2021年度 ハードウェアセキュリティ (4038)

■ 授業科目基本情報

科目区分	専門科目	**教職科目**	情報
単位数	1	**選択・必修・自由**	選択
授業形態	講義	**主な使用言語**	英語
開講時期	III	**履修登録システム**	使用する
履修登録期間	2021/10/14～2021/11/04	**履修取消期限**	2021/11/04

■ 教育プログラム別の履修区分

プログラム名	IS	CB	BS	BN	MS	CP	DS
履修区分	○	○	△	△	△	○	○
コア科目	–	–	–	–	–	–	–
履修方法	・修士論文研究又は特別課題研究を履修する場合は、基盤科目及び専門科目から12単位以上履修すること。 ・課題研究を履修する場合は、基盤科目及び専門科目から14単位以上履修すること。						

■ 授業科目概要

担当責任教員	林　優一
担当教員	林優一、藤本大介、Youngwoo Kim
教育目的／学修到達目標	【教育目的】 ハードウェアセキュリティの基礎となる要素技術と実際の脅威と抑止するための対策について理解することを目的とする。 【学修到達目標】 1) ハードウェアセキュリティについて説明、記述できる。 2) ハードウェアセキュリティの評価・対策・メカニズムについて整理、議論ができる。 3) ハードウェアセキュリティの必要性について俯瞰、表現できる。 4) ハードウェアセキュリティをシステムに実装する手法について理解できる。
授業概要／指導方針	【授業概要／指導方針】 情報セキュリティをシステムに実現する際、セキュリティアンカーとなるハードウェアの安全性確保に必要となる基盤知識を習得すると共に、ハードウェアを基礎として構成される上位レイヤーを含めたシステム全体のセキュリティを確保するための知見の獲得を目指す。また、情報セキュリティ分野における研究手法、セキュリティの確保が必要なる分野への応用についても学ぶ。 座学 【授業時間外学修（予習・復習等）の目安】 各回毎に授業内で与えられたAssignmentの予習2時間 各回毎に復習2時間程度

■ 授業計画

[1限目 9:20-10:50] [2限目 11:00-12:30] [3限目 13:30-15:00] [4限目 15:10-16:40] [5限目 16:50-18:20] [6限目 18:30-20:00]

回数	日付 [時間]	担当教員	テーマ	内容
1	10/21 [2]	林　優一	ハードウェアセキュリティ概要	ハードウェアセキュリティの概要について述べると共に、講義全体を俯瞰し、各回で学ぶ内容の位置づけを明確にする。

2	10/28 [2]	藤本　大介	暗号アルゴリズム	現代暗号における代表的なアルゴリズムを詳解すると共に、それらが利用されるアプリケーションの特徴について解説する。
3	11/4 [2]	藤本　大介	ハードウェア実装	アプリケーションに合わせて多種多様なハードウェアが使用される中、使用する計算資源が異なることで、実装に大きな差異が出る。本回では利用する計算資源を意識したアルゴリズムの実装方法について、いくつかの暗号アルゴリズムを例にとり実装例を示す。
4	11/11 [2]	Kim Youngwoo	計測技術	ハードウェアのセキュリティを評価するために必要となる計測技術について述べると共に、計測対象となる電磁信号の発生・伝搬過程について詳説する。
5	11/18 [2]	Kim Youngwoo	シミュレーション技術	ハードウェアセキュリティのメカニズム解明や対策技術の開発に必須となるシミュレーション技術について詳説する。
6	11/25 [2]	林　優一	漏えい信号による情報漏えいの脅威と対策	機器内部で実行される処理に応じて発生する電磁信号が情報を漏えいさせる事例について述べると共に、漏えいのメカニズム、評価法、及び対策技術について述べる。
7	12/2 [2]	藤本　大介	意図的な外乱が引き起こす脅威と対策	意図的な外乱により引き起こされるセキュリティ低下について述べると共に、その評価方法、対策方法について詳説する。
8	12/9 [2]	林　優一	ハードウェアトロージャンによる脅威と対策	ハードウェアトロージャンによるセキュリティ低下の脅威について述べると共に、それらを検出法及び抑止法について詳解する。

■ 授業日程

[1限目 9:20-10:50] [2限目 11:00-12:30] [3限目 13:30-15:00] [4限目 15:10-16:40] [5限目 16:50-18:20] [6限目 18:30-20:00]

回数	日付	時間	講義室	備考
1	10/21	2	エーアイ大講義室[L1](IS)	
2	10/28	2	エーアイ大講義室[L1](IS)	
3	11/4	2	エーアイ大講義室[L1](IS)	
4	11/11	2	エーアイ大講義室[L1](IS)	
5	11/18	2	エーアイ大講義室[L1](IS)	
6	11/25	2	エーアイ大講義室[L1](IS)	
7	12/2	2	エーアイ大講義室[L1](IS)	
8	12/9	2	エーアイ大講義室[L1](IS)	

■ テキスト・参考書

テキスト	特になし。講義資料を配布。
参考書	S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer-Verlag, 2007. Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

■ その他

履修条件	特になし
オフィスアワー	Eメールで連絡の上、日時を決める。
成績評価の方法と基準	・5段階（秀・優・良・可・不可）で評価する。 ・授業毎に求めるミニレポート（20%）、講義期間中に数回求めるレポート（30%）および最終レポート（50%）で評価する。
関連科目	特になし
関連学位	特になし
注意事項	特になし