一般財団法人大阪建築防災センター情報セキュリティ規程

目次

第１章　総則

（目的）

第１条　この規程は、情報セキュリティポリシーに基づき、一般財団法人大阪建築防災センター（以下「この法人」という。）が情報セキュリティを確保することにより、業務を継続的かつ効率的に遂行すること及び社会的信頼を獲得し、保持することを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

一「役職員等」とは、役員、正職員、常勤嘱託職員、時給契約職員、臨時の職員、派遣社員をいう。

二「情報資産」とは、次にあげるものをいう。

イ　役職員等や利用者がこの法人の業務上作成し、収集し、又は取得した情報であって、ハードウェア又は記憶装置に保存又は蓄積されているもの及び書類に記録されたもの。

ロ　ハードウェア、ソフトウェア、ネットワーク及び記憶装置で構成されるものであって、これら全体で情報を管理し業務処理を行うもの。

三「情報セキュリティ」とは、情報資産が備えるべき次に掲げる性質を健全に保つことをいう。

イ　機密性（権限を持つ者だけがアクセスできること。）

ロ　完全性（情報及びその処理方法の正確さ並びに完全さが保護されていること。）

ハ　可用性（許可された利用者が必要なときに情報及び情報システムへアクセスすることが保証されていること。）

四「情報資産に対する侵害」とは、情報の流失、漏洩、改ざん、破壊、障害等により情報資産が侵害されることをいう。

（対象の範囲）

第３条　この規程が対象とする情報資産は次のとおりとする。

一　この法人における全ての業務に係る情報

二　この法人の所有する知的財産及びそれに関する情報

三　施設、設備機器及び情報システムに関する契約文書、取扱説明書、使用許諾証明書

四　その他この法人の運営に必要な文書などの情報

第２章　組織体制

（情報セキュリティにおける理事長の役割・権限）

第４条　理事長は、この法人における全て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ものとする。

（情報セキュリティ責任者の設置）

第５条　この法人に、情報セキュリティ責任者を置き専務理事を充てるものとする。

（情報セキュリティ責任者の役割・権限）

第６条　情報セキュリティ責任者は、この法人における全ての情報資産の管理及び情報セキュリティ対策に関する決定権限及び責任を有するものとする。

２ 情報セキュリティ責任者を補佐するために、情報セキュリティ管理者を置くものとする。

３ 情報セキュリティ責任者は、情報セキュリティ管理者に対して、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ものとする。

４ 情報セキュリティ責任者は、この法人の情報資産に対する侵害が発生した場合又は発生のおそれがある場合には、必要かつ十分な措置を行う権限及び責任を有するものとする。

５ 情報セキュリティ責任者は、情報資産に関する情報セキュリティの維持・管理を行う権限及び責任を有するものとする。

６ 情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、情報セキュリティ管理者会議を活用し連絡体制を整備するものとする。

７ 情報セキュリティ責任者は、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役職員等に対する教育、訓練、助言及び指示を行うものとする。

（情報セキュリティ管理者の設置・役割）

第７条　情報セキュリティ管理者を各部・各支所に置くものとする。

２ 情報セキュリティ管理者は、部長、支所長をもって充てるものとする。

３ 情報セキュリティ管理者はその所管する各部・各支所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ものとする。

４ 情報セキュリティ管理者は、その所管する情報資産に係る情報セキュリティの維持・管理を行うものとする。

５ 情報セキュリティ管理者は、その所管する各部・各支所において、情報資産に対する侵害が発生した場合又は発生のおそれがある場合には、情報セキュリティ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ものとする。

（情報セキュリティ管理者会議の開催・招集）

第８条　情報セキュリティ対策全般の取組み状況について確認を行うため、総務・企画耐震・定期報告・防災評定・管理営業・企画調整の各部長で構成する情報セキュリティ管理者会議を年2回開催し、情報セキュリティ責任者に報告するものとする。

なお、管理営業部長は建築確認検査機構全体の、企画調整部長は構造計算適合性判定センター全体の取組み状況について、取りまとめを行うものとする。

２　情報システムの事故や情報セキュリティポリシー等への違反により情報資産に対する侵害が発生した場合、発生のおそれがある場合及び情報セキュリティ管理者から緊急に会議の招集要請があった場合は、所管する担当部長も出席する情報セキュリティ管理者会議を開催するものとする。

