国際科学技術協力基盤整備事業
日本－台湾研究交流
終了報告書

1. 研究課題名:「偽造困難なデバイスを用いた IoT セキュリティ管理システム」
2. 研究期間:2015 年 4 月～2018 年 3 月
3. 主な参加研究者名:

日本側チーム

	氏名	役職	所属	研究分担
研究代表者	田中 良夫	研究部門長	産業技術総合研究所・情報技術研究部門	WP1/2 全体の取りまとめ、台湾側との調整
研究参加者	古原　和邦	総括研究主幹	産業技術総合研究所・情報技術研究部門	WP1/2 全体の取りまとめ補助、台湾側との調整補助
研究参加者	須崎　有康	主任研究員	産業技術総合研究所・情報技術研究部門	WP1 のとりまとめ、IoT プラットフォーム完全性検証技術開発および解析用セキュリティデータの取得・研究
研究参加者	小方　一郎	主任研究員	産業技術総合研究所・情報技術研究部門	IoT デバイスの完全性検証に関する研究、解析用セキュリティデータの取得・研究
研究参加者	辛　星漢	主任研究員	産業技術総合研究所・情報技術研究部門	WP2 のとりまとめ、方式の提案/仕様策定、方式の安全性/特性評価
研究参加者	堀　洋平	主任研究員	産業技術総合研究所 ナノエレクトロニクス部門	方式の安全性/特性評価、偽造困難性解析用データの取得
研究期間中の全参加研究者数　　8名				

相手側チーム

	氏名	役職	所属	研究分担
研究代表者	Weicheng Huang	Research Fellow	NCHC・NARL	WP1/2 全体の取りまとめ、日本側との調整
主たる共同研究者	Yi-Lang Tsai	Associate Research Fellow	NCHC・NARL	WP1/2全体の取りまとめ補助、セキュリティ研究とアーキテクチャ
主たる共同研究者	Steven Hsiao	Research Fellow	NCHC・NARL	WP1、ビッグデータシステムとソフトウェアの展開
研究参加者	Bo-Yi Lee	Assistant Engineer	NCHC・NARL	WP1/2、セキュリティシステム実装、監視、分析

研究参加者	Jimmy Chung	Associate Research Fellow	NCHC・NARL	WP1、ビッグデータプラットフォーム配置と管理
研究参加者	Wei-Yu Chen	Associate Research Fellow	NCHC・NARL	WP2、セキュリティ研究と実装
研究期間中の全参加研究者数			10名	

4. 研究交流の概要

IoTデバイスの状態を管理・把握しながらからセキュアにデータを取得・検証する方法について、基礎理論から応用研究や実用化手法に至るまでの研究を、日本側は主にセキュリティ基盤技術、台湾側のチームは応用技術を中心にお互いの視点やノウハウを交換しながら共同研究を実施し、学会発表や招待講演、研究ネットワークの拡充、相手国および海外でのプレゼンスの向上、海外との新プロジェクトの提案や採択、国際標準の成立などにも繋がった。

5. 研究交流の成果

5－1 共同研究の研究・開発成果

基礎理論研究の成果については論文誌への採択、応用研究の成果については国際会議のプロシーティングス、招待講演、および今後の実用化に向けた民間との連携・展開などに繋がった。

5－2 国際連携による相乗効果

日本側のチームが得意とする認証鍵共有方式やシステム監視などのセキュリティ基盤技術を、台湾側のチームが得意とするセキュリティ応用技術とを有機的に組み合わせることにより、単一国では着想しえなかった双方の視点で最適な研究開発環境を整えることができ、また、その環境を活用して相互補完的に研究に取り組むことにより新たな視点での研究開発の促進と研究ネットワークの拡充、相手国および海外でのプレゼンスの向上を行うことができ、お互いに有益な相乗効果を得られた。

5－3 共同研究成果から期待される波及効果および進展

本共同研究の成果であるセキュアなブートローダなどに関して国内外の複数の会社が関心を示しており、実システムへの適用の検討や共同での応用プロジェクト提案を行っていると共に、本共同研究の基盤で我々の提案技術である AugPAKE が ISO/IEC 11770-4:2017 において国際標準化されるなど共同研究の範囲を超えた波及効果が出始めている。

5－4 研究交流の有効性・継続性（研究交流を通じた人材育成、協働関係の継続・発展性）

本研究交流事業を通して、組織文化や価値観、論理的思考の異なる海外メンバーと共に議論やブレインストーミングする能力や、それらを通してプロジェクトを遂行する能力の向上に繋がり、結果として海外との新プロジェクトの提案や採

