一般財団法人日本救急医療財団
個人情報セキュリティ管理規程

（目　的）

第１条　この規程は、一般財団法人日本救急医療財団（以下「当財団」という。）の個人情報保護規程第１３条の規定に基づき当財団の情報セキュリティ管理に必要な規程を定める。

（対象範囲）

第２条　当財団の情報セキュリティに関する管理については、個人情報保護規程によるほか、この規程に定めるところによる。

２　情報資産の範囲は、次のとおりとする。

（１）ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

（２）ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

（３）情報システムの仕様書及びネットワーク図等のシステム関連文書

（組織体制）

第３条　情報セキュリティ管理に関しての責任者を置く。

２　常務理事を、情報統括管理責任者とする。情報統括管理責任者は、当財団における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

３　事務局長を、情報統括管理責任者直属の統括情報セキュリティ管理責任者とする。統括情報セキュリティ管理責任者は情報統括管理責任者を補佐しなければならない。

（１）統括情報セキュリティ管理責任者は、当財団の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

（２）統括情報セキュリティ管理責任者は、当財団の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

（３）統括情報セキュリティ管理責任者は、情報セキュリティ管理責任者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

（４）統括情報セキュリティ管理責任者は、当財団の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、情報統括管理責任者の指示に従い、情報統括管理責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

（５）統括情報セキュリティ管理責任者は、当財団の共通的なネットワーク、情報　システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

（６）統括情報セキュリティ管理責任者は、緊急時等の円滑な情報共有を図るため、情報統括

管理責任者、統括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、情報システム担当者を網羅する連絡体制を整備しなければならない。

4　各部局の長を情報セキュリティ管理責任者とする。

（1）情報セキュリティ管理責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

（2）情報セキュリティ管理責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

（3）情報セキュリティ管理責任者は、その部局において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等（職員、非常勤職員及び派遣職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

5　各部局の長を、当該情報システムに関する情報システム管理責任者とする。

（1）情報システム管理責任者は、情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

（2）情報システム管理責任者は、情報システムにおける情報セキュリティに関する権限及び責任を有する。

（3）情報システム管理責任者は、情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

6　各部局の係員を、情報システム担当者とする。情報システム担当者は、情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（情報資産の分類と管理方法）

第4条　当財団における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱の制限を行うものとする。

2　機密性による情報資産の分類、分類基準、取扱制限は、次により行う。

（1）機密性3　財団の事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産。

（2）機密性2　財団の事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産。

一　私物パソコンでの作業禁止（機密性3の情報資産に対して）

二　必要以上の複製及び配付禁止

三　保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止

四　情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納

五　復元不可能な処理を施しての廃棄

六　信頼のできるネットワーク回線の選択

七　外部で情報処理を行う際の安全確認

八　外部記録媒体の施錠可能な場所への保管

（3）機密性１　機密性２又は機密性３の情報資産以外の情報資産。

一　完全性２　財団の事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、個人の権利が侵害される、又は財団の事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産。

①　バックアップ

②　外部で情報処理を行う際の安全確認

③　外部記録媒体の施錠可能な場所への保　管

二　完全性１　完全性２情報資産以外の情報資産。

①　可用性２　財団の事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、個人の権利が侵害される、又は財団の事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産

②　バックアップ、指定する時間以内の復旧

③　外部記録媒体の施錠可能な場所への保管

3　情報資産の管理は、次により行う。

（1）情報セキュリティ管理責任者は、その所管する情報資産について管理責任を有する。

（2）情報資産が複製又は伝送された場合には、複製等された情報資産も適正に管理しなければならない。

（3）職員等は、情報資産について適切な管理を行わなければならない。

（4）情報の作成。

一　職員等は、業務上必要のない情報を作成してはならない。

二　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（5）情報資産の入手。

一　当財団の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

二　当財団の者が作成した情報資産を入手した者は、当該情報の分類と取扱制限を順守しなければならない。

三　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理責任者に判断を仰がなければならない。

（6）情報資産の利用。

一　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

二　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

三　情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されてい

る場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

（７）情報資産の保管。

一　情報セキュリティ管理責任者又は情報システム管理責任者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

二　情報セキュリティ管理責任者又は情報システム管理責任者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

三　情報セキュリティ管理責任者又は情報システム管理責任者は、機密性２以上、完全性２又は可用性２の情報を記録した外部記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（８）電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

