抜粋版

INSTITUTE of INFORMATION SECURITY

C'est parti !

明日の信頼を創ろう。

情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

2016-2017

不確かな未来を照らし
より安全で確実な航路へと
情報セキュリティが導いてくれる

さらに便利に、より効率的に、もっと楽しく……。社会の隅々に各種の情報デバイスが行き渡り、それらをネットワークで結ぶことで多様なサービスが次々に生まれ、高度情報化という進化の道を歩み続ける社会。それは誰も見たことのない新大陸へと向かう巨大な船のようです。

これから私たちが上陸する新大陸は、例えばIoTで得られた膨大なデータをAIが解析し、人々の暮らしをサポートするといった安心で豊かで心躍る世界でしょう。しかし上陸地に至る航路はまだ定まらず、未知の脅威が行く手を阻み、大海原で行き先を見失うかも知れません。

そのような不確かな未来を前にしたとき、より安全で信頼のおける航路へと導くのが情報セキュリティの役割です。何をどうすれば安全なのか、という根本を数理科学の視点から読み解く技術力。リスクを〝見える化〟して検証し、人や組織がリスクを避けるよう促すマネジメント力。セキュアな考えで設計・製造を行い、安全性の高い物づくりを行うデザイン力。さらに外部からの攻撃に適切に対処し、組織を守る強固な防御力。それぞれの専門性を磨き、あるいは文理を超えてそれらを融合し、安全で信頼できる社会を創り、支える人がさらに求められていくでしょう。

こうした情報セキュリティ分野に特化した人材育成と高度な研究のため、2004年に開学したIISEC(情報セキュリティ大学院大学)では、10数年かけて日本の情報セキュリティ教育のスタンダードといえるプログラムを作り上げました。その中でも実社会で活躍した教員を中心とする教育・研究指導、講義と演習・実習による体験的教育、産学官連携の人材育成等は先進的な大学院教育の核となっています。今後は情報セキュリティ分野の多様な人材ニーズに応える教育機会の拡大も視野に、新大陸への水先案内人となる人材を一人でも多く育てたいと考えています。

博士前期課程
（修士課程）

育成する人材像
モデル履修プラン

■ 育成する人材像

○エンジニア、システムコンサルタント［技術系］

情報セキュリティに関する確かな専門知識と広い視野を備え、
セキュアなシステム・プロダクトの設計、開発、構築ができる技術者や、
技術面のコンサルティングを担う専門家

○セキュリティマネージャー、ビジネスコンサルタント［マネジメント系］

情報セキュリティに関する総合的な知識を持ち、社会の変動要因や
制約条件を踏まえて適正なリスク分析・評価を行い、企業・組織における
実効性のある政策提言や人間系セキュリティ対策を担うリーダー

■ 履修モデル［博士前期課程2年制プログラム］

［数理科学コース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
暗号・認証と社会制度（2単位）／暗号プロトコル（2単位）／アルゴリズム基礎（2単位）
数論基礎（2単位）／暗号理論（2単位）／計算代数（2単位）
個人識別とプライバシー保護（2単位）／統計的方法論（2単位）／統計的リスク管理（2単位）
セキュアシステム実習（2単位）
研究指導（6単位）

合　計　30単位

［サイバーセキュリティとガバナンスコース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
暗号・認証と社会制度（2単位）／個人識別とプライバシー保護（2単位）
インターネットテクノロジ（2単位）／不正アクセス技法（2単位）／情報システム構成論（2単位）
セキュアシステム実習（2単位）／情報セキュリティマネジメントシステム（2単位）
セキュア法制と情報倫理（2単位）／法学基礎（2単位）/セキュリティの法律実務（2単位）
研究指導（6単位）

合　計　30単位

［システムデザインコース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
ネットワークシステム設計・運用管理（2単位）／セキュアシステム構成論（2単位）
情報デバイス技術（2単位）／情報システム構成論（2単位）／オペレーティングシステム（2単位）
セキュアプログラミングとセキュアOS（2単位）／プログラミング（2単位）
ソフトウェア構成論（2単位）／セキュアシステム実習（2単位）／アルゴリズム基礎（2単位）
研究指導（6単位）

合　計　30単位

［セキュリティ／リスクマネジメントコース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
情報セキュリティマネジメントシステム（2単位）／セキュリティシステム監査（2単位）
セキュリティ管理と経営（2単位）／リスクマネジメント（2単位）／組織行動と情報セキュリティ（2単位）
統計的方法論（2単位）／Presentations for Professionals（2単位）
セキュア法制と情報倫理（2単位）／セキュアシステム実習（2単位）／不正アクセス技法（2単位）
研究指導（6単位）

合　計　30単位

◎必須科目　○履修標準科目

科目区分	授業科目名	履修区分	単位数	数理科学コース	サイバーセキュリティとガバナンスコース	システムデザインコース	セキュリティ／リスクマネジメントコース
専攻	情報セキュリティ輪講Ⅰ	必修	2	◎	◎	◎	◎
	情報セキュリティ特別講義	必修	2	◎	◎	◎	◎
	暗号・認証と社会制度	選択	2	○	○	○	○
	暗号プロトコル	選択	2	○		○	
	アルゴリズム基礎	選択	2	○		○	
	数論基礎	選択	2	○			
	暗号理論	選択	2	○			
	計算代数	選択	2	○			
	個人識別とプライバシー保護	選択	2	○	○	○	
	インターネットテクノロジ	選択	2	○	○	○	
	不正アクセス技法	選択	2		○	○	○
	ネットワークシステム設計・運用管理	選択	2		○	○	
	セキュアシステム構成論	選択	2	○		○	
	情報デバイス技術	選択	2	○		○	
	情報システム構成論	選択	2	○	○	○	
	オペレーティングシステム	選択	2	○	○	○	
	セキュアプログラミングとセキュアOS	選択	2	○	○	○	
	プログラミング	選択	2	○		○	○
	ソフトウェア構成論	選択	2	○		○	
	セキュアシステム実習	選択	2	○	○	○	○
	情報セキュリティマネジメントシステム	選択	2		○		○
	セキュリティシステム監査	選択	2				○
	セキュリティ管理と経営	選択	2		○		○
	リスクマネジメント	選択	2		○		○
	組織行動と情報セキュリティ	選択	2		○		○
	統計的方法論	選択	2	○	○	○	○
	統計的リスク管理	選択	2	○			○
	リスクの経済学	選択	2				○
	Presentations for Professionals	選択	2		○		○
	マスメディアとリスク管理	選択	2		○		
	セキュア法制と情報倫理	選択	2		○		○
	法学基礎	選択	2		○		○
	知的財産制度	選択	2			○	○
	国際標準とガイドライン	選択	2			○	○
	セキュリティの法律実務	選択	2		○		○
	情報セキュリティ輪講Ⅱ	選択	2	○	○	○	○
	特設講義	選択	2				
	特設実習	選択	2				
研究指導	研究指導	必修	6	◎	◎	◎	◎

［留意事項］・各コースの履修標準科目は、研究をスムーズに進めるために適切な科目選択ができるよう設定されているものです。各人の興味・関心領域、研究テーマに応じて4つのコースからひとつを選択し、科目選択の目安としてください。また、研究テーマが複数コースにまたがる学生や幅広い知識の獲得を目指す学生は、指導教員の履修指導のもと、他コースの標準科目も自由に履修することができます。・選択科目は20単位以上（10科目以上）修得してください。

■ 修了要件および学位

課程	標準修業年限	所要単位数	審査・試験等	学位
博士前期（修士）課程（2年制プログラム）	2年 ※1	30単位以上	修士論文審査および最終試験	修士（情報学）
博士前期（修士）課程（1年制プログラム）	1年	46単位以上	リサーチペーパー※2審査および最終試験	修士（情報学）

※1:教授会が優れた研究業績を上げたと認めた者については1年以上在学すれば足りるものとする。　※2:プロジェクト研究指導の成果物。

■ 取得可能資格

高等学校教諭専修免許状（情報）　※基礎資格を有した上で関連法規の定める所要の単位を取得し、博士前期課程を修了することが取得の条件になります。

■ 他大学院等との交流協定

2016年5月現在、以下の大学院・研究機関等と協定を締結しています。こうした大学間ネットワークを活用したさまざまな学習・研究機会等を利用することが可能です。

・神奈川県内の大学院間における大学院学術交流協定
・中央大学大学院理工学研究科
・国立情報学研究所
・東京大学大学院情報理工学系研究科
・The Information Security Group, Royal Holloway, University of London
・大連大学　　他

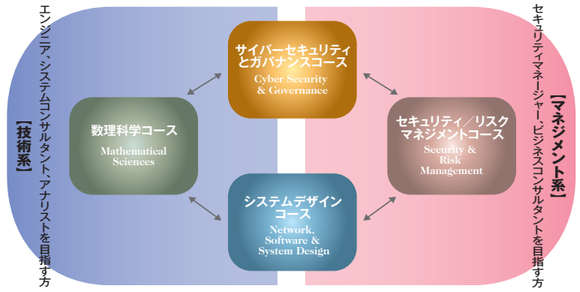
情報セキュリティ研究科
博士前期・博士後期

教育課程編成の考え方
カリキュラムの特色

広い視野に立って現実の情報セキュリティの問題解決を担う高度な専門技術者、実務家と、将来方向をリードする創造性豊かな研究者を育成。2016年10月より4つのコースをリニューアル。

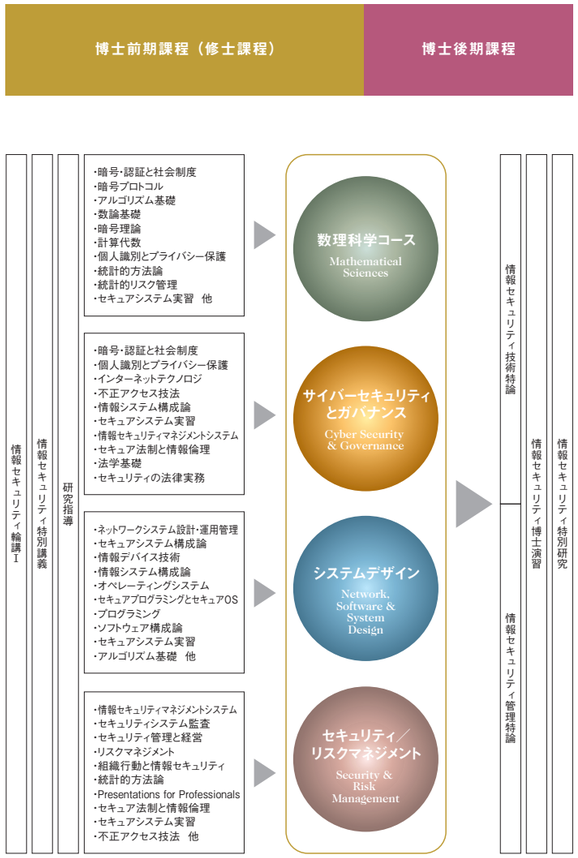
実社会における適正な情報セキュリティの実現には、暗号技術、ネットワーク技術、情報システム、管理運営、法制度、心理、情報倫理を融合させた総合的な対応が必要であり、それぞれの専門家が幅広い視野と見識をもって協力しあうことが不可欠です。情報セキュリティ研究科博士前期課程では、高度化・複雑化する企業・官公庁等の現場ニーズを踏まえ、4つのコースフレームを2016年10月よりリニューアルし、技術系・マネジメント系とも幅広い人材育成需要、教育需要に応えます。なお、指導教員の履修指導のもと、他のコースが推奨する科目も自由に履修することができます。博士後期課程では、博士前期課程修了の知識をベースに、情報セキュリティの構成要素に関わるそれぞれの専門分野における先端的な研究を行います。前期課程からの一貫教育を活かした情報セキュリティに関するより深化した教育研究によって、社会の多様な領域でそれぞれの中核的人材として活躍する研究者、研究指導者の育成を目指します。また、内部進学者のみならず、情報セキュリティ分野の研究経験をもった学外からの入学者にも後期課程の門戸を開くことによって、全体として多角的な視点から総合科学としての情報セキュリティの体系化に努めていきます。

■ 博士前期課程新4コース（2016.10～）



＜修了後の進路＞　情報通信／情報サービス／SIer／メーカー／セキュリティベンダー／シンクタンク／コンサルティングファーム／金融／流通／新聞・出版・印刷／教育・研究機関／調査機関／官公庁／博士後期課程進学　など

■ カリキュラムフレーム



■ 開設科目一覧

本学ウェブサイトからシラバスをご覧いただけます（一部科目を除く）

科目区分	授業科目名	履修区分	単位数	修了に必要な単位数 博士前期（2年制）	博士前期（1年制）	博士後期
専攻	情報セキュリティ輪講Ⅰ	必修	2	24	42	—
	情報セキュリティ特別講義	必修	2			
	暗号・認証と社会制度	選択	2			
	暗号プロトコル	選択	2			
	アルゴリズム基礎	選択	2			
	数論基礎	選択	2			
	暗号理論	選択	2			
	計算代数	選択	2			
	個人識別とプライバシー保護	選択	2			
	インターネットテクノロジ	選択	2			
	不正アクセス技法	選択	2			
	ネットワークシステム設計・運用管理	選択	2			
	セキュアシステム構成論	選択	2			
	情報デバイス技術	選択	2			
	情報システム構成論	選択	2			
	オペレーティングシステム	選択	2			
	セキュアプログラミングとセキュアOS	選択	2			
	プログラミング	選択	2			
	ソフトウェア構成論	選択	2			
	セキュアシステム実習	選択	2			
	情報セキュリティマネジメントシステム	選択	2			
	セキュリティシステム監査	選択	2			
	セキュリティ管理と経営	選択	2			
	リスクマネジメント	選択	2			
	組織行動と情報セキュリティ	選択	2			
	統計的方法論	選択	2			
	統計的リスク管理	選択	2			
	リスクの経済学	選択	2			
	Presentations for Professionals	選択	2			
	マスメディアとリスク管理	選択	2			
	セキュア法制と情報倫理	選択	2			
	法学基礎	選択	2			
	知的財産制度	選択	2			
	国際標準とガイドライン	選択	2			
	セキュリティの法律実務	選択	2			
	情報セキュリティ輪講Ⅱ	選択	2			
	特設講義	選択	2			
	特設実習	選択	2			
研究指導	研究指導	必修	6	6	—	—
	プロジェクト研究指導	必修	4	—	4	—
博士専門	情報セキュリティ特別研究	必修	6	—	—	8
	情報セキュリティ博士演習	必修	2			
	情報セキュリティ技術特論	選択	2			
	情報セキュリティ管理特論	選択	2			
計				30	46	8

