(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4825979号
(P4825979)
(45)発行日　平成23年11月30日(2011.11.30)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.　　F I
H04L 12/56 (2006.01)　　H04L 12/56　400Z
G06F 21/20 (2006.01)　　G06F 15/00　330A

請求項の数 9　(全 14 頁)

(21)出願番号　特願2007-24080(P2007-24080)
(22)出願日　平成19年2月2日(2007.2.2)
(65)公開番号　特開2008-193302(P2008-193302A)
(43)公開日　平成20年8月21日(2008.8.21)
審査請求日　平成22年1月28日(2010.1.28)

特許法第３０条第１項適用　２００６年１０月２５日
社団法人情報処理学会発行の「コンピュータセキュリティシンポジウム２００６　論文集」に発表

(73)特許権者　504133110
国立大学法人電気通信大学
東京都調布市調布ヶ丘一丁目５番地１
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100120455
弁理士　勝　治人
(72)発明者　小池　英樹
東京都調布市調布ヶ丘１丁目５番地１　国立大学法人　電気通信大学内
(72)発明者　向坂　真一
東京都調布市調布ヶ丘１丁目５番地１　国立大学法人　電気通信大学内
最終頁に続く

(54)【発明の名称】通信ログ視覚化装置、通信ログ視覚化方法及び通信ログ視覚化プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力する通信ログ入力手段と、
前記通信ログ入力手段から前記通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出する通信ログ解析手段と、
前記通信ログ解析手段が抽出した前記論理情報を入力して管理する論理情報管理手段と、
前記通信ログ解析手段が抽出した前記時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として前記論理情報と対応付けて管理する時間情報管理手段と、
前記論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段と、
表示に必要な論理情報、時間情報および位置情報を前記論理情報管理手段、前記時間情報管理手段および前記位置情報管理手段からそれぞれ読み出す情報取得手段と、
前記情報取得手段が読み出した前記論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、前記情報取得手段が読み出した前記時間情報を前記軸のいずれかと平行で前記第１平面と交差する第２平面に配置し、前記情報取得手段が読み出した前記位置情報を前記第１平面及び前記第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、前記第２平面には、前記第１平面と前記第２平面とが交差する線上

に表示される論理情報に対応した時間情報を表示する表示手段と、
を特徴とする通信ログ視覚化装置。
【請求項２】
前記第２平面は、前記第１平面に対して平行に移動可能であることを特徴とする請求項１記載の通信ログ視覚化装置。
【請求項３】
前記論理情報はポート番号を含むものであって、
前記表示手段は、ポート番号と当該ポート番号に対応する前記時間情報を表示することを特徴とする請求項１又は２に記載の通信ログ視覚化装置。
【請求項４】
通信ログ入力手段による、ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力するステップと、
通信ログ解析手段による、前記通信ログを入力するステップにおいて入力した前記通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出するステップと、
論理情報管理手段による、前記抽出するステップにおいて抽出した前記論理情報を入力して管理するステップと、
時間情報管理手段による、前記抽出するステップにおいて抽出した前記時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として前記論理情報と対応付けて管理するステップと、
情報取得手段による、表示に必要な論理情報、時間情報を前記論理情報管理手段、前記時間情報管理手段からそれぞれ読み出すとともに、前記論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段から前記位置情報を読み出すステップと、
表示手段による、前記情報取得手段が読み出した前記論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、前記情報取得手段が読み出した前記時間情報を前記軸のいずれかと平行で前記第１平面と交差する第２平面に配置し、前記情報取得手段が読み出した前記位置情報を前記第１平面及び前記第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、前記第２平面には、前記第１平面と前記第２平面とが交差する線上に表示される論理情報に対応した時間情報を表示するステップと、
を有することを特徴とする通信ログ視覚化方法。
【請求項５】
前記第２平面は、前記第１平面に対して平行に移動可能であることを特徴とする請求項４記載の通信ログ視覚化方法。
【請求項６】
前記論理情報はポート番号を含むものであって、前記表示するステップは、ポート番号と当該ポート番号に対応する前記時間情報を表示することを特徴とする請求項４又は５に記載の通信ログ視覚化方法。
【請求項７】
通信ログ入力手段による、ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力するステップと、
通信ログ解析手段による、前記通信ログを入力するステップにおいて入力した前記通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出するステップと、
論理情報管理手段による、前記抽出するステップにおいて抽出した前記論理情報を入力して管理するステップと、
時間情報管理手段による、前記抽出するステップにおいて抽出した前記時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として前記論理情報と対応付けて管理するステップと、

情報取得手段による、表示に必要な論理情報、時間情報を前記論理情報管理手段、前記時間情報管理手段からそれぞれ読み出すとともに、前記論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段から前記位置情報を読み出すステップと、

表示手段による、前記情報取得手段が読み出した前記論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、前記情報取得手段が読み出した前記時間情報を前記軸のいずれかと平行で前記第１平面と交差する第２平面に配置し、前記情報取得手段が読み出した前記位置情報を前記第１平面及び前記第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、前記第２平面には、前記第１平面と前記第２平面とが交差する線上に表示される論理情報に対応した時間情報を表示するステップと、

をコンピュータに実行させることを特徴とする通信ログ視覚化プログラム。

【請求項８】

前記第２平面は、前記第１平面に対して平行に移動可能であることを特徴とする請求項７記載の通信ログ視覚化プログラム。

【請求項９】

前記論理情報はポート番号を含むものであって、前記表示するステップは、ポート番号と当該ポート番号に対応する前記時間情報を表示することを特徴とする請求項７又は８に記載の通信ログ視覚化プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク監視して得られる通信ログを表示する技術に関する。

