主催：会津大学・株式会社エフコム

２０２５年度

サイバー攻撃対策演習講座

－「攻撃手法」から学ぶ実践型セキュリティ研修 －

【日　　程】演習　４日間
２０２５年　１２月　９日（火）～１２月１２日（金）

【会　　場】
会津大学（講義は事前配信あり）

【募集定員】
３０名

【受 講 料】
１人あたり３６３,０００円（税込）

【募集期間】
２０２５年１１月７日（金）まで

・定員になり次第、締め切らせていただきます。
・なお、定員に余裕がある場合、募集期間を延長して受付します。
講習会事務局までお問合せください。

本講座について

本講座は、**情報セキュリティに関する脅威と対策**、ならびに**サイバー攻撃および防御の手法**について具体的に理解し、企業などの組織においてサイバー攻撃への対応策を企画・適用できる**実践的なスキル**を身につけることを目的としています。今回も引き続き、これまで多くの受講者から高い評価を得てきた**「サイバー攻撃・防御演習」**をメイン講座とし、**最新の技術動向を取り入れた内容**で開催いたします。

経験豊富な講師陣による講座提供

※講師は都合により変更する場合がございます。予めご了承下さい。

○中村　章人（会津大学　教授、先端情報科学研究センター長 ）
国立研究開発法人産業技術総合研究所にて、オブジェクト指向分散システム、クラウド、コンピュータセキュリティ等の研究に従事。
2015年より現職。2017年より福島県警察サイバー犯罪対策アドバイザー。
近年は、構成の異なる多数のコンピュータのセキュリティ診断を効率よく実施する方式・システムの研究開発に取り組んでいる。

○阿部　泰裕（会津大学　上級准教授）
2001年に外資系コンピュータメーカー入社。アウトソーシング事業部にて自社、自動車・銀行業界等のシステム設計・構築・運用に従事。
大規模システムにおけるプロセスの自動化、インシデント対応等に携わる。2008年より外資系半導体検査メーカー等を経て、2013年より現職。

○福原　英之（株式会社コンピュート　代表取締役/三井物産セキュアディレクション株式会社 プリンシパルコンサルタント）
IT業界に長く在籍し、製品開発やシステムインテグレーション、システムアーキテクチャデザイン等に従事。
社内CSIRT立ち上げ等のシステムセキュリティ統括やリスク管理にに従事。

○佐々木　満春（株式会社エヌ・ティ・ティ エムイー　サービスクリエイション部 システムオペレーションセンタ）
2013年入社。NTT東日本のセキュリティ部門にて勤務後、NTT-CERTにて脆弱性情報の管理、リスク評価に関する業務を経験し、FIRSTなど国内外のカンファレンスにて登壇。現在は、ログ分析基盤の維持・運用・最適化、脅威インテリジェンス情報の活用、
新たなセキュリティ運用サービスの立ち上げ等に従事。

○鈴木　亮太（株式会社エヌ・ティ・ティ エムイー　サービスクリエイション部 システムオペレーションセンタ）
2017年入社。社内ネットワークの監視やセキュリティ製品の検証・社内導入を経験し、顧客向けのセキュリティ運用サービスの立ち上げを担当。
現在もセキュリティ運用サービスにて、EDR製品の運用や各種基盤・クラウド環境の構築等の業務に従事。

○国井　傑　（会津大学　客員教授、（株）エストディアン　代表取締役 ）
インターネットサービスプロバイダー企業での立上げ、運営に従事した後、2003年よりシマンテック認定トレーナーとして、ウイルス対策、ファイアウォール、DLPなどの製品トレーニングに従事。2013年からはSymantec Cyber Defense Academyトレーニングに参画し、マルウェア解析やインシデント対応トレーニングの開発やトレーナーの業務を担当。2006年よりMicrosoft　MVPとして、Microsoft365 Defender等のクラウドセキュリティのトレーニングを中心に担当。

