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

高田哲司[†] 小池英樹[†]

今日，計算機への不正侵入が大きな問題となっており，すでに様々な対策手法が提案されている．しかし既存の手法には種々の問題点があり，それらが原因となって不正侵入対策の普及は進んでいないといえる．よって既存の対策手法における問題を改善しうる新たな手法が望まれている．そこで我々は，4種類の作業からなる不正侵入対策手法を基に既存の対策手法における問題点の抽出を行った．この考察から我々は，不正侵入対策を強固にするためにはログ情報の調査作業を確実に遂行することが必要であることを認識した．そこで本研究では，その作業を支援する一手法として情報視覚化によるログ情報視覚化システムを提案する．本研究では，ログ情報の視覚化手法としてログ情報の要約表示と時間軸表示を提案する．これらを組み合わせてログ情報の調査作業を行うことで，効率良くかつ容易に作業が行えるようになり，一般ユーザでも自身でログ情報調査作業を行うことが可能になる．さらに我々は，この利点を利用することで既存の不正侵入検知システムが抱えている問題だけでなく，不正侵入対策における人的問題をも改善可能な集団監視による不正侵入対策を提案する．

A Proposal of Novel Intrusion Management Using Log Information Visualization Systems by Multiple Users

Tetsuji Takada[†] and Hideki Koike[†]

An intrusion to the computer becomes a serious threat. Some methods to cope with them are already proposed. Such methods, however, do not come to use widely, because these methods have some problems respectively. We extract the problem from existing intrusion management. As a result of it, we led that periodical log inspection makes a computer more secure against the intrusion. We suggest a log information visualization system that helps inspecting log information. We propose two visualization methods in this research. One is a summary visualization. The other is a time based visualization. Both methods enable an inspector to investigate log information more easily and effectively. This advantage makes it possible for a novice user to investigate log information. We also propose a novel intrusion management that monitors log information by multiple users using visualization systems. This method can improve not only the problem in existing intrusion detection systems but also the problem originated in human factor.

1. はじめに

今日，あらゆる分野で計算機の利用がすすんでおり，その安定運用の重要性について疑いの余地はない．一方，ネットワークを介した計算機への不正侵入や，内部ユーザによる計算機の不正利用は多数発生し，その脅威は増すばかりである[1),2)]．

この問題に対する対策手法として4つの段階からなる不正侵入対策手法が提案されている[3)]．現在，これらの各段階において様々な研究が行われており，Firewallをはじめとする不正侵入防止システムや不正侵入検知システム[4)~6)]が提案されている．

しかし，その一方で不正侵入対策における調査段階の作業は，システムの安全性を強化させるのに必要不可欠であるにもかかわらず，その作業内容は依然としてシステム管理者がエディタ等を用いて手作業により種々のログファイルを調査するという作業形態のままであり，多大な労力が必要とされる作業であるにもかかわらず，その作業を支援するシステムが存在しないのが現状である．

そこで本研究では，不正侵入対策をより堅牢にするためには調査段階における作業が重要であることに着目し，現状における問題点を考察することでそれを認識する．さらに我々は，それらの問題を改善するシス

† 電気通信大学大学院情報システム学研究科情報システム運用学専攻
Graduate School of Information Systems, University of Electro-communications

テムとして情報視覚化を用いたログ情報視覚化システムを提案し，そのプロトタイプを開発した．

我々が提案する手法は，情報視覚化技術を用いてログ情報を視覚化する．これにより文字情報として記録されているログ情報の調査作業を簡単かつ高速に遂行可能にする．また，調査作業が簡単化されることにより，一般ユーザを対策作業に従事させることが可能になる．そこで本研究では，この特徴を利用した集団監視による不正侵入対策手法を提案する．この手法は，既存の不正侵入対策手法における問題点だけでなく，セキュリティ問題において回避の困難な人的問題に対しても有効な方法であることを述べる．

本論文では，2 章で既存の不正侵入対策と，現在の検知および調査作業における問題点，さらに不正侵入対策手法における人的問題についてそれぞれ考察し，3 章で本研究で提案する情報視覚化を用いたログ情報調査支援システムの枠組みとそれによる利点について述べる．次に，提案した視覚化システムを利用した集団監視による不正侵入対策手法について 4 章で述べ，最後に 5 章で，関連研究との比較とプロトタイプシステムについて述べる．

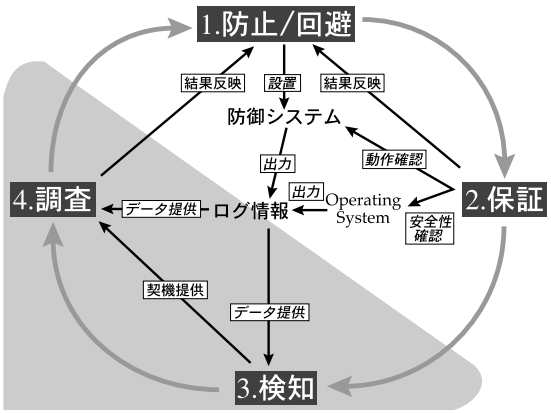

図 1 不正侵入対策の 4 段階
Fig. 1 Four stages in intrusion management.

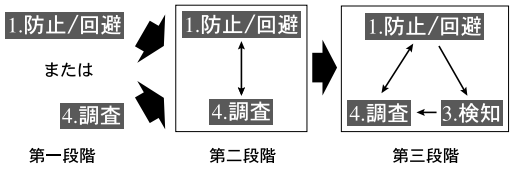

図 2 不正侵入対策の推移
Fig. 2 Transition of intrusion management.

2. 不正侵入対策 その終わりなき戦い

計算機への不正侵入およびユーザの不正利用が計算機の運用管理において大きな問題となりつつある．したがって危機管理の必要性のある運用環境だけでなく，計算機を運用するすべての管理者がこの問題に対して必要な対策を行う必要があり，これは国内法規としても明記されている[7]．

不正侵入対策には “終わり” がないため，対策作業を継続して行うことによりシステムの安全性を強化する必要がある．この特徴から，**図 1** のような 4 つの段階からなる不正侵入対策手法が有効であるといわれている[3]．これは 1. 防止/回避段階でセキュリティポリシーを立案し，種々の防御システムを導入する．2. 保証段階でシステム監査の実施，疑似不正侵入テストにて防御システムの動作確認を行い，3. 検知段階にて不正侵入を監視/検知し，4. 調査段階にて原因追求，犯人追跡のため種々のログ情報の調査を行う，というもので，これらの作業を継続して行うことで不正侵入に対する安全性を強化する手法である．

しかし，現実にはこれらすべての段階を確実に行うのは容易ではなく，多くの運用環境では**図 2** のように不正侵入対策が段階的に導入，実施されていると考えられる．

