(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年7 月27 日 (27.07.2006)

PCT

(10) 国際公開番号
WO 2006/077666 A1

(51) 国際特許分類[7]: G06F 15/00, 3/00, 11/32, 13/00, 17/40, H04L 12/20

(21) 国際出願番号: PCT/JP2005/011997

(22) 国際出願日: 2005 年6 月29 日 (29.06.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2004-381884
2004 年12 月28 日 (28.12.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 国立大学法人京都大学 (Kyoto University) [JP/JP]; 〒6068501 京都府京都市左京区吉田本町３６番地１ Kyoto (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 高倉 弘喜 (TAKAKURA, Hiroki). 伊藤 貴之 (ITOH, Takayuki). 沢田 篤史 (SAWADA, Atsushi). 小山田 耕二 (KOYAMADA, Koji).

(74) 代理人: 特許業務法人原謙三国際特許事務所 (HARAKENZO WORLD PATENT & TRADEMARK); 〒5300041 大阪府大阪市北区天神橋２丁目北２番６号 大和南森町ビル Osaka (JP).

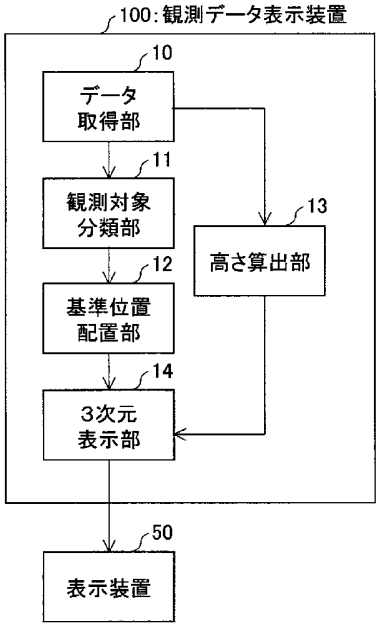
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,

[続葉有]

(54) Title: OBSERVATION DATA DISPLAY DEVICE, OBSERVATION DATA DISPLAY METHOD, OBSERVATION DATA DISPLAY PROGRAM, AND COMPUTER-READABLE RECORDING MEDIUM CONTAINING THE PROGRAM

(54) 発明の名称: 観測データ表示装置、観測データ表示方法、観測データ表示プログラムおよびそれを記録したコンピュータ読み取り可能な記録媒体



100... OBSERVATION DATA DISPLAY DEVICE
10... DATA ACQUISITION UNIT
11... OBSERVATION OBJECT CLASSIFICATION UNIT
12... REFERENCE POSITION ARRANGEMENT UNIT
14... THREE-DIMENSIONAL DISPLAY UNIT
13... HEIGHT CALCULATION UNIT
50... DISPLAY DEVICE

(57) Abstract: Observation values obtained from a plenty of observation objects are 3-dimensionally displayed. An observation data display device displays observation values obtained by observing an observation object. The observation data display device includes: a data acquisition unit for acquiring a pair of observation object identifier for identifying an observation object and an observation value obtained by observing the observation object; a reference position arrangement unit for arranging a reference position for displaying the observation value of the observation object in the two-dimensional plane according to the observation object identifier; a height calculation unit for calculating a height based on the observation value for each of the observation values; and a three-dimensional display unit causing the display device to display the image expressed by the height calculated by the height calculation unit in the reference position where the observation value is arranged by the reference position arrangement unit. This enables three-dimensional display of observation values obtained by a plenty of monitoring objects.

(57) 要約: 多数の監視対象から得られた観測値を３次元表示する。本発明の観測データ表示装置は、観測対象を観測して得られる観測値を表示する観測データ表示装置であって、

観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる観測値との組を取得するデータ取得部と、当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置部と、上記観測値に応じた高さを観測値ごとに算出する高さ算出部と上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる３次元表示部と、を備えている。これにより、多数の監視対象から得た観測値を３次元表示することができる。

WO 2006/077666 A1

SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

規則4.17に規定する申立て:

— 不利にならない開示又は新規性喪失の例外に関する申立て (規則4.17(v))

添付公開書類:

— 国際調査報告書

— 不利にならない開示又は新規性喪失の例外に関する申立て

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

観測データ表示装置、観測データ表示方法、観測データ表示プログラムおよびそれを記録したコンピュータ読み取り可能な記録媒体

技術分野

[0001] 本発明は、観測したデータを表示する観測データ表示装置、観測データ表示方法、観測データ表示プログラムおよびそれを記録したコンピュータ読み取り可能な記録媒体に関するものである。

背景技術

[0002] インターネットの不正アクセスやウィルス等による被害の拡大に伴い、近年ではIDS(Intrusion Detection System)の研究が活発であり、その商用化も進んでいる。これらIDS製品の多くは、監視対象のネットワークに一定の安全対策が施されていることを前提にして、不正現象(インシデント)を漏れなく検出している。そして、情報視覚化によってインシデントの統計的傾向を表現する手法もいくつか発表されている。

[0003] 従来のインシデントの表現手法の一つとして、文献1には、「見えログ」という手法が提案されている。この手法では、画面を水平方向に分割し、左側にインシデント全体の時間別件数を一列に棒グラフ表示し、その右側にユーザーが指定したある時間におけるインシデントの内訳を表示する。この手法はインシデントの時間的な全体的傾向と局所的傾向を同時に表現できる点に特徴がある。

[0004] またIDSとはデータ構造が異なるが、文献2では1台のウェブサーバーのアクセスログファイルを対象として、横軸に属性の種類、縦軸に属性値、を配置したParallel Coordinateという座標系に個々のアクセスを配置する手法が提案されている。この手法は不正アクセスの属性値の相関性を表現することで、不正アクセスの詳細な性格の理解を支援している。

[0005] また、上記の文献以外にも様々な研究がなされている(文献3～9)。さらには、各メーカが不正アクセス検知システムを発売しており、これらのシステムにもインシデントの統計的傾向を表現するインタフェースが搭載されている。

[0006] しかしながら、上記従来の技術は、多数の監視対象から得た観測値を3次元表示

することができないという問題点を有している。従来の技術が抱える問題点について、以下具体的に説明する。

[0007] 大学等の大規模組織における不正アクセス検知システムは、数千から数万の監視対象(コンピュータ)について毎秒千件以上の警報を発するという環境で運用されており、このような環境下で使用するには、膨大な監視対象を処理できることが必要とされる。また、警報の99%は誤報であり、誤報を除去しない限り真の不正アクセスは検出できない。従って、インシデント情報を3次元的に表示して、警報の内容を直感的に認識できることが必要とされる。

[0008] しかしながら、例えば、文献1, 2に記載の技術は、アクセスや計算機などのデータ要素を一次元的に画面に並べるため、数千、数万といった大規模なデータに対しては非常に概略的な傾向しか表現できないことが多い。また「この組織が集中的に狙われている」というような空間的な相関性を理解することが難しい。

[0009] また、米国SourceFire社が開発したシステムRNAでは、コンピュータの接続関係を三次元空間に表示するが、実際に大規模組織で評価した結果、コンピュータ数が3,000台を超えた辺りから、データ数の多さに表示が追従できなくなり、視認性も著しく低下する現象に陥った。

[0010] 以上のように、従来技術では、時間軸に沿って警報の変化数をグラフ化し全体の攻撃の推移を表示したもの、あるいは、特定の監視対象や警報について関連性が推測される警報を選択表示するものが提案されているが、監視対象全てを同時に表示しつつ、かつ、個々の状況を把握できるものはない。さらに警報を三次元グラフで表示するシステムも提案されているが、大多数を占める誤報によって重要な情報が隠されてしまっている。これらの手法では、一般に百台未満の監視対象で、1時間あたりの警報数も百件程度の環境を想定しているのがその理由である。

(文献1) 高田, 小池, 見えログ:情報可視化とテキストマイニングを用いたログ情報ブラウザ, 情報処理学会論文誌, 41, 12, pp. 3265-3275, 2002.

(文献2) Axelsson S., Visualization for Intrusion Detection Hooking the Worm, European Symposium on Research in Computer Security 2003, pp. 309-325, 2003.

(文献3) Lamping J., Rao R., The Hyperbolic Browser: A Focus+context Techniqu

e for Visualizing Large Hierarchies, J. Visual Languages and Computing, 7, 1, 33-55, 1996.

（文献4） Carriere J., et al., Research Report: Interacting with Huge Hierarchies Beyond Cone Trees, IEEE Information Visualization '95, pp. 74-81, 1995.

（文献5） Koike H., Fractal Views: A Fractal-Based Method for Controlling Information Display, ACM Trans. on Information Systems, 13, 3, pp. 305-323, 1995.

（文献6） Johnson B., et al., Tree-Maps: A Space Filling Approach to the Visualization of Hierarchical Information Space, IEEE Visualization '91, pp. 275-282, 1991.

（文献7） The Information Cube: Using Transparency in 3D Information Visualization, Third Annual Workshop on Information Technologies & Systems, pp. 125-132, 1993.

（文献8） Sprenger T. C., et al, H-BLOB: A Hierarchical Visual Clustering Method Using Implicit Surfaces, IEEE Visualization 2000, pp. 61-68, 2000.

（文献9） 山口, 伊藤, 池端, 梶永,階層型データ視覚化手法「データ宝石箱」とウェブサイトの視覚化,画像電子学会論文誌 , Vol. 32, No. 4, pp. 407-417, 2003.

発明の開示

[0011] 本発明は上記課題に鑑みてなされたものであり、その目的は、多数の監視対象から得た観測値を3次元表示することのできる観測データ表示装置、観測データ表示方法を実現することにある。

[0012] 本発明に係る観測データ表示装置は、観測対象を観測した観測値を表示する観測データ表示装置であって、上記課題を解決するために、観測対象を特定するための観測対象識別情報と該観測対象を観測した観測値との組を取得するデータ取得部と、上記観測対象識別情報に基づいて当該観測対象の観測値を表示するための基準位置を二次元平面内に配置する基準位置配置部と、観測対象の観測値を、上記基準位置配置部によって配置された基準位置からの高さとしてプロットする観測値プロット部と、上記観測値プロット部によって生成されたデータに基づいて観測値を表示装置に3次元表示する3次元表示部と、を備えることを特徴とする。

[0013] 上記構成によれば、基準位置配置部は、観測値を二次元平面内に配置するので、

多数の監視対象を観測できる。また、観測値プロット部が観測値を基準位置からの高さとしてプロットし、これを3次元表示部が3次元表示するので、多数の監視対象から得た観測値を3次元表示することが可能となる。

[0014] また、本発明に係る観測データ表示方法は、観測対象を観測した観測値を表示する観測データ表示装置による観測データ表示方法であって、上記課題を解決するために、観測対象を特定するための観測対象識別情報と該観測対象を観測した観測値との組を取得するデータ取得ステップと、上記観測対象識別情報に基づいて当該観測対象の観測値を表示するための基準位置を二次元平面内に配置する基準位置配置ステップと、観測対象の観測値を、上記基準位置配置ステップによって配置された基準位置からの高さとしてプロットする観測値プロットステップと、上記観測値プロットステップによって生成されたデータに基づいて観測値を表示装置に3次元表示する3次元表示ステップと、を含むことを特徴とする。

[0015] 上記構成によれば、基準位置配置ステップでは、観測値が二次元平面内に配置されるので、多数の監視対象を観測できる。また、3次元表示ステップでは、観測値プロットステップが観測値を基準位置からの高さとしてプロットしたデータに基づいて、3次元表示するので、多数の監視対象から得た観測値を3次元表示することができる。

[0016] また、本発明に係る別の観測データ表示装置は、観測対象を観測して得られる観測値を表示する観測データ表示装置であって、上記課題を解決するために、観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる観測値との組を取得するデータ取得部と、当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置部と、上記観測値に応じた高さを観測値ごとに算出する高さ算出部と上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる3次元表示部と、を備えていることを特徴とする。

[0017] また、本発明に係る別の観測データ表示方法は、観測対象を観測して得られる観測値を表示する観測データ表示方法であって、観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる観測値との組を取得するデータ取得

ステップと、当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置ステップと、上記観測値に応じた高さを観測値ごとに算出する高さ算出ステップと上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる3次元表示ステップと、を含んでいることを特徴とする。

[0018] 上記構成によれば、基準位置配置部が、観測値を二次元平面内に配置するので、多数の監視対象を観測して得られる観測値を表示装置などに表示することができる。また、高さ算出部が観測値を基準位置からの高さとして算出し、その高さによって観測値を3次元表示するので、多数の監視対象から得た観測値を効率的に表示することが可能となる。

図面の簡単な説明

[0019] [図1]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術について説明する図である。

[図2]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術について説明する図である。

[図3]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術について説明する図である。

[図4]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術について説明する図である。

[図5]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術について説明する図である。

[図6]本発明の一実施形態を示すものであり、観測データ表示装置に用いられる基本技術である基準位置配置部の処理工程を示す図である。

[図7]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の概要を示す図である。

[図8]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図9]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図10]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図11]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図12]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の概要を示す図である。

[図13]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図14]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図15]本発明の一実施形態を示すものであり、観測データ表示装置による表示結果の一例を示す図である。

[図16]本発明の一実施形態を示すものであり、IPアドレスを参照して8台の計算機を階層型データに格納した例を示す図である。

[図17]本発明の一実施形態を示すものであり、実施形態1に係る観測データ表示装置100の機能構成を示すブロック図である。

[図18]本発明の一実施形態を示すものであり、実施形態2に係る観測データ表示装置200の機能構成を示すブロック図である。

[図19]本発明の一実施形態を示すものであり、実施形態3に係る観測データ表示装置300の機能構成を示すブロック図である。

発明を実施するための最良の形態

[0020] 〔基本技術〕

まず、本発明の各実施形態に係る観測データ表示装置に共通する基本技術となる基準位置配置部の一例について、図1～図6を参照して説明する。なお、この基本技術については、伊藤、小山田による「平安京ビュー～階層型データを碁盤状に配置する視覚化手法」(可視化情報学会第9回ビジュアリゼーションカンファレンス抄録、2

003年発行）にも記載されている。

[0021] 階層型データの視覚化手法は、情報視覚化の研究分野の中でも、特に活発に研究されている分野のひとつである。代表的なものとして、以下のような手法がある。

[0022] （1）木構造を表現した手法。Hyperbolic Tree（文献3），Cone Tree（文献4），Fractal Views（文献5）など。

[0023] （2）画面空間の再帰分割による手法。Treemap（文献6）など。

[0024] （3）3次元空間で入れ子状に階層構造を構築し、半透明表示する手法。Information Cube（文献7），H-BLOB（文献8）など。

[0025] （4）2次元空間で入れ子状に階層構造を構築する手法。「データ宝石箱」（文献9）など。

[0026] 後述の各実施形態では、「できるだけ小さな画面空間に多くの情報を、碁盤状に整理された形式で表現する」という方針による階層型データの画面配置手法を用いた観測データ表示装置を提供する。本発明の各実施形態に係る観測データ表示装置に用いられる基本技術は、発明者自身による従来の視覚化手法「データ宝石箱」と類似した条件を前提にして構成されている。しかし、アルゴリズムが大きく異なるため、視覚化結果も大きく異なる。

[0027] 本発明の各実施形態に係る観測データ表示装置に用いられる基本技術は、長方形の入れ子構造によって階層型データを表現しており、具体的には、階層型データを構成する葉ノードをアイコンで表現し、枝ノードを入れ子状の長方形の枠で表現している。

[0028] 図1に、観測データ表示装置による階層型データの画面配置アルゴリズムを示す。なお、基本技術に関する以下の説明において、特に記載のない場合は各処理を基準位置配置部が行っているものとする。

[0029] 本発明の各実施形態に係る観測データ表示装置では、まず最下位階層に属する葉ノードに対応するアイコン（図1の場合は正方形）を隙間無く配置する。続いて、この上位階層に属する枝ノードを表現するために、アイコンを包括する長方形を生成する。さらに、上位階層の枝ノードを表現する長方形群を隙間無く配置し、同様にこれを包括する長方形を生成する。以上の処理を、最下位階層から最上位階層に向

