環境調和型セキュア情報システム研究室　1

1）当該研究室の研究成果について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

2）当該研究室構成員の学会活動について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

3）当該研究室構成員の社会貢献について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

4）当該研究室の競争的資金の獲得状況について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

5）国際共同研究・連携研究・連携教育活動の実績について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

6）共同利用・共同研究拠点活動の実績について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

特になし

7）その他、総合的なコメント

環境調和型セキュア情報システム研究室では、「セキュリティシステムの設計と検証」、「暗号コンピューティング」、「電磁情報セキュリティ」を研究のコアとし、安心・安全の基盤となるハードウェアセキュリティ技術の発展に大きく寄与している。本研究室の成果は学術分野に留まらず、企業との共同研究、特許出願などを通じて産業界にも寄与すると共に、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト（CRYPTREC，総務省（NICT），経産省（IPA）の合同プロジェクト）において、電子政府が推奨する暗号技術ガイドラインの策定に主査として関わり、「官」への貢献も少なくない。当該研究室の特筆すべき成果としては、ハードウェアセキュリティのトップカンファレンスである Cryptographic Hardware and Embedded Systems（CHES）に継続して論文が採択されていることが挙げられる。また、2014 年には同会議で最優秀論文賞を授与されていると共に、本間尚文教授は CHES において日本人唯一の Steering Committee も務めており、国際的にもハードウェアセキュリティ分野の中心にある研究室であると言える。今後も国内外のハードウェアセキュリティ研究分野を牽引していくことを期待する。

環境調和型セキュア情報システム研究室　2

1）当該研究室の研究成果について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

暗号技術を中心とした次世代の情報セキュリティ技術に関して、デバイス、システム、アプリケーションを横断する幅広いトピックスの研究に取り組んでいる。国際的な認知が高く、また難易度の高い学術論文誌および国際会議を選んで研究成果を報告している。「セキュリティシステムの設計と検証に関する研究」は理論研究に軸足を置きつつ、その具象として高次・多入出力ガロア体演算集積回路の設計法を導出している。長期的な研究トピックスであるが、腰を据えて取組んだ研究成果を着実に報告し、世界的な認知を得ている。「暗号コンピューティングに関する研究」と「電磁情報セキュリティに関する研究」では、国際的かつ学際的な連携研究のもと、時宜を得た最先端の研究成果を継続的に発信している。いずれの研究課題も世界的にトップの研究成果が創出されていると認められる。三年間(2016 ～ 2018)に学術論文 14 件、原著論文と同等に扱う査読付き国際会議発表論文 5 件、および査読付き国際会議 16 件と豊富な学術論文の刊行実績が示されている。これらの研究活動の全般について、第 14 回日本学術会賞、第 50 回市村学術賞貢献賞、German Innovation Award Gottfried Wagener Prize 2018、等を受賞しており、客観的な指標からも秀逸な研究成果であることが判断できる。

2）当該研究室構成員の学会活動について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

情報セキュリティ技術に関連する国内および海外の学術学会において主要な役割を担っている。とりわけ、ハードウェアセキュリティ分野で世界最高峰に位置付けられる International Workshop on Cryptographic Hardware and Embedded Systems（CHES）2017 のプログラム委員長を務めた実績が評価できる。当該分野は欧州にリーダーシップの重心が置かれている状況であるが、当該研究室の代表教員が学術面およびコミュニティ面で強力な牽引力を発揮することにより、世界から信頼されていることの証左である。国内学会においても研究会専門委員として活動しており、若い世代のリーダーとして頭角を現している。

3）当該研究室構成員の社会貢献について

(*) Excellent（) Very Good（) Good　() Fair（) Poor

情報セキュリティ技術に関連して顕著な社会貢献が認められる。教育活動においては、文部科学省「分野・地域を超えた実践的情報教育協働ネットワーク（enPiT)」においてハードウェアセキュリティ分野の専門教育プログラムを創出し、参加大学の多くの学生に実践しており、プログラム修了者の満足度も高い。国における活動として、総務省・経済産業省の下で暗号技術分野の運用方針を定め、あるいは新規技術の動向を見極めるべく、CRYPTREC 暗号技術評価委員会等の委員を継続し、また軽量暗号ワーキングの主査を務めている。この他、日本学術振興会、情報通信研究機構、産業技術総合研究所、情報処理推進機構、等における専門家としての委員会活動に貢献している。これらのことから、当該分野の社会的なリーダーとして積極的に活動していると判断できる。