博士前期課程
（修士課程）
授業科目概要
2016

専門的研究のための基礎固めからセキュリティ技術やマネジメントの最新動向まで情報セキュリティの新たな側面に気づく科目がきっと見つかります

ここでは博士前期課程の授業科目の一部についてご紹介しています。詳細は本学ウェブサイトでご確認いただけます。

TOPICS

JASA公認セキュリティ監査人（補）受験資格

選択科目「特設講義（セキュリティ監査）」
（後期2単位 担当：原田要之助 教授）を履修し、定められた講義・演習を受講することにより、NPO日本セキュリティ監査協会（JASA）が認定する公認情報セキュリティ監査人（補）の受験資格が得られます。また、履修終了後、JASAによる修了試験を受験して合格することで監査人補の資格が取得できます。平日日中の時間帯に開講している科目ですが、過去6年間で社会人学生を含む多数の方が本選択科目の履修とその後の受験を経て監査人補の資格を取得されました。

博士前期課程専攻科目（例）

■情報セキュリティ輪講Ⅰ（必修）
各自、発表テーマを選択し、そのテーマに基づいた調査を行い、その調査結果を口頭で発表して、参加者からの質疑を受け討論をおこなう。これにより、発表者・参加者は、新しい技術動向・マネジメント方法・社会動向・法制、などの知識を取得するとともに、考え方やノウハウなどを学ぶが、発表者にとっては修士論文作成の前段階作業でもある。

■情報セキュリティ特別講義（必修）
本科目は、広く情報セキュリティに関する各界からの専門家の講師をお招きし、セキュリティに関する講話をしていただき、情報セキュリティに関する最新の情報を習得すると共に受講者の知見を深めることを目的とする。講義は毎回、専門家の講師によるリレー方式により実施する。講師は、情報セキュリティ大学院大学連携教授のほか、官公庁、民間企業、研究機関等から広くお招きする予定である。

■暗号・認証と社会制度
情報社会の基盤技術である現代暗号の原理と機能について学ぶ。 暗号化・署名・鍵共有といった、主要な基本機能を正しく理解するとともに、それらの具体的な構成例についても学ぶ。さらに、これら基本機能が組み合わされて、より高次な機能が安全に実現される様子をS/MIMEやSSLを通じて観察する。また、属性ベース暗号など、より高機能な暗号技術についても紹介する。個々の技術の理解よりも、暗号技術の全体像を把握することを優先する。

■暗号プロトコル
近年、プライバシーに係る情報を秘匿しつつ、統計量のような有益な情報を得ることができるシステムの必要性が高まっている。このような一見実現困難と思えるシステムも、暗号プロトコルを利用すれば達成できる場合がある。
本講義では、暗号、認証、署名等について概説し、暗号プロトコル（秘密分散共有法、ゼロ知識証明など）の実現方法とその安全性について解説する。さらに、プライバシーの保護とセキュリティの両立を実現するプロトコル、双線形写像を用いた応用などについても解説する。

■個人識別とプライバシー保護
本講義では、最初に個人識別と本人認証の原理を技術の面から解説し、それをベースにインターネット社会における本人認証の仕組みと利用における技術的・法的課題について、具体的事例を通して学ぶ。次に、個人識別や本人認証技術と深い関係を持つプライバシー保護の問題について、法律的な視点と技術的な観点から問題点を理解する。最後に、講義の内容を基礎として演習を行い、受講者の理解を深めると同時に具体的事案に対する対応力を養うこととする。

■インターネットテクノロジ
インターネットは高度情報化社会の基盤となっており社会生活の利便性向上に大きく寄与している。他方、インターネットはサイバー犯罪やサイバー攻撃の手段としても利用され、個人ユーザや企業が情報セキュリティインシデントに巻き込まれるケースが増えている。このような状況から、インターネットと情報セキュリティ両分野の調和のとれた進歩が急務となっており、情報セキュリティ分野の研究開発に従事する者は勿論のこと、情報セキュリティを管理する立場の者であっても、インターネットの仕組みや最新技術および関連する情報サービスの動向をおさえておくことが肝要である。本講では、以上の視点から、インターネットテクノロジの基礎から応用まで幅広く考えていくこととしたい。

■不正アクセス技法
OSおよび各種アプリケーションソフトウェアおよびネットワークにおけるセキュリティを確保するだけでなく、暗号や認証プロトコルのセキュアな運用方法、および技術を習得することを目的として、対象となる攻撃方法、およびマルウェアの構成、検出方法について講義を行う。具体的には、サービス妨害（DoS攻撃）、脆弱性検査（ポートスキャン等）、侵入行為、ルート権限奪取、不正プログラム設置および実行（トロイの木馬等）等の不正アクセス方法、さらにコンピュータウイルス、ボット、およびそれらの対策手法としてのファイアーウォール、IDS、IPS、脆弱性検査システムの技術、運用等の技術的要因だけでなく、ソーシャルエンジニアリング等の社会的、人的要因についても議論する。

■セキュアシステム構成論
情報通信技術（ICT）の普及により、さまざまな場所において情報システムが構築され利用されている。ネットワークを介した情報システムの利用、情報システム間の連携は、より高機能かつ効率的なシステムの構築を可能とするだけでなく、利用者の利便性を飛躍的に向上させてきた。一方で、インターネットを通じて不特定多数のユーザが情報システム群にアクセスできる環境においては、無防備なシステムが当然のように攻撃の対象となりうる。そこで、本講義では「セキュアな情報システムとは何か」という観点で、情報システムにおけるセキュリティの考え方について学ぶ。

■情報システム構成論
情報システムは、コンピュータシステム、ネットワークシステム、端末などのハードウエアを組み合わせ、オペレーティングシステム、ミドルウエア、応用プログラムなどのソフトウエアを載せ、その応用目的に合わせて構成される。そのためには、プロセス間通信機構、OSインタフェース、インターネットインタフェース、仮想マシンなどの基本機構の理解と、クラウド、Web、GRIDなどのシステム及びXML言語、様々な応用システムとその開発技術、システム評価手法などの知識が基本である。更にAI技術は今後のシステムに必須の要素になるであろう。また、システムの要求性能を満たすための設計、信頼性・保守性・安全性などを考慮した作り、更には経営戦略やビジネス継続性などへの対応が必要である。本講義は、これらの基礎について学ぶとともに、最近のシステム技術の動向について考察する。

■セキュアプログラミングとセキュアOS
脆弱なソフトウェアシステムに対する攻撃が多発しており、社会全体に対して大きな影響を与えている。そこで、本授業では、攻撃に強くセキュアなソフトウェアを構築するときに有用となる原則、概念、技法、ガイドライン、ツールなどについて紹介および解説を行う。

■ソフトウェア構成論
システムをサイバー攻撃から守るため、脆弱性のない安全なシステム構築が求められる。そのための知識はユーザ側、開発側双方に必要となる。本授業では、セキュアなソフトウェアを構築するために前提となる、ソフトウェア開発手法を学ぶ。本授業では、主に、オブジェクト指向モデルに基づいた最新のソフトウェア開発手法を取り上げ、ユーザ側、開発側双方の観点でセキュリティ対策をソフトウェアの面から考えるための基礎について学ぶ。オブジェクト指向による開発の理解を深めるため、一部、UMLを用いた分析、設計手法やeclipseによるJava言語の実習を行う。

■セキュアシステム実習
本授業では「ネットワーク不正侵入とその防御および検知」をテーマとし、攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、実習を通して理解を深めるとともに、セキュアなシステム構築について考察する。使用するコンピュータのOSはWindowsとLinuxである。

■情報セキュリティマネジメントシステム
組織にとって、情報セキュリティの計画、設計・導入、運用・保守、見直し（PDCAサイクル）のマネジメントサイクルを構築することが重要となっている。この方法論として、情報セキュリティマネジメントシステム（ISMS）があり、ISO/IECの国際基準にもなっている。このISMSは、組織の意志決定に必要な管理体制（マネジメントの仕組み）が導入されいてること及び、情報セキュリティのリスクを低減するためのコントロール（管理策）が適切に維持・管理されていることを目的としている。
授業では、最初に、ISMSを整備・運用するために必要な考え方から始め、実際のコントロールについて講義形式で知識を習得させる。その後、演習形式でケーススタディに取り組み、理解を深める。
なお、授業では、2013年に大きく改定された新しい国際規格（ISO/IEC27001:2013、ISO/IEC27002:2013、ISO/IEC27000:2014）の改訂内容を授業に取り入れて構成する。

■セキュリティシステム監査
今日では、ITシステムが経営活動や業務活動に必須のものとなり、ITシステムの戦略的活用こそ組織価値を高める鍵をにぎっているといっても過言ではない。その一方で、ITシステムを巡る事件・事故は後を絶たず、セキュリティ管理の失敗が組織価値を大きく損なう結果をもたらすことも広く知られるようになってきた。この授業は、「セキュリティシステム監査」という名称が付されているが、「監査」では、上記の二面性を認識した上でセキュリティ管理状況の監査の問題を考えることも重要となる。もちろん、必要に応じて、国家試験なども意識してシステム監査人となるのに必要な知識や技能も伝授するが、ケーススタディやディスカッションも織り交ぜながら、理論と実務という観点から「監査」という行為、あるいは「監査人」の目線から、組織のセキュリティ管理をどう見るかという「センス」と、「問題解決能力」を養うことを主たる目的とする。

■リスクマネジメント
情報通信技術の利用と多様性が増し、企業経営に大きな影響をもたらすようになった。適切な情報セキュリティのあり方を考え、効果的に実践できるようにすることは、重要な経営課題のひとつとなったと言えよう。本講義では、経営における情報セキュリティ実践に必要な知識として、リスクマネジメントの基本的な理解を促し、情報セキュリティに係わるマネジメントとの関連を自ら考え実践上の取組みへと展開する能力を身につけることをねらいとする。

■統計的方法論
社会調査データは、その調査対象となっている社会のすがたを描き出すことのできる非常に貴重なものである。しかしながら、収集されたデータをただ眺めているだけでは社会のすがたは見えてこない。本授業では、社会調査に関する基礎的な知識をおさえたうえで、量的な社会調査データを適切に処理・分析する方法を学んでいく。それをとおして、データを分析することはもちろん、分析の結果を正しく読み取り、解釈することのできる能力の習得を目指す。

■セキュア法制と情報倫理
情報セキュリティを確保するためには各種の技術知識が不可欠であるが、同時にセキュリティを守るも破るも、人であることを忘れてはならない。人に関する研究は心理学・経営学・経済学・倫理学・法学など、様々な角度からアプローチが可能であるが、本講では最も実効性ある制度である「法」と、最も内面的な価値に近い「倫理」を組み合わせて、2名の担当者が相乗効果を出すよう協力して担当する。情報セキュリティの確保に当たって「人」の側面にどのような問題があるのかを理解し、さまざまな組織・場面における適切な対策について検討する上での基本的な知見を得ることを到達目標とする。

■Presentations for Professionals
The purpose of this course is to increase your ability to give simple and effective English language presentations about professional topics. The focus will be on gaining presentation and communication skills, not on pronunciation or grammar.This means that your English language speaking skills-for example pronunciation or grammar skills-do not matter very much for this course. If you have just basic English speaking ability and you want to learn or improve your presentation skills, you can take this course. You will find that designing and presenting your original ideas can be fun and challenging. There is nothing to fear!

博士前期課程
（修士課程）
授業科目履修例
2016年度

▼＜学部新卒学生Aさんの履修例＞ 数理科学コース

◆前期（4月6日～8月4日）　※■が履修科目

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						個人識別とプライバシー保護
2		プログラミング		リスクマネジメント		セキュリティシステム監査
3	数論基礎	オペレーティングシステム				セキュアシステム実習
4	アルゴリズム基礎	セキュアシステム構成論A		マスメディアとリスク管理	統計的方法論	
5	知的財産制度	（研究指導）	情報セキュリティ輪講Ⅰ	情報デバイス技術	法学基礎	
6	セキュリティの法律実務 or ソフトウェア構成論A	（研究指導）	インターネットテクノロジ	統計的リスク管理	暗号・認証と社会制度	

◆後期（10月1日～2月12日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル			ソフトウェア構成論B	
3	（研究指導）	リスクの経済学		特設講義（セキュリティ技術実践論）		
4		特設講義（セキュリティ監査）	（研究指導）	特設講義（ハッキングとマルウェア解析）	暗号理論	
5	情報システム構成論	（研究指導）	情報セキュリティ特別講義	国際標準とガイドライン or セキュア法制と情報倫理（隔週）	Presentations for Professionals	
6	計算代数	（研究指導）	情報セキュリティ輪講Ⅰ	特設講義（先進ネットワークセキュリティ技術） or 特設講義（セキュア社会基盤論）（隔週）	セキュアシステム構成論B	

▼＜社会人学生Bさんの履修例＞ セキュリティ／リスクマネジメントコース

◆前期（4月6日～8月4日）　※■が履修科目

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						個人識別とプライバシー保護
2		プログラミング		リスクマネジメント		セキュリティシステム監査
3	数論基礎	オペレーティングシステム				セキュアシステム実習
4	アルゴリズム基礎	セキュアシステム構成論A		マスメディアとリスク管理	統計的方法論	
5	知的財産制度	（研究指導）	情報セキュリティ輪講Ⅰ	情報デバイス技術 or セキュリティ管理と経営	法学基礎	
6	セキュリティの法律実務 or ソフトウェア構成論A	（研究指導）	インターネットテクノロジ	統計的リスク管理 or ネットワークシステム設計・運用管理	暗号・認証と社会制度	

◆後期（10月1日～2月12日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル			ソフトウェア構成論B	
3	（研究指導）	リスクの経済学		特設講義（セキュリティ技術実践論）		不正アクセス技法（隔週）
4		特設講義（セキュリティ監査）	（研究指導）	特設講義（ハッキングとマルウェア解析）	暗号理論	
5	組織行動と情報セキュリティ	（研究指導）	情報セキュリティ特別講義	国際標準とガイドライン or セキュア法制と情報倫理（隔週）	Presentations for Professionals	
6	情報セキュリティマネジメントシステム	（研究指導）	情報セキュリティ輪講Ⅰ	特設講義（先進ネットワークセキュリティ技術） or 特設講義（セキュア社会基盤論）（隔週）	セキュアシステム構成論B	

■ 授業時間帯

社会人の方が在職のまま就学できるよう、平日夜間や土曜日も授業を実施します。※

※博士前期課程の標準修業年限1年制プログラム（若干名）においては、平日昼間の通学も必要です。

時限	月曜日～金曜日	土曜日
1時限	9:00～10:30	9:00～10:30
2時限	10:40～12:10	10:40～12:10
3時限	13:00～14:30	13:00～14:30
4時限	14:40～16:10	14:40～16:10
5時限	18:20～19:50	16:20～17:50
6時限	20:00～21:30	

博士前期課程
（修士課程）

コース概要

コンサルティング能力を備えたエンジニア。技術やシステムに明るいマネージャー。
情報セキュリティ研究科博士前期課程では、情報セキュリティ全般にわたる広い視野と見識を備え、
リーダーとして現場における問題解決を担う高度な専門人材を育成します。

