庁内ＣＳＩＲＴ設置要綱

埼玉県情報セキュリティポリシーに規定する庁内ＣＳＩＲＴ（Computer Security Incident Response Team（シーサート）：情報セキュリティインシデント対応チーム）の詳細について下記のとおり定める。

記

１　庁内ＣＳＩＲＴの体制

庁内ＣＳＩＲＴの体制は次のとおりとし、庁内ＣＳＩＲＴの事務局を情報システム戦略課に置く。

（１）最高情報セキュリティ責任者（ＣＩＳＯ）の指揮のもと庁内にＣＳＩＲＴを設置し、ＣＳＩＲＴ責任者を置く。

（２）ＣＳＩＲＴ責任者は、情報セキュリティ運営管理者（情報システム戦略課長）をもって充てる。

（３）庁内ＣＳＩＲＴは、ＣＳＩＲＴ責任者のほか、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、外部専門家をもって構成する。その構成及び役割は別表１のとおりとする。

（４）外部委託事業者、外部専門家については、必要に応じＣＳＩＲＴ責任者が関係機関と調整のうえ定めるものとする。

２　役割

庁内ＣＳＩＲＴの役割は次のとおりとする。

（１）検知・連絡受付

業務に影響を与えたり情報セキュリティを脅かしたりする事件や事故（以下「情報セキュリティインシデント」という。）の発生に関する予兆等の検知、発見、情報セキュリティインシデントに関わる連絡・報告等の受付を行う。

（２）検査・分析

ア．事実関係を確認の上、情報セキュリティ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、情報セキュリティインシデントの処理に優先順位を付ける。

イ．ＣＩＳＯが「県民の生活や行政運用に重大な影響を与えるおそれがある情報セキュリティインシデント」と判断した場合（レベル３）及び「県民の生活や行政運用に重大な影響を与える情報セキュリティインシデント」と判断した場合（レベル４）は、次の（３）から

（５）の活動を行う。

ウ．情報セキュリティインシデントの影響が軽微又は一部に限定されると判断した場合（レベル２まで）は、通常業務の範囲内で対応する。

エ．影響度の判定基準は別表２に定める。

（３）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・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。

なお、ＣＩＳＯが初動対応としてインシデントの封じ込めのため必要と判断した場合にはネットワークからの切断を行う。

（４）報告・公表

被害状況や影響範囲等に応じ、内外の関係者（ＣＩＳＯ）、総務省、県警等）への報告及び対外的な対応（報道発表）を行う。

（５）事後対応

情報セキュリティインシデントの収束宣言を行い、報告書をまとめる。

（６）対応計画

情報セキュリティインシデントに係る対応計画を作成し、迅速かつ適切な行動につなげる。

３　連絡窓口（Point of Contact：ＰｏＣ）

情報セキュリティインシデントについて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（ポック）を定め、各課所に周知、公表するものとする。

ＰｏＣは、ＣＳＩＲＴ責任者が別に定める。

４　対象とする情報セキュリティインシデント

庁内ＣＳＩＲＴが扱う情報セキュリティインシデントは埼玉県情報セキュリティポリシーに規定する次の脅威に起因するものとする。

部外者の侵入、不正アクセス、コンピュータウイルス、サービス不能攻撃、標的型攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去等の発生又は発生が疑われる状態

５　附則

この要綱は、平成 28 年 10 月 14 日から施行する。

この要綱は、令和３年４月１日から施行する。

別表１　庁内 CSIRT 構成表

構成	担当	役割
CISO	企画財政部部長	CSIRT の指揮を行う。 情報セキュリティインシデントの影響度の判断を行う。 ネットワークからの切断の判断を行う。
CSIRT 責任者	情報システム戦略課長	情報セキュリティインシデント対応の責任者。情報セキュリティインシデント対応の作業全体を監督し評価する責任を負う。また、CISO や他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	情報システム戦略課副課長	CSIRT 責任者が不在の場合に権限を引き継ぐ。 また、報告・公表の役割を担う。
CSIRT 管理者	情報システム戦略課担当主幹	チームのリーダー。インシデントハンドラーの作業を監督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。ＣＳＩＲＴ全体の技術的な作業品質を確保・評価する責任を負う。
インシデントハンドラー	情報システム戦略課担当主査	情報セキュリティインシデントの分析及び対処法の検討、関係部署との調整を行う。CSIRT の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マネジメントを行う。
CSIRT 要員※	情報システム戦略課担当者 企業局担当職員 下水道局担当職員 議会事務局担当職員 教育局担当職員 その他必要と思われる関係者	インシデントハンドラーと協調してインシデント対応を行う。

外部委託事業者	県庁 LAN 保守事業者等	検査・分析、証拠の取得・保全・記録、情報セキュリティ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。
外部専門家	セキュリティベンダー	情報セキュリティ関連の専門知識・ノウハウを生かして、CSIRT が適切に機能するよう職員に対する支援を行う。 専門的見地から、検査・分析、証拠の取得・保全・記録、情報セキュリティ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。

※CSIRT 要員のうち、情報システム戦略課担当者以外の各局の要員は各局内の ICT 担当職員とし各局で選定する。

別表２

影響度の判定基準

影響度	判定基準	事例
レベル０	情報セキュリティインシデントの影響がない	過誤検知等を含むヒヤリハット
レベル１	情報セキュリティインシデントの影響が軽微な場合	・スタンドアロンで利用している端末機へのウイルス感染 ・記録媒体内のウイルス感染等
レベル２	情報セキュリティインシデントの影響が一部に限定される場合	・ネットワーク接続している端末機がウイルス感染したが他のシステム、端末機に影響していないもの ・CD、USB 等の外部記憶媒体経由によりウイルス感染拡大のおそれがある場合
レベル３	情報セキュリティインシデントが県民の生活や行政運用に重大な影響を与えるおそれがある場合	・ネットワーク接続の情報機器がウイルス感染し、広範な情報機器に感染のおそれがある場合 ・情報漏えいの可能性がある場合　等
レベル４	情報セキュリティインシデントが県民の生活や行政運用に重大な影響を与える場合	・ネットワーク接続の情報機器がウイルス感染し、更に広範な情報機器に感染した場合 ・長期間にわたりシステム又はネットワークを停止する必要がある場合 ・情報漏えいが確認された場合