令和７年設楽町訓令第３号

庁中一般
出先機関一般

設楽町 CSIRT 設置要綱を次のように定める。

令和７年１２月２２日

設楽町長　土 屋　　浩

設楽町訓令第３号

設楽町CSIRT設置要綱

（設置）

第１条　設楽町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、設楽町CSIRT(Computer Security Incident Response Team)(以下「CSIRT」という。)を設置する。

（役割）

第２条　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。

(PoC)

第３条　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(別表第１)、庁内外に周知、公表するものとする。

(対象インシデント)

第４条　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)

(体制)

第５条　CSIRT の体制は次のとおりとする。

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

(2)　CSIRT は、CSIRT 責任者、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、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(別表第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。

附　則

この訓令は、令和８年１月１日から施行する。

別表第１(第３条関係)　PoC

PoC	設楽町 CSIRT　(総務課)
所在地	愛知県北設楽郡設楽町田口字辻前 14 番地
対応時間	平日　8 時 30 分から 17 時 15 分まで
電話番号	0536-62-0511
FAX 番号	0536-62-1675
メール	(LGWAN・インターネット)somu@town.shitara.lg.jp

別表第 2(第 5 条関係)　CSIRT 構成

構成		担当	役割
CSIRT 責任者	最高情報セキュリティ責任者	副町長	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	統括情報セキュリティ責任者をもって充てる。	総務課長	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責任者をもって充てる。	総務課長	チームのリーダー。情報セキュリティインシデントハンドラーの作業を調整し、情報セキュリティインシデントハンドラーからの情報を収集し、情報セキュリティ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。情報セキュリティインシデント対応チーム全体の技術的な作業を監督し、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の中から CSIRT 責任者が指名する者。	総務課 課長補佐	情報セキュリティインシデント発生時の、情報セキュリティ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、情報セキュリティインシデントに対応する CSIRT を、中核として支え、対応方針を検討し、情報セキュリティ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	総務課 情報担当	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

	名する者。		
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 課長補佐	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 課長補佐	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	総務課 課長補佐	インシデントハンドリングにおけるマスコミ対応等
外部の専門家	セキュリティベンダー、NISC、IPA、JPCERT／		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

	CC、警察等から CSIRT 責任者が支援を要請する者。		討等に係る作業
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

別図(第 5 条関係)　CSIRT 体制(イメージ)