宮崎市情報セキュリティ
緊急時対応計画

平成２８年３月３１日策定

（令和５年３月１日最終改定）

宮　崎　市

第１　計画の目的

情報セキュリティインシデント、宮崎市情報セキュリティポリシー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又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、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。

第２　本計画で対象とする情報セキュリティインシデント

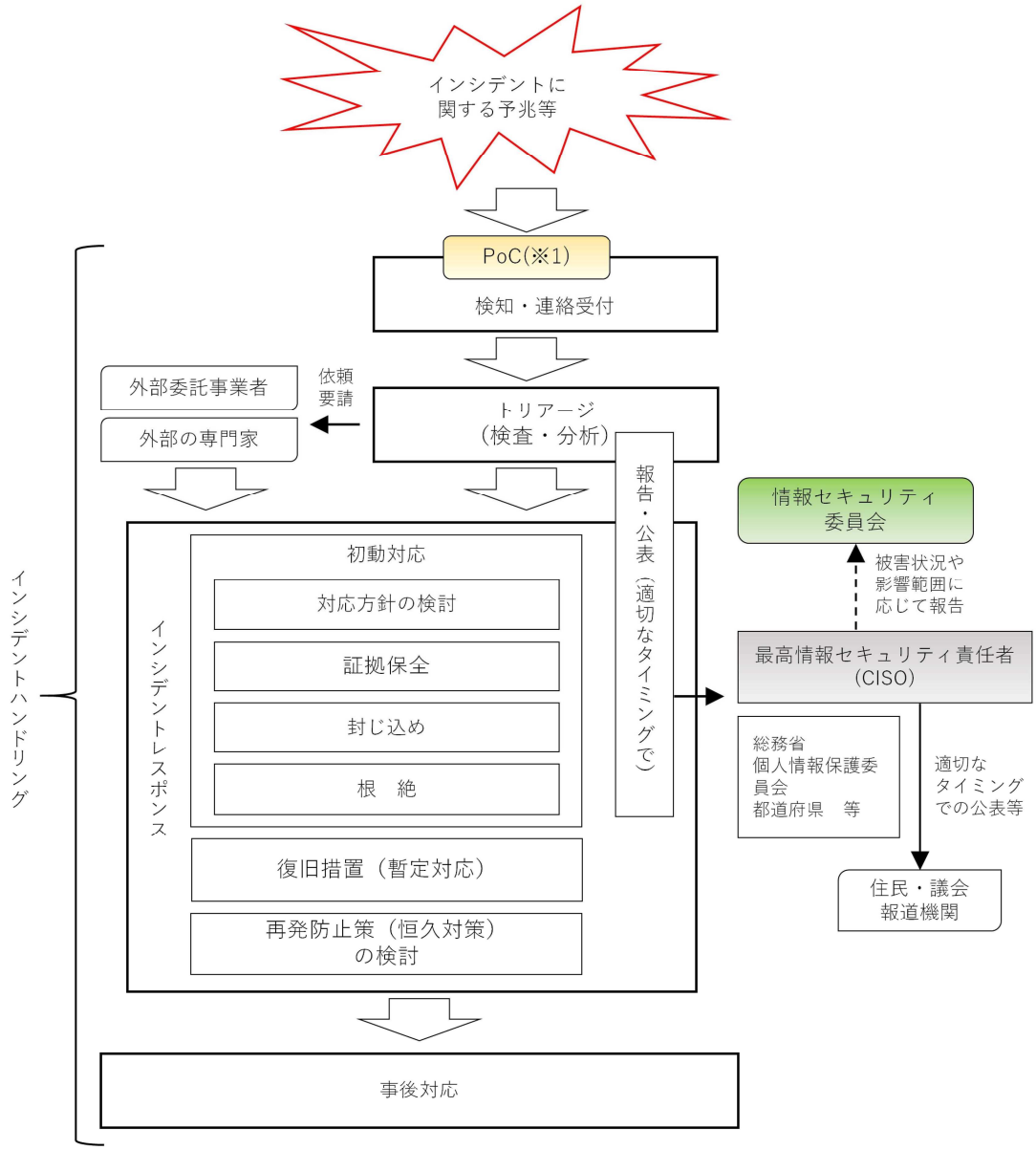
本計画で対象とする情報セキュリティインシデント（以下「インシデント」という。）は次のとおりとする。

