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8月26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	対面+遠隔同期	なし	110,000	第2期	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	対面+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	第2期	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	第2期	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	調整中	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	調整中	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 乗口 雅充 日野 隆史 福田 峰之	対面+遠隔同期	なし	110,000	第2期	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	対面+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	対面+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 対面講義会場は福岡市内を予定	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	対面+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 対面講義会場は福岡市内を予定	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	第2期 12/13　10:00～17:30 12/20　10:30～16:10 対面講義会場は福岡市内を予定	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	第2期 同期日 11/8　13:00～16:10 11/22　9:00～12:20 12/27　15:00～18:10 2/21　9:00～12:10 対面講義会場は福岡市内を予定	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) 対面講義会場は福岡市内を予定	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	調整中	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	調整中	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	調整中	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+遠隔同期型+遠隔非同期型	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 乗口 雅充 日野 隆史 福田 峰之	対面+遠隔同期型	第2期 同期日 11/14(金)　9:00～16:30 11/15(土)　9:00～18:00 11/21(金)　13:00～14:30 11/29(土)　9:00～16:30 対面講義会場は福岡市内を予定	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	対面+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 対面講義会場は福岡市内を予定	110,000円 (税込)

※最新の情報はKyutech ARISE HPをご確認ください。

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。			実施形態	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		遠隔同期+非同期	6/7	10/11
	2	Webセキュリティ演習1		遠隔同期+非同期		
	3	Webセキュリティ演習2		遠隔同期+非同期		
	4	Webアプリケーションセキュアプログラミング1		遠隔同期+非同期	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		遠隔同期+非同期		
	6	ARM64アセンブラ演習1		遠隔同期+非同期	6/21	10/25
	7	ARM64アセンブラ演習2		遠隔同期+非同期		
	8	仮想化とセキュリティ・Dockerコンテナ入門1		遠隔同期+非同期	6/28	11/8
	9	仮想化とセキュリティ・Dockerコンテナ入門2		遠隔同期+非同期		
	10	仮想化とセキュリティ・Dockerコンテナ入門3		遠隔同期+非同期		
	11	IoTセキュリティ演習1		遠隔同期+非同期	7/5	11/23
