情報システムの緊急事態における行動指針

１．目　的

この行動指針は、社会福祉法人津和野町社会福祉協議会（以下「本会」という。）における「情報セキュリティ」対策の一環として、本会の事業活動に重大な支障を来たすITに関わり取得、利用、管理、保存されるすべての情報（以下単に「情報」という。）の漏えいや不正アクセス、大規模災害発生などの緊急事態（以下単に「緊急事態」という。）における迅速かつ適切な情報システムおよび情報資産の保護・復旧を目的として、緊急時に備えた本会の役員、職員、臨時職員、パート職員（以下「役職員等」という。）の行動指針を定めるものである。

２．適用範囲

本会の情報システム及び情報資産に関して、すべての役職員に適用する。

３．原　則

この行動指針は、「リスク管理規程」に則り行うものとする。

４．定　義

情報システムとはコンピュータシステムとネットワークシステム、及びそれを制御するソフトウエア、その運用体制までを含んだものを言う。

情報資産とは、広義には、情報機器やネットワーク機器などのハード資産、及びコンピュータソフトウエア・ソースコードやデータベース・データ情報等のソフト資産すべての事をいう。また、狭義には、ソフト資産のことを言う。

５．活動主体

（１）　情報セキュリティ委員会

情報セキュリティ委員会は、緊急事態が発生した場合に、本会の「情報システムの運用管理に関する規程」第２章第５条に規定する、情報管理責任者（事務局長）の要請により招集される。

情報セキュリティ委員会の委員長は、本会の「情報システムの運用管理に関する規程」第２章第４条に規定する、情報統括管理責任者（会長）とする。

緊急事態が発生した際、情報セキュリティ委員会は、緊急事態の現状把握、対処方法及び事後対処方法を決定し、本会の情報システム及び情報資産の保護・復旧活動の指揮をとる。

（２）　情報システム管理者（部長・所長）

本会の「情報システムの運用管理に関する規程」第２章第５条に規定

する、情報システム管理者（部長・所長）は、役職員等から、緊急事態の発生もしくはその可能性の報告を受けた場合、あるいは自らがそれを検知した場合、情報管理責任者（事務局長）を通じて情報セキュリティ委員会の招集を要請する。

情報システム管理者（部長・所長）は、必要に応じて、情報セキュリティ委員会の決定に基づき、被害を受けた役職員等の復旧作業に全面的に協力し、本会の情報システム及び情報資産の保護・復旧に努める

（３）　役職員等

役職員等は、緊急事態の発生もしくはその可能性を検知した場合には、直ちに情報システム管理者（部長・所長）に報告のうえ、情報セキュリティ委員会の指示を受けながら本会の情報の保護・復旧に努める。

なお、役職員等は、役割分担を事前に明確化、緊急事態に対応するための緊急時行動計画書などの策定を心がけるものとする。

６．緊急事態発生時に対する行動指針

緊急事態（大規模災害を除く）発生時に対する行動指針は次のとおりとする。なお、大規模災害発生時の行動指針については、後記の７項による。

（１）　予防措置・検知措置

緊急事態の発生を回避するためまた、緊急事態が万一発生した場合にその状況を速やかに発見できるよう、本会の「情報システムの運用管理に関する規程」等の、本会の規程・規則に則り、例えば、以下のような情報セキュリティ保持のための活動や監視活動を平素から行う。

