平成 28 年度
国際化サイバーセキュリティ学特別コース
設立プログラム

委託業務成果報告書

平成 29 年 5 月 30 日

学校法人東京電機大学

目次

第 1 章

国際化サイバーセキュリティ学特別コースの概要

1.1　サイバーセキュリティ分野の成長性

1.1.1　時代背景

当該サイバーセキュリティ分野に関し、平成 25 年 6 月 25 日内閣官房情報セキュリティセンター、情報セキュリティ政策会議にて「サイバーセキュリティ戦略」が出された。その内容をまとめると、情報セキュリティを取り巻く環境変化は、極めて急速である。リスクは甚大化し、拡散し、グローバルレベルのものとなった。国家や重要インフラに対する「サイバー攻撃」が現実のものとなり、「国家安全保障」や「危機管理」上の課題となっている、国家や重要インフラの防護に最善の措置の導入が不可欠となっているという指摘となる。

さらにいまや Internet of Things: IoT と呼ばれる、あらゆるものがインターネットに接続される時代を迎えている。あらゆるものが情報セキュリティ上のリスクを抱える時代となってきた。また、インターネットに接続されない制御システムにおいても、同様にリスクが高まっている。すなわち、国民生活のあらゆる側面において、情報セキュリティ対策が不可欠の時代となった。情報セキュリティは「国民生活の安定」や「経済発展」に直結する課題となっている。

我が国は「世界最先端の IT 国家」の構築に取り組んでいる。世界最先端の IT 国家には、それにふさわしい「安全なサイバー空間」を実現しなければならない。急速に変化する環境の中で安全なサイバー空間を構築するには、これまで同様個々の主体における情報セキュリティの確保が不可欠であると同時に、サイバー空間にかかわるあらゆる主体の貢献が必要となっている。

このように、従来の「情報セキュリティ」確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢の明確化が求められている。さらに「世界を率先する強靭で活力あるサイバー空間」を有する「サイバーセキュリティ立国」が速やかに実現されることが期待されている。

1.1.2　サイバーセキュリティ人材育成の必要性と課題

我が国のあらゆる活動がサイバー空間に依存している状況においては、政府機関や企業等の対策実施主体が自らの組織を守るために対策を講じる人材を育成するだけでは、深刻化するリスクへの対応が困難となっている。従って、サイバー空間の拡大・浸透に伴う情報通信技術の利活用の広がりにより、高度かつ国際的な高度サイバーセキュリティ人材の裾野を広げていくことが必要である。

現在、国内における情報セキュリティに従事する技術者は、約 26.5 万人といわれているが、潜在的には約 8 万人のセキュリティ人材が不足している状態となっている。また、約 26.5 万人中、必要なスキルを満たしていると考えられる人材は 10.5 万人強であり、残りの 16 万人あまりの人材に対しては更に何らかの教育やトレーニングを行う必要があると考えられている。

従来の情報通信技術の利活用におけるセキュリティ人材不足に対応していくことが必要であることに加え、サイバー空間の拡大・浸透に伴う情報通信技術の利活用の広がりにより、新たな課題に対応しなければならない。セキュリティ人材も今後ますます不足してくると考えられ、人材の発掘、育成、活用を進めることは喫緊の実現課題である。

人材の量的不足の解消に向け積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題である。人材の確保に関しては、ソフトウェア関連分野における独創的なアイデアや技術、これらを活用する能力を有する優れた個人を発掘育成するための合宿研修や、情報セキュリティ人材が実践的技能を競うコンテスト等を産官学で連携し実施する必要がある。

我が国におけるサイバーセキュリティ従事者の能力の底上げと、突出した人材の発掘・育成を図っていくためには、社会全体で育成し活用するための仕組みが必要である。具体的には、情報セキュリティ人材と言っても多種多様であり、その求められるスキルは対象となる人材の属性によっても大きく異なることから、スキル標準の改善・活用を通じ、必要とされる能力・知識を明確化していく必要がある。

その上で、スキル標準を活用し、実践的な教育プログラム等に関する大学等専門教育課程の充実化、産学連携の強化や、公的資格・能力評価の改善や新設の必要性も含め、セキュリティレベルに対応した多様な資格・能力評価制度の在り方など、情報セキュリティ人材として求められるニーズに応える必要がある。

