INSTITUTE of INFORMATION SECURITY

【文部科学省「成長分野を支える情報技術人材の育成拠点の形成(enPiT)enPiT-Pro」選定】

2024 年度 情報セキュリティプロ人材育成短期集中プログラム（ProSec）

IoT セキュリティコース
― サプライチェーンからホームセキュリティまで ―

「IoT セキュリティコース」は、文部科学省「成長分野を支える情報技術人材の育成拠点の形成（enPiT）enPiT-Pro」に選定された「情報セキュリティ人材育成短期集中プログラム（ProSec）」に基づいて、情報セキュリティ大学院大学が開講する社会人向け集中コースとして提供しています。

本コースは、2 つの講座をセットにして提供します。それぞれ、講義とハンズオン方式の技術演習を組み合わせており、実践的な知識と技術の習得が可能です。2 つの講座は、それぞれ単独で受講いただけます。

2024 年度は、情報セキュリティ大学院大学にてオンサイトで開講いたします（ただし、今後の状況判断により変更となる可能性があります）。
〒221-0835 横浜市神奈川区鶴屋町 2-14-1 202 教室
（ＪＲ横浜駅より徒歩３分）

- **IoT-1： IoT 基礎セキュリティ［6 月 5 日（水）］**（1 日間、6 時間）
  - ✧ IoT の概念、IoT セキュリティ概観、IoT 関連法制度、ハードウェアセキュリティ、信頼の起点 、IoT ネットワーク、IoT の運用と規格、国際標準、認証(講義)
- **IoT-2： IoT 脆弱性検査［6 月 6 日（木）］**（1 日間、6 時間）
  - ✧ スマートホームの脆弱性検査（技術演習）

※最少開講人数 6 名

現代社会はインターネットを通して家庭のテレビやエアコンばかりでなく、工場の制御機器や町中の監視カメラなど多くの機械が繋がっています。これらは便利な反面、外部からの攻撃にさらされてセキュリティ管理が製品提供側はもちろん、使う側でもセキュリティ対応が求められるようになっています。本コースは開発する企業、販売する企業、活用する企業に最適のセキュリティコースです。サプライチェーンからホームセキュリティまでを対象にし、SBOM、TEE など安全保障のために活用が見込まれる技術の紹介も行います。法制度が進むヨーロッパの CRA: Cyber Resilience Act や国内の IoT 製品セキュリティ適合性評価制度なども含めて、IoT を担当する場合に考慮すべきセキュリティについて、講義と演習を

行います。マネージャクラスの方にとっての IoT への入門講座としても受講いただけます。

なお、本コースはその時々の専門知識や新しいサイバー攻撃に対応した特定のスキルを短期間で学ぶ、社会人集中コース（ProSec）として開講しております。また、ProSec プログラムでは、本学及び連携大学(東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学)提供の ProSec コースと組み合わせて、クイックコース修了認定を目指すこともできます。2021 年度以降に ProSec コースを受講されていた場合、授業・演習の内容によっては、修了認定の対象となりますので ProSec 事務局にお問合せください。

情報セキュリティ大学院大学
情報セキュリティ研究科長
大久保　隆夫

IoT-1：IoT 基礎セキュリティ（1 日間、6 時間）

● 前提知識

共通鍵暗号と公開鍵暗号の区別など暗号やプロトコル、またネットワークの基礎知識、および組み込みシステムに関する基礎知識を前提とします。
内閣府 SIP CPS プロジェクトで作成した「サイバー・フィジカル・セキュリティ対策検討ガイドブック」の１章と２章について議論するので読んでおくことを前提とします。
PDF https://www.nedo.go.jp/activities/ZZJP_100235.html

● 講座の目標と到達レベル

IoT のビジョンとアーキテクチャを従来型の IT と比較しながら考察し、その違いによって生じる IoT のセキュリティリスクを理解し、ハードウェアの信頼の起点からフォグコンピューティングに至る安全なシステムの構成法を学修します。また、IoT の国際標準、IoT システムサービスを運用する基礎知識を習得します。

● スケジュール

[IoT-1：IoT 基礎セキュリティ]

