Vol.2021-IS-156 No.9
2021/6/5

# 社会人向けサイバーセキュリティ講座「セキュアシステム設計・開発」の実践

柿崎 淑郎[1,a)]　寺田 真敏[1]

**概要**：東京電機大学では，2015 年より，社会人を対象とした学び直し講座として，国際化サイバーセキュリティ学特別コース “CySec” を開講しており，2020 年度末までに 309 名の受講生を受け入れ，155 名の修了生を輩出している．本稿では，CySec の一科目である “セキュアシステム設計・開発” の実践について紹介する．なお，本取組は情報システム教育コンテスト ISECON2020 において，優秀賞を受賞した．

## 1. はじめに

東京電機大学では，2015 年より，社会人を対象とした学び直し講座として，国際化サイバーセキュリティ学特別コース “CySec” を開講しており [1]，2020 年度末までに 309 名の受講生を受け入れ，155 名の修了生を輩出している．CySec は履修証明プログラム[*1]であり，開講している 7 科目すべてを修了した受講生には，学校教育法第 105 条に基づき，履修証明書が交付される．

本稿で紹介する “セキュアシステム設計・開発” は，CySec で開講している 7 科目のうちの 1 つであり，システム開発プロセスにおける各段階におけるセキュリティ対策について，演習を通して学ぶ，演習中心科目である．

システムをセキュアにする方法は大きく分けて 2 通りある．1 つは，セキュリティを十分に意識せずに作られたシステムに対して，脆弱性診断などを行い，問題箇所を改修することでセキュアなシステムにする方法，もう 1 つは，当初からセキュリティを意識し，セキュリティ・バイ・デザインの考え方でシステム構築を行う方法である．本実践では，システム開発プロセスの V モデルに従って，その各段階におけるセキュリティ対策を要件定義，設計，実装，テストと一連の流れに沿って，実践的に学修することで，セキュリティ・バイ・デザインによるセキュアなシステム設計および開発ができるようにすることを目標としている．

## 2. 国際化サイバーセキュリティ学特別コース CySec

内閣サイバーセキュリティセンター（NISC）の情報セキュリティ政策会議において，2013 年に「サイバーセキュリティ戦略」が初めて示された．その中では，「サイバーセキュリティ立国」の速やかな実現が期待として示されている．その後，2014 年にはサイバーセキュリティ基本法が成立し，日本におけるサイバーセキュリティの意識は急速に高まっていった．

この国家的要請に対し，東京電機大学は，文部科学省の平成 26 年度「高度人材養成のための社会人学び直し大学院プログラム」に対し，「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」を提案し，採択され，平成 26 年度（2014 年度）から平成 28 年度（2016 年度）まで支援をいただきながら，社会人を対象とした学び直し講座として，国際化サイバーセキュリティ学特別コース “CySec” を 2015 年度に開講した．

CySec は履修証明プログラムであり，開講している 7 科目（2015 年度から 2017 年度までは 6 科目）すべてを修了した受講生には，学校教育法第 105 条に基づき，履修証明書が交付される．また，文部科学省の職業実践力育成プログラム（BP）[*2] に当初より認定されており，厚生労働省の教育訓練給付制度の対象にもなっている．

CySec の 7 科目は，東京電機大学大学院未来科学研究科の自由履修科目として設置されており，社会人のみならず，未来科学研究科の修士生，他研究科の修士生も受講することができ，サイバーセキュリティを学ぼうとする者を広く受け入れいている．

開講科目は，体系的に学べるように，国際的な情報セキュリティ・プロフェッショナル認定資格である CISSP (Certified Information Systems Security Professional) の共通知識体系を基本としたカリキュラムを採用し，CISSP

[1] 東京電機大学
[a)] kakizaki@isl.im.dendai.ac.jp

[*1] https://www.mext.go.jp/a_menu/koutou/shoumei/

[*2] https://www.mext.go.jp/a_menu/koutou/bp/index.htm

を主催する (ISC)[2] の教育機関向けプログラムである International Academic Program (IAP) の日本国内で唯一のコース[*3]である．

