情報セキュリティ基本方針書

公益財団法人ひかり協会

目　　次

前　　文

公益財団法人ひかり協会（以下、協会という）は、保有する情報システムを情報資産と位置付け、これらの情報資産を保護・管理するために、「情報セキュリティ基本方針書」を制定し、情報セキュリティ組織の確立、人的・物理的セキュリティ対策などを推進するものである。

現在、協会は、インターネットに接続しないクローズドなネットワークを構築し、被害者等の重要な情報の保護を最優先している。この「情報セキュリティ基本方針書」は、情報セキュリティに係るマネジメントサイクル確立のための国際標準規格である ISO／IEC17799：2000 を元に作成された情報セキュリティ管理基準を拠り所に、現在の協会の組織と事業運営及びネットワークの現状を踏まえ、定めたものである。

１．情報セキュリティの基本的方針

協会は、情報セキュリティ基本方針を定めることにより、情報の漏洩、改ざん、破壊等の防止を図り、情報資産の保護を行うとともに、情報の適切な利用ルールを明確にすることにより情報資産の積極的な活用を行い、被害者救済業務の向上を目指す。

なお、特定個人情報の適正な取り扱いに関する基本方針は別途定める。

（１）情報セキュリティの目的

情報セキュリティとは、①人的脅威（不正行為、誤操作等）、②物理的脅威（システムの故障、誤作動等）、③自然災害（地震、火災、風水害等）などから、情報資産の機密性（アクセス制限）、完全性（改ざん・破壊からの保護）、可用性（必要な利用）を維持することであり、情報資産に対して適切な管理を確保することを目的とする。

（２）情報セキュリティに対する取組姿勢

協会が実施する救済事業の安全な運営を確立・維持するために、以下の取組姿勢で情報資産を保護・管理する。

①　情報セキュリティへの体制と取組を協会の内外に知らしめ、各個人の役割と責任を明確にする。

②　当法人における情報セキュリティを確立するため、専門の委員会を設置し管理及び統制を行う。情報資産に対しては、情報資産の管理体制を明確にし、その役割と責任を定め、管理及び統制を行う。

③　業務上、その情報資産を知ることや使用することが必要とされる者、またその権利がある者のみが情報資産を利用できるよう、アクセス制御と管理を行う。

④　定期的に教育を実施することにより、全職員への情報セキュリティへの取組の周知徹底を図る。

（３）情報セキュリティ文書体系

協会における情報セキュリティに係る文書は、以下のとおり構成される。

ア.『情報セキュリティ基本方針書』

情報セキュリティの目的、基本的な考え方について定めたものであり、協会における全ての情報資産が対象になる。

イ.『特定個人情報の適正な取り扱いに関する基本方針書』

特定個人情報等の適正な取り扱いの確保について組織として取り組むための基本方針を定める。

②　運用規程

個々の情報資産についての管理方法や運用手順等の取り決めを定めたものである。

ⅰ）『特定個人情報取扱規程』

ⅱ）『被害者の個人情報保護規程』

ⅲ）『定款事項に関する情報公開規程』

ⅳ）『情報開示規程』

ⅴ）『事務処理規程』及び『文書・会計帳簿保存要領』

ⅵ）『情報システム処理規程』

③　各種手順書
ⅰ）『救済業務の手引』
ⅱ）『総務関係業務マニュアル』
ⅲ）『防災マニュアル』
ⅲ）その他、OA 業務別マニュアルなど

（4）適用範囲

『情報セキュリティ基本方針書』の適用範囲は、協会が保有する全ての情報資産、及びそれらに関わる全ての役員・職員等を対象とする。

2．情報セキュリティの組織

（1）情報セキュリティ組織

協会は、協会内の情報セキュリティを管理するため、情報セキュリティ基盤の整備を図る。

そのため、情報資産管理委員会を設置し、情報セキュリティを主導するための明瞭な方向付けを行う。また、本部事務局及び各ブロックに情報セキュリティ管理者を置く。

①　情報資産管理委員会

情報資産管理委員会は、情報セキュリティの調整・推進に関する権限と責任を有し、情報セキュリティの確立と維持・向上に向けた検討や課題解決を行う。

情報資産管理委員会は、業務執行理事、事務局長、情報セキュリティ管理者によって構成される。

情報資産管理委員会の事務局を本部におく。

情報資産管理委員会の主な役割と責任は、以下のとおりとする。

ⅰ）情報セキュリティ規程類の策定・更新等に係る検討
ⅱ）情報セキュリティ事故・事件への対応
ⅲ）情報セキュリティ規程類の時代や業務への適合性の検討のための情報収集
ⅳ）情報セキュリティを確保するための管理方法の評価と推進

