船橋市ＣＳＩＲＴ設置要綱

令和４年４月１日

（趣旨）

第１条　この要綱は、「船橋市情報セキュリティ対策基準」2.(10)ＣＳＩＲＴの設置・役割の規定に基づき、船橋市情報セキュリティポリシーの適用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、船橋市CSIRT（以下「CSIRT」という。）を設置し、その役割及び体制等の基本的事項について定める。

（役割）

第２条　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・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、千葉県、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。

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・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改ざん等の発生又は発生が疑われる状態
盗難・紛失	船橋市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。

⑴　ＣＩＳＯは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。

⑵　ＣＳＩＲＴは、ＣＳＩＲＴ責任者、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、インシデント対応要員、外部委託事業者をもって構成し、その構成及び役割はＣＳＩＲＴ構成表（別表２）のとおりとする。

⑶　外部委託事業者については、インシデント対応要員が依頼し、外部の専門家等については、必要に応じてＣＳＩＲＴ責任者が関係機関に依頼するものとする。

⑷　ＣＳＩＲＴ体制は別図のとおり。

附　則

この要綱は、令和元年１１月１日から施行する。

附　則

この要綱は、令和４年４月１日から施行する。

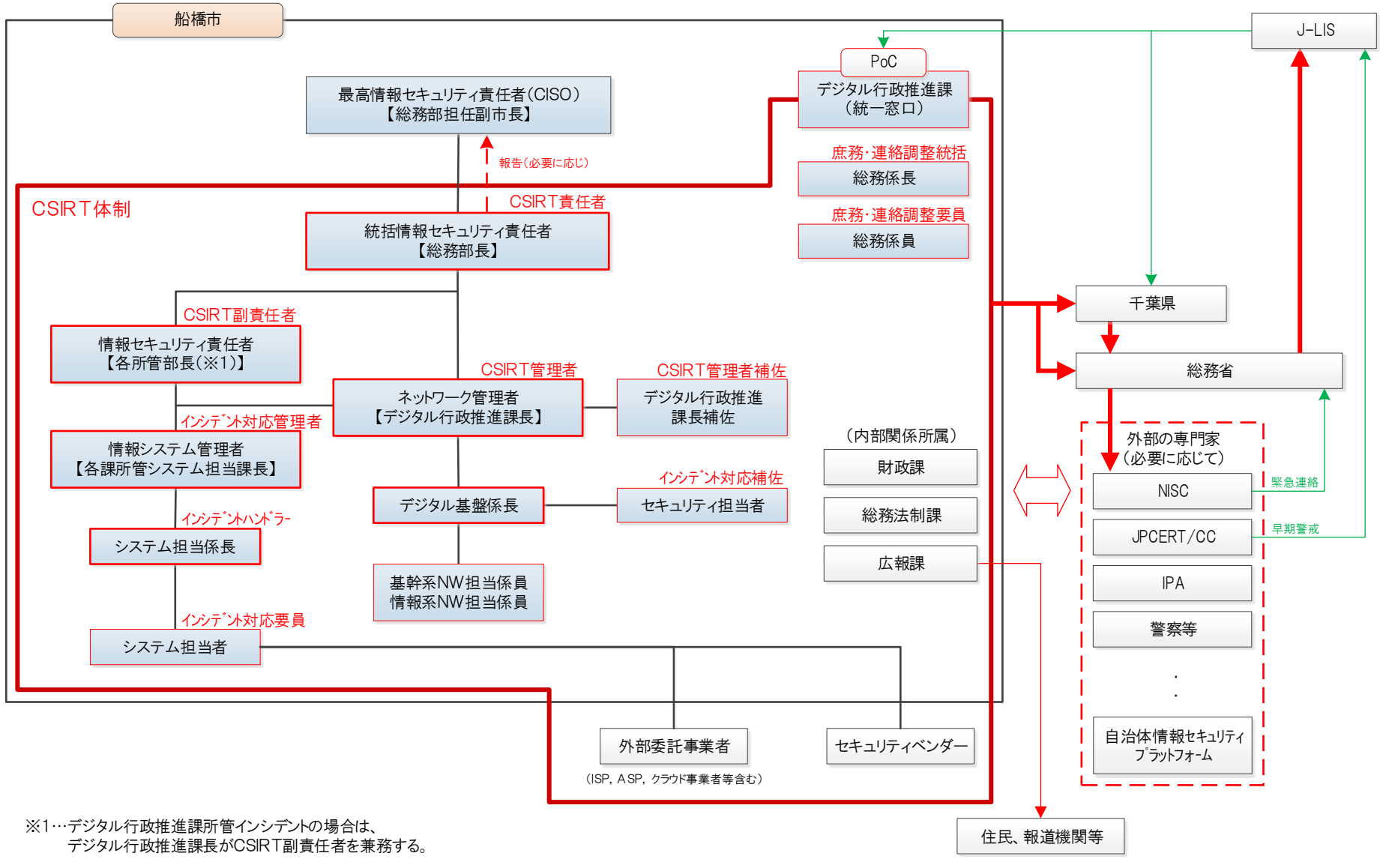
別表１　ＰｏＣ（統一的窓口）（第３条関係）

ＰｏＣ	船橋市ＣＳＩＲＴ（総務部デジタル行政推進課）
所在地	千葉県船橋市湊町２－１０－２５
受付時間	平日９時００分～１７時００分（メールは２４時間受付）
電話番号	０４７－４３６－２０７２
メール	funa-csirt@city.funabashi.lg.jp

別表２　ＣＳＩＲＴ構成表（第５条関係）

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。	総務部長	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、ＣＳＩＲＴに必要な要員・リソース・技能を確保する。
ＣＳＩＲＴ副責任者	各課所管インシデント	情報セキュリティ責任者をもって充てる。	各所管部長	ＣＳＩＲＴ責任者を補佐する。ＣＳＩＲＴ責任者が不在の場合は権限を引き継ぐ。
	デジタル行政推進課所管インシデント	ネットワーク管理者をもって充てる。	デジタル行政推進課長	
ＣＳＩＲＴ管理者		ネットワーク管理者をもって充てる。	デジタル行政推進課長	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。また、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。
インシデント対応管理者（※）各課所管インシデント時のみ役割設置		情報システム管理者をもって充てる。	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		インシデント対象のシステム等を所管する担当係長をもって充てる。	各所管係長	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、関係部署への応援依頼や調整を行う等、インシデント対応を実務的な観点から中核として支え、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。
インシデント対応要員		情報システム担当者等適任者を情報セキュリティ管理者が指名する。	各担当者	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。
外部委託事業者等		システムベンダー（開発、運用・保守事業者のほか、セキュリティ支援事業者等）との契約関係に基づき、ＣＳＩＲＴ責任者が支援を依頼する者。 セキュリティベンダー。	各ベンダー	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	財政課	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	総務法制課	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）等を行う。
	広報部門	広報課	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。
関係機関（CSIRT 体制範囲外）			
外部の専門家	ＮＩＳＣ、ＩＰＡ、ＪＰＣＥＲＴ/ＣＣ、警察等からＣＳＩＲＴ責任者が支援を要請する者。	各機関	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責任者が報告または支援を要請する者。		左記にて要請等をされた内容を行う。



※1…デジタル行政推進課所管インシデントの場合は、
デジタル行政推進課長がCSIRT副責任者を兼務する。