INSTITUTE of INFORMATION SECURITY

2020 年度 サイバーセキュリティ企業向け集中コース
「IoT セキュリティ」

IISEC Cyber-Security Corporate Training Course 2020:
"IoT Security"

サイバーセキュリティ企業向け集中コース「IoT セキュリティ」は、4 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。4 つの講座は、それぞれ単独で受講頂くことも可能です（ただし、IoT-4 に関しましては、原則として IoT-3 を受講済みであることが受講条件となります）。
2020 年度は、4 講座すべて Zoom を用いた遠隔オンライン開講といたします。

- **IoT-1： IoT デバイス［11 月 4 日］**
  - ✧ IoT デバイスと IoT ソフトウェア開発（講義、2 units）
  - ✧ mbed を使った IoT デバイス開発（技術演習、2 units）
- **IoT-2： IoT セキュリティ［11 月 5 日、6 日］**
  - ✧ IoT の概念、IoT セキュリティ概観、IoT 関連法制度、IoT ネットワーク、ハードウェアセキュリティ、信頼の起点（講義、6 units）
  - ✧ セキュア IoT デバイス演習（技術演習、2 units）
- **IoT-3： IoT 脅威分析［11 月 9 日、10 日］**
  - ✧ IoT の運用と規格、国際標準、認証（講義、1unit）
  - ✧ 機能安全、脅威分析手法（講義、3units）
  - ✧ スマートホームの脅威分析演習（技術演習、4 units）
- **IoT-4： IoT 脆弱性検査［11 月 11 日］**
  - ✧ スマートホームの脆弱性検査（技術演習、4 units）

※1 unit は約 90 分　　※定員…IoT-1：20 名、その他は定員なし

本集中コースは、IoT システムの開発に取り組む企業の技術者に最適のセキュリティコースです。これまで IT システムの管理開発に関わっていた方が、新たに IoT を担当する、あるいは、これまで組み込み系の開発に関わっていた方が、これから IoT へのセキュリティの導入を担当する場合など、IT 系、組み込み系の技術者が新たに考慮すべき IoT のセキュリティについて、講義と演習を行います。技術者だけでなく、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。

情報セキュリティ大学院大学
セキュアシステム研究所
所長　後藤　厚宏

SSLab

IoT-1：IoT デバイス（1 day, 4 units）

● 前提知識

コンピュータとネットワークのハードウェア、オームの法則、エレクトロニクス、C~C++プログラムの基礎知識を前提にします。

● 講座の目標と到達レベル

IoT デバイスを開発するための基礎となるハードウェアとソフトウェアの基礎知識を習得します。ハードウェアでは、IoT デバイスを構成する要素であるマイクロコントローラ、デバイスインタフェース、センサー、Wi-Fi モジュールを学修し、簡単な実験回路が作れることを目指します。ソフトウェアでは、デバイス(センサー)を制御する簡単なリアルタイムプログラムを作成し、クラウドコンパイラ mbed を用いた IoT デバイス開発の基礎を習得します。本コースを受講すると，IoT-2 以降をさらに良く理解することができます。

● 講義と演習環境

Zoom を使用して、オンラインで講義と演習を実施します。演習キットをご自宅に送付し、ARM の mbed 環境での演習を行います。演習キットは、演習終了後に、ご返送をお願いいたします。

● 受講準備

受講生は、USB ポートと有線 LAN ポートの付いたノート PC を各自でご用意ください。mbed オンラインコンパイラを利用しますので、あらかじめ次のアカウント登録を済ませておいてください。

【アカウント登録】

ARM mbed　https://www.mbed.com/en/　にユーザー登録し、そのアカウント名を infodevice@iisec.ac.jp に送ってください。サンプルプログラムを提供する mbed iisec チームに登録します。

● 主な講義・演習項目

- ✧ Unit 1: IoT デバイス
- ✧ Unit 2: IoT ソフトウェア
- ✧ Unit 3: IoT デバイス開発演習 1
- ✧ Unit 4: IoT デバイス開発演習 2

