明日の信頼を創ろう。

情報セキュリティ大学院大学

Établissons la confiance mutuelle pour un avenir meilleur.

INSTITUTE of INFORMATION SECURITY

2025-2026

学校法人 岩崎学園

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

未来をよりよく変えるチャンスがここに。
私たちIISECはデジタル社会の実現に不可欠な情報セキュリティを専門とする大学院大学です。
セキュリティに関する先進的な研究と、確かな実力で社会の発展を支える基幹人材の育成により、
あなたが自分の未来と社会の明日を変えていくチャンスを用意しています。

情報セキュリティの最前線で
未知の社会課題に挑む力を養おう。

情報セキュリティに専門特化し、理論と実務の両面から専門的な教育・研究を行ってきたIISEC。
2025年4月に学長に就任した桑名栄二学長と後藤厚宏前学長（教授・特別学長補佐）に、
IISECによる人材育成と情報セキュリティの未来像を語っていただきました。

学長
桑名 栄二
Eiji KUWANA

対談

特別学長補佐（前学長）
後藤 厚宏
Atsuhiro GOTO

日本のサイバーセキュリティは「人への投資」が足りない

桑名●本学が2025年3月までに送り出した修士58４名、博士54名は、すでに社会の各分野で情報セキュリティを担う重要な人材として活躍しています。また、後藤先生が長くプログラムディレクターを務めた内閣府のSIP（戦略的イノベーション創造プログラム）のように、本学はサイバーセキュリティに関する先進的な研究の推進役にもなってきました。そうした確かな実績を受け継ぎ、より混迷を増す時代に必要な次のセキュリティ人材を育てることが私の学長としての役割と考えています。

後藤●私自身は学長としてやり遂げられなかった部分も多いと感じていますが、桑名先生にはICT業界全体に広がる多様な人脈や実務の見識をもとに、本学を新たなステージに進めていただきたいと思います。私も自身の強みである官公庁とのコネクションなどを生かしてサポートしていきます。

桑名●ええ、ぜひお願いします（笑）。ただ、近年は企業もサイバーセキュリティを重要な経営課題と認識してはいますが、セキュリティ機器などハード面への投資が先行し、企業のレジリエンスに必要な「人への投資」がやや後回しにされがちであることに、私は課題意識を持っています。生成AIをはじめ技術が急速に進化する時代の人材育成は、大学を卒業して企業に勤めた後、本学のような大学院で自身の専門性を高め、企業に戻るといった循環型のキャリア形成が不可欠でしょう。むろん本学も社会や産業界の期待に応えるべく、カリキュラムをアップデートし続ける必要があります。

未知の社会課題に挑むため問題解決力を養う環境を用意

IISEC（情報セキュリティ大学院大学）はセキュリティ専門人材から「プラス・セキュリティ」人材まで広く育成する教育機関です。また学生一人ひとりの成長を促し、未知の課題に挑む問題解決能力を養う機会も豊富です。そうした本学への期待は高く、企業・官公庁等からの社会人学生派遣、連携教授制度による公的機関・企業等の教育活動への協力等、開学以来20年以上も変わらぬ支援をいただいています。

本学の強みは、セキュリティが文理を網羅・融合した総合科学であるという本質を踏まえ、暗号や認証、AI、マルウェア分析、セキュアな機器・システムの構築、法制度、組織マネジメント、心理学など、セキュリティを軸に全方位を学べる環境を整えていること。分野ごとに深い専門性を持ち、実務経験・指導経験の豊富な教員が在籍するほか、多様な分野の第一線にいる人材による講義も多く行っています。

一方、現代社会は自動車メーカーによるバッテリーやAIの研究など業界の境目がなくなり、セキュリティ対策も複合化しています。そのため本学では在学生の興味や課題意識、指導教員の助言をもとに、複数分野をクロスさせて学ぶ教育体系を構築。指導に意欲的な教員により横断的な学習・研究もしやすい環境で、今後の業務に必要な分野を追究する、課題解決に向けて複数の視点から検証する、境界領域のセキュリティの課題に取り組むなど、多様な研究を可能にします。

また、在学生は社会人学生が多く、実社会とつながる実践的な学習や研究を行っている点も特徴です。IISECでの学びは、あなたに大きな成長、次のキャリアへの変化、新たな選択に必要な変革をもたらしてくれるでしょう。

桑名●後藤先生の言う通り、本学は境界領域も含むサイバーセキュリティをリードする存在で、時代に先駆けて新たなセキュリティの課題を定義し、広く発信して社会を変える先駆者、ソートリーダーの役割を担っています。そうした先進的な教育・研究に加えて、問題解決能力をはじめ実務面ではクリティカル・シンキングやホリスティクな視点を鍛える場になっています。そして一人ひとりの個性を大事にしながら成長を促し、互いにリスペクトして新しい課題にチャレンジして、修了時に「楽しかった」と心から感じられる—自分の人生の中で充実した時間を過ごせる場になることは間違いありません。「自分はセキュリティが専門ではないから」と最初から諦めず、少しでも新しい知識への好奇心がある方は、ぜひ本学でその一歩を踏み出してみてください。

後藤●人材育成については、情報セキュリティ分野の知識・技能の習得はもちろん、予測不能な変化にも対応できるよう「未知の問題を解く力」も重要になります。本学の学生は教員の指導のもと、多様な研究で未知の問題を解くトレーニングを積み重ね、修了後に実務で直面する困難な課題を打開できる人材へと成長する機会を得ていると思います。

桑名●確かに本学は研究を通して学生を成長させる場なのは間違いありません。加えて学生の皆さんは未知の課題に好奇心を持って取り組み、「楽しんで研究する」ことも大事にしてほしいですね。ところで後藤先生は以前から「プラス・セキュリティ」人材へのニーズもよく話されていましたね。

後藤●現在はどの分野もサイバーセキュリティへの対策は不可避で、情報セキュリティの専門家のほかに、社会の各専門分野で必要なセキュリティの知識を習得した「プラス・セキュリティ」人材が求められています。しかもIISECには金融、メーカー、官公庁など多様な業界から学生が集まっていますから、他業界に視野を広げて自分をより客観的に見る力も養える環境ではないでしょうか。

桑名●特に機能の停止・低下が社会の大きな混乱を招く情報通信、金融、交通関係、エネルギーなど重要インフラの分野は、セキュリティの知識がマストです。IT部門に限らず人事や法務、知財など広い職種の方に学んでほしいですね。セキュリティインシデントでの賠償問題に欠かせない弁護士も「法律＋セキュリティ」で活躍の幅が広がるでしょう。

後藤●実際、私の研究室では弁護士をしている学生が企業のセキュリティ部門の学生と議論していますし、多様な業種・役職の社会人がフラットな交流の中で刺激し合える環境はIISECならではです。

社会で次のチャンスをつかむOB・OGの積極的な交流

桑名●社会に出てもその関係が続くのがIISECの良さで、OB・OGが本学を訪れて教員や在学生と交流する機会が多いことも特徴的です。

後藤●年2回のホームカミングパーティや修士論文・博士論文の発表会などでOB・OGと交流した在学生は非常に刺激を受けますし、各研究室のゼミにもオンラインでOB・OGが参加してくれます。

桑名●教員もOB・OGから業界の最新情報を聞けて、OB・OGは後輩たちの研究内容で自身の知識をアップデートできるWIN-WINの関係ですね。

後藤●先ほどの法律面と技術面の議論のように、現在の社会は複数分野にまたがる境界領域のセキュリティ対策が急務で、「プラス・セキュリティ」人材へのニーズは今後も拡大するでしょう。加えて本学のOB・OG同士で多職種の交流を重ねて、境界領域のセキュリティに取り組んでほしいですね。

本学の特徴

- **情報セキュリティに専門特化した独立大学院**
  単一専攻の小規模大学院ならではの機動力と親身な指導
- **広範な分野をワンストップで学べる「総合性」**
  暗号、ネットワーク、システム技術、マネジメント、法制度・倫理まで、幅広い分野をワンストップで対応
- **企業や官公庁が求める「実務指向」の人材育成**
  セキュリティ分野の高度な専門技術者、実務リーダー、創造性豊かな研究者を育成。複数の企業、大学と連携し、セキュリティ実務能力を向上させる機会を創出
- **社会人も在職のまま就学可能な時間帯と開講形態**
  社会人も受講しやすい平日昼夜間と土曜日に授業を実施
  特定曜日※の授業はすべてオンラインで開講
  ※詳細は大学事務局にお問合せください

新たな社会に挑むIISEC

■新入生レポート

IISECの幅広い授業やISSスクエアの受講、社会人学生との交流など成長の機会が豊富。

宇治川 ひかるさん　Hikaru UJIGAWA

情報セキュリティ研究科　博士前期課程1年

東京デザインテクノロジーセンター専門学校

スーパー IT科出身

時限	月	火	水	木	金	土	日
1	移動	大学院に登校	自宅で準備	自宅で準備	移動	大学院に登校	自宅で自習や研究のほか、家事をまとめて片づける気分転換に近所を散歩することも
2	NICT（情報通信研究機構）でRAのアルバイト 10時～18時	プログラミング	移動	移動	NICT（情報通信研究機構）でRAのアルバイト 10時～18時	自習	
3		オペレーティングシステム	ネットワークセキュリティ（中央大学）	電子社会と情報セキュリティ（中央大学）		情報セキュリティ技術演習Ⅰ	
4		大学院で自習	大学院に登校	大学院に登校			
5		須崎研究室のゼミに参加	情報セキュリティ輪講Ⅰ	情報デバイス技術（オンライン）			
6	移動	大学院の院生室で研究 22時30分まで	ソフトウェア構成論	大学院の院生室で研究 22時30分まで	移動	自宅で自習・研究のほか、家事をまとめて片づける	
α	自宅で自習 20時～22時		帰宅		自宅で自習 20時～22時		

1>指導教員の須崎先生との個人面談。必要な知識を補う授業や演習系の授業なども紹介してもらう　2>土曜日の「情報セキュリティ技術演習」では攻撃側と防御側に分かれてネットワーク不正侵入などの手法を実践的に学べる

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

◉学内での幅広い授業に加え外部の教育プログラムも充実

当初は就職を目指し、専門学校の4年制コースでセキュリティ対策の技術面を中心に学びました。しかし3年のときに参加したSecHack365を機に、情報セキュリティを深く追究したくなり大学院進学を決意しマネジメントや法制度といった視点でも研究でき、ISSスクエアやSecCapなどのプログラムも充実したIISECを選びました。

授業や研究指導では先生方がとても丁寧に教えてくれ、相談もしやすい環境だと感じます。社会人の学生も多く、1階ロビーで学生が交流するティータイムではさまざまな研究室の同級生・先輩と話せ、研究の方向性や将来について聞けるのもメリットで、多くの先輩が勧めてくれるインターンによる仕事体験も、研究の予定と調整して早く実現したいです。

◉ヘルスケアのデジタル化のため安全なデータ管理を研究予定

以前からヘルスケア分野にも興味があり、医療用ウェアラブル端末で得た個人の健康情報を安全に保存・運用するための環境整備などを、OSやハードウェアのセキュリティをテーマとする須崎先生の研究室で研究していく予定です。

現在は須崎先生からのアドバイスをもとに、情報を安全に保てるTEE（高信頼実行環境）の実現に向けてOSや情報デバイスを体系的に学んでいます。

私の1週間

◉2つの研究室による合同ゼミで多様な分野の知識が得られる

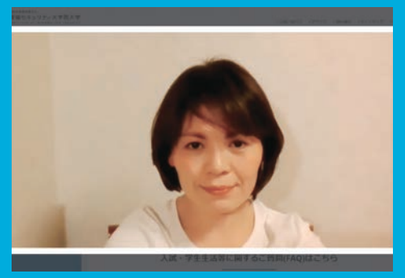
月・金曜日はRA（研究補助）を務めるNICTへの往復に時間がかかるため、自宅で2時間ほど自習する程度です。火曜日の須崎研究室のゼミでは研究指導に加え、隔週で大久保研究室とのトップカンファ輪講では評価の高い学会論文について発表も行います。選ぶ論文は自由なので、多様な分野の最先端の動きや発表者の論文への着眼点が学べて面白いです。

