

明日の信頼を創ろう。

情報セキュリティ大学院大学



To be aware of limitations is already to be beyond them.

2026 - 2027



学校
法人

岩崎学園

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。

情報セキュリティを総合科学と捉え、理論と実務の両面から専門的な教育・研究を行うIISEC。

桑名栄二学長と後藤厚宏特別学長補佐(前学長)が密接に連携する体制のもと

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

特別学長補佐

後藤 厚宏

Atsuhiko GOTO

対談



後藤●I S Sスクエアの分科会活動など、高度な問題解決能力を身につける機会は豊富です。

後藤●在学中は教員の指導のもと、学生は多様な研究経験を通して未知の問題を解くトレーニングを積み重ねることができます。修了後は実務で直面する困難な課題を打開できる力を持つ人材へと成長できるでしょう。

桑名●情報セキュリティの課題は、技術だけで完結するものではなく、社会、組織、制度、倫理、経営など、さまざまな領域と関わっています。そこで必要とされるのは、技術を理解したうえで、これらの文脈を踏まえてリスクを判断し、適切に対応できる人材です。本学は、こうした幅広い視野と実践力を備えた人材を育成します。

さらに修了生は官公庁や企業・団体などで活躍するセキュリティの中核人材であると同時に、I S E Cアラムナイの一員として

I S E Cの修了生は2026年3月で修士610名、博士60名を数え、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。早くからセキュリティ人材を育成してきた本学に対し、企業・官公庁等の信頼は厚く、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です。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し、加えて多様な分野の第一線

活発に交流。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に参加したOB・OGに在学生は非常に刺激を受け、OB・OGは後輩たちの研究内容を基に自身の知識をアップデートするなどWINWINの交流関係を築いています。

桑名●大学から直接本学に入学したストレートマスターの学生にとっては、多様なロールモデルと出会える貴重な交流になるはず。入学後はぜひ参加してください。

社会人も学びやすい時間割

全国で受講可能な体制も検討

I S E Cでは社会人が履修しやすいように平日夜間や土曜日にも授業を行い、オンラインやオンデマンドで受講可能な科目も拡充。さらに学外でのオンライン受講などに利用できるサテライト拠点の強化も検討中です。

にいる人材による講義も多く行っています。

異業種による新規参入やAIによる業務の拡張など、現在は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・研究を進めやすい環境で、「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ています。

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。I S E C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。

文理統合の知識と実務能力を習得し 「プラス・セキュリティ人材」に

I S E C(情報セキュリティ大学院大学) は、開学時から情報セキュリティを人・技術・社会を包括した総合科学と捉え、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、法制度、組織マネジメント、心理学、倫理など、多岐にわたる分野を統合した教育を特徴としてきました。AI、インテリジェンスと国際関係、経済安全保障といった近年のトピックスは「特設講義」などで体系的に学ぶ機会を設けています。

桑名●加えて本学では、リスクに直面した個人や組織が被害を最小限に抑え、迅速に復旧できるレジリエンスを身につけるため、実践的な対応力の育成にも注力しています。その一環として、仮想環境を用いたハンズオン形式の演習・実習を設け、システムへの攻撃と防御、インシデント対応、デジタルフォレンジック技術の利用などを実践的に学びます。

しかも現在は分野・業種を問わずサイバーセキュリティへの対策は不可欠です。専門家だけでなく、それぞれの分野・業種における業務知識や現編への理解を備えた人材が、セキュリティの知識・技能を習得し、現場のレジリエンスを高める「プラス・セキュリティ人材」として活躍することが求められています。

後藤●金融、メーカー、官公庁など多様な業界から学生が集まる本学は、他業界に視野を広げ、自分をより客観的に見る力も養えるでしょう。私の研究室では弁護士が企業のセキュリティ部門の学生と議論するなど、多様な業種・役職の社会人がフラットに交流しています。

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

生成AIをはじめ技術が急速に進化する中、予測不能な変化に対応できる「未知の問題を解く力」は今後さらに重要になってきます。I S E Cではゼミでの討論やハンズオン形式の

桑名●「プラス・セキュリティ人材」の育成は、首都圏に限らず、全国各地に共通する喫緊の課題です。本学では地理的・時間的な制約を超えて学べる環境整備を進めていきます。

またI S E Cには研究部門として、後藤特別学長補佐を所長に、各分野の専門家が客員研究員を務めるセキュアシステム研究所があり、政府や多様な研究機関と連携して、「重要産業のサプライチェーンリスク」「情報戦と安全保障プロジェクト」など、社会に直結する課題の解決に向けた研究開発も進めています。

桑名●こうした研究成果も教育に生かし、幅広い産業分野で将来の社会の安心・安全をリードできる「プラス・セキュリティ人材」を育成していきます。学んで自分を成長させたい方にぜひ来ていただきたいですね。

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
オンラインで受講可能な科目、オンデマンド科目も用意※
※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

■新人生レポート

セキュリティを総合的に学べる環境が魅力。
「形式検証」を大規模開発に生かす手法を研究中。

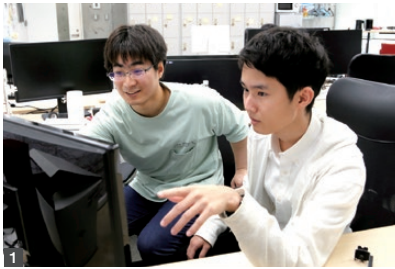
伊藤 駿介さん Shunsuke ITO

情報セキュリティ研究科 博士前期課程1年

岡山理科大学工学部情報工学科出身

時限	月	火	水	木	金	土	日
1		IISECに登校				IISECに登校	
2	自宅で自習 昼食後は IISECに登校	プログラミング	自宅で自習 昼食後は IISECに登校	自宅で自習 オンライン開講日 なので引き続き 自宅で受講	自宅で自習 昼食後は IISECに登校	セキュリティ システム監査	基本的に 自宅で課題や 研究に取り組む その他家事など
3		オペレーティング システム					
4	アルゴリズム基礎	研究室で研究を 進める	研究室で研究を 進める ティータイムに参加		研究室で研究を 進める	情報セキュリティ 技術演習I	
5	ティータイムに 参加した後で帰宅	ティータイムに 参加した後で帰宅	情報セキュリティ 精講I	情報デバイス技術 (オンライン)	ティータイムに 参加した後で帰宅		この週は SecHackで 知り合った メンバーと 外出して食事
6	ネットワーク設計と セキュリティ運用 (自宅でオンデマンド受講)	自宅で課題や 研究に取り組む その他家事など	ソフトウェア構成論	リスクマネジメントと 情報セキュリティ (オンライン)	自宅で課題や 研究に取り組む その他家事など	帰宅後、課題や 研究に取り組む その他家事など	
α	自宅で課題や 研究に取り組む		帰宅後、課題や 研究に取り組む	自宅で課題や 研究に取り組む			帰宅

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



1>授業の空き時間は研究室で研究を進める。同室の社会人の先輩からの意見を参考にできるのもIISECならではの 2>学年や研究室を超えて交流できる「ティータイム」は研究や仕事のこともざっくばらんに話せる貴重な時間

●CI／CDによる開発の安全性を
形式検証で厳密に確認する研究

大学で取り組んだ「形式検証」の研究を続けたくて、それを専門にされている大久保先生の研究室に入りました。現在の開発手法で主流のCI／CDで、複数の開発者が作成したコードを統合した際に、セキュリティ面の不具合が本当に起きないのかを形式検証で厳密に評価する方法を検討しています。私自身は大規模開発の経験がないので、大久保先生の指導や、そうした経験を持つ社会人学生の意見も参考に研究に取り組んでいます。