けて反復することで、データ全体の配置を決定する。以上の処理手順は、上述した「データ宝石箱」と同等の手順である。

[0030] 次に、各階層を構成する長方形群を画面配置するためのアルゴリズムの概要について説明する。本発明の各実施形態に係る観測データ表示装置では、まず階層型データ中の葉ノード群を正方形のアイコンで表現し、これを格子状に配列する。続いてこれらの葉ノードの親にあたる枝ノードを、葉ノード群を囲む長方形で表現する。続いて、長方形で表現された枝ノード群を画面上に効率よく配置することで、限られた画面空間上に大量の情報を表現する。

[0031] 本発明の各実施形態に係る観測データ表示装置では、枝ノードを表現する長方形群を、画面空間の横軸および縦軸に平行に、1個ずつ順に配置するものとする。このとき、以下の条件1，2を満たすように長方形群を画面空間に配置する。

[0032] [条件1] すでに配置されている長方形と干渉しない位置に長方形を配置する。

[0033] [条件2] [条件1]を満たす位置のうち、配置面積の拡大量が最小である位置に長方形を配置する。

[0034] アルゴリズムを要約した擬似コードを、図6に示す。

[0035] 次に、長方形群の画面配置アルゴリズムの詳細について説明する。本発明の各実施形態に係る観測データ表示装置では、長方形群の画面配置状況を管理するために、すでに配置された長方形の辺の延長線を用いて、画面領域を格子状に分割する(図2参照)。このとき、この分割処理によって作成された個々の格子領域について、すでに長方形が配置されている領域か、まだ配置されていない領域か、を判定し記録する。図2(右)の場合、灰色に塗られた格子領域は長方形が配置された領域であり、塗られていない格子領域は長方形が配置されていない領域である。

[0036] 以上の分割手法により、画面空間がx軸方向にp個、y軸方向にq個の領域に分割されたとする。このとき、画面空間を分割する線分のx座標値を小さい順にソートしたものをx_0～x_p、y座標値を小さい順にソートしたものをy_0～y_qと表す。このとき観測データ表示装置は、各々の長方形を配置する際に、p×q個に分割された格子領域を順に探索し、その内部に長方形を配置できるかどうか確認する。

[0037] 本発明の各実施形態に係る観測データ表示装置では、長方形の位置を決定する

ために、格子領域を探索しながら複数の候補位置を設定し、その中から最適な位置を選択する。

格子領域の探索順は以下の通りである。まず画面空間の中心点を含む格子領域を特定する。この格子領域が左からs番目、上からt番目にあるとき、本章ではこれを[s,t]と記述する。提案手法では、まず格子領域[s,t]を探索し、続いてそれを中心にして渦巻状に格子領域の探索順を定義する(図3(左)参照)。例えば[s−1,t−1]〜[s−1,t+1]を探索し、続いて[s−1,t+1]〜[s+1,t+1]を探索し…という順に格子を探索する。

[0038] このような手順を用いる理由は、長方形を画面空間の外側に配置するよりも、内側に配置するほうが、配置面積の拡大量が小さくなる可能性が高いからである。つまり、画面空間の内側の格子領域から順に探索することで、[条件1][条件2]の両方を満たす位置を早期発見し、処理の高速化に寄与できるからである。

[0039] 続いて、観測データ表示装置は、探索された各々の格子領域について、長方形の配置を試みる。このとき、すでに配置されている長方形との干渉判定によって、[条件1]を満たすかどうか確認する。また、長方形の配置による配置面積の拡大量の算出によって、[条件2]を満たすかどうか確認する。

[0040] 観測データ表示装置は、1個の格子領域について、以下に示す4点にて長方形の配置を試みる。まず長方形の縦横の長さを(w, h)とする。また、[s, t]番目の格子領域の4頂点のx座標値はx_s, x_{s+1}であり、y座標値はy_t, y_{t+1}である。また本明細書では、4頂点のx座標値がx_a, x_bでy座標値がy_c, y_dである長方形の位置を、[x_a, x_b, y_c, y_d]と記述する。このとき観測データ表示装置の基準位置配置部は、長方形の1頂点と格子領域の1頂点が重なるように、以下の4つの候補位置に長方形の配置を試みる(図3(右)参照)。

[0041] 候補1:[x_s, (x_s+w), y_t, (y_t+h)]

候補2:[(x_{s+1}−w), x_{s+1}, y_t, (y_t+h)]

候補3:[x_s, (x_s+w), (y_{t+1}−h), y_{t+1}]

候補4:[(x_{s+1}−w), x_{s+1}, (y_{t+1}−h), y_{t+1}]

以上のように候補位置を設定することで、長方形の1辺が隣接長方形の辺と同一線上に位置する可能性が高くなる。これが長方形の配置結果を「碁盤状に」見せる要因

である。

[0042] 以上のようにして導き出した候補位置の1つを、[x_a, x_b, y_c, y_d]と表現する。このとき観測データ表示装置では、x_a, x_b, y_c, y_dの4値と格子辺の座標値について、以下のような関係

$$x_i \leqq x_a \leqq x_{i+1},\ X_j \leqq x_b \leqq x_{j+1}$$

$$y_k \leqq y_c \leqq y_{k+1},\ y_l \leqq y_d \leqq y_{l+1}$$

が成立する整数値i, j, k, lを特定する。続いて、格子領域 [i,k]～[j,l] の合計 (k−i+1)×(l−j+1) 個に対して、すでに配置されている長方形との干渉を判定する。まったく干渉が見られなければ、その位置は[条件1]を満たしていると判定される(図4(左)参照)。

[0043] この位置に配置した長方形が、画面空間をはみ出さない場合には、その位置は[条件2]を満たしていると判定し、提案手法は格子領域の探索を中断し、その位置に長方形を配置することに決定する。画面空間をはみ出す場合には、画面空間の拡大量を算出する。このとき、

(a)[条件1]のみを満たす位置が他にない場合で、かつ、

(b)他の[条件1]のみを満たす位置と比較して画面空間の拡大量が最小である場合には、この位置を「仮の位置」とし、画面空間の拡大量とともに記録する。格子領域の探索処理を終了するまで「画面空間をはみ出さない位置」が全く見つからなかった場合には、この「仮の位置」に長方形を配置する。

[0044] 以上の処理によって長方形の位置を決定したら、長方形の辺を延長した線分で格子領域を分割する(図4(右)参照)。

[0045] 図5に、観測データ表示装置による階層型データの表示例を示す。この表示に用いたデータは、葉ノード1067個、枝ノード67個を含む。画面配置計算に要した計算時間は約0.1秒であった。

[0046] このように、本発明の各実施形態に係る観測データ表示装置には、階層型データを構成する情報を碁盤状に画面に配置できる基本技術(基準位置配置部)が用いられている。

[0047] 〔実施形態1〕

次に、本発明の一実施形態に係る観測データ表示装置について、図1，5，7を参照して説明する。本実施形態に係る観測データ表示装置の概要は以下の通りである。

[0048] インターネットのインシデントやウィルス等による被害の拡大に伴い、近年ではIDS(Intrusion Detection System)の研究が活発であり、その商用化も進んでいる。これらIDS製品の多くは、監視対象のネットワークに一定の安全対策が施されていることを前提にして、不正現象(インシデント)を漏れなく検出している。しかしながら、特に大規模で開放性の高いネットワークにおいてIDS製品を実際に運用してみると、以下のような問題が生じることがわかった(「沢田、高倉、岡部、開放型大規模ネットワークのためのIDSログ監視支援システム、情報処理学会論文誌、Vol. 44, No. 8, pp. 1861-1871, 2003.」)。

(1)インシデント1件ごとに1件の警報を送信するメール通報システムでは、警報メールの量が膨大になるだけでなく、その相関性や統計的傾向を理解することが困難である。

(2)最近のインシデントは複雑化する傾向にあり、複数のシグニチャ(インシデントの種類やパターン)によって一連のインシデントを構成するケースが多く、その全貌を把握するには機械的処理だけでは不十分である。

(3)インシデントの大量さゆえ、インシデントを事後分析するためのデータベースの運用も容易ではない。

(4)GUIによる従来の探索的な閲覧システムには、重要なインシデントを検索することが難しい、多忙な管理者では手に負えない、多数の管理者間の知識共有に向かない、遠隔からの業務に向かない、などの問題がある。

[0049] これらの問題点を解決し、安全性の高いネットワーク運用を実現するための手段はいくつか考えられる。例えばIDSが検出するインシデントを蓄積する統合管理型のデータベースにより、インシデントの事後分析を支援する研究がある(「大谷、桑田、小迫、井上、統合データベースを用いたインシデント検出情報の分析および意思決定支援システム、第13回データ高額ワークショップ、A1-6, 2002.」)。また、テキストマイニングや周期性解析などの分析的手法を用いて、精度の高いインシデント分析を目

指す研究がある(「宮本、泉、田村、福永、ネットワーク・サーバ運用監視支援システム、システム制御情報学会論文誌、Vol. 15, No. 6, pp. 279-287, 2002.」)。

[0050] 情報視覚化によってIDSの統計的傾向の理解を支援する手法もいくつか提案されている。文献1に記載されている、高田らの「見えログ」という手法では、画面を水平方向に分割し、左側にIDS全体の時間別件数を一列に棒グラフ表示し、その右側にユーザーが指定したある時間におけるIDSの内訳を表示する。またIDSとはデータ構造が異なるが、文献2では、ウェブサーバーのアクセスログファイルを対象として、横軸に属性の種類、縦軸に属性値、を配置した Parallel Coordinate という座標系に個々のアクセスを配置する手法をAxelssonが提案している。しかしこれらの手法は、アクセスや計算機などのデータ要素を一次元的に画面に並べるため、数千、数万といった大規模なデータに対しては非常に概略的な傾向しか表現できないことが多い。また「この組織が集中的に狙われている」というような空間的な相関性を理解することが難しい。このことから、データ要素を一次元的にではなく二次元的に画面配置し、大規模な情報を俯瞰するような視覚化手法を適用することが望ましいと考えられる。

[0051] 本実施形態では、大規模ネットワークを構成する数千、数万の計算機のIDSによる加害、被害の全貌を一画面にすべて表現することを目的とした観測データ表示装置について説明する。本実施形態の観測データ表示装置は、大規模階層型データを対象とした、上述の基本技術(基準位置配置部)を用いて、数千、数万もの計算機の分布図を表示し、その統計的傾向を一画面に全貌表示する。本実施形態の観測データ表示装置によれば、大量なインシデントの傾向を短時間で把握できると考えられる。

[0052] 上記の〔基本技術〕の項でも述べたとおり、本実施形態に係る観測データ表示装置は大規模階層型データを視覚化できる装置である。図5に、本実施形態に係る観測データ表示装置による階層型データを表示するための基準位置の配置例を示す。本実施形態に係る観測データ表示装置では、階層型データを構成する葉ノードをアイコンで、枝ノードを長方形の枠で表現し、長方形枠の入れ子構造によって階層構造を表現する。

[0053] 本実施形態に係る観測データ表示装置では、まず葉ノードを表現するアイコンを、

画面空間上に隙間無く配置する。続いて、この上位階層に属する枝ノードを表現するために、アイコンを包括する長方形を生成する。さらに、上位階層の枝ノードを表現する長方形群を隙間無く配置し、同様にこれを包括する長方形を生成する。以上の処理を、最下位階層から最上位階層に向けて反復することで、データ全体の基準位置の配置を決定する。図1に、本実施形態に係る観測データ表示装置による葉ノードおよび枝ノードの画面配置手順を示す。なお、このアルゴリズムは、上記の〔基本技術〕の項で述べたものと同一である。

[0054] このとき観測データ表示装置では、葉ノードおよび枝ノードを表現する長方形群を、以下の2条件を満たすように画面配置する。

[条件1] すでに配置されている長方形と干渉しない位置に長方形を配置する。

[条件2] [条件1]を満たす位置のうち、配置面積の拡大量が最小である位置に長方形を配置する。

[0055] この条件を満たすような画面配置を実現することによって、大規模な階層型データの全貌を、限られた画面空間にあますことなく表現することができる。

[0056] 本実施形態に係る観測データ表示装置は、数千、数万もの葉ノードを有する階層型データに対し、画面上で互いに重なり合うことなく、できるだけ小さい画面空間に余すことなく、またすべての葉ノードを対等な大きさで表現することができる。本実施形態の目的、たとえば

(a)数千・数万ものIPアドレスをもつ大規模ネットワーク環境を対象として、個々のIPアドレスに関するインシデントの統計的傾向の全貌を一画面に表現したい

(b)同一組織に属する計算機群(=IPアドレスの上位2, 3桁(ただし桁の単位はオクテット)が同一である計算機群)のインシデント傾向を、「インシデント群」として概略的に理解したい

というような目的において、本実施形態に係る観測データ表示装置は非常に適切な技術であるといえる。

[0057] 本実施形態に係る観測データ表示装置に入力するIDSデータとしては、一例として、Cisco社の Cisco Secure IDS 4320 (http://www.cisco.com/japanese/warp/public/3/jp/product/security/ids/index.html参照)が出力するIDSログデータファイルに

基づくものを使用することができる。当システムではシグネチャ(signature)と呼ばれる典型的なパターンに基づいてインシデントを検出するものである。検出された1回のインシデント検出に対してログファイルに出力するデータのうち、本実施形態では、一例として、以下のデータを参照するものとする。

・送信元IPアドレス

・受信先IPアドレス

・発生時刻

・不正の種類を表す正整数ID

・重要度を表すレベル(5段階)

本実施形態に係る観測データ表示装置では、ログファイルに記述された多数のインシデントに対して、送信元および受信先に記述されたIPアドレスを列挙し、観測対象分類部11がIPアドレスの各バイトの値を参照して階層構造を構築する。

[0058] 続いて、各々のIPアドレスに対して、送信元となったインシデント、受信先となったインシデントを集計する。換言すれば、不正アクセスを行った回数および不正アクセスを受けた回数をIPアドレスごとに集計する。このとき、発生時刻の範囲、インシデントの種類や重要度、などの条件を加え、条件を満たすインシデントだけを集計することもできる。

[0059] 続いて、ネットワークを構成する計算機のIPアドレスによって構成される階層型データを観測データ表示装置で表示する。このとき、観測値プロット部が、さらに各々のIPアドレスに相当する葉ノードに高さを与えることで、各々のIPアドレスの送信元および受信先となったインシデント数を表現する。また、図7に示すように、送信元となったインシデント数、受信先となったインシデント数、に別個の色を割り当てて表現することで、棒グラフを重ね合わせるように(積み重ねて)インシデント数を表現することが好ましい。そして、3次元表示部が、観測値プロット部によって生成されたデータに基づいて観測値を表示装置に3次元表示する。

[0060] このような観測データ表示装置を実現するための構成について以下に説明する。図17は、本実施形態に係る観測データ表示装置100の機能ブロックを示すブロック図である。観測データ表示装置100は、図17に示すように、データ取得部10、観測

対象分類部11、基準位置配置部12、高さ算出部13、3次元表示部14を備えている。

[0061] データ取得部10は、コンピュータネットワークにおいて計算機(観測対象)を特定するためのIPアドレス(観測対象識別情報)と、計算機が不正アクセスを行った件数および受けた件数(インシデント数、観測値)との組を取得するためのものである。データ取得部10は、例えば上述したように、インシデントに対して出力されたログファイルから、IPアドレスとインシデント数との組を抽出する。なお、データ取得部10は、さらに発生時刻、不正の種類を表す正整数ID、重要度を表すレベル(5段階)などを取得し、これらのパラメータに基づいてログファイルから抽出するインシデントを制限してもよい。

