元文科高第５９号
令和元年５月２４日

各国立大学法人の長
大学及び高等専門学校を設置する各地方公共団体の長
各公立大学法人の理事長
大学及び高等専門学校を設置する各学校法人の理事長
放送大学学園理事長
大学を設置する各学校設置会社の代表取締役
各大学共同利用機関法人機構長
独立行政法人国立高等専門学校機構理事長
殿

文部科学省総合教育政策局長
清水　明
（印影印刷）

文部科学省高等教育局長
伯井美徳
（印影印刷）

文部科学省研究振興局長
磯谷桂介
（印影印刷）

大学等におけるサイバーセキュリティ対策等の強化について（通知）

大学等におけるサイバーセキュリティ対策等については、平成28年に発出した「国立大学法人等における情報セキュリティ強化について（通知）」（平成28年6月29日付28文科高第365号）、「公立大学等における情報セキュリティ対策の強化について（通知）」（平成28年12月27日付 28文科高第882号）及び「私立大学等を設置する学校法人等における情報セキュリティ対策の強化について（通知）」（平成28年12月26日付 28文科高第879号）に基づき、各大学等において主体的な取組が行われています。

その結果、文部科学省が大学等から報告を受けたインシデントの件数は平成28年度をピークとして減少傾向にある一方でUSBメモリやノートパソコンの紛失・盗難による情報漏えい事案のように基本的な情報セキュリティ対策の未実施や意識の欠如に起因するインシデントが依然

として多く発生しています。また、マルウェア感染や不正アクセス等のサイバー攻撃についても、同様に非常に多く発生しており、とりわけ、国の政策に関わる情報や先端技術情報等の窃取を目的としたと思われる標的型攻撃（高度サイバー攻撃）も件数としては僅かではあるものの、発生しています。

このような背景のもと、平成30年7月には、政府の「サイバーセキュリティ戦略」が改定され、新たな施策として「4.2.4 大学等における安全・安心な教育・研究環境の確保」が追加され、大学等に対して、一定レベルのサイバーセキュリティ対策の実施を求めるとともに、文部科学省としても、大学等の取組を支援していくことが求められています。さらに、「4.3.2 我が国の防御力・抑止力・状況把握力の強化」として、科学技術競争力や安全保障等に係る技術情報を保護するため、先端的な技術情報等を保有する大学等に対して、サイバー攻撃による当該情報の漏えいを防止するための取組を促すとともに、文部科学省が支援することが求められています。

加えて、2020年東京オリンピック・パラリンピック競技大会（以下「2020年東京大会」という。）においては、我が国に対するサイバー攻撃の急増が予想されていることから、2020年東京大会の開催までに必要な対策を完了し、万全の体制で臨むことが求められています。

これらの状況に鑑み、文部科学省では、大学等におけるインシデントの再発防止及びサイバーセキュリティ対策等の更なる強化を目的として、各法人において必要と考えられる取組を、別添「大学等におけるサイバーセキュリティ対策等の強化について」のとおりまとめました。

ついては、とりまとめの趣旨に基づき、国立大学法人等においては、既存の「情報セキュリティ対策基本計画」について、「サイバーセキュリティ対策等基本計画」として令和元年9月末までに改定願います。また、公私立の大学及び高等専門学校においては、別添の取組により、サイバーセキュリティ対策等の強化に努めていただくよう改めてお願いします。

なお、こうした取組と併せて、大学等においては、不審者の侵入防止や、大学等で適正な管理が必要な物品等の紛失・盗難防止などの基本的なセキュリティ対策の強化にも努めていただくよう改めてお願いします。

○ 国立大学法人等･･･国立大学法人、大学共同利用機関法人、放送大学学園及び独立行政法人国立高等専門学校機構を指す。
○ 大学等･･･「国立大学法人等」に公立大学及び公立高等専門学校並びに私立大学等を設置する学校法人を加えたものを指す。

＜本件連絡先＞ 文部科学省代表番号：０３－５２５３－４１１１
（国立大学法人）高等教育局国立大学法人支援課法規係　内線：３７６０
（公立大学等）高等教育局大学振興課公立大学係　内線：３３７０
（私立大学等）高等教育局私学部私学行政課企画係　内線：２５３３
（放送大学学園）総合教育政策局生涯学習推進課放送大学振興係　内線：３４５９
（高等専門学校）高等教育局専門教育課高等専門学校係　内線：３３４７
（大学共同利用機関法人）研究振興局学術機関課機構総括係　内線：４３０２
（その他サイバーセキュリティ等全般に関すること）大臣官房政策課サイバーセキュリティ・情報化推進室　情報統括係・サイバーセキュリティ係　内線：２２４８

