(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2004-312083
(P2004-312083A)
(43)公開日　平成16年11月4日(2004.11.4)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	B	5K030

審査請求 未請求　請求項の数 4　OL　（全 10 頁）

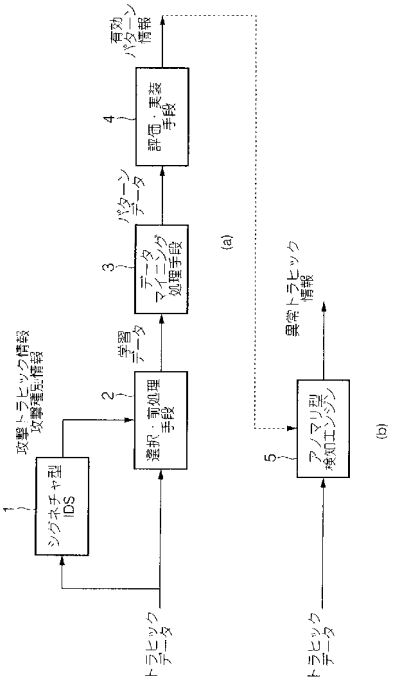
(21)出願番号　特願2003-99040(P2003-99040)
(22)出願日　平成15年4月2日(2003.4.2)

特許法第３０条第１項適用申請有り　平成１５年３月１９日　社団法人電子情報通信学会開催の「電子情報通信学会２００３年総合大会」において文書をもって発表

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100101465
弁理士　青山　正和
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(72)発明者　山田　明
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内
(72)発明者　三宅　優
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内
最終頁に続く

(54)【発明の名称】学習データ作成装置、侵入検知システムおよびプログラム

(57)【要約】
【課題】アノマリ型侵入検知システムにおいて用いられる学習データを自動的に生成することができる侵入検知システムを提供することを目的とする。
【解決手段】ネットワーク上を伝送するトラヒックデータを入力し、学習データ作成装置により作成された学習データと前記トラヒックデータから変数を選択する変数選択手段と、該選択された変数をニューラルネットや決定木等の解析アルゴリズムを用いて解析を行い、パターンを生成する処理手段と、該生成されたパターンを用いて前記解析結果を評価する評価手段とを有し、前記変数選択手段および処理手段、評価手段における処理を１回以上行うことにより、侵入の検知に有効なパターンを生成して異常なトラヒックデータを検知する侵入検知システムを提供する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ネットワーク上を伝送するトラヒックデータを入力し、
過去の不正アクセスに基づくトラヒックデータから作成されたパターンデータを記憶する記憶手段と、
該記憶手段に記憶されたパターンデータと前記ネットワークを伝送するトラヒックデータとを比較して、該パターンデータを含むトラヒックデータと攻撃種別とを抽出する比較抽出手段と、
該比較抽出手段から得られたトラヒックデータと攻撃種別から攻撃の有無が判定された学習データを作成する学習データ作成装置。
【請求項２】
ネットワーク上を伝送するトラヒックデータを入力し、予め攻撃の有無が判断された学習データから作成されたパターンに基づいて、ネットワークへの不正侵入を検知し出力する侵入検知システムであって、
前記請求項１に記載された学習データ作成装置により作成された学習データと前記トラヒックデータから変数を選択する変数選択手段と、
該選択された変数をニューラルネットや決定木等の解析アルゴリズムを用いて解析を行い、パターンを生成する処理手段と、
該生成されたパターンを用いて前記解析結果を評価する評価手段とを有し、
前記変数選択手段および処理手段、評価手段における処理を１回以上行うことにより、侵入の検知に有効なパターンを生成する侵入検知システム。
【請求項３】
ネットワーク上を伝送するトラヒックデータを入力し、
過去の不正アクセスに基づくトラヒックデータから作成されたパターンデータを記憶し、
該記憶されたパターンデータと前記ネットワークを伝送するトラヒックデータとを比較して、該パターンデータを含むトラヒックデータと攻撃種別とを抽出するとともに、
該抽出されたトラヒックデータと攻撃種別から攻撃の有無が判定された学習データを作成する学習データ作成プログラム。
【請求項４】
ネットワーク上を伝送するトラヒックデータと前記請求項３に記載された学習データプログラムにより作成された学習データとから変数を選択する第１のステップと、
該選択された変数をニューラルネットや決定木等の解析アルゴリズムを用いて解析を行い、パターンを生成する第２のステップと、
該生成されたパターンを用いて前記解析結果を評価する第３のステップとを有し、
前記第１から第３のステップにおける処理を１回以上行うことにより、侵入の検知に有効なパターンを生成する侵入検知プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワーク等への不正侵入を検知するための学習データ作成装置、侵入検知システムおよびプログラムに関する。
【０００２】
【従来の技術】
近年、インターネットの急速な発展に伴って、例えば、インターネットを活用した企業間取引や顧客へのサービス提供が活発に行われており、こうしたサービスは戦略的なビジネス展開を模索する企業にとって重要な課題になっている。しかしながら、インターネットの通信環境は、ハッカーによる不正侵入やウイルス感染といった様々な脅威にさらされており、特に、インターネットにおける不正アクセスは社会的な問題となっている。こうした事態に対応する手段としてファイヤウォールが提案されているが、ファイヤウォールは、企業内ネットワークとインターネットの中間に接続され、インターネットからの不正な

