情報セキュリティ人材育成プログラム SecCap の取り組み

猪俣 敦夫　大平 健司　松浦 知史　奥田 剛　門林 雄基　山口 英
藤川 和利　砂原 秀樹　曽根 秀昭　宮地 充子　後藤 厚宏　他

５つの連携大学が協力して開講する実践セキュリティ人材の育成コース（SecCap）によって，幅広いセキュリティ分野の最新技術や知識を具体的に体験的に習得することができる．技術面では，暗号をベースとする情報セキュリティ技術，Web サーバのセキュリティ技術，ネットワークセキュリティ技術から，法制度やリスク管理などの社会科学的な知識までをカバーする．受講生は，技術系，理論系，社会科学系の講義や実践演習・PBL から，それぞれが目指すキャリアパスに沿った割合で，主体的・自主的に調合した学習プログラムを作って受講できるようにしている．また，人材育成を進めるだけでなく，その育成ノウハウを全国の大学（参加大学）に広める活動を進めていく．これにより，実践セキュリティ人材育成の枠組み自体を作り上げることができ，実践セキュリティ人材育成のすそ野を広げ，我が国全体が必要とする人材の育成体制を作り上げることができると考えている．本稿では，SecCap の取り組み概要について述べる．

Information technology is an important and integral part of the current social infrastructure. Internet has come to play an important role in various foundations of our society and life. To maintain these systems and ensure infrastructure safety, many organizations, government bodies, and companies employ security experts. In addition, they have engineers to carry out their work properly. However, very few people must have heard of a management technique or a policy for information security. In order to establish the new special security courseware, we collaborated with four universities and some departments of the Japanese government for this research. In this paper, we introduce the novel learning style called “ SecCap ” for information security human development.

1　はじめに

近年の社会生活，産業，行政のすべてにおいて，情報セキュリティの必要性は高まる一方である．一般市民への普及啓発活動は重要であると同時に，高いセキュリティレベルを有する人材育成が必須である．我が国では，次の 3 つの層のすべてにおいて人材育成が急務である．1 つは，少数の世界的トップレベルの人材（トップガン）を発掘すること，2 つめは産業界や学術分野で，情報セキュリティ技術開発や研究を進めるセキュリティエキスパートの育成である．3 つめは，今回の事業が目指す幅広い IT 分野や組織運営においてセキュリティ実践力を持って社会や産業をリードする人材（実践セキュリティ人材）の育成である．実践セキュリティ人材は，

- IT 産業（製造系）においてセキュリティ要求レベルの高いプロダクト開発に携わる IT 技術者（セキュリティエキスパートと相談しながらシステム開発ができる人）
- 幅広い IT 利用企業（ユーザ企業）の IT 部門において，セキュリティベンダーやセキュリティコンサルタントと協力して，自社のセキュリティシステムを構築できる技術者

Introduction of a special human resource developement program (SecCap) for information security.

Atsuo Inomata, Hideki Sunahara, Hideaki Sone, Atsuko Miyaji, Atsuhiro Goto, 奈良先端科学技術大学院大学, 慶應義塾大学, 東北大学, 北陸先端科学技術大学院大学, 情報セキュリティ大学院大学, Nara Institute of Science and Technology, Keio university, Tohoku university, Japan Advanced Institute of Science and Technology, Institute of Information Security.

- CIO, CISO として，組織のセキュリティ経営を担う経営者
- IT 技術者を育成する教育機関（大学，専門学校など）の教育者

において，期待される人材である．このような人材育成は,「IT 技術＋セキュリティ技術」という意味でのマルチスペシャリスト人材の育成を目指していると言える．実践セキュリティ人材の育成は，広く社会生活全般に関わる産業，行政，教育の分野におけるリーダー的人材の厚みを増すことができる．その結果，我が国全体の安心・安全レベルの向上につながる．また，実践セキュリティ人材は，その上位レベルにあたるセキュリティエキスパート人材のベースであり，我が国のみならずグローバルに活躍するセキュリティエキスパート人材育成にもつながると考えられる．

本教育プログラムは，5 つの連携大学が協力して実践セキュリティ人材の育成コースを用意し，人材育成を進めるだけでなく，その育成ノウハウを，全国の大学（参加大学）に広める活動を進める．実践セキュリティ人材育成の枠組み自体を作り上げることにより，実践セキュリティ人材育成のすそ野を広げ，我が国全体が必要とする人材の育成体制を作り上げることができると考える．