[0062] 観測対象分類部11は、IPアドレス(観測対象識別情報)に基づいて計算機(観測対象)を階層的なクラスターに分類するためのものである。IPアドレスは階層構造を有しており、例えばIPv4規格では4つのオクテットからなる。ここで、先頭(すなわち1番目)のオクテットは最上位階層における位置を示し、末尾に近づくにつれ下位の階層における位置を示す。観測対象分類部11は、個々の計算機を葉ノードとして扱う。そして、IPアドレスによって規定される計算機ネットワークのトポロジーが、クラスターのトポロジーに対応するように、葉ノードに相当する計算機をクラスタリングする。例えば、オクテットごとに階層を設定し、各階層においてはオクテットの種類数(すなわち256個)のクラスターを作成し、計算機の有するIPアドレスのオクテットがクラスターの有するIPアドレスのオクテットと一致するか否かに応じて分類してもよい。なお、クラスターに分類する方法はこれに限定されるものではなく、例えば上記の手法によって作成されたクラスターが各階層内で何らかの法則に基づいて統合されていてもよい。また、本実施形態において、同一クラスター内における各ノード同士の遠近関係は無視してもよい。

[0063] 基準位置配置部12は、計算機(葉ノード)のインシデント数(観測値)を高さによって表示するための基準位置を決定するためのものである。ここで、基準位置配置部12は、観測対象分類部11によって分類されたクラスターに基づいて、各計算機の基準位置を決定する。なお、基準位置の決定方法は上述した基本技術の通りであり、

各計算機を葉ノードとして扱い、計算機が所属する階層的なクラスターを枝ノードとして扱う。ここで、基準位置は、XY平面座標系におけるX座標およびY座標によって表現される。

[0064] 高さ算出部13は、データ取得部10によって計算機ごとに取得したインシデント数を図7に示す棒グラフの高さとして表現するために、各IPアドレスを有する計算機ごとに、インシデント数に基づいた高さを算出する。本実施形態では、インシデント数として不正アクセスを行った件数および不正アクセスを受けた件数の双方を個別に表示するため、高さ算出部13が、不正アクセスを行った件数に基づいて第1の高さを算出するとともに不正アクセスを受けた件数に基づいて第2の高さを算出する。ここで、算出された第1の高さ、第2の高さは、それぞれ、不正アクセスを行った件数および受けた件数、不正アクセスを受けた件数に応じた高さとなっている。

[0065] 3次元表示部14は、各計算機のインシデント数が、基準位置配置部12によって配置された基準位置で、かつ、高さ算出部13によって算出された第1および第2の高さで3次元的に表現された画像データを作成する。例えば、3次元表示部14は、モデリング座標系としてXYZ空間座標系を設定し、基準位置配置部12によって決定されたX座標およびY座標で、かつZ座標が0の位置を計算機の基準位置とする。そして、その基準位置から＋Z方向に、高さ算出部13によって算出された第1および第2の高さだけ伸長した立体的な棒グラフをそれぞれ作成する。ここで、第1の高さを有する棒グラフと第2の高さを有する棒グラフとは、積み重ねて作成される。すなわち、2つの棒グラフがZ軸方向に連結された状態となっている。

[0066] 3次元表示部14は、この棒グラフの作成を全ての計算機について行っていく。そして、全ての計算機について棒グラフを作成すると、作成された3次元モデルを平面状の表示領域に表示させるために、作成された3次元モデルについて、モデリング座標系からスクリーン座標系へとジオメトリ変換を行う。これにより、図7に示すような不正アクセスの件数が立体的な高さとして表現された画像データを作成することができる。

[0067] 本実施形態では、大規模ネットワークへのインシデントの統計的傾向を一画面に表示する観測データ表示装置について説明した。本装置には以下のような利点があると考えられる。

・数千、数万といった大量な計算機を有する大規模ネットワークに対するインシデントの統計的傾向を、一画面に全貌表示できる。

・計算機空間上の位置と相関性のあるインシデント傾向の理解に向いている。

[0068] また、観測データ表示装置には、以下の機能をさらに付加してもよい。

・データマイニングやデータベース技術との連携により、悪意性の高いインシデントや被害の大きいインシデントを強調提示する機能。

・本実施形態に係る観測データ装置によって提示される情報を効果的に画面表示する情報視覚化機能。

・5～10分といった短期間ではなく、1週間、1ヶ月といった長期間を対象としたインシデントの傾向分析に向いた情報視覚化機能。

[0069] 〔実施形態2〕

次に、本発明の他の実施形態に係る観測データ表示装置について、図5，12を参照して説明する。本実施形態に係る観測データ表示装置の概要は以下の通りである。

[0070] インターネットの不正アクセスやウィルス等による被害の拡大に伴い、近年ではIDS(Intrusion Detection System)の研究が活発であり、その商用化も進んでいる。これらIDS製品の多くは、監視対象のネットワークに一定の安全対策が施されていることを前提にして、不正現象(インシデント)を漏れなく検出している。しかしながら、特に大規模で開放性の高いネットワークにおいてIDS製品を実際に運用してみると、以下のような問題が生じることがわかった(沢田、高倉、岡部、「開放型大規模ネットワークのためのIDSログ監視支援システム」、情報処理学会論文誌、Vol. 44, No. 8, pp. 1861-1871, 2003.)。

・警報メールの量が膨大になるだけでなく、その相関性や統計的傾向を理解することが困難である。

・複数のシグニチャ(インシデントの種類やパターン)によって一連のインシデントを構成するケースが多く、その全貌を把握するには不十分である。

・インシデントの大量さゆえ、インシデントを事後分析するためのデータベースの運用も容易ではない。

・GUIによる従来の探索的な閲覧システムには、運用上多くの問題がある。

[0071] これらの問題点を解決し、安全性の高いネットワーク運用を実現するために、統合管理型データベースを採用した研究(大谷、桑田、小迫、井上、「統合データベースを用いたインシデント検出情報の分析および意思決定支援システム」、第13回データ高額ワークショップ、A1-6, 2002.)や、テキストマイニングや周期性解析などの分析的手法を用いた研究(宮本、泉、田村、福永、「ネットワーク・サーバ運用監視支援システム」、システム制御情報学会論文誌、Vol. 15, No. 6, pp. 279-287, 2002.)が報告されている。

[0072] 情報視覚化によって不正アクセスの統計的傾向の理解を支援する手法もいくつか報告されている(文献1, 2)。これらの手法は、不正アクセスの時間的推移や属性を理解するのには向いているが、数千、数万といった膨大な計算機をもつ大規模なネットワークに対して局所的な傾向を理解することが難しい。例えば「この組織が集中的に狙われている」というような空間的な相関性を理解するためには、大規模な計算機ネットワーク空間を俯瞰できるような視覚化手法を適用することが望ましい。

[0073] 本発明者らは、上述したように、大規模階層型データを対象とした、上述の基本技術を用いて、数千、数万もの計算機の分布図を表示し、その統計的傾向を一画面に全貌表示する観測データ表示装置を提供する。この装置によって、大量なインシデントの計算機ネットワーク空間上での分布を短時間で把握することができる。

[0074] 本実施形態では実施形態1の変形例として、IDS視覚化画面の上で、インシデントの特徴的傾向をさらに強調する機能を有する観測データ表示装置について説明する。本実施形態では、上述した実施形態1に係る観測データ表示装置で視覚化したIDSに対して、以下の処理を行う機能を追加する。

・特徴的な統計的傾向をもつ計算機をハイライトする機能

・特定の計算機を送信元または受信先とするインシデントを計算機間の線分で表示する機能。

[0075] これらの機能は、インシデントに関する以下のような統計的傾向の理解を支援できる。

・設定ミスや故障等で発生する定期的なエラーと、人為的な集中攻撃インシデントや

、ネットワークに影響を与える重度のトラブル、との区別

・特定の計算機を送信元とするインシデントの、受信先との空間的相関性。または特定の計算機を受信先とするインシデントの、送信元との空間的相関性。

[0076] 上記の〔基本技術〕でも述べたとおり、本実施形態に係る観測データ表示装置は、大規模階層型データの視覚化を行う装置である。図5に、本実施形態に係る観測データ表示装置による階層型データの表示例を示す。本実施形態に係る観測データ表示装置では、階層型データを構成する葉ノードをアイコンで、枝ノードを長方形の枠で表現し、長方形枠の入れ子構造によって階層構造を表現する。

[0077] このとき本実施形態に係る観測データ表示装置では、葉ノードおよび枝ノードを表現する長方形群を、以下の2条件を満たすように画面配置する。

[条件1] すでに配置されている長方形と干渉しない位置に長方形を配置する。

[条件2] [条件1]を満たす位置のうち、配置面積の拡大量が最小である位置に長方形を配置する。

[0078] この条件を満たすような画面配置を実現することによって、大規模な階層型データの全貌を、限られた画面空間にあますことなく表現することができる。

[0079] 本実施形態に係る観測データ表示装置は、数千、数万もの葉ノードを有する階層型データに対し、画面上で互いに重なり合うことなく、できるだけ小さい画面空間に余すことなく、またすべての葉ノードを対等な大きさで表現することができる。本報告の目的、たとえば

・数千、数万ものIPアドレスをもつ大規模ネットワーク環境を対象として、個々のIPアドレスに関するインシデントの統計的傾向の全貌を一画面に表現したい

・同一組織に属する計算機群(＝IPアドレスの上位2,3桁が同一である計算機群)のインシデント傾向を、「インシデント群」として概略的に理解したい

というような目的において、本実施形態に係る観測データ表示装置は非常に適切な技術であるといえる。

[0080] 続いて、実施形態1と本実施形態との関係をより分かりやすくするために、実施形態1で説明したIDS視覚化手法について再び簡単に説明する。本実施形態に係る観測データ表示装置が入力データとするIDSデータは、上述のCisco社の Cisco Secur

e IDS 4320 が出力するIDSログデータファイルに基づくものである。検出された1回のインシデント検出に対してログファイルに出力するデータのうち、本実施形態に係る観測データ表示装置では、以下のデータを参照するものとする。

・送信元IPアドレス

・受信先IPアドレス

・発生時刻

・不正の種類を表す正整数ID

・危険度を表すレベル(5段階)。

[0081] 本実施形態に係る観測データ表示装置では、データ取得部が、ログファイルに記述された多数のインシデントに対して、まず送信元・受信先に記述されたIPアドレスを列挙し、IPアドレスの各バイトの値を参照して階層構造を構築する。

[0082] 続いて、データ取得部は、各々のIPアドレスに対して、送信元となったインシデント、受信先となったインシデントを集計する。換言すれば、不正アクセスを行った回数および不正アクセスを受けた回数をIPアドレスごとに集計する。このとき、発生時刻の範囲、インシデントの種類や重要度、などの条件を加え、条件を満たすインシデントだけを集計することもできる。

[0083] 続いて、基準位置配置部が、ネットワークに接続している計算機のIPアドレスによって構成される階層型データを、観測データ表示装置で表示する。このとき、高さ算出部が、各々のIPアドレスに相当する葉ノードに高さを与えることで、各々のIPアドレスの送信元および受信先となったインシデント数を表現する。また、図12に示すように、送信元となったインシデント数、受信先となったインシデント数、に別個の色を割り当てて表現することで、棒グラフを重ね合わせるように(積み重ねて)インシデント数を表現することが好ましい。そして、3次元表示部が、高さ算出部によって生成されたデータに基づいて観測値を表示装置に3次元表示する。

[0084] 続いて、実施形態1の観測データ表示装置に対する新しい機能拡張について述べる。本実施形態では、実施形態1の観測データ表示装置に対して、以下の機能拡張を試みた。

[0085] [機能拡張1] 特徴的な統計的傾向をもつ計算機をハイライトする機能

本機能では、一定のルールを満たすインシデント群を有する計算機を検出する、という処理を行うプラグイン関数を実装できるようにした。ハイライト部が、このプラグイン関数が検出した計算機を色濃く表示することで、特徴的な統計的傾向をもつ計算機をハイライトする。本実施形態では、非常に短い時間間隔でインシデントをn回以上連続送信（または受信）した計算機を検出する、というプラグイン関数を実装した。なお、本明細書において「インシデントを送信した計算機」および「インシデントの送信元」とは不正アクセスを試みた計算機のことをいい、「インシデントを受信した計算機」および「インシデントの受信先」とは不正アクセスを試みられた計算機のことをいう。この関数は、人為的かつ執拗な攻撃や、影響の大きい重度のトラブル、などをハイライトする効果があると考えられる。

[0086] [機能拡張2] 特定の計算機を送信元または受信先とするインシデントを計算機間の線分で表示する機能

本機能では、観測対象連結表示部が、特定の計算機（例えば画面上でマウスをクリックして指定）を送信元とするインシデントの受信先計算機、あるいは特定の計算機を受信先とするインシデントの送信元計算機、を画面上で線分表示する。この機能により、特徴的な攻撃を受けている（または発している）計算機の攻撃元（あるいは攻撃先）が、広く分布しているのか、特定の組織に集中しているのか、1台の計算機に特化しているのか、を理解する効果があると考えられる。

[0087] このような観測データ表示装置を実現するための構成について以下に説明する。なお、上述した実施形態1と同様の機能を有する部材については同一の部材番号を付し、その説明を省略する。図18は、本実施形態に係る観測データ表示装置200の機能ブロックを示すブロック図である。観測データ表示装置200は、図18に示すように、データ取得部20、観測対象分類部11、基準位置配置部12、高さ算出部13、および3次元表示部14と、さらにハイライト部21および観測対象連結表示部22とを備えている。

[0088] データ取得部20は、コンピュータネットワークにおいて計算機（観測対象）を特定するためのIPアドレス（観測対象識別情報）と、計算機が不正アクセスを行った件数および受けた件数（インシデント数、観測値）との組を取得するためのものである。デー

タ取得部20は、例えば上述したように、インシデントに対して出力されたログファイルから、IPアドレスとインシデント数との組を抽出する。

また、本実施形態においてデータ取得部20は、各インシデントの発生時刻の情報も取得する。

[0089] 観測対象分類部11、基準位置配置部12、高さ算出部13、および3次元表示部14は、上述した実施形態1と同様である。

[0090] ハイライト部21は、3次元表示部14によって表示された観測値のうち、特定の観測値を強調表示するためのものである。本実施形態では、ハイライト部21がデータ取得部20によって取得したインシデント情報(送信元のIPアドレス、受信先のIPアドレス、発生時刻)を基に、所定の時間間隔以下でインシデントをn回以上連続送信(または受信)した計算機を抽出し、抽出した計算機についてのインシデント数を強調表示する。ここで、強調表示の手法としては、検出した計算機について、インシデント数を表す棒グラフの明度を大きくするなどの手法が挙げられる。

[0091] なお、ハイライト部21は、3次元表示部14によって作成された画像に、明度を大きくした棒グラフを表示装置50で重ね合わせることによってインシデント数を強調表示してもよいし、あるいは、3次元表示部14が棒グラフを作成する際に、3次元表示部14に明度を大きくした棒グラフを作成させることによってインシデント数を強調表示してもよい。

[0092] 観測対象連結表示部22は、ある特定の計算機が送信した各インシデントの受信先を提示したり、ある特定の計算機が受信した各インシデントの送信元を提示したりするためのものである。前者について具体的に説明すると、観測対象連結表示部22は、特定の計算機と、その計算機から送信されたインシデントの受信先となった計算機とを線分で連結した画像を表示する。後者についても同様であり、以下では説明を省略する。

[0093] 観測対象連結表示部22は、データ取得部20が取得したインシデント情報(送信元のIPアドレス、受信先のIPアドレス)を基に、ある特定の計算機(IPアドレス)が送信元となったインシデントを抽出し、その受信先の計算機(IPアドレス)を特定する。そして、送信元の計算機と特定した受信先の計算機とを線分で連結した画像を作成する

。なお、特定の計算機は、例えば、ユーザーがマウスなどによってインシデント数を表す棒グラフをクリックすることによって選択されることが好ましい。

[0094] なお、観測対象連結表示部22は、3次元表示部14によって作成された画像に、線分を表示装置50で重ね合わせることによって送信元と受信先との関係を表示してもよいし、あるいは、3次元表示部14が棒グラフを作成する際に、3次元表示部14に線分を含んだ画像を作成させることによって送信元と受信先との関係を表示してもよい。

