２８文科高第８７９号
平成２８年１２月２６日

大学及び高等専門学校を設置する各学校法人の理事長
大学を設置する各学校設置会社の代表取締役　　殿

文部科学省高等教育局私学部長
村　田　善　則
（印影印刷）

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）

学校法人や国立大学法人等において、脆弱なパスワードの設定による不正アクセスやWebサイトの改ざん、マルウェアの感染による情報漏えい事案等、情報セキュリティインシデントの発生が急増しており、その被害も甚大化する傾向が見られています。

これらの状況に鑑み、文部科学省では、平成２８年１０月１２日付け２８文科政第６３号「文部科学省関係機関における情報セキュリティ対策の強化について（通知）」等において、情報セキュリティ対策の強化について求めてきたところです。

この間、国立大学法人等に対しては、平成２８年６月２９日付け２８文科高第３６５号「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）」（別添）において、国立大学法人等におけるセキュリティインシデントの再発防止並びに情報セキュリティ対策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について周知がなされているところです。

学校法人等においても個人情報を含む多くの情報を取り扱っており、万が一情報セキュリティインシデントが発生した場合には、当該法人の信用失墜を招くだけでなく、多くの関係者に多大な影響を及ぼすことになります。また、公共性の高い学校法人等において、情報セキュリティ対策は社会的に求められるものであり、経営上の重要課題となっています。

ついては、貴法人におかれても、下記のとおり、セキュリティポリシーの策定やその運用状況の確認等、情報システムからの漏えい等を防止するための対策に漏れがないかの点検を改めて実施するとともに、上記通知等も参考としながら、情報セキュリティに関する体制や規程の整備等、情報セキュリティの対策の強化に努めていただくよう改めてお願いします。

記

１．セキュリティポリシーの策定について

セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針であり、企業や組織の情報資産を情報セキュリティの脅威から守るために策定されるものであるが、文部科学省の「学術情報基盤実態調査」によると、平成２７年５月１日現在でセキュリティポリシーを策定済みの私立大学は全体の約６５％にとどまっている。

ついては、セキュリティポリシーを未策定の法人においては早急に策定を行うこと。また、セキュリティポリシーを策定済みの法人においても、最新のセキュリティ脅威や脆弱性、環境の変化等を意識して、必要に応じた改訂を行うことが望まれること。

２．各法人の実態に応じた情報セキュリティ対策の実施について

セキュリティポリシーの策定に加え、別添通知等を参考としながら、各法人において取り扱う情報に応じて適切な情報セキュリティ対策を実施すること。

（参考）

○セキュリティポリシーの策定状況について（平成２７年度学術情報基盤実態調査結果　１４頁）
http://www.mext.go.jp/component/b_menu/other/__icsFiles/afieldfile/2016/03/30/1368699_1.pdf

○国立情報学研究所　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
http://www.nii.ac.jp/csi/sp/

○独立行政法人情報処理推進機構　サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

○総務省　国民のための情報セキュリティサイト　「企業・組織の対策」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/index.html

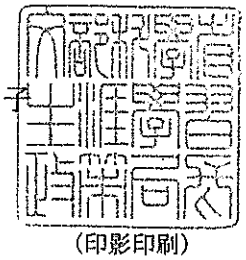
○同　「情報セキュリティポリシーの概要と目的」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-2.html

【本件連絡先】
文部科学省高等教育局
私学部私学行政課企画係
（電話）０３－６７３４－２５２７
（E-mail）sigakugy@mext.go.jp

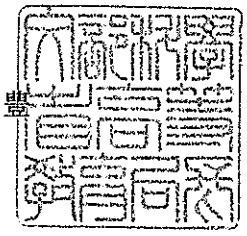
２８文科高第３６５号
平成２８年６月２９日

各国立大学法人の長
各大学共同利用機関法人機構長
放送大学学園理事長
独立行政法人国立高等専門学校機構理事長　殿

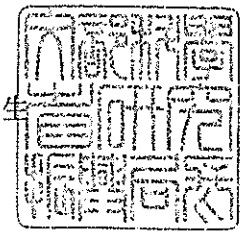
文部科学省生涯学習政策局長
有松育子


（印影印刷）

文部科学省高等教育局長
常盤豊


（印影印刷）

文部科学省研究振興局長
小松弥生


（印影印刷）

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）

昨今、国立大学法人等において、情報セキュリティインシデントの発生が急増しており、その被害も甚大化する傾向が見られています。

これらの状況に鑑み、文部科学省では、国立大学法人等におけるセキュリティインシデントの再発防止並びに情報セキュリティ対策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「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」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、必要な情報セキュリティ対策を組織的、計画的に実施するための「情報セキュリティ対策基本計画」を平成２８年度末までに策定をお願いします。