日程		時 限	内 容
6 月 5 日	水	09:30～16:50	・IoT セキュリティ:IoT のビジョン、M2M の増大、 IoT セキュリティ事例、MIRAI マルウェア ・IoT デバイスのアタックサーフェス: IoT デバイスのアーキテクチャ、サイドチャネル攻撃、耐タンパー性、信頼の起点、TEE、Trustzone ・制御システムセキュリティ: センサーに対する攻撃、Stuxnet ・IoT の運用と規格：ログ、ソフトウェア更新、SBOM、国際標準

※内容の詳細は変更される可能性があります。

IoT-2：IoT 脆弱性検査（1 日間、6 時間）

● 前提知識

コンピュータやネットワークの基礎的な知識は必須です。また、Linux 経験があることが望ましく、講義では、コマンドラインでの操作や vi エディタでの編集作業がありますので、事前に作業ができるように準備しておいて下さい。なお、講義の 1 週間前を目途に事前学習資料（使用する検査ツール操作説明資料）を配布いたします。本講座では、講義で使用する検査ツール操作について、予習をして頂くお願いをしております。

● 講義の目標と到達レベル

IoT システムのセキュリティ対策が、脅威分析を行った通りに実施されているか確認出来るようになることが目標です。スマートホームを想定した疑似環境への検査手順を検討し、検査ツールを使って実際に IoT デバイスを検査して脆弱性を検出するとともに、脆弱性を利用した脅威を再現するまでの技術を習得します。

● スケジュール

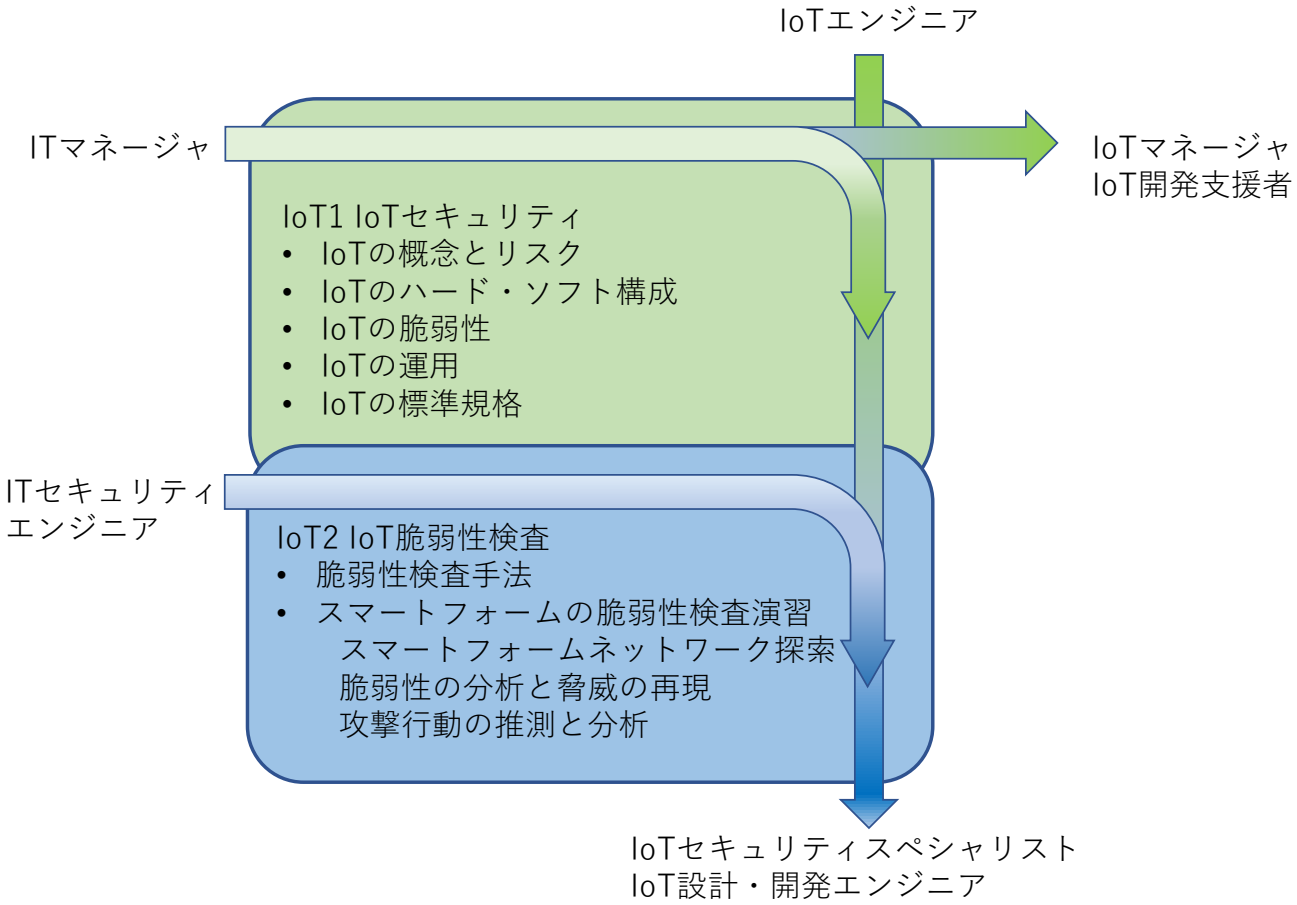
[IoT-2： IoT 脆弱性検査]

