ログファイルの視覚化による不正侵入検知手法の提案

高 田 哲 司　　小 池 英 樹

電気通信大学大学院 情報システム学研究科

今日、計算機への不正侵入が大きな問題となっている。これに対し計算機管理者は様々なログファイルやシステム情報を監視し、計算機が不正侵入されているか否かを判断する必要がある。しかし調査対象となる情報は膨大な量であり、その作業は熟練と特別な知識を要する。そこで本研究では3次元グラフィックスを用いてログファイル情報の視覚化を行った。本手法により、ログファイルに含まれている情報の認識が容易になる。結果として不正侵入検知が容易になる。

An intrusion detection system using visualization of computer logfiles

Tetsuji Takada and Hideki Koike

Graduate School of Information Systems
University of Electro-Communications

The increase of unauthorized access to computer systems is one of major issues in computer securities. System administrators have to monitor some logfiles or system's performance to know whether or not the systems are attacked.

There are, however, various kinds of logfiles and these files are usually located at different directories. It makes the intrusion detection more difficult.

This paper proposed a visualization approach for the intrusion detection. Four prototype visualization systems were developed. By using our visualizations, some intrusion detection tasks were performed more easily.

1. はじめに

今日、コンピュータセキュリティの重要性が声高に叫ばれている。Internetの普及に伴い、ネットワークに接続される計算機は増加の一途をたどり、情報収集手段としてのWWWや連絡手段としての電子メイルはすでに一部の者だけの技術ではない。

しかし、多くの計算機がネットワークに接続される事で、悪意をもったユーザによる計算機への不正侵入の危険性が増大し、近年多数の事件が報告されている。したがって計算機を利用するにあたって、不正侵入に対する対策をとる必要がある。

この問題に対する対策は、計算機の挙動を監視する事である。具体的に言うとOSが生成するログファイルや様々なシステム情報を監視し、計算機が不正侵入されていない事を確認する事である。しかし調査対象となるログファイルは膨大な量の情報を含んでおり、かつ計算機内に分散し、偏在していることがその監視作業を困難にしている。

そこで本研究では、情報視覚化技術を用いた不正侵入検知法を提案する。ログファイルを3次元グラフィックスを用いて視覚化する事により、ログファイル内に含まれる情報の認識が容易になり、結果として不正侵入検知が可能になる。本稿では、不正侵入対策への問題点を挙げ、本手法の提案と試作システムの紹介、そして不正侵入検知例について述べる。

2. 不正侵入対策

2.1 不正侵入対策における4つの場面

不正侵入対策には、以下の4つの場面からなるサイクルが必要であると言われている。[1)] このサイクルの繰り返しによりセキュリティを強化し、不正侵入の対処が可能になる。

I. 回避/防止
II. 保証
III. 検知
IV. 調査

日本においてもJPCERTをはじめ、多くの組織や研究者による活動により、コンピュータセキュリティの知識は普及しつつある。これにより多くの計算機環

境では、ファイアウォールやtcp_wrapperをはじめとした不正侵入防止システムが導入されている (I. 回避/防止)。またSATAN (Security Administrators Tool for Analyzing Networks) といった不正侵入攻撃シュミレータやCOPS(Computer Oracle and Password System) などのセキュリティチェックツールを用いて自計算機の安全性を検査し、保証している (II 安全性の保証)。

しかし、以下の理由により上記の対策だけで計算機が不正侵入される危険性がなくなるわけではない。

- 欠陥のないソフトウェアはない
  ソフトウェアの欠陥は次々と発見されている。この欠陥が場合によっては、新たな侵入手段を生む可能性を持っている
- 完全な不正侵入防止システムはない
  新しい侵入手段の発見や、人為的な問題があるため、ネットワークとの接続を維持したまま、不正侵入に対して絶対的な安全を保証する不正侵入防止システムはない

上記の理由より、不正侵入に対する対策は、前述の4つの場面のうちの(I),(II)だけでは不十分であり、(III)の不正侵入検知や、(IV)の不正侵入検知後の調査が必要不可欠である。

2.2 現在の不正侵入監視作業とその問題点

現在の不正侵入監視作業とは、豊富な経験と知識を持った計算機管理者がOSや不正侵入防止システムが生成するログファイルそして計算機の動作状況を定期的に監視し、不正侵入されていない事を確認することである。

