

コンテキストウェアオペレーティングシステムのための割込みを契機としたコンテキスト取得法

岩永 真幸[†]鈴木 和久^{††}毛利 公一^{†††}[†] 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、ユーザの個人情報や、企業の顧客情報や機密情報が漏洩する事件が多発している。このような背景から、2005年4月より個人情報保護法が施行された。企業は、情報を漏洩させると顧客の信用を大きく低下させてしまうため、情報漏洩の防止に力を入れている。しかし、情報漏洩事故は頻繁に発生している。

情報漏洩事故は、情報漏洩が発生した原因とその経路によって分類可能である。例えば、原因として人為的なもの(過失、不正行為)や、セキュリティ侵害(不正アクセス、ウイルス、ワーム)が挙げられる。特に、原因が人為的である場合、正当なアクセス権限を持つユーザによって情報漏洩が発生するため、既存技術による対策は困難である。また、経路として記録媒体(紙、光学ディスク、USBフラッシュメモリなど)や計算機自体の紛失・盗難、ネットワークへの情報流出などがある。特に、可搬性の高い記録媒体やネットワークは、情報の拡散が極めて早いという特徴があるため、それらを介した情報漏洩を防ぐことの意義は高い。

これらの原因、経路による情報漏洩を防ぐためには、情報漏洩が発生させる危険性の高い操作を禁止する、あるいはその危険性が高い計算機資源に対する書込みアクセスを制御する必要がある。現在、我々が開発しているOS Salvia [1] は、ファイルを保護の単位とし、ファイルごとに定義された保護ポリシーに基づき、当該ファイルにアクセスしたプロセスに対してアクセス制御を課す。その際、プロセスの動作(システムコール要求)が情報漏洩が発生させる危険性があるか否かを判定するために、Salviaではコンテキストを利用する。本論文では、コンテキストの取得方式について述べる。

2 Salviaのデータ保護方式

2.1 システムコール制御

Salviaは、システムコールの制御によりデータ保護を行う。ファイルに対するシステムコールが発行されると、コンテキストと保護ポリシーを比較し、システムコールの

実行の可否を判定する。

保護ポリシーには、システムコールごとにコンテキストを用いて、制御条件が記述されている。コンテキストを使用することで、ファイルに対する不正なアクセスである状況を記述することができ、危険性の高い状況でのシステムコールの実行を禁止できる。

2.2 コンテキストとデータ保護ポリシー

コンテキストには、計算機やプロセスの状況を示すパラメータとして、ユーザ、位置、時刻、IPアドレス、プロセスの動作履歴などがある。例えば、保護ポリシーによって社内のIPアドレスにのみ送信を許可することで、ネットワークによる情報の漏洩を防止することができる。また、データ提供者以外のユーザは読み込み可能であるが、書込みや他のプロセスとのデータ共有を禁止することで、提供者以外の人はファイルを見ることができず、改竄や記録媒体への書込みを禁止できる。さらに、社内でのみファイルの読み込みを許可することで、盗難によるデータ漏洩を防止したり、会議室内でかつ会議中のみファイルの読み込みを許可することで、会議で使用する重要なデータの漏洩を防止することもできる。

このようなコンテキストを用いたポリシーの記述によって、1章で述べた原因や経路による情報漏洩を防止する。位置やユーザのコンテキストは、無線LAN、RFIDなどのデバイスから取得可能な情報を用いて表現する。

3 コンテキスト取得方式

3.1 外部割込みを契機とするコンテキストの取得

周辺デバイスからコンテキストを取得する場合、ポーリングによってコンテキストを取得すると、その頻度が上がるにつれてオーバーヘッドが大きくなる。そこで、デバイスが割込みを生成する点に着目し、割込みを契機としてコンテキストを取得する方法を提案する。これにより、コンテキストの変化に応じた取得が可能となる。

3.2 解決すべき課題

本手法では外部デバイスから割込みが発生すると、コンテキストを取得する。しかし、割込みに対する処理内容は、デバイスや接続方法によって異なる。したがって、割込みを種類ごとに区別し処理する機能が必要となる。そこで、現在、コンテキストを取得することを想定しているデバイスを挙げる。

- 無線LAN
無線LAN基地局のESSIDと電波強度を利用する

A Context Acquisition Method in Interrupt Handler for Context-Aware OS

Masayuki Iwanaga[†], Kazuhisa Suzuki^{††}, and Koichi Mouri^{†††}

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

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

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

ことで、位置情報を取得する。ESSID からアクセスポイントを特定し、電波強度からアクセスポイントと計算機の距離を取得することができる。ESSID と電波強度を合わせて1つのコンテキストとし、特定の無線 LAN 基地局からの距離を位置コンテキストとして利用できる。特定したい場所に無線 LAN を設置することで、その周辺に計算機が存在することを認知することが可能となる。

