泉佐野市田尻町清掃施設組合

情報セキュリティポリシー

第１版　施行日　令和８年４月１日

総務大臣指針に基づく

第１章　泉佐野市田尻町清掃施設組合情報セキュリティポリシーの構成等

1.　策定根拠

泉佐野市田尻町清掃施設組合(以下「組合」という。)の情報セキュリティポリシー(以下「本ポリシー」という。)は、次の法律(以下「関係法」という。)の規定に基づき、総務大臣が示した指針を参照して策定するものである。

○　サイバーセキュリティ基本法(平成 26 年法律第 104 号)　抜粋

(定義)

第２条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式(以下この条において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体(以下「電磁的記録媒体」という。)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていることをいう。

(地方公共団体の責務)

第５条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

○　地方自治法(昭和 22 年法律第 67 号)　抜粋

(情報システムの利用に係る基本原則)

第 244 条の５　略

２　普通地方公共団体は、その事務の処理に係る情報システムの利用に当たって、サイバーセキュリティ(サイバーセキュリティ基本法第 2 条に規定するサイバーセキュリティをいう。次条第 1 項において同じ。)の確保、個人情報の保護その他の当該情報システムの適正な利用を図るために必要な措置を講じなければならない。

(サイバーセキュリティを確保するための方針等)

第 244 条の６　普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たってのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。

２　普通地方公共団体の議会及び長その他の執行機関は、前項の方針を定め、又はこれを変更したときは、遅滞なく、これを公表しなければならない。

３　総務大臣は、普通地方公共団体に対し、第１項の方針(政令で定める執行機関が定めるものを除く。)の策定又は変更について、指針を示すとともに、必要な助言を行うものとする。

４　［略］

○　個人情報の保護に関する法律(平成 15 年法律第 57 号)　抜粋

(安全管理措置)
第 66 条　行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。
2　前項の規定は、次の各号に掲げる者が当該各号に定める業務を行う場合における個人情報の取扱いについて準用する。
⑴　行政機関等から個人情報の取扱いの委託を受けた者　当該委託を受けた業務
⑵～⑷　［略］
⑸　前各号に掲げる者から当該各号に定める業務の委託(2 以上の段階にわたる委託を含む。)を受けた者　当該委託を受けた業務

2.　構成

本ポリシーは、この章及び次の 2 章で構成する。

第 2 章　情報セキュリティ基本方針
地方自治法第 244 条の 6 第 1 項の規定に基づき、情報セキュリティ(サイバーセキュリティを包含する概念)の確保、個人情報の保護その他当該情報システムの適正利用に関する基本的な方針を定めたもの。

第 3 章　情報セキュリティ対策基準
「情報セキュリティ基本方針」に基づき、情報セキュリティ対策(保有個人情報の安全管理措置を含む。以下同じ。)に関する具体的な内容を定めたもの。

また、本ポリシーとは別に、「情報セキュリティ対策基準」に基づき、個々の情報システムに関する具体的な実施手順を示した「情報セキュリティ実施手順」を整備するものとする。

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、公にすることにより組合の運営に重大な支障を及ぼすおそれがあることから、非公表とする。

3.　適用範囲

⑴　適用機関

本ポリシーは、組合の議会、管理者、監査委員及び公平委員会(以下「実施機関」という。)に適用する。

⑵　情報資産の範囲

本ポリシーが対象とする情報資産(以下「情報資産」という。)は、次のとおりとする。

①　実施機関が保有する情報(これらの印刷物を含む。)
②　①の情報を取り扱うネットワーク及び情報システム
③　②に関する仕様書又は設計書､図面その他の関連文書等(以下｢情報システム関連文書等」という。)

4. 職員の遵守義務

実施機関の職員(以下「職員」という。)は、業務の遂行に当たっては、次の法律等の関係規定のほか、本ポリシー及び「情報セキュリティ実施手順」を遵守する義務を負う。

○ 地方公務員法(昭和 25 年法律第 261 号)

○ 著作権法(昭和 45 年法律第 48 号)

○ 不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)

○ 泉佐野市田尻町清掃施設組合議会の個人情報の保護に関する条例(令和 5 年泉佐野市田尻町清掃施設組合条例第 2 号)

○ 泉佐野市田尻町清掃施設組合文書管理規程(昭和 40 年泉佐野市田尻町清掃施設組合訓令第 2 号)

5. 用語の定義

本ポリシーで使用する用語の意義は、関係法の例によるほか、次のとおりとする。

⑴ 文書等

文書、図面及び電磁的記録(電磁的方式で作られた記録)をいう。

⑵ 情報

職員が職務上作成し、又は取得した文書等であって、当該職員が組織的に用いるものとして、実施機関が保有しているものをいう。

⑶ 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とその構成機器(ハードウェア及びソフトウェア)をいう。

⑷ 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体その他の周辺機器で構成されるものであって、これらの全部又は一部で情報処理を行う仕組みをいう。