別添

文部科学省

大学等におけるサイバーセキュリティ対策等の強化について

1. 大学等におけるサイバーセキュリティ対策等の強化のための基本的な考え方

IT環境やサイバーセキュリティ等を取り巻く情勢の大きな変化や、サイバー攻撃のさらなる複雑化・巧妙化が生じており、求められる対策・対応も急速に高度化し、増大しつつある。

特に、大学等においてパブリッククラウドサービス（以下「クラウド」という。）が一層活用されるようになったことや、学内外のあらゆる場所に端末を持ち運び、インターネットに接続して教育・研究・業務を行うことが当たり前となったことで、従来の大学等における境界防御を中心とした対策に加えて、クラウド利用時の対策や端末側のサイバーセキュリティ対策の重要さが増している。

一方で、多様な構成員によって構成され、多岐にわたるIT資産、多様なシステムの利用実態を有する大学等の特性を踏まえると、フィジカル（実）空間における情報の機密性・完全性・可用性の確保のために行われる情報セキュリティ対策は依然として重要である。

そのような状況において、大学等が教育・研究・社会貢献といった役割を今後も果たしていくためには、「サイバーセキュリティ戦略」に示された３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）を踏まえながら、サイバーセキュリティを取り巻く情勢の変化に応じて求められる対策を着実かつ継続的に行うとともに、以下の考え方に基づいて、セキュリティ水準の維持・向上を絶えず図っていくことが必要である。

(1) 法人トップの強いリーダーシップに基づく必要な体制整備、資源確保、構成員の意識向上

公共性の高い大学等において、サイバーセキュリティ対策等は社会的に求められるものであり、経営上の重要課題との認識の下、法人全体として組織的・計画的に取り組むべきものである。

各大学等においてサイバーセキュリティ対策等を進めるに当たっては、学長や理事長等の法人のトップが自ら強いリーダーシップを発揮し、企画・人事・財務などの担当理事と連携しながら、取組に必要な体制の整備及び資源の確保を行い、組織全体として計画的に取り組むことが重要である。

また、各大学等が果たすべき役割を着実に遂行するためには、必要となる能力及び資産を確保し、安全かつ持続的な業務・サービスの提供に関する責任を全うすることが必要である。そのため、各法人のトップは、構成員に対して、主体的にサイバーセキュリティ等の確保に取り組むよう意識向上を促すことが必要である。

(2) 濃淡を付けバランスの取れた対策の実施

限りある資源を有効に活用し、効率的にサイバーセキュリティ対策等を推進するためには、法人として保護すべき重要な業務・サービスとそうでないものに分け、前者について優先順位を付けつつ、重点的に対策を行い、後者については各種ガイドライン等に基づき必要とされる最低限の対策を行うなど、濃淡を付けて取り組むことが重要である。また、取組に当たっては、IT投資

全体の最適化を行い、組織として得られる効用が最大化されるように実効性を重視し、バランスの取れたサイバーセキュリティ対策等を実施することも必要である。

(3) 先端技術情報を始めとする機微情報の保護

個人情報の適切な管理については言うまでもないが、一方で、先端的な技術情報についても適切な管理が社会的に強く求められている。そのため、先端的な技術情報を保有する大学等にあっては、当該情報の適切な管理は、我が国の科学技術競争力の維持及び強化や安全保障貿易管理のみならず、外部からの信頼確保等の点からも極めて重要である。

また、国の審議会等の委員を務める教職員についても、国等が保有する機密性の高い情報に接する機会があることから、当該情報を保護するための対策が必要である。

2. 各組織において必要な対応

2.1. 大学等が対応すること

2.1.1. 大学等が共通して対応すること

各大学等においては、1.の基本的な考え方に沿って、令和元年10月から令和4年3月を計画期間として、サイバーセキュリティ対策等の目標及び実施方針等を記載した「サイバーセキュリティ対策等基本計画」（以下「対策基本計画」という。）を策定するものとする。なお、上記計画期間を超えて対策基本計画を策定することは妨げない。対策基本計画を策定する際には、限られた資源で効果的かつ効率的に対策を講じる観点から、対策の重要性や優先順位とともに、これらに対応した適切な資源配分等も考慮するものとする。

対策基本計画については、定期的に進捗状況を評価し、その結果やサイバーセキュリティ等を取り巻く情勢の変化を踏まえ、必要に応じて見直すものとする。

なお、対策基本計画は、各法人等が既に策定している情報セキュリティポリシーや情報戦略等の計画との整合性にも留意して策定することとし、重大なセキュリティインシデント（以下「インシデント」という。）を招く恐れがあるものについては、対策基本計画の策定・改定を待たず、可能なものから速やかに実施するものとする。