就活や長期インターンを前提に5時限以降の科目を多く履修し、セキュリティ診断の会社などで短期インターンも経験しました。ただ授業ごとの課題提出も多いため、なるべく当日着手し、テーマを他分野の事例と結びつけるなど自分なりの視点でまとめる工夫をしています。

また、私は大学や高専を卒業後すぐに入学する学生が対象の特待生試験に合格し、学費が半額減免になりました。出願時期が6～7月と早いのですが、経済的な負担を経験したい人にお勧めです。

●基礎知識全体の底上げができる
実践的な知識も身につけられる

ゲームの自作から情報系に興味を持ち、大学も情報工学科を選択。その後、大学2年生でセキュリティミニキャンプやGoogle initiativeに参加し、大学3年生ではセキュリティキャンプ全国大会やSecHack365などにも参加する中で、ゲームからセキュリティへと興味の対象が移りました。しかし企業インターンでは自身の専門知識や業務への応用力が足りないと感じ、より深く学ぼうとIISECに入学しました。

大学ではセキュリティ関係の科目を学ぶ機会がなく、基礎知識にも濃淡がありました。IISECの幅広い科目を履修して全体を底上げ。経営者や監査の視点からセキュリティを考えた時、社会人の在学生からさまざまな業界の実践例を聞けたりと、技術面だけでなく総合的にセキュリティを学ぶことができます。

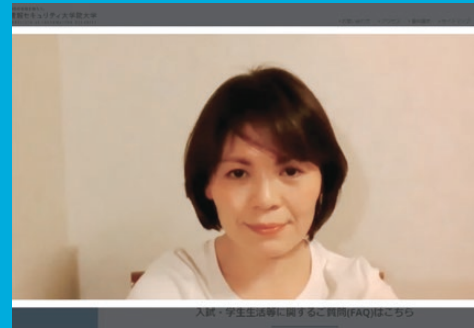
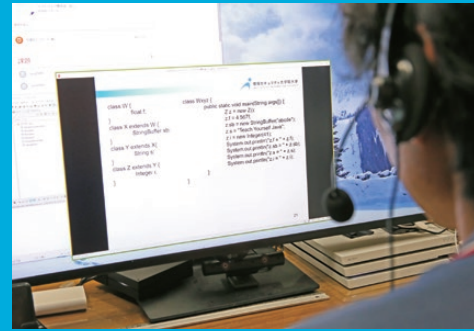
●学費が減免される特待生制度で
大学卒業後すぐに入学しやすくなる

オンライン受講の木曜日を除き4時限の頃には登校します。IISECには実務経験が豊富な先生も多く、企業ごとの強みやセキュリティの現状などを具体的に聞けるのも魅力の一つです。4時限の後に1階ロビーで在学生同士が交流する「ティータイム」に極力参加。先輩や他の研究室の社会人学生と話す視界が広がり、研究の進め方や各業界での仕事の様子も分かって今後の参考になります。

土曜日の「情報セキュリティ技術演習」は仮想環境の中でサイバー攻撃とその防御を体験できる演習。授業では漠然とした知識でも実践すると明確になって、より理解を深められる貴重な時間です。

●実務経験豊富な先生や社会人学生から
実社会でのセキュリティを学べる

私の1週間



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講義・演習を中心に、オンラインで受講可能な科目、オンデマンド受講の科目も設定するなど、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。

入学して実感した大学院の魅力

セキュリティの実践的な研究経験を企業が評価
業界の在学生や修了生との交流も就活のカギに。



阿部 草太さん
Sota ABE
博士前期課程 2 年
東海大学情報理工学部出身
(2025 年 4 月入学)

セキュリティ業界で専門性を生かせる就職を目指して入学

幼い頃にテレビで見たハッカーのドラマでセキュリティに興味を持ち、大学は情報系の学部に進み、研究テーマもPQC(耐量子計算機暗号)などセキュリティと関連がある量子コンピュータを選びました。企業説明会やインターンシップなどに参加しましたが、セキュリティを仕事にするなら大学院進学が必要だと感じてIISECに入学。セキュリティをキーワードに、「法学基礎」「実践的IoTセキュリティ」「オペレーティングシステム」など、文理横断で開講される科目を網羅的・体系的に学んで知識の幅を広げられました。

ドローンの測位信号の脆弱性に対する攻撃手法を研究

興味の始まりがハッカードラマだった影響で攻撃側の視点を学びたいと考え、仮想環境の中でシステムへの攻撃と防御を行う「情報セキュリティ技術演習」も履修。現在は大久保先生の研究室で、社会で急速に普及してきたドローンの脆弱性と攻撃手法を検討しています。中でもドローンが位置制御に使うGPSの通信が暗号化されていない脆弱性を利用し、誤った位置情報で誤誘導するGPSスプーフィングに着目。先行研究で紹介された事例を確認するため、現在はシミュレーション環境の構築を急いでいます。社会人学生が多いIISECでは、授業やゼミで業界の現状やビジネスに導入した場合の課題など実践的で多様な視点から意見が交わされます。学部卒の私も新たな発見・気づきの機会が得られ、ISSスクエアやenPiTではセキュリティを学ぶ他大学の学生と交流する中で、暗号についてより専門的な視点から学べました。

社会人との交流が研究でも就活でも大きな助けに

先輩や他の研究室の在学生と気楽に交流できる「ティータイム」の時間や、OB・OGが来校するホームカミングデーなどでセキュリティ業界の現場を詳しく知り、就活に臨めたのもメリット。企業の面接でも高く評価されました。私のように学部卒でIISECを検討している人には、就職にも強い点を強調したいですね。セキュリティ会社の内定を得て、攻撃手法を用いて組織のセキュリティ診断を行うレッドチームに加わる予定で、人と話すことが好きなので顧客へのヒアリングや説明がきちんとできるエンジニアを目指しています。

セキュリティと個人情報保護の観点が重要となる医療情報の利活用に対しEUの法制度との比較研究を解決策の一助に。



平瀬 伸恵さん
Nobue HIRASE
博士前期課程1年
株式会社インプレッションズ代表取締役
(2025年10月入学)

セキュリティリスクの観点を自社経営の参考に

私は人材育成のための研修会社を2015年に創業し、一般企業向け、医療機関・医療大学向けなど、各種の研修コンテンツを提供しています。そうした中で現在のメディアリテラシー教育への知見を広げたいと考え、科目等履修生としてIISECに入学。「セキュリティ経営とガバナンス」などの科目で、以前取得したMBAではセキュリティリスクまでマネジメントできないと気づき、自社の経営方針と整合性のあるセキュリティ対策を考えるため、正科生として博士前期課程に入学しました。IISECにはセキュリティ業界や官公庁で働く在学生も多く、当社のビジネス領域を越えて人脈が広がるなど素晴らしい学びの場だと感じています。

多様なステークホルダーに対する「落とし所」を模索

授業は「セキュリティの法律実務」や「ネットワーク設計とセキュリティ運用」など文理を問わず履修でき、文系出身の私でも技術系の科目を学べる機会が多いのも魅力です。私は医療業界とも関係が深く、研究テーマは「医療情報の利活用と個人情報保護に関する法的課題」に設定。医療分野の研究開発などのためにデータ収集と利活用を促す「次世代医療基盤法」が施行、改正されるも、なかなか医療DXは進まず、現場の負担も軽減されないことを喫緊の課題と捉えていました。入学後、所属する研究室の村上先生に相談したところ、EUのEHDS(欧州ヘルスデータスペース)などの参考例を示唆いただき、日本の現行制度の課題分析とEHDSとの比較検討から、多様なステークホルダーが納得できる形で医療情報の利活用のあり方を模索しています。

