情報セキュリティインシデント対応
（侵害時の対応と緊急時対応計画）
実施手順書

作成者	恩納村　総務課
作成日	平成 29 年 11 月 30 日
最終更新日	

目　　次

第１　総則 1
　１．目的 1
　２．基本的事項 1
第２　侵害時の対応 1
　１．初期対応 1
　２．復旧対応 2
　３．事後対応 2
第３　緊急時対応計画（準備） 3
　１．想定する情報セキュリティインシデント 3
　２．体制 3
　３．予防対策 4
　４．見直し 4
第４　緊急時対応計画（行動計画） 5
第５　緊急時対応計画（初動） 5
　１．統括情報セキュリティ責任者への連絡 5
　２．要員招集 5
　３．人命や情報資産の保護 6
第６　緊急時対応計画（復旧対策） 6
　１．機器・設備損害調査 6
　２．暫定対応実施（システム及び機器等の場合） 7
　３．復旧対応実施（システム及び機器等の場合） 7
　４．回復連絡（システム及び機器等の場合） 7
第７　事後検討期（再発防止策） 7
　１．原因調査・検証 7
　２．再発防止及び公表 8

第１　総則

１．目的

本手順書は、情報セキュリティインシデント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、情報システム及びネットワークの情報セキュリティ対策を実施するために具体的な対処手順を定めることを目的とする。

２．基本的事項

情報セキュリティ管理者は、情報セキュリティインシデントを認知した場合、次に掲げる対応を実施する。

（１）所管する情報システムにどのような影響が発生しているのか調査し、情報セキュリティ委員会事務局（以下「事務局」という。）に報告する。

（２）別紙「情報セキュリティインシデント判定基準」を参照し、情報セキュリティインシデント判定基準がレベル２の場合には、「侵害時の対応」に基づいて対処する。情報セキュリティインシデント判定基準がレベル３の場合には、「緊急時対応計画」又は「業務継続計画」に基づいて対処する。

（３）対処完了後、再発防止のため、統括情報セキュリティ責任者及び事務局に対して、様式「再発防止計画書」の記載事項に基づき、具体的予防策を検討し、報告する。

第２　侵害時の対応

１．初期対応

情報セキュリティ管理者は、情報セキュリティインシデント判定基準がレベル２以下の場合は、次のとおり対応する。

（１）物理的・環境的事故

職員等は、入口電子キーの故障、来訪者の不審行為又は不審物の発見等、執務室の情報セキュリティが担保されない環境を発見した場合は、直ちに情報セキュリティ管理者及び事務局に連絡し、対応を求める。

（２）技術的事故

① 情報セキュリティ管理者は、ネットワーク及び情報システムの停止を伴わない障害、防御された不正アクセス及び不正プログラムの感染又は侵入、対応可能な機器の故障及びソフトウェアの誤動作等が発生した場合は、直ちに事務局及び様式「(付表 B) 構築・保守連絡先一覧」に示す保守委託先の外部委託事業者に速やかに連絡し、対応を求める。

② 情報セキュリティ管理者は、緊急事態において被害の拡大を防ぐためにネッ

トワーク及び情報システムの緊急停止が必要な場合には、ネットワーク及び情報システムを停止する。この場合、統括情報セキュリティ責任者及び事務局に報告する。

③　情報セキュリティ管理者は、緊急事態でネットワーク及び情報システムが使用不可能な場合は、手作業による代替手段により事務作業を行うよう職員等に指導する。

（３）人的事故

職員等は、携帯電話や職員証の紛失等が発生した場合は、直ちに情報セキュリティ管理者及び事務局に連絡し、対応を求める。

２．復旧対応

（１）物理的・環境的事故

①　来訪者の不審行為等の場合、情報セキュリティ管理者及び事務局は、直ちに現地に駆けつけ来訪者に対し、不審行為をやめることをする。不審行為をやめない場合、警察に連絡し、対処を委ねる。

②　不審物の場合、情報セキュリティ管理者及び事務局は、直ちに現地に駆けつけ不審物の状況を確認する。危険性がある場合には、直ちに消防及び警察に連絡し、対処を委ねる。

