一般財団法人神戸住環境整備公社

情報セキュリティポリシー

制定日：平成 22 年 6 月 30 日
改正日：令和 5 年 10 月 1 日
施行日：令和 5 年 10 月 1 日

［ 目 次 ］

第１章　総論

１．目的

一般財団法人神戸住環境整備公社（以下、「公社」という。）の情報システムが取り扱う情報の重要性に鑑み、これらの情報を様々の脅威から防御し、情報資産の機密性、完全性及び可用性を維持するため、公社情報セキュリティポリシー（以下、「情報セキュリティポリシー」という。）を定める。

２．情報セキュリティポリシーの体系

この情報セキュリティポリシーは、公社の情報セキュリティ対策の基本で、基本方針と対策基準で構成される。

３．用語の定義

この情報セキュリティポリシーで使用する用語の定義は次のとおりとする。

1	ネットワーク	コンピュータ等を相互接続する通信網及びその周辺機器（ハード・ソフトの両ウェア）
2	情報システム	コンピュータ及びネットワークで構成され、情報処理を行う仕組み。
3	データ	電子計算機処理に係る記録媒体（入出力帳票、磁気テープ、磁気ディスク等）に記録されている情報又は通信回線により送信される情報。
4	情報セキュリティ	情報資産の機密性、完全性及び可用性を維持すること。
5	機密性	承認された者のみが情報に、アクセスできる状態を確保すること。
6	完全性	情報の真性（改ざん、破壊、消去がない状態）を確保すること。
7	可用性	承認された者のみが必要時に、必要なだけ情報にアクセスする状態を維持すること。

第２章　基本方針

１．情報セキュリティポリシーの適用範囲

(1) 組織の範囲

「一般財団法人神戸住環境整備公社組織規程」に規定する範囲とする。

(2) 情報資産の範囲

情報セキュリティポリシーが対象とする情報資産の範囲は、次のとおりとする。

ア： ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ： 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。）

ウ： 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

(3) 情報資産の対象

公社が実施する業務で扱う情報資産を本基本方針の対象とする。

２．職員等の義務

職員、委託業務等従事者等公社の業務に従事する者（以下、「職員等情報取扱者」という。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたり情報セキュリティポリシーを遵守するものとする。

３．情報セキュリティ管理体制

情報セキュリティ対策を推進・管理するため、次の者を置く。

(1) 情報セキュリティ最高責任者：理事長を充てる。

(2) 情報セキュリティ統括責任者：経営企画部長を充てる。

(3) 情報セキュリティ管理者：総務課長を充てる。

(4) 情報ネットワーク管理者：総務課長を充てる。

(5) 情報責任者：各部長を充てる。

(6) 情報管理者：各ラインの課長及びこれに相当する長を充てる。

(7) 業務システム責任者：各業務システムを所管する部の長を充てる。

(8) 業務システム管理者：各業務システムを所管する課の長を充てる。

(9) 情報セキュリティ監査統括責任者：専務理事を充てる。

４．対象とする脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生頻度や程度・影響を考慮し、情報セキュリティ対策を講じる。特に次の脅威には、十分な対策を講じる。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥・操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震・落雷・火災等の災害によるサービス及び業務の停止等
(4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

５．情報セキュリティ対策

上記４の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

(1) 情報資産の分類と管理
公社の情報資産を機密性、完全性及び可用性で分類し、分類に応じた情報セキュリティ対策。

(2) 物理的セキュリティ
コンピュータ設置場所への入退室、サーバ等の管理、通信回線及び端末機器等への物理的な対策。

(3) 人的セキュリティ
職員等の情報セキュリティ遵守事項を定め、研修及び啓発を行う等の人的な対策。

(4) 技術的セキュリティ
コンピュータ等の管理、アクセス制御、コンピュータウイルスの感染防止等、不正プログラム対策及び不正アクセス対策等の技術的対策。

(5) 運用
情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託等を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するための情報セキュリティインシデント発生時の対応手順書の策定。

(6) 業務委託等及び外部サービスの利用
業務委託等をする場合には、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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確認し、必要に応じて契約に基づき措置を講じるなどの対策。
外部サービスを利用する場合には、外部サービス利用基準に基づく対策。

６．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況評価のため、定期的及び必要に応じて情報セキュリティ監査及び自己点検を実施する。

７．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、セキュリティポリシーを見直す。

８．情報セキュリティ対策基準の策定

上記５、６及び７に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

９．情報セキュリティの個別基準の策定

対策基準を補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準（以下「個別基準」という。）を策定するものとする。なお個別基準は、公にすることにより公社の事業運営に重大な支障を及ぼすおそれがあることから非公開とする。

１０．情報セキュリティ実施手順の策定

対策基準及び個別基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順（以下「実施基準」という。）を策定するものとする。なお実施手順は 公にすることにより公社運営に、重大な支障を及ぼすおそれがあることから非公開とする。

第３章 対策基準

第 2 章基本方針に基づき情報セキュリティ対策等を実施するために適用範囲における共通の基準として具体的な遵守事項及び判断基準を次のとおり定める。

１．権限と責任

(1) 情報セキュリティ最高責任者

ア： 情報セキュリティ最高責任者は、公社の全情報資産の管理および情報セキュリティ対策につき、最終決定権限と責任を有する。

イ： 情報セキュリティ最高責任者は、情報セキュリティの専門家・職員をアドバイザーとしておくことができる。

ウ： サイバー攻撃もしくはそのおそれのあるもの、情報漏えいもしくはそのおそれのあるもの、システム上の欠陥及び誤動作のいずれか又は複数に該当する事案（以下「情報セキュリティインシデント」という。）に対処するための体制 （CSIRT Computer Security Incident Response Team 以下「 CSIRT 」という。）を整備し 役割を明確化する。

(2) 情報セキュリティ統括責任者

ア： 情報セキュリティ最高責任者を補佐する。

イ： 公社の全ての情報資産の開発、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。

ウ： 公社の情報資産の情報セキュリティ対策の統括的な権限及び責任を有する。

エ： 情報セキュリティ管理者、情報ネットワーク管理者、情報責任者、情報管理者、業務システム責任者、業務システム管理者に対して、情報セキュリティの指導及び助言を行う権限を有する。

オ： 公社の情報資産への情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、情報セキュリティ最高責任者の指示に従い、情報セキュリティ最高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実施する権限及び責任を有する。

カ： 緊急時等の情報提供を図るため、情報セキュリティ最高責任者、情報セキュリティ統括責任者、情報セキュリティ管理者、情報ネットワーク管理者、 情報責任者、情報管理者、業務システム責任者、業務システム管理者を網羅する連絡体制を整備しなけ

ればならない。

キ： 情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて情報セキュリティ最高責任者にその内容を報告しなければならない。

ク： 共通的なネットワーク、情報システム等の情報資産に関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

ケ： クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

(3) 情報セキュリティ管理者

情報セキュリティ管理者は､情報セキュリティ統括責任者を補佐し､その実務を担当する。

(4) 情報ネットワーク管理者

ア： 共通的なネットワーク、情報システム、情報等の情報資産における開発、設定の変更、運用見直し等を行う権限及び責任を有する。

イ： 共通的なネットワーク、情報システム、情報等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

ウ： 共通的なネットワーク、情報システム、情報等の情報資産に係る実施手順を策定し、その維持・管理を行う。

エ： 共通的なネットワーク、情報システム、情報等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は、情報セキュリティ統括責任者、情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

オ： 共通的なネットワーク、情報システム、情報等の情報資産のうちパーソナルコンピュータ等についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