1.1　学習・教育目標

我々のプログラムにおいて育成する実践セキュリティ人材は，実社会における実業経験を重ねることにより，情報セキュリティ・エンジニア，情報セキュリティ・マネージャー等の情報セキュリティ実践リーダーとなるマルチタレント人材になることを理想とする．これらの人材は最高情報セキュリティ責任者（CISO：Chief Information Security Officer) および実際に対策を立案し，その実行を指示する情報セキュリティ担当者（CISO 補佐）としての活躍が期待される．そのために，ソフトウェア・システム・製品の開発，システムコンサルティング，新事業の立案・企画業務などにおいて求められる情報セキュリティの実践的スキル，具体的には，OS，ソフトウェア，ネットワーク，システム設計・運用管理などのセキュアな構成技術とマルウェア対策に関する広範な知識・技術の習得を目指す．また，組織（企業）が IT 化された現在，自然災害，外部からの攻撃などのリスクから，情報資産や情報の流れを適切に管理することが必須である．そのため，IT に係るリスクの現状分析（調査，データ分析，モデル化），問題点の発見（事例研究など），対策の実施というマネジメントを構築し，実践できる人材を目指す．具体的には，企業・組織等でリスクマネジメント，BCP，事業企画，マーケティング，人材育成，教育研修等の業務に従事するために必要な実践的なリスクマネジメントについて，事例研究，調査分析を通じて知識応用力を習得する．

情報セキュリティ分野においては，5 つの連携大学を中心として，平成 25 年度は 60 名程度，順次，参加大学を 10 大学以上に拡大することにより，平成 28 年度は 100 名程度の実践セキュリティ人材の育成を目指す．この取組みでは，学生が“ SecCap ”と呼ぶ特別の履修コースを設け，その修了認定である「SecCap 認定」を学生が目指すことにより，履修学生の意識づけを高める．また，平成 29 年度以降において連携大学や参加大学が主体的に人材育成を継続できるようにするために，本履修コースを指導できる教員を育成することが必要である．本事業では，次世代においてセキュリティ分野の教育プログラムを開発し牽引するリーダー格教員を連携大学で各 1 名，そのリーダーの下，教育プログラムを実施する教員または候補者を連携大学で数名程度育成することを目指す．この教員養成は，参加大学にも広げていく．

1.2　教育内容

我々が取り組む SecCap では，幅広いセキュリティ分野の最新技術や知識を具体的に体験的に習得することができる．技術面では，暗号をベースとする情報セキュリティ技術，Web サーバのセキュリティ技術，ネットワークセキュリティ技術から，法制度やリスク管理などの社会科学的な知識までをカバーする．実践演習では，ハードウェアを対象としたもの，システムやソフトウェアを対象としたもの，企業組織のリスク管理を対象としたものなど，バラエティに富んだ演習コースが用意される．受講生は，技術系，理論系，社会科学系の講義や実践演習・PBL から，それぞれ

が目指すキャリアパスに沿った割合で，主体的・自主的に調合した学習プログラムを作って受講することができる（図 1）.

2 カリキュラム

情報セキュリティ分野では，5 つの連携大学（情報セキュリティ大学院大学，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）が中心となり，社会・経済活動の根幹に関わる情報資産および情報流通におけるセキュリティ対策を，技術面・管理面で牽引できる実践リーダーの育成を目指し，短期集中型演習として実施する技術実践演習，社会科学演習，理論的演習と，その基礎知識学習（事前），および，演習後の統合型学習の組合せからなる教育プログラムを用意する（図 2）.

2.1 基礎知識学習

情報セキュリティ・エンジニアとして身に付けるべきセキュリティ技術の基礎力として，OS，ソフトウェア，ネットワークなどのセキュアな構成技術，およびマルウェア対策に関する広範な知識・技術を習得する．基礎知識学習では，本事業で新たに連携大学共通の必修科目を用意するとともに，各連携大学のネットワーク関連，およびセキュリティ関連の基礎科目（所属大学指定科目）を活用する.

2.2 実践セキュリティ演習・PBL

産業界が求めるマルチタレント型の情報セキュリティ人材育成に向けて，情報セキュリティ分野全体で合計 10 から 20 程度の情報セキュリティに関する実践演習モジュールを用意する．実践演習モジュールは，技術実践演習，社会科学演習，理論的演習など，技術主体から社会科学主体まで，幅広いセキュリティ実践力をカバーするものであり，受講生は，所属大学の方針に従い，複数の演習モジュールを選択して受講できる．以下，演習モジュールの例を示す.

