	開講拠点大学	科目名	担当(予定)教員(と必要があれば所	授業概要（目的、テーマ、内容、学習目標等）
専門科目	東北大学	セキュリティ総論A（特別講義「セキュリティ総論A」）	曽根・菅沼・水木・和泉	情報セキュリティについて、その基礎となる知識を広く論じる。具体的には、一般的なユーザの視点から、情報セキュリティに関する基本的なリテラシー、攻撃・防御の事例を紹介し、開発・運用者の視点からプログラムやネットワークにおけるセキュリティリスクを説明する。さらに暗号技術がどのように世の中で利用されているかについてサーバ証明書等を例に取り述べ、大学などの組織における情報セキュリティ対策のためのポリシーなどの制度及び組織体制と利用者における情報倫理について述べる。
	大阪大学	セキュリティ総論B（セキュリティ基礎論）	宮地・河内・松井・新井・竹森	セキュリティ分野を垂直な2軸で網羅的にカバーすることを目的とします。 具体的には、"共通鍵暗号解析"から"マルウェア解析"及び"基盤理論"から"実用技術・標準化"という2軸により、セキュリティの基盤理論、暗号理論、実用化から標準化技術など最先端のセキュリティ技術までを守備した講義内容となります。
	東京電機大学	セキュリティ総論C（情報セキュリティの基礎と暗号技術（セキュリティ総論））	猪俣・広瀬	ネットワークを利用するに当たり、セキュリティに関する脅威と対策を理解させ、被害者にならないようにするとともに対策を一部実行できるようにする。
	慶應義塾大学	セキュリティ総論D	武田・手塚・猪俣・砂原	セキュリティについて学ぶためには、インターネットとそれに関連するシステムの基礎、暗号等を理解するための数学の基礎、インターネットに関わる法制度/社会制度について学ばなければならない。本講義では、セキュリティの基礎を学ぶとともに、これらシステム、数学、制度の基礎を学び、セキュリティの全体像について理解する。
	岡山大学	セキュリティ総論E	野上・福島・山内・五百旗頭・石原 他	現代情報化社会において情報を他人に盗み見られることなく安全に送受信するため、情報セキュリティ技術は重要な役割を果たす。中でも、データの秘匿化やユーザや機器の電子的な認証のための暗号技術、インターネット上で安全に情報通信を実現するためのネットワークセキュリティ技術、そしてWEBブラウザなどを通じてユーザが安心してサービスを利用できるようにするためのマルウェア検知・解析技術は必須のものである。本講義では、これら情報セキュリティ技術について網羅的に講義する。

演習科目	北海道大学	PBL演習-A（サイバーセキュリティ基礎演習）	飯田・南	本演習は、文部科学省「成長分野を支える情報技術人材の育成拠点の形成」（enPiT2）のPBL基礎科目の1つとして、セキュリティに関する基礎的な情報と利活用に関する実践的な内容を学ぶ。具体的には、グループ学習の形態をとり、ネットワークに接続された危機に記録される履歴（ログ）の発生環境や処理法に関し、小課題への取り組みを通じて学んだのち、履歴データの解析作業を実際に行い、解釈に至るまでのプレゼンテーションをグループで行うことを通じ、技術的知識の会得と、課題解決に対する共同作業の過程を学ぶ。
	東北大学	PBL演習-B（特別講義「クラウド・セキュリティ演習」）	菅沼・和泉他	クラウドサービスの開発から提供までの工程と実装時のセキュリティマネジメントを学び、IDC（インターネット・データセンター）上への模擬システムの展開をテーマとしたクラウドサービスのセキュリティ要件と運用要件の抽出を行い、クラウドサービス提供に係る実践的なセキュリティの考え方を身につけることを目標とする。
		PBL演習-Q（特別講義「ネットワークセキュリティ基礎演習」）	菅沼・和泉	TCP/IPネットワークおよびそのセキュリティ対策の基礎について学ぶ。具体的には実際にネットワーク機器を設定してネットワーク環境を構築し、そのネットワークを用いて攻撃の実例を体験することで、その脅威や対策について理解を深める。
	大阪大学	PBL演習-C（ビッグデータのプライバシー保護プロトコル演習）	河内・宮地	例えば多数の患者から集められた医療情報を解析した結果を医療診断に応用する等のビッグデータの解析において重要なのは提供された個人の情報のプライバシーを保護することである。本科目では講義を通じてその基盤暗号技術となる秘匿計算とその構成要素であるGarbled回路、紛失通信、共通鍵暗号方式、公開鍵暗号方式の原理を理解し、また演習を通じてそれらの技術の実装方法について理解を深める。
	和歌山大学	PBL演習-E（インシデントレスポンス演習）	川橋・藤本	本科目は,ネットワークおよびサーバで発生するトラブルの事例 と環境を基に,なぜトラブルが発生するのか,その発生要因は何 か,併せてその仕組みを理解する. セキュリティ事案はその延長にあり,発生原因の切り分けと封じ 込め,および解析方法について学ぶ.