不正侵入対策を行うきっかけは 2 種類あると考える．1 つはシステム管理者の不正侵入に対する強い危機感によるものであり，もう 1 つは実際に何者かによる不正侵入を経験することである．これによりログ情報の収集と定期的な調査作業または防止/回避システムの導入が不正侵入に対する対策の第一段階として行われるようになる（図 2 第一段階）．

しかし防止/回避対策による防御システムの導入だけではすべての不正侵入を防止できない．よってログ情報の調査を行うことでその不完全さを補完するようになる．一方，ログ情報の調査だけではまったく不正侵入防止の効果がないので，不正侵入防止のため必要な手段を行うことになる．つまり，防止/回避作業と調査作業を併用することでそれぞれの欠点を補完するようになる（第二段階）．

さらに次の段階として，調査段階におけるシステム管理者の負担軽減と多種多様な不正侵入を検知する目的で，不正侵入検知システムを導入する（第三段階）と考えられる．

この考察から，調査段階の作業は不正侵入対策における早期の段階から行う必要があることが理解できる．しかし，その一方で調査作業の内容は依然としてシステム管理者がエディタ等を用いて種々のログファイルを手作業で調査しているのが現状である．つまり，調査段階を除いた他の 3 段階においては，作業を支援す

表 1 不正侵入対策の各段階における支援システム
Table 1 Various tools for intrusion management.

不正侵入対策段階	支援システム例
防止/回避	種々の Firewall，SSH，TCP_Wrapper[8]等
保証	SATAN，COPS，Nessus[9]等
検知	種々の不正侵入検知システム
調査	存在しない

るシステムが存在するにもかかわらず，調査段階の作業を支援するシステムは存在しないという問題がある（**表 1** 参照）．

そこで本研究では，不正侵入対策における調査作業に注目し，その作業を支援するシステムとそれを用いた集団監視による不正侵入対策手法を提案する．次節では，検知作業と調査作業の関係について考察を行う．

2.1 検知作業と調査作業の関係とその問題点

図 1 を見てみると，4 段階の作業は 2 つのグループに分類することができる．それは不正侵入対策の能動的作業ともいえる防止/回避および保証作業と，不正侵入対策における受動的作業といえる検知および調査作業である．本節では不正侵入対策における受動的作業部に焦点を当て，検知作業と調査作業の従来までの関係と今後の改善策について考察する．

図 2 からも分かるとおり，従来までは不正侵入検知という分野は明確に存在せず，システム管理者がログ情報を手作業で “調査” することによって不正侵入を検出していた．しかしログ情報を手作業で調査するには多くの問題が存在する．それらを以下にあげる．

- 文字による情報源
  ログ情報は文字情報として提供される．したがって記録されている情報を把握するためには，それらを読んで理解しなければならず，その認識負荷は大きい．
- ログ情報の多様性と偏在性
  ログに記録されている情報やその記録形式は様々である．またログ情報が存在するディレクトリや情報の取得方法もそれぞれ異なるため，これらに関する知識が必要となる．
- 総合的な判断の必要性
  個々のログファイルに記録されている情報は，不正侵入検知の観点から考えると断片的な情報である．したがって不正侵入の調査では，種々のログ情報を慎重に調査し，それらの判断を総合して不正侵入の有無を判定する必要がある．
- 膨大な量
  調査すべき情報は単一のログ情報でも膨大な量になり，調査には多大な時間が必要となる．さらに前項で述べたとおり，調査作業では複数のログ情報を調査する必要があるため，調査にかかる時間も膨大な時間となる．
- 痕跡情報の抽出
  ログに記録されている情報は，そのすべてが不正侵入に関連した情報ではない．したがって不正侵入に関連した情報を抽出する必要がある．

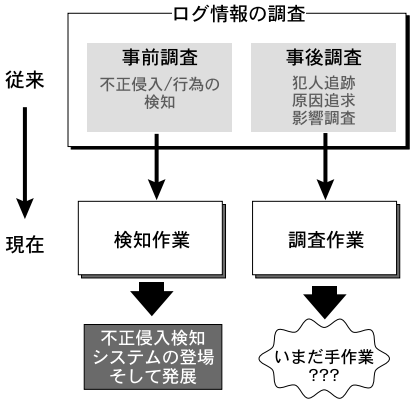

図 3 不正侵入対策における調査作業の推移
Fig. 3 A change of investigation task for intrusion management.

これらの問題点から，ログ情報の調査は単調で時間のかかる作業であることは明白である．また必要とされる知識や技術的要件も高いため，遂行可能なユーザはおのずと限定される．さらに人間による作業のため，ログ情報の認識や情報抽出の判断を誤る可能性をなくすことは不可能である．これらの問題が調査作業の遂行を敬遠させており，結果として不正侵入が発生しても，それらに対する適切な対処が行われないという事態を生んでいる．

この状況をふまえ，従来のログ情報の調査で行われていた役割のうち，事前調査に対応する作業の自動化が行われるようになった（**図 3** 参照）．これが現在の不正侵入検知システムであり，従来の調査作業のうち検知作業を自動化することにより不正侵入を迅速に認識可能にするとともに，システム管理者によるログ情報調査作業の負担を軽減するシステムとして確立したのである．

しかしながら，不正侵入検知システムはその有効性に疑いの余地はないものの，防止/回避段階の作業ほど普及していないと思われる．その原因として考えられる事項を以下にあげる．

- 万能ではない
  不正侵入防御システムと同様，不正侵入検知システムは万能ではなく，検知可能な不正侵入手法は

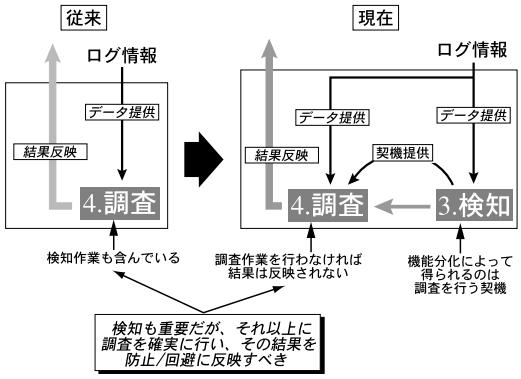

図 4 検知作業と調査作業の関係
Fig. 4 The relation of detection and investigation in intrusion management.