(5) 情報責任者

ア： 所管する部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。

イ： 情報責任者は、情報管理者を監督し、所管する部等の緊急時等の連絡体制の整備並びに職員等に対する助言及び指示を行う。

(6) 情報管理者

ア： 所管課内の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

イ： 情報セキュリティ統括責任者又は情報セキュリティ管理者の指示に従い公社の情報資産のうち所管組織内のパーソナルコンピュータ等の物理的セキュリティに関する管理を行う。

ウ： 所管課内における情報等の情報資産への情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ管理者、情報ネットワーク管理者、情報責任者へ速やかに報告を行い、指示を仰がなければならない。

(7) 業務システム責任者

ア： 当該業務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。

イ： 当該業務システム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。

ウ： 当該業務システムに関する実施手順の維持・管理を行う統括的な権限及び責任を有する。

エ： 当該業務システムについて、緊急時等の連絡体制の整備、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情報取扱者に対する助言及び指示を行う。

(8) 業務システム管理者

ア： 当該業務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。

イ： 当該業務システムの情報セキュリティ対策に関する権限及び責任を有する。

ウ： 当該業務システムに係る実施手順を策定し、その維持・管理を行う。

エ： 当該業務システムにおける開発、設定の変更、運用等についての作業を業務システム管理者が指名する者に行わせることができる。業務システム管理者は、当該業務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。

(9) 情報セキュリティ監査統括責任者

情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

(10) 兼務の禁止

ア： 情報セキュリティ対策の実施上、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者または許可者は、同じ者が兼務してはならない。

イ： 監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。情報セキュリティ対策の実施上、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者または許可者は、同じ者が兼務してはならない。

(11) 代行

情報セキュリティ最高責任者に事故があるときは､情報セキュリティ統括責任者がその事務を代行する。

(12) CSIRT

ア： CSIRT の設置

（ア） 情報セキュリティ最高責任者は、 情報セキュリティの統一的な窓口機能を有するCSIRT を設置し、CSIRT に所属する職員等を選任しなければならない。情報セキュリティ管理者を CSIRT 責任者とする。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

（イ） 情報セキュリティ最高責任者は、情報セキュリティの統一的な窓口が情報セキュリティインシデントについて部課等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

イ： CSIRT の役割

（ア）情報セキュリティ最高責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部課等に提供しなければならない。

（イ）情報セキュリティインシデントを認知した場合には、 情報セキュリティ最高責任者、神戸市等へ報告しなければならない。

（ウ）情報セキュリティに関して、神戸市の情報セキュリティの統一的な窓口機能を有する部署、外部の事業者等との情報共有を行わなければならない。

２．情報資産の分類と管理

(1) 情報資産の管理責任

ア： 管理責任

情報資産は、情報管理者がそれぞれ所管する情報資産についての管理責任を有する。クラウドサービスの環境に保存される情報資産についても管理し、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。また、情報管理者は、当該情報資産の利用範囲を定める。

イ： クラウドサービス利用終了に関する内容の確認

情報管理者は、クラウドサービスを更改する際の情報資産の移行及び、これら情報資産の全複製がクラウドサービスから削除されることの記述を含む、サービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

ウ： 職員等情報取扱者の責任

職員等情報取扱者は、情報資産の作成・入手・利用等に際しては、十分にその責任を自覚した上で行わなければならない。

エ： 複製等の管理

情報管理者は、情報が複製又は送られた場合には、当該複製等も原本と同様に管理しなければならない。

(2) 情報資産の分類と管理方法

ア： 情報資産の分類

（ア）対象となる情報資産は、各々の情報資産の機密性 完全性及び可用性を踏まえ次の重要性分類に従って分類する。

重要性分類	対象項目
機密性２	・公開することでセキュリティ侵害が生じるおそれがあるデータ ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に公社の信頼を著しく害するおそれのあるデータ ・公開することでセキュリティ障害が生じるおそれがあるデータ
完全性２	改ざん・誤りがあると第三者の権利が侵害される又は事務の的確な遂行に支障を及ぼす可能性がある
可用性２	・利用できないと第三者の権利が侵害される又は公社事務の安定的な遂行に支障を及ぼす可能性がある ・滅失し又は損傷した場合その復元が著しく困難であるため事務の円滑な運営が妨げられるおそれのあるデータ
機密性１	直ちに一般公表を前提としていない（広報等は行っていない）もの
完全性１	改ざん・誤りがあると組織に軽微な影響の発生可能性がある
可用性１	一定時間以上利用不可能であると第三者の権利が侵害される、又は公社事務の安定的な遂行に支障をきたす可能性がある。

（イ）情報資産の機密性、完全性、可用性のいずれかの重要性分類が 2 に分類される情報資産はこの対策基準の対象とする。また、重要性分類がいずれも 1 の情報資産も必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

イ： 情報資産の管理

（ア）情報資産の分類の表示

情報資産について、ファイル（ファイル名 ファイルの属性（プロパティ） ヘッダー・フッター等）格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

（イ）情報の作成

① 職員等情報取扱者は、業務上必要のない情報を作成してはならない。

② 情報を作成する者は、情報の作成時に重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

③ 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。

（ウ）情報資産の入手

① 公社内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。

② 外部者が作成した情報資産を入手した者は、重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

③ 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、情報管理者に判断を仰がなければならない。

（エ）情報資産の利用

① 情報資産を利用する者は、情報資産を業務上の目的以外に利用してはならない。

② 情報資産の分類に応じ、利用者及びアクセス制限を定めずに情報資産を利用できない。

③ 機密性２のデータは、情報管理者の許可を得た場合、複写、複製、送付・電子メール送信を行うことができる。また、権限のある者だけがアクセスできる環境で、保存・利用しなければならない。複数の権限ある者で情報を共有するときや、所属外に情報を電子メール等により送信するときは、パスワード等による暗号化による情報漏えい対策を施さなければならない。ただし、電子メール等による送信に必要な宛名や連絡先等については、この限りではない。

④ 情報資産を利用する者は、記電磁的記録媒体又は紙媒体に情報資産の分類が異なるデータ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。

（オ）情報資産の保管

① 情報管理者は、情報資産の重要性分類に従って、情報資産を適正に保管しなければならない。

② 情報管理者は、持ち運び可能な電磁的記録媒体を保管する場合は、耐火、耐熱、耐水

及び耐湿を講じた施錠可能な場所へ保管しなければならない。

③ 情報管理者は、持ち運び可能な電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所へ保管しなければならない。

④ 情報ネットワーク管理者及び業務システム管理者は、利用頻度の低い電磁的記録や、情報システムのバックアップで取得した情報を記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域への保管を考慮しなければならない。

（カ）情報資産の運搬

① 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、パスワード等による暗号化を行う、機密情報を運搬する専用のサービスを利用する等、情報資産の不正利用防止のための措置を講じなければならない。インターネットを利用した外部サービス等委託事業者等へ重要な情報資産を運搬する場合は、アクセス制御等のシステム設定が適切にされているか等確認しなければならない。

② 機密性２以上の情報資産を運搬する者は、情報管理者に許可を得なければならない。

③ 機密性２以上の情報資産を運搬する者は、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底しなければならない。

（キ）情報資産の提供・公表

① 機密性２の情報資産の外部への提供者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

② 機密性２の情報資産の外部への提供者は、情報セキュリティ管理者の事前許可の下に、日時、担当者及び提供概要を記録しなければならない。

なお、公社以外の者に提供する場合は、次に掲げる事項を明記した覚書を公社理事長と提供先の代表者との間で取り交わすものとする。

・データの内容に関する事項
・データの利用する業務の根拠法令に関する事項
・データの利用目的に関する事項
・データの提供方法に関する事項
・データの秘密の保持に関する事項
・データの目的外の利用及び第三者への提供の禁止に関する事項
・データの複写及び複製の禁止に関する事項
・データの取扱いに関する事故の発生時における報告義務に関する事項
・データの返還又は廃棄が必要な場合にあっては、データの返還又は廃棄に関する事項
・データの利用又は管理の状況の実地による調査等が必要な場合にあっては、当該調査の実施に関する事項

