諫早市情報セキュリティの基本方針に関する規則をここに公布する。

令和８年３月１１日

諫早市長　　大久保　潔　重

諫早市規則第６号

諫早市情報セキュリティの基本方針に関する規則

（目的）

第１条　この規則は、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（定義）

第２条　この規則において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

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。

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　情報セキュリティポリシー　この規則及び情報セキュリティ対策基準をいう。

⑸　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。

⑹　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。

⑺　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。

⑻　マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務（社会保障、地方税又は防災に関する事務をいう。）

又は戸籍事務等に関わる情報システム及びデータをいう。

⑼　ＬＧＷＡＮ接続系（総合行政ネットワーク系）　ＬＧＷＡＮ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（マイナンバー利用事務系を除く。）。

⑽　インターネット接続系　インターネットメール、ホームページ管理システム等に関わる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。

⑾　通信経路の分割　ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⑿　無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がないなど安全が確保された通信をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として想定するものは、次のとおりとする。

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、重要情報の詐取、内部不正等

⑵　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、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

⑶　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

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

（適用範囲）

第４条　この規則が適用される行政機関は、市長部局、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、上下水道局及び議会事務局とする。

２　この規則が対象とする情報資産は、次のとおりとする。

⑴　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

⑵　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。）

⑶　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

３　この規則は、情報資産を取り扱う全ての職員等（地方公務員法（昭和２５年法律第２６１号）第３条に規定する一般職及び特別職の職員をいう。以下同じ。）に適用する。

（職員等の遵守義務）

第５条　職員等は、情報セキュリティ対策の重要性について共通の認識を持ち、業務の遂行に当たって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を遵守しなければならない。

２　前項のほか、職員等は、業務の遂行において取り扱う情報資産を保護するため、当該情報資産を取り扱う際には、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）、諫早市個人情報の保護に関する法律施行条例（令和４年条例第２０号）等の情報セキュリティ対策基準に定める情報セキュリティに関連する法令を遵守しなければならない。

（情報セキュリティ対策の組織体制）

第６条　市の保有する情報資産について、情報セキュリティ対策を実施する全庁的な組織体制を確立する。

２　前項の規定に基づく組織体制として、最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）、最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報シス

テム管理者を置く。

3　ＣＩＳＯは、総務部の事務を担任する副市長をもって充てる。

4　副ＣＩＳＯは、総務部以外の事務を担任する副市長をもって充てる。

5　統括情報セキュリティ責任者は、総務部長をもって充てる。

6　情報セキュリティ責任者は、別表に掲げる者をもって充てる。

7　情報セキュリティ管理者は、情報システムを利用する課室等を所管する課長又は課長相当の職にある者をもって充てる。

8　情報システム管理者は、総務部デジタル推進課長をもって充てる。

（ＣＩＳＯ等の職務権限）

第７条　ＣＩＳＯは、市が保有する全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

2　副ＣＩＳＯは、ＣＩＳＯを補佐し、ＣＩＳＯに事故があるときは、その職務を代理する。

3　統括情報セキュリティ責任者は、ＣＩＳＯ及び副ＣＩＳＯを補佐し、情報セキュリティ対策全般を統括する。

4　情報セキュリティ責任者は、その所管する部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

5　情報セキュリティ管理者は、所管する課室等の業務のネットワーク及び情報システムの開発、設定の変更、運用及び運用の見直しを行い、又は必要に応じ情報システム管理者にこれらを委任するとともに、所管する課室等の情報資産に係る情報セキュリティ対策について当該課室等の職員等を指揮監督する。

6　情報システム管理者は、統括情報セキュリティ責任者を補佐し、情報セキュリティ対策について情報セキュリティ管理者に対し指導及び助言を行うとともに、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の遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ委員会の設置）

第８条　市の情報セキュリティ対策を統一的に実施するため、諫早市情報セキュリティ委員会（以下「委員会」という。）を設置する。

２　委員会は、ＣＩＳＯ、副ＣＩＳＯ、統括情報セキュリティ責任者及び情報セキュリティ責任者をもって組織する。

３　委員会の所掌事務その他必要な事項は、情報セキュリティ対策基準において定める。

（情報資産の分類と管理）

第９条　市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実施する。

（情報システム全体の強靭性の向上）

第１０条　情報セキュリティの強化を目的として、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、次の各号に掲げる三段階の区分に応じ、当該各号に定めるセキュリティ対策を講ずる。

⑴　マイナンバー利用事務系　原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

⑵　ＬＧＷＡＮ接続系　ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割することを原則とし、両システム間で通信する場合には、無害化通信を実施する。

⑶　インターネット接続系　不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。この場合において、高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（情報セキュリティ対策）

第１１条　前条のほか、第３条に規定する脅威から情報資産を保護

するため、次の各号に掲げる区分に応じ、当該各号に定めるセキュリティ対策を講ずる。

(1) 物理的セキュリティ　サーバ、情報システム室、通信回線及び職員等のパソコン等の管理についての物理的な対策を講ずる。

(2) 人的セキュリティ　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講ずる。

(3) 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対策を講ずる。

(4) 運用　情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講ずるとともに、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正に対応するため、緊急時対応計画を策定する。

(5) 業務委託　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き措置を講ずる。

(6) 外部サービス（クラウドサービス）の利用　外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講ずる。

(7) ソーシャルメディアサービスの利用　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(8) 評価・見直し　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上

を図る。この場合において、情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検）

第１２条　統括情報セキュリティ責任者、情報セキュリティ責任者又は情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第１３条　ＣＩＳＯは、情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシー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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損害等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第１４条　第６条から前条までに規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（情報セキュリティ実施手順の策定）

第１５条　前条の情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な実施手順を定めた情報セキュリティ実施手順を策定するものとする。

（情報セキュリティ対策基準等の非公開）

第１６条　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市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

（違反に対する措置等）

第１７条　この規則、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に違反する行為は地方公務員法第２９条第１項第１

号に該当し、違反した職員は、その重大性に応じて同条に規定する懲戒処分の対象とする場合がある。

2　市は、市が保有する情報資産を侵害した者に対し、その重大性、発生した事案の状況等に応じて損害賠償を請求することができる。

附　則

この規則は、令和８年４月１日から施行する。

別表（第６条関係）

情報セキュリティ責任者
教育長
上下水道事業管理者
議会事務局長
企画財務部長
こども福祉部長
健康保険部長
地域政策部長
農林水産部長
経済交流部長
建設部長
会計管理者
選挙管理委員会事務局長
監査委員事務局長
農業委員会事務局長