



## 研究テーマ

## 1 モバイル端末向け個人認証システムの開発

## 2 自動プログラムによる遠隔攻撃の対策に関する研究

## 3 匿名通信システムに関する研究



## 岡崎 直宣

おかざき なおのぶ  
工学教育研究部  
工学科情報通信工学プログラム担当

教授

## キーワード

ネットワークセキュリティ、モバイル端末の安全性向上技術、個人認証技術、CAPTCHA、匿名通信システム、IoT、センサネットワーク

特許情報・  
共同研究・  
応用分野など

## 特許

1. 個人認証装置及びプログラム, 特開2017-45184, 2017.
2. 個人認証用プログラム, 特開2017-58991, 2017.
3. 加速度センサを搭載したモバイル端末を正規の通信相手として認証する方法および認証装置, 特願2018-36579, 2018.
4. ランダムドットパターンCAPTCHAを用いたアクセス認証方法, 特願2018-214929, 2018.

## 研究概要

コンピュータネットワークの高機能化や、安全性に関する研究を行っています。

特に、モバイル端末の機能や利用環境の特性に着目し、安全性と使い易さの両立を目指した個人認証システムの開発を行っています。さらに、ボットと呼ばれる自動プログラムによる遠隔からの各種サービスに対する不正利用を防ぐためのCAPTCHA技術や匿名通信システムに対する指紋攻撃と呼ばれる匿名性を低下させる攻撃の対策技術にも取り組んでいます。

## 1 モバイル端末向け個人認証システムの開発

現在、爆発的に普及しているスマートフォンやタブレットなどのモバイル端末はPCと同等以上の個人情報を持している場合も多くなっています。ところが、パスワード等の入力の手間や、入力動作の覗き見による秘密情報の露呈の問題などがあり、十分な安全対策がされていないのが現状です。

一般に、システムの安全性は利便性とのトレードオフの関係にあり、その両立が課題となっています。本研究では、モバイル端末の有するタッチセンサやカメラなどの特徴的な機能の活用を図りながら、人混みの中や自宅といった利用環境の違いに応じて求められる安全性と利便性のバランスが異なることに着目して、様々な利用環境下で使い易さと安全性とのバランスを動的に保つ方法の開発等により、モバイル端末の安全性を総合的に向上するための研究を行っています。

## 2 自動プログラムによる遠隔攻撃の対策に関する研究

ボットと呼ばれる自動プログラムによる遠隔からの各種サービスに対するアカウントの大量取得などの不正利用を防ぐことを目的とした、人間とボットの動作を区別するための技術(CAPTCHA)が普及してきています。ところが、最近のボットの高性能化により、CAPTCHAに対する攻撃も高度になり、その対策が求められています。本研究では、特に「リレー攻撃」と呼ばれる従来の対策技術では全く防ぐことができない攻撃に耐性を持つ新たな手法の開発に向けた研究を行っています。

## 3 匿名通信システムに関する研究

現在のインターネットでは、通信内容を暗号化により秘匿することが比較的容易となり、一見その安全性が確保されているように感じるかも知れません。しかしながら、「誰が」「どこに」アクセスしたかといった情報は、暗号化だけではその秘密(「通信の匿名性」)を守ることができません。プライバシー保護の観点のみならず、時にはそれが生命の危険をもたらす場合もあることから、その匿名性を守る技術である「匿名通信システム」はますます重要になってきています。ところが最近、「指紋攻撃」と呼ばれる解析技術により、匿名通信システムに対する匿名性を低下させる攻撃が可能であることが示され、その対策技術の開発が望まれています。本研究では、攻撃者に解析のための情報を与えにくくすることにより、指紋攻撃に対してより頑強な匿名通信システムについて研究を行っています。

## ホームページ

## 技術相談に応じられる関連分野

・ネットワークセキュリティ全般、モバイル端末の安全性向上技術、個人認証技術

## メッセージ

上記の他、IoT技術の重要な部分を担うセンサネットワークについて、そこで求められる信頼性や省電力に注力したネットワーク構築技術などの研究を行っています。