D1001 情報セキュリティ対策基本規程

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） |
| 2017年10月17日  C1001 | 統一基準（平成28年度版）の改訂への対応とC1101との整合性確保 | 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 |
| 2019年12月27日  D1001 | 統一基準（平成30年度版）の改訂への対応と全体的な方針の見直し | 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。

D1001-01　（目的）

第一条　本規程は、Ａ大学（以下「本学」という。）における情報及び情報システムの情報セキュリティ対策について基本的なな事項を定め、もって本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

D1001-02　（適用範囲）（政府機関統一基準の対応項番1.1(2)）

第二条　本規程において適用対象とする者は、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とする。

解説：情報システムを運用・管理するすべての者とは、主としてポリシーに規定される全学総括責任者、全学実施責任者、情報セキュリティ監査責任者、部局総括責任者、部局技術責任者、部局技術担当者、区域情報セキュリティ責任者、職場情報セキュリティ責任者、全学情報セキュリティアドバイザー、及び全学／部局情報セキュリティ委員会を指すが、教職員や学生等のいわゆる一般利用者にあっても、本学の情報システムの運用・管理を行う場合はこれに該当する。

解説：臨時利用者には、来学中に利用する訪問者や受託業務従事者等を含む。

２　本規程において適用対象とする情報は、以下とする。

一　教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

二　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報

三　第一号及び及び第二号のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。

解説：情報システムには、学外に設置されているが本学の業務に利用されるクラウドサービスも含まれる。

D1001-03　（用語定義）（政府機関統一基準の対応項番1.3）

第三条　本規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

解説：(1) 用語の取り扱い  
用語は、ポリシー、実施規程、手順・ガイドライン等を通して統一しておくこと。ただし、それぞれの規程の適用範囲に応じて特に定義しておくべき事柄については、それぞれの規程に定義を定めることができる。例えば、学生は「D2201 情報サービス利用規程」を閲読してこれを遵守しなければならないが、「D2101 情報セキュリティ対策基準」には必ずしも目を通さなくてよい。もちろん、アカウンタビリティの観点から、必要な場合に閲覧できるように準備しておくことは必要である。  
サンプル規程集は、上位からポリシー（D1000及びD1001）、実施規程（D2\*\*\*）、手順（D3\*\*\*）のような階層構造を有する。複数の下位規程において共通の用語を上位規程に定めることで、用語の不統一や同じ定義が複数の規程に現れる煩雑さをなくすことができる。しかし、ポリシーに詳細な用語定義を盛り込むことが規程体系の形式上難しかったり、用語定義を追加・変更するたびにポリシーを改訂することが手続き上複雑だったりするため、必要な用語定義を規程毎に置くことも多い。上位規程では参照しないが下位規程で参照する用語について、上位規程には置かず下位規程でその都度定める方法である。  
(2) 利用者等  
「利用者等」に外部委託の第三者を含むよう明記することも考えられる。なお、「本学情報システムを取り扱う」とは、情報システムを運用・管理するだけでなく、情報システムに係る情報を作成・利用することも含まれる。  
本規程では、利用者、臨時利用者を含む広い概念として「利用者等」という用語を用いている。なお、主体認証の場面では、情報システムにアクセスする主体として利用者等に加え他の情報システムや装置も含めた「主体」という用語が用いられる。  
(3) 情報の格付け及び取扱制限  
情報の格付け及び取扱制限は、機密性、完全性、可用性の３つの観点を区別して行われなければならない。本規程では、機密性、完全性、可用性のそれぞれについて３ないし２段階の区分を定めている。これらの定義は「D2104 情報格付け基準」においても参照されるため、上位規程である「D1001 情報セキュリティ基本規程」に置くことも考えられる。

一　外部委託

本学の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。

解説：外部委託に関する具体的な規定については、D2101（情報セキュリティ対策基準」第七章を参照のこと。



二　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。

三　機器等

情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

解説：「情報システム」、「機器等」及びその関係については、巻末（参考図２）参照。

四　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。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

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、第二号と第四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。

五　記録媒体

情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、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、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。

六　サーバ装置

情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。

七　CSIRT（シーサート）

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。

八　実施手順

対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

九　情報

　本規程第二条第２項に定めるものをいう。

解説：本規程の適用を受ける「情報」の範囲については巻末の（参考図１）参照。  
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。

|  |
| --- |
| 参考：第二条第２項（抄）  ２　本規程において適用対象とする情報は、以下とする。  一　教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）  二　その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報  三　第一号及び及び第二号のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報 |

十　情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）若しくは本学情報ネットワークに接続されるものをいう。

解説：「情報システム」、「機器等」及びその関係については、巻末（参考図２）参照。  
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。

|  |
| --- |
| 参考：第二条第３項（抄）  ３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。 |

十一　情報セキュリティインシデント

JIS Q 27000:2014における情報セキュリティインシデントをいう。

解説：JIS Q 27000:2014において、情報セキュリティインシデントは「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」と定義されている。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。

