学校法人 岩崎学園

明日の信頼を創ろう。

情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

2020-2021

Et le jour se lève.

INSTITUTE of
INFORMATION
SECURITY

サイバー空間と現実が融合する社会に急速に移行する2020年。必要なものは両空間の安全性・信頼性を確保するサイバー・フィジカル・セキュリティ。

予期しない出来事が、人と人とのつながりや働き方、社会全体のあり方まで変えてしまう。私たちはそうした大きな変化の中にいます。オンラインによる交流は物理的距離に関係なく広がり、DX（デジタルトランスフォーメーション）が進まなかった企業が一気にデジタル化・リモート化するなど利便性が向上した面も見られます。一方で在宅勤務における情報セキュリティ、移動制限などのリスクを抱えるグローバルサプライチェーンの再稼働、人々の不安に乗じたフェイクニュース等による情報操作といった各種課題への対応も急務といえます。なかでもサイバー空間と現実世界が相互に影響し合う社会で、安全性・信頼性を確保するサイバー・フィジカル・セキュリティの充実は欠かせません。

2004年開学のIISEC（情報セキュリティ大学院大学）は、当初から暗号や認証、マルウェア分析、セキュアな機器・システムの構築、組織マネジメントなど、サイバー空間から現実までを対象とし、実務経験・指導経験が豊富な教員を中心に、実践力を養う教育および研究指導を行ってきました。状況によりオンラインや校舎内で講義・演習を提供し、異なるバックボーンを持つ在学生の交流を促す工夫も行うなど、現実の変化に迅速に対応する機動力も特色の一つです。今起きている変化を前向きに捉え、サイバーフィジカルシステムをベースにSDGsにも配慮した新たな世界の夜明けを迎えるために。IISECで学ぶ情報セキュリティは次世代の社会を作るカギとなります。

2020年の世界と私 IISEC

■新入生レポート

情報セキュリティインシデントから組織が学び失敗を強みに変える品質マネジメントを研究。

床波 大貴さん　Hiroki TOKONAMI

情報セキュリティ研究科 博士前期課程1年

富士ゼロックス株式会社

時限	月	火	水	木	金	土	日
1	業務	業務	業務	業務	業務	個人識別とプライバシー保護	平日より遅めに起床。平日にできなかった家事などを済ませる
2						セキュリティシステム監査	
3						情報セキュリティ技術演習I	軽く体を動かすなどリフレッシュ
4							平日の夕食のために料理を作り置き
5	知的財産制度	研究指導	情報セキュリティ輪講I	リスクマネジメントと情報セキュリティ（校舎）	法学基礎		IISECの同級生とオンライン飲み会など
6	ソフトウェア構成論	夕食のために料理を作り置き	ネットワーク設計とセキュリティ運用	不確実性下の意思決定（校舎）	暗号・認証と社会制度	自宅で当日の復習	リラックスの時間
α	自宅で当日の復習			帰宅後、自宅で当日の復習	自宅で当日の復習	早めに就寝	

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

1>6月から日中は基本的に出社で、退社後に通学するには横浜駅近くのIISECは便利。 2>校舎で講義を受けるときは、空き時間に院生室で復習も。ただ、同級生との交流は校舎内では難しいため、意見交換や雑談はメールや休日のオンラインミーティングを活用。

◉先生方の真摯な対応に感銘 学ぶ意欲に応えてもらえると思った

大学の研究室で品質マネジメントを専攻し、入社後も一貫して全社の品質マネジメント、ICTサービスや業務委託サービスの品質保証・品質マネジメントなどを担当してきました。ここ数年で品質管理でも情報セキュリティの観点が重視されるようになり、DevOps、アジャイルといった新たな開発手法とセキュリティの両立なども課題となっていました。

そこで情報セキュリティを大学院で専門的に学びたいと考え、昨年5月に行われたIISECのオープンキャンパスに参加。学長の後藤先生をはじめ先生方が非常に熱心で、その後に個別相談で訪れた際も真摯に対応いただき、「先生との距離が近く、様々な疑問に丁寧に答えてもらえる」と確信して入学を決めました。

◉人のマネジメントを接点とし 組織学習を研究テーマに

これまで社内での品質管理は業務プロセスの標準化に着目したものが主流で、その先の人へのアプローチ、例えば人の意識や心理への対処などは困難でした。しかしIISECでは人のマネジメントも重要分野。こうした情報セキュリティと品質マネジメントの接点を生かし、「情報セキュリティインシデントの再発防止に向けて人の意識・行動の変容を目指す組織学習」を研究テーマに据えました。

私の1週間

◉講義からの学びだけでなく 同級生からの学びも積極的に

業務と大学院の両立のため早めに出社し、16時頃に退社。その後に講義を受け、当日中に復習を終えるよう心がけました。4月、5月はオンライン講義のみで、仕事も在宅中心でしたが、6月には出社となり、IISECも一部の講義は校舎で再開。上記時間割はその頃のものです。

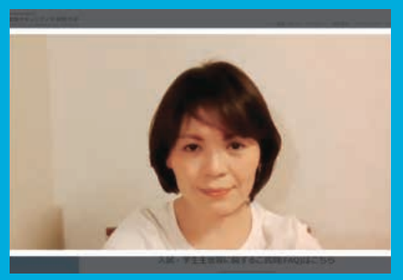
通学機会が減ると経験豊富な業界の同級生や先輩方との交流が限られますが、オンラインの掲示板、自主的な同級生オンラインミーティングなどで積極的な交流を図りたいと考えています。

◉失敗を繰り返さないための 適切な組織学習を研究

講義の中でも「リスクマネジメントと情報セキュリティ」「個人識別とプライバシー保護」では興味のあるテーマを自由に調査・発表する演習があり、情報セキュリティマネジメントの意義や情報の信頼性について気づきを得ることができました。

さらに1年次後期は組織行動、心理学など研究に沿った科目の履修を増やし、幅広く学んだ知識を研究や業務の中で整理・実践していきたいと思っています。

情報セキュリティインシデントという失敗を、組織の体質を強くする学習機会にして継続的な改善に結びつける。情報セキュリティをこのような品質マネジメントの事例として検証する予定です。



2020年の世界と私 IISEC

在宅勤務やオンライン講義など未体験の連続 難しい状況で学ぶ新入生、在学生の思いと 修了生からの応援メッセージを届けます。

今年4月からのIISECの2020年度前期は、新しい生活様式のもと、短時間の新入生オリエンテーション後は全てオンライン講義に切り替え、緊急事態宣言が解除された6月以降は、状況に応じてオンラインと校舎での講義・演習を行うなど、これまでとは異なる形で進みました。

そうした中でも変わらなかったのは、熱心に学ぶ在学生とそれを支援する教員の真摯な姿勢、変化に迅速に対応するIISECの機動力です。

巻頭特集では、新入生が学んだ内容と各自のリアルな1週間、現在の社会課題を踏まえて2年次の在学生が取り組む研究について紹介。

さらにセキュリティ業界やアカデミアなど、IISECで磨いた専門性を活かして活躍する修了生からの応援メッセージも掲載しています。

多様なバックグラウンドを持つ在学生が、情報セキュリティを軸に幅広く学び、教員や在校生同士の交流で新たな知見を得ていく。

開学以来、変わることのない理念で実践教育・高度研究を行ってきたIISECの“今”をお伝えします。

■在校生インタビュー

入学して実感した大学院の魅力

プログラミングとOSのセキュリティへの興味から入学。メモリ安全性を重視したRustを研究テーマに。

千脇貴之さん
Takayuki CHIWAKI
木更津工業高等専門学校専攻科出身
デロイト トーマツ サイバー合同会社に内定
博士前期課程２年

脆弱性や不正侵入を体験でも学ぶカリキュラム

私が学んでいた高等専門学校専攻科の特別講義で、田中英彦先生（当時のIISEC学長）の講義を聴いてセキュリティに興味を持ちました。専攻科ではプログラミングを学習していたので、その安全性を支えるOSのセキュリティを研究したいと考えてIISECに入学。1年次はセキュリティの基礎を学ぶため幅広い科目を履修し、特に「情報セキュリティ技術演習」ではネットワークの脆弱性や不正侵入を体験から学び、代表的な脆弱性の分類とそれを利用した侵入の手口などを知ることができました。

クリティカルな攻撃を受けにくいメモリ管理

並行してOSのセキュリティや情報のアクセス制御を研究する橋本先生のゼミに入り、前期はOSのセキュリティの現状を資料や論文などで調べ、1年次後期はクリティカルな攻撃を受けやすいメモリをどう守るかを中心に研究。これが現在の研究テーマ「Rustによる安全性の高いプログラミング」へと発展しました。Rust は比較的新しいプログラミング言語で、安全性を重視しながらメモリ管理も柔軟にできるなどの特色があります。橋本先生に研究手法や論文のまとめ方を相談しながら進めています。

2年次4月からはオンラインでの講義やゼミとなり、学生同士の議論では少しやりにくさがあるものの、基本的には通学時とさほど変わらず学習できています。ただ、IISECは社会人学生が多く、講義以外でそうした方にセキュリティ業界の話を聞く機会が減ってしまったのが残念です。今後はオンラインでも雑談ができるような仕組みを作ってもらえると有り難いですね。

希望通りセキュリティ業界に就職

就職はセキュリティ業界志望で、業界経験が豊富なIISECの先生方に企業情報を聞き、採用担当も務めた先輩からのアドバイスなども踏まえ、1年次10月頃から就職活動。希望していたデロイト トーマツ サイバー合同会社に内定しました。まずSOCに配属予定ですが、OSのセキュリティについては今後は技術面からの研究も続けるつもりです。