択、国際標準化の場での粘り強い議論や交渉・調整能力の向上、およびその結果としての国際標準の成立などにも繋がった。

Infrastructure Development for Promoting International S&T Cooperation
Japan－Taiwan Joint Research Exchange Program
Executive Summary of Final Report

1. Project Title:「IoT Security Management System with Unclonable Devices」
2. Project Period:April, 2015 ～ March, 2018
3. Main Participants:

Japan-side

	Name	Title	Affiliation	Role
PI	Yoshio Tanaka	Director	AIST・ITRI	WP1/2, Project management and arrangement with Taiwanese team
Collaborator	Kazukuni Kobara	Principal Research Manager	AIST・ITRI	WP1/2, Helping of project management and arrangement with Taiwan team, IoT platform and its data integrity
Collaborator	Kuniyasu Suzaki	Senior Research Scientist	AIST・ITRI	WP1 management, IoT platform and its data integrity
Collaborator	Ichiro Ogata	Senior Research Scientist	AIST・ITRI	IoT platform and its data integrity
Collaborator	SeongHan Shin	Senior Research Scientist	AIST・ITRI	WP2 management, scheme proposal and evaluation
Collaborator	Yohei Hori	Senior Research Scientist	AIST・Nanoelectronics RI	Evaluation of unclonability and necessary data acquisition
Total number of participating researchers in the project: 8				

Partner-side

	Name	Title	Affiliation	Role
PI	Weicheng Huang	Research Fellow	NCHC・NARL	WP1/2, Project management and arrangement with Japanese team
Co-PI	Yi-Lang Tsai	Associate Research Fellow	NCHC・NARL	WP1/2, Helping project management, security research and architecture
Collaborator	Steven Hsiao	Research Fellow	NCHC・NARL	WP1, Big Data system deployment software development
Collaborator	Bo-Yi Lee	Assistant Engineer	NCHC・NARL	WP1/2, Security system implementation, monitor and analysis
Collaborator	Jimmy Chung	Associate Research Fellow	NCHC・NARL	WP1, Big Data platform deployment and management

Collaborator	Wei-Yu Chen	Associate Research Fellow	NCHC・NARL	WP2, Security research and implementation
Total number of participating researchers in the project: 10 Number				

4. Scope of the joint project

On the method of securely acquiring and verifying significant data from IoT devices while managing the status of them to integrate with Big Data Analysis platform, the joint team has conducted collaborative research both from security fundamentals by the Japanese team and from application by the Taiwan team. The project succeeded in publication of research results, expansion of research network with invited talks, improvement of presence in partner country and overseas by proposing and acceptance of new projects with overseas, and with establishment of international standards.

5. Outcomes of the joint project

5－1 Intellectual Merit

The results of fundamental or theoretical researches were published in international journals. The results of applied research were presented in international conferences or as invited talks, and then succeeded in further collaboration with private sectors toward applied researches.

5－2 Synergy from the Collaboration

Without combination of both teams' strength and viewpoints, we could not construct optimal research environment that could not be conceived by any single county. The synergy from the collaboration succeeded in expansion of research network and presence in overseas, and then triggered the further international collaboration project to come.

5－3 Potential Impacts on Society

Several companies are interested in the research results on our secure boot loader, and under discussion to make them practical use. A part of the discussion brought a proposal and submission of a joint project with EU. Another technology component, AugPAKE has been internationally standardized in ISO / IEC 11770-4: 2017. As these tell us, impacts beyond the scope of collaborative research have been starting to appear in society.

5－4 Effectiveness and Continuity of Exchange
(Human Resource Cultivation, Development and Sustainability of the Cooperation, etc.)

Throughout this project, we have been able to improve the skills to discuss and brainstorm together with overseas members with different organizational culture, values and logical thinking, and the ability to carry out the project with them. These improved skills and ability result in the proposal and launch of a new project with overseas, and the great help in tough discussion and negotiation in standardization of our technologies in ISO/IEC 11770-4.

