C1001 情報システム運用基本規程

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  A1001 | 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  A1001 | 一部語句の調整と解説の追記 | 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 |
| 2011年3月31日  A1001 | 定義の見直し及び担当者の役割に関して不明確であった一部の条文を修正 | 冨士原裕文（富士通） |
| 2013年7月5日  B1001 | 文書番号の変更のみ | － |
| 2015年10月9日  C1001 | C2101の改定内容と整合をとるための用語定義等の見直し | 金谷吉成（東北大学） |

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。

C1001-01　（目的）

第一条　本規程は、Ａ大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め、もって本学の保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

C1001-02　（適用範囲）

第二条　本規程は、本学情報システムを運用・管理するすべての者、並びに利用者及び臨時利用者に適用する。

解説：来学中に利用する訪問者や受託業務従事者などの臨時利用者を含む。

C1001-03　（定義）

第三条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。  
(1) 本学により、所有又は管理されているもの  
(2) 本学との契約あるいは他の協定に従って提供されるもの

解説：情報ネットワークに接続されている情報処理システムだけではなく、スタンドアロンの情報処理システムも含まれる。また、上記の二つの項目に該当しない機器、例えば私物PCであっても本学の情報ネットワークに接続する時は本規程の対象となる。第五号の事務情報システムは情報システムに含まれるので、ここで定義してもよい。

二　情報

　情報には次のものを含む。

(1)　情報システム内部に記録された情報

(2)　情報システム外部の電磁的記録媒体に記録された情報

(3)　情報システムに関係がある書面に記載された情報

解説：情報には、ネットワークに接続している、いないに関わらず情報処理システムの内部に記録されている情報、及び情報システム外部の電磁的記録媒体に記録された情報、その情報を印刷した紙も含まれる。情報システムの運用管理に関する資料（仕様、設計、運用、管理、操作方法などの資料）を含む考え方もありうる。

三　情報資産

情報システム並びに情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。

四　事務情報

　事務情報とは情報のうち次のものをいう。

(1) 「法人文書の管理に関する規程」の対象となる法人文書

(2)　(1)以外の法人文書で、部局長が指定した文書

五　事務情報システム

　事務情報を扱う情報システムをいう。

解説：事務情報システムには、事務局が運用責任を持つ情報システムばかりではな  
く、教員等が成績管理に使用するパソコン等も含まれる。

六　ポリシー

　本学が定める「C1000 情報システム運用基本方針」及び「C1001 情報システム運用基本規程」をいう。

七　実施規程

ポリシーに基づいて策定される規程及び、基準、計画をいう。

八　手順

実施規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

九　利用者

教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。

解説：利用者とは本学情報システムを単に使用するだけではなく、パソコンをはじめとした機器を情報ネットワークに接続して使用する者を含む。教職員等及び学生等に限定しない考え方もありうる。第十二号の臨時利用者は関連するので、ここで定義しても良い。

十　教職員等

本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局総括責任者が認めた者をいう。

解説：同窓会、生協、TLO、インキュベーションセンター、地域交流センター、財団などの職員を含む考え方もある。また、受託業務従事者についても委託業務の内容に応じて教職員として扱う考え方もある。学内規定の体系の中で「教職員」「学生」が定義されているならば、第十号と第十一号は省略可能であるが、定義に含む範囲に注意が必要である。

十一　学生等

本学通則に定める学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。

十二　臨時利用者

教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

解説：訪問者や受託業務従事者などの本学構成員以外の者が本学情報システムを臨時に利用する場合は、所定の手続きで身元を確認した上で、ポリシー及び関連規程を遵守することを条件に利用を許可するものとする。

十三　情報セキュリティ

　　情報資産の機密性、完全性及び可用性を維持することをいう。

解説：情報セキュリティには、情報資産の機密性、完全性及び可用性を維持することが含まれ、適切なアクセス制限を確保するとともに、情報を保全して一貫性を確保し、利用に支障が生じないように対策を施すことが求められる。また、情報セキュリティが損なわれた場合に、その情報資産だけではなく、社会的評価が損なわれたり、他者への二次的損害を与えたりするなど、被害が拡大することもあるので、多面的な情報セキュリティ対策が必須である。

