平成 26 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 27 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 時代の背景

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 本プロジェクトの特色

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取得すべき能力

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。

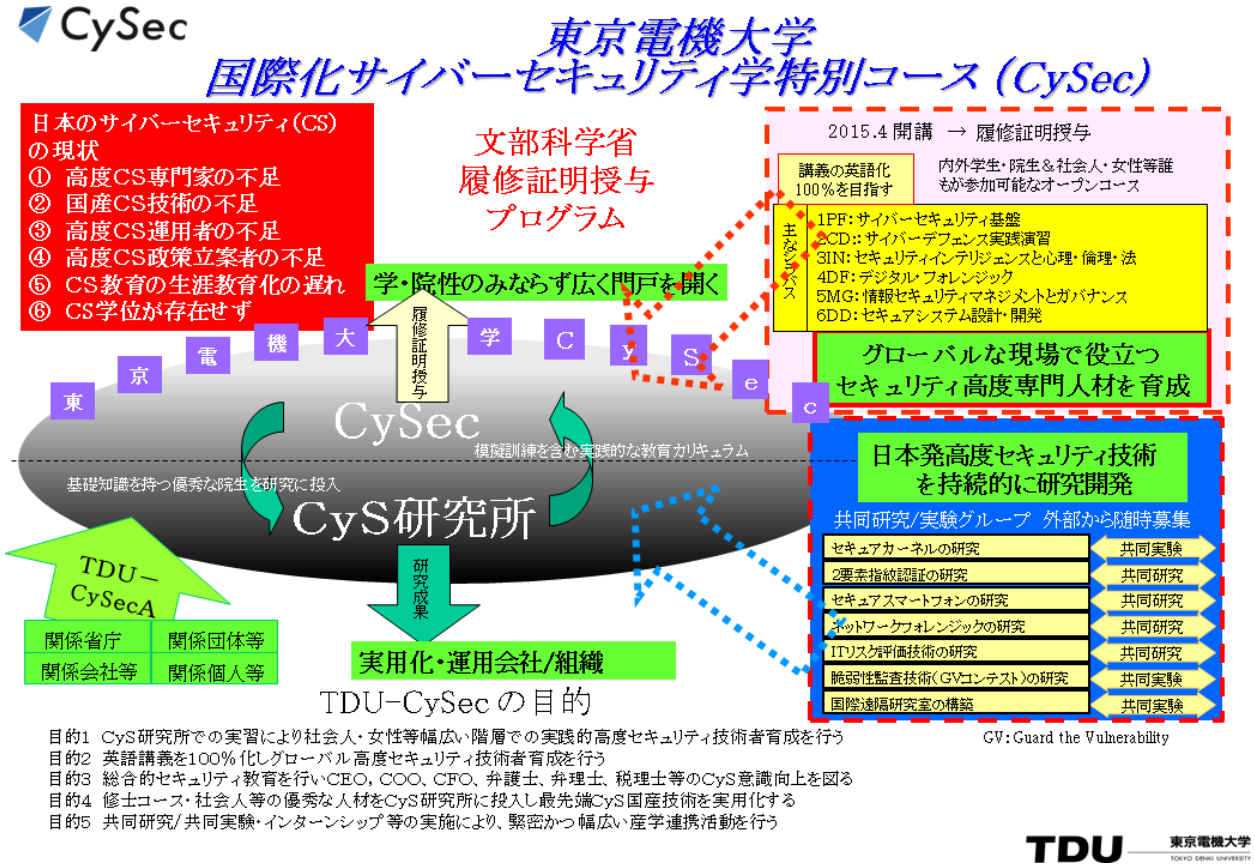

図１　　国際化サイバーセキュリティ学特別コースの位置づけとビジョン

本ビジョン達成のために図 2 の様に CySec を東京電機大学未来科学研究科に設置し、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。

