主催：会津大学・株式会社ＦＳＫ

WEB会議システムとリモートデスクトップを活用して
職場・自宅などから遠隔で参加できる　**オンライン研修**

2021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】講習：２０２２年１月３１日（月）～２月　４日（金）５日間

【演習方法】オンライン研修（オンライン方法の詳細は別紙参照）

【募集定員】３０名

【受講料】１人あたり３３０,０００円（税込）
（3名以上でお申し込みの場合、団体料金プランあり）

【募集期間】２０２１年１２月２１日（火）まで
（定員になり次第、締め切らせていただきます。）

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。

本年度の
特別講義

ＮＴＴ東日本
ネットワーク事業推進本部
ネットワークセキュリティ推進室

大手通信キャリア電気通信設備の
セキュリティ対策全般を担う現場より
最新の攻撃動向や取り組みについて
ご紹介します

本講座について

本講座は、情報セキュリティの脅威と対策ならびにサイバー攻撃と防御の手法を具体的に理解し、企業等の組織においてサイバー攻撃に対する対応策の企画、適用が可能な実践力を身につけることを目的として実施します。

本年度は平成25年度より実施した本講座において大変に評判の高かった「サイバー演習」を中心に、最新の技術動向を反映して開催いたします。本講座には以下のような特徴があります。

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　上級准教授）
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。

○小林　淳史（東日本電信電話㈱　ネットワーク事業本部　ネットワークセキュリティ推進室）
ＮＴＴ入社後は、ＩＳＤＮ・移動体通信網の交通機開発に従事。その後研究所にてトラヒック監視技術の研究に携わりながらIPFIXの標準化に貢献。IETFでは、ＲＦＣ５９８２、６１８３，６６１５等を執筆。現在は、セキュリティ運用サービスの企画・運用業務に従事。

○川内　裕文（東日本電信電話㈱　ネットワーク事業本部　ネットワークセキュリティ推進室）
2011年入社。NTTセキュリティUS　セキュリティオペレーションセンターにて、セキュリティアナリスト・脅威情報の収集・CASB検証として従事。帰国後は、本社にてマネージドセキュリティサービスの立ち上げ・基盤構築・運用を担当。

○福原　英之（三井物産セキュアディレクション（株）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。

○山崎　治郎（会津大学　客員教授）
1988年ネットワンシステムズ株式会社創立時よりネットワークエンジニアとして、多数の大手企業や通信事業者の情報通信用のネットワーク設計・構築に携わる。2012年8月に会津大学に招聘され、”持続循環社会を実現するスマートグリッドのためのビッグデータ・スマートアナリシス”をテーマとした研究開発に従事。再生可能エネルギーに関連した実証プロジェクトを産業技術総合研究所、各研究機関と推進。主な研究分野は、スマートグリッド・再生可能エネルギーに関する通信ネットワーク・ビッグデータ解析技術等。

○国井　傑　（(株)エストディアン　代表取締役　シマンテック認定トレーナー ）
インターネットサービスプロバイダー企業での立ち上げ、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。Microsoft　MVP。

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演習を行います。このサイバー演習に理想的な環境をベースとして本講座向けに作成したシナリオを用いた実践的な演習を中心に実施します。本学の講座の特色として、「攻撃手法」から防御技術を学ぶことに重点をおいた演習です。

過去の演習　（本年はオンラインで開催）

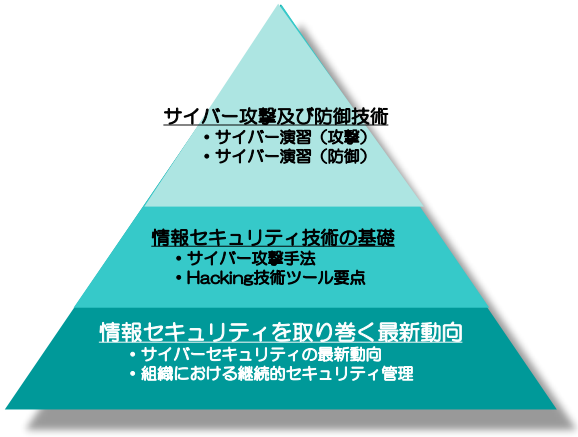
サイバーレンジとは：

サイバー攻撃・防御の演習を実施することができる演習環境アプライアンスで、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模擬した環境を仮想環境上に構築する事が可能です。本環境を用いて攻撃者と防御者に分かれての様々な演習を繰り返して実施することができ、これにより実践的なサイバーセキュリティ専門家の育成が可能となります。