３　情報セキュリティ管理者会議の運営責任者に企画耐震部長を充てるものとし、庶務は企画耐震部で行うものとする。

（情報システム管理担当者の設置）

第９条　各部・各支所において、情報システムを管理するシステム管理担当者を置くものとし実務担当者をもって充てるものとする。

２ 情報システム管理担当者は、情報システムに係る情報セキュリティ実施手順の維持・管理を行わなければならないものとする。

３ 情報システム管理担当者は、情報資産に対する侵害が発生した場合又は発生のおそれがある場合には、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ものとする。

（コンプライアンス委員会の役割）

第１０条　コンプライアンス委員会は、情報セキュリティ対策を統一的に行うため、以下に掲げる情報セキュリティに関する重要な事項について、情報セキュリティ責任者に報告を求めるものとする。

一　情報セキュリティ規程等の改訂に関すること

二　情報セキュリティの事故、障害についての調査、分析に関すること

三　情報システムの導入・開発についての計画に関すること

四　情報セキュリティについての監査、自己点検に関すること

五　その他、情報セキュリティ責任者が定めたこと

２ コンプライアンス委員会はこの法人における情報セキュリティ対策全般について、情報セキュリティ責任者へ提言を行うものとする。

（システムネットワーク委員会）

第１１条　この法人における電子情報関係の共有化を図るためシステムネットワーク委員会を設置し、各部に情報セキュリティ責任者が指名するシステムネットワーク委員を置く。システムネットワーク委員は情報セキュリティ管理者等の指示等に従い、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ものとする。なお、システムネットワーク委員は、情報システム管理担当者が兼ねることができるものとする。

２　システムネットワーク委員会の委員長は総務部長、副委員長に企画耐震部長を充てるものとし、庶務は総務部で行うものとする。

第３章　情報資産の管理方法

（情報資産の管理）

第１２条　情報セキュリティ責任者は、必要に応じて情報資産について、管理方法及び取り扱いの制限を行わなければならないものとする。

２ 情報セキュリティ管理者は、その所管する情報資産について管理責任を有するものとする。また、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前項の管理方法に基づき管理しなければならないものとする。

３ 情報資産を取り扱う者は、適切な取り扱いをしなければならないものとする。

４ 情報資産を取得した者あるいは作成した者は、取得した情報資産に疑義や不明なことがある場合、情報セキュリティ管理者に判断を仰がなければならないものとする。

（物理的セキュリティの適切な管理）

第１３条　情報セキュリティ責任者は、すべての情報資産を適切に管理するため、物理的セキュリティの管理方法を定めなければならないものとする。

定める項目は次のとおりとする。

一　管理区域の管理

二　情報資産を取り扱うために必要な設備の管理

２　情報セキュリティ管理者、情報システム管理担当者は、前項で定める管理方法に基づき、

その所管する情報資産に関する物理的セキュリティを適切に管理しなければならないものとする。

（人的セキュリティの適切な管理）

第１４条　情報セキュリティ責任者は、この法人のすべての情報資産を適切に管理するため、人的セキュリティの管理方法を定めなければならないものとする。

定める項目は次のとおりとする。

一　役職員等の遵守事項

二　研修・訓練

三　事故、欠陥等の報告

四　パスワード等の管理

２ 情報セキュリティ管理者、情報システム管理担当者は、前項で定める管理方法に基づき、その所管する情報資産に関する人的セキュリティを適切に管理しなければならないものとする。

（役職員等の遵守事項）

第１５条　役職員等は、情報セキュリティポリシー及び本規程（以下「情報セキュリティポリシー等」という。）を遵守しなければならないものとする。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、速やかに所属の情報セキュリティ管理者に相談し、指示を仰がなければならないものとする。

２ 役職員等は、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、業務を離れた後も業務上知り得た情報を漏らしてはならないものとする。

（情報セキュリティポリシー等の掲示）

第１６条　情報セキュリティ管理者は、役職員等が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならないものとする。

（外部委託事業者への対応）

第１７条　情報セキュリティ管理者は、情報資産を取り扱う業務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について、必要な内容を理解させ、実施及び遵守させなければならないものとする。

（情報セキュリティに関する研修・訓練への参加）

第１８条　役職員等は、定期的に情報セキュリティに関する研修・訓練に参加するものとするものとする。

（事故、欠陥等の報告）

第１９条　役職員等は、情報セキュリティに関する事故、欠陥等を発見した場合、速やかに各部・各支所の情報セキュリティ管理者に報告しなければならないものとする。

２ 情報セキュリティ管理者は、報告のあった事故、欠陥等について、必要に応じて情報セキュリティ責任者に報告しなければならないものとする。

３ 情報セキュリティ責任者は、報告のあった事故、欠陥等についてコンプライアンス委員会に報告するとともに当該事故、欠陥等が情報システムに関連する場合、速やかに情報システム管理担当者に指示をしなければならないものとする。

