

[ポスター発表] 研究報告

SINETStreamにおけるセキュアなデータ共有機構の開発

北川 直哉^{1,a)} 竹房 あつ子^{1,b)} 合田 憲人^{1,c)}

Development of a Secure Data Sharing Mechanism for SINETStream

1. はじめに

多種多様なセンサデバイスで収集したデータをクラウド上に蓄積し、機械学習等のデータ解析を活用した研究を可能にする IoT (Internet of Things) アプリケーションシステムの研究がさかに行われている。国立情報学研究所では、モバイル回線網を学術情報ネットワーク SINET の VPN に直接接続させた「SINET 広域データ収集基盤」(モバイル SINET) を運用しており、安全な IoT 実験環境の構築のための接続環境を提供している [1]。また、モバイル SINET を利用して収集したデータを活用した IoT アプリケーションの開発を支援する SINETStream を開発し、公開している [2] [3]。SINETStream は、現在までに Linux などの利用環境を想定した Java 版と Python 版、およびスマートフォンをセンサデバイスとして利用する環境を想定した Android 版をオープンソースソフトウェアとして公開しており、SINET の利用の有無を問わず利用可能となっている。

クラウドを活用した IoT アプリケーションシステムの構築を支援するプラットフォームとして、My-IoT [4] や FIDO Device Onboard (FDO) [5] が挙げられる。これらを利用することで、システム開発者はエッジハードウェアの管理やセンサ群のグループ化などの処理を容易に行うことができるが、秘匿情報を扱う際の暗号化処理やグループ間での柔軟なアクセス制御など、安全にデータ管理するための機能を有していない。一方、IoT アプリケーションの開発では文献 [6] のように、バイタル情報などの秘匿性の高い情報を共有する必要がある場合があり、暗号化や適切なアクセス制御を実現した安全なデータ共有が容易に行える IoT アプリケーションプラットフォームが望まれている。しかし、複数のデバイスやグループ間で暗号鍵を共有するのは非常に煩雑で容易ではない上に、設定ミスなどの

事故のリスクを排除できない課題がある。

このような課題に対し、筆者らは SINETStream において安全かつ容易にデータの暗号化や研究グループ内でのデータ共有が実現可能な機構を開発した(以降、本稿ではこの機構を提供するサーバを「コンフィグサーバ」と記述する)。本機構は、学認 IdP を用いて利用者の認証を行い、また従来方式では煩雑だったデータ暗号鍵の管理をシステム内のセキュアな KVS で保管することで、安全な秘匿情報の共有を容易に実現することができる。また、秘匿情報は暗号化された状態で利用者に提供し、利用者の秘密鍵で復号処理を行うことで、閲覧を許可されたユーザのみがデータを閲覧できるようにした。これまで SINETStream では、使用するメッセージブローカへの接続パラメータなどを記した設定ファイルの配布手段が課題となっていたが、本機構を利用することでデータ暗号鍵などの秘匿情報が含まれる設定ファイルを安全に配布することが可能になる。

2. システム構成と処理の流れ

データストリームの管理者はコンフィグサーバの管理画面(Web UI)から SINETStream を用いたデータ収集に必要なメッセージブローカの IP アドレス等の設定情報と、データストリームを共有するグループメンバーの登録を行う。管理者が登録したデータは、コンフィグサーバ内の関係データベースに保存され、データ暗号鍵などの秘匿情報はセキュアな KVS である HashiCorp Vault 内に保存される。なお、コンフィグサーバは学認の SP として構築した。

コンフィグサーバの利用シナリオとして、(1) 各利用者が SINETStream の設定ファイルをコンフィグサーバからダウンロードする方法、(2) SINETStream の対応ライブラリがコンフィグサーバ API を用いて SINETStream の設定パラメータをコンフィグサーバから自動的に取得する方法、の 2 つが挙げられる。これらの 2 つのシナリオを利用する際の処理について本節で述べる。

また、文献 [2] [3] が示すように、SINETStream はセンサデバイス等から収集したデータを大学に設置したサーバやクラウドストレージへ保存する機能を提供している。この

¹ 国立情報学研究所
National Institute of Informatics, Chiyoda-ku, Tokyo 101-8430, Japan

a) kitagawa@nii.ac.jp

b) takefusa@nii.ac.jp

c) aida@nii.ac.jp

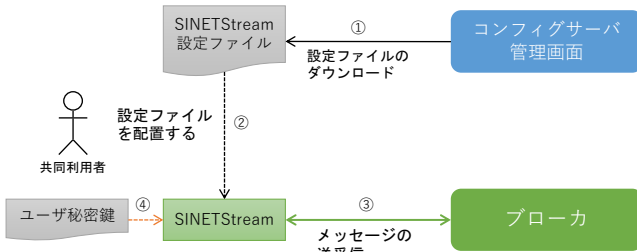


図 1 利用者が設定ファイルをダウンロードする場合の処理の流れ

ため、秘匿性の高いデータを扱う場合には、ストレージ上では暗号化された状態でデータを保存する必要があるが、かつデータの復号時には各利用者が秘匿データをダウンロード後に各自のユーザ秘密鍵で復号する必要があることが知られている [7]。したがって、本稿で述べるコンフィグサーバを利用する場合にも、暗号化されたままストレージに保存された秘匿データの復号は各利用者が各自で行う必要があることに注意されたい。

