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　５ 年　 ６ 月 ２１ 日現在

機関番号：１２６０８
研究種目：若手研究
研究期間：2019～2022
課題番号：１９Ｋ２０２５４

研究課題名（和文）ヘルスケアにおけるプライバシー保護を重視した認証付き遠隔監視・データ共有機構

研究課題名（英文）A Privacy-Preserved Remote Monitoring and Data Sharing Mechanism with Authentication for Healthcare Systems

研究代表者

金　勇（Jin, Yong）

東京工業大学・学術国際情報センター・マネジメント准教授

研究者番号：６０７２５７８７

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：2019年度は主に目的システムを実装するためのローカル環境を設計・構築し、目的の機能を実現するためのプラットフォームの設計と機能確認を行った。2020年度は主にプロトタイプシステムを実装し、ローカル環境において全体的な機能評価を行った。2021年度はヘルスケア機器のデータを暗号化してリアルタイムに登録・更新するためのDNSシステムを実装し、クライアントが効率的にIoTデータを照会可能なシステムを構築した。2022年度は主にユーザのプライバシー強化を考慮し、提案システムに対してヘルスケア機器のデータ暗号化に加え、データ登録、更新、同期、照会などの通信路の暗号化を実施した。

研究成果の学術的意義や社会的意義
本研究では、遠隔医療・ヘルスケアシステム等における個人情報、プライバシー及び重要な医療関連データを扱う時のセキュリティの着目し、個人情報漏洩防止とプライバシー保護の対策として、データの暗号化を考慮した遠隔医療・遠隔ヘルスケアシステムを対象に、安全な遠隔監視とデータ共有の仕組みを構築・実現を目的としている。本研究では現在最も広く使われている分散データベースの一つであるDNSを活用して目的のシステムを実現し、この成果は大規模なIoT機器を安全かつ安定に扱う一つの実現方法を学術的に示した。また、実社会においてヘルスケアシステムへのDNSシステムの応用についてその実現可能性を示した。

研究成果の概要（英文）：In fiscal 2019, we designed and constructed a local experimental environment and verified the platform for the objective system. In fiscal 2020, we implemented a prototype system and conducted a preliminary experiment for the entire system. In fiscal 2021, we constructed a DNS system for registering and updating the IoT data with encryption and implemented a effective inquiry system for the IoT data from the client. In fiscal 2022, we enhanced the user privacy protection and conducted the encryption for the communication link for IoT data registration, update, synchronization, and inquiry in addition to the IoT data encryption.

研究分野：ネットワークセキュリティ

キーワード：Healthcare system　Internet of Things　IoT　DNS　DNS over TLS　DoT　Docker

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年、IoT(Internet of Things)社会の発展に伴い、遠隔監視・制御への要求が高まりつつある。特に、高齢者社会の深刻化により、遠隔医療・ヘルスケアサービスも増えており、個人情報、プライバシーや医療データを担当医師以外に公開しないことが求められている。既存の多くのシステムでは、暗号化されてない遠隔通信やデータ伝送方式を使ったり、クラウド上に暗号化されてないデータを保存したりするため、通信路での盗聴だけでなくクラウドサービス業者側からのデータ漏洩も懸念されている。その中には、安全な通信を使う VPN(Virtual Private Network)を利用したサービスもあるが、この方法には高い導入コスト、スケールしない問題が考えられる。また、暗号化通信(HTTPS)を使った遠隔テレビ会議システムの利用も挙げられるが、医師との時間調整や日常確認だけを行うには人手不足の問題がある。遠隔医療システムの他に、高齢者社会において一人暮らしの日常生活を確認するための遠隔ヘルスケアも社会的な課題になっている。この場合、重要な医療関連データを扱ってないが、個人情報漏洩やプライバシー暴露が重要視されているため、適切な暗号化通信とデータ(写真、レポート等)転送方法が求められている。例えば、日常の生活状況を透過的に家族に伝えたり、身体情報を家族に遠隔で確認して貰ったりする場合、クラウドサービスを含め、データを暗号化して保存し、安全に共有（転送、取得、廃棄等）可能な仕組みが要求される。

２．研究の目的

本研究の着目点は遠隔医療・ヘルスケアシステム等における個人情報、プライバシー及び重要な医療関連データを扱う場合、いかに認証された相手だけ安全・安心に遠隔から情報を取得および暗号化されたデータを復号し、更に、必要な制御ができるスケーラビリティを考慮した軽量な仕組みを設計、実現できるかにある。そこで、本研究の目的は、個人情報漏洩防止とプライバシー保護の対策として、データの暗号化を考慮した遠隔医療・遠隔ヘルスケアシステムを対象に、安全な遠隔監視とデータ共有の仕組みを構築・実現することである。