[0095] 本実施形態では、実施形態1の観測データ表示装置に対して

・統計的特徴をもつ計算機のハイライト

・インシデントを送受信する計算機間の線分表示

の2つの拡張を行った。この結果として、以下の効果を得ることができる。

・設定ミスや故障等で発生する定期的なインシデントと、人為的な集中攻撃インシデントや、ネットワークに影響を与える重度のトラブル、との区別。

・特定の計算機を送信元とするインシデントの、受信先との空間的相関性。または特定の計算機を受信先とするインシデントの、送信元との空間的相関性。

[0096] また、本実施形態に係る観測データ表示装置に対して、さらに以下の機能拡張を行うこともできる。

・データマイニングやデータベース技術との連携により、悪意性の高いインシデントや被害の大きいインシデントの特定を高性能化する機能

・悪意性や被害の小さいインシデントの表示を目立たなくする表示機能

・不正アクセス傾向の時系列変化を効果的に表現する情報視覚化機能

・5～10分といった短期間ではなく、1週間、1ヶ月といった長期間を対象としたインシデントの傾向分析に向いた情報視覚化機能。

[0097] 〔実施形態3〕

本発明のさらに他の実施形態に係る観測データ表示装置について、図5, 8, 12, 16を参照して説明する。本実施形態に係る観測データ表示装置の概要は以下の通りである。

[0098] 計算機ネットワークのセキュリティ維持管理の目的で、近年IDS(侵入検知システム

)技術の研究開発が進んでいる。しかし現状のIDS製品には、ログ出力情報の膨大さ、複雑化するネットワーク攻撃の分析技術の不足、などの課題が残っている。本実施形態ではこの課題を改善する一手段として、情報視覚化の技術を適用してネットワーク侵入検知データの概要理解と詳細探索を支援する技術を提供する。本実施形態では計算機ネットワークに分布する計算機群をIPアドレスで階層化して、上述した基本技術による情報視覚化技術を用いて画面表示する。この画面表示上に侵入検知データの統計量をマッピングすることで、現実性のあるネットワーク侵入検知の振る舞いをいくつか観察できる。

[0099] インターネットの不正アクセスやウィルス等による被害の拡大に伴い、近年ではIDS(Intrusion Detection System)の研究が活発であり、その商用化も進んでいる。これらIDS製品の多くは、監視対象のネットワークに一定の安全対策が施されていることを前提にして、不正現象(インシデント)を漏れなく検出している。しかしながら、特に大規模で開放性の高いネットワークにおいてIDS製品を実際に運用してみると、以下のような問題が生じることがわかった(沢田, 高倉, 岡部,「開放型大規模ネットワークのためのIDSログ監視支援システム」, 情報処理学会論文誌, 44, 8, pp. 1861-1871, 2003)。

・インシデント1件ごとに1件の警報を送信するメール通報システムでは、警報メールの量が膨大になるだけでなく、その相関性や統計的傾向を理解することが困難である。

・最近の不正アクセスは複雑化する傾向にあり、複数のシグニチャ(インシデントの種類やパターン)によって一連の不正アクセスを構成するケースが多く、その全貌を把握するには機械的処理だけでは不十分である。

・インシデントの大量さゆえに、インシデントを事後分析するためのデータベースの運用も容易ではない。

・GUIによる従来の探索的な閲覧システムには、重要なインシデントを検索することが難しい、多忙な管理者では手に負えない、多数の管理者間の知識共有に向かない、遠隔からの業務に向かない、などの問題がある。

[0100] これらの問題点を解決し、安全性の高いネットワーク運用を実現するための手段は

いくつか考えられる。本実施形態では、CG技術によって情報の特徴を提示する「情報視覚化」という技術を適用した観測データ表示装置について説明する。本実施形態の観測データ表示装置は、大規模階層型データを対象とした、上述の基本技術を用いて、数千、数万もの計算機を有する大規模ネットワークに広がるインシデントに対して、その統計的傾向を一画面に全貌表示する。本実施形態に係る観測データ表示装置により、大量なインシデントの傾向を容易に把握できるだけでなく、従来のGUI技術の問題をも改善できると考えられる。

[0101] 不正アクセスの検出、警告、分析に関する技術は、すでにいくつか商品化されているが、いずれの製品にしても上述した問題点を解決してはいない。この問題に対して、いくつかの改善手法が提案されている。例えばIDSが検出するインシデントを蓄積する統合管理型のデータベースにより、インシデントの事後分析を支援する研究がある(大谷, 桑田, 小迫, 井上, 「統合データベースを用いた不正アクセス検出情報の分析および意思決定支援システム」, 第13回データ高額ワークショップ, A1-6, 2002.)。また、テキストマイニングや周期性解析などの分析的手法を用いて、精度の高いインシデント分析を目指す研究がある(宮本, 泉, 田村, 福永, 「ネットワーク・サーバ運用監視支援システム, システム制御情報学会論文誌」, 15, 6, pp. 279-287, 2002.)。

[0102] 情報視覚化によってインシデントの統計的傾向を表現する手法もいくつか発表されている。文献1では、「見えログ」という手法が提案されている。この手法では、画面を水平方向に分割し、左側にインシデント全体の時間別件数を一列に棒グラフ表示し、その右側にユーザーが指定したある時間におけるインシデントの内訳を表示する。この手法はインシデントの時間的な全体的傾向と局所的傾向を同時に表現できる点に特徴がある。またIDSとはデータ構造が異なるが、文献2では、1台のウェブサーバーのアクセスログファイルを対象として、横軸に属性の種類、縦軸に属性値、を配置した Parallel Coordinate という座標系に個々のアクセスを配置する手法をAxelssonが提案している。この手法は不正アクセスの属性値の相関性を表現することで、不正アクセスの詳細な性格の理解を支援している。

[0103] 以上の従来手法と異なって本実施形態の観測データ表示装置は、数千、数万規模の多数の計算機が接続された大規模ネットワークを対象として、その個々の計算

機にて送受信されるインシデントの計算機ネットワーク空間上での分布を視覚化することを目的としている。本報告の提案手法は、大量な不正アクセスの中に潜む人為的な要因、例えば

・一台の計算機から大量の計算機を攻撃する。

・大量の計算機から一台の計算機を攻撃する。

・ある特定の組織に属する計算機に組織外からウィルスを配置すると、その計算機が攻撃者に転じて、一斉に他者を攻撃する。

・ある特定の組織に属する多数の計算機を、組織外から一斉に攻撃する。

というように、計算機の空間的分布に関係ある人為的要因の視覚化に向いていると考えられる。

[0104] 本実施形態に係る観測データ表示装置は、大規模な階層型データの全貌を一画面に表現することを目的としたものである。本実施形態に係る観測データ表示装置は、階層型データを構成する葉ノードをアイコンで表現し、枝ノードを入れ子状の長方形の枠で表現している。なお、これらの機能は、基準位置配置部によって得られる。

[0105] 図5に、本実施形態に係る観測データ表示装置による階層型データの視覚化例を示す。観測データ表示装置は、数千、数万もの葉ノードを有する階層型データに対し、画面上で互いに重なり合うことなく、できるだけ小さい画面空間に余すことなく、またすべての葉ノードを対等な大きさで表現することができる、という点において他の階層型データ視覚化装置に対する優位性をもつ。

[0106] 本実施形態に係る観測データ表示装置では、ネットワークに接続されている計算機のIPアドレスに注目して計算機群をグループ化する。まずIPアドレスの上位1バイト(オクテット)目が同一である計算機をグループ化し、続いて上位2バイト目が同一である計算機をグループ化し、さらに上位2バイト目が同一である計算機をグループ化することで、4段階の階層を有する階層型データを構築する。図16は、IPアドレスを参照して8台の計算機を階層型データに格納した例を示す図である。これを上述した基本技術で視覚化することにより、ネットワーク上の計算機の分布図を表現する。

[0107] 本実施形態に係る観測データ表示装置を用いて各計算機をアイコン表示することにより、個々の計算機に関するデータを画面上で重なりなく表現できるとともに、IPア

ドレスの上位バイトが同一である計算機群(多くの場合、同一組織に属する計算機群)を画面上で一集団として認識することができる。このような表現は、本実施形態の目的、たとえば

・数千・数万ものIPアドレスをもつ大規模ネットワーク環境を対象として、個々のIPアドレスに関する不正アクセスの統計的傾向の全貌を一画面に表現したい

・同一組織に属する計算機群(=IPアドレスの上位2,3桁が同一である計算機群)の不正アクセス傾向を、「不正アクセス群」として概略的に理解したい

というような目的において非常に適切な技術であるといえる。

[0108] 本実施形態の観測データ表示装置に入力されるデータとなる不正アクセスデータは、上述した、Cisco社の Cisco Secure IDS 4320 が出力するIDSログデータファイルに基づくものである。当システムではシグネチャ(signature)と呼ばれる典型的なパターンに基づいて不正アクセスを検出するものである。データ取得部は、以下の処理を行う。検出された1回の不正アクセス検出に対してログファイルに出力するデータのうち、本実施形態に係る観測データ表示装置は、以下のデータを参照する。

・送信元IPアドレス。

・受信先IPアドレス。

・発生時刻。

・不正の種類を表す正整数ID。

・危険度を表すレベル(5段階)。

[0109] 本実施形態では、データ取得部がログファイルに記述された多数の不正アクセスに対して、まず送信元、受信先に記述されたIPアドレスを列挙し、IPアドレスの各バイトの値を参照して階層構造を構築する。

[0110] 続いて各々のIPアドレスに対して、データ取得部が、送信元となった不正アクセス数、受信先となった不正アクセス数を集計する。このとき、発生時刻の範囲、不正アクセスの種類や重要度、などの条件をユーザーに設定させ、条件を満たす不正アクセス数だけを集計することもできる。

[0111] 続いて、基準位置配置部が、IPアドレスによって構成される階層型データを上述の基本技術で表示する。このとき、各々のIPアドレスに相当する葉ノードに高さを与える

ことで、各々のIPアドレスの送信元および受信先となった不正アクセス数を表現する。図12に示すように、送信元となった不正アクセス数、受信先となった不正アクセス数、に別個の色を割り当てて表現することで、棒グラフを束ねるように不正アクセス数を表現することが好ましい。

[0112] 不正アクセス視覚化の効果を高めるために、本実施形態の観測データ表示装置は以下の拡張機能を持つことが好ましい。これらの拡張機能によって、上述の文献(沢田, 高倉, 岡部,「開放型大規模ネットワークのためのIDSログ監視支援システム」, 情報処理学会論文誌, 44, 8, pp. 1861-1871, 2003)にて提案されているログ監視支援システムの方針の大半を満たすことができる。具体的には、下記の拡張機能(1), (2)によって、不正アクセスの全体的な統計分布を俯瞰するだけでなく、その詳細分析をも可能にする。また、下記の拡張機能(3)によって、管理者による手動操作の手間を低減し、Webブラウザを用いて汎用的な閲覧手段を提供することができる。

[0113] (1)特異な不正アクセスのハイライト機能

上記拡張機能(1)として、例えば、ハイライト部が、数値的に特異な傾向のある不正アクセス群をもつ棒グラフを、特に明るい色で表現する機能が挙げられる。また、例えば、

・非常に多くの受信先に同一送信元から一斉発信している不正アクセス、

・非常に多くの送信先から同一受信元が一斉受信している不正アクセス

・直前の時間帯よりも不正アクセス数が急増しているIPアドレス

をハイライトすることで、ネットワーク管理者に注意を促すことができる。

[0114] (2)特定IPアドレスに注視した視覚化機能

上記拡張機能(2)として、例えば、特定IPアドレスに相当する棒グラフを画面上でクリックすると、そのIPアドレスを送信元あるいは受信先とする不正アクセスだけを再集計して表示する機能、および観測対象連結表示部22がその送信先と受信先を連結する線分を表示する機能が挙げられる。この機能によりネットワーク管理者は、特定の計算機に関わる不正アクセスの詳細を探索することができる。ただしこの機能は、下記の拡張機能(3)で紹介するWebブラウザ上でのレポート機能では実現しない。

[0115] (3)一定時間ごとのレポート機能

上記拡張機能(3)として、一定時間ごと(例えば5分ごと)に不正アクセス数を集計して視覚化し、その結果を、観測結果保存部がJPEG画像に保存する、という機能が挙げられる。そのJPEG画像群に対する目次となるようなWebページを自動生成することで、本手法特有のユーザインタフェースを用いることなく、Webブラウザだけで不正アクセスの出現傾向を観察できる。

[0116] このような観測データ表示装置を実現するための構成について以下に説明する。なお、上述した実施形態1および2と同様の機能を有する部材については同一の部材番号を付し、その説明を省略する。図19は、本実施形態に係る観測データ表示装置300の機能ブロックを示すブロック図である。観測データ表示装置300は、図18に示すように、データ取得部30、観測対象分類部11、基準位置配置部12、高さ算出部13、3次元表示部14、ハイライト部21、および観測対象連結表示部22と、さらに観測結果保存部31および観測データ画像データベース32を備えている。

[0117] データ取得部30は、コンピュータネットワークにおいて計算機(観測対象)を特定するためのIPアドレス(観測対象識別情報)と、計算機が不正アクセスを行った件数および受けた件数(インシデント数、観測値)との組を取得するためのものである。データ取得部30は、例えば上述したように、インシデントに対して出力されたログファイルから、IPアドレスとインシデント数との組を抽出する。

また、データ取得部30は、各インシデントの発生時刻の情報も取得する。そして、本実施形態においてデータ取得部30は、インシデントを、発生時刻の情報に基づいて一定時間ごと(例えば5分ごと)に集計する。

[0118] 観測対象分類部11、基準位置配置部12、高さ算出部13、3次元表示部14、ハイライト部21、および観測対象連結表示部22は、上述した実施形態1、2と同様である。

[0119] 観測結果保存部31は、3次元表示部14によって表示装置50に表示させる画像を、観測データ画像データベース32に保存するためのものである。上述したように、データ取得部30は、インシデントを一定時間ごとに集計するため、観測データ画像データベース32には、一定時間ごとの観測結果を示す画像が蓄積されることになる。また、観測データ表示装置300がハイライト部21を備えている場合、ハイライト表示した

画像を保存することが好ましい。このため、観測結果保存部31は、3次元表示部14によって作成された画像に、ハイライト部21によるハイライト効果を反映した画像を観測データ画像データベース32に保存する。なお、観測データ画像データベース32は、RAM又はHDDなどの画像データを記憶できる各種記憶装置によって実現される。

[0120] 本実施形態では、上述の基本技術を用いて、大規模ネットワークへの不正アクセスの統計的傾向を一画面に表示する観測データ表示装置について説明した。本実施形態の観測装置100は、観測対象がコンピュータネットワークに接続されたコンピュータであり、観測対象識別情報が、コンピュータに割り当てられたコンピュータネットワークにおける階層構造を有するアドレス情報であり、基準位置配置部が、アドレス情報を階層ごとの部分情報に分割し、上位階層の部分情報から順に、部分情報が同一であるコンピュータをグループ化することにより、各コンピュータの基準位置をグループごとにまとめて二次元平面内に配置するものである。

[0121] 本実施形態に係る観測データ表示装置には、さらに以下の拡張機能を付加してもよい。

(a) データマイニングやデータベース技術などとの連携による、悪意性の高い不正アクセスや被害の大きい不正アクセスを効果的に警告できる情報視覚化機能。

(b) 5～10分といった短期間ではなく、1週間、1ヶ月といった長期間を対象とした不正アクセスの傾向分析に向いた情報視覚化機能。

(c) 不正アクセス傾向の時系列変化を効果的に表現する情報視覚化機能。

[0122] 本実施形態に係る観測データ表示装置は、IPアドレスを元に検査対象と計測値を三次元空間に分類する、上述の基本技術を拡張し、警報数を棒グラフ表示するとともに攻撃元および攻撃先の関連性を線分で表示し、その時間変化を動画的に表示する機能、および、不必要な警報を表示から除去する装置を開発した。これにより、不正アクセスの前後で発生した現象まで特定可能となり、従来の検知システムでは把握困難であった、個々の監視対象に関する不正アクセスの前兆現象(偵察活動)および不正アクセス対策後の二次被害(報復的攻撃やごく少数の検知回避を試みた攻撃)までもが視認できるようになる。また、可視化システムが標準装備すべき、視点の変

