# 地方独立行政法人大阪市博物館機構情報セキュリティ管理規程

平成31年４月１日
大阪市博物館機構規程第 85 号

## 第１章　総則

（趣旨）

第１条　この規程は、地方独立行政法人大阪市博物館機構（以下「機構」という。）情報システム及び情報システムにより処理される情報、情報通信ネットワーク及び情報通信ネットワークにより伝達される情報その他の機構が保有する情報資産に関する情報セキュリティの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　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 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。

(2) 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をいう。

(3) セキュリティポリシー　この規程及び第９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情報で電磁的記録媒体に記録されているものをいう。

(8) 情報システム　電子計算機、電気通信回線等により情報処理の業務を一体的に行う仕組みをいう。

(9) 情報通信ネットワーク　電子計算機を相互に接続するための通信網並びにこれを構成するハードウェア及びソフトウェアをいう。

（10）館等　機構の内部組織である、事務局、大阪市立美術館、大阪市立自然史博物館、大阪市立東洋陶磁美術館、大阪市立科学館、大阪歴史博物館をいう。

（11）課等　地方独立行政法人大阪市博物館機構公文書管理規程第２条第３項に規定する課等をいう。

（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、大阪市個人情報の保護に関する法律の施行等に関する条例（令和５年大阪市条例第５号）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。

## 第２章　情報セキュリティに係る体制

（最高情報セキュリティ責任者等の設置等）

第４条　機構に最高情報セキュリティ責任者を置き、副理事長をもって充てる。

２　機構に統括情報セキュリティ責任者を置き、事務局長をもって充てる。

３　最高情報セキュリティ責任者は、機構における情報セキュリティを総括し、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。

４　統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐する。

（館等情報セキュリティ責任者の設置等）

第５条　事務局、大阪市立美術館、大阪市立自然史博物館、大阪市立東洋陶磁博物館、大阪市立科学館、大阪市立大阪歴史博物館、大阪中之島美術館準備室（以下「館等」という）における情報セキュリティ対策の適正な実施を推進するため、館等に館等情報セキュリティ責任者を置く。

２　館等情報セキュリティ責任者は、館長及び事務局長等をもって充てる。

３　館等情報セキュリティ責任者は、最高情報統括責任者の命を受け、館等における情報セキュリティ対策の実施その他館等における情報セキュリティに関する事務を掌理する。

（情報セキュリティ責任者の設置等）

第６条　課等において取り扱う情報資産の適切な管理を図るため、課等に情報セキュリティ責任者を置く。

２　情報セキュリティ責任者は、課等の課長（担当課長を含む）をもって充てる。

３　情報セキュリティ責任者は、課等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、情報通信ネットワークの利用状況等を把握し、課等において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指導、助言又は調整を行う。

４　情報セキュリティ責任者は、館等情報セキュリティ責任者の命を受けて、その所管に係る情報資産に関し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。

（情報セキュリティに係る連絡調整体制）

第７条　最高情報セキュリティ責任者は、情報セキュリティ対策の実施について館等相互間の連絡調整を行う。

２　館等情報セキュリティ責任者は、前項の規定に準じて、館等における情報セキュリティに関する連絡体制を構築し、館等における情報セキュリティ対策の実施について連絡調整を行う。

## 第３章　情報セキュリティ対策

（情報資産の分類）

第８条　館等情報セキュリティ責任者は、館等が保有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９条　最高情報セキュリティ責任者は、機構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。

（情報セキュリティ実施手順の作成）

第10条　館等情報セキュリティ責任者は、その所管する情報システム又は情報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、情報セキュリティ実施手順を作成し、最高情報セキュリティ責任者の承認を得なければならない。

（ソフトウェアライセンスの管理）

第10条の２　館等情報セキュリティ責任者は、館等において使用するソフトウェアのライセンス（当該ソフトウェアに係る使用許諾契約により認められた当該ソフトウェアを使用する権利をいう。以下「ソフトウェアライセンス」という。）を適切に管理しなければならない。

２　館等情報セキュリティ責任者は、ソフトウェアライセンスの管理状況を適宜調査し、その内容を定期的に最高情報セキュリティ責任者に報告しなければならない。

３　最高情報セキュリティ責任者は、前項の規定による報告を受けた場合において、必要があると認めるときは、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。

４　ソフトウェアライセンスの管理の方法その他必要な事項は、最高情報セキュリティ責任者が定める。

（業務の委託）

第11条　館等情報セキュリティ責任者は、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セキュリテ

ィ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12条　情報セキュリティ責任者は、館等が保有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、その状況を調査するとともに、当該事故の内容を館等情報セキュリティ責任者に報告しなければならない。

２　館等情報セキュリティ責任者は、前項の規定による報告を受けたときは、直ちに、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最高情報セキュリティ責任者に報告しなければならない。

３　最高情報セキュリティ責任者は、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。

## 第４章　検証及び見直し

（情報セキュリティ検査の実施）

第13条　最高情報セキュリティ責任者は、機構において情報セキュリティポリシーが遵守され、情報セキュリティ対策が適切かつ確実に実施されているかどうかを検証するため、定期的に検査を実施しなければならない。

２　最高情報セキュリティ責任者は、前項に規定する検査のほか、必要と認めるときは随時に検査を行うことができる。

３　最高情報セキュリティ責任者は、前２項に規定する検査（以下「情報セキュリティ検査」という。）の結果に基づき、必要があると認めるときは、講ずべき改善措置の内容を定めなければならない。

４　館等情報セキュリティ責任者は、前項の規定により最高情報セキュリティ責任者が定める改善措置を適切かつ確実に実施しなければならない。

５　情報セキュリティ検査の実施方法その他必要な事項は、最高情報セキュリティ責任者が定める。

（見直しの実施）

第14条　最高情報セキュリティ責任者は、情報セキュリティをめぐる情勢の動向、変化等を勘案し、及び情報セキュリティ検査の結果を踏まえ、適宜情報セキュリティポリシーに検討を加え、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　館等情報セキュリティ責任者は、前項の規定に準じて、情報セキュリティ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。

## 第５章　データ管理

（データの管理）

第15条　館等情報セキュリティ責任者は、データの取扱いに当たっては、漏えい、滅失、

き損、改ざん並びに不正な利用及び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、最高情報セキュリティ責任者が定める。

## 第６章　雑則

（施行の細目）

第16条　この規程の施行に関し必要な事項は、最高情報セキュリティ責任者が定める。

附　則

（施行期日）

１　この規程は平成 31 年４月１日から施行する。

附　則

（施行期日）

１　この規程は、令和８年４月１日から施行する。

# 地方独立行政法人大阪市博物館機構情報セキュリティ対策基準

## 1　目的

この地方独立行政法人大阪市博物館機構情報セキュリティ対策基準（以下「対策基準」という。）は、地方独立行政法人大阪市博物館機構情報セキュリティ管理規程（以下「規程」という。）第９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さまざまな脅威から守り、機密性、完全性及び可用性(注) を維持することによって、法人の運営サービスを安全に提供し、もって法人の円滑な運営に対する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(ISO7498-2：1989)

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　定義

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ほか、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。

(1)　CISO

最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）をいう。

(2)　システム管理者

項番６の情報システムに係る管理体制・役割に規定する業務管理者、サーバ等管理者及び端末機管理者をいう。

(3)　ネットワーク管理責任者

項番６のネットワークに係る管理体制・役割に規定する機構情報通信ネットワーク管理責任者及び館等情報通信ネットワーク管理責任者をいう。

(4)　職員

地方独立行政法人大阪市博物館機構に勤務するすべての者。

(5)　端末機

パソコンやモバイル端末等の機器をいう。

(6)　情報セキュリティインシデント

情報セキュリティに関する問題として捉えられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。

(7)　標的型攻撃

明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

(8)　機構情報通信ネットワーク

機構において共通の基盤となる情報通信ネットワークをいう。

(9)　館等情報通信ネットワーク

館等における業務運営のための独自のネットワークをいう。

(10)　機構内情報ネットワーク

全館に情報の共有及び活用を行うためのネットワークをいう。

(11)　外部接続集約ネットワーク

業務システム所管課が独自に運用・整備するモバイルワーク端末等に対してインターネットへの接続サービスを提供するネットワークをいう。

(12)　電磁的記録媒体

法人が業務上必要のため調達した USB メモリ、光学メディア、外付けハードディスク等の電磁的方式で作られた記録に係る記録媒体をいう。

3　適用範囲

この対策基準の適用範囲は、館等の職員及び館等の保有する情報資産のうち、情報システム化に関するもの及び最高情報セキュリティ責任者が必要と認めたものとする。

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)　大規模・広範囲にわたる疾病による要員不足に伴う情報システム運用の機能不全等

