NFS Logging System の開発

03H114 矢田 淳一郎

1　はじめに

UNIX システムで利用されるファイル共有システム NFS(Network File System) は、ローカルエリアネットワークで広く使われている。NFS は 1984 年に Sun Microsystems 社によって開発され、ネットワークを介して複数のコンピューター間でファイルシステムを共有するために使われるプロトコルの名称である。NFS を使うとネットワーク上にあるコンピュータのファイルシステムを、あたかも自分のコンピュータにあるファイルシステムのように操作することができる。ファイルシステムを他のコンピュータに提供するコンピュータを NFS サーバ、他のコンピュータにあるファイルシステムを利用するコンピュータを NFS クライアントという。アドレスの管理だけでなく NIS(Network Information Service) を使ったネットワーク規模のユーザ管理を利用することが出来る。

しかし、NFS にはセキュリティの基本であるアクセスを記録する機能がない。セキュリティの基本は 24/7(24 時間× 週 7 日ノンストップ) の運用監視体制である。そして、ネットワークセキュリティの管理がしっかりできていなくてはならない。

NFS Logging System は、NFS のアクセスを記録することによりセキュリティの向上を目指す。コンピュータの利用状況やデータ通信の記録、操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身などを記録する。不正アクセスの抑止力 (思い留まらせる) につながり、セキュリティの向上が期待できる。

このシステムにより、NFS へのアクセスの常時監視ができる。また障害発生時の原因追求等の、管理者の負荷を減らすことができる。

2　本システムについて

NFS Logging System は、tcpdump を用いて、NFS へのアクセスの常時監視をすることによりセキュリティを高め、障害発生時の原因追求を容易にし、管理者や技術者の負荷を減らすことを目指す。

tcpdump を利用し、パケットに含まれている送信元、宛先アドレスやプロトコル、アプリケーションなどの情報を記録していく。

tcpdump とは、ネットワーク上に流れるパケットをモニター (監視) するもので、様々な条件を指定してパケットを拾い上げることができる。単純にモニタリングするだけでなく、マシンからパケットが流れているかや、パケットそのものも覗くことまで出来る。ネットワークに障害が発生した場合など、その原因を見極めるために使われるツールである。

抽出された状態では管理者としても見難いので、大事な部分だけを抜粋するプログラムを作成する。時間、どこから、誰が、どのファイルに対して、何の操作をなどを表示する。ユーザ名には id を表示、ファイルには inode を表示する。

3　まとめ

現在では、ローカルエリアネットワークで広く使われている NFS にはセキュリティの基本であるログを監視するシステムがない。そこで tcpdump を用いて、nfs(2049) のポートを監視した。Ruby を用いて取り込んだデータを誰が見ても解かりやすい状態に変更した。これにより、誰がどのファイルにどのような操作をしたかなどを記録するプログラムを作成した。inode、id に関してのプログラムも別で作成した。

今後、このシステムを利用し、研究室で管理を行ない、運用上の問題点を洗い出し、改良を加えていく予定である。