アクセスを遮断するフィルタとして機能を果たすものであり、ファイヤウォールを設置したネットワークシステムでは、内部から外部へのゲートウェイ的なアクセスを可能にし、インターネットの各種サービスを安全に利用できるようになるという利点を有するものの、ハッカーによる不正侵入おいては、サービスが提供されているため、ファイヤウォールによりフィルタすることができないトラヒックに含まれる攻撃ややサービスそのものを妨害する攻撃（サービス不能攻撃（ＤｏＳ： Ｄｅｎａｉａｌ ｏｆ Ｓｅｒｖｉｃｅ）等、さまざまな攻撃を受ける危険性がある。

【０００３】

こうした問題点に対応するために、ネットワークへの侵入を自動的に検出する侵入検知システム（ＩＤＳ：Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ）が提案されている。前述のファイヤウォールは不要なサービスのトラヒックをフィルタリングすることにより、攻撃を防ぐことが可能であるが、必要なサービスのトラヒックに攻撃が含まれている場合には、攻撃を防ぐこともこれを検知することもできない。特に、サービスそのものが脆弱である場合には、攻撃を防御することも、これを検知することもできない。一方、ＩＤＳにおいては、サービス提供の有無に関わらず、トラヒックに攻撃が含まれているか否かを検知できるため、攻撃の量や種類をも検知できるという特色を有している。

【０００４】

この侵入検知システムは検知する対象によって、シグネチャ型ＩＤＳとアノマリ型ＩＤＳとに分類される。シグネチャ型ＩＤＳは、既知の不正アクセスを検知するものであり、具体的には、過去の不正アクセスに伴う攻撃パターンを予めシグネチャとして登録しておき、ネットワーク上を伝送しているパケットデータをミラーリング等の手法で収集し、この収集したパケットデータと予め登録しておいたシグネチャとのパターンマッチングにより、攻撃の有無を判断するものである。なお、最近では、パケット単位でのパターンマッチングだけでなく、ＴＣＰ（ＴＣＰ：Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）コネクションを再構築してパターンマッチングを行う方式を実装したシステムも存在する。

【０００５】

一方、アノマリ型ＩＤＳは、ネットワーク上を伝送しているパケットデータを収集し、これに統計処理、データマイニング処理等を施して得たモデルによって、攻撃の有無を検知する方式である。例えば、統計処理による場合には、特定のポート番号にいくつのパケットがきたのかを監視し、これから、平均値や合計値を求め、あるいは、これらの取得データと過去のデータとを比較することにより、モデルを導き出す。また、データマイニング方式による場合には、予め攻撃の有無が判断された学習データ（Ｔｒａｉｎｉｎｇ Ｄａｔａ）を用いてモデルを作成し、このモデルをもとに、収集したパケットに対して攻撃の有無を判断する方式である（以上、例えば、非特許文献１参照）。なお、学習データからモデルを作成する際には、決定木やニューラルネットの手法が用いられる。

