明日の信頼を創ろう。

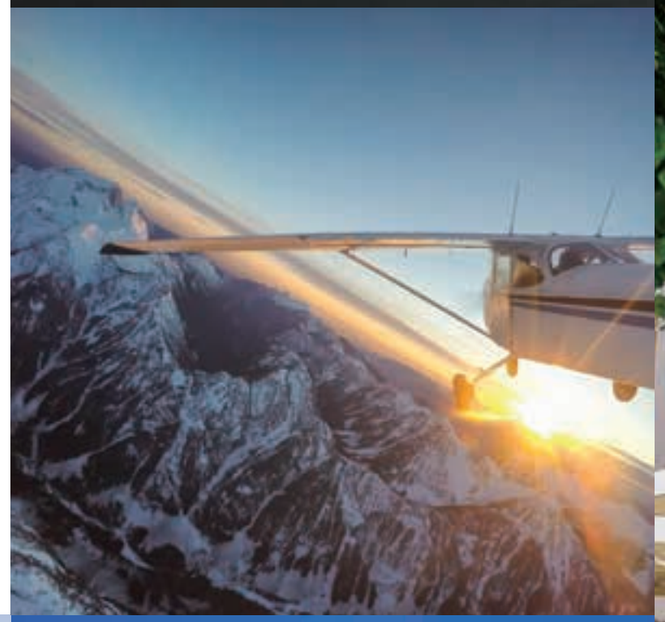
情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

抜粋版

2019-2020

リアルとサイバーが融合し、
想像を超えたイノベーションが加速する。
共有する未来には、
情報セキュリティの力が必要だ。



新たな技術でリアルとサイバーの垣根が取り除かれ、世界中の人々が豊かな暮らし、環境、未来を共有する社会の実現へ。そのためにはインフラの安全性・信頼性の確保からサイバー攻撃への対応までさまざまな領域で情報セキュリティの力が必要です。2020年に行われる東京オリンピック・パラリンピック、2025年に予定される大阪の日本国際博覧会など、これからの日本は国際的なイベント開催が続き、サイバー攻撃に備える社会づくりや人材育成において世界的に注目される時期ともいえます。

2004年に開学したIISEC（情報セキュリティ大学院大学）では、こうした情報セキュリティの重要性に早くから着目し、高い専門性を持つ人材育成を目的に教育・研究を進めてきました。修了生は博士前期・博士後期合計で400名を超え、企業や省庁など社会の各分野で活躍中です。しかもこの人脈を在学時から生かすため、IISECの学生は入学直後に同窓会にも入会し、修了生と活発に交流しています。

さらに文理融合の学問体系と、実務経験・指導経験が豊富な教員を中心に、実践力を養う教育・研究指導も大きな特色。多様な科目を選ぶ指針となるよう4つのコースフレームを設定し、専門性や将来の目標に合う学習設計を容易にする一方、興味に応じてコース間の自在な履修も可能な柔軟なカリキュラムです。このような先進的な教育により、国際都市・横浜から世界の情報セキュリティを担う人材を育てていきます。

CHANGE MY LIFE 大学院でこう変わった［新入生編］

稲葉 啓太さん

高校生に情報リテラシーを教えられる教師になるため専門知識を磨いています。

情報セキュリティ研究科 博士前期課程1年

國學院大學経済学部卒業

時限	月	火	水	木	金	土	日
1	アルバイト	自宅学習	アルバイト	自宅学習	アルバイト		勉強もアルバイトもしない完全オフ日で、気持ちを切り替え
2		プログラミング		リスクマネジメント		早めに来て予習	
3		オペレーティングシステム		統計的方法論		情報セキュリティ技術演習I	
4		セキュアシステム構成論		マスメディアとリスク管理			
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	研究指導	インターネットテクノロジ	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	帰宅	
α	21:30に終わってそのまま帰宅。講義の復習は翌朝早くから始めることが多い						

授業時間	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	—
α	22:00 ～ 24:00	18:00 ～ 24:00

1>横浜駅近くで、通学に便利なこともIISECを選んだポイント。 2>指導教員の稲葉先生の授業「統計的方法論」では、研究の推進に必要なデータ処理・分析手法を学んでいます。 3> 4時限と5時限の間は1階ラウンジでティータイム。セキュリティ業界で働く先輩・同級生から、ざっくばらんな話が聞けます。 4>学校で中高生の個人情報をどう扱っているかというテーマの先行研究を調査。

◉セキュリティには法律や心理学が重要と聞いて入学を決意

大学の経済ネットワーキング学科で、IT活用や情報ネットワークの面白さを知り、それを高校生に伝えたくて情報科教員を目指しました。しかし学部卒では知識・経験が足りないと考えてIISECへの進学を検討。情報を適切に扱って得られるメリットと不十分な知識がもたらすリスクが専門的に学べ、社会人学生とも交流できる点が魅力でした。

とはいえ文系出身でも数理関係の科目は大丈夫なのだろうかと不安に思い、入学前の大学院説明会には2度参加。特に2度目は情報セキュリティや安全に関する教育が専門の稲葉緑先生の模擬講義で、「情報セキュリティは技術と法律と心理学が重要」と聞き、学ぶ分野の幅広さに興味を持って入学を決意しました。

◉高校生の情報リテラシー向上に役立つ科目を念頭に履修

私が高校の情報科で、生徒に身につけてほしいと考えるのが情報リテラシー。IISECではリスク分析や対策のマネジメントを目的とした「セキュリティ／リスクマネジメントコース」が近いと考え、このコースに沿って科目を選択しています。ビジネスモデル特許をはじめ知的財産の現状を知る「知的財産制度」のほか、「インターネットテクノロジ」「情報デバイス技術」など私にとって未知の分野が学べる科目も充実しています。

私の1週間

◉社会人学生と親密に話せる「ティータイム」は貴重な時間

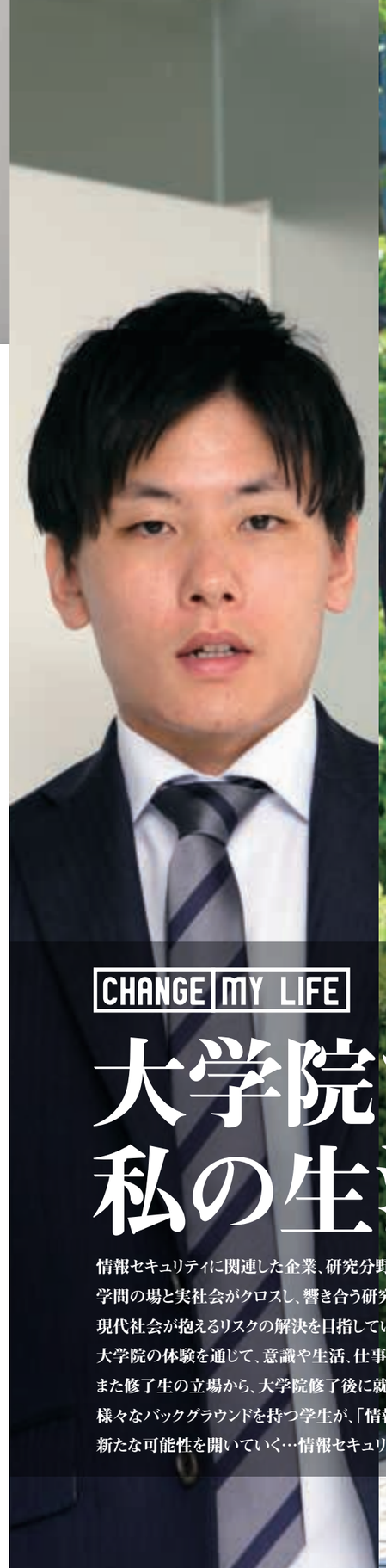
土曜日を除いて2時限から5時限からに分かれ、5時限からの日は講義までアルバイトに従事。ただ後期からは履修科目が少し増えて日中の空き時間が減るので、教員免許を生かして市内の学校での非常勤勤務も考えています。

4時限と5時限の間は1階ラウンジに希望者が集まり、さまざまな話題で語り合う「ティータイム」。今のセキュリティ業界の動向など、教室での会話よりくだけた裏話的な話も聞けるので、より深い知識と広い視野を持つ教師になれるよう積極的に参加したいと思います。

◉私たちとは情報の捉え方が異なる高校生に必要なセキュリティ教育

火曜日5・6時限は指導教員の稲葉先生の研究室で研究指導。私のテーマは「中学校・高校の生徒への効果的なセキュリティ教育」と「学校自体の情報セキュリティの向上」で、稲葉先生のアドバイスも参考にまとめていく予定です。

私たちの世代が「情報は探して利用する」と考えるのに対し、現在の中高生はTikTokの人気で分かるように「情報は発信してコミュニケーションするもの」と感じているのでしょう。そうしたギャップを前提とした心理学的アプローチも含め、個人情報の適切な扱いなどのセキュリティ教育を研究したいと思います。



