様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ９ 月　 １ 日現在

機関番号：２１６０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２９８

研究課題名（和文）ウェアラブル機器向けのセキュリティフレームワーク

研究課題名（英文）Information Security Framework for Wearable Devices

研究代表者
ＳＵ　Ｃｈｕｎｈｕａ（Su, Chunhua）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：４０７１６９６６

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：近年，IoT環境におけるウエアラブル機器の使用は普及しつつある．本研究はウエアラブル機器自身とそれに複数の接続機器の間の相互認証，ウエアラブル機器とその連携するIoT機器のセキュリティ上の脆弱性に対する安全なセキュリティパッチ更新・管理方式，ユーザのプライバシ保護したトレーサビリティなどの３つの機能を実現するフレームワークおよびその関連サイバーセキュリティ技術を提案した．また，ウエアラブル機器だけに止まらず，AI技術とブロックチェンを導入してIoT機器全般の利活用の情報基盤向けのセキュリティ要件の強化手法を示した．さらにそのデータの二次利用する際のプライバシ保護の強化技術の研究も行なった．

研究成果の学術的意義や社会的意義
ウェアラブル機器は小型の組込みシステムでユーザーとその周辺から情報を収集して処理し，遠隔のクラウドサーバー引き渡してさらに分析するという動きが一般的である．この一連の処理過程でセキュリティとプライバシの問題が懸念されている．本研究は従来の情報システムと異なりのウエアラブル機器のモビリティとソーシャルという特徴を考えて，軽量化かつ頑丈なセキュリティ要件を開発した．さらに本研究はウェアラブル機器の新たなセキュリティメカニズムの設計と実装検証を行った．本研究で得られた成果はウエアラブル機器とその関連データの利活用するための安心・安全な実用化や利用者個人情報の保障などの社会要請に答えた．

研究成果の概要（英文）：In recent years, the usage of wearable devices in IoT environments has become more and more widespread. This research mainly focus on following three aspects: the wearable devices security primitives and the multiple contacted devices applications for mutual authentication mechanism, the security patch update management for vulnerabilities in wearable devices, user privacy protection and data traceabilty. We developed a general framework and related cyber security technologies for those IoT-enable wearable security concerns. We also introduce AI and blockchain technologies to enhance our security primitive in the framework. Furthermore, we proposed technologies for strengthening privacy protection when the data is used for secondary purposes.

研究分野：情報セキュリティ

キーワード：IoT機器　ウエアラブル機器　暗号技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年，IoT 環境におけるウエアラブル機器の使用は普及しつつある．ウェアラブル機器はセンサーを搭載した小型の組込みシステムでユーザーとその周辺から情報を収集して処理し，遠隔のクラウドサーバー引き渡してさらに分析するという動きが一般的である．この一連の処理過程でセキュリティとプライバシの問題が懸念されている．また，従来の情報システムと異なりのウエアラブル機器のモビリティとソーシャルという特徴があり，接続デバイスから収集されるデータの活用時の発生したプラバイシの問題が複雑化となりつつある．本研究はこのような背景を考慮して，ウェアラブル機器のセキュリティメカニズムの設計と実装検証に焦点を当て，その中に一番重要と思われる課題であるウエアラブル機器の認証や機器のセキュリティ上の脆弱性対策と機器の使用者のプライバシ保護を取り上げる．

２．研究の目的

本研究はウエアラブル機器自身とそれに複数の接続機器の間の相互認証，ウエアラブル機器とその連携する IoT 機器のセキュリティ上の脆弱性に対する安全なセキュリティ要件更新方式，ユーザのプライバシ保護したトレーサビリティなどの３つの機能を実現するフレームワークを構築することが目的である．

