公益財団法人岐阜市教育文化振興事業団
情報セキュリティポリシー

第１版

目　　次

第１章　　情報セキュリティ基本方針

（目的）

第１条　公益財団法人岐阜市教育文化振興事業団（以下「事業団」という。）が保有する情報資産に関して機密性、完全性及び可用性を維持するため、事業団が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（適用範囲）

第２条　基本方針の適用範囲は、事業団事務局、事業団が管理する施設及び実施する事業において取り扱う次の項目を対象とする。

(1) ネットワーク及び情報システムで取り扱う情報、機器

(2) 情報資産を利用するすべての者

(3) 情報システムの仕様書及びネットワーク図等のシステム関連文書

（用語の定義）

第３条　次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 情報資産

業務を遂行するために役立つ情報の集まりをいう。

(2) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(3) 完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

(4) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(5) 情報セキュリティ

情報の機密性、完全性及び可用性を維持することをいう。

(6) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(7) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(8) 情報セキュリティポリシー

本基本方針、次章以降に定める情報セキュリティ対策基準（以下「対策基準」という。）、情報セキュリティ実施手順（以下「実施手順」という。）及び情報セキュリティ緊急時対応計画（以下「緊急時対応計画」という。）をいう。

（職員の遵守義務）

第４条　一般職員、嘱託職員、臨時職員（以下「職員」という。）及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたっては情報セキュリティポリシー（以下「ポリシー」という。）を遵守しなければならない。

（対象とする脅威）

第５条　事業団は、情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の進入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、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊・消去等
(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
(5) 電力供給の途絶、通信の途絶等のインフラの障害からの波及等

(情報セキュリティ対策)

第６条　前記の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制
事業団が保有する情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。
(2) 情報資産の調査
事業団が保有する情報資産について調査を行う。
(3) 物理的セキュリティ
情報システム及びその設置場所等の管理について、物理的な対策を講じる。
(4) 人的セキュリティ
情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の必要な人的な対策を講じる。
(5) 技術的セキュリティ
コンピュータの管理、アクセス制御、不正プログラム対策、不正アクセス等の技術的な対策を講じる。
(6) 運用
情報システムの監視、ポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じるものとする。

(情報セキュリティポリシーの見直し)

第７条　ポリシーの見直しが必要となった場合または情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合は、ポリシーを見直す。

(対策基準、実施手順及び緊急時対応計画の策定)

第８条　本方針に規定する対策等を実施するために、対策基準、実施手順、緊急時対応計画を策定する。

第２章　　情報セキュリティ対策基準

(目的)

第９条　事業団が保有する情報資産に関して、基本方針に定められた情報セキュリティを確保するために、遵守すべき行為及び判断等の基準を定めることを目的とする。

１　組織体制

(情報セキュリティ委員会)

第１０条　事業団の情報セキュリティの維持を目的として情報セキュリティ委員会（以下「委員会」という。）を設ける。

２　委員会は次の代表者で構成する。
(1) 委員長
(2) 副委員長
(3) 委員
３　委員会の役職は下記の職員を充てる。

役職	職名
委員長	理事長
副委員長	事務局長
委員	施設長（総体は統括監）、総務課長

４　委員会の役割は下記のとおりとする。
(1) ポリシーの策定、改訂
(2) 情報資産の調査
(3) 情報資産に関するリスクアセスメント、リスクマネジメント
(4) ポリシーに関する文書の配布、改廃
(5) ポリシーの遵守状況の調査
(6) ポリシー違反者への対処
５　委員会は各作業を実施するにあたり作業部会を設けることができ、その責任者はいずれかの委員とする。

