本文書について

１．背景

　大学の教育、研究、運営などの活動における情報化の進展とともに、情報セキュリティが重要になっている。情報セキュリティレベルを確保し向上させていくために、各大学においてその必要性を十分に認識し、情報セキュリティの基本方針と組織・体制、対象を決定して、情報セキュリティポリシー、実施規程、啓発用テキストなどを作成することが必要である。しかし、情報セキュリティポリシー等の策定は、大学における教学との関係、大学の組織および運営における意思決定や運用・利用の扱い方などを考慮しなければならず、あるいは法律・制度や組織運営、情報・通信・セキュリティ技術等に関する専門知識が求められるために、取り組みが難しい課題である。

　この取り組みを支援するために、例えば、全国共同利用大型計算機センター群による「大学のセキュリティポリシーに関する研究会」は「大学における情報セキュリティポリシーの考え方」（平成14年5月）を作成して、大学における問題点と具体例の分析などを示した。あるいは、電子情報通信学会は「ネットワーク運用ガイドライン検討ワーキンググループ」を設置し、ネットワークの健全な運用・利用の実現に資することを願って「高等教育機関におけるネットワーク運用ガイドライン」（平成15年4月）を作成し各高等教育機関が独自の規程類を整備するためのキャンパスネットワークの運用管理ポリシーと実施要領策定に関する指針を提言した。

　これらの資料によって、考え方や指針、解説が提供されたが、これらを参照するだけで上述の難しい課題を解決することは困難であり、さらに参考となる具体的なサンプル規程集や詳細な運用マニュアルを必要とする意見も少なくない。また、情報セキュリティに関する最近の状況として、個人情報の保護に関する法律の施行や「政府機関（等）の情報セキュリティ対策のための統一基準」（以下、「政府機関統一基準」）の制定があり、セキュリティ水準の向上も求められている。国立大学においては、平成16年度の法人化後に情報システムの運用や情報セキュリティの確保を実施する組織と予算について、全学的方針と新しい制度の構築が新しい課題として加わった。

　このような高等教育機関を取り巻く社会情勢の変化をガイドラインに反映させる必要があり、高等教育機関における情報セキュリティポリシーのサンプル規程集として、本文書の作成を検討することとなった。

２．経緯

　本文書の検討は、国立情報学研究所 学術情報ネットワーク運営・連携本部が設置した「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」（以下、「策定作業部会」）と、社団法人電子情報通信学会が企画室のもとに設置した「ネットワーク運用ガイドライン検討ワーキンググループ」（以下、「検討WG」）との合同で実施された。

　国立情報学研究所の策定作業部会は、「大学における情報セキュリティポリシーの考え方」から政府機関統一基準を踏まえた見直しを行い、国立大学法人等に適した標準的かつ活用可能な情報セキュリティポリシーの策定を行って各大学へ提供するために設置された。ネットワーク，認証，事務及びこれらの運用が密接に関係することから、策定作業部会には国立情報学研究所のネットワーク作業部会，認証作業部会，学術ネットワーク研究開発センター、ならびに全国共同利用情報基盤センター群のコンピュータ・ネットワーク研究会と認証研究会、および国立大学法人等情報化推進協議会とも連携して対応し、文部科学省の大臣官房政策課情報化推進室と研究振興局情報課、および内閣官房情報セキュリティセンターの協力も得た。

　電子情報通信学会の検討WGは、平成15年度からの第二期で策定してきた「高等教育機関におけるネットワーク運用ガイドライン（第二版）」を完成させて成果を公開するために活動を延長して利用者，教育・倫理の領域を中心に引き続き検討することとして、電子情報通信学会の技術と社会・倫理研究専門委員会とインターネットアーキテクチャ研究専門委員会から協力を得た。