解説：「情報セキュリティインシデント」は日本産業規格（JIS）にて次の通り定義されている。

|  |
| --- |
| 参考：JIS Q 27000:2014（抄）  ・ 情報セキュリティインシデント  望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。  ・ 情報セキュリティ事象  情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。 |

十二　情報セキュリティ関連規程

ポリシーに基づいて策定される規程、基準及び計画を総称したものをいう。

十三　情報セキュリティ対策推進体制

本学の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。

十四　対策基準

本学が定める「D2101 情報セキュリティ対策基準」及び同基準から参照される関連基準をいう。

十五　端末

情報システムの構成要素である機器のうち、利用者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、本学が調達又は開発するもの以外を指す「本学支給以外の端末」がある。また、本学が調達又は開発した端末と本学支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。

解説：「本学至急以外の端末」には、学外関係者が学内に持ち込む端末（モバイル端末に限らず、共同研究機関が学内に設置する端末等を含む）のほか、教職員等や学生等の私物端末を含む。

十六　通信回線

複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

十七　通信回線装置

通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

十八　ポリシー

　本学が定める「D1000 情報セキュリティ対策基本方針」及び本規程をいう。

十九　モバイル端末

端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

解説：大学の場合、大学資産に限定せず、教職員や学生の私物端末も含めることが望ましい。

二十　要管理対策区域

本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

二十一　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。第十八号の臨時利用者は関連するので、ここで定義しても良い。

二十二　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。

D1001-04　（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　本学における情報セキュリティに関する事務を統括する全学総括責任者を置く。学長がこれを任命する。

２　全学総括責任者を助けて本学における情報セキュリティに関する事務を整理し、全学総括責任者の命を受けて本学の情報セキュリティに関する事務を統括する全学総括副責任者１人を必要に応じて置くこと。

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。

解説：「全学総括責任者」について  
全学総括責任者は、本学における情報セキュリティ対策の推進の責任者であり、全学の情報セキュリティ対策を推進するため、組織をふ瞰し、資源配分の方針決定を適切に行うなどリーダーシップを発揮することが求められる。その際には、国内外の情報セキュリティに関連する動向を注視するとともに、有益な最新の技術の活用を検討するなど、先手を打って必要な対策をとることが重要である。  
全学総括責任者は、情報セキュリティに関する全学の方向付けを行う事務について自ら直接関与すべきであることから、情報セキュリティ関連規程及び対策推進計画を決定するとともに、重大な情報セキュリティインシデントが発生した場合には、それに対処するための必要な指示その他の措置を行うこととしている。

３　全学総括責任者は、次に掲げる事務を統括すること。

一　情報セキュリティ対策推進のための組織・体制の整備

二　情報セキュリティ対策基準の決定、見直し

三　対策推進計画の決定、見直し

四　情報セキュリティインシデントに対処するために必要な指示その他の措置

五　前各号に掲げるもののほか、情報セキュリティに関する重要事項

解説：情報セキュリティインシデントについては、第三条（用語定義）に示すとおりであるが、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものとして、実際に業務等への影響は顕在化していないものの、そのおそれがある場合を含むことに留意する必要がある。情報システムに関する情報セキュリティインシデントとしては、例えば、以下が考えられる。  
・要機密情報が含まれる電子メールの外部への誤送信  
・要機密情報が保存されたUSBメモリの紛失  
・不正プログラムへの感染  
・外部からのサーバ装置、端末への不正侵入  
・サービス不能攻撃等による情報システムの停止

４　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。

D1001-05　（全学情報セキュリティ委員会の設置）（政府機関統一基準の対応項番2.1.1(2)）

第五条　全学総括責任者は、対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者を構成員とする全学情報セキュリティ委員会を置くこと。

解説：「全学情報セキュリティ委員会」について  
全学総括責任者は、横断的な事項を審議するため、情報セキュリティを推進する情報セキュリティ対策推進体制及び各部局（部門）の代表者から構成される委員会を設置する。  
委員長及び委員は、全学総括責任者の指名によるが、全学総括責任者自らが委員長を兼ねてもよい。  
委員会は、各部門間の意見調整を図り情報セキュリティ対策と組織の方針を整合的なものとする機能を持つことから、組織全体としての方向付けを要する対策基準及び対策推進計画を審議事項とする必要がある。その他の審議事項については、本学の実態に応じて柔軟に運用すればよいが、例えば、遵守事項 2.1.1(6)に規定する情報セキュリティ対策推進体制に担わせる具体的な役割や、その役割に基づく情報セキュリティ対策の推進状況の確認・評価に係る事項を審議することが考えられる。  
また、委員会の配下に実務を担当する下位委員会を設置し、実務レベルの詳細な事項を調整することで、委員会の運営を効率化することも考えられる。

