学校情報の管理について

室　岡　和　彦

１．はじめに

ＩＴ化の進展に伴ない、学校が扱う情報は紙媒体の公文書類だけではなく、ウェブページ(ホームページを含む)のコンテンツや、ワープロソフトで作られた入試問題など、電子情報の機能と不可分の関係をもつようになってきた。特に、個人情報の不正な収集や個人情報の漏洩などが社会問題することを受けて、学校における個人情報や著作権の扱いは、学校運営と生徒の教育の２つの側面で大きく変わりつつある。学校情報に係わる問題の所在と解決について、実質的に情報専門委員会を運営してきた立場から、情報セキュリティと個人情報に絞って考察し、今後の学校情報の管理運営について方向性を示す。

２．これまでの経緯

附属高校が情報について関わってきた課題は、情報の漏洩等のセキュリティー、インターネットのホームページウェブ上に載せられた情報の扱い、個人情報の３つである。いずれも、ＩＴ化社会や情報の電子化と深く関わり、新しい形の問題として登場してきた。情報に関わる危機管理については、今後さらに重大な意味をもつことが予想される[1)]。以下、これら３つの問題について経緯を述べる。なお、これらの問題は形を変えて生じる可能性が高く、今後とも問題点を注意深く見守り柔軟に対応していく必要があると考える。

(1)　情報セキュリティ

お茶の水女子大学附属学校部では、平成15年度から情報専門委員会を設けて情報機器の設置や情報の管理を行ってきた。大学では、平成16年、大学事務局の情報機器等の盗難事件を契機に、情報セキュリティ対策強化の必要性が認識された。具体的には、情報セキュリティポリシーの作成、扱う情報を機密性と可用性の２面からの構造化、管理組織の明文化を行うことによって管理体制が整えられた。附属学校園でも、生徒の情報を実際に扱う際に漏洩等に対するセキュリティが確保されるとともに、情報の扱いについて不便さを感じないような管理体制、機動性のある管理組織の体制作りが課題になった。この課題は、高校及び附属学校園でも同じであり、大学の管理体制に基づいて具体化する必要が生じてきた。

平成15年度は、こうした状況のもとで、大学が作成した情報セキュリティポリシーの趣旨を受けて、学校情報を機密性と可用性の２面から構造化し、適正な管理運営についての指針「附属学校園セキュ

リティポリシー」を作成して学校情報の管理を組織し、情報の漏洩や盗難などの危機に対応できる体制を整えた。ただし、教職員や児童・生徒が情報を扱うときの注意事項をまとめることまではなされなかった。

情報セキュリティは、情報公開と密接に関わる。特に入試情報の公開と開示について基準を定める必要が生じてきた。平成17年度は、情報専門委員会と入学進学専門委員会で、入学検定について、募集要項の内容を公開する日時とその内容、募集・応募・受検人数等を公開情報とすること、情報の公開方法について検討する一方で、受検からの情報開示請求があった場合に開示する情報についても検討した。また、入試問題の公開については、これまでは予備校から請求があった場合、郵送費だけで無条件に渡したり、窓口の訪問者に記名させて渡していたが、２次利用等が考えられることから著作権者と連絡をとった上で入試問題を利用することを義務付けることになった。

(2) ウェブページの管理

情報公開法に基いて、大学が発信する情報の公開を推進するよう文部科学省から各大学に要請がなされた。一方、本大学では、ある研究室が張ったウェブページの内容が体外的に問題となった。こうした背景があって、大学では平成16年にウェブページ運用指針を作成し、各学部や附属学校部でもウェブページの管理体制を明確にすることとなった。各附属学校園が開設しているウェブページにおいても、公開する情報や肖像権に係わる制限などについて基準を明確にする必要が生じてきた。

特に、入学検定については、募集要項の内容を公開する日時とその内容、募集・応募・受検人数などの情報など、入試に関わる情報をウェブページで公開する際、どの情報を公開し、どの情報を請求があった場合に開示するかを各附属校園で共通した基準にしておく必要が生じてきた。また、ウェブページに関わり、例えば公開した情報を悪用した場合の対処など、ウェブページに記載した情報について生じた危機への対応を共同して行う必要が増してきた。

