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）

サイバーセキュリティの技術的側面・非技術的側面の両方を含む講義・演習

2025年11月10日 現在

九州大学 KYUSHU UNIVERSITY × Kyutech ARISE

講　座　概　要

特　　徴	企業が情報システムを利用するのは、その企業の目的を果たすためです。その事業継続のためにサイバー攻撃から情報システムを守ることは、企業経営の最重要課題となり、そのための人材をその企業内で育成することも大切な課題です。企業で育成すべき人材がサイバーセキュリティ対策のために学ぶべきこととしては、サイバーセキュリティに関連する情報技術を習得するのも大切ですが、関連法制、危機管理、ヒューマンファクタ、サイバーセキュリティ関連ビジネスなど多岐にわたる情報技術以外の要素も体系的に学ぶ必要があります。また本講座では、九州大学で2018年から実施してきたProSec-IT/SECKUNの経験から実施してきた社会人が学び易いさまざまな工夫をここでも継承しています。
受講資格	•学歴や経験は問いません •組織のCISO、CISO補佐、サイバーセキュリティ責任者、先端技術者を目指す方、経営管理部門の方、ユーザ企業の情報システム管理部門、サイバーセキュリティを含む情報技術に興味を持ち社会に貢献したいと考える方
募集時期	第1期　2025年4月～2025年7月19日（土） 第2期　2025年4月～2025年12月13日（土）
受講期間	第1期　2025年5月26日（月）～2025年9月26日（金） 第2期　2025年10月1日（水）～2026年3月1日（日）

詳細はKyutech ARISE　HPをご確認ください。

お問合せ　株式会社Kyutech ARISE　Mail: info@kyutech-arise.co.jp

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）

サイバーセキュリティの技術的側面・非技術的側面の両方を含む講義・演習

系統	科目・概要	講師名	実施方法	定員	受講料（税込）	2025年度開講時期	学習時間（目安）
テック(Tech)系	**サイバーセキュリティ基礎演習1** サイバーセキュリティ対策を行うための基礎となるシステム、ネットワークの利用方法について、基礎的なコマンドの利用方法、考え方などをゼロベースから学ぶ。	小出 洋	遠隔非同期 (一部同期あり)	なし	44,000	第1期 および第2期	22.5時間
	サイバーセキュリティ基礎演習2 ウェブ、サイバーセキュリティ、マイクロアーキテクチャ攻撃など、ネットワークおよびCPUアーキテクチャなどの観点から演習とともに学ぶ。	岡村 耕二 粕淵 卓 谷本 輝夫 長谷川 陽介 池田 奎吾	遠隔同期	なし	110,000	通年 2025年度の応募は締め切りました	26時間
	クラウドコンピューティングとセキュリティ クラウド環境の特徴と、その「便利さの裏にあるリスク」と「管理の方法」を技術・運用・法制度の観点から体系的に学ぶ。	近藤 宇智朗 平賀 博司 松本 照吾 松山 保 森田 浩平	遠隔同期	なし	110,000	第2期	26時間
	フォレンジック演習 サイバー攻撃、情報漏洩などのインシデントが発生した際に、その原因や影響を技術的に調査・分析するスキルを実践的に学ぶ演習を行う。	赤松 孝彬 折田 彰 杉山 一郎	対面+遠隔同期	なし	66,000	2025年度 開講無し	10.5時間
	サイバーセキュリティ概論 昨今のサイバーセキュリティ、情報セキュリティの現状について網羅的に学ぶ。	中井 博 西尾 太一 原 昌巳 吉井 和明	対面+遠隔同期	なし	66,000	2025年度 開講無し	12時間
	AIセキュリティ特論 近年急速に発展しているAIにおけるセキュリティ対策を学ぶ。特に、機械学習及び生成AIに関する攻撃手法及びその対策に関する知識を習得する。さらに、AIシステムに対する脅威モデリング演習を通して、AIシステムに対する脅威を理解する。	服部 祐一	対面+遠隔同期	なし	110,000	第2期	22.5時間
戦略・マネージメント(Strat/Mgmt)系	**セキュリティ心理学** 人間の心理や行動等の観点からのセキュリティを対象とし、ノンテクニカルな面からのセキュリティの考え方と対策を学ぶ。	内田 勝也	対面+遠隔同期	なし	110,000	2025年度 開講無し	22.5時間
	情報セキュリティマネジメントシステムとリスクマネジメント 情報セキュリティマネジメントシステム（ISMS）とリスクマネジメント(情報セキュリティのPDCAサイクル)について学ぶ。	内田 勝也	対面+遠隔同期	なし	110,000	2025年度 開講無し	22.5時間
	クライシスマネージメント演習 昨今、サイバー安全保障、経済安全保障等、サイバー分野問題は国際動勢の流れを受けて大きく変化している。本講座では、これら問題の背景を含めた最新状況を解説する。また、事例を基に各部署要判断事項の作成体験及びBCP体験型机上演習を通じてサイバー攻撃による大規模システム障害時における事業継続（BCP）の体制構築手法について学ぶ。	岡谷 貢 有本 真由	対面+遠隔同期	なし	110,000	第2期	22.5時間
	セキュリティとコンプライアンス経営 企業の資産（情報・人材・信頼）を守りながら、法的責任や倫理的責任を果たし、持続可能で信頼される経営を実現するための考え方を学び、受講生の具体的な課題を抽出したものを共有する。	大久保 紀彦	対面+遠隔同期 +遠隔非同期	なし	44,000	2025年度 開講無し	15時間
	ビジネスイノベーションと安全保障 イノベーションを引き起こす経営とともに、「技術が社会・国家・世界に与える影響」を視野に入れた経営を考える際に念頭におくべき知識・スキルを学ぶ。	大木 元 東海林 昌幸 白川 聖明 日野 隆史 福田 峰之 原田 将志	対面+遠隔同期	なし	110,000	2025年度 開講無し	21時間
	セキュリティ関連法と実務 情報セキュリティに関する法律、ガイドラインなどを理解し、実際のビジネスや業務運用などへの適用方法について学ぶ。	中井 博 西尾 太一 湯淺 墾道	遠隔同期	なし	110,000	第2期	15時間

