

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

平成 31 年 4 月

国立研究開発法人新エネルギー・産業技術総合開発機構

株式会社三菱総合研究所

株式会社エヌ・ティ・ティ・データ

株式会社日立製作所

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」事業により作成しました。

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「当機構」という)は、以下の条件のもとで本ドキュメント(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)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機構の許可なく、それらの宣伝、広告活動に当機構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機構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、当機構は、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、明示たとと黙示たとを問わず、一切の保証を行わないものとします。また、当機構は、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. 当機構は、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。当機構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機構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
1.1 本ドキュメントの目的.....	1
1.2 水道情報活用システム標準仕様のドキュメント.....	2
1.2.1 ドキュメント体系.....	2
1.2.2 対象読者と役割.....	3
1.2.3 本ドキュメントの対象読者.....	4
1.3 参考文献.....	5
1.4 用語の説明.....	8
1.5 本ドキュメントの記載範囲.....	10
2. 概要.....	11
2.1 水道標準プラットフォームの役割と特徴.....	11
2.1.1 広域アプリケーション向け提供サービス.....	11
2.1.2 ゲートウェイ向け提供サービス.....	12
2.1.3 利用者向け提供サービス.....	13
システム監視.....	14
2.2 システム化方針.....	15
2.2.1 サービス指向アーキテクチャ(SOA)の採用.....	15
2.2.2 オープンソース技術の採用.....	16
2.2.3 クラウドサービスの採用.....	16
3. ユーザーインターフェイスモジュール.....	17
3.1 概要.....	17
3.1.1 機能概要.....	17
3.1.2 機能一覧.....	17
3.2 機能要件.....	22
3.2.1 ポータルサイト機能.....	22
3.2.2 事業体運用支援向け管理機能.....	22
3.2.3 アクセス制御機能.....	23
3.3 利用プロトコルと暗号化について.....	25
3.3.1 利用プロトコルについて.....	25
3.3.2 暗号化について.....	25

4. 認証局モジュール.....	26
4.1 概要.....	26
4.1.1 機能概要	26
4.1.2 機能一覧	26
4.2 機能要件.....	28
4.2.1 データ保護用証明書/秘密鍵提供機能	28
4.2.2 証明書/秘密鍵管理機能	35
5. データセキュリティモジュール	38
5.1 概要.....	38
5.1.1 機能概要	38
5.1.2 機能一覧	38
5.1.3 データ暗号化/復号方式	39
5.1.4 電子署名方式	49
5.2 機能要件.....	55
5.2.1 データ保護用証明書/秘密鍵取得機能	55
5.2.2 データ暗号化機能	57
5.2.3 データ復号機能	59
5.2.4 電子署名付与機能	61
5.2.5 電子署名検証機能	63
6. データ蓄積モジュール.....	65
6.1 概要.....	65
6.1.1 機能概要	65
6.1.2 各データの保持方針	65
6.1.3 データ蓄積方式	65
6.1.4 データ蓄積方式の選択	68
6.1.5 機能一覧	68
6.2 機能要件.....	69
6.2.1 データ蓄積機能	69
6.2.2 データ提供機能	71
6.2.3 過去データ退避機能	73
6.3 データベースの選定.....	73
7. システム監視モジュール.....	74

7.1 概要.....	74
7.1.1 機能概要	74
7.1.2 監視範囲	74
7.1.3 機能一覧	75
7.2 機能要件.....	77
7.2.1 システム監視機能	77
7.2.2 リアルタイム監視機能	77
7.2.3 メール通知機能	78
7.2.4 レポート機能	78
8. マスタ管理モジュール.....	79
8.1 概要.....	79
8.1.1 機能概要	79
8.1.2 機能一覧	79
8.1.3 対象マスタ情報	80
8.2 機能要件.....	81
8.2.1 マスタ情報提供	81
8.2.2 マスタ情報更新	82
8.2.3 マスタ情報追加	83
8.2.4 マスタ情報削除	83
8.3 データベースの選定.....	84
9. 運用支援モジュール.....	85
9.1 概要.....	85
9.1.1 機能概要	85
9.1.2 機能一覧	85
9.1.3 機能提供の対象	86

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。

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図を以下に示す(図 1-1)。

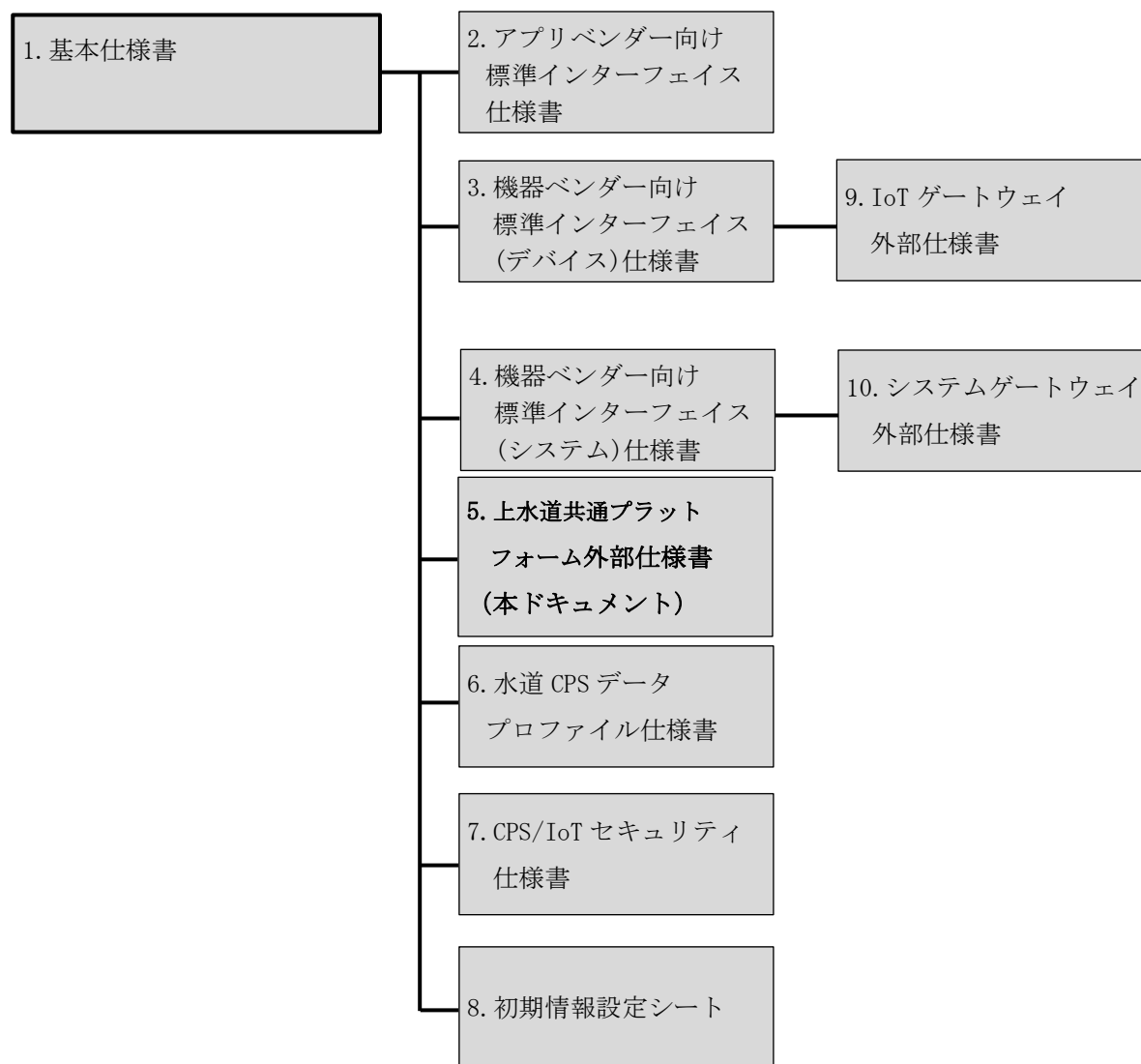


図 1-1: ドキュメント体系図

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 事業者：

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者。

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。

1.2.3 本ドキュメントの対象読者

本ドキュメントの対象読者を以下に示す（表 1-1）。

水道標準プラットフォーム外部仕様書(本ドキュメント)は、主に⑤プラットフォームマーが参照すべきドキュメントである。

表 1-1: 参照すべきドキュメントと対象読者

No.	ドキュメント名		対象読者 (1.2.2 項を参照)				
			①	②	③	④	⑤
1	基本仕様書 (本ドキュメント)		○	○	○	○	○
2	別冊	アプリベンダー向け 標準インターフェイス仕様書	—	○	—	—	○
3		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	—	—	○	—	○
4		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	—	—	—	○	○
5		水道標準プラットフォーム外部仕様書	—	△	△	△	○
6		水道 CPS データプロファイル仕様書	—	○	○	—	○
7		CPS/IoT セキュリティ仕様書	—	○	○	○	○
8		初期情報設定シート	○	△	△	△	○
9		IoT ゲートウェイ外部仕様書	—	—	○	—	—
10		システムゲートウェイ外部仕様書	—	—	—	○	—

【凡例】 ○：必須、△：任意

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: 参考ドキュメント

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I o T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.pdf

経済産業省「平成28年度I o T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I o T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 (<u>A</u> rtificial <u>I</u> ntelligence)	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 (<u>A</u> pplication <u>P</u> rogramming <u>I</u> nterface)	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 (<u>D</u> ata <u>U</u> niversal <u>N</u> umbering <u>S</u> ystem 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 (<u>F</u> ully <u>Q</u> ualified <u>D</u> omain <u>N</u> ame)	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 (<u>I</u> nternet <u>A</u> ssigned <u>N</u> umbers <u>A</u> uthority)	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 (<u>J</u> apanese <u>A</u> rticle <u>N</u> umber)	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 (<u>M</u> ultipurpose <u>I</u> nternet <u>M</u> ail <u>E</u> xtension)	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)。

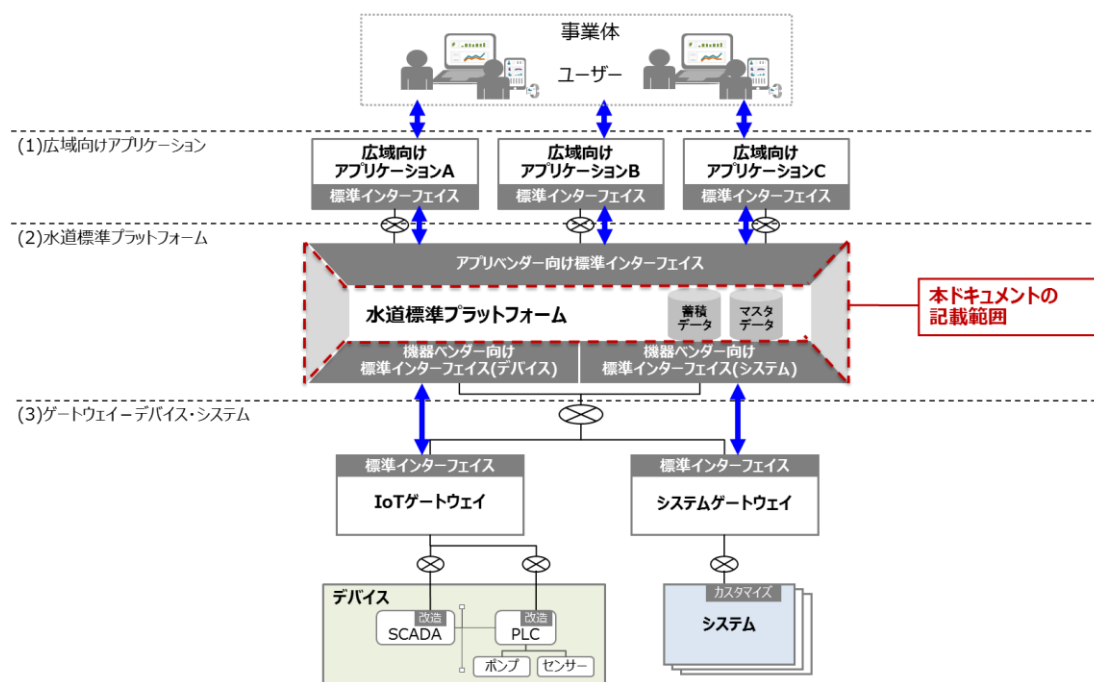


図 1-2: ドキュメント体系図

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。

上記の特徴を踏まえ、水道標準プラットフォームが提供するサービスは以下の通りである。

2.1.1 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 2-1)。

表 2-1: 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

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】
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

2.1.2 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 2-2）。

表 2-2: 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

2.1.3 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 2-23)。

表 2-3: 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

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 2-4)。

表 2-4: 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。

No.	システム処理機能	説明
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。
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。

2.2 システム化方針

2.2.1 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組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 2-1)。

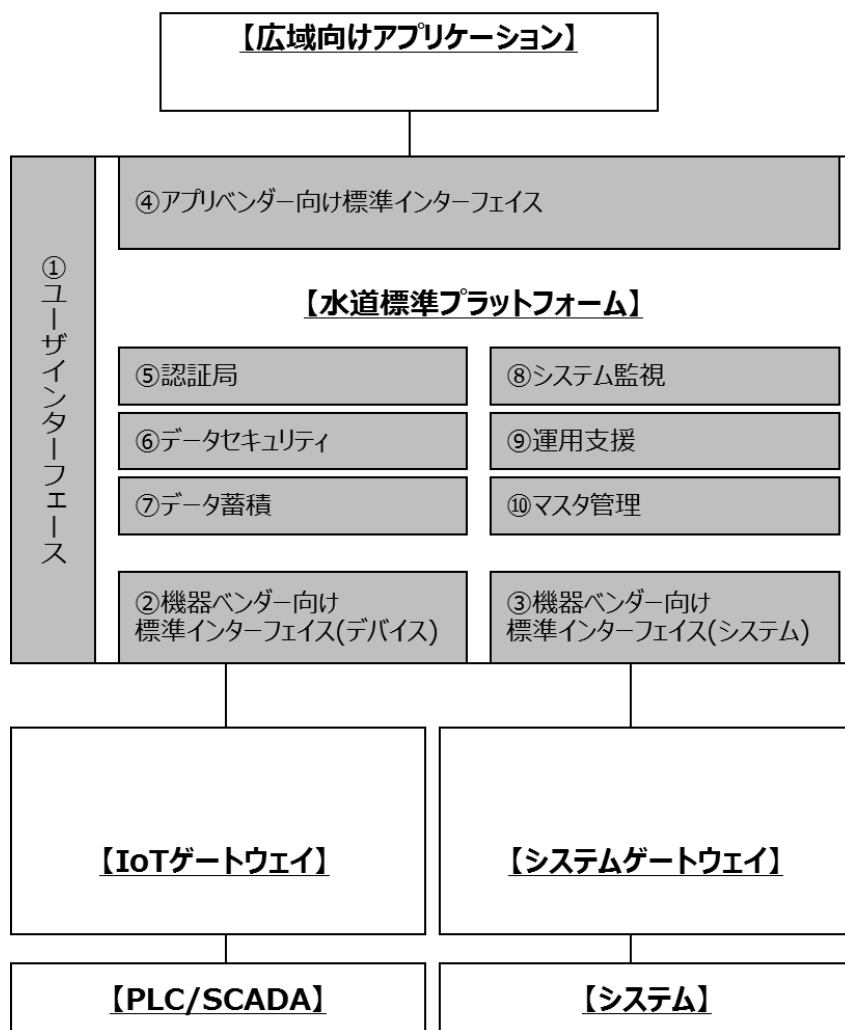


図 2-1: 水道標準プラットフォームのモジュール構成

2.2.2 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。

2.2.3 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。

- ・ サーバ拡張が容易に行えるため、利用者数(サーバ負荷・データ発生数)に合わせて、サーバ構成の変更が容易・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。

