岸和田市貝塚市清掃施設組合情報セキュリティポリシー

第 5 版

令和６年６月

岸和田市貝塚市清掃施設組合

はじめに

■　情報セキュリティとは

情報セキュリティとは、本組合が保有する情報資産の機密性、完全性、可用性を維持することをいう。

① 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。

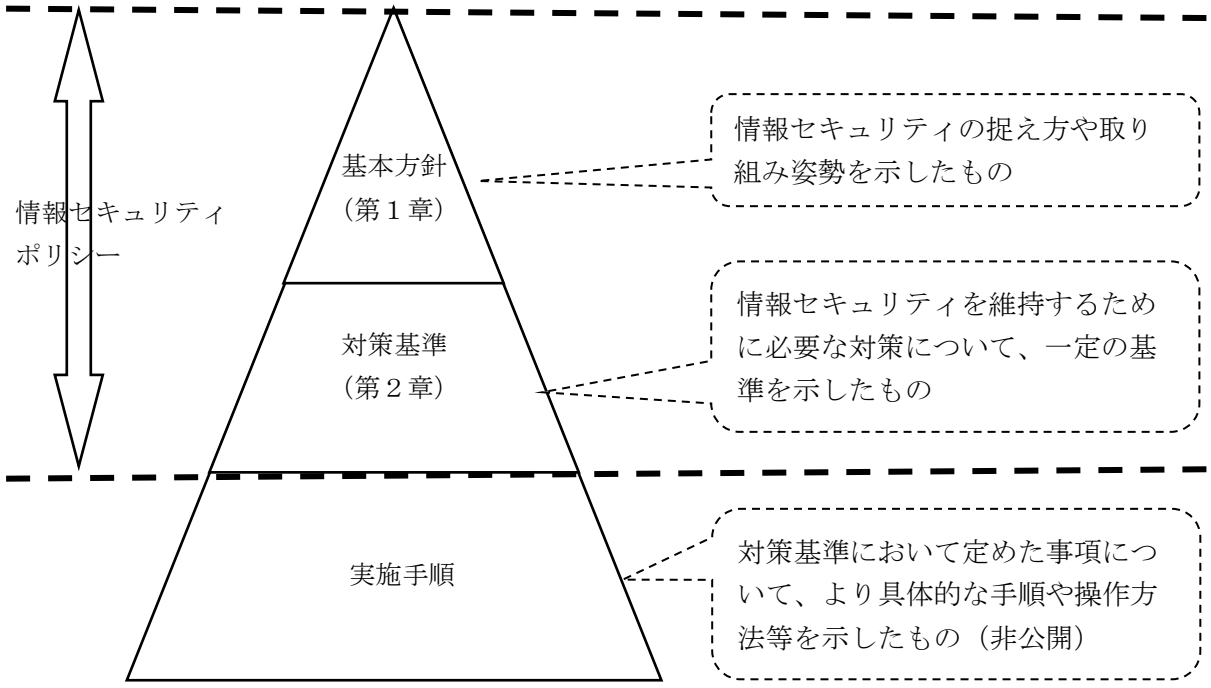
② 完全性
情報が常に完全かつ安全に維持され、改ざんや破壊等がされないようにすること。

③ 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。

■　構成

情報セキュリティを適正に維持するための方策について、本組合ではそれを３階層による構成としている。そのうち、上位の２階層（基本方針、対策基準）を情報セキュリティポリシーと定め、ここに取りまとめる。【下図参照】

【構成イメージ図】



目次

第１章　情報セキュリティ基本方針 1

１．目的 1
２．位置づけ 1
３．定義 1
４．対象範囲 2
５．対象範囲外への対応 2
６．情報セキュリティポリシー及び関連法令等の遵守 2
７．情報資産に対する脅威 3
８．運用体制 3
９．情報資産の分類 3
10．対策 3
11．情報セキュリティ対策基準の策定 4
12．情報セキュリティ実施手順の策定 4
13．セキュリティ対策の点検と情報セキュリティポリシーの見直し 4

第２章　情報セキュリティ対策基準 5

１．組織及び体制 5
２．情報資産の分類及び管理 8
３．物理的セキュリティ対策 9
４．人的セキュリティ対策 10
５．技術的セキュリティ対策 11
６．情報システムの開発及び運用・保守 14
７．外部サービスの利用 15
８．重要度Ｂ以上の情報を扱う外部サービスの利用 15
９．緊急時の対応 16
10．適合性 17

第１章　情報セキュリティ基本方針

１．目的

岸和田市及び貝塚市の市民の財産、プライバシー等の保護及び岸和田市貝塚市清掃施設組合（以下「組合」という。）の安定的な運営を図ることを目的として岸和田市貝塚市清掃施設組合情報セキュリティ基本方針（以下「本基本方針」という。）を制定する。

２．位置づけ

本基本方針は、組合の保有する情報資産についての情報セキュリティ対策を、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策を実施するうえでの基本的な事項を定めたものである。

