学校法人 岩崎学園

明日の信頼を創ろう。

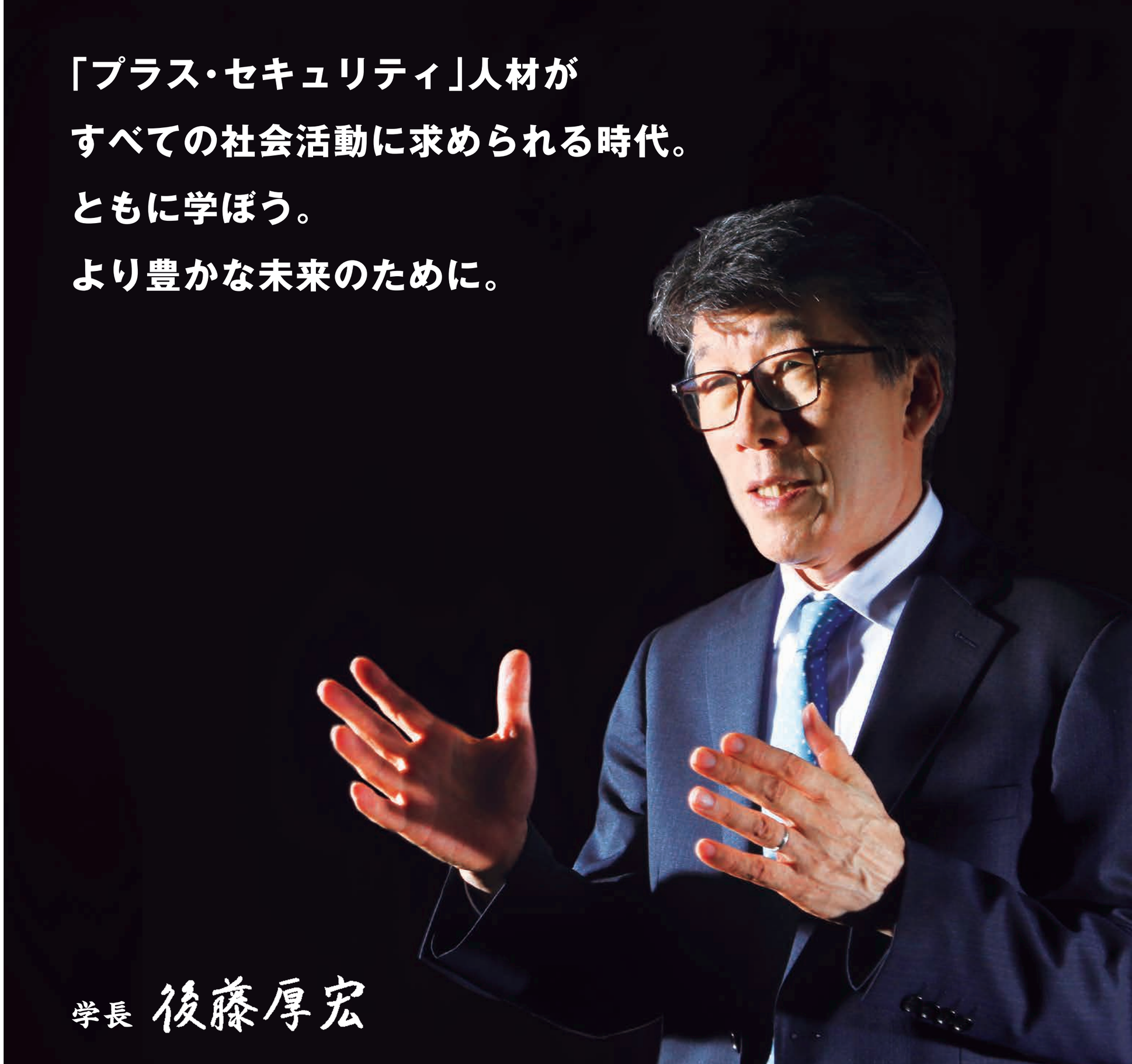
情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

2022-2023

Si vous vous intéressez à...

「プラス・セキュリティ」人材が
すべての社会活動に求められる時代。
ともに学ぼう。
より豊かな未来のために。



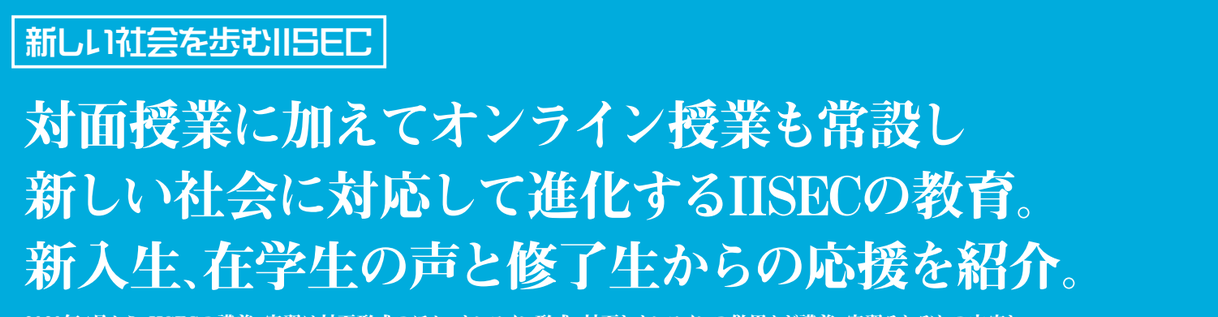
学長 後藤厚宏

人口減少や環境政策の対応など、さまざまな課題を抱える日本では、各産業や行政の分野でDXによる業務変革の必要性が以前から言われていました。コロナ禍を経て、その動きはますます加速するでしょう。一方、すべての社会活動でDX化を進めるには、「プラス・セキュリティ」人材の大幅な不足が指摘されています。これはデジタル化された業務に必要なセキュリティのスキルを持つ人材を指し、必要となる業界は金融、流通、観光、製造、医療・福祉など社会のさまざまな分野に広がっています。
そうした業界ごとに異なるセキュリティのニーズにも対応し、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、広く人材育成をサポートできるのが、私たちIISEC（情報セキュリティ大学院大学）です。

その強みは、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、マルウェア分析、セキュアな機器・システムの構築、組織マネジメントまで、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本学なら、今後の業務に必要な分野を追究することも、課題解決に向けて複数の視点から検証することも可能でしょう。また、在学生は社会人学生が多くを占め、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。
世界が大きく揺れ動く中、ピンチをチャンスに変え、より豊かな未来をつくるために。IISECでの学びは、あなたを次のステップに向けて成長させてくれます。

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



新しい社会を歩むIISEC

対面授業に加えてオンライン授業も常設し新しい社会に対応して進化するIISECの教育。新入生、在学生の声と修了生からの応援を紹介。

2020年4月から、IISECの講義・実習は対面形式のほか、オンライン形式、対面とオンラインの併用など講義・実習それぞれの内容と、在学生の受講しやすさを考慮した教育・研究体制を実践しています。
こうしたリアルとオンラインが交錯し、融合する環境のもと、進化を続けるIISECでの教育と研究について、巻頭特集では、新入生が学んだ内容と各自のリアルな1週間、現在の社会課題を踏まえて2年次の在学生が取り組む研究について紹介。
さらにセキュリティ業界やアカデミアなど、IISECで磨いた専門性を生かして活躍する修了生からの応援メッセージも掲載しています。
多様なバックグラウンドを持つ在学生が、情報セキュリティを軸に幅広く学び、教員や在校生同士の交流で新たな知見を得ていく。
開学以来、変わることのない理念で実践教育・高度研究を行ってきたIISECの“今”をお伝えします。

