ログ情報の視覚化による不正侵入検知システム

Intrusion detection system using a visualization of logging information

高田 哲司　　小池 英樹*

Summary. Today, computer security is recognized a critical problem in information systems. System administrator must do two things. One is to build a computer security system such as firewall. The other is to monitor a various logging information periodically. However, it is time consuming to analyze logging information which is generally written in text. Therefore, the latter work tends to be disregarded.

In this research, we proposed to visualize logging information of computer systems for intrustion detection. It makes easy to recognize a vast amount of logging information. Our visualization system integrates two or more logging information into one visualization. It lighten administrator's burden in investigating logging information.

We developed visualization system of computer access log and command execution log. Using our system, it becomes easier to detect intrusion.

1　はじめに

今日、コンピュータセキュリティの重要性について疑う余地はない。計算機をネットワークに接続して利用する場合、セキュリティ対策を行う必要がある。主なセキュリティ対策は、ファイアウォールをはじめとしたセキュリティシステムの構築と定期的なシステム監視の二つであると考える。しかし多くの運用環境では、後者のシステム監視がおろそかにされがちである。

そこで本研究では、不正侵入検知を目的としたログ情報の視覚化を行った。ログ情報が視覚化されることにより、従来の文字による表示よりも直感的に情報を理解する事ができ認識負荷を軽減する。また複数のログ情報が一つの表示に統合される事で不正侵入調査を容易にする。

本研究では前述の考えに基づき、ログ情報視覚化システムを開発した。以降では不正侵入検知の問題点とログ情報の視覚化に関する考察、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　不正侵入検知の問題点とログ情報の視覚化

不正侵入検知の問題点

不正侵入対策は大きく二つある。それはファイアウォールをはじめとしたセキュリティシステムを構築することと、OSやセキュリティツールが生成するログを監視し、

* Tetsuji Takada, Hideki Koike, 電気通信大学大学院 情報システム学研究科

不正侵入がない事を監視することである。しかし後者の監視作業は以下の理由によりおろそかにされがちである。

1. ログ情報は膨大な量である
   システム管理者は定期的に膨大な量のログ情報を監視し、疑わしい記録がないことを確認しなければならない

2. ログ情報が偏在している
   前述の監視作業は必ずしも単一のログ情報が対象というわけではない。状況によっては複数のログ情報を個別に調査し、これらの調査結果をもって不正侵入が発生していたか否かを総合的に判断しなければならない

3. 極めて単調な作業である
   既存のログ情報は文字によって記録されている。その情報の認識には読解し、それらを理解する必要があり、認識負担が大きい。さらに、調査対象は単一のログファイルとは限らないので、不正侵入がないと判断できるまでそれを繰り返さなければならない。

そこで本研究では、不正侵入検知を目的としてログ情報を視覚化する。ログ情報を視覚化することにより以下の利点が考えられる。

- 認識負荷の軽減
  ログ情報が視覚化されることで、文字による表示よりも直感的にログ情報の理解が可能になる。したがってログ情報の認識負荷が軽減される

- ログ情報の統合表示
  複数のログ情報が一つの図として統合されて視覚化されることにより、複数のログ情報を個別に調査する必要がなくなる

- 不正侵入として疑わしい挙動の明白化
  図的に視覚化されることにより、平常時のシステム挙動と不正侵入として疑わしい場合の挙動の違いが明白になる。これにより不正侵入として疑わしい状況の把握が初級者でも可能になる

ログ情報の視覚化と時刻情報

ログ情報とは、**「ある事象とその発生時刻の対が、時刻順に記録された情報」**と言える。したがってログ情報の視覚化において時刻情報の扱いは重要な問題となる。

本研究では、手始めに時刻情報を使用してオブジェクト位置を決定するシステムを試作した。しかしその試作システムでは、不正侵入に関する情報が得にくいことがわかった。したがってログ情報の視覚化は、時刻情報を基準にするのではなく、ログ情報に含まれる事象情報に焦点を当てて行うことが望ましいという結果を得た。よって本研究では、この知見を基にシステムの構築を行う。