グローバルに活躍できる国際性を持つサイバーセキュリティ専門家を育成等することも重要である。このため、サイバーセキュリティ専門家を志望する人々を、国際会議への参加や海外の専門大学院等への留学を支援するとともに、国内における国際会議の招致や開催を推進することも重要である。

人材の発掘・育成を、採用・活用につなげていくことも必要である。そのため、政府機関が率先して、情報セキュリティ人材の登用を行うことが望まれる。

以上述べてきた状況を鑑みると、我が国におけるサイバーセキュリティ従事者の能力の底上げ

と、突出したサイバーセキュリティ高度専門家の発掘・育成を図っていくためには、社会全体で育成し活用するための仕組みが必要である。

しかし現在では残念ながら、実務に直結した実践的なサイバーセキュリティ専門家の育成のための、4 年制大学が提供する専門的かつ体系的な教育プログラムは、国内には存在しない。このため、サイバーセキュリティ専門家を必要とする国内企業は、育成のためには海外専門機関への派遣を必要とする現状がある。

本提案プログラムはこのような現状を解消するため、多くの有能な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ることを目的としている。

1.1.3 女性の活躍が期待される分野

情報セキュリティの運用においては、技術的施策の頑強性だけでなく、異常の察知や PDCA サイクル等による改善を「人」が「継続性」をもって行うことが極めて重要である。その実現のためには、様々な能力やバックグラウンドをもつ多様な人材の育成・活用が必須であり、ともあれば男性に偏りがちな従来的「理工系」教育では十分な成果を得ることができない。国際的な状況をみても、グローバルに活躍するホワイトハッカーは性別に関係なく現れており、その意味でも男性に偏した技術職人材の分布を是正し、特に女性の優れた人材の発掘を行うことが有益でありかつ急務でもある。日本企業においても優秀な女性情報セキュリティエンジニアや CISO が活躍できるような環境の整備が必須である。

内閣府男女共同参画局が平成 23 年 5 月に「第 12 分野 科学技術・学術分野における男女共同参画」で示しているように、科学技術・学術は、我が国及び人類社会の将来にわたる発展のための基盤であり、「知」の獲得をめぐる国際的な競争が激化している。我が国が国際競争力を維持・強化し、多様な視点や発想を取り入れた研究活動を活性化するためには、女性研究者の能力を最大限に発揮できるような環境を整備し、その活躍を促進していくことが不可欠である。

1.1.4 本プログラムの特色

以上述べてきたように、サイバーセキュリティ（以下 CyS）のより一層の充実は、社会を安心・安全・豊かにするための喫緊の課題であり、本プロジェクトではこの課題解決に取り組んでいる。

本プログラムは、社会構成員全員の CyS 意識の高揚を先導する、高度 CyS 専門家を養成することを目的とする。本プログラムの特色は、CyS 技術領域だけでなく法律・経済・外交・心理・倫理等の分野の教育を行い、経営・運用・折衝・監査等も先導可能な高度 CyS 専門家の養成をめざすことである。社会活動に参加する人々の CyS 意識を高めるために子育て層も学びやすい環境を整えた上で、CyS の最先端を維持するために世界状況を常に視野にいれるプログラムを提供するものである。

1.2　プログラムの目的と修得すべき能力

情報セキュリティ人材は産業界から今まさにもっとも強く求められる人材である。その人材像としては、単に情報セキュリティを知っているだけではなく、指導的立場で先導的に情報セキュリティ対策等を推進することができる者が求められている。本プログラムでは、企業において CISO（最高情報セキュリティ責任者）、または上級セキュリティエンジニアを目指す受講者が、履修証明プログラムとして取得することを想定している。

指導的立場で先導的に情報セキュリティ対策等を推進することができる能力を修得すべく、本プログラムでは、企業において CISO（最高情報セキュリティ責任者）または上級セキュリティエンジニアを目指す者を、受講者として想定している。特に受講者としては、30 歳代のセキュリティ従事者、40 歳代の CISO 補佐（エンジニア系、マネジメント系）等の学び直し受講者を想定している。

