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、本市における情報セキュリティ対策の基準を定めたものである。

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。

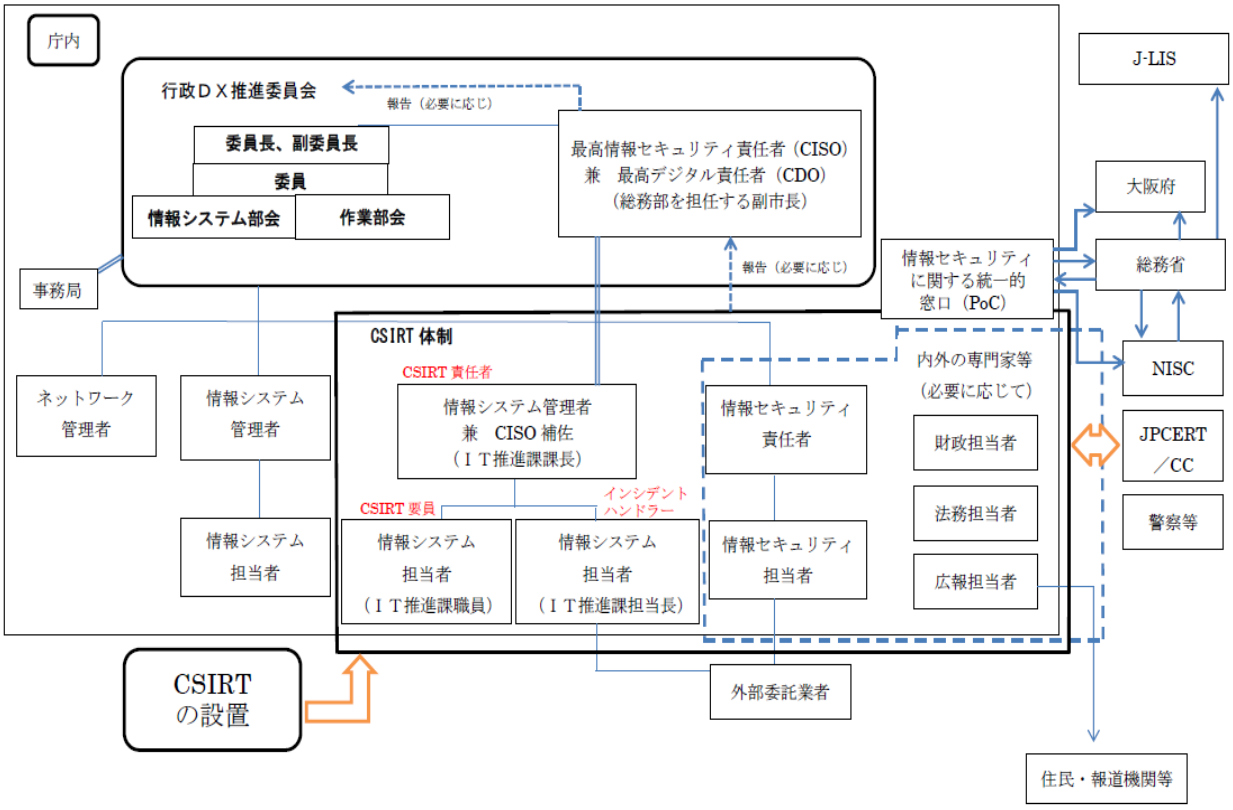

図１　情報セキュリティ運用体制

（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	名称	役職等	主な役割等
1	ＣＩＳＯ（情報セキュリティ統括責任者）	総務部を担任する副市長	○情報セキュリティに関する全ての責任と権限を有する。 ○行政ＤＸ推進委員会の委員長を務め、必要に応じて委員を召集し、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	総務部 ＩＴ推進課長	○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。 ○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	総務部 ＩＴ推進課長	○全庁的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	所属長 （全課長）	○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本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、行政ＤＸ推進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。

項番	名称	役職等	主な役割等
6	情報システム管理者	各情報システム所管課長	○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

岸和田市行政ＤＸ推進委員会（以下「委員会」という。）が、本市の情報セキュリティ対策について、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】（岸和田市行政ＤＸ推進委員会設置要綱第３条）

① 行政ＤＸに係る計画の策定及び推進に関すること。
② 情報システムの新規導入並びに既存の情報システムの基本機能の仕様変更（軽易な変更を除く。）及び運用計画期間の更新に関すること。
③ 情報セキュリティポリシーの策定及び改定並びに運用に関すること。
④ セキュリティ侵害に関する情報収集及び発生予防並びにセキュリティ侵害の発生時における対応に関すること。
⑤ その他行政ＤＸに関する重要な事項、情報システムの管理及び運用に係る重要な事項並びに情報セキュリティに関する重要な事項に関すること。