十四　電磁的記録

　　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

解説：法律の定める「電磁的記録」の定義である。電子的方式、磁気的方式に限らず、媒体の化学変化を応用する方式や紙面上の記録方式であっても、人の知覚による認識ができず、コンピュータシステムによる記録と読取を目的としたものはこれに含まれる。一方、マイクロフィルムのように人の知覚による認識を前提とした方式を用いた記録は含まない。

電磁的記録として扱われる記録方式を用いる媒体の例：

メモリ、ハードディスク、CD、DVD、光磁気(MO)ディスク、磁気テープ、

磁気カード、ICカード、二次元バーコード（QRコード等）

電磁的記録ではないものの例：

人の知覚による認識を目的としたコンピュータからの印刷出力、

入力用に記入する伝票、フォーム等の帳票類、マイクロフィルム

十五　情報セキュリティインシデント

　　情報セキュリティに関し、意図的または偶発的に生じる、本学規程または法律に反する事故あるいは事件をいう。

解説：情報セキュリティインシデントの例としては、地震等の天災、火災、事故等によるネットワークを構成する機器や回線の物理的損壊や滅失によるネットワークの機能不全や障害、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等がある。その疑いがある場合及びそれに至る行為もこれに準じて扱うことが適当であろう。

十六

　　本学において発生した情報セキュリティインシデントに対処するため、本学に設置された体制をいう。Computer Security Incident Response Teamの略。

十七　明示等

情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

解説：情報ごとに格付けを記載することにより明示することを原則とするが、その他にも、当該情報の格付けに係わる認識が共通となる措置については、明示等に含まれる。例えば、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等に明記し、当該情報システムを利用するすべての者に当該規定を周知することができていれば明示等に含むものである。

C1001-04　（全学総括責任者）（政府機関統一基準の対応項番2.1.1(1)）

第四条　本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置く。学長がこれを任命する。

２　全学総括責任者は、ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を行う。

解説：その業務に関する予算と人事の権限および責任を有する副学長あるいは理事に相当する者が望ましい。全学総括責任者は、いわゆる最高情報責任者（CIO）の役を務める。  
いわゆる最高情報セキュリティ責任者（CISO）と同じ者を充てる考え方と、相互チェックのために異なる者を充てる考え方とがありうる。

３　全学総括責任者は、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

４　全学総括責任者は、全学向け教育及び全学情報システムを担当する部局技術担当者向け教育を統括する。

５　全学総括責任者に事故があるときは、全学総括責任者があらかじめ指名する者が、その職務を代行する。

６　全学総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置く。

解説：情報セキュリティに関する専門家を情報セキュリティアドバイザーとして置くことを定めた事項である。本学における情報セキュリティ対策については、情報システムに関する技術や事案に対する対処等の専門的な知識及び経験が必要となるため、実施規程の策定・導入から運用、評価、見直しまで専門的な助言を行う専門家を活用することが重要である。  
全学総括責任者が、情報システムに関する専門的な知識及び経験を高度な水準で有しているため、専門家の助言を必要としないといった特殊な場合を除き、置くことを義務付けているものである。なお、情報セキュリティアドバイザーはいわゆるCIO補佐官に相当すると考えられる。

C1001-05　（全学情報システム運用委員会）（政府機関統一基準の対応項番2.1.1(2)）

第五条　本学情報システムの円滑な運用のための最終決定機関として、本学に全学情報システム運用委員会を置く。

解説：全学総括責任者が主宰し、本学情報システムの目的に合致した健全な運用と利用を実現できるよう、情報システム運用に関する決定を行う。  
情報システムのセキュリティに関する最終決定機関としての役割を兼ねる考え方と、あるいは別の機関を設ける考え方がある。委員会形式とは限らない。

