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

2018-2019

情報セキュリティが支える
新たなイノベーションが
時代の流れを変えていく。

人はつながることでイノベーションを生み、社会を変えてきました。つながりによる情報の共有、知識の継承、集団行動は、狩猟や農耕から工業、情報へと産業構造の変革を促し、地域と世界の距離を縮め、新たな仕事や生活を育み、一人ひとりの可能性を大きく広げています。

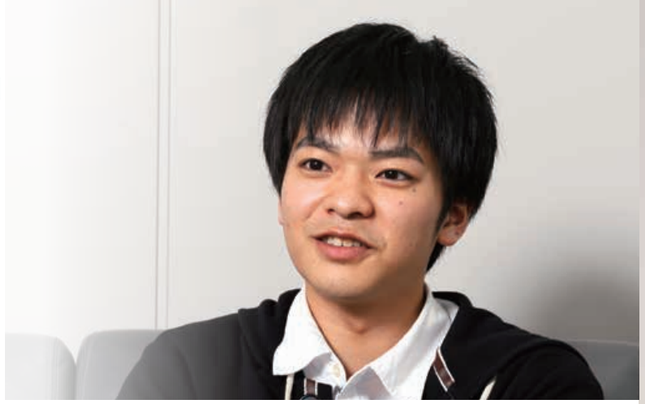
そして今、人々は高度な情報ネットワークが現実社会と複雑に交わるSociety 5.0に足を踏み入れました。24時間休みなく膨大な情報が収集・解析され、個人の意思決定や社会サービスに活用される社会で、「情報セキュリティ」は安全・安心を支える重要なファクターとなっています。

2004年に開学したIISEC（情報セキュリティ大学院大学）は、今後の社会基盤となる情報セキュリティに早くから着目し、文理融合の学問体系の構築、高い専門性を持つ人材育成を目的に教育・研究を進めてきました。

内容は暗号などの数理科学、ネットワーク、システムデザイン、リスクマネジメント、企業統治や法制・倫理など幅広く、それらを実務経験・指導経験が豊富な教員が中心となって担当し、実践力を養う教育と研究指導を行っています。さらに講義と演習による体験的教育、産学官が連携した人材育成などで、情報セキュリティの知識を体系的に学び、修士・博士論文にまとめる力が身につけられます。

また多様な科目を選ぶ指針となるよう4つのコースフレームを設定。自らの専門性や将来の目標に合った学習設計を容易にする一方、興味に応じてコース間の自在な履修も可能な柔軟なカリキュラム構成となっています。

IISECの修了生は博士前期・博士後期合計で約400名となり、すでに企業や省庁など社会の各分野で活躍中です。そうした同窓生のつながりも大きな強みとして、日本と世界の情報セキュリティを進化させ、より豊かで安心できるSociety 5.0の実現を目指していきます。



CHANGE MY LIFE 大学院でこう変わった［新入生編］

門口 雅志さん

社会のさまざまな分野と密接に関わる情報セキュリティを基礎から学びたい。

情報セキュリティ研究科　博士前期課程1年

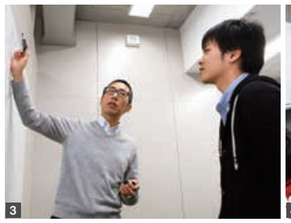
木更津工業高等専門学校専攻科卒業
専攻科在籍中、IISECでのインターンなどで情報セキュリティへの関心を深め、文理を融合させて学べる点も魅力に感じて入学。

時限	月	火	水	木	金	土	日
1	午前中は自宅で過ごし、早めの昼食を済ませて大学院へ。JR川崎駅のそばに住んでいるので、横浜駅近くのIISECまで通学は便利						
2						セキュリティシステム監査	
3	研究室で資料や論文を読む自習時間。	オペレーティングシステム	研究室で資料や論文を読む自習時間。	統計的方法論	研究室での自習時間		日曜日は完全オフ日。自宅で読書やゲームなど。夕方から近くに買い物に
4	16:20からはティータイムに参加	セキュアシステム構成論	16:20からはティータイムに参加	研究室での自習時間とティータイム	アルゴリズム基礎	情報セキュリティ技術演習I	
5	AIと機械学習	研究指導	情報セキュリティ輪講I	情報デバイス技術			
6	ソフトウェア構成論	研究指導	インターネットテクノロジ	ネットワークシステム設計・運用管理			
α	気分を切り替えて帰宅。研究が本格化したら研究室に居残りする可能性も						

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


1


2


3


4

1>多様なバックグラウンドを持つ学生や先生と気軽に話せる「ティータイム」は楽しみな時間。 2>研究室で以前の研究事例などを先輩に質問。 3>毎週火曜日は研究指導で担当教員の橋本先生からアドバイスを受けます。 4>「情報デバイス技術」の講義風景。

◉技術と人間の心理の両面からアプローチする点に興味

親戚に「興味のある分野に集中できるから」と勧められ高専に入学。情報工学を専門に選び、研究室では脳波を計測して脳の活性化の度合いを調べて、効果的な学習方法を検討していました。

情報セキュリティに関心を持ったのは専攻科への進学後で、技術と人間の心理の両面からアプローチする面白さに加え、今後重視される分野という将来性への期待もありました。高専本科5年＋専攻科2年卒業で学士が得られるため、IISECの博士前期課程に入学。幸い特待生入試に合格したので、学費の負担が軽減されたのもよかったですね。

◉脆弱性を持たせたシステムを攻撃するなど実習も実践的

入学して1カ月足らずですが「AIと機械学習」など今の話題を取り上げる講義や、コンピュータのハードウェア、デバイスが幅広く学べて技術面の知識の整理に役立つ「情報デバイス技術」などに期待しています。また土曜日午後の「情報セキュリティ技術演習I」は実験用に脆弱性を持たせたシステムを実際に攻撃するなど、貴重な経験ができるのが楽しみです。

私は工学が専門でしたが、指導教員の橋本先生にも「法律や心理も重要」とアドバイスを受け、大学院では「人がどう考えるか」「社会にどう影響するか」など視野を広げて学びたいと思います。

私の1週間

◉午後の空き時間は研究室で自習 人脈が広がるティータイムも楽しみ

授業の終了が21時30分と遅いため、午前中の履修がない日は自宅で過ごし、12時頃に大学院到着。夕方からの授業なら、自分が所属する橋本研究室で参考書や過去の論文を読むなど自習するほか、大学院のTA（教育補助業務従事者）として講義の準備なども手伝っています。

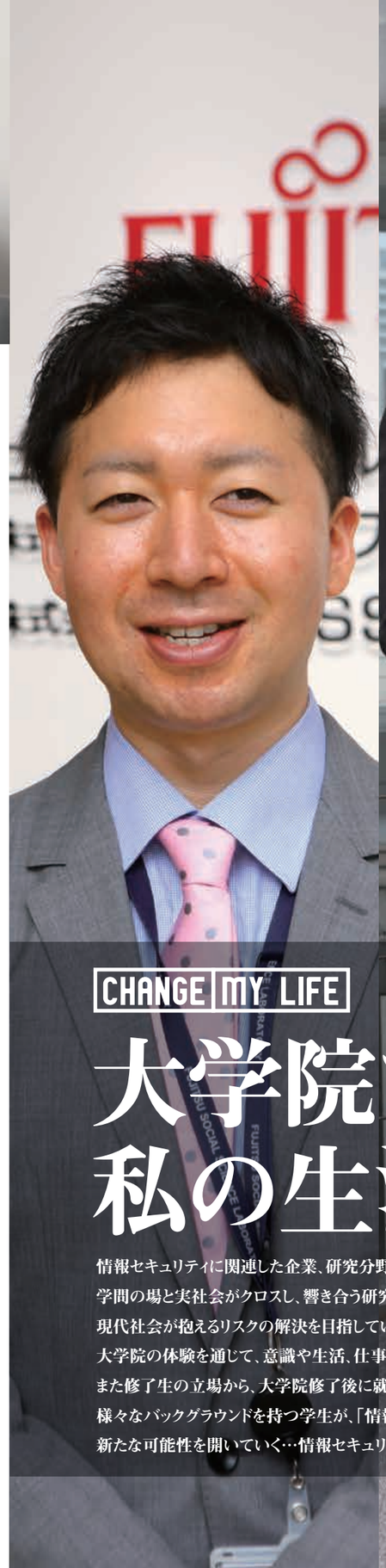
16時20分からは1階ラウンジでの「ティータイム」になるべく参加。コーヒーやお茶が無料になりますし（笑）、先生も学生も研究室に関係なく集まって、気軽に話ができる時間が楽しみなんです。

