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 4 年 5 月 1 日

施 行 日 ： 令 和 4 年 5 月 1 日

一般財団法人神戸住環境整備公社

[目 次]

第１章　総論 1
１．目的 1
２．セキュリティポリシーの体系 1
３．用語の定義 1
第２章　基本方針 1
１．セキュリティポリシーの適用範囲 1
２．職員等の義務 2
３．情報セキュリティ管理体制 2
４．情報資産への脅威 2
５．情報セキュリティ対策 2
６．情報セキュリティの個別基準及び実施手順の作成 2
７．情報セキュリティ監査及び自己点検の実施 3
８．情報セキュリティポリシーの見直し 2
第３章　対策基準 3
１．権限と責任 3
２．情報資産の分類と管理 4
３．物理的セキュリティ 7
４．人的セキュリティ 9
５．技術的セキュリティ 12
６．運用面のセキュリティ 18
７．情報セキュリティ個別基準の策定 19
８．情報セキュリティ実施手順の策定 20
９．セキュリティポリシー等の違反に対する扱い 20
１０．評価・改善・見直し 20

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、「セキュリティポリシー」という。）を定める。

２．セキュリティポリシーの体系

この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．セキュリティポリシーの適用範囲

(1) 組織の範囲は、「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) 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：（物理資産）

コンピュータ・ネットワーク・記録媒体等の有体物で、かつ、情報利用に必要な資産

イ：（データ資産）

データ及び情報システムの設計等に関する情報

ウ：（ソフト資産）

コンピュータ等の情報機器で稼動するプログラム

エ：（サービス資産）

電源、メールサービス等契約により提供される情報システムに関連する業務

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) 情報セキュリティ監査統括責任者：専務理事を充てる。

４．情報資産への脅威

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) 部外者による不正アクセス又は不正操作によるデータやプログラムの持ち出し･盗聴･改ざん･消去、機器及び媒体の破壊・盗難等

(2) 職員等情報取扱者の意図しない操作、不正アクセス・不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の破壊・盗難、規定外の端末接続によるデータ漏洩等

(3) 地震・落雷・火災等の災害、事故、故障等によるサービス及び業務の停止

５．情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため、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対策。

(3) 人的セキュリティ

職員等情報取扱者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､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。

(5) 運用面のセキュリティ

情報システムに関し、セキュリティポリシーの遵守状況の確認等、運用面の対策。また、情報資産への侵害に対する緊急時対応計画を策定。

６．情報セキュリティの個別基準及び実施手順の作成

第３章第２項(2)の表に基づき、具体的な内容や実施手順を定めた研修、ソフトウェア管理及び監査・自己点検基準（以下「情報セキュリティ個別基準」という。）並びにソフトウェア管理手順書（以下「情報セキュリティ実施手順」という。）を策定することができる。

７．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、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。

８．情報セキュリティポリシーの見直し

必要に応じて、適宜、セキュリティポリシーの見直しを行う。

第３章　対策基準

基本方針に基づき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： 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： 情報セキュリティの専門家・職員をアドバイザーとしておくことができる。

(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： 公社の情報資産のうち、公社ネットワークに関する管理を情報ネットワーク管理者に行わせることができる。

オ： 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。

カ： 公社の情報資産への情報セキュリティ侵害があり又はそのおそれがある場合、情報セキュリティ最高責任者の指示に従い必要に応じて報告し（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。

キ： 緊急時等の情報提供を図るため、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、情報管理者を網羅する連絡体制を整備しなければならない。

(3) 情報セキュリティ管理者

ア： 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。

イ： 情報ネットワーク管理者、情報責任者、情報管理者に対して、情報セキュリティ統括責任者の指示に従い情報セキュリティの指導及び助言を行う。

ウ： 公社の情報資産への情報セキュリティ侵害があり又はそのおそれがある場合、情報セキュリティ統括責任者の指示に従い（不在の場合には自らの判断に基づき）、情報ネットワーク　管理者、情報責任者、情報管理者に円滑な情報提供を行わねばならない。

エ： 情報セキュリティ統括管理者の指示に従い公社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。

オ： 公社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。

(4) 情報ネットワーク管理者

ア： 公社の情報資産への侵害があり又はそのおそれがある場合、情報セキュリティ管理者、情報セキュリティ統括責任者、情報セキュリティ最高責任者へ速やかに報告を行い、指示を求める。