サイバーレンジを用いたサイバー攻撃・防御演習

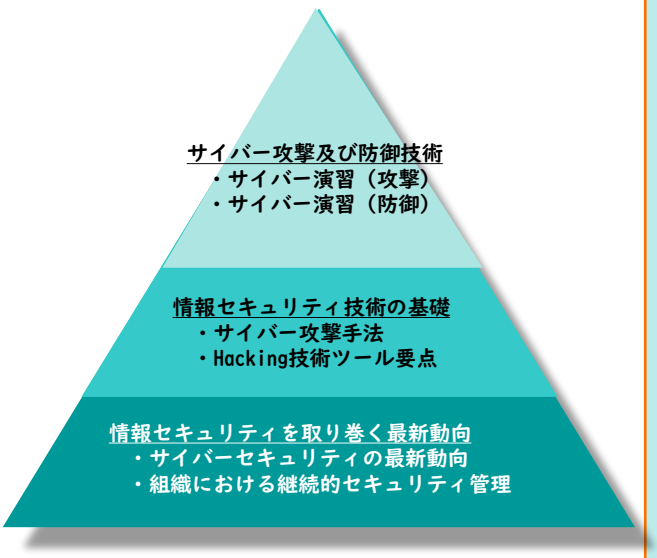
本講座では、**「サイバーレンジ」**と呼ばれる**サイバー攻撃・防御演習システム**を用いた**実践的**な演習を行います。本講座専用に設計されたシナリオを、サイバー演習用の環境上で実行し、実践力の向上を図ります。また、本講座の大きな特色として、**攻撃手法**から**防御技術を学ぶ**という、攻撃者視点を取り入れた演習スタイルを採用しています。

サイバーレンジとは：

サイバー攻撃・防御の演習を実施するための**専用アプライアンス**です。この環境では、サーバーやネットワーク機器を含む大規模なITインフラを、現実さながらに仮想空間上で再現することが可能です。本環境を活用することで、受講者は攻撃者と防御者の役割に分かれ、さまざまなシナリオに基づいた演習を繰り返し実施できます。これにより、実践的なスキルを備えたサイバーセキュリティ専門人材の育成が可能となります。

情報セキュリティの最新動向・管理・技術を網羅

講座の前半では、**情報セキュリティの基礎知識**と**サイバー攻撃手法**について、**最新動向**や**企業事例**を交えた講義を行います。実際のインシデント事例を紹介しながら、後半の**サイバー演習**での実践で理解を深め、**学習意欲を高めるカリキュラム構成**となっています。



ごあいさつ

会津大学では、民間企業及び公共・社会インフラへの情報通信の普及の急速な拡大とともに増大する情報セキュリティの脅威に対応できる専門的人材を育成するため、「サイバー攻撃対策演習講座」を２０１３年度から実施してまいりました。

ますます強まっているサイバーセキュリティ対策へのニーズに応えるため、本年度も本講座を継続することにいたしました。受講者の皆様は、本講座を通して実践的な知識を習得いただけるものと大いに期待しております。

公立大学法人会津大学 理事長 兼 学長　東原 恒夫

講座内容

講義は**録画による事前配信**を行い、演習は会津大学**現地会場での実践演習**を中心に実施します。

◆好きな時間に事前に受講可能な
講義動画の配信

○　昨今の攻撃事例とSOCにおける対応事例
昨今のサイバー攻撃事例やセキュリティオペレーションセンタ（SOC）のインシデント対応事例を紹介。
SOCにおけるセキュリティ対応で重要な役割を担うSIEM（Security Information and Event Management）を用いた検知の仕組みについて解説。

○　SOCの運用とそれを支える技術について
セキュリティオペレーションセンタ（SOC）での日常的な業務内容や、セキュリティ運用を支える技術・プロセスを紹介。
業務活動の中で必要とされる技術や知識について解説。

○　サイバーセキュリティインシデントの事例
インシデント発生時の対応は、組織の環境によって異なる。
どのように準備し、対応すべきか、そのエッセンスを解説。

○　IaCとセキュリティ
根本的な対策が難しい攻撃が増える中で、
IaC（Infrastructure as Code）がサイバーレジリエンスや脆弱性管理にどう役立つかを解説。

○　DX時代の組織的セキュリティ管理
外部からの攻撃だけでなく、内部人員の行為によるインシデントも増加傾向にある。
講師の経験をもとに、実践的な対応や考慮点、組織における継続的な体制強化について解説。