水・木曜日はISSスクエアに含まれる授業を中央大学で受け、IISECに移動して授業に出席。木曜日はすべての授業がオンライン開講ですが、私は大学院の院生室で受講し、その後は22時30分まで研究の時間に充てています。

◉安全な環境を実現するため技術の基礎を学ぶ授業も受講

授業の「オペレーティングシステム」や「情報デバイス技術」では発展してきた歴史的背景や基礎知識を学ぶことで、専門学校で習得した実践的な技術の裏付けとなり体系的な見方も養えました。

このほかSecCapの集中講座「情報セキュリティPBL演習」でWEB上の攻撃手法がどう行われるかをグループに分かれて検討し、ISSスクエアの研究活動であるネットワーク分科会ではCTFの勉強会に参加するなど、学ぶ機会が非常に多くて充実しています。



新たな社会に挑むIISEC

セキュリティ分野の高度な専門性に加え複雑な社会課題に挑む問題解決能力を養うIISEC。新入生、在学生の今と修了生からの応援を紹介。

2004年開学のIISECは、情報セキュリティに専門特化した教育・研究に加え、一人ひとりの成長を促す大学院大学です。
バックグラウンドも多彩な在学生は自身の興味・関心を軸に広く学び、教員や在学生同士の交流で新たな知見を得て、
混迷の時代の中でもキャリアアップ、新たな分野へのチャレンジ、次のチャンスをつかむ転職などを実現。
さらにOBOGも「IISEC人脈」ともいえるコミュニティで交流を続け、新たな成長の機会をつかんでいます。
平日昼夜や土曜日の対面形式の講義・演習を中心に、オンライン開講の科目を集約した曜日も設定するなど、
IISECでは「FACE TO FACE」を重視しながら、在学生の7割近くを占める社会人学生も学びやすいよう配慮。
巻頭特集では充実した学生生活を送る新入生や在学生と、社会で活躍する修了生からの応援メッセージを紹介します。

■新入生レポート

ベストなセキュリティ対策の提案を目指し マネジメントなど新たな知識を身につける。

小栗 美優さん　Miyu OGURI
情報セキュリティ研究科　博士前期課程1年
株式会社NTTデータ先端技術
セキュリティ&テクノロジーコンサルティング事業本部

時限	月	火	水	木	金	土	日
1						大学院に登校	
2		リモートワーク 10時～16時	リモートワーク 10時～16時 その後は 大学院に登校	リモートワーク 10時～16時		セキュリティ システム監査	
3	出社して業務 10時～18時30分				土曜日の受講が出勤扱いのため休日を金曜日に振り替え。	情報セキュリティ技術演習Ⅰ	友人と都内に謎解きゲームに出かけるなどでリフレッシュ。今後、大学院の課題提出などが増えたら勉強に充てることも
4					大学院の課題や研究のほか、息抜きに謎解きにも取り組む		
5		稲葉研究室のゼミに参加 17時30分～19時（オンライン）	情報セキュリティ輪講Ⅰ	リスクマネジメントと情報セキュリティ（オンライン）			
6			ソフトウェア構成論	法学基礎（オンライン）		大学院の研究室で自習または先輩に研究の進め方を相談	
α	家事は平日の空き時間にこまめに片づける。業務もリモートワーク中心で時間調整がしやすい						

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>水曜日の「情報セキュリティ輪講」は毎回3名の学生が発表。参加者からの質疑応答で理解を深められる。2>大学院に登校する日は授業の前後を院生室で過ごす。研究について自分とは異なる視点からアドバイスを受けることも。

私の1週間

◉実務経験が豊富な教員による業務に役立つ授業も多数受講

授業は技術とマネジメントをバランスよく学ぶサイバーセキュリティとガバナンスコースを参考に履修。「情報セキュリティ輪講」は毎回3名の学生が研究発表を行い、私の業務に関連したテーマでは前のめりになりますし、異なる分野では新たな知識が得られるのが魅力。各自がリスクマネジメントに関連したテーマで発表する「リスクマネジメントと情報セキュリティ」では仕事上の課題を選ぶ学生も多く、企業のセキュリティ対策を行う私の業務にも役立ちそうです。

土曜日の「セキュリティシステム監査」は監査の実務に携わる第一人者が実例を用いて教えてくれ、「情報セキュリティ技術演習」では仮想環境での攻撃と防御をセキュリティ対策のためのレッドチームで活躍する方から学べます。

◉対面とオンラインのバランスで仕事と勉強を両立しやすい環境

今は週4日の授業で登校は2日のみ。仕事も月曜日以外はリモートワークで、授業の日の業務は16時までになるなど、ＩＩＳＥＣの学びやすさ、勤め先の働きやすさのおかげで、仕事と授業と家事をやりくりして充実した毎日を送っています。今後は課題も増えるので、時間をうまく管理しながら新たな人間関係や知識を広げたいと思います。

◉マネジメントや法制度の観点から学んだセキュリティを業務に生かす

大学で情報セキュリティを扱う研究室に所属し、入社後はＳＯＣチームのアナリストとして企業へのＵＴＭ・ＩＰＳの導入や運用を担当してきました。技術者としてだけでなく、案件責任者の役割を期待されるようになる中で、マネジメントの視点からお客さまに提案する力、自社で新たなサービスを考える力などの必要性を感じ、法律やマネジメントの観点でもセキュリティを学べるＩＩＳＥＣに入学しました。

社会人学生が中心で、さまざまな組織のセキュリティ対策について話が聞けて興味の幅が広がりますし、バックグラウンドや経験の違いから研究の相談ができる人が身近にいるのは頼もしいですね。

◉不足するセキュリティ人材謎解きを切り口に人材の育成を

私は「情報セキュリティ人材の育成」を研究テーマとしており、趣味でもある謎解きゲームの愛好家はセキュリティ分野に適性があるのではとの仮説を検証予定。サイバーセキュリティ心理学が専門の稲葉先生の指導の下で研究を進めていますが、やりたいテーマに適した先生が見つかるのもＩＩＳＥＣの幅広さだと思います。

謎解きと、与えられた課題を解いて正解を探すＣＴＦの近似性が研究の発端ですが、類似した先行研究も意外と多く、今はそれらの論文が私の研究にどのように生かせるかを精査しています。

■在学生インタビュー

入学して実感した大学院の魅力

量子コンピュータに耐える暗号の研究に加え セキュリティのスペシャリストとしても成長した。

松浦 栄亮さん
Eisuke MATSUURA
博士前期課程２年
帝塚山学院大学リベラルアーツ学部出身
（2024年4月入学）

PQC 有力候補だった方式の弱点を突いた方法をもとにした新たな暗号を研究中

大学時代から情報セキュリティに興味を持ち、PQC（耐量子計算機暗号）の必要性をまとめた卒業論文も執筆。さらにこの分野で専門性を高め、自分自身も成長したいと考えてIISECに入学しました。暗号を扱う3つの研究室の中でも理論寄りの有田先生の研究室に入り、PQCのうち公開鍵や秘密鍵サイズが小さい同種写像暗号を研究しています。この暗号は計算コストの高さの克服が急がれていますが、私の研究ではそうした計算の効率化に用いられる手法を応用して新たな暗号プロトコルを作り、プログラムの実装まで進める予定です。

研究集会やインターンシップでハイレベルな研究に触れる機会も

1年のときは同種写像の数学的な理論面を深掘りし、2年からは同種写像の暗号としての技術面を発表。研究室の学生や有田先生からのフィードバックをもとに理解を深めています。これ以外にIISECは学外での研究会やインターンシップの機会が多いのも特徴で、有田先生から私の研究内容に近いからと京都大学数理解析研究所の研究集会を紹介いただき、ISSスクエア主催のインターンシップでは富士通研究所で富岳に実装可能な環境を用いて仮想的な量子コンピュータによる既存の暗号への解読にチャレンジするなど、ハイレベルな研究にも携わることができました。

周囲の助けも得ながら研究を進められる環境

IISECでは仮想環境でネットワークへの侵入や防御を行う「情報セキュリティ技術演習」など実践的な科目も充実し、就職活動中の面接でセキュリティインシデントの対処を聞かれたときも具体的に回答できて高く評価されました。来年4月にはセキュリティエンジニアとして就職予定ですが、桑名先生の「クリティカル・シンキングとイノベーション」で学んだ多角的思考はビジネスの現場でも役立つと期待しています。最後に、これから入学する方は「毎日の積み重ねを大切に」「しっかり休息を取る」「何事も一人で抱え込まない」という3点を大事に学んでください。研究で行き詰まったときも、先生や研究室の学生と話せば違うアイデアが見つかったり気持ちが楽になったりします。周囲の助けが得られるのもIISECの良さなのですから。

量子コンピュータ実現が金融機関にもたらすリスクと 社会全体への影響を定量的に予測するモデルを検討。

村上 誠樹さん
Masaki MURAKAMI
博士前期課程1年
三井住友信託銀行株式会社
（2024年10月入学）

デジタル技術のセキュリティを習得するために入学

自動車メーカーでデータサイエンティストとして勤務した後、2022年に転職し、現在は当行のデータ利活用に向けたシステム開発に取り組んでいます。IISECに入学したのは、脆弱性診断に代表されるセキュア開発の知識を効率的に習得し、デジタル技術のセキュリティについて知見を深めることでキャリア形成の幅を広げるため。入学後は文理を超えた情報セキュリティの知識を幅広い授業から体系的に学べ、研究では後藤先生の指導のもと、量子コンピュータの実用化が金融機関にもたらすリスクを定量的な根拠から算出する予測モデルの構築を目指しています。

量子コンピュータ実現時を見据えたセキュリティ対策を政策提言に

重要インフラである金融機関の機能が継続停止した場合、そのリスクは社会全体に影響することから、予測の根拠にはマクロ経済の統計データを検討し、サイバー被害が日本経済にもたらす影響に関する先行研究を参考にしています。加えて、量子コンピュータ実現に備えてPQC（耐量子計算機暗号）への移行対応を促すアメリカ政府のホワイトペーパーや、専門機関による施策提言を評価し、適切な対策を実施するための指針も検討予定。最終的には、金融機関をはじめとした企業全体が適切にセキュリティ対策を進められることを目指し、第三者機関の認証制度を設けるなどの政策提言もまとめたいと考えています。

2年間で大きく成長できる機会が豊富

IISECには社会人学生が多く、官公庁からの派遣者や1990年代からIT業務に携わってきたベテランなど、多様なバックグラウンドを持つ方とのディスカッションで自身の知見も広がります。また暗号に関する理学系授業も多く用意されているため、専門的な知識も深掘りでき、ISSスクエアやSecCapでは他大学の授業も広く履修可能です。さらに後藤研のゼミでは、セキュリティ分野で活躍する修了生も参加し、在学生の研究内容を実務の視点からフィードバックをいただけるなど魅力的な教育環境です。これからの企業に必要なセキュリティ分野の知識や視座を身につけ、自分の成長を促す多くの刺激を得られる、唯一無二の大学院だと感じています。

■修了生からのメッセージ

セキュリティ業界の先輩たち

どの仕事でも必須となったセキュリティの知識。
大学での専門分野が違っても
興味とやる気があればここで学べます。

廣田 凪さん　Nagi HIROTA
情報セキュリティ研究科 博士前期課程修了
（伊藤忠テクノソリューションズ株式会社）

IISECで習得したセキュリティの考え方が
SIerの仕事で必要な知識の基礎になった

大学の講義やITパスポート試験をきっかけにセキュリティに興味を持ち、より深く勉強したいと考えてIISECに入学しました。大学で医療系と情報系の両分野を学んだことから、入学後は医療事務科の学生に向けた情報セキュリティ教育について研究。研究室はマネジメント系でしたが、授業は技術系も含めてどの分野でも受講できるので、大学時代には機会がなかった演習も数多く経験できました。

