校内ＬＡＮ・校務ＩＴ化時代における学校情報セキュリティの取組み

－ セキュリティを確保しながら使いやすい環境を目指して －

愛知県小牧市立桃ヶ丘小学校　教諭　丹羽　敦
an-niwa@komaki-aic.ed.jp

キーワード：小学校，セキュリティ、校内ＬＡＮ、運用ルール、検疫サーバー

１．はじめに

小牧市の小学校では、平成７年度から情報機器の整備がはじまり、学校内にはパソコンなどの情報機器があふれている。肥大化したネットワークのセキュリティを確立することは、容易ではない。2006年夏にコンピュータ室の機器の入れ替えに伴い、セキュリティの強化を図るセキュリティポリシーや運用ルールを確立するだけでなく、実際の設定などネットワークデザインと検疫サーバーの導入により、教育実践・校務支援において使いやすく、セキュリティを守る取組みを実践的に行ってきた。

２．現状と問題点

（１）整備の現状

桃ヶ丘小学校においては、パソコン教室、普通教室、校務ＩＴ化のために職員に配布されたラップトップなど約100台のパソコンに、授業用や校務支援用サーバーが５台が運用されている。校内各所には情報コンセントと無線ＬＡＮアクセスポイントがあり、さらに学校と教育センターがＷＡＮで接続されている。サーバーには児童名簿や成績など、個人情報が蓄積され、グループウエアが運用されている。また、同じネットワークがインターネットに接続され、学習支援やリサーチなどの教育活動に利用されている。

写真１　職員室での校務支援

（２）過去に起こった事例と問題点

かつて、小牧市内の小中学校において、次のような問題事例が発生した。

- 電子メールの第三者不正中継
- ウイルス感染
- ｗｅｂページ改竄
- 個人パソコン盗難にともなう、成績データの紛失

また、現在、校内各所にパソコンが設置されており、端末からの情報アクセス、また、無線ＬＡＮアクセスポイントや情報コンセントからの直接アクセスによるデータの漏洩の可能性がある。さらに、教職員のデータ持ち出しについてもその勤務の特殊性から日常的に行われている。

写真２　普通教室での活用

３．セキュリティ対策の取り組みの実際

（１）教育ネットワークの構築

以前は、各小中校にサーバーを設置し、それぞれインターネットに接続していた。また、教育委員会にあるサーバーとのデータのやり取りも、インターネットを経由していた。しかし、これでは、情報の漏洩の危険性があり、また、サーバーの管理も大変である。

小牧市では、2005年から教育ネットワークを構築し、各学校とセンターサーバーを専用線で結び、インターネットへの接続は、センターサーバー経由に一本化した。これにより、市内小中学校のインターネット接続について、一元管理ができ、外部からのアタックや不正侵入の防止、各小中校のホームページについて、管理がしやすくなった。また、教育委員会や学校間、センターサーバーとのデータのやりとりについて、閉鎖されたネットワーク内なので、安心して行えるようになった。

写真３　コンピュータ教室

さらに、教育センターには、データサーバーやビデオサーバー等も設置し、市内の小中学校間での教育利用に便宜を図っている。

（２）各校におけるＶ－ＬＡＮの構築

校内には、コンピュータ室と普通教室、そして職員室の３つのセグメントが設定されている。個人情報などの重要なデータは職員室のセグメント内のみで処理と保存を行っているので、コンピュータ室、普通教室のセグメントとはＶ－ＬＡＮで切り離し、職員室側へのアクセスを遮断した。逆に職員室セグメントからのコンピュータ室、普通教室

へのアクセスは可能にし、授業活用を容易にしている。また、教育利用に関するデータは、児童側のセグメントに格納している。

（3）セキュリティポリシー、運用ルールの確立

セキュリティポリシーや運用ルールを市内統一で作成し、実行している。ユーザーアカウントについては、校務支援にかかわるものは、全て職員個人のアカウントでログオンし、処理をすることにした。児童用パソコンにつては、低学年児童の特性も考えて、自動ログオンをする設定になっているが、グループウエア等で自己のデータを扱う場合は、ソフトウエアレベルにおいて児童個人のアカウントでログオンし、使用することにしている。