受講生の知識を均一化し，ベースライン化のために，CISSP 講座として，サイバーセキュリティ基盤 I，II の 2 科目を開講している．また，法律・経済・外交・心理・倫理等の幅広い関連知識を学修するために，座学中心科目として，セキュリティインテリジェンスと心理・倫理・法，情報セキュリティマネジメントとガバナンスの 2 科目を開講している．さらに，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修得するために，デジタル・フォレンジック，サイバーディフェンス実践演習，セキュアシステム設計・開発の 3 科目を開講している．特に，演習中心科目であるサイバーディフェンス実践演習とセキュアシステム設計・開発については，隔週土曜日に 3 コマを集中的に学ぶことで，演習時間を確保することに留意している．

## 3. セキュアシステム設計・開発

“セキュアシステム設計・開発” では，システム開発プロセスの V モデルに従って，その各段階におけるセキュリティ対策を要件定義，設計，実装，テストと一連の流れに沿って，実践的に学修することで，セキュリティ・バイ・デザインに基づくセキュアなシステム設計および開発ができるようにすることを目標としている．

セキュアシステム設計・開発の単元は，毎年度見直しており，開講年度によって少しずつ異なっているが，2019 年度は以下の構成で実施された．

**総論**

本科目を俯瞰し，何のために何を学ぶのかを明確にするために，セキュリティ・バイ・デザインの考え方，関連するガイドラインやベストプラクティス，セキュリティ開発ライフサイクル（SDL）について紹介する．

**セキュアプログラミング（ネイティブアプリケーション）1, 2**

Visual Studio を用いて C 言語で作成される Windows アプリケーションの安全な実装について，バッファオーバーフロー（BOF）が発生するメカニズムと実際の対処法を学ぶ．

**セキュアプログラミング（Web アプリケーション）1, 2**

PHP で作成された Web アプリケーションを題材にして，クロスサイトスクリプティング（XSS），SQL インジェクション（SQLi），クロスサイトリクエストフォージェリ（CSRF）などの脆弱性が含まれたサンプルアプリケーションを解析しながら修正し，脆弱性への対応と安全な実装について学ぶ．

**セキュアインフラ構築（ネットワーク）**

ネットワークインフラをセキュアに構築するために，サイバー攻撃手法の変遷を概観し，サイバー攻撃のモデル化とその対処方法を学ぶとともに，脆弱性の深刻度を評価する指標について学修する．

**セキュアインフラ構築（サーバ）**

セキュアなサーバインフラの構築法を学ぶために，サーバに対するサイバー攻撃とその対応，ソフトウェアファイアウォールの正しい設定方法，SELinux の利用方法などを学び，サーバ堅牢化手法について学修する．

**セキュリティ脅威分析 1, 2**

具体的な例題に対する脅威情報の収集と分析について，データフロー図，脅威ツリー，脅威分類体系 STRIDE，脅威影響評価 DREAD，脅威モデリングツールなどによって演習を通して学ぶ．

**プロジェクト・マネジメント演習**

システム開発を行う上で重要なプロジェクト・マネジメントにおいて，セキュリティの視点を含めた演習を行う．

**セキュリティ要求仕様と分析手法 1, 2**

セキュリティ・バイ・デザインを実現するために，脅威分析，被害分析，攻撃分析，ミスユースケースを演習し，学修する．

**開発手法コモンクライテリア（ISO/IEC 15408） 1,2**

IT 製品や情報システムに対して，情報セキュリティを評価し認証するための評価基準であるコモンクライテリア（ISO/IEC 15408）について，特に，セキュリティターゲット，セキュリティ保証要件，セキュリティ機能要件を演習によって学修する．