現在は商社系SIerのセキュリティエンジニアとして、主に顧客のセキュリティ運用に携わっています。実際の仕事では新しく学ぶことも多いのですが、IISECで身につけたセキュリティの考え方の基礎は活かせています。特に生成AIは業務の中でもよく聞くワードになっているため、今後も積極的に情報収集をしたいと考えています。

セキュリティ分野の幅広い科目が用意され
多様な知識を学びやすい環境

今やセキュリティの知識はどの業界、職種でも必須となり、セキュリティエンジニアに限らず、SEやIT系の職業以外でも役に立つ知識だと思います。ただ、セキュリティといっても幅広い内容があり、自分の専門以外はなかなか手を出しにくい部分もあるのは確か。その点、IISECではセキュリティに関する講義が多岐にわたって用意され、自分の研究に直接関係ない部分の講義も比較的気軽に学ぶことができます。研究のヒントになる場合もあるので、興味を持った分野は積極的に受講してみてください。大学で全くセキュリティを学ばなかった学生の方も、興味とやる気があれば大丈夫です。

IISECでの実践的な学習を活かし
オフェンシブ関連の業務を数多く担当。
「修了生」の経歴が信頼を得る機会にも。

大場 清さん　Kiyoshi OBA
情報セキュリティ研究科 博士前期課程修了
（監査系コンサルティングファーム勤務）

エンタープライズセキュリティ分野にも
広く役立つIISECでの学びと経験

学部生時代は法学部で国際法や情報法などを学んでいましたが、サイバーセキュリティ分野への強い関心から、体系的な学びを求めて情報セキュリティ大学院大学（IISEC）の門を叩きました。産官学が連携した教育体制はもちろん、様々な現場で活躍する社会人学生が多く集う、その多様性と実践的な学びに強く惹かれたのが入学の決め手です。

修了後は監査系コンサルティングファームに勤務し、多様な案件を経験してきました。

現在はレッドチーム演習やTLPTなどのオフェンシブ関連の案件を中心に担当していますが、IISECでの学びは、特定の専門的な業務にとどまらず、企業全体のセキュリティに関わる「エンタープライズセキュリティ」のあらゆる場面で活かされています。技術的な知識やシステムアーキテクチャ、セキュリティマネジメント、国内外の法規制動向といった、多角的かつ体系的な知見が、日々の業務の確かな基盤となっています。

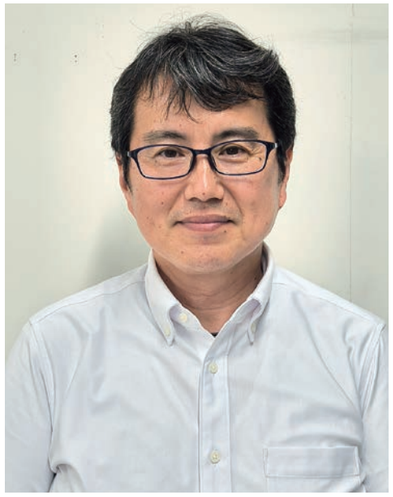
さらに、「IISEC修了生」という経歴が、お客様からの信頼獲得につながっていると実感する機会も数多くあります。

新たな脅威と向き合い学び続けて
困難を乗り越える醍醐味を感じてほしい

生成AI等の技術活用が広がり社会が変化する中で、「人々の安心・安全という普遍的な価値を守る」というセキュリティの役割は、ますます重要性を増していくと感じています。この分野は、常に新しい技術や脅威と向き合い、学び続ける必要がある挑戦的な世界です。多くの困難（Hard Things）もありますが、それを乗り越える達成感こそが、この分野の大きな醍醐味だと思います。

もし皆さんが、こうした挑戦に魅力を感じ、安心・安全な社会に貢献したいという想いがあれば、IISECは素晴らしい学びの場になると思います。

情報セキュリティは知的好奇心の塊。
IISECでの多くの学びが
新たな道を開く。



増山 一光さん　Kazumitsu MASUYAMA
情報セキュリティ研究科 博士後期課程修了
（嘉悦大学 准教授）

コンピュータウイルスからの復旧作業で
情報セキュリティ教育が不可欠と実感

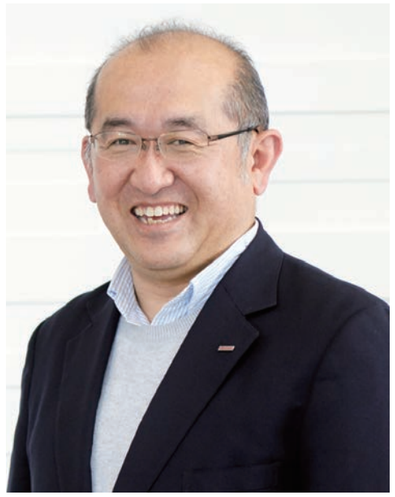
私は大学を卒業して、神奈川県の公立高等学校の教員（商業科）として勤務してきました。情報セキュリティとの出会いは、2001年に流行したコンピュータウイルス「Code Red」で、勤務していた高校内のパソコンのほとんどが感染したため駆除や復旧作業に追われました。この時の経験から、これからは情報セキュリティに関する知識や技能が不可欠であると痛感しました。

それから数年が経過した後に、情報セキュリティ大学院大学の存在を知って入学を検討。高校の教員としてフルタイムで勤務している中で、大学院で学ぶことには躊躇しましたが、通常勤務後に大学院の授業を受けることができ、さらに土曜日にも授業が設定されている時間割があると知って、学習環境を考慮して2008年度に入学を決めました。

高校生への情報セキュリティ教育を実践後
大学准教授という新たな道へ

修士課程では仕事、家庭、研究のバランスをとる必要があり、時間のやりくりが大変だろうと思っていました。ただ、入学後は授業や研究活動を通じて知的好奇心が高まっていたせいか、実際にはそれほどの苦労とは感じませんでした。修士課程修了後、博士課程に進むかどうかは本当に悩みましたが、これをチャンスと捉えて活かすべきだと思い進学。博士課程では「情報セキュリティ教育」を主眼に置いて研究活動を行い、2012年度に無事修了することができました。その後は、主に高校生に向けた情報セキュリティ教育の実践を続け、2025年度からは嘉悦大学の准教授として勤務しています。このように、私にとってIISECは情報セキュリティという学びを通じて、多くの人と出会え、新たな道を開いてくれた大学院です。ぜひ、みなさんも「はじめの一歩」を踏み出してください。

IISEC教員との出会いから
暗号学の体系的な学び直しを決意し、
デジタルIDの最先端の研究に没頭。



森山 光一さん　Koichi MORIYAMA
情報セキュリティ研究科 博士後期課程修了
（株式会社NTTドコモ）

そうだ、大学院に行こう。

慶應義塾大学大学院 理工学研究科 計算機科学専攻に学び、社会人になってから丸27年を迎えつつあった2021年1月、社内でのセキュリティ対策とグローバルでの標準化活動、そして国の検討会にも構成員（有識者）として招聘をいただくなど充実した時間を過ごしつつ、まだ自分に足りていないものがある認識がありました。そんなとき、コロナ禍にあってオンラインながらIISECの大塚玲先生とご一緒する機会があり（2021年1月）、そうだ、大学院博士後期課程に進もう、暗号学について体系的に学びなおし、最新のアプローチでデジタルアイデンティティの課題に向き合おうと思い、その日のうちに先生にメールをお送りしたのです。翌日、さっそくお返事をいただき、勇気づけられ、入学を決意し、研究に着手しました。

そして、グローバルに通用する最先端の研究

IISECでの日々は、フルタイムの社会人として時間の確保には苦労しましたが、大変充実したものでした。聴講というかたちで前期課程の学生に混ざって「情報セキュリティ」を支える領域を多面的に学びながら、博士演習として自身の専門分野と異なる領域の先生方（セキュリティ心理学・法務）からも直接の指導を受ける機会に恵まれました。そして、暗号学については数論基礎から暗号理論まで体系的に学びつつ、プライバシーを確保しながら不正対策を必須要件とするため、シビル耐性を有する自己主権型デジタルアイデンティティに関する研究に取り組みました。アカデミアにおけるグローバルでの最先端に導いてくださる先生方がいらっしゃるIISECで、皆さんも新しいチャレンジに向き合ってみてはいかがですか?

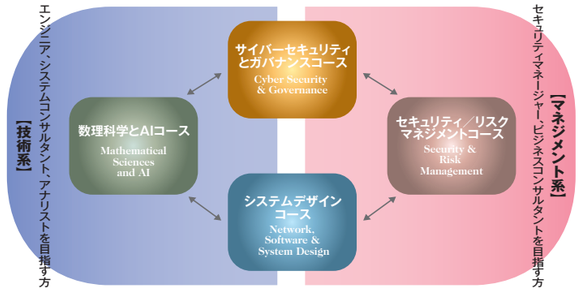
情報セキュリティ研究科
博士前期・博士後期

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。

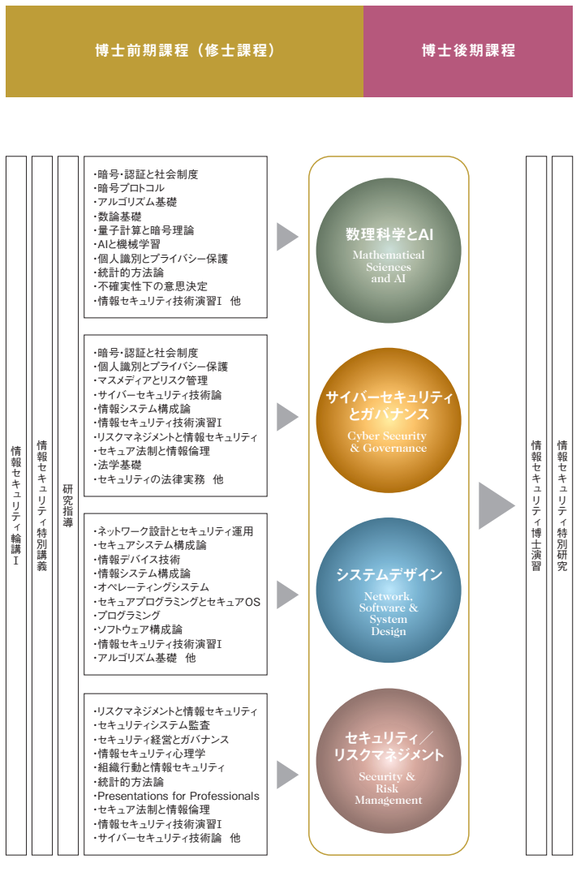
実社会における適正な情報セキュリティの実現には、暗号技術、ネットワーク技術、情報システム、管理運営、法制度、心理、情報倫理を融合させた総合的な対応が必要であり、それぞれの専門家が幅広い視野と見識をもって協力しあうことが不可欠です。情報セキュリティ研究科博士前期課程では、高度化・複雑化する企業・官公庁等の現場ニーズを踏まえ、技術系・マネジメント系とも幅広い人材育成需要、教育需要に応えるため、4つのコースフレームを設定しています。なお、指導教員の履修指導のもと、他のコースが推奨する科目も自由に履修することができます。博士後期課程では、博士前期課程修了の知識をベースに、情報セキュリティの構成要素に関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



■ 2025年度開設科目一覧

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	40	—
	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			
	量子計算と暗号理論	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			
	サイバーセキュリティ技術論	選択	2			
	ネットワーク設計とセキュリティ運用	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			
	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と情報セキュリティ	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			
	不確実性下の意思決定	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	情報セキュリティ演習	必修	6	22	—	—
	研究指導Ⅰ	必修	6			
	研究指導Ⅱ	必修	10			
	プロジェクト研究指導	必修	6	—	6	—
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Ⅰ	必修	1			
	情報セキュリティ博士演習Ⅱ	必修	1			
	情報セキュリティ博士演習Ⅲ	選択	1			
計				46	46	8

