ヒューマンインタフェース 88－8
（2000．5．12）

3次元らせん表示を用いたUNIXログの視覚化

關根 章裕　　小池 英樹

電気通信大学情報 システム学研究科

計算機に侵入された場合における唯一の情報源にログがある。よって、ログの調査は非常に重要である。しかしながら、ログに記録されている情報量は膨大であり、内容は複雑である。複数のログの比較調査になると、その情報量と内容の複雑さから、比較調査作業はより困難となる。そこで本研究では、一次元時系列データであるUNIXログを3次元らせん表示を用いて複数同時に視覚化することで、従来のウインドウによるテキスト表示の時よりも多くのデータをコンパクトに表示する。さらに特徴情報の抽出を行うと共に、ログ間の相互関係を表示することによる、ログの調査作業の軽減をはかるための手法を提案する。

Visualization of UNIX log using 3D Spiral

Akihiro Sekine　　Hideki Koike

Graduate School of Information Systems

University of Electro-Communications

Summary. This paper described a novel visualization technique for UNIX log using 3-D spiral. The 3-D spiral visualization makes it possible to display larger number of log entries than text-based log viewers. Moreover, it becomes much easier to recognize periodical events. Using this framework, we visualized three UNIX log files such as wtmpx log, pacct log, and sulog. Also those three logs aresimultaneously visualized in one spiral.

1. はじめに

最近の官公庁への不正侵入事件に代表されるように、不正侵入事件が頻発している。計算機への不正侵入が発生した場合には、不正侵入者の行動追跡のために、計算機に残されたさまざまな状態遷移を記録したものである複数のログファイル（以下、単にログと略す）を調査する。すなわち、ログこそが不正侵入が発生した場合における唯一の証拠である。そのため、ログの調査は非常に重要である。

そこで、本研究では、単一及び複数のログの調査の軽減を目的とする、3次元らせん表示を用いた視覚化手法を提案する。

以下、2章では従来のログの調査方法と問題点を、3章では3次元らせん表示の提案を、4章では実装を、5章ではUNIXログの視覚化例を、6章ではUNIXログの比較検討例を、7章では考察を、8章では、まとめと今後の課題を述べる。

2. 従来のログ調査方法の問題点

2.1 一次元時系列データ

ログは、システムの状態遷移や、ユーザのシステム内での行動が、起きた時間順に記録された一次元時系列データである。

1つのログを調査する場合は、画面またはウインドウに記録された時刻順に従い、ログエントリ1つにつきその内容を1行でテキスト表示する。この調査方法の欠点について述べる。第1に、ログの情報量は膨大であるため、全てのログエントリを表示することは不可能であり、そのため数日分、あるいは数時間分のログエントリしか表示できない。第2に、テキスト表示であり、かつ、表示できる

時間範囲が狭いため、１日間隔、あるいは１週間間隔で記録されるような周期的に現れるログエントリの発見は困難である。第３に、色で識別されていないテキストで表示されるため、ログエントリの内容による分類（rootのログインと一般ユーザのログインなど）を把握することが困難である。

2.2 複数のログの調査方法と問題点

従来の方法で複数のログ間の関連を調査する場合、ウインドウを複数開き、そこにログを表示し、各ウインドウを行ったり来たりしながら調査を行う（図１）。

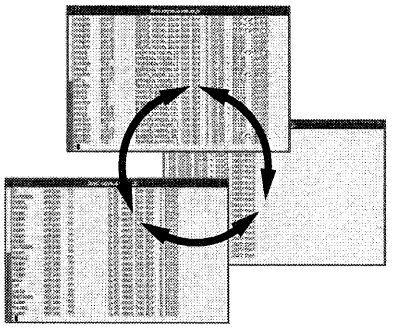

図１ 従来のログの調査方法

この調査方法における欠点を述べる。第１に、ウインドウを行き来する必要があるため、非効率的かつ、重要な情報を見落とす可能性がある。第２に、表示しているログ同士の時間範囲の一致を図ることが難しいため、ログエントリ同士の時間的なつながりの把握が困難である。第３に、複数のウインドウで別々にログを表示しているので、個々のログエントリ内容の統合を困難にしている。