　策定作業部会と検討WGは、平成18年8月に合同で検討と策定を開始した。総論・体制，ネットワーク運用，認証運用，事務利用，利用者，教育・倫理の６つの領域分科会を設定し、領域ごとに電子メールを中心とした検討と会合を行った。各領域に幹事及び幹事補佐をおいて、検討をとりまとめ、あるいは関連する領域分科会と連絡し、必要に応じて他の分科会に参加した。また各領域の幹事と策定作業部会の主査・副主査、検討WGの主査・幹事により幹事会を構成し、全体の調整にあたった。また、国立情報学研究所の研究部門の共同研究課題（国立情報学研究所・岡田仁志，代表・神戸学院大学・小川賢）による研究とも連携した。策定作業部会の運営と取りまとめの支援は、外部（みずほ情報総研株式会社）に担当を委託した。策定作業部会と検討WG はいずれも年度末までの期限で設置された。その成果を「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」としてとりまとめて、平成19年2月にインターネットで配布を始めた。これには、想定される規程体系のうち基本方針、規程類から手順書、教育テキストまで17本のサンプル規程を収めて、本文298ページ（ほかに前文7ページ）であった。また、成果の普及のため「大学における情報セキュリティおよび電子認証基盤に関するワークショップ」および電子情報通信学会総合大会において説明を実施した。

　平成18年度の活動では時間的制約などで公開レベルまで精査できずサンプル規程集の公開対象外とした部分があり、情報セキュリティポリシーの規則体系としての完成度を高める要請に応えてサンプル規程集を完成させるため、また公開済みのサンプル規程集に対するコメントに対応するために、策定作業部会と検討WGのいずれも平成19年10月まで活動を延長し、前年度と同様の連携体制により合同で検討と策定を継続した。平成19年度の活動は、課題が多く残っている領域の検討を推進して完成させるために、領域を再構成して５の大領域と10の小領域として、運用（運用総論領域、システム運用領域、情報管理領域）、認証（認証運用領域）、事務（事務領域）、利用（利用領域、自己点検領域）、教育（利用者教育領域、管理者教育領域、役職者教育領域）の分科会を設定した。その成果が本書であり、平成19年8月の「情報セキュリティセミナー」等で成果普及のための説明を実施した。

　なお、策定作業部会は平成19年10月末で解散し、公開したサンプル規程集に対する対応や次回改訂に向けた準備等に対応するための組織として、国立情報学研究所 学術情報ネットワーク運営・連携本部に「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」が平成19年12月に設置され、以後サンプル規程集についての継続的な更新を行っている。

　本書と関連資料は国立情報学研究所の以下のWebサイトにて配布している。

（参考）http://www.nii.ac.jp/service/sp/

３．策定

　本文書でとりまとめたサンプル規程集は、政府機関統一基準を踏まえ、各機関の事情に合わせて作成する際の具体的な参考として役立つよう、大学に適した標準的かつ活用可能な情報セキュリティ規程群を策定したものである。情報セキュリティに関する規程のほかに、情報セキュリティポリシーも含み、一部のマニュアルも対象に含めたが、いずれも期間内に検討可能であった範囲で成果を収録した。必ずしも必要性や重要度に沿って優先順位をつけて策定したとは限らない。政府機関統一基準は大学が準拠するよう要求しているものではないが、政府機関以外でも情報セキュリティ対策の体系の例として参照し利用する価値があるので、大学の事情に合わせて可能な範囲で政府機関統一基準の考え方にあわせる形で策定した。ほかにも情報セキュリティに係わる基準としてISOのものやプライバシーマーク制度などがそれぞれの目的により定められているが、それらも含めて検討して、大学における実施にもっとも適する規程とすることを意図した。

　サンプル規程集は電子情報通信学会の検討WGにおいて策定された「高等教育機関におけるネットワーク運用ガイドライン」をベースとして含む形となっている。ただし、同ガイドラインがネットワーク運用に関するセキュリティに重点を置いたものであるのに対し、本文書では「政府機関の情報セキュリティ対策のための統一基準」が情報資産のセキュリティを確保することを目的としていることを考慮し、対象を情報システムにおけるネットワーク運用以外の要素まで広げている。

　サンプル規程集のスタイルとして、規程の条文サンプルと解説から構成した。規程のスタイルや文章は大学の慣習に沿ったものとしたが、基準など一部では情報セキュリティポリシーの分野の標準的なスタイルを採った。それぞれの条文について、規定している内容が理解しにくい項目や、各大学の状況に応じて修正することが望ましい項目、他の選択（政府機関統一基準やISOのものとの相違など）や議論の余地があるものは解説を付記して、各大学における策定の参考として供した。各大学等で本文書を参考として自組織向けの規程等を作成する際には、これらの内容を参照した上で必要な修正や加除を検討していただきたい。例えば、仮想A大学と比べて学部数が多い大学や複数キャンパスにまたがる大学等では導入に際してセキュリティの管理体制を含め、各規程の前提条件の適合性に関する検討を行うことが望ましい。なお、定め方に判断の幅がある部分については、必ずしも一貫した規程になっていない部分もありえる。

