CL-004

セキュリティ教育指導者向け指導要領についての考察
Design of teaching guidelines for security instructors

千葉 寛之[†‡] 加藤 朗[†] 砂原 秀樹[†]
Hiroyuki Chiba Akira Kato Hideki Sunahara

1. はじめに

セキュリティが対象とする分野は、技術、非技術に限らず非常に広範囲にわたる。また、基礎理論からビジネスの現場での実践に関して多くの知見を身に着ける必要がある。

筆者等は、セキュリティ専門家人材育成において、その習熟度に応じた育成手法の整備についての研究を行っており、その中で、異なる分野においてそれぞれ高度なセキュリティ人材の育成を担っているセキュリティ専門家が、基本的なセキュリティ概念を共有し、それぞれの分野におけるセキュリティ問題についての解決スキルについて相互理解できる体系の整備を進めている[1]。これにより、セキュリティ指導者を支援するとともに、社会全体として共通認識をもってセキュリティの業務に取り組むセキュリティ人材の質的向上に寄与できると考えている。

本発表では、上記の考え方に基づき、セキュリティ指導者を支援する指導要領についての具体的な例を紹介し、実現における課題について論じる。

2. セキュリティ人材育成に関する現状

2.1 セキュリティ知識・スキル体系についての現状

セキュリティの知識体系の整備については、様々な取り組みが行われている。

JNSA の SecBoK[2] では、2003 年に公開された「情報セキュリティに関するスキルマップ」をベースに 2007 年に知識体系 (SecBoK) として整備されて以来、米国 NICE フレームワークとの整合をとるなど継続的に改訂されている。知識・スキル項目は、３段階のレベルに分類されている。ISC2 の CISSP8 ドメイン[3] は、セキュリティ資格 CISSP のスコープを示した体系として提示されている。

IPA は、IT 人材向けのスキル標準 ITSS に対して、強化すべきオプション項目として ITSS+「セキュリティ領域」[4] を策定。ITSS と同様にスキル項目とは独立した７つの共通レベルが適用されている。

情報処理学会では、2017 年にカリキュラム標準 J17[5] を策定、サイバーセキュリティに関しては側面的カリキュラム標準として素案が示されている。

日本シーサート協議会の「CSIRT 人材の定義と確保 Ver.2.1」[6] では、インシデントレスポンスに関わるセキュリティ人材を整理し具備すべきスキル項目を提示している。

NEC、日立、富士通による統合セキュリティ人材モデル[7] は、米国 NICE フレームワークの分類を用いて、実際に企業の現場で定義されているセキュリティ人材との対応付けを整理している。

米国では、NIST の NICE フレームワーク[8] が, セキュリティ人材のリファレンスとして職務役割 (Work role) に対して、業務 (task)、知識 (knowleage)、スキル(skill) が定義され、人材育成や採用において参照されている。ただし、記述レベルが抽象的という特徴がある。

以上、様々な知識体系が整備され活用されているが、主に中上級のセキュリティ人材が習得すべきスキル項目が示されていること、初学者が学ぶべき基礎概念から高度な知識・スキルへのレベルアップの連続性を俯瞰した体系は未整備である。

2.2 セキュリティ人材育成施策の現状

セキュリティ人材育成に関する施策に関しても、様々な取り組みが行われている。

enPiT[9] では、サイバーセキュリティに関する実践的な内容を含む教育講座を、複数の大学間で単位取得を含めて連携し、大学院生向け、学部生向け、社会人向けに対して人材育成を推進してきた(2021 年から自主運営)。

東京電機大学の CySec[10] は、サイバーセキュリティの上級技術者や CISO を目指す社会人を対象に、技術系および非技術系を含めた教育講座を提供し、履修証明書を発行している、

セキュリティキャンプ[11] や SecHack365[12] は、主に若年層を対象に次代を担うセキュリティ人材を発掘・育成することを目的に、高度なセキュリティ技術を推進している。

産業サイバーセキュリティセンター(ICSCoE) の中核人材育成プログラム[13] では、社会インフラや産業基盤におけるセキュリティ人材を育成するため、企業からの派遣形式による１年間のトレーニングを実施、OBOG によるコミュニティも推進している。

実践的サイバー防御演習 CYDER[14] では、主に地方公共団体や国の機関の担当者向けにインシデント対応をロールプレイ型の演習による訓練教育を実施している。

これらの国内の取組みは、演習や体験を重視したより実践的な教育内容が重視され、様々な演習形式が提供されている。ただし、様々な演習形式が独自に運営されており、そこで習得できる知識やスキルについては、受講生に依存しているのではないかと考える。

米国においては、NICE フレームワーク[8] が広く参照され、米国国家安全保障局により Centers of Academic Excellence in Cybersecurity(CAE) プログラム [15] として、サイバーセキュリティ人材を育成する大学のプログラムを認可する制度が運営されており、各大学が独自のプログラムを提供している。

† 慶應義塾大学 Keio University
‡ 株式会社日立製作所 Hitachi, Ltd.