共同研究における主要な研究成果リスト

1. 論文発表等

＊原著論文（相手側研究チームとの共著論文）

＊査読有り

1. SeongHan Shin, Kazukuni Kobara, Chia-Chuan Chuang, Weicheng Huang, "A Security Framework for MQTT," In Proc. of the 2016 IEEE International Workshop on Cyber-Physical Systems Security (CPS-Sec), IEEE, October 2016

＊原著論文（相手側研究チームを含まない日本側研究チームの論文）

1. SeongHan Shin, Kazukuni Kobara, Hideki Imai, "On Finding Secure Domain Parameters Resistant to Cheon's Algorithm," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E98-A, No. 12, pp. 2456-2470, December 2015, 10.1587/transfun.E98.A.2456
2. SeongHan Shin, Kazukuni Kobara, "Key Establishment Using Physically Unclonable Functions," In Proc. of the 2015 International Symposium on Internet of Things & Internet of Everything (CSCI-ISOT), pp. 352-355, December 2015
3. Kazukuni Kobara, "Cyber Physical Security for Industrial Control Systems and IoT," IEICE Trans. on Information and Systems, Invited Paper, Vol. E99-D, No. 4, pp. 787-795, April 2016
4. SeongHan Shin, Kazukuni Kobara, "A Secure Anonymous Password-based Authentication Protocol with Control of Authentication Numbers," In Proc. of the 2016 International Symposium on Information Theory and its Applications (ISITA2016), pp. 330-334, November 2016
5. SeongHan Shin, Kazukuni Kobara, "Simple Anonymous Password-Based Authenticated Key Exchange (SAPAKE), Reconsidered," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E100-A, No. 2, pp. 639-652, February 2017
6. SeongHan Shin, Kazukuni Kobara, "A Secure MQTT Framework from PUF-based Key Establishment," In Proc. of the 2017 International Symposium on Internet of Things & Internet of Everything (CSCI-ISOT 2017), pp. 1296-1301, December 2017
7. SeongHan Shin, Kazukuni Kobara, "How to Preserve User Anonymity in Password-Based Anonymous Authentication Scheme," IEICE Trans. on Information and Systems, Vol. E101-D, No. 3, pp. 803-807, March 2018

2. 学会発表

＊口頭発表（相手側研究チームとの連名発表）

発表件数：1 件（招待講演：0 件）

＊口頭発表（相手側研究チームを含まない日本側研究チームの発表）
　　発表件数：5 件（招待講演：2 件）

＊ポスター発表（相手側研究チームとの連名発表）
　　発表件数：2 件

＊ポスター発表（相手側研究チームを含まない日本側研究チームの発表）
　　発表件数：1 件

3. 主催したワークショップ・セミナー・シンポジウム等の開催
1. Workshop on IoT Security、主催者：Weicheng Huang（NCHC・Research Fellow）/田中良夫（産総研・部門長）、National Center for High-Performance Computing（新竹、台湾）、2016 年 3 月 14 日、参加人数 20 名程
2. Joint Workshop of AIST & NCHC for the International Collaboration Project、主催者：Weicheng Huang（NCHC・Research Fellow）/田中良夫（産総研・部門長）、National Center for High-Performance Computing（新竹、台湾）、2018 年 2 月 6 日～8 日、参加人数 20 名程

4. 研究交流の実績
【合同ミーティング】
- 2015 年 4 月 7 日：キックオフミーティング、産業技術総合研究所つくばセンター本部情報棟会議室、つくば、日本
- 2015 年 6 月 1 日：進捗確認ミーティング、NCHC 会議室、新竹、日本
- 2016 年 3 月 11 日：進捗確認ミーティング、NCHC 会議室、新竹、日本
- 2016 年 6 月 6 日：進捗確認ミーティング、産業技術総合研究所臨海副都心センター会議室、東京、日本
- 2016 年 11 月 7 日：進捗確認ミーティング、産業技術総合研究所臨海副都心センター会議室、東京、日本
- 2017 年 3 月 14 日：進捗確認ミーティング、NCHC 会議室、新竹、日本
- 2017 年 11 月 21 日：進捗確認ミーティング、産業技術総合研究所臨海副都心センター会議室、東京、日本
- 2018 年 2 月 8 日：最終確認ミーティング、NCHC 会議室、新竹、日本

5. 特許出願
　　研究期間累積出願件数：0 件

6. 受賞・新聞報道等

7. その他
　以下の MOST/JST 合同ワークショップにおいて、ローカルホストを務めるなどの貢献を行った。
- Taiwan-Japan Workshop on "Security and Dependability Technologies for IoT Devices"、主催者：MOST/JST、2017 年 4 月 17 日、参加人数 32 名