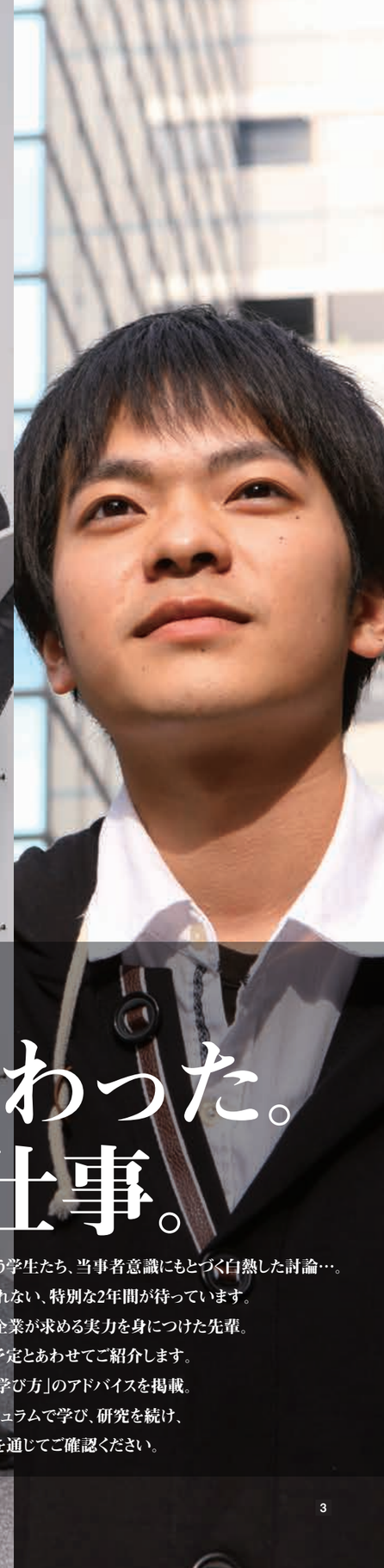
この大学院は社会人学生が多く、しかも省庁、セキュリティ企業、マスコミ関係など多様なバックグラウンドの先輩・同級生がいるため、今の社会の動きやセキュリティに対する考え方などが直接聞けて、研究の参考になっています。

日曜日は今のところオフ日。自宅で読書やゲームなどで気分転換しています。

◉機械学習でダークWebから情報収集する方法を研究予定

研究テーマは、研究室の先輩から引き継いだ「ダークWebを対象に、機械学習で自然言語を処理するシステムによって情報を抽出する」こと。ダークWebにありがちな偽情報をどう見分けるかなど課題は多いのですが、過去の文献を読んで類似例を探っています。





CHANGE MY LIFE

大学院でこう変わった。私の生活、私の仕事。

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

CHANGE MY LIFE 大学院でこう変わった［新入生編］

坂田 伸也さん

企業グループ全体のセキュリティ体制に必要な幅広い知識と専門性を養うため入学。

情報セキュリティ研究科　博士前期課程1年

昭和シェルビジネス&ITソリューションズ株式会社　www.sbis.co.jp
セキュリティ担当部署への異動で、業務上の必要性を感じて入学し、
企業グループ全体のセキュリティという業務直結の研究テーマを検討中。

◉科目等履修生ではもったいない その思いから博士前期課程に入学

大学を卒業して昭和シェルグループや関連会社の情報システムを支える企業に入社し、ITプロジェクトの上流工程やプロジェクト管理を約20年担当した後、数年前にグループ全体のセキュリティやIT統制を担う部署に異動。それまで「開発時のルール」程度に捉えていたセキュリティに関して、専門家になる必要が出てきました。

そこで上司の勧めもあり、情報セキュリティ教育で定評のあるIISECの科目等履修生となり、業務と関連の深い2科目を受講。そこで様々な企業や機関のセキュリティ担当の方々が昼夜学ばれている姿を目の当たりにし、多様なセキュリティ人材がいる大学院での経験は、自分にも自社にもメリットになると考えて博士前期課程に入学しました。

◉セキュリティ分野の知識を背景に 経営層に強くアピールしたい

仕事では自社や関連会社の経営層との接点も多く、履修科目は経営の視点を踏まえたセキュリティ／リスクマネジメントコースを参考に選択。ただ、技術や最新トレンドの裏付けも必要と考え、2年間で情報セキュリティを体系立てて学び、現状の課題も整理したいと思っています。文理を超えて学べるIISECで幅広い知識が習得できる期待に満ちていますが、もし入学せず自社での業務経験と独学だけで過ごしていたら……と仮定するとゾッとしますね。

◉企業グループ内のセキュリティなど 業務直結型の研究テーマを選択

セキュリティ対策やIT統制といっても、当グループは関連会社も含めたサプライチェーン全体が対象のため、企業風土や地域・規模の違いなどを踏まえつつ、共通で順守するガイドラインと企業別にカスタマイズする部分が共存できる体制の整備が必要です。しかも石油精製のプラントは国の重要インフラでもあり、それらを動かすシステムのセキュリティをどう強固に保つかも重要です。

私は研究テーマにこれらの点を盛り込む予定で、指導教授の原田先生と相談しながら企業グループ全体のセキュリティを考えたいと思っています。

私の1週間

◉どうしても外せない講義以外は フルタイムの業務後に受講

私は入学の前年に、科目等履修生として「リスクマネジメント」「セキュリティ経営とガバナンス」を履修していた関係で、前期は火・水・土曜日のみが通学日です。火曜日は外せない講義のため早退しますが、講義の空き時間は研究室にいて、過去の論文や資料を読む時間に充てるなど有効活用しています。

水曜日はフルタイムの業務を終えて大学院に。5限開始の18時20分に間に合うよう、通学日と仕事の締切が重なる場合は前倒しで進めるなど、当日の業務をなるべく減らすよう調整しています。

時限	月	火	水	木	金	土	日
1	業務	業務	業務	リスクマネジメント ※前年履修済み	業務	個人識別とプライバシー保護	日曜日は家事や家族との時間を優先するものの、趣味のソフトボールを楽しむときも。場合により大学院の講義の復習やレポート作成にも着手
2						セキュリティシステム監査	
3				業務		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					
5		研究指導	情報セキュリティ輪講I	セキュリティ経営とガバナンス ※前年履修済み			
6	帰宅	研究指導	インターネットテクノロジ	帰宅	帰宅	帰宅	
α		空き時間は研究室で論文を読むほか、業務メールのチェックも行う					

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


1


2


3


4

1>研究室にいられる曜日は限定的ですが、同室の先輩や同級生の話は刺激的。 2>空き時間を利用して業務メールもチェック。 3>研究室のほか図書館にも過去の研究論文がそろっているので参考に。 4>毎週火曜日の原田研究室ゼミ。このほか月1回、土曜日に研究室の客員研究員なども加わった討論も行われます。

CHANGE MY LIFE 大学院でこう変わった［修了生編］

中山 幸郎さん

自分の専門分野を仕事で活用するため情報セキュリティの知識が必要だった。

情報セキュリティ研究科　博士前期課程　2016年3月修了

株式会社富士通ソーシアルサイエンスラボラトリ（富士通SSL）
サイバーセキュリティ事業本部　第一システム部
理学部物理学科卒業後、数学を仕事に生かすプラスαの習得を
目指して入学。数学と情報の接点となる暗号分野を専門にする。

◉暗号文のままで演算可能な 完全準同型暗号を研究テーマに

大学進学の際に物理学科を選んだのは、純粋に数学や物理学が好きだったから。就職はあまり意識していませんでした。しかし就活時期になると、自分の専門を生かして働くにはプラスαが必要と痛感して大学院進学を検討。数学と親和性の高い情報系の中でも、将来性に期待できるセキュリティ分野を学ぼうと思い、IISECに入学しました。

入学時は暗号の知識をもとに仮想通貨を作りたいと考え、暗号理論とその実装を専門とする有田先生の研究室に配属。そこで完全準同型暗号に興味を持ち、自分の研究テーマに選んだのです。

◉情報セキュリティ分野を 体系的に学べるカリキュラム

完全準同型暗号を使えば暗号文のまま計算できるため、プライバシーを保護した状態でデータ処理を行うのに適しています。しかし鍵サイズ、暗号文サイズ、計算量などが膨大になるという問題点があるため、私は無駄を抑えたパラメータ設定でそれらを解決するアイデアを検討し、修士論文にまとめました。

こうした最先端の研究ができる一方、広範な情報セキュリティ分野を体系的に学べるのもIISECの魅力。加えて演習・実習など体験的学習の機会も多く、例えば仮想ネットワーク内でPCを攻撃する実習などにも参加しました。

◉顧客のセキュリティ対策のほか セキュリティ専門の勉強会でも活動

大学院での就活は情報セキュリティを学んだことが強みとなり、現在の会社に内定。入社時から顧客企業のセキュリティ対策を扱う部署に配属され、経験豊かなメンバーと協力して企業のセキュリティ診断サービスなどを担当。また暗号に詳しいことからセキュリティ担当者の勉強会で講師を依頼されるなど、社外での活動も活発に行っています。


1


2


3

1>チームで業務を進めているため、進捗の把握などメンバーとのミーティングは毎日必須。 2>顧客へのヒアリングのため外出。富士通SSLは日本全国の企業と取引があるため泊まりがけの出張も。 3>勉強会などで使う発表用資料は、ビルの別フロアにある富士通グループの社内サテライトオフィス「F3rd（エフサード）」も利用。集中して取り組めるので便利。