数理科学 コース
Mathematical Sciences

あなたの作ったアルゴリズムがセキュリティの新しいステージを拓く

◆コース概要と研究キーワード

情報セキュリティには、暗号、匿名化、形式検証、学習、クラスタリング、マイニングなど、数多くの数理的な問題が存在しています。数理科学コースでは、これら、情報セキュリティに関わる、数理的な諸問題を深く理解し、よりよい解決を見出すことで、より効率的でより強力な情報セキュリティを実現するための基盤構築を目指します。講義による知識習得にとどまらず、少人数のセミナーや個別指導を通じて学習・研究を進めます。修了後は、企業・研究機関・行政機関等において、専門技術職・研究職を始めとするテクニカルスタッフとしての活躍が期待されます。

研究キーワード：数論アルゴリズム、公開鍵暗号、準同型暗号、デジタル署名、認証、ゼロ知識証明、暗号プロトコル、秘密分散、形式検証、匿名化、差分プライバシ、学習、人工知能基礎、ビックデータセキュリティ基礎、クラスタリング、マイニング 他

◆修士論文イメージ

情報セキュリティに関わる、数理的な問題について、オリジナルな手法の提案や既存手法の改良あるいは実装評価を行い、論文にまとめます。実装評価については、ソフトウェア/ハードウェアとそれに付随する技術文書（開発物の理解と使用に必要十分なもの）を修士論文として提出することも可能です。適切な課題設定、論理的で説得力ある論旨の展開、客観的で検証可能な成果記述が重視されます。

コースリーダーからのメッセージ

有田 正剛 教授
Seiko ARITA

チューリングが暗号解読のためにチューリングマシンを発明したように、情報セキュリティには、暗号を始めとして、匿名化、形式検証、統計処理など数理的な課題がたくさんあります。数理的な学問に関心のあるみなさん、ぜひ、情報セキュリティを数理科学の観点から研究してみませんか? あなたの作ったアルゴリズムやマシンが情報セキュリティの一翼を担うことも夢ではありません。

システムデザイン コース
Network, Software & System Design

“セキュリティ・バイ・デザイン”でネットワーク社会の安全を守る

◆コース概要と研究キーワード

企業・研究機関等で研究開発、ソフトウェア・システム・製品の開発、システムコンサルティング、新事業の立案・企画業務などに従事されている方、あるいは従事することを目指している方を対象とし、OS、ソフトウェア、ネットワーク、システム設計・運用管理などのITシステム技術、およびそれらの安全でセキュアな構成法に関する広範な知識・技術を習得します。さらに、セミナーや個別指導を通じて得られた知識と技術を統合する実践能力を身につけます。また、経営管理や法制度等の周辺領域の知識を身につけることで、セーフティ&セキュリティビジネスの推進に必要な幅広い視野を養います。

研究キーワード：セキュリティ・バイ・デザイン、脅威分析、ビッグデータ分析、脆弱性評価、セキュリティテスト、フォレンジック、プライバシー保護、知的財産権管理、セキュアシステム、セキュアOS、マルウェア対策、センサーネットワーク、ディペンダブルシステム、ソフトウェア工学、人工知能、仮想化環境、組み込みソフト、制御システム、セイフティ設計 他

◆修士論文イメージ

学問的課題や実世界で起きている問題を取り上げ調査・分析をし、その解決策を提案、実装評価／紙上評価して、学術論文スタイルにまとめます。 また、セーフティとセキュリティに関連するソフトウェアを開発し、設計仕様、ソースコード等とともに修士論文として提出することも可能です。

コースリーダーからのメッセージ

大久保 隆夫 教授
Takao OKUBO

安全でセキュアなITシステムは、現在のそして将来の私達の生活に必須のものです。画期的なITシステムに挑戦したい方、新しいシステムを提案したい方、また現在のシステムをより良くしたいと思っている方、一緒に研究をしましょう。

サイバーセキュリティとガバナンス コース
Cyber Security & Governance

先端技術とサイバー規範を併せ持つサイバーレスキュー隊のリーダーへ

◆コース概要と研究キーワード

本コースでは、日々増加するサイバー攻撃の検知・分析・防御技術と、それを支える脅威情報の収集分析能力を有する専門人材、および、企業や政府・自治体においてサイバー攻撃対処を担うSOC/CSIRT組織を構築・運用するマネージャ人材を育成します。そのために、本コースではデジタル・フォレンジックやネットワーク等、サイバーセキュリティの先端技術とともに、実社会におけるサイバー攻撃対処で必要となるセキュリティ関連法制や国際動向等の知識を習得することにより、総合的な対処能力を身につけます。

研究キーワード：インシデント対応、SOC/CSIRT運用、フォレンジックとマルウェア分析、攻撃検知と防御、サイバースレットインテリジェンス（CTI）、サイバーセキュリティ基本法、不正アクセスと営業秘密、脆弱性情報・脅威情報の共有技術とフレームワーク（ISAC） 他

◆修士論文イメージ

実世界で起きている問題を調査・分析し、その解決策を提案、実装評価／紙上評価して、学術論文スタイルにまとめます。技術に重点を置く場合は、実験評価システムを使った脆弱性やマルウェアの実データの分析や、新たな解析ツールの開発評価の結果を論文にまとめます。法制度や社会フレームワークに重点を置く場合は、各自の関心に合わせてインシデント事例や判例などをリサーチし、課題を発見し、先行研究や問題点に対する考察を加えて具体的に課題を解決する提言を行います。

コースリーダーからのメッセージ

湯淺 墾道 教授
Harumichi YUASA

サイバー攻撃への対処は、個人の社会生活、産業や行政機関にとって必須です。攻撃の検知・分析・対処技術やデジタル・フォレンジックなどの先端技術とともに、攻撃対処を支える法制度の理解、サイバーセキュリティを取り巻く国際的な状況など、幅広い知識が求められています。本コースでは、CSIRTなどのアナリストを目指したい方、今後、経営企画や法務部門でセキュリティ経営を担う方や危機管理を担当する方をお待ちしています。

セキュリティ／リスクマネジメント コース
Security & Risk Management

適切なセキュリティ投資・対策・監査で、ITリスクの脅威から組織を守る

◆コース概要と研究キーワード

組織は、外部からのサイバー攻撃、委託先や従業員による重要情報の持ち出しなどITのリスクが重要になってきています。そのためにはリスクを特定して、適切な対応が必要です。本コースでは、組織のリスクから情報を適切に保護・管理し、組織の機会につなげるリスクマネジメントを実践します。また、経営者の観点からセキュリティ戦略策定、セキュリティ対策の投資、効果測定、監査などのリスクガバナンスを実践します。すなわち、リスク分析や対策のマネジメントのみならず、ガバナンスを構築し実践できる人材を育成します。企業・組織等でリスクマネジメント、IT戦略、マーケティング、人材育成、教育研修、監査、コンサルティング等の業務に従事されている方、あるいは従事することを目指している方に、事例研究、調査分析を通じて、実践的知識の習得と応用力を養います。

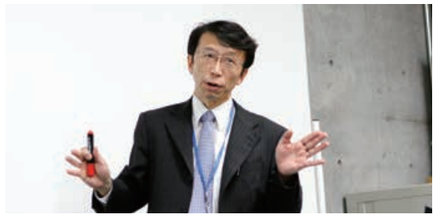
研究キーワード：リスクマネジメント、リスク分析、リスク戦略、セキュリティ投資、セキュリティ監査、リスク評価、ISMSとPマーク、BCP/BCM、セキュリティ教育、インシデント分析、セキュリティアンケート調査、クラウドのセキュリティ 他

◆修士論文イメージ

組織（企業）活動における事件・事象あるいは現象面からリスクをマネジメントおよびガバナンスする課題について、実証分析（アンケート調査など）をベースに分析、提言などを論文スタイルにまとめて提出します。論文は、アカデミックな観点も重要ですが、社会における実証的な分析、組織（企業）への実践的な価値など多面的に評価されます。

コースリーダーからのメッセージ

原田 要之助 教授
Yonosuke HARADA



社会生活のあらゆる場面でITのリスクが顕在化しています。個人情報の漏えい事故は個人情報保護法が施行されて10年たっても増え続けています。本年からは、マイナンバーが利用されますが、漏えい事件が無くなるとは思えません。これは、組織や社会が、リスクについて十分に認知してリスク分析や対策を実施できていないからです。
本コースでは、リスクについての仕事で実践されておられる方、情報分野のリスクマネジメントを学習・実践されたい方、組織のCISOなどを目指しておられる方を歓迎します。人文・社会科学系か技術系か等は問いません。共に研究して、知識を深め実践していきたいと考えています。

博士前期課程
（修士課程）

目的別
カリキュラム
活用パターン

情報セキュリティ研究科博士前期（修士）課程は、本学が提供する正規の授業科目や研究指導はもちろん、大学間連携・産学連携によるオプションプログラム等も充実しており、興味・関心・目的に応じてさまざまなカリキュラムの活用が可能です。また、いずれの場合も、社会人学生を含む多くの方々が、在学期間中、学会・研究会での発表、セキュリティコンテストへの参加、懸賞論文への応募等に積極的にチャレンジしています。

パターン1 修士学位取得専念型

修士論文に向けての知識の獲得と研究に重点を置きたい

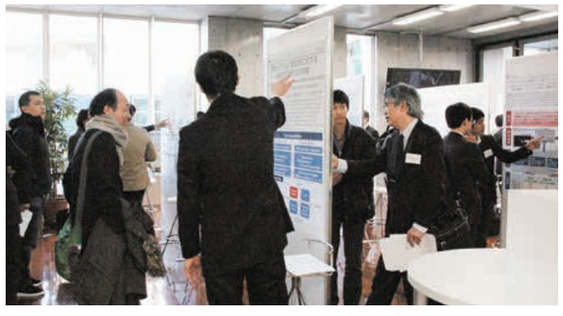
特にオプションプログラムは選択せず、各コースの履修標準科目を中心に履修して研究を進めるための知識の獲得や補強に努めるとともに、所属研究室での研究指導やディスカッションを通じて研究遂行能力を高め、在学中は修士論文作成に向けた研究に重点的に取り組みたい、という方を想定しています。神奈川県内の20以上の大学が加盟する大学院学術交流協定制度を利用して、研究テーマに関連する他大学院の開講科目を履修することも可能です。

▶これまで提出された修士論文題目は
情報セキュリティ研究科ウェブサイトでご覧いただけます。
http://lab.iisec.ac.jp/

パターン2 ISS square 併修型

研究室や大学を超えた活動を通じて幅広い視野を養い、研究を実務に生かしたい

ISSスクエア（研究と実務融合による高度情報セキュリティ人材育成プログラム）は、本学と中央大学、国立情報学研究所他、11の企業・研究機関の産業連携による博士前期（修士）課程生のためのオプションプログラムです。本学の充実した講義群に加え、サブゼミ的な位置づけの研究分科会や分野横断型のワークショップでの活動、セミクローズドなセキュリティ関連施設等の見学会、シンポジウムでの成果発表等を通じて高度な問題発見能力と解決能力を身につけます。現役学生の方はセキュリティ実務に関するインターンシップ実習のチャンスもあります。2年間の本プログラム修了時には、修士学位に加え、ISSサーティフィケートが授与されます。現職の社会人学生の方も数多く本プログラムに参加し修了されていますので、興味のある方はぜひチャレンジすることをおすすめします。



パターン3 ISS square & enPiT SecCap 併修型

ISSスクエアの活動に加えできるだけ実践的な演習や実習に取り組みたい

enPiT（分野・地域を越えた実践的情報教育協働ネットワーク）は、全国15大学院の教員や企業の技術者を結集したプログラムで、そのセキュリティ分野enPiT-Securityについて、本学を含む5つの連携大学が協力して実践セキュリティ人材育成コースSecCapを開講しています。実社会が取り組むインシデント分析やセキュリティ実装、脅威や攻撃への対処技術に関する演習を含む幅広い実践的な夏季（8-9月）演習プログラムを中心に、共通講義科目、まとめとしての先進講義科目群等が用意されています。本学では、このSecCapはISSスクエアのサブセットプログラムとして提供され、1年次終了時点で、プログラム修了者にはSecCap認定証が授与されます。ISSスクエア参加者の約9割が本プログラムも併修されていますので、興味のある方はぜひチャレンジすることをおすすめします。

実践演習をサポートしてくれるOBOGの声

若月 里香｜情報セキュリティ大学院大学 特任助手
（2013年3月情報セキュリティ研究科博士前期課程修了）

技術系演習のサポートをしています。技術系演習では、NW検査やログ分析、Webアプリケーション検査、フォレンジックを実際に自分でやっていただきます。講師を務めるのは、実務でそれらに携わっている方々です。昨年度は、情報系から文系の学生さんまで、苦しみつつ楽しみつつ腕を磨いていかれました。多くの方の挑戦をお待ちしています！

小杉 史郎｜情報セキュリティ大学院大学客員講師（株）横浜ITサポート代表取締役
（2006年3月情報セキュリティ研究科修士課程修了）

enPiT演習の「組織における情報セキュリティ管理」に関するテーマを担当しています。組織では、どうやって職員一人一人のセキュリティ意識を高め、セキュリティ上のきまりを守ってもらうかに苦労しています。いろいろアイデアを練りながら効果的な教育・啓発ツールを考える演習講座となっています。是非受講してみてください。

星 智恵｜情報セキュリティ大学院大学客員講師
ネットワンシステムズ（株）市場開発本部 ソリューション・サービス企画室
（2008年9月情報セキュリティ研究科博士前期課程修了）

誰でもが出来る仕事ではなく自分の軸となる能力を身につけようと大学院進学を選びました。大学院は単に「知る」のではなく実社会で使える力を身につけるための気づきの場です。enPiT『インシデント対応とCSIRT基礎演習』ではサイバー攻撃に備えたインシデント対応のフレームワークを演習を中心に学習します。

＊ISSスクエア、SecCapへの参加は、入学後に説明を聞いたうえで決めていただくことができます。いずれのプログラムも、参加登録にあたって追加学費は発生しません。ただし、見学会参加や他大学で開講される授業、セミナー出席等への交通費は自己負担となりますので、予めご了承ください。

研究と実務融合による高度情報セキュリティ人材育成プログラム ISS square

文部科学省の平成19年度「先導的ITスペシャリスト育成推進プログラム」に採択されたISSスクエアは、情報セキュリティ大学院大学、中央大学、国立情報学研究所他、企業・研究機関11社の産学連携による高度情報セキュリティ人材育成プログラムです。暗号・認証、ネットワーク、システム、ソフトウェア、マネジメント、法制・倫理までトータルにカバーされた講義群、インターンシップや見学会、企業現場の実務家によるオムニバス講義などにより、経営・研究開発現場における現状の理解と問題の把握が促進されるとともに、サブゼミ的な位置づけの研究分科会や分野横断型のワークショップでの活動を通して、高度な問題発見能力と解決能力を身につけます。ISSスクエア活動の集大成としての年度末のシンポジウムでは、連携企業の皆様による成果発表審査も行われ、ISSスクエアプログラム修了者には、情報セキュリティ・スペシャリスト・サーティフィケートが授与されます。2008年の開始以来、本学からは120名以上の方がサーティフィケートを取得され、毎年、社会人学生を含む多くの方が本プログラムに参加されています。

