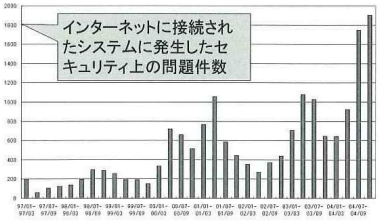
「居心地のよさ・使いやすさ」と「安全」を両立させる情報セキュリティ技術の研究・開発

情報化社会の進展とともに、個人が扱う情報量は増大し、また個人に関する情報の多くがネットワーク上に蓄えられるようになりました。便利な反面、最近では逆に、情報漏えい、データ改ざん、盗聴、詐取など、情報のセキュリティ（安全性）が問題になってきました。

図１に見られるように、ネットワーク上でのセキュリティを脅かす報告が、年々増えてきています。そこで、情報を安全にコントロールすることが必要となります。そのための技術の一つに、耐タンパデバイスを使用する方法があります。耐タンパデバイスとは、タンパ（情報不正取得、改ざん）に対して耐性のあるデバイス（装置、素子）のことです。本研究室では、この耐タンパデバイスであるICカードを技術の核として、より安全で居心地のいい社会を実現するための情報セキュリティ技術の研究開発を行っています。



出展（JPCERT/CC, http://www.jpcert.or.jp）

図１　日本国内における不正アクセス報告件数の年次推移

図２に、本研究室で取り組んでいる研究テーマを示します．本研究室では、耐タンパデバイスの安全性評価、バイオメトリックス個人認証、WEBと連動したセキュリティシステムを３つの柱として、研究開発を進めています。

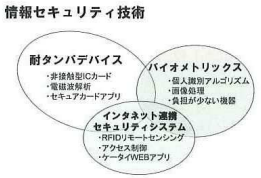


図２　取り組んでいる研究テーマ

ICカードとは

最近のニュースで、キャッシュカードやクレジットカードの磁気ストライプに記録されている個人情報をコピー（スキミング）して、偽カードを作り、本人が知らない間に現金を詐取される事件が多数報告されるようになりました。磁気ストライプを用いたシステムは、情報の書き込みや読み込みを制限することができないため、比較的簡単にカードに蓄えられた情報を操作することができます。そこで、セキュリティ強化のため、銀行やクレジットカード会社は、ICカードの導入を推進しています。このICカードとは、CPUとメモリを搭載した小さなコンピュータのことです。実際、20年位前の初期のパーソナルコンピュータと同等の計算能力を、厚さ0.76mmの１枚のカード内部で実現しています。ICカードがプログラムを処理できるということは、用途に応じてICカードを個別に設定できたり、ICカードと外部の通信やメモリへの書き込みを暗号化できることを意味しています。また、情報を記憶しているメモリも通常のパソコンや 携帯電話のメモリと構造が違い、外部からの解析で簡単にデータが読み出せない特殊な構造をしています。つまり、ICカードは、安全な情報保管庫といえます。ICカードには、図３に示すように、金色の電極端子が表面に露出している接触型と、アンテナをカードの中に内蔵し、電波で通信を行う非接触型の２つのタイプがあります。今後は、JRで使われている乗車券（スイカ）や携帯電話に搭載された非接触型ICカードが急速に普及すると予想されています。

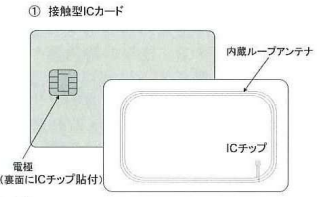


図３　ICカードの種類
①と②の機能を同時に持つコンビ型ICカードもある

ICカードを用いたセキュリティ技術

本研究室では、この非接触型ICカードや個人の身体的特徴を用いて個人を機器が特定する方法（バイオメトリックス）を用いて、誰もが安全に暮らすことができる社会基盤の構築を目指して研究開発を行っています。次に、研究室で取り組んでいるテーマについて説明します。

