別添

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

厚 生 労 働 省

健康局水道課

序　文

近年のわが国の IT 化の進展は目覚しく、地方公共団体や民間企業において業務の効率化などのために IT がさまざまな分野で利用されている。

水道事業においても他の分野と同様に IT の利用が積極的に図られているが、一方で情報システム障害によって安全な水の安定供給に支障をきたすことがないよう、適切なセキュリティ対策を実施することが求められている。

このようなことから、内閣官房に設置されている情報セキュリティ基本問題委員会では、従来の重要インフラ分野を情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービスとしていたが、平成 17 年 4 月 22 日の第 2 次提言において、医療、水道、物流を追加すべきとした。これを受けて、情報セキュリティ政策会議が平成 17 年 12 月 13 日に策定した「重要インフラの情報セキュリティ対策に係る行動計画」（その後、平成 21 年 2 月 3 日に「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」に改訂。）において、各重要インフラ分野において望ましい情報セキュリティ対策の水準を「安全基準等」として明示するよう努力することとされた。また、平成 24 年 4 月 26 日の同行動計画（改定版）においては、①東日本大震災発生時における複数の IT システムの同時的な障害発生及びその際の事業継続計画（BCP）の実施、②政府関係機関や重要インフラ事業者等への IT システム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化について、早期に取組を強化・補強すべき点についても反映が行われた。

このような中で、情報セキュリティ政策会議は、各重要インフラ分野における「安全基準等」の策定・改定を支援するために「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」（以下「指針」という。）及び同対策編（以下「対策編」という。）を策定している。指針では、それぞれの事業分野においてその特性に応じた必要または望ましい情報セキュリティ対策の水準を「安全基準等」という形で明示し、個々の事業者が重要インフラの担い手として自主的に取り組むことにより、その「安全基準等」を満たすべく努力し、また満たしているかを自ら検証することが必要とされている。

厚生労働省では、水道事業者が情報セキュリティ対策を行うため、平成 18 年 10 月 31 日に「水道分野における情報セキュリティガイドライン」（以下「ガイドライン」という。）を策定（平成 20 年 3 月 27 日改定）しており、水道分野における「安全基準等」として位置づけているものである。

今般、平成 25 年 2 月 22 日に「指針」が改定され、平成 25 年 3 月 26 日に「対策編」が改定されたことを受け、「指針」及び「対策編」に基づいて、ガイドラインの改定を行った。

なお、「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」においては、対象とする水道の重要システムや、サービスの検証レベルについて以下のように定めている（別紙 1「対象となる重要インフラと重要システム」、別紙 2「重要インフラサービスと検証レベル」）。

IT 障害やその影響の例

・水道による水の供給の停止

・不適当な水質の水の供給　等

対象となる重要システム例

・水道施設や水道水の監視システム

・水道施設の制御システム　等

検証レベル

・IT の機能不全により、断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと

また、「指針」においてはガイドラインを策定するにあたって以下に留意することが示されている。

本ガイドラインは、これらを踏まえ策定したものである。

① 4 つの柱

ア 組織・体制及び資源の確保

イ 情報についての対策（情報の格付け、ライフサイクルに着目した取扱い）

ウ 情報セキュリティ要件の明確化に基づく対策

エ 情報システムについての対策

② 5 つの重点項目

ア IT 障害の観点から見た事業継続性確保のための対策

イ 情報漏えい防止のための対策

ウ 外部委託における情報セキュリティ確保のための対策

エ IT 障害発生時の利用者の対応のための情報の提供等の対策

オ IT に係る環境変化に伴う脅威のための対策

（参考）情報セキュリティに係るこれまでの経緯

	内閣官房情報セキュリティセンター（NISC）			厚生労働省健康局水道課
	行動計画	指針	指針　対策編	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）

目　次

1. 総則

1.1. 目的

本ガイドラインは、水道事業者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な考えられる措置を示すことに加えて、水道事業者の情報セキュリティに対する現状認識や今後必要となる対策のレベルへの理解を深めることを意図している。

水道事業が国民生活において重要なインフラであることは誰もが認めるところである。また効率的、かつ合理的な水道の構築に向けて、尚一層、IT の活用が必要不可欠となる状況であることは時代の趨勢とも言える。

このことは水道においても他の重要インフラと同様に多くの情報セキュリティリスクに曝されていることを意味する。

一方で 2001 年 9 月 11 日に現実にテロの脅威に直面した米国では、テロ組織が瞬時に壊滅的混乱や打撃を与えることのできる標的として重要インフラの情報システムに着目しているとの認識のもと、電力業界をはじめとする各重要インフラ業界や国家をあげて情報セキュリティ対策に取り組んでいる。発生原因の一部に情報システムの不具合も含まれるとされる 2003 年 8 月 14 日の北米大停電の影響の大きさを考えれば、原因がテロ事件ならずとも情報セキュリティ対策の重要性が伺える。

このような状況を調査し、とりまとめた「電力重要インフラ防護演習に関する調査報告書」（2004 年 8 月：独立行政法人情報処理推進機構）では、以下のような事例が報告されており、現在のわが国を取り巻く情勢においても無視できない内容であると考えられる。

- サイバーテロ演習において、特別チームがコンピュータに侵入して重要インフラの制圧に失敗したことは一度も無い。
- 共通の標準技術への移行による脆弱性情報は攻撃側にも入手しやすい。
- ニーズが先行してセキュリティ対策が後手に回っている。
- 2000 年春、製造ソフトウェアを開発した豪企業の元従業員が地方公務員職を断られた際、無線送信機を使って同地域の汚水処理施設の制御システムに侵入し、264,000 ガロンもの未処理下水を近くの河川や公園に放流した。
- 一部の米政府機関や諜報機関は、アルカイダのメンバーが給水及び浄水施設を管理する制御システムの情報を、多くの Web サイトから入手していた形跡があると発表している。
- カナダの Canadian Office of Critical Infrastructure Protection and Emergency

Preparedness（OCIPEP）による 2001 年 11 月の報告では、「米国の法執行機関及び諜報機関は、アルカイダのメンバーが SCADA の情報を探しているという兆候を発見した」ものの、主に水道（衛生）システムに関するものだったという。

・サイバーと物理的な攻撃を同時、あるいは連続的に行う「swarming attack」の可能性が、被害側の対応の遅延や混乱を一層誘発するものとして、重要インフラにとって新たな脅威となっている。

・強力な電磁パルスを発生させる E 爆弾により、瞬時に日本や北米全域などの広範囲のあらゆる情報システムを停止に追い込むことが可能と考えられる。

（参考文献）「電力重要インフラ防護演習に関する調査報告書」（2004 年 8 月：独立行政法人情報処理推進機構）

実際に上下水道の事例が記載されていることや、E 爆弾のように特定の重要インフラではなく広範囲に無差別に攻撃する脅威などは、わが国の水道においても情報セキュリティリスクを軽視できないものと再認識するものである。

いくつかの事例は組織の内部外部を問わず、あらゆる側面で情報セキュリティリスクに曝されていることを示し、また無差別な防ぎようの無い情報セキュリティリスクに対しては、障害発生後の事業継続性確保が重要であることなどを示唆している。

このような状況に対応すべく本ガイドラインを策定するに至ったが、この実施内容に沿って各水道事業者が全ての安全対策を一度に実現することは現実的には財政的理由やセキュリティ人材の不足の課題から困難であると考えられる。

したがって、まずは本ガイドラインや文中に記載した参照すべき資料に目を通し、情報セキュリティ対策の重要性への理解を深めるとともに、各水道事業者の状況に応じて、対策の効果、及び実施可能性を勘案して、優先すべき対策から実施することが重要である。

「セキュア・ジャパン 2009」（2009 年 6 月 22 日：情報セキュリティ政策会議）や「情報システムの信頼性向上に関するガイドライン第 2 版」（平成 21 年 3 月 24 日：経済産業省）では、セキュリティ人材の育成、セキュリティ対策の実効性の担保、横断的な情報セキュリティ基盤の形成などが謳われ、情報セキュリティ環境の変化に応じて見直すことが必要とされている。

本ガイドラインについても今後の状況の変化に応じ、適宜見直していくこととしており、各水道事業者においてもこれを参考にしつつ、継続的な情報セキュリティ対策の充実が求められる。

1.2. 保護対象

水道事業者が利用する以下のような情報システムを対象とする（以下、「水道情報システム」という）。

なお、既往の実施内容（例えば、他企業、他業界の基準、地方公共団体の基準）で統一的に扱われる情報システム等については、該当する他の基準、ガイドラインを参照する必要がある。

表 1　水道情報システム～保護対象とする情報システムの例～

区分	システム名称	概　　要
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。
	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。
	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。
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。
	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。
	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。
	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。
	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。
	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。
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もに一元的に管理するシステム。
	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。
	資産管理システム	水道事業者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。
	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。
	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。

上記個々の情報システムの資産についてはさらに以下の区分ができる。

表 2　情報システムの資産区分と内容

資産区分	内容
データ資産	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
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
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
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

【参考】 個人情報の保護対策について

個人情報の保護対策に関しては、経済産業省が特徴的な取組を行っている事業者（水道、電気、ガスを含む）を対象にヒアリング調査を行い、効果的・効率的な取組の具体例を取りまとめた、「平成 20 年度『個人情報の適正な保護に関する取組実践事例調査』報告書」に事業者別の事例が多数掲載されている。

水道事業者においては、給水台帳の管理システムや検針・水道料金システム等で個人情報を管理している場合があり、これら情報については適切な保護対策が求められる。水道事業者は、本報告書の取組実践例等を参照のうえ、事業者の規模、業務形態、業務内容等に合致した効果的かつ効率的な取組を積極的に導入し、個人情報保護の水準を高めていくことが重要である。

本報告書は、本章「Ⅰ．本報告書の構成と見方」、「Ⅱ．個人情報保護対策の場面ごとの取組事例」と「Ⅲ．中小企業における効果的な取組」」、「Ⅳ．個人情報保護対策に関するコストの事例」、「Ⅴ．事業者ごとの個人情報保護対策取組事例」の 5 つの章に分かれている。

以下、それぞれの章の主な内容について紹介する。

(1)　「Ⅱ．個人情報保護対策の場面ごとの取組事例」について

第Ⅱ章では、個人情報保護対策を考えていく上でいくつかの重要な場面を挙げ、その場面ごとに、今回の調査対象となった事業者が実施している取組を整理している。なお、それぞれの場面ごとの事例は、「平成 18 年度事例→平成 19 年度事例」の順番で整理している。