イ： 公社ネットワークに関する権限と責任を有する。

ウ： 公社ネットワークにおける情報資産に対する侵害があり又はそのおそれがある場合、情報セキュリティ管理者へ報告をする。

(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情報取扱者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ソコン等の物理的セキュリティに関する管理を行う。

ウ： 所管課内の情報資産への情報セキュリティ侵害があり又はそのおそれがある場合、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、指示を求める。

(7) 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。

(8) 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。

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、情報ネットワーク管理者・情報管理者等権限のある者（以下、「情報資産管理責任者」という）がその所管する情報資産の管理責任を有するとともに、当該情報資産の利用範囲を定める。

イ： （情報取扱者の責任）

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

ウ： （複製等の管理）

データが複製又は送られた場合、それらも原本と同様に管理する。

(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（データだけではなくそれらが含まれる記録媒体、パソコン、システム等も同様に扱う）は、次のものとする。

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)上の表にある情報資産は、この対策基準の対象とする。また、これ以外の情報資産も、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。

イ：（情報資産に対するリスク分析の実施）

(ア)公社が保有する情報資産につき、予め重要性分類に従い、リスク分析を行う。

(イ)情報セキュリティ最高責任者は、基準を設け、受容可能なリスク水準を定める。

(ウ)リスク分析の結果、受容可能なリスク水準を上回る場合、リスク対応計画書を作成し、情報セキュリティ最高責任者の承認を得て、リスク管理を行う。この計画書には、リスク対応の活動内容、資源、責任体制及び優先順位等を記載する。

(エ)リスク分析及び受容可能なリスクの水準等は、情報セキュリティに関する状況の変化等を踏まえ、必要に応じて見直しを行う。

ウ：（情報資産の管理方法）

(ア)情報資産の管理

① 情報資産は、第三者が簡単に重要性を判別できないよう適切な管理を行う。

② 全ての情報資産を明確に識別して管理する。

(イ)データの作成

① 業務上必要のないデータを作成しない。

② データの作成時に重要性分類に基づき、管理する。

③ 作成中のデータも、紛失や流出等を防止する。また、作成途上の不要データは消去する。

(ウ)情報資産の入手

① 公社内の者が作成した情報資産の入手者は、入手元の情報資産の分類に基づいた取扱いをする。

② 外部者作成の情報資産も入手者は、重要性分類に基づき、当該情報を管理する。

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、情報資産管理責任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権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、情報資産管理責任者の許可があれば、複写、複製、送付及び送信できる。ただし、パスワード等の情報漏洩対策がなければＥメールで送信できない。

④ Ｅメールにより機密性１のデータを送信する者は、必要に応じて、パスワード等による情報漏洩対策を施さなければならない。

⑤ 情報資産の利用者は、記録媒体に情報資産の分類が異なるデータが複数ある場合、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

情報資産管理責任者は、次のことを行う。

① 情報資産の重要性分類に従って、情報資産を保管する。

② 最終確定データの記録媒体は、書込禁止措置をしたうえで保管する。

③ 持ち運び可能な記録媒体は、耐火、耐熱、耐水及び耐湿対策をして、施錠可能な場所への保管等適切な管理をする。

④ 情報システムのバックアップで取得したデータの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する。

⑤ 機密性１以上の情報資産が保管された記録媒体の搬送にあたっては、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用防止のための措置を施す。

⑥ 機密性１以上の情報資産が保管された記録媒体を情報資産管理責任者の許可なく運搬することを禁じる。

(カ)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を設定する。

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する。

③ 情報資産管理責任者は、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。

(キ)情報資産の廃棄

① 記録媒体が不要となった場合は、データの消去を行ったうえで焼却、裁断又は溶解等により復元不可能な状態にして廃棄する。

② 廃棄を行う者は、その処理について、日時、担当者及び処理内容を記録する。

③ 廃棄を行う者は、情報資産管理責任者の許可を得なければならない。

エ：（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する。

(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、必要に応じて更新する。

(エ)文書を廃棄する場合は、廃棄文書が誤用されないようにする。また、廃棄文書を保持する必要がある場合には、廃棄文書と分かる識別を施さなければならない。

オ：（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、管理を行う。

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）

情報資産管理責任者は、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)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。

(エ)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。

(オ)当該システムに関連なきコンピュータ、通信回線装置、記録媒体等の管理区域への持ち込みは禁ずる。

イ：情報ネットワーク管理者・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、湿度等の影響をできる限り排除した場所に設置する。