③ 情報資産管理者は、一般財団法人神戸住環境整備公社情報公開要綱に基づく申請により、情報資産を公開するときには、公開する情報資産の完全性を確保しなければならない。

（ク）情報資産の廃棄等

① 情報資産の廃棄や機器のリース返却等を行う者は、情報を記録している電磁的記録媒体について、当該媒体の初期化等を行ったうえで物理的に破壊する等、復元不可能な状態にしなければならない。紙媒体が不要となった場合は、焼却 裁断 溶解等により

廃棄しなければならない。

② 情報資産の廃棄やリース返却等を行う者は、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。

③ 情報資産の廃棄や機器のリース返却を行う者は、情報管理者の許可を得なければならない。

④ クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

ウ： 文書の管理

（ア）対策基準を実施していくうえで必要な情報セキュリティに係る文書（以下「文書」という）は、一般財団法人神戸住環境整備公社公文書管理規程の定めに従い管理しなければならない。

（イ）文書を作成又は更新する場合は、情報責任者の承認を受けなければならない。

（ウ）文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

（エ）文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

エ： 記録の管理

対策基準の効果的運用の証拠として、記録を作成し、適切な管理をしなければならない。

３．物理的セキュリティ

(1) サーバ等の管理

ア： 入退室の管理

情報システム管理者及び業務システム管理者は、重要性分類２のデータが入っている記録媒体の保管場所及びそれを取扱うコンピュータ設置場所の入退室について、管理を行う。

特に、ネットワークの基幹機器及び重要な情報システムの設置部屋（以下「管理区域」という）は、次の事項に従い厳重な管理を行う。

（ア）管理区域を新設する場合は、外部からの進入が困難なものにする。

（イ）管理区域から外部に通ずるドアは必要最小限とし、無断立入りを防止する。

（ウ）情報システム室内の機器等に転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じる。

（エ） 許可された者のみが管理区域の機器の操作をすることでき、その他の者は必要以上に管理区域への入室することはできない。

（オ） 外部からの訪問者が管理区域に入室する場合、管理区域への入退室を許可された者が付き添って管理区域に入室する。

（カ）管理区域について、当該システムに関連しない又は個人所有である端末、モバイル端末（執務区域外に持ち出して使用が可能な端末）、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（キ）情報管理者は、執務区域については、許可された者以外の立入を制限するなどの適正な入退室管理を行わなければならない。

イ： 情報ネットワーク管理者・業務システム管理者・情報管理者は「ウ：～コ：」につき次のことを行う。

ウ： 装置の取付け等

（ア）ネットワーク機器及び情報システム機器の取付けの場合、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正な固定を行う等必要な措置を講じなければならない。

（イ）システムの停止で、重大な影響を及ぼすおそれがあるものについては可能な限り二重化等を行う。

（ウ）利用者の ID、パスワード等の設定により、権限外の者の容易な操作を防止する。

エ： 電源

（ア）サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ）落雷等による過電流に対してサーバ等の機器を保護するための措置を講じなければならない。

オ： 配線

（ア）配線の変更、追加は、情報ネットワーク管理者及び業務システム管理者等限られた者の権限とする。

（イ） 通信ケーブル及び電源ケーブルの損傷等防止に、配線収納管の使用等必要な措置を施さなければならない。

（ウ） 施設管理部門から主要箇所の通信ケーブル及び電源ケーブルの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。

（エ）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正に管理しなければならない。

（オ） 自ら又は職員等及び契約により操作を認められた委託事業者等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講じなければならない。

カ： 機器等の定期保守及び修理

（ア）可用性２のサーバ等の機器は、定期保守を実施しなければならない。

（イ）記憶装置等を内蔵する機器を外部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、事業者に故障を修理させるにあたり、委託事業者等との間で、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。

キ： 消火薬剤及び消防用設備

管理区域に配置する消火薬剤及び消防用設備等が機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

ク： 敷地外への機器の設置

公社の事務所外にサーバ等の機器を設置する場合、情報セキュリティ統括責任者の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況に

ついて確認しなければならない。

ケ： 機器の廃棄等

（ア）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、全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。

（イ）クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする場合、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用すること。

コ： 機器等の搬出入

（ア）機器等を搬入する場合、予め、当該機器等の既存情報システムに与える影響について、 情報管理者が命じた者に確認を行わせる。

（イ）機器等の搬入出には情報管理者が命じた者が同行する等の必要な措置を行う。

(2) ネットワークの管理

情報ネットワーク管理者及び業務システム管理者は、次の「ア：」～「エ：」のとおりネットワークの管理を行わなければならない。

ア： 通信装置等及び通信装置等の文書の保管

公社内の通信回線及び通信回線装置を、施設管理部門と連携し、適正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正に保管しなければならない。

イ： 通信回線による外部へのネットワーク接続

通信回線による外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

ウ： 情報システムに通信回線を接続

所管する情報システムにおいて機密性２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、適正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や送信する情報を必要最小限にする等、情報保護のために適正な措置を講じなければならない。

エ： ネットワークおけるセキュリティ対策

（ア）ネットワークに使用する回線は伝送途上で情報が破壊、盗聴、改ざん、消去等が生じないよう十分なセキュリティ対策を実施しなければならない。

（イ）ネットワークで使用する回線を選択するにあたって、必要な可用性を考慮しなければならない。

(3) 端末等の管理

情報ネットワーク管理者・業務システム管理者は、次の「ア：」～「エ：」とおり端末等の管理を行う。

ア： 盗難防止

情報管理者は、執務区域等の端末等について、盗難防止のための措置を講じなければならない。また情報管理者は、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の措置を講じなければならない。

電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

イ： 情報システム及び端末のセキュリティ設定

情報システムへのログインに際し、パスワード、IC カード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。また、必要に応じて電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用するものとする。

ウ： 暗号化機能の利用

端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末等にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。また 電磁的記録媒体についても取り扱う情報の重要度に応じてデータ暗号化機能を備える媒体を使用しなければならない。

エ： モバイル端末のセキュリティ

（ア）モバイル端末とは、端末のうち執務区域外に持ち出して使用が可能な端末をいい、端末の形態は問わない。

（イ）紛失・盗難に遭った際の対応として、遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは、それらの機能を活用しモバイル端末内のデータを消去しなければならない。

（ウ）モバイル端末には覗き見防止の措置を講じなければならない。

（エ）モバイル端末を執務区域外で業務利用する場合は、上記対策に加え、端末の紛失・盗難対策として、普段からパスワードによる端末ロックを設定しておかなければならない。また、執務区域外で機密性２以上の情報を処理・保管する場合は、管理システム（MDM）を導入しなければならない。

４．人的セキュリティ

(1) 職員等情報取扱者の責務

職員等情報取扱者は「ア：」～「ケ：」に定める事項を守らなければならない。

ア： セキュリティポリシー等の遵守義務

セキュリティポリシー及びこれに基づく文書の規定事項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がある場合は、速やかに情報管理者等権限のある者に相談し、指示を仰がなければならない。