２　全学情報セキュリティ委員会の委員長及び委員は、全学総括責任者が情報セキュリティ対策推進体制及びその他の業務を実施する部局の代表者から指名すること。

３　全学情報セキュリティ委員会は、次に掲げる事項を審議すること。

一　情報セキュリティ対策基準

二　対策推進計画

三　前各号に掲げるもののほか、情報セキュリティに関し必要な事項

D1001-06　（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)）

第六条　全学総括責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。

解説：「情報セキュリティ監査責任者」について  
本学における情報セキュリティ対策は、全学総括責任者の指揮の下で推進することとなるが、全学総括責任者は、自らが決定した情報セキュリティ対策が適切に実施されているか否かを正しく把握する必要がある。そのため、全学総括責任者は、情報セキュリティ監査責任者にその実施状況等の確認を行わせることにより、情報セキュリティ対策の実効性を確保しようとするものである。  
なお、情報セキュリティ監査責任者は、組織のまとまりごとの情報セキュリティに関する事務を担う部局総括責任者よりも職務上の上位の者を置くことが望ましい。  
情報セキュリティ監査責任者は、情報セキュリティ対策が適切に実施されているか否かを監査し、その結果について全学総括責任者に的確に報告しなければならない。  
情報セキュリティ監査責任者は、これら監査事務を効率的に実施するため、担当者（監査実施者）を置き、必要に応じて外部組織を活用するなど、監査実施体制の整備を行う。  
なお、本学の実情に応じて、監査責任者を補佐する立場として監査副責任者を独自に設置してよい。

D1001-07　（管理運営部局）

第七条　全学情報セキュリティ委員会は、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。

D1001-08　（管理運営部局が行う事務）

第八条　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　全学情報セキュリティ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

D1001-09　（全学実施責任者・部局総括責任者の設置）（政府機関統一基準の対応項番2.1.1(4)(a) 及び2.1.1(4)-1,2）

第九条　全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置くこと。そのうち、部局総括責任者を統括し、全学総括責任者及び全学総括副責任者を補佐する者として、全学実施責任者１人を選任すること。

解説：「部局総括責任者」について  
全学総括責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能となる組織のまとまりごとに、その対策を委ねた方が効率的であることから、取りまとめの責任者として、部局総括責任者を設置する。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。  
部局総括責任者は、全学総括責任者の委任に基づき、所管する組織の情報セキュリティ対策を推進及び運用するため、組織内の体制整備及び事務を行う。  
本学における情報セキュリティ確保のための体制の整備にあたっては、本学の業務形態やその組織の有する実情を踏まえ、組織全体として情報セキュリティマネジメントが機能する体制整備を行うことが重要であり、以下のような場合には、特に部局総括責任者の役割が重要となる。  
例えば、大学等の研究教育機関においては、業務形態や組織の態様が比較的一様な事務的業務を行う一般の行政機関とは異なり、管理部門と研究部門という 異なる形態の部門が存在する。さらに、研究教育機関の中には、多様で異なる研究分野を一機関内に包含するものがある。このような場合には、それぞれの研究分野が異なることから、各研究部門の研究活動に一定の独立性が認められるケースがある。効果的な研究開発の実施の観点から研究部門の自主性が重んじられる場合がある一方、情報セキュリティの観点からは、組織全体としての統一的なセキュリティの確保が求められ、両者をどのように両立していくかが課題となる。  
また、個々の教員に関しても、行政事務のようなオフィスワークとは異なり、学外での精力的な活動等、業務遂行において、より画一的でない情報機器の利用形態をとる場合がある。  
従って、これらの機関における情報セキュリティの確保は、その業務形態や組織の実情を踏まえて講じられることが求められる。一般に、研究開発機関における各研究部門の長は、部局総括責任者として役割を担うことが想定されるが、その際は、次のような事項に留意するとよい。  
教員にとっては、研究開発成果を創造するという重要な役割があり、学部等の長はその指導的立場にある。そこで、各学部等の長が、その研究内容に関する立場と同様に、情報セキュリティ対策についても部局総括責任者として各研究者に対してリーダシップを発揮することが効果的と考えられる。  
さらに、各学部等において主体的に情報システムを導入し、その情報セキュリティ対策をそれぞれの部門が担っている場合には、情報セキュリティ対策推進体制とは別に、これら部門において情報セキュリティ対策を講じる実務的機能を確保するとともに、その機能を担う者の能力の維持・向上に取り組むことが求められる。この場合、情報セキュリティ対策推進体制においては、各学部等を含む組織全体の情報セキュリティの対策状況をタイムリーに把握し、必要に応じて課題への機敏な対応が可能となるように、これら各研究部門との連携体制を構築することが必要となる。情報セキュリティ対策推進体制と各学部等を相互に連携させるとともに、各学部等内の情報セキュリティ対策を指揮する立場にあるのが部局総括責任者であり、その点において各学部等の長の役割に期待されるところは大きいといえる。

解説：「全学実施責任者」について  
全学総括責任者は、自らの事務及び全学総括副責任者の事務を補佐させるため、組織のまとまりごとに設置する部局総括責任者のうちから１人を全学実施責任者として選任する。  
全学実施責任者は、全学総括責任者からの委任（全学総括責任者が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、全学総括責任者に残る。）に基づき本学の情報セキュリティ対策について総合調整する事務を担うとともに、全学総括責任者及び全学総括副責任者を補佐する役割を担う。例えば、対策基準や対策推進計画の案の作成を担うことが想定される。

