一般社団法人つくばスマートシティ協議会　CSIRT 設置要項

令和６年４月１日制定

（設置）

第１条　一般社団法人つくばスマートシティ協議会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と、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専門的知見及び情報の収集力等を具備した緊急即応チームとして、一般社団法人つくばスマートシティ協議会 CSIRT（Computer Security Incident Response Team：シーサート、以下「CSIRT」という。）を設置するものとする。

（定義）

第２条　この要項において使用する用語の意義は、一般社団法人つくばスマートシティ協議会情報セキュリティポリシーの例による。

（体制）

第３条　CSIRT の体制は、次に掲げるとおりとする。

（１）　CSIRT は、CSIRT 責任者、CSIRT 管理者、インシデントハンドラー、CSIRT 要員、外部委託事業者及び外部の専門家をもって構成し、その構成及び役割は別表第１のとおりとする。

（２）　外部委託事業者及び外部の専門家については、必要に応じて CSIRT 責任者又は CSIRT 管理者が関係機関に支援を要請することによって定めるものとする。

（役割）

第４条　CSIRT の役割は、次に掲げるとおりとし、総称してインシデントマネジメントという。

（１）　平常時の事前準備及び予防等

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の実施

イ　インシデントの発生を想定した訓練又は演習等の定期的な実施

ウ　インシデントの対応手順等の定期的な評価及び見直しの実施

エ　その他 CSIRT 責任者又は CSIRT 管理者が定める事項の実施

（２）　インシデント発生時及び事後の対応（以下「インシデントハンドリング」という。）

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、発見及びインシデントに関わる連絡等の受付を行う。

イ　優先順位の設定（「トリアージ」という。）

事実関係を確認した上でインシデント発生の有無を判断し、必要に応じて注意喚起等の情報発信を行うとともに、インシデントの処理に優先順位を設定する。

ウ　実務的な対応（「インシデントレスポンス」という。）

インンシデントの検査、分析、対応方針の検討、拡大防止及び根絶、証拠の取得及び記録、復旧措置等から再発防止策の検討までを実施する。

エ　報告及び公表

被害状況や影響範囲等に応じて、CISO、つくば市 CSIRT、警察等の関係機関へ報告する。また、報道発表や関係住民への連絡等対外的な対応を行う。

オ　事後対応

インシデントの収束を確認し、インシデントハンドリングの記録を作成する。

（統一的な窓口の設置）

第５条　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）を別表第２のとおり設置し、インシデントに関する連絡受付の役割を担うものとする。

（対象インシデント）

第６条　CSIRT が扱うインシデントは、次の各号に掲げるものとする。

（１）　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をいう。ただし、メンテナンス等による計画停止は、除くものとする。

（２）　サイバー攻撃　コンピュータウイルス等の感染、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の改ざん等の発生又は発生が疑われる状態をいう。

（３）　盗難又は紛失　業務情報の盗難若しくは紛失の発生又は発生が疑われる状態をいう。これらは、第三者による被害のほか職員の犯行に起因するものを含むものとする。ただし、紙媒体の盗難又は紛失については、発生の原因に情報システムの設定不良又は不具合等を含むもののみとする。

附　則

この要項は、令和６年４月１日から施行する。

別表第１（第３条関係）

構成		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。	インシデントマネジメントの各作業を監督し評価する責任を負う。また、CISO 及び関係機関等との調整を行う。CSIRT に必要な要員、リソース及び技能を確保する。
CSIRT 管理者	情報管理者をもって充てる。	インシデントハンドラーの作業を調整する。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、CSIRT 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。
インシデントハンドラー	CSIRT 管理者が指名する者をもって充てる。	インシデントの分析及び対処法の検討、関係者等との調整を行う。CSIRT において実務的な中核となり、対応方針の検討等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	書記等のうち、CSIRT 管理者が指名する者をもって充てる。	インシデントハンドラーを補助し、インシデント対応に当たる。
外部委託事業者	開発事業者、運用保守事業者、ISP、ASP 及びクラウド事業者等一般社団法人つくばスマートシティ協議会と契約関係のある事業者のうち、CSIRT 責任者又は CSIRT 管理者が支援を要請する者をいう。	検査及び分析、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、復旧措置及び再発防止策の検討等に係る一部作業を担う。
外部の専門家	セキュリティベンダー、NISC、IPA、JPCERT/CC 及び警察等のうち、CSIRT 責任者又は CSIRT 管理者が支援を要請する者をいう。	検査及び分析、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、復旧措置及び再発防止策の検討等に係る一部作業を担う。
その他	上記のほか CSIRT 責任者又は CSIRT 管理者が必要によって支援を要請する者	CSIRT 責任者又は CSIRT 管理者から要請された内容を担う。

別表第２（第５条関係）

PoC	一般社団法人つくばスマートシティ協議会 CSIRT （政策イノベーション部科学技術戦略課内）
所在地	茨城県つくば市研究学園一丁目１番地１
電話番号	029-883-1312
ＦＡＸ番号	029-868-7640
メール	tkb.sc298@gmail.com