情報セキュリティ基本規程

基本方針

公益財団法人助成財団センター（以下「当センター」と言う）の事業運営の上で、情報システムやインターネットなど（IT）は、いまや欠かせないものになりました。IT の導入による業務効率の影響は甚だしく、また、事業支援ツールとしても今後も大いに活用していくべきものと考えています。

また、過去そして未来の当センターの情報資産を、あらゆる脅威から守るため、それらを管理する情報システムの利用における権利と義務を明らかにし、当センター内の情報システムの安全かつ適正な利用を図るべく、当センターの「情報セキュリティ基本規程」（以下「本規程」と言う）を策定し、情報セキュリティならびに運用管理における対策を遂行します。当センターは、常に高い IT リテラシーを持って、利用者への安全・安心を構築します。

（目 的）

第 1 条　本規程は、「基本方針」に基づき、当センターにおける情報セキュリティ維持及び推進を行うために必要な基本的事項を定めたものであり、IT に関わり取得、利用、管理、保存されるすべての情報（以下「情報」と言う）の取扱い、また情報システムの運用管理に関して遵守すべき行為および判断等の基準を定め、当センターの情報セキュリティを確立することを目的とする。

（定 義）

第 2 条　本規程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）「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。

（2）「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。

（3）「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。

（4）「リスク」とは、想定される脅威（情報資産に対して損害を与える要因）が、情報資産に対して損害を与える可能性をいう。

（5）「システムリスク」とは、コンピュータウイルスによる重要な情報の消去、不正アクセスにより個人情報の流出など、情報システムの停止や誤作動、データの紛失などにより当センターやユーザーに損失を被るリスクのことをいう。

（６）「リスク評価」とは、情報資産について、脅威に対する脆弱性を分析し、かつリスクが顕在化した場合の事業に対する影響度を評価することをいう。

（７）「情報セキュリティ」とは、情報資産に対し、A 機密性（正当に許可した者だけが当該情報資産にアクセスできること）、B 完全性（正確及び完全であるよう、情報資産を不正な改ざん及び破壊から保護すること）および C 可用性（正当にアクセスを許可された者が、使用許諾の範囲内で、必要な時に円滑に当該情報資産にアクセスできること）を確保し、維持することをいう。

（８）「サイバーセキュリティ事案」とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行等、サイバーセキュリティが脅かされる事案をいう。

（９）「対象情報」とは、リスク評価の結果、情報セキュリティの確保及び維持が必要と判断した情報をいう。

（１０）「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。

（１１）「対象情報システム」とは、リスク評価の結果、情報セキュリティの確保及び　維持が必要と判断した情報システムをいう。

（１２）「対象情報資産」とは、対象情報及び対象情報システムの総称をいう。

（１３）「緊急事態」とは、情報セキュリティの確保および維持に重大な影響を与える災害、障害、セキュリティ侵害等の事態をいう。

（１４）「ＩＴリテラシー」とは、情報を取捨選択する「情報基礎リテラシー」、パソコンの操作に関わる「コンピュータリテラシー」、インターネットの概念に関わる「ネットワークリテラシー」という３つによって構成されている能力をいう。

（１５）「スマートデバイス」とは、スマートフォン、タブレット等の携行可能な情報通信機器 もしくは当センターが判断した機器をいう。

（１６）「SNS (Social Networking Service)」とは「Facebook」（フェイスブック）や、「Twitter」（ツイッター）、「Instagram」（インスタグラム）、「LINE」（ライン）他、　対象となる全てのサービスをいう。

（１７）「マルウェア」とはパソコン等に害をなす「malicious software(悪意があるソフトウェア)」の略語で、不具合を起こす意図で作られているソフトやプログラムを総じていう。

（「ウイルス」は「マルウェア」の一つである。）

（１８）「サイバー攻撃」とは、サーバやパソコンなどのコンピュータシステムに対し、ネットワークを通じて破壊活動やデータの窃取、改ざんなどを行うことをいう。

（適用対象）

第 3 条　本規程は、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。また、情報の媒体を問わず、当センターの保有する全ての情報に適用する。

