大学における情報リスクの分析と業務継続の条件とは？
ー情報漏えい事故対応と個人情報保護法、地域大学連携の基礎知識ー

江戸川大学名誉教授　　市川昌

（ねらい）
非常時における情報セキュリティ対応のために情報リスクの分析が必要です。サイバー攻撃や標的型攻撃を含む情報危機が高まるなかで、日常的にも大学内で起こりがちな情報流失漏えい事故（incident）のリスク対応は難しく王道を模索するより日頃の努力が大切です。情報資産漏えいで大学という教育研究の場で、注意したいのは情報リスクの危機意識の共有と組織的対応です。日常の業務過程のなかでこれだけは注意しておいた方が安全だといういくつかの法的および技術的ポイントはあります。この講習ではどこでも起こりやすいインシデントを想定して、大学におけるICTの効果的活用のために非常事態も予測しながら、情報リスクの分析、法的対応、地域大学連携について学ぶ機会としたいと思います。

（情報漏えいの事故発生をなくすために日常的な対応手順と法的知識が課題）

1、なぜ情報資産流失・個人情報保護法違反者がなくならないのか？

ＳＥＣＯＭは、情報漏えいの８０％は内部による人的盗難、不正アクセスとします。情報流失による内部秘密漏えい・著作権、個人情報保護法などの法令違反事故などのおそろしい結果イメージを明確に周知教育する必要性があります。
なぜ情報管理規則、内部規定を組織化し、周知化しても、常に情報漏えいおよび流失事故がなくならないかの原因を考えるとき、罰則強化、責任体制強化を重視するひとがいますが、それは必要条件ですが、十分条件ではありません。なぜならば最近のケースでは情報に無知なひとよりも、熟練した技能者、責任者のミス判断から事故が発生することが少なくないからです。情報をより良く役立てるためにこそ、日常的な相互管理体制を見直して、無用なトラブルを亡くしましょう。

多くの事故発生は情報への無知、不慣れからでなく、自校だけは大丈夫という情報優良校といわれているところでも、慣れからくる「こころの油断」に原因があります。
ＪＮＳＡ２０１２年「企業等情報セキュリティ・インシデント２３５７件の調査報告」
個人情報漏えい人数　９７２万６５人　インシデント原因リスク分析

「内訳」内部管理ミスによるもの	１３９１件	５９．０％
情報機器の誤システム操作	４７４件	２０．１％
紛失置き忘れ	１８９件	８．０％
外部侵入盗難	８８件	３．７％
不正情報持ち出し	６０件	１．５％
目的外使用	１１件	０．５％
バグ・セキュリテイホール	２８件	１．２％
ワーム・ウイルス	９件	０．４％（日本情報セキュリティ協会資料）

そのためにインシデント対応のパターン化と徹底とともに、事故が引き起こす被害ケースがどれだけ大きな問題となるか。特に「情報流失は物品盗難よりも被害拡大」となる恐ろしさについて組織員全体が認識を改める必要があります。特に情報流失阻止のため法的コンプライアンスを守り事故を生みやすい土壌を再点検しましょう。

２．情報セキュリティシステムの確立は基礎的な業務の確認と個人情報の保護

大学内の事故原因を調べると、教職員によるＵＳＢメモリーなど媒体紛失、フィッシング、複合機器のシステムエラー、ＩＤ盗難によるなりすまし、研究室ＰＣ盗難など日常的な業務におけるエラーが多く、管理責任の欠如が課題とされています。

第１段階　情報流失・法的違反をどのように初期対応し報告するか。

(1)　流失・違反の初期対応は早いほど良い。－何が、どこで、いつ、誰が、影響はどこまで？関連部署は？連絡体制は？などシステム的対応を考えましょう。
(2)　情報事故の連絡体制の確認。日常的な緊急連絡体制、情報の一元化と守秘義務の確認、リスク対応の意志決定順序などができていますか？

