公益財団法人神奈川芸術文化財団
情報セキュリティポリシー

公益財団法人神奈川芸術文化財団

「第２章 情報セキュリティ対策基準」の内容は、情報セキュリティの確保に支障を及ぼす恐れのある情報を含むことから、記載しておりません。

＜目 次＞

神奈川芸術文化財団情報セキュリティポリシー

序 神奈川芸術文化財団情報セキュリティポリシーの構成

公益財団法人神奈川芸術文化財団(以下、「財団」という。)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。）は、定款に定められた目的を達成するために行うすべての事業、業務の遂行に際し、財団が保有又は取り扱う情報資産を事故、災害、犯罪等から保護するための情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものをいう。情報セキュリティポリシーは、財団が保有又は取り扱う情報資産に関する業務に携わる全ての職員等に情報セキュリティへの取組みを浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分である情報セキュリティ基本方針と情報セキュリティを取り巻く状況の変化に依存する部分である情報セキュリティ対策基準により構成する。

また、情報セキュリティポリシーに基づき、コンピュータ、ネットワーク及び情報システム（以下「情報システム等」という。）又は施設ごとの情報セキュリティに係る具体的な実施手順を、情報セキュリティ実施手順として策定することとする。

情報セキュリティポリシー及び情報セキュリティ実施手順の構成

<table>
<tr><th>分類</th><th>文 書 名</th><th colspan="2">内　　容</th></tr>
<tr><td rowspan="2">情報セキュリティポリシー</td><td rowspan="2">神奈川芸術文化財団情報セキュリティポリシー</td><td>情報セキュリティ基本方針</td><td>情報セキュリティ対策に関する統一的かつ基本的な方針。</td></tr>
<tr><td>情報セキュリティ対策基準</td><td>情報セキュリティ基本方針に基づき定める電子的な情報システム等に共通の情報セキュリティ対策の基準
※紙文書等の取り扱いは別途文書規程にて定める</td></tr>
<tr><td>情報セキュリティ実施手順</td><td>情報セキュリティ点検に関する基準等</td><td colspan="2">情報セキュリティポリシーに基づいて、施設ごとに定める具体的な実施手順</td></tr>
</table>

第１章　情報セキュリティ基本方針

Ⅰ　目的

財団の情報システム等が取り扱う情報には、県民や利用者等の個人情報のみならず財団運営上重要な情報など、外部に漏えい等した場合に重大な結果を招く情報も含まれている。

したがって、これらの情報及び情報を取り扱う情報システム等を様々な脅威から防御することは、県民や利用者等の情報、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに財団に対する県民や利用者等からの信頼の維持向上に寄与するものである。

本基本方針は、財団が保有又は取り扱いする情報資産の機密性、完全性及び可用性を維持するため、財団が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

Ⅱ　定義

情報セキュリティポリシーにおいて、次に掲げる用語の意義は、以下の各号に定めるところによる。

(1)　情報

財団が保有または取り扱うすべての情報のことをいい、公開・非公開の別や紙文書や電子データ上の情報、映像・音声情報等を問わない。

(2)　コンピュータ

汎用コンピュータ、サーバ、ワークステーション、端末及びこれらに類するもの並びにこれらの運営に必要な機器をいう。

(3)　端末

ネットワークに接続し、データの送受信や処理を行う機器を言い、パーソナルコンピュータや業務用携帯電話、タブレット機器等が該当する。但し記憶装置やマウス等の周辺機器は含まれない。

(4)　ネットワーク

コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。財団内にて使用するネットワークを「財団ネットワーク」と呼ぶ。

(5)　情報システム

コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。

(6)　データ

コンピュータ又は記録媒体やクラウドサービスに記録されている電磁的記録をいう。

(7)　情報資産

財団が保有又は取り扱う情報及びコンピュータ、ネットワーク、情報システムをいう。

(8)　記録媒体

データを記録するための媒体をいう。例えば、磁気テープ、フロッピーディスク、ハードディスク、ＵＳＢメモリ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、ボイスレコーダ、デジタルカメラ、ＳＤメモリカードなど。

