神　戸　市　道　路　公　社
情報セキュリティポリシー

制定日：平成２２年　２月　１日
改正日：令和　７年　７月　８日

神戸市道路公社

改訂履歴

施行年月日	版番号	改訂理由・内容
平成 22 年２月１日	第 1.0 版	初版発行
平成 25 年４月１日	第 1.1 版	職制改正に伴う一部改正
令和４年４月１日	第 1.2 版	職制改正に伴う一部改正
令和５年４月１日	第 1.3 版	有期雇用職員就業規則改正に伴う一部改正
令和６年１月 15 日	第 1.4 版	執務室外の情報処理作業の制限の一部改正
令和７年７月８日	第 1.5 版	・情報セキュリティ環境の強化に伴う管理及び運用等の一部改正 ・パソコン端末の持ち出し可能化に伴う情報漏えい対策に係る一部改正 ・情報資産の分類及び管理適正化に係る一部改正

目　　次

１．目的

本公社において保有する情報資産は、業務運営上重要な情報が多数含まれており、情報資産を様々な脅威から防御することは、継続的かつ安全・安定的な有料道路・駐車場サービスの実施を確保するためにも必要不可欠である。

このため、本公社の情報資産の機密性、完全性及び可用性を維持することを目的として神戸市道路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．定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

ハードウェア、ソフトウェア、ネットワーク等で構成され、情報処理を行う仕組みをいう。

（３）情報資産

情報システム及びネットワークにより処理、保管、通信、送付されるすべての情報をいう。

（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をいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

３．情報セキュリティポリシーの適用範囲

（１）組織の範囲

経営企画部及び道路管理部とする。

（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は次のとおりとする。ただし、ETC に関する情報資産、神戸市土木積算システム及び設備積算システムに関する情報資産については、別の定めに基づきセキュリティ対策を実施するものとし、これらの情報資産については、本セキュリティポリシーの対象から除くものとする。

① 物理資産

コンピュータ・ネットワーク・記録媒体等物理的な形状を有する資産であり、かつ情報を利用するのに必要な資産

② 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

③ ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

④ 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

４．職員等の義務

役員、職員（再任用職員を含む。以下同じ）、有期雇用職員及び委託業務等従事者（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、業務の遂行にあたっては情報セキュリティポリシーを遵守しなければならない。

また、人材派遣職員に業務を行わせる場合においても、本ポリシーを遵守させるものとする。

５．管理体制及び権限と責任

本公社の情報資産について、適切に情報セキュリティ対策を推進・管理するための組織体制を確立するため、次に掲げるものを置く。

（１）情報セキュリティ最高責任者（経営企画部長）

情報セキュリティ最高責任者は、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。

（２）情報セキュリティ統括責任者（経営企画部経営企画課長）

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を補佐するとともに、本公社のすべての情報資産における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。また、情報管理者に対して情報セキュリティ対策に関する指導及び助言を行う権限を有する。

（３）情報管理者（各課長）

情報管理者は、課内における情報資産の情報セキュリティ対策及び当該システムにおける開発、設定の変更、運用、見直し対策等を行う権限及び責任を有する。

（４）情報セキュリティ監査統括責任者（経営企画課長）

情報セキュリティ監査統括責任者は、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。

（５）情報化推進会議

情報セキュリティ統括責任者及び情報管理者により構成され、情報セキュリティに関する重要な事項を審議する。

情報化推進会議の事務局は、経営企画課総務係に置く。

６．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度合いや発生した場合の影響を考慮するものとする。特に次の脅威については、十分な措置を講じるものとする。

（１）部外者による不正アクセス又は不正操作、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、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・盗聴・改ざん・消去、重要情報の詐取、機器及び媒体の盗難等

（２）職員等情報取扱者による意図しない操作、不正アクセス又は不正操作による情報資産の

無断持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難、規定外の端末接続によるデータ漏えい等

（3）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、業務委託等の管理の不備、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