4）当該研究室の競争的資金の獲得状況について

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

情報セキュリティ技術に関連する競争的研究資金を数多く獲得している。とりわけ、本評価期間において、科学研究費補助金・基盤研究（A）の研究代表者として、ガロア体算術演算に関連した研究課題が連続して採択されていることは特筆すべきと考える。研究室構成員が継続して科学研究費補助金を獲得している。また、受託研究費においても、企業との共同研究や財団による研究助成の研究代表者、および関連省庁による国家プロジェクトの分担研究者として研究費を獲得している。さらに、研究室に最近着任した若い教員は JST さきがけ制度の研究代表者として採択されている。このように、研究室の学術活動を積極的に推進するための資金を獲得していると判断できる。

5）国際共同研究・連携研究・連携教育活動の実績について

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

情報セキュリティ技術分野で世界的に存在感を知らしめている Telcom ParisTech や Katholieke Universiteit Leuven 等の研究チームと国際共同研究を継続している。双方の代表研究者および研究員や学生の相互訪問による共同研究の実践も活発であり、国際共著論文の刊行につながっている。国内においても、横浜国立大学、奈良先端大学院大学、NTT、三菱電機、産総研、等の情報セキュリティ研究分野の拠点組織と密接に連携し、競争的研究資金による受託共同研究や enPiT 等による受託教育活動を展開している。国際共同研究・連携研究・連携教育活動について幅広い実績を有していると考える。

6）共同利用・共同研究拠点活動の実績について

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

前項（5）に記載した国際連携や国内連携において電気通信研究所の共同利用・共同研究拠点活動の制度を活用している。具体的には、Telcom ParisTech や KU Leuven の教員を招聘した研究教育プログラムを実施し、国内連携機関の研究者や学生と交流する機会としている。また、同制度による国内研究者との連携から、共同の研究発表や研究提案が行われている。このように、共同利用・共同研究拠点活動について実質的かつ実効的な活動実績を有すると判断できる。

7）その他、総合的なコメント

新進気鋭の若手研究者が主宰する精力的な研究室として、とりわけハードウェアセキュリティを中心とした情報セキュリティ分野における世界的な学術活動に期待が持てる。学術研究拠点としての電気通信研究所を牽引し、新規の研究開発分野開拓と若い研究者の継続的育成を担うことが強く期待される。

環境調和型セキュア情報システム研究室　3

1. How would you evaluate the research activities in this period?

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

The level of production is remarkable. The most recognized journals and workshops are targeted with great success. The research activities are split into two main topics: cryptographic computing and electromagnetic information security, where the team produced pioneering research results in both domains.

2. How would you evaluate the activities of the members in the laboratory for the academic societies?

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

Prof. Homma is one of the leading international researchers in the field of Hardware Security. This is evidenced by his numerous invited talks and his contribution at international level, notably for the CHES conference which is the most recognized in the domain of Hardware security, but also CARDIS and PROOFS workshops. The assistant Professor Rei Ueno is a proficient researcher which is now a security expert for optimizing the cryptographic implementations.

3. How would you evaluate the contribution of the laboratory to society?

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

The main research topics, cryptographic computing and electromagnetic information security presents a great societal interest where the laboratory highly contributed. Indeed the cryptographic implementations are used in all our pervasive digital connected devices, and the understanding of electromagnetic emanations is fundamental in order to improve the privacy of the users.

The scientific results of the team greatly enhanced the security against physical attacks, the complexity to reduce the implementation cost, the privacy/confidentiality of secret data stored in digital devices.

4. How would you evaluate the lab's level of funding?

( ) Excellent (*) Very Good ( ) Good ( ) Fair ( ) Poor

This strategic research field would deserve more researchers as the Hardware security represents a vast topic with the emergence of IoTs, autonomous cars and other smart connected systems.

5. How would you evaluate the lab's collaborative research, including international joint research and collaborative education?

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

The team has strong international collaborations with Telecom ParisTech in France, and KUL in Belgium. There were many visits for long periods in Europe and many european visitors came to RIEC, thus allowing to maintain a high level of collaborative research.

6. RIEC is one of Japan's "Joint usage/Research Center" or "Nation-wide Cooperative Research Projects" institutes. How would you evaluate the achievements of work done under this framework?

(*) Excellent ( ) Very Good ( ) Good ( ) Fair ( ) Poor

The collaboration with other Japonese laboratories is very fruitful, as evidenced by the numerous publications in domestic conferences. The closer collaboration with NAIST and Kobe University allows to leverage the collaborations at international level and target high ranked papers and conferences.

7. Additional or overall comments

Overall, the laboratory has an impressive scientific production per researcher, and is internationally recognised. The collaboration with other Japonese labs is also excellent. This proves the dynamism and the research quality of the team. The strategic topic of Hardware security could even be leveraged by an increase of researchers to take advantage of the team's international recognition and the emergence of novel applications, as IoT and connected cars, and new technologies .