このサイバー攻撃/防御演習では、“インシデントハンドラー”と呼ばれる情報セキュリティ事故対応者に必要となる実践的なスキルを身に付けることを目指します。すなわちインシデントの検知、状況分析、的確な対応指示が具体的できることです。CSIRTに必要な要員育成に最適な演習です。

情報セキュリティの最新動向・管理・技術を網羅

講座の前半で情報セキュリティ全般とサイバー攻撃手法の基本的知識を習得するための講義を実施します。
講義内容は、サイバーセキュリティの最新動向、企業のセキュリティ管理の学習を踏まえた上で、サイバー攻撃手法、組織における継続的セキュリティ管理など情報セキュリティ技術の基礎領域をカバーしています。講義では、実際に発生した具体事例等の紹介を行い、学習者の探究心を喚起します。
そして、講座後半で実施するサイバー演習への理解を深めることで、学習目標達成の動機づけを図ることができる学習効果の高いカリキュラムとなっています。



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、経済産業省の「産学連携イノベーション促進事業」の採択を受け、「サイバー攻撃対策演習講座」を平成25年度から実施し、２７年度からは独立した事業として継続してまいりました。

ますます強まるニーズに答えるため、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　学長　宮崎　敏明

講座内容

講義は実践演習を中心に、計５日間で下記内容を実施します。（講義・演習名及び内容は変更の場合がございます。ご了承ください）

	講義・演習名	講義・演習概要とねらい
講義	昨今の攻撃事例とインシデント対応事例	インシデントが発生した際には、SOCでの緊急対応が迫られるます。過去の対応事例を元に、どのような解析・是正措置がなされたのか解説します。
講義	セキュリティオペレーションセンタの日常業務	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やプロセスを紹介し、業務活動の中で必要とされる技術や知識について解説します。
講義	サイバーセキュリティインシデントの事例	インシデントが発生した際は、現実的な対応はそれぞれの組織のおかれた環境によって異なります。どのように準備して対応すべきか、そのエッセンスを解説します。
講義	IaCとセキュリティ	根本的な対策が難しい攻撃が増えることが想定される中、IaC（Infrastructure as Code）が、サイバーレジリエンスと脆弱性管理にどう役立つかについて解説いたします。
講義	DX時代の組織的セキュリティ管理	セキュリティインシデントは、外部からの攻撃ばかりでなく内部人員の行為を原因とするものも増加傾向にあります。講師の経験などから実践的な対応・考慮点について解説し、組織における継続的な体制の強化について解説します。
講義	IoTセキュリティ	IoTの特徴とセキュリティ上の課題・リスクについて理解を深め、その対策のポイントと検討の流れについて解説します。
講義	サイバーセキュリティインシデントの事例	インシデントが発生した際は、現実的な対応はそれぞれの組織のおかれた環境によって異なります。どのように準備して対応すべきか、そのエッセンスを解説します。
講義	Microsoft Defender for Endpointを利用したインシデント対応	Microsoft Defender For Endpointは、攻撃を迅速に阻止し、組織内の対象の防御を進化させるのに役立つことから、インシデント発生時の対応について解説いたします。
講義	サイバー攻撃概説・セキュリティを理解するための技術要点解説	サイバー攻撃を理解する上で必要となる攻撃の基本原理、標的ネットワークの偵察技法と技術、主要な通信プロトコルについてセキュリティの観点で要点を解説します。またWebアプリケーションの攻撃原理やWindows/Linuxプログラムの解析に関する基礎的な講義に加え、標的型攻撃の威力を実感してもらうためのデモンストレーションも行います。
講義	Hackingで使用される技術・ツール要点解説	攻撃者がサイバー攻撃で使用するツールにはどのようなものがあるのか？その動作原理は？といった基本的な事項について要点を解説します。受講生は「攻撃者ができること」を知ることで、攻撃者の観点から自組織の防御策の有効性をより深く理解できるようになります。
演習	サイバー演習　攻撃（初級）	サイバー演習環境上の仮想企業のDMZを標的として、偵察、侵入、情報搾取を行うことで、攻撃者がどのような思考をして攻撃を行うのか？どのようなツールを使用して攻撃を行うのか？サイバー攻撃とはどういうものかを理解します。
演習	サイバー演習　攻撃（中級）	サイバー演習環境を利用し、仮想企業のDMZおよび内部ネットワークに対して実際に偵察、侵入、情報搾取を行います。自らサイバー攻撃することにより標的型攻撃が流行している背景を実体験し、攻撃者はどのようにして内部ネットワークを攻撃するのかを理解します。
演習	サイバー演習　防御（中級）	サイバー演習環境を利用して実際に行ったサイバー攻撃に対して、適切なセキュリティ設定や脆弱性対策の重要性、効果的な防御手法を理解します。

