

養護学校における情報セキュリティポリシーの策定

ー 個人情報の取扱いと個人所有パソコンの接続に考慮した対策について ー

愛知県立豊橋養護学校 教諭 山本 全実

k601470i@m2.aichi-c.ed.jp

キーワード：個人情報、セキュリティポリシー、養護学校、個人所有パソコン

1. はじめに

愛知県では平成19年度以降、生徒用サーバ、職員用サーバ並びに教職員にパソコンが整備される。特に教職員パソコンは、教育用機器と行政ネットワーク用端末の両方で利用するため、セキュリティポリシーの策定が急務となった。そこで、利便性をできるだけ損なわず個人情報の取扱いと従来から接続している個人所有パソコンについて配慮したセキュリティポリシー策定の経緯について報告する。

2. ネットワーク環境

本校は、個人情報を取り扱うデータベースサーバと教職員が作ったファイルを保管するファイルサーバが、ファイヤウォールで仕切られたネットワーク内で稼働している。データベースサーバに直接アクセスできるのは、管理者のみである。それ以外の教職員は、Perlで作成したWebアプリケーションを経由してアクセスする。電子ファイルは、ファイルサーバの決められたフォルダに保存・蓄積するようになっている。ファイルサーバへアクセスするためには、IDとパスワード（英大文字、英小文字、数字を必ず一つ以上含む8文字以上の類推されにくいもの）が必要となる。学校が所有するパソコン（端末）は4台で、それ以外に100台程度の個人所有パソコンがネットワークに接続されている。

3. 情報の洗い出しと重み付け

(1) 洗い出し

本実践を行うため、情報セキュリティ委員会を従来からある個人情報保護委員会の中に位置付け、収集する情報の範囲を「個人情報を含むもの」から「学校で取り扱うすべての情報」に拡大して取り組んだ。夏季休業中に本委員会を開き、洗い出す手順を説明した。洗い出しは、部主事と分掌主任を情報管理者とし、そこを中心に行った。この日は終日、本作業に取り組んでいただくようお願いしてあったので、効率よく作業を進めることができた。しかし、小学部、中学部、高等部、指導部（生徒指導部）、進路指導部、教務部は、他の分掌と比べると情報量が多く、本作業を終えるのに3日から5日ほどかかった。

実際の作業は、洗い出しの中心となる部や分掌ごとにシートを分けたエクセルファイルを共有設定してファイルサーバに置いた。情報管理者は、ファイル名を確認しながら指定したエクセルのシート（共有）へ入力していった。

(2) 情報を守る必要性の判断基準

次のように判断基準を設けて情報を守る必要性の項目に対して「大」、「中」、「小」が、選択できるよう工夫した。また、「大」については、取り扱う方法を明確にした。

○「小」についての判断基準

- ・消えてもよい情報、消されてもよい情報、リサイクル、リユースされない情報
- ・公開されてもよい情報、一般公開されている情報
- ・希望者又は一般に配布している情報、漏えいしても支障のない情報

○「中」についての判断基準

- ・リサイクル、リユースされる情報、消えると困る情報、漏えいしても支障のない情報

○「大」についての判断基準

- ・リサイクル、リユースされる情報、消えると困る情報かつ個人情報を含むもの、漏えいしてはならない情報

○「大」についての取扱い

- ・各ファイルについてはパスワード付きで保存、持ち出す場合は暗号化
- ・個人情報については、データベースサーバで管理
- ・盗難、紛失、情報漏えい時は教育委員会へ報告、保護者へ文書配布し、児童生徒の安全を確保できるよう通知

(3) 対策の必要性の判断基準

○「大」についての判断基準

- ・情報資産を個人所有の媒体やパソコンに保存して管理している場合
- ・個人情報を含む情報資産をファイルサーバで管理している場合

- 「中」についての判断基準…個人情報を含まない情報資産をファイルサーバで管理している場合
- 「小」についての判断基準…データベースサーバで情報資産を管理している場合