■中山さんのある一日

9:00 出社後、真っ先にセキュリティ関連のニュースを確認。企業の担当者も読む一般サイトから専門家のブログまで目を通した後、メールチェックへ。

9:30 所属する診断チームの朝会。チーム内の誰が、どんな案件を進めているかなど最新情報を共有する。

10:00 一緒に仕事を進めるチームのメンバーとミーティング。進捗状況、各自の予定、今日の業務の確認など。効率的に進むように1日の仕事の流れを打ち合わせ。

10:30 昨日依頼された案件のため、診断対象の企業のホームページや顧客から入手した資料を見てみる。

11:00 本日午後、顧客のもとで行うセキュリティ診断の最終チェック。社内ネットワークの脆弱性確認が目的のため、診断専用のパソコンで診断ツールの設定やスクリプトの仕込みを確認する。先方でリターンキーを押せばすべての診断が終わる、のが理想。

12:00 外出。自社のある武蔵小杉駅周辺は昼食時間も非常に混み合うので、客先に向かう間に食事を済ませることに。途中で別の顧客からの電話に対応。

14:00 先方の担当者と診断内容を最終確認した後、診断の実施。問題なく終了したのでひと安心。

16:00 帰社。今日の診断結果を報告書にまとめる。途中で分かりやすい書き方などを上司にアドバイスを求める。17:00を回り、区切りのいいところで退社。

私の1日

◉顧客との打ち合わせをもとに セキュリティリスクを診断

私の主な業務は企業のセキュリティ診断で、顧客企業の社内外ネットワーク、使用アプリケーション、WEBの脆弱性の有無を調査し、それらの問題点と解決策を報告書として提出しています。

仕事では診断依頼があった先方を訪問して現状をヒアリングし、その結果をもとに診断ツールを準備。多くの場合は先方の社内または弊社からインターネット経由でツールおよびマニュアルで診断を行い、診断で取得した情報を分析した上で報告書を作成し、先方に説明するといった流れです。

常に新たな脆弱性と攻撃手法の情報を入手して診断方法を変更するなど、攻撃者の動きへの対応は必須。しかし報告書は難しくせず、原因は完結に、対処は具体的に書いて、顧客が「何をすればいいのか」が明確になるよう配慮しています。このように同期入社の中で私が一歩先んじた働きができるのも、大学院で幅広く学んだおかげだと思います。

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）／暗号理論（2単位）／AIと機械学習（2単位）
個人識別とプライバシー保護（2単位）／統計的方法論（2単位）／統計的リスク管理（2単位）
情報セキュリティ技術演習Ⅰ（2単位）
研究指導（6単位）＜必修＞

合　計　30単位

［サイバーセキュリティとガバナンスコース］履修例

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

合　計　30単位

［システムデザインコース］履修例

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

合　計　30単位

［セキュリティ／リスクマネジメントコース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
情報セキュリティマネジメントシステム（2単位）／セキュリティシステム監査（2単位）
セキュリティ経営とガバナンス（2単位）／リスクマネジメント（2単位）／組織行動と情報セキュリティ（2単位）
統計的方法論（2単位）／Presentations for Professionals（2単位）／セキュア法制と情報倫理（2単位）
情報セキュリティ技術演習Ⅰ（2単位）／サイバーセキュリティ技術論（2単位）
研究指導（6単位）＜必修＞

合　計　30単位

◎必須科目　○履修標準科目

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

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

■ 修了要件および学位

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

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

■ 他大学院等との交流協定

2018年5月現在、以下の大学院・研究機関等と協定を締結しています。こうした大学間ネットワークを活用したさまざまな学習・研究機会等を利用することが可能です。

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

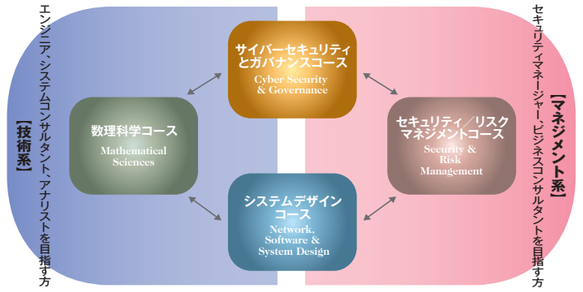
情報セキュリティ研究科
博士前期・博士後期

教育課程編成の考え方
カリキュラムの特色

広い視野に立って現実の情報セキュリティの問題解決を担う高度な専門技術者、実務家と、将来方向をリードする創造性豊かな研究者を育成。

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

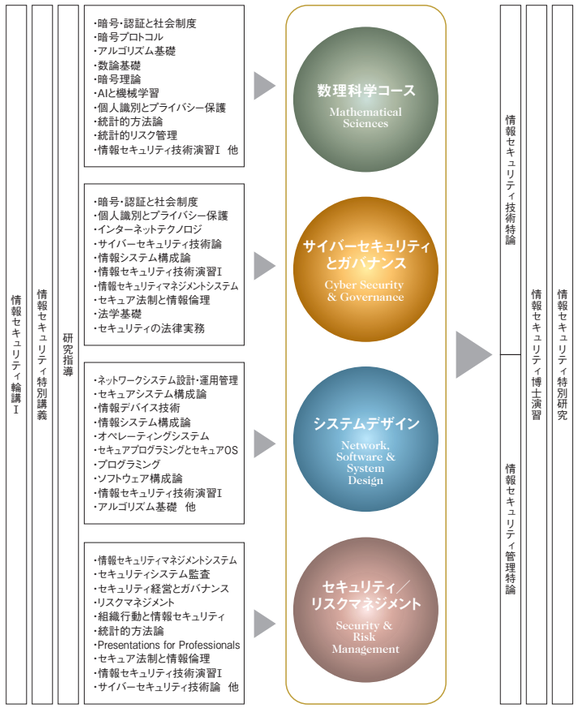
■ 博士前期課程4コース



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

■ カリキュラムフレーム

博士前期課程（修士課程）　博士後期課程



■ 開設科目一覧

本学ウェブサイトからシラバスをご覧いただけます（一部科目を除く）

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

博士前期課程
（修士課程）
授業科目概要
2018

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

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

TOPICS

JASA公認セキュリティ監査人（補）受験資格

選択科目「特設講義（セキュリティ監査）」
（後期2単位 担当：原田要之助 教授）を履修し、定められた講義・演習を受講することにより、NPO日本セキュリティ監査協会（JASA）が認定する公認情報セキュリティ監査人（補）の受験資格が得られます。また、履修終了後、JASAによる修了試験を受験して合格することで監査人補の資格が取得できます。平日日中の時間帯に開講している科目ですが、過去8年間で社会人学生を含む多数の方が本選択科目の履修とその後の受験を経て監査人補の資格を取得されました。

博士前期課程専攻科目（例）

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

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

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

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

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

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

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

■セキュアプログラミングとセキュアOS
現代の我々の社会は、ソフトウェアで制御されていると言っても過言ではない。しかし、世の中のソフトウェアシステムは多くの脆弱性を抱えたまま稼働しているのが実情である。そのため、多発するサイバー攻撃により、社会全体で様々な悪影響が生じている。そこで、本授業では、攻撃に強くセキュアなソフトウェアを構築・運用するために有用となるソフトウェアの設計・実装・運用に関する原則、概念、技法、ガイドライン、ツールなどについて紹介および解説を行う。

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

■情報セキュリティマネジメントシステム
本科目では、組織における情報セキュリティのリスクを管理するのに必要な管理体制（マネジメントの仕組み）が導入及び、リスクを低減するためのコントロール（管理策）が適切に維持・管理方法の習得すること目的としている。併せて、国際規格であるISO/IEC27001及び27002についての策定の背景、議論、国際的なコンセンサス形成などのプロセスについても概説する。

■セキュリティシステム監査
本授業では、セキュリティ管理が適切に機能しているかどうかを第三者の立場で評価・検証する場合の考え方と具体的な方法論を学習する。セキュリティ管理では、経営層の積極的な関与のもと、組織全体としての対応が求められることから、そのような視点を重視して授業を進める。必要に応じて、国家試験なども意識してシステム監査人となるのに必要な知識や技能も伝授するが、ケーススタディやディスカッションも織り交ぜながら、理論と実務という観点から、「監査」という行為、あるいは「監査人」の目線で、組織のセキュリティ管理をどう見るかという「センス」と、「問題解決能力」を養うことを主たる目的とする。

■リスクマネジメント
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、ケーススタディと個人研究を通し、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。

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

■セキュア法制と情報倫理
情報セキュリティを確保するためには各種の技術知識が不可欠であるが、同時にセキュリティを守るも破るも、人であることを忘れてはならない。人に関する研究は心理学・経営学・経済学・倫理学・法学など、様々な角度からアプローチが可能であるが、本講では最も実効性ある制度である「法」と、最も内面的な価値に近い「倫理」を組み合わせて、2名の担当者が相乗効果を出すよう協力して担当する。

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

TOPICS

2018年度新規開講科目

■AIと機械学習
本授業では、情報理論、確率論の基礎的な議論から始め、サポートベクターマシンにおけるカーネル法、畳み込みニューラルネットワーク等の機械学習の諸理論を学ぶ。また、古典論理、定理証明系、確率推論、探索等のAIシステムの基礎技術を学習し、情報セキュリティの問題解決に機械学習を応用する知識の習得を目指すこととする。