＜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支援第一係　内線：３７５７

（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

（放送大学学園）
生涯学習局生涯学習推進課放送大学振興係　内線：３４５９

（独立行政法人国立高等専門学校機構）
高等教育局専門教育課高等専門学校係　内線：３３４７

（その他情報セキュリティ全般に関すること）
大臣官房政策課情報システム企画室情報監理係　内線:３０６０

【機密性２（文部科学省及び関係機関内限り）】

文部科学省

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

１．国立大学法人等における情報セキュリティ強化に向けた基本的な考え方

昨今、国立大学法人等において、脆弱なパスワードの設定による不正アクセスやＷｅｂサイトの改ざん、複合機等のインターネットに接続する機器の設定不備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情報セキュリティインシデントが多発している。

国立大学法人等は教育、研究、社会貢献といった責務を負っており、それら業務の遂行と組織の運営において、また、グローバル化の進展が著しい状況において、情報基盤が必要不可欠なものであることは言うまでもない。

万一、不正アクセス等による情報漏えいやＷｅｂサイトの改ざん等の情報セキュリティインシデントが発生した場合、国民の権利侵害や業務遂行が困難になるなど、当該法人の信用失墜を招くだけでなく、多くの関係者に多大な影響を及ぼすことになる。

公共性の高い国立大学法人等において、情報セキュリティ対策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・計画的に取り組む事項である。

今後も国立大学法人等がその責務を果すためには、情報セキュリティ水準の維持・向上を図っていくことが不可欠であり、国立大学法人等の最高情報セキュリティ責任者（ＣＩＳＯ）の下、技術的な対策や監査などの情報セキュリティリスク管理に向けた積極的な取組とともに、情報セキュリティインシデントの発生を前提とし、企画・法務・広報などの担当理事と連携した対応体制の構築と訓練による対処能力の向上を図ることが必要である。

※「国立大学法人等」とは、国立大学法人、大学共同利用機関法人、放送大学学園の他、国立高等専門学校機構を指している。

２．国立大学法人等において必要とされる対策

法人全体として情報セキュリティ対策を実施するため、ＣＩＳＯは法人内に存在する情報セキュリティリスクを適切に評価し、中長期的な視点をもって当該リスクを制御するため「情報セキュリティ対策基本計画」（以下「対策基本計画」という。）を法人全体の計画として策定し、必要な対策を計画的に進めて行く必要がある。

また、対策基本計画の進捗状況は、毎年度、自己点検や監査によって把握するとともに、実施過程における人的・物的な整備を要する対策についても、優先度を勘案し計画的に実施していくことが必要である。

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、重大な情報セキュリティインシデントを招く恐れがあるものについては、対策基本計画の策定を待たず、可能なものから速やかに実施していく必要がある。

(1) 情報セキュリティ対策基本計画の策定（H28 年度内に実施）

① 各法人は情報セキュリティインシデントの発生状況や自組織を取り巻く昨今の脅威、取り扱う情報の機密性や重要性等を考慮して、自組織における情報セキュリティリスクを適切に評価する。

② 評価結果を踏まえ、情報セキュリティポリシーに基づき、対策基本計画を策定する。

③ 個別の情報セキュリティ対策に対する取組への方向付けを行うため、特筆すべき事項については、対策基本計画の「全体方針」として記載する。

④ 対策基本計画の「個別取組」の方針は「全体方針」に沿って、情報セキュリティに関する教育、情報セキュリティ対策の自己点検、監査、技術的な対策を推進するために必要な取組について記載する。

⑤ その際、情報セキュリティインシデントの発生を前提とし、外部ネットワークとの接続部分だけでなく内部ネットワークも含めた多重的な対策についても記載する。

⑥ 「個別取組」を計画的に実施するため、一連の取組実施予定時期が全体として把握できるよう工程をまとめる。

(2) 情報セキュリティインシデント対応体制及び手順書等の整備（H28 年 9 月末迄）

① 情報セキュリティインシデントが発生した場合のインシデント対応体制を明確にするとともに、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担当部門について手順書を作成し、関係者間で共有しておく。

② 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を事前に把握しておくこと。また、情報システムの停止やネットワーク遮断等の必要な手順書を作成し、関係者間で共有しておく。

