

コース名	専門人材特化型コース					
講座名	社会人向けサイバーセキュリティ人材育成講座(九州大学SECKUN) (共同事業)					
科目名	クラウドコンピューティングとセキュリティ					
必修・選択	—	単位	—			
概要・目的	<p>クラウドや生成AIの利用が加速している中、基本的なクラウドの技術、モダンな開発、運用手法などが十分に理解されていないケースもあり、リスクが過剰にフォーカスされることもある。</p> <p>まず「クラウドセキュリティ」として、クラウドや生成AIを取り巻く基本的な概念を踏まえ、セキュリティに従事する専門家（技術者および非技術者）が、どのようにセキュリティに向き合うべきかを伝えることを目的としている。ここでは、クラウドサービスの例としてAWSを取り上げるが、本講座の内容はAWSに特化したものではない。</p> <p>次に、「クラウドネイティブアーキテクチャとセキュリティ」として、クラウドネイティブなアーキテクチャの特性を理解し、その脅威やリスクを評価できる素地を身に着ける。クラウドネイティブな環境を採用することにより、システムの開発、デプロイ、運用はより迅速かつ柔軟になった一方で、セキュリティ上の脅威やリスクも従来とは大きく異なるものへと変化しているため、従来の対策がそぐわないことが起こりうる。そこで、本講義では、クラウドサービスの特性、コンテナ技術がもたらすセキュリティ上の考慮事項、マイクロサービスアーキテクチャのセキュリティリスクなどの広範なトピックについて、ハンズオンを通して理解を深めてもらう予定である。</p> <p>さらに、「セキュアな実行環境としてのWebAssembly」として、WebAssemblyの可能性と課題についての理解を目指す。このために、WebAssemblyの概要と、そのセキュリティ的観点での解説を通して、クラウド上を含むサーバサイド利用を主軸に解説する。ユースケース（ブラウザ、サーバサイド、組み込み）を整理し、規格についても解説をする。その上でOSS製のサーバサイド実装とwasm-tools、WAT形式でのプログラムなどを用いて、実際に手を動かしながらWebAssemblyの動作を確認する。</p> <p>また、WebAssemblyのサンドボクシングの概要を整理する。具体的には線形メモリの概要とその意義、WebAssembly System Interface (WASI) について、具体的なWASI実装とpreopens等の機構について説明を行う予定である。</p> <p>最後に、「ソフトウェアサプライチェーンセキュリティ」として、ソフトウェアサプライチェーンを取り巻く複雑なセキュリティ課題について理解を深める。現代のソフトウェア開発では、個々のアプリケーションやシステムだけでなく、その開発、構築、配布、運用といった全段階に潜む脆弱性が、組織全体に甚大な影響を及ぼす可能性がある。本講義を学習することで、受講者はソフトウェアサプライチェーンセキュリティの重要性を認識し、そのリスクを特定、評価、そして緩和するための具体的な知識とスキルを習得できる。</p>					
到達目標	<ul style="list-style-type: none"> <li>クラウドの基本的な概念や仕組み、クラウドが選ばれる理由を説明できる</li> <li>クラウドセキュリティにおける従来のセキュリティ管理との差異や活用を理解できる。</li> <li>生成AIにおけるセキュリティ上の考慮事項を理解できる。</li> <li>ソフトウェアサプライチェーンにおける主要な脅威と影響範囲を特定し、説明できる。</li> <li>ソフトウェアサプライチェーン全体におけるセキュリティリスクを評価し、優先順位付けができる。</li> <li>WebAssemblyをサーバサイドで動作させることができ</li> <li>WebAssemblyの線形メモリなど主要な仕様を把握できる</li> <li>WebAssemblyのサーバサイド実行とWASIについてその意義を理解できる</li> <li>クラウドネイティブなアーキテクチャの特性を理解し、脅威やリスクを評価できる</li> </ul>					
授業方法	講義 + 演習	実施形態	遠隔同期			
評価方法	毎回のポートフォリオの記入および演習の進捗リストにより、講義の理解と演習の実施状況を確認し、総合的に評価を行う。			開講日		
授業項目	1	セキュアな実行環境としてのWebAssembly1（近藤）		11/23		
	2	セキュアな実行環境としてのWebAssembly2（近藤）				
	3	クラウドセキュリティ1(松本／平賀)				
	4	クラウドセキュリティ2(松本／平賀)		1/24		
	5	クラウドセキュリティ3(松本／平賀)				
	6	クラウドセキュリティ4(松本／平賀)				
	7	クラウドセキュリティ5(松本／平賀)		2/1		
	8	クラウドセキュリティ6(松本／平賀)				
	9	クラウドセキュリティ7(松本／平賀)				
	10	クラウドセキュリティ8(松本／平賀)		2/7		
	11	クラウドセキュリティ9(松本／平賀)				
	12	ソフトウェアサプライチェーンセキュリティ1(松山)				
	13	ソフトウェアサプライチェーンセキュリティ2(松山)		2/28		
	14	ソフトウェアサプライチェーンセキュリティ3(松山)				
	15	クラウドネイティブアーキテクチャとセキュリティ1(森田)				
	16	クラウドネイティブアーキテクチャとセキュリティ2(森田)		3/1		
使用教材	<p>[授業項目1,2] スライド、サンプルコード [授業項目15,16] 本講義では Docker を利用する予定です。Docker が起動・実行できるコンピュータをご用意ください。</p>					
特記事項	<p>※開講日に参加出来ない場合、後日講義動画を視聴する事により受講可能</p> <p>[授業項目1,2] 対面参加者は自分のノートPCを持参すること（Macを推奨するが、Windowsの場合WSL環境を有効にしそこで作業する）対面以外の参加者は十分に動作サポートができない可能性があるので、留意すること</p>					