３．定義

本基本方針及び情報セキュリティ実施手順にて使用する用語の定義は、以下のとおりとする。

①　ネットワーク
　コンピュータ等を通信回線で接続することにより、一体として情報の処理を行う情報通信網、その構成機器をいう。

②　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　情報セキュリティポリシー
　本基本方針及び情報セキュリティ対策基準をいう。

④　個人情報
　個人情報の保護に関する法律（平成15年法律第57号）第２条第１項に規定する個人情報をいう。

⑤　特定個人情報
　行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)第２条第８項に規定する特定個人情報をいう。

⑥　情報セキュリティインシデント
　望まない単独若しくは一連の情報セキュリティ事象、予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

４．対象範囲

（１）組織の範囲

①　組合の内部の組織（実施機関）

管理者、公平委員会、監査委員及び議会

②　組合の外部の組織

組合の保有する情報資産を取扱う外部委託事業者等（当該受託業務に限る。）

（２）人の範囲

上記（１）①に掲げる実施機関の指揮監督権に服する全ての職員（一般職もしくは特別職、常勤もしくは非常勤の地方公務員をいう。ただし組合議会議員は除く。）及び②の組織の従業者であって本組合の情報資産の取扱いに従事している者（以下「職員等」という。）

（３）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。

①　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②　ネットワーク、情報システムで取り扱う情報

③　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　情報資産の範囲には、各種申請書等の紙情報を原則含まないが、情報システムから紙等の有体物に出力された情報や、業務上の理由により情報資産の所管部署から持ち出される入力帳票については、対象範囲内とする。

５．対象範囲外への対応

本基本方針の対象範囲外とした紙情報についても、本基本方針の趣旨を尊重しつつ、これまでと同様、当該文書の取扱いを定めた関連法令等に基づいて、引続き適正な取扱いに努めるものとする。

６．情報セキュリティポリシー及び関連法令等の遵守

（１）職員の責務

①　職員は、情報セキュリティの重要性を認識し、業務の遂行にあたっては、情報セキュリティポリシーを遵守する義務を負う。また、情報資産の利用や保管等を行う際は、個人情報の保護に関する法律（平成15年法律第57号）等関連する法令等を遵守しなければならない。

②　情報セキュリティポリシーに違反した職員は、生じた結果の重大性及び違反の悪質性等の状況に応じて、地方公務員法等に基づき懲戒処分等の対象になることがある。

（２）外部委託事業者等への対応

外部委託事業者等に対しても、情報セキュリティの重要性を認知させ、契約書等において情報セキュリティポリシーの遵守事項及び違反した場合の責任について明確にするものとする。

７．情報資産に対する脅威

（１）情報資産に対する主な脅威として以下の脅威を想定し、情報セキュリティ対策を実施する。

・不正アクセス、コンピュータウイルス等不正プログラム攻撃、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洩、破壊、盗聴、改ざん、消去、情報の搾取、無断持ち出し、内部不正等

・無許可ソフトウェアの使用、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、機器故障等の非意図的要因による情報資産の漏洩、破壊、消去等

・搬送中の事故等による情報資産の盗難、紛失等

・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

・事故、機器故障等によるサービス及び業務の停止

・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

（２）職員等は、上記（１）の脅威に対し認識を深めるとともに、これら以外の脅威についても注意を払わなければならない。

８．運用体制

情報セキュリティ対策の推進、情報セキュリティへの侵害（以下「セキュリティ侵害」という。）に対する迅速な対応を図るための本組合の運用体制を確立するものとする。

なお、セキュリティ侵害とは、「７.情報資産に対する脅威」に記述するような脅威が発生した状態をいう。

９．情報資産の分類

情報資産を内容に応じて分類し、その重要度に即した対策を講じるものとする。

10．対策

「７.情報資産に対する脅威」で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じるものとする。

① 物理的対策

情報システムを設置する施設への不正な立ち入りや、自然災害により起こる破壊、盗難等から情報資産を保護するために行う入退室管理等の物理的な対策

② 人的対策

情報資産を取り扱う職員等の情報セキュリティに関する権限や責任・運用体制の明確化、情報セキュリティポリシーの内容を周知徹底するために行う教育・訓練等の人的な対策

③ 技術的対策

情報資産を不正なアクセス等から適正に保護するための情報資産へのアクセス制限、コンピュータウイルス等不正プログラムからの脅威への対策等の技術的な対策

11. 情報セキュリティ対策基準の策定

「10.対策」で示した対策を講じるにあたって、職員等が遵守すべき事項や判断の基準等を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を実施する上で必要となる一定の基準を示した、情報セキュリティ対策基準を策定するものとする。

12. 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を確実に実施していくためには、個々の情報資産に関する具体的な対策の方法や手順を定めておく必要がある。そのため、情報セキュリティ対策基準に基づく実施マニュアルとして、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、具体的な対策の手順やノウハウについて記述するものであり、公開することにより行政運営に重大な支障を及ぼすおそれがあるため、非公開とする。