	12	IoTセキュリティ演習2		遠隔同期+非同期		
	13	IoTセキュリティ演習3		遠隔同期+非同期		
	14	Moving Target Defense演習1		遠隔同期+非同期	7/12	12/21
	15	Moving Target Defense演習2		遠隔同期+非同期		
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。		実施形態	開講日
授業項目 1	サイバーセキュリティ演習1（岡村）		遠隔同期	8/23
授業項目 2	サイバーセキュリティ演習2（岡村）			
授業項目 3	サイバーセキュリティ演習3（岡村）			
授業項目 4	サイバーセキュリティ演習4（岡村）			
授業項目 5	サイバーセキュリティ演習5（岡村）		遠隔同期	8/24
授業項目 6	サイバーセキュリティ演習6（岡村）			
授業項目 7	サイバーセキュリティ演習7（岡村）			
授業項目 8	サイバーセキュリティ演習8（岡村）			
授業項目 9	マイクロアーキテクチャ攻撃１（谷本）		対面 +遠隔同期	9/14
授業項目 10	マイクロアーキテクチャ攻撃２（谷本）			
授業項目 11	マイクロアーキテクチャ攻撃３（谷本）			
授業項目 12	マイクロアーキテクチャ攻撃４（谷本）			
授業項目 13	Webセキュリティ入門１（長谷川）		遠隔同期	10/18
授業項目 14	Webセキュリティ入門２（長谷川）			
授業項目 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）		対面 +遠隔同期	10/25
授業項目 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）			
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			

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	フォレンジック演習			
必修・選択	―	単位	―	
概要・目的	前半のデジタルフォレンジックの概要と証拠保全およびデジタルフォレンジック解析基礎演習パートではサイバーインシデントや不正調査、犯罪捜査等で活用されるデジタルフォレンジックの基礎を習得する。あらゆる事象にデジタル機器が関係する社会において、過去に発生した事象を把握するためには、デジタルフォレンジックの活用が欠かせない状況である。 講義では、デジタルフォレンジックの概要を学び、デジタルフォレンジックがどのようなプロセスで実施され、どのようにデジタル証拠を保全するのかを習得する。演習では、架空のインシデントで被害を受けた端末のディスクイメージから、侵害の原因や攻撃者活動の特定に有用ないくつかの証跡（レジストリ、ファイルシステム情報、イベントログ等）について、その分析方法を学び、実際に分析する。 後半の動的マルウェア解析パートでは、マルウェア感染によるインシデント発生時において、マルウェアがシステム上でどのように動作し、どのような痕跡を残し、最終的にどのような被害をもたらすのかを迅速かつ正確に調査・分析できる基礎的な動的解析技術を習得する。			
到達目標	まず、デジタルフォレンジックの概要を理解する。サンプルの証拠の分析を通じて、デジタルフォレンジック調査の一端を経験する。 次に、実際のインシデント対応において、マルウェアの挙動を理解し、適切な封じ込め、駆除、復旧策を立案・実施するための実践的な知識とスキルを身につけることを目指す。			
授業方法	講義	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	デジタルフォレンジックの概要と証拠保全　（杉山/赤松）			12/13
授業項目 2	デジタルフォレンジック解析基礎演習①　（杉山/赤松）			
授業項目 3	デジタルフォレンジック解析基礎演習②　（杉山/赤松）			
授業項目 4	デジタルフォレンジック解析基礎演習③　（杉山/赤松）			
授業項目 5	動的マルウェア解析1（折田）			12/20
授業項目 6	動的マルウェア解析2（折田）			
授業項目 7	動的マルウェア解析3（折田）			
授業項目 8				
授業項目 9				
授業項目 10				
授業項目 11				
授業項目 12				
授業項目 13				
授業項目 14				
授業項目 15				
使用教材	[授業項目5～7] スライド、解析用仮想環境、マルウェア検体、解析ソフトウェア			
特記事項	[授業項目1～4] 解析基礎演習で取り扱う内容（現時点での想定であり、一部変更の可能性があります。） 1. フォレンジックイメージの取り扱い方法 2.ウェブアクセス履歴の分析 3.ファイルシステムに関する証跡の分析 4.プログラムの実行痕跡の分析 5.イベントログの分析 6.データ窃取に係る痕跡の分析 7.その他（Windows端末以外のフォレンジック概要等説明） ※当日受講不可の場合、録画した講義動画視聴による後日の受講可能。 [授業項目5～7] 講座内で使用するマルウェア検体の実行と解析を行うため、Windows の仮想マシン環境を各自でご準備ください。準備方法については、別途手順をご連絡します。			

