阿波西高等学校におけるセキュリティポリシー作成の過程と問題点

ー 情報漏洩防止と教職員の意識変革 ー

徳島県立阿波西高等学校　教諭　山下　和利
yamashita-kazutoshi-1@mt.tokushima-ec.ed.jp

キーワード：情報セキュリティ，セキュリティポリシー作成，情報セキュリティ運用

１．はじめに

本研究は，情報セキュリティポリシー策定・運用事業の研究指定を徳島県教育委員会（以下県教委）が受け，県教委からの依頼に基づき行った。

本校におけるＩＴ関連の環境は，教員１名につき，ノートＰＣが１台貸与（内２７人分は生徒用と共用）され，職員室で無線ＬＡＮで運用されている。また，県内の県立学校は，徳島県教育情報ネットワークで結ばれている。また，授業におけるＰＣの利用，職員会議でのＰＣの利用，連絡簿としての掲示板の活用，校内連絡用としての E-mail の利用など県内の他の学校と比較してもＰＣの活用は多いと思われる。

しかし，明確な運用規程等が無く，また，昨年度は，一部のＰＣがトロイの木馬系のウイルスに感染するなどセキュリティの上で危険な状態であり，セキュリティポリシーの作成の必要性を感じていた。

２．ポリシーの作成の過程と問題点

２．１ ポリシー作成のスケジュール

６月に校内組織としてセキュリティポリシー作成委員会を設置し，教務課情報担当者を委員として，ポリシー策定のためのスケジュールを決定した。夏季休業中に全職員に各個人，校務分掌で所有する情報資産の洗い出しを依頼し，その後，資産の整理やリスク，対策について委員を中心に作成し，１０月中旬に，電子媒体に対するポリシーを策定し，１１月から運用を開始した。また，冬季休業中にアンケートを行い，ポリシーの遵守状況を確認した。それと同時に紙媒体に対するポリシーを作成し，２月から運用を開始する。

２．２ ポリシー作成の問題点と改良点

（１） 情報資産の洗い出し

全教員が所有する情報資産を洗い出して提出することで，職員の情報資産に対する意識の向上につながるという好結果を得ることはできたが，正確な資産の把握に時間と労力がかかった。実際には２回調査をやり直し，３回目でほぼ満足できる結果を得ることができた。１回目の調査の後，委員を中心にすべてのデータから情報資産の一覧表を作成し，所有の有無や所有形態（紙媒体 or 電子媒体）について書き込んでもらった。

（２） 資産に対する脅威の評価

学校が所有する資産の数が膨大になるため，資産毎に脅威を評価したり，リスク対応を考えるのは難しいという意見が委員の中から起き，本校では資産を生徒に関するもの，職員に関するもの，ネットワーク等に関するもの，公開されているが保護すべき資産，学校経営上必要な資産，保護者等に関するもの，最も取扱いに注意を払うものに分類し，その中でカテゴリー（１～５）に分類した。

（３）ポリシーの作成

最初，ポリシー作成についてはフローチャート的な図表を中心に作成していくことを検討していたが，話し合いの結果，ポリシーを文書化して，その後重要な内容については，フローチャートを作成することになった。しかし，ハンドブックの雛形では，イメージすることが難しいと考え，文例を探し，ＮＰＯ日本ネットワークセキュリティー協会（ＪＮＳＡ）の情報セキュリティポリシーサンプル（0.92a 版）をベースに，校内の状況に合わせてポリシーを作成した。しかし，その作業量が膨大になり，教員としての日常の業務との間でかなり苦しんだ。しかし，ポリシーを文書化することで全体像を把握することができ，セキュリティを運用・管理していく上で，様々な校務上の問題点の把握に役立った。