3　ログ情報視覚化システム

本研究では、UNIXが動作している計算機を対象に、不正侵入検知を目的としたログ情報視覚化システムを開発した (図1)。本章では、開発した試作システムについて述べる。

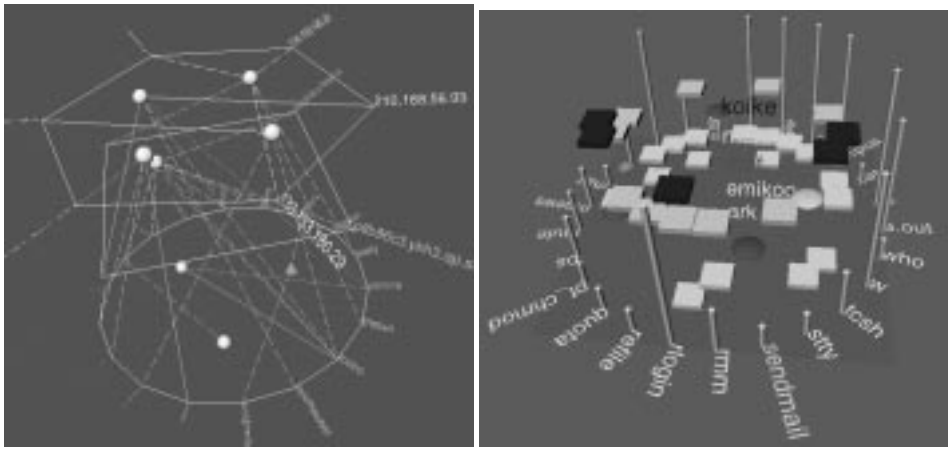

図 1. ログ情報視覚化システム

3.1 システム構成

本システムは、二つの処理から構成される。

- 情報収集処理
  OSやセキュリティツールが生成する様々なログ情報やシステムの状態を監視し、情報を収集する。現在Sun Solaris2.6上で動作しており、wtmpxファイル、syslogファイル、sulogファイル、acctファイルから情報を収集している
- 視覚化処理
  情報収集処理で得られた情報を三次元グラフィックスを用いて視覚化する。またユーザからのインタラクションを受け付け、表示データのフィルタリングや視点の制御を行う

3.2 視覚化手法

本研究では二つのシステムを試作した。本節ではそれぞれの表示法について説明を行う。

アクセス状況の視覚化

図1左は、計算機へのアクセス状況を視覚化したシステムである。計算機へのアクセスとは、「あるユーザがある計算機(ホスト)からある方法でログインする」ということができる。そこで本システムでは、ホストとユーザ情報を円形状に配置し、その関係を線で結ぶことでアクセス状況を視覚化した。

円形状に視覚化した理由は以下の通りである。

1. ホスト、ユーザの二者間の関係がコンパクトに表示可能であり、その関係を表す線の交差も少ない
2. 視覚化情報を回転させる事で、概要を見ながら同時にその詳細情報も監視する事が可能

