情報セキュリティの現状と学校現場への警鐘

ネットワンシステムズ株式会社　セキュリティ事業推進本部長　山崎　文明
f-yamasaki@netone.co.jp

キーワード：モラル，情報セキュリティ，個人情報保護，情報漏えい

はじめに

学校セキュリティポリシーの必要性が理解された結果、セキュリティポリシーの策定済学校数は、確実に増加していると思われる。一方、ポリシーの策定過程において「現状を追認するのか」、「理想をもとめるのか」との議論は、各校に共通している。すなわち、行動規範として教職員に求める運用規則については、現場の意見集約のもとにセキュリティポリシーへ反映されるが、技術対策に関しては、新たに設備投資を伴うため、現在のＩＴ環境を前提とするのか、設備投資を前提にポリシーの策定を行うのかといった前述の議論が例外なく行われているのが実情である。情報セキュリティの確保は、行動規範を遵守するだけで実現できるものではなく、セキュリティ対策技術の実装が、不可欠である。セキュリティ水準を高めるために実装されるべき最低限の対策を示した基準の策定が求められる。

２　調査報告書に見る情報セキュリティの現状

２．１ 情報セキュリティポリシーの普及と実効性

警察庁生活安全局情報技術犯罪対策課が、東証１部、２部上場企業や店頭公開企業、通信、医療、教育、行政といったいわゆる大手企業、団体を対象に行い、昨年１月に公表した「不正アクセス対策等の実態調査（平成１９年１月）」にセキュリティポリシーの導入状況に関する調査結果がある。調査対象企業のほとんどがセキュリティポリシーを「策定済み」か「策定予定」と回答している。「策定済み」６２．０％ 、「策定中」１６．０％ 、「策定予定」１７．８％、これらを足し合わせると９５．８％もの企業が情報セキュリティに関心を示し、何らかの取り組みをしていることがわかる。一方、これら大手企業、団体からの個人情報漏洩事件・事故は、連日のように報道され、未だ終息する気配が見えない。情報漏洩事件・事故を起こした企業や団体の中にはＩＳＭＳやプライバシーマークの認証取得組織も含まれており、セキュリティポリシーの実効性や第三者認証制度の有効性に疑念が生じる。

２．２　進んでいないセキュリティ技術対策

同調査報告書には、「情報セキュリティ対策実施上の問題点」に関する経年変化についても報告されている。注目すべきは、ここ３年間変わらず、半数の企業・団体が「どこまで行えばよいのか基準が示されていない」と回答している点である。調査結果から読み取れることは、「セキュリティポリシーを策定してはみたものの、具体的に何をやれば良いのかわからない。」という実態が読み取れる。こうした実態は、現在の学校教育現場にも当てはまる。そもそもＩＳＭＳは、情報セキュリティを強化するためのマネジメントシステム、すなわち組織の仕組みとして計画、実行、監査、改善（いわゆるＰＤＣＡ）が実践されていることに対する認証制度ではあっても、客観的なセキュリティ水準を保証するものではない。その本質は、自らがリスク分析を行い、認識されるリスクを個々の企業・団体が許容しうるレベルに低減するための対策を行うという点にある。言い換えればセキュリティポリシーは、「自己責任」を原則としている。