③ 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更新を行う。
④ インシデント対応を行う職員を対象とした教育訓練を定期的に（少なくとも年１回以上）実施してインシデントへの対応力を高めておく。

(3) 情報セキュリティポリシーや関連規程の組織への浸透（速やかに実施）

① 情報セキュリティポリシーや関連規程は、最新のセキュリティ脅威や脆弱性の他、教育研究機関を取り巻く環境の変化等を意識して必要に応じた改訂を行う。
② 情報の格付けや取扱区分を明確に定義し、構成員誰もが必要な時に参照できるよう文書の存在場所を周知しておく。特に、個人情報や重要な情報等を扱う学務、診療、財務部門等では当該情報の取扱規則や手順書を策定しておく。

(4) 情報セキュリティ教育・訓練や啓発活動の実施（速やかに実施）

① 役職員（学長・理事、部局長等）、情報システム管理者、重要情報を取り扱う担当者に対して、その責任に応じた情報セキュリティ対策を理解し、役割に応じた責務が果たせるよう必要な情報セキュリティ教育や訓練を定期的に実施する。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。
② 情報セキュリティインシデント発生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定期的に実施する。
③ 非常勤職員や派遣職員、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「情報セキュリティ対策ガイドライン」のような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。

(5) 情報セキュリティ対策に係る自己点検・監査の実施（H28 年度から実施）

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行う。
② 当該年度で実施した自己点検の結果を踏まえ、必要な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 中立性を有する第三者による情報セキュリティ監査を実施し、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。

(6) 情報機器の管理状況の把握及び必要な措置の実施（H28 年度から実施）

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。

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 個人情報など重要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重要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こと。
④ 今後の利用予定が無い不必要なグローバルＩＰアドレスは、プライベートＩＰアドレスへの移行を検討するとともに、日本ネットワークインフォメーションセンター（ＪＰＮＩＣ）へ返却するなど所有しないという選択肢も検討する。
⑤ 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こと。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。
⑥ パスワードの設定時は、強度の高いパスワード（例：英数大小特殊文字を含む８文字以上）とし、組織変更やインシデント発生の恐れがあるなどの場合に必要に応じて適宜変更を行うとともに、他との使いまわしをさせないなど第三者による不正利用を防止する。

※ 上記に記載する取組の検討にあたっては、国立大学法人等の実情に沿った標準的なポリシーや手順書等の雛形として策定された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（ＮＩＩ）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（2015 年版補訂）」も適宜参照することが望ましい。

以上

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

参考資料

背景

1. **基本的な情報セキュリティ対策の未実施や意識の欠如**に起因する不正アクセスやWebサイトの改ざん、情報漏えいなどの情報セキュリティインシデントが多発。
2. 法人の**信用失墜や業務遂行に重大な影響**を及ぼすなど、法人の運営に支障をきたす。
3. 今日、情報セキュリティ対策の強化は社会的に**経営上の重要な課題**。

新たな取組が必要

国立大学法人等

基本的な考え方

○最高情報セキュリティ責任者（CISO）は**情報セキュリティリスクを適切に評価**、**中長期的な視点**により情報セキュリティ対策 基本計画を策定し、**法人全体として組織的・計画的に実施。**

○情報セキュリティリスクの低減に向けて積極的に取り組むとともに、企画・法務・広報などの担当理事と連携した対応**体制の構築**と訓練による対処能力の向上を図ることが必要。

○PDCAサイクルの運用によって、定期的な情報セキュリティ対策の改善を実施。

実施する対策

1. 情報セキュリティ対策基本計画の策定**（平成28年度内）**
   ◆中長期的な視点を含めた法人全体の計画
2. 情報セキュリティインシデント対応体制及び手順書等の整備**（平成28年9月末迄）**
   ◆体制や手順書等の整備及び定期的な訓練の実施
3. 情報セキュリティポリシーや関連規程の組織への浸透**（速やかに）**
   ◆適宜改訂するとともに構成員に対する周知徹底
4. 情報セキュリティ教育・訓練や啓発活動の実施**（速やかに）**
   ◆構成員に対する定期的な実施及び学生等に対する周知徹底
5. 情報セキュリティ対策に係る自己点検・監査の実施**（平成28年度から）**
   ◆改善策を情報セキュリティ対策基本計画に反映し、継続的なフォローアップを実施
6. 情報機器の管理状況の把握及び必要な措置の実施**（平成28年度から）**
   ◆グローバルIPアドレスを付与する情報機器やソフトウェアにおける適切な管理・運用