CHANGE MY LIFE

大学院でこう変わった。私の生活、私の仕事。

情報セキュリティに関連した企業、研究分野の第一線で活躍する教授陣。社会人が約8割という学生たち。当事者意識にもとづく白熱した討論…。
学問の場と実社会がクロスし、響き合う研究体験。この大学院大学には、他の大学院では得られない、特別な2年間が待っています。
現代社会が抱えるリスクの解決を目指している方。未知の分野で知的興奮を実感している方。企業が求める実力を身につけた先輩。
大学院の体験を通じて、意識や生活、仕事への考え方がどう変わったか、それぞれの1週間の予定とあわせてご紹介します。
また修了生の立場から、大学院修了後に就職した仕事の内容や、「仕事に役立つ大学院での学び方」のアドバイスを掲載。
様々なバックグラウンドを持つ学生が、「情報セキュリティ」を軸に幅広い分野を網羅するカリキュラムで学び、研究を続け、
新たな可能性を開いていく…情報セキュリティ大学院大学の魅力を、在学生、修了生の変化を通じてご確認ください。

CHANGE MY LIFE 大学院でこう変わった［新入生編］

鈴木 優一さん

外部のクラウドサービスまで考慮したセキュリティを実現できる人材を目指す。

情報セキュリティ研究科 博士前期課程1年

さくら情報システム株式会社
業界も専門分野も異なる教員・学生が、セキュリティをテーマに、
それぞれの切り口で講義や研究を行う点にもひかれてIISECに入学。

時限	月	火	水	木	金	土	日
1	土曜日の受講が勤務扱いとなるため、月曜日は原則振替休日。朝夕の子どもの送り迎えのほか、講義の予習・復習のため図書館などに行くことも（業務の都合で出社もあり）	業務	業務	業務	業務	個人識別とプライバシー保護	日曜日は家族と一緒に過ごせる貴重な日。妻と分担して家事を終わらせる。その他、プライベートの時間（趣味、食事会など）
2						院生室で文献等を調べる	
3		オペレーティングシステム				情報セキュリティ技術演習I	
4		セキュアシステム構成論		マスメディアとリスク管理			
5		研究指導	情報セキュリティ輪講I	セキュリティ経営とガバナンス			
6		研究指導	インターネットテクノロジ	ネットワークシステム設計・運用管理	帰宅	帰宅	
α		帰宅	帰宅	帰宅			

授業時間	月曜日～金曜日	土曜日		月曜日～金曜日	土曜日
1時限	9:00～10:30	9:00～10:30	5時限	18:20～19:50	16:20～17:50
2時限	10:40～12:10	10:40～12:10	6時限	20:00～21:30	—
3時限	13:00～14:30	13:00～14:30	α	22:00～24:00	18:00～24:00
4時限	14:40～16:10	14:40～16:10			


1


2


3


4

1>指導教員の藤本先生に研究テーマを絞り込む方向性を相談。2>講義の空き時間や終了後は落ち着いて勉強できる院生室に。先輩が質問に答えてくれます。3>毎週火曜日の5・6時限は研究指導で、現在は先輩方が研究の進捗を発表。4>図書室にはセキュリティ関連の文献もそろうので便利。

◉顧客ニーズに応えるためセキュリティの知識を養う

私は三井住友銀行の子会社であるさくら情報システムのデータセンターで、オープン系システムを中心としたサーバー運用のほか、お客様のシステムの構築・設計なども担当してきました。

当社のデータセンターはISMSやプライバシーマーク等を取得し、セキュリティ強化を図っていますが、近年増えているのが「クラウドサービスの利用も検討したい」というご希望です。これに応えるには、セキュリティに関する幅広い知識や概念をもとに、製品・サービスの導入を提案できる人材が必要と危機感を持っていたとき、上司にIISECで学ぶことを勧められて入学を決めました。

◉クラウドサービスをより安全に提供するための実装指針を検討

現在は技術系の科目に加えマネジメントや法律に関する科目も幅広く履修し、企業経営におけるセキュリティの重要性を痛感しています。研究テーマはクラウドサービスのセキュリティ関連を扱う予定で、上流工程で安心・安全に使えるクラウドサービスを提供するための枠組み、実装指針の確立を目指しています。

実は入学と同時に、新製品・サービス創出などを主導する技術開発部に異動したのですが、開発とセキュリティとは密接な関係にあり、IISECでの経験をさらに広く生かせると期待しています。

私の1週間

◉経営学や心理学などの視点でセキュリティを考える講義が新鮮

5・6時限と土曜日の講義を中心に、研究指導のある火曜日などは午後から受講し、業務が重なる金曜日は終日社内に。月曜日は振替休日ですが、勉強のため図書館などに行くことも多いですね。

データセンターの運用が主務だったので、「オペレーティングシステム」「インターネットテクノロジ」などは経験で得た知識を体系的に整理しつつ、より深く学べる科目。逆に企業経営を考える「セキュリティ経営とガバナンス」は非常に新鮮で、組織の中でどうセキュリティを実現していくかの参考になります。

また「情報セキュリティ輪講」は各自が発表する最近の技術動向や社会制度などをもとに討議。知識が広がると同時に、調査や研究の進め方なども学べます。

◉経営の視点からのアドバイスで思考の幅が広がっていく

指導教員の藤本先生はリスクマネジメントなど経営の視点からセキュリティを見てきた方。現場の経験から考える私とは異なる視点から助言をいただけ、思考の幅が広がります。社内のセキュリティ人材不足に危機感を抱き、自分がそのロールモデルを目指そうと考えたことも入学目的の一つなので、研究テーマを絞って論文を書くだけでなく、多様な科目を学んで知識を広げ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）／AIと機械学習（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）
情報セキュリティ技術演習Ⅰ（2単位）
研究指導（6単位）＜必修＞

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）／サイバーセキュリティ技術論（2単位）／情報システム構成論（2単位）
情報セキュリティ技術演習Ⅰ（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）＜必修＞

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）／情報セキュリティ技術演習Ⅰ（2単位）／アルゴリズム基礎（2単位）
研究指導（6単位）＜必修＞

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）
セキュリティ経営とガバナンス（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）
情報セキュリティ技術演習Ⅰ（2単位）／サイバーセキュリティ技術論（2単位）
研究指導（6単位）＜必修＞

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	○			
	AIと機械学習	選択	2	○			
	実践的IoTセキュリティ	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	○	○	○	
	サイバーセキュリティ技術論	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	○		○	
	情報セキュリティ技術演習Ⅰ	選択	2	○	○	○	○
	情報セキュリティ技術演習Ⅱ	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				○
	セキュリティ経営とガバナンス	選択	2		○		○
	リスクマネジメント	選択	2		○		○
	情報セキュリティ心理学	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。

■ 他大学院等との交流協定

2019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

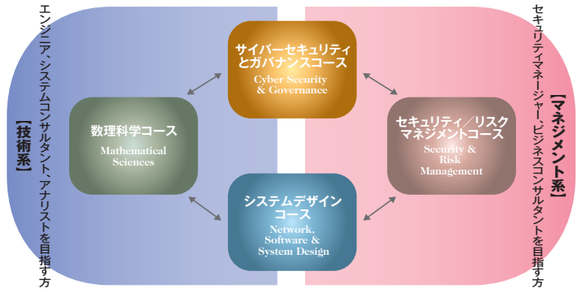
情報セキュリティ研究科
博士前期・博士後期

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。

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、技術系・マネジメント系とも幅広い人材育成需要、教育需要に応えるため、4つのコースフレームを2016年10月にリニューアルしました。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。

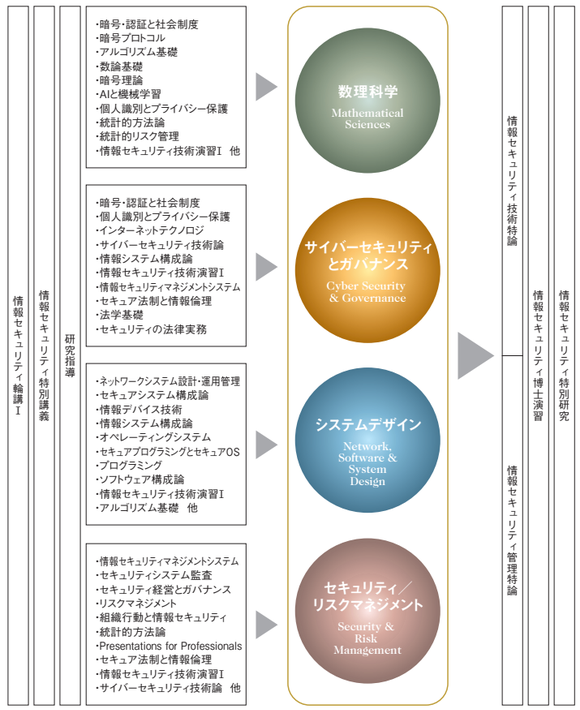
■ 博士前期課程4コース



＜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

博士前期課程（修士課程）　博士後期課程



■ 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）

（※2020年度より、選択科目の一部を改訂する予定です）

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			
	AIと機械学習	選択	2			
	実践的IoTセキュリティ	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			
	サイバーセキュリティ技術論	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			
	情報セキュリティ技術演習Ⅰ	選択	2			
	情報セキュリティ技術演習Ⅱ	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			
	セキュリティ経営とガバナンス	選択	2			
	リスクマネジメント	選択	2			
	情報セキュリティ心理学	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			
	情報セキュリティ博士演習	必修	2	—	—	8
	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
2019

