実施手順（システム管理者用）の策定と運用

センター員　大渕　寛、中原勝俊

１．理想と現実の妥協点を求めて

平成１４年末に基本となる「情報セキュリティポリシー」（以下ポリシーと略す）（案）ができたが、より具体的な規程を持つ「実施手順」がなければ実際に現場で活用することはできない。また、ポリシーは実施手順を作るための基礎でもある。ポリシーを策定するときに、「これ以上の説明は実施手順に書こう。」と後回しにしたことも多くあり、「実施手順ではできるだけ具体的に、分かりやすく、詳細に記述しよう！」と意気込んで策定を開始した。しかし、「理想と現実」の妥協点を探すことが最も重要なポイントとなった。セキュリティ確保を目的としながらも、実行可能な規程にしなければならないからだ。

２．まずは情報処理センターが管理する範囲

実は「システム管理者用実施手順」と言っても「システム」と呼ぶべきものは校内に複数ある。情報処理センターが管理する教育用電算システムやネットワーク基盤システム、事務部の電算システム、その他学科で構築したシステムも多数あるはずである。今回はまず情報処理センターが管理する部分に関するものに限定することにした。具体的には次にあげる部分である。

①校内ＬＡＮ基盤部（ＬＡＮ管理室内）
②校内ＬＡＮ幹線及び支線（光ケーブル、スイッチ、端子盤、情報コンセント等）
③情報処理センター第１演習室システム及び第２演習室システム
④ＣＡＤ室システム

更にこの実施手順が他のシステムでの基礎となることも期待された。皆様が使用されるシステムについての手順を作成する場合を想像していただきたい。

３．実施手順の構成

実施手順の基礎となる「ポリシー」の項目を基本として(1)定義等 (2)物理的セキュリティ、(3)人的セキュリティ、(4)技術的セキュリティ、(5)運用　の５章構成とした。

(1) 定義等

本章では「ポリシー」との関係、対象範囲、用語定義、システム管理者の責務といった、後に続く項目を考える上での重要な基準について記述した。対象範囲や専門用語として「パラメータ」と「スイッチ」を特に取り上げて説明した。これらの用語は一般的には複数の意味で使われているので、本手順での意味を明記した。

(2) 物理的セキュリティ

管理区域、入退室、機器の搬入搬出、機器取り付け、配線などについての具体的な指針を規定した。情報セキュリティ確保のために特に重要な区域を「第１種セキュリティ管理区域」として指定したこと。更に、本校が加入している「ＳＩＮＥＴ」のルータを長崎大学総合情報処理センターに設置していることを意識して「外部（本校外）に設置する機器の要件等」という項目も設けた。

(3) 人的セキュリティ

保守業務の外部委託での注意点、職員や学生への教育・訓練に関すること、セキュリティインシデント（事故・欠陥・侵害等）への準備についての指針を記述した。「セキュリティインシデント」は情報セキュリティに関する分野ではごく普通に使われるようになった言葉なので、あえて外来語としてカタカナのまま使った。

(4) 技術的セキュリティ

センターの各種サーバで記録しているログ等の取得や管理、ネットワーク機器やサーバの管理手順、ネットワーク機器などのハードウェアの利用手順について定めた。更にＯＳやアプリケーションソフト等のソフトウェアのセキュリティパッチの適用についても規定した。また、コンピュータウィルス対策手順についても規定したが、ＭＳブラスターの騒動後、さらに詳細な対策手順を示す必要性も感じられた。このような経験を踏まえて今後の実施手順の評価・見直しを図らなければならないことを痛感した。

(5) 運用

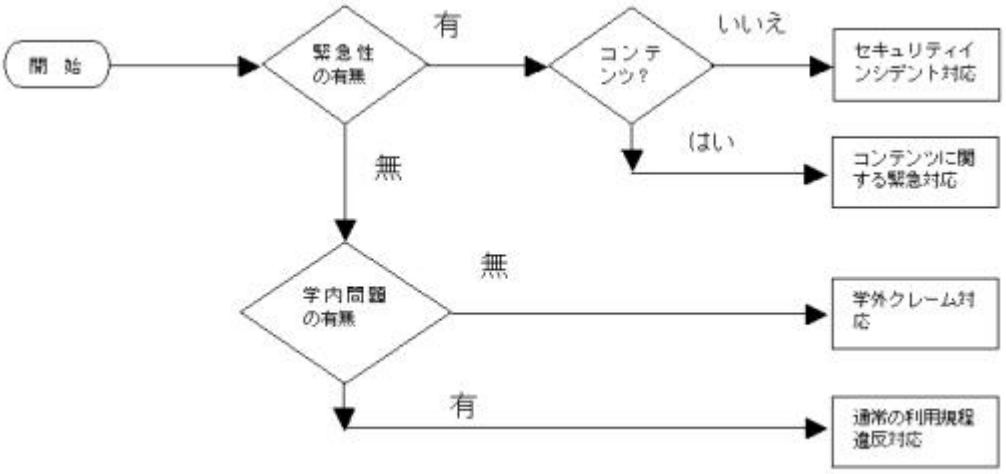
本手順書の中で最も難しい項目だった。インシデントやクレーム、規則違反への対応方法が含まれるので、運用を間違うと新たな問題を生む原因にもなりかねないからである。法的な根拠も必要なので、委員全員で検討を重ねた。次に挙げる項目について規定したが、これを見るだけで大変難しい問題であることがご理解いただけると思う。

