IEICE 関西支部 ICT 基礎講座「暗号技術とセキュリティ設計の基礎」ご案内

近年の情報通信関連開発では、必要とされる技術の多様化と開発期間の短縮により、若手技術者が OJT を通して基礎知識や基礎技術を習得することが難しくなっていると指摘されています。また、これまで予想されなかった分野で情報通信技術が適用されることも増えており、大学・大学院教育で身に付けた技術分野を越えた多彩な技術を修得する必要性が高まっています。

このような状況に鑑み、電子情報通信学会関西支部では、情報通信に関するさまざまな技術を集中講義形式で学習できる講座「IEICE 関西支部 ICT（Information and Communication Technology）基礎講座」を開講しています。本講座は基礎的な知識や技術に重点を置きながら、基礎から展開して最先端技術へ至るまで講義・実習することを目的としています。各講座の受講者数を 15 名程度の少人数に絞ることで講師との双方向コミュニケーションを可能とし、短期間で先端技術の基礎を習得することを狙っております。例年好評を頂いております「暗号技術とセキュリティ設計の基礎」の講座を今年度も下記のとおり開講いたします。今回は学生の方も参加しやすい土曜日に開催と致しました。皆様の積極的な受講をお待ちしております。

日　時：2024 年 3 月 2 日（土）9:40～16:50

場　　所：中央電気倶楽部　315 号室　（大阪市北区堂島浜 2-1-25）
（地図：https://www.chuodenki-club.or.jp/about/access/）
ドージマ地下センター南詰を右側に上がり、右へ約 50m、左側のレンガ造り建物

内　容：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。
シラバスは右記 URL からご覧いただけます。 http://www.ieice.org/kansai/ict/

講　師：白石 善明 氏（神戸大学）

受講料：会員：8,000 円、学生: 2,000 円、非会員: 17,000 円（会員、非会員共に消費税込み）
（電気、映像情報メディア、照明、情報処理学会会員は電子情報通信学会会員と同じ扱いと致します。）

募集人数：5 名以上、最大 15 名程度
（開講2週間前までに申込み人数が5名に達しない場合、開講しないこともあります）

申込み方法：参加希望者は、電子情報通信学会関西支部のホームページ
（http://www.ieice.org/kansai/）からお申込み下さい。
尚、E-mail でも受け付けますので、下記にお申込み下さい。

申込期限: 2024 年 2 月 19 日（月）

振込期限: 2024 年 2 月 22 日（木）

問い合わせ先：〒530-0004 大阪市北区堂島浜 2-1-25 中央電気倶楽部内（314 号室）
関西電気関連学会事務センター

TEL: (06) 6341-2529, FAX: (06) 6341-2534

E-mail denki4g@ares.eonet.ne.jp

主　催:電子情報通信学会関西支部

以上

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	[〇] 1日コース　　[ ] 2日コース	
開講日時	2024 年 3 月 2 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	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	