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。

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
本講義では、暗号・認証に関しその技術的要点を全般的に把握し、それら暗号・認証技術が現代社会においてどのような場面でどのような役割をになっているか、制度面の課題は何かについて学ぶ。加えて、暗号・認証技術の新しい展開を概観し、将来の暗号・認証のあるべき姿について考察する。社会科学系の学生および暗号・認証の実社会における応用について知見を深めたい技術系の学生を対象とする。数学的および情報科学的な予備知識はなるべくその都度説明する。

■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。

■AIと機械学習
本講義では、情報セキュリティへの応用も活発化しているAIと機械学習の理論について学ぶ。講義は3つの部分に分かれている。最初の3回はAI技術の全体像を概観し、続く7回はC.M. Bishop著「パターン認識と機械学習」を教科書として機械学習の基礎理論を学ぶ。後半の5回はIan Goodfellow他著の「Deep Learning」を参考書として最近の深層学習の話題を取り上げ、最終回の演習では学生が独自に実験した内容を発表する。

■セキュアシステム構成論
情報通信技術（ICT）の普及により、あらゆる場所で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。

■セキュアプログラミングとセキュアOS
サイバー攻撃に対して脆弱なソフトウェアシステムが社会の隅々にまで浸透し、社会全体に大きな負の影響を与えるようになっている。本科目では、攻撃に強くセキュアなソフトウェアを構築・運用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を行う。そして、完璧な防御方法はないことを前提に、ソフトウェアシステムの出入口での対策、一部に問題が発生した場合の影響範囲の局所化、最小権限の原則にしたがったアクセス制御、アクセス主体の管理などの手法とこれらの組み合わせに基づく考え方を解説する。

■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。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言語プログラミングの実習を行う。

■実践的IoTセキュリティ
本講義では、IoTのビジョンから始めて、IoTデバイスとIoTネットワークのそれぞれにおけるセキュリティの脅威と対策の方法を学ぶ。特に、一般のPC系のITにはない、組み込み・制御・ハードウェアなどのセキュリティの脅威を予測し、安全なシステムやサービスを設計・開発する方法、その安全性を検証し、長期間安全に運用する方法を学ぶ。IoTデバイスを実際に操作して暗号通信を行う演習、スマートホームの模擬環境に対する脅威分析と脆弱性検査の演習によって、IoTセキュリティを体得する。IoTセキュリティの実像に迫るため、IoTの実態に詳しい専門家による授業も加える。

■セキュリティシステム監査
本授業では、セキュリティ管理が適切に機能しているかどうかを第三者の立場で評価・検証する場合の考え方と具体的な方法論を学習する。セキュリティ管理では、経営層の積極的な関与のもと、組織全体としての対応が求められることから、そのような視点を重視して授業を進める。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」の目線で、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。

■情報セキュリティ心理学
本科目では、「人間の行動は個人と周囲との相互作用から決定づけられる」という心理学の観点から情報セキュリティに関連する問題について解説する。具体的には、セキュリティに関する不適切な判断や行動を人間が選択するメカニズムを中心に説明する。また、このような問題への対策の考案に役立つ心理学の知見を紹介する。

■統計的方法論
本科目では、研究上の問いを科学的に、かつ、効率的に検証することを可能とする統計的手法の基礎的な知識・技術について講義する。研究上の問いに対する答えを導くための実験・調査での結果を予測するには、収集するデータやその分析方法に関する知識が必須である。授業の各回では、各統計手法に関する知識を説明した後、統計ソフトであるSPSSを使いながら情報セキュリティの研究を題材にした仮想のデータを処理・分析する方法を学ぶ。

■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。

■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!

TOPICS

2020年度新規開講予定科目

■不確実性下の意思決定
本科目では、リスク含む「不確実性」の下での意思決定について、大きく次の３つの内容を取り扱う。①A.Waldの「統計的決定関数」に基づく意思決定論におけるベイズ解（この場合の不確実性の源泉は自然環境などの変動）、②複数のプレーヤーによって行われるゲーム（この場合の不確実性の源泉は利害の対立する相手の行動）、③期待効用最大化行動に関する心理学からの批判としてのkahneman&Tveskyのプロスペクト理論と行動経済学。

■ネットワーク設計とセキュリティ運用
ネットワークの設計とそのセキュリティ運用は社会や企業活動にとってサイバーセキュリティ確保の要である。本科目では、ネットワーク設計を支える理論（待ち行列、トラヒック、グラフ、信頼性等）、企業ネットワークや公衆ネットワークの主要な構造とネットワーク制御（輻輳制御、迂回制御等）、およびネットワークのセキュリティ制御（IDS/IPS、FW、UTM等）、さらに新時代のネットワーク（5G、IoT用、仮想ネットワーク等）の動向について学ぶ。

■リスクマネジメントと情報セキュリティ
本科目では、リスクマネジメントに関する基礎として、リスクやリスクマネジメントの定義、リスク処理のさまざまな手段、リスクマネジメントのプロセスについて学習する。また、情報セキュリティマネジメントについて、組織における情報セキュリティのリスクを管理するのに必要な管理体制（マネジメントの仕組み）や、リスクを低減するためのコントロール（管理策）について講義する。リスクマネジメントと情報セキュリティマネジメントの関係について理解し、組織における実践的取り組みへと展開する能力の習得を目指す。

博士前期課程
（修士課程）

授業科目履修例
2019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8日～8月3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		オペレーティングシステム		統計的方法論	数論基礎	情報セキュリティ技術演習Ⅰ
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		
5	AIと機械学習	（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	ソフトウェア構成論	（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10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				
3	（研究指導）	リスクの経済学		情報セキュリティ心理学		サイバーセキュリティ技術論（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	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	実践的IoTセキュリティ or 特講（サイバー・インテリジェンス）	Presentations for Professionals	
6	特講（ブロックチェーン理論）	（研究指導）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B or セキュア法制と情報倫理	国際標準とガイドライン	

▼＜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8日～8月3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		オペレーティングシステム		統計的方法論	数論基礎	情報セキュリティ技術演習Ⅰ
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		
5	知的財産制度 or AIと機械学習	（研究指導）	情報セキュリティ輪講Ⅰ	セキュリティ経営とガバナンス	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	（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10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				
3	（研究指導）	リスクの経済学		情報セキュリティ心理学		サイバーセキュリティ技術論（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	実践的IoTセキュリティ or 特講（サイバー・インテリジェンス）	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	セキュアシステム構成論B or セキュア法制と情報倫理	国際標準とガイドライン	

■ 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、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、セキュアシステム、セキュアOS、マルウェア分類／検知／対策、攻撃検知／解析、人工知能セキュリティ、仮想化環境、組み込みソフト、制御システム、車載システム、ロボット、ハードウェアセキュリティ、セーフティ設計 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

本コースでは、情報セキュリティリスクを特定し、適切な対応を取るための専門的な知識とそれを基盤とした応用力を身につけ、時には大胆な見直しを経営層に提言したり、自ら率先して組織を動かすリーダーとして活動する人材の育成を目標としています。情報を適切に活用することと同じように、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できる人材であること。そのため、リスク分析や対策のマネジメントのみならず、人間の心理や行動を理解し、セキュリティ行動を後押ししたり、効果の高い教育を構築・実践する方法を開発するなど、幅広い分野について学習していきます。企業・組織等で、リスクマネジメントやガバナンス、人材育成や教育研修、新規事業開発、情報通信技術の利活用、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、基礎知識とそれを応用し実践に生かす能力を身につけていただきます。

研究キーワード：リスクマネジメント、ガバナンス、セキュリティ行動と心理、リスク学習プログラム、セキュリティ行動規範作成、リスク分析、リスク戦略、リスク評価、ISMS、BCP/BCM、組織行動、レビュテーションコントロール、セキュリティ教育 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考察しながら作成します。

コースリーダーからのメッセージ

藤本 正代 教授
Masayo FUJIMOTO

外部からのサイバー攻撃や内部犯罪など、あらゆる組織において多様化し複雑化している情報セキュリティリスクといかに向き合うかが、経営の重要課題になっています。さらに、近年はAI、IoT、5Gなど、情報通信技術の進展がめざましく、社会経済活動が大きく変化する時代に差し掛かっています。どのような組織も、それらを積極的に活用し、リスクを取って新たな挑戦をしなければ生き残ることは難しいでしょう。そのためには、経営の重要課題の一つとして情報セキュリティ戦略を位置づけ、必要な知識を習得し応用展開することが成長戦略の鍵になると考えています。

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

ISSスクエア 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

ISSスクエア＋enPiT-Security 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（成長分野を支える情報技術人材の育成拠点の形成）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卒業生の声