（4）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

7．情報資産の分類及び管理

（1）情報資産の分類

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セキュリティ対策を講じるものとする。重要な情報資産は以下のものとする。

分　類	定　　義
機密性	公社業務で取り扱う情報資産のうち、漏えい等が生じた際に権利利益の侵害の度合いが大きいもの又は、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに非常に留意すべき情報資産。 ・特定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道路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侵害が生じるおそれがあるデータ
完全性	公社業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公社業務の的確な遂行に支障（軽微なものを除く）を及ぼす恐れがある情報資産。
可用性	公社業務で取り扱う情報資産のうち、滅失、紛失、損傷した場合、その復元が著しく困難又は当該情報資産が利用不可能となることにより、公社業務の安定的な遂行や円滑な運営に支障（軽微なものを除く）を及ぼす恐れのある情報資産。

（2）情報資産の管理方法

① 情報資産の管理

ア　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（クラウドサービス環境に保存される情報資産を含む）。

イ　職員等及び委託業務従事者等は、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うえで行わなければならない。

ウ　情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

エ　全ての情報資産を明確に識別し、重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。

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

② 情報の作成

ア　業務上必要のない情報を作成してはならない。

イ　作成途上の情報についても、紛失や流出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。

③ 情報資産の利用

ア　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。

イ　７（１）の機密性にに該当する情報を、複数の権限ある者で共有するときや、公社外部に電子メール等により送信しなければならないときは、パスワード設定等の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 情報資産の保管

ア　情報管理者は、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

イ　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に保管しなければならない。

⑤ 情報資産の廃棄

ア　パソコン端末・サーバ機器等の電磁的記録媒体が不要となった場合は、当該媒体の初期化等を行ったうえで、焼却・裁断・溶解・物理的破壊等により復元不可能な状態にして廃棄しなければならない。リース返却等を行う場合も同様とする。

イ　電磁的記録媒体等の情報資産の廃棄や機器のリース返却等を行う場合は、情報管理者の許可を得なければならず、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。

ウ　電磁的記録媒体等の情報資産の廃棄又はリース返却における復元不可能化について、委託事業者への委託によることを妨げない。ただしこの場合、委託事業者と守秘義務契約を締結するなど秘密保持体制の確保とこれを遵守させるとともに、当該事業者に処理を行った日時、担当者及び処理内容を提出させ、確実に情報の漏えいを防止する措置を講じなければならない。

エ　クラウドサービスを利用する場合、クラウドサービスを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。

８．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ずるものとする。

（１）物理的セキュリティ対策

コンピュータ設置場所への入退室、サーバ等の管理、通信回線及び端末等への物理的な対策を講じる。

（２）人的セキュリティ対策

情報セキュリティに関し、職員等情報取扱者が遵守すべき事項を定めるとともに、研修・訓練及び啓発を実施するなど人的な対策を講じる。

（3）技術的セキュリティ対策

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等不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（4）運用面のセキュリティ対策

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、業務委託等を行う場合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を講じる。

９．物理的セキュリティ対策

（1）サーバ等の管理

① 入退室の管理

ア　情報管理者は、重要な情報資産データが記録されている記録媒体の保管場所及びそれを取り扱うコンピュータ設置場所（以下「管理区域」という。）の入退室について、厳格な管理を行わなければならない。

イ　外部からの訪問者が管理区域に入室する場合には、職員の承諾を必要とするものとし、必要に応じて立ち入り区域を制限した上で、職員が付き添うものとする。

ウ　管理区域には、当該区域内での作業に必要なものを除き、管理区域内に設置する情報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、通信回線装置、電磁的記録媒体等を持ち込ませてはならない。持ち込ませる場合は情報管理者の許可を得るものとする。

② 機器の取り付け等

ア　サーバ等の情報システム機器の取付けを行う場合、温度、湿度等の環境条件を十分留意した場所に設置し、固定式ラックを用いるなど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　サーバ等の情報システム機器等を新たに設置又は更新する場合、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者等に確認を行わなければならない。