IISEC なら業務で活用できる力が身につく

IISECはセキュリティについて多方面から学べ、各界のスペシャリストを講師に招く特別講義では、その方が第一線で得た経験を非常に興味深く聞くことができます。すでに自身の業務でも「SNSからの情報漏洩対策」などのテーマで、インシデントへの初期対応を理解してクライアントごとにアドバイスできるなど、IISECでの経験が役立っています。オンラインやオンデマンドで受講できる科目も増え、働く社会人がさらに学びやすい環境になりました。最初は科目等履修生からでも構いません。まず一歩踏み出してください。

生成AIで一層高まる偽情報リスクについて発生・拡散・対策の観点で分析し対応を検討。

岡本 恵理子さん Eriko OKAMOTO
情報セキュリティ研究科 博士前期課程1年
株式会社ビジョン・コンサルティング
コンサルティング&IT事業本部コンサルティング部



時 限	月	火	水	木	金	土	日
1						個人識別と プライバシー保護	
2	朝からIISECに 登校して 院生室で仕事	自宅から リモートワーク または 出社して仕事	顧客を訪問後 都内のIISECの サテライト オフィスに移動	自宅から リモートワーク		セキュリティ システム監査	
3					自宅から リモートワーク または 出社して仕事		平日にできない まとまった 家事や買い物 または課題の レポートのまとめ
4						情報セキュリティ 技術演習I	
5	AIと機械学習	稲葉研究室の ゼミに参加 19時30分～ (オンライン)	情報セキュリティ 輪講I (オンライン)	リスクマネジメントと 情報セキュリティ (オンライン)			
6	セキュリティの 法律実務		帰宅して 家事など 空き時間に 授業の課題の レポートまとめ	業務終了後は 家事など 空き時間に 授業の課題の レポートまとめ	業務終了後は 家事など この日はIISECの 勉強は休んで リフレッシュ	帰宅して 家事など 空き時間に 授業の課題の レポートまとめ	
a		帰宅して家事など 授業の課題のレポートまとめ					

	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	18:20～19:50	16:20～17:50
2 時限	10:40～12:10	10:40～12:10	20:00～21:30	～
3 時限	13:00～14:30	13:00～14:30	22:00～24:00	18:00～24:00
4 時限	14:40～16:10	14:40～16:10		



1>土曜日の「情報セキュリティ技術演習」は攻撃・防御の状況がリアルに分かり、学んだ内容が“腹落ち”する 2>仕事、家庭、勉強と忙しく過ごす中、登校した日は院生室でも仕事をするなど有効活用。一方で休む日を設けることも大事

●セキュリティ推進業務に関わる体系的な知識の必要性から入学

私はITコンサルティング会社に在籍し、メディア業界を顧客にサイバーセキュリティ対策など長期にわたりセキュリティ推進業務に従事しています。しかし業務を根本から変えそうな生成AIに刺激を受け、2023年に通信制大学に3年次編入「FOI」してAIや機械学習の専門知識を習得。卒業後はセキュリティに関する知識をさらに広げ、体系的に整理する必要性を感じIISECに入学しました。

●AIの基礎理論や法律の観点など知識を広げて偽情報への対応を検討

入学後はセキュリティ心理学が専門の稲葉先生の研究室で、「生成AIで格段に高まった偽情報リスクに企業・組織はどう対応すべきか」を研究。今は先行研究から偽情報の発生、拡散、対策に関する論文を分析して検討しています。稲葉先生の研究指導はオンライン開講なのでどこにいても参加でき、研究に役立つ論文の紹介や方向性の示唆など非常に手厚くサポートしていただけます。加えて「AIと機械学習」で基礎理論を強化し、「セキュリティの法律実務」では偽情報などのセキュリティ対策について法律での扱いなども学んでいます。

私の1週間 講義と演習で理解が深まり在 student との交流で視野が広がる

土曜日の「個人識別とプライバシー保護」はAIエージェントによる認証の課題など、外部の専門家も招いて最先端の話題を深く学べる貴重な機会です。また「情報セキュリティ技術演習」では仮想環境でのシステムへの攻撃やデジタルフォレンジックの実践など、経験。私の業務はマネジメント寄りなので、実際に手を動かしてセキュリティの奥深くまで学べるのはとても魅力的です。それに在 student は多様な業界で働く社会人が中心なので、それぞれセキュリティ対策の進み具合や社内の協力体制などが違い、その中でどう対策するかといった取り組み事例を聞けるのはコンサルタントとしても非常に参考になります。

●オンライン受講もあり学びやすいリスクリングにも適した2年間

平日は日中を仕事、夕方からは授業と分け、月曜日と土曜日以外はオンラインで受講。仕事もリモートワーク中心なので、月曜日の空き時間は院生室の隔離されたスペースで仕事「FOI」をして、顧客訪問の際はIISECの都内サテライトオフィスで授業を受けるなど工夫しています。実務にすぐ生かせる実践的な内容も多く、AIによる変化を不安に感じる方やリスクリングを考えている方などもぜひIISECで学んでほしいですね。

セキュリティ業界の先輩たち

弁護士としてIISecで学び、法務領域でも情報学の学位を有する人材が注目される時代が訪れつつあると感じる。



片岡 弘さん Hiroshi KATAOKA
情報セキュリティ研究科 博士後期課程修了
(麻布台片岡法律経済事務所・八雲法律事務所顧問)

法律実務家と情報学

役所を定年退官し、弁護士登録をしました。訴訟に用いるデジタル証拠は、削除や改ざんが容易なため、デジタルフォレンジックやメタデータの開示などに関する訴訟手続の整備が必要になります。そこで、米国のeディスカバリという手続に注目し、デジタル証拠の特性に応じた手続の在り方について、技術面を含めて研究したいと思い、IISecの門を叩きました。IISecでの研究生活は充実して楽しいものでした。1年目は、週5日ほど通学して修了に必要な単位を取得し、2年目は修士論文作成を中心にしました。修士論文は、ディスカバリの越境的適用に関する問題点と対応の在り方を主たるテーマにしました。

修士(情報学)という学位は、データや情報セキュリティに関する基本的な事柄を学んだことを証明するもので、この分野で活躍したいと考える弁護士等の法律実務家にとって、専門性を示すのに相応しい学位だと思っています。

博士号取得を経て国際的AIガバナンス論の研究へ

研究を進めるなかで、データの越境移転に関する統一的ルールはなく、むしろ各国間で主張の対立が深まっていることを知りました。そのため、博士後期課程では、国際的データガバナンスに関する研究を軸にしました。約2年間で、国内および国際的な学会で合計10回を超える発表をし、内外の学術誌にも小論を掲載していただきました。博士論文は、「サイバー空間分裂回避のための越境的データガバナンス規範再構成」というテーマとしました。

博士号取得後は、サイバーセキュリティ法務を専門とする八雲法律事務所の顧問として名を連ねるとともに、研究生活を続けており、データやAI資源利用の国際的相互依存性に着目し、多中心的(ポリセントリック)ガバナンス論を基礎とする小論を作成するなどしています。最近では、フロンティアAIの利用をめぐる議論などを踏まえ、AI資源利用に関する国際的ガバナンスを確立すべきであるという考えに基づいて研究を展開しています。

