



## 社会インフラ(水道)のサプライチェーン (プロフィール例)

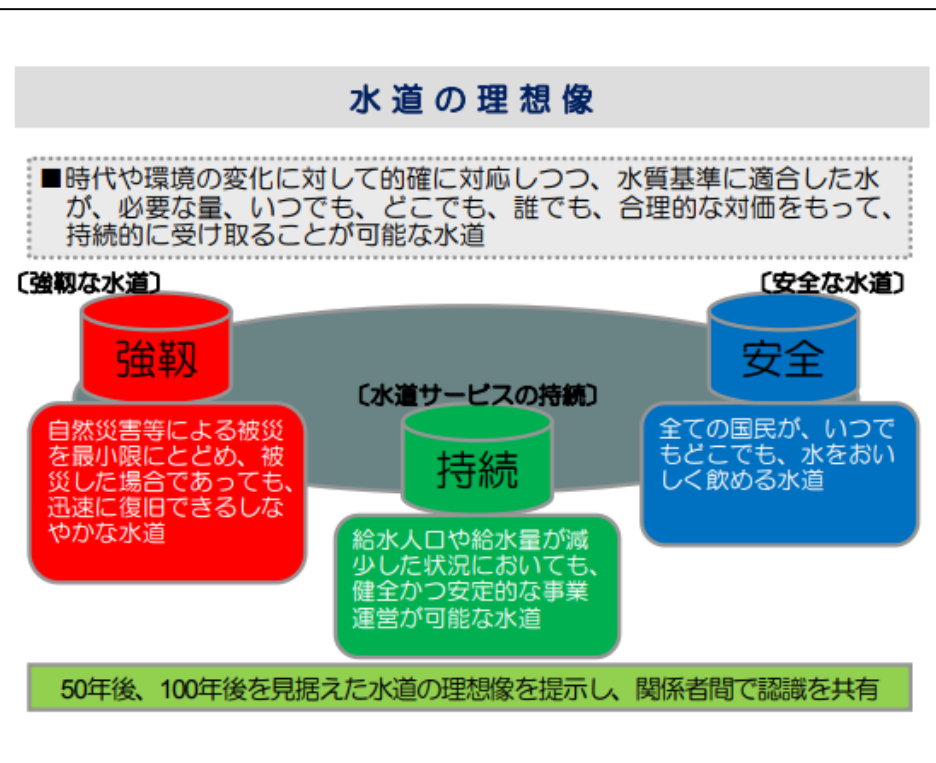
2018年3月

株式会社 日立製作所 IoT推進本部  
IoTプロジェクト推進本部 サイバー・フィジカル・システム部

# 社会インフラ(水道)におけるミッション

厚生労働省の「新水道ビジョン」では、強靱・持続・安全な水道をめざすことが示されている。

## ビジョン(水道)



出典：平成25年 厚生労働省 健康局「新水道ビジョン」

## ミッション(水道)

### 強靱

- ・ 災害時でも必要最低限の水供給
- ・ 断水時の応急給水活動の展開
- ・ 水の供給のバックアップ体制の構築
- ・ 重要給水拠点に供給するための施設を最優先に、段階的に耐震化

### 持続

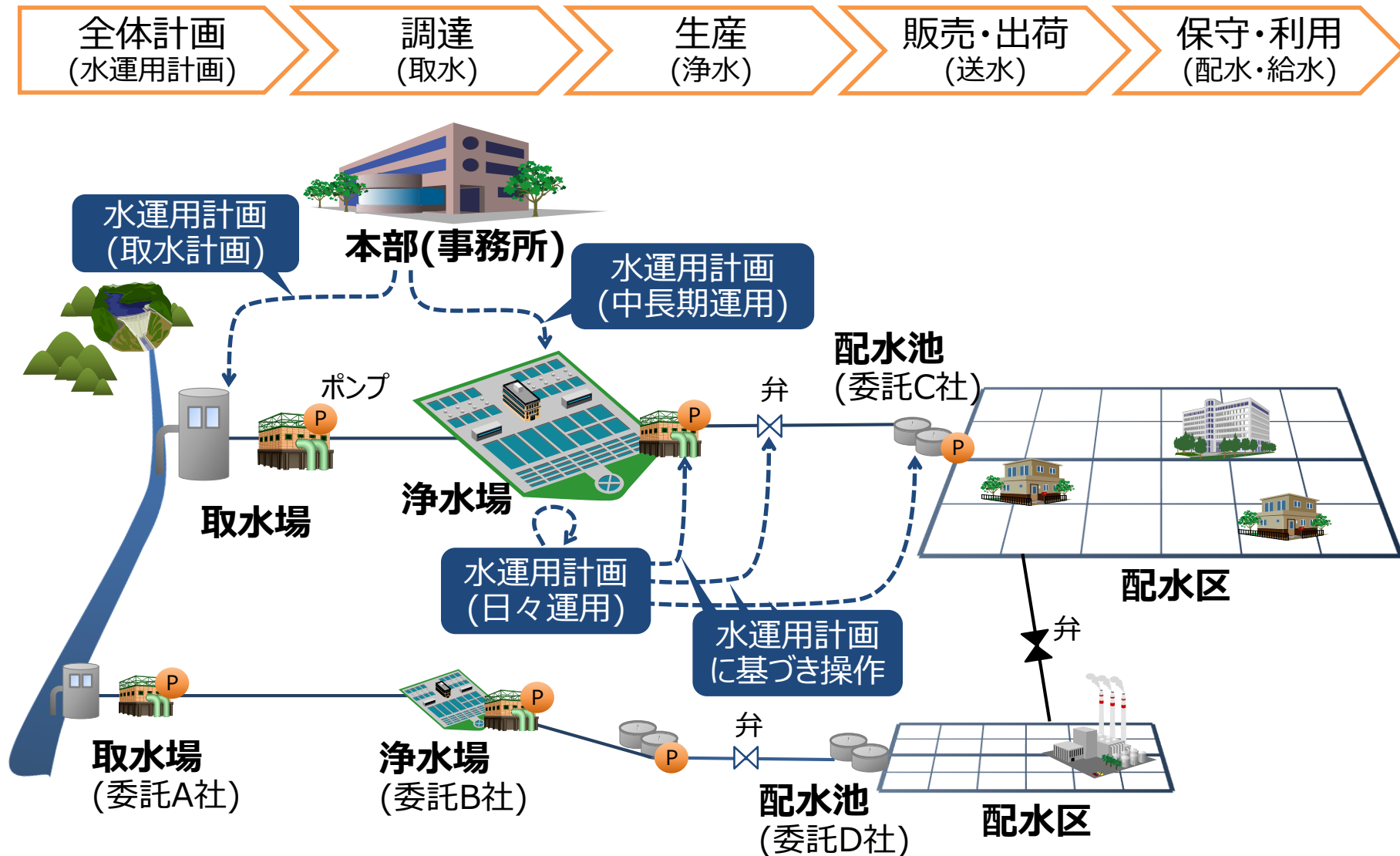
- ・ 人口や給水量が漸減し続ける中で事業規模を段階的に縮小
- ・ 技術者の確保、施設の管理・更新
- ・ 将来必要となる資金の確保