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！

星 智恵｜情報セキュリティ大学院大学客員講師
株式会社豆蔵　IT戦略支援事業部
（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200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/

成長分野を支える情報技術人材の育成拠点の形成 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す。2017年4月からは大学院生向け成長分野を支える情報技術人材の育成拠点の形成（enPiT 1）として自主展開を図っており、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
2018-2019

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

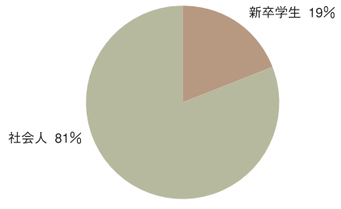
■ 社会人学生の所属組織

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】(2018-2019実績)
インフォシスリミテッド／エヌ・ティ・ティ・コミュニケーションズ(株)／エヌ・ティ・ティ・コムウェア(株)／NTTテクノクロス(株)／LM総合法律事務所／海上保安庁／外務省／神奈川県警察／(株)エヌ・ティ・ティ・エムイー／(株)小野測器／(株)協和エクシオ／(株)センチュリーインフォテック／(株)JR東日本情報システム／(株)タツノ／(株)東陽テクニカ／(株)日立システムズ／(株)Beyond Soft Japan／(株)富士通ソフトウェアテクノロジーズ／(株)本田技術研究所／(株)ミライト・テクノロジーズ／金融庁／警察庁／警視庁／埼玉県警察／埼玉県／さくら情報システム(株)／CsSoft(株)／ジェイアール東海情報システム(株)／昭和シェルビジネス&ITソリューションズ(株)／第一生命保険(株)／(独)日本学術振興会／(独)国立印刷局／日本コムシス(株)／日本電気(株)／日本電気計器検定所／東日本旅客鉄道(株)／日立キャピタル(株)／防衛省／横浜市役所／楽天(株)／陸上自衛隊　など

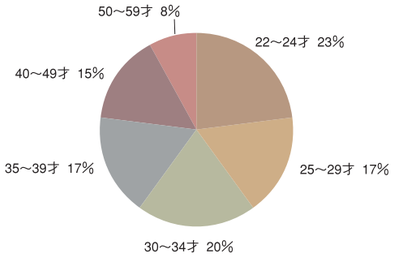
■ 現況

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。



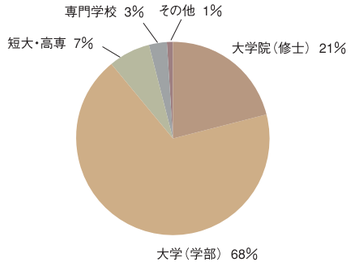
■ 年齢構成(入学時)

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、業務実績を有する研究者、技術者、実務家も在学中です。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】(2018-2019実績)
(学)昭和女子大学／(株)アーク情報システム／(株)サーバーワークス／(株)富士通研究所／(株)三井住友銀行／合同会社ゼロワン研究所／日本オラクル(株)／パナソニック(株)／東日本電信電話(株)／三菱ケミカルシステム(株)　など

博士前期課程
(修士課程)

在学生
インタビュー

入学して実感した大学院の魅力…研究の充実感、教員や学生同士の交流、
自分自身が成長した点など、それぞれの立場から語っていただきました。

多様なサイバー攻撃で選挙に干渉することを狙う
デジタルゲリマンダーへの対処を提言。

長迫智子さん
Tomoko NAGASAKO
独立行政法人 日本学術振興会
博士前期課程2年

インテリジェンスの専門家からも学べる
私は幼少期にニュースで見た事件の衝撃から国の安全保障の重要性を認識し、そうした仕事に就くことを目標にしてきました。リアルな空間からサイバー空間に安全保障の領域が広がる中、必要な知識を身につけたいと考えてIISECに入学。インテリジェンスの現場で働く専門家の講義では最前線のお話を聞くことができてとても勉強になりました。そして、インシデント対応、脆弱性検査、不正侵入等を体験する技術系の実習などは、私のような人文系出身の人間でも、基礎から理解できるように非常に丁寧にカリキュラムが組まれており、先生にも親身にご指導いただけたので安心して演習に取り組め、実際の技術を体得できて非常に面白かったです。

国際法で裁けない海外からのサイバー攻撃
修士論文は湯淺先生の指導のもと、サイバー攻撃による選挙干渉で特定の候補者を優位または不利にすることを狙う「デジタルゲリマンダー」をテーマに執筆中。選挙の公的な報告書や新聞記事などをもとに各国が受けたサイバー攻撃の事例を研究し、日本での対応を検討しています。海外からのサイバー攻撃でも、選挙情報への不正アクセスやリーク、フェイクニュースの拡散程度では干渉行為と見なされず、現状では、国際法での対処は難しいと見られます。このため論文では、SNSやフェイクニュース規制等の事前策と、不正な資金の流れから攻撃実行者と指示関係にある国家機関の関係を実証し制裁を与える事後策という、各国でとられている対策を両輪として検討しつつ、加えて、アトリビューション能力の強化と官庁の縦割りによるサイバー戦略への弊害を克服するため、サイバーインテリジェンスに総合的に対処するサイバーセキュリティ庁の創設を一案として考えています。

研究内容や将来の進路を業界人脈が支援
またIISECは多様なバックグラウンドの学生が在籍し、加えて在学中から同窓会に入り、社会で活躍する卒業生とも交流が深まるのも特色。私の研究についても、関係機関の方や関連分野の研究者の方からご意見、ご助言をいただいたり、研究テーマに密接な研究会やセミナーをご紹介いただいたりと、人脈面でも多くのご助力をいただきました。将来のために思い切ってIISECに入学して、一気に世界が開けたように感じます。そして最後には、先生、在学生、卒業生の人脈を通じて昔からの目標をかなえたいですね。

家庭でも活躍するロボットやIoTの開発に必須の
ミドルウェア。そのセキュリティについて研究中。

亘理克好さん
Katsuyoshi WATARI
本田技研工業株式会社
博士前期課程2年

ますます身近になるロボットに必要なセキュリティ
本田技研工業には長年のロボティクス研究の実績があり、近年は自律制御型やIoTをはじめ、家庭や街中で利用される機器が市場にみられるようになっています。それと同時に、人や物を傷つけない、情報漏えいを起こさない、乗っ取りの危険を回避できるなど、セキュリティの担保が大きな課題となってきています。国際規格や法の整備が十分でない中、まずセキュリティの全体像を学びたいと考えた私は、上司の勧めでIISECに入学。「セキュリティ・バイ・デザイン」の考えにひかれ、大久保先生の研究室を選びました。

セキュリティが強化されたミドルウェアの注意点
設計段階からセキュリティを組み込んだ開発を行うのがセキュリティ・バイ・デザインで、私はロボティクス開発で一般的に使われるミドルウェアを、この視点から研究しています。ミドルウェアは少し前にセキュリティ対応の仕様が公開され、プログラム同士の通信にもセキュアな方式が採用されたため、現在はその脆弱性の有無や通信速度などを検証。暗号化した通信は暗号化しない場合に比べて最大1/2の速度に落ちるため、即時のレスポンスが必要な状況には注意が必要と分かりました。今後は自社の開発でも設計段階からセキュリティを組み込むよう求め、周囲の部署や全社的にも広げたいと考えています。

社内のセキュリティ意識を高める旗振り役に
当社でも全社的にセキュリティを重視し、従業員対象の勉強会などは開かれていますが、業務直結の内容や顕在化したリスクへの対応に偏りがちです。しかしIISECで学んで、セキュリティは技術からマネジメントまで含む広範な分野だと実感。セキュリティ業界にいる先生方や学生、あるいは官公庁などからの得た最新の知見も踏まえ、社内のセキュリティ意識向上の旗振り役も担うようになりたいですね。

博士後期課程

在学生&修了生
インタビュー

博士後期課程には、博士前期（修士）課程で研究の魅力に目覚めた進学者から
学界・産業界で相当の業績を有する研究者・専門技術者まで幅広く在籍しています。
博士後期課程進学を目指したきっかけ、そして修了した感想は？
在学生と修了生にそれぞれの思いを語っていただきました。

CSIRTのインシデント対応を効果的・効率的に行うため、2つの技術を博士論文で提案。

Hiroki HADA　羽田大樹さん
情報セキュリティ研究科 博士後期課程修了
（NTTセキュリティ・ジャパン株式会社）

博士前期課程で開発した手法とは異なる視点から行うマルウェア解析

IISECの博士前期課程で学ぶ中で、実務に役立つ知見が得られたと同時に、よりアカデミックな研究にも興味がわき、博士後期課程に入学しました。研究テーマは修士論文でも扱ったマルウェアの静的解析で、以前に研究していた「既存のツールを利用したバイナリ比較」の弱点を克服するため、その機能に該当する関数がどこにあるのか、解析済みのマルウェアと比較して、効率よく迅速に特定する手法を新たに開発しました。これによりマルウェアが持つ通信機能などを迅速に解析できるようになりました。さらに手法の有効性を実証するため、実際にインシデントを起こしたマルウェアを多数用いて静的解析も行い、非常に良好な結果が得られました。