弁護士としてIISecで学び、弁護士実務や企業法務の領域でも情報学の学位を有する人材が注目される時代が訪れつつあると感じています。

多角的かつ包括的な視点から複雑な社会問題を解決できる知識を身に付けられるのがIISecの魅力。



鈴木 悠さん Haruka SUZUKI
情報セキュリティ研究科 博士後期課程修了
(株式会社ラック)

拡散される偽情報への対策を

心理学の視点で検討するためIISecへ

大学で社会心理学を専攻し、専門学校でネットワークセキュリティを学んだ後、2006年に株式会社ラックに入社しました。入社後は主にセキュリティコンサルティング業務に従事していたのですが、出産・育児を機に「心理学というバックグラウンドを活かして社会貢献したい」と考えるようになり、2018年に研究職にジョブチェンジをしました。

海外レポートを調査していたところ、ソーシャルメディア上で拡散されるデイスインフォメーション(偽情報)が大きな問題となっていることを知りました。日本でも対策が必要だろうと手探りで研究を続ける中、「IISecに心理学博士の先生がいる」と紹介を受け、研究の学術的な価値を高めるために入学しました。

デイスインフォメーションの問題を解決するためには、技術的な対策だけでなく、法律・ガバナンスといった政策的な対策やユーザーを支援する認知的な対策も重要です。博士後期課程で履修できる博士演習では、専門領域が異なる複数の教員から指導を受けられるなど、IISecは複雑な社会問題を多角的かつ包括的な視点から解決するための知識を身に付けられます。博士後期課程修了後は、IISecで得られた視座のもと、総務省有識者会議の構成員として日本のサイバーセキュリティ政策の推進に貢献しています。

文理融合の知識でキャリアを磨き

「プラス・セキュリティ人材」に

近年、AIが標的の情報を収集・プロファイリングし、パーソナライズ化した攻撃をするという「人の脆弱性を狙ったサイバー攻撃の自動化」が進みつつあります。このため、これまでの技術的な対策に加え、悪意のある操作から人を守るための情報セキュリティが必要になってきます。

技術と人の観点から情報セキュリティの研究をできるのがIISecです。IISecでは、分野横断的な複雑な研究課題に取り組むことができます。サイバー攻撃は今後ますます多様化し続けることが考えられるため、文理融合の知識をIISecで習得し、プラス・セキュリティ人材になっておくことをお勧めします。

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Slerの仕事に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Sler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しています。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。

多様な業界・職種に関わるセキュリティIISecで自身の専門性とリンクさせて将来のキャリアを切り拓く力に。



松浦 栄亮さん Eisuke MATSUURA
情報セキュリティ研究科 博士前期課程修了
(三井物産セキュアディレクション株式会社)

理論的に根拠を積み重ねて結論を得る思考法が社会で生き抜く基盤に

学部生時代はPQC(Post-Quantum-Cryptography)の社会課題に関して研究していました。その過程でPQCを支える数学的な基盤に加え、サイバーセキュリティを取り巻く技術・社会課題にも強い関心を持つようになり、IISecへ進学しました。現在はIISecで培った知識や経験を活かし、セキュリティエンジニアとしてセキュリティ分野に携わっています。

IISecでは、セキュリティ分野を広く体系的に学ぶだけでなく、自らの研究テーマとして深く掘り下げられた点が大きな財産になっています。セキュリティという実社会と密接に関わるテーマを対象に、理論的に考え、根拠を積み重ねながら結論へ近づいていく経験は、単なる講義だけでは得られない学びでした。また、この思考法は、現在セキュリティ企業で働くうえでも非常に役立っています。複雑な事象を分解し、技術的背景やリスクを整理したうえで、根拠を持って判断する力は、実務において、ひいては今後の社会を生き抜く上で重要な基盤になっていると感じます。

生成AIや量子コンピュータの時代に

必要なセキュリティ人材を目指す

今後、生成AIの活用拡大や量子コンピュータの発展などにより、セキュリティを取り巻く環境はさらに大きく変化していくと考えています。新しい技術が社会に浸透するほど、それを安全に活用するためのセキュリティ人材の重要性は高まります。IISecには、幅広い業界からセキュリティに関心を持つ人材が集まっており、専門性を深めるだけでなく、多様な視点を得られる環境があります。

セキュリティは特定分野だけに閉じたものではなく、あらゆる業界・職種に関わる重要な力です。ぜひIISecでの学びを通じて、自分自身の専門性とセキュリティを結びつけてほしいと思います。IISecで得られる知識や考え方、そしてIISecで得た人とのつながりは、将来のキャリアを切り拓く大きな支えになるはずです。

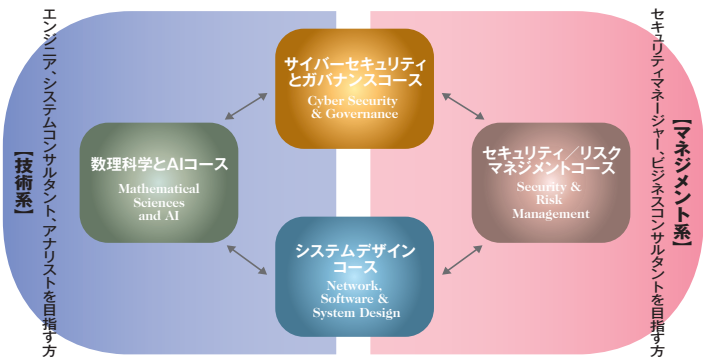


OBOGの協力による就職セミナー

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。

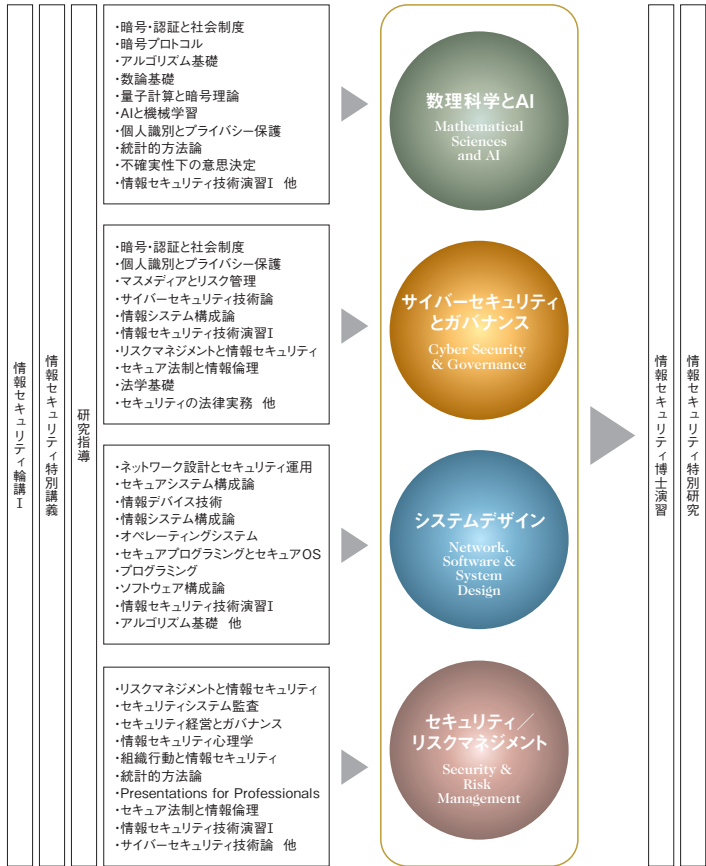
実社会における適正な情報セキュリティの実現には、暗号技術、ネットワーク技術、情報システム、管理運営、法制度、心理、情報倫理を融合させた総合的な対応が必要であり、それぞれの専門家が幅広い視野と見識をもって協力しあうことが不可欠です。情報セキュリティ研究科博士前期課程では、高度化・複雑化する企業・官公庁等の現場ニーズを踏まえ、技術系・マネジメント系とも幅広い人材育成需要、教育需要に応えるため、4つのコースフレームを設定しています。なお、指導教員の履修指導のもと、他のコースが推奨する科目も自由に履修することができます。博士後期課程では、博士前期課程修了の知識をベースに、情報セキュリティの構成要素に関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