● GPS

GPS は、測位データから軽度、緯度、高度を示す値を取得できる。この値から現在の位置を特定することができる。絶対的な位置を取得でき、電波の届く屋外で利用できる。

● RFID

RFID はタグにユーザや位置を特定するデータを記録させ、そのデータを読取ることによって位置やユーザコンテキストとして利用することができる。例えば、机にパッシブタグを埋込むことで計算機の位置コンテキストとして利用したり、アクティブタグのある部屋の壁などに埋め込むことで計算機が特定の場所に存在する位置コンテキストとして利用したりできる。また、ユーザタグを所持し、ユーザが計算機に接続された受信機にパッシブタグをかざすことで、ユーザコンテキストとして利用することもできる。

● Bluetooth

Bluetooth も読み取るデータを位置やユーザコンテキストとして取得できる。例えば、Bluetooth によってユーザや位置を特定するデータを送信することで、ユーザや位置コンテキストとして利用する。コンテキストの利用状況は、RFID と似た状況を想定しており、Bluetooth をユーザごとに所持しユーザコンテキストを取得するか、机や部屋に埋込むことで位置コンテキストを取得する。

表 1 に上記のデバイスの接続方法を記す。以上のデバイスと接続方式によって割込み発生時の処理を区別することによって、コンテキストを取得することが可能となる。

3.3 実装方式

Salvia は、Linux カーネル 2.6.8 を基に拡張している。Linux の割込みの仕組みを図 1 に示す。割込みが発生すると irq_desc テーブルを参照して割込みハンドラを呼び

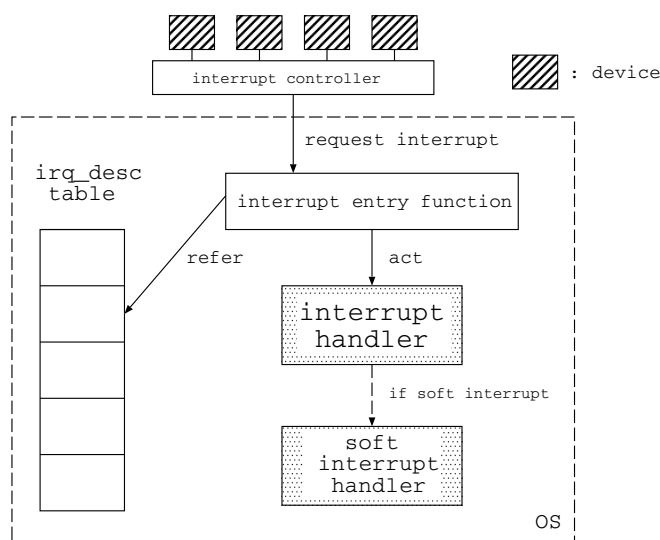


図 1 割込み処理

出す。外部デバイスが割込みを発生させた場合の割込みハンドラは、割込みを発生させたデバイスドライバである。割込みには、応答性を必要とする処理を割込みハンドラで実行し、応答性を必要としない処理は後でソフト割込みハンドラで行うものが存在する。コンテキストの取得は、割込みハンドラあるいはソフト割込みハンドラの中に実装する。実装には、デバイスを区別しコンテキストの取得が必要なデバイスのみ取得する機能が必要である。これにより、前節で述べたデバイスや接続方式にかかわらずコンテキストを取得することが可能となる。

デバイスドライバは、キャラクタ型デバイスとブロック型デバイスに分類することができる。キャラクタ型デバイスはデータを 1 バイトずつ処理するため、1 バイトずつ流れてくるデータの中からコンテキストを取得する必要がある。また、ブロック型デバイスは、データをブロック単位で処理するので、ブロックデータの中からコンテキストを取得する必要がある。これにより、割込みを契機としたコンテキストの取得が実装可能となる。

4 おわりに

本論文では、データの漏洩を防止するためにコンテキストを用いることの有用性について述べ、外部デバイスから割込みを契機としてコンテキストを取得する方法について述べた。本手法により、OS 内で外部デバイスからのコンテキストを利用することが可能となる。

参考文献

- [1] 鈴来和久, 一柳淑美, 毛利公一, 大久保英嗣: Privacy-Aware OS Salvia におけるデータアクセス時のコンテキストに基づく適応的データ保護方式, 情報処理学会論文誌: コンピューティングシステム Vol.47 No. SIG3, PP.1-PP.15 (2006 年 3 月)。

表 1 デバイスの接続方法

無線 LAN	USB, PCMCIA
GPS	PCI, USB, PCMCIA
Bluetooth	PCI, USB