こうした課題を解決するために、情報専門委員会を中心になって、各附属学校園のウェブページに共通して記載するコンテンツやその更新、危機管理について検討し、大学が作成したウェブページ運用指針を踏まえた形で附属学校園におけるウェブページ運営規則を作成した。

(3) 個人情報

平成17年４月に個人情報保護法が施行された。また、私立学校向けに「個人情報に関する運用指針」が文部科学省から通知された。附属高校においても、生徒から情報を収集し、保有、修正、廃棄等をする際、また例外条項を適用する際には、一定のルールに沿って行う必要が生じてきた。この個人情報保護法のもとでは、生徒が事故に巻き込まれたりした場合にその生徒の氏名や電話番号などの個人情報を警察や病院などに知らせることができないなどの不都合が生じてきた。

平成17年度は、個人情報によって年度頭書に生徒から集める情報とその利用目的を明確にする必要

が生じてきた。

大学では、平成17年３月に、(国)お茶の水女子大学個人情報の管理に関する規則、(国)お茶の水女子大学個人情報公開取扱要項、(国)お茶の水女子大学個人情報の開示・訂正・利用停止審査基準を作成し、個人情報の収集・保存・修正・廃棄、危機対応等に対処する基準を設けた。

情報専門委員会では、これらの規則、要項、基準に基づいて、個人情報を管理・運用するときの指針、個人情報に関わる情報の公開や情報開示について検討した。また、附属中学校及び附属高等学校が行う入学検定試験問題は個人情報と直接的な関わりはないが、著作権や個人情報を学校情報の立場から検討した。

また、附属学校園における個人情報の収集、体系化、保存、ＰＴＡ等への流用、廃棄など「個人情報の運用」、さらに個人情報の管理体制を附属学校部として明確にする必要も出てきた。

個人情報保護法が施行された平成17年度の当初は、ともすれば神経過敏になる傾向が見られた。学校における生徒や教職員の個人情報は、一般企業の場合と異なり、個人情報で企業が利益を上げたり、個人に利益を与えたりするものではなく、教育活動のために学校と個人がお互いに利用しあうものであることから、学校の実態に即し、使いやすさや使える範囲を狭めない等の立場からの見直しが必要になっている。

３．情報セキュリティの考え方

情報セキュリティへの対応は、単に情報の安全管理だけではなく、情報発信や情報漏洩の危険性に対する対策も必要となる。情報セキュリティとは、学校などの組織で保有しているファイルやデータベースといったデータ、ＣＤ－ＲＯＭやフロッピーディスクなどのメディア、そして紙の資料などの情報資産を、職員が引き起こす失敗や外部の要因によって引き起こされる脅威から守ることである。情報セキュリティを内外の脅威から守るために、情報の機密性や完全性、可用性を維持していくために規定した組織の方針や行動指針を情報セキュリティポリシーという。情報セキュリティポリシーを教職員組織にきちんと認識させることは、学校の情報資産を情報セキュリティ脅威から守るだけでなく、その導入や運用を通して教職員の情報セキュリティに対する意識の向上や、生徒・保護者に対する信頼性の向上といった副次的なメリットも得られる。

なお、危機に対する認識が欠けていると、危機に対して全く無防備だったり、逆に過剰に防備することがある。また、危機が起こったとき、それが貴重な体験であることを認識せず、後代に残すことをしないで終わってしまう可能性がある。安全性（危機）に対して正しい見方、適切な対処、有効な活用が、情報セキュリティの基本的な考え方である。

(1)　情報とその管理方式

各校園が管理する情報は、ふつう、下記のような機密性、完全性及び可用性という視点から、「ウイ

ルスからの防御」、「ユーザー権限とユーザー認証の管理」、「パスワード管理の推奨」、「バックアップの推奨」などについて管理する[2)]。

① **機密性**：情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。国際標準化機構（ＩＳＯ）が定める標準に定義されるもので、Confidentialityの訳語。

