

教総第 298 号
平成 14 年 8 月 9 日

本 庁 各 課 長
各教育振興事務所
各教育機関の長
各 県 立 学 校 長

} 様

教 育 長

コンピュータネットワーク利用における個人情報保護について（通知）

近年、コンピュータネットワークが整備されるに伴い、個人情報が外部へ流出し、悪用される事例が相次いでおります。

また、本年 6 月、他県にて高校の卒業生名と進路先データがインターネットのホームページ上に掲載された例のように、本県でも行政機関の所有する児童・生徒などの個人情報がコンピュータネットワークを通して流出し、人権侵害等の問題が発生することが強く懸念されております。

ついては、別添「コンピュータネットワーク利用における個人情報保護について」を精読のうえ、コンピュータネットワークの利用に際しては、個人情報保護について最善の対策を講じ、漏洩することのないよう取扱には十分留意願います。

担当：政策企画担当 仁尾
内線 3514

コンピュータネットワーク利用における個人情報保護について

基本的な考え方

1. 個人情報¹の取扱には岐阜県個人情報条例などの関係法令の内容を遵守し、最新の注意を払うとともに、外部への漏洩が起きないように最善の対策を講じること。
2. コンピュータネットワークの管理を徹底し、情報中心ネットワークの危険性について十分に認識しておくこと。
3. 個人情報の記録された記憶媒体（ハードディスク、フロッピーディスク、光磁気ディスク、半導体メモリなど）の管理を徹底すること。
4. コンピュータやネットワークに関する所属内の利用規程や要領を厳守すること。

個人情報を漏洩させないための対策方法

- 原則として、外部ネットワークと接続状態にあるコンピュータで個人情報は扱わない。
- 個人情報をハードディスクに記録しているコンピュータはネットワークに接続しない。（RENTAI 接続の機器を除く）
- ハードディスク（HD）、フロッピーディスク（FD）や光磁気ディスク（MO）、その他（CD や DVD など）の記憶媒体に個人情報を保存した場合、耐火金庫に保管するなど、厳重に管理し、盗難、遺失が発生しないようにする。
- ネットワーク接続の有無に関わらず、コンピュータにはウィルス²対策ソフトを導入し、最新のウィルスに対応できる状態にしておく。
- 万一ウィルス感染が認められた場合には、感染が広がらないよう速やかに最善の措置を施し、問題解決を図る。
- パソコン本体及び記憶媒体の廃棄、譲渡の際には、記憶媒体の物理的な破壊や消去ソフトの利用により、個人情報の消去を完全に行うこと。

日常の情報管理について

- 所属内に存在する様々なデジタル情報について、その種類や量、記録されている場所、利用許可範囲、管理責任者等を明確にするとともに、所属全体として総括的に管理する。
- 職員が個人的にネットワーク機器等の設定変更を行わない。
- インターネットに公開するホームページ上の情報は必ず所属長の決裁の後に公開する。
- 個人の顔写真などの個人情報をホームページ上に公開する場合には、必ず本人及び保護者から許諾を得る。
- 情報にアクセスするために必要なパスワードは、定期的に変更することにより漏洩を防ぐ。
- 日常的にネットワークを監視し、ウィルス感染など異常がないかを確認する。
- 所属宛の電子メールは一日1回以上は確認し、通常の事務文書規定と同様に扱う。また、不審、不明な電子メールの扱いには十分注意する。

個人情報漏洩すると想定される例とその対策

- 個人情報であることを認識せずに漏洩する例

例 1) 学校のホームページ上に部活動の情報を掲載したが、その中に本人と保護者の承諾のない顔写真の画像があり、結果として個人の氏名、顔写真、活動成績等が第三者に特定されてしまうことになった。

→ **許諾されていない個人情報は公開しない。**

例 2) 卒業生に記念として CD-ROM を配布したが、その中に卒業生の住所録や進路先のデータがあった。数年後、ホームページ上に実名入りで一覧表が掲載された。

→ **許諾されていない個人情報は公開しない。**

デジタルデータは簡単に転送・複製できるので、使用者側にも取扱に注意させる。

- 個人情報であることを認識しながら、取り扱いを誤って漏洩する例

例 3) 部活の選手名簿を電子メールで対戦相手に送付する際、送信先メールアドレスを間違えてしまい、第三者に選手名簿が漏洩した。

→ **個人情報を扱う場合は機器の取り扱いを慎重にする。**

例 4) 表計算ソフトやデータベースソフトを使った成績処理システムを作成し、校内 LAN 上のサーバ機に保存することで、ネットワーク経由の成績処理を行っていた。このサーバ機への接続はユーザ名とパスワードによるもので、このパスワードが第三者に知られたことにより、蓄積されていた過去数年分の成績データが外部に漏洩した。

→ **個人情報を扱う場合は機器の取り扱いや操作を慎重にする。**

パスワードの管理を徹底する。

個人情報の記録された記憶媒体の管理を徹底する。(不要となったデータの消去など)

- セキュリティについて技術的に問題がないと誤認していて個人情報が漏洩する例

例 5) 職員用と生徒用のネットワークを機器の設定によって分離し、職員用ネットワーク上で生徒の進学先情報を共有していたが、外部からの不正アクセスにより、機器の設定が変更され、進学先情報が漏洩した。

→ **セキュリティレベルを再確認し、機器の設定用パスワードの管理を厳重にする。**

例 6) 電子メールを使って生徒との間で教育相談的な指導をしていた。メールアドレス等の間違いもなかったが、通信情報を第三者に傍受され、相談内容がインターネット上の電子掲示板に掲示されていた。

→ **外部ネットワークでは常に通信傍受の可能性があることを考慮したメールの内容にする。**

例 7) 個人を特定できる情報を保存していたパソコンをインターネット接続用パソコ

ンとして使用することにした。セキュリティを考慮してウィルス対策ソフトも最新のものとしていたが、対策が出来ていない新種のウィルスの感染し、メールにハードディスク内のファイルが自動的に添付され、複数の宛先に配信された。このウィルス付きメールの受信者はさらにウィルス感染し、不特定多数に個人情報漏洩した。

→個人情報の記録された記憶媒体の管理を徹底する。(不要となったデータの消去など)

ウィルスソフトが常に安全とは限らないことを認識する。

【用語説明】

- 1 個人情報： 個人に関する情報であり、文章記述、画像、音声、記号等により当該個人を識別できるもの。また、その情報単独では個人を特定できなくても、他の情報と組み合わせると個人として照合できるもの。
- 2 ウィルス： コンピュータのウィルスは他人のシステムやファイルに何らかの被害を与えることを目的として作成されたプログラムで、ファイルやオペレーティングシステムの一部を書き換えるなどして、自身の複製を生成したり、メールやホームページなどのネットワーク接続経路により他のシステムに侵入を試みる動作をするものがある。
メールを使って感染経路を広げるタイプのウィルスにおいては、感染者は被害者と思いがちであるが、感染後はネットワーク上で他人に対してもウィルスを送信するため、実際には加害者となる。