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

2020 年 3 月

株式会社 JECC（水道施設情報整備促進事業委員会）

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」事業により作成したものに、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」により改訂しました。

株式会社 JECC 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「当社等」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社等の許可なく、それらの宣伝、広告活動に当社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社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、当社等は、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、当社等は、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. 当社等は、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。当社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、本ドキユ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社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

1.1 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. CPS/IoT セキュリティの実装方式.....11

2.1 識別子(ID)の付与.....11
2.2 相互認証と通信経路の暗号化.....13
2.3 アクセス制限.....15
2.3.1 ユーザ認証.....15
2.3.2 広域向けアプリケーションへのアクセス制限.....17
2.3.3 ゲートウェイへのアクセス制限.....18
2.4 データの暗号化.....19
2.4.1 データ送信時のデータ暗号化.....22
2.4.2 データ受信時のデータ復号.....23
2.4.3 暗号アルゴリズムと署名アルゴリズム.....24
2.5 セキュリティ対策の選択.....26
2.6 認定制度.....27

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書の別冊である。

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、基本仕様で規定した基本的に守るべきルールの 1 つである CPS/IoT セキュリティ（水道情報活用システムで対応すべきセキュリティ対策）の詳細仕様を記載したドキュメントである。

水道情報活用システムは水道標準プラットフォームと、それに接続される様々なアプリケーション、ゲートウェイによって構成されるため、流通される事業体のデータを情報漏洩やなりすましによるデータ改ざんから守るためには、アプリケーション開発ベンダー、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、プラットフォーマー、システムインテグレーターの間で水道情報活用システムのセキュリティ仕様を統一し、またシステムとして構築する必要がある。