■実践的IoTセキュリティ
IoTの普及に伴い、今後数年間で、数百億個のモノがインターネットに接続され、情報収集や物理的制御に活用されるようになるとされる。本授業では、そこで生じる新たなセキュリティの脅威を正しく予測し、セキュアな機器を設計し、安全に運用するための技術や制度について、一部演習を交えながらオムニバス形式で講義を行う。

■情報セキュリティ心理学
本授業では、「人間の行動は個人と周囲から受ける影響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、情報セキュリティ事故およびサイバー犯罪に関する要因を多角的に捉え、様々な対策に目を向けるための知識や考え方を習得する。はじめに、犯罪に対する動機や加害者が狙う被害者の心の隙について解説する。続いて、犯罪抑制に必要な要素を紹介する。また、被害者が対策を躊躇する心理を示したうえで、対策を効果的に進めるための工夫などについて説明する。

博士前期課程
（修士課程）
授業科目履修例
2018年度

▼＜学部新卒学生Aさんの履修例＞ 数理科学コース

◆前期（4月9日～8月4日）　※■が履修科目

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

◆後期（10月1日～2月9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）	リスクの経済学			情報セキュリティ心理学	サイバーセキュリティ技術論（隔週）
4		特設講義（セキュリティ監査）	（研究指導）	特設講義（ハッキングとマルウェア解析）	暗号理論	
5	情報システム構成論	（研究指導）	情報セキュリティ特別講義	実践的IoTセキュリティ or 特設講義（サイバー・インテリジェンス）	Presentations for Professionals	
6	情報セキュリティマネジメントシステム	（研究指導）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B or セキュア法制と情報倫理	国際標準とガイドライン	

▼＜社会人学生Bさんの履修例＞ セキュリティ／リスクマネジメントコース

◆前期（4月9日～8月4日）　※■が履修科目

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

◆後期（10月1日～2月9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）	リスクの経済学			情報セキュリティ心理学	サイバーセキュリティ技術論（隔週）
4		特設講義（セキュリティ監査）	（研究指導）	特設講義（ハッキングとマルウェア解析）	暗号理論	
5	組織行動と情報セキュリティ	（研究指導）	情報セキュリティ特別講義	実践的IoTセキュリティ or 特設講義（サイバー・インテリジェンス）	Presentations for Professionals	
6	情報セキュリティマネジメントシステム	（研究指導）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B or セキュア法制と情報倫理	国際標準とガイドライン	

■ 授業時間帯

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

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

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

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、よりよい解決を見出すことで、より効率的でより強力な情報セキュリティを実現するための基盤構築を目指します。講義による知識習得にとどまらず、少人数のセミナーや個別指導を通じて学習・研究を進めます。修了後は、企業・研究機関・行政機関等において、専門技術職・研究職を始めとするテクニカルスタッフとしての活躍が期待されます。

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

有田 正剛 教授
Seiko ARITA

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

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

“セキュリティ・バイ・デザイン”でネットワーク社会の安全を守る

◆コース概要と研究キーワード

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

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

大久保 隆夫 教授
Takao OKUBO

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

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

先端技術とサイバー規範を併せ持つサイバーレスキュー隊のリーダーへ

◆コース概要と研究キーワード

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

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

湯淺 墾道 教授
Harumichi YUASA

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

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

適切なセキュリティ投資・対策・監査で、ITリスクの脅威から組織を守る

◆コース概要と研究キーワード

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

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

原田 要之助 教授
Yonosuke HARADA

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

博士前期課程
（修士課程）

目的別
カリキュラム
活用パターン

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

パターン1 修士学位取得専念型

修士論文に向けての知識の獲得と研究に重点を置きたい

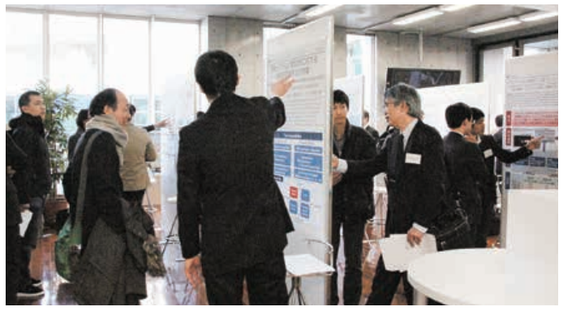
特にオプションプログラムは選択せず、各コースの履修標準科目を中心に履修して研究を進めるための知識の獲得や補強に努めるとともに、所属研究室での研究指導やディスカッションを通じて研究遂行能力を高め、在学中は修士論文作成に向けた研究に重点的に取り組みたい、という方を想定しています。神奈川県内の20以上の大学が加盟する大学院学術交流協定制度を利用して、研究テーマに関連する他大学院の開講科目を履修することも可能です。

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

パターン2 ISS square 併修型

研究室や大学を超えた活動を通じて幅広い視野を養い、研究を実務に生かしたい

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



パターン3 ISS square & enPiT SecCap 併修型

ISSスクエアの活動に加えできるだけ実践的な演習や実習に取り組みたい

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

実践演習をサポートしてくれる卒業生の声

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

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

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

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

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

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

文部科学省の平成19年度「先導的ITスペシャリスト育成推進プログラム」に採択されたISSスクエアは、情報セキュリティ大学院大学、中央大学、国立情報学研究所他、企業・研究機関11社の産学連携による高度情報セキュリティ人材育成プログラムです。暗号・認証、ネットワーク、システム、ソフトウェア、マネジメント、法制・倫理までトータルにカバーされた講義群、インターンシップや見学会、企業現場の実務家によるオムニバス講義などにより、経営・研究開発現場における現状の理解と問題の把握が促進されるとともに、サブゼミ的な位置づけの研究分科会や分野横断型のワークショップでの活動を通して、高度な問題発見能力と解決能力を身につけます。ISSスクエア活動の集大成としての年度末のシンポジウムでは、連携企業の皆様による成果発表審査も行われ、ISSスクエアプログラム修了者には、情報セキュリティ・スペシャリスト・サーティフィケートが授与されます。2008年の開始以来、本学からは170名以上の方がサーティフィケートを取得され、毎年、社会人学生を含む多くの方が本プログラムに参加されています。

詳しくは http://iss.iisec.ac.jp/

成長分野を支える情報技術人材の育成拠点の形成 enPiT SecCap

文部科学省の平成24年度「情報技術人材育成のための実践教育ネットワーク事業」に採択されたenPiTは、クラウドコンピューティング、セキュリティ、組み込みシステム、ビジネスアプリケーションの4分野を対象とし、それぞれの分野に専門領域を有する全国の15大学院の教員や企業の技術者を結集したプログラムです。2017年4月からは大学院生向け成長分野を支える情報技術人材の育成拠点の形成（enPiT 1）として自主展開を図っており、セキュリティ分野（enPiT-Security）は、5つの連携大学（情報セキュリティ大学院大学、東北大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学）が協力して開講する実践セキュリティ人材の育成コース（SecCap）により、幅広い産業分野において求められている「セキュリティ実践力のあるIT人材」の育成を目指します。暗号、システム、ネットワーク、監査、マネジメントまでの幅広い演習プログラムと、最新の実習環境、そして実社会が取り組むインシデント分析やセキュリティ実装の演習も行い、情報セキュリティへの脅威や攻撃への対処技術を実践的に体験習得します。

詳しくは http://www.seccap.jp/

情報セキュリティ研究科
博士前期・博士後期

在学生プロフィール
2017-2018



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。

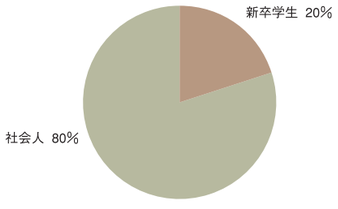
【所属組織一覧】(2017-2018実績)
ウィングアーク1st(株)／NECフィールディング(株)／NTTコミュニケーションズ(株)／NTTテクノクロス(株)／エヌ・ティ・ティ・コムウェア(株)／沖電気工業(株)／海上自衛隊／海上保安庁／外務省／(株)アイネス／(株)エヌ・ティ・ティ・エムイー／(株)サーバーワークス／(株)静岡銀行／(株)JR 東日本情報システム／(株)タツノ／(株)東陽テクニカ／(株)日立システムズ／(株)日立製作所／(株)Beyondsoft Japan／(株)本田技術研究所／(株)読売新聞社／金融庁／警察庁／警視庁／(公社)日本医師会／埼玉県警察／CsSoft(株)／ジェイアール東海情報システム(株)／昭和シェルビジネス&ITソリューションズ(株)／(独)国立印刷局／(独)日本学術振興会／東日本旅客鉄道(株)／法務省／防衛省／モルガンスタンレーグループ／横浜市役所 など

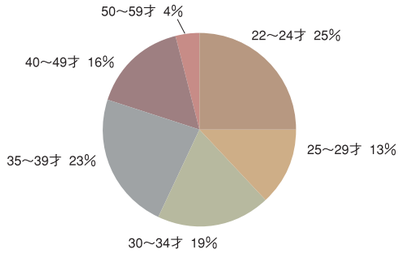
■ 現況

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

■ 年齢構成(入学時)