GAFAなどに個人データが集積される功罪など利用者の視点からプライバシー保護を見直す。

上條英夫さん
Hideo KAMIJO
損害保険会社を定年退職
博士前期課程1年
（2019年10月入学）

業務でサイバーセキュリティ対策が不可欠に

私は損害保険会社に入社後、IT部門に配属され、ここ10年ほどはシステムリスク管理を担当してきました。損保会社は金融機関であり、顧客の健康状態などセンシティブな情報も扱うため、非常に厳しいセキュリティ対策が求められます。近年はサイバーセキュリティへの対応も不可欠ですが、私は業務に限らずセキュリティ全般を学びたいと思うようになり、同社退職を前にIISECに入学しました。

オンライン講義は効率的な学習が可能

10月入学なので1年次後期からのスタート。火・水・木は17：00 過ぎに退社して5時限目から講義を受け、それ以外の日も仕事の後に空き時間を作ってレポートや課題の作成に充てました。講義の中でも、「情報セキュリティ特別講義」はセキュリティ業界の最新情報を幅広く知るため、実務者やジャーナリストなどが週替わりで講師を務めるリレー式の講義で、これは私が学びたい内容そのものでした。

今年4月からはオンライン講義に移行し、一時は通学して学ぶ機会もありました。講義はオンラインで何ら問題なく、逆に通学に必要な時間を予習・復習に充てられるのがメリットでした。しかし「情報デバイス技術」のように回路の組み立まで行うものは、これまで触れたことのない世界であったということもあり、オンラインではなく通学授業でよかったと感じています。

ゼミはセキュリティに関する幅広い領域を扱う後藤先生のゼミで、多様なバックグラウンドの社会人が集まるため、私の気づかない視点から意見がもらえて研究を多角的に検討するのに役立っています。

GAFA、接触確認アプリとプライバシー

利用者がなかなか増えない新型コロナウイルス接触確認アプリは、「プライバシーが国に把握されるのでは?」といった漠然とした不安が妨げの一つと考えられます。一方、GAFAなどにプライバシーに関する情報が集積・利用されている実態があります。「AI・IoT 時代における利用者視点でのプライバシーの考察」をテーマに、どうすれば利用者が安心してサービスを利用できるかをプライバシーの観点から研究したいと考えています。

■新入生レポート

テレワークなど働き方改革を進めるためゼロトラストネットワークを研究予定。

高木 祥一さん　Shouichi TAKAGI
情報セキュリティ研究科 博士前期課程1年
NTTコムウェア株式会社

時限	月	火	水	木	金	土	日
1	業務	講義準備	業務	業務	土曜日分の振替休日	個人識別とプライバシー保護	休日
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				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	アルゴリズム基礎	マスメディアとリスク管理			
5	知的財産制度	研究指導	情報セキュリティ輪講I	リスクマネジメントと情報セキュリティ			
6	ソフトウェア構成論	研究指導	ネットワーク設計とセキュリティ運用	帰宅		帰宅	
α		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>大学院への通学が可能な時期は、図書館にある過去の論文から先行研究を調べることも。2>パソコンは業務用と私用（大学院のオンライン受講用）を自宅のデスクにセット。業務終了から数秒で講義が受講できるので便利。通学はほかの在学生と会える楽しみがある一方で、移動のために業務時間が削られるのでスケジュール調整を慎重に。

私の1週間

◉技術とマネジメントの両面から学べるハイブリッドな講義も

火・土はフルタイムで大学院の講義や演習を受け、月・水・木も退社後に受講。土も講義・演習があり、金はその振替休日です。私は勤務先の国内留学扱いなので、職場の上司やメンバーの協力で業務を軽減してもらえ、感謝しています。

前期の「個人識別とプライバシー保護」は、技術面は後藤先生、マネジメント面は藤本先生がそれぞれの専門性をもとに講義されるので、認証に関わる幅広い知識を学んで整理ができそうです。一方で「セキュアシステム構成論」ではシステムの脆弱性と具体的な攻撃例を知り、業務に直結する知識も身につきました。

◉オンラインでも討論は容易
今後は顔を合わせての交流に期待

4月初頭の新入生オリエンテーション後、約2カ月はオンラインのみの講義・演習に。その間は仕事もフル在宅勤務で、一日中パソコンの前で過ごしました。少人数での討論は、講義で使うビデオ会議システムの小部屋を作る機能を活用。自分が見たWEBを参加者と共有するなど、情報共有が容易なのはメリットでした。

残念なのは、毎日16時30分から1階ロビーに在学生が集まるティータイムで会える人が少ないこと。様々な社会人との交流もIISECの魅力なので、何か別の機会が持てればと思います。

◉社内セキュリティの強化に
必要な認証分野の知識を深める

私は入社以来、お客様の社内セキュリティのコンサルティングや製品導入に携わり、近年は認証・アカウント管理の分野が業務の中心になっていました。ただ、セキュリティの知識は実務で必要な部分だけ身につけてきたため、一度その全体像を体系的に学び、さらに自分の得意分野も磨きたいと思って入学しました。

IISECの幅広い科目の中で、1年次の前期は「ソフトウェア構成論」などネットワークや技術寄りの科目を多めに履修し、後期は心理系、マネジメント系の科目の履修を増やして、文理をバランスよく学びたいと考えています。

◉全アクセスを危険と見なす
考えが働き方を変える

研究では、テレワークの推進などで改めて注目されている「ゼロトラストネットワーク」を扱う予定です。外部の脅威から社内を守るという現状の考えから、社内外を問わず全アクセスが危険と見なして対処する考えに転換すれば、場所を意識せず働けるようになり、働き方改革が一層浸透するでしょう。その核となる機能の一つが認証で、私がこれまで培ってきた専門性も生かせると考えています。

ゼミの大久保先生もこの分野に興味をお持ちで、オンラインまたは通学で定期的に個別指導を受け、資料の集め方や考えを深めるヒントをもらっています。

■修了生からのメッセージ

セキュリティ業界の先輩たち

目標が明確な方も、幅広く学びたい方も
多様な知識の習得と貴重な学友との交流で
有意義に過ごせる場所です。

H.K.さん
情報セキュリティ研究科 博士前期課程修了
（地方公共団体勤務）

ダークウェブ上の様々な違法データを
人工知能で分析する手法を研究

私は法学部を卒業後、SI企業に就職し、SEとして4年間勤務した後、情報技術関連の専門採用で地方公共団体に転職しました。入職後、近年のサイバーセキュリティ情勢に対応できる人材の育成プログラムの一環として、2019年にIISECに入学。

IISECでは、技術分野・マネジメント分野・法律分野等、様々な授業を通して、あらゆる角度からの情報セキュリティへのアプローチについて学びながら、ダークウェブ上のデータを人工知能で分析する手法の研究を行いました。

IISECは、他では理系・文系と分けられてしまうような研究分野の学生が一堂に会し、様々なアプローチで大きな課題に対して解決策を探求している、非常に希少な大学院です。学部卒の学生から留学生、社会人、そして定年後の方等、学生のバックボーンも十人十色です。

コロナ禍で注目される組織の情報保護対策
多様な観点で考察できるのはIISECのおかげ

多彩な授業や、研究室をはじめとするキャンパスライフでは、他の企業や官公庁から派遣された学生の方々と活発な意見交換を行う機会に多く恵まれ、かけがえのない学友にも出会うことができました。

新型コロナウイルスの影響を受けて、世界中でリモートワークが急速に拡大している今、自身の研究テーマに関連することだけでなく、組織の情報保護対策について、技術的要素・マネジメント手法・心理的アプローチ等の観点で考えを巡らせられているのは、IISECでの授業と、学友たちとの交流から得た最大の学びだと感じます。

研究したいこと・学びたいことがはっきりしている方も、漠然と情報セキュリティに興味がある方も、きっと有意義な時間を過ごすことができる場所、それがIISECだと思います。

IISECでセキュリティの本質を学び
安全に、より良い形で社会の変化を
促せる専門家を目指してください。

唐沢勇輔さん　Yusuke KARASAWA
情報セキュリティ研究科 博士前期課程修了
（Japan Digital Design株式会社）

セキュリティを体系的に学ぶため入学
働きながら修士課程が修了できるのも魅力

私は慶應義塾大学で国際政治を専攻し、卒業後に縁あってソフトウェア企業に就職しました。在籍中は開発部門で主にセキュリティ製品を担当していました。1年ほど前に転職し、今はJapan Digital Design株式会社というMUFGのフィンテック子会社でセキュリティを担当しています。

IISECへの入学を検討し始めたのは、ソフトウェア企業でセキュリティ製品の担当になって数年が経過した頃でした。海外の専門誌を読むなど自分なりに勉強したのですが、なかなか全体感がつかめずもどかしい思いをしており、セキュリティを体系的に学びたいと考えたのがきっかけです。オンライン講義だけの学校より、「物理的に学校に通う」のが時間を確保しやすいのではと考え、IISECへの受験を決めました。働きながら修士課程を修了できる点や、学ぶ分野の範囲が幅広く「全体感をつかみたい」という私の希望に合っていたのも選んだ理由です。

様々なバックグラウンドの社会人と接し
議論に参加することで理解が深まった

講義はとても面白く、様々なバックグラウンドの方との交流も楽しかったのを覚えています。他の方の研究に触れ、議論に参加することで理解も深まりました。また、自身の研究を通じて1つの分野を深く調べ、手を動かしたのも良い経験でした。もちろん、働きながら学校に通うのは大変でしたが、当時の上司や同僚の理解もあり、IISECが社会人学生向けに教育内容や制度が設計されているのも大きかったように感じます。

現在はコロナ禍で世の中が大きく変わり、急速にリモートワークが広がっています。私自身はさほど混乱なく仕事ができていますが、苦労している企業も多いようです。こうした局面で、セキュリティ専門家の仕事は変化を止めるのではなく、セキュアな形で変化を促すことだと思います。セキュリティの具体策は時代によって変化しますが、その本質は急には変わりません。ぜひIISECでそうした本質を学んでいただき、社会を安全に、より良い形で変化させていけるよう、一緒に頑張りましょう。

