

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2008-193302
(P2008-193302A)

(43) 公開日 平成20年8月21日(2008.8.21)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 12/56 (2006.01)	H04L 12/56 400Z	5B285
G06F 21/20 (2006.01)	G06F 15/00 330A	5K030

審査請求 未請求 請求項の数 12 O L (全 15 頁)

(21) 出願番号	特願2007-24080 (P2007-24080)	(71) 出願人	504133110 国立大学法人 電気通信大学 東京都調布市調布ヶ丘1丁目5番地1
(22) 出願日	平成19年2月2日(2007.2.2)	(74) 代理人	100083806 弁理士 三好 秀和
特許法第30条第1項適用申請有り 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		(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

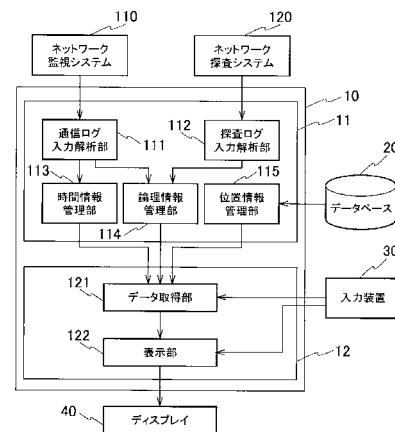
(54) 【発明の名称】 通信ログ視覚化装置、通信ログ視覚化方法及び通信ログ視覚化プログラム

(57) 【要約】

【課題】 不審な通信を行っている通信機器の設置位置を知る。

【解決手段】 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111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。これにより、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。

【選択図】 図1



【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 アドレスなどの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と前記時間情報とを関連付けて表示するとともに、前記論理情報と前記位置情報とを関連付けて表示する表示手段と、

を有することを特徴とする通信ログ視覚化装置。

【請求項 2】

前記表示手段は、前記論理情報、前記時間情報および前記位置情報を仮想 3 次元空間上の互いに交差する平面にそれぞれ配置するとともに、前記論理情報を表示する面と前記時間情報を表示する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】

前記時間情報を表示する面は、前記論理情報を表示する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 2 記載の通信ログ視覚化装置。

【請求項 4】

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 乃至 3 のいずれかに記載の通信ログ視覚化装置。

【請求項 5】

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 アドレスなどの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読み出すステップと、

表示手段による、前記読み出すステップにおいて読み出した前記論理情報と前記時間情報とを関連付けて表示するとともに、前記論理情報と前記位置情報とを関連付けて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 6】

前記表示するステップは、前記論理情報、前記時間情報および前記位置情報を仮想 3 次

10

20

30

40

50

元空間上の互いに交差する平面にそれぞれ配置するとともに、前記論理情報を表示する面と前記時間情報を表示する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ことを特徴とする請求項 5 記載の通信ログ視覚化方法。

【請求項 7】

前記時間情報を表示する面は、前記論理情報を表示する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 6 記載の通信ログ視覚化方法。

【請求項 8】

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 5 乃至 7 のいずれかに記載の通信ログ視覚化方法。

10

【請求項 9】

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 アドレスなどの論理情報と時間に関する情報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、

20

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読み出すステップと、

表示手段による、前記読み出すステップにおいて読み出した前記論理情報と前記時間情報とを関連付けて表示するとともに、前記論理情報と前記位置情報とを関連付けて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 10】

30

前記表示するステップは、前記論理情報、前記時間情報および前記位置情報を仮想 3 次元空間上の互いに交差する平面にそれぞれ配置するとともに、前記論理情報を表示する面と前記時間情報を表示する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ことを特徴とする請求項 9 記載の通信ログ視覚化プログラム。

【請求項 11】

前記時間情報を表示する面は、前記論理情報を表示する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 10 記載の通信ログ視覚化プログラム。

【請求項 12】

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 9 乃至 11 のいずれかに記載の通信ログ視覚化プログラム。

40

【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】

50

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。

10

【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。

20

【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アドレスなどの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、を有することを特徴とする。

30

40

【0009】

本発明にあつては、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

50

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。

【0010】

上記通信ログ視覚化装置において、表示手段は、論理情報、時間情報および位置情報を仮想3次元空間上の互いに交差する平面にそれぞれ配置するとともに、論理情報を表示する面と時間情報を表示する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ことを特徴とする。

