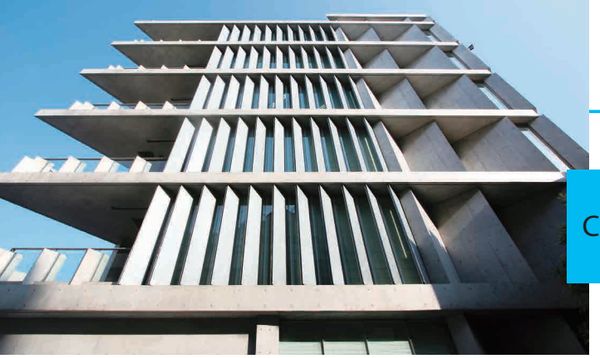


CASE 1

情報セキュリティ 大学院大学

DX時代の社会の信頼と安心を創る

DX時代の申し子

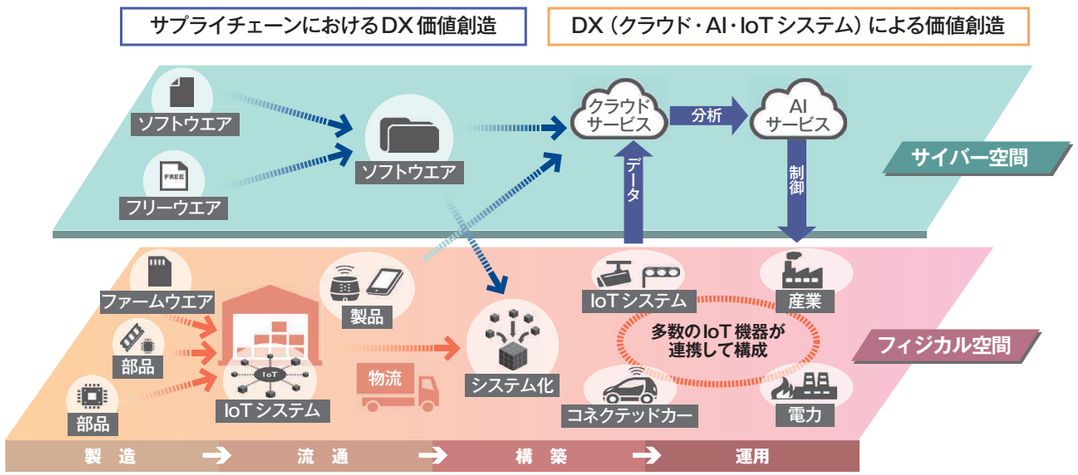
DXとはデジタル・トランスフォーメーションの略語であり、各種のデジタル技術を駆動して価値を創造することを意味している。具体的には、IoTを利用してフィジカル空間の様々なデータを収集し、それをサイバー空間上のクラウド上においてAIで分析し、その知見を人間社会をより良くすることに利用するものである。図1に見るように、フィジカル空間にサイバー空間を融合させたサイバー・フィジカル・エコシステムがそれであり、この動きは一層加速されよう。タクシーの配車アプリがその一例と聞けば、イメージは明確になる。人間が調整していたタクシーに対する需要と供給をアプリが行ってくれることで、タクシー利用者もタクシー会社も時間や手間のコストを下げることができ、ここにwin-winの関係が生じる。

後藤厚宏　学長

しかしながら、反面、DXが実現する技術は、サイバー犯罪・攻撃の恰好の対象になる。フィジカルな社会生活がグローバル化している中、サイバー空間における犯罪や攻撃は大規模化し、社会に莫大な損害を与えるというリスクがある。では、社会の利便性を高め、かつ、リスクを最小限に抑制するにはどうすべきか。これが、情報セキュリティという考え方だ。世界中で情報セキュリティ対策の重要性が謂われているものの、それに対応できる人材育成が追いついていないのが日本の現状である。