新しい社会を歩むIISEC

■新入生レポート

センシティブな個人情報が集積される医療機関のセキュリティが研究テーマ。

廣田 凪さん　Nagi HIROTA
情報セキュリティ研究科　博士前期課程1年
高崎健康福祉大学健康福祉学部医療情報学科出身

時限	月	火	水	木	金	土	日
1	平日午前中は自宅で家事のほか、大学院の課題に取り組む			（木曜日はすべての授業がオンライン）	自宅で家事や大学院の課題	個人識別とプライバシー保護	今のところ日曜日は完全に勉強はOFF日。遠方で行われるイベントなどに日帰りや1泊2日で出かけることも
2						セキュリティシステム監査	
3						情報セキュリティ技術演習Ⅰ	
4	院生室で自習や論文の下調べ	セキュアシステム構成論A	院生室で自習や論文の下調べ	マスメディアとリスク管理			
5	知的財産制度	オンラインによる藤本研究室のゼミ。担当学生が研究の進捗を発表し、ディスカッションする	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	法学基礎		
6	セキュリティの法律実務		ネットワーク設計とセキュリティ運用	院生室で自習や論文の下調べ	院生室で自習や論文の下調べ	CTFがテーマのISSスクエア分科会。オンライン開講	
α	帰宅後、食事を終えて大学院の課題。夜型なので午前2時頃まで続ける						

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

1>授業の前後は院生室で学習。社会人学生からセキュリティ業界の話を聞く機会も。 2>この日は「法学基礎」でセキュリティを考えるベースとなる法学全般を学ぶ。

◉大学でセキュリティに興味を持ち専門的に学べるIISECに入学

大学は医療系と情報系にまたがる学科で、両分野を学んだことから医療機関のセキュリティに興味を持ちました。

大学を卒業してIISECに進学したのは、セキュリティの中でもマネジメント領域の専門性を身につけ、将来は医療系のセキュリティコンサルタントを目指したいと考えたから。技術面だけでなくマネジメントまで幅広く習得できる大学院は、国内ではここだけだと思います。

◉指導教員のアドバイスをもとに医療職のセキュリティ教育を研究

入学後はセキュリティに関する幅広い知識を得るため、法学からネットワークなどの工学分野までバランスよく履修。ネットワーク経由での不正侵入や防御を行う「情報セキュリティ技術演習Ⅰ」など、非常に実践的な内容はIISECでなければ経験できなかったでしょう。

また、授業はディスカッションや個別発表が多く、さまざまな業界で働く学生の意見を聞くのも勉強になります。

私はセンシティブな個人情報が集まる医療機関の中でも、診療報酬の請求などを担当する医療事務職のセキュリティ教育を研究予定。ただ、先行研究も少ないテーマなので、指導教員の藤本正代先生と相談し、まずは医療事務を育てる専門学校のカリキュラムから、学生時代に受けるセキュリティ教育を調べています。

私の1週間

◉全科目オンライン開講の日以外は横浜キャンパスに通学して学習

大学卒業後すぐにIISECに入学し、現在は大学院中心の生活です。平日の履修科目は4時限以降なので、午前中は自宅にいて朝食、家事などに充て、それまでに出た課題にも取り組んでいます。

授業は全科目がオンライン開講の木曜日を除き、横浜キャンパスで受講。通学にも便利な立地で、授業後に駅ビルなどで買い物をして帰る日もあります。

受講科目の中で、法学分野は「セキュリティの法律実務」「知的財産制度」など3科目あり、被害者側に立証責任が生じるケースのように、自分にはなじみがない法的な考え方にやや苦労しています。一方、「セキュアシステム構成論」をはじめ、インシデントの実例も扱う授業はイメージしやすく、興味も深まります。

◉授業発表やレポート課題が多く主体的に学べる環境

入学して実感したのは、授業での個別発表やレポート課題の提出が多いこと。もともと私が夜型のこともあり、授業後に帰宅したら、当日出された課題や締切間近の課題、自分が担当する発表の準備と、午前2時頃まで勉強しています。

こうした自ら学んでいく環境や、ISSクエアやenPITなど他大学との共同プログラムへの参加を通じて、修了までに大きく成長できると期待しています。

■新入生レポート

心理学の視点で他者に効果的に働きかけ職場全体のセキュリティ向上を目指したい。

小林 泰大さん Yasuhiro KOBAYASHI
情報セキュリティ研究科　博士前期課程1年
NTTコミュニケーションズ株式会社

時限	月	火	水	木	金	土	日
1		自宅で勤務。始業は9:30から10:00頃		木曜日はすべての授業がオンライン		キャンパスへ移動	
2	土曜日の授業も業務扱いのため、日曜日と月曜日が休日に。まとまった時間を活用して、授業の課題に取り組む、研究に役立つテーマを探索するなど		自宅で勤務	自宅で勤務	自宅で勤務	セキュリティシステム監査	休日は、いったん仕事や学校のあれこれを忘れ、自宅でのんびりと過ごす。たまにサイクリングなど。
3				統計的方法論		情報セキュリティ技術演習I	
4			キャンパスへ移動。夕食	授業モードの頭で課題に取り組む	キャンパスへ移動。夕食		
5		17:30から稲葉先生による研究指導（稲葉研究室の研究指導はすべてオンライン）	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	法学基礎		ただし、課題やゼミ発表が佳境のときは「休日返上」も
6			ネットワーク設計とセキュリティ運用	クリティカルシンキングとイノベーション	暗号・認証と社会制度	帰宅。月1回ほどISSスクエア分科会にオンライン参加	
α	夕食後は仕事も勉強もオフの時間に						

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

1>IISECの図書室で研究の参考になる論文を探す。2>「輪講」での発表に質問。セキュリティの多様な分野の理解を深められる。

私の1週間

◉全科目オンラインの木曜日は課題などに集中して取り組める

私の所属部署はコアタイムのないフレックス制でリモート勤務が基本。学費や勤務条件でも援助も受け、業務を早めに終えて18時20分開始の5時限からIISECで授業を受けるなど、あまり無理せず仕事と大学院の両立ができています。

また、木曜日は全科目がオンラインでの開講で、仕事も在宅のため移動時間はゼロ。授業の課題などに集中して取り組みやすい日です。稲葉研究室も個別指導はすべてオンラインなので、遠方に住む社会人学生も受講しやすいと思います。

◉多様な業種の在学生や他大学との交流も大学院に通う魅力

それ以外の日はIISECの横浜キャンパスに登校。セキュリティ業務に携わる多様な業界の在学生と直接話せる機会も生まれるなど、通学のメリットは大きいですね。加えて、IISECのほか複数の大学・大学院と企業などの共同教育プログラム・ISSスクエアにも参加し、知識や交流の幅を広げています。

入学して数カ月で、充実した授業内容を書き留めたノートは2冊目に。これは今後の業務で役立つ糧になると確信しています。また、幅広い科目や人的交流を通じて、セキュリティの事象をさまざまな角度から見られるようになり、職場で管理や助言する際の幅も広がりました。

◉セキュリティに関する学術的な裏付けの必要性を感じた

これまで研究開発部門でセキュリティ技術研究や、同部門のセキュリティオペレーションを歴任。しかし部署内のルール運用やメンバーへの助言などのように、他者を巻き込んで業務を進めていく際、最新の知見や学術的な裏付けの必要性を感じてIISECに入学しました。

この大学院は全体がセキュリティを研究対象としている点がユニークで、私も暗号など技術的な分野のほか、法学、経営、心理学まで幅広く受講。演習・実習では、不正アクセスへの対応も実践的に学べるなど、業務にも非常に役立つ魅力的なカリキュラムでした。

◉興味が広がる全研究生参加の輪講 研究はセキュリティ心理学がテーマ

そうしたセキュリティ研究の幅広さ、分厚さを実感するのが、週1回の必修科目で、全研究生が参加する「情報セキュリティ輪講」です。機械学習から安全保障、マネジメントまで、各自の研究の方向性も分かり、自分の興味も広がります。また、1年次、2年次を通じて所属する研究室は、セキュリティ心理学をテーマとする稲葉緑先生の研究室を選択。人に働きかけてセキュリティを向上させるマネジメントの観点から、職場のセキュリティマネージャーに必要な助言・サポートなどについて先行研究も参考に考え、実務に生かしたいと思っています。