情報セキュリティの最前線を
働きながら学べる貴重な大学院で
社外でも通用する力が身につけられる。

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

グローバルに展開する大手電機メーカーと個人情報漏洩事故が起きた大手教育企業で通算15年、情報セキュリティガバナンスの構築、運用と個人情報保護に取り組んできましたが、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。また、実務の中で感じる矛盾などを、客観的な立場で整理して発信することで、課題解決につなげたい、という思いもありました。

在学中は、国際的に幅広い知見をお持ちの指導教員の先生に加え、実務経験から社会への達観した見識のある先生からご指導も受けられました。博士課程では博士ゼミで、指導教員以外の3名の先生から小さなテーマのご指導を得る機会があります。技術系の先生方からの鋭い指摘も、文理融合のこの大学の良いところだと思います。

切磋琢磨しつつも家族的な研究室のメンバーは、卒業後も貴重なネットワークになっています。

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

博士論文では、情報を流出させた企業・団体に厳しく、不適正に流通する名簿の販売者・利用者の処分は不十分という、日本の個人情報保護規範のアンバランスさを指摘。消費者が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考察しました。今後は個人情報保護の実効性を高める制度の導入などで、企業がビジネスに安心して取り組める環境整備の研究も考えています。

企業の情報セキュリティの責任者として悩むことは人材育成です。何事もなくて当然、と思われがちな情報セキュリティの仕事は、しばしば社内では影が薄く、また孤独です。彼ら彼女らを活かすには、私は、社外に目を向けることだと思います。社外の情報セキュリティコミュニティのネットワークに入り、社外で通用する力をつければ、転職などで活躍できる職種でもあります。欧米的なコミュニティですので、学位や資格も評価されます。IISECは働きながら学べる貴重な大学院だと思います。

サイバーセキュリティ分野に必要な
コアな技術から社会・経営まで学び
人生の新たな扉を開くチャンスに。

北野晴人さん　Haruhito KITANO
情報セキュリティ研究科 博士後期課程修了
（デロイトトーマツサイバー合同会社 パートナー（執行役員））

経営者としてのキャリアを持ち、研究者でもある先生の指導で
現実に即したセキュリティ研究ができた

私の博士論文「日本的経営における内部不正行為抑止の研究」は、従業者のモチベーション及び、組織との心理的関係（会社への帰属意識や仕事への取り組み姿勢など）や企業の人事・評価制度なども研究対象とし、同時に企業活動を支える「人」と「情報」に関するマネジメントが向かうべき方向性を研究したものです。経営資源全般に影響を及ぼす情報セキュリティは、本来なら経営者による経営行動の一部のはずです。そうした観点での研究成果が少なかった当時、私が研究をまとめられたのは、企業人と研究者の双方のバックグラウンドを持つ人材がそろうIISECだからこそだと思います。

特に私の指導教員だった林紘一郎先生（2019年3月退任）は、大企業経営者のキャリアをお持ちで、かつサイバーセキュリティ研究の専門家という貴重な方です。この恩師なしには研究を続けるのが難しかった可能性もあるでしょう。

サイバーセキュリティと企業経営を一体的に研究できる
環境で生まれた、日本企業への新たな成長戦略提案

私が上記論文で示した「ハイブリッドな経営」とは、日本的と言われる経営手法の有用な部分は残しつつ、成果主義などの今後重要となる要素を取り入れる人事施策と、一元的なIT基盤構築を推進するという提言です。私は以前から「働く人が幸せな職場は不正も起きにくい」との考えを持ち、そうした社内環境を実現する経営の一つとして「ハイブリッド型経営」に期待しています。これらの研究は私の業務とは異なる分野でしたが、そのおかげで企業経営の視点や考え方を学ぶことができました。この学びはまさに現在の自分の仕事に役立っていると思います。また将来の選択肢も広がったと感じます。

この大学院に多い30、40代の社会人学生は今後のキャリア形成のために入学していると思いますが、専門を深掘りするか違う分野に広げるか、そのどちらも対応できるのがIISECの魅力です。サイバーセキュリティの分野は、今後、デジタルトランスフォーメーションが進む社会で、その加速を支えるという非常に重要な役割を担っています。また常に変化と進化を続けるため、知的にとてもエキサイティングな世界です。コアなテクノロジーから社会・経営・法制度まで幅広く高度な学びを数多く得て、人生における新しい扉を開くチャンスがここにあると思います。

博士前期課程（修士課程）

育成する人材像 モデル履修プラン

■ 育成する人材像

○エンジニア、システムコンサルタント［技術系］

情報セキュリティに関する確かな専門知識と広い視野を備え、
セキュアなシステム・プロダクトの設計、開発、構築ができる技術者や、
技術面のコンサルティングを担う専門家

○セキュリティマネージャー、ビジネスコンサルタント［マネジメント系］

情報セキュリティに関する総合的な知識を持ち、社会の変動要因や
制約条件を踏まえて適正なリスク分析・評価を行い、企業・組織における
実効性のある政策提言や人間系セキュリティ対策を担うリーダー

■ 履修モデル［博士前期課程2年制プログラム］

［数理科学コース］履修例

情報セキュリティ輪講Ⅰ（2単位）＜必修＞［通年］／情報セキュリティ特別講義（2単位）＜必修＞
暗号・認証と社会制度（2単位）／暗号プロトコル（2単位）／アルゴリズム基礎（2単位）
数論基礎（2単位）／量子計算と暗号理論（2単位）／AIと機械学習（2単位）
個人識別とプライバシー保護（2単位）／統計的方法論（2単位）／不確実性下の意思決定（2単位）
情報セキュリティ技術演習Ⅰ（2単位）
研究指導（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）
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（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（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＞
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（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	○			
	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	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

2020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

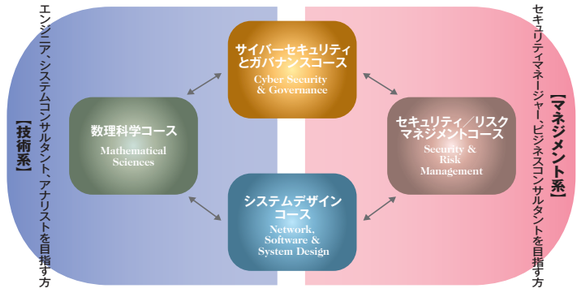
情報セキュリティ研究科 博士前期・博士後期

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。

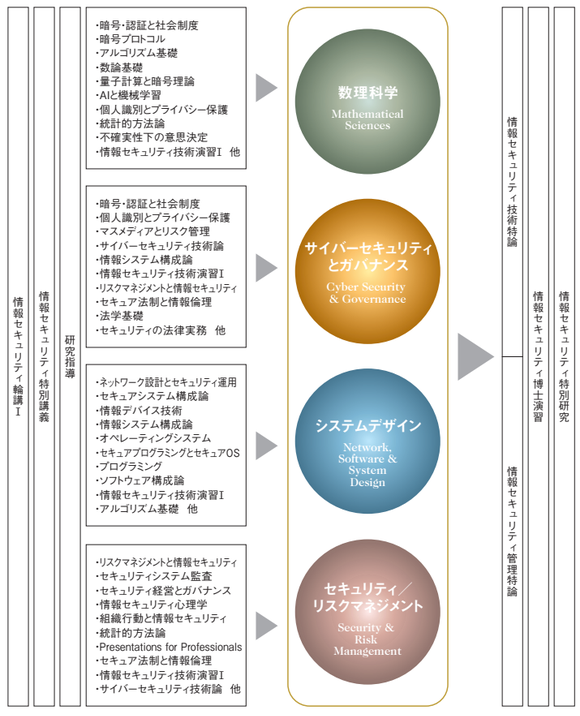
実社会における適正な情報セキュリティの実現には、暗号技術、ネットワーク技術、情報システム、管理運営、法制度、心理、情報倫理を融合させた総合的な対応が必要であり、それぞれの専門家が幅広い視野と見識をもって協力しあうことが不可欠です。情報セキュリティ研究科博士前期課程では、高度化・複雑化する企業・官公庁等の現場ニーズを踏まえ、技術系・マネジメント系とも幅広い人材育成需要、教育需要に応えるため、4つのコースフレームを2016年10月にリニューアルしました。なお、指導教員の履修指導のもと、他のコースが推奨する科目も自由に履修することができます。博士後期課程では、博士前期課程修了の知識をベースに、情報セ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



■ 2020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	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			
	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	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

INSTITUTE of INFORMATION SECURITY

博士前期課程
（修士課程）

授業科目概要
2020

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

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

博士前期課程専攻科目（例）

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

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

■暗号・認証と社会制度
本講義では、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理工学系の学生を対象とする。数学的および情報科学的な予備知識はなるべくその都度説明する。

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

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

■AIと機械学習
本講義では、情報セキュリティへの応用も活発化しているAIと機械学習の理論について学ぶ。講義は2つの部分に分かれている。最初の10回はC.M. Bishop著「パターン認識と機械学習」を教科書として機械学習の基礎理論を学ぶ。後半の5回はIan Goodfellow他著の「Deep Learning」を参考書として最近の深層学習の話題を取り上げ、最終回の演習では学生が独自に実験した内容を発表する。

■セキュアシステム構成論
情報通信技術（ICT）の普及により、あらゆる場所で情報システムが構築され利用されている。ネットワークを介した情報システムの利用、情報システム間の連携は、より高機能かつ効率的なシステムの構築を可能とするだけでなく、利用者の利便性を飛躍的に向上させてきた。一方で、インターネットを通じて不特定多数のユーザが情報システム群にアクセスできる環境においては、無防備なシステムが当然のように攻撃の対象となりうる。そこで、本講義では「セキュアな情報システムとは何か」という観点で、情報システムにおけるセキュリティ対策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
社会の隅々にまで浸透したソフトウェアシステムは、サイバー攻撃に対して脆弱なことが多く、社会全体に大きな負の影響を与えている。本科目では、攻撃に強くセキュアなソフトウェアを構築・運用するときに有用となる原則、概念、技法、ガイドライン、ツールなどについて紹介を行う。そして、完璧な防御方法はないことを前提に、ソフトウェアシステムの出入口での対策、一部に問題が発生した場合の影響範囲の局所化、最小権限の原則にしたがったアクセス制御、アクセス主体の管理などの手法とこれらの組み合わせに基づく考え方を解説する。