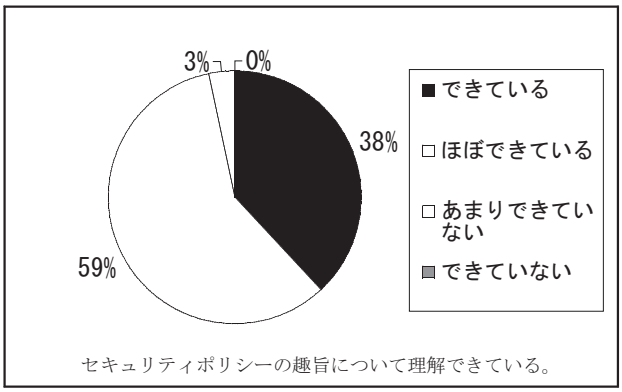
また，手順書には，実際の操作の仕方を説明する図表（電子メールの使い方（ＢＣＣ等），Ｗｅｂサービス，ファイルへのパスワード付与，暗号化ソフトの使用方法・・・）を入れ，職員の理解に役立つよう工夫した。

（４）ポリシーの周知

ポリシーの内容が膨大になったため，内容を職員に周知する会議に約７時間要した。しかし，運用をしていく上で必要なことであり，避けて通ってはいけないことであることが，後に説明するアンケート結果からわかる。

３．アンケートの結果から見えるポリシーの運用の現状

冬季休業中に全職員に対して，アンケートを行い，問いに対して，「できていない」を１，「あまりできていない」を２，「ほぼできている」を３，「できている」を４で，答えてもらった。



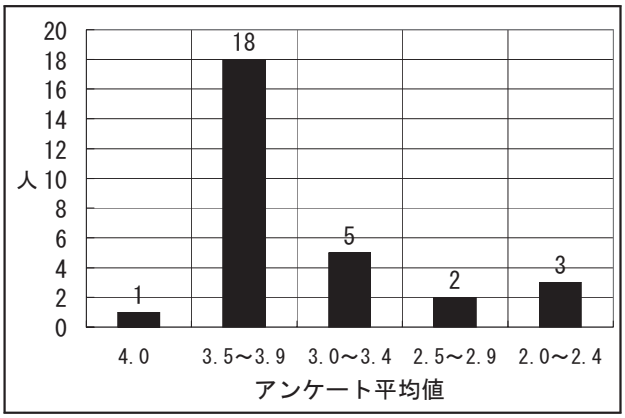


図１　セキュリティポリシーアンケート集計結果

アンケートの結果から，職員の意識改革がかなり進んだことと，大多数の職員がセキュリティについて考えながら，仕事をすることができているということがわかる。一部の職員からポリシーの導入で「手間がかかるが，セキュリティポリシーを守ることで自分が守られているということがわかった。」などの肯定的な意見も寄せられた。

４．職員の協力体制の重要性

ポリシーを導入する一番の鍵は，管理職の理解と職員の協力である。本校の場合，管理職の理解は大変大きく，限られた予算の中でファイルサーバの新規導入やネットワーク監視ソフトの導入などハード面の整備だけでなく，職員に対する連絡の中で，全国で起こった漏洩事故の周知など積極的に関わっていただけた。また，職員も忙しい中，資産調査やポリシーの導入のための会議に積極的に参加し，不明な点を積極的に質問する姿が見られた。係の職員だけががんばったらポリシーを作ることができるが，単なる形だけの文章だけになってしまい，実効性の全くないものになってしまう。そうならないためにも職員の協力体制をどのように築くかが最重要課題になると考える。

５．ポリシー作成と運用の課題

（１） 継続性

運用において見直しを絶えずすることは重要であるが，そのためには職員の意識をどのように高めていけるかどうかによってポリシーの有効性が変わってくる。今年の研究を通して考えた結果，毎年各職員が所有する資産を調査することにより，意識を継続させることができると考える。また，ポリシーで自分達が守られているという意識を持たせることが重要であると考える。

（２） 有効性の確認

ポリシー作成の際に一番悩んだことは，専門家でないものが作成したポリシーの有効性である。企業はポリシー作成に第三者等の意見を求め，作成することが多い。第三者の意見を求めることで内部から見えなかったことが見える可能性が大きく，またポリシーの有効性を高めることができると思う。しかし，専門家でない者が，学校の実情をふまえてポリシーを作成することは，担当者のみならず，同僚教職員の意識変革をする上で多いに有用であると考える。

（３） ハンドブックの内容

ポリシーの作成の手順等参考になる点も多いが，失敗例や問題点の記述があれば，今後作成する学校において参考になることが大きいと思う。また，ポリシーを運用している学校の紹介や職員の意見等も掲載することでその有効性や重要性を多くの職員が認識できると思う。