

コンテキストに適応可能なデータ保護機構における ファイルアクセス制御

一柳 淑美 † 鈴来 和久 ‡‡ 毛利 公一 † 大久保 英嗣 †

† 立命館大学理工学部情報学科 ‡‡ 立命館大学大学院理工学研究科

1 はじめに

近年、各種のネットワークサービスを利用するためには、ユーザのプライバシ情報やサービス情報をネットワーク上で送受信する機会が増加してきている。また、ユビキタス環境を想定した場合、サービスを提供するサーバが、ユーザにとって意図しないプライバシ情報の収集や分析を行う可能性がある。このような環境では、プライバシ情報の扱いが重要な研究課題となる。そこで、我々は、プライバシ情報の漏洩や拡散を防止する機能を有するオペレーティングシステム（以下、OSと記す）を開発している。本OSでは、上記の環境での適用を前提とするために、変化しうる状況（コンテキスト）に適応可能なデータ保護機構を実現している。ここで、コンテキストとは以下のものを意味する。

- 利用者
- 時刻
- 位置情報
- プロセスを実行している計算機

本OSでは、上記のコンテキストの監視と管理、コンテキストの変化に応じたデータ保護をOSレベルで実現し、アプリケーションの信頼性にかかわらずデータの拡散を防ぐことを目的としている。本稿では、特に、データ保護機構におけるファイル管理について述べる。

2 データ保護機構の概要

2.1 特徴

本機構では、プライバシ情報を、ユーザが、第3者やアプリケーションに知られたくない情報と定義する。このプライバシ情報を保護する手法として、認証や暗号化といったセキュリティ技術[1]、知的財産権や著作権が存在するデータのコピーを防止する技術[2]が存在する。既存の技術と比較した場合の提案手法の利点としては、以下のものが挙げられる。

- 既存のファイルシステムで使用できる。
- 特殊なシステムコールを使用しない。
- コンテキストの変化に応じた保護ができる。

File Access Control Method for Context-Aware Data Protection Mechanism

Yoshimi Ichiyanagi[†], Kazuhisa Suzuki^{‡‡}, Koichi Mouri[†], and Eiji Okubo[†]

[†]Department of Computer Science, Faculty of Science and Engineering, Ritsumeikan University

^{‡‡}Graduate School of Science and Engineering, Ritsumeikan University

アプリケーションにおけるデータ保護は、アプリケーションの信頼性が問題になる。信頼性の低いアプリケーションの場合、プライバシ情報が漏洩する可能性がある。本手法では、OSがデータ保護を行うため、アプリケーションに不具合や悪意がある場合においても、データを保護することができる。

2.2 適用例

位置情報システムを利用した周辺の地図や店舗の広告といった現在位置周辺の情報を提供するサービス例を考える。この例の場合、旅先の見知らぬ場所では、サービスの必要性が高いが、生活している場所ではサービスの必要性は低いと考えられる。また、サービス提供者がログを解析することにより、ユーザの行動パターンが特定される危険性や、ユーザの意思には関係なくユーザの位置情報が第3者に通知される可能性がある。このため、サービスで扱う位置情報をユーザが希望しない目的に利用されることを防ぐ必要がある。そこで、現在位置を注目すべきコンテキストとして扱い、コンテキストに応じてサービス実行の可否や、サービスを利用するためには送受信するデータの保護強度を制御する。これにより、ユーザの望むプライバシ保護を実現する。

次にインターネット上のショッピングサイトの例を考える。ユーザが購入した商品を配送するため、ユーザの住所や氏名をショッピングサイト側のデータベースに登録しておく必要がある。ショッピングサイトの運営者は、この登録された情報をデータベースに一定期間保存することにより、次回の購入手続き時の処理を簡略化している可能性がある。このとき、データベースにアクセス可能なアプリケーションが存在するため、プライバシ情報を読み込み、データを拡散させる危険性がある。したがって、データの拡散を防ぐために、適切なタイミングでデータベースから削除する必要がある。そこで、時刻や実行するトランザクションをコンテキストとして注目し、予めユーザが設定した条件とコンテキストが一致した場合にプライバシ情報を削除する。

3 データ保護機構の実装

3.1 全体構成

本機構では、特に、ハードディスクに格納されたファイルに対して、プログラムがデータコピーを行うことによって発生するデータの拡散と漏洩を防止する手法としてファイルのアクセス制御と削除を行う。そのデータ保護機構を、図1に示す。