■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。本授業では、主に、オブジェクト指向モデルに基づいた最新のソフトウェア開発手法を取り上げ、ユーザ側、開発側双方の観点でセキュリティ対策をソフトウェアの面から考えるための基礎について学ぶ。オブジェクト指向による開発の理解を深めるため、一部、UMLを用いた分析、設計手法やeclipseによるJava言語プログラミングの実習を行う。

■実践的IoTセキュリティ
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。

■情報セキュリティ心理学
本科目では、「人間の行動は個人と周囲との相互作用から決定づけられる」という心理学の観点から情報セキュリティに関連する問題について解説する。具体的には、セキュリティに関する不適切な判断や行動を人間が選択するメカニズムを中心について説明する。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 English grammar.This means that your English language speaking skills - for example pronunciation or grammar skills - do not matter very much for this course. If you have just basic English-speaking ability and you want to learn or improve your presentation skills, you can take this course. In it, you will learn skills that you can apply to your Japanese presentations too. You will also discover that designing and presenting your original ideas can be fun and challenging. Try it and see what you can do!

TOPICS

2020年度新規開講科目

■不確実性下の意思決定
本科目では、リスクは不確実性の一形態であるという考え方に立って、不確実性を表現する数学モデルすなわち確率・確率分布に関する基礎、および不確実性の下での意思決定（合理的な行動）の基本的な考え方について講義を行うことをねらいとしている。具体的には大きく次の3つの内容を取り扱う。①A.Waldの「統計的決定関数」に基づく意思決定論におけるベイズ解（この場合の不確実性の源泉は自然環境などの変動）、②J.von Neumann & O.Morgenstern の「複数のプレーヤーによって行われるゲーム」の理論（この場合の不確実性の源泉は利害の対立する相手の行動）、③期待効用最大化行動に関する心理学からの批判としてのD.Kahneman & A.Tveskyのプロスペクト理論と行動経済学である。

■ネットワーク設計とセキュリティ運用
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、本科目では、企業（プライベート）ネットワークを主対象に最新の要素技術を利用したネットワークシステムの設計・運用管理手法、および、クラウドと仮想ネットワーク技術について考えていくこととする。また、昨今、重要性が増しているネットワークセキュリティ事故対応チーム（ＣＳＩＲＴ）の活動概要について学ぶ。

■リスクマネジメントと情報セキュリティ
本科目では、リスクマネジメントに関する基礎として、リスクやリスクマネジメントの定義、リスク処理のさまざまな手段、リスクマネジメントのプロセスについて講義する。リスクマネジメントと情報セキュリティマネジメントの関係について理解するとともに、情報セキュリティガバナンスの定義や全体像、ネットワーク社会の進展により複雑化する組織における情報セキュリティマネジメントを学ぶことにより、組織の経営管理とセキュリティの関係について学習する。さらに、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つけることをねらいとする。

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

博士前期課程
（修士課程）

授業科目履修例
2020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6日～8月15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				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	数論基礎	統計的方法論		情報セキュリティ技術演習Ⅰ
4		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理		
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）	ネットワーク設計とセキュリティ運用	特設講義（インターネットテクノロジ）or 不確実性下の意思決定	暗号・認証と社会制度	

◆後期（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		情報セキュリティ心理学		サイバーセキュリティ技術論（隔週）
4		セキュリティ経営とガバナンス	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	情報システム構成論	（研究指導）	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	特設講義（ブロックチェーン理論）	（研究指導）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B or セキュア法制と情報倫理	特設講義（データ・サイエンスとアナリティクス）	

▼＜社会人学生Bさんの履修例＞ セキュリティ／リスクマネジメントコース

◆前期（4月6日～8月15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				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	数論基礎	統計的方法論		情報セキュリティ技術演習Ⅰ
4		セキュアシステム構成論A	アルゴリズム基礎	マスメディアとリスク管理		
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	リスクマネジメントと情報セキュリティ	法学基礎	
6	セキュリティの法律実務 or ソフトウェア構成論	（研究指導）	ネットワーク設計とセキュリティ運用	不確実性下の意思決定	暗号・認証と社会制度	

◆後期（10月1日～2月10日）

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
1						セキュアプログラミングとセキュアOS（隔週）
2	（研究指導）	暗号プロトコル				
3	（研究指導）	国際標準とガイドライン		情報セキュリティ心理学		サイバーセキュリティ技術論（隔週）
4		セキュリティ経営とガバナンス	（研究指導）	特設講義（ハッキングとマルウェア解析）	量子計算と暗号理論	
5	情報システム構成論 or 組織行動と情報セキュリティ	（研究指導）	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	特設講義（ブロックチェーン理論）	（研究指導）	情報セキュリティ輪講Ⅰ	セキュアシステム構成論B or セキュア法制と情報倫理	特設講義（データ・サイエンスとアナリティクス）	

※新型コロナウイルス感染拡大の影響により、2020年度は遠隔講義を併用して開講しています。

■ 授業時間帯

社会人の方が在職のまま就学できるよう、平日夜間や土曜日も授業を実施します。※
※博士前期課程の標準修業年限1年制プログラム（若干名）においては、平日昼間の通学も必要です。

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

博士前期課程
（修士課程）

コース概要

コンサルティング能力を備えたエンジニア。技術やシステムに明るいマネージャー。
情報セキュリティ研究科博士前期課程では、情報セキュリティ全般にわたる広い視野と見識を備え、
リーダーとして現場における問題解決を担う高度な専門人材を育成します。

数理科学コース
Mathematical Sciences

あなたの作ったアルゴリズムがセキュリティの新しいステージを拓く

◆コース概要と研究キーワード

情報セキュリティには、暗号、匿名化、形式検証、学習、クラスタリング、マイニングなど、数多くの数理的な問題が存在しています。数理科学コースでは、これら、情報セキュリティに関わる、数理的な諸問題を深く理解し、よりよい解決を見出すことで、より効率的でより強力な情報セキュリティを実現するための基盤構築を目指します。講義による知識習得にとどまらず、少人数のセミナーや個別指導を通じて学習・研究を進めます。修了後は、企業・研究機関・行政機関等において、専門技術職・研究職を始めとするテクニカルスタッフとしての活躍が期待されます。

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

有田 正剛 教授
Seiko ARITA

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

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

“セキュリティ・バイ・デザイン”でネットワーク社会の安全を守る

◆コース概要と研究キーワード

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

研究キーワード：セキュリティ・バイ・デザイン、脅威分析、脆弱性評価、セキュリティテスト、フォレンジック、プライバシー保護、セキュアシステム、セキュアOS、マルウェア分類／検知／対策、攻撃検知／解析、人工知能セキュリティ、仮想化環境、組み込みソフト、制御システム、車載システム、ロボット、ハードウェアセキュリティ、セーフティ設計 他

◆修士論文イメージ

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

コースリーダーからのメッセージ

大久保 隆夫 教授
Takao OKUBO

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

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

先端技術とサイバー規範を併せ持つサイバーレスキュー隊のリーダーへ

◆コース概要と研究キーワード

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

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

湯淺 墾道 教授
Harumichi YUASA

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

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

適切なセキュリティ投資・対策・監査で、ITリスクの脅威から組織を守る

◆コース概要と研究キーワード

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

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

◆修士論文イメージ

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

コースリーダーからのメッセージ

藤本 正代 教授
Masayo FUJIMOTO

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

博士前期課程
（修士課程）

目的別
カリキュラム
活用パターン

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

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

パターン1 修士学位取得専念型

修士論文に向けての知識の獲得と研究に重点を置きたい

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

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

パターン2 ISS square 併修型

研究室や大学を超えた活動を通じて幅広い視野を養い、研究を実務に生かしたい

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

パターン3 ISS square & enPiT SecCap 併修型

ISSスクエアの活動に加えできるだけ実践的な演習や実習に取り組みたい

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

講義・演習をサポートしてくれる卒業生の声

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

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

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

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

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

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

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

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

文部科学省の平成19年度「先導的ITスペシャリスト育成推進プログラム」に採択されたISSスクエアは、情報セキュリティ大学院大学、中央大学、国立情報学研究所他、企業・研究機関11社の産学連携による高度情報セキュリティ人材育成プログラムです。暗号・認証、ネットワーク、システム、ソフトウェア、マネジメント、法制・倫理までトータルにカバーされた講義群、インターンシップや見学会、企業現場の実務家によるオムニバス講義などにより、経営・研究開発現場における現状の理解と問題の把握が促進されるとともに、サブゼミ的な位置づけの研究分科会や分野横断型のワークショップでの活動を通して、高度な問題発見能力と解決能力を身につけます。ISSスクエア活動の集大成としての年度末のシンポジウムでは、連携企業の皆様による成果発表審査も行われ、ISSスクエアプログラム修了者には、情報セキュリティ・スペシャリスト・サーティフィケートが授与されます。2008年の開始以来、本学からは200名以上の方がサーティフィケートを取得され、毎年、社会人学生を含む多くの方が本プログラムに参加されています。

詳しくは　http://iss.iisec.ac.jp/

成長分野を支える情報技術人材の育成拠点の形成 enPiT SecCap

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

詳しくは　http://www.seccap.jp/

博士後期課程

育成する人材像
課程概要

情報セキュリティ研究科博士後期課程では、確かな専門知識とマルチメジャーの視点を備え、
先端的な研究経験を通じて情報セキュリティに関する問題解決を先導するための能力を養います。