更や拡大・縮小表示にも対応することが好ましい。

[0123] また、各実施形態に係る観測データ表示装置は、可視化情報の動画的な表示や可視化された情報に対する更なる分類・フィルタリングオペレーションを行える仕組(インタフェース)をさらに備えてもよい。

[0124] 本実施形態に係る観測データ表示装置は、万から億程度の監視対象の計測値を三次元表示する。さらに、監視対象の大多数では平常値としてほぼゼロに近い値が計測される一方、ごく少数の対象で毎秒数千以上の値を、しかも、その99%が誤検知として計測される環境で、真の異常値を強調表示することができる。

[0125] 最後に、観測データ表示装置の各機能、特に、データ取得部、基準位置配置部、観測値プロット部、高さ算出部、3次元表示部、ハイライト部、観測対象連結表示部、観測結果保存部は、ハードウェアロジックによって構成してもよいし、次のようにCPUを用いてソフトウェアによって実現してもよい。

[0126] すなわち、観測データ表示装置は、各機能を実現する制御プログラムの命令を実行するCPU(central processing unit)、上記プログラムを格納したROM(read only memory)、上記プログラムを展開するRAM(random access memory)、上記プログラムおよび各種データを格納するメモリ等の記憶装置(記録媒体)などを備えている。そして、本発明の目的は、上述した機能を実現するソフトウェアである観測データ表示装置の制御プログラムのプログラムコード(実行形式プログラム、中間コードプログラム、ソースプログラム)をコンピュータで読み取り可能に記録した記録媒体を、上記観測データ表示装置に供給し、そのコンピュータ(またはCPUやMPU)が記録媒体に記録されているプログラムコードを読み出し実行することによっても、達成可能である。

[0127] 上記記録媒体としては、例えば、磁気テープやカセットテープ等のテープ系、フロッピー(登録商標)ディスク/ハードディスク等の磁気ディスクやCD-ROM/MO/MD/DVD/CD-R等の光ディスクを含むディスク系、ICカード(メモリカードを含む)/光カード等のカード系、あるいはマスクROM/EPROM/EEPROM/フラッシュROM等の半導体メモリ系などを用いることができる。

[0128] また、観測データ表示装置を通信ネットワークと接続可能に構成し、上記プログラムコードを通信ネットワークを介して供給してもよい。この通信ネットワークとしては、特

に限定されず、例えば、インターネット、イントラネット、エキストラネット、LAN、ISDN、VAN、CATV通信網、仮想専用網(virtual private network)、電話回線網、移動体通信網、衛星通信網等が利用可能である。また、通信ネットワークを構成する伝送媒体としては、特に限定されず、例えば、IEEE1394、USB、電力線搬送、ケーブルTV回線、電話線、ADSL回線等の有線でも、IrDAやリモコンのような赤外線、Bluetooth(登録商標)、802．11無線、HDR、携帯電話網、衛星回線、地上波デジタル網等の無線でも利用可能である。なお、本発明は、上記プログラムコードが電子的な伝送で具現化された、搬送波に埋め込まれたコンピュータデータ信号の形態でも実現され得る。

[0129] 以上のように、本発明の観測データ表示装置は、観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる観測値との組を取得するデータ取得部と、当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置部と、上記観測値に応じた高さを観測値ごとに算出する高さ算出部と上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる3次元表示部と、を備えた構成となっている。よって、上述したように、多数の監視対象から得られた観測値を3次元表示することができる。

[0130] また、上記観測データ表示装置は、上記観測対象識別情報に基づいて観測対象を階層的なクラスターに分類する観測対象分類部をさらに備え、上記基準位置配置部が、観測対象の観測値を表示するための上記基準位置を、上記階層的なクラスターに基づいて、二次元平面における入れ子状の構造となるように配置することが好ましい。

[0131] 上記構成によれば、基準位置が、観測対象を識別する識別情報に基づいて入れ子状の構造となるように配置される。よって、各観測対象の観測値が表示される際に、観測対象が識別情報に応じてグルーピングされることになる。このため、ユーザーは、観測値と観測対象との関係を容易に把握することができる。例えば、観測値として不正アクセス数、観測対象としてコンピュータネットワークに接続されたコンピュータ

、識別情報としてIPアドレスを用いれば、コンピュータがIPアドレスに基づいて(例えば、セグメントごとなどに)グルーピングされるので、ユーザーは、どのネットワークでどの程度不正アクセスが存在するかを容易に把握することができる。

[0132] また、上記基準位置配置部は、同一のクラスターに分類される観測対象の基準位置が一塊になるように、基準位置を配置することが好ましい。

[0133] また、上記観測対象はコンピュータネットワークに接続されたコンピュータであり、上記観測対象識別情報は、上記コンピュータに割り当てられた上記コンピュータネットワークにおける階層構造を有するアドレス情報であることが好ましい。

[0134] 上記構成によれば、コンピュータネットワークに接続された多数のコンピュータを観測して得られた観測値を3次元表示することができる。

[0135] また、上記観測値は、不正アクセスを試みた件数、不正アクセスを試みられた件数の一方または両方であることが好ましい。

[0136] 上記構成によれば、コンピュータネットワークに接続された多数のコンピュータを観測して得られた不正アクセス件数を3次元表示することができる。

[0137] また、上記観測データ表示装置は、不正アクセスの試みたコンピュータと不正アクセスを試みられたコンピュータとの対応関係を示す線分を、両コンピュータのそれぞれの基準位置あるいは基準位置上の棒グラフを両端として表示装置に表示させる観測対象連結表示部をさらに備えていることが好ましい。

[0138] 上記構成によれば、不正アクセスを試みたコンピュータと、その不正アクセスが試みられたコンピュータとの関係を明確に表示することができる。

[0139] また、上記観測データ表示装置は、画像データを格納する記憶部と、3次元表示部によって表示装置に表示させる画像の画像データを、上記記憶部に格納する観測結果保存部とをさらに備えていることが好ましい。

[0140] 上記構成によれば、観測結果を示す画像データを記憶部に保存することができる。よって、後から適宜画像データを記憶部から読み出し、観測対象の観測値がどのようなものであったかを3次元表示された画像として閲覧することができる。

[0141] また、上記観測値は、不正アクセスを試みた件数、不正アクセスを試みられた件数の一方または両方であり、上記データ取得部は、所定時間ごとの上記観測値を抽出

するものであり、上記観測結果保存部は、上記所定時間ごとの観測値について作成された画像の画像データを、上記記憶部に格納することが好ましい。

[0142] 上記構成によれば、記憶部には、所定時間ごとの不正アクセスの件数を観測し、一覧表示した画像データが蓄積される。よって、或る不正アクセスの前後においてその不正アクセスと関連して発生した不正アクセスを特定することができ、従来の検知システムでは把握困難であった、個々の監視対象に関する不正アクセスの前兆現象(偵察活動)および不正アクセス対策後の二次被害(報復的攻撃やごく少数の検知回避を試みた攻撃)までもが視認できるようになる。

[0143] また、上記観測データ表示装置は、上記観測対象がコンピュータネットワークに接続されたコンピュータであり、上記観測対象識別情報が、上記コンピュータに割り当てられた上記コンピュータネットワークにおける階層構造を有するアドレス情報であり、上記基準位置配置部が、上記アドレス情報を階層ごとの部分情報に分割し、上位階層の部分情報から順に、部分情報が同一であるコンピュータをグループ化することにより、各コンピュータの上記基準位置をグループごとにまとめて二次元平面内に配置するものであってもよい。

[0144] 上記構成によれば、例えばIPアドレス等の階層構造を有するアドレス情報に基づいて、ネットワーク上のコンピュータをグループ化することができるので、ネットワーク上に分散配置されたコンピュータを観測対象とする、観測データ表示装置を実現できる。

[0145] また、上記観測データ表示装置は、上記観測値が、観測対象であるコンピュータが送信元となった不正アクセスおよび受信先となった不正アクセス回数であり、上記観測値プロット部が、送信元となった不正アクセスを示す棒グラフと受信先となった不正アクセス回数を示す棒グラフとを重ねて、上記基準位置にプロットするものであってもよい。

[0146] 上記構成によれば、IDS(Intrusion Detection System)に好適に用いることができる観測データ表示装置を実現できる。

[0147] また、上記観測データ表示装置は、不正アクセスの送信元となったコンピュータと当該不正アクセスの受信先となったコンピュータとの対応関係を示す線分を、両コンピ

ュータのそれぞれの基準位置あるいは基準位置上の棒グラフを両端として表示する観測対象連結表示部をさらに備えるものであってもよい。

[0148] 上記構成によれば、不正アクセスの送信元のコンピュータと受信先のコンピュータとの関係が視覚的に表示されるため、不正アクセス元及び又は不正アクセス先のコンピュータを瞬時に識別することができる。

[0149] なお、上記観測データ表示装置は、コンピュータによって実現してもよく、この場合には、コンピュータを上記各部として動作させることにより上記観測データ表示装置をコンピュータにて実現させる観測データ表示装置の観測データ表示プログラム、およびそれを記録したコンピュータ読み取り可能な記録媒体も、本発明の範疇に入る。

[0150] 〔実施例1〕

実施形態1で説明した観測データ表示装置の一実施例について、図8～11を参照して説明するが、上述の実施形態1はこれに限定されるものではない。

[0151] 観測データ表示装置を機能させるためのプログラムを Java(登録商標) 1.4 の上で実装し、IBM ThinkPad A31p (CPU 1.7GHz, RAM 756MB)および Microsoft Windows(登録商標) 2000 の上で実行した。GUIは Java(登録商標) Swing ライブラリを用いて実装し、3次元画像生成機能は Java(登録商標) AWT ライブラリを用いて実装した。

[0152] 実験に用いたIDSログファイルは、実在するネットワーク環境で6時間にわたって記録したもので、61822行のインシデント記録をもち、3984個のIPアドレスにわたってインシデントが検出されている。測定の結果、IDSログファイルの読み込みに120秒、階層型データ構築およびビューの適用に合計約0.6秒、アクセス数の再集計およびJPEG画像生成に平均7.1秒を要したことが分かった。

[0153] 以下に提示する画像例では、各々のIPアドレスについて、送信元となったインシデント数を青で、受信先となったインシデント数を赤で表示している。送信先・受信元ともにゼロであったIPアドレスに相当する葉ノードは、高さゼロの灰色のアイコンで表示している。

[0154] 図8は、ある時刻から5分間のインシデントの集計結果、図9はその直後5分間の集計結果、図10はその2時間後の5分間の集計結果、図11はさらにその2時間後の5分

間の集計結果、をそれぞれ視覚化した例である。

[0155] 図8の対象時点では、多数の送信元にインシデントの発生源を仕掛けて、多数の受信先にインシデントを試していたと思われる傾向が見られる。図9の対象時点では、インシデントの発生源をうまく起動できた計算機から、特定の受信先に向けて集中的に攻撃させていることがわかる。図9の対象時点では、図10で送信元となった計算機は既に対処されているものの、同様なインシデント発生源を他の計算機に仕掛けて、さらに別の受信先も集中的に攻撃していることがわかる。図11ではさらに別に、特定のドメイン内にある多数の計算機が横断的にインシデントを受信していることがわかる。

[0156] 〔実施例2〕

実施形態2で説明した観測データ表示装置の一実施例について、図13～15を参照して説明するが、上述の実施形態2はこれに限定されるものではない。

[0157] 観測データ表示装置を機能させるためのプログラムを Java(登録商標) 1.4 の上で実装し、IBM ThinkPad A31p (CPU 1.7GHz, RAM 756MB)および Microsoft Windows(登録商標) 2000 の上で実行した。GUIは Java(登録商標) Swing ライブラリを用いて実装し、3次元画像生成機能は Java(登録商標) AWT ライブラリを用いて実装した。

[0158] 以下に示す実行例は、実在する計算機ネットワークの1時間のIDSログファイルを用いたものである。このログファイルには、1569台の計算機に関わる30306行のインシデントが記録されている。なお実行例の一部は、白黒印刷された紙面上では効果を認識できないことを断っておく。

[0159] 図13は1時間のインシデントの総計を表示したものである。白丸の部分に、受信先となったインシデントを多数もつ計算機が4台見られるが、このうち1台は棒グラフの色が暗くなっている。この1台の受信したインシデントは、執拗な人為的攻撃や、影響の大きい重度なトラブルである可能性が低いので、他の3台よりも危険度が低い、と考えられる。このように、図13から、多数の攻撃を受けた計算機が白丸の中に4台見られるが、そのうち1台は棒グラフの色が暗いので、他の3台より危険度が低いと認識することができる。

[0160] 図14は、図13に白丸で示した4台のうち、棒グラフの色が明るくなっている計算機

のうち1台を指定して、その送信先を黄色い線で示したものである。この結果から、特定の計算機に不正アクセスを送信している計算機は非常に多数あるが、その大半は広い意味での同一組織内の計算機であることがわかる。また、この送信元である計算機のインシデントに着目すると、その多くの計算機は1,2回のインシデントを受信するとともに、多数のインシデントを同一計算機に送信していることがわかる。この事実は、送信元である多数の計算機が、インシデントを受信したことがきっかけで送信者に転じた可能性を示唆している。このように、図14から、多数の計算機から1台の計算機に不正アクセスを送信しているが、その送信元の大半が送信以前に1,2回の不正アクセスを受信していることがわかる。

[0161] 図15は、インシデントを多数受信している別の計算機を指定した例である。この計算機は、狭い意味での同一組織の多数の計算機からインシデントを受信している。詳しく調べたところ、このインシデントは悪意的な攻撃ではなく、組織的に必要に迫られて同一計算機に例外的なアクセスをしていたのが、インシデントとして検出されていた、ということがわかった。このように図15から、同一組織の複数の計算機から1台の計算機に不正アクセスを送信していることがわかる。

[0162] 〔実施例3〕

実施形態3で説明した観測データ表示装置の一実施例について、図8, 9, 10, 14, 15を参照して説明するが、上述の実施形態2はこれに限定されるものではない。

[0163] 本実例では、実在する大規模ネットワークに実際に生じた大量のインシデントの視覚化例を提示し、どのような現象を視覚的に理解できたか、について解説する。

[0164] 観測データ表示装置を機能させるためのプログラムを Java(登録商標) 1.4 の上で実装し、IBM ThinkPad A31p (CPU 1.7GHz, RAM 756MB)および Microsoft Windows(登録商標) 2000 の上で実行した。GUIは Java(登録商標) Swing ライブラリを用いて実装し、画像生成機能は Java(登録商標) AWT ライブラリを用いて実装した。また危険度レベルや発生時刻の範囲などで条件をつけて不正アクセス数を集計するためのGUIを開発した。

[0165] 以下、図8～10、14, 15を用いて、実在するネットワーク環境で記録したIDSデータを視覚化した例を示す。この例では、各々の計算機について、送信元となった不正

アクセス数を青で、受信先となった不正アクセス数を赤で表示している。送信先・受信元ともにゼロであった計算機は、高さゼロの灰色のアイコンで表示している。なお実行例の一部は、白黒印刷された紙面上では効果が認識できないことを断っておく。

[0166] 図8～10は、6時間にわたって記録した61822行の不正アクセス記録をもち、3984個のIPアドレスにわたって不正アクセスが検出されたIDSの例である。測定の結果、本実施例の観測データ表示装置は、IDSログファイルの読み込みに120秒、階層型データ構築およびビューの適用に合計約0.6秒、アクセス数の再集計およびJPEG画像生成に平均7.1秒を要した。

[0167] 図8は、ある時刻から5分間の不正アクセスの集計結果、図9はその直後5分間の集計結果、図10はその2時間後の5分間の集計結果、をそれぞれ視覚化した例である。これらの視覚化結果から、以下のような不正アクセス群を観察できた。

[0168] 図8の対象時点では、多数の送信元計算機から、多数の受信先計算機に不正アクセスを試していたと思われる傾向が見られる。図9の対象時点では、不正アクセスの発生源をうまく起動できた計算機に、特定の計算機に向けて集中的に攻撃させていることがわかる。図10の対象時点では、図9で送信元となった計算機は既に対処されているものの、他の計算機にも不正アクセス発生源が仕掛けられ、新たに別の計算機も集中的に攻撃されていることがわかる。なお図8～10において、送信元はネットワーク外の計算機、受信先はネットワーク内の計算機である。