ブラックリストにある悪性サイトを4項目で分類し、より効果的に対応

博士論文は『効果的・効率的なインシデントレスポンスの実現技術』で、CSIRTのインシデント対応への提案を行っています。論文は2つの技術からなり、一つは前述のようにインシデント対応の初動におけるマルウェア解析を効率化し、迅速な対応を可能にすること。もう一つがブラックリストを効果的に活用するための分類で、「所有者」「コンテンツ」「現在の状態」「最終更新」の4項目で分類し、CSIRTが合理的な判断を行う手かがりを提供するものです。実際に400件の悪性サイトを自ら分類し、通信遮断が必要かなど適切な判断ができることも示しました。
こうした技術が定着していけば、CSIRTの初期対応がより効果的・効率的なものに発展し、セキュリティの質を担保しながら業務の負担軽減にもつながると期待しています。

ブロックチェーンやAIを活用し、効率性や安全性に優れたSCM構築へ。その中核となる人材を目指します。

Tatsuo MITANI　三谷辰雄さん
情報セキュリティ研究科 博士後期課程1年
（三菱ケミカルシステム株式会社）

匿名性確保を目的に準同型暗号を導入セキュリティ上の課題を検討

私は、三菱ケミカルホールディングスグループで、デジタル分野の最新技術を利用したシステム開発を研究する部署に属し、次世代のSCM（サプライチェーンマネジメント）構築のプロジェクトに携わっています。今回のSCMはトレーサビリティや利便性の向上を図るため、ブロックチェーンの導入を想定しています。それに必要な専門知識を身につけるためIISECに入学し、暗号プロトコルやIoTセキュリティなどに詳しい大塚先生の研究室で指導を受けています。
従来のブロックチェーンのような分散環境ではデータが改ざんされにくい、リカバリーが比較的容易といったメリットがある一方、データが共有されて匿名性が保てないなどのデメリットもあります。そこで研究では暗号化したデータをそのまま処理できる準同型暗号という技術を活用し、利便性とプライバシー保護を両立可能なブロックチェーンを検討しています。

AIやIoTの技術をビジネスに生かし自分自身も成長するのが目標

IISECへの通学は研究室全員が集まる研究指導日と、大塚先生による個別指導日の週2回。同室の先輩・同級生も暗号通貨やAIなどが研究テーマで、指導日にそうした発表を聞くとヒントになることも数多くあります。これはセキュリティを軸に多方面から研究を行っているIISECならではの強みでしょう。
今後の目標は、急速に進化するAIやIoTの技術をキャッチアップし、新たなビジネスも視野に入れて事業に生かし、自分も成長すること。博士号取得はそのチャレンジの一つと考えています。

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2018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
Message

後藤厚宏

学長●情報セキュリティ研究科長●教授　Atsuhiro GOTO

文理融合の教育・研究から多様な情報セキュリティ分野で活躍できる人材を育てる

日々の暮らしを支える社会インフラが多様な情報システムで運用される時代。社会を揺るがす事件・事故の引き金となるサイバー攻撃への対応、IoTやBig Dataといった技術の活用に向けて、適切な情報セキュリティ対策は不可欠となっています。

私は当大学院の学長のほか内閣府SIP「重要インフラ等におけるサイバーセキュリティの確保」のプログラムディレクターなども務め、情報通信から交通、エネルギーまでさまざまな業界と関わっていますが、その経験から情報セキュリティが社会の全分野で必要とされ、幅広い知識と実践力を持つ人材育成が急務であると実感します。これは開学当初から多様な分野にまたがる情報セキュリティに対し、文理融合のコースで教育・研究を行ってきた当大学院の先進性を示すものといえるでしょう。

将来の目標に応じたコースフレームをもとにそれぞれの専門性を高める

そうした教育の特徴の一つが、当大学院の幅広い科目の中から、将来の目標に応じて履修内容を整理した4つのコースフレームです。どのコースも情報セキュリティ全般を学ぶ科目を基本に、例えば膨大なデータ処理など数理的な問題を研究する「数理科学コース」では主に技術系、企業や組織のセキュリティマネジメントを学ぶ「セキュリティ／リスクマネジメントコース」では主にマネジメント系の科目を選択します。

一方「システムデザインコース」と「サイバーセキュリティとガバナンスコース」は技術とマネジメントの両分野にまたがり、「システムデザインコース」はセキュアなシステム構築手法を、「サイバーセキュリティとガバナンスコース」ではオペレーション面から情報セキュリティの実務についての専門性を習得します。現在の情報セキュリティ対策はオペレーション面を重視しますが、今後はそれでは足りず、システム設計からセキュリティを重視した作り方をする必要が出てきます。「システムデザインコース」はそれを先取りしたものです。

加えて2017年度からは技術系にはIoTのセキュリティとAIのセキュリティ、マネジメント系には人間心理を担当する教員が加わり、教育・研究の幅が広がっています。

多様なバックボーンの仲間が大学院で同じ時間を共有し育まれる人脈は貴重

このような教育内容の幅広さに加え、ハンズオンによる実践的な学習も特徴です。技術系でサイバー攻撃の模擬演習を行うだけでなく、マネジメント系でもグループワークによる討議などを積極的に開講。さらに当大学院を含む産学官連携の人材育成プログラム「ISSスクエア」、全国の大学教員や企業の技術者が協働で作り上げてきた実践教育「enPiT／SecCap」など、他大学や企業と連携する教育プログラムも豊富に用意しました。講義の内容を演習で経験し、実践的な力を養うという手法は実務力育成を目指す当大学院ならではです。

しかも当大学院は社会人学生が多く、官公庁、システム開発の企業、セキュリティ対策が専門の企業などバックボーンも多様で、教員も実務家や実務経験者がほとんど。そうした学生と教員がFace to Faceの関係で濃密な講義や実習を行い、非常に深く広い人間関係が築けるのは、通信制の教育機関や資格取得を主目的とする講座にない魅力。大学院修了後も続く貴重な人脈を形成する絶好の機会といえます。

そして明日役立つ知識だけでなく、5年後、10年後の社会で主役となれるよう、革新的なアイデアを生む力、考える力をしっかり養ってほしいと考えています。

■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。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。2017年4月より同学長。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等を歴任。2015年11月より内閣府SIPプログラムディレクタ。2019年2月よりサイバーセキュリティ戦略本部員。

■主な研究業績
1. 後藤厚宏, 重要インフラにおける取組みと展望, 情報処理 Vol.58, No.11, 2017
2. Y. Tanaka, M. Akiyama, and A. Goto, Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware, Journal of Computational Science, ELSEVIER, 2017
3. Shigeo Mori, Atsuhiro Goto, Japanese Cybersecurity Policies Reviewed by Cybersecurity Capacity Maturity Model, Journal of Disaster Research, Vol.13 No.5, 2018
4. 羽田大樹, 後藤厚宏, CSIRTのためのWebブラックリストの分類提案, 情報処理学会論文誌 Vol.59 No.9, 2018
5. 後藤厚宏, 伊藤公祐, サイバーセキュリティの技術展望～セキュアなIoT社会に向けた取り組み～, 行政&情報システム vol54, Dec 2018

■主な研究テーマ
1. IoTとサプライチェーンセキュリティ
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
4. クラウドと仮想ネットワーク

■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

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・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。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。2017年4月より同学長。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等を歴任。2015年11月より内閣府SIPプログラムディレクタ。2019年2月よりサイバーセキュリティ戦略本部員。

■主な研究業績
1. 後藤厚宏.重要インフラにおける取組みと展望.情報処理 Vol.58, No.11,2017
2. Y. Tanaka, M. Akiyama, and A. Goto, Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware, Journal of Computational Science, ELSEVIER, 2017
3. Shigeo Mori, Atsuhiro Goto, Japanese Cybersecurity Policies Reviewed by Cybersecurity Capacity Maturity Model, Journal of Disaster Research, Vol.13 No.5, 2018
4. 羽田大樹、後藤厚宏.CSIRTのためのWebブラックリストの分類提案.情報処理学会論文誌 Vol.59 No.9, 2018
5. 後藤厚宏, 伊藤公祐. サイバーセキュリティの技術展望～セキュアなIoT社会に向けた取り組み～. 行政&情報システム vol54, Dec 2018

■主な研究テーマ
1. IoTとサプライチェーンセキュリティ
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
4. クラウドと仮想ネットワーク

■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

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. Hiroaki Anada, Seiko Arita, Short CCA-Secure Attribute-Based Encryption, Advances in Science, Technology and Engineering Systems Journal, Volume 3, Issue 1, pp. 261-273, 2018.
2. Seiko Arita, Sari Handa, Subring Homomorphic Encryption, ICISC 2017, LNCS vol 10779, pp. 112-136, Seoul, Korea, 2017
3. Seiko Arita, Shota Nakasato, Fully Homomorphic Encryption for Classification in Machine Learning, In Proc. IEEE BITS 2017, Hong Kong, China, 2017.