【０００６】

【非特許文献１】

Ｅｄｗａｒｄ Ｇ．Ａｍｏｒｏｓｏ著「Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ、Ｔｒａｐｓ、Ｔｒａｃｅ Ｂａｃｋ、ａｎｄ Ｒｅｓｐｏｎｓｅ」Ｉｎｔｒｕｓｉｏｎ Ｎｅｔ Ｂｏｏｋｓ社、１９９９年２月１日発行

【０００７】

【発明が解決しようとする課題】

しかし、シグネチャ型ＩＤＳは、コンピュータウィルス（Ｗｏｒｍ）や攻撃ツール（例えば、Ｅｘｐｌｏｉｔ ｃｏｄｅ等）を用いるスクリプトキディ等、攻撃パターンが一定である場合には、ネットワークへの不正侵入を高い確率で検知することが期待できるが、シグネチャに登録されていない未知の攻撃や亜種の攻撃を検知することが困難であるという問題がある。一方、アノマリ型ＩＤＳにおいては、未知の攻撃や亜種の攻撃を検知することができるという特徴を有し、高い確率で、ネットワークへの不正侵入を検知することが期待できる。

【０００８】
しかし、アノマリ型ＩＤＳで用いられるモデルを生成するための学習データは、一般には、ネットワークシステムに関する習熟者が攻撃の有無を判断したデータや、模擬的に攻撃がまったく存在しないデータを用いて作成されるため、これを一般に入手することが困難であるという問題がある。
【０００９】
そこで、本発明は、上述した問題点に鑑みてなされたものであって、アノマリ型侵入検知システムにおいて用いられる学習データを自動的に生成することができる侵入検知システムを提供することを目的とする。
【００１０】
【課題を解決するための手段】
前記課題を解決するため、本発明は、以下の手段を提案している。
請求項１に係る発明は、ネットワーク上を伝送するトラヒックデータを入力し、過去の不正アクセスに基づくトラヒックデータから作成されたパターンデータを記憶する記憶手段と、該記憶手段に記憶されたパターンデータと前記ネットワークを伝送するトラヒックデータとを比較して、該パターンデータを含むトラヒックデータと攻撃種別とを抽出する比較抽出手段と、該比較抽出手段から得られたトラヒックデータと攻撃種別から攻撃の有無が判定された学習データを作成する学習データ作成装置を提案している。
【００１１】
請求項３に係る発明は、ネットワーク上を伝送するトラヒックデータを入力し、過去の不正アクセスに基づくトラヒックデータから作成されたパターンデータを記憶し、該記憶されたパターンデータと前記ネットワークを伝送するトラヒックデータとを比較して、該パターンデータを含むトラヒックデータと攻撃種別とを抽出するとともに、該抽出されたトラヒックデータと攻撃種別から攻撃の有無が判定された学習データを作成する学習データ作成プログラムを提案している。
【００１２】
これらの発明によれば、過去の不正アクセスに基づくトラヒックデータから作成されたパターンデータを記憶し、これとネットワークを伝送するトラヒックデータとを比較してトラヒックデータと攻撃種別とを抽出し、これにより学習データを作成するため、学習データの取得が容易になる。
【００１３】
請求項２に係る発明は、ネットワーク上を伝送するトラヒックデータを入力し、予め攻撃の有無が判断された学習データから作成されたパターンに基づいて、ネットワークへの不正侵入を検知し出力する侵入検知システムであって、前記請求項１に記載された学習データ作成装置により作成された学習データと前記トラヒックデータから変数を選択する変数選択手段と、該選択された変数をニューラルネットや決定木等の解析アルゴリズムを用いて解析を行い、パターンを生成する処理手段と、該生成されたパターンを用いて前記解析結果を評価する評価手段とを有し、前記変数選択手段および処理手段、評価手段における処理を１回以上行うことにより、侵入の検知に有効なパターンを生成する侵入検知システムを提案している。
【００１４】
請求項４に係る発明は、ネットワーク上を伝送するトラヒックデータと前記請求項３に記載された学習データプログラムにより作成された学習データとから変数を選択する第１のステップと、該選択された変数をニューラルネットや決定木等の解析アルゴリズムを用いて解析を行い、パターンを生成する第２のステップと、該生成されたパターンを用いて前記解析結果を評価する第３のステップとを有し、前記第１から第３のステップにおける処理を１回以上行うことにより、侵入の検知に有効なパターンを生成する侵入検知プログラムを提案している。
【００１５】
これらの発明によれば、ネットワークへの不正侵入を前記学習データを用いて判断するた

