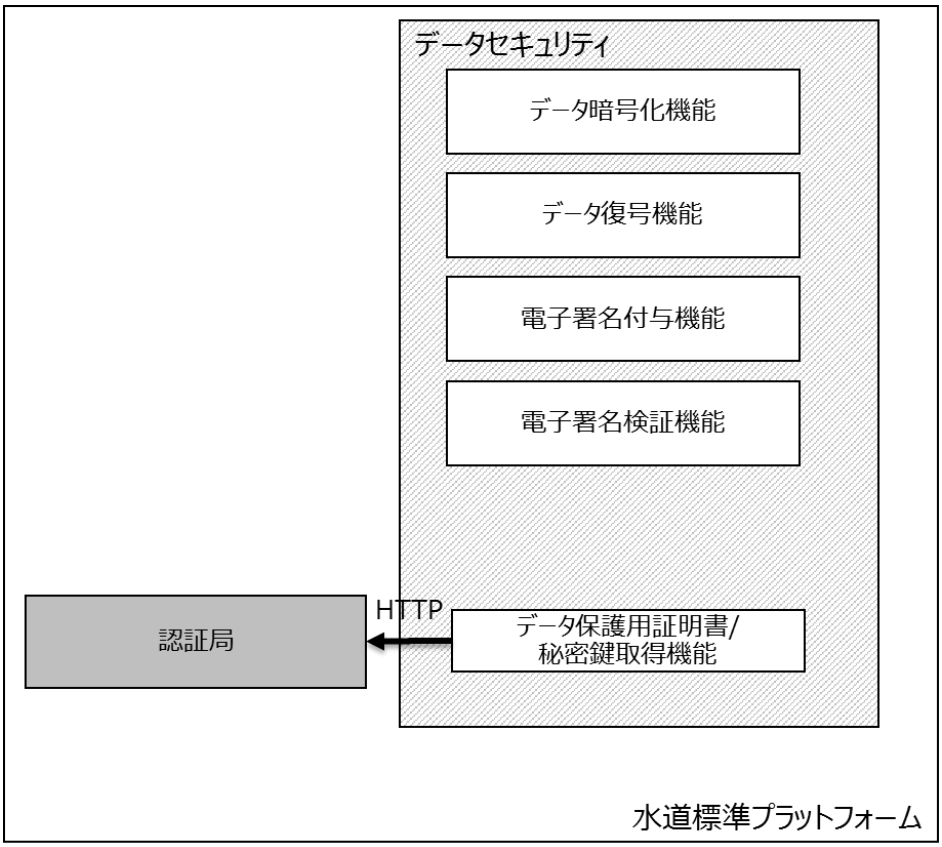


図 5-10 データ保護用証明書/秘密鍵提供機能の提供経路

(c) リクエスト概要

データセキュリティから認証局へ要求する際に連携する情報を以下に記載する(表 5-8)。

表 5-8: リクエスト概要

項目	内容
ID	以下の何れかを指定する。 ・ アプリケーション ID ・ ゲートウェイ ID ・ 水道標準プラットフォーム ID(「0000」を指定)
要求コード	以下の何れかを指定する。 ・ 証明書 ・ 秘密鍵(ID が「0000」の場合のみ指定可能)

(d) レスポンス概要

認証局からデータセキュリティへ応答する際に連携する情報を以下に記載する(表 5-9)。

表 5-9: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
証明書 / 秘密鍵情報	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ 証明書データ ・ 秘密鍵データ
ルート証明書 / 証明書失効リスト	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ ルート証明書データ ・ 証明書失効リストデータ

(e) 通信プロトコルと取得するデータ

通信プロトコルと取得するデータについて、以下の通り(表 5-10)。

表 5-10:通信プロトコルと取得するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	水道標準プラットフォームルート証明書 / 証明書失効リスト 水道標準プラットフォーム秘密鍵（データ保護用） ゲートウェイ証明書（データ保護用） アプリケーション証明書（データ保護用）

5.2.2 データ暗号化機能

(1) 標準インターフェイス向け提供機能

(a) 機能概要

標準インターフェイスへ、通信データの暗号化を実施する機能を提供する。
対象標準インターフェイスは以下の通り。

- アプリベンダー向け標準インターフェイス
- 機器ベンダー向け標準インターフェイス（デバイス）
- 機器ベンダー向け標準インターフェイス（システム）

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 5-11)。

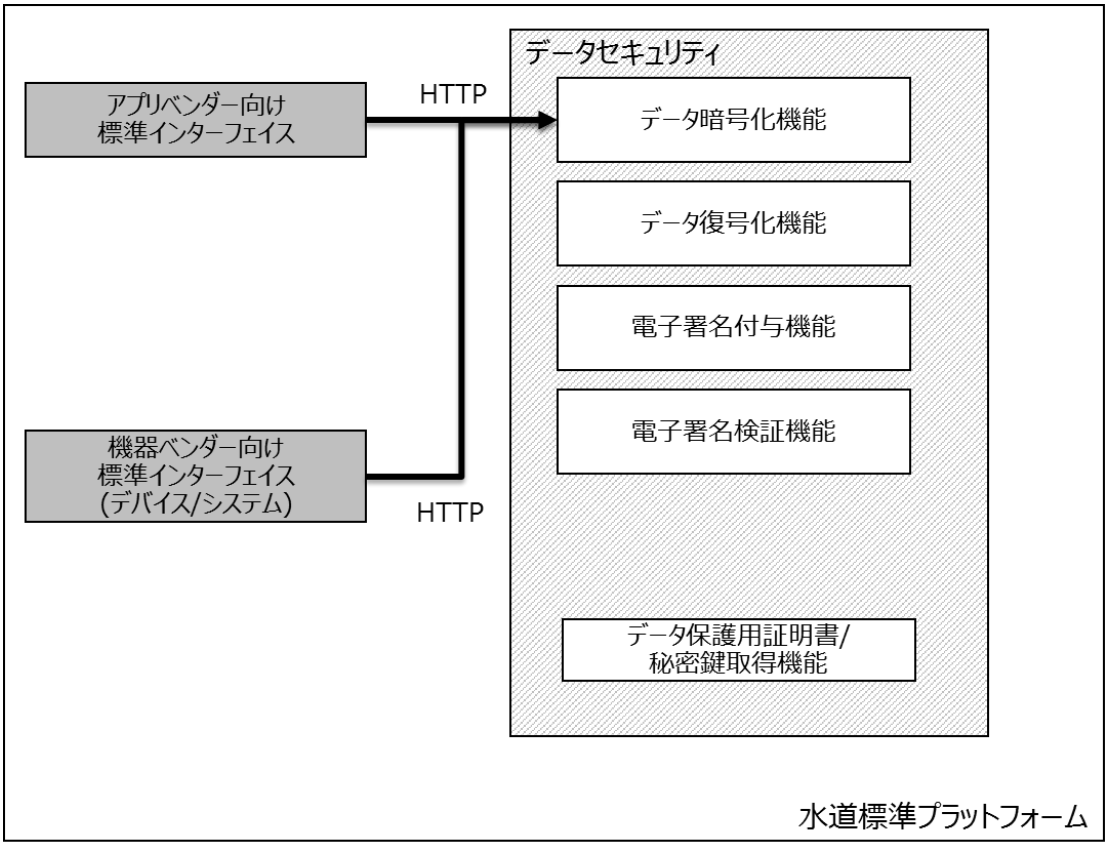


図 5-11 データ暗号化機能の提供経路

(c) リクエスト概要

標準インターフェイスからデータセキュリティへ、要求する際に連携する情報を以下に記載する(表 5-11)。

表 5-11: リクエスト概要

項目	内容
送付先 ID	以下の何れかを指定する。 ・ アプリベンダー向け標準インターフェイスの場合 アプリケーション ID ・ 機器ベンダー向け標準インターフェイスの場合 ゲートウェイ ID
データ形式	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式
暗号化対象データ	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式(複数ファイル可)

(d) レスポンス概要

データセキュリティから標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 5-12)。

表 5-12: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
暗号化データ	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ データプロファイル(JSON 形式)(暗号化済) ・ ファイル形式(暗号化済)

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 5-13)。

表 5-13:通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	データプロファイル(JSON)形式データ(暗号化済) ファイル形式データ(暗号化済)

5.2.3 データ復号機能

(1) 標準インターフェイス向け提供機能

(a) 機能概要

標準インターフェイスへ、通信データの復号を実施する機能を提供する。

対象標準インターフェイスは以下の通り。

- アプリベンダー向け標準インターフェイス
- 機器ベンダー向け標準インターフェイス（デバイス）
- 機器ベンダー向け標準インターフェイス（システム）

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 5-12)。

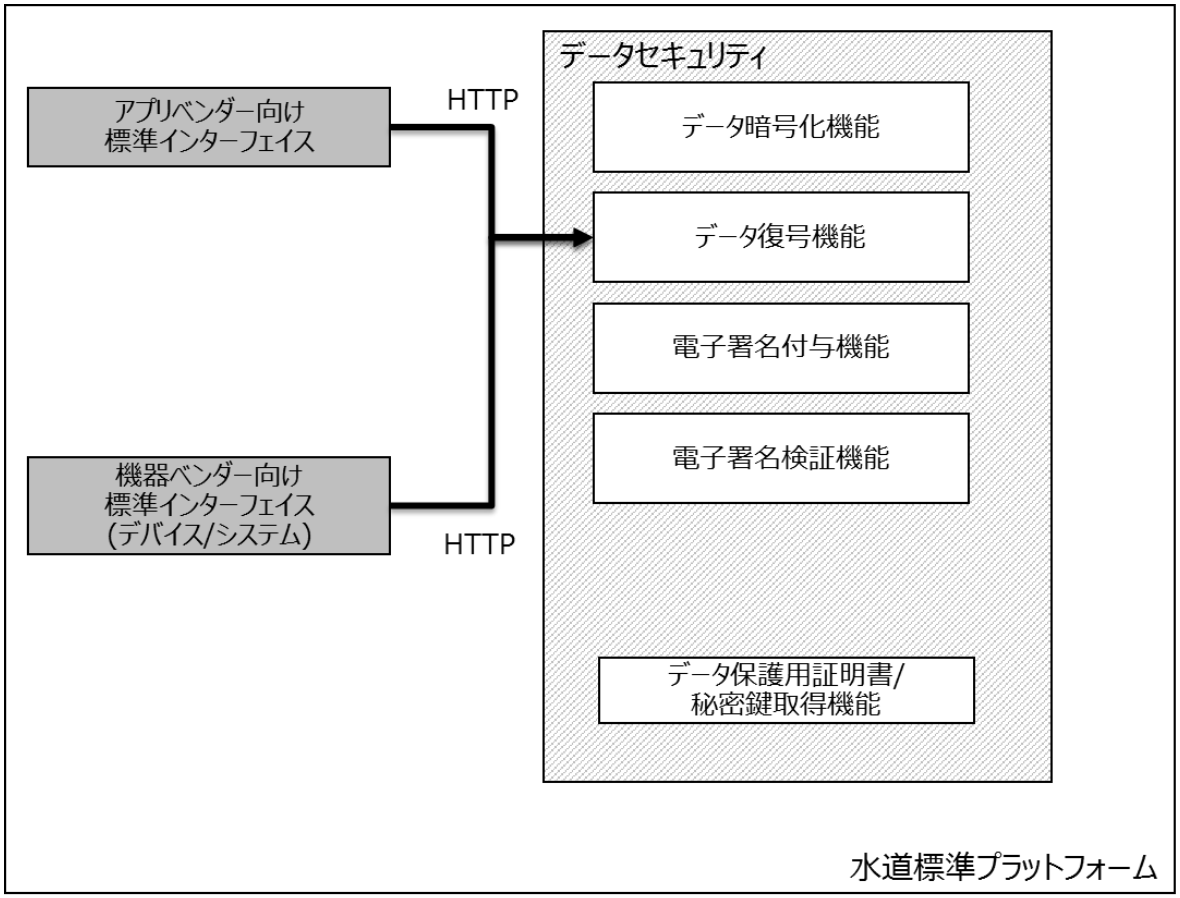


図 5-12: データ復号機能の提供経路

(c) リクエスト概要

標準インターフェイスからデータセキュリティへ、要求する際に連携する情報を以下に記載する(表 5-14)。

表 5-14: リクエスト概要

項目	内容
送付先 ID	以下の何れかを指定する。 ・ アプリベンダー向け標準インターフェイスの場合 アプリケーション ID ・ 機器ベンダー向け標準インターフェイスの場合 ゲートウェイ ID
データ形式	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式
暗号化データ	以下の何れかを指定する。 ・ データプロファイル(JSON 形式)(暗号化済) ・ ファイル形式(暗号化済)