【背景技術】

【０００２】

近年、ネットワークセキュリティ監視の重要性が増している。一般にネットワーク監視装置が出力するログは非常に膨大で、監視者が手作業により解析するのは困難である。

【０００３】

これに対し、ログを視覚化表示することで監視者の負担を軽減するシステムが提案されている。例えば、広域ネットワークにおける通信のトレンド（流行しているウィルスの種類など）を分析するものとして非特許文献１に記載の技術が知られている。

【非特許文献１】Y.Hideshima、H.Koike、"Starmine : A visualization system for cyber attacks"、Asia Pacific Symposium on Information Visualisation、２００６年、p. 131-138

【発明の開示】

【発明が解決しようとする課題】

【０００４】

ところが、内部ネットワークの監視は、広域ネットワーク監視や通信機器毎の監視とは異なる側面を有している。内部ネットワークの監視においては、計算機に対して不正アクセスが発生した場合、その計算機の設置場所に直接赴き、計算機の停止、ネットワークから物理的に切断するなど、素早く対応することが重要である。

【０００５】

しかしながら、従来のセキュリティログの視覚化システムは、通信量の時系列の変化を示す時間情報のみを表示するもの、あるいは、ＩＰアドレスなどの論理情報のみを表示するものが多く、これらの情報だけでは、不正アクセスが発生している計算機がどの場所に設置してあるものなのか瞬時には判断できないという問題がある。

【０００６】

また、非特許文献１に示す技術は、広域ネットワークを監視するためのものであり、攻撃を受けている通信機器の具体的な設置場所まで特定することはできないので、内部ネットワークの監視に用いることはできない。

【０００７】
本発明は、上記に鑑みてなされたものであり、その課題とするところは、内部ネットワークの監視に際して、不審な通信を行っている通信機器の設置位置を知ることができるようにすることにある。
【課題を解決するための手段】
【０００８】
第１の本発明に係る通信ログ視覚化装置は、ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力する通信ログ入力手段と、通信ログ入力手段から通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出する通信ログ解析手段と、通信ログ解析手段が抽出した論理情報を入力して管理する論理情報管理手段と、通信ログ解析手段が抽出した時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として論理情報と対応付けて管理する時間情報管理手段と、論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段と、表示に必要な論理情報、時間情報および位置情報を論理情報管理手段、時間情報管理手段および位置情報管理手段からそれぞれ読み出す情報取得手段と、情報取得手段が読み出した論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、情報取得手段が読み出した時間情報を軸のいずれかと平行で第１平面と交差する第２平面に配置し、情報取得手段が読み出した位置情報を第１平面及び第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、第２平面には、第１平面と第２平面とが交差する線上に表示される論理情報に対応した時間情報を表示する表示手段と、を特徴とする。
【０００９】
本発明にあっては、ネットワークを監視する監視システムが出力する通信ログを入力し、ＩＰアドレスなどの論理情報と、パケットを捕捉した時間などの時間に関する情報とを抽出する通信ログ解析手段と、論理情報を管理する論理情報管理手段と、抽出した時間に関する情報に基づいて所定の期間毎の通信量を集計し、時間情報として論理情報と対応付けて管理する時間情報管理手段と、通信機器の配置場所を特定する位置情報をその通信機器を示す論理情報と対応付けて管理する時間情報管理手段と、論理情報、時間情報および位置情報のそれぞれの情報を読み出して、論理情報と時間情報とを関連付けて表示するとともに、論理情報と位置情報とを関連付けて表示する表示手段とを有することにより、不正侵入の形跡が見られる時間情報に対応した論理情報に該当する通信機器の配置場所を素早く特定することができるので、不正侵入に対する対策を迅速に行うことを可能とする。
【００１１】
本発明にあっては、各情報を仮想３次元空間上に配置することによって、すべての情報を瞬時に確認し判断することができるとともに、視点を変えて表示することができるので、注目したい情報をより鮮明に表示することを可能とする。
【００１２】
上記通信ログ視覚化装置において、第２平面は、第１平面に対して平行に移動可能であることを特徴とする。
【００１３】
本発明にあっては、時間情報を表示する面を論理情報を表示する面に対して平行に移動可能にすることにより、表示する論理情報の変更を素早く行うことを可能とする。
【００１４】
上記通信ログ視覚化装置において、論理情報はポート番号を含むものであって、表示手段は、ポート番号と当該ポート番号に対応する時間情報を表示することを特徴とする。
【００１５】
本発明にあっては、ポート番号とそのポート番号に対応する時間情報を表示することにより、不正侵入の対象や種類を知ることができる。
【００１６】

第２の本発明に係る通信ログ視覚化方法は、通信ログ入力手段による、ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力するステップと、通信ログ解析手段による、通信ログを入力するステップにおいて入力した通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出するステップと、論理情報管理手段による、抽出するステップにおいて抽出した論理情報を入力して管理するステップと、時間情報管理手段による、抽出するステップにおいて抽出した時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として論理情報と対応付けて管理するステップと、情報取得手段による、表示に必要な論理情報、時間情報を論理情報管理手段、時間情報管理手段からそれぞれ読み出すとともに、論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段から位置情報を読み出すステップと、表示手段による、情報取得手段が読み出した論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、情報取得手段が読み出した時間情報を軸のいずれかと平行で第１平面と交差する第２平面に配置し、情報取得手段が読み出した位置情報を第１平面及び第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、第２平面には、第１平面と第２平面とが交差する線上に表示される論理情報に対応した時間情報を表示するステップと、を有することを特徴とする。