[0169] 図14，15は、別のIDSデータを視覚化した上で、特定の棒グラフを画面上でクリックして、その棒グラフに対応するIPアドレスが送信元または受信先になっている不正アクセスを線分で表現した例である。

[0170] 図14に示す例では、1台の計算機が多数の計算機から不正アクセスを受信しているが、その送信元となっている計算機群の大半では、1,2回の不正アクセスを受信した後に、多数の不正アクセスを同一計算機に向かって送信していることがわかる。この視覚化結果から、多数の計算機が同様に乗っ取られた結果として、同一計算機が集中攻撃されている可能性がある、と判断して詳しく調べたところ、この不正アクセス自体が一種の誤報であることがわかった。

[0171] 図15に示す例では、1台の計算機が同一組織に属する複数の計算機から不正アクセスを受信している。この結果は、組織ぐるみで不正アクセスを発生している可能性を示唆している。

[0172] 本発明は上述した各実施形態および各実施例に限定されるものではなく、請求項に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせて得られる実施形態についても本発明の技術的範囲に含まれる。

産業上の利用の可能性

[0173] 本発明の観測データ表示装置は、毎秒数千以上のペースで生成されるデータの内、ごく一部に異常値あるいは特異値が発生する全て環境に適用できる。たとえば、ネットワークにおける不正アクセス検知システム、ユビキタスコンピューティング環境で生成されるデータに対する解析ソフトウェア、株価変動の異常を検知するソフトウェア、入院患者のセンサーデータの急変動を強調表示するシステムなどが挙げられる。

請求の範囲

[1] 観測対象を観測した観測値を表示する観測データ表示装置であって、

観測対象を特定するための観測対象識別情報と該観測対象を観測した観測値との組を取得するデータ取得部と、

上記観測対象識別情報に基づいて当該観測対象の観測値を表示するための基準位置を二次元平面内に配置する基準位置配置部と、

観測対象の観測値を、上記基準位置配置部によって配置された基準位置からの高さとしてプロットする観測値プロット部と、

上記観測値プロット部によって生成されたデータに基づいて観測値を表示装置に3次元表示する3次元表示部と、を備えることを特徴とする観測データ表示装置。

[2] 上記観測対象がコンピュータネットワークに接続されたコンピュータであり、

上記観測対象識別情報が、上記コンピュータに割り当てられた上記コンピュータネットワークにおける階層構造を有するアドレス情報であり、

上記基準位置配置部が、上記アドレス情報を階層ごとの部分情報に分割し、上位階層の部分情報から順に、部分情報が同一であるコンピュータをグループ化することにより、各コンピュータの上記基準位置をグループごとにまとめて二次元平面内に配置するものであることを特徴とする請求項1に記載の観測データ表示装置。

[3] 上記観測値が、観測対象であるコンピュータが送信元となった不正アクセスおよび受信先となった不正アクセス回数であり、

上記観測値プロット部が、送信元となった不正アクセスを示す棒グラフと受信先となった不正アクセス回数を示す棒グラフとを重ねて、上記基準位置にプロットするものであることを特徴とする請求項2に記載の観測データ表示装置。

[4] 不正アクセスの送信元となったコンピュータと当該不正アクセスの受信先となったコンピュータとの対応関係を示す線分を、両コンピュータのそれぞれの基準位置あるいは基準位置上の棒グラフを両端として表示する観測対象連結表示部をさらに備えることを特徴とする請求項3に記載の観測データ表示装置。

[5] 観測対象を観測して得られる観測値を表示する観測データ表示装置であって、

観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる

観測値との組を取得するデータ取得部と、

当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置部と、

上記観測値に応じた高さを観測値ごとに算出する高さ算出部と、

上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる3次元表示部と、を備えていることを特徴とする観測データ表示装置。

[6] 上記観測対象識別情報に基づいて観測対象を階層的なクラスターに分類する観測対象分類部をさらに備え、

上記基準位置配置部が、観測対象の観測値を表示するための上記基準位置を、上記階層的なクラスターに基づいて、二次元平面における入れ子状の構造となるように配置することを特徴とする請求項5に記載の観測データ表示装置。

[7] 上記基準位置配置部は、同一のクラスターに分類される観測対象の基準位置が一塊になるように、基準位置を配置することを特徴とする請求項6に記載の観測データ表示装置。

[8] 上記観測対象はコンピュータネットワークに接続されたコンピュータであり、

上記観測対象識別情報は、上記コンピュータに割り当てられた上記コンピュータネットワークにおける階層構造を有するアドレス情報であることを特徴とする請求項5から7の何れか1項に記載の観測データ表示装置。

[9] 上記観測値は、不正アクセスを試みた件数、不正アクセスを試みられた件数の一方または両方であることを特徴とする請求項8に記載の観測データ表示装置。

[10] 不正アクセスの試みたコンピュータと不正アクセスを試みられたコンピュータとの対応関係を示す線分を、両コンピュータのそれぞれの基準位置あるいは基準位置上の棒グラフを両端として表示装置に表示させる観測対象連結表示部をさらに備えていることを特徴とする請求項9に記載の観測データ表示装置。

[11] 画像データを格納する記憶部と、

3次元表示部によって表示装置に表示させる画像の画像データを、上記記憶部に格納する観測結果保存部とをさらに備えていることを特徴とする請求項5から10に記

載の観測データ表示装置。

[12] 上記観測値は、不正アクセスを試みた件数、不正アクセスを試みられた件数の一方または両方であり、

上記データ取得部は、所定時間ごとの上記観測値を抽出するものであり、

上記観測結果保存部は、上記所定時間ごとの観測値について作成された画像の画像データを、上記記憶部に格納することを特徴とする請求項11に記載の観測データ表示装置。

[13] 観測対象を観測した観測値を表示する観測データ表示装置による観測データ表示方法であって、

観測対象を特定するための観測対象識別情報と該観測対象を観測した観測値との組を取得するデータ取得ステップと、

上記観測対象識別情報に基づいて当該観測対象の観測値を表示するための基準位置を二次元平面内に配置する基準位置配置ステップと、

観測対象の観測値を、上記基準位置配置ステップによって配置された基準位置からの高さとしてプロットする観測値プロットステップと、

上記観測値プロット部によって生成されたデータに基づいて観測値を表示装置に3次元表示する3次元表示ステップと、を含むことを特徴とする観測データ表示方法。

[14] 観測対象を観測して得られる観測値を表示する観測データ表示方法であって、

観測対象を特定するための観測対象識別情報と当該観測対象を観測して得られる観測値との組を取得するデータ取得ステップと、

当該観測対象の観測値を表示するための基準位置を、上記観測対象識別情報に基づいて二次元平面内に配置する基準位置配置ステップと、

上記観測値に応じた高さを観測値ごとに算出する高さ算出ステップと

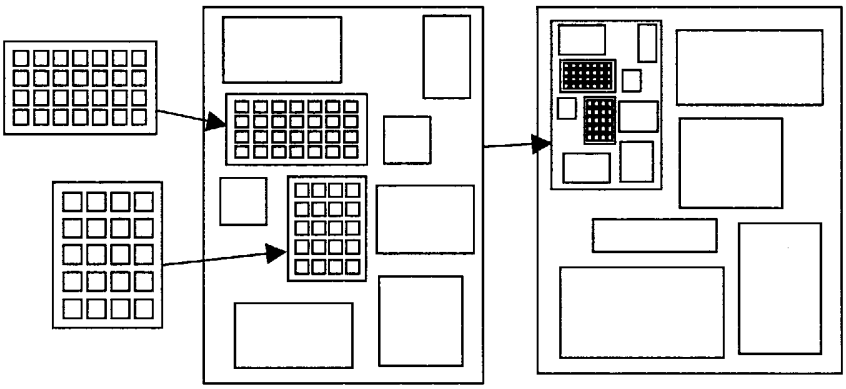
上記観測値が、上記基準位置配置部によって配置された基準位置において、上記高さ算出部によって算出された高さによって表現された画像を、表示装置に表示させる3次元表示ステップと、を含んでいることを特徴とする観測データ表示方法。

[15] 請求項1から12のいずれか1項に記載の観測データ表示装置を動作させる観測データ表示プログラムであって、コンピュータを上記の各部として機能させるための観測

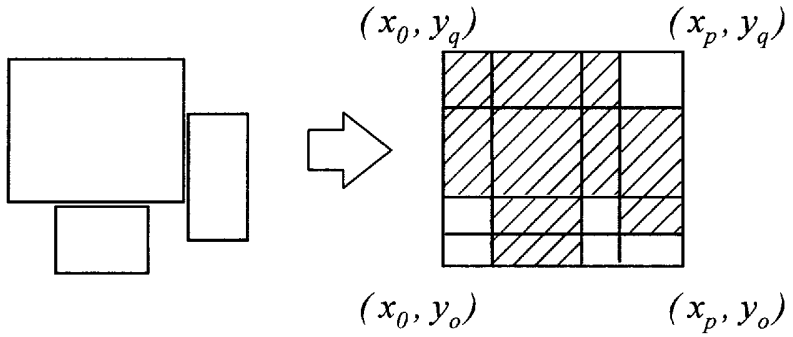
データ表示プログラム。

[16] 請求項15に記載の観測データ表示プログラムを記録したコンピュータ読み取り可能な記録媒体。

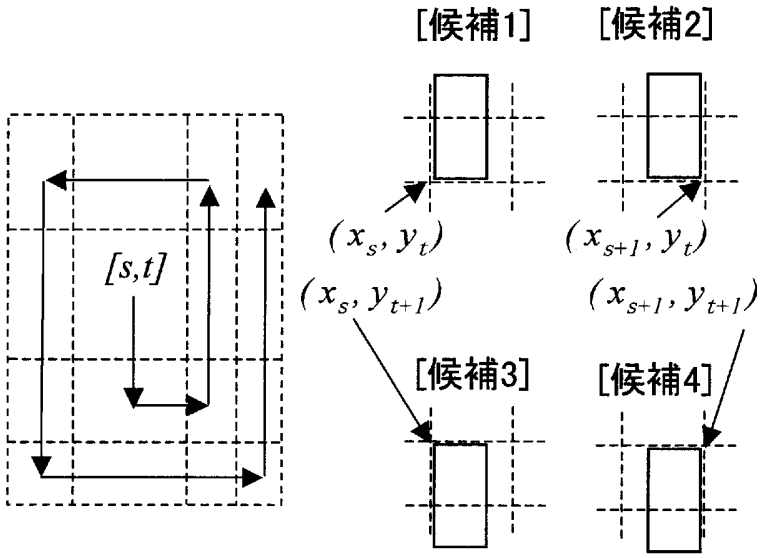
[図1]



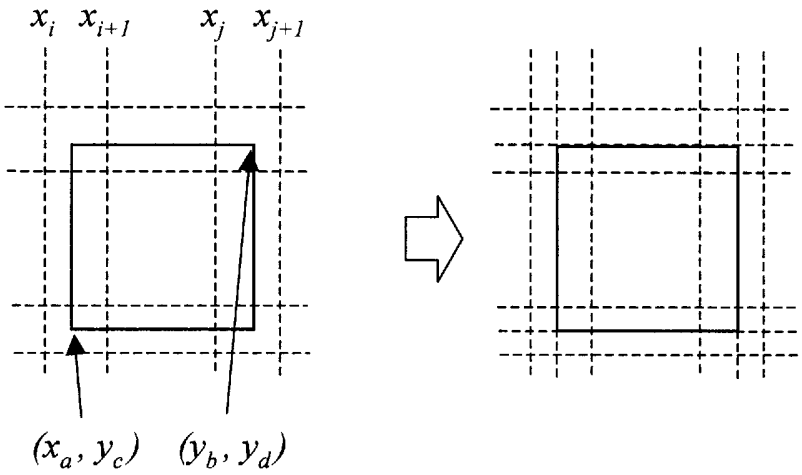
[図2]


(x_0, y_q)
(x_p, y_q)
(x_0, y_o)
(x_p, y_o)

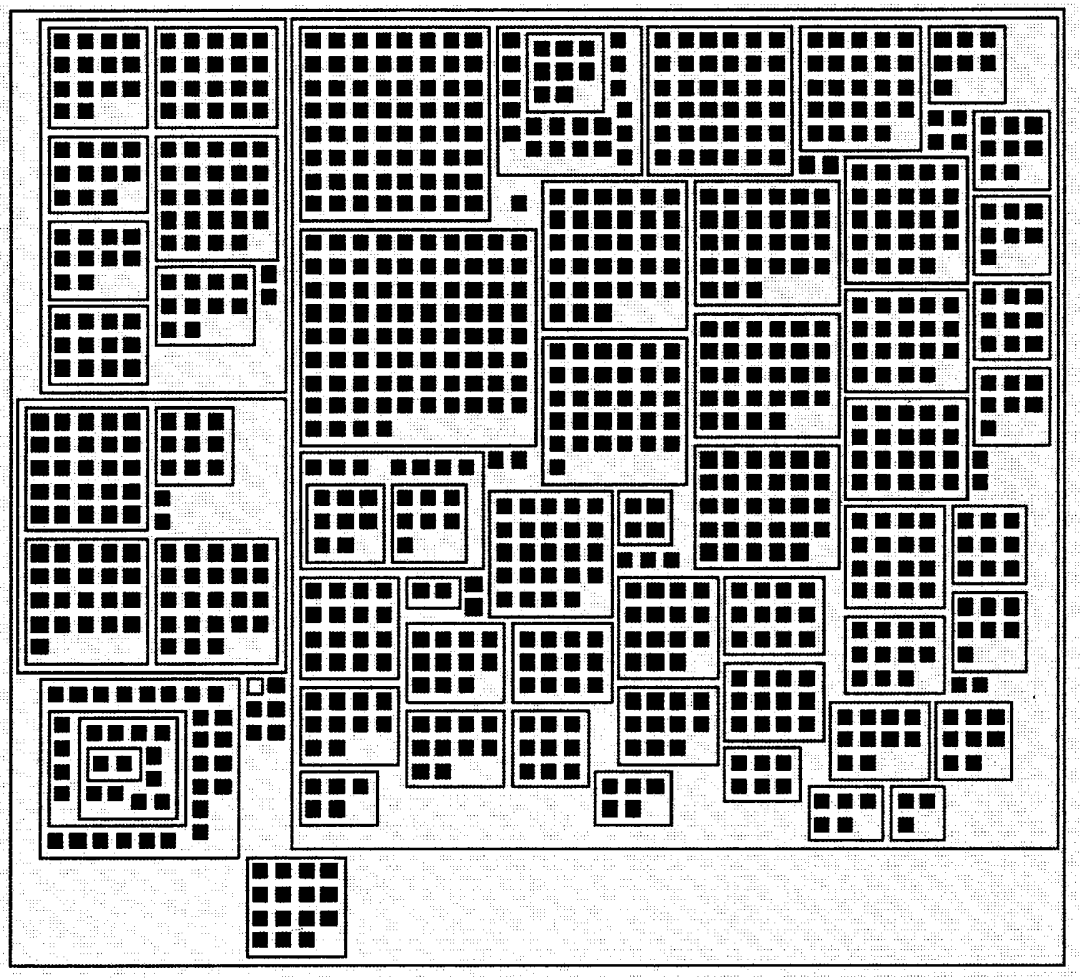
[図3]


[候補1]
[候補2]
[s,t]
(x_s, y_t)
(x_{s+1}, y_t)
(x_s, y_{t+1})
(x_{s+1}, y_{t+1})
[候補3]
[候補4]

[図4]



[図5]



[図6]