め、未知の攻撃や亜種の攻撃に対しても高い検知率を有するシステムを構築することができる。また、学習データから不正侵入を判断するパターンを決定する手段として、ニューラルネットや決定木等の解析アルゴリズムを用いたことから、目的変数が予め決められたデータを入力することにより学習を行い、その結果を利用して目的変数から未知の事象に対して予測を行うことができる。

【００１６】

【発明の実施の形態】

以下、本発明の実施形態に係る侵入検知システムについて図１から図４を参照して詳細に説明する。

本発明の実施形態に係る侵入検知システムは、図１（ａ）および（ｂ）に示すように、シグネチャ型ＩＤＳ１と、選択・前処理手段２と、データマイニング処理手段３と、評価・実装手段４と、アノマリ型検知エンジン５とを備えている。なお、図１（ａ）は、パターンデータを生成するためのブロックを、同図（ｂ）は、侵入検知のためのブロックを示している。また、パターンデータを生成するためのブロックと侵入検知のためのブロックとは、同時に動作させてもよいし、交互に繰り返し動作させてもよい。

【００１７】

シグネチャ型ＩＤＳ１は、主に、システム上を伝送するパケットデータを入力し、各パケットデータに対する攻撃の有無やその種類を判定するシステムである。一般的なシグネチャ型ＩＤＳ１は、システム上を伝送するパケットデータを取り込むパケットキャプチャ機能を含んでいるものが多い。シグネチャ型ＩＤＳ１の仕組みは、予め攻撃と判定するパターンデータを登録しておき、パケットキャプチャ機能で取り込んだパケットデータと登録されたパターンデータとのパターンマッチングを行って、上記判定を行うものである。

【００１８】

パターンマッチングの対象は、パケットデータそのものである場合もあるが、コネクション毎のマッチングを行う場合もある。シグネチャ型ＩＤＳ１の出力は、ＡＳＣＩＩテキスト形式や攻撃パケットデータそのものである場合が多いが、既に製品化されたシグネチャ型ＩＤＳ１では、それぞれ異なる出力形式が採用されており、共通フォーマット侵入検知交換フォーマット（例えば、ＩＤＥＦ：Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｅｘｃｈａｎｇｅ　Ｆｏｒｍａｔ等）を採用しているものもある。

【００１９】

本実施形態におけるシグネチャ型ＩＤＳ１は、図示しない既存のシグネチャ型ＩＤＳ接続用インターフェースを有しており、システム上を伝送するトラヒックデータを入力して、パターンマッチングを行い、攻撃トラヒック情報と攻撃種別情報とを出力する。なお、ＩＤＥＦにより記述されたデータを入力対象とすることもできる。

【００２０】

選択・前処理手段２は、各パケットデータに対して、フォーマットにおけるすべての変数を抽出する。一般に、ネットワーク上を伝送するトラヒックデータは、パケットデータと呼ばれる単位のバイナリデータに分割することができる。バイナリデータは、それぞれ決められたデータフォーマットにより規定されている。各パケットデータは、ＩＰ（ＩＰ：Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）やポート、シーケンスナンバーといった変数に分類できるため、この処理においては、入力したトラヒックデータをパケット毎、ＩＰ毎、ポート毎、ＴＣＰコネクション毎のそれぞれを対象に変数を抽出する。なお、ここで、ＴＣＰコネクション毎とは、シーケンスナンバーにより関連付けられるものである。

【００２１】

次に、抽出した変数の中から解析に必要な変数を選択する。変数の選択は、予め変数を決定しておく場合もあるが、シグネチャ型ＩＤＳにより得られるデータに基づいて、変数を決定する場合もある。こうして得られたデータは、次に、データマイニング処理に適した形式に成形されて、学習データとして出力される。なお、データマイニング処理には、汎用的なデータマイニングソフトも利用できる。この場合のデータ形式としては、ＡＳＣＩＩテキスト形式やリレーショナルデータベースに保存した形式となる。

