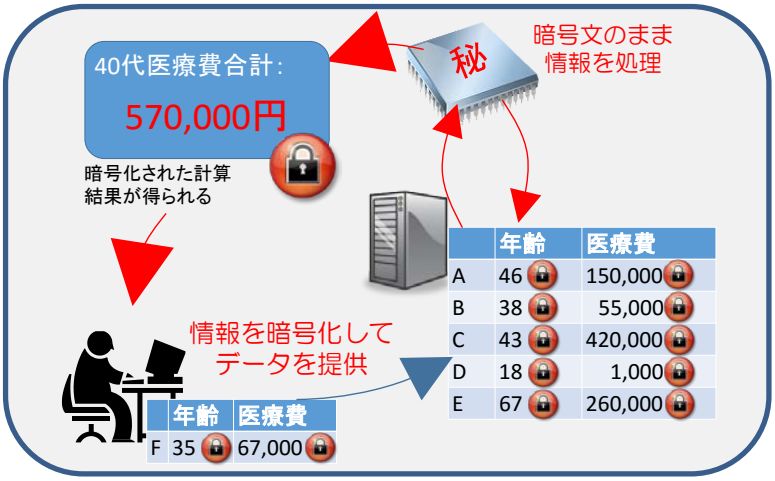
情報科学部　情報セキュリティ研究室

教授　尾花　賢

◆ 研究テーマ

情報セキュリティ研究室では，今日普及が急速に進んできているクラウドコンピューティングを安心安全に利用するための暗号技術の研究を行っています。その中でも特に，秘密分散法や秘匿演算法と呼ばれる暗号技術に取り組んでいます。秘密分散法は，秘密にしたい重要なデータを，複数の部分情報に分散して管理する技術で，一定の個数の部分情報が集まらない限り，元の秘密情報がどのようなデータであったのか全くわからないことを保証する技術です。秘密分散法は，その性質から，重要な情報をクラウドストレージに保存する際などに重要な技術となります。秘匿演算法は，データを暗号化して保存し，そのデータを復号することなく，検索や，統計処理など様々な情報処理を行うことを可能にする暗号技術です。秘匿演算法は，健康情報など，プライバシーに関わる情報を用いてサービスを実現する際に，我々の重要なデータを情報漏洩から守ってくれる鍵となる技術です。



◆ 展示内容

今回のオープンキャンパスでは，情報を暗号化したまま様々な情報処理を実現する秘匿演算法に関するふたつのデモを行います。ひとつ目のデモは，データを暗号化したまま特定のキーワードに合致するデータの検索を可能とする検索可能暗号と呼ばれる技術に関するデモです。もうひとつのデモは，複数のグッズを保有している二人が，お互いの保有しているグッズを相手に教えることなく，両者がともに保有しているグッズを明らかにすることを可能とするプライバシー保護型共通集合計算プロトコルと呼ばれる技術に関するデモです。どちらのデモも，クラウド上でデータを持っている人のプライバシーを保護しつつ，特定の処理を実現するのに適した技術になっています。これらの技術の後ろでは，複雑な数学を利用した暗号が活躍しています。数学に興味がある人は，どのようにして暗号化したままの検索や，暗号化したままでの共通集合の計算が可能になっているのか，その仕組みについて積極的に質問して，数学が実世界で非常に役にたつものであることを実感してみると，数学の面白さを改めて感じることができるのではないかと思います。