(4) 実践と考察

洗い出しを進めていく中で、同じ名前の情報資産であっても、記入された内容によって重要度が異なることが分かった。例えば、「児童生徒個票」である。保護者に配布する様式は、配布を前提としたものなので漏えいの脅威を恐れることはない。また、必要に応じて変更していくので消えてしまうと困るから重要度は「中」とした。個人情報が記入された後も「児童生徒個票」と、名前は変わらないが、漏えいしては困るので、重要度は「大」とした。

次に、収集した個人情報を電子情報化する場合である。ワープロや表計算で一覧表にまとめたり、データベースに入力したりしたものが該当する。こちらも、漏えいしては困るので重要度は「大」とした。

これ以外に学級通信や学年通信など公開を前提とした情報がある。配布するまでは、消えると困る情報なので重要度「中」だが、配布後は、役目を終えるので「小」となる。今回は、作成途中の情報は、洗い出しの範囲外としたので「小」とした。

4. ファイルの管理と運営

(1) フォルダ構成

年度ごとにフォルダを作成する。その中を情報管理者ごとに細分化した。具体的には、部、分掌、各種委員会ごとにフォルダを作成した。このように情報資産の管理者を明確にすることによって洗い出し作業を効率よく行うことができた。また、各種様式用のフォルダを独立して作成した。これは、次年度以降も継続利用が考えられるので自動消去スクリプトが誤って消去しないようするためである。

(2) 個人情報を含むものは、個人情報の項目をすべて明記

情報を洗い出すときに個人情報を含むものは、その項目（氏名、住所、電話番号…）まで、正確に洗い出した。漏えいした場合、個人情報の項目が分かれば、保護者により適切に注意を呼びかけることができる。例えば、電話番号が含まれている場合は、振り込め詐欺へ悪用されることが予想できる。

(3) 情報資産のライフサイクルと廃棄

洗い出した情報資産には、保存年限（廃棄年度）を設定する。永年保存のものを除き、年度末にスクリプトで自動的に消去することができる。

5. 情報セキュリティポリシー作成と工夫

本校で定める「愛知県立豊橋養護学校ネットワーク利用規程」に「個人情報の取扱いに関する規程」及び「愛知県立学校セキュリティポリシー」で定めた必須事項を加え、「愛知県立豊橋養護学校情報セキュリティポリシー（利用者用）」として新たに作成した。また、情報化推進者及びネットワーク担当者向けに「愛知県立豊橋養護学校情報セキュリティポリシー（管理者用）」を設けた。

本校の現状から考えられる脅威に対して次のように考えた。管理する側から操作環境を統一できるものについては、管理者用のセキュリティポリシーに盛り込み、サーバ側の設定により解決した。そうでないものについては、利用者用のセキュリティポリシーに盛り込んで、利用する個々の教職員によって解決してもらうよう内容を整理した。具体的には個人情報の蓄積については、データベースサーバを中心に管理し、管理者用のポリシーに明記した。データベースサーバで管理できない個人情報を含むファイルについては、ファイルサーバにパスワード付きで保存するというポリシーを定め、利用者用のポリシーに明記した。

実際の運用に当たって、一般の教職員は、利用者用のポリシーに従って活用していく。また、管理責任者、情報化推進者、ネットワーク担当者は、利用者及び管理者用のポリシーに従って業務を行う。このように利用者用と管理者用に分けることによって、各ポリシーの対象とする範囲が明確になり、スムーズに実施されるよう工夫した。

6. 今後の課題と展望

今回作成した情報セキュリティポリシーをスムーズに伝えるために管理者用にQ&Aが必要と感じた。個々の内容について「必ず守らなければならないもの」なのか「できるだけ守った方がよいものなのか」という微妙なニュアンスを伝えたり、利用環境やコンテンツが変わったときに改訂が必要な項目ということを伝えたりする内容である。また、利用者には、画面のハードコピーをふだんに使った操作手順書の準備といつでも手軽に閲覧できる環境が必要と感じた。