(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は、十分な容量の予備電源を備え付ける。

(イ)落雷等による過電流に対してサーバ等の機器への保護措置を施す。

オ：（配線）

(ア)配線の変更、追加は、情報ネットワーク管理者・情報管理者等特定の者の権限とする。

(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す。

(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　場合連携して対応する。

(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、適切に管理する。

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、定期保守を実施する。

(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る。

消去できない場合、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。

キ：（消火薬剤及び消防用設備）

消火薬剤及び消防用設備等は、機器及び記録媒体に支障を与えないこと。

ク：（敷地外への機器の設置）

情報セキュリティ統括責任者の許可を得なければ、公社の事務所外にサーバ等の機器を設置できない。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）

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、全データを消去の上、復元不可能な状態にしなければならない。

コ：（機器等の搬入出）

(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

ア：情報ネットワーク管理者・情報管理者は、ネットワークの管理を行う。

イ：（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、適切に管理する。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する。

ウ：（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す。

エ：（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、適切な回線の選択を行う。また、必要に応じ、送受信される情報の暗号化を行う。

オ：（ネットワークおけるセキュリティ対策）

ネットワークに使用する回線は送信途上でデータの破壊、盗聴、改ざん、消去等が生じないようセキュリティ対策をする必要がある。

(3) 端末等の管理

情報ネットワーク管理者・情報管理者は、次のとおり端末等の管理を行う。

ア：（盗難防止）

執務室等の端末等に、盗難防止のため、必要に応じてワイヤーによる固定等の物理的措置を講じる。

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パスワードの入力を必要とするように設定する。また、必要に応じて、ハードディスクパスワード等を併用し、端末のディスクデータの暗号化等の機能を有効に活用する。

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、遵守しがたい点がある場合、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：　(法令等の遵守義務)

職務の遂行にあたり法令等を遵守しなければならない。

・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）
・著作権法（昭和 45 年法律第 48 号）
・個人情報の保護に関する法律（平成 15 年法律第 57 号）
・一般財団法人神戸住環境整備公社個人情報保護規程
・一般財団法人神戸住環境整備公社公文書管理規程

ウ：　(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、情報資産を利用し、又、開発、設定の変更、運用、更新等の作業を行う。

エ：　(個人所有の情報資産の持ち込み禁止)

個人所有のパソコン及び記録媒体等の持ち込みは禁止する。

オ：　(情報資産の持ち出し及び Web サイト等の送信禁止)

次の行為は禁止する。

(ア)所属外への持ち出し

ただし、情報資産のバックアップ等、合理的理由があり、かつ情報管理者等権限のある者の許可を得た場合には、記録作成のうえで所属外へ持ち出しできる。

(イ)Web サイト等を利用した外部への送信

ただし、公開しているデータ及び情報管理者等権限のある者の許可を得た国・県・市への報告等は除く。

カ：　(業務目的外の利用禁止)

業務目的外でのパソコン等の利用、情報システムへのアクセス、E メールの利用及びインターネットへのアクセス等は禁止する。

キ：　(端末等の利用)

(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・情報管理者の許可なく変更できない。

(イ)端末や記録媒体、データが印刷された文書等が、第三者に使用され、又は情報管理者等の管理権限者の許可なき情報閲覧を防ぐため、離席時の端末のロックや記録媒体、文書等の閲覧し難い場所への保管等の措置を講じなければならない。

ク：　(執務室外における情報処理作業の制限)

