セキュリティログ同期解析プログラム

03H005 伊藤 一

1　はじめに

今日までに、コンピュータの技術は急速に発展してきた。特に、インターネットの規模は世界規模にまで発展し、今では経済や社会の基盤となり、なくてはならないものになっている。

その発展とともに、コンピュータを用いた犯罪も増加してきた。代表的なのは、コンピュータシステムを破壊するなど、コンピュータに対して被害を与えるプログラム、俗にウイルスプログラムと呼ばれるものがある。また、サーバに対してアクセスを集中させることで、サーバを不安定な状態にさせる DOS 攻撃などもある。

このようにネットワークは様々な危険にさらされてきた。その度に、それらの対策のためのセキュリティソフトウェアが開発された。例えば、ウイルス対策用ソフトウェアや Fire Wall 用ソフトウェアなどが挙げられる。そのソフトウェアの数や種類は、世界中に数多く存在し、利用されている。

しかし、その結果、セキュリティ対策ソフトが乱立し、各々が優れた機能を持っているが、それらを統合的に管理することが難しくなっている。それは、高いセキュリティを維持するためには、セキュリティ対策の要であるログ情報を迅速に把握する必要があるからだ。

本システムは、これらの対策ソフトの持つログ情報をまとめることで、セキュリティ担当者たちが、トラブルなどの原因を突き止めやすくし、一刻も早くセキュリティ対策に取り組めるようにすることを目的とする。

2　システムの説明

セキュリティにかかわるログの情報は一概に膨大な量になりがちである。それは、企業や個人が、セキュリティ対策のために、大抵そのログを最低数ヵ月は保存しておくためである。そのため、トラブル発生時などで保存しておいたログを調べる場合、その膨大な量のために、とても手間のかかる作業になる。しかも、ソフトウェアが独自にログを保持することが多い。それらのログに対して目を通すことは、セキュリティを向上させることにつながるが、情報量が多く、なかなか難しい。

そこで、ログの情報をデータベースに登録し、複数のログ情報を一度に参照することができれば、効率良くログに目を通すことが可能になる。また、このことを Web ブラウザを使用して行うことにより、複雑な操作や知識を必要とせず、簡単な操作でシステムを利用することができ、的確な作業を迅速に行うことが可能になる。

3　まとめ

本開発では、ログの情報をまとめることができるシステムの開発目的とした。開発システムとしては、PHP と Apache、MySQL を使用することで、Web ブラウザを操作するだけで、ログをまとめることを可能にした。Web ブラウザの対応については、パソコンで一般的に使用されている Web ブラウザや一部の携帯電話の Web ブラウザでも利用可能であることが確認された。

セキュリティに関しては、ローカルネットワークで動作することを前提としたため、ほとんど対策は施してない。しかし、MySQL のデータベースにアクセスする際には、データベース名からテーブル名、ユーザパスワードまで入力をしなければならないので、データベースに関しては、ある程度のセキュリティを保つことができている。

今後の課題としては、システムの拡張性とセキュリティを高めることが重要になる。今回は、軽快に動くことを目的としたため、余計な機能を排除してシンプルなシステムとなる。このシステムは Web ブラウザで利用可能なので、インターネットを経由しても利用可能ですが、セキュリティ対策があまり施されていないので、セキュリティ対策が必要だと考えらる。