### 安全

- ・ 水源に応じた水道施設の整備と浄水処理における水質管理
- ・ 水源の保全
- ・ 水質などの情報を広報・周知

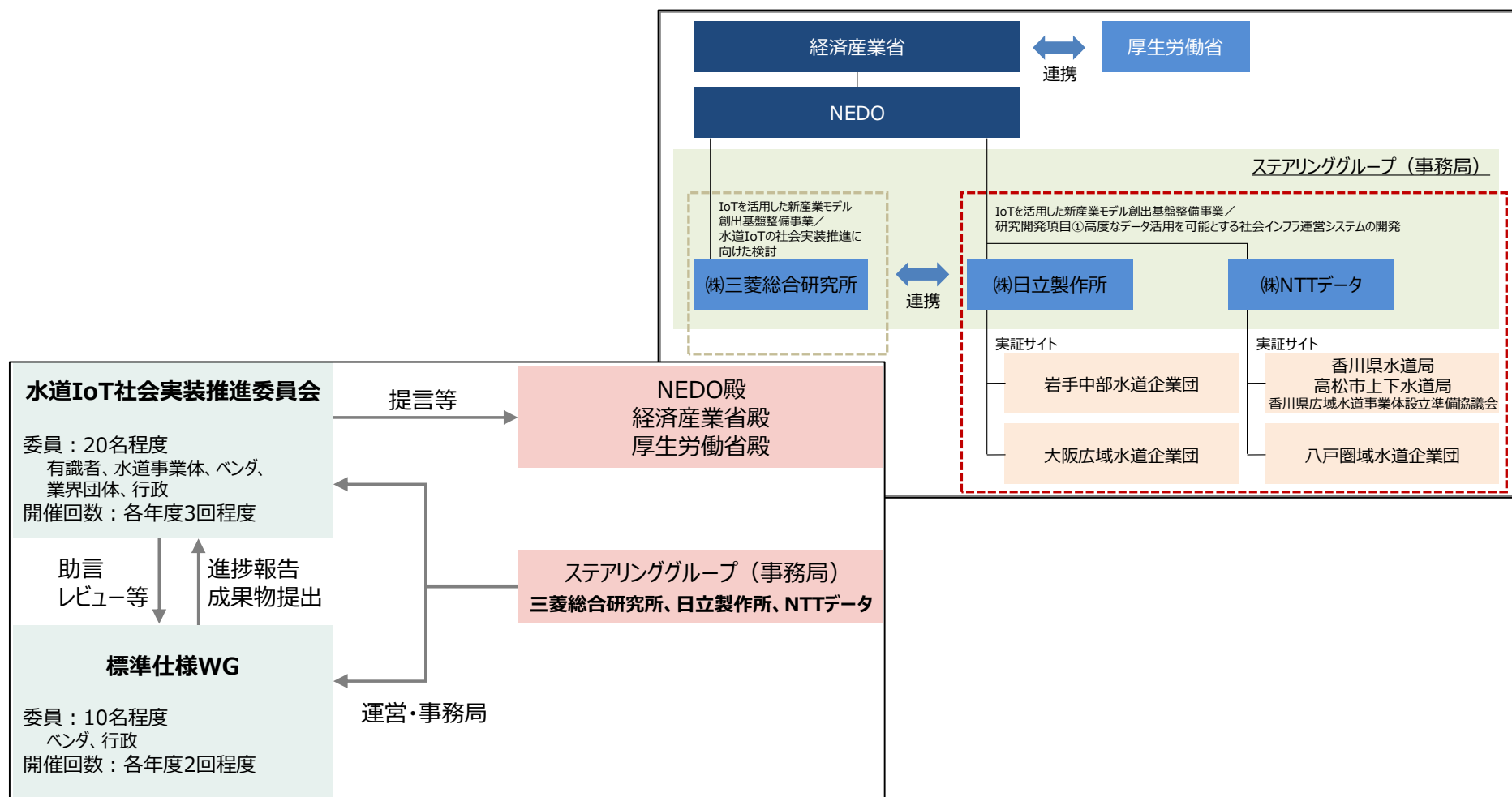
# 社会インフラ(水道)の運用フロー

社会インフラ(水道)の運用フローの概要を以下に示す。



# 平成29年度～平成30年度 実証事業 実施体制

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／ 研究開発項目①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」



# 平成29年度～平成30年度 実証内容の概要

CPSの仕組みが水道事業の「持続可能な事業運営」に資するかを実証で評価する。

## 【持続可能な事業運営】

### ■ 課題

水需要減少に伴う収益減少  
施設老朽化に伴う大量の更新投資  
ベテラン職員の大量退職による技術継承問題

### ■ 解決の方向性

広域化  
・各団体が行う別々の業務を一元化、統一化  
・広域の遠隔管理と自動化による効率化  
・ダウンサイジング計画やリスク管理に対応する量的・質的マンパワーの確保  
・専門的、総合的知識の蓄積と共有による技術の継承



資  
す  
る  
か  
を  
評  
価

## 【実証での取り組み】

### ■ 手段

CPSの仕組みを活用する  
・CPSの仕組みで、既存の資産と情報(データ)を総動員して活用

### ■ シナリオの効果評価

- A. 施設老朽化や水需要減少に伴う施設統廃合
- B. 施設・設備の状態の変化に伴う日々・中長期の水運用
- C. ベテラン職員の大量退職に対する技術継承

### ■ CPS実装における標準仕様

- ・水平分業の確立
- ・アーキテクチャと守るべきルール

### ■ CPS実装におけるセキュリティ対応マニュアル

- ・セキュリティの確立

### ■ 事業体への広報・普及活動

- ・先行導入事業体へのインセンティブ

# 平成29年度～平成30年度 実証シナリオ

CPSの仕組みを活用したシナリオの効果評価に関して、水道事業のコストであるアセット系費用やオペレーション系費用、人件費等のそれぞれの費用に対して、期待される効果を以下に示す。

## A. 施設老朽化や水需要減少に伴う施設統廃合

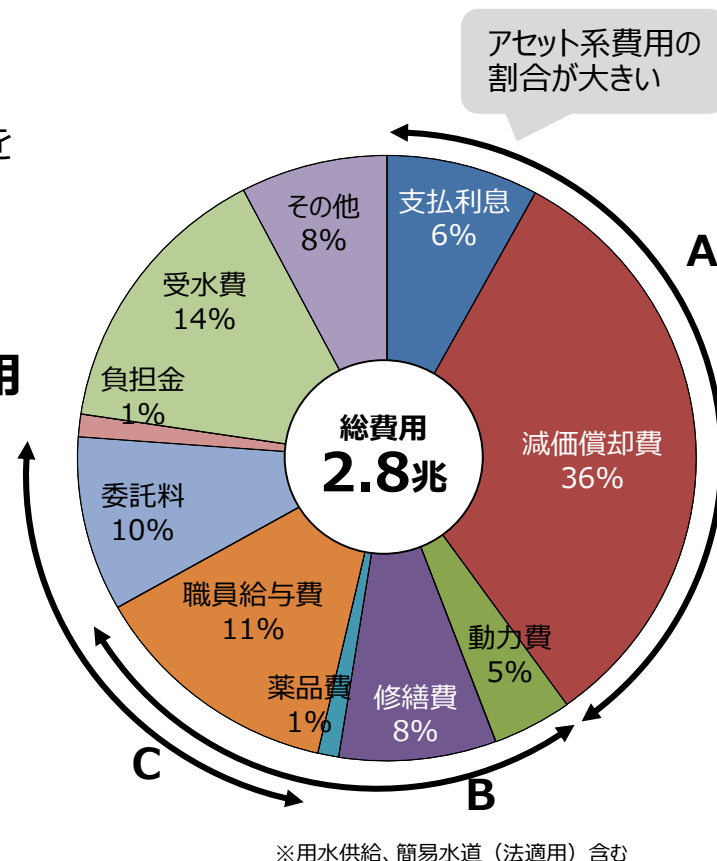
CPSの仕組みを活用して、状況や条件の変化に応じて随時見直さなければならない施設統廃合計画の策定に必要なデータを一元的に把握することで、繰り返し実施される施設統廃合計画の策定にかかる期間を短縮でき、施設の統廃合ができるか  
⇒将来の更新投資の抑制に資するかを評価

## B. 施設・設備の状態の変化に伴う日々・中長期の水運用

CPSの仕組みを活用して、需要量や水源、施設・設備等の日々変化する状態をモニタリングすることで、日々、中長期の水運用を持続でき効率化できるか  
⇒安全、安心の水道水を低廉価で安定供給することに資するかを評価