■ 2026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			
研究指導	特設講義	選択	2	22	—	—
	特設実習	選択	2			
	情報セキュリティ演習	必修	6			
	研究指導Ⅰ	必修	6			
博士専門	研究指導Ⅱ	必修	10	—	6	—
	プロジェクト研究指導	必修	6			
	情報セキュリティ特別研究	必修	6			
	情報セキュリティ博士演習Ⅰ	必修	1			8
	情報セキュリティ博士演習Ⅱ	必修	1			
博士専門	情報セキュリティ博士演習Ⅲ	選択	1	—	—	8
	情報セキュリティ博士演習Ⅳ	選択	1			
計				46	46	8

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

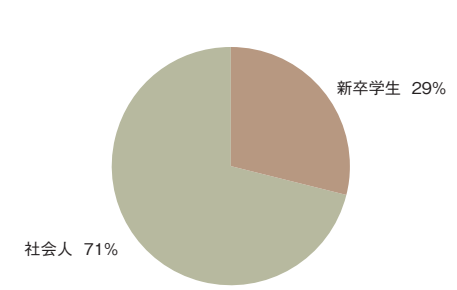
■ 社会人学生の所属組織

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】(2025-2026実績)
(株)エーアイセキュリティラボ／エクシオグループ(株)／(株)エヌ・ティ・ティ エムイー／(株)NTTデータ先端技術／NTTテクノクロス(株)／(株)NTTドコモ／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／キーウェアソリューションズ(株)／金融庁／警察庁／公安調査庁／(独)国立印刷局／(株)シーイーシー／CTCテクノロジー(株)／清水建設(株)／ソニー(株)／テルモ(株)／東京海上ディアーアル(株)／ニッセイ情報テクノロジー(株)／日本生命保険(相)／(株)日本総合研究所／パナソニックホールディングス(株)／東日本旅客鉄道(株)／(株)日立システムズ／防衛装備庁／(株)マープル／(株)三井住友銀行／三井住友信託銀行(株)／三菱電機(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。



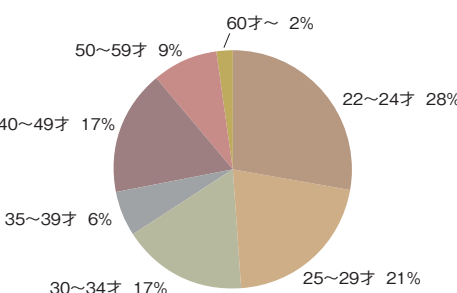
■ 博士後期課程

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】(2025-2026実績)
NTT(株)／NTTテクノクロス(株)／(株)NTTドコモ／NTTドコモビジネス(株)／警察庁／公安調査庁／さくら情報システム(株)／弁護士(第一東京弁護士会)／東京都立産業技術大学院大学／(株)日立システムズ／防衛省／防衛大学校／三井住友ファイナンス&リース(株)／楽天グループ(株)／(株)ラック

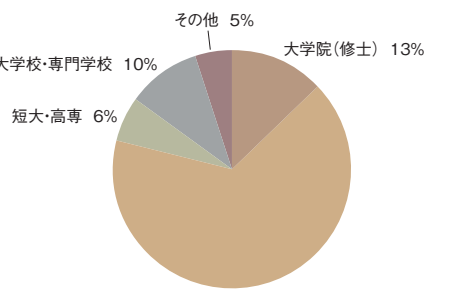
■ 年齢構成(入学時)

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。



博士前期課程
(修士課程)

授業科目履修例
2026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1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	暗号・認証と 社会制度	情報セキュリティ 技術演習Ⅰ
4	アルゴリズム基礎				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	セキュリティの 法律実務		ソフトウェア 構成論	リスクマネジメントと 情報セキュリティ	国際標準と ガイドライン	
オンデマンド講義 法学基礎 ネットワーク設計とセキュリティ運用						

▼＜社会人学生の1年次履修例＞

◆前期 (4月7日～8月1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	(研究指導)	プログラミング				セキュリティ システム監査
3	(研究指導)	オペレーティング システム		統計的方法論	暗号・認証と 社会制度	情報セキュリティ 技術演習Ⅰ
4	アルゴリズム基礎	(研究指導)			数論基礎	
5	知的財産制度 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 or 特設講義 (インテリジェンスの基礎)	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	リスクマネジメントと 情報セキュリティ	国際標準と ガイドライン	
オンデマンド講義 法学基礎 ネットワーク設計とセキュリティ運用						

■ 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。

◆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						セキュア プログラミングと セキュアOS
2						
3				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 隔週開講
4	特設講義 (ブロックチェーン理論)	暗号プロトコル	(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	情報システム 構成論 or セキュア法則と 情報倫理	Presentations for Professionals	
6	特設講義 (AIセキュリティ) 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 or セキュリティ経営と ガバナンス	特設講義 (データ・サイエンスと アナリティクス)	

◆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						セキュア プログラミングと セキュアOS
2	(研究指導)	プログラミング				
3	(研究指導)	オペレーティング システム		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 隔週開講
4	特設講義 (ブロックチェーン理論)	暗号プロトコル	(研究指導)	特設講義 (ハッキングと マルウェア解析) or 特設講義 (国際関係論)	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	情報システム 構成論	Presentations for Professionals	
6	特設講義 (AIセキュリティ) 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 or セキュリティ経営と ガバナンス	特設講義 (データ・サイエンスと アナリティクス)	

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)

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

■ 履修モデル[博士前期課程2年制プログラム]

○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
[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) 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							

■ 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

2026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

・東京大学大学院情報理工学系研究科

・中央大学大学院理工学研究科

・The Information Security Group, Royal Holloway, University of London

・国立情報学研究所

・大連大学 他

○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

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。

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

▼【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1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	（研究指導）	プログラミング				セキュリティ システム監査
3	（研究指導）	オペレーティング システム		統計的方法論	暗号・認証と社会制度	情報セキュリティ 技術演習I
4	アルゴリズム基礎	（研究指導）			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 特設講義 （クリティカル・シンキ ングとインバケーション）	特設講義 （クリティカル・シンキ ングとインバケーション）	
6	セキュリティの 法律実務		ソフトウェア構成論	リスクマネジメントと 情報セキュリティ	国際標準と ガイドライン	

オンデマンド講義 法学基礎 ネットワーク設計とセキュリティ運用

▼【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1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	（研究指導）	プログラミング				セキュリティ システム監査
3	（研究指導）	オペレーティング システム		統計的方法論	暗号・認証と社会制度	情報セキュリティ 技術演習I
4	アルゴリズム基礎	（研究指導）			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	情報デバイス技術 or 特設講義 （インディペンデンスの基礎）	特設講義 （クリティカル・シンキ ングとインバケーション）	
6	セキュリティの 法律実務		ソフトウェア構成論	リスクマネジメントと 情報セキュリティ	国際標準とガイドライン	

