河津町役場

情報セキュリティポリシー

令和６年７月２３日

第１章　河津町役場セキュリティポリシー基本方針

１．目　的

河津町が取り扱う情報資産には、町民の個人情報のみならず行政運用上重要な情報など部外へ漏洩した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報を様々な脅威から防御することは、町民の財産及びプライバシーを守るためにも事務の安定的な運営のためにも必要不可欠である。ひいては、このことが河津町に対する町民からの信頼向上に寄与するものである。また、個人番号（マイナンバー）制度の施行により、河津町としても個人番号を含む特定個人情報を取り扱うことにより、より強固な情報セキュリティが求められている。

このため、河津町の情報資産の機密性、完全性、可用性(注)を維持するための対策として河津町情報セキュリティポリシー（以下「セキュリティポリシー」という。）を策定し河津町における情報セキュリティの基本方針とするものである。

（注）国際標準化機構（ISO）が定めるもの（ＩＳＯ　１７７９９）

機密性（confidentiality）　：情報にアクセスすることが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保護すること。

可用性（availability）　：許可された利用者が必要な時に情報にアクセスできることを確実にすること。

２．定義

１）ネットワーク

河津町における本庁舎内部部局、教育委員会、幼稚園及び公営企業会計を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）とする。

２）情報資産

ネットワークや情報システムで取り扱う情報及びこれらに関する設備、電磁的記録媒体を情報資産とする。

３）情報システム

パソコン及びその周辺機器で情報資産を作成、保存、印刷できる機能を有するもの及びソフトウェアを情報システムとする。

４）マイナンバー利用事務系

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）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。

５）LGWAN 接続系

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。）。

６）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。

７）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。

３．セキュリティポリシーの位置付けと職員等の義務

セキュリティポリシーは、河津町の情報セキュリティ対策の頂点に位置するものである。したがって、河津町が所管する情報資産に関する業務全体に携わるすべての職員及び外部委託者等は、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共に業務の遂行に当ってセキュリティポリシーを遵守する義務を負うものとする。

４．情報資産の脅威

セキュリティポリシーを遵守するうえで、情報資産を脅かす脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

１）地震、落雷、火災等の災害並びに事故、機器故障等の物理的要因によるサービス及び業務の停止

２）規定違反、操作・設定ミス、内部不正、委託管理の不備、監査機能の不備等の人的要因による情報資産の漏洩、破壊、消去等

３）不正アクセス、プログラム上の欠陥、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技術的な要因による情報資産の漏洩、改ざん、消去、重要情報の搾取等

５．情報セキュリティ対策

上記４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ずるものとする。

１）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、情報資産への損傷、妨害等から保護するために物理的な対策を講ずる。

２）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等にセキュリティポリシーの内容を周知する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

３）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に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面の対策、また、システム開発等の外部委託、ネットワークの監視、セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

４）情報システム全体の強靭性の向上

情報システム全体に対し、次の対策を講ずる。

① マイナンバー利用事務系においては、可能な限りほか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、情報の流出を防ぐ。

② LGWAN 接続系においては、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。なお、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。

③ 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高度な情報セキュリティ対策を講ずる。高度な情報セキュリティ対策として、県内市町共同利用の自治体情報セキュリティクラウドの導入を実施する。

５）外部サービスの利用

外部委託を実施する場合には、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要な情報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。

約款による外部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。

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、発信できる情報等を規定し、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。

6．情報セキュリティ監査及び自己点検の実施

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監査及び自己点検を実施する。

7．評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により運用改善を行い情報セキュリティの向上を図る。また、セキュリティポリシーの見直しが必要に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に新たに対策が必要となった場合には、セキュリティポリシーの見直しを実施する。

8．情報セキュリティ対策基準の策定

上記５、６及び７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記した情報セキュリティ対策基準を策定する。