詳しくは http://iss.iisec.ac.jp/

分野・地域を越えた実践的情報教育協働ネットワーク enPiT SecCap

文部科学省の平成24年度「情報技術人材育成のための実践教育ネットワーク事業」に採択されたenPiTは、クラウドコンピューティング、セキュリティ、組み込みシステム、ビジネスアプリケーションの4分野を対象とし、それぞれの分野に専門領域を有する全国の15大学院の教員や企業の技術者を結集したプログラムで、2013年より本格スタートしました。セキュリティ分野（enPiT-Security）は、5つの連携大学（情報セキュリティ大学院大学、東北大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学）が協力して開講する実践セキュリティ人材の育成コース（SecCap）により、幅広い産業分野において求められている「セキュリティ実践力のあるIT人材」の育成を目指します。暗号、システム、ネットワーク、監査、マネジメントまでの幅広い演習プログラムと、最新の実習環境、そして実社会が取り組むインシデント分析やセキュリティ実装の演習も行い、情報セキュリティへの脅威や攻撃への対処技術を実践的に体験習得します。

詳しくは http://www.seccap.jp/

情報セキュリティ研究科
博士前期・博士後期

在学生プロフィール
2015-2016



OBOGの協力による就職セミナー

さまざまなバックグラウンドを持つ仲間たちとのコラボレーション
新しいパラダイムもかけがえのないネットワークもここから生まれる。

独立大学院である本学には、幅広い年齢、職種、立場の方々が在籍しています。
キャリアの充実やステップアップのため、業務上の要請、あるいは純粋にアカデミックな関心からと、進学の動機やきっかけもさまざまです。
多彩なバックグラウンドを持つ仲間たちとの異文化交流ともいえるような日々の議論や活動は、お互いに理解を深め、
情報セキュリティの新しい側面を見出すきっかけになるとともに、教室の内外での貴重なネットワークの形成にもつながっています。

博士前期課程

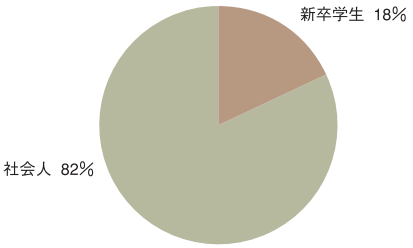
■ 社会人学生の所属組織

システムインテグレーター、通信キャリア、セキュリティベンダー、ソフトウェアハウスなどに勤務するSE、研究者、営業担当者をはじめ、ユーザー企業のセキュリティ担当者、システム担当者、人事・総務担当者、教育・研究機関や官公庁の職員など、在学生の所属業界・職種は多岐にわたっています。

【所属組織一覧】(2015-2016実績)
(一社)共同通信社／NHN Techorus (株)／NTTコミュニケーションズ(株)／NTTコムウェア(株)／NTTコムセキュリティ(株)／NTTデータ先端技術(株)／海上保安庁／(株)アーク情報システム／(株)アイネス／(株)エヌ・ケイコーポレイト／(株)JR東日本情報システム／(株)ジョイント・システムズ・サービス／(株)DNP情報システム／(株)日立システムズ／金融庁／警察庁／警視庁／(公財)湘南産業振興財団／埼玉県警察／ジェイアール東海情報システム(株)／ソニー(株)／ソフトバンク(株)／東芝ITサービス(株)／(独)国立印刷局／日本電気(株)／日本放送協会／東日本旅客鉄道(株)／フォレストソフト(株)／富士通セミコンダクターITシステムズ(株)／ベライゾンジャパン合同会社／防衛省／法務省／三菱重工業(株)／横浜銀行／横浜市役所　など

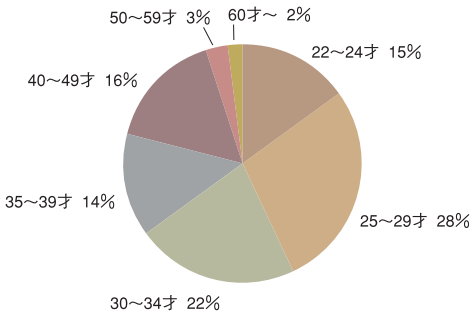
■ 現況

約8割の方が社会人学生です。時間をやり繰りし、仕事と学業を両立させています。また、いったんキャリアをリセットした後、次のステップに備えるべく一定期間学業に専念されているケースも見られます。就業経験のない新卒学生の方にとっては、こうした方々との交流も、近未来の自分像やキャリアプランを描くうえでの貴重な経験となるでしょう。



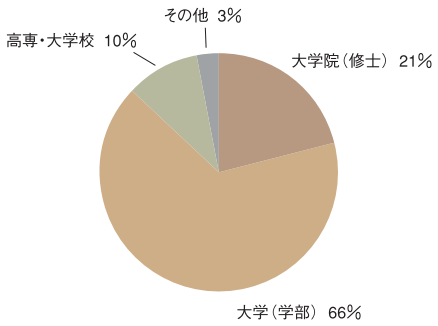
■ 年齢構成(入学時)

20代半ばから30代の中堅社会人をはじめ、幅広い年代の方々が学んでいます。ジェネレーションを超え、同じ学生という立場で活発な交流が図られています。



■ 最終学歴

4年制大学学部卒のほか、高専・専門学校等を卒業後、実務経験を積んで入学された方、すでに他大学院にて修士号を取得されている方など、最終学歴はさまざまです。また、出身学部についても、理工系のみならず、社会科学系や人文科学系、学際系など幅広く、本学にはアカデミックなバックグラウンドにおいても多様な方々が集っているといえます。



博士後期課程

博士後期課程には、既に相当の研究実績、業務実績を有する企業や行政機関の研究所に所属する研究者、技術者も在学中です。これは、情報セキュリティに関する新たな学問体系の構築をめざす本学にとって、後期課程学生同士や教員との切磋琢磨による優れた学際的研究成果の蓄積が期待できるばかりでなく、博士前期課程学生への教育効果の向上という観点からも非常に心強い存在となっています。

【所属組織一覧】(2015-2016実績)
NTTコミュニケーションズ(株)／NTTコムセキュリティ(株)／(株)アーク情報システム／(株)富士通ソーシアルサイエンスラボラトリ／警察庁／堤歯科医院／東日本電信電話(株)／三菱電機インフォメーションシステムズ(株)／ヤフー(株)　など

博士後期課程

育成する人材像
課程概要

情報セキュリティ研究科博士後期課程では、確かな専門知識とマルチメジャーの視点を備え、
先端的な研究経験を通じて情報セキュリティに関する問題解決を先導するための能力を養います。

■ 育成する人材像

情報セキュリティの将来方向をリードする研究者

情報セキュリティに関する
高度な研究・分析能力と専門的知見を生かし、
社会の多様な領域でそれぞれの
中核的人材として活躍する研究者、研究指導者等を育成。

本課程の学生は、学際的な総合科学としての情報セキュリティ全般にわたる広い視野と見識を深めながら、その中の特定領域における高度に専門的な研究を行い先鋭的な学問の構築を経験することになります。これを通じて、産学官のさまざまな教育・研究機関の中核を担う自立した研究者、研究指導者、企業や行政機関等で活躍する実務研究者、ならびに当該分野における確かな教育能力と研究能力とを兼ね備えた大学教員等を育成します。

■ 修了要件および学位

次の3つの条件を全て満たすことを博士後期課程の修了要件とします。
また、本学において授与する博士の学位に付記する専攻分野の名称は博士（情報学）［Doctor of Philosophy in Informatics］となります。

1. 標準修業年限:
3年（ただし、教授会が特に優れた業績を上げたと認める者については、当該課程に1年以上在学すれば足りるものとする）
※2007年度から2015年度までの間に本学博士後期課程を修了し、博士の学位を授与された方のおよそ3分の1は標準修業年限未満（1年から2年半）で博士学位を取得されています。

2. 所要単位数:
特別研究6単位以上＋博士演習2単位以上→合計8単位以上

3. 博士請求論文:
必要な研究指導を受けた上、研究テーマに関する論文を作成し、中間発表を実施後、学位論文審査と専門分野の口述試験を受け、合格すること。

■ 後期課程科目概要

学生は、自ら新規なテーマを案出し、その中身を充実させて学会等に報告して批判を受け、それらの批判に耐えられる論理を構築することによって、新たな研究領域を切り開き、独立した研究者としての基礎を身につけることを基本とします。これを実現するために、博士後期課程においては、次のような科目を用意しています。

情報セキュリティ特別研究（必修6単位）
研究室内での密で定常的な研究討論を通して、博士前期課程学生を指導する経験を積むことや、自己テーマの深掘りによる研究能力・研究指導力の醸成を行います。

情報セキュリティ博士演習（必修2単位）
複数教員とのセミナーを通じて、複数分野における研究ポイントと教え方を学び、専門領域の多視点化と自己研究の客観化の素養を身につけます。

情報セキュリティ技術特論・情報セキュリティ管理特論（選択各2単位）
各教員の専門分野に応じて、博士後期課程学生用に編成された講義で、これによって先端的な技術や考え方を身につけます。

■ 修了後の進路

明確な目的意識に裏打ちされた研究を推し進めることにより、社会的ニーズに即した先端技術、手法として理論を考究するとともに、セキュリティに関する知識・技術をベースに情報セキュリティ分野の新しい方向性、あり方、技術を研究し切り開いていく人材として、本課程修了後は、以下のようなフィールドを中心に活躍が期待されています。

- 行政機関が設置する情報セキュリティ関連の研究所にて研究に従事
- 大学等高等教育機関にて、研究者、研究指導者、大学教員として情報セキュリティ教育研究に従事
- 情報関連企業などにおける情報セキュリティに関する先端的なシステムプロダクトの研究開発
- 情報通信関連企業、シンクタンクで研究に従事
- 研究者の素養と経営観を兼ね備えた人材として組織をリードする情報セキュリティ管理責任者（CISO）、各種プロジェクト責任者

学長　教授 Hidehiko TANAKA

田中英彦

対談

情報セキュリティ研究科長　教授 Atsuhiro GOTO

後藤厚宏

情報セキュリティ分野をより深く、広く。多様な人材育成ニーズに応える教育で世界を変えたい。

IoT、BigData、AI進化する情報活用社会の中で情報セキュリティが重要に

田中　2004年に開学したIISEC（情報セキュリティ大学院大学）も13年目に入りました。その間、スマートフォンの普及をはじめ様々な情報サービスが進化し、人々の暮らしがより便利に、幸せになった一方で、悪意のある攻撃は対象が拡大し、その手法も巧妙になったと感じます。

後藤　確かにここ10数年で、人間の不得意な部分をコンピュータが代わりにやってくれることが一気に増え、生活や仕事の利便性も飛躍的に向上しました。豊かさ、便利さ、効率の良さを求めるのは人間の自然な欲求で、それは止められないでしょう。情報を様々な形で活用する中で、安全性や信頼性、安心感などを担保する情報セキュリティの役割はますます重要になりますね。

田中　IoT、BigData、AIといった技術用語もすっかり一般化しました。

後藤　IoTで無数の物がつながれば、やりとりされるデータ量も一気に膨れ上がります。その処理にBigDataの技術が使われ、効果的な活用にAIの助けを借りる……。すべては個別の事象でなく、情報活用社会という大きな動きをそれぞれ違う角度から見たものと言えます。ただ田中学長が数十年前からAIに取り組まれてきたように、物と物をつなぐ、膨大なデータを処理するといった情報化は昔から連綿と続いてきたことで、今に始まったことではありませんね。

デジタル化された情報をどのように守るかを考えるサイバーセキュリティ対策

田中　そうした情報化の恩恵を享受する場合、重要なのは信頼性です。情報を活用する様々なサービスが生活必需品になれば、安定的に継続して使えないと困る訳で、社会インフラとしての信頼性が求められるのです。さらにはそのサービス内容が確かなものでないと、安心して利用できないでしょう。また情報をどんどん活用しているうちに、本人が了承してない情報まで流出する可能性もあるなど、プライバシーの面でも問題は大きくなってきます。

後藤　より便利なサービスを提供するところに、多くの情報が集まるのは当然です。そして私たちの仕事や生活、政治や経済まで同じサービスに依存していけば、当然悪意のある攻撃もそこに集約された情報を狙うでしょうね。

田中　重要なサービスほど狙われやすい。そのような情報セキュリティの問題解決を手助けできるのが、私たちの大学院だという自負はあります。開学当初から情報セキュリティ専門の教育・研究を続けてきたのですから。中でも近年重視しているのは「サイバーセキュリティ」への対応で、もともと情報セキュリティのカバー範囲は非常に広く、紙に書かれた文章なども含む情報全般のセキュリティを指します。しかし現在の大きな問題は、コンピュータに取り込んだデジタル情報をどう守るかというサイバーセキュリティなのです。

文理融合の考えは変えず、時代のニーズにより即した形を目指し4つのコースをリニューアル

後藤　サイバーセキュリティ対策は個人にとどまらず、企業や国のガバナンスでも非常に重要です。ガバナンスは日本語で「統治」と訳され、何となく「治まる＝静的状態」と思われがちですが、本来は企業や国のリソースをどう活用して目的を遂げるかという意思決定のこと。ガバナンスとは日々変化する状況に対応するダイナミックなものです。

田中　当大学院でも博士前期課程の2年制プログラムで2016年10月生から適用される新4コースの中に「サイバーセキュリティとガバナンスコース」を用意しています。この名称で、サイバー攻撃の検知・分析・防御技術と攻撃に対処する組織のマネジメントの両面を学ぶ、という特色が分かりやすくなりましたね。

後藤　今回のコース変更は、そのように名称や概念などを時代に合わせて置き換えたもので、開学以来の「情報セキュリティは多様な分野にまたがり、その教育・研究には文理融合のコースがふさわしい」という考えに変わりありません。

田中　確かに暗号などは情報セキュリティの大切な基盤技術ですが、データを隠したり、秘密裏に通信したりと狭い見方をされがちでした。

後藤　ですから技術面の基盤になるという意味合いで「数理科学コース」と変更しています。これはBigDataやAIのベースにもなっている分野です。一方、リスクの「見える化」やマネジメント分野を中心とするのが「セキュリティ／リスクマネジメントコース」、セキュアな物づくりに関して幅広く学ぶのが「システムデザインコース」となっています。

2年間の大学院教育を核に、短期講座、オンライン学習など多様な学び方を提供する

田中　4つのコースにもとづく実践的な講義・実習に加え、企業や他大学との連携に力を入れている点も大きな特色です。「研究と実務融合による高度情報セキュリティ人材育成プログラム（TSSスクエア）」「分野・地域を越えた実践的情報教育協働ネットワーク（enPiT／SecCap）」などはその代表例で、企業・研究機関や様々な大学院と連携して教育・研究を行っています。

後藤　これらは学生に大人気で、以前受講した人が「また受けたい」と希望することも多いプログラムです。あまりに希望者が増えて受講調整をしないといけないほどですが（笑）。

田中　開学当初、日本に情報セキュリティ分野の専門教育・研究を行う教育機関はありませんでしたが、私たちがそれを手探りで進め、経験の中で磨き上げ、日本の情報セキュリティ教育のスタンダードを作り上げたと言えるでしょう。