２　情報資産の調査

（情報資産の調査）
第１１条　委員会は、保護すべき情報資産について調査を行う。
（リスクの抽出）
第１２条　委員会は、調査したすべての情報資産について物理的・人的・技術的環境におけるリスクの抽出を行う。
(1) 物理的脅威　侵入、破壊、故障、停電、災害等
(2) 人的脅威　誤操作、持ち出し、不正行為、パスワードの不適切管理等
(3) 技術的脅威　不正アクセス、盗聴、コンピュータウイルス、改ざん・消去、Dos攻撃、なりすまし等

３　物理的セキュリティ

（機器の管理）
第１３条　コンピュータ等の機器及びネットワーク機器は、適切な物理的対策を講じなければならない。
２　前項の機器は、当該機器の管理施設において、適切に管理をしなければならない。

４　人的セキュリティ

（最高情報セキュリティ責任者）
第１４条　理事長を最高情報セキュリティ責任者（以下「最高情報責任者」という。）とし、すべての情報セキュリティに関する権限・責任を持つとともに、情報セキュリティの運用に関する重大な事項について決定を行う。
（情報セキュリティ統括担当官）

第１５条　事務局長を情報セキュリティ統括担当官（以下「統括担当官」という。）とし、情報セキュリティ担当官の統括を行う。

（情報セキュリティ担当官）

第１６条　各施設の長（総合体育館は統括監）及び総務課長を情報セキュリティ担当官（以下「担当官」という）とし、各施設または課における指示系統、意見の集約を行う。

（情報セキュリティ対策の遵守義務）

第１７条　職員は、情報セキュリティポリシー及び実施手順に記載されている内容を遵守しなければならない。

（教育の実施）

第１８条　統括担当官は、情報資産に携わるすべての職員に対し、必要に応じて情報セキュリティ教育を実施しなければならない。

（インシデントに対する報告）

第１９条　職員は、インシデント（情報セキュリティに関する事故やシステム上の欠陥等）を発見した場合は、速やかに担当官に報告をし、その指示を仰がなければならない。

２　前項により報告を受けた担当官は、軽微な事項を除き、統括担当官に対し報告しなければならない。

（情報漏えいの禁止）

第２０条　情報資産を扱うすべての職員は、知り得た情報を外部に漏らしてはならない。

２　異動、退職等により業務を離れる場合においても、外部に対し情報を漏らしてはならない。

(パスワードの管理)

第２１条　情報システムを扱うすべての職員は、次のとおり厳格にパスワードの管理を行わなければならない。

(1) パスワードを秘密にしておくこと。

(2) パスワードのメモは原則作成しないこと。ただし、メモが安全確実に保管される場合はその限りではない。

(3) 情報システムまたはパスワードに対する危険の恐れがある場合は、直ちにパスワードの変更を行うこと。

(4) 適切な長さを持つパスワードを選択すること。また、その文字列については、想定しにくいものにしなければならない。

(5) パスワードは、情報システムに関わる職員以外に使用させないこと。

(6) 機器にパスワードを記憶させないこと。

５　技術的セキュリティ

（コンピュータ機器及びネットワークの管理）

第２２条　機器の取扱及び管理方法については、次のとおり定める。

(1) 機器の更新については、内容、必要性、計画を文書にて統括担当官に提出し、承認を得たうえで行うこと

(2) 緊急時に直ちに対処できるようにするため、特に重要なシステムには、非常用の予備システムを準備すること。また、非常用の予備システムの動作検証は、適宜行うこと。