13. セキュリティ対策の点検と情報セキュリティポリシーの見直し

日々の情報セキュリティに対する脅威に対応するため、情報セキュリティポリシーに定める事項及び実施手順に基づく具体的対策の実施状況を定期的又は必要に応じて点検する。

また、情報セキュリティポリシーの内容についても必要に応じて見直し、本組合におけるセキュリティレベルの向上を図るものとする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針（第１章）に沿った個々の対策を具体化したものであり、本組合における情報セキュリティ対策の基準となるものである。

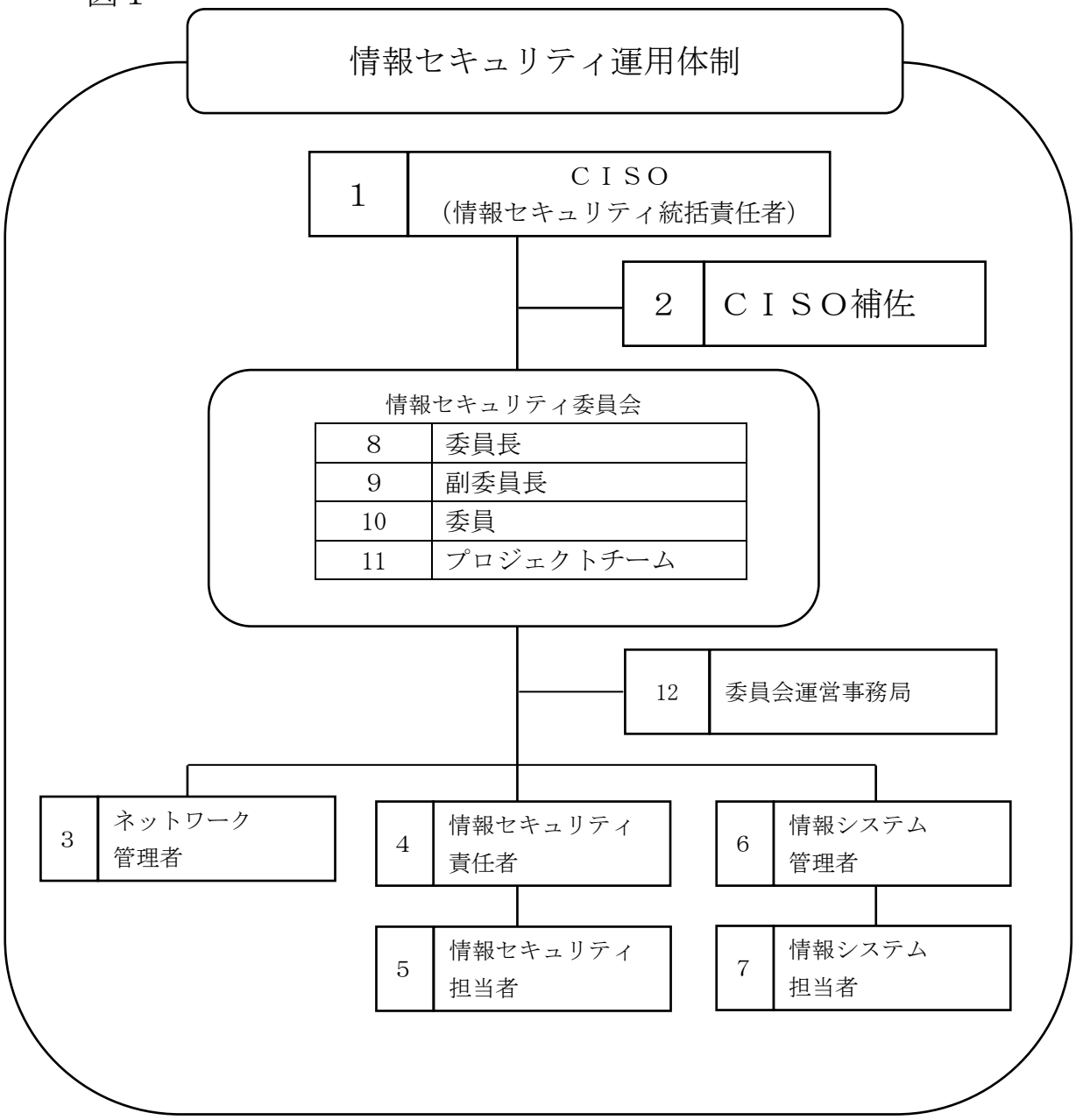
１．組織及び体制

（１）運用体制

情報セキュリティ対策の推進及び情報セキュリティインシデントへの迅速な対応等を行うため、図１に示す運用体制を確立する。

また、必要に応じて外部の有識者に助言を求めることができるものとする。

図１



（2）情報セキュリティ運用関係者の役割

情報セキュリティ運用体制の中でのそれぞれの役割、責任及び権限の範囲等を明確にするため、役割等一覧を表１に示す。

表１　情報セキュリティ対策運用体制役割等一覧　　※項番は、図１中の番号に対応

項番	名称	役職	主な役割等
1	ＣＩＳＯ（情報セキュリティ統括責任者）	事務局長	○情報セキュリティに関する全ての責任と権限を有する。 ○情報セキュリティ委員会の委員長を務め、必要に応じて委員を招集し、委員会を開催する。 ○セキュリティ侵害発生時（発生の可能性が高い場合も含む）には、侵害内容や状況等の報告を受け、対策等を指示する。
2	ＣＩＳＯ補佐	事務局次長	○情報システムの開発、運用、更新等の際、セキュリティ技術の面からＣＩＳＯを補佐する。 ○必要に応じて、情報セキュリティ委員会へ助言を行う。 ○ＣＩＳＯと協議の上、情報セキュリティ責任者及び担当者、情報システム管理者及び担当者に対し、情報セキュリティに関する指導、助言を行うことができる。 ○情報セキュリティ実施手順の維持、管理を行う。 ○セキュリティ侵害発生時には、ＣＩＳＯの指示に従って必要な措置を行う責任と権限を有する。この場合、職員等はＣＩＳＯ補佐の指示に従わなければならない。
3	ネットワーク管理者	総務課長	○本組合ネットワークの情報セキュリティに関する責任と権限を有する。
4	情報セキュリティ責任者	各課長	○所属内の情報セキュリティに関する責任と権限を有し、所属内において、情報セキュリティ対策の指導や情報セキュリティポリシーの普及及び遵守の徹底を図る。 ○所管する情報資産について、情報資産管理台帳及び情報セキュリティ実施手順の作成、管理を行う。 ○セキュリティ侵害発生時には、情報セキュリティ委員会に侵害内容や状況等を報告し、所属内に対処を指示する。
5	情報セキュリティ担当者	情報セキュリティ責任者が指名した者	○情報セキュリティ責任者の指示の下、所属内の情報セキュリティ対策を実施する。 ○セキュリティ侵害発生時には、情報システム管理者と協力し、速やかに情報セキュリティ責任者へ侵害内容や状況等の報告を行い、責任者の指示の下、適切な対処を行う。