③　電子キーの故障等の場合、事務局が現地に駆けつけ確認を行う。必要に応じて専門業者に連絡をとり、修理等を行う。

（２）技術的事故

①　情報セキュリティ管理者及び事務局は、保守委託先の外部委託事業者と協力して、情報セキュリティインシデント発生の原因を特定する。

②　情報セキュリティ管理者及び事務局は、原因が特定され、安全性が確認でき次第、システムを再起動させる。

（３）人的事故

携帯電話や職員証等を紛失した職員等は、事務局と協力して紛失物を探すとともに、機能が無効化するように手続を行う。

また、再発行等の手続を行い、新たに準備する。

３．事後対応

①　情報セキュリティ管理者は、発生した緊急事態について、様式「インシデント報告書（IT 障害)」に基づき、記録を作成し、保管する。

② 情報セキュリティ管理者は、緊急事態が復旧した場合は、速やかに全職員に対して連絡する。

③ 情報セキュリティ管理者は、緊急事態の復旧後に、様式「インシデント報告書（IT 障害)」に基づいて再発防止策を検討し、統括情報セキュリティ責任者に報告する。

④ 統括情報セキュリティ責任者は、報告を受けた再発防止策に基づき、必要な措置を実施する。

第３　緊急時対応計画（準備）

１．想定する情報セキュリティインシデント

本計画において想定する情報セキュリティインシデントは、別紙「インシデント判定基準」のレベル３に該当する場合であるが、具体的な種別を表１に示す。ただし、自然災害、疫病、テロ、大規模な障害等により、全庁的に影響が発生し、業務の実施が困難な状況である場合には、別途定める業務継続計画に従う。

表１　想定する情報セキュリティインシデント一覧

種別	内容
障害	機器故障等によるネットワーク又は情報システムの停止
事故	情報漏えい等、パソコンや電子媒体の盗難、法令違反等

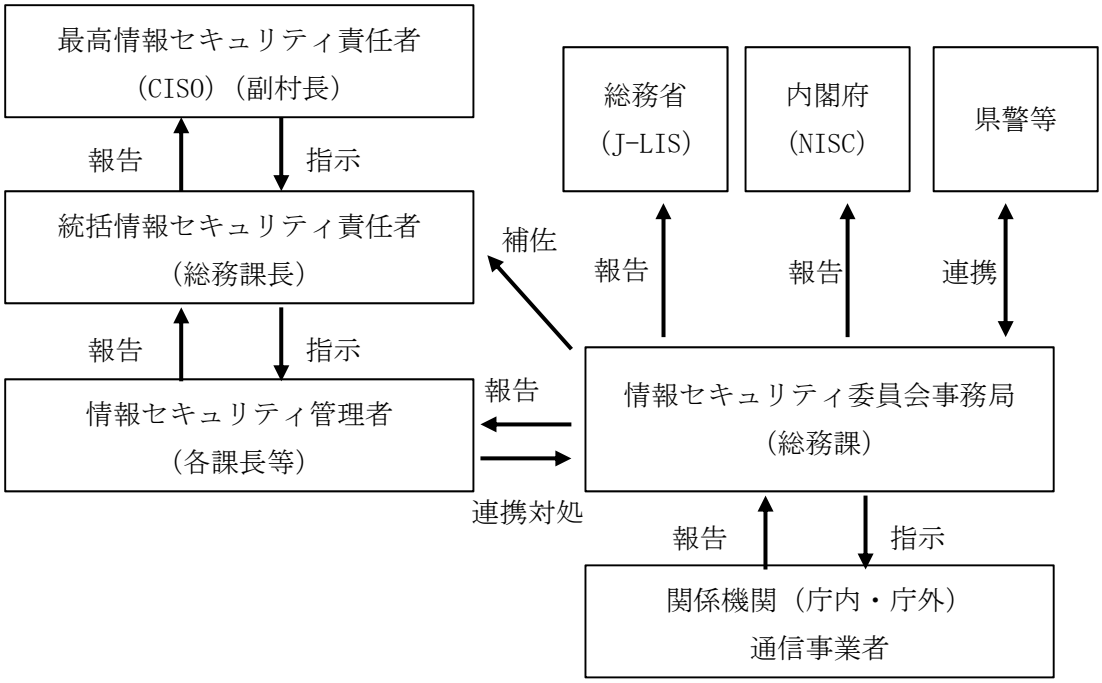
２．体制

本計画においては、迅速かつ機動的な対応を行うため、表２の実施体制を定める。ただし、最高情報セキュリティ責任者が必要があると認めた場合、恩納村情報セキュリティポリシーの組織体制に移行する。