２　全学実施責任者は、命を受け、次の事務を統括すること。

一　要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

二　情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ

三　情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備

四　例外措置の適用審査記録の台帳整備等

五　情報セキュリティインシデントに対処するための緊急連絡窓口の整備等

六　前各号に掲げるもののほか、情報セキュリティ対策に係る事務

解説：「D2101第ｘ条「実施手順を整備」について」を参照のこと。

３　部局総括責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。

一　定められた区域ごとの区域部局総括責任者の設置

二　部局の職場情報セキュリティ責任者の設置

三　情報システムごとの部局技術責任者の設置

四　情報セキュリティインシデントの原因調査、再発防止策等の実施

五　情報セキュリティに係る自己点検計画の策定及び実施手順の整備

六　前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

D1001-10　（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)及び2.1.1(4)-3）

第十条　部局総括責任者は、「D2101情報セキュリティ対策基準」第五十四条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統括する区域情報セキュリティ責任者 1 人を置くこと。

解説：「区域情報セキュリティ責任者」について  
部局総括責任者は、所管する組織のまとまりの情報セキュリティ対策のうち施設及び環境に係る対策について、定められた区域ごとにその対策を推進する責任者として区域情報セキュリティ責任者を指名する。  
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。  
・単一の教室、研究室、事務室等の管理組織が利用する執務室及び会議室を管理する場合は、職場情報セキュリティ責任者  
・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  
・ロビー、廊下等を管理する場合は、施設等の管理に関する部門の責任者  
なお、「D2101情報セキュリティ対策基準」第五十五条で後述するクラス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、施設の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。

D1001-11　（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)及び2.1.1(4)-4）

第十一条　部局総括責任者は、教室、研究室、事務室等の管理組織単位ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者1人を置くこと。

解説：「職場情報セキュリティ責任者」について  
部局総括責任者は、教室、研究室、事務室等の管理組織単位内の情報の取扱い及び情報セキュリティ対策の責任者として、職場情報セキュリティ責任者を設置する。職場情報セキュリティ責任者は、情報の取扱い等に関して、その是非を判断する役割を担うため、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又はそれに相当する者であることが望ましい。

２　職場情報セキュリティ責任者は、命を受け、教室、研究室、事務室等の管理組織単位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統括すること。

D1001-12　（部局情報セキュリティ委員会）

第十二条　各部局に部局情報セキュリティ委員会を置く。

２　部局情報セキュリティ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

D1001-13　（部局情報セキュリティ委員会の構成員）

第十三条　部局情報セキュリティ委員会は、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

D1001-14　（部局情報セキュリティ委員会の委員長）

第十四条　部局情報セキュリティ委員会の委員長は、部局総括責任者をもって充てる。

D1001-15　（部局技術責任者の設置）（政府機関統一基準の対応項番2.1.1(4)(d) 及び2.1.1(4)-5,6）

第十五条　部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局技術責任者を、当該情報システムの企画に着手するまでに選任すること。

解説：「部局技術責任者」について  
部局総括責任者は、情報システムごとの情報セキュリティ対策及び運用の責任者として、部局技術責任者を指名する。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。  
部局技術責任者は、所管する情報システムのライフサイクル全般にわたって適切に情報セキュリティ対策を実施することが求められる。このため、部局総括責任者は、新規の情報システムについて企画に着手するまでに部局技術責任者を選任しなければならない。本学 LAN システムのような本学内で共通的に利用されるシステム、特定部門における個別業務システム等、本学の全ての情報システムについて、情報システムごとにセキュリティ対策の運用の責任の所在を明確にすることが重要である。また、アプリケーションのみ別組織が管理するといったように、情報システムを共同で管理する場合は、あらかじめ責任分担を明確にする必要がある。  
部局技術責任者は、情報セキュリティ対策の技術的事項について補佐する者（本条第項で定める部局技術担当者）をデータベース、アプリケーション等の装置・機能ごとに、必要に応じて置き、技術的対策の実効性を確保することが望ましい。

２ 部局技術責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。

３　部局技術責任者は、所管する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こと。

解説：「部局技術担当者」について  
部局技術担当者は、部局技術責任者が定めた手順や判断された事項に従い、所管する情報システムのセキュリティ対策を実施する。  
必要な単位ごととは、例えば部屋ごとに1名を任命することが考えられる。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。

D1001-16　（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)及び2.1.1(5)-1）

第十六条　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こと。

解説：「全学情報セキュリティアドバイザー」について  
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及び全学総括副責任者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本学内の教職員等を充ててもよい。この場合、当該教職員等が部局総括責任者やその他の責任者を兼務してもよい。