①　役職員等のアクセス管理に関する設定状況の点検を行う。

②　役職員等のネットワークやソフトウエアへのアクセス状況の監視やアクセス履歴の点検を行う。

③　役職員等は、情報の厳格な取扱・管理を行う。

④　ウイルス検査を実施するなど安全な電子メールの利用を行い、情報の漏洩を防ぐ。

⑤　ネットワークセキュリティ確保のための不正アクセスなどの対策を行う。

⑥　ネットワークに対する物理的・論理的アクセス管理を行う。

⑦　機器管理に関しては、情報セキュリティ確保のための対策を行うとともに、保管・利用状況の点検を行う。

⑧　最新の不正アクセス対策などの情報セキュリティに関する情報を収集する。

⑨　役職員等へのセキュリティ教育を行う。

（２）　対　処

緊急事態が万一発生した場合の対処については、次のとおりとする。

①　優先順位の決定

発生し得る緊急事態に対して、その対処活動は、本会に関連する団体や、個人等に対して、本会が重大な被害を与える可能性のある場合を最優先に行う。

②　連　絡

ａ　本会各部署への連絡

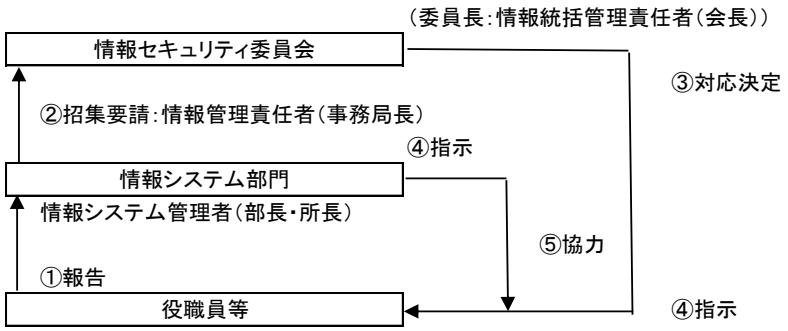
緊急事態の発生を検知した部署は、５項に示す責務に従い、緊急事態発生に関する情報を、情報システム管理者（部長・所長）に報告する。

報告を受けた情報システム管理者（部長・所長）は、情報管理責任者（事務局長）に連絡するとともに、情報セキュリティ委員会の招集を要請する。

情報セキュリティ委員会は、関連する部所へ連絡し、対処活動への協力要請や対処方法の指示などを行う。

また、緊急事態の状況に応じて、行政や所轄庁などへ状況説明を行い、報道機関等への対処方法を検討する。

★緊急事態発生時の連絡体制



ｂ　本会以外の団体や、個人などへの連絡

緊急事態の発生により、本会に関連する、団体や個人以外に重大な影響や被害を与えた場合、関連する役員等は、必要に応じて情報セキュリティ委員会の指示の下、随時、本会以外の団体や、個人などに連絡を取る。

Ｃ　公的機関への連絡

情報セキュリティ委員会は、緊急事態の状況に応じて、以下の公的機関への連絡を判断し、公的機関の協力・連携を確保する。

例１）警察や法的機関等
例２）ＪＰＣＥＲＴコーディネーションセンター（コンピューター緊急対応センター）
例３）独立行政法人情報処理推進機構（ＩＰＡ）
など。

③　応急措置

情報システム管理者（部長・所長）は、情報セキュリティ委員会の指示の下に、関連する役職員等と協力し、被害拡大の防止及び業務活動の継続を目的として、被害状況に応じて応急措置を速やかに講じる。たとえば、外部からの脅威による場合は以下の措置を講じる。

例１）不正アクセスの侵入経路と思われるネットワークの切り離し
例２）不正アクセスを受けたと思われるコンピューターの動作状況の監視またはシャットダウン
例３）業務活動を継続する為の代替え手段の確保など。

また、本会以外の団体や、個人などに重大な影響や被害を与えた場合には、関連する役職員等は、情報セキュリティ委員会の判断に従い、本会の団体や、個人などに対する対応措置を速やかに講じる。

④　被害状況の把握

緊急事態が発生した場合には、関連する役職員等は、情報セキュリティ委員会の指示の下に、情報システム管理者（部長・所長）と協力し、被害状況の把握を速やかに行う。たとえば、以下の項目を調査・究明する。

例１）本会の役職員等による、または外部からの不正アクセスなどにより受けた被害状況（情報漏えい、改ざん、破壊など）とその影響範囲。
例２）本会の役職員等による、または外部からの不正アクセスなどにより受けた日時、その侵入経路、方法（必要に応じ、加害者の特定も行う。）
例３）機密情報の漏えい有無（漏えい痕跡がある場合、漏えいした機密情報及びその漏えい先の特定を行う。）
例４）本会外への被害拡大や影響波及の有無
など。

⑤　復　旧

情報システム管理者（部長・所長）は、情報セキュリティ委員

会の指示の下に、関連する役職員等と協力し、被害を受けた情報システムが正常稼働できるよう、また失われた情報を取り戻せるよう、復旧作業を実施する。

（３）事後対応

緊急事態発生及びその対処が完了した後には、関連する役職員等は、情報セキュリティ委員会の指示の下に、情報システム管理者（部長・所長）と協力し、再発防止のための根本対策を検討、実施する。たとえば、下記の事項を実施する。

例１）原因究明

被害発生に対する原因の明確化を行う。本会の役職員等または、外部からの人的災害によるものであるか、情報システムに潜む脆弱性によるものであるか、厳しく原因究明を行い、人的災害の場合は、行動指針の見直しや、役職員への指導を徹底して行う。

例２）情報システムの脆弱性調査

被害を受けた情報システムの脆弱性を調査する。ここでは、被害状況の把握を詳細に実施し、当該情報システムのセキュリティ上の欠陥を洗い出す。

このとき、情報システム的対策のみに焦点を当てることなく、日々の運用状況や利用状況における問題点の有無などの社会システム的対策（※１）についても調査を実施しなければならない。

