C2301 年度講習計画

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2月15日  A2301 | 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 |
| 2007年10月31日  A2301 | 教育テキスト作成ガイドラインの拡充に対応した修正及び追記 | 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 |
| 2013年7月5日  B2301 | 文書番号の変更のみ | － |
| 2015年10月9日  C2301 | 文書番号の変更のみ | － |

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。

解説：「C2101 情報システム運用・管理規程」において、利用者等に対する講習について「講習計画の定める講習」との定めがあるので、利用者向け年度講習計画を定めることになる。部局総括責任者、部局技術責任者及び部局技術担当者に対して「情報セキュリティ対策の教育」との定めがあり、これについてはその実施概要を部局で情報システムの運用管理に携わる者向けの講習計画の形で定めるのが良いと考えられる。また、役職者に対する教育についても講習計画の形で明確化することが望ましい。よって、ここでは利用者向け年度講習計画に加えて、システム管理者向けと役職者向けの講習計画も定めている。

１．適用範囲

　本文書は、以下の目的で実施される講習の年度計画について規定するものである。なお、いずれの講習とも、情報セキュリティ対策教育を単独で行う必要はなく、関連分野と合わせた講習の中で実施する形で差し支えない。

(1) 新たに大学の情報システムを利用することとなった学生、教職員等を対象とした、情報セキュリティ対策の基礎知識習得のための講習（以下、「基礎講習」と表記）

(2) (1)以外の利用者（教職員、学生等）を対象とした、最新状況への対応法等からなる情報セキュリティ対策の基礎知識習得のための講習（以下、「定期講習」と表記）

(3) 情報システム管理者を対象とした、運用に必要な情報セキュリティ対策の応用知識習得のための講習（以下、「システム管理者講習」と表記）

(4) 学長、事務局長、全学総括責任者（CIO）、部局総括責任者（部局長）を対象とした、大学運営における情報セキュリティ対策の基本的知識を理解するための講習（以下、「役職者講習」と表記）

解説：関連規程:「C1001 情報システム運用基本規程」C1001-5（第五条）、C1001-08（第八条）、「C2201 情報システム利用規程」C2201-07（第七条）

　なお、臨時職員、臨時利用者等、一時的に大学の設備を利用する利用者への教育については、本文書によらず、各利用者の利用条件に応じて必要かつ簡潔な教育を実施するものとし、本文書の適用範囲としない。

２．年度講習計画

　年度講習計画を策定する場合には、対象者と実施時期に応じて以下の４種類を区別し、それぞれの区分について実施時期と教育する内容を定めること。

(1) 基礎講習：学生の場合は入学・編入学後の関連講義の初回、もしくは利用者講習会において、また教職員については着任後の講習会において、情報システムを利用する際の事故やトラブルの発生を予防するために、事前に理解しておくべき知識を集中的に教育するもの

(2) 定期講習：すでに(1)を習得済みの利用者に対し、習得状況の維持・確認や最新動向の教育などを目的として実施するもの

(3) システム管理者講習: 情報システムの管理者に対して、技術面を中心として、法令なども含めて実施するもの

(4) 役職者講習：着任時および年1回（部局総括責任者については全学情報システム運用委員会等の席上で年1回）、本学における情報セキュリティの状況と、大学運営における情報セキュリティのあり方について実施するもの