(d) レスポンス概要

データセキュリティから標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 5-15)。

表 5-15: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
暗号化データ	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ データプロファイル(JSON 形式) ・ ファイル形式(複数ファイル可)

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 5-16)。

表 5-16: 通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	データプロファイル(JSON)形式データ ファイル形式データ(複数ファイル可)

5.2.4 電子署名付与機能

(1) 標準インターフェイス向け提供機能

(a) 機能概要

標準インターフェイスへ、通信データの電子署名を付与する機能を提供する。
対象標準インターフェイスは以下の通り。

- アプリベンダー向け標準インターフェイス
- 機器ベンダー向け標準インターフェイス（デバイス）
- 機器ベンダー向け標準インターフェイス（システム）

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 5-13)。

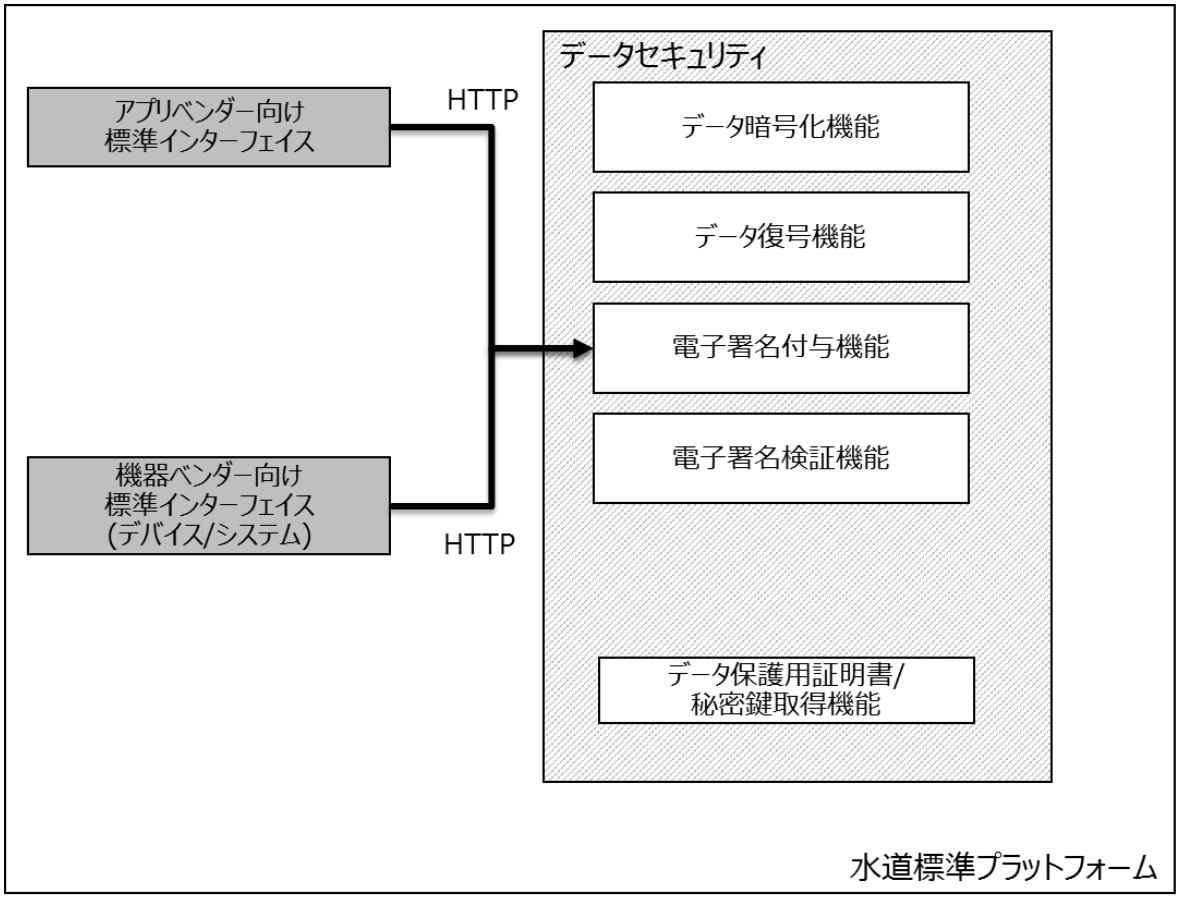


図 5-13: 電子署名付与機能の提供経路

(c) リクエスト概要

標準インターフェイスからデータセキュリティへ、要求する際に連携する情報を以下に記載する(表 5-17)。

表 5-17: リクエスト概要

項目	内容
送付先 ID	以下の何れかを指定する。 ・ アプリベンダー向け標準インターフェイスの場合 アプリケーション ID ・ 機器ベンダー向け標準インターフェイスの場合 ゲートウェイ ID
データ形式	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式
電子署名データ	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式(複数ファイル可)

(d) レスポンス概要

データセキュリティから標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 5-18)。

表 5-18: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
暗号化データ	以下の何れかを指定する。 (ステータスコードが「200 番台」の場合のみ) ・ データプロファイル(JSON 形式)(電子署名済) ・ ファイル形式(電子署名済)

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 5-19)

表 5-19:通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	データプロファイル(JSON)形式データ(電子署名済) 電子署名ファイル

5.2.5 電子署名検証機能

(1) 標準インターフェイス向け提供機能

(a) 機能概要

標準インターフェイスへ、通信データの電子署名を検証する機能を提供する。

対象標準インターフェイスは以下の通り。

- アプリベンダー向け標準インターフェイス
- 機器ベンダー向け標準インターフェイス（デバイス）
- 機器ベンダー向け標準インターフェイス（システム）

(b) 提供経路

機能を提供経路する経路を以下に図示する(図 5-14)。

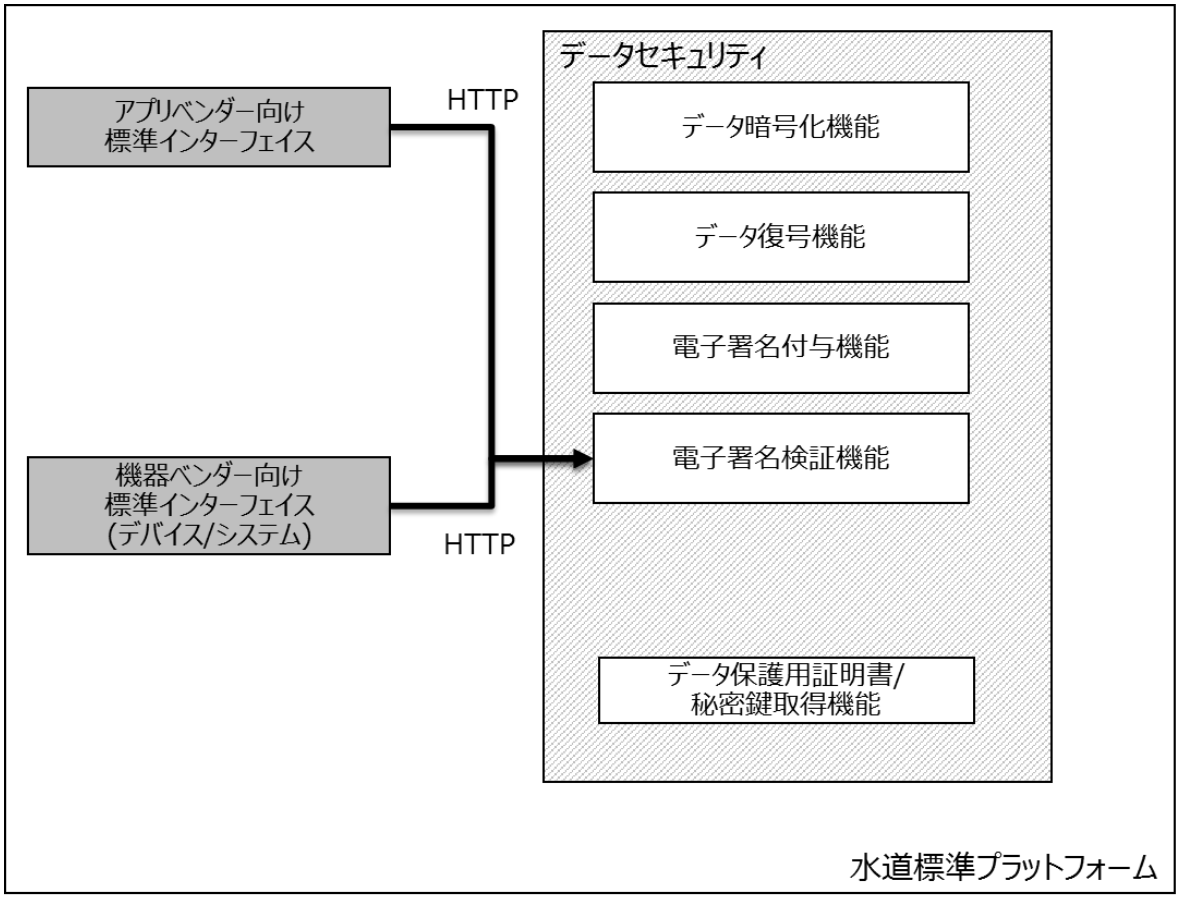


図 5-14: 電子署名検証機能の提供経路

(c) リクエスト概要

標準インターフェイスからデータセキュリティへ、要求する際に連携する情報を以下に記載する(表 5-20)。

表 5-20: リクエスト概要

項目	内容
送付先 ID	以下の何れかを指定する。 ・ アプリベンダー向け標準インターフェイスの場合 アプリケーション ID ・ 機器ベンダー向け標準インターフェイスの場合 ゲートウェイ ID
データ形式	以下の何れかを指定する。 ・ データプロファイル(JSON 形式) ・ ファイル形式
暗号化データ	以下の何れかを指定する。 ・ データプロファイル(JSON 形式)(電子署名済) ・ ファイル形式(電子署名済)

(d) レスポンス概要

データセキュリティから標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 5-21)。

表 5-21: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)

(e) 通信プロトコルと提供データ

通信プロトコルと提供するデータについて、以下の通り(表 5-22)。

表 5-22: 通信プロトコルと提供するデータ

通信プロトコル	提供するデータ
HTTP を利用した REST 通信	電子署名検証結果

6. データ蓄積モジュール

6.1 概要

6.1.1 機能概要

本モジュールでは、「機器ベンダー向け標準インターフェイス(デバイス)」、「機器ベンダー向け標準インターフェイス(システム)」及び「アプリベンダー向け標準インターフェイス」より、連携されたデータを、水道標準プラットフォーム内部データベースにて蓄積管理を行う。

また、蓄積管理されたデータを「アプリベンダー向け標準インターフェイス」よりデータ抽出要求を受け取り、要求情報に合致したデータを抽出し、返却する。

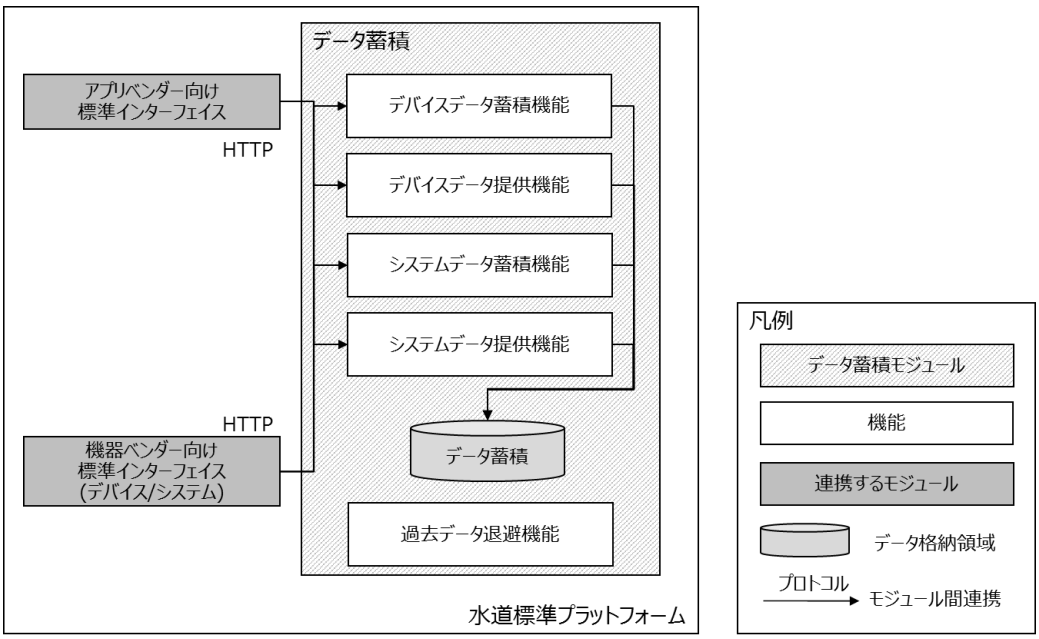


図 6-1: データ蓄積概要

6.1.2 各データの保持方針

「機器ベンダー向け標準インターフェイス(デバイス)」より連携されるデータは、発生データ量が多大であるため、蓄積データは一定期間のみを保持とし、古いデータから順次削除する。但し、削除対象のデータは、削除前に対象データをファイルに退避しておくものとする。

