「水道分野における情報セキュリティガイドライン」
（第 4 版）

平成 31 年3月

厚生労働省　医薬・生活衛生局　水道課

目次

1. 総則

1.1. 改訂の背景とポイント

日進月歩で発展するICT（Information and Communication Technology、情報通信技術）により、社会生活は大きな発展を遂げる一方、ICTへの依存度が高まるにつれ、これまで以上にサイバー攻撃に対するセキュリティ（以下「サイバーセキュリティ」という。）を含む情報セキュリティの取組の必要性が増している。特に、東京2020オリンピック・パラリンピック競技大会（以下「東京2020大会」という。）を控える我が国として、サイバーセキュリティの取組は急務である。

厚生労働省では、水道事業者及び水道用水供給事業者（以下「水道事業者等」という。）が自ら実施する情報セキュリティ対策の参考となるよう、「水道分野における情報セキュリティガイドライン（第3版）」（2013年6月）を策定しているところであるが、それ以降、情報セキュリティの取組は、ヒトやモノを繋ぐというICTの特徴を踏まえ単独ではなく関係機関との連携が重要である点や、目まぐるしいICTの発展とサイバー攻撃の複雑化・巧妙化に対応する点から、重要インフラ（情報通信、金融、鉄道、電力、ガス、医療、水道等）における情報セキュリティに対する政府や重要インフラ事業者等の共通の行動計画の見直し等が政府により行われてきたところである。

また、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（平成30年4月4日サイバーセキュリティ戦略本部）では、重要インフラ事業者等が、重要インフラ分野の特性に応じた必要な又は望まれる情報対策を着実に実施するとともに、情報セキュリティ対策を継続的に改善していくことの重要性を指摘している。

このため、情報セキュリティに対するこれらの背景を踏まえ、「水道分野における情報セキュリティガイドライン（第4版）」（以下「ガイドライン」という。）を策定するものであり、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示したものとして、上記の安全基準等策定指針における「安全基準等」に位置づけられるものである。

ガイドラインの策定に当たっては、「重要インフラの情報セキュリティ対策に係る第4次行動計画」（平成29年4月18日サイバーセキュリティ戦略本部決定、平成30年7月25日サイバーセキュリティ戦略本部改定）（以下「第4次行動計画」という。））等を参考にしており、第3版のガイドラインからの主な改訂のポイントは、次のとおりである。

【主な改訂のポイント】

① PDCA サイクルによる情報セキュリティ対策の実施と見直しの考え方の充実（1.2 関係（全般））

- 水道事業者等における情報セキュリティ対策は、PDCAサイクルを踏まえて継続的に改善していくことが重要である点を強調するとともに、その点が明確となるよう章立てを構成した。
- 具体的には、D（実行）として第6章に「訓練の実施」を新たに追加するとともに、C（監査）として第7章に「監査」を設け内容を充実させた。

② 情報セキュリティの取組における経営層の役割の追加、最高情報セキュリティ責任者の役割の充実（2.2 関係）

- 情報セキュリティに対する取組を推進又は支援することは、経営層として果たすべき役割の一つであるという観点から、経営層が担う具体的な役割を新たに明記した。
- 最高情報セキュリティ責任者の実施する活動として、リスクの認識と組織全体での対応方針の策定、必要な資源（予算、人材等）の確保等、具体的な内容を新たに明記した。

③ インシデント発生時における対応の追加（4 関係）

- インシデントが発生した際の対応計画（コンティンジェンシープラン）を事前に策定する必要があること等を新たに明記。
- コンティンジェンシープラン内容として、被害の拡大抑制（インシデントハンドリング）のための措置と、重要サービスの継続（IT-BCP）に必要な措置について整理した。

④ 平時及びインシデント発生時における関係機関との連携体制の追加（5 関係）

- 事業者だけでは、サイバー攻撃等に対処しきれないこともあることから、平時における関係機関との情報交換や、インシデント発生時における関係機関との情報連絡の必要性を明記するとともに、関係機関の役割を整理。

⑤ その他

- 制御系システムにおける対応として、多層的な防御の実施の必要性を強調するとともに、古いバージョンのOSのアップデート等の具体的対策を明記するなどの追加等を行った。

（参考）重要インフラにおける情報セキュリティに係る主なガイドライン等の策定状況

	内閣官房情報セキュリティセンター（NISC）			厚生労働省医薬・生活衛生局水道課
	行動計画	指針	指針対策編　他	ガイドライン
平成 17 年 12 月 13 日	重要インフラの情報セキュリティ対策に係る行動計画			
平成 18 年 2 月 2 日		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針		
平成 18 年 10 月 31 日				水道分野における情報セキュリティガイドライン
平成 19 年 6 月 14 日		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針改定版		
平成 20 年 3 月 27 日				水道分野における情報セキュリティガイドライン（改訂版）
平成 22 年 2 月 3 日	重要インフラの情報セキュリティ対策に係る第 2 次行動計画			
平成 22 年 5 月 11 日		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第 3 版）		
平成 22 年 7 月 30 日			重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第 3 版）対策編	
平成 24 年 4 月 26 日	重要インフラの情報セキュリティ対策に係る第 2 次行動計画　改定版			

平成 25 年 2 月 22 日		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第 3 版）改定版		
平成 25 年 3 月 26 日			重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第 3 版）対策編改定版	
平成 25 年 6 月 3 日				水道分野における情報セキュリティガイドライン（第 3 版）
平成 26 年 5 月 19 日	重要インフラの情報セキュリティ対策に係る第3次行動計画			
平成 27 年 5 月 25 日		重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 4 版）	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 4 版）対策編	
平成 29 年 4 月 18 日	重要インフラの情報セキュリティ対策に係る第4次行動計画			
平成 30 年 4 月 4 日		重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第 5 版）	重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書	
平成 30 年 7 月 25 日	重要インフラの情報セキュリティ対策に係る第4次行動計画（改定）			
平成 31 年 3月 29 日				水道分野における情報セキュリティガイドライン（第 4 版）

1.2. ガイドラインの構成と凡例

(1) ガイドラインの構成

ガイドラインの構成は、情報セキュリティ対策を継続的に改善していくことが重要であるとの観点から、PDCA サイクルを踏まえた構成としている。

「2. 体制の構築」では、平時及びインシデント発生時における情報セキュリティを担う体制の在り方について規定している。「3. 対策の実施」では、情報セキュリティにおけるインシデントの発生を防ぐための予防措置の在り方について規定している。「4. インシデント発生時の対応」では、インシデント発生の対応として、インシデントハンドリング及び IT-BCP の在り方について規定している。最後に、「5. 関係機関との連携」では、平時及びインシデント発生時における情報セキュリティに関係する機関との連携の在り方について規定している。これら 4 つのパートが、PDCA サイクルのうち P（Plan：計画）に該当する部分である。

以下、「6. 訓練の実施」が D（Do：実行）、「7. 監査の実施」が C（Check：監査）に該当する。これらのパートを踏まえ、P で検討した各種の体制や計画の実行性を検証し、実行性に課題がある場合は、A（Action：改善）を実施することが必要である。

(2) ガイドラインの凡例

ガイドラインでは、次のとおり、目的に応じて枠の意味や言葉の使い方を統一している。

① 枠の凡例

下記の枠（二重実線枠）は、各パートにおいて水道事業者等が実施すべき取組を列記している。

下記の枠（一点鎖線）は、各パートにおいて水道事業者等が参照するとよい資料や事例を列記している。

② 言葉の使い方の凡例

言葉の使い方の凡例は、下記のとおりである。

表 1-1: 言葉の使い方の凡例

#	言葉使い	用法
1	~必要である	最低限実施すべき取組
2	~望ましい	できる限り実施することが望ましい取組

1.3. 用語の定義

ガイドラインの中で使用される用語の定義は、下記のとおりである。

表 1.3-1:用語の定義・用語集

あ	
安全区域 【あんぜんくいき】	電子計算機、通信回線装置を設置した部屋の内部で、部外者の進入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域のこと。
インシデント	情報システムに対して発生した事故や事案の総称。
インシデントハンドリング	コンティンジェンシープランとして、インシデント発生の早期覚知と被害の拡大抑制を図る活動。
受け渡し業者 【うけわたしぎょうしゃ】	安全区域において作業している水道事業従事者との物品の受け渡しを目的とする者のことで、宅配便の集配、事務用品の納品などを行うものなどが例として挙げられる。
か	
可用性 【かようせい】	情報へのアクセスを許可された者が、必要時に中断なくアクセスできる状態を確保すること。滅失や紛失、あるいは利用不可能となると事業遂行に大きく影響する情報は、可用性確保に対してレベルの高い対策が求められる。 ～レベルについて～ 可用性 2 情報:　水道事業で取り扱う情報(書面を除く)の内、その滅失や紛失、あるいは利用不可能となると事業遂行に大きく影響する情報のこと 可用性 1 情報:　可用性 2 情報以外の情報のこと

完全性 【かんぜんせい】	情報が破壊、又は、改ざん、消去されていない状態を確保すること。改ざん、又は、誤びゅう、破損により国民（水道サービス利用者）の権利が侵害されたり、水道事業の的確な遂行に支障をきたしたりするような情報は、完全性確保に対してレベルの高い対策が求められる。 ～レベルについて～ 完全性 2 情報：　水道事業で取り扱う情報（書面を除く）の内、改ざん、又は、誤びゅう、破損により国民（水道サービス利用者）の権利が侵害されたり、水道事業の的確な遂行に支障をきたしたりするような情報 完全性 1 情報：　完全性 2 情報以外の情報のこと
機密性 【きみつせい】	情報に関してアクセスを認可された者だけがこれにアクセスできること。秘密文書に相当するものは要機密情報として機密性が最も高く定義される。 ～レベルについて～ 機密性 3 情報：　水道事業で取り扱う情報の内、秘密文書に相当する機密性を要する情報のこと 機密性 2 情報：　秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報のこと 機密性 1 情報：　機密性 3 情報、又は機密性 2 情報以外の情報のこと
クラウドコンピューティング 【くらうどこんぴゅうてぃんぐ】	データサービスやインターネット技術等がネットワーク上にあるサーバ群（クラウド（雲））にあり、ユーザーは今までのように自分のコンピュータで加工・保存することなく、「どこからでも、必要なときに、必要な機能だけ」を利用することができるコンピュータネットワークの利用形態。
コンティンジェンシープラン 【こんてぃんじぇんしーぷらん】	インシデント発生時にその被害の軽減と早期の復旧を目指す計画の総称。
さ	