（事故、欠陥等の是正・記録等）

第２０条　情報セキュリティ責任者は、事故、欠陥等を引き起こした各部・各支所の情報セキュリティ管理者及び情報システム管理担当者と連携し、これらの事故、欠陥等を分析し、記録を保存し、結果を理事長に報告しなければならないものとする。

（ユーザアカウントの取り扱い）

第２１条　役職員等は、自己の管理するユーザアカウントに関し、次の各号の事項を遵守しなければならないものとする。

一　自己が利用しているユーザアカウントは、他人に利用させてはならないものとする。

二　共用ユーザアカウントを利用する場合は、共用ユーザアカウントの利用者以外に利用させてはならないものとする。

（パスワードの取り扱い）

第２２条　役職員等は、自己の管理するパスワードに関し、適切に管理しなければならないものとする。

（技術的セキュリティ）

第２３条　情報セキュリティ責任者は、この法人の情報資産を適切に管理するため、システムネットワーク委員会を活用して技術的セキュリティの管理方法を定め、適切に管理しなければならないものとする。

定める項目は次のとおりとする。

一　ハードウェアの導入・調達・保守・管理

二　ネットワークの維持・管理

三　情報システム及び情報サービスの導入・調達・開発・管理

四　セキュリティ侵害対策・違反防護策等の導入・維持・管理

五　その他

第４章　情報セキュリティポリシー等の遵守状況の確認

（遵守状況の確認及び対処）

第２４条　情報セキュリティ責任者は、情報セキュリティポリシー等の遵守状況について確認を

行い、問題を認めた場合には、コンプライアンス委員会に報告を行わなければならないものとする。

２ 情報セキュリティ責任者は、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ものとする。

（役職員等の報告義務）

第２５条　役職員等は、情報セキュリティポリシー等に対する違反行為や問題を発見した場合、直ちに各部・各支所の情報セキュリティ管理者に報告を行わなければならないものとする。

２ 報告を受けた情報セキュリティ管理者は、情報セキュリティ責任者に報告をしなければならないものとする。

３ 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責任者が判断した場合は、理事長に報告するとともに適切に対処しなければならないものとする。

第５章　侵害時の対応

（侵害時の対応）

第２６条　情報セキュリティ責任者は、情報システムや情報セキュリティポリシー等への事故・違反により情報資産に対する侵害が発生した場合又は発生の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、緊急時対応方法を定め、コンプライアンス委員会に承認を得るものとする。

２　緊急時対応方法には、以下の内容を定める。

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

第６章　外部委託

（外部委託先の選定基準）

第２７条　この法人は、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の確認をした上で契約締結を行うものとする。

（契約項目）

第２８条　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各号の情報セキュリティ要件を明記した契約の締結を行うものとする。

一　情報セキュリティポリシー等に関する規定の遵守

二　委託先の責任者、委託内容、作業者、作業場所の特定

三　従業員に対する教育の実施

四　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

五　再委託に関する制限事項の遵守

六　委託業務終了時の情報資産の返還、廃棄等

七　情報セキュリティポリシー等が遵守されなかった場合の規定（損害賠償等）

第７章　法令遵守

（法令遵守）

第２９条　役職員等は、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、関係法令を遵守し、これに従わなければならないものとする。

第８章　違反時の対応等

（懲戒処分等）

第３０条　情報セキュリティポリシー等に違反した役職員等は懲戒処分等の対象とすることが

できるものとする。

第９章　評価・見直し

（取組状況の報告）

第３１条　情報セキュリティ責任者は、情報資産における情報セキュリティ対策状況について、情報セキュリティ管理者会議から定期及び必要に応じて報告を行わせるものとする。

（理事会への報告）

第３２条　情報セキュリティ責任者は、取組状況を取りまとめ、定期的に理事会に報告を行うものとする。

（文書等の保管）

第３３条　情報セキュリティ責任者は取組状況の報告に関わる文書等について、紛失しないように適切に保管しなければならない。

（情報セキュリティポリシー等の見直し）

第３４条　この法人は、情報セキュリティポリシー等について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

（施行期日）

１　この規程は、平成２９年2月１日から施行する。

２　この規程は、平成３０年４月１日から施行する。