■ 育成する人材像

情報セキュリティの将来方向をリードする研究者

情報セキュリティに関する
高度な研究・分析能力と専門的知見を生かし、
社会の多様な領域でそれぞれの
中核的人材として活躍する研究者、研究指導者等を育成。

本課程の学生は、学際的な総合科学としての情報セキュリティ全般にわたる広い視野と見識を深めながら、その中の特定領域における高度に専門的な研究を行い先鋭的な学問の構築を経験することになります。これを通じて、産学官のさまざまな教育・研究機関の中核を担う自立した研究者、研究指導者、企業や行政機関等で活躍する実務研究者、ならびに当該分野における確かな教育能力と研究能力とを兼ね備えた大学教員等を育成します。

■ 後期課程科目概要

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

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

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

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2019年度までの間に本学博士後期課程を修了し、博士の学位を授与された方のおよそ3分の1は標準修業年限未満（1年から2年半）で博士学位を取得されています。

2. 所要単位数：
特別研究6単位以上＋博士演習2単位以上→合計8単位以上

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

■ 修了後の進路

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

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

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
2019-2020

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

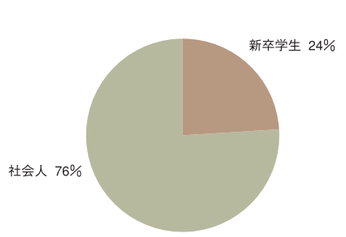
■ 社会人学生の所属組織

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】（2019-2020実績）
エヌ・ティ・ティ・コミュニケーションズ（株）／エヌ・ティ・ティ・コムウェア（株）／NTTテクノクロス（株）／LM総合法律事務所／海上保安庁／外務省／神奈川県警察／（株）ウフル／（株）エヌ・ティ・ティ エムイー／（株）小野測器／（株）協和エクシオ／（株）JR東日本情報システム／（株）静岡銀行／（株）センチュリーインフォテック／（株）タツノ／（株）ディー・エヌ・エー／（株）日立システムズ／（株）富士通ソフトウェアテクノロジーズ／（株）ミライト・テクノロジーズ／（株）ラック／警察庁／埼玉県／さくら情報システム（株）／ジェイアール東海情報システム（株）／第一生命保険（株）／東京海上日動火災保険（株）／（独）国立印刷局／日本コムシス（株）／日本電気（株）／日本放送協会／日本電気計器検定所／農林中央金庫／東日本旅客鉄道（株）／日立キャピタル（株）／富士ゼロックス（株）／防衛省／法務省／横浜市役所／楽天（株）／陸上自衛隊　など

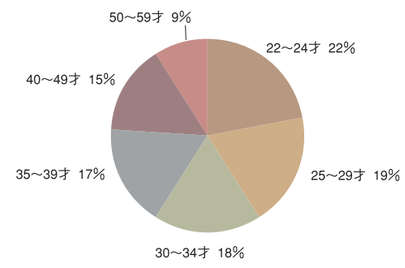
■ 現況

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



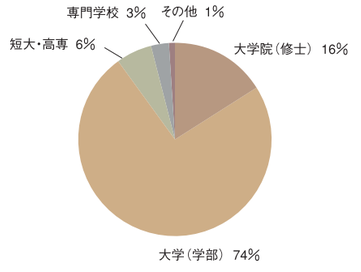
■ 年齢構成（入学時）

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



■ 最終学歴

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



博士後期課程

博士後期課程には、既に相当の研究実績、業務実績を有する研究者、技術者、実務家も在学中です。これは、情報セキュリティに関する新たな学問体系の構築をめざす本学にとって、後期課程学生同士や教員との切磋琢磨による優れた学際的研究成果の蓄積が期待できるばかりでなく、博士前期課程学生への教育効果の向上という観点からも非常に心強い存在となっています。

【所属組織一覧】（2019-2020実績）
NTTコミュニケーションズ（株）／オムロンヘルスケア（株）／（学）昭和女子大学／（株）サーバーワークス／（株）富士通研究所／（株）本田技術研究所／（株）三井住友銀行／（公財）笹川平和財団／合同会社ゼロワン研究所／（国研）産業技術総合研究所／Cs soft（株）／日本オラクル（株）／パナソニック（株）／三菱ケミカルシステム（株）　など

後藤厚宏

学長● 教授 Atsuhiro GOTO

■プロフィール
1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。2011年7月より本学教授。2014年4月より同情報セキュリティ研究科長。2017年4月より同学長。IEEE Computer SocietyのBoard of Governor, 情報処理学会理事、enPiTセキュリティ分野代表等を歴任。2015年11月より内閣府SIPプログラムディレクタ。2019年2月よりサイバーセキュリティ戦略本部員。

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

■主な研究テーマ
1. IoTとサプライチェーンセキュリティ
2. 重要インフラのセキュリティ
3. インターネットセキュリティ技術とID管理技術
4. クラウドと仮想ネットワーク

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

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

サイバーもフィジカルもシームレスに対応するセキュリティが不可欠な時代

情報が社会インフラや企業活動を支え、フィジカル空間とサイバー空間を融合したCPS（サイバー・フィジカル・システム）は社会に新たな価値を生み出しています。一方、サイバー空間の脅威がフィジカル空間での被害を引き起こし、またその逆も起こり得る時代となり、両空間を一体的に捉えたセキュリティは必要不可欠といえるでしょう。

本学はこうした現状に先駆け、2004年の開学当初からネットワークやデバイス、暗号といった情報技術分野と、法律、組織マネジメント、人間の心理や倫理などの社会・マネジメント分野を融合した情報セキュリティ教育を行ってきました。多様な分野にわたる情報セキュリティについて俯瞰しながら、それぞれの専門分野の知識・実践力を深められるのが大きな魅力です。

特に2020年は新型コロナウイルス感染症への対策により、人と人とのコミュニケーションや社会での働き方が大きく変わり、サイバー空間とフィジカル空間との融合が進みました。新たなつながりが生まれると同時に、より広い層にセキュリティへの関心を高めてもらう必要も出てきています。私は内閣府SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」のディレクターなども務めていますが、政府に「変化するのが当たり前の時代」との認識が浸透している手応えがあり、日本や世界が新たなフェーズに進むように感じています。

そうした中で本学は情報セキュリティを専門とする教育・研究機関として、セキュリティ業界で活躍するスペシャリストの育成はもちろん、企業の経営層、官公庁職員、社会のサービスインフラを担う人材などにもアプローチし、新たな生活様式におけるサイバー・フィジカル・セキュリティの推進役を果たしていきます。すでに経営層を対象とした短期集中プログラムも検討中です。

実務家・実務経験者も含む教員による実践的な講義 ハンズオンでの教育も重視

本学では情報セキュリティに関する幅広い科目を学習する際の指針となるよう、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を設けています。教員には実務家や実務経験者なども多く、各科目を実社会で得た知識・経験と統合して教え、学生はディスカッションやレポートによって自らの考えを掘り下げていきます。加えてハンズオンによる教育にも力を入れ、グループワークによる討議、サイバー攻撃の模擬演習なども取り入れています。また本学を含む産学官連携の人材育成プログラム「ISSスクエア」、全国の大学教員や企業の技術者が協力する実践教育「enPiT／SecCap」への参加も可能です。これらの講義・演習は一部をオンラインで提供し、コミュニケーションが活発になるよう工夫を加え、必要なときは十分な感染症対策を行った上で対面式でも実施するなど、状況に応じて適切な方法で教育を行っています。

多様なバックボーンを持つ在学生や同窓生のつながりは社会でも大きな強みになる

本学の在学生は20代から60代まで幅広く、社会人が8割を占め、セキュリティの専門企業、システム開発を行う企業、官公庁、メーカー、金融業などバックボーンは多彩です。大学院在籍中にそのような学生同士、さらには教員と広く深い人間関係が築けるのも本学の特徴の一つ。大学院修了後はそれぞれの立場からセキュリティに携わっていくため、卒年の離れた同窓生との交流も深まるなど、貴重な人脈を形成する絶好の機会といえます。

私が好きな言葉は「多様性」です。多様性によって分断されるのではなく、自分と他人との違いを意識し、それを前提につながり合い、新しいこと・面白いことに取り組む姿勢はこれからますます重要になるでしょう。本学が持つ多様性が、今後の社会を変える革新的なアイデアや思考力・実行力を育む一助になると考えています。

産学連携を意識した教授陣。

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

専任

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. Seiko Arita, Sari Handa, Fully Homomorphic Encryption Scheme Based on Decomposition Ring, IEICE TRANS., Vol.E103-A,No.1,pp.195-211,Jan. 2020.
2. 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.
3. Seiko Arita, Sari Handa, Subring Homomorphic Encryption, ICISC 2017, LNCS vol 10779, pp. 112-136, Seoul, Korea, 2017

■主な研究テーマ
主な研究対象領域は:
- 格子暗号や同種写像に基づく暗号などの、耐量子計算機暗号
- 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、ブロックチェーンベースの暗号プロトコル

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

■担当コース
数理科学コース、サイバーセキュリティとガバナンスコース

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（2015-2019）、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）。日本銀行金融研究所客員研究員（2020）。電子情報通信学会、情報処理学会、IEEE、IACR、IFCA各会員。電子情報通信学会バイオメトリクス研究専門委員会委員長、電子情報通信学会ISEC研究専門委員会委員。情報処理学会論文誌編集委員。

■主な研究業績
1. Yuhei Otsubo, Akira Otsuka, Mamoru Mimura, Takeshi Sakaki, "o-glasses: Visualizing x86 Code fromBinary Using a 1d-CNN," IEEE Access, Vol. 8, pp 31753-31763, IEEE 2020.
2. Yuhei Otsubo, Akira Otsuka, Mamoru Mimura, Takeshi Sakaki, Hiroshi Ukegawa, "o-glassesX: Compiler Provenance Recovery withAttention Mechanism from a Short Code Fragment," Proceedings of NDSS Workshop on Binary Analysis Research (BAR2020). (preprint)
3. Tatsuo Mitani, Akira Otsuka, "Confidential and auditable payments," In Proceedings of 4th Workshop on Trusted Smart Contract, WTSC'20. Kota Kinabalu, IFCA 2020. (to appear from Springer)
4. Tatsuo Mitani, Akira Otsuka, "Traceability in Permissioned Blockchain," IEEE Access, Vol. 8, pp 21573–21588, IEEE 2020.
5. Tatsuo Mitani, Akira Otsuka, "Traceability in Permissioned Blockchain," In Proceedings of the 2nd IEEE International Conference on Blockchain, 286-293. Blockchain-2019. Atlanta, GA. USA: IEEE ,2019.
6. M. Kadoguchi, S. Hayashi, M. Hashimoto, A. Otsuka, "Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning," In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), 2019, pp. 200–202.
7. Taisei Takahashi and Akra Otsuka. "Short Paper: Secure Offline Payments in Bitcoin," In Proceedings of 3rd Workshop on Trusted Smart Contract, WTSC'19. St. Kitts, IFCA 2019. Lecture Notes in Computer Science, LNCS 11559, pp.12-20, Springer, 2020.