ウ 機器等の搬出入には、職員等が同行する等の必要な措置を講じなければならない。

③ サーバの冗長化

情報資産については二重化等を行い、障害発生時においてもバックアップデータ等により早期にデータ復旧できるよう、同一データを保持する等の対策を講じなければならない。

④ 機器の電源

サーバ等の機器の電源については、落雷等による過電流対策を施してサーバ等の機器を保護するための措置を講じるとともに、停電等による電源供給の停止に備え、当該機器を正常に停止するまでの間に十分電力を供給できる容量の予備電源を備え付けなければならない。

⑤ 通信ケーブル等の配線

ア　通信ケーブル等の配線に当っては、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、配線収納管を使用する等必要な措置を施さなければならない。

イ　ネットワーク接続口（ハブのポート等）は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。

ウ　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。

⑥ 機器等の定期保守及び修理

ア　サーバ等の機器は、必要に応じ保守点検を実施しなければならない。

イ　記憶装置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、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など秘密保持体制の確認を行わ　なければならない。

⑦ 機器の廃棄等

ア　機器を廃棄、リース返却等を行う場合、機器内部の記憶装置から全ての情報を消去のうえ、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）をする場合は、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とする

（2）ネットワークの管理及びセキュリティ対策

ア　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うえ、適正な回線を選択しなければならない。また、必要に応じて、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。

イ　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。

ウ　ネットワークに使用する回線は、伝送途上において情報の破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策が実施されたものでなければならない。

エ　モバイル端末を含む、公社が支給する情報端末を、情報セキュリティ統括責任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。

（3）端末や電磁的記録媒体等の管理

① 端末等からの情報漏えい防止策

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、盗難又は紛失を防止しなければならない。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。

② 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、「持ち出し専用パソコン端末」を指す。

イ　執務区域外への持ち出し時には、モバイル端末へのデータ等の情報の格納・保存は禁止する。ただし、理事会での使用等、通信等ができないクローズ環境であり、複数の職員等による監視ができ、限りなく盗難又は紛失の可能性がなく、十分な管理が可能な、閉鎖された環境下にある場合で、情報セキュリティ統括責任者が許可した場合に限り、

使用後に速やかに保存した情報を削除することを条件に、データ等の情報のモバイル端末への保存を特別に可とする。

ウ　紛失・盗難に遭った際の対応として、直ちに接続先の執務室内端末側で回線接続を直ちに遮断しなければならない。また、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。

エ　モバイル端末を執務区域外で業務利用する場合は、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。

③ パソコン端末、電磁的記録媒体、ソフトウェア等の管理

ア　情報セキュリティ統括管理者は、公社が調達し使用するパソコン端末、モバイル端末、電磁的記録媒体、ソフトウェア（ライセンスを含む）について、支給状況、使用状況、保管状況等を把握し、「管理台帳」を作成して随時管理しなければならない。

イ　公社から支給されるUSBフラッシュメモリ等の電磁的記録媒体の管理は、各所属における集中管理方式とし、情報管理者は各所属で管理する電磁的記録媒体の保管状況等を「電子記録媒体管理台帳」によって随時管理しなければならない。

ウ　情報管理者は、所属で管理する電磁的記録媒体を職員に使用させるときは、貸出・返却状況、利用目的及び格納するデータ等情報の内容等を「電子記録媒体貸出（持ち出し）承認兼返却確認簿」によって随時管理及び確認しなければならない。

エ　情報セキュリティ統括責任者は少なくとも年に１回以上、「管理台帳」及び「電子記録媒体管理台帳」を検査し、管理状況の適正さを確認しなければならない。

10. 人的セキュリティ対策

（１）職員等の責務

① 情報セキュリティポリシー等の遵守義務

職員等情報取扱者は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守し、情報システム及び情報資産を適切に管理しなければならない。