以下、大学等が共通して対応すべきことを示す。各大学等においては、これらの対応が円滑になされるよう、学長、機構長、理事長等の法人のトップが責任をもってCISOを支援するとともに、構成員の意識向上を図ることとする。

(1) 実効性のあるインシデント対応体制の整備

① インシデント発生時の対処として想定される以下のプロセスが迅速かつ的確に行われるよう、実効性のあるインシデント対応体制(CSIRT)を整備する。[1]

- 検知／連絡受付
- トリアージ[2]
- インシデントレスポンス
- 報告／情報公開

その際、インシデント対応を内製化できる部分とできない部分を分け、後者については、外部専門家の支援を迅速に受けられる体制を整備する。また、必要に応じて企画・法務・広報等の組織内の関連部門と連携して対処できる体制を整備する。

② 文部科学省の法人所管課を通じて通知されるインシデント対応要領に従い、文部科学省の法人所管課を始めとする関係部署への報告・連絡、被害拡大防止等、迅速かつ的確な初動対応とそれに関わる手順書や緊急連絡網を担当部門において作成し、関係者間で共有しておく。インシデント対応体制や手順書を既に整備している場合も、常に最新のセキュリティ脅威や脆弱性を意識して、適時適切に更新を行う。また、外部からの通報を受けられるよう、大学等の公式ウェブサイト等に外部からのインシデント通報受付窓口を明示する。

③ 自組織の名前で外部に公開している自組織管理下の情報機器やサービス（外部ホスティングサービスやクラウド等を利用している場合を含む）を定期的に調査し、把握しておく。また、緊急時に停止可能な情報機器と業務継続のため無停止が求められる情報機器についても事前に把握しておく。さらに、情報システムの停止及びネットワークの遮断並びにこれらの復旧等の必要な手順書を作成し、関係者間で共有しておくとともに、手順書に基づき適切に対応するための訓練を実施する。

④ インシデント発生時のみならず、平時からインシデントの予防や早期発見につながる活

---

[1] CSIRT構成員については、可能な限り専任の担当者を置くことが望ましい。

[2] インシデント対応に当たり、優先順位付けを行うもの。

動（ログの分析、脆弱性情報の確認・評価、公開サーバ等に対する脆弱性診断やOSINT[3]等）を行う。

⑤ インシデント対応を行う担当者（担当役員を含む）を対象としたインシデント対応訓練を定期的に（少なくとも年１回以上）実施し、インシデントへの対応力を高めておく。また、担当者を外部の研修・演習やカンファレンス等に積極的に派遣し、知識・技術の習得や人脈の構築を促進する。

(2) サイバーセキュリティ等教育・訓練や啓発活動の実施

① 「任務保証」の考えに基づき[4]、各々の組織の業務・サービスを着実に遂行するために必要となる能力及び資産を確保するため、全構成員が主体的にサイバーセキュリティ等の確保に取り組むべきであることを繰り返し啓発する。

② 全構成員が共通して受講すべきセキュリティ教育に加え、役員、部局長、部課長、システム管理者、重要情報を取り扱う担当者に対して、その役職と責任に応じたサイバーセキュリティ教育や啓発活動を定期的（毎年度）に実施する。また、教育・訓練の受講状況や結果を把握し、未受講者にも受講を促す仕組みを整備する。

③ インシデント防止のみを想定するのではなく、インシデントが発生した場合に、迅速かつ的確に対応できるよう実践的かつ関係部門横断的な対応訓練も実施する。

④ 教育・訓練や啓発活動の実施内容として、過去に自組織でインシデントが発生している場合は、当該インシデントに係る知見が引き継がれるよう、インシデントの概要、原因及び再発防止策等に係る内容を含める。

⑤ 非常勤職員や派遣職員、非常勤講師や客員教員等、随時採用される職員だけでなく、新・編入生や留学生対応としてリーフレットを作成し、大学等の情報システムやネットワークを利用する際に遵守させるべき必要最低限の事項について周知徹底を行う。

(3) 情報セキュリティ対策に係る自己点検及び監査の実施

① 構成員が自らの役割に応じた情報セキュリティ対策が実施できていることを確認するため自己点検を定期的（毎年度）に実施し、点検結果を踏まえた改善策を対策基本計画に反映し、継続的にフォローアップを行う。

② 内部又は中立性を有する第三者による情報セキュリティ監査を定期的（毎年度）に実施し、指摘事項に対する改善策を対策基本計画に反映し、継続的にフォローアップを行う。

③ 自己点検及び監査の実施内容として、過去に自組織でインシデントが発生している場合は、当該インシデントに係る知見が引き継がれるよう、インシデントの概要、原因及び再発防止策等に係る内容を含める。