イ： 指示に基づいた情報資産の利用等

情報管理者等権限のある者の指示等に従い、情報資産を利用するとともに、又、開発、設定の変更、運用、更新等の作業を行う。

ウ： 支給以外の端末モバイル及び電磁的記録媒体等の業務利用

支給以外の端末モバイル端末及び電磁的記録媒体等（データ保存機能のないマウスやキーボード等の PC 周辺機器を除く）を原則として業務に利用してはならない。ただし、支給以外の端末の業務利用については，情報セキュリティ統括責任者が利用手順を定め、この利用手順に従い情報管理者の許可を得て利用することができる。

エ： 情報資産の持ち出し禁止

（ア） 所属外への持ち出し

情報管理者の許可を得た場合に限り、記録を作成したうえで、執務区域外へ情報資産を持ち出すことができる。

（イ） 持ち出しの記録

情報管理者は、端末等の持ち出しについて 記録を作成し保管しなければならない。

オ： 業務以外の目的での使用の禁止

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等を行ってはならない。

カ： 端末やモバイル端末におけるセキュリティ設定変更の禁止

（ア） 端末のソフトに関するセキュリティ機能の設定を情報ネットワーク管理者又は業務システム管理者の許可なく変更してはならない。

（イ）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管理者の許可なく情報を閲覧されることのないように、離席時の端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等の適正な措置を講じなければならない。

キ： 執務区域外における情報処理作業の制限

（ア）執務区域外で情報処理作業を行う場合には、情報管理者の許可を得なければならない。

（イ）執務区域外で端末を使用して情報処理作業を行う場合には，大量または機微な個人情報を取り扱ってはならない。また，公共の場又は公共の乗り物内においては個人情報の取り扱ってはならない。

（ウ）紛失・盗難を防止するため、 移動の際は細心の注意をもってモバイル端末を携行しなければならない。

（エ）覗き見を防止するため、執務区域外において職員等以外の目に触れないように取り扱わなければならない。

（オ）不正使用を防止するため、モバイル端末を使用しないときは、他者に端末が使用されないように必要な対策を取らなければならない。

（カ）モバイル端末でデータを保存する場合、指定されたファイルサーバの領域にデータを保存することとし、原則として端末内にデータを保存してはならない。

（キ）使用しているモバイル端末について、定期的に情報管理者の確認を受けなければならない。

（ク）執務区域外でモバイル端末を使用する場合 原則としてモバイル端末をプリンタに接続して、機密性 2 以上の情報資産の出力等を行ってはならない。

ク： 退職時の遵守事項

異動、退職等により従来の業務から離脱する場合には、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。

ケ： クラウドサービス利用時等の遵守事項

クラウドサービスの利用にあたっても情報セキュリティポリシー等を遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(2) 研修

ア： 情報セキュリティに関する研修・訓練

情報セキュリティ最高責任者は、定期的に情報セキュリティに関する研修・訓練を実施させなければならない。また、定期的にクラウドサービスを利用する職員等情報取扱者の情報セキュリティに関する意識向上、教育及び訓練を実施させるとともに、委託先等を含む関係者については委託先等で教育、訓練が行われていることを確認させなければならない。

イ： 研修計画の策定及び実施

（ア）情報セキュリティ統括責任者は、職員等情報取扱者に関する研修を実施する場合、研修計画を定期的に策定し、情報セキュリティ最高責任者に報告しなければならない。

（イ）職員等情報取扱者を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

（ウ）新規採用職員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。

（エ）研修は、情報セキュリティ統括責任者、情報セキュリティ管理者・情報ネットワーク管理者・情報責任者・情報管理者・職員等情報取扱者に対し、それぞれの役割、情報セキュリティへの理解度等に応じたものにしなければならない。

（オ）情報管理者は、所属の研修の実施状況を記録し、情報セキュリティ統括責任者及び情報責任者に対して、報告しなければならない。

（カ）情報セキュリティ統括責任者は、研修の実施状況を分析、評価し、情報セキュリティ最高責任者に、情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

ウ： 緊急時対応訓練

情報セキュリティ最高責任者は、緊急時対応を想定した訓練を定期的に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、訓練実施の体制範囲等を定め、また効果的に実施できるようにしなければならない。なお、情報セキュリティ最高責任者は、 緊急時対応訓練の実施結果を受けて、緊急時の体制や対応手順の改善を行わなければならない。

エ： 研修・訓練への参加

全ての職員等情報取扱者は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため、定められた研修・訓練に参加する。

(3) 情報セキュリティインシデントの報告

ア： 情報セキュリティインシデントの報告

（ア）職員等情報取扱者は、情報セキュリティインシデントを発見、若しくは外部から報告を受けた場合、速やかに情報管理者に報告しなければならない。

（イ）報告を受けた情報管理者は、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。また、当該情報セキュリティインシデントが公社のネットワークに関連する場合、情報ネットワーク管理者や業務システム管理者に対しても報告しなければならない。あわせて当該情報セキュリティインシデントの重要性又は緊急性によっ

ては、情報管理者から直接 CISO に報告しなければならない。

（ウ）業務システム管理者は、報告された情報セキュリティインシデントについて、必要に応じ業務システム責任者に報告しなければならない。

（エ）情報管理者は、報告のあった情報セキュリティインシデントについて、神戸市等業務上の関係機関に必要な連絡を行うとともに、情報責任者に報告しなければならない。また、情報セキュリティインシデントの重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

（オ） 情報セキュリティ統括責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みを構築させなければならない。

イ： 情報セキュリティインシデントの報告内容

（ア） 情報管理者等から情報セキュリティ管理者への報告は、以下の内容を含むものとする。

(1) 件名
(2) 判明した日時
(3) 発生した日時
(4) 通報者
(5) 事件事故等の内容
(6) 漏えいした情報
(7) 想定される原因
(8) 事件事故等への対応
(9) 復旧方針

（イ）業務システム管理者は、クラウドサービス事業者からの報告については、情報セキュリティインシデント発生時の報告手順を定め、クラウドサービス事業者の状況を適正かつ速やかに確認できるよう、インシデント発生時の報告に必要な要件を契約や SLA に定めるか、クラウドサービスの利用前に利用規約等を確認すること。

ウ： 情報セキュリティインシデント原因の究明・記録・再発防止等

（ア）CSIRT は､報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

（イ）CSIRT は、情報セキュリティインシデントであると評価した場合、情報セキュリティ最高責任者に速やかに報告しなければならない。

（ウ）CSIRT は、情報セキュリティインシデントに関係する情報管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

（エ）CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また 情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し 情報セキュリティ最高責任者に報告しなければならない。

（オ）情報セキュリティ最高責任者は、 CSIRT から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(4) アクセスのための認証情報及びパスワードの管理

ア： ID の管理

（ア） 情報システム管理者及び業務システム管理者は、ID の適正な管理を行わなければならない。

（イ）職員等情報取扱者は、自己の管理する ID に関し、次の事項を遵守しなければならない。

①他人に自己が利用している ID を利用させてはならない。

②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

イ： パスワードの管理

（ア）職員等情報取扱者は、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 パスワードは、他者に知られないように管理しなければならない。

② 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。

③ パスワードは十分な長さ（原則として 8 文字以上）とし、文字列は想像しにくいもの（英字（大文字・小文字区別有） 数字 記号を組み合わせたものなど）としなければならない。

④ パスワードを記載したメモを作成する場合は、特定の場所に施錠して保存する等により、他人が容易に見ることができない措置をとる。

⑤ パスワードが流出したおそれがある場合には、情報管理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。

