地方独立行政法人天王寺動物園情報セキュリティ管理規程

令和３年４月１日
最近改正　令和５年８月１日

（趣旨）
第１条 この要綱は、地方独立行政法人天王寺動物園（以下「法人」という。）が保有する情報資産の情報セキュリティ確保のために必要な事項を定めるものとする。
（定義）
第２条 この要綱における用語の意義は、次の各号に定めるところによる。
(1) 情報資産 情報システム及び情報通信ネットワークの開発及び運用管理に係るファイル（データを記録している電磁的記録をいう。以下同じ。）及びドキュメント（情報システムの設計書、操作手引書、プログラムリスト、ネットワーク構成図その他の電子計算機の運用に関する文書をいう。）、情報システム及び情報通信ネットワークで取り扱うデータに係るファイル並びに情報システム及び情報通信ネットワークを構成する機器。
(2) 情報セキュリティ 情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに定められた範囲での利用可能な状態を維持することをいう。
(3) 情報セキュリティポリシー この要綱及び第７条に規定する情報セキュリティ対策基準をいう。
(4) 情報セキュリティ対策 情報セキュリティを確保するために実施する各種の対策をいう。
(5) 電子計算機処理 電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。
(6) 電磁的記録 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。
(7) データ 電子計算機処理に係る電磁的記録又はドキュメントに記録されている情報をいう。
（職員の責務）
第３条 職員は、情報セキュリティの重要性を十分に認識し、情報セキュリティポリシーを遵守するとともに、条例その他の関連する法令等を遵守し、情報資産を適切に管理しなければならない。
（最高情報統括責任者等の設置）
第４条 法人における情報化を推進し統括するため、法人に最高情報統括責任者、情報統括責任者及び副情報統括責任者を置く。

２ 最高情報統括責任者は、法人における情報化に関する事務を統括するものとし、副理事長をもって充てる。
３ 情報統括責任者は、最高情報統括責任者の命を受け、次の各号に掲げる事務を掌理するものとし、総務部長をもって充てる。
（１）情報化に伴う情報システムの企画、開発及び運用に関すること
（２）通信ネットワークの整備及び運用に関すること
（３）情報システムの企画、開発及び運用並びに通信ネットワークの整備及び運用に係る経費の縮減に関すること
（４）その他情報セキュリティの確保に関して必要な事務
４ 副情報統括責任者は、情報統括責任者を補佐するものとし、総務課長をもって充てる。
（ＩＴ責任者等の設置）
第５条 法人における情報通信の技術の適正な利用を推進するため、ＩＴ責任者を置く。
２ ＩＴ責任者は、自らの所掌事務における情報化に関する事務を掌理するものとし、総務課長および運営課長、飼育展示課長、動物診療課長、施設課長をもって充てる。
３ ＩＴ責任者は、所属職員に対する情報セキュリティポリシーの遵守に関する指導、助言及び研修その他自らの所掌事務における情報セキュリティ対策が、適切かつ確実に実施されるよう必要な措置を講じなければならない。
（情報資産の分類）
第６条 ＩＴ責任者は、所管する情報資産をその内容に応じて分類し、重要度に応じた情報セキュリティ対策を実施しなければならない。
（情報セキュリティ対策基準の作成）
第７条 情報統括責任者は、法人における情報セキュリティ対策の実施に関する統一的な基準を定めるため、情報セキュリティ対策基準を作成しなければならない。
（情報セキュリティ対策実施手順の作成）
第８条 ＩＴ責任者は、所管する情報システム又は通信ネットワークにおける情報セキュリティ対策の実施に関し必要となる事項を定めるため、情報セキュリティ対策実施手順を作成し、情報統括責任者に報告しなければならない。
（業務の委託）
第９条 情報統括責任者は、電子計算機処理業務の全部又は一部を委託しようとする場合は、データの秘密保持に関する事項、契約又は協定に違反したときの契約解除又は指定の取消しに関する事項、損害賠償に関する事項その他最高情報統括責任者が定める事項を委託契約書又は協定書に明記するなど、情報資産の適切な管理のため

に必要な措置を講じなければならない。

（事故発生時の措置）

第10条　ＩＴ責任者は、所管する情報資産に漏えい、滅失、き損、改ざん等の事故が発生したときは、直ちにその状況を調査し、必要な措置を講ずるとともに、事故の内容及び講じた措置を情報統括責任者に報告しなければならない。

