# 内容の要旨

| 報告番号 | 甲　第4361号 | 氏　名 | 豊田　健太郎 |
|---|---|---|---|

主論文題目：

A Study on Security and Privacy for Ad-hoc Network, VoIP Service and RFID-enabled Supply Chains System

（アドホックネットワーク，VoIPサービス，およびRFIDサプライチェーンシステムにおけるセキュリティとプライバシに関する研究）


パーソナルコンピュータや携帯電話によるインターネットの利用者増大に伴い，ネットワークを介した様々な攻撃が問題となっている．これまで，これらの攻撃を防止するために共通鍵および公開鍵暗号方式，認証，デジタル署名技術などのセキュリティ技術が確立されてきた．一方，無線センサデバイス，スマートフォン，RFID (Radio Frequency Identification)といった多様な無線通信可能なデバイスの技術的進歩に伴い，我々の生活をより豊かにするような新しいシステムおよびサービスが急速に普及し始めている．しかしながら，これらのデバイスを用いたシステムやサービスには，アドホックネットワークにおいて信頼できる第三者機関を用いた認証ができないこと，VoIPサービスでは格安な通話料金を悪用した迷惑電話を発信する行為，RFIDに書き込まれた情報の不正読取によるプライバシ侵害などといった既存のセキュリティ技術だけでは対処できない問題が存在する．したがって，これらに対する対策および防御策を講じることは喫緊の課題となっている．

本論文では，より安全・安心なシステムおよびサービスの実現に向け，アドホックネットワークにおける認証，VoIPサービス，およびRFIDサプライチェーンシステムにおけるセキュリティおよびプライバシ保護手法を提案し，理論計算，計算機シミュレーションおよび実験によりその有効性を示す．本論文の構成を以下に示す．

第1章では，無線センサデバイス，スマートフォン，RFIDを用いたシステムおよびサービス，またそれらに対する脅威および対策について概観し，本研究の目的および位置付けを明確にする．

第2章では，無線センサデバイスおよびスマートフォンがアドホックネットワークにおいて，端末間通信のひとつであるFFS (Feige-Fiat-Shamir) プロトコルの演算量を低減する方法として，認証における検証時に1,024ビットの変数の乗算が演算の負荷となっていることに着目し，乗算回数を低減しつつも，従来求められている安全性を確保する方式を提案する．そして安全性証明，理論計算およびAndroidデバイスを用いた実測により，計算時間を低減可能であることを示す．

第3章では，IP電話を始めとする音声通話サービスにおいて，複数の通話に関する特徴量を基に，発信者を2つのクラスタに分類することで学習を必要としない迷惑電話発信者手法を提案する．そして実通話データセットおよび生成したデータセットを用いたシミュレーションにより本方式の有効性を示す．

第4章では，RFIDを用いた物流管理システムにおいてタグに書き込まれた製品情報 (EPC: Electronic Product Code)を漏洩させることなく商品を配送する方法として，タグのEPCに乱数をマスクした上でその乱数を認証サーバに置き，認証が成功した場合に正しいEPCを復元できる仕組みを提案する．提案方式では認証に必要な情報を閾値秘密分散法により商品のタグに書き込んだ上で，ダミーの情報を付加したタグを一緒に配送することで安全な認証情報の配送を可能とする．そして安全性証明，理論計算および市販されているRFIDデバイスを用いた実験により有効性を示す．

第5章は，結論であり，本論文の内容および今後の課題を総括している．

# 論文審査の要旨

| 報告番号 | 甲　第 4361 号 | 氏　名 | 豊田 健太郎 |
|---|---|---|---|

| 論文審査担当者： | | | | |
|---|---|---|---|---|
| | 主査 | 慶應義塾大学教授 | 工学博士 | 笹瀬　巌 |
| | 副査 | 慶應義塾大学教授 | 工学博士 | 山中　直明 |
| | | 慶應義塾大学教授 | 博士(工学) | 大槻　知明 |
| | | 慶應義塾大学教授 | 博士(工学) | 眞田　幸俊 |
| | | アテネ大学教授 | Ph.D. | MATHIOPOULOS　Panagiotis |

工学士、修士（工学)、豊田健太郎君提出の学位請求論文は、「A Study on Security and Privacy for Ad-hoc Network, VoIP Service and RFID-enabled Supply Chains System　(アドホックネットワーク、VoIP サービス、および RFID サプライチェーンシステムにおけるセキュリティとプライバシに関する研究)」と題し、全 5 章から構成される。

パーソナルコンピュータや携帯電話によるインターネット接続の普及に伴い、ネットワークを介した様々な攻撃を防止するために、共通鍵および公開鍵暗号方式、認証、デジタル署名技術などのセキュリティ技術が確立されてきた。一方、無線センサデバイス、スマートフォン、RFID (Radio Frequency Identification)等の無線通信可能なデバイスの技術的進歩に伴い、新たなシステムやサービスが急速に普及し始めている。しかしながら、アドホックネットワークでは信頼できる第三者機関を用いた認証が困難、VoIP サービスでは格安な通話料金を悪用した迷惑電話発信が増加、RFID では書き込まれた情報の不正読取によるプライバシ侵害等、既存のセキュリティ技術だけでは対処できない問題がある。したがって、これらに対する対策および防御策を講じることは、喫緊の課題となっている。

本論文では、アドホックネットワークにおける認証、VoIP サービス、および RFID サプライチェーンシステムにおけるセキュリティおよびプライバシ保護手法を提案し、理論計算、計算機シミュレーションおよび実験により、提案方式の有効性を示している。

第 1 章では、無線センサデバイス、スマートフォン、RFID を用いたシステムおよびサービスにおけるセキュリティとプライバシに対する課題を示し、本論文の目的と位置付けを述べている。

第 2 章では、無線センサデバイスやスマートフォンを用いるアドホックネットワークにおいて、端末間認証のひとつである Feige-Fiat-Shamir プロトコルの演算量を低減する方法として、検証時に 1024 ビットの変数の乗算が演算の負荷となっていることに着目し、乗算回数を低減しつつ、要求される安全性を確保できる方式を提案している。そして、安全性証明、理論計算および Android デバイスを用いた実測により、提案方式が計算時間を低減可能であることを示している。

第 3 章では、IP 電話を始めとする音声通話サービスにおいて、複数の通話に関する特徴量を基に発信者を 2 つのクラスタに分類することにより、学習を必要としない迷惑電話発信者検出手法を提案し、実際の通話履歴および生成したデータセットを用いて、提案方式の有効性を示している。

第 4 章では、RFID を用いた物流管理システムにおいて、タグに書き込まれた製品情報 (EPC: Electronic Product Code)を漏洩させることなく商品を配送する方法として、タグの EPC に乱数をマスクした上でその乱数を認証サーバに置き、認証が成功した場合に正しい EPC を復元できる仕組みを提案している。提案方式では、認証に必要な情報を、閾値秘密分散法により商品のタグに書き込み、ダミーの情報を付加したタグを一緒に配送することで、安全な認証情報の配送を可能としている。そして、安全性証明、理論計算および市販 RFID デバイスを用いた実験により、提案方式の有効性を示している。

第 5 章は結論であり、本論文の内容および今後の課題を総括している。

以上、本論文の著者は、アドホックネットワークにおける認証、VoIP サービス、および RFID サプライチェーンシステムにおけるセキュリティおよびプライバシ保護手法を提案し、それらの有効性を明らかにしており、工学上、工業上寄与するところが少なくない。よって、本論文の著者は博士(工学)の学位を受ける資格があるものと認める。