表　個人情報保護の場面・項目

場面・項目	説明
1.　個人情報保護対策の準備 （規定づくり・体制づくり）	個人情報保護対策を行う上での前提となる社内体制の整備や、規程づくり・改訂の方策に関する取組
2.　個人情報の取得	個人情報取得の際の本人（情報主体）に対する同意のとり方、利用目的の伝え方や配慮などに関する取組
3.　個人情報の利用	個人情報を適切に利用する方法、利用する上での配慮などに関する取組
4.　個人情報の適切な管理	
(1)　個人情報の管理システム （物理的・技術的措置を中心に）	情報システムの構築・運用に関する取組など、物理的措置・技術的措置に関する取組
(2)　従業員等への教育方法	従業者、派遣職員等に法や社内規程等を周知し、意識を高めさせるための取組
(3)　個人情報の盗難対策	個人情報の含まれる情報媒体が盗難に遭わないようにする工夫。車上荒らし対策などの取組
(4)　ノート PC の安全対策	ノート PC の盗難対策、暗号化やパスワードによる保護など適切な管理のための取組
(5)　外部委託先の監督方法	外部委託先の選択の際の配慮、及び業務遂行中の適切な管理方策、評価等を行うための取組
(6)　規定の遵守状況等の日常的点検・確認の方法	規程などの遵守状況について、日常業務の中で適切に点検・確認を行う上での取組
(7)　初歩的ミスの防止策 （FAX、メールの誤送信など）	FAX やメールの誤送信等の初歩的なミスの防止のための取組
5.　個人情報の消去・破棄	個人情報を消去・廃棄する上で導入している機器や対策に関する取組
6.　個人情報の点検・監査	規程等の遵守状況や管理状況等を確認するために実施される監査に関する取組
7.　個人情報に関する苦情処理・開示請求対応	個人情報に関する本人からの問い合わせや苦情、開示請求に対応に関する取組
8.　個人情報に関する事故（漏えい・き損等）発生	漏えい・き損等の事故発生時に迅速且つ適切に対応するための方策や、顧客対応などに関する取組
9.　その他	上記 1～8 には分類されない取組

(2)　「Ⅲ．中小企業における効果的な取組」について

第□章では、中・小規模の企業の取組を中心に、設備投資や人的負担を抑える工夫をしながら効果的な個人情報保護対策をとっている事例のみを取り上げて再整理している。

(3)　「Ⅳ．個人情報保護対策に関するコストの事例」について

第□章では、個人情報保護対策に要するコストの観点から整理している。個人情報保護対策のコストについて、個人情報保護対策として金銭的・人的投資を行っ

ている取組を 15 の視点から取り上げ、それぞれの取組を実施している場合にどの程度の金銭的・人的コストをかけているのかという概算を整理している。

(4) 「Ⅴ．事業者ごとの個人情報保護対策取組事例」について

第□章では、調査対象事業者ごとに個人情報保護の取組を整理している。

個人情報保護の取組については、個別の取組が独立して存在しているのではなく、いくつかの取組が合わさることで効果を発揮することを狙っている場合も少なくない。事業者の個人情報保有数や規模、取組経緯などによって対策の内容は異なってくるし、どのような部分に力を入れて対策を行っているのか、ということも事業者によって異なる。本章では、積極的な取組を行っている事業者の個人情報保護に関する取組の全体像を掴んでもらうことを目的としている。

（参考文献）「平成 20 年度『個人情報の適正な保護に関する取組実践事例調査』報告書」(2009 年 3 月：経済産業省商務情報政策局、http://www.meti.go.jp/policy/it_policy/privacy/061215kozinzyouhou.htm)

1.3. システムの重要度

情報システムの重要度は一般に以下の 3 つの項目をもとに検討される。

機密性 : アクセスを許可された者だけが情報にアクセスできることを確実にすること

完全性 : 情報及び処理方法が正確であること及び完全であることを保護すること

可用性 : 許可された利用者が必要なときに、情報及び関連する資産にアクセスできることを確実にすること／水道サービスの提供のために水道情報システムの稼動を確実にすること

ここではこれらについて 4 つの重要度を設定し、その重要度を要求水準とすると以下のような分類が考えられる。

表 3　重要度／要求水準の分類 (1)

重要度 要求水準	機密性	完全性	可用性
非常に高 (A)	・ 特定の関係者のみ開示可能なもの ・ 漏洩した場合業務への影響が非常に大きい	・ 情報及び処理は常に正確、完全であるべきもの ・ 不完全な場合、業務への影響が非常に大きい	・ 情報及び処理が常に継続できること ・ 継続できないと、業務への影響が非常に大きいもの
高 (B)	・ 特定の部署のみ開示可能なもの ・ 漏洩した場合業務への影響が大きい	・ 情報及び処理にできるだけ完全性が求められるもの ・ 不完全な場合、業務へ	・ 情報及び処理をできるだけ継続できること ・ 継続できないと、業務

		の影響が大きい	への影響が大きいもの
中 （C）	・ 内部では開示・提供可能なもの ・ 漏洩した場合業務への影響は小さい	・ 情報及び処理がある程度完全であるべきもの ・ 不完全な場合、業務への影響は小さい	・ 情報及び処理がある程度継続できること ・ 継続できない場合、業務への影響は小さい
低 （D）	・ 各種媒体で既に公開している情報 ・ 漏洩しても業務への影響がほとんどない	・ 情報及び処理が完全でなくてもよいもの ・ 不完全でも、業務への影響がほとんどない	・ 情報及び処理に継続性を求めなくてもよいもの ・ 継続できなくても業務への影響がほとんどないもの

上記表の分類基準は、一般的（抽象的）な表現であるため、より具体的な表現で整理すると以下のようになる。

表 4　重要度／要求水準の分類 (2)

重要度 要求水準	機密性	完全性	可用性
非常に高 （A）	・水道使用者の個人情報 ・職員の個人情報	・水道使用者の個人情報 ・職員の個人情報 ・水道料金に関する情報 ・経理に関する情報 ・水質／水量への影響が大きい監視制御システム	・水の供給全体に大きく影響するシステム ・リアルタイム処理しているシステム
高 （B）	・設計書など発注に関する情報	・システム仕様やネットワークに関する情報 ・水道施設に関する情報	・外部とのデータ交換など行っているシステム ・他のシステムと連携しているシステム ・利用頻度の多いシステム
中 （C）	・その他業務で利用している情報	・その他業務で利用している情報	・その他業務で利用しているシステム
低 （D）	・各種媒体で既に公開している情報	・情報及び処理が完全でなくてもよいもの	・情報及び処理に継続性を求めなくてもよいもの

水道事業者が業務で利用する水道情報システムには、個々の情報システム特性により重要度の評価は異なると考えられる。水道事業を重要インフラの観点から捉えた場合、給水サービス（水の供給）を停止させないことが最も重要であることを前提に評価しなければならない。ここでは参考までに水道情報システムについて、個人情報の有無やそのシステムの一般的な目的（役割）と停止したときの影響の大きさなどをもとに各評価項目及びシステムとしての総合的な重要度を検討した例を以下に示す。その際、各情報システムの給水サービスへの影響度の直接性（大・小）を評価に加えた例とした。

このような評価を各水道事業者がそれぞれの状況に応じて実施することが求められ

る。

表 5　水道情報システムの重要度／要求水準の例

システム区分	給水への影響	個人情報	機密性	完全性	可用性	重要度
制御系システム						
浄水場の監視制御システム	大		B	A	A	A
ポンプ場の運転システム	大		B	A	A	A
水運用システム	大		B	A	A	A
技術系システム						
管路情報システム	小		B	B	B	B
電子ファイリングシステム	小		B	B	B	B
給水台帳システム	小	有	A	A	B	B
設備管理システム	小		B	B	B	B
設計積算システム	－		B	B	C	B
管網解析システム	小		C	C	C	C
事務系システム						
検針／水道料金システム	－	有	A	A	B	B
財務会計システム	－		A	A	B	B
資産管理システム	－		B	B	C	C
人事管理システム	－	有	A	A	C	B
文書管理システム	－		C	C	C	D

1.4. 想定される脅威と脆弱性

「指針」をもとに以下の脅威を対象と捉える。

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、ウィルス攻撃、サービス不能攻撃（DoS）、情報漏えい、重要情報の搾取、内部不正　等

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

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、コンピュータ施設の損壊、大規模・広範囲にわたる疾病による要

員不足に伴うコンピュータ施設の運用に係る機能保全　等

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

水道事業者が利用している環境により水道システムに対する脅威、脆弱性は異なるが、一般的に想定される脅威、脆弱性を列挙すると以下のような項目が考えられる。

表 6　脅威／脆弱性

分　類		内　容
意図的脅威	遠隔的（ネットワーク経由）	不要データ送信（過負荷）
		データ流出、改ざん
		システム操作（プログラム改ざん）
		ウィルス、SPAMメール
	直接的	ハードウェア破壊
		盗難（コンピュータ、記録データ、文書）
		直接操作によるデータコピー（漏洩）、改ざん
		重要情報の搾取
		内部不正
非意図的脅威、脆弱性	ソフトウェア	プログラムミス（バグ）
		他システムとの連携不良（Version不整合）
		OS変更による動作不良（Version不整合）
		設計・開発の不備
	ハードウェア	システム機器の故障、劣化
		電力業者の障害／停電
		ガス業者の障害／供給途絶
		通信業者での障害／通信途絶
		空調機器故障
		各種リソース（回線、ディスクなど）容量の不足
		通信、処理過負荷
		メンテナンス不備
	利用者（個人）	各種操作ミス
		電源、通信ケーブル引き抜き
		失火
		水もの接触
		未許可ソフト、データのインストール使用
		データの外部持ち出し、置き忘れ
		パスワード掲示（記録）
		パスワード忘れ
	管理者（組織）	開発、データ処理等の委託先管理不十分
		内部・外部監査機能の不備
		セキュリティ対策の未実施
		マネジメントの欠陥
環境的脅威		地震
		停電
		落雷
		火災
		上記以外による停電
		大規模・広範囲にわたる疾病

1.5. ガイドライン活用における判断基準

以降に述べる実施内容の全てについて、原則的に以下の判断基準を適用するものとする。

① ガイドラインに示される個々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。

② 実施すべき対策については、各水道事業の規模（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。

③ 特に小規模の水道事業者においては、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なども含めてセキュリティ確保に努めることで、水道事業者独自でのセキュリティ対策組織などは簡素化できるものと考えられる。

④ なお、本書に記載する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。

⑤ 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などを行っている場合、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。

⑥ 浄水場の維持管理などの業務委託や、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においては、受託者に水道事業者（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. 組織・体制及び資源の対策

2.1. 組織・体制及び人的資源の確保

【趣旨】

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運用、評価、見直しする組織体制の確立が必要である。

重要インフラにおける情報セキュリティ対策は、水道情報システムを直接利用する者だけではなく、関連する職員に与えられる職務、権限に応じて、組織的に取り組むことが必要である。

ただし、小規模な水道事業などにおいては、その人員体制、財政状況に応じて情報セキュリティを損ねない範囲で適切に簡素化、あるいは帰属する市町村と統合的に対策され得るものとする。

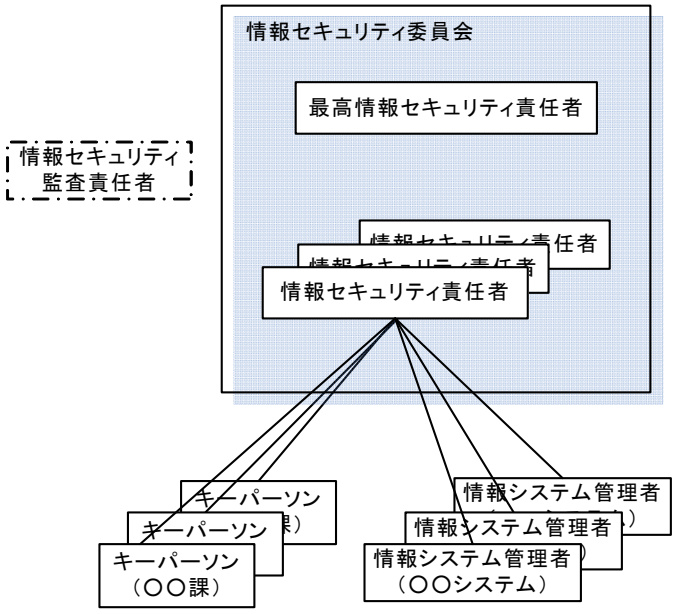

図 1　情報セキュリティの組織

また、IT 障害に関する情報を重要インフラ分野内で共有することで重要インフラ事業者の対応能力の向上を促すため、各重要インフラ分野において、「情報共有・分析機能（セプター※）」を整備することとされている。水道分野では、平成 20 年 3 月に（社）日本水道協会に水道セプターが設置された。このため、水道事