## C. ベテラン職員の大量退職に対する技術継承

CPSの仕組みを活用して、ベテラン職員の技術をデータとして蓄積することで、知見の共有や現場の支援に活用できるか  
⇒少子高齢化に伴う人手不足への対応、ベテラン職員の知見の共有に資するかを評価

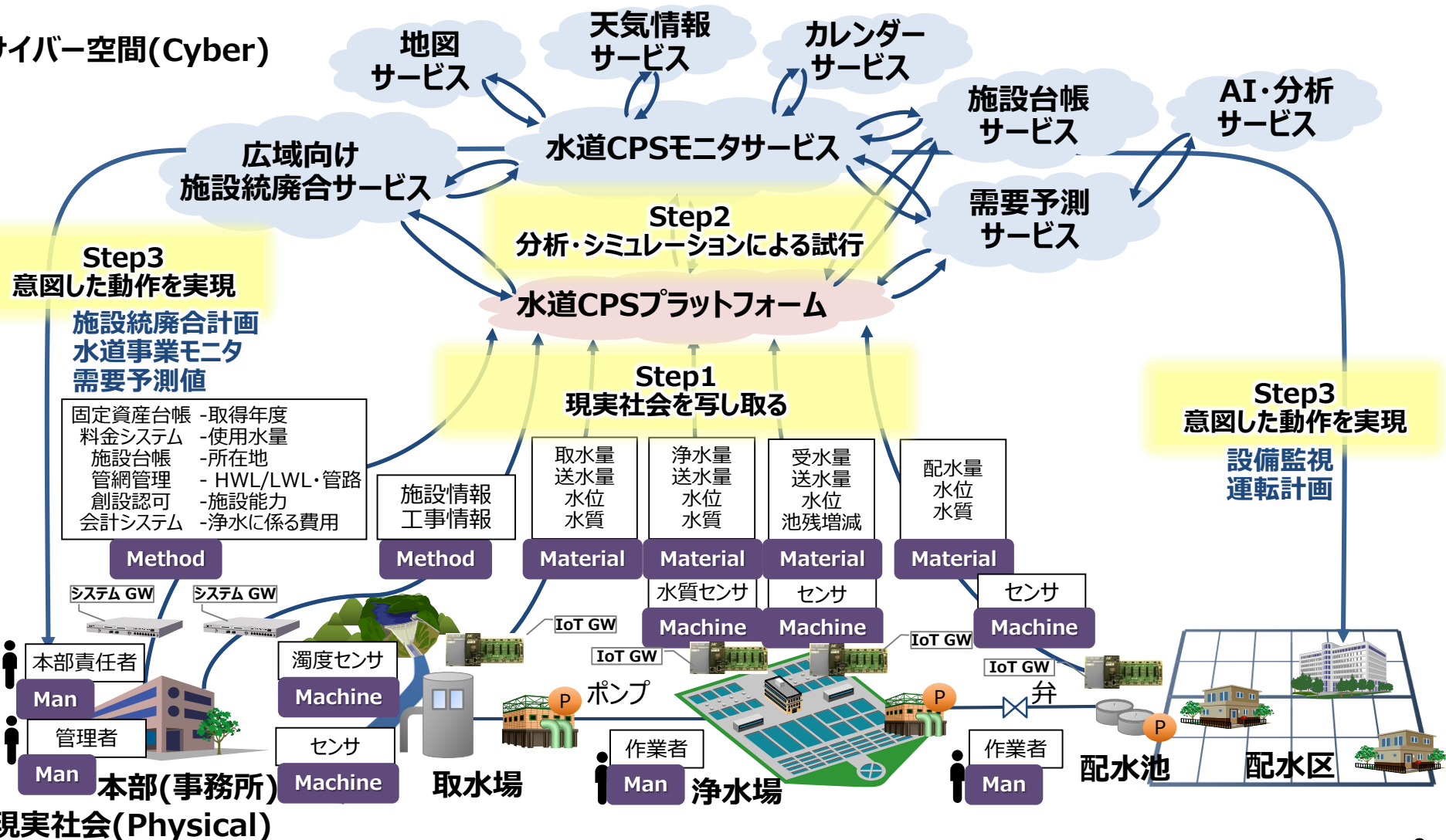


出典：総務省「平成27年度地方公営企業年鑑」をもとに作成

# 社会インフラ(水道) CPSにおけるユースケース例

社会インフラ(水道)CPSにおける水道CPSモニタサービスのユースケース例を示す。

サイバー空間(Cyber)



# CPS実装における標準仕様

CPS実装における標準仕様を以下に示す。

## 1. 全体構成(アーキテクチャ)

## 2. 役割(ルール)

### ① 識別子(ID)付与・管理とアクセス制限

- ・ ユーザの識別(ユーザIDリスト)
- ・ アプリケーションの識別(アプリケーションIDリスト)
- ・ ゲートウェイの識別(ゲートウェイIDリスト)

### ② 識別子(ID)に基づく認証方式の規定

- ・ 電子署名付与/検証の方式
- ・ 相互認証の方式
- ・ 通信経路の暗号化方式
- ・ データの暗号化方式

### ③ データをやり取りする手順の規定

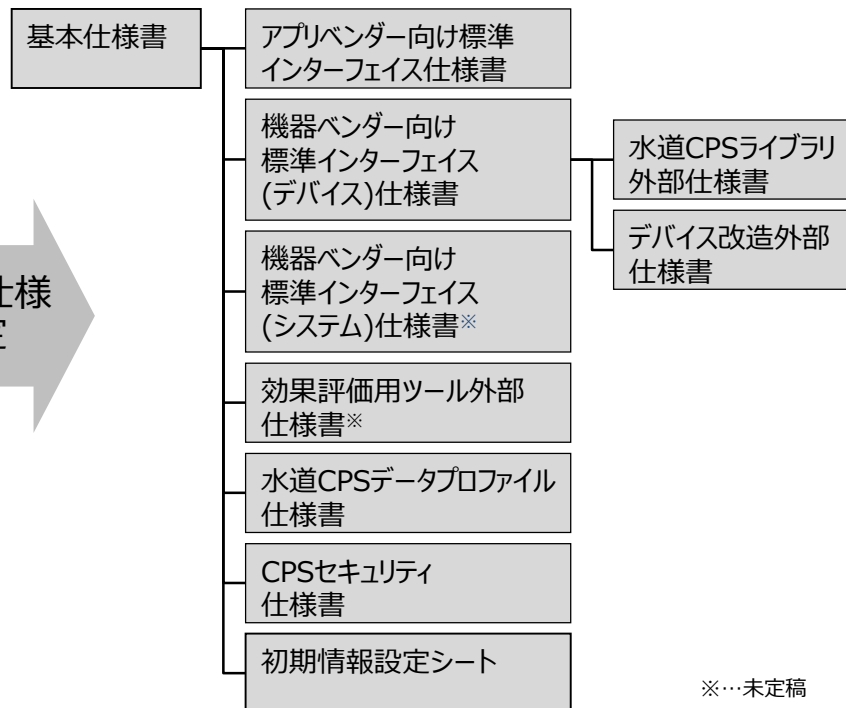
- ・ 標準インターフェイス
- ・ プロセス/モノの認証
- ・ 通信プロトコル

### ④ 現場の設備データの収集

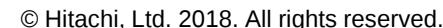
- ・ 現場の設備データの意味づけ(データプロファイル)
- ・ 現場の計測データモデル管理

## <社会インフラ(水道)CPSシステム標準仕様>

標準仕様  
で規定



- ・分析・シミュレーション
- ・クラウド(サービス)間連携



## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 経営者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                        | 対策ポイント                                                             | 区分    |    |
|----|-------|-----------------------------|--------------------------------------------------------------------|-------|----|
| 1  | STEP3 | 体制・人材の確保<br>・セキュリティ管理責任者の任命 | 水道事業者におけるセキュリティ管理責任者を任命し、組織内でセキュリティ対策を取る体制を整えることで、効果的なセキュリティ対策を取る。 | マニュアル | 任意 |