⑥ 複数の情報システムを扱う職員等情報取扱者は、同一パスワードを複数システムで用いない。

⑦ 仮のパスワード（初期のパスワード含む）は、最初のログインの時点で変更しなければならない。

⑧ サーバ、ネットワーク機器及び端末等にパスワードを記憶させてはならない。

⑨ 職員等情報取扱者間でパスワードを共有してはならない（ただし共有 ID に対するパスワードは除く）。

（イ）情報ネットワーク管理者・業務システム管理者・情報管理者は、パスワードの照会等には一切応じない。

５．技術的セキュリティ

(1) コンピュータ及びネットワークの管理

ア： 情報の保存

情報の保存については、情報ネットワーク管理者及び業務システム管理者等管理権限のある者が定める方法により保存を行わなければならない。

イ： ファイルサーバの設定等

情報ネットワーク管理者が情報を共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

（ア）職員等情報取扱者が使用できるファイルサーバの容量を設定し、職員等情報取扱者に周知しなければならない。

（イ）ファイルサーバを所属等の単位で構成し、職員等情報取扱者が他所属等のフォルダ・

ファイルを閲覧・使用できないように設定しなければならない。

（ウ）特定の職員等情報取扱者が取扱う権限を持つ情報については、同一所属でも、権限のない者が閲覧及び使用できないよう設定しなければならない。

ウ： 情報ネットワーク管理者・情報管理者は、「エ：」～「セ：」の各項目のことを行わなければならない。

エ： ログの取得等

（ア）各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

（イ）ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

（ウ）取得したログを定期的に点検又は分析する機能を設け必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

（エ） システムから自動出力したログ等について 必要に応じ、外部記録媒体にバックアップしなければならない。

オ： 情報システム仕様書等の保管

ネットワーク構成図、情報システム仕様書等について、記録媒体の形態に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないように、適正に管理しなければならない。

カ： 情報資産のバックアップ

（ア）必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を実施しなければならない。

（イ）クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が公社の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップのための対応を実施しなければならない。

キ： 他団体との情報システムに関する情報等の交換

他団体と情報システムに関する情報及びソフトを交換する場合、その取扱いに関する事項をあらかじめ定め、情報セキュリティ統括責任者及び業務システム責任者の許可を得なければならない。

ク： システム管理記録及び作業の確認

（ア）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、作業記録を作成しなければならない。

（イ）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を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

（ウ）情報ネットワーク管理者及び業務システム管理者又は職員等情報取扱者がシステム変更等の作業を行う場合は、2 名以上で作業し、互いにその作業を確認しなければならない。

ケ： ネットワークの接続制御 経路制御等

（ア）アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また ネットワークサービスを利用する権限を有しない者が当該サービスを利用できるようにしてはならない。

（イ） 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ェア等を設定しなければならない。

（ウ）不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

コ： 外部の者が利用できるシステムの分離等

（ア）電子申請の汎用受付システム等、外部の者（情報取扱者以外の者）が利用できるシステムにおいては、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、情報セキュリティ対策について特に強固に対策を講じなければならない。

（イ）外部の者が利用できるシステムにおいて、機密性２以上の情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、不正アクセスを防止するため認証情報を設定しなければならない。

（ウ）外部の者が利用できるシステムにおいて、個人情報の保護に関する法律施行令第２条に規定する要配慮個人情報または財産的価値のある情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、多段階認証又は多要素認証を利用できるようにしなければならない。

サ： 外部ネットワークとの接続制限等

（ア）外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、適用範囲における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。

（イ）接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。当該外部ネットワークの瑕疵により公社のデータの漏えい、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応するため、必要に応じて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するよう努めなければならない。

（ウ） ウェブサーバ等をインターネットに公開する場合、公社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上で接続しなければならない。

（エ） 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 適用範囲における情報資産に脅威が生じることが想定される場合には 速やかに当該外部ネットワークとの接続を物理的に遮断しなければならない。

シ： Web サイトでの情報公開時の注意事項

（ア）Web サイトにより情報を公開・提供する場合に、所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、DoS 攻撃等を防止しなければならない。

また なりすまし防止などの観点から、ドメイン変更時に旧ドメインを一定期間保有したりするなどドメインを適正に設定し管理しなければならない。

（イ）メールシステムを含め各業務システムにおいても他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策等適正な管理をしなければならない。

（ウ）新たに Web サイトを公開する場合、全てのページで TLS 通信を利用すること。なお現状未対応の公開 Web サイトは、全てのページで TLS 通信を利用するために必要な作業を実施しなければならない。

ス： 複合機のセキュリティ管理

（ア）複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

（イ）複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

（ウ）複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

セ： IoT 機器を含む 特定用途機器のセキュリティ管理

所管する特定用途機器について、 取り扱う情報利用方法、通信回線への接続形態等により何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

ソ： 無線 LAN 等の利用

（ア）職員等情報取扱者は、公社の管理するネットワーク（以下「内部ネットワーク」という。）において、無線 LAN を利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。

（イ）合理的な理由があり情報セキュリティ統括責任者が情報セキュリティを確保するために別途定める要件を満たす場合、 情報セキュリティ管理者の許可を得て無線 LAN を利用した接続等を行うことができる。

タ： 無許可ソフトウェアの導入等の禁止

（ア）職員等情報取扱者は、端末やモバイル端末に情報ネットワーク管理者に無断でソフトウェアを導入してはならない。

（イ）職員等情報取扱者は、業務を円滑に遂行するために必要なソフトウェアがある場合、情報ネットワーク管理者が定める手続きを行い必要な許可を得て導入することができる。

（ウ）職員等情報取扱者は、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用してはならない。

チ： 機器構成の変更の禁止

職員等情報取扱者は、ネットワーク及び各自に供与された端末等に対して、端末及びその他機器の接続、増設又は改造を行ってはならない。軽微な機器の増設の場合は、情報システム管理者及び業務システム管理者等権限のある者の許可を必要とする。

ツ： 電子メールのセキュリティ管理

（ア）電子メールの利用を希望する場合は、その所属長が利用者を特定し、メールアドレスの取得を申請するものとする。

（イ）情報ネットワーク管理者及び業務システム管理者は、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。

（ウ）情報ネットワーク管理者及び業務システム管理者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

（エ）情報セキュリティ管理者は、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。

（オ）メールアドレス保有者の義務

① 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。

② 複数の宛先に電子メールを送信する場合、必要な場合以外、他の送信先のメールアドレスがわからないようにしなければならない。

③ 重要な電子メールの誤送信をした場合、情報管理者に報告しなければならない。

④ 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。

テ： 電子署名・暗号化

（ア）職員等情報取扱者は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性の確保することが必要な場合には、情報セキュリティ統括責任者が定めた電子署名、暗号化又はパスワード設定等セキュリティを考慮して、送信しなければならない。

（イ）職員等情報取扱者は、暗号化を行う場合に情報セキュリティ統括責任者が定める以外の方法を用いてはならない。また 情報セキュリティ統括責任者が定めた方法で暗号のための鍵を管理しなければならない。

（ウ）情報セキュリティ統括責任者は、電子署名の正当性を検証するための情報又は手段を署名検証者へ安全に提供しなければならない。

ト： 無許可でのネットワーク接続の禁止

（ア）職員等情報取扱者は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者及び業務システム管理者等権限のある者によって定められたネットワークと異なるネットワークに接続してはならない。

（イ）情報ネットワーク管理者及び業務システム管理者等権限のある者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限するよう努めなければならない。

ナ： 利用可能なネットワークプロトコル

職員等情報取扱者が利用できるネットワークプロトコルは、業務上必要最低限のものとする。

二： 障害記録

情報ネットワーク管理者及び業務システム管理者は、所管するシステムにおいて、職員等情報取扱者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体系的に記録し、適正に保存しなければならない。