■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、ブロックチェーン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、Web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。日本ソフトウェア科学会実践的IT教育研究会運営委員。電子情報通信学会会員、IEEE CS会員、ACM会員。脅威分析研究会幹事、国際会議WESPrオーガナイザー。SIP　サイバーセキュリティ人材育成担当。経済産業省　産業サイバーセキュリティ研究会 ワーキンググループ1 分野横断サブワーキンググループ委員など。

■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)
6. 大久保 隆夫: セーフティとセキュリティ,<小特集>乗り物のセキュリティと安全性,情報処理 No.57, vol.7,pp.630-631 (2016)

■主な研究テーマ
セキュリティ・バイ・デザイン、脅威分析、ソフトウェア/システムセキュリティ、マルウェア解析/ネットワークセキュリティ、制御システムセキュリティ、IoTセキュリティ、セキュリティとセーフティ、AI応用システムのセキュリティ構築、検証に関する研究

■主な担当科目
ソフトウェア構成論、アルゴリズム基礎、情報セキュリティ技術演習Ⅰ、実践的IoTセキュリティ、情報セキュリティ輪講Ⅰ、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

大塚　玲

教授
Akira OTSUKA

■プロフィール
大阪大学工学研究科博士前期課程修了。東京大学大学院工学系研究科電子情報工学専攻博士課程修了。博士（工学）。野村総合研究所,東京大学生産技術研究所,産業技術総合研究所などを経て2017年4月より本学教授。2006年-2010年産業技術総合研究所情報セキュリティ研究センター・セキュリティ基盤技術研究チーム長。2007年-2014年中央大学研究開発機構教授。東京理科大学大学院工学研究科非常勤講師（2009年から3年間）、城西大学理学部数学科非常勤講師（2015年-）、北陸先端科学技術大学院大学情報科学研究科非常勤講師（2016年）。電子情報通信学会、情報処理学会、IEEE等各会員、情報処理学会論文誌編集委員、電子情報通信学会バイオメトリクス研究専門委員会委員長（2019年6月-）。

■主な研究業績
1. Taisei Takahashi and Akira Otsuka. “Short Paper: Secure Offline Payments in Bitcoin,” In Proceedings of 2019 on Workshop on Trusted Smart Contract, WTSC’19. St. Kitts, IFCA 2019. (preprint, to appear from Springer LNCS)
2. Tetsushi Ohki and Akira Otsuka, “Theoretical Vulnerability in MAP Speaker Adaptation” Proceedings of 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP2017), (2017).
3. Tetsushi Ohki and Akira Otsuka, "Theoretical vulnerability in likelihood-ratio-based biometric verification," 2014 IEEE International Joint Conference on Biometrics (IJCB), pp.1-8, (2014).
4. Akira Otsuka, Hideki Imai , “Unconditionally Secure Electronic Voting”, Towards Trustworthy Elections; New Directions in Electronic Voting, David Chaum and Markus Jakobsson and Ronald L. Rivest and Peter Y. A. Ryan and Josh Benaloh and Miroslaw Kutylowski and Ben Adida Eds., Lecture Notes in Computer Science Vol. 6000, Springer, ISBN 978-3-642-12979-7, pp. 107-123, (2010).
5. Manabu Inuma, Akira Otsuka, and Hideki Imai, “Theoretical framework for constructing matching algorithms in biometric authentication systems,” Proceedings of the Third IAPR/IEEE International Conference on Biometrics (ICB 2009), LNCS 5558, 293-300, (2009).

■主な研究テーマ
情報セキュリティ理論（Blockchain, 敵対的機械学習の安全性など）

■主な担当科目
AIと機械学習、暗号・認証と社会制度、特設講義(ブロックチェーン理論)、研究指導

■担当コース
数理科学コース

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。2017年度 IPSJ Outstanding Paper Award 受賞。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. XOR-based Hierarchical Secret Sharing Scheme, K. Shima, H. Doi, Proc. of IWSEC 2018, LNCS 11049, pp.206-223, Springer (2018).
2. A Hierarchical Secret Sharing Scheme over Finite Fields of Characteristic 2, K. Shima, H. Doi, Journal of Information Processing, Vol.25(2017), pp.875-883 (2017).
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).
5. 利用履歴を秘匿できるコンテンツ配信・課金方式に関する研究, 飛田孝幸, 山本博紀, 土井洋, 真島恵吾, 情報処理学会論文誌, 第50巻,第9号, pp.2228-2242 (2009).

■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. 暗号技術の高速化と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

藤本　正代

教授
Masayo FUJIMOTO

■プロフィール
1993年5月MIT技術政策大学院修了。2000年6月東京工業大学社会理工学研究科経営工学専攻博士課程修了。経営工学博士。GLOCOM客員研究員。インターリスク総研及び富士ゼロックス株式会社にて、情報セキュリティに係る調査研究・コンサルティング、医療情報システム関連の業務等に従事。2004年～2018年情報セキュリティ大学院大学客員教授、2007年～2017年筑波大学客員教授。内閣サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会委員、総務省情報通信審議会や国立研究開発法人審議会の専門委員ほか、政府機関等の委員会委員。企業や団体向け講演、多数。日本セキュリティマネジメント学会、情報処理学会所属。2009年情報化月間総務省情報通信国際戦略局長表彰受賞。2019年4月より本学専任教授。

■主な研究業績
1. INFORMATION SECURITY SHARING OF NETWORKED MEDICAL ORGANIZATIONS: CASE STUDY OF REMOTE DIAGNOSTIC IMAGING, E-Health IFIP Advances in Information and Communication Technology, Volume 335, pp.90-101 (2010.9)Masayo Fujimoto, Koji Takeda, Tae Honma, Toshiaki Kawazoe, Noriko Aida, Hiroaki Hagiwara, Hideharu Sugimoto
2. INDUSTRIAL INNOVATION, GOVERNMENT AND SOCIETY: TELEMEDICINE AND HEALTHCARE SYSTEMS IN JAPAN Science and Public Policy, Vol 27, No. 5, pp. 347-366, (2000.10),Fujimoto M., Miyazaki K.
3. SHAPING ELECTRONIC COMMUNICATION: THE METASTRUCTURING OF TECHNOLOGY IN THE CONTEXT OF USE Organization Science Vol. 6, No. 4. pp.423-444　(1995.7-8) Orlikowski W., Yates J., Okamura K., Fujimoto M.
4. 「不確かなもの」を小さくしていく「組織文化」の醸成を―情報セキュリティにおけるリスクマネジメントとは」,特集「サイバー攻撃に負けない組織づくり」,インタビュー記事月刊J-LIS,Vol.5 NO.3:pp.12-15,(2018.6)
5. IoT時代の製品開発プロセスと品質保証～組織的視点からの考察～日本セキュリティ・マネジメント学会　第29回全国大会発表予稿集,(2015.6)藤本正代

■主な研究テーマ
情報セキュリティマネジメント、情報セキュリティガバナンス、科学技術政策、組織経営、
組織間連携とセキュリティ・リスクマネジメント、イノベーションとセキュリティ・リスクマネジメント

■主な担当科目
個人識別とプライバシー保護、リスクマネジメント、国際標準とガイドライン、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

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、2015-17年NEDO技術戦略研究センター電子情報機械システムユニット長。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、エンベッデッドシステムスペシャリスト。2016年より本学教授。2018年よりNEDO研究評価委員。

■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
IoTセキュリティ
制御システムセキュリティ
ロボットとAIのセキュリティ

■主な担当科目
情報デバイス技術、AIと機械学習、アルゴリズム基礎、
情報システム構成論、実践的IoTセキュリティ、研究指導

■担当コース
システムデザインコース

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。内閣府少年インターネット環境の整備等に関する検討会委員。
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
荻野　司
客員教授
Tsukasa OGINO

■プロフィール
重要生活機器連携セキュリティ協議会　代表理事
長岡技術科学大学大学院工学研究科博士前期課程了、首都大学東京大学院都市環境科学研究科博士後期課程了 博士(工学)。キヤノン(株)中央研究所を経て、各種製品の研究・開発やISP事業に携わる。2003年〜2014年まで株式会社ユビテック代表取締役社長。(社)日本ネットワークインフォメーションセンター(JPNIC)のIP 担当理、IPv6 普及・高度化推進協議会常務理事を歴任。現在は、IoTセキュリティにおける標準化、技術開発を推進。京都大学 宇宙総合研究ユニット特任教授(2014年〜)。
■担当科目
実践的IoTセキュリティ

兼任
生越　由美
客員教授
Yumi OGOSE

■プロフィール
東京理科大学 経営学研究科 技術経営専攻教授
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、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、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
佐藤　直
客員教授
Naoshi SATO

■プロフィール
情報セキュリティ大学院大学名誉教授
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月から2017年3月まで本学専任教授。2017年4月より本学客員教授。
■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
情報セキュリティ技術演習Ⅰ
特設講義(ハッキングとマルウェア解析)

