NFS Logging System の開発

03H114 矢田 淳一郎

Week 22(2006 年 10 月 6 日)

1　目的

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ます。しかし、セキュリティの基本であるログを監視するシステムがありません。NFS Logging System は、NFS のアクセスログを記録することによりセキュリティの向上を目指します。

2　概要

NFS は Sun が開発したネットワークファイルシステムです。NFS を使うと他の場所にあるコンピュータのファイルを、あたかも自分のコンピュータにあるファイルのように操作することができます。

通常、ログには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などが記録されます。

NFS のログを記録するためにネットワーク上を流れるパケットを dump することにより、誰がどのような処理を行なったかなど記録します。また、不正アクセスの抑止力 (思い留まらせる) につながります。よってセキュリティの向上が期待できます。

tcpdump コマンドを利用し、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きます。tcpdump コマンドとは、ネットワーク上に流れるパケットをモニター (監視) するツールです。

3　まとめ

このシステムにより、NFS へのアクセスの定常的な監視ができます。これによりセキュリティの向上が期待できます。また障害発生時の原因追求を容易に行なうことができます。