3. ３次元らせん表示の提案

３次元らせん表示を用いてUNIXログを視覚化する目的について述べる。単一のログを表示した時においては、（１）出来るだけ多くのログエントリを描いた上でその特徴を抽出するために、膨大なログエントリをコンパクトに表示し、（２）不正に周期的にシステムの情報を送信していると思われるようなコマンドなどを発見するために、周期的に記録されたログエントリの発見を容易にし、さらに、（３）ログエントリの内容に応じてアイコンの色を変えることで、ログエントリ内容の把握を容易にする。

また、複数のログを表示した時においては、（１）比較調査を従来よりも効率的にすることで重要な情報の見落としを防止し、（２）複数ログの比較調査を容易にするために、表示しているログ同士の時間範囲を一致させ、（３）個々のログエントリの内容を総合して調査することで、複数のログエントリから把握できる内容の発見を支援する。

4. 実装

4.1 構造

３次元らせん表示を用いてUNIXログを視覚化するシステムは、さまざまなログフォーマットを統一的に扱い描画するために、ログ読み込みプラグインと３次元らせんブラウザの２つの部分からなる。

ログ読み込みプラグインは、さまざまなフォーマットで記録されているログからログエントリを読み出し、ログエントリ一つ一つを３次元らせんブラウザで扱える共通のデータフォーマットに変換する。３次元らせんブラウザは、これらを共通データフォーマットになったログエントリの内容に基づき、ログエントリの描画を行う。この概念を図２に示す。

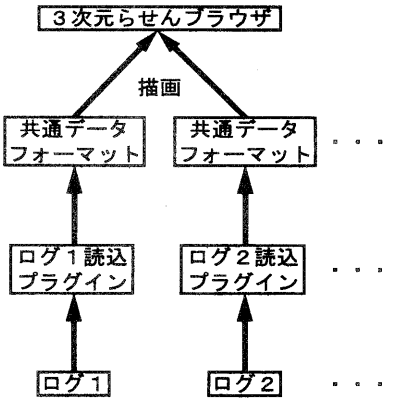

図２ ３次元らせん表示の構造

4.2 共通データフォーマット

共通データフォーマットは、ログエントリが記録された時刻、ログの内容、らせん表示するときのアイコンと色といった情報で構成されている。このようなプラグイン形式と共通データフォーマットを用いた理由は、プラ

グインをプラグイン・ディレクトリに追加するだけで、新たに別のログの読み込みが可能となる点であり、共通データフォーマットの採用により、全てのログの表示を3次元ブラウザ側で統一的に扱えるためである。これにより、特定のログのためにブラウザ側は特別な処理を行う必要が無い。

4.3 視覚化モデル

次に3次元らせん表示の概念についてのべる。3次元らせん表示では、膨大なログの描画を簡潔にするために、1つのログエントリが1つのアイコンとして、らせんの上に描かれる。また、ログエントリの内容に応じてアイコンの色を変えることで、ログエントリの把握を容易にしている。まず、単一のログを3次元らせん表示を用いて視覚化したときの概念図を図3に示す。図3において、y軸正の方向にいくほど時間の新しいログエントリを表示している。また、ログエントリの記録時間の認識を容易にし、ある時間帯に集中して記録されるログエントリを把握するために、らせん一周を12時間または24時間としている（マウス操作によって変更可能）。

