情報セキュリティ管理規程

2015 年 12 月 1 日改定

（目的）

第１条　この規程は、公益財団法人中部圏社会経済研究所（以下「本財団」という。）が保有もしくは取り扱う情報のセキュリティ管理に関する基本的な事項を定め、適切な財団経営に寄与することを目的とする。

（適用範囲）

第２条　この規程は、本財団のすべての役職員に適用する。

２　この規程が対象とする情報は、電子化または非電子化にかかわらず、本財団が保有するすべての情報をいい、法令に別段の定めのない限り、本財団役職員の本財団に係る職務執行および業務遂行によって新たに生成または拡充された情報および外部から入手して所有する情報も含むものとする。

（用語の定義）

第３条　この規程における用語の定義は次のとおりとする。

（１）電子化情報とは、情報技術によって電磁的に処理可能な状態にある情報をいう。

（２）情報資産とは、情報およびその関連の資産をいい、情報記憶媒体、情報システム、ネットワークなどを含む。

（３）開示とは、手段・方法ならびに本財団内外を問わず、特定の相手方または不特定多数の相手方に対し、電磁的または非電磁的な方法により、送信・伝達・送付もしくは表明し、または提示することをいう。

（４）アクセスとは、情報を閲覧し、情報を使用することをいう。

（５）アクセス権限とは、アクセスできる権限をいう。

（６）アクセス権者とは、アクセス権限を有する者をいう。

（７）情報セキュリティとは、情報を必要とするアクセス権者が正規の情報を適正に利用できるよう、情報を安全に保護することをいう。

（８）情報セキュリティ管理とは、情報セキュリティを維持・運用・保全し、向上させるため、情報ならびに情報セキュリティ環境を管理することをいう。

（責任と権限）

第４条　本財団役職員は，本財団が保有または他団体等から預かっている情報のセキュリティを保全しこれに対する注意義務を負う。

２　本財団は、情報セキュリティを適正に管理するために、情報セキュリティ統括責任者、情報セキュリティ管理者および情報管理者を置く。

３　情報セキュリティ統括責任者は、本財団全体を統括し、情報セキュリティについて最終責任を負うものとし、代表理事をもって充てる。
４　情報セキュリティ管理者は、情報セキュリティ統括責任者を補佐し、本財団の情報セキュリティ管理の運営について全体を統括する実質的な責任と権限を持つものとし、事務局長をもって充てる。
５　情報管理者は、情報セキュリティ管理者を補佐するとともに、各部署が所管する情報の管理を行うものとし、各部署の長もしくは情報セキュリティ管理者が指名する者をもって充てる。

（不正入手の禁止）
第５条　本財団役職員は，他者に帰属する情報を非合法にまたは社会的批判を招く手段により入手してはならない。また提供を相手方に強要したり，相手方の申し出を受諾したりしてはならない。

（目的外利用の禁止）
第６条　本財団役職員は、本財団が保有または他団体等から預かっている情報を定められた目的以外に利用してはならない。
２　本財団役職員は、本財団が保有または他団体等から預かっている情報資産を私的な目的に利用してはならない。
３　本財団役職員は、本財団が保有または他団体等から預かっている情報を許可なく財団外に持ち出したり、他社に開示したりしてはならない。
４　本財団役職員は、本財団が保有または他団体等から預かっている情報を非合法な手段による利用、本財団の定款および規程類に違反した利用ならびに社会通念に反する利用をしてはならない。

（機密情報）
第７条　機密情報とは、許可した者以外に開示したり、目的外に利用された場合、経営資源としての価値を損なう恐れのある情報をいう。
２　本財団は、他団体等から預かっている情報について、当該他団体等が機密情報と指定し、かつ、本財団が同意した場合は機密情報として取り扱う。

（機密区分の設定）
第８条　本財団の機密情報には、機密区分を設定する。
２　機密区分は、次の各号とし、機密区分の付与は、情報管理者が行い、適宜、見直す。
（１）極秘　　経営上重要で、限られた関係者にのみ開示される情報
（２）対外秘　財団外には開示してはならない情報
３　情報管理者は、機密区分を新設または変更した場合には、情報セキュリテ

ィ管理者に報告するとともに、所属部署内に周知徹底する。
４　機密区分の解除は、情報セキュリティ管理者が行う。

（機密区分の表示）
第９条　機密情報には、機密区分を明示する。
２　機密情報が電子化情報の場合、モニター表示時および印刷時に機密区分を表示できるようにする。

（機密情報へのアクセス管理）
第１０条　機密情報へのアクセス権限は、情報管理者が付与する。
２　機密情報へのアクセス許可は、担当業務に必要な範囲とし、利用目的を制限するとともに、アクセス権者を制限する。
３　他団体等から預かっている機密情報は、本財団の情報と同等以上のアクセス管理を行うことに加え、契約書、誓約書等がある場合には、それらに基づき厳重に管理するとともに、求めに応じてアクセス状況を証明できる体制をとらなければならない。
４　機密情報へのアクセスログは一定期間残すものとし、業務監査時に監事の監査を受けるものとする。

（機密情報の管理）
第１１条　極秘に該当する機密情報は、施錠管理する。
２　原則として、同一ファイル中に異なる機密区分の情報を混在させず、アクセス権者ごとにファイルを分割する。
３　やむをえず混在させる場合は、機密レベルの最も高い区分の管理方法を適用する。
４　原則として、機密情報は複製をしてはならない。
５　機密情報が電子化情報の場合は、原則として、共有サーバ内の指定したフォルダに保管し、パスワード管理するものとし、パソコンのローカルディスクおよび記録媒体へ保存してはならない。

（機密情報の開示等）
第１２条　機密情報をアクセス権者以外に開示する場合は、情報セキュリティ管理者の許可を受ける。
２　機密情報の開示は、特定の対象者のみに限定し、開示を受けた者が第三者へ再開示することを禁止する。
３　極秘情報の開示にあたっては、原則として機密保持契約を締結する。
４　極秘情報については、原則としてネットワーク経由での送付を禁じる。
５　本財団役職員は，退任後または退職後も，在職中に知り得た機密情報を他

に開示したり不正に使用したりしてはならない。

（個人情報の取扱い）
第１３条　個人情報の取扱いは、法令および個人情報保護規程による。ただし、特定個人情報等の取扱いは、法令および特定個人情報等取扱規程による。

（文書管理）
第１４条　文書管理に係る取扱いについては、この規程に従うほか、文書管理規程による。

（緊急事態）
第１５条　情報セキュリティに関する緊急事態が発生した場合は、本財団役職員は情報セキュリティ管理者に発生した事態および状況等を遅滞なく報告するとともに、その指揮に従い対応する。

（誓約書の提出）
第１６条　職員は、採用時に機密情報の取扱いに関する誓約書に署名のうえ、本財団に提出する。

（教育）
第１７条　本財団は、年に１回以上、全職員を対象とした情報セキュリティ教育を実施する。
２　前項のほか、採用および着任時には情報セキュリティに係る手続きを中心とした教育を実施し、各部署の長への就任時には情報管理者としての教育を実施する。

（改廃）
第１８条　この規程の改廃は、理事会の決議により行う。

（細則）
第１９条　この規程に定めるもののほか、必要な事項は別に定める。

附　則（２０１３年８月１日）
この規程は、２０１３年８月１日より施行する。

附　則（２０１５年１２月１日）
この規程は、２０１５年１２月１日より施行する。