実践的情報セキュリティ人材の育成の取り組み ～その成果と課題・展望～

キーワード；情報セキュリティ，人材育成，産学連携，実践的演習，ゲーミフィケーション

長谷川長一[†1]
ラック [1]

1. はじめに

ネットワークや情報システムの複雑化，サイバー攻撃の増加や巧妙化などの背景から，実践的情報セキュリティ人材の育成が急務かつ大きな課題となっている．この解決のために取り組んでいる教育手法やその具体的事例を取り上げる．

2. 人材育成の取り組み

2.1 演習の設計

実践的情報セキュリティ人材の育成においては，ネットワーク環境を利用したグループ演習形式が用いられることが多い．その設計の際に，「経験学習モデル」「アクティブラーニング」，シリアスゲームの評価指標の「RETAIN モデル」等を参照している．

また，実際に発生したサイバー攻撃や障害等を基に，脅威やインシデントのシナリオを作成し，ケーススタディや実機を利用した演習を設計している．

表 1　アクティブラーニングのプロセス

段階	概要
ステージ 1	問題の理解と問題の再定義（真の問題は何かを考え，定義する）
ステージ 2	目標の設定と標準化（目標を設定し，それをグループや組織のものとする）
ステージ 3	行動計画の作成と検証（行動計画を作成し，具体的な段取りをつけ，検証する）
ステージ 4	実行とリフレクション（具体的に行動し，その結果をグループで省察する）

2.2 演習の実施と評価

演習を実施するにあたっては，そのためのネットワークやシステム環境を構築し，実施してきた．これらは，デジタル化や授業のハイフレックス化等の様々な環境変化に適応した運用管理を行っている．

また，経験学習やアクティブラーニングの観点（特に振り返りとフィードバック）から，実施内容を記録，測定，評価を効率的かつ効果的に行えるシステムとして，設計・開発されている．[1]

2.3 取り組みの事例

このような教育を実施するにあたっては，様々な取り組みが長年行われてきた．産学連携では大学・大学院における「分野・地域を越えた実践的情報教育協働 NW(enPiT)」 のセキュリティ分野(enPiT-Security)［2］，国立高専における「Society5.0 型未来技術人財育成事業（Conpass5.0）」［3］，「KOSEN サイバーセキュリティ教育推進センター(K-SEC)」[4]等である．その中で，ゲーミフィケーションを取り入れた「CTF」「情報危機管理コンテスト」等のコンテストイベントや，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(JNSA)のゲーム教材（「セキュリティ専門家人狼」「Malware Containment」）［5］を利用したもの等もある．その他にも，情報セキュリティ分野と IoT 分野，AI 分野の組み合わせた演習(高専での「海事サイバーセキュリティ演習」)等，幅広く取り組みを行っている．

3. おわりに

これからの課題として，以下の項目を挙げたい．

- 変化(セキュリティ分野の知識・技術,デジタル化等)への適応
- 実践的教育のできる「ファシリテーター」の育成
- 組織連携の強化
- 測定と評価プロセスの強化

最後に，今後の継続的取り組みとその成果に，期待していただければと思う．

参考文献

［1］情報処理学会論文誌 デジタルプラクティス 63 号，「実践的人材を育てる情報セキュリティ演習の設計と実施」中川慶祐，長谷川長一，藤本章宏，吉廣卓哉，川橋裕，(2025-07-15)
https://www.ipsj.or.jp/dp/contents/publication/63/
［2］「分野・地域を越えた実践的情報教育協働 NW(enPiT)」 のセキュリティ分野(enPiT-Security)
https://www.seccap.jp/
［3］独立行政法人国立高等専門学校機構：高専発！「Society 5.0 型未来技術人財」育成事業（GEAR 5.0／COMPASS 5.0)
https://www.kosen-k.go.jp/nationwide/gear5-0-compass5-0
［4］独立行政法人国立高等専門学校機構 KOSEN サイバーセキュリティ教育推進センター
https://www.kosen-k.go.jp/Portals/0/K-SEC/
［5］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 教育部会 ゲーム教育ワーキンググループ
https://www.jnsa.org/edu/secgame/index.html

†1 CHOICHI HASEGAWA LAC Ltd.