- Web アプリケーションセキュリティ検査演習（技術系）：Web サーバの構築や運用に必要となる Web アプリケーションセキュリティ検査の知識及び技術を習得し，独力で Web アプリケーションセキュリティ検査を実施できる基礎スキルを身につけることを狙いとする．具体的には，脆弱性を持つ Web サーバが設置された環境を利用し，主要な検査項目の実習を集中して行う.
- システム攻撃，防御演習 (技術)：脆弱性のあるシステムをインターネットに接続した場合，どのように攻撃されるのか，攻撃に対してどのように防御するのか等について理解する．具体的には，システムの攻撃によく利用される脆弱性や攻撃の原理，防御技術について概観し，実際の攻撃ツールを解析し，その原理を学ぶ．最終的に，実験結果をもとに安全なシステム運用の手法についてグループごとに議論，考察する.
- 情報セキュリティ演習 (理論)：暗号アルゴリズムの組み合わせにより，どのように暗号プロトコルを実現するかを説明し，実際に，最新情報セキュリティ理論で数式処理ソフトウェア Mathematica を用いて実装した暗号アルゴリズムを用いて，各種暗号プロトコルの実装を行う．さらに，RFID タグや携帯端末，VANET などの様々なアプリケーションで脚光を浴びている楕円曲線暗号について解説するとともに，最新情報セキュリティ理論で実装した暗号アルゴリズムを用いて，実際に楕円曲線暗号の実装も行う.
- 事業継続マネジメント演習（社会科学）：事業継続を可能とする管理体制を整備・運用するために必要な考え方，これに対応する IT のサービス継続について総合的な観点から学習する．さらに，企業をモデルとしたケーススタディにより，理解を深める．講義形式とケーススタディをもとに事業継続計画を策定する.

2.3 先進科目 (応用知識・CBL 等)

基礎知識学習と実践セキュリティ演習・PBL 等で養った実践力を補強するための統合的学習科目である．以下，学習の例を示す.

- 先進ネットワークセキュリティ技術：実社会での活動事例をベースに，実践セキュリティ演習にて体験的に習得したネットワークセキュリティ技術の実社会での役割と今後の技術展望や課題に

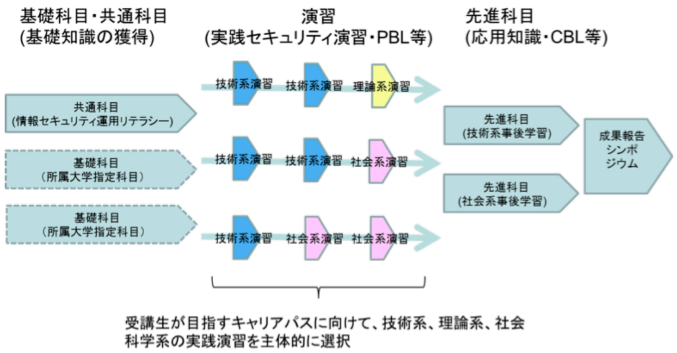

図 1　SecCap 学習プログラム

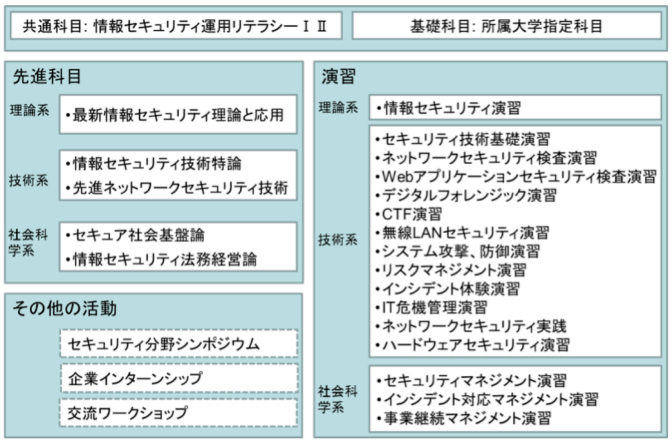

図 2　SecCap プログラムの学習フロー

ついて学ぶことにより，先進ネットワークセキュリティ技術について理解し応用力を深める．実社会での事例として，企業組織や官庁・自治体の内部で活動するネットワークセキュリティ事故対応チーム（CSIRT）と，セキュリティベンダー等が提供するセキュリティオペレーションセンター（SoC）を取り上げ，社会における役割と今後の課題について学ぶ．更に，インシデント対応とイベント分析の実践演習，フォレンジックの実践演習をとして知見を深める．