３．研究の方法

研究代表者はこれまで従事してきた IoT 機器向けの認証暗号や軽量化共通鍵暗号の安全性分析の研究経験を生かし，各種攻撃に対するが頑丈なセキュリティと認証精度向上を同時に実現するウェアラブル機器のトランスペアレント認証に応用できるように改善したいと考える.生体の情報を処理する機械学習と軽量化暗号技術に基づいた手法を組み合わせすることで，認証システムのセキュリティと精度向上させる．また，ウエアラブル向けの実装検証を行う以外も提案方式をランダム関数あるいはランダム置換との識別不能性という仮定で安全性証明手法を取り入れ，理論的な証明可能安全性も提供する．さらにウェアラブル機器にも効率的に利用可能な技術を新しく開発する．今まで研究してきた匿名性とトレーサビリティ両方のトレーオフを柔軟に制御できる安全な対話型プロトコルの再設計とそのウェアラブル機器への拡張することができることに考慮に入れ，ウェアラブル機器の性能に合わせた高速データ処理のできる実装手法を提案する．それにより，新たなセキュリティフレームワークを確立させる．また，上記のプロトタイプの試作と性能評価を行うと同時に，人工知能やブロックチェンなどの技術を導入して，新しいセキュリテイ保護方式を試みる．

４．研究成果

2018 年度では，一連のイベントに対する脳波反応に基づいたウエアラブル機器向け認証システムを構築した．提案されたシステムでは，提案された認証システムで参加者のウエアラブル機器から脳波データを収集するために市販の脳波ヘッドセットを使用し．脳波データ収集プロセスの後，システム内で認証トークンとして機能し，認証システム自体をサポートするために，脳から特徴を抽出するために機械学習ベースのアプローチを提案した．

また，ウエアラブル機器用の代表的軽量化暗号をホワイトボックス方式の実装に関連する実用上の問題を検討し，SPN および Feistel 構造が持つ軽量化暗号 KLEIN，Present，および LBlock のホワイトボックス実装した．　そのパフォーマンスとコストをホワイトボックスの AES 実装と比較し，ホワイトボックスの実装がブロックと暗号化鍵の長さだけでなく，暗号の構造とそのホワイトボックスの実装方法も実装コストに強く影響することを示した．その研究をさらに展開して,Google Brain などの研究機関で提案されたニューラルネットワークに基づいた自動セキュリティ保護方式に注目し，IoT 機器の安全性強化の応用に検討した．これは，既存の共通鍵暗号設計原則とは異なるアプローチであり，対称鍵暗号化がどのように機能するのか，およびこの方式に対するセキュリティ要件は何かについての IoT 機器に置かれる状況によって変える可能性がある．我々はいくつかの統計モデルに基づいて提案された共通鍵暗号化方式の安全性を理論と実装で検討した．そしてさらに，我々ははるかに強力な敵対者を導入することによって，高度なディープラーニング技術に基づく IoT 機器やその利活用の情報基盤向けのセキュリティ要件の強化手法を示した．

2019 年度最初にウェアラブル機器をはじめとする IoT 環境 8 ビット AVR プロセッサー向けの楕円曲線暗号の新しい軽量化・高速化実装技術を開発した．具体的に中国の標準技術 SM2 と米国 NIST が推奨する 256 ビットの楕円曲線でのスカラー倍算の効率的で安全なコンパクトな実装と同じビット長の楕円曲線でのスカラー倍算を提案し，既存の実装技術に比較してより軽量かつ高速的性能を達成した．

また，IoT ウェアラブル機器によって収集されたデータはストレージとデータ共有のために信頼できない外部クラウドサーバー委託される場合，プライバシ保護の目的で暗号化されたデータの操作の複雑で検索スキームも非効率的になる．その問題を解決するため，効率的かつ安全な

K 最近傍（KNN）方式を提案した．改良した準同型暗号を利用して 2 つのサーバーが承認されたランキング法を使用してデータアクセスと検索パターンの両方を隠すという目標を実現できる KNN の新しい計算手法を提案した．データのセキュリティを保護すると同時に，データ操作の効率を向上させた．提案手法のパフォーマンスを検証する実装も行われた．