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
種茂　文之
客員教授
Fumiyuki TANEMO

■プロフィール
エヌ・ティ・ティ・アドバンステクノロジ株式会社 セキュリティ事業本部 主席技師
名古屋大学工学部情報工学科、同大学大学院情報工学専攻修了後、1993年日本電信電話株式会社に入社、2018年より現職。ネットワークセキュリティ、CSIRT構築・運用の研究開発や企画運営等に携わる。現在は、インシデント対応支援やSOC等のマネージドセキュリティサービス提供業務に従事。
■担当科目
特設実習(セキュリティ実践Ⅰ、Ⅱ)

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
原田　要之助
客員教授
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。1979年日本電信電話公社(現NTT)研究所入所、1999年情報通信総合研究所。2010年4月から2019年3月まで本学専任教授。2019年4月より本学客員教授。その他、1995年〜2011年大阪大学工学部大学院特任教授。また、中央大学理工学部・大学院、サイバー大学、フェリス女学院大学で非常勤講師を務める。
■担当科目
情報セキュリティマネジメントシステム
セキュリティ経営とガバナンス
特設講義(セキュリティ監査)

兼任
廣松　毅
客員教授
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月から2017年3月まで本学専任教授。2017年4月より本学客員教授およびセキュアシステム研究所特別研究員。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。2018年11月〜現在、日本学術会議人文学・社会科学データインフラストラクチャー構築推進センター・センター長。
■担当科目
統計的リスク管理、リスクの経済学

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、システム監査学会常任理事、日本監査研究学会会長、日本内部統制学会常任理事、情報処理技術者試験委員、会計検査院情報公開・個人情報保護審議会委員、金融庁・行政事業レビュー有識者会議メンバー、海上保安庁入札監視委員などを兼任。『原談 不正一最前線』(同文舘出版、2019年)『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年より現職。現在、情報通信工学、特にサイバーセキュリティ、情報理論、符号理論、暗号理論等の研究、教育に従事。2018年経済産業大臣賞受賞、2019年総務省情報通信功績賞受賞
■担当科目
サイバーセキュリティ技術論

兼任
Ray Roman
客員教授

■プロフィール
東北大学会計大学院 ビジネス・コミュニケーション教授
Doctor of Laws, Harvard University; 1991
■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 NTTセキュアプラットフォーム研究所 主任研究員
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、プライバシー保護の技術と法制度に関する研究開発に従事。国立研究開発法人 理化学研究所 革新知能統合研究センター(AIP)客員研究員、情報ネットワーク法学会元理事。
■担当科目
セキュリティの法律実務

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
情報セキュリティ技術演習Ⅱ

※上記は2019年4月現在

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、各省庁・自治体のセキュリティ、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、(一財)日本サイバー犯罪対策センター理事等を務める。

■主な研究業績
1. 『電子化社会の政治と制度』(オプアワーズ、2006年3月)
2. 「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)
3. 「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—」『情報セキュリティ総合科学』第6巻(2014年)
4. 「ディジタルゲリマンダの法規制の可能性」情報処理58巻12号(2017年12月)
5. 「理念・原理・制度とサイバーセキュリティ法制 −選挙を中心に−」情報通信政策研究2巻1号(2018年12月)

■主な研究テーマ
1. プライバシー・個人情報に関する各国の憲法、法律上の規定の比較研究
2. インターネット選挙運動、フェイクニュースなど政治・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、
特設講義(サイバーインテリジェンス)、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
稲葉　緑
准教授
Midori INABA

■プロフィール
2006年、名古屋大学大学院環境学研究科社会環境学専攻、博士後期課程修了。博士(心理学)。2005年、独立行政法人交通安全環境研究所非常勤研究員、2006年より国立大学電気通信大学大学院情報システム学研究科助教。2009年ロンドン市立大学心理学科客員研究員。2013年よりJR東日本研究開発センター安全研究所研究員。2017年4月より本学准教授。研究テーマはセキュリティ行動を支援するシステム・仕組みの検討。国土交通省運輸審議会運輸安全確保部会専門委員。日本心理学会、情報処理学会、日本応用心理学会等会員。情報処理学会論文誌編集委員、ヒューマンインタフェース学会論文誌編集委員、情報処理学会セキュリティ心理学とトラスト研究会運営委員、自動車技術会ヒューマンファクター部門運営委員、等。

■主な研究業績
1. 稲葉 緑, 鉄道分野におけるヒューマンエラー教育-社員向けヒューマンエラー体験型学習ツールの開発を例に,システム/制御/情報(vol.61), 226-232, 2017年
2. 清 雄一,稲葉 緑,大須賀昭彦,安心できるプライバシ指標の調査,情報処理学会論文誌,56巻, 1—14, 2015年
3. Inaba, M., K. Tanaka, Risk presentation aimed at improving older drivers' understanding of their problems via simulator-based education programs, SICE-JCMSI 5巻, 326—334, 2012年
4. Inaba, M., Individualistic attitudes toward attractive rewards in older people: an experimental study using ultimatum games, Japanese Psychological Research 57巻, 91—102 2015年
5. 稲葉 緑,田中健次,水害時の避難へのモチベーションに影響を及ぼす情報提示内容についての実験的検討, 災害情報 9巻, 127—136, 2011

■主な研究テーマ
効果的なセキュリティ教育および教育プログラム、セキュリティ問題行動を抑制するしくみ、
リスク認知とリスク回避情報システム、ヒューマンエラー

■主な担当科目
統計的方法論、情報セキュリティ心理学、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
橋本　正樹
准教授
Masaki HASHIMOTO

■プロフィール
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、不正侵入検知・防御等。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)専門委員、情報処理学会論文誌ジャーナル/JIP編集委員会委員、日本ソフトウェア科学会SIG-rePiT主査(2019年度)、CSITS2019 Programme Committee Member、NETSAP2019 Workshop Organizer 等。

■主な研究業績
1. Masashi Kadoguchi, Shota Hayashi, Masaki Hashimoto, Akira Otsuka: Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning, Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (IEEE ISI 2019), Shenzhen, 2019. (in press)
2. Toshihiro Yamauchi, Yohei Akao, Ryota Yoshitani, Yuichi Nakamura, Masaki Hashimoto: Additional Kernel Observer to Prevent Privilege Escalation Attacks by Focusing on System Call Privilege Changes , Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (IEEE DSC 2018), pp.172-179, 2018.
3. 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.
4. 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.
5. Hashimoto, M., Kim, M., Tsuji, H. and Tanaka, H.: Policy Description Language for Dynamic Access Control Models, Proceedings of the 8th IEEE International Symposium on Dependable, Autonomic & Secure Computing (IEEE DASC 2009), 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/サイバー攻撃技術
3. OSINT/Intelligence Mining　4. ネットワークセキュリティ

■主な担当科目
オペレーティングシステム、情報セキュリティ技術演習Ⅰ、情報セキュリティ輪講Ⅰ、特設講義(ハッキングとマルウェア解析)、研究指導

■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（2018年度ご参考）

- 4/6 入学式・新入生歓迎会
- 4/9 前期開講
- 5/26 春季オープンキャンパス ホームカミングパーティ
- 8/1 前期授業期間終了
- 9/1 修士論文等発表会（9月修了）
- 10/1 後期開講
- 10/12 第15回アドバイザリーボード
- 11/10 秋季オープンキャンパス ホームカミングパーティ
- 2/9 後期終講
- 2/23 修士論文等発表会（3月修了）
- 3/23 学位記授与式

■ 入学式
2018.4.6

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
2019.2.23

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。

2018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
2019.3.23

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（2019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 研究開発本部 研究開発センター サイバーセキュリティ技術センター 研究主幹	秋山 浩一郎	株式会社KDDI総合研究所 取締役執行役員副所長 （兼）KDDI株式会社 技術企画本部 情報セキュリティフェロー	田中 俊昭
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	大久保 一彦	日本電気株式会社 セキュリティ研究所 所長	谷 幹也
株式会社日立製作所 研究開発グループ 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 主管研究員	鍛 忠司	株式会社富士通研究所 セキュリティ研究所長 （兼）ブロックチェーン研究センター長	津田 宏
東京電機大学 研究推進社会連携センター特別専任教授（特命教授） （兼）サイバーセキュリティ研究所 所長	佐々木 良一	パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略室 主幹技師	中野 学
日本アイ・ビー・エム株式会社 東京基礎研究所 セキュリティ&ハイブリッドクラウドイノベーション担当部長	佐藤 史子	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
沖コンサルティングソリューションズ株式会社 代表取締役社長	杉尾 俊之	横浜国立大学 大学院 環境情報研究院 教授	松本 勉
国立研究開発法人産業技術総合研究所 理事 情報・人間工学領域 領域長	関口 智嗣	国立研究開発法人情報通信研究機構 執行役 サイバーセキュリティ研究所 所長	矢野 博之

