学校法人国立音楽大学情報セキュリティに関する規程

制定　平成29年12月20日
改正　　2020年９月16日

第１章　総則「情報セキュリティ基本方針」

（基本理念及び情報セキュリティ基本方針の目的）

第１条　学校法人国立音楽大学（以下「本法人」という。）において、基本的理念である「自由、自主、自律の精神を以て良識ある音楽家、教育家を育成し、日本及び世界の文化の発展に寄与する。」ことを実践し、また社会的責務を果たすためには、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。

そのために、本法人の教職員、学生、その他の構成員は、情報資産の価値を十分に認識し、本法人の情報資産を守るだけではなく、外部に対する不正な情報提供、情報資産の侵害などが行われないように努め、情報システムの信頼性を高めていかなければならない。

（運用の基本方針）

第２条　前条の目的を達するため､「学校法人国立音楽大学情報セキュリティに関する規程」（以下「本規程」という。）を制定し、本法人の全構成員に周知を図ることとする。

(1) 本法人に対する情報セキュリティ侵害を阻止すること。
(2) 学内外の情報セキュリティを侵害する行為を抑止すること。
(3) 情報資産の管理・運用を行うこと。
(4) 情報セキュリティ侵害の早期検出と迅速な対応を実現すること。

（利用者の義務）

第３条　本法人の提供する情報資産に関連するサービスを利用する者や運用の業務に携わる者は、本規程を遵守する責任があり、また情報資産の保護（権限のないアクセス、改ざん、複写、破壊、漏えいなどの禁止)、関連法令の遵守（不正アクセス禁止法、著作権法、個人情報保護法など）に努めなければならない。

（用語の定義）

第４条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

(1) 情報

本法人の教育・研究・管理運営に関わる者が作成し、又は収集及び取得した内容が記録された文書、電子文書、情報システム内のデータ、その他それに準ずるものをいう。

(2) 情報システム

本法人内を構成する全ての情報ネットワーク機器及び電子計算機（機器に導入のソフトウェアを含む）をいう。またこれらの機器で構成され利用者に提供されている全ての仕組み及び運用管理のために提供されている仕組み並びにこれらを運用管理する体制を含む。

(3) 情報資産

情報システム、情報ネットワークに接続された情報ネットワーク機器及び電子計算

機、並びにそこで取り扱われる情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料など）をいう。

(4) 情報セキュリティ

情報の機密性、完全性、可用性を保護し維持すること。

機密性　：許可された者だけが情報資産にアクセスできること

完全性　：情報資産や情報システムが破壊、改ざん、消去されていないこと

可用性　：許可された者は必要なときに情報資産を利用できること

(5) 情報セキュリティ監査

情報セキュリティに従い、企業情報セキュリティマネジメントが適切に実施されているか、情報セキュリティマネジメント（基本方針・リスク分析など）機能の有効性を評価すること。

(6) 安全区域

電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室、又はサーバルームなどの内部であって、予め許可を受けた者以外の者の侵入、自然災害の発生などを原因とする情報セキュリティの侵害に対して施設及び環境面から対策が講じられている区域をいう。

（対象範囲）

第５条　本規程の対象範囲は「本法人が管理する情報資産」及び「本法人の諸活動に伴い、業務委託先において取り扱われる情報資産」をいう。

（対象者）

第６条　本規程は、本法人の情報資産を利用する全ての者を対象とする。（以下「利用者」という。）

(1) 役員、教員（非常勤教員を含む。）

(2) 職員（臨時職員、派遣職員など含む。）

(3) 学生（研究生、科目履修生、委託生など含む。）・生徒・児童・園児・保護者・保証人

(4) 委託業者、学外者など

第２章　情報セキュリティ対策基準

（趣旨）

第７条　この対策基準は、基本方針の目的を達成するために、必要な組織・体制、基準、指針などを定めるものとする。

（組織及び体制）

第８条　責任者、管理者など本法人における情報セキュリティを確保するために、組織及び体制を定める。

２　情報セキュリティ組織・体制図は別表の通りとする。

（情報セキュリティ最高責任者）

第９条　本法人の情報セキュリティの最高責任者を置き、理事長をもって充てる。情報セキュリティ最高責任者は、本法人の情報セキュリティに関する総轄的な意思決定を行い、内外に対する責任を負う。

（情報セキュリティ実施責任者）

第10条　本法人の情報セキュリティの実施責任者を置き、教育研究組織においては各学校長・園長、事務組織においては総務・財務部長をもって充てる。また、情報セキュリティ実施責任者は、各部署の情報セキュリティに関する権限と責任を有する。

（情報セキュリティ担当者）

第11条　各部署に情報セキュリティ担当者を置き、次に掲げる者をもって充てる。情報セキュリティ担当者は、 個々の情報機器、ソフトウェア及び情報を管理・監督し、情報セキュリティを維持するための責任を負う。研究室などにおいて、利用者自らが直接管理する情報資産を持つ場合については、各利用者が、そのセキュリティに関する責任を負う。