識別コード 【しきべつこうど】	情報システムにアクセスする主体を特定するために情報システムが認識するコード（符号）のこと。原則として、一つの主体と一つの情報システムの組み合わせに対して一つの識別コードが付与されなければならないが、情報システムの制約、利用状況に応じて「共用識別コード」として複数主体に共用されることもあり得る。
主体 【しゅたい】	情報システムにアクセスする人、あるいは装置のこと。
主体認証 【しゅたいにんしょう】	識別コードを提示した主体が、その識別コードを付与された正当な主体であるか否かを、識別コードと併せて提示された主体認証情報とで認証することを主体認証という。主体認証情報の例としてはパスワードなどがある。
水道事業従事者 【すいどうじぎょうじゅうじしゃ】	各水道事業等の職員、並びに各水道事業等の指揮命令に服している者の内、各水道事業等の管理対象である情報、及び情報システムを取り扱う者のこと。
スマートデバイス 【すまあとでばいす】	情報処理端末（デバイス）のうち、単なる計算処理だけでなく、あらゆる用途に使用可能な多機能端末のこと。明確な定義はないが、スマートフォンやタブレット型 PC 等を総称するものとして用いられている場合が多い。
セプター 【せぷたあ】	CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）のこと。 情報共有・分析機能を意味し、それぞれの重要インフラごとに整備される。水道分野のセプターの事務局は、公益社団法人日本水道協会が担っている。さらに、各重要インフラ間の横断的な情報共有を図る目的で「重要インフラ連絡協議会（セプターカウンシル）」が設置されている。
ソーシャルネットワーキングサービス 【そうしゃるねっとわあきんぐさあびす】	SNS（Social Networking Service）のこと。人と人とのつながりを促進・サポートする、コミュニティ型のウェブサイト。知人等とのコミュニケーションや、新たな人間関係を構築する場を提供する会員制サービスのこと（SNS を参照）。
た	
端末 【たんまつ】	水道事業従事者が直接操作を行う電子計算機のことで、PC の他に PDA なども含まれる。

庁舎内 【ちょうしゃない】	水道事業従事者が所属し、水道事業において管理される組織、建物、部屋などの庁舎の内のこと。必ずしも一つの建物ではなく、独立した複数の「庁舎内」が存在する場合もある。
電子計算機 【でんしけいさんき】	コンピュータ全般のことを指し、情報システムを構成するサーバや端末、周辺機器などの装置全般のことをいう。
取扱制限 【とりあつかいせいげん】	情報の取扱いについて、複製禁止、持ち出し禁止、再配布禁止、暗号化必須、読後廃棄などの制限事項をいう。
な	
は	
標的型攻撃 【ひょうてきがたこうげき】	複数の攻撃手法を組み合せ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃。
ま	
や	
要安定情報 【ようあんていじょうほう】	滅失や紛失、あるいは利用不可能となると事業遂行に大きく影響する情報は可用性確保に対してレベルの高い対策が求められる。このような情報のことを要安定情報と言う。
要機密情報 【ようきみつじょうほう】	機密文書に相当するものは要機密情報として機密性が最も高く定義される。また、機密文書ではないが、一般に公表することを前提としていないため比較的機密性が高いと言えるものも要機密情報とされる。
要保全情報 【ようほぜんじょうほう】	改ざん、又は、誤びゅう、破損により国民（水道サービス利用者）の権利が侵害されたり、水道事業の的確な遂行に支障をきたしたりするような情報は完全性確保に対してレベルの高い対策が求められる。このような情報のことを要保全情報という。
要保護情報 【ようほごじょうほう】	要安定情報、要機密情報、要保全情報をまとめて要保護情報という。
ら	

ライフサイクル 【らいふさいくる】	ガイドラインでは情報システムや情報のライフサイクルの意味で使っている。 情報システムの場合は、その計画、設計、実装、運用、廃棄を指し、情報の場合は、その発生、利用（複製、移送、提供を含む）、保存、消去を指す。
わ	
A.B.C.～	
BCP	BCP（Business Continuity Plan）のこと。企業等のリスクマネジメントの一部であり，災害や情報システムのトラブルに対し事業を形成する業務プロセスや資産を的確に守るための計画のことを指す（事業継続計画を参照）。
CSIRT	Computer Security Incident Response Team の略。サイバー攻撃による情報システムの不具合など、コンピュータセキュリティに係るインシデントに対処するための組織のこと。なお、事業者によって CSIRT を組織として常設している場合とインシデント発生時のみ設置する場合がある。
IT-BCP	重要インフラサービスの提供に必要な情報システムに関する事業継続計画。IT（Information Technology）は情報技術。BCP（Business Continuity Plan）、事業継続計画のことであり、企業等のリスクマネジメントの一部であり、災害や情報システムのトラブルに対し事業を形成する業務プロセスや資産を的確に守るための計画のことを指す。
J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japan の略で、独立行政法人情報処理推進機構（IPA）が取り組んでいる官民連携によるサイバー攻撃に関する情報共有の取組。IPA を情報ハブ（集約点）として、参加組織間で情報共有を行い、高度なサイバー攻撃への対策に繋げていくことを目的としている。

1.4. ガイドライン活用の判断基準

ガイドラインで以降に示される個々の対策の実施内容については、その必要性をそれぞれの情報システム及び情報について検討し、必要と判断される場合に実施する。

実施すべき対策については、各水道事業等の規模（給水量、人員、財政状況）や地域水道ビジョン等における水道として目指す目標レベルに応じて、各水道事業者等が実現レベル、実現方法を決定するものとし、ガイドラインに示すとおりに実施することを強制するものではない。特に小規模の水道事業者等においては、その帰属する地方公共団体が運用する情報セキュリティの対策により包括的に対応すること等も含めてセキュリティ確保に努めることにより、水道事業者等による独自でのセキュリティ対策組織等は簡素化できる可能性がある。

なお、ガイドラインに記載した事項は各自治体が定めるセキュリティポリシーと対立するものではなく、重要インフラの視点から事業継続の確保のための対策をより積極的に強化することが求められる。水道用水供給事業と受水団体との関係においては、システムの一部共有やデータの連携等を行っている場合、両者の情報セキュリティ対策を尊重し、対応を協議することが求められる。

浄水場の維持管理等の業務委託、情報システムの構築及びメンテナンスの委託等の外部委託においては、受託者に水道事業者等（あるいは地方自治体）の情報セキュリティ対策の遵守を要求する。

2. 体制の構築

2.1. 概要

水道事業者等が情報セキュリティ等の取組を実施する上で必要となる、平時及びインシデント発生時の体制を構築する。

- □ 水道事業者等として経営層や幹部職員を加えた事業者全体としての体制を構築する
- □ 経営層や幹部職員、一般職員が果たす役割を明確にする
- □ インシデント発生時における連絡体制、対応体制を明確にする

2.2. 平時からの体制

情報セキュリティ対策を確実に実行してその効果を発揮するためには、セキュリティ対策を実施するため、経営層から幹部職員、一般職員までの個々の役割と責任が明確となった情報セキュリティ体制の確立が必要である。

(1) 経営層

情報セキュリティに対する取組を推進又は支援することは、経営層として果たすべき役割の一つであり、責任である。経営層自らがリーダーシップを発揮し、水道事業者等として情報セキュリティに取り組む必要がある。なお、「サイバーセキュリティ経営ガイドライン Ver2.0」（平成 29 年 11 月経済産業省／独立行政法人情報処理推進機構）」に記載されている「経営者が認識すべき 3 原則」を参考に、経営層は下記の役割を担うことが望ましい。

表 2-1:経営層が担う役割

#	原則	内容
1	経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要	経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施すべきである
2	関係機関や委託先も含めたサプライチェーンに対するセキュリティ対策が必要	自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきである
3	平時及びインシデント発生時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示等、関係者との適切なコミュニケーションが必要	平時から関係者にサイバーセキュリティ対策に関する情報開示を行うこと等で信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである

(2) 幹部職員

① 最高情報セキュリティ責任者

最高情報セキュリティ責任者（CISO：Chief Information Security Officer）も、水道事業者等としての情報セキュリティの取組を組織的に推進する責任を有している。「サイバーセキュリティ経営ガイドライン Ver2.0」（平成 29 年 11 月経済産業省／独立行政法人情報処理推進機構）」に記載されている「サイバーセキュリティ経営の重要 10 項目」を参考に、次の活動を実施することが望ましい。

最高経営情報セキュリティ責任者は、水道技術管理者のような権限を持った幹部職員や情報セキュリティに関する知見を持ち、組織内で当該分野に関して権限と責任を付与できる幹部職員（部長級）が想定される。

表 2-2：最高情報セキュリティ責任者が実施する活動

#	項目
1	情報セキュリティに関するリスクの認識、組織全体での対応方針の策定
2	情報セキュリティに関するリスク管理体制の構築
3	情報セキュリティの対策に必要な資源（予算、人材等）の確保
4	情報セキュリティに関するリスクの把握とリスク対応に関する計画の策定
5	情報セキュリティに関するリスクに対応するための仕組みの構築
6	情報セキュリティ対策における PDCA サイクルの実施
7	インシデント発生時の緊急対応体制の整備
8	インシデントによる被害に備えた復旧体制の整備
9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
10	情報共有活動への参加を通じたサイバー攻撃情報の入手、有効活用及び提供

② 情報セキュリティ責任者

情報セキュリティ責任者は、部署単位及びその部署で管理しているシステムの情報セキュリティ対策を統括する。情報セキュリティに知見を有し、組織内に一定程度の権限と責任を持つ幹部職員（課長（係長）級）の職員が想定される。

③ 情報セキュリティ監査責任者

情報セキュリティ監査責任者は、情報セキュリティ対策の実施状況について監査

を行い、その結果を最高情報セキュリティ責任者に報告する。また、情報セキュリティ委員会（（４）参照）にオブザーバとして出席して助言を行うことが望ましい。情報セキュリティ監査責任者は、情報セキュリティ責任者に適切に助言を行い得る者が就くことが望ましく、実行を担保するために、水道事業者等の外部の者に依頼する（委託含む）ことも考えられる。

(3) 一般職員（情報セキュリティ等に知見のある職員）

水道施設における情報システムごとのセキュリティ対策を実施する。また、情報セキュリティ責任者の指揮のもと、部署単位のセキュリティ対策を中心となって実施することが望ましい。他の職員の対策について具体的な支援を行うとともに、事業認可者（厚生労働省又は都道府県）及び水道セプターとの連絡窓口を担うことが想定される。

(4) 情報セキュリティ委員会等

情報セキュリティ対策を円滑に実施するために委員会を設置して、ガイドラインを参考に水道事業者等独自の対策基準（内規）を作成する。また、対策の実施状況の確認、問題点の改善等について検討する。委員長は最高情報セキュリティ責任者が兼務し、委員は部署単位の情報セキュリティ責任者が兼務する等、部署や情報システムのセキュリティ対策の実効性の確保に努める。

2.3. インシデント発生時の体制

発生したインシデントを自ら検知又は検知した職員からの報告を受けた際に、インシデントによる被害の拡大を抑制するためのインシデント対応チームを予め構築しておくことが必要である。インシデント対応チームの構築については、水道事業者等の組織規模に応じていくつかのパターンが考えられるため、自組織の実情に応じた体制を構築することが必要である。

表 2-3:水道事業者等の組織規模別のインシデント対応チーム

#	組織規模	設置	担当者	インシデント対応チーム
1	比較的小規模の事業者で、専属のインシデント対応チームを設置できない場合	非常設	兼務	情報セキュリティに精通している職員が、業務の一部として、インシデント発生時にのみ対応チームを編成
2	比較的中規模の事業者で、専属のインシデント対応チームを設置が困難な場合	一部常設	専任・兼務	インシデント対応チームを平時から常設しているが、一部のチームメンバーは専任ではなく、チームのコアとなる職員のみが専任でチームを編成
3	比較的大規模の事業者で、専属のインシデント対応チームを設置できる場合	常設	専任	専任のメンバーによりインシデント対応チームを平時から専門部署として常設