■在校生インタビュー

入学して実感した大学院の魅力

自動運転の車による事故の法的責任を検証するため周囲の車が持つデータから事故車の挙動を探れないかを研究。

松本 悟さん
Satoru MATSUMOTO
警察庁サイバー警察局情報技術解析課
博士前期課程2年
（2020年10月入学）

技術の進展で変わる事故現場への対応を目指して

警察庁の技術職として、捜査に関わる電磁的記録を扱うデジタルフォレンジックを担当しています。交通関係の案件を扱う中で、近い将来問題となる自動運転車による違反・事故の法的責任に興味を持ち、体系的に研究しようと IISECに入学しました。仕事は必要な技術の話に終始しがちですが、大学院では情報倫理やマネジメントなど幅広く学べ、自らの業務を異なる観点から見つめ直すことができました。学生同士のディスカッションも多く、官公庁のほか、セキュリティベンダーやユーザー企業など、さまざまな立場の社会人学生からの意見で視野も広がりました。

自動運転の特性を生かしたデータ収集で事故車の挙動を追う

事故や事件に関する電磁的証拠は、警察が証拠となるデータの保全と解析を行うのが一般的です。しかし、自動運転の車では車体の大破やマルウェアの感染などにより、データの収集・解析ができないケースも考えられます。私はその解決策の一つとして、自動運転の車が周りの車と協調して動くよう想定されている点に着目。周囲にいた車が持つデータから、事故を起こした車の挙動などを調べられないか検討しています。周囲から得た情報を機械が直接判断して動く点で、自動運転の車と IoTは類似しています。私の指導教員の松井俊浩先生は IoT研究の第一人者で、IoTで使われる技術や運用上の課題など貴重なアドバイスをいただきながら、論文執筆が進められました。一方、周囲を認識するセンサーや通信機器が外部からの攻撃対象になりやすい点も IoTと類似しており、今後は自動運転の車も情報の入り口部分のセキュリティ強化が必要と考えています。

セキュリティに関する最新情報を業務にも生かす

このほか IISEC と中央大学、企業などの共同プログラムである ISS スクエアの分科会にも参加。月１回ほどのオンライン開催でしたが、私が研究していた自動運転やIoT以外の専門分野も討議する機会ができ、新たな知見も得られました。大学院で知識・技術を自らアップデートする力も養えたと思いますし、職場に戻っても常にセキュリティに関する最新の情報を手に入れ、それらを業務に生かせると期待しています。

インシデントの原因ともなる委託者・受託者間のズレを防ぐ適切な業務委託契約のあり方を提案する。

高濱 総一郎さん
Souichiro TAKAHAMA
日本コムシス株式会社
博士前期課程2年

自社のセキュリティ対策のため体系的に学ぶ

私は通信建設会社に勤務し、大手通信キャリアの研究開発を経て、現在は自社や企業グループ全体のインフラ管理やセキュリティ業務に携わっています。近年、顧客との業務委託契約に必要なセキュリティ対策について、個々の部署からの問い合わせが急増し、グループ全体の整合性や効果を検証する必要性を感じていました。そこで、セキュリティの体系的な知識と、自社以外の多様な企業の事例を学ぶためにIISEC に入学しました。

仕事の確実性を高める思考法も習得

「クリティカル・シンキングとイノベーション」の授業では、ロジカルシンキング、デザインシンキングなど多様な思考法と、それらからイノベーションに至る過程を学び、学生同士のディスカッションも活発に行われました。こうした思考法は、自社の業務の効率化や新たな取り組みにも役立っています。また、ISSスクエアで参加した法制・倫理分科会では、AI 活用の課題と各国の法制度など最新のトピックを討議し、視野が広がりました。私の研究テーマは業務委託契約における企業のセキュリティ対策で、各社が適切なガイドラインをもとに対策を行って契約したはずが、深刻なインシデントが起こる理由と、事故を防ぐ実効性のある対策をまとめています。所属する研究室の後藤先生からのアドバイスで、これまでに起きた事例の先行調査から原因を抽出。特に委託者と受託者それぞれが認識する責任分界点のズレと、それを生じさせるコミュニケーションギャップに私は注目し、互いが触れにくい部分まで十分に詰めて話し合いができる環境や条件を検討しています。

多様な社会人との交流を卒業後も続けたい

まだ在学中ですが、社内のセキュリティ対策や業務の改善について確かな理論や情報をもとに提言できるようになり、提案内容の質も高められたなど、IISEC で学んだ成果が出ています。さらに個人的には、仕事だけでは出会えない多様な業界・ポジション、幅広い世代の社会人と、学生同士というフラットな立場で交流し、人脈ができたことが何よりの財産だと感じています。卒業後も交流を続け、自分を成長させたいですね。

■修了生からのメッセージ

セキュリティ業界の先輩たち

真偽不明な情報・ディスインフォメーションを人へのアプローチで解決する手法を研究。その成果をもとに国立の研究所に出向中。

中嶋 悠さん　Haruka NAKAJIMA
情報セキュリティ研究科 博士前期課程修了
（株式会社ラック）

大学院で知識の幅が広がり
物事を俯瞰的・多角的に分析できるように

私は文系で、大学時代には社会心理学を専攻していました。セキュリティベンダーに就職して、技術者として働きながら出産・育児を経る中で、自分の強みを生かして社会に貢献したいと考え、研究職になりました。安全保障におけるサイバーセキュリティを心理学の観点から研究していたのですが、研究の学術的な価値を高めるために、幅広い分野の専門家が集結しているIISECに入学しました。

仕事柄、セキュリティの技術的な知識はありましたが、仕事で触れることがない経営学や法学などのセキュリティに関連する知識を習得できるのがIISECの魅力です。知識の幅が広がると物事を俯瞰的・多角的に分析できるようになり、セキュリティ上の課題だけでなく、組織や企業における問題解決にも役立てることができます。

高度化・複雑化するセキュリティの問題に
取り組める幅広い対応力がこれから必要

在学中はソーシャルメディアで人がディスインフォメーションを共有するメカニズムについて研究。ディスインフォメーションとは虚偽または誤解を招くような情報のことです。このような情報に惑わされる人を減らし、社会の混乱を防ぐために、現在はIISECの博士後期課程で人へのアプローチによる解決策を研究しています。このような研究活動が、国立研究開発法人への出向にもつながりました。

IISECではセキュリティの技術的な側面に加え、幅広い分野にまたがる研究をすることができます。高度化・複雑化するセキュリティの問題に取り組み、社会に貢献できる人材を一緒に目指しましょう。

体系的な知識と専門性を身につけ多様な学生との交流で見識を広げる。そうした経験が社会を生き抜く武器に。

中山 幸郎さん　Sachiro NAKAYAMA
情報セキュリティ研究科 博士前期課程修了
（日本アイ・ビー・エム株式会社 X-Force Red）

拡大するセキュリティ市場で
得意分野を活かした活躍を目指す

私はIISECで学んだ後、企業や研究所でサイバーセキュリティの業務に携わり、2022年1月から現在の勤め先でオフェンシブセキュリティサービスを中心とした業務を担当しています。

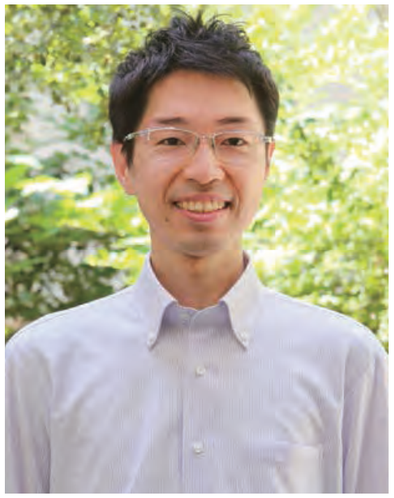
大学卒業後すぐにIISECに入学したのは、当時から拡大傾向にあったセキュリティ市場で、自分が得意とする数学を活かして活躍したいと考えたから。授業でセキュリティを体系的に学び、研究は専門性をとことん追究できる環境、企業や官公庁をはじめ様々な社会人学生との交流から得られる実践的な知識・経験など、IISECでの2年間は、どんな職場や業務にあっても私の武器になってくれます。

