一般社団法人つくばスマートシティ協議会
情報セキュリティ緊急時対応計画

一般社団法人つくばスマートシティ協議会
令和６年４月策定

目次

1　目的

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。）の発生又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及び各要項への違反等により、情報資産に対するセキュリティ侵害事案が発生した場合において、連絡、証拠保全、被害拡大の防止、復旧及び再発防止等の措置を迅速かつ適切に実施することで、被害の最小化又は未然防止を図ることを目的とする。

2　用語に関する定義

本計画において使用する用語は、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及び一般社団法人つくばスマートシティ協議会 CSIRT 設置要項の例による。

3　対象とするインシデント

本計画で対象とするインシデントは、一般社団法人つくばスマートシティ協議会 CSIRT 設置要項に準じ、次のとおりとする。

（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

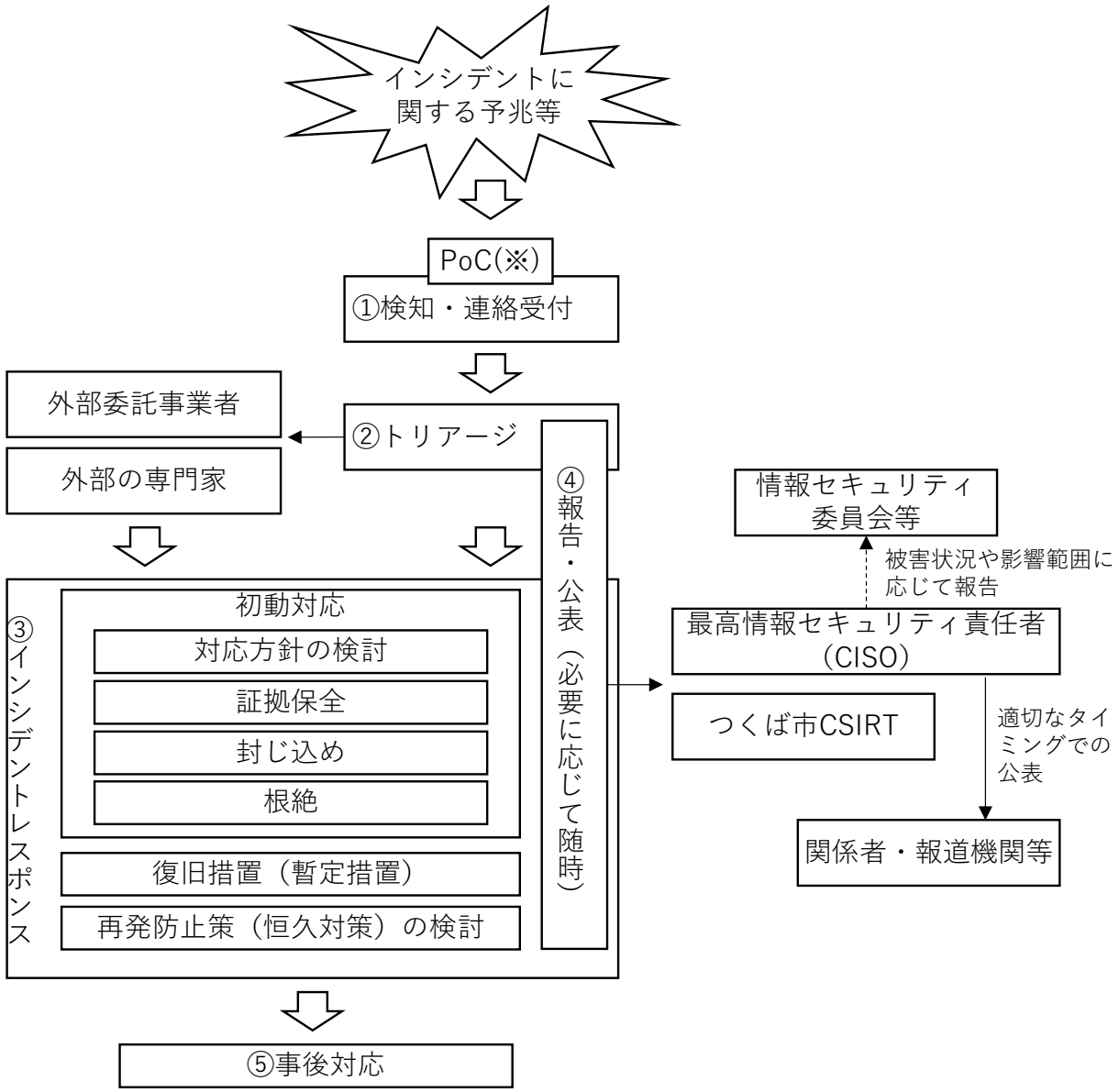
業務情報の盗難又は紛失の発生、又は発生が疑われる状態をいう。これらは、第三者による被害のほか職員の犯行に起因するものを含むものとする。た