３．研究の方法

まず、本研究では図１のように、１つの家庭(ホームネットワーク)で１つのドメイン名を所有し、そのドメイン名の配下に各ヘルスケア機器の名前がサブドメイン名として登録されている環境を想定する。各ヘルスケア機器を使用するとその「使用履歴」を DNS サーバに登録することにより、認証された相手だけが遠隔から確認することにする。ここでは、DNS システムだけで「使用履歴」が確認できるため軽量なシステムで実現し、更に、DNS 固有の認証機能と暗号化技術を利用してプライバシー保護を考慮した手法を実現する。

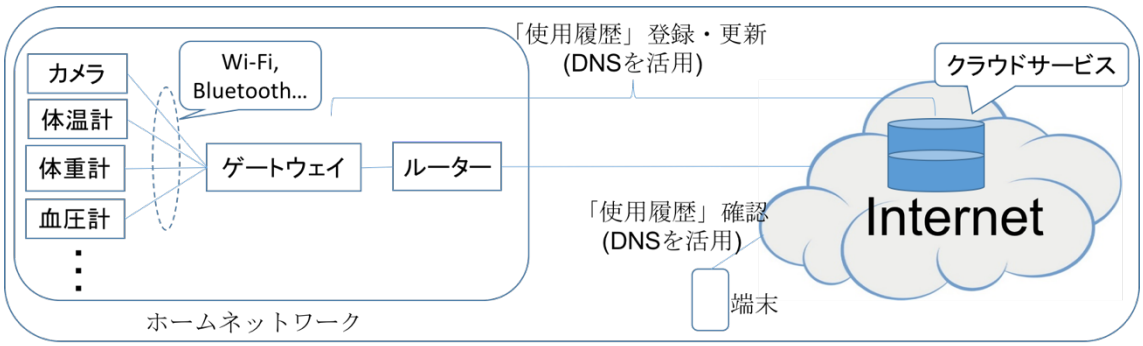

図１. DNSを活用したヘルスケア機器使用履歴の登録、更新および遠隔確認の仕組み

次に、本研究では図２のようにヘルスケア機器の「使用履歴」に応じて必要なデータ(写真、レポート等)を暗号化して保存するデータベースを構築し、その都度遠隔から取得及び廃棄可能な動的な仕組みをコンテイナー技術と DNS を連携して実現する。その後、「使用履歴」の確認と暗号化データの取得に必要な認証及びデータの暗号化・復号化に必要な認証の仕組みを実現する。

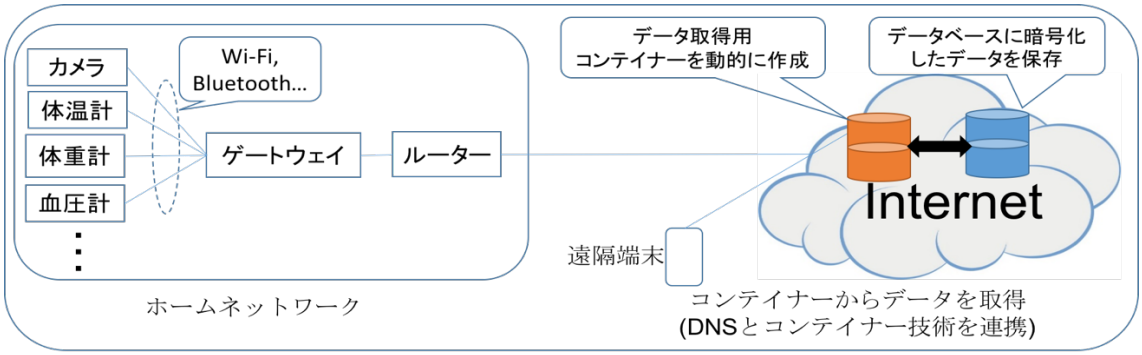

図2. DNSとコンテイナー技術を連携した軽量かつ動的データ共有機構の仕組み

最後に、IETF の標準化動向に応じて通信路の暗号化によりユーザプライバシー保護の強化を実施する。近年、インターネットユーザのプライバシー保護が注目されており、名前解決におけるユーザプライバシー保護を目的とした DNS over TLS (DoT)や DNS over HTTPS (DoH)など通信路の暗号化方式が IETF により標準化された。また、本来計画していた大規模ネットワークでの性能評価実験は新型コロナ禍の影響により、実験環境の検討及び構築に支障が出たため、IETF の標準化動向に応じてユーザのプライバシー強化へ方針変更を行った。これにより、ヘルスケア機器のデータの暗号化だけでなく、通信路の暗号化を加えることにより、ユーザのプライバシー漏洩防止がより期待できる。ヘルスケア機器のデータ種類に関しては、まずテクストデータのみ対応し、今後バイナリデータへの対応を実施する予定である。

