特集　社会人の学び直しDX化 ～大学でのリカレント教育の積極化とオンライン化～

国際化サイバーセキュリティ学特別コースCySec

東京電機大学
未来科学部教授　寺田　真敏

1．はじめに

本学では、大学として、大学院生だけではなく、多くの社会人が最先端の国際的サイバーセキュリティ学を習得し、高度な情報セキュリティ能力を有する人材としてステップアップし、国際的にも活躍することを可能とすべきという考えに基づき、2014年、国際化サイバーセキュリティ学特別コースCySec[1]を立ち上げました。さらに、2016年、学部生を対象としたセキュリティ人材育成を進める「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」[2]を開始することにより、学部生、大学院生、社会人を対象とした基礎から応用までの体系的に学べる場を整備してきたという状況にあります（図１）。

本稿では、CySecの概要と、新型コロナウィルス感染症対策に伴うオンライン対応での取組みを紹介したいと思います。

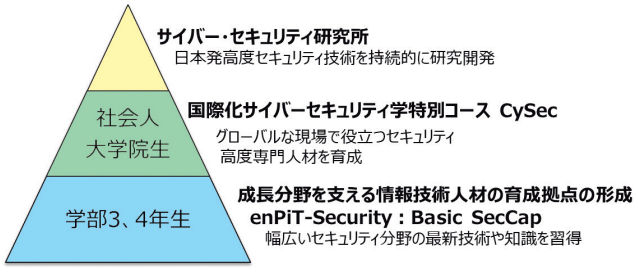

図１　運営体制

2．CySecの特徴

本学において、CySecは大学院未来科学研究科に設置、CySec科目は未来科学研究科の科目として開講することで、他研究科の大学院生、社会人も履修できるよう研究科の壁を超えた学際的な開講形態をとっています。ここでは、ユニークな点を多数有するCySecについて説明します。

（1）実務・実践を意識した幅広い開講科目

開講科目は、体系的に学べるよう、国際的な情報セキュリティ・プロフェッショナル認定資格であるCISSP（Certified Information Systems Security Professional）[3]の共通知識体系を基本とした科目のほか、攻撃者の意図や行動を「洞察する」科目、法律・倫理など制度的枠組みを「理解する」科目など、１年間の受講期間で前期４科目／後期３科目、合計７科目で構成されています（表１）。また、講義も座学だけではなく、受講者がチームを組みディスカッションによって課題を解決していく形式や、ハンズオンなどの演習形式を組み込んでいます。各科目は、学術的知見を有する大学教員による理論的・体系的な教育と、第一線でセキュリティ対策を行う企業等からの講師との協働体制で運営しています。

表１　開講科目

（1）　サイバーセキュリティ基盤（1PF1Ⅰ、1PFⅡ）
　基本的な内容を網羅的かつ系統的に学習するとともに、最新事例をケーススタディで学び、セキュアな情報システム構築の知識と基礎を養う。

（2）　サイバーディフェンス実践演習（2CD）
　ネットワークやセキュアプロトコル、公開鍵暗号基盤などについて演習を通し学び、不正アクセス、トラフィック増幅、マルウェアなどの各種サイバー攻撃とその対応について、演習を中心として学習する。

（3）　セキュリティインテリジェンスと心理・倫理・法（3IN）
　インシデントの犯罪心理学、行動心理学を学ぶとともに、関連する法規について事例を通して学習し、最高情報セキュリティ責任者CISOに必要な基礎知識を習得する。

（4）　デジタル・フォレンジック（4DF）
　インシデント発生時に適切に対応できるように、捜査や刑事・民事裁判に必要な証拠を、情報処理技術を用いて明らかにする技術や学問であるデジタル・フォレンジックの考え方や基本技術を習得する。

（5）　情報セキュリティマネジメントとガバナンス（5MG）
　情報セキュリティの計画、設計・導入、運用・保守、見直しのPDCAサイクルを実施する方法論である情報セキュリティマネジメントシステムを中心としてケーススタディで実践的に学ぶ。