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)　組織・体制及び役割・責任

機構の情報資産について、全館的な組織・体制及び役割・責任に基づき情報セキュリティ対策を行う。

(2)　情報資産の分類と管理

機構の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て分類し、当該分類に基づき情報セキュリティ対策を行う。

(3)　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。

(4)　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。

(5)　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)　運用

情報システムの監視、情報セキュリティポリシー（以下「ポリシー」という。）の遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じるものとする。

(7)　業務委託とクラウドサービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者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。

クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。

(8)　評価及び見直し

点検・評価を実施し運用改善を行い、必要に応じて適宜ポリシーの見直しを行う対策を講じるものとする。

6　組織・体制及び役割・責任

(1)　館等の情報セキュリティに係る管理体制・役割

規程第４条から第６条に基づき、館等の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　CISO

CISO は、館等における情報セキュリティを総括し、館等情報セキュリティ責任者に対し、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。

②　統括情報セキュリティ責任者

統括情報セキュリティ責任者は、CISO の命を受けて、以下の情報セキュリティに関する必要な措置を行う。

ア　館等情報セキュリティ責任者、情報セキュリティ責任者、システム管理者、ネットワーク管理責任者に対する情報セキュリティに関する指導及び助言を行う。

イ　機構の情報資産に対するセキュリティインシデントが発生した場合又はセキュリティインシデントのおそれがある場合の必要かつ十分な措置を行う。

ウ　機構の情報資産に関する情報セキュリティ実施手順（以下「実施手順」という。）の維持・管理を行う。

エ　緊急時等の円滑な情報共有を図るための緊急連絡網の整備を行う。

オ　緊急時の CISO への早急な報告及び回復のための対策を行う。

カ　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の適時把握、必要に応じた CISO への内容報告を行う。

②　館等情報セキュリティ責任者

館等情報セキュリティ責任者は、情報セキュリティに関する連絡体制の構築並びに職員に対するポリシーの遵守に関する指導、助言及び研修その他館等における情報セキュリティの確保のために必要な措置を行う。

④　情報セキュリティ責任者

情報セキュリティ責任者は、規程第 6 条第 3 項及び第 4 項の規定に基づき、必要な措置を行う。

ア　情報セキュリティ責任者は、職員に対するポリシーの遵守に関する指導、助言又は研修その他情報セキュリティの確保のために必要な措置を行う。

イ　情報セキュリティ責任者は、前項の役割を達成するために、館等情報セキュリティ責任者の許可を得て、その役割を補佐する副情報セキュリティ責任者をおくことができる。

(2)　情報システムに係る管理体制・役割

各情報システムの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　業務管理者

ア　業務管理者は、各情報システムに係る業務を所管する課等のリーダー又は情報セキュリティ責任者（以下「リーダー等」という。）をもって充てる。

イ　業務管理者は、所管する情報システムの開発及び運用、保守の実施並びに管理を担う。

ウ　業務管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

エ　業務管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

オ　業務管理者は、情報システムの運用を開始しようとするときは、サーバ等管理者と協議し、運用管理の体制並びに業務の運用形態・計画及び当該システムに係るハードウェア・ソフトウェアの運用管理の方法等を定めなければならない。

カ　業務管理者は、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、帳票の出力等に至る業務全体の実施状況を把握・管理するとともに、適時、サーバ等管理者と協議し、システムの保守を適切に実施しなければならない。

②　サーバ等管理者

ア　サーバ等管理者は、システムの稼働管理（死活監視、媒体交換等）を担い、システムに係るサーバ等を設置する課等のリーダー等をもって充てる。

イ　サーバ等管理者は、システムの運用計画並びに実施手順等に基づき、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　端末機管理者

ア　端末機管理者は、円滑に業務処理が実施されるようシステムの利用管理を担い、当該システムに係る端末機を設置する課等のリーダー等をもって充てる。

イ　端末機管理者は、システムの利用者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。）並びに実施手順等に基づき、安全性に十分配慮し適切な利用が行われるよう、端末機の運用管理を行わなければならない。

(3)　ネットワークに係る管理体制・役割

機構通信ネットワーク及び館等通信ネットワークの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　機構情報通信ネットワーク管理責任者

機構情報通信ネットワーク管理責任者は、機構情報通信ネットワークの稼働状況及び障害の管理、ネットワーク上へのアクセス権限の設定など、ネットワークの運用管理を担い、統括情報セキュリティ責任者をもって充てる。

②　館等情報通信ネットワーク管理責任者

ア　館等情報通信ネットワーク管理責任者は、館等情報通信ネットワークの整備及び運用管理を担い、当該ネットワークに係る業務を所管する課等のリーダー等をもって充てる。

イ　館等情報通信ネットワーク管理責任者は、館等情報通信ネットワークを整備する場合、機構情報通信ネットワークに準じて、安全性及び信頼性を確保するための体制を定めなければならない。

ウ　館等情報通信ネットワーク管理責任者は、規程に基づき、館等情報通信ネットワークにおける実施手順を策定しなければならない。

③　情報セキュリティ責任者

情報セキュリティ責任者は、機構情報通信ネットワーク管理責任者、館等情報通信ネットワーク管理責任者及び施設を管理する者と連携を図り、館等におけるアクセス権限の管理、障害に関する連絡調整など、館等におけるネットワークの適切な運用管理を行う。

(4)　情報セキュリティに係る連絡調整体制

①　CSIRT（情報セキュリティに関する統一的な窓口）の設置・役割

ア　CISOは、CSIRT（Computer Security Incident Response　Team）を整備し、その役割を明確化しなければならない。

イ　CISO は、CSIRT を事務局に設置し、CISO を CSIRT 責任者とする。CSIRT 責任者は、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。

ウ　CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて館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。

③　館等相互間の連絡調整

CISO は、情報システム等の整備・運用に関する規程に規定する情報システム等整備・運用連絡調整会議において、情報セキュリティ対策の実施について館等相互間の連絡調整を行い、機構における情報セキュリティ対策の適切な管理を推進する。

③　館等における連絡体制

館等情報セキュリティ責任者は、館等における情報資産に関する情報セキュリティ対策に万全を期すため、情報セキュリティ対策の連絡体制を設置し、以下の関係者その他必要と認める者を随時招集し、館等における情報セキュリティ対策の実施について連絡調整を行う。

ア　情報セキュリティ責任者

イ　システム管理者

ウ　館等情報通信ネットワーク管理責任者

④　サイバー攻撃等侵害時における緊急連絡体制

CISO は、サイバー攻撃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おそれがある場合、緊急連絡体制を設置し、情報セキュリティに関する統一的な窓口を通じて、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。

ア　館等情報セキュリティ責任者

イ　情報セキュリティ責任者

ウ　ネットワーク管理責任者

⑤　クラウドサービス利用における組織体制

業務管理者は、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。

7　情報資産等の分類と管理

館等情報セキュリティ責任者は、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　データの分類

対象となるシステムのデータは、各々のデータの機密性、完全性、可用性を踏まえ、以下の重要性分類に従って分類し、重要性分類に従ったアクセス権限を適切に設定しなければならない。

| 重 要 性 分 類 |
|---|
| Ⅰ　個人情報及び業務上必要とする最小限の者のみが扱うデータ |
| Ⅱ　公開することを予定していないデータ及びセキュリティ侵害が事務の執行等に重大な影響を及ぼすデータ |
| Ⅲ　外部に公開するデータのうち、セキュリティ侵害が、本法人事務に影響を及ぼすデータ |
| Ⅳ　上記以外のデータ |

②　情報資産の管理責任

ア　管理責任

館等情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

イ　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。

ウ　重要性の効力

情報セキュリティ責任者は、データ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①の分類に基づき管理しなければならない。

③　クラウドサービスの環境に保存される情報資産

館等情報セキュリティ責任者は、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①の分類に基づき管理しなければならない。

④　データの作成

ア　職員は、業務上必要のないデータを作成してはならない。

イ　データを作成する者は、データの作成時に①の分類に基づき、当該データの重要性分類を定めなければならない。

ウ　データを作成する者は、作成途上のデータについても、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、データの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。

