

組織・体制に関する対策基準

1. 趣旨

本文書では、本学の情報セキュリティマネジメントを遂行する組織・体制を定め、管理・運用組織および構成員それぞれの役割、責任および免責事項について記述する。

2. 組織・体制

情報セキュリティの管理・運用組織の構成を下図に示す。

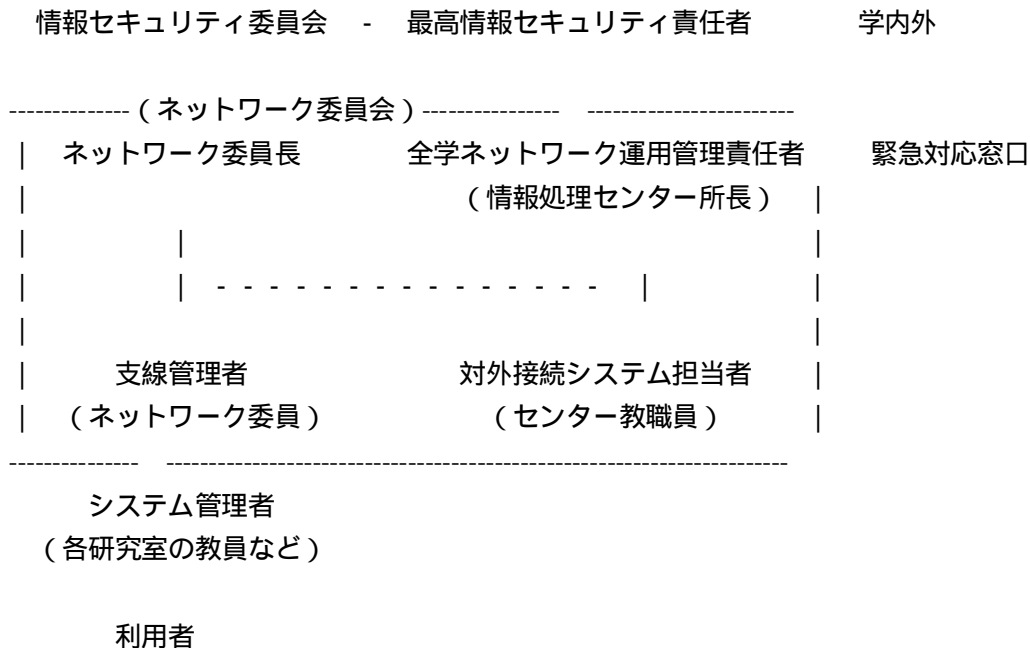


図1 情報セキュリティ管理・運用組織の構成図

2.1 最高情報セキュリティ責任者

最高情報セキュリティ責任者は、「岡山理科大学情報セキュリティポリシー」に基づき、以下に記述する学内のすべての情報セキュリティに関する総括的な権限と責任を有する。

- ・情報セキュリティ委員会を組織し、すべての部署におけるポリシー遵守の励行。
- ・全学ネットワーク運用管理責任者およびネットワーク委員会に対する情報システムの円滑な運用に必要な措置の指示。
- ・全学ネットワーク運用管理責任者およびネットワーク委員会が行った緊急避難措置への対処。
- ・全学ネットワーク運用管理責任者およびネットワーク委員会による定常的なセキュリティ対策の措置、ならびにセキュリティ管理の状況に関する報告への対処。
- ・理事会、教授会および大学協議会への情報セキュリティに関する重要事項の報告または勧告。
- ・情報セキュリティに関する学外からの苦情への対応（損害賠償請求など法的対応部署との連携を含む）ならびに学外から受けた被害への対応（被害回復請求など）。

2.2 全学ネットワーク運用管理責任者

情報処理センター所長は全学ネットワーク運用管理責任者として、全学の情報システムが円滑に運用されるよう、情報セキュリティの保持と強化のための技術的な調査検討を行うとともに、緊急時の総括的な連絡窓口として機能する。

- ・全学ネットワーク運用管理責任者は、情報セキュリティを守るために必要と判断した時は、ネットワーク委員長と連携し、緊急避難措置をとることができる。そして、その事実を速やかにネットワーク委員会に報告し事後対策を講じなければならない。
- ・全学ネットワーク運用管理責任者は、全学の情報セキュリティの管理および監査の実施に関し、最高情報セキュリティ責任者を補佐し、情報セキュリティの保持と強化のために必要な技術的措置を提案する。

2.3 情報セキュリティ委員会

情報セキュリティ委員会は全学の情報セキュリティに関し、以下に記述する基本的なセキュリティポリシーの策定および重要事項の決定を行うとともに、対外的な対応等を行う。

- ・セキュリティポリシーの策定と見直し。
- ・セキュリティポリシーの遵守の励行および違反に対する措置。
- ・教育研究活動におけるネットワークの利用ルールの制定。
- ・学内の他の意思決定機構との調整。
- ・外部との折衝。
- ・ネットワーク委員および教員への情報セキュリティに関する教育および啓蒙。
- ・教職員および学生等への幅広い初心者教育。

