鼓: 不正侵入検知を目的としたログ情報視覚化システム

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

不正侵入対策において人間がログ情報を閲覧することは必要である．一方，ログの閲覧には情報認識負荷の大きさとその量の膨大さという問題があり，その作業遂行を阻害している．そこで本論文では，ログの閲覧を支援する手法として情報視覚化を用いる手法を提案し，それに基づくログ情報視覚化システム “鼓” を構築した．本システムを用いることにより，ログ情報の閲覧によって不正侵入として疑わしい事象の検出を従来よりも容易に行なうことが可能になる．また鼓を用いた不正侵入事象の検知例についても述べている．

Tsudumi: Log Information Visualization System for Intrusion Detection

Tetsuji Takada and Hideki Koike

Graduate School of Information Systems
University of Electro-Communications

This paper describes about a log information visualization system called “Tsudumi” for intrusion detection. The system administrator have to investigate some log-files regularly to detect intrusive trails. There are, however, two problems for this task. One is that recognizing log information is hard task for human. The other is that the amount of log information is usually enormous.

We introduce information visualization technique to help recognizing log information. By using Tsudumi, the administrator can perform a log recognition task easily than before. It is also possible for administrator to detect suspicious trails by browsing visualized log information. We illustrate some visualized suspicious trails as intrusion.

1. はじめに

計算機への不正侵入は多発しており，その対策は急務である．この問題に対する対策手法として四段階の作業を繰り返し行なうことによる不正侵入対策の継続的な強化(図1)が望ましいと言われている[1)]．この対策手法を実現するためには，検知および調査段階の作業を確実に行ない，その結果を防止/回避作業に反映させることが不正侵入対策の強化において必要不可欠である．

そこで本論文では，検知作業を確実に行なうためにはシステム管理者が定期的にログ情報を閲覧することが重要であることをはじめに述べ，その一方で，その作業にはいくつかの問題点があることを指摘する．そこでそれらの問題を改善する一手法として情報視覚化を用いる手法を提案し，その提案に基づき構築したログ情報視覚化システム “鼓” とその実用例について述べる．

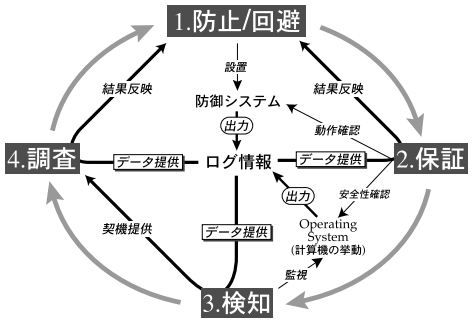

図1　四段階の作業に基づく不正侵入対策

2. 不正侵入対策におけるログ閲覧

不正侵入対策においてシステム管理者が定期的にログを閲覧する作業は必要である．本章では本作業の必要性と問題点について述べたのち，情報視覚化を用いた改善手法を提案する．

2.1 ログ閲覧の必要性

検知作業とは，様々な情報から不正侵入と思われる事象を “検出” し，それをシステム管理者に迅速に “通知” することである．従来，システム管理者はログを手作業で閲覧することにより検知作業を行なってきた．

一方，近年不正侵入検知システム[2] (Intrusion Detection System と呼ばれる．以降IDS と略す) が普及しつつある．しかし以下の理由によりログ閲覧の必要性に変化はないといえる．

1. 導入や運用管理の困難である
   IDS は熟練システム管理者の作業支援が目的である．よってIDS を扱えない場合にはログを閲覧する必要がある．
2. 万能なシステムではない
   IDS 自身があらゆる不正侵入を検知可能ではなく，また不正侵入検知を誤ることもある．これらの欠点を補完するためにログを閲覧する必要がある．

したがってIDS の導入有無にかかわらず，今後も不正侵入対策として不正侵入を検知するためにシステム管理者がログを閲覧する必要性はあるといえる．

2.2 人間によるログ閲覧作業における問題点

ログの閲覧作業は不正侵入対策において必要である．しかしその一方で，ログの閲覧作業は敬遠されている．人間によるログ閲覧作業を阻害する問題点を以下に挙げる．

- 情報認識負荷の高さ
  ログに記録されている情報を理解するためには記録されている情報を全て読み，さらにそれを意味のある情報として解釈する必要がある．これゆえログ情報の概要把握も極めて困難である．
- 膨大な情報量
  閲覧すべき情報量が膨大であるため，システム管理者は単調で退屈な作業を長時間行なわなければならない．
- 複数の情報源
  個々のログに記録されている情報は断片的な情報であるため，不正侵入検知を行なうためには複数のログを個々に閲覧し，得られた情報を総合して判断を行なう必要がある．また情報間の関連付けも閲覧者が行なわなければならない．