◆2021年度　時間割予定

講義は【WEB会議ソフト】を使用　／　演習は【WEB会議ソフト／遠隔操作ソフト】を使用

		1月31日（月）		2月1日（火）	2月2日（水）	2月3日（木）	2月4日（金）
	9:00～10:00		1限目	【講義】会津大学 上級准教授　中村　章人 IaCとセキュリティ	【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）
	10:00～10:10			休憩	㈱エストディアン 国井　傑 （DMZに対する攻撃演習）	㈱エストディアン 国井　傑 （仮想企業に対する標的型攻撃演習）	㈱エストディアン 国井　傑 （実践的な防御策の策定演習）
	10:10～11:10		2限目	【講義】会津大 上級准教授　阿部　泰裕 DX時代の組織的セキュリティ管理			
	11:10～11:20			休憩			
	11:20～12:20		3限目	【講義】会津大学 客員教授　山崎　治郎 IoTセキュリティ			
	12:20～13:20			昼食休憩			
	13:20～14:20	13:20～　WEB接続受付 13:50～　開講式	4限目	遠隔操作ソフト操作説明及び演習環境の確認 【講義】㈱エストディアン 国井　傑 Microsoft Defender　For Endpoint　を利用したインシデント対応			（演習結果発表・解説）
	14:20～14:30	休憩					休憩
1限目	14:30～15:30	【講義】　東日本電信電話㈱ 川内　裕文 セキュリティオペレーションセンタの日常業務	5限目				15:30　閉講式 16:30　解散
	15:30～15:40	休憩		休憩			
2限目	15:40～16:40	【講義】　東日本電信電話㈱ 小林　淳史 昨今の攻撃事例とインシデント対応事例	6限目	【講義】㈱エストディアン 国井　傑 セキュリティを理解するための技術的要点解説			
	16:40～16:50	休憩		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	
3限目	16:50～17:50	【講義】三井物産セキュアディレクション㈱　福原　英之 サイバーセキュリティインシデントの対応例	7限目	【講義】㈱エストディアン 国井　傑 Hackingで使用される技術・ツール要点解説			

＜本講座の特色＞
職場・自宅等遠隔地から受講可能なオンライン研修です。
「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】	2022年1月　31日（月）13：50開講式予定 ～ 2月　4日（金）16：30終了予定 計5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。
【講習方法】	WEB会議ソフト及びリモートデスクトップソフトを活用したオンライン研修 （オンライン研修方法は別紙参照してください）。 ※オンライン研修のための環境の準備が難しい場合、事務局にご相談ください。 ●貸し出し用遠隔演習パソコンセット（受講料とは別に必要） ノートパソコン1台、モバイルWifiルータ 1台、宅配専用BOX及び宅配便料（往復）　1式 合計　54,395円（税込） ※台数に限りがあるため、講座の申し込みにあわせて申請お願いします。 ※遠隔演習に必要な環境をセットアップした状態で送付させていただきます。
【受講料】	1人あたり330,000円（税込） ※合計5日分です。 ※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。 ＜団体料金プラン＞ 3名～4名で団体様でお申込みの場合、1割引き：1人あたり297，000円（税込） 5名～　で団体様でお申込みの場合、2割引き：1人あたり264，000円（税込） 利用条件：同一企業・団体からの取りまとめてのお申込みの場合ご利用可能。 また適用は募集定員の範囲内となるため、申し込みの際は事務局にお問い合せ下さい。
【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。 URL　：　https://www.u-aizu.ac.jp/information/cyber2021.html
【募集期間】	2021年12月21日（火）まで （定員になり次第、締め切らせていただきます。）
【その他】	※募集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ＦＳＫ　講習会担当：小林・石井・三森
Tel　0246-27-1253（平日9:00～17:00）
E-mail　seminar@fsk-brain.co.jp

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

1．0版