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	サイバーセキュリティ概論			
必修・選択	―	単位	―	
概要・目的	情報セキュリティに関わる現実にある法的側面や個人情報の取扱などの課題を具体的に理解する事を目的とする。 　まず。情報セキュリティに関する知識を学ぶ前提として、技術の利用に伴う法的責任や社会的影響を理解する。ここでは、実際に発生した刑事事件や法的トラブルを題材に、どのような行為が処罰や損害賠償等の社会的制裁につながるかを学び、情報を扱う際に求められる倫理観や規範意識をもつ。 情報技術は、善にも悪にも使うことができる力であり、その使い方を誤れば重大な結果を招く。情報セキュリティ技術に触れる際には、単なる操作技術にとどまらず、その背景にある社会的ルールや責任を意識する必要がある。トラブルを未然に防ぐ判断力と姿勢は、実務において重要な基盤となる。 　次に、安易なHowToや●●主義といった大風呂敷を広げた解釈論が多く出回っている法律分野について、ユーザーとして必要十分な文法や法律実務における使われ方に加え、法律家がいうところの事実認定の概要を理解することで、眼の前の問題が法律問題であるのか、法律問題であるとしてどのように分析すればよいか、調べるべき事実はどういったものかといったことを素早く見つけられるようにする。 　また、「個人情報」「プライバシー（情報）」「セキュリティ」これら3つの概念はそれぞれが共有し合う部分と独立して存在している。これらが曖昧であるからこそ、このデータプライバシーに関わる実務が常に混乱しているのが現状である。ヤフー株式会社、株式会社メルカリで、セキュリティ、データプライバシー、プライバシーポリシーの構成・概念企画、運用などを行ってきた経験から、これらの3つの概念を明確に認識し、それぞれの実務が安全にかつ頭の整理がスッキリした状態で取り組めるようになることを目指す。 　最後に、実際に稼働しているオンライン広告サービス（LINEヤフー広告）を例に取り、サービスの仕組みや取り扱われるパーソナルデータなどの重要情報に対する安全管理措置、さらにそれらの情報を活用する際の考え方を学ぶ。これを通じて、ITサービス企業が守るべき価値や、ビジネス・社会との関わりについて理解を深める。			
到達目標	情報セキュリティに関連する刑事責任および民事責任の基本的な枠組みを理解し、説明できる。 情報の各種取扱いについて、法的・倫理的な問題点を自ら検討し判断できる。 情報技術の利用場面において、社会的・法的なルールを踏まえた適切な行動を選択できる。 法律問題にあたった際に、一次文献である条文を読むことができる 条文を調べる前に、おそらく、何らかの法律があるはずだというセンスを磨くことができる 事実と評価を峻別することで、正しく議論を行う能力を養うことができる 「個人情報」「プライバシー（情報）」「セキュリティ」のそれぞれの違いが理解できる。 「法律上の個人情報」を認識し、また法律外の情報（非個人情報）であっても考える視点があることを認識し、対応するようにしていただくマインドセットを持つことができる。 日本の様々な事案を参考に、守るべき重要なポイントを認識できる 企業における情報保護や情報活用の基本的な考え方を理解し、ITサービスに対してそれを利用する側と、企画・開発・運用する側両方の視点で価値や課題を考察できる。			
授業方法	講義＋演習	実施形態	対面＋遠隔同期	
評価方法	ポートフォリオの内容により理解度などを総合的に判断し成績評価を行う。		実施形態	同期日
授業項目 1	情報セキュリティとリーガルマインド１〔吉井〕		対面+遠隔同期	11/8
2	情報セキュリティとリーガルマインド２（吉井）			
3	広告サービスと情報セキュリティ１（原）		対面+遠隔同期	11/22
4	広告サービスと情報セキュリティ２（原）			
5	個人情報保護法とプライバシーの実務１（中井）		対面+遠隔同期	12/27
6	個人情報保護法とプライバシーの実務２〔中井〕			
7	法制度調査手法１（西尾）		対面+遠隔同期	2/21
8	法制度調査手法２（西尾）			
9				
10				
11				
12				
13				
14				
15				
16				
使用教材	[授業項目3,4]では、演習においては受講者をチーム分けして、オンライン会議のグループチャット機能を使用予定。 [授業項目5,6]では、講師が用意するスライドのみを用いる。 [授業項目7,8]では、配付されるテキスト（pdf）を用いる。			
特記事項	講義を録画するため、同期日以降も講義動画視聴による受講が可能である。 [授業項目7,8]では、他の科目であるサイバーセキュリティ訴訟実務において導入する。その上で、こちらの講義では上記テキストに特化した内容とする。			

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＋遠隔非同期		