後藤　最近は官公庁や一般企業など利用者の立場から情報セキュリティを学びたいという要望も増え、教育ニーズの広がりを実感します。

田中　これまでの教育の積み重ねに加え、研究成果も修士論文・博士論文として蓄積されています。これらを完成させた修了生は博士前期・博士後期を合わせて300人を超え、多くが情報セキュリティ分野に携わっている人材。今後は同窓生同士のつながりも大きな力になるでしょう。

後藤　そういった大学院教育の太い幹があるからこそ、各方面から寄せられる情報セキュリティ教育の要望に対し、短期集中講座、オンライン学習、企業向け教育と多様な教育プログラムを提供できるのです。今後は当大学院修了生に向けたリカレント教育なども含め、さらに幅広い教育の機会を検討したいと考えています。

田中　私はセキュリティの中核技術は、海外からの輸入でなく国内で独自開発すべきと考えていますから、大学院でよりコアな技術者を育てる教育にも是非力を入れたいですね。

全員が論文を執筆することで、トレンドに流されない普遍的な力を身に付けていく

田中　ただ常に新たな問題が生まれる情報セキュリティの最前線では、トレンドに流されない普遍的な力も重要で、それは大学院教育という太い幹の部分で養う必要があるでしょう。コンピュータが人間に近づく今こそ、時代を変えていくような人間の力が改めて問われています。

後藤　その点では、当大学院の入学者全員が学位論文あるいは特定課題研究報告書を書いて修了する教育に大きな意義があると思っています。論文執筆を経験すると、課題を設定して解決策を模索し、指導教員のアドバイスを受けながら論理を組み立て、全体構造を把握して書き上げるという、多面的な力が伸ばせますから。

田中　論文のテーマ設定は意外に難しく、「何を課題とするか」で論文の出来具合が決まることも多いのです。しかしそうした経験で得られる「問題を見つけ、解決につながる課題を抽出する力」は、時代を超えて活用できるものです。

後藤　そして課題を解く中で、どのような創造性を発揮したかという経験も陳腐化しません。

田中　文理融合の情報セキュリティ分野は、自然に複眼的思考が養え、問題を見つけ、課題を設定する力も高められるでしょう。研究者でなくても、研究の経験はその人を大きく育てるのです。

専任

有田　正剛

教授

Seiko ARITA

■プロフィール
京都大学大学院理学研究科数学専攻修了、中央大学大学院理工学研究科情報工学専攻修了。博士（工学）。日本電気株式会社インターネットシステム研究所主任研究員を経て、2004年4月情報セキュリティ大学院大学教授に就任。

■主な研究業績
1. Seiko Arita, Shota Nakasato, Fully Homomorphic Encryption For Point Numbers, preprint.
2. Hiroaki Anada, Seiko Arita, Kouichi Sakurai, Attribute-Based Two-Tier Signatures: Definition and Construction, ICISC2015, Seoul, Korea, Nov. 2015.
3. Seiko Arita, Sari Handa, Two Applications of Multilinear Maps: Group Key Exchange and Witness Encryption, ASIAPKC 2014, pp.13-22, June 2014.

■主な研究テーマ
主な研究対象領域は:
- 楕円曲線暗号、格子暗号、イデアル格子暗号など暗号プリミティブ
- 鍵共有、コミットメント、ゼロ知識証明など暗号プロトコル
- 閾値復号、関数型暗号、完全準同型暗号など高機能暗号

■主な担当科目
数論基礎、暗号・認証と社会制度、暗号理論、研究指導、情報セキュリティ特別研究

■担当コース
数理科学コース、サイバーセキュリティとガバナンスコース

専任

大久保　隆夫

教授

Takao OKUBO

■プロフィール
1991年東京工業大学物理情報工学専攻修了。同年株式会社富士通研究所に入社。リバースエンジニアリング、分散開発環境、アプリケーションセキュリティの研究に従事。2006年、情報セキュリティ大学院大学入学、2009年同修了。博士（情報学）。2013年より本学准教授。2014年より同教授。情報処理学会コンピュータセキュリティ研究会専門委員。電子情報通信学会会員、日本ソフトウェア科学会会員、IEEE CS会員、計測自動制御学会 認証工学研究会会員。京都府警 サイバー犯罪対策研究会会員。Aviation Security研究会幹事、脅威分析研究会幹事。

■主な研究業績
1. 大久保 隆夫，田中 英彦：効率的なセキュリティ要求分析手法の提案,情報処理学会論文誌 Vol. 50,No.10 pp.2484-2499 (2009)
2. Takao Okubo, Kenji Taguchi, Haruhiko Kaiya and Nobukazu Yoshioka:MASG: Advanced Misuse Case Analysis Model with Assets and Security Goals,IPSJ Journal of Information Processing Vol.22(2014) No.3, pp.536-546 (2014)
3. Takao Okubo, Haruhiko Kaiya and Nobukazu Yoshioka:Analyzing Impacts on Software Enhancement Caused by Security Design Alternatives with Patterns,International Journal of Secure Software Engineering, Vol.3. No.1. pp.37-61 (2012)
4. 吉岡信和，大久保隆夫，宗藤誠治：セキュリティソフトウェア工学の研究動向,コンピュータソフトウェア Vol.28,No.3 pp.43-60 (2011)
5. 大久保隆夫：企業におけるセキュリティ分析技術の実効性,<特集>セキュリティ要求工学の実効性，情報処理　No.50, vol.3, pp. 230-234 (2009)

■主な研究テーマ
セキュリティ・バイ・デザイン、セキュリティ要求分析、ソフトウェアセキュリティ、Web、モバイルセキュリティ、制御系、組み込み系セキュリティ(IoT、車載、航空システム)、脅威分析、脆弱性評価、形式検証手法、攻撃手法に関する研究

■主な担当科目
ソフトウェア構成論、オペレーティングシステム、アルゴリズム基礎、セキュアシステム実習、特設講義（セキュリティ技術実践論）、研究指導

■担当コース
システムデザインコース、サイバーセキュリティとガバナンスコース

専任

佐藤　直

教授

Naoshi SATO

■プロフィール
中央大学理工学部電気工学科卒業。博士（工学）。NTTサービスインテグレーション基盤研究所主幹研究員として、研究成果のビジネス化の促進、情報通信サービス品質の評価設計に従事。2004年4月より本学教授。

■主な研究業績
1. Approaching a Target Using a Protection Feature Based on Received Signal Strength Indicator, ICORES 2016,Feb. 2016,K.Ishii, N.Sato
2. 修士論文等にみる情報セキュリティ大学院大学のシステムセキュリティ研究動向, 情報セキュリティ総合科学,vol.6, 2014年11月,佐藤直
3. セキュリティポリシーに基づくネットワークトラヒック制御の提案，　情報システム学会誌,Vol.9, No.2, 2014年3月,岡田康義,西川康宏,堀琢磨,佐藤直
4. 高校生のフィッシング詐欺に対する情報セキュリティ意識に関する考察，コンピュータ利用教育学会論文誌,Vol.4, 2013年3月,増山一光,佐藤直
5. Proposal of SNS Membership Qualification System Using Security Information Database, Asia Pacific & MEA Cup 2013,Mar. 2013,Y.Okada, K.Ishii, N.Sato
6. 配送情報の機械学習による迷惑メールのフィルタリング，日本セキュリティ・マネジメント学会誌,第26巻,第1号,2012年5月,本田致道,佐藤直
7. 学校設定科目によるコンピュータウィルス対策教育の実践，　教育情報研究,第27巻,第3号,2012年2月,増山一光,佐藤直

■主な研究テーマ
1.セキュアな通信のためのネットワーク構成・制御技術　2.サイバー攻撃防御技術
3.サイバー犯罪解析技術　4.ハッキング技術　5.セキュリティの定量的評価手法

■主な担当科目
ネットワークシステム設計・運用管理、インターネットテクノロジ、セキュアシステム実習、研究指導、
情報セキュリティ特別研究、特設講義（ハッキングとマルウェア解析）、特設講義（セキュリティ技術実践論）

■担当コース
システムデザインコース、セキュリティ／リスクマネジメントコース

専任

土井　洋

教授

Hiroshi DOI

■プロフィール
1988年3月岡山大学理学部数学科卒業、1988年4月より1996年3月まで日立ソフトウェアエンジニアリング株式会社勤務。1994年3月北陸先端科学技術大学院大学情報科学研究科修了、2000年9月岡山大学大学院自然科学研究科修了。博士（理学）。中央大学研究開発機構助教授を経て、2004年4月より本学教授。情報処理学会コンピュータセキュリティ研究運営委員会専門委員、横浜市個人情報保護審議会委員。

■主な研究業績
1. Partially Doubly-Encrypted Identity-Based Encryption Constructed from a Certain Scheme for Content Centric Networking, M. Sato, M. Mohri, H. Doi, Y. Shiraishi, Journal of Information Processing, Vol.24, No.1, pp.2-8 (2016).
2. Ciphertext Divided Anonymous HIBE and Its Transformation to Identity-Based Encryption with Keyword Search,　K. Tomida, H. Doi, M. Mohri, Y. Shiraishi, Journal of Information Processing, Vol.23, No.5, pp.562-569 (2015).
3. A Fully Secure Spatial Encryption Scheme, D. Moriyama, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.28-35 (2011).
4. Secure and Efficient IBE-PKE Proxy Re-Encryption, T. Mizuno, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.36-44 (2011).

■主な研究テーマ
電子署名,認証,暗号プロトコル等の安全性と電子社会システムへの応用に関する研究,特に
1. プライバシ保護関連技術及びその応用に関する研究
2. 認証方式や暗号方式の安全性に関する研究

■主な担当科目
暗号プロトコル、プログラミング、研究指導、情報セキュリティ博士演習、情報セキュリティ特別研究

■担当コース
数理科学コース、システムデザインコース

専任

林　紘一郎

教授

Koichiro HAYASHI

■プロフィール
東京大学法学部卒業。日本電信電話公社（当時）入社後、NTTアメリカ社長（本社役員待遇）、Nextel（現Sprint-Nextel）社取締役などを歴任。慶應義塾大学メディア・コミュニケーション研究所教授を経て、2004年4月以降、情報セキュリティ大学院大学教授(この間、2009年4月より2012年3月まで同学長・教授)。2012年4月より博士後期課程学生を主に担当。経済学博士（京都大学）。博士（法学、慶應義塾大学）。

■主な研究業績
1.『インフォミュニケーションの時代』中央公論社、1984年
2.『ネットワーキングの経済学』NTT出版、1989年
3.『ユニバーサル・サービス』（田川義博氏と共著）、中央公論社、1994年
4.『著作権の法と経済学』（編著）勁草書房、2004年
5.『情報メディア法』東京大学出版会、2005年
6.『進化するネットワーキング』（湯川抗・田川義博両氏と共著）NTT出版、2006年
7.『倫理と法一情報社会のリテラシー』（矢野直明氏と共著）産業図書、2008年
8.『引用する極意・引用される極意』（名和小太郎氏と共著）勁草書房、2009年
9.『セキュリティ経営』（田川義博・淺井達雄両氏と共著）勁草書房、2011年

■主な研究テーマ ・関心領域
情報セキュリティ
インターネットの自由と規律
技術標準、知的財産、メディアのあり方などをめぐる、法と経済学

■主な担当科目
情報セキュリティ特別研究、セキュア法制と情報倫理、個人識別とプライバシー保護

産学連携を意識した教授陣。

本学では、技術教育のみならず、法学、経済学、経営学、倫理学といった
人文・社会科学諸分野にもわたる学際的なアプローチによる教育・研究指導を行います。
そのため教授陣は、学界、産業界をはじめとした様々なフィールドの第一線で活躍中の研究者、技術者、実務家らを招聘し、
産学連携を意識した高度な専門教育を行う体制を整えています。
学際的な総合科学である情報セキュリティにふさわしく、情報セキュリティ関連の先端的研究の第一人者、トップマネジメント経験者、
IT系企業のエンジニア、ジャーナリスト、起業家、弁護士らをはじめとした多彩な顔ぶれによるプロフェッショナル集団です。

学長

田中　英彦

教授

Hidehiko TANAKA

■プロフィール
東京大学大学院工学系研究科電気工学専門課程修了。工学博士。東京大学にて計算機アーキテクチャ、並列処理、人工知能、分散処理、メディア処理などの教育・研究に従事。東京大学大学院情報理工学系研究科長を経て、2004年4月情報セキュリティ大学院大学情報セキュリティ研究科長・教授。2012年4月より同学長。情報処理学会功績賞、人工知能学会論文賞、ACM SIGGRAPH'99 Impact Paper Award、人工知能学会功績賞、東京都科学技術功労者表彰、経済産業大臣表彰など受賞。日本ネットワークセキュリティ協会(JNSA)会長、IEEE Life Fellow、情報処理学会名誉会員、人工知能学会名誉会員、東京大学名誉教授。

■主な研究業績
(1)より安全なシステム構築のために～CC-Case_iによるセキュリティ要件の見える化、日本セキュリティマネジメント学会誌、2016年1月.
(2)ファイル構造検査による悪性MS文書ファイルの検知, 情報処理学会論文誌, 2014年5月,
(3)悪性文書ファイルに埋め込まれたRATの検知法, 情報処理学会論文誌, 2014年2月.
(4)多変量解析による標的型攻撃の分類, 情報処理学会論文誌, 2013年12月.
(5)特徴データベースを用いない効率的な仮想マシンモニタ検出方式の提案，情報処理学会論文誌, 2011年9月,
(6)論理プログラミングを基礎とした認可ポリシ記述言語, 情報処理学会論文誌, 2010年9月.
(7)機密情報共有に有用な情報フロー制御モデルの提案, 情報処理学会論文誌, 2010年2月.
(8)効率的なセキュリティ要求分析手法の提案, 情報処理学会論文誌, 2009年10月.
(9)定点観測によるボットネットの観測とMalwareの動作挙動解析システムの提案，情報処理学会論文誌, 2008年4月.
(10)Parallel Inference Engine PIE, ohmsha, August 2000.
(11)非ノイマン型コンピュータ，電子情報通信学会，1989年11月.