(ア)情報セキュリティ統括責任者は、機密性１以上、可用性２、完全性２の情報資産を執務室外で処理する場合における安全管理措置を定める。

(イ)個人所有のパソコンを使用して、執務室外で情報処理作業を行ってはならない。

ケ：　（守秘義務等）

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、その後も業務上知り得た情報を漏らしてはならない。

(2) 研修

ア：　（職員等に対する研修の実施）

情報セキュリティ最高責任者は、定期的に職員等情報取扱者に対する情報セキュリティに関する研修を実施する。

イ：　（研修計画の策定及び実施）

(ア)情報セキュリティ管理者は、職員等情報取扱者に関する研修を実施する場合、研修計画を策定し、情報セキュリティ最高責任者に報告する。

(イ)職員等情報取扱者を対象とする情報セキュリティ研修を毎年度最低１回実施する。

(ウ)新規採用職員を対象とする情報セキュリティ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とする。

(オ)情報セキュリティ管理者は、毎年度１回、情報セキュリティ最高責任者に対して、情報セキュリティ研修の実施状況について報告する。

ウ：　（緊急時対応）

情報セキュリティ最高責任者は、緊急時対応を想定したマニュアルを作成し、職員等情報取扱者は、習熟しなければならない。

エ：　（研修への参加）

全ての職員等情報取扱者は、定められた情報セキュリティ研修等に参加する。

(3) 事故等の報告・分析等

ア：　（事故等の報告）

(ア)職員等情報取扱者は、情報セキュリティに関する事件・事故、システム上の欠陥及び誤動作を発見、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等権限のある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等権限のある者は、速やかに情報セキュリティ管理者に報告する。また、当該事故等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にも報告する。

(ウ)情報管理者は、報告された事故等につき、必要に応じ情報責任者に報告する。

(エ)情報セキュリティ管理者は、報告された事故等について、必要に応じ、情報セキュリティ最高責任者に報告する。

イ：　（事故等の分析・記録等）

事故等を引き起こした部門の情報管理者・情報責任者は、情報セキュリティ管理者と連携し、事故等を分析し、記録を保存する。

(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)職員等情報取扱者は、他人に自己が利用している ID を利用させてはならない。

(イ)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)自己のパスワードに関し、次の事項を遵守しなければならない。

① パスワードは秘密にし、パスワードの照会等には一切応じない。

② 情報システム又はパスワードにつき危険のおそれがある場合、情報ネットワーク管理者・情報管理者等権限のある者に速やかに報告し、パスワードを速やかに変更する。

③ パスワードを記載したメモを作成しない。やむを得ずメモする場合には、他人に分からない場所に保管する。

④ 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とする。

⑤ パスワードを変更した場合は、過去に使用したパスワードを再利用しない。

⑥ 複数の情報システムを扱う場合、同一パスワードを複数システムで用いない。

⑦ 仮のパスワードは、最初のログインの時点で変更する。

⑧ パソコン等のパスワードの記憶機能を利用しない。

⑨ パスワードを共有しない。

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

(5) 外部委託に関する管理

ア：　(契約書の記載事項)

(ア)情報処理業務の外部委託の場合は、下記事項を明記した契約を締結する。

① 業務上知り得た情報・データ（以下「データ等」という）の秘密保持に関する事項

② 第三者への委託の禁止又は制限に関する事項

③ データ等の目的外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 データ等の取扱いに関する検査の実施に関する事項

⑦ 契約違反の場合における契約の解除及び損害賠償に関する事項

⑧ 委託業務終了時の資産の返還、廃棄等に関する事項

⑨ 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 委託先の責任者、委託内容、作業者、作業場所の特定に関する事項

(イ)次に掲げる事項も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 従業員に対する研修の実施に関する事項

③ 委託業務の定期報告及び緊急時報告義務に関する事項

④ 外部施設等への搬送時における盗聴、不正コピー等の防止に関する事項

イ：　(セキュリティ確保への取組み状況等の調査)

情報ネットワーク管理者・情報管理者は、当該委託先事業者のセキュリティ確保への取組み状況、情報セキュリティマネジメントシステムに係る認証取得の状況、個人情報保護に関する取組み状況の調査を行い、契約締結後も、必要に応じ、調査を行い、安全の確保に努める。情報セキュリティ管理者が求めた場合は、状況報告する。

ウ：　(再委託)

再委託を受ける事業者がある場合、「４．人的セキュリティ(5)外部委託に関する管理」のア、

イに定める事項は再委託を受ける事業者にも適用する。

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：（データ保存）

データ保存は、情報ネットワーク管理者等管理権限のある者が定める方法で行う。

イ：（ファイルサーバの設定等）

情報ネットワーク管理者がデータ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する。

(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する。

(ウ)特定の職員等情報取扱者が取扱う権限を持つデータは、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する。

ウ：情報ネットワーク管理者・情報管理者は、「エ：」～「コ：」の各項目のことを行う。

エ：（アクセス記録の取得等）

(ア)アクセス記録及び情報セキュリティの確保に必要な記録を取得し、窃取、改ざん、誤消去を防ぐ措置を行った後、一定期間保存する。又、不正アクセスの兆候を見つけるため定期的にそれらを分析する。

(イ)システムから自動出力したアクセス記録等を、必要に応じ、外部記録媒体にバックアップする。

オ：（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関し、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の閲覧、紛失がないように、適切な保管をする。