表２　実施体制

実施者	役割
統括情報 セキュリティ責任者	本計画遂行の責任者。計画の発動や終了の決定、要員招集など全体指揮を行う。また、所管課等に対して情報資産、情報システム及びネットワークの運用状況の連絡を行う。
情報セキュリティ 管理者	所管する情報資産、情報システム及びネットワークの状況について、統括情報セキュリティ責任者及び事務局へ連絡を行う。
事務局	設備面：サーバやネットワーク機器、設備の被害状況を把握し、必要であれば予備機への切替えやバックアップデータの復旧等の手配を行う。 広報面：情報セキュリティ管理者などから情報を集め、情報資産、情報システム及びネットワークの利用者に被害状況と復旧の見通しを広報する。

図１　連絡体制図



３．予防対策

統括情報セキュリティ責任者は、表１の想定する情報セキュリティインシデントに対し、緊急時に即応できるように、図１に記載する連絡体制図に従って確実に行動できるよう次の予防対策を行う。

①　連絡網の最新化
②　重要な情報資産のバックアップ
③　主要電子機器の代替機確保

４．見直し

最高情報セキュリティ責任者又は統括情報セキュリティ責任者は、次の場合、緊急時対応計画の見直しを検討し、必要に応じて改定する。

①　「業務継続計画」の変更
②　想定する情報セキュリティインシデントの変更
③　人事異動や組織の大幅な変更
④　対象とする情報システムの構成変更
⑤　準拠すべき法令等の施行、改正
⑥　その他最高情報セキュリティ責任者又は統括情報セキュリティ責任者が必要と認める場合

第４　緊急時対応計画（行動計画）

緊急事態発生時の行動の大まかな流れは、図２のとおりである。

図２　緊急事態発生時の行動の流れ

各局面	行動フロー	関連規程と様式
初動期 （応急対策） ※緊急事態発生後 約１時間まで	情報ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ発生 ↓ 統括情報セキュリティ責任者への連絡 ↓ 要員招集 ↓ 人命や情報資産の保護	様式 （付表 A）要員連絡先一覧
対応期 （復旧対策）	機器・設備損害調査 ↓ 暫定対応実施 ↓ 復旧対応実施 ↓ 回復連絡	様式 （付表 B）構築・保守連絡先一覧 （以下各所管で準備） 予備機切替手順 予備回線切替手順 サーバ復旧手順 データリストア手順 ネットワーク復旧手順
事後検討期 （再発防止策）	原因調査・検証 ↓ 再発防止及び公表	様式 再発防止計画書

第５　緊急時対応計画（初動）

初動期においては、統括情報セキュリティ責任者への連絡と要員の招集を行う。なお、統括情報セキュリティ責任者は、職員及び関係者の安全確保を最優先し、その後復旧対策の実施に移るものとする。手順は、次のとおりとする。

１．統括情報セキュリティ責任者への連絡

①　職員等は、情報漏えい等の発生並びに情報システム及びネットワークの異常が発生した場合、統括情報セキュリティ責任者に内容を報告する。

②　統括情報セキュリティ責任者と連絡がとれない場合、事務局に連絡する。

２．要員招集

①　統括情報セキュリティ責任者は、緊急時対応計画を発動するうえで、情報漏えい等の状況、情報システム及びネットワークの状況並びに緊急時対応計画の

発動について、最高情報セキュリティ責任者に報告する。

② 統括情報セキュリティ責任者は、様式「(付表 A) 要員連絡先一覧」に基づき、緊急時対応計画の実施に関わる要員を招集する。なお、招集できない要員がいる場合には、要員に対する作業の割当て内容を見直すとともに、必要に応じて他の職員に対して応援を指示する。

３．人命や情報資産の保護

① 統括情報セキュリティ責任者は、緊急時対応計画を発動するうえで、人命が危機にさらされている場合は、人命の尊重を第一に考え、警察・消防への連絡等必要な措置を講ずる。

