情報セキュリティ理解のための先端暗号技術入門

― 量子時代に向けた暗号技術の基礎と、高機能暗号、耐量子計算機暗号の理解へ向けて ―

オンライン開催 11/25（木） 基礎編

基礎的な暗号知識と数学理論、カードベース暗号理論のご紹介

＜実習あり＞

1. 全体概要（オリエンテーション）と暗号技術の基礎
   ― 國廣 昇 氏（筑波大学　システム情報系　教授）
2. カードベース暗号 ◆実習あり
   ― 水木 敬明 氏（東北大学 サイバーサイエンスセンター 准教授）
3. 現代の暗号技術を支える数学 ◆実習あり
   ― 安田 雅哉 氏（立教大学 理学部 数学科 准教授）

暗号技術の基礎（RSA 暗号・楕円曲線暗号）や、整数論、素因数分解、代数等の数学理論を学び、実際のプログラム実装に触れていきます。

全日程 3 日
各日 10:00-16:30
会場併設

オンライン開催 11/29（月） 先端編

量子計算と暗号技術の基礎、量子時代の暗号技術開発について

＜実習あり＞

1. 格子理論を用いた暗号攻撃 ◆実習あり
   ― 高安 敦 氏（東京大学大学院 情報理工学系研究科 講師）
2. 量子計算基礎とその暗号への応用 ◆実習あり
   ― 國廣 昇 氏
3. 耐量子計算機暗号
   ― 篠原 直行 氏（情報通信研究機構 研究マネージャー）

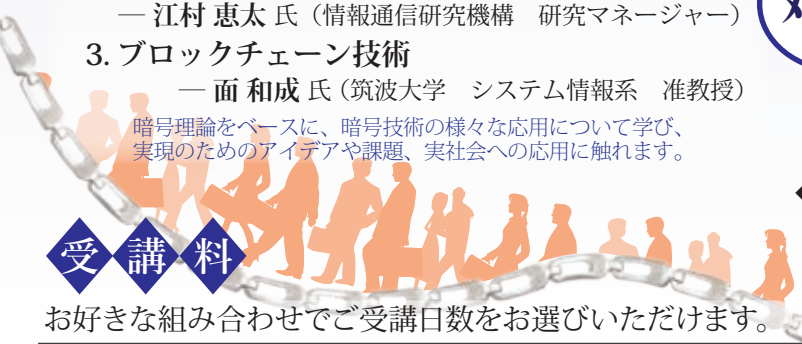
量子計算の基礎概念や、耐量子計算機暗号の理論に触れ、到来する量子時代に必要な知識を学ぶことができます。

オンライン開催 11/30（火） 応用編

様々な暗号応用技術（秘密計算、高機能暗号やブロックチェーン技術）

1. 秘密計算
   ― 大原 一真 氏（産業技術総合研究所　研究員）
2. 高機能暗号と証明可能安全性
   ― 江村 恵太 氏（情報通信研究機構　研究マネージャー）
3. ブロックチェーン技術
   ― 面 和成 氏（筑波大学　システム情報系　准教授）

暗号理論をベースに、暗号技術の様々な応用について学び、実現のためのアイデアや課題、実社会への応用に触れます。



対象者

定員 15 名（先着順）

企業、研究機関にご所属で、
◆量子時代の暗号技術について学び始めたい方
◆情報通信、サイバーセキュリティ分野の技術開発に携わる方
◆新たなコンピュータの開発を目指す方、コンピュータ技術（ハード、ソフトウェア）のセキュリティや暗号技術に携わる方
◆DX、IoT の導入、設計に携わる方
◆暗号技術の開発、実装に携わる方
◆数学（mod 計算、ベクトルなど）に馴染みがあり、暗号技術に関心をお持ちの方
◆現代の暗号（共通鍵暗号、公開鍵暗号、デジタル署名、RSA暗号等）からさらに進んだ技術の導入を検討している方
・・・・・・など

受講料

お好きな組み合わせでご受講日数をお選びいただけます。

区　分	全日程	1 日受講
A　一般	48,000円	18,000円
B　KISTEC パートナー団体会員 C　神奈川県内中小企業＊	38,400円	
D　C 以外の神奈川県内企業 E　神奈川県内在住の個人の方	43,200円	

※ 神奈川県内中小企業とは事業所が神奈川県内にあり、資本金が3億円以下、または、企業全体の従業員が300人以下である企業をさします。

オンライン開催（ZOOM 使用）
※ 講師と話せる会場受講も可能です。
※ 諸状況によりオンライン開催のみとなる可能性がございます。
※ オンラインでのご受講が難しい場合は、お気軽にご相談ください。

※詳細はホームページをご覧ください。
https://www.kistec.jp/learn/researcher/sentanango/

主催（地独）神奈川県立産業技術総合研究所

カリキュラム編集者からのメッセージ

暗号技術は、既に私たちの生活にすっかり溶けこみ、暗号なしでは、もはや生活することはできません。今、広く利用されている RSA 暗号や楕円曲線暗号などの公開鍵暗号は、現代の暗号技術の基盤であるにもかかわらず、量子時代の到来により、瞬く間に解読されてしまう可能性があります。そのため、安全に使える暗号技術を準備しておくことが、情報通信技術の必須課題となっています。

