安全なソフトウェア流通実行システム SoftwarePot

中村 理 (lee@osss.is.tsukuba.ac.jp) †1
神田 勝規 (kanda@osss.is.tsukuba.ac.jp) †1
大山 恵弘 (oyama@yl.is.s.u-tokyo.ac.jp) †3
加藤 和彦 (kato@is.tsukuba.ac.jp) †2,†4

1. 概　　要

近年，インターネットに代表されるオープンなネットワークが普及している．このため，様々な作者によるソフトウェアの流通やネットワークを通じた計算機へのアクセスが盛んになっている．流通しているソフトウェアの中には，悪意を持って計算機の資源へアクセスを行うものや，悪用されることで計算機システムを乗っ取ることが可能な脆弱性をもつ物も存在する．

このため，私達の研究グループでは，オープンなネットワーク上で流通されるソフトウェアを安全に実行するためのシステムである SoftwarePot を開発している．SoftwarePot は，完全には信頼することのできないソフトウェアの実行を資源へのアクセスを制限した仮想的な実行環境 (ポット空間) で行う (図 1)．たとえば，ポット空間内で動作するソフトウェアからは，ローカルのファイルシステムとは異なる仮想的なファイルシステムが見える．仮想的なファイルシステムのファイル名とファイル実体との対応付けは，ソフトウェア実行時に決定することができる．この対応付けを適切に指定することで，ソフトウェアの実行に必要の無いファイルを隠蔽したり，ファイルの必要な一部分だけをソフトウェアに見せたりすることができる．ほかにアクセスを制限できる資源として，ネットワーク資源が挙げられる．このような資源へのアクセス制限はセキュリティポリシーとしてユーザーから与えられる．仮想的な実行環境と資源へのアクセス制御は，システムコールの引数の検査と書き換えによって実装されている．SoftwarePot によるソフトウェアの実行制御の様子を図 2 に示す。

SoftwarePot はソフトウェアから透過的なミドルウェアとして実現されている．そのため，SoftwarePot の中で動作するソフトウェアは，特別な言語または，ライブラリを使用する必要がなく，既存のレガシーバイナリを SoftwarePot で動作させることができる．

また，SoftwarePot ではソフトウェアをポットファイルとよばれるアーカイブファイル形式で流通する．ソフトウェアの利用者は，このポットファイルを直接実行することで，ソフトウェアを計算機システムにインストールすること無く実行することができる．このため，ソフトウェアのインストールによって，計算機システムが不正に改竄されたり，不安定になったりすることを防ぐことができる．

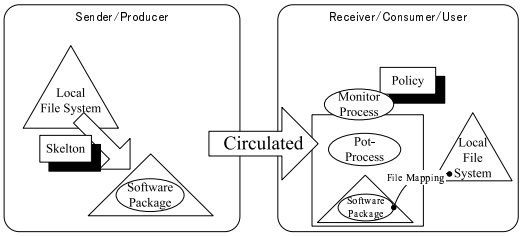

図 1　SoftwarePot の概観

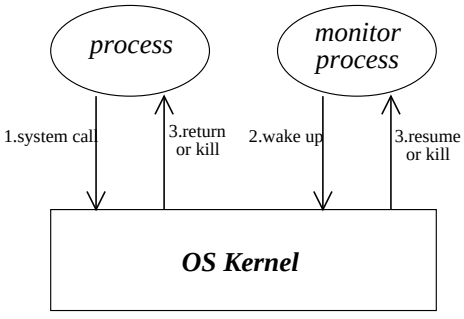

図 2　SoftwarePot によるソフトウェアの実行制御

†1 筑波大学 大学院 博士課程システム情報工学研究科
Doctoral Program in System and Information Engineering, University of Tsukuba
†2 筑波大学 電子・情報工学系
Institute of Information Science and Electronics, University of Tsukuba
†3 東京大学 大学院 情報理工学系研究科
Graduate School of Information Science and Technology, University of Tokyo
†4 科学技術振興事業団 さきがけ研究 21
Japan Science and Technology Corporation, Presto