令和8年度事業計画　（新1年目）

技術検討会「サイバーレジリエンス」

世話役　　中嶋卓雄(東海大学名誉教授)

1　事業概要

目的	サイバーレジリエンス技術者育成のため、より実践な最新の攻撃手法と防御策を学ぶ「ホワイトハッカー育成講座」を実施する。また、企業のシステム担当者のセキュリティ意識向上と組織のレジリエンス(回復力・対応力)強化を目的とし、CSIRTの立ち上げやインシデント初動対応を学ぶ「実践インシデント対応チーム育成講座」を実施する。これにより、技術的な「攻撃・防御スキル」と組織的な「管理・対応能力」の双方を向上させる。
内容	I. ホワイトハッカー育成講座(セキュリティ技術者向け) ◆ Wireshark等を用いたネットワーク解析技術の習得 ◆ dd, FTK-Imager, Autopsy等を用いたデジタルフォレンジック技術の習得 ◆ Metasploit Frameworkによるペネトレーションテストの実践 ◆ PortSwiggerやOWASP Juice Shopを用いた脆弱性診断手法の習得 II. 実践インシデント対応チーム育成講座 (企業システム担当者向け)◆ インシデント対応チーム(CSIRT)の立ち上げと役割分担の策定 ◆ 防御的資産管理(脆弱性管理) ◆ ランサムウェア感染時の初動対応(ネットワーク遮断、証拠保全)訓練◆ 定常的なアクセス管理とSIEMによるログ管理
計画	毎月1、2回程度、以下の2つの形式で技術検討会を開催する。 ホワイトハッカー育成講座:120分(現地＋リモート)、実践的なツール操作を含む演習。 実践インシデント対応チーム育成講座:60分(リモート想定)、全10回で現場担当者がインシデント発生時にすべきことを明確にする講義とワークショップ。
キーワード	ホワイトハッカー、デジタルフォレンジック、CSIRT、インシデントレスポンス、脆弱性診断、ペネトレーションテスト、資産管理
目標及びその進め方	技術者向けには最新の攻撃ツールと防御手法を実践形式で習得させ、企業担当者向けには組織的なサイバーレジリエンス体制の構築と有事の行動指針を確立させることを目標とする。 ① システム解析技術習得: 参加者の理解度に応じ、WiresharkやMetasploit等のオープンソースツールを用いた解析・診断の実習を行う。② 脆弱性診断技術習得:自組織の脆弱性を診断するための手法を脆弱性診断ツールを利用して実習を行う。③ 組織体制構築: 企業担当者が自組織のCSIRT体制(役割分担、連絡網)を設計し、資産管理や認証強化などの予防策を具体化する。④ インシデント対応実践: ランサムウェア等の具体的なインシデントシナリオに基づき、検知から初動対応、証拠保全までの一連の流れをシミュレーションし、組織の対応能力を強化する。 産業技術センター等と協力して、サイバーレジリエンス分野の技術力向上につなげていく。 コーディネート役は熊本高専(八代キャンパス)の小島俊輔氏
対象者	● セキュリティ、サイバーレジリエンスエンジニア ● 企業内情報システム担当者者
会員	随時募集する

2　支出計画　　単位:千円

	RIST負担分					備考
	設備費	原材料費	消耗品費	その他	合計	
予算	50			150	200	

3　予算積算　　(単位:千円)

	品名	単価	個数	価格	備考
設備費	脆弱性ホスト構築セット	50	1	50	
原材料費				0	
消耗品費				0	
その他	講師旅費・謝金、会場費など	150	1	150	
合計				200	