(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6827266号
(P6827266)
(45)発行日　令和3年2月10日(2021.2.10)　(24)登録日　令和3年1月21日(2021.1.21)

(51)Int.Cl.　　F I
G06F 21/55 (2013.01)　　G06F 21/55 340
G06F 11/34 (2006.01)　　G06F 11/34 152

請求項の数 5　(全 18 頁)

(21)出願番号　特願2016-6455(P2016-6455)
(22)出願日　平成28年1月15日(2016.1.15)
(65)公開番号　特開2017-126283(P2017-126283A)
(43)公開日　平成29年7月20日(2017.7.20)
審査請求日　平成30年9月12日(2018.9.12)
審判番号　不服2020-7665(P2020-7665/J1)
審判請求日　令和2年6月3日(2020.6.3)

（出願人による申告）平成２７年度、総務省、「サイバー攻撃の解析・検知に関する研究開発」研究開発委託契約に基づく開発項目「利用者の行動特性に基づくサイバー攻撃検知技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　坂本　喜則
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　松原　正純
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　小林　賢司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
最終頁に続く

(54)【発明の名称】検知プログラム、検知方法および検知装置

(57)【特許請求の範囲】
【請求項１】
過去ログに含まれる事象の中から、所定の事象を抽出し、前記所定の事象ごとに、前記所定の事象と関連する複数の関連事象を前記所定の事象を起点とする所定の時間幅にわたって抽出し、
前記所定の事象および前記関連事象に対応するパターンデータを作成し、
前記パターンデータを前記所定の事象の時間順に結合した学習モデルを構築し、
前記学習モデルと、発生した事象に応じて入力されるイベントデータとの照合結果をもとに異常の検知を行う処理をコンピュータに実行させ、
前記パターンデータを作成する処理は、事象の種別ごとに予め設定されたマスキングのルールをもとに、前記所定の時間幅にわたって抽出された所定の事象および関連事象に対応するパターンデータを、当該抽出された所定の事象および関連事象の種別に応じたマスキングのルールに基づきマスキングする
ことを特徴とする検知プログラム。
【請求項２】
前記抽出する処理は、前記起点に対して事象ごとに予め設定された終点のルールをもとに、前記所定の事象および前記関連事象の中で前記起点に対する終点が最も長くなる時間幅で抽出を行う
ことを特徴とする請求項１に記載の検知プログラム。
【請求項３】

前記学習モデルを構築する処理は、前記所定の事象ごとに作成されたパターンデータにおいて、互いに共通する共通部をマージして前記学習モデルを構築する
ことを特徴とする請求項１または２に記載の検知プログラム。
【請求項４】
過去ログに含まれる事象の中から、所定の事象を抽出し、前記所定の事象ごとに、前記所定の事象と関連する複数の関連事象を前記所定の事象を起点とする所定の時間幅にわたって抽出し、
前記所定の事象および前記関連事象に対応するパターンデータを作成し、
前記パターンデータを前記所定の事象の時間順に結合した学習モデルを構築し、
前記学習モデルと、発生した事象に応じて入力されるイベントデータとの照合結果をもとに異常の検知を行う処理をコンピュータが実行し、
前記パターンデータを作成する処理は、事象の種別ごとに予め設定されたマスキングのルールをもとに、前記所定の時間幅にわたって抽出された所定の事象および関連事象に対応するパターンデータを、当該抽出された所定の事象および関連事象の種別に応じたマスキングのルールに基づきマスキングする
ことを特徴とする検知方法。
【請求項５】
プロセッサが、
過去ログに含まれる事象の中から、所定の事象を抽出し、前記所定の事象ごとに、前記所定の事象と関連する複数の関連事象を前記所定の事象を起点とする所定の時間幅にわたって抽出し、
前記所定の事象および前記関連事象に対応するパターンデータを作成し、
前記パターンデータを前記所定の事象の時間順に結合した学習モデルを構築し、
前記学習モデルと、発生した事象に応じて入力されるイベントデータとの照合結果をもとに異常の検知を行う処理を実行し、
前記パターンデータを作成する処理は、事象の種別ごとに予め設定されたマスキングのルールをもとに、前記所定の時間幅にわたって抽出された所定の事象および関連事象に対応するパターンデータを、当該抽出された所定の事象および関連事象の種別に応じたマスキングのルールに基づきマスキングする
ことを特徴とする検知装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、検知プログラム、検知方法および検知装置に関する。
【背景技術】
【０００２】
従来、大規模コンピュータシステムやネットワークシステム等の監視対象のシステムにおいては、サイバー攻撃などによるシステム障害等の異常（アノマリ）検知が行われている。このアノマリ検知においては、例えばシステムにおける過去の時系列データを過去のメタデータとしてメタデータ化して格納する。そして、システムにおけるリアルタイムの時系列データについてメタデータを生成し、過去のメタデータと照合することで、システムの障害等の検知を行う。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００６－２７５７００号公報
【特許文献２】特開平０２－２９８９４号公報
【特許文献３】特開２００９－２８９２２１号公報
【特許文献４】特開２００３－１７７９０１号公報
【発明の概要】