校務支援データについては、貸与されたラップトップ内への保存を禁止し、サーバーに保存することにしている。また、重要データの持ち出しは禁止するとともに、機器やデータの持ち出しについては、所属長の許可を必要とし、データについては持ち出しメディアのパスワードロックやデータの暗号化を条件にしている。

校務支援用ラップトップを全教職員に配布したことにより、個人所有のパソコンの接続を特別な場合を除き禁止した。

（4）校内ネットワークの監視と検疫サーバーの導入

校内ネットワークの状況については、常に管理ソフトで状況をモニターできる体勢にし、必要であれば警告や画面のロック、電源の入切が可能になっている。

無線ＬＡＮについては、暗号化とＭＡＣアドレスの制限により、外部から接続されることを防止しているが、校内の情報コンセントにパソコンを接続される事態も想定して、検疫サーバーを導入した。検疫サーバーでは、接続されたパソコンの起動時に、ＭＡＣアドレスが登録されているかの確認、ウイルスに感染していないかどうかのチェック、ウイルス対策ソフトの定義データが最新のものか等の確認を行い、いずれかに不備があれば、ネットワークへの接続を遮断するものである。これにより、端末の状態を把握するだけでなく、「予期せぬパソコン」の接続によるデータ流出を防ぐことが可能になった。の

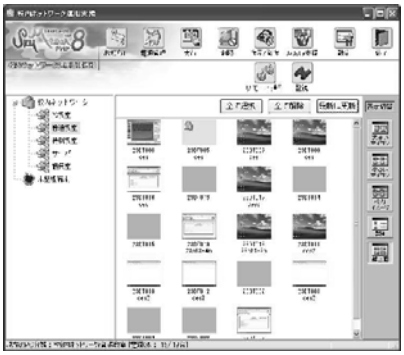

写真４ ネットワーク管理

（5）フィルタリング

児童が安心してインターネットを利用するために、フィルタリングを実施している。ただし、フィルタリングは、センターサーバーでは行わず、各校において行っている。これは、各校の実情と利用方法にあわせてカスタマイズできるよう配慮した。

また、児童の電子メール活用については、学校独自でサーバー運用を行っていたときは可能であったが、センターサーバー化にともない、実質的に停止している。しかし、一部の学校では、フィルタリング機能を持った児童用ｗｅｂメールを利用して、実践に取り組んでいる。

写真５ 検疫サーバーによる不正アクセス監視

（6）バックアップ

学校には、数々のデータが存在する。児童作品から校務データ、そして個人情報まで、膨大な量になっている。そのほとんどはサーバー内に格納されているが、もし何らかの障害が発生し、データが破損したら取り返しのつかないことになる。しかし、各所にコピーを置くのも、情報漏洩の観点から問題がある。

データについては、サーバー格納とし、サーバー自体にＲＡＩＤ機能を持たせ、サーバー間でミラーリングを行い、万が一に備えている。さらに、バックアップツールで、毎日深夜に、差分データの収集を行い、週末には全体をバックアップして、データ破損に備えている。

（7）緊急時対応計画

「情報資産の侵害」のような事例が発生した場合の連絡及び対応について、マニュアル化した。学校だけでなく、市役所担当課やサポート業者をふくめて、どのような対応をするかあらかじめ計画を作成しておき、緊急時に備えている。

４．おわりに

セキュリティと使いやすさは、相反するところがある。さらに小学校ならではの特殊性と、教育利用と校務支援が相乗りしていることなど、複雑な要因が絡んでいる。その中で、よりよい方策を考え、セキュリティについて模索してきた。しかし、セキュリティ対策については、次々に新たな問題が発生してくるので、終わりはない。常に最新の情報に目を向けて、アンテナを高くし、日々の備えをおこたらないことが、肝心だろう。