- セキュア社会基盤論：情報セキュリティに関する法律，経済，経営その他の社会基盤に関する基礎的な知識を習得すると同時に，情報セキュリティに関わる具体的な問題を解決する手法を，実際のインシデントに基づくケースやデータベースを利用しながら習得することを狙いとする．情報資産が格納されているパソコンの盗難，個人情報の漏洩，プライバシーに関わる情報の利活用などの具体的なインシデントや事例を想定し，これらに対してどのような法律の規定が適用され，先行事例に対してどのような判決が下されたのか，どのようなリスクがありどのようにマネジメントすることが可能か等について，各受講者が実際に調査する演習形式も取り入れ，取るべき対処の方法を具体的に立案する能力を習得していく．

2.4 その他

本教育プログラムでは，産業界の人材ニーズと育成プログラムのマッチングを強化するために，前節にて紹介した実践セキュリティ演習や講義を連携企業・連携組織と共同で開発し実施する．また，学生間・社会人（企業）間の人的ネットワーキングを醸成するために，セキュリティ実践力の腕試しの場としてCTF（Capture The Flag）への積極的な参加，企業インターンシップ，海外との交流，参加学生主体のセミナーの実施を予定している．

2.5 SecCap 認定

本教育コースでは，基礎知識学習のために新たに用意する「情報セキュリティ運用リテラシー（必修科目）と既存の科目の中から選定した「所属大学指定科目」)，演習 (実践セキュリティ演習・PBL 等)，および，応用学習のために用意する先進科目（応用知識・CBL 等）の所定単位を修了した学生には，実践セキュリティ人材の入り口に立てたことを示す称号「SecCap 認定」を授与する．

2.6 教員養成計画

- 連携大学の教員の取組み：若手教員を中心に，演習指導を通して情報セキュリティ分野での実践教育の進め方を体得する．また，基礎知識学習や事後の統合 CBL では，幅広い専門性を有する学内の教員が指導を分担し，連携大学それぞれの教育実績を本教育プログラムに活用する．
- 外部の人材の活用方法：連携企業においてセキュリティ業務を担当するエキスパート人材を招き，大学教員と共同で演習の開発・指導を実施することにより，外部人材の知見を大学教員が直接体得できる機会を増やす．また，連携大学，企業，有識者によるワークショップを開催し，コース認定や開発した実践演習について議論し，来年度の教育に反映するとともに，産業界が求める人材ニーズについての相互理解を深める．
- 夏季に集中的に実施する実践セキュリティ演習の期間に，連携大学以外の大学（参加大学）向けの実践演習ガイダンスと教員向け指導方法習得演習を実施し，外部人材の知見を連携大学外へも定着させることを目指す．
- 外部人材の知見をツールとして定着させるために，平成 28 年度には，実践演習のパッケージ化開発を行う．また，実環境利用型演習で用いる機材なども，順次，小型化・モジュール化し，個々の大学での導入・実施が容易になるように準備を進める．

2.7 実施体制

- セキュリティ分野全体の実施体制（図 3, 図 4)
  5 つの連携大学が中心となり，特徴ある多彩な演習と，そのための基礎知識学習，および応用学習からなる実践セキュリティ人材育成コース (SecCap コース) を用意する．その中で，実践力を体験的に身に付ける演習では，我が国のセキュリティ関連事業をリードする連携企業が，演習教材の開発を共同で行うとともに，実際の演習指導にも講師として参画する．また，学生の CTF イベントへの参加やインターンシップの受け入れについても支援いただく予定である．
- セキュリティ分野運営委員会
  5 つの連携大学の担当教員とスタッフによる分野運営委員会を構成し，平成 24 年度は SecCap コースウェアの基本設計，コースの修了認定の考え方を取りまとめ，平成 25 年度からの人材育成コース開講の準備を進め，現在，プログラムを実施中である．
- 連携大学と参加大学
  平成 24 年度から SecCap コースウェア開始に向けて，連携 5 大学間での単位互換協定を締結の準備を進めてきた．これにより，SecCap コースウェアとして 5 つの連携大学が分担して開講する基礎知識学習，実践演習，応用学習の講義と演習を，相互に履修できる体制とした．特に，コース認定の必修講義である基礎学習の科目は，奈良先端科学技術大学院大学と情報セキュリティ大学院大学の 2 か所で開講（遠隔講義形式）し，他連携大学の学生は，他科目の履修状況に合わせて選択できるようにした．参加大学は，各連携大学がホ