オンデマンド講義 法学基礎 ネットワーク設計とセキュリティ運用

▼【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1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	（研究指導）	プログラミング				セキュリティ システム監査
3	（研究指導）	オペレーティング システム		統計的方法論	暗号・認証と社会制度	情報セキュリティ 技術演習I
4	アルゴリズム基礎	（研究指導）			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	情報デバイス技術 or 特設講義 （インディペンデンスの基礎）	特設講義 （クリティカル・シンキ ングとインバケーション）	
6	セキュリティの 法律実務		ソフトウェア構成論	リスクマネジメントと 情報セキュリティ	国際標準とガイドライン	

オンデマンド講義 法学基礎 ネットワーク設計とセキュリティ運用

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p27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

2026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、2026年7月時点の実績・計画に基づいて掲載されています。

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、大規模言語モデル、AIEージェント、数論アルゴリズム、耐量子計算機暗号、量子暗号、コミットメントプロトコル、ゼロ知識証明、秘密分散、匿名化 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、DevSecOps、脅威分析、リスク評価、フォレンジック、マルウェア分析、攻撃検知と防御、脆弱性検知、欺瞞、CTI、OSINT、ゼロトラスト、生成AI応用、AI活用のセキュリティ問題、システムセキュリティ、セキュアOS、ハードウェアセキュリティ、TEE 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



AIによる開発の自動化が進展する一方で、「自動化されたシステムの安全性・信頼性をいかに人間が担保するか」は、これまで以上に重要な研究課題となっています。そのためには、従来のセキュリティ技術に加え、新たな課題に対応するための知識と実践力が求められます。本コースでは、受講者一人ひとりのキャリアや専門性に応じて、多様なセキュリティ技術を学ぶ機会を提供します。理論と実践の双方を通じて、次世代のセキュリティを支える力を養います。皆様の積極的な挑戦を心より歓迎します。

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、AI法、能動的サイバー防御法、インテリジェンス 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実データ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、レピュテーションコントロール、セキュリティ教育 他
--------------	---

◆修士論文イメージ

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

コースリーダー
からの
メッセージ

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。

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

パターン1

修士学位取得専念型

修士論文に向けての 知識の獲得と研究に重点を置きたい

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

▶これまで提出された修士論文題目は

情報セキュリティ研究科ウェブサイトをご覧ください。

<https://lab.iisec.ac.jp/>



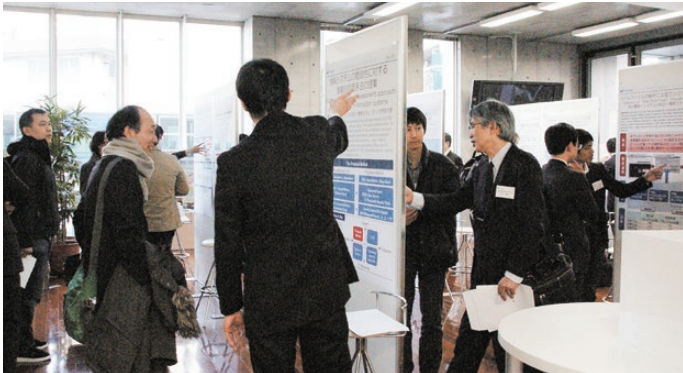
パターン2



ISSスクエア 併修型

研究室や大学を超えた活動を通じて 幅広い視野を養い、研究を実務に生かしたい

ISSスクエア(研究と実務融合による高度情報セキュリティ人材育成プログラム)は、本学と中央大学、国立情報学研究所他、11の企業・研究機関の産業連携による博士前期(修士)課程生のためのオプションプログラムです。本学の充実した講義群に加え、サブゼミ的な位置づけの研究分科会や分野横断型のワークショップでの活動、セミクロー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。



*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3



ISSスクエア + enPiT-Security 併修型

ISSスクエアの活動に加えてできるだけ 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。



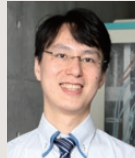
講義・演習をサポートしてくれる卒業生の声

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、攻撃コードやマルウェアに関する研究に取り組んでいました。担当する講義は「特設講義(ハッキングとマルウェア解析)」です。座学に加えて、グループワークや提供VMを用いたハンズオンを通じて、基礎技術や実践力を身につけることができます。また、大久保研究室において研究指導を担当します。研究の進め方の基礎から、論文執筆や学会等での発表まで、皆さんの挑戦を支援します。

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 ISSsquare

文部科学省の平成19年度「先進的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、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324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



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
中核の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。

博士前期課程
(修士課程)授業科目概要
2026

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)

■情報セキュリティ論講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。暗号・認証技術の基礎を習得し、実社会における応用について知見を深めたい学生を対象とする。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

暗号プロトコルとは、複数のパーティがお互いの入力を隠したまま、必要な情報のみをやりとりし、目標とする機能を協調して実現する方法である。「協調して」とは言ってもプロトコルを実行するパーティには悪意を持って他のパーティの情報を盗み取ろうとするものがいるので、暗号技術を用いて安全性を確立することが肝要となる。この講義では、暗号プロトコルのフォーマルな安全性定義を踏まえた上で、その実現方法の理論的な基礎を学ぶ。さらに、より実践的な方式として zk-SNARK や準同型暗号についても学ぶ。

■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、法制度的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、インターネットの基盤技術に対する理解を深めた上で、それらに基づいて守るべき企業(プライベート)のネットワークや情報資産を防御する方法および要素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、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

本科目では、情報システムの重要な位置を占めるソフトウェアについて、その脆弱性を可能な限り事前に排除し、よりセキュアなソフトウェアを設計・構築・運用するための原則、概念、技法、ガイドライン、プログラミング言語固有の問題、ツールなどについて紹介する。そして、ソフトウェアの脆弱性を完全になくすことは困難であることを前提に、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を行う、セキュア OS の考え方を解説する。

■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

本講義は実務家教員が担当し、リスクマネジメントの基礎を体系的に学ぶとともに、情報セキュリティマネジメントとの関係を理解することを目的とする。リスクの定義・分類、リスク処理手法、リスクマネジメントのプロセスを整理し、組織における情報セキュリティガバナンスの役割と重要性を考察する。さらに、ネットワーク社会の進展に伴い高度化するサイバーリスクを分析し、経営戦略と統合した視点からリスクマネジメントを実践する能力を養う。加えて、全6回の演習では発表と討議を行う双方向型ゼミ形式とし、実践的なリスクアセスメントと対応策の策定を通じてリスク管理における理論と実務の橋渡しを図る。

■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×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

近年では、サイバー攻撃がますます複雑化、巧妙化しており、様々なタイプのサイバーインシデントが発生するようになっていく。このようなインシデントについては、技術的観点からの対応だけではなく、法的・倫理的観点からの対応や、企業ガバナンスの観点からの対応が必要になる。この授業は、サイバー空間において発生している様々なタイプのインシデントについて取り上げた上で、法律、制度、倫理などの多様な観点から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 business 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. Recent student comments: "Through this class, I overcame my resistance to presentation preparation and learned how to prepare and give a good presentation." Try this class and see how you can improve! (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、予測分析をはじめとするデータ・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)は、「前提や常識を疑い、物事を多角的に捉える」思考法であり、イノベーションの基盤となる。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に加え、ロジカルシンキングやデザインシンキングの理論と実践手法を体系的に学び、それらをイノベーション創出やビジネスプロセス設計へ応用する方法を理解する。事例分析と討議を通して多面的な問題把握力を養い、全3回の演習では発表とフィードバックを行う双方向型のゼミ形式で実施する。必要に応じてゲスト講師も招く。

■ 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2025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案するとともに、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



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、特設講義(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

- 主な研究業績
1. 水上昌大, 有田正剛, 耐量子安全なゼロ知識サムチェックプロトコルの構成について, 情報処理学会研究報告 Vol.2026-CSEC-112 No.62, 2026/3.