⑤　データの入手

ア　他の課等が作成したデータを入手した者は、入手元の重要性分類に基づいた取扱いをしなければならない。

イ　外部の者が作成したデータを入手した者は、①の分類に基づき、当該データの重要性分類を定めなければならない。

ウ　データを入手した者は、入手したデータの重要性分類が不明な場合、情報セキュリティ責任者に判断を仰がなければならない。

⑥　情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ　情報資産を利用する者は、電磁的記録媒体、ドキュメント等の情報資産に記録されたデータの重要性分類に応じ、適正な取扱いをしなければならない。

ウ　情報資産を利用する者は、電磁的記録媒体に重要性分類が異なるデータが複数記録されている場合、最高度の重要性分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑦　電磁的記録媒体等の管理

ア　情報セキュリティ責任者は、データを記録した電磁的記録媒体を長期保管する場合は、必要に応じて書込禁止の措置を講じなければならない。

イ　情報セキュリティ責任者は、データの重要性が容易に識別できるよう、ファイルが格納された記録媒体等の保管について台帳整備し、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、ファイルのバックアップを定期的に取得するよう努め、所定の場所において適切に管理しなければならない。さらに、外付けハードディスクや外付けSSD等のサーバ、パソコン等の端末機の外に置きケーブル等で接続するタイプの記憶装置（以下「外付けハードディスク等」という。）の場合は、これら外付けハードディスク等の現物と台帳に記録された識別番号について定期的に照合点検しなければならない。

⑧　データの送信

ア　外部ネットワークを利用し、本法人以外のものと、電子メール等により重要性分類Ⅱ以上のデータを送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

イ　重要性分類Ⅱ以上のデータをメールにより取り扱う必要がある者は、情報セキュリティ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取の確認を行う等、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、上記の取扱いに準じ、適切に運用を行わなければならない。

⑨　データの運搬

ア　重要性分類Ⅱ以上のデータを法人外へ持ち出す者は、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設定を行う等、データ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。

イ　情報セキュリティ責任者は、データが格納された記録媒体等の授受について台帳整備しなければならない。また、データを搬送するときは、データの漏えい、滅失、き損、改ざん等を防止するため適切な措置を講じなければならない。

⑩　情報資産の管理及び取扱い

情報セキュリティ責任者は、情報資産の管理については、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）、大阪市個人情報の保護に関する法律の施行等に関する条例（令和5年大阪市条例第5号。以下「個人情報保護条例」という。）その他の関連する法令等及び規程に基づき、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。

⑪　情報資産の廃棄等

ア　情報資産を廃棄する者は、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わなければならない。

イ　情報資産を廃棄する者は、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。

ウ　ファイルが格納された電磁的記録媒体等の廃棄を行う者は、情報セキュリティ責任者の許可を得なければならない。ただし、システムに関するものである場合は、システム管理者の許可を得なければならない。

エ　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。

## 8　物理的セキュリティ

### サーバ等の管理

①　機器の取付け

サーバ等管理者は、サーバ等の機器の取付けを行う場合、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、震災時の転倒又は盗難の防止のため、適切に固定する、施錠する等必要な措置を講じなければならない。

③　サーバ等の冗長化

サーバ等管理者は、保護データを取り扱い、かつ、システムの停止によって、法人の業務運営等に大きな影響を及ぼす可能性があるシステム（以下「重要システム」という。）のサーバ等の機器については、原則として冗長化を図り、メインサーバに障害が発生した場合には速やかにセカンダリサーバで対応を行えるようにするなど、システム運用が停止しない措置を講じなければならない。

③　サーバ等の機種更新

サーバ等管理者は、サーバ等の機種更新を行おうとする時、特に並行稼働時においては、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、容量並びに現時点での設備の残存能力、容量を把握し、適切な対応を講じなければならない。

④　機器の電源

ア　サーバ等管理者は、業務要件やシステムの特性に応じて、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　サーバ等管理者は、業務要件やシステムの特性に応じて、落雷等による過電流に対して、サーバ等の機器や主要なネットワーク機器を保護するための措置を講じなければならない。

⑤　通信ケーブル等の配線

ア　業務管理者及びネットワーク管理責任者は、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講じなければならない。

イ　業務管理者及びネットワーク管理責任者は、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。なお、施設管理部門から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。

ウ　業務管理者及びネットワーク管理責任者は、主要なネットワーク機器（ハブ、ルータ等）及び配線を管理者以外の者が容易に操作できないような場所に格納又は設置する等適正に管理しなければならない。

⑥　機器の定期保守及び修理

ア　業務管理者及びネットワーク管理責任者は、機器の定期保守を実施するとともに、その記録を適切に保存しなければならない。

イ　業務管理者及びネットワーク管理責任者は、電磁的記録媒体を内蔵する機器を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、 業務管理者及びネットワーク管理責任者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約の締結を行わなければならない。

⑦　法人外への機器の設置

サーバ等管理者は、法人外にサーバ等の機器を設置する場合、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。

⑧　機器の廃棄等

ア　業務管理者及びネットワーク管理責任者は、電磁的記録媒体の含まれる機器を廃棄、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）をする者は、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。なお、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できる。

9　人的セキュリティ

(1)　職員の遵守事項

①　ポリシー等の遵守

職員は、ポリシー及び実施手順を遵守しなければならない。

② 業務以外の目的での使用の禁止

職員は、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を行ってはならない。

④ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

ア 業務管理者は、情報資産を法人外で処理する場合における安全管理措置を実施手順で定めなければならない。

イ 職員は、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、定められた場所以外に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。

ウ 職員は、情報セキュリティ責任者の許可なくして、端末機又は電磁的記録媒体等を執務室以外に持ち出してはならない。ただし、業務用パソコン貸与規程に定める業務用パソコンの持ち出しについて、次の事項を遵守する場合においては、この限りでない。

・持ち出し中は常時携行するなど、本人が責任をもって管理し、当日中に持ち帰ること
・持ち運ぶ前には業務用パソコン内にデータが保存されていないことを確認のうえ、ロック、ログオフ、またはシャットダウンを行うこと
・持ち出し先の会議室等において職員が不在になる場合、盗難防止のため施錠等による措置を講じること

エ 職員は、法人外で情報処理業務を行う場合には、情報セキュリティ責任者の許可を得なければならない。

④ 貸与以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア 職員は、貸与以外の端末機及び電磁的記録媒体等（以下、「私物端末機等」という。）を原則業務に利用してはならない。ただし、業務上必要な場合は、館等情報セキュリティ責任者の許可を得て利用することができる。

イ 職員は、私物端末機等を用いる場合には、館等情報セキュリティ責任者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤ 持ち出し及び持ち込みの記録

情報セキュリティ責任者は、端末機及び電磁的記録媒体の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、端末機のソフトウェアに関するセキュリティ機能の設定を業務管理者の許可なく変更してはならない。

⑦ 机上の端末等の管理

職員は、使用する機器や電磁的記録媒体について、権限を有しない者に使用されること又は閲覧されることがないように、離席時の端末機のロックや容易に閲覧されない場所での使用等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

職員は、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

職員は、クラウドサービスの利用にあたってもポリシーを遵守し、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 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、ウェブで利用できるフリーメール、ネットワークストレージサービス等について、許可されたサービス以外は使用してはならない。ただし、情報セキュリティ責任者が業務上、必要と判断した場合を除く。

⑪　ポリシー等の掲示

情報セキュリティ責任者は、職員が常にポリシー及び実施手順を閲覧できるように掲示しなければならない。

⑫　委託事業者に対する説明

業務管理者及びネットワーク管理責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、ポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を周知しなければならない。

(2)　研修・訓練

①　情報セキュリティに関する研修・訓練

ア　CISO は、定期的に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。

イ　CISO は、定期的にクラウドサービスを利用する職員の情報セキュリティに関する意識向上、教育を実施するとともに、委託先を含む関係者については委託先等で教育が行われていることを確認しなければならない。

②　研修計画の策定及び実施

ア　CISO は、幹部を含め全ての職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

イ　研修計画において、職員が毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

ウ　新規採用の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、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

オ　CISO は、研修の実施状況を分析、評価して、情報セキュリティの更なる改善に努めなければならない。

③　ポリシー等の啓発

ア　CISO は、情報システム等整備・運用連絡調整会議等において、ポリシーの周知徹底を行わなければならない。また、研修等の機会を利用して、情報セキュリティの啓発に努めなければならない。幹部を含め全ての職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