以降の章では、水道標準プラットフォームの各モジュールについて、外部仕様を記載する。

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）。

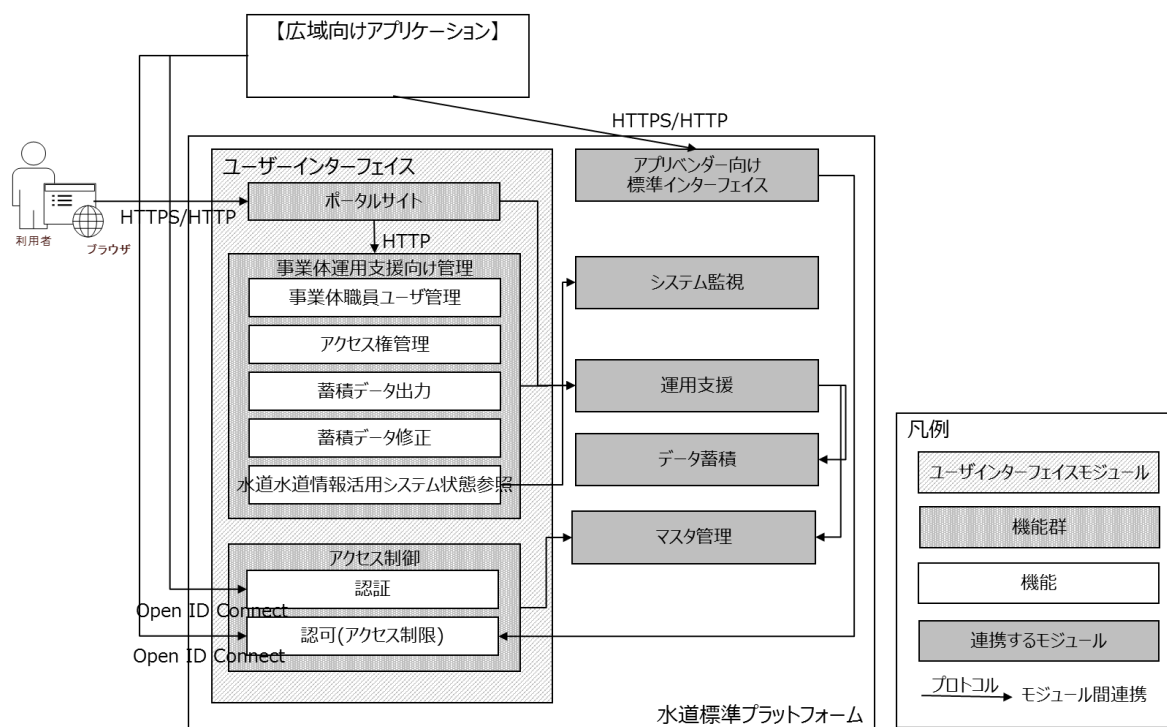


図 3-1: ユーザーインターフェイスの機能(モジュール)構成

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。
	プラットフォーム	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、プラットフォームにて行う。
		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)。

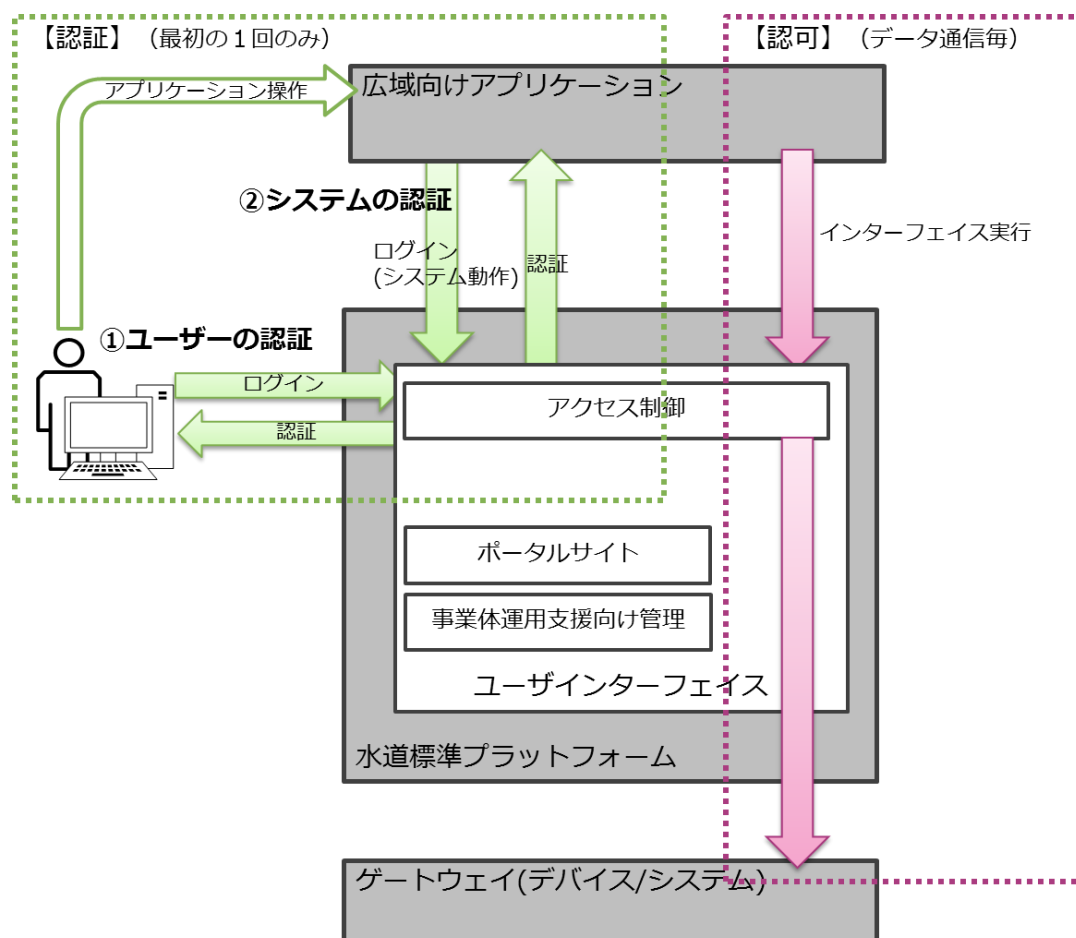


図 3-2: アクセス制御機能概要

(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）

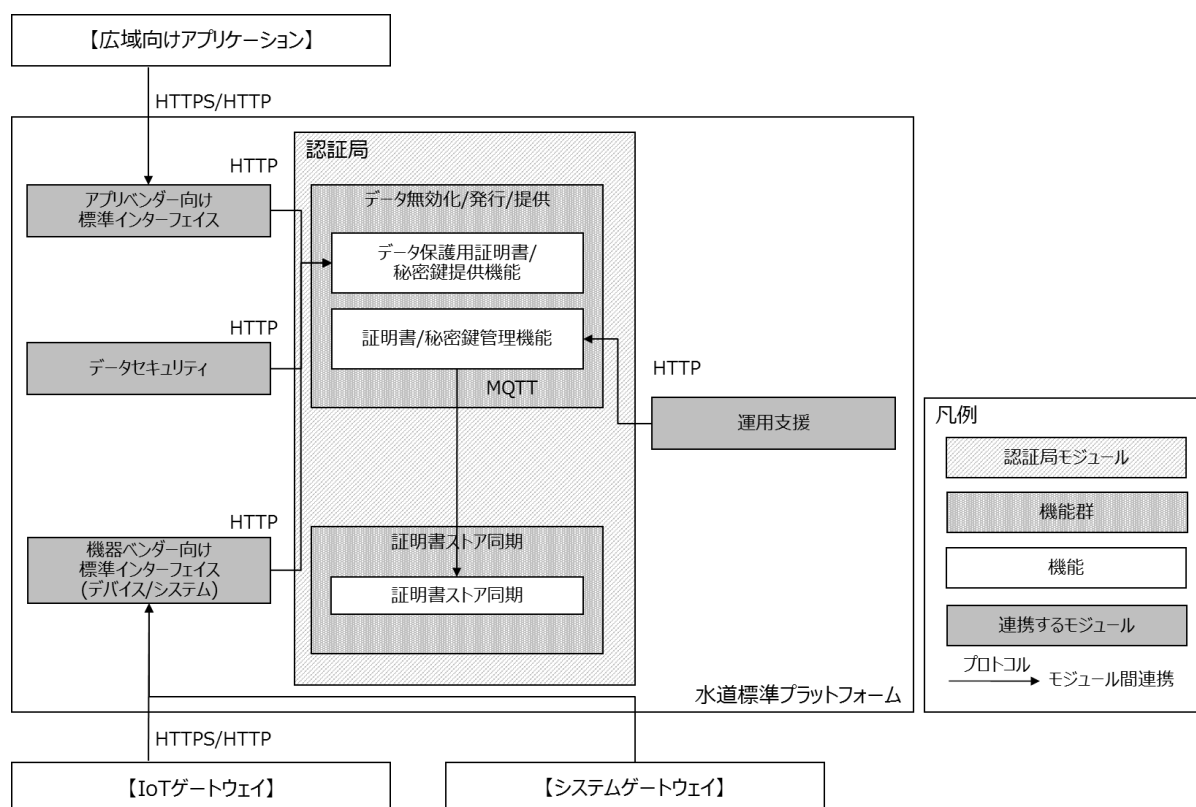


図 4-1: 認証局の機能(モジュール)構成

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ケーション証明書(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)。