## セキュリティ管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                             | 対策ポイント                                                                                                                   | 区分    |    |
|----|-------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP3 | 適切なセキュリティマネジメントの実施<br>・ISMSに準拠した運用の実施            | 水道事業者において、ISMSに基づいたセキュリティマネジメントシステムを構築し、運用することで、サイバー攻撃によるリスクを低減することができる。                                                 | 標準仕様  | 推奨 |
| 2  | STEP3 | 適切なセキュリティマネジメントの実施<br>・CSMSに準拠した運用の実施            | 水道事業者において、CSMSに基づいたセキュリティマネジメントシステムを構築し、運用することで、サイバー攻撃によるリスクを低減することができる。                                                 | 標準仕様  | 任意 |
| 3  | STEP1 | プライバシー保護<br>・プライバシー保護の法令に準拠したプライバシー情報の取り扱いルールを作成 | 現場(浄水場、配水地等)に設置された監視カメラ等から収集したデータに対し、個人情報保護やプライバシー保護に関する国際的な基本原則「OECD 8 原則」に則り、運用管理を行うルールを作成することで、CPSの運用におけるプライバシー侵害を防ぐ。 | マニュアル | 任意 |
| 4  | STEP3 | 基本方針の策定<br>・セキュリティポリシーの策定 (PDCA 実施体制の整備含む)       | 水道事業者におけるセキュリティポリシーを策定することで、セキュリティ問題に対して十分な対策を取り、セキュリティ問題の発生や被害の拡大を防ぐ。                                                   | マニュアル | 任意 |
| 5  | STEP3 | 基本方針の策定<br>・セキュリティ対策組織立ち上げ                       | 水道事業者において、セキュリティ対策組織を立ち上げることで、セキュリティ問題に対して十分な対策を取り、セキュリティ問題の発生や被害の拡大を防ぐ。                                                 | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

## セキュリティ管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                | 対策ポイント                                                                                                        | 区分    |    |
|----|-------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------|----|
| 6  | STEP3 | リスク管理<br>・リスクアセスメント（リスクの特定・分析・評価）の実施                | 水道事業者に存在するリスクの特定や分析、評価を行い、そのリスクに対するセキュリティ対策の内容、優先順位、対策範囲の特定等をあらかじめ行うことで、重大なセキュリティ問題の発生や被害の拡大を防ぐ。              | マニュアル | 任意 |
| 7  | STEP3 | リスク管理<br>・セキュリティルールの策定                              | 水道事業者において定めたセキュリティポリシーや、リスクアセスメントの実施結果を元に、セキュリティルールを定めることでセキュリティ対策の推進を図ることができ、大なセキュリティ問題の発生や被害の拡大を防ぐ。         | マニュアル | 任意 |
| 8  | STEP3 | リスク管理<br>・セキュリティ運用マニュアルの作成                          | 水道事業者におけるセキュリティ対策を考慮した運用を確立することで、重大なセキュリティ問題の発生や被害の拡大を防ぐ。                                                     | マニュアル | 任意 |
| 9  | STEP3 | セキュリティ対策のPDCA実施<br>・セキュリティリスクに対するPDCAの実施            | 水道事業者におけるセキュリティ対策運用の継続的な見直しを行うことで、新たなリスクへの対応の特定や、既存の対策の改善を図ることができ、重大なセキュリティ問題の発生や被害の拡大を防ぐ。                    | マニュアル | 任意 |
| 10 | STEP3 | 各種法令への対応<br>・営業機密の保護等、業界のガイドラインや、法令を考慮したセキュリティ対策の立案 | 水道事業者における既存のガイドラインや、個人情報保護法、不正競争防止法等の法令を考慮した社内ルールを策定する。これにより、他の事業者との間でデータを共有した場合においても、業務上の公正な競争秩序を維持することができる。 | マニュアル | 任意 |