(3) 定期的に情報システムのバックアップを取ること。

(4) 不必要にネットワークに接続しないこと
(5) 情報セキュリティに関する教育を適宜行うこと。
(情報システムの使用)
第２３条　利用者に対する情報システム使用について、次のとおり定める。
(1) 業務目的以外の使用の原則禁止
(2) 業務上のデータの持ち出しの禁止
(3) 無許可ソフトウェアの導入の禁止
(4) 機器構成の無許可で変更の禁止
(アクセス制御)
第２４条　職員は、システムにアクセスする場合は、システム管理者が設定したパスワードを使用しなければならない。
２　パスワードは、推測しにくいものを設定しなければならない。
３　職員は、パスワードによってアクセス制御されたＷｅｂサイトの閲覧において、パスワードをＷｅｂブラウザに記憶させる設定を行ってはならない。
４　職員は、アクセス制御されたＷｅｂサイトの閲覧時に離席または閲覧しなくなった場合は、必ずＷｅｂブラウザを終了させるか、ＯＳのパスワード付スクリーンロックを実施しなければならない。
(システム開発、導入、更新)
第２５条　新たに情報システムの開発または導入若しくは更新を行う場合は、適切な情報セキュリティ対策を講じる。
２　新たな機器、ソフトウェア及びサービスの導入の際は、事前に不具合の確認等を行う。
３　故障等により修理または廃棄する機器については、その機器に存在する情報が外部に漏えいしないよう対策を講じる。
(コンピュータウイルス対策)
第２６条　コンピュータウイルスに感染することを防止するために、次の対策を行う。
(1) コンピュータウイルス対策ソフト（以下「ウイルス対策ソフト」という。）の導入、更新
(2) 重要なソフトウェアや情報システムの更新
(3) ＵＳＢメモリやＦＤ等の電磁的記録媒体のウイルスチェックの実施
(4) 無許可ソフトウェアの導入の禁止
(5) 外部ネットワークからファイル及びソフトウェアを取り入れる際の、サーバ側、端末側におけるスキャンの実行
(脆弱性情報の収集・配布)
第２７条　担当官は、使用するソフトウェア及びハードウェアに関する脆弱性情報を適宜収集する。
２　担当官は、職員に対して収集した情報の周知を図る。

６　運用

(遵守状況の確認)
第２８条　担当官は、職員がポリシーを遵守しているか、適宜確認を行う。
２　担当官は、インターネットを介した不正アクセスを含めた情報システムの稼働状況について適宜確認を行う。
(侵害時の対応策)
第２９条　情報セキュリティが侵害された場合、または侵害される恐れがある場合

は、緊急時対応計画に基づき関係者への連絡や侵害の証拠保全、被害拡大の防止、復旧等の必要な措置を取らなければならない。
２　情報資産が外部への被害拡大の恐れがある場合には、その防止に努める。
３　当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合は、警察及び関係機関と緊密な連携に努める。
（法令遵守）
第３０条　情報システムの運用においては、事業団が定めるポリシーのほか、情報資産の運用に関わる関係法令及び事業団の関係規程を遵守する。
（情報セキュリティに関する違反）
第３１条　担当官は、ポリシーに違反した職員について統括担当官に報告する。
２　業務中に情報セキュリティに係る違反的な行動がみられた場合は、担当官の指示により、直ちに端末の使用を停止させる等の措置をとる。
（対策基準の見直し）
第３２条　委員会は、ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえて、必要に応じて対策基準の見直しを行う。

第３章　　情報セキュリティ実施手順

（目的）
第３３条　事業団が保有する情報資産に関して、対策基準に沿った情報セキュリティを実施するための詳細な手順や内容を定めることを目的とする。
（適用範囲）
第３４条　本実施手順により管理する対象は、事業団が扱う情報システム及びこれらに関する設備、電磁的記録媒体、文書とする。
（管理組織）
第３５条　管理・運営体制は以下のとおりとする。

役割	職名	説明
最高情報セキュリティ責任者	理事長	情報セキュリティ全般おける最高意思決定者
情報セキュリティ統括担当官	事務局長	情報セキュリティ担当官の統括
情報セキュリティ担当官	施設長（総体は統括監）、総務課長	情報資産のセキュリティの維持、管理