第２段階　流失・紛失・違法コピーなどの情報の調査と回復の方法

(1)　初動調査に必要な対応項目のチェック（デジタルかアナログか、人間系か）
(2)　対応の追跡と検証（連絡済みの確認、情報内容の確認、回収回復のチェック）
(3)　外部・マスコミ・地域などへの対応の一元化（部内外の広報システム）

第３段階　今後の情報事故を防ぐための情報管理システム

(1)　調査結果としての原因、対応などの記録の保存方法をチェクしましょう。
(2)　管理組織、職員規則、業務手順、機器管理、外部契約を見直しましょう。
(3)　教職員、管理者、従業員などへのPRやFD研修を続けましょう。

３．情報流失漏えいのこわさは「個人情報保護法による訴訟」

成立経緯は、１９８０年プライバシーの保護と個人データの国際流通についてのＯＥＤＣ勧告が国際化の条件となり、２００３年５月２３日個人情報保護法成立、２００５年４月１日全面施行となった。

個人情報保護法は、情報事故が起こった場合、当該組織の内部の組織防衛では逃げ切れず、外部社会から法令違反の明確なケースと触法事例が糾弾されるので、管理者は法律の意義と考え方を社会常識として知っている必要がある。個人情報のインシデントは、被害者が当事者である企業、大学・学校などの団体を訴えると賠償金などの巨大リスクを負う。法的には刑事罰では６か月以下の懲役または３０万円以下の罰金。民事訴訟の判例は１人あたり数千円―数万円、対象者数が大きいと企業・団体は倒産するおそれもある。最近教育産業ベネッセ・コーポレーションが児童生徒の顧客情報７６０万件、２０７０万件の情報流失が問題となり、システム開発の孫請け子会社の社員が逮捕されて管理責任が問われ、個人情報保護法の抜け穴が問題とされた。

（１）個人情報保護法とは

第1条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取り扱いに関し、基本理念および政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる条項を定め、

国および地方自治体の責務等を明らかにするとともに、
個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、
個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

（目的）個人情報の有用性の配慮と個人の権利利益の保護

――――――――――――

（２）個人情報、個人データ、保有個人データの差異に注意

第２条 「個人情報とは生存する個人に関する情報」であることに注意
当該する氏名、生年月日、その他の記述による個人の識別
（他の情報データベースと容易に照合可能で特定の個人を識別できる）

法施行令第2条　個人情報取扱事業者とは、個人情報データベースなどを事業の用に供しているもの（ただし国の機関、地方自治体、独立行政法人、地方独立行政法人、その他取り扱う個人情報の量および利用方法（取り扱う個人の数が5000を超えないものは除外）

5000件を超えなくても厚生労働省ガイドラインでは病院、診療所などリスクは大きい。
文部省ガイドラインは学校法人は大規模、小規模の差なく法的倫理を尊重する。

「個人データ」とは、個人情報取扱事業者が管理する個人情報データベース等を構成する個人情報をいう。（第２条の４）
「保有個人データ」とは、開示、内容の訂正、追加または削除、利用の停止、消去および第三者への提供の停止を、行うことのできる権限を有する個人データである。（個人情報管理者の特定と個人データの分離、暗号記録などが望ましい）

４．個人情報を取り扱う場合、利用目的を特定しなければならない。

学校における生徒等に関する適正な取り扱いに関する指針（文部科学省の指針）
「利用目的」を曖昧にせず、授業アンケートでも「卒業生の就職状況をパンフレットにするため」など具体的に特定して情報取得にあたることを要請。
第16条により、「本人の同意を得ずに利用目的の範囲を外れて、個人情報を扱ってならない」と明記。（利用目的同意書または一括承諾書などの重要性、文書の証拠）

最高裁判決「早稲田大学講演会参加者名簿提供事件」の判例

（大学は公的機関要請でも目的外利用の承認の時間のあるときは注意する必要性）

第１６条「あらかじめ許可をとった利用目的の範囲を超えて目的外利用は不可」
第１６条の除外事項
「法令に基く場合、人の生命、身体、財産の保護、公衆衛生（介護）の向上」
など制限事項についての枠が厳しく定められている。