【００１８】

上記通信ログ視覚化方法において、第２平面は、第１平面に対して平行に移動可能であることを特徴とする。

【００１９】

上記通信ログ視覚化方法において、論理情報はポート番号を含むものであって、表示するステップは、ポート番号と当該ポート番号に対応する時間情報を表示することを特徴とする。

【００２０】

第３の本発明に係る通信ログ視覚化プログラムは、通信ログ入力手段による、ネットワーク上を流れるパケットを検査して不正侵入の監視を行う監視システムが出力する通信ログを入力するステップと、通信ログ解析手段による、通信ログを入力するステップにおいて入力した通信ログを受信し、当該通信ログからＩＰアドレスを含む論理情報と時間に関する情報とを抽出するステップと、論理情報管理手段による、抽出するステップにおいて抽出した論理情報を入力して管理するステップと、時間情報管理手段による、抽出するステップにおいて抽出した時間に関する情報を入力し、所定の期間毎の通信量を集計して時間情報として論理情報と対応付けて管理するステップと、情報取得手段による、表示に必要な論理情報、時間情報を論理情報管理手段、時間情報管理手段からそれぞれ読み出すとともに、論理情報と当該論理情報に関連した通信機器の配置場所を特定する位置情報とを対応付けて管理する位置情報管理手段から位置情報を読み出すステップと、表示手段による、情報取得手段が読み出した論理情報を当該論理情報に含まれるＩＰアドレスの所定の部分の値を一方の軸、別の部分の値を他方の軸に対応させた仮想３次元空間上の第１平面に配置し、情報取得手段が読み出した時間情報を軸のいずれかと平行で第１平面と交差する第２平面に配置し、情報取得手段が読み出した位置情報を第１平面及び第２平面それぞれと交差する第３平面に配置して前記論理情報と関連付けて表示し、第２平面には、第１平面と第２平面とが交差する線上に表示される論理情報に対応した時間情報を表示するステップと、をコンピュータに実行させることを特徴とする。

【００２２】

上記通信ログ視覚化プログラムにおいて、第２平面は、第１平面に対して平行に移動可能であることを特徴とする。

【００２３】

上記通信ログ視覚化プログラムにおいて、論理情報はポート番号を含むものであって、表示するステップは、ポート番号と当該ポート番号に対応する時間情報を表示することを

特徴とする。

【発明の効果】

【００２４】

本発明によれば、内部ネットワークの監視に際して、不審な通信を行っている通信機器の設置位置を知ることができる。

【発明を実施するための最良の形態】

【００２５】

以下、本発明の実施の形態について図面を用いて説明する。

【００２６】

図１は、本実施の形態における通信ログ視覚化装置１０を用いた通信ログ視覚化システムの構成を示すブロック図である。同図に示すように、本通信ログ視覚化システムは、ログ解析部１１と視覚化処理部１２とを備えた通信ログ視覚化装置１０と、データベース２０と、入力装置３０と、ディスプレイ４０とを備えており、ネットワーク監視システム１１０、ネットワーク探査システム１２０が出力する各種ログを入力して、ネットワークの管理・監視に便利な形態で通信ログの情報を出力するものである。なお、通信ログ視覚化装置１０は、演算処理装置、記憶装置、メモリ等を備えたコンピュータにより構成できるものであり、各部の処理はプログラムによって実行される。このプログラムは通信ログ視覚化装置１０が備えた記憶装置などに記憶されており、記録媒体に記録することも、ネットワークを通して提供することも可能である。

【００２７】

まず、通信ログ視覚化装置１０のログ解析部１１について説明する。図１に示すように、ログ解析部１１は、通信ログ入力解析部１１１、探査ログ入力解析部１１２、時間情報管理部１１３、論理情報管理部１１４および位置情報管理部１１５を備えている。

【００２８】

通信ログ入力解析部１１１は、ネットワーク監視システム１１０が出力する通信ログを入力し、その通信ログからパケットを検査した時刻などを示す時間に関する情報と、ＩＰアドレス、ポート番号などの論理情報を抽出する。抽出した時間に関する情報に基づいて所定の期間毎の通信量を集計し、時間情報として論理情報と対応つけて時間情報管理部１１３に格納する。抽出した論理情報は、論理情報管理部１１４に格納する。なお、論理情報には、パケットの方向（アウトバウンド、インバウンド）や各種プロトコルに含まれるフラグなどのネットワーク監視に有効な情報を含んでも良い。また、通信ログは、ある程度の期間分をまとめて入力するものでもよいが、ネットワーク監視システム１１０が出力する度に随時入力することで不正侵入をより早く発見することができる。

【００２９】

ネットワーク監視システム１１０には、例えば、Proventia（登録商標）や snort などの侵入検知システム（ＩＤＳ：Intrusion Detection System）を用いる。侵入検知システムは、ネットワークを流れるパケットを検査して不正侵入を検知してネットワーク管理者に通知するものであり、パケットの補足時間、パケットの送信元、送信先など多数の情報を通信ログとして出力する。

【００３０】

探査ログ入力解析部１１２は、ネットワーク探査システム１２０が出力する探査ログを入力し、実際に稼働している通信機器のＩＰアドレス、ポート番号などの論理情報を抽出する。実際に稼働している通信機器が接続されているＩＰアドレス、空いているポートなどの論理情報は、論理情報管理部１１４に格納され、管理される。ネットワークに割り当てられたすべてのＩＰアドレスに通信機器が接続されていることは少なく、また、空いているポートから侵入されることが多いので、ネットワーク探査システム１２０を用いて稼働している通信機器、空いているポート、稼働しているサービスなどを調べる。これにより、無効なＩＰアドレスなどに対する攻撃に関する通信ログなどの不要なもののフィルタリングが可能になる。