本ドキュメントでは、水道情報活用システムにおけるセキュリティの詳細仕様を示し、上記の実現を目的とする。

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)。

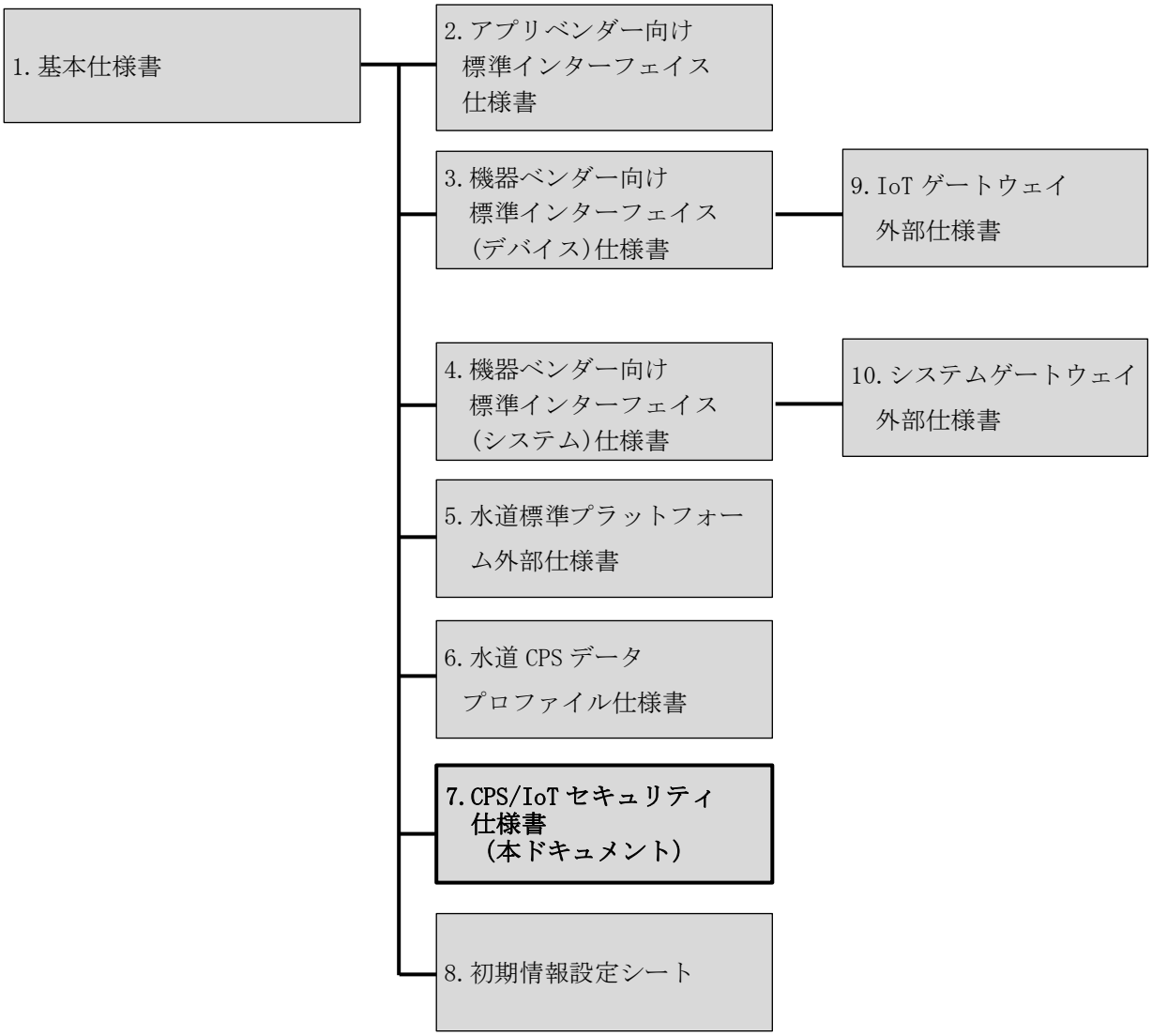

図 1-1: ドキュメント体系図

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)。

CPS/IoT セキュリティ仕様書(本ドキュメント)は、②アプリケーション開発ベンダー、③IoT ゲートウェイ・デバイスベンダー、④システムゲートウェイ・システムベンダー、⑤プラットフォーマー、⑥システムインテグレータ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	⑥
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、※： 未定稿

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為の識別子。

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

本ドキュメントは、水道情報活用システムにおける、CPS/IoT セキュリティ仕様として、CPS/IoT セキュリティの実装方式を示す。

社会インフラ水道情報活用システム標準仕様では､IoT ゲートウェイからデバイスに対して、制御信号などのデバイスの動作に係わる指示を送ることは想定していない。制御信号などを送る場合は、RAS(Reliability、Availability、Serviceability)の観点を十分に考慮した上で、各社の競争領域として設計し、実装すること。

2. CPS/IoT セキュリティの実装方式

水道情報活用システムにおける CPS/IoT セキュリティの実装方式について示す。

2.1 識別子(ID)の付与

水道標準プラットフォームが、不正なユーザーや不正な広域向けアプリケーション、不正なゲートウェイからの接続を防ぎ、デバイス・システムのデータに対するアクセス管理を正しく行うため、水道情報活用システムの構成要素をそれぞれ一意に識別する識別子(ID)を付与する。付与する識別子(ID)を以下に示す。

- テナント ID
- 事業体 ID
- ユーザーID
- アプリケーション ID
- ゲートウェイ ID
- 施設 ID
- 設備 ID
- 機器 ID
- システム ID
- 業務 ID
- データ ID

識別子(ID)の詳細については、基本仕様書 3.1.2 項を参照。

アプリケーション ID とゲートウェイ ID に対して発行される電子証明書の種類と用途を以下に示す(表 2-1)。

表 2-1: 識別子(ID)に対して発行する電子証明書

No.	識別子(ID)	種類	用途
1	アプリケーション ID	アプリケーション証明書 (TLS 用)	広域向けアプリケーションと水道標準プラットフォームの間の通信における「相互認証」や「通信経路の暗号化」で使用する。
2		アプリケーション証明書 (データ保護用)	「データ暗号化」で使用する。
3	ゲートウェイ ID	ゲートウェイ証明書 (TLS 用)	ゲートウェイと水道標準プラットフォームの間の通信における「相互認証」や「通信経路の暗号化」で使用する。
4		ゲートウェイ証明書 (データ保護用)	「データ暗号化」で使用する。

電子証明書の取得方法については、アプリベンダー向け標準インターフェイス仕様書の 2.3 節及び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、機器ベンダー向け標準インターフェイス(システム)仕様書の 2.1 節を参照。

2.2 相互認証と通信経路の暗号化

相互認証と通信経路の暗号化の概略については、基本仕様書に記載されている。
本節では、相互認証と通信経路の暗号化の実施手順について示す。

相互認証と通信経路の暗号化は、水道標準プラットフォームをサーバー、広域向けアプリケーション及び IoT ゲートウェイをクライアントとして、SSL/TLS の仕様に従って実施する。
広域向けアプリケーションやゲートウェイが、水道標準プラットフォームとの通信において、相互認証と通信経路の暗号化で利用する鍵情報及び電子証明書を以下に示す(表 2-2)。

表 2-2: 相互認証と通信経路の暗号化で利用する鍵情報及び電子証明書

No.	種類	取得方法
1	アプリケーション秘密鍵(TLS 用)	アプリケーション開発ベンダーが、プラットフォーマーから取得する。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の 2.3 節を参照。
2	アプリケーション証明書(TLS 用)	
3	サーバールート証明書	
4	サーバー秘密鍵(TLS 用)	プラットフォーマーが保持する。
5	サーバー証明書(TLS 用)	
6	アプリケーションルート証明書	
7	ゲートウェイルート証明書	
8	ゲートウェイ秘密鍵(TLS 用)	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・システムベンダーが、プラットフォーマーから取得する。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)仕様書及び機器ベンダー向け標準インターフェイス(システム)仕様書の 2.1 節を参照。
9	ゲートウェイ証明書(TLS 用)	
10	サーバールート証明書	

広域向けアプリケーションと水道標準プラットフォームとの間の通信開始時の処理において、SSL/TLS の通信手順に従い、通信相手の電子証明書を相互に検証(相互認証)する。同様に IoT ゲートウェイと水道標準プラットフォームとの間の通信開始時の処理において相互認証する。相互認証の完了後、通信経路の暗号化を行い、通信を開始する。

相互認証や通信経路の暗号化においては、中立的な PF の運営組織で運営される認証局 (CA)が発行した証明書を利用する。また、中立的な PF の運営組織で運営される認証局 (CA)が発行した証明書や暗号技術に用いる鍵情報は、必要に応じて、耐タンパー性を持つ領域に格納し、外部からの不正アクセスや改ざんを防止することで、セキュリティを向上させることも可能である。