２　全学情報システム運用委員会は以下を実施する。

一　ポリシー及び全学向け教育の実施ガイドラインの改廃

二　情報システムの運用と利用及び教育に係る規程及び手順の制定及び改廃

解説：情報システムの運用と管理及び管理者に関することについて、情報システム運用・管理規程を定める。  
情報システムの円滑な運用のために、情報システムの利用及び利用者に関することについて情報システム利用規程を定めて、利用者に対して制約を課す。  
利用者は、契約等により本学情報システムを利用する権利を有するが、その利用に伴うすべての行動について責任を自覚しなければならない。本学情報システムを利用した情報発信は本学内にとどまらず、社会へ広く伝達される可能性があることを自覚し法令遵守等、責任をもった行動が望まれる。また、目的に示す基本理念を大きく逸脱するような私的利用や商業利用は制限される。  
本学情報システムの運用においては、表現の自由とプライバシーに最大限配慮するが、第三者に対する誹謗中傷や名誉毀損、著作権侵害等と判断されるコンテンツを制限する場合がある。また、利用者の通信の秘密を尊重するが、ネットワークの円滑な運用のため、必要最小限の範囲において通信ログを保存・調査する場合がある。このほか、上位ネットワークプロバイダの定める利用規約（AUP）の制約もありうる。  
情報システム運用委員会が実施する教育を受講し内容を十分理解の上、所定の手続きをとりポリシー及び関連規程の遵守を承諾した者に本学情報システムを利用する許可（アカウント等）が与えられる。利用者が、本学情報システムに接続する機器を持ち込み使用する場合は、別途定める基準に従うものとする。

三　情報システムの運用と利用に関する教育の年度講習計画の制定及び改廃、並びにその計画の実施状況の把握

解説：利用者に対して、情報セキュリティ管理の内容を周知しポリシーの他、必要な実施規程及び、関連する実施手順の遵守を図るため、毎年、年度講習計画を策定し、教育・啓発を実施する。

四　情報システム運用リスク管理規程の制定及び改廃、並びにその実施状況の把握

解説：リスク分析と対策手順の策定について、情報システム運用リスク管理規程を定める。

五　情報セキュリティ監査規程の制定及び改廃、並びにその実施

解説：情報システム運用について、定期的な見直しを行うとともに、学内外の適切な者による監査等を実施し、その結果に基づいた必要な改善を行うことを情報セキュリティ監査規程として定める。  
情報システムに係る情報セキュリティ監査の実施は、リスク分析結果、実施手順の整合性及びその実施状況について行う。情報セキュリティ監査業務の一部又は全部を、本学以外の事業者に委託することができる。情報セキュリティ監査の実施にあたっては、個人情報を関係者以外に開示してはならない。

六　情報システム非常時行動計画の制定及び改廃、並びにその実施

解説：不測の事態への対応手順を定める情報システム非常時行動計画（contingency plan）の実施には、情報システムの運用と利用に関する事件、事故の発生時の対応が含まれる。  
情報システム非常時行動計画を作成して、コンピュータ犯罪等の事件や情報セキュリティ事故、災害等のトラブルが発生した場合の連絡体制及び対応手順を整備し、これをあらかじめ関係者に周知しておく。これには、外部からの苦情等、トラブルの通知について受付窓口を設置し、エスカレーションルールを定めることも含まれる。  
トラブルが発生した場合には、情報システム非常時行動計画に従って速やかに緊急対策チームを編成するとともに、適切な対応を行う。トラブル対応が完了した後も、トラブル原因を究明し、その対策をポリシー等に反映し、トラブルの再発防止に努める。

七　情報セキュリティインシデントの再発防止策の検討及び実施

C1001-06　（全学情報システム運用委員会の構成員）（政府機関統一基準の対応項番2.1.1(2)-1）

第六条　全学情報システム運用委員会は、委員長及び次の各号に掲げる委員をもって組織する。

一　全学実施責任者

二　部局総括責任者

三　部局技術責任者

四　その他全学総括責任者が必要と認める者

解説：全学総括責任者は委員長としてこの委員会の構成に含まれ、次の条で規定されている。

C1001-07　（全学情報システム運用委員会の委員長）（政府機関統一基準の対応項番2.1.1(2)-1）

第七条　全学情報システム運用委員会の委員長は、全学総括責任者をもって充てる。

２　委員長は、会務を総理する。

C1001-08　（全学実施責任者）（政府機関統一基準の対応項番2.1.1(4)(a)）

第八条　本学に全学実施責任者を置く。

解説：本学情報システムについて、構成の決定などの整備と、技術的問題（第２項）と教育（第３項）及び連絡・通報窓口（第４項）を含む運用に関する事項を実施する者である。  
全学実施責任者は管理運営部局のセンター長や上級の職員が想定されるが、全学総括責任者が兼務する考え方もありうる。