――――――――――――――――――――――――

個人データ内容の正確性の確保と安全管理

第１９条　「個人データを正確かつ最新の内容に保つように努めなければならない」
正確化、最新化の要請は努力義務にとどまりまるが注意すべき。

第２０条　「個人データの漏えい、滅失、毀損の防止。安全管理の必要、適切な処置を講じなければならない」

（漏えいとは個人データが外部流失すること、滅失は失われること、毀損は内容の破壊、書き換え、変更などを含む。「講じなければならない」は、法的義務を意味する。
経済産業省ガイドラインでは、組織的安全管理、人的安全管理、物理的安全管理、技術的安全管理を含む総合的な安全管理体制を要請している。）

第２２条　「委託をした者に対する必要かつ適切な監督をしなければならない」業務アウトソーシングの場合も監督指導の責任があることを明記している。

（文部科学省の指針では「外部委託先選定基準を設けること。委託内容の明示。漏えい盗難の注意義務、再委託の場合は必ず文書報告、契約期間の明記、事故発生等の場合の報告義務、複写複製の絶対禁止等」を学校分野ガイドラインで指示している。）

最高裁判決「宇治市住民基本台帳外部委託業者による漏えい事件」の判例

（地方自治体など公的事業者は、外部委託業者への指導監督の責任を有する）

―――――――――――――――

◎　個人情報保護法第17条関連（適正な取得）

　第16条関連（利用目的による制限）

学生、父母などの保護者、地域住民などから情報を収集するときに、利用目的を明確にして適切な事前説明をしましたか。アンケート、個人データなどをとるときには、同意書または承諾書など記録をとっておくこと。

◎　個人情報保護法第20条（安全管理処置）

研究室、事務室などで情報の漏えい、紛失などがあったときに、適切な対応をとっていますか。特に教育研究の研究室、事務室での出入りの責任体制や機器管理のルートを明確に。インシデントが発生または発生のおそれのあるときは迅速に連絡しあうように努めましょう。

個人情報についてのアクセス権を設定し、アクセス制御に努め、業務委託に注意。
個人情報を管理している事務局、研究室など入退出、カギの管理、パソコンのアクセスについては慎重な対応をするように努めましょう。研究室での学生指導と情報管理マニュアル。特に契約業者との業務委託における責任体制、契約条件の損害補償、外部関係の管理。

◎　個人情報や個人情報データ、個人保有データなどを取得したとき説明した目的と違う機関に告知をする、または目的外利用といわれるような行為をしていませんか。事前に取得データが教育研究以外に利用することが予想されるときは対象者に必ず承認を得ること。また非承諾者のオプトアウトの人権を尊重し、必要な場合は契約条件を明記する。

◎ 開示、訂正、利用制限（第25条から第27条）
情報収集の際に情報取得（一括）承認書等の書面または口頭で目的を説明しましたか。
情報取得を拒否した方についてのオプトアウトなどの説明や対応をしましたか。
開示および訂正、削除、利用停止などについては、学内委員会または事務局で内規、または施行条件を明確にして、クライアントである学生、父母、教職員には誠実に対応し、本人確認の手続きをした後できるだけ速やかに判断、実施の可否を伝えるようにしましょう。

「刑法161条の2」は電磁的記録不正作出（コンピュータによる文書偽造）を禁じています。
「不正アクセス禁止法」ではアクセス制限のある情報に他人のID，パスワードを利用して侵入することを犯罪とし、1年以下の懲役、50万円以下の罰金を課します。
（2000年2月制定）
知的財産権侵害としては特許権、著作権、意匠権、商標権違反などで告訴できる。