④ 監査の実施内容として、情報システムの脆弱性診断だけでなく、情報セキュリティポリシーや実施手順書等の遵守状況を確認するために行うマネジメント監査についても実施する。

⑤ 法人全体として、実効性のある自己点検・監査実施体制を整備[5]する。

---

3 公開情報を元にサイバー攻撃等に係る脅威情報等を収集・分析するもの。

4 「任務保証」とは、企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保することである。その際には、一部の専門家に依存するのではなく、各々の組織の「任務」に該当する業務・サービスを遂行する観点から、その責任を有する者が主体的にサイバーセキュリティの確保に取り組むことが肝要である。すなわち、これは、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。（出典：「サイバーセキュリティ戦略」（平成30年7月27日閣議決定））

5 各法人における監査の在り方にもよるが、例えば、計画策定や連絡調整等の管理業務は業務監査担当部署が主体となって行い、

(4) 他機関との連携・協力

大学等は共通の情報基盤を利用しており、共通性が見られるサイバーセキュリティ上の課題を有していることから、単独で実施するよりも他機関と連携・協力してすることが有効な場合があることから、以下の取組等について、実施を検討する。

① セキュリティ機器やサービス等について、複数の大学等で共同調達・共同利用する。

② セキュリティポリシー、実施手順書、調達仕様書の雛形、注意喚起文、教育・訓練コンテンツなど、サイバーセキュリティ対策等に係る様々な文書について、複数の大学等で作成・共有する。

③ セキュリティ監査について、あらかじめ協定や覚書を交わした近隣の大学等との間で相互監査を実施する。

④ 災害復旧・事業継続対応について、あらかじめ協定や覚書を交わした遠隔地の大学等との間で、相互にバックアップデータの保管やバックアップサイトの整備を行う。

⑤ インシデント発生時の対応について、あらかじめ協定や覚書を交わした近隣の大学等との間で救援体制を整備する。

⑥ 複数の大学等の CSIRT 間でインシデント情報や脅威情報、対処経験、機器やツールの情報や知見を共有したり、共同で訓練・演習を行う。

(5) 必要な技術的対策の実施

① グローバルＩＰアドレスを付与する情報機器は漏れ無く把握し管理する。なお、情報機器の把握ができていない場合は、実態について調査し把握することについて対策基本計画に盛り込み、正確にＩＰアドレスが管理できる仕組みを検討する。なお、クラウドサービスやホスティングサービス等を利用して学外に構築しているシステムについても、可能な限り把握し管理する。

② グローバルＩＰアドレスを使用する情報機器については、通信要件を把握して不必要な接続を遮断する等適切なアクセス制御[6]と権限管理を行う。研究室等において管理者に無許可でサーバ等が設置されないよう必要な措置等を講ずる。

③ オペレーティングシステムやアプリケーションソフトウェア等について、必要に応じて更新ができる仕組みを構築し適用漏れが無いようにする。また、ソフトウェアのサポート期間等のライフサイクル等を考慮した適切なソフトウェアの運用管理を行う。

④ 学外からアクセス可能なウェブメールシステムやクラウドメールシステムについて、多要素認証の導入や定期的なログの確認など、不正アクセス対策を強化する。多要素認証を導入できない場合は、強度の高いパスワードの設定や、定期的なパスワード変更の実施、学外の他システムとのパスワードの使い回しの禁止など、対策を強化する。また、ユーザのアカウント情報は定期的に棚卸しを行うとともに、退職者のアカウントは速やかに削除又は停止する[7]。

⑤ 外部からマルウェア感染等に伴う不審な通信に係る情報が提供された際に、当該不審な通信の発生源となっている端末を特定するために必要なログ等（例えば、DNS サーバや DHCP サーバのログ等）について、平時から取得・管理[8]する。

⑥ 法人内に存在する全ての ActiveDirectory 等の利用者や資源を登録・管理しているサー

専門的知見を要するヒアリングや検査などの実務は情報セキュリティ担当部署が行うなど、役割を分担して実施することが考えられる。

6 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）P.183~P.184「6.1.2 アクセス制御機能」の解説を参照。

7 退職者のアカウントは、退職後１ヶ月程度以内に削除又は停止する事が望ましい。

8 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）P.188~P.191「6.1.4 ログの取得・管理」の解説を参照。

バを特定し、アカウントの棚卸し、ログ取得、パッチ適用等の基本的な対策を実施する。また、重要情報を扱う部門の ActiveDirectory サーバ等については、別添に示す参考資料等を参照し、標的型攻撃を踏まえた多層防御及び堅牢化[9]を行う。