２　全学実施責任者は、全学総括責任者の指示により、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく規程並びに手順等の実施を行う。

３　全学実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用並びに利用及び情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

４　全学実施責任者は、本学の情報システムのセキュリティに関する連絡と通報において本学情報システムを代表する。

５　全学実施責任者は、全学総括責任者の推挙により学長が任命する。

C1001-09　（情報セキュリティ監査責任者）（政府機関統一基準の対応項番2.1.1(3)）

第九条　全学総括責任者は、情報セキュリティ監査責任者を置く。

２　情報セキュリティ監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

解説：本ポリシーに基づき監査を行う責任者を定めた事項である。  
情報セキュリティ監査責任者は、部局総括責任者が所管する組織における情報セキュリティ監査を実施するため、情報セキュリティ対策を実行する各責任者と兼務することはできない。  
監査の実効性を確保するために、部局総括責任者より職務上の上席者を情報セキュリティ監査責任者として置くことが望ましい。  
このサンプルと異なって全学総括責任者から独立させて、本学に情報セキュリティ監査責任者を置くことと学長が任命することを定めて、全学総括責任者の指示に基づくことを削除する考え方もありうる。  
情報セキュリティ監査責任者は、本学の情報セキュリティに関する情報を共有するために、全学情報システム運用委員会にオブザーバとして参加することが望まれる。情報セキュリティ監査責任者の業務を補佐するために、各部局内及び部外の担当者を置く必要性を検討することが望まれる。また、業務の実効性を担保するために外部組織の活用も考えられる。  
本学に監査室のような組織があったとしても、それをここの監査責任者あるいは実施組織とできるかについて、情報セキュリティ監査の業務を担当するために適格かの確認を要する。

C1001-10　（管理運営部局）

第十条　全学情報システム運用委員会は、本学情報システムの管理運営部局を定める。

解説：規程の中で管理運営部局を定めても良い。  
例えば、事務局総務部である。ただし、幹線ネットワークと外部ネットワーク接続の運用は情報メディアセンターの業務であるし、情報メディアセンターを管理運営部局とする考えもある。

C1001-11　（管理運営部局が行う事務）

第十一条　管理運営部局は、全学実施責任者の指示により、以下の各号に定める事務を行う。

一　全学情報システム運用委員会の運営に関する事務

二　本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ

三　講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ

四　本学の情報システムのセキュリティに関する連絡と通報

C1001-12　（部局総括責任者）（政府機関統一基準の対応項番2.1.1(4)(a)）

第十二条　各部局に部局総括責任者を置く。部局長が任命する。

解説：部局内情報システムの運用に責任を持つ者である。VPNなどによる拡張ネットワークの部分を含む。学部長が兼ねても良いし、あるいは学部長をもって充てることを規定しても良い。

２　部局総括責任者は、部局における運用方針の決定や情報システム上での各種問題に対する処置を担当する。

C1001-13　（部局情報システム運用委員会）

第十三条　各部局に部局情報システム運用委員会を置く。

２　部局情報システム運用委員会は以下の各号に掲げる事項を実施する。

一 部局におけるポリシーの遵守状況の調査と周知徹底

二　部局におけるリスク管理及び非常時行動計画の策定及び実施

三　部局における情報セキュリティインシデントの再発防止策の策定及び実施

四　部局における部局技術担当者向け教育の計画と企画

C1001-14　（部局情報システム運用委員会の構成員）

第十四条　部局情報システム運用委員会は、委員長及び次の各号に掲げる者を委員として組織する。

一　部局技術責任者

二　部局技術担当者

三　その他部局総括責任者が必要と認める者

C1001-15　（部局情報システム運用委員会の委員長）

第十五条　部局情報システム運用委員会の委員長は、部局総括責任者をもって充てる。

C1001-16　（部局技術責任者）（政府機関統一基準の対応項番2.1.1(4)(d)）

第十六条　部局に部局技術責任者を置く。部局長が任命する。

解説：部局総括責任者は部局技術責任者を兼務することができる。

２ 部局技術責任者は、部局情報システムの構成の決定や技術的問題に対する処置を担当する。

３　部局技術責任者は、部局技術担当者に対して、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

C1001-17　（部局技術担当者）（政府機関統一基準の対応項番2.1.1(4)-6）

第十七条　部局技術責任者は、当該部局の情報システムの管理業務において必要な単位ごとに、部局技術担当者を置く。部局技術担当者は部局技術責任者が推挙し部局長が任命する。なお、部局技術責任者自ら部局技術担当者を兼務することができる。