IoT-2：IoT セキュリティ（2 days, 8 units）

● 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。IoT デバイスに関しては、IoT-1 の受講をお奨めします。

● 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。IoT の法制度、規格や認証制度、また、IoT システムサービスを運用する基礎知識を習得します。IoT システムの信頼の基点となる暗号鍵の秘匿法をセキュア IoT デバイス演習で習得します。

● 講義と演習環境

Zoom を使用して、オンラインで講義と演習を実施します。演習は、教室で講師陣が行う演習を Zoom を通じて観察していただきます。

● 主な講義・演習項目

- ✧ Unit 1: IoT セキュリティ
- ✧ Unit 2: IoT デバイスのアタックサーフェス
- ✧ Unit 3: 制御システムセキュリティ
- ✧ Unit 4: IoT 関連法制度
- ✧ Unit 5: IoT ネットワーク
- ✧ Unit 6: ハードウェアセキュリティとセキュアマイコン
- ✧ Unit 7: IoT デバイスの暗号通信演習
- ✧ Unit 8: IoT デバイスの信頼の起点演習

■ 特記事項

本講座(IoT-2)は輸出管理の対象となる技術を取り扱うため、 日本国の非居住者は受講できません。
非居住者とは、日本に引き続いて 6 箇月以上居住していない方を指します。

IoT-3：IoT 脅威分析（2 days, 8 units）

● 前提知識

脆弱性やネットワークに対する攻撃の基礎知識、脆弱性データベース（CVE、CWE）などを知っていることが望ましいです。

● 講義の目標と到達レベル

IoT システムの開発・展開前にセキュリティを十分に検討することができるように、IoT に関連する運用と規格、および、リスクを想定し、対策を検討する脅威分析技術を学修します。演習では、いくつかの IoT デバイスから構成されるスマートホームを想定し、実際に脅威分析を行います。

● 講義と演習環境

Zoom を使用して、オンラインで講義と演習を実施します。演習では、Zoom のブレークアウトセッションを使用して、グループワークを実施していただきます。

● 主な講義・演習項目

- ✧ Unit 1:　IoT の運用と規格
- ✧ Unit 2:　機能安全
- ✧ Unit 3:　脅威分析手法　セキュリティ・バイ・デザイン、要求段階での脅威分析(被害分析)
- ✧ Unit 4:　脅威分析手法　設計段階での脅威分析(攻撃分析)
- ✧ Unit 5～6:　要求段階での脅威分析(被害分析)演習
- ✧ Unit 7～8:　設計段階での脅威分析(攻撃分析)演習

IoT-4: IoT 脆弱性検査（1 day, 4 units）

● 受講条件

「IoT-3： IoT 脅威分析」を受講済みであること。（応相談）

● 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。

● 講義と演習環境

~~Zoom を使用して、オンラインで講義と演習を実施します。演習は、教室で講師陣が行う演習を Zoom を通じて観察していただくとともに、~~CTF (capture the flag) 形式の演習ガイドを行います。CTF サーバーにブラウザから接続し、課題に回答いただきます。

