主催：会津大学・株式会社ＦＳＫ
演習教材提供：株式会社シマンテック

2018
新規講座
追加

インシデント対応のための
フォレンジック技術

2018年度

サイバー攻撃対策演習・情報セキュリティ講座

－「攻撃手法」から学ぶ実践型セキュリティ研修－

【日　程】講習：２０１８年１２月３日（月）～１２月７日（金）５日間
【会　場】会津大学
【募集定員】３０名
【受講料】１人あたり３７８,０００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】２０１８年１０月５日（金）まで
（定員になり次第、締め切らせていただきます。）

本年度の
特別講義

シマンテックコーポレーション
チーフストラテジーオフィサー

ジュゼッペ　小林

アークサイト日本法人社長及び
日本HPセキュリティ部門の
戦略事業担当を歴任。
Mandiant社（現FireEye社）の
日本事業責任者を経て現職。
また、数多くの米IT企業の
日本法人代表を務める。

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。平成25年度から29年度に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」を中心に実用的な内容を集中形式にして、本年度開催いたします。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。

○山崎　文明（ネットワンシステムズ(株)、情報安全保障研究所　首席研究員）

大手外資系会計監査法人にてシステム監査に永年従事。システム監査技術者(経済産業省) /英国規格協会公認BS7799 情報セキュリティ・スペシャリスト。システム監査、情報セキュリティ、個人情報保護に関する専門家として情報セキュリティに関する内閣官房安全保障危機管理室、サイバーテロ演習評価委員会委員など政府関連委員会委員を歴任。2006年ネットワンシステムズ株式会社入社。現在は、一般社団法人メディカルITセキュリティフォーラム　理事。また、公益財団法人ハイパーネットワーク社会研究所　共同研究員として研究に従事。

○林　　隆史（新潟大学　教授、会津大学　客員教授）

情報セキュリティ、次世代情基盤などの研究に従事。福島県、会津若松市、郡山市、埼玉県などの情報化アドバイザーや福島県警察のサイバーセキュリティアドバイザーを10年以上つとめ、総務省「自治体のシステム構築のあり方検討会」 などを歴任。情報セキュリティについては、セキュリティマネジメント、エンタープライズアーキテクチャからサイバーセキュリティ、制度とセキュリティなどを包括的に研究している。

○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ティング、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　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。

○ジュゼッペ　小林（シマンテックコーポレーション　チーフストラテジーオフィサー　）

専門はセキュリティーポリシー、プラットフォーム、及びSOCオペレーションを最先端技術で、日本企業の現状に合致した形で構築、アドバイスすること。サイバーセキュリティー攻撃のコンサルティング企業であるMandiant社（現FireEye社）の日本事業責任者を経て現職に至る。
また、SIEMベンダーであるアークサイト（現HP）日本法人社長及び日本HPセキュリティー部門戦略事業担当も歴任した他、Arcot（現CA）,Tricipher（現VMware）,Passmark（現EMC-RSA）などのセキュリティー事業でも日本市場展開を担う。また米IT企業（Teradata, BroadVision, Wind River, Clouderaなど十数社）の日本法人代表を務めた経歴を持つ。University of San Franciscoコンピューターサイエンス学部卒。

○国井　傑　（(株)ソフィアネットワーク　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。

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。

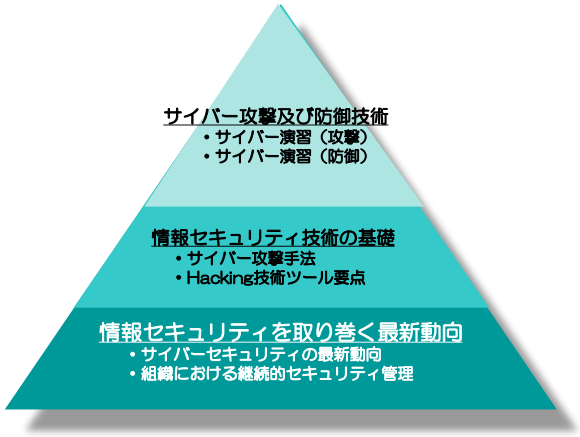
サイバーレンジとは：

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・情報セキュリティ講座」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　　岡　崖一