## 4. 本取組の特徴

本取組では，システム開発プロセスの V モデルに従って，要件定義，設計，実装，テストなどの各段階におけるセキュリティ対策を実践的に学修することで，セキュリティ・バイ・デザインによるセキュアなシステム設計および開発ができるようにすることを目標としている．

システム開発において，V モデルで示される上流工程と下流工程は異なる業務として認識されており，それぞれ異なる担当者が独立したスキルで対応することが多い．そのため，V モデルの段階間におけるコミュニケーションにおいては，プロジェクトマネージャが重要な役割を果たす．

セキュリティ分野においても，設計開発，運用，分析は，異なる業務として認識されており，独立したスキルであると理解されており，それぞれの分野に特化したスキルは有していても，隣接分野には知識が乏しいことは珍しくない．この背景には，セキュリティの学問体系が十分に成熟しておらず，また，実務で活躍している現役社会人の多くは，学生時代にセキュリティを専門とした教育を受けていないことが挙げられる．このような世代の学生時代には，セキュ

[*3] 2020 年 6 月時点において

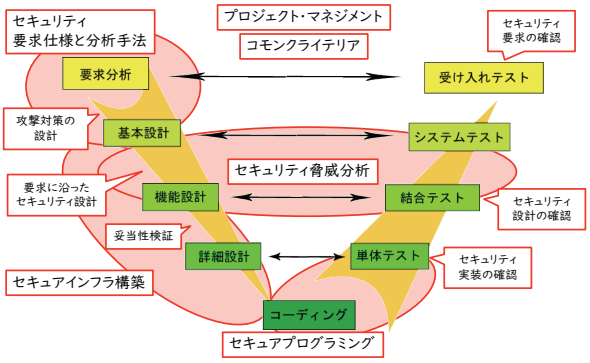


**図 1** 各単元と V モデルの対応

リティはネットワークの文脈で学ぶことが多く，ネットワーク系科目の 1 単元としてセキュリティが扱われる程度である．そのため，現役社会人は，業務に必要なセキュリティの知識を業務の中から獲得していることが多い．つまり，自らが業務で扱う範囲のセキュリティに関する知識はしっかりと獲得していても，その周辺や隣接分野のセキュリティに関する知識を十分に保有していない現状がある．

本取組では，システム開発の V モデルに沿って，一連の流れを演習することで，隣接分野への理解を醸成し，分野間コミュニケーションができる人材を育成する．図 1 にセキュアシステム設計・開発の各単元とシステム開発の V モデルの対応を示す．V モデルの各段階におけるセキュリティ対策を学ぶことで，視野が広がり，自らの専門分野における取り組みを見直すきっかけにもなる．また，V モデルの各段階でのセキュリティを徹底することで，システム全体の堅牢性が向上し，セキュリティ・バイ・デザイン，システム開発ライフサイクルの考えを元にしたリスクマネジメントとセキュリティ対策コストの見積もりもできるようにカリキュラムを構成している．

CySec は 30 代から 40 代中盤の受講生が大半であり，これからのキャリアアップを目指す上で，知識体系や学問体系に基づいた学修は効果的である．特に，セキュリティエンジニアの受講生にとっては，実務に直結する内容であり，受講生の満足度は高い．また，本取組だけの成果ではないが，修了生の中にはキャリアアップや転職に成功した例があり，特に，ベンダ系講座よりも大学の学問体系で学修したことが高く評価されている．

## 謝辞

本取組を支えていただいている CySec 講師のみなさま，CySec に関連するスタッフのみなさまに感謝いたします．

### 参考文献

[1] Kaikizaki, Y., Sasaki, R., Okochi, T. and Yasuda, H.: CySec: Cybersecurity Review Program for Professionals in Japan, *Advances in Networked-Based Information Systems. NBiS 2020. Advances in Intelligent Systems and Computing*, Springer, pp. 280–289 (online), DOI: 10.1007/978-3-030-57811-4$_2$6(2020).