２　情報統括責任者は、前項の規定による報告を受けたときは、再発防止のために必要な措置が適切に講じられるよう指導及び監督を行わなければならない。

（見直しの実施）

第11条　情報統括責任者は、情報セキュリティをめぐる情勢の変化を踏まえ、適宜情報セキュリティ対策基準に検討を加え、必要があると認めるときは、これを変更しなければならない。

２　ＩＴ責任者は、前項の規定に準じて、情報セキュリティ対策実施手順に検討を加え、必要があると認めるときは、これを変更しなければならない。

（データの管理）

第12条　ＩＴ責任者は、条例第２条第５項に規定する電子計算機処理に係る電磁的記録及び入出力帳票の取扱いに関し、漏えい、滅失、き損、改ざん及び不正な利用、提供等を防止するなど、適切に管理しなければならない。

２　データの管理の方法その他必要な事項は、情報統括責任者が別に定める。

（通信ネットワークの管理及び整備）

第13条　情報統括責任者は、通信ネットワークの整備及び運用に関する要綱を定め、これに基づき、通信ネットワークの管理及び整備を行わなければならない。

（施行の細目）

第14条　この要綱の施行に関し必要な事項は、情報統括責任者が定める。

附則

（施行期日）

この規程は、令和３年４月１日から施行する。

附則

（施行期日）

この規程は、令和５年８月１日から施行する。

地方独立行政法人天王寺動物園情報セキュリティ対策基準

令和３年４月１日
最近改定　令和４年10月１日

１ 目的

この地方独立行政法人天王寺動物園情報セキュリティ対策基準（以下「対策基準」という。）は、地方独立行政法人天王寺動物園情報セキュリティ管理規程（以下「規程」という。）第７条に基づき、法人における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な基準を定めることにより、法人が保有する情報資産を様々な脅威から守り、機密性、完全性及び可用性(注) を維持することによって園内サービスを安全に提供し、もって法人事業の円滑な運営と来園者の信頼を確保することを目的とする。

（注）：国際標準化機構(ISO)が定めるもの(IS07498-2：1989)
機密性(confidentiality) ： 情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性(integrity) ： 情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性(availability) ： 許可された利用者が必要なときに情報アクセスできることを確実にすること。

２ 用語

この対策基準において使用する用語は、規程において使用する用語の例による。

３ 適用範囲

この対策基準の適用範囲は、法人職員及び法人の保有する情報資産とする。

４ 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1)　不正アクセス、ウイルス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程違反、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、火災等の災害等

(4)　電力供給の途絶、通信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

脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1)　情報資産の管理

保有する情報資産を機密性、完全性及び可用性を踏まえ重要性に応じた情報セキュリティ対策を行う。

(2)　物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員の端末機等の管理について、物理的な対策を講じる。

(3)　人的セキュリティ

情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(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、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。

６ 組織・体制及び役割・責任

(1)　情報セキュリティに係る管理体制・役割

規程第４条及び第５条に基づき、情報セキュリティ対策が円滑に推進されるための体制・役割を定める。

①　最高情報統括責任者

最高情報統括責任者は、法人における最高情報セキュリティ責任者として、法人における情報セキュリティ対策に関する事務を統括する。

②　情報統括責任者

ア　情報統括責任者は、最高情報統括責任者の命を受け、法人における情報セキュリティ対策に関する統括的な事務を掌理する。

イ　情報統括責任者は、ＩＴ責任者に対し、情報セキュリティ対策の統一的な実施に必要な指導、助言又は調整を行う。

③　副情報統括責任者

副情報統括責任者は、情報統括責任者を補佐する。

④　ＩＴ責任者

ア　ＩＴ責任者は、自らの所掌事務における情報セキュリティ対策の実施、その他情報セキュリティに関する事務を掌理するものとする。

イ　ＩＴ責任者は、自らの所掌事務における各情報システムの開発及び運用状況、データの管理状況、通信ネットワークの利用状況等を把握し、所管する情報資産の情報セキュリティ対策が適切かつ確実に実施されるよう必要な措置を講じなければならない。

ウ　ＩＴ責任者は、所属職員に対する情報セキュリティポリシー（以下「ポリシー」という。）の遵守に関する指導、助言及び研修その他、自らの所掌事務における情報セキュリティ対策が適切かつ確実に実施されるよう必要な措置を講じなければならない。