こうした中、情報セキュリティに特化した人材の育成を掲げて登場したのが、情報セキュリティ大学院大学（以下、IISEC）である。現実の情報セキュリティの問題解決を担う高度な専門技術者や実務家と、情報セキュリティの将来をリードする研究者を養成し、DXが進む中、社会の信頼と安心を創ることへの貢献をミッションとして、学校法人岩崎学園が2004年に開学した。学部を持たず、修士課程（1年制、2年制）・博士課程からなる大学院のみの大学だ。2年制の修士課程の募集人数は40名、1年制は若干名、博士課程は8名と、規模はさほど大きくはないが、まさに、DX時代の申し子として誕生した大学院大学である。

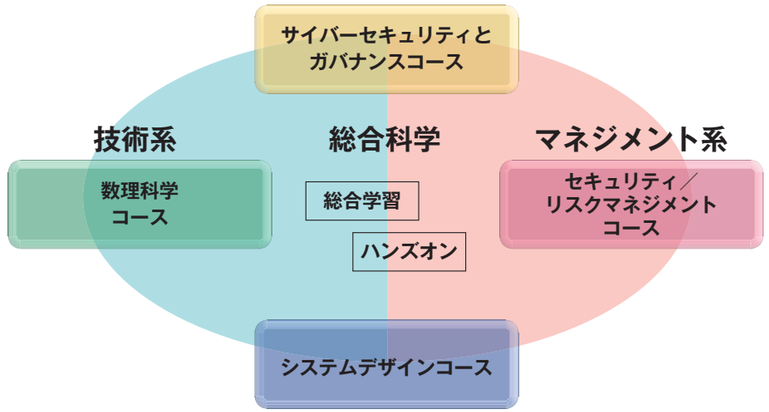
図1　DXとサイバー・フィジカル・エコシステム



情報セキュリティという学問と教育：全体と個別

情報セキュリティの必要性は社会的には高まっているが、その教育・研究をするための情報セキュリティ学という学問体系が確立しているかと問われれば、多くの者は首を傾げよう。では、IISECはどのように情報セキュリティの教育・研究を行っているのだろう。後藤厚宏学長は、その経緯について次のように話す。「一般的に言われるサイバーセキュリティとは、文字通り、あくまでもサイバー空間の問題でありインターネットを使用するうえでのセキュリティを考えればよかったのですが、今では、フィジカル空間も含め社会全体のセキュリティという視点が不可欠です。こうなると情報工学をベースにしたいわゆる理系の学問に依拠するだけではだめで、例えば、社会のルールを考える法学、組織のマネジメントを考える経営学、人間の心理を考える心理学等文系の学問も含めた文理融合の総合科学として、情報セキュリティの教育・研究を考えることが必要になります。この考え方が開学当初から本学の柱でしたが、社会生活における情報セキュリティが扱う対象の拡大とともに、多様な学問領域からのアプローチがますます重要になってきました」。情報セキュリティの教育・研究とは、1つのディシプリン（学問体系）を構築し、その精緻化を目的とするというよりは、ある課題に対して多様なディシプリンからアプローチすることで解決を目指すというタイプに属すると言ってよい。

図2　4つのモデルコース



いわば、モード論でいうところのモード2型の学問であるが、それが教育プログラムにおいてどのような工夫となって表れているかを見よう。キーワードは、全体の把握と個別の深化である。まず、解くべき課題がどの範囲に拡がっているかという全体を把握する視点を持たねばならない。そのうえで、どの部分を深化させるかを決めてアプローチするのである。図2の博士前期課程の教育プログラムは、全体を把握する「総合学習」と「ハンズオン」、個別の深化のための4つのモデルコースからなる。

「総合学習」では必修科目が2科目あり、1科目は、情報セキュリティに関する最新情報を習得するための各界の専門家のリレー講義、もう1科目は、全教員・学生が参加しての、学生の研究発表である。「ハンズオン」は、演習であるが、ここで多様な技術力・実践力を高める。こうした中で情報セキュリティの全貌を把握する視点を涵養する。

情報セキュリティが多様な学問からのアプローチを必要とするため、それを大きく4つの領域に分け、それらを軸として専門性を深めるのである。「サイバーセキュリティとガバナンス」では、サイバーセキュリティの先端技術と、攻撃への対処に必要な法体系の学習が中心、「セキュリティ／リスクマネジメント」では、経済学、経営学、心理学等を応用してリスク回避・管理を学ぶ。「システム