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		対面 +遠隔同期 +遠隔非同期	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		対面 +遠隔同期 +遠隔非同期	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		対面 +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 +遠隔同期	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 +遠隔同期	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	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			
必修・選択	―	単位	―	
概要・目的	情報セキュリティマネジメントシステム（ISMS：Information Security Management System（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について学び、情報セキュリティでも、マネジメントサイクル（ＰＤＣＡ）を構築する方法を身に付ける。 ISO/IECで対応するISMS認証があり、ISO/IECにて対応しているが、ISO/IEC設定の背景を考え、制度を正しく理解し、セキュリティマネジメントとしての考察を行い、特に、ISMSの構築、運用、審査（英語では、監査：Audit）を概観する。 情報セキュリティマネジメントの中心となるリスクマネジメントの観点から、情報システムにおける脅威や脆弱性への対応として、リスクマネジメントの考え方について総合的な観点から学ぶ。			
到達目標	ISO/IEC認証の知識に加え、背景を正しく理解し、セキュリティマネジメントとしての考察ができる。情報システムにおける脅威や脆弱性を理解し、リスクマネジメントに対応できる。			
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、受講態度、レポート、小テス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	オリエンテーション（情報セキュリティマネジメントシステム）			
2	企業・組織と情報セキュリティ		対面+遠隔同期	調整中
3	情報セキュリティマネジメントシステムの歴史、背景			
4	情報セキュリティ実施基準			
5	監査		遠隔同期	
6	マネジメントレビュー			
7	PDCAサイクル			
8	情報セキュリティマネジメントシステム認証制度		遠隔同期	
9	オリエンテーション（リスクマネージメント）			
10	リスクとは？　リスクマネジメントとは？			
11	リスクを考える。　安全と安心、脅威と脆弱性		遠隔同期	
12	リスク分析。　リスク判断、管理策			
13	リスクの軽減。　受容、回避、制限			
14	効果測定		対面+遠隔同期	
15	おわりに			
使用教材				
特記事項	講義回数：1日程あたり3コマ×5回 10/5および11/9の対面講義会場は福岡市内を予定 講義は11:20開始、17:00終了予定(途中休憩あり) 開講後の申し込み受付不可			

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	セキュリティ心理学			
必修・選択	―	単位	―	
概要・目的	【人のセキュリティ】、即ち、人間の心理や行動等を考えたセキュリティについて学ぶ。具体的には、国内では、『サイバーセキュリティ』とか『セキュリティ』というと【ネットワークセキュリティ／コンピュータセキュリティ／暗号等】を想像する方が多いが、最近は、ネットワーク化されたコンピュータ業務を企業関係者だけでなく、外部の一般の人たちも利用することも多くなってきた。また、数年で人事異動があり、セキュリティの知識・経験が継続しない企業・組織では、知識・経験等の継続を考える必要がある。システム設計者の想定外の操作を端末利用者が行う場合があることを学ぶ。 　また、セキュリティでは、事件・事故発生後に対応するのではなく、事前に問題点を把握し、その対応が必要になる。多くの端末利用者の特性を考え、システム対応だけでなく、関係する人達への教育・訓練の必要性、業務処理のセキュリティなどに対して、有用な事柄を例にして学ぶ。			
到達目標	最近のシステムやセキュリティでは、技術的セキュリティ分野だけを見据えるのではなく、心理学や行動科学等を考えた幅広い知識・経験を持つことが大切になる。また、学んだ知識・スキル・姿勢を活用して、セキュリティに関わる様々な状況において対応できる。			
授業方法	講義＋演習	実施形態	対面＋遠隔同期	
評価方法	本講義に関連レポート等（50%）及びプレゼンテーション評価／出席率等（50%）により評価する。		実施形態	同期日
授業項目 1	はじめに		対面+遠隔同期	調整中
2	情報／セキュリティの特徴			
3	セキュリティ心理学の必要性			
4	事件・事故からセキュリティ心理学を学ぶ		遠隔同期	
5	ソーシャルエンジニアリング			
6	ヒューマンエラー（組織エラー）			
7	環境犯罪学		遠隔同期	
8	人間の6つの脆弱性			