また、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、法令等を遵守し、これに従わなければならない。

② 業務目的外の利用禁止

職員等情報取扱者は、業務外の目的でパソコン端末等の利用、情報システムへのアクセス、電子メールアドレスの利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。

③ 公社所有外の情報資産の持ち込みの禁止

職員等情報取扱者は、公社の所有するパソコン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。以下同じ。）以外の機器を原則として業務に利用してはならず、執務区域内への持ち込みも禁止する。

④ 情報資産の持ち出し等の禁止

ア　職員等情報取扱者は、支給されたパソコン端末、電磁的記録媒体及びデータ等の情報資産の公社外への持ち出しを原則として禁止する。

イ　職員等情報取扱者は、執務区域外で情報処理作業を行う際は、情報セキュリティ統括責任者の許可を得た場合に限り、公社外への「持ち出し専用パソコン端末（モバイ

ル端末）」の持ち出しができるものとする。

ウ　職員等情報取扱者は重要な情報資産を公社外へ持ち出してはならない。ただし、合理的理由のある場合、かつ情報管理者等管理権限のある者の許可を得た場合に限り、公社外への持ち出しができるものとする。

⑤ 執務室外における情報処理作業の制限

ア　職員等情報取扱者は、執務区域外で情報処理作業を行う場合には、情報管理者等管理権限のある者の許可を得なければならない。

イ　職員等情報取扱者は、執務区域外で情報処理作業を行う際、公社外への持ち出しを許可するパソコン端末は「持ち出し専用パソコン端末（モバイル端末）」に限るものとし、執務室内で使用しているパソコン端末その他の端末(タブレット端末やスマートフォン)による情報処理を行ってはならない。

ウ　職員等情報取扱者は、在宅勤務のため公社外で情報処理作業を行う場合、原則として持ち出しを許可されたモバイル端末によることとするが、情報セキュリティ統括責任者に許可を得た場合に限り、個人所有のパソコン端末及び通信回線を使用して作業することができるものとする。

エ　職員等情報取扱者は、執務区域外のモバイル端末又は在宅勤務時に許可された個人所有端末から公社の管理するネットワークにアクセスするときは、公社の情報サーバ等の情報資産に直接的に接続してはならず、情報セキュリティ統括責任者が許可する通信手段に限るものとする。

オ　職員等情報取扱者は紛失・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。また、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。

カ　職員等情報取扱者は、執務区域外でモバイル端末を使用する場合、モバイル端末から直接プリンタに接続して情報資産の出力等を行ってはならない。

キ　職員等情報取扱者は、執務区域外でのモバイル端末の使用を終了するときは、接続履歴等を確実に消去したうえで、速やかに公社に返却するものとする。

⑥ 持ち出しの記録

情報セキュリティ統括責任者は、パソコン端末等の持ち出しについて、持ち出し及び返却の記録を作成し、保管しなければならない。

⑦ 端末等の利用

ア　職員等情報取扱者は、パソコン端末等のソフトウェアに関するセキュリティ機能の設定を情報管理者の許可なく変更してはならない。

イ　職員等情報取扱者は、パソコン端末や電磁的記録媒体、データが印刷された文書等について、第三者に使用されること、又は情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時のパソコン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、適切な措置を講じなければならない。

⑧ 異動、退職時等の遵守事項

職員等情報取扱者は、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。

⑨ クラウドサービス利用時等の遵守事項

職員等情報取扱者は、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。

⑩ 業務以外の目的での ウェブサイト閲覧の禁止

職員等情報取扱者は、業務以外の目的でウェブ サイトを閲覧してはならない。

（2）研修

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、定められた研修に参加しなければならない。

（3）事故等の報告・分析等

① 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した場合、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統括責任者に報告しなければならない。

ウ　情報セキュリティ統括責任者は、報告のあった事故等について、必要に応じて、情報セキュリティ最高責任者に報告しなければならない。

② 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は、情報セキュリティ統括責任者と連携し、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。