【００３１】

ネットワーク探査システム１２０には、例えば、nmap などのポートスキャンツールを使用する。ポートスキャンツールは、ネットワークを通じてサーバなどの通信機器にアクセスし、セキュリティホールを探すツールである。ポートスキャンツールによって、通信機器のＯＳの種類や空いているポート番号、稼働するアプリケーションソフトの種類などを知ることができる。

【００３２】

データベース２０には、ＩＰアドレスとそのＩＰアドレスが割り当てられた通信機器の設置場所に関する位置情報とを対応付けて格納してあり、位置情報管理部１１５は、データベース２０を参照し、ＩＰアドレスなどの論理情報に対応した位置情報を取得する。なお、位置情報管理部１１５がデータベース２０を備えた構成であってもよい。

【００３３】

このように、ログ解析部１１は、ネットワーク監視システム１１０、ネットワーク探査システム１２０が出力した各種ログから時間情報、論理情報を抽出し、データベース２０から位置情報を取得する。なお、ネットワーク監視システム１１０は、ネットワークの監視が目的であるので、常時稼働しているが、ネットワーク探査システム１２０は、ネットワークの構成に変更があった時や、例えば、一週間に一回など、適宜稼働して論理情報を更新するもので良い。また、データベース２０に格納されているＩＰアドレスと位置との関連を示す情報も、ネットワークの構成に変更があった時などに更新するもので良い。

【００３４】

次に、通信ログ視覚化装置１０の視覚化処理部１２について説明する。図１に示すように、視覚化処理部１２は、データ取得部１２１および表示部１２２を備える構成であり、入力装置３０、ディスプレイ４０が接続されている。入力装置３０には、例えば、マウスなどのポインティングデバイスやキーボードが利用され、ＧＵＩ（Graphical User Interface）を介して直感的に操作をすることや、キーボードによりコマンドを直接して素早く操作することができる。以下、各部の処理について詳細に説明する。

【００３５】

データ取得部１２１は、表示する論理情報をログ解析部１１の論理情報管理部１１４から読み出し、読み出した論理情報に対応する時間情報を時間情報管理部１１３から読み出すとともに、読み出した論理情報に対応する位置情報を位置情報管理部１１５から読み出す。また、利用者は、入力装置３０を介して、表示したい論理情報をデータ取得部１２１に入力する。入力する論理情報としては、例えば、ＩＰアドレス、ネットワークアドレス、ポート番号、パケットの方向（アウトバウンド、インバウンド）などがある。このように、表示する情報を選別し、いらない情報をフィルタリングすることにより、注目したい情報を他の情報に埋もれさせることなく表示することができる。

【００３６】

表示部１２２は、データ取得部１２１が読み出した時間情報、論理情報および位置情報の関連が分かるように統合的に表示する。時間情報と論理情報とを関連付けて表示するとともに、論理情報と位置情報とを関連付けて表示することで、時間情報から得られた不正侵入の形跡からその時間情報に対応する通信機器のＩＰアドレスが分かり、そのＩＰアドレスから通信機器の位置情報を素早く知ることができる。また、利用者は、入力装置３０を介して、表示の形態を変更することが可能である。

【００３７】

次に、表示される画面について説明する。図２は、表示部１２２により出力される画面の構成を示す図である。同図に示すように、表示される画面は論理情報面２１０、時間情報面２２０および位置情報面２３０のそれぞれの面が垂直に交差するように仮想３次元空間上に配置され、画面右側には、ポートに関する情報を示すポート情報領域２１５が設けられている。なお、利用者は、接続された入力装置３０を用いて、時間情報面２２０などの情報面を正面から見るように視点を変更したり、各情報面を展開して表示するように指示することができる。以下、各情報面について詳細に説明する。

【００３８】

図３は、図２に示す論理情報面２１０を説明するための図である。論理情報面２１０では、IP Matrix を用いてＩＰアドレス空間を表現した。本実施の形態では、３２ビットで表現されるＩＰアドレスのうち下位１６ビットを用いて、縦軸に第３オクテット、横軸に第４オクテットをとり、実際に稼働している通信機器のＩＰアドレスを点で表現した。実際に稼働している通信機器のみを表示することにより、攻撃されやすい通信機器を注目して監視し、危険な状態にある通信機器の早期発見をすることが可能となる。また、ネットワーク探査システム１２０の探査ログから抽出した通信機器に使用されているＯＳの種類に応じて論理情報面２１０に描画される点の色を変えて表示した。外部からの攻撃は、特定のＯＳに対してのみ有効な攻撃が多いため、論理情報面２１０でＯＳの種類が判断できると、攻撃を受けている通信機器への対応が緊急に必要なものであるのか否かを素早く判断することができる。

【００３９】

図４（ａ）、（ｂ）は、ポート情報領域２１５を説明するための図である。図４（ａ）に示すポート情報領域２１５には、論理情報管理部１１４が管理する論理情報のうち、攻撃先ポートに関する情報を表示しており、縦軸にポート番号を示し、横軸には各ポートに対する攻撃量の対数を取ったものを示している。また、縦軸の下から２５％は、well known port と呼ばれる０番から１０２４番までのポートを示し、残りの７５％で６５５３５番までのポートを示している。well known port は、ウェブやメール、ＤＮＳ等の重要なサービスで用いられていることが多く、攻撃対象となりやすいことから、注意して監視すべきものであるので、他のポートよりも表示領域を多く取ることで、重要な情報を見落とさないようになっている。