（2020.10.9 追記）

オンサイトで行うのと同等の演習を、オンラインでご受講いただくことが可能になりました。

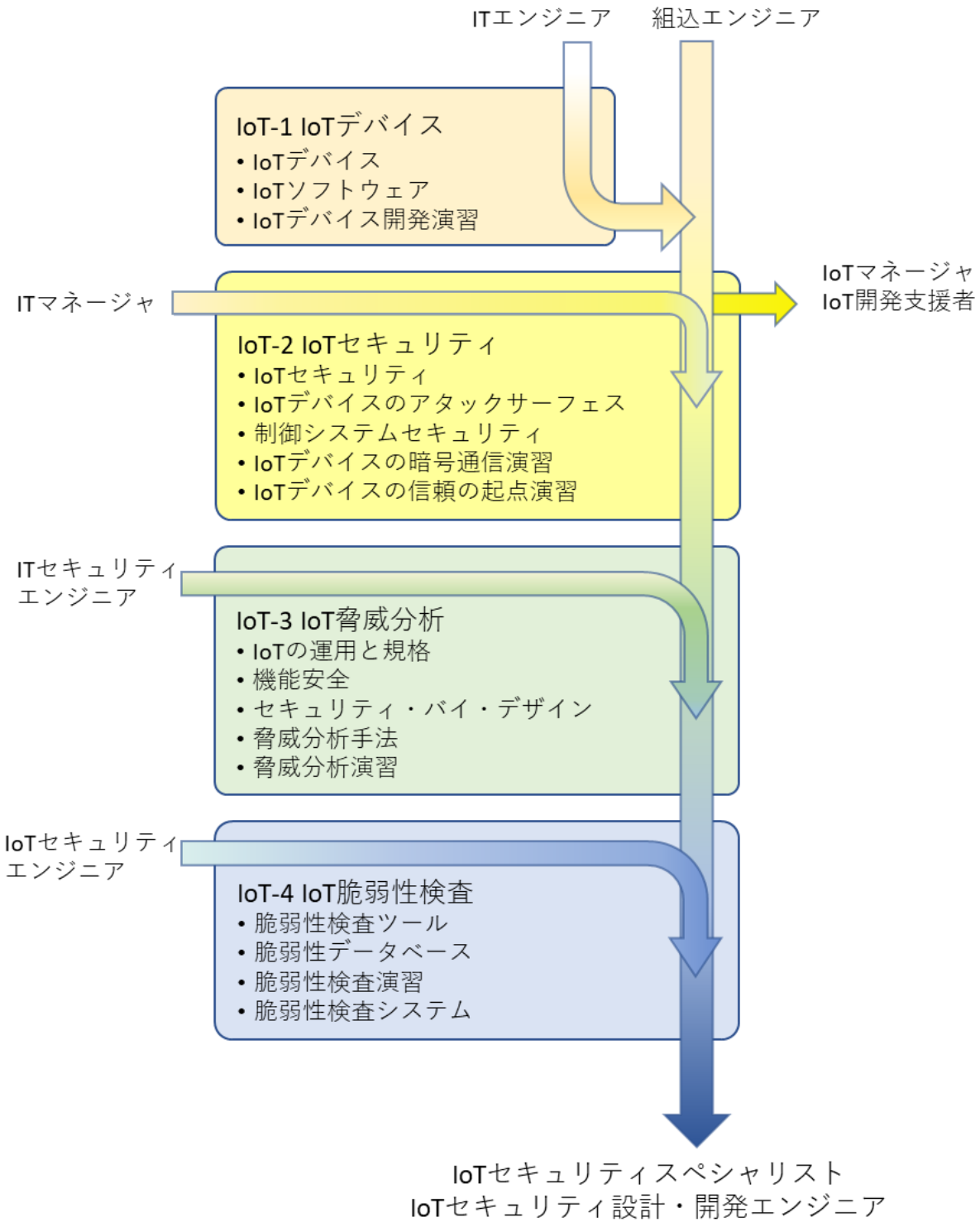
遠隔のご自宅または職場の PC から大学内の検査器にログインし、ご自身で検査ツールを駆使して脆弱性検査を実施いただきます。

● 主な講義・演習項目

- ✧ Unit 1: 脆弱性検査ツールと脆弱性データベース
- ✧ Unit 2～3: 脆弱性検査演習
- ✧ Unit 4: 脆弱性検査システム

◆コースの位置づけ

本コースは、IoT-1、IoT-2、IoT-3 の 3 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（IoT-4 に関しましては、原則として IoT-3 を受講済みであることが受講条件となります)。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、4 つの講座を通して受講されることをお勧めします。



◆講座日程

[IoT-1： IoT デバイス]

日 程		時 限	内 容
11 月 4 日	水	09:20～10:50	IoT デバイス: マイクロコントローラ、センサー
		11:00～12:30	IoT ソフトウェア: RTOS、デバイスプログラミング、開発環境
		13:30～15:00	IoT デバイス開発演習 1: mbed、LPC1768、Blinky、AD/DA、PWM、タイマー、センサー入力
		15:10～16:40	IoT デバイス開発演習 2: mems 加速度センサー、音響生成、Wi-Fi 接続