CISO 補佐には、CISO に必要な総合的な知識の獲得が重要となる。エンジニア系 CISO 補佐には、法やマネジメントに関する知識を強化することが必要であり、マネジメント系 CISO 補佐には、インシデント対応やフォレンジックなどの技術的知識を獲得させる必要がある。また、CISO 補佐や上級セキュリティエンジニアへのステップアップを目指す、セキュリティ従事者に対しては、最新の事例や動向、技術を学ぶとともに、関連する法や倫理についての知識を深めることが求められる。

CISO、上級セキュリティエンジニアの共通知識として、情報セキュリティの基礎的知識の向上を目指し、CISSP に基づいたセキュリティ核技術の知識を修得させる。

CISO に求められる能力として、マネジメント能力とガバナンス能力がある。情報セキュリティマネジメントの国際標準を正しく理解するとともに、 ケーススタディによる実践から、ISMS の継続維持を可能とする能力を修得させる。

上級セキュリティエンジニアのための能力として、現代社会には欠かせない通信・ネットワークのセキュアな構築・運用法を修得させるとともに、ネットワークを用いた各種の攻撃について、その内容を理解するとともに、適切な対策を選択・実施するための能力を演習から修得させる。また、セキュアシステムの設計方法、分析手法を学び、実践する能力を修得させる。さらに、セキュアプログラミングと脆弱性検査手法を学ぶことで、システムの脆弱性に対して適切な対策を行える能力を修得させる。

これら知識および能力を修得することで、CISO または上級セキュリティエンジニアとして、キャリアアップおよび企業内での情報セキュリティにおける中核的先導的立場での活躍が期待される。

受講者が修得すべき能力として、情報セキュリティに関する法知識、マネジメント能力とガバナンス能力、インシデント対応やフォレンジックなどの技術的知識が挙げられる。

この能力を修得するために,「サイバーセキュリティ基盤」「サイバーディフェンス実践演習」「セキュリティインテリジェンスと心理・倫理・法」「デジタル・フォレンジック」「情報セキュリティ

マネジメントとガバナンス」「セキュアシステム設計・開発」の 6 科目を開講する。授業を担当する講師は第一線のセキュリティ研究を行っている東京電機大学教員の他に、海外も含む外部の最先端セキュリティ企業等から講師を招き、事例紹介や海外の最新動向、先端ケーススタディを取り入れた演習、アクティブ・ラーニングスタイルを取り入れた授業を行う。

全ての科目は 15 時限 135 時間開講され、通常科目では夜間時間（18 時 10 分以降）に週 2 コマ、集中科目では指定した土曜日に 3 コマで実施する。

履修資格として、大学卒業程度の基本的な情報セキュリティの知識を有し、最高情報セキュリティ責任者 (Chief Information Security Officer: CISO) または上級セキュリティエンジニアを目指すものを対象とする。

成績評価においては、各科目の最終試験で成績評価を行う。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る。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行う。いずれも概ね、6 割以上の理解・達成をもって、合格とする。修了要件は受講開始から 4 年以内に、6 科目 135 時間を全て修めた者について、本プログラムの修了とし、履修証明書を授与する。

1.3 CySec 実現のためのビジョンと運営組織

2020 年の東京オリンピック開催で予想される世界からのサイバー攻撃に備え、2018 年までには、高度セキュリティ専門家（CyS-HS: High level Specialist on Cyber Security）を多数育成する必要がある。この目的の達成には、残された時間が少ないことに鑑み、素質ある人物を短期間の集中的教育を行わなければならない。日本の教育は一部に進んでいる大学があるものの、レベルの高さ、育成人数が少ない等まだまだ不十分である。このままでは最先端 ICT 国家を目指す日本にとって大きな痛手が懸念される。この状況を打破するには、産官学一体となり、欧米・特に米国の協力を得ながら、促成教育体制を整え、直ちに適性ある人の高度化教育を開始する必要がある。

図 1.1 に本プログラムのビジョンを示す。高度セキュリティ専門家とは高レベルのセキュリティ知識を持ち、優れたインシデント対応能力を有し、指揮官としての判断・決断力があるグローバルな人脈を持っている人物である。

本ビジョン達成のために、平成 28 年度は図 1.2 に示す CySec 組織を東京電機大学未来科学研究科下に設置し、CySec 科目は東京電機大学未来科学研究科の科目として開講し、他研究科ならびに大学院へ進学する先行履修生の学生も履修できるようにするなど、研究科の壁を超えた学際的な開講形態をとった。