【００２２】
データマイニング処理手段３は、例えば、決定木やニューラルネットおよびＫ－ｍｅａｎｓなどの手法を用いて、選択・前処理手段２から入力される学習データを処理するものである。これらの手法は、入力として説明変数と目的変数とからなる多変数データを用いるものであり、この多変数データは複数の事象とそれに対応する説明変数および目的変数とにより構成される。
【００２３】
一般に、目的変数は１つであり、説明変数は複数存在する。また、ニューラルネットなどを用いたデータマイニング処理では、目的変数が予め決められたデータを入力することにより学習を行い、その結果を利用することにより、目的変数から未知の事象に対して予測を行う。本実施形態においては、一例として、パケットデータ毎、ＩＰ毎、ポート毎、ＴＣＰコネクション毎のそれぞれを事象として、抽出された変数を説明変数とし、攻撃の有無もしくは攻撃の種類を目的変数としている。
【００２４】
評価・実装手段４は、データマイニング処理手段３から出力されたパターンデータが攻撃トラヒックデータや異常トラヒックデータを検知するために有効であるかどうかを評価する。具体的には、評価・実装結果を人間が判断する場合やデータマイニング処理手段３から出力されたパターンデータをシステムに一旦適用して、その適用の結果から、何らかの閾値を設けることにより評価する方法などが考えられる。
【００２５】
仮に、評価の結果が有効なものでないと判断された場合には、選択・前処理手段２に戻って、もう一度、学習データの生成を行う。一方、有効であると判断された場合、その有効な特徴を検知方法として実装し、システムに適用する。アノマリ型検知エンジン５は、実装された有効な特徴を利用して、目的変数の決定されていないデータの目的変数を予測する機能を果たす。
【００２６】
次に、図２を用いて、学習データ作成の処理フローについて説明する。
本実施形態において、学習データを得るためには、まず、ネットワークを伝送するトラヒックデータからパケットデータをダンプする（ステップ１０１）。ダンプされたパケットデータは、シグネチャ型ＩＤＳ１内のインターフェースを介して入力される（ステップ１０２）。入力されたパケットデータは、予め登録されているシグネチャとマッチング処理され（ステップ１０３）、入力されたパケットデータと予め登録されているシグネチャが一致しているときは、攻撃トラヒック情報と攻撃種別が抽出された後、選択・前処理手段２に出力され、パケットの分類および変数の選択が行われる（ステップ１０４）。
【００２７】
その後、目的変数に攻撃種別が記入され（ステップ１０５）、データマイニング処理が可能な形式に成形される（ステップ１０６）。続いて、すべてのパケットデータについて、予め登録されているシグネチャとのマッチング処理が完了したかが判断され、すべてのパケットデータについてマッチング処理が完了していると判断されたときは（ステップ１０７）、学習データを出力して終了する（ステップ１０８）。一方、すべてのパケットデータについてマッチング処理が完了していないと判断したときは（ステップ１０７）、ステップ１０１に戻って、新たなパケットデータをトラヒックデータからダンプする。
【００２８】
さらに、パケットデータと予め登録されているシグネチャが一致していない判断されるときは（ステップ１０３）、すべてのパケットデータについてマッチングが完了しているか否かを判断し、完了していると判断したときは（ステップ１０７）、学習データを出力して（ステップ１０８）終了する。一方、すべてのパケットデータについてマッチングが完了していないと判断したときは、ステップ１０１に戻って、処理を続行する。
【００２９】
次に、図３を用いて、データマイニング処理からパターンデータの生成までの流れについ