自身で考え、行動し、成長する力を磨き
変化の激しい業界を生き抜く人材に

現在のセキュリティ市場では、コロナ禍を機にリモートアクセスに関連する製品のセキュリティが注目されています。このように時代により重点分野が変わるセキュリティ業界で生き抜くには、知識やスキルのアップデートが欠かせません。IISECで磨いた「自身で考え、行動し、成長できる能力」をぜひ活かしてほしいと思います。

また、セキュリティ業界にはペネトレーションテストなどの攻撃分野、インシデントレスポンス・監視などの防御分野、その他、研究、製品開発、コンサルタント、保守・運用など様々な分野があります。そうした分野ごとにプロフェッショナルといえる先生方や社会人学生が見つかるのもIISECの強み。在学中に交流を深め、ここでしかできない経験の中で自分の進路を考えてはどうでしょうか。

様々な業界で働く社会人学生や先生方との交流で得られた人脈は今でも私の財産となっています。



大竹 剛さん　Go OHTAKE
情報セキュリティ研究科 博士後期課程修了
（NHK放送技術研究所）

放送のネット配信サービスに必要な
暗号の知識を体系的に学ぶため入学

私は大学で制御工学を専攻した後、2001年にNHKに入局しました。入局以来現在まで、放送技術研究所において、インターネットを利用した放送サービスを安全・安心に提供するための暗号技術を研究しております。

入局当初は暗号の知識が全くなかったので、共同研究先の外部の専門家に教えて頂くなど、手探りの状態が続きました。暗号理論を体系的に学ぶ機会があればと思っていたところ、2006年に当時の上司から「IISECに行ってみない?」と勧められたことがきっかけで入学しました。3年間の在学中に、研究業務に必要な暗号の専門知識が増えたことはもちろん、様々な業界で働く社会人学生のみなさんや先生方との交流により得られた人脈は私の財産です。

情報セキュリティの幅広い知識を身につけ
将来のキャリア形成に役立ててほしい

近年、放送を取り巻く環境は大きく変化しました。テレビで放送コンテンツを視聴するよりも、スマホやタブレットなどのモバイル端末でインターネット上の動画コンテンツを視聴するユーザが増えています。このような状況を踏まえ、NHKは公共メディアとしてユーザに信頼されるコンテンツをいつでも・どこでも・誰もが安心して視聴できる環境を整えるための研究開発を進めています。

情報セキュリティは様々な業界で欠かせないものであり、その重要性は年々高まっています。入学を検討中の方は、IISECの授業や研究を通して、暗号技術だけでなく、法律やマネジメントなど情報セキュリティに関する幅広い知識を身につけ、将来のキャリア形成に役立てて頂きたいと思います。

情報と法学の学際領域の研究を深めるため IISECで学び、博士号も取得。その縁で、今は後進の育成に力を注いでいます。

村上 康二郎さん　Yasujiro MURAKAMI
情報セキュリティ研究科 博士後期課程修了
（情報セキュリティ大学院大学教授）

IISEC入学後は1年半で博士号取得
当時の勤め先の待遇も向上した

私は、慶應義塾大学法学部および同大学大学院法学研究科で法学を学びました。2002年に同大学院博士課程を単位取得退学した後、都内の私立大学の専任教員になりました。

当時は、文系の場合は、必ずしも博士号は必須ではないという雰囲気がありました。ただ、私の場合は、純粋な法律学ではなく、情報技術と法律学が交錯する学際的な領域を研究しているため、博士号があった方が有利だと思いました。当初は、論文博士も考えましたが、IISECでは最短で1年間で博士号をとれるので、1年間であれば、課程博士であっても、実質的には論文博士に近いのではないかと考えました。結果的には、博士号を取るのに1年半かかりましたが、所属大学での待遇や周囲の見る目が変わりましたので、IISECに入学して良かったと思っています。また、そういった縁もあって、2022年4月に、IISECの教授に就任しました。

DXの普及などで注目される情報セキュリティ
情報と法学に精通した人材の育成が急務

新型コロナウイルスの影響でテレワークが広がり、今後は、DXの推進や、超スマート社会の本格的な実現によって、ますます情報セキュリティは重要になります。情報セキュリティというと、暗号技術などの技術的な側面に目が行きがちです。もちろん、技術も重要ですが、情報セキュリティを実現するためには、法制度を整備し、適切に運用していくことも重要です。ところが、現在では、セキュリティ技術と法制度の両方に精通した人材が不足しています。この両者について、高いレベルで学べるところは、日本国内では、IISEC以外には存在しないと思います。ぜひ、IISECに入学して、技術と法律の両方をマスターして欲しいと思います。

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)／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	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

2022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。

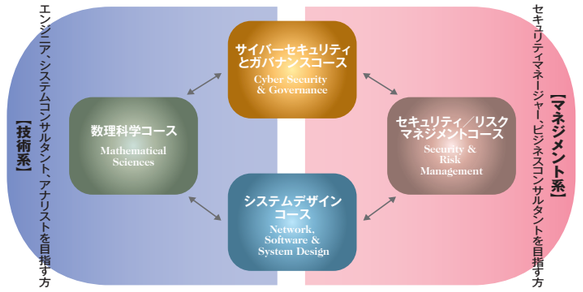
・神奈川県内の大学院間における大学院学術交流協定
・中央大学大学院理工学研究科
・国立情報学研究所
・東京大学大学院情報理工学系研究科
・The Information Security Group, Royal Holloway, University of London
・大連大学　他

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。

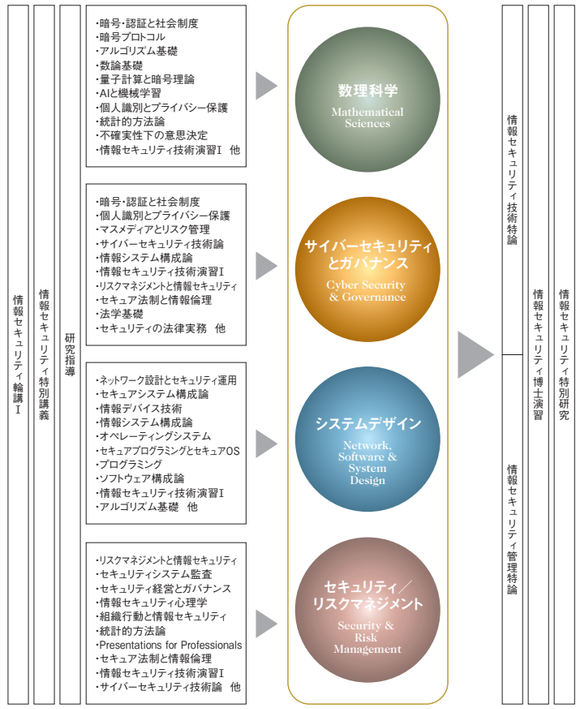
■ 博士前期課程4コース



＜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

博士前期課程（修士課程）　博士後期課程



■ 2023年度開設予定科目一覧

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

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［2年制］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3日）

	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				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		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理	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	法学基礎	
6	セキュリティの法律実務	（研究指導Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	ネットワーク設計とセキュリティ運用	特設講義（クリティカル・シンキングとイノベーション）	暗号・認証と社会制度	

【後期】（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		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	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	情報システム構成論 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	実践的IoTセキュリティ	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	（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	セキュアシステム構成論B	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3日）

	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				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		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理	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	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Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	ネットワーク設計とセキュリティ運用	特設講義（クリティカル・シンキングとイノベーション）	暗号・認証と社会制度	

【後期】（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		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	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	情報システム構成論 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	実践的IoTセキュリティ	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	（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	セキュアシステム構成論B	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3日）

	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				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		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理	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	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Ⅰ・研究指導Ⅱ・プロジェクト研究指導）	ネットワーク設計とセキュリティ運用	特設講義（クリティカル・シンキングとイノベーション）	暗号・認証と社会制度	

【後期】（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		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	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	情報システム構成論 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	実践的IoTセキュリティ	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	（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	セキュアシステム構成論B	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）