(9)　モバイル端末

端末のうち、自席にとどまらず、財団内外に携帯し、利用できる端末（貸与コンピュータ、貸与携帯電話）をいう。

(10)　IoT 機器を含む特定用途機器
　プリンタやスキャナー、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、ネットワークに接続されている又は電磁的記録媒体を内蔵しているものをいう。
(11)　外部サービス
　財団の業務運営に必要な事務を実施するために、Microsoft365 をはじめとした、事業者等の財団外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において財団が保有又は取り扱う情報資産が取り扱われる場合に限る。
(12)　クラウドサービス
　ネットワークに接続されたコンピュータを運営する事業者等が提供する様々なサービス・機能を利用する形態をいう。
(13)　ソーシャルメディア
　インターネット上において不特定多数の者が情報を交換・共有する仕組みをいう。例えば、ブログ、ソーシャルネットワーキングサービス、動画共有サイトなど。
(14)　ソーシャルメディアサービス
　インターネット上において不特定多数の者が情報を交換・共有する仕組みを提供するサービスをいう。
(15)　機密性
　情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
(16)　完全性
　情報が最新かつ正確な情報で維持され、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。
(17)　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。
(18)　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。
(19)　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の対策をいう。
(20)　情報セキュリティインシデント
　望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。
(21)　職員等
　財団ネットワークに接続し、財団に関する業務を行う者をいう。財団理事・財団職員・派遣職員・業務委託先等が該当する。
(22)　施設
　財団がその事務を処理する目的で使用する建物及び敷地をいう。

Ⅲ　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、財団が保有または取り扱う情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の指針となるものである。

したがって、財団が保有又は取り扱う情報資産に関する業務に携わる全ての職員等は、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、業務の遂行に当たって情報セキュリティポリシーを遵守するものとする。

Ⅳ　情報セキュリティ管理体制

財団は、財団が保有又は取り扱う情報資産について、情報セキュリティ対策を推進及び管理するための体制を以下のとおり確立する。

(1)　最高情報セキュリティ責任者

専務理事を、最高情報セキュリティ責任者（CISO：Chief Information Security Officer 、以下「CISO」という。）とする。

CISOは、財団が保有又は取り扱う情報資産の情報セキュリティを統括する。最高情報セキュリティ責任者が不在の場合は、統括情報セキュリティ管理者（事務局長）が統括する。

(2)　統括情報セキュリティ管理者

事務局長を、統括情報セキュリティ管理者とする。

・統括情報セキュリティ管理者は、CISOを補佐する。

・統括情報セキュリティ管理者は、情報セキュリティ管理者及び情報システム管理者等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。

・統括情報セキュリティ管理者は、財団が保有又は取り扱う情報資産に対するセキュリティ侵害又はセキュリティ侵害の恐れのある場合には、CISOの指示に従い、必要かつ十分な全ての措置を行う。

・統括情報セキュリティ管理者は、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を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

(3)　情報セキュリティ管理者

事務局次長、神奈川県民ホール支配人、神奈川芸術劇場副支配人及び神奈川県立音楽堂館長を、情報セキュリティ管理者とする。

・情報セキュリティ管理者は、施設内における情報セキュリティを統括する。

・情報セキュリティ管理者は、施設において保有又は取り扱う情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに当該施設における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職員等に対する教育、訓練、助言及び指示を行う。

・情報セキュリティ管理者は、施設内における情報資産に対する侵害又は侵害の恐れのある場合には、情報システム管理者等へ速やかに報告を行い、指示を仰ぐものとする。

・情報セキュリティ管理者は、施設に係る情報セキュリティ実施手順の策定、維持及び管理を行う。

・情報セキュリティ管理者は、職員等に端末による作業を行わせる場合には、情報セキュリティポリシーについて、特に注意を喚起し、守るべき実施手順を理解させ、かつ実施及び遵守させるものとする

(4)　ネットワーク管理者

事務局次長を、財団ネットワークに関するネットワーク管理者とする。

・ネットワーク管理者は、保有又は取り扱うネットワークの構築、設定の変更、運用、更新等を行う。
・ネットワーク管理者は、保有又は取り扱うネットワークの情報セキュリティを統括する。
・ネットワーク管理者は、保有又は取り扱うネットワークにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに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職員等に対する教育、訓練、助言及び指示を行う。
・ネットワーク管理者は、保有又は取り扱うネットワークに係る情報セキュリティ実施手順の策定、維持及び管理を行う。
・神奈川芸術劇場の一部の業務用ネットワーク（以下「KAAT-STAFF」という。）については、当該ネットワークを利用する課の長（舞台技術課長）をネットワーク管理者とする。

(5)　情報システム管理者

経営企画課長を、当該情報システムに関する情報システム管理者とする。
・情報システム管理者は、保有又は取り扱う情報システムの開発、設定の変更、運用、更新等を行う。
・情報システム管理者は、保有又は取り扱う情報システムの情報セキュリティを統括する。
・情報システム管理者は、保有又は取り扱う情報システムにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに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職員等に対する教育、訓練、助言及び指示を行う。
・情報システム管理者は、保有又は取り扱う情報システムに係る情報セキュリティ実施手順の策定、維持及び管理を行う。
・情報システム管理者は、保有又は取り扱う情報システムに係る実務担当者を定める。
・KAAT-STAFF については、当該システムを利用する課の長（舞台技術課長）を情報システム管理者とする。