0) 長方形を1個ずつ選択し、以下の処理を適用する。

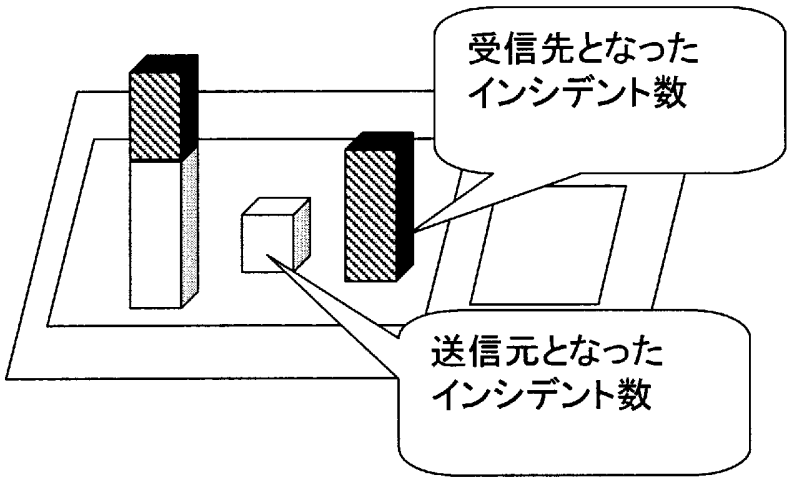
1) 画面中心に位置する格子領域から順番に、渦巻状に1個ずつ格子領域を探索する。

2) 格子領域内部に4通りの候補位置を算出し、各々の候補位置について、(2-1)～(2-4)の処理を適用する。すべての候補位置について処理が終わったら1) に戻って他の格子領域を探索する。

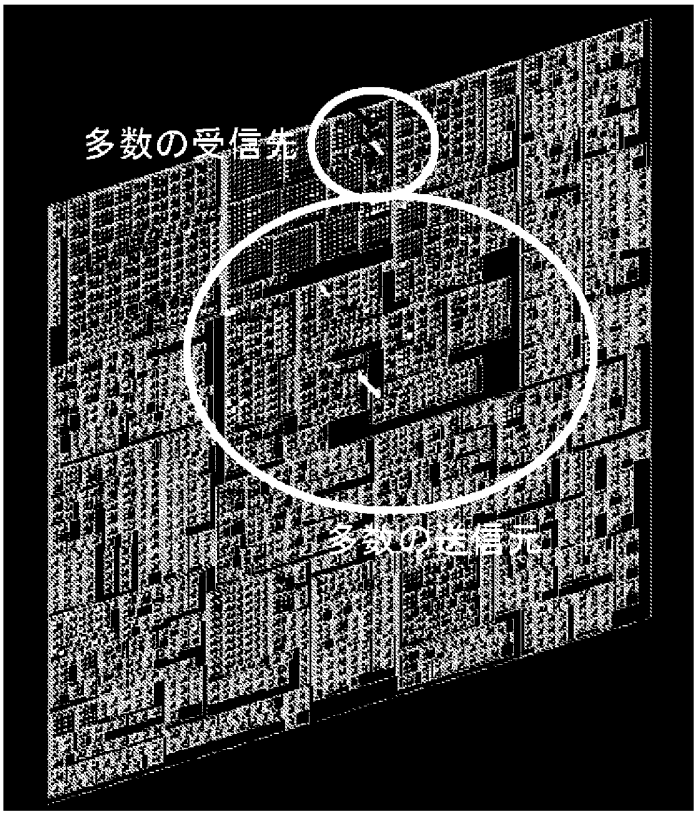
(2-1) 長方形を試しに候補位置に配置し、すでに配置されている長方形との干渉を判定する。
(2-2) 長方形の干渉があるならば、2)に戻って他の候補位置を算出する。
(2-3) 長方形の干渉がなく、しかもその配置によって配置面積の拡大を生じないならば、格子領域の探索を中断して、配置を決定し、3)に進む。
(2-4) 長方形の干渉がなく、配置によって生じる配置面積の拡大が過去最小ならば、その位置を「仮の位置」として、拡大量とともに記録する。

3) (2-3)から進んできたときはその位置に、さもなければ「仮の位置」に、長方形を配置し、格子分割を更新する。
0) に戻って、次の長方形について処理を進める。

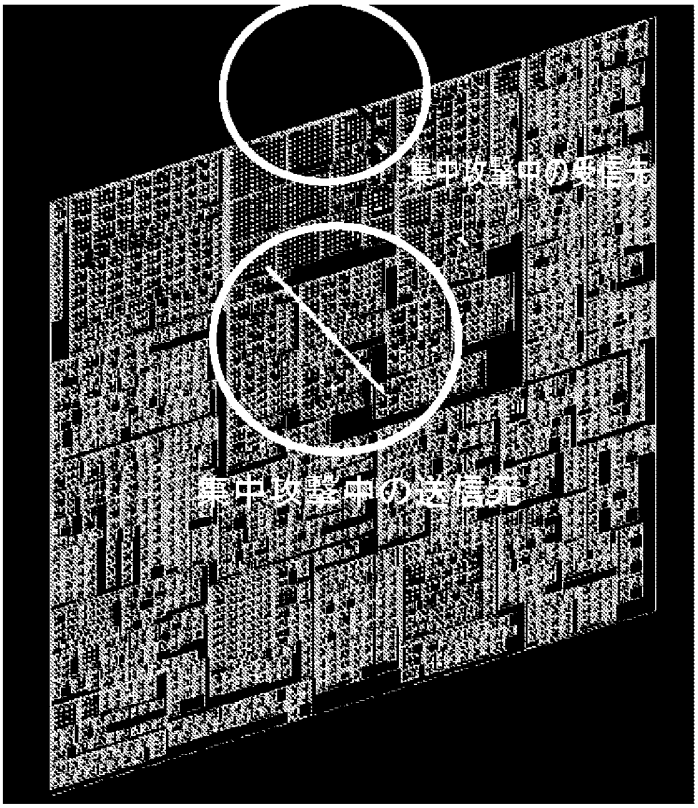
[図7]



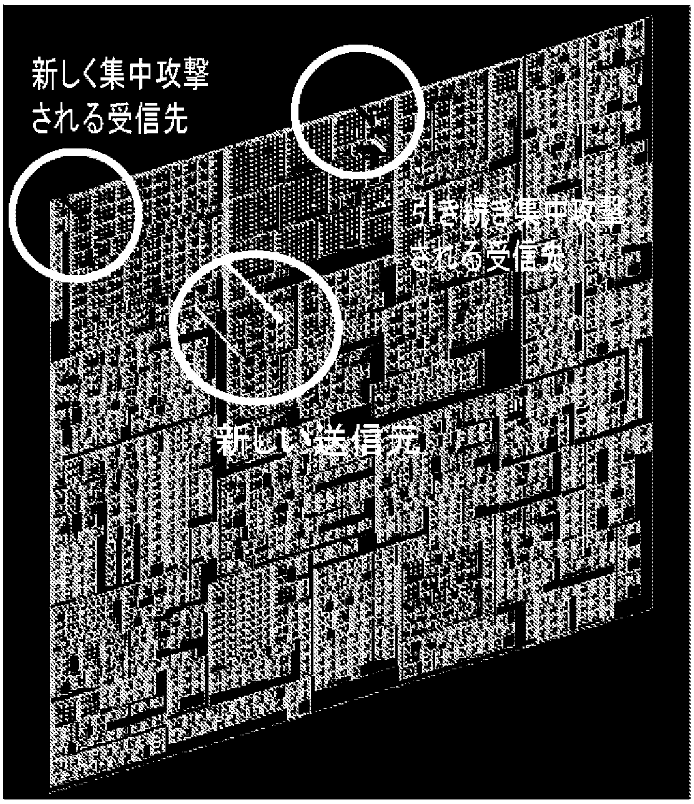
[図8]



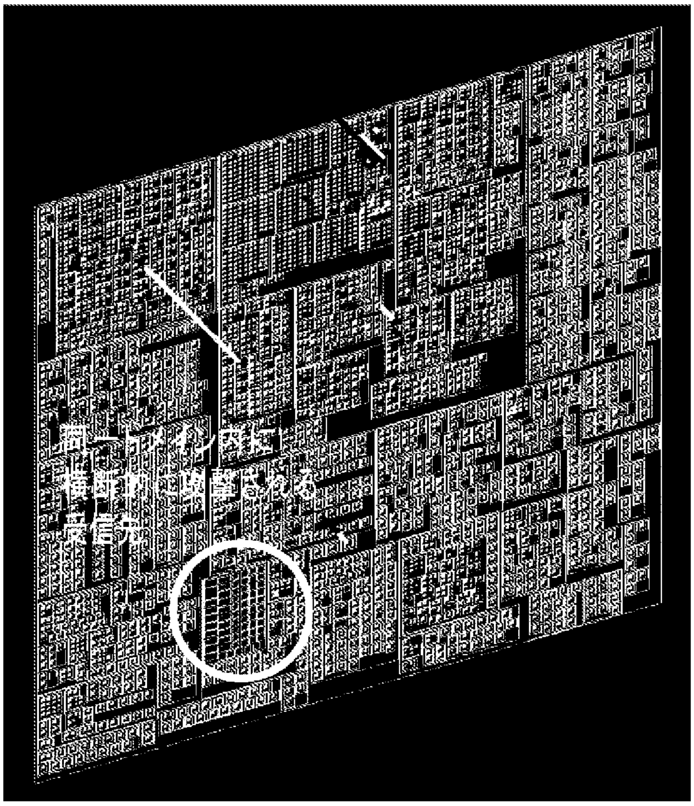
[図9]



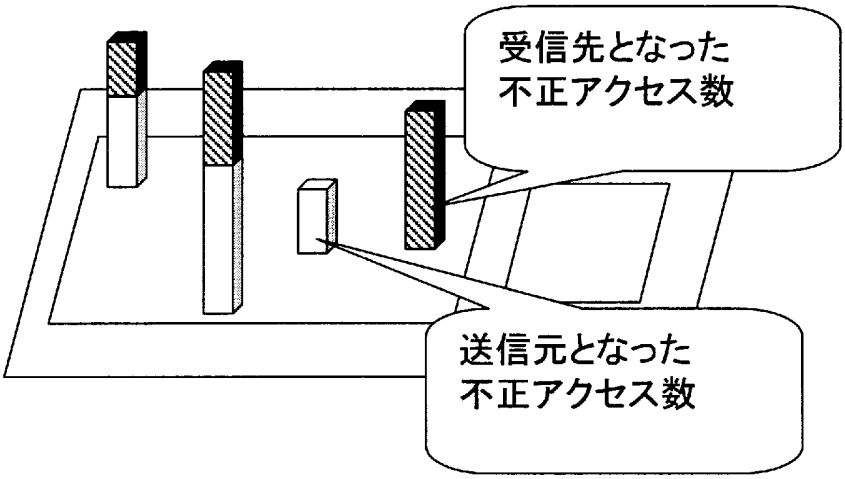
［図10］



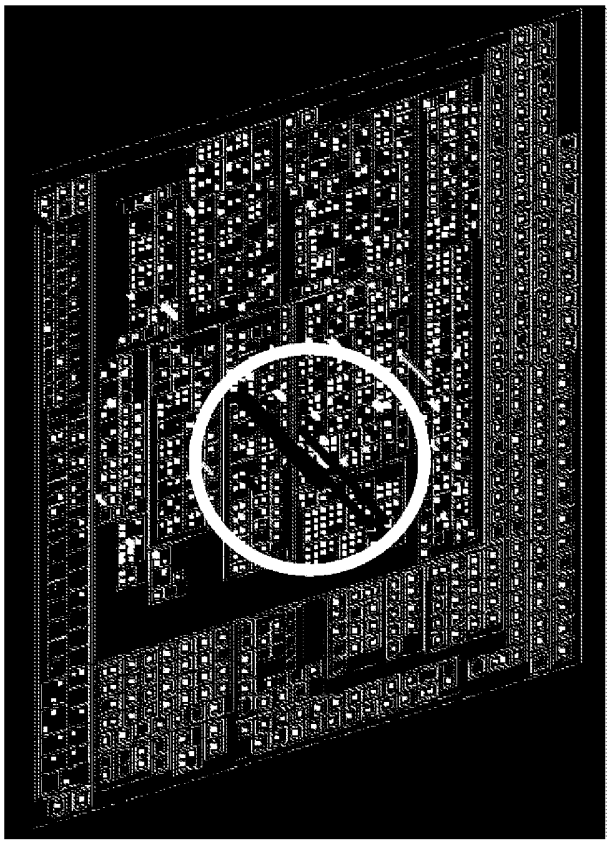
［図11］



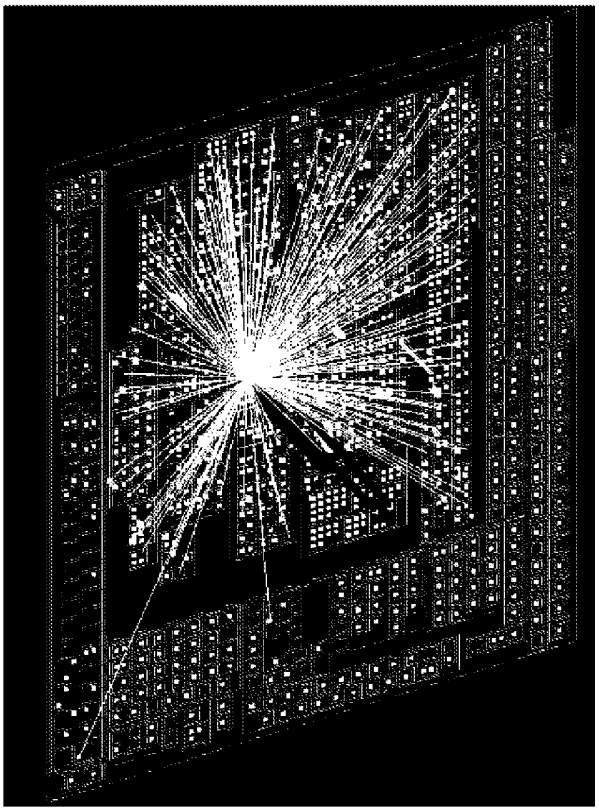
[図12]



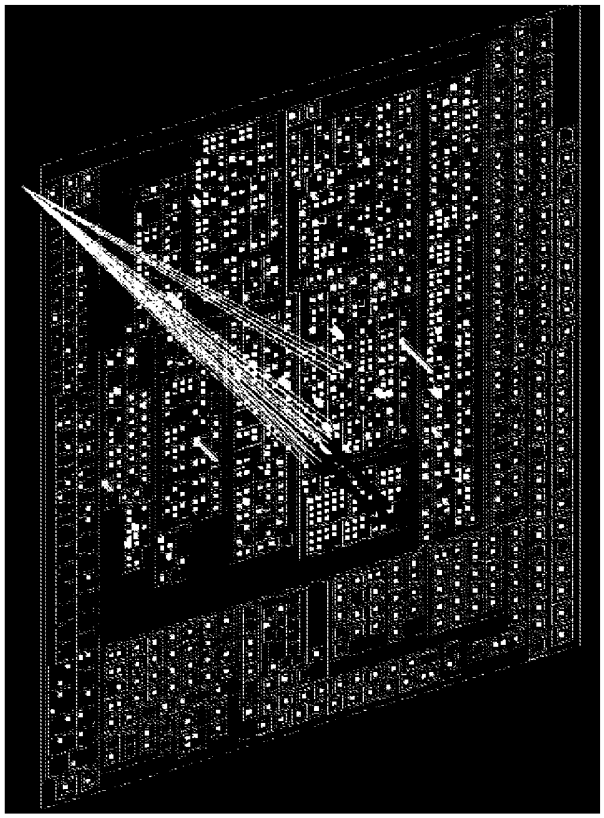
[図13]