エ　ＩＴ責任者は、情報資産の利用者（以下「利用者」という。）がデータ及びプログラムを利用できる権限（以下「アクセス権限」という。）等に基づき、安全性に十分配慮し適切な利用が行われるよう、パソコン等の管理を行わなければならない。

(2)　情報システムに係る管理体制・役割

法人における情報システムの整備及び運用について、安全性及び信頼性を確保するための体制・役割を定める。

①　業務管理責任者

ア　業務管理責任者は、情報システムの運用・保守の実施並びに管理を担うものとし、当該情報システムに係る業務を所管するＩＴ責任者をもって充てる。

イ　業務管理責任者は、情報システムの運用を開始しようとするときは、システム運用管理責任者と協議し、情報セキュリティ対策手順を作成しなければならない。

ウ　業務管理責任者は、情報システムの運用において、入力資料の作成、電子計算機処理、帳票の出力などに至る業務全体の実施状況を把握・管理しなければならない。

②　システム運用管理責任者

ア　システム運用管理責任者は、法人における当該情報システムの適切な運用管理を担うものとし、ハードウエア（端末機、プリンタ等）及びソフトウエアの運用管理を担うＩＴ責任者をもって充てる。

イ　システム運用管理責任者は、情報システムが正常に稼働するよう、安全性に十分配慮し適切な運用管理を行わなければならない。

③　副システム運用管理責任者

ア　副システム運用管理責任者は、システム運用管理責任者を補佐するものとする。

(3)　通信ネットワークに係る管理体制・役割

規程第13条に基づき、法人における通信ネットワークの整備及び運用について、安全性及び信頼性を確保するための体制・役割を定める。

①　総括ネットワーク管理責任者

総括ネットワーク責任者は法人通信ネットワークの整備及び運用管理において情報セキュリティを確保するために必要な措置を講じるものとし、情報統括責任者をもって充てる。

②　施設ネットワーク管理責任者

施設ネットワーク管理責任者は、法人における通信ネットワークの整備及び運用管理

において、情報セキュリティを確保するために必要な措置を講じるものとし、これらの施設において通信ネットワークを所管するＩＴ責任者をもって充てる。

７ 不正アクセス等侵害時における緊急連絡体制

情報統括責任者は、不正アクセス等による緊急の事態により情報資産に重大な被害が生じた場合又は生じる恐れがある場合、以下の関係者その他必要と認める者と連携を図り、情報セキュリティ対策が適切に実施されるよう監督、指導を行わなければならない。

・情報統括責任者
・業務管理責任者
・システム運用管理責任者
・施設ネットワーク管理責任者

８ 情報資産等の管理

ＩＴ責任者は、以下の情報セキュリティ対策を行わなければならない。

(1) 情報資産の管理責任

① 管理責任

情報資産は、ＩＴ責任者が適切に管理する責任を有する。

② 利用者の責任

情報資産を業務上利用する職員は、適切に利用する責任を有する。

③ 重要性の効力

データが複製又は伝送された場合には、当該複製等も管理しなければならない。

(2) データ及び情報資産の管理

① データの管理

ＩＴ責任者は、データの作成にあたり、次の各号により取り扱わなければならない。

（ア） 業務上必要のないデータを作成してはならない。

（イ） 作成途上のデータであっても漏えい、滅失、き損、改ざん等を防止しなければならない。また、作成途上で不要になった場合は、当該データを消去しなければならない。

② 情報資産の管理

ア 情報資産の管理及び取扱い

（ア） 情報資産の管理については、大阪市個人情報保護条例（平成７年大阪市条例第11号。以下「個人情報保護条例」という。）及び規程に基づき、データの漏えい､滅失、き損、改ざん、消去、盗難等の防止を図るため必要な措置を講じなければならない。

（イ） 最高情報統括責任者は、法人が保有する情報資産を他の法人等に利用させようとするときは、セキュリティ対策上支障がないか確認しなければならない。また、情報資

産を利用させようとする他の法人等と情報セキュリティに係る連絡調整体制を構築し、ポリシー及び情報セキュリティ対策手順に準じた情報資産の取扱いを指導及び遵守させなければならない。

（ウ） 情報資産は、重要性に応じて、適切に取り扱わなければならない。

イ 情報資産の利用

（ア） 業務以外の目的に情報資産を利用してはならない。

（イ） 情報資産について、定められた場所以外で利用してはならない。ただし、業務遂行上、外部への持ち出しが不可欠である場合については、ＩＴ責任者の許可を得て持ち出すことができる。