て説明する。
データマイニング処理手段３は、選択・前処理手段２から学習データを入力する（ステップ２０１）。入力された学習データには、目的変数として攻撃種別が記入されているため、データマイニング処理手段３においては、この目的変数を入力することにより学習を行い、その結果を利用して目的変数から未知の事象に対して予測を行う（ステップ２０２）。
【００３０】
データマイニング処理における予測により、有効な結果が得られた場合には（ステップ２０３）、このデータマイニングの結果をパターンデータとして評価・実装手段４に出力し（ステップ２０４）、良好な評価が行えた場合には、このモデルをアノマリ型検知エンジン５に出力する（ステップ２０５）。一方、データマイニング処理における予測により、有効な結果が得られない場合には（ステップ２０３）、図２のフローチャートに戻って、学習データを再構築する（ステップ２０６）。
【００３１】
次に、図４を用いて、システムの侵入検知の処理について説明する。なお、本図においては、事前に、図２および図３のフローチャートにしたがって、モデルが構築できているものとする。
ネットワーク上を伝送するトラヒックデータは、パケット単位でダンプされて（ステップ３０１）アノマリ型検知エンジン５に出力される（ステップ３０２）。アノマリ型検知エンジン５に入力されたパケットデータは、パケットごとに分類され、変数の選択が行われる（ステップ３０３）。変数の選択が行われたパケットデータは、データマイニングに適した形式に成形され（ステップ３０４）、登録されているモデルとマッチング処理される（ステップ３０５）。
【００３２】
マッチング処理の結果、パケットデータと登録されたモデルとが一致すると判断されたとき（ステップ３０５）は、異常トラヒック情報を出力し（ステップ３０６）、次に、すべてのパケットデータについてマッチング処理が完了したかを確認し、すべてのパケットデータについてマッチング処理が完了したと判断したときは処理を終了する（ステップ３０７）。
【００３３】
一方、すべてのパケットデータについて、マッチング処理が完了していないと判断したときは、ステップ３０１に戻って処理を続行する。また、パケットデータと登録されたモデルとが一致しないと判断されたときは（ステップ３０５）、すべてのパケットデータについてマッチング処理が完了したかを判断し（ステップ３０７）、完了したと判断したときは処理を終了し、完了していないと判断したときは、ステップ３０１に戻って、処理を続行する。
【００３４】
以上、図面を参照して本発明の実施形態について詳述してきたが、具体的な構成はこれらの実施の形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計変更等も含まれる。例えば、図４のフローチャートにおいては、ダンプしたパケットデータを選択・前処理してアノマリ型検知エンジンに入力する形態について説明したが、選択・前処理を行わず、ダンプしたパケットデータを直接、アノマリ型検知エンジンに入力するような構成であってもよい。
【００３５】
また、本実施形態においては、攻撃トラヒック情報の抽出、攻撃種別情報の抽出にシグネチャ型ＩＤＳを用いて説明したが、ＩＤＳの検知結果としては、既存のＩＤＳの検知結果であればどのようなものでもよいし、必ずしもシグネチャ型である必要はない。
【００３６】
【発明の効果】
以上のように、この発明によれば、アノマリ型ＩＤＳに用いる有効なパターンデータの生

成に必要な学習データをシグネチャ型ＩＤＳを利用して生成することとしたことから、従来、熟練者等によらなければ入手が困難であった学習データを容易に入手することができるという効果がある。

【００３７】

また、上記有効なパターンデータをアノマリ型ＩＤＳに適用することにより、シグネチャの登録されていない未知の攻撃や亜種の攻撃を検知できるという効果がある。さらに、シグネチャ型ＩＤＳにより生成した学習データを用いて侵入検知に有効なパターンデータを生成し、これをアノマリ型ＩＤＳに適用したことから、より高い検知率を期待できるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施形態に係る侵入検知システムの構成図である。

【図２】本発明の実施形態に係る侵入検知システムにおける学習データの生成フローチャート図である。

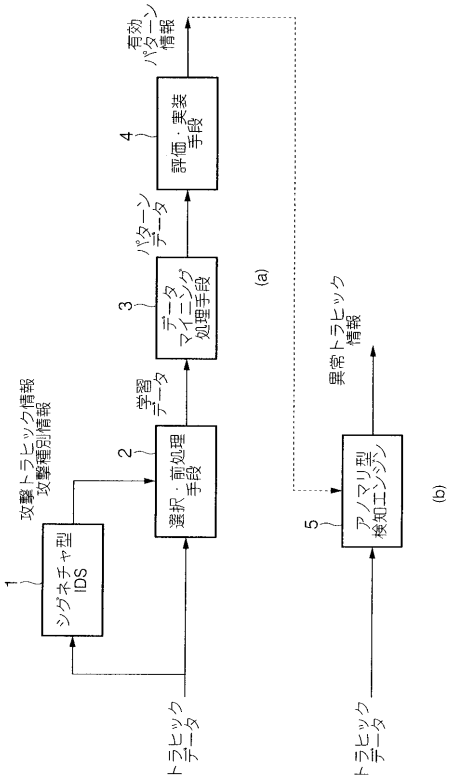
【図３】本発明の実施形態に係る侵入検知システムにおけるデータマイニング処理からパターンデータの作成までを示すフローチャート図である。

