2ZA-5

動的テイント解析とOSの連携による情報漏洩防止手法の提案

大石 達也† 樫山 武浩† 瀧本 栄二† 毛利 公一†
†立命館大学

1 はじめに

近年，個人情報は電子化され，計算機により管理されている．それに伴い，電子化された個人情報が漏洩する事件が多発している．文献 [1] では，情報漏洩の要因として，管理ミス，アプリケーションの誤操作，紛失・置き忘れ，盗難などが挙げられている．特に，管理ミス，誤操作，紛失・置き忘れは，正当な権限を持つ者によって引き起こされる人為的なミスであり，それらが 80 %という高い割合で占めている．しかし，暗号や認証といった既存のセキュリティ技術は，外部からの攻撃を防止することを目的としているため，人為的なミスによる情報漏洩を防止することは困難である．

以上の背景から，我々は，人為的なミスによる情報漏洩を防止することを目的としたオペレーティングシステム TA-Salvia の開発を行っている．

2 TA-Salvia

2.1 概要

TA-Salvia は，OS で個人情報などのデータの漏洩を防止する．TA-Salvia のデータ保護モデルを図 1 に示す．TA-Salvia は，保護すべきデータを含むファイル（以下，保護ファイル）を保護対象とする．また，OS が保護ファイルを読み込んだプロセスを制御対象する．具体的には，プロセスを監視し，ファイル，ソケット，パイプなどの計算機資源への出力を制御することにより，データの漏洩を防止する．

2.2 データ保護ポリシ

保護すべきデータは，ユーザや計算機の状況によって利用目的や提供範囲が異なるため，データごとに異なるアクセス制御をプロセスに課す必要がある．そこで，TA-Salvia では，データの保護方針を定義したデータ保護ポリシ（以下，ポリシ）をファイル単位で設定することを可能とする．

ポリシには，データを読み込んだプロセスに対して，計算機やプロセスの利用状況に応じたアクセス制御を適応する条件を記述する．条件としては，プロセスを制御するための条件としてユーザ ID，ネットワークなどコンテキストを設定する．

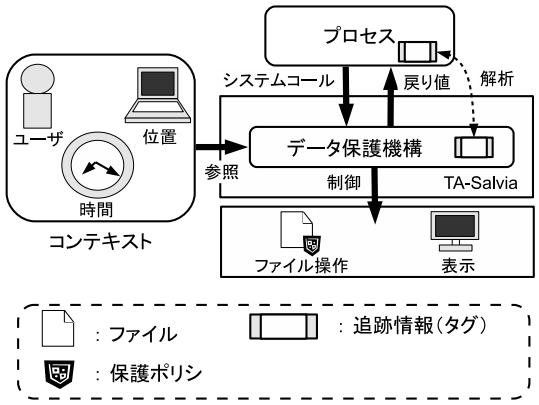

図 1 TA-Salvia のデータ保護モデル

2.3 アクセス制御

データ保護機構では，プロセスが発行するシステムコールをフックすることで，OS 上で動作する全てのプロセスに変更を加えることなくデータ保護を実現している．

プロセスからファイルのデータを読み込むシステムコールが発行されたときは，保護ファイルのデータを扱うプロセスを監視する．そして，データを計算機資源へ書き込むシステムコールが発行されたときは，出力されるデータの発生源である保護ファイルを特定し，それに設定されたポリシに従ってアクセス制御を課す．

3 動的テイント解析

プロセスがデータを計算機資源へ出力する際に，その出力を制御対象否かを判定するには，出力されるデータの発生源までデータの流れ（以下，データフロー）をさかのぼる必要がある．本稿では，動的テイント解析を用いて実現する．テイント解析は，追跡するデータをテイント（汚染）とみなし，プログラムの実行中にそのデータフローを追うことで，そのデータがどのような影響を与えたかを解析する技術である．テイント解析では，追跡対象のデータに対してタグやラベルといったテイント情報を関連付け，プログラム実行時のデータの依存関係に従いテイント情報を伝播させる手法が用いられている．TA-Salvia におけるテイント情報は，どの保護ファイルからのデータであることを示すためのポリシ識別情報として用いる．データを計算機資源へ書き込むシステムコールが発行されたときに，

A Proposal for Method to Prevent Information Leakage by Cooperation with Dynamic Taint Analysis and OS
Tatsuya OISHI†, Takehiro KASHIYAMA†, Eiji TAKIMOTO†and Koichi MOURI†
†Ritsumeikan University.