さらに IoT システムを構成する重要な要素の一つが、M2M（Machine-to-Machine）通信やデータ転送を容易にする通信プロトコルを注目した．ウェアラブル機器向けの通信プロトコルの中でも，軽量で使いやすい MQTT（Message Queue Telemetry Transport）のアプリケーションは世界中に数多く存在しています．ただし，そのセキュリティ技術の実装とサポートはまだ非常に脆弱である．我々MQTT を利用したウェアラブル機器と IoT システムのセキュリティ要件を体系的に調査し，必要とさせるセキュリティ要件と実装・サポートされている機能の間のギャップを特定して，セキュリティが強化された MQTT フレームワークを開発した．我々提案と実装したフレームワークにおいては，ウェアラブル機器の認証，暗号鍵の合意，およびポリシーの承認を容易にした．さらに，MQTT セキュリティの機能拡張は，既存の MQTT の API と互換性も実現した．提案したフレームワークと暗号鍵アグリゲーションを用いた 2 段階認証のプロトタイプを実装して評価した．

2020 年度はウエアラブル機器関連システムの侵入検知，移動ウエアラブル機器の位置管理，ロケーションベースのサービスなど，IoT 環境で広範なアプリケーションに応用できるデバイスフリー位置特定技術（DFL）の改良方法を研究開発し，2019 年度のウエラブル機器アーキテクチャの下で，IoT 機器やタグを装備せずにターゲットを特定する方法の実装検証を行なった．具体的に現在の DFL 関連の機械学習アルゴリズムは位置推定でグループ構造が考慮されていないため，位置特定の精度が低く，信頼性/堅牢性が弱いという問題がある．これらの課題を克服するために我々は信号のグループ構造を考慮して，安全性の信頼できるブロックスパース方法を提案した．さらにネットワーク関連のプライバシーを保護するために，元のセンシング信号にガウスノイズを追加した．我々の実験結果は，我々の提案がノイズの多い条件下でも正確な位置特定と管理及び信号回復パフォーマンスを実現し，近年の DFL 方法よりも優れていることを示した．また，ウエラブル機器向けの高い暗号鍵生成率とアクティブな攻撃下での秘密鍵の相関性をどのように確保するかという問題を解決し，ウエアラブル通信用のチャネル特性に基づく秘密鍵の生成方法も提案・実装検証した．さらに証明書なしの署名（CLS）を開発してウエラブル機器などの IoT データの信頼性を保護するための適切な暗号化プリミティブも提案した．我々のバッチ検証と無効な署名識別を備えた安全で効率的な CLS はセキュリティとパフォーマンスの既存提案よりも優れていることを示した．最後にブロックチェーンアーキテクチャに基づく個人のウエラブル機器情報共有プラットフォームのフレームワークを設計し，技術的詳細と技術的利点を実装検証した．提案したプラットフォームをクレジットブラックリストに適用してウエラブル機器利用者のデータ収集の検証コストの削減と信用データの安全な共有を実現した．