※各科目の詳細はKyutech ARISE HPより、シラバスをご確認ください。

お問合せ　株式会社Kyutech ARISE　Mail: info@kyutech-arise.co.jp

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）

サイバーセキュリティの技術的側面・非技術的側面の両方を含む講義・演習

テック(Tech)系

科目	講師名	実施方法	開講時期	受講料
サイバーセキュリティ基礎演習１	小出　洋	遠隔非同期型（一部同期あり）	第1期及び第2期 ・第1期同期日 （土曜日10:00-12:00） 6/7　SSH, Webｾｷｭﾘﾃｨ 6/14　Webﾌﾟﾛｸﾞﾗﾐﾝｸﾞ 6/21　ｱｾﾝﾌﾞﾗ 6/28　Dockerｺﾝﾃﾅ 7/5　IoTｾｷｭﾘﾃｨ 7/12　MTD ・第2期同期日 (10:00-12:00) 10/11　SSH, Webｾｷｭﾘﾃｨ 10/18　Webﾌﾟﾛｸﾞﾗﾐﾝｸﾞ※ 10/25　ｱｾﾝﾌﾞﾗ 11/8　Dockerｺﾝﾃﾅ 11/23　IoTｾｷｭﾘﾃｨ 12/21　MTD ※10/18のみ13:00-15:00	44,000円 （税込）
サイバーセキュリティ基礎演習２	岡村 耕二 粕淵 卓 谷本 輝夫 長谷川 陽介 池田 奎吾	遠隔同期型	通年 同期日 8/23、8/24　8:30～16:30 9/14　9:00～16:20 10/18　9:00～12:10 10/25　13:00～16:10 2025年度の応募は締め切りました	110,000円 （税込）
クラウドコンピューティングとセキュリティ	近藤 宇智朗 平賀 博司 松本 照吾 松山 保 森田 浩平	遠隔同期型	第2期 2025年 11/23　13:00～16:10 2026年 1/24　13:00～18:00 2/1　13:00～18:00 2/7　13:00～18:00 2/28　13:00～18:00 3/1　9:30～12:30	110,000円 （税込）
フォレンジック演習	赤松 孝彬 折田 彰 杉山 一郎	対面+遠隔同期型	2025年度開講無し	66,000円 （税込）
サイバーセキュリティ概論	中井 博 西尾 太一 原 昌巳 吉井 和明	対面+遠隔同期型	2025年度開講無し	66,000円 （税込）
AIセキュリティ特論	服部 祐一	対面+遠隔同期型	第2期 同期日 10/26、11/1、11/30、12/7、12/14 (10:00-16:00 途中休憩あり) 対面会場は福岡市内予定	110,000円 （税込）