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等の改ざんの発生又は発生が疑われる状態
盗難・紛失	地方公共団体が管理する重要な情報（例 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）

第３　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。



（※１）ＰｏＣ（Point Of Contact、ポック）：情報セキュリティに関する統一的な窓口の連絡先（別表１参照）

２．　インシデントハンドリングの具体的手順

インシデントハンドリングの具体的手順は次のとおりとし、宮崎市ＣＳＩＲＴ（以下「ＣＳＩＲＴ」という。）（※２）がこれに当たるものとする。ＣＳＩＲＴの設置については別途定めることとする。

（※２）ＣＳＩＲＴ（Computer Security Incident Response Team、シーサート）：情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制

（1）検知・連絡受付

ア　職員等は、検知、発見、通報等によりインシデントの発生に関する予兆等に気付いた場合、情報セキュリティ管理者を通じて直ちにＰｏＣ（別表参照）に連絡する。

イ　ＣＳＩＲＴ要員（情報システム担当者）は、ＰｏＣに寄せられたインシデントに関わる連絡・通報等を受け付ける。

（2）トリアージ（検査・分析）

ア　インシデントハンドラー（情報システム担当者）は、得られた情報に基づき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に応じてインシデントの処理に優先順位を付ける。その際、必要に応じて、通報者や外部委託事業者、外部の専門家等と情報をやり取りして詳細を確認する。

（3）インシデントレスポンス

（3－1）初動対応（対応方針の検討、証拠保全、封じ込め、根絶）の実施

ア　インシデントハンドラー（情報システム担当者）は、当該インシデントの関連部署及び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（情報システム管理者）、ＣＳＩＲＴ副責任者（情報セキュリティ責任者）を通じてＣＳＩＲＴ責任者（統括情報セキュリティ責任者）に報告する。

イ　ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）は、必要に応じ外部委託事業者及び外部の専門家等に作業の依頼、協力等の要請を行う。

ウ　インシデントハンドラー（情報システム担当者）は、対応方針に基づき、必要に応じ外部委託事業者及び外部の専門家等と連携・協力して、証拠を取得、保全、確保、記録し、インシデントを封じ込め、根絶する。

エ　もし、新たなマルウェアの感染等が検出されたら、全ての影響のあるホストを特定するために検査・分析の手順を繰り返し（２（2））、インシデントを封じ込め、根絶する。

（3－2）復旧措置（暫定対応）の実施

ア　インシデントハンドラー（情報システム担当者）は、対応方針に基づき、必要に応じ外部委託事業者及び外部の専門家等と連携・協力して、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。

イ　復旧後、必要と認められる期間、再発の監視を行う。

（3－3）再発防止策（恒久対策）の検討

ア　インシデントハンドラー（情報システム担当者）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実施手順の改善を含め、再発防止策を検討しＣＳＩＲＴ管理者（情報システム管理者）、ＣＳＩＲＴ副責任者（情報セキュリティ責任者）を通じてＣＳＩＲＴ責任者（統括情報セキュリティ責任者）に報告する。

イ　ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）は、再発防止策を最高情報セキュリティ責任者（ＣＩＳＯ）へ報告する。

ウ　最高情報セキュリティ責任者（ＣＩＳＯ）は、情報セキュリティ委員会（別表２）等に報告し、再発防止策が有効であると認められた場合はこれを承認し、インシデントの概要と併せ職員等に周知する。