② **完全性**：情報及び処理方法の正確さおよび完全である状態を安全防護すること。国際標準化機構（ＩＳＯ）が定める標準に定義されるもので、Integrityの訳語。

③ **可用性**：認可された利用者が、必要なときに情報にアクセスできることを確実にすること。国際標準化機構（ＩＳＯ）が定める標準に定義されるもので、Availabilityの訳語。

附属学校園の情報は、大学の情報セキュリティポリシーに基づいて、機密性、可用性の２つの観点から高・中・低の３段階に類型化し、それぞれの規準に従って管理する。

(a) 機 密 性

・**高**：非公開情報であり、それを金庫等に保管し、各校園の情報管理責任者あるいは情報管理責任者に許可された者のみ閲覧することができる。

・**中**：限定公開情報であり、各校園の教職員のみ閲覧することができる。

・**低**：公開情報であり、特定のコンピュータを用いて不特定多数が閲覧することができる。

(b) 可 用 性

・**高**：各校園の教職員が自由に書き換え可能な情報である。電子ファイルは、共有可能な情報として各校園の情報専門委員が管理する。

・**中**：電子ファイルのデータとして内部の者のみが閲覧可能な情報であり、各校園の情報管理責任者が管理する。

・**低**：書き換えができない情報である。利用する場合は、各校園の情報管理責任者の許可が必要である。

◎は電子媒体、○は紙媒体の例

	可用性　　低	可用性　　中	可用性　　高
機密性 高	情報管理責任者の許可が必要、紙面でのみ閲覧可能 ◎入試情報 ○児童・生徒の個人情報	情報管理責任者の許可が必要、指定のスタンドアロンＰＣでのみ閲覧可能 ◎児童・生徒・教員名簿 ○学校日誌	管理責任者の許可が必要、ＰＤＦファイルとして借用可 ◎○とも存在しない。
中	当該校園教員のみ、ＰＤＦファイルとしての記憶媒体で閲覧可能 ◎卒業者名簿、物品供用簿 ○通学証明書発行台帳	当該校園教員のみ閲覧可、電子ファイルとして記憶媒体で共有可 ◎入学検定問題と成績 ○募集要項、予決算表	当該校園教員のみ閲覧可、パスワード保護ネットで電子ファイルとして共有可 ○出席簿
低	お茶大関係者のみ、指定のスタンドアロンＰＣで閲覧可能 ○入学式次第	お茶大関係者は閲覧可パスワード保護ネットで閲覧可能 ○学校要覧	お茶大関係者は閲覧可、電子ファイルとして共有可能 ○成績証明書申込書

(2)　危機対応と評価

学校には、情報だけでなく、生徒の人身事故や教職員の引き起こす事故がある。そうした中で特に大きなものを危機と考える。万全な安全性確保のためには、問題が起こったときにその重大性のレベルを認識している必要がある。一般に、問題の重大性には次のようなレベルが考えられ、レベル４が危機としてよいであろう。

レベル１：許容可能（放置してよい）

レベル２：許容可能だが要検討

レベル３：望ましくない、対応が必要

レベル４（危機）：許容できない、緊急対応が必要

また、情報に関連した危機には次のような分類がなされている例がある[1)]。

・不正な情報：スパムメール、チェーンメール、覚せい剤などの情報

・法律違反：著作権法、プライバシー保護法（肖像権を含む）、セクハラなどの違反

・事故：天災や人災による機械の故障、停電、ケーブル切断

・情報の漏洩：個人情報の漏洩

・セキュリティ：不正侵入、ウィルス、担当者による持ち出し

こうした危機への対応には、ふつう次の４段階の対応が考えられる。それは城を守るときの考え方に似ており、情報管理についてもこの考え方を適用するとうまくいくと考えている。なお、この考え方は、教育における危険性への対応など、これからの社会に生きる人が全て理解している必要がある重要なものと考える。