3. 対策の実施

3.1 概要

水道事業者等は重点的に対策を講じるべきリスクを特定し、平時から各種の情報セキュリティ対策を実施する。

- □ 水道事業者等として重点的に対策を講じるべきリスクが何かについて特定する
- □ 洗い出されたリスクに対して必要な対策を実施する

3.2. 情報についての対策

(1) 情報の格付け

水道事業等において取り扱う情報は様々であり、そのセキュリティの程度は目的や用途により異なると考えられることから、情報の格付けを行い情報セキュリティの実施を確実なものとする必要がある。

- □ 情報セキュリティを実施する組織(情報セキュリティ委員会)は、水道事業等で取り扱う情報について格付け(重要度による分類:A～D)を行うとともに、それに応じた取扱制限の基準、期限を明示するための手順を用意すること
- □ 電磁的記録については機密性、完全性及び可用性の観点から要機密情報、要保全情報、要安定情報に分類し、書面については機密性の観点から分類すること

(2) 情報の取り扱い

① 情報の作成と入手

水道事業において取り扱う情報について、水道事業従事者の個々によりその取扱いについての認識が異なると情報セキュリティを確実に実施できない可能性が考えられる。したがって、情報の作成、入手の段階でその取扱いが定義されることが必要となる。

(業務以外の情報の作成、又は入手の禁止)

- □ 水道事業従事者が水道事業等の遂行以外の目的で情報システムに関わる情報を作成したり入手したりしないような措置を講じること

(情報の作成、又は入手における格付けと取扱制限)

- □ 水道事業従事者が情報の作成時、又は入手時に当該情報の格付けと取扱制限を検討するような措置を講じること
- □ この取扱制限については、当該情報の参照が許される者が認識できるように明示すること
- □ 既に格付けされた情報を引用する場合は、その情報について既定された取扱制限を継承しなければならない
- □ 格付けや取扱制限の変更を必要とすると考えられる場合は、そもそもの情報作成者、あるいは提供者に相談すること
- □ 相談を受けた者は、必要に応じて新たな格付けや取扱制限を決定すること

② 情報の利用

情報システムの利用者の認識不足に伴い、情報の利用が不適切となる場合が発生すると考えられるが、このことは情報セキュリティが損なわれるリスクを増大させるものとなるため、情報の利用についての対策が必要となる。

（業務以外の情報利用の禁止）

- □ 水道事業従事者が水道事業等の遂行以外の目的で情報システムに関わる情報を利用しないような措置を講じること

（格付けと取扱制限に沿った利用）

- □ 水道事業従事者がそれぞれに明示された格付け、取扱制限に沿って情報を利用するような措置を講じること

（要保護情報の利用）

- □ 要保護情報はその格付け、取扱制限を超えて、放置したり外部へ持ち出したりしてはならない
- □ また、必要以上に複製、配布してはならない
- □ 機密性について秘密文書と規定されるものは、その制限期間を明記し、期間中であっても格付けを下げる必要がある場合は、変更に必要な手続きをとって対応すること

③ 情報の保存

水道事業等を遂行する上で、業務の合理性から情報の保存を行う必要が認められる。情報が保存される限り情報セキュリティが損なわれる可能性も継続するため、保存に対する対策も必要となる。

（格付けに応じた情報の保存）

- □ 情報セキュリティ責任者は情報システムに保存された要保護情報について適切なアクセス制御を行い、保護を実施すること
- □ 水道事業従事者が、情報が保存された外部記憶媒体、書面について、情報の格付けに応じた適切な管理を行うような措置を講じること
- □ 電磁的な記録の場合は、情報の格付けに応じて暗号化や電子署名などの適用を行うこと
- □ バックアップは情報保護のために複写を実施するものであるが、その必要性について十分な検討を行った上で、実施することを定めること
- □ 災害等への対策が必要であれば、被災しないための対策を講じること

（保存期間）

- □ 保存期間が定められている情報について、保存期間中は適切に保存するための対策を講じるとともに、保存期間満了後はその期間延長が必要でない場合に速やかに消去すること

④ 情報の移送

情報はオンライン、あるいは外部記録媒体、書面などによって移送され得るが、いずれの場合も移送の機会が情報セキュリティを損ねないようにするための対策が求められる。

（情報の移送に関する許可及び届出）

- □ 情報の移送を必要とする場合は、当該情報の取扱制限に応じ、担当セキュリティ責任者の許可の取得、あるいは届出を実施すること
- □ 定常的に移送を行う必要のある情報については、その手順、保護対策について予め定めておくこと

（情報の送信と運搬の選択）

- □ 要機密情報の移送が必要な場合は安全確保に留意した上で、送信、又は運搬のいずれかを決定し、情報セキュリティ責任者に届け出ること

（移送手段の選択）

- □ 安全確保に留意して移送手段（送信や運搬の具体的な手段）を決定し、情報セキュリティ責任者に届け出ること

（書面に記載された情報の保護対策）

- □ 書面に記載された情報を移送する場合も、外見から内容がわからないようにしたり、「親展」に指定したりするなど、安全対策に留意すること

（電磁的記録の保護対策）

- □ 電磁的記録の移送においてはパスワード保護や暗号化などの安全対策を講じることも検討し、必要に応じて実施すること

⑤ 情報の提供

水道事業等の外部への情報提供を必要とする場合に、提供先での利用により情報セキュリティが損なわれないための対策を講じる必要がある。

（情報の公表）

- □ 情報を公表する場合、当該情報が公表を許されるものであることを確認しなければならない
- □ 電磁的記録を公表する場合は、付随して情報漏えい等について防止策を講じること

（他者への情報提供）

- □ 水道事業従事者が機密情報を水道事業等の外部へ提供する場合は、情報セキュリティ責任者の許可を得るようにすること
- □ 機密情報ではないが外部への提供に制限のあるものについて、外部へ提供する場合は情報セキュリティ責任者へ届け出ること
- □ 提供先において水道事業等において定められた格付け、取扱制限に沿って利用されるように対策を講じること
- □ 電磁的記録を提供する場合は、付随して情報漏えい等について防止策を講じること

⑥ 情報の消去

不要となった情報の放置は情報セキュリティを損ねる要因となりかねないため、適切に消去するための対策が求められる。

（電磁的記録の消去方法）

- □ 情報システムを構成する装置を廃棄する場合には、電磁的記録の全てを復元困難な状態にすること
- □ 他者へ装置を提供する場合は、復元困難な状態にする必要性を検討し、適宜実施するこ

と

□ 装置の設置場所が安全とは言えない状況（無人、外部への開放など）に置かれる場合は、要保護情報は復元困難な状態にすること

（書面の廃棄方法）

□ 電磁的記録同様、復元困難な状態とするためにシュレッダーでの裁断、焼却、溶解などの措置を講ずること

3.3 リスク分析

水道事業者等が保有する全ての情報システムに対して、あらゆるリスクを想定した対策を講じることが望ましいが、現実的には困難である。そのため、重点的に対策を講じるべきリスクとは何かを定期的に分析することが必要である。なお、リスクアセスメントを実施する具体的な手法については、次の手引書等が参考となる。

【参考となる手引書等】

- 「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）」（平成 30 年 4 月サイバーセキュリティ戦略本部重要インフラ専門調査会）
- 「制御システムのセキュリティリスク分析ガイド第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」（平成 30 年 10 月独立行政法人情報処理推進機構セキュリティセンター）

なお、ガイドラインでは、主なリスクとして次を想定するが、水道事業者等としてリスクの加重、追加をして差し支えない。

表 3-1：想定されるリスク

#	要因	内容
1	サイバー攻撃をはじめとする意図的要因	不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス感染（標的型メール攻撃、危険性の高い USB）、サービス利用不能攻撃（DoS/DDoS）、情報漏えい、重要情報の搾取、内部不正 等
2	非意図的要因	開発・設計の不備、操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障 等
3	災害や疾病	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設（含むデータセンター）の損壊、大規模・広範囲にわたる疾病による要員不足 等
4	他分野の障害からの波及	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）等

3.4 対策を講じるべき情報システムの特定

(1) 優先サービスの選定

新たな脅威の発生や技術的脆弱性の発見に加えて、重要インフラ事業者等を取り巻く事業環境の変化や利害関係者からの新たな要求等によって、情報セキュリティに対して水道事業者等に求められる対応は絶えず変化するため、水道事業者等として想定すべきリスクも常に変化する。また、想定すべきリスクの対象も多岐にわたる。そのため、全てのリスクを洗い出し、それらに対して対策を講じることは不可能であることから、水道事業者等として防護し、継続すべき重要インフラサービスを優先サービスとして定め、対策を講じるべきリスクを限定せざるを得ない。

なお、ガイドラインでは、「住民に対する安全な水の供給」を優先サービスとして定めた。

(2) 優先的に対策を講じる情報システムの特定

上記で特定された優先サービスに必要不可欠な、防護・優先復旧すべき情報システムを特定する。インシデント発生時においても情報システムの運用を継続するためには、情報システムの運用を継続させるために必要となる、人員、サーバ、情報通信ネットワーク、データ、手順書、外部委託者等の構成要素に対して、網羅的に対策を実施することが重要である。そのためには、防護・優先復旧すべき情報システムを支える構成要素を特定しなければならない。特定しなければならない情報システムの構成要素、水道事業者等として検討の対象となる水道情報システムの種類、水道情報システムの資産区分は次のとおりである。

表 3-2:情報システムの構成要素

#	構成要素	構成要素の説明
1	施設※1	情報システム機器の設置環境(庁舎、データセンターの場所・堅牢性・自家発電設備の有無・代替環境の有無、電力系統の多重性等)
2	ネットワーク	情報システムを利用するために必要な情報通信ネットワーク(庁舎内及び拠点間等の外部)の敷設状況(利用キャリア・種類・ルート分散状況等)
3	周辺機器	複合機やプリンター等の設置状況、外付け HDD 等の管理状況(データの暗号化等)
4	ハードウェア	サーバ等のハードウェア機器の役割、台数及び所在(代替機がある場合はそれも含む)
5	システム領域	アプリケーションやシステム設定情報等の情報システム復旧に必要なデータの所在及び管理状況(バックアップ媒体の外部保管、データ暗号化及びデータ改ざん防止措置等)
6	データ領域	重要なデータの所在及び管理状況(バックアップ媒体の外部保管、データ暗号化及びデータ改ざん防止措置等)
7	システム運用体制	システムの被害状況の早期確認や適切な対応を実施するための運用の人的体制と役割分担、手順書の整備及び連絡手段の確保
8	ベンダの継続能力	非常時における情報システムベンダの支援・協力体制(ベンダの事業継続能力把握、サービス品質保証契約の締結等)