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                               | 対策ポイント                                              | 区分      |
|----|-------|----------------------------------------------------|-----------------------------------------------------|---------|
| 1  | STEP1 | 通信経路の暗号化<br>・暗号化通信 (TLS、DTLS、IPsec 等) に対応した通信機器の導入 | 通信経路は、SSL/TLSを用いて暗号化する。                             | 標準仕様 必須 |
|    | STEP3 |                                                    | SSL/TLSにおいては、第三者(認証局(CA))が発行した証明書を利用することが望ましい。      | 標準仕様 任意 |
|    |       |                                                    | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。         | 標準仕様 任意 |
| 2  | STEP1 | アクセス制御<br>・アクセス元に対する識別、認証、認可の実施                    | 水道CPSシステムの構成要素へのアクセスを制限し、許可された対象のみにアクセスを許容する。       | 標準仕様 必須 |
|    |       |                                                    | 許可された対象からのアクセスは、予め設定された権限の範囲に制限する。                  | 標準仕様 必須 |
| 3  | STEP1 | 接続元の識別<br>・接続元となる通信相手の識別                           | 水道CPSシステムの構成要素に対して識別子(ID)を付与し、一意に識別する。              | 標準仕様 必須 |
|    | STEP3 |                                                    | 接続元の識別においては、第三者(認証局(CA))が発行した識別子(ID)を利用することが望ましい。   | 標準仕様 任意 |
|    |       |                                                    | 識別子(ID)は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。     | 標準仕様 任意 |
| 4  | STEP1 | 接続元の認証<br>・相互認証による接続元の認証                           | 通信の開始時には、SSL/TLSのプロトコル仕様に従い、双方で通信相手の正当性を確認(相互認証)する。 | 標準仕様 必須 |
|    | STEP3 |                                                    | 相互認証では、第三者(認証局(CA))が発行した証明書を利用することが望ましい。            | 標準仕様 任意 |
|    |       |                                                    | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。         | 標準仕様 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP           | 対策内容                              | 対策ポイント                                                                                                                                                    | 区分       |
|----|----------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 5  | STEP1<br>STEP3 | 接続先の識別<br>・接続先となる通信相手の識別          | 水道CPSシステムの構成要素に対して識別子(ID)を付与し、一意に識別する。                                                                                                                    | 標準仕様 必須  |
|    |                |                                   | 接続先の識別においては、第三者(認証局(CA))が発行した識別子(ID)を利用することが望ましい。                                                                                                         | 標準仕様 任意  |
|    |                |                                   | 識別子(ID)は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                                                                           | 標準仕様 任意  |
| 6  | STEP1<br>STEP3 | 接続先の認証<br>・相互認証による接続先の認証          | 通信の開始時には、SSL/TLSのプロトコル仕様に従い、双方で通信相手の正当性を確認(相互認証)する。                                                                                                       | 標準仕様 必須  |
|    |                |                                   | 相互認証では、第三者(認証局(CA))が発行した証明書を利用することが望ましい。                                                                                                                  | 標準仕様 任意  |
|    |                |                                   | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                                                                               | 標準仕様 任意  |
| 7  | STEP1          | IoT機器で利用する機能の管理<br>・通信プロトコルの管理、監視 | IoT機器(監視カメラ、IoTゲートウェイ等)で不要なポート、プロトコル等の利用を停止することで、IoT機器への不正アクセスによる不正な情報(データ)の生成や、マルウェア感染等によるIoT機器から外部への通信による情報(データ)の漏えい等の被害を防ぐ。                            | マニュアル 任意 |
| 8  | STEP1          | 機能の分離<br>・利用者機能とシステム管理機能の分離       | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)において、ユーザーがアクセスできる機能と、システムの運用担当者がアクセスできる機能を分離することで、IoT機器の管理機能への不正アクセスによるIoT機器の設定変更や、IoT機器が収集した情報(データ)の漏えい等の被害を防ぐ。 | マニュアル 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                | 対策ポイント                                                                                                                                                                                                  | 区分    |    |
|----|-------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 9  | STEP1 | ネットワークの分割<br>・ネットワークの物理的、または論理的な分割                  | 現場(浄水場、配水地等)のネットワークを物理的、または論理的に分割することで、不正アクセスや、ネットワークの負荷がネットワーク全体に影響を及ぼすことを防ぐ。                                                                                                                          | マニュアル | 任意 |
| 10 | STEP1 | IoT機器への不正な無線接続対策、マルウェア感染対策<br>・Bluetooth等による無線接続の制限 | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に対し、不特定なBluetooth対応IoT機器への接続停止、またはBluetooth機能を無効化する。この対策を行うことで、IoT 機器に対する不正アクセスによる内容の参照や、マルウェアに感染等による情報(データ)の漏えい、不正な情報(データ)の生成を防ぐ。                             | マニュアル | 任意 |
| 11 | STEP1 | IoT機器への不正な無線接続対策、マルウェア感染対策<br>・無線LANアクセスポイントの認証強化   | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に対し、現場で無線LAN を利用する場合のESSID の設定、MAC アドレスフィルタリング、強固な号化方式(WPA2 等)の設定等を行い、認証機能を強化する。この対策を行うことで、IoT 機器に対する不正アクセスによる内容の参照や、マルウェアに感染等による情報(データ)の漏えい、不正な情報(データ)の生成を防ぐ。 | マニュアル | 任意 |
| 12 | STEP1 | 外部ネットワークからの不正侵入対策<br>・ファイアウォール、IDS/IPSの導入           | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に対し、現場で無線LAN を利用する場合のESSID の設定、MAC アドレスフィルタリング、強固な号化方式(WPA2 等)の設定等を行い、認証機能を強化する。この対策を行うことで、IoT 機器に対する不正アクセスによる内容の参照や、マルウェアに感染等による情報(データ)の漏えい、不正な情報(データ)の生成を防ぐ。 | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                      | 対策ポイント                                                                                                                                                                               | 区分    |    |
|----|-------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 13 | STEP1 | 外部ネットワークからの不正侵入対策<br>・接続元のMACアドレス、IoT機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無確認 | 現場(浄水場、配水地等)において、IoT機器(監視カメラ、IoTゲートウェイ等)への接続元のMACアドレス、IoT機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無確認を行う。これにより、現場に設置されたIoT機器に対する不正ログイン、マルウェア感染等による情報(データ)の漏えい、IoT機器での不正な情報(データ)の生成を防ぐことができる。 | マニュアル | 任意 |
| 14 | STEP1 | 適切な認証機能の利用<br>・認証失敗時の再試行の制限                                               | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)への一定回数以上のログイン失敗によるロックアウトや、再ログインまでの間隔を設ける機能を実装することで、IoT機器に対する不正ログインを防止し、IoT機器の設定変更や、IoT機器が収集した情報(データ)の漏えい等の被害を防ぐ。                            | マニュアル | 任意 |
| 15 | STEP1 | アクセス制御<br>・適切なセッションの管理                                                    | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)へのアクセスに対し、アクセス元を識別・認証して適切なアクセス制御を行うことで、IoT機器に対する不正ログインを防止し、IoT機器の設定変更や、IoT機器が収集した情報(データ)の漏えい等の被害を防ぐ。                                        | マニュアル | 任意 |
| 16 | STEP1 | 電子証明書の管理<br>・証明書の有効期限の設定                                                  | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に発行する証明書には、機器に対してアクセスを許可する期間を有効期限として設定する。認証で使用する電子証明書の有効期限を適切に設定することで、IoT機器に対する不正ログインを防止し、IoT機器の設定変更や、IoT機器が収集した情報(データ)の漏えい等の被害を防ぐ。         | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                     | 対策ポイント                                                                                                                                                                                   | 区分    |    |
|----|-------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 17 | STEP2 | 外部ネットワークからの不正侵入対策<br>・ネットワーク監視によるサイバー攻撃検知                | 水道事業のプラットフォームに対し、ファイアウォールや、IDS/IPS等を導入する。これにより、外部ネットワークからの不正アクセス、利用を許可していないアプリケーションによる通信を検知・防御し、集中監視制御アプリケーション等のアプリケーションへのマルウェア感染や、サイバー攻撃を受けることによる情報（データ）の漏えい、誤動作による不正な分析結果の生成を防ぐことができる。 | マニュアル | 任意 |
| 18 | STEP2 | 外部ネットワークからの不正侵入対策<br>・ファイアウォール、IDS/IPSの導入                | 水道事業のプラットフォームにおいて、ネットワーク監視によるサイバー攻撃検知を行う。これにより、外部ネットワークからの不正アクセス、利用を許可していないアプリケーションによる通信を検知・防御し、集中監視制御アプリケーション等のアプリケーションへのマルウェア感染や、サイバー攻撃を受けることによる情報（データ）の漏えい、誤動作による不正な分析結果の生成を防ぐことができる。 | マニュアル | 任意 |
| 19 | STEP2 | 認証とアクセス管理<br>・パスワード、生体認証、電子証明書等、二つの認証機能を組み合わせた二要素認証機能の実装 | 水道事業のプラットフォームにおいて、二つの認証機能を組み合わせた二要素認証機能を利用する。これにより、不正なユーザによるサイバー空間に保管される業務情報の不正閲覧による漏えいを防ぐ。                                                                                              | マニュアル | 任意 |
| 20 | STEP2 | 不審ユーザ・機器の検知<br>・アクセス履歴（場所・時間・端末等）が参照可能な機能の実装             | 集中監視制御アプリケーション等のアプリケーションを実行するサーバや通信機器に対し、ユーザのアクセス履歴を分析し、不正アクセスを検知する運用を行う。これにより、アクセス元の場所・時間、アクセス頻度等の情報をもとに不正アクセスを検知することができ、サイバー空間に保管される業務情報の不正閲覧・漏えいを防ぐことができる。                            | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                                                                                                          | 対策ポイント                                                                                                                                                                                                                                                    | 区分    |    |
