

プライバシー保護のための OS における ネットワーク機構

西村 和憲[†] 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 ^{††} 立命館大学大学院理工学研究科 ^{†††} 立命館大学情報理工学部

1 はじめに

近年、ユーザがネットワーク上で種々のサービスを受けたり、企業が作業の効率化を図るために、ユーザのプライバシー情報が電子化されている。そのため、ユーザのプライバシー情報が、電子メールやファイル転送などの方法でネットワーク上へ流出する危険性が生じている。ユーザのプライバシー情報の漏洩は、ユーザだけでなく、企業にもイメージダウンやその存続に関わるような大きな被害が生じる。従来のセキュリティ技術では、盗聴・侵入・破壊・改ざん・なりすましなどの不正な操作による情報の漏洩・拡散を防ぐことが可能である。しかし、ユーザの誤操作や正当なユーザによる悪意のある操作、データ漏洩を考慮していないアプリケーションによるデータ漏洩を防ぐことは困難である。

また、プライバシー情報を利用する計算機が移動したり、種々の計算機と通信することで、ユーザの状況、計算機の種類、プロセスの通信状態が変化する。このような変化に応じて、計算機に保存されているプライバシー情報が漏洩する危険性も変化する。このような状況下においても、データを保護する必要がある。

我々は、従来のセキュリティ技術に加えて、計算機やユーザの変化しうる状況（コンテキスト）に適応したデータ保護を実現し、プライバシー情報を作成・所有する者（以下、データ作成者）の意図に反するデータ送信を防止する手法に関して研究している。特に、コンテキストに適応したアクセス制御によりデータ漏洩を防止するオペレーティングシステム（以下、OS）を開発している [1]。本稿では、OS 内の通信に関するシステムコール処理において、データ通信を制御する機構を実装することにより、プライバシー情報の漏洩を防ぐ手法を提案する。本手法は、OS 内で制御するため、アプリケーションの信頼性を問わずに制御できる。また、既存のアプリケーションにも適応可能である。本手法により、データ作成者は、保護するファイルごとに、特定の IP アドレス以外には送信禁止とすることができる。また、重要なデータをデータ作成者が許可していない計算機や悪意をもった権限の

あるユーザに送信することや、データ作成者が許可していないユーザが、このデータを送信することを防ぐことができる。

2 想定シナリオ

ネットワークを介してユーザの誤操作・正当な操作により、データが漏洩するシナリオを以下に述べる。

ユーザ A は、会社の建物内で顧客情報のような保護を必要とするデータ（以下、保護データ）を用いて、作業している。ユーザ A は、同じ建物にいる上司に作業内容を報告するため、保護データと作業内容を送信した。また、ユーザ A は、自宅で作業を進めるため、保護データを自宅の FTP サーバにファイル転送した。

これは、重要なデータが容易に持ち出し可能であることを示す。また、ユーザ A が使用した FTP アプリケーションが、悪意のあるアプリケーションならば、自宅の FTP サーバ以外のサーバに勝手にコネクションを張られ、ファイルを転送する危険性が生じることを示している。

このシナリオで、データの漏洩を防止するために着目すべき点には、次のものがある。

- ユーザ A のファイルを送信する権限の有無
- 保護データの重要度
- 通信先計算機の IP アドレス

これらに着目することで、ファイルの重要度に応じて、許可された IP アドレスのみにファイルの送信を許可するといったユーザごとの保護ができる。具体的には、社内間でのデータの送受信と、保護が必要でないデータを社外へ送信することは許可するが、社内から社外へ保護データを送信することは禁止するといった保護ができる。このデータ保護手法を適用することにより、顧客情報のような保護データを会社の建物の外へ流出することを防止できる。

3 通信におけるコンテキストに適応したデータ保護

3.1 全体構成

データ保護機構は、Linux カーネル 2.6.6 に変更を加えた形で実装し、コンテキスト管理部（Context Watcher）とプロセス挙動制御部（Action Control Mechanism）から構成される。コンテキストに適応可能なデータ保護機構の全体構成を図 1 に示す。保護対象ファイルは、データ保護ポリシーに記述されたポリシーに従って保護されている。データ保護ポリシーとは、データ作成者の意図を記述

Network Mechanism in Privacy-Aware OS

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

[†] Faculty of Science and Engineering, Ritsumeikan Univ.

^{††} Graduate School of Science and Engineering, Ritsumeikan Univ.

^{†††} College of Information Science and Engineering, Ritsumeikan Univ.