3. 習熟過程を考慮したセキュリティ人材育成モデル

筆者らは、社会全体として有効なセキュリティ人材育成を推進するために、専門分野を含む多種のセキュリティ人材の習熟プロセスを俯瞰し、セキュリティ人材を育成するための要件を整理し、それを実現する人材育成モデルを提唱している[1]。人材育成モデルは、知識・スキル体系を定義する心技体モデル、習得プロセスを定義する守破離モデルから構成される。

3.1 人材育成モデルについての要件

前述した既存のセキュリティ人材育成施策を踏まえて、以下の課題を設定する。

知識スキル体系については、様々な知識スキル体系に対して、横断的に俯瞰する視点を設定する。そのためには、基本となるセキュリティ概念を整理した上で、多岐に渡るセキュリティ関連分野を俯瞰する視点が必要となる、俯瞰的な視点には、倫理等の非技術分野も含める必要がある。また、基礎となる普遍的な知識スキルと技術の進化や最新動向に合わせてアップデートすべき知識スキルを整理する必要がある。

育成施策については、演習や体験形式によるスキル獲得を中心に、座学による知識習得やワークショップ形式による議論等を踏まえて、習熟レベルに応じた育成モデルを整備することにより、人材育成を見える化する。また、習得する知識スキルの到達目標として、実際に行われているセキュリティに関する業務への適用について明示することで、育成の内容の有効性を確認できるようにする。これにより、セキュリティ人材育成における指導者が、人材育成を実施する上で必要な視点を提供することにより、指導者をサポートすることを可能とする。

以上を踏まえた、セキュリティ人材育成モデルについての要件を以下とする。

(1) セキュリティの本質的な概念と、多岐に渡るセキュリティ分野の関係が整理されていること

(2) 普遍的な知識スキルと最新動向に合わせてアップデートすべき知識スキルが整理されていること

(3) 多岐に渡るセキュリティ人材の業務における問題構造の整理と必要スキルが明示されていること

(4) 本質理解から実業務における問題解決スキルの習得に至る習熟過程がモデル化されていること

(5) 習熟過程におけるセキュリティ指導者の支援と育成方法が明示されていること

3.2 心技体モデル(知識・スキル体系)

心技体とは本来、武道やスポーツにおいて、精神、技術、体格を意味するとされており、倫理面を含めた基礎から応用までを包含する体系として、整備する(表１)。

表１　心技体モデル

分類	内容	整備、取得のための環境・道具
【心】 マインド・倫理	信念・モチベーション セキュリティに関する倫理	モチベーションや倫理意識を維持できるコミュニティ・イベント
【体】 普遍的な知識・スキル	基本概念 原理・セキュリティの目的定義 IT基本知識 基本ツール利用スキル	背景・概念が整理された良質なリファレンス（知識体系）
【技】 業務毎の問題解決スキル	業務毎に定義された問題構造定義 問題解決スキル	最新脅威動向、最新技術(活用) 制度等最新動向のアップデート

心は、セキュリティ人材として身に着けておくべき信念や心構えを示すものであり、倫理に関する素養もここに含まれる。単に倫理だけではなく、セキュリティ人材としてのモチベーションを持つための思考や自身を客観的に観察する視点も含めることが必要と考えている。表２に「心」の例を示す。

表２　心技体モデル「心」

型	分類	教育内容（例）
心：	マインド	・前向き思考を支える世界観 ・ハッカー的思考 ・自身の認知バイアスの理解
	セキュリティに関する倫理	・倫理についての自覚 ・倫理的な行動をするための心構え ・倫理に反する行動の要因理解 ・順守すべき法制度 ・明文化されていないモラル意識
	好奇心に基づく理解	・ブラックボックスを作らない理解プロセス ・対象分野や前提に基づく理解 ・対象分野や前提が異なる概念の識別

体は、セキュリティ人材に広く必要な普遍的な知識・スキルとし、セキュリティに関する基本的な概念や IT に関する理解、さらに実践で扱う基本的なツールに関する知識・スキルを含むものとする。表３に「体」び例を示す。

表３　心技体モデル「体」

型	分類	教育内容（例）
体：	基本概念・原理	セキュリティの本質理解、リスク概念、要素技術
	セキュリティ基礎知識	セキュリティマネジメント基礎、インシデントレスポンス基礎、マルウェア基礎、etc.
	IT基本知識	ITに関する知識(情報理論、計算機アーキテクチャ、OS、NW、プログラミング、etc.)
	基本ツール利用法	知識を活用して作業を行うために必要なツールの一般的な操作方法

