D2301 年度講習計画

国立情報学研究所 学術研究プラットフォーム運営・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委員会

**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 | － |
| 2018年2月7日 | 全面改訂 | 上田浩（京都大学）  須川賢洋（新潟大学）  中西通雄（大阪工業大学） |
| 2019年12月27日 D2301 | 全面改訂 | 上田浩（法政大学）  須川賢洋（新潟大学）  中西通雄（大阪工業大学）  長谷川明生（中京大学） |
| 2024年3月26日  D2301 | 統一基準（令和5年度版）の改訂への対応 | 高等教育機関における情報セキュリティポリシー推進委員会事務局 |

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。

解説：大学における情報セキュリティに関する教育の必要性について  
情報セキュリティは、一般論として、組織とその事業の運営にとって質や継続性に重大な影響を及ぼしかねない要素である。大学の組織運営においてもそれはあてはまる。さらに、教育機関である大学にとって、学生に対して情報セキュリティに関する教育を行い、情報を取り扱うために必要な資質を習得させることも欠かせない。  
大学では多くの場合に、コンピュータのネットワーク接続やシステム設定のような管理業務を、「情報部」のような部署が一元的に行うのではなく、部局や研究室、事務室ごとにいわゆる「管理者」を定めて委ねていることが多いと考えられる。したがって、情報セキュリティの維持のために多くの「管理者」への教育も欠かせない。

解説：「D2101 情報セキュリティ対策基準」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。

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）

解説：一般利用者向け教育（基礎講習、定期講習）について  
これは、情報処理演習で情報教育システムや情報ネットワークを利用する立場の学生や、事務情報システムを端末やPCから利用する一般職員などを想定している。これらの対象者には、それらの利用に関して法律や学内規程によって定められている順守事項や許諾範囲、あるいはマナーや心がけるべきことがあることを理解させることができるように、教育しなければならない。  
これらの対象者は情報システムやネットワークの設定操作や運用のような管理について権限をもたず、それに関する責任もないと考えられるので、管理に関する教育は必要がない。ただし、規定されている内容を利用者が理解するための最低限の技術的な知識も教育内容に含まれる。  
一般利用者向けの教育は、学生の入学あるいは教職員の採用のときのように、新たな利用者に加わった者を対象として実施する「基礎講習」が基本である。これは、1年生の情報処理演習の講義や、あるいは新規採用者講習の中で実施することも考えられる。そのほかに、定期的な再教育と、技術面や法律・制度面の最新知識を習得させるために「定期講習」も行う。

(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）

解説：システム管理者向け教育  
A大学には、全学的な情報システムを設置し運用する情報メディアセンターのほかに、部局や研究室でウェブサーバや電子メールサーバなどの情報システムを運用することがある。そのいずれのケースでも、情報セキュリティを高いレベルで維持できるように運用管理しなければならない。したがって、その管理を担当するシステム管理者に対して、情報セキュリティ対策の応用知識を定期的に教育する必要がある。  
情報メディアセンター以外の一般の部局におけるシステム管理者に対しては、部局における運用に必要な技術や状況などの知識を習得させるために「部局管理者」向けの教育を講習会などのスタイルで情報メディアセンターが実施する。  
システム管理者のうち、情報メディアセンターの教職員については、とくに専門的分野に携わっていることから、他の部局の管理者と分けて教育を実施することが適当と考えられる。これは情報メディアセンターが内部的に実施するものであるが、学外のセミナー等を利用する方法もとりうる。  
なお、たとえばPC一台ごと、ネットワーク機器一台ごとについて適切なシステム管理が必要であって、PCやネットワークを設置する者には管理者責任を負えるような専門的知識の教育をなすべきであるという考え方があり、あるいはPCやネットワーク機器の設置を何らかの有資格者に限定すべきであるというような考え方もあり、厳密にはそうしなければならない。しかし一方で、専門的知識を習得した管理者をすべてのPCについて割り当てることは、多くの大学において現実的ではないことが考えられ、たとえば一般利用者とシステム管理者の中間的な位置づけの教育を実施する考え方もありうる。

(4) 学長、事務局長、全学総括責任者（CISO）、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：CISO/役職者向け教育について  
大学の運営、とくに業務遂行とそのための予算配分と人員配置に責任のある執行部（理事会、事務局長、CIOなど）を対象とする教育は、情報セキュリティ対策の必要性と課題について理解を得るためのものである。その内容は、技術などの各論的知識ではなく、情報セキュリティのためのコスト（人と予算）の理解を得て、また、状況を的確に把握して、必要な対策を指揮できるように備えておくことである。

　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：なぜ情報セキュリティを考える必要があるか？   1. 情報セキュリティの定義 2. 大学におけるインシデント事例の紹介 3. 学内関連規程と情報セキュリティポリシーの遵守   B. 情報セキュリティに関連する技術   1. 全学情報システムの使い方 2. ネットワーク基礎(TCP/IP, Wi-Fi, Web, 電子メール) 3. 技術的脅威と対策  * マルウェア * Webに関連する脅威 * 電子メールに関連する脅威   C. 情報セキュリティに関連する法律   1. サイバーセキュリティ基本法 2. 個人情報, プライバシー, 肖像権への配慮 3. コンピュータ犯罪の禁止  * 不正アクセス * データ破壊とウイルス作成  1. 知的財産や機密情報の保護  * 著作権 * 不正競争防止法   D. 情報セキュリティに関連する倫理   * 全学情報システムの利用にあたって * 情報発信 * アクセシビリティ * ネット依存症 | 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 |

(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 |  |
| 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。 |

解説：大学における情報セキュリティ教育のテキストについて  
情報セキュリティ教育のそれぞれの種別について、教育を実施する際のテキスト（あるいは教材）が必要である。一般利用者を対象とする教育のうち、一般論については市販の教科書（情報処理演習の一部としているものを含む）を利用することもありうる。しかし、いずれの種別の教育でも各大学の情報セキュリティポリシーや情報システムサービスなどによって具体的な情報に関する内容が異なるので、その情報についてテキストを独自に準備することが必要になる。とくに、CIO/役職者向け教育はその大学における情報セキュリティの状況を説明することが重要であるから、そのときの状況を取り入れた説明資料を情報メディアセンターにおいて作成することが必要になる。  
サンプル規程集に収録している「D3301 教育テキスト作成ガイドライン(一般利用者向け)」は、基礎講習及び定期講習において教育すべき内容の参考として、ガイドラインの形式で示すものである。