限定される．また不正侵入検知システムでは不正侵入を誤って検知する可能性もある．

- 導入および運用管理の困難さ
  不正侵入検知システムの導入や運用管理に必要とされる知識や技術的な要件は高い．またシステムの初期設定，検知すべき不正侵入事象に関する情報の維持管理，定期的な運用状況の監視等が必要となり，運用管理は容易な作業ではない．
- システムへの負荷の増大
  不正侵入検知システムを導入することで，計算機またはネットワークへの負荷を増大させる可能性がある．
- 汎用性
  検知手法によっては，Operating System の機能に依存するものや，現在の運用機器とは別に不正侵入検知システム専用の機器を必要とするものがある．

これらの問題が，不正侵入検知システムの普及を妨げており，システム管理者の多くは手作業で従来どおりの調査作業，すなわち検知を目的とした事前調査と原因追求等の事後調査を行っていると考えられる（図 3 参照）．

ここで現在の検知作業と調査作業の関係について考える．検知作業とは，従来までログ情報の調査で行っていた作業の一部を自動化したものであることは前述した．つまり，現在の検知作業と調査作業は対象としている入力データが同一なのである．検知作業の確立によって得られるようになった利点とは，不正侵入として疑わしい事象が自動的にシステム管理者に通知されることにより，調査作業を行うべき契機が従来よりも多く得られるようになるということである（**図 4** 参照）．

しかし図 4 からも分かるとおり，不正侵入対策における受動的作業部は入力がログ情報である一方で，その出力は調査作業の結果を防止/回避作業に反映させることである．つまり検知作業が自動化されたとしても調査作業の必要性に変化はない．したがって不正侵入検知システムを導入したとしても不正侵入として疑わしき事象が通知されたときにはログ情報の調査をしなければならないのである．それゆえ調査段階の作業における問題点を改善する必要がある．

上記の具体例として以下のような状況が考えられる．監視対象の計算機でパスワードファイルに見知らぬエントリが追加されていることが不正侵入検知システムで検知され，システム管理者に通知されたとする．これに対しシステム管理者は即座にそのエントリを削除することで対処した．しかし，この通知だけではなぜパスワードファイルが改ざんされたかが不明のままであり，だれがそれを行ったのかも不明である．したがって，前述の対処法では根本的に何も解決されておらず，防止/回避システムにその結果が反映されていないため，同一の手法で再び不正侵入され，パスワードファイルを改ざんされる恐れがある．

この問題も，不正侵入検知システムの導入を阻害し，システム管理者が従来どおり手作業でログ情報を調査しようとすることの一要因であると考える．

2.2 人的問題

本節では，不正侵入対策における人的問題について言及する．不正侵入対策が “終わり” のない作業である以上，その作業を完全に自動化するのはきわめて困難であり，何らかの形で人間の介入が必要である．その点を考慮すると，不正侵入対策における特定者への依存はいくつかの問題を生じさせる．

まず 1 つ目は特定者への依存による人為的セキュリティホールである．不正侵入検知システムを使用するユーザは，そのほとんどがシステム管理者であると考えられる．しかしながら，現在システム管理者がおかれている状況は非常に厳しいといえる[10]．その主たる理由として，1) その多くが専任者ではなく，併任または有識者によるボランティア集団であること，2) システム管理者は有識者ゆえ，本来の業務でも多忙である可能性が高いと想定されること，3) システム管理者は社会的需要に対して絶対数が不足しており，管理者 1 人が管理すべき計算機台数も多くなる傾向が高く，それゆえすべての計算機に対して十分な対策作業が行えない，といった問題があげられる．

これらの要因により，システム管理者だけで不正侵入対策作業を行うことはきわめて困難であるといえ，

システム管理者が何らかの理由で運用環境を不在にする場合には，不正侵入対策がまったく行われない状況を生み出すことになる．

また，システム管理者に対する信頼性の問題もある．不正侵入検知システムが適切に稼働していたとしても，不正侵入通知後にシステム管理者が適切な対処を行わなければ対策作業としての効果は期待できない．また，システム管理者自身が不正を働いていた場合，現状ではそれを検知することはほぼ不可能である．セキュリティにおける最大の問題は人間であるといわれていることからも，特定者へ依存した不正侵入対策は危険であるといえる．

2つ目は対策作業に要求される知識や技術的要件の高さである．多くの計算機運用環境では，不正侵入対策をシステム管理作業の一環と見なし，その作業をシステム管理者に依存していると考えられる．しかしシステム管理作業と不正侵入対策作業に必要とされる知識や技術的要件は異なるため，システム管理が可能なユーザであっても不正侵入対策が可能であるとは限らない．その例として，ftp サーバを構築し，外部に対して ftp サービスを提供することと，anonymous ftp サーバをセキュリティ上安全に運用できるように ftp サーバを構築し，さらに Firewall の透過性を確保するという場合に必要とされる知識や技術的な要件の違いを考えればそれは明白である．

さらに今日の Free UNIX 系 OS の台頭により，初級システム管理者はますます増大すると予測され，システム管理者の不足問題はますます悪化すると考えられる．このような初級管理者は，不正侵入対策はもちろんシステム管理に対する知識や技術も十分でないため，不正侵入防御システムの導入や不正侵入検知システムの利用が困難であることは明らかである．もちろん，一般ユーザが不正侵入に対し不安を抱いたとしても，現状では不正侵入対策に参加することができないという問題もある．

これまでの考察から，不正侵入対策においてログ情報調査作業すなわち不正侵入検知とその事後調査を確実に行うことが，その対策を強化するために必要不可欠である．また図 4 からも分かるとおり，調査作業が遂行されなければ防止/回避段階へのフィードバックが行われなくなり，不正侵入対策をより強固なものにすることが不可能になる．

なお，運用環境に不正侵入防御システムや検知システムを導入するためには利用するユーザの理解が必要となる．そのためにも検知を目的としたログ情報の調査を行うことにより，自身が利用している運用環境が実際に不正侵入の攻撃を受けていることを認識する必要がある．

そこで本研究では，ログ情報の調査作業を支援するシステムとして情報視覚化を用いたログ情報調査支援システムを提案し，これらの問題の改善を試みる．

3. 情報視覚化によるログ情報調査支援システム

これまでの考察から，ログ情報調査作業を定期的かつ確実に遂行する必要がある．そこで我々はその作業を支援するため，情報視覚化を用いたログ情報調査支援システムを提案する．本章ではログ情報視覚化システムとその利点について述べる．

情報視覚化とは，情報を抽象化する能力と図への親しみやすさ等の特徴を利用し，情報に対する人間の理解をより早く深くすることである．さらに単に情報を図として提示するだけでなく，図とのインタラクションも重要視する[11]．

これらの特徴をログ情報に適用することで，人間によるログ情報の把握を促進し，その調査作業を支援する．これにより，従来よりも高い頻度でログ情報調査作業が遂行されることが期待される．ここで我々は，ログ情報の特性を考慮し，不正侵入調査を目的としてログ情報の視覚化を行う際には 2 つの方法が存在すると考える．