※最新の情報はKyutech ARISE HPをご確認ください。

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）

サイバーセキュリティの技術的側面・非技術的側面の両方を含む講義・演習

戦略・マネージメント(Strat/Mgmt)系

科目	講師名	実施方法	開講時期	受講料
セキュリティ心理学	内田 勝也	対面+遠隔同期型	2025年度開講無し	110,000円 (税込)
情報セキュリティマネージメントシステムとリスクマネージメント	内田 勝也	対面+遠隔同期型	2025年度開講無し	110,000円 (税込)
クライシスマネージメント演習	岡谷　貢 有本　真由	対面+遠隔同期型	第2期 同期日 11/ 1(土) 11/16(日)	110,000円 (税込)
セキュリティとコンプライアンス経営	大久保 紀彦	対面+遠隔同期 +遠隔非同期	2025年度開講無し	44,000円 (税込)
ビジネスイノベーションと安全保障	大木 元 東海林 昌幸 白川 聖明 日野 隆史 福田 峰之 原田 将志	対面+遠隔同期型	2025年度開講無し	110,000円 (税込)
セキュリティ関連法と実務	中井 博 西尾 太一 湯淺 墾道	遠隔同期型	第2期 同期日 11/22(土)　13:00～18:00 12/27(土)　13:00～14:30 2/21(土)　13:00～16:30 2/22(日)　9:00～16:30	110,000円 (税込)

※最新の情報はKyutech ARISE HPをご確認ください。

テック(Tech)系

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		サイバーセキュリティ基礎演習1			
必修・選択		―	単位	―	
概要・目的		サイバーセキュリティの技術的な側面であるWeb、IoT、アセンブラ、仮想化技術に関連する幾つかの基本的な要素技術を習得する。さらに発展的な内容である Moving Target Defense を習得する。この講義・演習によりサイバーセキュリティの要素技術に関する学び方を身に付ける。			
到達目標		サイバーセキュリティに関連する要素技術を習得する。新しい要素技術の学び方を理解する。			
授業方法		講義＋演習	実施形態	遠隔同期＋遠隔非同期	
評価方法		演習の進捗状況により総合的に評価する。		第1期 同期日	第2期 同期日
授業項目	1	SSHクライアントの使い方		6/7	10/11
	2	Webセキュリティ演習1			
	3	Webセキュリティ演習2			
	4	Webアプリケーションセキュアプログラミング1		6/14	10/18
	5	Webアプリケーションセキュアプログラミング2			
	6	ARM64アセンブラ演習1		6/21	10/25
	7	ARM64アセンブラ演習2			
	8	仮想化とセキュリティ・Dockerコンテナ入門1		6/28	11/8
	9	仮想化とセキュリティ・Dockerコンテナ入門2			
	10	仮想化とセキュリティ・Dockerコンテナ入門3			
	11	IoTセキュリティ演習1		7/5	11/23
	12	IoTセキュリティ演習2			
	13	IoTセキュリティ演習3			
	14	Moving Target Defense演習1		7/12	12/21
	15	Moving Target Defense演習2			
使用教材		スライド、IoT用の実験電子部品			
特記事項		遠隔同期で演習支援予定。時刻は各日10:00～12:00 ※10/18のみ13:00～15:00 受講生からの質問対応、ハンズオンでうまく行かない場合についての問題解決を一緒に行う。 各回の演習支援を録画した動画を、後日受講生に配信予定。			

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	サイバーセキュリティ基礎演習2		
必修・選択	―	単位	―

概要・目的

サイバーセキュリティに関する具体的な事例を挙げながら、セキュリティを維持するための基礎的な講義と演習を行うことで実戦的な知識を身に付ける。

まず、サイバー演習用のソフトウェアを用いたハンズオン形式でサイバーセキュリティについて学ぶ。サイバー演習では、典型的なサイバー攻撃についてまず座学により技術的な用語や概念を学び。次に、各人のノートパソコンに導入された演習環境によって実機と同じ感覚で学習、体験を行い、本演習で得られたセキュリティ対策のための知識、技術の確認を行う。また、攻撃を受けた脆弱性の修復方法についても学ぶ。本サイバー演習によって、ネットワークやサーバの実際の管理・運用業務に直接携わらなくても、サイバー攻撃を体験し、それを防ぐ技術を習得することができる。

