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）

2006 年 10 月
（2008 年 3 月一部改訂）

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」（同政策会議の下の重要インフラ専門委員会（水道分野からは㈳日本水道協会石井健睿工務部長（当時）が参加）において原案とりまとめ）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。平成 18 年 2 月 2 日には「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。）が情報セキュリティ政策会議において決定され、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なった。

以上のことから、「指針」に基づいて、水道事業者が情報セキュリティ対策を行うためのガイドラインをとりまとめた。

なお、「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ことから、これを踏まえ本ガイドラインを策定したものである。

①4 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

②３つの重点項目

ア　情報システム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

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進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～Windows などの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およ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。

以上は『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)から転載した。転載にあたり意を損ねない範囲で一部改変した。

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すべ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 2006』(2006 年 6 月 15 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』(平成 18 年 6 月 15 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

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、業務への影響が大きい	・ 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）	・ 顧客情報 ・ 職員情報	・ 顧客情報 ・ 職員情報 ・ 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文書	・ その他業務で利用している文書	・ 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		・

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：不正侵入、ウィルス攻撃、サービス不能攻撃（Dos)、等

非意図的要因：操作・設定ミス、プログラム上の欠陥（バグ)、システム監査（ウィルスチェックなど）の不備、外部委託、等

災　　害：地震、水害、落雷、火災、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	備考
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	
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）	
	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	
		通信業社での障害/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	
	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利用	
		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	
		監査不十分	
		セキュリティ対策の未実施	
環境的脅威		地震	
		水害	
		落雷	
		火災	
		上記災害による停電	

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すべ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. 組織と体制の構築

2.1. 組織体制

【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うるものとする。

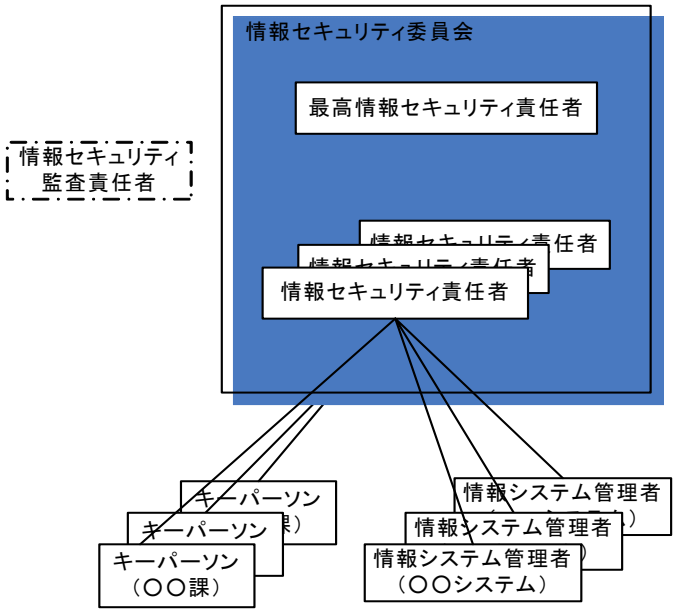

図 1　情報セキュリティの組織

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（CEPTOAR※）」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 CEPTOAR が設置されたところであり、平成 20 年 4 月よりその運用が開始される予定である。このため、水道事業者は厚生労働省のみでなく、水道 CEPTOAR とも連携を図っていくことが必要である。