|----|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 21 | STEP2 | サイバー空間のサーバ、通信機器、回線の故障予防、復旧対策<br>・サーバ、通信機器の定期的なシステムバックアップ<br>・サーバ、通信機器、回線の品質管理<br>・サーバ、通信機器の予備機、予備回線、無停電電源装置の確保<br>・サーバ、通信機器、回線の冗長化<br>・サーバ、通信機器、回線の故障の検知<br>・サーバ、通信機器、回線の交換作業 | 集中監視制御アプリケーション等のアプリケーションを実行するサーバ、通信機器、回線の定期的なシステムバックアップ、交換作業や回線工事の明確な手順を確立した品質管理、無停電電源装置の導入、予備機確保による故障発生時の迅速な交換対応、冗長化、情報（データ）の送受信が行えない場合に再送を行う設計、故障検知機能の実装等、可用性の維持を考慮した運用を行う。これにより、サイバー空間のサーバ、通信機器、回線で不具合が生じた場合においても、迅速な原因の特定、サービスの復旧等により、被害の拡大を防ぐことができる。 | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                      | 対策ポイント                                                                                                                                                                                       | 区分   |    |
|----|-------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----|
| 1  | STEP1 | IoT機器間通信の改ざん対策<br>・改ざん検知に対応した通信（OPC UA等）を行うIoT機器の導入                       | 送信するデータには、電子署名を付与し、通信中における改ざんを検知することが望ましい。                                                                                                                                                   | 標準仕様 | 任意 |
|    |       |                                                                           | 電子署名の付与においては、第三者(認証局(CA))が発行した証明書を利用することが望ましい。                                                                                                                                               | 標準仕様 | 任意 |
|    |       |                                                                           | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                                                                                                                  | 標準仕様 | 任意 |
| 2  | STEP1 | 通信データの暗号化<br>・暗号鍵・復号鍵を使用した通信データの秘匿化                                       | 重要なデータは、データそのものを暗号化し、送信する。<br>データの暗号化は共通鍵暗号を用い、共通鍵を公開鍵暗号で暗号化してデータと共に送信する。<br><データの暗号化><br>アルゴリズム：AES(共通鍵はセッション毎に生成)<br>鍵長：128bit,192bit,256bit<br><共通鍵の暗号化><br>アルゴリズム：RSA-OAEP<br>鍵長：2048bit | 標準仕様 | 必須 |
| 3  | STEP1 | 情報（データ）の改ざん対策<br>・収集データに対し電子署名やメッセージ認証コード(MAC)、チェックサム、タイムスタンプ等を付与し、改ざんを検知 | 送信するデータには、電子署名を付与し、通信中における改ざんを検知することが望ましい。                                                                                                                                                   | 標準仕様 | 任意 |
|    |       |                                                                           | 電子署名の付与においては、第三者(認証局(CA))が発行した証明書を利用することが望ましい。                                                                                                                                               | 標準仕様 | 任意 |
|    |       |                                                                           | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                                                                                                                  | 標準仕様 | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                 | 対策ポイント                                                                                                                                                                                       | 区分   |    |
|----|-------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----|
| 4  | STEP2 | 信頼できるサービス提供者の選定<br>・ITSMS を取得したIoT サービスのプラットフォーム提供者の選択                               | 水道事業のプラットフォームにおいて、ITSMSに基づいたサービスの運用管理を行うことで、サービス停止時間の長期化、サービス停止の再発等を低減することができる。                                                                                                              | 標準仕様 | 推奨 |
| 5  | STEP3 | 通信データの暗号化<br>・暗号鍵・復号鍵を使用した通信データの秘匿化                                                  | 重要なデータは、データそのものを暗号化し、送信する。<br>データの暗号化は共通鍵暗号を用い、共通鍵を公開鍵暗号で暗号化してデータと共に送信する。<br><データの暗号化><br>アルゴリズム：AES(共通鍵はセッション毎に生成)<br>鍵長：128bit,192bit,256bit<br><共通鍵の暗号化><br>アルゴリズム：RSA-OAEP<br>鍵長：2048bit | 標準仕様 | 必須 |
| 6  | STEP3 | サイバー空間から送られる情報（データ）の改ざん対策<br>・処理結果に対し電子署名やメッセージ認証コード(MAC)やチェックサム、タイムスタンプ等を付与し、改ざんを検知 | 送信するデータには、電子署名を付与し、通信中における改ざんを検知することが望ましい。                                                                                                                                                   | 標準仕様 | 任意 |
|    |       |                                                                                      | 電子署名の付与においては、第三者(認証局(CA))が発行した証明書を利用することが望ましい。                                                                                                                                               | 標準仕様 | 任意 |
|    |       |                                                                                      | 証明書は、必要に応じて、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                                                                                                                  | 標準仕様 | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                                                        | 対策ポイント                                                                                                                                                      | 区分    |    |
|----|-------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 7  | STEP1 | IoT機器間通信の暗号化<br>・暗号化通信（OPC UA等）に対応したIoT機器の導入                                                                                | 現場(浄水場、配水地等)で使用するIoT機器（HMI、SCADA、PLC等）間で通信が行われる際、暗号化通信（OPC UA等）の機能を利用し通信経路上の情報（データ）を暗号化することで、情報（データ）の盗聴による業務情報の漏えいを防ぐ。                                      | マニュアル | 任意 |
| 8  | STEP2 | 保管データの暗号化<br>・保管データの秘匿化                                                                                                     | 水道事業のプラットフォームにおいて、現場(浄水場、配水地等)のIoT機器(監視カメラ、IoTゲートウェイ等)から収集したデータや、サイバー空間で得られた分析結果等のデータを暗号化して保管する。これにより、インターネット経由によるサイバー空間に保管される業務情報の不正閲覧による漏えいを防ぐ。           | マニュアル | 任意 |
| 9  | STEP2 | プライバシー保護<br>・プライバシー保護の法令に準拠したプライバシー情報の取り扱いルール作成                                                                             | 水道事業のプラットフォームにおいて、現場(浄水場、配水地等)に設置された監視カメラ等から収集したデータに対し、個人情報保護やプライバシー保護に関する国際的な基本原則「OECD 8原則」に則り管理・運用を行う。これにより、CPSの運用におけるプライバシー侵害を防ぐことができる。                  | マニュアル | 任意 |
| 10 | STEP3 | サイバー空間から送信された不正な処理結果に対応する仕組み<br>・現場のIoT機器がサイバー空間から送信された処理結果に対し、IoT機器の稼働許容範囲との比較を行い、不正な処理結果の受信時の動作停止、またはIoT機器のみの判断でも適切な動作を行う | 現場(浄水場、配水地等)にて、過去の分析結果の情報（データ）をもとに、サイバー空間からの受信した情報（データ）の異常を検知する等、機能安全を考慮したIoT機器を導入する。これにより、現場人員の判断で異常を検知し、IoT機器の動作を停止することで、IoT機器の誤動作による現場人員の怪我、IoT機器の破損を防ぐ。 | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                                             | 対策ポイント                                                                                                                                                                        | 区分    |    |
|----|-------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 11 | STEP3 | サイバー空間の処理結果の正当性確認<br>・現場のIoT機器がサイバー空間から送信された処理結果に対し、IoT機器の稼働許容範囲との比較を行い、不正な処理結果の受信時の動作停止、またはIoT機器のみの判断でも適切な動作を行う | 現場(浄水場、配水地等)において、あらかじめ決められた閾値を超える分析結果や、過去の分析結果の情報(データ)をもとに不正と判断できる分析結果の検知により、サイバー空間から現場のIoT機器への送信停止や、IoT機器側での動作停止、IoT機器のみの判断による適切な動作を行う。これにより、不正確な情報(データ)の混入に伴う業務運用効率の低下等を防ぐ。 | マニュアル | 任意 |
| 12 | STEP3 | IoT機器の動作の正当性確認<br>・現場のIoT機器がサイバー空間から送信された処理結果と実際のIoT機器の動作結果と比較して、異常の検知や動作の停止を行う                                  | 水道事業のプラットフォームから現場(浄水場、配水地等)のIoT機器へ送信した結果と、IoT機器の動作結果を比較し、不正と判断できる動作結果をIoT機器が検知する仕組みを実装する。これにより、不正確な情報(データ)の混入に伴う業務運用効率の低下等を防ぐ。                                                | マニュアル | 任意 |
| 13 | STEP3 | セキュリティイベントの適切な分析機能、手順の実装<br>・アラート通知後の相関分析の実施                                                                     | 水道事業者において、セキュリティイベントの分析を行うにあたり、セキュリティイベントの相関分析を行うことで、セキュリティインシデントの発生を正確に特定することができる。                                                                                           | マニュアル | 任意 |
| 14 | STEP3 | セキュリティイベントの適切な分析機能、手順の実装<br>・外部の脅威情報と比較したイベント検知内容の分析                                                             | 水道事業者において、セキュリティイベントの分析を行うにあたり、外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントの発生を正確に特定することができる。                                                                                     | マニュアル | 任意 |
| 15 | STEP3 | 集中管理の仕組みの導入<br>・IoT機器の稼働情報等を集中管理する仕組みの導入                                                                         | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)の稼働情報や設定情報等を集中管理することで、管理対象となるIoT機器の状態確認や設定変更を迅速に行うことができる。                                                                            | マニュアル | 任意 |