(1) 大学の教育研究組織

個々のクライアント機器により情報システムを利用する全教員

(2) 附属中学・高等学校・小学校の教育研究組織

個々のクライアント機器により情報システムを利用する全教員

(3) 附属幼稚園の教育研究組織

園長が指名した者

(4) 事務組織

各部署課長（課長が置かれていない部署においては課長補佐）

（ネットワーク管理責任者）

第12条　メディアセンターにネットワーク管理責任者を置く。ネットワーク管理責任者は、基幹ネットワークと業務用サーバを運用・管理しセキュリティを維持するための責任を負う。管理責任者として、メディアセンター事務室課長を充てる。なお、学内ＬＡＮ関連の事項に関しては、メディアセンター運営機構及びＩＣＴ推進委員会においても審議する。

（情報セキュリティ委員会）

第13条　情報セキュリティ委員会は、最高責任者及び実施責任者の指示により、基本方針の維持及び見直しの他、情報資産に対する重大な脅威への警戒・監視、情報セキュリティに関わる事件・事故の調査・分析及び再発防止策の立案、啓発活動などを責務とする。委員会の運営などに関し、必要な事項については、「国立音楽大学情報セキュリティ委員会規程」の定めるところによる。

第３章　情報セキュリティ運用方針

（物理的セキュリティ）

第14条　情報セキュリティ運用方針のうち、物理的セキュリティについては、次の各号の通りとする。

(1) 情報システムの設置など

情報セキュリティ実施責任者、情報セキュリティ委員会は、サーバ機などの重要な情報システム、情報資産をそれぞれ設定された安全区域内に設置、また正当なアクセス権のない者が使用できないよう、セキュリティ確保に努める。

(2) 情報機器及び記録媒体の盗難対策

情報セキュリティ実施責任者は、情報機器及び記録媒体の盗難予防に努める。

(3) 情報機器及び記録媒体の学外への持ち出し

利用者は、個人情報及び本法人の重要なデータが入った情報機器及び記録媒体を、原則として学外へ持ち出してはならない。やむを得ず、情報機器、又は記録媒体を学外へ持ち出す場合は、情報セキュリティ実施責任者の承認を得た上で、情報の漏えいが発生しないよう、情報セキュリティ対策を講じる。

(4) 情報機器及び記録媒体の学内への持込み

利用者は、情報機器及び記録媒体を学内へ持ち込む場合は、ウィルスチェックを行うなど、情報セキュリティ対策を講じる。

(5) 情報のバックアップ

利用者及び情報セキュリティ委員会は、サーバ機器などに記録するデータを必要に応じて定期的にバックアップを行う。

(6) 情報機器及び記録媒体の処分

利用者は、情報機器及び記録媒体を破棄する場合は、残存情報が第三者に読み取られることのないよう、適切な情報セキュリティ対策を講じる。

（人的セキュリティ）

第15条　情報セキュリティ運用方針のうち、人的セキュリティについては、次の各号の通りとする。

(1) 教育・研修

情報セキュリティ最高責任者は、情報セキュリティに関する啓発や教育を実施するため、必要な措置を講じるよう努めるものとする。

(2) 利用者の義務

① 利用者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたっては、本規程及びその他関連法令等を遵守しなければならない。

② 利用者は、内外に対して、情報セキュリティを損ねる行為をしてはならない。

③ 利用者は、アクセス権限のない情報にアクセスしたり、許可されていない情報を利用したりしてはならない。

(3) 事故・障害時の報告・対応

① 利用者は、情報セキュリティに関する事故・障害及び公開情報の改ざん等を発見した場合には、直ちに情報セキュリティ実施責任者、情報セキュリティ担当者又はネットワーク管理者に報告しなければならない。

② ネットワーク管理者は、内外から情報システムの不正使用、情報資産の不正な利用等にかかわる苦情、通報等があった場合には、速やかに調査を行わなければならない。

③ ネットワーク管理者は、調査の結果、不正が確認されたときは、関係する通信の遮断、該当する情報システムの切離し等必要な措置を直ちに講じ、情報セキュリティ実施責任者に報告しなければならない。

④ 情報セキュリティ実施責任者は、重大な事故が発生した場合は、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。

⑤ 情報セキュリティ実施責任者は、重大な事故について審議する必要がある場合は、情報セキュリティ委員会を招集しなければならない。

(4) 委託契約

情報システムの開発又は運用管理を外部委託する場合は、外部委託業者から再委託を受ける業者等も含め､本規程を遵守することを明記した契約を締結するものとする。

（技術的セキュリティ）

第16条　情報セキュリティ委員会は、管理する機器・ソフトウェアについて、常にその構成を把握し、セキュリティに関わる更新、ウィルス対策など適切なセキュリティの維持に努める。