（９）情報資産の運搬。

一　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

二　機密性２以上の情報資産を運搬する者は、情報セキュリティ管理責任者に許可を得なければならない。

（１０）情報資産の提供・公表。

一　機密性２以上の情報資産を外部に提供する者は、必要に応じパスワードの設定を行わなければならない。

二　機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理責任者に許可を得なければならない。

三　情報セキュリティ管理責任者は、公開する情報資産について、完全性を確保しなければならない。

（１１）情報資産の廃棄。

一　機密性２以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

二　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

三　情報資産の廃棄を行う者は、情報セキュリティ管理責任者の許可を得なければならない。

（物理的セキュリティ）

第５条　当財団における物理的セキュリティについては、次により管理するものとする。

２　物理的セキュリティについては、次により行う。

（1）サーバ等の管理

一　情報システム管理責任者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

二　通信ケーブル等の配線

①　情報システム管理責任者は、統括情報セキュリティ管理責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電、落雷等による過電流に対して、情報を保護するためのバックアップ措置を講じなければならない。

②　統括情報セキュリティ管理責任者及び情報システム管理責任者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、必要な措置を講じなければならない。

③　統括情報セキュリティ管理責任者及び情報システム管理責任者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

④　統括情報セキュリティ管理責任者及び情報システム管理責任者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

⑤　統括情報セキュリティ管理責任者及び情報システム管理責任者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

三　機器の定期保守及び修理

①　情報システム管理責任者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

②　情報システム管理責任者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理責任者は、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

四　情報システム管理責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（2）通信回線及び通信回線装置の管理

一　統括情報セキュリティ管理責任者は、通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

二　統括情報セキュリティ管理責任者は、外部へのネットワーク接続を必要最低限に限定し、

できる限り接続ポイントを減らさなければならない。

三　統括情報セキュリティ管理責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

四　統括情報セキュリティ管理責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（３）職員等のパソコン等の管理

一　情報システム管理責任者は、執務室等のパソコン等の端末について、盗難防止のための措置を講じなければならない。

二　情報システム管理責任者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

（人的セキュリティ）

第６条　人的セキュリティについては、次により管理するものとする。

２　職員等の遵守事項については、次により行うものとする。

（１）職員等の遵守事項

一　職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理責任者に相談し、指示を仰がなければならない。

二　職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

三　パソコン等の端末の持ち出し及び外部における情報処理作業の制限。

①　情報統括管理責任者は、機密性２以上、可用性2、完全性2 の情報資産を外部で処理する場合における安全確認をしなければならない。

②　職員等は、当財団のパソコン等の端末、記録媒体、情報資産及びソフトウエアを外部に持ち出す場合には、情報セキュリティ管理責任者の許可を得なければならない。

③　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理責任者の許可を得なければならない。

④　職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理責任者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

四　職員等は、私物のパソコン及び記録媒体を持ち込んではならない。ただし、業務上必要な場合は、情報セキュリティ管理責任者の許可を得て、これらを持ち込むことができる。

五　情報セキュリティ管理責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

六　職員等は、パソコン等の端末のソフトウエアに関するセキュリティ機能の設定を情報セキュリティ管理責任者の許可なく変更してはならない。

七　職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三者に使用されること、又は情報セキュリティ管理責任者の許可なく情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

八　職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（2）情報セキュリティ管理責任者は、非常勤及び派遣職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び派遣職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

（3）情報セキュリティ管理責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（4）情報セキュリティ管理責任者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

3　研修・訓練等については、次により行うものとする。

（1）情報統括管理責任者は、必要に応じて情報セキュリティに関する研修・訓練を実施しなければならない。

（2）研修計画の立案及び実施

一　情報統括管理責任者は、幹部を含めすべての職員等に対する情報セキュリティに関する研修計画を必要に応じて立案しなければならない。

二　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

三　研修は、統括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、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（3）情報統括管理責任者は、緊急時対応を想定した訓練を必要に応じて実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるようにしなければならない。

（4）幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

4　事故、欠陥等の報告については、次により行うものとする。

（1）職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ管理者に報告しなければならない。

（2）報告を受けた情報セキュリティ管理責任者は、当該事故等が情報システムに関連する場

合、速やかに統括情報セキュリティ管理責任者及び情報システム管理責任者に報告しなければならない。

（3）情報セキュリティ管理責任者は、報告のあった事故等について、必要に応じて情報統括管理責任者及び情報セキュリティ管理責任者に報告しなければならない。

（4）職員等は、当財団が管理するネットワーク及び情報システム等の情報資産に関する事故、欠陥について、外部から報告を受けた場合、情報セキュリティ管理責任者に報告しなければならない。