５．主な発表論文等

〔雑誌論文〕　計25件（うち査読付論文　11件／うち国際共著　10件／うちオープンアクセス　4件）

１．著者名 Zhou Lu、Su Chunhua、Yeh Kuo-Hui	４．巻 18
２．論文標題 A Lightweight Cryptographic Protocol with Certificateless Signature for the Internet of Things	５．発行年 2019年
３．雑誌名 ACM Transactions on Embedded Computing Systems	６．最初と最後の頁 1～10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3301306	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Zhou Lu、Su Chunhua、Hu Zhi、Lee Sokjoon、Seo Hwajeong	４．巻 18
２．論文標題 Lightweight Implementations of NIST P-256 and SM2 ECC on 8-bit Resource-Constraint Embedded Device	５．発行年 2019年
３．雑誌名 ACM Transactions on Embedded Computing Systems	６．最初と最後の頁 1～13
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3236010	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Huang Huakun、Han Zhaoyang、Ding Shuxue、Su Chunhua、Zhao Lingjun	４．巻 11
２．論文標題 Improved Sparse Coding Algorithm with Device-Free Localization Technique for Intrusion Detection and Monitoring	５．発行年 2019年
３．雑誌名 Symmetry	６．最初と最後の頁 637～637
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/sym11050637	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Zhao Lingjun、Su Chunhua、Huang Huakun、Han Zhaoyang、Ding Shuxue、Li Xiang	４．巻 11
２．論文標題 Intrusion Detection Based on Device-Free Localization in the Era of IoT	５．発行年 2019年
３．雑誌名 Symmetry	６．最初と最後の頁 630～630
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/sym11050630	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Zhao Bo、Fang Liming、Zhang Hanyi、Ge Chunpeng、Meng Weizhi、Liu Liang、Su Chunhua	４．巻 19
２．論文標題 Y-DWMS: A Digital Watermark Management System Based on Smart Contracts	５．発行年 2019年
３．雑誌名 Sensors	６．最初と最後の頁 3091～3091
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s19143091	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Chen Jiageng、Su Chunhua、Yan Zheng	４．巻 2019
２．論文標題 AI-Driven Cyber Security Analytics and Privacy Protection	５．発行年 2019年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1～2
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2019/1859143	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ya Liu, Liang Cheng, Fengyu Zhao, Chunhua Su, Zhiqiang Liu, Wei Li, Dawu Gu	４．巻 13
２．論文標題 New Analysis of Reduced-Version of Piccolo in the Single-Key Scenario	５．発行年 2019年
３．雑誌名 KSII Transactions on Internet and Information Systems	６．最初と最後の頁 4727-4741
掲載論文のDOI（デジタルオブジェクト識別子） 10.3837/tiis.2019.09.022	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Zhou Lu、Sun Xin、Su Chunhua、Liu Zhe、Raymond Choo Kim-Kwang	４．巻 479
２．論文標題 Game theoretic security of quantum bit commitment	５．発行年 2019年
３．雑誌名 Information Sciences	６．最初と最後の頁 503～514
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ins.2018.03.046	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Guo Cheng、Zhuang Ruhan、Su Chunhua、Liu Charles Zhechao、Choo Kim-Kwang Raymond	4．巻 6
2．論文標題 Secure and Efficient ${K}$ Nearest Neighbor Query Over Encrypted Uncertain Data in Cloud-IoT Ecosystem	5．発行年 2019年
3．雑誌名 IEEE Internet of Things Journal	6．最初と最後の頁 9868～9879
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2019.2932775	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Cheng Lichen、Liu Jiqiang、Su Chunhua、Liang Kaitai、Xu Guangquan、Wang Wei	4．巻 99
2．論文標題 Polynomial-based modifiable blockchain structure for removing fraud transactions	5．発行年 2019年
3．雑誌名 Future Generation Computer Systems	6．最初と最後の頁 154～163
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2019.04.028	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Zhou Lu、Su Chunhua、Li Zhen、Liu Zhe、Hancke Gerhard P.	4．巻 93
2．論文標題 Automatic fine-grained access control in SCADA by machine learning	5．発行年 2019年
3．雑誌名 Future Generation Computer Systems	6．最初と最後の頁 548～559
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2018.04.043	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ge Chunpeng、Zhou Lu、Xia Jinyue、Szalachowski Pawel、Su Chunhua	4．巻 7
2．論文標題 A Secure Fine-Grained Micro-Video Subscribing System in Cloud Computing	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 137266～137278
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2942651	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Fang Liming、Yin Changchun、Zhou Lu、Li Yang、Su Chunhua、Xia Jinyue	4．巻 507