２　部局技術担当者は、部局技術責任者の指示により、部局の情報システムの運用の技術的実務を担当し、利用者への教育を補佐する。

解説：例えば、部屋ごとに1名を任命する。情報コンセントや無線アクセスポイントの場合には、接続する者ではなく設置者側から任命する。VPNなどによる外部への拡張ネットワークの接続サーバには必ず置く必要がある。  
部局の規模が大きいケースでは、部局技術担当者が多数になるので、学科や建物など適切な単位で中間的なグループ化を設けたほうが良いこともある。部局技術担当者として任命される者の要件については、大学職員であることが考えられるが、運用の実態と齟齬が生じないように定める。

C1001-18　（区域情報セキュリティ責任者の設置）（政府機関統一基準の対応項番2.1.1(4)(b)）

第十八条　部局総括責任者は、施設及び環境に係る対策を行う単位ごとの区域を定め、その区域ごとに、区域情報セキュリティ責任者1人を置く。

２　区域情報セキュリティ責任者は、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を総括する。

解説：「C2101 情報システム運用・管理規程」第五十四条第１項（区域ごとの対策の決定）で定める区域ごとに、当該区域における情報セキュリティ対策の事務を総括する者を置くことを定めた事項である。  
「施設及び環境に係る対策を行う単位ごとの区域」には、教室、研究室、事務室やサーバ室だけでなく、建物内のロビーや廊下といった区域も含まれる。そのため、本学において漏れなく情報セキュリティ対策を実施する観点から、それぞれの区域に区域情報セキュリティ責任者を置く必要がある。  
「対策を行う単位」は、当該区域の利用用途や設置環境等を勘案して、例えば、  
・部局又は研究室単位で管理している部屋（会議室等）ごと  
・情報システムが設置された部屋（サーバ室等）ごと  
等とすることが挙げられる。また、上記以外の区域（ロビー、廊下等）を一つの区域とする場合も考えられる。  
区域情報セキュリティ責任者は、所管する区域について規定された対策の基準に従い、自ら対策を定めそれを実施する。また、区域情報セキュリティ責任者は、その役割の性質上、施設の管理者が兼任することが想定される。定める単位としては、例えば以下が考えられる。  
・単一の研究室が利用する部屋（会議室等）を管理する場合は、職場情報セキュリティ責任者  
・複数の研究室が利用する部屋（会議室等）を管理する場合は、部局総括責任者  
・情報システムが設置された部屋（サーバ室等）を管理する場合は、部局技術責任者  
・異なる区域（クラスが異なる場合も含む）をまとめて管理する場合は、部局総括責任者  
・教室、研究室、事務室又はサーバ室以外の区域（ロビー、廊下等）を管理する場合は、建物等の管理に関する部門の責任者  
なお、「C2101 情報システム運用・管理規程」第五十三条第１項（要管理対策区域における対策）で規定するクラス１は、施設管理の観点から行う措置が、情報セキュリティ上の対策と同等であれば、施設管理者が指定されていることをもって、区域情報セキュリティ責任者を設置しているとみなしてよい。

C1001-19　（職場情報セキュリティ責任者の設置）（政府機関統一基準の対応項番2.1.1(4)(c)）

第十九条　部局総括責任者は、教室、研究室、事務室等の管理組織ごとに、職場情報セキュリティ責任者1人を置く。

２　職場情報セキュリティ責任者は、教室、研究室、事務室等の管理組織における情報の取扱いその他の情報セキュリティ対策に関する事務を総括する。

解説：教室、研究室、事務室等の管理組織単位での情報セキュリティ対策の事務を統括する者を置くことを定めた事項である。  
職場情報セキュリティ責任者は、所管する事務や利用者等における情報の取扱い等に関して、その是非を判断し、情報の持ち出しや公開等についての責任を有する者であり、例えば、部局においては部局長（部局総括責任者）、研究室においては教授、委員会等においては当該委員会等の委員長、医局においては医局長、事務組織内の課室においては課室長などが想定される。部局総括責任者が教室、研究室、事務室等の管理組織ごとに1人任命するものである。

