データのコピー制限と利用記録提供の機密実行環境を利用した実装の提案

曽山 暉史[1]　新城 靖[1]　石黒 淳[1]

1. 序論

今日，インターネット上ではショッピングサイトや動画配信プラットフォームなどの様々なサービスが提供されている．これらのオンラインサービスを利用する際，利用者は自らの個人情報を提供することも多い．例えば，ショッピングサイトで購入した商品を受け取るための住所情報や，電子的に利用料金を決済するためのクレジットカード情報などが必要となる．

ここで，サービス提供者に預けた個人情報を保護することが極めて重要となるが，利用者はいったんサービス側に個人情報を提供すると，自身の情報がどのように扱われているのかに関する情報を得られないのが現状である．サービスの提供に必要な最小限度の利用・移動・複製を超えた操作が提供した個人情報に対して行われるおそれもあるが，利用者がこれを知る術はない．

そこで本研究では，サービス側に提供した個人情報などのデータの利用・コピー操作に対して，提供者自身が制限を設けられることや，データの利用・コピーが行われた事実を，後から追跡できるようにすることを目的とする．本研究では，これを機密実行環境（Trusted Execution Environment, TEE）を用いて実装する方法を提案する．本研究ではまず，サービスを利用する際の個人情報保護を想定して機能を設計する．

2. 脅威モデル

本研究では，以下の攻撃を想定する．

- プログラムの内容や，主記憶の内容が改変される
- プロセスは任意のタイミングで停止される
- 永続記憶内のデータは改竄・ロールバック攻撃される
- ネットワーク上を流れるデータは盗聴・改竄される

3. 提案手法

3.1 概要

本研究では，データのコピー制限と利用記録の提供を，図 1 に示したようなプログラムで実装する．サービスの利用者は，自らのデータに対する操作を制限するためのポリシーを添えて，サービス側の機密実行環境で動作している「データ管理プログラム」に対して，データを提供する．サービス側で提供されたデータを利用する際は，データ管理プログラムに対して閲覧を要求する．この際，ポリシーに基づいて閲覧を許可するかどうかを判断し，判断の結果を「ログサーバ」に送信する．ログサーバはログを記録し，データ管理プログラムに対して記録が完了した旨を通知する．最後に，この通知を受け取ったデータ管理プログラムがデータを表示する．また，サービス側が別のノードにデータをコピーしようとする際も，同様に管理プログラムによって可否が判断され，判断の結果がログサーバに送信される．

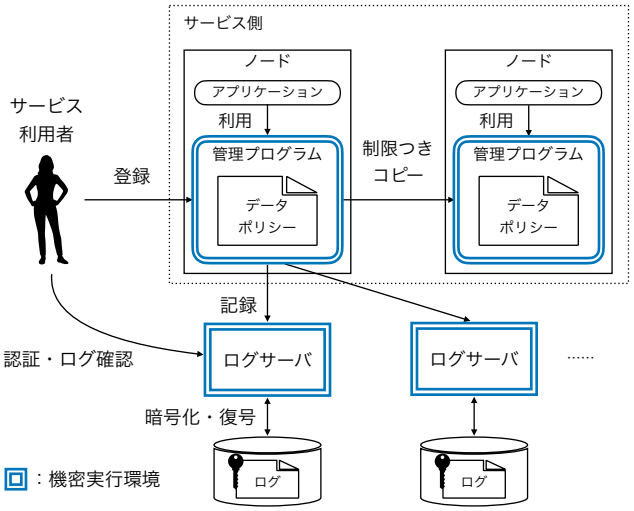

図 1　機密実行環境を利用したデータのコピー制限と利用記録の実装

サービスの利用者は，ログサーバに要求を送ることによって，自身のデータに対する利用記録を閲覧できる．このとき第三者のデータに紐づいた操作のログが返されることを防ぐため，ログサーバは利用者を認証し，アクセス制御を行う．結果として，自身のデータに対する操作のログのみが返され，閲覧できる．

サービス側のノードや，ログサーバが動作するノードは，データ提供者にとって信頼できるものではない．2 章で述べたように，プログラムの改変やプロセスの停止などの試みによって，操作の制限やログの記録が妨害される可能性