授業科目履修例
2022年度

▼＜学部新卒（ストレートマスター）学生Aさんの履修例＞

※ が履修科目

◆前期（4月7日～8月3日）

	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				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		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理	数論基礎	
5	AIと機械学習	（研究指導Ⅰ）	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Ⅰ）	ネットワーク設計とセキュリティ運用	特設講義（クリティカル・シンキングとイノベーション）	暗号・認証と社会制度	

◆後期（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		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	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	情報システム構成論	（研究指導Ⅰ）	情報セキュリティ特別講義	実践的IoTセキュリティ	Presentations for Professionals	
6	特設講義（ブロックチェーン理論）	（研究指導Ⅰ）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B	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Bさんの履修例＞

※ が履修科目

◆前期（4月7日～8月3日）

	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				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		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理	数論基礎	
5	知的財産制度	（研究指導Ⅰ）	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	法学基礎	
6	セキュリティの法律実務	（研究指導Ⅰ）	ネットワーク設計とセキュリティ運用	特設講義（クリティカル・シンキングとイノベーション）	暗号・認証と社会制度	

◆後期（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		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	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	情報システム構成論 or 組織行動と情報セキュリティ	（研究指導Ⅰ）	情報セキュリティ特別講義	実践的IoTセキュリティ	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	（研究指導Ⅰ）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B	特設講義（データ・サイエンスとアナリティクス）	

※一部の授業科目は遠隔講義を併用して開講します。

■ 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	

INSTITUTE of INFORMATION SECURITY

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、昨今のＡＩや機械学習の発展を踏まえ，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、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：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、システム（組み込み／IoT／制御）／Web／クラウド）セキュリティ、ゼロトラストアーキテクチャ、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

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

◆コース概要と研究キーワード

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

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。

＊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

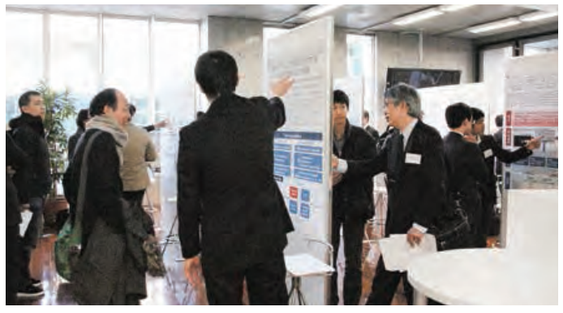
特にオプションプログラムは選択せず、各コースの履修標準科目を中心に履修して研究を進めるための知識の獲得や補強に努めるとともに、所属研究室での研究指導やディスカッションを通じて研究遂行能力を高め、在学中は修士論文作成に向けた研究に重点的に取り組みたい、という方を想定しています。神奈川県内の20以上の大学が加盟する大学院学術交流協定制度を利用して、研究テーマに関連する他大学院の開講科目を履修することも可能です。

▶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。
http://lab.iisec.ac.jp/

パターン2 ISS square 併修型

研究室や大学を超えた活動を通じて幅広い視野を養い、研究を実務に生かしたい

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



パターン3 ISS square & enPiT SecCap 併修型

ISSスクエアの活動に加えできるだけ実践的な演習や実習に取り組みたい

enPiT（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

若月 里香｜情報セキュリティ大学院大学 特任助手
（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！

田中 恭之｜情報セキュリティ大学院大学 客員講師
NTTコミュニケーションズ株式会社
（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）

「情報セキュリティ技術演習Ⅰ」を担当しています。本講義では、サイバー攻撃とその対策をハンズオン形式で基礎から応用までじっくり取り組みます。私は 2011 年にセキュリティ分野でのキャリアを積み始めた頃に受講しました。毎週楽しみにしていた講義のひとつでしたが、振り返るとこの講義でセキュリティエンジニアとしての基礎力が身に付いたと実感しています。実務に携わる立場として、現場での経験を講義に活かしていきたいと思います。

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 システム技術本部 セキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT
（情報セキュリティ研究科博士後期課程修了）

「情報セキュリティ特別講義」は、共同で講義を運営していく稲葉先生と相談しながら、参加する皆さんがよい知見を得られるよう、自身の知見を皆さんに移転したり、さまざまな背景を持つ先生をお招きしたりという、特段「この分野のこのトピックについて」という縛りのない講義である、と理解しています。皆さん聞いたことのある手法について深掘りするか、あれを作った当事者に語っていただくか、いろいろ考えつつ準備しておりますので、ちょっとお待ち下さいね。

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250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

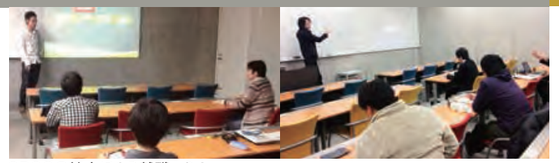
文部科学省の平成24年度「情報技術人材育成のための実践教育ネットワーク事業」に採択されたenPiTは、クラウドコンピューティング、セキュリティ、組み込みシステム、ビジネスアプリケーションの4分野を対象とし、それぞれの分野に専門領域を有する全国の15大学院の教員や企業の技術者を結集したプログラムです。2017年4月からは大学院生向け成長分野を支える情報技術人材の育成拠点の形成（enPiT 1）として自主展開を図っており、セキュリティ分野（enPiT-Security）は、5つの連携大学（情報セキュリティ大学院大学、東北大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学）が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/

INSTITUTE of INFORMATION SECURITY

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
2021-2022



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】(2021-2022実績)
IQVIA ジャパン／麻布台片岡法律経済事務所／NRIセキュアテクノロジーズ(株)／NTTコミュニケーションズ(株)／NTTテクノクロス(株)／F5ネットワークスジャパン(同)／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)協和エクシオ／(株)セキュアベース／(株)ミライト・テクノロジーズ／(株)レオンテクノロジー／キヤノンビズアテンダ(株)／金融庁／警察庁／警視庁／JCOM(株)／(独)国立印刷局／日本コムシス(株)／日本生命保険相互会社／防衛省／法務省／三井住友海上火災保険(株)／三井住友信託銀行(株)／横浜市役所　など

■ 現況

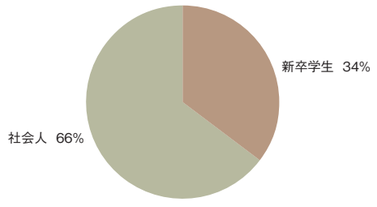
約7割の方が社会人学生です。時間をやり繰りし、仕事と学業を両立させています。また、いったんキャリアをリセットした後、次のステップに備えるべく一定期間学業に専念されているケースも見られます。就業経験のない新卒学生の方にとっては、こうした方々との交流も、近未来の自分像やキャリアプランを描くうえでの貴重な経験となるでしょう。

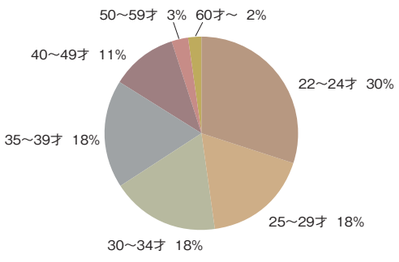
■ 年齢構成(入学時)

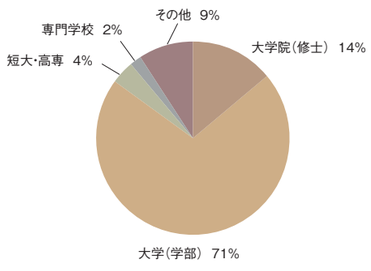
20代半ばから30代の中堅社会人をはじめ、幅広い年代の方々が学んでいます。ジェネレーションを超え、同じ学生という立場で活発な交流が図られています。

■ 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】(2021-2022実績)
NTTアドバンステクノロジ(株)／NTTコミュニケーションズ(株)／オムロンヘルスケア(株)／(株)NTTドコモ／(株)日立システムズ／(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)豆蔵／(株)ラック／環境省／(公財)笹川平和財団／(国研)産業技術総合研究所／さくら情報システム(株)／Cs soft(株)／第一生命保険(株)／東京都立産業技術大学院大学／日立ジョンソンコントロールズ空調(株)／陸上自衛隊　など

博士前期課程
(修士課程)