本機構で実現するファイルアクセス制御のポリシは、Access Control List(以下、ACLと記す)に記述されている。ACLは、ファイルアクセスを制限するコンテキストの条件が記述されたリストである。ACLは、保護対象のファイルと対になって、共にファイルとしてハードディスクに保存されるものとする。また、ファイルを削除するきっかけとなるコンテキストの条件も、ACLと一緒にファイルに保存される。ACLとファイルを削除するコンテキストの条件が、データ保護ポリシとなる。

Context Watcherは、データ保護ポリシから必要なコンテキストを取得する。そして、そのコンテキストを監視し、変化を Action Control Mechanism に通知する。Action Control Mechanism は、その通知されたコンテキストに応じて、データ保護ポリシに基づいたファイルのアクセス制限や削除を行う。

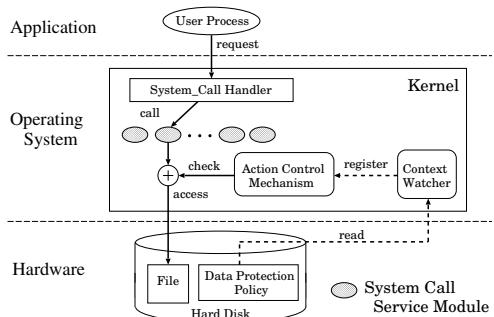


図 1 データ保護機構の概要

ユーザプロセスがファイルにアクセスする場合、カーネルが提供するシステムコールを用いる。このため、本OSでは、システムコールをフックし、ユーザプロセスのファイルアクセスの制限とファイル削除を行うことによりデータ保護を実現する。

3.2 ファイルアクセス制御

open システムコールの処理手順を以下に示す(図2参照)。

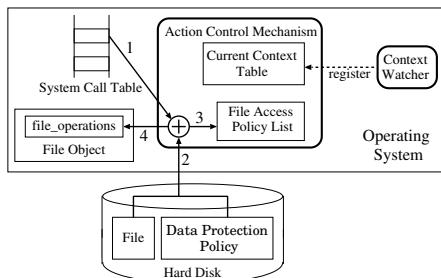


図 2 open システムコール処理

1. open システムコールをフックする。
2. ファイルとデータ保護ポリシが記述されたファイルをオープンする。いずれかのファイルがオープンできない場合は、保護の必要がないと判断し、通常の open システムコールの処理を行う。
3. データ保護ポリシ、オープンするファイルのファイルオブジェクトのアドレス、プロセス ID を File Access Policy List に登録し、データ保護ポリシが記述されているファイルをクローズする。

4. File Access Policy List に登録されているデータ保護ポリシと Current Context Table に登録されているコンテキストに応じて、ファイルオブジェクトに登録されている read/write サービス関数へのポインタを削除した後、open システムコールの処理を継続する。また、ファイルがクローズされるまで、コンテキストの変化とデータ保護ポリシに基づき、定期的に read/write サービス関数へのポインタの登録や削除を行う。

保護するファイルに対して read アクセスが行われた場合、保護すべきファイルのデータがユーザプロセスのデータ領域に保存されている可能性がある。このとき、Action Control Mechanism は、write システムコールをフックし、保護するファイルのデータ保護ポリシに応じて write システムコールを制限する。

3.3 ファイル削除

保護ポリシが記述されているファイルに、ファイルを削除するコンテキストの条件が記述されている場合がある。このコンテキストの条件が満たされた場合、Action Control Mechanism はファイルを削除する。ただし、すべてのファイルを常時監視することが不可能なため、Action Control Mechanism は、保護するファイルをオープンしているユーザプロセスが存在している場合、強制的にファイルを削除する。存在しない場合、ユーザプロセスがファイルをオープンするのをきっかけとしてファイルを削除する。本手法は、以下に示す資源に対して適用する。

- ハードディスク
- メモリに保存されているディスクキャッシュ
- 当該ファイルに read アクセスしていたユーザプロセスのデータ領域・スワップ領域

しかし、ユーザプロセスのデータ領域の初期化を行うと当該プロセスは処理の継続が不可能となる。このとき、Action Control Mechanism は、ファイルのデータ保護ポリシによって、プロセスが終了するまで当該データ領域の初期化を行わない。

4 おわりに

本稿では、コンテキストの変化に適応したデータ保護機構の概要と構成について述べた。提案手法を適用することにより、OS がファイルのアクセス制御と削除を行い、プライバシ保護を実現する。現在、ファイルアクセス制御のプロトタイプを Linux のローダブルカーネルモジュールを用いて実装中である。

参考文献

- [1] Simson Garfinkel: “PGP: Pretty Good Privacy,” O'Reilly & Associates(1995).
- [2] 森 亮一, 河原 正治, 大瀧 保広: “超流通: 知的財産権処理のための電子技術,” 情報処理学会, pp. 155–161(1996).