【0011】

本発明にあつては、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。

10

【0012】

上記通信ログ視覚化装置において、時間情報を表示する面は、論理情報を表示する面に対して平行に移動可能であることを特徴とする。

【0013】

本発明にあつては、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つて、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】

本発明にあつては、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。

20

【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アドレスなどの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読み出すステップと、表示手段による、読み出すステップにおいて読み出した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ステップと、を有することを特徴とする。

30

【0017】

上記通信ログ視覚化方法において、表示するステップは、論理情報、時間情報および位置情報を仮想3次元空間上の互いに交差する平面にそれぞれ配置するとともに、論理情報を表示する面と時間情報を表示する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ことを特徴とする。

40

【0018】

上記通信ログ視覚化方法において、時間情報を表示する面は、論理情報を表示する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つて、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

50

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アドレスなどの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読み出すステップと、表示手段による、読み出すステップにおいて読み出した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。

10

【0021】

上記通信ログ視覚化プログラムにおいて、表示するステップは、論理情報、時間情報および位置情報を仮想3次元空間上の互いに交差する平面にそれぞれ配置するとともに、論理情報を表示する面と時間情報を表示する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、時間情報を表示する面は、論理情報を表示する面に対して平行に移動可能であることを特徴とする。

20

【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】

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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】

50

データ取得部 1 2 1 は、表示する論理情報をログ解析部 1 1 の論理情報管理部 1 1 4 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 1 1 3 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 1 1 5 から読み出す。また、利用者は、入力装置 3 0 を介して、表示したい論理情報をデータ取得部 1 2 1 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 1 2 2 は、データ取得部 1 2 1 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 3 0 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 1 2 2 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 2 1 0、時間情報面 2 2 0 および位置情報面 2 3 0 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 2 1 5 が設けられている。なお、利用者は、接続された入力装置 3 0 を用いて、時間情報面 2 2 0 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 2 1 0 を説明するための図である。論理情報面 2 1 0 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 1 2 0 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 2 1 0 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 2 1 0 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 2 1 5 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 2 1 5 には、論理情報管理部 1 1 4 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ため、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 2 1 5 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 2 1 5 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

10

20

30

40

50

報領域 2 1 5 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。

【 0 0 4 1 】

図 5 は、時間情報面 2 2 0 を説明するための図である。時間情報面 2 2 0 は、横軸に時間を示し、縦軸にネットワーク監視システム 1 1 0 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 2 2 0 に表示される時系列グラフ 2 2 3 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 2 2 2 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。

10

【 0 0 4 2 】

同図に示すように、時間情報面 2 2 0 は、仮想 3 次元空間上で論理情報面 2 1 0 に対して垂直に配置し、論理情報面 2 1 0 と時間情報面 2 2 0 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 2 2 3 として表示される。時系列グラフ 2 2 3 は、符号 2 2 2 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 2 2 1 との交点を原点として描画され、論理情報面 2 1 0 と時間情報面 2 2 0 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 2 2 0 には、複数の時系列グラフ 2 2 3 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 2 2 1 の位置に応じて異なる色を用いて描画する。

20

【 0 0 4 3 】

また、時間情報面 2 2 0 は、論理情報面 2 1 0 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 2 1 0 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 2 5 4 であることが多いので、第 4 オクテットの値が 1 または 2 5 4 になるように時間情報面 2 2 0 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 2 2 0 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。

【 0 0 4 4 】

なお、論理情報面 2 1 0 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 2 2 0 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。

30

【 0 0 4 5 】

図 6 は、論理情報面 2 1 0 および時間情報面 2 2 0 とともに表示される位置情報面 2 3 0 に表示する地図を示す図である。論理情報面 2 1 0 に表示された IP アドレスを示す点と、位置情報面 2 3 0 に表示された地図上の点とを線で結び、論理情報面 2 1 0 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 2 2 0 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 2 2 0 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 2 0 に格納しておく。

40

【 0 0 4 6 】

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

50

めに I R C サーバに接続して攻撃者の命令を待っている。

【 0 0 4 7 】

図 7 は、6 6 6 7 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 6 1 0 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 I P アドレスから 6 6 6 7 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 2 2 5 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 2 2 0 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 I P アドレスを示した論理情報面 2 1 0 上の点と、その I P 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 2 3 0 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。