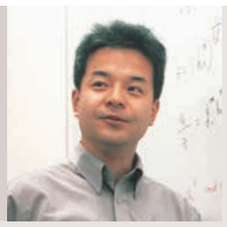
■主な研究テーマ
情報セキュリティ基礎理論（Blockchain, AIセキュリティなど）

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

■担当コース
数理科学コース

専任

土井　洋
教授
Hiroshi DOI



■プロフィール
1988年3月岡山大学理学部数学科卒業、1988年4月より1996年3月まで日立ソフトウェアエンジニアリング株式会社勤務。1994年3月北陸先端科学技術大学院大学情報科学研究科修了、2000年9月岡山大学大学院自然科学研究科修了。博士（理学）。中央大学研究開発機構助教授を経て、2004年4月より本学教授。2017年度 IPSJ Outstanding Paper Award 受賞。情報処理学会コンピュータセキュリティ研究運営委員会専門委員、横浜市個人情報保護審議会委員。

■主な研究業績
1. XOR-based Hierarchical Secret Sharing Scheme, K. Shima, H. Doi, Proc. of IWSEC 2018, LNCS 11049, pp.206-223, Springer (2018).
2. A Hierarchical Secret Sharing Scheme over Finite Fields of Characteristic 2, K. Shima, H. Doi, Journal of Information Processing, Vol.25(2017), pp.875-883 (2017).
3. A Fully Secure Spatial Encryption Scheme, D. Moriyama, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.28-35 (2011).
4. Secure and Efficient IBE-PKE Proxy Re-Encryption, T. Mizuno, H. Doi, IEICE Trans. Fundamentals, Vol.E94-A, No.1, pp.36-44 (2011).
5. 利用履歴を秘匿できるコンテンツ配信・課金方式に関する研究, 飛田孝幸, 山本博紀, 土井洋, 真島恵吾, 情報処理学会論文誌, 第50巻,第9号, pp.2228-2242 (2009).

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

■主な担当科目
暗号プロトコル、アルゴリズム基礎、研究指導、情報セキュリティ博士演習、情報セキュリティ特別研究

■担当コース
数理科学コース、システムデザインコース

専任

藤本　正代
教授
Masayo FUJIMOTO

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

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

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

■主な担当科目
リスクマネジメントと情報セキュリティ、個人識別とプライバシー保護、国際標準とガイドライン、
セキュリティ経営とガバナンス、研究指導

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

学長

後藤　厚宏
教授
Atsuhiro GOTO

■プロフィール
1984年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術の研究開発等に従事。2007年よりNTT情報流通プラットフォーム研究所長、2010年よりNTTサイバースペース研究所長。2011年7月より本学教授。2014年4月より同情報セキュリティ研究科長。2017年4月より同学長。IEEE Computer SocietyのBoard of Governor, 情報処理学会理事、enPiTセキュリティ分野代表等を歴任。2015年11月より内閣府SIPプログラムディレクタ。2019年2月よりサイバーセキュリティ戦略本部員。

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

■主な研究テーマ
1. IoTとサプライチェーンセキュリティ
2. 重要インフラのセキュリティ
3. インターネットセキュリティ技術とID管理技術
4. クラウドと仮想ネットワーク

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

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

副学長

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、2020年4月より副学長を併任。九州大学・中央大学・愛知学院大学・横浜市立大学非常勤講師、各省庁・自治体のセキュリティ、個人情報保護関係の審議会委員、ベネッセホールディングス情報セキュリティ監視委員会委員、（一財）日本サイバー犯罪対策センター理事等を務める。

■主な研究業績
1. 『電子化社会の政治と制度』（オプアワーズ、2006年3月）
2. 「アメリカの電子投票におけるVVPATの現状と課題」『情報ネットワーク・ローレビュー』第6巻（2007年5月）
3. 「個人情報保護法改正の課題 ―地方公共団体の個人情報保護の問題点を中心に―」『情報セキュリティ総合科学』第6巻（2014年）
4. 「ディジタルゲリマンダの法規制の可能性」情報処理58巻12号（2017年12月）
5. 「理念・原理・制度とサイバーセキュリティ法制 ー選挙を中心に」情報通信政策研究2巻1号（2018年12月）

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

■主な担当科目
法学基礎、セキュリティの法律実務、セキュア法制と情報倫理
特設講義（サイバーインテリジェンス）、研究指導

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

情報セキュリティ研究科長

大久保　隆夫
教授
Takao OKUBO

■プロフィール
1991年東京工業大学物理情報工学専攻修了。同年株式会社富士通研究所に入社。リバースエンジニアリング、分散開発環境、Webアプリケーションセキュリティの研究に従事。2006年、情報セキュリティ大学院大学入学、2009年同修了。博士（情報学）。2013年より本学准教授。2014年より同教授。2020年4月より情報セキュリティ研究科長。情報処理学会コンピュータセキュリティ研究会専門委員。日本ソフトウェア科学会実践的IT教育研究会運営委員。脅威分析研究会幹事、電子情報通信学会会員、IEEE CS会員、ACM会員。経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ1 分野横断サブワーキンググループ委員など。

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

■主な研究テーマ
セキュリティ・バイ・デザイン、脅威分析、脆弱性検知/予測、マルウェア解析/攻撃検知
組込みセキュリティ（車載、ロボットなど）、AI応用システムのセキュリティ構築、検証に関する研究

■主な担当科目
ソフトウェア構成論、プログラミング、情報セキュリティ技術演習I、実践的IoTセキュリティ、情報セキュリティ輪講I、研究指導

■担当コース
システムデザインコース、サイバーセキュリティとガバナンスコース

兼任
上沼　紫野
客員教授
Shino UENUMA

■プロフィール
虎ノ門南法律事務所所属弁護士
東京大学法学部卒業。Washington University in St.LouisにてLL.M.取得。知的財産権、IT関連、渉外法務等を中心に業務を行う。内閣府少年インターネット環境の整備等に関する検討会委員。
最高裁司法研修所刑事弁護教官（2012−2015）
■担当科目
セキュリティの法律実務

兼任
荻野　司
客員教授
Tsukasa OGINO

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

兼任
生越　由美
客員教授
Yumi OGOSE

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

兼任
佐藤　直
客員教授
Naoshi SATO

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

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
高橋　雅夫
客員教授
Masao TAKAHASHI

■プロフィール
独立行政法人 統計センター 情報技術センター長
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）を経て2019年より現職。在職中に筑波大学大学院システム情報工学研究科修了。博士（工学）。
■担当科目
特設講義（データ・サイエンスとアナリティクス）

兼任
種茂　文之
客員教授
Fumiyuki TANEMO

■プロフィール
エヌ・ティ・ティ・アドバンステクノロジ株式会社　セキュリティ事業本部　主席技師
名古屋大学工学部情報工学科、同大学大学院情報工学専攻修了後、1993年日本電信電話株式会社に入社、2018年より現職。ネットワークセキュリティ、CSIRT構築・運用の研究開発や企画運営等に携わる。現在は、情報セキュリティコンサルティングやサイバー演習支援サービスの提供業務等に従事。
■担当科目
特設実習（セキュリティ実践Ⅰ、Ⅱ）
ネットワーク設計とセキュリティ運用

兼任
辻　秀典
客員教授
Hidenori TSUJI

■プロフィール
株式会社情報技研 代表取締役社長
株式会社Premo（東大CPUベンチャー）代表取締役CEO
東京工業大学工学部情報工学科卒業、東京大学大学院工学系研究科情報工学専攻修了。博士（工学）。株式会社インターネット総合研究所を経て、株式会社情報技研を設立。2020年に新たにIoT時代を見据えたCPUベンチャーの株式会社Premoを東大内に共同設立。業務では、ICTシステムおよび情報セキュリティに関するコンサルティングはじめ、各種ICTシステムの提案、開発、構築に携わる。専門分野は、計算機アーキテクチャ、セキュアシステム構成、セキュアシステム基盤、メディア処理等。
■担当科目
セキュアシステム構成論

兼任
原田　要之助
客員教授
Yonosuke HARADA

■プロフィール
情報セキュリティ大学院大学 名誉教授
1979年京都大学大学院工学部数理工学専攻修了。1979年電信電話公社（現NTT）研究所入所、1999年情報通信総合研究所。2010年4月から2019年3月まで本学専任教授。2019年4月より本学客員教授。その他、1995年〜2011年大阪大学工学部大学院特任教授。また、中央大学理工学部・大学院、サイバー大学、フェリス女学院大学、電気通信大学などで非常勤講師を務める。また、国際標準ではISO/IEC JTC1のSC27（セキュリティ）、SC40（ITガバナンス）の規格のEditorとして活動。SC42（AI）ではJWG1のConvenorを務める。
■担当科目
セキュリティ経営とガバナンス