なお水道標準プラットフォームでは、定期的に証明書のバージョンを最新化するが、古いバージョンの証明書を一定期間保持するため、広域向けアプリケーションやゲートウェイが古いバージョンの証明書でも対応可能とする。（図 2-1）

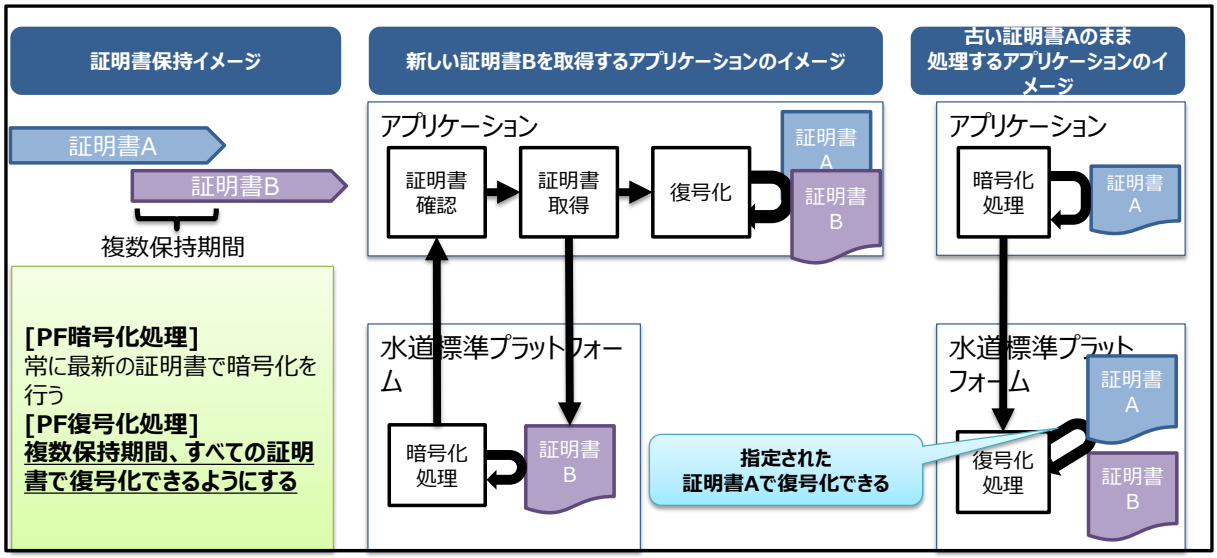

図 2-1：証明書の複数バージョン保持による処理イメージ

なお、広域向けアプリケーションは、事業体ユーザーとの間の通信においても同レベルの通信暗号化を実施する。

2.3　アクセス制限

アクセス制限の概略については、基本仕様書に記載されている。本節では、アクセス制限の実施手順と具体例について示す。

事業体ユーザーが広域向けアプリケーションを利用する際には、水道標準プラットフォームでユーザー認証を実施する。ユーザー認証の結果は、ユーザーがデータにアクセスする際の制御に利用される。水道標準プラットフォームは、ユーザー認証の結果を利用して、そのユーザーがアクセス可能なゲートウェイ、広域向けアプリケーションであるかを判別し、アクセス制限を行う。

2.3.1　ユーザ認証

ユーザー認証の例を以下に示す(図 2-2)。

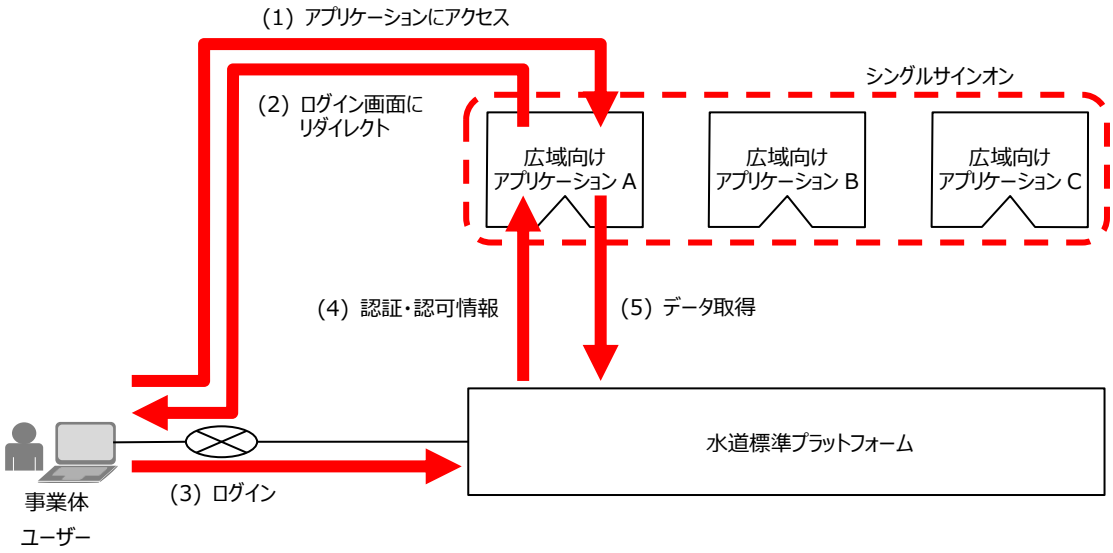

図 2-2: 水道情報活用システムにおけるユーザー認証の例

広域向けアプリケーションは、アプリベンダー向け標準インターフェイスを呼び出す際、アクセストークン等の認証・認可情報を使用する。認証・認可情報は水道標準プラットフォームで以下の通り評価される。