（ウ） 保護データを外部へ持ち出すときは、必要に応じて暗号化又はパスワード設定を行わなければならない。

ウ 記録媒体の管理

（ア） ＩＴ責任者は、記録媒体の保管について媒体の種別、作成年月日等必要な事項を記載した台帳を整備し、データの重要性が容易に識別できるようにするとともに、これらを所定の場所において適切に管理しなければならない。また、記録媒体のバックアップを定期的に取得し、所定の場所において適切に管理しなければならない。

（イ） ＩＴ責任者は、保護データを記録した記録媒体を保管する場合は、鍵のかかるキャビネット等施錠できる場所に保管し、又は予備を作成して別の施設に保管しなければならない。

（ウ） ＩＴ責任者は、記録媒体に不要なデータが放置されないよう、不要となったデータを速やかに消去するなど、適正に運用しなければならない。

（エ） ＩＴ責任者は、情報資産を廃棄するときは、データ消去その他の適切な措置を講じなければならない。特に、保護データについては、情報を復元できないよう確実に消去を行うとともに、行った処理について、日時、担当者、処理内容等その他必要な事項を記録しなければならない。

（オ） ＩＴ責任者は、プログラムの登録・廃棄についてプログラム登録簿を作成し、適切に管理しなければならない。

9 物理的セキュリティ

(1) 情報システムにおける措置

① サーバ等

ア 装置の取り付け等

（ア） サーバ等を取り付ける場合は、火災、水害、埃、振動、温度及び湿度等の影響を可能な限り排除した場所に設置するとともに、当該場所については、職員が不在時の盗難防止のため、施錠等による措置を講じなければならない。

（イ） 重要なデータを取り扱い、かつ、システムの停止によって、原則として当該機器等

の管理及び運用を行うための部屋（以下「情報システム室」という。）に設置しなければならない。

（ウ） サーバ等の取り付けに当たっては、震災時の転倒又は盗難の防止のため、適切に固定する等必要な措置を講じなければならない。

（エ） 配線については、傍受又は損傷を受けることがないように可能な限り必要な措置を講じなければならない。また、主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

イ　電源設備

サーバ等の電源については、停電時に当該機器を適切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。また、落雷等による異常電流に対してサーバ等を保護するための措置を講じなければならない。

ウ　サーバ等の機種更新

サーバ等の機種更新を行おうとする時、特に並行稼動時においては、サーバ等の設置場所における電源設備、空調設備等の能力及び容量並びに現時点での設備の残存能力及び容量を把握し、適切な対応を講じなければならない。

②　端末機等

ア　執務室等における措置

情報資産を保管する執務室等については、職員が不在時の盗難防止のため、執務室等の施錠等による措置を講じなければならない。 また、端末機等の施錠可能なロッカー等での保管およびロッカーがない場合は、セキュリティーワイヤーを用いて固定措置を講じ、盗難防止につとめなければならない。なおセキュリティーワイヤーの鍵はIT責任者もしくはIT責任者が指定した職員が保管することとする。

イ　情報システム室における措置

情報システム室に設置される端末機等については、震災時の転倒又は盗難の防止のため、適切に固定する等必要な措置を講じなければならない。

ウ　持出用機器の措置

法人が用意する持出用機器についてはIT責任者が保管および管理することとし、管理台帳に必要事項を記入の上、IT責任者の承認を受けた上で使用することとする。

(2)　通信ネットワークにおける措置

①　通信ネットワーク構築上の措置

ア　通信ネットワークについては、取り扱う情報の重要性及び必要性に応じて、物理的又は論理的に切り分けて構築しなければならない。

イ　通信ネットワークの外部への通信ネットワーク接続については、公益上特に必要である場合を除き行わないこととし、かつ、接続する場合であっても、必要最小限の範囲に限る。また、接続ポイントを一元化し、情報セキュリティ対策を集約的に実施できるようにする。

② 通信ネットワーク機器等

ア 通信ネットワークの基幹機器（管理用及び認証用サーバ、交換機等）については、情報システム室に設置しなければならない。また、通信ネットワークの運用上重要な機能を有するサーバ等については、障害発生時に通信ネットワークの運用が停止しないように二重化を図る等必要な措置を講じなければならない。

イ 主要な通信ネットワーク機器（ハブ、ルータ等）については、システム運用管理責任者が容易に操作できないような場所に格納する等必要な措置を講じるとともに、通信ネットワーク機器等の構成管理を適切に行わなければならない。