2. 松浦栄亮, 黒澤敦, 有田正剛, 2次元の同種写像を用いた耐量子安全なコミットメントスキームの構成に関する研究, 日本応用数理学会 第22回研究部会連合発表会 C3-3-4, 2026/3.

3. 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.

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および量子暗号
- 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、暗号プロトコル、量子計算と暗号理論、情報セキュリティ輪講Ⅱ、研究指導

■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客員研究員。2013年よりJRR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., Kusakami, 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. Azezes (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、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、特設講義(ブロックチェーン理論)、特設講義(AIセキュリティ)、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

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

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

Atsuhiko GOTO

■主な研究業績

1. 小梶 顯義, 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, Atsuhiko 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, Atsuhiko 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 ・重要インフラのセキュリティと大規模リスク対応
・インターネットセキュリティ技術 ・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、サイバーセキュリティ技術論、情報セキュリティ特別講義、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

22

21

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

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所博士後期課程了 博士(工学)。キャン(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

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
全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、全沢星橋大学等を経て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
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

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。産学博士。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、海上保安庁入庁監視委員、情報総研推進機構契約監視委員会委員、日本公認会計士協会監査・保証基準委員会委員有識者懇談会議長、日本内部監査協会名誉会員などを兼任。[異議不正-最新報] (同文館出版、2019年) [ITのリスク-統制-監査] (同文館出版、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
Mitsuhiro 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

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、2016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



専任

小林 良樹
教授
Yoshiki KOBAYASHI



■プロフィール
早稲田大学博士(学術)、ジョージワシントン大学修士(MIPP)、香港大学修士(MIPA)、トロント大学修士(MBA)。1987年、東京大学法学部卒業後に警察庁入庁。在香港日本国総領事館領事、在米国日本国大使館参事官、内閣情報調査室審議官等として主に国際テロ対策等安全保障関係の業務に従事。2019年3月、内閣官房内閣審議官(内閣情報調査室・内閣情報分析官)を最後に退官。2019年4月から2026年3月まで明治大学公共政策大学院(専門職大学院ガバナンス研究科)特任教授を務めた後、同年4月より現職。あわせて防衛大学校の非常勤講師等も務める。専門はインテリジェンス研究(政策判断、意思決定、情勢分析のシステム)、テロリズム、テロ対策等。現在の主な研究テーマは、「安全と権利自由の両立のための、インテリジェンス組織のガバナンスの在り方」、経済安全保障(組織におけるリスク評価と意思決定支援の制度)等。詳細はこちら: <https://researchmap.jp/read0152553>

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。

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。

専任

盛合 敏
教授
Satoshi MORIAI



■プロフィール
1988年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。NTT情報通信処理研究所、株式会社ぶらなネットワークス、NTTサイバースペース研究所、NTTソフトウェアイノベーションセンター、NTTテクノクロス等を経て、2026年4月より本学教授。この間、オペレーティングシステム(マイクロカーネル、分散リアルタイムOS、セキュアOS)、インターネット、高可用システム、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マネジメントに従事。

■主な研究業績

- 小林良樹「インテリジェンスの基礎理論」(講談社、2025年)
- 小林良樹「なぜ、インテリジェンスは必要なのか」(慶應義塾大学出版会、2021年)
- 小林良樹「テロリズムとは何かー(恐怖)を読み解くリテラシー」(慶應義塾大学出版会、2020年)
- 小林良樹「犯罪学入門:ガバナンス・社会安全政策のアプローチ」(慶應義塾大学出版会、2019年)
- Kobayashi, Y. (2024). The Lessons Learned from the Tokyo Subway Sarin Gas Terrorist Attack by Aum Shinrikyo on 20 March 1995. Corder, Gray & Wright, Martin (ed.). Routledge International Handbook of Policing Crises and Emergencies, Routledge, pp. 402-413. <https://doi.org/10.4324/9781003265214-32>
- Kobayashi, Y. (2023). Integrating Japan's Intelligence Community: analyzing the effectiveness of the Director of Cabinet Intelligence as a coordinating body. Intelligence and National Security, 38(7), 1151-1170. <https://doi.org/10.1080/02684527.2023.2228044>
- Kobayashi, Y. (2020). The Intelligence Community in Japan: Small Intelligence of Economic Superpower - Reform in Progress. de Graaf, Bob (ed.). Intelligence Communities and Cultures in Asia and the Middle East: A Comprehensive Reference, Boulder, USA: Lynne Rienner Publishers, pp. 149-162. <https://doi.org/10.1515/9781626378957>
- Kobayashi, Y. (2015). Assessing Reform of the Japanese Intelligence Community. International Journal of Intelligence and CounterIntelligence, 28(4), 717-733. <https://doi.org/10.1080/08850607.2015.1051453>

■主な研究テーマ

・インテリジェンスのガバナンス・カウンターインテリジェンス・テロリズム・経済安全保障

■主な担当科目

特設講義(インテリジェンスの基礎)、特設講義(国際関係論)

■担当コース

サイバーセキュリティとガバナンスコース

■主な研究業績

- Taichi Takemura, Ryo Yamamoto, Kuniyasu Suzuki, TEE-PA: TEE Is a Cornerstone for Remote Provenance Auditing on Edge Devices With Semi-TCB, IEEE Access, 2024
- Kuniyasu Suzuki, 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.
- Kuniyasu Suzuki, 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.
- Nguyen Anh Quynh, Kuniyasu Suzuki, VirtICE: Next Generation Debugger for Malware Analysis, BlackHat USA, 2010.
- 須崎有康, IPA未踏事業, KNOPIX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、セキュリティ／リスクマネジメントコース

■主な研究業績

- 村上康二郎「プライバシー権と個人情報保護法制の関係に関する一試論」情報セキュリティ総合科学16号1～20頁(2025年)
- 村上康二郎「プライバシー権論における信託義務説の再検討」情報セキュリティ総合科学15号1～18頁(2025年)
- 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)
- 村上康二郎「プライバシー権に関する信託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)
- 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)
- 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、個人識別とプライバシー保護

■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

■主な研究業績

- 森田和孝、藤田智成、盛合敏. Sheepdog:仮想マシンのための対称型クラスタストレージ. 情報処理学会 ACS論文誌 Vol.5 No.2, 2012年3月.
- 佐藤孝治、小西隆介、木原諒司、天海良治、盛合敏. ログ構造化ファイルシステムNILFSの設計と実装. 情報処理学会 ACS論文誌 Vol.2 No.1, 2009年3月.
- Y. Tamura, K. Sato, S. Kihara, and S. Moriai. Kemari: Virtual Machine Synchronization for Fault Tolerance. USENIX Annual Technical Conference 2008, June 2008.
- S. Moriai and H. Tokuda. Dynamic Loadable Object Support for Real-Time Mach Kernels. International Conference on Worldwide Computing and Its Applications, March 1997.
- S. Moriai, S. Kihara, and A. Nambu. Memory Management Mechanism and External Resource Manager Interface for Continuous Media Objects. Mach/Chorus Workshop in USENIX 1994 Symposium on Operating Systems Design and Implementation, Nov. 1994.