したファイルであり、ファイルとしてハードディスクに保存されている。コンテキスト管理部は、必要なコンテキストを取得し、プロセス挙動制御部にコンテキストを通知する。このとき、コンテキスト管理部は、コンテキストリストにシステムコールの履歴を登録する。プロセス挙動制御部は、コンテキスト管理部から通知されたコンテキストとデータ保護ポリシーを比較してシステムコールの実行許可・不許可を判断する。以上の構成要素により、コンテキストに適応したデータ保護を実現する。

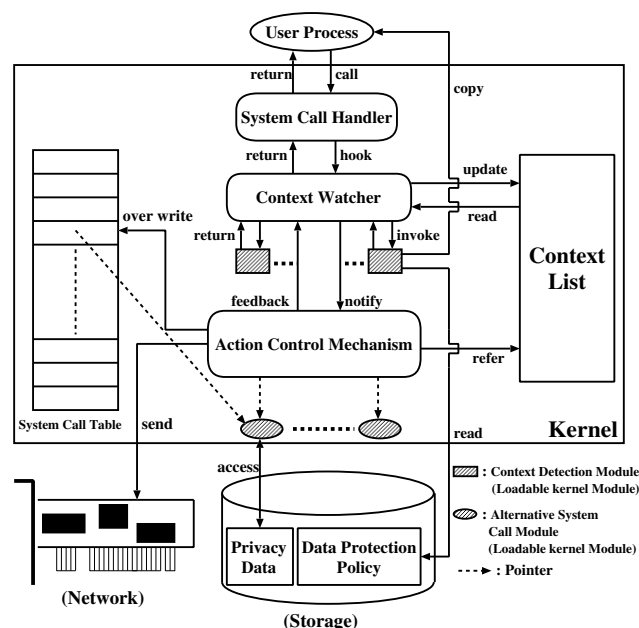


図 1 システム構成

3.2 ネットワークにおけるコンテキスト

通信におけるコンテキストに適応したデータ保護において、通信処理を制御するために着目するコンテキストは次のとおりである。

- ユーザ ID
- 実効ユーザ ID
- 時刻
- 通信先計算機の IP アドレス
- システムコールの履歴

これらをコンテキストとして、コンテキスト管理部が取得することで、次の 3 つのデータ保護を行うことが可能である。(1) システムコールの履歴から `sys_socket()` の戻り値であるソケットディスクリプタの取得によって、複数のソケット通信を行っていても、一意に通信先ポート番号や通信先 IP アドレスを識別することが可能である。そのため、通信アプリケーションの特定ができ、暗号化通信なら許可し、暗号化されていない通信ならば禁止するといった制御が可能となる。(2) 通信先計算機の IP アドレスの取得によって、送信先計算機の指定が可能である。(3) コンテキストリストからシステムコールの履歴を取得することにより、保護するファイルが読み出さ

れていることが把握できるため、このファイルのデータ漏洩を防止できる。

3.3 通信における制御手法

3.2 節で述べたコンテキストを用いて、通信におけるデータ保護を実現するために、`sys_socketcall()` システムコールの処理内で通信の可否を制御する。また、通信におけるデータ漏洩を防ぐためにコネクションを確立する処理とデータを送信する処理を制御する。コネクションを確立する場合のサービス関数には、`sys_connect()` がある。また、データを送信する場合のサービス関数には、`sys_send()`、`sys_sendmsg()`、`sys_sendto()` がある。

コネクションを確立するサービス関数やデータを送信するサービス関数の実行が許可された場合、通常のサービス関数（`sys_connect()`、`sys_send()` など）が呼ばれる。また、コネクションを確立するサービス関数やデータを送信するサービス関数の実行が禁止された場合、`sys_socketcall()` システムコールが呼ぶ従来のサービス関数の代わりに、通信を制御するための関数が呼び出され、その実行を禁止する。

コネクションを確立する場合、発行された `sys_connect()` の引数より、通信先の IP アドレスと通信先のポート番号を取得する。次に、保護するファイルが読み出されているかをコンテキストリストから検索する。保護するファイルが読み出されていた場合、そのファイルが送信される危険性があるため、コネクションを確立する段階で、保護ポリシーに応じた制御を行う。このとき OS は、どのファイルを送信しようとしているのか把握できないため、同一プロセスにおいて保護を必要とするファイルが読み出された履歴があれば、コネクションを確立する処理を制御する。

データを送信する場合、コネクションが確立してからデータが送信されるまでの間に、保護するファイルが読み出されたり、他の通信が開始されている可能性がある。このため、データを送信するサービス関数と同じソケットディスクリプタを持つ `sys_connect()` の引数（通信先 IP アドレス、通信先ポート番号）をコンテキストリストから取得し、`sys_connect()` と同様の手法で、データを送信する制御を行う。

4 おわりに

本稿では、コンテキストに適応した OS のネットワーク機構において、着目すべきコンテキストや制御の手法について述べた。この手法により、動的に変化するコンテキストと静的な保護ポリシーとを比較することで、動的なデータ保護を実現することが可能である。

参考文献

- [1] 鈴木 和久, 毛利 公一, 大久保英嗣: “プライバシー保護を実現するオペレーティングシステムにおけるコンテキスト管理手法,” 情報処理学会研究会報告 2004-OS-96, Vol.2004, No.63, pp.7-14(2004).