そこで実際に不正侵入監視作業がどのように行われるか、ファイアウォールとtcp_wrapperが稼働しているUNIX計算機を前提に、具体例を挙げて考察する。

1. **アクセス状況の調査**

まず以下の事象に関する調査から始める。

- 見知らぬ計算機からアクセスされていないか
- ログイン処理の失敗が繰り返されていないか

そのためには以下の作業を行わなければならない。

- ファイアウォールのアクセスログを調査し、見知らぬ計算機からのアクセスを示すログがないかを探索する
- syslogファイルを眺め、膨大な量の情報の中からtcp_wrapperによるログ情報を抽出する。さらにその中に見知らぬ計算機からのアクセスを示すログがないかを探索する
- 上記同様にsyslogファイルを眺め、繰り返しログイン失敗のログを探索する

2. **ログイン状況の調査**

前述の事象が発見されたら、次に計算機に不正侵入しているかを調査する必要がある。具体的にはログイン履歴情報を調査することであり、“last” と呼ばれるコマンドを使用して “wtmpファイル” というログファイルの内容を調査することである。このログファイルも膨大な量の情報が含まれており、そのログ情報の中から見知らぬ計算機からアクセスしているユーザがいるかどうかを探索しなければならない。

3. **不正侵入者の挙動調査**

計算機への侵入が認められれば、その次に不正侵入者が計算機上で何を行ったかを調査する必要がある。具体的には以下の作業が必要になる。

コマンドの実行履歴情報やファイルの更新履歴情報を調査する必要がある。具体的には以下の作業を行う。

- どのようなコマンドを実行したか?
  “acctcom” というコマンドを使用してコマンド実行履歴情報を調査し、見知らぬ計算機からアクセスしたユーザがどのようなコマンドを実行したかを調査する
- 重要なファイルが新規作成/削除/変更されていないか?
  “ls” コマンドやエディタを使用して、セキュリティ上重要なファイルが改ざんされていないかを確認する

もちろん上述の監視作業で全ての不正侵入手段が検知可能ではない。しかし上記例から、人手による不正侵入監視作業は、困難であることがわかると同時に以下のような問題点が明らかになる。

- 不正侵入監視知識の必要性
  不正侵入監視作業を行うには、ログファイルの存在場所から不正侵入である事象まで、OSやセキュリティに関する膨大な知識が必要となる
- ログファイルの分散/偏在性
  ログファイルが分散、偏在していることが調査作業を困難にしている
- 膨大な情報量
  人が手作業により容易に処理できる量ではない
- 対象情報の抽出
  ログファイルはセキュリティに関する情報のみを含んでいるわけではない。必要な情報をログファイルから抽出する必要がある
- 単調作業
  極めて単調な作業である

2.3 関 連 研 究

不正侵入の試みや不正侵入されたという事象を検知するシステムとして不正侵入検知システム☆があり、多くの研究が行われている。以下に例を挙げる。

- NIDES[3)]
  SRI International's Computer Science Laboratoryで研究が行われている不正侵入検知システムである。特徴は、不正侵入の発見方法としてエキスパートシステムと統計的手法の両方を用いている事である。

☆ Intrusion Detection System. 略してIDSと呼ばれる

- NSM
  University of California, Davisで研究が行われており、Network監視を基本としたシステムである。不正侵入を検知するためにaudit trailを使用せず、networkのtraffic情報を用いている。
- USTAT[4)]
  USTATはUniversity of California, Santa Barbaraで開発されたシステムで、その特徴は、ユーザの利用状況を状態遷移としてとらえ不正侵入を検知している事である。

上記に挙げるように侵入者を発見するために様々な方法が考案されている。しかしこれらのシステムは、熟練者向けシステムであるといえる。

多くのシステムは、不正侵入検知を計算機管理者に通報するのみであり、どのような判断から不正侵入を検知したかが不明であるため、事後の調査を行う必要がある。

ここで我々は、不正侵入監視作業を計算機管理者のみに依存しているのは危険であると考える。それは、彼らが不在であったり、様々な理由により監視作業を行えなくなる可能性があり、またおろそかにもなる傾向もあるからである。

そこで我々は、計算機管理者以外のユーザも不正侵入監視作業に参加できるようにすべきであると考える。これにより、管理者が不在、その他の理由により不正侵入監視作業が行えない場合においても、管理者以外のユーザが不正侵入監視作業を代行することができ、堅牢な監視体制を確立する事が可能である。