（４）報告・公表

ア　インシデントハンドラー（情報システム担当者）は、トリアージの結果、対応方針の変更、対応状況の進捗等については、適宜、ＣＳＩＲＴ管理者（情報システム管理者)、ＣＳＩＲＴ副責任者（情報セキュリティ責任者）を通じてＣＳＩＲＴ責任者（統括情報セキュリティ責任者）に報告する。

イ　ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）は、被害状況や影響範囲等に応じて最高情報セキュリティ責任者（ＣＩＳＯ）へ報告する（報告様式１）。

あわせて、総務省が定める様式により、総務省及び宮崎県等関係機関に報告する。職員等に速やかに情報提供すべきと判断した場合は、注意喚起等の周知を行う。必要に応じて、関係する住民への連絡、議会への報告、報道機関等への公表を行う。

（５）事後対応

ア　ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）は、インシデントの収束宣言を行う。

イ　ＣＳＩＲＴ責任者（統括情報セキュリティ責任者）は、インシデントの対応のフォローアップを行うとともに、１か月を目途にインシデントに関わった関係者を集め反省会を開催し、最終報告書を取りまとめる。

第４　平常時の事前準備・予防等

１．　事前準備・予防等

取得されているログの種類や内容、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、適用されている予防策等は、あらかじめ確認等しておくこととする。

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・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・演習等の結果等と併せ定期的に評価・見直しを行うこととする。

別表１

ＰｏＣ	宮崎市ＣＳＩＲＴ　（情報政策課）
所在地	宮崎市橘通西１丁目１番１号
対応時間	平日　8 時 30 分～17 時 15 分　※メールは 24 時間受付
電話番号	0985-21-1712
ＦＡＸ番号	0985-22-6106
メール	（インターネット）　03jyouho@city.miyazaki.miyazaki.jp （ＬＧＷＡＮ）　03jyouho@city.miyazaki.lg.jp

別表２

委員長	情報政策担当部長（総務部長）
副委員長	情報政策担当課長（情報政策課長）
委員	セキュリティポリシー担当係長（情報政策課） システム運用担当係長（情報政策課） ＤＸ担当係長（情報政策課） 個人情報保護担当係長（総務法制課） 内部統制推進担当係長（市役所改革推進課）

報告様式１

令和○○年○○月○○日

最高情報セキュリティ責任者（ＣＩＳＯ）

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（第○報）

このことについて、業務において○○○○○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サービスへの影響並びにシステムの概要

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・影響範囲（損害規模等）
（情報漏えいの場合は、漏えいした情報の概要及び件数）

５．事案が情報セキュリティインシデントに該当するか否かの判断結果

６．対応状況（初動対応、復旧措置（復旧状況及び復旧見込み、復旧に要する金額等））

７．再発防止策（恒久対応）

８．対外的な対応（報道発表、住民への連絡、総務省・都道府県・ＮＩＳＣ・警察機関等への連絡）
９．その他
対応記録等は別紙のとおり

（記入要領）

・記載に当たっては、報告時点で判明している内容を記載する。判明していない部分は未記入でも可。報数を重ねていくうちに埋めていく。だたし、トリアージの段階で、第１項～第５項までは、極力把握し報告できるようにしておく。
・○○○○及び１（１）の記載例
ＩＴ障害の場合の記載例 ：情報の破壊、システム等の利用困難、マルウェア等の感染、不正コード等の実行、システム等への侵入、外部からのサイバー攻撃等
情報漏えいの場合の記載例：ＵＳＢメモリ等記録媒体や書類等の紛失、ＵＳＢメモリ等記録媒体や書類等の盗難、Ｗｉｎｎｙ等のファイル共有ソフトの利用による流出、メールの誤送信による流出等
・第５項は、トリアージ（検査・分析）に基づくの結果を記載する。
・第６項は、インシデントレスポンスに基づく初動対応（対応方針の検討、証拠保全、封じ込め、根絶）及び復旧措置に係る対応状況を記載する。
・第９項の対応記録等（対応記録、証拠等）は、インシデントハンドリングの過程で担当等において取っておいたものを添付する。