情報システムの緊急事態における行動指針

（目 的）

第 1 条　この指針は、公益財団法人助成財団センター（以下「当センター」と言う）における情報セキュリティ対策の一環として、当センターの事業活動に重大な支障をきたす機密情報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における迅速かつ適切な情報資産の保護・復旧を目的として、緊急時に備えた取扱者の行動規準を定めるものである。

（適用対象）

第 2 条　この行動指針は、当センターの役員、職員、パートタイマー職員、臨時職員および嘱託職員等の有期契約職員（以下「役職員等」と言う）に適用する。

（原 則）

第 3 条　この行動指針は、「リスク管理規程」に則り行うものとする。

（定 義）

第 4 条　この行動指針における用語の定義は、次の各号に定めるとおりとする。

（１）「システム統括管理責任者」とは、当センターの「情報セキュリティ基本規程」に基づき定められた、システムを統括管理する責任者をいう。

（２）「情報システム」とは、情報を取り扱う機器装置等のハードウェア、ソフトウェア、プログラム、伝送経路等及び、これらにより構成される電子システム及びその収納施設等をいい、 情報に関連する一切の資産及び処理方法を含む。

（３）「情報」とは、有形、無形を問わず、当センターが保有する一切の情報（当センター固有の情報の他、契約その他の正当な手段に基づき入手した、あらゆる情報を含む。）をいう。

（４）「情報資産」とは、情報資産とは、情報およびその関連の資産（媒体と伝達手段）をいい、情報記録媒体、情報利用手段、情報保管手段、情報システム、ネットワークなどを含む。

（５）「機密情報」とは、情報資産の中で、許可した者以外に開示したり、目的外に利用された場合、当センターが運営資源としての価値を損なう恐れのある情報をいう。

(緊急事態の報告等)

第 5 条 緊急事態が発生した際の当センターの報告体制主体は、次の各号に定めるとおりとする。

（１）役職員等は、緊急事態の発生もしくはその兆候を検知した場合には、直ちに情報システム担当責任者に報告するものとする。

（２）情報システム担当責任者は、役職員等から緊急事態の発生もしくはその兆候を検知したと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、システム統括管理責任者に報告するものとする。

（３）システム統括管理責任者は、前項の報告を受けた場合、速やかに事業継続計画（第６条）を実行するとともに、情報システム担当責任者に対し、当該緊急事態の原因究明を行うことを指示する。又、システム統括管理責任者は代表理事を委員長とする臨時の情報セキュリティ委員会（コンプライアンス・重大事案検討会議を必要に応じて、組み替えて設置するものとする。緊急事態対策室と同じ役職員等により構成）の招集を要請する。

（４）情報セキュリティ委員会は、緊急事態が発生した場合に、システム統括管理責任者の要請により招集される。情報セキュリティ委員会は、緊急事態への対処方法および事後対処方法を決定し、当センターの情報システムの保護・復旧活動の指揮を行うことにより、事態の収束を図るものとする。

（５）情報システム担当責任者は、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、当センターの情報システムの保護・復旧に努める。

（６）システム統括管理責任者は、緊急事態の再発防止の観点から、事態の収束後に、対応結果について、必要に応じ情報セキュリティ委員会に報告する。

（事業継続計画（BCP：Business Continuity Plan））

第 ６ 条 システム統括管理責任者は、緊急事態が生じた場合においても、事業活動に支障を来たさない、又は支障を最小限化するための計画（以下「事業継続計画」という。）を常に立案、策定、周知及び見直し、改善を行うものとする。

２ 情報システム担当責任者は、役割分担を事前に明確化し、緊急事態に対応するための事業継続計画とは別に、緊急時行動計画書などを策定しておくものとする。

３ 情報システム担当責任者は、事業継続計画の実効性について定期的に見直し、必要に応じ改善を図るものとする。

４ 情報システム担当責任者は、役職員等で行う連絡ミーティングの場を利用して、事業継続計画の策定等を行うために必要な事項等を確保するとともに、この周知徹底、運用及び見直し、改善を図る。

（緊急事態発生時に対する行動指針）

第 ７ 条 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、後記の第８条による。

２ 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、役職員等は、当センターの「情報セキュリティ基本規程」に準じ、情報システムのリスク管理に対する措置を行う。また、平素より以下のようなリスク管理を常に意識した行動を行う。

(1) 情報システム担当責任者は、常に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。

(2) 情報システム担当責任者が中心となり、役職員等で行う連絡ミーティングの場を利用して、予防措置・検知措置に関する情報の周知徹底を行うなど、常に情報の共有を行う。など。

3 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)緊急事態の把握

役職員等は、第５条(緊急事態の報告等)に従い、事態を検知した場合には、直ちに発生時に確認できる事項を簡潔に連絡する。緊急事態発生事象の早期検知の遅れにより、事態の深刻化を招き、異常事態の長期化や影響が大きくなる恐れがあることを理解し、第一発見者が事象を看過ごす事の無いよう、事態を検知した場合には、できるだけ早いタイミングで一報を入れる。

(2)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、当センターのステークホルダーなどに対して当センターが重大な影響や被害を与える可能性のある場合を最優先に行う。

(3)連 絡

ａ．当センター内の連絡

情報セキュリティ委員会の招集により、当センター全役職員への連絡を行う。

緊急事態の状況に応じて、理事会・評議員会・企画委員会などへ状況説明を行う。

ｂ．当センターステークホルダーなどへの連絡

緊急事態の発生により、会員をはじめとする当センターステークホルダーなど重大な影響や被害を与えた場合、情報セキュリティ委員会の指示の下、必要に応じて随時、当センターステークホルダーなどへ連絡をとる。