6	情報システム管理者	各課長	○所管している情報システムのセキュリティ対策について全てを管理する責任と権限を有する。 ○所管している情報システムの情報セキュリティ実施手順を作成し、当該情報システム利用課の情報セキュリティ責任者へ提供する。
7	情報システム担当者	情報システム管理者が指名した者	○担当する情報システムに関して、情報システム管理者の指示に従い、開発、運用、更新等の作業を行う。

（3）セキュリティ統括組織

岸和田市貝塚市清掃施設組合情報セキュリティ委員会（以下「委員会」という。）が、本組合の情報セキュリティについて、統括的な管理を行う。委員会の中でのそれぞれの役割、責任及び権限の範囲等を明確にするため、委員会の役割等一覧を表２に示す。

【委員会の所掌事務】

① 本組合の情報セキュリティに関する重要事項についての協議及び決定に関すること。
② 岸和田市貝塚市清掃施設組合情報セキュリティポリシーの制定及び改正、運用、普及並びに教育に関すること。
③ セキュリティ侵害についての情報収集及び侵害発生の予防に関すること。
④ セキュリティ侵害時の対応に関すること。
⑤ 情報セキュリティポリシーとの適合性点検の実施及びその結果を基に行う改善策の協議に関すること。

表２　委員会役割等一覧　　※項番は、図１中の番号に対応

項番	名称	役職	主な役割等
8	委員長	事務局長	○委員会を統括する。
9	副委員長	事務局次長	○委員長を補佐し、委員長に事故があるときは、その職務を代理する。
10	委員	各課長	○運営事務局と連携し、委員会に付議する事項についての調整等を行う。 ○緊急を要するセキュリティ侵害の発生時には、委員長と対応策等についての協議を行う。 ○情報セキュリティに関する重要事項について協議する。 ○セキュリティ侵害及びセキュリティに関する点検の結果に対する改善策を協議する。 ○セキュリティ侵害発生時には、必要に応じて、委員長と対応策等についての協議を行う。
11	プロジェクトチーム	委員長が指名した者	○必要に応じて委員会の指示の下設置され、情報セキュリティポリシーを維持するための改訂等を行う。
12	委員会運営事務局	総務課	○情報セキュリティポリシーの運用、普及及び教育を推進する。 ○委員会の決定事項を推進する。 ○セキュリティ侵害に関する情報を収集し、必要に応じて委員会へ報告する。

２．情報資産の分類及び管理

（１）情報の重要度による分類

情報セキュリティ責任者は、各々が所管する情報資産について適正な取扱いを図るため、情報の重要度により表３に示す分類を行うものとする。

表３　情報の分類

重要度	分類	情報の内容
A	個人情報	○個人に関する情報であって、特定の個人を識別し得る情報
B	行政情報（重要）	○セキュリティ侵害が行政事務の執行に支障を及ぼす情報 例）重要度Ｃを除く行政情報
C	行政情報（軽易）	○セキュリティ侵害が行政事務の執行に軽微な支障を及ぼす情報 例）誰でも利用可能な情報であり、既に公開済みの情報