6.1.3 データ蓄積方式

ゲートウェイから水道標準プラットフォームへのデータ蓄積について、データ蓄積方式を以下に記載する。水道標準プラットフォームとしては、下記全ての蓄積方式を実装する事とし、要件に沿って選択できるようにする。

(1)　随時データ取得方式

(a)　処理フロー

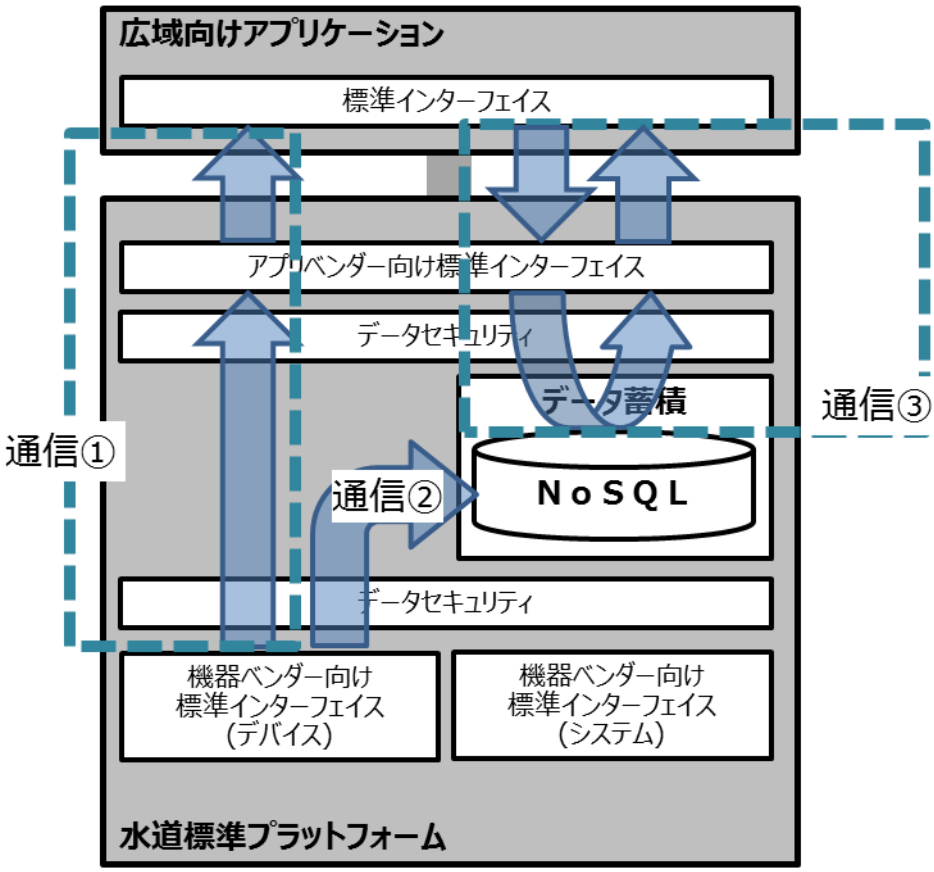


図 6-2:処理フロー 随時データ取得方式

- (図 6-2 通信①)広域向けアプリケーションからの定周期監視等により、ゲートウェイからデータを定期的に広域向けアプリケーションへ送信する。
- (図 6-2 通信②)水道標準プラットフォーム内において、広域向けアプリケーションへの送達と同時に並行してデータを蓄積する。
- (図 6-2 通信③)過去データを取得する際は、広域向けアプリケーションから水道標準プラットフォームに取得要求を送り、水道標準プラットフォーム内に蓄積されているデータを取得する。

(2)　一括データ取得方式

(a)　処理フロー

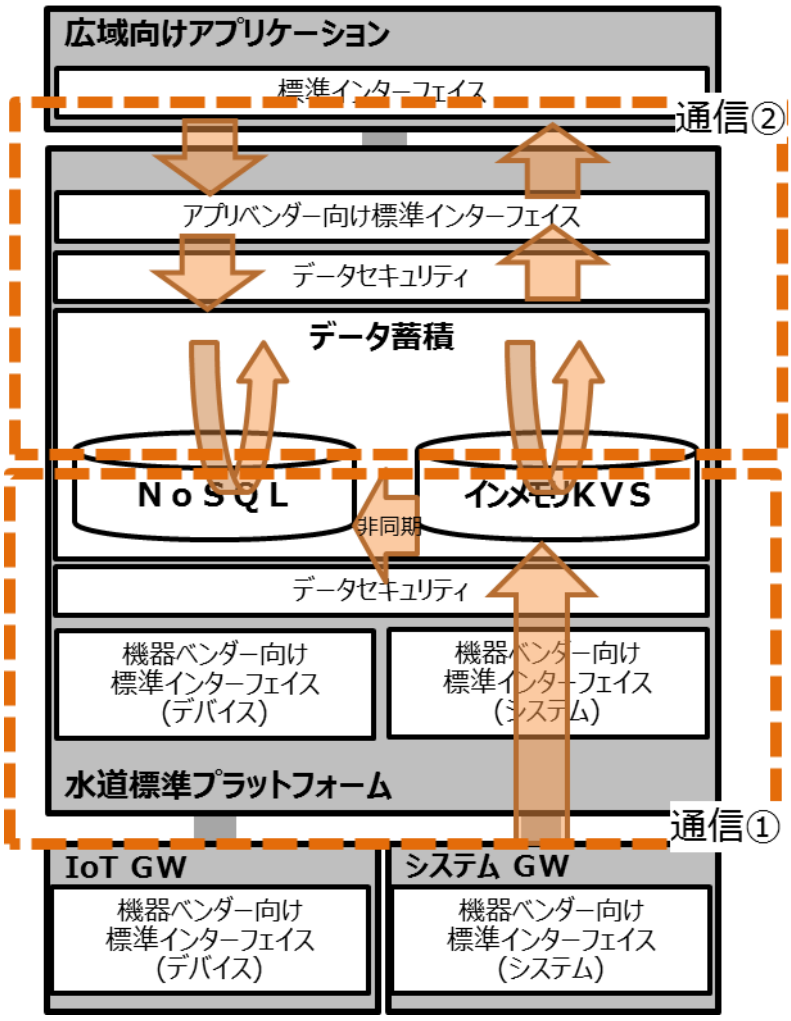


図 6-3:処理フロー 一括データ取得方式

- (図 6-3 通信①)ゲートウェイからデータを定期的に水道標準プラットフォームへ送信し、水道標準プラットフォーム内でデータを蓄積する。
- (図 6-3 通信②)データを取得する際は、広域向けアプリケーションから水道標準プラットフォームに取得要求を送り、水道標準プラットフォーム内に蓄積されているデータを取得する。

6.1.4 データ蓄積方式の選択

業務要件により、データ蓄積方式を選択する必要がある。以下に、ユースケースを記載する。

(1) 随時データ取得方式を採用するケース

以下のような特性がある場合、随時データ取得方式が適している。

- リアルタイムにゲートウェイから伝送されたデータを広域向けアプリケーションで受け取りたい場合
- 必要なデータ以外、蓄積する必要はない場合

具体的な例としては、リアルタイムな機器の計測値監視や状態監視(ポンプ監視や流量監視など)が想定される。

(2) 一括データ取得方式を採用するケース

以下のような特性がある場合、一括データ取得方式が適している。

- ゲートウェイが取得するデータは全て蓄積する場合
- ゲートウェイから広域向けアプリケーションへのデータ伝送にリアルタイム性を求められない場合

具体的な例としては、既存システムからのデータ伝送(台帳システムからのデータ伝送など)が想定される。

6.1.5 機能一覧

データ蓄積の機能一覧を以下に示す(表 6-1)。

表 6-1: データ蓄積機能一覧

No	機能名	説明
1	デバイスデータ蓄積/提供	デバイスデータの蓄積 及び、外部モジュールへの提供を行う。
2	システムデータ蓄積/提供	システムデータの蓄積 及び、外部モジュールへの提供を行う。
3	過去データ退避	定周期監視データの過去データの追い出しを行う。

6.2 機能要件

6.2.1 データ蓄積機能

デバイスデータ及びシステムデータの蓄積を実施する。

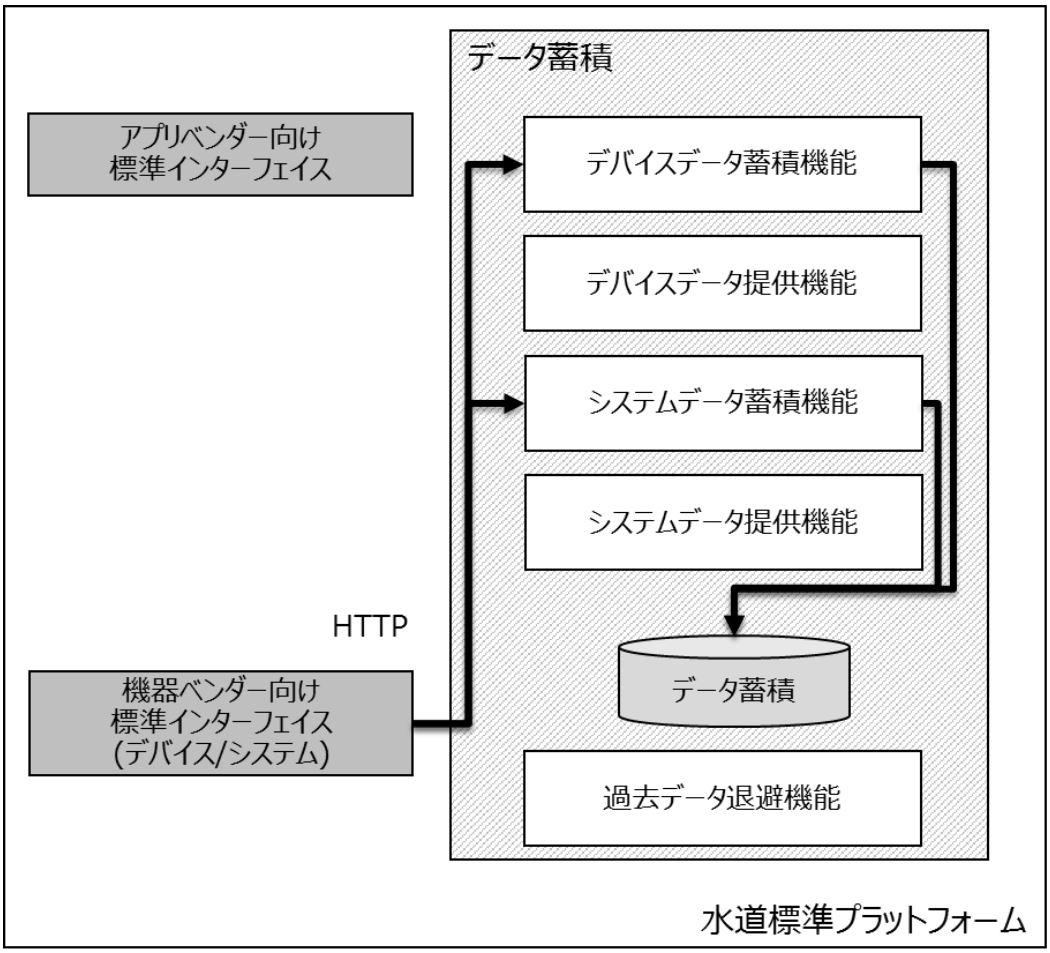


図 6-4: データ蓄積機能概要

(1) デバイスデータ蓄積

「機器ベンダー向け標準インターフェイス(デバイス)」より連携されたデータを蓄積データ(監視)データベースに格納する。

(a) リクエスト概要

機器ベンダー向け標準インターフェイスからデータ蓄積へ要求する際に連携する情報を以下に記載する(表 6-2)。

表 6-2: リクエスト概要

項目	内容
蓄積種別	以下のいずれかを設定。 ・ 通過データ蓄積方式(方式 A) : "01"

