ＩＥＩＣＥ関西支部ＩＣＴ基礎講座

講座名	暗号技術とセキュリティ設計の基礎	
コース	[○] 1日コース　　[ ] 2日コース	
開講日時	2022 年 11 月 5 日（土） 午前 9 時 40 分～午後 4 時 50 分（途中昼食と休憩の合計約 1 時間 10 分を含みます）	
事前知識	特に必要としない．可能であれば，簡単なプログラミングの経験（言語は問わない），基本的な TCP/IP ネットワーキングとセキュリティについての理解など．	
特　徴	多方面の分野の技術者にセキュリティの考え方が求められてきています．本講義では，まず情報セキュリティの基本的な考え方を示し，データを保護するための暗号技術に関する初歩的な数学的知識と公開鍵暗号・電子署名を手で計算をしながら理解します．そして，暗号技術以外の各種のセキュリティ対策を概観し，脅威分析とセキュリティ対策選定の演習をすることでセキュリティ設計の基本を学びます．	
対　象	セキュリティの基本的な考え方を理解したい方，暗号技術の原理を理解したい方，セキュリティ設計の基礎を学びたい方．	
テキスト	なし（資料は事前に郵送または配布）	
参考書	なし	
授業概要	サイバー攻撃に関する話題が絶え間なく聞こえてきます．IoT（Internet of Things）やインダストリー 4.0 などの文脈においては，セキュリティを専門とする技術者だけで被害を未然に防いだり，最小化できなくなってきたりしており，多方面の分野の技術者にセキュリティの考え方が求められてきています．本講座では，まず，情報セキュリティの基本的な考え方を概観します．次に，盗聴・改ざん・偽造からデータを保護する暗号技術について，基本を理解するのに必要な初歩的な数学的知識を説明します．そして，離散対数問題に基づく公開鍵暗号と電子署名の ElGamal 暗号と Schnorr 署名を理解します．これらの中核的な要素技術に加えて各種のセキュリティ対策を概観し，セキュリティ設計のための脅威分析とセキュリティ対策選定の基本について学びます．IoT 関連のシステムのいくつかの例を用いた演習によりセキュリティ設計に関する理解を深めます．	
授業項目	1．(9:40-11:10) 情報セキュリティの考え方: ・情報セキュリティとその対策 ・情報セキュリティの基本的問題 2．(11:15-12:45) アクセス制御の考え方: ・ユーザの認証 ・情報の保護 暗号技術の基礎: ・公開鍵暗号の原理 ・暗号で使われる数の世界	3．(13:45-15:15) ElGamal 暗号，Schnorr 署名: ・合同式，位数，原始元，フェルマーの定理 ・離散対数問題 ・ElGamal 暗号 ・Schnorr 署名 4．(15:20-16:50) セキュリティ設計の基礎: ・脅威分析 ・セキュリティ対策
事前学習および備考	事前学習は特に必要ありません．	
講　師	白石　善明　（しらいし　よしあき）　博士（工学） 神戸大学　大学院工学研究科電気電子工学専攻　准教授	