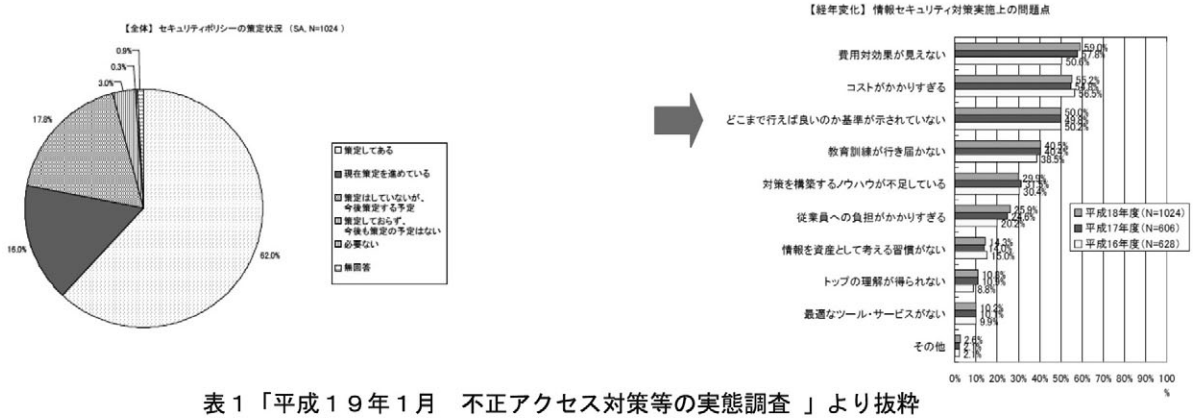

表１「平成１９年１月　不正アクセス対策等の実態調査 」より抜粋

２．３　教育現場の実態と懸念事項

一方、警察庁生活安全局生活安全企画課が２００３年に公表した「ハイテク犯罪等に係る被害状況の調査」からは、小、中、高、大学における不正アクセスの実態が見て取れる。

不正アクセスは、不正アクセス禁止法で懲役１年の刑に処せられる重罪であるにもかかわらず、過去１年間に内部からの不正アクセスがあったと回答した学校が８．３％も存在するという事実は、看過できない。同調査は、企業内における不正アクセスも対象にしているが、内部の不正アクセスがあったとする企業は６％であることから、学校内のモラルは、一般企業と比較して低いと言わざるを得ない。さらに不正アクセスに気づかない学校も多いであろうことを加味すると最優先で対策が実施される必要があると判断される。

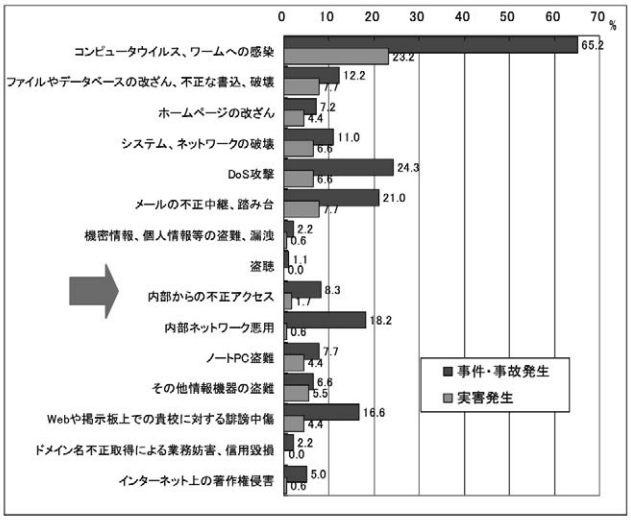

表２「平成１５年３月　ハイテク犯罪等に係る被害状況の調査」より抜粋

３．　求められる実装対策基準

３．１　学校標準実装対策基準の導入

児童・生徒の個人情報を扱う学校教育現場に求められるセキュリティ水準は、本来、各校の都合で決められるものではなく、機微な個人情報を扱う環境にふさわしい一定水準以上のセキュリティ対策を求めていく必要がある。

学校教育現場と比較してＩＴ環境や人材に恵まれていると思われる企業ですら、その半数がセキュリティポリシーを策定したしたものの、どこまでやればいいかわからないという現状は、学校教育現場に当てはめればなおさらであり、民間企業の轍を踏まないためにも、導入されるべきセキュリティ対策技術基準の策定が急務である。

３．２　参考となるクレジットカード業界のセキュリティ対策基準

民間企業でも一定水準のセキュリティを確保するためにセキュリティ対策技術基準を策定する動きがある。その一つにクレジットカード業界がその導入を推進している PCI　DSS（Payment Card Industry Data Security Standard）がある。同基準では、クレジットカード情報を保護するための１２の要求事項を定めている。さらにそれぞれの要求事項に対して詳細な基準が設けられており、導入主体の判断で実効性が左右される事態を極力排除する工夫が成されている。

安全なネットワークの構築・維持	要件 1 ： カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること 要件 2 ： システムパスワードと他のセキュリティ・パラメータにベンダー提供の初期値を使用しないこと
カード会員データの保護	要件 3 ： 保存されたカード会員データを安全に保護すること 要件 4 ： 公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
脆弱性を管理するプログラムの整備	要件 5 ： アンチウイルス・ソフトウェアを利用し、定期的に更新すること 要件 6 ： 安全性の高いシステムとアプリケーションを開発し、保守すること
強固なアクセス制御手法の導入	要件 7 ： カード会員データへのアクセスを業務上の必要範囲内に制限すること 要件 8 ： コンピュータにアクセスする利用者毎に個別の ID を割り当てること 要件 9 ： カード会員データへの物理的アクセスを制限すること
定期的なネットワークの監視およびテスト	要件 10 ： ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること 要件 11 ： セキュリティシステムおよび管理手順を定期的にテストすること
情報セキュリティポリシーの整備	要件 12 ： 情報セキュリティに関するポリシーを整備すること

表３　ＰＣＩ　ＤＳＳの１２の要求事項

４．まとめ

「カード会員情報」を「個人情報」と読み替えれば PCI　DSS の要求事項が学校教育現場にも当てはまることが理解される。個人情報は、カード会員情報と同様に秘匿されるうるものではなく、必然的に利活用されるものである。カード会員情報の不正使用の防止を目的に制定された PCI　DSS は、保護されるべき情報である個人情報の実装レベルでの対策基準としても十分活用できる基準であり、同基準を参考にして学校教育現場に求めるべき対策基準が策定されることが望まれる。

参考文献

PCI データセキュリティスタンダード（https://www.pcisecuritystandards.org/）