（※１）社会システム的対策とは、情報技術による対策以外の人的、法的な対策をいう。

例３）防止策の検討・実装

被害を受けた情報システムの脆弱性を解決するために、セキュリティ設計を再度実施し防止策の検討を行い、セキュリティ機能の追加実装を行うか、あるいは情報システムの再構築を行う。対外ネットワーク接続を実施している場合には、その構成・方法から見直しを図る。

また、不正アクセスを受けたネットワークやコンピュータには、侵入者によりバックドア（※２）を作成されていることが想定されるため、すべての情報システムについて、各種設定状況に異常がないか、不審なプログラムやネットワークサービスがないかなどを速やかに点検する。もしくは、必要に応じて、情報システムの再導入、再設定を行う。

（※２）バックドアとは、侵入者が再度容易に侵入

できるよう施した細工のことをいう。たとえば、ユーザーIDを追加しておく、不正なプログラムを配備する、ネットワーク構成機器の設定情報を変更する、などがあげられる。

例４）作業記録の作成・保管

異常事態の見地、被害の状況、応急措置、根本対策などの作業記録を作成し保管・保持する。特に、不正アクセスを検知したアクセス履歴などのデータは、必ず保管・保存する。

７．大規模災害発生時に対する行動指針

大規模災害発生時に対する行動指針は次のとおりとする。なお、情報システムに係る事項以外の大規模災害発生時の行動指針については、別に定める「リスク管理規程」に準じるものとし、この行動指針では言及しない。

（１）予防措置

情報システム管理者は（部長・所長）は災害発生時を想定し、関連する役職員等と協力して、その故障や破壊が所有する情報システムの可用性に重大な影響を与え、その結果として業務の遂行およびこの法人以外の団体や会員、個人などへの業務上の影響を招くおそれがあると判断した機器類については、たとえば、次のような対策を事前に講ずる。

例１）機器やデータのバックアップに関する技術、手法、体制の強化

例２）ネットワークや情報機器の設置環境における安全面の充実

例３）ネットワークの多重化

例４）代替え機の準備やバックアップサイトの設置

例５）保守契約の締結

など。

（２）対　処

大規模災害が万一発生した場合の対処については、次のとおりとする。

① 優先順位の決定

本会以外の団体や会員、個人などに影響を与える情報システムを高い優先順位に位置付ける。また、コンピュータや外部記録媒体などに格納された機密情報に対しても優先順位を付与し、その安全確保について留意する。

② 連　絡

連絡体制は、６－（２）－②に準ずる。

③ 災害発生直後の要員確保

情報セキュリティ委員会は、役職員等の安否確認後、安全面を確保したうえで情報システム管理者（部長・所長）を中心に、復旧作業要員を招集する。

④ 被害状況の把握

出勤した情報管理責任者（事務局長）および情報システム管理者（部長・所長）また、役職員等は情報セキュリティ委員会の指示に従い、たとえば、下記項目についての被害状況を調査する。

例１）電話の稼働状況

例２）電力の供給状況

例３）ネットワークの状況

例４）情報システム稼働状況

例５）情報を格納したコンピュータや外部記憶媒体などの状況など。

⑤　応急措置

情報セキュリティ委員会は応急処置として、被害拡大の防止措置を講ずる。

⑥　復　旧

復旧作業は、下記要領により行う。

ａ．復旧計画立案の前提

業務復旧のために必要な情報システムは最優先で復旧させる、また情報資産の安全確保と復旧を行う。

この場合には、情報セキュリティ委員会の判断の下に、緊急的措置として本会の各種規程・規則の遵守よりも、まずは情報システムの稼働を優先させてもかまわないものとする。

ｂ．復旧計画の立案

電力の供給を前提として、情報セキュリティ委員会の判断の下に、情報システム管理者（部長・所長）を中心に、業務復旧に必要な情報システムを特定し、その復旧めどについて検討する。

また、関連する役職員等を中心に、本会以外の団体や会員、個人などへの影響度、復旧までの業務代替えの可能性や、復旧の優先度、復旧後の情報システム縮退稼働の可能性などについても検討する。

ｃ．復旧作業

情報システム管理者（部長・所長）は、稼働可能な機器類を調達し、ネットワーク、情報機器の最低限の構成を確保する。

本会で、最低限の構成確保が困難な場合には、外部に対して支援可能かを打診し、可能な限り協力を仰ぐ。

８．行動指針の改廃

この行動指針の改廃は、理事会決議による。

９．実施期日

この行動指針は、平成３０年１月２６日から施行する。