①監視項目・監視手順
②監視記録の管理手順
③運用管理における人権に配慮した留意事項
④緊急時の対応一次判断の手順
⑤セキュリティインシデント対応手順
⑥コンテンツに対する緊急対応
⑦外部からのクレーム時の対応
⑧通常の利用規約違反行為への対応

「⑤セキュリティインシデント対応手順」では問題が１システム内では収まらないので、学校全体の問題としてとらえ、各所の責任者名や連絡先を明記した。
「コンテンツ」とは掲載や記述の内容のことで、⑥ではこれが常識はずれである場合の対応方法を規定した。ここでは最近社会問題となっている各種の人権侵害等に該当するような問題も含まれる。

また、昨年１１月に九州大学で開催された「情報セキュリティーポリシー入門講座」や情報処理センター長が各方面から収集した情報・資料が多分に活かされた。

「④緊急時の対応一次判断の手順」では次のとおり判断プロセスを図示することにより明確にした。



４．運用状況

「ポリシー」及び「実施手順」は平成１５年度から運用を始めたが、早速適応する場面があり、その結果課題も浮かび上がっている。

(1) メッセージによるトラブル等

教官宛に匿名による（他人のアカウントを使用）電子メールでいやがらせと思えるメッセージが届いたり、掲示板での匿名による無責任な発言が問題になった。
また、パソコンが無断使用されればメール内容などが簡単に暴露されてしまうことは低次元だが意外な盲点として心配される。このようなことは加害・被害者共に意識が薄い場合に発生するので、低学年のうちからの情報倫理教育が重要である。前記の「いやがらせメール」の後すぐに利用者向けの実施手順と教育用の抜粋集も配布したが、全学生に倫理を徹底するための教育を続ける必要がある。

(2) ＭＳブラストの脅威

平成１５年８月になって猛威をふるったこのコンピュータウイルスは後に「ネットワークウイルス」と分類されている。ＬＡＮに接続しているだけで感染するという点が今までのウイルスとは違っていた。ＯＳのセキュリティホールを修正することだけがユーザにできる防御策である。この修正パッチをあてる必要性について本実施手順では「４．技術的セキュリティ　(12)システム開発、導入、保守等の要件」に明記していた。しかし、この問題は職員が業務に使っている各パソコンにも必要なことであり、一般ユーザが各自で処置する必要がある。結局、ウイルスの脅威が目前に迫った盆明け（平成１５年８月）になってから大急ぎで通知を配布し、修正作業とその支援を実施した。その甲斐あって校内での感染はなかった。結果はそれなりに評価できるかもしれないが、後に「ＯＳの重要な修正パッチが公開された時点ですぐに全ユーザに修正が必要なことを周知すべきであった」ことが反省点となった。また、感染したノートパソコンの持ち込み１件と民間通信プロバイダと接続された無線インターフェースからの感染１件が見つかった。どちらも校内での拡散はなくて幸運であった。

(3) スパムメール

受信者の承諾を得ずに一方的に送られてくる迷惑な電子メールのことであるが、ほとんどが英語で書かれた宣伝メールであり、公序良俗に反する内容が多いのが特徴である。中にはウイルスの活動により送信されたものもあると考えられる。最近多くのユーザから「気持ちが悪い」、「必要なメールが埋もれて迷惑だ」と情報処理センターに苦情が寄せられるようになった。これに対する手順などは「ポリシー」にも「実施手順」にも記載していなかった。ほとんどのユーザが不快に感じている問題であるので、なんらかの対策指針を規定する必要がある。既に本センターではメールの「from」情報から多くの送信元をマークして、受信を拒否する設定を実施している。その結果週に３千件ものメールを遮断している。しかし、種類が多く、次から次へとアドレスを変更しながら活動する相手を全て掴むことはできない。また、「スパムメール」なのかどうかは最終的には受信者の受け取り方で決定される面もある。拒否対象として登録するのは受信者の強い要望があったものだけである。用のないドメインを文字列で検索して拒否する方法も効果的だが、受信者以外の者が勝手に通信を遮断する結果となるので無闇には使えない。対策は今後の課題となっている。現在もＭＳブラストや亜種の出現で大量のウイルスやスパムメールがトラフィック上に大きな影響を及ぼしており、今日、これらの対策も必要であると考えている。

５．終わりに

情報セキュリティポリシーは、「Plan-Do-Check-Action」という実施サイクルでスパイラル的に向上させることが求められているので、運用を通して問題箇所を改善する予定である。情報技術の発達は急速なので、ポリシーも手順も理想に近づいては遠ざかることを繰り返すと考えられる。ネットワークウイルスの登場により、一時的にウイルス対策プログラムの有効性が低下しているのかもしれない。状況の変化は今後も一層激しいと予想されるので、評価・見直しを怠ればすぐに陳腐化するし、システムを安定的に維持管理することが困難になるはずである。

今後の取り組みとして重要と思えることを下記にあげる。

(1) 情報セキュリティポリシーに則したセキュリティ教育や研修の徹底
(2) ＩＤＳ（侵入検知システム）の導入等、セキュリティを維持するために必要予算措置
(3) 中期計画・中期目標に沿った運用
(4) ポリシー遵守に関する監査の実施

なんとか第１版を作ったばかりのこの取り組みが今後発展し、本校の伝統の一部となれば幸いである。