表 3-3:水道情報システムの種類

#	区分	システム名称	概要
1	制御系	浄水場の監視制御システム	浄水処理を適切に行うために、各種機器の働きを制御する一連のシステム
2		ポンプ場の運転システム	ポンプ吐出圧(水量)、運転台数等を制御するシステム
3		水運用システム	地区ごとの水需要(推定値)をもとに、複数の浄水場、配水場などからの送配水量について効率的に調整するためのシステム
4	技術系	管路情報システム	地理情報システムを利用して配水管等の位置情報及び施設情報を管理するシステム
5		電子ファイリングシステム	配水管工事竣工図、写真などイメージデータを管理するシステム
6		給水台帳システム	給水装置の情報(使用者の個人情報を含む)を管理するシステム
7		設備管理システム	浄水場や配水場などの機械、電気・計装設備の情報を管理するシステム
8		設計・積算システム	管路などの設計を支援する CAD システムと作成した設計図面をもとに積算を行う 2 つのシステムからなる
9		管網解析システム	配水管網内の水理状況、水質状況をシミュレーションするシステム
10	事務系	検針／水道料金システム	水道使用者のメータ水量を検針するためのシステム及び検針した値を使用者の個人情報などとともに一元的に管理するシステム
11		財務会計システム	予算、契約、決算等について管理するシステム
12		資産管理システム	水道事業者等の有する資産について償却状況、今後の見込みなどを管理するシステム
13		人事管理システム	職員の個人情報、人事考課、給与算定などを管理するシステム
14		文書管理システム	業務の中で発生する各種文書類を一元的に管理するシステム

表 3-4:情報システムの資産区分と内容

#	資産区分	内容
1	データ資産※2	データベース及びデータファイル、システム仕様に関する文書、操作マニュアル、その他記録保管された資料
2	ソフトウェア資産	システムソフトウェア、保守用ツール、など
3	ハードウェア資産	コンピュータ装置、制御装置、通信装置、記録装置、出力装置、その他(電源、空調)、什器
4	サービス資産	システムが行う計算処理及び制御、通信サービス、データ蓄積、出力など

※1 災害による障害の発生しにくい設備の設置及び管理

水道サービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい適切な場所を設置の際に検討するとともに、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施する等、適切な設備及び管理を行う仕組みを構築する必要がある。

※2 データ資産の管理

システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うとともに、事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する必要がある。

3.5 情報システムについての対策

(1) 主体認証機能

情報システムの利用において本来アクセス権限のない者が不正にアクセスすることで情報セキュリティが損なわれることを防止するため、情報システムにアクセスする者の主体認証を行うことが望ましい。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、全ての情報システムについて、情報システムの重要性及び取り扱う情報の制限に応じて主体認証機能の適用の必要性を検討する
- □ 主体認証が必要と決定された情報システムには、その機能を適用しなければならない
- □ 要保護情報を取り扱う情報システムについては、主体認証を必須とする
- □ 主体認証そのものを秘密に取り扱う必要がある場合は、そのための対策を講じること
- □ 主体認証情報の通信、保存においては暗号化を行うべきであり、不可能な場合はそのことを利用者に通知すること
- □ 主体認証を適切に機能させるために、主体認証情報の定期的な変更を求めること
- □ 主体認証情報が不正に利用されることが検知された場合は、直ちに主体認証の利用を停止する措置を講ずることができるようにしておくこと
- □ 主体認証に利用する情報や道具について、不正に利用されないための措置を講ずること
- □ 生体認証を利用する場合は当該者の同意を得た上で実施するものとし、認証以外の目的に利用しないこと、プライバシーを侵害しないことに留意すること
- □ 主体認証の機能には不正の検知、認証の記録、認証コードの共有においても個人を特定する機能等を盛り込むこと
- □ 水道事業従事者に対して、自己に付与された識別コードについて、自身のみの利用を実現するための規則を認識し、遵守させること
- □ 他者に付与された識別コードの利用を行ってはならない
- □ 識別コードを利用する必要がなくなった場合には、その識別コードが利用不可能となるための措置をとれるように、水道事業従事者は識別コードの管理者に届け出ること
- □ 人事異動などに応じて一斉かつ大量に識別コードの抹消が必要となるような場合は、届出を不要とするような規定を予め定めておくこと
- □ 管理者権限の識別コードは、管理者としての行動を行う場合にのみ利用することとしなければならない
- □ 主体認証情報は、それを不正に利用されないような対策を講ずること
- □ 不正に利用される危険が生じた場合、水道事業従事者は情報セキュリティ責任者に報告し、情報セキュリティ責任者は不正利用の防止措置を発動すること
- □ 主体認証情報を他人に知られたり、教えたり、忘却したり、紛失したり、盗まれたりしないように努めること

(2) アクセス制御機能

情報システムを認可された複数の主体が利用することになるが、これに応じて情報システムには重要度の異なる情報が共存することとなる。どの主体がどの情報にアクセスすることを許可されているのか、情報ごとのアクセス制御が望ましい。なお、主な対策は、次のとおりである。

- □ アクセス制御は全ての情報システムについて、その導入の必要性が検討されなければならず、特に要保護情報を取り扱う情報システムにおいては必須とすること
- □ アクセス制御が必要と判断された情報システムについては、アクセス制御機能を設けなければならない
- □ アクセス制御を強化するため、利用者の権限管理（属性）以外のアクセス制御機能として、利用時間による制御や端末指定による制御、強制アクセス制御等を導入すること
- □ 情報の格付け、取扱制限に沿って、情報システムに装備された機能を活用し、アクセス制御設定を実施しなければならない
- □ 規定されたアクセス制御を実施する機能が情報システムに装備されていない場合は、利用者が運用上で注意を払うことでアクセス制御を遵守すること

(3) 権限管理機能

主体認証やアクセス制御に関する情報の機密性、完全性を守らなければ不正アクセスの発生につながるため、この機密性、完全性を確保するための権限管理を行うことが望ましい。なお、主な対策は、次のとおりである。

- □ 全ての情報システムについて権限管理の必要性が検討されなければならず、特に要保護情報を取り扱う情報システムについては必須とすること
- □ 権限管理が必要と決定された情報システムには権限管理機能を導入しなければならない
- □ 権限管理を行うための識別コードは、権限管理機能のみを利用できるものとすること
- □ 主体認証情報の再発行が必要となる場合には、当該の主体が既に作成した情報への不正アクセスを防止する目的から、主体認証情報の再発行が自動化されること
- □ 権限管理操作の不正を防止するために、二人が関与しなければ権限管理操作が完遂しないデュアルロック機能を設けること
- □ 複数主体が共用する識別コードの利用については、情報システム毎の事情に応じてその可否を検討すること
- □ 原則として識別コードは主体個々に付与されること
- □ 権限管理については、権限管理を実施する者、主体情報の初期配布方法、アクセス制御の設定方法、変更管理手続きを明確に定めなければならない
- □ 主体の側からの申請に基づいて権限管理を行う方法では、その主体の正当性を確認する手続き、当該の主体に対してのみ発行する手続きが必要となる
- □ 識別コードの発行の際、その識別コードの共用可否を付与する主体に明示すること
- □ 管理者権限は職責に即して最小限の範囲に付与するものとし、過大に付与してはならない
- □ 権限管理者は、水道事業従事者が当該の識別コードを必要としなくなった場合にはそれを無効にしなければならず、主体認証情報格納装置を付与している場合はそれを返還させること
- □ 権限管理者は識別コードの追加、削除を実施する際には、不適切なアクセス制御、不要な識別コードの有無について点検を行うこと
- □ 識別コードは一人の主体に対して一つの情報システムで一つとすることが原則であり、これらの付与状況を記録しておくこと
- □ 一旦付与された識別コードをその後他の主体に付与することは禁止しなければならない
- □ 付与した識別コードが何らかの理由により使用できなくなった主体から代替手段の利用申請があった場合、権限管理者はその主体の正当性、代替手段の許可の必要性を検討し、必要が認められる場合にのみ代替手段を提供すること
- □ 識別コードの不正使用が認められた場合、ただちに識別コードの利用を停止させること

(4) 証跡管理機能

情報システムの制御、管理の実効性を高めること、情報セキュリティ上の問題発生時の対処を目的に証跡管理が求められる。証跡管理の実施が不正利用や過失の抑制、事後の追跡を可能とすることが望ましい。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、全ての情報システムについて証跡管理の必要性を検討し、必要と判断された場合には証跡管理機能を設けること
- □ 証跡の利用目的に有効な情報項目を検討し、その記録の設定を行うこと
- □ 証跡の取得ができなくなった場合、あるいはできなくなる恐れがある場合の対処方法とその機能を整備しておくこと
- □ 記録された証跡に対しても、消去や改ざん等の不正が行われることのないようにアクセス制御等の対策を講じること
- □ 証跡管理の効率化、合理化のために、証跡の点検、分析、セキュリティ検知事項の報告等について自動化機能等を設けること
- □ 情報セキュリティ責任者は、情報セキュリティ責任者が定めた操作に沿って証跡の記録を取得しなければならない
- □ 証跡の保存期間については情報セキュリティ責任者が定め、適切に保存し、期間満了後に延長の必要がなければ速やかに消去すること
- □ 証跡の取得ができなくなった場合、あるいはできなくなる恐れがある場合には、定められた対処方法を実施すること
- □ 情報セキュリティ責任者は、取得した証跡について定期的、あるいは必要に応じて点検、分析し、その結果に応じた情報セキュリティ対策を実施すること
- □ 実施した対策について情報セキュリティ責任者に報告すること
- □ 監視要員等は、情報セキュリティ侵害の可能性を検知した場合、予め定められた措置をとらなければならない
- □ 利用者に対しては証跡の記録、活用が行われることを周知しておかなければならない

(5) 信頼性確保のための機能

情報システムのトラブル等のリスクを減少させるとともに、システムの一部にトラブルが発生した場合にも継続して運用できるような対策を実施し、システムの信頼性を確保することが望ましい。なお、主な対策は、次のとおりである。

□ システム機器の処理を分散し、機器間での負荷を均等化する等負荷分散に努めること
□ システム機器の予備機の設置や、通信回線の複数化等、冗長化構成に努めること

(6) 暗号と電子署名(鍵管理を含む)

情報漏えい、改ざん防止に有効な具体的対策として、暗号化、電子署名の利用が望ましい。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、書面以外の電磁的記録における要保護情報に対して暗号化や電子署名の必要性を検討し、必要と判断される場合は適用すること
- □ 暗号化や電子署名を利用する際には、必要とされる安全性、信頼性について検討し、可能な限り電子政府推奨暗号リストに記載されたアルゴリズムを用いること
- □ アルゴリズムが暗号としての実用価値を失った場合に暗号化機能をすぐに交換できるように、複数のアルゴリズムを選択可能としたり、コンポーネント化したりして情報システムを構成しておくこと
- □ 暗号の復号、電子署名の付与に用いる鍵について第三者からの物理的な攻撃から保護するための耐タンパー性(解析の困難さ)を有すること
- □ 情報セキュリティ責任者は、選択したアルゴリズムが適切に実装されているか否かを確認しなければならない
- □ 暗号化、電子署名に用いる鍵について、その生成に関連する情報、保存規定等の鍵管理について、それらが露呈した場合の対策も含めて定めておくこと
- □ 電子署名については、その正当性を検証するための情報、手段を署名検証者へ提供しなければならない
- □ 鍵情報の紛失等に備えて、そのバックアップ、あるいは預託管理について定めておくこと
- □ 利用するアルゴリズムの評価(暗号としての実用的な価値)については、「電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト」であるCRYPTREC(Cryptography Research and Evaluation Committees)の発表に関心を払う等、情報収集を適切に継続すること
- □ 水道事業従事者が要保護情報の移送、外部記録媒体への保存に際して暗号化、電子署名付与の必要性を検討し、必要な場合はそれを実施させるような措置を講じること
- □ 水道事業従事者が鍵情報について適切な管理を実施するような措置を講じること