しかし、暗号技術を議論する上で、安全性だけを気にするわけにはいきません。暗号化し、安全に情報を保持することだけがゴールではなく、暗号化した上で、その情報をいかに有効活用するかが重要です。それにも関わらず、労力をかけて集めた有用なデータでさえ、秘密にしてしまう事例も多く見られます。こうした状況に対して、データを暗号化したままなんらかの有用な計算ができる準同型暗号、秘匿計算などの高機能暗号は、応用技術として広がりつつあります。ビットコインを代表例とするブロックチェーン技術も暗号技術を基礎としたものであり、今後、さらにこの分野の応用・開発が加速していくことでしょう。

本講座では、初日で RSA 暗号・楕円曲線暗号という基礎から暗号理論とその技術に触れ、その安全性議論の基礎となる整数論、素因数分解、代数等の数学理論を学び、実際にプログラムへ実装することにも触れていきます。2 日目は量子計算の基礎概念や、ショアのアルゴリズムによる現代暗号の安全性への影響、次世代暗号としての耐量子計算機暗号（ポスト量子暗号）の理論をまとめ、到来する量子時代に必要な知識を学ぶことができます。3 日目は、暗号技術の様々な応用として、秘密計算、高機能暗号やブロックチェーン技術まで幅広くカバーし、実現アイデアや実社会への応用について触れます。

量子計算機時代の暗号技術の課題・最新動向に触れたい、基礎理論を学びなおしたいという研究者・技術者の皆様のご受講をお待ちしております。

— **國廣 昇**（筑波大学　システム情報系　教授）

後援・協賛（一部申請中）

（一社）CIEC（コンピュータ利用教育学会）、（一社）情報システム学会、（一社）情報科学技術協会、（一社）情報処理学会、（一社）人工知能学会、（一社）電気学会、（一社）電子情報通信学会、（特非）日本ネットワークセキュリティ協会、（一社）日本暗号資産ビジネス協会、（一社）日本応用数理学会、（一社）日本危機管理学会、（一社）日本機械学会、（一社）日本計算工学会、（一社）日本数学会、（公社）計測自動制御学会、コンピュテーション研究会、川崎商工会議所、株式会社ケイエスピー

申込要項

必ずご確認の上お申し込みください。

- 必ずZOOMの推奨環境を事前にご確認ください。また、「オンライン講座に関する規約」をご一読の上、ご確認いただける場合のみ、FAXでのお申込みを受付いたします。
- PC、インターネット通信環境（有線LAN接続、Wi-Fi推奨）、PCに接続可能なマイク、カメラ、スピーカーをご用意ください。（PCに内蔵されている場合は不要）
- 受講資格はお申込みをいただいた方(1 申込 1 名)に限ります。
- 申込締切後、受講決定者には受講票・受講料請求書等の必要書類をお送りします。また、受講日前日までにお申込みいただいたご住所へ印刷テキストをお送りします。
- 申込締切後でも、定員に余裕がある場合はお申込みを受付けられる場合がありますのでお問合せください。
- 全受講コースお申込みの場合、全日程の出席者には「修了証」を送付いたします。
- 講義中、許可なく講義内容の一部、およびすべてを複製、転載または撮影、配布、印刷など、第三者の利用に供することを禁止します。
- やむを得ない事情により、日程・内容等の変更や中止をする場合があります。
- その他、お申込みについてご不明な点は、主催者へお問い合わせください。

詳細はこちら

HP または FAX にてお申込みいただけます。

*FAXでお申し込みの場合は、お手数ですが着信確認のお電話をお願いいたします。

https://www.kistec.jp/learn/researcher/sentanango/

FAX送付先　044-819-2097

お問い合わせ

地方独立行政法人
神奈川県立産業技術総合研究所

〒213-0012 神奈川県川崎市高津区坂戸 3-2-1　KSP 東棟 1 F
Tel (044)819-2033
E-mail　manabi@kistec.jp　URL　https://www.kistec.jp/

情報セキュリティ理解のための先端暗号技術入門 コース 受講申込書

* 規約確認	□「オンライン講座に関する規約」を確認しました
* 全日程受講	□
選択受講	□ 11/25(木)　□ 11/29(月)　□ 11/30(火)
フリガナ 氏名	
フリガナ 企業名	
所属・役職名	
所在地	〒　－
E-mail	
TEL FAX	TEL　(内　)　FAX

＊太枠内は必須項目です。必ずご記入のご確認をお願い申し上げます。
＊の項目は、該当するものに○・✓印をつけて下さい。

備　考（会議室受講のご希望やテキスト送付先があればご記載ください）

＊性別　男　女

＊年代　10代以下　20代　30代　40代　50代　60代　70代以上

＊資本金
3億円以下　3億円超～10億円未満　10億円以上　該当なし

＊従業員数
300人以下　301人～1,000人未満　1,000人以上

＊この講座のご案内はどこでご覧になりましたか
ダイレクトメール(郵送)　メールマガジン(KISTEC発行 / 学会や関連団体)　雑誌・会報等　チラシ　ポスター　KISTECホームページ　学会や関連団体のホームページ　講師から　上司から　受講生から　その他（　）

＊今後、KISTECからの情報をお送りしてよろしいですか
郵送　：　要　・　不要　/　メールマガジン　：　要　・　不要

＊KISTEC科学技術理解増進パートナーシップの会員ですか
はい　・　いいえ

個人情報の利用及び提供の制限　申込書にご記入いただいた個人情報は、当所の事業等に関する情報や参加者募集の案内などの範囲内で利用または提供いたします。個人情報は、取扱目的以外に利用したり、第三者に提供することはありません。

（コースID：21オ）