2.1. 人間・管理・インシデントハンドリング

はじめに

大学や研究所の IT 環境において、セキュリティの確保は重要な課題である。国立大学法人等にあっては、セキュリティポリシーおよびガイドラインのひな形が示され、ポリシー策定およびポリシーに基づいたセキュリティ体制の整備が急務となっている。

一方で、インターネットのセキュリティ状況は悪化の一途をたどっている。そのような状況で、個々の利用者の日常的行動が組織のセキュリティに大きな影響を与える。情報セキュリティにおける組織や人間の在り方について検討し整理した。

セキュリティにおける人間要因

どんなに高性能なセキュリティアプライアンスやセキュリティソフトウェアを導入したとしても、その導入による安心感に満足してしまっては、効果は限定的なものになり、かえって脆弱性を作りかねない。情報セキュリティを維持するためには、情報システムを企画、運用・管理、そして利用する人間の心構えが重要である。たとえば、ファイル共有ソフトウェアで特定のファイルのダウンロードを実行することにより（たとえば Winny や BitTorrent）、自動的に著作権等を侵害する可能性のある他のファイルの配布の中継に加担してしまうことや、ウィルス対策ソフトウェアのパターンファイルに登録されるまでの時間が長いスピア攻撃（特定少数を標的とする攻撃）への対処の方法など、利用者の高いセキュリティ意識がなければ防げない。好奇心からウィルスを実行してみるなどは言語道断である。

このためには、構成員全員に情報セキュリティ教育を行う必要がある。定期的に開催する講習会や、自分のペースで進められる e-Learning システムのコンテンツでの提供が考えられる。情報セキュリティ教育は、新たな技術の習得ではなく、セキュリティ意識の啓発であるので、何らかの形での強制力を持った義務化が必要である。

セキュリティ教育の対象は構成員全員ではあるが、大学の場合、役員、教員、事務職員、学生のそれぞれの立場での対応が必要である。役員に対しては、情報システム投資の中に情報セキュリティ投資が必須なこと、教員に対しては、成績データ等の個人情報と研究情報等のそれぞれのセキュリティレベルの認識などである。

組織のセキュリティの水準は、もっとも低いレベルに制約されることになるので、セキュリティ教育に当たっては、入門教育、初級教育を重視するべきである。小中学生向け教材はそれ以外の場面でも有用である。公開されている情報セキュリティ教材について URL をスライド形式の資料中にまとめたので参考にしてほしい。JNSA のセキュリティキャラバン、ハイパーネットワーク社会研究所の情報モラルセミナー等の無料のセミナー、講習会の利用も考えられる。

セキュリティの管理

セキュリティポリシーを作成し、ガイドライン等の整備をし、PDCA サイクルを実施することは、組織のセキュリティ確保にとって重要である。しかし、セキュリティポリシーやガイドラインを策定し、体制を用意しただけでは不十分である。誰のための何のためのセキュリティポリシーであり、セキュリティ体制であるか、組織の構成員が考え行動可能なように、組織としてセキュリティ戦略を立てて日常的に行動すべきである。

セキュリティポリシーやガイドライン策定については、「高等教育機関向けセキュリティポリシーのひな形」が参考になる。

組織のセキュリティ体制や実施状況については、セキュリティ監査が不可欠である。内部監査だけでは不十分で、第三者機関による定期的な監査と問題指摘が重要である。その際に、監査の対象や期間について十分な検討が必要になる。監査に際して、監査人の資格要件や監査結果データに関する秘密保持契約についても検討が必要である。第三者監査を実施する際の仕様書例を付録 A に添付した。

監査の成果がセキュリティ状況の改善につながらないと意味がない。第三者監査とともに、組織内の部局間での相互監査やテーマを決めての近隣大学間での相互監査は、セキュリティ意識の

向上に役立つと思われる。
組織のセキュリティ体制の外部への表明として、ISMS やプライバシーマーク等の取得以外にも、組織のセキュリティ情報を審査格付けするセキュリティ格付け会社が発足し、セキュリティ格付けのトライアルを開始している。
また、ポリシーやガイドライン遵守を個々の利用者の意識に委ねる状態では不十分で、シンクライアントシステム等のミスの発生しないシステムや不正のできないセキュアなシステムの導入整備も重要である。
CSIRT（インシデントレスポンスチーム）を整備し、インシデントハンドリング体制や連絡窓口の整備が急務であるが、今後はセキュリティを日常的に戦略的に考え行動するセキュリティオペレーションズセンター（SOC）という考えも重要である。セキュリティ管理全体を BCP(Business Contingency Plan)/BCM(Business Contingency Management)の中に取り込む考えもある。

インシデントハンドリング

セキュリティマネージメントに携わっていると、一定の割合でセキュリティインシデントの発生に遭遇する。インシデントは、ウィルス感染かもしれないし、不正侵入かもしれない。またいつ発生するのかも予想できない。しばらく発生していないなと思っていると、続いて複数のインシデントが発生してんてこ舞いになることもある。マネージメントでは、いずれのインシデントに対しても一定以上の速度で対応しなければならないが、作業の優先順位を正しく決めるためのトリアージを定めておくとずいぶんと楽になる。このトリアージという言葉は、救急医療の分野で使われている用語で、Wikipedia には「最善の救命効果を得るために多数の傷病者を重症度と緊急性によって分別し、治療の優先度を決定すること」とある。
トリアージと同じくらい大切なことに、ハンドリングにおいて中心的な役割を担う PoC（Point of Contact）という連絡窓口を決めておくことがある。PoC が車輪のハブのような役目を果たし、これによりインシデントハンドリングという車輪がまわって前に進んでいける。しかし、たとえ PoC がスキルフルな人物であったとしても、PoC が一人で全てを背負い抱えてしまわないようにマネージメントでは制御していかないといけない。それにはあらかじめ、取り扱うインシデントの範囲などを定めた規則類を整備しておくのが有効である。この規則がインシデントハンドリングの基本文書となるだろう。

文書では、最初にインシデントハンドリングの対象となる組織の構成員と取り扱うインシデントの種類をはっきりさせる。次にハンドリング手順を定めておく。事後報告のための書式も定めておき、すべての局面においてインシデントに対し個別対応することをできるだけ避ける。さらにそれらがきちんとまわっていくかどうか、イメージトレーニングや演習（サイバードリル）についても文書に書き下しておくとよい。これらの準備ができていれば、組織に重大インシデントが発生した時に必ず役に立つ。ハンドリングに関する各種の情報は、JPCERT/CC のサイト（http://www.jpcert.or.jp/csirt_material/）から得られる。また、WG 活動で大学などの場合のハンドリングの手順の例を作成したので、付録 B につけた。

まとめ

セキュリティの確保にあたって、個人の倫理やスキルに負う部分が大きいことから、組織人に対して、何をどうするか、どのような対策を実施すれば有効であるかを

- セキュリティにおける人間要因
- セキュリティの管理
- インシデントハンドリング

の観点からとりまとめた。
セキュリティ体制整備の助けになれば幸いである。