2.3 情報視覚化によるログ閲覧作業支援の提案

前述の問題点を改善し，ログ閲覧作業を支援する一手法として本研究では情報視覚化を用いた手法を提案する[3)4)]．

情報視覚化とは膨大な量の情報を抽象化して表示することにより，人間が情報を理解したり操作するのを支援する手法である．これをログに応用することにより情報認識負荷の問題を改善し，ログ情報の概要把握を可能にする．また膨大な情報量という問題に対しても情報を抽象化して表現することにより対応可能である．さらに複数のログの閲覧が必要という問題についても，複数の情報を一つの図として表現し，情報間の関連性を視覚的に表現することにより対応可能であり，ログ閲覧者の作業負担を軽減することが可能になる．

3. ログ情報視覚化システム: 鼓

本研究では，前述の提案に基づいたログ情報視覚化システム “鼓” を構築した．本システムはUNIX 系OS が稼働する単一計算機を対象とし，過去一定期間内に発生した次の三種類の情報を統合して視覚化するシステムである

1. 監視対象計算機へのアクセス状況
2. 監視対象計算機におけるユーザの利用状況
3. 管理者権限の取得状況

3.1 システム構成

鼓はログ情報収集処理と視覚化処理の二大処理から構成される (図2参照)．これらの処理はサーバ/クライントの関係になっており，ネットワークを通じて遠隔計算機のログを閲覧することも可能である．

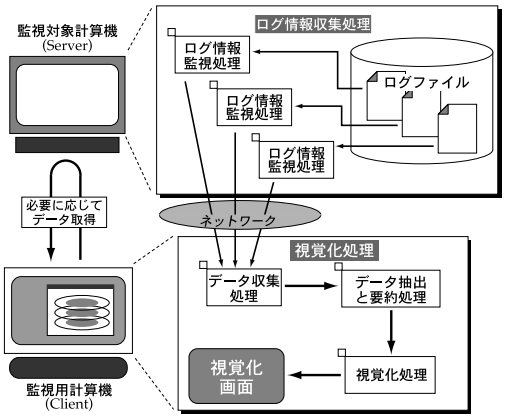

図2　鼓のシステム構成図

ログ情報収集処理では視覚化に必要な情報を収集し，それらを必要に応じて視覚化処理へ供給する処理を行なう．現在の実装ではSolaris2.6, IRIX6.5, Linux の3種のOS 上で動作しており，表1に示す情報源から情報を得ている．

視覚化情報	情報源
アクセス情報	TCP_Wrapper が出力するログ
ユーザ利用状況	wtmpx ログファイル
管理者権限取得状況	sulog またはsyslog 内のsu コマンドに関するログ

表1　視覚化情報とその情報源

視覚化処理ではログ情報収集処理から情報を受け取り，それらを図化してユーザに提示する．また図に対する対話的処理が可能であり，より詳細な情報の取得やフィルタリング処理を直観的に実行可能である．

3.2 視覚化手法について

本節では鼓におけるログ情報の視覚化手法について説明する．

鼓では不正侵入検知を目的とした要約表示[4]を行なっている．ログは時刻情報と事象情報の組として情報を保持している．しかし不正侵入検知においてまずはじめに必要なことは，検知対象の計算機において発生した全事象を把握し，その中から疑わしい事象を検出することである．よって過去一定期間のログを事象情報に注目して要約し，その結果を視覚化する(図3)．ログ情報の要約と視覚化手法の併用により膨大な量のログに記録されている事象情報の迅速な把握を支援する．