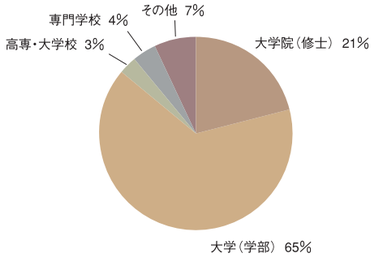
20代半ばから30代の中堅社会人をはじめ、幅広い年代の方々が学んでいます。ジェネレーションを超え、同じ学生という立場で活発な交流が図られています。





■ 最終学歴

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



博士後期課程

博士後期課程には、既に相当の研究実績、業務実績を有する研究者、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。

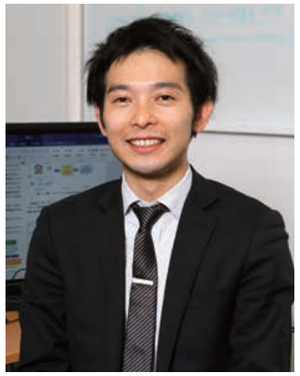
【所属組織一覧】(2017-2018実績)
EYアドバイザリー&コンサルティング(株)／NTTセキュリティジャパン(株)／(学)昭和女子大学／(株)アーク情報システム／(株)三井住友銀行／合同会社ゼロワン研究所／日本放送協会／東日本電信電話(株)／富士ソフト(株)／三菱電機インフォメーションシステムズ(株) など

博士前期課程
(修士課程)

在学生
インタビュー

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

リソース不足や仕様の混在など課題が山積みのIoT。
それらに有効なセキュリティ対策を検討しています。


丹羽雅哉さん
Masaya NIWA
NTTテクノクロス株式会社
博士前期課程2年

サービス全体を見通せる人材への成長を目指して入学

入社以来、セキュリティ関連の部署でシステム基盤の開発と導入、維持管理などを担ってきましたが、近年はウエアラブルデバイスをはじめ IoT導入の検討機会も増えています。しかし現状では自社サービスの構築からコンサルとして行う他社のサービス構築まで、サービス全体を貫くセキュリティ設計への対応は不十分で、IoTも含む全レイヤを通じたセキュリティ検討が進んでいません。私はセキュリティの観点でサービス全体を見通すことのできる人材を目指し、IISECで情報セキュリティ全般を学んだ上で、機器認証など特定分野を突き詰めたいと考えました。

IoTとシステム間の機器認証のセキュリティを研究

IoTのセキュリティはデバイスのリソース不足で十分なセキュリティ対策が難しいことや、通信プロトコルや出力ログなどが異なる多様なデバイスが混在するなど、システムとしての管理を困難にする課題が山積みです。私は「セキュリティバイデザイン」がテーマの大久保研究室で、そうした課題に対する有効なセキュリティ対策を検討中です。修士論文は IoTとシステム間の機器認証について検討する予定で、修了後も実践を重ね、IoTセキュリティの有識者と呼ばれるよう努力したいと考えています。

最先端の知識や人脈で自己成長のチャンス

IISECの魅力は、様々な分野の第一線で活躍する方々が専任講師や外部講師となり、業界セミナーでも聞けない最先端の知識や新たなビジネスの着眼点などを学べることです。在学生の皆さんも多様なバックグラウンドや得意分野を持たれており、演習でのディスカッションや普段のコミュニケーションも刺激的で勉強になります。さらに卒業生とも深いつながりができ、自分を成長させるチャンスに満ちています。ここで身につけた知識・技術、人脈はソフトウェア開発、サービスやソリューションの考案や提案などすべての業務に活かせると思います。

侵入されることを前提に、侵入コストを高めて
攻撃を中断させる「欺瞞による防御」を研究。


杉生雅樹さん
Masaki SUGIU
株式会社日立システムズ
博士前期課程2年

欠けている知識がないよう情報セキュリティ全般を学ぶ

IISECに入学したのは入社2年目のとき。インターネットゲートウェイのセキュリティ対策の商材を提供する仕事をする中、企業の特色や使用している製品、業務で身につけた知識には偏りができると感じ、広範な情報セキュリティ分野全般の基礎知識を身につけたいと思ったのがきっかけでした。1年生の講義は、暗号など業務との関連が薄い科目を除いて幅広く履修したおかげで、抜けていた分野がカバーでき、顧客や社の先輩たちとの話も十分対応できるようになりました。ただ攻撃も進化しますから一度学んで終わりではなく、今後も自主的に勉強を続けるつもりです。

欺瞞によって侵入コストを上げ、あきらめさせる

能動的に学ぶ演習・実習も特徴的で、例えば土曜日の3・4・5限の「情報セキュリティ技術演習 I」は脆弱性検査や不正侵入を講義で学び、実習で理解を深める方式。こうした内容をきちんと教わる機会はないので非常に参考になりました。修士論文のテーマは「欺瞞を使った防御機構」で、攻撃者によるネットワークへの侵入を完全には防げないという前提に立つもの。侵入後に次々と欺瞞情報を提供することで正しい情報にたどり着く手間を増やし、攻撃をあきらめさせるやり方はすでに海外で注目されています。修士論文をきっかけに自分の理解を深め、いずれ本格的に普及したときにはこの分野の第一人者になっていたいですね。

在学中に生まれる人脈の深さ・広さは IISEC独自

入学前、先輩方から頻繁に「人脈が魅力」と聞きましたが、入学して本当に実感しました。官公庁やセキュリティ企業など様々な背景の在学生とセキュリティを軸に話ができ、その分野では第一人者といえる方が同じゼミ生として私の発表を真剣に受け止め、議論のキャッチボールをしてくれるのです。知識はどこも同じかもしれませんが、深く広い人脈はIISEC独自のもの。通信制では得られない豊かな時間が過ごせます。

博士後期課程
在学生&修了生インタビュー

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

消費者が自分の情報の流通を検知し、法律の実効性を高めて、安心できる仕組みを論文で提言。

Keiko KANEKO　金子啓子さん
情報セキュリティ研究科 博士後期課程修了
（大阪経済大学 准教授）

情報セキュリティに関する知識を補完した上で、博士号の取得が目標

大手電機メーカーで情報セキュリティ本部長、個人情報保護担当理事を務め、個人情報漏えい事故が起きた企業グループのCLO（最高法務責任者）となり、セキュリティ向上に取り組んできました。ただ、大学とアメリカのロースクールで法律は学んだものの、情報セキュリティの知識は実務の中で習得したため、足りない部分も多いと感じていました。大学院で教授の指導を受けて学び直し、論文で自分の考えをまとめたいと考えたのです。また私自身も大学教員になって情報セキュリティの研究を進めることも視野に、博士号取得にチャレンジしました。

個人情報の扱いでアンバランスな面を是正して、消費者主体の情報管理へ

私は博士論文で、日本の個人情報保護規範が情報を流出させた企業・団体への処罰や批判が重く、不適正に流通する名簿を販売・利用する業者の処分は不十分といったアンバランスさを指摘。そのため消費者は情報の不適正利用への不安を和らげる手段がなく、それが個人情報を扱う側への圧力となる現状を、海外との比較で考察しました。2015年の個人情報保護法の改正で業者への処分が強化された一方、個人情報の流通を検知する仕組みは未整備なため、海外の電話勧誘拒否制度（Do Not Call）の導入も検討しました。
現在の日本はレピュテーションリスクを恐れた企業が、個人情報の扱いに過剰に萎縮している面もあり、個人情報保護の実効性を高める制度の導入でそれらを是正し、ビジネスに安心して取り組める環境整備を目指せたらと考えています。

品質管理手法を参考に日本の物づくりにおけるセキュリティ品質管理の世界標準規格を作り上げたい。

Kousuke ITO　伊藤公祐さん
情報セキュリティ研究科 博士後期課程1年
（一般社団法人 重要生活機器連携セキュリティ協議会（CCDS））

メーカーが開発する組み込み機器のセキュリティ調査にも取り組む

私は、メーカーで研究開発と新規事業に携わり、ネットワーク関連企業への転職後は事業企画のほか、研究部門で組み込み機器のセキュリティ調査などを担当。重要生活機器連携セキュリティ協議会（CCDS）の事務局を務める中、メーカーが製造工程でどの程度セキュリティ対応したかを外部に示せるかに関心を持つようになりました。
メーカーは製品工程でのセキュリティ対応といわれても、必要性は認識しているものの実行に移せていないのが現状。そこで私がこれまで得てきた知識・経験を体系的に整理し、メーカーの製品へのセキュリティ対応状況の管理に参考となる規格が作れないかと考えIISECに入学。情報セキュリティ関連規格の多くが欧米発であるのに対し、セキュリティを品質管理に組み入れる試みは、世界中で品質重視と評価される日本メーカーに強みのある分野でしょう。日本が注力してきた品質管理の中で使える部分は生かし、情報セキュリティの視点で要素を加えるハイブリッドな仕様を考えています。