（情報セキュリティおよび情報システムの運用管理体制）

第 4 条　当センターは、情報の機密性、安全性、可用性を維持するために、情報セキュリティおよび情報システムの運用に係る管理者を定め、その役割・責任を明確にする。

2　システムリスクの重要性を十分に認識した上で、事務局長をシステムを統括管理する責任者（以下「システム統括管理責任者」と言う）と定める。

3　システム統括管理責任者は、当センターにおける情報セキュリティおよび情報システムの運用管理に係る業務を実施する責任と権限を有するものとする。

4　当センターにおける情報セキュリティ維持及び向上に必要な基準、規程類の制定、これらの周知徹底、運用及び見直し、改善については、必要に応じて、定款第 53 条第 1 項第 1 号の企画委員会に図るとともに、理事会にてその承認を得るものとする。

5　実際に情報セキュリティおよび情報システムの運用業務を担当する職員等（以下「情報システム担当責任者等」と言う）を決定し、当センターにおける情報システムに関する次の業務を行うものとする。システム統括管理責任者は、次の業務の遂行に係わる権限・責任を情報システム担当責任者等に委譲する。

A．パソコン及びパソコン周辺機器、ソフトウェア、情報記録媒体の管理
B．「アイデンティティ（ID)」と「アクセス」の管理
C．インターネットサーバに係るシステム管理
D．内部サーバ（クラウドサーバ含む）の運用管理
E．ネットワークの接続・運用セキュリティ管理
F．クラウドサービスの利用管理
G．電子メール、SNS 利用管理

（システムリスク管理）

第 5 条　システムリスクについて、役職員等は常にその重要性を十分認識し、システムリスクに対する情報の共有化、対応等を検討し、当センターにおけるシステムリスクに対し迅速かつ適切な対応の実施を目指す。

2 システムリスクの管理においては、業務内容の変更、システムの導入・廃棄、その他体制に影響を与えうる事象に応じて適宜見直し、常に有効なシステムリスク管理を実施する。

3 システム統括管理責任者は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応については、事業運

営および当センターの信用への重大な課題と認識し、当センター代表理事と協議の上、日頃より態勢を整備する。

4 システム統括管理責任者は、当センター内外のコンピュータシステム等の進展や、クラウドサービス利用による環境の変化によりリスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にある等、事業運営に重大な影響を与える可能性があることを十分踏まえ、当センター代表理事と協議の上、リスク管理態勢を整備し、日頃より適宜見直しを行う。

5 情報システム担当責任者等は、システム統括管理責任者の指示に従い、定期的に情報システムの運用におけるシステムリスクの特定・分析・評価を実施し、その結果を報告する。

6 情報システム担当責任者等は、情報セキュリティにおいて、当センターが保有する情報資産を日頃より十分把握し、当センターの情報資産について定期的にセキュリティ診断などを実施することでシステムリスク評価を行い、対策が必要な場合は速やかにシステム統括管理責任者に報告しなければならない。

（対象情報資産に関する情報セキュリティ）

第 6 条　役職員等は、業務の遂行上必要な限度において、対象情報資産を適切に利用・管理しなければならない。

2 役職員等は、対象情報資産の管理にあたり、当センターの「個人情報保護に関する基本方針」および個人情報の取扱に関する法令、国が定める指針等を遵守しなければならない。

3 システム統括管理責任者を管理責任者と定め、役職員等が対象情報資産を適切に管理するために必要な次の施策の周知徹底・運用を行う。

A．必要な範囲以外での複製の作成の禁止

B．第三者への譲渡・貸与・開示等の禁止

C．機密の漏洩・紛失・盗難の防止

D．個人情報の流出の防止

（対象情報システムに関する情報セキュリティ）

第 7 条　システム統括管理責任者は当センターが保有する対象情報システムについて、その設計、開発から導入、運用、保守を通じ、対象情報システムの重要度や特性に適合した情報セキュリティの確保、維持のための施策（コンピュータウィルス・サイバー攻撃からの保護、バックアップ管理、WEB サイトの改ざん防止、システムの停止、ネットワークの管理、クラウドサービスの安全な利用、不正アクセス対策等を含む）、そのための運用管理を講じるものとする。