（4）パスワードの管理

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。

ア　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。

イ　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てはならない。

ウ　情報システム又はパスワードに対する危険のおそれがある場合には、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しなければならない。

エ　複数の情報システムを扱う場合は、同一のパスワードを複数のシステム間で用いてはならない。

オ　職員等情報取扱者の間でパスワードを共有してはならない。

（5）外部委託に関する管理

① 契約書の記載事項

駐車場管理業務、有料道路付帯設備等維持管理業務、料金徴収業務など、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、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

ア　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

イ　第三者への委託（再委託）の禁止又は制限に関する事項

ウ　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
エ　データ等の複写及び複製の禁止に関する事項
オ　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
カ　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
キ　委託業務終了時の情報資産の返還、廃棄等に関する事項
ク　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
ケ　委託先の責任者、委託内容、従事者及び従事者の所属、作業場所の特定に関する事項

② 業務委託終了時の対策

業務委託の終了に際して、以下の対策を実施しなければならない。

ア　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認。
イ　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消。

③ 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、上記①②に定める事項は再委託を受ける事業者にも適用する。

11. 技術的セキュリティ対策

（1）コンピュータ及びネットワークの管理

① ファイルサーバの設定等

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、特定の職員のみが取扱う権限を持つデータ等の情報については、同一所属であっても、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。

② 情報資産のバックアップ

情報管理者は、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。

③ ウェブサイトでの情報公開時の注意事項

情報管理者は、ウェブサイトにより情報を公開・提供する場合に、当該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。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。

④ 複合機のセキュリティ管理

ア　情報管理者は、複合機（コピー、プリンター、スキャナー、ＦＡＸなど複数の機能を兼ね備えた機器をいう。）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に応じた適正なセキュリティ要件を満たす機器を調達するものとする。
イ　情報管理者は、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　情報管理者は、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。

⑤ 無線ＬＡＮの利用

ア　公社管理区域内でパソコン端末等を用いる者（職員及び委託業務従事者を含む）は、適用範囲内の内部ネットワークにおいて、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原則として禁止する。

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管理区域内に限り、無線ＬＡＮを利用した接続等を行うことができるものとする。

⑥ 電子メール

ア　メールアドレス保有者は、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。

イ　メールアドレス保有者は、複数の宛先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わからないようにしなければならない。

ウ　メールアドレス保有者は、重要な電子メールを送信する場合、誤送信がないよう十分に注意し、誤送信した場合には、情報管理者に速やかに報告しなければならない。

⑦ 無許可端末の接続禁止

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

⑧ 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、公社から支給されたパソコン端末等に対して、情報セキュリティ統括責任者に無断又は情報セキュリティ統括責任者が定めるもの以外の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、情報セキュリティ統括責任者の許可を得た場合に限り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。

⑨ 機器構成の変更の制限

職員等情報取扱者は、ネットワーク及び公社から支給された端末等に対して、パソコン端末及びその他機器等の接続、増設又は改造を行ってはならない。

⑩ 業務外ネットワークへの接続の禁止

職員等情報取扱者は、公社から支給されたパソコン端末等を、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。

⑪ ウェブ会議サービスの利用時の対策

職員等情報取扱者は、ウェブ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しなければならず、ウェブ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。

（２）アクセス制御

① 情報管理者は、所管するネットワーク又は情報システムにアクセスする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必要最小限の範囲で適切に設定する等、システ

ム上制限しなければならない。

② 情報管理者は、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が当該サービスを利用できるようにしてはならない。

③ 外部からのアクセス

ア　職員が公社外での情報処理等作業に伴って公社内部のデータ等情報へのアクセスが必要な場合、情報セキュリティ統括責任者は、リモートデスクトップ接続等によるアクセスに限り許可するものとし、直接内部ネットワークにアクセスすることを許可してはならない

イ　情報セキュリティ統括責任者は、外部からのリモートデスクトップ接続等による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。