関連会社や取引先も含めた製造工程全体のセキュリティを管理

博士後期課程の3年間で、私は「メーカーがセキュアな製品であることを顧客や利用者に示すための品質表示規格」を策定し、メーカーでの自己評価やチェック項目といった製造工程で使えるツールづくりも検討の予定。製品の製造では関連会社や取引先が作った部品の利用も多く、各社の部品のセキュリティ品質が製品にも重要になります。こうした規格の策定により、万が一、インシデントがあっても、セキュアな製品づくりをしてきたメーカーの責任範囲が限定されてリスクヘッジができ、新たな物づくりを促す機会になると期待しています。

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2017年度までの間に本学博士後期課程を修了し、博士の学位を授与された方のおよそ3分の1は標準修業年限未満（1年から2年半）で博士学位を取得されています。

2. 所要単位数：
特別研究6単位以上＋博士演習2単位以上→合計8単位以上

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

■ 後期課程科目概要

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

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

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

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

■ 修了後の進路

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

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

学長
Message

後藤厚宏

学長●情報セキュリティ研究科長　Atsuhiro GOTO

■プロフィール
1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術、高信頼クラウドコンピューティング技術、ID管理技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。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。

■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. 田中恭之, 後藤厚宏. 統計的方法を用いた未知マルウェア検出手法の提案と評価. 情報処理学会 論文誌 vol 57, No9, 2016
4. 森　滋男, 後藤厚宏. サイバーセキュリティと情報漏えい対策. 行政&情報システム vol51, Dec 2015
5. 後藤厚宏. ビッグデータ活用におけるガバナンス. 情報処理 vol 56, No.10, 2015

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

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

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

文理融合の教育・研究から多様な情報セキュリティ分野で活躍できる人材を育てる

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

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

将来の目標に応じたコースフレームをもとにそれぞれの専門性を高める

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

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

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

多様なバックボーンの仲間が大学院で同じ時間を共有し育まれる人脈は貴重

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

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

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

専任

大塚　玲
教授
Akira OTSUKA

■プロフィール
大阪大学工学研究科博士前期課程修了。東京大学大学院工学系研究科電子情報工学専攻修了。博士（工学）。野村総合研究所,東京大学生産技術研究所,産業技術総合研究所などを経て2017年4月より本学教授。2006年-2010年産業技術総合研究所情報セキュリティ研究センター・セキュリティ基盤技術研究チーム長。2007年-2014年中央大学研究開発機構教授。東京理科大学大学院工学研究科非常勤講師（2009年から3年間）、城西大学理学部数学科非常勤講師（2015年-）、北陸先端科学技術大学院大学情報科学研究科非常勤講師（2016年）。

■主な研究業績
1. Tetsushi Ohki and Akira Otsuka, "Theoretical Vulnerability in MAP Speaker Adaptation" Proceedings of 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP2017), (2017).
2. Tetsushi Ohki and Akira Otsuka, "Theoretical vulnerability in likelihood- ratio-based biometric verification," 2014 IEEE International Joint Conference on Biometrics (IJCB), pp.1-8, (2014).
3. Akira Otsuka, Hideki Imai , "Unconditionally Secure Electronic Voting", Towards Trustworthy Elections; New Directions in Electronic Voting, David Chaum and Markus Jakobsson and Ronald L. Rivest and Peter Y. A. Ryan and Josh Benaloh and Miroslaw Kutylowski and Ben Adida Eds., Lecture Notes in Computer Science Vol. 6000, Springer, ISBN 978-3-642-12979-7, pp. 107-123, (2010).
4. Manabu Inuma, Akira Otsuka, and Hideki Imai, "Theoretical framework for constructing matching algorithms in biometric authentication systems," Proceedings of the Third IAPR/IEEE International Conference on Biometrics (ICB 2009), LNCS 5558, 293-300, (2009).
5. Akira Otsuka, Goichiro Hanaoka, Junji Shikata, Hideki Imai, "An unconditionally secure electronic cash with computational Untraceability," IEICE Trans. Fundamentals, Vol. 85-A, No. 1,(2002).

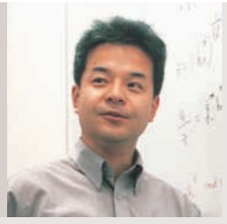
■主な研究テーマ
情報セキュリティ理論（Blockchain, 敵対的機械学習の安全性など）

■主な担当科目
AIと機械学習、暗号・認証と社会制度、アルゴリズム基礎、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。情報処理学会コンピュータセキュリティ研究運営委員会専門委員、横浜市個人情報保護審議会委員。

■主な研究業績
1. 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).
2. A Fully Secure Spatial Encryption Scheme, D. Moriyama, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.28-35 (2011).
3. Secure and Efficient IBE-PKE Proxy Re-Encryption, T. Mizuno, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.36-44 (2011).
4. 利用履歴を秘匿できるコンテンツ配信・課金方式に関する研究, 飛田孝幸, 山本博紀, 土井洋, 真島恵吾, 情報処理学会論文誌, 第50巻,第9号, pp.2228-2242 (2009).

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

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

■担当コース
数理科学コース、システムデザインコース

専任

林　紘一郎
教授
Koichiro HAYASHI

■プロフィール
東京大学法学部卒業。日本電信電話公社（当時）入社後、NTTアメリカ社長（本社役員待遇）、Nextel（現Sprint-Nextel）社取締役などを歴任。慶應義塾大学メディア・コミュニケーション研究所教授を経て、2004年4月以降、情報セキュリティ大学院大学教授(この間、2009年4月より2012年3月まで同学長・教授)。2012年4月より博士後期課程学生を主に担当。2014年以降は、内閣サイバーセキュリティ戦略本部員を兼務。経済学博士（京都大学）。博士（法学、慶應義塾大学）。

■主な研究業績
1. 『インフォミュニケーションの時代』中央公論社、1984年
2. 『ネットワーキングの経済学』NTT出版、1989年
3. 『ユニバーサル・サービス』（田川義博氏と共著）、中央公論社、1994年
4. 『著作権の法と経済学』（編著）勁草書房、2004年
5. 『情報メディア法』東京大学出版会、2005年
6. 『進化するネットワーキング』（湯川抗・田川義博両氏と共著）NTT出版、2006年
7. 『倫理と法ー情報社会のリテラシー』（矢野直明氏と共著）産業図書、2008年
8. 『引用する極意・引用される極意』（名和小太郎氏と共著）勁草書房、2009年
9. 『セキュリティ経営』（田川義博・淺井達雄両氏と共著）勁草書房、2011年
10. 『情報法のリーガル・マインド』勁草書房、2017年

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

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

専任

原田　要之助
教授
Yonosuke HARADA

■プロフィール
1979年京都大学大学院工学部数理工学専攻修了。電信電話公社（現NTT）研究所で通信ネットワークの監視、制御システム、セキュリティアーキテクチャの研究等に従事。1999年より情報通信総合研究所にてコンサルやセキュリティ監査に従事。OPCWの情報セキュリティ監査にも従事し、2000年から2008年まで監査チームリーダを務める。2010年4月情報セキュリティ大学院大学教授に就任。日本セキュリティマネジメント学会会長、情報処理学会電子化知的財産社会基盤研究会主査、システム監査学会理事。元ISACA国際本部副会長。日本セキュリティ監査協会資格認定委員長。日本ITガバナンス協会理事、iMISCA理事。ISO/IEC SC40/WG1の国内委員会主査及びISO/IEC38503のEditor、ISO/IEC SC27/WG1の国内委員及びISO/IEC27014（情報セキュリティガバナンス）のCo-editor。中央大学大学院非常勤講師、サイバー大学非常勤講師、フェリス女学院大学非常勤講師。2013年ISC2より、Senior Information Security Professional Categoryで表彰。

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

■主な研究テーマ
情報セキュリティマネジメントとガバナンス、情報セキュリティ監査とシステム監査、IoTのセキュリティマネジメント

■主な担当科目
情報セキュリティマネジメントシステム、セキュリティ経営とガバナンス、
特設講義（セキュリティ監査）、研究指導

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

産学連携を意識した教授陣。

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

学長・情報セキュリティ研究科長

後藤　厚宏
教授
Atsuhiro GOTO

■プロフィール
1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術、高信頼クラウドコンピューティグ技術、ID管理技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。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。

■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. 田中恭之, 後藤厚宏.統計的方法 を用いた未知マルウェア検出手法の提案と評価.情報処理学会 論文誌 vol 57, No9, 2016
4. 森　滋男、後藤厚宏. サイバーセキュリティと情報漏えい対策. 行政&情報システム vol51, Dec 2015
5. 後藤厚宏.ビッグデータ活用におけるガバナンス.情報処理 vol 56, No.10,2015

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

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

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

専任

有田　正剛
教授
Seiko ARITA

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

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

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

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

■担当コース
数理科学コース、サイバーセキュリティとガバナンスコース

専任

大久保　隆夫
教授
Takao OKUBO

■プロフィール
1991年東京工業大学物理情報工学専攻修了。同年株式会社富士通研究所に入社。リバースエンジニアリング、分散開発環境、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。Aviation Security研究会幹事、脅威分析研究会幹事、ドローンセキュリティ研究会主査、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。