図 1.1　国際化サイバーセキュリティ学特別コースの位置づけとビジョン

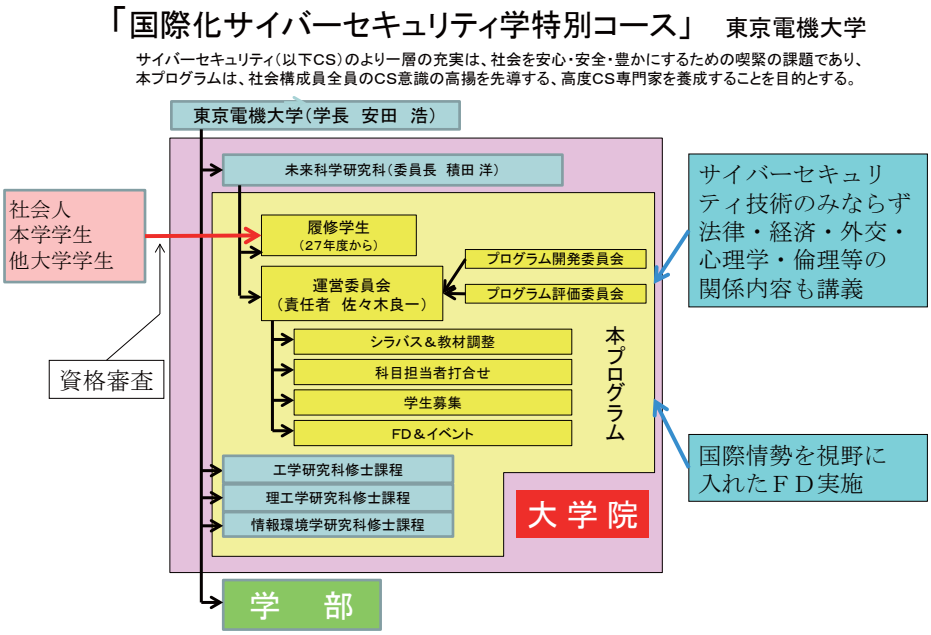

図 1.2　平成 28 年度の東京電機大学内部における CySec 組織図

第 2 章

国際化サイバーセキュリティ学特別コースの取り組み

2.1　シラバスの特色

サイバーセキュリティ分野においては、知識を有するだけではなく、その知識を活かして、実際に活用・運用できる能力が不可欠である。情報セキュリティの統括的責任を持つ CISO、インシデントや脆弱性に直接対応する上級セキュリティエンジニアとしての実践的な能力の修得が肝要である。本プログラムでは、普遍的な知識を与えるのみならず、最新の事例に触れることの重要性を重視し、企業等で活躍されている専門家を招聘し、事例紹介と事例に基づくワークショップ形式の演習を実施する。演習においては、協力企業等から提供される機器・ソフトウェアを活用して、実例に基づく、インシデント対応、フォレンジック、脅威分析、リスク分析、脆弱性検査を実践的に学ぶことができる最先端のプログラムになるように科目を設計している。

2.2　科目構成

2.2.1　科目体系

本プログラムでは、企業における情報セキュリティを統括する CISO や、セキュアな情報システムの開発において主導的役割を果たす上級セキュリティエンジニアを、育成すべき高度人材像としている。そのような人材には、最先端の情報セキュリティ技術に精通するのみならず、法律・倫理など制度的枠組みに関する理解や、攻撃者の意図や行動に関する洞察、企業におけるコンプライアンスを実現するためのガバナンスなど、幅広くかつ高度な能力が必要とされる。そこで、本プログラムでは以下の 6 科目（演習中心科目 3 講座、座学ワークショップ形式科目 3 講座）を開講した。

1PF　サイバーセキュリティ基盤（座学ワークショップ形式科目）
2CD　サイバーディフェンス実践演習（演習中心科目）
3IN　セキュリティインテリジェンスと心理・倫理・法（座学ワークショップ形式科目）

4DF　デジタル・フォレンジック（演習中心科目）
5MG　情報セキュリティマネジメントとガバナンス（座学ワークショップ形式科目）
6DD　セキュアシステム設計・開発（演習中心科目）