9	インテリジェンス（OSINT【オシント】Open Source Intelligence			
10	物理的セキュリティ		遠隔同期	
11	だまし：欺術			
12	行動経済学とセキュリティ心理学			
13	セキュリティ教育・訓練		対面+遠隔同期	
14	セキュリティ文化の確立			
15	おわりに			
使用教材				
特記事項	講義回数：1日程あたり3コマ×5回 9/6および10/4の対面講義会場は福岡市内を予定 講義は11:20開始、17:00終了予定(途中休憩あり) 開講後の申し込み受付不可			

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）		日程調整中
	2	有本弁護士講義「国際法制等」１		
	3	アクションチャート作成講義		日程調整中
	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）		日程調整中
	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		日程調整中
	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		日程調整中
	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）		日程調整中
	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）		日程調整中
	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		対面講義の会場は福岡市内を予定しています。 開講日が決定次第、掲載します。 開講後も受講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 ※　（授業項目10.11）の対面講義は、東京、大阪、広島等何れかで実施予定です。		

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	セキュリティとコンプライアンス経営				
必修・選択	―	単位	ー		
概要・目的	企業におけるマネジメントとは、内外のステークホルダー･関係者に経営課題の重要性を認識してもらい、行動変容を促すことです。その課題の重要性は問題発生時の企業の法的責任を直視することで浮かび上がってくるのであり、「セキュリティー」もそのような経営課題の一つとして捉えることができます。この課題に対し､「経営学」「法学」の両面からアプローチをすることで、セキュリティーに携わる管理職をはじめとする受講生の方々に、経営者視点を得てもらいます。分析モデルとしてLSMAP（Legal Stakeholders MAP）を用い、講義・演習を分りやすく進めます。				
到達目標	LSMAPモデルで、受講生が現在の業務において抱えているセキュリティー諸課題を漏れなくダブりなく客観的に分析し、その重要性とコンプライアンス視点をはじめとする改善策･改革案を役員･決定権者に説明し理解を得ていく力を獲得する。役員レベルの受講生には、セキュリティー課題を洗い出してプライオリティーづけし、その解決を中長期的にマネジメントに組み込んでいく力を得ていただく。				
授業方法	講義＋演習	実施形態	対面＋遠隔同期＋遠隔非同期		
評価方法	毎回の講義への貢献度及び提出課題(50%)＋最終発表（50%）			実施形態	同期日
授業項目 1	LSMAP１（取引関係）クライアントとサプライヤー			非同期	
2	提出課題へのコメント　LSMAP２（内部関係）従業員、役員			非同期	
3	提出課題へのコメント　LSMAP２（内部関係）株主			非同期	
4	提出課題へのコメント　LSMAP３（外部関係）加害者、被害者、同業他社			非同期	
5	提出課題へのコメント　LSMAP Plus1（公的関係）行政、司法			非同期	
6	受講生が抱えている課題（演習）受講生相互の議論　講師からのコメント			遠隔同期	
7	受講生からの中間報告１（演習）　〃			遠隔同期	
8	受講生からの中間報告２（演習）　〃			遠隔同期	
9	受講生からの発表１（演習）各自のアクションプラン　業界を超えた理解・共感			対面+遠隔同期	
10	受講生からの発表２（演習）　〃			対面+遠隔同期	
11					
12					
13					
14					
15					
使用教材					
特記事項	2025年度非開講				

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	ビジネスイノベーションと安全保障			
必修・選択	―	単位	―	