カ：（情報資産のバックアップ）

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行う。

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、取扱い事項を定め、情報セキュリティ統括責任者及び情報責任者の許可を得る。

ク：（通信回線によるデータの送信）

通信回線によりデータを送信する場合、専用通信回線を使用する、送信するデータを必要最小限にする等データ保護のための措置を講じる。

ケ：（外部の者が利用するシステム）

インターネット等により外部の者が利用できるシステムは、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ける等、特に強固な情報セキュリティ対策をとる。

コ：（Web サイトでの情報公開時の注意事項）

Web サイトで情報を公開・提供する場合、当該サイトに係るシステムで情報の漏洩・改ざん・消去、踏み台、Dos 攻撃等を防止する。また、メールシステムを含め各業務システムでも、他のシステムに対する攻撃の踏み台にならぬようにウイルス対策など適切な管理をする。

サ：（無線 LAN の利用の禁止）

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。

シ：（無許可ソフトの導入等の禁止）

(ア)職員等情報取扱者は、各自の端末に情報ネットワーク管理者が定めた以外のソフトは導入できない。ただし、業務遂行に必要なソフトは、情報ネットワーク管理者及び情報セキュリティ管理者の許可を得て利用できる。

(イ)職員等情報取扱者による不正コピーのソフトの導入又は使用を禁止する。

ス：（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の端末等に、端末及びその他の機器の増設又は改造を行ってはならない。業務遂行上の合理的理由でモデム、ルータ等の機器を設置し、他の環境（インターネット等）へのネットワーク接続を行うことや、公社外からのアクセスが可能な仕組みの構築の場合は、情報セキュリティ統括責任者の許可を必要とする。軽微な機器の増設の場合は、情報ネットワーク管理者等権限のある者の許可を必要とする。

セ：（E メール）

(ア)E 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、各課庶務担当者を経由してメールアドレスの取得を申請する。

(イ)情報セキュリティ管理者は、E メールの送受信容量の上限を設定し、上限を超える E メールの送受信を不可能にする。

(ウ)情報セキュリティ管理者は、E メールに添付されるファイルについて、セキュリティ上の問題が想起されるファイルは、送受信を制限できるようにする。

(エ)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 E メールを送信しない。

② 複数の宛先に E 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する。

③ 重要 E メールの誤送信は、情報管理者・情報セキュリティ管理者に報告する。

④ 自動転送機能を用いて、E メールを転送しない。

ソ：（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が必要な場合には、情報セキュリティ管理者が定める電子署名、暗号化又はパスワード設定等の方法を用いて、送信する。

(イ)職員等情報取扱者は、情報セキュリティ管理者が定める方法で暗号化と鍵の管理を行う。

タ：（無許可端末の接続禁止）

職員等情報取扱者は、情報ネットワーク管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

チ：（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。

ツ：（障害記録）

情報ネットワーク管理者・情報管理者は、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、保存しなければならない。

(2) アクセス制御

情報ネットワーク管理者・情報管理者は、アクセス制御として次のことを行う。

ア：（利用者の識別及び認証）

所管するネットワーク又は情報システムに権限がない職員等情報取扱者がアクセスできないように、利用者の識別及び認証等適切な対応を行う。

イ：（利用者登録）

(ア)利用者の登録、変更、抹消、登録した情報資産の管理、異動、出向及び退職時における利用者 ID の取扱い等は、定められた方法で行う。必要な利用者登録・変更・抹消の申請を受けること。ただし、所属等ごとに配布された ID 等は除く。

(イ)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、点検する。

(ウ)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する。

ウ：（特権管理等）

(ア)管理者権限等の特権を与えた ID を利用する者必要最小限にし、ID 及びパスワードの漏洩等の防止のため、ID 及びパスワードを厳重に管理する。

(イ)情報ネットワーク管理者・情報管理者の特権を代行する者は、当該管理者が指名し、情報セキュリティ統括責任者が認めた者であること。

(ウ)特権を与えた ID 及びパスワードの変更は、原則として外部委託業者に行わせない。

(エ)特権を与えた ID 及びパスワードは、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する。

(オ)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とする。

エ：（ネットワークにおけるアクセス制御）

アクセス可能なネットワーク及び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る。また、ネットワークサービスを利用する権限を有しない職員等情報取扱者は当該サービスの利用ができないようにする。