　情報システムの利用者認証（主体認証）については、ID とパスワードによる認証から生体認証、さらにはPKI(Public Key Infrastructure)を使用した認証などさまざまなものがあるが、ID とパスワードによる利用者認証を対象とした。PKIによる利用者認証については、国立情報学研究所によるUPKI電子証明書発行サービスにおいて各種の参考ドキュメントが公開されているので、次のサイトを参考にされたい。

（参考） https://certs.nii.ac.jp/document/

４．サンプル規程

　サンプル規程集は、仮想の国立大学法人Ａ大学における体制と規則を想定して検討した。Ａ大学の概要は次の通りである。

* 文学部と理学部の２学部で構成され、両学部とも在学生が1,000人（１学年250名）ずつである。さらに、学内共同利用施設として情報メディアセンターや図書館がある。
* 全学ネットワークと主要な情報システムに関して、図１のような構成を有する。
* 学内ネットワークや学内共同利用の情報システムは情報メディアセンターの担当であり、Ａ大学の管理運営部局は情報メディアセンターである。なお、事務情報システムは事務局が担当する。
* 副学長の一人がいわゆる最高情報責任者（CIO）であり、最高情報セキュリティ責任者（CISO）の役も兼ねており、本サンプルでは全学総括責任者となっている。



図１　Ａ大学のネットワーク構成図

　サンプル規程集は、図２に示すような階層構造を有する。情報セキュリティ対策に関する基本的な考え方を定めた基本方針と情報セキュリティ対策に関する基本的事項を定めた基本規程をポリシー、ポリシーに基づいて、運用・管理や利用、教育等に関する事項を定めた規則を実施規程、実施規程に基づいて策定される手順やマニュアルなどを手順等としている。最上位のポリシーは全学規程として制定すべきものであるが、実施規程には全学情報セキュリティ委員会で決定すべき規程の他に各大学の運営体制によって情報メディアセンターあるいは事務局の内規とすべきものがあり、手順については、内規あるいは手引書とすべきものなどがある。手順等のうち、各大学における情報セキュリティ対策のために遵守すべき規則として策定されることが望ましい標準的な内容を手順とし、各大学での実情に即した内容で策定されることが望ましい事項はガイドラインとした。各階層において必要となるポリシー、実施規程、手順等の体系を図３に示す。

ポリシー

・

管理者向け手順

・利用者向けガイドライン

・教育カリキュラム・テキスト等

図２ ポリシー・実施規程・手順等の位置付け

・

情報セキュリティ対策基準

・情報サービス利用規程

・年度講習計画等

実施規程

手順等

情報セキュリティ対策基本規程

情報セキュリティ対策基本方針

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ポリシー |  | 実施規程 |  | 手順・ガイドライン等 |
| D1000  情報セキュリティ対策基本方針  D1001  情報セキュリティ対策基本規程 |  | D2101 情報セキュリティ対策基準  D2102 情報格付け基準  D2103情報セキュリティインシデント対応チーム（CSIRT）設置規程 |  | C3100 情報セキュリティ対策手順の策定に関する解説書  C3101 例外措置手順書  D3102 情報格付け取扱手順  D3103 インシデント対応手順策定に関する解説書  C3104 情報システム運用リスク評価手順  D3106 情報セキュリティ非常時行動計画に関する解説書 |
|  |  |
|  | D2201 情報サービス利用規程 | → | C3200 情報システム利用者向け文書の策定に関する解説書 |
|  | D3251情報機器取扱ガイドライン  D3252 電子メール、メッセージング利用ガイドライン  D3253 ウェブブラウザ利用ガイドライン  D3254 情報発信ガイドライン  D3255 認証情報管理ガイドライン |
|  |  |
|  | D2301 年度講習計画 | → | C3300 教育テキストの策定に関する解説書  D3301 教育テキスト作成ガイドライン(一般利用者向け)  C3302 教育テキスト作成ガイドライン(システム管理者向け)  D3303 役職員向け説明資料作成ガイドライン |
|  |  |
|  | C2401 情報セキュリティ 監査規程 | → | C3401 情報セキュリティ監査実施手順 |
|  |  |
|  | C2601 全学認証基盤運用管理規程  C2602 全学認証基盤接続規程  C2603 全学認証基盤アカウント利用規程 |  | C3600 認証手順の策定に関する解説書  C3601 情報システムアカウント取得手順 |
|  |  | C2651 証明書ポリシー(\*)  C2652 認証実施規程(\*) |  |  |