(6) その他必要な対策の実施

① 組織として守る必要がある情報を特定し、脅威や発生確率に基づくリスク評価を行った上で、実施すべき対策を検討するとともに、対策に必要な予算や体制を措置する。

② サイバーセキュリティを取り巻く状況が変化しても、一定水準の対策レベルを維持していくため、各大学等において独自色の強い対策を実施するのではなく、「政府機関等の対策基準策定のためのガイドライン」や「高等教育機関向けサンプル規程集」、文部科学省から別途提示予定のガイドラインや対策事例集、その他各組織・団体が作成している最新のガイドラインや対策資料等を参照し、各大学等において必要な対策を実施する。

③ クラウドの利用に当たっては、情報の適正な取扱いが行われていることを直接確認することが一般に容易ではないことや、国内法以外の法令が適用されるリスクがあることなどの特性を踏まえるとともに、多要素認証が設定可能であるか否かを確認する。

④ 大学等支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置や、大学等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置に関する手順等を整備する。

⑤ USB メモリ等の外部電磁的記録媒体を用いて要機密情報を取り扱うことを許容する場合は、取扱いに関する手順等を定める。

⑥ 外部委託先において必要なセキュリティ対策が確実に実施されるよう、外部委託先に求めるセキュリティ要件を各大学等内で統一的に整備し、調達仕様書等へ記載するとともに、外部委託先における対策の履行状況を確認する。

⑦ 教室、研究室、事務室、会議室、サーバ室等の情報を取り扱う区域において、区域の明示、施錠、入退室管理等の対策を講じ、当該区域で取り扱う情報や情報システム等のセキュリティを確保するとともに、重要な書類や外部記録媒体、ノートパソコン等の備品、その他毒物、劇物等の化学物質等を含む適正な管理が必要な物品等について、管理を徹底し、紛失・盗難の対策を講じる。

2.1.2. 国立大学法人等が対応すること

(1) 情報セキュリティ対策基本計画の評価及び見直し（令和元年 9 月末まで）

① 各法人は現行の情報セキュリティ対策基本計画の実施状況を自己評価する。

② 自己評価結果並びに上記 1、2.1.1 及び 2.1.2(2)(3)を踏まえた上で、令和元年 10 月から令和 4 年 3 月までを計画期間とする「サイバーセキュリティ対策等基本計画」として改定する。

(2) セキュリティ・IT 人材の育成

① 各法人における司令塔機能の強化

(ア)CISO・CIO を補佐し、学内を指揮監督できる専門人材を副 CISO・副 CIO として学内

---

9 例えば「ログを活用した Active Directory に対する攻撃の検知と対策」（2017 年 7 月 JPCERT/CC）等を参照。
https://www.jpcert.or.jp/research/AD.html

外から登用したり、担当部署を設置するなど、セキュリティ・ITに係る司令塔機能を強化する。

② 戦略マネジメント層及び実務者層の確保・育成

(ア)セキュリティ・ITに係る統括部局の体制の整備及び人材の拡充を実施する。

(イ)セキュリティ関連資格保有者や危機管理業務従事者など、有為な人材を確保する。

(ウ)セキュリティ対策業務に従事する一定の専門性を有する人材を育成する。

(エ)セキュリティ・ITに係る統括部局や執行部の役職員に対して、学内外の研修や演習に参加させ、計画的に人材を育成する。

(オ)将来的にCISOや戦略マネジメント層になり得る教職員等を確保・育成するため、実務者層における中長期的なキャリアパスを構築する。

③ 外部人材（即戦力の高度専門人材）の活用

(ア)サイバー攻撃やインシデントレスポンスに知見を有する人材が不足する場合、過渡期における一時的な対応として、例えば、民間企業等から専門家をクロスアポイントメント制度等を活用して受け入れ、内部人材の育成に資する。

(3) 災害復旧計画及び事業継続計画におけるセキュリティ対策に係る記載の追加等

① 各法人の災害復旧計画（DR）及び事業継続計画（BCP）において、サイバー攻撃やその他大規模システム障害等を踏まえた、可用性の維持に係るサイバーセキュリティ対策等の記載があるかどうか確認する。記載がない場合、各法人の授業・研究・業務の実情を踏まえ、記載が必要と判断される場合は追記する。

② 附属病院の診療系システムのように、システムの停止が国民の生命、身体及び財産に大きな影響を及ぼしうるシステムについては、情報システム運用継続計画（IT-BCP）を策定する。