1 つは要約表示である．多くの場合，ログ情報は膨大な量である．よって情報視覚化技術を用いたとしても，これらすべてを一度に提示することは人間の情報認識能力を超えてしまい，逆に情報理解のために負担を強いることになる．ここで，ログ情報の量が膨大になる理由の 1 つとして，個々の事象が繰り返し記録されていると考えることができる．具体的な例として「ホスト A から telnet を使用してアクセスした」という情報が，その事象の発生した数だけログ情報の中に存在することがあげられる．ログ情報では，事象と時刻を対にして記録しているため，発生した時刻が異なれば単一事象が複数回記録されるためである（**図 5** 参照）．

不正侵入検知では，監視対象の計算機内において発生したすべての事象の把握が，調査者にとってまずはじめに行うべきことである．すなわち監視対象の計算機において「何が行われたのか」が把握できなければ，ログ情報の調査を行うユーザはそれらに対して不正侵入か否かの判断を行うことができないのである．したがって，計算機内で発生した事象の把握に焦点をおいた視覚化手法として要約表示が必要であるといえる．

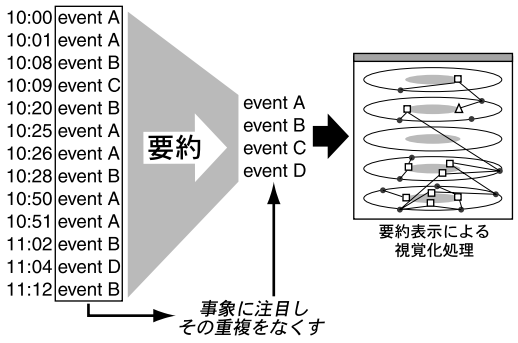

図 5 ログ情報の要約

Fig. 5 Log summarization method for summary visualization.

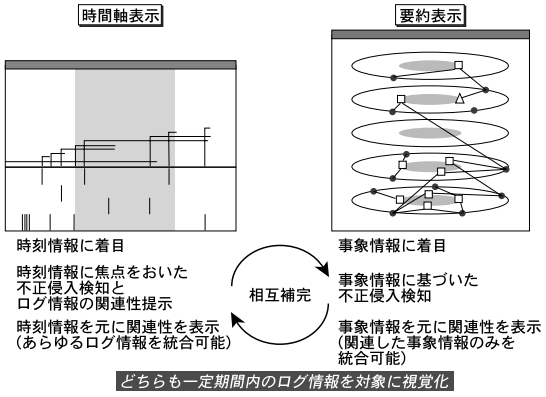

図 6 要約表示と時間軸表示の特徴

Fig. 6 The features of summary visualization and time based visualization.

要約表示とは膨大な量のログ情報から監視対象で発生した個々の事象のみを抽出し，それらの発生時刻や発生回数を無視して視覚化する手法である．つまりログ情報に含まれる時刻情報を無視することでログ情報内の重複をなくし，発生した事象だけを抽出することで，不正侵入検知に必要な全事象の把握を支援する方法である（図 5 参照）．

もう 1 つの視覚化手法は時間軸表示である．この手法は，その名のとおりログ情報に含まれる時刻情報に注目して視覚化を行う方法である．ログ情報は，その量に比例して時刻情報の値域も大きくなる．この問題については，情報視覚化の分野でも様々な研究が行われているが[12),13)]，広範な値域を持つ時刻情報の視覚化手法は，いまだ有効な手法が確立されていない．したがって本研究では，ある一定の期間内に記録された情報を対象とした視覚化を行った．

不正侵入検知では時刻情報も重要な情報であり，時間情報や一定期間内における各事象の頻度を基にした不正侵入検知手法も存在する．また時刻情報は，複数のログ情報を関連づけるための基準情報としても重要である．なぜならば，ある特定のログ情報において疑わしい事象が発見された場合，その判断を確実にするためには該当ログの記録時刻付近における関連ログ情報を調査することが必要不可欠だからである．

また双方の視覚化手法において，複数のログ情報を統合した視覚化を行っている．不正侵入検知では多くの場合，複数のログを調査する必要がある．たとえば，**su** コマンドを使用して特権取得を試行した痕跡を見つけた場合，それを行ったユーザを特定し，次にそのユーザの使用したコマンド群を調査する必要がある．その調査によって不正侵入または不正行為としての疑惑が深まった場合，さらにそのユーザはどこの計算機から監視対象の計算機へアクセスしているか等を調査する必要がある．この例からもログ情報の調査において複数のログを調査する必要があることは明らかである．

情報視覚化を用いて複数のログ情報が 1 つの図として調査者に提示されることにより，調査者はログ情報を個々に手作業で調査する必要がなくなると同時に，調査者自身がログ情報間の関連づけを行う必要もなくなる．結果として関連した複数のログ情報の統合視覚化は，調査作業における作業負荷を軽減することが可能になる．また時間軸表示では，時刻情報を基準として複数のログ情報を統合するため，時間に基づく情報間の関連性が図として明示的に示されるという利点がある．

これら 2 種類の視覚化手法を連携させて使用することにより，次のような効果的な調査方法が可能になる．はじめに要約表示を閲覧することでログ情報に含まれている疑わしい事象を検知し，次に時間軸表示でその事象が発生した時刻前後の関連ログ情報の状況を調査する．その中に疑わしい事象を示す関連ログ情報が存在するならば，それに対する要約表示を調査することで，疑わしい事象を探索するということの繰返しによりログ情報の調査が可能になる（**図 6** 参照）．

3.1 ログ情報の視覚化による利点

ログ情報の視覚化による利点を，検知/調査作業の問題点と関連づけて整理する（**図 7** 参照）．

1 つ目は，文字による情報提示法とその膨大な量である．文字による情報提示では，調査者はそれらを読んで理解しなければならず，記録されている情報を把握するまでの認識負荷が大きいといえる．さらにその量の膨大さが本作業を単調かつ時間のかかる作業にしている．しかし情報視覚化を用いることにより，情報

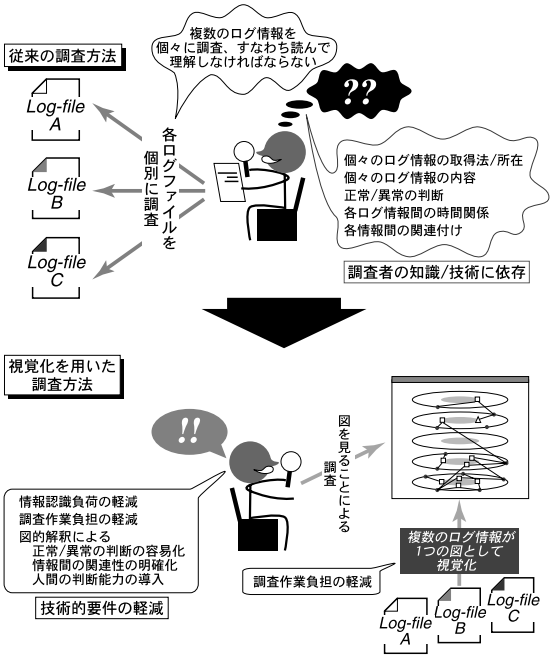

図 7 ログ情報調査における視覚化システムの利点
Fig. 7 The advantages in log information investigation using visualization system.