デザイン」では、情報工学を中心にしたシステム技術の学習に特化しており、「数理科学」では、暗号、アルゴリズム、統計等の数理科学からなるプログラムが編成されている。全体の把握と個別の深化がバランス良く配置されている。

これらのコースワークを統合するのが、修士論文である。これが学生の成長に果たす役割は大きいと学長は強調する。自らの研究テーマを定め、自分で問いを立て、自力で分析して結論を出すという、修士論文執筆のプロセスを経ることで、学生は与えられたことを学習するという姿勢から、自分で学んで解決する姿勢へと変化するそうだ。確かに、実務の世界は課題を定めそれを自力で解決することの日々である。従って、修士論文とは「研究」を通じて実務で求められる資質や能力を獲得できる仕掛けなのだ。

学問と現場を繋ぐ

“学生が、ここでの教育・研究を現場に持って帰ることができる”。これが教育のモットーである。後述するが、学生の多くは社会人であり、何らかの形で情報セキュリティに関わる仕事をしている者が多い。そうした学生のニーズは、まずもって、実践的な技術力、課題解決力を高めることにある。前述のフォーマルなカリキュラム以外にも、それを可能とする工夫を各所に見ることができる。

その1つが教員構成である。10人の専任教員、16人の兼任教員の大半が、大学以外の民間企業等での職務経験がある。兼任教員は、大学教員等の研究者以外に、企業の経営層、エンジニア、ジャーナリスト、起業家、弁護士といった多彩な顔ぶれから構成されている。また、IISECでは、連携教授、アドバイザリーボードという制度を設けており、前者は大学内外の情報セキュリティの最先端の研究者14人で構成され、研究会や特別講義等を通じて教育・研究のサポートをする役割、後者は情報セキュリティに関連する産業界や学界のトップ層23人を据え、大学が今後進むべき方向についてアドバイスする役割を依頼している。

このユニークな教員構成によって、学問と現場を繋ぐことができ、学生のニーズに応える教育ができるのだろう。後藤学長は、「情報セキュリティに知悉している方に対する需要は高まっており、皆さん引っ張りだこです。これだけの第一線の教員をリクルートすることは、実は大変です。とりわけ、連携教授、アドバイザリーボードのメンバーは、ご本務もあってご多忙な中、本当に熱心に教育・研究に力を注いで下さり、ありがたい限りです」と言う。

もう1つは、文部科学省の競争的資金を得て、他大学と連携した情報セキュリティ人材の育成を行っていることである。現在2つのプログラムがある。第1は、「先導的ITスペシャリスト育成推進プログラム」に採択されて2008年から開始しているISSスクエアであり、参加者にはサーティフィケートが付与される。IISEC、中央大学、国立情報学研究所に11社の企業・研究機関が加わり、研究と実務とを融合することで先端的な情報セキュリティ人材の育成を目指している。具体的には、サブゼミ的な研究分科会・ワークショップ・インターンシップ・見学会・他大学の学生との交流等が行われ、学生に対しては第2の専門として履修を推奨している。学生の人気は高く、これまで200名以上が参加しているという。

第2は、「情報技術人材育成のための実践教育ネットワーク事業」に採択されて、2013年からスタートしているenPiT-Securityである。IISEC、東北大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学の5大学が連携し、産業界が求める実践的な情報セキュリティ人材の育成のためのコースを提供するプログラムである。

これら競争的資金への採択とは、IISECの16年余に渡る学問と現場を繋ぐことに一貫してきた教育・研究が、情報セキュリティ対策を求め人材育成が急がれるようになった近年の時代の要請に、うまくマッチした結果ということができよう。

