サイエンティフィック・システム研究会　　2016 年 1 月 18 日
システム技術分科会 2015 年度第 2 回会合

室蘭工業大学におけるセキュリティポリシー策定とその運用

刀川 眞
国立大学法人　室蘭工業大学
情報メディア教育センター

[アブストラクト]
室蘭工業大学では 2008 年に、NII などによるいわゆる「サンプル規程集」をベースに情報セキュリティポリシーを策定した。策定に際しては小規模工科系単科大学の特性を活かし、また事務部門と密接に連携して実効性重視を心がけた。その後ポリシーに基づき、講習会などの啓発活動、ウイルス対策ソフトや汎用ソフトの学内無償提供、サーバ疑似アタックや PC スキャンなどを実施し、ISMS や BCMS の国際認証取得、クラウド利用ガイドライン作成などにも取り組んでいる。一方で限られた資源の有効利用やセキュリティ活動のインセンティブ確保など、情報セキュリティ活動の本質に関わる課題も残されている。

[キーワード]
情報セキュリティポリシー，サンプル規程集、ISMS、BCMS

1.　はじめに

情報システムやネットワークが組織運営の要となりつつある現在、それらの安全かつ安定した運用は組織の永続的発展の基盤である。このことは企業などと較べ存立基盤や行動原理、ガバナンスなどで大きな違いのある大学でも同様である。しかし組織特性の違いもあり、大学における情報セキュリティのレベルは他と較べて決して満足のいくものではない。このような状況を改善し、また量的・質的に変化・増大している脅威に備えるため、バックボーンとなるセキュリティポリシーについて改めて考えるのは意義あることである。その一助になることを目指し、室蘭工業大学における情報セキュリティポリシーの策定とその後の運用・展開を提示する。

2.　セキュリティポリシーの策定

（1）基本方針

室蘭工業大学では 2008 年に、国立情報学研究所（NII）と電子情報通信学会による「高等教育機関の情報セキュリティ対策のためのサンプル規程集」（以下、サンプル規程集）をベースに情報セキュリティポリシーを策定した。策定に際しては情報ネットワーク基盤を

管理・運用している情報メディア教育センターが主になり、学内展開や事務手続き上の正当性を確保するため事務部門（企画・評価室）との共同体制を採った。周知のように「サンプル規程集」は膨大な量があり、そのままでは実用に供しにくい。そこで本学のポリシーでは形式的完全性よりも実用性を重視し、極力、コンパクトで運用性の向上を目指した。具体的には簡素化のため、次に示す方針を定めた。

・サンプル規程集では理系/文系の複数学部総合大学が前提なのに対し、本学は単科大学のため意志決定階層を減らす。
・サンプル規程集では事務部門に特化した規程も用意されているが、本学では事務部門も全学ポリシーを適用する。
・サンプル規程集でのガイドライン類（電子メール利用、ウェブブラウザ利用など）は本学利用ルール策定時の参考にはするものの、本学のポリシーにはしない。

その一方で次の方針も定めた。

・管理単位として事務局全体を一部局とはせず、実態に合わせ各課・室ごとにする。
・策定したポリシー類はすべて学長決裁による正規の規則とする。

（2）責任者

サンプル規程集では責任者として、各部局に部局総括責任者、部局技術責任者を配置している。しかし実質的にセキュリティ管理が可能なのは日常で実務的に接している範囲である。そこで、教員は個々の流儀で PC などを使いまた研究室を運営していることから、各教員を情報セキュリティ責任者とする。これに対して事務部門は組織としての活動が中心のため、課・室長に相当する者を責任者とする。なおいずれも必要に応じて情報技術担当者を配置できるものとした。

（3）意思決定機関

本学には以前から情報統括責任者(CIO)が設置されており、また学内情報基盤に関する意思決定機関として情報基盤委員会がある。情報基盤委員会は CIO を委員長とし、各学科代表の教員、事務局課長、及び情報メディア教育センターの教員から構成されている。効率化のため、情報セキュリティに関してもこの委員会で扱い、最高情報セキュリティ責任者（CISO ）は CIO が兼ねることとした。