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。

4　インシデントハンドリングについて

（1）インシデントハンドリングの概略

対応フローは次のとおりとする。



※PoC（Point Of Contact）：情報セキュリティに関する統一的な窓口の連絡先

（２）インシデントハンドリングの具体的手順

① 検知又は連絡受付

CSIRT 要員は、PoC（下表参照）に寄せられたインシデントに関わる連絡及び通報等を受け付ける。また、連絡及び通報を受け付けた時点から、当該インシデントにおいて発生した事象及びそれに対する CSIRT の対応について、時系列順に記録を行うこととする。

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
メール	tkb.sc298@gmail.com

② トリアージ

（Ｉ）CSIRT 要員は、通報の種類に応じて下表のとおり事実関係の確認を行い、必要に応じて外部委託事業者及び外部の専門家と協力してログ等の検査及び分析を行う。

通報の種類	事実関係の確認の方法
職員等からの通報	通報者へヒアリングを行い、インシデントの兆候を発見した経緯及び当該情報システムやネットワーク状況（電源や LAN ケーブル等の接続を含む）を確認する。
庁内システム等からのアラート	警報又はアラート等を発した機器及び情報システムを特定し、当該機器及び情報システムの運用・保守等を担当している外部委託事業者に問い合わせる。

市民等からの通報	通報が虚偽でないことを確認するため、通報者の連絡先を控え、折り返しの連絡を行う。通報者が組織の場合は組織の代表番号を調べ、折り返しの連絡を行う。メールで通報があった場合も、通報者の電話番号を確認し、電話連絡にて確認を行う。虚偽がなく正しい通報であることが確認されたら、内容の具体的なヒアリングを行う。
つくば市、都道府県、国、自治体セプター（J-LIS）等からの通報	電話による通報の場合は、上記の方法に準じて、通報が虚偽でないことを確認する。メールによる通報の場合は、上記の方法に準じて、正しい通報であることを確認する。虚偽がなく正しい通報であることが確認されたら、内容の具体的なヒアリングを行う。

（Ⅱ）インシデントハンドラーは、通報及びCSIRT要員が行った事実確認によって得られた情報に基づき、インシデント判断基準表（別表１）を参考にインシデント発生の有無を判断する。インシデントの発生と判断した場合は、被害状況や影響範囲等に応じてインシデントの処理に優先順位を付ける。CSIRT のみでは優先順位の判断が困難な場合は、外部委託事業者及び外部の専門家に情報提供等の協力を依頼する。

（Ⅲ）インシデントハンドラーは、トリアージの時点でインシデントの発生は無いと判断した場合、当該事案をCSIRTで取り扱わないことをCSIRT管理者に報告する。CSIRT 管理者は、通報者へトリアージ結果の連絡を行い、必要に応じて職員への注意喚起等を行う。

③ インシデントレスポンス

（Ⅰ）初動対応（対応方針の検討、証拠保全、封じ込め及び根絶）の実施

（ア）インシデントハンドラーは、外部委託事業者等と連携し、また、必要に応じて外部の専門家等と協力して対応方針を検討し、CSIRT 管理者及び CSIRT 責任者に報告する。対応方針の検討については、下表の項目について留意する。

対応方針検討における留意事項
・インシデントの影響範囲及び損害規模の把握 ・対応に要する時間の見積り及び復旧のスケジュール確認 ・対応に必要な人員及び人材の確保 ・必要なコストの積算及びそれに対する予算措置 ・連絡や通知をする必要がある機関の確認及び外部への報告対応

（イ）　CSIRT 管理者は、必要に応じて外部委託事業者及び外部の専門家等に作業の依頼や協力等の要請を行う。

（ウ）インシデントハンドラーは、対応方針に基づき、必要に応じて外部委託事業者及び外部の専門家等と連携して、証拠の取得、保全及び記録を行い、インシデントを封じ込め、根絶する。具体的な手順は下表のとおりとする。

対応項目	対応方法
証拠保全	インシデントに関わる情報システム機器（端末、サーバ及びネットワーク機器等）に残されているログ及び証跡等を収集し、取得する。
封じ込め	被害の拡大を防ぐため、インシデントの内容に応じて、インシデントに関わる情報システム機器の稼働停止、ネットワークの遮断及び隔離等の作業を行う。その際、証拠保全の作業に影響が出ないよう留意する。