2.4 情報視覚化による不正侵入検知システム

そこで本研究では、情報視覚化技術を用いた不正侵入検知システムを提案し、3次元グラフィックスを用いてログファイルの情報を視覚化するシステムを試作した。これにより以下の利点が考えられる。

- 情報が図表として視覚化される事により、文字の羅列による表示よりも認識負担が軽減され、膨大な量の情報も容易に認識可能になる
- 分散していたログファイル情報を統合して表示可能になる。これにより個々にログファイルを調査するだけでは把握しにくい情報間の関連性が明らかになり、監視作業を支援できる
- 侵入として疑わしい挙動が容易に把握可能になる。ログファイル情報の初期分析を行うため、初心者だけでなく熟練者にとっても作業負荷を軽減できる

上記の利点から、ログファイル内の情報がより直感的に把握可能になり、様々な事象が管理者以外のユーザにも理解可能になる。結果として、管理者以外のユーザが不正侵入監視作業に参加できるようになり、前節で述べた堅牢な監視体制を確立する事が可能になる。またログファイル情報の初期分析も行われるため、単にログファイルを眺めているだけでは気づかない情報も把握することができる。

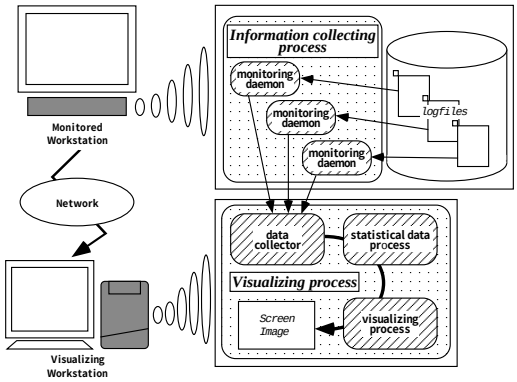

図1　システム構成図

3. ログファイル視覚化システム

本研究では、不正侵入検知システムとしてUNIXが動作している計算機を対象としたログファイル視覚化システムを試作した。本章では試作システムについて述べる。

3.1 システムの枠組

試作システムの枠組は、情報収集処理と視覚化処理の2つの処理部から構成される(図1参照)。

- 情報収集処理
  OSやセキュリティツールが生成する種々のログファイルを一定間隔で監視し、新規情報があれば情報収集を行う。本処理部はdaemon、組み込み関数、別コマンドとして開発してきた。今後は汎用性、リアルタイム性向上のためにdaemon形式の開発を目指す。
  現在daemonとして稼働している情報収集処理は以下の通りである。ただし動作環境としてSUN Solaris2.6のもとでsystem accountingとtcp_wrapperが稼働していることを仮定している。
  1. ログイン履歴情報収集
     wtmpログファイルを監視
  2. アクセス履歴情報収集
     syslogファイルを監視している。現在はtcp_wrapperのログと繰り返しログイン失敗の2点に対象を絞り情報収集を行っている
  3. “su”コマンド実行履歴情報収集
     sulogファイルの監視
  4. コマンド実行履歴情報収集
     pacctファイルを監視
  5. 指定したファイルの属性変化情報
     ユーザが明示的に指定したファイルについて、stat関数で得られる情報とファイルから作成したMD5情報を保持し、これらの

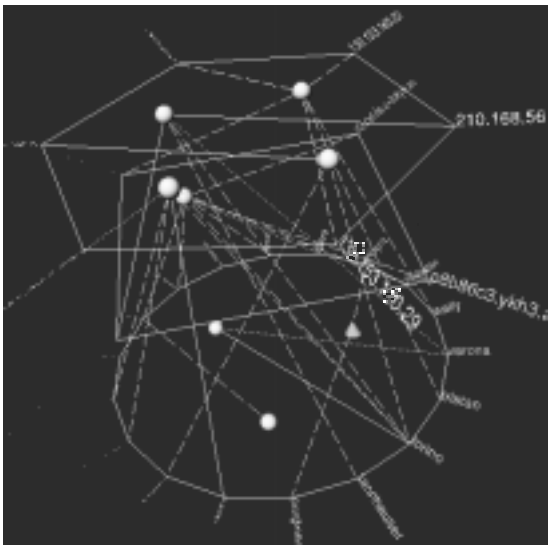

図2　ログイン履歴情報の視覚化例

情報の変化を履歴情報として収集している

- 視覚化処理
  情報収集処理で得られた情報を3次元グラフィックスを用いて視覚化している。現在、Silicon Graphics社製ワークステーション **O2** 上にて動作している。また本処理ではユーザからの要求を受け付け、それに対する反応も行う