【発明が解決しようとする課題】
【０００４】
しかしながら、上述した従来技術では、間欠的で長期間にわたる事象を伴う異常を検知することが困難であるという問題がある。
【０００５】
例えば、間欠的で長期間にわたる事象を伴う異常としては、メールやＷｅｂを連携した高度な標的型攻撃による異常があり、一例としてやり取り型標的型メール攻撃による異常がある。このやり取り型標的型メール攻撃では、攻撃元から標的へのメール間隔が数日に及ぶ場合がある。
【０００６】
このように、攻撃元から標的へのメールが間欠的で長期間にわたって行われる場合には、過去の時系列データにおいてメール間に生じた数々の別事象が混じることとなる。よって、リアルタイムに得られた時系列データとの照合を行った場合に、メール間に生じた数々の別事象との不一致により異常の検知精度が低減することがある。また、異常検知のために保持する過去の時系列データのデータ量が膨大なものとなり、高速に照合を行うことが困難なものとなる。
【０００７】
１つの側面では、間欠的で長期間にわたる事象を伴う異常の検知を可能とする検知プログラム、検知方法および検知装置を提供することを目的とする。
【課題を解決するための手段】
【０００８】
第１の案では、検知プログラムは、過去ログに含まれる事象の中から、所定の事象を抽出し、所定の事象ごとに、所定の事象と関連する複数の関連事象を所定の事象を起点とする所定の時間幅にわたって抽出する処理をコンピュータに実行させる。また、検知プログラムは、所定の事象および関連事象に対応するパターンデータを作成する処理をコンピュータに実行させる。また、検知プログラムは、パターンデータを所定の事象の時間順に結合した学習モデルを構築する処理をコンピュータに実行させる。また、検知プログラムは、学習モデルと、発生した事象に応じて入力されるイベントデータとの照合結果をもとに異常の検知を行う処理をコンピュータに実行させる。また、パターンデータを作成する処理は、事象の種別ごとに予め設定されたマスキングのルールをもとに、所定の時間幅にわたって抽出された所定の事象および関連事象に対応するパターンデータを、当該抽出された所定の事象および関連事象の種別に応じたマスキングのルールに基づきマスキングする。
【発明の効果】
【０００９】
本発明の１実施態様によれば、間欠的で長期間にわたる事象を伴う異常を検知できる。
【図面の簡単な説明】
【００１０】
【図１】図１は、実施形態にかかる検知装置の構成例を示すブロック図である。
【図２】図２は、学習モデルの構築とアノマリ検知の概要を説明する説明図である。
【図３】図３は、学習モデルを説明する説明図である。
【図４－１】図４－１は、学習モデルの構築にかかる処理の一例を示すフローチャートである。
【図４－２】図４－２は、学習モデルの構築にかかる処理の一例を示すフローチャートである。
【図５】図５は、定義・ルール情報を説明する説明図である。
【図６】図６は、部分管理表とアノマリ・パターンを説明する説明図である。
【図７】図７は、アノマリ・パターンの圧縮を説明する説明図である。
【図８】図８は、共通部のマージを説明する説明図である。
【図９】図９は、アノマリ検知にかかる処理の一例を示すフローチャートである。