【００４０】

図４（ｂ）は、ポート情報領域２１５をポインティングデバイスなどにより選択したときの様子を説明するための図である。ポート情報領域２１５を選択した場合には、図４（ｂ）の右側に示されるように、選択した部分の上下１％に該当する部分が２０％に拡大して表示されるので、ポートに関する情報をより詳しく得ることができる。なお、ポート情報領域２１５においてポートを指定することで、指定のポートに関連する情報のみを画面に表示することができるので、画面に表示される情報が厳選されるので、より容易に不正侵入の発見を行うことができる。

【００４１】

図５は、時間情報面２２０を説明するための図である。時間情報面２２０は、横軸に時間を示し、縦軸にネットワーク監視システム１１０が検知した所定の時間あたりの通信量（攻撃量）を示している。時間情報面２２０に表示される時系列グラフ２２３は、対応する論理情報に対する通信量を時系列でグラフ化して表示したものであり、符号２２２に示す位置を現在における通信量として、図上の左に向かって過去の通信量が示されている。本実施の形態においては、１時間ごとの通信量を算出して時系列グラフとして描画した。

【００４２】

同図に示すように、時間情報面２２０は、仮想３次元空間上で論理情報面２１０に対して垂直に配置し、論理情報面２１０と時間情報面２２０とが交差する線上に存在する論理情報に対する通信量が時系列グラフ２２３として表示される。時系列グラフ２２３は、符号２２２で示す現在の時刻と、ＩＰアドレスの第３オクテットの値で規定されるベースライン２２１との交点を原点として描画され、論理情報面２１０と時間情報面２２０とが交差する線上に存在する論理情報を示す点と直線で結ばれている。時間情報面２２０には、複数の時系列グラフ２２３が表示されるのでそれらを区別しやすくするために、各時系列グラフのベースライン２２１の位置に応じて異なる色を用いて描画する。

【００４３】

また、時間情報面２２０は、論理情報面２１０の横軸に対して平行にスライドさせることが可能であり、論理情報面２１０の横軸に設定した第４オクテット毎に個々のＩＰアドレスの時系列グラフを表示することが可能である。例えば、一般にルータの第４オクテットの値は、１または２５４であることが多いので、第４オクテットの値が１または２５４

になるように時間情報面２２０を設定することでルータに対する通信量をまとめて見ることができる。なお、第４オクテットの値が０になるように時間情報面２２０を設定した場合には、ＩＰアドレスの第３オクテットまでの値で指定されるサブネット毎の通信量の合計を表示するようになっている。

【００４４】

なお、論理情報面２１０の縦軸を第４オクテット、横軸を第３オクテットとして縦軸と横軸を入れ替えた場合、時間情報面２２０には、ＩＰアドレスの第３オクテットまでの値で指定されるサブネットに含まれる各ＩＰアドレスの時系列グラフが表示されるので、そのサブネットに含まれる通信機器に対する通信ログをまとめて表示することができる。

【００４５】

図６は、論理情報面２１０および時間情報面２２０とともに表示される位置情報面２３０に表示する地図を示す図である。論理情報面２１０に表示されたＩＰアドレスを示す点と、位置情報面２３０に表示された地図上の点とを線で結び、論理情報面２１０に示したＩＰアドレスを有する通信機器が実際にどこに存在しているのかをわかりやすく表示している。ＩＰアドレスと地図上の点とを結ぶ線は、時間情報面２２０で時系列グラフを描画した色に対応する色を用いて描画するので、時間情報面２２０で発見した不正侵入などの形跡を有する時系列グラフを持つＩＰアドレスを有する通信機器の配置場所を瞬時に判断することが可能となる。なお、一般的にＩＰアドレス空間と地図上の位置に規則性はないので、あらかじめＩＰアドレスとそのＩＰアドレスを割り当てた通信機器の配置場所とを対応付けてデータベース２０に格納しておく。

【００４６】

次に、本通信ログ視覚化システムを利用して不正侵入を検出した例を示す。図７は、ボットネットと思われる不審なＩＲＣ（Internet Relay Chat）通信を検出したときの表示画面である。なお、説明のために画面の一部を拡大して表示してある。ボットネットとは、ボットと呼ばれるプログラムをコンピュータに侵入させ、外部から不正に遠隔操作できる通信機器で構成されたネットワークのことである。ボットは外部からの命令を受けるためにＩＲＣサーバに接続して攻撃者の命令を待っている。

【００４７】

図７は、６６６７番のポートで、アウトバウンド（外向き）の通信のみが表示されるように、符号６１０で示すコマンド列を入力したものである。その結果、数カ所のＩＰアドレスから６６６７番ポートへのアクセスで警告が出ていることがわかる。また、符号２２５で示すように、２つの通信機器でほぼ同一の通信量の変化を示している。時間情報面２２０に表示された時系列グラフを選択することにより、その時系列グラフに対応するＩＰアドレスを示した論理情報面２１０上の点と、そのＩＰアドレスを有する通信機器の設置場所を示した位置情報面２３０上の点が線で結ばれて表示されるので、ネットワーク管理者は、不正侵入の疑いのある通信機器の設置場所を素早く特定でき、その通信機器の管理者に連絡をしたり、通信機器の設置場所へ向かうことができる。