業者は厚生労働省のみでなく、水道セプターとも連携を図っていくことが必要である。

※セプター（CEPTOAR）：**C**apability for **E**ngineering of **P**rotection, **T**echnical **O**peration, **A**nalysis and **R**esponse。政府からの情報窓口及び事業者への周知、関係機関（他分野のCEPTOAR 等）との情報共有、重要インフラ連絡協議会への参加等の役割を担うこととされている。

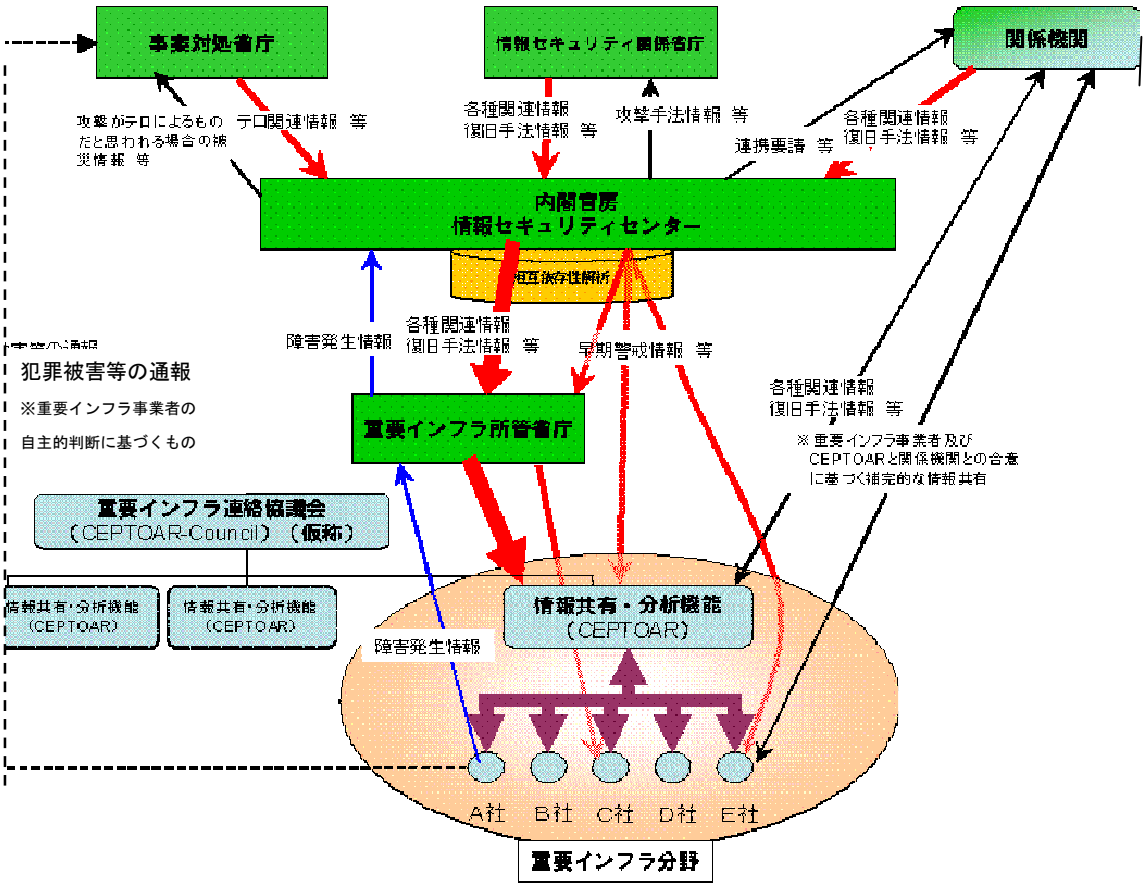

図 2　関係機関における情報共有体制（イメージ）

（内閣官房情報セキュリティセンター作成資料を一部改）

2.1.1. 最高情報セキュリティ責任者

【実施内容】

(1)　水道事業者の情報セキュリティについて、組織的な取り組みの推進とその責任を明確にすること。

(2)　水道事業者のトップ（幹部クラス）が水道情報システムの最高セキュリティ責任者になること。

2.1.2. 情報セキュリティ委員会

【実施内容】

(1) 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、本ガイドラインを参考に水道事業者独自の対策基準（内規）を作成すること。

(2) 実施状況の確認、問題点の改善などについて検討すること

(3) 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など、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こと。

2.1.3. 情報セキュリティ責任者

【実施内容】

(1) 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こと。

(2) 課長（係長）クラスの職員が想定される。

2.1.4. キーパーソン

【実施内容】

(1) 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。

(2) 他の職員の対策について具体的な支援を行うこと。

(3) 厚生労働省等の事業認可者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。

2.1.5. システム管理者

【実施内容】

(1) 個々の水道情報システムごとのセキュリティ対策を実施すること。

(2) キーパーソンが兼務することも考えられる。

2.1.6. 情報セキュリティ監査責任者

【実施内容】

(1) 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こと

(2) 情報セキュリティ委員会にオブザーバとして出席して助言すること。

(3) 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い。

(4) 実行を担保するために、水道事業者外部の者に依頼する（委託含む）こと

も考えられる。

2.2. 情報セキュリティ人材の育成等

2.2.1. 研修及び人材の育成

【趣旨】

情報セキュリティ対策を策定した後に、水道事業従事者にその内容を周知徹底することが重要である。

また、継続的に情報セキュリティ人材の育成を行うとともに、要員の管理を行うことが望ましい。

【実施内容】

(1) 情報セキュリティ対策に関する研修などを通じて対策について理解を深め、実行できるようにすること。

(2) 情報セキュリティ委員会において、周知徹底を図るための資料などを作成・配布すること。

(3) 年 1 回以上のセキュリティ研修（外部研修含む）を実施し、情報セキュリティ人材の育成に努めることが望ましい。

2.2.2. 重大障害時の対応

【趣旨】

情報セキュリティ委員会では、情報システム障害により水の供給に影響を及ぼすような重大な障害が発生したときに備えておく必要がある。

【実施内容】

(1) 事前に復旧手順、連絡先などについて整備し、年 1 回以上訓練しておくこと。

(2) 情報交換が必要な関係団体との窓口（連絡方法、担当者など）を定めこれを関係団体に連絡すること。

(3) 実際に重大障害が発生した場合には、その障害対応を指揮することと同時に、行政部局の情報セキュリティ担当部署及び外部の関係団体、並びに別に定めるとおり厚生労働省等の事業認可者へ迅速に報告すること。なお、厚生労働省において重大障害が発生した旨の報告を受けた場合は、その内容を水道セプターに情報提供を行うこととしていることに留意すること。

(4) 障害の記録を作成して原因の調査と再発防止に努めること。

(5) 重大障害等とは、監視制御系システムの「機密性」、「完全性」、「可用性」が侵害され水の供給に影響を及ぼすものをいい、これらに影響を及ぼさない

軽微な故障などは対象としない。

(6) 東日本大震災で生じた複合的な障害の教訓を踏まえ、事業継続の障害となる情報セキュリティ上のリスクを十分想定すること。

2.3. 外部監査等による情報セキュリティ対策の評価

2.3.1. 自己点検

【趣旨】

情報セキュリティ対策の実効性を担保するために点検を実施する。

【実施内容】

(1) 情報セキュリティ委員会は水道情報システムの年度点検計画を作成し、点検票、実施手順書を作成すること。

(2) キーパーソンを通じて、点検票、手順書に基づいて利用者(職員)に情報セキュリティ対策の実施状況について自己点検を指示すること。

(3) 点検の結果、対策について不備が発見された場合には、キーパーソンはその記録を情報セキュリティ委員会に提出すること。

(4) 情報セキュリティ委員会（委員長）は報告に基づいて情報セキュリティ責任者に改善を指示すること。

2.3.2. 監査

【趣旨】

情報セキュリティ対策の妥当性を検証するために監査を実施する。

【実施内容】

(1) セキュリティ監査責任者は、年度監査計画を作成し最高情報セキュリティ責任者の承認を得ること。

(2) 監査の実施にあたっては、被監査部門から独立した者に監査を依頼すること。

(3) 必要に応じて外部監査を実施することが望ましい。

(4) 監査結果について最高情報セキュリティ責任者に報告すること。

(5) 最高情報セキュリティ責任者は監査報告に基づいて、必要な是正措置を情報セキュリティ責任者に指示をすること。

3. 情報セキュリティ対策

3.1. 情報についての対策

3.1.1. 情報の格付け

【趣旨】

水道事業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。

【実施内容】

(1) 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。

(2) 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。

3.1.2. 情報の取り扱い

3.1.2.1. 情報の作成と入手

【趣旨】

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。

【実施内容】

1） 業務以外の情報の作成、または入手の禁止

(1) 水道事業従事者が水道事業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。

2） 情報の作成、または入手における格付けと取扱制限

(1) 水道事業従事者が情報の作成時、また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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

3.1.2.2. 情報の利用

【趣旨】

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。

【実施内容】

1) 業務以外の情報利用の禁止

(1) 水道事業従事者が水道事業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。

2) 格付けと取扱制限に沿った利用

(1) 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。

3) 要保護情報の利用

(1) 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。

(2) また、必要以上に複製、配布してはならない。

(3) 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。

3.1.2.3. 情報の保存

【趣旨】

水道事業を遂行する上で、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。

【実施内容】

1) 格付けに応じた情報の保存

(1) 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。

(2) 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。
(3) 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。
(4) 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。
(5) 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。

2) 保存期間

(1) 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。

3.1.2.4. 情報の移送

【趣旨】

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。

【実施内容】

1) 情報の移送に関する許可及び届出

(1) 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。
(2) 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。

2) 情報の送信と運搬の選択

(1) 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、また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。

3) 移送手段の選択

(1) 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。

4) 書面に記載された情報の保護対策

(1) 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。

5) 電磁的記録の保護対策

(1) 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。

3.1.2.5. 情報の提供

【趣旨】

水道事業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。

【実施内容】

1） 情報の公表

(1) 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。

(2) 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。

2） 他者への情報提供

(1) 水道事業従事者が機密情報を水道事業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。

(2) 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。

(3) 提供先において水道事業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。

(4) 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。

3.1.2.6. 情報の消去

【趣旨】

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。

【実施内容】

1） 電磁的記録の消去方法

(1) 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。

(2) 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。

(3) 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。

2） 書面の廃棄方法

(1) 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。

3.2. 情報セキュリティ要件の明確化に基づく対策

3.2.1. 情報セキュリティ確保のために求められる機能

3.2.1.1. 主体認証機能

【趣旨】

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に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求められる。

【実施内容】

1） 主体認証について

(1) 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こと。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 主体認証に利用する情報や道具について、それらが不正に利用されないための措置を講ずること。

(9) 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。

(10) 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などを盛り込むこと。

2） 水道事業従事者における識別コード、主体認証情報の管理

(1) 水道事業従事者に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。

(2) 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。

(3) 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取れるように、水道事業従事者は識別コードの管理者に届け出ること。