①　危機対応１：機　　械

安全が脅かされたときに、それを最初に防ぐ「防波堤」の役割を果たすものである。情報セキュ

リティに関しては、自動的に働く機械として、ハードではファイアーウオール、暗号化ソフトなどがあげられる。

② 危機対応２：道　　具

安全が脅かされたときに、それを２番目に防ぐために、人が操作して防ぐ「ゲート」の役割を果たす。情報セキュリティに関しては、ハードではシステムのミラーリング、ソフトではワクチンソフトのインストールなどがあげられる。

③ 危機対応３：安全手順

安全が脅かされたときに、それを３番目に防ぐために、安全手順に従う「土嚢」の役割を果たす。情報セキュリティに関しては、ワクチンソフトでの定期的なチェックなどがあげられる。

④ 危機対応４：個人の安全認識

上記の３つの危機対応でチェックすることができなかったとき、最後の砦は「これはおかしい、こうしなければ」という個人の危機認識である。各人が下記のような危機が存在しそれにどう対処するかについて正しい認識をもち、常に気をつけていることが大切である。

なお、情報を管理する際の安全性の確保については、個人レベル、システムレベルで多少異なる[3)]。例えば、上記②のミラーリングは、個人では不要である。

一般に、危機は、上記の「機械」で防ぐことができず、「道具」でも防ぐことができず、「安全手順」でもだめで、「個人の安全認識」にも引っかからないときに初めて発生する。

もし、危機が発生したとき、責任を論ずるのは簡単である。しかし、その危機が上記①～④のどの部分で防ぐのが妥当であったか、その部分にどのような問題があって防げなかったか、何が脆弱であったかをきちんと評価することが当局者のなすべきこととして最重要課題である。

危機が起こったとき、システム的な対応とそれにに対する科学的な視点に立った評価が、これからの社会にとって非常に重要になるであろう。また、こうした評価結果は、本校だけでなく他校に対してもあてはめることができるので、広報活動をする必要のある、かけがえのない貴重なノウハウであると考える。

(3) 学校情報管理体制

附属学校園の情報を管理する組織は、情報管理責任者（附属学校部長）の下に各学校園の情報管理責任者（校園長）、その下に各校園の専門委員を置く。情報専門委員は、管理責任者の諮問を受けて基本方針や運用等の審議を行う。

また、学校情報の管理を、文部科学省の通知[4)]に基づいて、物理セキュリティ、人的セキュリティ、技術的セキュリティに分けて次のように行う。これらの管理体制は、高校だけでなく、附属学校園に共通したものである。

(a)　物理的セキュリティ

・**設置場所の管理**：サーバを含む機器は適切な場所に置き、各校園の情報専門委員が管理

・**情報の取扱い**：機密性が高い情報は書き換え不能な媒体に保存し、各校園の情報管理責任者が保管。データをバックアップした媒体は、上の設置場所で管理し、廃棄は情報専門委員が計画的に行う。

(b)　人的セキュリティ

・**情報の扱い**：各校園の教職員は、上記の機密性及び可用性に即した取扱いをする。

・**啓蒙・教育活動**：情報専門委員は各校園の教職員に対し情報セキュリティの啓蒙・教育を行う。

・**大学との連絡**：情報管理責任者及び情報専門委員会は、大学のシステム管理部会と連絡をとり、各校園の情報システムの円滑な運用を図る。

(c)　技術的セキュリティ

・**設備の利用**：情報専門委員会は、情報セキュリティの侵害防止のために必要な対策をとる。

・**設備の改変**：各校園における学内ＬＡＮ等の改変は情報専門委員会の許可を得て行う。

４．個人情報の考え方

個人情報保護法の施行に伴ない、学校が扱う個人情報についても単なる個人情報、整理された保有個人データなどのように明確な規定がなされ、その収集、整理、保存、流用、修正、廃棄などの管理については、各個人に対して説明責任が生じ、一定のルールに従って行うことが必要になった。ここでは、一般的な意味での個人情報及び学校における個人情報、学校での扱いについて述べる。