授業科目概要
2022

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。

■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、社会科学系の学生が法制度やマネジメント等の研究課題に取組む際の基盤となる知識として、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に解説し、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・マネジメント的課題について、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、マネジメント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。

■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、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. 講義は 2 つの部分に分かれている。最初の 10 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践した内容を発表する。

■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、IoT 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、組織の経営管理とセキュリティ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、「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、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 English language presentations about professional topics. The focus will be on gaining presentation and communication skills, not on English 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. In it, you will learn skills that you can apply to your Japanese presentations too. You will also discover that designing and presenting your original ideas can be fun and challenging. 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。

TOPICS

2022年度新規開講科目

■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(批判的思考法)とは、ひと言でいえば「前提を疑う」「常識を疑う」ということであり、そこからイノベーションも生まれてくる。セキュリティの世界においてもインシデントの予測と防止、対処、分析などにおいて、明示的・暗示的にクリティカルシンキングのアプローチは用いられている。本科目では、クリティカルシンキングとそれに関連するさまざまな思考法について紹介するとともに、イノベーションについての基礎知識と実例を紹介していく。テーマの特性上、ディスカッションが中心であり、話題提供者としてゲスト講師を呼ぶ場合がある。

学長
Message

後藤 厚宏

学長 ● 教授 Atsuhiro GOTO

多様な人材と交流ができる
対面での授業を基本に
オンライン受講日も設定

本学は情報セキュリティに専門特化した大学院大学で、横浜キャンパスは横浜駅近く、再開発により商業施設、ホテル、オフィスビルなどが並ぶエリアにあります。通学に便利な好立地に加え、在学生の約7割を占める社会人も在職のまま修了できるよう、2004年の開学時から、平日昼夜間と土曜日に授業を行っています。コロナ禍で、やむなくオンライン中心の授業になった際、私たちが痛感したのは、多様な学生と教員が同じ時間・空間を共有する大切さでした。隣にいる学生に気軽に質問したり、異なる業界の学生同士が気軽に情報交換したりできる人間関係の豊かさは、代え難いものがあります。

そうした思いから対面での授業をいち早く再開した一方、社会人学生の通学負担軽減の観点から、2022年度から特定曜日の選択科目の授業をオンライン開講とする体制もスタートさせるなど、学生の利便性を高めています。このように状況に適した機敏な対応ができるのも、単一専攻で小規模な大学院ならではの機動力と自負しています。

暗号から法制度・倫理まで
広範なセキュリティ分野を
ワンストップで学べる

情報セキュリティは、暗号、ネットワーク、システム技術などの技術分野はもちろん、マネジメント、法制度・倫理まで、多様な分野にまたがり、それらを融合して考える必要があります。本学は小規模な大学院ですが、これら広範な分野についてそれぞれ専門の教員が在籍し、情報セキュリティについてワンストップで学べる点が大きな特徴です。教育内容や研究テーマは実践的で、企業や官公庁が求める実務志向の人材育成を行っています。また、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。そうした科目選択の指針となるよう、将来の目標により履修内容を整理した4つのコースフレームも設けています。教員は実務経験者も多く、研究と実務の融合による教育体制、指導体制を整えており、在学生は対面・オンラインを問わず、グループワークや深い議論によって自らの考えを掘り下げ、アウトプットすることを身に付けます。加えてハンズオンによる教育にも力を入れ、サイバー攻撃や防御の模擬演習なども取り入れています。

さらに本学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力する実践教育「enPiT／SecCaP」への参加も可能です（いずれもオンライン開催の場合があります）。

DX導入とセキュリティなど
企業が直面する課題を
研究テーマにする学生も

数年前から、日常の業務の中でセキュリティに関するスキルが求められる「プラス・セキュリティ」人材の不足がいわれていましたが、リモートワークの普及などで、その必要性はさらに高まっています。本学の在学生も、セキュリティベンダーのほか、ユーザー企業である製造業、金融業、あるいは官公庁など幅広く、研究テーマもDX導入とセキュリティなど、それらの企業・団体が直面する課題を取り上げるケースも少なくありません。

セキュリティの広範な分野を融合させて学び、実践的な課題の研究を通じて問題解決能力を養う本学の2年間は、「プラス・セキュリティ」人材となってキャリアアップするためにも有効だといえるでしょう。

複雑化した社会の課題解決に取り組むとき、複数の分野から多角的に見ると、行き詰まりを打開できることはよくあります。その点、本学はワンストップで学べる強みを生かし、例えば在学生の学習・研究で技術的な観点に法律の視点を加えるなら、法律分野の教員を訪ねてアドバイスをもらうこともできます。さらに本学では、それぞれの在学生が所属する研究室の研究指導教員に加え、2022年度からメンター教員制度を設け、在学生一人一人がより円滑に研究活動を行い、本学の教育資源・環境を十分に活用できるような指導体制を用意しています。

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2021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。

■ 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

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。

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-)、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)。大阪大学非常勤講師(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、情報処理学会、人工知能学会、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主幹事、電子情報通信学会ISEC研究専門委員会委員、情報処理学会論文誌編集委員。

■主な研究業績
1. Koichi Moriyama, Akira Otsuka, “Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors,” In Proceedings of the 5th IEEE International Conference on Blockchain. Blockchain 2022. Espoo, Finland: IEEE ,2022.
2. Takahashi, Taisei, and Akira Otsuka. “Probabilistic Micropayments with Transferability.” In Computer Security – ESORICS 2021 – 26th European Symposium on Research in Computer Security, Proceedings, pp. 390–406. Lecture Notes in Computer Science 12972. Springer, 2021.
3. Ryotaro Nakata and Akira Otsuka. “CyExec”: A High-Performance Container-Based Cyber Range With Scenario Randomization.” IEEE Access Vol 9, pp. 109095–109114, IEEE 2021.
4. Yuhei Otsubo, Akira Otsuka, Mamoru Mimura, Takeshi Sakaki, “o-glasses: Visualizing x86 Code from Binary Using a 1d-CNN,” IEEE Access, Vol. 8, pp 31753-31763, IEEE 2020.
5. Tatsuo Mitani, Akira Otsuka, “Confidential and auditable payments,” In Proceedings of 4th Workshop on Trusted Smart Contract, WTSC’20, Kotakinabalu. Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, vol 12063. pp 466-480, Springer, Cham.
6. Mitani Tatsuo, Akira Otsuka, “Traceability in Permissioned Blockchain,” IEEE Access, Vol. 8, pp 21573–21588, IEEE 2020.
7. 大塚 玲, “ブロックチェーンを利用した暗号資産の安全性と匿名性:原理と限界,” 金融研究, 第41巻, 第1号, 日本銀行金融研究所, 2022.

■主な研究テーマ
情報セキュリティ基礎理論（ブロックチェーン、AIセキュリティなど）

■主な担当科目
AIと機械学習、アルゴリズム基礎、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。

■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科学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。

■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. DX with Cybersecurityのために必要な教育カリキュラム 日本セキュリティ・マネジメント学会誌 2021年 34 巻 3 号 1-2(2021.3)
5. 「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)

■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
リスクマネジメントと情報セキュリティ、個人識別とプライバシー保護、国際標準とガイドライン、
セキュリティ経営とガバナンス、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, Hideki Asoh, et. Al., “Integrated Natural Spoken Dialogue System of Jijo-2 Mobile Robot for Office Services”, Proc. Of American Association for Artificial Intelligence (AAAI), 1999
2. Toshihiro Matsui and Satoshi Sekiguchi, “Multithread Implementation of an Object Oriented Lisp System, EusLisp,” in Advanced LISP Technology (Eds.) Taiichi Yuasa and Hiroshi G. Okuno, IPSJ, Taylor and Francis, 2002.
3. 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）
4. 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.
5. Dang Duy Thang and Toshihiro Matsui, “A Label-based Approach for Automatic Identifying Adversarial Examples with Image Transformation”, Proc. Of the Seventh International Symposium on Computing and Networking (CANDAR’19, IEEE), Nagasaki, 2019.
6. Dang Duy Thang and Toshihiro Matsui, “Adversarial Examples Identification in an End-to-end System with Image Transformation and Filters”, IEEE ACCESS, 2020.