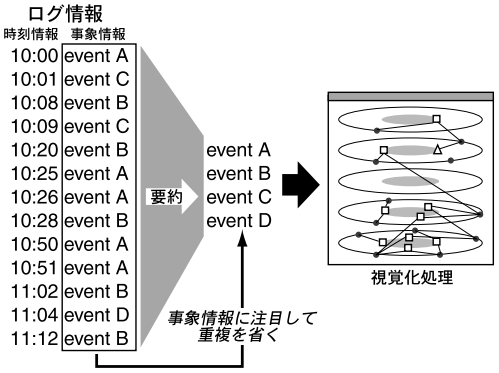

図3　ログの要約

鼓の概観を図4に示す．

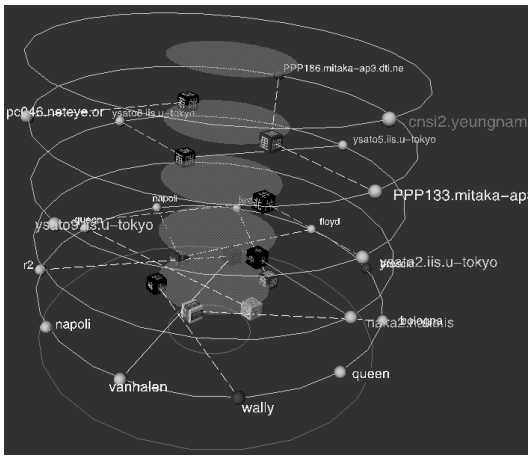

図4　鼓による視覚化例

図4からもわかる通り，同心円が層状に重ねられた概観になっている．そこで層状と各層内の同心円における表示法についてそれぞれ説明を行なう．

1. **層状表示**　　層状表示は，アクセス情報が持つアクセスホスト情報を規則に応じて分類する意味を持つ☆．アクセス制御やファイアウォールは，ホストやドメイン名/IP アドレスによる規則を定義することにより通信制御を行なっており，これは規則に基づき不正侵入検知を行なう IDS でも用いられている手法である．

鼓ではこの手法を視覚的に応用することにより，ログから不正侵入であると推測される事象の抽出を行なう．既存のシステムでは通信の許可/拒否または不正侵入か否かの二値判断であるが，鼓では視覚的に分類を行なうため，安全であると推測される規則から不正侵入に違いないと思われる規則まで無制限に規則を定義する事が可能であり，また安全であると推測される情報も全てユーザに提示する．

図5にアクセスホスト情報の分類規則例を示す．

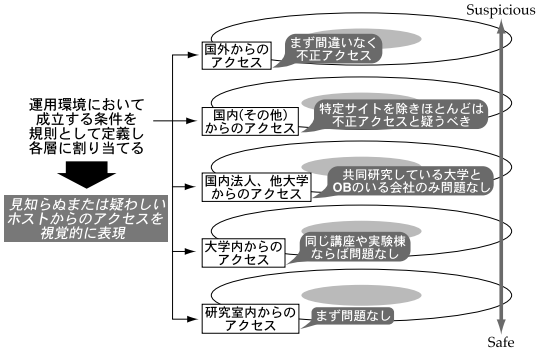

図5　アクセスホスト分類規則の定義例

図5の例では安全であると推測されるアクセスホスト群の規則を下位層に，不正侵入として疑わしいと推測される規則を上位層に割り当てている．これによりアクセス情報のうち不正侵入であると推測される情報が上位層に抽出されることになる．したがってシステム管理者は，上位層に注目することによって膨大な量のアクセス情報から注目すべき情報を容易に識別可能になる．

2. **同心円表示**　　各層の同心円内に表示される情報は最下層とそれ以外の層で異なる．最下層は管理者権限の取得状況を，その他の層はアクセス情報とユーザの利用状況が表示される．以下ではそれらの表示法について説明する．

I. **アクセス情報とユーザ利用状況表示**　　最下層以外の同心円内における表示法を図6に示す．

同心円の内周には利用したユーザが色または画像付きの立方体で，外周にはアクセスホストが球で表示される．各ホスト名は存在を表す球の近くに文字で表示される．一方，ユーザ名は文字で明示せず，必要に応じて対話的処理を用いて取得する．また，管理者権限の取得を試みたユーザは，ユーザを表すオブジェクト

☆ ただし最下層は除く

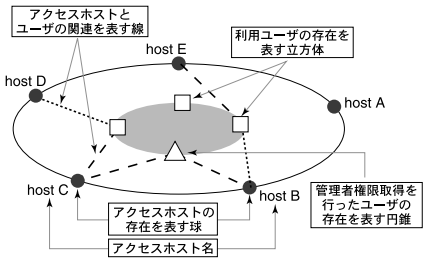

図6　アクセス情報とユーザ利用状況の表示法

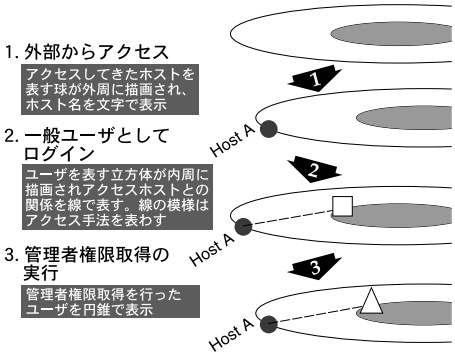

図7　アクセス情報とユーザ利用状況の表示法とその推移

が立方体ではなく円錐で表示される．

またユーザとアクセスホストとの間には，その関係を表す線が描画される．さらに計算機の利用方法が線の模様として表示される．長破線の場合は遠隔からの端末利用を，短破線の場合はファイル転送を，実線の場合は双方の利用があったことを示している．

