D3303 役職員向け説明資料作成ガイドライン

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10月31日  A3303 | 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 |
| 2015年10月9日  C3303 | 高等教育機関の実態に合わせた内容の見直し | 曽根秀昭（東北大学）  高倉弘喜（国立情報学研究所） |
| 2021年3月25日  D3303 | 「役職者向け説明資料作成ガイドライン」として内容の見直しを実施 | 曽根秀昭（東北大学）  高倉弘喜（国立情報学研究所） |

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。

　本書は、役職者（学長、事務局長、部局長（部局総括責任者））を対象とした大学運営における情報セキュリティ対策の基本的知識を説明する項目を示すものである。

解説：対象は、大学執行部、経営陣。情報セキュリティの常識と事例を中心に、教育する。情報セキュリティのためのコスト（人、予算）の必要性を説明する。情報セキュリティ対策はコストがかかるものであり効果が直ちに見えないこともあるので、予防的な対処は理解が得られにくいことがある。しかし、セキュリティ対策をあらかじめ施さないままにインシデント被害が発生すると、原因の特定や対処が困難になり、その困難な対応を直ちに短期間で実施することを迫られて、結果的に割高なコストがかかりがちで非効率的である。また、大学の評価が低下することに起因する副次的な被害につながることもあるので、「保険」のような必要コストであるという理解もありうる。

**１. 本学における情報セキュリティ状況**

役職者に対して、本学における情報セキュリティ対策の状況とインシデント発生状況等について、最低年1回、及び必要なときに以下の項目例について資料とともに報告する。

・本学のネットワーク・情報基盤について最近の状況（新しいサービス、運用・利用形態）

・本学の情報セキュリティ体制（ルール，チーム）

・インシデント発生状況の詳細情報（扱い件数の統計）＋対応状況（緊急措置，報道対応）

・重大インシデント（学外に対して重大な被害を与え、あるいは報道・苦情など問題化したもの）の詳細な分析

・本学外におけるインシデント発生状況の情報

**2. 情報セキュリティ対策に必要な措置**

2.1　情報セキュリティ対策の必要性

・普段から情報セキュリティ対策を十分にしておかないと、インシデント発生時に業務遂行に支障が生じ、また対応にコストがかかって、労力と費用が失われる。情報セキュリティ対策にも労力と費用を要するので、合理的な労力および費用について考察して実施する。

・情報セキュリティは、大学の存亡にかかわりかねない重大な問題である。情報セキュリティ対策を怠ったがために、重大インシデントが起こった場合の影響を考えてみる。この場合、直接的に業務遂行に支障が生じるだけでなく、大学の評価が低下する。例えば、研究データの管理能力や研究成果の正当性が疑われるために、研究活動に困難が生じるとともに、共同研究が拒否される。さらに、社会的評価の低下は、受験生の減少にもつながる。共同研究先や受験生が減少する結果、大学経営が厳しくなって情報セキュリティ対策の実施が困難になり、さらに重大インシデントを呼び込むことになる。その結果、大学経営に非常に重大な影響を及ぼしかねない。

・情報ネットワークや情報システムあるいは情報の取り扱いについて，全学的な運営計画のなかでこれらの計画や運用に関わる責任をもつのが「CIO」の役割とされている。このサンプル規程集では，「D1001 情報システム運用基本規程」第四条で定める全学総括責任者が相当する。

・大学における情報セキュリティ対策の中でも、特に事務情報と医療情報については、特別な配慮を要する。事務情報には、学籍や職員に関する個人情報、財務情報、調達情報などがあり、適切な格付けに基づいた取り扱いを要する。教員が扱う同種の情報についても同様である。また、医学部を有しない本学においても、学生の保健管理、あるいは人に係わる研究において医療情報をもつことがありうる。

・研究の成果は、やがて公表するものであっても、研究成果発表のプライオリティ維持のため、あるいは特許取得のため、情報管理が必要とされる。学生が実験で得た結果もその対象に含まれる。企業等との共同研究であれば、さらに厳密な管理が求められる。安全保障貿易管理の対象となる研究情報については、定められた手続きに従い管理することが求められる。また、研究公正の担保には所定の期間にわたって確実な保存が必要である。