3. セキュリティポリシーの運用と展開

策定したセキュリティポリシーに基づき、以下に示すセキュリティ強化活動を展開している。

（1）教育・講習

情報セキュリティポリシーに関連して「年度講習計画」があり、本学でもそれに基づき次のような講習を行っている。

・教職員・編入生向け基礎講習‥‥新任時、集合受講（4～5 回/年）
・学生向け基礎講習‥‥‥‥‥‥‥‥入学時、学科別集合受講（1 回/年）

・留学生向け基礎講習‥‥‥‥‥‥入学時、集合受講（2 回/年）
・教職員向け定期講習‥‥‥‥‥‥毎年、自席から PC で受講（1 回/年）
・幹部向け講習‥‥‥‥‥‥‥‥‥‥毎年、集合受講（1 回/年）
・サーバ管理者向け講習‥‥‥‥‥任命時、集合受講（随時）

（2）サーバ疑似アタック

学外に公開しているサーバに対して疑似アタックをかけ、脆弱性があれば改善勧告や指導を行う。改善されない場合は最悪、ネットワークから遮断する。本活動はサーバの脆弱性低減とともに、使用済みサーバの廃棄促進の効果もある。

（3）PC ウィルス対策ソフト等の導入促進と確認スキャン

ウィルス対策ソフトの導入促進のため、学内向けにウィルス対策ソフトの無償提供を行う。またウィルス対策ソフトの導入状況や定義ファイルの更新状況、OS の更新状況を把握するため、学内 PC に対しスキャンをかける。

（4）標的型攻撃訓練

昨今、特に問題が顕在化している標的型攻撃への取組みとして、標的型攻撃を模したメールを送信し、開封者の開封後の行動（トラップ設定）を把握し注意を喚起する。

（5）セキュリティ強化月間の取組み

学内のセキュリティ意識の向上と強化を目指し、年に 2 回、強化月間を設ける。期間中に上記活動を集中させると共に、テーマを定め（パスワード強化、標的型メール対策など）啓発ポスターの学内公募などボトムアップ型での意識高揚も図る。

（6）クラウドバックアップ

データの完全性・可用性の向上を目指し、重要データを学外クラウドにバックアップする。また学内から外部クラウドを利用する際の安全性確認のため、学外クラウド利用のガイドラインを制定する。

（7）ISMS,BCMS 国際認証取得

情報メディア教育センターは学内神経系であるネットワークインフラを提供しており、自身の情報セキュリティや事業継続性の維持・確保は大学全体にとっても極めて重要である。そこでセンターの活動状態を客観的に評価するとともに、その向上を目指し ISMS（Information Security Management System)と BCMS（Business Continuity Management System）の国際認証を取得した。

４． おわりに

これまでの経緯を振り返って見ると、策定したポリシーが実際のセキュリティ向上活動に直接・具体的に展開されることは稀である。しかしセキュリティ活動を行う上で、関係者の認識基盤を確認したり意識を合せるなど、その後の活動を展開する上での「礎」としての役割は大きい。「礎」があれば活動がぶれずに一貫性を保つことができるからである。また本学の場合、ポリシーの実質的検討は情報メディア教育センターが担ったが、正規文書

としての適切性確認やポリシーの学内周知、悪質な場合の強制力行使などの段階では事務部門の協力が欠かせない。これらをスムーズに行い、さらにその後に発生する問題や課題に対処するには両者の緊密な連携が必要である。本学ではポリシー策定の開始時点から両者は連携し、また CIO・CISO と常時、意識合わせをしていたことなどにより大枠では旨くいったと考える

一方で投入できる時間や資金など限られた資源の有効活用や、特にポリシーにより活動の制約を受けかねない教職員のモチベーション維持やインセンティブ確保は極めて大きな課題である。いくら高邁なポリシーであっても利用されなければ意味がない。他校をはじめとする学外の状況や技術進歩を常に把握することはもちろんのこと、利用の実状やセキュリティ活動の実効性なども常時確認し、絶えず適用性に配慮し続けることが肝要である。セキュリティポリシーの策定は、ゴールではなくスタートなのである。

[参考文献]

(1)国立情報学研究所ほか : 高等教育機関の情報セキュリティ対策のためのサンプル規程集、2007 年 10 月 31 日（http://www.nii.ac.jp/csi/sp/）

(2)石坂徹ほか : 単科大学における情報セキュリティポリシーの策定と運用、情報処理学会全国大会, 情報処理学会第７１回全国大会講演論文集（４）,pp.449-450, 2009 年 03 月

(3)石坂　徹ほか : 小規模大学における教職員向け情報セキュリティ教育の実践、大学情報システム環境研究、VOL.13、2010 年 3 月