４．研究成果

まず、目的システムに基づいたプロトタイプを実装するためのローカルネットワーク環境を設計・構築し、目的の機能を実現するためのプラットフォームの設計と一部の機能確認を行った。具体的には、ヘルスケア機器の「使用履歴」を暗号化してリアルタイムに登録・更新するための DNS システムを設計し、DNS システムへの登録、更新及び問合せログが効率的に取れるようなシステムを構築した。次に、目的のシステム設計に基づいたプロトタイプを実装し、ローカル実験環境において全体的な機能評価を行った。具体的には、ヘルスケア機器の「使用履歴」を暗号化してリアルタイムに登録・更新するための IoT システム及び DNS システムを実装し、DNS 登録、更新及び問合せログが効率的に取れるようなシステムを構築した[図 3]。特に、IoT 機器から取得したデータを全て暗号化してから特定のユーザがインターネット経由で照会及びダウンロードできる機能の実装に工夫した。更に、DNS システム上に登録された「使用履歴」に応じて必要なファイル(写真やレポート等)を暗号化して保存するデータベースシステムの構築とそのバイナリデータを遠隔からダウンロード及び削除可能なコンテイナーを動かす環境の実装を行った[図 4 と図 5]。特に、セキュリティとプライバシーを重視し、必要な時に関連情報の問合せ及び関連ファイルのダウンロードが可能なコンテナー機能だけでなく、認証と暗号化に加えてダウンロードが終わった後に即座にコンテナーを削除するようなシステムの実装に工夫した。また、上記のプロトタイプシステムにおいて、全体的な機能評価を行い、その成果を国際会議にて発表を行なった。