2.1.3. 公私立大学が対応すること

公私立大学においてもサイバーセキュリティ対策等を着実に実施するため、2.1.1の取組に加え、以下の取組に努めるものとする。

(1) サイバーセキュリティ対策等推進のための組織・体制の整備

① 各大学においてサイバーセキュリティ対策等を推進するため、以下を例とする組織・体制を整備する。

(ア)最高情報セキュリティ責任者（CISO）の設置

(イ)情報セキュリティ委員会の設置

(ウ)情報セキュリティ監査責任者の設置

(エ)統括情報セキュリティ責任者・情報セキュリティ責任者等の設置

(オ)最高情報セキュリティアドバイザーの設置

(カ)情報セキュリティ対策推進体制の整備

(キ)インシデントに備えた体制（CSIRT）の整備

(2) 情報セキュリティポリシー及び実施手順書の策定

① 各大学において情報セキュリティ水準を適切に維持し、リスクを総合的に低減させるため、自組織において遵守すべき対策の基準として情報セキュリティポリシーを策定する。

② 各大学は、情報セキュリティポリシーにおいて定めた対策を実施するため、具体的な実施手順書を作成する。

2.1.4. 先端的な技術情報等を保有する大学等が対応すること

我が国の科学技術競争力や安全保障に係る先端的な技術情報等を保有する大学等においては、組織全体に共通して実施するセキュリティ対策に加え、当該技術情報等をサイバー攻撃等の脅威から保護するために必要な対策を重点的に実施していく必要がある。

(1) 先端的な技術情報等の漏えいを防止するために必要な措置の実施

① 我が国の科学技術競争力や安全保障貿易管理に係る先端的な技術情報等、組織として保護対象とする情報を特定する[10]。

② 当該情報をサイバー攻撃等の脅威から保護するため、産業競争力強化法（平成二十五年法律第九十八号）第二条第十九項第一号の規定に基づき定められた「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」も参考に対応を行う。

(2) 高度サイバー攻撃を踏まえた技術的対策

① 内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）等が作成・公開している高度サイバー攻撃対策に係る各種資料等に基づき、速やかに技術的対策を講じる。

② 先端的な技術情報を取り扱う機器については、真に必要な場合を除きグローバルＩＰアドレスを付与しないこととする。グローバルＩＰアドレスを付与した機器から当該情報を取り扱う機器へのアクセスがある場合には、当該アクセスを監視・保護する機能を備える。

(3) サプライチェーン・リスクへの対応

情報システム・機器・役務等の調達に当たっては、サプライチェーン・リスクを軽減するための要求要件を調達仕様書に記載するなど、必要な対策を講じる。

(4) 組織内における必要な予算及び人材の優先的な確保

上記(1)～(3)の実施に必要な予算及び人材を優先的に確保する。

---

10 当該情報の特定に当たっては、例えば、各大学等において、宇宙・原子力等の研究分野のうち、一定規模の競争的資金やプロジェクト研究、共同研究などに限定した上で、各法人に設置された安全保障貿易に係る管理部門や産学連携部門とセキュリティ担当部門が連携しながら特定作業を行うことなどが考えられる。

参考資料

1. サイバーセキュリティ全般

- サイバーセキュリティ戦略（平成30年7月27日閣議決定）（抄）
  https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

4. 目的達成のための施策
4.2. 国民が安全で安心して暮らせる社会の実現
4.2.4 大学等における安全・安心な教育・研究環境の確保

大学及び大学共同利用機関等（以下「大学等」という。）は、多様な構成員によって構成され、多岐にわたるIT資産、多様なシステムの利用実態を有する。このような大学等の特性を踏まえ、安全・安心な教育・研究環境を確保するためには、大学等において自律的にサイバーセキュリティ対策を行うとともに、大学等の連携協力によるサイバー攻撃への対応体制の構築や情報共有等を国が積極的に支援することが重要である。

(1) 大学等の多様性を踏まえた対策の推進

大学等の経営層は、自らサイバーセキュリティ対策の重要性を認識した上で、サイバーセキュリティ対策を経営上の重要課題と位置付け、対策を推進するための計画等に基づき自律的かつ組織的に取り組むとともに、フォローアップを実施することによりサイバーセキュリティ対策を一層推進する必要がある。

こうした取組に当たっては、様々な教育・研究を実施している大学等の多様性を踏まえつつ、守るべきIT資産を特定し、サイバーセキュリティに係るリスクの評価を行い、リスクに応じて重点的に実施するべきマネジメント面・技術面における対策を検討することが求められる。また、事案に適切かつ迅速な対処をするための能力の向上に向けた取組や、これらの対策を組織的かつ着実に実施するための体制についても検討する必要がある。

国は、大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する各層別研修及び実践的な訓練・演習の実施、事案発生時の初動対応への支援を通じて、大学等における自律的かつ組織的な取組を促進する。

(2) 大学等の連携協力による取組の推進

大学等は、共通の情報基盤を利用しており、共通性が見られるサイバーセキュリティ上の課題を有している。こうした大学等の実態を踏まえたサイバーセキュリティ対策の強化が重要であり、各々の相互協力による取組の一層の促進が求められている。

