C3500 各種マニュアル類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  A3500 | 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  C3500 | 他文書の改定に伴う参照内容の修正 | 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。

1. 本書の目的

　「高等教育機関の情報セキュリティ対策のためのサンプル規程集」（以下サンプル規程集）では、「C2501 事務情報セキュリティ対策基準」に基づいた情報セキュリティ対策実施手順書の雛形として「C3501 各種マニュアル類」を策定することとしている。「C2501 事務情報セキュリティ対策基準」は、「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」（以下政府機関統一基準）と「府省庁対策基準策定のためのガイドライン」（以下ガイドライン）における基本対策事項をもとにしており、その内容は用語の違いをのぞき、多くの部分で共通である。政府機関統一基準に準拠した実施手順書の雛形としては、「政府機関統一基準適用個別マニュアル群」（以下統一基準マニュアル群）と呼ばれる文書群が整備されている。よって事務情報セキュリティ対策基準に基づいた「C3501 各種マニュアル類」の作成に当たっては、統一基準マニュアル群を基とすることが適切である。

　一方、政府機関統一基準の平成24年度版から平成26年度版への改定において、大幅な変更が行われた結果、統一基準マニュアル群については平成24年度版までを対象とした文書群は更新対象外となり、平成26年度版に対応した新たな文書が作成・公表されることとなった。そこで本文書は、今後平成26年度版の政府機関統一基準に準拠した統一基準マニュアル群が改訂・追加されるのに備え、統一基準マニュアル群中の文書を基に「C3501 各種マニュアル類」を作成する際の手順および注意事項について記したものである。

1. 「C3501 各種マニュアル類」作成にあたっての基本的な考え方

　本文書で述べる「C3501 各種マニュアル類」とは、「C1001 情報システム運用基本規程」第三条四に定義された事務情報システムの運用にあたり、「C2501 事務情報セキュリティ対策基準」を満たした情報システムの操作もしくは電子化された情報資産の取り扱いを、各業務を担当する教職員等が容易に理解し実行できるようにまとめたものである。統一基準マニュアル群の構成は2015年9月現在、表１のようになっている。

表 1　政府機関統一基準適用個別マニュアル群の構成（2015年9月時点）

|  |
| --- |
| 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書 |
| スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書 |

1. 「C3501各種マニュアル類」作成の基本的な手順

　既に述べたように、政府機関統一基準及びガイドラインの基本対策事項と、「C2501 事務情報セキュリティ対策基準」は用語の違いをのぞいて多くの部分が共通であるため、統一基準マニュアル群の各文書に対し以下のような作業を行うことにより、効率的に「C3501 各種マニュアル類」等を作成することができる。

* 1. 用語の置換

　政府機関統一基準及びガイドラインと「C2501事務情報セキュリティ対策基準」の間にはのような用語の差異があるため、統一基準マニュアル群の各文書内の対応する用語を置き換えることによってある程度機械的に各種マニュアル類の雛形を作成することができる。ただし完全に機械的な置換を行うと表現が崩れる部分があるため、適宜修正する必要がある。また、中にない政府機関特有の用語が今後統一基準マニュアル群に表れる可能性もある。

表 2　政府機関統一基準とC2501の主な用語の対応

|  |  |  |
| --- | --- | --- |
|  | 政府機関統一基準 （府省庁等対象） | C2501 事務情報セキュリティ対策基準 （高等教育機関対象） |
| 役職名等 | 最高情報セキュリティ責任者 | 全学総括責任者 |
| 情報セキュリティ監査責任者 | 情報セキュリティ監査責任者 |
| 最高情報セキュリティアドバイザー | 情報セキュリティアドバイザー |
| 総括情報セキュリティ責任者 | 全学実施責任者 |
| 情報セキュリティ責任者 | 部局総括責任者 |
| 情報システムセキュリティ責任者 | 部局技術責任者 |
| 情報システムセキュリティ管理者 | 部局技術担当者 |
| 課室情報セキュリティ責任者 | 職場情報セキュリティ責任者 |
| 区域情報セキュリティ責任者 | 区域情報セキュリティ責任者 |
| 情報セキュリティ委員会 | 全学情報システム運用委員会　または　 部局情報システム運用委員会 |
| 利用者・関係者 | 行政事務従事者 | 事務従事者 |
| 国民 | 学生や学外利用者 |
| 職員 | 本学構成員 |
| 組織・施設 | 政府機関 | 本学 |
| （各）府省庁 | 本学　または　（各）部局 |
| 庁内または庁舎内 | 学内 |
| 業務 | 行政事務 | 事務 |
| 行政職務 | 職務 |
| その他 | 国民の権利が侵害され | 大学の運営に支障を及ぼす |

* 1. 情報セキュリティ対策基準の構成の違いに起因する修正

　政府機関統一基準は府省庁においては最上位に位置する規程であるが、「C2501事務情報セキュリティ対策基準」には上位規程として「C1001 情報システム運用基本規程」があり、事務情報以外を取り扱う情報システムに関する他の規程も並列に存在するため、それらとの整合性を取ることが必要である。特に事務情報以外を取り扱う情報システムに関するマニュアル等が作成された場合には、情報システム利用者が遵守するべきマニュアル等は事務情報システムにかかるものになるか否かで異なってくるため、利用者が混乱しないような工夫が求められる。例えば事務情報システムに関連するマニュアルを他の情報システムに関連するマニュアル内の対策基準全てを含むように記述し、事務情報システムを利用する可能性のある者には事務情報システム向けの各種マニュアル等で代替可能にするなどの措置が考えられる。

* 1. その他各大学固有の事情に応じた修正

　その他、各大学で「C2501事務情報セキュリティ対策基準」を基に施した修正等に関しては各種マニュアル類にも反映させる必要がある。