赤字下線が2019年度版として公表済みの文書（文書番号の冒頭がDのその他の文書は策定中）

網掛け部分は、技術系の規程・手順書（より現場に近いレベルでの策定・運用を可能とするもの）

(\*) 外部文書の参照のみ

(\*\*) 各大学にて策定することを想定

図３　ポリシー・実施規程・手順等の体系

　なお、各大学における情報セキュリティの確立のためには、これらのポリシーや実施規程、手順の整備だけではなく、図４に示すとおり、ポリシーに沿った教育活動や組織の運用、さらにはその状況の監査と評価・見直しが重要で、いわゆるPlan・Do・Check・Actionのサイクルを回す必要がある。本ポリシーで規定している組織を図示すると、図５のとおりとなるので、参考にしていただきたい。

|  |  |  |
| --- | --- | --- |
| ポリシーの策定  実施規程と手順の整備 | → | 教育  運用 |
| ↑ |  | ↓ |
| 評価及び見直し | ← | 監査 |

図４　ポリシーの評価及び見直し



図５　情報セキュリティ管理体制

　本ポリシー及び、実施規程、手順における管理体制は、2018年7月に内閣サイバーセキュリティセンターから発行された「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年度版）の体制と表１のとおりに対応づけられるので参考にされたい。

表１　情報システム運用管理体制の対応

|  |  |  |
| --- | --- | --- |
|  | 政府機関統一基準 | 本サンプル規程集 |
| 1 | 最高情報セキュリティ責任者 | 全学総括責任者 |
| 2 | 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 |
| 3 | 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 |
| 4 | 統括情報セキュリティ責任者 | 全学実施責任者 |
| 5 | 情報セキュリティ責任者 | 部局総括責任者 |
| 6 | 情報システムセキュリティ責任者 | 部局技術責任者 |
| 7 | 情報システムセキュリティ管理者 | 部局技術担当者 |
| 8 | 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 |
| 9 | 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 |
| 10 | 上司 | 上司 (注) |
| 11 | 情報セキュリティ委員会 | 全学情報セキュリティ委員会 |
| 12 | 部局情報セキュリティ委員会 |

(注) 研究室においては教授、学生にとっては担当教員を指す一般用語として上司を使用している。

　A大学における情報取扱区域に関するクラス分類を下表に示す。A大学では政府機関統一基準においてクラス1の要件として定義されている「セキュリティゲート」または「警備員等による立ち番」を満たす施設は事務棟、情報メディアセンター、図書館の3箇所のみであるため、これ以外の施設は原則としてすべてクラス0の区域として扱う。クラス１の区域のうち、個別に施錠可能な区域（事務室、機器室、学長室等）をクラス2とする。さらに重要情報や設備を設置し、担当外の事務従事者の立入を制限する必要がある区域（サーバ室、資料保管室（＝バックアップメディアの保管場所として想定））をクラス3としている。

表２　情報取扱区域のクラスの決定

|  |  |  |
| --- | --- | --- |
|  | 政府機関統一基準における定義 | A大学における設定 |
| クラス0 | クラス３、クラス２及びクラス１以外の区域であり、情報セキュリティを確保するため、利用制限対策を実施する必要がある区域 | 学内における下記以外のすべての区域 |
| クラス1 | 最低限必要な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域 | 事務棟内立入制限区域  情報メディアセンター内立入制限区域  図書館内立入制限区域 |
| クラス2 | クラス１より強固な情報セキュリティを確保するための管理対策及び利用制限対策を実施する必要がある区域 | 事務室、学長室及びこれに準ずる個別施錠が可能な区域 |
| クラス3 | クラス２より強固な情報セキュリティを確保するための厳重な管理対策及び利用制限対策を実施する必要がある区域 | （本欄の内容は本来非公開とすべきものであるが、サンプル用に掲載）  情報メディアセンター内サーバ室  事務棟内資料保管室 |
| クラス4 以上 | （政府機関統一基準外） | 区域設定無し。 |