- ユーザー認証：登録されたユーザーのアクセスか否か
- アクセス制御：アクセスしようとしているデータに対してアクセス権限があるか否か

認証方式は OpenID Connect とする。OpenID Connect の方式においては、水道標準プラットフォームがリソースサーバー(サービスプロバイダー)、広域向けアプリケーションがクライア

ントに該当する。広域向けアプリケーションは、認証リダイレクト URL の実装等、OpenID Connect に必要な機能を実装する。

OpenID Connect の仕様により、広域向けアプリケーションにアクセストークンが付与されたタイミングで、ID トークンも同時に付与される。ID トークンは Json Web Token(JWT)形式のトークンであり、トークン上に含まれるユーザー情報を利用して、広域向けアプリケーションで独自の認可処理に利用できる。

広域向けアプリケーションは、OpenID Connect に準拠したアクセス先(トークンエンドポイントやユーザー情報エンドポイント)を利用できる(表 2-3)。

表 2-3: 利用可能なアクセス先(エンドポイント)の URL

No.	項目	内容※
1	トークンエンドポイント	https://[水道標準プラットフォームのホスト名]/auth/realms/[レルム名]/protocol/openid-connect/token
2	ユーザー情報エンドポイント	https://[水道標準プラットフォームのホスト名]/auth/realms/[レルム名]/protocol/openid-connect/userinfo

※: [水道標準プラットフォームのホスト名]と[レルム名]はプラットフォーマーに確認する。

2.3.2 広域向けアプリケーションへのアクセス制限

広域向けアプリケーションへのアクセス制限では、ユーザーが所属する事業体で利用する広域向けアプリケーションに対してのみログインできるように制限する。これにより、広域向けアプリケーション内のデータは、他の事業体のユーザーによるアクセスから保護される。広域向けアプリケーションへのアクセス制限の例を以下に示す(図 2-3)。

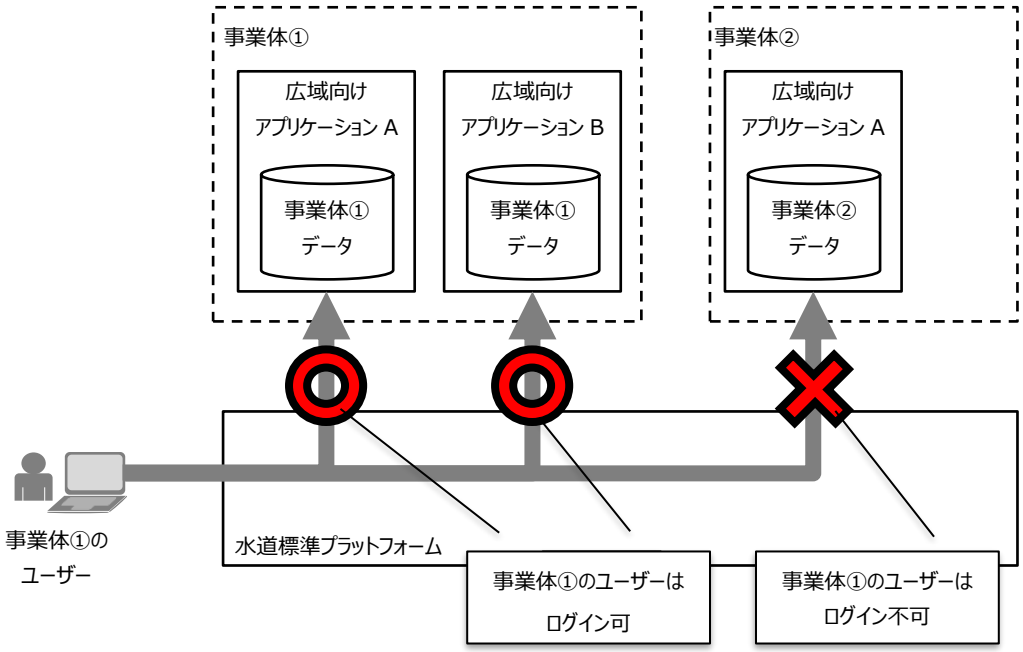

図 2-3: 広域向けアプリケーションへのアクセス制限の例

2.3.3 ゲートウェイへのアクセス制限

ゲートウェイへのアクセス制限では、ユーザーが所属する事業体で登録申請したゲートウェイに対してのみアクセスできるように制限する。これによりゲートウェイは、他の事業体のユーザーによるアクセスから保護される。ゲートウェイへのアクセス制限の例を以下に示す(図2-4)。

