不正侵入検出手法に関する一考察

6G－6

藤井 誠司、大越 丈弘、辻 宏郷、小林 信博、太田 英憲、勝山 光太郎
三菱電機(株) 情報技術総合研究所

1. はじめに

インターネットの普及に伴い、インターネットに接続した組織内ネットワークへの不正侵入およびシステムの破壊などの犯罪行為が近年増加している。これに対するサイトのセキュリティ管理ポリシー[1]として、ファイアウォールを使用する不正侵入を防止するポリシーと、システムログ収集を使用する不正侵入後に、不正侵入者を追跡し、その行動を記録し、不正侵入者を特定するポリシーがある。

従来、サイトのセキュリティ管理ポリシーとしては不正侵入を防止するポリシーを取ることが多い。それは、不正侵入者を追跡するポリシーは不正侵入によるダメージを受けたシステムを回復するためのコストが必要となるためである。しかし、前者のポリシーでは一度侵入を許してしまえば、不正アクセスに対する有効な対策がない。そこで、後者のポリシーも組み合わせて利用することが重要となる。

本稿では、後者のポリシーを実現するシステムログ収集について改良した不正侵入防止手法について報告する。本手法は、コンピュータのユーザに対して、そのコンピュータの実システムの作業領域を割り当てず、仮想的な作業環境を提供することにより、不正侵入よってシステムがダメージを受けずに、侵入者のログを収集し、侵入者を特定できることを特徴とする。

A proposal for intrusion detection system
Seiji Fujii, Takehiro Ohkoshi, Hirosato Tsuji, Nobuhiro Kobayashi, Hidenori Ohta, Kotaro Katsuyama, Information Technology R & D Center, Mitsubishi Electric Corporation

2. 従来の不正侵入検出手法の問題点

インターネットより不正侵入者は、一般的に以下の方法により、内部ネットワークに侵入する。

① ターゲットシステムのセキュリティホールを探す。
② セキュリティホールを利用して、システムに侵入する。
③ 特権アカウント(root)になる。
④ システムログ収集プログラムの停止または置換えを行う。
⑤ システム内で、リソースに対して、不正アクセスを行う。
⑥ 侵入の痕跡を隠ぺいするためにシステムログの改修または削除を行う。

上記の不正侵入方法において、システムログ収集は不正侵入者の攻撃の目標となっていることが解る。これは、従来のシステムログ収集の手法が次のような問題点を持つためである。

- ＵＮＩＸなどの既存のＯＳでは、すでにログの管理手法が広く知られている[2]ために、ログファイルが直接攻撃される。
- syslog や acct などのロギ収集機能は本来、不正侵入の検出を目的としていないために、不正侵入を解析するために十分な情報を記録しない。

3. 不正侵入検出手法

従来、ログインしたユーザに対して、実システムとユーザの操作環境は同一であった。ユーザは、フ

ファイルシステム、メモリ空間およびプログラム管理について、制限はあるにしても、アクセスすることが可能である。このため、ユーザによるシステムへの不正アクセスの防止を困難としている。

そこで、図1に示す構成の不正侵入検出手法を提案する。本不正侵入検出手法を実現するシステムでは、システムの実体である実システム、システムにアクセスするユーザに割り当てるユーザ操作環境、ユーザ操作環境を管理するユーザ操作環境管理、ユーザ操作環境から受信した操作記録データを管理し、それに基づいて実システムを管理する操作記録管理から構成される。

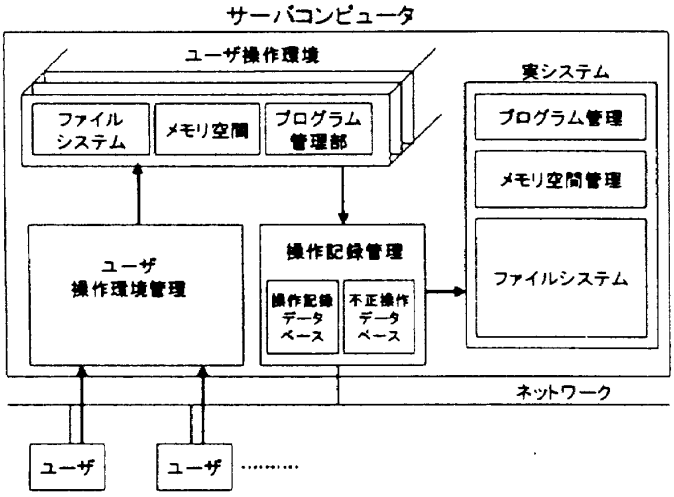

図1 不正防止手法によるシステム構成図

3.1. ユーザ操作環境管理

本不正侵入検出手法におけるユーザ操作環境管理では、次のような機能を持つことを特徴とする。

- **ユーザ操作環境を割り当て**
  ユーザが接続している実システムとは別のユーザが作業を行うためのユーザ操作環境を割り当てる。
- **操作記録データの取得**
  ユーザ操作環境では、ユーザの作業は自由に行うことができるが、その作業はリアルタイムに実システムに反映されず、操作記録データとして、操作記録管理に送信する。

以上のように、ユーザ毎にユーザ操作環境を割り当て、そこで作業を実行するようにしているので、不正侵入者による不正アクセスから保護することができる。

3.2. 操作記録管理

本不正侵入検出手法における操作記録管理は、次のような機能を持つことを特徴とする。

- **操作記録データの蓄積**
  ユーザ操作環境から送られてくる操作記録データを操作記録データベースへ記録する。
- **操作記録データの調査**
  操作記録データベース中の操作記録データが正常か不正アクセスであるかを調査する。
- **実システムの更新**
  不正アクセスではない操作記録データに基づき、実システムの状態を変更する。
- **不正アクセスデータの通知および記録**

以上のように、ユーザの操作が不正操作ではないことを検証した後に実システムに反映するので、実システムを安全に管理することができる。

4．おわりに

本稿では、ネットワーク経由で接続し、サーバシステム上で作業を行うユーザに対して、サーバの実システムの作業領域を割り当てず、仮想的な作業環境を提供することにより、不正侵入よってシステムがダメージを受けずに、侵入者のログを収集し、侵入者を特定できる不正侵入検出手法について報告した。今後は、実装を行い、評価を実施する。

5．参考文献

[1] J.Holbrook, P.Reynolds, "Site Security Handbook." RFC1244, July 1991

[2] S.Garfinkel, G.Spafford, "Practical UNIX Security" O'Reilly & Associates, Inc., 1991