(7) セキュリティホール対策

情報システムを構成する装置において、動作するソフトウェアには悪意を持った第三者の攻撃対象となるセキュリティホールが存在する可能性がある。情報システムへの不正侵入、サービス不能攻撃、ウィルス感染、踏み台、情報漏えい等セキュリティ上の大きな脅威に繋がり、水道事業者等に対する社会的信用の失墜を招きかねない。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、情報システムを構成する装置について、セキュリティホール及びその対策の情報を収集し、運用開始時に適切に対応すること
- □ 要安定情報を取り扱う情報システムに対してセキュリティホール対策を講じる場合は、サービス提供が中断しないように装置の冗長性を確保すること
- □ 情報セキュリティ責任者は、構成する装置に変更があった場合、セキュリティホール対策に必要となる装置情報を更新すること
- □ 対象となる装置についてセキュリティホールに関する公開された情報を適宜入手すること
- □ 入手したセキュリティホール関連情報をもとにそのリスクを分析し対策計画を作成すること
- □ 対策計画に基づいて実施し、その記録を残すこと
- □ 対策の実施において留意しなければならない事項として、対策方法（対策用のファイル等）の入手は信頼のできる方法にて実施され、完全性検証方法が用意されている場合は、検証を実施すること
- □ 情報セキュリティ責任者は可能な限り短い周期で定期的にセキュリティホール対策の情報収集、状況確認を実施し、不適切な状態にある装置に対処すること
- □ セキュリティホールに関する情報を他の情報セキュリティ責任者と共有し、連携して対応すること

(8) 不正プログラム対策

不正プログラムによる感染は当該システム、並びにその他のシステムへのシステム破壊、サービス不能等につながる脅威となる。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、水道事業従事者に対して不正プログラム感染回避のための留意事項を含む日常的対策を定めること
- □ 装置に対してはアンチウィルスソフトウェアを導入し、不正プログラムの進入経路として想定される全てに対して対策を講ずること
- □ アンチウィルスソフトウェアは異なる複数の提供元のものを組み合わせて導入することで最新情報等への対応の時間的リスク分散に配慮すること
- □ 通信による不正プログラムの拡散を防ぐための対策を講じること
- □ 情報セキュリティ責任者は不正プログラムに関する情報収集に努め、必要に応じて水道事業従事者に対処の実施を指示すること
- □ 水道事業従事者にアンチウィルスソフトウェア等により定期的に全てのファイルについての検査を行わせ、検出された不正プログラムについては実行しないようにさせるとともに情報セキュリティ責任者へ報告させなければならない
- □ アンチウィルスソフトの導入がシステム運用の障害となる場合は、当該システムがウィルスのリスクから保護されるように、外部ネットワークとの分離等の措置を講ずること
- □ アンチウィルスソフトについては常に最新の状態を保つとともに、自動検査機能を有効にして利用すること
- □ 外部から取り込むファイルについても同様に必ず検査を行い、不正なものは取り込まないようにしなければならない
- □ 情報セキュリティ責任者は、不正プログラム対策について適宜状況把握を行い、見直しを行うこと
- □ 可能であれば、実施している不正プログラム対策で十分に対応できない事態に備えて専門家の協力を得られる体制を構築すること

(9) サービス不能攻撃対策

インターネットを経由してサービスを提供する情報システムでは、利用者の自由なアクセスによる利便性を確保するために、情報セキュリティが損なわれる可能性がある。これらのリスクにはサービス不能攻撃により当該システムのサービス利用が不可能となることや、当該システムが踏み台となって他社に対してサービス不能攻撃を行うこと等が考えられる。水道事業等では、インターネットを利用した監視制御機能等はこのようなリスクに対する対策を適切に検討し、サービスの可用性を確保することが望ましい。なお、主な対策は、次のとおりである。

- □ インターネットからのアクセスを受ける情報システムについては、その装置が装備している SYN Cookie、SYN Flood 対策機能等を活用してサービス不能攻撃対策を講ずること
- □ 情報セキュリティ責任者は、サービス不能攻撃を受けた場合に、装置を共用する他のサービスへの影響も考慮して通信回線装置、及び通信回線を構築すること
- □ 装置のうち、最も可用性を求められるものから優先順位を付けつつ、サービス不能攻撃に対する監視方法を定めておくこと
- □ 情報セキュリティ責任者は、要安定情報を取り扱う情報システムについて、サービス不能攻撃の影響を排除し、又は低減する対策装置を導入すること
- □ 実際にサービス不能攻撃を受けた場合に対しても、その対処を効果的に実施できるようにシステム操作のための通信回線の冗長化等を用意すること
- □ 水道事業者等側での装置だけではサービス不能攻撃を回避できない場合も考慮し、通信事業者との連携についても定めておくこと
- □ 情報セキュリティ責任者は装置の監視を十分に行い、記録を残すこと
- □ その記録をサービス不能攻撃の検知技術向上に反映し、対策そのものも適宜見直しを行うこと

(10) 安全区域の設定

情報システムの設置環境について、悪意のある者が接触できる状況では物理的な破壊や情報漏えい、改ざん等のリスクがある。また、設置環境によっては自然災害による損傷のリスクもある。これらのリスクに対応するために、安全区域を定めて対策をとることが望ましい。安全区域の具体例としては中央監視室、制御盤室等が相当する。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は定めた安全区域に不審者を立ち入らせない措置を講ずること
- □ できる限り障壁、施錠等の対策によりセキュリティレベルの異なる区域から隔離し、入退出を制限すること
- □ 入退出にあたっては主体認証を実施すること
- □ 主体認証により承認された者が未承認の者を同伴する等して入退室を行わないようにしなければならない
- □ 全ての入退出の理由や期間等の情報を記録したり、継続的に立ち入る者の承認手続きを設けたりすること
- □ 立ち入りが承認された者に変更がある場合は、その変更内容を事前に把握し記録する仕組みを構築すること
- □ 安全区域に訪問者がある場合、訪問者についてもその身分の確認、記録をすること
- □ 訪問者について、訪問相手となる水道事業従事者が訪問者を審査する手順（取次ぎ、出迎え等）を採用すること
- □ 訪問者に対しては必要以上に立ち入らないように制限を設け、さらには水道事業従事者が付き添うこと
- □ 入退室の承認にあたっては、その承認されているレベルを外見上で識別できるような仕組み（ストラップや ID カードの着用等）を導入すること
- □ 受け渡し業者との物品受け渡しについては、安全区域外で行う、あるいは情報システムに接触できない場所において水道事業者等が付き添う等の方策を講ずること
- □ 要保護情報を取り扱う情報システムについては装置を他の情報システムから物理的に隔離し安全区域を設定すること
- □ 要保護情報を取り扱う情報システムは安全区域から移動してはならない
- □ 要保護情報、要機密情報を取り扱う情報システムについては、その格付けに応じて、不正操作、盗み見、ケーブルからの盗聴、電磁波による漏えい等を防止する対策を講ずること
- □ 安全区域においては、立ち入りを承認されていることを確認できる身分証明書を他の職員から容易に常時視認できるように着用すること
- □ 要保護情報を取り扱う情報システムについては、安全区域への物品等の持ち込み、持ち出しについて情報セキュリティ責任者の承認を得るとともに、その記録を残すこと
- □ 当該の情報システムに関連しない情報機器を安全区域に持ち込むことについては制限を

定めること

- □ 安全区域での作業を監視するための措置（立会い、監視カメラ）を講ずること
- □ 要保護情報を取り扱う情報システムについて、自然災害、人為的災害から装置を保護するための物理的対策を講ずること
- □ 災害が発生した場合において、作業者の安全を確保した上で必要に応じて情報システムの電源を遮断できる措置を講ずること
- □ 停電等の要因により電力供給が途絶した場合において、情報システムへの影響を最小限とするため、必要に応じて予備電源を設ける等の措置を講ずること

(11) 電子計算機共通対策

ウィルス感染、不正侵入等の外部的要因により情報セキュリティを損なうことに加え、水道事業従事者の不適切な利用等の内部的要因により損なうことも起こり得る。これらのリスクについて対策を講じておくことが望ましい。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、電子計算機のセキュリティ維持に関する規定を整備すること
- □ 電子計算機の管理状況の確認等を容易にするためにも、全ての電子計算機について、管理する水道事業従事者、及び利用者を特定する文書の整備を行うこと
- □ 電子計算機の利用には主体認証、権限管理を導入しなければならない
- □ 全ての電子計算機についてセキュリティホール対策、アンチウィルスソフトを導入すること
- □ 適正な運用のために、仕様書や操作マニュアル等の電子計算機関連文書を整備すること
- □ 要保護情報を取り扱う電子計算機は安全区域に設置されなければならないが、移動体での利用については情報セキュリティ責任者の承認の下で例外とされ得る
- □ 電子計算機の設置にあたっては、処理性能確保のための設計やシステム品質確保等の対策を考慮するとともに、要安定情報を取り扱う電子計算機についてはサービスの可用性確保のために冗長構成とすること
- □ 機器納品時のマルウェア感染の可能性を考慮し、サプライチェーンにおける情報セキュリティを意識した機器を調達すること
- □ 情報セキュリティ責任者は、電子計算機のセキュリティ維持に関する規定に沿って運用管理を行うこと
- □ この規定は適宜見直しを行うこと
- □ 水道事業従事者に水道事業遂行以外の目的で電子計算機を利用させてはならない
- □ 情報セキュリティ責任者は、電子計算機のセキュリティ維持についてセキュリティホール、及び不正プログラムへの対策をとること
- □ 電子計算機を管理する水道事業従事者、電子計算機の利用者に変更が生じた場合、及び電子計算機の構成を変更した場合、これを管理文書に反映し保存すること
- □ 情報セキュリティ責任者は、電子計算機で利用される全てのソフトウェアについて定期的に状態把握を行い、不適切な状態にあるものを発見した場合は是正すること
- □ システムの統合、更新時には十分な検証等を行うこと
- □ 情報セキュリティ責任者は、電子計算機の運用を終了する場合に、ソフトウェアを利用したデータ消去、あるいは物理的破壊等により全ての情報を復元困難な状態にすること

(12) 端末

電子計算機のうち、特に端末についてはその利用者が必ずしも情報システムについての専門知識を持ち合わせていないことから、情報セキュリティを損ねる可能性が高くなる。また、可搬性が高いことから盗難等のリスクも高まる。なお、主な対策は、次のとおりである。

- □ 端末において利用可能なソフトウェアを規定する、あるいは利用禁止のソフトウェアを既定する等して制限を設けること
- □ 移動体については情報セキュリティ責任者の承諾のもとで利用するものとし、庁舎内で利用されるのと同等の保護手段が講じられること
- □ 特に要機密情報を取り扱う移動体では、内蔵記録媒体において暗号化を行うと同時に盗難防止の措置を講じること
- □ 必要に応じて情報を保存できない端末を利用すること
- □ 無用なリスクを避けるため規定のソフトウェア以外は利用してはならない
- □ 暗号化、盗難防止措置を必要に応じて講じること
- □ 水道事業従事者に情報システムセキュリティ責任者が許可を与えた通信回線、通信方法だけを利用させること
- □ 情報セキュリティが損なわれた場合やその可能性が検知された場合に記録の分析を適切に行えるようにし、情報システムに関わる全ての装置の時刻の同期を取っておくこと