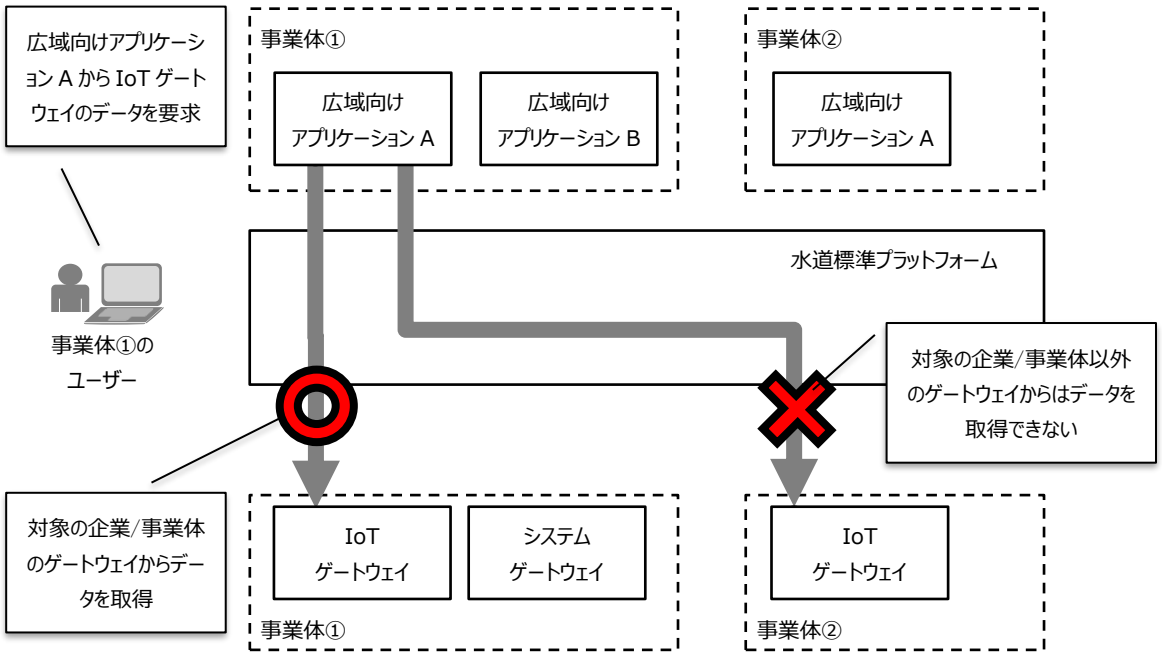

図 2-4: ゲートウェイへのアクセス制限の例

2.4 データの暗号化

データの暗号化の概略については、基本仕様書に記載されている。
本節では、データの暗号化の実施手順について示す。

通信経路での盗聴だけでなく、水道情報活用システム内での盗聴を防ぐためには、通信経路の暗号化に加えて、データそのものを暗号化することが必要となる。重要なデータを暗号化することで、流通する経路や一時保存の環境に依らず、データの機密性を確保することが可能となる。

送受信するデータに適用するデータプロファイルの構成概要を以下に示す(図 2-5)。

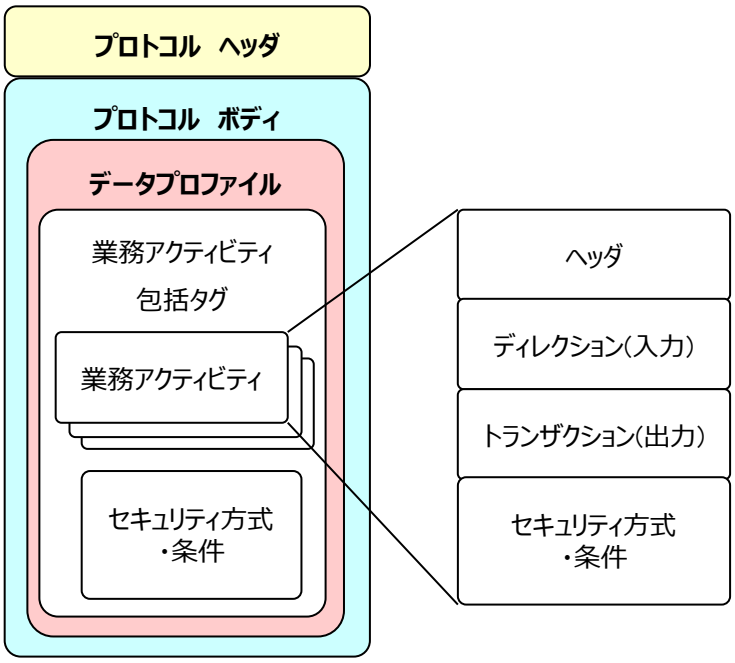

図 2-5: データプロファイルの構成概要

データ暗号化では、データプロファイルのディレクション(入力)、トランザクション(出力)の一部または全てを暗号化する。具体的な暗号化の範囲は、セキュリティ強度と利便性を考慮し、データプロファイルで実装する。暗号化の範囲は、水道 CPS データプロファイル仕様書の 2.3.3 項および 2.3.4 項を参照。