技は、最新動向を踏まえて変化する最新の知識・スキルとし、実際にセキュリティに関する業務に取り組む際に必要となるスキルを含むものとする。技は、セキュリティに関して行われる実際の業務の単位で整理され、それぞれの業務において、解決すべき問題構造を示すことを特徴とする。これにより、身に着けた知識・スキルが実際の業務にどのように活用され役立つことができるかを学ぶことができる。

表４　心技体モデル「技」

型	分類	教育内容（イメージ）
技：	インシデントレスポンス	問題構造 「テーマ(解決する課題・問題)」 「ゴール(解決状態)」 「手順・方法」 「必要スキル」 「評価方法」 ケーススタディによる実践
	セキュリティ監査	
	脅威分析	
	フォレンジック	
	マルウェア解析	
	セキュリティマネジメント	
	セキュア開発	

3.3 守破離モデル(習得プロセス)

守破離は、千利休の教えから、茶道や武道などにおける修行の段階を示したものであり、反復や試行錯誤を繰り返すことによって次の段階に進むというニュアンスがあり、知識スキルを習得するプロセスを提示している。

守は、基本的に、反復等により習得する段階であり、セキュリティ概念理解、要素技術の理解、基本的なツールの習得を含む

破は、演習や体験形式により、習得した知識スキルを適用する段階であり、実際の業務における問題構造を理解して、試行錯誤を伴い習得する段階である。

離は、自らが習得した知識スキルをベースによりよい問題解決のやり方を考える段階である。

表５　守破離モデル

段階	習得スキル	習得方法	実現のためのリファレンス
【守】	・概念理解 ・要素技術 ・ツール	座学、自習 自身の言葉での説明(論述、面接、ワークショップ)	導出過程を含めた良質の知識体系
【破】	・業務毎(※1)に定義された問題解決能力	演習形式によるスキル取得 ・シナリオ演習 ・ワークショップ	実問題の問題構造の定義 実務と知識スキルのマッピング
【離】	・問題解決手法の開発、進化 ・新分野における手法の確立	有識者コミュニティにおける議論・フィードバック	セキュリティコミュニティにおける共有手段

3.4 セキュリティ人材育成における習熟プロセス

心技体モデルと守破離モデルを用いることにより、 セキュリティ人材の育成を推進する。典型的なセキュリティ人材の育成プロセスを以下に示す(図１)。

(１) 心×守フェーズ
倫理や心構えに関して学ぶ段階である
(２) 体×守フェーズ
基本的な概念や要素技術を理解する段階である
(３) 技 (体) ×破フェーズ
習得した知識スキルを用いて、演習形式により問題解決を体験する段階である。

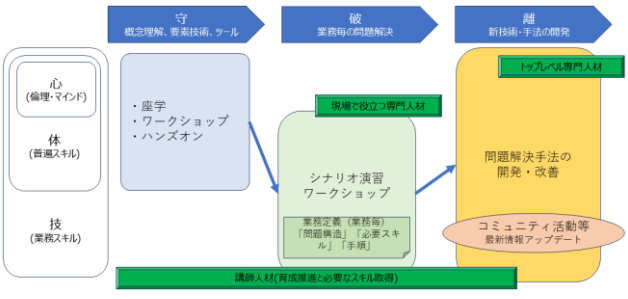

図１　心技体×守破離による習熟プロセス

4. セキュリティ人材育成における指導者の課題

セキュリティ人材育成を担う指導者は、セキュリティ人材育成を推進する上で重要な役割を担っており、その育成は重要な課題である。

ただし、教育対象分野が広いため、一人の指導者がすべての分野を把握することはできない。そのため、異なる分野のセキュリティ専門家が他の分野についても分担して推進している現状にある。ある分野のセキュリティ専門家であることから、他のセキュリティ分野についての理解が期待されるが、属人的な状況にある。

そこで、特定の分野のセキュリティ指導者が他のセキュリティ分野の教育を行うことを支援する仕組みを検討する。セキュリティ指導者を一から育成するよりも効果的であり、セキュリティ指導者間の共通認識を醸成することで、将来的には、セキュリティ指導者のコミュニティにより次代のセキュリティ指導者の育成に寄与することも考えられる。

特に実際に手を動かす演習形式の人材育成は有効であり盛んにおこなわれているが、単に見よう見まねで経験をするだけではなく、何を習得するかの指針を与えることができれは、教育効果が向上すると考える。

5. 指導者向けガイドラインの設計

ここでは、特定のセキュリティ分野について、セキュリティ指導者に対して広義の指導要領として提示すべき内容を整理する。ここでは、習熟プロセスのうち、技(体)×破フェーズを想定する。