(13) サーバ装置

サーバ装置は情報システムのサービスを提供するという性格上、その情報セキュリティが損なわれた場合の水道サービスの停止、水道事業への信用失墜等の影響範囲は大きなものとなりかねない。なお、主な対策は、次のとおりである。

- □ 通信回線を利用してサーバ装置の保守作業を行う場合は、必要に応じて送受信される情報の暗号化を行うこと
- □ サービスの提供、サーバ装置の運用管理に利用するソフトウェアは定めておかなければならない
- □ 利用が認められていないサーバアプリケーションは稼動させないことに加えて、利用が認められているサーバアプリケーションであっても利用しない機能は無効化すること
- □ 可能であれば、利用禁止のサーバアプリケーションはサーバ装置から削除しておくこと
- □ 情報セキュリティ責任者は定期的にサーバ装置の構成変更を確認し、それに伴うセキュリティへの影響について対応すること
- □ 要安定情報を取り扱うサーバ装置に対しては定期的にバックアップを取得し、取得した記録媒体は安全に管理すること
- □ サーバ装置に対する作業はその詳細（日時や内容）を記録すること
- □ 必要に応じて証跡管理を実施すること
- □ 端末同様にサーバ装置の時刻も同期すること
- □ サーバ装置について常時監視を行う措置をとり、不正検知、異常検知を行うこと
- □ 要安定情報を取り扱うサーバ装置についてはサービスの可用性を確保するために負荷分散のための措置を講ずること

(14) 通信回線を介して提供するアプリケーション共通対策

IP ネットワークの技術普及に起因する通信回線を介したセキュリティ脅威全般に関するリスクが存在する。情報システムのライフサイクル全般に対して適切な対策を実施することが望ましい。なお、主な対策は、下記のとおりである。

- □ 通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備すること
- □ 前述の規定に基づき、日常的、定期的に運用管理を実施すること
- □ 水道事業従事者に通信回線を介して提供されるサービスを私的な目的で利用させてはならない
- □ システムの統合・更新時には十分な検証等を行うこと

(15) 電子メール

電子メールについてはその不適切な利用、あるいは電子メールを利用した悪意のある行為等多くのリスクにさらされている。電子メールサーバを水道事業者等にて設置、運用する場合は、電子メールサーバの適切な管理、電子メールの適切な利用が望ましい。なお、主な対策は、次のとおりである。

- □ 電子メールサーバが電子メールの不適切な中継を行わないように設定すること
- □ 電子メールクライアントから電子メールサーバへの送受信における水道事業従事者の主体認証機能を備え、標的型攻撃の主な侵入経路である「なりすましメール」や「フィッシング」等への対策を講じること
- □ 水道事業従事者が水道事業遂行に関わる情報を含む電子メールを送受信させる場合、自身の水道事業等が運営、あるいは外部委託した電子メールサーバを利用させること
- □ 電子メールの利用に際して不正なスクリプト等の実行を回避するため、HTML メールの操作にあたってはこうしたリスクに留意すること
- □ 水道事業従事者の情報リテラシー向上を促し、操作やリスクに対する知識を高めること

(16) ウェブ

IP ネットワークにおける標準的な技術として広く利用されるウェブについてもシステムのライフサイクル全般において適切に対策を実施することが望ましい。なお、主な対策は、次のとおりである。

- □ 特殊文字、攻撃の糸口となる不要な情報を取り扱わないようにすること
- □ 要機密情報、要保護情報を取り扱う情報システムにおいては情報を特定し、ウェブサーバに保存しないように配慮すること
- □ ウェブサーバの正当性を保証するために電子証明書を利用すること
- □ ウェブからのダウンロードにおいては、電子署名による配布元の確認を行うこと
- □ 無用なリスクを回避するためには、当該の水道事業等以外のウェブサイトについて水道事業従事者が閲覧することのできるものを制限し、定期的に見直しを行うこと

(17) 通信回線共通対策

通信回線の利用に伴い、通信回線の不正利用や接続した装置への不正アクセス、送受信データの盗聴、改ざん、破壊等のリスクが存在する。なお、主な対策は、次のとおりである。

- □ 通信回線構築のリスクを検討し通信回線を構築すること
- □ 要安定情報を取り扱う場合は、サービスの可用性を確保するのに十分な通信性能を確保すること
- □ 通信回線について仕様書、設計書、回線の構成図等通信回線装置関連文書を整備すること
- □ アクセス制御等を効果的に実施するために、電子計算機を適切にグループ化し、通信回線上で分離すること
- □ 分離されたグループ間の通信については通信要件を検討しアクセス制御を行うこと
- □ 送受信される情報については暗号化の必要性を検討し、必要と判断される場合は暗号化すること
- □ 通信回線については物理的な安全対策を講ずること
- □ 通信回線装置の保守、診断等に遠隔地からの接続を行うサービスについて主体認証等のセキュリティ確保策を講ずること
- □ 通信回線装置は安全区域に設置し、ソフトウェアに対してはセキュリティホール対策を講ずること
- □ 通信回線に電気通信事業者の専用線サービスを活用する場合はサービスレベルについての契約を締結しておくこと
- □ 通信回線の利用にあたっては電子計算機の主体認証を実施すること
- □ 必要に応じて証跡管理を実施すること
- □ 要安定情報を取り扱うシステムについては必要に応じて冗長構成とすること
- □ 通信回線を利用する電子計算機の識別コード、利用者とその識別コード等を管理すること
- □ 前述の情報を変更した場合はその変更を記録し保存すること
- □ 情報セキュリティ責任者は定期的に通信回線の構成、装置の設定、アクセス制御設定等の変更を確認し、それにともなうセキュリティへの影響について対策を行うこと
- □ 承認されていない装置は通信回線に接続してはいけない
- □ 情報システムのセキュリティ確保が困難となった場合、他の情報システムと共用する通信回線から分離し、閉鎖的な通信回線に変更すること
- □ 通信装置のセキュリティホール対策、時刻同期等は電子計算機や端末と同様に実施すること
- □ 通信回線の運用終了に伴い、通信装置の内蔵記憶装置の情報を復元困難な状態にすること

(18) 庁舎内通信回線の管理

庁舎内であっても、通信回線の利用に伴い、通信回線の不正利用や接続した装置への不正アクセス、送受信データの盗聴、改ざん、破壊等のリスクが存在する。なお、主な対策は、次のとおりである。

- □ 通信回線への論理的接続の前に、電子計算機が接続の許可を得たものであることを主体認証等の仕組みにより確認する措置を講ずること
- □ 通信要件の変更、アクセス制御、セキュリティホール対策等は適時に見直しを行い、適切な対策を実施すること
- □ 情報セキュリティ責任者は要安定情報を取り扱う情報システムの通信回線利用状況を分析し、性能低下、異常について検知、対応すること
- □ 不正アクセス等の監視の目的から通信内容の監視を行うこと
- □ VPN、無線 LAN、リモートアクセスの環境を構築、提供する場合には、それぞれ利用の開始終了の申請手続き、暗号化、電子計算機の識別、主体認証とその管理、通信回線の範囲等を適切に検討、決定すること

(19) 庁舎外通信回線との接続

庁舎外通信回線との接続により、外部からの要因による情報セキュリティリスクが高まる。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、情報セキュリティ責任者の承認に基づいて庁舎内通信回線を庁舎外通信回線と接続すること
- □ 庁舎外通信回線に接続することによって情報セキュリティを確保できないと判断される場合は、庁舎内通信回線を庁舎外通信回線と独立したものとして構築すること
- □ 情報システムのセキュリティ確保が困難な状況が発生した場合、他の情報システムと共有している庁舎内通信回線、又は庁舎外通信回線から独立した通信回線に構成を変更すること
- □ 通信回線の変更に際し、及び定期的にアクセス制御設定の見直しを行うこと。
- □ セキュリティホール対策、通信回線の利用状況管理、通信内容の監視を適切に実施すること

(20) 制御系システムにおける対応

制御系システムは、一般の事務システムとは異なり、外部のネットワークとは遮断されている場合が多いことから、外部からのサイバー攻撃に対しては強靭であと考えられるが必ずしもそうではない。

また、制御系システムにおいては、古いバージョンの OS 等が利用されているケースがある一方、OS のアップデートや不具合対策のモジュール適用も容易でないことから、多層的な防御を実施していくことが必要である。主な対策は、次のとおりである。

① システム導入前の対策

制御系システムを導入する前の段階から、次のような対策を講じることが望ましい。

表 3-5:システム導入前の対策

#	対策	内容
1	セキュリティ要件の提示	制御系システムの導入(調達)に関する仕様書作成の段階で、セキュリティ対策の具体的な要件(ネットワークの分離、USB メモリ等の外部記憶媒体からの感染防止、脆弱性対策等)を提示
2		導入後の運用・保守契約においても、上記同様のセキュリティ対策の具体的な要件(脆弱性対策等)を提示
3	ハードウェア暗号モジュール	暗号処理や鍵管理デバイスについて、国際規格をクリアした(認証等を取得した)デバイスを利用

② システム導入後の対策

制御系システムを導入した後(運用)の段階では、下記のような対策を講じることが望ましい。

表 3-6:システム導入後の対策

#	対策	内容
1	外部からの感染阻止	USB メモリの接続の制限・禁止、運用・保守点検用の PC 接続時の安全性確認の実施
2	更新プログラム(パッチ)の適用	ベンダと協力し、適時セキュリティ更新プログラムを適用
3	OS のアップデート	OS が古いことで発生する「セキュリティホール(セキュリティ上の脆弱性、脆弱な箇所)」を狙うウィルス攻撃からシステムを防護するため OS をアップデート
4	監視体制の構築	セキュリティ事件・事故の検知や分析を行うため、制御システムのネットワークを流れるデータ、ログデータを監視する体制を構築

【参考となるガイドライン等】

- 「重大な経営課題となる制御システムのセキュリティリスク」第 3 版(平成 29 年 3 月独立行政法人情報処理推進機構)

(21) 外部委託における情報セキュリティ確保のための対策

重要情報の漏洩は、内部からのみならず、委託先からの場合も想定される。事業継続性の確保には、委託先と連携したセキュリティレベルの向上が必須であり、その上で水道事業者等による委託先の情報セキュリティ対策が必要である。

水道事業等においては、浄水場の維持管理等の業務委託や、情報システムの構築やメンテナンスの委託等の外部委託が実施されており、その際、委託業者が水道事業者等のシステムを利用することも考えられる。このような場合も考慮して、水道事業者等の情報セキュリティ基準を委託業者にも適用することが必要である。なお、主な対策は、次のとおりである。