（個人情報の取扱い）
第３６条　個人情報に関する基本方針は、下記のとおりとする。
(1) 個人情報を扱うパソコンは、原則インターネットに接続してはならない。
(2) 個人情報の入った電磁的記録媒体は、職場外へ持ち出してはならない。
(3) 不要になった個人情報は、速やかに削除しなければならない。
（情報管理）
第３７条　事業団で扱う情報の管理については、下記のとおりとする。
(1) 機器、情報資産は適切に管理し、業務以外の目的に使用しないこと。
(2) 重要な情報資産や特定個人情報等を取り扱う機器、電磁的記録媒体または文書等は、施錠できるキャビネット・書庫等に保管すること。
(3) パスワードをむやみに記録したり、他人に教えたりしないこと。
(4) 自己の所有するパソコンを持ち込んで使用しないこと。

(5) 離席する際は、ファイルや使用ソフトを閉じるまたは終了させるか、ＯＳのパスワード付スクリーンロックを実施すること。
(6) プリンタやコピー機、ＦＡＸ等から出力された文書は速やかに回収すること。
(7) 重要な情報資産に関する文書を廃棄する際は、裁断、溶解等で情報が判読できないように処理すること。また、廃棄するまでは、施錠管理された場所で保管すること。
(情報システム機器利用時の遵守事項)
(8) 使用するパソコンには盗難防止ワイヤーを設置すること。
(9) システムのハードウェアは無断で改造したり、他のネットワークに接続したりしないこと。
(10) ＯＳやソフトウェアにはセキュリティホール（情報セキュリティ上の欠陥）が発見されることがあるため、迅速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用すること。
(11) ＵＳＢメモリやＦＤ等の電磁的記録媒体は、随時ウイルスチェックを行うこと。
(12) パソコンは、パスワード付きスクリーンセイバー等の設定や起動時のパスワード設定等を施すこと。
(13) 電磁的記録媒体やシステムＩＤ・パスワードに関する関連文書は、金庫または施錠できるキャビネットに施錠保管すること。
(14) 雷の発生または災害時には、状況に応じて速やかに業務を終了し、コンセントを抜くなど機器破損の防止のために必要な措置を講じること。
(15) パソコンに重要データを表示している場合は、他人に盗み見されないよう周囲に配慮すること。
(ソフトウェアの取扱い)
(16) ソフトウェアを使用承諾契約で定められた数量を超えてコピーしたり、インストールしたりしないこと。
(17) 事業団が所有するソフトウェアを個人所有のパソコンにインストールしないこと。また、私物のソフトウェアを事業団のパソコンにインストールして使用しないこと。
(電子メールの取扱い)
(18) 職務以外の目的で電子メールを使用しないこと。
(19) 不審なメールは開封したり、添付ファイルの実行を行ったりせず、削除すること。
(コンピュータウイルスに対する遵守事項)
(20) 業務で使用するすべてのパソコンにウイルス対策ソフトをインストールすること。
(21) ウイルス対策ソフトの定義ファイルは、自動アップロード等により常に最新の状態を保つこと。
(22) ウイルス感染の被害に備え、システムのバックアップを行うこと。
(23) パソコンにウイルス感染が確認された場合は、直ちにＬＡＮケーブルを外し、担当官に報告すること。ＵＳＢメモリやＦＤ等を使用していた場合は、ほかで使用せずに隔離して、担当官の指示に従うこと。
(事故発生時の手順)
(24) 情報漏えい・盗難・紛失・ウイルス感染等の情報セキュリティ事故が発生した場合、担当官は、統括担当官に対し、速やかに「情報セキュリティインシデント事案の発生について（報告第〇報)」（様式１）により報告すること。
(25) 統括担当官は、事故の報告を受けた場合、ネットワークの停止、切断等の緊急

対応と事故原因の特定や被害の影響範囲を把握すること。また、最高情報責任者に報告をすること。

(26) 最高情報責任者は、事故の報告を受けた場合、関係機関に報告すること。

第４章　　情報セキュリティ緊急時対応計画

（目的）

第３８条　事業団が保有する情報資産に関して、インシデントやポリシーの違反等によりセキュリティ侵害事案が発生した場合または発生の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、被害の最小化または未然防止を図ることを目的とする。