2 システム統括管理責任者は、対象情報システムに関する管理上のセキュリティに関して統括を行う。

3 システム統括管理責任者は、システムリスク管理に従い、定期的に実施するシス

テムリスクの特定・分析・評価の結果に基づき、対象情報システムを適切に管理するために必要な施策の周知徹底、運用を行い、必要に応じてシステム基盤等の変更の都度、見直し、改善を図る。

4 役職員等は、システム統括管理責任者指導のもと、対象情報システムの利用及び管理に際し、本規程および「サイバーセキュリティ基本法」等、国が定める情報セキュリティ関連の法律・ガイドラインを遵守しなければならない。

5 当センターの管理する WEB サイトの利用者に対して、留意事項を説明するための適切な措置を講じるものとする。

（人的セキュリティ）

第 8 条　役職員等は情報セキュリティの重要性を認識し、本規程を遵守するよう、必要な教育および啓発を定期的、継続的に実施し、役割と責任に応じた知識と技術の修得に努めるものとする。

2 役職員等は当センター「リスク管理規程　第２章 役職員の責務」に則り、就任時に情報セキュリティの確保、維持に関する必要な事項を定めた秘密保持契約書又は守秘義務契約書への署名、捺印し、当センターに提出しなければならない。

3 システム統括管理責任者は、役職員等に対して、情報の適正な管理についての教育・普及に努めるために、役職員等で行う連絡ミーティングの場を利用してその周知徹底をしなければならない。

4 本規程への違反が明らかになった場合は、当センター「リスク管理規程」「コンプライアンス規程」および「職員・就業規則」「有期職員・就業規則」の定めに従い、違反を行った役職員等に対する処分を行うものとする。

(PC の利用とセキュリティ対策)

第 9 条　当センターが支給･貸与する PC の利用にあたり､以下を注意すると同時に、利用については情報システム担当責任者等の指示に従う。

2 当センターネットワークにて利用する PC は、当センターが支給・貸与する PC のみとする。

3 当センターが支給・貸与する PC に導入するソフトウェアは、以下を遵守しなければならない。

（1）PC の利用者（役職員等）は、情報システム担当責任者等が PC を初期導入した際のソフトウェアを基本使用し、勝手に変更・削除してはならない。

（2）規定されたソフトウェア以外で､業務上やむを得ず使用する必要がある場合は、情報システム担当責任者等に申請し、許可を得なければならない。

（3）PC の利用者（役職員等）は、情報システム担当責任者等が提供するソフトウェア情報をもとに最新の修正プログラム等を適用しなければならない。

（4）PC の利用者（役職員等）は、情報システム担当責任者等が設定したマルウェア対策ソフトの設定を変更してはならない。

（５）PC の利用者（役職員等）は、ドライブ全体に対するマルウェア対策ソフトの定期スキャンを無効化してはならない。やむを得ずスキャンを停止した場合は、できるだけ早く定期スキャンを再開しなければならない。

４　PC の情報の不正利用防止、盗難・紛失に備え、以下の通り PC のパスワード管理を遵守しなければならない。

（１）情報システム担当責任者等は、PC の支給・貸与を行う場合、推測されない安全なパスワードを都度作成しなければならない。

（２）PC の利用者（役職員等）は、PC の支給・貸与を受けた場合、第三者の目に触れることがなくかつ自分が忘れない方法で、パスワードを厳重に保管する。

（３）情報システム担当責任者等は、設定したパスワードについて、「長く」「複雑に」「使い回さない」という点に注意し、定期的に変更しなければならない。

５　当センターが支給・貸与する PC での情報の取扱いは、以下を遵守しなければならない。

（１）PC の利用者（役職員等）は、PC で権限のない対象情報を取り扱う場合には、システム統括管理責任者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