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
2024-2025



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

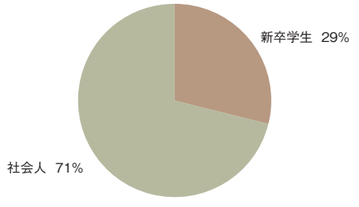
■ 社会人学生の所属組織

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】(2024-2025実績)
アクサ生命保険(株)／AIGビジネスパートナーズ(株)／エクシオグループ(株)／NTTテクノクロス(株)／NTTドコモソリューションズ(株)／NTTドコモビジネス(株)／海上保安庁／(株)エヌ・ティ・ティ エムイー／(株)NTTデータ先端技術／(株)NTTドコモ／(株)シーイーシー／(株)日本総合研究所／(株)日立システムズ／(株)三井住友銀行／キーウェアソリューションズ(株)／CryptoGames(株)／警察庁／サイバートラスト(株)／CTCテクノロジー(株)／JCOM(株)／ソニー(株)／(独)国立印刷局／日本生命保険相互会社／パナソニックホールディングス(株)／東日本旅客鉄道(株)／法務省／防衛装備庁／三井住友信託銀行(株)／八雲法律事務所　他

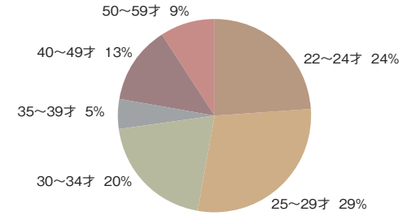
■ 現況

約7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。



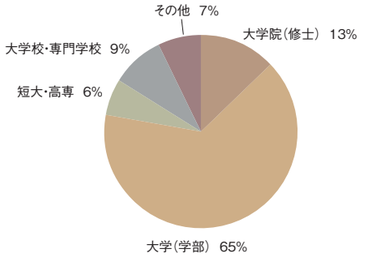
■ 年齢構成(入学時)

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】(2024-2025実績)
NTT(株)／(株)NTTドコモ／(株)ラック／警察庁／さくら情報システム(株)／東京都立産業技術大学院大学／パロアルトネットワーク(株)／日立ジョンソンコントロールズ空調(株)／弁護士(第一東京弁護士会)／法務省／防衛省／防衛大学校／三井住友ファイナンス&リース(株)　他

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］

［数理科学とAI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）／量子計算と暗号理論（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）／不確実性下の意思決定（2単位）
情報セキュリティ技術演習Ⅰ（2単位）
研究指導（22単位）＜必修＞

合　計　46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）
マスメディアとリスク管理（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）
リスクマネジメントと情報セキュリティ（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（22単位）＜必修＞

合　計　46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＞
ネットワーク設計とセキュリティ運用（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（22単位）＜必修＞

合　計　46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＞
リスクマネジメントと情報セキュリティ（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）／情報セキュリティ心理学（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（22単位）＜必修＞

合　計　46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	数理科学とAI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	○			
	量子計算と暗号理論	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	○	○	○	
	サイバーセキュリティ技術論	選択	2		○	○	○
	ネットワーク設計とセキュリティ運用	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			○	
	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と情報セキュリティ	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	○	○	○	○
	不確実性下の意思決定	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Ⅰ、研究指導Ⅱ 情報セキュリティ演習	必修	22	◎	◎	◎	◎

［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	46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	特定課題研究報告書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。

■ 他大学院等との交流協定

2025年7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

博士前期課程
（修士課程）

授業科目履修例
2025年度

▼＜学部新卒学生（ストレートマスター）の1年次履修例＞

◆前期（4月7日～8月2日）　※ が履修科目

	月曜日	火曜日	水曜日	木曜日（オンライン）	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				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		情報セキュリティ技術演習Ⅰ
4	アルゴリズム基礎	国際標準とガイドライン			数論基礎	
5	AIと機械学習	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ輪講Ⅰ	情報デバイス技術	特設講義（クリティカル・シンキングとイノベーション）	
6	ネットワーク設計とセキュリティ運用		ソフトウェア構成論	法学基礎	暗号・認証と社会制度	

◆後期（10月1日～2月9日）

	月曜日	火曜日	水曜日	木曜日（オンライン）	金曜日	土曜日
1						情報システム構成論
2	（研究指導）	暗号プロトコル				
3	（研究指導）			情報セキュリティ心理学	マスメディアとリスク管理	サイバーセキュリティ技術論 隔週開催
4	セキュリティ経営とガバナンス	セキュア法制と情報倫理	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	実践的IoTセキュリティ	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ特別講義	セキュアプログラミングとセキュアOS	Presentations for Professionals	
6	特設講義（ブロックチェーン理論）		情報セキュリティ輪講Ⅰ	セキュアシステム構成論	特設講義（データ・サイエンスとアナリティクス）	

▼＜社会人学生の1年次履修例＞

◆前期（4月7日～8月2日）　※ が履修科目

	月曜日	火曜日	水曜日	木曜日（オンライン）	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				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		情報セキュリティ技術演習Ⅰ
4	アルゴリズム基礎	国際標準とガイドライン			数論基礎	
5	知的財産制度 or AIと機械学習	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ輪講Ⅰ	リスクマネジメントと情報セキュリティ	特設講義（クリティカル・シンキングとイノベーション）	
6	セキュリティの法律実務 or ネットワーク設計とセキュリティ運用		ソフトウェア構成論	法学基礎	暗号・認証と社会制度	

◆後期（10月1日～2月9日）

	月曜日	火曜日	水曜日	木曜日（オンライン）	金曜日	土曜日
1						情報システム構成論 隔週開催
2	（研究指導）	暗号プロトコル				
3	（研究指導）			情報セキュリティ心理学	マスメディアとリスク管理	サイバーセキュリティ技術論 隔週開催
4	セキュリティ経営とガバナンス	セキュア法制と情報倫理	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	実践的IoTセキュリティ or 組織行動と情報セキュリティ	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ特別講義	セキュアプログラミングとセキュアOS	Presentations for Professionals	
6	特設講義（ブロックチェーン理論） or 不確実性下の意思決定		情報セキュリティ輪講Ⅰ	セキュアシステム構成論	特設講義（データ・サイエンスとアナリティクス）	

■ 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。※

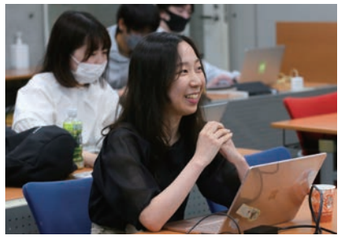
※博士前期課程の標準修業年限1年制プログラム（若干名）においては、平日昼間の通学も必要です。

※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講しています。

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）
社会人学生の
学びやすさ

働きながら修士学位取得を目指す社会人の皆さんへ



本学には、学部新卒のストレートマスターの学生はもちろんのこと、さまざまな組織・職域から多くの意欲的な社会人学生が集い、仕事を続けながら修士学位の取得を目指しています。
現職の社会人学生の就学への負担を軽減すべく、本学では開学当初より平日昼夜と土曜日に授業を開講している他、さまざまな取り組みを進めています。コロナ禍を経て蓄積したオンライン授業、ハイブリッド授業のノウハウを活かしつつ、対面授業による教育効果を重視し、カリキュラム全体としてバランスの取れた開講形態となるよう配慮しています。

■平日昼夜＋土曜日に授業を開講

平日昼間の授業科目の履修が難しい場合は、月～金の平日18:20からと、土曜日9:00から開講されている授業科目を履修して単位を修得することが可能です。

■特定曜日の授業はオンラインで開講

2022年度以降、毎週木曜日には、前期・後期あわせて8科目ほどの選択科目が開講されています。同曜日の授業科目は、一部を除き、原則として全ての回をオンラインで実施しています。

■必修授業科目はハイブリッドで受講可能

現在、水曜日の夜間に開講されている2つの必修科目「情報セキュリティ輪講Ⅰ（通年科目）」「情報セキュリティ特別講義（10月からの半期科目）」については、対面＋オンラインのハイブリッドで開講しており、2年制博士前期（修士）課程の社会人入試で合格された方は、オンラインでの受講も可能です（一般入試による入学者、1年制修士はオンライン受講対象外）。なお、情報セキュリティ輪講Ⅰで、自身が発表を担当する回については大学校舎への登校が必要となります。

■科目等履修生として一定の単位数を先取りすることが可能

本学では講義形式の選択科目を中心に、大学院正規課程の授業科目の一部を、科目等履修生として履修し、単位を修得することが可能です。これらの単位は、本学に正規の学生として入学した際、所定の条件※を満たせば、正規課程修了所要単位として認定されるとともに、科目等履修生として納入した履修料は学費の総額から差し引かれます。

※正規課程入学時点の学則に、当該科目あるいは等価科目が記載されていること。

■入学時期は4月または10月

本学の設置法人である学校法人岩崎学園による奨学金制度（年額500,000円の無利子貸与）は、有職の社会人も応募可能※です。

※詳細は、本パンフレットのp28および公式サイトにてご確認ください。

■厚生労働省教育訓練給付制度

2025年7月現在、博士前期課程、博士後期課程とも、厚生労働省教育訓練給付制度（一般教育訓練）の指定講座となっています。
課程修了後、受給資格等所定の要件を満たしている方がハローワークで申請を行った場合、支払った学費総額の20％相当額（上限10万円）が雇用保険から支給される制度です。

※本ページの情報は、2025年7月時点の実績・計画に基づいて掲載されています。

博士前期課程
（修士課程）
社会人学生の
通学パターン

教員と学生による濃密な学習、多様な交流を促進するため本学では対面授業を重視しています。
なお、多忙な社会人学生の皆さんは、オンライン開講の授業の活用を含め、
以下の週4日通学から週1日通学のパターンを参考に、学び方を検討してください。

■ 社会人学生の１年次履修例

通学　オンライン

▼【パターン1】対面受講メイン型（週４通学）

必修科目、選択科目、研究指導（ゼミ）とも、原則として大学校舎に通学して受講します。

【前期】（4月7日～8月2日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	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				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		情報セキュリティ技術演習Ⅰ
4	アルゴリズム基礎	国際標準とガイドライン			数論基礎	
5	知的財産制度	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ輪講Ⅰ	情報デバイス技術 or リスクマネジメントと情報セキュリティ	特設講義（クリティカル・シンキングとイノベーション）	
6	セキュリティの法律実務		ソフトウェア構成論	法学基礎	暗号・認証と社会制度	

【後期】（10月1日～2月9日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	金曜日	土曜日
1						情報システム構成論
2	（研究指導）	暗号プロトコル				
3	（研究指導）	セキュリティ経営とガバナンス		情報セキュリティ心理学	マスメディアとリスク管理	サイバーセキュリティ技術論（隔週）
4	セキュリティ経営とガバナンス	セキュア法制と情報倫理	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	実践的IoTセキュリティ or 組織行動と情報セキュリティ	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ特別講義	セキュアプログラミングとセキュアOS	Presentations for Professionals	
6	特設講義（ブロックチェーン理論）or 不確実性下の意思決定		情報セキュリティ輪講Ⅰ	セキュアシステム構成論	特設講義（データ・サイエンスとアナリティクス）	

▼【パターン2】バランス型（週2～3通学）

原則として大学校舎に通学して受講し、一部の選択科目についてはオンライン開講のものを履修します。

【前期】（4月7日～8月2日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	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				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		情報セキュリティ技術演習Ⅰ
4	アルゴリズム基礎	国際標準とガイドライン			数論基礎	
5	知的財産制度 or AIと機械学習	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ輪講Ⅰ	リスクマネジメントと情報セキュリティ	特設講義（クリティカル・シンキングとイノベーション）	
6	セキュリティの法律実務 or ネットワーク設計とセキュリティ運用		ソフトウェア構成論	法学基礎	暗号・認証と社会制度	