（5）報告を受けた情報セキュリティ管理責任者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ管理責任者及び情報システム管理責任者に報告しなければならない。また、当該事故等がネットワークに関連する場合は、統括情報セキュリティ管理責任者に報告しなければならない。

（6）情報セキュリティ管理責任者は、当該事故等について、必要に応じて情報統括管理責任者及び情報セキュリティ管理責任者に報告しなければならない。

（7）統括情報セキュリティ管理責任者は、事故等を引き起こした部門の情報セキュリティ管理責任者及び情報システム管理責任者と連携し、これらの事故等を分析し、記録を保存しなければならない。

5　職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

（1）パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

（2）パスワードを記載したメモを作成してはならない。

（3）パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

（4）パスワードが流出したおそれがある場合には、情報セキュリティ管理責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

（5）パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

（6）複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

（7）仮のパスワードは、最初のログイン時点で変更しなければならない。

（8）パソコン等の端末のパスワードの記憶機能を利用してはならない。

（9）職員等間でパスワードを共有してはならない。

（技術的セキュリティ）

第7条　技術的セキュリティについては、次により管理するものとする。

2　コンピュータ及びネットワークの管理については、次により行うものとする。

（1）文書サーバーの設定等

一　情報システム管理責任者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

二　情報システム管理責任者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

三　情報システム管理責任者は、住民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（2）統括情報セキュリティ管理責任者及び情報システム管理責任者は、ファイルサーバ等に記録された情報について、必要に応じて定期的にバックアップを実施しなければならない。

（3）情報システム管理責任者は、他の団体と情報システムに関する情報及びソフトウエアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ管理責任者及び情報セキュリティ管理責任者の許可を得なければならない。

（4）システム管理記録及び作業の確認

一　情報システム管理責任者は、所管する情報システムの運用において実施した作業について、記録しなければならない。

二　統括情報セキュリティ管理責任者及び情報システム管理責任者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録し、窃取、改ざん等をされないように適切に管理しなければならない。

三　統括情報セキュリティ管理責任者、情報システム管理責任者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2名以上で確認しなければならない。

（5）統括情報セキュリティ管理責任者及び情報システム管理責任者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（6）統括情報セキュリティ管理責任者及び情報システム管理責任者は、職員等からのシステム障　害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（7）ネットワークの接続制御、経路制御等

一　統括情報セキュリティ管理責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウエア等を設定しなければならない。

二　統括情報セキュリティ管理責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（8）情報システム管理責任者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（9）外部ネットワークとの接続制限等

一　情報システム管理責任者は、所管するネットワークを外部ネットワークと接続しようとする場合には、情報統括管理責任者及び統括情報セキュリティ管理責任者の許可を得なければならない。

二　情報システム管理責任者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、内部のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

三　情報システム管理責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

四　統括情報セキュリティ管理責任者及び情報システム管理責任者は、ウェブサーバ等をインターネットに公開する場合、ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

五　情報システム管理責任者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ管理責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（１０）統括情報セキュリティ管理責任者は、無線LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

（１１）電子メールのセキュリティ管理

一　統括情報セキュリティ管理責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

二　統括情報セキュリティ管理責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

三　統括情報セキュリティ管理責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

四　統括情報セキュリティ管理責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

五　統括情報セキュリティ管理責任者は、システム開発や運用等のための外部委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

（１２）電子メールの利用制限

一　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

二　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

三　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

四　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理責任者に報告し

なければならない。

五　職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（１３）無許可ソフトウエアの導入等の禁止

一　職員等は、パソコン等の端末に無断でソフトウエアを導入してはならない。

二　職員等は、業務上の必要がある場合は、統括情報セキュリティ管理責任者及び情報システム管理責任者の許可を得て、ソフトウェアを導入することができる。

三　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１４）機器構成の変更の制限

一　職員等は、パソコン等の端末に対し機器の改造及び増設・交換を行ってはならない。

二　職員等は、業務上、パソコン等の端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ管理責任者及び情報システム管理責任者の許可を得なければならない。

（１５）職員等は、統括情報セキュリティ管理責任者の許可なくパソコン等の端末をネットワークに接続してはならない。

（１６）業務以外の目的でのウェブ閲覧の禁止

一　職員等は、業務以外の目的でウェブを閲覧してはならない。

二　統括情報セキュリティ管理責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理責任者に通知し適切な措置を求めなければならない。

3　アクセス制御については、次により行うものとする。

（1）統括情報セキュリティ管理責任者又は情報システム管理責任者は、ネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

