むつ市ＣＳＩＲＴ設置要綱

令和２年４月１日
むつ市告示第１１６号

（設置）

第１条　むつ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、むつ市電子自治体推進会議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、むつ市ＣＳＩＲＴ（Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍをいう。以下同じ。）を設置するものとする。

（役割）

第２条　むつ市ＣＳＩＲＴの役割は、次のとおりとする。

⑴　インシデント発生時の対応

ア　検知及び連絡受付

インシデントの発生に関する予兆等の検知及び発見並びに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又は分析により判断し、被害状況、影響範囲等の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、確保及び記録並びにインシデントの封じ込め及び根絶）の実施、復旧措置（暫定対策）の実施及び再発防止策の検討を行う。

エ　報告及び公表

被害状況、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、青森県、内閣サイバーセキュリティセンター（ＮＩＳＣ）、警察機関等）への報告及び対外的な対応（報道発表及び関係住民への連絡）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。

⑵　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及び予防

イ　インシデントの発生を想定した訓練及び演習の定期的な実施

ウ　インシデントの対応に関する手順等の定期的な評価及び見直し

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い、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をいう。）（別表第１）を整備し、庁内外に周知及び公表するものとする。

（対象インシデント）

第４条　むつ市ＣＳＩＲＴが扱うインシデントは、別表第２のとおりとする。

（体制）

第５条　むつ市ＣＳＩＲＴの体制は、別表第３のとおりとする。

附　則

この要綱は、令和２年４月１日から施行する。

別表第１（第３条関係）

ＰｏＣ	むつ市ＣＳＩＲＴ（総務部総合情報課）
所在地	青森県むつ市中央一丁目８番１号
対応時間	平日　８時３０分～１７時１５分
電話番号	０１７５－２２－１１１１　内線２１４１
メール	（ＬＧＷＡＮ・インターネット） ｊｏｈｏ＠ｃｉｔｙ．ｍｕｔｓｕ．ｌｇ．ｊｐ
確認項目	①事象を発見した日時（いつ） ②事象を発見したサイト又は場所（どこで） ③発見した内容（何がどのように） ④発見者の氏名・連絡先

別表第２（第４条関係）

情報システムの停止等	情報システム、ネットワーク、サーバ及び端末の利用に支障をきたす状態をいう。
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をいう。
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）の盗難若しくは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。）をいう。

別表第３（第５条関係）

構成		役割
ＣＳＩＲＴ責任者	統括情報セキュリティ責任者（総務部長）	インシデント対応の総責任者。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や他の組織等との調整役となり、危機を打開し、チームに必要な要員、リソース及び技能を確保する。
ＣＳＩＲＴ副責任者	情報セキュリティ責任者（市長部局の長、行政委員会事務局等の長等）	所管する部局等のインシデント対応について、ＣＳＩＲＴ管理者からの情報を収集し作業を監督する。ＣＳＩＲＴ責任者が不在の場合に権限を引き継ぐ。
ＣＳＩＲＴ管理者	情報システム管理者（各情報システムの担当課室長等）	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。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。
ＣＳＩＲＴ要員	担当課室職員	ＣＳＩＲＴ管理者を補助し、ともにインシデント対応に当たる。
インシデントハンドラー	総合情報課長	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。
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）、インターネットに接続するサービスを提供する事業者（ＩＳＰ）、インターネット等を通じてソフトウェアを利用するサービスを提供する事業者	検査、分析、証拠の取得、保全、確保及び記録、インシデントの封じ込め及び根絶、復旧措置、再発防止策の検討等に係る一部作業を行う。

	（ＡＳＰ）、クラウド事業者等の契約関係のある外部の事業者であって、ＣＳＩＲＴ責任者が支援を依頼する者	
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。
	総務部門	インシデントハンドリングにおける法的対応等を行う。
外部の専門家	セキュリティベンダー、ＮＩＳＣ、ＩＰＡ、ＪＰＣＥＲＴ／ＣＣ、警察等のうちＣＳＩＲＴ責任者が支援を要請する者	検査、分析、証拠の取得、保全、確保及び記録、インシデントの封じ込め及び根絶、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	左記により要請等された作業を行う。