② 統括情報セキュリティ責任者は、緊急時対応計画を発動するうえで、情報資産、情報システム及びネットワークに存在する重要性分類Ⅱ以上の情報資産が漏えい、滅失及び毀損等の脅威にさらされている場合は、情報システム及びネットワークの緊急停止又は切断等の必要な措置を講ずる。なお、緊急停止等の措置を行う場合、様式「(付表 B) 構築・保守連絡先一覧」により、保守委託先の外部事業者等のアドバイスを得ることができる。

③ 統括情報セキュリティ責任者は、情報システム及びネットワークを緊急停止又は切断する場合若しくはした場合、最高情報セキュリティ責任者に報告する。

④ 事務局は、情報漏えい等が確認された場合又はそのおそれがある場合、速やかに被害状況を把握し、統括情報セキュリティ責任者に報告する。併せて、被害状況の庁外への報告に備えるため、被害状況の整理を指示する。

第６　緊急時対応計画（復旧対策）

対応期においては、情報漏えい等発生時の状況、機器・設備の被害状況等を把握し、外部専門家や外部委託業者などと連携しつつ、必要な人的支援及び機器・設備を手配する。復旧に必要な、人員、対策、必要な機器・設備が準備でき次第、復旧作業を開始する。

１．機器・設備損害調査

① 事務局は、被害状況の把握を指示し、情報を収集するとともに、被害状況と復旧の暫定見通しを統括情報セキュリティ責任者に伝える。

また、必要に応じて調達の必要のある機器・設備について、手配やバックアップデータを早急に取り寄せる。

② 事務局は、統括情報セキュリティ責任者からの指示に基づき、情報漏えい等やシステムの被害状況、影響範囲、復旧の見通し等を関連機関（庁内・庁外）へ連絡するとともに、内外からの問い合わせに対応する。

③ 事務局は、庁内ネットワークに障害の原因が存在する場合は、様式「(付表 B)

構築・保守連絡先一覧」に基づき、ネットワークの保守委託先の外部事業者等に連絡し、現在の状況や復旧の見通しを確認する。

２．暫定対応実施（システム及び機器等の場合）

① 統括情報セキュリティ責任者は、正式な復旧手続が行われるまでに長時間を要することが予想される場合は、代替手段による運用の開始を事務局に指示する。

② 事務局は、統括情報セキュリティ責任者の指示に基づき、代替手段として、予備機との切替えや予備回線との切替えを保守委託先の外部事業者等と協力して実施する。

③ 事務局は、代替手段による運用開始について、情報システム及びネットワークの利用者に連絡するとともに、利用者からの問合せに対応する。

３．復旧対応実施（システム及び機器等の場合）

① 統括情報セキュリティ責任者は、原因を特定し、回復の目途がついた段階で、事務局に復旧開始を指示する。

② 事務局は、各種手順に従い、保守委託先の外部事業者等と協力して、サーバやネットワーク機器及び電力等を復旧させるよう努める。

４．回復連絡（システム及び機器等の場合）

① 事務局は、サーバやネットワーク機器等を復旧した場合、稼動状況の確認を行い、統括情報セキュリティ責任者に報告する。

② 事務局は、情報システム及びネットワークの復旧について、関係機関（庁内・庁外）並びに情報システム及びネットワークの利用者に通知する。

③ 事務局は、情報システム及びネットワークが復旧した後も、サーバやネットワーク機器等の稼動状況が安定するまで監視する。

第７　事後検討期（再発防止策）

１．原因調査・検証

発生した緊急事態に関して、回復後にその内容を詳細に検証し、再発防止策の検討材料とする。

① 統括情報セキュリティ責任者は、復旧作業後に関係者と協力し、情報漏えい等並びに情報システム及びネットワークに関する緊急事態の原因について、調査分析により明らかにする。

② 統括情報セキュリティ責任者は、原因調査に際して、次の内容について、整理する。

ア　発生原因・兆候
イ　対処の経緯
ウ　緊急事態の特性・被害内容

③　統括情報セキュリティ責任者は、原因調査を行う場合、必要に応じて外部の専門組織（保守委託先の外部事業者等、警察、セキュリティコンサルタント等）と連携する。

２．再発防止及び公表

同様の緊急事態の再発を防止し、又は被害の発生を最小限に食い止めるため、検証結果に基づき、緊急事態の再発防止策を検討するとともに、当該事案について、公表する。

①　統括情報セキュリティ責任者は、明らかにした緊急事態の発生原因から、情報資産、情報システム及びネットワークを保護するため、再発防止策を検討する。なお、再発防止策については費用対効果を考慮し、有効な対策を選択する。