【図１０】図１０は、異常検知の一例を説明する説明図である。
【図１１】図１１は、やりとり型標的型メール攻撃における異常検知を説明する説明図である。
【図１２】図１２は、実施形態にかかる検知装置のハードウエア構成の一例を示すブロック図である。
【発明を実施するための形態】
【００１１】
以下、図面を参照して、実施形態にかかる検知プログラム、検知方法および検知装置を説明する。実施形態において同一の機能を有する構成には同一の符号を付し、重複する説明は省略する。なお、以下の実施形態で説明する検知プログラム、検知方法および検知装置は、一例を示すに過ぎず、実施形態を限定するものではない。また、以下の各実施形態は、矛盾しない範囲内で適宜組みあわせてもよい。
【００１２】
図１は、実施形態にかかる検知装置１の構成例を示すブロック図である。図１に示す検知装置１は、例えばＰＣ（パーソナルコンピュータ）等の情報処理装置である。
【００１３】
検知装置１は、例えば、大規模コンピュータシステムやネットワークシステム等の監視対象のシステム（図示しない）において過去に発生した事象が時系列順に記述された過去ログ２０を読み込んで学習モデル１３を構築する。検知装置１は、監視対象のシステムにおいてリアルタイムに発生した事象に応じて入力されるイベントデータ３０を受け付け、構築された学習モデル１３と、イベントデータ３０との照合結果をもとに監視対象のシステムにおける異常（アノマリ）を検知し、検知結果をユーザへ報知する。例えば、検知装置１は、アノマリ検知の検知結果を他の端末装置２や所定のアプリへ出力し、端末装置２における検知結果の表示やアプリ通知などを介してユーザへの検知結果の報知を行う。
【００１４】
過去ログ２０およびイベントデータ３０における事象については、様々なものがあってよく、特に限定しない。例えば、監視対象のシステムへのサイバー攻撃などをアノマリとして検知する場合には、メール受信、メール操作、ＰＣ操作、Ｗｅｂアクセス、データ通信などの事象がある。また、監視対象のシステムにおける不正入場などをアノマリとして検知する場合には、監視カメラの映像やカードキーの操作などにより検出されたユーザの行動などの事象がある。また、監視対象のシステムにおける環境異常をアノマリとして検知する場合には、センサにより検出された温度、湿度などの事象がある。
【００１５】
なお、本実施形態では、監視対象のシステムへのサイバー攻撃をアノマリとして検知する検知装置１を例示する。よって、過去ログ２０およびイベントデータ３０には、メール受信、メール操作、ＰＣ操作、Ｗｅｂアクセス、データ通信などのサイバー攻撃にかかる各種事象が含まれるものとする。
【００１６】
図１に示すように、検知装置１は、前処理部１０ａ、１０ｂ、定義・ルール情報１１、学習モデル構築部１２、学習モデル１３、アノマリ検知部１４、分散・並列処理部１５および出力部１６を有する。
【００１７】
前処理部１０ａ、１０ｂは、入力されたデータについて、データの整形・加工などの前処理を行う。前処理部１０ａは、監視対象のシステムより入力された過去ログ２０に前処理を行い、処理後のデータを学習モデル構築部１２に出力する。前処理部１０ｂは、監視対象のシステムより入力されたイベントデータ３０に前処理を行い、処理後のデータをアノマリ検知部１４に出力する。なお、前処理部１０ａ、１０ｂについては、過去ログ２０およびイベントデータ３０で分ける構成とすることなく、１つの前処理部を共有する構成であってもよい。
【００１８】

過去ログ２０およびイベントデータ３０に対する前処理としては、過去ログ２０およびイベントデータ３０に含まれる各事象の内容を予め定められた条件に従ってグループ分けし、数値や文字に変換する変換処理がある。これにより、例えば過去ログ２０およびイベントデータ３０に含まれる事象の内容が互いに同じ場合には、前処理部１０ａ、１０ｂの前処理によって同一の数値または文字に変換されることとなる。

【００１９】

定義・ルール情報１１は、学習モデル１３の構築についての定義・ルールを示す情報である。ユーザにより予め設定された定義・ルール情報１１がメモリなどの記憶装置に格納されている。学習モデル構築部１２は、前処理後の過去ログ２０をもとに、定義・ルール情報１１に従って学習モデル１３を構築する。構築された学習モデル１３は、メモリなどの記憶装置に格納される。アノマリ検知部１４は、過去ログ２０より構築された学習モデル１３と、前処理後のイベントデータ３０とを照合し、監視対象のシステムにおいてリアルタイムに発生した事象、すなわち監視対象のシステムの現状における異常（アノマリ）の検知を行う。アノマリ検知部１４は、検知結果を出力部１６に出力する。出力部１６は、アノマリ検知部１４による検知結果を端末装置２や所定のアプリなどに出力する。