	岡山大学	PBL演習-F（暗号ハードウェアセキュリティ演習）	野上・五百旗頭・石原	IoT時代において情報を他人に盗み見られることなく安全に交換するために暗号技術は重要な役割を果たす。その一方で暗号計算のハードウェア実装の仕方によっては、その理論的な解読困難さにも関わらず物理的な手段によって短時間で解読できる攻撃（サイドチャネル攻撃）が知られている。本講義では、暗号技術の歴史と原理、用途について学ぶとともに、ハードウェア実装を体験し、その基礎を学ぶ。さらに、ハードウェア実装された暗号計算に対するサイドチャネル攻撃による解読を体験し、攻撃原理とその防御のための基礎知識を学ぶ。
		PBL演習-G（クロスサイトスクリプティング対策演習）	横平・福島・山内・佐藤・石原 他	多くのWebサービスが提供されている現代において，Webサービスを介して多くの重要な情報がやりとりされており，これに伴い，Webサービスを標的とした攻撃が多く確認されている．Webサービスを標的とした攻撃の代表的な例として，クロスサイトスクリプティングがある．クロスサイトスクリプティングでは，Webアプリケーションの脆弱性を利用して，攻撃者に任意のコードを実行される可能性がある．そこで，クロスサイトスクリプティングの原理を学び，攻撃の流れと対策方法を実験を通して学習する．また，効果的なセキュリティ対策を講じられるように，攻撃者がもつ技術や視点を，ゲーム形式（CTF: Capture The Flag）で学習する．
	九州大学	PBL演習-H（セキュリティエンジニアリング演習）	金子	本講義では，センサーデバイスなどのハードウェアを利用したIoT機器のエンジニアリングを行うにあたって必要なセキュリティ対策について学習していきます． 本講義では，サイバーアタックの方法とサイバーディフェンスの方法を演習を通じて体験的に学ぶことで，より深くサイバーセキュリティに関する知識と技術を修得することを目的としています．本講義では，グループを作って，サイバーアッタクとサイバーディフェンスの演習を行います．
		PBL演習-L（サイバーセキュリティ演習）	岡村	演習装置を用いた、ハンズオン形式のサイバー演習を行ないます。演習では、サイバーセキュリティに関する２種類の攻撃を扱います。具体的な内容は講義の時に説明しますが、サーバへの攻撃体験、脆弱性のあるサーバ検索、暗号プログラミングなどの演習を行います。
		PBL演習-P（サイバーセキュリティハンズオン演習）	小出	演習装置を用いた、ハンズオン形式のサイバー演習を行ないます。演習では、サイバーセキュリティに関する２種類の攻撃を扱います。具体的な内容は講義の時に説明しますが、データベースへの攻撃、サーバへの攻撃などの演習を行います。
	東京電機大学	PBL演習-I（情報ネットワーク演習（セキュリティPBL））	猪俣・広瀬	インターネット(IPネットワーク網)を構築するには、パソコン、スイッチ、ルータなどのネットワーク機器を接続し、ネットワークとして動作させるための適切な情報を設定しなければならない。本授業では、ルータ設定をおこない、インターネットがどのように構築されているのかをイメージする。さらに構築したネットワーク上にセキュアなWebサーバを立て、サーバへのトラヒック監視を行うことにより、ネットワークセキュリティの重要性について基本から学ぶ。なお、授業形式は、全体として「反転授業」として実施する。
		PBL演習-J（CSIRTとリスクマネジメント演習（セキュリティ先進PBL））	猪俣・広瀬 他	本講義では、情報セキュリティにおけるマネジメントとして、リスク分析、デジタルフォレンジックなどの運営方式について学ぶことを目的とする。何かしらのサイバー攻撃が発生した場合、その状況を的確に把握することが重要である。そこで、CSIRT(Computer Security Incident Response Team)と呼ばれる組織では、的確に情報共有を行い、迅速な対応を行うが、そのために幅広い知識が必要となる。本演習では、企業の専門家と一緒になって問題解決に取り組むこととする。実際には、いくつかの課題に対して、議論形式で状況を認識し、問題を整理するトレーニングを行う。最終的には、その総括としてグループで発表を行うこととする。
	慶應義塾大学	PBL演習-K	砂原・山内	本科目は、Basic SecCapコースに関連する講義等で得られた基礎知識の実践力を養うために、実際の環境に展開し、グループ内で問題意識の共有を目指すものである。受講者は、個別に専門的な知識を習得するだけでなく、グループ（集団）活動として、役割分担、責任範囲を明確にした上でセキュリティ問題に取り組むことが要求される。また応用、適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバで構成されたグループ内で議論を展開させ、最適解を得ることが目的である。