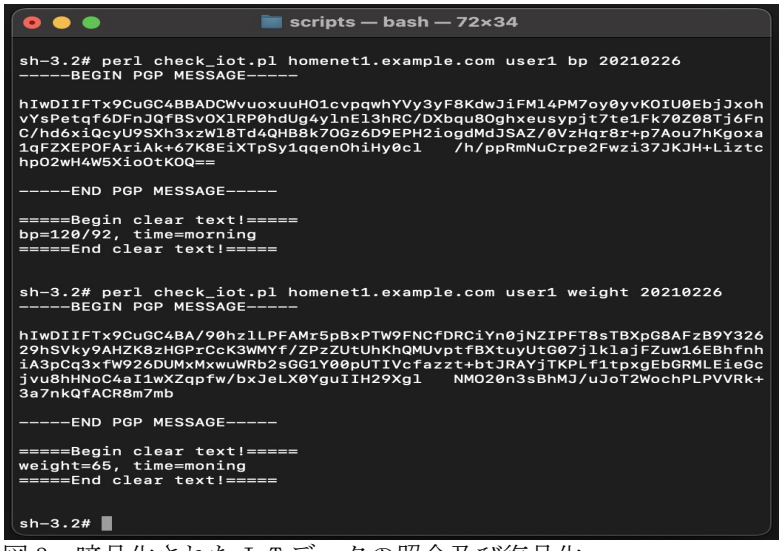

図 3. 暗号化された IoT データの照会及び復号化

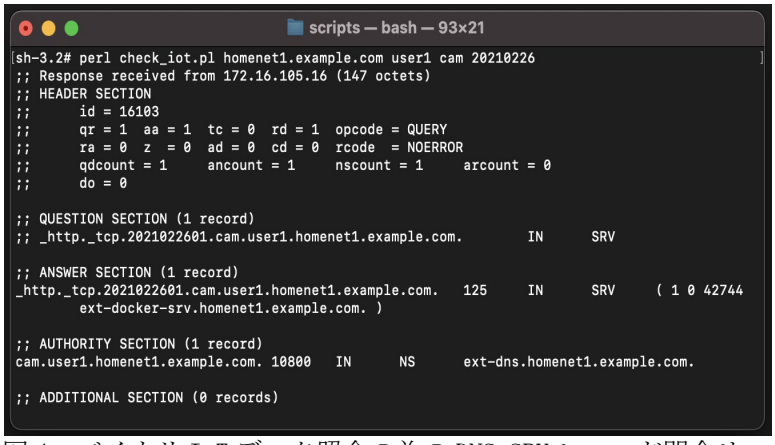

図 4. バイナリ IoT データ照会の為の DNS SRV レコード問合せ

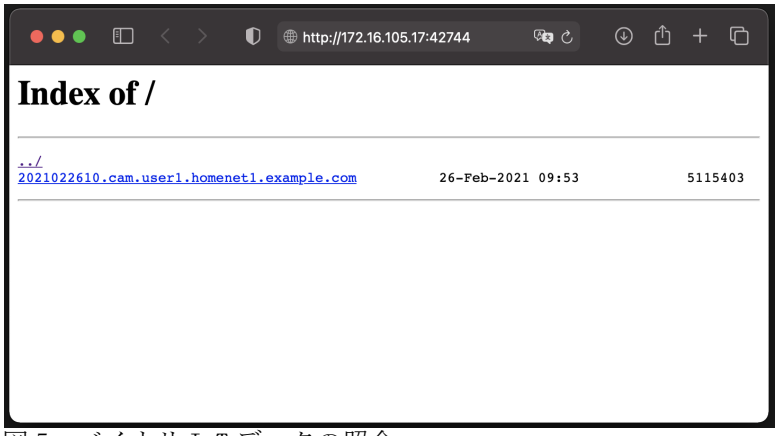

図 5. バイナリ IoT データの照会

最後に、ユーザのプライバシー強化を考慮し、提案システムに対してヘルスケア機器のデータ暗号化に加え、データ登録、更新、同期、照会などの通信路の暗号化を実施した。近年、インターネットユーザのプライバシー保護が注目されており、名前解決におけるユーザプライバシー保護を目的とした DNS over TLS (DoT)や DNS over HTTPS (DoH)など通信路の暗号化方式が IETF により標準化された。また、本来計画していた大規模ネットワークでの性能評価実験は新型コロナ禍の影響により、実験環境の検討及び構築に支障が出たため、IETF の標準化動向に応じてユーザのプライバシー強化へ方針変更を行った。具体的には、ホームネットワーク内におけるデータベースへのヘルスケア機器のデータ登録と更新、外部ネットワーク(インターネット)におけるクライアントからのヘルスケア機器のデータ照会、またホームネットワーク内のデータベースと外部ネットワーク(インターネット)のデータベース間のデータ同期の際の通信路の暗号化を実施した。これにより、ヘルスケア機器のデータの暗号化だけでなく、通信路の暗号化を加えることにより、ユーザのプライバシー漏洩防止が実現できた。ヘルスケア機器のデータ種類に関しては、まずテクストデータのみ対応し、今後バイナリデータへの対応を実施する予定である。また、上記の通信路の暗号化拡張に関して国内研究会にて発表を行った。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　10件）

１．発表者名 相良隼，金勇，飯田勝吉，高井昌彰
２．発表標題 DoTを用いたプライバシー配慮型IoTデータ照会システムの検討
３．学会等名 信学技報
４．発表年 2023年

１．発表者名 砂原悟，金勇，飯田勝吉
２．発表標題 DoHに基づくDNS権威サーバアーキテクチャに関する一検討
３．学会等名 電子情報通信学会　インターネットアーキテクチャ研究会
４．発表年 2022年

１．発表者名 砂原悟，金勇，飯田勝吉
２．発表標題 IPヘッダ情報からのプライバシー漏洩を防ぐDoHに基づく新たな名前解決機構
３．学会等名 電子情報通信学会　インターネットアーキテクチャ研究会
４．発表年 2022年

１．発表者名 S. Sunahara, Y. Jin, and K. Iida
２．発表標題 A proposal of DoH-based domain name resolution architecture including authoritative DNS servers
３．学会等名 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)（国際学会）
４．発表年 2022年

１．発表者名 Y. Jin, M. Tomoishi, and N. Yamai
２．発表標題 Secure Remote Monitoring and Cipher Data Sharing for IoT Healthcare System with Privacy Preservation
３．学会等名 2021 The 5th International Conference on Cloud and Big Data Computing (ICCBDC)（国際学会）
４．発表年 2021年

１．発表者名 陸子健，金勇，山井成良，友石正彦
２．発表標題 家庭向けの遠隔ヘルスケアにおけるDNSを活用した監視システムの試作
３．学会等名 情報処理学会インターネットと運用技術研究会研究報告
４．発表年 2021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0件

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