・情報システムには，ハードウェアの耐用年数だけではなく，ソフトウェアにも機能とセキュリティレベル維持の耐用年数がある。このことを意識して，情報システムの構築と運用の計画には，運用期間中のセキュリティレベル維持のためのシステム保守（最新のセキュリティリスクを反映した設定見直し、セキュリティアップデート等）計画と期間終了を見据えた次期更新計画も意識する必要がある。サーバに限らず、パソコンやモバイル端末についても同様である。

・学内の情報サービス機能を，学外の商用サービス（クラウドサービス）を利用することで実現する方法があり，コスト削減や可用性向上のメリットも期待できる。これらを選定する際に，通常時の運用管理から運用事故発生時の対応までのセキュリティ対策も含めて検討すべきである。なお，外国のサービスについては，適用法を確認し，また，サービスの処理や保存の対象となる情報に機密情報や輸出管理技術などが含まれないかも確かめて判断する。

2.2　情報セキュリティの責任体制

・情報セキュリティ対策の有効化のために、情報システム運用管理体制を整備することが必要である。これには，人員と予算の確保及び規程類の制定が含まれる。

・「D2101 情報セキュリティ対策基準」に基づき、情報セキュリティ対策の最終責任は全学総括責任者にある。

・情報セキュリティ対策のために、通常業務として情報メディアセンター（管理運営部局）が整備、運用、監視を行う。

・現場である部局で対応に当たる部局統括責任者，部局実施責任者及び技術担当者から，情報メディアセンター及び全学総括責任者へ，及び逆方向の連絡体制の構築と役割分担をあらかじめ定めておく。担当者・連絡先の点検を兼ねて、定期的に情報を流すなどの活用を行なうことが望ましい。

・インシデント発生時の判断と対応は、「本学インシデント対応手順」に従い、本学CSIRT及び関係部署が担当し、法務と技術の両面から遺漏のなく行うことが必要である。広報も重要である。必要に応じて情報セキュリティ分野の法務について実務経験のある弁護士等の助言を得ることが望ましい。

・学外のクラウドサービスを利用する場合，あるいは運用やサービスを委託する場合には，情報セキュリティ体制の中でサービス提供業者などの責任範囲も明確にしておく。

・停電（計画と事故を含む）や大規模自然災害のときに情報システムが停止すると，大学の業務，とくに緊急業務の遂行に支障を及ぼすことが懸念される。情報システムの可用性を保障するために，非常時に情報システムを運用するための計画（情報システムBCP）をあらかじめ定めておくことが必要である。これには，非常時の業務継続に必要とされるシステムの選別（学外への配置を含む）や，運用に関係する職員の体制と連絡網の用意などが含まれる。

**3. 情報システムの構築・運用・インシデント対応**

3.1　体制の整備に関する課題

・情報セキュリティは情報システムの運用と利用のための安全保障である。  
情報システムの構築時から、しっかり設備と体制をつくることが、情報セキュリティ対策の予防とインシデント発生時の対応に必要である。情報セキュリティ対策は、投資（労力と費用）効率を考慮すべきである。  
情報セキュリティ規程を制定しても、実効的な設備および体制を構築しなければ、情報セキュリティ対策にならない。情報セキュリティ規程を制定しても現実的な要員と費用の確保が不足して実施することができない場合、情報セキュリティ管理の責任が問われる。

・情報セキュリティのため、通常運用の体制とインシデント対応のための体制の二つを整備することが必要である。  
通常業務体制のために、情報メディアセンター（管理運営部局）の情報セキュリティ体制を整備する。すなわち、体制構築のための人員および必要な予算を確保する。  
インシデント対応の体制のために、インシデント対応手順に合わせて、CSIRTおよび学内の法務と技術、広報等に関係する部署により体制を整備する。必要に応じて専門の弁護士等と契約する。