- □ 情報セキュリティ責任者は、情報セキュリティ責任者の承認に基づいて庁舎内通信回線を庁舎外通信回線と接続すること
- □ 国際規格（JIS X5080 など）を踏まえた既存の取組等を参考に、情報セキュリティを確保する観点を含めて、外部委託可能な範囲の明確化や委託先の選定基準、委託先に求める情報セキュリティ対策項目や事業者としての管理方法を明示すること
- □ 通常監視業務、維持管理業務の他、PFI や施設全体の運転業務（小規模事業体）など全般にわたっての取り決めを行うこと
- □ システムの賃貸借や設計業務委託などにおいても、扱う情報に応じた対策を講ずること
- □ 上記のような取り決めや対策等においては、委託業者に水道事業者等と同じ又は同レベル以上の情報セキュリティ対策の実施を位置づけること
- □ 基本契約の締結や委託内容・取扱い情報の重要性に応じたとるべき情報漏えい防止対策等の強化対策事項の契約への盛り込み等、契約者双方の責任の明確化と合意形成を行うこと
- □ 万一、情報漏えい等の障害が発生したペナルティについても、合意形成を行っておくこと
- □ 情報システム障害発生時における委託先の措置や重要インフラ事業者等としての対処方法（委託先及び委託元との間の連絡体制や委託先と委託元一体となったトラブル対処方法等）を明示すること
- □ 障害発生の直接原因が委託先にあるとしても、市民からの信用を失墜する可能性があることに配慮し、不安感、不信感を招かないためにも十分な説明責任を果たすべきであることを認識すること
- □ 重要インフラとして可能な限り水道水の供給を停止させないための対策、行動基準を具体的に定めること

(22) IT に係る環境変化に伴う脅威への対策

社会環境や技術環境等の状況は刻々と変化しており、IT 障害を引き起こす新たな脅威が顕在化することがある。このような脅威として、電子計算機の性能の向上により暗号の解読が容易になる IPv4 アドレス枯渇に伴う「IPv6 への以降」、従来型の携帯電話と比較して情報セキュリティに対する意識が低い傾向にある「スマートデバイスの普及」や「SNS サービスの利用」、自身のコントロール下にない外部サーバを利用するため、インシデント発生時に必要な情報にアクセスできない場合のある「クラウドコンピューティング」等が考えられる。

このような情報システムの基盤を支える社会環境や技術環境等の変化について、IT 障害発生の未然防止のための適切な対策を検討すること。なお、主な対策は、次のとおりである。

- □ 平素から IT に係る社会環境や技術環境等の変化に留意するとともに、重要インフラ分野間（電力、ガス、情報通信等の他分野との間）のリスクコミュニケーション等により情報交換を行い、新たな情報の収集に努めること
- □ スマートフォンやタブレット PC 等の導入を検討する場合は、外出先での紛失や盗難による情報漏えいリスクを十分に認識し、情報セキュリティ対策にデバイス自体の管理方法や、デバイスに保存可能な情報・インストール可能なアプリケーションの範囲等を明確に盛り込むこと
- □ クラウドコンピューティングの利用を検討する場合は、クラウドサービスのデメリットやクラウド利用に伴う脅威をよく理解し、利用するサービスの限定化と、インシデント発生時の対策についても検討しておくこと

4. インシデント発生時の対応

4.1. 概要

インシデントが発生した際の対応計画（コンティンジェンシープラン）を事前に策定し、インシデントが発生した場合であっても、被害を軽減し、かつ水道水の供給を継続できることが必要である。ガイドラインにおけるコンティンジェンシープランとして、①被害の拡大抑制（インシデントハンドリング）、②重要サービスの継続（IT-BCP）の措置を講じる。

- □ インシデント発生を迅速にインシデント対応チームに報告する体制を構築する
- □ 対応すべきインシデントを判断する優先順位等を検討する
- □ インシデント発生を迅速に事業者外の関係者に連絡できる体制を構築する
- □ 情報システムが利用できなくなった場合の復旧策、代替策を検討する

4.2. インシデントハンドリング

インシデントハンドリングとして、次の 4 つの活動を行う。

表 4-1:インシデントハンドリングとして実施する活動

#	活動	概要
①	検知・連絡受付	インシデントの発生を検知し、必要な部署に連絡する
②	トリアージ	発生したインシデントに対して、対応の優先順位を付ける
③	インシデント・レスポンス	優先順位の高いインシデントに対して対処する
④	報告・情報公開	外部の関係者に対してインシデント発生を報告する

① 検知・連絡受付

定期的又は不定期に行なわれる保守作業、職員等のサービス対象者からインシデント発生の連絡を受ける。連絡窓口としてインシデント対応チームを構築するとともに、インシデントを検知した際は速やかにインシデント対応チームに報告するといった手順書と判断基準を事前に定め、職員に対して普段から周知・教育する。また、訓練を実施し、情報の伝達・転送がスムースに行われることを確認する。

保守作業の最中などに発見したり、あらかじめ用意したシステムによって異常が検知されたり

といった、基本的に自組織内で検知する方法で、定期的又は不定期に行われる保守作業において、侵入や改ざんの痕跡を調べるといったインシデントの検知に必要なチェック項目と、チェックの方法をあらかじめ明確にしておき、それらの手順を自動化した「異常検知システム」を導入する場合は、「何を持って異常とみなすのか」といった点を充分に整理して、誤検知を可能な限り最小限にまで抑制する。

② トリアージ

インシデント対応チームとして対応すべきインシデントを見定めるため、報告を受けたインシデントに対して、事実確認の上、インシデントとして該当するか否か、該当する場合は対応の優先順位を付ける。迅速かつ的確に優先順位を付けることができるよう、事前にトリアージのため、重要インフラサービス障害の深刻度や当該障害に関する情報の重要度を踏まえた判断基準を決めておく。

表 4-2:優先順位の判断基準

深刻度		定義
レベル4	危機	サービスの持続性又はサービスに関する安全性に、著しく深刻な影響が発生
レベル3	高	サービスの持続性又はサービスに関する安全性に、大きな影響が発生
レベル2	中	サービスの持続性又はサービスに関する安全性に、一定の影響が発生
レベル1	低	サービスの持続性又はサービスに関する安全性に、ほぼ影響なし
レベル0	なし	サービスの持続性又はサービスに関する安全性に、影響なし

インシデント対応チームが対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織のポリシーなどに照らして可能な範囲で詳細に報告者に回答するとともに、情報をやり取りした関係者に報告する。インシデント対応チームが対応すべきと判断した場合には、インシデントを「レスポンス(対処)」の対象とする。

③ インシデント・レスポンス

トリアージの結果、インシデント対応チームが対応すべきと判断したインシデントに対して、まず事象の分析を実施し、インシデント対応チームとして対処すべき事象か否かを再度検討するだけでなく、技術的な対処が可能か否かを判断する。

自組織での技術的な対応が困難な場合（例えば外注先でなければ対応ができないような問題など）は、主に経営層と連携し、対応計画を策定して実施する。その過程において、必要に応じて IT 関連部署との情報共有や連携を行う。

技術的対応の可否によらず、対応計画の策定や実施に際しては、必要に応じて外部の専門機関や当該インシデントに関係している可能性のあるサイト（関係者）に対して、対応の支援を依頼し、必要な情報の提供を要請する。

④　報告・情報公開

対応計画の策定及び実施と並行して、必要に応じて、メディアや一般に向けたプレスリリースや監督官庁（厚生労働省）への報告を実施する。

4.3. IT-BCP

インシデントが発生した際、インシデントハンドリングにより被害の拡大を防止するとともに、既に生じた被害に対して、早期の復旧（リカバリー）を行う必要がある。しかしながら、被害を受けた情報システムのリカバリーが完了するまでの間、つまり情報システムが利用できない期間においても、水道サービスを継続することが必要である。

上記を達成するため、事前に情報システムが利用できない期間においても水道サービスを継続するための計画として IT-BCP（Information Technology Business Continuity Plan: 事業継続計画）を定める。

(1) 非常時優先業務と情報システムの特定

IT-BCPの対象となる、情報システムが利用できない期間においても停止させることが認められない業務やサービスを非常時優先業務として特定し、その非常時優先業務に必要不可欠な情報システムを特定する。非常時優先業務の特定は情報セキュリティやサイバー攻撃に限った対策ではなく、地震や風水害などの自然災害、テロに対しても実施する必要がある。

なお、非常時優先業務の特定については、次を参照することが望ましい。

【参考となるイドライン等】
「大規模災害発生時における地方公共団体の業務継続の手引き」（平成 28 年 2 月内閣府）
「市町村のための業務継続計画作成ガイド」（平成 27 年 5 月内閣府）

(2) 目標復旧時間の算出

非常時優先業務を継続するために必要な情報システムに対して、情報システムを復旧させる目標復旧時間（RTO：Recovery Time Objective）を算出する。

(3) 対策の検討

目標復旧時間までに情報システムを復旧させる必要があるが、復旧までの間、情報システムは利用できない。そのため、情報システムが利用できない期間における対策を検討し、情報システムを利用せずとも最低限の非常時優先業務を継続する。

情報システムが利用できない期間における対策の一つが代替手段の活用である。代替手段の

活用とは、情報システムを利用せず別の手段を用いて非常時優先業務を継続させることである。代替手段としては手作業による非常時優先業務の継続、代替機（バックアップ機、予備機）による非常時優先業務の継続がある。

なお、IT-BCP に必要な対策については、次を参照することが望ましい。

【参考となるガイドライン等】
「IT-BCP 策定モデル」（平成 25 年 6 月内閣官房情報セキュリティセンター）

5. 関係機関との連携

5.1. 概要

情報セキュリティをより効果的・効率的に実施するため、厚生労働省や各種専門機関等の関係機関との連携を平時及びインシデント発生時の段階でそれぞれ実施する。

- □ 平時から最新の情報セキュリティに関する情報を入手できるよう、関係機関との情報交換を実施する
- □ インシデントが発生した際、関係機関に対して支援や助言を要請できるよう、関係機関との情報連絡のための窓口を用意する

5.2. 平時からの連携

系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されることもある。その結果、他社の2次被害を誘発し、加害者となる恐れもある。また、緊急時の原因特定などの際に、これらの企業からの協力を得られないことにより事業継続に支障が生ずる。

また、システム管理などの委託業務において、自組織で対応する部分と委託する部分の境界が不明確となり、対策漏れが生じる恐れがある。

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加して積極的な情報提供を行うとともに、経営層は自組織の CSIRT に情報入手を行わせる。また、入手した情報を有効活用するため、経営層は CSIRT に環境整備をさせる。情報共有活動への参加により、解析した攻撃手法などの情報を用いて、他社における同様の被害を未然に防止することができるが、情報共有ができていないと、社会全体において常に新たな攻撃として対応することとなり、企業における対応コストが低減しない。

情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要である。情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する。

- □ 独立行政法人情報処理推進機構（IPA）や一般社団法人 JPCERT コーディネーションセンター等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に活かす。
- □ CSIRT 間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集等を通じて、自組織のサイバーセキュリティ対策に活かす。
- □ IPA に対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいて、マルウェア情報や不正アクセス情報の届出をする。
- □ 一般社団法人JPCERTコーディネーションセンターにインシデントに関する情報提供を行い、必要に応じて調整を依頼する。
- □ サイバー情報共有イニシアチブ（J-CSIP）などの情報共有の仕組みを利用する。

表 5-1：関係機関の役割（平時）

#	関係機関	平時の役割
1	内閣官房（事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、NISCと相互に情報の共有を行う。
2	内閣官房（NISC）	重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
3	厚生労働省	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をNISC及び必要に応じ該当するセプターに連絡する。NISCから受領したシステムの不具合等に関する情報を該当するセプターに提供する。
4	セプターカウンシル	セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。
5	セプター事務局	重要インフラ所管省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。
6	水道事業者等	システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。

