特定非営利活動法人せんだい・みやぎＮＰＯセンター
情報セキュリティ運用規程

第１章　総則

第１条　目的

この規程は、特定非営利活動法人せんだい・みやぎＮＰＯセンター（以下「センター」という）が扱う情報および情報セキュリティの適正な取り扱いに必要な事項を定めることにより、センターの情報資産を安全かつ適正に運用することを目的とする。

第２条　定義

この規程における用語の定義は、次の各号に定めるところによる。

（１）情報

センターの運営にかかる全ての業務情報をいう。電子的に記録された情報、書類等物理的に存在する非電子化情報、センター職員が業務の過程で知った情報が含まれる。

（２）情報セキュリティ

情報の機密性、完全性、可用性のバランスを継続的に運用または改善するしくみをいう。

（３）情報機器

情報の管理運用に必要な、コンピュータ、周辺機器、ソフトウェアおよびそれらが構成するネットワークのことをいう。

（４）情報資産

上記各号を総称して情報資産という。

第３条　適用範囲

この規程の適用者は、センターの職員、外部委託者、インターン、ボランティア等を含めた、センターの情報を利用するすべての者とする。

第４条　評価と見直し

情報セキュリティに関わる環境変化に適宜対応するため、定期的な評価を実施する。必要が認められた際は、速やかに見直しを行い、第３条に掲げた者に対して周知徹底をする。

第２章　情報セキュリティの管理体制

第５条　情報セキュリティマネジメント体制

センター内に情報セキュリティを管理する組織を設置し、その体制を「情報セキュリティマネジメント体制（以下「マネジメント体制」という）」とする。

２　マネジメント体制の最高責任者は、代表理事とし、センター全体の情報セキュリティを統括管理しその責任を負う。

３　代表理事はマネジメント体制の管理を行う責任者（以下「管理責任者」という）を指名する。

４　管理責任者は、特別の事由が無い場合は、事務局長とする。また、センターが指定管理者や受託者となった施設（以下「施設」という）に関しては、その施設の長を管理責任者とする。

５　管理責任者は、情報セキュリティの運営状況の管理と把握を行い、最高責任者へ報告する。

６　管理責任者は、システム管理者を指名する。

７　システム管理者は、情報セキュリティ管理の実務を担当する。

第６条　事業における管理体制

センターが実施する事業における情報セキュリティの管理は、事業の主担当の責務とする。

２　施設で実施する事業における情報セキュリティの管理は、事業の主担当の責務とする。

３　委託事業における情報セキュリティの管理は、事業の主担当の責務とする。

４　その他外部と共同で行う事業については、その事業の主担当の責務とする。

５　上記第２項から第４項に該当する事業については、この規程の他、設置者、委託者、共同する組織が定める規程を遵守しなければならない。

６　各事業における主担当は、システム管理者へ管理の状況を報告しなければならない。

第７条　施設における管理体制

施設においては、この規程の他に施設の設置者が定める規程を遵守しなければならない。

第３章　情報資産の管理と運用

第８条　基本的義務

情報資産の管理と運用は日常の業務の一環として取り組まなければならない。

２　情報資産の管理と運用はセンターの職員の責務である。

第９条　情報の取得

情報は業務上必要な範囲のみ取得し、必要以上に取得してはならない。

２　個人情報や公開情報を取得する際は、その利用目的をあらかじめ情報提供者に公表・通知しなければならない。

３　情報の提供を強要してはならない。

第１０条　目的外利用の禁止

情報は、定められた目的以外に利用してはならない。

２　情報資産は、私的な目的に利用してはならない。

３　情報は、非合法な手段による利用、センターの規則に違反した利用および社会通念に反する利用をしてはならない。

第１１条　情報の開示

センターの外へ情報を開示する場合は、管理責任者の許可を受けなければならない。

２　施設や委託事業等におけるセンター外への情報の開示においては、前項の他、施設の設置者や委託者が定める規程を遵守しなければならない。

３　この規程に定める範囲以外での利用が業務上生じる場合は、事前に管理責任者の許可を得なければならない。

第１２条　情報の保持と廃棄

情報は保存期間を定め、期間が終了したものは速やか且つ適切な手段で廃棄しなければならない。また、保存期間内の情報や期間を定めない情報については、毀損、紛失、漏洩等が無いよう、適切に管理しなければならない。

第１３条　インターンやボランティアの管理

原則として、インターンやボランティア等に関しては、機密情報や個人情報の取り扱いは行わない。業務上必要な場合は、管理責任者の承認を必要とする。

２　施設におけるインターンやボランティア等については、機密情報や個人情報の取り扱いはいかなる場合でも行うことは出来ない。

３　インターンやボランティア等は、センター職員の管理のもとに業務を行う。

第１４条　誓約書の提出

センターの職員と外部委託者は、入社時に情報の取り扱いに関する守秘義務を記した成約書に署名しなければならない。

2　退職する場合は、理由の如何を問わず、退職後も前項に掲げる守秘義務を遵守しなければならない。

3　個人情報を取り扱うインターンやボランティア等については、事前に守秘義務を記した誓約書に署名しなければならない。また個人情報を取り扱わない場合でも、一般的な守秘義務等を記した誓約書に署名しなければならない。