ウ 主要な通信ネットワーク機器については、落雷等による異常電流及び停電等の電気的障害に対し必要な措置を講じなければならない。

③ 通信回線

ア 通信ネットワークは、専用回線又は高いセキュリティ機能を有する回線により構成し、外部からの情報の盗聴及び情報の漏えい等を防止しなければならない。

イ 通信ネットワークは、必要な範囲の通信回線においてバックアップ用の回線を敷設する等、障害の発生に備えなければならない。

(3) 情報システム室における措置

① 管理区域

ア 情報システム室については、外部からの侵入が容易にできない管理区域としなければならない。

イ 管理区域から外部に通じるドアについては必要最小限とし、施錠、警報装置、監視装置等により許可されていない者の立入りを防止しなければならない。

ウ 情報システム室については、外部にその表示を行わない等、できるだけ所在を明らかにしないようにしなければならない。

④ 機器等の搬入

ア 情報システム室に機器等を搬入する場合は、あらかじめ当該機器等の既存システムに対する安全性について確認を行わなければならない。

イ 機器等の搬入には、立会い等必要な措置を講じなければならない。

⑤ 火災・震災等災害に対する措置

ア 情報システム室は、防火区画を設ける等の防火及び防煙に対する措置を講じなければならない。

イ 情報システム室の消火設備は、サーバ等や記録媒体に影響を与えるものであってはならない。また、火気の取り扱いについて厳重な管理を行わなければならない。

ウ 情報システム室を設置する建物及び情報システム室は、地震等に対する耐震措置を講じなければならない。また、情報システム室内の機器類は転倒防止措置を講ずるとともに、緊急時に職員及び外部委託事業者が円滑に避難できるように配置しなければならない。

エ　情報システム室には、浸水及び漏水防止等の措置を講じなければならない。

オ　空気調和設備は、急激な温湿度変化等に対処するため、その容量に配慮しなければならない。

⑥　電気的障害に対する措置

ア　情報システム室は、無停電電源装置の設置等、落雷等による異常電流に対する措置を講じなければならない。

イ　停電による情報システム等の停止が業務運営等に重大な影響を及ぼす可能性がある場合、必要に応じ、自家発電装置の設置等の措置を講じなければならない。

10 人的セキュリティ

(1)　職員における情報セキュリティの徹底

①　ポリシー等の遵守

全ての職員は、ポリシー及び情報セキュリティマニュアルに定められている事項を遵守しなければならない。

②　教育、研修

ア　ポリシーの周知等

(ア)　情報統括責任者は、ポリシーの周知徹底を行わなければならない。また、研修機会等を利用して、情報セキュリティの啓発に努めなければならない。

(イ)　ＩＴ責任者は、所属職員に対しポリシー及び情報セキュリティマニュアルの遵守について啓発しなければならない。

(ウ)　ＩＴ責任者は、所属職員がポリシー及び情報セキュリティマニュアルについて理解し、情報セキュリティ上の問題が生じないよう、教育、指導を行わなければならない。

イ　情報システムに係る情報セキュリティの徹底

業務管理責任者は、研修の実施等により、情報システムの運用に関わる職員を対象に、情報システム及び当該情報システムにより処理されるデータに係る情報セキュリティマニュアルの実施に必要な知識及び技術等について教育、指導を行わなければならない。