【００４８】

以上説明したように、本実施の形態によれば、ネットワーク監視システム１１０が出力する通信ログを入力し、通信機器のＩＰアドレスなどを示す論理情報と、所定の期間毎の通信量を示す時間情報とを抽出して管理するとともに、通信機器の配置場所を特定する位置情報をその通信機器を示す論理情報と対応つけて管理するログ解析部１１と、論理情報、時間情報および位置情報のそれぞれの情報を読み出して、論理情報面２１０、時間情報面２２０および位置情報面２３０のそれぞれに各情報面に表示された情報の関連がわかるように表示する視覚化処理部１２とを有することにより、時間情報面２２０で不正侵入の形跡を発見した場合、その通信機器の配置場所を位置情報面２３０で瞬時に確認することが可能となるので、不正侵入に対する対応策を迅速に行うことができる。

【００４９】

本実施の形態によれば、論理情報面２１０、時間情報面２２０および位置情報面２３０のそれぞれの面が垂直に交差するように仮想３次元空間上に配置することにより、全体を

把握しやすく、また、各情報面を仮想３次元空間上に配置しているので視点を変更することができ、視点を変更することでより詳しく情報を知ることができる。さらに、時間情報面２２０を論理情報面２１０に平行に移動可能とすることで、時間情報面２２０と論理情報面２１０との交線上に該当する通信機器個々の時系列グラフ２２３を時間情報面２２０に表示することができる。

【００５０】

本実施の形態によれば、ポート毎の通信量をポート情報領域２１５に表示することで、不正侵入の種類などを推定することが可能となる。また、ポート情報領域２１５でポートを指定し、指定のポートの情報のみを表示するようにすることで、画面に表示される情報が厳選されるので、より容易に不正侵入の発見を行うことができる。

【００５１】

本実施の形態によれば、ネットワーク探査システム１２０の探査ログを入力し、実際に稼働している通信機器の論理情報（ＩＰアドレス、ポート番号など）を取得することで、稼働していないＩＰアドレスに対する攻撃を示す通信ログなどの不要な通信ログをフィルタリングすることができるので、不正侵入の発見をより容易にすることができる。

【図面の簡単な説明】

【００５２】

【図１】一実施の形態における通信ログ視覚化システムの構成を示すブロック図である。

【図２】図１の通信ログ視覚化システムの表示画面の例を示す説明図である。

【図３】図２の表示画面の論理情報面を説明するための概略図である。

【図４】図２の表示画面のポート情報領域を説明するための概略図である。

【図５】図２の表示画面の時間情報面を説明するための概略図である。

【図６】図２の表示画面の位置情報面を説明するための概略図である。

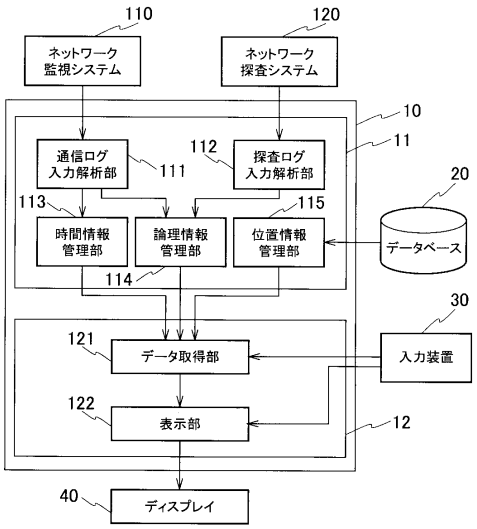
【図７】本通信ログ視覚化システムによって不正侵入を発見した際の表示画面を示す説明図である。

【符号の説明】

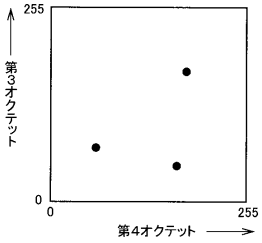
【００５３】

１０…通信ログ視覚化装置
１１…ログ解析部
１２…視覚化処理部
１１０…ネットワーク監視システム
１１１…通信ログ入力解析部
１１２…探査ログ入力解析部
１１３…時間情報管理部
１１４…論理情報管理部
１１５…位置情報管理部
１２０…ネットワーク探査システム
１２１…データ取得部
１２２…表示部
２０…データベース
３０…入力装置
４０…ディスプレイ
２１０…論理情報面
２１５…ポート情報領域
２２０…時間情報面
２３０…位置情報面

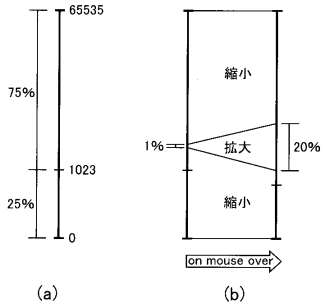
【図１】


110
120
ネットワーク
監視システム
ネットワーク
探査システム
10
11
通信ログ
入力解析部
111
112
探査ログ
入力解析部
20
113
115
時間情報
管理部
論理情報
管理部
位置情報
管理部
データベース
114
30
121
データ取得部
入力装置
122
表示部
12
40
ディスプレイ