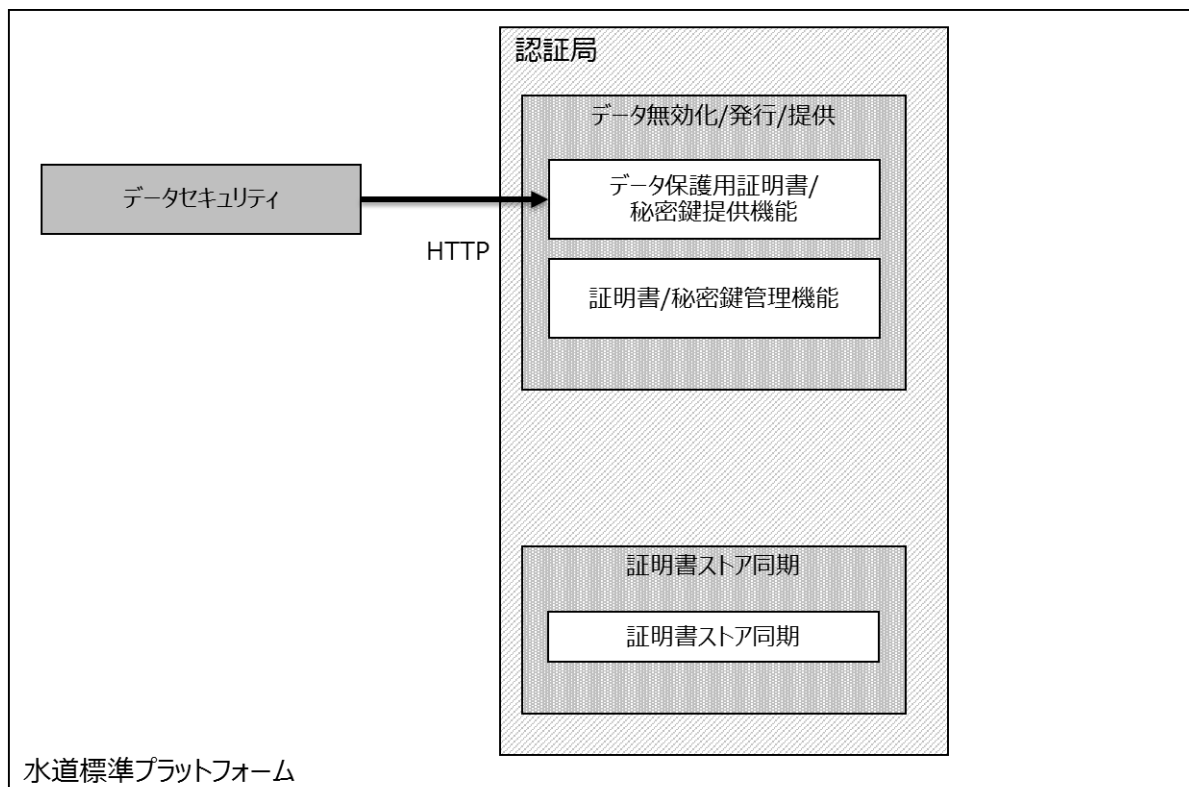


図 4-2: データ証明書/秘密鍵提供機能 データセキュリティ向け提供経路

(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)。

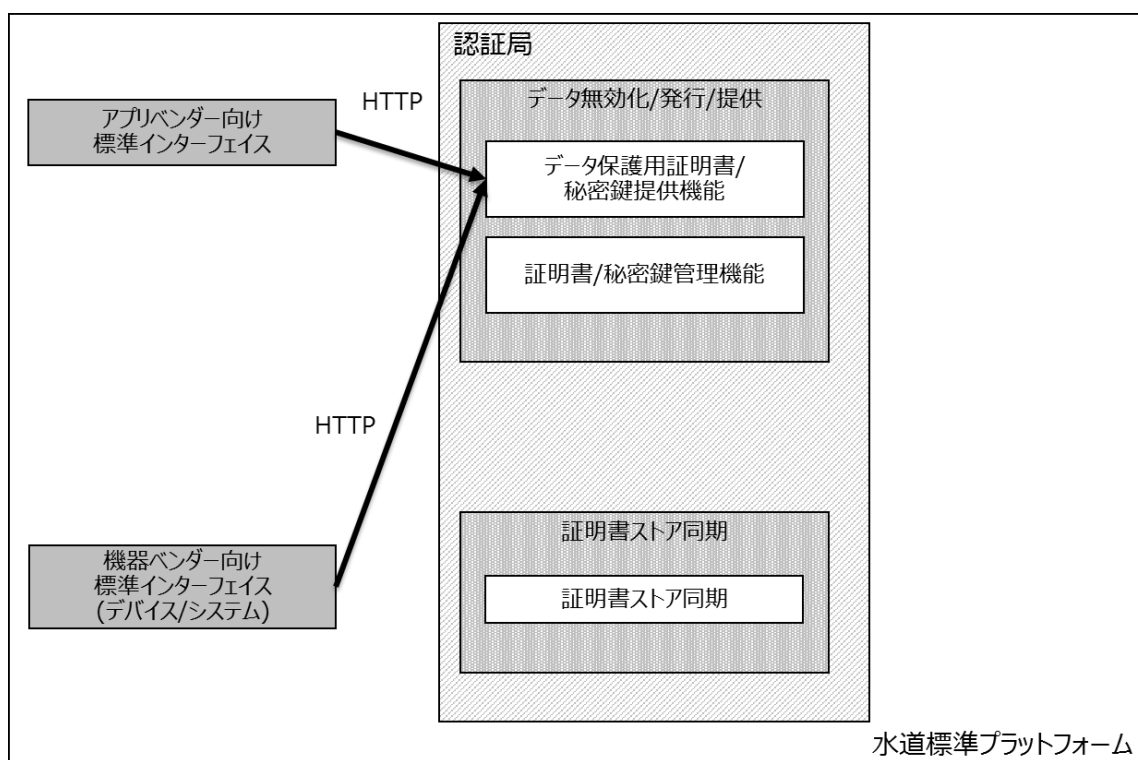


図 4-3: データ保護用証明書/秘密鍵提供機能 標準インターフェイス向け提供経路

(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)。

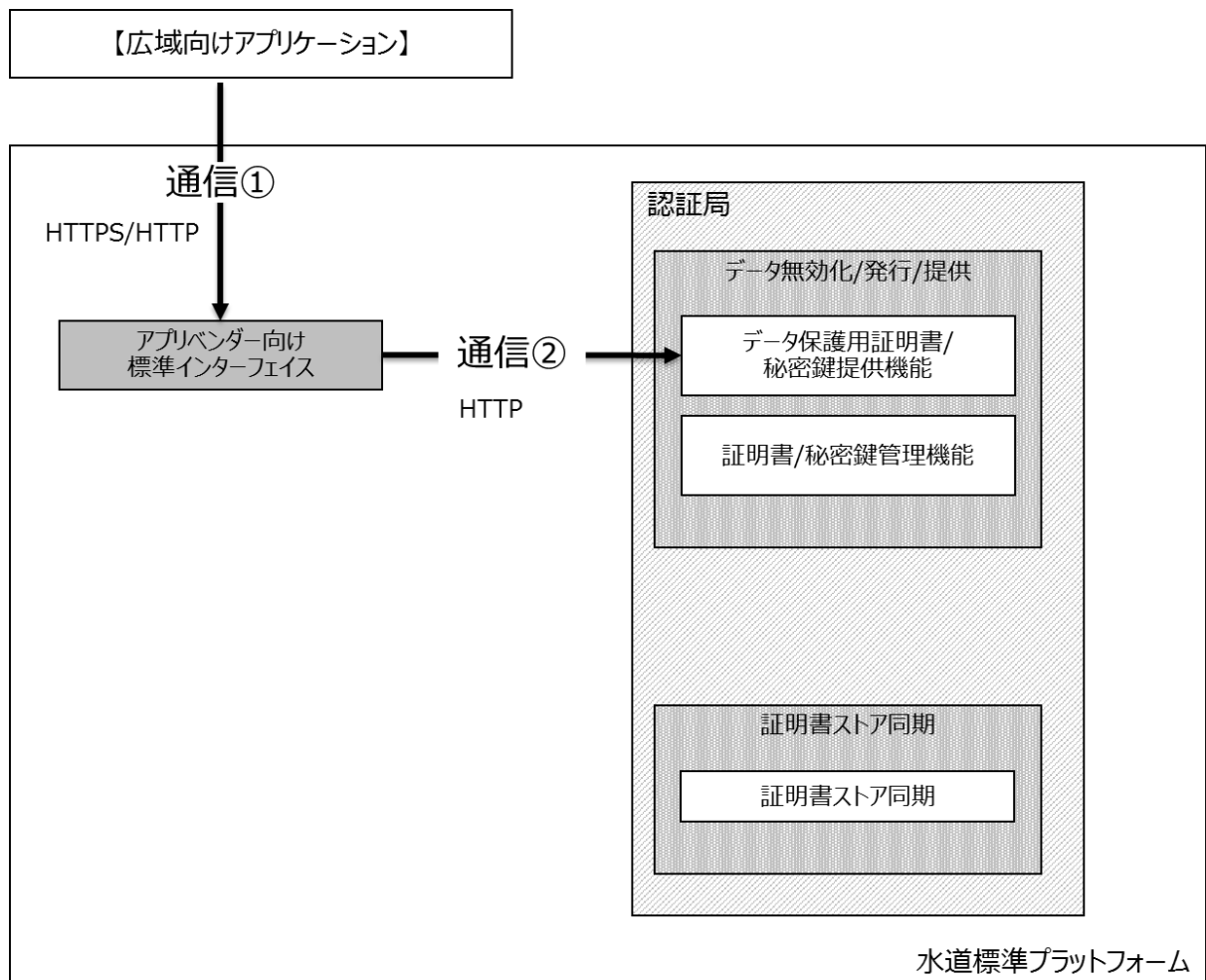


図 4-4: 広域アプリケーション向け提供経路

(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 4-4)。

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)。

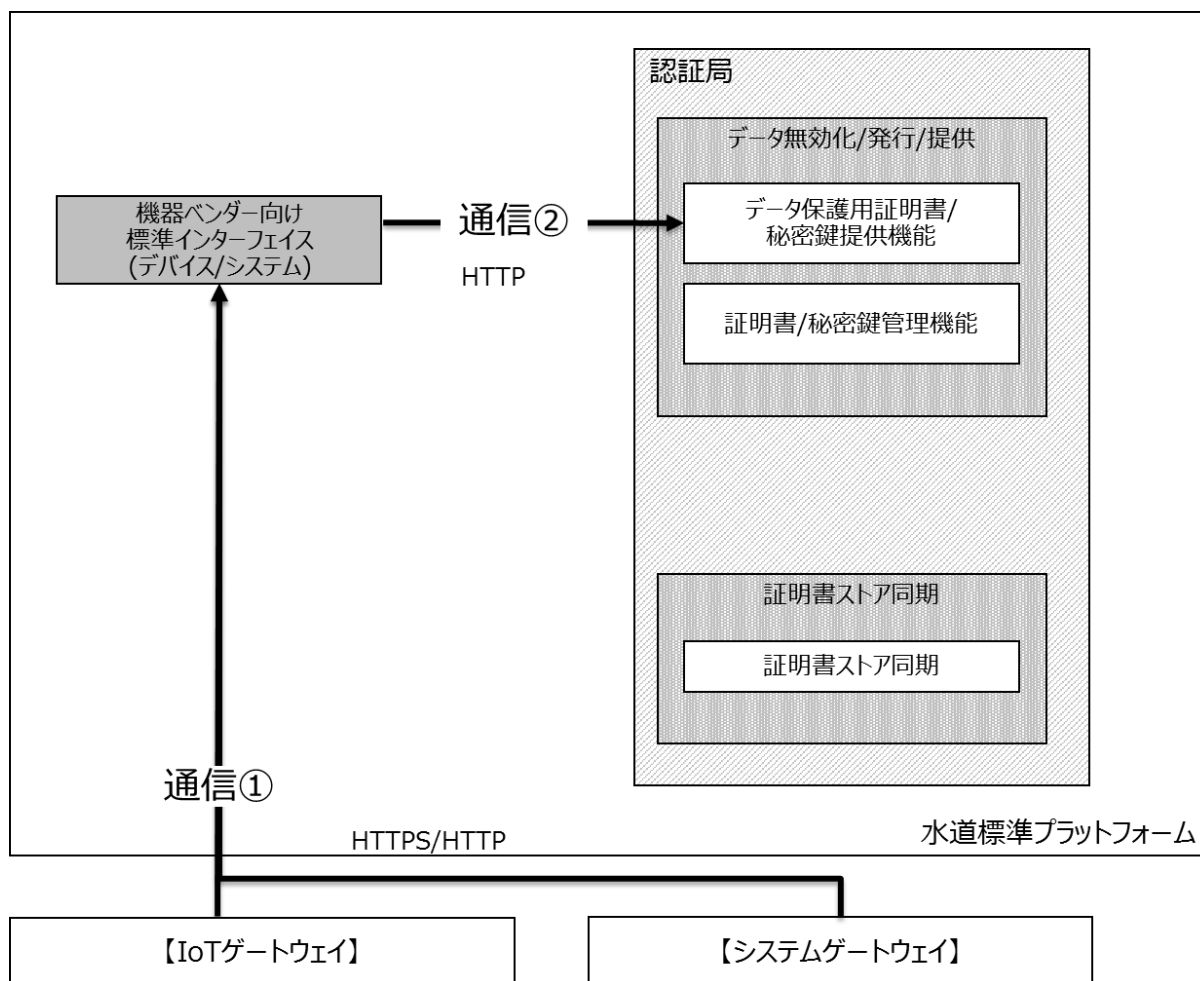


図 4-5: ゲートウェイ向け提供経路

(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 4-4)。

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)。

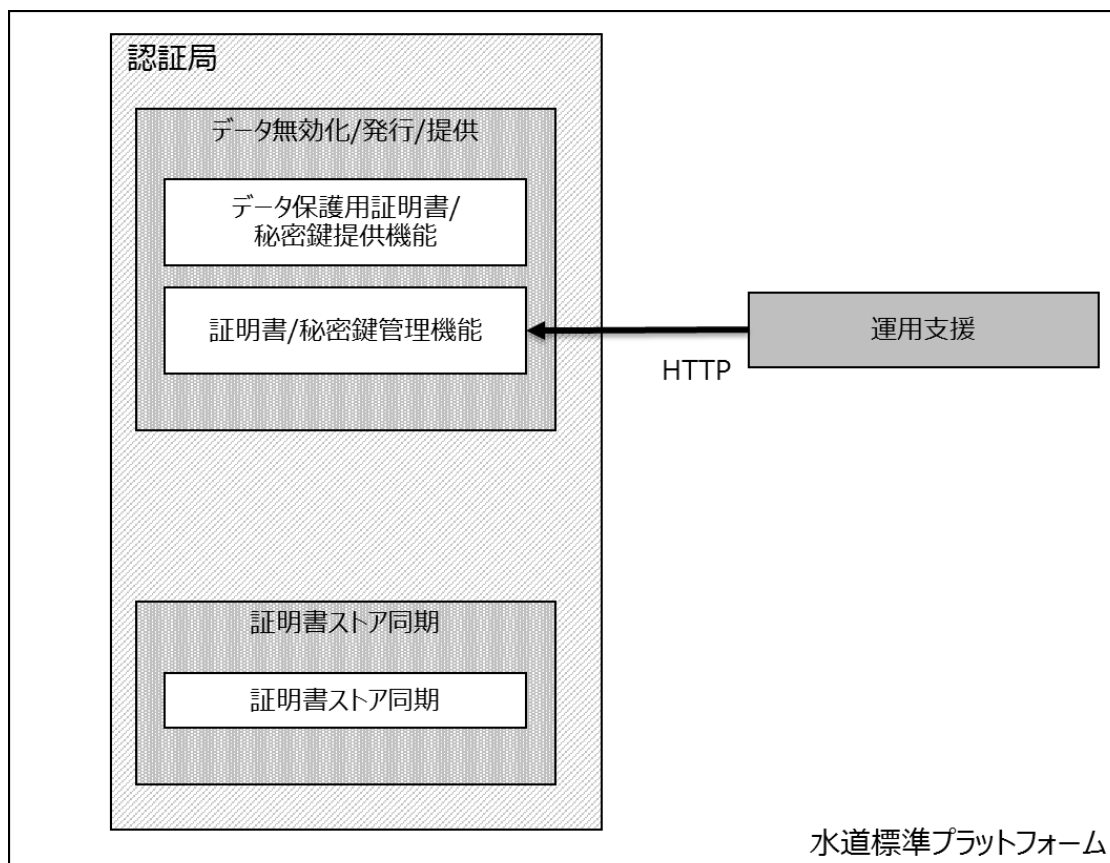


図 4-6: 運用支援向け提供経路

(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。

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)。

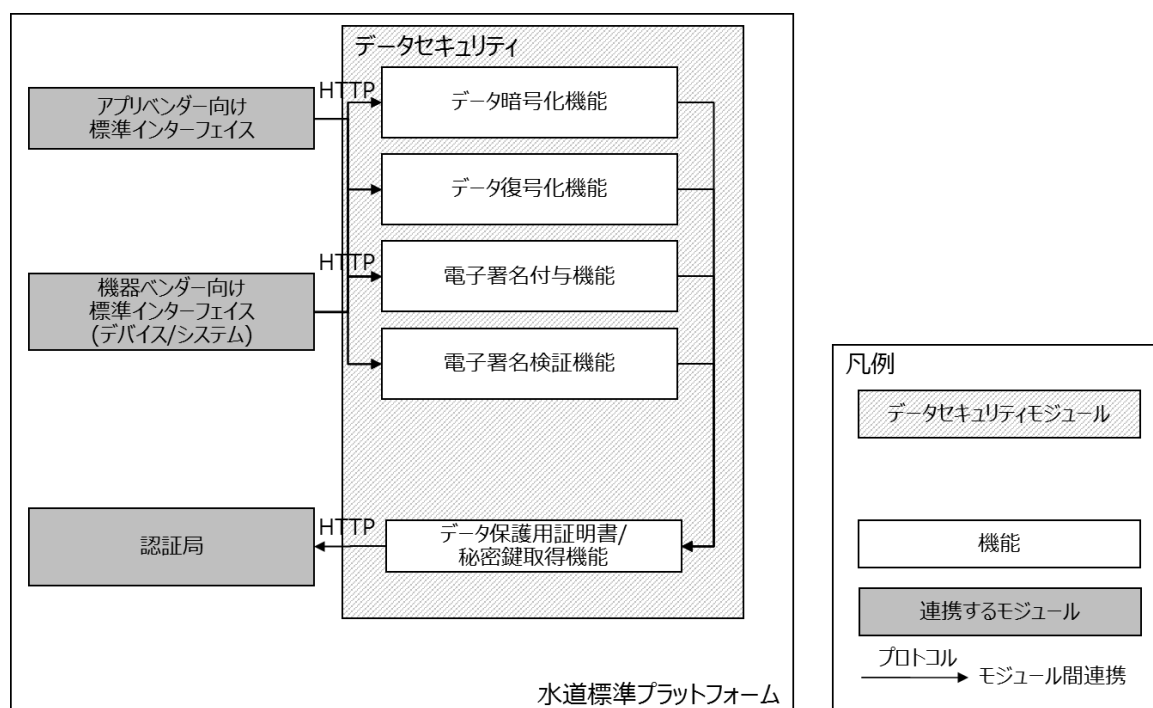


図 5-1: データセキュリティ機能構成

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
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(XML)形式