（２）情報資産管理台帳の作成

情報セキュリティ責任者は、所属内における情報資産の管理を円滑に行うため、各情報システムに関連づけた目録を作成しなければならない。

なお、情報資産管理台帳の記載内容については、必要に応じて更新を行うものとする。

（３）情報資産の管理

情報セキュリティ責任者は、所属内における情報資産について、（１）の重要度に応じた適切な対策を講じることにより管理しなければならない。

なお、具体的な対策については、後述の物理的対策、人的対策、技術的対策、システム開発・運用・保守、緊急時対応計画が記述された実施手順書を作成しなければならない。

３．物理的セキュリティ対策

（１）セキュリティ区画の分類

情報セキュリティを確保するために、その情報資産が使用・保管できる空間を限定し、管理水準を定め、表４に示すセキュリティ区画を設定する。

表４　セキュリティ区画

区画の区分	区画の管理水準（例示）	情報資産の例	
		使用	保管
L4	常時施錠され、厳重な入退室管理、室内での作業管理、その他厳重な管理空間 （例示） サーバー室、使用時以外施錠しているサーバーラック	サーバー等	サーバー等
L3	常時施錠され、管理者の明示の許可を受けた少数の者だけがアクセスできる空間 （例示） 使用時以外施錠しているロッカー・ラック、施錠された机の引出し	該当なし	重要度Ａの情報を保存したパソコン・媒体 サーバーをリモート操作することができる機器
L2	在室者の監視下で、管理者の明示の許可を得て入退室する空間 （例示） 事務室、時間外に施錠している事務室	重要度Ａの情報を保存したパソコン・媒体 サーバーをリモート操作することができる機器 重要度Ａの情報にアクセスできる機器	重要度Ｂの情報を保存したパソコン・媒体 重要度Ａの情報にアクセスできる機器
L1	在室者の監視下で、不特定の人が入退室する空間 （例示） 事務室、時間外に施錠していない事務室	重要度Ｂ・Ｃの情報を保存したパソコン・媒体 重要度Ｂ・Ｃの情報にアクセスできる機器	重要度Ｃの情報を保存したパソコン・媒体 重要度Ｂ・Ｃの情報にアクセスできる機器
L0	不特定の人が比較的自由に出入りする空間 （例示） ロビー、廊下等、カウンターの外側	該当なし	該当なし

＊　複数の重要度にわたる情報を保存しているときは、上位の重要度を適用すること。
＊　重要な情報については、暗号化等の対策をとることが望ましい。
＊　区画Ｌ２の事務室について、時間外施錠されないところは時間外のみ区画Ｌ１とする。
＊　盗難防止用チェーン等で対策されたパソコン等は、区画Ｌ２に相当するものとする。

（２）区画図

情報セキュリティ責任者は、表４で定めた区画の区分に従い、所管の事務室等の区画図を作成しなければならない。

（３）情報資産以外の管理

情報セキュリティ責任者は、紙情報などの管理についても、セキュリティ区画の分類による保管に努めなければならない。

（４）サーバーの設置

① 情報システム管理者及びネットワーク管理者は、サーバーを設置する場合は火災、水害、落雷、磁界、振動等の影響を受けにくい場所に設置すること。

② 情報システム管理者及びネットワーク管理者は、サーバーの電源について落雷等による過電流対策を施し、停電時には機器が正常に停止するまでの間の十分な電力を供給しうる予備電源を備えつけること。

（５）機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

４．人的セキュリティ対策

（１）職員の責務

① 職員は、情報セキュリティポリシー及び情報セキュリティ実施手順に定められている事項を遵守すること。

② 職員は、端末機及びサーバーの操作は、情報システム管理者が定める運用時間内に行うこと。

③ 職員は、業務目的以外での情報システムへのアクセス及びこれを利用したメールの送受信を行わないこと。

④ 職員は、情報システムの使用を終了し、又は中断する場合は、適切な操作をすること。

⑤ 職員は、情報システム管理者の許可を得ず、情報システムにソフトウェアのインストール及び周辺機器等を接続しないこと。

⑥ 職員は、情報システムを使用するにあたり、外部に情報が漏れることのないよう必要な対策を講じること。

⑦ 職員は、情報セキュリティ責任者の許可を得ず、情報資産を事務室外に持ち出さないこと。

（２）外部委託事業者等の管理

① 情報セキュリティ責任者は、情報資産を取り扱うことが予想される外部委託事業者等と契約等を締結する際には、岸和田市貝塚市清掃施設組合電子計算機及び情報システム管理運用規程（平成30年規程第１号）第10条各号に規定されるもののほか、必要に応じて、次の事項を追加すること。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

・提供されるサービスレベルの保証（ＳＬＡ）
・委託事業者の従業員に対する教育の実施
・委託業務の定期報告義務
・本組合による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）
・その他情報資産の保護に関し必要な事項

