2023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

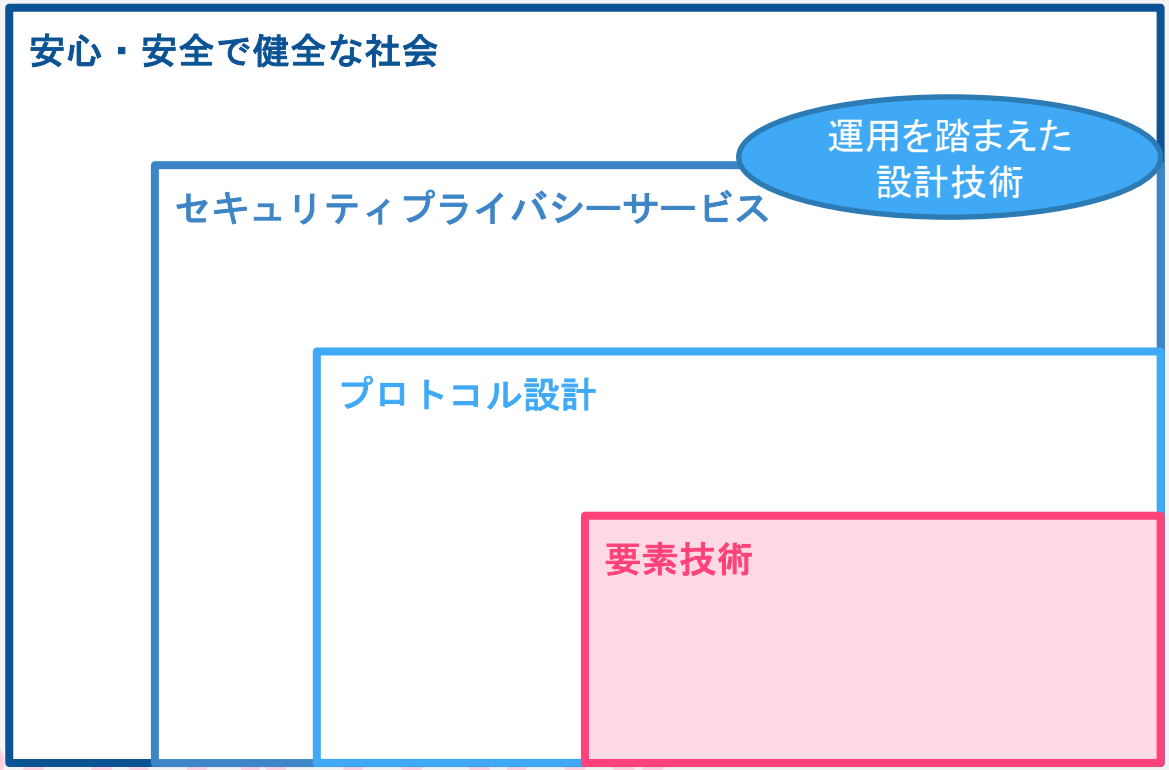
SAKO LABORATORY

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・プライバシサービスを探究する

SAKO LABORATORY

電子投票の例

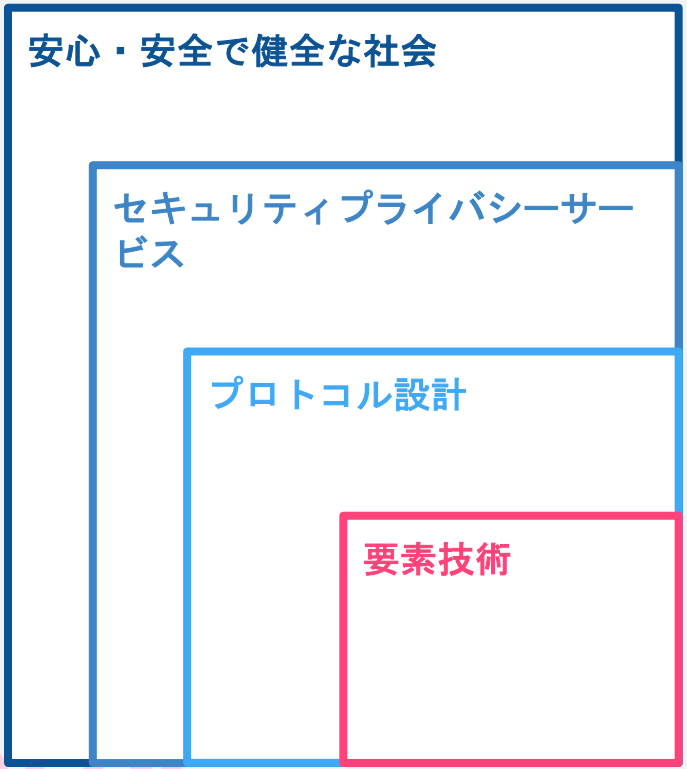
- 一人ひとりの意見を反映する仕組み
- 電子投票システム
- 安全な実装
- 社会ルール
- 電子投票の要件
- 投票プロトコル設計
- 安全性評価
- ミックスネット
- ゼロ知識証明
- 公開鍵暗号・確率暗号



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
- 自己主権ID管理
- 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



２つのアプローチ

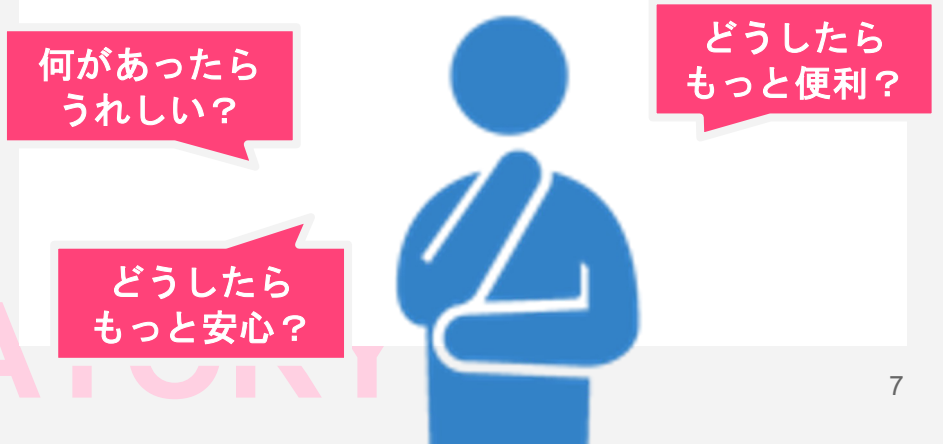
佐古研究室では目的に対して２つのアプローチ取り組んでいます

サービスの探求

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



要素技術

暗号プロトコルはセキュリティ・プライバシ・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.

研究室運営

研究室の運営方針について

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に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。

研究室での活動について

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

その他の活動について

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
  - 現在は研究室運営を円滑にすすめるためのWebアプリケーション開発をアジャイル開発手法を学びながら行っています

研究室訪問

SAKO LABORATORY

研究室訪問

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20日（月）22日（水）23日（木）
  - ㄴ 20・22日：11:00～17:00（随時）・面談は午後のみ
  - ㄴ 24日：10:00～12:00（随時）
- **場所**：55号館 S 8階 807号室
  - ㄴ 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

参考文献

- 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)
- 太田・黒澤・渡辺：情報セキュリティの科学(1995)
- 光成：クラウドを支えるこれからの暗号技術(2015)
- 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)

SAKO LABORATORY