【後期】（10月1日～2月9日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	金曜日	土曜日
1						情報システム構成論
2	（研究指導）	暗号プロトコル				
3	（研究指導）	セキュリティ経営とガバナンス		情報セキュリティ心理学	マスメディアとリスク管理	サイバーセキュリティ技術論（隔週）
4	セキュリティ経営とガバナンス	セキュア法制と情報倫理	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	実践的IoTセキュリティ or 組織行動と情報セキュリティ	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ特別講義	セキュアプログラミングとセキュアOS	Presentations for Professionals	
6	特設講義（ブロックチェーン理論）or 不確実性下の意思決定		情報セキュリティ輪講Ⅰ	セキュアシステム構成論	特設講義（データ・サイエンスとアナリティクス）	

▼【パターン3】オンライン受講メイン＋週末通学型（週1通学）

必修科目（情報セキュリティ輪講Ⅰ、情報セキュリティ特別講義）をオンラインで履修（要申請）し、選択科目については、木曜日のオンライン開講のものを中心に、一部は土曜日の対面授業を履修します。研究指導については、指導教員と相談のうえ、オンラインでの指導をメインに研究を進めます。なお、オンライン受講メインのパターンでも、自身が担当となる必修科目での発表や修了のための審査は、原則として大学校舎で実施します。

【前期】（4月7日～8月2日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	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				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		情報セキュリティ技術演習Ⅰ
4	アルゴリズム基礎	国際標準とガイドライン			数論基礎	
5	知的財産制度 or AIと機械学習	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ輪講Ⅰ	リスクマネジメントと情報セキュリティ	特設講義（クリティカル・シンキングとイノベーション）	
6	セキュリティの法律実務 or ネットワーク設計とセキュリティ運用		ソフトウェア構成論	法学基礎	暗号・認証と社会制度	

【後期】（10月1日～2月9日）※木曜日の科目は原則として遠隔授業で、それ以外の曜日は対面授業として開講します。

	月曜日	火曜日	水曜日	木曜日（オンライン）	金曜日	土曜日
1						情報システム構成論
2	（研究指導）	暗号プロトコル				
3	（研究指導）	セキュリティ経営とガバナンス		情報セキュリティ心理学	マスメディアとリスク管理	サイバーセキュリティ技術論（隔週）
4	セキュリティ経営とガバナンス	セキュア法制と情報倫理	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	実践的IoTセキュリティ or 組織行動と情報セキュリティ	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	情報セキュリティ特別講義	セキュアプログラミングとセキュアOS	Presentations for Professionals	
6	特設講義（ブロックチェーン理論）or 不確実性下の意思決定		情報セキュリティ輪講Ⅰ	セキュアシステム構成論	特設講義（データ・サイエンスとアナリティクス）	

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。

数理科学とAI コース
Mathematical Sciences and AI

我々とともに数理を磨き、鍛えよう

◆コース概要

数理科学とAIコースでは、情報セキュリティに関わる数理的な諸問題に取り組みます。暗号技術はもちろんのこと、匿名化やデータプライバシー保護技術など幅広く扱います。昨今のAIや機械学習の発展は、これら数理的な情報セキュリティ課題に対する新しいアプローチを産んでいます。また、量子計算機の到来は暗号理論の基礎からの見直しを迫っています。伝統的な暗号技術を踏まえ、機械学習やAIの手法を取り込んだ、量子計算機時代の新たな情報セキュリティの数理科学の構築を共に目指しましょう。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、大学・研究機関、行政機関等において、高度エンジニア・研究職としての活躍が期待されます。

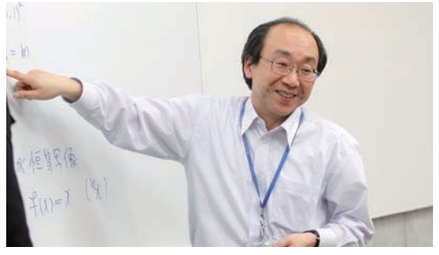
研究キーワード：深層学習、強化学習、数論アルゴリズム、耐量子計算機暗号、ゼロ知識証明、秘密分散、匿名化、差分プライバシー、他

◆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



情報セキュリティを支える暗号理論や機械学習には数理的なセンスと技術が欠かせません。量子計算機の登場も予想されますがその能力を引き出すには、ますます数理的なセンスが大切になるでしょう。我々と共に情報セキュリティに関わる数理的な諸問題に取り組み、数理的なセンスと技術を磨き、鍛えませんか?

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

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・運用管理などのシステム技術全般、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、AI応用（脆弱性検知、評価、マルウェア分類/検知/対策、攻撃検知/解析、フィッシング検知）、フォレンジック、セキュリティテスト、セキュアシステム、セキュアOS、欺瞞、仮想化環境、システム（組み込み/IoT/制御/Web/クラウド/ゲーム）セキュリティ、ゼロトラストアーキテクチャ、ハードウェアセキュリティ 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、セキュリティや安全性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。画期的なセキュリティ技術に挑戦したい方、また現在のシステムをよりセキュアに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

セキュリティに関する技術と法制度の両方に精通したスペシャリストへ

◆コース概要

本コースでは、サイバー攻撃の検知・分析・防御技術、脅威情報の収集分析技術などのセキュリティ技術と、個人情報保護法、不正アクセス禁止法、電子署名法などの法制度の両方に精通した人材を育成します。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・セキュリティなど、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など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、サイバーセキュリティ基本法、プライバシー保護、個人情報保護法、不正アクセス禁止法、電子署名法、国際法 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、評価して、学術論文にまとめます。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セキュリティに関する事例や判例・学説などを調査し、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

村上 康二郎 教授
Yasujiro MURAKAMI

サイバーセキュリティの確保は、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、セキュリティに関する法制度や国際的な状況など、幅広い知識が求められています。本コースでは、弁護士、公務員の方や、企業の法務部門・経営部門でセキュリティを担う方、コンサルティング会社でセキュリティのコンサルティングを担う方、CSIRTなどのアナリストを目指したい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

本コースでは、情報セキュリティリスクのマネジメントについて専門的な知識と応用力を身につけ、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。生き残りと発展を遂げるために組織が取り組むDXの成功のためにも、変革に伴う情報セキュリティリスクを適切に把握し対応するマネジメント力が不可欠です。その中には、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の知識が含まれます。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、レビュー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

稲葉 緑 教授
Midori INABA

クラウドやIoT、生成AIといった先進的な情報通信技術の普及により、利便性が飛躍的に高まる一方で、詐欺や偽情報の拡散といった新たな脅威が顕在化しています。こうした状況においては技術的対策に加え、組織における戦略的なセキュリティマネジメント、また、人間の脆弱性に対するアプローチが不可欠です。本コースではこのような課題に意欲的に取り組みたい方をお待ちしています。

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。

＊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。

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

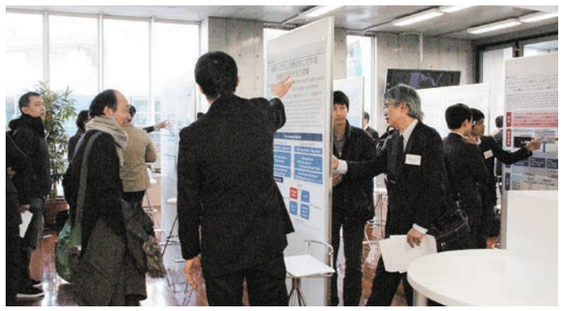
特にオプションプログラムは選択せず、各コースの履修標準科目を中心に履修して研究を進めるための知識の獲得や補強に努めるとともに、所属研究室での研究指導やディスカッションを通じて研究遂行能力を高め、在学中は修士論文作成に向けた研究に重点的に取り組みたい、という方を想定しています。神奈川県内の20以上の大学が加盟する大学院学術交流協定制度を利用して、研究テーマに関連する他大学院の開講科目を履修することも可能です。

▶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。
https://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（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。

講義・演習をサポートしてくれる卒業生の声

田中 恭之｜情報セキュリティ大学院大学 客員講師
NTT株式会社
（情報セキュリティ研究科博士前期課程および同博士後期課程修了）

IISEC では、博士前期および後期課程で5年間勉強させて頂き、主にマルウェア関連の研究をしていました。今回、客員講師のお話を頂き、少しでも貢献できればと思い担当させて頂くことになりました。慣れない面もありますが、講義資料も適宜ブラッシュアップして行きますので、よろしくお願いいたします。「特設講義（ハッキングとマルウェア解析）」で皆様にお会いするのを楽しみにしております。

羽田 大樹｜情報セキュリティ大学院大学 客員講師
NTTセキュリティ・ジャパン株式会社
（情報セキュリティ研究科博士前期課程および同博士後期課程修了）

大久保研究室にて研究指導を行い、また講義では「情報セキュリティ技術演習Ⅰ」「プログラミング」を担当しています。「情報セキュリティ技術演習Ⅰ」は、サイバー攻撃と対策をハンズオン形式で基礎から学ぶ内容で、私自身もセキュリティを学び始めたころ毎回楽しみに受講しており、この講義で基礎を固めることができました。研究も講義も、最新の動向を取り入れながら、実務と理論のバランスを重視して取り組んでいます。

宮本 久仁男｜情報セキュリティ大学院大学 客員講師
株式会社NTTデータグループ
（情報セキュリティ研究科博士後期課程修了）

私が担当する講義は、「Capture The Flag（CTF）入門と実践演習」です。こちらの講義は、キャンパスでの講義や演習だけでは完結せず、世の中で開催されているCTFに参加して、レポートを提出していただくことまでを実施内容に含みます。このため、講義に出席して課題や演習をこなすだけでは完結せず、何らかの形で外部で開催されている競技に参加していただく必要があり、通常の講義よりも自主性が求められます。CTFに参加することで、何がどうプラスになるか？参加するのに加えてを伝えられるように試みます。もし興味をお持ちいただけるようでしたら、参加をお待ちしております。

中山 幸郎｜情報セキュリティ大学院大学 客員講師
日本アイ・ビー・エム株式会社 X-Force Red
（情報セキュリティ研究科博士前期課程修了）

「情報セキュリティ技術演習Ⅰ」では、実際に現場で行われる技術に近い手法も取り入れながら座学とハンズオンを通してセキュリティの知識と技術力を磨く講義になっています。情報収集やマルウェア検知、Web アプリケーションやネットワークへの攻撃など幅広く学び、体験できるため他の授業で学んだ知識の定着にも繋がると考えます。その中で私は学生の皆様に楽しく最前線の学びを提供し、研究や仕事へ活かしていただきたいと思っています。

神橋 基博｜情報セキュリティ大学院大学 客員講師
株式会社三井住友銀行
（情報セキュリティ研究科博士後期課程修了）

「国際標準とガイドライン」および「セキュリティ経営とガバナンス」の2つの講義を担当します。これらの講義では、単なる知識の習得にとどまらず、ユースケースの検討、ディスカッションを通じて、実践的な理解を深めていただくことを重視しています。
各テーマに対して、「自分ならどう対応するか」という視点を持ち、他の受講者との意見交換を積極的に行ってください。多様な視点に触れることで、より深い洞察が得られるはずです。

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 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300名に上る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 https://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 https://www.seccap.jp/

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。

■ 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。

■ 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2024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。

■ 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

博士前期課程
（修士課程）

授業科目概要
2025

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、などの知識を修得するとともに、考え方やノウハウなども学ぶが、発表者にとっては、修士論文作成の重要な前段階作業でもある。本科目は必修科目である。

■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学び、その動向を把握する。さらに、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担っているかについて学ぶ。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理工学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前提とせず、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、高機能暗号のいくつかについても解説する。

■個人識別とプライバシー保護
本科目では、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・法制度的・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、法制度の視点と技術の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。

■ネットワーク設計とセキュリティ運用
インターネットや携帯電話は、高度な情報活用を可能とし、あらゆる生活シーンに不可欠なツールとなった。昨今では、公共体・民間企業におけるネットワークの構築や利用の巧拙は組織の存否を左右する程の重要事項となっている。また、情報セキュリティは何らかの形でネットワークの機能や性能に関わっていることが多い。以上から、インターネット等の高度なネットワーク技術と関連する情報セキュリティ技術を習得した技術者と管理者が広く望まれている。そこで、本講では、企業（プライベート）ネットワークを主対象に最新の要素技術を利用したネットワークシステムの設計・運用管理手法、昨今注目されている Zero Trust Network、および、クラウドと仮想ネットワーク技術について考えていくこととする。また、昨今、重要性が増しているネットワークセキュリティ事故対応チーム（CSIRT）の活動概要について学ぶ。