３．計画例

(1) 基礎講習

　情報セキュリティ対策の基礎知識だけでなく、法令、マナー、学内関連諸規程について併せて教育を実施する。

| 講習時期 | 講習内容 | 備考 |
| --- | --- | --- |
| 4月～5月、 および10月 | A. 導入事項  ①事故から身を守るための知識  ・事故例と対策の必要性（導入として）  ②利用規則と罰則  ・目的外利用の禁止  ・大学設備・環境の損壊、重大な影響を及ぼす行為の禁止  ・他利用者への迷惑行為の禁止  ・パスワード等の適正管理  ③学内情報システムの基本理念  ・言論の自由、学問の自由  ・他者の生命、安全、財産を侵害しない  ・他者の人格の尊重  B. 情報セキュリティの基礎的知識  ・Internet のしくみ（IP address, URL, https）  ・virusとworm（感染兆候と予防対策+事後対策）  ・spyware（予防対策）  ・情報発信（個人情報、責任、Accessibility）  ・迷惑メール（対策）  ・phishing、架空請求（しくみと注意喚起、対策）  ・ファイル交換（情報漏洩、著作権）  C. マナー・関連法令  ①法令の遵守  ・個人情報・秘密情報の保護  ・不正アクセス行為の禁止  ・著作権・肖像権  ②利用上のマナー  ・社会慣行の尊重  ・ネットワーク利用のマナーの理解と尊重  ・運用への協力  ・ネット中毒  D. 便利な使い方  ・Webメール  ・学外から学内へのアクセス手段 | 講義「情報リテラシー」が必修の学科については、その講義の中で実施する。それ以外の学科では、情報メディアセンター主催の講習会を受講するものとする。教職員については、情報メディアセンター主催の教職員向け講習会を受講するものとする。  毎回の講義の中で、関連学習  内容に関連した情報セキュリ  ティに関する知識を習得させ  る |

(2) 定期講習

　最新の情報セキュリティ動向を教育するためのテキストを配布する。

| 講習時期 | 講習内容 | 備考 |
| --- | --- | --- |
| 6月～7月 | ・最近の脅威の動向  ・主要な情報セキュリティ対策の確認 | ｅラーニング形式による実施も検討 |

(3) システム管理者講習

　講義および、必要に応じて実習形式にて実施する。

| 講習時期 | 講習内容 | 備考 |
| --- | --- | --- |
| 4月～5月 | ・システム管理の重要性  ・最低限知っておくべきセキュリティ対策 | 講義初回時に、サーバ運用等に際して最低限必要なセキュリティ知識を初回に集中的に習得させる |
|  | （各回カリキュラムによる） | ２回目以降の講義で、カリキュラムに応じた知識の習得を図る（「C3302 教育テキスト作成ガイドライン（システム管理者向け）」参照） |

(4) 役職者講習

　簡単な資料を用いて短時間の報告により実施する。以下の計画のほか、重大インシデント発生の際には臨時で実施する。

|  |  |  |  |
| --- | --- | --- | --- |
| 役職 | 講習時期 | 講習内容 | 備考 |
| 学長、事務局長 | 着任時および年1回 | ・CIOによる本学の情報セキュリティ状況報告（体制・対策、事例）  ・テキスト：　状況報告資料 | 学長への状況報告は、詳細情報よりも、統計および重大インシデント（学外に対して重大な被害を与えたもの）の発生事例に重点をおく |
| 全学総括責任者（CIO） | 着任時および１年に１回 | ・大学運営における情報セキュリティのあり方  (1) 本学における情報セキュリティ状況  ・インシデント発生状況の詳細情報（扱い件数の統計）  ・重大インシデントの詳細な分析  (2) 情報セキュリティ対策に必要な措置  ・情報セキュリティ対策の必要性  ・情報セキュリティの責任体制  (3) 情報システムの構築・運用・インシデント対応  ・体制の整備に関する課題  ・体制の整備の方法  ・テキスト：　メディア教育センター教員が進講。「C3303 教育テキスト作成ガイドライン（CIO/役職者向け）」を参照。 |  |
| 部局総括責任者（各部局長） | １年に１回（全学情報システム運用委員会（または役員会、部局長会議など）の席上） | ・CIOが学内ケーススタディを出す。メディア教育センター教員が状況報告を補佐するのも可。  ・テキスト：　状況報告資料 | 状況報告には、ケーススタディと、統計がある。  状況報告は、ケーススタディが効果的。必要に応じて秘密扱い。  また、状況の分析を外部講師に依頼することも効果的。 |