■主な研究業績
1. 大久保 隆夫, 田中 英彦: 効率的なセキュリティ要求分析手法の提案, 情報処理学会論文誌 Vol. 50,No.10 pp.2484-2499 (2009)
2. Takao Okubo, Kenji Taguchi, Haruhiko Kaiya and Nobukazu Yoshioka:MASG: Advanced Misuse Case Analysis Model with Assets and Security Goals, IPSJ Journal of Information Processing Vol.22(2014) No.3, pp.536-546 (2014)
3. Takao Okubo, Haruhiko Kaiya and Nobukazu Yoshioka:Analyzing Impacts on Software Enhancement Caused by Security Design Alternatives with Patterns, International Journal of Secure Software Engineering, Vol.3. No.1. pp.37-61 (2012)
4. 吉岡 信和, 大久保 隆夫, 宗藤 誠治: セキュリティソフトウェア工学の研究動向, コンピュータソフトウェア Vol.28,No.3 pp.43-60 (2011)
5. 大久保 隆夫: 企業におけるセキュリティ分析技術の実効性, <特集>セキュリティ要求工学の実効性, 情報処理　No.50, vol.3, pp. 230-234 (2009)
6. 大久保 隆夫: セーフティとセキュリティ, <小特集>乗り物のセキュリティと安全性,情報処理 No.57, vol.7,pp.630-631 (2016)

■主な研究テーマ
セキュリティ・バイ・デザイン、脅威分析、ソフトウェア/システムセキュリティ、マルウェア解析/ネットワークセキュリティ制御システムセキュリティ、IoTセキュリティ、セキュリティとセーフティ、形式検証手法のセキュリティ応用、攻撃手法に関する研究

■主な担当科目
ソフトウェア構成論、アルゴリズム基礎、情報デバイス技術、情報セキュリティ技術演習Ⅰ、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、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。一般社団法人モバイルコンテンツ審査・運用監視機構事務局長副代表理事。
最高裁司法研修所刑事弁護教官(2012−2015)
■担当科目
セキュリティの法律実務

兼任
荻野　司
客員教授
Tsukasa OGINO

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

兼任
生越　由美
客員教授
Yumi OGOSE

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

兼任
小村　誠一
客員教授
Seiichi KOMURA

■プロフィール
NTTアドバンステクノロジ株式会社 主幹技師、セキュリティプリンシパル
早稲田大学理工学部数学科卒業、同大学大学院理工学研究科(数学専攻)修了。CSIRT業務、インシデント対応のための研修・訓練・教材作成やCSIRT評価モデルの検討・改善活動に従事。日本シーサート協議会 CSIRT評価モデル検討WG主査。
著書:CSIRT -構築から運用まで- (共著 2016年NTT出版)
■担当科目
特設実習(セキュリティ実践I、II)

兼任
佐藤　直
客員教授
Naoshi SATO

■プロフィール
情報セキュリティ大学院大学名誉教授
中央大学理工学部電気工学科卒業。博士(工学)。NTTサービスインテグレーション基盤研究所主幹研究員として、研究成果のビジネス化の促進、情報通信サービス品質の評価設計に従事。2004年4月から2017年3月まで本学専任教授。2017年4月より本学客員教授。
■担当科目
ネットワークシステム設計・運用管理
インターネットテクノロジ
情報セキュリティ技術演習I
特設講義(ハッキングとマルウェア解析)

兼任
柴山　悦哉
客員教授
Etsuya SHIBAYAMA

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

兼任
周佐　喜和
客員教授
Yoshikazu SHUSA

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

兼任
竜田　敏男
客員教授
Toshio TATSUTA

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

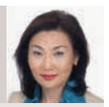
兼任
辻　秀典
客員教授
Hidenori TSUJI

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

兼任
廣松　毅
客員教授
Takeshi HIROMATSU

■プロフィール
東京大学名誉教授／情報セキュリティ大学院大学名誉教授
東京大学教養学部教養学科卒業、東京大学大学院経済学研究科修士課程修了。東京大学教養学部助手、同助教授を経て、1989年11月〜2009年3月東京大学教授(先端科学技術研究センター、大学院総合文化研究科・教養学部)。2009年4〜2017年3月本学専任教授。2017年4月より本学客員教授およびセキュアシステム研究所特別研究員。日本学術会議19期会員、20−21期・23期連携会員。2007年10月〜2015年9月内閣府統計委員会委員。
■担当科目
統計的リスク管理
リスクの経済学

兼任
藤本　正代
客員教授
Masayo FUJIMOTO



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

兼任
堀江　正之
客員教授
Masayuki HORIE

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

兼任
丸山　満彦
客員教授
Mitsuhiko Maruyama

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

兼任
森井　昌克
客員教授
Masakatu Morii

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

兼任
Ray Roman
客員教授

■プロフィール
東北大学会計大学院 ビジネス・コミュニケーション教授
Doctor of Laws, Harvard University; 1991
■担当科目
Presentations for Professionals

兼任
小林　雅一
客員准教授
Masakazu KOBAYASHI

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

兼任
藤村　明子
客員准教授
Akiko FUJIMURA

■プロフィール
日本電信電話株式会社 NTTセキュアプラットフォーム研究所 主任研究員
慶應義塾大学法学部法律学科、同大学大学院政策・メディア研究科修了後、日本電信電話株式会社に入社。同社在職中に中央大学大学院法務研究科修了。法務博士(専門職)。情報セキュリティ、個人情報保護、プライバシ保護の技術と法制度に関する研究開発に従事。国立研究開発法人 理化学研究所 革新知能統合研究センター(AIP)客員研究員、情報ネットワーク法学会元理事。
■担当科目
セキュリティの法律実務

兼任
塩月　誠人
客員講師
Makoto SHIOTSUKI

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

※上記は2018年4月現在

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。

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

■主な研究テーマ
IoTセキュリティ
制御システムセキュリティ
ロボットとAI

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

■担当コース
システムデザインコース

専任
湯淺　墾道
教授
Harumichi YUASA

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

■主な研究業績
1. 『電子化社会の政治と制度』(オブアワーズ、2006年3月)
2. "A Consideration of the 2007 Upper House election in Japan". Journal of Asian Women's Study. vol.16, pp97-102 (2008).
3. 「アメリカの電子投票におけるVVPATの現状と課題」『情報ネットワーク・ローレビュー』第6巻(2007年5月)187-203頁
4. 「個人情報保護法改正の課題 ―地方公共団体の個人情報保護の問題点を中心に―」『情報セキュリティ総合科学』第6巻(2014年)53-92頁
5. 「ディジタルゲリマンダの法規制の可能性」情報処理58巻12号(2017年12月)

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

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

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

専任
稲葉　緑
准教授
Midori INABA

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

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

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

■主な担当科目
統計的方法論、情報セキュリティ心理学、研究指導

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

専任
橋本　正樹
准教授
Masaki HASHIMOTO

■プロフィール
2001年、立命館大学文学部人文総合科学インスティテュート卒業。学部在籍時より新規法人の立ち上げに参画し、以降同社にて情報システムの運用管理・監視サービス業務に従事。2007年、情報セキュリティ大学院大学・情報セキュリティ研究科・博士前期課程修了。2010年、同博士後期課程修了。博士(情報学)。2010年より同助教、2014年より同准教授。2014年4月-2015年3月、ロンドン大学ロイヤルホロウェイ校情報セキュリティグループの訪問研究員として英国に滞在。専門はアクセス制御、OSセキュリティ、不正侵入検知・防御等。情報処理学会、電子情報通信学会、日本ソフトウェア科学会、IEEE各会員。電子情報通信学会／情報通信システムセキュリティ研究会(ICSS)専門委員、情報処理学会／コンピュータセキュリティ研究会(CSEC)専門委員、情報処理学会論文誌ジャーナル/JIP編集委員会委員、ECC2018 Local Organizing Committee Member、NETSAP2018 Workshop Organizer 等。

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

■主な研究テーマ
1. アクセス制御技術/OSセキュリティ
2. 不正侵入検知・防御/サイバー攻撃技術
3. OSINT/Intelligence Mining
4. ネットワークセキュリティ

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

■担当コース
システムデザインコース

INSTITUTE of INFORMATION SECURITY

■ 主な年間スケジュール（2017年度ご参考）

- 4/6 入学式・新入生歓迎会
- 4/7 前期開講
- 5/27 春季オープンキャンパス ホームカミングパーティ
- 7/29 前期授業期間終了
- 8/26 修士論文等発表会（9月修了）
- 10/2 後期開講
- 10/6 第14回アドバイザリーボード
- 11/11 秋季オープンキャンパス ホームカミングパーティ
- 2/10 後期終講
- 2/24 修士論文等発表会（3月修了）
- 3/24 学位記授与式