根絶	インシデントの内容に応じて、情報システムの脆弱性の修正及び設定の見直し、ウイルス駆除、不適切なデータ及び構成要素の削除等の作業を行い、インシデントの原因を根絶する。

（Ⅱ）復旧措置（暫定対応）の実施

（ア）インシデントハンドラーは、対応方針に基づき、外部委託事業者及び外部の専門家等と連携して、影響を受けたシステムを運用可能な状態に戻し、正常に機能していることを確認の上、インシデントから復旧させる。復旧方法については下表のとおりとする。

被害状況	復旧方法
修復可能な場合	インシデント発生以前のバックアップ等によって修復が可能な場合は、バックアップにインシデントの原因が含まれていないことを調査の上、これを利用して修復を行う。
修復不可能な場合	バックアップ等の不備、あるいはバックアップでも修復不可能な被害の場合は、新規に情報システム等を構築する。その際、新規システム構築期間中の代替策についても検討を行う。

（イ）復旧後、必要と認められる期間、インシデントの再発及び関連活動の有無について監視を行う。

（Ⅲ）再発防止策（恒久対策）の検討

（ア）インシデントハンドラーは、当該インシデントに係る調査を実施し、情報セキュリティポリシー及び各要項の見直しを含め、再発防止策を検討し、CSIRT 管理及び CSIRT 責任者に報告する。

（イ）CSIRT 責任者は、再発防止策を最高情報セキュリティ責任者（以下「CISO」という。）へ報告する。

④ 報告・公表

（Ⅰ）インシデントハンドラーは、トリアージの結果、対応方針の変更及び対応状況の進捗等については、適宜、CSIRT 管理者及び CSIRT 責任者に報告する。

（Ⅱ）CSIRT 責任者は、被害状況や影響範囲に応じて CISO へ報告する。

（Ⅲ）CSIRT 責任者又は CSIRT 管理者は、職員等に速やかに情報提供すべきと判断した場合は、注意喚起などの周知を行う。必要に応じて、つくば市 CSIRT その他の関係者への連絡及び報道機関等への公表を行う。

⑤ 事後対応

（Ⅰ）CSIRT 責任者は、インシデントの収束を確認し、CISO に報告する（報告様式１）。

（Ⅱ）CSIRT 責任者は、当該インシデントハンドリングの内容について、通報からトリアージ及びインシデントレスポンスまでの一連の過程及び手順の評価を行い、その結果を記録する。

（Ⅲ）CISO は、情報セキュリティ委員会（以下「委員会」という。）を開催し、当該インシデントの発生から収束までの一連の過程及び再発防止策等を報告し、委員会の承認を得る。

5　平常時の事前準備・予防等

（1）事前準備及び予防等

取得されているログの種類及び内容や外部委託事業者との契約内容といった、インシデント発生時に必要な情報又は適用されている予防策等は、あらかじめ確認しておくこととする。

① 連絡体制の整備と保守

CSIRT 体制の発動時に備えて、関係連絡先一覧を作成し、最新の状態を維持しておく。

② インシデントの検査・分析に必要な情報の精査

システムやネットワーク構成図等は最新の状態を維持し、インシデント発生時に迅速に対応できるよう備える。また、現状の情報システムで取得できるログの種類を確認し、インシデント発生時に不足が生じることが考えられる場合は、情報システムの管理者又は外部委託事業者等と連携し対応を検討する。ログが適正に取得されているかの管理や、インシデント発生時のログ採取手順の確認についても、平常時から行っておく。

③ 外部委託事業者との契約内容の確認

インシデント発生時に、外部委託事業者との契約内容を確認し、依頼できる作業内容及び責任範囲をあらかじめ明確にしておく。

（2）訓練・演習

インシデント発生時に CSIRT 体制が適切に機能するよう、また、その対応力の向上に向け、インシデントの発生を想定した訓練や演習を定期的に実施することとする。

（3）評価・見直し

インシデント発生時の対応手順等は、情報セキュリティに関する脅威や技術等の変化に対応するため自己点検を行い、訓練や演習等の結果等と併せ定期的に評価及び見直しを行うこととする。