イ　館等情報セキュリティ責任者は、館等における情報セキュリティの連絡体制を利用し、情報セキュリティ責任者その他必要と認める者に対し、ポリシー及び実施手順の周知徹底を行わなければならない。また、館等が実施する研修等により、所属員に対しポリシー及び実施手順の遵守について啓発しなければならない。

ウ　情報セキュリティ責任者は、所属職員がポリシー及び実施手順について理解し、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。

④　情報システムに係る情報セキュリティの徹底

業務管理者は、研修の実施等により、システムの運用に関わる職員を対象に、システム及び当該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の実施手順並びに実施に必要な知

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。

⑤　ネットワークに係る情報セキュリティの徹底

機構情報通信ネットワーク管理責任者は情報セキュリティ責任者、その他必要と認める者に対し、ネットワークにおける実施手順並びに実施に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。

⑥　緊急時対応訓練

CISO は、標的型攻撃への対応を想定した訓練を実施しなければならない。訓練計画は、ネットワークの規模等を考慮し、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。

⑦　研修・訓練への参加

職員は、定められた研修・訓練に参加しなければならない。

(3)　情報セキュリティインシデントに対する報告

①　発生した所管（インシデント発生部門）の速やかかつ主体的な対応

ア　職員は、システムの利用に際して情報セキュリティインシデントを発見した場合又は外部等から通報を受けた場合は、速やかに端末機管理者に報告しなければならない。

イ　職員は、ネットワークの利用に際して情報セキュリティインシデントを発見した場合は、速やかにネットワーク管理責任者に報告しなければならない。

ウ　職員は、システム管理者又はネットワーク管理責任者の指示に従い、情報セキュリティインシデントに対し適切に対処しなければならない。

エ　職員は、情報セキュリティインシデントを発見した場合又は外部等から通報を受けた場合、情報セキュリティ責任者に報告しなければならない。

(4)　ＩＤ及びパスワード等の管理

①　ＩＤの取扱い

職員は、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。

・自己が利用しているＩＤは、他人に利用させてはならない。

・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。

②　パスワードの取扱い

職員は、アクセス権限に係る情報を適切に管理し、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。

・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

・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。

・パスワードは十分な長さ（最低８文字以上とする。）とし、文字列は想像しにくいものにしなければならない。

・パスワードが流出したおそれがある場合には、端末機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。

・複数の情報システムを扱う職員は、必要でない限り同一のパスワードをシステム間で用いてはならない。

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

・サーバ、ネットワーク機器及びパソコン等の端末機等にパスワードを記憶させてはならない。

・職員間でパスワードを共有してはならない（ただし、共用ＩＤに対するパスワードは除く）。

③　パスワードの管理

業務管理者は、職員のパスワードに関する情報を厳重に管理しなければならない。

10　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

①　バックアップの実施

ア　業務管理者及びサーバ等管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

イ　業務管理者は、バックアップコピーを取得するデータ、取得の方法及びサイクルを定めサーバ等管理者は、それに基づいてデータのバックアップを適切に実施しなければならない。

ウ　サーバ等管理者は、プログラムの変更の都度、プログラムのバックアップコピーを取得しなければならない。

エ　サーバ等管理者は、データのバックアップ取得後、次のデータのバックアップ取得までの間、必要に応じて、データベースの更新記録情報を取得しなければならない。

オ　業務管理者は、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、その機能の仕様が本法人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を行わなければならない。

②　システム管理記録及び作業の確認

ア　業務管理者は、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　業務管理者は、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　業務管理者又は情報システム担当者及び契約により操作を認められ委託事業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。

③　情報システムの設計書等の管理

業務管理者は、ネットワーク構成図、情報システム設計書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

④　ログの取得等

ア　業務管理者、サーバ等管理者及びネットワーク管理責任者は、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。また、窃取、改ざん、消去されないように必要な措置を講じなければならない。

イ　業務管理者及びネットワーク管理責任者は、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　業務管理者、サーバ等管理者及びネットワーク管理責任者は、取得したログを定期に又は随時に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。

⑤　障害記録

業務管理者及びネットワーク管理責任者は、職員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、障害記録として記録し、適正に保存しなければならない。

⑥　ネットワークの接続制御、経路制御等

ア　ネットワーク管理責任者は、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。

イ　ネットワーク管理責任者は、ネットワークの機密保護を図るため、当該ネットワークへアクセスが可能な利用者及びその利用範囲等アクセス権限を定めなければならない。

ウ　ネットワーク管理責任者は、ネットワーク設定情報について不正に変更されないよう、アクセス管理を行うとともに、障害時等に備え、設定情報のバックアップを確保しなければならない。また、ネットワーク構成等に関する情報は、関係者以外に開示してはならない。

エ　ネットワーク管理責任者は、ネットワーク上の通信利用状況並びにネットワーク設計の稼働実績及び資源の利用状況を把握するとともに、障害箇所の検知機能を備え、ネットワークの性能改善に向け必要な措置を講じる等、ネットワークを適正な稼働状況に保たなければならない。

オ　ネットワーク管理責任者は、ネットワーク利用に大きな支障を生じさせかねない大容量のファイルの通信を制限する等、ネットワークの円滑な利用を図っていかなければならない。

カ　ネットワーク管理責任者は、本法人情報通信ネットワーク又は館等情報通信ネットワークに接続するサーバ及び端末機等機器を特定する識別記号を設定・配付し、ネットワークへの接続を適切に管理しなければならない。

キ　ネットワーク管理責任者は、情報セキュリティ責任者と連携し、サーバ及び端末機等機器を本法人情報通信ネットワーク又は館等情報通信ネットワークに不正に接続させることが無いよう、監視等を行わなければならない。

⑦　外部ネットワークとの接続制限等

ア　機構情報通信ネットワークに外部ネットワークを接続しようとするときは、ネットワーク管理要綱に従わなければならない。また、館等情報通信ネットワークに外部ネットワークを接続しようとするときは、館等情報通信ネットワーク管理責任者は、適切に実施及び管理を行わなければならない。

イ　ネットワーク管理責任者及びシステム管理者は、本法人情報通信ネットワーク及び館等情報通信ネットワーク並びにシステムを外部ネットワークと接続するときは、接続しようとする外部ネットワークに係るネットワーク構成、セキュリティレベル並びに法人内部のネットワーク及びシステムにおけるリスク等を詳細に検討し、必要な情報セキュリティ対策が講じられることを明確にし、法人内の全てのネットワーク、情報システム等の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。

ウ　業務管理者及びネットワーク管理責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、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処するため、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。

エ　業務管理者及びネットワーク管理責任者は、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、不要なサービスの停止等、必要な措置を講じなければならない。

オ　ネットワーク管理責任者は、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、

情報資産に脅威が生じることが想定される場合には、館等情報セキュリティ責任者及びCISOと協議のうえ、速やかに当該外部ネットワークを物理的に遮断しなければならない。

カ　業務管理者及びネットワーク管理責任者は、法人外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、法人外からネットワーク、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。

⑧　複合機のセキュリティ管理

ア　情報セキュリティ責任者は、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、サーバ等と同等にポリシーに準じた適正なセキュリティ対策を講じなければならない。

イ　情報セキュリティ責任者は、必要に応じて複合機が備えるパスワード設定や認証、ファクス誤送信防止、ハードディスクなどの記憶装置の暗号化等の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　情報セキュリティ責任者は、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。

⑨　IoT機器を含む特定用途機器のセキュリティ管理

業務管理者及びネットワーク管理責任者は、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。

⑩　無線 LAN 及びネットワークの盗聴対策

ア　業務管理者およびネットワーク管理責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

イ　業務管理者およびネットワーク管理責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑪　電子メールのセキュリティ管理

ア　ネットワーク管理責任者は、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。

イ　ネットワーク管理責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　ネットワーク管理責任者は、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。

エ　ネットワーク管理責任者は、職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員に周知しなければならない。

オ　ネットワーク管理責任者は、情報システムの開発や運用、保守等の委託事業者による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

⑫　電子メールの利用制限

ア　職員は、自動転送機能を用いて、外部へ電子メールを転送してはならない。ただし業務遂行上やむを得ない場合はネットワーク管理責任者の許可を得て行うことができる。

イ　職員は、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。

ウ　職員は、複数人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

ルアドレスが分からないようにしなければならない。

エ　職員は、重要な電子メールを誤送信した場合、情報セキュリティ責任者に報告しなければならない。

⑬　電子署名・暗号化

職員は、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を確保することが必要な場合には、電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