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

3.2.1.2. アクセス制御機能

【趣旨】

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求められる。

【実施内容】

1) アクセス制御機能の導入

(1) 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。

(2) 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。

(3) アクセス制御を強化する意味合いから、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、強制アクセス制御などを導入すること。

2) 水道事業従事者による適正なアクセス制御

(1) 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。

(2) 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。

3.2.1.3. 権限管理機能

【趣旨】

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機能が必要となる。

【実施内容】

1） 権限管理機能の導入

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

2） 識別コードと主体認証情報の付与管理

(1) 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。

(2) 原則として識別コードは主体個々に付与されること。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 識別コードは一人の主体に対してひとつの情報システムでひとつとするこ

とが原則であり、これらの付与状況を記録しておくこと。

(10) 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。

3) 識別コードと主体認証情報における代替措置の適用

(1) 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。

(2) 識別コードの不正使用が認められた場合、ただちにその識別コードの利用を停止させること。

3.2.1.4. 証跡管理機能

【趣旨】

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と期待される。

【実施内容】

1) 証跡管理機能の導入

(1) 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。

(2) 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。

(3) 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象方針とその機能を整備しておくこと。

(4) 記録された証跡に対しても、消去や改ざんなど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。

(5) 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などについて自動化機能などを設けること。

2) 情報セキュリティ責任者による証跡の取得と保存

(1) 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。

(2) 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。

(3) 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。

3） 取得した証跡の点検、分析及び報告

(1) 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。

(2) 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。

(3) 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。

(4) 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。

3.2.1.5. 信頼性確保のための機能

【趣旨】

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求められる。

【実施内容】

(1) 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など、負荷分散に努めること。

(2) システム機器の予備機の設置や、通信回線の複数化など、冗長化構成に努めること。

3.2.1.6. 保証のための機能

【趣旨】

情報が適切な状態に管理されていることを保証するために、情報セキュリティの対策の実施状況を確認するなどの保証のための機能が求められる。

【実施内容】

(1) 保証のための対策の必要性を検討し、必要な場合はその機能を設けること。

3.2.1.7. 暗号と電子署名（鍵管理を含む）

【趣旨】

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、電子署名の利用が求められる。

【実施内容】

1） 暗号化機能及び電子署名の付与機能の導入

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

2) 暗号化及び電子署名の付与に関わる管理

(1) 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、保存規定などの鍵管理について、それらが露呈した場合の対策も含めて定めておくこと。

(2) 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。

(3) 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。

(4) 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など、情報収集を適切に継続すること。

3) 暗号化機能及び電子署名の付与機能の利用

(1) 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。

(2) 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。

3.2.2. 情報セキュリティについての脅威

3.2.2.1. セキュリティホール対策

【趣旨】

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、情報漏えいなどセキュリティ上の大きな脅威に繋がり、水道事業者に対する社会的信用の失墜を招きかねない。

【実施内容】

1） 情報システムの構築時

(1) 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。

(2) 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。

2） 情報システムの運用時

(1) 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。

(2) 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。

(3) 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。

(4) 対策計画に基づいて実施し、その記録を残すこと。

(5) 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(対策用のファイルなど)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。

(6) 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。

(7) 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。

3.2.2.2. 不正プログラム対策

【趣旨】

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。

【実施内容】

1） 情報システムの構築時

(1) 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

(2) 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。

(3) 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。

(4) 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。

2) 情報システムの運用時

(1) 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。

(2) 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。

(3) 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などの措置を講ずること。

(4) 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。

(5) 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。

(6) 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。

(7) 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。

3.2.2.3. サービス不能攻撃対策

【趣旨】

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などが考えられる。

水道事業では、インターネットを利用した監視制御機能など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しなければならない。

【実施内容】

1) 情報システムの構築時

(1) 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 対策機能などを活用してサービ

ス不能攻撃対策を講ずること。

(2) 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。

(3) 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。

(4) 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、または低減する対策装置を導入すること。

(5) 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などを用意すること。

(6) 水道事業者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。

2) 情報システムの運用時

(1) 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。

(2) こ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。

3.2.3. 情報システムのセキュリティ要件

【趣旨】

情報システムのライフサイクルに合わせたセキュリティ要件を特定し、対策を実施することが求められる。

【実施内容】

1) 情報システム計画・設計

(1) 情報セキュリティ責任者は、情報システムのライフサイクル全般にわたって、セキュリティ維持の体制確保についてセキュリティ要件を定めなければならない。

(2) セキュリティ要件を満たすために必要な措置（機器の調達、ソフトウェア開発、セキュリティ機能設定、セキュリティについての脅威への対策、システム構成要素）について定めること。

(3) 重要なセキュリティ要件があると認められる場合には、セキュリティ設計仕様書（ST：Security Target）について第三者機関の ST 評価、ST 確認を受けること。

(4) 当該情報システムがセキュリティ要件を満たすことが確認された後は、運用段階への導入の方法、体制、手順、工程、期間、教育、障害対応についてセキュリティの観点から定めること。

(5) 可能であれば、製品選択においてはISO/IEC 15408（JIS X 5070：セキュリティ技術　情報技術セキュリティの評価基準）に基づくITセキュリティ評価及び認証制度による認証を取得しているものを選択すること。

2) 情報システムの構築・運用・監視

(1) 構築・運用・監視のそれぞれの段階にあっては、セキュリティ要件に基づいて定めた対策を実施すること。

3) 情報システムの移行・廃棄

(1) 移行・廃棄の段階にあっては、当該システムの情報の消去、廃棄、再利用について適切な措置をとること。

4) 情報システムの見直し

(1) 情報セキュリティ責任者は、適宜情報セキュリティ対策の観点からの情報システムの見直しの必要性を検討し、必要であれば見直しを実施すること。

3.3. 情報システムについての対策

3.3.1. 施設と環境

3.3.1.1. 安全区域の設定

【趣旨】

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、改ざんなどのリスクがある。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求められる。

水道事業における安全区域の具体例としては中央監視室、制御盤室などが相当する。

【実施内容】

1) 立ち入り及び退出の管理

(1) 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。

(2) できる限り障壁、施錠など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。

(3) 入退出にあたっては主体認証を実施すること。

(4) 主体認証により承認された者が未承認の者を同伴するなどして入退室を行わないようにしなければならない。

(5) 全ての入退出の理由や期間など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。

(6) 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。

2) 訪問者及び受け渡し業者の管理

(1) 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。

(2) 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、出迎えなど）を採用すること。

(3) 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。

(4) 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 カードの着用など）を導入すること。

(5) 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が付き添うなどの方策を講ずること。

3) 電子計算機及び通信回線装置のセキュリティ確保

(1) 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。

(2) 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。

(3) 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などを防止する対策を講ずること。

4) 安全区域内のセキュリティ管理

(1) 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。

(2) 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。

(3) 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。

(4) 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。

5) 災害及び障害への対策

(1) 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。

(2) 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。

(3) 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などの措置を講ずること。

3.3.2. 電子計算機

3.3.2.1. 電子計算機共通対策

【趣旨】

ウィルス感染、不正侵入など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など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必要である。

【実施内容】

1) 電子計算機の設置時

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 適正な運用のために、仕様書や操作マニュアルなどの電子計算機関連文書を整備すること。

(6) 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。

(7) 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。

(8) 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。

2) 電子計算機の運用・保守時

(1) 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。

(2) この規定は適宜見直しを行うこと。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

(7) システムの統合、更新時には十分な検証等を行うこと。

3) 電子計算機の運用終了時

(1) 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などにより全ての情報を復元困難な状態にすること。

3.3.2.2. 端末

【趣旨】

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などのリスクも高まる。

【実施内容】

1) 端末の設置時

(1) 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などして制限を設けること。

(2) 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。

(3) 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。

(4) 必要に応じて情報を保存できない端末を利用すること。

2) 端末の運用時

(1) 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。

(2) 暗号化、盗難防止措置を必要に応じて講じること。

(3) 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。

(4) 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ておくために、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。

3.3.2.3. サーバ装置

【趣旨】

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サービス停止、水道事業への信用失墜などの影響範囲は大きなものとなりかねない。

【実施内容】

1） サーバ装置の設置時

(1) 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。

(2) 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。

(3) 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。

(4) 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。

2） サーバ装置の運用時

(1) 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。

(2) 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。

(3) 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

(4) 必要に応じて証跡管理を実施すること。

(5) 端末同様にサーバ装置の時刻も同期すること。

(6) 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。

(7) 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。

3.3.3. アプリケーションソフトウェア

3.3.3.1. 通信回線を介して提供するアプリケーション共通対策

【趣旨】

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が求められる。

【実施内容】

1） アプリケーションの導入時

(1) 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。

2） アプリケーションの運用・保守時

(1) 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。

(2) 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。

(3) システムの統合・更新時には十分な検証等を行うこと。

3.3.3.2. 電子メール

【趣旨】

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など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求められる。

【実施内容】

1） 電子メールの導入時

(1) 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。

(2) 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。

2） 電子メールの運用時

(1) 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。

(2) 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。

(3) 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。

3.3.3.3. ウェブ

【趣旨】

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必要がある。

【実施内容】

1） ウェブの導入時

○情報提供者が行うべき対策

(1) 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。

○情報提供者・情報利用者共通の対策

(2) 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。

(3) 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。

2） ウェブの運用時

○情報利用者が行うべき対策

(1) 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。

○情報提供者が行うべき対策

(2) 無用なリスクを回避するためには、当該の水道事業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。

3.3.4. 通信回線及び通信回線装置

3.3.4.1. 通信回線共通対策

【趣旨】

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、破壊などのリスクが存在する。

【実施内容】

1） 通信回線の構築時

(1) 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。

(2) 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。

(3) 通信回線について仕様書、設計書、回線の構成図など通信回線装置関連文書を整備すること。

(4) アクセス制御など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。

(5) 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。

(6) 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。

(7) 通信回線については物理的な安全対策を講ずること。

(8) 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。
(9) 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。
(10) 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。
(11) 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。
(12) 必要に応じて証跡管理を実施すること。
(13) 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。

2) 通信回線の運用時

(1) 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などを管理すること
(2) 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。
(3) 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、アクセス制御設定などの変更を確認し、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。
(4) 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。
(5) 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。
(6) 通信装置のセキュリティホール対策、時刻同期などは電子計算機や端末と同様に実施すること。

3) 通信回線の運用終了時

(1) 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。

3.3.4.2. 庁舎内通信回線の管理

【趣旨】

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、破壊などのリスクが存在する。

【実施内容】

1) 庁舎内通信回線の構築時

(1) 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などの仕組みにより確認する措置を講ずること。

2) 庁舎内通信回線の運用時

(1) 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。
(2) 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。
(3) 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。

3) 回線の対策

(1) 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、通信回線の範囲などを適切に検討、決定すること。

3.3.4.3. 庁舎外通信回線との接続

【趣旨】

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。

【実施内容】

1) 庁舎内通信回線と庁舎外通信回線との接続時

(1) 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。
(2) 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。

2) 庁舎外通信回線と接続している庁舎内通信回線の運用時

(1) 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、また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。
(2) 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。
(3) セキュリティホール対策、通信回線の利用状況管理、通信内容監視を適切に実施すること。