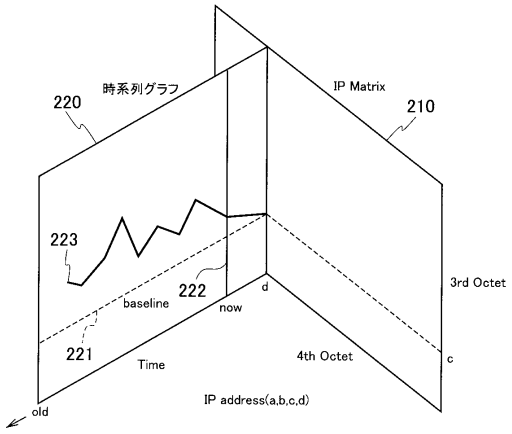
【図３】


255
第3オクテット
0
0
255
第4オクテット

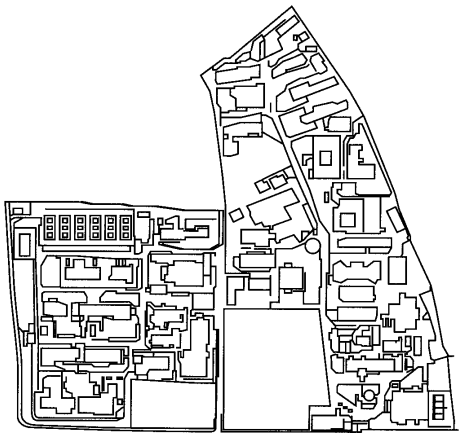
【図４】


65535
75%
1023
25%
0
縮小
1%
拡大
20%
縮小
on mouse over
(a)
(b)

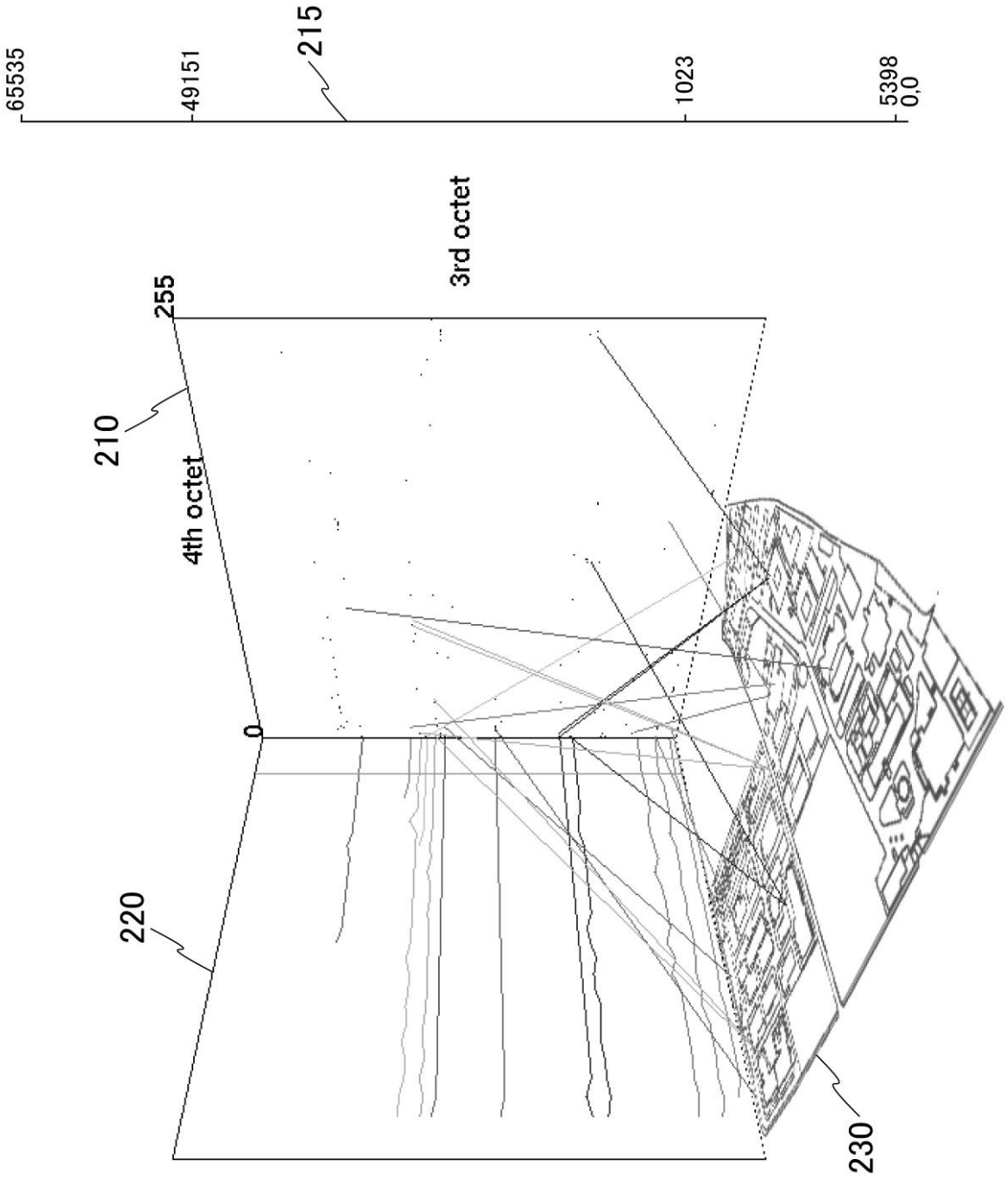
【図５】


時系列グラフ
IP Matrix
220
210
223
222
baseline
now
d
3rd Octet
221
Time
4th Octet
c
IP address(a,b,c,d)
old