（2）職員等による外部からのアクセス等の制限

一　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ管理責任者及び当該情報システムを管理する情報システム管理責任者の許可を得なければならない。

二　統括情報セキュリティ管理責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

三　統括情報セキュリティ管理責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

四　統括情報セキュリティ管理責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

五　統括情報セキュリティ管理責任者及び情報システム管理責任者は、外部からのアクセス

に利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

六　職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

（3）パスワードに関する情報の管理

一　統括情報セキュリティ管理責任者又は情報システム管理責任者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

二　統括情報セキュリティ管理責任者又は情報システム管理責任者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（4）情報システム管理責任者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

4　システム開発、導入、保守等については、次により行うものとする。

（1）情報システムの調達

一　統括情報セキュリティ管理責任者及び情報システム管理責任者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

二　統括情報セキュリティ管理責任者及び情報システム管理責任者は、機器及びソフトウエアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（2）情報システムの開発

一　情報システム管理責任者は、システム開発の責任者及び作業者を特定しなければならない。

二　システム開発における責任者、作業者のＩＤの管理

① 情報システム管理責任者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

② 情報システム管理責任者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

三　情報システム管理責任者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

（3）情報システムの導入

一　開発環境と運用環境の分離及び移行手順の明確化

①　情報システム管理責任者は、システム開発・保守及びテスト環境からシステム運用環

境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

② 情報システム管理責任者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

二 テスト

① 情報システム管理責任者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

② 情報システム管理責任者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

③ 情報システム管理責任者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（4）システム開発・保守に関連する資料等の保管

一 情報システム管理責任者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

二 情報システム管理責任者は、テスト結果を一定期間保管しなければならない。

三 情報システム管理責任者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（5）情報システムにおける入出力データの正確性の確保

一 情報システム管理責任者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

二 情報システム管理責任者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

四 情報システム管理責任者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6）情報システム管理責任者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（7）情報システム管理責任者は、開発・保守用のソフトウエア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

5 不正プログラム対策については、次により行うものとする。

（1）統括情報セキュリティ管理責任者は、不正プログラム対策として、次の事項を措置しなければならない。

一 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへ

の侵入を防止しなければならない。

二　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

三　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

四　所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウエアを常駐させなければならない。

五　不正プログラム対策ソフトウエアのパターンファイルは、常に最新の状態に保たなければならない。

六　不正プログラム対策のソフトウエアは、常に最新の状態に保たなければならない。

（2）情報システム管理責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

一　サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウエアをシステムに常駐させなければならない。

二　不正プログラム対策ソフトウエアのパターンファイルは、常に最新の状態に保たなければならない。

三　不正プログラム対策のソフトウエアは、常に最新の状態に保たなければならない。

四　インターネットに接続していないシステムにおいて、記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、当財団が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウエアを導入し、定期的に当該ソフトウエア及びパターンファイルの更新を実施しなければならない。

（3）職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

一　パソコン等の端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

二　外部からデータ又はソフトウエアを取り入れる場合には、必ず不正プログラム対策ソフトウエアによるチェックを行わなければならない。

三　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

四　端末に対して、不正プログラム対策ソフトウエアによるフルチェックを定期的に実施しなければならない。

五　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行わなければならない。

六　統括情報セキュリティ管理責任者が提供するウイルス情報を、常に確認しなければならない。

七　コンピュータウイルス等の不正プログラムに感染した場合は、LAN ケーブルの即時取り外し又は機器の電源遮断を行わなければならない。

6　不正アクセス対策については、次により行うものとする。

（1）統括情報セキュリティ管理責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

一　使用されていないポートを閉鎖しなければならない。

二　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ管理責任者及び情報システム管理責任者へ通報するよう、設定しなければならない。

（2）情報統括管理責任者及び統括情報セキュリティ管理責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3）情報統括管理責任者及び統括情報セキュリティ管理責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）統括情報セキュリティ管理責任者及び情報システム管理責任者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの内部のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）統括情報セキュリティ管理責任者及び情報システム管理責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する情報セキュリティ管理責任者に通知し、適切な処置を求めなければならない。

7　セキュリティ情報の収集については、次により行うものとする。

（1）セキュリティホールに関する情報の収集・共有及びソフトウエアの更新等統括情報セキュリティ管理責任者及び情報システム管理責任者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウエア更新等の対策を実施しなければならない。

（2）統括情報セキュリティ管理責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（運　用）

第８条　運用については、次により管理するものとする。

2　情報システムの監視については、次により行うものとする。

（1）統括情報セキュリティ管理責任者及び情報システム管理責任者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