次に、 コンピュータ・システムに対するソフトウェアを用いた攻撃の1つである「マイクロアーキテクチャ攻撃」について、その原理や成立条件、対処法について学ぶ。ソフトウェアのハードウェア上での振る舞いに着目してセキュリティを考察する視点を身に着ける。プロセッサ・シミュレータを用いた演習により、マイクロアーキテクチャ・レベルの動作解析を体験する。

さらに、Webアプリケーションに対する攻撃手法の原理とその対策について技術的要素の基礎知識を習得する。また、Webアプリケーションへの攻撃に対する脅威の考え方についても習得する。

最後に、「8割解けるCTF(Capture The Flag)」をコンセプトにしたWEST-SEC CTFを開催する。

CTFは、「初心者」であっても、答えとなるFlagを「ゲームを通じて」探しながら、チームで力を合わせ「みんなで楽しく」、基礎から網羅的に「セキュリティが学べる」コンテンツである。一方的な講義と違い、セキュリティの問題に関して、自らが考え、チームと相談し、各種ツールを駆使し、調べることを通じて答えを導き出すプロセスを学ぶ。

到達目標

セキュリティに関する脆弱性に対する典型的なサイバー攻撃のパターン・シナリオを理解する。脆弱性を発見し、修復できる能力を身に付けることができる。

加えて、プロセッサおよびメモリ・アーキテクチャとマイクロアーキテクチャ攻撃に関する基本的な知識を習得した上で、プロセッサ・シミュレータを用いたマイクロアーキテクチャ・レベルの動作解析を通して緩和法の重要性を理解できる。さらに、Webアプリケーションに対する攻撃と対策の手法を習得できる。Webアプリケーションに対する脅威についての考え方を理解できる。

最後に、CTFを理解し、他のCTFへの参加意欲が高まり、セキュリティの基礎知識を持ったうえで、課題に対して考えたり相談しながら答えを導き出す力を養うことができる。

授業方法	講義＋演習	実施形態	対面＋遠隔同期

評価方法

受講生から提出されたポートフォリオから理解度、演習の進捗管理チェックリストから演習の遂行の度合いを判断し、総合的に評価を行う。

授業項目

		実施形態	開講日
1	サイバーセキュリティ演習1（岡村）	遠隔同期	8/23
2	サイバーセキュリティ演習2（岡村）		
3	サイバーセキュリティ演習3（岡村）		
4	サイバーセキュリティ演習4（岡村）		
5	サイバーセキュリティ演習5（岡村）	遠隔同期	8/24
6	サイバーセキュリティ演習6（岡村）		
7	サイバーセキュリティ演習7（岡村）		
8	サイバーセキュリティ演習8（岡村）		
9	マイクロアーキテクチャ攻撃１（谷本）	遠隔同期同期	9/14
10	マイクロアーキテクチャ攻撃２（谷本）		
11	マイクロアーキテクチャ攻撃３（谷本）		
12	マイクロアーキテクチャ攻撃４（谷本）		
13	Webセキュリティ入門１（長谷川）	遠隔同期	10/18
14	Webセキュリティ入門２（長谷川）		
15	ＣＴＦを使った実践的なセキュリティのゲーミフィケーション1（粕淵・池田）	遠隔同期	10/25
16	ＣＴＦを使った実践的なセキュリティのゲーミフィケーション2（粕淵・池田）		

使用教材

[授業項目1～8]
IPA 脆弱性体験学習ツール AppGoat
[授業項目9～12]
スライドおよびPC。PCは Docker コンテナを実行可能なものを各自準備すること。
[授業項目13,14]
インターネットに接続可能でWebブラウザー、テキストエディタ等が利用可能な、自身で自由に設定変更やアプリケーションの追加が可能なPC

特記事項

授業項目1～14の講義は、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
[授業項目1～8]
Windows ソフトウェアが動作するPCが必要
[授業項目15,16]
一部の問題を解くのに、TeraTermなどのSSHに接続するツール、パケットキャプチャのソフトであるWiresharkが必要です。

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	ー	単位	ー
概要・目的	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。 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。 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。 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。 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。 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。		
到達目標	・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 ・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。 ・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。 ・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。 ・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。 ・WebAssemblyをサーバサイドで動作させることができる ・WebAssemblyの線形メモリなど主要な仕様を把握できる ・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 ・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		
授業方法	講義＋演習	実施形態	対面＋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)	1/24
	4	クラウドセキュリティ2(松本／平賀)	
	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)	2/1
	7	クラウドセキュリティ5(松本／平賀)	
	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)	2/7
	10	クラウドセキュリティ8(松本／平賀)	
	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)	2/28
	13	ソフトウェアサプライチェーンセキュリティ2(松山)	
	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)	3/1
	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)	

