研究室紹介

情報セキュリティの世界最先端の研究室 宮地研究室！！

電気電子情報通信工学専攻　情報通信工学コース
サイバーセキュリティ工学領域　宮地研究室
博士後期課程３年　宮地　秀至

✧　宮地研究室について

宮地研究室は工学研究科の電気電子情報通信工学専攻の情報通信コースに所属しています．学部生では，工学部の電子情報工学科の情報通信工学コースに所属しています．宮地研究室は 2022 年度では 3 名の先生と 1 名のスタッフ，10 名の学部生（4 回生：9 名と早期配属の 3 回生:1 名），22 名の博士前期課程，7 名の博士後期課程の学生，2 名の研究生の合計 44 名が在籍している大所帯研究室です！！大所帯研究室で，研究分野はセキュリティやプライバシーの多岐の分野に広がっているため，宮地研究室に所属しているだけで多くのことが学べることが魅力の一つです．また，15 名が海外から来られているので，英語での交流が活発で，英語が話せるようになるのも魅力の一つです．今回はそんな魅力だらけの宮地研究室について紹介していきます！

✧　研究内容

情報セキュリティという概念は情報の機密性，完全性，可用性の 3 つの原則を満たすことを言います．情報セキュリティの機密性を守るために，暗号化が重要となり，宮地研究室ではこの暗号化に関する研究が行われています．例えば，アナログの事象をオンラインで実現するためには，オンライン上で機密性を満たす必要があります．このオンライン上の安全を実現するための様々な研究が存在しております．今回はその中から宮地研究室で実際に研究されている 3 つの研究を紹介します．1 つ目は，オンライン上に実現するアルゴリズムに相当する『プロトコルの構築』です．2 つ目は，セキュリティとは異なる概念である『プライバシー保護』です．3 つ目は，暗号の安全性を評価する『暗号解析』です．下記にこの 3 つについて簡単に説明します．

1. **プロトコルの構築**

   プロトコルの構成には，ブロックチェーンの構成や誰が文書に署名したかを保証する『署名』などがあります．署名などはブロックチェーンやオンラインで文書の取引を行うときに必要不可欠な技術なので，安全にプロトコルを構築することは重要な技術です．

2. **プライバシー保護**

   プライバシー保護はセキュリティとは異なる概念です．セキュリティはあるデータを暗号化した後,そのデータを復号する処理が必要となりますが,プライバシー保護では,暗号化してから元のデータに復号しません．プライバシー保護を行うために元のデータにノイズをかけるという処理などが実行されます．プライバシー保護は病院のカルテの個人情報を取り扱うときに使用される重要な技術です．

3. **暗号解析**

宮地研究室では，耐量子計算機暗号の一つである格子暗号の評価がメインに研究が行われております．格子暗号の評価の部分は数学の知識をかなり必要とするため，難しい内容の一つなのでなかなかこの分野も行われている研究室は少ないです．なので，暗号解析の研究も網羅していることも宮地研究室ならではのよさです！

✧ **ENLINKER**

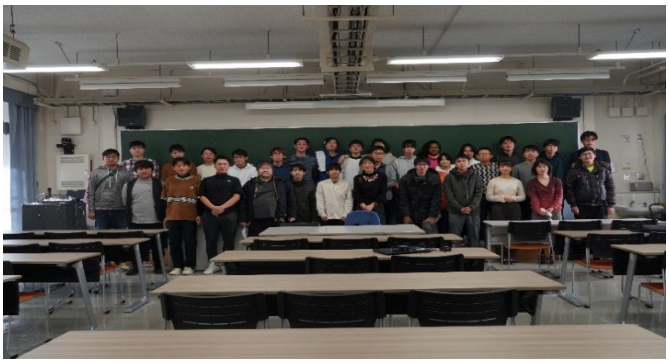
最後に私の研究も簡単に紹介します！私は SNS×プライバシーの研究をしています．阪大生限定で使用できる『ENLINKER』という名称で宮地研究室の Po-Chu Hsu 氏らと共に運営しています．我々は，SNS に関する様々な問題を解決するための研究をしております．現在 ENLINKER では，プライバシー問題の解決だけでなく，大阪大学の学生が交流できるように運営しております．ENLINKER では，学生同士の情報交換なども行われております．是非 ENLINKER のホームページにお越しください！(https://enlinker.com/)

✧ **イベント**

宮地研究室はイベントの多い研究室です！今年は吹田祭，研究室の卒業生との交流イベント，BBQ，新年会などたくさんのイベントの交流も行いました．このイベントの様子を写真で紹介します！

9 月の BBQ

10 月の吹田祭



1 月の新年会

✧ **最後に**

ここまで拙いながらも宮地研究室の紹介を行ってきました．宮地研究室では，多くの研究分野があり，イベントなど多くのことを行える研究室です．さらに，自分がやりたい研究は自由にできる風通しのよさもあります．宮地研究室のよさがひとつでも多く伝わると幸いです．是非一度宮地研究室のホームページまでお越しください！

- 宮地研究室：https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/index-jp.html