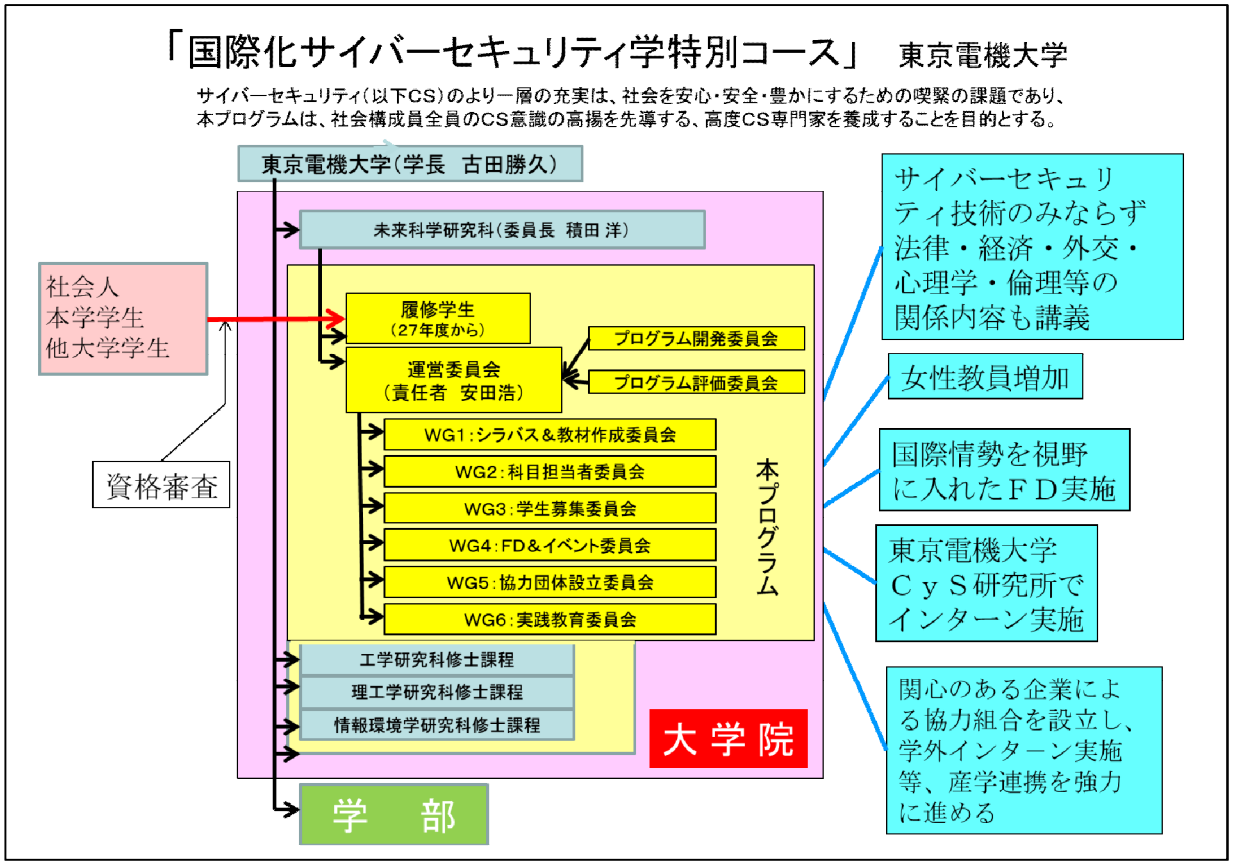

図 2　CySec の東京電機大学内部の組織図

第 2 章
国際化サイバーセキュリティ学特別コースの具体化

2.1 シラバスの特徴

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 シラバス構成・授業時間・コマ数

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、集中科目では隔週の土曜日に 3 コマで実施する。

2.2.2 支援制度

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 成績の判断基準と履修証明

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。各科目の概要について、以下で紹介する。

(1PF)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。

(2CD)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。

(3IN) 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。

(4DF)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。

(5MG)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。

(6DD)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。

キャリアアップ：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（ＣｙＳ）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。

2.4 募集要項

募集要項の抜粋を以下に示す。詳細は付録 2 を参照のこと。

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。

2.4.1 教育目的

悪意ソフト攻撃は増加の一途であり、サイバーセキュリティ（以下ＣｙＳと略す）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る。そのためには、社会活動に参加するすべての人々のＣｙＳ意識を高める必要がある。