使用教材	[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。
特記事項	※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 [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

テック(Tech)系

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	AIセキュリティ特論			
必修・選択	―	単位	ー	
概要・目的	近年急速に発展しているAIにおいて、そのセキュリティ対策を理解することは非常に重要である。 本講座では、機械学習及び生成AIに関する攻撃手法及びその対策に関する知識を習得する。さらに発展的な内容である AIシステムに対する脅威モデリング演習を行うことにより、AIシステムに対する脅威を理解するとともに脅威モデリングの手法を習得する。			
到達目標	機械学習及び生成AIに対する攻撃手法とその対策について理解し説明できる。 また、脅威モデリングの手法について理解し、実施できる。			
授業方法	講義＋演習	実施形態	対面＋遠隔同期	
評価方法	出席状況、レポート等の結果を総合的に判断し、評価する。		実施形態	同期日
授業項目 1	はじめに		遠隔同期	10/26
2	機械学習とは			
3	機械学習に対する攻撃手法とその対策			
4	機械学習に対する攻撃手法とその対策		遠隔同期	11/1
5	生成AIに対する攻撃手法とその対策			
6	生成AIに対する攻撃手法とその対策			
7	生成AIに対する攻撃演習		遠隔同期	11/30
8	生成AIに対する攻撃演習			
9	生成AIに対する攻撃演習			
10	脅威モデリングとは		対面	12/7
11	AI脅威モデリング演習			
12	AI脅威モデリング演習			
13	AI脅威モデリング演習		対面	12/14
14	AI脅威モデリング演習			
15	おわりに			
使用教材	スライド Pythonスクリプト			
特記事項	1日あたり3コマ実施予定 第1回と第2回講義(授業項目1～6)の様子は録画し後日配信するため、実施日以降も申込可能(11/20まで) 第3回受講開始までに第1回および第2回の講義参加、あるいは講義動画を視聴しておく必要あり			

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		クライシスマネージメント演習		
必修・選択		―	単位	ー
概要・目的		国際情勢を背景に経済安保、サイバー安保等サイバー分野に関わる政府体制整備が急務な中、サイバーセキュリティは国家安全保障の一部としてのサイバー活動問題に変化。サイバー安保関連法解説を中心にサイバー分野問題の背景と最新動向を解説します。また、サイバー攻撃が事業継続問題に発展した場合の各部署要判断対応事項を整理したアクションチャート（行動計画）作成体験とBCP体験型机上演習によりサイバー攻撃に関わる組織内BCP体制を考える事が出来る人材を育成します。		
到達目標		サイバー分野問題全体を俯瞰理解した上で、アクションチャート（行動計画）作成体験と机上演習により、BCP(事業継続計画）作成スキルを身につける。		
授業方法		講義＋演習	実施形態	対面＋遠隔同期
評価方法		演習の進捗状況により総合的に評価する。		開講日
授業項目	1	サイバー分野問題概論１（コース開始時の諸情勢を基に）		11/1(土) 10:00～12:00
	2	有本弁護士講義「国際法制等」１		日程調整中
	3	アクションチャート作成講義		
	4	アクションチャート作成実習１（講義、課題設定）		
	5	アクションチャート作成実習２（グループ作業）		
	6	アクションチャート作成実習２（グループ作業）		
	7	アクションチャート作成実習３（発表）		
	8	BCP体験型机上演習（医療分野シナリオ）１		
	9	BCP体験型机上演習（医療分野シナリオ）２		
	10	BCP体験型机上演習（製造分野シナリオ）１		
	11	BCP体験型机上演習（製造分野シナリオ）２		
	12	分野問題概論２（コース終了時の諸情勢を基に）		
	13	有本弁護士講義「国際法制等」２		
	14	命の講義「さあ～命の話をしよう！」（前半：自衛隊パイロット体験から）		
	15	命の講義「さあ～命の話をしよう！」（後半：東北震災体験から）		
使用教材				
特記事項		11/1の初回講義は遠隔同期形式(対面無し)で実施いたします。 2回目以降の開講日は決定次第、掲載します。 11/1開講後も受講お申し込みは可能です。 途中参加の方には講師よりオンライン形式にて、補講を実施いたします。 補講日程につきましては、講師よりご連絡いたします		

