喜安記念業績賞受賞に寄せて

受賞業績　**サイドチャンネル攻撃対策技術の開発と実用化**

鳥居 直哉 [*1]　伊藤 孝一 [*1]　武仲 正彦 [*1]　伊豆 哲也 [*2]　高崎 裕美子 [*3]

[*1] (株) 富士通研究所セキュアコンピューティング研究部
[*2] FUJITSU Laboratories of Europe Limited Intelligent Society Platform Research Division
[*3] 富士通セミコンダクター (株) プロダクトデベロップメント部

このたびは，喜安記念業績賞という大変栄誉な賞を受賞でき，光栄に思う．研究活動から ISO/IEC 15408 EAL4+ 取得のための事務活動に至るまで，さまざまな苦労を十年以上繰り返した上での受賞であり，喜びもひとしおである．

受賞対象となった業績は，電子マネーで使われる IC カード技術を支えるセキュリティ技術である．IC カードは，スキミングの脅威にさらされていた磁気カードに代わる決済手段として注目されており，チップを分解しないと内部の暗号鍵を得ることができないため安全と考えられていた．しかし，1998 年に，チップを分解せずに消費電力から暗号鍵を解読する「サイドチャネル攻撃」が知られるようになった．この攻撃に対する安全性評価基準を確立，FeliCa チップ製品として広く実用化を行ったことが評価され，受賞に至った．

最初に苦労したのが，当時多くの解読成功研究結果が発表されたにもかかわらず，どんな IC カードに対しどんな実験を行ったかという実験条件が公開されていなかったことである．論文の実験室の様子を写した写真から細かい実験条件を読み取る，等の試行錯誤を繰り返した結果，日本で初めてサイドチャネル攻撃実験に成功することができた．

次の問題は攻撃を防ぐための対策法開発であった．どんなチップに対しても安全な対策法が求められたが，すべてのチップに対し対策評価実験を行うのは不可能であった．そこで，チップ種類に関係なく，シグナル成分を理論的に評価する安全性評価基準を世界に先駆けて開発，この基準を用いて開発した FeliCa チップは，セキュリティの国際標準 ISO/IEC 15408 のレベル EAL4+ という，民生品としては最高レベルの安全性を第三者認定されるに至った．これらの研究成果は，サイドチャネル攻撃分野における世界最高レベルの国際会議 CHES (Cryptographic Hardware and Embedded System) で発表され，世界中から大きな注目を集めた．

苦労も多かったが，安全な FeliCa チップを日本中に普及するという夢があったため，研究を続けることができた．受賞にあたり，多大なるアドバイスをくださった先生方や研究者の皆様に深く感謝を申し上げるとともに，研究の進め方や製品化のアドバイス，叱咤激励をいただいた共同受賞者の皆様，および同僚・先輩・後輩の皆様に厚く御礼を申し上げます．

(2014 年 5 月 15 日受付)

鳥居 直哉 (正会員)　torii.naoya@jp.fujitsu.com
1983 年阪大大学院工学研究科通信工学専攻・博士前期課程修了．同年 (株) 富士通研究所に勤務，現在，セキュアコンピューティング研究部部長．

伊藤 孝一　ito.kouichi@jp.fujitsu.com
2009 年東工大イノベーションマネジメント研究科・博士後期課程修了．博士 (工学)．1997 年 (株) 富士通研究所入社．現在，セキュアコンピューティング研究部主任研究員．

武仲 正彦　ma@jp.fujitsu.com
2009 年筑波大・システム情報工学研究科・博士後期課程修了．博士 (工学)．1992 年 (株) 富士通研究所入社．現在，セキュアコンピューティング研究部主管研究員．

伊豆 哲也 (正会員)　izu@jp.fujitsu.com
2007 年電通大・情報理工学研究科・博士後期課程修了．博士 (工学)．1997 年 (株) 富士通研究所に勤務．現在，欧州富士通研究所インテリジェントソサイエティプラットフォーム研究部マネージャ．

高崎 裕美子　takasaki.yumiko@jp.fujitsu.com
1999 年お茶の水女子大・大学院人間文化研究科・博士前期課程修了，同年富士通 (株) 入社．現在，富士通セミコンダクター (株) プロダクトデベロップメント部プロジェクト課長．