概要・目的	本講義では「ビジネス・イノベーションと安全保障」を対象とし、複数人の講師によるオムニバス形式で実施する。「ビジネス・イノベーションと安全保障」に関する報道・レコメンド等が、保有端末・SNS等を伝播しない日は無い。最近では、そうした情報流通は、半導体規制などの経済安全保障という国家レベルは勿論であるが、反転してミクロに分散し、端末保有者一人一人の問題関心に寄り添いそれを好餌（稀少財）として消費し、その解析結果をGAFAMなどのプラットフォーマーにフィードバックし、消費者の関心という情報資源の配分をグローバルに効率化している。 まず、われわれの日常がプラットフォーマーのグローバル・イノベーションの波に絡め取られていく動向が決定的となった2019年に、講師（白川）が、EUの競争政策当局と公取委との共催シンポジウムに登壇し、パネルディスカッション（https://www.jftc.go.jp/kokusai/EUJapanCompetitionWeek.html）をおこなった際の発表・講義内容をベースとしてオリジナル教材を用いて行われる。 次に、デジタル社会の発展とともにセキュリティリスクは深刻化を増していることから、ビジネスプラットフォームを保護する発見的手法の1つとしてセキュリティ監視と運用の目的を理解し、セキュリティリスクが顕在化する惧れがある事態（セキュリティインシデント）に備える対応態勢を学ぶ。特にSOC（Security Operation Center）とCSIRT（Computer Security Incident Response Team）の役割を詳しく学習する。 第三に、現在のテクノロジー変革期におけるサイバーセキュリティの脅威と対策を学ぶ。AIの進化がサイバー攻撃に与える影響や、証券口座乗っ取り、能動的サイバー防御といった最新事例を通して、社会変化とセキュリティの関連性について理解を深める。 また、実際に講師が遭遇した過去の重大インシデント事例から実践的な対応策を学び、情報社会の安全な発展に貢献できる人材となることを目指す。 第四に、日本における経済安全保障の議論は、どこから始まり、その背景には何があったのかを学ぶと共に、米国は国家戦略としての経済安全保障を世界戦略にいかに活用しているのかを学ぶ。 第五に経済安全保障の前提になっているルール形成がどのような概念によって構成されているのか、その原理を理解すると共に経済活動における活用事例を学ぶ。サイバーセキュリティ基本法策定プロセスの中でどのようなビジネスを想定し、振興しようとしていたのか、国内外の事例を学びながら、その本質を探る。 最後に、サイバーセキュリティ業界の構成を理解する。セキュリティ対策に投資をするユーザー企業と、サービスやセキュリティ製品の販売をなどを行うプレーヤー企業の現状や動向についての理解を深め、自身のミッション達成の基礎知識として活用できることを目指す。 また、新規ビジネスを立ち上げ、持続的に成長させていくための戦略的思考を学ぶ。その際、実際の事例を用いながら、フレームワークを活用し、外部環境と内部資源の両面から新規事業を成功に導くための視点を養う。			
到達目標	（１）イノベーションに関する経済学・ＡＩ・セキュリティに関して、分野を横断する問題関心の視座を形成できる。 （２）自社のルール形成戦略およびセキュリティレベルの向上のための原理的な思考枠組みをイメージできる。 （３）セキュリティ監視・運用の目的と必要性、セキュリティインシデントに備えた対応態勢を理解し、ビジネスを推進する際にセキュリティ監視運用も含めた提案ができる。加えて、システム構築の際にセキュリティ運用を意識して何を作成する必要があるのか（攻撃シナリオの作成、保護資産一覧の作成等）の一覧を作成できる。 （４）AIの急速な進化がサイバーセキュリティに与える影響と、それに伴う新たな脅威について説明できる。加えて、サイバーセキュリティの時事的なテーマについて（証券口座乗っ取りや能動的サイバー防御等）対策や論点を理解し説明できる。 （５）過去に発生した重大なインシデント事例から得られる教訓を学び、インシデント対応の重要なポイントを説明できる。 （６）日本における経済安全保障の本質及び歴史を理解することにより、経済安全保障をビジネスの中に落とし込むことができる （７）ルール形成戦略を理解し、サイバーセキュリティ関連ビジネスを構築し、経済的価値を存続するビジネスだけでなく、新たな価値を見出すビジネスを実行できる （８）ユーザ企業のセキュリティ部門（もしくはセキュリティ担当）が抱えやすい問題は何かを理解して、問題解決に向けて自社組織にて改善提案ができるレベルになること （９）新規ビジネスを外部環境・競争構造から分析できる （１０）自社の強みや機会をSWOTなどを通じて可視化し、戦略の方向性を検討できる （１１）ポジショニングマップを活用し、差別化の切り口を構築できる			
授業方法	講義	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 理解度等を判断し、総合的に評価を行う。	実施形態	開講日
授業項目	1	セキュリティと経済安全保障１（福田）	対面+遠隔同期	11/14
	2	セキュリティと経済安全保障２（福田）		
	3	サイバーセキュリティとイノベーション１（福田）		
	4	サイバーセキュリティとイノベーション２（福田）		
	5	デジタル・プラットフォーマーの競争戦略とルール形成戦略１（白川）	対面+遠隔同期	11/15
	6	デジタル・プラットフォーマーの競争戦略とルール形成戦略２（白川）		
	7	デジタル・プラットフォーマーの競争戦略とルール形成戦略３（白川）		
	8	デジタル・プラットフォーマーの競争戦略とルール形成戦略４（白川）		
	9	デジタル・プラットフォーマーの競争戦略とルール形成戦略５（白川）		