## ライフサイクル

## 生産技術担当者が実施すべきセキュリティ対策

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

| 項番 | STEP  | 対策内容                                                     | 対策ポイント                                                                                                                     | 区分    |    |
|----|-------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP1 | IoT機器内部の不正閲覧対策<br>・耐タンパー性を備えたIoT機器を選定する                  | 第三者(認証局(CA))が発行した証明書や、情報(データ)を暗号化で使用する鍵情報は、耐タンパー性を持つセキュアモジュールに格納することが望ましい。                                                 | 標準仕様  | 任意 |
| 2  | STEP1 | セキュリティ対策が実装されたIoT機器の選択<br>・第三者機関によるセキュリティ認証を取得したIoT機器の選択 | 水道CPSシステムの構成要素は、セキュリティに関する機能の信頼性や、実効性、安全性を確認するための手段として、第三者による認定を取得すること。                                                    | 標準仕様  | 任意 |
| 3  | STEP3 | IoT機器が安全に動作する仕組み<br>・機能安全を考慮したIoT機器の選択                   | 水道CPSシステムの構成要素は、セキュリティに関する機能の信頼性や、実効性、安全性を確認するための手段として、第三者による認定を取得すること。                                                    | 標準仕様  | 任意 |
| 4  | STEP1 | セキュアブート機能の実装<br>・ソフトウェアの適切な起動順序確認機能を実装したIoT機器の導入         | IoT機器(監視カメラ、IoTゲートウェイ等)の起動時に、起動するソフトウェアの適切な順序を確認することで、マルウェア感染等によるIoT機器から外部への通信による情報(データ)の漏えいや、IoT機器での不正な情報(データ)の生成等の被害を防ぐ。 | マニュアル | 任意 |
| 5  | STEP1 | セキュアブート機能の実装<br>・不正なソフトウェアの起動防止機能を実装したIoT機器の導入           | IoT機器(監視カメラ、IoTゲートウェイ等)の起動時に、不正なソフトウェアの起動を防止したりすることで、マルウェア感染等によるIoT機器から外部への通信による情報(データ)の漏えいや、IoT機器での不正な情報(データ)の生成等の被害を防ぐ。  | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                         | 対策ポイント                                                                                                                                             | 区分    |    |
|----|-------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 6  | STEP1 | 正規品であるソフトウェアの導入<br>・ソフトウェアの提供者により、正規であることが認証されたソフトウェアの導入     | 問い合わせ窓口やサポート体制等が確立されたIoT機器(監視カメラ、IoTゲートウェイ等)を選定することで、IoT機器提供者からの定期的な修正プログラムの入手、IoT機器故障発生時の交換作業を迅速に行うことができ、IoT機器のセキュリティレベル低下、業務運用効率の低下等を防ぐ。         | マニュアル | 任意 |
| 7  | STEP1 | 正規であることを検証できる仕組みを実装したソフトウェアの導入<br>・ソフトウェアでのID(識別子)や電子証明書等の実装 | 現場(浄水場、配水地等)で使用するIoT機器(監視カメラ、IoTゲートウェイ等)において、正規であることを検証する仕組みを実装したソフトウェアを利用することで、模倣品等の品質や信頼性が低いソフトウェアの利用によるマルウェア感染や、不正確な情報(データ)の混入に伴う業務運用効率の低下等を防ぐ。 | マニュアル | 任意 |
| 8  | STEP1 | 正規品であるIoT機器の導入<br>・IoT機器の提供者により、正規であることが認証されたIoT機器の導入        | 現場(浄水場、配水地等)において、正規のIoT機器(監視カメラ、IoTゲートウェイ等)を利用することで、模倣品等の品質や信頼性が低いIoT機器の利用による、不正な情報(データ)の混入や誤動作の発生、故障頻度の上昇に伴う業務運用効率の低下等を防ぐ。                        | マニュアル | 任意 |
| 9  | STEP1 | 正規であることを検証できる仕組みを実装したIoT機器の導入<br>・IoT機器でのID(識別子)や電子証明書等の実装   | 現場(浄水場、配水地等)において、正規のIoT機器(監視カメラ、IoTゲートウェイ等)を利用することで、模倣品等の品質や信頼性が低いIoT機器の利用による、不正な情報(データ)の混入や誤動作の発生、故障頻度の上昇に伴う業務運用効率の低下等を防ぐ。                        | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                                    | 対策ポイント                                                                                                                                                                                                                                        | 区分    |    |
|----|-------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 10 | STEP1 | IoT機器、通信機器、回線の故障予防、復旧対策<br>・IoT機器、通信機器、回線の冗長化<br>・IoT機器、通信機器の予備機、予備回線、無停電電源装置の確保<br>・IoT機器、通信機器、回線の品質管理 | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)、通信機器、回線の冗長化や、無停電電源装置の導入、予備機確保による故障発生時の迅速な交換対応を行う。また、IoT機器、通信機器の可用性を実現するため、情報(データ)の送受信が行えない場合に情報(データ)を再送する設計、情報(データ)が欠損した場合でもIoT機器の継続動作が可能な設計を行う。これにより、IoT機器、回線に不具合が生じた場合でもIoT機器の稼働が完全に停止してしまうことを防ぐ。 | マニュアル | 任意 |
| 11 | STEP1 | IoT機器への物理的セキュリティ対策<br>・不要なポート(ネットワークポート、USB、シリアルポート等)の閉塞                                                | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)本体に対し、不要なネットワークポート、USB、シリアルポート等の物理的な閉塞を行う。この対策を行うことで、IoT機器に対する許可されたユーザ以外の不正アクセスによる内容の参照、マルウェアに感染等による情報(データ)の漏えいを防ぐ。                                                                                  | マニュアル | 任意 |
| 12 | STEP1 | IoT機器への物理的セキュリティ対策<br>・監視カメラによる現場の監視                                                                    | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)の導入エリアに対し、使用する鍵・入退室リストの管理、生体認証の導入、監視カメラの設置、持ち物や体重検査等の対策を実装する。この対策を行うことで、IoT機器導入エリアに対する入退場の状況を確認でき、不正侵入者を検知することができる。                                                                                  | マニュアル | 任意 |
| 13 | STEP1 | IoT機器の適切なセキュリティ設定の実施<br>・工場出荷時のパスワードの変更                                                                 | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に対し、強固なパスワードの設定を行うことで、IoT機器への不正ログインによるIoT機器の設定変更や、IoT機器が収集した情報(データ)の漏えい等の被害を防ぐ。                                                                                                                      | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                 | 対策ポイント                                                                                                                                                           | 区分    |    |
|----|-------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 14 | STEP1 | IoT機器の適切なセキュリティ設定の実施<br>・IoT機器の利用環境に適した設定値の利用（工場出荷時の設定値を使用しない）       | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に対し、パスワードの定期的な変更、IoT機器上の不要なサービスの停止、利用環境に適した設定値を使用する等の対策を行うことで、IoT機器への不正ログインによるIoT機器の設定変更や、IoT機器が収集した情報（データ）の漏えい等の被害を防ぐ。 | マニュアル | 任意 |
| 15 | STEP1 | 不正ソフトウェアの搭載を防ぐ仕組みを実装したIoT機器の導入<br>・導入するIoT機器に搭載されているソフトウェアを事前に確認する   | 現場(浄水場、配水地等)へ導入するIoT機器(監視カメラ、IoTゲートウェイ等)に対し、搭載されているソフトウェアを事前に確認する運用を行うことで、意図しないソフトウェアの動作による誤動作、マルウェア感染等による情報（データ）の漏えい、IoT機器での不正な情報（データ）の生成を防ぐ。                   | マニュアル | 任意 |
| 16 | STEP1 | 不正ソフトウェアの搭載を防ぐ仕組みを実装したIoT機器の導入<br>・導入後のIoT機器に対し、ソフトウェアの追加インストールを制限する | 現場(浄水場、配水地等)において、ソフトウェアのインストールを制限する機能を実装したIoT機器(監視カメラ、IoTゲートウェイ等)を導入することで、意図しないソフトウェアの動作による誤動作、マルウェア感染等による情報（データ）の漏えい、IoT機器での不正な情報（データ）の生成を防ぐ。                   | マニュアル | 任意 |
| 17 | STEP3 | セキュリティバイデザインの実践<br>・あらかじめセキュリティ対策が実装されたIoT機器の選択                      | あらかじめセキュリティ対策が実装されたIoT機器(監視カメラ、IoTゲートウェイ等)を現場(浄水場、配水地等)へ導入することで、運用フェーズでのIoT機器へのセキュリティ対策費用の増加を防ぐ。                                                                 | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                            | 対策ポイント                                                                                                                                                                        | 区分    |    |
|----|-------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 18 | STEP3 | リスク管理<br>・IoT機器の保守契約手続き                                                         | 問い合わせ窓口やサポート体制等が確立されたIoT機器(監視カメラ、IoTゲートウェイ等)を選定することで、IoT機器提供業者からの定期的な修正プログラムの入手、IoT機器故障発生時の交換作業を迅速に行うことができ、IoT機器のセキュリティレベル低下、業務運用効率の低下等を防ぐ。                                   | マニュアル | 任意 |
| 19 | STEP3 | IoT機器の動作の正当性確認<br>・現場のIoT機器がサイバー空間から送信された処理結果と実際のIoT機器の動作結果と比較して、異常の検知や動作の停止を行う | 現場(浄水場、配水地等)において、サイバー空間から現場のIoT機器へ送信した結果と、IoT機器の動作結果を比較し、不正と判断できる動作結果をIoT機器が検知する機能安全の仕組みを実装する。これにより、IoT機器の誤動作による現場人員の怪我、IoT機器の破損を防ぐ。                                          | マニュアル | 任意 |
| 20 | STEP3 | リモートアップデート機能の提供<br>・IoT機器に対する迅速な脆弱性対策の実施                                        | 現場(浄水場、配水地等)において、脆弱性が残存したIoT機器が稼働し続けることで、外部からの不正アクセスを引き起こしやすくなる。IoT機器(監視カメラ、IoTゲートウェイ等)に対し、リモート環境から迅速に脆弱性対策を行うことで、IoT機器に対する不正アクセスによる、情報(データ)の漏えい、IoT機器での不正な取得データの生成を防ぐことができる。 | マニュアル | 任意 |