■主な研究テーマ

・クラウドセキュリティ、高可用システム、ネットワークセキュリティ
・セキュアでリアルタイムなシステム基盤(OS、言語、クラウド基盤)

■主な担当科目

アルゴリズム基礎、オペレーティングシステム、情報システム構成論、セキュアプログラミングとセキュアOS

■担当コース

システムデザインコース

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の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。



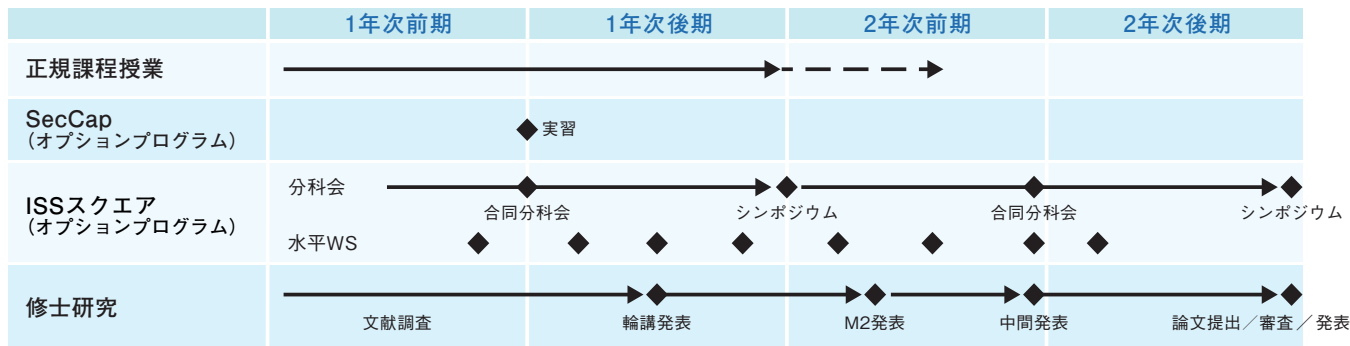
院生自習・実験室は平日は夜22時30分まで、土曜日は夜21時30分まで開放しています。(2026年度)



教育研究環境

新しい一步に向けて、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。

■ 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

当該年度修了生に加え、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（2026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	国立研究開発法人 産業技術総合研究所 執行役員 情報・人間工学領域 領域長	田中 良夫
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	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KDDI総合研究所 取締役執行役員 副所長	清本 晋作	富士通株式会社 富士通研究所 エグゼクティブアドバイザー	津田 宏
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	NTT株式会社 NTT社会情報研究所 所長	中嶋 良彰
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	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
三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 グループマネージャー	鈴木 大輔	国立研究開発法人産業技術総合研究所 フェロー 早稲田大学 理工学術院総合研究所 客員上席研究員/研究院 客員教授	松本 勉 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（2026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	株式会社日立製作所 研究開発グループ	志村 明俊
日本放送協会(NHK) 理事・技師長	伊藤 寿浩	Digital Innovation R&D Managing Director	
株式会社NTTデータグループ 部門執行役員 技術革新統括本部長	稲葉 陽子	神奈川県 副知事	首藤 健治
早稲田大学 研究院 教授	遠藤 典子	日本経済新聞社 編集委員	須藤 龍也
三菱電機株式会社 上席執行役員 研究開発本部長	岡 徹	株式会社MM総研 理事長	関口 和一
NTTDコムビジネス株式会社 取締役 執行役員 経営企画部長	奥澤 慎哉	慶応義塾 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
ニッセイ情報テクノロジー株式会社 代表取締役社長	岸淵 和也	横浜市 副市長	松浦 淳
富士通株式会社 情報セキュリティ本部 CISO戦略統括部xSIRT室 室長	北泉 公之	国立研究開発法人情報通信研究機構 執行役 理事	盛合 志帆
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	早稲田大学基幹理工学部 情報通信学科 教授	森 達哉
芝浦工業大学 客員教授	國井 秀子	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
独立行政法人情報処理推進機構 理事長	齊藤 裕		
株式会社東芝 総合研究所	斯波 万恵		
AIデジタルR&Dセンター セキュリティ技術部			

敬称略、氏名五十音順

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

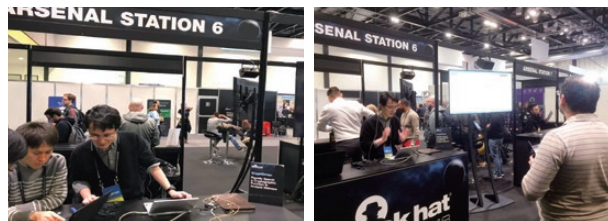
■ 課程外教育プログラム等の優待受講

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 (※2026年4月現在)
第一種奨学金 (無利子)	50,000円又は88,000円 (博士前期課程の場合)
	80,000円又は122,000円 (博士後期課程の場合)
第二種奨学金 (有利子)	5, 8, 10, 13, 15万円のなかから選択

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

② 岩崎学園奨学金(有職の社会人も利用可能です)

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

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

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

■ 特待生制度

人物、学業成績が特に優秀であり、自立心と向上心が旺盛な情報セキュリティ研究科博士前期課程[2年制]入学志願者*の中から特待生選抜試験に合格した者に対し、授業料等の減免を行う制度です。

(※4年制大学等卒業見込み者に限ります。出願資格の詳細については、本学ウェブサイトに掲載の特待生選抜学生募集要項にてご確認ください)

○ 特待生選抜試験に合格した場合の初年度学費

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

○ 特待生募集人数:若干名(特待生Ⅰ、特待生Ⅱとも)

情報セキュリティ大学院大学 セキュアシステム研究所

Secure System Laboratory



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

2025年度より、セキュアシステム研究所は、次の4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ます。

① 重要産業のサプライチェーンリスクにおける アジャイルガバナンス プロジェクト (CA:Critical Industries Risk and Agile Governance)

金融機関などの重要産業におけるサプライチェーンリスク分析と、環境変化に迅速に対応可能なガバナンスに関わる調査・提言を行います。

② 情報戦と安全保障プロジェクト (IN:Information Warfare and National Security)

現代社会の情報戦が安全保障に大きな影響をもたらす懸念が高まっています。この課題について、国際政治学、認知心理学、AI およびビッグデータ分析技術など、多角的に分析・調査を進めます。

③ サイバーセキュリティプロジェクト (CS:Cyber Security)

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2つの活動を進めます。

- ・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。
- ・最新セキュリティ技術や政策のグローバル動向を調査します。

④ セキュリティ人材キャリア開発プロジェクト (HR:Human Resource)

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。

■ 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。

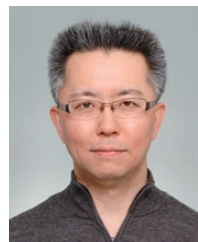


岩井 博樹
株式会社サイント
代表取締役

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。最近では、サイバーインテリジェンスに注力しています。

今や情報セキュリテ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



ゼミ合宿



新入生歓迎パーティ



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の、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。



〒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

Contents

- 1 桑名栄二学長と後藤厚宏特別学長補佐（対談）
- 3 新しい社会を歩むIISec
- 9 在校生プロフィール
- 10 情報セキュリティ研究科（修士課程・修士課程）について
- 11 修士前期課程紹介
- 20 修士後期課程紹介
- 21 教員紹介
- 25 フォトメッセージ
- 30 セキュアシステム研究所紹介

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	情報セキュリティ総合科学専攻	博士前期（修士）課程 [2年制]	2年	55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。