５．アクション・プランのために

（１） 事業者の情報セキュリティ保護に対する法的対応、組織、責任体制を明確にして、大学等の教育機関としての誠意を示すことが大切です。

（２） 個人情報などの収集、利用、提供および管理についての規定を明示します。

（３） 個人情報、学内情報などに関する開示請求、訂正、削除または利用停止などの対応規定を明確にします。

（４） 情報セキュリティに関する教育研修、検討委員会設置などに努めます。

（５） 情報保護などに関する業務監査などのシステムをつくります。

（６） 組織全体のガバナンスとしての学長、担当理事、事務長、各学内の学部学科、研究機関、図書館、付属機関などの情報文書部門管理者の明確化。情報開示、情報訂正などの要請業務の取り扱いマニュアルを規定します。

（７） 災害など非常事態における地域連携、大学間連携など情報資産の総合管理。

６．大学および短期大学の２０１３年情報セキュリティ対策自己点検評価調査からーハードのセキュリティ管理からソフトの情報資産、研修、事故対応システムへ

私立大学情報教育協会がまとめた「情報セキュリティ対策の自己点検・評価状況調査（平成２５年度）によると、情報セキュリティの対策の自己評価に回答を寄せた加盟校２２１校（大学１６７校、短大５４校）の平均的傾向を概観すると、情報インフラ整備、個別大学の情報資産管理の重要性が理解されつつあるが、情報セキュリティＦＤ研修の不足、事故対応マニュアル不備、情報媒体管理の遅れなどいくつかの傾向が見えてきます。

（チェックリストによる５点満点で、実施しているが５点、一部対応４点、計画中３点、必要性は感じる１点、必要性を感じない０点で評価）

情報資産の重要度について適切な基準設定がされているか？	大学２．５	短大３．１
情報資産の種類に応じたアクセス権の設定がされているか？	大学４．１	短大４．１
情報資産の重要度に応じた取扱いの手順が定められているか？	大学２．９	短大３．１
情報資産のリスク評価基準が明確になっているか？	大学２．１	短大２．１
情報セキュリティにたいする専門組織が設定されているか？	大学３．７	短大３．５
組織単位でセキュリティに取り組む体制ができているか？	大学３．１	短大３．２
情報セキュリティ・ポリシーが公開、周知徹底されているか？	大学３．３	短大３．０
情報セキュリティ・ポリシー教育が適切に実施されているか？	大学２．７	短大２．７
事故対応体制、マニュアルが明確にされていますか？	大学２．９	短大３．１
ファイアーウオール、ログの定期的管理されていますか？	大学４．７	短大４．１
サーバーのアクセス把握とログの保存はされていますか？	大学４．４	短大４．３
情報媒体のＵＳＢメモリー、ディスクドライブの管理基準は？	大学３．２	短大３．２
情報媒体のパスワード対応、暗号化の紛失事故の対応は？	大学３．１	短大３．２

7. 地域の大学間連携共同教育推進事業などの日常的な地域連携の重要性。

災害などの非常事態の情報セキュリティ対応には日常的な地域の連携が重要である。

私立大学連盟では２０１３年（平成２５年３月）「大規模自然災害に対する私立大学間の協力・連携のあり方」で、理想として全国的な私立大学の相互支援ネットワークの構築をあげ、私立大学の法人の独立性、建学理念の差異、規模性格の差などを乗り越えて、できることから大学は業務継続計画をたてて協調することの必要性をあげている。

連携の課題としてあげているのは以下の６点である。

(1)大学の災害対策などノウハウの共有、
(2)危機管理体制の構築の重要性―情報資産で何をどう共有、分散させるか。
(3)このための大学間連携の可能性―緊急時の代替情報ネットワークは？
(4)情報資産の再生のための管理―ICTを活用した事業継続のための課題
(5)災害時の情報収集の共有
(6)地域社会への貢献と連携

(地域連携のための事例)
将来予測される南海大地震などの災害などの対策から小規模の地域連携へ

たとえば将来予想される南海地震、太平洋津波災害などの事故対応として九州、四国、中国地方の高知、徳島、岡山、九州、島根などの国立大学の相互支援協定、カウンターパート方式が注目される。京都５大学の龍谷大学、京都大学、同志社大学などの教学の大学間共同教育推進事業は、地域間の資格制度の平準化から始まり相互協力を模索している。淑徳、関西国際、北陸学院、くらしき作陽大学などの「主体的な学びの為の教学マネージメント協定」が進み、千葉県では江戸川、川村、中央学院、二松学舎、麗澤などの災害時などを含めた日常的な「図書館相互利用提携協定」の見直しなどは、どこの地域でも行われていることだが、できることから情報の共有を進めるという地域連携の第１歩となる。

