

高度なサイバーセキュリティ人材の育成を目指す

「サイバーセキュリティ特別専門学修プログラム」

日本で高度なサイバーセキュリティ人材を育成するため、東京工業大学では「サイバーセキュリティ特別専門学修プログラム」を展開している。その特色について、東京工業大学情報理工学研究所サイバーセキュリティ研究センター長の田中圭介教授に聞いた。



東京工業大学情報理工学研究所サイバーセキュリティ研究センター長 田中圭介教授

いまやサイバーセキュリティは政府だけでなく、民間企業にとってもますます重要なものになっているが、サイバーセキュリティに必要なのはネットワークのことで、ハードウェアに熟知するだけでなく、従業員のマネジメント力の養成といったところにまでおよぶのだ。そのため、日本にはそれらを網羅した教育カリキュラムがほとんどなく、サイバーセキュリティ人材が不足しているという。

そこで2016年4月に東京工業大学は、野村総合研究所、楽天、NTT、産業技術総合研究所、内閣サイバーセキュリティセンターと協力して「サイバーセキュリティ特別専門学修プ

ログラム」を立ち上げた。東京工業大学情報理工学研究所サイバーセキュリティ研究センター長の田中圭介教授によると「大学院生を対象とした副専攻相当のもので、サイバーセキュリティ概論、サイバーセキュリティ暗号理論、サイバーセキュリティガバナンス、サイバーセキュリティ攻撃・防御第一、サイバーセキュリティ攻撃・防御第二、サイバーセキュリティ攻撃・防御第三の6科目を中心とする特別専門学修科目から構成されており、サイバーセキュリティに関する理論と実践の両面から学ぶことができる」と話す。

講師陣は野村総合研究所や楽天、NTT、産総研などから派遣されているが、そのほか、東京工業大学の情報処理担当の教員も含まれているという。「サイバーセキュリティの現場のことを学べるだけでなく、攻撃内容を含めたデータを活用し、研究に生かすこともできるのが特

徴だ」と田中教授。さらに、このプログラムには補助金に依存していないという特徴もある。「サイバーセキュリティ関連の講座の多くは補助金に依存しているが、このプログラムは補助金に依存していないので、持続的かつ長期的な視点でサイバーセキュリティ人材の育成に取り組むことができる」という。

では、このプログラムを履修した学生たちにはどのような活躍の場があるのだろうか。その点について、田中教授は「企業や組織において、経営陣と情報システム部門をつなぎながらサイバーセキュリティを担う人材になることが期待される。また、サイバーセキュリティの内容は企業や組織の規模によって大きく異なるので、それぞれに合わせた対策を講じるコンサルタントのような役割を担うこともできる」と田中教授。さらに「これからはハードウェアやソフトウェアの設計時にサイバーセキュリティの概念を組み込んでおくことが重要になるので、開発部門のなかでも活躍の場が増えてくるはずだ」と予測する。

が、進化の激しいサイバー攻撃に一朝一夕で対応するのは難しい。四国・高知のあるテレビ局のセキュリティ担当者によれば、サイバー攻撃は月平均1万回にも上るといふ。当面、こういった攻撃に対応するにはケイスイケースではなく、いったん攻撃を受け入れてから処理していくという手法を採用することも必要ではないか。

ともあれ、「真の意味で役立つサイバーセキュリティとするには、そういった処方箋を学ぶだけでなく、経営学をはじめとした文系の知識も必要になる。プログラムの充実をはかり、さらに社会に求められるものにしていきたい」と田中教授。はたとされる人材が十分に配置される日はいつか、待ち遠しい。

仕事をする以上、添付ファイルを開かざるをえない...

ウイルスを完全隔離

※ 添付ファイルを開く時の不安はこれで解消!! 従来とは全く異なる発想のセキュリティツール



米国連邦政府機関をはじめ 世界と日本の重要な公的機関・有名企業を含む 400社以上が Bromium を導入しています

※2013年以降、Bromiumは累計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(米国Bromium社調べ)
詳細は【BROAD Security Square】で <https://bs-square.jp/columbus>

株式会社ブロード 〒100-0014 東京都千代田区永田町1-11-30 サウスヒル永田町7F
TEL: 03-6205-7463 (代表)