(a) 概要

データプロファイル(XML)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 5-2、図 5-3)。

【送信側での暗号化処理方式】

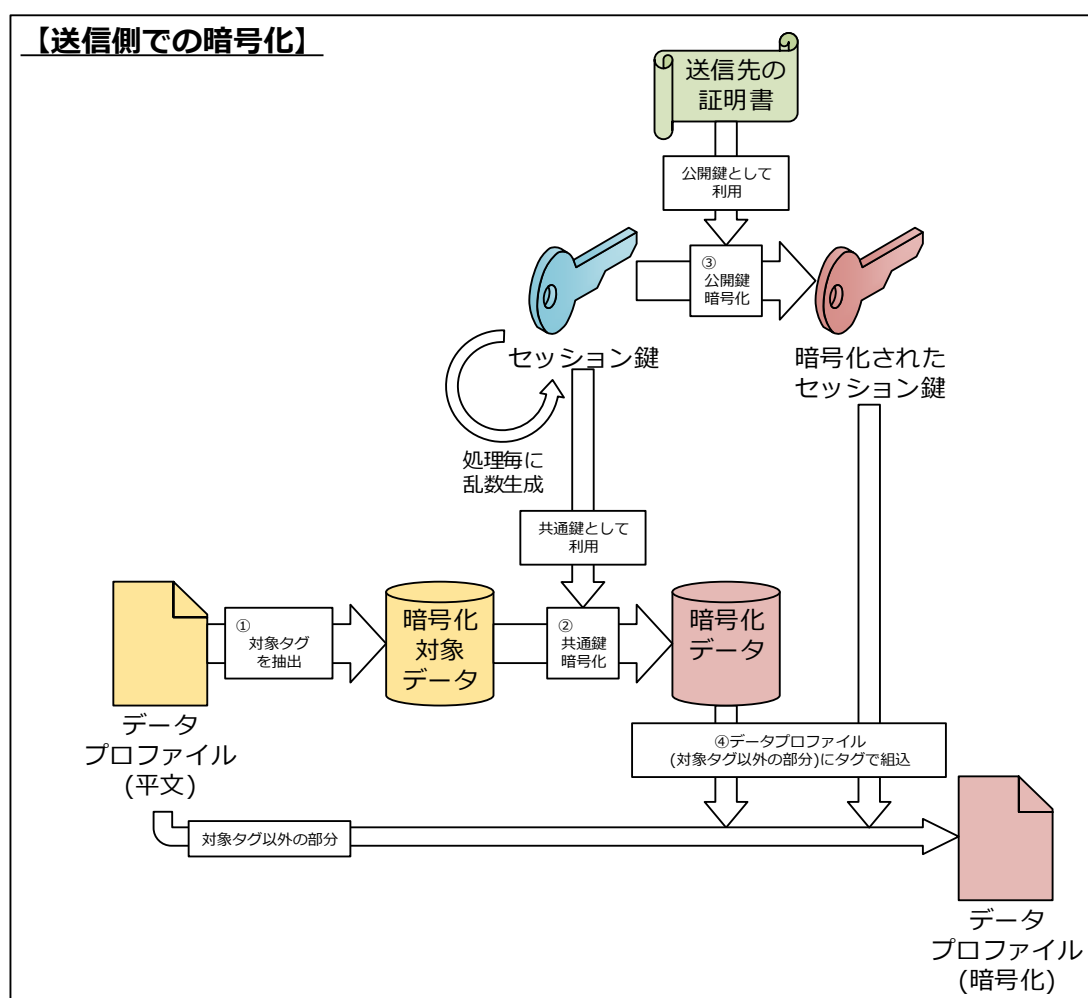


図 5-2:送信側での暗号化処理方式

- ① 「データプロファイル(平文)」から対象のタグを「暗号化対象データ」として抽出する。
- ② 処理毎に乱数生成した「セッション鍵」を共通鍵として、①で抽出した「暗号化対

象データ」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 「送信先の証明書」を公開鍵として、②で利用した「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。
- ④ ②と③で生成した「暗号化データ」と「暗号化されたセッション鍵」をデータプロファイル(対象タグ以外の部分)にタグで組み込んで、「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】

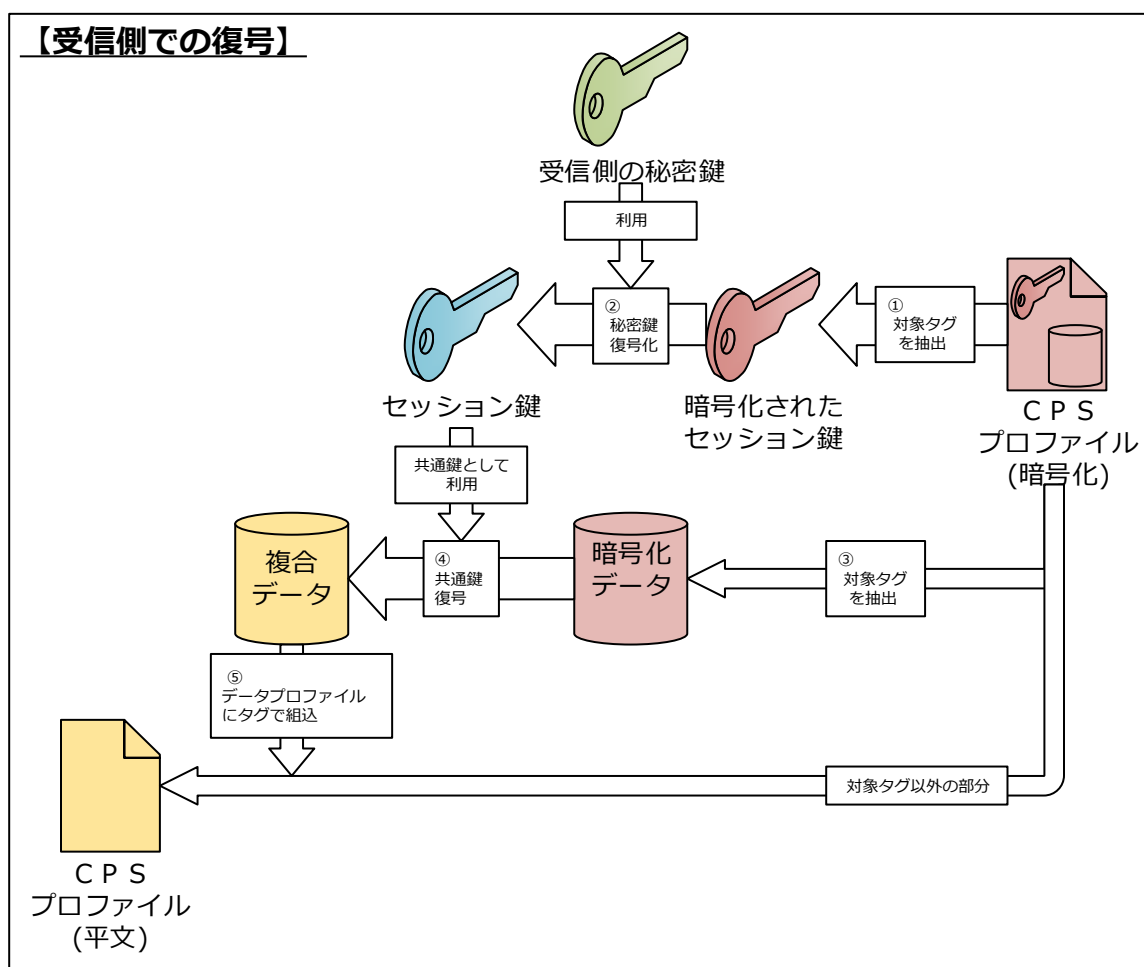


図 5-3:受信側での復号処理方式

- ① 「データプロファイル(暗号化)」から対象のタグを「暗号化されたセッション鍵」として抽出する。
- 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)」から対象のタグを「暗号化データ」として抽出する。
- 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、「復号データ」を生成する。
- ⑤ ④で生成した「復号データ」データプロファイル(対象タグ以外の部分)にタグで組み込んで、「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

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) 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 5-4、図 5-5)。

【送信側での暗号化処理方式】

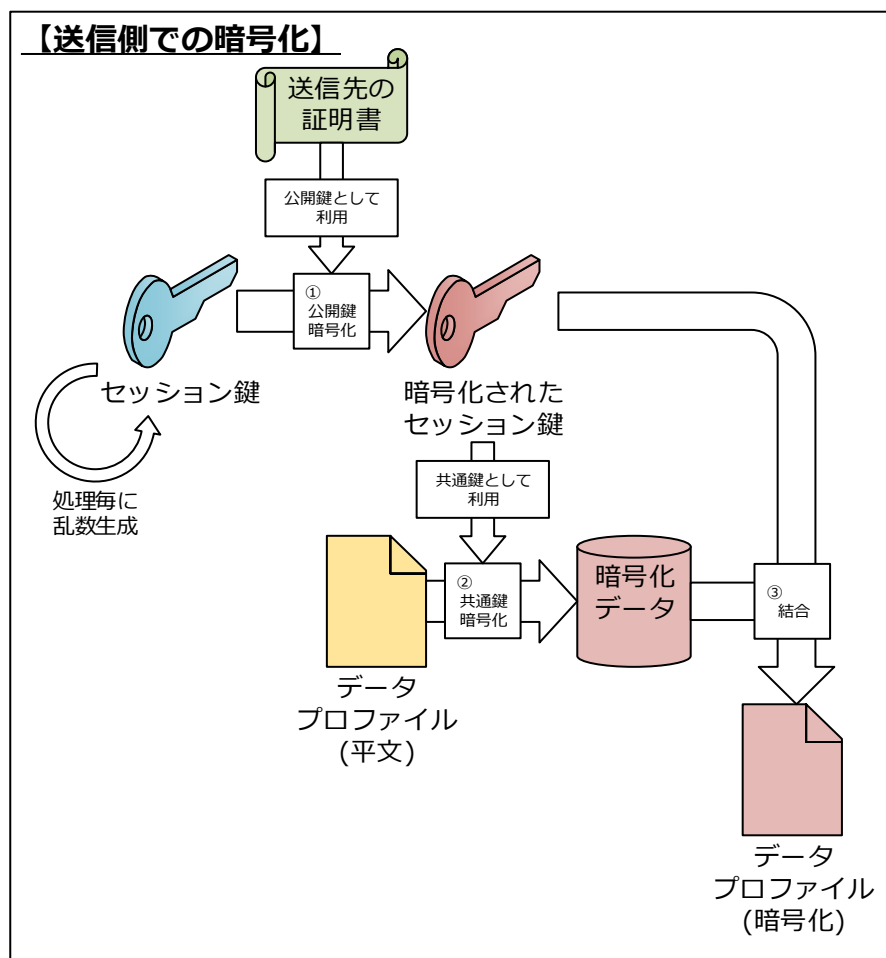


図 5-4: 送信側での暗号化処理方式

- 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、「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】

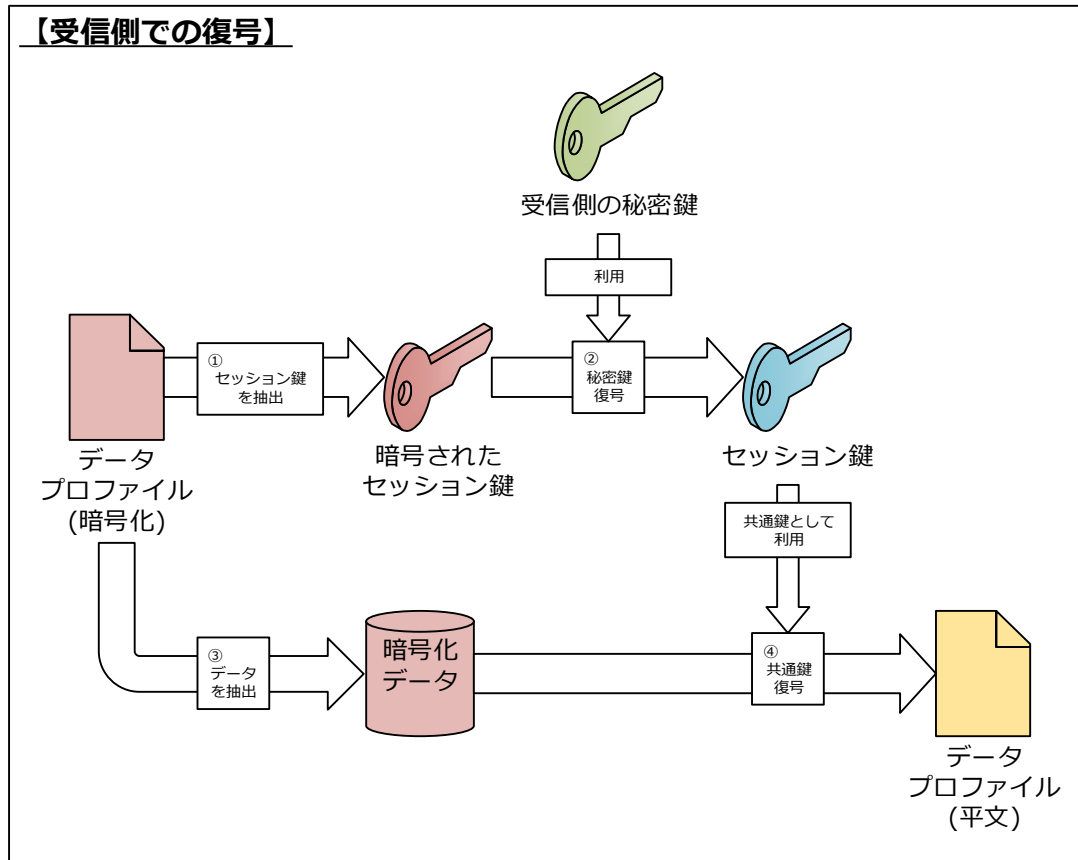


図 5-5: 受信側での復号処理方式

- 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 5-4)。

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
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 5-5)。