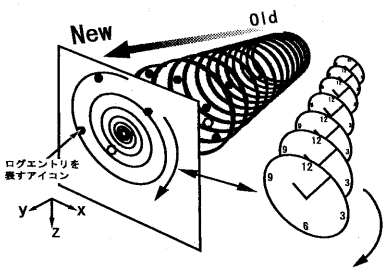

図3 単一ログの視覚化

さらに、複数のログを3次元らせん表示を用いて視覚化し、比較検討するときの概念図を図4に示す。

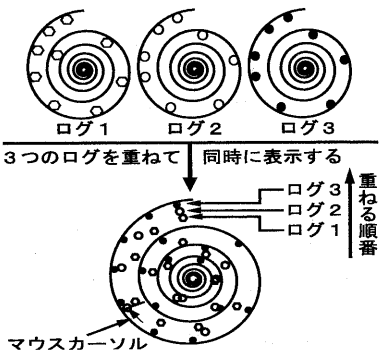

図4 複数ログの統合

3次元らせん表示を用いて複数のログを視覚化し比較検討する場合、複数ログの時間範囲を統一するために、複数のログを一つのらせんにまとめて同時に表示する。こうすることで、複数の異なったログ内にほぼ同じ時刻に記録されたログエントリの認識が容易となるので、それらの内容の統合した結果発見される事実の認識を支援することが可能となる。図4では、ログ1、ログ2、ログ3の順番でらせんを重ねて表している。重ねる順番によって、一番最後に重ねたログのアイコンがらせんの一番外側に表示される。

4.4 ユーザインターフェース

4.4.1 ログエントリ内容の表示

従来のウインドウ表示と3次元らせん表示とのユーザインターフェースの違いについて述べる。らせん表示では、画面下部にらせんがあらわす時間範囲が表示される（図5）。また、ログエントリを表すアイコンにマウスカーソルを重ねることで、画面下部にログの内容が表示され、それと同時に、そのログエントリが記録された時刻を線であらわす。また、ログイン期間などの場合は線が多数描かれ、扇型となる。こうすることで、ログイン期間を記録したログエントリなどの場合にはその期間を視覚的に表示でき、その結果、ログイン期間の認識を容易にする。

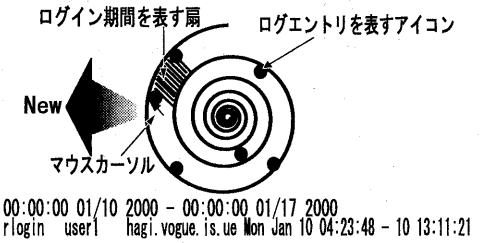

図5 ログエントリ内容の表示

4.4.2 タイムシフト

ウインドウ表示では、時間的に新しい（古い）ログを表示するためには、ウインドウについているスクロールバー、あるいはカーソルを上下に動かしていたが、3次元らせん表示では、Shft+ マウス右ボタンでカーソルを画面左右に動かすことで、らせんをネジのように動かすことが出来、時間的に新しい（古い）ログを表示する（図6）。すなわち、ネジのように動かすことがスクロールバーを上下に動かすことに相当する。

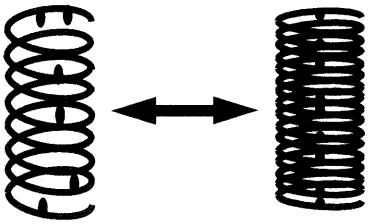

図６ スクロール

また、３次元らせん表示では表示できる時間範囲の変更もマウスによって行う。これは、ウインドウに表示できるログの行数を変更することに相当する。Shift+ マウス右ボタン＋マウス中ボタンでカーソルを上下することによって、ログ１日分から、１週間分、１ヶ月分、１年分と連続的に表示できる時間範囲を変更できる（図７）。この操作方法によって、利用者が見たいと思った時間範囲を瞬時にインタラクティブに変えられ、かつ、表示できる時間範囲が変わることで、例えば、１週間間隔で記録されているログの発見が容易となる。

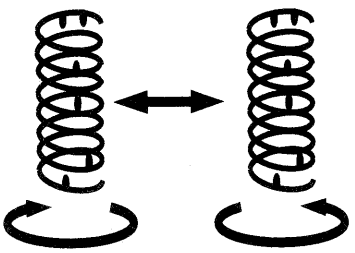

図７ 表示時間範囲の変更

さらに、らせん１周３６０度が表す時間範囲を Shift+ マウス中ボタンでカーソルを左右に動かすことで１２時間か２４時間のどちらかに変えることが出来る。

4.4.3 視点移動

らせんを見る位置も変更が可能である。Alt+ マウス中ボタンでカーソルを上下に動かすことで、視点をらせん全体を縦から真上、真上から縦とインタラクティブに変える事が出来る（図８）。