	京都大学	PBL演習-M（情報セキュリティ演習）	岡部・宮崎・小谷	外部からの不正アクセスの試みを検知する侵入検知システム(IDS)では、膨大な数の警報が発せられ、その解析は人手では困難である。ここでは、IDSの仕組みと役割を学んだ上で、機械学習によりIDSの警報ログから正常通信と攻撃を分類する演習を実施する。
	長崎県立大学	PBL演習-N（Webアプリケーションファイアウォールによる攻撃検知演習）	松田	本講座は，Webアプリケーションの仕組みを理解し，外部からの攻撃を防御するWebアプリケーションファイアウォール(WAF)の設定をすることで攻撃を検知する方法を学習する。
	静岡大学	PBL演習-O（サイバー攻防演習）	西垣・大木・峰野・野口・長谷川・原子	多岐にわたるWebシステムへのサイバー攻撃の原因を理解し、インシデントに対する初動対応から再発防止策まで技術面だけでなく情報連絡系統についてもケーススタディを通して体感し，実践で役立たせるための基礎能力を養うことを目標とする。

先進演習科目（先進PBL）	東北大学	先進PBL-A（特別講義「制御システムセキュリティ演習」）	曽根・和泉	電力、ガス、ビル、化学の分野の制御システムのサイバーセキュリティの基礎と対策を学び、実際に模擬システムを用いて、サイバー攻撃が発生した場合の各分野における影響と対応策への理解を深めて、制御システムセキュリティの基本的な考え方を身につけることを目標とする。
	大阪大学	先進PBL-C（システム構築におけるセキュリティ機能実装とセキュリティ監視・運用演習）	野川	企業で行われる実践的なセキュリティ対策を学ぶ。 またログ解析・分析によるセキュリティ監視・運用方法を理解する。
		先進PBL-D（実践安全な公開鍵暗号の設計と解読演習）	宮地・鄭	本科目では公開鍵暗号を用いてモノのインターネット(IoT)のデータを保護する方法を学び，実際に実装する方法について習得する。 サイバーセキュリティの基礎である暗号には共通鍵暗号および公開鍵暗号の二種類がある。前者では各参加者は一つ以上の秘密鍵を事前に共有していることが仮定するので，n端末のネットワークではn^2個の鍵を管理する必要があり、IoTへの応用では現実的でない．一方，公開鍵暗号は，n端末のセキュアネットワークを1個の鍵で実現し，理論的に魅力的な解決方法を提供する．しかし，多くのIoT機器は計算・メモリ・通信能力が非常に限られおり，公開鍵暗号を利用することが容易ではない．さらに，多数のIoT機器を用いた攻撃も考えられる． 本PBL演習ではIoTのデータを保護する公開鍵暗号の実現方法さらには暗号解読手法まで理論的にアルゴリズムを習得することを目的とする．また公開鍵暗号及び解読の実装アルゴリズムの考え方を習得する．
		先進PBL-J		
	東京電機大学	先進PBL-E（物理セキュリティ攻撃と対策（先端セキュリティ））	猪俣・広瀬 他	情報セキュリティにおいては技術的な知識のみならず、情報共有を行うといった人間同士の活動が重要となる。本演習ではPBL(Project Based Learning)形式で実施し、グループ内で問題意識の共有、役割、ディスカッションをベースとする。具体的には、セキュリティインシデントが発生した際の初動対応を学ぶとともに、CSIRT(Computer Security Incident Response Team)を運用する上でのマネジメント手法についても学ぶ。最後には、成果報告会として発表会を実施し、評価を行うこととする。なお、本演習はPBL演習形式であるため、講義全体が「反転授業」での実施となる。
	慶應義塾大学	先進PBL-F（インシデントハンドリング演習）	砂原・山内	本科目は、Basic SecCapコースに関連する講義等で得られた基礎知識を活用し、PBL演習で得られた実践力をより深めるために、より具体的な環境に展開し、グループ内で問題意識の共有を目指すものである。受講者は、個別により実践的な知識を習得するだけでなく、グループ（集団）活動として、役割分担、責任範囲を明確にした上でセキュリティ問題に取り組むことが要求される。また応用、適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバで構成されたグループ内で議論を展開させ、最適解を得ることが目的である。今年度においては、以下の演習プログラムを提供する予定である。なお、セキュリティPBL演習を履修する際には、それぞれ履修要件があるため注意すること。