（対象とする情報セキュリティインシデント）

第３９条　本計画で対象とするインシデント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	コンピュータウイルス、不正アクセス、DoS 攻撃、標的型攻撃及びホームページ等の改ざんの発生または発生が疑われる状態
漏えい・盗難・紛失	事業団が管理する重要な情報の漏えい・盗難・紛失また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）

（インシデントハンドリング）

第４０条　インシデントハンドリングの概略の対応フローは（図１）のとおりとする。

２　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する。

(1) 検知・連絡受付

ア　職員は、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づいた場合、担当官に連絡する。

(2) 検査・分析

ア　担当官は、得られた情報に基づき事実関係を確認のうえ、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。

(3) インシデントレスポンス

(3-1) 初動対応の実施

ア　統括担当官は、必要に応じて外部関係者・専門家等に作業・協力等の依頼を行う。

イ　担当官は、当該インシデントの関連部署及びその他関係者等と連携し、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、統括担当官に報告する。

ウ　担当官は、対応方針に基づき、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。

(3-2) 復旧措置の実施

ア　担当官は、対応方針に基づき、必要に応じて外部関係者・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の確認の上、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) 再発防止策の検討

ア　担当官は、当該インシデントに係る調査を実施し、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、統括担当官に報告する。

イ　統括担当官は、再発防止策を最高情報責任者へ報告する。

ウ　最高情報責任者は、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に通知する。

(4) 報告・公表

ア　担当官は、検査・分析の結果、対応方針の変更、対応状況の進捗等について、適宜、統括担当官に報告する。