（２）PC の利用者（役職員等）は、システム統括管理責任者の許可無く、機密情報を外部媒体に保管してはならない。

（３）PC の利用者（役職員等）は、機密情報取り扱い後には、不必要となった機密情報を直ちに PC と外部媒体から削除しなければならない。

６　当センターが支給・貸与する PC の利用は、利用を許可した以下の場所のみとする。

（１）当センターの事務フロア、会議室。

（２）研修、在宅勤務等で PC の外部持ち出しが認められた場所。

７　PC を外部に持ち出す際は、以下を遵守しなければならない。

（１）PC を社外に持ち出す際には、情報システム担当責任者等の承認を得る。また、情報システム担当責任者等はどの PC が持ち出されているか、記録を付け管理する。

（２）PC の利用者（役職員等）は、社外に PC を持ち出す場合、盗難・窃盗に遭わない様に、また紛失しない様に、細心の注意を払い取り扱わなければならない。

（３）PC の利用者（役職員等）は、社外で PC を利用する場合、情報の盗み見に細心の注意を払い取り扱わなければならない。

（４）PC ハードディスクには、できる限り機密情報を保存しない。

（５）PC を社外に持ち出し、自宅や、他組織のネットワークに接続した場合は、マルウェア対策ソフトを用いて、マルウェアチェックを実施し、異常が発見されなかったことを確認した後でなければ、当センター内ネットワークに接続してはならない。

８　当センターが支給・貸与する PC の利用にあたり、以下を注意する。

（１）PC の利用者（役職員等）は、利用環境を整理整頓すると共に、デスクトップを整理し、クリアスクリーンを心がけなければならない。

（２）PC の利用者（役職員等）は、PC 利用に伴う、PC 及びそれに付随する機器の紛失・盗難、また情報漏えい等セキュリティインシデントが発生した場合、その旨を速やかにシステム統括管理責任者に報告・対応しなければならない。

９ PC または媒体の再利用および廃棄を行う場合は、対象情報におけるリスクと　安全性を充分検討した上で、情報システム担当責任者等が稟議書を提出し、指定された方法にて再利用および廃棄処理を行う。

（私有スマートデバイスの取扱い）

第１０条　当センターの事業において、業務効率の向上および、当センターの信頼を確保するために、役職員等が私有するスマートデバイスを使用する場合は、その取扱いに関し、以下を遵守しなければならない。

（１）役職員等は、その私有するスマートデバイスから当センターの情報システム・ファイルサーバ等へ接続することは、原則禁止とする。

（２）役職員等が私有するスマートデバイスで、当センターの電子メール、事業で使用する情報資産、顧客情報、業務アプリケーションの使用等もしくは、有線 LAN、無線 LAN 等へ接続、使用することができる。なお、利用許可の範囲は、当センターが認めた所定の範囲とする。

（３）役職員等は、私有するスマートデバイスの管理、運用にあたり、業務で利用する情報とプライベートで利用する情報を、明確に分けておかなければならない。

（４）当センターは、役職員等が私有スマートデバイスに当センターの対象情報であって持出し、複製、第三者への開示が禁止された情報が含まれている場合には、システム統括管理責任者をして当該情報を消去させることができる。

（５）役職員等は、退職や業務遂行において私有するスマートデバイスを利用する必要がなくなった場合、また機種変更などの事由により私有するスマートデバイスを変更する場合、役職員等は本規程第８条を準用する事により、利用していた私有スマートデバイスに登録されている当センターの事業に係るすべての対象情報を消去するものとする。

（６）当センターは、業務上認められた場合を除き、役職員等が私有するスマートデバイスの通信費用、保守費用、データバックアップ費用、紛失等での再取得費用等を一切負担しない。

（７）役職員等は、私有するスマートデバイスを紛失しもしくは盗難に遭った場合、またはコンピュータウイルスに感染し、もしくはそのおそれがあると判断した場合には、直ちに情報システム担当責任者等に報告しなければならない。

（電子メールの利用とセキュリティ対策）

第１１条　電子メールの利用にあたっては、情報システム担当責任者等が指定した電子メールソフトウェアを用いなければならない。また、当該ソフトウェアを常に最新の状態に保たなければならない。

２ 電子メールの利用にあたっては、常にマルウェア対策ソフトウェア（セキュリティ対策ソフトウェア）を使用しなければならない。また、当該ソフトウェアを常に最新の状態に保たなければならない。