	岡山大学	先進PBL-G（安全性評価のための衝突型暗号攻撃演習）	野上・石原	IoT時代において情報を他人に盗み見られることなく安全に交換するために暗号技術は重要な役割を果たす。その中で、楕円曲線暗号やRSA暗号など公開鍵暗号は、ユーザや機器を電子的に認証するために用いられており、その鍵長などセキュリティパラメータは、計算量的な安全性評価に基づいて適切に設定されなければならない。本演習では、楕円曲線暗号を具体的なターゲットとして、衝突型の暗号解読攻撃プログラムを実装し、その計算量的な安全性の評価方法について学ぶ。
	東北大学	先進PBL-H（特別講義「Cyber OPS演習」）	曽根・菅沼・和泉	本コースではアソシエイトレベルのSOC (Security Operations Center) アナリストに必要な知識・スキルを学習します。一般的なセキュリティの概念について学習すると当時に、基本的な脅威分析、イベントの関連性分析、悪意のあるアクティビティの識別、インシデント対応を講義及び演習を通して学びます。本コースはシスコ技術者認定CCNA Cyber OPSの取得を目的として設計されたコースです。
		先進PBL-Ｉ（特別講義「サイバー攻撃演習」）	曽根・和泉 他	サイバーセキュリティ人材不足が叫ばれる中、サイバーセキュリティの動向を理解し、攻撃に対応するために必要となる基礎知識を習得することを目標とする。具体的にはバッファオーバーフローやクロスサイトスクリプティングなど脆弱性に関する説明を行った上で、演習環境にて実際に攻撃を行い理解を深める。また、演習では攻撃者の視点で考察を行い、防御するために必要な観点を身に着ける。
	慶應義塾大学	Cyber OPS演習		

先進演習科目（大学院インターンシップ）	北陸先端科学技術大学院大学	大学院インターンシップA（セキュアクラウド理論演習）	面・奥村・宮地	本科目は，セキュアクラウドシステムで使われる最新のセキュリティ理論を実装を通して学ぶだけでなく，解読実験等のグループ演習も行い，数学のセキュリティ技術への応用手法を深く理解することを目的とする．
		大学院インターンシップF（認証技術によるWebシステムのセキュリティ対策実践）	滝口・宮地	不正アクセス等の様々な脅威から守り、安心して利用できるICTシステムを実現しなければいけない。セキュリティ対策の中で重要な対策の一つである"ユーザ認証"について実践を通して深く理解することを目的とする。
	奈良先端科学技術大学院大学	大学院インターンシップB（ハードウェアセキュリティ基礎演習）	藤本・林・藤川	情報通信機器から情報漏えいが生じるメカニズムを習得し、HWセキュリティの重要性を学ぶ。
		大学院インターンシップH（電磁波セキュリティ基礎演習）		
	慶應義塾大学	大学院インターンシップC(モバイルアプリの脆弱性検出とその対策)	砂原・山内	スマートフォン向けアプリ開発において混入しやすい脆弱性について理解するとともにセキュアな設計・コーディング方法について体得するまた演習を踏まえスマートフォン向けアプリ開発において脆弱性が混入しにくくするための仕組みや対策方法についてグループで考察し発表する。
	情報セキュリティ大学院大学	大学院インターンシップD（脅威分析演習）	大久保 他	ソフトウェア開発を対象とした脅威分析の知識・技術を体験的に習得する。
		大学院インターンシップE（ハードニング基礎演習）	小村 他	Webシステムの構築・管理に必要となる、基本的かつ総合的なセキュリティ知識・技術を体験的に習得する。
	東北大学	大学院インターンシップG（特別講義「ネットワークセキュリティ実践」）	グレン・角田・和泉	情報セキュリティとネットワークセキュリティは、現在の情報化社会における多面的かつ最重要な課題である。本授業では実践的なハンズオンを通して、情報セキュリティとネットワークセキュリティに関する基本的な課題と性質を理解することを目的とする。 具体的には、様々なプロトコルやアプリケーションが有する脆弱性について確認し，それらの脆弱性が攻撃者による偵察行為や攻撃にどのように利用されるのかを見ていく。また、いくつかの一般的な攻撃に関する手口やそれに対する対策について考える。 受講者は実践的なハンズオンを通じて上記の各項目に関する理解を深めるとともに、その過程でセキュリティに関する問題発見から解決までを主導できるリーダーの役割を担うための力を養う。