ヌ： 業務以外の目的での Web サイト閲覧の禁止

（ア）職員等情報取扱者は、業務以外の目的で Web サイトを閲覧してはならない

（イ）情報ネットワーク管理者及び業務システム管理者等権限のある者は、職員等情報取扱者のウェブ利用について、明らかに業務に関係のないWebサイトを閲覧していることを発見した場合は、情報管理者に通知し適正な措置を求めなければならならない。

ネ： Web会議サービス利用時の対策

（ア）職員等情報取扱者は、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

（イ）職員等情報取扱者は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

ノ： ソーシャルメディアサービスの利用

（ア）情報管理者は、公社が管理するアカウントでソーシャルメディアサービスを利用する場合、次の情報セキュリティ対策を行わなければならない。

① 公社のアカウントによる情報発信が、実際の公社のものであることを明らかにするために、公社の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

② パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

（イ）機密性２の情報はソーシャルメディアサービスで発信してはならない。

（ウ）利用するソーシャルメディアサービスごとの責任者を定めなければならない。

（エ）アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

（オ）可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、公社のWebサイトに当該情報を掲載して参照可能とすること。

(2) アクセス制御

情報ネットワーク管理者及び業務システム管理者は、アクセス制御として次の「ア：」～「ク：」の各項目のことを行わなければならない。

ア： アクセス制御

所管する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情報取扱者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。

イ： 利用者IDの取り扱い

（ア）所管するネットワーク又はシステムに権限がない職員等情報取扱者がアクセスすることが不可能となるように、利用者の識別及び認証等適正な対応を行わなければならない。

（イ）利用者の登録・変更・抹消等の情報管理、職員等情報取扱者の異動、出向、退職に伴う利用者 ID の取扱い等については、定められた方法に従って行わなければならない。必要な利用者登録・変更・抹消は、情報システム管理者及び業務システム管理者に対する申請により行う。ただし 所属等ごとに配布された ID 等については除く。

（ウ）利用されていないIDの放置がないか、人事管理部門と連携し、点検しなければならない。

（エ）IDに割り当てているアクセス権の正当性確保のため、定められた方法で点検しなけれ

ばならない。

ウ： 特権 ID の管理等

（ア） 管理者権限等の特権 ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

（イ） 特権 ID 及びパスワードの変更について、原則として委託事業者に行わせてはならない。

（ウ） 特権 ID 及びパスワードについて、職員等情報取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

（エ） 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。

（オ） 特権 ID を初期設定以外のものに変更しなければならない。

エ： 外部からのアクセス

（ア） 外部からのアクセスの許可する場合、合理的理由の必要最低限のものに限定しなければならない。

（イ） 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。

（ウ） 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。

（エ） 外部からのアクセスに利用するモバイル端末を職員等情報取扱者に貸与する場合、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。

（オ） 公社内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則禁止しなければならない。

オ： 内部ネットワーク間の接続

他の内部ネットワークとの接続については、あらかじめ接続先の内部ネットワークの管理者と協議し、以下の内容を確認したうえで接続しなければならない。

（ア） 接続によりそれぞれの情報資産に影響が生じないこと

（イ） 接続した場合のそれぞれの情報システムの責任範囲

（ウ） 障害発生時の対応体制

カ： 自動識別の設定

公社のネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるよう必要に応じてシステムを設定するものとする。

キ： ログイン試行回数の制限等

ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等情報取扱者がログインしたことを確認することができるようにシステムを設定しなければならない。

ク： 認証情報の管理

（ア） 職員等情報取扱者の認証情報を厳重に管理しなければならない。認証情報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認証情報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。

（イ）職員等情報取扱者のパスワードを発行する場合において、仮のパスワードを発行する場合、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。

（ウ）仮のパスワードも含めパスワードを発行する場合、パスワードは十分な長さ（原則として 8 文字以上）とし、文字列は想像しにくいもの（英字（大文字・小文字区別有）数字・記号を組み合わせたものなど）としなければならない。

（エ）特権 ID のパスワードは定期的（概ね 6 か月以内）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ないものとする。

（オ）認証情報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。

(3) システム開発、導入、保守等

情報ネットワーク管理者及び業務システム管理者は、システム開発、導入、保守等のため、次の「ア：」～「ケ：」の各項目のことを行わなければならない。

ア： 情報システムの調達

（ア）情報システム開発、導入、保守等の調達に当たっては、一般に公開する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。

（イ）機器及びソフトウェアの調達に当たっては、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。

（ウ）情報セキュリティ管理者は、適正に情報セキュリティ対策を推進・管理するための基礎資料として、情報システム台帳を作成し、整理する。情報ネットワーク管理者及び業務システム管理者は、情報システムを新たに調達したり、既にある情報システムを廃止したりしたときは、情報セキュリティ管理者からの求めに応じて、その旨を報告しなければならない。

（エ）機密性２以上の情報資産を扱う情報システムを開発または導入する場合は、情報セキュリティ管理者の審査を受け、許可を得なければならない。

イ： 情報システムの開発

（ア）ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、次の事項を定める。

① 責任者及び監督者
② 従事者及び作業範囲
③ 開発するシステムと運用中のシステムとの分離
④ 開発・保守に関する設計仕様等の成果物の提出
⑤ セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
⑥ アクセス制限
⑦ 機器の搬入出の際の許可及び確認
⑧ 記録の提出義務
⑨ 仕様書・マニュアル等の定められた場所への保管
⑩ 情報システムに係るソースコードの適正な方法での保管
⑪ 開発・保守を行った者の利用者 ID、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消
⑫ 情報システムセキュリティ実施手順書等の整備

（イ）ネットワーク及び情報システムの開発にあたって、不正にコピーしたソフトウェア及び個人所有のソフトウェアの導入又は使用等問題のある行為が発生しないようにしなければならない。

（ウ）ネットワーク及び情報システムの開発にあたって、コンピュータウイルス等対策ソフトウェアを導入する等、ウイルス感染やサイバー攻撃による情報漏えい等が発生しないようにしなければならない。

ウ： 情報システムの導入

（ア）開発環境と運用環境の分離及び移行手順の明確化

① システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。

② 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。

③ 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。

④ 導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

⑤ 導入するシステムやサービスのリスクを把握し、適切にコントロールされていることを確認した上で導入しなければならない。

（イ）テスト

① 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 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。また、作業については、作業経過を確認しながら実施するとともに作業内容を記録しなければならない。

③ 保有個人情報及び機密性の高い生データを試験データに使用してはならない。ただし、合理的な理由がある場合で、情報セキュリティ統括責任者が許可した場合は、この限りではない。

④ 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

⑤ 試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

エ： システム開発・保守に関連する資料等の整備・保管

（ア）システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

（イ）担当するシステムにおいて行ったシステム変更等の作業やテスト結果については、職員等情報取扱者による十分な検証が行われ、その結果が上長により承認された作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適正に管理を行わなければならない。

（ウ）情報システムに係るソースコードを適正な方法で保管しなければならない。

オ： 情報システムにおける入出力データの正確性の確保

（ア）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。

（イ）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。

（ウ）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。

カ： 情報システムの変更管理

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。

キ： ソフトウェアの保守及び更新

ソフトウェア等を更新又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、速やかに対応を行わなければない。

ク： 委託業務等従事者の身分確認

作業前に委託業務等従事者に対して身分証明書の提示を求め、契約で定められた資格を有するものが作業に従事しているか確認をすることができるようにしておかなければならない。

ケ： システム更新又は統合時の検証等

システム更新・統合時に伴うリスク管理体制の構築、移行、基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