3.4. IT 障害の観点から見た事業継続性確保のための対策

3.4.1. 事業継続性確保のための個別対策の実施対策

【趣旨】

情報システムの停止が水道事業全般的な事業継続性を損ねないように、対象と

なる情報システムにおいて、それぞれのシステムの特徴を鑑みたうえで必要となる事業継続性確保に向けた対策が必要である。

【実施内容】

(1) 事業継続性確保の全般的な対策として、ISMS（Information Security Management System：情報セキュリティマネジメントシステム）の基準（JIS Q 27002）を参考に、以下に記載する事項について検討すること。

・継続すべき重要業務の洗い出し（順序立て）
・重要要素（ボトルネック）の抽出
・事業継続計画の策定
・被害の想定
・訓練・教育の実施
・マネジメント

(2) 水道事業における継続すべき重要業務は、水の供給（給水サービス）であることから、制御系システムはその停止が水道水供給の停止に直結し得る最も重要なシステムと位置づけること。

(3) 特にウェブの応用による汎用システムを採用している場合などは、その脆弱性を補完するための対策をとること。

(4) 事業継続計画に策定すべき内容として、重要拠点機能の確保、バックアップの考慮などについては以下の観点を考慮して対策を講じること。

・情報システム障害の影響範囲が直ちに水供給停止につながらない場合は、水供給の状況を適切に監視しつつ情報システム障害の復旧を行う。
・情報システム障害により一部施設の運転を継続できない場合には、障害の発生した情報システムを切り離し、他の施設から水融通することや配水場単位で運転することなどにより、極力水の供給を継続できるようにシステムを構築しておく。
・制御系システムが障害を受けた場合でも手動にて水供給できるように、手動操作手段の確保や自然流下系施設の配置、緊急時用の貯留水量の確保等についてもできるだけ配慮する。
・社会全体で対応が望まれる脅威（新型インフルエンザ等）を想定した、非常時の人員配置や組織体制を構築しておく。
・障害が相互に波及する可能性のある重要インフラ分野（電力、ガス、情報通信等）においてサービス障害が発生した場合の対策についても検討しておく。
・標的型攻撃、制御システムへの攻撃等、最近の情報セキュリティを取り巻く環境変化への対応についても検討しておく。

(5) 自然流下系施設による水の供給機能は、重要インフラの中でも水道だけが有する優れた特徴であり、このような水道施設の特徴を活かした水供給シス

テムの構築を、地震対策などの視点のみならず情報セキュリティ対策の視点からも実施すること。

(6) 東日本大震災において重要インフラ分野に生じた複合的な障害（電力・通信の途絶、燃料の不足、機器水没等）を踏まえた情報セキュリティ上のリスクを想定しておく。

3.4.2. 事業継続計画との整合性への配慮

【趣旨】

情報セキュリティに限らず、水道事業全般にわたる事業継続に関わる対策が事業継続計画として策定されているべきであり、これに情報セキュリティ分野における事業継続対策は整合していなければならない。また、事業継続計画は、適宜点検され、必要に応じ対策の改善が行われなければならない。

【実施内容】

(1) 情報セキュリティ分野における事業継続対策を考える際には、以下の各ガイドラインにより情報セキュリティのことも踏まえた水道事業全般にわたる事業継続に係る内容を把握した上で、情報セキュリティにおいて、それと整合のとれた対策を盛込むこと。

・事業継続ガイドライン第二版－わが国企業の減災と災害対応の向上のために－（平成 21 年 11 月、内閣府防災担当）

・企業における情報セキュリティガバナンスのあり方に関する研究会報告書参考資料　事業継続計画策定ガイドライン（平成 17 年 3 月、経済産業省）

(2) 水道用水供給事業と受水団体間の事業継続計画においても整合性に留意が必要である。

(3) 障害が相互に波及する可能性のある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）において、リスクコミュニケーション等の連絡・連携に平時より務めること。

(4) セプターカウンシルにおいて集約される相互理解、ベストプラクティス等の具体的な事例共有等、分野横断的な情報を積極的に収集し、適宜情報セキュリティ対策に反映すること。

3.5. 情報漏えい防止のための対策

【趣旨】

重要インフラにおいて発生する情報漏えいは、その機能の停止、低下につながる恐れがあるため、その発生防止及び再発防止対策に取り組む必要がある。

3.5.1. 保護すべき情報の類型化

【実施内容】

(1) 漏えい対策の対象となる保護すべき情報を類型化すること。

3.5.2. 保護すべき情報の管理

【実施内容】

(1) 保護すべき情報及び当該情報が記録された媒体を安全に取り扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置を明示すること。

3.5.3. 不正アクセスによる脅威への対策

【実施内容】

(1) 保護すべき情報が保存された電子計算機や外部記録媒体の盗難、紛失及びその場合の情報漏洩を防止するための措置を明示すること。

(2) 保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏洩を防止するための措置を明示すること。

(3) 水道では、特に遠隔的な不正アクセスによる直接的な被害を生じさせない（水道停止に至らない）ようにする対策を講ずること。

3.5.4. 内部関係者による脅威への対策

【実施内容】

(1) 内部関係者による情報漏えいを抑止するための措置を明示すること。

(2) 情報漏えいの追跡性確保のための措置を明示すること。

(3) 情報セキュリティに関するリテラシー（知識、能力）を向上させるための措置や、取扱いミスを低減させるための措置を明示すること。

3.5.5. 情報漏えい発生時の対応策の準備

【実施内容】

(1) 情報漏洩の発生に備えて、当該事象へ対応するための体制、及び対処手順等を明示すること。

3.6. 外部委託における情報セキュリティ確保のための対策

【趣旨】

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による委託先の情報セキュリティ確保対策が必要である。

水道事業においては、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のシステムを構築したり運転したりするだけでなく、委託業者と水道事業者が共通の情報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。

3.6.1. 委託先管理の仕組み

【実施内容】

(1) 国際規格（JIS X 5080 など）を踏まえた既存の取組み等を参考に、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等を明示すること。

(2) 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。

(3) 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。

(4) 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と同じまた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。

3.6.2. 外部委託実施における情報セキュリティ確保対策の徹底

【実施内容】

(1) 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。

(2) 万一情報漏洩等の障害が発生した場合のペナルティについても合意形成を行っておくこと。

3.6.3. IT 障害発生時の対応策の整備

【実施内容】

(1) 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が一体となったトラブル対処方法等）を明示すること。

(2) 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。

(3) 重要インフラとして可能な限り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。

3.7. IT 障害発生時の利用者の対応ための情報の提供等の対策

【趣旨】

水道サービスの停止・低下が発生した際、利用者が安心して対応が行えるような情報提供を行うことが重要である。

【実施内容】

1) IT 障害による水道サービスの停止等の情報の提供

(1) 水道サービスの停止状況、復旧（可能であれば見込みを含む。）等の情報の適時の提供の方策を明示すること。

2) IT 障害防止のための取組みに関する情報の提供

(1) 利用者の安心に資する観点から、水道サービスの停止・低下を防止するための情報セキュリティ対策に関する取組みについて、提供範囲に留意しつつ、対外的な説明に努めること。

3.8. IT に係る環境変化に伴う脅威のための対策

【趣旨】

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 への移行」、従来型の携帯電話と比べて利用者の個人情報等が集約される可能性があるが、パソコン利用者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出来ない場合のある「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。

【実施内容】

(1) 平素から IT に係る社会環境や技術環境等の変化に配慮するとともに、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、新たな情報の共有に務めること。

(2) 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。

(3) 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。

【対策編】具体的な対策項目

Ⅰ．本資料の位置づけ

本資料は、水道事業における情報セキュリティ確保のために、重要インフラ専門委員会が平成 25 年 3 月 26 日に改訂した「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」策定にあたっての指針　対策編（第３版)」を、本ガイドラインの内容に合わせて再構成したものである。安全基準等の継続的な改善を行う際、具体的な対策項目を確認するためのチェックリストとして活用いただければ幸いである。

また、各水道事業者等において、重要インフラとしての水道事業の特性を踏まえつつ、適宜対策項目の追加等を行い、安全基準等の継続的改善を実施することを期待する。

Ⅱ．具体的な対策項目

以下に、本ガイドライン 2 章以降の目次に沿った具体的な対策項目を示す。

2. 組織・体制および資源の対策

2.1. 組織・体制及び人的資源の確保

水道事業者等における情報セキュリティ対策のPDCAサイクルを機能させるために、その運用等に係る組織及び体制の確立及びこれを支える資源の確保が重要である。

情報セキュリティ対策は、それに係る全ての職員が、職制及び職務に応じて与えられている権限と責務を理解した上で、準備された資源によって、負うべき責務を履行することで実現される。

このため、情報セキュリティ対策を実施する組織・体制及び資源の確保について明示されることが必要である。

なお、組織・体制及び資源の確保には、例えば、情報セキュリティに関わる人材育成や教育といった基礎的・長期的な取り組みから、情報セキュリティ対策の実効性を確保する上で必要な自己点検・監査の実施等具体的な対策項目が含まれる。

〇組織・体制の確立

・情報セキュリティ基本方針の策定

・情報セキュリティに関する組織体制の整備（責任者・責任部門・委員会等の設置、役割・責任分担の明確化等

・情報セキュリティ関係規程の整備（違反への対処、例外措置等）

・人的資源確保（雇用条件の明示、守秘契約の締結、懲戒手続等）
・IT障害発生時の体制・対応手順の整備（「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」が想定するサイバー攻撃、非意図的要因、災害や疾病等の脅威が引き起こすIT障害に関わる情報の集約及び共有体制を含む）

○教育・訓練の実施

・情報セキュリティ対策の教育・訓練計画の策定
・教育・訓練実施記録の保管
・訓練シナリオの具体化・高度化
・地域での連携促進策の検討
・同業種における相互支援の事前訓練

○自己点検・内部監査の実施

・自己点検の実施
・内部・外部監査の実施
・情報セキュリティ対策の見直し

2.2. 情報セキュリティ人材の育成等

知的財産としての「人財」という観点から、情報セキュリティ人材の育成や要員の管理を行うことが望ましい。

・情報セキュリティ人材の育成・活用・管理に関する規定の整備（情報処理技術者試験、情報システムユーザースキル標準等を活用し、社内人材育成マップ等の作成とこれに基づく社内教育コースの整備等を記載）
・インシデント発生時に対応ができる人材の計画的な育成

2.3. 外部監査等による情報セキュリティ対策の評価

技術的な対策は多くの事業者等で行われているが、今後は外部監査等による情報セキュリティ対策の評価を行うことが望ましい。

・情報セキュリティ監査等の実施
・情報セキュリティ対策の見直し

3. 情報セキュリティ対策

3.1. 情報についての対策

3.1.1. 情報の格付け

取扱う情報について、その重要度に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から、情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配付禁止）が明示されるべきである。

〇重要性に応じた適切な措置

・資産の洗出し（体制、洗出し項目、洗い出し基準等）

・情報のライフサイクルと情報の格付けに応じた情報セキュリティ対策

3.1.2. 情報の取り扱い

情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階における情報セキュリティ対策が明示されるべきである。