は抽象化されて図として提示されるため，その認識に必要とされる負担は軽減される．また視覚化により，同一表示領域内において文字表示よりも多くの情報を提示することが可能になるため，前述の特徴とあわせて認識負担を軽減することが可能になる．

2つ目は，ログ情報の多様性と偏在性の問題である．調査者はログ情報の調査を行うにあたって，各ログの取得方法や所在，そして各ログが保持している情報の内容といった事前知識が必要とされる．これは，作業を行うユーザを限定する一因となっている．しかし視覚化システムを用いることにより，これらの技術的要件は視覚化システム内に隠蔽されるため，調査を行うユーザに必要とされる知識は図の解釈方法だけとなる．したがって調査者に必要とされる技術的要件を軽減することが可能になる．

3つ目は，不正侵入の痕跡情報の抽出である．既知の痕跡情報についてはその認識が容易なように図的表現が行われており，その抽出作業を支援する．なお，本システムは不正侵入検知システム同様あらゆる不正侵入の検知が可能なわけではない．双方ともに既知の知識や種々の手法を用いた規則を基に疑わしいと推測される事象を抽出している．しかし視覚化システムの利点は，不正侵入検知の判断に人間の持つ知識を導入可能にすることである．記録されているログ情報を人間に認識させることにより，人間の持つ知識や判断能力を痕跡情報の抽出のために利用することが可能になる．

4つ目は，複数のログ情報の調査を1つの図を閲覧することで可能になるということである．不正侵入検知では，種々のログが保持している情報を理解したうえでなければ不正侵入か否かの判断が不可能である．そのため従来は，事象情報の理解のために複数のログ情報を1つ1つ把握し，その関連づけを調査者が自身で行う必要があった．しかし視覚化システムでは，複数の情報を1つの図として提示でき，かつそれらの関連性を提示することも可能であるため，作業負担を軽減することが可能になる．

このように，視覚化システムによって得られる利点により，検知/調査段階の作業における種々の問題点を改善することが可能になる．

4. 集団監視体制による不正侵入対策手法

本章では，不正侵入対策における問題点の1つとしてあげられている人的問題をも改善可能な集団監視による不正侵入対策手法を提案し，その詳細について述べる．

個々の運用環境に依存するが，多くの運用環境ではシステム管理者ではないものの，それに準じるシステム管理や不正侵入に関する知識を持つ中級ユーザは少なからず存在すると考えられる．そこで本研究で提案した視覚化システムを利用し，これらのユーザを不正侵入対策に参加させることで集団監視による不正侵入対策が可能になる（**図 8** 参照）．提案した視覚化システムを用いることで，調査者は図的表現を理解することだけでログ情報の調査作業を行うことが可能になる．したがって調査者に必要とされる知識や技術的要件を低くすることが可能になり，結果としてシステム管理者以外の多くのユーザも調査作業を遂行することが可能になるからである．

X Window System のツールに xload というプログラムが存在する．これは計算機の負荷状況をグラフとして表示するもので，これを使用することで一般ユーザであっても計算機の負荷を視覚的に認識することが可能になり，現在自分が使用している計算機の負荷が正常なのか異常なのかを知ることが可能になる．そこで計算機の負荷が異常ならば，ユーザはシステム管理者にその旨を通知し適切な対処を依頼することができる．すなわち自身で対処することはできないが，迅速な対処を促すことは可能になる．視覚化システムを用いた集団監視を行うことによって，これと同様の仕組

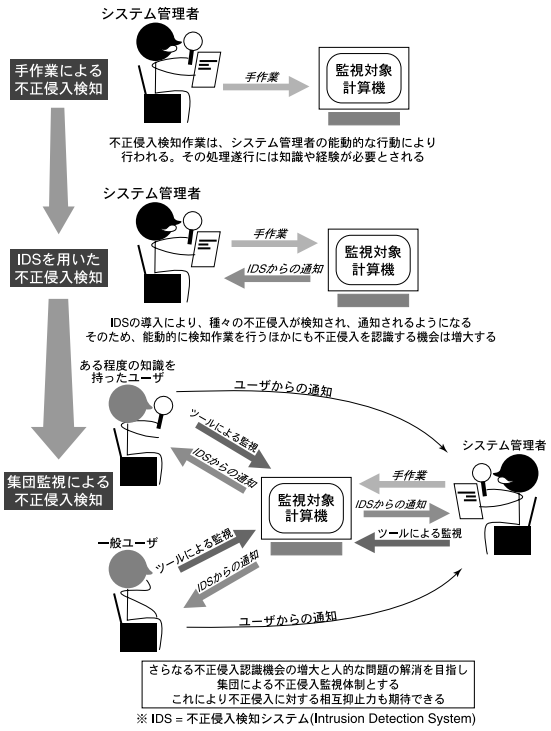

図 8 集団監視体制による不正侵入対策
Fig. 8 Monitoring by multiple users for intrusion detection.

みを不正侵入対策に導入することが可能になる．

集団監視による不正侵入対策が実現されることにより，システム管理者，一般ユーザ双方ともに利点が生じる．システム管理者における利点は以下のとおりである．

- 作業負担の軽減
  システム管理者だけで行っていた作業を多人数で行うことになり，システム管理者の作業負担を軽減することが可能になる．
- 有識者ユーザの能力導入による調査能力の向上
  知識を持った中級ユーザを不正侵入調査作業に従事させることにより，より多くの知識を基にした調査作業が可能になる．
- 人為的セキュリティホールに対する対策
  2.2 節で述べた不正侵入対策における人的問題を解決することが可能になる．これはシステム管理者だけでなく一般ユーザにおける利点でもある．