⑭　無許可ソフトウェアの導入等の禁止

ア　職員は、端末機に無断でソフトウェアを導入してはならない。

イ　職員は、業務上の必要がある場合は、業務管理者及び情報セキュリティ責任者等の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、CISO が定めたソフトウェアライセンス管理要綱に基づき、ソフトウェアのライセンスを管理しなければならない。

ウ　職員は、著作権法や使用許諾契約等に違反するソフトウェアの使用又は複製等を行ってはならない。

⑮　機器構成の変更の制限

ア　職員は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員は、業務上、端末機に対し機器の改造及び増設・交換を行う必要がある場合には、業務管理者及び情報セキュリティ責任者等の許可を得なければならない。

⑯　業務外ネットワークへの接続の禁止

ア　職員は、ネットワーク管理責任者の許可なく端末機または電磁的記録媒体を機構情報通信ネットワーク及び館等情報通信ネットワークに接続してはならない。

イ　職員は、貸与された端末を、有線・無線を問わず、その端末を接続して利用するようシステム管理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。

ウ　業務管理者及びネットワーク管理責任者は、貸与した端末について、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ことが望ましい。

⑰　業務以外の目的でのウェブ閲覧の禁止

ア　職員は、業務以外の目的でウェブを閲覧してはならない。

イ　機構情報通信ネットワーク管理責任者は、職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、当該職員が属する館等の情報セキュリティ責任者に通知し適切な措置を講じなければならない。また、機構情報通信ネットワーク管理責任者は、機構内情報ネットワークの利用に当たり、業務目的以外のインターネットへのアクセス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。

⑱　Web 会議サービスの利用時の対策

ア　統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

イ　職員は、本法人の定める利用手順に従い、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しなければならない。

ウ　職員は、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じなければならない。

⑲　ソーシャルメディアサービスの利用

ア　情報セキュリティ責任者は、本法人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、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

・本法人のアカウントによる情報発信が、実際の本法人のものであることを明らかにするために、本法人の自己管理ウェブ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。

・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　重要性分類Ⅱ以上のデータはソーシャルメディアサービスで発信してはならない。ただし、身体人命に危険が及ぶ可能性が高い事業において緊急性を要する場合を除く。

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　可用性が求められる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、本法人の自己管理 Web サイトに当該情報を掲載して参照可能としなければならない。

(2)　アクセス制御等

①　アクセス制御

ア　業務管理者は、所管するシステムの機密保護を図るため、当該システムの利用課等の長に協議し当該システムへアクセスが可能な利用者及びその利用範囲等アクセス権限を明確にし、設定しなければならない。業務管理者は、アクセス権限を機構情報通信ネットワーク又は館等情報通信ネットワーク上に設定しようとするときは、ネットワーク管理責任者に協議しなければならない。

イ　業務管理者及びネットワーク管理責任者は、システム及びネットワークへのアクセス権限については、ユーザＩＤ及びパスワードにより管理を行うことを基本とし、取り扱う情報の重要度に応じてパスワード以外にＩＣカード認証・生体認証等を併用した二要素認証を適用しなければならない。

②　利用者ＩＤの取扱い

ア　業務管理者及びネットワーク管理責任者は、利用者ＩＤ及びパスワードについて、当該システムを利用する課等のリーダー等に協議し、次の事項を定めなければならない。

・利用者ＩＤ及びパスワードの付与及び削除手続き

・利用者ＩＤの保管方法

・パスワードの守秘義務

・パスワードの変更時の管理方法

・その他業務管理者及びネットワーク管理責任者が必要と認める事項

イ　業務管理者及びネットワーク管理責任者は、職員は、業務上必要がなくなった場合は、利用者登録を抹消しなければならない。

ウ　業務管理者及びネットワーク管理責任者は、利用されていないＩＤが放置されないよう、点検しなければならない。

③　特権を付与されたＩＤの管理等

ア　業務管理者及びネットワーク管理責任者は、管理者権限等の特権を付与された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　業務管理者又はネットワーク管理責任者の特権を代行する者は、業務管理者又はネットワーク管理責任者が指名し、情報セキュリティ責任者が認めた者でなければならない。

ウ　業務管理者及びネットワーク管理責任者は、特権を付与されたＩＤ及びパスワードについて、一般利用者のユーザＩＤ及びパスワードよりもセキュリティ機能を強化しなければならない。

エ　業務管理者及びネットワーク管理責任者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

③　職員による外部からのアクセス等の制限

ア　職員が法人外から機構情報通信ネットワーク、館等情報通信ネットワーク又は内部のシステムにアクセスする場合は、業務管理者及びネットワーク管理責任者の許可を得なければならない。

イ　業務管理者及びネットワーク管理責任者は、機構情報通信ネットワーク、館等情報通信ネットワーク又は内部のシステムに対する法人外からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ　業務管理者及びネットワーク管理責任者は、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。

エ　ネットワーク管理責任者は、法人外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。

オ　業務管理者は、法人外からのアクセスに利用する端末機を職員に貸与する場合、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。

カ　職員は、法人外から持ち込んだ又は持ち帰った端末機等を本法人のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ責任者の許可を得なければならない。

キ　業務管理者及びネットワーク管理責任者は、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として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者のＩＤ、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報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。

⑤　ウイルス感染等への対応

ア　ネットワーク管理責任者及び業務管理者は、ウイルス感染またはその予兆を発見したときは、影響範囲及び感染経路等を調査し、ウイルスの駆除等必要な対策を速やかに講じなければならない。

イ　ネットワーク管理責任者及び業務管理者は、ウイルスによりネットワーク及びシステム等情報資産に影響が生じたときは、侵害時の対応に基づき必要な措置を講じなければならない。

⑥　自動識別の設定

業務管理者及びネットワーク管理責任者は、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システムを設定することが望ましい。

⑦　ログイン時の表示等

業務管理者及びネットワーク管理責任者は、システム及びネットワークへのアクセス権限の把握、管理を適切に行わなければならない。また、ログインにおいて、正しくない操作が繰り返しなされた場合、ロックをかける等アクセスの制御を行わなければならない。

⑧　認証情報の管理

ア　業務管理者及びネットワーク管理責任者は、職員等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　業務管理者は、職員に対してパスワードを発行する場合は、仮のパスワードを発行し、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　業務管理者及びネットワーク管理責任者は、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。

⑨　特権による接続時間の制限

業務管理者は、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。

(3)　システム開発、導入、保守等

①　情報システムの調達

ア　業務管理者は、情報システム開発、導入、保守等の調達に当たっては、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　業務管理者は、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。

②　情報システムの導入

ア　業務管理者は、開発環境と運用環境の分離及び移行手順の明確化に関し、次の事項を遵守しなければならない。

・システム開発、保守及びテスト環境と本番のシステム運用環境を分離しなければならない。

・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。

・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。

・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。

イ　業務管理者は、テストに関し、次の事項を遵守しなければならない。

・新たに情報システムを導入する場合、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。

・運用テストを行う場合、あらかじめ開発、保守環境環による操作確認を行わなければならない。

・個人情報及び機密性の高いデータを、テストデータに使用してはならない。

③　システム開発・保守に関連する資料等の整備・保管

ア　業務管理者及びサーバ等管理者は、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　業務管理者及びサーバ等管理者は、テスト結果を一定期間保管しなければならない。

④　情報システムにおける入出力データの正確性の確保

ア　業務管理者は、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　業務管理者は、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　業務管理者は、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。

エ　業務管理者は、ウェブサイトを構築する場合は、予め定めたドメイン名の使用を調達仕様書に含め、そのドメインで当該ウェブサイトを運用しなければならない。また、当該ドメインを廃止する際に、廃止されるドメイン上で運用停止に関する案内を行い、当該ドメインの運用停止後も１年以上当該ドメインを保持し続ける等、第三者の組織が当該ドメインを早期に取得することを避けるよう対策を講じた上で、廃止手続を行わなければならない。

⑤　情報システムの変更管理

業務管理者及びサーバ等管理者は、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。

⑥　システム更新又は統合時の検証等

業務管理者及びサーバ等管理者は、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 。

⑦　機構情報通信ネットワークを利用したシステムの導入

業務管理者及びサーバ等管理者は、機構情報通信ネットワークを利用したシステムを導入しようとするときは、機構情報通信ネットワーク管理責任者に協議し、ネットワークへの接続テストを行うとともに、アクセス権限を明確にし、アクセスの管理等に関する事項を定めなければならない。