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している。

2.4.2 教育課程

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最高情報セキュリティ責任者（Chief Information Security Officer: 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。そのような人材を育成するため、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と、座学ワークショップを合わせて実施する。

具体的には、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を育成するために、以下の 6 科目(演：演習中心 3 講座、講：講義・ワークショップ中心 3 講座)を開講する。

開講する科目は、大学院修士課程レベルの内容である。

① サイバーセキュリティ基盤	(1PF)	(講)
② サイバーディフェンス実践演習	(2CD)	(演)
③ セキュリティインテリジェンスと心理・倫理・法	(3IN)	(講)
④ デジタル・フォレンジック	(4DF)	(演)
⑤ 情報セキュリティマネジメントとガバナンス	(5MG)	(講)
⑥ セキュアシステム設計・開発	(6DD)	(演)

2.4.3 履修証明書

学校教育法に基づく履修証明制度により、プログラム修了者には、「国際化サイバーセキュリティ学特別コース 履修証明書」を授与する。

【本プログラムにおける履修証明書交付要件】

開講される 6 科目を修得すること

【履修証明制度概要】

平成 19 年度の学校教育法の改正により、大学等における「履修証明制度」が創設された。

これは、学生を対象とした学位プログラムの他に、社会人等を対象とした 120 時間以上の学習プログラム（履修証明プログラム）を提供し、修得した者に履修証明書を発行する制度である。履修証明制度には、以下の 3 点の特徴がある。

（1）大学の学位に比べ、より短期間に修得することが可能

（2）再就職やキャリアアップに役立つ社会人向けの教育プログラム

（3）プログラム修了者には、学校教育法に基づき履修証明書を交付

※履修証明制度に関する文部科学省 Web ページ

http://www.mext.go.jp/a_menu/koutou/shoumei/

2.4.4 募集人員

国際化サイバーセキュリティ学特別コース　2015 年度　定員 20 名

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 1 に講師一覧を示す。

表 1　CySec プログラム　講師一覧

氏名	会社名	役職
岩井将行	東京電機大学	准教授
齊藤泰一	東京電機大学	教授
大鐘博子	株式会社 NSD	IT ｽﾍﾟｼｬﾘｽﾄ
佳山こうせつ	富士通株式会社	ﾏﾈｼﾞｬｰ
河野省二	株式会社ディアイティ	副事業部長
金野千里	独立行政法人　情報処理推進機構	ﾗﾎﾞﾗﾄﾘｰ長
武智洋	日本電気株式会社	ｼﾆｱｴｷｽﾊﾟｰﾄ
小熊慶一郎	株式会社 KBIZ	代表取締役
小林浩史	日本電気株式会社	ｴｷｽﾊﾟｰﾄ
河野健二	慶應義塾大学	准教授