■ 入学式
2017.4.6

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

■ 修士論文等発表会
2018.2.24

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

2017年度も暗号理論からセキュリティ技術、マネジメント手法に至るまで多彩なテーマの修士論文が発表されました。

■ 学位記授与式
2018.3.24

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

■ 情報セキュリティ大学院大学連携教授（2018年4月現在）

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

株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹	秋山 浩一郎	国立研究開発法人産業技術総合研究所 理事 情報・人間工学領域 領域長	関口 智嗣
日本電信電話株式会社 セキュアプラットフォーム研究所 所長	大久保 一彦	株式会社KDDI総合研究所 取締役執行役員副所長 総務部門長・セキュリティ部門長	田中 俊昭
株式会社日立製作所 テクノロジーイノベーション統括本部 システムイノベーションセンタ セキュリティ研究部 部長	鍛 忠司	日本電気株式会社 セキュリティ研究所 所長	谷 幹也
パナソニック株式会社 イノベーション戦略室 戦略企画部 ソフトウェア戦略担当 理事	梶本 一夫	株式会社富士通研究所 セキュリティ研究所長 （兼）ブロックチェーン研究センター長	津田 宏
東京電機大学 研究推進社会連携センター特別専任教授（特命教授）（兼）サイバーセキュリティ研究所 所長	佐々木 良一	三菱電機株式会社 開発本部 役員技監 松井暗号プロジェクト統括	松井 充
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&サービス担当部長	佐藤 史子	横浜国立大学 大学院 環境情報研究院 教授	松本 勉
沖電気工業株式会社 経営基盤本部 政策調査部 上席主幹	杉尾 俊之	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 所長	宮崎 哲弥

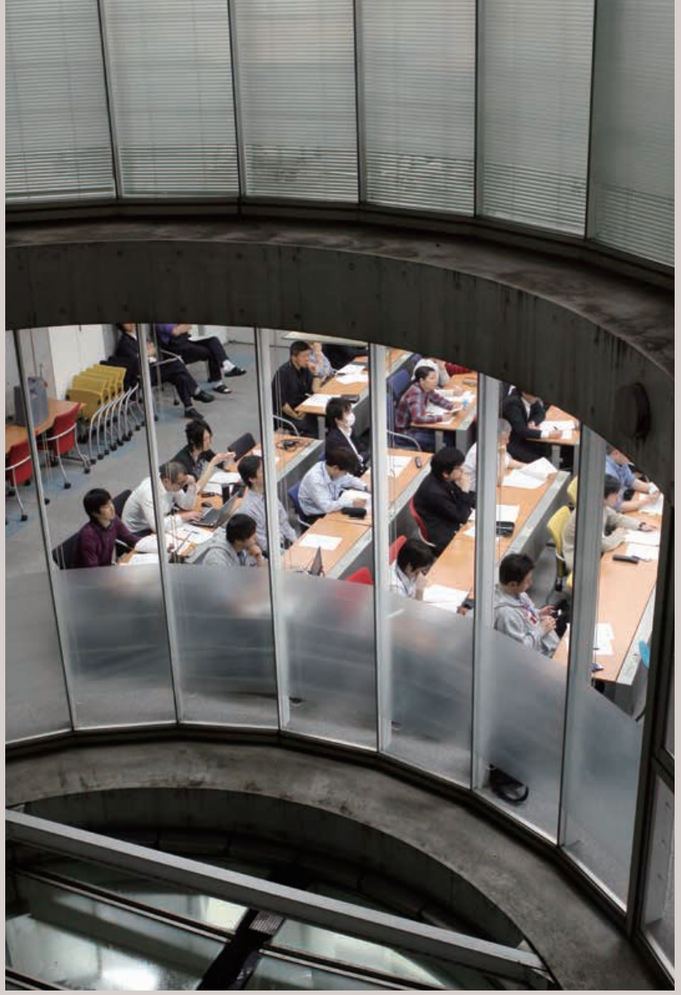
敬称略、氏名五十音順

■ 情報セキュリティ大学院大学アドバイザリーボードメンバー（2018年4月現在）

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

早稲田大学政治経済学術院 教授	縣 公一郎	日本経済新聞社 編集委員	関口 和一
株式会社OKIソフトウェア 代表取締役社長	猪﨑 哲也	朝日新聞社 IT専門記者・前編集委員	平 和博
株式会社日立ソリューションズ 監査室 室長	石川 明	日本放送協会 専務理事 技師長	児野 昭彦
NTTコミュニケーションズ株式会社 経営企画部長	稲葉 秀司	慶應義塾大学 大学院政策・メディア研究科 教授	土屋 大洋
株式会社エヌ・ティ・ティ・データ 取締役常務執行役員 技術革新統括本部長	木谷 強	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
芝浦工業大学大学院工学マネジメント研究科 客員教授	國井 秀子	神奈川県 副知事	中島 正信
早稲田大学理工学術院 教授	後藤 滋樹	横浜市 副市長	渡辺 巧教
東京電機大学 研究推進社会連携センター特別専任教授（特命教授）（兼）サイバーセキュリティ研究所 所長	佐々木 良一		
日本電信電話株式会社 代表取締役副社長 研究企画部門長	篠原 弘道		
日本電気株式会社 シニアオフィサー	庄司 信一		

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。

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

教育研究環境

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

■ 学費等納入金

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

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

［博士前期課程2年制プログラム4月入学の学費納入例］

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

■ 奨学金

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

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

種別	貸与月額（※2018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
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
デロイト トーマツ サイバーセキュリティ先端研究所
主任研究員

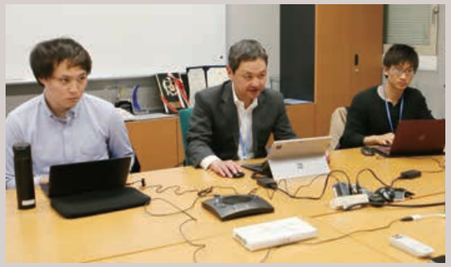
セキュア構築、侵入検知システムの導入設計、セキュリティ監視業務等を経てデジタルフォレンジック業務に携わる。サイバー攻撃被害の解析や訴訟事件等のデジタル鑑定解析、セキュリティ対策評価等を担当。
著作として「標的型攻撃セキュリティガイド」等がある。

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

名和 利男
サイバーディフェンス研究所
専務理事／上級分析官

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

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



ホームカミングパーティ

新入生歓迎パーティ

1Fホールでのweekday tea-time

ゼミ合宿

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

■Contents

Japan University Accreditation Association since 1947
UNIVERSITY ACCREDITED 2017.4~2024.3

■学生募集課程概要

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

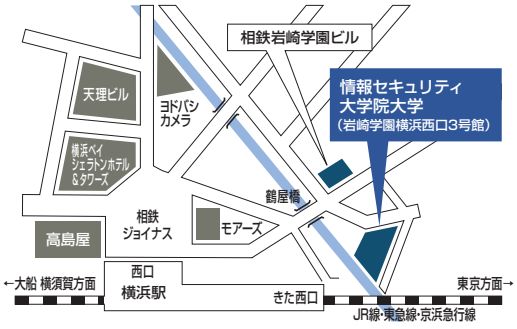
詳細は本学ウェブサイトでご確認ください。

■入学者選考方法

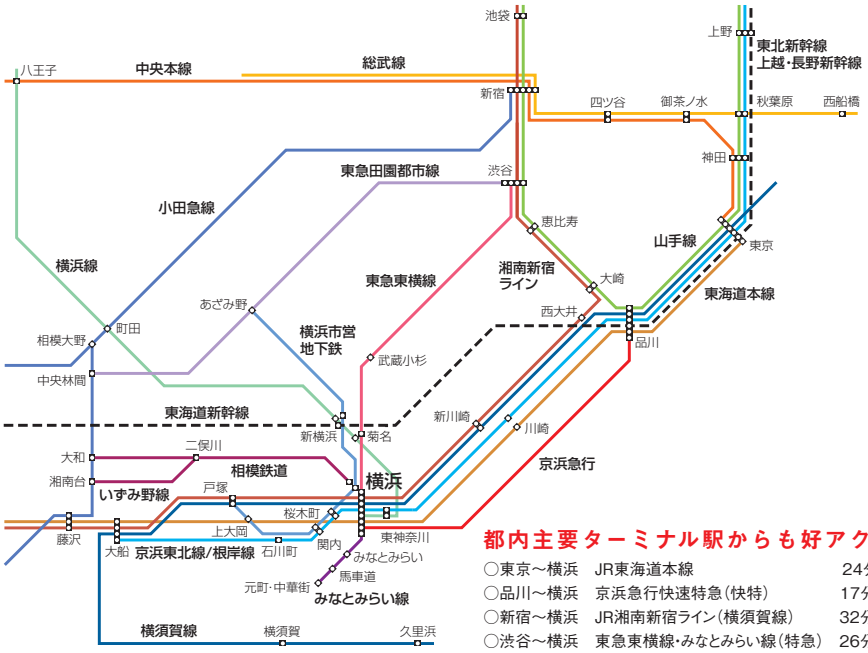
博士前期（修士）課程［2年制］	一般入試	面接（プレゼンテーションを含む）および志望理由書、学業成績、小論文等出願書類審査を総合して行う
	社会人入試	面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士前期（修士）課程［1年制］		面接（プレゼンテーションを含む）および研究計画書等出願書類審査を総合して行う
博士後期課程		口述試験（プレゼンテーションを含む）および研究計画書等出願書類審査によって、研究能力を総合的に判定する

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

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



（横浜駅きた西口より徒歩1分）



都内主要ターミナル駅からも好アクセス

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