（2）統括情報セキュリティ管理責任者及び情報システム管理責任者は、重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じな

ければならない。

（3）統括情報セキュリティ管理責任者及び情報システム管理責任者は、外部と常時接続するシステムを常時監視しなければならない。

3　情報セキュリティポリシーの遵守状況の確認については、次により行うものとする。

（1）遵守状況の確認及び対処

一　情報セキュリティ管理責任者及び情報セキュリティ管理責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに情報統括管理責任者及び統括情報セキュリティ管理責任者に報告しなければならない。

二　情報統括管理責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

三　統括情報セキュリティ管理責任者及び情報システム管理責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（2）情報統括管理責任者及び情報統括管理責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

（3）職員等の報告義務

一　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ管理責任者及び情報セキュリティ管理責任者に報告を行わなければならない。

二　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ管理責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

4　侵害時の対応については、次により行うものとする。

（1）当財団は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切に対処しなければならない。

（2）緊急時対応計画には、以下の内容を定めなければならない。

一　関係者の連絡先

二　発生した事案に係る報告すべき事項

三　発生した事案への対応措置

四　再発防止措置の策定

（3）当財団が自然災害等に備えて事業継続計画を策定する場合、当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4）当財団は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

5　外部委託については、次により行うものとする。

（1）情報セキュリティ管理責任者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（2）情報システムの運用等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

一　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

二　委託先の責任者、委託内容、作業者、作業場所の特定

三　提供されるサービスレベルの保証

四　従業員に対する教育の実施

五　提供された情報の目的外利用及び受託者以外の者への提供の禁止

六　業務上知り得た情報の守秘義務

七　再委託に関する制限事項の遵守

八　委託業務終了時の情報資産の返還、廃棄等

九　委託業務の定期報告及び緊急時報告義務

十　財団による監査、検査

十一財団による事故時等の公表

十二情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（3）情報セキュリティ管理責任者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ管理責任者に報告するとともに、その重要度に応じて情報統括管理責任者に報告しなければならない。

6　例外措置については、次により行うものとする。

（1）情報セキュリティ管理責任者及び情報システム管理責任者は、情報セキュリティ管理関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、情報統括管理責任者の許可を得て、例外措置を取ることができる。

（2）情報セキュリティ管理責任者及び情報システム管理責任者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに情報統括管理責任者に報告しなければならない。

（3）情報統括管理責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

7　職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

（1）当財団就業規則及び服務規程

（2）著作権法（昭和四十五年法律第四十八号）
（3）不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）
（4）個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）
（5）当財団個人情報保護規程

8　懲戒処分等については、次により行うものとする。
（1）情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、当財団の就業規則による懲戒処分の対象とする。
（2）職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。
一　統括情報セキュリティ管理責任者が違反を確認した場合は、統括情報セキュリティ管理責任者は当該職員等が所属する課室等の情報セキュリティ管理責任者に通知し、適切な措置を求めなければならない。
二　情報システム管理責任者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ管理責任者及び当該職員等が所属する課室等の情報セキュリティ管理責任者に通知し、適切な措置を求めなければならない。
三　情報セキュリティ管理責任者の指導によっても改善されない場合、統括情報セキュリティ管理責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ管理責任者は、職員等の権利を停止あるいは剥奪した旨を情報統括責任者及び当該職員等が所属する課室等の情報セキュリティ管理責任者に通知しなければならない。

（監　査）
第９条　監査については、次により管理するものとする。
（1）統括情報セキュリティ管理責任者を情報セキュリティ監査統括責任者とし、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行うものとする。
（2）監査を行う者の要件
一　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
二　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。
（3）監査実施計画の立案及び実施への協力
一　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案しなければならない。
二　被監査部門は、監査の実施に協力しなければならない。
（4）外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業

者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。

（5）情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（6）情報統括管理責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（7）監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

2　自己点検については、次により管理するものとする。

（1）実施方法

一　統括情報セキュリティ管理責任者及び情報システム管理責任者は、所管するネットワーク及び情報システムについて、必要に応じ自己点検を実施しなければならない。

二　情報セキュリティ管理責任者は、情報セキュリティ管理責任者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じ自己点検を行わなければならない。

（2）統括情報セキュリティ管理責任者、情報システム管理責任者及び情報セキュリティ管理責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（3）自己点検結果の活用

一　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

二　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3　情報セキュリティ委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要があると認めた場合、その見直しを行うものとする。

附　則

この規程は、平成１９年　４月　１日から施行する。

附　則

この規程の改正は、平成２４年　４月　１日から実施する。