3.2　試作システム

本節では、これまでに開発した試作システムを紹介する。

3.2.1　ログイン履歴情報の視覚化

ログイン履歴情報の視覚化(図2)は、計算機へのアクセス状況の把握を目的としたシステムで、ログイン履歴情報、アクセス履歴情報、“su” コマンド実行履歴情報を統合して視覚化を行った。概観は、多角形上の枠により「層」を形成した形状である。この各層は、アクセス元ホストの信頼度を表し、疑わしいアクセス元ホストの認識を容易にしている。

枠外周には、文字によりアクセス元ホスト名が表示され、枠内周にはユーザを表す球または円錐が表示される。ユーザ情報は、その形状によって “su” コマンドを実行し、異なるユーザへのなりかわりが成功したか否かを表し、色によりLAN内で共通の一般ユーザなのか、または計算機限定のユーザ☆なのかを知ることが可能である。またユーザとアクセス元ホスト間は線で結ばれ、その線の種類によってアクセス方法を知ることが可能である。

またユーザはマウスによるドラッグ操作により、様々な位置へ視点の移動が可能である。さらに表示されているオブジェクトをマウスでピックすることで表示情報のフィルタリングが可能である。

☆ root、admなど

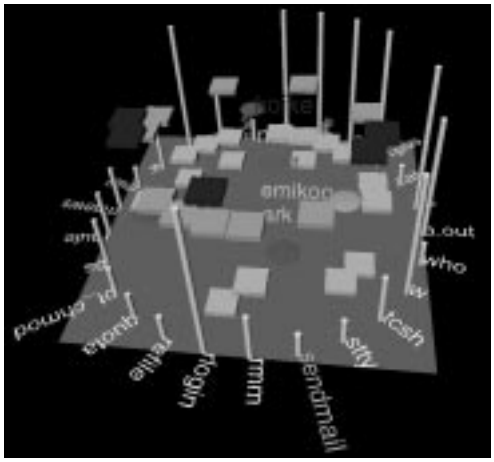

図3　コマンド実行履歴の視覚化例

本システムにより、以下のことが把握できる。

- 現在作業中のユーザ名
- 各ユーザのアクセス元ホスト名
- “su” コマンドを実行したユーザ

結果として

- 見知らぬホストからのアクセス
- “su” コマンドによるなりすまし
- ありえないユーザの計算機利用

といった事象が監視可能である。

3.2.2　コマンド実行履歴の視覚化

コマンド実行履歴情報の視覚化(図3)は、計算機内でのコマンド実行状況の把握を目的としたシステムで、コマンドとログインに関する履歴情報を統合して視覚化を行った。

概観は、最下層に実行されたコマンド名が円形状に表示され、その実行頻度を表す円柱が付随して描かれている。またその円の内部には、各ユーザ毎のコマンド実行状況を表す輪が層状に描かれている。

本システムにより、以下のことが把握できる。

- 計算機内で実行された全コマンド
- 計算機内で実行された全コマンドの使用頻度
- 各ユーザのコマンド実行状況
- ユーザの各コマンド実行方法(端末からの入力による起動、もしくはcron,rshによる間接的な起動)