6 科目（各 15 時限）を設置する。総時間数は 1 コマを 90 分として計算し、135 時間とする。定職を持つ社会人の受講を鑑み、通常科目では夜間時間（18 時 10 分から）に週 2 コマ、集中科目では 3 週ごとの土曜日に 3 コマで実施する。

2.2.2　社会人受講者を見据えた学習スタイル

育児層にある社会人には、支援制度を活用してもらう体制を構築した。社会人の学びやすさを考慮し、全ての科目は半期で行われ、1 年で全科目が開講される。次半期では、科目曜日を入れ替えて開講することで、様々なライフスタイルの社会人が学ぶ機会を得られるようにし、最短 1 年、最長 4 年での修了を可能としている。

履修資格は大学卒業程度の基本的な情報セキュリティの知識を有し、CISO または上級セキュリティエンジニアを目指すものを対象とする。受講上の注意として受講にあたっては、1PF サイバーセキュリティ基盤を最初に学ぶことを推奨する。CISO やマネジメント指向の経営層に対しては、5MG 情報セキュリティマネジメントとガバナンス、エンジニア指向の CISO 補佐や上級セキュリティエンジニアを目指す者に対しては各種演習科目を先行して履修することが推奨される。

2.2.3　成績基準と履修証明

各科目の最終試験で成績評価を行う。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る。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行う。いずれも概ね、6 割以上の理解・達成をもって、単位合格とする。受講開始から 4 年以内に、6 科目を全て修めた者について、本プログラムの修了とし、履修証明書を授与する。

2.3　科目概要

本プログラムの各科目のシラバス詳細については付録 1 に示す。

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共同によって実施される。これによって、高度情報セキュリティ人材に必要とされる知識と能力の獲得を可能とする。あわせて、東京電機大学サイバーセキュリティ研究所内の設備を使用した演習の実施によって技術を向上させる。それと同時に、受講者間での交流を促進し、情報セキュリティの実務において重要となる高度セキュリティ人材間の人的ネットワークの構築にも資する。

各科目の概要について、以下で紹介する。

2.3.1 サイバーセキュリティ基盤

サイバーセキュリティ基盤は、講義中心科目である。本プログラムを学修する上での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。

2.3.2 サイバーディフェンス実践演習

サイバーディフェンス実践演習は、演習中心科目である。LAN、WAN、無線やセキュアプロトコル、PKI などについて演習を通し学び、不正アクセス、DDoS 攻撃、マルウェアなどの各種ネットワーク攻撃とその対応について、演習を中心として学習する。さらに、セキュアネットワークデザインの方法論と実践的演習を行い、先進的な知識を身につける。

2.3.3 セキュリティインテリジェンスと心理・倫理・法

セキュリティインテリジェンスと心理・倫理・法は、講義中心科目である。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、CISO に必要な基礎知識を修得する。また、インシデンスレスポンスおよびフォレンジックの基本について学び、上級セキュリティエンジニアとしてのインシデントへの基本的な対応能力を養う。

2.3.4 デジタル・フォレンジック

デジタル・フォレンジックは、演習中心科目である。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。CISO 志向の受講者向けには法リテラシーと法廷対応の能力、上級セキュリティエンジニア志向の受講者向けには、フォレンジックの具体的な技術力を修得させることができる。

2.3.5 情報セキュリティマネジメントとガバナンス

情報セキュリティマネジメントとガバナンスは、講義中心科目である。企業の事業継続における情報セキュリティマネジメントとガバナンスについて、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、ISMS を中心としてケーススタディで学ばせる。本科目は主に CISO 志向のニーズに対応し、コンプライアンスならびにインシデントへの実践的な対応能力を修得させることができる。

2.3.6 セキュアシステム設計・開発

セキュアシステム設計・開発は、演習中心科目である。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、演習を通して体得させる。セキュアシステムの基本とセキュリティ要求分析を学び、コモンクライテリアに基づいて、情報システムの評価および分析を実践する。また、セキュアプログラミングの基本を学び、脆弱性がどのように組み込まれ、それをどのように発見し、修正・対策するかについて、ケーススタディで実践的に学ぶ。本科目は主に上級セキュリティエンジニア志向のニーズに対応する専門的科目である。