ウ　通信ネットワークに係る情報セキュリティの徹底

総括ネットワーク管理責任者は、通信ネットワークにおける必要な知識及び技術等について周知徹底を行わなければならない。

③　職員における情報管理

ア　情報の適切な処理及び業務目的以外の使用禁止

(ア)　職員は、設定されているアクセス権限に基づき、業務上必要な情報の処理を適切に処理しなければならない。

(イ)　職員は、業務目的以外での情報システムへのアクセス及びホームページの閲覧、メ

ールの使用、ファイルサーバの利用等を行ってはならない。

（ウ） 職員は利用目的が不明なプログラムを作成、配付、保存してはならない。

イ　情報の漏えい等の防止及びアクセス権限情報の管理

（ア） 職員は、業務管理責任者の許可なくして、パソコン等を執務室以外に持ち出してはならない。持ち出しが必要な場合は、持出用端末の持出を優先すること。

（イ） 職員は、業務管理責任者が許可したパソコン等を使用するものとし、私物のパソコン等を業務で使用し、又は執務室内に持ち込んではならない。

（ウ） 職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

（エ） 職員は、アクセス権限に係る情報を適切に管理し、自己の保有する暗証符号（以下「パスワード」という。）に関しては、次の事項を遵守しなければならない。

・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ないこと

・パスワードは十分な長さ（最低4 文字以上とする。）とし、文字列は想像しにくいものとすること

・パスワードは定期的に変更すること

・仮のパスワードは、最初のログイン時点で変更すること

・パソコン等にパスワードを記憶させないこと

・パスワードが流出した可能性がある場合は、速やかにＩＴ責任者に報告し、パスワードを変更すること

（オ） 職員は、使用するパソコン等について、権限を有しない者の使用や閲覧を防止するため、パソコン等から離れる場合にはロック又はログオフにする等適切な措置を講じなければならない。

ウ　無許可ソフトウエアの導入等の禁止

（ア） 職員は、業務管理責任者等の許可なくパソコン等へのソフトウエアのインストール及びアンインストール、若しくは機器の改造、設定変更及び増設、交換を行ってはならない。

（イ）職員は、著作権法等に違反するソフトウエアの使用又は複製等を行ってはならない。

エ　事故、欠陥に対する報告

（ア） 職員は、情報システムの利用に際して事故、欠陥を発見した場合又は来園者等外部から通報を受けた場合は、速やかにＩＴ責任者に報告しなければならない。

（イ） 職員は、通信ネットワークの利用に際して事故、欠陥を発見した場合は、速やかに業務管理責任者に報告しなければならない。

（ウ） 職員は、業務管理責任者の指示に従い、事故、欠陥に対し適切に対処しなければならない。

（エ） 職員は、情報セキュリティに対する事故、情報システム上の欠陥及び誤動作を発見

した場合又は来園者等外部から通報を受けた場合は、システム運用管理責任者に報告しなければならない。

(2)　外部委託における管理

①　委託処理に当たっての基本原則

ア　情報システム及び通信ネットワーク（以下「情報システム等」という。）の運用及び保守を所管する業務管理責任者、及びシステム運用管理責任者は、これらの業務の全部又は一部を事業者に委託しようとする場合、主体性が損なわれないよう法人の責務等次の点に留意するとともに、事業者において情報セキュリティ対策が徹底されるよう必要な 措置を講じなければならない。

（ア）　調整・管理機能、スケジュール等業務全体の遂行を左右する重要な要件や機能を法人のコントロール下におくこと。

（イ）　情報システム等に係わる業務を委託しようとするときは、情報システム等のブラックボックス化を防止するために、定期的に検討会議等を設置するなど適切な措置を講じること。

イ　情報システム等に係る業務の委託については、事業者において厳重な情報セキュリティ対策が実施されるように管理、指導を行わなければならない。

ウ　情報システム等の開発、運用等において複数の事業者が関わる場合は、その分担範囲・責任範囲を明確にするとともに、それらの連携を確保しなければならない。

②　委託処理における措置

ア　次の事項を委託契約書若しくは協定書（以下「委託契約書等」という。）に明記し、事業者にその内容を遵守させなければならない。

・データの秘密保持に関する事項
・再委託の禁止又は制限に関する事項
・データの無断使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
・事故発生時における報告義務に関する事項
・データの保護管理のために必要な措置及びデータの処理状況の監督等に関する事項
・以上の定めに違反した場合における契約解除、個人情報保護条例第16 条第2 項に規定する公表等の措置及び損害賠償に関する事項

イ　上記の事項以外に必要に応じて、次の事項を委託契約書等に明記し、事業者にその内容を遵守させなければならない。

・入出力帳票の授受及び搬送に関すること
・入出力帳票の委託先における保管及び廃棄に関すること
・その他データの保護に関し必要なこと

ウ　事業者における情報セキュリティの徹底を図るため、次の項目に留意し適切に管理、指導を行わなければならない。

（ア） 委託業務の処理に当たっては、委託先となる事業者について次の事項を調査、確認すること。

・委託先の事業概要
・委託業務処理のための使用機器構成
・データ保護に関する委託先の規定等
・データの管理体制
・委託業務を行う事業所の防災及び保安対策
・事故等緊急時における連絡体制
・その他ＩＴ責任者が必要と認める事項