・通常業務の中で，インシデントの予防に有益な情報セキュリティ関連情報の収集と，学内への注意喚起にあたる業務も考慮すべきである。

・学外のクラウドサービスの利用や学外への運用委託をする際には，サービス提供業者との連絡体制について，故障など事故発生時の情報消失や運用中断に備えて，用意しておく。

3.2　体制の整備の方法

・情報セキュリティの体制を整える際に、重要な決定がかかわる業務は本学職員が担当し、その他の要員は学外への業務委託や派遣などのアウトソーシングも選択肢になりうる。情報セキュリティ対策のための設備、あるいはその運用と監視もアウトソーシングの対象になる。インシデント対応のアウトソーシングについては、大学運営を勘案した判断を要する面に十分に考慮すべきである。アウトソーシングには、臨機応変に最適化できることや長期的人件費を削減できるメリットがあるが、継続的な取り組みも含めて、費用対効果を十分に検討して判断する。

・情報セキュリティ対策ソフトを部局ごと、あるいはPC一台ごとに導入したりしているようなケースも考えられる。しかし、一般的に全学ライセンスのような形態をとるほうが対策を徹底しやすく、費用対効果が良くなると期待できるので、全学的な取り組みに改めることが望ましい。教育の効果や実施の徹底のためにも、全学レベルで取り組む姿勢を示すことは有意義である。

・情報セキュリティ対策に関連する情報を学内に周知する際に，注意喚起のための関係者への情報提供という直接的な効果のほかに，関係者を含めて情報セキュリティ体制と担当を再確認する効果も考慮して，定期的に周知を発することが望ましい。

**4. ケーススタディ**

解説：以下はあくまでも例なので、最新の事例を収集する。

4.1　不正侵入の事例

　不正侵入の事件が発生した結果、外部から苦情が届き、不正侵入されたサーバの修復に加えて広報などの対応も必要になって、大きな労力を費やし、大学の社会的評判を落とすことになった例がある。被害者から損害賠償を請求された例もある。

　・ウェブサーバが不正侵入されて、ウェブページを改ざんされた大学の例。

　・不正侵入された結果、踏み台となって、スパムサーバや不正アクセスに利用された例。同様に、フィッシングサイトを置かれた例。インターネットの掲示板に不適切な発言を書き込むアクセスの踏み台として悪用された例。

4.2　情報漏えいの事例

　大学がもつ情報が漏えいした場合、社会的信頼を損なうほか、個人情報である場合などに損害賠償責任が生じる例がある。

・学生の成績情報が漏えいした大学の例。

・職員が使用するパソコンがウイルス（暴露ウイルスと呼ばれる種類）に感染し、取扱注意の情報が漏えいした大学や官公庁の例。

・クラウドサービスを不正アクセスされて情報を持ち出されたのに検知できなかった大学の例。

・海外出張中に持ち歩いていたパソコンを食事中のレストランで盗難にあい、研究情報や個人情報が失われた大学教員の例。

4.3　ID・パスワードの漏えいの事例

・学内情報サービス（あるいは、宅配サービスや通販サービス、銀行など）を装った偽のウェブサイトに誘導する攻撃（フィッシング）にあってIDとパスワードを入力したために，その情報が流出した例。さらに，そのIDとパスワードを用いてメールサーバを含むクラウドサービスを悪用されて大量の迷惑メールを発信され、または情報流出を起こした例。

・学内外の情報サービスで認証連携しているIDとパスワードの認証データベースを持つ認証サーバに脆弱性を放置していたために不正アクセスを受け、認証情報を流出させたために、自組織のIDをすべて無効にせざるを得なくなり、すべての業務が停止した大学の例。

