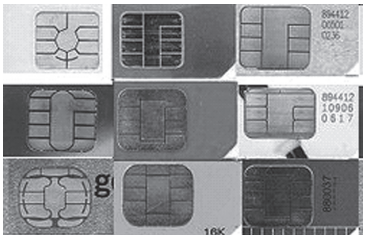
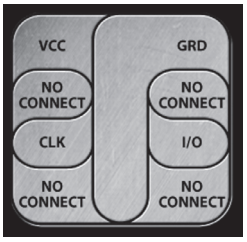
マイクロチップの秘密を 盗み出す技術・守る技術

磁気ストライプカードの時代が徐々に終わり、Suica、ICOCA、Edy、nanako、WaONなど、ICカードが広範に普及してきました。ICカードは一種の電子マネーであり、偽造の可能性があります。ICカードは一種のコンピュータで、内部では暗号の処理を行っています。その鍵をハードウェアの特性を利用して取り出す攻撃技術が登場し、業界で大きな脅威となっています。本講演では、磁気ストライプカードの危険性、ICカードの仕組み、暗号の仕組みなどを解説するとともに、最新の攻撃技術、攻撃に対する耐性の評価技術を紹介します。特に、チップを強制的に誤動作させ、誤った出力をさせ、その出力結果と正常な処理結果との比較によって内部情報を取り出す差分誤動作解析（=DFA：Differential Fault Analysis）について詳しく紹介します。DFAに関してはBellcoreの研究者が1997年のEUROCRYPTでその基本的な手法を発表して以来、膨大な理論的検討がなされています。しかし、公表されている実験的検討は数少なく、誤動作の詳細については未知の状態が続いていました。最近になって、講演者を含むいくつかの研究グループが強制誤動作は必ずしもランダムエラーを引き起こすわけではないことを実験的に明らかにしつつあります。本講演では、これらの実験結果を紹介し、「強制誤動作とは何か」という問題を考察します。



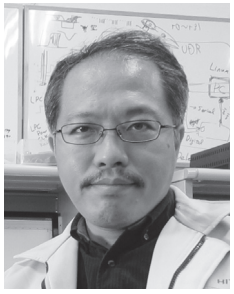


2012年1月30日（月）16:30～18:00

慶應義塾大学日吉キャンパス　来往舎1階シンポジウムスペース

参加費：無料（学生の来場歓迎）

会場準備の都合上、塾外の方は事前申し込みをお願いいたします



講師：**神永　正博** 氏

◇東北学院大学工学部電気情報工学科教授

1991年東京理科大学理学部数学科卒業、1994年京都大学大学院理学研究科数学専攻博士課程中退、2003年 博士（理学）（大阪大学）。1994年東京電機大学助手、1998年日立製作所中央研究所研究員、2004年東北学院大学工学部講師、2005年助教授（准教授）を経て、2011年より同教授。専門はシュレーディンガー作用素論及びハードウェアセキュリティ。著書に『カードセキュリティのすべて』（日本実業出版）、『不透明な時代を見抜く「統計思考力」』（ディスカヴァー）、『ウソを見破る統計学』（講談社ブルーバックス）など。

REC for NS
research and education center for natural sciences

慶應義塾大学　自然科学研究教育センター事務局（日吉キャンパス来往舎1階）
〒223-8521 横浜市港北区日吉 4-1-1　Tel：045-566-1111　URL：http://www.sci.keio.ac.jp/