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こと。

一　全学の情報セキュリティ対策の推進に係る全学総括責任者及び全学総括副責任者への助言

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

D1001-17　（情報セキュリティ対策推進体制の整備）（政府機関統一基準の対応項番2.1.1(6)及び2.1.1(6)-1）

第十七条　全学総括責任者は、本学の情報セキュリティ対策推進体制を整備し、その役割を規定すること。

２　全学総括責任者は、情報セキュリティ対策推進体制の責任者を定めること。

３　全学総括責任者は、以下を含む情報セキュリティ対策推進体制の役割を規定すること。

一　情報セキュリティ関係規程及び対策推進計画の策定に係る事務

二　情報セキュリティ関係規程の運用に係る事務

三　例外措置に係る事務

四　情報セキュリティ対策の教育の実施に係る事務

五　情報セキュリティ対策の自己点検に係る事務

六　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

解説：「本学の情報セキュリティ対策推進体制を整備」・「情報セキュリティ対策推進体制の役割を規定する」について  
本学の情報セキュリティ対策を推進するためには、組織横断的に施策を取りまとめて推進する情報セキュリティ対策推進体制が必要であり、本項では、そのような体制とその役割を組織として明確化することを求めている。  
情報セキュリティ対策推進体制の基本的な役割は、本基本対策事項各号に定める事項を基本とし、組織の特性等に応じ、その他必要な事項を追加するなどして規定する必要がある。その他にも、例えば以下の事項を役割として担うことが考えられる。  
・情報セキュリティ委員会の運営に係る事務  
・サイバーセキュリティ基本法第25条第１項第２号に基づきサイバーセキュリティ戦略本部が実施する監査（以下「本部監査」という。）への対応に係る事務内閣官房内閣サイバーセキュリティセンターから発出される事務連絡や調査依頼事項等への対応に係る事務  
また、「本規程第９条解説「全学実施責任者」について」に記載のとおり、全学実施責任者が本学の情報セキュリティ対策について総合調整する事務を担っていることから、情報セキュリティ対策推進体制は、統一基準において全学実施責任者の役割として規定されている事項に係る実務を含む事務を担う体制として位置付けるとよい。  
さらに、「D2101情報セキュリティ対策基準」第七十一条において部局技術責任者に求めている脆弱性対策の状況の定期的な確認を支援するために、ソフトウェアに関する脆弱性情報の公開状況を確認し、部局技術責任者と情報共有を行うなど、情報システムの情報セキュリティ対策を推進するための事務を担うことなども考えられる。

解説：「情報セキュリティ対策推進体制の責任者」について  
前述のおり、情報セキュリティ対策推進体制は、全学実施責任者が担う実務を中心とした事務を遂行するための体制として機能させることを想定している。そのため、本項で定める責任者として、全学実施責任者を充てることが考えられる。ただし、実際の組織構成等に応じて全学実施責任者以外の者を充てることを妨げるものではない。

D1001-18　（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(7)及び2.1.1(7)-1,2,3,4）

第十八条　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責任者を置くこと。また、CSIRT内の業務統括及び外部との連携等を行う教職員等を定めること

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こと。

解説：「CSIRT」について  
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。

解説：「CSIRTに属する教職員等」について  
CSIRTに属する教職員等は、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者を含めることが考えられる。CSIRTが設置された部門において、求められる知識や技能等を有する者が不足している場合には、CSIRTが設置された部門以外の教職員等をCSIRTに属する教職員等として充てることも考えられる。  
また、CSIRTに属する教職員等には、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。  
なお、他の部門の教職員等をCSIRTに属する教職員等として充てる場合には、職務命令としてCSIRTに係る職務を兼任させるなど、当該教職員等が支障なく活動できるよう留意する必要がある。

解説：「CSIRT責任者」について  
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。

解説：「CSIRT 内の業務統括及び外部との連携等を行う教職員等｣について  
CSIRT内の業務統括及び外部との連携等を行う教職員等は、CSIRT責任者の指揮の下、CSIRTの業務や連絡を一元的に管理し統括する機能を担う。ここでいう教職員等は、一人の教職員等に制限するものではなく、いわゆる総括班のような位置付けで複数名置くことが望ましい。

解説：「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」について  
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。

４　全学総括責任者は、以下を含むCSIRTの役割を規定すること。

一　本学に関わる情報セキュリティインシデント発生時の対処の一元管理

　・全学における情報セキュリティインシデント対処の管理

　・情報セキュリティインシデントの可能性の報告受付

　・本学における情報セキュリティインシデントに関する情報の集約

　・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

　・情報セキュリティインシデントへの対処に関する指示系統の一本化

二　情報セキュリティインシデントへの迅速かつ的確な対処

　・情報セキュリティインシデントであるかの評価

　・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデン  
　トへの対処全般に関する指示、勧告又は助言

　・文部科学省への連絡

　・外部専門機関等からの情報セキュリティインシデントに係る情報の収集

　・他の機関等への情報セキュリティインシデントに係る情報の共有

　・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

解説：「全学における情報セキュリティインシデント対処の管理」について  
情報セキュリティインシデントへの対処に当たっては、「検知／連絡受付」「、トリアージ（情報セキュリティインシデントであるか否かの評価、優先度付け等）」、「インシデントレスポンス（応急措置の実施、原因調査、復旧、再発防止等）」、「報告／情報公開（報道発表等の対外対応）」といったプロセスが必要となる。  
CSIRTには、上記のプロセス全体について、本学内外の関係組織と連携・調整を図り、状況を把握し、適宜幹部等への報告を行うとともに、迅速かつ的確な対処が行われるように当事者部局への指示・勧告・助言を行うことが求められる。

