宮崎市ＣＳＩＲＴ設置要綱

平成２８年３月３１日策定

宮　崎　市

１．　設置

宮崎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、宮崎県情報政策担当課と連携し、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、専門的知見を有するとともに、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、宮崎市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（暫定対策）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、都道府県、ＮＩＳＣ、警察機関等）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　インシデントの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

インシデントについて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．　ＣＳＩＲＴ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、インシデント対応管理者、インシデントハンドラー、ＣＳＩＲＴ要員、外部委託事業者、外部の専門家等をもって構成し、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．　情報セキュリティ委員会

（１）情報セキュリティ委員会は、ＣＩＳＯから必要に応じてインシデントに係る報告を受け、分析・評価し、助言する。

（２）情報セキュリティ委員会の体制は、次のとおりとする。

委員長	情報政策担当部長（総務部長）
副委員長	情報政策担当課長（情報政策課長）
委員	セキュリティポリシー担当係長（情報政策課） システム運用担当係長（情報政策課） ＤＸ担当係長（情報政策課） 個人情報保護担当係長（総務法制課） 内部統制推進担当係長（市役所改革推進課）

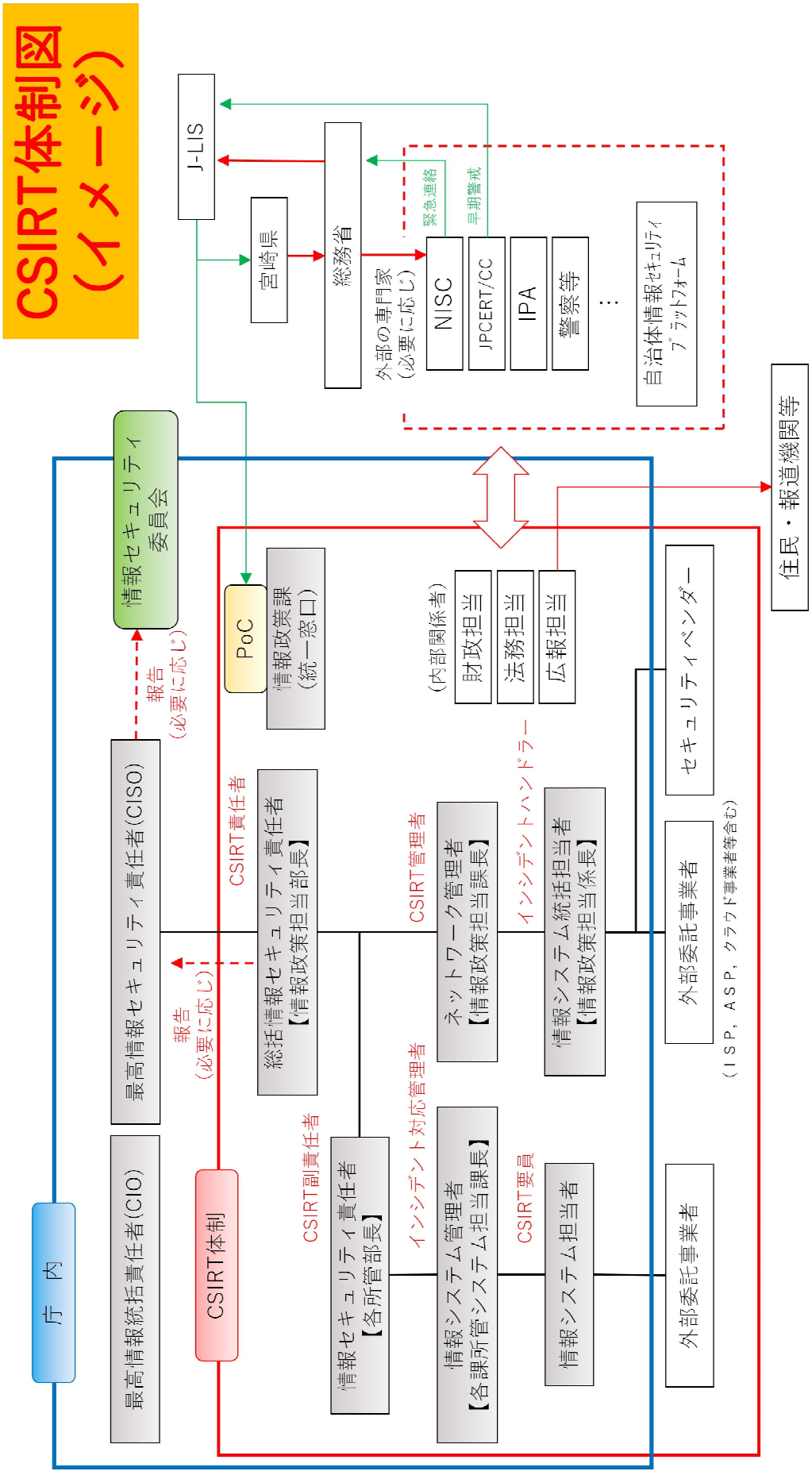
別表１　ＰｏＣ

ＰｏＣ	宮崎市ＣＳＩＲＴ　（情報政策課）
所在地	宮崎市橘通西１丁目１番１号
対応時間	平日　8時30分～17時15分　※メールは24時間受付
電話番号	0985-21-1712
ＦＡＸ番号	0985-22-6106
メール	（インターネット）　03jyouho@city.miyazaki.miyazaki.jp （ＬＧＷＡＮ）　03jyouho@city.miyazaki.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。	情報政策担当部長	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	情報セキュリティ責任者をもって充てる。	各所管部局長	CSIRT責任者が不在の場合に権限を引き継ぐ。
ＣＳＩＲＴ管理者	ネットワーク管理者をもって充てる。	情報政策担当課長	インシデント対応の統括リーダー。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。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。
インシデント対応管理者	情報システム管理者をもって充てる。※各課所管システムでのインシデント時のみ設置	各所管課長	インシデント対応の実務管理者。CSIRT管理者からの支援を受けながら、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CSIRT副責任者等の関係者に提供する。
インシデントハンドラー	情報システム統括担当者をもって充てる。	情報政策担当係長	インシデント対応の実務リーダー。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。
CSIRT要員	情報システム担当者の中からCSIRT管理者が指名する者		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）、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を行う。
内部関係者	財政部門		インシデントハンドリングにおける予算対応等を行う。
	法務部門		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）等を行う。
	広報部門		インシデントハンドリングにおけるマスコミ対応等を行う。
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CSIRT責任者が支援を要請する者		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作業を行う。
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を行う。

別図　ＣＳＩＲＴ体制　（イメージ）



附　則

この要綱は、平成２８年３月３１日から施行する。

附　則

この要綱は、令和５年３月１日から施行する。