②　情報セキュリティ管理責任者

情報セキュリティ管理責任者は、協会全体における情報セキュリティの推進に関する責任者であり、事務局長がその任にあたる。

情報セキュリティ管理責任者の主な役割と責任は、以下のとおりとする。

ⅰ）情報セキュリティ確保のための管理と指導
ⅱ）情報セキュリティに係る各種の問題・課題への対処・対応

③ 情報セキュリティ管理者

情報セキュリティ管理者は、情報セキュリティ管理責任者を補佐して情報セキュリティ確保のための管理等を行う。事務局次長・各地区センター長がその任にあたり、本部事務局・各ブロックにおける情報セキュリティの推進を図る。

（2）情報資産管理上の役割と責任

協会は、情報を適切に管理し情報セキュリティを維持していくために、情報資産の管理体制を明確にする。

情報資産を保護・管理する上で、以下の役割と責任を定める。

①　情報資産管理責任者

情報資産の保護・管理を行うため、情報資産管理責任者を置く。

情報資産管理責任者は、事務局長とする。

②　情報システム管理者

情報資産管理責任者を補佐するため、情報システム管理者を置く。

情報システム管理者は、情報資産管理責任者の指示に基づき、情報システムやネットワークにおける情報セキュリティ確保の仕組みを提供・運用・管理し、アクセス管理を実施する。

情報システム管理者は、事務局次長とする。

③ 情報システム担当者

情報システム管理者を補佐し、その任を具体的に遂行するため、情報システム担当者を置く。

④ 利用者

利用者は、情報セキュリティの仕組みのもとで、情報を利用・加工する。全ての職員が対象となる。

３．情報資産の分類及び管理

（１）情報資産

① 情報

管理対象となる情報は、協会が所有するすべての情報及び外部から入手した情報であり、コンピュータや磁気媒体等に電磁的に記録された情報のほか、各種文書類や写真なども含む。

② 情報システム

管理対象となる情報システムは、協会内の情報を扱うハードウェア及びソフトウェア全てである。

（２）情報の分類と区分及び管理

情報資産の分類と区分及び管理については、『事務処理規程』及び『文書・会計帳簿保存要領』に規定する。

（３）媒体の取り扱い

情報資産を搬送可能な媒体に保管・保存する場合については、定められた管理と取り扱いを遵守しなければならない。

（４）アクセス制御

電子情報に対するアクセス制御は、情報資産管理責任者によって承認された利用者のみが情報にアクセスできるように、情報システム管理者が設定する。

電子情報以外の情報（紙媒体に印刷された情報等）については、物理環境セキュリティにてアクセスを制御する。

また、情報資産管理責任者は、定期的に利用者のアクセス権の適合性を確認しなければならない。

（５）アクセス管理

情報システム管理者は、電子情報の利用者の識別と認証を可能にするために、情報資産管理責任者の指示に基づき、利用者へのユーザーＩＤ及び認証機能を提供する。

４．人的セキュリティ

協会は、保有する情報資産にアクセスする者に対して必要かつ適切な管理・監督を行うとともに、定期的に適切な教育・啓発を実施するものとする。

（１）業務上のセキュリティに関する責任

業務上の情報セキュリティ責任を明確化し、業務マニュアル等の文書に記述する。また、情報セキュリティに係わる重要な職務に就く者については、その責任を文書で伝える。

（２）採用・退職における情報セキュリティ

① 新たに職員を雇用する時には、情報セキュリティポリシーの遵守を採用の基準とし、雇用期間中及び退職後も機密保持等の責任が明示された誓約書の提出を求める。また、退職時には協会の情報資産の返却を求めるなど、業務上知り得た情報についての機密保持等の管理を実施する。

② 協力専門家や救済事業協力員などの協力者についても、退任時には協会の情報資産の返却を求めるなど、業務上知り得た情報についての機密保持等の管理を実施する。

（３）情報セキュリティ教育

情報セキュリティの確立と維持・向上は、業務に携わる全ての者が遵守しなければ難しい。その

ため、秘密管理の意識を培い維持するために適切な教育を行い、この方針書の内容の周知徹底に努めるものとする。

（4）第三者による情報利用及び業務委託

① 協会の情報資産の利用を第三者に許す場合は、利用させる情報の価値に応じてセキュリティ要求事項を明確にし、契約等を通して確約させる。

② 協会の情報資産を利用する業務の外部への委託は、セキュリティ管理対策及び手順を含むセキュリティ要件を契約書等に記述し、合意した上で行う。

（5）情報セキュリティ事故への対処

情報セキュリティ事故が発生した場合、迅速で的確な対応ができるように、あらかじめ事故の対応体制及び対処方法を整備する。情報セキュリティ事故の対応には、報告・連絡、組織内外への通知、影響範囲の特定、被害拡大の防止、回復、原因究明・分析及び再発防止を実施できるように考慮する。また、情報セキュリティ事故を未然に防止できるように、情報システムの異常や弱点の発見など、事故の予兆が発見された際の連絡・対応体制についても整備する。