このため、学術情報ネットワークを運営する機関は、国立大学及び大学共同利用機関と連携し、サイバー攻撃を観測・検知・分析するシステムを構築し、情報提供を行うとともに、監視能力の機能維持・強化及び戦略マネジメント層の育成に向けた共同研究や技術職員への研修を実施する。

さらに、国は、大学等の事案対応体制を強化するため、複数の大学等の事案対応を行うチームにおいてサイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための取組を支援する。

4.3. 国際社会の平和・安定及び我が国の安全保障への寄与
4.3.2 我が国の防御力・抑止力・状況把握力の強化
(1) 国家の強靭性の確保
② 我が国の先端技術・防衛関連技術の防護

先端技術は、経済的な優位性を保障するだけでなく、安全保障上も重要な国家的資産である。宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等、我が国の安全保障上重要な技術を扱う事業者及び関係省庁における人的要因によるリスク軽減も含めたサイバーセキュリティ対策を強化する。特に防衛産業が取り扱う技術情報等は、それが漏洩・流出した場合の我が国の安全保障上の影響が大きいため、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組を行う。これらについて、官民連携の下、下請け企業等を含めた防衛産業のサプライチェーン全体に適用することを前提とした検討を行う。

また、先端技術情報を保護する観点から、国立研究開発法人や先端的な技術情報を保有する大学等における対策を促進する。

2. 情報セキュリティポリシー等の策定に資するガイドライン等

- 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）」
  https://www.nisc.go.jp/active/general/kijun30.html
- 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（2017年版）
  https://www.nii.ac.jp/service/sp/
- 教育情報セキュリティポリシーに関するガイドライン
  http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm
- 中小企業の情報セキュリティ対策ガイドライン（2019年1月 IPA）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

3. 先端技術情報の保護に資するガイドライン等

- 技術等情報漏えい防止措置の実施の促進に関する指針(平成30年9月25日 内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第五号)
  http://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/02.pdf
- 技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準(平成30年9月25日 内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第三号)
  http://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf
- 安全保障貿易に係る機微技術管理ガイダンス(大学・研究機関用)(第三版)
  http://www.mext.go.jp/a_menu/kokusai/oshirase/08011704.htm

4. その他、ガイドラインやレポート等

4.1. CISO向け

- CISOハンドブック (2018年5月 JNSA)
  https://www.jnsa.org/result/2018/act_ciso/index.html
- サイバーセキュリティ経営ガイドライン Ver2.0 (2017年11月16日 経済産業省)
  http://www.meti.go.jp/policy/netsecurity/mng_guide.html
- サイバーセキュリティ経営ガイドライン解説書 (2017年5月15日 IPA)
  https://www.ipa.go.jp/files/000056148.pdf
- 経営者が知っておくべきセキュリティリスクと対応について (2013年4月9日 JPCERT/CC)
  https://www.jpcert.or.jp/research/APTRiskReport20130409.pdf

4.2. CSIRT関係

- サイバーインシデント緊急対応企業一覧 (2018年10月 JNSA)
  https://www.jnsa.org/emergency_response/
- セキュリティ対応組織の教科書 v2.1 (2018年9月 ISOG-J)
  https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

  https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx
- CSIRTマテリアル (2015年11月26日 JPCERT/CC)
  https://www.jpcert.or.jp/csirt_material/
- CSIRTスタータキット Ver2.0 (2011年8月 NCA)
  http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

4.3. 普及啓発・人材育成関係

- サイバーセキュリティ意識・行動強化プログラム～「参加・連携・協働」の実現を目指して～ (2019年1月24日 サイバーセキュリティ戦略本部)
  https://www.nisc.go.jp/active/kihon/pdf/awareness2019.pdf
- サイバーセキュリティ人材育成取組方針の決定について (2018年5月31日サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会)
  https://www.nisc.go.jp/conference/cs/pdf/jinzai-hoshin2018.pdf
- サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書 ～「戦略マネジメント層」の育成・定着に向けて～ (2018年5月31日サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ)
  https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf
- 「橋渡し人材のスキル認定の基準」について (2018年4月3日 サイバーセキュリティ対策

推進会議）
https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai14/pdf/14shiryou05.pdf

- サイバーセキュリティ人材育成総合強化方針（2016年3月31日　サイバーセキュリティ戦略本部）
https://www.nisc.go.jp/active/kihon/pdf/jinzai_kyoka_hoshin.pdf