解説：「専門的知見の提供、対処作業の実施」について  
本学において、サイバーセキュリティや情報セキュリティインシデントへの対処に係る専門組織や専門知識を持った教職員等を有する場合は、それらの組織・教職員等のCSIRTへの組み込み、又は情報セキュリティインシデント発生時に連携できる体制の構築を行うことが望ましい。

５　全学総括責任者は、実務担当者を含めた実効性のあるCSIRT体制を構築すること。

解説：「実務担当者を含めた実効性のある CSIRT体制」について  
CSIRT体制には、情報セキュリティインシデント対処における全学総括責任者への早急な状況報告、被害拡大防止及び復旧のための対策の実施を果たし 得るよう、実務担当の教職員等を複数含むことが必要である。  
また、CSIRTは、全学情報セキュリティアドバイザー等から情報セキュリティインシデントへの対処の支援が円滑に受けられるような体制とすることが望ましい。

６　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に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておくこと。

解説：「外部の専門家等による必要な支援を速やかに得られる体制」について  
外部の専門家等による必要な支援を迅速に得られる体制の構築の例としては、情報セキュリティインシデント発生時にそうした事案への対処に精通した専門家を速やかに派遣してもらうための契約を事業者と結ぶこと等が挙げられる。

７　全学総括責任者は、全学における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定すること。

解説：「役割分担を規定」について  
情報セキュリティインシデント発生時に、関係者が速やかに必要な対処を行えるように、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局（広報担当部局、調達担当部局、サイバーセキュリティ専門部局等）の役割分担をあらかじめ定めておくことが望ましい。ただし、役割分担は、情報セキュリティインシデントの種類や規模、影響度合い等によって変更されることも考えられるため、発生の頻度が比較的高いと考えられる情報セキュリティインシデントを想定した役割分担をあらかじめ定めておき、必要に応じて役割分担を再設定することも考えられる。

D1001-19　（全学BCPとの整合）

第十九条　全学実施責任者は、情報セキュリティ関連規程の整備又は見直しを指示するに際し、当該規程が満たすべき要件としてA大学事業継続計画（全学BCP）との整合性の確保を含めること。

D1001-20　（兼務を禁止する役割）（政府機関統一基準の対応項番2.1.1(8)）

第二十条　教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

　一　承認又は許可（以下本条において「承認等」という。）の申請者と当該承認を行う者（以下、本条において「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：「承認権限者等の上司又は適切な者」について  
承認等の申請において、申請する者と承認する者が同一の場合又は申請する者が承認する者の上司である場合は、手続規定において定められた承認権限者等をもって承認等の可否の判断を行うことは適切とは言えない。  
このような場合に対応するために、承認権限者等の上司等をもって承認するなどの手続をあらかじめ定めておく必要がある。  
部局総括責任者等よりも高位の教職員等が承認等を申請する場合においては、例えば、全学総括責任者が当該承認等の判断を行うことが想定される。他方、技術的な事項は、承認権限者等の上司よりも内容を理解している者が可否の判断を行う方が適切な場合もあり、この場合には、本来の承認権限者等が判断してよい。  
また、全学総括責任者と同等以上の職位の者が、承認等を申請する場合も想定される。このような場合においても、全学総括責任者が、適切に判断することが考えられる。

D1001-21　（対策基準の策定）（政府機関統一基準の対応項番2.1.2(1)）

第二十一条　全学総括責任者は、全学情報セキュリティ委員会における審議を経て、サイバーセキュリティ戦略本部決定「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定めること。また、対策基準は、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。

解説：「全学情報セキュリティ委員会における審議を経て、サイバーセキュリティ戦略本部が決定した最新の「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定める」について  
対策基準の策定に当たっては、あらかじめ、全学情報セキュリティ委員会において審議を行うとともに、情報セキュリティの知見を持つ者に意見を求めるなどして、規定内容の網羅性や妥当性について確認した上で決定することが望ましい。なお、最新の「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」の内容に準拠させることで、「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定めることが可能である。  
また、対策基準は、「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」に記載されている内容に基づき、リスク評価の結果を踏まえ、定期的に見直しの必要性を確認するなど常に最新の状況に適合させることが重要である。

解説：「リスク評価の結果を踏まえた上で定める」について  
対策基準の策定に当たっては、情報セキュリティを取り巻く様々な脅威や、本学の業務、取り扱う情報の特性及び保有する情報システムの特性等を踏まえた上で、リスク評価を行うことが重要である。リスク評価は、リスク分析の成果に基づき、如何なるリスクへの対策が必要か、講ずべき対策の優先順位はどうするかなどについて意思決定を支援することを目的に実施するものである（図参照）。本学の業務、取り扱う情報及び保有する情報システムの特性に応じてリスクは異なることから、本学における情報セキュリティを確保するためには、リスク評価を実施し、対策基準に定めるべき対策事項等を決定することが重要である。  
リスク評価手法については、本学の情報セキュリティに係るマネジメント能力の成熟度や機関等の置かれた環境に応じたふさわしい手法を選ぶとよい。リスク評価に係る規格には、ISO31000:2009, Risk management－Principles and guidelines（国内標準としては、JIS Q 31000:2010 リスクマネジメント－原則及び指針（以下「JIS Q 31000:2010」という。））等がある。これらを活用するなどし、適切な評価を実施するとよい。また、重点的に守るべき業務及び情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成28年10月7日情報セキュリティ対策推進会議）に従って、対策を講ずることが必要である。  
  