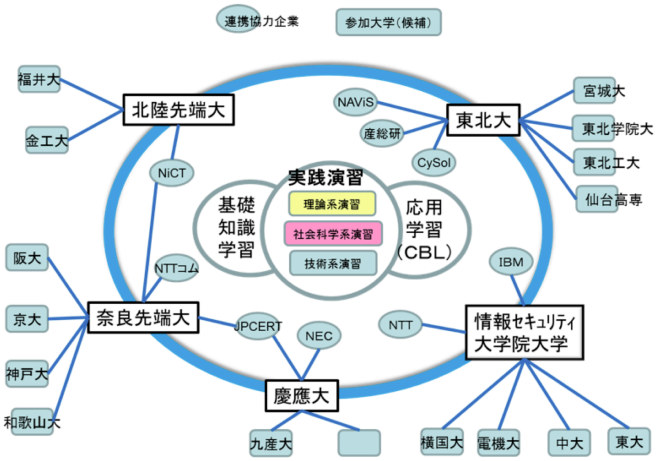

図 3　SecCap 実施体制 1

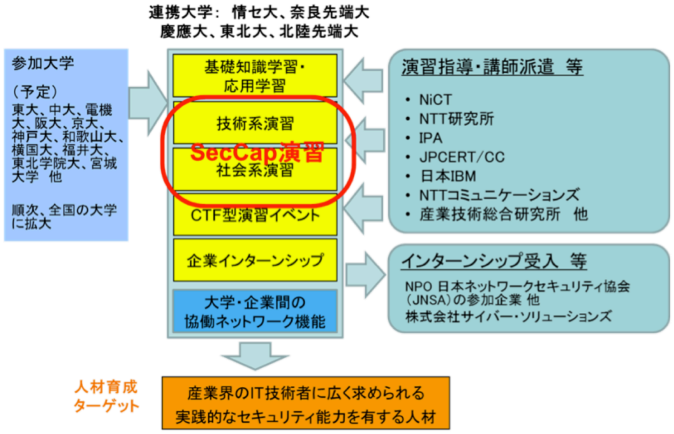

図 4　SecCap 実施体制 2

スト役となり，SecCap コースウェアを参加大学の学生に提供する体制とした．ホスト役の連携大学は，適宜，参加大学と（既存または新規の）単位互換協定等を結び，参加大学の学生が SecCap コースウェアの（一部の）講義や演習を受講できるようにするとともに，参加大学の学生の履修管理やコース認定について支援することとした．

3　まとめ

我々は，幅広い産業分野において求められている「実践的なセキュリティ技術を習得した人材（実践セキュリティ人材）の育成を目指し，5 つの連携大学が協力して開講する実践セキュリティ人材の育成コースであり，幅広いセキュリティ分野の最新技術や知識を具体的に体験的に習得することができるように SecCap コースウェアの設計を行った．技術面では，暗号をベースとする情報セキュリティ技術，Web サーバのセキュリティ技術，ネットワークセキュリティ技術から，法制度やリスク管理などの社会科学的な知識までをカバーする．具体的に，受講生は，技術系，理論系，社会科学系の講義や実践演習・PBL から，それぞれが目指すキャリアパスに沿った割合で，主体

的・自主的に調合した学習プログラムを作って受講することができる．さらに，人材育成を進めるだけでなく，その育成ノウハウを，全国の大学（参加大学）に広める活動を進めていくことを念頭に入れている．これにより，実践的な情報セキュリティ人材育成の枠組み自体を作り上げることができ，実践セキュリティ人材育成のすそ野を広げ，我が国全体が必要とする人材の育成体制を作り上げることができると考えている．なお，SecCap の詳細については，http://seccap.jp/ にて公開している．

謝辞 SecCap を運営するにあたり，慶應義塾大学 山内 正人先生，東北大学 本間 尚文先生，林 優一先生，菅沼 拓夫先生，北陸先端科学技術大学院大学 面和成先生，布田 裕一先生，陳 嘉耕先生，田中 覚先生，情報セキュリティ大学院大学 田中英彦学長，佐藤直先生，湯淺 墾道先生，橋本正樹先生，日向由美子様，enPiT 各拠点後担当者様，多大なる関係各所の方々からの協力をいただいている．なお，本プログラムは文部科学省 情報技術人材育成のための実践教育ネットワーク形成事業 (enPiT) による支援のもと運営している．ここに深く感謝する．