松下綾子	アルプスシステムインテグレーション株式会社	
奥村恭弘	NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ株式会社	担当課長
林郁也	NTT コミュニケーションズ株式会社	担当課長
六宮智悟	トレンドマイクロ株式会社	統括責任者
松木晋祐	株式会社 ACCESS	課長
木村仁美	トレンドマイクロ株式会社	ｽﾍﾟｼｬﾘｽﾄ
草場英仁	三井物産セキュアディレクション株式会社	
国分裕	三井物産セキュアディレクション株式会社	ｼﾆｱｴｷｽﾊﾟｰﾄ
小西明紀	三井物産セキュアディレクション株式会社	
中西克彦	NEC ネクサソリューションズ株式会社	
正木健介	NRI セキュアテクノロジーズ株式会社	ｾｷｭﾘﾃｨｱﾅﾘｽﾄ
安田浩	東京電機大学	教授
杉浦芳樹	NTT データ先端技術株式会社	
角尾幸保	日本電気株式会社	主席研究員
松浦幹太	東京大学	教授
大河内智秀	三井物産セキュアディレクション株式会社	ｼﾆｱﾌﾟﾛﾃﾞｭｰｻ
越智啓太	法政大学	教授
橋本豪	西村あさひ法律事務所	弁護士
高取芳宏	オリック東京法律事務所	弁護士
土屋日路親	総務省	主査
伊藤潤	三井物産セキュアディレクション株式会社	ｼﾆｱｴｷｽﾊﾟｰﾄ
満永拓邦	一般社団法人 JPCERT／CC	
佐々木良一	東京電機大学	教授
上原哲太郎	立命館大学　情報理工学部	教授
野﨑周作	株式会社 UBIC	執行役員
白濱直哉	有限責任監査法人トーマツ	シニアマネジャー
八槇博史	東京電機大学	准教授
桜庭信之	西村あさひ法律事務所	弁護士
中島一樹	トヨタ自動車株式会社	主幹
原田要之助	情報セキュリティ大学院大学	教授
金児茂	三井物産セキュアディレクション株式会社	ｴｷｽﾊﾟｰﾄ
北原幸彦	NRI セキュアテクノロジーズ株式会社	ｾｷｭﾘﾃｺﾝｻﾙﾀﾝﾄ
烏山雄大	三井物産セキュアディレクション株式会社	ｴｷｽﾊﾟｰﾄ
大木栄二郎	学校法人　工学院大学	常務理事
柿崎淑郎	東京電機大学	助教
久保正樹	一般社団法人 JPCERT／CC	リーダー
戸田洋三	一般社団法人 JPCERT／CC	

寺田真敏	株式会社日立製作所	
井上吉隆	NTT スマートコネクト株式会社	担当課長
亀田勇歩	SCySK 株式会社	エヴァンジェリスト
大久保隆夫	情報セキュリティ大学院大学	教授
宮坂肇	NTT データ先端技術株式会社	ｴｸﾞｾﾞｸﾃｨﾌﾞｽﾍﾟｼｬﾘｽﾄ

第 3 章
国際化サイバーセキュリティ学特別コースの実行

3.1 受講生の集まり状況の報告

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。その結果、2015 年 2 月 12 日に本プログラム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／業務をする予定の社会人３４名の応募があり、内 33 名の履修を決定した。女性は 6 名であった。2015 年 4 月より開始される本プログラムの各授業には、25 名の学生と 47 名の大学院生を迎える予定であり、最大 72 名の履修者を基にプログラムを開始する予定である。

平成 26 年度内の成果ではないが、平成 27 年 4 月に開講された CySec 講義の様子を図 3 に示す。

図 3　開講された CySec の講義の様子

3.2 CySec オープニングシンポジウム

平成 27 年度の開講を控え、講師陣がサイバーセキュリティのグローバルな状況を把握するために、海外からサイバーセキュリティ専門家を招き、「東京電機大学国際化サイバーセキュリティ学特別コース オープニングシンポジウム」を開催した。開催内容は下記である。

日時　：　平成 27 年 2 月 13 日(金曜日)　13:00-19:00
場所　：　東京電機大学　東京千住キャンパス 1 号館　2F 丹羽ホール
主催　：　東京電機大学未来科学研究科　国際化サイバーセキュリティ学特別コース(CySec)
共催　：　東京電機大学研究推進社会連携センター(ＣＲＣ)

■プログラム

12:15-　　受付開始
13:00-13:30　開　　会　「東京電機大学国際サイバーセキュリティ学特別コースについて」
　　東京電機大学　未来科学研究科委員長　安田　浩
13:30-14:10　講　　演　「東京オリンピックに向けたサイバーセキュリティ」
　　内閣サイバーセキュリティセンター副センター長　内閣審議官
　　谷脇　康彦氏※
14:10-14:50　講　　演　「グローバルサイバーセキュリティ最新事情」　(同時通訳)
　　リッジシュミットサイバー共同経営者、
　　元米国大統領サイバーセキュリティ補佐官　Mr. Howard Schmidt※
14:50-15:10　休　　憩
15:10-15:50　講　　演　「金融におけるサイバーセキュリティ」　(同時通訳)
　　VP, Operational Governance, Scotiabank　Mr. Greg Thompson※
15:50-16:30　講　　演　「サイバーセキュリティの基盤」　(同時通訳)
　　Senior Instructor and Consultant, Mile2
　　Mr. Kevin Henry※
16:30-16:40　閉　　会　東京電機大学　学長　古田　勝久
17:00-19:00　意見交換会　1 号館 1 階 100 周年ホール