イ　統括担当官は、被害状況や影響範囲等に応じて最高情報責任者へ報告する。最高情報責任者は関係機関に報告するとともに、必要に応じて報道機関等への公表を行う。

(5) 事後対応

ア　統括担当官は、インシデントの収束宣言を行う。

イ　統括担当官は、当該インシデントの対応に関する最終報告書を取りまとめ、最高情報責任者に報告する。

(6) 情報セキュリティ委員会の招集

ア　最高情報責任者は、委員会を招集し、当該インシデントに関する報告を行う。

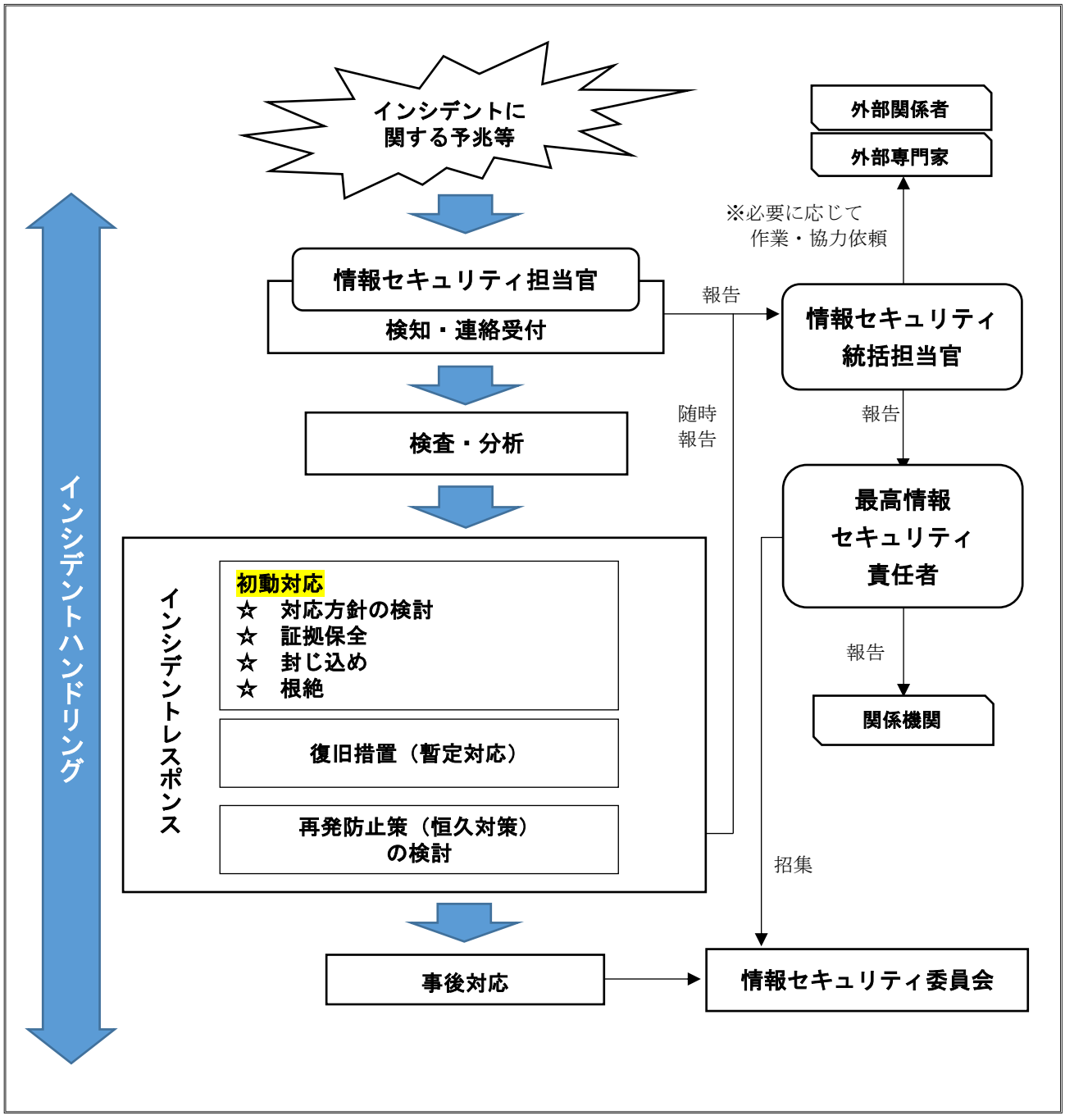
(平常時の対応)

第４１条　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、必要に応じて見直しを行う。

附　則

このポリシーは平成３１年１月３１日から適用する。

（図１）


インシデントに
関する予兆等
外部関係者
外部専門家
※必要に応じて
作業・協力依頼
情報セキュリティ担当官
検知・連絡受付
報告
情報セキュリティ
統括担当官
検査・分析
随時
報告
報告
最高情報
セキュリティ
責任者
インシデントレスポンス
初動対応
☆ 対応方針の検討
☆ 証拠保全
☆ 封じ込め
☆ 根絶
復旧措置（暫定対応）
再発防止策（恒久対策）
の検討
報告
関係機関
招集
事後対応
情報セキュリティ委員会
インシデントハンドリング

（様式１）

平成〇〇年〇〇月〇〇日

（情報セキュリティ統括担当官）

（情報セキュリティ担当官）

情報セキュリティインシデント事案の発生について（報告第〇報）

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
（５）確認した被害状況・影響範囲

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．対応状況（初動対応・復旧措置等（復旧の状況及び見込み、復旧に要する金額等））

４．事案が発生した原因（及び原因として想定される行為）

５．再発防止策（恒久対応）

６．対外的な対応（報道発表・関係機関への連絡等）

７．その他
対応記録は別紙のとおり

（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こと。判明していない部分は未記入でも可。未記入部分は、報数を重ねる毎に補填すること。ただし、検査・分析の段階で、第 1 項から第 3 項までは、極力把握し、報告すること。

・第 3 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こと。

・第 7 項の対応記録等（対応記録や証拠等）は、インシデントハンドリングの過程で作成した資料を添付すること。