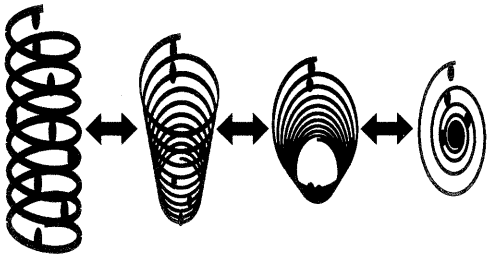

図８ 視点移動（真上 - 縦）

さらに、Alt+ マウス右ボタン＋マウス中ボタンでカーソルを左右に動かすことで、視点をらせんに近づけたり遠ざけたり出来る（図９）。これをらせんを真上から眺めているときに行うことで、時間的に古いアイコンを拡大してみることが可能となる。

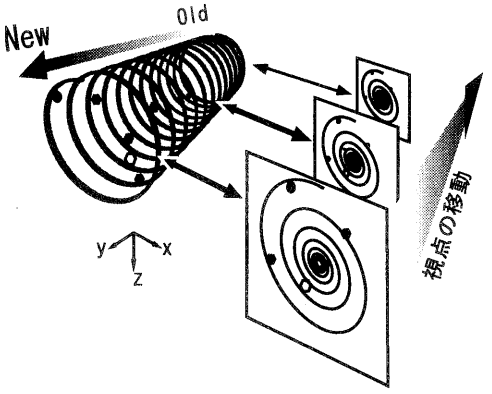

図９ 視点移動（ズーム）

5. UNIX ログの視覚化例

この章では、実際に３次元らせん表示を用いて各種 UNIX ログを視覚化したものを示す。

5.1 時間範囲の変更

図１０に、１週間の wtmpx ログ（誰が、いつ、どのホストからログインし、いつログアウトしたのか）を３次元らせん表示を用いて視覚化したものを示す。図１１に、１ヶ月のログを３次元らせん表示を用いて視覚化したものを示す。このように、らせん全体の長さは変化させずに、らせん１周３６０度の個数を増やすことで、らせん全体が表している表示時間の範囲だけを変えることが出来る。

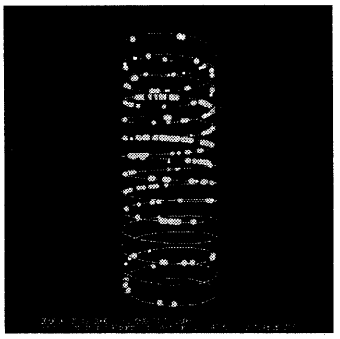

図 10 時間範囲の変更

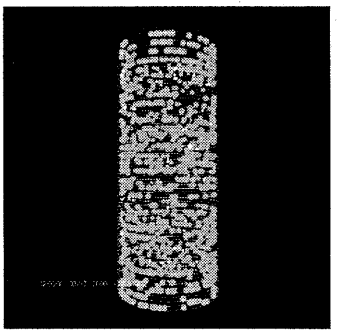

図 11 時間範囲の変更

次に、図１２に、wtmpx ログを視覚化したものでらせん一周を１２時間に設定したものを示す。図１３に、らせん一周を２４時間に設定したものを示す。

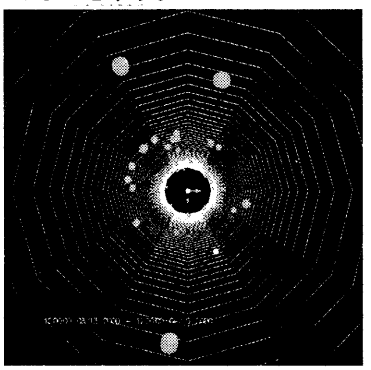

図 12 らせん１周が表す時間の変更（１２時間）

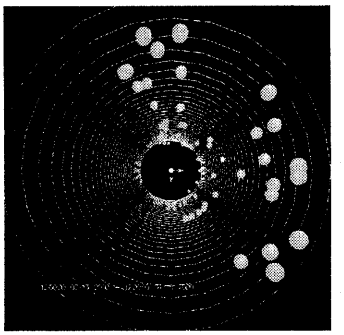

図 13 らせん１周が表す時間の変更（２４時間）

この表示例では、ある一人のユーザによるログイン、ログアウトだけ表示するようにあらかじめフィルタがかけられている。図１２では、１２時間表示のためこのユーザの特徴があまりよくわからないが、図１３では、２４時間表示にすることで特徴があらわれてくる。この例におけるユーザは、主に夜間にログインし、早朝にログアウトしていることが容易に把握できる。