（イ） 重要な情報を処理する場合等においては、必要に応じ、委託契約書等の他、機密保護等に係る覚書を交わすこと

（ウ） 事業者における情報セキュリティ対策の実施責任者を定めさせること

（エ） 重要な情報を処理する場合等必要に応じ、事業者において、委託業務に関わる事業者の職員から機密保護等の誓約書をとらせること。また、必要に応じ、事業者において、当該職員に対し情報セキュリティに関する研修を実施させること

（オ） 事業者における情報セキュリティ対策の実施状況について適宜報告を求めること。また、必要に応じ、事業者の管理記録簿の確認又は作業場所の立ち入り検査等を行うこと

（カ） 重要な情報を処理する場合等必要に応じ、法人職員が処理に立ち会うこと

（キ） 委託業務に関わる事業者の職員に対し身分証明書等の携帯、着用を義務付ける等、契約で定められた資格を有する者が作業に従事していることを確認すること

（ク） 契約又は協定に基づき作業を行う者の認証符号（以下「ユーザＩＤ」という。）、パスワード等について、作業終了後、不要となった時点で速やかに抹消すること

（ケ） 契約又は協定に基づき取り扱ったデータ等については、契約又は協定終了後、不要となった時点で速やかに返還又は消去させること

11 技術的セキュリティ

(1) 不正アクセス対策

① アクセス記録の取得等

ア 総括ネットワーク管理責任者及び施設ネットワーク管理責任者は、通信ネットワークの利用に当たり、業務目的以外のホームページの閲覧等不適切な利用が行われないように制限をかけることができる。

イ 総括ネットワーク管理責任者及び施設ネットワーク管理責任者は、職員が業務目的以外の不適切な利用を行おうとしていることが判明した場合、適切な措置を講じなければならない。

② 外部通信ネットワークとの接続に係る措置

ア　総括ネットワーク管理責任者及び施設ネットワーク管理責任者は、通信ネットワークを外部接続するときは、情報統括責任者の承認を受け、適切に実施及び管理を行わなければならない。

イ　施設ネットワーク管理責任者は、データ提供のために法人以外の者と情報システムの接続を行うときは、情報統括責任者に報告を行い、適切に実施及び管理を行わなければならない。

ウ　外部からのアクセスの許可は、必要最小限にしなければならない。また、外部から通信ネットワーク、情報システムにアクセスする場合は、外部アクセスサーバに対してのみ接続を許可する等、内部への不正なアクセスを防御する構成としなければならない。

エ　外部からの不正なアクセスを防御するため、ファイアウォール、侵入検知装置の設置、ポートの管理、アクセス状況の監視等、必要な措置を講じなければならない。

オ　総括ネットワーク管理責任者、業務管理責任者、システム運用管理責任者及び施設ネットワーク管理責任者は、情報セキュリティに関する最新の情報を収集し、通信ネットワーク、情報システムの端末機及びサーバ等のソフトウエアに最新のプログラム修正を行うことにより、セキュリティホールを防ぐ等、必要な措置を講じなければならない。

カ　外部通信ネットワークを利用し、法人以外の者と通信（メールの利用又はホームページによる情報提供等を行う場合を除く。）を行うときは、原則として重要なデータは取り扱ってはならない。業務上、当該データの取り扱いが特に必要な場合については、情報の漏えい、改ざん等を防止するため、あらかじめ個人情報保護条例に基づき必要な対処を行うとともに、通信先との相互の認証、データの暗号化、セキュリティの高い通信回線の利用等必要な措置を講じなければならない。また、その際、使用する暗号鍵については厳重に管理しなければならない。

キ　外部通信ネットワークを利用し、法人以外の者とメールにより事務連絡を行うときは、原則として重要な情報は取り扱ってはならない。業務上、重要な情報の取り扱いが特に必要な場合については、ＩＴ責任者の承認を得るとともに、連絡相手のメールアドレス及びメール受け取りの確認、データの暗号化を行う等､厳格に取り扱わなければならない。なお、法人内においてメールを利用する場合においても、上記の取り扱いに準じ、適切に運用を行わなければならない。

ク　ホームページを利用した情報提供等においても、原則として個人情報は取り扱ってはならない。ただし、利用者へのサービス向上の観点から個人情報を取り扱う必要があるときは、あらかじめ個人情報保護条例に基づき必要な対処を行い適正に運用しなければならない。なお、法人内向けのホームページについても、上記の取り扱いに準じ、適切に運用を行わなければならない。