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

(3) 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 5-5、図 5-6)。

【送信側での暗号化処理方式】

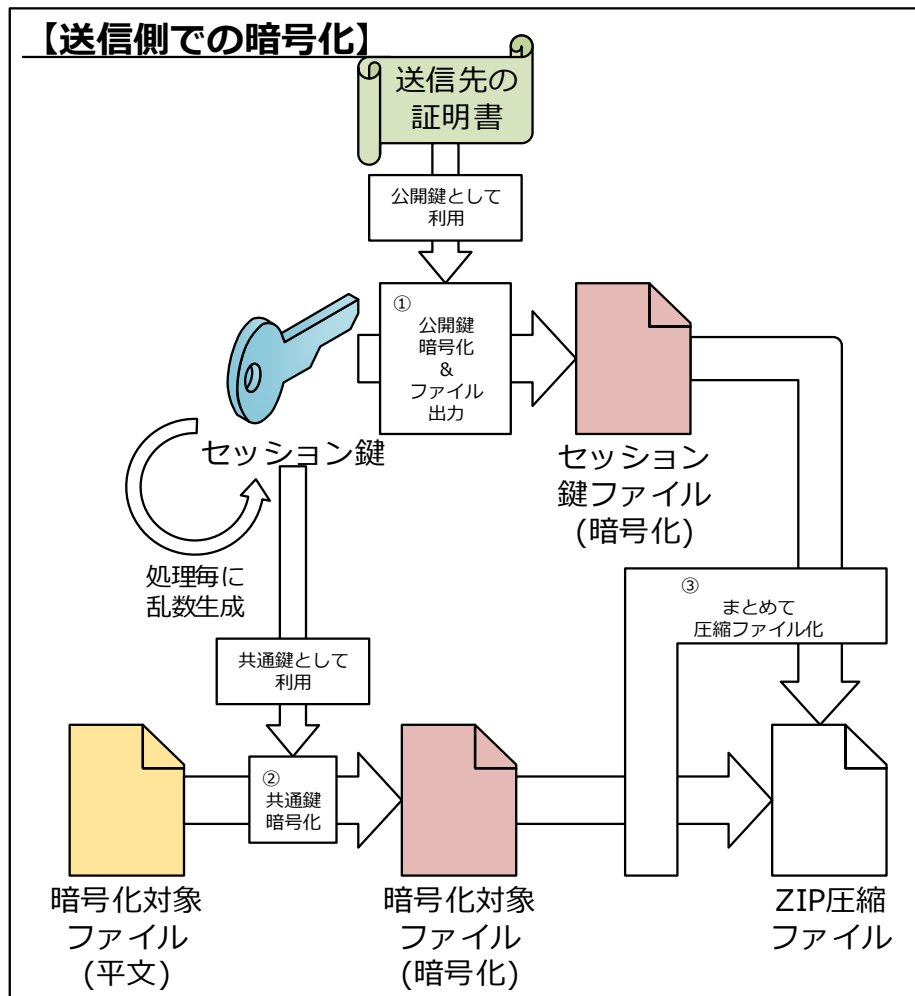


図 5-6: 送信側での暗号化処理方式

- 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】

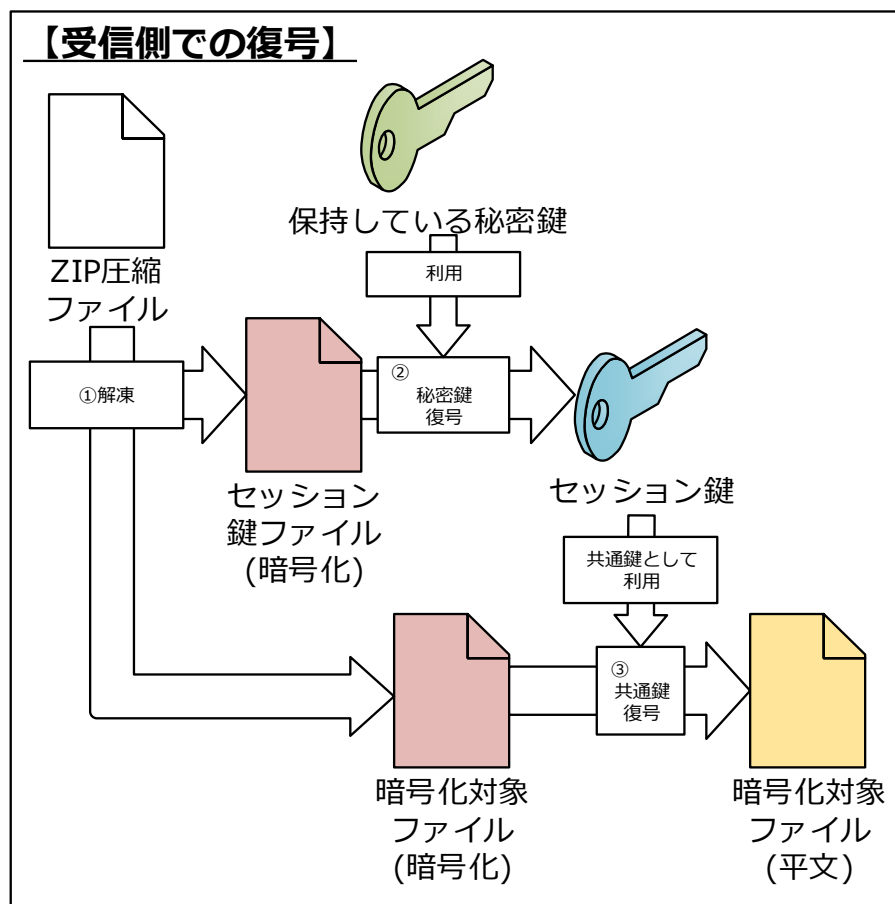


図 5-7:受信側での復号処理方式

- 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 5-6)。

表 5-6: 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 5-7)。

表 5-7: 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(XML)形式

(a) 概要

データプロファイル(XML)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】

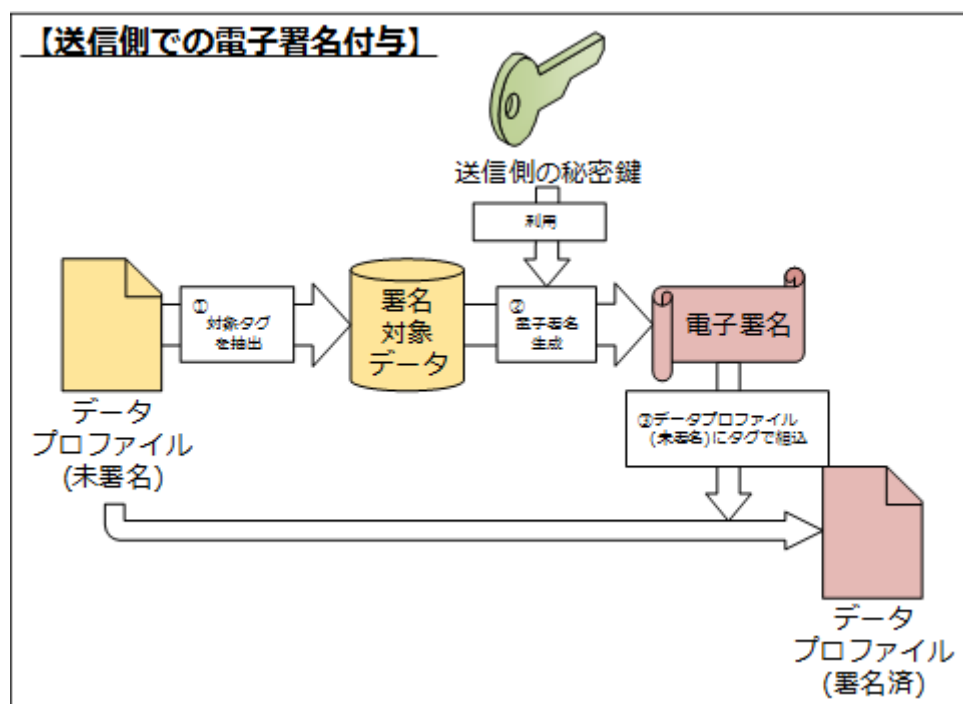


図 5-8:送信側での電子署名付与方式

- ① 「データプロファイル(未署名)」から対象のタグを「署名対象データ」として抽出する。
- ② ①で抽出した「署名対象データ」と「送信側の秘密鍵」を利用して、「電子署名」を生成する。
- ③ ②で生成した「電子署名」をデータプロファイル(未署名)にタグで組み込んで、「データプロファイル(署名済み)」を生成する。

【受信側での電子署名検証方式】

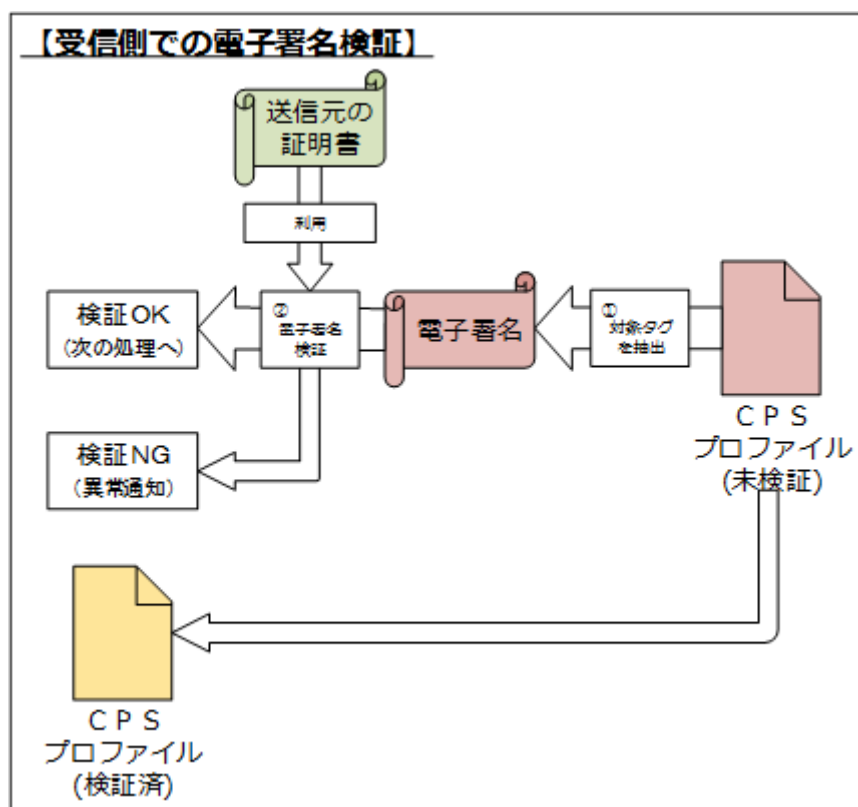


図 5-9:受信側での電子署名検証方式

- ① 「データプロファイル(未検証)」から対象のタグを「電子署名」として抽出する。
- ② 「送信元の証明書」を利用して、①で抽出した「電子署名」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 5-8)。

表 5-8: 電子署名アルゴリズム

項番	区分	方式
1	正規化	Exclusive XML Canonicalization Version 1.0 (omit comments)
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) 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 5-10、図 5-11)

【送信側での電子署名付与方式】

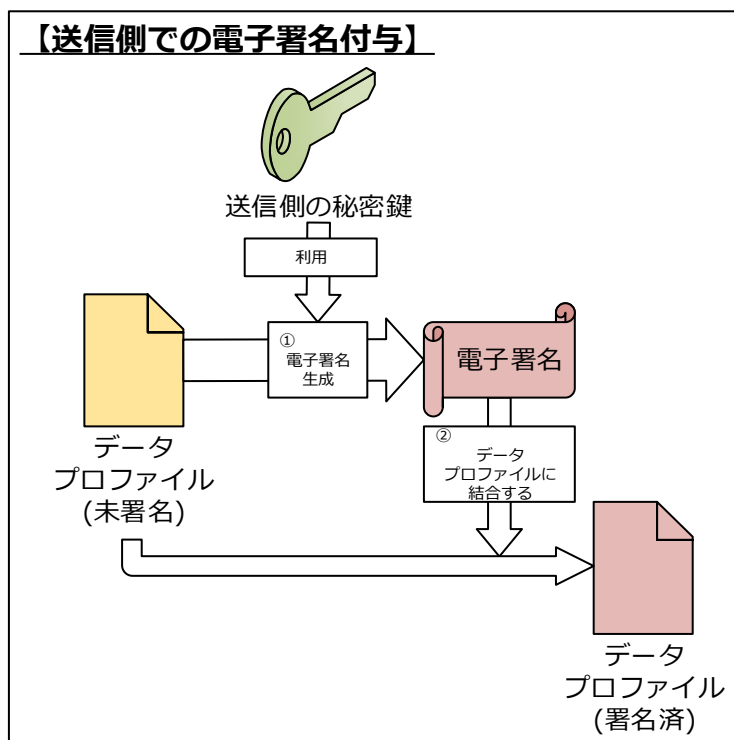


図 5-10: 送信側での電子署名付与方式

- 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】

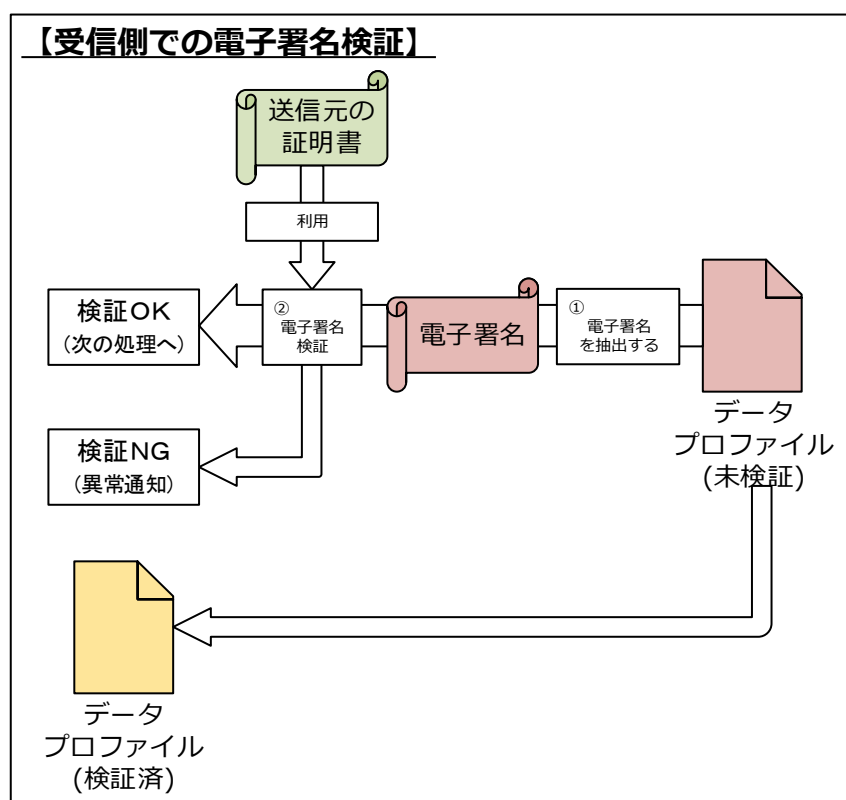


図 5-11:受信側での電子署名検証方式

- 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 5-9)。

表 5-9: 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

(3) 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 5-12、図 5-13)