一般ユーザにおける利点は以下のとおりである．

- 自身による調査作業が可能
  不正侵入調査作業が困難だったユーザも自身で調査作業を行うことが可能になり，一般ユーザに対して自ら検知/調査作業を行えることによる安心感を持たせることが可能になる．
- 不正侵入に対する啓蒙
  一般ユーザは検知を目的とした調査作業を行う中で不正侵入の実態を認識することになり，不正侵入に対する一般ユーザの意識を改善することが可能になる．
- 不正行為に対する抑止力効果
  集団監視になることで，いつ，どこで，だれが不正侵入対策作業を行っているかが不明確になり，安易に不正行為を行うことをとどまらせるといった抑止力効果を生む．

これらの利点からも分かるように集団監視による不正侵入対策は，既存の手法における問題点だけでなく，人的問題をも解決しうる新たな手法である．つまりシステム管理者の怠慢で不正侵入対策を行っていなかったとしても，他のユーザがログ情報を調査することにより不正侵入対策の遂行が可能になる．さらにその結果をシステム管理者に通知して，適切な対処を促すことも可能になる．

システム管理者においても，自身による調査，不正侵入検知システムからの通知に加えて，一般ユーザからの通知が加わることになり，より多くの不正侵入検知手段を得ることになる（図 8 参照）．また，計算機の台数が多いため，システム管理者だけでは個々の計算機に対して十分な対策ができなかった運用環境でも，その作業を他のユーザに遂行させることによって，各計算機においても従来以上に不正侵入対策作業を行うことが可能になる．結果として，既存の手法よりもより強固な不正侵入対策を構築することが可能であるといえる．

5. 考　　察

5.1 既存研究との比較と今後の課題

ログ情報に対する視覚化システムとしては SeeLog [14] や SeeSoft [15] があり，ログ情報の調査における情報視覚化の有効性を示している．また同グループでは Visual Data Mining [16] という論文で，情報視覚化によるデータベースからの情報抽出として電話の不正使用の検出を行い，情報視覚化による不正検出能力の一端を示している．また，Visual Audit Browser [17] では，セキュリティ監査ログに情報視覚化を適用し，ログ情報の解析支援を試みている．

しかし，これらのシステムはログ情報の解析支援や不正検出としての個々のシステムであり，それらを用いた対策手法や運用法についての考察は行われていない．

また不正侵入対策を含めたネットワークセキュリティについて情報処理学会学会誌[18]にいくつかの問題が提起されている．1つ目は,「セキュリティ問題は人間の怠慢と注意不足にあり，それゆえになくなることも爆発的に増えることもないだろう．したがって最低限の努力をし続けていかなければならない」とある．これは本論文における主張と同一であり，図1で示すとおりである．視覚化システムを用いてログ情報の調査作業を支援することで，この枠組みにおける対策が継続して行われるようになると考える．また作業には人間が介在するため，人為的な問題は発生し続けるとも指摘しており，人的問題の改善も可能な本手法は，新たな不正侵入対策手法として有効であるといえる．

2つ目は，啓蒙活動である．「必要なのは正しい知識を基に自ら判断を行うことであり，やみくもに厳重な防御システムを構築することではない」と指摘されている．現状の不正侵入に対する情報配布手段は World Wide Web が中心である．それゆえ関心のあるシステム管理者は能動的に情報を取得することが予測できるが，不正侵入に関心のない一般ユーザがそれらを取得するとは考えられず，それゆえ不正侵入に対する啓蒙を期待することはできない．

しかし本研究で提案する手法では，一般ユーザも視覚化システムを用いてログ情報を見ることにより，現実に発生している不正侵入行為を認識することになる．結果として不正侵入に対する一般ユーザの意識を改善させる効果が期待できる．これにより意識の高いユーザだけでなく一般ユーザをも対象にし，かつ「不正侵入をされる恐れがある」という伝聞ではなくて,「実際に不正侵入されている」という現実の事象を使用することにより，従来よりも確実に不正侵入の啓蒙を行うことが可能になるといえる．

なお，本手法ではログ情報を多くのユーザが見ることが前提になっており，それゆえにプライバシの問題が発生する．これは運用環境におけるセキュリティポリシと関連する問題である．一般の電気通信事業者においてはセキュリティ確保とプライバシの問題の双方を解決する必要があり，現在も有効な解決法が模索されている．

しかし，企業や大学等であれば，その組織に属する機器は特定の目的のために設置されており，その目的や運用規則をユーザに明確にすることで電子メールの閲覧は可能であると考えられている[19]．これはログ情報についても適用可能であると考えられ，本論文で提案する枠組みを使用することは可能であると考えている．しかし，ログ情報の閲覧を無制限に許可することは問題であり，なんらかの制限を加える必要もあると考える．

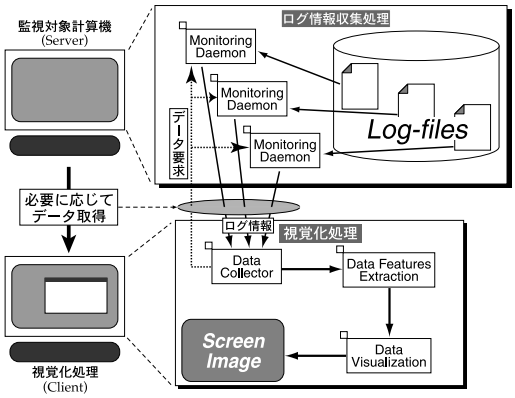

図 9 視覚化システムの処理概要
Fig. 9 An overview of log information visualization system.

5.2 プロトタイプシステム

本研究では，これまでの考察を基にプロトタイプシステムを構築した．本システムは情報収集処理と視覚化処理の2大処理から構成されている．システム構成図を**図 9** に示す．

現在，Sun Microsystems 社の Solaris2.6 が稼働している計算機を監視対象の計算機とし，ユーザの計算機利用履歴情報を wtmpx ログファイル，ユーザのなりかわり情報を sulog ログファイルならびに特定ネットワークサービスへのアクセス情報を TCP_Wrapper[8] を用いて syslog ログファイルから取得している．これらの情報は，ログ情報収集処理が個々のログを監視し，収集している．

視覚化処理では，必要に応じて情報収集処理からデータを取得し，事象情報や時刻情報を抽出したうえで，それらを視覚化する．

要約表示の視覚化方法を，**図 10** に示す．要約表示はアクセス情報，ユーザの利用履歴情報，ユーザのなりかわり情報の各事象に注目した視覚化が行われており，その事象とは，1. 外部からアクセスされる，2. あるユーザでログインする，3. ユーザが他のユーザになりかわる，というストーリに基づいている．これらの事象に対応する図的表現が図 10 上図のように割り当てられており，図を見ることでそれらの事象を把握することが可能である．

また要約表示では同心円状の円盤が層を構成している（図 10 下図参照）．これらの層には，調査者が運用環境におけるアクセス制限や各ホストグループからのアクセスの発生確率に基づいて定義した規則を割