５．2019年度版について

　2019年度版のサンプル規程集の作成にあたっては、規定内容を政府機関統一基準の平成30年度版が定める遵守事項に準じたものに改訂するとともに、これまで学内の事務職員向けと、教育・研究業務に従事する教職員向けに２種類の体系を用意していたのを改め、単一の体系で全学を対象とすることとした。これは、サンプル規程集の初版策定時、大学等の教育及び研究の現場に対して中央省庁等政府機関と同レベルの情報セキュリティ対策を直ちに導入することが現実的でなかったことによる。その後、教育及び研究の環境における情報セキュリティ対策が進展するとともに、平成30年以降に国立研究開発法人等、研究業務を行う機関が政府機関統一基準の適用対象となったことを踏まえ、推進部会における検討の結果、大学等においても政府機関統一基準と同水準の情報セキュリティ対策の実施を機関全体に求めることが適切との判断に至り、上述のような見直しを行った。このほか、これまでのサンプル規程集には、策定の母体となった「高等教育機関におけるネットワーク運用ガイドライン」からの継承により、規程の目的においてネットワークの運用管理を挙げているものが含まれていたが、2019年度版では政府機関統一基準と同様に情報及びそれを扱う情報システムにおける情報セキュリティ対策を対象とすることで統一した。さらに、大学等における情報の利用環境に関する近年の変化を踏まえ、利用者向けの教育や利用ガイドラインに関する文書の内容を実態に合わせたものに更新した。

　これらの変更によるサンプル規程集における体系の変化を、図６と図７に示す。今回策定した文書については、文書番号冒頭の記号をDとしている。これまでサンプル規程集として公開しているA～Cで始まる文書番号の文書とは、同じ番号であっても内容が整合しないものが含まれることに留意されたい。



図６　サンプル規程集の規程体系（2017年版まで）



図７　サンプル規程集の規程体系（2019年度版）

　以下、2019年度版のサンプル規程集を大学等で利用するにあたり、留意すべき事項を示す。

(1) 政府機関統一基準との相違

　2019年度版のサンプル規程集においては、大学等の特徴をもとに、政府機関統一基準に対応する規程及び基準において、次表に示すような変更を加えている。

表３　遵守事項に関する政府機関統一基準との相違箇所の一覧

| 変更事項 | 該当箇所 | 政府機関統一基準との相違とその背景 |
| --- | --- | --- |
| 学生等の扱い | 全体 | 大学等高等教育機関においては、雇用に基づく就業規則に縛られない学生等が学内の教育及び研究活動に関わる点で政府機関統一基準が想定する前提条件と異なることから、学生を含むユーザとして「利用者等」を定義し、全体的な調整を行っている。 |
| D2101（情報セキュリティ対策基準）第九条 | 学生等に対する行為中止命令や懲罰委員会への報告等、政府機関統一基準で扱わない措置を規定している。 |
| 情報システムの範囲 | D1001（情報セキュリティ対策基本規程）第三条第10号 | 大学等が調達又は開発するものだけでなく、共同研究における連携機関が有する情報システム等、大学等の情報ネットワークに接続されるものを含めている。 |
| 「全学情報システム」の定義 | D1001（情報セキュリティ対策基本規程）第四条第４項 | 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「全学情報システム」として定義し、これらに限定した対策を講じることを容易にしている。 |
| 管理運営部局の決定 | D1001（情報セキュリティ対策基本規程）第七条、第八条 | 情報セキュリティ委員会が学内で利用する情報システムの管理運営部局を定めることと、同部局が担当する業務内容を規定している。管理運営部局をトップダウンで決定することが難しい大学等においては、このように情報セキュリティ委員会で決定することと定めることが考えられる。 |
| 部局情報セキュリティ委員会の設置 | D1001（情報セキュリティ対策基本規程）第十二条、第十三条、第十四条 | 情報セキュリティ対策に関して部局毎に一定の独立性を確保する必要がある場合には、部局単位の情報セキュリティ委員会の設置が考えられる。 |
| 全学BCPとの整合 | D1001（情報セキュリティ対策基本規程）第十九条 | 政府機関統一基準ではBCPとの整合は前提として明記されていないが、大学等においては個別に検討されている可能性があることから、整合性を確保すべきことを規定中に明記した。 |
| 情報の目的外利用等の制限 | D2101（情報セキュリティ対策基準）第四十条 | 教育研究事務の遂行以外の目的で情報を利用等しないことを努力義務とした。 |
| 通信の監視及び情報の保護 | D2101（情報セキュリティ対策基準）第百二十一条、第百二十二条、第百二十三条、第百二十四条 | 大学等で管理・運用する情報システムにおいて扱う情報には、政府機関統一基準が前提とする環境とは異なり、雇用関係にない利用者等の情報を保護する必要がある場合の扱い等についての規定を追加した。 |
| 電子証明書 | D2101（情報セキュリティ対策基準）第百二十五条第３項 | 政府認証基盤（GPKI）の代わりにUPKI電子証明書発行サービスの利用を推奨した。 |
| 電子署名 | D2101（情報セキュリティ対策基準）第百四十四条第５項 |
| 脆弱性対策 | D2101（情報セキュリティ対策基準）第百二十九条第３項 | 学内で開発されたソフトウェアについても、脆弱性対策の対象となることを解説に追記した。 |
| 学内設備管理 | D2101（情報セキュリティ対策基準）第二百六条、第二百七条、第二百八条 | 学内の「情報コンセント」や学外から持ち込まれた機器の学内ネットワークへの接続、その他情報関連の資源管理に関する規定を追加した。 |
| 学内ネットワーク管理 | D2101（情報セキュリティ対策基準）第二百九条 | 部局単位でネットワーク管理を行う場合の対応に関する規定を追加した。 |
| 学外ネットワーク対応 | D2101（情報セキュリティ対策基準）第二百十条 | 上流ネットワークの利用規程（AUP）への対応に関する規定を追加した。 |