３ 電子メールで送受信される情報は以下の通り保護しなければならない

（１）電子メールの利用者（役職員等）は、当センターの事業に関わる情報や、当センターが保有する個人情報などの機密情報をメールにて送受信する場合は、機密情報の内容に応じて暗号化、電子署名などの処置を施さなければならない。

（２）電子メールの利用者（役職員等）は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（３）当センターのセミナー案内やメールマガジンなどのように電子メールで同報送信する場合は、送信先メールアドレスが受信者に閲覧できないよう、電子メールの一斉配信機能を利用するかBCCを利用しなければならない。また、これらのメール等の送信にあたっては、オプトインの取得、オプトアウトの設置等の「特定電子メールの送信の適正化等に関する法律」の遵守をしなければならない。

４ 電子メールを利用にあたっては、当センターに被害を招かないため、以下を遵守しなければならない。

（１）電子メールの利用者（役職員等）は、事業目的以外に電子メールを利用してはならない。

（２）電子メールの利用者（役職員等）は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易にURLリンクをクリックしてはならない。不審だと疑われるメールを受信した場合は、即座に情報システム担当責任者等に報告し、適切な処理を行わなくてはならない。

（３）電子メールの利用者（役職員等）は、外部のコミュニケーションツール等へメールアドレスを登録する場合は、当該ツールの信頼性、および事業への必要性を充分考慮した上で登録しなければならない。また、登録意義の無くなった場合は、直ちに脱退しなくてはならない。また公序良俗に反する発言をしてはならない。

（４）電子メールの利用者（役職員等）は、電子メールの送信にあたっては、添付するファイルの容量を考慮しなければならない。規定容量以上のファイルを送信せざるを得ない場合は、情報システム担当責任者等に相談の上、指定されたファイル共有サイト・ファイル転送サイトを利用しなければならない。また添付するファイルにマルウェア感染が無いことをマルウェア対策ソフトにて確認後、メールを送信しなければならない。

（５）電子メールの利用者（役職員等）は、その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メールはテキスト形式で送信するよう設定しなければならない。

（SNSの利用とセキュリティ対策）

第１２条　SNS 上に当センターの事業、取組み、イベント等の情報を発信することを通じ、当センターの利用者・その他関係者のみならず多くの SNS ユーザーに当センターに対する理解を深めていただくとともに、ユーザーの利便性を高めることを目的とする。そのために役職員等は SNS を十分理解し、自覚をもって正しく運用しなければならない。

２ 業務目的で公式に SNS を利用する際には以下を遵守しなければならない。

（１）業務を目的に公式 SNS を利用する役職員等は、事前に、利用目的を明らかにし、公式アカウント名であることを認識し、責任をもって情報発信を行わなければならない。

（２）SNS に記述する内容は、当センターWEB サイト等に記述する公開情報に準ずる。

（３）虚偽の情報を発信し、他のユーザーを惑わせること、混乱させることを行わない。その内容が当センターの信用失墜とならないよう、情報が誤っていた場合は、速やかに謝罪し、訂正しなければならない。

（４）SNS 利用において、他のユーザーからのクレーム、中傷、炎上等に巻き込まれた場合は、直ちにシステム統括管理責任者および情報システム担当責任者等に報告しなければならない。

（５）公式アカウントに関わる ID・パスワードは第 4 条（情報セキュリティおよび情報システムの運用管理体制）に準じ管理されるものとし、第 6 条（対象情報資産に関する情報セキュリティ）に従って、適切な利用を行わなければならない。

３ 業務目的外（私的利用）で SNS を利用する際には以下を遵守しなければならない。

（１）役職員等は SNS を私的利用する場合、当センターの非公開情報の漏えい、法律・公序良俗に違反する記載をしてはならない。一人ひとりの情報発信が、当センターを代表した発言として受け止められる可能性があることを理解し、全体に影響を持つことを十分に認識し、自分の発言には責任を持たなければならない。

