

# 学習者の個人情報を守っていますか？

eラーニング・サービスのための個人情報保護ガイド

パブリックコメント版



2003年3月 \* \* 日

先進学習基盤協議会

## 背景

教育機関はもともと学習者の連絡先や成績情報など多くの個人情報を持っていましたが、これらの個人情報は施設もしくは組織内で厳しく管理されてきました。しかし、教育機関のコンピュータがネットワークに接続され、さらに、単位互換や学校間の連携が広がりネットワーク上で履修情報や成績情報が交換されるようになってきています。企業や医療機関でも細心の注意を計っていながらも個人情報の流出がたびたび起こっていますし、教育機関においてもこれまで以上のセキュリティの確保と個人情報取り扱いへの配慮が求められています。

## 目的

本ガイドは、eラーニング・サービス提供者が適正に個人情報を管理することを促進することを目的としています。

## なぜ個人情報保護が必要か

社会の情報化が進むに伴い個人情報保護の重要性がクローズアップされています。個人情報の流出は、名簿の売買が行われるなど、これまでもさまざまな問題点を持っていましたが、ネットワークの広まりとともに、流出する情報の量や範囲などが従来になく広がる危険性がでてきたからです。平成11年に行った総務省の調査によると、特に個人情報の流出について漏れてほしくない情報としては、半数以上の人住所などの情報に加えて学歴や成績情報と答えています。

実際に教育機関は個人情報を大量に管理しており、これらが流失した場合には社会的な影響が非常に大きいと考えられます。

教育事業者が持っている主な個人情報は以下のものがあります。

- ・ 個人名
- ・ 性別、年齢
- ・ 連絡先(住所、電話番号)
- ・ 履修情報
- ・ 成績情報                      など

更に、事業者によっては、保護者の職業、進学先などさらに多くの情報を持っています。また、eラーニングを円滑に行うために学習者情報を交換するための標準作りも海外で行われています。この中の個人情報の項目には、上記のものに加えて学習目標や進捗情報、卒業証明なども入っています。

個人情報は流出するだけでなく、提出した個人情報がどのように管理されている

のか、修正は可能かなども最近では重要になっており、個人情報を収集するにあたり個人情報保護ポリシーを定め公開している事業者も増えてきています。

### 個人情報流出のリスク

個人情報の流出にはさまざまなルートが存在しています。関係者の不注意が原因としては多いですが、故意に情報を持ち出す行為も最近では増えています。

主な要因としては以下のものが考えられます。

- ・ 関係者による持ち出し
  - 管理が不十分な個人情報を持ち出される
- ・ 機器や媒体の置き忘れ
  - 電車や食堂などにノートパソコンやメディアを置き忘れる
- ・ 誤操作による流出
  - ファイルのコピーやメールの送信先を間違えて個人情報が流出する
- ・ 廃棄機器から流出
  - 古くなって廃棄したパソコンから個人情報が流出する
- ・ ネットワーク上での漏洩
  - ネットワークで個人情報を交換しているときに第三者により盗聴される
- ・ 不正侵入による盗難
  - 教育機関のコンピュータに進入され、ファイルを盗まれる
- ・ ウィルスによる予期しない転送
  - ウィルス感染による異常動作により、ファイルが自動送出される

### 信頼されるeラーニング・サービス提供者になるために

個人情報が流出しないために、職員に対する啓発をはじめとして多くの取り組みを行う必要があります。

- ・ セキュリティポリシーを整備する
  - 情報システムのセキュリティ対策だけでなく、人的運用まで含んだセキュリティの基本方針を整備する
- ・ 個人情報簿ポリシーを策定する
  - 個人情報の収集、保管、修正、廃棄等、取り扱いに関して基本方針を整備する
- ・ 不正侵入やウィルスに対する対処をする
  - システム保護のために適切な装置やソフトウェアを入れるとともに、常に最新の状態にアップデートしておかなければならない

