米子市上下水道局審議会等
情報セキュリティポリシー

米子市上下水道局

令 和 ８ 年 ４ 月 １ 日　策定

基本方針

１　目的

米子市上下水道局（以下「上下水道局」という。）が法律及び条令に基づき設置する審議会等（以下「審議会等」という。）の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、外部に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び当該情報を取り扱う情報システムを様々な脅威から保護することは、住民の財産及びプライバシー等を守るために不可欠であり、また、行政事務の安定的な運営を確保し、上下水道局に対する住民の信頼の維持向上に資するものである。

また、近年のデジタル技術の進展により、デジタル社会に対応したデジタル・ガバメントの実現が期待されているところである。上下水道局がこれらに積極的な対応をするためには、管理しているすべての情報システムが高度な安全性を有することが不可欠な前提条件である。

このため、本審議会等の情報資産の機密性、完全性及び可用性を維持するための対策(以下「情報セキュリティ対策」という。)を講じるため、米子市上下水道局審議会等情報セキュリティポリシー（以下、「情報セキュリティポリシー」という。）を策定し、本審議会等における情報セキュリティ対策の基本的な方針（以下、「基本方針」という。）として、情報セキュリティ対策の対象、位置付け等を定めるとともに、地方自治法第 244 条の６第１項に規定するサイバーセキュリティを確保するための方針に位置づける。

２　定義

(1)　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

(2)　情報システム

コンピュータ（ハードウェア及びソフトウェア)、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3)　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4)　情報セキュリティポリシー

本基本方針をいう。

(5)　機密性

情報にアクセスすることを認められた者のみが当該情報にアクセスできる状態を確保することをいう

(6)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7)　可用性

　情報にアクセスすることを認められた者が、必要なときに中断されることなく情報にアクセスできる状態を確保することをいう。

3　対象とする脅威

情報資産に対する脅威として、以下のものを想定する。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2)　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

(1)　適用機関の範囲

　本基本方針が適用される対象は、審議会等の各委員（以下、「各委員」という。）及び審議会等の情報資産を取り扱うすべての者とする。

(2)　情報資産の範囲

　本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

5　各委員の遵守義務

　各委員は、情報セキュリティの重要性について共通の認識を持ち、業務等の遂行に当たって本基本方針を遵守しなければならない。

6　情報セキュリティ対策

　本審議会等は、上記３の脅威から情報資産を保護するために、必要に応じて以下の情報セキュリティ対策を講じる。

(1)　組織体制

　本審議会等の情報資産について、情報セキュリティ対策を推進する組織体制を確立

する。

(2)　情報資産の分類と管理

審議会等の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を講じる。

(3)　物理的セキュリティ

情報システム及び関連施設への入退室管理、機器管理等の物理的な対策を実施する。

(4)　人的セキュリティ

情報セキュリティ教育及び研修実施するとともに、各委員が遵守すべき事項を明確化するとともに、

(5)　技術的セキュリティ

情報システムの管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6)　運用管理

情報システムの監視、本基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、本基本方針の運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(7)　業務委託及び外部サービスの利用

業務委託及びクラウドサービス等の外部サービスを利用する場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

７　情報セキュリティ監査等の実施

本基本方針の遵守状況及び情報セキュリティ対策の実効性を確認するため、必要に応じて情報セキュリティ監査又は自己点検を実施する。

８　継続的改善

情報セキュリティ対策について、計画（Plan）、実施（Do）、評価（Check）、改善（Action）のPDCAサイクルによる継続的な改善を図る。

９　本基本方針の見直し

情報セキュリティ監査の結果、本基本方針の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、本基本方針を適宜見直すものとする。