■主な研究テーマ
情報社会を構成する様々な情報システムについて、セキュアなシステム構成法、信頼性高い構成法、利用者が長期に依存できる継続性の維持など、人々が安心して情報システムに頼った生活を営み、生き生きとした社会を作り上げるための諸技術の研究開発をテーマとしています。すなわち、OSや仮想マシン、クラウドコンピューティングなどのセキュアシステム基盤、セキュアなソフトウエア構成手法やアクセス制御方式などのセキュアシステム構築手法、侵入対策やマルウエア対策などのネットワークセキュリティ技術等の研究を行っています。

■主な担当科目
情報システム構成論、情報デバイス技術、情報セキュリティ特別研究、研究指導

■担当コース
システムデザインコース、サイバーセキュリティとガバナンスコース

情報セキュリティ研究科長

後藤　厚宏

教授

Atsuhiro GOTO

■プロフィール
1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術、高信頼クラウドコンピューティグ技術、ID管理技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。現在、IEEE Computer SocietyのBoard of Governor、情報処理学会理事。enPiTセキュリティ分野代表。2011年7月より本学教授。2014年4月より同情報セキュリティ研究科長。2015年11月より内閣府SIPプログラムディレクタ。

■主な研究業績
1. I. Mizukoshi, A. Nakanishi, A. Goto. Firmware Update Trend in the Internet of Things -An Empirical Survey of Japanese HGW Vendors-. The International Conference on Computing Technology, Information Security and Risk Management (CTISRM2016). March 2016.
2. 森 滋男、後藤厚宏. サイバーセキュリティと情報漏えい対策. 行政&情報システム vol51, Dec 2015.
3. 後藤厚宏.ビッグデータ活用におけるガバナンス.情報処理 vol.56, No.10,2015
4. 田中恭之，後藤厚宏.悪性文書ファイル内のROP攻撃コード静的判定手法.情報処理学会 論文誌 vol.56, No9, 2015
5. Y.Tanaka, A. Goto. N-ROPdetector: Proposal of a method to detect the ROP attack code on the network. ACM CCS2014 SafeConfig 2014 : Cyber Security Analytics and Automation, Nov. 2014.

■主な研究テーマ
1. IoT技術とビッグデータ・クラウド
2. 重要インフラのセキュリティ
3. インターネットセキュリティ技術とID管理技術

■主な担当科目
個人識別とプライバシー保護
ネットワークシステム設計・運用管理
情報システム構成論
特設講義（情報セキュリティ運用リテラシーI・II）
特設実習（セキュリティ実践I・II）
研究指導

■担当コース
サイバーセキュリティとガバナンスコース、システムデザインコース、セキュリティ／リスクマネジメントコース

兼任
上沼　紫野
客員教授
Shino UENUMA

■プロフィール
虎ノ門南法律事務所所属弁護士。
東京大学法学部卒業。Washington University in St.LouisにてLL.M.取得。知的財産権、IT関連、渉外法務等を中心に業務を行う。一般社団法人モバイルコンテンツ審査・運用監視機構事務局長常任理事。
最高裁司法研修所刑事弁護教官(2012−2015)
■担当科目
セキュリティの法律実務

兼任
生越　由美
客員教授
Yumi OGOSE

■プロフィール
東京理科大学専門職大学院教授
1982年東京理科大学薬学部卒業、経済産業省特許庁入庁、審査第三部審査官、審判部審判官を経て、97年審判部書記課長補佐、03年特許審査第二部上席総括審査官(室長)、同年10月政策研究大学院大学助教授、05年東京理科大学専門職大学院教授、現在に至る。現在、内閣官房IT戦略本部農林水産部会委員、総務省独立行政法人評価委員会情報通信・宇宙開発分科会委員、農林水産 技術会議専門委員、経済産業省 関東経済産業局・広域関東圏知的財産戦略本部員などを務める。
■担当科目
知的財産制度

兼任
柴山　悦哉
客員教授
Etsuya SHIBAYAMA

■プロフィール
東京大学情報基盤センター 情報メディア教育研究部門教授
1983年京都大学理学研究科数理解析専攻修士課程修了。東京工業大学助手、龍谷大学講師、東京工業大学助教授、同教授を経て2008年4月より現職。専門はソフトウェアセキュリティ、プログラミング言語、ユーザインタフェースソフトウェア。理学博士(1991年、東京大学)。
■担当科目
セキュアプログラミングとセキュアOS

兼任
周佐　喜和
客員教授
Yoshikazu SHUSA

■プロフィール
横浜国立大学大学院環境情報研究院教授
1984年東京大学大学院経済学研究科博士課程単位取得退学。横浜国立大学経営学部講師・助教授、横浜国立大学大学院環境情報研究院助教授を経て、2005年より現職。専門は経営学。
■担当科目
組織行動と情報セキュリティ

兼任
竜田　敏男
客員教授
Toshio TATSUTA

■プロフィール
情報セキュリティ大学院大学 セキュアシステム研究所 客員研究員
1966年早稲田大学第一理工学部電気工学科卒業。日本無線株式会社電子計算機課、日本アイ・ビー・エム株式会社製品開発研究所、標準部門などを経て、2005年より情報セキュリティ大学院大学客員研究員。 専門分野は、情報セキュリティ標準化、および標準と知財。2010年よりISO/IEC JTC1/SC27/WG2の Vice-Convenor に就任。2013年に情報セキュリティ分野の標準化活動に対して経済産業大臣表彰を受賞。
■担当科目
国際標準とガイドライン

兼任
辻　秀典
客員教授
Hidenori TSUJI

■プロフィール
株式会社情報技研 代表取締役社長
東京工業大学工学部情報工学科卒業、東京大学大学院工学系研究科情報工学専攻修了。博士(工学)。株式会社インターネット総合研究所を経て、株式会社情報技研を設立。業務では、ICTシステムおよび情報セキュリティに関するコンサルティングはじめ、各種ICTシステムの提案、開発、構築業務に携わる。研究テーマは、セキュアシステム基盤、セキュアシステム構成、著作権情報管理、メディア処理等。電子情報通信学会 ヒューマンコミュニケーショングループ 食メディア研究会専門委員。
■担当科目
セキュアシステム構成論

兼任
藤本　正代
客員教授
Masayo FUJIMOTO

■プロフィール
筑波大学客員教授
富士ゼロックス株式会社パートナー
GLOCOM客員研究員
MIT科学技術政策大学院修士課程修了。東京工業大学大学院博士課程修了。博士(工学)。専門は経営と情報通信技術、リスクマネジメント。経営コミュニケーション。
■担当科目
リスクマネジメント

兼任
堀江　正之
客員教授
Masayuki HORIE

■プロフィール
日本大学商学部・大学院商学研究科教授
カリフォルニア大学ロサンゼルス校(UCLA)客員研究員を経て現職。商学博士。現在、システム監査学会理事、日本監査研究学会常務理事、日本内部統制学会理事、情報処理技術者試験委員、金融庁・行政事業レビュー有識者会議メンバーなどを兼任。『ITのリスク・統制・監査』(同文舘出版、2009年、編著)『IT保証の概念フレームワーク−ITリスクからのアプローチ』(森山書店、2006年)、『システム監査の理論』(白桃書房、1993年)他、著書多数。
■担当科目
セキュリティシステム監査

兼任
丸山　満彦
客員教授
Mitsuhiko Maruyama

■プロフィール
公認会計士、情報システム監査人(CISA)／デロイト トーマツ リスクサービス株式会社代表取締役社長／デロイトトーマツ サイバーセキュリティ先端研究所 所長 兼務。
1992年監査法人トーマツ入社。1998年より2000年までDeloitteのデトロイト事務所に勤務。製造業グループ他米国企業のシステム監査を実施。帰国後、リスクマネジメント、コンプライアンス、情報セキュリティ、個人情報保護関連の監査及びコンサルティングに従事。経済産業省の情報セキュリティ監査研究会、情報セキュリティ総合戦略策定委員会、個人情報保護法ガイドライン策定委員会他、国土交通省、厚生労働省の情報セキュリティ関連の委員会等の委員、日本情報処理開発協会ISMS技術専門部会等の委員を歴任。2012年3月末まで内閣官房情報セキュリティセンター情報セキュリティ指導官。
■担当科目
セキュリティシステム監査

兼任
森井　昌克
客員教授
Masakatu Morii

■プロフィール
神戸大学大学院工学研究科教授
1989年大阪大学大学院工学研究科博士後期課程通信工学専攻修了、工学博士。愛媛大学助教授、徳島大学工学部教授などを経て、2005年神戸大学工学部電気電子工学科教授。2007年より現職。現在、マルチメディア情報通信工学、ネットワークセキュリティ、情報理論、暗号理論等の研究、教育に従事。
■担当科目
不正アクセス技法

兼任
森　直彦
客員教授
Naohiko Mori

■プロフィール
1984年京都大学大学院工学研究科情報工学専攻修士課程修了。NTT研究所にて計算機システムの高信頼化方式の研究、OSの性能評価等に従事。NTTコミュニケーションズ株式会社にて同社公式Webサイトの開発・運用、コンシューマ向け認証サービスの開発、高機密情報保管システムの開発等に従事。現在、NTTアドバンステクノロジ株式会社にて企業向けセキュリティサービス・コンサルティングビジネスのグループを主管。特定非営利活動法人 日本ネットワークセキュリティ協会 幹事。
■担当科目
特設実習(セキュリティ実践II)

兼任
Daniel Dolan
客員教授

■プロフィール
早稲田大学大学院会計研究科教授
Ph.D. Speech Communication (Cultural Communication), University of Washington; 1998
■担当科目
Presentations for Professionals

兼任
小林　雅一
客員准教授
Masakazu KOBAYASHI

■プロフィール
ジャーナリスト／KDDI総研リサーチフェロー
1985年東京大学物理学科卒業。同大学院理学系研究科を修了後、総合電機メーカーや出版社勤務を経て米国留学。1995年ボストン大学にて マスコミュニケーション修士号取得。著書に「AIの衝撃　人工知能は人類の敵か」(講談社現代新書、2015年)、「クラウドからAIへアップル、グーグル、フェイスブックの次なる主戦場」(朝日新書、2013年)など多数。
■担当科目
マスメディアとリスク管理

兼任
藤村　明子
客員准教授
Akiko FUJIMURA

■プロフィール
日本電信電話株式会社 セキュアプラットフォーム研究所 研究主任
慶應義塾大学法学部法律学科、同大学大学院政策・メディア研究科修了後、日本電信電話株式会社に入社。同社在職中に中央大学大学院法務研究科修了。法務博士(専門職)。情報セキュリティ、個人情報保護、プライバシ保護の技術と法制度に関する研究開発に従事。情報ネットワーク法学会元理事、デジタル・フォレンジック研究会幹事。
■担当科目
セキュリティの法律実務

兼任
小﨑　俊二
客員講師
Shunji KOZAKI

■プロフィール
情報セキュリティ大学院大学 客員研究員
早稲田大学理工学研究科修士課程修了。化学メーカー、ITベンチャー企業勤務を経て情報セキュリティ大学院大学情報セキュリティ研究科入学。同修了。博士(情報学)。専門分野は代数曲線暗号。
■担当科目
計算代数

兼任
塩月　誠人
客員講師
Makoto SHIOTSUKI

■プロフィール
ネットワークセキュリティコンサルタント
合同会社セキュリティ・プロフェッショナルズ・ネットワーク 代表社員
鹿児島大学理学部地学科卒業。システム開発、システム・ネットワーク管理を経て、セキュリティ監査や各種セキュリティコンサルティング業務に従事。その後、中央大学における実践的セキュリティ人材育成に携わり、2008年、セキュリティ教育事業を行う合同会社を設立、現在に至る。
■担当科目
特設実習(Windowsセキュリティ)

兼任
苫米地　なつ帆
客員講師
Natsuho TOMABECHI

■プロフィール
東京大学社会科学研究所附属社会調査・データアーカイブ研究センター 助教
2016年東北大学大学院教育学研究科博士課程後期3年の課程修了。博士(教育学)。専門は家族社会学・計量社会学。
■担当科目
統計的方法論

※上記は2016年4月現在

専任
原田　要之助
教授
Yonosuke HARADA

■プロフィール
1979年京都大学大学院工学部数理工学専攻修了。電信電話公社(現NTT)研究所で通信ネットワークの監視、制御システム、通信ネットワークのセキュリティアーキテクチャの研究等に従事。1999年より情報通信総合研究所にてコンサルやセキュリティ監査に従事。OPCWの情報セキュリティ監査にも従事し、2000年から2008年までチームリーダを務める。2010年4月情報セキュリティ大学院大学教授に就任。セキュリティマネジメント学会会長、情報処理学会電子化知的財産社会基盤研究会幹事、システム監査学会理事、電子情報通信学会、経営情報学会、IEEE Computer Society等所属。元ISACA国際本部副会長。日本セキュリティ監査協会資格認定委員長。日本ITガバナンス協会理事、iMISCA理事、ISO/IEC SC40/WG1の国内委員会主査及びISO/IEC38503のEditor、ISO/IEC SC27/WG1の国内委員会委員及びISO/IEC27021のCo-editor。中央大学大学院非常勤講師、サイバー大学非常勤講師、フェリス女学院大学非常勤講師。2013年ISC2より、Senior Information Security Professional Categoryで表彰。

■主な研究業績
1. Information security governance framework(共著、2009年9月、Proceedings of the first ACM workshop, 'Proceedings of the first ACM workshop on Information security governance'、pp.1-6)
2. デジタル社会の編成原理(著書共著、2003年1月、NTT出版、pp.98-122)
3. JRMS2010解説書(組織のリスクマネジメントを測定・診断するツール)(共著、日本情報処理開発協会、2010年5月)
4. CobiT実践ガイドブック(共著、監修と執筆)、日経BP社、2008年9月、pp.138-151)
5. あなたの組織を守る危機管理, 危機管理研究会(共著, ぎょうせい, 2012)
6. ITリスク学(共著, 第8章"ITシステムのリスクマネジメントの全体像", 共立出版, 2013)
7. ISO/IEC 27002:2013(JIS Q27002:2014)情報セキュリティ管理策の実践のための規範 解説と活用ガイド(共著, 第8章及び第14章, 2015)

■主な研究テーマ
情報セキュリティマネジメントとガバナンス、情報セキュリティ監査とシステム監査、
複数企業グループにおけるITガバナンス、情報セキュリティガバナンス

■主な担当科目
情報セキュリティマネジメントシステム、セキュリティ管理と経営、特設講義(セキュリティ監査)、研究指導

■担当コース
セキュリティ／リスクマネジメントコース、サイバーセキュリティとガバナンスコース

専任
廣松　毅
教授
Takeshi HIROMATSU

■プロフィール
東京大学教養学部教養学科卒業、東京大学大学院経済学研究科修士課程修了。東京大学教養学部助手、同助教授、ハーバード大学イェンチン研究所客員研究員等を経て、1989年東京大学教授(先端科学技術研究センター)、1995年より2009年3月まで同(大学院総合文化研究科・教養学部)。2009年4月情報セキュリティ大学院大学教授に就任。2012年4月より特任(専任)教授として博士後期課程学生の指導を主に担当。日本学術会議19期会員、20−21期・23期連携会員。2007年10月〜2015年9月　内閣府統計委員会委員