2.4 ネットワーク委員

ネットワーク委員は、ネットワーク管理・運用単位（以下、「支線」）の情報システム管理の実施に関し、ネットワーク委員会および情報処理センターとの連絡などの対応にあたる。そのために、以下のことを行うことができる。

- ・情報セキュリティの保持と強化のための技術的な調査および対策の実施。
- ・システム管理者に対し、必要な技術的措置の提案。

また、支線において、システム管理者（各研究室の教員など）の協力の下に、支線の管理・運用にあたる。

ネットワーク委員は、各支線において情報セキュリティを守るために必要と判断したとき、緊急避難措置をとることができる。緊急避難措置をとった場合には、全学ネットワーク運用管理責任者にその事実を速やかに報告しなければならない。

2.5 ネットワーク委員会

ネットワーク委員会は、全学の情報システムのセキュリティ管理を実施するための連絡調整およびネットワーク委員への技術的助言等の支援を行う。

ネットワーク委員会は情報処理センターとの連携の下にネットワーク委員を通じて、すべてのセキュリティポリシー対象者に情報セキュリティに関する情報の周知を図らなければならない。

ネットワーク委員長は、ネットワーク委員会において、情報セキュリティの保持と強化のために

必要な技術的措置を検討し、実施に関する協議を行う。

全学ネットワーク運用管理責任者は、情報セキュリティを守るために必要と判断した時は、ネットワーク委員長と連携し、緊急避難措置をとることができる。ただし、その措置については、速やかに最高情報セキュリティ責任者に報告するとともに、ネットワーク委員会の承認を受けなければならない。同時に、その措置によって影響を及ぼすと判断される情報資産のシステム管理者に、その旨を速やかに通知しなければならない。当該システム管理者から対応策の実施が完了した旨の報告がなされたときは、ネットワーク委員会に図り、速やかに対応策を検討し、十分であると判断した場合は、緊急避難措置を直ちに解除する。各ネットワーク委員およびシステム管理者から緊急避難措置の依頼があった場合も必要性を判断して同様の措置を行うものとする。ネットワーク委員会は緊急時に迅速に対応できるよう、委員会の審議方法を整備しておかなければならない。

2.6 情報処理センター

情報処理センターは全学の情報システム管理の実施に関し、緊急時の連絡など、総括的な対応にあたり、以下に記述する役割を担う。

- ・全学的な情報セキュリティの保持と強化のための技術的な調査検討、および必要な技術的措置の提案。
- ・セキュリティ監査の実施。
- ・緊急時の総括的な連絡窓口。

情報処理センターは、緊急時に即時に対応できる体制を整備しておかなければならない。

2.7 システム管理者

「物理的セキュリティに関する対策基準」で規定される情報関連機器の経理上の管理者を、原則として、当該情報システムのシステム管理者とする。ただし、学科や学部、部局で共有して利用する情報関連機器は学科等の代表者をシステム管理者とする。前述にかかわらず、当該情報関連機器を占有使用する教員はその機器のシステム管理者である。システム管理者は、個々の情報システムを維持・管理し、運用に則したパラメータの設定やセキュリティパッチの実施などセキュリティを維持するための責任を負う。

システム管理者の監督下において他の教職員あるいは大学院生等にシステム管理業務を委託もしくは補助させる場合、そのシステム管理業務の責任と権限の範囲を明確に定めこれを厳守させなければならない。またどのような場合においても、最終的な責任は当該システム管理者にある。

2.8 利用者

すべての「情報セキュリティポリシー」対象者は、「岡山理科大学情報セキュリティポリシー」を遵守し、ポリシーおよび実施手順に従って情報関連機器を利用しなければならない。さらに、システム管理者からセキュリティ維持管理のために協力を依頼された場合は、それに従わなければならない。

3．不正アクセス等への対応

ネットワーク委員会および情報処理センターは、外部または内部からの不正アクセスを検出した場合、情報セキュリティ委員会が定めた緊急措置手順に従い、関連する通信の遮断または該当する情報機器の切り離しを実施する。ただし、あらかじめ手順に定められていない場合は、最高情報セキュリティ責任者が判断する。

情報セキュリティ委員会は、不正アクセスが継続する場合、当該情報機器またはそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。

情報セキュリティ委員会は、不正アクセス等「岡山理科大学情報セキュリティポリシー」に違反した大学構成員の身分に関する処分について、その権限を有する理事会、教授会等に対し、違反行為の報告および処分の勧告を行う。

情報セキュリティ委員会は、上記の措置、報告および勧告に際し、その調査と判断の内容を開示する手続きを定めなければならない。また、当該構成員がその内容に不服がある場合の異議申し立て方法を定めておかなければならない。

4．施行期日

本対策基準は、平成16年11月1日より施行する。