(1) 不正アクセスなどへの対応

不正アクセスの防止及び検出するための適切な手段を講じる。

(2) アクセス制限

教育研究組織、又は事務組織において、情報の内容に応じてアクセス可能な利用者を定め、不正なアクセスを阻止するために必要なアクセス制限を行う。

(3) ログの保存

システムなどのアクセス・操作ログなど、保存期間を定めて保存する。

（セキュリティ基本方針の評価及び更新）

第17条　情報セキュリティに従い、セキュリティ基本方針の実効性について、適切に実施されているか、基本方針・リスク分析などを定期的に評価し、改善が必要と認められた場合は、セキュリティレベルの高い、かつ遵守可能な基本方針に更新する。

第４章　罰則・処分

（罰則・処分）

第18条　情報セキュリティ委員会責任者は、利用者が本規程に違反した場合には、法令、本法人就業規則、学則などに基づき、処分・その他の措置を行う。

第５章　規程の改廃

（規程の改廃）

第19条　本規程の改廃は、情報セキュリティ委員会が審議し、理事会において決定する。

附　則

本規程は、平成29年12月20日から施行する。

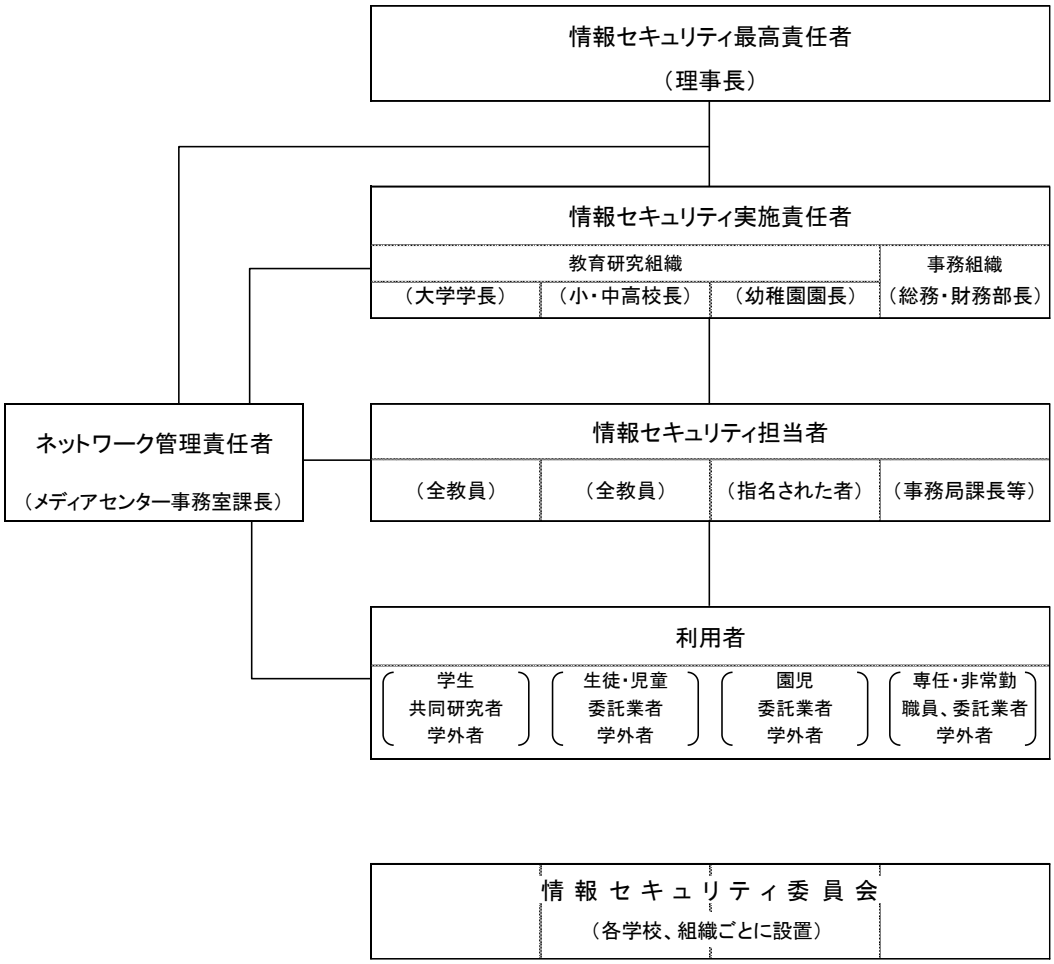
附　則

本規程は、平成31年４月１日から施行する。

附　則

本規程は、2020年９月16日から施行する。

別表　組織・体制図


情報セキュリティ最高責任者
（理事長）
情報セキュリティ実施責任者
教育研究組織
事務組織
（大学学長）
（小・中高校長）
（幼稚園園長）
（総務・財務部長）
ネットワーク管理責任者
（メディアセンター事務室課長）
情報セキュリティ担当者
（全教員）
（全教員）
（指名された者）
（事務局課長等）
利用者
学生
共同研究者
学外者
生徒・児童
委託業者
学外者
園児
委託業者
学外者
専任・非常勤
職員、委託業者
学外者
情 報 セ キ ュ リ テ ィ 委 員 会
（各学校、組織ごとに設置）