一般社団法人つくばスマートシティ協議会
情報セキュリティ緊急時対応計画

別添

別表１ インシデント判断基準表

（１）情報システムの停止等に係る判断基準表

影響度	判断基準	事例
レベル 0	インシデントとはみなさない	・端末単体の障害（ネットワーク及びハードウェア障害等） ・情報システムの一時的又は局地的な障害で、職員の業務及びサービスに影響が無い又は影響が及ぶ前に復旧が可能なもの ・通信回線業者側の一時的又は局地的なネットワーク障害で、職員の業務及びサービスに影響が無い又は影響が及ぶ前に復旧が可能なもの ・雷による一時的な停電　等
レベル 1	軽微なインシデントとみなすもの	・情報システム等の障害で、サービスには影響が無いが、一部職員の業務に影響を及ぼすもの ・情報システム等の障害で、他の情報資産に影響を及ぼすことがないもの ・フロア又は建物全体の一時的な電源障害 ・一部の電源系統の障害　等
レベル 2	重大なインシデントとみなすもの	・情報システムの障害で、職員全体及びサービスに影響を及ぼす可能性のあるもの ・情報システムの障害で、他の情報資産に影響を及ぼす可能性のあるもの ・長期間に渡り情報システム又はネットワークを停止する必要があるもの ・長時間の停電　等

（２）サイバー攻撃に係る判断基準の事例

影響度	判断基準	事例
レベル 0	インシデントとはみなさない	・ウイルスを検知したが、端末のウイルス対策ソフトが駆除した場合　等

レベル 1	軽微なインシデントとみなすもの	・サイバー攻撃の形跡が検知されたが、セキュリティ対策機器やソフトウェア等で駆除した場合 ・スタンドアロンで利用している端末へのウイルス感染 ・記録媒体内のウイルス感染 ・ネットワーク接続している端末にウイルス感染したが他の情報システムや端末に影響していないもの　等
レベル 2	重大なインシデントとみなすもの	・情報システム等から外部に向けた攻撃を行っている形跡が確認された場合 ・ウイルス感染した記録媒体を介して、情報システム等に感染又は感染のおそれがある場合 ・ネットワーク接続機器がウイルス感染し、広範な情報に感染又は感染のおそれがある場合 ・サイバー攻撃やウイルス感染により、長期間にわたり情報システム等を停止する必要がある場合 ・情報漏えいの可能性がある場合　等

（3）盗難又は紛失に係る判断基準の事例

影響度	判断基準	事例
レベル 0	インシデントとはみなさない	・情報を紛失したが、紛失後すぐに他者への漏えいの危険が無い場所で発見された場合　等
レベル 1	軽微なインシデントとみなすもの	・情報を保管していない情報機器又は記録媒体の盗難又は紛失が発生した場合 ・職員の業務又はネットワークの稼働に影響の無い機器の盗難又は紛失が発生した場合

		・個人情報を含まない情報であるが、業務上知る必要のない職員がアクセスできる状態になっていた場合 ・個人情報又は業務情報とは関係のない情報を含んだ記録媒体を持ち出した場合 ・暗号化等の情報漏えい対策がされている情報機器又は記録媒体の盗難又は紛失が発生した場合 ・暗号化されている情報の漏えい ・職員等の機微でない個人情報の漏えい等
レベル 2	重大なインシデントとみなすもの	・職員の業務又はネットワーク稼働に影響がある機器の盗難又は紛失が発生した場合 ・暗号化していない個人情報及び業務情報等の重要な情報を保管している情報機器又は記録媒体の盗難又は紛失が発生した場合 ・個人情報又は業務情報等の重要な情報で、業務上知る必要のない職員がアクセスできる状態になっていた場合 ・個人情報の漏えい ・重要なシステム又はネットワークの設計書等の漏えい　等

報告様式１

〇〇年〇〇月〇〇日

最高情報セキュリティ責任者（CISO）様

統括情報セキュリティ責任者

（CSIRT 責任者）

情報セキュリティインシデント事案の発生について（報告）

このことについて、業務において〇〇〇〇〇の事案が発生したため、下記のとおり報告いたします。

記

１ 事案の状況

（１）発生した事案の種類

（２）発生日時

（３）発生場所

（４）発生した事案の概要

２　事案が発生したサービスの概要及び影響並びに情報システムの概要

３　事案が発生した原因（及び原因として想定される行為）

４　確認した被害状況及び影響範囲（損害規模）

5　対応状況（初動対応、復旧措置（復旧状況及び見込み、復旧に要する額等））

6　再発防止策（恒久対策）

7　対外的な対応（報道発表、住民への連絡、総務省、警察機関等）

8　その他（時系列の対応記録等）

（参考１）インシデント発生時の報告・指示体制図