②　統括情報セキュリティ責任者は、緊急事態の再発防止策を検討する場合、次の内容について、検討する。

ア　発生原因の排除
イ　発生の兆候への早期対応
ウ　被害軽減対策の実施
エ　対応体制の整備
オ　関係者・機関に対する研修の実施
カ　記録の作成
キ　有効な未然防止策の検討

③　統括情報セキュリティ責任者は、再発防止策について、様式「再発防止計画書」を用いて情報セキュリティ委員会に報告し、承認を得なければならない。

④　統括情報セキュリティ責任者は、承認を得た再発防止策について、速やかに実施する。

⑤　最高情報セキュリティ責任者は、当該事案の事実関係、発生原因、影響範囲及び再発防止策等について、速やかに公表する。

＜別紙＞　情報セキュリティインシデント判定基準

		レベル1	レベル2	レベル3
判定		セキュリティ事故とはしない	セ キ ュ リ テ ィ 事 故	
基準		・一時的にリスクとして想定した事象が発生した状態で、実害のほとんどないもの、又は計画されたもの ・定められた対策を遵守していない状態で、事故とは呼べないもの ・システム又はサービスのセキュリティの弱点又はその疑いがあるもの	・事故による影響が軽微なもの ・復旧に特別な対応を必要としないもの ・ネットワークに対する外部からの攻撃でシステム的に防御されたもの	・情報漏えい等が実際に発生した場合 ・長期間のシステム停止等可用性に重大な影響が発生した場合 ・外部からの攻撃により被害が発生した場合
事件・事故の種類・例	物理・環境的事故	・来訪者受付のミス （職員が了解しているもの） ・建物内各種設備（エレベータ、コピー機等）の点検等による停止、一部故障又はメンテナンス ・職員在室時の入口開放状態 ・収納庫等の破損 ・上記以外で軽微な問題があるとき	・入口電子キー故障 ・来訪者の事務室内の不審行為 ・不審物の発見	・不審者の侵入 ・運営に支障をきたすレベルの物理的・環境的障害
	電子的事故	・メンテナンス等による計画的なNW、サービス停止 ・クライアント端末への定められた管理策の未実施（パスワード設定等） ・限られた範囲でのデータの紛失・誤った変更（復旧可能） ・上記以外にシステム又はサービスのセキュリティに弱点又はその疑いがある場合	・ネットワーク又はハード障害で概ね2時間以内に回復（ただし障害の原因が明らかに外部からの攻撃である場合はレベル3とする。） ・システムにより防御された不正アクセスや、ウイルスメール等の不正プログラム対策ソフトウェアでのガード ・機器（クライアント又はネットワーク機器等）の故障で、代替機等により対応可能なもの ・組織内システムの軽微なバグ ・ソフトウェアの誤動作	・回復の見込みのたたないネットワーク障害 ・外部からの攻撃によるサーバ等停止 ・サーバ又はクライアントのコンピュータウイルス感染 ・重要性分類Ⅰの情報の大量喪失又は改ざん（故意若しくは過失又は復旧の可否を問わず）
	人的事故	・離席による情報放置 ・職員証不携帯 ・共有スペースでの業務に関する会話 ・上記以外に軽微な問題があるとき	・携帯電話等の紛失 ・職員証の盗難又は紛失	・情報漏えい等（故意又は過失を問わず） ・法令違反 ・モバイル端末や電子媒体等の盗難又は紛失
対 応		・必要に応じて注意喚起等（課長等） ・システム又はサービスのセキュリティに弱点又はその疑いがある場合は、事務局へ報告	・様式「インシデント報告書（IT障害）」の作成 ・事務局へ報告	・様式「インシデント報告書（IT障害）」の作成 ・事務局へ報告 ・緊急時対応計画又は業務継続計画により対処