視覚化対象のログにおいて起こりうる状況が鼓によってどのように表示され，推移するかを図7に示す．

II. **管理者権限取得状況表示**　最下層は管理者権限取得状況が表示される．管理者権限の取得という事象はユーザ間の遷移として捉える事が可能である．したがってその遷移を矢印を用いて同心円内に表示する．

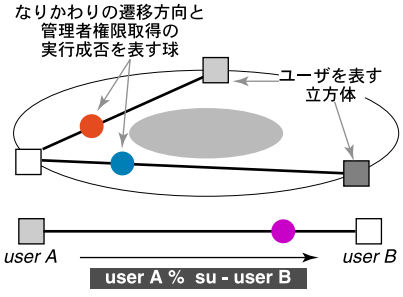

図8　管理者権限取得情報の表示法

この層では，外周に管理者権限取得に関連した全ユーザを他の層と同様の立方体で表示する．一方，ユーザ間の遷移を表す矢印を線と球にて疑似的に表現している (図8)．また矢印の矢である球の色により管理者取得行為の成否を表している．成功時には赤，失敗時には青を割り当てており，これにより管理者権限の取得に関連したユーザとその遷移状況ならびに実行成否を視覚的に把握する事が可能である．

3.3　対話的機能

鼓では情報視覚化手法を用いることにより，ログ情報の閲覧を支援するいくつかの対話的機能を実現している．この機能により図的表現から知り得た情報の詳細や特定情報の抽出を視覚化システム内で直観的に行なう事が可能である．以下にその機能を紹介する．

- 視点の移動
  マウスを用いて視点を移動する事が可能であり，様々な位置から視覚化情報を閲覧することができる．
- ユーザおよびアクセスホストに基づく情報抽出
  マウスでユーザやアクセスホストを表すオブジェクトを選択することにより，選択した情報に関連した情報のみを表示することが可能である．これにより注目した情報とその関連情報を抽出することが可能である．
- ホスト名の簡略化によるアクセスホスト表示の要約化
  アクセスホスト名はドメイン名の木構造に基づき簡略化する事が可能である．これによりアクセスホスト情報の情報量制御が可能になるとともに，アクセスホストの概要把握を支援する．図9はこの機能の実行例である．
- 表示対象期間の変更
  鼓では現在時刻を基準として過去一定期間の情報を視覚化している．この視覚化対象期間を変更することが可能である．
- 表示層の部分表示
  層の数が多くなるにつれて下層や中間層にある情報の視認性が劣化する．この問題を改善するため，鼓では層単位で表示制御を行なうことが可能である．

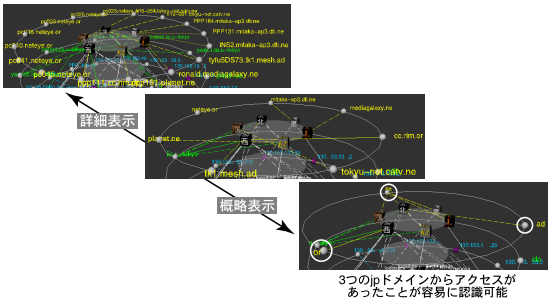

図9　ドメイン名によるアクセスホストの要約表示例

3.4　実　用　例

本章では鼓を利用して検出可能な不正侵入と思われる事象として3つの例を紹介する．

見知らぬホストからのアクセス例

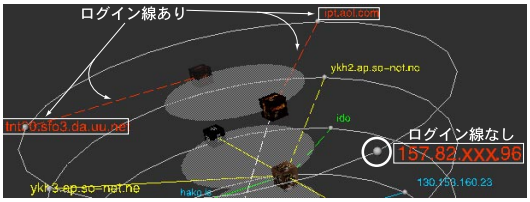

図 10　ネットワークを通じた外部からの不正アクセス

図 10は，外部からの不正なアクセスと思われる事象の視覚化例である．その根拠は二つあり，一つはアクセスされるはずのない計算機からアクセスされていることである．これはこの視覚化例の最上位層にアクセスホストの表示があることから認識できる (図 5参照)．