■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。Christopher M. Bishop & Hugh Bishop 著「Deep Learning: Foundations and Concepts」を教科書として機械学習の基礎理論から最近の深層学習の話題を講義する。最終回に期末テストと解説を実施する。

■実践的 IoT セキュリティ
各種センサーを搭載する小さなデバイスを数多くネットワークして、新しいサービスを提供する IoT のセキュリティが懸念されている。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、Io セキュリティを体得する。

■セキュアプログラミングとセキュア OS
社会の隅々にまで浸透したソフトウェアシステムは、サイバー攻撃に対して脆弱なことが多く、社会全体に大きな負の影響を与えている。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。

■情報セキュリティ技術演習Ⅰ
本授業は、「ネットワーク経由の情報セキュリティ攻撃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ことを目指す。また、その上で、セキュアなシステムの構築方法についても考察する。使用するコンピュータの OS は Windows と Linux である。

■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するとともに、情報セキュリティガバナンスの定義や全体像、ネットワーク社会の進展により複雑化する組織における情報セキュリティマネジメントを学ぶことにより、組織の経営とサイバーリスクの関係について学習する。さらに、演習を通し、自ら考え実践上の取組みへと展開する能力を身に着けることをねらいとする。

■情報セキュリティ心理学
本科目では、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、情報処理・判断における限界やバイアスなど、人が情報セキュリティにおいて望ましくない行動をとるメカニズムについて説明する。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。

■不確実性下の意思決定
情報セキュリティの分野においては、リスク＝事故の発生確率 x 事故による損失（これは、統計学的には期待損失と呼ばれるものである）と表わされることが多い。しかしこのリスクのとらえ方は必ずしも一般的ではない。リスクの本質はそれが不確実であること、そしてその発生と影響の大きさに「ちらばり」や「バラツキ」があることである。本講義では、リスクを経済学ではどうとらえるのかを明らかにした後、３段階（確実性・予測可能なリスク・予測不可能なリスク）での意思決定に関する理論の紹介をおこなう。さらに、意思決定において必ずしも合理的には行動できない人間を対象とした行動経済学や実験経済学の理論等を紹介する。授業は主に経済学を基本として進めるが、経済学の予備知識は必要としない内容である。なお、実験手法に基づくアクティブラーニングを授業の中に取り入れ、理論の検証もおこなう。

■セキュア法制と情報倫理
情報セキュリティを確保し、情報社会の安定をはかるためには、法制度だけではなく、倫理が実効的に機能することが必要である。法も倫理も規範の一種であるが、情報社会において発生する全ての問題を法制度によって完全に解決することは困難であるため、倫理的な対応も重要である。本授業は、情報セキュリティに関係する様々な問題を幅広く取り上げ、それらについて、法と倫理の両方の側面から、総合的に検討しようとするものである。

■Presentations for Professionals
The purpose of this course is to increase your ability to give simple and effective presentations in English on professional topics. The focus will be on gaining presentation and communication skills that improve your presentations in any language.This means that even if you lack confidence in your present English language skills—for example, pronunciation or grammar—you can still gain much from this course. If you have just basic English-speaking ability and a desire to improve your presentation skills, you can take this course. In it, you will learn skills that you can apply to presentations in your other language(s) too. Not only that! You will also discover that designing and presenting your original ideas can be fun and challenging. A recent student commented, “Through this class, I overcame my resistance to presentation preparation and learned how to prepare and give a good presentation.” Try it and see what you can do!（日本語での質問、相談も可能。）

■特設講義（データ・サイエンスとアナリティクス）
セキュリティ事故を想定した事業リスクマネジメントの一環として、セキュリティ対策における適切な仮説の設定や KPI 導入においても、データ・サイエンスやアナリティクスの知見・手法を活用することの重要性が高まっている。本科目においては、演習等を取り入れながら、モデリング、データ可視化、予測分析を始めとするデータ・サイエンスに関する実践的な知識を身に付けることを目的とする。

■特設講義（クリティカル・シンキングとイノベーション）
クリティカルシンキング（批判的思考）とは、「前提や常識を疑い、物事を多角的に考える」思考法であり、イノベーションの源泉となる。セキュリティ分野においても、セキュリティビジネスの開発、インシデントの予測・防止・対処・分析などの場面で、明示的または暗示的にクリティカルシンキングのアプローチが用いられている。本講義では、クリティカルシンキング、ロジカルシンキング、デザインシンキングの理論と実践手法を学び、それらがイノベーション創出やビジネスプロセス設計にどのように応用されるかを理解する。また、実例の紹介と分析を通じて、異なる視点から問題を捉え、多角的に考察する力を養う。講義はディスカッションを中心に進め、必要に応じてゲスト講師を招くこともある。

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

桑名　栄二

教授
Eiji KUWANA

■プロフィール
1984年電気通信大学大学院電気通信学研究科修士課程修了（計算機科学専攻）。1984年日本電信電話公社入社。NTT研究所にてソフトウェア工学、コンピュータネットワーク技術、CSCW、サイバーセキュリティ技術、クラウドコンピューティング技術等の研究開発等に従事。2010年NTT情報流通プラットフォーム研究所長、2012年NTTセキュアプラットフォーム研究所長。2013年NTT Innovation Institute, Inc., COO。2015年NTT先端技術総合研究所長。2016年NTTアドバンステクノロジ株式会社取締役、2021年NTTテクノクロス株式会社代表取締役社長。2023年9月から本学教授。2025年4月学長就任。2017年-2021年内閣府 総合科学技術・イノベーション会議 専門委員。2021年よりISC2（International Information Systems Security Certification Consortium）理事。博士（工学）（筑波大学、2000年）。

■主な研究業績
1. 佐藤亮太, 間形文彦, 高橋克巳, 桑名栄二:情報セキュリティの失敗事例における原因の類型化とその対策に関する考察, 情報処理学会論文誌, Vol.54, No.9, (2013)
2. 桑名栄二 他:広域災害対応型クラウド基盤構築に向けた研究開発（高信頼クラウドサービス制御基盤技術）, 総務省 ICTイノベーションフォーラム2013予稿集 (2013)
3. Herbsleb, J. D., Kuwana, E.,:An Empirical Study of Information Needs in Group Software Design, 情報処理学会論文誌, Vol.39, No.10, (1998)
4. Kuwana, E., et al.:Computer-supported meeting environment for collaborative software development, Information and Software Technology, Vol. 38, No.3, (1996)
5. Kuwana, E., Hervsleb, J. D.: Representing Knowledge in Requirements Engineering: An Empirical Study of What Software Engineers Need to Know. In Proc. of IEEE Requirement Engineering'93, (1993)

■主な研究テーマ
クラウドセキュリティ、DevSecOps
AI利用とセキュリティ、AIガバナンス
セキュリティ人材育成、セキュリティマネージメント、経営と情報セキュリティ、システムセキュリティ

■主な担当科目
情報システム構成論、国際標準とガイドライン、リスクマネジメントと情報セキュリティ、
セキュリティ経営とガバナンス、特設講義（クリティカル・シンキングとイノベーション）、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他

特別学長補佐

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。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を歴任。2011年7月より本学教授。2015年11月より内閣府SIPプログラムディレクター。日本学術会議連携会員（第23-24期）。2019年2月よりサイバーセキュリティ戦略本部員。2017年4月から2025年3月まで本学学長。

■主な研究業績
1. 小椋 顕義, 後藤 厚宏, 情報通信産業に対するサイバー攻撃による経済的波及被害の分析と考察, 電子情報通信学会論文誌D Vol.J108-A,No.1, 2025
2. 後藤 厚宏, デジタル依存時代に求められるサプライチェーンのレジリエンス, 情報処理学会 論文誌 Vol.65 No.9 2024
3. Taichi Aoki, Atsuhiro Goto, Graph visualization of dark web hyperlinks and their feature analysis, International Journal of Networking and Computing, 2021, 11.2
4. Kosuke Ito, Shuji, Morisaki, Atsuhiro Goto, IoT Security Quality Metrics Method and its Conformity with Emerging Guidelines, IoT 2021, 2(4)
5. 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
6. 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

■主な研究テーマ
- IoTとサプライチェーンセキュリティ
- インターネットセキュリティ技術
- 重要インフラのセキュリティと大規模リスク対応
- クラウド、ビッグデータ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、ネットワーク設計とセキュリティ運用、情報システム構成論、
国際標準とガイドライン、enPiT/SecCap特設講義と特設実習、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

情報セキュリティ研究科長

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。脅威分析研究会幹事、国際会議MW2SP2016オーガナイザー、SEのためのセキュリティ教育検討委員会主査、「東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究」検討委員会委員・航空ワーキンググループ主査、日本サイバー犯罪対策センター理事。

■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 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. The design of secure IoT applications using patterns: State of the art and directions for research Eduardo B. Fernandez, Hironori Washizaki, Nobukazu Yoshioka, Takao Okubo Internet of Things 15 100408-100408 (2021)
5. Hironori Washizaki, Tian Xia, Natsumi Kamata, Yoshiaki Fukazawa, Hideyuki Kanuka, Takehisa Kato, Masayuki Yoshino, Takao Okubo, Shinpei Ogata, Haruhiko Kaiya, Atsuo Hazeyama, Takafumi Tanaka, Nobukazu Yoshioka, G. Priyalakshmi Systematic Literature Review of Security Pattern Research, Inf. Vol.12, No.1, pp.1-27 (2021)

■主な研究テーマ
セキュリティ・バイ・デザイン、脅威分析、システムセキュリティ、Webセキュリティ AI応用（マルウェア解析、攻撃検知、脆弱性検知、フィッシング検知）、フィンガープリンティング応用、ゼロトラストアーキテクチャ導入、欺瞞システム、OSINT応用

■主な担当科目
ソフトウェア構成論、プログラミング、情報セキュリティ技術演習I、情報セキュリティ輪講I
研究指導I/II、（特設）脅威分析とリスク波及評価

■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

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. 清原達成, 有田正剛, カードベース暗号の量子計算による実現に関する研究, 情報処理学会研究報告 Vol.2025-CSEC-108 No.55, 2025/3.
2. 末吉璃子, 有田正剛, 深層強化学習によるナップサック問題の解法に関する研究, 2023年度人工知能学会全国大会, 2T1-GS-10-02, 2023/6.
3. 安光一平, 有田正剛, 符号ベースのマルチレシーバーKEMの構成について, 情報処理学会研究報告 Vol.2023-CSEC-100 No.6, 2023/3.
4. Seiko Arita, Sari Handa, Fully Homomorphic Encryption Scheme Based on Decomposition Ring, IEICE TRANS., Vol.E103-A,No.1,pp.195-211,Jan. 2020.

■主な研究テーマ
主な研究対象領域は:
- 格子暗号、符号ベース暗号、同種写像ベース暗号などの、耐量子計算機暗号の構成及び機械学習アルゴリズムを用いた解析
- 閾値復号、関数型暗号、完全準同型暗号など高機能暗号
- 鍵共有、コミットメント、ゼロ知識証明などの暗号プロトコル

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

■担当コース
数理科学とAIコース、サイバーセキュリティとガバナンスコース

専任

稲葉　緑

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年より情報セキュリティ大学院大学准教授。2025年4月より同教授。研究テーマは情報セキュリティに関して望ましい行動を支援するシステム・仕組みの検討。日本心理学会、情報処理学会等会員。現在、国土交通省運輸審議会運輸安全確保部会専門委員。情報処理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委員、総務省サイバーセキュリティ人材育成分科会構成員等を歴任。

■主な研究業績
1. 稲葉 緑,菊池大地, 情報セキュリティ対策停滞の心理的要因を考慮した中小金融機関向け対策促進策の検討, 62-12, 1926-1936, 2021年.
2. 稲葉 緑, 情報化社会におけるリスクコミュニケーション, 安全工学, 58-6, 439-445, 2019年.
3. 稲葉 緑, 主観的リスク認知, ヒューマンエラーの発生要因と削減・再発防止策,技術情報協会, 47-57(第2章第1節), 2019年.
4. 稲葉 緑, 鉄道分野におけるヒューマンエラー教育, システム/制御/情報, 61-6,226-232, 2017年.
5. Inaba, M., Shirai, I., Kusukami, K., Haga, S. Development of interactive educational game about human error — In a case of developing a serious game to learn slips — P.Carvalho, P. Arezes (共編), Ergonomics and Human Factors in Safety Management, CRC Press, Chapter 12, 253-270, 2016年.

