C3100 情報システム運用・管理手順の策定に関する解説書

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年10月31日  A3100 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3100 | 文書構成と文書番号の見直しへの対応 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

　本書は、「C2101 情報システム運用・管理規程」を実際に適用する際に用いられる、情報セキュリティ対策を円滑に実施するための文書（手順、ガイドライン及びマニュアル等）の策定に関して、概要を解説するものである。

１．文書構成

　情報システムの運用・管理に係る手順等（C3101～C3104）として、次に掲げる4種類の文書を用意した。

　C3101 例外措置手順書

　C3102 インシデント対応手順

　C3103 情報格付け取扱手順

　C3104 情報システムリスク評価手順

ポリシー及び関連する実施規程に従い、実際に情報システムを運用・管理する場合、情報セキュリティ維持のためにとるべき対策は多岐にわたる。そのためサンプル規程集では、個々の場面場面に応じて、そこで遵守すべき事項を複数の文書に定めることとした。これらの文書の他、さらに具体的な操作マニュアルとして、例えば次のような文書を整備することも考えられる。

　・オペレーティング・システム設定手順（Windows®、Linux®、FreeBSD®等）

　・ソフトウェア設定手順（DNS、SMTP、POP/IMAP、FTP、HTTP、SSL、SSH、

　　VPN、IPFW等）

　・通信機器設定手順（ファイアウォール、ルータ、ハブ等）

　あらかじめ詳細な手順を定めておくことで、情報システムを運用・管理する者が実施すべき事項が明確となり、情報セキュリティの向上につながる。ただし、実施規程や手順として定めた場合、そこには当然強制力が働くため、実施規程・手順のレベルで定めるか、ガイドライン・マニュアルのレベルで定めるかについては、慎重に検討する必要がある。

２．情報システムの運用・管理に係る手順等（C3101～C3104）の概要

(1) C3101 例外措置手順書

　大学の業務を遂行するに当たって、ポリシー及び関連する実施規程・手順が業務の適正な遂行を著しく妨げる等の理由により、そこに規定された方法とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。こうした場合において、情報セキュリティを維持しつつ柔軟に対応できるようにするための例外措置を定める。

(2) C3102 インシデント対応手順

　災害等によるネットワーク設備の損壊、利用者等による規定違反や学外から学内への攻撃行為等により発生したインシデントへの対応について、具体的な対応手順を定める。インシデントが発生した場合、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。対応を誤ると無用な被害の拡大を招くことが懸念されるため、インシデントの発見から対処にいたる手続きを定め、適切な対処を実施することが必要である。

(3) C3103 情報格付け取扱手順

　情報システムで取り扱う情報は格付けされ、格付けに応じて適切に取り扱う必要がある。取扱いが不適切なため、機密性が求められる情報の漏えい、完全性が求められる情報の改ざん等が生じた場合には、大学活動の停止や社会的信用の失墜の要因となる可能性もある。このようなリスクを軽減するため、教職員等が情報を適切に取り扱うために必要な事項を定める。

(4) C3104 情報システム運用リスク評価手順

　情報システムを適切に運用し管理するためには、情報システムに対するさまざまなリスクに応じて、適切かつ効率的、あるいは実現可能なセキュリティ対策を実施する必要がある。そうしたリスクを検討するための手順として、情報資産の洗い出し、脆弱性分析、資産価値判断、脅威の判断、リスク値の算出、対策の必要性判断について定める。

３．情報システムの運用・管理に係る手順等（C3101～C3104）の使い方

　これらの文書は、各大学が情報システムの運用・管理に係る実施手順等を作成する際の参考資料として提供されるものであり、実際の各大学の実施手順等がこれと同一の内容で作成されるものではない。各大学においては、サンプル規程集で定められた以上の情報セキュリティ確保を目標としながら、各大学の状況や特性を踏まえつつ、これらの文書を参考として実施手順等を策定する。文書の使い方として、本文書をそのまま取り込む、構成や表現を変えて盛り込む

等の方法がある。

４．事務情報セキュリティ対策基準との関係

　サンプル規程集では、事務局管理の情報及び情報システムと、その他の大学の研究教育業務に係る情報及び情報システムとで、規程体系を二分している。すなわち、「C2101 情報システム運用・管理規程」には本文書及びC3101～C3104の各手順が対応するのに対して、「C2501 事務情報セキュリティ対策基準」には「C3500 各種マニュアル類の策定に関する解説書」が対応する。事務情報システムに関連する文書（手順、ガイドライン及びマニュアル等）については、「C3500 各種マニュアル類の策定に関する解説書」を参照されたい。