※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。

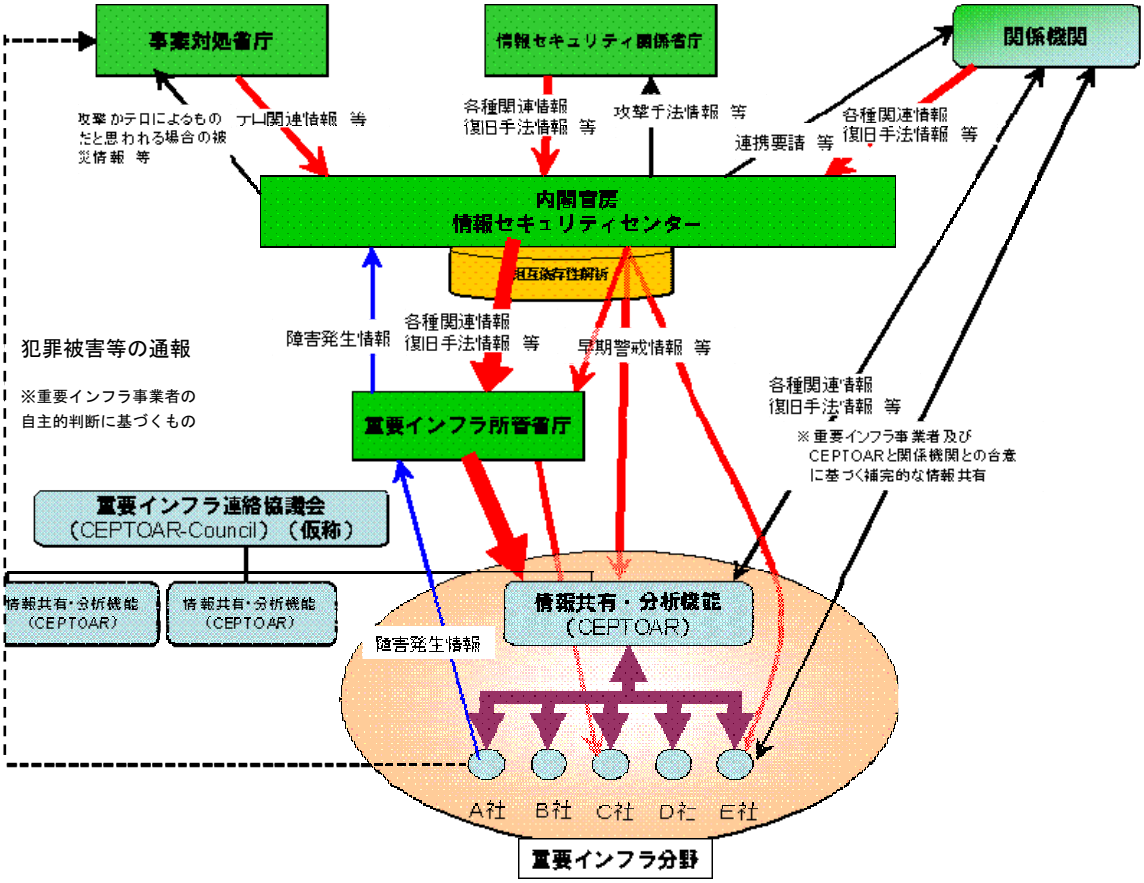

図 2　関係機関における情報共有体制（イメージ）

（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 CEPTOAR 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う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. 運用

2.2.1. 研修

【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。

【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）を実施すること。

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CEPTOAR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。

2.3. 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) 必要に応じて水道事業者外部に監査の一部を請け負わせて実施すること。
(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。

2.4. 見直し

【趣旨】

情報セキュリティ対策を取り巻く環境の変化に対応するために見直しを実施する。

【実施内容】

(1) 監査とは別に、情報セキュリティ委員会は、情報セキュリティ対策の見直しの必要性について適宜検討し、必要があると認められる場合にはその見直しを行うこと。

3. 情報についての対策

3.1. 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。

3.2. 情報の取扱い

3.2.1. 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。

3.2.2. 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。

3.2.3. 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。

3.2.4. 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。

3.2.5. 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。

3.2.6. 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。

4. 情報セキュリティ要件の明確化に基づく対策

4.1. 情報セキュリティについての機能

4.1.1. 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、すべ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の利用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。

4.1.2. 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。

4.1.3. 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、変管理手続き、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。

4.1.4. 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、すべ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。

4.1.5. 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。

4.1.6. 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。

4.1.7. 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。

4.2. 情報セキュリティについての脅威

4.2.1. 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、およ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元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。

4.2.2. 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、ならびにその他のシステムへのシステム破壊、サービス不能等に繋がる脅威となる。

【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すべ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すべ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。

4.2.3. 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。

(1) 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、および通信回線を構築すること。

(2) 装置の内、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。

(3) 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。

(4) 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。

(5) 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。

4.3. 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亘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。

5. 情報システムの構成要素についての対策

5.1. 施設と環境

5.1.1. 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しくみを構築すること。

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) 入退室の承認に当たっては、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しくみ(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。