兼任
廣松　毅
客員教授
Takeshi HIROMATSU

■プロフィール
情報セキュリティ大学院大学名誉教授・東京大学名誉教授
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、ハーバード大学イェンチン研究所客員研究員等を経て、1989年東京大学教授（先端科学技術研究センター）、1995年より2009年3月まで同（大学院総合文化研究科・教養学部）。2009年4月から2017年3月まで本学専任教授。2017年4月より本学客員教授およびセキュアシステム研究所特別研究員。日本学術会議19期会員、20-21期・23期連携会員。2007年10月〜2015年9月内閣府統計委員会委員。2018年11月〜現在 日本学術会議 人文学・社会科学データインフラストラクチャー構築推進センター・センター長。
■担当科目
不確実性下の意思決定

兼任
堀江　正之
客員教授
Masayuki HORIE

■プロフィール
日本大学商学部・大学院商学研究科教授
カリフォルニア大学ロサンゼルス校（UCLA）客員研究員を経て現職。商学博士。現在、システム監査学会常任理事、日本監査研究学会会長、日本内部統制研究学会監事、情報処理技術者試験委員、会計検査院情報公開・個人情報保護審議会委員、金融庁・行政事業レビュー有識者会議メンバー、海上保安庁入札監視委員などを兼任。『扉談　不正一最前線』（同文舘出版、2019年）『ITのリスク・統制・監査』（同文舘出版、2009年、編著）『IT保証の概念フレームワーク—ITリスクからのアプローチ』（森山書店、2006年）、『システム監査の理論』（白桃書房、1993年）他、著書多数。
■担当科目
セキュリティシステム監査

兼任
丸山　満彦
客員教授
Mitsuhiko Maruyama

■プロフィール
公認会計士、情報システム監査人（CISA）
PwCコンサルティング合同会社　パートナー
1992年大手監査法人に入社。1998年より2000年まで米国の会計事務所に勤務。製造業グループ他米国企業のシステム監査を実施。帰国後、リスクマネジメント、コンプライアンス、情報セキュリティ、個人情報保護関連の監査及びコンサルティングに従事。2020年6月より現職。経済産業省の情報セキュリティ監査研究会、情報セキュリティ総合戦略策定委員会、個人情報保護法ガイドライン策定委員会他、国土交通省、厚生労働省の情報セキュリティ関連の委員会等の委員、日本情報処理開発協会ISMS技術専門部会等の委員を歴任。2012年3月末まで内閣官房情報セキュリティセンター情報セキュリティ指導官。
■担当科目
セキュリティシステム監査

兼任
森井　昌克
客員教授
Masakatu Morii

■プロフィール
神戸大学大学院工学研究科教授
1989年大阪大学大学院工学研究科博士後期課程通信工学専攻修了、工学博士。愛媛大学助教授、徳島大学工学部教授などを経て、2005年より現職。現在、情報通信工学、特にサイバーセキュリティ、情報理論、暗号理論、暗号理論等の研究、教育に従事。2018年経済産業大臣賞受賞、2019年総務省情報通信功績賞受賞
■担当科目
サイバーセキュリティ技術論

兼任
Ray Roman
客員教授

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

兼任
小林　雅一
客員准教授
Masakazu KOBAYASHI

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

兼任
藤村　明子
客員准教授
Akiko FUJIMURA

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

兼任
塩月　誠人
客員講師
Makoto SHIOTSUKI

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

※上記は2020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。2018年よりNEDO研究評価委員。

■主な研究業績
1. Toshihiro Matsui, Hideki Asoh, et. Al., “Integrated Natural Spoken Dialogue System of Jijo-2 Mobile Robot for Office Services”, Proc. Of American Association for Artificial Intelligence (AAAI), 1999
2. Toshihiro Matsui and Satoshi Sekiguchi, “Multithread Implementation of an Object Oriented Lisp System, EusLisp,” in Advanced LISP Technology (Eds.) Taiichi Yuasa and Hiroshi G. Okuno, IPSJ, Taylor and Francis, 2002.
3. 山崎信行、松井俊浩、「並列分散リアルタイム制御用レスポンシブプロセッサ」、日本ロボット学会誌、Vol. 19, No. 3, 2001（論文賞受賞）
4. 松井俊浩、「オブジェクト指向型ロボットプログラミング言語EusLisp」、日本ソフトウェア科学会コンピュータソフトウェア、Vol. 23, No. 2, pp. 62-71, 2006.
5. Dang Duy Thang and Toshihiro Matsui, “A Label-based Approach for Automatic Identifying Adversarial Examples with Image Transformation”, Proc. Of the Seventh International Symposium on Computing and Networking (CANDAR'19, IEEE), Nagasaki, 2019.
6. Dang Duy Thang and Toshihiro Matsui, “Adversarial Examples Identification in an End-to-end System with Image Transformation and Filters”, IEEE ACCESS, 2020.

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

■主な担当科目
情報デバイス技術、プログラミング、情報システム構成論、実践的IoTセキュリティ、研究指導

■担当コース
システムデザインコース

専任
稲葉　緑
准教授
Midori INABA

■プロフィール
2006年、名古屋大学大学院環境学研究科社会環境学専攻、博士後期課程修了。博士（心理学）。2005年、独立行政法人交通安全環境研究所非常勤研究員、2006年より国立大学電気通信大学大学院情報システム学研究科助教。2009年ロンドン市立大学心理学科客員研究員。2013年よりJR東日本研究開発センター安全研究所研究員。2017年4月より本学准教授。研究テーマはセキュリティ行動を支援するシステム・仕組みの検討。国土交通省運輸審議会運輸安全確保部会専門委員。情報処理学会論文誌編集委員、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、中曽根平和研究所「デジタル技術と経済・金融」研究会研究委員等。日本心理学会、日本応用心理学会等会員。

■主な研究業績
1. 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.
2. 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.
3. 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.
4. Inaba, M., Shirai, I., Kusukami, K., Haga, S. Development of interactive educational game about human error — In a case of developing a serious game to learn slips — P.Carvalho, P. Arezes（共編）, Ergonomics and Human Factors in Safety Management, CRC Press, Chapter 12, 253—270, 2016年.
5. 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.

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

■主な担当科目
統計的方法論、情報セキュリティ心理学、研究指導

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

専任
橋本　正樹
准教授
Masaki HASHIMOTO

■プロフィール
情報セキュリティ大学院大学情報セキュリティ研究科博士後期課程修了。博士（情報学）。2010年より同助教、2014年より同准教授。2014年4月-2015年3月、ロンドン大学ロイヤルホロウェイ校情報セキュリティグループの訪問研究員として英国に滞在。専門はアクセス制御、OSセキュリティ、不正侵入検知・防御等。情報処理学会、電子情報通信学会、日本ソフトウェア科学会、IEEE各会員。電子情報通信学会／情報通信システムセキュリティ研究会（ICSS）専門委員、情報処理学会／コンピュータセキュリティ研究会（CSEC）専門委員、情報処理学会論文誌ジャーナル/JIP編集委員会委員、日本ソフトウェア科学会SIG-rePiT主査（2019年度）、CSITS2019 Programme Committee Member、NETSAP2019 Workshop Organizer 等。

■主な研究業績
1. Yamauchi, T., Akao, Y., Yoshitani, R. et al. Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes. Int. J. Inf. Secur. (2020). https://doi.org/10.1007/s10207-020-00514-7
2. M. KADOGUCHI, S. HAYASHI, M. HASHIMOTO and A. OTSUKA, "Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 2019, pp. 200-202, doi: 10.1109/ISI.2019.8823360.
3. Toshihiro Yamauchi, Yohei Akao, Ryota Yoshitani, Yuichi Nakamura, Masaki Hashimoto: Additional Kernel Observer to Prevent Privilege Escalation Attacks by Focusing on System Call Privilege Changes , Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (IEEE DSC 2018), pp.172-179, 2018.
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.

■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

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。

■ 主な年間スケジュール（2019年度ご参考）

4/6	入学式・新入生歓迎会
4/8	前期開講
5/25	春季オープンキャンパス ホームカミングパーティ
8/3	前期授業期間終了
8/31	修士論文等発表会（9月修了）
10/1	後期開講
10/11	第16回アドバイザリーボード
11/16	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
2/22	修士論文等発表会（3月修了）
3/21	学位記授与式

■ 入学式
2019.4.6

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
2020.2.22

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。

2019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
2020.3.21

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。

※新型コロナウイルス感染拡大防止のため、例年より簡素化して実施しました。

■ 情報セキュリティ大学院大学連携教授（2020年8月現在）

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

株式会社東芝 研究開発本部 研究開発センター サイバーセキュリティ技術センター 研究主幹	秋山 浩一郎	株式会社KDDI総合研究所 取締役執行役員副所長 (兼)KDDI株式会社 情報セキュリティ本部 情報セキュリティフェロー	田中 俊昭
株式会社日立製作所 研究開発グループ テクノロジーイノベーション統括本部 システムイノベーションセンタ 主管研究長	鍛 忠司	日本電気株式会社 研究開発ユニット 上席技術主幹	谷 幹也
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	久保田 実	株式会社富士通研究所 セキュリティ研究所長 (兼)ブロックチェーン研究センター長	津田 宏
東京電機大学 研究推進社会連携センター特別専任教授（特命教授） （兼）サイバーセキュリティ研究所 所長	佐々木 良一	パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略部 戦略課 課長	中野 学
日本アイ・ビー・エム株式会社 東京基礎研究所 セキュリティ&ハイブリッドクラウドイノベーション担当部長	佐藤 史子	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	平田 真一
沖コンサルティングソリューションズ株式会社 代表取締役社長	杉尾 俊之	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
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	横浜国立大学 大学院 環境情報研究院 教授	松本 勉