(1)　個人情報と保有個人データ

生徒や教職員など、高校ではさまざまな個人情報を扱っており、それらをまとめた名簿が受験産業などに流出している危険性も指摘されてきた。一方、文字や写真などをディジタル化し、インターネットを利用して情報を送受信するＩＴ革命といわれる時代にあって、住民基本台帳法など個人情報のデータベースからの個人情報の流出･漏洩の危険性が増大している。

学校教育では、生徒がこれからの社会で個人情報の適切な収集、管理をすることが必要なことから情報教育が行われるようになり、平成15年度から高校でも「情報」が必修教科となって高校生全員が個人情報について学習するようになった。学校で個人情報を扱うにはこうした背景がある。

氏名、住所、性別、年齢、生年月日、電話番号、勤務先など、個人を特定できる情報や、他の情報と組み合わせることにより個人を特定できる情報のことを個人情報という。このうち、住所、氏名、性別、生年月日は基本４情報と呼ばれ、公開される可能性が高い個人情報である。同じ個人情報でも社会的差別の原因になる事項である、思想、信条、宗教、本籍地、病歴、犯罪歴などは、原則的に非公開であり、事業者はこれを収集しないように求められている。こうしたことは、学校でも教育する

内容になりつつある[5]。

個人情報保護法が定める個人情報は、基本的には生存している個人に関する情報で、含まれる記述などから特定の個人が識別できる情報のことをいい、次のように、個人情報、個人データ、保有個人データの３つが定められている[6]。

個人情報 ｛ 個人情報：生存する特定の個人が識別できる情報
個人情報 ｛ 個人データ：データベース化した個人情報
個人情報 ｛ 保有個人データ：６ヶ月を超えて保有し、継続利用する個人データ

(2) データベース

個人情報はばらばらに保存されることもあるが、あいうえお順など体系的に整理し索引をつけるなどして検索できるようにして保存することが多い。こうしたものの中でコンピュータの中に保存したものをデータベースということが多い。ここで、「個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するもの」[6]で、コンピュータや手作業で検索処理できるようにしたものを個人情報データベース等という。本校における保有個人データベースには次のようなものがある。

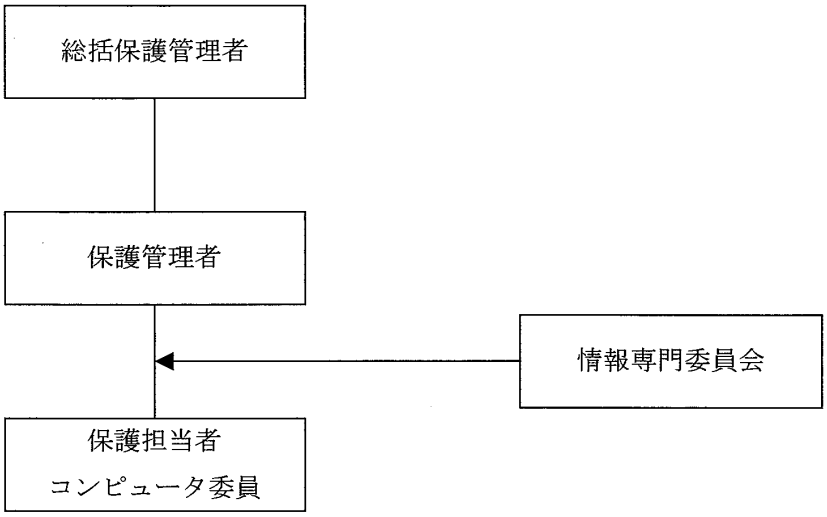
① 生徒家庭票	② 災害時生徒データ票	③ 災害緊急連絡カード
④ 日本スポーツ振興センター災害給付契約同意書		
⑤ 健康調査カード	⑥ 心臓病調査票	⑦ 入学検査に係る情報
⑧ 生徒教職員名簿	⑨ 後援会員名簿	⑩ 出 席 簿
⑪ 通 知 表	⑫ 成績原票	⑬ 成績一覧表
⑭ 調 査 書	⑮ 学 籍 簿	⑯ 進路一覧表