データ暗号化で利用する鍵情報及び電子証明書を以下に示す(表 2-4)。

表 2-4: データ暗号化と利用する鍵情報及び電子証明書

No.	種類	取得方法	利用箇所
1	アプリケーション秘密鍵(データ保護用)	アプリケーション開発ベンダーが、プラットフォーマーから取得する。	プラットフォームから受信したデータを復号化する際に利用する。この秘密鍵は、No.4-1のアプリケーション用公開鍵証明書（データ保護用）に対応する。
2	アプリケーション証明書(データ保護用)	プラットフォーマーが保持する。	プラットフォームから、アプリケーションにデータ送信する際の暗号化の際に利用する。
3	サーバー秘密鍵(データ保護用)	プラットフォーマーが保持する。	アプリケーションまたはゲートウェイから受信したデータを復号化する際に利用する。
3-1	アプリケーション用		この秘密鍵は、No.2のアプリケーション用公開鍵証明書（データ保護用）に対応する。
3-2	ゲートウェイ用		この秘密鍵は、No.6のゲートウェイ用公開鍵証明書（データ保護用）に対応する。
4	サーバー証明書(データ保護用)	プラットフォーマーが保持する。	プラットフォームから受信したデータを復号化する際に利用する。この証明書は、No.1のアプリケーション秘密鍵(データ保護用)に対応する。
4-1	アプリケーション用	証明書ファイル取得 IF にて取得する。	アプリケーションから、プラットフォームにデータ送信する際の暗号化の際に利用する。
4-2	ゲートウェイ用		ゲートウェイから、プラットフォームにデータ送信する際の暗号化の際に利用する。
5	ゲートウェイ秘密鍵(データ保護用)	IoT ゲートウェイ・デバイスベンダー及びシステムゲートウェイベンダーが、プラットフォーマーから取得する。	プラットフォームから受信したデータを復号化する際に利用する。この秘密鍵は、No.4-2のゲートウェイ用公開鍵証明書(データ保護用)に対応する。

No.	種類	取得方法	利用箇所
6	ゲートウェイ証明書(データ保護用)	プラットフォーマーが保持する。	プラットフォームから、ゲートウェイにデータ送信する際の暗号化の際に利用する。
7	セッション鍵	広域向けアプリケーションまたはゲートウェイおよびプラットフォームにおいて通信毎に生成する。	データ送信する側がデータ暗号化の際に共通鍵として利用する。
7-1	アプリケーションからプラットフォームへ通信用	アプリケーションにて生成	
7-2	プラットフォームからアプリケーションへ通信用	プラットフォームにて生成	
7-3	プラットフォームからゲートウェイへ通信用	プラットフォームにて生成	
7-4	ゲートウェイからプラットフォームへ通信用	ゲートウェイにて生成	

2.4.1 データ送信時のデータ暗号化

(1) データ暗号化の付与の処理順

広域向けアプリケーション及びゲートウェイがデータ送信をする際の、データ暗号化の付与の処理順を以下に示す(図 2-6)。

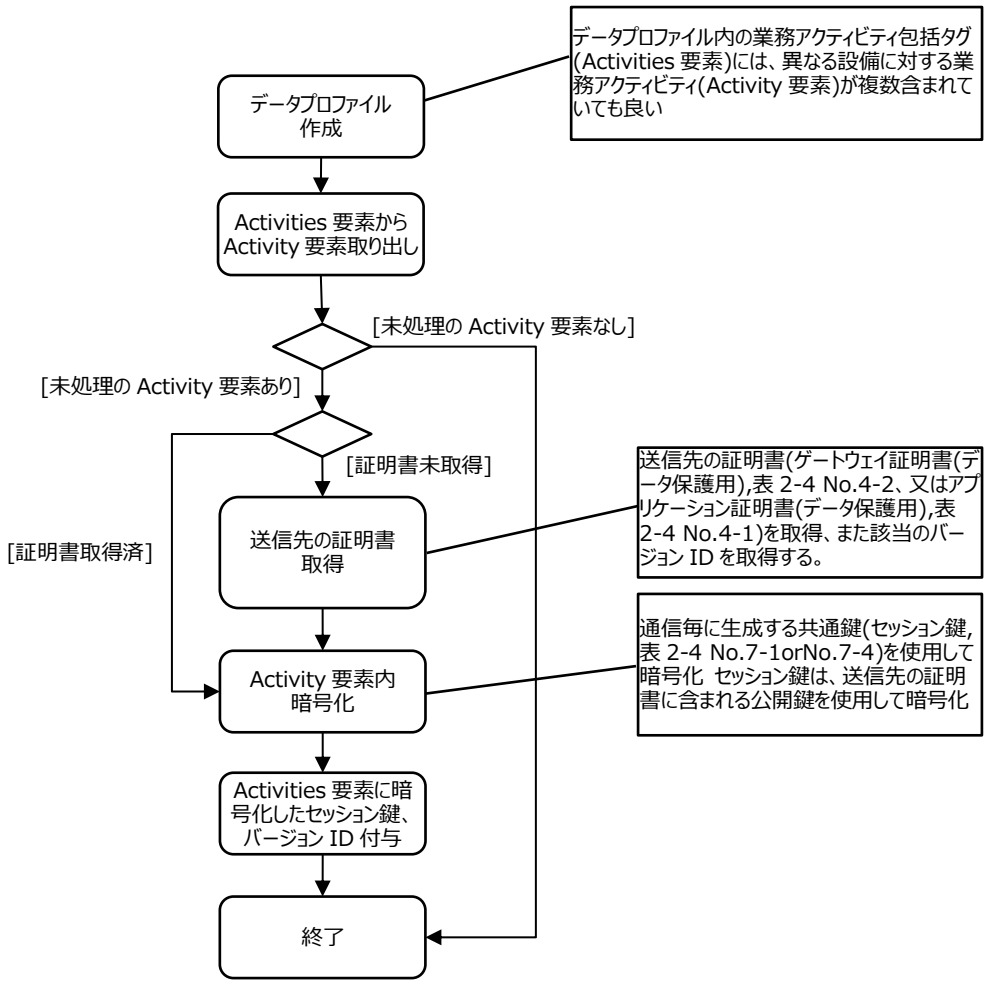

図 2-6: データ送信時の処理(データ暗号化の付与)