2．論文標題 A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine	5．発行年 2020年
3．雑誌名 Information Sciences	6．最初と最後の頁 143～160
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ins.2019.08.020	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Chien Hung Yu、Chen Yi Jui、Qiu Guo Hao、Liao Jian Fu、Hung Ruo Wei、Lin Pei Chih、Kou Xi An、Chiang Mao Lun、Su Chunhua	4．巻 32
2．論文標題 A MQTT-API-compatible IoT security-enhanced platform	5．発行年 2020年
3．雑誌名 International Journal of Sensor Networks	6．最初と最後の頁 54～54
掲載論文のDOI（デジタルオブジェクト識別子） 10.1504/IJSNET.2020.104463	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Zhou Lu、Yeh Kuo-Hui、Hancke Gerhard、Liu Zhe、Su Chunhua	4．巻 35
2．論文標題 Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints	5．発行年 2018年
3．雑誌名 IEEE Signal Processing Magazine	6．最初と最後の頁 76～87
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MSP.2018.2846297	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Chiu Wayne、Su Chunhua、Fan Chuan-Yen、Chen Chien-Ming、Yeh Kuo-Hui	4．巻 10
2．論文標題 Authentication with What You See and Remember in the Internet of Things	5．発行年 2018年
3．雑誌名 Symmetry	6．最初と最後の頁 537～537
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/sym10110537	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Mamun Mohammad Saiful Islam、Su Chunhua、Yang Anjia、Miyaji Atsuko、Ghorbani Ali	４．巻 43
２．論文標題 OTP-IoT: An ownership transfer protocol for the Internet of Things	５．発行年 2018年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 73～82
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2018.10.009	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Zhou Lu、Su Chunhua、Sun Xin、Zhao Xishun、Choo Kim-Kwang Raymond	４．巻 88
２．論文標題 Stag hunt and trust emergence in social networks	５．発行年 2018年
３．雑誌名 Future Generation Computer Systems	６．最初と最後の頁 168～172
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2018.05.053	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Zhou Lu、Su Chunhua、Wen Yamin、Li Weijie、Gong Zheng	４．巻 86
２．論文標題 Towards practical white-box lightweight block cipher implementations for IoTs	５．発行年 2018年
３．雑誌名 Future Generation Computer Systems	６．最初と最後の頁 507～514
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2018.04.011	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yeh Kuo-Hui、Su Chunhua、Hou Jia-Li、Chiu Wayne、Chen Chien-Ming	４．巻 6
２．論文標題 A Robust Mobile Payment Scheme With Smart Contract-Based Transaction Repository	５．発行年 2018年
３．雑誌名 IEEE Access	６．最初と最後の頁 59394～59404
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2018.2874021	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Cha Shi-Cho、Chuang Ming-Shiung、Yeh Kuo-Hui、Huang Zi-Jia、Su Chunhua	4．巻 6
2．論文標題 A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices	5．発行年 2018年
3．雑誌名 IEEE Access	6．最初と最後の頁 20779～20787
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2018.2820716	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Zhou Lu、Li Xiong、Yeh Kuo-Hui、Su Chunhua、Chiu Wayne	4．巻 91
2．論文標題 Lightweight IoT-based authentication scheme in cloud computing circumstance	5．発行年 2019年
3．雑誌名 Future Generation Computer Systems	6．最初と最後の頁 244～251
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2018.08.038	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Zhou Lu、Li Xiong、Yeh Kuo-Hui、Su Chunhua、Chiu Wayne	4．巻 91
2．論文標題 Lightweight IoT-based authentication scheme in cloud computing circumstance	5．発行年 2019年
3．雑誌名 Future Generation Computer Systems	6．最初と最後の頁 244～251
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.future.2018.08.038	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Zhou Lu、Chen Jiageng、Zhang Yidan、Su Chunhua、Anthony James Marino	4．巻 80
2．論文標題 Security analysis and new models on the intelligent symmetric key encryption	5．発行年 2019年
3．雑誌名 Computers & Security	6．最初と最後の頁 14～24
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.cose.2018.07.018	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Bagus Santoso、Chunhua Su	４．巻 25
２．論文標題 A New Identification Scheme based on Syndrome Decoding Problem with Provable Security against Quantum Adversaries	５．発行年 2019年
３．雑誌名 Journal of Universal Computer Science	６．最初と最後の頁 294～308
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計12件（うち招待講演　0件／うち国際学会　5件）