もう一つはアクセスしたがログインして利用していないことである．これは右下のアクセスホストを表す球からログインして利用したことを示す線が存在しないことから認識できる．

これらの結果から，ネットワークを通じた外部の計算機からの不正アクセスであると推測できる．

複数ドメインからのアクセス

二つ目の例として複数ドメインからのアクセスを例に挙げる．図 11はその視覚化例である．

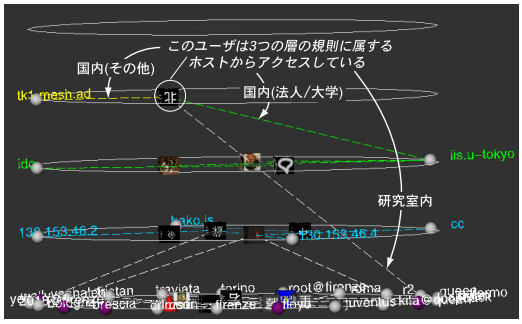

図 11　複数ドメインからのアクセス

この図の上から二段目の層に表示されているユーザは，複数の層に属するアクセスホストからログインしたことを表す線が描かれている．この例では自研究室内，国内の他大学/法人および国内の計算機からアクセスしていることを表していた．この事象は不正侵入かもしれないと疑うべき事象であるといえる．

この例の場合，視覚化表示だけでは断定できないが，現実との比較やシステム管理者の経験を加味することで確実な判断が可能になる．この表示が過去 10 分間の情報で該当ユーザがその間研究室内で作業をしていたという現実の事象が既知ならば，図 11の例は不正侵入として対処する必要があるといえる．なぜならば，研究室内で作業をしているのに研究室外の計算機から監視対象の計算機にアクセスして利用するはずがないと考えられるからである．一方，システム管理者の経験として「該当ユーザは国内の他大学/法人の計算機からアクセスして使用したことはない」という知識を持っていたと仮定すると，図 11の表示は同様に不正侵入として疑うべき状況であると言える．

ユーザによる不正行為

図 12は，様々なユーザオブジェクトの表示例である．

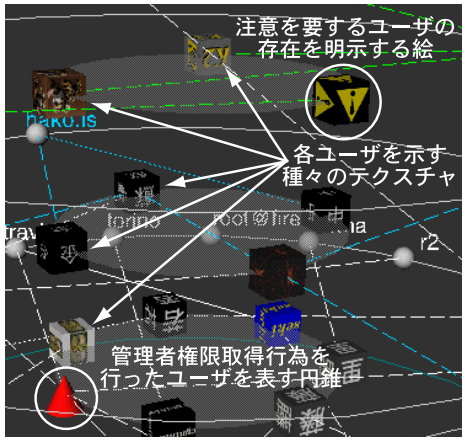

図 12　様々なユーザオブジェクト

前述の通りユーザを表す立方体には様々な絵や色を割り当てることが可能である．これを応用することで，ユーザ名に基づく不正行為を明示することが可能になる．その一例としてログインして使用しないユーザを明示する方法について述べる．

図 12右上の立方体には交通標識の注意と同様の絵が張り付けられている．この絵は通常時には計算機にログインして利用しないユーザを表しており，システム管理者への注意を喚起する意味でこの絵を用いている．当研究室ではOB のユーザアカウントにこの手法を適用している．この手法による注意喚起は他にも考えられる．一方，管理者権限取得にかかわったユーザは立方体のかわりに円錐を用いて明示されるため，その存在を迅速に認識可能である (図 12左下)．

4. 考　　察

ログ情報視覚化システム “鼓” における利点と今後の課題について考察する．

4.1 利　　点

鼓によって発生する検知作業の利点は以下の通りである．

一つ目はログ情報を視覚化することにより情報認識負荷を軽減したことである．これはログ情報の閲覧作業を読んで理解するという行為から抽象化した図を見るという行為に変換させたためである．

二つ目は複数のログ情報を統合して表示することにより，ログ閲覧における作業負担を軽減したことである．これにより閲覧者が複数のログを個々に閲覧し，情報間の関連付けを行なう必要がなくなるためである．

三つ目は視覚化を行なうにあたりログ情報を要約したため，事象情報の把握が容易になったことである．これと視覚化手法との双方の効果によりログ情報の概要把握を容易にし，結果として不正侵入として疑わしい事象の検出を支援する．