2.4.2 データ受信時のデータ復号

(1) データ復号の処理順

広域向けアプリケーション及びゲートウェイが、データを受信した際の復号の処理順を以下に示す(図 2-7)。

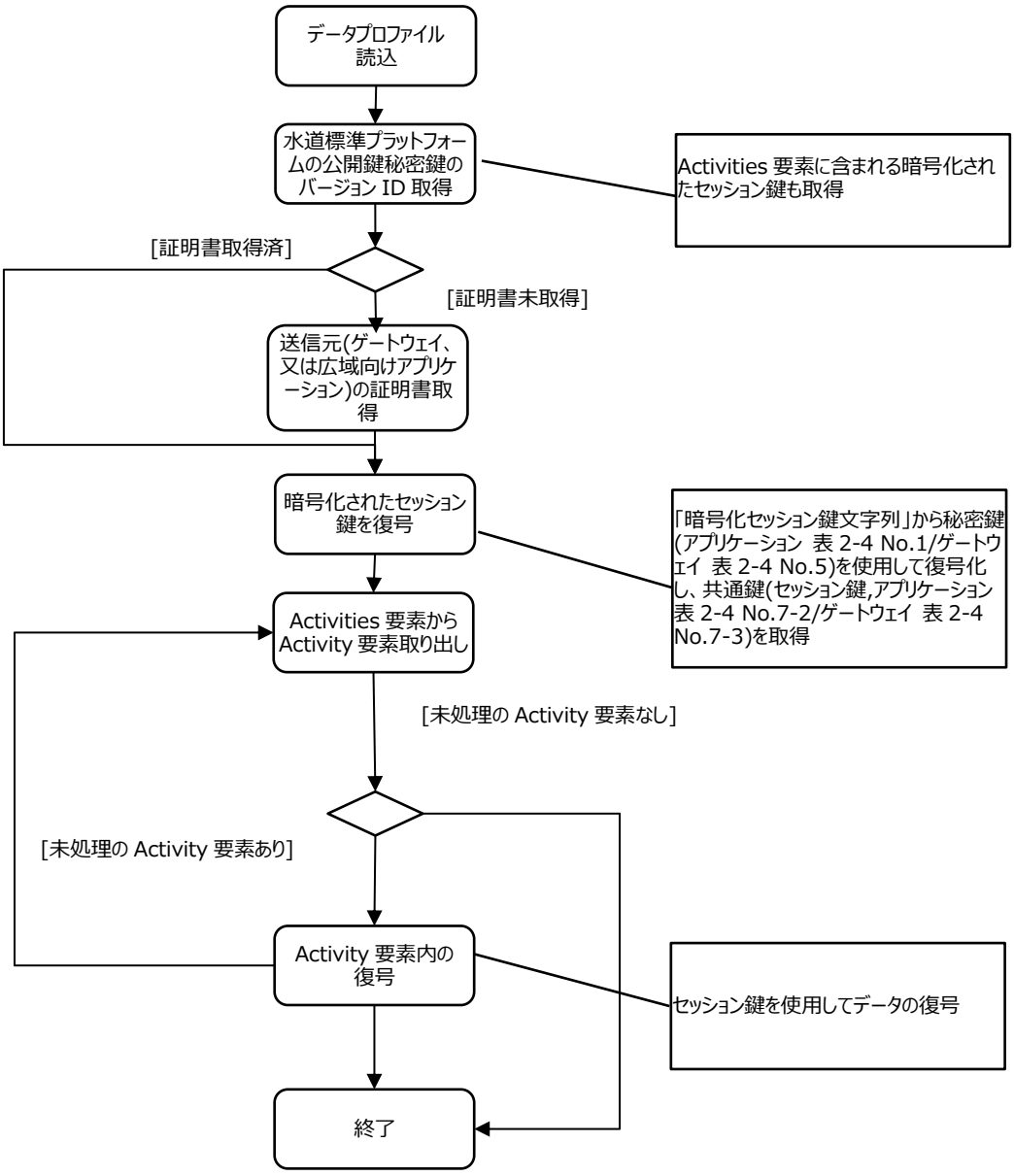

図 2-7: データ受信時の処理(復号)

2.4.3 暗号アルゴリズムと署名アルゴリズム

広域向けアプリケーション、ゲートウェイ、水道標準プラットフォームが採用する暗号アルゴリズムおよび署名アルゴリズムは、現時点では、下記のアルゴリズムを採用する。

ただし、セキュリティにおける技術動向や水道情報活用システムのシステム環境は、将来において変化していく為、その時点で適切なアルゴリズムの採用を検討し選択肢として追加されるものとする。