② 情報セキュリティ責任者は、所管する情報システムに係る開発等の業務を外部の事業者に委託し、当該事業者の従業員等の派遣を受けるときは、必要に応じてその代表及び本人の双方から秘密保持等のための情報資産の適正な取扱いに関する誓約書を提出させること。

（3）パスワードの管理

① パスワードは、口外及びメモ書き等により、他に漏らさないこと。
② パスワードは、情報システム及びパソコン等の端末に記憶させないこと。
③ パスワードは、定期的に変更すること。
④ パスワードは、十分な長さとし、他人が容易に推測できるようなパスワードを使用しないこと。

（4）教育及び訓練

① ＣＩＳＯは、職員に対し、権限と責任に応じた次の事項について情報セキュリティポリシーに関する研修を実施すること。
・情報セキュリティポリシーの周知徹底
・関連法令等の理解
・関連する実施手順の理解（関連する部門対象者への教育）
・情報セキュリティ事故対策の教育訓練
② 職員は、定められた研修に参加し、情報セキュリティポリシー及び実施手順を理解し、情報セキュリティ上の問題を生じさせないようにすること。

５．技術的セキュリティ対策

（1）コンピュータウイルス等不正プログラム対策

① ネットワーク管理者及び情報システム管理者は、情報システムに不正プログラム対策ソフトを導入するなどの適正な不正プログラム対策を講じること。
② ネットワーク管理者及び情報システム管理者は、不正プログラム対策ソフトの定義ファイルを、常に最新のものに更新すること。
③ ネットワーク管理者及び情報システム管理者は、不正プログラム感染時の対策手順を定めること。

（2）ネットワークの管理

① ネットワーク管理者は、ネットワークにおける情報及びネットワークを支える基盤の保護を確実にするため、ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること。
② ネットワーク管理者は、ネットワークに接続したサービス及び情報を、許可されていないアクセスから確実に保護すること。
③ ネットワーク管理者及び情報システム管理者は、公衆ネットワークを通過するデ

ータの機密性及び完全性を保護するため、並びにネットワークに接続した情報システムを保護するために、必要に応じて、特別な管理策を確立すること。

④　ネットワーク管理者及び情報システム管理者は、無線による通信を導入する場合、暗号化及びＭＡＣアドレスによる制御等の対策を講じること。

（３）機器及び媒体の取扱い

①　情報セキュリティ責任者及び情報システム管理者は、コンピュータの取外し可能な記録媒体（光ディスク、フロッピーディスク、ＵＳＢメモリ、ハードディスク、磁気テープ等）及び情報システムから印刷された文書の管理手順を定めること。

②　情報セキュリティ責任者及び情報システム管理者は、機器及び媒体の廃棄、修理にあたり情報の消去等について手順を定めること。

（４）公開ＷＥＢサーバー等の保護

インターネットに公開するＷＥＢサーバー等の情報システムの管理者は、不正アクセスや改ざん、サービス不能攻撃等の対策を講じること。

（５）情報の交換

①　情報セキュリティ責任者及び情報システム管理者は、他の組織との間で交換される情報の紛失、改ざん又は誤用を防止するため、他の組織との間の情報及びソフトウェアの交換手順について合意を取り交わすこと。なお、重要性に応じて契約又は協定等を締結すること。

②　情報セキュリティ責任者は、電子メールにおけるセキュリティ上の脅威を回避するよう努めること。

（６）アクセス権限の管理

ネットワーク管理者及び情報システム管理者は、情報資産を不正なアクセスから保護するためにアクセス権限の管理にあたり、次の事項を実施しなければならない。

①　利用者ごと、又は利用者からなるグループごとに対するアクセス権限の割り当て及び使用を制限し、管理すること。

②　利用者ごと、又は利用者からなるグループごとに対するアクセス制御に関するルールを定めること。

③　アクセス制御に関するルールは、明確に許可していなければ原則的に禁止するという前提に基づくこと。

④　個人情報を含む特に重要な情報に関しては、個別のアクセス制御を考慮すること。

⑤　すべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続を定めること。

⑥　アクセス権限の割り当てを定期的に検査して、許可されていないアクセス権限は速やかに削除すること。

⑦　利用者に対し、アクセス制御の必要性を周知徹底すること。

（７）パスワードの管理

ネットワーク管理者及び情報システム管理者は、情報資産を不正なアクセスから保護するためにパスワードの管理にあたり、次の事項を実施しなければならない。

① 利用者認証については、ユーザーＩＤ及びパスワード又は物理的認証手段を設定すること。
② ユーザーＩＤ及びパスワード又は物理的認証手段の割り当ては、正規の手続によって管理すること。
③ 操作が誰の責任によるものかを追跡できるように、認証の記録を取ること。また、認証に失敗した試みについても記録すること。
④ 推測されにくいパスワードであることを確実にするために、有効な機能を提供すること。
⑤ 利用者がパスワードを選択する場合、仮のパスワードは最初のログイン時に変更させるようにすること。
⑥ 情報システムへログインするための手順は、３回以上の認証失敗後は権限を停止するなど、許可されていないアクセスの恐れを最小限に抑えるように設計すること。