（２）役職員等が関係各団体・個人等と SNS 上で交流する場合、双方の立場をわきまえ、 常に相手への敬意、配慮を忘れず、社会人として良識の範囲で交流しなければならない。

（３）役職員等は SNS のセキュリティ設定の問題により、自身の SNS のアカウントが乗っ取られ、悪用される可能性のあることに注意しなければならない。また、S NS の設定により、自分のプライバシーデータ、写真、位置情報等が予期せず公開される可能性のあることに注意しなければならない。

４ 当センターは、役職員等が SNS を私的利用する場合、利用者間または第三者間のトラブルによって役職員等または第三者に生じるいかなる損害についても、一切の責任を負うものではない。

（情報の発信）

第１３条　いかなる場合においても、下記に該当する情報の発信は禁止する。また、情

報の閲覧に関しても同様とする。

- 著作権、商標、肖像権を侵害するおそれのあるもの
- 役職員等および第三者のプライバシーを侵害するおそれのあるもの
- 他者の社会的評価にかかわる問題に関するもの
- 他者の名誉・信用を傷つけるおそれのあるもの
- 当センターの信用・品位を傷つけるおそれのあるもの
- わいせつな内容に該当するおそれのあるもの
- 不正アクセスを助長するおそれのあるもの
- 違法行為または違法行為をあおるおそれのあるもの
- 役職員等の個人的な状況や意見等の情報（職務上必要な場合を除く）
- 人種、思想、信条、職業等の差別、または差別を助長させるもの
- 単なる噂(信頼性の確保できない情報)や噂を助長させるもの
- 営利を目的とするもの
- 当センターの機密情報、職務上知り得た秘密や個人情報を含む情報
- その他公序良俗に反するおそれのあるもの

（マルウェアやサイバー攻撃対策）

第１４条　サイバー攻撃は多種多様であるため、情報漏洩リスク、事業継続リスク、賠償責任リスク、風評リスクなど、大きなダメージを受けかねないことを理解し、システム統括管理責任者は常にサイバー攻撃を受ける可能性があるという危機意識を持って最新の対策を講じなくてはならない。

２ 情報システム担当責任者等は、当センターの全てのサーバ、PC およびスマートデバイス（業務に利用する私有スマートデバイスも含む）にマルウェア対策ソフトウェアを導入しなければならない。

３ 役職員等は、PC 等利用する際には、マルウェア対策ソフトウェアの常駐設定を確認し、ファイルへのアクセス等、常時スキャンできるように設定していなければならない。

４ 役職員等は、利用している PC 等について、常時スキャンだけではなく一週間に一度、ファイル全体に対するスキャンを実施するように設定する。

５ 役職員等よりマルウェア感染の連絡を受けた情報システム担当責任者等は、即刻ネットワーク機能を停止することを指示し、現状の把握をすると同時に、速やかにシステム統括管理責任者に報告しなければならない。

６ マルウェアが検知された場合、情報システム担当責任者等は、そのマルウェアの特性上どのような挙動を示すか予測し、影響範囲の特定を行い、マルウェアが検知されなかった場合、ファイアウォールのログを確認し、怪しいログが残っていないかどうかを確認するなどして、原因の特定を行わなくてはならない。

７ 経済産業省が定めている「サイバーセキュリティ経営ガイドライン」に則り対策を進める。

（マルウェアやサイバー攻撃に関する教育の受講）

第１５条　PC、およびシステム、ネットワークの利用にあたっては、役職員等はマルウェアやサイバー攻撃に関する基本的な知識を理解しなければならない。そのためにシステム統括管理責任者は、役職員等で行うミーティングの場を利用して定期的に最新の情報を共有しなければならない。

（WEB サービス・インターネットおよびネットワーク利用におけるセキュリティ対策）

第１６条　インターネット閲覧によるマルウェア感染を防ぐ為に、役職員等は、業務上関係のないサイトの閲覧をしてはならない。

２ 役職員等は、URL リンクをクリックするとき、リンク先の URL を確認してからクリックしなければならない。この場合、リンク先が、信頼できない URL である場合は、クリックしてはならない。また、バナー広告についても同様で、業務上必要のないバナー広告はクリックしてはならない。