■主な研究業績
1. 廣松毅・小林稔・坪根直毅・栗田学・大平号声『非生産部門における情報装備の経済効果に関する定量分析』日本社会情報学会『日本社会情報学会学会誌:学術論文』第16巻1号 2004年3月 pp.43-60 <日本社会情報学会平成16年度学会賞『優秀論文賞』受賞>廣松毅他著『経済時系列分析』多賀出版、2006
2. 廣松毅他著『経済統計』新世社、2006
3. 廣松毅他編著『現代社会における情報システムのマネジメント』中央経済社、2009
4. 廣松毅『情報セキュリティ事故が企業評価に与える影響の分析-イベント・スタディ分析を用いたリスク評価の試み』『情報セキュリティ総合科学』(紀要)Vol.3 2011 pp.91-106
5. 廣松毅(2012)「個人情報保護法による情報セキュリティ意識の変化に関する定量的評価-イベント・スタディ法を用いた意識変化の定量分析の試み」『情報セキュリティ総合科学』(紀要)Vol.4 2012 pp.150-170
6. 濱田良隆・廣松毅「情報セキュリティにおける逸脱行動の助長および抑止要因に関する考察−組織構成員による情報持ち出し逸脱行動についてのアンケート調査結果分析−」日本経営情報学会『経営情報学会誌』第21巻3号2012年12月pp.205-226
7. Nakamuro, M., Inui, T., Senoh, W. & Hiromatsu, T. "Are Television and Video Games Really Harmful for Kids?" *Contemporary Economic Policy* 33(1) 2015, pp.29-43
8. 相羽律子・廣松毅「情報セキュリティ対応に関する組織の意思決定を支援するモデルの統計データによる検証」一般社団法人・経済産業統計協会『経済統計研究』第43巻III号　pp.32-52

■主な研究テーマ
情報セキュリティリスクの定量的な把握(情報セキュリティリスクに関する数理的・統計的分析)
情報セキュリティに関する経済的社会的分析(情報セキュリティリスクに関する経済学・社会学的な分析)

■主な担当科目
情報セキュリティ博士演習、情報セキュリティ特別研究、統計的リスク管理、リスクの経済学

専任
松井　俊浩
教授
Toshihiro MATSUI

■プロフィール
1982年東京大学大学院情報工学専門課程修士修了、1990年同大学院工学博士、1982年通商産業省工業技術院電子技術総合研究所、知能ロボットのプログラミングシステムの研究。1991年〜1999年米国スタンフォード大学、MIT、オーストラリア国立大学の客員研究員。2001年産業技術総合研究所企画本部、2003年産総研デジタルヒューマン研究センターにて分散型実時間計算システムの研究。2007年産総研副研究統括、2012年セキュアシステム研究部門長、2015年NEDO技術戦略研究センター(TSC)。日本ロボット学会、計測自動制御学会等の論文賞等十数件。日本ロボット学会フェロー、情報セキュリティスペシャリスト。2016年より、NEDO-TSCの電子情報機械システムユニット長および本学教授。

■主な研究業績
1. Toshihiro Matsui and Michiharu Tsukamoto, "An Integrated Method for Robot Teleoperation Using Multi-Media Display," Proc. Of Int. Symposium on Robotics Research (ISRR), 1989 (研究賞受賞)
2. 松井俊浩、関口智嗣、「マルチスレッドを用いた並列EusLispの設計と実現」、情報処理学会論文誌、第36巻、8号、pp. 1885-1896、1995年8月.
3. 松井俊浩、麻生英樹、John Fry他、「オフィス移動ロボットJijo-2 の音声対話システム」、日本ロボット学会誌、第18巻、2号、pp. 300-307, 2000年3月 .
4. 山崎信行、松井俊浩、「並列分散リアルタイム制御用レスポンシブプロセッサ」、日本ロボット学会誌、Vol. 19, No. 3, 2001 (論文賞受賞)
5. 松井俊浩、「オブジェクト指向型ロボットプログラミング言語EusLisp」、日本ソフトウェア科学会コンピュータソフトウェア、Vol. 23, No. 2, pp. 62-71, 2006.

■主な研究テーマ
制御システムセキュリティ、組み込みシステムセキュリティ、生命型セキュリティ、
ロボットプログラミングシステム

■主な担当科目
情報デバイス技術、情報システム構成論、研究指導

■担当コース
システムデザインコース

専任
湯淺　墾道
教授
Harumichi YUASA

■プロフィール
慶應義塾大学大学院法学研究科博士課程退学。九州国際大学法学部専任講師、助教授、准教授をへて2008年4月より教授。2008年9月より九州国際大学副学長。2011年4月より本学教授、2012年4月より学長補佐を併任。九州大学・中央大学・愛知学院大学・横浜市立大学非常勤講師、各自治体の個人情報保護関係の審議会委員、ベネッセホールディングス情報セキュリティ監視委員会委員、情報ネットワーク法学会副理事長等を務める。

■主な研究業績
1. 『電子化社会の政治と制度』(オブアワーズ、2006年3月)
2. 「インターネット選挙運動解禁の課題」『選挙』66巻4号(2013年4月)3-8頁
3. "A Consideration of the 2007 Upper House election in Japan". Journal of Asian Women's Study. vol.16, pp97-102 (2008).
4. 「アメリカの電子投票におけるVVPATの現状と課題」『情報ネットワーク・ローレビュー』第6巻(2007年5月)187-203頁
5. 「個人情報保護法改正の課題 −地方公共団体の個人情報保護の問題点を中心に 問題点を中心に −」『情報セキュリティ総合科学』第6巻(2014年)53-92頁

■主な研究テーマ
1. プライバシー等に関する各国の憲法、法律上の規定の比較研究
2. 電子投票、インターネット選挙運動など政治・選挙と情報に関する法制度の研究
3. 地方自治体における情報公開や個人情報保護に関する研究
4. 自治基本条例の制定や指定管理者制度の導入など自治体における改革の研究
5. サイバーセキュリティに関する法制度の研究

■主な担当科目
法学基礎、セキュリティの法律実務、セキュア法制と情報倫理、研究指導

■担当コース
サイバーセキュリティとガバナンスコース、セキュリティ／リスクマネジメントコース

専任
橋本　正樹
准教授
Masaki HASHIMOTO

■プロフィール
2001年、立命館大学文学部人文総合科学インスティテュート卒業。学部在籍時より新規法人の立ち上げに参画し、以降同社にて情報システムの運用管理・監視サービス業務に従事。2007年、情報セキュリティ大学院大学・情報セキュリティ研究科・博士前期課程修了。2010年、同博士後期課程修了。博士(情報学)。2010年より同助教、2014年より同准教授。2014年4月-2015年3月、ロンドン大学ロイヤルホロウェイ校情報セキュリティグループの訪問研究員として英国に滞在。専門はアクセス制御、OSセキュリティ。情報処理学会、電子情報通信学会、日本ソフトウェア科学会、IEEE各会員。電子情報通信学会／情報通信システムセキュリティ研究会(ICSS)専門委員、情報処理学会／コンピュータセキュリティ研究会(CSEC)運営委員、情報処理学会論文誌ジャーナル/JIP編集委員会委員等。

■主な研究業績
1. 橋本正樹: アクセス制御技術とその最新動向, 日本セキュリティ・マネジメント学会誌, Vol.29, No.3, pp.21-27, 2016.
2. 安藤類央, 橋本正樹, 山内利宏: 仮想化技術による安全なファイルアクセスログ外部保存機構, 情報処理学会論文誌, Vol.54, No.2, pp.585-595, 2013.
3. 原田季栄, 半田哲夫, 橋本正樹, 田中英彦: アプリケーションの実行状況に基づく強制アクセス制御方式, 情報処理学会論文誌, Vol.53, No.9, pp.2130-2147, 情報処理学会, 2012.
4. 橋本正樹, 安藤類央, 前田俊行, 田中英彦: 情報セキュリティ向上に向けたOS研究の動向, 情報処理学会論文誌:コンピューティングシステム(ACS), Vol.5, No.2, pp.51-62, 情報処理学会, 2012.
5. 橋本正樹, 金美羅, 辻秀典, 田中英彦: 論理プログラミングを基礎とした認可ポリシ記述言語, 情報処理学会論文誌, Vol.51, No.9, pp.1682-1691, 情報処理学会, 2010.
6. Hashimoto, M., Kim, M., Tsuji, H. and Tanaka, H.: Policy Description Language for Dynamic Access Control Models, DASC'09: Proceedings of the 8th IEEE International Symposium on Dependable, Autonomic & Secure Computing, Chengdu, China, IEEE Computer Society, pp. 37-42, 2009.

■主な研究テーマ
1. アクセス制御技術/OSセキュリティ、 2. 不正侵入検知・防御

■主な担当科目
アルゴリズム基礎、オペレーティングシステム、セキュアシステム実習、
特設講義(ハッキングとマルウェア解析)、特設講義(セキュリティ技術実践論)

■担当コース
システムデザインコース

■ 主な年間スケジュール（2015年度ご参考）

- 4/6 入学式
- 4/7 前期開講
- 新入生歓迎会
- 5/23 春季オープンキャンパス
  ホームカミングパーティ
- 7/31 前期授業期間終了
- 8/29 修士論文等発表会（9月修了）
- 10/1 後期開講
- 10/16 第12回アドバイザリーボード
- 11/7 秋季オープンキャンパス
  ホームカミングパーティ
- 2/12 後期終講
- 2/20 修士論文等発表会（3月修了）
- 3/19 学位記授与式

■ 入学式
2015.4.6

設置母体である学校法人岩崎学園の各姉妹校との合同入学式が、パシフィコ横浜で開催されました。

■ 修士論文等発表会
2016.2.20

博士前期（修士）課程での研究成果の集大成となる修士論文の発表会が一般公開として開催されました。

2015年度も暗号理論からセキュリティ技術、マネジメント手法に至るまで多彩なテーマの修士論文が発表されました。

■ 学位記授与式
2016.3.19

学長から修了生一人ひとりに学位記が授与されるとともに、優れた研究成果を上げた学生に対して表彰状と記念品が贈られました。

■ 情報セキュリティ大学院大学連携教授（2016年4月現在）

本学をはじめとする大学の研究者と企業とが連携を取り、情報セキュリティ技術の研究開発や教育を推進するために、連携教授の仕組みを設けております。現在、以下に示すような大学・企業の方々にご就任いただき、研究会・特別講義などの活動をおこなっております。

株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹	秋山 浩一郎
日本電信電話株式会社 セキュアプラットフォーム研究所 所長	梅本 佳宏
日本アイ・ビー・エム株式会社 東京ソフトウェア＆システム開発研究所 クラウド開発部長	浦本 直彦
株式会社日立製作所 テクノロジーイノベーション統括本部 システムイノベーションセンタ セキュリティ研究部 部長	鍛 忠司
パナソニック株式会社 全社CTO室 ソフトウェア戦略担当 理事	梶本 一夫
東京電機大学 未来科学部 教授	佐々木 良一
沖電気工業株式会社 経済・政策調査部 部長	杉尾 俊之
国立研究開発法人産業技術総合研究所 情報・人間工学領域 領域長	関口 智嗣
株式会社富士通研究所 知識情報処理研究所 サイバー・システムセキュリティプロジェクト プロジェクトディレクター	武仲 正彦
株式会社KDDI研究所 執行役員	田中 俊昭
日本電気株式会社 ビジネスイノベーション統括ユニット 技術イノベーション戦略本部長兼IoT戦略室エグゼクティブエキスパート	谷 幹也
三菱電機株式会社 開発本部 役員技監 松井暗号プロジェクト統括	松井 充
横浜国立大学 大学院 環境情報研究院 教授	松本 勉
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所長	宮崎 哲弥

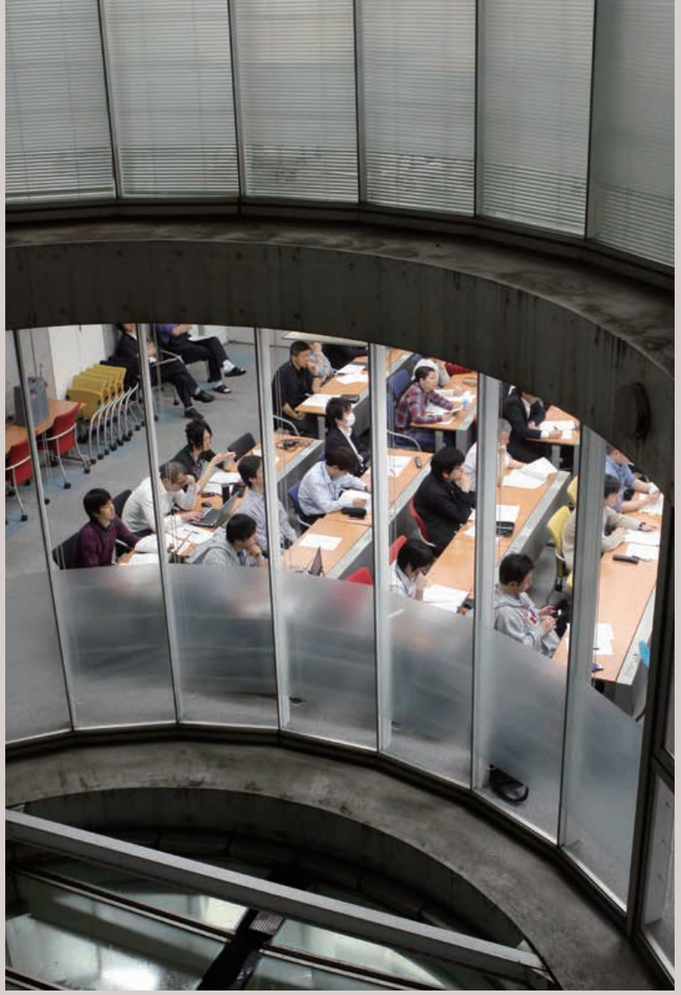
敬称略、氏名五十音順

■ 情報セキュリティ大学院大学アドバイザリーボードメンバー（2016年4月現在）

本学では、研究教育活動全般についてのご支援と、研究動向並びに教育効果に対するご助言・ご示唆をいただき、本学のポテンシャルの向上と活性化を図るべく、各界の有識者より成るアドバイザリーボードを設置しております。私たちは、情報セキュリティの将来方向をリードする高度な人材育成と社会貢献を実現するため、アドバイザリーボードよりいただくご助言を真摯に受け止め、大学として進むべき方向性を精査し続けてまいります。

早稲田大学政治経済学術院 教授	縣 公一郎
沖電気工業株式会社 常務執行役員 情報責任者、情報・技術本部長	猪﨑 哲也
株式会社日立ソリューションズ 技術統括本部 統括本部長	石川 明
パナソニック株式会社 AVCネットワークス社 イノベーションセンター 所長	江坂 忠晴
株式会社エヌ・ティ・ティ・データ 常務執行役員 技術革新統括本部長	木谷 強
株式会社富士通エフサス 取締役会長	工藤 義一
芝浦工業大学大学院工学マネジメント研究科 教授	國井 秀子
神奈川県 副知事	黒川 雅夫
早稲田大学理工学術院 教授	後藤 滋樹
国立研究開発法人 情報通信研究機構 理事長	坂内 正夫
東京電機大学未来科学部 教授 内閣サイバーセキュリティセンター サイバーセキュリティ補佐官	佐々木 良一
NTTコミュニケーションズ株式会社 経営企画部長	佐々倉 秀一
日本電信電話株式会社 代表取締役副社長 研究企画部門長	篠原 弘道
日本電気株式会社 シニアオフィサー	庄司 信一
日本経済新聞社 論説委員兼編集委員	関口 和一
慶應義塾大学 大学院政策・メディア研究科 教授	土屋 大洋
三菱電機株式会社 顧問	堤 和彦
独立行政法人 情報処理推進機構 理事長	富田 達夫
株式会社東芝 取締役 執行役専務	西田 直人
朝日新聞社 ジャーナリスト学校主任研究員 記者	服部 桂
日本放送協会 理事・技師長	浜田 泰人
横浜市 副市長	渡辺 巧教