（８）ネットワークのアクセス制御

ネットワーク管理者及び情報システム管理者は、情報資産を不正なアクセスから保護するためにネットワークのアクセス制御にあたり、次の事項を実施しなければならない。

① 指定された経路以外の経路を、利用者が選択できないようにすること。
② 遠隔地からの利用者のアクセスには、認証を行うこと。
③ 遠隔コンピュータシステムへの接続は、認証されること。
④ ネットワーク機器のポートへのアクセスは、セキュリティを保つように制御されること。
⑤ 不正なアクセスが行われないよう、ネットワーク内に制御策を導入し、情報サービス、利用者及び情報システムを分割するよう考慮すること。
⑥ 外部委託事業者等のネットワークサービスを使用する場合は、使用するサービスのセキュリティの特質について明確な説明を受け、必要があれば対策を行うこと。

（９）管理者のアクセス制御

ネットワーク管理者及び情報システム管理者は、情報資産を不正なアクセスから保護するために管理者のアクセス制御にあたり、次の事項を実施しなければならない。

① システムユーティリティの使用は制限し、厳しく管理すること。
② 技術支援要員（オペレータ、ネットワーク技術者、システムプログラマ、データベース管理者等）は、その操作が誰の責任によるものかを追跡できるように、各個人の利用者ごとに識別できるもの（ユーザーＩＤ等）を保有すること。
③ 許可されていない者によるアクセスを防止するため、管理者権限によるログインは管理者権限が必要な操作を行うときだけとし、短時間の離席であっても管理者権限をログアウトすること。

(10) システムアクセス及びシステム使用状況の監視

ネットワーク管理者及び情報システム管理者は、情報資産を不正なアクセスから保護するためにシステムアクセス及びシステム使用状況の監視にあたり、次の事項を実施しなければならない。

① 利用者が明確に許可された操作を実行するために、情報処理設備の使用状況を監

視する手順を確立すること。
② 監視の結果は記録し、定期的に確認すること。
③ 情報システムが直面する脅威を把握し、その対策を講じるために、監視記録を検証すること。
④ 将来の調査及びアクセス制御の監視を補うために、例外事項、その他のセキュリティに関連した事象の記録を作成して、一定期間保存すること。
・記録には、ユーザーＩＤを含めること。
・記録には、ログイン及びログアウトの日時を含めること。
・記録には、端末のＩＤ又は所在地を含めること。
・記録には、情報システムへのアクセスを試みて、成功及び失敗した記録を含めること。
・記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること。
⑤ 記録の正確性を保証するためにコンピュータの時計は正しく設定すること。

(11) モバイルコンピュータの利用

ネットワーク管理者及び情報システム管理者は、モバイルコンピュータを外部で用いるときに業務情報のセキュリティが危険にさらされないよう、物理的保護、アクセス制御、暗号化、バックアップ及びコンピュータウイルス等の不正プログラム対策等について、実施手順に記述しなければならない。

６．情報システムの開発及び運用・保守

情報システム管理者は、情報システムの開発及び運用・保守を行う場合、次の事項を実施しなければならない。

（1）システム開発

① 情報セキュリティが確保されていること。また、すでに稼動している情報システムへの影響の有無を確認すること。
② 業務用ソフトの選定や評価にあたっては、セキュリティ対策を考慮すること。
③ 許可を受けた者以外、プログラムやシステムファイルの作成、更新及び削除を行わせないこと。
④ ベンダー又は外部委託事業者等が支援のために情報システムにアクセスするときは、承認と監視を行うこと。
⑤ データの誤入力を防止する機能を装備すること。また、異常データの入出力を防止する機能を装備すること。
⑥ パソコンで稼動する情報システムは、以下の点を考慮すること。
・利用者の権限に応じたアクセス制御が実施されたパソコンを使用すること。
・基本ソフトやアプリケーションソフトは、ベンダーによって維持、サポートされているものを使用すること。
⑦ 情報システムのテストは、できる限り本番データに近い内容と量で行うこと。ただし、本番のデータベースを直接使用しないこと。
⑧ 情報システムのテストであっても、本番と同等のアクセス制御を行うこと。
⑨ 情報システムのテスト結果の確認は、開発者と利用者の双方で行うこと。

（2）システム運用

① 情報システム管理者は、システム構築にあたり作成したドキュメント類を適正に

管理し保管すること。

② 情報システム管理者は、情報処理設備のセキュリティを保った運用を確実にするため、実施手順に基づいた操作手順書を作成すること。

③ 情報システム管理者は、情報処理の完全性及び可用性を維持するため、データ及びソフトウェアのバックアップは、定期的に取得し検査すること。

④ 情報システム担当者は、自分の作業の記録をとること。

⑤ 情報システム担当者は、情報セキュリティインシデント発生時は情報システム管理者に報告を行い、実施手順に従い適正な処置をとること。

⑥ ネットワーク管理者及び情報システム管理者は、セキュリティの維持に必要な情報（アクセスログ等）を適切に管理し、定期的に分析すること。

⑦ ネットワーク管理者及び情報システム管理者は、設備の管理に関する責任及び手順を確立すること。

⑧ ネットワーク管理者及び情報システム管理者は、情報セキュリティインシデント発生時において市民サービスへの影響を最小限にするよう対策をとること。

⑨ ネットワーク管理者及び情報システム管理者は、情報システムの稼動やジョブの実行、パラメータの設定、データのバックアップやログの取得は可能な限り自動化し、人手による介入を削減すること。