2.4 募集要項

募集要項を付録 2 に示す。

東京電機大学では、「国際化サイバーセキュリティ学特別コース」として、6 科目（135 時間）を開講する。このコースは、履修証明制度に対応する。

2.5 講師陣

講師は第一線のセキュリティ研究を行っている東京電機大学教員の他に、海外も含む外部の最先端セキュリティに関連する団体・組織・企業から講師を招き、事例紹介や海外の最新動向、先端ケーススタディを取り入れた演習、アクティブ・ラーニングスタイルを取り入れた授業を行う。以下表 2.1 に平成 28 年度の講師一覧を示す。

2.6 職業実践力育成プログラム（BP）の認定

本プログラムは、社会構成員全員の CyS 意識の高揚を先導する、高度 CyS 専門家を養成することを目的としており、CyS 技術領域のみの教育ではなく、法律・経済・外交・心理・倫理等の分野で、CyS に関わりのある内容も高度なレベルで教育することで、経営・運用・折衝・監査等も先導可能な高度 CyS 専門家を養成することにある。

サイバー攻撃は日進月歩の如く目まぐるしく変化・進化しており、高度な CyS 意識ならびに技術を維持するためには、常に学び続ける必要性があり、「学び続ける」社会人参加型の教育が必要となる。

平成 27 年 3 月の教育再生実行会議提言（第 6 次提言）を受けて文部科学省より「職業実践力育成プログラム」（BP）認定制度が開始された。平成 27 年 12 月 15 日付けで本プログラムも BP 認定され、将来的に、本プログラムのさらなる発展・拡充に際して、BP 認定による厚生労働省の教育訓練給付制度との連携により、社会人の学びやすさがさらに増すことが期待され、「学び続ける」社会人参加型教育の実現に寄与していく。

表 2.1　CySec プログラム 平成 28 年度講師一覧

名前	所属
市田 達也	株式会社リクルートテクノロジーズ
伊藤 潤	三井物産セキュアディレクション株式会社
井上 吉隆	NTT セキュアプラットフォーム研究所
猪俣 敦夫	東京電機大学
岩井 将行	東京電機大学
上原 哲太郎	立命館大学　情報理工学部
大鐘 博子	株式会社 NSD
大久保 隆夫	情報セキュリティ大学院大学
大河内 智秀	三井物産セキュアディレクション株式会社
大森 英直	株式会社ジェイアイエヌ
奥田 茂	AIU 損害保険株式会社
小熊 慶一郎	株式会社 KBIZ
奥村 恭弘	NTT コミュニケーションズ株式会社
越智 啓太	法政大学
柿崎 淑郎	東京電機大学
金児 茂	三井物産セキュアディレクション株式会社
亀田 勇歩	SCSK 株式会社
佳山 こうせつ	富士通株式会社
河野 省二	株式会社ディアイティ
木村 仁美	トレンドマイクロ株式会社
草場 英仁	三井物産セキュアディレクション株式会社
久保 正樹	一般社団法人 JPCERT/CC
小林 浩史	NEC マネジメントパートナー株式会社
小村 誠一	NTT アドバンステクノロジ株式会社
金野 千里	独立行政法人　情報処理推進機構（IPA）
齊藤 泰一	東京電機大学
齋藤 良平	ハミングヘッズ株式会社
櫻庭 信之	西村あさひ法律事務所
佐々木 良一	東京電機大学
白濱 直哉	デトロイトトーマツリスクサービス（株）
高取 芳宏	オリック東京法律事務所
土屋 日路親	総務省
角尾 幸保	日本電気株式会社
角田 朱生	三井物産セキュアディレクション株式会社
寺田 真敏	株式会社日立製作所
富樫 晃	神奈川県立東部総合職業技術校
戸田 洋三	一般社団法人 JPCERT/CC
中島 一樹	トヨタ自動車株式会社
野　周作	株式会社 FRONTEO
橋本 豪	西村あさひ法律事務所
長谷川 長一	株式会社ラック
林 郁也	NTT コミュニケーションズ゛株式会社
原田 要之助	情報セキュリティ大学院大学
平井 康雅	株式会社 NTT データ
正木 健介	NRI セキュアテクノロジーズ株式会社
松木 晋祐	株式会社ベリサーブ
満永 拓邦	東京大学大学院
安田 浩	東京電機大学
八槇 博史	東京電機大学
山谷 晶英	三井物産セキュアディレクション株式会社
六宮 智悟	トレンドマイクロ株式会社