(6)　コンピュータ管理者

経営企画課長を、当該コンピュータに関するコンピュータ管理者とする。
・コンピュータ管理者は、保有又は取り扱うコンピュータの設定、運用、更新等を行う。
・コンピュータ管理者は、保有又は取り扱うコンピュータの情報セキュリティを統括する。
・コンピュータ管理者は、保有又は取り扱うコンピュータにおける情報資産に対する侵害又は侵害の恐れのある場合の連絡体制の構築並びに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職員等に対する教育、訓練、助言及び指示を行う。
・コンピュータ管理者は、保有又は取り扱うコンピュータに係る情報セキュリティ実施手順の策定、維持及び管理を行う。
・KAAT-STAFF に接続するコンピュータについては、当該コンピュータを利用する課の長（舞台技術課長）をコンピュータ管理者とする。

(7)　情報セキュリティ監査統括管理者

統括情報セキュリティ管理者は、情報セキュリティ監査統括管理者として監査室長を指名し、情報資産に対する情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行うものとする。

(8)　デジタル戦略会議

財団の情報セキュリティの維持管理を統一的な視点で行うため設置されるものとし、CISOの元、マネジメント会議メンバー及びデジタル戦略アドバイザーにて構成される。情報セキュリティポリシーの策定等の情報セキュリティに関する重要な事項を審議する。

(9)　職員等
・職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順のうち職員等向けに定められている事項を遵守するものとする。
・職員等は、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については、速やかに上長を通じ情報セキュリティ管理者に相談し、指示等を仰ぐものとする。
(10)　情報セキュリティに関する統一的な窓口（CSIRT）の設置
・CISOは、情報セキュリティインシデントの統一的な窓口の機能を有する組織（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）をCSIRT責任者と共に整備し、情報セキュリティインシデントについて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する。
・統括情報セキュリティ管理者をCSIRT責任者とし、あらかじめ指定された職員及び財団本部職員で構成する。
・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を定める。
・CSIRTは、CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を財団内に提供する。
・CSIRTは、情報セキュリティインシデントを認知した場合、独立してその任にあたり、特に緊急を要する場合は自らの判断により、その他の場合はCISO又はCSIRT責任者の指示に従い、関係者に対する指示や財団内への情報提供等、必要な措置をとることとする。
・CSIRTは、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行うものとする。
・CSIRTは、情報セキュリティに関して、関係機関等の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。
・CSIRTは、情報セキュリティインシデントを認知した場合には神奈川県庁の所管課等へ報告しなければならない。
(11)　情報セキュリティに関する内部報告
　CSIRTから職員等及びその他の関係者への情報セキュリティに関する報告については、Microsoft Teams並びに電子メール等による一斉同報によることとする。

Ⅴ　情報の分類
　財団は、情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

Ⅵ　情報資産への脅威
　情報セキュリティ対策基準を策定する上で、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し、特に情報セキュリティ対策を講ずべき脅威を以下のとおりとする。
・部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等
・職員等の誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末及び媒体の接続による情報漏えい等
・地震、落雷、火災等の災害及び事故、故障等による業務の停止
・大規模・広範囲にわたる疾病による職員等の要員不足に伴う情報システム運用の機能不全

Ⅶ　情報セキュリティ対策

ネットワーク管理者は、上記Ⅵで示した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ものとする。

(1)　情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じるものとする。

・個人番号利用事務を取り扱う業務においては、取り扱う者は、情報セキュリティ対策基準の適用範囲外のネットワーク（以下「外部ネットワーク」という。）からの直接通信をできないようにし、端末からの情報持ち出し不可設定等導入等により、県民や利用者・関係者情報の流出を防ぐ。

・財団ネットワークにおいては、Microsoft365 Entra ID の認証によりインターネットの通信経路を制限する。

・インターネット接続においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。また、インターネットへの接続は、ネットワーク管理者があらかじめ許可した接続口のみとする。

(2)　物理的対策

情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策

(3)　人的対策

情報セキュリティに関する役割等を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を講じるための対策

(4)　技術的対策

情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策

(5)　運用における対策

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、委託を行う際の情報セキュリティ確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

Ⅷ　情報セキュリティ対策基準の策定

財団が保有又は取り扱う情報資産について、上記Ⅶの電子的な情報資産に係る情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。このため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を別途定めるものとする。

Ⅸ　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、情報セキュリティ管理者は、保有又は取り扱う情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼす恐れがあるため取扱いに注意するものとす

る。

Ⅷ　情報セキュリティ監査の実施

　財団は、情報セキュリティポリシーが遵守されていることを検証するため、定期的に外部監査を実施するものとする。

Ⅸ　評価及び見直しの実施

　財団は、情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を行うとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。