第４章　機密情報の管理

第１５条　機密情報

許可した者以外に開示したり、目的外に利用された場合、資産としての価値や、センターの運営を損なう恐れのある情報を機密情報とする。

第１６条　機密区分の設定

センターの情報には、機密区分を設定する

2　機密区分は、次の各号とする

（１）極秘

（２）厳秘

（３）事務所外秘

（４）社外秘

3　機密区分の付与は、マネジメント体制で決定し、適宜、見直さなければならない。

4　管理責任者は、機密区分の変更内容について、関連する範囲に周知徹底しなければならない。

第１７条　機密情報の管理

機密情報の責任者は、管理責任者とする。

2　機密情報は次の各号の規程に応じて適切に管理しなければならない。

（１）物理的機密情報（書類、名簿等）

施錠できる保管庫に保管し、その所在を表示してはならない。

（２）電子的機密情報

同一のファイルの中に異なる機密区分の情報を混在させてはならない。また同一のファイルの中に異なるアクセス権限者の情報を混在させてはならない。

3　機密情報や情報機器は、毀損、紛失、漏洩等が無いよう、適切に管理しなければならない。

第１８条　機密情報へのアクセス管理

機密情報へのアクセス権限は、マネジメント体制での承認のもと、管理責任者が設定し、システム管理者により付与するものとする。

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する。

３　機密情報については、利用目的を制限するとともに、アクセス権限者を制限する。

４　機密情報へのアクセス状況については記録と定期的な点検を行い、求めに応じてその状況を証明できる体制をとらなければならない。

第１９条　電子化情報の取り扱い

電子化情報は、その特性を考慮し、情報セキュリティの確保に努めるものとする。

２　電子化された機密情報の保管は、指定したサーバーに限定して認めるものとする。

３　電子化された機密情報の複製は、情報資産の保護を目的としたバックアップ以外には認めない。また、バックアップされた電子化情報は、機密区分の「極秘」とし、必要な措置をとらなければならない。

４　前項の機密情報を、物理的に複製する場合は、業務の必要性に応じてシステム管理者が承認し、業務遂行の後には直ちにシステム管理者へ返却するものとする。

第２０条　ネットワークセキュリティの確保

ネットワークを介した情報資源へのアクセスは、ユーザーＩＤとパスワードにより厳重に管理されなければならない。

２　ユーザーＩＤとパスワードは、システム管理者が適切に管理するとともに、定期的に変更し、不正なアクセスを予防しなければならない。

３　機密情報のネットワークでの送付については、マネジメント体制での承認のもと管理責任者が設定した規程に従い制限しなければならない。

第２１条　個人情報の取り扱い

個人情報の取り扱いは、個人情報保護法および、センターの個人情報保護規程に準拠して行うものとする。

第２２条　知的財産権の尊重

知的財産権は、これを尊重し、知的財産権を侵害しないように最大限の努力をしなければならない。

第５章　緊急時の対応

第２３条　緊急事態の想定と対応計画

情報セキュリティに関して、緊急事態を想定した対策案を別途定める。

2　情報セキュリティに関する緊急事態の発生に備え、複数の連絡手段による連絡網を整備する。

第２４条　緊急事態発生時の対応

情報セキュリティに関する緊急事態が発生した場合は、管理責任者の指揮のもとに対応する。

2　緊急事態の影響度に応じて、管理責任者またはシステム管理者は、最高責任者および関連する組織へ報告し、マネジメント体制全体が協力して解決に当たるものとする。

第６章　情報セキュリティ教育

第３４条　基本的教育

マネジメント体制担当者に対しては、定期的に情報セキュリティ管理者研修を実施する。

2　前項に掲げた者の以外で、第３条で定めた者に関しては、初任者研修時に情報セキュリティ教育を実施し、定期的に情報セキュリティ研修を実施する。

3　情報セキュリティ管理の状況を、定期的に第３条で定めた者へ周知し、管理レベルの向上に資するものとする。

第７章　情報セキュリティ監査

第３５条　マネジメント体制による管理

マネジメント体制は、情報セキュリティ管理の状況を自己点検し、管理レベルの向上に努めなければならない。

第３６条　情報セキュリティ監査

情報セキュリティの内部監査を実施しなければならない。

2　情報セキュリティの管理に要する費用と、実施の効果を把握し、バランスのとれた情報セキュリティが構築されているかを監査しなければならない。

3　施設における監査の場合は、関係先へ監査結果を報告しなければならない。

第９章　罰則

第３７条　処罰

情報セキュリティ管理規程に違反した者は、センター就業規則に基づき処罰する。

第１０章　雑則

第３８条　別規程の適用

この規程に定めるものの他、施設の管理や、委託事業等を受けた際に協定した規程については、その規程もセンター職員は遵守することとする。

附則　　平成 17 年 7 月 1 日制定
　　平成 21 年 9 月 1 日改訂
　　平成 27 年 7 月 1 日改訂