■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、プログラミング、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

学長

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. Taichi Aoki and Atsuhiro Goto, Graph visualization of dark web hyperlinks and their feature analysis, In 2021 International Journal of Networking and Computing (IJNC). IEEE, 2021.
6. Kosuke Ito, Shuji Morisaki, and Atsuhiro Goto, IoT Security Quality Metrics Method and its Conformity with Emerging Guidelines, IoT 2021, 2(4), MDPI

■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、経済インフラに向けたセキュリティ基盤
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、仮想ネットワークとZeroTrust

■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、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

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、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。2020年4月より情報セキュリティ研究科長。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。脅威分析研究会幹事、電子情報通信学会会員、IEEE CS会員。近著に「イラスト図解 この一冊ですべてわかるセキュリティの基本（共著、SBクリエイティブ）」。

■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、脆弱性検知/予測、マルウェア解析/攻撃検知、
システムセキュリティ、ゼロトラストアーキテクチャ、フィンガープリンティング応用、AI応用セキュリティ技術

■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、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

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. 岡村貴仁, 有田正剛, 同種写像問題に基づくパスワードベース認証付き鍵共有について, 情報処理学会研究報告 Vol.2022-CSEC-96 No.22, 2022/3.
2. Seiko Arita, Sari Handa, Fully Homomorphic Encryption Scheme Based on Decomposition Ring, IEICE TRANS., Vol.E103-A,No.1,pp.195-211,Jan. 2020.
3. 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.

■主な研究テーマ
主な研究対象領域は:
- 格子暗号、同種写像ベース暗号、符号ベース暗号などの、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
数理科学コース、サイバーセキュリティとガバナンスコース

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。司法試験予備試験考査委員(2020ー)
■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。現在は、IoTセキュリティにおける標準化、技術開発を推進。
■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
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
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
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　主幹担当部長(TM)
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
株式会社情報技研 代表取締役社長
株式会社Premo(東大CPUベンチャー) 代表取締役CEO / Founder
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年に新たにIoT時代を見据えたCPUベンチャーの株式会社Premoを東大内に共同設立。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、構築に携わる。専門分野は、計算機アーキテクチャ、セキュアシステム構成。2020年より、マイナンバーカード機能のスマートフォン搭載等にセキュリティの専門家として関わる。
■担当科目
セキュアシステム構成論

兼任
中西　晶
客員教授
Aki NAKANISHI

■プロフィール
明治大学経営学部専任教授
東京都立科学技術大学助教授等を経て現職。京都大学卒業後、民間企業に就職。その後、筑波大学で経営学修士、東京工業大学で博士(学術)を取得。安全・セキュリティの人的・組織的側面を研究。現在、内閣サイバーセキュリティセンター普及啓発・人材育成専門調査会構成員等。
■担当科目
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。情報の非対称における住宅選択行動等を主に研究。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

兼任
藤村　明子
客員教授
Akiko FUJIMURA

■プロフィール
日本電信電話株式会社 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、プライバシ保護の技術と法制度に関する研究開発に従事。情報ネットワーク法学会元理事。
■担当科目
セキュリティの法律実務

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、日本監査研究学会理事(前会長)、日本内部統制研究学会監事、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・企業会計審議会委員(監査部会長)、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。『票談 不正ー最前線』(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ー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、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、2020年情報セキュリティ文化賞受賞。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
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
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

兼任
湯淺　墾道
特定教授
Harumichi YUASA

■プロフィール
明治大学教授
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月から2021年3月まで本学教授。九州大学・中央大学・愛知学院大学・横浜市立大学非常勤講師、各自治体の個人情報保護関係の審議会委員、ベネッセホールディングス情報セキュリティ監視委員会委員、情報ネットワーク法学会副理事長等を務める。

※上記は2022年4月現在

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『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)
2. 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)
3. 村上康二郎『情報セキュリティに関する法』自動認識第25号52～56頁(2012年)
4. 村上康二郎『クラウド・コンピューティングにおける個人情報保護の課題』情報セキュリティ総合科学第4巻118～136頁(2012年)
5. 村上康二郎『情報プライバシー権と表現の自由の関係に関する一試論―アメリカにおける議論を参考にして―』法政論叢第48巻第1号141～176頁(2011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、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。情報処理学会論文誌編集委員、自動車技術会ヒューマンファクター部門運営委員、フィッシング対策協議会技術・制度検討WGメンバー等。情報処理学会、日本心理学会、自動車技術会等会員。

■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
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。専門は不正侵入検知・防御、マルウェア解析、OSINT技術等。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。情報処理学会・論文誌ジャーナル/JIP査読委員、電子情報通信学会・英文論文誌D編集委員、経済産業省・電気保安制度WG委員、IEEE・NETSAP Workshop Organizer等多数。

■主な研究業績
1. Y. Masubuchi, M. Hashimoto, A. Otsuka, "SIBYL: A Method for Detecting Similar Binary Functions Using Machine Learning," IEICE Transactions on Information and Systems, Vol. E105-D, No.4, pp.755-765, Apr. 2022.
2. A. Kanda, M. Hashimoto, "Identification of TLS Communications Using Randomness Testing," 2021 IEEE 45nd Annual Computer Software and Applications Conference (COMPSAC), 2021, pp. 1099-1106, doi: 10.1109/COMPSAC51774.2021.00150.
3. Yamauchi T, Akao Y, Yoshitani R, Nakamura Y, Hashimoto M. Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes. International Journal of Information Security. 2020. https://doi.org/10.1007/s10207-020-00514-7.
4. M. Kadoguchi, H. Kobayashi, S. Hayashi, A. Otsuka and M. Hashimoto, "Deep Self-Supervised Clustering of the Dark Web for Cyber Threat Intelligence," 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 2020, pp. 1-6, doi: 10.1109/ISI49825.2020.9280485.
5. H. Kobayashi, M. Kadoguchi, S. Hayashi, A. Otsuka and M. Hashimoto, "An Expert System for Classifying Harmful Content on the Dark Web," 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 2020, pp. 1-6, doi: 10.1109/ISI49825.2020.9280536.
6. M. Kadoguchi, S. Hayashi, M. Hashimoto and A. Otsuka, "Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 2019, pp. 200-202, doi: 10.1109/ISI.2019.8823360.
7. T. Yamauchi, Y. Akao, R. Yoshitani, Y. Nakamura and M. Hashimoto, "Additional Kernel Observer to Prevent Privilege Escalation Attacks by Focusing on System Call Privilege Changes," 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018, pp. 1-8, doi: 10.1109/DESEC.2018.8625137.

■主な研究テーマ
1. OS/ネットワークセキュリティ　2. 不正侵入検知・防御　3. OSINT　4. マルウェア解析

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

■担当コース
システムデザインコース

■ 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］

	1年次前期	1年次後期	2年次前期	2年次後期
正規課程授業	→	→	→	→
SecCap（オプションプログラム）		◆実習		
ISSスクエア（オプションプログラム）	分科会	分科会 ◆合同分科会	分科会 ◆シンポジウム	分科会 ◆合同分科会 ◆シンポジウム
	水平WS	水平WS ◆	水平WS ◆	水平WS ◆
修士研究	→ 文献調査	→ ◆輪講発表	→ ◆M2発表	→ ◆中間発表 → ◆論文提出／審査／発表

■ 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。

● 修士論文等発表会

博士前期（修士）課程の研究成果の集大成となる修士論文の発表会がオンラインにて開催されました。2021年度も数理科学系理論、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、特定課題研究報告が発表されました。