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（2020年8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	朝日新聞社 編集委員	須藤 龍也
NTTコミュニケーションズ株式会社 取締役 イノベーションセンター長	稲葉 秀司	株式会社MM総研 代表取締役所長	関口 和一
沖電気工業株式会社 コーポレート本部 情報企画部 部長	長田 肇	神奈川県 副知事	武井 政二
日本電信電話株式会社 取締役 研究企画部門長	川添 雄彦	日本放送協会 専務理事 技師長	児野 昭彦
株式会社三井住友銀行 名誉顧問 前会長	北山 禎介	慶應義塾大学 総合政策学部長	土屋 大洋
芝浦工業大学大学院 客員教授	國井 秀子	国立研究開発法人 情報通信研究機構 理事長	徳田 英幸
早稲田大学 名誉教授	後藤 滋樹	独立行政法人 情報処理推進機構 理事長	富田 達夫
横浜市 副市長	小林 一美	株式会社エヌ・ティ・ティ・データ 執行役員 技術革新統括本部長	冨安 寛
富士通株式会社 執行役員常務 海外リージョン Americasリージョン長	斎藤 淳一	三菱電機株式会社 開発本部 役員技監	中川路 哲男
		パナソニック株式会社 コネクティッドソリューションズ社 常務	行武 剛
日本電気株式会社 エンタープライズビジネスユニット 執行役員常務	堺 和宏	株式会社 日立ソリューションズ セキュリティプロフェッショナルセンタ チーフセキュリティアナリスト	米光 一也
東京電機大学 研究推進社会連携センター 顧問 客員教授	佐々木 良一		

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。

■ 所属研究室（ゼミ）を越えた交流機会

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





Refresh and enrich

■ 課程外教育プログラム等の優待受講

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

■ 客員研究員制度を利用した研究活動の継続

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

■ 学費等納入金

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

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

［博士前期課程2年制プログラム4月入学の学費納入例］

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

■ 奨学金

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

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

種別	貸与月額（※2020年4月現在）
第一種奨学金（無利子）	50,000円又は88,000円（博士前期課程の場合）
	80,000円又は122,000円（博士後期課程の場合）
第二種奨学金（有利子）	5，8,10,13,15万円のなかから選択

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

② 岩崎学園奨学金（有職の社会人も利用可能です）

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

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

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

■ 特待生制度

人物、学業成績が特に優秀であり、自立心と向上心が旺盛な情報セキュリティ研究科博士前期課程［2年制］入学志願者※の中から特待生選抜試験に合格した者に対し、授業料等の減免を行う制度です。
（※4年制大学等卒業見込み者に限ります。出願資格の詳細については、本学ウェブサイトに掲載の特待生選抜学生募集要項にてご確認ください）

○ 特待生選抜試験に合格した場合の初年度学費

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

○ 特待生募集人数:若干名（特待生Ⅰ、特待生Ⅱとも）

INSTITUTE of INFORMATION SECURITY

情報セキュリティ大学院大学
セキュアシステム研究所
Secure System Laboratory

所長 後藤 厚宏
情報セキュリティ大学院大学
学長・教授

本研究所では、拡大・多様化するIT技術の恩恵を、多くの人々が安心して享受できるようなセキュアな社会を実現するため、様々な分野の専門家の協力を得て、セキュリティに関する研究活動を行っています。
研究スタッフには、情報セキュリティに関する技術、経営、法律、倫理等のスペシャリストを、学界、実業界から招聘して、将来の社会インフラを支えるセキュアシステムに向けた研究開発を強く推進していきます。

■ セキュアシステム研究所のプロジェクト

セキュアシステム研究所は、次の５つのプロジェクトにて研究開発活動、調査研究活動を進めています。

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

新たな(未知の)セキュリティ脅威への対応するために、サイバーセキュリティの様々な情報収集・分析・交換を通して信頼できる社会基盤作りへの貢献を目指します。具体的には、次の４つの活動を進めます。

- 情報収集のための新技術の研究を行い、それを用いた独自の情報収集を進めます。
- 産官学のセキュリティエキスパートが寄合所(“Cyber security meet up”)としての人的な交流の場を作ります。
- 信頼関係に基づくセキュリティ情報の交換(“Trusted” Cyber Security Information eXchange : TSIX)を運営します。
- 最新セキュリティ技術の評価検証を行います。

❷ セキュリティ国際標準化 (IS: International Standardization)プロジェクト

セキュリティ分野の国際標準化の推進戦略の立案と提言を進めます。また、国際標準化を担う次世代人材を育成することによって、我が国のセキュリティ技術による国際標準化に貢献します。

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

セキュリティ人材のキャリアデベロップメントに関わる調査・提言を進めます。そのために、日本ネットワークセキュリティ協会(JNSA)や情報セキュリティ教育事業者連絡会(ISEPA)など、セキュリティ人材育成の関係機関と連携を密にします。

❹ Internetと通信の秘密 (SC: Security in Communications)プロジェクト

ビッグデータ時代のプライバシー、通信の秘密の在り方と法制度、通信キャリアやクラウドプロバイダーの役割など、通信の秘密とプライバシーに関する調査・提言を進めます。

❺ 航空制御システム (AC: Aviation Control Systems)プロジェクト

航空業界の専門家と情報セキュリティの専門家が密に議論する研究会活動を通じて、航空制御のセキュリティ課題について調査研究と提言活動を進めます。

■ Messages

客員研究員を代表してお二方からメッセージをいただきました。

岩井 博樹
株式会社サイント
代表取締役

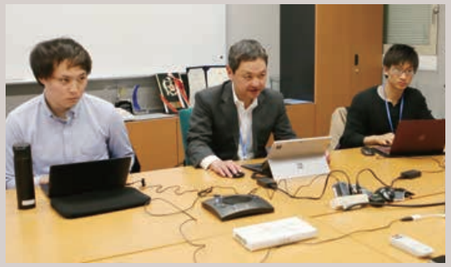
セキュア構築、侵入検知システムの導入設計、セキュリティ監視業務等を経てデジタルフォレンジック業務に携わる。サイバー攻撃被害の解析や訴訟事件等のデジタル鑑定解析、セキュリティ対策評価等を担当。
著作として「標的型攻撃セキュリティガイド」等がある。

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

名和 利男
株式会社サイバーディフェンス研究所
専務理事／上級分析官

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

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



ホームカミングパーティ

1Fホールでのweekday tea-time

新入生歓迎パーティ

ゼミ合宿

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

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

http://www.iisec.ac.jp/

〒221-0835　神奈川県横浜市神奈川区鶴屋町2-14-1
お問い合わせ先　045-311-7784　iisec@iwasaki.ac.jp

Japan University Accreditation Association
since 1947
UNIVERSITY ACCREDITED
2017.4~2024.3

IWASAKI GAKUEN
学校法人 岩崎学園

■Contents

■学生募集課程概要

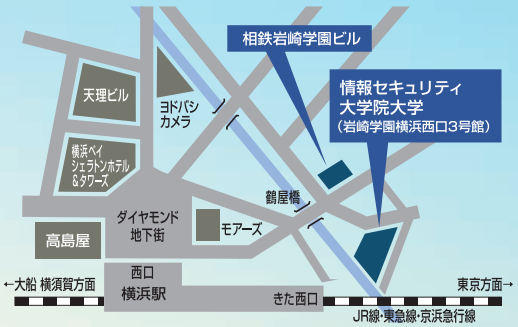
研究科	専攻	課程	標準修業年限	募集人員
情報セキュリティ研究科	情報セキュリティ専攻	博士前期（修士）課程［2年制］	2年	40名
		博士前期（修士）課程［1年制］	1年	若干名
		博士後期課程	3年	8名

詳細は本学ウェブサイトでご確認ください。

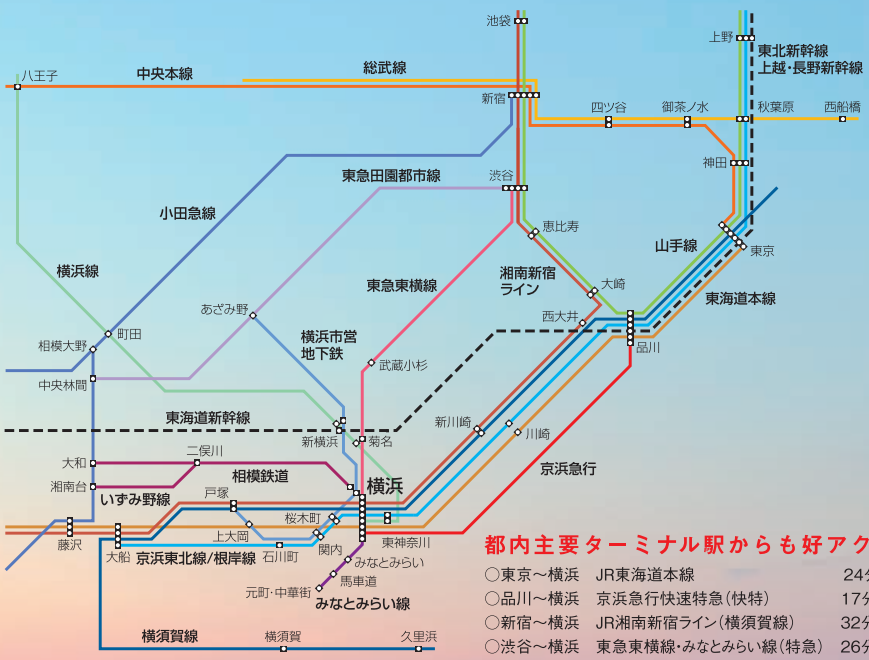
■入学者選考方法

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

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



（横浜駅きた西口より徒歩1分）



都内主要ターミナル駅からも好アクセス

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