(4) 不正プログラム対策

ア： 情報ネットワーク管理者等の措置事項

情報ネットワーク管理者、業務システム管理者及び情報管理者は、必要に応じて、次の事項を措置しなければならない。

（ア）所管するサーバ及び端末に、コンピュータウイルス等対策ソフトウェアを常駐させなければならない。

（イ）情報システムにおいて、電磁的記録媒体を使用する場合、公社が管理しているものを職員等情報取扱者に使用させるとともに当該媒体の使用にあたりウイルスチェックを行わせなければならない。

（ウ）コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たなければならない。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を実施しなければならない。

（エ）業務で利用するソフトウェアは パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを原則として利用してはならない。

（オ）コンピュータウイルス対策ソフトウェア等の設定変更権限については、一括管理し、情報管理者が許可した職員を除く職員等 に当該権限を付与してはならない。

（カ）ランサムウェアへの事前対策として、不正プログラム対策が適切に講じられているかを確認しなければならない。

（キ）仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及び

サービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

イ： 職員等情報取扱者の遵守事項

職員等及び委託業務従事者等は、次の事項を遵守しなければならない。

（ア）端末において、コンピュータウイルス等対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。

（イ）外部ネットワーク及び電磁的記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（ウ）外部ネットワーク及び電磁的記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（エ）差出人が不明であるなど、不審な電子メールを受信した場合は速やかに削除する。

（オ）端末に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

（カ）情報セキュリティ管理者が提供するコンピュータウイルス等の情報を常に確認する。

（キ）添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

（ク）コンピュータウイルス等に感染したおそれがある場合は、速やかに情報管理者に報告するとともに、その指示に従い、LAN ケーブルの取り外しや端末の通信機能の停止等、他への感染を防止する措置を講じる。

（ケ）端末には、業務に必要なソフトウェアのみをインストールするとともに、端末に導入されているソフトウェアについて、情報ネットワーク管理者及び業務システム管理者等から最新版へのアップデートの指示等があったときは、速やかにその指示に従う。

（コ）メールや SMS に添付されている URL は安易にクリックせず、ウェブサイトにアクセスする際は、あらかじめ登録している URL からアクセスする。

（サ）Web サービスにログインする場合に、多要素認証等の設定が可能な場合、有効化する。

ウ： 専門家の支援体制

情報セキュリティ統括責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、コンピュータウイルス等対策ソフトのサポート契約を締結する等外部の専門家の支援を受けられるようにしておかなければならない。

(5) 不正アクセス対策

情報ネットワーク管理者及び業務システム管理者は次の「ア：」～「カ：」の各項目のことを行わなければならない。

ア： 使用されていないポートの閉鎖等

（ア）使用されていないポートを閉鎖しなければならない。

（イ）不要なサービスについて、機能を削除又は停止しなければならない。

（ウ） 不正アクセスによるデータの書換えを検出する等 Web サイトの改ざんを防止しなければならない。

（エ）ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用しなければならない。

（オ）情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（カ）情報セキュリティポリシー等におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

（キ）クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

（ク）パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が､情報セキュリティポリシー等を満たすことを確認しなければならない。クラウドサービスのシステムやアプリケーション設定を変更するユーティリティプログラムは、原則として使用を禁止する。利用が必須なものは情報ネットワーク管理者又は業務システム管理者の承認を取得し、利用を管理した上で使用すること。

イ： 攻撃への対処

サーバ等に攻撃を受けた場合又は攻撃の予告等サーバ等に不正アクセスされることが明白な場合、システムの停止、他のネットワークとの切断等、必要な措置を講じる。また、各関係機関との連絡を密にして情報の収集に努める。

ウ： 内部からの攻撃への対処措置

職員等情報取扱者が使用している端末からの公社内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。

エ： 職員等による不正アクセス時の措置

職員等情報取扱者による不正アクセスを発見した場合は、当該職員等情報取扱者が所属する課の情報管理者に通知し、適正な処置を求めなければならない。

オ： サービス不能攻撃

外部からアクセスできる情報システムに対して､第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない

カ： 標的型攻撃

情報システムにおいて、標的型攻撃による内部への侵入を防止するために、研修・啓発や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

キ： 記録の保存

情報セキュリティ最高責任者及び情報セキュリティ統括責任者は、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。

(6) セキュリティ情報の収集

ア： セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

（ア）情報セキュリティ管理者は、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 ソフトウェア更新等の対策を実施しなければならない。

（イ）情報ネットワーク管理者又は業務システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、業務に対する影響や保有するデータへの影響について特定すること。その上で、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

イ： 不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ管理者は、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 職員等情報取扱者に周知しなければならない。

ウ： 情報セキュリティに関する情報に関する情報の収集及び共有

情報セキュリティ管理者は、情報セキュリティ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、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

６．運用

(1) 情報システムの監視

情報ネットワーク管理者及び業務システム管理者は、次の「ア：」～「エ：」の各項目のことを行わなければならない。

ア： 事象の検知

セキュリティに関する事象を検知するため、情報システムの監視を行う。

イ： 時刻同期

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又はサーバ間の時刻同期ができる措置を施す。

ウ： 外部接続システム

外部と接続するシステムを稼働中、常時監視する。

エ： クラウドサービス

（ア）必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定する。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに、監視により業務継続の上で必要となる容量・能力を予測し、業務を維持できるように努める。

（イ）利用するクラウドサービスが、本文書の「5. (1)エ：ログの取得等」に定めた基準を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討する。

（ウ）クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認する。

(1) サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

(2) クラウドサービス利用の終了手順

(3) バックアップ及び復旧

(2) セキュリティポリシー等の遵守状況の確認

ア： 遵守状況の確認及び対処

（ア） 情報管理者は、情報セキュリティポリシー及びこれに基づく文書の遵守状況について確認を行い、問題を認めた場合には、速やかに情報セキュリティ管理者に報告しなければならない。

（イ）情報セキュリティ管理者は、発生した問題について、適正かつ速やかに対処しなければならない。

（ウ） 情報ネットワーク管理者及び業務システム管理者は、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及びこれに基づく文書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正かつ速やかに対処しなければならない。

イ： 端末モバイル端末及び電磁的記録媒体等の利用状況調査

情報ネットワーク管理者及び業務システム管理者は、不正アクセス、不正プログラム等の調査のために、職員等情報取扱者が使用している端末、モバイル端末及び電磁的記録媒体等のログ、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。

ウ： 職員等情報取扱者の報告義務

（ア）職員等情報取扱者は、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、直ちに情報管理者に報告を行わなければならない。

（イ） 当該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情報セキュリティ統括責任者が判断した場合において、職員等情報取扱者は、緊急時対応手順書に従って適正に対処しなければならない。

(3) 管理者権限の代行

情報ネットワーク管理者、業務システム管理者及び情報管理者の権限を代行する者は、それぞれが指名する。

(4) 侵害時の対応等

ア： 情報セキュリティインシデント発生時の対応手順書の策定

（ア）情報セキュリティ統括責任者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ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正に実施するために、情報セキュリティインシデント発生時の対応手順書を定めておき、セキュリティ侵害時には当該手順書に従って適正に対処しなければならない。

（イ）情報セキュリティ統括責任者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した、情報セキュリティインシデント発生時の対応手順書を定めておき、セキュリティ侵害時には当該手順書に従って適正に対処しなければならない。

イ： 情報セキュリティインシデント発生時の対応手順書に盛り込むべき内容

情報セキュリティインシデント発生時の対応手順書には 以下の内容を定めなければ

ならない 。

（ア）緊急時連絡網

（イ）意思決定の所在

（ウ）発生した事案に係る報告すべき事項

（エ）発生した事案への対応措置

（オ）再発防止措置の策定

ウ： 緊急連絡網に盛り込むべき内容

緊急時の連絡先（所属、役職、電話番号、電子メールアドレス等）及び連絡順序がわかるように記載する。公社内部や委託先だけでなく、警察・関係機関も記載されていることが望ましい。