ウ　情報セキュリティ統括責任者は、外部からのアクセスに利用するモバイル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。

（3）システム開発、導入、保守等

① 情報システムの調達

ア　情報セキュリティ統括責任者は、情報システムの調達にあたっては、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　パッケージソフト利用時においても、機能要件以外に可用性、性能・拡張性、運用・保守性、セキュリティなどの要件を明確化し、ベンダが要件への対応について疎明することで、品質が保障されるようにしなければならない 。

② 情報システムの開発等

情報セキュリティ統括管理者は、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。

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

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

③ 情報システムの移行

ア　情報セキュリティ統括責任者は、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。また、移行の際、情報システムに記録されているデータ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に配慮しなければならない。

イ　情報セキュリティ統括責任者は、新たに情報システムを導入する際には、すでに稼

動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。また、既存の情報システムを更新する際は、すでに稼動している情報システムとの連携について、十分な試験を行わなければならない。

④ ソフトウェアの保守及び更新

情報セキュリティ統括責任者は、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らない。

（4）コンピュータウイルス等不正プログラム対策

① 情報セキュリティ統括責任者の実施事項

ア　コンピュータウイルス等の情報について職員等情報取扱者に対する注意喚起を行う。

イ　コンピュータウイルス等に関する情報収集に努める。

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とする。

② 情報管理者等の実施事項

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つ。また、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行う。

③ 職員等情報取扱者の遵守事項

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ＵＳＢフラッシュメモリ等の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ＵＳＢフラッシュメモリ等への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　差出人が不明な電子メール又は不自然なファイルが添付された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　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。

キ　コンピュータウイルス等に感染した場合は、ＬＡＮケーブルの即時取り外し又は機

器の電源遮断を行う。

ク　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、最新版へのアップデートを随時行う。

ケ　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。

（５）不正アクセス対策

① 不正アクセス防止

情報セキュリティ統括責任者及び情報管理者は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

ア　不正アクセスによるデータの書換えを検出する等、ウェブサイトの改ざんを防止する。

イ　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。

② 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、不正アクセス行為の禁止等に関する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。

③ 標的型攻撃

情報セキュリティ統括責任者及び情報管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

12. 運用面のセキュリティ対策

（１）情報セキュリティポリシー等の遵守状況の確認及び対処

情報管理者は、所管の範囲において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統括責任者に報告しなければならない。情報セキュリティ統括責任者は、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。

（２）運用管理における留意点

① セキュリティポリシー等の閲覧

情報セキュリティ統括責任者及び情報管理者は、職員等情報取扱者が常に情報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しなければならない。

② 職員等情報取扱者の報告義務

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。

（３）緊急時の対応

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重大なセキュリティ侵害が発生した場合又は発生

する恐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・再発防止等を迅速かつ適切に実施しなければならない。

13. 情報セキュリティポリシー等に関する違反に対する対応

（1）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、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、情報セキュリティ統括責任者及び情報責任者は、速やかに次の措置を講じなければならない。

① 当該職員等情報取扱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 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 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統括責任者に報告する。

14. 評価・改善・見直し

（1）監査

① 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。

② 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報化推進会議に報告しなければならない。情報化推進会議は受けた報告結果を基に議論の上、必要があれば、報告内容に応じた必要な指示をしなければならない。

③ 監査調書等の保管

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適切に保管しなければならない。

④ 指摘事項への対処

ア　情報セキュリティ監査統括責任者は、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、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

イ　情報セキュリティ監査統括責任者は、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。また、公社内で横断的に改善が必要な事項については、情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければ

ならない。

（2）自己点検

① 実施方法

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。

② 自己点検結果等の報告

ア　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化推進会議に報告しなければならない。

③ 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等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）改善

① 是正措置

情報管理者は、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。

② 予防措置

情報管理者は、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、監査及び自己点検において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ための措置を施さなければならない。

（4）情報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、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、に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーに対して必要があると認めた場合その見直しを行う。