4.4. 調達関係

- IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ（2018年12月関係省庁申合せ）
https://www.nisc.go.jp/active/general/pdf/chotatsu_moshiawase.pdf
- セキュリティ要件確認支援ツール（2018年11月　独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/isec-sras/index.html
- IT製品の調達におけるセキュリティ要件リスト活用ガイドブック（2018年2月　独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/it-product/guidebook.html
- 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（2016年10月　内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2015年5月　内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/active/general/sbd_sakutei.html
- 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）（2013年3月　総務省、経済産業省）
http://www.soumu.go.jp/main_content/000206523.pdf

4.5. 監査関係

- 情報セキュリティ監査実施手順の策定手引書（2017年4月　内閣官房内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf
- 情報セキュリティ監査基準　Ver1.0（経済産業省）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf

4.6. 業務継続関係

- 中央省庁業務継続ガイドライン 第2版(首都直下地震対策)(2016年4月内閣府(防災担当))
http://www.bousai.go.jp/taisaku/chuogyoumukeizoku/pdf/gyoumu_guide_honbun160427.pdf
- 中央省庁における情報システム運用継続計画ガイドライン及び関連資料（2013年6月　内閣官房情報セキュリティセンター）
https://www.nisc.go.jp/active/general/itbcp-guideline.html
- ITサービス継続ガイドライン改訂版（2012年 経済産業省）
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_IoformationSecurityServiceManagementGuidelineKaiteiban.pdf

4.7. 情報システム（設計・構築・運用等）

- デジタル・ガバメント推進標準ガイドライン(2018年3月30日各府省情報化統括責任者(CIO)連絡会議決定)
https://cio.go.jp/guides
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline.pdf
- SSH サーバセキュリティ設定ガイド V1.0（2015年3月 NCA）
http://www.nca.gr.jp/imgs/nca_ssh_server_config_v01.pdf
- SSL/TLS暗号設定ガイドライン（2018年5月　CRYPTREC）
https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
- Webサイト等の整備及び廃止に係るドメイン管理ガイドライン（2018年3月30日 各府省情報化統括責任者（CIO）連絡会議決定）

https://cio.go.jp/sites/default/files/uploads/documents/domain_guideline.pdf

- OWASP Top 10 2017（2017年12月 OWASP）
  https://www.owasp.org/images/2/23/OWASP_Top_10-2017%28ja%29.pdf
- 安全なウェブサイトの作り方 改訂第7版（2015年3月 IPA）
  https://www.ipa.go.jp/security/vuln/websecurity.html

4.8. クラウド関係

- クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第1版（2018年7月 総務省）
  http://www.soumu.go.jp/main_content/000567140.pdf
  http://www.soumu.go.jp/main_content/000567229.pdf
- クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）（2018年7月 総務省）
  http://www.soumu.go.jp/main_content/000566969.pdf
- 政府情報システムにおけるクラウドサービスの利用に係る基本方針（2018年6月7日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）
  https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

4.9. サイバー攻撃対策関係

- ログを活用したActive Directoryに対する攻撃の検知と対策（2017年7月 JPCERT/CC）
  https://www.jpcert.or.jp/research/AD.html
- 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（2016年10月 サイバーセキュリティ対策推進会議）
  https://www.nisc.go.jp/active/general/risk.html
- 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて（2016年3月 JPCERT/CC）
  https://www.jpcert.or.jp/research/apt-guide.html
- 「高度標的型攻撃」対策に向けたシステム設計ガイド（2014年9月 独立行政法人情報処理推進機構セキュリティセンター）
  https://www.ipa.go.jp/security/vuln/newattack.html
- フィッシング対策ガイドライン 2018年度版（2018年3月 フィッシング対策協議会）
  http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

4.10. 情報管理関係

- NIST SP800-171 連邦政府外のシステムと組織における管理された非格付け情報の保護（2016年12月 米国国立標準技術研究所）
  https://www.ipa.go.jp/files/000057365.pdf
- 管理された非格付け情報の保護対策マネジメントガイドライン ―NISTSP800-171対応のISMSのために―（2018年2月 JASA）
  http://www.jasa.jp/information/public_doc/pdf2017/管理された非格付け情報の保護対策マネジメントガイドライン.pdf

4.11. 医療情報関係

- クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第1版（2018年7月 総務省）（再掲）
  http://www.soumu.go.jp/main_content/000567140.pdf
  http://www.soumu.go.jp/main_content/000567229.pdf
- 医療情報システムの安全管理に関するガイドライン 第5版（2017年5月 厚生労働省）
  https://www.mhlw.go.jp/stf/shingi2/0000166275.html
- 医療情報を受託管理する情報処理事業者向けガイドライン 第2版（2012年10月 経済産業省）
  http://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf

4.12. インシデント関係レポート

- 産総研の情報システムに対する不正なアクセスに関する報告（2018年7月 産業技術総合研究所）
  https://www.aist.go.jp/aist_j/news/announce/au20180720.html