表２　委員会役割等一覧

項番	名称	役職等	主な役割等
1	委員長	総務部を担任する副市長 （ＣＩＳＯが兼任）	○委員会を統括する。
2	副委員長	総務部長	○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。
3	委員	全部長及び上下水道局長（総務部長を除く）	○情報セキュリティに関する重要事項について協議する。 ○必要に応じ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。 ○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。

項番	名称	役職等	主な役割等
			○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。
4	事務局	総務部ＩＴ推進課	○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。

（４）ＣＳＩＲＴの設置・役割

ＣＩＳＯは、情報セキュリティインシデントに対処するため、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うための体制（Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）を設置する。

【ＣＳＩＲＴの役割等】ＣＳＩＲＴの体制役割等一覧を表３に示す。

① ＣＳＩＲＴは、情報セキュリティに関する統一的な窓口とする。

② ＣＳＩＲＴは、情報セキュリティインシデントと思われる事案が発生した場合は、その状況を確認し、情報セキュリティインシデントであるか評価を行う。

③ ＣＳＩＲＴは、情報セキュリティインシデントであると判断した場合は、速やかにＣＩＳＯに報告する。

④ ＣＳＩＲＴは、被害の拡大防止等を図るため、情報セキュリティインシデントに関係する情報セキュリティ責任者に対して応急措置の実施及び復旧に係る指示、勧告、助言を行う。

⑤ ＣＳＩＲＴは、報道機関への通知公表が必要な場合等、必要に応じて、広報部門や法規部門その他関係部署を要員とすることができる。

⑥ 重大な情報セキュリティインシデントが発生した場合は、状況に応じて、ＣＩＳＯ、大阪府、総務省、内閣官房内閣サイバーセキュリティセンター等に報告する。

表３　ＣＳＩＲＴ体制役割等一覧

項番	名称	役職等	主な役割等
1	ＣＳＩＲＴ 責任者	総務部ＩＴ推進課長 （ＣＩＳＯ補佐）	○セキュリティインシデント発生時には、ＣＩＳＯに侵害内容や状況等を報告し、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ＣＳＩＲＴ責任者の指示に従うこと。

項番	名称	役職等	主な役割等
2	インシデント ハンドラー	総務部ＩＴ推進課 担当長	○インシデント発生時の、インシデント分析及び対処法の検討、関係部署との調整を行う等、インシデントに対応するＣＳＩＲＴを、実務的な観点から中核として支え、対応方針を検討し、インシデントハンドリング全体に係るプロジェクトマネジメント等を行う。
3	ＣＳＩＲＴ要員	総務部ＩＴ推進課 職員	○セキュリティインシデント発生時には、ＣＳＩＲＴ責任者に報告し、情報を収集し、被害の拡大防止や復旧に努める。
4	ＣＳＩＲＴ要員 （必要に応じて）	財政担当者	インシデントハンドリングにおける予算対応等
		法務担当者	インシデントハンドリングにおける法的対応等
		広報担当者	インシデントハンドリングにおけるマスコミ対応等

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４に示す分類を行うものとする。

表４　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正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５に示すセキュリティ区画を設定する。

表５　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） サーバ室､使用時以外施錠しているサーバラック	サーバ等	サーバ等
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	該当無し	重要度Ａの情報を保存したパソコン･媒体 サーバ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） 一般道路、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。

＊ 盗難防止用ワイヤー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５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、サーバを設置する場合は火災、水害、落雷、温度、湿度、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。特にマイナンバー利用事務系にて利用した記憶装置については物理破壊を施すこと。

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、適正な操作をすること。

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、岸和田市電子計算機及び情報システム管理運用規程（平成 12 年庁達第７号）第 11 条各号に規定されるものの外、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
・市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 課ＩＤ等の共有するＩＤのパスワードは、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サーバ等の保護

インターネットに公開するＷＥＢサーバ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(利用者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、利用者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．情報システム全体の強靭化

ネットワーク管理者は、情報資産を不正なアクセスから保護するためにインターネット接続系から分離するにあたり、次の事項を実施しなければならない。

（１）マイナンバー利用事務系

① マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにすること。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行うこと。なお、外部接続先もインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

② 情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用すること。

（イ）情報の持ち出し不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定すること。

（２）ＬＧＷＡＮ接続系

① ＬＧＷＡＮ接続系とインターネット接続系の分離

ＬＧＷＡＮ接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすること。

（３）インターネット接続系

① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視及びＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じること。

② 市区町村のインターネット接続口を集約する大阪版自治体情報セキュリティクラウドに参加するとともに、関係省庁や大阪府等と連携しながら、情報セキュリティ対策を推進すること。

（４）管理系

① 管理系においては、マイナンバー利用事務系、ＬＧＷＡＮ接続系、インターネット接続系との環境間の通信環境を分離した上で、システム運用上必要な通信だけを許可できるようにすること。