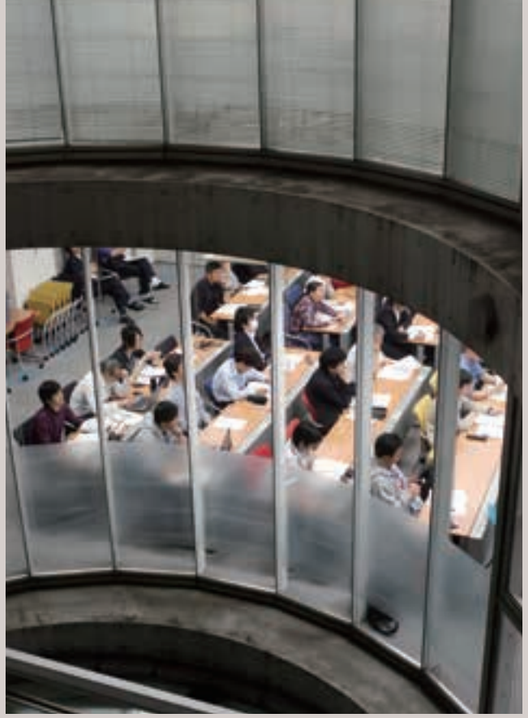
敬称略、氏名五十音順

■ 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（2019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	日本経済新聞社 編集委員	関口 和一
株式会社日立ソリューションズ 監査室 室長	石川 明	桜美林大学 リベラルアーツ学群 教授	平 和博
NTTコミュニケーションズ株式会社 経営企画部長	稲葉 秀司	日本放送協会 専務理事 技師長	児野 昭彦
沖電気工業株式会社 経営企画本部 情報企画部 部長	長田 肇	慶應義塾大学 大学院政策・メディア研究科 教授	土屋 大洋
日本電信電話株式会社 取締役 研究企画部門長	川添 雄彦	国立研究開発法人 情報通信研究機構 理事長	徳田 英幸
株式会社エヌ・ティ・ティ・データ 取締役常務執行役員 技術革新統括本部長	木谷 強	独立行政法人 情報処理推進機構 理事長	富田 達夫
芝浦工業大学大学院 客員教授	國井 秀子	三菱電機株式会社 開発本部 役員技監	中川路 哲男
早稲田大学 名誉教授	後藤 滋樹	神奈川県 副知事	中島 正信
富士通株式会社 執行役員常務 テクノロジーソリューション部門 グローバルサイバーセキュリティビジネスグループ長	斎藤 淳一	株式会社東芝 特別嘱託	西田 直人
日本電気株式会社 執行役員常務	堺 和宏	パナソニック株式会社 コネクティッドソリューションズ社 常務	行武 剛
東京電機大学 研究推進社会連携センター特別専任教授（特命教授） （兼）サイバーセキュリティ研究所 所長	佐々木 良一	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。

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。

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、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。

ようこそ「情報セキュリティ大学院大学」へ。
入学後が肝心。修了後はもっと肝心。

日本初の情報セキュリティに特化した独立大学院である本学に入学された皆様には、同窓会との連携による人脈形成から修了後の学び直しまで、在学中のみならず修了後もIISECコミュニティならではのさまざまな機会を提供します。

Human network

■ IISEC Alumni（同窓会組織）との連携

本学では、学部新卒学生はもちろんのこと、様々な組織に所属する社会人が学んでいます。
この組織横断的な人脈を修了後も活かしていただくために、同窓会組織であるIISEC Alumni（アラムナイ）と連携した取り組みを行っています。

•IISEC Alumni Reunion

IISEC同窓生の交流を目的としたイベントで、IISEC修了生の方々によるご自身のお仕事や活動等についての講演会と、在学生、教職員を交えた懇親会を毎年開催しています。




•就職相談会

実力のある人材は引く手あまたなセキュリティ業界。各企業で活躍中のOBOGによる就職相談会、業界セミナーを開催しています。

■ 所属研究室（ゼミ）を越えた交流機会

単一研究科単一専攻の大学院ならではのアットホームな雰囲気。ゼミ横断的な勉強会やOBOGを交えた懇親イベントなど、ご自身の直接的な専門領域、研究分野にとどまらず、知見や人脈を広げていただくためのさまざまな機会があります。「情報セキュリティ」をキーワードに集った大学院生同士として、研究の進捗はもちろんのこと、進路や仕事に関する悩みなど本音で話し合えるフラットな関係性は、在学中のみならず、修了後も続く貴重な財産です。

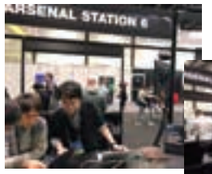




Refresh and enrich

■ 課程外教育プログラム等の優待受講

ムービングターゲットとも言われる情報／サイバーセキュリティ。大学院で体系的な知識を身に付けた後も、常に知識・スキルのアップデートが要求されます。本学大学院の正規課程修了後に、OBOGの方が科目等履修生として特定の授業科目の履修を希望される場合は履修料が半額となる他、日々開発される実践演習等の課程外教育プログラムについても優待価格で受講できるなど、修了後の学び直しも応援します。



■ 客員研究員制度を利用した研究活動の継続

本学の博士前期課程に入学されるのは、一部の研究職の方を除き、これまで研究経験がなかった方がほとんどですが、大学院入学を契機に研究活動に取り組んだことにより興味を深め、大学院修了後も業務と並行して自分のペースで研究の継続を希望される方も。こうした方々のため、本学では客員研究員の制度を設けています。また、学外には非公開としている全研究室横断型科目「情報セキュリティ輪講Ⅰ」の聴講がOBOGには認められており、後輩である在学生が取り組むタイムリーなセキュリティ課題のキャッチアップも可能です。

■ 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（※2019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）

INSTITUTE of INFORMATION SECURITY

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

所長 **後藤 厚宏**
情報セキュリティ大学院大学
学長・教授

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。
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。

■ セキュアシステム研究所のプロジェクト

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。

❹ Internet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
株式会社サイント
代表取締役

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
株式会社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。

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

Japan University Accreditation Association since 1947
UNIVERSITY ACCREDITED 2017.4~2024.3

■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

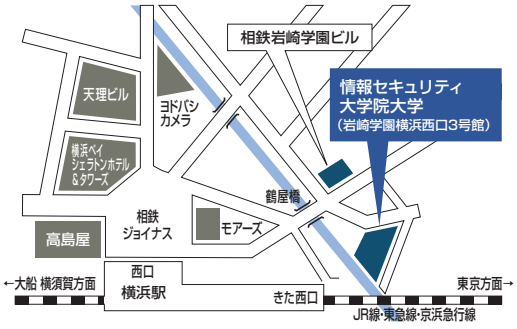
詳細は本学ウェブサイトでご確認ください。

■入学者選考方法

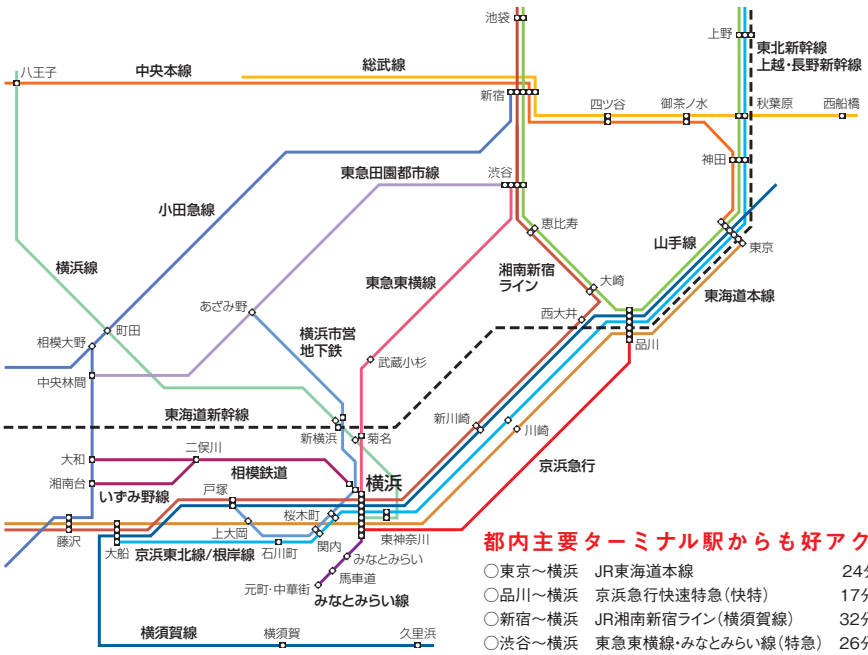
博士前期（修士）課程［2年制］	一般入試	面接（プレゼンテーションを含む）および志望理由書、学業成績、小論文等出願書類審査を総合して行う
	社会人入試	面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士前期（修士）課程［1年制］		面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士後期課程		口述試験（プレゼンテーションを含む）および研究計画書等出願書類審査によって、研究能力を総合的に判定する

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。

明日の信頼を創ろう。
情報セキュリティ大学院大学　http://www.iisec.ac.jp/
INSTITUTE of INFORMATION SECURITY
〒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
IWASAKI GAKUEN 学校法人 岩崎学園



（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