■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、情報セキュリティ特別講義、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

大塚　玲

教授
Akira OTSUKA

■プロフィール
1991年大阪大学工学研究科博士前期課程修了。同年より野村総合研究所。2002年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）。2005年4月より2017年3月まで産業技術総合研究所。2017年4月より情報セキュリティ大学院大学教授。2006-2010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。2007-2014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（2009-2011）,城西大学理学部数学科非常勤講師（2015-2022）,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)。大阪大学大学院工学研究科非常勤講師（2022-）。日本銀行金融研究所客員研究員(2020-2021)。電子情報通信学会シニア会員,情報処理学会シニア会員,IEEE,IACR,IFCA各会員。電子情報通信学会バイオメトリクス研究専門委員会顧問,人工知能学会安全性とセキュリティ研究会（SIG-SEC）主査。JNSAサイバーセキュリティ産学連携協議会代表。

■主な研究業績
1. Koichi Moriyama, Akira Otsuka, "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors," IEICE Transactions on Information and Systems, Vol.E107-D, No.9, Sep. 2024 (to appear).
2. Yuhei Otsubo, Akira Otsuka and Mamoru Mimura, "Compiler Provenance Recovery for Multi-CPU Architectures Using a Centrifuge Mechanism." IEEE Access 12, 34477–34488 (2024).
3. Hiroaki Maeshima and Akira Otsuka, "Robustness Bounds on the Successful Adversarial Examples: Theory and Practice." Preprint at http://arxiv.org/abs/2403.01896 (2024).
4. Taishi Higuchi and Akira Otsuka, "Electronic Cash with Open-Source Observers," Proceedings of The 3rd Workshop on Decentralized Finance (DeFi '23) in Association with Financial Cryptography 2023.
5. Minami Someya, Yuhei Otsubo and Akira Otsuka, "FCGAT: Interpretable Malware Classification Method using Function Call Graph and Attention Mechanism," Proceedings of NDSS Workshop on Binary Analysis Research (BAR2023).
6. Taisei Takahashi, Taishi Higuchi and Akira Otsuka, "VeloCash: Anonymous Decentralized Probabilistic Micropayments With Transferability," in IEEE Access, vol. 10, pp. 93701-93730, 2022.

■主な研究テーマ
AIセキュリティ, 大規模言語モデル・生成AI、暗号理論、デジタル通貨（CBDC）やブロックチェーン
自己主権型デジタルアイデンティティに関する研究

■主な担当科目
AIと機械学習,アルゴリズム基礎（計算複雑性理論）,特設講義（ブロックチェーン理論）,
暗号・認証と社会制度,研究指導

■担当コース
数理科学とAIコース

兼任
上沼　紫野
客員教授
Shino UENUMA

■プロフィール
LM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。こども家庭庁少年インターネット環境の整備等に関する検討会委員。サイバーセキュリティ戦略本部員（2023～2025）
■担当科目
セキュリティの法律実務
個人識別とプライバシー保護

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。現在は、IoTセキュリティにおける標準化を推進するとともに、CTF形式による実践的なセキュリティ教育活動に従事。
■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
東京理科大学専門職大学院嘱託教授
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～24年東京理科大学専門職大学院教授。現在、総務省国立研究開発法人審議会委員、総務省国立研究開発法人審議会・宇宙航空研究開発機構部会委員、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。サンケン電気株式会社社外取締役（23～24年）、社外取締役・監査等委員（25年～）。株式会社マナック・ケミカル・パートナーズ社外取締役（24年～）。TRY国際弁理士法人顧問弁理士（25年～）。
■担当科目
知的財産制度

兼任
小林　良樹
客員教授
Yoshiki Kobayashi

■プロフィール
明治大学公共政策大学院特任教授。博士（学術）（早稲田大学）。
1987年東京大学法学部卒業後、警察庁入庁。在米国日本国大使館参事官、内閣官房内閣審議官（内閣情報調査室）等を経て2019年3月退官、同年4月より現職。専門はインテリジェンス研究。防衛大学校非常勤講師（2018年～）。
■担当科目
セキュリティの法律実務、個人識別とプライバシー保護、
セキュア法制と情報倫理、特設講義（脅威分析とリスク波及効果）

兼任
柴山　悦哉
客員教授
Etsuya SHIBAYAMA

■プロフィール
大学共同利用機関法人 情報・システム研究機構 理事
東京大学 特命教授
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、東京大学教授を経て2024年4月より同特命教授、2025年4月より情報・システム研究機構理事。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）。東京大学名誉教授、東京工業大学（現東京科学大学）名誉教授。
■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
1989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
高橋　雅夫
客員教授
Masao TAKAHASHI

■プロフィール
公立大学法人 長野大学 企業情報学部 教授
総理府（統計局）、総務庁（統計センター、統計局、行政監察局等）、総務省（統計局、政策統括官室等）、独立行政法人 統計センター 情報技術センター長を経て2021年より現職。筑波大学大学院システム情報工学研究科修了。博士（工学）。
■担当科目
特設講義（データ・サイエンスとアナリティクス）

兼任
種茂　文之
客員教授
Fumiyuki TANEMO

■プロフィール
NTTアドバンステクノロジ株式会社
ソーシャルプラットフォーム・ビジネス本部　エグゼクティブスペシャリスト
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、情報セキュリティコンサルティングやサイバー演習支援サービスの提供業務等に従事。
■担当科目
特設実習（セキュリティ実践Ⅰ、Ⅱ）
ネットワーク設計とセキュリティ運用

兼任
辻　秀典
客員教授
Hidenori TSUJI

■プロフィール
株式会社Premo 代表取締役 Founder CEO
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。2020年にCPS/IoT時代を見据えた半導体設計スタートアップの株式会社Premoを東大教授らと共同設立。同年、セキュリティの専門家として総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会の立ち上げに貢献。2022年よりデジタル庁 マイナンバーカードの機能のスマートフォン搭載等に関する検討会オブザーバー、同事前検討会有識者。2024年総務省不適正利用対策に関するワーキンググループ 構成員。
■担当科目
セキュアシステム構成論

兼任
藤澤　美恵子
客員教授
Mieko FUJISAWA

■プロフィール
金沢大学人間社会研究域教授
東京工業大学大学院修了（博士（工学））、一橋大学経済研究所、金沢星稜大学等を経て2015年より現職。都市経済学・実験経済学の教育に従事。情報の非対称性を踏まえた住宅選択行動や環境配慮行動を促すフレーミング等を主に研究。2020年都市住宅学会論文賞受賞他。
■担当科目
不確実性下の意思決定
リスクマネジメントと情報セキュリティ
セキュリティ経営とガバナンス
特設講義（クリティカル・シンキングとイノベーション）

兼任
藤村　明子
客員教授
Akiko FUJIMURA

■プロフィール
NTT株式会社 NTT社会情報研究所 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、プライバシー保護等の法律及び情報技術に関する学際分野の研究開発に従事。現在、地方公共団体情報システム機構(J-LIS)認証業務情報保護委員会委員等を兼務。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
個人識別とプライバシー保護

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・大学院商学研究科特任教授
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、システム監査学会副会長、日本ガバナンス研究学会（旧日本内部統制研究学会）理事、情報処理技術者試験委員、会計検査院情報公開・個人情報保護審査会委員、金融庁・企業会計審議会委員（監査部会長・内部統制部会長）、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、情報処理推進機構契約監視委員会委員、日本公認会計士協会監査・保証基準委員会有識者懇談会議長、日本内部監査協会名誉会員などを兼任。『裏話不正一最前線』（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）
PwCコンサルティング合同会社　パートナー
1992年大手監査法人に入社。1998年より2000年まで米国の会計事務所に勤務。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。2020年6月より現職。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、サイバーセキュリティ経営ガイドライン策定委員会、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
盛合　敏
客員教授
Satoshi MORIAI

■プロフィール
NTTテクノクロス株式会社 専任マネージャー
東北大学大学院工学研究科情報工学専攻博士課程修了、工学博士。日本電信電話株式会社（現NTT株式会社）に入社、NTT情報通信処理研究所、株式会社ぶららネットワークス、NTTソフトウェアイノベーションセンタ等を経て、2013年より現職。その間、神奈川大学、慶應大学、日本工業大学の非常勤講師を兼任。オペレーティングシステム（リアルタイムOS、セキュアOS）、インターネット、分散ストレージ、クラウド基盤の研究開発、および、これらの技術を活用した大規模システムの構築運用やセキュリティオペレーションに従事。
■担当科目
オペレーティングシステム

兼任
森井　昌克
客員教授
Masakatu Morii

■プロフィール
神戸大学名誉教授
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。2024年まで神戸大学大学院工学研究科教授。現在、近畿大学情報科学研究所サイバーセキュリティ部門長。日本医療研究開発機構(AMED)プログラムスーパーバイザー。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、開発に従事。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、2020年情報セキュリティ文化賞受賞、2024年総務大臣表彰。電子情報通信学会フェロー。
■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
Professor, Tohoku University(ret.)
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総合研究所リサーチフェロー
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『ゼロからわかる量子コンピュータ』（講談社現代新書、2022年）、『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
塩月　誠人
客員講師
Makoto SHIOTSUKI

■プロフィール
ITセキュリティコンサルタント
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年より16年間セキュリティ教育事業を行う合同会社を経営、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2025年7月現在

専任
須崎　有康
教授
Kuniyasu SUZAKI

■プロフィール
1991年東京農工大学大学院博士後期課程中退。同年、通商産業省工業技術院電子技術総合研究所に入所。1997-8年オーストラリア国立大学の客員研究員。2001年改組により国立研究開発法人産業技術総合研究所。2001年イリノイ大学アーバナ・シャンペーン校の客員研究員。2009年東京大学より博士（情報理工学）。2022年9月より本学教授。2010年IPA日本OSS貢献者賞。2019年よりTCG Invited Expert。

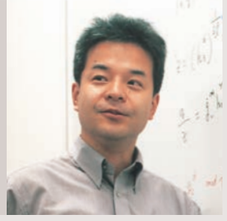
■主な研究業績
1. Taichi Takemura, Ryo Yamamoto, Kuniyasu Suzaki, TEE-PA: TEE Is a Cornerstone for Remote Provenance Auditing on Edge Devices With Semi-TCB, IEEE Access, 2024
2. Kuniyasu Suzaki, Kenta Nakajima, Tsukasa Oi, Akira Tsukamoto, TS-Perf: General Performance Measurement of Trusted Execution Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone, IEEE Access, 2021.
3. Kuniyasu Suzaki, Akira Tsukamoto, Andy Green, Mohammad Mannan, Reboot-Oriented IoT: Life Cycle Management in Trusted Execution Environment for Disposable IoT devices, Annual Computer Security Applications Conference (ACSAC), 2020.
4. Nguyen Anh Quynh, Kuniyasu Suzaki, VirtICE: Next Generation Debugger for Malware Analysis, BlackHat USA, 2010.
5. 須崎有康, IPA未踏事業, KNOPPIXホスティング環境, 2003, どこからともなくブートするOS, 2004.