・学外の情報サービスで、学内のメールアドレスをIDとし、これと同じパスワードを用いていたために、その情報が流出し、学内情報サービスの悪用を許してしまった例。

4.4　情報システム管理の体制ができてない事例

　情報システムや情報セキュリティの体制が整備されていない場合に、業務に多大な支障が生じた例がある。

・大学院生が主体になって仕様書を作成し、システムを構築した。その後、リプレースのとき、その大学院生は卒業したため誰も仕様書を書けなかった大学の例。

・ネットワーク担当の教授が主体となってシステムを構築した後に定年退職となり、システムを理解する人が学内に皆無になったという大学の例。

・ネットワーク運用を学生（あるいは非常勤教員）に依存していたところ、その人が卒業（任期切れ）になった後、誰もネットワーク管理ができなくなり、安定運用ができず業務に支障をきたしたという大学の例。

・教員が開発したシステムを利用していたが、システム管理や保守の計画がなかったために業務に支障が生じたシステムの例。

・システムの導入の際に，設置業者の作業（ネットワーク接続，システム設定）を把握しなかったために不適切な設置・運用になって，インシデントが発生した例。

・コンピュータにインストールするソフトウェアの管理が不十分だったために，悪意のあるソフトウェアを意図に反してインストールしてしまい，情報流出インシデントが発生した事例。

・コンピュータにインストールするソフトウェアの管理が不十分だったために，許されるライセンス数を超えてインストールしてライセンス違反が生じた事例。

・実験装置の制御用に組み込まれたコンピュータやこれにインストールされたソフトウェアが耐用年数を過ぎても，専用システムの都合のために更新できない例。

・電気製品がインターネット接続機能をもっているにも関わらず，表面上は情報システムであると意識しにくいため，その機能の情報セキュリティ対策が不十分であることを把握できないまま接続して使用していたためにインシデントが発生した例。

・時限プロジェクトで使用していた専用の汎用ドメイン名（www.example.jpのような形式）が，プロジェクトが終了してドメイン名の有効期間が過ぎた後に他者に取得されて悪用されていた事例。

4.5　インシデント対応の体制ができてない事例

・インシデントが発生した部局の担当者が取材に対して，全学の体制と協調することなく応じて，不用意な発言が報道されてしまった例。

・インシデントに関する取材に対して，体制に従わず広報から部局に丸投げとなった結果、不適切な対応となってしまった例。

・インシデント発生後の役割分担が機能せず、技術担当者など特定の者に所掌範囲外の作業までもが集中した結果、インシデント対応が後手に回り被害が拡大してしまった例。

・インシデント対応が長期化（1年前後以上）して、調査の必要が生じても対応できず、調査体制を維持できなかった例。

4.6　ソフトウェアの耐用期限を意識していない事例

　ソフトウェアの耐用期限が過ぎても、それを使い続けていて，次のシステムへの移行していないため、業務の継続に支障を生じる例がある。

・Windows XPは実験装置等で大量に使用されており、そのサポートの年限は数回延長されたにも関わらず、リプレースが困難だったため、サポート終了後にソフトウェアのセキュリティ維持ができなくなったにも関わらず、インターネットに接続してデータ転送したときにシステム侵入を受けたという，2019年の例。

・ソフトウェアのサポート期間は、OEM版など種別により異なることを把握しておらず、サポート終了に気付かないまま使用し続けていた例。

・ソフトウェアはセキュリティ更新が提供されなくなった時点で耐用期間が過ぎたと考えるべきであるのに，更新されなくなったフリーソフトウェアの安全性確認を失念し、使用し続けていた例。

・ソフトウェアが最新のハードウェアに対応できず、システム全てのリプレースが必要となった例。

4.7　著作権侵害の事例

・学生がインターネットに公開されたファイル交換システム上で長期間にわたって商用ソフトウェア（あるいは、音楽や映画）を配布した結果、多額の損害賠償が問題になったという例。

・教員がBGM（商業作品）を用いてオンライン講義を行っていたので動画配信から削除されたという例。

・商用ソフトウェアについて、許諾されるライセンスを大幅に超えて利用し続けた結果、損害賠償を支払った大学の例。

4.8　その他の事例

・学生が学内からインターネットの掲示板に名誉毀損を疑われる発言を書き込んだ結果、訴えられた例。同様に、インターネットオークションに海賊版ソフトウェアを出品した例。