5.2 wtmpx ログの視覚化例

図１４に、wtmpx ログ（誰が、いつ、どのホストからログインし、いつログアウトしたのか）をテキストで表示したものを示す。図１５に、wtmpx ログを３次元らせん表示を用いて視覚化したものを示す。

```
誰が    どの端末に どのホストから          いつから          - いつまで
nezumi  pts/6      host1.vogue.is.uec.ac.jp Wed Apr 12 16:25   ログイン中です。
ushi    pts/4      host2.vogue.is.uec.ac.jp Wed Apr 12 16:20 - 16:26  (00:06)
tora    pts/4      host3.vogue.is.uec.ac.jp Wed Apr 12 15:49 - 16:17  (00:28)
usagi   pts/5      host4.vogue.is.uec.ac.jp Wed Apr 12 15:43 - 17:35  (01:51)
tatsu   pts/2      host5.vogue.is.uec.ac.jp Wed Apr 12 15:40 - 16:28  (00:48)
```

図 14 wtmpx ログのテキスト表示

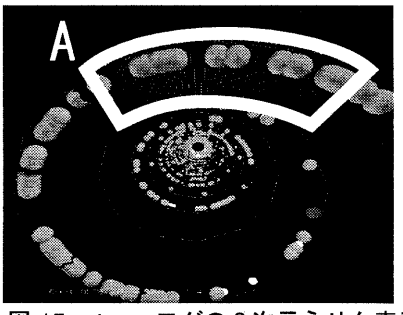

図 15 wtmpx ログの３次元らせん表示

これにより、ユーザがログインしていた期間が扇形（図１５のＡの部分）に表示されるため、長時間ログインしていたユーザや通常ではログインしていない時間にログインしているといった情報（真夜中のログインなど）もわかる。

5.3 pacct ログの視覚化例

図１６に、pacct ログ（誰が、いつ、どのようなコマンドを使用したか）をテキストで表示したものを示す。図１７に pacct ログを３次元らせん表示を用いて視覚化したものを示す。

コマンド名	誰が	コマンド実行時間	いつ実行したか
ps	hakobera	0.02 secs	Wed Apr 19 01:26:54 JST 2000
w	hakobera	0.03 secs	Wed Apr 19 01:26:56 JST 2000
pt_chmod	hakobera	0.01 secs	Wed Apr 19 01:28:04 JST 2000
telnet	seri	0.02 secs	Wed Apr 19 01:27:26 JST 2000
ndtpd	nazuna	0.01 secs	Wed Apr 19 01:27:26 JST 2000
sync	gogyou	0.06 secs	Wed Apr 19 01:28:23 JST 2000
rlogin	nazuna	0.03 secs	Wed Apr 19 01:33:35 JST 2000

図 16 pacct ログのテキスト表示

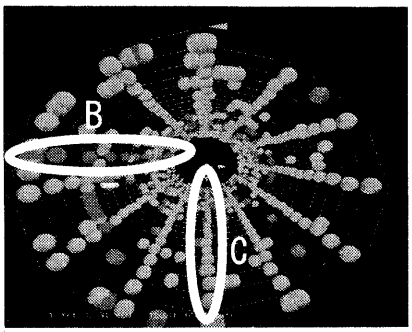

図 17 pacct ログの３次元らせん表示

図１７から、定期的に実行されているコマンドと実行しているユーザが一目でわかるため、不正に定期的にシステムの情報を送っていると考えられうるコマンドなどの発見が容易になる。図１７の B の部分は root によって定期的に実行されているコマンド、C の部分は一般ユーザによって定期的に実行されているコマンドである。

5.4 sulog ログの視覚化例

図１８に、sulog ログ（誰が、いつ、誰にスイッチしたか）をテキストで表示したものを示す。図１９に、sulog ログを３次元らせん表示を用いて視覚化したものを示す。