３ 役職員等は、業務上不必要なファイルやソフトウェア、不審なファイルなどをダウンロードしてはならない。

４ 役職員等は、当センター内外の WEB サーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃や不正なアクセスを目的として当センター内外のシステムを利用してはならない。

５ 他人の ID を用いて、当センター内外のネットワーク、インターネット上のサイトへアクセスしてはならない。

６ 役職員等は、故意もしくは不注意を問わず、当センター内外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

（クラウドサービスの導入とセキュリティ対策）

第１７条　IT 基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、システム統括管理責任者がサービスプロバイダの情報として、必要な機能やセキュリティ対策等をあらかじめ十分評価したうえで選定しなければならない。

クラウドサービスは、インターネットに接続していればどこからでも利用でき便利である一方、第三者の不正アクセスのリスクが高くなるが、クラウドサービス自体のセキュリティは当センター側では制御ができないことを理解する。

２ クラウドサービスを提供する事業者の信頼性を確認するとともに、そのクラウドサービスの稼働率やサービス品質保証により安全・信頼性を確認しなければならない。

３ クラウドサービスの利用が終了した時のデータの取り扱い条件、個人情報保護など関連法規制の遵守などを規定した利用規約等についても前もって確認しなければならない。

４ 新規クラウドサービス等の外部クラウドサービス等の導入は、理事長の許可を得て行う。

（クラウドサービスの運用・管理）

第１８条　クラウドサービスを安全に利用するために、当センターの情報システム担当責任者等を管理担当者とし、クラウドサービスを利用する役職員等の利用範囲と、権限を適切に管理するための運用体制を決定する。

２ クラウドサービスの利用においては、なりすましや不正ログインを防ぐために、パスワードなどの認証機能を適切に設定・管理しなれればならない。

３ クラウドサービスを利用する際は、以下Ａからバックアップ機能を確認し、必要に応じて独自のバックアップ対策を実施するなど、サービス停止やデータの消失・改ざん等に、自ら責任を持って備えなければならない。

Ａ．クラウドサービスに付帯するバックアップ機能及び復元機能

Ｂ．クラウドサービス利用者自身が追加・開発するバックアップ機能及び復元機能

Ｃ．バックアップデータの暗号化（暗号化の必要性を含む）

Ｄ．バックアップデータのローカルでの保管及び隔地保管

Ｅ．バックアップデータの保存期間

（本規程についての教育・普及）

第１９条　システム統括管理責任者は、役職員等に対して、本規程に乗っ取り情報の適正な管理についての 教育・普及に努めなければならない。 そのためにシステム統括管理責任者は、役職員等で行うミーティングの場を利用して本規程について周知徹底をしなければならない。

（規程等の遵守）

第２０条　役職員等は、情報セキュリティの重要性を認識の上、本規程およびその他の情報セキュリティに関連する各種法令、国が定める指針およびその他の規範および第三者との契約に定められた事項を遵守しなければならない。

２ 以下列挙する。

（１）サイバーセキュリティ基本法（平成 26 年法律第 104 号）

（２）著作権法（昭和 45 年法律第 48 号）

（３）不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

（４）不正競争防止法（平成 5 年法律第 47 号）

（５）特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）

（６）個人情報の保護に関する法律（平成 15 年法律第 57 号）

（７）サイバーセキュリティ経営ガイドライン（経済産業省／IPA）

（８）組織における内部不正防止ガイドライン（IPA）

（違反時の措置）

第２１条　故意、重過失により当センターの情報・情報システム等をき損させた場合は、その原因を作った役職員等に修復費用の弁済を求めることがある。

２ 本規程およびその他の関係規程類への違反が明らかになった場合は、コンプライアンス規程および就業規則等の定めに従い、違反を行った役職員等に対する処分を行うものとする。

（例外事項）

第２２条　業務都合等により本規程の遵守事項を守れない状況が発生した場合は、システム統括管理責任者に報告し、例外の適用承認を受けなければならない。

附 則

（規程の改廃）

第２３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２４条 この規程は、２０２０年７月１日から施行する。