項目	内容
	・　随時データ蓄積方式(方式 B) : "02"
事業体 ID	事業体 ID を指定する
蓄積データ	-

(b)　レスポンス概要

データ蓄積から機器ベンダー向け標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 6-3)。

表 6-3: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・　200 番台(正常) ・　400 番台(異常)

(2)　システムデータ蓄積

「機器ベンダー向け標準インターフェイス(システム)」より連携されたデータを蓄積データ(システム)データベースに格納する。

(a)　リクエスト概要

機器ベンダー向け標準インターフェイスからデータ蓄積へ要求する際に連携する情報を以下に記載する(表 6-4)。

表 6-4: リクエスト概要

項目	内容
蓄積種別	以下のいずれかを設定。 ・　通過データ蓄積方式(方式 A) : "01" ・　随時データ蓄積方式(方式 B) : "02"
事業体 ID	事業体 ID を指定する
蓄積データ	-

(b)　レスポンス概要

データ蓄積から機器ベンダー向け標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 6-5)。

表 6-5: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・　200 番台(正常) ・　400 番台(異常)

6.2.2 データ提供機能

定周期監視データ及びシステムデータの提供を実施する。

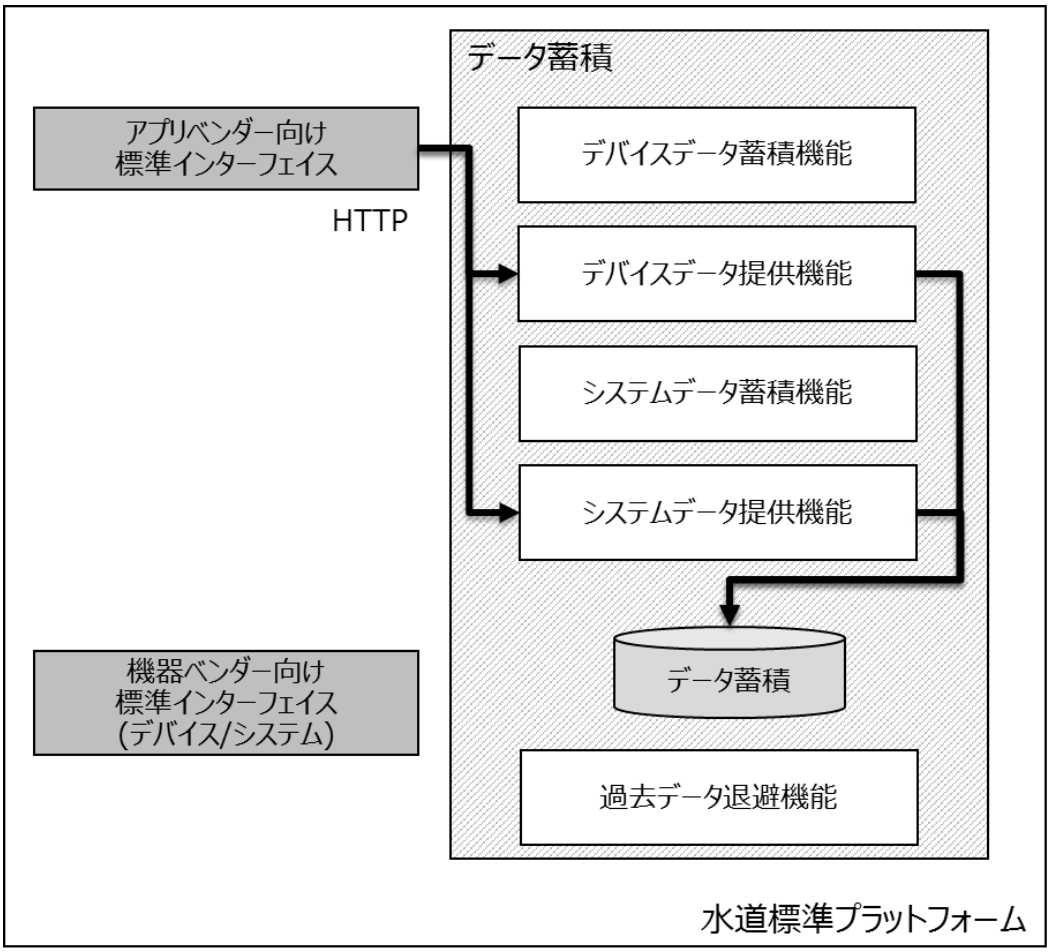


図 6-5: データ提供機能概要

(1) デバイスデータ提供

「アプリベンダー向け標準インターフェイス」よりデバイスデータ取得要求を受け付け、要求で指定された条件に合致するデータを蓄積データ(デバイス)のデータベースより検索し、検索結果を「アプリベンダー向け標準インターフェイス」に返却する。

(a) リクエスト概要

機器ベンダー向け標準インターフェイスからデータ蓄積へ要求する際に連携する情報を以下に記載する(表 6-6)。

表 6-6: リクエスト概要

項目	内容
事業体 ID	事業体 ID を指定する
抽出条件	抽出したいデータの条件を記載する。

項目		内容
	データ取得開始時刻	抽出開始時間
	データ取得終了時刻	抽出終了時間
	施設ＩＤ	施設ＩＤを指定
	設備ＩＤ	設備ＩＤを指定
	機器ＩＤ	機器ＩＤを指定
	計測値区分コード	計測値区分コードに紐づく計測項目番号コレクション
	計測項目番号	計測項目番号に紐づく実績データ

(b)　レスポンス概要

データ蓄積から機器ベンダー向け標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 6-7)。

表 6-7: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200 番台(正常) ・ 400 番台(異常)
抽出データ	入力した条件によって、抽出されたデータ。

(2)　システムデータ提供

「アプリベンダー向け標準インターフェイス(システム)」よりシステムデータ取得要求を受け付け、要求で指定された条件に合致するデータを蓄積データ(システム)のデータベースより検索し、検索結果を「アプリベンダー向け標準インターフェイス」に返却する

(a)　リクエスト概要

機器ベンダー向け標準インターフェイスからデータ蓄積へ要求する際に連携する情報を以下に記載する(表 6-8)。

表 6-8: リクエスト概要

項目		内容
抽出条件		抽出したいデータの条件を記載する。
	データ取得開始時刻	抽出開始時間
	データ取得終了時刻	抽出終了時間
	システムＩＤ	システムＩＤを指定
	業務ＩＤ	業務ＩＤを指定
	項目ＩＤ	項目ＩＤを指定
	データ行番号	データ行番号を指定

(b)　レスポンス概要

データ蓄積から機器ベンダー向け標準インターフェイスへ応答する際に連携する情報を以下に記載する(表 6-9)。

表 6-9: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・　200 番台(正常) ・　400 番台(異常)
抽出データ	入力した条件によって、抽出されたデータ。

6.2.3 過去データ退避機能

(1)　定周期監視データ退避

一定周期毎に実行され、蓄積データ(監視)データベースを、古いデータより一定量ファイルに退避することにより蓄積データ(監視)データベースの格納データ量を一定に保つ。

※実行周期、削除量は実行環境の処理性能に合わせて調整できるものとする。

6.3 データベースの選定

「蓄積データ(システム)」のデータに関しては、事業体毎に管理するデータ項目が異なることが想定される。そのため、事業体毎に別々のテーブル定義情報を定義する必要がなく、データ内に項目定義情報を含有して管理可能な NoSQL データベースの採用を基本とする。

ただし、アプリケーションによっては、大量のトランザクション処理が必要なものがあるため、ACID（原子性（Atomicity)、一貫性（Consistency)、独立性（Isolation)、耐久性（Durability)）を実装した RDB の採用にも対応する。

7. システム監視モジュール

7.1 概要

7.1.1 機能概要

システム監視は、水道標準プラットフォームのシステム管理者に対して、水道標準プラットフォームおよびゲートウェイのシステム状態を監視するための機能を提供する機能群である。水道標準プラットフォームのシステム管理者は、水道標準プラットフォームおよびゲートウェイのシステム状態を監視し、環境の故障を適切に検出することで可用性の確保を行う。また、水道情報活用システムを利用する事業体の事業体運用管理者に対しても、監視項目をリアルタイムで確認するための画面を提供することで、システム状態の共有を可能とする。

7.1.2 監視範囲

システム監視の監視範囲について、水道標準プラットフォームを構成する機能モジュールのシステム状態を監視する。ゲートウェイのシステム監視について、ゲートウェイ上にシステム監視モジュールを導入し、システム監視の情報が水道標準プラットフォームにて一元管理可能なようにする。

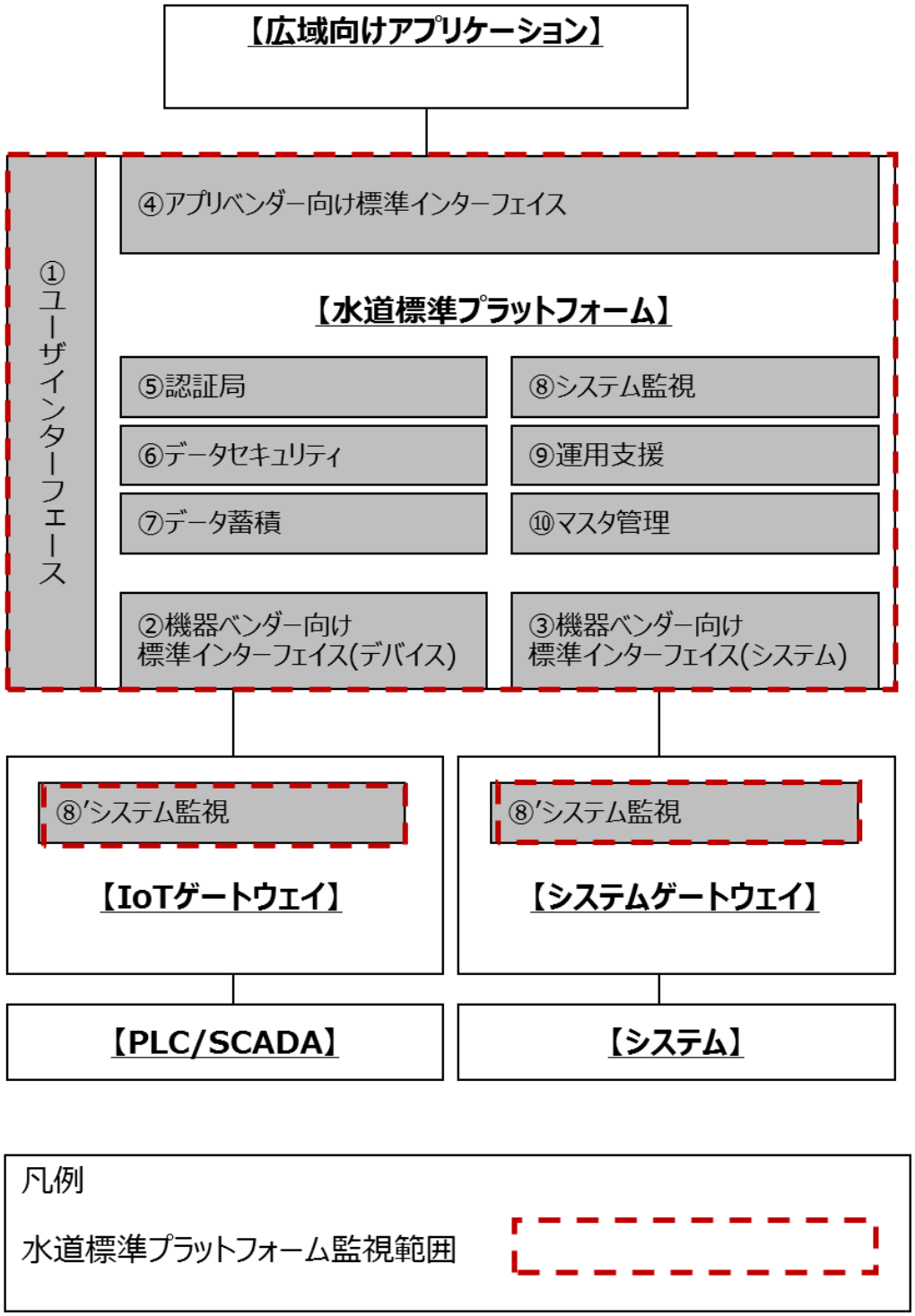


図 7-1:システム監視 監視範囲

7.1.3 機能一覧

システム監視の機能一覧を記載する。システム監視モジュールに必要な機能は、非機能要件やシステム運用方法等により、要件が変更となる。よって、必要最小限の機能例として、以下に記載する(表 7-1)。