（6）　セキュアシステム設計・開発（6DD）
　セキュアなシステム設計・開発、脆弱性検査とその対策について、演習を通して体得する。

（2）社会人による社会人のための講座

受講人数は、人的ネットワークの構築にも資するよう各年度、社会人枠として前期40名・後期15名を募集し、顔が見える人数としています。受講者は、専門のエンジニア、一般企業のIT部門、法務担当など様々なキャリアの方が参加しているだけではなく、所属元の業種も多岐に亘っています。また、年齢構成も20代から50代までと幅広いことから、多様な視点でサイバーセキュリティを捉えることができる機会となります。さらに、第一線でセキュリティ対策を行う企業等からの講師陣約50名との協働によって運営することで、講義においては、講師の経験をもとにした話を聞けるだけではなく、質疑応答においても、実務・実践を意識した意見交換が行われています。この点では、社会人による社会人のための講座とも言え、受講者だけではなく、講師自身にとっても学びの場として活用して頂いています。

（3）enPiT、CySec効果

本学においては、情報セキュリティに関して、学部生はenPiT、大学院生はCySecと、学部大学院連携カリキュラムとしての役割を果たしています。enPiTのセキュリティ分野については、enPiT-Security連携校として、本学以外にも13大学が参加しています。これは、同学年の他大学の学部生と共に、講義、演習を共にすることで、コミュニケーション機会が増えるだけではなく、異なる視点や意見に触れることでもあり、良い刺激になっています。CySecについては、大学院生が学外の社会人と講義、演習を共にすることで、情報セキュリティに関して、実践的で現場感のある講義に触れる機会となり、既存の授業を補完する役割を果たしています。

（4）履修証明制度

CySecでは、学校教育法に基づく履修証明制度により、修了者には、「国際化サイバーセキュリティ学特別コース 履修証明書」を授与しています。成績評価は、各科目での最終試験で成績評価をしています。講義中心科目では、論述式試験によって、総合的な理解度を測り、演習中心科目では、総合的な演習課題を与え、その達成度によって評価をします。いずれも概ね、６割以上の理解・達成をもって合格としています。修了要件は受講開始から４年以内に７科目160.8時間をすべて修めた者について、本コースの修了とし、履修証明書の授与となります。

（5）(ISC)²教育機関向けプログラムの活用

CySecの科目構成におけるユニークな点のひとつに、国際的な情報セキュリティ・プロフェッショナル認定資格CISSPの取得を視野に入れたところにあります。米国などでは企業間取引にCISSP保有者の設置を求められる場合があります。国内でも、サイバーセキュリティ事案（以降、インシデント）が発生した際に対処するための体制構築に取組む動きが広まると共に、CISSPなどのセキュリティ資格を持つ人材が体制の中心的な役割を担っています。今後、グルーバルな現場で活躍していくためには、セキュリティ資格が必要不可欠になっていくことを踏まえて、CISSPの認定機関である（ISC)²（International Information Systems Security Certification Consortium）が提供するCISSP認定資格取得のための教育機関向けプログラムIAP（International Academic Program)[4]を活用しています。CySecでは、サイバーセキュリティ基盤（1PF1Ⅰ、1PFⅡ）の２科目が、国内で唯一のIAPのCISSPコースとなっています。

3．オンライン講義を利用した小さなチャレンジ

2020年以降、新型コロナウィルス感染症対策に伴い、演習の一部をオンデマンド講義とすることを除いて、リアルタイムオンライン講義を主体とした講義形態としました。

ここでは、オンライン講義により受講のための移動時間がゼロとなったことを利用した取組みについて紹介します。それは、帰宅移動時間を有効活用したコミュニケーション不足の解消です。この取組みは、金曜５時限目（18：00～19：40）に開講しているサイバーセキュリティ基盤（1PF1Ⅰ）の１科目だけですが、講師の協力を得て、講義終了後の10分～20分を使って講師と意見交換しようというものです。次ページ表２は、2020年度の初回講義終了後に、受講者への連絡掲示板に投稿した開催説明の記事です。もちろん、講義終了後ですので任意参加という形態です。す

