



2024年度 佐古研究室紹介

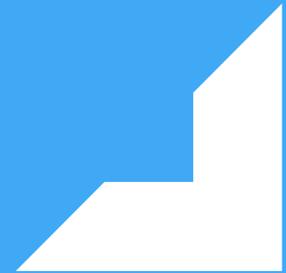
早稲田大学基幹理工学部情報理工学科
佐古研究室

アジェンダ

1. 研究目的
2. 研究内容
3. 研究室運営
4. 個別面談



研究目的



安全・安心で健全なIT社会を実現するために必要な
要素技術・運用を踏まえた設計技術を研究し、
具体的なセキュリティ・プライバシーサービスを探究する



要素技術？設計？運用？

一人ひとりの意見を反映する仕組み

電子投票システム

安全な実装

社会ルール

電子投票の要件

投票プロトコル設計

安全性評価

ミックスネット

ゼロ知識証明

公開鍵暗号・確率暗号

安心・安全で健全な社会

セキュリティプライバシーサービス

運用を踏まえた
設計技術

プロトコル設計

要素技術

分散型デジタルアイデンティティの例

GAFAにアカウントBANされたら嫌だ

たくさんパスワードを管理するの大変

自己情報コントロールの実現

安全な実装

社会エコシステム

W3C, IETFにおける標準化

Verifiable Credentials Data Model

JSON-LD

選択的開示

オープンソースライブラリ

匿名認証・ゼロ知識証明

鍵管理

ブロックチェーン

ワクチン証明書

TrustedWeb

成績証明書？

ドローンの相互
認証？

安心・安全で健全な社会

セキュリティプライバシーサービス

プロトコル設計

要素技術

佐古研究室では目的に対して2つのアプローチ取り組んでいます

サービスの探究

安全・安心で健全なIT 社会を実現するために必要な具体的なセキュリティ・プライバシーサービスを探究する

要素技術の深耕

要素技術をより安全に
社会で使えるように深める

何があったらうれしい？

どうしたらもっと安心？

どうしたらもっと便利？

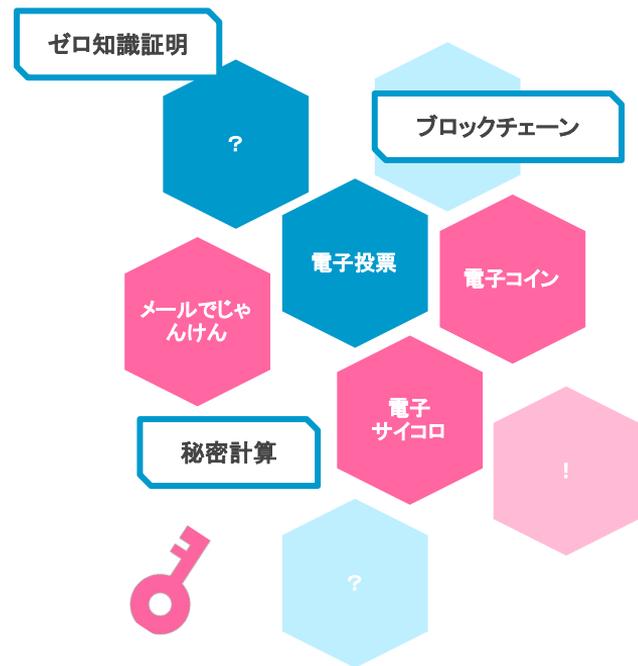


暗号プロトコルはセキュリティ・プライバシー・公平性などを実現させる

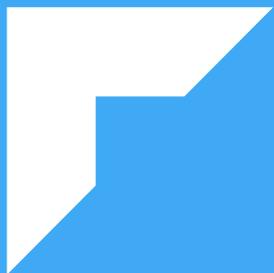
マジックプロトコルです

第三者をはさまず、メールやチャットでじゃんけんができる？
生年月日を開示せずに20歳以上であることを証明できる？
プログラムにお任せではなく、「福引き」の公平さを確認できる？

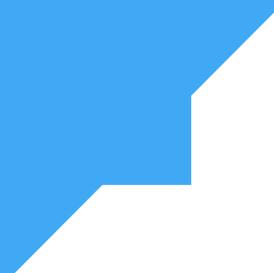
一見できなさそうに思えることを次々に実現可能にする、
数々の**マジックプロトコル**が暗号技術をつかって構成できます。