表 7-1: システム監視 機能例

No	機能名		説明
1	システム監視		水道標準プラットフォームおよびゲートウェイの監視対象についてシステム監視を行う。
2		死活監視	監視対象が動作しているかどうか継続的に監視する。
3		障害監視	監視対象に障害発生していないか継続的に監視する。
4		リソース監視	監視対象のリソース使用状況を継続定期に監視する。
5		パフォーマンス監視	監視対象のパフォーマンス状況を継続定期に監視する。
6		ゲートウェイのデータ欠損監視	監視対象ゲートウェイのデータ欠損が発生していないか継続定期に監視する。
7	リアルタイム監視		監視項目をリアルタイムで確認するための画面を提供する。
8	メール通知		故障を検出した際に故障の重要度(故障レベル)に従って、メール通知する。
10	レポート		ゲートウェイの障害状況や稼働情報をレポート形式で定期的に配布する。
11		障害情報レポート	ゲートウェイの 1 日分の障害レポートの表示およびダウンロードが可能な障害状況管理画面を提供する。
12		稼働情報レポート	ゲートウェイの 1 日分の稼働レポートの表示およびダウンロードが可能な稼働状況管理画面を提供する。

システム毎に必要となる機能は以下の通り(表 7-2)。

表 7-2: システム毎の必要機能一覧

No	機能名		水道標準 プラットフォーム	ゲートウェイ (IoT/システム)
1	システム監視		-	-
2		死活監視	○	○
3		障害監視	○	○
4		リソース監視	○	○
5		パフォーマンス監視	○	○
6		ゲートウェイのデータ欠損監視	○	-
7	リアルタイム監視		○	○
8	メール通知		○	-
10	レポート		○	-
11		障害情報レポート	○	-

No	機能名	水道標準 プラットフォーム	ゲートウェイ (IoT/システム)
12	稼働情報レポート	○	-

7.2 機能要件

7.2.1 システム監視機能

システム監視として、以下の監視を実現する(表 7-3)。各機能の監視処理方式及び監視対象については、非機能要件を基に適切な処理方式を選択する事とする。

表 7-3: システム監視 機能要件

No	機能名	要件
1	死活監視	監視対象が動作しているかどうか継続的に監視する。 ・ 監視間隔や閾値等を個々に設定可能なこと。 ・ IP パケットや API 等により、監視対象からの応答有無や応答内容により、死活判定可能なこと。
2	状態監視	監視対象に異常が発生していないか継続的に監視する。 ・ プロセスやログ、SNMP トラップ等、要件に合わせ監視対象の状態を複数、監視可能なこと。
3	リソース監視	監視対象のリソース使用状況を継続定期に監視する。 ・ 監視間隔や閾値等を個々に設定可能であること。 ・ プロセッサやメモリ、記憶領域、ネットワーク帯域等にリソースを監視できること。
4	パフォーマンス監視	監視対象のパフォーマンス状況を継続定期に監視する。 ・ 監視間隔や閾値等を柔軟に設定可能であること。 ・ HTTP 等のリクエストを監視対象に対して送信し、監視対象のパフォーマンス情報を取得する事により、監視を実施すること。
5	ゲートウェイのデータ欠損監視	監視対象ゲートウェイのデータ欠損が発生していないか継続定期に監視する。データ欠損検出ログのメッセージをパターンマッチング判定（文字列監視）する事で、監視を実現する。

7.2.2 リアルタイム監視機能

システム監視情報をリアルタイムに画面表示すること。本機能は、水道標準プラットフォームのシステム管理者等が参照し、水道標準プラットフォーム及びゲートウェイのシステム状況を確認する。

7.2.3　メール通知機能

メールサーバーと連携し、システムの監視情報を運用者にメール通知する。監視内容や発生事象により、個別にメール送信先を設定できる事とする。また、通知内容として重要度や監視対象設備、検出日時、検出内容等を個別に設定できる事とする。メール通知有無や通知先は、要件を定めた上で、適切に設定する事とする。

7.2.4　レポート機能

ゲートウェイの障害状況や稼働情報をレポート形式で画面に表示する。以下に、機能要件をします。

- ゲートウェイにて発生した 1 日分の異常情報レポート/稼働情報レポートの表示及びダウンロードが可能であること。
- 発生時刻、復旧時刻、発生状況、発生原因、等の情報を出力可能であること。
- レポートは過去 1 週間分の表示およびダウンロードを可能とすること。
- システム監視は毎日午前 3 時以降、ゲートウェイから障害レポート取得を行う。
- 取得したレポート内容はデータベースに蓄積し、過去 1 週間分保持すること。
- レポート取得時刻にゲートウェイにて通信障害が発生した場合、リトライを実施すること。

8. マスタ管理モジュール

8.1 概要

8.1.1 機能概要

データベースサーバーにて管理されている各マスタテーブル情報のデータ提供及び、データ更新の要求を受け付ける。

8.1.2 機能一覧

マスタ管理の機能一覧を以下に示す(図 8-1、表 8-1)。

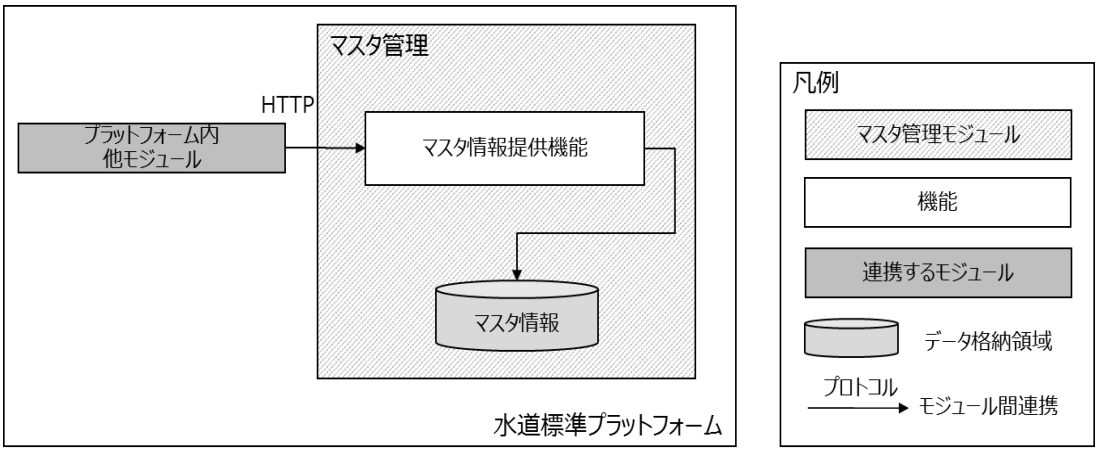


図 8-1 :マスタ管理 機能(モジュール)構成

表 8-1:マスタ管理 機能一覧

機能名	概要
マスタ情報提供	外部機能より指定された条件に合致する情報を抽出し外部機能に提供する。 本機能は１マスタにつき、１機能構成とする。 例）施設マスタの情報を提供する機能は、施設マスタ提供 設備マスタの情報を提供する機能は、設備マスタ提供

8.1.3 対象マスタ情報

マスタ管理で扱うマスタ情報は以下の通り(表 8-2)。

表 8-2:マスター一覧

大項目		
	中項目	
	マスタ名称	概要
所在管理情報		

所在 ID 管理		
	施設マスタ	施設情報を管理する。
	設備マスタ	設備情報を管理する。
	機器マスタ	機器情報を管理する。
	計測項目マスタ	計測項目情報を管理する。
	ゲートウェイマスタ	事業体が管理しているゲートウェイ毎の情報を管理する。
	ゲートウェイ-データ種別管理	事業体毎の設備 ID または機器 ID に紐づくゲートウェイ ID、データ種別を管理する。
アプリケーション管理情報		
アプリケーション管理情報		
	アプリケーションマスタ	アプリケーション情報を管理する。

8.2 機能要件

8.2.1 マスタ情報提供

マスタ情報提供機能は以下の処理を実施する。

- 外部機能からマスタ情報提供の要求を受け付ける。外部機能がマスタ情報提供を要求する際は、抽出条件を指定する。
- 要求された情報に合致するマスタテーブルの情報を検索し、データ抽出を行う。
- 抽出されたデータを要求元のモジュールに返却する。

(a) リクエスト概要

プラットフォーム内の他モジュールからマスタ管理へ要求する際に連携する情報を以下に記載する(表 8-3)。

表 8-3: リクエスト概要

項目	内容
抽出条件	マスタからデータ抽出に必要な条件を指定する。

(b) レスポンス概要

マスタ管理からプラットフォーム内の他モジュールへ応答する際に連携する情報を以下に記載する(表 8-4)。

表 8-4: レスポンス概要

項目	内容
ステータスコード	以下の何れかを指定する。 ・ 200(正常) ・ 404(異常)
データ	抽出されたデータ

8.3 データベースの選定

マスタ管理でのデータ管理は RDB を採用する。マスタ管理機能で管理するマスタ情報は、予めデータ構造を決める事が可能であり、データ構造は頻繁に変更されない事が想定されるため、RDB が適している。

9. 運用支援モジュール

9.1 概要

9.1.1 機能概要

運用支援は、水道 CPS/IoT リファレンスモデルにおける「水道標準プラットフォーム」の運用業務を支援する機能を提供するモジュールである。

9.1.2 機能一覧

運用支援の機能一覧を以下に示す(表 9-1)。

表 9-1: 運用支援 機能一覧

No	機能名	説明
1	データ流通状況監視機能	水道標準プラットフォーム内の各標準インターフェイス、アプリケーション、ゲートウェイに連携し、アプリケーション-ゲートウェイ間のデータ流通状況を参照する機能を提供する。
2	水道標準プラットフォーム監視機能	水道標準プラットフォーム内のシステム監視、ユーザーインターフェイスに連携し、水道情報活用システム監視機能を提供する。
3	ユーザー管理機能	水道標準プラットフォーム内のマスタ管理モジュール、ユーザーインターフェイスに連携し、水道情報活用システムの利用者情報を参照/登録/変更/削除する機能を提供する。
4	アプリケーション管理機能	水道標準プラットフォーム内のマスタ管理、認証局、ユーザーインターフェイスに連携し、アプリケーション情報を参照/登録/変更/削除する機能を提供する。
5	ゲートウェイ管理機能	水道標準プラットフォーム内のマスタ管理、認証局、ユーザーインターフェイスに連携し、ゲートウェイ情報を参照/登録/変更/削除する機能を提供する。
6	計測データモデル管理機能	水道標準プラットフォーム内のマスタ管理、ユーザーインターフェイスに連携し、各種マスタ情報を参照/登録/変更/削除する機能を提供する。
7	蓄積データ管理機能	水道標準プラットフォーム内のデータ蓄積、ユーザーインターフェイスに連携し、水道標準プラットフォームに蓄積されているデータを参照/更新/削除する機能を提供する。
8	アプリケーション監視機能	アプリケーションから、システム監視データを収集し、ユーザーインターフェイスに対し、情報を提供する。
9	ゲートウェイ監視機能	ゲートウェイから、システム監視データを収集し、ユーザーインターフェイスに対し、情報を提供する。