【送信側での電子署名付与方式】

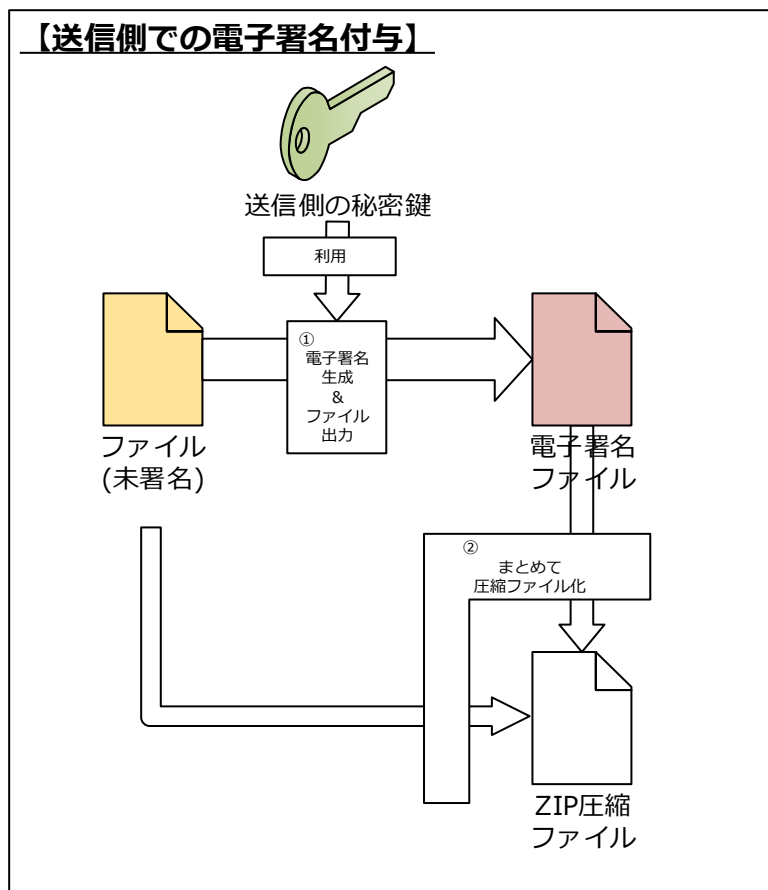


図 5-12: 送信側での電子署名付与方式

- 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】

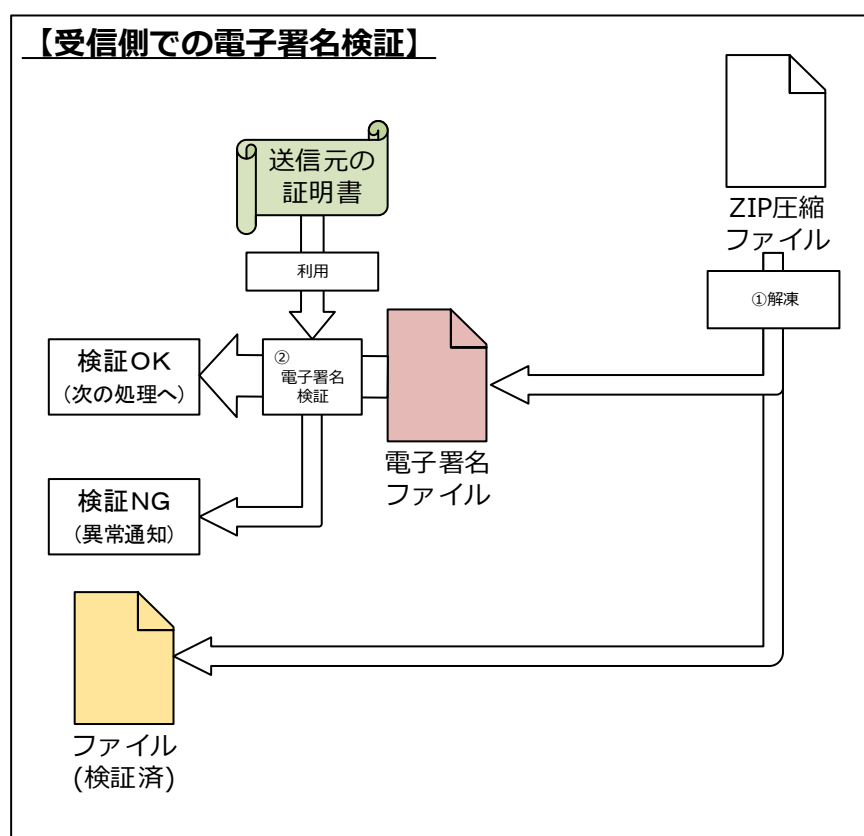


図 5-13:受信側での電子署名検証方式

- 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 5-10)。

表 5-10: 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 5-14)。

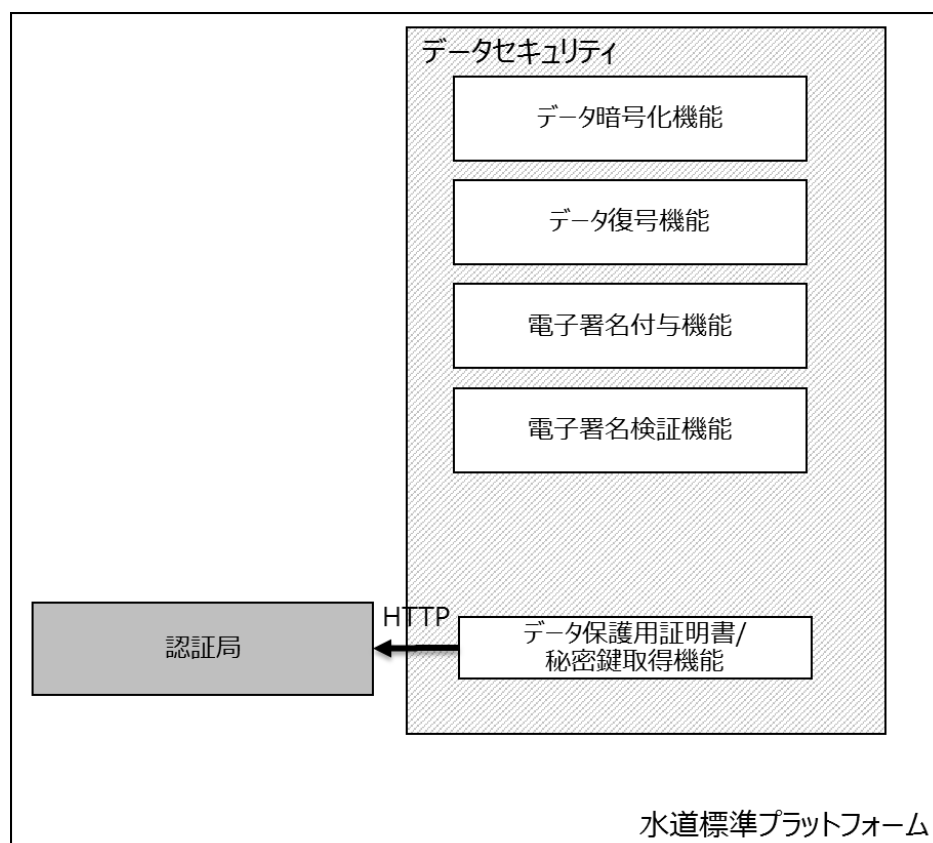


図 5-14 データ保護用証明書/秘密鍵提供機能の提供経路

(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 5-11)。

表 5-11: 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 5-12)。

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)
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 5-13)。

表 5-13: 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 5-15)。

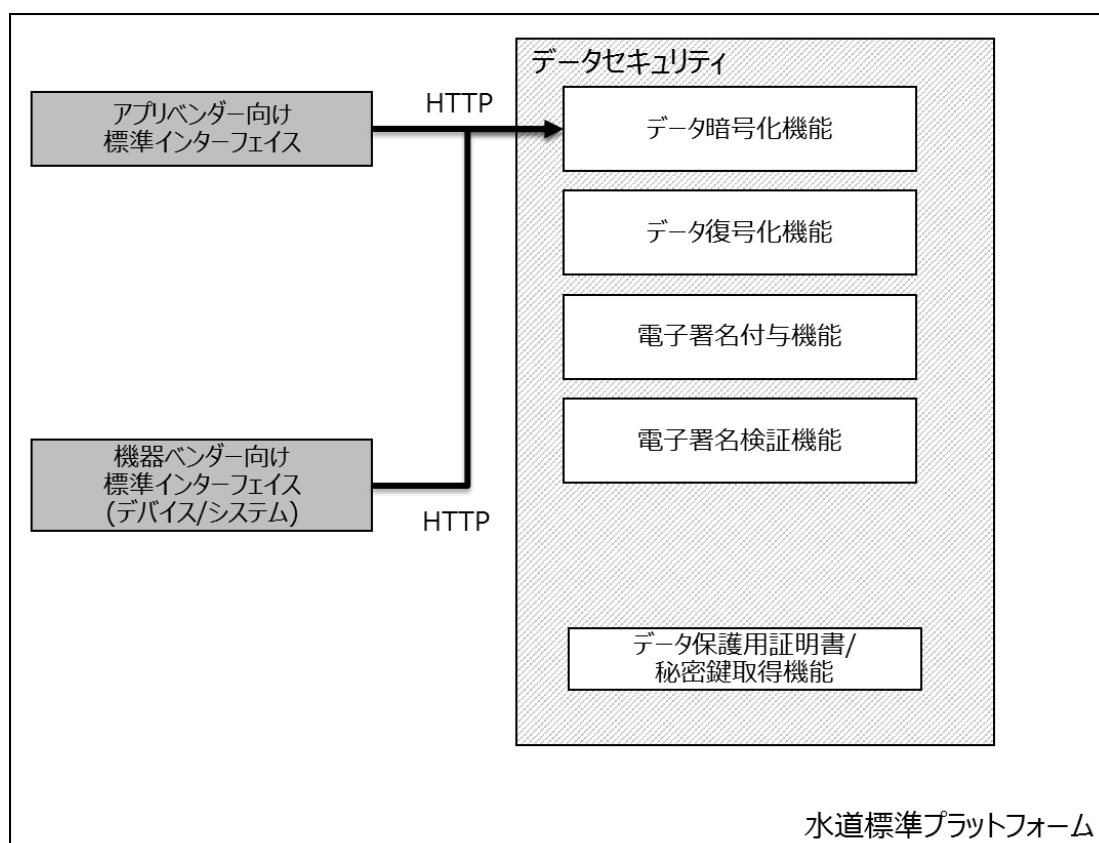


図 5-15 データ暗号化機能の提供経路

(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 5-14)。

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(XML 形式) ・ 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(XML 形式) ・ 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 5-15)。

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(XML 形式)(暗号化済) ・ 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 5-16)。

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(XML)形式データ(暗号化済) 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 5-16)。

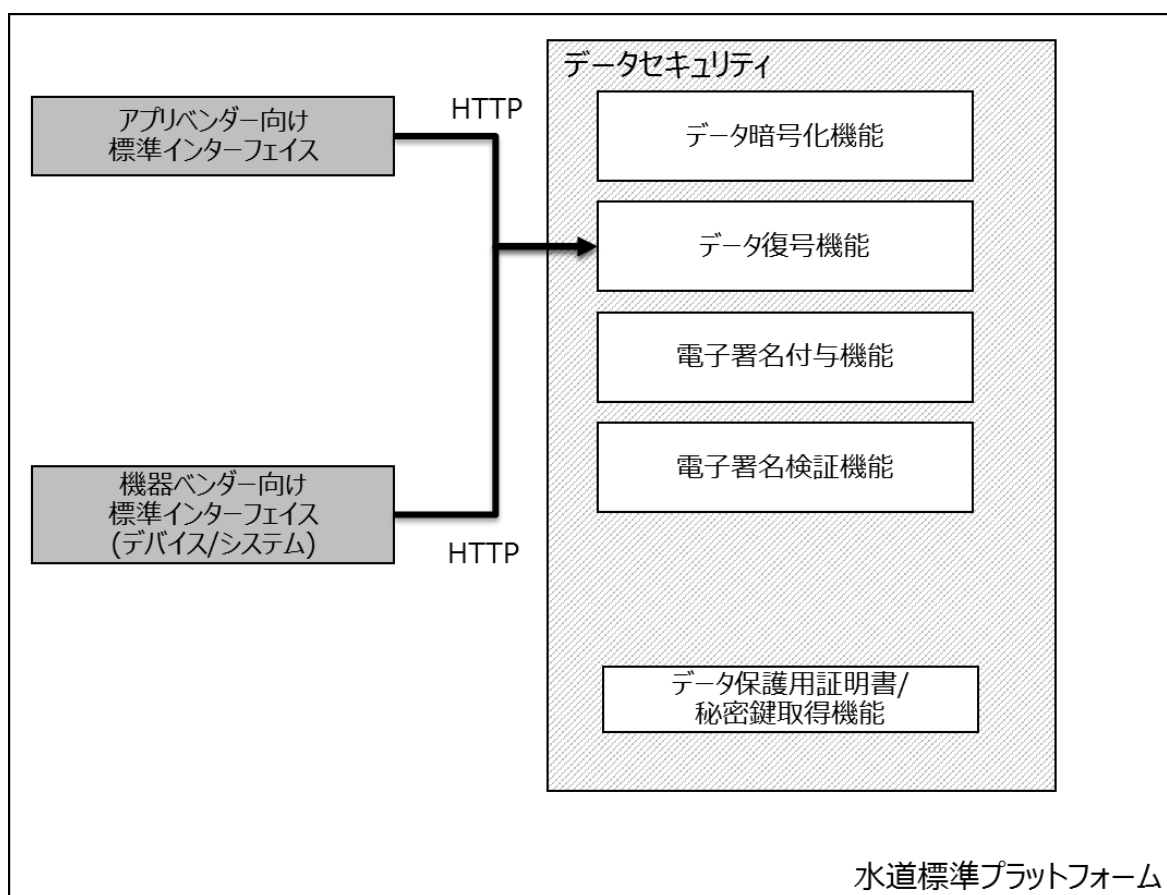


図 5-16: データ復号機能の提供経路

(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 5-17)。

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(XML 形式) ・ 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(XML 形式) (暗号化済) ・ 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 5-18)。

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(XML 形式) ・ 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 5-19)。

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(XML)形式データ 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 5-17)。

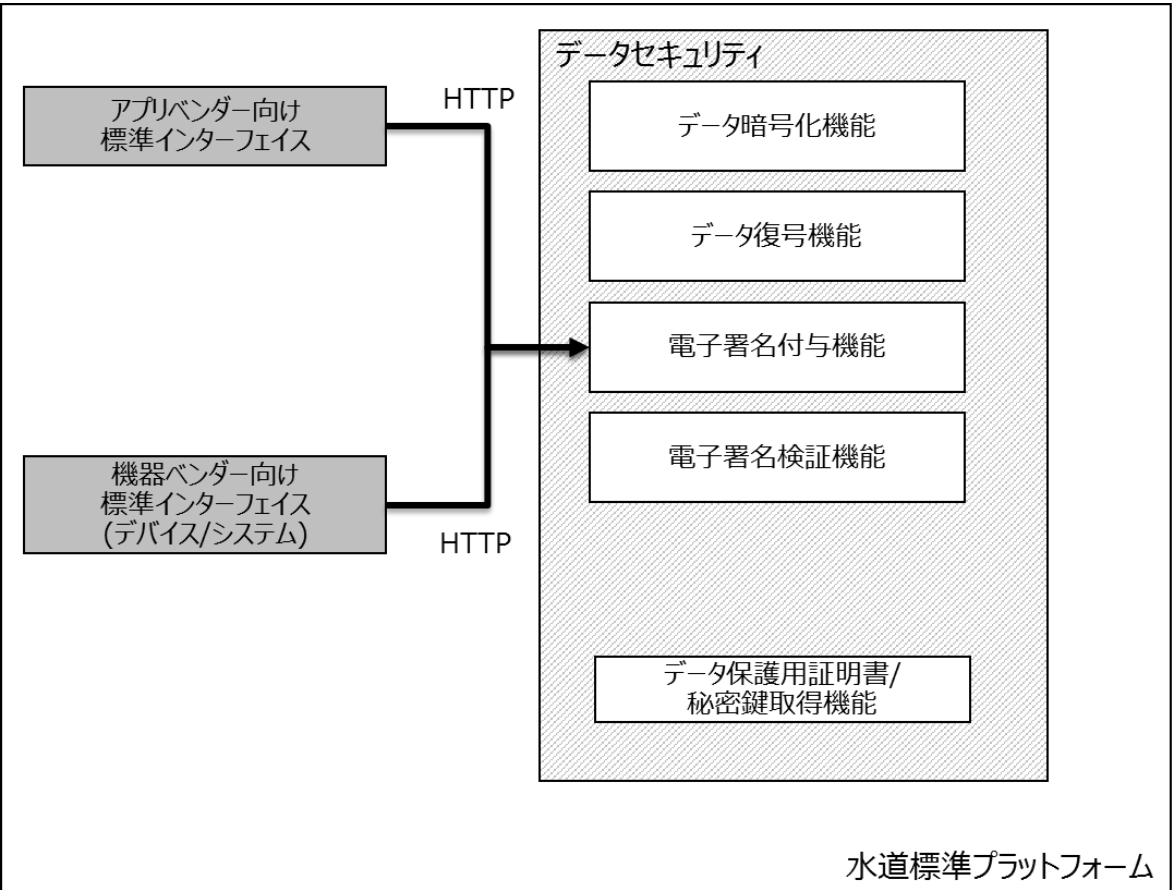


図 5-17: 電子署名付与機能の提供経路

(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 5-20)。

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(XML 形式) ・ 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(XML 形式) ・ 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 5-21)。