〇情報の作成と入手

・目的外の作成・入手の禁止

・台帳等作成

・作成・入手時における格付けと取扱制限の決定

・作成時点の情報の格付けの継承

・格付けの変更手続き

〇情報の利用

・情報の利用に関する許可及び届出に係る措置

・目的外利用の禁止

・格付け及び取扱制限に従った情報の取扱い

・格付け及び取扱制限の見直し

・アクセス履歴の保存

・アクセス制御・出力制御

・離席時の対策（端末ロック等）

〇情報の保存

・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載）

・情報の保存期間に従った管理

〇情報の移送

・情報の移送に関する許可及び届出に係る措置

・作業責任者・手続きの明確化

・作業担当者の識別、認証、権限付与

・移送手段の選択

・書面の保護対策

・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等）

〇情報の提供

・提供に関する許可及び届出

・付加情報の削除

〇情報の消去

・情報の消去に関する許可及び届出
・電磁的記録の消去記録の保管　（消去の確認、消去記録の保管等）

3.2. 情報セキュリティ要件の明確化に基づく対策

3.2.1. 情報セキュリティ確保のために求められる機能

主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

〇主体認証

・主体認証機能の導入
・主体認証技術の選択（知識、所有、生体認証、及び多要素認証等）
・利用者IDの管理（個人単位のID付与、不要IDの削除等）
・主体認証情報の管理（暗号化、パスワードの定期変更・最低文字数の制限、ID毎に異なるパスワードの設定等）
・利用者の責任（パスワードの利用、端末管理、クリアデスク・クリアスクリーン方針）
・不正使用検知時における主体認証の利用停止措置

〇アクセス制御

・アクセス制御機能の導入
・利用者アクセスの管理（利用者登録、特権管理、利用者パスワードの管理、利用者アクセス権のレビュー等）
・ネットワークのアクセス制御方針の策定
・利用者属性以外に基づくアクセス制御機能の導入（利用時間による制御、利用時間帯による制御、利用端末の識別、強制アクセス制御等）

〇権限管理

・権限管理機能の導入
・利用者IDと主体認証情報の付与管理
・利用者IDと主体認証情報における代替手段等の適用

〇証跡管理

・証跡管理機能の導入実施
・証跡取得と保存
・取得した証跡の点検、分析及び報告
・証跡管理に関する利用者への周知

〇負荷分散

・トラフィックの分散処理、予備機の設置
・負荷状態の監視制御機能の充実

〇冗長化

・ネットワークの適切な管理・制御、通信経路の迂回措置
・ハードウェアの予備
・（アプリケーション機能を含めた）情報システムの冗長対策

3.2.2. 情報セキュリティについての脅威

セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

〇セキュリティホール

・情報収集
・対応計画の策定
・対応内容の記録
・定期チェック
・不正アクセスの監視・検出（IDSの使用）
・通信フィルタリング（ファイアウォール、ウェブアプリケーションファイアウォール（WAF）等）
・外部ネットワークからの遮断等
・アンチウィルスソフトウェアの使用（端末、ゲートウェイ）、メンテナンス、定期検査、セキュリティパッチ適用
・利用していない通信ポート等の非活性化、マクロ実行の抑制
・早期発見・早期回復対策（監視、障害の検出、障害箇所の切り分け、障害時の縮退・再構成、取引制限、リカバリ機能）

〇不正プログラム

・情報収集
・OS／アプリケーションのセキュリティ設定
・アンチウィルスソフトウェアの導入
・パターンファイルの更新
・パッチ適用
・定期的なウィルス検査

〇サービス不能攻撃

・通信フィルタリング
・通信回線の冗長化
・通信事業者との連携
・電子計算機、通信回線装置及び通信回線の監視と記録

3.3. 情報システムについての対策

3.3.1. 施設と環境

入退出の管理や安全区域の確保、停電時、断水時の対応等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。

○入退出の管理

・入退出管理（障壁、施錠、主体認証、入退出履歴の記録、継続的に立ち入る者の承認、侵入監視装置の設置、最小限の施設表示）

・訪問者、清掃業者及び物品の搬出入業者の管理（身分の記録、入室審査手順、立ち入り制限区域の設定、職員等の立ち会い・付き添い、ストラップ・IDカード、情報システムに接触できない場所での受け渡し）

○安全区域の確保

・設置場所の配慮（バックアップセンターの設置、遠隔地でのバックアップ媒体保管、災害を受けにくい場所への設置等）

・物理的セキュリティ境界の設定

・電子計算機及び通信回線装置のセキュリティ確保（不正操作・盗み見等の防止対策）

・安全区域内のセキュリティ管理策（身分証明書の携帯・常時視認、物品等の持ち込み・持ち出しの情報セキュリティ責任者の承認・記録、コンピュータ・外部記録媒体等の持ち込み制限、作業の監視）

・防犯対策（侵入防止装置、赤外線検知装置、トラップセンサーの設置、記録用機器の使用制限、盗難防止装置）

○電力供給の途絶・通信の途絶・水道供給の途絶への対応

・防災対策（建物の耐震・免震構造及び防火構造化、設備の転倒等防止対策・防火対策・落雷対策・防水対策、監視設備・警報装置・非常口及び非常灯設置等）

・自家発電装置、無停電電源装置、予備電源

・空調（加湿を含む）設備の冷却水の備蓄等

・通信回線の冗長化

・燃料の備蓄等（自家用発電設備、車両等）

3.3.2. 電子計算機

電子計算機の設置時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

〇設置時

・文書（仕様書・設計書、機種・利用ソフトウェアの種類及びバージョン情報、管理者・利用者情報、利用者ID管理情報、構成要素のセキュリティに関する手順等）整備及び変更管理手順の明確化
・供給元及び更新情報、保守期間等が明確な機器の利用
・情報システムの受入れに必要な要求事項（受入れ基準）の明確化
・情報システムの受入れ前試験実施と合否判定基準の明確化
・サプライチェーンにおける情報セキュリティを考慮した機器の調達（信頼のできるベンダーから調達する等）
・安全区域への設置
・防災対策（設備の転倒等防止対策・防火対策・落雷対策・防水対策、監視設備・警報装置・非常口及び非常灯設置等）
・電子計算機の十分な性能（処理能力・容量・拡張性）の確保
・電子計算機の負荷分散・冗長構成化
・不要なアプリケーションの利用禁止・不要な機能の無効化・削除
・端末で利用可能なソフトウェアの制限
・端末の盗難防止対策
・モバイル端末に対するセキュリティ機能の装備（ワンタイムパスワード、暗号化、遠隔ロック、遠隔消去等）
・記録媒体を持たない端末の利用
・サーバ装置に対する暗号化機能の装備（遠隔保守時）
・障害時、緊急時の対応手順の策定

〇運用時（保守時含む）

・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・定期的調査による利用ソフトウェアの把握
・不正行為及び不正アクセスの検知（アクセスログ確認、侵入検知システム・アンチウイルスソフトウェア使用等）
・稼働状態監視（通常時、繁忙時のシステムの性能、容量、処理能力管理）による異常検知
・運用管理記録、障害記録、作業記録の作成・管理
・端末等の盗難防止対策
・モバイル端末で利用する電磁的媒体の暗号化

・利用可能な通信回線、通信方法の制限
・情報システム内の時刻同期化
・構成管理（機器管理、外部接続管理）
・情報システムの構成変更の定期的な確認
・定期的なバックアップ取得とバックアップ媒体の安全管理（遠隔地保等）
・定期的なパスワードの変更
・障害時、緊急時を想定した訓練（復旧テスト等）の実施
・外部委託業者の作業の監視
・利用ソフトウェアのアップデート、脆弱性に関する情報収集
・主体認証（ネットワーク接続時も含む）
・セキュリティホール対策（検査、対応）
・無線LAN使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・内部と外部のネットワークの分離
・防災対策の定期的な見直し

〇システム統合時

・統合に伴うリスク管理体制の構築
・移行基準の明確化
・統合後の業務運営体制の検証

〇運用終了時

・廃棄計画・手順の策定
・電磁的記録（媒体）の情報抹消

3.3.3. アプリケーションソフトウェア

アプリケーションソフトウェアの導入時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

〇導入時

・情報セキュリティ要件の検討、仕様化
・運用体制（管理者、障害時の連絡体制、委託先窓口等連絡先、通常時以外の特別体制）の決定及び周知
・文書（仕様書・設計書、機種・利用ソフトウェアの種類及びバージョン情報、管理者・利用者情報、利用者ID管理情報、構成要素のセキュリティに関する手順等）整備及び変更管理手順の明確化
・バージョン管理
・開発環境と本番環境の分離

・ソフトウェア開発を外部委託する場合の契約手順
・電子メールの不正中継禁止
・電子メール送信時及び受信時の送信ドメイン認証（SPF等）
・主体認証
・ウェブにおける特殊文字使用の禁止、無効化
・ウェブにおける脆弱性のある作りこみの回避
・攻撃に利用されるウェブサーバ情報の送信を防ぐ対策
・公開するサーバ上に保存する情報の制限
・電子証明書による正当性の証明
・通信情報（データ）の暗号化

〇運用時（保守時含む）

・利用ソフトウェア管理、バージョン管理
・利用ソフトウェアのアップデート、脆弱性に関する情報収集
・電子署名による配布元の確認（ソフトウェアダウンロード時）
・HTMLメール使用時の注意
・電子メールの対策・制限（添付ファイルの保護、不正中継禁止、送受信容量の制限、自動転送、業務外利用、送信先アドレス漏洩の防止、電子署名、暗号化、迷惑メールフィルター）
・外部ネットワークとの接続制限（プロキシ経由等）
・データバックアップ、バックアップ媒体の安全管理
・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・証跡管理
・不正検知
・稼働状態監視（通常時、繁忙時の性能、容量、処理能力管理）による異常検知
・無許可ネットワーク、外部ネットワーク接続の禁止
・運用管理記録、障害記録、作業記録の作成・管理（外部委託業者の作業管理も含む。）
・主体認証（ネットワーク接続時も含む）
・セキュリティホール対策（検査、対応）
・無線LAN使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・内部と外部のネットワークの分離
・構成管理（機器管理、外部接続管理）

〇システム統合時

・統合に伴うリスク管理体制の構築
・移行基準の明確化

・統合後の業務運営体制の検証

〇運用終了時

・廃棄計画・手順の策定

・電磁的記録（媒体）の情報抹消

3.3.4. 通信回線及び通信回線装置

通信回線及び通信回線装置の構築から運用、運用終了又は停止に至るまでの対策が明示されるべきである。

〇構築時

・未承認機器からの通信の遮断

・通信の暗号化

・通信性能の確保

・遠隔地からの保守時の対策

・外部からの侵入が困難な回線の選択

・原則公衆回線からの接続の禁止（例外時はコールバックやユーザの限定）

・移動、転倒防止措置

・不特定多数が接続するネットワークとの接続禁止

・改ざん防止対策

・盗聴防止対策

・客観的に評価された製品等の導入の検討

・供給元及び更新情報、保守期間等が明確な機器の利用

・文書（仕様書、規程、マニュアル、利用者管理）の整備及び変更管理手順の明確化

〇運用時

・変更管理

・運用管理記録の作成

・稼働監視

・利用する機器、利用者及び識別コードの管理

・リモートアクセス時の対策（主体認証、証跡管理、アクセス制限、機密性確保、利用可能な端末の管理）

・不要なポートの閉塞

・無許可ネットワーク、外部ネットワーク接続の禁止

・制御系ネットワークの分離

・ルータによるDoS攻撃対策

・入退室管理（障壁、施錠、主体認証、記録、継続的に立ち入る者の承認、侵入監視装置の設置、施設の最小限表示）

・データバックアップ、バックアップ媒体の安全管理
・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・証跡管理
・不正検知、異常（非日常状態の）検知
・稼働監視（通常時、繁忙時の性能、トラブル時の復旧時間、再発防止策の実施状況、システム容量・能力管理）
・情報収集（利用ソフトウェア）
・運用管理記録、障害記録、作業記録の作成・管理（外部委託業者の作業管理も含む）
・主体認証（ネットワーク接続時も含む）
・時刻同期
・セキュリティホール対策（検査、対応）
・無線LAN使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・構成管理（機器管理、外部接続管理）
・ネットワーク構成等に関する情報の秘匿