9.1.3 機能提供の対象

運用支援が機能を提供するモジュールについて、以下に一覧で示す(表 9-2)。

表 9-2:運用支援 機能一覧

提供先のシステム名			
	提供先のモジュール (機能群)名称	利用用途	提供するデータ
広域向けアプリケーション			
	標準インターフェイス	データ流通状況提供	データ流通内容
	システム監視	システム監視状況提供	システム監視内容
水道標準プラットフォーム			
	アプリベンダー向け標準インターフェイス(デバイス)	データ流通状況提供	データ流通内容
		システム監視状況提供	システム監視内容
	アプリベンダー向け 標準インターフェイス (システム)	データ流通状況提供	データ流通内容
		システム監視状況提供	システム監視内容
	システム監視	水道標準プラットフォーム監視状況提供	水道標準プラットフォーム 監視内容
	マスタ管理	データ操作内容提供	水道情報活用システム利用者情報 操作内容
			アプリケーション情報 操作内容
			ゲートウェイ情報 操作内容
			各種マスタ情報 操作内容
	データ蓄積	蓄積データ操作内容提供	水道標準プラットフォーム 蓄積データ操作内容

提供先のシステム名			
	提供先のモジュール (機能群)名称	利用用途	提供するデータ
	認証局	初期情報登録時の情報提供	ゲートウェイ登録情報 アプリケーション登録情報
	ユーザーインターフェイス	データ流通状況提供	データ流通内容
		システム監視状況提供	システム監視内容
		水道標準プラットフォーム監視状況提供	水道標準プラットフォーム 監視内容
		データ操作内容提供	水道情報活用システム利用者情報 操作内容
			アプリケーション情報 操作内容
			ゲートウェイ情報 操作内容
			各種マスタ情報 操作内容
		蓄積データ操作内容提供	水道標準プラットフォーム 蓄積データ操作内容
	機器ベンダー向け 標準インターフェイス (デバイス)	データ流通状況提供	データ流通内容
		システム監視状況提供	システム監視内容
	機器ベンダー向け 標準インターフェイス (システム)	データ流通状況提供	データ流通内容
		システム監視状況提供	システム監視内容
IoT ゲートウェイ			
	機器ベンダー向け 標準インターフェイス (デバイス)	データ流通状況提供	データ流通内容

提供先のシステム名			
	提供先のモジュール (機能群)名称	利用用途	提供するデータ
	システム監視	システム監視状況提供	システム監視内容
システムゲートウェイ			
	機器ベンダー向け 標準インターフェイス (システム)	データ流通状況提供	データ流通内容
	システム監視	システム監視状況提供	システム監視内容

10. 構成要件

10.1 テナント化

【元となる技術・サービス要素】

テナント
クラウドサービスにおいては、多数の利用者が別々の契約にて、同じ水道標準プラットフォームを利用しており、互いの処理負荷等の影響を分離する必要がある。一般に、クラウドサービスでは 「テナント」 という単位でリソースを契約し、影響の分離を実現しているため、水道標準プラットフォームサービスをクラウドを使って構築する場合には、「テナント」 適切な単位で分割することが、クラウドのリソースを使うために重要なポイントとなる。

【必要なシステム構成】

クラウド上に水道標準プラットフォームを構築する際に、ある水道事業者やベンダーのソフトウェアの処理負荷が想定の性能を超えて大きくなった場合に、他の水道事業者の処理性能が低下するような事態を避ける必要がある。このためには、大きく、共通的な機能、事業者データの蓄積機能、ベンダーのアプリケーションという３つのテナントに区切る構成とすることで、相互の影響を最小化する。**（要求Ｂ①　障害影響の局所化）**

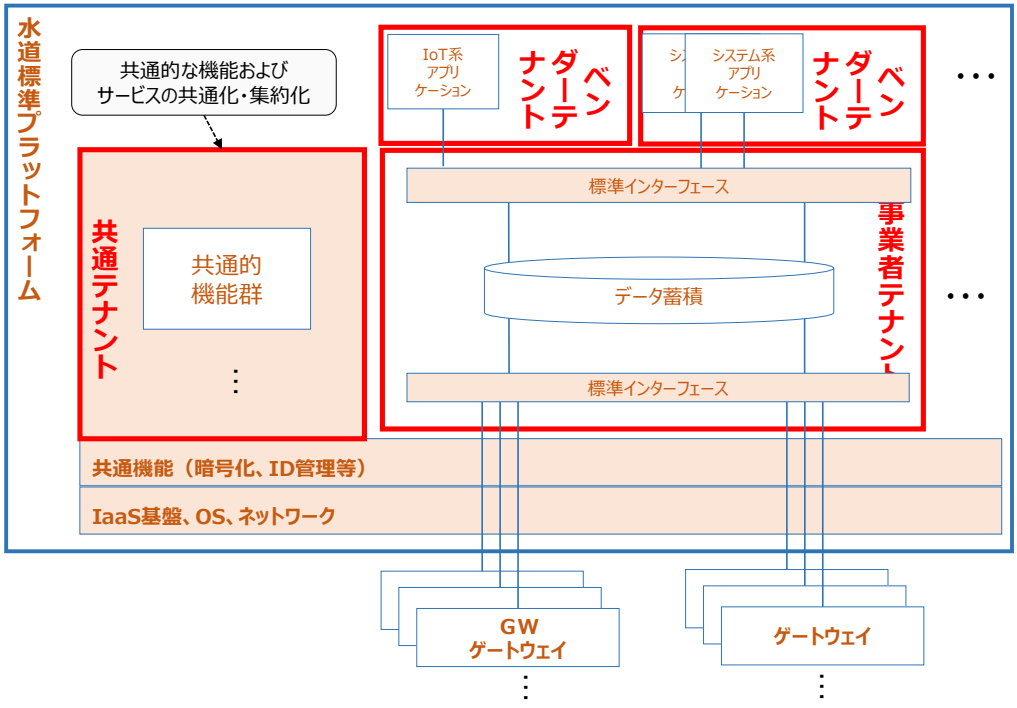
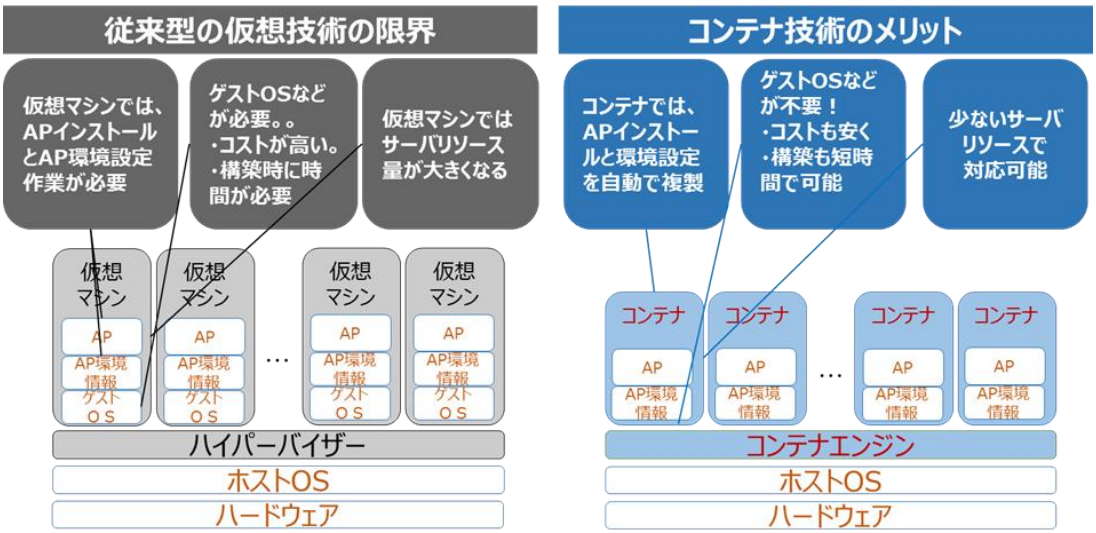


図 10-1：水道標準プラットフォーム全体でのテナント構成適用について

10.2　コンテナ化

【元となる技術・サービス要素】

コンテナ
コンテナは昨今急速に普及している仮想化技術の１つで、サービスとその実行環境をパッケージ化できるため、ソフトウェア開発者にとっては、煩わしいデプロイ作業から解放される（工数を削減できる）といったメリットがある。さらに、従来型と比べ「OS やミドルウェア」などを複数置く必要がないために従来型よりも安価となり、また簡単に「アプリケーション」ごとに増設できることでアプリケーション開発コストが圧縮できる。 

【必要なシステム構成】

コンテナはクラウド上のアプリケーションやソフトウェア稼働において、処理負荷の削減に有効であり、水道標準プラットフォームの各ソフトウェアの稼働環境に適用可能と考える。さらに、デプロイの工数削減のメリットから、特に事業者テナントとベンダーテナントにおいて具体的に以下のようなメリットが発揮されると想定する。**（要件 A①　コストダウン）**

（１）事業者テナント

事業者テナントにおいては、事業者の増加や、各事業者での処理量の増減により、サーバーの増減作業が発生する。コンテナを採用しておくことで、例えば受信データ量が増加した時にも短時間でサーバー数を増やし、常に、必要な数だけのサーバーリソースだけを確保すれば良いことになる。

（２）ベンダーテナント

ベンダーテナントでは、アプリケーションの導入や改修において、多数の試験や導入作業が発生する。その際に、コンテナ技術を活用することで、大きな工数の削減でき、ベンダーの水道標準プラットフォーム利用が促進されると期待できる。

10.3　システム系データ流通

【必要なシステム構成】

事業者からは多くのベンダーの参加を期待されていることに対し、アプリケーションの標準インターフェイス対応状況が途上であることを鑑み、ベンダーのアプリケーションと水道標準プラットフォーム上のデータとの接続については、暫定期間を 2025 年 3 月末として、従来のベンダーの「独自方式」での接続を許可する方針とする。なお、その場合でも、データ流通の機能は維持する必要があるため「標準インターフェイス」を活用して、他のアプリケーションがデータを取得できる仕組みを提供する。**（要求 B③　ベンダー参画を促すための措置）**