結果として

- 該当ユーザが使うはずのないコマンドが実行されている
- 本人の知らないうちに、コマンドが実行されている。

といった不正侵入として疑わしい事象が検知可能である。

またマウスによる表示オブジェクトのピックにより、実行コマンドの表示を計算機単位からユーザ単位、セッション単位へと移行することが可能であり、表示情報

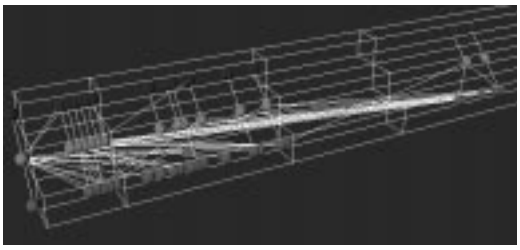

図 4　ファイルの時刻情報の視覚化

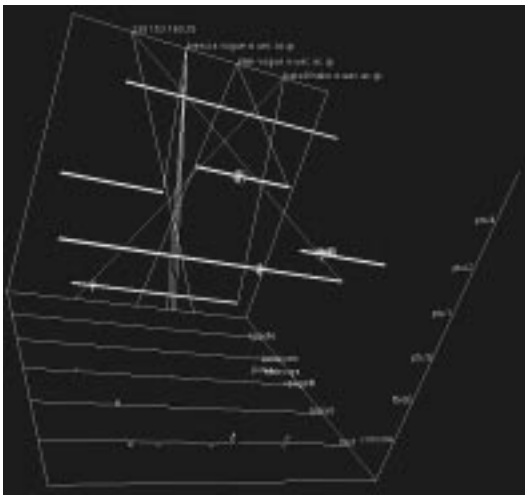

図 5　種々の情報の統合視覚化例

のフィルタリングが可能である。

3.2.3　ファイルの時刻情報の視覚化

UNIXにおけるファイルには、3種類の時刻情報が存在する。これらの情報の把握を目的として視覚化を行った(図4)。

本システムによってファイルの時刻情報がより直感的に把握可能になり、ファイルがアクセス、更新されたり、許可権限が変更された場合にその状態変化が容易に認識可能になる。これをセキュリティ上重要なファイルに適用することで、不正侵入監視作業を支援することが可能である。

3.2.4　セキュリティ情報の統合視覚化

これまでは、個々のセキュリティ情報に焦点をあてて視覚化を行った例を紹介した。本節では、今までに焦点をあてた種々のセキュリティ情報をより統合的に視覚化した例を紹介する。

図5は、ある時間間隔内に発生したセキュリティに関する情報を統合して視覚化した例である。この表示には以下の情報が含まれている。

- アクセス履歴
- ログイン履歴
- suコマンド実行履歴
- コマンド実行履歴

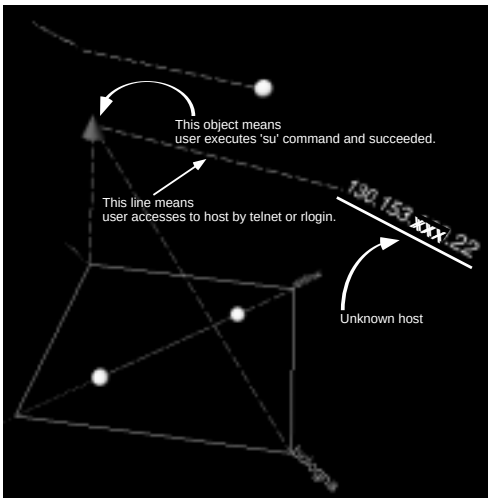

図 6　不正侵入検知例

- ファイルの状態情報変更履歴

この方法では、個々の情報内に含まれる特徴は隠蔽されてしまうが、一つの視覚化表示で様々なセキュリティ情報を同時に見ることができる。また時刻を基準とした表示を行っているため、個々の情報間の時間関係が直接認識できる利点がある。

このように時間を基準にした視覚化は必要である。セキュリティ上、ある異常な事態が発生した際に、同時刻で何が行われていたか、またその後に何が発生したかを知る必要があることは多い。時刻を基準にした視覚化は、このような作業を直接支援可能にする。

4.　不正侵入検知例

本章では、ログファイル視覚化システムを利用して、不正侵入が検知可能であることを以下の不正侵入事例を例に挙げて示す。

ネットワークを通じて計算機に不正侵入した。計算機の使用状況をうががい、その後suコマンドを実行してrootユーザになり、/etc/inetd.confを編集した。

図6ではログイン履歴情報視覚化での不正侵入検知例である。図6の表示は、視覚化結果に疑わしい表示があったため、表示情報のフィルタリングを行ったものである。その結果として次のような疑わしい挙動が認識される。

- 見知らぬホスト名表示が存在する
  見知らぬホストからのアクセスがあったことを示す
- 見知らぬホスト名とユーザを表すオブジェクトを結ぶ線が存在する
  見知らぬホストからあるユーザになりすまし、ログインに成功していることを示す
- ユーザを表すオブジェクトが赤い円錐表示である