⑧　システムの保守における不具合の確認

業務管理者及びサーバ等管理者は、システムの保守を行うときは、不具合の確認を行い、既存のシステムの運用に影響が出ないようにしなければならない。

(4)　不正プログラム対策

①　ネットワーク管理責任者の措置事項

ア　外部のネットワークから受信したファイルは、インターネットのゲートウェイにおいてにコンピュータウイルス等の不正プログラムのチェックを行うなど、不正プログラムのネットワークやシステムへの侵入を防止しなければならない。

イ　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ　所管するサーバ及び端末機に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

エ　システムがインターネットに接続している場合、不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つように努めなければならない。

オ　不正プログラム対策のソフトウェアは、常に最新の状態に保つように努めなければならない。

カ　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、貸与以外の電磁的記録媒体を職員に利用させてはならない。また、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

キ　端末機に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない

ク　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利用してはならない。また、当該製品の利用を予定している期間中にパッチ

やバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

ケ　仮想マシン（仮想化技術を利用してコンピュータ内に疑似的に再現されたもうひとつのコンピュータ）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。

②　業務管理者の措置事項

ア　所管するサーバ及び端末機に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

イ　システムがインターネットに接続している場合、不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つように努めなければならない。

ウ　不正プログラム対策のソフトウェアは、常に最新の状態に保つように努めなければならない。

エ　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、貸与以外の電磁的記録媒体を職員に利用させてはならない。また、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

オ　端末機に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない

カ　不正プログラム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、システム管理者が許可した職員を除く職員に当該権限を付与してはならない。

③　職員の遵守事項

ア　端末機において、不正プログラム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てはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、開かず速やかに削除しなければならない。

エ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

オ　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更など次の事項を実施しなければならない。

・パソコン等の端末の場合、LAN ケーブルの即時取り外しを行わなければならない。

・モバイル端末の場合、直ちに利用を中止し、通信を行わない設定への変更又はシャットダウンを行わなければならない。

④　専門家の支援体制

CISO 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、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

①　業務管理者及びネットワーク管理責任者の措置事項

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ウェブページの改ざんを防止するために、データの書換えを検出し、実施手順等に準じた連絡体制に基づき通報するよう、設定することが望ましい。

エ　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査することが望ましい。

②　館等情報セキュリティ責任者の措置事項

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。

③　不正アクセス等発見時の対応

ア　ネットワーク管理責任者及び業務管理者は、不正アクセスによる攻撃を受け、ネットワーク及び情報システム等情報資産に影響が生じたときは、別途定める侵害時の対応に基づき適切な措置を講じなければならない。

イ　ネットワーク管理責任者及び業務管理者は、攻撃の予告等により攻撃を受けることが明確になった場合、情報システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

ウ　ネットワーク管理責任者及び業務管理者は、不正アクセスによるネットワーク及び情報システムへの攻撃を発見したときは、影響範囲及び侵入経路等の調査並びに攻撃の記録を保存し、必要な対策を速やかに講じなければならない。また、必要に応じて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。

④　内部からの踏み台攻撃への対策

業務管理者及びネットワーク管理責任者は、職員及び委託事業者が使用しているパソコン等の端末からの法人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。

⑤　職員による不正アクセス

業務管理者及びネットワーク管理責任者は、職員による不正アクセスを発見した場合は、当該職員が属する課等の情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

⑥　サービス不能攻撃への対策

業務管理者及びネットワーク管理責任者は、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。

⑦　標的型攻撃への対策

業務管理者及びネットワーク管理責任者は、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。

(6)　セキュリティ情報の収集

①　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

業務管理者、サーバ等管理者及びネットワーク管理責任者は、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。

②　不正プログラム等のセキュリティ情報の収集・周知

業務管理者、サーバ等管理者及びネットワーク管理責任者は、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、職員に周知しなければならない。

③　情報セキュリティに関する情報の収集及び共有

業務管理者、サーバ等管理者及び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、必要に応じて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。

11　運用

(1)　情報システム等の適正運用

①　実施手順の作成

ア　業務管理者は、ポリシーに基づき、当該システム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た実施手順を作成し、館等情報セキュリティ責任者の承認を得なければならない。

イ　ネットワーク管理責任者は、ポリシーに基づき、当該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た実施手順を作成し、館等情報セキュリティ責任者の承認を得なければならない。

ウ　館等情報セキュリティ責任者は、当該実施手順について CISO に承認を得なければならない。

②　運用管理手法、運用計画の明確化

ア　業務管理者は、システムの運用を開始する前に、運用管理の手法及び体制等について明らかにしなければならない。

イ　サーバ等管理者は、システムの運用に当たり、業務管理者と協議し、運用計画を策定し、年間・月間・週間等における運用スケジュール及びシステムの運用時間及び運用形態等運用管理に必要な事項を明確にしなければならない。

ウ　ネットワーク管理責任者は、ネットワークの運用に当たり、運用管理の手法及び体制、運用計画を明らかにしなければならない。

③　情報システムにおける機器操作の適正化

ア　情報システムのサーバ等の機器についてはサーバ等管理者、また端末機については端末機管理者が、それぞれ指示若しくは承認した者が操作を行わなければならない。

イ　業務管理者及びサーバ等管理者は、操作マニュアル等を作成し、研修を実施する等機器操作の適正化に努めなければならない。また、システムの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

④　ネットワークにおける機器操作の適正化

ア　ネットワーク機器の操作については、ネットワーク管理責任者が指示若しくは承認した者が行わなければならない。

イ　ネットワーク管理責任者は、操作マニュアル等を作成する、又は利用方法の周知を行う等ネットワークの利用の適正化に努めなければならない。また、ネットワークの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

⑤　情報システム等の監視

ア　重要システムの運用に当たっては、サーバ等管理者は、セキュリティに関する事案を検知するため 、情報システムを常時監視しなければならない。

イ　サーバ等管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

ウ　重要システムの運用に当たっては、サーバ等管理者は、不正なアクセスによる攻撃を検知するため、外部と常時接続するシステムを常時監視しなければならない。

エ　ネットワークに係る情報セキュリティに関する事案を検知するため、ネットワーク管理責任者は、ネットワークの稼働監視を行わなければならない。特に、外部と接続する機構情報通信ネットワークについては、ファイアウォール、侵入監視装置等を用い、不正なアクセスによる攻撃を受けていないかどうか監視、分析を行わなければならない。

オ　監視により得られた結果については、消去や改ざんされないために必要な措置を講じ、定期的に安全な場所に保管しなければならない。

⑥　運用障害に対する予防措置

ア　業務管理者は、情報システム及びネットワークに障害又は侵害が発生し、システムが利用できない場合に備え、法人運営への影響を最小限に抑えるため、代替処理方法を定めなければならない。

イ　情報システムに被害が生じるおそれがある事案を発見した場合、サーバ等管理者は、業務管理者と協議のうえ、予防措置を講じなければならない。また、サーバ等管理者及び業務管理者は、直ちに館等情報セキュリティ責任者に報告しなければならない。

ウ　館等情報セキュリティ責任者は、直ちに、当該事案をCISOに報告しなければならない。

エ　ネットワークに被害が生じるおそれがある事案を発見した場合、ネットワーク管理責任者は、予防措置を講じなければならない。また、ネットワーク管理責任者は、直ちに、当該事案をCISOに報告しなければならない。

⑦　クラウドサービス運用時の遵守事項

ア　業務管理者及びネットワーク管理責任者は、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しなければならない。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、業務が維持できるように努めなければならない。

イ　業務管理者及びネットワーク管理責任者は、(クラウドサービス利用者の活動、例外処理、過失及び情報セキュリティ事象等を記録した)イベントログ取得の範囲や保存期間等を定め、利用するクラウドサービスがその内容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しなければならない。

ウ　業務管理者及びネットワーク管理責任者は、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次の重要な操作に関して、手順化し、確認しなければならない。

・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
・クラウドサービス利用の終了手順
・バックアップ及び復旧

(2)　ポリシー等の遵守状況の確認

①　遵守状況の確認及び対処

ア　館等情報セキュリティ責任者は、館等において、ポリシー及び所管する情報資産に係る実施手順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CISOに報告しなければ