日 程		時 間	内 容
6 月 6 日	木	09:30～16:50	・脆弱性検査手法の学習（システム構成の理解、検査起点の分析など） ・脆弱性検査ツールの学習（ネットワークスキャンツール、脆弱性スキャンツールなど） ・脆弱性検査演習：スマートホームを想定した疑似環境の脆弱性検査 ・CTF（Capture The flag）による演習

※内容の詳細は変更される可能性があります。

◆コースの位置づけ

本コースは、IoT-1、IoT-2 の 2 つの講座に関しましては、個別に選択、受講頂くことが可能です。しかしながら、後半部分は前半部分の知識と技術習得を前提にしますので、2 つの講座を通して受講されることをお勧めします。



◆講義と演習環境

情報セキュリティ大学院大学において、講義と演習を実施します。演習に必要な PC は本学が提供します。IoT2 の演習は本学内の演習実験装置にブラウザで接続し、CTF (Capture The Flag) サーバーから与えられる設問をクリアしていく方法で行います。

◆申し込み方法と受講料のお支払い

1. 受講申込みについて

添付の「受講申込書」に必要事項をご記入いただき、メール添付で情報セキュリティ大学院大学 ProSec 事務局(Email:prosec@iisec.ac.jp)宛にお申込みください。
「受講申込書」は、以下ご案内ページからもダウンロードいただけます。

[情報セキュリティプロ人材育成短期集中プログラム(ProSec)Non-Degree Program]
http://www.iisec.ac.jp/admissions/prosec/

2. 受講料

IoT-1：IoT 基礎セキュリティ（1 日間,6 時間）　55,000 円／人 (税込)
IoT-2：IoT 脆弱性検査　（1 日間, 6 時間）　55,000 円／人 (税込)

コース	申込締切日	開講日程	お支払期限
IoT-1	2024/5/21	2024/6/5	2024/7/末
IoT-2	2024/5/22	2024/6/6	2024/7/末

3. 受講前の手続き

(ア) 本学より計算書をご送付しますので、注文書を申込み期限までにお送りください。
(イ) 注文書受領後、本学より、受講登録完了のメール(受講案内)と受講料のご請求書をお送りします。ご請求額を請求書記載の銀行口座あてにお振込みください。なお、振込手数料はお振込者様にてご負担願います。

4. 受講申込みの際の注意事項等

- 注文書受領後のキャンセルは承ることができません。また、コースを欠席なさった場合でも、一旦納入された受講料は原則として返金できませんので、予めご承知おきください。
- 申込締切日(開講 2 週間前)時点で申込者が最少開講人数に達しない場合、開講を中止させていただくことがございます。その際は速やかに申込代表者の方にご連絡いたします。
- 受講申込みの際に、受講者各位と定常的に連絡可能なメールアドレスをご記載ください。
- その他、詳細につきましては、お申込みいただいた際に、別途ご連絡させていただきます。

【問い合わせ先】
情報セキュリティ大学院大学
ProSec 事務局
Email：prosec@iisec.ac.jp