【図４】本発明の実施形態に係る侵入検知システムにおける侵入検知のフローチャート図である。

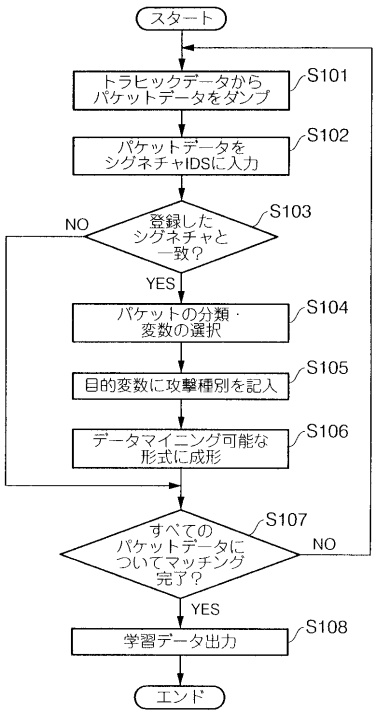
【符号の説明】

１・・・シグネチャ型ＩＤＳ、２・・・選択・前処理手段、３・・・データマイニング処理手段、４・・・評価・実装手段、５・・・アノマリ型検知エンジン、

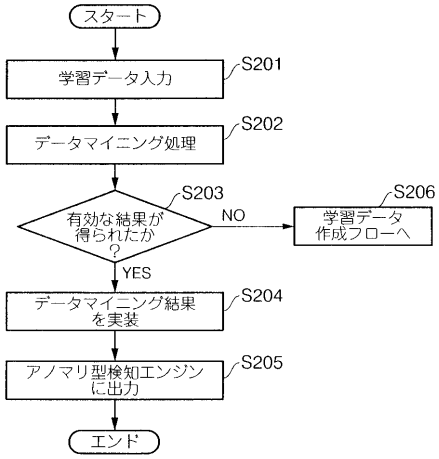
【図１】



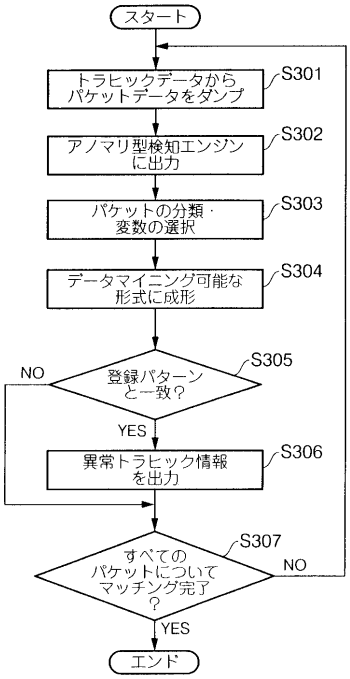
【図２】



【図３】


スタート
学習データ入力
S201
データマイニング処理
S202
有効な結果が得られたか？
S203
NO
学習データ作成フローへ
S206
YES
データマイニング結果を実装
S204
アノマリ型検知エンジンに出力
S205
エンド

【図４】


スタート
トラヒックデータからパケットデータをダンプ
S301
アノマリ型検知エンジンに出力
S302
パケットの分類・変数の選択
S303
データマイニング可能な形式に成形
S304
登録パターンと一致？
S305
NO
YES
異常トラヒック情報を出力
S306
すべてのパケットについてマッチング完了？
S307
NO
YES
エンド

フロントページの続き

(72)発明者　田中　俊昭
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内
(72)発明者　中尾　康二
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内

Ｆターム(参考) 5K030 GA15　HA08　HC01　HD03　KA07　LC18　MA13