SU いつ	成功か失敗か	端末名	誰から-誰に
SU 04/07 12:14	+	ttyp0	nazuna-root
SU 04/07 12:53	-	ttyp0	nazuna-root
SU 04/10 16:34	+	pts/6	gogyou-hakobera
SU 04/10 16:36	+	pts/6	gogyou-hakobera
SU 04/10 16:48	+	pts/9	hakobera-gogyou

図 18 sulog ログのテキスト表示

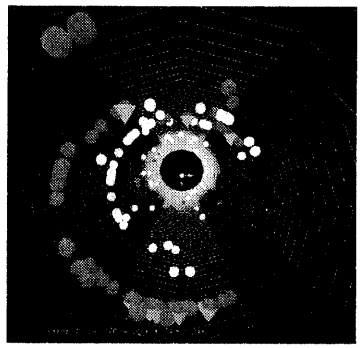

図 19 sulog ログの３次元らせん表示

表 1. sulog を表すアイコンの色

赤：危険 user→root 成功
黄：警告 user→user 成功
緑：注意 user→root 失敗
青：通常 user→user 失敗

上表には、図１９で使用されているアイコンの色の対応を示す。図１９では、root へのスイッチが成功したログが赤で表示されるため、システム管理者が通常ログインしていない時間帯のアイコンをチェックすることでシステム管理者以外のものが root になっていないかがわかる。その他、黄色で表示されるものは、一般ユーザが他の一般ユーザにスイッチしたもの、緑や青は、スイッチの失敗を表す。

6. 複数ログの比較検討例

図２０に、複数のログを統合して表示したものを示す。これは、図４において、ログ１が sulog、ログ２が pacct、ログ３が wtmpx に相当する。

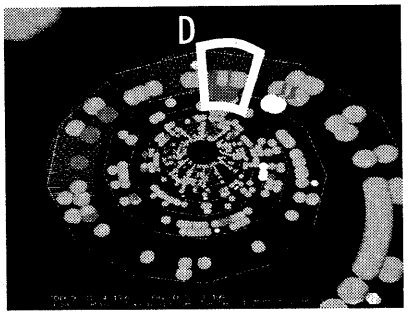

図 20 wtmpx、pacct、sulog を統合化した視覚化

図２０のＤの部分には、赤すなわち、root ニスイッチしたアイコンや root が実行したことを示すアイコンが重なっている。そこで、それら複数のアイコンにマウスカーソルを重ねることで、ログエントリの内容が画面下部に表示されるので、表２の内容が容易に把握できる。

表 2. D 部分のアイコンの内容

slogin	user1	bologna.vogue.is.uec Tue Dec 14 22:55:43 - 15 03:13:34
config.s	user1	Tue Dec 14 23:30:03 1999
config.j	user1	Tue Dec 14 23:32:57 1999
gmake	root	Tue Dec 14 23:38:52 1999
SU		Tue Dec 14 23:48:00 1999 + ttyp0 user1 - root

このように、３次元らせんを統合化した視覚化により、ユーザ user が何らかのプログラムをコンパイルし、root 権限でインストールしたことがわかる。システム管理者はこのプログラムが何を行うのか、また、その動作によりにシステムがどのような影響を受けるのかを注意深く監視する必要がある。

7. 考察

7.1 関連研究

膨大なデータをコンパクトに描くものに Mackinlay らの Perspective Wall[1] がある。これは、線形データを３次元の壁上に表示するシステムであり、局所的詳細と大局的概略を統合した表示を可能とした。この３次元の壁は途中２カ所で折れ曲がり、中央部分は計算機画面と平行だが、左右部分はそれぞれ端が画面奥行き方向に遠ざかっている。この壁に時系列データを表示すると、中央の壁に表示されるデータはその詳細を見ることができ、一方、左右の壁に表示されるデータはその存在だけを把握することができる。

３次元らせん表示と位置的な要因を結びつけることで時間軸データと位置データの統合をするものに、Hewagamage らの時簡空簡パターンの視覚化システム [3] がある。これを用いることで例えば、モバイル端末を使用して仕事をしているユーザの情報へのアクセス、その内容（電子メール、ファックスなど）及びアクセス期間と地図上での位置を結び付けることを可能としている。

