# 異なる計算機間で正常動作情報を共有する異常検知システム

大田原　渉1　　大山　恵弘 1

## 1. 背景と目的

アプリケーションのシステムコールを監視しながら動作するセキュリティシステムについてはこれまでに多くの研究がなされている。アプリケーションの正常な実行におけるシステムコールの挙動を学習することで異常を検知する手法も多くの研究で広く用いられている[1]。しかし、既存手法においては正常動作を異常として検知することもあり、更なる精度の向上が求められている[2]。さらに正常な動作を学習させるのに手間がかかるという問題があった。

本研究ではアプリケーションの監視によって得られたデータを、同じアプリケーションを監視するシステム間で共有して防御に役立てるような異常検知システムを提案する。様々な計算機から来る正常動作の情報を集めて作られたデータベースをサーバで管理することで、正常動作データベースの精度の向上を図る。異常検知にはシステムコールの N-gram を用いる[3]。

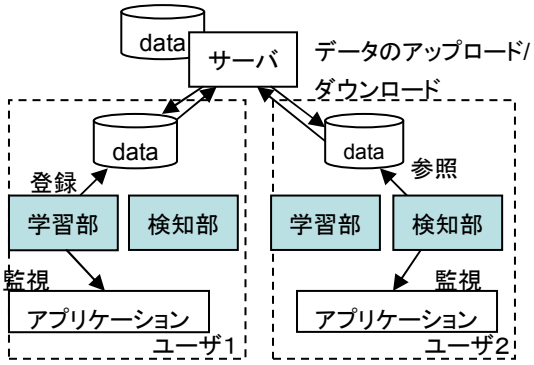
## 2. 設計方針

本システムは学習部と検知部により構成される。

### 2.1 学習部

ptrace システムコールを用いてアプリケーションを監視し、呼び出されるシステムコールを順に取得する。順番に N 個並んだシステムコールを 1 つの組として、それを自分の計算機が持つデータベースにその組の出現回数と共に記録する。そのデータベースの情報は定期的にサーバにアップロードされる。アップロードの際には OS やアプリケーションの名前、送信元の情報も同時に送信する。

サーバでは複数の計算機から送られてきたシステムコール列を集め管理する。サーバのデータベースは定期的にユーザの計算機にダウンロードされ、個々のユーザが持つデータベースにその情報を反映させる。




図：本システムのイメージ

### 2.2 検知部

学習部と同様にアプリケーションを監視する。システムコール列がデータベースに存在するか否かを調べ、存在しなかった場合は危険であると判断し警告を出し、それをデータベースに登録するか否かをユーザに問い合わせる。

## 3. 現状と今後

現在は学習部によって得られたシステムコール列をサーバへ送信する部分までの実装、および大まかな検知部の実装が終了した段階である。

サーバと検知部の実装を進め、本システムを用いた場合のオーバーヘッド等の測定を Apache 等の実際のアプリケーションを対象にして行おうと考えている。

### 参　考　文　献

[1] Michael E. Locasto et al., Software Self-Healing Using Collaborative Application Communities, DARPA Application Communities Workshop, October 2004.

[2] Christina Warrender et al., Detective Intrusions Using System Calls: Alternative Data Models, IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 133-145, 1999.

[3] Stephanie Forrest et al., Intrusion Detection using Sequences of System Calls, Journal of Computer Security, Volume 6, Number 3, pp. 151-180,1998.

1 電気通信大学大学院情報工学専攻