(2) 注意事項について

　サンプル規程集を構成する文書のうち、その内容が統一基準に準拠している規程及び基準については、(1)に示した変更点を除き、統一基準の内容をそのまま適用している、この結果、統一基準において個別機関の事情を反映可能とすることを目的に導入されている以下の表現についてもそれらの文書中に含まれている。

　①メタ規定：関連する規定を整備することが遵守事項となっているもの

　②例示：「以下を例とする」等の表現により規定内容が曖昧なもの

これらの表現に修正を加えることなくそのまま大学等の規程等として運用すると、策定した規程や基準が統制としての効力を十分に発揮しない恐れがある。そこで、2019年度版より新たにサンプル規程集における該当箇所に「注意：」の見出しによる注意書きを赤字で挿入し、規程等の整備担当者に対して注意を促すこととした。

(3) 解説について

　「政府機関等の対策基準策定のためのガイドライン」（平成30年度版）に記載されている解説事項は、政府機関固有の内容を除き、「D1001（情報セキュリティ対策基本規程）」及び「D2101（情報セキュリティ対策基準）」のいずれかの解説として図表を含めて掲載している。また、大学等において規程・基準等の文書を規定する上で考慮すべき事項について、これまでと同様サンプル規程集独自の解説として記載しているので参考にされたい。

６．検討メンバー（所属は参加時点のもの）

○大学共同利用機関法人情報・システム研究機構 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」

稲葉宏幸（京都工芸繊維大学），上田浩（法政大学），上原哲太郎（京都大学），  
岡田仁志（副主査，国立情報学研究所），小川賢（幹事，神戸学院大学），  
岡部寿男（京都大学），折田彰（京都大学），金谷吉成（東北大学），木下宏揚（神奈川大学），  
佐藤周行（東京大学），佐藤慶浩（オフィス四四十六），庄司勇木（日本開発研究所三重），  
須川賢洋（新潟大学），曽根秀昭（主査，東北大学），高倉弘喜（国立情報学研究所），  
中村素典（京都大学），中山雅哉（東京大学），西村浩二（広島大学），  
長谷川明生（中京大学），浜元信州（群馬大学），冨士原裕文（富士通），丸橋透（明治大学）

○大学共同利用機関法人情報・システム研究機構 国立情報学研究所 学術情報ネットワーク運営・連携本部「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」