プロフィール　靏　浩二（つる こうじ）
国立高等専門学校機構 大分工業高等専門学校 制御情報工学科 助教授
昭和38年：福岡県福岡市生まれ。
63年：九州大学大学院総合理工学研究科情報システム学専攻修了後、日本電信電話株式会社（NTT）研究開発技術本部電子応用研究所勤務
平成16年：大分工業高等専門学校に勤務。現在に至る。

①　耐タンパデバイスである非接触ICカードの安全性検証技術

近年、安全だと思われていたICカードにおいても、信号入出力の際のわずかな漏洩信号を統計的に解析して、ICカードに蓄えられている情報（暗号鍵）を突き止めたり、電子線やレーザーをICチップに照射して、わざと誤動作させて内部の情報を読み取るなど、図４に示すよう様々な解析が試みられるようになってきました。本研究室では、そのような解析手法の中で、非接触型ICカードにおいて最も危険度の高いと考えられている差分電磁波解析（DEMA）に対する安全性検証技術の開発を行っています。また、非接触型ICカードにおける安全性の高いソフトウェア開発方法や、図５に示すような通信エリア測定を行うことにより、通信距離を拡大する方法についての検討も行っています。

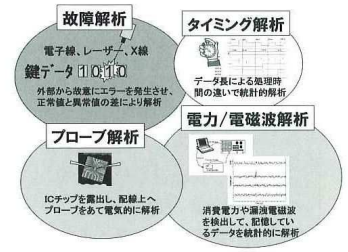


図４　ICカードに対する不正解析技術

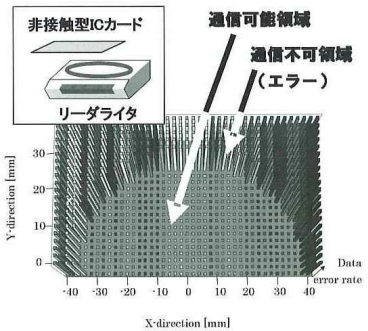


図５　非接触型ICカードの通信エリア測定

②　「居心地のよさ」と「セキュリティ」を両立させるバイオメトリックス（生体認証）技術の開発

テロや犯罪の多発により、空港や重要施設に生体認証システムの導入が拡大しています。個人を識別できる高い精度を求めるバイオメトリックスの方法としては、虹彩や指紋を用いる方法が実現されています。しかし、これらの認証方法は専用の装置に体の一部を押し当てたり、覗き込むなど、利用者に特定の行動を強制する側面があります。本研究室では、個人認証率はさほど高くなくとも、人間の自然な行動、例えばドアの開け方や歩き方、しぐさの癖などから、決められたエリア内で、個人を何度かフィルタリングすることにより、セキュリティを保つ方法の研究を行っています。安全と居心地のよさを同時に達成できるセキュリティシステムの開発を目指しています。

③　インターネットと連動したRFIDシステムの開発

RFID（非接触型タグ）は、ICカードのような計算機能は持っていませんが、電波による呼びかけに対して、タグが持っている識別データ（ID）を電波で返してきます。これも、ICカードと同じように電池が不要です。このRFIDをいろいろな物品につけて、物品調査や物流管理用として研究開発が進められてきました。RFIDは、単にバーコードに代わる商品識別としてだけではなく、現実世界とネットワーク空間に広がる仮想世界をつなぐキーデバイスとして期待されています。本研究室では、このRFIDを用いて、広い建物内での所在確認など、インターネットと連動したリモートセンシングシステムの開発を目指しています。また、大分県工業団体連合会（産学官交流企画調整会議）が行っているトレーサビリティ研究会（代表幹事：川辺正行氏）にも参加しています。

今回ご紹介したICカードやバイオメトリックスなど、情報セキュリティ技術に興味をお持ちの方は、靏研究室までご連絡ください。また、研究室の訪問や見学も歓迎します。今後は、企業など外部機関の方々と連携をとりながら、研究領域を広げていきたいと考えています。

Email　tsuru@oita-ct.ac.jp
ＵＲＬ　www.oita-ct.ac.jp/w3seigyo/tsuru_hp