暫定的に認める対応案を以下に示す。

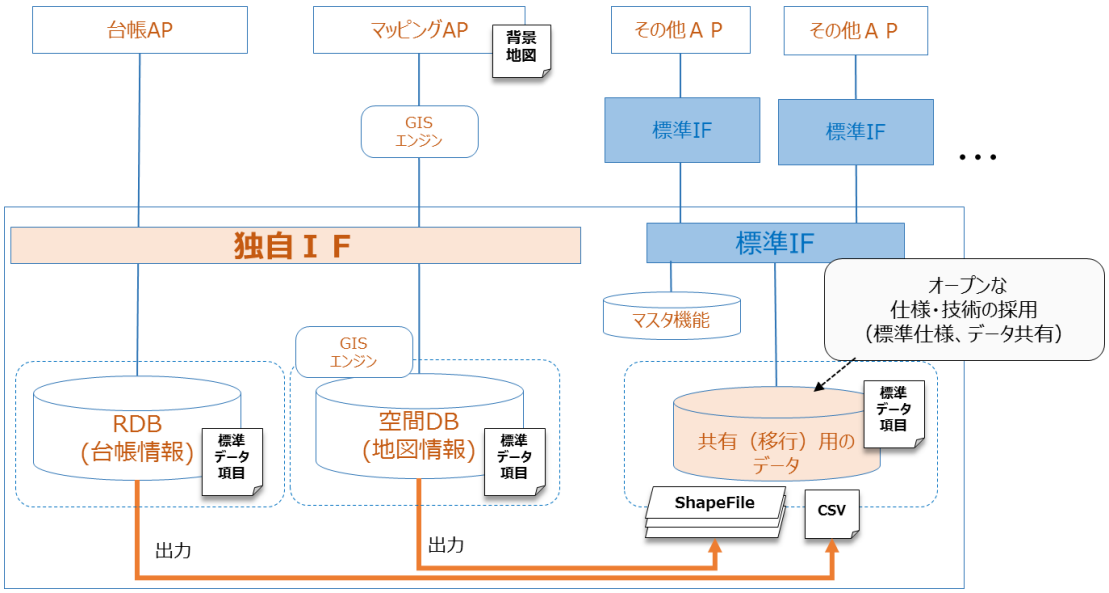


図　10-2：ベンダー対応の暫定案（独自ＩＦを暫定的に認める）

なお、参考として水道標準プラットフォームが予定している最終形を以下に示す。

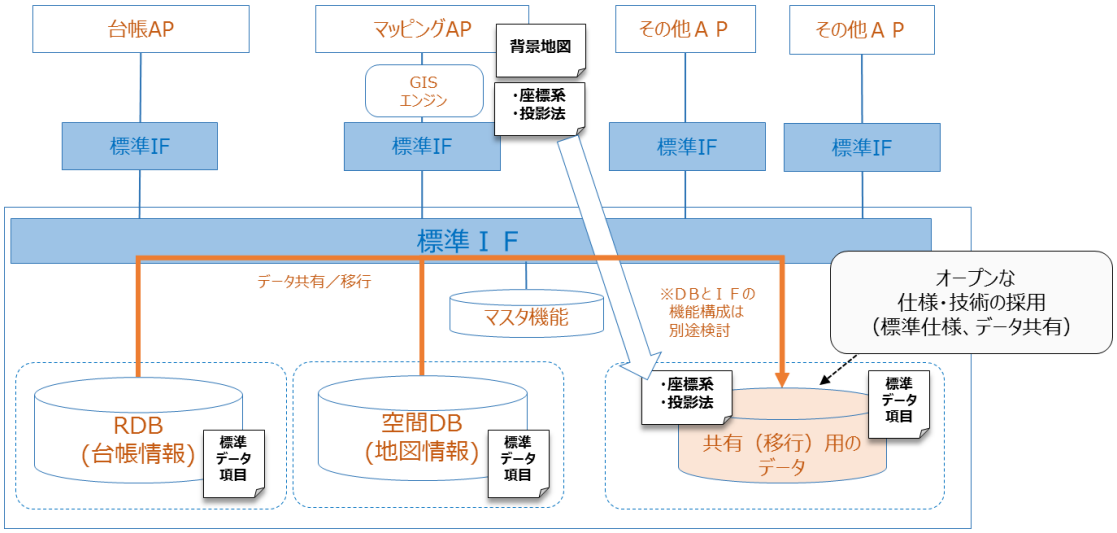


図 10-3：ベンダー対応の本来の形（標準ＩＦで実現）

10.4 監視／制御の分離

【必要なシステム構成】

データ収集のトラフィックが増大しても、制御操作を確実に実施できるようにする必要がある。これには、通常の「監視信号(上り信号)」と、「制御信号(下り信号)」とを分離した構成をとることで、制御信号が確実に現地 GW に届くようにする。**（要求 B①　障害影響の局所化）**

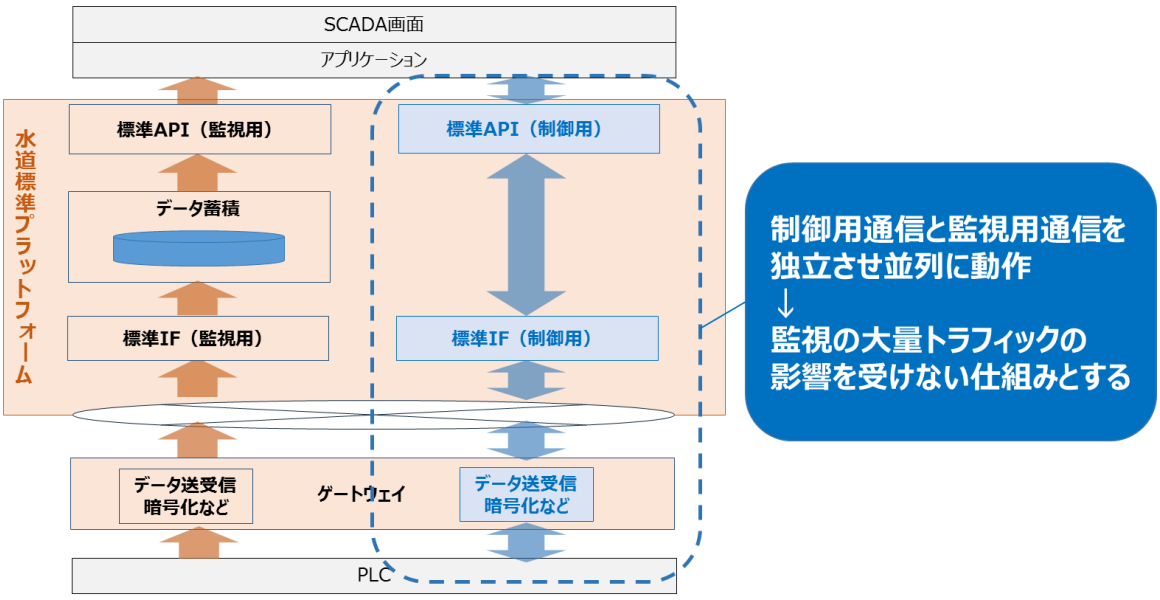


図 10-4：制御信号の確実性

10.5　アーキテクチャの全体像

以上の構成要件を踏まえて、水道標準プラットフォームのアーキテクチャの全体像は下図のように具体化される。

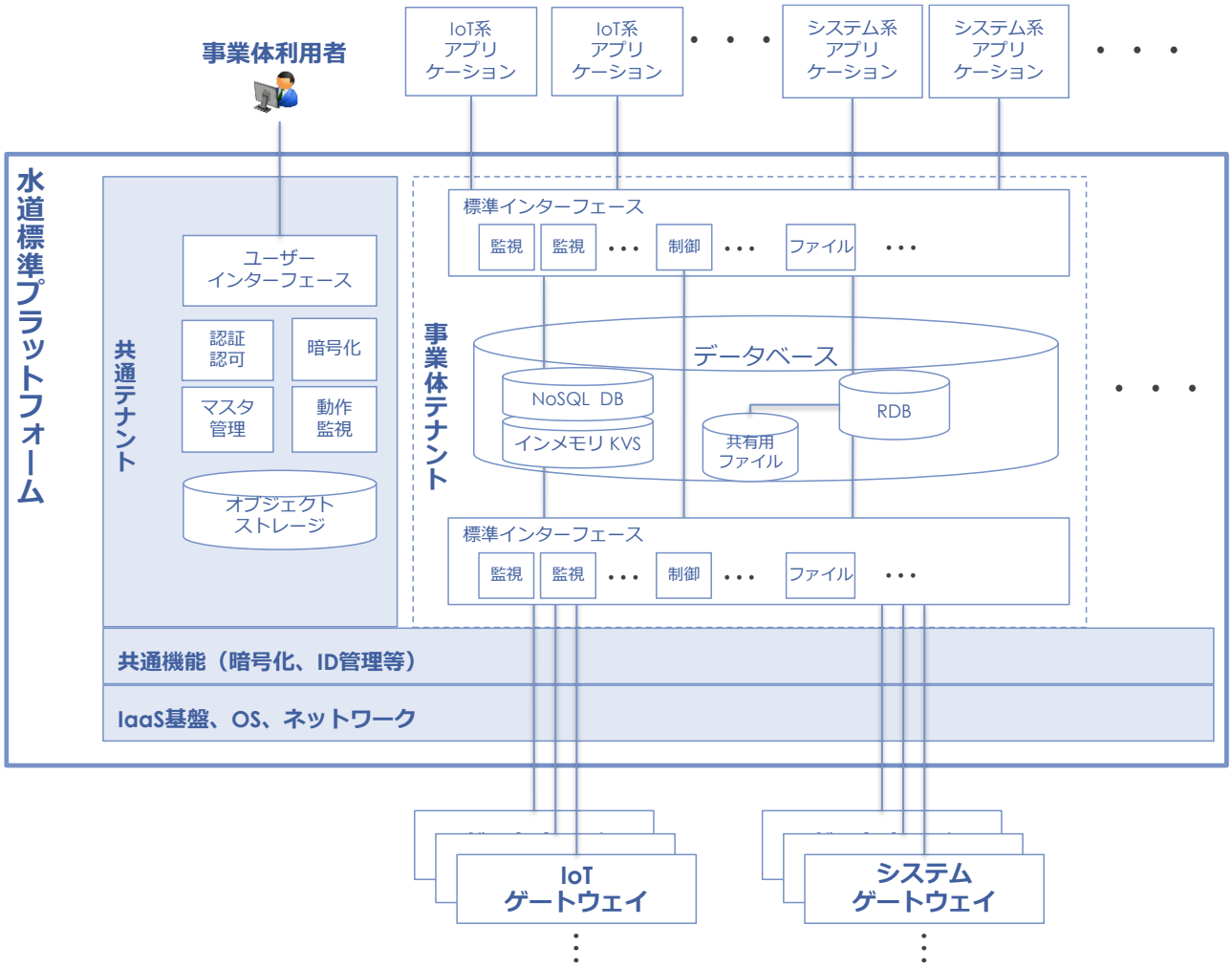


図 10-5 システムアーキテクチャ全体像　（共通テナント、事業者テナント具体化後）

11. 非機能要件

水道標準プラットフォームは、既存の水道業務システム（監視制御システム、台帳システム等）と同等、もしくは、それ以上のサービスを提供する必要がある。よって、非機能要件の設定に際しては、既存の水道業務システムの現状を踏まえて以下を設定する。

要件項目の設定にあたっては、独立行政法人　情報処理推進機構（略称　ＩＰＡ）にて制定している「非機能要求グレード 2018※」を基にする。この資料は、IT 系企業を幅広く調査し、その結果をもとに非機能要求項目を網羅的にリストアップして分類するとともに、それぞれの要求レベルを段階的に示したものである。

※https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html

11.1　可用性

水道業務の中でも、特に、取水～浄水～配水に関わる監視制御の分野においては、業務の高い継続性が求められる。そのため、冗長構成により、１台のサーバー停止でも水道標準プラットフォームの機能を停止せずにサービスを継続する構成を基本とする。ただし、冗長構成ではサービスコストが増えるため冗長構成を採用するかどうかは事業者の判断となる。

以上を踏まえ、可用性の方針としては以下の通りとする。

・単一障害時は業務停止を原則許容せず処理を継続させる。
・業務停止を伴う障害が発生した場合、障害発生時点まで復旧可能とする。

具体的には、主要なシステム要素は原則 2 重化し、単一故障点をなくす。データバックアップ/アーカイブバックアップ/システムバックアップリアルタイムもしは定期的に取得し、復旧できるようにする。

【非機能要件一覧】

#	項目	小項目	小項目説明	メトリクス（指標）	要件設定
1	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	運用時間（通常）	２４時間無停止
2				運用時間（特定日）	２４時間無停止
3				計画停止の有無	無し
4		業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲	ポータル画面からアクセス可能なサービスすべて
5				サービス切替時間	１５分未満（サーバー再起動）
6				業務継続の要求度	単一障害時は業務停止を許容せず、処理を継続させる

					（冗長構成の場合）
7		目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO（目標復旧地点）	障害発生時点（日次バックアップ+アーカイブからの復旧）
8				RTO（目標復旧時間）	2時間以内
9				RLO（目標復旧レベル）	データ流通、蓄積、制御が実施可能なレベル
10		目標復旧水準（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。	システム再開目標	１週間以内に再開
11		稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合。	稼働率	99.99%
12	回復性	可用性確認	可用性として要求された項目をどこまで確認するかの範囲。	確認範囲	データ流通、蓄積、制御を範囲とする。

11.2 性能・拡張性

性能に対する要求としては、現行の水道業務において利用されているシステムと同等かもしくはそれ以上であることが要求される。NEDOの実証事業「IoTを活用した社会インフラ等の高度化推進事業」において取りまとめられた水道業務システムの現状を踏まえ、データ流通およびデータ蓄積に対する性能要件は以下の通りとする。

■監視制御業務

項目		データ要件
監視頻度	場内	１秒
	場外	１秒
制御応答時間	場内	２秒
	場外	３秒
制御頻度及び間隔		通常時　　１０回/日 ピーク時　５分に１回（計２０回）

蓄積期間	■秒データ　　：２ヶ月～ ■帳票データ　：３０年～ ・日報（時間統計データ） ・月報（日統計データ） ・年報（月統計データ）

■台帳業務、会計業務、料金業務

項目	データ要件		
	台帳データ（設備台帳、管路台帳、点検）	会計データ	料金データ
データ内容	設備機器及び管路などの基本諸元情報や点検結果	予算や収支などの財務情報や固定資産、工事等	調定、収入、水道料金等
データ量	5MB/月（画像データが含まれる場合は増加）	100MB/年	340MB/年
収集頻度※	１ヶ月/回	１年/回	１年/回
蓄積期間(PF)	削除しない（除却された施設は１０年間残す）	５０年分	５０年分
蓄積期間(GW)	２ヶ月	２年	２年