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	セキュリティ関連法と実務				
必修・選択	―	単位	―		
概要・目的	まず、情報セキュリティやサイバーセキュリティに関する実務においては、関連する法令を理解し、遵守することが不可欠である。またインシデントハンドリング等においても、法令に基づく対応が求められる。そこでサイバーセキュリティに関連する法律について学ぶ。 加えて、2023年に電気通信事業法が改正された。電気通信事業法は「通信の秘密」等に関する法律で、一見すると自分たちの事業には関係が無いと考えがちであるが、今回の改正で、いわゆるCookieに対する規制が事実上導入され（外部送信規律）、多くのウェブサイト運営者に影響するものになった。この法律の前提となる議論、総務省の本来の目的、そして運用が始まった同法について、法律の成立から企業実務の対応までを対象賞とする。担当者が所属した株式会社メルカリの中で、他社（株式会社リクルート、LINEヤフー株式会社など）やJIAAといった団体で議論していきながら辿り着いたことなどを手掛かりに、そして、受講者が所属する企業等が未対応であった場合に、何を事を考えて実施すれば良いのかなどのヒントとなることを目指す。 最後に、ビジネスを行うには、技術や経営、会計といった様々なスキルに加え、法律も重要なスキルといえる。特に、IT分野では、様々な立法がなされているところであるが、こういった法律を、正しく読み解くためには法律全体を通して貫かれている文法とでもいうべき事項や、最先端の法律が使えなくなったときに立ち返るべき民法などの基本法の知識が必要となる。 ここでは、まず、法律とはなにか、法律で一体何を決めているのか、条文をどのように読めばよいのかといった、法律ユーザーとしての基本を学び、その上で、基本法であるが、ビジネスにおいて非常に重要な民法を全体的に学ぶ。時間があれば、技術者にとって縁の深い、知的財産権法にも触れる。これらを学習することで、法律を使う上で信頼できる情報が何であるか、それをどう読み解くのかといった「正しい法律の使い方」を習得することができ、新しい法律に出会ったときにも対応する力を身につけることができる。また、法務や経営層と対話をする際の共通言語としての法律を身につけることができる。				
到達目標	サイバーセキュリティに関する主要な法律の内容を理解できる。 インシデントハンドリング等において法令に基づいて対応することができる。 サイバーセキュリティに関する最新の立法を理解できる。 「電気通信事業法」の改正の内容を把握し、自社のビジネスへの影響度を把握できる。さらに、営業における対応方針を思慮できるまでになる。 条文を読むこと、探すことができる。また、深読みという名の不可読みを回避し、法律に関する情報の取捨選択ができるようになる。 民法（特に債権法）について、どのような考え方に基づいてどのような制度があるのかを知ることで、契約実務を中心としたビジネス対応力を身につけることができる。				
授業方法	講義	実施形態	対面＋遠隔同期		
評価方法	講義への出席、および、受講生、講師とのディスカッション毎回の講義のポートフォリオの内容を総合して評価を行う。			実施形態	同期日
授業項目 1	デジタル新法1（湯浅）			遠隔同期	11/22
2	デジタル新法2（湯浅）				
3	デジタル新法3（湯浅）				
4	改正電気通信事業法（中井）			対面+遠隔同期	12/27
5	サイバーセキュリティ訴訟実務1（西尾）			対面+遠隔同期	2/21
6	サイバーセキュリティ訴訟実務2（西尾）				
7	サイバーセキュリティ訴訟実務3（西尾）			対面+遠隔同期	2/22
8	サイバーセキュリティ訴訟実務4（西尾）				
9	サイバーセキュリティ訴訟実務5（西尾）				
10	サイバーセキュリティ訴訟実務6（西尾）				
使用教材	[授業項目1～3] サイバーセキュリティ関係法令Q＆Aハンドブック https://security-portal.nisc.go.jp/guidance/law_handbook.html [授業項目4] 講師が用意するスライドのみ ※参考：「Cookieポリシー作成のポイント」 [授業項目5～10] 特になし。法律文法については、拙作のテキストを配信します。				
特記事項	講義実施日程 11/22　13:00～18:00 12/27　13:00～14:30 2/21　13:00～16:30 2/22　9:00～16:30				