⑩ 相互監視の観点から、情報システムの操作は複数人で行うこと。ただし、情報セキュリティインシデント発生時などの緊急時はこの限りでない。

（3）システム変更

① 情報システム管理者は、情報処理設備及び情報システムの変更について、その記録を適切に管理すること。また、情報セキュリティに影響を及ぼすシステム変更についてはＣＩＳＯに報告すること。

② 情報システム管理者は、情報システムの変更に際し、外部委託を行うときは契約書等において情報セキュリティポリシーを遵守する義務を課すこと。

７．外部サービスの利用

（1）情報システムにおいて外部サービスを利用する場合

情報システム管理者は６の規定を実施しなければならない。新規のシステムにおいて外部サービスを利用する場合、または既存のシステムにおいて新規に外部サービスを利用する場合は、ネットワーク管理者の承認を得ること。

（2）情報システム以外で外部サービスを利用する場合

職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で外部サービスを利用すること。

８．重要度Ｂ以上の情報を扱う外部サービスの利用

情報システム管理者及び情報セキュリティ管理者は、７の規定に加え、下記事項を実施しなければならない。情報システム以外において外部サービスの利用を開始する場合は、ネットワーク管理者の承認を得なければならない。

・情報セキュリティ対策が適切になされていることの確認。
・外部サービス提供者によるデータの目的外利用の禁止。
・意図しないデータ変更を防止する体制が取られているかの確認。

・外部サービス提供者の実績、施設の場所、リージョン、及びＳＬＡ等の観点に基づく、データの可用性を担保できる状態にあることの確認。
・外部サービス提供者において情報セキュリティインシデントへ迅速に対応できる体制がとられていることの確認。
・外部サービス提供者において、情報セキュリティ対策その他の契約の履行状況の確認ができる体制がとられていることの確認。
・必要に応じ本市の情報セキュリティ監査を受け入れることを外部サービス提供者に約束させること。
・外部サービス提供者のセキュリティ対策や契約の履行が不十分であった場合の対策や責任分界点、法律上の紛争が発生した場合の所管裁判所、本市に無断での再委託の禁止等を契約に盛り込むこと。
・外部サービスの利用終了時に、適切に情報及び機器等が廃棄される体制がとられていることの確認。

９．緊急時の対応

情報セキュリティインシデントが発生した際に、迅速かつ円滑に必要な措置を実施するため、次の事項を定める。

（１）情報セキュリティインシデントへの対応

① 職員等は、情報セキュリティインシデントを発見した場合、当該情報資産を所管する情報セキュリティ責任者へ直ちに報告すること。
② 情報セキュリティ責任者は、情報セキュリティインシデントに関する情報を取りまとめ、ＣＩＳＯへ報告すること。
③ ＣＩＳＯは、情報セキュリティインシデント対象となった情報資産の重要度や情報セキュリティインシデントにより生じた結果の重大性等に応じて委員会を開催し、対処方法の検討や外部への報告についての協議を行うこと。
④ ＣＩＳＯは、情報セキュリティインシデントの報告を受けた後、情報セキュリティ責任者に対し速やかに指示を行い、復旧や被害の拡大防止に努めること。
⑤ 職員等は、情報セキュリティ責任者の指示に従い、復旧や被害の拡大防止に努めること。

（２）再発防止

① 情報セキュリティ責任者は、セキュリティ侵害への対応を完了させた後、その原因を究明し、結果を基にして、速やかに再発防止策を講じること。
② 情報セキュリティ責任者は、セキュリティ侵害の発生から再発防止策の実施までの一連の記録を収集し、ＣＩＳＯへ報告すること。
③ 職員等は、情報セキュリティ責任者の指示に従い、復旧や被害の拡大防止に努めること。

10. 適合性

（1）法令等の遵守

職員等は、職務の遂行において情報資産を使用する場合、関係する法令等を遵守しなければならない。

（2）点検等

① 情報セキュリティ責任者は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうかについて点検を行うこと。また、情報セキュリティ責任者はこれをとりまとめ、委員会に報告を行うこと。

② 委員会は、新たに必要な対策が発生した場合、又は点検の結果を踏まえ委員会において情報セキュリティポリシーの実効性を評価し見直しが必要となった場合、情報セキュリティポリシーの見直し内容及び時期についての決定を行い、更新すること。

③ 委員会は、更新に際して必要に応じて情報セキュリティポリシープロジェクトチームを設置すること。