上記の要求条件から、監視制御業務の監視頻度として　「１秒」　という要件がもっとも厳しい条件であり、通信回線や現地設置装置での遅延を除外すると、IoT ゲートウェイのインターフェイスから、アプリケーションのインターフェイスまでの処理目標を　５００ミリ秒以内　と設定する（下図参照）。

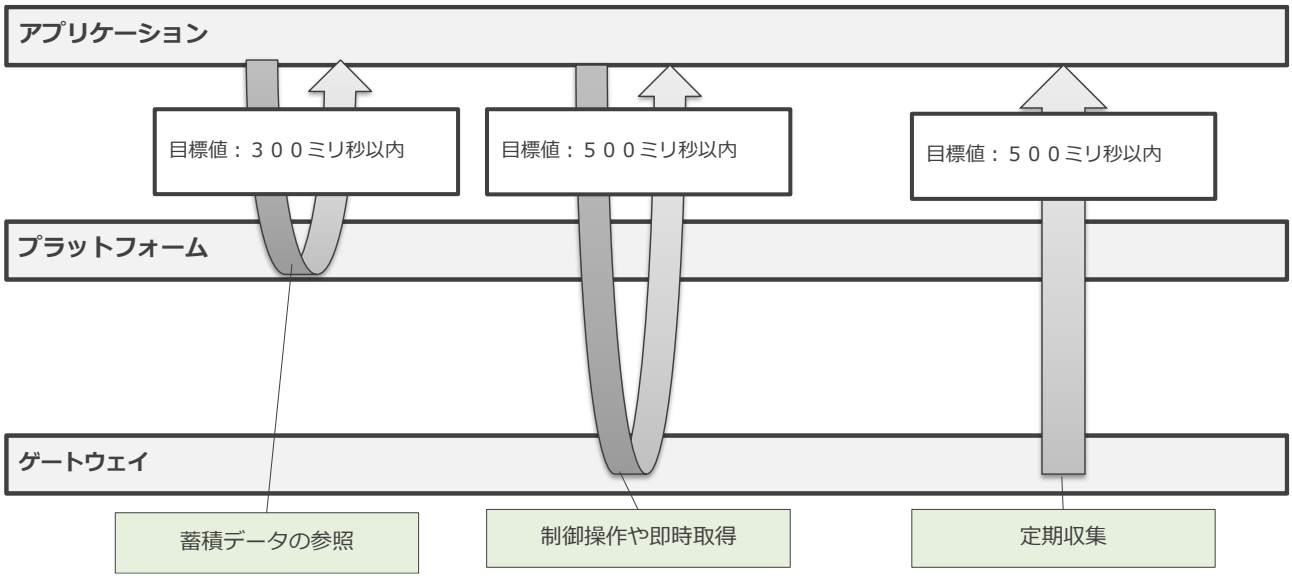


図 11-1： 処理性能の目標値

なお、IPA の「非機能要求グレード 2018」 に従い、目標値の順守率は以下の通りとする。

場合	順守率
ピーク時	８０%
平常時	９０%

11.3 運用・保守性

水道業務の中でも、特に、取水～浄水～配水に関わる監視制御の分野においては、２４時間３６５日の連続運転が必要となり、水道標準プラットフォームの運用・保守性についてについても、それを念頭に設定する必要がある。一方で、エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となり、障害を未然に防止できるなど、システムの品質を維持するための運用コストが下げる事ができる。

これらを前提として以下のように運用・保守性の要件を定める。

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
1	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。	運用時間（通常）	２４時間無停止
2				運用時間（特定日）	２４時間無停止
3		バックアップ	システムが利用するデータのバックアップに関する項目。	外部データの利用可否	外部データ利用不可
4				バックアップ利用範囲	障害発生時のデータ損失防止
5				バックアップ自動化の範囲	1 ステップのみ手動で行う
6				バックアップ取得間隔	システム構成の変更時など、任意のタイミング
7				バックアップ保存期間	サービスが継続する限り保管しておく必要がある。
8		運用監視	システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	監視情報	スケールアウトのタイミングを決定するため、エラー情報だけでなく、リソース使用状況も監視
9				監視間隔	リアルタイム監視（分間隔）
10	保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を	計画停止の有無	システムを停止できる時間帯が存在しない。

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
			目的とした、事前計画済みのサービス停止に関する項目。		
11		運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。	保守作業自動化の範囲	業務機能の起動・停止など定期的に行う処理は自動化するが、ログの削除など非定期に実行する処理は管理者が手動で実施する
12	運用環境	開発用環境の設置	ユーザーがシステムに対する開発作業を実施する目的で導入する環境についての項目。	開発用環境の設置有無	運用環境と同一の開発環境を設置する
13		試験用環境の設置	ユーザーがシステムの動作を試験する目的で導入する環境についての項目。	試験用環境の設置有無	システムの開発用環境と併用する
14		マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	マニュアル準備レベル	システムの通常運用のマニュアルを提供する
15		リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	リモート監視地点	遠隔地でリモート監視を行う
16				リモート操作の範囲	リモート操作は行わおない
17		外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。	外部システムとの接続有無	社外の外部システムと接続する
18	サポート体制	保守契約（ハードウェア）	保守が必要な対象ハードウェアの範囲。	保守契約（ハードウェア）の範囲	クラウド業者のサービスを契約
19		保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲。	保守契約（ソフトウェア）の範囲	水道標準プラットフォームソフトウェアの保守を実施

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
20		ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。	ライフサイクル期間	10 年以上
21	その他の運用管理方針	内部統制対応	IT 運用プロセスの内部統制対応を行うかどうかに関する項目。	内部統制対応の実施有無	既存の社内規定に従って、内部統制対応を実施する
22		サービスデスク	ユーザーの問合せに対して単一の窓口機能を提供するかどうかに関する項目。	サービスデスクの設置有無	新規にサービスデスクを設置する

11.4 移行性

水道標準プラットフォームは１０年以上を継続して稼働することを想定しており、長期的には、水道標準プラットフォームの移行が発生する可能性があるが、１０年後の利用動向、技術動向は大きく変わる可能性があるため、現時点での要件設定は実施しないこととする。

11.5 セキュリティ

水道事業は国の重要インフラの一つとされ、そのデータ保護は、水道事業に関わる情報システムの基本的な要件の一つである。そのための対策としては下図に示す①～⑧が挙げられる。

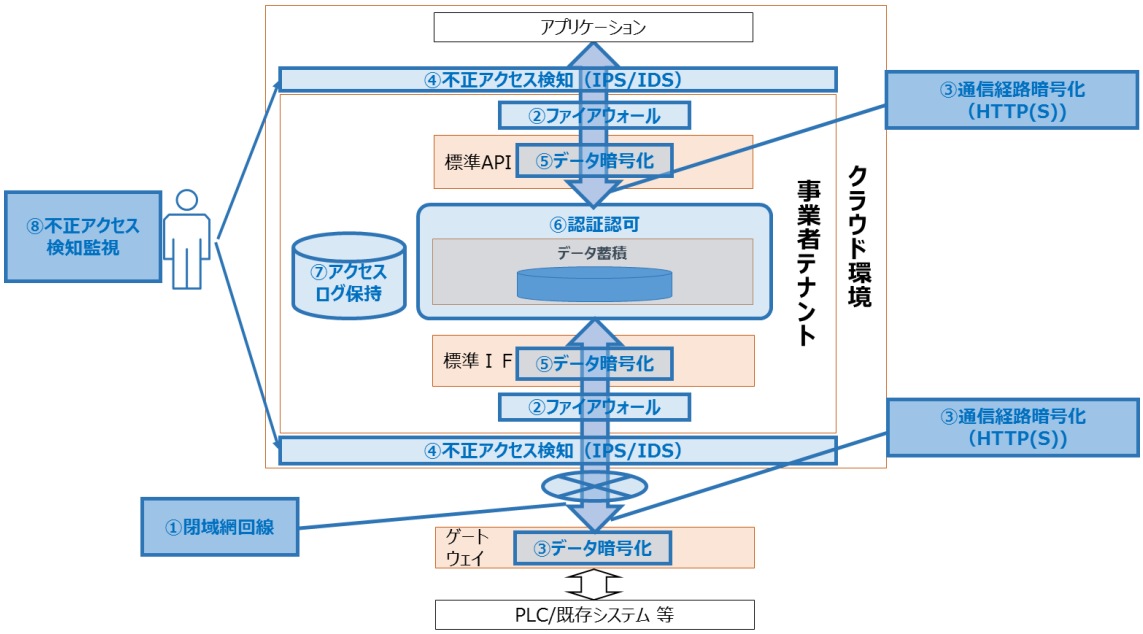


図 11-2：セキュリティ性の確保

上記を要件項目として以下の表に整理する。

要件項目	要件内容	対策項目との関連
アクセス・利用制限	ユーザーとアプリケーションの両方の認証認可を行い事業者テナント毎にアクセスを分離	⑥認証認可
データの秘匿	データの暗号化を行い、所定の受信者のみが復号できるようにする。	⑤データ暗号化
不正追跡・監視	操作やアクセスに関するログ取得	⑦アクセスログ保持

ネットワーク対策	ネットワークのアクセス制限と不正検知	①閉域網回線 ②ファイヤウォールの利用 ④不正アクセス検知（IPS/IDS） ⑧不正アクセス検知監視
マルウェア対策	コンピュータウィルスの検知及び駆除	（クラウドサービスを利用）
Ｗｅｂ対策	Web アプリケーション特有の脅威、脆弱性に関する対策	（クラウドサービスを利用）

上記を踏まえ、具体的な非機能要件項目を以下に示す。

■非機能要件項目

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
1	前提条件・制約条件	情報セキュリティに関するコンプライアンス	ユーザが順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。	順守すべき社内規程、ルール、法令、ガイドライン等の有無	順守すべき規程、法令、ガイドライン等が存在する。

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
2	セキュリティリスク分析	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	リスク分析範囲	ネットワークを通じた、不特定多数の攻撃者からの脅威にさらされる。また、重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、システム全体のリスクを分析する必要がある。
3	セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント（設計書や環境定義書、実装済みソフトウェアのソースコードなど）に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。	ネットワーク診断実施の有無	重要情報を取り扱うため、内部ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。
4				Web 診断実施の有無	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。
5	アクセス・利用制限	認証機能	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。	管理権限を持つ主体の認証	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
			なお、認証するための方式としては、ID/パスワードによる認証や、IC カード等を用いた認証等がある。		
6		利用制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例） ドアや保管庫の施錠、USB や CD-RW やキーボードなどの入出力デバイスの制限、コマンド実行制限など。	システム上の対策における操作制限度	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可
7	データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	伝送データの暗号化の有無	重要情報の暗号化は、データの通信経路の種別により決定する。 インターネット網…データ暗号化必須 閉域網…データ暗号化任意
8				蓄積データの暗号化の有無	有り （事業者側で決定）
9	不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるか	ログの取得	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行し」「その結果、どのようになったか」を確認し、その後の対策を迅速に実施するために、ログを取得する必要があ

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
			は、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。		る。
10				ログ保管期間	６か月 監視 MW によるログ監視を実施することで、ログの保管期間を短くする。
11				不正監視対象（装置）	重要度が高い資産を扱う範囲、あるいは、外接部分
12				不正監視対象（ネットワーク）	重要度が高い資産を扱う範囲、あるいは、外接部分
13				不正監視対象（侵入者・不正操作等）	重要度が高い資産を扱う範囲、あるいは、外接部分
14	ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御	踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施する必要がある。 [–] 踏み台等の脅威を許容する場合
15		不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	不正通信の検知範囲	不正な通信を確認し、対策を迅速に実施すうために、不正検知を実施する必要がある。

#	中項目	小項目	小項目説明	メトリクス(指標)	要件設定
16		サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	ネットワークの輻輳対策	DoS/DDoS 攻撃のサービス停止攻撃に対応する必要がある。 （可用性と関連する）
17	マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。	マルウェア対策実施範囲	マルウェアの感染により、重要情報が漏洩する脅威等に対抗するために、マルウェア対策を実施する必要がある。
18	Web 対策	Web 実装対策	Web アプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	セキュアコーディング、Web サーバーの設定等による対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Web サーバーに対する対策を実施する必要がある。
19				WAF の導入の有無	システムに侵入されることによる、情報の漏洩、踏み台等の脅威に対抗するために、機器による、侵入抑止、検知を実施する必要がある。

- 以上 -