5．物理的・環境的セキュリティ

（1）セキュリティエリア

協会の本部事務局及び各ブロックの業務に従事する者が日常業務を行う場所（事務所）をセキュリティエリアとする。このエリアは、救済業務に携わる関係者が立入可能であり、それ以外は立入が制限されるエリアである。物理的な不法侵入や業務への不正な介入を防止し、情報資産を盗難や破壊から保護するために、以下の必要な対策を講じる。

ⅰ）事務所内に職員等の要員が不在になるときは、窓・扉に施錠する。

ⅱ）取り扱いに慎重を要する情報は、第三者に容易に見られないようにする。

ⅲ）危険物・可燃物は極力排除し、保管の必要性がある場合は安全管理を徹底する。

ⅳ）許可なしの写真・ビデオなどの記憶装置の使用は、認めない。

（2）機器のセキュリティ

情報資産を取り扱う機器は、予期せぬ障害（停電などの電源障害）等から防御するため、その機器の種類及びその機器が取り扱う情報の区分に基づいて設置し管理する。

ⅰ）情報処理装置及び記憶装置は、盗難や破壊のリスクから守るよう設置・管理する。

ⅱ）装置の継続的な可用性・完全性を維持するため、キーボードカバーなどの保護具の使用や、装置の正しい保守を実施する。

ⅲ）サーバ管理においては、無停電電源装置（UPS）を設置し、容量が十分であることを定期的に点検する。

（3）事務所環境における情報セキュリティ

事務所において、機器や電子媒体への不正なアクセスが行われないように、防御するための措置を励行する。また盗難などが発生しないよう、機器や電子媒体の持ち込み持ち出しを禁止する。

ⅰ）個人の所有する情報処理機器類を業務情報の処理に用いないよう徹底する。

ⅱ）情報処理機器類を事務所から持ち出さないよう徹底する。

ⅲ）書類及び磁気媒体は、使用していないときや退所時には、適切に施錠された書庫等に保管する。

ⅳ）取り扱いに慎重を要する重要な情報は、使用していないときや退所時には施錠された書庫等に保管する。

ⅴ）コンピュータや印字装置は、ログオン状態で離席しない。

（4）防犯・防災対策

防犯・防災対策については、『防災及び災害時復旧マニュアル』に定める。

６．情報システムのセキュリティ

情報システムのセキュリティについては、『情報システム処理規程』に定める。

７．適合性

（1）法令等との適合

協会の救済業務従事者は、刑法及び民法、その他の法令、規制または契約上の義務、並びに情報セキュリティ要求事項を遵守する。

（2）当方針書との適合

協会の救済業務従事者は、情報セキュリティ基本方針書を遵守しなければならない。

（3）監査

情報セキュリティ基本方針書が遵守されていることを確実にするため、定期的な監査を実施する。

① 内部監査

定期的あるいは必要に応じて、内部監査組織による内部監査を実施し、情報セキュリティ基本方針書が正しく運用されていることや情報システムが正しく設計･運用されていることを確認する。

② 監事監査

定期的あるいは必要に応じて、監事による監査を実施し、情報セキュリティ基本方針書が正しく運用されていることや情報システムが正しく設計・運用されていることを確認する。

③ 自己検査

職員は、定期的に情報セキュリティに関する自己検査を実施し、自己の情報セキュリティにおける状況を確認するとともに情報セキュリティに対する意識を高め、情報セキュリティ知識の習得に努める。

（4）罰則

本書で定める情報セキュリティ基本方針書に違反した場合は、『就業規則』の定めに従って懲戒する。

附　則

１．この基本方針書は、2010 年３月 14 日より適用する。

（2010 年３月 14 日　第 150 回理事会）

２．この改正基本方針書は、2011 年４月１日より適用する。

（2011 年３月 12 日　第 156 回理事会）

３．この改正基本方針書は、2016 年１月 17 日より適用する。

（2016 年１月 17 日　第 187 回理事会）

４．この改正基本方針書は、2020 年４月１日より適用する。

（2020 年３月 16 日　第 214 回理事会）