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)
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(XML 形式)(電子署名済) ・ 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 5-22)

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	データプロファイル(XML)形式データ(電子署名済) 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 5-18)。

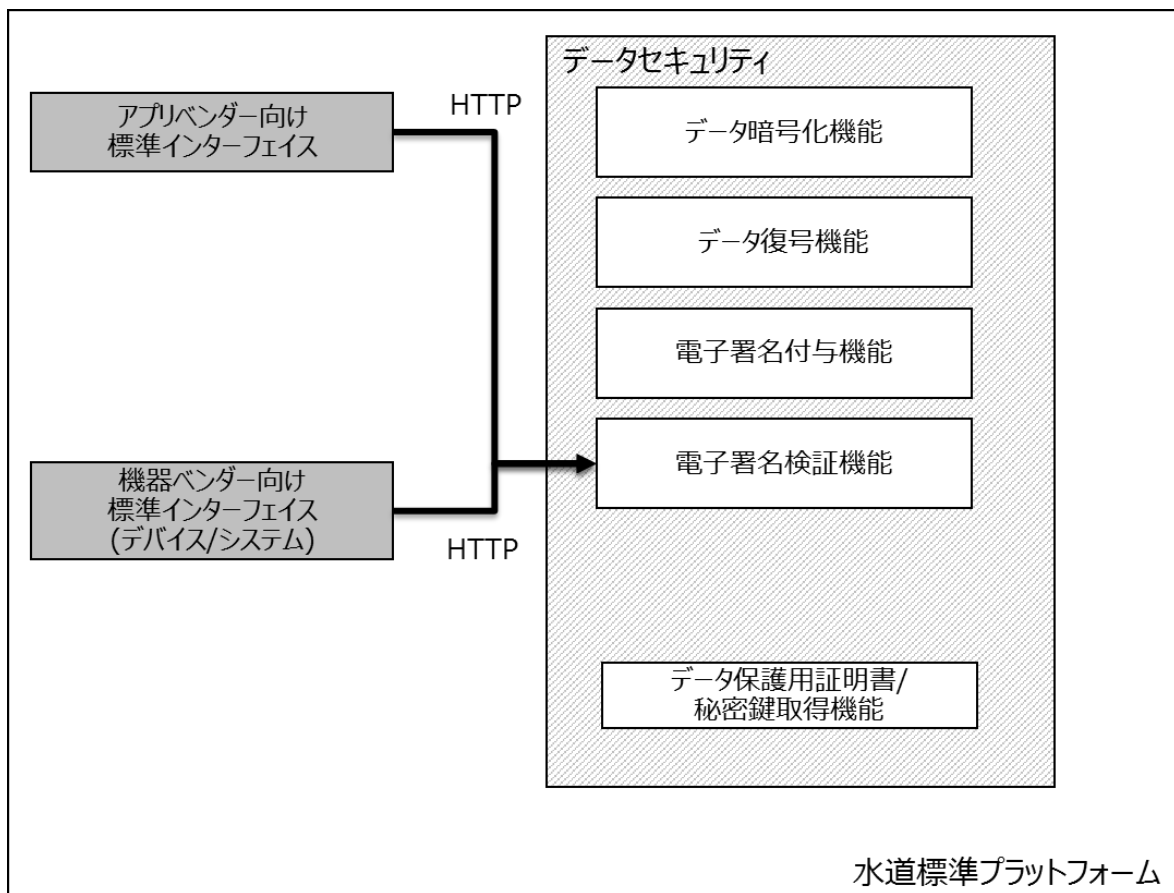


図 5-18: 電子署名検証機能の提供経路

(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 5-23)。

表 5-23: 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(XML 形式) ・ 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(XML 形式)(電子署名済) ・ 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 5-24)。

表 5-24: 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 5-25)。

表 5-25: 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。

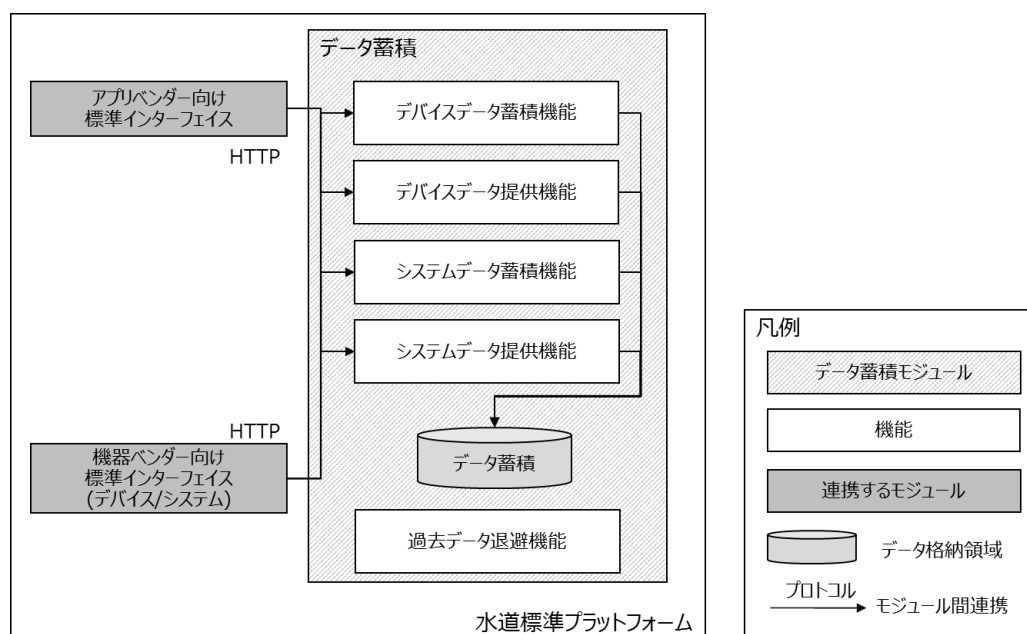


図 6-1: データ蓄積概要

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

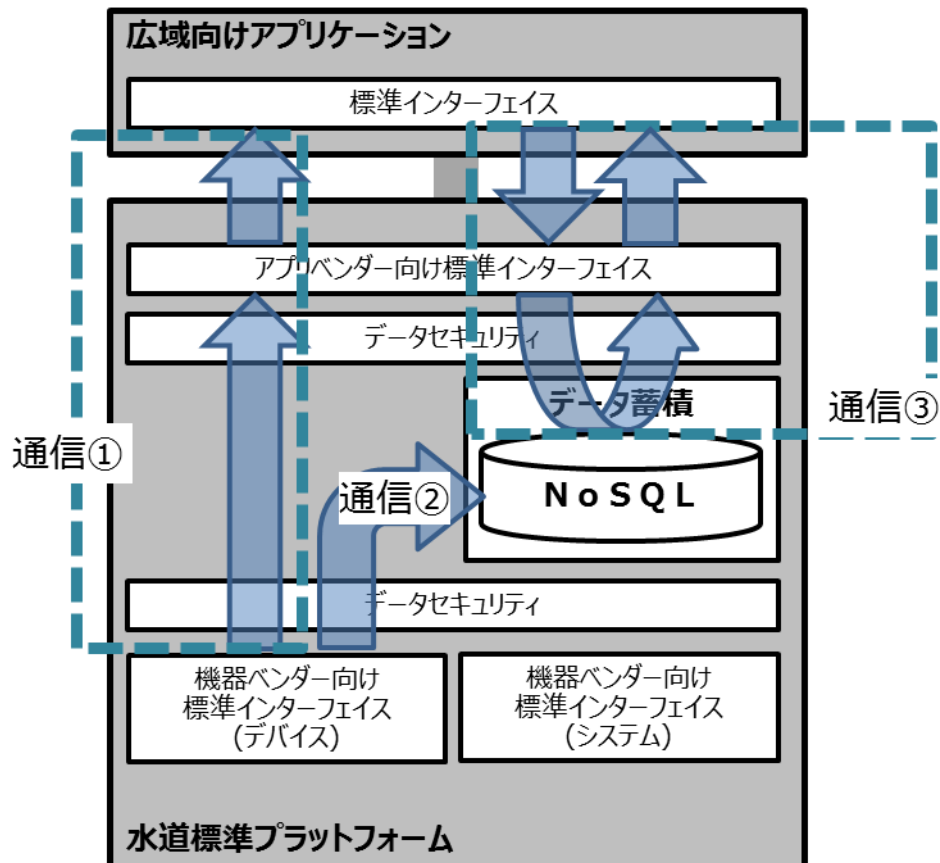


図 6-2: 処理フロー 随時データ取得方式

- ・ (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

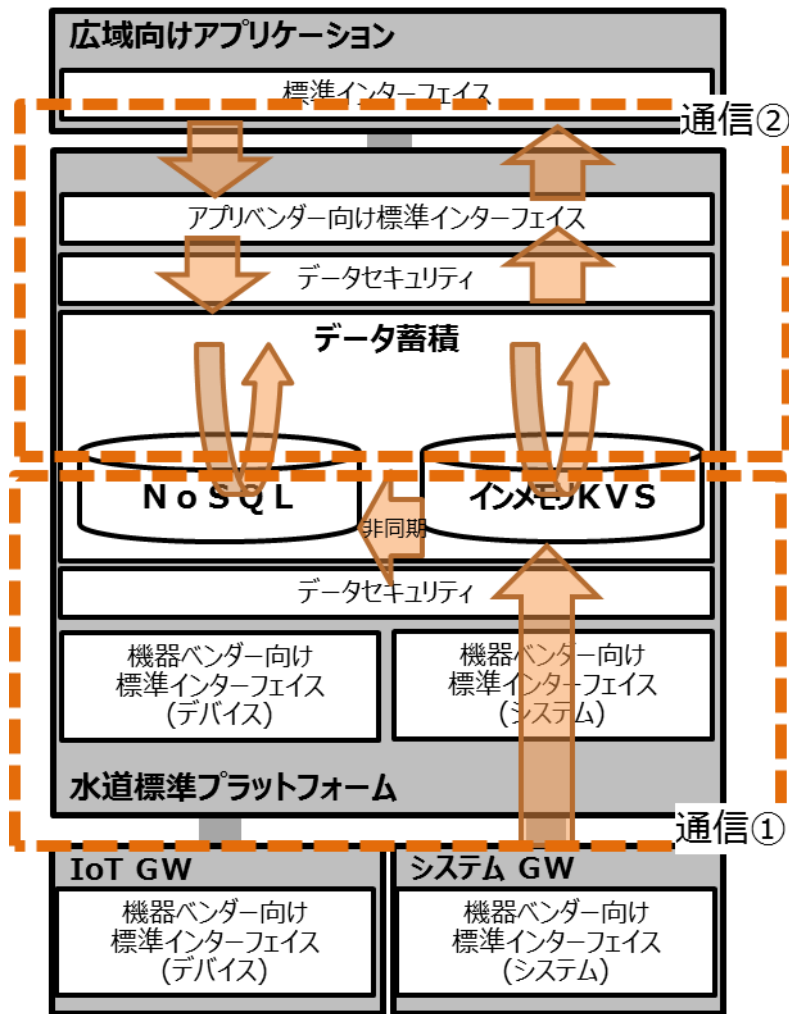


図 6-3: 処理フロー 一括データ取得方式

- ・ (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 6-5 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。