ならない。

イ　CISO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　ネットワーク管理責任者及び業務管理者は、ネットワーク及びサーバ等のシステム設定等におけるポリシー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切かつ速やかに対処しなければならない。

エ　CISO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、館等情報セキュリティ責任者に報告を求めることができる。

②　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

情報セキュリティ責任者は、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端末機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。

③　ポリシー違反を確認した場合の措置

職員のポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

・情報システムの利用者が違反を確認したときは、端末機管理者に報告し、端末機管理者は業務管理者及びサーバ等管理者に報告すること。また、情報システムの稼働又は運用に係る担当者が違反を確認したときは、サーバ等管理者及び業務管理者に報告すること。

・報告を受けた業務管理者は、館等情報セキュリティ責任者に報告すること。

・報告を受けた館等情報セキュリティ責任者は、適切な措置を行うこと。

・館等情報セキュリティ責任者の指導によっても改善されない場合、CISOは、当該職員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、CISOは、職員の権利を停止あるいは剥奪した旨を館等情報セキュリティ責任者に通知すること。

・ただし、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CISOが判断した場合において、CISOは、当該職員のネットワーク又はシステムを使用する権利を停止あるいは剥奪することができる。

(3)　情報システム等の障害時、侵害時の対応

①　障害時の対応

ア　情報システムにおける措置

(ｱ)　責任体制

業務管理者及びサーバ等管理者は、情報システムの障害時における連絡及び対処の責任者となり、関係者との連携により情報システムを速やかに回復しなければならない。

(ｲ)　障害時における対応方法の周知

業務管理者は、サーバ等管理者と協議し、情報システムの運用を開始する前に、障害時における対応マニュアルを作成し、関係者に周知しなければならない。

(ｳ)　障害時の連絡及び対処

a　端末機管理者は、障害を発見したときは、直ちに、業務管理者に連絡しなければならない。また、業務管理者は、必要に応じてこれをサーバ等管理者に連絡しなければならない。

b　サーバ等管理者は、情報システムの運用に障害を発見したときは、直ちに、障害状況及び影響範囲を調査するとともに、必要に応じて障害状況等を業務管理者に連絡しなければならない。また、業務管理者は、必要に応じてこれを障害に関係する端末機管理者に連絡しなければならない。

c　業務管理者及びサーバ等管理者は、障害に関係する端末機管理者と連携し、情報システムの回復に向け適切な措置を講じなければならない。

d　業務管理者及びサーバ等管理者は、障害・故障の発生に関係した部門から原因及び処理の

報告を求めるとともに、当該障害・故障の原因及び処理結果について障害記録簿を作成・記録しなければならない。

e　業務管理者は、障害の被害が重大な場合又は情報システムの運用に著しい支障（以下「重大障害」という。）が発生している場合は、直ちに、所属の館等情報セキュリティ責任者に報告を行わなければならない。

f　報告を受けた館等情報セキュリティ責任者は、直ちに、CISO に報告を行わなければならない。

(ｴ)　再発防止措置

業務管理者及びサーバ等管理者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

(ｵ)　事後検証

CISO は、報告のあった障害事案について、再発防止に向け必要な改善措置が講じられているか館等情報セキュリティ責任者に報告を求めることができる。

イ　ネットワークにおける措置

(ｱ)　責任体制

ネットワーク管理責任者は、障害時における連絡及び対処の責任者となり、関係者との連携によりネットワークを速やかに回復しなければならない。

(ｲ)　障害時における対応方法の周知

ネットワーク管理責任者は、障害時における対応方法について、関係者に周知しなければならない。

(ｳ)　障害時の連絡及び対処

a　機構情報通信ネットワーク管理責任者及び情報セキュリティ責任者は、障害を発見したときは、相互に連絡しなければならない。

b　ネットワークを利用して情報処理を行おうとする課等（以下「利用課等」という。）のリーダー等は、障害を発見したときは、直ちに、情報セキュリティ責任者を通じて機構情報通信ネットワーク管理責任者に連絡しなければならない。

c　機構情報通信ネットワーク管理責任者及び情報セキュリティ責任者は、障害を発見し、又は障害の連絡を受けたときは、相互に連携し、直ちに、障害状況及び影響範囲を調査するとともに、機構情報通信ネットワーク管理責任者は障害に関係する情報セキュリティ責任者を通じて利用課等のリーダー等に当該障害状況等を連絡しなければならない。

d　機構情報通信ネットワーク管理責任者は、障害に関係する情報セキュリティ責任者及び利用課等のリーダー等と連携し、障害の回復に向け適切な措置を講じなければならない。

e　機構情報通信ネットワーク管理責任者は、障害発生に関係した部門から障害の原因及び処理の報告を求めるとともに、ネットワーク上の障害、故障の原因及び処理結果について障害記録簿を作成、記録しなければならない。

f　機構情報通信ネットワーク管理責任者は、機構情報通信ネットワークに重大障害が発生している場合は、直ちに、CISO に報告を行わなければならない。

g　館等情報通信ネットワーク管理責任者は、障害時の連絡及び対処等について、上記の内容に準じ適切な対応を行わなければならない。

(ｴ)　再発防止措置

ネットワーク管理責任者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

(ｵ)　事後検証

CISO は、報告のあった障害事案について、再発防止に向け必要な改善措置が講じられているかネットワーク管理責任者に報告を求めることができる。

②　侵害時の対応

ア　情報システムにおける措置

(ｱ)　責任体制

館等情報セキュリティ責任者は、所管する情報資産において、不正行為等による情報の漏え

い、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速に実施するとともに、再発防止の措置を講じなければならない。また、CISOは、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

(ｲ) 侵害時の対応方法の周知

館等情報セキュリティ責任者は、所管する情報資産に対し作成される実施手順において、侵害時の対応方法を明記させるとともに、関係する管理者、職員に対し当該対応方法について周知を行わなければならない。

(ｳ) 侵害時の連絡

a 情報システムの利用者が侵害事案の発生を発見したときは、直ちに、端末機管理者に報告し、端末機管理者は業務管理者及びサーバ等管理者に報告しなければならない。また、情報システムの稼働又は運用に係る担当者が侵害事案の発生を発見したときは、直ちに、サーバ等管理者及び業務管理者に報告しなければならない。

b 報告を受けた業務管理者は、直ちに、所属の館等情報セキュリティ責任者に報告を行わなければならない。

c 報告を受けた館等情報セキュリティ責任者は、直ちに、CISOに報告しなければならない。

d 館等情報セキュリティ責任者は、侵害事案が法令等に違反するものと見込まれる場合、CISOと協議し、警察等関係機関に通報しなければならない。

e CISOは、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、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。

f 侵害を発見した者又は侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在の場合その他の場合において、急を要するときは、上記の規定にかかわらず、直ちに、当該侵害事案を報告すべき者の上位の者に報告しなければならない。

(ｴ) 事案への対処

a 業務管理者及びサーバ等管理者は、侵害事案が発生したときは、次の事項について調査を実施しなければならない。

・事案の内容
・事案が発生した原因
・確認した被害
・影響範囲

b サーバ等管理者は、次の事案が発生し情報資産保護のために情報システムの停止がやむを得ない場合は、業務管理者に協議の上、情報システムを停止しなければならない。ただし、情報資産を保護するため急を要する場合には、サーバ等管理者は当該協議をしないで情報システムを停止することができる。

・情報システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等不正プログラムが情報に深刻な被害を及ぼしているとき
・その他の情報資産に係る重大な被害が想定されるとき

c 業務管理者及びサーバ等管理者は、事案に係る情報システムのアクセス記録及び現状を保存するとともに、事案に対処した経過を記録しなければならない。

d 事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を講じた後、情報システムの復旧を行う。

e 館等情報セキュリティ責任者は、上記の対処に当たり、業務管理者及びサーバ等管理者から随時報告を求め、作業の実施を管理しなければならない。

(ｵ) 再発防止措置

業務管理者及びサーバ等管理者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。また、館等情報セキュリティ責任者は、改善措置の実施について確認を行うとともに、再発防止に向け、関係する管理責任者、職員に対し対応方法について周知を行わなければならない。

(ｶ) 事後検証

CISOは、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているか館等情報セキュリティ責任者に報告を求めることができる。