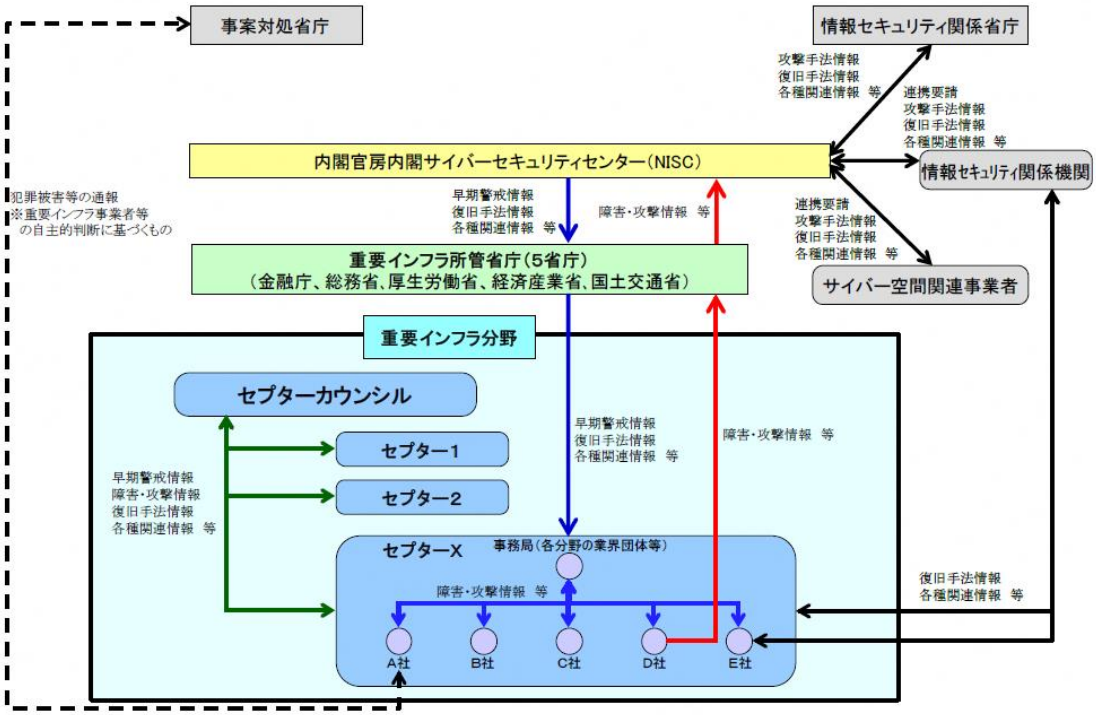

図 5-1:平時における情報共有体制

5.3. インシデント発生時における連携

「第 4 次行動計画」のとおり、水道事業者等は、関係機関（セプターカウンシル、セプター、重要インフラ所管省庁及び内閣官房等）と連携し、システムの不具合等に関する情報連絡、サイバー攻撃手法及び復旧手法に関する情報等の収集、情報セキュリティ関係機関との合意に基づく補完的な情報共有を行う。

オリンピックやサミットなど自組織の所在する地域外において大きなイベントが開催される場合は、サイバー攻撃に対する備えが特に必要となるため、関係機関と連携し普段よりも高い警戒体制を構築し、インシデント発生又はその予兆を確認した場合は速やかに関係機関に共有する。

表 5-2：関係機関の役割（インシデント発生時）

#	関係機関	インシデント発生時の役割
1	内閣官房（事態対処・危機管理担当）	平時の役割に加え、NISCと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、NISCと相互に情報の共有を行う。
2	内閣官房（NISC）	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、情報セキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
3	厚生労働省	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。
4	セプターカウンシル	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。
5	セプター事務局	平時の役割に加え、必要に応じて大規模重要インフラ サービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。
6	水道事業者等	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。

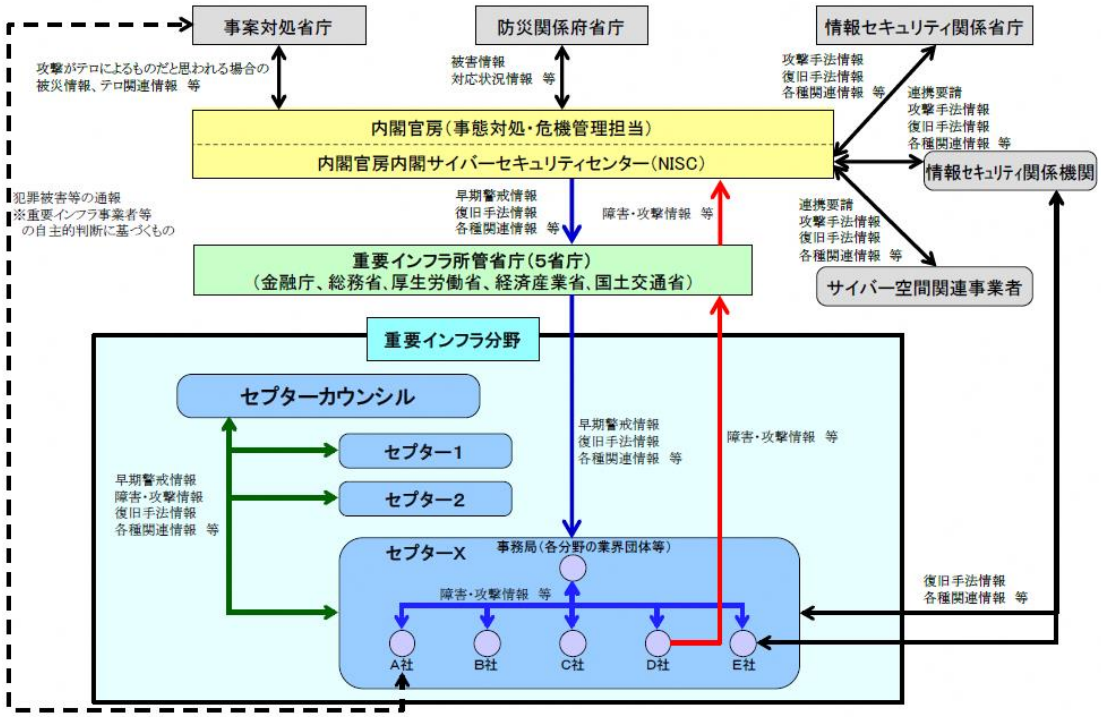

図 5-2:インシデント発生時における情報共有体制

6. 訓練の実施

6.1. 概要

構築した体制や策定した計画について、職員に周知・共有するとともに、訓練を通じてインシデント発生時における職員の対応力を向上させる。

- □ 自組織の練度に応じて、研修会やワークショップ等を活用し、職員に対する情報セキュリティに関する知識や自組織の情報セキュリティに関する体制や計画を共有する
- □ 職員に対する教育や周知ができた段階から、インシデント発生時における職員の対応力をさらに向上させるため訓練を実施する

6.2. 訓練の実施

情報セキュリティやサイバー攻撃に対して万全の対策を講じ、如何なるインシデントの発生を防止することは極めて困難である。そのため、インシデントが発生しないことを想定するのではなく、発生を前提として、発生時にどの様な対応（応急対策）が必要であるかを検討し、対策を講じるとともに、職員の対応力向上が必要不可欠である。

また、事前対策及び事後対応として講じることとした措置を実際に運用するためにも、職員への教育が必要である。さらに教育・訓練を通じて、策定した各種計画やガイドラインの課題を洗い出し、改善を実施することで、より実行性の高いマニュアルに改訂していくことが重要である。

職員に対して訓練を実施する際、情報セキュリティやサイバー攻撃に対する十分な知識や情報が無ければ訓練を実施したとは言えないことから、訓練を実施する前に知識や情報を共有する機会として、教育のための研修会やワークショップを開催することが望ましい。

職員に対する教育・訓練を実施する流れとして、次のステップを取ることが望ましい。これらのステップを踏むことで、職員として情報セキュリティやサイバー攻撃に対する知識や情報を得ることができるとともに、情報セキュリティやサイバー攻撃に対する意識が醸成される。

表 6-1：訓練の流れ

STEP	イベント	目的	方法（一例）
STEP 1	研修会	水道事業者等の職員として身に着けておくべき情報セキュリティに関する知識、インシデント対応時の役割や組織を認識	外部専門家等が講師として講演を実施
STEP 2	ワークショップ	リスクアセスメントを自ら実施し、水道サービスに係る情報システムの脆弱性を認識	ワークショップ形式でリスクアセスメントを実施
STEP 3	訓練	インシデント発生時の職員の対応力向上、策定した各種のインシデント対応計画の実行性を検証	訓練シナリオを作成し、インシデント対応を図上訓練、情報システムを活用した実地訓練を実施

7. 監査の実施

7.1. 概要

実施した各種の情報セキュリティ対策が実際に機能しているかについて検証を行うため、監査を実施する。

- □ 自組織内部にて監査人を選出し、組織内における情報セキュリティ対策の実施状況、ルールの運用状況を確認(監査)する
- □ 外部の専門機関の協力のもと、各種テストを実施し、自組織の情報セキュリティに関する脆弱性の有無を確認する

7.2. 監査の実施

監査には、次のとおり、内部監査と第三者による外部監査の 2 つの方法がある。

(1) 内部監査

教育を受けた内部監査人を自組織内から選任し、組織内における情報セキュリティ対策の実施状況、ルールの運用状況の確認を実施する。

表 7-1:内部監査の一例[1]

#	監査	対象	内容
1	質問(ヒアリング)	職員	マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、関係者に対して口頭で問い合わせ、説明や回答を求める監査技法
2	閲覧(レビュー)	文書(規定類や台帳)、機器	マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、規定、手順書、記録(電磁的な記録も含む) 等を調べ読む監査技法
3	観察	機器	マネジメント体制又はコントロールについての整備状況又は運用状況を評価するために、監査人自らが現場に赴き、目視によって確かめる監査技法
4	再実施	機器	コントロールの運用状況を評価するために、監査人自らが組織体のコントロールを運用し、コントロールの妥当性や適否を確かめる監査技法

[1]「脆弱性検査と脆弱性対策に関するレポート―組織で提供するソフトウェアの検査と組織内のシステムの点検のための脆弱性検査を―(平成 25 年 8 月独立行政法人情報処理推進機構)」

(2) 外部監査

第三者による外部監査として、次のような方法がある。

表 7-2:外部監査の一例[2]

#	監査	内容
1	システムセキュリティ検査	サーバやネットワークシステムの運用開始以降に発見される既知の脆弱性の有無、運用に対してセキュリティ上好ましくない設定等の有無を点検
2	ペネトレーションテスト	サーバやネットワークシステムに対して、攻撃者が侵入できるかどうか、進入された場合どの様なことが発生する可能性があるかを検査

【参考となるガイドライン等】
「情報セキュリティ監査手続ガイドライン」(平成 21 年 7 月経済産業省)

[2]「脆弱性検査と脆弱性対策に関するレポート―組織で提供するソフトウェアの検査と組織内のシステムの点検のための脆弱性検査を―」(平成 25 年 8 月独立行政法人情報処理推進機構)