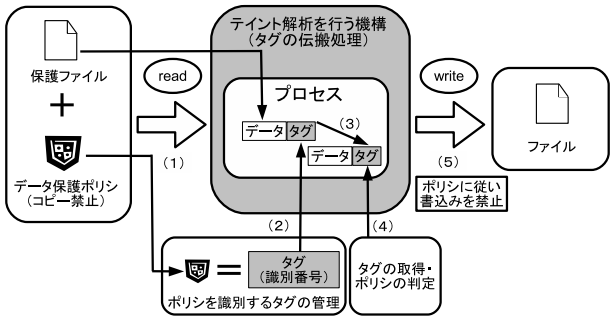

図 2　TA-Salvia によるアクセス制御の手順

ポリシ識別情報を保護対象のデータと関連付けて追跡することで，データの出力時に，その情報からデータの発生源となった保護ファイルのポリシを特定し，そのデータの条件に応じたアクセス制御を課すことでデータの漏洩を防止する．

4　処理方式

TA-Salvia によるアクセス制御の手順を図 2 に示す．また，以下に処理内容を示す．

1. TA-Salvia で保護ファイルのデータを読み込む read システムコールが呼び出されたとき，その保護ファイルに設定されいるポリシとそのポリシを特定するタグを対応付けて管理する．
2. タグは，保護対象のデータフローを追跡するために読み込まれたデータに対して関連付けられる．
3. 関連付けられたタグは，プログラムが実行毎に，テイント解析を行う機構でタグの有無を確認し，データの依存関係に従って他のデータに伝播される．
4. 情報漏洩の可能性がある操作，write システムコールが実行された場合，読み込むデータに対して関連付けられたタグの有無を確認する．
5. タグが登録されている場合は，保護対象のデータが含まれている可能性があるため，タグと対応するポリシに従ってシステムコールの実行の可否を判定し，アクセス制御を行う．

タグは，それぞれのポリシを識別するために用いる．TA-Salvia は，タグに任意の番号を割り当て管理する．保護対象外のデータは，テイント解析を行う機構にてデータフローの追跡を行わないようにする必要があるため，タグにゼロの値を設定する．

5　実装方法

動的テイント解析は，オーバヘッドが大きくなるがハードウェア拡張することで高速化が実現されている [2]．本稿では，このハードウェアでの動的テイント解析を前提として開発している．このため，以下を実現する必要がある．

- ハードウェアの物理メモリとレジスタの記憶領域に対応するテイント解析用の記憶領域を用意できること．このテイント解析用の記憶領域は，ポリシを識別するタグを格納することを可能とする．
- テイント解析用の記憶領域のタグを伝播させる機能を有するプロセッサを用意できること．本稿では，プロセッサにテイント解析の機能が実装されていること前提とする．
- OS からテイント解析用の記憶領域にタグを読書きするためのインタフェースをハードウェアが用意できること．このインターフェースを用いて，プロセスが保護ファイルのデータを読み込む際に，そのデータを格納された記憶領域に対応するテイント解析用の記憶領域を指定してタグを付加する．また，データが格納された記憶領域からデータを読み込む場合も同様に，対応するテイント解析用の記憶領域を指定してタグを取得する．これにより，保護データを追跡するこを可能とする．

本稿では，ポリシを識別するタグ伝搬をテイント解析を用いたハードウェアエミュレータである Argos[3] を改良して実現することを計画する．

6　おわりに

本稿では，TA-Salvia が動的テイント解析を用いて，データが出力される際に元のファイルごとに設定されているポリシを特定し，そのポリシに従ってアクセス制御を課すことで人為的ミスを要因とした情報漏洩を防止することを述べた．今後は，実装を進めていく予定である．

参考文献

[1] NPO 日本ネットワークセキュリティ協会: “JNSA 2010 年度情報セキュリティインシデントに関する調査報告書，” http://www.jnsa.org/result/incident/data/2010incident_survey_PIL_v1.4.pdf, 2010.

[2] G. Edward Suh, Jae W. Lee, David Zhang, Srinivas Devadas: “Secure Program Execution via Dynamic Information Flow Tracking ,”In Proceedings of the 11th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-XI), pages 85–96, 2004.

[3] Georgios Porgokalidis, Asia Slowinska, Herbert Bos: “Argos: An emulator for fingerprinting zero-day attacks,” In Proc. ACM SIGOPS EUROSYS’2006, pages 15–27, Leuven, Belgium, April 2006.