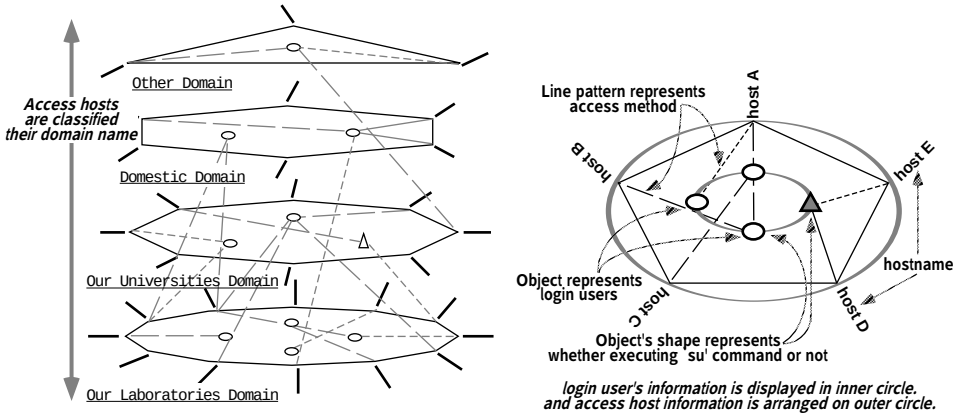

図 2. アクセス状況視覚化の表示方法

アクセス元ホストおよびユーザ情報は、層をなしている平面上に配置される。この層は、アクセス元ホストを分類しており、その分類基準にはドメイン名を用いている。現在、層の下位レイヤから順に研究室内、大学内、国内、その他のドメインの四つに分類している (図2)。よって上位のレイヤにホスト名が表示された場合、それが不正侵入によるアクセスである可能性が高いといえる。

各レイヤは、同心円状に情報が配置される (図2)。外周にはアクセス元ホスト名が文字で、内周にはログインユーザが球または円錐のオブジェクトで描画される。円錐形のオブジェクトは、そのユーザが "su" コマンドを実行したことを表し、それが赤色であれば "su" コマンドによるユーザのなりかわりに成功した事を意味する。またユーザオブジェクトの属するレイヤは、該当ユーザのアクセス元ホストが属するレイヤのうち最上位のものとなる。

ユーザとアクセス元ホストの関連は、線で結ばれることで表される。またこの関連を表す線は、その描画パターンによって各アクセスで使用されたプロトコルを表す。telnetやrloginならば粗い破線、ftpならば細かい破線、両方法によるアクセスがあった場合は実線によって線が描画される。

また本システムでは、その表示情報量の増加にともない、ユーザとアクセス元ホストの関連を表す線が全体の視認性を悪化させる。そこでマウスによるインタラクションによって、ユーザの注目情報に関連する線だけを表示することを可能にした。さらにユーザオブジェクトおよびホスト名をピッキングすることにより、線表示が個々の情報に関連したものに限定され、表示の視認性が向上する。

コマンド 実行状況の視覚化

図1右は、コマンドの実行状況を視覚化したシステムである。

本システムでは、実行コマンド名がその実行回数を表す円柱とともに円形に配置され、その内側には各ユーザ毎のコマンド実行状況を表すオブジェクト群が層状に描画される。また各レイヤの中心にはユーザ名が表示される。

各レイヤに表示されるオブジェクトは、その形状がコマンドの実行形態を表す。四角ならば制御端末からの入力による実行、球ならばcronやrshなど制御端末以外

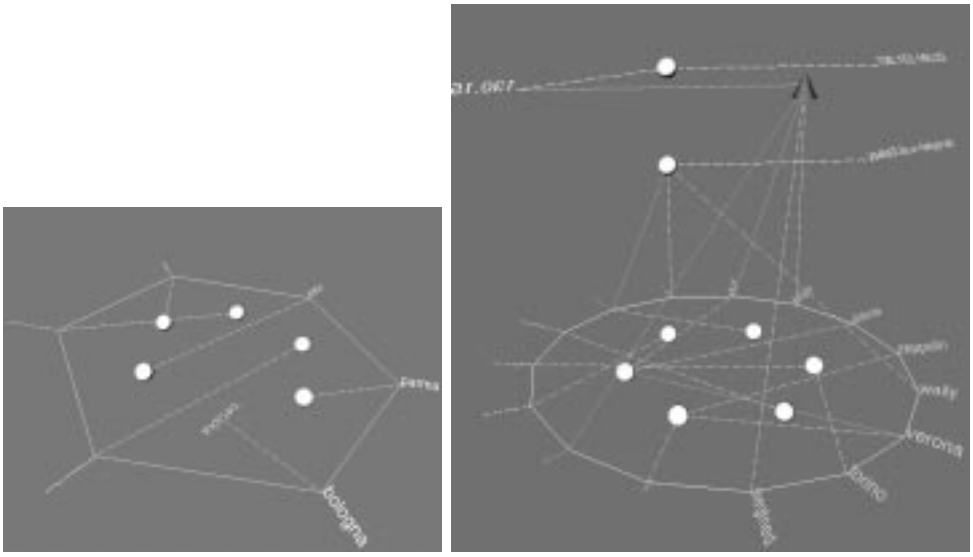

図 3．不正侵入検知例

からの実行であることを意味する。なおオブジェクトがない場合は、そのコマンドをユーザが実行していないことを表す。

また各レイヤの中心に表示されるユーザ名をピッキングすることで特定ユーザのみ、さらには特定ユーザの特定セッションのみの表示へと表示情報を興味のある情報のみへ制御することが可能である。これによりユーザの注目する情報のみの表示にすることができ、視認性が向上する。