四つ目はユーザが定義する規則をログに適用することで不正侵入として疑わしい事象を視覚的に抽出し，明示可能としたことである．この規則をシステム管理者が定義してユーザ間で共有することにより，多数のユーザによる不正侵入対策が可能になる[4]．また視覚化システムは全事象情報を表示することで人間による判断を促すシステムであるため，既定の規則が網羅していない事象も認識でき，それをもとに個々の運用環境にあった不正侵入検知の規則構築を支援することも可能である．

4.2 今後の課題

本節では鼓における今度の課題について述べる．

一つは視覚化手法の洗練化が挙げられる．今回提案した表示法が不正侵入検知を目的とした表示として効果的か評価を行ない，必要ならば視覚化手法を変更して洗練化する必要がある．また洗練化においては，スケーラビリティや他のログ情報視覚化システムとの統合も考慮する必要がある．

もう一つは不正侵入として疑わしい事象の抽出手法の強化である．鼓ではログに対してユーザの知識や経験を基に定義した規則を適用することにより不正侵入として疑わしい事象の検出を行なっている．しかし閲覧者に知識や経験がなければ不正侵入事象の検出は困難である．今後は不正侵入検知システムが実現している検知手法を視覚化システムに統合する必要がある．

4.3 ログの閲覧を支援するシステムとの比較

ログの閲覧を支援する他のシステムと鼓との差異について述べる．

はじめにログの閲覧をGUIで操作可能にするシステムが存在する[7]．しかしこれは本質的にエディタ等による閲覧手法と同様であり，既存の問題点を改善していない．一方，本手法と同様にログ情報をその事象情報に注目し集計し，グラフ等に図化する方法が存在する．しかしここで用いられている集計方法は単純な集計であり，不正侵入として疑わしいと推測される事象を抽出しているわけではない．またシステム管理者が不正侵入検知規則を知識や経験として持っていたとしてもそれをログに適用することはできないという欠点もある．

また，ログ情報の閲覧を情報視覚化を用いて支援する手法もいくつか提案されている[5][6]．これらはログを多量の文字情報とみなし，そこから様々な特徴を抽出して図化することによりログ情報の調査作業を支援するシステムである．しかしログ情報の個々の意味や事象情報に特化したシステムではないため，概要の把握は困難であり検知作業を支援することは困難であるという問題がある

5. おわりに

本研究では，不正侵入対策作業として必要不可欠なログ情報の閲覧を支援する一手法として情報視覚化を用いることを提案し，その実装例として構築したログ情報視覚化システム “鼓” について述べた．

不正侵入対策の検知作業におけるログ閲覧の目的は，計算機内において発生した全ての事象を迅速に把握し，その中から不正侵入として疑わしい事象を検出することである．この作業は不正侵入検知システムが普及しても必要な作業であるとともに，不正侵入検知システムを補完する作業であることについても述べた．

この作業を支援するため，ログを事象情報に特化して要約するとともに，情報視覚化を用いて情報を抽象化して表示するログ情報視覚化システムはログ閲覧における既存の問題点を改善可能であることを述べた．またシステム管理者が持つ不正侵入検知規則をログに適用し，その結果を視覚的に表現することにより，不正侵入として疑わしい事象を容易に検出可能であることを例を用いて示した．

参考文献

1) 川又英紀: 米国セキュリティ最新事情 - 不正侵入はこう防げ, 日経コンピュータ, No.448, pp.188-195, (July 1998).
2) Teresa F. Lunt, Detecting Intruders in Computer Systems, *Conference on Auditing and Computer Technology*, (1993).
3) 高田哲司, 小池英樹: ログファイルの視覚化による不正侵入検知手法の提案, コンピュータセキュリティシンポジウム ’98, 情報処理学会, pp.153-158, (1998).
4) 高田哲司, 小池英樹: ログ情報視覚化システムを用いた集団監視による不正侵入対策手法の提案, 情報処理学会論文誌, Vol.41, No.8, pp.2216-2227, (2000).
5) 高田哲司, 小池英樹: 見えログ: テキストマイニングと情報視覚化を用いたログ情報ブラウザ, マルチメディア，分散，協調とモバイルシンポジウム (DICOMO2000), pp.541–546, (June 2000).
6) Eick S.G., Nelson M.C. and Schmidt J.D.: Graphical Analysis of Computer Log Files, *Comm. OF THE ACM*, Vol.37, No.12, pp.50–56, (1994).
7) Georg C.F.Greve, The Xlogmaster, (1998). http://www.gnu.org/software/xlogmaster/index.html