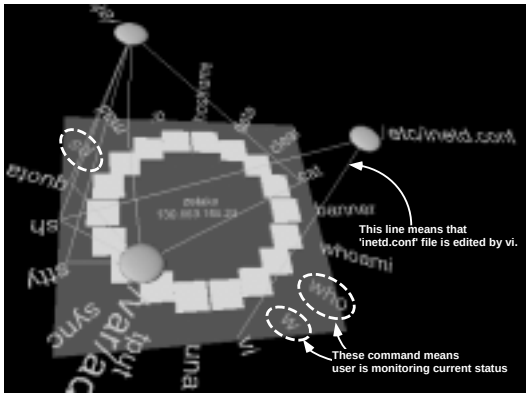

図7　不正侵入調査例

suコマンドを実行しており、それが成功していることを示す

これらの結果より、見知らぬホストから不正侵入されており、suコマンドにより他のユーザになり変わっている可能性が高いことがわかる。

さらに不正侵入者が何を行ったのかを調査する必要がある。図7は、コマンド実行履歴情報視覚化による不正侵入調査例であり、前述の検知結果を基に、視覚化対象情報のしぼり込みを行ったものである。

その表示から次のことが認識される。

- “who”,“w”,“ps” といったコマンドを実行して計算機内の現状をうかがっている
- コマンド “vi” とファイル “/etc/inetd.conf” が線で結ばれている。これは、viによりinetd.confを改ざんした可能性がある事を示している

これらの結果を総合すると、不正侵入者である可能性が非常に高いと判断できる。また/etc/inetd.confが改ざんされていないか、ファイルの内容を確認する必要がある。

5. 問　題　点

本章では、試作システムの構築を通して発生した問題点、および今後の課題について述べる。

- 情報収集部
  - (1)　ログファイルの改ざん/削除
    不正侵入検知はログファイルなしには不可能である。よって内容の正確さとその存在を保証する必要がある。保証レベルに応じて様々な対策が考えられるが、本システムとしても対策を考える必要がある。
- 視覚化処理部
  - (1)　ネットワーク監視
    不正侵入の手口には、単一ホストの監視だけでは発見不可能なものがある。networkで接続された複数台の計算機の監視が必要である。
  - (2)　不正侵入検知の通知
    不正侵入があった際に、それが即時に認識できるような工夫が必要である。侵入事象が一層顕著になるような視覚化手法の考案、および警報音などによるユーザへの通知を考える必要がある。
  - (3)　視覚化処理の統合
    監視作業を行うにあたって、監視対象情報ごとに異なるシステムを実行するのはユーザにとって手間であり、1つのシステムで様々な視覚化表示を見ることが出来ることが望ましい。よって視覚化処理部の統合を行う必要がある。

6. おわりに

本研究では、不正侵入検知を目的としてログファイル情報を3次元グラフィックスを用いて視覚化することを提案し、試作システムを開発した。本手法により膨大な量であり、かつ偏在するログファイル情報を統合し、その特徴を視覚化することによって、ログファイル情報の認識が容易になる。結果として、不正侵入対策における不正侵入検知作業を支援することが可能になると同時に、セキュリティ監視の熟練者でなくても不正侵入監視作業が可能になる。また、試作システムを用いて不正侵入検知が可能であることを示した。

今後は、システムの統合と、より直感的に不正侵入が認識可能になる表示法の工夫、そして実運用環境での不正侵入検知評価を行う。

参　考　文　献

1) 不正侵入はこう防げ, 日経コンピュータ, No.448, pp188-195, July, 1998
2) Teresa F. Lunt, Detecting Intruders in Computer Systems, *Conference on Auditing and Computer Technology*, 1993
3) Debra Anderson. Thane Frivold. Alfonso Valdes, Next-generation Intrusion Detection Expert System(NIDES) A Summary, SRI-CSL-95-07, SRI International, Menlo Park, CA, May 1995
4) Koral Ilgun. Richard A. Kemmerer. Phillip A. Porras, State Transition Analysis: A Rule-Based Intrusion Detection Approach, *IEEE Transactions on SOFTWARE ENGINEERING*, Vol.21, No.3, pp181-199, 1995
5) Eleen Frisch著. 谷川哲司監訳, UNIXシステム管理 改訂版, オライリージャパン/オーム社, 1998