オ：（強制的な接続制御、径路制御）

(ア)不正アクセスを防止するため、適切なネットワーク経路制御を施す。

(イ)フィルタリング及びルーティングは、設定の不整合を防止するため、ファイアウォール、ルータ等に搭載されている通信ソフト等を設定する。

カ：（無人状態にある装置の管理）

サーバ又は端末等が無人状態になる場合、適切なセキュリティ対策を施す。

キ：（外部からのアクセス）

(ア)外部からのアクセスの許可は、合理的理由の必要最低限のものに限定する。

(イ)内部ネットワークおよび情報システムへのアクセス方法及び利用方法等は、通信途上の機密性及び利用者の真正性が確保できるものとする。

(ウ)職員等情報取扱者は、外部から持ち帰ったパソコン等の端末を内部ネットワークへ繋ぐ前に、ウイルス感染の有無等を確認する。

ク：（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は、情報資産に影響が生じないことを確認し、それぞれの情

報システムの責任範囲を明確にしたうえで、接続する。

なお、接続する前に、予め情報セキュリティ統括責任者に協議する。

ケ：（外部ネットワークとの接続）

(ア)外部ネットワークとの接続は、当該ネットワークのネットワーク構成、構成機器、セキュリティ技術等を詳細に調査し、公社の情報資産に影響がないことを確認のうえで、情報セキュリティ管理者の許可に基づき接続する。

(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接続を採用し、外部ネットワークの瑕疵による公社のデータの漏洩、破壊、改ざん又はシステムダウン等で業務への悪影響に対応するため、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る。

(ウ)接続した外部ネットワークのセキュリティに問題があり、公社の情報資産へ支障のおそれがある場合、外部ネットワークとの接続を物理的に遮断できる。

コ：（ネットワーク機器の自動識別）

公社のネットワークの使用機器は、機器固有情報等により端末とネットワークのアクセス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。

サ：（ログインの制限等）

ログインの設定等により、正当なアクセス権を持たない職員等情報取扱者が利用できないようにシステムを設定する。

シ：（パスワードに関する情報の管理）

(ア)職員等情報取扱者のパスワードに関する情報を厳重に管理する。また、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る。

(イ)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、活用する。

(ウ)仮のパスワードも含め、パスワードは十分な長さとし、文字列は推測が困難なものとする。

(エ)パスワードは必要に応じて変更し、過去に使用した物は、再利用は避ける。

(3) システム開発、導入、保守等

情報ネットワーク管理者・情報管理者は、システム開発、導入、保守等のため、次のことを行う。

ア：（情報システムの調達）

情報システムの調達の際は、次のことを行う。

(ア)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する。

(イ)機器及びソフトの調達は、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する。

イ：（情報システムの開発等）

一般に公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り、次の事項を定める。

(ア)責任者及び監督者

(イ)作業者及び作業範囲

(ウ)開発するシステムと運用中のシステムとの分離

(エ)開発・保守に関する設計仕様などの成果物の提出
(オ)セキュリティ上問題となるおそれのあるハード及びソフトの使用禁止
(カ)アクセス制限
(キ)機器の搬入出の際の許可及び確認
(ク)記録の提出義務
(ケ)仕様書・マニュアル等の定められた場所への保管
(コ)情報システムに係るソースコードの適切な方法での保管
(サ)開発・保守を行った者の利用者 ID、パスワード等の開発・保守終了後に不要となった時点での速やかな抹消

ウ：（情報システムの移行）
(ア)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する。また、移行の際、情報システムの記録データの保存を確実に行い、情報システムの停止等の影響を最小限にする。
(イ)新たな情報システムの導入時には、既存情報システムに接続する前に、十分な試験を行う。また、システムの更新時には、既に稼働中の情報システムとの連携につき、十分な試験を行う。
(ウ)擬似環境による動作確認後に情報システムの移行を行う。又、作業は、作業経過を確認しながら実施し、作業内容を記録する。
(エ)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ない。ただし、合理的理由があり、情報セキュリティ統括責任者が許可した場合は、使用できる。
(オ)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する。

エ：（情報システムの入出力データ）
情報システムの設計は次の点に留意する。
(ア)情報システムの入出力データは、範囲、妥当性のチェック機能および不正な文字列等の入力の除去機能を必要に応じて組み込むようにする。
(イ)内部処理によって誤ったデータに書き換えられる等の可能性がある場合に、書き換え等の検出チェック機能を組み込むようにする。
(ウ)情報システムから出力されるデータは、保存情報の処理が正しく反映されるようにする。