〇運用終了時

・廃棄計画・手順の策定
・電磁的記録（媒体）の情報抹消

3.4. IT 障害の観点から見た事業継続性確保のための対策

3.4.1. 事業継続性確保のための個別対策の実施

IT障害を未然に防止するための措置、IT障害の発生を早期発見するための措置、及びIT障害が発生した場合の拡大防止や迅速復旧のための措置が明示されるべきである。その際、東日本大震災に見られた広域災害・複合障害や新型インフルエンザ等、社会全体で対応が望まれる脅威についても考慮されるべきである。

〇未然防止措置

・指揮命令系統の明確化
・権限委譲、代行順位の決定
・重要拠点（指揮拠点）の確保
・事業継続計画の策定・事業継続計画の教育・訓練計画の策定・訓練の実施
・事業継続計画の教育・訓練実施記録の保管、緊急連絡ルールの確定（連絡先、連絡事項、連絡手段）
・連絡不可能な場合（通信途絶等）の緊急行動ルールの確定
・所管省庁への連絡体制
・情報システム・通信回線の冗長化、代替手段の整備

・信頼性設計
・物理的な不正侵入の防止
・他情報システムとの独立、接続点の最小化
・情報システムの定期点検及び更新
・緊急時の処理増加等を考慮した情報システムの余裕設計
・代替情報システムの作業手順書策定

〇早期発見のための措置

・情報システムの稼働監視
・不正アクセス、不正トラフィックの監視
・様々な主体が提供する災害・障害発生時の情報サービスの活用
・制御設備等の状態監視、異常検知手法の検討

〇拡大防止・早期復旧のための措置

・複数の連絡手段の準備
・自家発電装置等で使用する燃料の準備
・対外的な情報発信、情報共有
・バックアップシステムの整備、代替手段及び代替手段に必要なシステムの準備
・バックアップ稼働計画、復帰計画の策定
・情報の格付けに応じたデータバックアップ（オンライン、媒体保管等）、遠隔地への保管
・通信途絶時でも必要最小限の業務を継続するための準備
・業界内での相互理支援に備えたデータ形式の標準化推進
・クラウドシステム等専門ITサービスの活用促進
・システム通信回線の確保、通信途絶時のシステム運用ルール
・連絡手段の確保
・機器操作マニュアルの整備（非常時運転方法、自動／手動の切替え方法等を含む）
・設備点検等チェックリストの整備
・広報、利用者からの問い合わせへの対応

〇社会全体で対応する脅威に対する準備

・パンデミック対策（コンピュータセンターのオペレータ要員の確保等）
・大規模災害、津波等、発生確率が低いが発生時の影響が甚大なリスクへの対策検討（事業継続の阻害要因を整理したリスクマップの作成）

3.4.2. 事業継続計画との整合性への配慮

事業継続計画が策定される場合には、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである。その際、相互依存関係にある重要インフラ分野間（情報通信、電力、水道分野等と他分野の間、またそれ以外の事業者及び関係組織との間）において、リスクコミュニケーション等の連絡・連携に平時より努めるべきである。

〇事業継続計画との整合性の確保

・事業継続計画の実施優先順位と判断基準の明確化
・事業継続計画の実施条件の明確化
・事業継続計画の定期的な見直し
・事業継続計画と情報セキュリティ対策との間の整合性確保
・平時からのリスクコミュニケーションの実施（セプターカウンシルの活用等）
・意思決定・権限委譲ルールの見直し
・非常時の重要データの持ち出し優先順位・ルール等の検討
・データ等災害対策関連技術の標準化
・災害時の通信手段の見直し

3.5. 情報漏えい防止のための対策

3.5.1. 保護すべき情報の類型化

漏えい対策の対象となる保護すべき情報を類型化し、明示されるべきである。

〇保護すべき情報の類型化

・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け
・情報資産の洗出し方法（体制、洗出し項目、洗出し基準）、情報、情報システムについてのランク付け
・情報資産の機密性、完全性、可用性に基づく分類
・安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた重要度に応じた分類）
・個人データ取扱台帳の整備、リスクアセスメント結果に応じた分類

3.5.2. 保護すべき情報の管理

保護すべき情報及び当該情報が記録された媒体を安全に取扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置が明示されるべきである。

〇情報の作成と入手

・目的外の作成・入手の禁止

・台帳等作成
・作成・入手時における格付けと取扱制限の決定
・作成時点の情報の格付けの継承
・格付けの変更手続き

〇情報の利用

・情報の利用に関する許可及び届出に係る措置
・目的外利用の禁止
・格付け及び取扱制限に従った情報の取扱い
・格付け及び取扱制限の見直し
・アクセス履歴の保存
・アクセス制御・出力制御
・離席時の対策（端末ロック等）
・要保護情報の利用にあたっての措置（情報交換の方針及び手順、取外し可能な媒体の管理、重要情報の内部漏えい、盗難、紛失、流出への対策）
・書類や電子媒体の持ち出し管理（書類等の保管ルール、端末への資料の保管、持出しに関するルールや制限）

〇情報の保存

・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載）
・情報の保存期間に従った管理
・安全な場所への保管（自然災害を被る可能性が低い地域への保管、外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管）
・内容表示の記号化（媒体等に保存情報内容が想定できるタイトル表示をすることの禁止）
・バックアップの分散、隔地保管

〇情報の移送

・情報の移送に関する許可及び届出に係る措置
・作業責任者・手続きの明確化
・作業担当者の識別、認証、権限付与
・移送手段の選択
・書面の保護対策
・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等）

〇情報の提供

・情報の提供に関する許可及び届出
・付加情報の削除

〇情報の消去

・情報の消去に関する許可及び届出
・電磁的記録の消去手続き（消去の確認、消去記録の保管等）

3.5.3. 不正アクセスによる脅威への対策

保護すべき情報が保存されたPCや外部記録媒体の盗難､紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための措置が明示されるべきである。

○ＰＣや外部記録媒体の盗難、紛失を防止するための措置

・入退室管理
・PC・外部記録媒体の原則外部持ち出し禁止
・移動可能な機器の盗難防止策、情報盗難の防止等の措置の実施

○ＰＣや外部記録媒体からの情報漏えいを防止するための措置

・安全管理措置を講ずるための組織体制の整備、規定整備とそれに従った運用
・個人データの取扱状況を一覧できる手段の整備
・雇用契約時及び委託契約時における非開示契約の締結
・職員に対する教育・訓練の実施
・保存の際のパスワード、暗号化等の対策の実施
・電子メールを送信する場合の宛先確認

○アプリケーションからの情報漏えいを防止するための措置

・取扱者の責任と権限の明確化
・取扱手順の規定と実施状況の確認
・主体認証機能、アクセス制御機能、権限管理機能
・データ漏洩防止（暗証番号等の漏洩防止、相手端末確認機能）
・破壊・改ざん防止（排他制限機能、不良データ検出機能、ファイル突合機能）
・予防策（取引制限機能、事故時の取引禁止機能、電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能）
・ネットワーク上からの不正アクセス対策（ファイアウォール、アンチウイルスソフトウェア、IDS、WAF）、不正侵入防止機能（使用されていないポートの閉鎖、データの書き換えを検出する設定、定期的な改ざんの有無の検査）
・攻撃の記録の保存と関係機関との連携
・検知策（アクセスログの取得・保管、不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
・早期発見策（監視機能、障害の検出及び障害箇所の切り分け機能）
・早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

3.5.4. 内部関係者による脅威への対策

内部関係者による情報漏えいを抑止するための措置、情報漏えいの追跡性確保のための措置の他、情報セキュリティに関するリテラシーを向上させるための措置や取扱いミスを低減させるための措置が明示されるべきである。

〇内部関係者による情報漏えいを抑止するための措置

- 個人データ管理責任者の選定（閲覧等の利用時の管理者の許可）
- 役割・責任分担の明確化等
- 外部での情報処理に関する規定の整備（事業者外での情報処理の制限）
- 個人データを取り扱う職員及び権限の明確化
- 守秘・非開示契約の締結（不当な目的での使用等の禁止）
- 書類等の保管ルール（施錠可能なキャビネットへの保管、鍵の管理）
- 端末への資料の保管、持出しに関するルールや制限
- 入退室管理や常時監視（カメラ）等の導入
- 破壊・改ざん防止（排他制限機能、アクセス制限機能、不良データ検出機能、ファイル突合機能、IDの不正使用防止機能）
- 事業者支給以外のシステムによる情報処理の制限
- 異常発見時の対応（管理者への連絡と適切な処置の実施）
- 内部からの攻撃の監視（職員の監督とモニタリング）
- 退職後の個人情報保護規程

〇情報漏えいの追跡性確保のための措置

- 証跡管理
- 検知策（不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
- 早期発見策（監視機能、障害の検出及び障害箇所の切り分け機能）
- 早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

〇リテラシーを向上させるための措置

- 情報セキュリティ対策の教育・訓練

〇取扱いミスを低減させるための措置

- 取引制限機能、事故時の取引禁止機能
- 電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能
- 外部ネットワークからのアクセス制限、不正侵入防止機能

3.5.5. 情報漏えい発生時の対応策の準備

情報漏えいの発生に備えて、当該事象へ対応するための体制及び対処手順等が明示されるべきである。

〇体制

・責任・権限を有する担当者の選任
・緊急連絡体制の構築
・報告事項、対応措置、代替手段などの規定

〇対処手順

・事実関係の把握、漏えい情報の範囲の特定）
・情報漏えい経路の特定（システム・端末の調査等）
・情報漏えい継続の阻止、被害の最小化（対象通信の遮断や対象サーバ等をネットワークから隔離するための運用フロー等の整備）
・本人への通知、事実関係の公表・広報等
・所管省庁への報告
・関係機関への周知・情報漏えいに至った経緯・原因等の解析
・再発防止策の検討と対策の実施
・情報漏えい事案等への対応状況の記録・分析

3.6. 外部委託における情報セキュリティ確保のための対策

3.6.1. 委託先管理の仕組み

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等が明示されるべきである。

〇外部委託可能な範囲の明確化や委託先の選定基準

・委託目的の明確化
・委託可能な業務範囲の明確化
・委託先選定基準の明確化（経営状況、信頼度・受託実績、技術水準、情報セキュリティ対策の実施状況（諸規定整備含む）、障害発生時の対応力等）
・委託先選定手続きの明確化

〇委託先に求める情報セキュリティ対策項目

・委託元と同等以上の情報セキュリティ対策
・情報セキュリティ対策の遵守方法
・委託先に求める情報セキュリティ対策の周知
・機密保持（機密保持契約）、目的外利用の禁止（確認書の提出）
・個人情報を扱う場合の要件の明確化
・委託先作業時の申請
・作業報告書の提出

〇事業者としての管理方法

・提供する情報の最小化
・委託先がアクセス可能な情報資産の制限
・委託先の情報セキュリティ対策の実施状況の確認

・納品検査時の情報セキュリティ対策の確認
・委託先が再委託する際の対応策の整備
・定期点検・監査の実施
・保守用専用アカウントの設定

3.6.2. 外部委託実施における情報セキュリティ確保対策の徹底

基本契約の締結や委託内容・取扱い情報の重要性に応じて、必要な情報漏えい防止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が明示されるべきである。