4　不正侵入検知例

本章では、アクセス状況視覚化システムを例にとり、どのような不正侵入が検知可能かを示す。不正侵入であると考えられる状況として以下の例を挙げる。

1. 見知らぬ計算機からのアクセス
2. 複数ドメインからの同時アクセス
3. “su” コマンドの実行

図3左は平常時の表示例であり、右は疑わしい場合の表示例となる。図3右では上記の三つの状況がすべて視覚化されている。**1**の状況は、レイヤの上位層にアクセスしたホスト名が表示されることで表される。これにより研究室や大学内以外の計算機からアクセスされている事が認識できる。**2**の状況は、ユーザオブジェクトに複数のレイヤからアクセスを表す線が描画されていることで表される。またアクセスを表す線が同一レイヤ内のみであっても、複数の線がある場合は異なるドメインからのアクセスという場合もあり得るため、前述同様に疑わしいと言える。**3**の状況は、円錐形のユーザオブジェクトが存在することで表される。該当するユーザは “su” コマンドを実行した事を表しており、前述通り、色によってその成否が認識できる。

5　問題点と今後の課題

本章では、本システムにおける問題点/今後の課題について述べる。

1. 情報収集処理について
   - 情報記録ファイルの改ざん、削除防止
     情報収集処理では、収集した情報をファイルに保存している。これは不正侵入者によって改ざん/削除される危険がある。“ls” コマンドで見えないファイルにする、またメモリ上に情報を維持するなどの対策が必要である
2. 視覚化処理について
   - 時刻を基準とした視覚化
     今回のプロトタイプによる考察から、時刻を基準とした視覚化は概要を把握するのに適さないことがわかった。しかし不正侵入に関する調査のため、局所的な時間関係は必要となる。時刻情報の視覚化手法や、概要表示との統合方法なども含めた検討が必要である
   - 様々なログ情報の視覚化
     現状は、計算機へのアクセス状況とコマンドの実行状況の視覚化システムだけである。これだけでは不正侵入検知の情報源として不十分である。多様化する不正侵入に対し、それらの検知が可能になるよう、さまざまな情報の視覚化を試みる必要がある。

6　おわりに

本研究では不正侵入検出を目的としてログ情報を視覚化した。

ログ情報の視覚化方法についてプロトタイプを試作し考察した結果、時刻情報にとらわれず事象情報に注目した視覚化がログ情報の概要把握にとって望ましいという知見を得た。またログ情報が視覚化されることにより以下の利点がある。**1**. 文字による表示より直感的に情報を認識でき、認識負荷を軽減する。**2**. 複数のログ情報が一つに統合表示されることで、不正侵入の調査負荷を軽減する。

前述の考えに基づき、計算機へのアクセス状況とコマンドの実行状況に関するログ情報視覚化システムを開発した。今後は、視覚化手法の洗練と実運用環境下における不正侵入検知の評価を行う予定である。

参考文献

[1] Stephen G. Eick. Michael C. Nelson. Jeffery D. Schmidt, Graphical Analysis of Computer Log Files, *COMMUNICATIONS OF THE ACM* Vol.37, No.12, pp50-56, 1994

[2] Phillip A. Porras. Peter G. Neumann, EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, *National Information Systems Security Conference*, 1997 (http://www.csl.sri.com/emerald)

[3] Teresa F. Lunt. Detecting Intruders in Computer Systems, *Conference on Auditing and Computer Technology*, 1993

[4] 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