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、行政庁

例２）ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）

例３）情報処理振興事業協会（ＩＰＡ）など。

(4)初動措置

情報システム担当責任者は、被害の拡大が懸念されるときは、情報セキュリティ委員会の決定に従い、速やかに応急措置を実施し被害拡大の防止に努める。たとえば、不正アクセスにより情報システムが漏えい、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。

(5)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担当責任者と協力し、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） 不正アクセスなどにより受けた被害状況（漏えい、改ざん、破壊など）とその影響範囲

例２） 不正アクセスなどを受けた日時、その侵入経路、方法（必要に応じ、加害者の特定も行う）

例３）機密情報の漏えいの有無（漏えい痕跡がある場合、漏えいした機密情報およびその漏えい先の特定を行う。）

例４）会員をはじめとする当センターステークホルダーなどへの被害拡大や影響波及の有無

例５） 当センターの事業運営に重大な影響を与える可能性の有無 など。

(6)応急措置

システム統括管理責任者は、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、情報セキュリティ委員会に報告の上、たとえば、以下の項目の代替手段による運用の開始などの応急措置を速やかに講じる。

例１）システム統括管理責任者は、事業活動を継続するため「事業継続計画」に従った代替手段の確保を講じる。

例２）情報システム担当責任者は、システム統括管理責任者の指示に基づき、代替手段として、予備機への調達・切替えや予備回線への調達・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。

例３）代替手段による運用開始について、情報セキュリティ委員会にて必要があると判断した場合は、会員をはじめとする当センターステークホルダーなどに連絡するとともに、問合せに対応する。

また、会員をはじめとする当センターステークホルダーなどに重大な影響や被害を与えた場合には、情報セキュリティ委員会にて決定した、対応措置を速やかに講じる。など。

(7)復 旧

システム統括管理責任者は、情報セキュリティ委員会の指示の下に、原因を特定し、回復の目途がついた段階で、情報システム担当責任者に復旧開始を指示する。

情報システム担当責任者は、各種手順に従い、保守委託先の外部事業者等と協力して、被害を受けた情報システムが正常稼動できるよう、復旧作業を実施する。

4 事後対処

緊急事態発生およびその対処が完了した後には、情報セキュリティ委員会の指示の下に、情報システム担当責任者は、再発防止のための根本対策を検討、実施する。たとえば、下記の事項を行う。

例１） 原因究明

被害発生に対する原因の明確化を行う。保守委託先の外部事業者等と協力して、当センターの役職員等または、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、役職員等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、保守委託先の外部事業者等と協力して、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。対社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の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、再設定を行うことが望ましい。

（※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。

例４）作業記録の作成・保管

異常事態の検知、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・保存する。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。など。

（大規模災害発生時に対する行動指針）

第 8 条　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、情報システムにかかる事項以外の大規模災害発生時の行動指針（役職員等の安否状況の早期確認など）については、別に定める当センターの「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

システム統括管理責任者は災害発生時を想定し、その故障や破壊が所管する情報システムの可用性に重大な影響を与え、その結果として事業の遂行および当センターステークホルダーに影響を招くおそれがあるとの考えのもと、情報システムのリスク管理に対する予防措置を行う。たとえば日頃より定期的に、当センター「情報セキュリティ基本規程」および「事業継続計画」に則り、情報システムの強化対策を講ずる。

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)災害状況の把握

被災直後に、当センターの被災状況の早期把握を行う。建物内への立入り制限による復旧活動拠点の喪失や、復旧要員の不足などがないかを確認する。そのために、下記③連絡により情報セキュリティ委員会の招集が出来るかどうか、また情報伝達による最新の情報を情報セキュリティ委員会で共有出来るかを見極める。

情報セキュリティ委員会の機能に問題が無い場合は、「事業継続計画」に則り、情報システムにおける復旧の業務範囲・復旧に要する時間・復旧の時点の目標を決定する。

(2)優先順位の決定

当センターステークホルダー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、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。

(3)連 絡

連絡体制は、第７条（３）③に準ずる。

(4)被害状況の把握

システム統括管理責任者は安全面を確保した上で、情報システム担当責任者および出勤 した役職員等は、情報セキュリティ委員会として、たとえば、下記項目についての被害状況を調査する。

例１）通信インフラ（電話・インターネットなど）の稼動状況

例２）エネルギーインフラ（電力・ガスなど）の供給状況

例３）当センター内ハードウェア IT インフラ（パソコン・サーバーなど）の損壊状況

例４）当センター内ソフトウェア IT インフラ（情報システムなど）の稼動状況 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。必要に応じて、保守委託先の外部事業者等の協力を依頼する。

(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

「事業継続計画」に則り、事業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、緊急的措置として当センターの平時の各種の規程・規則の遵守よりも、まずは情報システムの稼動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

通信インフラ、エネルギーインフラの稼働・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、システム統括管理責任者を中心に、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、当センター以外の団体や会員、個人などへの影

響度、復旧までの業務代替の可能性や、復旧の優先度、復旧後の情報システム縮退稼動の可能性などについても検討する。

ｃ．復旧作業

情報システム担当責任者は、稼動可能な機器類を調達し、ネットワーク、情報機器などの最低限 IT インフラの構成を確保する。

当センター内で、最低限の構成確保が困難な場合には、必要に応じて、保守委託先の外部事業者等の協力を依頼する。

（行動指針の改廃）

第 9 条 この規程の改廃は、理事長の判断により行う。ただし、この規程の趣旨に反しない軽微な事項については、専務理事の判断により改定することができる。

（実施期日）

第１０条　この行動指針は、２０２０年７月１日から施行する。