10

【 0 0 4 8 】

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 1 1 0 が出力する通信ログを入力し、通信機器の I P 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 1 1 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 2 1 0、時間情報面 2 2 0 および位置情報面 2 3 0 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 1 2 とを有することにより、時間情報面 2 2 0 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 2 3 0 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。

20

【 0 0 4 9 】

本実施の形態によれば、論理情報面 2 1 0、時間情報面 2 2 0 および位置情報面 2 3 0 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 2 2 0 を論理情報面 2 1 0 に平行に移動可能とすることで、時間情報面 2 2 0 と論理情報面 2 1 0 との交線上に該当する通信機器個々の時系列グラフ 2 2 3 を時間情報面 2 2 0 に表示することができる。

30

【 0 0 5 0 】

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 2 1 5 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 2 1 5 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。

【 0 0 5 1 】

本実施の形態によれば、ネットワーク探査システム 1 2 0 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（I P 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 I P 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。

40

【 図面の簡単な説明 】

【 0 0 5 2 】

【 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 】

50

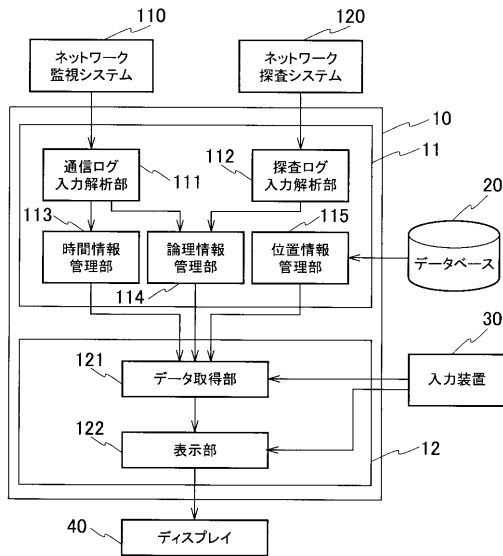
【 0 0 5 3 】

- 1 0 ... 通信ログ視覚化装置
- 1 1 ... ログ解析部
- 1 2 ... 視覚化処理部
- 1 1 0 ... ネットワーク監視システム
- 1 1 1 ... 通信ログ入力解析部
- 1 1 2 ... 探査ログ入力解析部
- 1 1 3 ... 時間情報管理部
- 1 1 4 ... 論理情報管理部
- 1 1 5 ... 位置情報管理部
- 1 2 0 ... ネットワーク探査システム
- 1 2 1 ... データ取得部
- 1 2 2 ... 表示部
- 2 0 ... データベース
- 3 0 ... 入力装置
- 4 0 ... ディスプレイ
- 2 1 0 ... 論理情報面
- 2 1 5 ... ポート情報領域
- 2 2 0 ... 時間情報面
- 2 3 0 ... 位置情報面