〇基本契約の締結

・委託先の情報セキュリティ対策（委託元と同レベル）
・機密保持（機密保持契約）、目的外利用の禁止
・再委託の制限
・委託管理責任者の設置
・委託業務内容、委託業務の執行場所、作業者、作業内容の特定
・契約内容の遵守状況を委託元が確認できる事項
・契約内容が遵守されない場合の対処手順（損害賠償請求）
・監査への協力
・契約の解約・解除に関する事項
・契約終了時の情報資産の返却及び消去

〇情報の重要性に応じた対策事項の契約への盛り込み

・取扱う情報資産に応じた対策の選定
・データ等の取扱いに関する事項（保管場所・保管方法）
・委託元と同等以上の情報セキュリティ対策の実施

〇契約者双方の責任の明確化と合意形成

・委託元・委託先双方の責任分界点の明確化
・委託先に求める情報セキュリティ対策項目の遵守
・遵守方法及び管理体制に関する取り決め
・施設全体の運用業務全般にわたる取り決め
・損害賠償に関する規定の合意

3.6.3. IT システム障害発生時の対応策の整備

IT障害発生時における委託先の措置や水道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が一体となったトラブル対処方法等）が明示されるべきである。

〇ＩＴ障害発生時における委託先の措置

・対処方法を含んだ契約の締結
・対処方法の事前の周知
・異常検知ツールの活用
・異常状態の記録・保存
・連絡体制の整備
・障害箇所の切り離し
・原因の特定
・修正プログラムの適用

〇水道事業者等としての対処方法

・問題発生時の対処の合意
・利用者への説明責任の認識
・行動基準の規定
・責任分界点の明示
・緊急時及び平常時の連絡体制の整備（業界内、ベンダー等）
・事実関係の確認
・外部要因による障害の防止
・委託先との情報共有
・他システムへの影響調査
・IT障害対応の訓練、演習の計画及び委託先を含めた実施

3.7. IT 障害発生時の利用者の対応のための情報の提供等の対策

3.7.1. IT 障害による水道サービスの停止等の情報の提供

水道サービスの停止状況、復旧（可能であれば見込みを含む。）等の情報の適時の提供の方策が明示されるべきである。

・サービス停止状況、復旧（見込み）情報の提供

3.7.2. IT 障害防止のための取組みに関する情報の提供

利用者の安心に資する観点から、水道サービスの停止・低下を防止するための情報セキュリティ対策に関する取組みについて、提供範囲に留意しつつ、対外的な説明に努めるべきである。

・情報セキュリティ報告書、CSR報告書、各種ディスクロージャ資料等の作成

・ウェブサイト、電子メール等による情報提供

3.8. IT に係る環境変化に伴う脅威のための対策

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「暗号の危殆化」や、インターネットの普及によるIPv4アドレス枯渇に伴う「IPv6への移行」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べきである。

・継続的な情報収集
・平時からの情報収集の実施
・新たな脅威が顕在化時点で速やかに検討体制が構築できる準備
・「暗号危殆化」に関する継続的な情報収集の実施（電子政府推奨暗号リスト等参照）
・「IPv6移行」に関する継続的な情報収集と実装検討の実施
・クラウドコンピューティングサービスに対する継続的な情報収集の実施
・SNS利用の職場利用禁止の徹底、アクセス制限
・水道事業者及び外部委託企業等に対するスマートデバイス管理の周知・徹底

用語の定義

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、部外者の親友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
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、または、改ざん、消去されていない状態を確保すること。改ざん、または、誤びゅう、破損により国民(水道サービス需要者)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、または、誤びゅう、破損により国民(水道サービス需要者)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もの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、または機密性 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新しいコンピュータネットワークの利用形態。
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、ひとつの主体とひとつの情報システムの組み合わせに対してひと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言う。主体認証情報の例としてはパスワードなどがある。
事業継続計画 【じぎょうけいぞくけいかく】	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（BCP を参照）。
水道事業従事者 【すいどうじぎょうじゅうじしゃ】	各水道事業の職員、並びに各水道事業の指揮命令に服している者の内、各水道事業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。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。かならずしもひとつの建物ではなく、独立した複数の「庁舎内」が存在する。
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言う。
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言う。
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、または、誤びゅう、破損により国民(水道サービス需要者)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言う。
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言う。
ら	
ライフサイクル 【らいふさいくる】	本書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.D	
BCP 【びいしいぴい】	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)。
E.F.G	

H.I.J.K	
ISAC 【あいざっく】	Information Sharing and Analysis Center のこと。 セキュリティに関する情報の分析・共有を目的とした組織として業界、業種ごとに設立されており、米国の電力業界の ISAC である ESISAC（Electric Sector ISAC）などがある。水道分野の場合は米国の Water ISAC があり、水道事業者間での情報交換のほかに、連邦安全保障機関、連邦法執行機関、情報局、衛生局とも情報交換している。 国内では通信業界に Telecom-ISAC Japan が設立された。
L.M.N.O.P	
OCIPEP 【おうしいあいぴいいいぴい】	Canadian Office of Critical Infrastructure Protection and Emergency Preparedness のこと。 カナダ国の重要インフラ防御緊急事態準備部門で 2001 年 2 月に国防省内に設立された文民組織。重要インフラの保護と緊急事態への対応についてフレームワークづくりと連邦政府内、及び州政府等との調整を行う。
Q.R.S	
SNS 【えすえぬえす】	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（ソーシャルネットワーキングサービスを参照）。
SYN Cookie 【しんくっきい】	SYN Flood 攻撃への対応策。
SYN Flood 攻撃 【しんふらっどこうげき】	サーバを機能停止に追い込む DoS（Denial of Services）攻撃の手法の一つで、ネットワークを利用して不正なデータを送信し、コンピューターや通信装置を使用不能にしたり、トラフィックを増大させてネットワークを麻痺させたりする攻撃のこと。
T.U.V	
W.X.Y.Z	

参照すべき資料

公表資料			
資料名	発行年	作成団体	アドレス
第2次情報セキュリティ基本計画「IT時代の力強い「個」と「社会」の確立に向けて」	H21	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	www.nisc.go.jp/materials/index.html
情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方～「セキュア・ジャパン」の実現に向けた情報セキュリティ政策のPDCAサイクル確立へ～	H19	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	www.nisc.go.jp/materials/index.html
「セキュア・ジャパン」の実現に向けた取組みの評価等及び合理性を持った持続的改善の推進について	H19	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	www.nisc.go.jp/materials/index.html
政府機関の情報セキュリティ対策のための統一基準	H21	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	www.nisc.go.jp/materials/index.html
セキュア・ジャパン2009 ～すべての主体に事故前提の自覚を～	H21	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	www.nisc.go.jp/materials/index.html
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	H24	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	http://www.nisc.go.jp/active/infra/pdf/infra_rt2-2.pdf
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）	H25	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	http://www.nisc.go.jp/active/infra/pdf/anzenkijyun3.pdf
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	H25	内閣官房情報セキュリティセンター（NISC） 重要インフラ専門委員会	http://www.nisc.go.jp/active/infra/pdf/infra_pl_taisaku10.pdf
電力重要インフラ防護演習に関する調査報告書	H16	独立行政法人情報処理推進機構	www.ipa.go.jp/security/fy15/reports/infra/documents/infra_2004.pdf
情報セキュリティ読本 三訂版 －IT時代の危機管理入門－	H21	独立行政法人情報処理推進機構	
行政情報システムの安全対策指針	H11	総務庁	
情報システム安全対策基準	H7、H9	通商産業省	www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf
情報システム及びネットワークのセキュリティのためのガイドライン－セキュリティ文化の普及に向けて（仮訳）	H4、H14	OECD 経済産業省	www.meti.go.jp/policy/netsecurity/oecd2002.htm

情報セキュリティ 2012	H24	内閣官房情報セキュリティセンター（NISC） 情報セキュリティ政策会議	http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf
東日本大震災における重要インフラの情報システムに係る対応状況等に関する調査	H23	内閣官房情報セキュリティセンター（NISC） 調査研究	http://www.nisc.go.jp/inquiry/pdf/infra_shinsai_report.pdf

公表資料

資料名	発行年	作成団体	備考
「情報セキュリティの基本問題に係わるテーマに関する調査研究」報告書（概要版）	H16	内閣官房情報セキュリティセンター（NISC） 株式会社日立製作所 （平成 16 年度内閣官房情報セキュリティ対策推進室委託調査）	www.bits.go.jp/inquiry/
事業継続ガイドライン 第二版－わが国企業の減災と災害対応の向上のために－	H21	内閣府 防災担当	www.bousai.go.jp/MinkanToShijyou/guideline02.pdf
企業における情報セキュリティガバナンスのあり方に関する研究会報告書	H17	経済産業省	www.meti.go.jp/report/data/g50331dj.html
平成 20 年度「個人情報の適正な保護に関する取組実践事例調査」報告書	H21	経済産業省 商務情報政策局	www.meti.go.jp/policy/it_policy/privacy/061215kozinzyouhou.htm

JIS 及び関連資料

資料名	発行年	作成団体
JIS Q 2001: 2001 リスクマネジメントシステム構築のための指針	H13	日本工業標準調査会 日本規格協会
JIS Q 15001: 2006 個人情報保護マネジメント・システム－要求事項	H18	日本工業標準調査会 日本規格協会
JIS X 0008: 2001 (IPSJ/ITSCJ/JSA) 情報処理用語－セキュリティ	H13	日本工業標準調査会 日本規格協会
JIS X 0134: 1999 (ISO/IEC 15026: 1998) システム及びソフトウェアに課せられたリスク抑制の完全性水準	H11	日本工業標準調査会 日本規格協会
JIS X 5070-1: 2000 (ISO/IEC 15408-1: 1999) セキュリティ技術－情報技術セキュリティの評価基準－第 1 部：総則及び一般モデル	H12	日本工業標準調査会 日本規格協会
JIS X 5070-2: 2000 (ISO/IEC 15408-2: 1999) セキュリティ技術－情報技術セキュリティの評価基準－第 2 部：セキュリティ機能要件	H12	日本工業標準調査会 日本規格協会
JIS X 5070-3: 2000 (ISO/IEC 15408-3: 1999) セキュリティ技術－情報技術セキュリティの評価基準－第 3 部：セキュリティ保証要件	H12	日本工業標準調査会 日本規格協会

JIS Q 27002: 2006 (ISO/IEC 17799: 2005) 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範	H18	日本工業標準調査会 日本規格協会

ウェブサイト		
サイト名	作成団体	アドレス
内閣官房情報セキュリティセンター	内閣官房情報セキュリティセンター（NISC: National Information Security Center）	www.nisc.go.jp
情報セキュリティに関する政策、緊急情報	経済産業省	www.meti.go.jp/policy/netsecurity
NERC	North American Electric Reliability Council	www.nerc.com
ES-ISAC	Electricity Sector Information Sharing and Analysis Center	www.esisac.com
Water ISAC	Water Information Sharing and Analysis Center	www.waterisac.org
独立行政法人情報処理推進機構（IPA）	独立行政法人情報処理推進機構（IPA）	www.ipa.go.jp
組織の情報セキュリティ対策自己診断テスト	独立行政法人情報処理推進機構（IPA）	www.ipa.go.jp/security/benchmark