地域の大学間連携としては千葉県柏市を中心に地域自治体と大学が協力して町づくりに参加する「大学コンソーシアム柏」は柏市周辺の１１大学、国立の東大、千葉

大などと私立の江戸川、淑徳、麗澤などが参加して、災害時を含めた教育研究の連携を進めるインフラ基盤整備として可能性のある事例である。
　また東京都三鷹市の杏林大学では地域の三鷹、八王子、羽村市と医学、看護、保健、総合政策などの学部が「地域交流の包括協定を結び、「都市型高齢社会の地域と大学」の相互協力のネットワークを進めている。

文部省の「大学間連携共同教育推進事業」の国公立大学と私立大学の連携

　被災地である福島県では文部省の「大学間連携共同教育推進事業」において、「ふくしまの未來を拓く強い人材づくり共同教育プログラム」として福島大学が中心になり、会津、福島県立医科、いわき明星、奥羽、郡山女子などの大学間連携による情報ネットワークを進めている。

　被災地をかかえる東日本の広域大学連携では山形大学を中心に会津、札幌、東北芸術工科、東日本国際、明海、日本女子、東京家政学院などの「東日本広域の大学間連携による教育の質保証、向上システムの構築プロジェクトが注目される。
また宇都宮大学を中心に国際医療福祉、自治医科などの大学群で「連携大学の特色を生かしたクラウドによる教養・専門教育」のプロジェクトの今後も期待される。

　内陸に位置する宇都宮大学では、海岸線に近い横浜国立大学と２大学による教育、研究、管理などすべての部門での災害時を含む日常的な業務の連携が、トップ・マネージメントで合意されて実施されている。

8. 情報セキュリティ・マネージメント・システム（ISMS）と7要素

　ＩＳＭＳに取り組む全体的な枠組みは、ＩＣＴの効果的活用のための情報セキュリティに対する基本方針及び目的に従い具体的なプロセス、手順を決めて、運用し、評価して、見直して継続的に業務を進めることである。この流れはＰｌａｎ　，Ｄｏ，Ｃｈｅｃｋ，Ｓｅｅ　ａｎｄ　ＡｃｔのＰＤＣＡサイクルという循環過程とされる。
　情報セキュリティについてＪＩＳ　Ｑ　２７００２：２００６では情報セキュリティの基本的な７原則を次のように定義している。
「情報の機密性（Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ）、完全性（Ｉｎｔｅｇｎｉｔｙ）および可用性（Ａｖａｉｌａｂｉｌｉｔｙ）を維持すること。さらに真正性（Ａｕｔｈｅｎｔｉｃｉｔｙ）、責任追跡性（Ａｃｃｏｕｔａｂｉｌｉｔｙ）、否認防止（Ｎｏｎ－ｒｅｐｕｔａｔｉｏｎ）および信頼性（Ｒｅｌｉａｂｉｌｉｔｙ）のような特質を維持することを付加したい」

参考書
五十嵐聡「情報セキュリティ初級認定試験公式テキスト2013」技術評論社
かんたん合格情報セキュリティスペシャリスト試験（インプレス）のセキュリティ対策
wikipedia［個人情報保護法、大学間連携共同教育推進事業、私立大学情報教育協会］
日本私立大学連盟「大規模自然災害に対する大学間の協力、連携のあり方について」
情報セキュリティ大学院大学「情報セキュリティ事故対応ガイドブック」
文部省「ICTを効果的に活用した「新しい学び」学びのイノベーション事業実証研究報告
私立大学情報教育協会「未来を拓く大学教育のイノベーションを考える・教育改革FD／ICT理事長・学長等会議開催報告」（大学教育と情報）2013年度NO．４