	10	セキュリティ監視・運用概論（東海林）	遠隔同期	11/21
	11	社会環境とセキュリティ１（日野）	対面+遠隔同期	11/29
	12	社会環境とセキュリティ２（日野）		
	13	サイバーセキュリティ業界とユーザー企業のミッションの現状と動向（原田）	遠隔同期	
	14	新規ビジネスの成長戦略とルール形成戦略（大木）	対面+遠隔同期	
	15			

使用教材	[授業項目5～9] 以下の２つの教材（いずれも講師の発表論文等）は事前に配布し、受講前に一読されることを希望するが、内容は講義で解説するので、不明点があっても全く問題ない。本講義の中心となる内容は、講義時にプレゼン資料にて提供する。 ・「デジタル・プラットフォーマー規制について～プラットフォーマー（実務家）の観点から」（『公正取引』 2019年6月号） ・「デジタル・プラットフォーマーを理解するための１０冊」（BUSINESS LAW JOURNAL　2020年2月号） [授業項目11,12] 講師からの配布資料のみ [授業項目13] PCのみ（PPTでの講義）
特記事項	開講日に受講不可の場合、録画した講義動画視聴による後日の受講可能。

<table>
<tr><td>コース名</td><td colspan="3">専門人材特化型コース</td></tr>
<tr><td>講座名</td><td colspan="3">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）</td></tr>
<tr><td>科目名</td><td colspan="3">セキュリティ関連法と実務</td></tr>
<tr><td>必修・選択</td><td>―</td><td>単位</td><td>―</td></tr>
<tr><td>概要・目的</td><td colspan="3">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。</td></tr>
<tr><td>到達目標</td><td colspan="3">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。</td></tr>
<tr><td>授業方法</td><td>講義</td><td>実施形態</td><td>対面＋遠隔同期</td></tr>
<tr><td colspan="2">評価方法</td><td colspan="2">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。</td></tr>
<tr><td rowspan="16">授業項目</td><td>1</td><td>デジタル新法1（湯浅）</td><td rowspan="3">遠隔同期</td><td rowspan="3">11/22</td></tr>
<tr><td>2</td><td>デジタル新法2（湯浅）</td></tr>
<tr><td>3</td><td>デジタル新法3（湯浅）</td></tr>
<tr><td>4</td><td>改正電気通信事業法（中井）</td><td>対面+遠隔同期</td><td>12/27</td></tr>
<tr><td>5</td><td>サイバーセキュリティ訴訟実務1（西尾）</td><td rowspan="2">対面+遠隔同期</td><td rowspan="2">2/21</td></tr>
<tr><td>6</td><td>サイバーセキュリティ訴訟実務2（西尾）</td></tr>
<tr><td>7</td><td>サイバーセキュリティ訴訟実務3（西尾）</td><td rowspan="4">対面+遠隔同期</td><td rowspan="4">2/22</td></tr>
<tr><td>8</td><td>サイバーセキュリティ訴訟実務4（西尾）</td></tr>
<tr><td>9</td><td>サイバーセキュリティ訴訟実務5（西尾）</td></tr>
<tr><td>10</td><td>サイバーセキュリティ訴訟実務6（西尾）</td></tr>
<tr><td>11</td><td></td><td></td><td></td></tr>
<tr><td>12</td><td></td><td></td><td></td></tr>
<tr><td>13</td><td></td><td></td><td></td></tr>
<tr><td>14</td><td></td><td></td><td></td></tr>
<tr><td>15</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">使用教材</td><td colspan="3">[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。</td></tr>
<tr><td colspan="2">特記事項</td><td colspan="3">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</td></tr>
</table>