5.2. 電子計算機

5.2.1. 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すべての電子計算機について、管理する水道事業従事者、およ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) すべ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の導入すること。
(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元で例外とされうる。
(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。

2) 電子計算機の運用時

(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すべ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。

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。

5.2.2. 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、可搬性の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臓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。

5.2.3. 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。

5.3. アプリケーションソフトウェア

5.3.1. 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に利用させてはならない。

5.3.2. 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かか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当たっては不正なスクリプト等の実行を回避するため、HTML メールの操作に当たってはこうしたリスクに留意すること。

5.3.3. 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

(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。

(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

(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。

(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。

5.4. 通信回線

5.4.1. 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) 通信回線の利用に当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、通信装置の内臓記憶装置の情報を復元困難な状態にすること。

5.4.2. 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しく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、応じて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。

5.4.3. 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) 庁舎外通信回線への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、およ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。

6. 事業継続性確保対策

6.1. 事業継続性確保のための対策

【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 X 5080)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う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。

(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。

6.2. 事業継続計画との整合性

【趣旨】

情報セキュリティに限らず、水道事業全般に亘る事業継続にかか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亘る事業継続にかか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一版－わが国企業の減災と災害対応の向上のために－　平成 17 年 8 月 1 日　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。

7. 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。

7.1. 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。

7.2. 保護すべき情報の管理

【実施内容】

(1) 保護すべき情報およ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。

7.3. 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。

7.4. 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。

7.5. 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。

8. 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。

8.1. 委託先管理のしくみ

【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。

8.2. 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・取扱い情報の需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。

8.3. 情報システム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。

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

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うる。
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。
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、なら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。
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	
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	
CEPTOAR 【せぷたあ】	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。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(CEPTOAR-Council)」(仮称)の設置が検討されている。
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 WaterISAC 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	
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

資料名	発行年	作成団体	備考
公表資料			
政府機関の情報セキュリティ対策のための統一基準	2005	情報セキュリティ政策会議	
セキュア・ジャパン 2006 -「セキュア・ジャパン」への第１歩-	2006	情報セキュリティ政策会議	
情報システムの信頼性向上に関するガイドライン	H18	経済産業省	
電力重要インフラ防護演習に関する調査報告書	2004	IPA 独立行政法人情報処理推進機構	
公共施設におけるセキュリティマネジメント技術	2006	電気学会公共施設研究会	
情報セキュリティ読本	2006	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	
情報セキュリティ対策ベンチマーク		IPA 独立行政法人情報処理推進機構	
情報システム安全対策基準	H7、 H9	通商産業省	
OECD 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）	1992、 2002	OECD 経済産業省	http://www.meti.go.jp/policy/netsecurity/oecd2002.htm
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	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 http://www.bits.go.jp/inquiry/
事業継続ガイドライン第一版－わが国企業の減災と災害対応の向上のために－	H17	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	H17	経済産業省	
JIS、および関連資料			
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 15001:1999 個人情報保護に関するコンプライアンス・プログラムの要求事項	H11	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)	H12	日本工業標準調査会 日本規格協会	

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			
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 X 5080:2002 (ISO/IEC 17799:2000) 情報技術－情報セキュリティマネジメントの実践のための規範	H14	日本工業標準調査会 日本規格協会	
JIS X 5080:2002　情報セキュリティマネジメントガイド	2002	日本規格協会	
情報セキュリティ対策マネジメント標準(JIS X 5080:ISO/IEC 17799)の解説	H14	電子商取引推進協議会セキュリティ WG	
ウェブサイト			
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)	http://www.nisc.go.jp/index.html
情報セキュリティに関する政策、緊急情報		経済産業省	http://www.meti.go.jp/policy/netsecurity/index.html
NERC		North American Electric Reliability Council	http://www.nerc.com/
ESISAC		Electricity Sector Information Sharing and Analysis Center	http://www.esisac.com/
WaterISAC		Water Information Sharing and Analysis Center	http://www.waterisac.org/
独立行政法人情報処理推進機構　セキュリティセンター		IPA 独立行政法人情報処理推進機構	http://www.ipa.go.jp/security/index.html
情報セキュリティ対策ベンチマーク　セルフチェック		IPA 独立行政法人情報処理推進機構	https://isec.ipa.go.jp/benchmark-new/member/