※各講師の略歴を付録 3 に示す。

図 4 に示すように各講師による活発な議論と討論会が行われた。また、海外講師の英語による講演には同時通訳を活用した。

図 4　CySec オープニングシンポジウムの様子

3.3 業務の実績の説明

業務スケジュールを表 2 に示す。サイバーセキュリティにおける討論会を 2015 年 2 月 13 日に 18 名にて行った。更に本プログラムに係る講師を集めた外部講師説明会を 2015 年 3 月 9 日、11 日に行った。また幹事会および FD として 21 回会合を開き本履修証明プログラムのあり方を徹底的に議論した。出来上がった 6 教科のシラバスを基に評価委員会・開発委員会合同開催を第 1 回 2015 年 1 月 22 日、第 2 回 2015 年 3 月 27 日に分け開催し、外部評価委員による本プログラムの妥当性と魅力、社会的意義を確認した。

表 2　平成 26 年度　実施日程表

１０月	１１月	１２月	１月	２月	３月
■キックオフ 2014 年 10 月 8 日 ■幹事会 準備会 10 月 3 日 第 1 回 10 月 22 日 第 2 回 10 月 30 日	■幹事会 第 3 回 11 月 6 日 第 4 回 11 月 13 日 第 5 回 11 月 20 日 第 6 回 11 月 27 日	■幹事会 第 7 回 12 月 4 日 第 8 回 12 月 11 日 第 9 回 12 月 18 日 第 10 回 12 月 25 日	■評価委員会・開発委員会(合同開催) 第 1 回 2015 年 1 月 22 日 ■幹事会 第 11 回 1 月 8 日 第 12 回 1 月 15 日 第 13 回 1 月 22 日 第 14 回 1 月 29 日	■オープニングシンポジウム 2015 年 2 月 13 日 ■FD1 2015 年 2 月 13 日 ■幹事会 第 15 回 2 月 12 日 第 16 回 2 月 19 日 第 17 回 2 月 26 日	■FD2 2015 年 3 月 9 日、11 日 ■評価委員会・開発委員会(合同開催) 第 2 回 2015 年 3 月 27 日 ■幹事会 第 18 回 3 月 5 日 第 19 回 3 月 19 日 第 20 回 3 月 26 日 第 21 回 3 月 31 日

3.4 WEB サイトによる学び直しプログラム広報

本委託費で開発した WEB サイト https://CySec.dendai.ac.jp において、受講希望者や受講生にプログラムの詳細やシンポジウムなどのイベントについて、情報発信を行うと同時に、Facebook 等で最新情報を積極的に配信している。WEB サイトの一部を図 5 に示す。