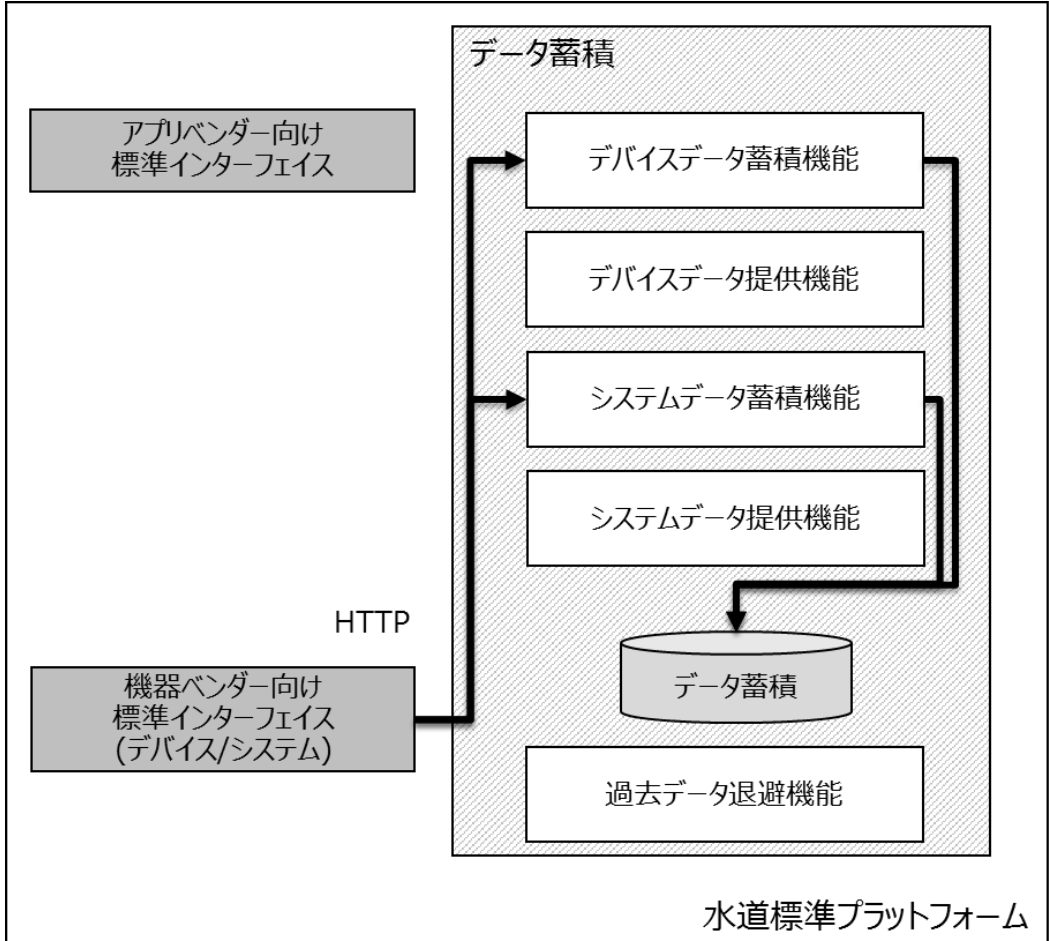


図 6-4: データ蓄積機能概要

(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 4-4)。

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。

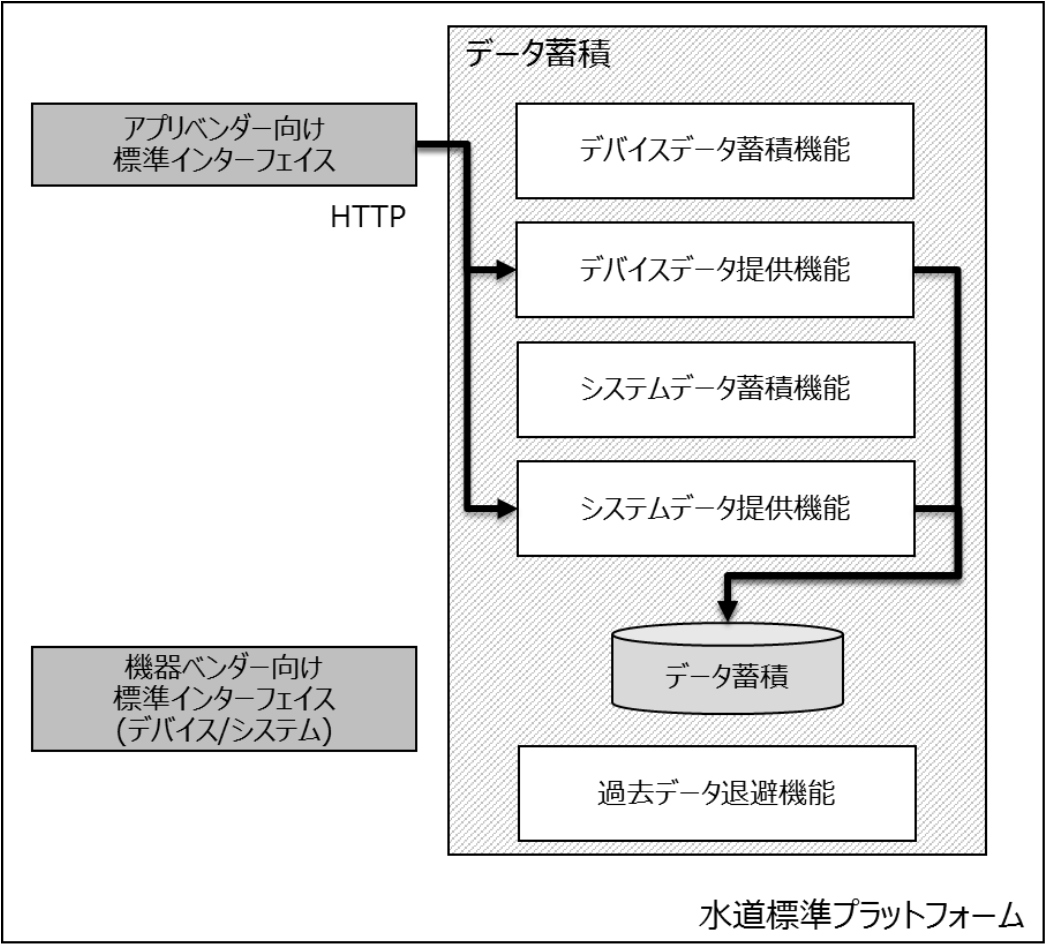


図 6-5: データ提供機能概要

(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 I D	施設 I Dを指定
設備 I D	設備 I Dを指定
機器 I D	機器 I D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 I D	システム I Dを指定
業務 I D	業務 I Dを指定
項目 I D	項目 I D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 データベースを採用する。

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。

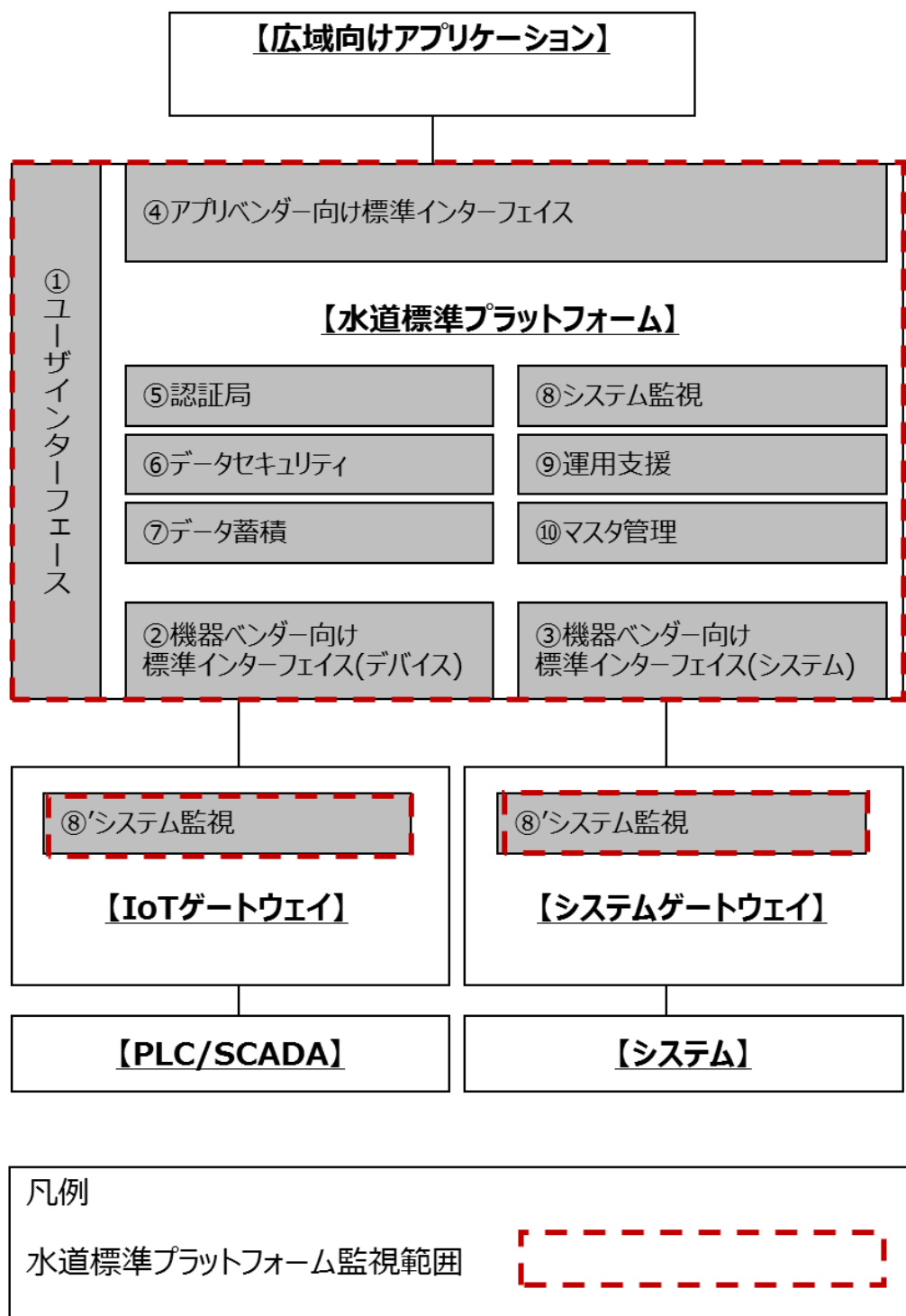


図 7-1:システム監視 監視範囲

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的に監視する。
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的に監視する。
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的に監視する。
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。

システム毎に必要な機能は以下の通り(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的に監視する。 - 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的に監視する。 - 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的に監視する。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)。

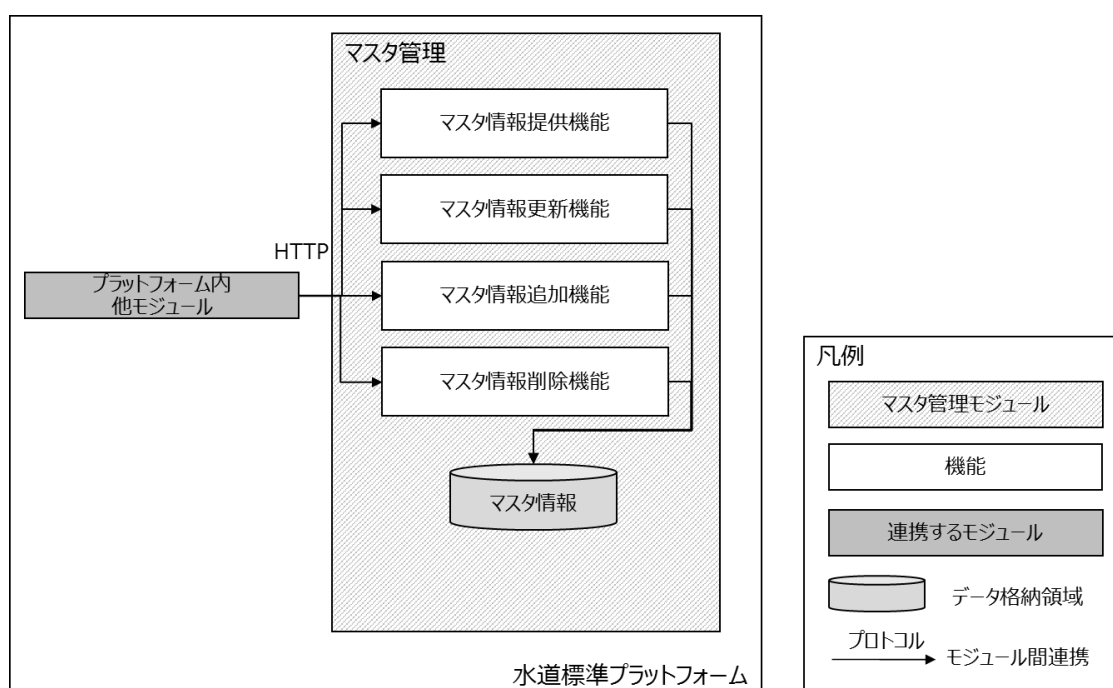


図 8-1 : マスタ管理 機能(モジュール)構成

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テーブル及び条件に合致する情報を抽出し外部機能に提供する。
マスタ情報更新	外部機能より指定されたテーブル及び条件に合致する情報を、指定された内容で更新する。
マスタ情報追加	外部機能より指定された指定されたテーブルに対し、指定されたレコード情報を追加する。
マスタ情報削除	外部機能より指定された指定されたテーブル及び条件に合致する情報を削除する。

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		
	都道府県マスタ	都道府県情報を ID 管理する。
	市区町村マスタ	市区町村情報を ID 管理する。
	事業体マスタ	事業体情報を ID 管理する。
	施設マスタ	施設情報を ID 管理する。
	施設関連マスタ	施設 ID から施設 ID への変換割り当て管理を行う。
	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	機器 ID 毎に接続されるゲートウェイの ID を管理する。
	システムマスタ	システム情報を ID 管理する。
	業務マスタ	業務情報を ID 管理する。
	データ項目マスタ	データ項目情報を ID 管理する。
所在区分管理		
	設備区分マスタ	設備内容を区分管理する。 (取水門(湖水・ダム)、着水井、等々)
	処理区分マスタ	設備毎の実施内容を区分管理する。 (取水、浄水、等々)
	機器区分マスタ	機器内容を区分管理する。 (ポンプ、水位計、等々)
	計測分類マスタ	計測する内容を分類管理する。 (センサ計測値、センサ状態、異常有無)
	計測値区分マスタ	計測分類毎に、計測内容詳細情報を管理する。 ※以下、計測分類毎の管理情報を示す(カッコ書きは管理情報の一例) センサ計測値⇒計測値区分(水位)/単位コード(03) ※1 センサ状態⇒計測値区分(ON/OFF)/状態コード(1) ※2 異常有無⇒計測値区分(軽故障発生)/異常コード(1) ※2 ※1 単位マスタより単位コード変換 ※2 状態・異常変換マスタより状態コード、異常コード変換 ※具体的なコードについては、”基本仕様書 4.5 水道構成モデルと計測データモデル”参照。
	システム区分マスタ	システムの種別を管理管理する。 (公営企業会計システム/水道施設台帳システム、等々)
	業務区分マスタ	業務の種別を管理管理する。 (固定資産台帳/工事台帳/決算/予算関連、等々)

	データ項目区分マスタ	データ項目の種別を管理管理する。 (固定資産番号/ 資産名称/ 会計区分、等々)
コード変換管理		
	単位マスタ	計測値区分マスタで管理される単位情報をコード管理する。 (02⇒m ³ /h、03⇒m、etc.)
	状態・異常変換マスタ	計測値区分毎の状態・異常 値の変換コードを管理する。 ※以下、計測値区分毎の管理情報を示す(カッコ書きは管理情報の一例) V2001(軽故障発生)⇒0(軽故障発生)/1(軽故障回復) V1013(ON/OFF 状態)⇒0(ON)/1(OFF) ※具体的なコードについては、”基本仕様書 5 水道構成モデルと計測データモデル”参照。
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 ID 管理する。
	アプリケーション関連マスタ	事業体毎のアプリケーション ID を紐づけ管理する。
ユーザー権限管理情報		
	ユーザー権限管理情報	
	ユーザマスタ	ユーザー情報を ID 管理する。
	権限ロールマスタ	権限ロール情報を ID 管理する。 (001:全機能使用可能、002:照会のみ、003:照会/制御)
	ユーザー関連マスタ	ユーザーID 毎の権限ロール ID を紐づけ管理する。

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更新の要求を受け付ける。外部機能がマスタ情報更新を要求する際は、取得対象のマスタ種別及び、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
テーブル名	抽出対象のテーブル名を指定する。
抽出条件	事業体 ID 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 番台(正常) 400 番台(異常)
データ	抽出されたデータ

8.2.2 マスタ情報更新

マスタ情報更新機能は以下の処理を実施する。

- 外部機能よりマスタ情報更新の要求を受け付ける。外部機能がマスタ情報更新を要求する際は、更新対象のマスタ種別及び、更新対象の条件、変更する内容を指定する。
- 要求された情報に合致するマスタテーブルの情報に対し、データ更新を行う。

(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 8-5)。

表 8-5: リクエスト概要

項目	内容
テーブル名	更新対象のテーブル名を指定する。
更新内容	更新対象項目、更新内容を指定する。
更新条件	更新条件を指定する。

(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 8-6)。

表 8-6: 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)
更新件数	更新レコード件数を出力する。

8.2.3 マスタ情報追加

マスタ情報追加機能は以下の処理を実施する。

- 外部機能よりマスタ情報追加の要求を受け付ける。外部機能がマスタ情報追加を要求する際は、追加対象のマスタ種別及び、追加対象の条件、追加する内容を指定する。
- 要求された情報に合致するマスタテーブルの情報に対し、データ追加を行う。

(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 8-7)。

表 8-7: リクエスト概要

項目	内容
テーブル名	追加対象のテーブル名を指定する。
追加対象項目	対象項目、内容を指定する。

(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 8-8)。

表 8-8: 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(通常) 400 番台(異常)
追加件数	追加レコード件数を出力する。

8.2.4 マスタ情報削除

マスタ情報削除機能は以下の処理を実施する。

- 外部機能よりマスタ情報削除の要求を受け付ける。外部機能がマスタ情報削除を要求する際は、削除対象のマスタ種別及び、削除対象の条件を指定すること。
- 要求された情報に合致するマスタテーブルの情報に対し、データ削除を行う。

(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 8-9)。

表 8-9: リクエスト概要

項目	内容
テーブル名	削除対象のテーブル名を指定する。
削除条件	削除条件を指定する。

(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 8-10)。

表 8-10: 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(通常) 400 番台(異常)
削除件数	削除レコード件数を出力する。

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

- 以上 -