敬称略、氏名五十音順



授業シーン

仕事や生活の中で感じた
問題意識をもとに大学院で学び、
その成果を社会にダイレクトに生かせること。
多様な価値観、知識、キャリアを持つ
教員や在学生との間で生まれるシナジー効果。
事例研究、実習、輪講、複数教員による指導、演習など、
科目内容に応じて教育効果を高める
授業の方式を採用し、
高度な分析能力、問題解決能力を涵養します。

より現実に即した環境で、不正侵入検知システム（IDS）、ファイアウォール、セキュアプログラミングをはじめとした情報セキュリティに関する実際的専門的な実習が可能になるよう、各種サーバを多数設置しています。また、希望者にはノートパソコンを無償貸与します。

情報セキュリティに関する書籍、雑誌を図書室に配架するほか、学内からACM DigitalLibrary、IEEE、Springer LNCS、LexisNexis at Lexis.comなどのオンラインデータベースへアクセスでき、最新の国際的な情報資源による調査・研究活動が可能です。

院生自習・実験室は平日はもちろん土日・祝日も朝8時から夜11時まで開放しています。

教育研究環境

新しい一歩に向けて、従来のやり方を見直す。
より専門的な知識を得るために、
幅広い視野を身につける。
今のあなたに起きた小さな変化が、
未来の自分を、そして社会さえ変えるきっかけになるかも知れません。
情報ネットワークでつながることが当然の世界を、
より安全で、使いやすく、幸せにするために…。
情報セキュリティが持つ豊かな可能性を武器に、
明日に貪欲に挑み続ける人と一緒に育つ大学院が、
ここ横浜にあります。

■ 学費等納入金

項目	金　額		
	博士前期（修士）課程（2年制プログラム）	博士前期（修士）課程（1年制プログラム）	博士後期課程
入学金	300,000円	300,000円	300,000円
授業料（年額）	1,000,000円	1,800,000円	800,000円
施設設備費（年額）	150,000円	150,000円	150,000円
実習費（年額）	50,000円	50,000円	50,000円
初年度学費合計	1,500,000円	2,300,000円	1,300,000円

備考　（1）　2年次以降の学費は、入学金を除いた金額となります。なお、本学博士前期課程修了者が博士後期課程に進学した場合、博士後期課程の入学金は全額免除となります。
（2）　授業料、施設設備費、実習費については、各々2分の1を前期学費及び後期学費とします。

［博士前期課程2年制プログラム4月入学の学費納入例］

初年度　各入学手続締切日まで　計900,000円（入学金300,000円＋前期学費600,000円）
9月末日まで　後期学費600,000円
2年次　4月20日まで　前期学費600,000円
9月末日まで　後期学費600,000円

■ 奨学金

学業成績、人物ともに優秀であり、経済的理由により学資が不足する学生に対して、下表の奨学金制度があります。
詳細はお問い合わせください。

①日本学生支援機構（予約採用を除き、募集時期は毎年春です。本学では学部新卒学生の方を中心に、希望者の多くが採用されています。）http://www.jasso.go.jp/

種別	貸与月額（※2016年4月現在）
第一種奨学金（無利子）	50,000円又は88,000円（博士前期課程の場合）
	80,000円又は122,000円（博士後期課程の場合）
第二種奨学金（有利子）	5, 8,10,13,15万円のなかから選択

・貸与方法　本人の預金口座に、原則として毎月1回当月分を振込
・貸与総額　（博士前期課程第一種奨学金 月額88,000円の場合）×24ヶ月＝2,112,000円
・返還方法　大学院修了後、日本学生支援機構が定める期間内に返還

② 岩崎学園奨学金（有職の社会人も利用可能です）

貸与額	募集人数
年額　500,000円（無利子）	若干名（収容定員の20%以内）

・貸与方法　4月入学の場合は前期学費（10月入学の場合は後期学費）に対し貸与※
※奨学生採用者は貸与額を差し引いた学費を納入することになります

・貸与総額　（博士前期課程2年制プログラムの場合）年額500,000円×2年=1,000,000円
・返還方法　大学院修了後、奨学生本人が毎月均等もしくはボーナス併用により返還（4年以内）
・その他　応募者に対し、入学前に採用結果を通知

■ 特待生制度

人物、学業成績が特に優秀であり、自立心と向上心が旺盛な情報セキュリティ研究科博士前期課程［2年制］入学志願者※の中から特待生選抜試験に合格した者に対し、授業料等の減免を行う制度です。
（※4年制大学等卒業見込み者に限ります。出願資格の詳細については、本学ウェブサイトに掲載の特待生選抜学生募集要項にてご確認ください）

○ 特待生選抜試験に合格した場合の初年度学費

種別	金　額
特待生Ⅰ	300,000円（入学金 300,000円、授業料 免除、施設設備費 免除、実習費 免除） ・特待生Ⅰの初年度学費は、上記のとおり入学金以外全額免除となります。なお、原則として2年次の学費も全額免除となりますが、1年次の学業成績が一定基準に達することが条件となります。
特待生Ⅱ	900,000円（入学金 300,000円、授業料 500,000円、施設設備費 75,000円、実習費 25,000円） ・特待生Ⅱの初年度学費は、上記のとおり入学金以外は、半額免除となります。なお、原則として2年次の学費も半額免除となりますが、1年次の学業成績が一定基準に達することが条件となります。

○ 特待生募集人数:若干名（特待生Ⅰ、特待生Ⅱとも）

情報セキュリティ大学院大学

セキュアシステム研究所

Secure System Laboratory

情報セキュリティ大学院大学
学長 教授 田中 英彦

本研究所では、拡大・多様化するIT技術の恩恵を、多くの人々が安心して享受できるようなセキュアな社会を実現するため、様々な分野の専門家の協力を得て、セキュリティに関する研究活動を行っています。
2012年度より、後藤厚宏教授が研究所長を務め、研究スタッフには、情報セキュリティに関する技術、経営、法律、倫理等のスペシャリストを、学界、実業界から招聘して、将来の社会インフラを支える セキュアシステムに向けた研究開発を強く推進していきます。

所長 後藤 厚宏

■ セキュアシステム研究所のプロジェクト

2014年度より、セキュアシステム研究所は、次の５つのプロジェクトにて研究開発活動、調査研究活動を進めています。

❶サイバーセキュリティ (CS : Cyber Security)プロジェクト

新たな(未知の)セキュリティ脅威への対応するために、サイバーセキュリティの様々な情報収集・分析・交換を通して信頼できる社会基盤作りへの貢献を目指します。具体的には、次の４つの活動を進めます。

- 情報収集のための新技術の研究を行い、それを用いた独自の情報収集を進めます。
- 産官学のセキュリティエキスパートが寄合所(“Cyber security meet up”)としての人的な交流の場を作ります。
- 信頼関係に基づくセキュリティ情報の交換(“Trusted” Cyber Security Information eXchange : TSIX)を運営します。
- 最新セキュリティ技術の評価検証を行います。

❷セキュリティ国際標準化 (IS: International Standardization)プロジェクト

セキュリティ分野の国際標準化の推進戦略の立案と提言を進めます。また、国際標準化を担う次世代人材を育成することによって、我が国のセキュリティ技術による国際標準化に貢献します。

❸セキュリティ人材キャリア開発 (HR: Human Resource)プロジェクト

セキュリティ人材のキャリアデベロップメントに関わる調査・提言を進めます。そのために、日本ネットワークセキュリティ協会(JNSA)や情報セキュリティ教育事業者連絡会(ISEPA)など、セキュリティ人材育成の関係機関と連携を密にします。

❹Internetと通信の秘密 (SC: Security in Communications)プロジェクト

ビッグデータ時代のプライバシー、通信の秘密の在り方と法制度、通信キャリアやクラウドプロバイダーの役割など、通信の秘密とプライバシーに関する調査・提言を進めます。

❺航空制御システム (AC: Aviation Control Systems)プロジェクト

航空業界の専門家と情報セキュリティの専門家が密に議論する研究会活動を通じて、航空制御のセキュリティ課題について調査研究と提言活動を進めます。

■ Messages

客員研究員を代表してお二方からメッセージをいただきました。

岩井 博樹

デロイト トーマツ サイバーセキュリティ先端研究所
主任研究員

セキュア構築、侵入検知システムの導入設計、セキュリティ監視業務等を経てデジタルフォレンジック業務に携わる。サイバー攻撃被害の解析や訴訟事件等のデジタル鑑定解析、セキュリティ対策評価等を担当。
著作として「標的型攻撃セキュリティガイド」等がある。

今や世界中でサイバー攻撃被害が相次いでおり、その被害は一個人から国家レベルまで様々です。その影響範囲は国益にも影響をおよぼしつつあります。このような状況に対抗するため、現在国内ではサイバーセキュリティの専門家の育成が急務となっています。特にインシデント解析のジャンルは、攻撃者の手の内を知る上で重要な技術であるため大変注目されています。
今後、サイバー攻撃は世界中のサイバー攻撃者により個人～国家レベルまで益々増大することが予測されます。これらの脅威に対し、一緒に戦っていける仲間を一人でも増やしていきたいと思います。

名和 利男

サイバーディフェンス研究所
専務理事／上級分析官

航空自衛隊プログラム管理隊における防空システム管理業務やJPCERT/CCにおける早期警戒の実務経験をベースに、CSIRT構築・運用やサイバー演習の支援などに従事しています。最近は、サイバーインテリジェンスに注力しています。

今や情報セキュテリィは公共施策やビジネスにおいて必須のものとなっているにもかかわらず、急激かつ高度に変化する情報セキュリティの動向をキャッチアップすることは並大抵のことではありません。しかし、攻撃する側が機械ではなく人間であることに注目し、彼らの行動や置かれている状況を把握及び理解することにより、本質的な攻撃特性を見出すことが可能となります。
そこで、さまざまな環境下で情報セキュリティにかかる対処能力を発揮することを求められる方々と、最近の事例の内情や対処の実態を積極的に共有及び議論させていただきながら、防御側全体の対処能力の向上を実現させていきたいと思っています。

沿革

- 2004 ●開学(情報セキュリティ研究科修士課程[2年制])
- 2005 ●表彰事業として「情報セキュリティ文化賞」を創設
- 2006 ●修士課程第1期生輩出
  ●博士後期課程設置。博士前期(修士)課程に1年制プログラムを設置
  ●大学附置研究所として、セキュア社会システム研究所(現 セキュアシステム研究所)を開設
  ●研究開発プロジェクト『企業における情報セキュリティの実効性あるガバナンス制度のあり方』が平成18年度社会技術研究開発事業研究開発プログラム「ユビキタス社会のガバナンス」に採択
- 2007 ●産学連携教育プロジェクト『研究と実務融合による高度情報セキュリティ人材育成プログラム(ISSスクエア)』が文部科学省「平成19年度先導的IT スペシャリスト育成推進プログラム」に採択
  ●平成19年度情報化月間情報化促進貢献企業等表彰において経済産業大臣表彰「情報セキュリティ促進部門」を受賞
  ●博士後期課程より第1号の博士学位取得者を輩出
- 2008 ●博士前期(修士)課程2年制プログラムに4コース制を導入
- 2009 ●『研究と実務融合による高度情報セキュリティ人材育成プログラム(ISSスクエア)』第1期認定証取得者を輩出
- 2010 ●2010年日本APEC首脳会議(横浜開催)にかかるサイバーテロ対策活動協力に対し、神奈川県警察本部より感謝状を受領
- 2011 ●研究プロジェクト「暗号技術の導入による機密情報の適切な保護方式の研究～グローバル社会における持続的な経済発展のための基盤技術として～」が文部科学省「平成23年度私立大学戦略的研究基盤形成支援事業」に採択
- 2012 ●15大学連携による共同申請取組『分野・地域を越えた実践的情報教育協働NW』が文部科学省「平成24年度情報技術人材育成のための実践教育ネットワーク形成事業」に選定
- 2013 ●セキュアシステム研究所をリニューアル
- 2014 ●開学10周年

ホームカミングパーティ

新入生歓迎パーティ

1Fホールでのweekday tea-time

ゼミ合宿

情報セキュリティ大学院大学が位置する神奈川県横浜市は、国際観光都市としてはもちろんのこと、新たな産業、ビジネス、文化、芸術の受発信拠点として日々進化しつづけています。本学のキャンパスは横浜駅きた西口徒歩1分の好立地にあり、多彩な商業施設が集積するこのエリアは、発展著しいみなとみらい21地区に隣接しています。

■Contents

UNIVERSITY
ACCREDITED
2010.4〜2017.3

■学生募集課程概要

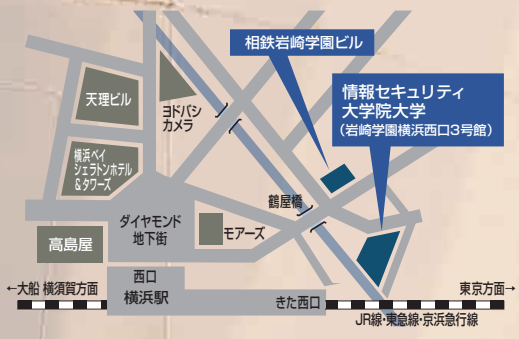
研究科	専攻	課程	標準修業年限	募集人員
情報セキュリティ研究科	情報セキュリティ専攻	博士前期（修士）課程［2年制］	2年	40名
		博士前期（修士）課程［1年制］	1年	若干名
		博士後期課程	3年	8名

詳細は本学ウェブサイトでご確認ください。

■入学者選考方法

博士前期（修士）課程［2年制］	一般入試	面接（プレゼンテーションを含む）および志望理由書、学業成績、小論文等出願書類審査を総合して行う
	社会人入試	面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士前期（修士）課程［1年制］		面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士後期課程		口述試験（プレゼンテーションを含む）および研究計画書等出願書類審査によって、研究能力を総合的に判定する

学生募集要項、入学願書等は本学ウェブサイトよりダウンロードできます。また、大学院説明会、オープンキャンパス等の入試イベントについての情報も随時ウェブサイト上でご案内していますので、あわせてご覧ください。



（横浜駅きた西口より徒歩1分）

都内主要ターミナル駅からも好アクセス

○東京〜横浜　JR東海道本線　24分
○品川〜横浜　京浜急行快速特急（快特）　17分
○新宿〜横浜　JR湘南新宿ライン（横須賀線）　32分
○渋谷〜横浜　東急東横線・みなとみらい線（特急）　26分

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
http://www.iisec.ac.jp/
〒221-0835　神奈川県横浜市神奈川区鶴屋町2-14-1　お問い合わせ先　045-311-7784　iisec@iwasaki.ac.jp
学校法人 岩崎学園