[IoT-2： IoT セキュリティ]

日 程		時 限	内 容
11 月 5 日	木	09:20～10:50	IoT セキュリティ: IoT のビジョン、IoT の層構造, IoT セキュリティ事例, MIRAI マルウェア
		11:00～12:30	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、JTAG (保守ポート)、計測セキュリティ
		13:30～15:00	制御システムセキュリティ: 制御ネットワーク、PLC、Stuxnet、Trusted OS
		15:10～16:40	IoT 関連法制度: 通信の秘密、リバースエンジニアリング、ログ、PSIRT
11 月 6 日	金	09:20～10:50	IoT ネットワーク: Wi-Fi、Bluetooth、LPWA、MQTT、機器認証、フォグ
		11:00～12:30	ハードウェアセキュリティとセキュアマイコン: サイドチャネル攻撃、耐タンパー性、信頼の起点、Trustzone、TSIP
		13:30～15:00	IoT デバイスの暗号通信演習: ソフトウェアによる暗号化
		15:10～16:40	IoT デバイスの信頼の起点演習: TSIP を使用した暗号化

[IoT-3： IoT 脅威分析]

日 程		時 限	内 容
11 月 9 日	月	09:20～10:50	IoT の運用と規格: 国際標準、EDSA 認証、CC 認証
		11:00～12:30	機能安全: IEC61508、ハザード分析(FTA/FMEA/Hazop/STAMP/STPA)
		13:30～15:00	脅威分析手法: セキュリティ・バイ・デザイン、ライフサイクル、要求段階での脅威分析(被害分析)、被害のインパクト評価
		15:10～16:40	脅威分析手法: 設計段階での脅威分析(攻撃分析)、Attack Tree、リスク評価
11 月 10 日	火	09:20～10:50	要求段階での脅威分析(被害分析)演習: 資産の識別、脅威の識別、インパクト評価
		11:00～12:30	
		13:30～15:00	設計段階での脅威分析(攻撃分析)演習: 脅威モデリング、Attack Tree 分析、リスク評価・対策設計
		15:10～16:40	

[IoT-4： IoT 脆弱性検査]

日 程		時 限	内 容
11 月 11 日	水	09:20～10:50	脆弱性検査ツールと脆弱性データベース
		11:00～12:30	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
		13:30～15:00	
		15:10～16:40	脆弱性検査システム: 脆弱性検査演習で使用した脆弱性検査システムの構成

◆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セキュアシステム研究所(SSL)事務局(Email:ssl-info@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。

[情報セキュリティ大学院大学 SSL 企業向け集中コースご案内]
https://www.iisec.ac.jp/sslab/courses.html

2. 受講料

IoT-1：IoT デバイス（1 day, 4 units）50,000 円／人（税別）
IoT-2：IoT セキュリティ（2 days, 8 units）100,000 円／人（税別）
IoT-3：IoT 脅威分析（2 days, 8 units）100,000 円／人（税別）
IoT-4：IoT 脆弱性検査（1 day, 4 units）50,000 円／人（税別）

コース	申込締切日	開講日程	お支払期限
IoT-1	2020/10/21	2020/11/4	2020/12/末
IoT-2	2020/10/21	2020/11/5, 6	2020/12/末
IoT-3	2020/10/26	2020/11/9, 11/10	2020/12/末
IoT-4	2020/10/26	2020/11/11	2020/12/末

3. 受講前の手続き

- 本学より計算書をご送付しますので、社印のある注文書を申込み期限までにお送りください。
- 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)時点で最少開講人数に達しない場合、開講を中止することがあります。その際は速やかに申込代表者の方にご連絡いたします。
- 4 講座すべて Zoom を用いた遠隔オンライン開講といたします。ご受講の際は、Zoom への接続が可能な環境をご用意ください。
- 受講申し込みの際に、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
セキュアシステム研究所
事務局
Email：ssl-info@iisec.ac.jp