エ： 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ統括責任者は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。

オ： 情報セキュリティインシデント発生時の対応手順書の見直し

情報セキュリティ統括責任者は、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、必要に応じて情報セキュリティインシデント発生時の対応手順書の規定を見直さなければならない

(5) 例外措置

ア： 例外措置の許可

情報ネットワーク管理者、業務システム管理者及び情報管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、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する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、情報セキュリティ最高責任者の許可を得て、例外措置を講じることができる。なお、情報セキュリティ統括責任者が 軽微な例外措置と判断したものについては、当該責任者の許可により、例外措置を講じることができる。

イ： 緊急時の例外措置

情報ネットワーク管理者、業務システム管理者及び情報管理者は、前項に該当する場合であって、事務の遂行に緊急を要し前項に定める許可を得る時間的な猶予のないときは、 例外措置を実施し、実施後速やかに情報セキュリティ最高責任者に報告しなければならない。

ウ： 例外措置の申請書等の管理

情報セキュリティ最高責任者は、例外措置の申請書、報告書及び審査結果を適正に保管させなければならない。

(6) 法令順守

（ア）職員等情報取扱者は、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 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）

② 著作権法（昭和 45 年法律第 48 号）

③ 個人情報の保護に関する法律（平成 15 年法律第 57 号）

④ サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑤ 一般財団法人神戸住環境整備公社個人情報保護規程
⑥ 一般財団法人神戸住環境整備公社公文書管理規程

（イ）情報ネットワーク管理者及び業務システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

(7) 懲戒処分

ア： 懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員等情報処理取扱者並びにその監督責任者は、その重大性、発生した事象の状況等に応じて、一般財団法人神戸住環境整備公社職員就業規則による懲戒処分の対象となる。

イ： 再発防止の指導等

職員等情報取扱者に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、情報管理者は、速やかに次の措置を講じなければならない。

① 再発防止の指導その他適切な措置

該当者に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

② 使用権の停止・剥奪

指導等によっても改善されない場合、当該職員等情報取扱者の情報資産の使用権を停止あるいは剥奪する。

③ 報告

違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について情報セキュリティ管理者に報告する。

7．業務委託等と外部サービスの利用

(1)業務委託等

ア： 委託事業者の選定基準

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、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の実施が確保されることを確認しなければならない。

イ： 契約書の記載事項

（ア）重要な情報資産を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務委託においては、当該委託先事業者等との間で、下記事項を明記した契約を締結しなければならない。

① データその他業務上知り得た情報（以下「データ等」という。）の秘密の保持に関する事項
② 第三者への委託等（以下「再委託」という。）の禁止又は制限に関する事項
③ データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

④ データ等の複写及び複製の禁止に関する事項
⑤ データ等の取り扱いに関する事故の発生時における報告義務に関する事項
⑥ データ等の取り扱いに関する検査の実施に関する事項
⑦ 契約に違反した場合における契約の解除及び損害賠償に関する事項
⑧ 委託業務終了時の情報資産の返還、廃棄等に関する事項
⑨ 情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
⑩ 事故時等の公表に関する事項
⑪ 委託先等の責任者、委託等の内容、従事者の所属、作業場所の特定に関する事項
⑫ 委託先等の責任者及び従事者に対する研修の実施に関する事項
⑬ 情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項
⑭ 情報のライフサイクル全般での管理義務に関する事項

（イ） 前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。
① 提供されるサービスレベルの保証に関する事項
② 委託業務等の定期報告及び緊急時報告義務に関する事項
③ 外部施設等への搬送時における紛失、盗聴、不正コピー等の防止に関する事項

ウ： 確認・措置等

情報ネットワーク管理者及び業務システム管理者は、契約締結後においても、当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について、定期的若しくは随時、調査を行い、安全を確保しなければならない。情報セキュリティ統括責任者から内容の報告を求められた場合には、報告を行わなければならない。

エ： 再委託等

再委託（再々委託を含む。以下同様）を受ける事業者がある場合、「7.業務委託等と外部サービス（1)業務委託等」のイ、ウに定める事項は再委託を受ける事業者にも適用する。

(2) 外部サービスの利用

事業者等の公社の外部の組織が、情報システムの一部又は全部の機能を、その組織が定めた利用規約等に基づいて提供するサービスにおいて、公社の情報資産を取り扱う場合は、情報セキュリティ最高責任者が別途整備する外部サービス利用基準に基づいて行うこととする。

８．情報セキュリティ個別基準の策定

情報セキュリティ統括責任者は、情報セキュリティポリシーを補完するために必要な事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

９．情報セキュリティ実施手順の策定

情報セキュリティ統括責任者及び業務システム責任者は、情報セキュリティポリシーに基づき、所管するシステム等（専用 PC や Web サイトのうち保有個人情報を取扱うものも含む)に対する情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定させなければならない。

１０．評価・見直し

(1) 監査

ア： 実施方法

情報セキュリティ最高責任者は、情報セキュリティ監査統括責任者に命じ、情報セキュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。。

イ： 監査を行う者の要件

（ア）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。

（イ）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。

ウ： 監査実施計画の立案及び実施への協力

（ア）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、監査実施計画を策定し、情報セキュリティ最高責任者に報告しなければならない。

（イ）被監査部門は、監査の実施に協力しなければならない。

エ： 委託事業者等に関する監査

情報セキュリティ監査統括責任者は、委託先事業者等に対して、委託先事業者等からの再委託等（再々委託を含む）の事業者も含めて、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。

オ： 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ最高責任者に報告しなければならない。

カ： 保管

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正に保管しなければならない。

キ： 監査結果への対応

情報セキュリティ最高責任者は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また 指摘事項に関係しない情報管理者等に対しても、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。なお、社内で横断的に改善が必要な事項については、情報セキュリティ統括責任者に対し、当該事項への対処を指示しなければならない。

ク： 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

(2) 自己点検

ア： 実施方法

（ア）情報ネットワーク管理者及び業務システム管理者は、所管するネットワーク及び情報

システムの情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を実施しなければならない。

（イ） 情報管理者は 所管する所属の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、定期的及び必要に応じて自己点検を行わなければならない。

イ： 報告

（ア）情報ネットワーク管理者、業務システム管理者及び情報管理者は、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、情報セキュリティ統括責任者に報告しなければならない。

（イ）情報セキュリティ統括責任者は、報告を受けた点検結果及び改善策を情報セキュリティ最高責任者に報告しなければならない。

ウ： 自己点検結果の活用

（ア）職員等情報取扱者は、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。

（イ）情報セキュリティ最高責任者は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し､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。

エ： 改善

情報ネットワーク管理者、業務システム管理者及び情報管理者は次のことを行わなければならない。

（ア） 是正措置

業務上発見された問題､監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

（イ）予防措置

業務上予見される問題、他の組織で発生したものと同種の情報セキュリティに関する事件・事故等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

(3) 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ最高責任者は、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合、情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。

附 則

1　この情報セキュリティポリシーは、平成 22 年 7 月 1 日から施行する。

2　この情報セキュリティポリシーの施行に伴い、「神戸市都市整備公社情報ネットワーク運営要綱」は、施行と同時に廃止する。

附 則

このセキュリティポリシーは、平成 25 年 4 月 1 日から施行する。

附 則

この情報セキュリティポリシーは、令和 4 年 5 月 1 日から施行する。

附 則

この情報セキュリティポリシーは、令和 5 年 10 月 1 日から施行する。