１．発表者名 Hao Jiang, Weizhi Meng, Chunhua Su, Kim-Kwang Raymond Choo
２．発表標題 CAVAEva: An Engineering Platform for Evaluating Commercial Anti-malware Applications on Smartphones
３．学会等名 15th International Conference on Information Security and Cryptology (Inscrypt2019)（国際学会）
４．発表年 2019年

１．発表者名 Hung-Yu Chien, Chunhua Su
２．発表標題 A Fault-Tolerant and Flexible Privacy-Preserving Multisubset Data Aggregation in Smart Grid
３．学会等名 International Conference on Computational Science & Intelligence and Applied Informatics (CSII 2019)（国際学会）
４．発表年 2019年

１．発表者名 Hung-Yu Chien, Xi-An Kou, Mao-Lun Chiang, Chunhua Su
２．発表標題 Secure and Efficient MQTT Group Communication Design
３．学会等名 International Conference on Computational Science & Intelligence and Applied Informatics (CSII 2019)
４．発表年 2019年

１．発表者名
Weizhi Meng, Wenjuan Li, Lijun Jiang, Kim-Kwang Raymond Choo, Chunhua Su

２．発表標題
Practical Bayesian Poisoning Attacks on Challenge-Based Collaborative Intrusion Detection Networks

３．学会等名
24th European Symposium on Research in Computer Security (ESORICS 2019)

４．発表年
2019年

１．発表者名
Hung-Yu Chien, Guo-Hao Qiu, Ruo-Wei Hung, An-Tong Shih, Chunhua Su

２．発表標題
Hierarchical MQTT with Edge Computation

３．学会等名
10th International Conference on Awareness Science and Technology (iCAST 2019)

４．発表年
2019年

１．発表者名
Zhaoyang Han, Chunhua Su, Shuxue Ding, Huakun Huang, Lingjun Zhao

２．発表標題
Device-Free Localization via Sparse Coding with Log-Regularizer

３．学会等名
10th International Conference on Awareness Science and Technology (iCAST 2019)

４．発表年
2019年

１．発表者名
Bagus Santoso, Yasutada Oohama, Chunhua Su

２．発表標題
Measuring Security of Symmetric Encryption Schemes Against On-the-Fly Side-Channel Key-Recovery Attacks.

３．学会等名
13th International Conference on Network and System Security (NSS 2019)

４．発表年
2019年

１．発表者名
Jingjing Song, Haiwu He, Zhuo Lv, Chunhua Su, Guangquan Xu, Wei Wang

２．発表標題
An Efficient Vulnerability Detection Model for Ethereum Smart Contracts

３．学会等名
13th International Conference on Network and System Security (NSS 2019)

４．発表年
2019年

１．発表者名
Chunpeng Ge, Lu Zhou, Jinyue Xia, Pawel Szalachowski, Chunhua Su

２．発表標題
A Secure Fine-Grained Identity-Based Proxy Broadcast Re-encryption Scheme for Micro-video Subscribing System in Clouds

３．学会等名
4th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2019)

４．発表年
2019年

１．発表者名
Hiroaki Anada, Tomohiro Matsushima, Chunhua Su, Weizhi Meng, Junpei Kawamoto, Samiran Bag, Kouichi Sakurai

２．発表標題
Analysis of Variance of Graph-Clique Mining for Scalable Proof of Work

３．学会等名
Conference on Information Security and Cryptology 2019（国際学会）

４．発表年
2018年

１．発表者名
Ruoyu Deng, Na Ruan, Ruidong Jin, Yu Lu, Weijia Jia, Chunhua Su, Dandan Xu

２．発表標題
SpamTracer: Manual Fake Review Detection for O2O Commercial Platforms by Using Geolocation Features

３．学会等名
Conference on Information Security and Cryptology 2019（国際学会）

４．発表年
2018年

１．発表者名 Weizhi Meng, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, Jinguang Han
２．発表標題 CPMap: Design of Click-Points Map-Based Graphical Password Authentication
３．学会等名 IFIP TC11: Security and Protection in Information Processing Systems 2018（国際学会）
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計1件

国際研究集会	開催年
13th International Conference on Network and System Security	2019年～2019年

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関