鳥取県西部広域行政管理組合
情報セキュリティポリシー

令和８年４月

鳥取県西部広域行政管理組合

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、鳥取県西部広域行政管理組合（以下「本組合」という。）が所管する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。

情報セキュリティポリシーは、本組合の全職員（会計年度任用職員を含む。以下「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら、一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた「情報セキュリティ基本方針」と情報資産を取り巻く状況の変化に依存する部分「情報セキュリティ対策基準」に分けて策定することとした。

また、情報システムごとに具体的な情報セキュリティ対策を行う必要があることから、情報システムを所管する所属において、必要に応じ情報セキュリティポリシーに基づく実施手順（以下「情報セキュリティ実施手順」という。）を策定することとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は公表することにより本組合の情報セキュリティの確保に支障を及ぼすおそれがあるため、非公表とする。

＜情報セキュリティポリシーの構成＞

文　書　名		内　　容	適用範囲
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針	本組合の事務局・消防局、会計室、監査委員、監査委員の事務を補助する書記長・書記長補佐・書記、議会に置く書記長・書記
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準	本組合の事務局・消防局、会計室、監査委員の事務を補助する書記長・書記長補佐・書記、議会に置く書記長・書記

第１章　情報セキュリティ基本方針

１　目的

本組合が取り扱う情報は、個人情報のみならず行政運営上重要な情報を含んでおり、複雑化、高度化する情報社会においては、情報資産の安全性を確保することが重要となっている。

そのため、本組合の所管する情報資産の機密性、完全性及び可用性（注）を確保するための対策を整備するため、鳥取県西部広域行政管理組合情報セキュリティポリシーを定めることとする。

このうち、情報セキュリティ基本方針（以下「本基本方針」という。）においては、本組合の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象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ものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

機密性（confidentiality）	：情報にアクセスすることを認可された者だけがアクセスできることを確実にすること。
完全性（integrity）	：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性（availability）	：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

⑴　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。

⑵　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　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。

⑷　認定審査事務系

認定審査事務に関わる情報システム及びその情報システムで取り扱うデータをいう。

⑸　消防指令系

消防局における高機能消防指令センター及び救急デジタル無線システム並びにこれらのシステムで取り扱うデータをいう。

⑹　インターネット接続系

インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

3　適用範囲

⑴　行政機関の範囲

本情報セキュリティ基本方針が適用される行政機関の範囲は、本組合の事務局・消防局、会計室、監査委員、監査委員の事務を補助する書記長・書記長補佐・書記、議会に置く書記長・書記とする。

⑵　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

4　遵守義務

本基本方針が適用されるすべての行政機関は、情報セキュリティの重要性について共通の認識を持つとともに、当該業務の遂行に当って本基本方針を遵守する義務を負うものとする。

5　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定する。

⑴　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、重要情報の搾取、内部不正等

⑵　情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、委託管理の不備、マネジメントの欠陥、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

⑶　災害等による業務の停止等

⑷　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

⑸　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

6　情報セキュリティ対策

本組合の情報資産を上記５で示した脅威から守るため、必要に応じて次のセキュリティ対策を講ずるものとする。

⑴　組織体制

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。

⑵　情報資産の管理と分類

情報資産の内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　認定審査事務系においては、原則として、他の領域との通信をできないようにし、認定審査事務に係る個人情報の流出を防ぐ。

イ　消防指令系においては、インターネット接続系の情報システムとの通信経路を論理的に分離する。なお、両システム間で通信が必要な場合には、必要な通信だけを許可するよう設定する。

ウ　インターネット接続系においては、不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

⑷　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損害及び利用の妨害等から保護するための物理的な対策を講ずる。

⑸　人的セキュリティ対策

情報セキュリティにし、職員等、各委員及び各議員等が遵守すべき事項を定めるとともに、十分な教育・啓発が行われるよう必要な対策を講ずる。

⑹　技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的対策を講ずる。

⑺　運用等におけるセキュリティ対策

情報システムの監視、情報セキュリティ対策の遵守状況の確認等、運用面の対策を講ずる。

⑻　業務委託と外部サービスの利用

業務委託を行う場合には、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く措置を講じる。

7　情報セキュリティ対策基準の策定

上記６の情報セキュリティ対策を実施するに当たり、遵守すべき事項や、判断等の統一的な基準（以下「情報セキュリティ対策基準」という。）を必要に応じ定めるものとする。

8　情報セキュリティ実施手順の策定

情報セキュリティ対策基準の基本的な用件に基づき、情報セキュリティ対策を具体的に実施するための情報セキュリティ実施手順を、必要に応じ定めるものとする。

9　緊急時等の対応

情報システムに関連する事故、欠陥等への対策、情報資産の漏えい等が発生した場合の対応など、緊急事態が発生した場合に、迅速かつ適切な対応を図るため、緊急時等の対応方法を定めるものとする。

10　評価及び見直し

情報セキュリティポリシーに定める情報セキュリティ対策について評価を実施するとともに、情報システムの変更、情報セキュリティを取り巻く状況の変化等を踏まえ、必要に応じて見直しを実施するものとする。