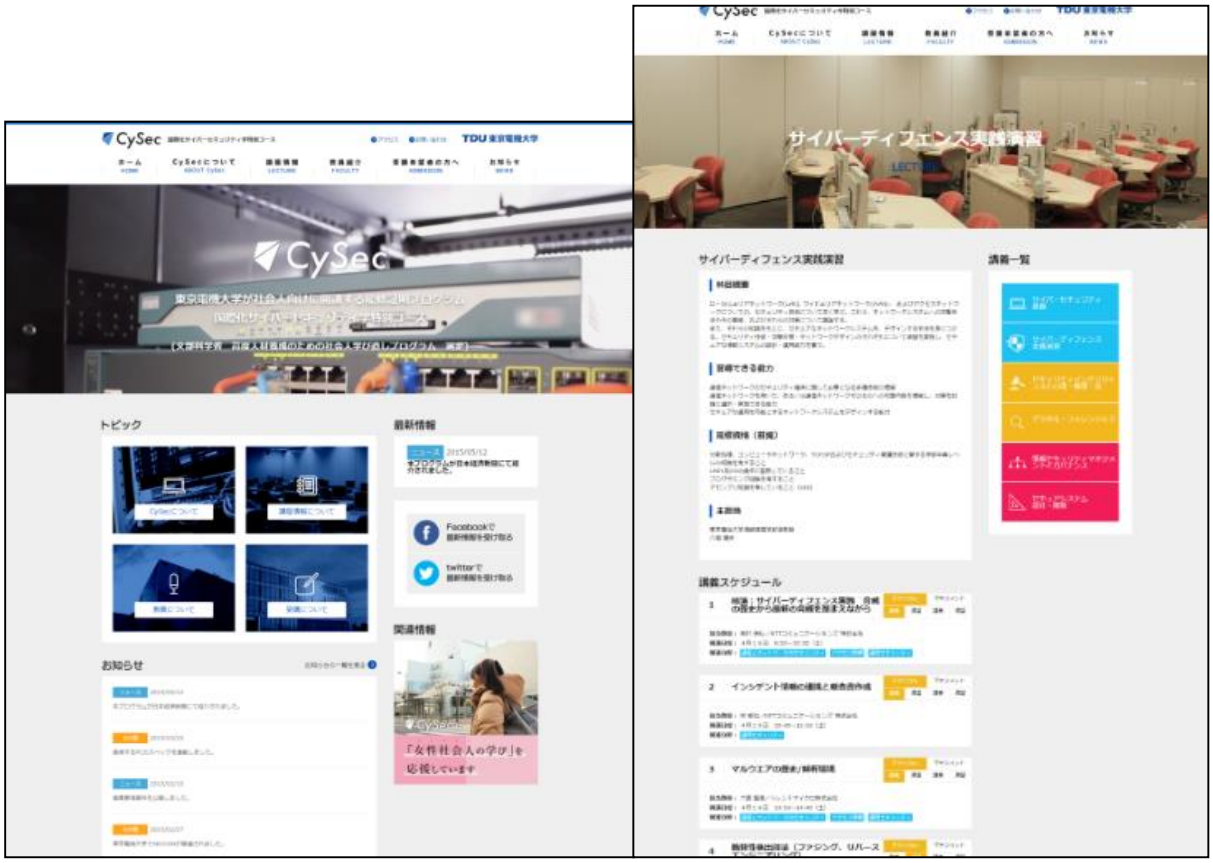

図 5　CySec プログラム広報用の WEB ページ

3.5 メディア掲載実績

本プログラムは 2014 年 10 月から活動を開始しており、サイバーセキュリティに対する関心の高まりのせいか、メディアからの取材を受けることも多かった。以下にリストで示す。

媒体：日本経済新聞社
内容：大学～知の明日を築く～
　　東京電機大学サイバー・セキュリティ研究所 / 「情報を守れ」精鋭育てる
掲載日：2015 年 1 月 8 日(木)

媒体：日本経済新聞社
内容：防げサイバー攻撃(下)
　　敵の手読む天才育てよ / 日本、産学官で巻き返し
掲載日：2015 年 3 月 17 日(火)

第 4 章
本報告書のまとめと今後の展望

本委託業務の結果、2015 年 2 月 12 日に最初の履修生募集を行った。定員２０名としていたが、34 名の社会人の応募があり、経歴・意欲等を審査した結果、履修にかなうとして定員を超える 33 名の履修を決定した。女性は 6 名であった。2015 年 4 月より大学院進学予定の先行履修者 25 名、大学院生 47 名が加わり、最大 72 名の履修者に対してプログラムを開始する予定である。

2015 年秋期には 10 名程度、2016 年春期には 30 名程度の受講生の受け入れを予定し、準備を進めている。マスメディアやセキュリティ関連企業から一般企業・官公庁にいたるまで注目度は高いが、今後も積極的に広報活動を行う予定である。

本プログラム実施により初年度（2015 年度）に 20 名程度が履修証明書を取得する見込みであり、以降暫時取得者は増加し、年 40 名以上となっていくことを期待している。