オ：（ソフトの保守及び更新）
ソフト等を更新、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、導入する。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は、速やかに対応する。

カ：（委託業務等従事者の身分確認）
作業前、委託業務等従事者に身分証明書の提示を求め、契約で定められた有資格者が作業に従事しているか確認できるようにする。

キ：（作業の確認）
契約で操作を認められた委託業務等従事者が重要なシステム変更等の作業を行う場合、　2名以上で作業し、互いにその作業を確認する。

ク：（作業管理記録）
担当するシステムで行ったシステム変更等の作業は、作業記録を作成する。作成した作業記録は、窃取、改ざん等をされないように管理を行う。

(4) ウイルス等不正プログラム対策

ア：（情報セキュリティ管理者の実施事項）

(ア)ウイルス等の情報について職員等情報取扱者に注意喚起を行う。

(イ)常時ウイルス等に関する情報収集に努める。

(ウ)ウイルス対策ソフト及び定義ファイルは常に最新のものにする指導等を行う。

イ：（情報ネットワーク管理者等の実施事項）

(ア)所管するサーバ及び端末に、ウイルス等対策ソフトを常駐させる。

(イ)情報システムでフロッピーディスク等の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、かつ、当該媒体の使用前にウイルスチェックを行わせる。

(ウ)ウイルス等対策ソフト及び定義ファイルは常に最新のものに保つ。インターネットに接続していないシステムでも、定期的に当該ソフト及び定義ファイルの更新を行う。

ウ：（職員等情報取扱者の遵守事項）

(ア)端末にウイルス等対策ソフトが導入されている場合、当該ソフトの設定を変更しない。

(イ)外部ネットワーク及びフロッピーディスク等の記録媒体とのデータ又はソフトの取り入れの際、又は、送信・書き込みの際は必ずウイルス等対策ソフトによるチェックを行う。

(ウ)差出人不明又は不自然なファイルが添付された E メールの受信時は、速やかに削除し、差出人不明又は不自然なファイルが添付された E メールが、頻繁に受信する場合は、迷惑メール機能等を使用してメールソフトに当該Ｅメールのアドレスを覚えさせて、　受信しないようにし、不用意に添付ファイルを開かないようにする。

(エ)ウイルス等対策ソフトの完全スキャンを端末には定期的に行い、スキャン実行を途中で止めない。

(オ)情報セキュリティ管理者からのウイルス等情報を常に確認する。

(カ)添付ファイルのあるメールを送受信する場合は、ウイルス等対策ソフトでチェックを行う。

(キ)ウイルス等に感染した場合、LAN ケーブルの即時取り外し又は機器の電源遮断を行う。

エ：（専門家の支援体制）

情報セキュリティ統括責任者は、不測の事態に備え、外部の専門家の支援体制を設けておかなければならない。

(5) 不正アクセス対策

情報管ネットワーク理者・情報管理者は、次のことを行う。

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の閉鎖。

(イ)不正アクセスによるデータの書換えの検出、Web サイトの改ざん防止。

(ウ)ソフトのセキュリティホール発見時の速やかな修正プログラムの適用。

イ：（攻撃の予告等への対処措置）

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公社内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視する。

エ：（職員等による不正アクセス時の措置）

職員等情報取扱者の不正アクセスがあった場合、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、適切な措置を求める。

オ：（記録の保存）

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は、法律違反等犯罪の可能性がある不正アクセスを受けた場合、不正アクセスの記録の保存に努めるとともに、警察・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

情報セキュリティ管理者は、セキュリティホール等の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情報を共有しなければならない。

６．運用面のセキュリティ

(1) 情報システムの監視

情報ネットワーク管理者・情報管理者は次のことを行う。

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：（常時監視）

外部と接続するシステムを稼働中、常時監視する。

(2) セキュリティポリシー等の遵守状況の確認及び対処

情報ネットワーク管理者・情報管理者は、常に、所管の範囲で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の確認を行い、問題がある場合には速やかに情報セキュリティ管理者に報告する。情報セキュリティ管理者は、発生した問題に、適切かつ速やかに対処しなければならない。

(3) 運用管理における留意点

ア：（調査権限のある職員の指名）

情報セキュリティ管理者は、情報漏洩、不正アクセス、ウイルス等の調査のために、パソコン、記録媒体、アクセス記録及びメール等の情報を調査する権限を有する職員を指名する。