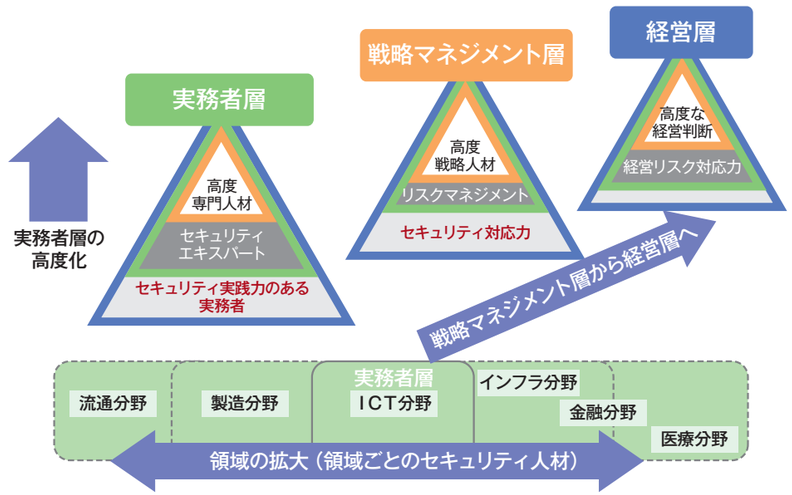
情報セキュリティに関する梁山泊を目指して

では、そのメリットが開花しているかと言えば、そうとも言い切れない。というのは、必ずしも志願者が増えないからである。どのような学生が学んでいるのか、学生のプロフィールを見てみよう。学生の80%は社会人であり、そのうち20%は既に修士号を持つ高学歴集団である。業種を見れば、2018年10月と2019年4月入学者41名のうち、情報サービス9名、官公庁9名、情報通信5名と続き、それ以外は、メーカー、金融・保険、専門サービス、自営等と極めて多岐にわたる。年代では20歳代16名、30歳代14名が最多であり、何らかの形で情報セキュリティと関わる仕事をしている者が多いが、学部時代の専門は必ずしも情報系ではない。これに対しては、科目内容や履修方法に関する工夫があるため、学部の専門との関連がないことは不利にはならないという。

興味深いのは、毎年60～70%が企業からの派遣であることだ。派遣が多数を占めているということは、企業からその実績が認められてのことであり、しかも社会的要請は高まっているため、志願者は増加傾向にあると想定できる。しかし、40名の定員はかろうじて埋まっている状況が続いており、決して安泰ではないという。情報セキュリティ対策は認知されるようになっても、その課題に対処する高度人材を育成する場があることに関しての認知度は低い。また、日本企業が全体として、社員の大学院での再学習に消極的な風潮が強いことの影響は大きい。

そこで、現在新たなターゲットとしてその獲得を目指しているのが、企業の経営層である（図3）。それは、単に新規の学生マーケットを開拓するというだけではない。情報セキュリティという問題が、冒頭に示したようにサイバー空間とフィジカル空間の融合の中で生じること、そこでのリスクが人間社会や企業組織に与える影響が大きいことを考えると、スペシャリストである技術者や実務家の域を超えて、企業の経営層が状況を見極めて判断することが重要になってくるからである。とはいえ、そうした職位にある者が修士号取得を目指して2年間を割くことは、実際問題としては困難である。しかし、短期集中コースであれば、多忙な経営層も時間を当てることができよう。

図3　実務者層・戦略マネジメント層から経営層へ



これらの層の間に情報セキュリティの重要性の認知が高まれば、社会的リスクを下げることに繋がるうえ、社員の大学院での再教育や企業内研修についての需要が見込めるかもしれない。現在、前述のenPiTプログラムの中に、enPiT-Proとして60時間～120時間の履修証明プログラムを開始しており、また、企業向けの2～6日間の短期研修コースを設けている。これらの打って出る試みは、当該大学の成否だけでなく、今後の日本社会が情報セキュリティをどう考えていくかの試金石のようにも思う。

OB・OGとの連携を強化することも重要である。幸いにもOB・OG会は盛んであり、業種を超えたネットワークができており、業界を超えて仕事の相談や情報交換をする場となっているが、それが大学を支える一翼となることも期待されている。

IISECに関わる多様な人が多様な形で大学を利用し、新たに人を呼び込む場とするといった構想が目に浮かぶ。「情報セキュリティに関する梁山泊を目指すというのが、先代の学長からの構想です」と後藤学長は語られる。この夢の実現は、そう遠くはないように思う。

（吉田 文 早稲田大学教育・総合科学学術院教授）

▶カレッジマネジメントTOPページへ戻る