● 学位記授与式

2021年度も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した。

※新型コロナウイルス感染拡大防止のため、マスクを着用して実施しました。

■ 情報セキュリティ大学院大学連携教授（2022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 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 技監	秋山 浩一郎
株式会社日立製作所 研究開発グループ 社会システムイノベーションセンタ 主管研究長	鍛 忠司
株式会社 KDDI 総合研究所 執行役員 先端技術研究所セキュリティ部門長	清本 晋作
東京電機大学 研究推進社会連携センター 顧問 客員教授	佐々木 良一
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
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
国立研究開発法人産業技術総合研究所 執行役員 兼 情報・人間工学領域 領域長 情報化統括責任者、最高情報セキュリティ責任者	関口 智嗣
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
日本電気株式会社 研究・開発ユニット 上席技術主幹	谷 幹也
富士通株式会社 フェロー兼研究本部 データ&セキュリティ研究所長	津田 宏
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部 部長	中野 学
日本電信電話株式会社 社会情報研究所 所長	平田 真一
三菱電機株式会社 開発本部 役員技監	松井 充
横浜国立大学 大学院 環境情報研究院 教授	松本 勉
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 研究所長	盛合 志帆
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

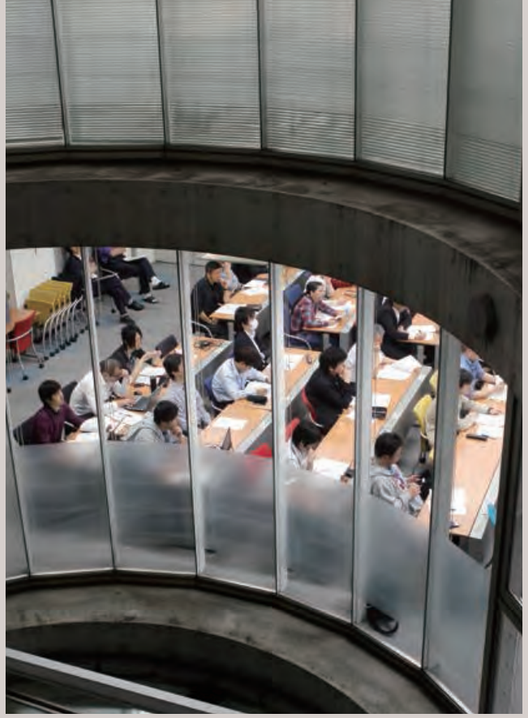
敬称略、氏名五十音順

■ 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（2022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。

早稲田大学政治経済学術院 教授	縣 公一郎
横浜市 副市長	伊地知 英弘
沖電気工業株式会社 理事 コーポレート本部 情報企画部長	長田 肇
日本電信電話株式会社 代表取締役副社長	川添 雄彦
株式会社三井住友銀行 名誉顧問	北山 禎介
芝浦工業大学 客員教授	國井 秀子
日本放送協会 理事・技師長	児玉 圭司
早稲田大学 名誉教授	後藤 滋樹
株式会社東芝 特別嘱託	斉藤 史郎
日本電気株式会社 執行役員副社長	堺 和宏
東京電機大学 研究推進社会連携センター 顧問 客員教授	佐々木 良一
三菱電機株式会社 常務執行役 知的財産渉外、知的財産担当、開発本部長	佐藤 智典
朝日新聞社 編集委員	須藤 龍也
株式会社MM総研 代表取締役所長	関口 和一
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 カンパニー副社長	髙嶋 靖彦
神奈川県 副知事	武井 政二
慶應義塾 常任理事	土屋 大洋
国立研究開発法人 情報通信研究機構 理事長	徳田 英幸
独立行政法人 情報処理推進機構 理事長	富田 達夫
株式会社エヌ・ティ・ティ・データ 執行役員 技術革新総括本部長	冨安 寛
NTTコミュニケーションズ株式会社 取締役執行役員 経営企画部長	藤嶋 久
富士通株式会社 サイバーセキュリティ事業戦略本部 本部長代理	森 玄理
株式会社日立ソリューションズ セキュリティプロフェッショナルセンタ チーフセキュリティアナリスト	米光 一也

敬称略、氏名五十音順



授業シーン

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

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

情報セキュリティに関する書籍、雑誌を図書室に配架するほか、学内からACM DigitalLibrary、IEEE、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。

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。

院生自習・実験室は平日は10時30分まで、土曜日は夜21時30分まで開放しています。（2022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。

■ 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。

■ 都内サテライトオフィス（IISEC東京オフィス）での勉強会

2021年秋に、在学生の自習スペースや個別研究指導、打合せ等での活用に資するため、東京・丸の内の新東京ビル内に本学のサテライトオフィスが開設されました。在学中はもちろんのこと、本学修了後も、大学主催やOBOG有志による勉強会、各種行事等で有効に活用いただけるよう、運用体制の整備を進めています。

■ 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。）http://www.jasso.go.jp/

種別	貸与月額（※2022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

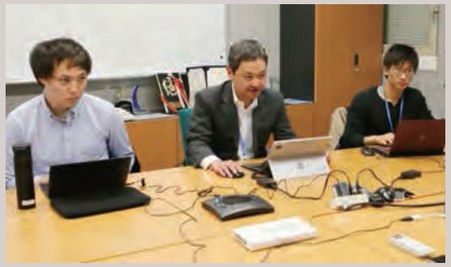
セキュア構築、侵入検知システムの導入設計、セキュリティ監視業務等を経てデジタルフォレンジック業務に携わる。サイバー攻撃被害の解析や訴訟事件等のデジタル鑑定解析、セキュリティ対策評価等を担当。
著作として「標的型攻撃セキュリティガイド」等がある。

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
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
since 1947
UNIVERSITY ACCREDITED
2017.4~2024.3

学校法人 岩崎学園

■Contents

■学生募集課程概要

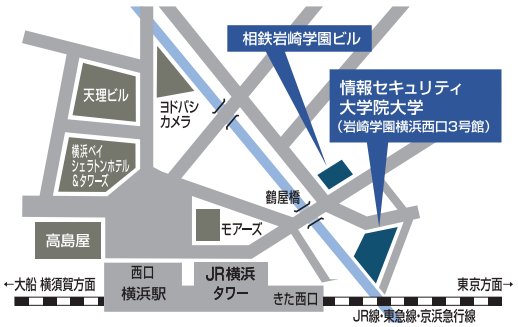
研究科	専攻	課程	標準修業年限	募集人員
情報セキュリティ研究科	情報セキュリティ専攻	博士前期（修士）課程［2年制］	2年	40名
		博士前期（修士）課程［1年制］	1年	若干名
		博士後期課程	3年	8名

詳細は本学ウェブサイトでご確認ください。

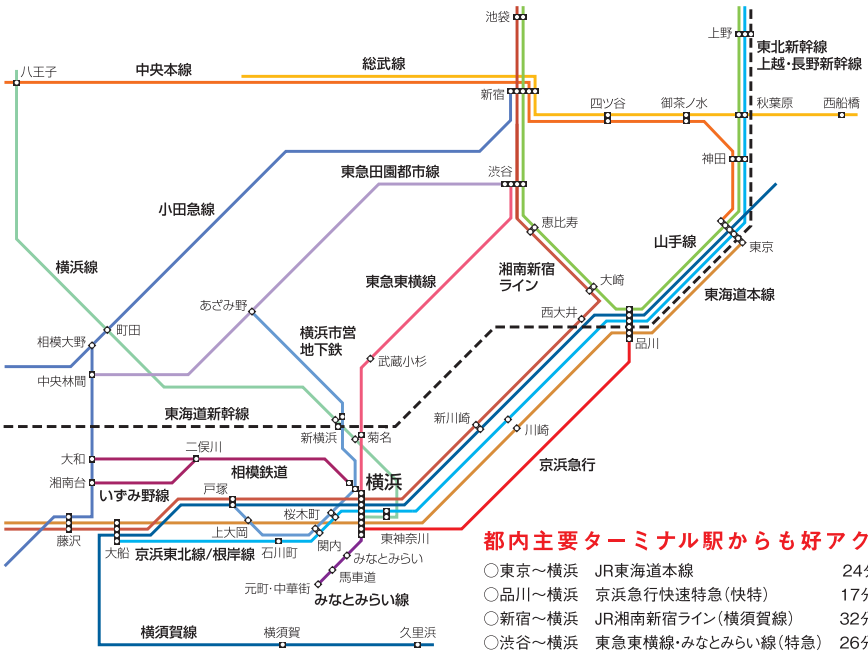
■入学者選考方法

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