[1] 筑波大学
University of Tsukuba

がある．このような，信頼できない場所でもプログラムを完全に動作させるために，機密実行環境を利用する．データ管理プログラムとログサーバのプログラムを機密実行環境で動作させることによって，2 章で述べた攻撃に対応する．

3.2 データ管理プログラム

データ管理プログラムは，サービス利用者から提供されたデータを暗号化して保存し，ポリシーの管理と操作制限を行う．外部からデータの利用要求があったとき，データ管理プログラムはまずポリシーを参照する．ポリシーには，操作の可否を判定するためのルールが記載されており，データをコピー可能な残回数や，ノードのホスト名・IP アドレスなどを用いて操作を制限できる．次に，ポリシーの判定結果にかかわらず，ログサーバに操作を記録する．最後に，記録が正常に完了した旨の返答をログサーバから返ってきたことを確認し，データを返す．

データをコピーするときも同様に，ポリシーに基づいて操作の可否を判定する．コピーの際には，文献 [1] で述べた手法を拡張した分散トランザクションを実行する．操作の最中にプロセスが終了されたり，電源やネットワークが切断されたりした場合は状態をロールバックする．また，トランザクション失敗後に操作をやり直す際は，ログサーバに記録したログを活用し，トランザクションの状態を回復して再開する．

3.3 ログサーバ

ログサーバは，データ管理プログラムによって実行された操作の記録を取る機能を持つ．データ管理プログラムから送られてきたログを受け取り，永続記憶に保存する．この永続記憶は信頼できず，ログを改竄されたり，削除されたりする可能性があるため，ログを暗号化して保存する．改竄や削除があった場合は復号に失敗するため，これらの攻撃を検知できる．

ログサーバはこのほかに，データの提供者の要求に応じてログを確認させる機能を持つ．このとき，他人のデータに対する操作のログを勝手に閲覧できないよう，閲覧者を認証し，アクセス制御を行う．

なお，ログサーバは複数動作させ，可用性を向上させる．この高い可用性はログを記録するときのみならず，データの提供者がログを閲覧するときにも利点がある．さらに，ログサーバ同士は定期的に通信し，各々が保存しているログの内容を同期する．

4. 実装

本研究では，機密実行環境として Intel Software Guard Extensions (SGX) を利用する．データ管理プログラムとログサーバのプログラムは，Rust 言語によって実装する．Rust は，言語仕様のレベルで型安全性・メモリ安全性が保証されており，この特徴はセキュリティを重視する本研究において重要である．

また，Rust から Intel SGX の機能を利用するため，Rust SGX SDK [*1]を使用する．さらに，データ管理プログラムとログサーバ間，ログサーバ同士の通信プロトコルとして，gRPC [*2]を使用する．

5. 関連研究

Custos[2] は，機密実行環境とそれに備わる暗号化機能を使用し，ログを記録する研究である．この研究は複数のノードを用いてログを分散して記録する点で，本研究と共通している．本研究では，ログの閲覧の際のアクセス制御に対応する点や，ログを利用した分散トランザクションの管理に対応する点が異なる．

6. まとめ

本研究は，ネットワーク上のサービスに提供したデータの利用・コピーを制限し操作の記録を追跡すること，ならびにこれらの機能を，可用性が高い状態で提供することを目的とする．これを実現する手法として，機密実行環境で動作するデータ管理プログラムとログサーバを実装する．

現在，管理プログラムの基本的な機能は動作している．今後の課題は，ログを活用した分散トランザクション方法および，ログサーバ間におけるログの同期を実装することである．さらに，個人情報の保護以外のアプリケーションとして，本提案手法を著作物の管理にも利用できるように拡張したいと考えている．

謝辞 本研究は部分的に JSPS 科研費 21K19756 の助成を受けた．

参考文献

[1] 石黒 淳，新城 靖：インターネットで利用可能な機密実行環境間の原子的なデータ移動，コンピュータシステム・シンポジウム論文集，Vol. 2022, pp. 1–10 (2022).
[2] Paccagnella, R., Datta, P., Hassan, W. U., Bates, A., Fletcher, C., Miller, A. and Tian, D.: Custos: Practical Tamper-Evident Auditing of Operating Systems Using Trusted Execution, Network and Distributed System Security Symposium, National Science Foundation, pp. 1–18 (2020).

[*1] https://github.com/apache/incubator-teaclave-sgx-sdk
[*2] https://grpc.io/