サーバを利用したアンチウイルスシステム

菊池 剛1　　大山 恵弘1

1. はじめに

近年、多くのコンピュータウイルスによる被害が発生しており、PC の利用にはアンチウイルスの稼働は欠かせないものとなっている。

しかし、アンチウイルスの稼働には多くの CPU やメモリを消費するため、性能の低い PC では他の処理が重くなってしまう。また既存のアンチウイルスでは新しいウイルスに対応するためにウイルス情報のアップデートを頻繁に行わなければならないといった問題がある。

そこで本研究では、サーバを利用したアンチウイルスシステムを提案する。クライアントではウイルス検査の処理を行わず、アクセスしたファイルや通信の内容をサーバに送るのみとする。そしてサーバ上でウイルスチェックを行う。そうすることによって CPU やメモリの負荷の削減、サーバ上のウイルス情報をアップデートするだけで常に最新のウイルスに対応可能といったメリットが得られる。

2. 基本設計

本システムは Linux/x86 を対象とする。本システムの全体図を図 1 に示す。動作は以下のようにクライアントでの処理とサーバでの処理の 2 つに分けられる。

2.1 クライアント

アプリケーションプロセスが作成された場合、そのプロセスの監視を行うモニタプロセスも作成し、1 つのアプリケーションプロセスを 1 つのモニタプロセスが監視する。モニタプロセスは ptrace システムコールを用いてアプリケーションプロセス

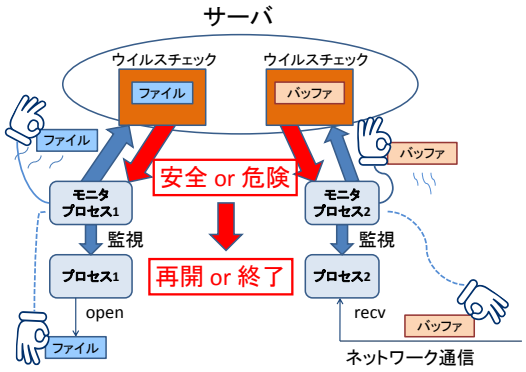

図 1: 本システムの概要

のシステムコールを監視し、ファイルアクセスやネットワーク通信が行われたらプロセスをいったんストップさせ、内容をサーバに送る。

その後サーバからの結果を受け取り、安全ならばプロセス再開、危険ならばプロセスを終了させるといった処理を行う。

2.2 サーバ

送られてきたファイルや通信の内容に対してアンチウイルスソフト ClamAV[1]を用いてウイルスチェックを行い、結果をモニタプロセスに送信する。

3. 現状と今後の予定

現在はシステムの実装を行っており、サーバとクライアントの処理の実装が終了した。しかし現在のシステムではファイルアクセスのたびにファイルをサーバに送りチェックを行うので処理速度が遅いといった問題がある。そこで今後、アイドル時間にファイルをサーバに送って検査を行い、その結果を利用するなどの方法により処理時間の改善を図っていく。

またカーネルのファイルやネットワーク処理部分にフックを入れる方法での実装も進めていく。この方法で実現できればモニタプロセスを複数作る

1 電気通信大学 電気通信学部 情報工学科

ことなく全プロセスを監視できるので監視漏れがなく、オーバーヘッドの少ないシステムとなる。

謝　辞

本研究の一部は総務省戦略的情報通信研究開発推進制度（SCOPE）の支援を受けて行われた。

参　考　文　献

[1]　ClamAV.　http://clamav.net/