(*)は任意記入事項（省略可能）

〇開講科目名
セキュリティ基礎論I
〇開講科目名（英）
Foundations of Security I
〇対象所属(*)

〇担当教員
宮地 充子, 新井 悠(トレンドマイクロ), 竹森 敬祐(KDDI/KDDI総合研究所)

〇開講言語
日本語

〇授業の目的・概要
セキュリティ分野を垂直な2軸で網羅的にカバーすることを目的とします。
具体的には、"共通鍵暗号解析"から"マルウェア解析"及び"基盤理論"から"実用技術・標準化"という2軸により、
セキュリティの基盤理論、暗号理論、実用化から標準化技術など最先端のセキュリティ技術までを守備した講義内容となります。

【マルウェア解析入門】（担当：新井 悠）
情報セキュリティにおける脅威の最大勢力のひとつであるマルウェアの解析手法について基礎的領域を学習する。
実行ファイルの構造やメタデータ、あるいはAPIなどのOSの低レイヤー構造についても解説し、
それらをコードによって抽出・特定することで自動的に解析を実施する。また機械学習を使うことで、
マルウェアを自動的に判定することを実現する。

【スマホ／IoT時代のプライバシ保護】（担当：竹森 敬祐）
スマホやPCを利用する際に、知らないうちに個人データが外部に送信されている。
ビッグデータ解析やAIの発展で生活が便利になる中で、個人データを扱う事業者が、
プライバシ保護に向けて求められる取り組みを学ぶ。

【IoTデバイスのセキュリティV字開発】（担当：竹森 敬祐）
様々な物がインターネットに繋がるInternet of Things(IoT)の時代がやってくる。
繋がることでのサイバー攻撃への備えは重要であり、本講義では過去の攻撃事例を振り返り、
IoTデバイスを安全に設計／実装／検査する開発の流れを学ぶ。

〇学習目標
【マルウェア解析入門】（担当：新井 悠）
リバース・エンジニアリングのような特殊技能を養成するのではなく、コードによる自動解析力を養成することで、
大量に出現するマルウェアに対処する能力を持った人材を育成する。

【スマホ／IoT時代のプライバシ保護】（担当：竹森 敬祐）
個人データ取扱い事業者の立場で、「透明性の確保」、「利用者関与の機会」とは何かを理解する。

【IoTデバイスのセキュリティV字開発】（担当：竹森 敬祐）
IoTデバイス開発者の立場で、「リスク分析」、「セキュリティV字開発」の基礎を理解する。

【セキュリティ技術の標準化】

セキュリティ技術をどのように標準化するのかについて、具体的な事例を用いて
習得する。

〇履修条件・受講条件(*)
特に事前知識は仮定しないが、下記があるとより理解が深まる。

【マルウェア解析入門】（担当：新井 悠）
Pythonによるプログラミング技能

【スマホ／IoT時代のプライバシ保護】（担当：竹森 敬祐）
事前知識は必須ではないが、以下の資料に目を通しておくと、理解が深まる。
スマートフォン・プライバシー・イニシアティブⅢ
http://www.soumu.go.jp/menu_news/s-news/01kiban08_03000250.html

【IoTデバイスのセキュリティV字開発】（担当：竹森 敬祐）
事前知識は必須ではないが、以下の資料に目を通しておくと、理解が深まる。
・IoTセキュリティガイドライン
http://www.iotac.jp/wp-content/uploads/2016/01/03-IoTセキュリティガイドライン
ver1.0別紙%EF%BC%91.pdf
・情報セキュリティ10大脅威 2018（1章）
https://www.ipa.go.jp/files/000065376.pdf

〇授業計画
【マルウェア解析入門】（担当：新井 悠）
【第1回 マルウェア解析のための基礎知識】
マルウェア解析に必要な基礎知識、専門用語について解説する。
【知識単位】マルウェア、Python

【第2回 PEファイル入門】
Windowsにおける実行ファイルの形式であるPEフォーマットについて学習する。
同時にそれらメタデータにアクセスするためのライブラリを使用し、自動で抽出するコードを作成する。
【知識単位】マルウェア、Python

【第3回 外部リソースとWeb APIへのアクセス】
ビッグデータを提供するサイトのRestful APIにアクセスし、クエリを行うことでJSON形式のデータを入手する。
そしてその結果を整形して表示するコードを作成する。また、Windows APIを取得し、マルウェアの感染動作に関連する部分を抽出して自動判定に使用する。
【知識単位】マルウェア、Python

【第4回 機械学習によるマルウェア判定】
第二回で使用したPEファイルのメタデータを教師データに使用することで、Data Drivenな機械学習エンジンを作成する。
機械学習エンジンを作製し、自動的にマルウェア判定を行うコードを開発する。
【知識単位】マルウェア、Python、機械学習

【スマホ／IoT時代のプライバシ保護】（担当：竹森 敬祐）
これまでのプライバシ侵害事故を振り返り、個人データ取扱い事業者に
求められる対策について学ぶ。具体的には、利用者関与の機会、
透明性の確保に向けた取り組みを理解する。
【知識単位】スマートフォンプライバシーイニシアティブ、GDPR、透明性の確保、利用者関与の機会

【IoTデバイスのセキュリティV字開発】（担当：竹森 敬祐）
これまでのサイバー攻撃事例を振り返り、クルマやIoTデバイスを提供
する事業者に求められるセキュリティ開発手順を学ぶ。具体的には、

リスクを洗い出し、これを軽減する対策を図る流れを理解する。
IoTセキュリティガイドライン、セキュリティV字開発、リスク分析、防御/検知/一次対処/回復

〇授業外における学習
演習課題（教育システムで提示）
テキストの予習及び演習課題（教育システムで提示）。
テキストの予習（教育システムで提示）。

〇教科書・教材(*)
【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
宮地充子著，「代数学から学ぶ暗号理論」，日本評論社

【マルウェア解析入門】（担当：新井 悠）
新井 悠、岩村 誠、川古谷 裕平、青木 一史、星澤 裕二 著
アナライジング・マルウェア ――フリーツールを使った感染事案対処

〇成績評価［評価方法・割合の記載は必須］
[評価の観点] 講義内容の理解度
[評価方法] レポート提出
[評価基準] レポート課題

〇オフィスアワー(*)

〇コメント(*)

〇特記事項(*)
講義の一部にプログラミング演習を含むのでノートPCを所有している学生は持参すること。