飯田勝吉（東京工業大学），板垣毅（東北大学），上原哲太郎（京都大学），

岡田仁志（副主査，国立情報学研究所），岡部寿男（京都大学），岡村耕二（九州大学），

折田彰（京都大学），垣内正年（奈良先端科学技術大学院大学），笠原義晃（九州大学），

金谷吉成（東北大学），上岡英史（芝浦工業大学），貴志武一（東京工業大学），

鈴木孝彦（九州大学），曽根秀昭（主査，東北大学），高井昌彰（北海道大学），

高倉弘喜（京都大学），竹内義則（名古屋大学），谷本茂明（国立情報学研究所），

中野博隆（大阪大学），中山雅哉（東京大学），西村浩二（広島大学），林田宏三（熊本大学），平塚昭仁（徳島大学），布施勇（徳島大学），松下彰良（東京大学），南弘征（北海道大学），湯浅富久子（高エネルギー加速器研究機構）

協力：文部科学省大臣官房政策課情報化推進室，文部科学省研究振興局情報課，

内閣官房情報セキュリティセンター

○社団法人電子情報通信学会「ネットワーク運用ガイドライン検討ワーキンググループ」

稲葉宏幸（京都工芸繊維大学），岡田仁志（国立情報学研究所），

小川賢（幹事，神戸学院大学），垣内正年（奈良先端科学技術大学院大学），

金谷吉成（東北大学），木下宏揚（神奈川大学），楠元範明（早稲田大学），

佐藤慶浩（日本HP），下川俊彦（九州産業大学），須川賢洋（新潟大学），

曽根秀昭（主査，東北大学），高倉弘喜（京都大学），高橋郁夫（弁護士），

辰己丈夫（東京農工大学），中西通雄（大阪工業大学），中野博隆（大阪大学），

西村浩二（広島大学），野川裕記（東京医科歯科大学），長谷川明生（中京大学），

冨士原裕文（富士通），前野譲二（早稲田大学），丸橋透（ニフティ），三島健稔（埼玉大学）

７．参考資料等

**ア. 情報セキュリティポリシーに関連するもの**

(1) 政府機関の情報セキュリティ対策のための統一基準群（サイバーセキュリティ戦略本部）

https://www.nisc.go.jp/active/general/index.html

国の行政機関及び独立行政法人等を対象とする情報セキュリティ対策のための統一的な枠組みとして公表されている。

(2) 教育情報セキュリティポリシーに関するガイドライン（文部科学省）

http://www.mext.go.jp/a\_menu/shotou/zyouhou/detail/1397369.htm

今後の学校（小学校、中学校、義務教育学校、高等学校、中等教育学校及び特別支援学校）における情報セキュリティポリシーの考え方及び内容について解説したものである。

(3) 学術認証フェデレーション“学認”（国立情報学研究所）

https://www.gakunin.jp/

国内大学等と学術サービスを提供する企業を対象に、国立情報学研究所が運営している認証連携基盤である。

**イ. 情報セキュリティや著作権保護に関するもの**

(1) 内閣サイバーセキュリティセンター

http://www.nisc.go.jp/

政府機関の情報セキュリティ対策のための統一基準に関する関連資料がある。

(2) 警察庁 サイバー犯罪対策プロジェクト

http://www.npa.go.jp/cyber/

サイバー犯罪に関する啓発資料等。

(3) 総務省 国民のための情報セキュリティサイト

http://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/

情報セキュリティ対策に関する啓発資料等。

(4) 経済産業省 情報セキュリティ政策

http://www.meti.go.jp/policy/netsecurity/

情報セキュリティ監査制度に関する基準類等がある。

(5) 独立行政法人情報処理推進機構（IPA）　情報セキュリティ

http://www.ipa.go.jp/security/

コンピュータウイルスや不正アクセスの届出状況や、各種啓発資料を参照できる。

(6) 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

http://www.jpcert.or.jp/

最新の脅威に関する注意喚起や緊急報告等。

(7) 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）

http://www.jnsa.org/

情報セキュリティ対策製品・サービス提供企業の会員による各種活動成果を公開。

(8) 特定非営利活動法人情報セキュリティ研究所（RIIS）

http://www.riis.or.jp/

情報セキュリティ関連のシンポジウムや研修を実施。

(9) 公益社団法人著作権情報センター（CRIC）

http://www.cric.or.jp/

著作権に関する関係法令やQ&A集などを参照することができる。

(10) プロバイダ責任制限法ガイドライン等協議会（一般社団法人テレコムサービス協会内）

http://www.telesa.or.jp/consortium/provider/

著作権関係ガイドライン等が参照できる。

(11) インターネットホットラインセンター

http://www.internethotline.jp/

有害情報や違法情報に関する具体例などがある。