［改定履歴］

版	更新年月日	改定理由及び内容	承認	審査	担当
1.0 版	平成 29 年 11 月 30 日	新規制定			

＜様式＞

再発防止計画書

情報セキュリティ委員会　様

平成　　年　　月　　日
統括情報セキュリティ責任者

以下の通り再発防止策を検討しましたので、承認をお願いします。

今回の緊急事態の概要	**※インシデント報告書（IT 障害）の緊急事態の概要を記載（添付要）**
発生組織 **（システム名若しくは課名を記載）**	
原因	

■再発防止策について

対応方針	**※原因排除、早期対応、被害軽減策の視点から記載のこと**					
対応策	内容		計画（○○年度）			
			第 1Q	第 2Q	第 3Q	第 4Q
	1					
	2					
	3					
その他						

作成時の注意
対応策については、以下の内容について検討すること

・発生原因の排除、発生の兆候への早期対応、被害軽減対策の実施、対応体制の整備、関係者・機関に対する研修の実施、記録の作成、有効な未然防止策の検討　等

最高情報ｾｷｭﾘﾃｨ責任者

＜様式＞

様式1

（地方公共団体→総務省）

インシデント報告書（IT障害）

（第　　報*）

※1：(*が付与された項目は必須事項)

情報連絡日時*　　平成　　年　　月　　日

情報連絡元*	団体名：		担当者名：	
	部局名：			
	電話番号：		FAX番号：	
	電子メールアドレス：			

①発生した事象の分類（別紙参照）

事象の類型		事象の例	チェック（1つのみ選択（※2））
未発生の事象		予兆・ヒヤリハット	□
発生した事象	機密性を脅かす事象	情報の漏えい （組織の機密情報等の流出など）	□
	完全性を脅かす事象	情報の破壊 （Webサイト等の改ざんや組織の機密情報等の破壊など）	□
	可用性を脅かす事象	システム等の利用困難 （制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	□
	上記につながる事象（※3）	マルウェア等の感染 （マルウェア等によるシステム等への感染）	□
		不正コード等の実行 （システム脆弱性等をついた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によるシステム等への侵入）	□
		その他	□

※2：最初に検知した事象を1つのみ選択する。

※3:機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の分類（別紙参照）

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	□
	ユーザーID等の誤り	□
	DoS攻撃等の大量アクセス	□
	情報の不正取得	□
	内部不正	□
	適切なシステム運用等の未実施	□
偶発的な原因	ユーザの操作ミス	□
	ユーザの管理ミス	□
	不審なファイルの実行	□
	不審なサイトの閲覧	□
	外部委託先の管理ミス	□
	機器等の故障	□
	システムの脆弱性	□
	他分野の障害からの波及	□
環境的な原因	災害や疾病等	□
その他の原因	その他	□
	不明	□

＜様式＞

◆情報連絡の内容(※4)　（別紙有無*:　□有　□無）

項目	情報の内容
③分野名*(※5)	政府・行政サービス分野
④事象が発生した事業者等名	
⑤概要	判明日時:　平成　年　月　日　時　分 （発生日時:　平成　年　月　日　時　分）
	事象が発生したシステム等:
	発生事象の概要: システムの稼働状況:　□影響なし　□停止中　□一部稼働中　□復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※5)　逸脱の有無:　□有　□無 他の重要インフラ分野への波及の可能性:　□有　□無
⑦該当事象に係る推移等	日時 / 事象・対応状況等 （補足情報）
	対外的な対応状況 報道発表、報道等への掲載:　□済　□予定有　□無　（済・予定有では日時・件名を記入） NISC以外に連絡を行った先
⑧今後の予定	□事象継続中（続報あり） □事後調査実施中（続報あり） □今後の対応策を継続検討（続報なし） □対応完了（続報なし）
⑨その他 ・得られた教訓等	

※4:情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。

※5:「重要インフラの情報セキュリティ対策に係る第3次行動計画」に定める「分野名」、「サービス維持レベル」を指す。

<様式>

付録

情報連絡様式作成時のチェックリスト

※本チェックリストシートは様式作成時に作成者が確認すべき項目を列挙したものであり、総務省への提出は不要です。（特に第1報は当該チェックリストに限らず様式中で空欄があってもかまいません。速報性を重視して作成してください。）

