教員氏名： **櫻井幸一 教授**　　対応する教育課程：C / B

所属：　情報学部門

(1) 研究テーマ

私の研究室では，安全かつ信頼できる情報社会構築のための情報基盤技術を研究している．卒業研究では，暗号やプログラム解析をはじめとする情報セキュリティのための要素技術，また，それらを応用したシステム化技術を取り上げる．

(a) 暗号によるプライバシー保護，不正防止など

暗号を用いた情報の秘匿だけでなく，匿名性の保障，アクセス制御，暗号文検索に加え，電子現金（Bitcoin など）やデジタル著作権管理（DRM）などクラウド化時代における新しいセキュリティ技術を研究している．

(b) 計算機システムの信頼性・安全性確保技術

不正プログラム実行，データベース等アプリケーションシステムへの不正アクセス等，信頼性・安全性確保におけるさまざまな問題が存在している．また，情報家電，携帯端末の高機能化で計算機システムは多様化しており，新たなアプローチが必要である．未知のウイルスにも対抗可能な振る舞い解析，不正ボットプログラムの検知，仮想化技術による OS 内部保護，ネットワークデータ解析による攻撃検知などの研究を行っている．

(c) 不正内部利用者による脅威への対策

計算機システムでは，これまで正当な権利が与えられている利用者による不正はあまり考慮されてこなかった．クラウドコンピューティングの普及により今後はゲーム理論などを応用し，新たな脅威への対策を考えている．

(d) 電子透かし，偽造画像対策

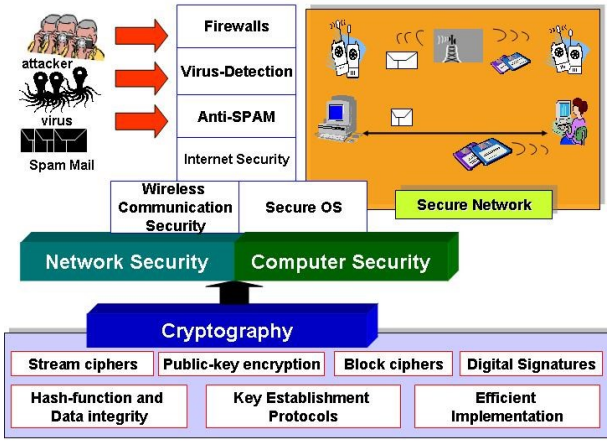
デジタル画像の著作権保護のための電子透かしや偽造画像検出などのマルチメディアセキュリティについて研究している．海賊版の流通防止に必須の技術であり，画像処理や人工知能，機械学習の応用などに興味のある学生は是非挑戦を．

(e) 高速暗号実装技術

GPU と呼ばれるグラフィックス用高速処理装置を暗号実装へ応用することで高速化を図る研究を行っている．また，高速実装技術の暗号解読への応用についても研究を進めている．

(2) 研究室紹介

迷惑電子メール・計算機ウイルス・サービス停止攻撃(DoS 攻撃)の 3 つは, 現在も解決策がなく社会の問題となっており，私の研究室でもこれらの対策が大きな研究課題である．さらに，著作権等の権利保護技術，プライバシー保護技術なども近年重要な課題である．情報セキュリティ以外にも，数論アルゴリズムにも興味を持って研究してきた．研究・ゼミ・学生指導は川本助教と連携して行っている．基礎理論に限定せず，コンピュータやクラウドコンピューティングに興味ある方・プログラム・インターネットが好きな方，大歓迎！！



(3) キーワード

情報セキュリティ，マルチメディアセキュリティ，暗号理論，スパム対策，オペレーティングシステム，ネットワークセキュリティ，クラウドコンピューティング，電子透かし，生体認証，ゲーム理論，仮想化技術

現在行っている研究の内容は，研究室のウェブページで紹介している．

http://itslab.inf.kyushu-u.ac.jp/index-j.html