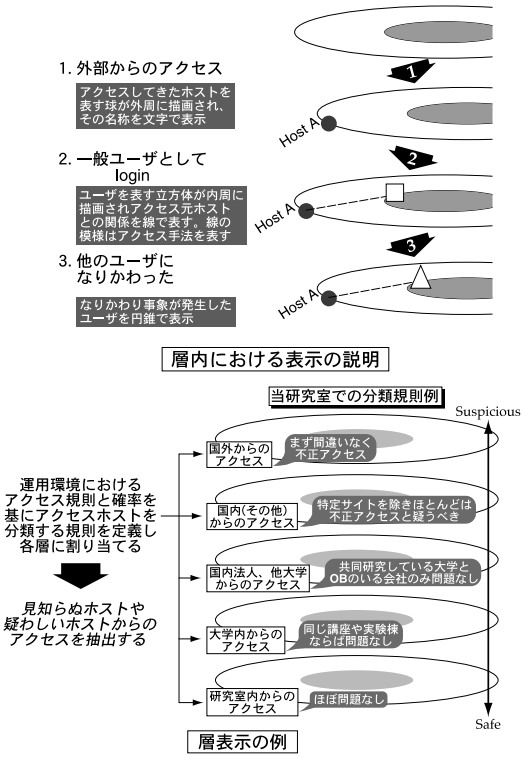

図 10 要約表示の視覚化方法
Fig. 10 The visual method of summary visualization.

り当てることが可能である．この規則を利用することで，アクセス元ホストが各層に分類されて表示される．図 10 下図では，当研究室におけるアクセス元ホストの分類規則を示している．この規則では疑わしいと推測されるアクセスほど層の上位部に表示されるように定義しており，上位層に注目することで不正侵入として疑わしいアクセスや見知らぬホストからのアクセスを認識することが可能である．

これらの図的解釈を前提に考えると，**図 11** の視覚化例では層の最上位層に線が 1 本も接続されていない球が存在する．すなわち見知らぬ計算機からアクセスされているが，ログインすることによるユーザの利用は発生していないということが分かる．この事象は，監視対象の計算機にアクセスしたもののログインして計算機を利用することができなかった不正侵入者による不正アクセスであろうと推測される．

図 12 は時間軸表示による視覚化例とその視覚化方法に関する説明図である．

時間軸表示では，要約表示と同一のログ情報が時刻情報を基準として描画される．プロトタイプシステムでは横軸を時間軸とし過去 24 時間以内に記録されたログ情報を視覚化している．画面上半分はユーザの利

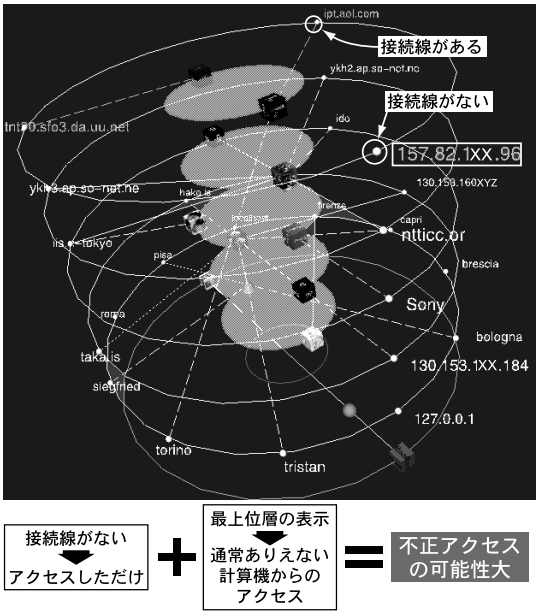

図 11 プロトタイプにおける要約表示
Fig. 11 Summary display on prototype visualization system.

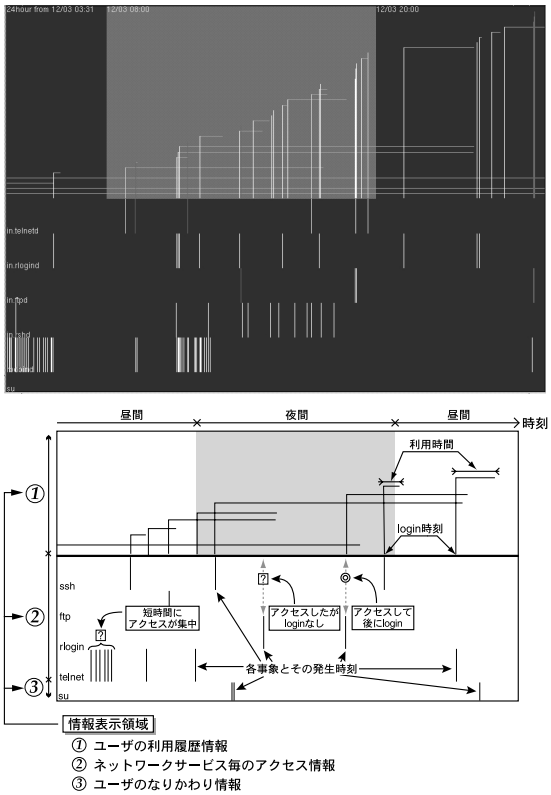

図 12 時間軸表示による視覚化例とその視覚化方法
Fig. 12 An example and the method of time based log information visualization system.

用履歴情報を，下半分ではネットワークサービスごとのアクセス情報とユーザのなりかわり情報を画面を帯状に分割して表示している．図 12 下図は，その詳細を表している．

ユーザ利用履歴情報を表示する領域では，各情報が下から上へそして右へ線が描かれることでユーザの利用履歴情報を表現している．縦方向の線の位置がユーザが login した時刻を表し，横方向の線はその長さでユーザが計算機を利用した時間を表している．なおこの領域内では背景が灰色になっている部分と黒色の部分が存在するが，これは昼夜の時間帯を明確にしており，黒色の部分が夜間を表している．

画面下半分では，個々のネットワークサービスやプログラムが注目すべきログ情報を出力した時刻に相当する位置に縦線を描くことで情報を表現している．ここで注目すべき情報とは，ユーザが指定したサービスやプログラムから出力するログ情報すべてを対象としている．ただし，運用の過程で調査者が表示不要と見なしたログメッセージを規則として定義することでそれらを表示対象外にすることは可能である．

この視覚化手法によって，ログ情報が保持している事象の有無とその時刻が明確になる．また，複数種のログ情報が時刻を基準として視覚化されているためその関連が図的に表現され，ユーザにその関連づけを負担させる必要がなくなる．さらに発生頻度を基にした不正侵入検知も可能になる．