(3)　コンピュータウイルス対策

職員は、次の事項を遵守しなければならない。

・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、必ずウイルスチェックを行う

こと
・情報システム室管理責任者の許可を得て持ち出したパソコン等を法人の通信ネットワークに接続しようとするときは、当該パソコン等についてコンピュータウイルスの感染の有無及びセキュリティパッチの適用状況等について確認を行うこと
・データが添付されたメールを送受信するときは、当該データにウイルスが感染していないかどうか確認を行うこと
・差出人が不明又は不自然に添付されたデータは開かず速やかに削除すること
・私物の携帯電話、タブレット及びパソコン等通信機能がある機器を、業務管理責任者の許可なくして法人が管理する通信ネットワークに接続させないこと

(4)　情報システムの導入及び保守における措置

①　情報システムの調達

業務管理責任者は、情報システムの調達に当たって、調達仕様書が情報セキュリティの確保の上で問題のないようにしなければならない。

②　情報システムの導入

業務管理責任者は、情報システムを導入する前に十分なテストを行い、不具合の発見及び解消に努めなければならない。

③　システムの保守

業務管理責任者及びシステム運用管理責任者は、情報システムの追加、変更、廃棄等をしたときは、その際の履歴を記録するとともに、ドキュメントの変更整備を行わなければならない。

④　機器の保守等

ア　記憶媒体の含まれる機器について、外部の業者に修理させる場合は、当該機器に記憶されている内容が消去された状態で行わなければならない。ただし、情報を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。

イ　記憶媒体の含まれる機器を廃棄する場合は、当該機器に記憶されている内容を廃棄しなければならない。特に、重要なデータを格納する機器については、データを復元できないよう確実に消去しなければならない。

12 ポリシー等の遵守

(1)　ポリシー等の遵守状況の確認

①　ＩＴ責任者は、自らの所掌事務において、ポリシー及び所管する情報資産に係る情報セキュリティ対策手順が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに、情報統括責任者に報告しなければならない。

②　情報統括責任者は、ポリシー等の遵守状況及び問題発生の状況について確認を行うた

め、ＩＴ責任者に随時報告を求めることができる。

③　所管する情報資産に係る情報セキュリティ対策手順の作成方法等については、情報統括責任者が定める。情報統括責任者は、手順の作成又は見直しが行われた場合、ＩＴ責任者から報告を受けなければならない。

(2)　端末機及び記録媒体等の利用状況調査の権限

情報統括責任者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、端末機及び記録媒体等のアクセス記録、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)　ポリシー等に関する違反に対する対応

法令及びポリシーに違反した職員及び当該職員の管理監督者については、その重大性、発生した事案の状況等に応じて、懲戒処分等の対象となることがある。

13 点検・評価及び見直し

(1)　点検・評価

①　ＩＴ責任者は、所管する情報資産に係る情報セキュリティ対策手順に基づき必要な情報セキュリティ対策が実際に実施されているかどうか、また、記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行わなければならない。外部委託事業者に委託している場合、ＩＴ責任者は、ポリシーの遵守について定期的に点検を行わなければならない。

②　ＩＴ責任者は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、ポリシーの記載に疑義が生じたときは、直ちに情報統括責任者に報告しなければならない。

③　情報統括責任者は、ＩＴ責任者に対し、情報セキュリティ対策の点検実施の要請及び点検結果の報告を求めることができる。

(2)　セキュリティ対策の見直し、変更

①　情報統括責任者は、情報セキュリティをめぐる情勢の変化及び情報セキュリティ監査の結果を踏まえ、適宜対策基準の実効性を評価し、必要があるときは見直し、変更を行わなければならない。

②　情報統括責任者は、対策基準の変更を行ったときは、速やかにＩＴ責任者その他関係者に周知を行わなければならない。

③　ＩＴ責任者は、所管する情報資産について、ポリシーの変更並びに情報セキュリティをめぐる情勢の変化等に伴い、適宜情報セキュリティ対策の見直しを行ない、必要があると認めるときは、当該情報システム及び通信ネットワークの手順書の変更を行わなければならない。

14 対策基準等の取り扱い

公にすることにより法人の事業運営に重大な支障を及ぼすおそれのある情報については、非公開とする。

附則

（施行期日）

この対策基準は令和 3 年 4 月 1 日より施行する。

附則

（施行期日）

この対策基準は令和 4 年 10 月 1 日より施行する。