SAKO LABORATORY



研究室運営



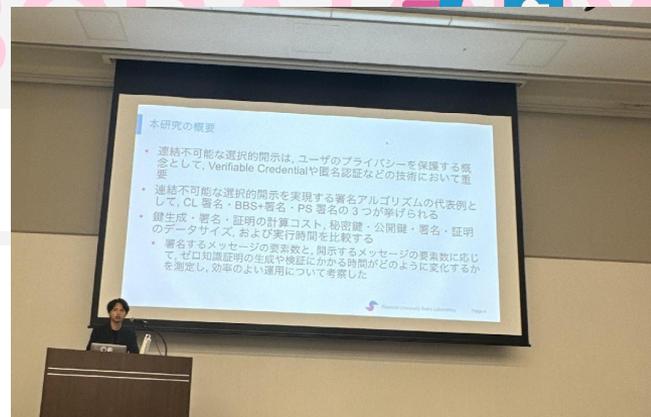
SAKO LABORATORY

研究室の運営方針「自分軸で見つける研究テーマ」

- 一人ひとりが自分ごととして「安心安全で健全なIT社会」を実現するために関わってください。
- 基本的に**テーマを自分で選んでOK**
 - ↳ 興味のある人はブロックチェーン、Verifiable Credentials, MyData Servicesと一緒に取り組みましょう
- お互いをリスペクトして、建設的に議論し、知識を共有する。(私にも教えてください！)
- 「**暗号と情報セキュリティシンポジウムSCIS**」や「**コンピュータセキュリティシンポジウムCSS**」に研究成果を発表することを目標とします。国際会議にもチャレンジしましょう。

国内外問わず、積極的に学会に参加しています

- ACNS, SCIS, CSS, CSECなど
様々な学会で積極的に研究成果
を発表しています
- 学会を通じて、産学様々な方と交
流し、自身の研究に活かすことが
できます



研究室では毎週のゼミでのトピック発表や輪講が主な活動です

- ゼミ(2023年後期は基本木曜日3限。2限になる時もあり)では持ち回りで**自分の関心のあるトピックについて調査して発表**を行っています
- また、基本的な暗号理論やブロックチェーンに関する書籍を分担して読み、それを発表する**輪講**にも参加することができます
 - プロ研究生・初学者向け 和書(半年読切)
 - 4年生以上向け Anderson「Security Engineering」洋書
- 上記の活動を通して研究テーマを探し、それについて研究をしていきます

前述の活動以外にプロジェクト参加や、研究室メンバー主体の活動もあります

- **研究室外との共同のプロジェクト**に参加することもあります
 - └ 現在進行中のNICTのSSI-IoTプロジェクトや社会科学系の制度設計プロジェクトがあります。
- **研究室メンバー(学生)が主体**となって活動を行うこともあります
 - └ 現在は、研究から得たアイデアを具現化したシステムを作成し、国際的なハッカソンに提出したりしています。

実装したアプリやライブラリを海外のハッカソンに出したりしています

- 研究して得られた成果などを，国際的なハッカソンに出すことができます
- このプロジェクトは，ウェブアプリやデスクトップアプリ，物理的なラズパイと暗号技術と絡めて提出し，準優勝しました。



<https://devpost.com/software/an-anonymous-door-unlocking-with-anonymity-revocation>



合宿やクリスマス会等(任意参加)



軽井沢合宿(2023/9)
研究マップを作ってBBQ



クリスマス
カタンの会



下記の時間に 学生が研究室で待機しています
少しでも興味がある方は お気軽にお越しください！

- **日時**: 3月18日(月)19日(火)21日(木)
 - └ 18・19日: 10:00～17:00(随時)
 - └ 21日: 10:00～12:00(随時)
- **場所**: 55号館 S 8階 807号室
 - └ ドアが閉まっていたらノックしてください
- **個人面談予約先**: kazuesako@aoni.waseda.jp

研究室のHPはこちら
<https://sako-lab.jp>



- Boneh & Shoup: A Graduate Course in Applied Cryptography(2020)
<https://toc.cryptobook.us/>
- Ross Anderson: Security Engineering (2021)
- 伊豆・田中・花岡・岩田: とことんやさしい暗号の本(2010)
- 光成: クラウドを支えるこれからの暗号技術(2015)
- " : 暗号と認証のしくみと理論がこれ1冊でしっかりわかる本(2021)
- 黒澤: 現代暗号への招待(2010)、現代暗号の基礎数理(2019)
- ブロックチェーン技術の教科書(2018)
- ブロックチェーン技術の未解決問題(2017)