図　リスクマネジメントプロセスのイメージ図（JIS Q 31000:2010 による）  
  
以下では、国際標準に基づいたリスク評価の手法を解説する。  
リスク評価は、リスクの大きさが受容可能か否かを決定するために、リスク分析の結果をリスク基準と比較するプロセスのことを言う。これは、リスク対応に関する意思決定を手助けするものである。  
まず、リスク水準を把握する手法の例として、以下に４種類の手法を示す。



|  |
| --- |
| ① ベースラインアプローチ  既存の基準をもとにセキュリティ対策のベースラインをリスク基準として作成し、実際の運用がベースラインの求める基準を満たしているかという観点で評価していく方法。簡単な方法であるが、選択する基準によっては、求める対策のレベルが高すぎたり低すぎたりする場合がある。  ② 非形式的アプローチ  コンサルタント、組織又は担当者が、自身の知見や経験に基づき評価を行う方法。短時間に実施することが可能であるが、属人的な判断に偏るおそれがある。  ③ 詳細リスク分析  システムについて情報資産ごとに「資産価値」、「脅威」、「脆弱性」及び「セキュリティ要件」を識別し、これらをリスク基準に照らして評価する方法。厳密なリスク評価が行える一方、多くの工数や費用がかかる。  ④ 組合わせアプローチ  複数のアプローチの併用。よく用いられるのは、「① ベースラインアプローチ」と「③ 詳細リスク分析」の組合わせ。ベースラインアプローチと詳細リスク分析の両方のデメリットを相互に補完し、作業の効率化や分析制度の向上を図ることができる。  ※枠内、情報処理推進機構、  https://www.ipa.go.jp/security/manager/protect/pdca/risk\_ass.htmlを基に作成また、「ISMS ユーザーズガイド(JIP-ISMS111-3.0)」から文書を引用(④組合わせアプローチの説明に係る「相互に～向上を図ること」の記述 |

組織の情報セキュリティに係るマネジメント能力の成熟度が比較的十分でない組織においては、簡易な方法である「ベースラインアプローチ」を適用することが考えられる。  
簡易なリスク評価の進め方として、例えば、前述した「ベースラインアプローチ」に着目し、機関等のポリシーをリスク基準として用いることが考えられる。  
その際は、自己点検や情報セキュリティ監査をリスク評価プロセスの一部として活用すれば、リスク評価をより効率的に実施できる。  
  
リスク評価に当たっては、特に、以下の５点に留意し検討すると、リスク評価が必要になることや、それを行う目的が分かるようになる。リスク評価においては、その目的意識を明確に持つことが重要である。

|  |
| --- |
| ① 守るべき資産は何か。  ② その資産にはどのようなリスクがあるか。  ③ セキュリティ対策により、リスクはどれだけ低減するか。  ④ 実施しようとしたセキュリティ対策の失敗により、どのようなリスクがもたらされるか。  ⑤ 対策にはどれ程のコストとどのような二律背反の要素が付随するか。 |

また、リスク評価に際しては、リスクマネジメントプロセス全体に留意し、リスク対応を行った後、モニタリング及びレビューを行い、更なる改善を図ることが望ましい。  
  
次に、リスク分析の結果をリスク基準と比較するプロセスについて解説する。  
リスク基準決定の際は、JIS Q 31000の支援規格でもあるJIS Q31010:2012 リスクマネジメント－リスクアセスメント技法（IEC/ISO31010:2009,Risk management- Risk assessment techniques）において、リスクの発生確率、リスクレベル等を決定する旨が記載されている。これを踏まえ、脅威事象が発生する可能性を"非常に高い／高い／中間／低い／非常に低い"、脅威事象が負の影響をもたらす可能性を"非常に高い／ 高い／中間／低い／非常に低い"などと各々分類し、両者のマトリクスで結果を整理しリスク基準を決定する方法等がある（次表参照）。  
  
表　リスク基準例（発生した脅威事象が組織の業務、資産又は個人に被害をもたらす総合的な可能性:NIST SP800-30 rev1(情報処理推進機構訳)による）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 脅威事象が負の影響を もたらす可能性  脅威事象が  発生する可能性 | 非常に 低い | 低い | 中間 | 高い | 非常に 高い |
| 非常に高い | 低い | 中間 | 高い | 非常に  高い | 非常に  高い |
| 高い | 低い | 中間 | 中間 | 高い | 非常に  高い |
| 中間 | 低い | 低い | 中間 | 中間 | 高い |
| 低い | 非常に  低い | 低い | 低い | 中間 | 中間 |
| 非常に低い | 非常に  低い | 非常に  低い | 低い | 低い | 低い |