べての日程を通じて、講義終了時刻になると一定数が離席しますが、意見交換にはおおよそ３割～６割の受講生が参加するという結果でした（図２）。

表２　意見交換に関する開催説明

件名：トピックについて講師と意見交換しよう
1PFⅠの初回の講義に参加された方は、おおよそ雰囲気は分かるかと思いますが、講義の最後10分（19：30-19：40）あるいは、講義の終わった後の10分（19：40-19：50）くらい、講師をいれて意見交換するという場を作りたいと思います。講師側からの一方的なものというのではなく、意見交換のトピックを提案する、意見交換の場で発言するなど、受講生の皆さんにも積極的に参加して頂ければと思います。 つきましては、受講生の皆さんからトピックを募集します。もちろん、そのトピックについて、語りたい！ということもウェルカムです。「トピックについて講師と意見交換しよう」で、こんな話を聞いてみたい、こんな話をしてみたい、ということを投稿ください。

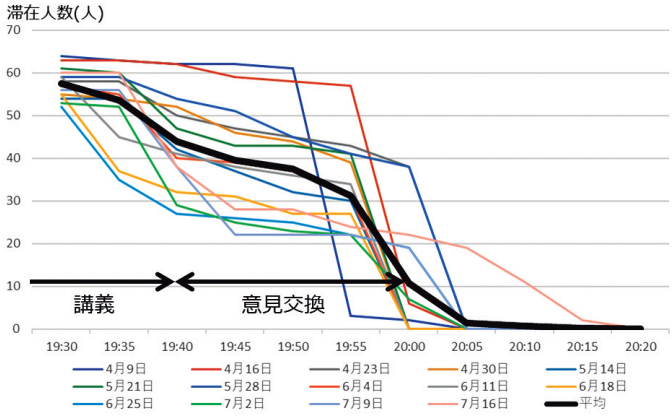

図２　講義終了前後の滞在人数推移（2021）

意見交換の場の雰囲気は、2020年度と2021年度に大きな違いはありませんが、取上げるトピックの分野や意見交換の進め方には、年度毎に多少の違いがでてきました。トピックの分野については、2020年度はオンライン化初年度ということもあり、VPN（Virtual Private Network）機能のセキュリティ問題やリモートワークなど、2021年度は講義の内容や職場で感じているサイバーセキュリティに関する問題意識などが取上げられました。進め方については、2020年度は講師同士の会話に受講者が相乗りする形態でしたが、2021年度はオンラインツールのチャット活用だけではなく、受講者からの積極的な発言を通して進められました。

社会人を対象とした「リカレント教育」におけるオンライン講義は、受講のための移動時間をゼロにできること、講義を録画できること、そして、CySec受講者にとっては、サイバーセキュリティ対策について意見を聞くことができる場としての意義は大きいようです。これは、受講者の声からも読み取ることができます（表３）。

表３　受講者の声

項目	内容
オンライン講義について	● 業務後すぐにオンラインで参加できるのが助かりました。 ● コロナの影響でリモートでの授業となりましたが、移動時間がなくなったため、早退する必要がなくなったのはとてもありがたかったです！ ● 過去の講義の録画も再度チェックできるのは後から復習するのに役立ちとてもありがたかったです。 ● 録画を何度も見直せたのがよかったです。 ● リモート開催、録画を公開してくださるおかげで気軽に勉強することができたので助かりました。
意見交換について	● 授業と授業後の雑談どちらも大変勉強になりました。 ● 実務に則した内容だった事は勿論、講義後の雑談の時間が非常に有意義でした(講義と直接関係ない質問を行える)。

４．おわりに

大学院生にとってのCySecは、「セキュリティを知っている○○分野のエキスパート」になるためのキッカケを提供する場です。大学院生が学外の社会人と講義、演習を共にすることで得られる実践的な現場感を「リカレント教育」の副次的な効果として活用していきたいと考えています。

「リカレント教育」としてのCySecは、社会人を対象に、サイバーセキュリティに関して、そのキャリアアップに必要な高度かつ専門的な知識・能力を修得するための場です。サイバーセキュリティの経験値を講師から受講生という次世代に伝える場としても活用していきたいと考えています。

参考文献および関連URL

[1] 国際化サイバーセキュリティ学特別コースCySec. https://cysec.dendai.ac.jp/, (参照2021-08-11)
[2] [文部科学省] 成長分野を支える情報技術人材の育成拠点の形成（enPiT) enPiT-Security (Basic SecCap). https://www.enpit.jp/, (参照2021-08-11)
[3] (ISC)² Japan. CISSPとは. https://japan.isc2.org/cissp_about.html, (参照2021-08-11)
[4] (ISC)² International Academic Program. https://www.isc2.org/IAP, (参照2021-08-11)