以下内容が【当該事象に係る推移等】に記載されているか確認してください。（該当しない場合や不明な場合は不要です。）

標的型メール受信時のチャックリスト		
A-1	□	標的型メールの「件名」、「本文」、「送信元メールアドレス」、「添付ファイル名」等を記載しましたか？
A-2	□	標的型メールの添付ファイルや掲載URLを開いてしまった場合、その日時を記載しましたか？ ※以下「ウイルス被害（ランサムウェア・スパイウェア等）のチェックリスト」もあわせて参照してください。

ウィルス被害（ランサムウェア・スパイウェア等）のチェックリスト		
B-1	□	ウイルス感染が疑われる端末をネットワークから隔離（LANケーブルの抜線や無線LANスイッチのOFF等）した日時を記載しましたか？
B-2	□	ウイルス感染が疑われる端末と接続されていたネットワークをインターネット等外部ネットワークから隔離した場合、隔離した日時を記載しましたか？
B-3	□	OSやアプリケーション等の脆弱性を悪用されたウイルス感染の場合、最新パッチの適用有無等を記載しましたか？
B-4	□	感染経路がウェブサイトであった場合、関連URL（誘導元URLや誘導先URL 等）を記載しましたか？
B-5	□	ウイルス感染が疑われる端末の台数を記載する場合は「X台中のY台」といった形で、全台数（Y台）もあわせて記載しましたか？

DDoS攻撃被害のチェックリスト		
C-1	□	攻撃に関する情報（犯行予告や犯行声明など）がある場合、記載しましたか？
C-2	□	攻撃元のIPアドレス数（特定国からだけなのか、不特定多数のIPからなのかなど）が判明できた場合、記載しましたか？

リスト型攻撃被害のチェックリスト		
D-1	□	攻撃とみられるログインにより成功した（とみられる）回数を記載しましたか？
D-2	□	ログインが成功した際に閲覧が可能な情報の範囲（個人情報や決算情報など）を記載しましたか？

その他共通事項		
Z-1	□	【判明日時】には、当該事象に気づいた日時を記載しましたか？ （ログ解析等により事象が発生していた日時が明らかになった段階で【発生日時】も記載してください。）
Z-2	□	【発生事象の概要】には、当該事象の概要、被害状況、現状等を（簡潔に）記載しましたか？
Z-3	□	【サービス維持レベルの逸脱の有無】の「サービス維持レベル」は、第3次行動計画別紙2を指します。 逸脱している場合は「有」にチェックしましたか？
Z-4	□	【当該事象に係る推移等】には、当該事象発生以降の対応状況等を時系列に記載しましたか？ ※保守やセキュリティを担当するベンダー等へ連絡した場合、個人情報等の漏えいが確認された場合、サービスを停止した場合等の主な事項を列挙してください。 ※アクセスログの解析等により情報流出の疑いがある場合（関連ログは要保全）、流出の可能性があるデータの件数及び種類（名前・住所・クレジットカード番号等）を記載してください。

＜様式＞

(付表 A)要員連絡先一覧

担当名	所属部署、役職	庁内連絡先	非常時連絡先
最高情報セキュリティ責任者	副村長	098-966-1200	
統括情報セキュリティ責任者	総務課　課長	098-966-1200	
事務局（総務課）	総務課　行政係 係長及びシステム担当者	098-966-1200	
情報セキュリティ管理者 兼情報システム管理者	議会事務局　局長	098-966-1199	
〃	企画課　課長	098-966-1201	
〃	建設課　課長	098-966-1203	
〃	商工観光課　課長	098-966-1280	
〃	農林水産課　課長	098-966-1202	
〃	上下水道課　課長	098-966-1198	
〃	学校教育課　課長	098-966-1209	
〃	社会教育課　課長	098-966-1210	
〃	中学校統合推進室　室長	098-966-1210	
〃	出納室　室長	098-966-1208	
〃	村民課　課長	098-966-1205	
〃	税務課　課長	098-966-1206	
〃	福祉健康課　課長	098-966-1207	

＜様式＞

(付表 B)構築・保守連絡先一覧

機器・設備	数量	事業者名	担当者名	連絡先
サーバ機 A	1	○○社	営業担当者 保守担当者	営業時間内連絡先 営業時間外連絡先
サーバ機 A 用 UPS	1			
サーバ機 B	1			
サーバ機 B 用 UPS	1			