⑸ 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当該情報システムで取り扱う情報をいう。

⑹ 内部接続系

実施機関内部の情報システム及び当該情報システムで取り扱う情報をいう。

⑺ 情報セキュリティ

情報の機密性(情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。)、完全性(情報が破壊又は改ざん若しくは消去されていない状態を確保することをいう。)及び可用性(情報にアクセスすることを認められた者だけが、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。)を維持することをいう。

⑻ 非公開情報

泉佐野市田尻町清掃施設組合情報公開条例(令和 7 年泉佐野市田尻町清掃施設組合条例第 2 号)第 7 条に規定する非公開情報をいう。

第2章　情報セキュリティ基本方針

1.　対象とする脅威

情報セキュリティに関する事故又は攻撃であって、実施機関の業務運営や情報セキュリティを脅かす可能性が高いもの(以下「インシデント」という。)として、次のものを対象とする。

⑴　内部インシデント(職員の意図的又は非意図的行為によるもの)

①　電子メールの誤送信や添付又は送信に係る設定の過誤よる情報の漏えい

②　アクセス権限を有する職員による情報の消去又は改ざん

③　ログイン ID・パスワードの使い回し又は管理の不備による不正アクセス

④　許可のないアプリケーション、ハードウェア及びソフトウェアの使用による情報の漏えい、マルウェア(不正かつ有害に動作させる意図で作成されたソフトウェア等の総称。)感染

⑤　非公開情報が含まれた情報資産の紛失、盗難

⑥　情報システム等の欠陥、業務委託先の管理・監督不備

⑦　①から⑥のほか、本ポリシー又は「情報セキュリティ実施手順」遵守義務違反、内部不正

⑵　外部インシデント(悪意のある第三者の行為によるもの)

①　標的型攻撃によるマルウェア感染

②　ランサムウェアによる身代金要求

③　不正ログインによる乗っ取り又はなりすまし

④　サービス不能攻撃によるサービスの停止

⑤　情報資産の持出しを目的とした不正侵入

⑶　その他のインシデント(非常災害又は事故等に起因するもの)

①　設備・機器等の物理的損壊、故障

②　利用する外部サーバや外部サービスの障害、停止及びそれに伴うデータの損失

③　電力供給、通信の途絶に伴う情報システムの停止

2.　情報セキュリティ対策

上記 1 の脅威から情報資産を保護するため、次の情報セキュリティ対策を講じる。

なお、個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法第 26 条第 1 項第 2 号に規定するサイバーセキュリティに関する対策の基準に基づき、取り扱う保有個人情報の内容に照らして適正なサイバーセキュリティの水準を確保するものとする。

⑴　組織体制

情報セキュリティ対策を推進する組織体制、権限及び責任を定める。

⑵　情報資産の分類と管理

情報の秘匿性等(個人識別の容易性、匿名化の程度及び要配慮個人情報の有無並びに漏えい等(漏えい、滅失又は毀損をいう。以下同じ。)が発生した場合に生じ得る被害の性質及び程度をいう。以下同じ。)の観点から情報資産を分類し、当該分類に応じた対策を講じる。

⑶　保有個人情報その他の非公開情報の安全管理措置

保有個人情報その他の非公開情報に係る情報資産に関しては、当該情報の秘匿性等に応じて、必要な安全管理措置を講じる。

⑷　情報システム全体の安全性及び信頼性の確保

インターネット接続系における監視機能及び無害化(コンピュータウイルス等の付着がない安全が確保された状態にすることをいう。以下同じ。)機能の実効性を保持することにより、内部接続系を含む情報システム全体の安全性及び信頼性を確保する。

⑸　物理的セキュリティ

情報資産の適正な管理のために必要な物理的対策を講じる。

⑹　人的セキュリティ

情報セキュリティ対策に係る職員の遵守事項を定め、これを周知するほか、必要に応じて、研修を実施するものとする。

⑺　技術的セキュリティ

コンピュータ等の管理、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な対策を講じる。

⑻　インシデントへの対応

インシデントの発生時に迅速かつ適切に対応するため、あらかじめその報告窓口と報告を受けた後の対処手順等を定める。

⑼　個人情報関連業務の委託

保有個人情報を取り扱う情報システム等の導入、運用及び保守等に関する業務を外部に委託するに当たっては、当該個人情報の安全管理を主眼に置いた業者選定基準を定めるものとする。

また、仕様書及び契約書に当該業務に係る情報セキュリティ要件その他必要事項を明記した上で、その履行状況を適時適切に確認するとともに、契約違反行為を確認したときは、契約に基づく措置を講じるものとする。

3.　監査及び自己点検の実施

本ポリシーの遵守状況を検証するため、必要に応じて、監査及び自己点検を実施する。

4.　本ポリシーの見直し

監査及び自己点検の結果等を踏まえて本ポリシーの実効性を評価し、必要に応じて、本ポリシーの見直しその他の措置を講じるものとする。