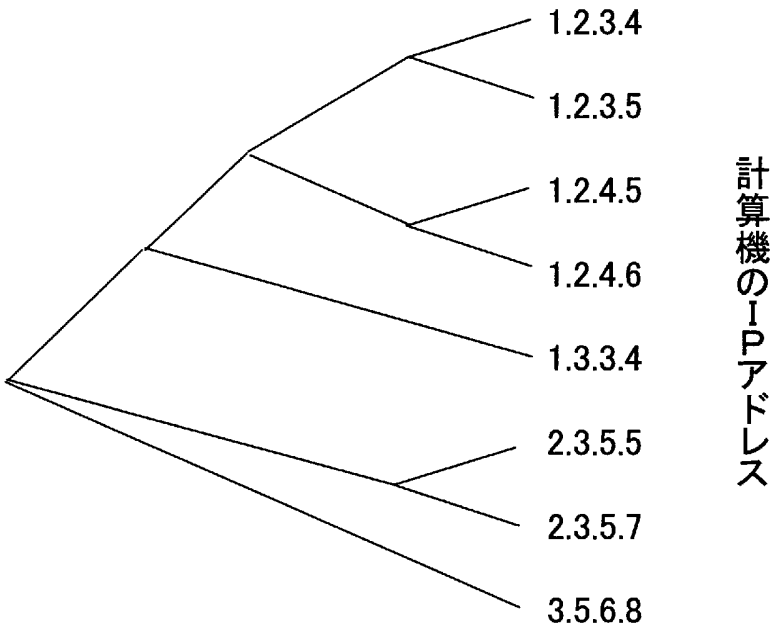
[図14]



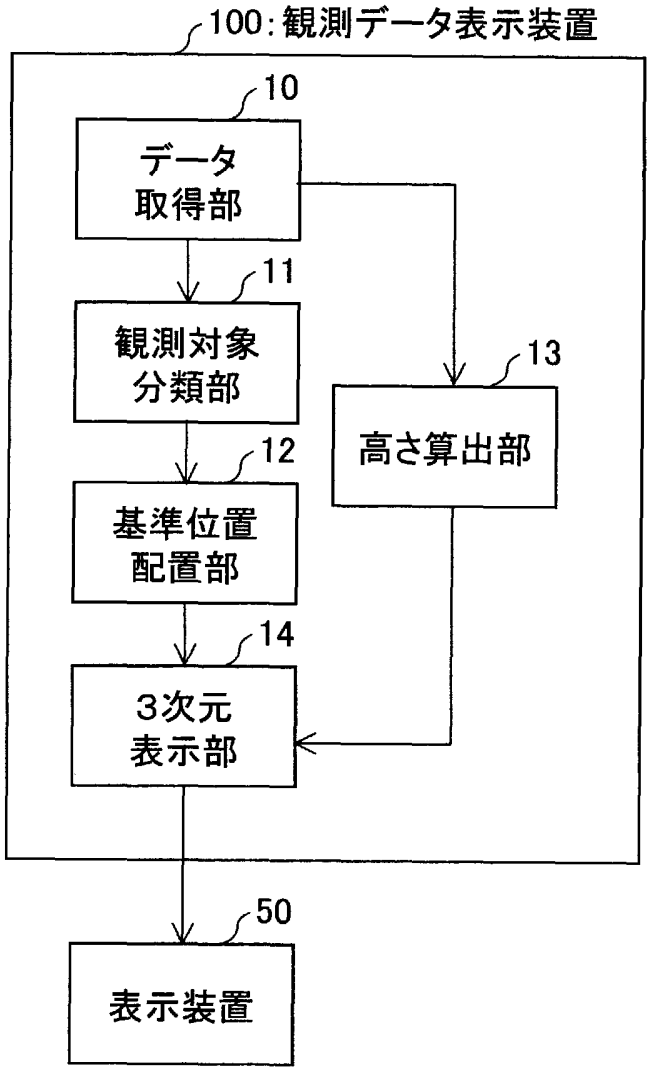
[図15]



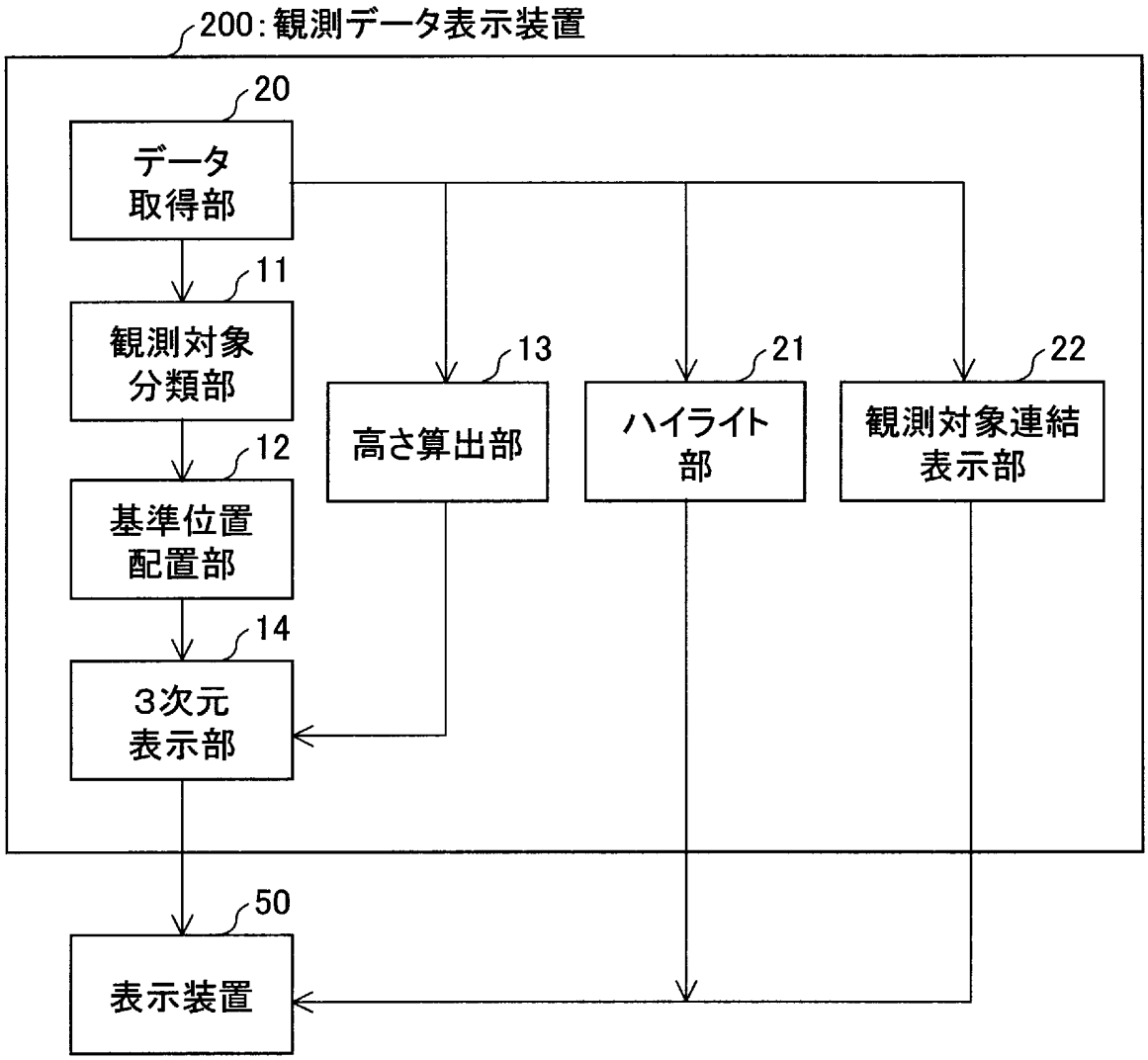
[図16]



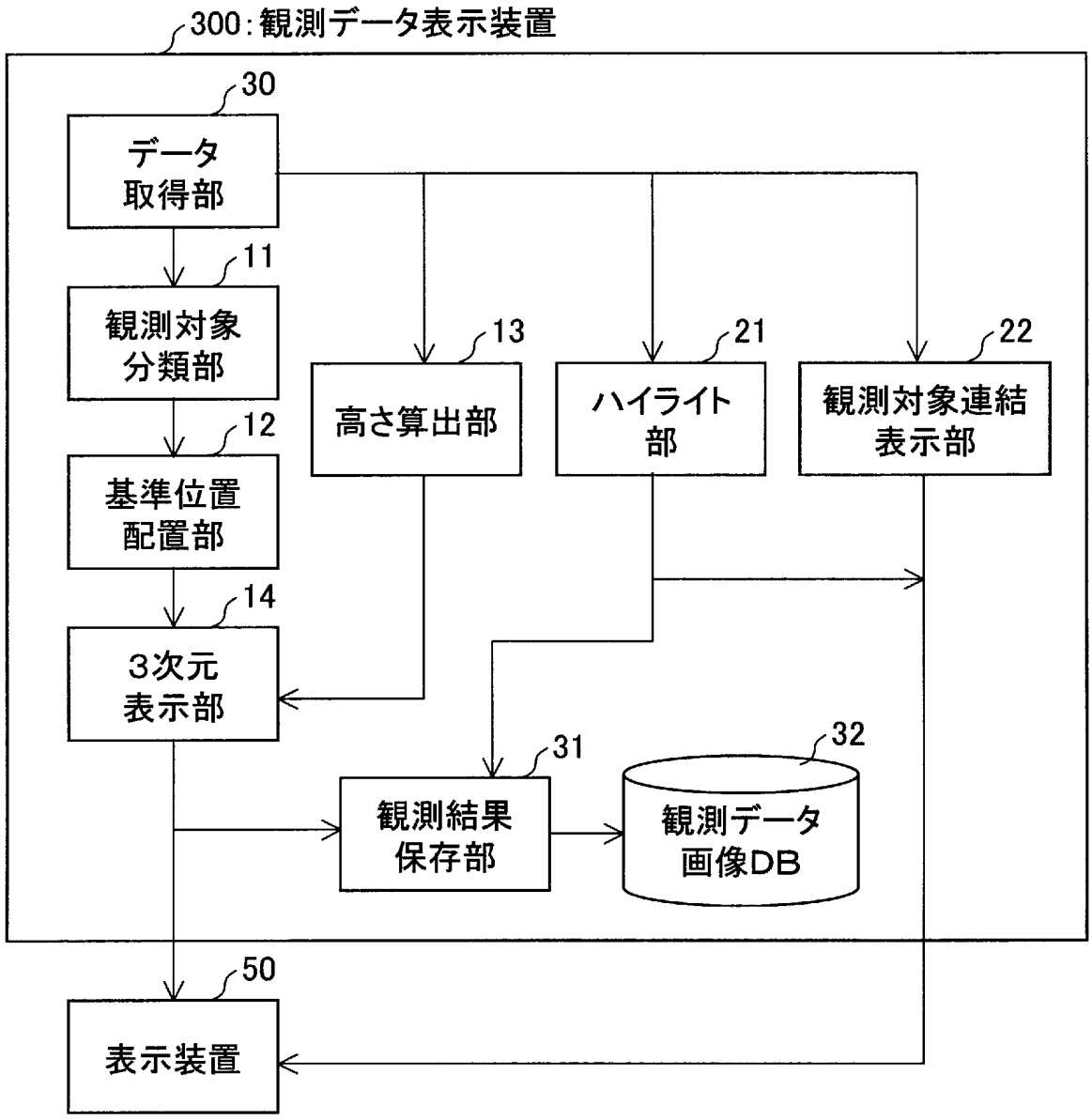
[図17]


100:観測データ表示装置
10
データ
取得部
11
観測対象
分類部
12
基準位置
配置部
13
高さ算出部
14
3次元
表示部
50
表示装置

[図18]


200:観測データ表示装置
20
データ取得部
11
観測対象分類部
12
基準位置配置部
14
3次元表示部
13
高さ算出部
21
ハイライト部
22
観測対象連結表示部
50
表示装置

[図19]


300:観測データ表示装置
30
データ取得部
11
観測対象分類部
12
基準位置配置部
14
3次元表示部
13
高さ算出部
21
ハイライト部
22
観測対象連結表示部
31
観測結果保存部
32
観測データ画像DB
50
表示装置

KJ0528

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

VIII-5-1	不利にならない開示又は新規性喪失の例外に関する申立て 不利にならない開示又は新規性喪失の例外に関する申立て（規則4.17(v)及び51の2.1(a)(v)） 氏名（姓名）	本国際出願 に関し、 国立大学法人京都大学　Ｋｙｏｔｏ　Ｕｎｉｖｅｒｓｉｔｙ は、本国際出願の請求項に記載された対象が以下のように開示されたことを申し立てる。
VIII-5-1(i)	開示の種類:	刊行物
VIII-5-1(ii)	開示の日付:	2004年 07月 01日 (01.07.2004)
VIII-5-1(iii)	開示の名称:	「平安京ビューによるＩＤＳデータの視覚化」（可視化情報　２００４　Ｖｏｌ．２４　Ｓｕｐｐｌ．　Ｎｏ．１　第３２回可視化情報シンポジウム講演論文集　４５９～４６２頁）
VIII-5-1(iv)	開示の場所:	
VIII-5-1(i)	開示の種類:	その他 ＣＤ-ＲＯＭ
VIII-5-1(ii)	開示の日付:	2004年 10月 08日 (08.10.2004)
VIII-5-1(iii)	開示の名称:	「平安京ビューによるＩＤＳデータの視覚化　～第２報」　（第１０回ビジュアリゼーションカンファレンス-新しい社会を創るビジュアリゼーション-　予稿集ＣＤ-ＲＯＭ（可視化情報　Ｖｏｌ．２４，Ｓｕｐｐｌ．　Ｎｏ．３，　ＩＳＳＮ　０９１６-４７３１）　ＶＣ１０-５）
VIII-5-1(iv)	開示の場所:	
VIII-5-1(i)	開示の種類:	刊行物
VIII-5-1(ii)	開示の日付:	2004年 12月 09日 (09.12.2004)
VIII-5-1(iii)	開示の名称:	「ネットワーク不正侵入監視のための視覚化の一手法」（分散システム／インターネット運用技術シンポジウム２００４年度　論文集　６３～６８頁）
VIII-5-1(iv)	開示の場所:	
VIII-5-1(v)	本申立ては、次の指定国のためになされたものである。:	すべての指定国

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/011997

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, 3/00, 11/32, 13/00, G06T17/40, H04L12/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, 3/00, 11/32, 13/00, G06T17/40, H04L12/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	Takayuki ITO et al., "'Data Hosekibako' -Visual Data Mining no Jitsugen ni Mukete", Information Processing Society of Japan Kenkyu Hokoku, 23 May, 2003 (23.05.03), Vol.2003, No.51, pages 113 to 118	1,5-9,11-16 2-4,10
A	WO 2000/005651 A1 (RAYTHEON CO.), 03 February, 2000 (03.02.00), Full text; all drawings & US 6269447 B1 & EP 1097420 A & JP 2002-521748 A	1-16
A	JP 2004-318552 A (KDDI Corp.), 11 November, 2004 (11.11.04), Full text; all drawings (Family: none)	1-16

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 September, 2005 (08.09.05)	27 September, 2005 (27.09.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/011997

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-336130 A (NTT Data Corp.), 25 November, 2004 (25.11.04), Full text; all drawings (Family: none)	1-16
A	JP 2004-38940 A (Shia Insaito Sekyuriti Kabushiki Kaisha), 05 February, 2004 (05.02.04), Full text; all drawings & US 2003/0200308 A1	1-16

国際調査報告

国際出願番号 PCT／JP2005／011997

A． 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] G06F15/00, 3/00, 11/32, 13/00, G06T17/40, H04L12/20

B． 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] G06F15/00, 3/00, 11/32, 13/00, G06T17/40, H04L12/20

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	伊藤貴之他,「データ宝石箱」～ビジュアルデータマイニングの実現に向けて,情報処理学会研究報告, 2003.05.23,第2003巻, 第51号, p.113-p.118	1,5-9,11-16
A		2-4,10
A	WO 2000/005651 A1(RAYTHEON COMPANY) 2000.02.03,全文,全図 & US 6269447 B1 & EP 1097420 A & JP 2002-521748 A	1-16
A	JP 2004-318552 A(KDDI株式会社) 2004.11.11,全文,全図 (ファミリーなし)	1-16

☑ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 08．09．2005	国際調査報告の発送日 27.9.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5S 9555 宮司 卓佳 電話番号 03－3581－1101 内線 3546

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2004-336130 A(株式会社エヌ・ティ・ティ・データ) 2004.11.25,全文,全図（ファミリーなし)	1-16
A	JP 2004-38940 A(シーア・インサイト・セキュリティ株式会社) 2004.02.05,全文,全図 & US 2003/0200308 A1	1-16