## ライフサイクル

全体計画



システム導入



IoT機器導入



運用・保守



廃棄

## セキュリティ管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                        | 対策ポイント                                                                                     | 区分    |    |
|----|-------|---------------------------------------------|--------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP3 | 定期的な教育・訓練<br>・従業員向けの定期的なセキュリティ対策教育の実施       | セキュリティ対策を考慮した運用について、水道事業者内の全従業員へ教育により周知徹底し、定期的な見直しを行うことで、セキュリティ問題発生時の対応の遅れ、被害の防止、被害の拡大を防ぐ。 | マニュアル | 任意 |
| 2  | STEP3 | 定期的な教育・訓練<br>・従業員向けの定期的なセキュリティインシデント対応訓練の実施 | セキュリティ問題が発生した時の対応を水道事業者内の全従業員へ教育により周知徹底し、定期的な見直しを行うことで、セキュリティ問題発生時の対応の遅れ、被害の防止、被害の拡大を防ぐ。   | マニュアル | 任意 |

## システム管理責任者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                           | 対策ポイント                                                                                                 | 区分    |    |
|----|-------|--------------------------------|--------------------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP3 | IoT機器の資産管理<br>・IoT機器の資産の棚卸しと管理 | 現場(浄水場、配水地等)において、無断で導入された監視カメラ、IoTゲートウェイ等、資産管理されていないIoT機器が知らないうちにマルウェアに感染することによる、セキュリティインシデントの対応遅れを防ぐ。 | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                                              | 対策ポイント                                                                                                                                                                                      | 区分    |    |
|----|-------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP1 | IoT機器の認証とアクセス管理<br>・セキュリティポリシーに従ったアクセス権の定義                                                        | 水道CPSシステムの構成要素へのアクセスを制限し、許可された対象のみにアクセスを許容する。<br><br>許可された対象からのアクセスは、予め設定された権限の範囲に制限する。                                                                                                     | 標準仕様  | 必須 |
| 2  | STEP1 | IoT機器、通信機器、回線の故障予防、復旧対策<br>・IoT機器、通信機器、回線の定期メンテナンス<br>・IoT機器、通信機器、回線の故障の検知<br>・IoT機器、通信機器、回線の交換作業 | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)、通信機器、回線の定期メンテナンスや、故障検知機能の実装、IoT機器交換作業の明確な手順の確立等の品質管理を徹底する。これにより、IoT機器、通信機器、回線で不具合が生じた場合においても迅速な原因の特定、サービスの復旧等により、被害の拡大を防ぐことができる。                  | マニュアル | 任意 |
| 3  | STEP1 | IoT機器への悪意のあるコードの混入防止<br>・IoT機器に対するウイルスチェックの実施                                                     | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)で定期的にウイルスチェックを行うことで、IoT機器のマルウェアに感染等による情報(データ)の漏えいや、IoT機器での不正な情報(データ)の生成を防ぐことができる。                                                                  | マニュアル | 任意 |
| 4  | STEP1 | IoT機器の継続的な脆弱性対策<br>・IoT機器のセキュリティパッチの定期的な更新                                                        | 現場(浄水場、配水地等)において、脆弱性が残存したIoT機器が稼働し続けることで、外部からの不正ログイン・不正操作・不正参照を引き起こしやすくなる。IoT機器(監視カメラ、IoTゲートウェイ等)に対し定期的な脆弱性対策を行うことで、IoT機器に対する不正ログイン、マルウェアに感染等による、情報(データ)の漏えい、IoT機器での不正な情報(データ)の生成を防ぐことができる。 | マニュアル | 任意 |

## CPS実装におけるセキュリティ対応マニュアル

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                        | 対策ポイント                                                                                                                                                                                               | 区分    |    |
|----|-------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 5  | STEP3 | 正規アップデートの利用<br>・IoT機器の提供者より公開された正規アップデートの利用 | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)のアップデートファイル(マルウェア対策ソフトの最新の定義ファイル、ファームウェア、不具合修正パッチ等)提供元の真正性を確認することで、不正なアップデートファイルをIoT機器へ適用することによるマルウェアの感染等の問題を防ぐ。                                            | マニュアル | 任意 |
| 6  | STEP3 | リスク管理<br>・IoT機器に関する脆弱性情報の収集                 | セキュリティベンダが用意した脅威情報サイトの情報を逐次入手することで、最新のセキュリティインシデント情報や、現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)に関する脆弱性情報を把握することができる。IoT機器に脆弱性がある場合、IoT機器の提供者より修正パッチを入手し該当のIoT機器へ適用することで、CPS全体のセキュリティレベルの低下を防ぐことができる。 | マニュアル | 任意 |

## ライフサイクル

全体計画

システム導入

IoT機器導入

運用・保守

廃棄

## 生産技術担当者が実施すべきセキュリティ対策

| 項番 | STEP  | 対策内容                                                                      | 対策ポイント                                                                                                                                                            | 区分    |    |
|----|-------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 1  | STEP1 | IoT機器廃棄時に識別子の完全削除<br>・IoT機器固有の識別子を読み取りできない状態にする                           | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)の廃棄時に、IoT機器内部に保存されている正規IoT機器を一意に識別するID(識別子)や認証情報を読み取りできない状態(記憶領域の物理的破壊、製造元指定の方法等)にする。これにより、これらの情報を流用した不正なIoT機器の流通を防ぐ。    | マニュアル | 任意 |
| 2  | STEP1 | IoT機器、外部記憶媒体廃棄時の情報(データ)完全削除<br>・IoT機器、外部記憶媒体に保存されている情報(データ)を読み取りできない状態にする | 現場(浄水場、配水地等)に設置されたIoT機器(監視カメラ、IoTゲートウェイ等)や外部記憶媒体の廃棄時に内部に保存されている情報(データ)を読み取りできない状態(記憶領域の物理的破壊、製造元指定の方法等)にする。これにより、廃棄後の情報(データ)を読み取られることによる設計情報データなどの情報(データ)の漏えいを防ぐ。 | マニュアル | 任意 |

**END**



2018年3月

株式会社 日立製作所 IoT推進本部  
IoTプロジェクト推進本部  
サイバー・フィジカル・システム部

**HITACHI**  
Inspire the Next 