2.1 利用者が設定ファイルをダウンロードする場合

図 1 に、利用者が SINETStream の設定ファイルをダウンロードする場合の処理の流れを示す。

利用者は、コンフィグサーバの管理画面から SINETStream の設定ファイルをダウンロードする (①)。この際、コンフィグサーバの管理画面では学認フェデレーションの IdP を用いてユーザ認証を行う。次に、SINETStream 上にメッセージブローカへの接続パラメータなどを記した設定ファイルを設置した上で (②)、SINETStream とブローカ間のメッセージ送受信を行う (③)。なお、設定ファイルに秘匿情報が含まれている場合にはダウンロードした設定ファイルに暗号化された値が含まれているため、各利用者が保持するユーザ秘密鍵を用いて暗号化された値を SINETStream のコンフィグサーバ対応ライブラリが自動的に復号処理を行う (④)。

2.2 SINETStream ライブラリが API を利用する場合

図 2 に、SINETStream の対応ライブラリがコンフィグサーバ API を用いて SINETStream の設定パラメータをコンフィグサーバから取得する場合の処理の流れを示す。利用者は、コンフィグサーバの管理画面からコンフィグサーバの認証情報 (サーバのアドレスや API アクセスキー等) をダウンロードし (①)、SINETStream の実行環境にコンフィグサーバの認証情報を配置する (②)。コンフィグサーバは、REST API によって SINETStream の設定パラメータの要求および応答のやりとりを行うほか (③)、データ暗号化鍵などの秘匿情報の要求および応答のやりとりを行う (④)。以上の処理を行い、SINETStream とブローカ間でメッセージ送受信を行う (⑤)。なお、2.1 節で述べた利用者が設定ファイルをダウンロードする場合と同

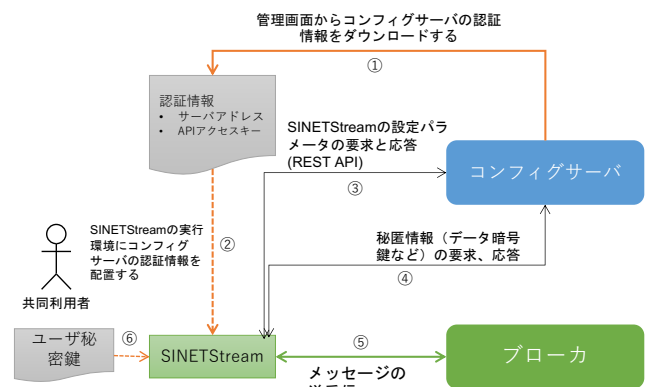


図 2 対応ライブラリが API を利用する場合の処理の流れ

様にコンフィグサーバから取得した秘匿情報は暗号化されているため、各利用者が保持するユーザ秘密鍵を用いて SINETStream のコンフィグサーバ対応ライブラリが自動的に復号処理を行う (⑥)。

3. おわりに

本稿では、IoT アプリケーションの開発において需要が高まっている安全な機密情報の共有を実現する、SINETStream を活用したデータ共有機構について述べた。本データ共有機構に対応するライブラリは、Java 版および Python 版を近日公開予定である。また、今後は Android 対応ライブラリを開発し、リリースする予定である。

4. 謝辞

本研究にご協力いただいた数理工研の小泉敦延様、鯉江英隆様、遠藤雅彦様に深く感謝いたします。また、本稿の執筆にあたりご議論いただいた広島大学の近堂徹准教授に深く感謝いたします。

参考文献

- [1] “SINET 広域データ収集基盤実証実験” <https://www.sinet.ad.jp/wadci>.
- [2] “SINETStream” <https://www.sinetstream.net>.
- [3] A. Takefusa, J. Sun, I. Fujiwara, H. Yoshida, K. Aida, and C. Pu, “SINETStream: Enabling Research IoT Applications with Portability, Security and Performance Requirements”, Proc. of 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp.482-492, 2021.
- [4] “My-IoT コンソーシアム” <https://www.my-iot.jp>.
- [5] “FIDO Device Onboard (FDO)” <https://fidoalliance.org/specifications/download-iot-specifications/>.
- [6] 近堂徹, 町澤まろ, “脳生理情報のクラウド解析プラットフォーム実現に向けた通信手法の検討”, マルチメディア, 分散協調とモバイルシンポジウム 2021 論文集, pp. 237-242, 2021.
- [7] K. Yokogi, N. Kitagawa, and N. Yamai, “IoT-oriented Secure Data Sharing Using Public Cloud”, Journal of Information Processing, 2021. (in press)