第 3 章

国際化サイバーセキュリティ学特別コースの実施と成果

3.1 受講状況報告

日本社会一般のセキュリティチュートリアルの高まりを受けて、社会人への本コースへの認知度が拡大した。平成 27 年 2 月 12 日に本プログラム第一期生となる受講者の募集を行ったところ、企業の第一線で業務している、あるいは将来的に業務予定の社会人から 34 名の応募があり、33 名（女性は 6 名）に対して受講者と決定した。この他にも、大学院科目先行履修制度の活用による本学大学院進学予定の学部生 25 名および本学大学院生 47 名を加え、72 名の履修者を迎えて、本プログラムは平成 27 年 4 月より開講された。さらに平成 27 年 7 月 14 日より、平成 27 年度後期受講者を若干名募集したところ、10 名の応募があり、9 名を新たな受講者として迎え入れた。

平成 28 年度においては、前期 34 名，後期 7 名を新たな受講生として迎え入れ、その役割と成果を果たしている。

平成 28 年度における CySec 開講科目の受講者数を表 3.1 に示す。また、CySec 講義の様子を図 3.1 に示す。

表 3.1　平成 28 年度 CySec 開講科目と受講者数

	CySec 受講生	大学院生	先行履修生	合計
1PF サイバーセキュリティ基盤	42	15	7	64
2CD サイバーディフェンス実践演習	39	18	0	57
3IN セキュリティインテリジェンスと心理・倫理・法	34	17	9	60
4DF デジタルフォレンジック	36	14	6	56
5MG 情報セキュリティマネジメントとガバナンス	31	12	0	43
6DD セキュアシステム設計・開発	34	12	0	46

図 3.1　開講された CySec 講義の様子

3.2　平成 28 年度修了式実施報告

本プログラム初めての修了生を輩出する平成 27 年度修了式を平成 28 年 3 月 11 日に挙行し、18 名（うち大学院生 1 名を含む）の修了者に対して、古田学長より履修証明書が授与された。当日は CySec 講師 24 名も出席し、本プログラム第一期修了生の門出を祝うとともに、今後の活躍を祈念した。

本プログラム 2 年目となる平成 28 年度においては、前期修了生 8 名、後期修了生 27 名（うち大学院生 6 名を含む）となり、最短 1 年での修了を目指す者から、家庭や業務などのライフスタイルから複数年度をかけて修了を目指す者まで、多様な修了生を輩出することができた。本プログラムの開始から 2 年目終了時点において、47 名の修了生を送り出すことができ、また平成 29 年度前期には新たに 35 名の受講生を迎え入れる予定であり、益々の発展を目指していきたい。修了式の

様子を図 3.2 に示す。

また、修了生が今後も CyS の最新事情や情報交換を行えるように、同窓会に相当する仕組みを準備し、さらに学び続けられる環境を提供した。修了生主催の勉強会、修了式などの定期的なタイミングでの受講生と修了生との懇親など、情報交換の場として、発展している。

図 3.2　修了式の様子

3.3　授業評価アンケート結果と分析

各講義において学期末に授業改善を目的として授業評価アンケートを実施した。授業評価アンケートは本学所定様式と本プログラム独自様式の 2 方式で実施した。

概ね好意的な評価が多く、特に 2CD サイバーディフェンス実践演習、4DF デジタル・フォレンジック、6DD セキュアシステム設計・開発の演習科目においては、座学では学べない実践的な学習ができたことについて大変高い評価を得た。また、本プログラムの特色である法知識、マネジメント、ガバナンス、インシデント対応に関する講義についても大変好評を得た。これらについて大学等で学ぶことができる機会が希少であり、CySec として重要な役割を果たしていると考えられる。

一方で、改善すべき点も指摘された。大きな問題としては講義時間の超過があった。この問題は

以前より指摘されており、2 年目においては改善策を講じたものの、オムニバス形式で構成されている関係上、その限られた時間の中で多くのことを伝えたいと考える講師の想いとそのような講師からもっと学びたいと考える積極的な受講者の相乗効果により、90 分という限られた講義時間の中で完結することの難しさが際立った。

また、演習科目においては個々のスキルが不均一であることによる進捗の差がみられた。事前準備として課題などを準備し、一定水準までスキルを高める努力はしたが、十分な効果を発揮したとはいえず、より一層の改善が必要である。