７．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 岸和田市電子計算機及び情報システム管理運用規程（平成 25 年庁達第 11 号）で定める情報システム導入計画書を提出し、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）を適正に管理し、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、その記録を適正に管理すること。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。

８．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７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は情報システム導入計画書にその旨を記載すること。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。

９．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８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。またマイナンバー利用事務系の標準準拠システム等をガバメントクラウド上に構築する場合、情報システム管理者は「岸和田市情報セキュリティポリシー_別冊_ガバメントクラウド編」に記載する各事項についても実施しなければならない。

・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。

10. 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及び情報セキュリティに関する統一的な窓口へ直ちに報告すること。

② ＣＳＩＲＴ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及び図２にある外部関係機関に速やかに報告すること。

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、情報セキュリティ戦略の意思決定を行うこと。なお、委員会は、必要に応じて危機管理監に意見を求めるものとする。

④ ＣＳＩＲＴは発生した情報セキュリティインシデントの情報を把握、分析した上で情報セキュリティ責任者に対して、速やかに被害の拡大防止等を図るため措置の実施及び復旧にかかる指示又は勧告を行うこと。

⑤ 職員等は、情報セキュリティ責任者及びＣＳＩＲＴの指示に従い、復旧や被害の拡大防止に努めること。

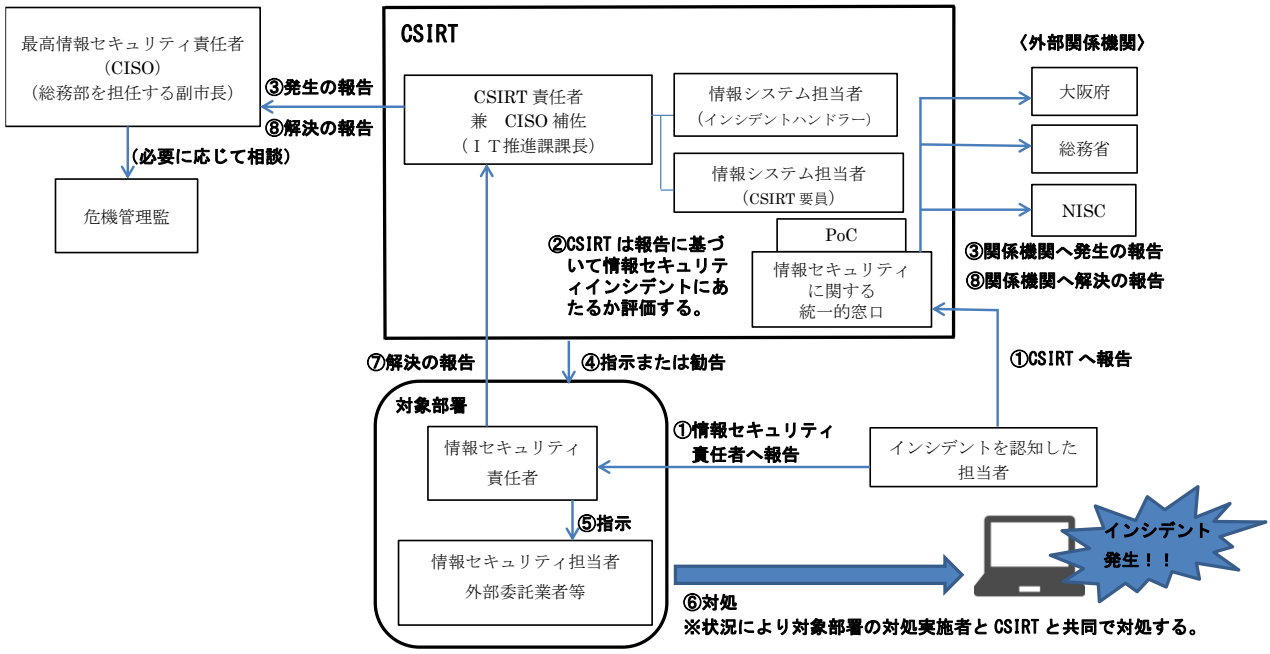

図２　情報セキュリティインシデントへの対応フロー

（２）再発防止

①　ＣＳＩＲＴは、情報セキュリティインシデントの原因を究明し、記録を保存すること。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＳＯに報告すること。

②　ＣＩＳＯは、ＣＳＩＲＴから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。

③　職員等は、情報セキュリティ責任者の指示に従い、再発防止に努めること。

11. 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）監査等

①　委員会は、情報セキュリティ監査統括責任者を任じ、情報セキュリティ対策状況について、定期的又は必要に応じて情報セキュリティ監査を行うこと。また、情報セキュリティ監査統括責任者は、監査結果をＣＩＳＯ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。