「前提知識」として、心技体モデルの「心」および「体」を含む。「心」「体」は、セキュリティ人材に共通の知識・スキルである。さらに、教育対象分野に該当する「技」の知識・スキルを含める。「技」には、前述した通り、対象領域において解決すべき問題構造が示されており、教育によって身に着ける知識・スキルが実用的なレベルであることを支援する。

「教育コンテンツ」は、教育を行う際の一般的なテキスト、ツール、環境を含む。既存の教育コンテンツを扱うことも可能である。

「教育プロセス」は、守破離モデルの「破」に基づくプロセスを定義する。

「指導に関するメタ知識」では、教育コンテンツに直接表記されないが、教育を実施した際の効果や影響についての情報を提供する。うまくいかなかった例や、前提知識が不足していた場合に、どのような影響が発生するのか、教育の実施前後で、どのような違いが期待できるか等である。

表５　指導者向けガイドライン（例）

項目	内容（例）
前提知識	心技体モデルの「心」「体」及び、教育対象項目に該当する「技」
教育コンテンツ	演習形式の教育 ・教育テキスト、ツール、環境
教育プロセス	守破離モデルの「破」に基づいた、演習形式の教育プロセス
指導に関するメタ知識	・問題解決の良い例、悪い例 ・特定の前提知識不足の影響範囲 ・演習の結果得られる経験

6. おわりに

本発表では、習熟度を考慮したセキュリティ人材育成モデルに基づき、セキュリティ人材育成を担う指導者に提供する指導要領を整備するための考え方を提示した。

今後は、既存の教育施策に対する適用を通じて、セキュリティ指導者をより適切に支援する仕組みとして整備していきたい。

謝辞

本研究は、慶應義塾大学大学院メディアデザイン研究科のドクターコースにおける研究として取り組みを開始したものであり、セキュリティに限らず教育分野に関わるメディアデザイン研究科の先生やメンバの方々に感謝したい。また、これまでにセキュリティ人材育成や教育に関して、ご指導を受けたすべての方々に感謝するとともに、本研究の今後の推進に引き続きご指導を賜りたいと考えている。

参考文献

[1] 千葉寛之、加藤朗、砂原秀樹、 “習熟過程を考慮したセキュリティ人材育成モデルの構想”、 DICOMO2025。
[2] 特定非営利活動法人日本ネットワークセキュリティ協会. セキュリティ知識分野（secbok）人材スキルマップ. https://www.jnsa.org/result/skillmap/, 2021. Accessed on May 20, 2025.
[3] ISC2. CISSP CBK8 ドメイン. https://japan.isc2.org/cisspgaiyou.html. Accessed on May 20, 2025.
[4] 独立行政法人情報処理推進機構. Itss セキュリティ領域. https://www.ipa.go.jp/jinzai/skill-standard/plus- it-ui/itssplus/security.html, 2020. Accessed on May 20,2025.
[5] 一般社団法人情報処理学会. カリキュラム標準 j17. https://www.ipsj.or.jp/annai/committee/education/j07/curriculum j17.html, 2017. Accessed on May 20, 2025.
[6] 一般社団法人日本シーサート協議会. CSIRT 人材の定義と確保 ver.2.1. https://www.nca.gr.jp/activity/PDF/recruit- hr20201211.pdf, 2020. Accessed on May 20, 2025.
[7] ＮＥＣ，日立，富士通. 統合セキュリティ人材モデル. https://www.hitachi.co.jp/New/cnews/month/2018/10/1024.pdf, 2018. Accessed on May 20, 2025.
[8] NIST. Nice framework: Current ver-sions. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions, 2025. Accessed on May 20, 2025.
[9] enPiT. enpit security. https://www.seccap.jp/gs/index.html,2020. Accessed on May 20, 2025.
[10] 東京電機大学. Cysec: 国際化サイバーセキュリティ学特別コース. https://cysec.dendai.ac.jp/, 2014. Accessed on May 20, 2025.
[11] 独立行政法人情報処理推進機構. セキュリティ・キャンプ. https://www.ipa.go.jp/jinzai/security- camp/index.html, 2025. Accessed on May 20, 2025.
[12] 独立行政法人情報通信研究機構. Sechack365. https://sechack365.nict.go.jp/, 2025. Accessed on May 20, 2025.
[13] 独立行政法人情報処理推進機構. 中核人材育成プログラム. https://www.ipa.go.jp/jinzai/ics/core human resource/index.html, 2025. Accessed on May 20, 2025.
[14] 独立行政法人情報通信研究機構. 実践的サイバー防御演習 cyder. https://cyder.nict.go.jp/index.html, 2025. Ac- cessed on May 20, 2025.
[14] NSA. National centers of academic excellence. https://www.nsa.gov/Academics/Centers-of-Academic- Excellence/, 2025. Accessed on May 20, 2025.