(1) 暗号アルゴリズム

暗号アルゴリズムは、データ送信側と受信側で同一のアルゴリズムを利用する。

(a) データの暗号化と復号

共通鍵方式を利用してデータの暗号化、復号を行なう。使用する暗号のアルゴリズムを以下に示す(表 2-5)。

表 2-5: データの暗号化と復号で使用するアルゴリズム

No.	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
4	ブロック長	128bit
5	パディング	PKCS#7

※: 終端で端数データが発生した場合は、No.5 に示す方式でパディングを行う

(b) 共通鍵の暗号化と復号

共通鍵方式を利用してセッション鍵の暗号化、復号を行なう。使用する暗号のアルゴリズムを以下に示す(表 2-6)。

表 2-6: セッション鍵の暗号化と復号で使用するアルゴリズム

No.	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

(c) データ暗号化における XML 仕様

データ暗号化したデータと、データ暗号化に使用したセッション鍵は、XML 暗号の仕様に従ってデータプロファイルに組み込む。

(2) 署名アルゴリズム

署名アルゴリズムは、データ送信側と受信側で同一のアルゴリズムを利用する。

(a) 電子署名で使用するアルゴリズム

電子署名の付与と検証で使用するアルゴリズムを以下に示す(表 2-7)。

表 2-7: 電子署名で使用するアルゴリズム

No.	区分	アルゴリズム
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

(b) 電子署名の付与における XML 仕様

データに付与される電子署名の値は、XML 署名の仕様に従ってデータプロファイルに組み込む。

2.5 セキュリティ対策の選択

「データの受け渡しが安全に行われること」を実現するセキュリティ対策として、①閉域網の利用、②通信経路の暗号化、③データの暗号化、の３つが挙げられる。(図 2-8)

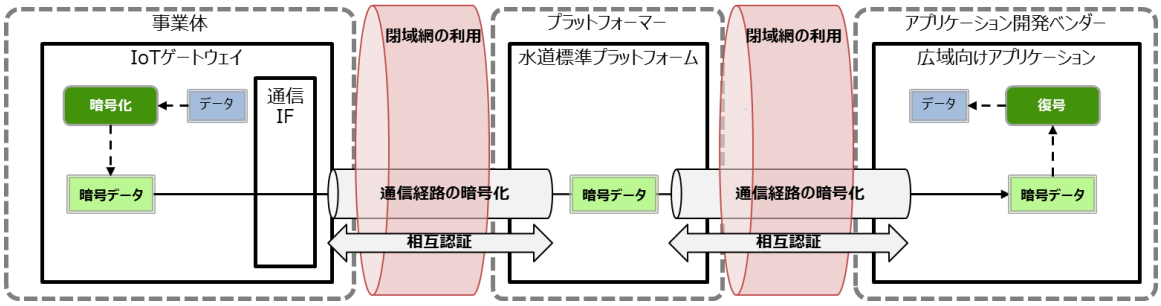

図 2-8: 「データの受け渡しが安全に行われること」を実現するセキュリティ対策

対策を数多く実施することはセキュリティを向上させるが、一方で、計算処理量や通信データ量の増加をまねくためシステムコストとのバランスを取る必要がある。そのため、現状の監視制御システムにおける利用状況を鑑み、セキュリティ対策として「①閉域網の利用」を実施している場合には「②通信経路の暗号化」と「③データの暗号化」の対策は重複する要素が大きく、「③データの暗号化」のほうが計算処理コストが大きいことから「②通信経路の暗号化」の対策のみでも良いとする。

なお、「①閉域網の利用」を実施している場合、ゲートウェイ側や保守端末側のネットワークから、公衆網（インターネット）に接続する場合に、①のセキュリティ要件が守れなくなるという問題がある。そのため、ゲートウェイおよび保守端末は水道標準プラットフォーム接続の専用端末とし、公衆網（インターネット）への接続は原則禁止とする。端末の初期セットアップやメンテナンスのために公衆網（インターネット）への接続が必要となる場合は、水道標準プラットフォームのネットワークとは切り離した状態で実施し、端末内のウィルスチェックを十分に実施した上で、水道標準プラットフォームのネットワークに接続すること。

2.6 認定制度

認定制度の詳細については、基本仕様書に記載されている。

詳細は基本仕様書の 3.1.6 項を参照。

本節では、認定の取得要否について示す。

水道情報活用システムの各サブシステムのベンダー、プラットフォーマーは、セキュリティに関する機能の信頼性・実効性や安全性を確認するための手段として、第三者による認定取得が望ましい。

主な認証・規格の取得要否を以下に示す(表 2-8)。

表 2-8: 主な認証・規格の取得要否

No.	認定制度 (認証・規格)	取得要否			
		アプリケーション開発ベンダー	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	プラットフォーマー
1	ISMS	○	○	○	○
2	ITSMS	○	－	－	○
3	CSMS	－	－	－	－
4	EDSA	－	－	－	－
5	FIPS 140-2	－	－	－	－
6	PCI DSS	－	－	－	－
7	SP800-171	－	－	－	－
8	NERC CIP	－	－	－	－

【凡例】 ○: 推奨、－: 任意

- 以上 -