C1001-20　（全学情報セキュリティアドバイザーの設置）（政府機関統一基準の対応項番2.1.1(5)）

第二十条　全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置く。

２　全学総括責任者は、以下を例とする全学情報セキュリティアドバイザーの業務内容を定める。

一　本学全体の情報セキュリティ対策の推進に係る全学総括責任者への助言

二　情報セキュリティ関係規程の整備に係る助言

三　対策推進計画の策定に係る助言

四　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

五　情報システムに係る技術的事項に係る助言

六　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

七　利用者に対する日常的な相談対応

八　情報セキュリティインシデントへの対処の支援

九　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

解説：全学総括責任者は、情報セキュリティに関する技術的事項等について自らへの助言等を含む本学の情報セキュリティ対策への助言、支援等を行う者として全学情報セキュリティアドバイザーを置く。  
全学情報セキュリティアドバイザーは、本学における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち情報セキュリティに関する資格及び実務経験を有する者である必要がある。  
なお、外部人材のみならず学内の職員を充ててもよい。この場合、当該職員が部局総括責任者やその他の責任者を兼務してもよい。

C1001-21　（情報セキュリティインシデントに備えた体制の整備）（政府機関統一基準の対応項番2.1.1(6)）

第二十一条　全学総括責任者は、CSIRTを整備し、その役割を明確化する。

２　全学総括責任者は、教職員等のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本学における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置く。

３　全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

解説：本学の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、本学が、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備することが必要である。  
一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRTは、時々刻々と明らかになる情報を基に、状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で幹部に状況を報告する。  
  
CSIRTに属する職員は、本学における情報セキュリティインシデントを認知した際、全学総括責任者の指揮の下、これに対処する職員であることから、全学総括責任者に対して適切に状況を報告し、全学総括責任者の指示を受け適切に対処できることが必要である。  
現場の対処においては、情報セキュリティ、情報システム等に関する知識及び技能を持つ者で、本学のネットワーク構成や個別システムの部局技術責任者及び管理者を把握している職員が当たることが望ましい。  
また、CSIRTに属する職員には、上述した技術的な対処のほか、発生した情報セキュリティインシデントの影響の大きさによっては、対外的な対応も必要となることから、広報を担当する職員をCSIRTに含めておくことも考えられる。  
  
CSIRT責任者とは、情報セキュリティインシデントの対処に係る責任者であり、情報セキュリティインシデントに関する全般的な対応が求められる。ただし、重大な情報セキュリティインシデントが生じ、全学総括責任者自らが、情報セキュリティインシデントへ対処する必要があるときには、その指揮監督の下で必要な対応を行うこととなる。  
  
CSIRT責任者が情報システムを所管している場合、当該情報システムの情報セキュリティインシデントを認知した際、二つの役職が利害相反関係にあることから、全学総括責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。  
これを避けるため、例えば、CSIRT責任者には部局総括責任者以外の者を充てる、全学総括責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途CSIRT責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保することが必要である。

C1001-22　（CSIRTの役割）（政府機関統一基準の対応項番2.1.1(6)-1,2）

第二十二条　全学総括責任者は、以下を含むCSIRTの役割を規定する。

一　報告窓口からの情報セキュリティインシデントの報告の受付

二　情報セキュリティインシデントの全学総括責任者等への報告

三　対外的な連絡

四　被害の拡大防止を図るための応急措置の指示又は勧告

２　全学総括責任者は、CSIRTの代表者（PoC（Point of Contact））を置く。

解説：CSIRTの代表者は、学内外の関係機関と必要に応じて、情報セキュリティインシデントに関する情報共有を行うなど、外部窓口の役割を担うことが想定される。

C1001-23　（役割の分離）（政府機関統一基準の対応項番2.1.1(7)）

第二十三条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

　一　承認又は許可事案の申請者とその承認又は許可を行う者（以下、本項において「承認権限者等」という。）

　二　監査を受ける者とその監査を実施する者

解説：承認又は許可する役割の者自らが、申請をする場合には、その申請について自らが承認又は許可することはできない。このため、組織・体制及び申請手続を整備するに当たっては、このことに十分留意する必要がある。