◆受講生同士の気づきを促す
会場での実践演習

○　Microsoft Defender for Endpointを利用したインシデント対応

○　セキュリティを理解するための技術要点解説

○　Hackingで使用される技術・ツール要点解説

○　サイバー演習 攻撃（初級）

○　サイバー演習 攻撃（中級）

○　サイバー演習 防御（中級）

※演習内容は変更になる場合がございます。

◆2025年度　時間割予定

講義は【アーカイブ配信】

12月上旬から開講日まで
【講義】 ・録画によるアーカイブ配信

演習は【現地会津大学キャンパス】で開催

		12月9日（火）		12月10日（水）	12月11日（木）	12月12日（金）
	9:00～10:00		1限目	【サイバー演習】 攻撃（初級） （DMZに対する攻撃演習）	【サイバー演習】 攻撃（中級） （仮想企業に対する標的型攻撃演習）	【サイバー演習】 防御（中級） （実践的な防御策の策定演習）
	10:00～10:10		休憩			
	10:10～11:10		2限目			
	11:10～11:20		休憩			
	11:20～12:20		3限目			
	12:20～13:20	昼食休憩	休憩			
1限目	13:20～14:20	13:00～　受付開始 13:15～　開講式	4限目			
休憩	14:20～14:30	休憩	休憩			
2限目	14:30～15:30	【講義】 Microsoft Defender For Endpointを利用したインシデント対応	5限目			（演習結果発表・解説）
休憩	15:30～15:40		休憩			休憩
3限目	15:40～16:40	セキュリティを理解するための技術的要点解説	6限目			15:30　閉講式 16:30　解散
休憩	16:40～16:50		休憩	（演習結果発表・解説） ※随時休憩	（演習結果発表・解説） ※随時休憩	
4限目	16:50～17:50	Hackingで使用される技術・ツール要点解説 ※随時休憩	7限目			
		会場移動（会津若松駅周辺ホテ				
		18:30～ 懇親会（演習グループ発表及び自己紹介） 20:30　現地解散				

＜本講座の特色＞
講義は、いつでも受講可能な**動画アーカイブ配信**です。
演習及び演習に関連する講義は、現地会場で開催します。
演習では**「攻撃手法」を学ぶ**ことで、防御する立場の際も、より攻撃者の視点に立った防御策の策定に取り組むことができます。

※講義の内容や時間割は今後変更する場合があります。

受講対象

以下の要件を満たし、より高度な情報セキュリティの知識・技能習得を希望される方を対象としています。

①情報通信分野全般の基礎知識を有し、Linuxコマンドを理解できる
②システム/ネットワーク管理・運用業務で3年程度の技術者経験がある
③情報セキュリティに関する知識・技能の習得及び実社会での活用に意欲を持っている

開催概要

【日程】	**2025年12月 9日（火）13：15 開講　予定** **～12月12日（金）16：30 終了　予定** **（計　4日間）**
【カリキュラム】	前記「講座内容」をご参照下さい。 ※講義、演習はすべて日本語で行います。
【　会　場　】	**公立大学法人会津大学** **先端ICTラボ（LICTiA）** 〒965-8580 福島県会津若松市一箕町鶴賀 https://u-aizu.ac.jp/access/ ※会津若松駅周辺から会津大学会場まで、 本講座にて送迎のバスをご用意します。
【募集定員】	３０名
【受講料】	1人あたり**３６３，０００円（税込）** ※会場での講義・演習４日間及び配信用講義を含みます。 ※受講料のお支払いは、開催決定後、請求書を発行させていただき、 講座開催日前日までのお振込みをお願いしております。 詳細は、別途ご案内をさせていただきます。
【講座申込方法】	受講申込書に必要事項を記載し、E-mail又はＦＡＸにて以下の申込先にご送付下さい。 お申し込み後、申し込み受付の連絡をさせていただきます。 申込受付の連絡をもちまして、正式な申し込みとなります。 なお受講案内・申込書等電子データは、以下大学ホームページに掲載します。 ※正式申込み後のキャンセルは不可となります。 URL　：　https://u-aizu.ac.jp/information/2025-5.html
【募集期間】	２０２５年１１月　７日（金）まで （定員になり次第、締め切らせていただきます。）
【その他】	※開催時の定員に達しない場合、本講習会が中止となる場合がありますことをご了承願います。

定員に余裕がある場合、
募集期間を延長して受付します。
講習会事務局までお問合せください。

【お問い合わせ】

＜講習会事務局：お問合せ・申込先＞
株式会社エフコム　講習会担当：佐々木
Tel　024-922-2660（平日9:00～17:00）
Fax　024-922-2450
E-mail　s-sasaki@f-com.co.jp

＜大学担当部門＞
公立大学法人 会津大学　復興創生支援センター　担当：屋代
Tel　0242-37-2533（平日9:00～17:00）
Fax　0242-37-2778
E-mail　revitalization@u-aizu.ac.jp

２．５版