この視覚化によって認識可能な不正侵入事象としては，アクセスされているが login はしていない状況がどの時刻に発生しているかがあげられる．図 12 下図において，ネットワークサービスの領域にアクセスを表す線の表示があるにもかかわらず，ユーザの利用履歴情報を表示する領域の同時刻付近に login して計算機を利用しはじめたユーザがいないことからそれが認識できるからである．

この事象を認識した調査者は，不正アクセスであると推測されるアクセス履歴情報からアクセス元ホストを特定し，その時刻周辺において当該ホストから異なるネットワークサービスを利用して不正にアクセスしていないかを調査する必要がある．さらに，該当時刻付近から利用を開始したユーザのアクセス元ホストを調査する必要もあるだろう．これらの調査作業も時間軸表示による視覚化システムで支援可能である．

一方，短時間内にアクセスログのみが多数発生しているという事象も時間軸表示による視覚化によって検知可能になる．このような事象においてアクセス元ホストがアクセスを許可されているホスト，すなわちそれが内部ユーザの不正行為であった場合，要約表示だけでこの事象を検知することはほぼ不可能である．このように時間軸表示による視覚化を用いることで，要約表示では検知の困難な内部ユーザの不正行為を検知することも可能になる．

本研究室内における稼働実績として，研究室外部の計算機からネットワークを通じた不正アクセスの検出やユーザのなりかわりを行うはずのないユーザによる **su** コマンドの実行検出で数十件の検知例があり，その効果をあげている．またログ情報調査の遂行頻度についても，従来まではまったく作業を行わない日が多数あったが，視覚化システムの導入にともない日に複数回は視覚化システムを使用してログ情報を調査するようになり，作業遂行頻度が改善されることが確認されている．

6. おわりに

本論文では，既存の不正侵入対策手法について検知と調査段階の考察を行い，問題点の抽出を行った．

この考察から我々は，不正侵入対策をより強固するためには，不正侵入防止システムや不正侵入検知システムの導入も重要だが，それに加えて不正侵入調査作業を確実に遂行することが重要であることを明確にした．そこで本研究では，調査作業を支援するシステムとしてログ情報視覚化システムを提案し，その利点について述べた．

さらに，ログ情報視覚化システムを用いることで不正侵入調査作業が簡単化され，一般ユーザを不正侵入対策作業に従事させることが可能になる．本研究ではこの利点に着目し，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を提案した．

この手法は，これまでの不正侵入検知システムが内包していた種々の問題点だけでなく，不正侵入対策を特定者に依存することに起因する人的問題の改善をも可能にする．

今後は，本論文での議論に基づく視覚化システムの構築を進めるとともに，本論文における議論の正当性について評価を継続して行う予定である．

参考文献

1) JPCERT/CC：JPCERT/CC が受け付けた不正アクセス報告件数の推移，
http://www.jpcert.or.jp/stat/reports.html
(Apr. 2000).
2) CERT/CC: CERT/CC Statistics 1988–1999,
http://www.cert.org/stats/cert_stats.html
(Oct. 1999).

3) 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，pp.188–195 (July 1998).
4) Valdes, A., Anderson, D. and Frivold, T.: Next-generation Intrusion Detection Expert System (NIDES) A Summary, SRI-CSL-95-07, SRI International Computer Science Laboratory (May 1995). http://www.csl.sri.com/.
5) Vigna, G. and Kemmerer, R.A.: NetSTAT: A Network-based Intrusion Detection Approach, *14th Annual Computer Security Applications Conference*, pp.25–34 (Dec. 1998).
6) Bro, P.V.: A System for Detecting Network Intruders in Real-Time, *Proc. 7th USENIX Security Symposium* (Jan. 1998).
7) 警察庁：不正アクセス行為の禁止等に関する法律，http://www.npa.go.jp/hightech/fusei_ac2/houann.htm (Aug. 1999).
8) Wietse Zweitze Venema: TCP Wrapper. ftp://ftp.porcupine.org/pub/security/index.html.
9) Deraison, R.: The Nessus Project, http://www.jp.nessus.org/.
10) 警察庁：ハイテク犯罪に関するアンケート. http://www.npa.go.jp/hightech/enquete/index.htm (Feb. 1998).
11) 平川，安村（編）：ビジュアライゼーション，bit 別冊ビジュアルインタフェース—ポスト GUI を目指して，pp.22–44, 共立出版 (1996).
12) Carlis, J.V. and Konstan, J.A.: Interactive visualization of serial periodic data, *11th Symposium on User Interface Software and Technology*, pp.29–38 (Nov. 1998).
13) Rekimoto, J: Time-machine computing: A time-centric approach for the information, *12th Symposium on User Interface Software and Technology*, pp.45–54 (Nov. 1999).
14) Eick, S.G., Nelson, M.C. and Schmidt, J.D.: Graphical Analysis of Computer Log Files, *Comm. ACM*, Vol.37, No.12, pp.50–56 (1994).
15) Steffen, J.L., Eick, S.G. and Sumner. Jr., E.E.: SeeSoft – A tool for visualizing line oriented software statistics, *IEEE Trans. Softw. Eng.*, Vol.18, No.11, pp.957–968 (1992).
16) Wills, G.J., Cox, K.C., Eick, S.G. and Brachman, R.J.: Visual Data Mining: Recognizing Telephone Calling Fraud, *Data Mining and Knowledge Discovery*, Vol.1, No.2, pp.225–231 (1997).
17) Hoagland, J.A.: Audit Log Analysis Using the Visual Audit Browser Toolkit, Technical Report, CSE-95-11, Computer Science Department U.C.Davis (1995). http://seclab.cs.ucdavis.edu/awb/AuditWorkBench.html.
18) 浅香 緑，野村隆昌：情報処理インタラクティブエッセイ，情報処理，Vol.40, No.11, pp.1142–1147 (1999).
19) 生田哲朗，名越秀夫：LEGAL EYE 社員の電子メイルをチェックするのは違法か，日経 Internet Technology，pp.154–155 (Aug. 1999).

(平成 11 年 12 月 6 日受付)
(平成 12 年 6 月 1 日採録)

高田 哲司（学生会員）

1995 年電気通信大学大学院電気通信学研究科電子情報学専攻修士課程修了．現在，電気通信大学大学院情報システム学研究科情報システム運用学専攻博士課程在学中．情報視覚化の研究に従事．特に情報視覚化，不正侵入検知に関心がある．IEEE/CS 会員．

小池 英樹（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学大学院情報システム学研究科助教授．現在に至る．1994〜1996 年 U.C. Berkeley 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，情報検索システム，パーセプチュアルユーザインタフェース，情報セキュリティに興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞受賞．IEEE/CS, ACM，日本ソフトウェア科学会各会員．