２　前項の定めに係わらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。

解説：承認や許可事案の内容によっては、承認権限者等が承認等の可否の判断を行うことが適切でない場合も想定される。このような場合は、その上司に申請し承認等を得ることになる。  
なお、「兼務を禁止する役割の規定」を遵守する必要がある。したがって、自らが承認権限者の上司であったとしても、当該上司は自らに係る承認等の事案について自らが承認等してはならない。

３　教職員等は、前事項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

解説：承認権限者等の上司が承認等を行った場合に、当該上司に当該承認権限者等が遵守すべき事項に準じて、措置を講ずることを求める事項である。  
例えば、機密性３情報、完全性２情報又は可用性２情報について、本学外での情報処理や本学支給以外の情報システムによる情報処理を職場情報セキュリティ責任者に代わって、その上司が許可する場合は、その上司に対して、許可の記録を取得することなどが求められる。

C1001-24　（情報の格付け）

第二十四条　全学情報システム運用委員会は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規定を整備する。

解説：本学情報システムで取り扱う情報に対し、格付けを行うために必要となる基準等を定めることを求める事項である。なお、本規程に基づく情報の格付けについては「C2104 情報格付け基準」を参照されたい。  
なお、本条項では政府機関統一基準に準拠し、書面については機密性の観点のみを考慮すればよいこととしているが、情報の格付け等の実施に際しては、情報システムに関する設計書等の書面についても完全性や可用性の観点から考慮することが望ましい。

C1001-25　（学外の情報セキュリティ水準の低下を招く行為の防止）

第二十五条　全学実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規定を整備する。

解説：学外の情報セキュリティ水準の低下を招く行為の防止に関して、全学実施責任者が、規定を整備することを求める事項である。学外の情報セキュリティ水準の低下を招く行為としては、例えば、以下のものが挙げられる。  
・本学のウェブのコンテンツを利用するために、ブラウザのセキュリティ設定の下方修正を明示的に要求する行為  
・本学のウェブにより実行形式のファイル（Windows® の場合、「.exe」ファイル）を提供（メールに添付する場合も同様）する行為  
・本学のウェブにより署名していない実行モジュール（Java® アプレットやWindows® のActiveX® ファイル）を提供する行為  
・本学からHTML メールを送信する行為  
なお、後者の２つについては、利用者のウェブブラウザ等のセキュリティ設定の下方修正を誘発する可能性がある行為である。

２　本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

解説：学外の情報セキュリティ水準の低下を招く行為の防止に関する各部局の役割を定めた事項である。本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、組織及び個人として措置を講ずることが重要である。

C1001-26　（情報システム運用の外部委託管理）

第二十六条　全学総括責任者は、本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

解説：その際、当該第三者との契約等により責任の範囲を明確にしておくものとする。

C1001-27　（情報セキュリティ監査）

第二十七条　情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシー（情報システム運用基本方針及び本規程）に基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める情報セキュリティ監査規程に従う。

解説：情報セキュリティの確保のためには、本ポリシーに基づく実施規程、手順が適切に運用されることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、独立性を有する者による情報セキュリティ監査を実施する必要がある。

C1001-28　（見直し）

第二十八条　本ポリシー、実施規程及び手順を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

解説：本ポリシーに基づく実施規程、手順の内容を、必要に応じて見直すことを求める事項である。見直しを行う時期は、新たなセキュリティ脅威の出現、監査の評価結果等により、セキュリティ対策に支障が発生しないように本ポリシーに基づく実施規程、手順を整備した者が判断する必要がある。  
情報セキュリティ対策の課題及び問題点に対処するため本ポリシーに基づく実施規程、手順を見直した者は、当該規定を見直した者が所属する部門以外の部門においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、その課題及び問題点に関連する部門の本ポリシーに基づく実施規程、手順を整備した者に対しても、同種の課題及び問題点の有無を確認するように連絡することを推奨する。

２　本学情報システムを運用・管理する者、並びに利用者及び臨時利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。

解説：本ポリシーに基づく実施規程、手順としては整備されていない情報セキュリティ対策についても、その見直しを本学情報システムを運用・管理する者、並びに利用者及び臨時利用者に求める事項である。