決定したリスク基準とリスク分析の結果を比較し、その結果、発生した脅威事象が組織の業務、資産又は個人に被害をもたらす総合的な可能性（以下「発生した脅威事象の総合的な可能性」という。）が「非常に高い」となった場合は、そのリスクを回避する（JIS Q 31000:2010,5.5.1 a 参照）ことが考えられる。  
発生した脅威事象の総合的な可能性が「高い」、「中間」又は「低い」となった場合は、リスク源を除去する（JIS Q 31000:2010,5.5.1 c 参照）などリスクの低減、「非常に低い」となった場合は、リスクの保有（JIS Q 31000:2010,5.5.1 g 参照）による対応が考えられる。  
ただし、例えば、脅威事象が発生する可能性が「非常に低い」、脅威事象が負の影響をもたらす可能性が「非常に高い」場合で、発生した脅威事象の総合的な可能性が「低い」となっていた場合は、低減でなく、他者とそのリスクを共有する（ JIS Q 31000:2010,5.5.1 f 参照）リスク移転による対応を行うことが考えられる。  
リスクに対し、どのような対応を行うかは、一意に決まるものではない。目的、リスク対応が新たに生み出すリスクの有無、費用対効果等を踏まえ、対応を決める時点において最善の対応を選択することが望ましい。  
JIS Q 31010:2012 リスクマネジメント－アセスメント技法には、脅威事象が発生する可能性、脅威事象が負の影響をもたらす可能性を組み合わせ活用するための数値等は例示されていないが、National Institute of Standards and Technology（米国国立標準技術研究所）Special Publication 800-30 revision1（以下「NIST SP800-30 rev1」という。）に参考となる表（既出表参照）、解説があるので記載する。  
  
＜脅威事象が発生する可能性について（NIST SP800-30 rev1(情報処理推進機構訳)による）＞

|  |
| --- |
| * 脅威事象が発生する可能性 定性的な値：非常に高い、半定量的な値：96-100 エラー、アクシデント又は天災が発生するのはほぼ確実である、あるいは 1 年間に100回以上発生する。 * 脅威事象が発生する可能性 定性的な値：高い、半定量的な値：80-95 エラー、アクシデント又は天災が発生する可能性は高い、あるいは1年間に10回ないし100回発生する。 * 脅威事象が発生する可能性 定性的な値：中間、半定量的な値：21-79 エラー、アクシデント又は天災が発生する可能性はある程度ある、あるいは1年間に1回ないし10回発生する。 * 脅威事象が発生する可能性 定性的な値：低い、半定量的な値：5-20 エラー、アクシデント又は天災が発生する可能性は低い、あるいは1年間に1回未満発生するが、10年おきに2回以上発生する。 * 脅威事象が発生する可能性 定性的な値：非常に低い、半定量的な値：0－4 エラー、アクシデント又は天災が発生する可能性はほとんどない、あるいは10年おきに1回未満発生する。 |

＜脅威事象が負の影響をもたらす可能性について（NIST SP800-30 rev1(情報処理推進機構訳)による）＞

|  |
| --- |
| * 脅威事象が負の影響をもたらす可能性 定性的な値：非常に高い、半定量的な値：96-100 脅威事象が開始された／発生した場合、負の影響がもたらされるのはほぼ確実である。 * 脅威事象が負の影響をもたらす可能性 定性的な値：高い、半定量的な値：80-95  脅威事象が開始された／発生した場合、負の影響がもたらされる可能性は高い。 * 脅威事象が負の影響をもたらす可能性 定性的な値：中間、半定量的な値：21-79 脅威事象が開始された／発生した場合、負の影響がもたらされる可能性はある程度ある。 * 脅威事象が負の影響をもたらす可能性 定性的な値：低い、半定量的な値：5-20 脅威事象が開始された／発生した場合、負の影響がもたらされる可能性は低い。 * 脅威事象が負の影響をもたらす可能性 定性的な値：非常に低い、半定量的な値：0－4 脅威事象が開始された／発生した場合、負の影響がもたらされる可能性はほとんどない。 |

＜リスク評価に係る用語＞

|  |
| --- |
| 参考：JIS Q 31000:2010 リスクマネジメント－原則及び指針（抄）   * リスク基準（JIS Q 31000:2010, 2.22 のとおり） リスクの重大性を評価するための目安とする条件。 * コミュニケーション及び協議（JIS Q 31000:2010, 5.2 のとおり） リスクの運用管理において、情報の提供、共有、取得及び意思決定に影響を与えるなどの人々又は組織との対話を行うために、組織が継続的に及び繰り返し行うプロセス。 * リスクアセスメント（JIS Q 31000:2010, 5.4 のとおり） リスク特定、リスク分析及びリスク評価を網羅するプロセス全体を指す。 * モニタリング及びレビュー（JIS Q 31000:2010, 5.6 のとおり） リスクアセスメントを改善するため、更なる情報の入手や傾向等の分析を行うこと。 |

（参考図１）本規程の適用を受ける「情報」の範囲



（参考図２）「情報システム」、「機器等」及びその関係