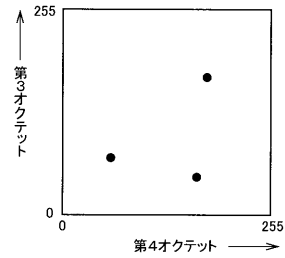
10

20

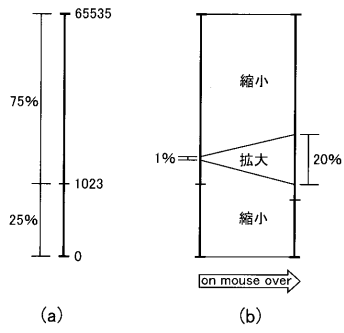
【 図 1 】



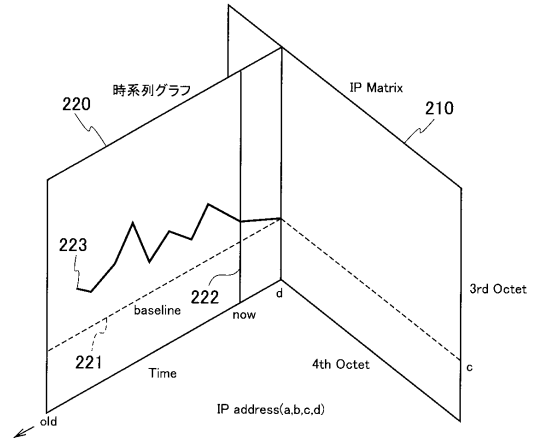
【 図 3 】



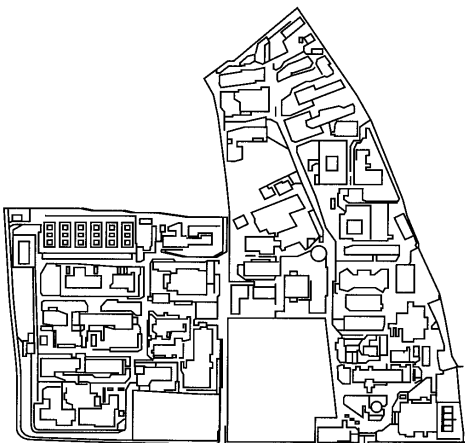
【 図 4 】