ログを視覚化し、侵入を検知するものに、高田らのログ情報視覚化システム [6] がある。このシステムでは、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ている。アクセス元ホストおよびユーザ情報は、アクセス元ホストを分類した層構造をしており、平面上に配置される。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。

7.2 本手法の考察

本研究における３次元らせん表示を用いた UNIX ログの視覚化手法についての有効性と問題点について述べる。３次元らせん表示を用いることで、従来は不可能であった膨大な情報量を持つログをコンパクトに表示することが可能となり、その結果、１日間隔、あるいは１週間間隔で記録されるような周期的に現れるログエントリの発見が容易となった。さらに、アイコンでログエントリを表示し、その色を変えることで、重要な内容を持つログエントリとそれほど重要でないログエントリが容易に認識できるようになった結果、調査すべきログエントリへの指標付けが可能となった。しかしながら、らせんの半径が小さすぎるとアイコンが重なってしまい、ログエントリ内容の認識が困難となる。

また、現段階では、アイコンから得られる情報量が少ない。さらに、従来のようにテキスト情報を一覧できないという問題もある。これらを解決するために、アイコンの種類を増やすことで、Visual Vocabulary を充実させ、アイコンから得られる情報量を増やし、テキスト情報を一覧する時と同様に多くのログエントリ内容が把握できるようにし、怪しいと思われるログ情報の発見が容易になるように

する必要がある。

複数のログを３次元らせんに統合し、同時に表示することで、個々の異なったログエントリ内容を総合し、そこから発見される内容の把握を支援する。しかしながら、現在あやしいと思われるログエントリは、アイコンの色が赤で集中しているところや、定期的なもの、通常では現れない時間帯に描かれたアイコンを調査することで複数のログの調査を行っている。今後は、これらを自動的に行うようにすることで、より調査作業の軽減を図る必要がある。

実際にログを読み込み、表示するためにログは表示を行う計算機の補助記憶装置に保存しておく。そのため、ログの転送が必要となるが SecureShell などを用いて転送を行うことで、不必要な改ざんを防ぐことが出来る。侵入された計算機のログを表示し調査をおこなうコマンドは、改ざんされていることが多い。このため、ログをどこか他のところで調査する必要がある。このことによる欠点は、ログのリアルタイムの表示が出来ない点である。

8. まとめ

本研究では、一次元時系列データである UNIX ログを３次元らせん表示を用いて視覚化する手法を提案した。この結果、膨大な情報量を持つログをウインドウにテキストベースで表示するよりも多く表示することができる。また、らせんの特徴を生かし、記録された時刻を認識することが簡単になり、さらに、複数のログを一つのらせんに同時に描くことによって、ログエントリ同士の関連付けからユーザの行動を追跡することが容易となった。

今後の課題として、あやしいと考えられるログエントリの自動検出を行えるようにする必要がある。

参考文献

[1]John V.Carlis and Joseph A Konstan,Interactive Visualizaton of Serial Periodic Data,Proceedings of the ACM Symposium on User Interface Software and Technology pp29-38, Nov.1-4

[2]Stephen G. Eick and Paul J. Lucas,Displaying Trace Files,Software Practice and Experience, 26(4),pp399-409, Apr.(1996).
(1998).

[3]K.Priyantha Hewagamage,Masahito Hirakawa and Tadao Ichikawa,Interactive Visualization of Spatiotemporal Patterns Using Spirals on a Geographical Map, 1999 IEEE Symposium on Visual Languages IEEE Computer Society,pp296-303(1999).

[4]Jock D. Mackinlay, George G. Robertson, and Stuart K. Card, THE PERSPECTIVE WALL: Detail and context smoothly integrated, Human Factors in Computing Systems CHI'91 Conference Proceedings, pp173-179(1991).

[5] 小池英樹 , 赤井一章 ,SpiralBrowser: 時間軸検索を支援するファイル検索インターフェースの開発 , 日本ソフトウェア科学会第１４回大会論文集 , pp121-124(1997).

[6] 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論文集 情報処理学会 , pp153-158(1998).