イ　ネットワークにおける措置

(ｱ)　責任体制

ネットワーク管理責任者は、ネットワークにおいて、不正行為等による情報の漏えい、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速に実施するとともに、再発防止の措置を講じなければならない。また、CISO は、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

(ｲ)　侵害時の対応方法の周知

ネットワーク管理責任者は、情報セキュリティ実施手順において、侵害時の対応方法を明記するとともに、関係する管理責任者、職員に対し当該対応方法について周知を行わなければならない。

(ｳ) 侵害時の連絡

a　機構情報通信ネットワークの利用者が侵害事案の発生を発見したときは、直ちに、利用課等のリーダー等に報告し、利用課等のリーダー等は情報セキュリティ責任者を通じて機構情報通信ネットワーク管理責任者に報告しなければならない。また、ネットワークの運用管理担当者が侵害事案の発生を発見したときは、直ちに、機構情報通信ネットワーク管理責任者に報告を行わなければならない。機構情報通信ネットワーク管理責任者は関係する情報セキュリティ責任者に連絡を行わなければならない。

b　報告を受けた機構情報通信ネットワーク管理責任者は、直ちに、CISO に報告を行わなければならない。

c　館等情報通信ネットワークにおいて侵害事案の発生を発見した利用者又は運用管理担当者は、直ちに、館等情報通信ネットワーク管理責任者に報告しなければならない。館等情報通信ネットワーク管理責任者は、直ちに、所属の館等情報セキュリティ責任者に報告を行わなければならない。

d　報告を受けた館等情報セキュリティ責任者は、直ちに、CISO に報告を行わなければならない。

e　ネットワーク管理責任者は、侵害事案が法令等に違反するものと見込まれる場合、CISO と協議し、警察等関係機関に通報しなければならない。

f　CISO は、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、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。

g　侵害を発見した者又は侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在の場合その他の場合において、急を要するときは、上記の規定にかかわらず、直ちに、当該侵害事案を報告すべき者の上位の者に報告しなければならない。

(ｴ)　事案への対処

a　ネットワーク管理責任者は、侵害事案が発生したときは、次の事項について調査を実施しなければならない。

・事案の内容
・事案が発生した原因
・確認した被害・影響範囲

b　ネットワーク管理責任者は、次の事案が発生し情報資産保護のためにやむを得ない場合は、ネットワークの停止を含む必要な措置を講じなければならない。

・ネットワークの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき
・本法人のメールサーバ等が原因となって他者に被害を与えるおそれがあるとき
・その他の情報に係る重大な被害が想定されるとき

c　ネットワーク管理責任者は、事案に係る情報システムのアクセス記録及び現状を保存するとともに、事案に対処した経過を記録しなければならない。

d　事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を講じた後、ネットワークの復旧を行う。

e　機構情報通信ネットワークに係る対処に当たり、CISO は、機構情報通信ネットワーク管

理責任者から随時報告を求め、作業の実施を管理しなければならない。また、館等情報通信ネットワークに係る対処に当たり、館等情報セキュリティ責任者は、館等情報通信ネットワーク管理責任者から随時報告を求め、作業の実施を管理するとともに、CISO に作業状況について報告しなければならない。

(ｵ) 再発防止措置

ネットワーク管理責任者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。機構情報通信ネットワーク管理責任者は、機構情報通信ネットワークの改善措置の実施について、また館等情報セキュリティ責任者は、館等情報通信ネットワークの改善措置の実施について確認を行うとともに、再発防止に向け、関係する管理責任者、職員に対し対応方法について周知を行わなければならない。

(ｶ) 事後検証

CISO は、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているかネットワーク管理責任者に報告を求めることができる。

(4) 例外措置

① 例外措置の許可

館等情報セキュリティ責任者及び機構情報通信ネットワーク管理責任者は、ポリシー及び関係規程等を遵守することが困難な状況で、行政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、CISO に許可を受けて、例外措置を取ることができる。

② 緊急時の例外措置

館等情報セキュリティ責任者及び機構情報通信ネットワーク管理責任者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後直ちに CISO に報告しなければならない。

③ 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

(5) 法令遵守

① クラウドサービスへの商用ライセンスのあるソフトウェアのインストール

業務管理者及びネットワーク管理責任者は、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。

② 懲戒処分

ポリシーに違反した職員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、懲戒規程に基づき懲戒処分の対象となる場合がある。

12 業務委託とクラウドサービスの利用

(1) 業務委託

① 委託処理に当たっての基本原則

ア 業務管理者又はネットワーク管理責任者は、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又は事業者の再委託を許可する場合、主体性が損なわれないよう本法人の責務等次の点に留意するとともに、委託事業者（事業者及び再委託を受けた事業者をいう。以下同じ。）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。

・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本法人のコントロール下におくこと。

・情報システム及びネットワークに係る業務を委託しようとするときは、システム等のブラックボックス化を防止するために、適切な措置を講じること。

イ　業務管理者又はネットワーク管理責任者は、情報システムに係る業務の委託については、委託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　業務管理者又はネットワーク管理責任者は、情報システム及びネットワークの開発、運用等において複数の委託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。

エ　業務管理者又はネットワーク管理責任者は、クラウドサービスを利用する場合は、データの重要性分類に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

②　委託事業者の選定基準

ア　館等情報セキュリティ責任者は、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を確認しなければならない。

イ　館等情報セキュリティ責任者は、委託事業者の選定にあたっては、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定することが望ましい。

③　契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・ポリシー及び実施手順の遵守
・事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・本法人による監査、検査
・本法人によるセキュリティインシデント発生時の公表
・ポリシーが遵守されなかった場合の規定(損害賠償等)

③　確認・措置等

ア　業務管理者及びネットワーク管理責任者は、委託事業者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定期的に確認し、必要に応じ 、③の契約に基づき措置を実施しなければならない。また、その内容を館等情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

イ　業務管理者及びネットワーク管理責任者は、重要な情報を処理する場合等必要に応じ、本法人職員を処理に立ち会わせなければならない。

ウ　業務管理者及びネットワーク管理責任者は、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しなければならない。

エ　業務管理者及びネットワーク管理責任者は、作業を行う者のユーザＩＤ、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しなければならない。

(2)　クラウドサービスの利用

①　クラウドサービスの利用に係る規定の整備

CISO は、クラウドサービスの利用に関する規定を整備しなければならない。

②　クラウドサービスの選定

業務管理者は、取り扱う情報の格付及び取扱制限を踏まえ、CISO が別途整備するクラウドサービス利用基準に従って外部サービスの利用を検討しなければならない。

13　評価及び見直し

(1)　検査

①　実施方法等

CISO は、規程第 13 条の規定に基づき、情報セキュリティ検査を実施する。

②　検査結果への対応

CISO は、規程に定める情報セキュリティ検査の指摘事項が被検査部門以外の所管する情報資産に対して、同様の課題及び問題点がある可能性がある場合は、当該課題及び問題点の有無を館等情報セキュリティ責任者に報告を求めることができる。

(2)　自己点検

①　実施方法等

ア　業務管理者及びネットワーク管理責任者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。委託事業者に委託している場合、業務管理者は、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。

イ　館等情報セキュリティ責任者は、情報セキュリティ責任者と連携して、所管する館等における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、定期的に自己点検を行わなければならない。

②　報告

館等情報セキュリティ責任者は、 自己点検結果と自己点検結果に基づく必要な改善等を取りまとめ、CISO に報告しなければならない。

③　自己点検結果の活用

ア　職員は、自己点検結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　CISO は、館等情報セキュリティ責任者に対し、情報セキュリティ対策の自己点検実施の要請及び自己点検結果の報告を求めることができる。

(3)　ポリシー及び関係規程等の見直し

①　ポリシー及び関係規程等の改善

ア　CISO は、検査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ 、ポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

イ　CISO は、対策基準の変更を行ったときは、速やかに館等情報セキュリティ責任者その他関係者に周知を行わなければならない。

②　館等の所管する情報システム及びネットワークの情報セキュリティ対策の見直し

館等情報セキュリティ責任者は、所管する情報システム及びネットワークについて、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、当該システム及びネットワークの実施手順の変更を

行わなければならない。

④　機構情報通信ネットワークの情報セキュリティ対策の見直し

CISO は、機構情報通信ネットワークについて、ポリシーの変更に伴う情報セキュリティ対策の見直しを行わなければならない。

14　対策基準等の取扱い

対策基準及び実施手順のうち、公にすることにより本法人の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

この対策基準は、令和８年４月１日より施行する。