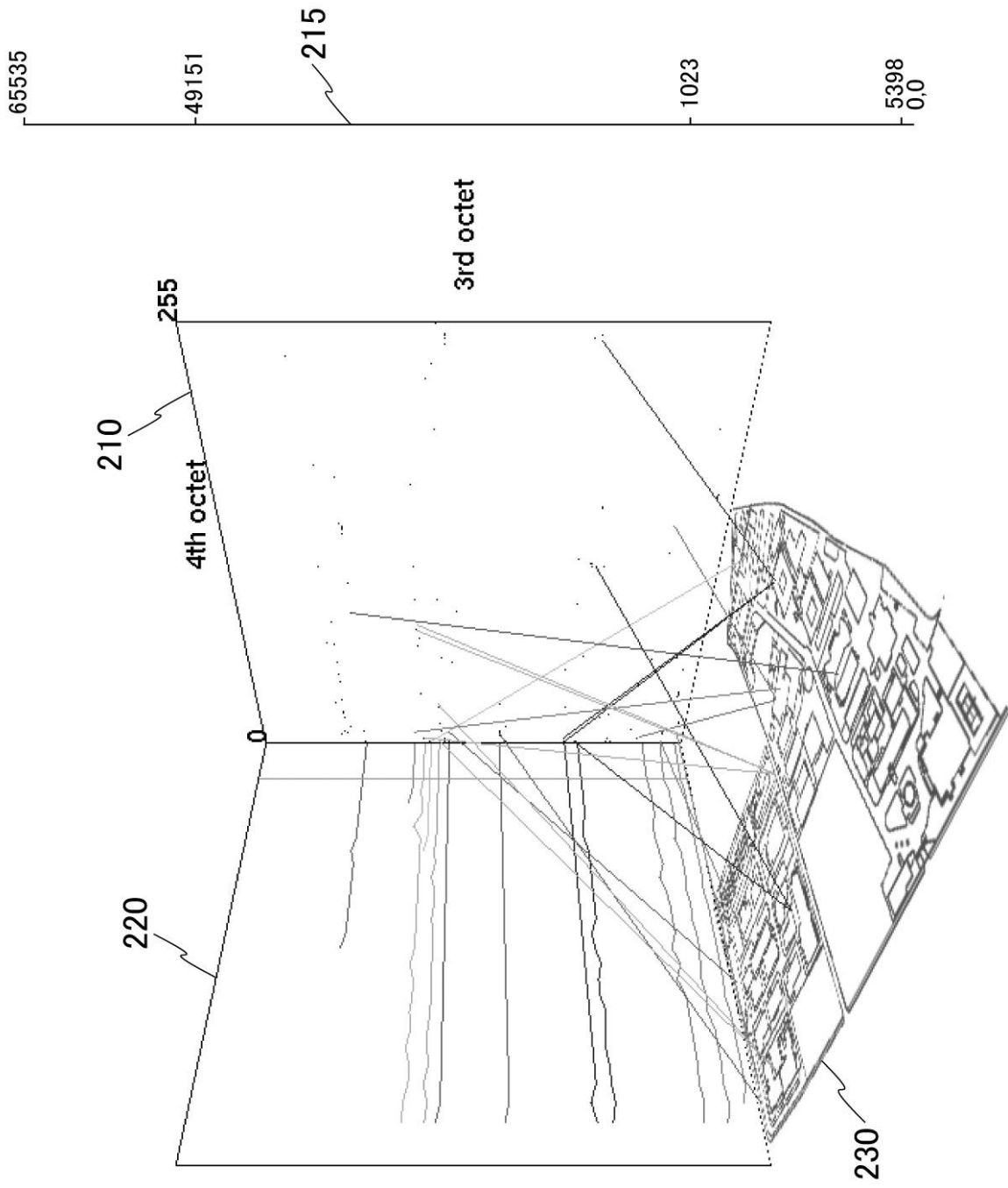
【 図 5 】



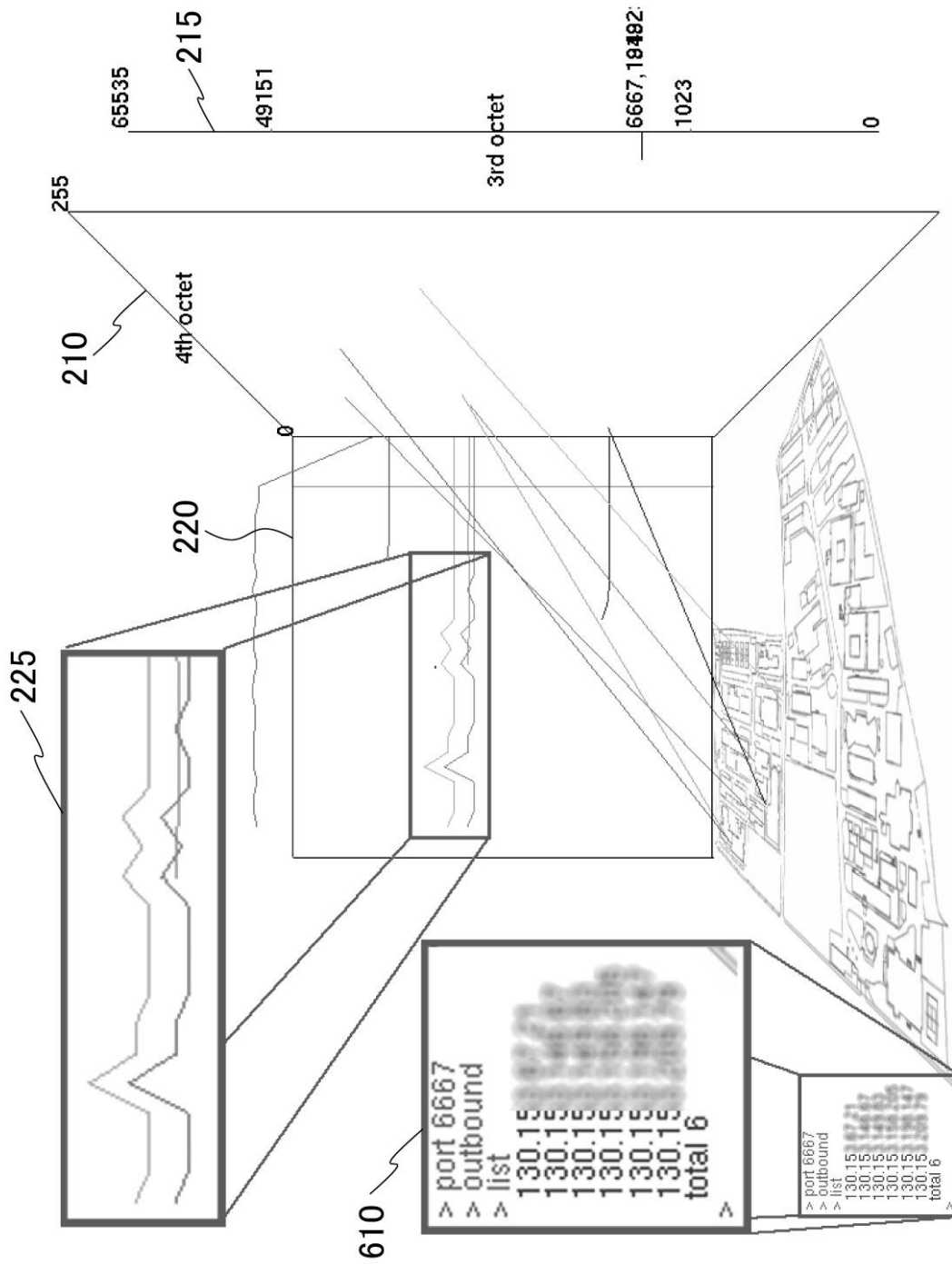
【 図 6 】



【 図 2 】



【 図 7 】



フロントページの続き

Fターム(参考) 5B285 AA05 AA06 AA07 BA01 CA32 CA33
5K030 GA15 HA08 HC01 JA10 KX30 LD18 MA04 MB18 MC07 MC08
MC09