イ：（セキュリティポリシー等の閲覧）

情報ネットワーク管理者・情報管理者は、職員等情報取扱者が常にセキュリティポリシー及びこれに基づく文書を参照できるよう配慮する。

ウ：（管理者権限）

情報ネットワーク管理者・情報管理者の権限代行者は、各自が指名する。

エ：（職員等の報告義務）

(ア)職員等情報取扱者は、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、直ちに情報セキュリティ管理者・情報管理者に報告を行う。

(イ)違反行為が直ちに情報セキュリティ上重大な支障になると情報セキュリティ管理者が判断した場合、緊急時対応計画に従って対処する。

(4) 緊急時の対応

ア：　（緊急時対応計画の策定）

情報セキュリティ統括責任者及び情報責任者は、情報資産への重大な侵害が発生し、又は発生するおそれがある場合、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、緊急時対応計画を策定する。

イ：　（緊急時対応計画に盛り込むべき内容）

(ア)関係者の連絡先

(イ)意思決定の所在

(ウ)発生した事象に係る報告すべき事項

(エ)発生した事象への対応措置

(オ)再発防止措置の策定

ウ：　（緊急時対応計画の見直し）

情報セキュリティ管理者・情報責任者は、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、必要に応じて緊急時対応計画を見直す。

(5) 例外措置

情報ネットワーク管理者・情報管理者は、次の例外措置をとれる。

ア：　（例外措置の許可）

やむを得ない状況のため、セキュリティポリシーを遵守できない場合は、情報セキュリティ最高責任者の許可を得て、例外措置をとれる。

イ：　（緊急時の例外措置）

前項の場合で事前許可をとれないときは、例外措置の実施後、速やかに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切に保管しなければならない。

7．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、セキュリティポリシーを補完するため、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できる。

8．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・情報責任者は、セキュリティポリシーに基づき、所管するシステム等に対する情報セキュリティ対策実施の具体的手順を定めた情報セキュリティ実施手順を策定できる。

9．セキュリティポリシー等の違反に対する扱い

(1) 懲戒処分

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取扱者並びにその監督責任者は、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。

(2) 再発防止の指導等

職員等情報取扱者に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ある場合、情報ネットワーク管理者・情報管理者は速やかに次の措置を講じる。

ア：当該職員等情報取扱者に違反事実を通知し、再発防止の指導その他の措置を行う。

イ：指導等で改善なき場合、職員等情報取扱者の情報資産使用権を停止・剥奪する。

ウ： 違反行為・指導内容・その他措置状況を情報セキュリティ管理者に報告する。

１０. 評価・改善・見直し

(1) 監査

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、必要に応じ監査を行わせる。情報セキュリティ監査統括責任者は、以下の要領で監査を実施する。これに対し、被監査部門は監査の実施に協力する。

ア： （監査を行う者の要件）

次の２つの要件を満たすものに監査を依頼する。

(ア)被監査部門から独立した者。

(イ)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。

イ： （監査実施計画の策定・監査結果の報告）

監査にあたり、監査実施計画を策定する。また、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する。

ウ： （委託先事業者に対する監査）

委託先業者（再委託も含めて）に対して、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う。

エ： （監査調書等の保管）

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保管する。

オ： （指摘事項への対処）

監査の指摘事項に関係する情報管理者等に対し、その対処を指示する。また、関係しない情報管理者に対しても、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る。

カ： （監査結果の活用）

情報セキュリティ最高責任者は、情報セキュリティ対策等の見直し時に監査結果を活用する。

(2) 自己点検

情報ネットワーク管理者及び情報管理者は、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の自己点検を必要に応じて行う。

ア： （自己点検結果等の報告）

点検結果とその改善策を取りまとめ、情報セキュリティ管理者と情報セキュリティ統括責任者に報告する。情報セキュリティ統括責任者は情報セキュリティ最高責任者に報告する。

イ： （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、自己権限の範囲内で改善を図る。

(イ)情報セキュリティ最高責任者は、セキュリティ対策等の見直し時に点検結果を活用する。

(3) 改善

情報ネットワーク管理者及び情報管理者は次のことを行う。

ア： （是正措置）

業務上発見された問題、監査・自己点検で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措置を施す。

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事件・事故、監査及び自己点検で指摘されうる問題等の発生を未然に防止するため、その原因を除去する措置を施す。

(4) セキュリティポリシーの見直し

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、セキュリティポリシーを必要に応じ見直しをする。

附　則

1　この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。