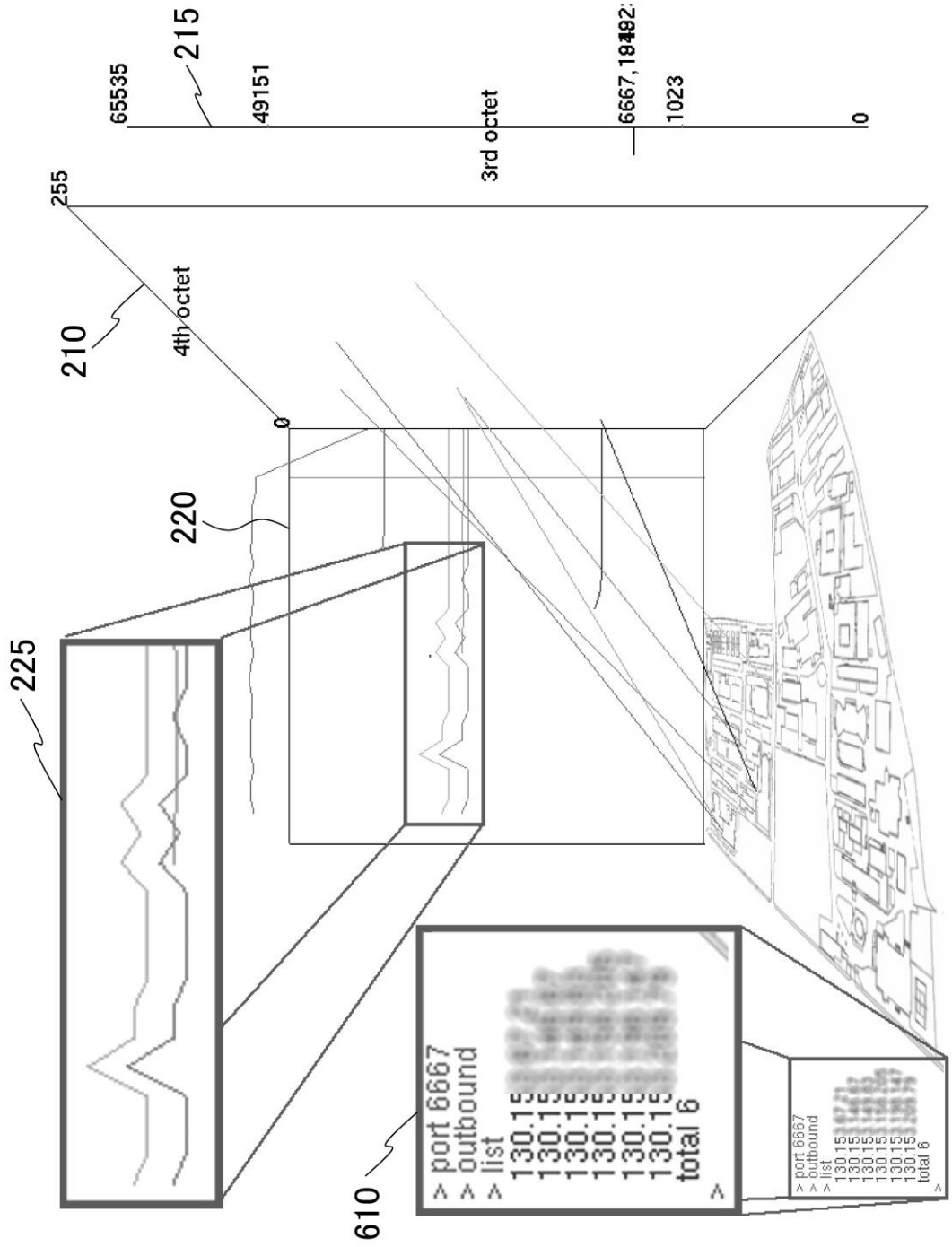
【図６】



【図２】


65535
49151
215
1023
5398
0,0
3rd octet
255
210
4th octet
0
220
230

【図７】


65535
215
49151
3rd octet
6667, 19482
1023
0
255
210
4th octet
0
220
225
610
> port 6667
> > outbound
> > list
130.15
130.15
130.15
130.15
130.15
130.15
total 6
>
> port 6667
> > outbound
> > list
130.15
130.15
130.15
130.15
130.15
130.15
total 6
>

フロントページの続き

審査官　安藤　一道

(56)参考文献　特開２００３－３１９４３３（ＪＰ，Ａ）
浅沼、大野、小池，内部ネットワーク監視のための視覚化方法の提案，FIT２００５（第４階情報科学技術フォーラム），FIT(電子情報通信学会・情報処理学会)推進委員会，２００５年　８月２２日，LK-003，pp.213-214
秀島　裕介　Yusuke　Hideshima，複数拠点におけるサイバー攻撃監視のためのＩＰＭａｔｒｉｘ　IPMatrix for Cyber Threat Monitoring Using Multiple Senssors，コンピュータセキュリティシンポジウム２００６　論文集　Computer Security Symposium 2006 (CSS2006)，日本，社団法人情報処理学会　Information Processing Society of Japan，２００６年１０月，第2006巻，pp.227-232
江端、小池，不正侵入調査を目的とした複数ログの時系列視覚化システム，情報処理学会論文誌，社団法人情報処理学会，２００６年　４月，Vol.47 No.4，pp.1099-1107
新川、山之上，IPアドレスとポートによる二次元平面を用いた通信トラフィックの可視化について，情報処理学会研究報告　2006-DSM-43，社団法人情報処理学会，２００６年　９月１５日，pp.31-36
大野　一広　KAZUHIRO　ONO，IP Matrix，情報処理学会論文誌　第４７巻　第４号　IPSJ Journal，日本，社団法人情報処理学会　Information Processing Society of Japan，２００６年　４月，第47巻

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６
Ｇ０６Ｆ　２１／２０