■主な研究テーマ
システムソフトウェアセキュリティ、ハードウェアセキュリティ
Confidential Computing, Trusted Execution Environment, TPM(Trusted Platform Module)およびSE(Secure Element)を使ったセキュリティ

■主な担当科目
オペレーティングシステム、情報デバイス技術、情報システム構成論、実践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、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。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。

■主な研究業績
1. New Proof Techniques Using the Properties of Circulant Matrices for XOR-based(k, n) Threshold Secret Sharing Schemes, K. Shima, H. Doi, Journal of Information Processing Technical Note, Vol.29, pp.266-274 (2021).
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、アルゴリズム基礎、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
数理科学とAIコース、システムデザインコース

専任
村上　康二郎
教授
Yasujiro MURAKAMI

■プロフィール
1994年慶應義塾大学法学部法律学科卒業、1998年同大学院法学研究科修士課程修了、2002年同博士課程単位取得退学、2009年情報セキュリティ大学院大学博士課程修了。博士（情報学）、修士（法学）。東京工科大学専任講師、同准教授、同教授を経て、2022年4月に情報セキュリティ大学院大学教授に着任。これまで、慶應義塾大学湘南藤沢キャンパス非常勤講師、経済産業省・総務省などの政府関係委員会の委員長・委員、情報ネットワーク法学会理事などを歴任。現在は、ISO/IEC JTC1 SC27/WG5委員などを務める。

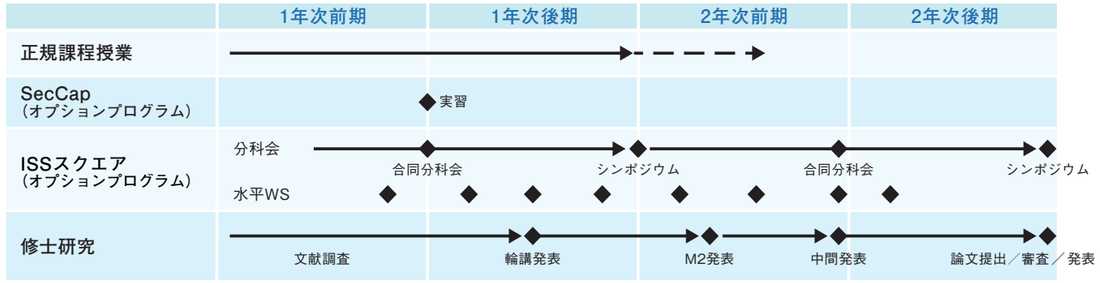
■主な研究業績
1. 村上康二郎「プライバシー権論における信認義務説の再検討」情報セキュリティ総合科学15号1～18頁（2025年）
2. 村上康二郎「情報プライバシー権の類型化に向けた一考察」情報通信政策研究第7巻第1号Ⅱ-1～Ⅱ-22頁（2023年）
3. 村上康二郎「プライバシー権に関する信認義務説と多元的根拠論」情報ネットワーク・ローレビュー第21巻28～47頁（2022年）
4. 村上康二郎「現代情報社会におけるプライバシー・個人情報の保護」（日本評論社、2017年）
5. 村上康二郎「プライバシー影響評価（PIA）に関する国際的動向と我が国における課題」情報ネットワーク・ローレビュー第13巻33～56頁（2014年）

■主な研究テーマ
情報セキュリティの法律問題に関する研究
プライバシー権に関する法理論的な研究
個人情報保護法制に関する研究

■主な担当科目
セキュリティの法律実務、法学基礎、セキュア法制と情報倫理

■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

■ 入学から修了までの流れのおおよそのイメージ［博士前期（修士）課程2年制プログラム］



■ 主な行事

● 新入生オリエンテーション

教育研究指導方針の説明や各種手続きについてのお知らせ、校舎案内等により、今後本学で学んでいくにあたっての準備をします。

● ホームカミングパーティ

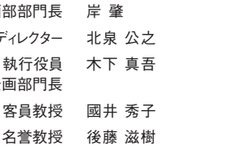
年に2回開催されるホームカミングパーティでは、OB・OGはもちろんのこと、多くの教職員、在学生等も参加し、交流を深めます。

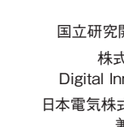
● 学位論文等発表会

研究成果の集大成となる修士論文・博士論文等の発表会が8月、2月に開催されます。

● 学位記授与式

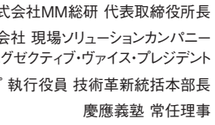
学長から修了生一人一人に学位記が授与されるとともに、優れた研究成果を上げた学生に対して表彰状と記念品が贈られます。

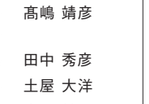


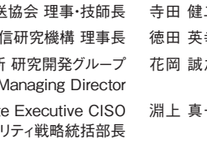


● 修了記念パーティ

当該度修了生に加え、過年度の修了生も参加し、にぎやかに開催しています。







■ 情報セキュリティ大学院大学連携教授（2025年7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 総合研究所 AIデジタルR&Dセンター セキュリティ基盤研究部 エキスパート	秋山 浩一郎	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	田中 良夫
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 研究所長	井上 大介	日本電気株式会社 グローバルイノベーション戦略部門 シニアプロフェッショナル	谷 幹也
株式会社日立製作所 研究開発グループ サービスシステムイノベーションセンタ 主管研究長	鍛 忠司	富士通株式会社 富士通研究所 フェロー SVP	津田 宏
株式会社KDDI総合研究所 取締役執行役員 副所長	清本 晋作	日本電信電話株式会社 NTT社会情報研究所 所長	中嶋 良彰
日本アイ・ビー・エム株式会社 東京基礎研究所 ハイブリッドクラウド&セキュリティ担当部長	佐藤 史子	パナソニック ホールディングス株式会社 テクノロジー本部 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部 部長	中野 学
沖コンサルティングソリューションズ株式会社 シニアマネージングコンサルタント	杉尾 俊之	三菱電機株式会社 開発本部 開発本部 主席技監	松井 充
国立情報学研究所 アーキテクチャ科学研究系 教授	竹房 あつ子	国立研究開発法人産業技術総合研究所 フェロー	松本 勉
		早稲田大学 理工学術院総合研究所 上席研究員/研究院教授	吉岡 信和

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（2025年7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。

国立大学法人 東京大学 特命教授	相田 仁	日本経済新聞社 編集委員	須藤 龍也
横浜市 副市長	伊地知 英弘	株式会社MM総研 代表取締役所長	関口 和一
早稲田大学 研究院 教授	遠藤 典子	パナソニック コネクト株式会社 現場ソリューションカンパニー エグゼクティブ・ヴァイス・プレジデント	髙嶋 靖彦
三菱電機株式会社 上席執行役員 知的財産担当 研究開発本部長	岡 徹	株式会社NTTデータグループ 執行役員 技術革新統括本部長	田中 秀彦
NTTドコモビジネス株式会社 取締役 執行役員 経営企画部長	奥澤 慎哉	慶應義塾 常任理事	土屋 大洋
沖電気工業株式会社 情報企画部部門長	岸 肇	日本放送協会 理事・技師長	寺田 健二
富士通株式会社 セキュリティ本部 CISO戦略統括部 シニアディレクター	北泉 公之	国立研究開発法人情報通信研究機構 理事長	徳田 英幸
NTT株式会社 執行役員 研究開発マーケティング本部 研究企画部門長	木下 真吾	株式会社日立製作所 研究開発グループ Digital Innovation R&D Managing Director	花岡 誠之
芝浦工業大学 客員教授	國井 秀子	日本電気株式会社 Corporate Executive CISO 兼 サイバーセキュリティ戦略統括部長	淵上 真一
早稲田大学 名誉教授	後藤 滋樹	株式会社日立ソリューションズ セキュリティソリューション事業部 セキュリティサイバーレジリエンス本部チーフセキュリティアナリスト	米光 一也
株式会社東芝 特別嘱託	斉藤 史郎		
独立行政法人情報処理推進機構 理事長	齊藤 裕		
神奈川県 副知事	首藤 健治		

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・実験室は平日は夜22時30分まで、土曜日は夜21時30分まで開放しています。（2025年度）

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。


唐沢 勇輔
情報セキュリティ大学院大学
第4代同窓会長

情報セキュリティ研究科
博士前期課程2013年度修了（田中研究室）

Japan Digital Design株式会社
Head of TDD 兼 VP of Security

同窓会では、会員同士のつながりを深める「IISEC Alumni Reunion」やIISEC現役生向けの合同企業説明会の開催、大学主催イベントへの協力など、いろいろな活動を行っています。卒業年次や研究室に関係なく、誰でも気軽に参加できるオープンでフラットなコミュニティを目指しています。
興味のあるイベントがあれば、ぜひ気軽に参加してみてください。皆さんにお会いできるのを楽しみにしています！

■ 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。





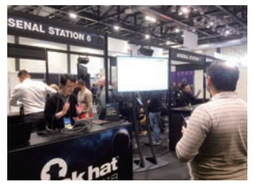
Refresh and enrich

■ 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。



■ 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。） https://www.jasso.go.jp/

種別	貸与月額（※2025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
特別学長補佐・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。
研究メンバーには、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
日本サイバーディフェンス株式会社
シニアエグゼクティブアドバイザー

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

1Fホールでのweekday tea-time

新入生歓迎パーティ

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。

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

https://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

Japan University Accreditation Association
UNIVERSITY ACCREDITED
2024.4～2031.3

学校法人 岩崎学園

■Contents

■学生募集課程概要

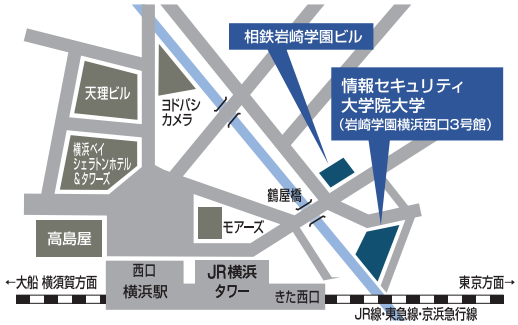
研究科	専攻	課程	標準修業年限	募集人員
情報セキュリティ研究科	情報セキュリティ専攻	博士前期（修士）課程［2年制］	2年	40名
		博士前期（修士）課程［1年制］	1年	若干名
		博士後期課程	3年	8名

詳細は本学ウェブサイトでご確認ください。

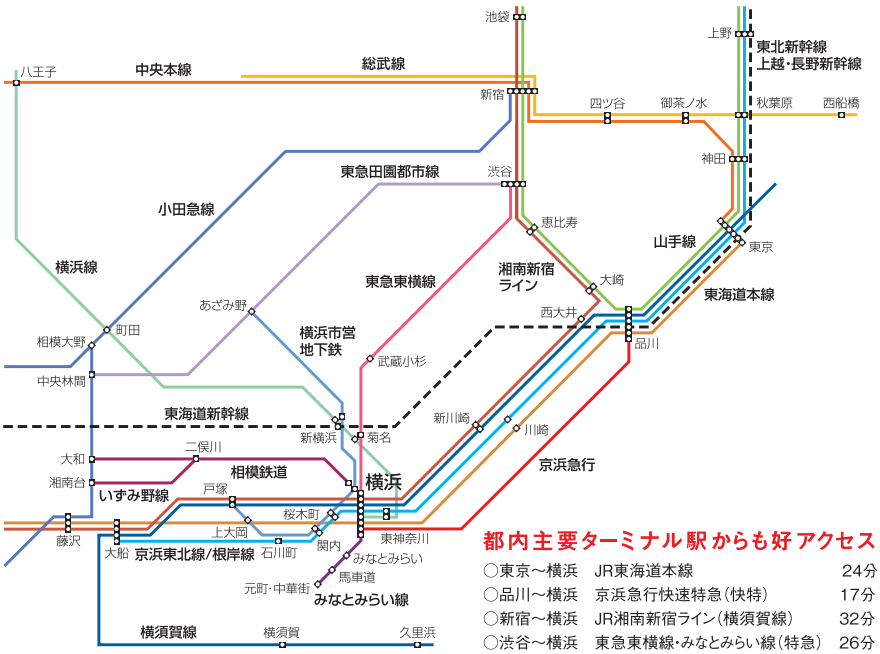
■入学者選考方法

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