- ・ ファイルを暗号化する
  - 個人情報と保存しているファイルを暗号化して、第三者が見られないようにする
- ・ 個人情報が特定できないファイル構成にする
  - 個人情報のデータをいくつかのファイルに分割して、一部のファイルの流出では個人が特定できないようにする
- ・ 機器やメディア廃棄時には適正な処理を行う
  - 記録装置、メディアの完全消去ソフトなどで消去するか、専門廃棄業者に処理を依頼する
- ・ 職員の意識啓発を行う
  - 誤操作を防ぐには、日頃から個人情報を扱っていることを職員に自覚させ、細心の注意で情報を扱うように啓発する

## 個人情報保護ポリシーの整備

個人情報保護ポリシーは、事業者毎に整備していくことになりますが、以下のOECDの8原則が満たされている必要があります。

### 収集制限の原則

個人データの収集は、自ら登録を行うなど、適法かつ公正な手段によるべきであり、データ保持者に通知又は同意を得て行うべきである

### データの正確性の原則

個人データは、受講のためなど、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、完全、最新に保たねばならない

### 目的明確化の原則

個人情報の収集目的は、収集前もしくは収集時に明確化されなければならない、その後の利用は収集目的にかなない、かつ明確化されたものに制限するべき

### 利用制限の原則

個人データは、明確化された目的以外に使用されるべきではない

### 安全保護の原則

個人データは、紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない

### 公開の原則

個人データに関する利用、運用、ポリシーは一般に公開されなければならない。また、データ管理者が容易にわかるように明示しなければならない

### 個人参加の原則

個人情報登録者に関するデータの所在を確認し、本人に対して知らしめられる

べきである。また、自分に関するデータについて異議申立ができ、異議が認められた場合には、データの消去、修正、完全化、補正ができなければならない責任の原則

データ管理者は、以上の原則を実施するための措置に従う責任を有するべき

このOECDの8原則を参考にして国内では「個人情報保護基本法制に関する大綱」が2001年に閣議決定されています。この内容も参照することが望ましいです。また、(財)日本情報処理開発協会では、「プライバシーマーク制度」を1998年から運用していることから、このマークを取得することも受講者の安心につながるものと考えられます。

### 子供向けの個人情報保護

インターネットを子供が利用する場合の個人情報の扱いについては、学校のホームページで写真を載せるときに顔と名前が一致しないようにするなど、これまでも国内で論議されてきました。米国においては、児童オンラインプライバシー保護法(COPPA)が制定されており、子供向けのサイトではプライバシーに関する注意書きを載せること、両親の承諾を取ることで、第三者に情報を提供するときには両親の承認を得ることなどオンライン上で情報を集める事業者を法で規制しています。

### eラーニング事業者に期待されること

事業者が行うべきことは簡単です。個人情報の流出を防ぐことと学習者に安心される運用を行うことです。

また、ネットワークを通じて情報が流通することを考えると、個人情報を交換する事業者についても、このガイドにある観点から見定める必要があります。自社が集めた個人情報が他社から流出した場合にも、責任が問われるとともに、ブランド、信用力に大きな傷が付くことに留意しなければなりません。

## 参考

「プライバシー保護と個人データの流通についてのガイドラインに関する理事会勧告」  
OECD 1980年

<http://www.jipdec.or.jp/security/MarkSystem.html>

「個人情報保護基本法制に関する大綱」情報通信技術(IT)戦略本部個人情報保護  
法制化専門委員会平成12年

<http://www.kantei.go.jp/jp/it/privacy/houseika/taikouan/1011taikou.html>

「プライバシーマーク制度」(財)日本情報処理開発協会平成10年

<http://www.jipdec.or.jp/security/MarkSystem.html>

The Children's Online Privacy Protection Act of 1998 (COPPA)

<http://www.ftc.gov/opa/1999/9910/childfinal.htm>

IMS Learner Information Package Information Model Specification V.1 2001

<http://www.imsproject.org>