延岡市ＣＳＩＲＴ設置要綱

令和３年９月１７日策定

延岡市企画部情報政策課

１．　設置

延岡市情報セキュリティポリシーの及ぶ範囲に関わる情報セキュリティインシデント（以下「インシデント」という。）に、迅速かつ適切に対応するため、インシデント対応への即応力、専門的知見、情報セキュリティ委員会等において迅速かつ的確な意思決定を行うために必要な情報の収集力等を具備した緊急即応チームとして、延岡市ＣＳＩＲＴ（以下「ＣＳＩＲＴ」という。）を設置するものとする。

２．　役割

ＣＳＩＲＴの役割は次のとおりとする。

（１）インシデント発生時の対応

ア　検知・連絡受付

インシデントの発生に関する予兆等の検知、発見、内部外部からのインシデントに関わる連絡・報告等の受付を行う。

イ　トリアージ

事実関係を確認の上、インシデントが発生したかどうかを検査・分析により判断し、被害状況や影響範囲等事態の全体像を把握した上で、インシデントの処理に優先順位を付ける。

ウ　インシデントレスポンス

初動対応（対応方針の検討、証拠の取得・保全・確保・記録、インシデントの封じ込め・根絶）の実施、復旧措置（応急対策）の実施及び再発防止策（恒久対策）の検討を行う。

エ　報告・公表

被害状況や影響範囲等に応じ、内外の関係者（最高情報セキュリティ責任者（ＣＩＳＯ）、総務省、宮崎県、内閣サイバーセキュリティセンター（ＮＩＳＣ）、宮崎県警察本部等）への報告及び対外的な対応（報道発表、関係住民への連絡）を行う。

オ　事後対応

インシデントの収束宣言を行い、報告書をまとめる。

（２）平常時の事前準備・予防等

ア　インシデント発生時の対応に必要な事前準備・予防

イ　インシデント発生を想定した訓練・演習の定期的な実施

ウ　インシデントレスポンス手順等の定期的な評価・見直し（自己点検）

エ　その他ＣＳＩＲＴ責任者が定めるもの

３．　ＰｏＣ（情報セキュリティに関する統一的な窓口）

CSIRT において、インシデント発生時に庁内外の者からの連絡受付の役割を担う、情報セキュリティに関する統一的な窓口となるＰｏＣ（Point of Contact、ポック）を整備し（別表１）、庁内外に周知、公表するものとする。

４．　対象インシデント

ＣＳＩＲＴが扱うインシデントは次のものとする。

情報システムの停止等	情報システム、ネットワーク、サーバ及び端末等の利用に支障をきたす状態
外部からのサイバー攻撃	コンピューター・ウイルス、不正アクセス、ＤｏＳ攻撃、ＤＤｏＳ攻撃、標的型攻撃及びホームページ等の改ざんの発生又は発生が疑われる状態
盗難・紛失	地方公共団体が管理する重要な情報（住民情報、企業情報、入札情報、技術情報等）の盗難・紛失又はこれらの可能性が疑われる状態（内部犯行に起因するものを含む）

５．　体制

ＣＳＩＲＴの体制は次のとおりとする。

（１）ＣＳＩＲＴにＣＳＩＲＴ責任者を置き、統括情報セキュリティ責任者をもって充てる。

（２）ＣＳＩＲＴは、ＣＳＩＲＴ副責任者、ＣＳＩＲＴ管理者、インシデントハンドラー、ＣＳＩＲＴ要員、外部委託事業者、内部関係者等をもって構成し、その構成及び役割はＣＳＩＲＴ構成表（別表２）のとおりとする。

（３）外部委託事業者、外部の専門家等については、必要に応じＣＳＩＲＴ責任者が関係機関に依頼、要請等して定めるものとする。

（４）ＣＳＩＲＴ体制は別図のとおり。

６．この要綱に定めるもののほか、必要な事項は、ＣＩＳＯが定める。

附 則

この要綱は、令和３年９月１７日から施行する。

別表１　PoC（情報セキュリティに関する統一的な窓口）

PoC	延岡市 CSIRT（情報政策課）
所在地	延岡市東本小路 2-1
対応時間	平日 8 時 30 分～17 時 15 分
電話番号	0982-22-7004
FAX 番号	0982-34-6553
メール	（インターネット）jouho-k@city.nobeoka.miyazaki.jp （LGWAN）jouho-k@city.nobeoka.lg.jp

別表２　CSIRT 構成

構成		担当	役割
ＣＳＩＲＴ責任者	統括情報セキュリティ責任者をもって充てる。	企画部長	インシデント対応の責任者。インシデント対応の作業を監督し評価する責任を負う。また、ＣＩＳＯやほかの組織などとの調整役となり、危機を打開し、チームに必要な要員・リソース・技能を確保する。
ＣＳＩＲＴ副責任者	部局情報セキュリティ責任者をもって充てる。	市長部局の部・局長（総合支所長を含む。）、消防長、上下水道局長、教育部長、議会事務局長、	ＣＳＩＲＴ責任者が不在の場合に権限を引き継ぐ
ＣＳＩＲＴ管理者	統括情報セキュリティ管理者をもって充てる。	情報政策課長	チームのリーダー。インシデントハンドラーの作業を調整し、インシデントハンドラーからの情報を収集し、インシデントに関する最新情報を必要な関係者に提供する。また、高い技術的な技能とインシデント対応経験を持ち、インシデント対応チーム全体の技術的な作業品質を監督して、その品質に最終的な責任を持つ。
インシデントハンドラー	情報システム担当者（係長クラスを想定）の中から	情報政策課長補佐	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

	ＣＳＩＲＴ責任者が指名する者		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。
ＣＳＩＲＴ要員	情報システム担当者の中からＣＳＩＲＴ責任者が指名する者	情報政策課員	インシデントハンドラーを補助し、ともにインシデントハンドリングに当たる。
外部委託事業者	システムベンダー（開発事業者、運用・保守事業者等)、ＩＳＰ、ＡＳＰ、クラウド事業者等契約関係のある外部の事業者に対しＣＳＩＲＴ責任者が支援を依頼する者		検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る一部作業
内部関係者	財政部門	財政課	インシデントハンドリングにおける予算対応等
	法務部門	総務課 契約管理課	インシデントハンドリングにおける法的対応（契約を含む）等
	広報部門	経営政策課	インシデントハンドリングにおけるマスコミ対応等
	個人情報保護部門	総務課	インシデントハンドリングにおける個人情報保護対応等
外部の専門家	セキュリティベンダー、ＮＩＳＣ、ＩＰＡ、ＪＰＣＥＲＴ／ＣＣ、警察等からＣ		検査・分析、証拠の取得・保全・確保・記録、インシデントの封じ込めと根絶、復旧措置、再発防止策の検討等に係る作業

	ＳＩＲＴ責任者が支援を要請する者		
その他	上記のほかＣＳＩＲＴ責任者が支援を要請等する者		左記にて要請等された内容