(3) 個人情報の管理

学校情報は、個人情報の他に入試情報、成績関連の情報などがある。それらの収集、処理、蓄積、廃棄等は、一定の手順に従って行うことが個人情報保護法で義務付けられている。実際には、学校運営の効率化、危機への対応などの観点から、附属校園で歩調を合わせ、共通した処理方式で行うことが望ましい。その具体的な方法は、文部科学省の指針[6]、本大学の規則[7]に基づいてポリシーとして策定してきた。

(a) 組　　織

附属学校部及び各附属学校園の情報管理組織は、次のように構成されている。ここで、総括保護管理者は情報担当の副学長、保護管理者は附属学校部長および各学校園長、保護担当者は各学校園の副校長が担当する。



・**総括保護管理者**：附属学校園の情報全般を管理者する。

・**保護管理者**：保有個人情報を適切に管理し、保有個人情報の秘匿性等に応じてアクセス権を有する者（実際は各学校園のコンピュータ委員）を指名する。

・**保護担当者**：保護管理者を補佐し、保有個人情報の管理についての事務を行う。

・**情報専門委員**：保有個人データベースのシステム設計など情報管理についての事務を行う。

(b) 業　務

上記の保護担当者やコンピュータ委員が保護管理者の下で行う業務内容は、本大学の規則[7]によれば、次のように定めることができる。

① 研　修

各学校園の教員に対して、保有個人情報の取扱いの研修に参加する機会を与える。

② アクセス管理

個人情報データベースをアクセスする際、必要に応じてパスワードを用いてアクセス権を識別し、その管理について定め、アクセス状況を記録し、定期的に分析する。

また、アクセス記録の改ざんや不正な消去防止のための措置をとり、保有個人情報の秘匿性その他の内容に応じてアクセスする権限を有する者だけがアクセスすることのできる保有個人情報を定める。

③ 媒体の管理

保有個人情報の複製・送信、記録媒体の外部への持出し等の管理、保有個人情報に誤りがあった場合の修正等を行う。

④ 台帳の整備

保護管理者は、保有個人情報の内容に応じて台帳等を整備し、利用及び保管について記録する。

⑤ 端末及びサーバの管理

情報システムの端末の盗難または紛失の防止措置、第三者に閲覧されないための措置を定める。

また、基幹的なサーバ等の機器を設置する部屋の施錠と入退室の記録などを行うとともに、災害時に備え情報サーバ室に適切な設備を施す。

⑥ 廃　　棄

情報管理者は、保管期限を過ぎた保有個人情報を計画的かつ完全に廃棄する。

こうした、概括的な業務内容をポリシーに明記することによって、各附属学校園で個人情報の取扱い基準や取扱いマニュアルが一定の「土俵」の中で作成されることになる。

５．おわりに

ここでは、情報セキュリティ、個人情報を中心に、学校情報とその管理の構造について述べてきた。情報管理は、情報セキュリティポリシー、個人情報ポリシーの下に情報セキュリティや個人情報の取扱い基準やWebページ取扱基準があり、その下に対策マニュアルが作成されるものであるとの考え方[8]に沿っている。

ここでは、学校情報、情報セキュリティ、附属学校園の情報セキュリティポリシー、個人情報、個人情報保護ポリシーなどについて、危機管理の新しい視点から定義と関連性を明確にしたつもりであり、この点が新しさである。

しかし、情報セキュリティ、個人情報、Webページの管理についての具体的な基準、それらをもとにしたマニュアルについては平成18年度の情報専門委員会の課題であることから、ここでは述べなかった。

参考文献・参考ＵＲＬ

1) 辰巳丈夫「情報化社会と情報倫理」共立出版、2004. 9

2) 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/joho_tsusin/security/index.htm

3) 「情報Ｂ教科書」実教出版2005

4) 文部科学省「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（通知）16国文科総第64号　平成16年９月17日付」

5) 高橋参吉他「情報倫理」実教出版　2002. 3

6) 文部科学省「学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」解説　2005. 1

7) (国)お茶の水女子大学個人情報の管理に関する規則、平成17年３月

8) (有)データーランド「情報管理責任者のためのネットワークセキュリティハンドブック」(株)明光商会