本プログラム独自様式のアンケートでは、本講義が業務にどのように役立ったかを自由記述で尋ねた。「体系的に学ぶことができた」「最新事例・動向が学べた」「フォレンジックの演習が役立った」など様々な面から受講生の業務に役立つ実践的な知識を教授できていると思われる。また、詳細をこの報告書に記することはできないが、個々の具体的な業務において深く関連し、直接的に役立っているとの回答もあり、CySec 講義が大変有意義で効果的なサイバーセキュリティ教育として機能していることがわかる。

3.4 業務実績

本プログラム運営委員会を 12 回実施し、本プログラムの健全な運営ならびに更なる発展に尽力した。評価委員会・開発委員会を各学期末に実施し、前期末に講師反省会も実施した。本プログラムの初年度にあたり、講義の進め方、学内講師と外部講師との連携、カリキュラムの問題点などが挙げられ、改善に向けた議論を行った。

FD 活動は 5 回実施した。講師意見交換会を各学期の開始に先だち実施し、本プログラムの目的とその役割、講師としての立ち居振る舞いと受講生からの期待について確認するとともに、更なる発展のために議論を尽くした。平成 28 年 4 月には SECURETOKYO2016 の後援をし、前期科目「サイバーセキュリティ基盤」に関係する CISSP 資格保有者を中心に 140 名超の参加者を集め、最新のセキュリティ情報の提供を行った。平成 28 年 11 月には同様に CISSP 関連イベント「CISSP/SSCP 限定会合」を共催し、CISSP 資格保有者を中心に学外 42 名の参加者があり、CISSP 保有者と資格獲得を目指す方々に向けた情報提供を行った。平成 29 年 2 月に開催されたサイバーセキュリティシンポジウム道後 2017 では学内関係者が会場の講演やディスカッションに積極的に参加し、議論を深めた。

平成 28 年 11 月には本プログラム主催の CySec シンポジウム 2016 を実施し、関係者を除き 89 名の参加があった。本シンポジウムでは海外より講師 3 名を招き、グローバルサイバーセキュリティ最新事情、情報セキュリティにおける脅威インテリジェンスと教育の価値について講演を頂いた。平成 29 年 3 月には本プログラム共催でサイバーセキュリティシンポジウム 2017 in TDU を実施し、先進的な研究の推進、高度専門技術者の育成、実務活動の実践の統合的アプローチを紹介した。

3.5 広報活動

本委託費で開発した広報用 Web サイト（https://cysec.dendai.ac.jp）において、プログラム詳細およびカリキュラム、シンポジウムなどのイベントについて、情報発信を行うとともに、Facebook 等の SNS を通じて最新情報を積極的に配信している。Web サイトの一部を図 3.3 に示す。

図 3.3　CySec の Web サイト

第 4 章

本報告書のまとめと今後の展望

本プログラム初年度となる平成 27 年度においては前期 33 名、後期 9 名の受講者に加え、本学大学院進学予定の学部生 25 名および本学大学院生 47 名を加えた 79 名の受講者に対して講義が開始された。平成 28 年度においては、前期 34 名、後期 7 名の新たな受講生を迎え入れ、当初の計画通りに本プログラムを運営している。

本プログラム初年度となる平成 27 年度には 18 名の修了生を輩出し、平成 28 年度前期には 8 名，後期には 27 名が修了し、履修証明書を授与された。本プログラム開始から 2 年目終了時点において、83 名の受講生を迎え入れ、47 名の修了生を送り出すことができた。平成 29 年度前期には新たに 35 名の受講生を迎え入れる予定であり、今後も年間 20 名程度の修了生が見込んでおり、CySec 修了生の活躍が広く社会において期待される。

受講者からの授業評価アンケートの結果は概ね好意的であり、本プログラムの目的は果たされていると考えられる一方で、解決すべき課題も残されており、改善に向けてより一層の注力が必要である。

本プログラムは今後も年間 40 名程度の受講者受入を継続し、社会全体の CyS 意識向上を目指すのみならず、本国の国防にも寄与する重要な役割を担う修了生を輩出し続けることを目指し、サイバーセキュリティに強い東京電機大学として、国内外に認知されるようにさらなる努力を続けていく。