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・演習名および内容は変更する場合がございます。予めご了承ください）

	講義・演習名	講義・演習概要とねらい
講義	サイバー攻撃の最前線	サイバーセキュリティの最新事例と動向について解説します。
講義	企業セキュリティとサイバーセキュリティ概論	セキュリティはシステムだけでなく、企業をはじめその組織の活動や人も含めて考える必要があります。本講義ではエンタープライズアーキテクチャやエンタープライズセキュリティ計画などを紹介します。その上で、サイバーセキュリティで重要な全体安全と結果安全、サイバーインテリジェンスなどについて解説します。
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。
講義	組織における継続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（新規講座）	インシデント対応のためのフォレンジック技術	サイバーインシデント発生時には、ネットワーク上で発生した事象の確認と被害を受けた端末の状態を把握する必要があります。従来のツールでは習得に時間がかかることから、本講座では、より迅速に対応策の検討が行えるよう被害状況の情報収集とその可視化を効率的に行う方法について解説します。
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。

◆2018年度　時間割予定

		12月3日（月）	12月4日（火）	12月5日（水）	12月6日（木）	12月7日（金）
1限目	9:00～10:00		【講義】組織における継続的セキュリティ管理	【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			
2限目	10:10～11:10	特別講義	【講義】シマンテック 	（DMZに対する攻撃演習）	（仮想企業に対する標的型攻撃演習）	（企業における実践的な防御策の策定演習）
	11:10～11:20		休憩			
3限目	11:20～12:20		【講義】ネットワンシステムズ			
	12:20～13:20		昼食休憩			
4限目	13:20～14:20	13:00～　受付 13:50～　開講式 新規講座追加	【講義】インシデント対応のためのフォレンジック技術①			
	14:20～14:30	休憩	休憩			
5限目	14:30～15:30	【講義】サイバー攻撃の最前線	【講義】インシデント対応のためのフォレンジック技術②			（演習結果発表・解説）
	15:30～15:40	休憩	休憩			休憩
6限目	15:40～16:40	【講義】企業セキュリティとサイバーセキュリティ概論	【講義】セキュリティを理解するための技術的要点解説			15:30　閉講式 16:30　解散
	16:40～16:50	休憩	休憩			
7限目	16:50～17:50	【講義】サイバーレジリエンスに向けて	【講義】Hackingで使用される技術・ツール要点解説	（演習結果発表・解説） ※随時休憩	（演習結果発表・解説） ※随時休憩	
		会場移動 19:00～ 演習グループ発表 及び自己紹介 20:45　現地解散				

＜本講座の特色＞
具体的な「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】	2018年12月　3日（月）13：00受付開始 ～12月　7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。
【会場】	公立大学法人会津大学 〒965-8580 福島県会津若松市一箕町鶴賀 http://www.u-aizu.ac.jp/access.html
【募集定員】	30名
【受講料】	1人あたり378,000円（税込） ※合計5日分です。テキスト代を含みます。 ※交通費、宿泊費、飲食費は含まれておりません。 ※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、2割引き：1人あたり302，400円（税込） 5名～9名で団体様でお申込みの場合、 3割引き：1人あたり264，600円（税込） 10名以上の団体様でお申込みの場合、4割引き：1人あたり 226，800円（税込） 利用条件：同一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：http://www.u-aizu.ac.jp/information/cyber2018.html
【宿泊施設】	宿泊費は受講者負担となります。各自にて、ご予約をお願いします。 ※推奨宿泊施設は追ってご案内させていただきます。
【募集期間】	2018年10月5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】	※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。

【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・樋口
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
Tel　0242-37-2533（平日9:00～17:00）
Fax　0242-37-2778
E-mail　revitalization@u-aizu.ac.jp