【００２０】

分散・並列処理部１５は、複数のスレッドを用いるなどして検知装置１における各処理を分散・並列化する。例えば、分散・並列処理部１５は、アノマリ検知部１４におけるアノマリ検知にかかる処理を分散・並列化する。このようにアノマリ検知部１４における処理を分散・並列化することで、アノマリ検知をより高速に行うことができ、アノマリ検知のリアルタイム性を向上することができる。なお、分散・並列処理部１５による処理の分散・並列化は、前処理部１０ａ、１０ｂ、学習モデル構築部１２における各処理に適用してもよい。

【００２１】

図２は、学習モデル１３の構築とアノマリ検知の概要を説明する説明図である。図２の上段には、過去ログ２０に含まれる各事象が時間順に示されている。ここで、メール相手（ａ、ｂ…）はやり取り型標的型メール攻撃とは無関係のものとし、メール相手（ｘ）はやり取り型標的型メール攻撃を行う相手であるものとする。また、期間Ｔ１は、所定のメール相手（図示例ではメール相手ｘ）のメール受信に応じたメール操作の期間を示すものとする。また、期間Ｔ２は、所定のメール相手（図示例ではメール相手ｘ）のメール受信に応じたメール操作に関連した全ての事象が終了するまでの期間（関連期間とも呼ぶ）を示すものとする。

【００２２】

図２に示すように、学習モデル構築部１２は、定義・ルール情報１１に記述された定義・ルールを参照して過去ログ２０に含まれる事象の中から所定の事象（図示例では、メール相手ごとのメール受信であり特定事象または主軸と呼ぶ）を抽出する。具体的には、学習モデル構築部１２は、メール相手（ａ、ｂ、…、ｘ）ごとのメール受信という特定事象（主軸）を抽出する。次いで、学習モデル構築部１２は、この特定事象ごとに、定義・ルール情報１１に記述された定義・ルールに示された特定事象と関連する複数の関連事象について、特定事象を起点とする所定の時間幅にわたって抽出する。

【００２３】

例えば、メール操作、ＰＣ操作、Ｗｅｂアクセス、通信データなどの１～Ｎの関連事象が定義・ルールに示されている場合、学習モデル構築部１２は、特定事象および関連事象（１～Ｎ）を、全ての事象が終了するまでの期間Ｔ２にわたって抽出する。この特定事象および関連事象の抽出が行われる時間幅（例えば期間Ｔ２）については、以後の説明で部分とも呼ぶものとする。学習モデル構築部１２は、特定事象に対応する部分ごとに、特定事象および関連事象を抽出する。

【００２４】

次いで、学習モデル構築部１２は、期間Ｔ２にわたって抽出された特定事象および関連事象の内容に対応するパターンデータ（以下、アノマリ・パターンとも呼ぶ）を作成する

。具体的には、学習モデル構築部１２は、特定事象および関連事象の内容に応じて前処理により数値や文字で変換した値を時間順に並べたアノマリ・パターンを作成する。

【００２５】

なお、学習モデル構築部１２は、各部分のアノマリ・パターンの作成において、特定事象および関連事象における事象ごとのアノマリ・パターンを互いに時間的に整合が取れた形にする。具体的には、学習モデル構築部１２は、定義・ルール情報１１において事象ごとに予め設定されたマスキングのルールをもとに、特定事象および関連事象の中であるタイミングで実体のない事象については所定のマスキングを行う。これにより、事象ごとのアノマリ・パターンを時間的に整合した形とする。

【００２６】

例えば、ＰＣ操作を伴うＷｅｂアクセスが行われた場合には、関連事象のＰＣ操作およびＷｅｂアクセスにおいて同じタイミングで実施内容に対応するアノマリ・パターンが生成される。これに対し、ＰＣ操作を伴わないＷｅｂアクセスが行われた場合には、Ｗｅｂアクセスが行われたタイミングでＰＣ操作の実体がなく、互いのアノマリ・パターンの時間的な整合が取れなくなる。したがって、実体のないＰＣ操作については、予め設定されたマスキングのルールに基づくマスキング・パターンで補填することで、互いのアノマリ・パターンを時間的に整合した形とする。

【００２７】

次いで、学習モデル構築部１２は、特定事象ごとの各部分のアノマリ・パターンを時間順に結合（統合）して学習モデル１３を構築する。例えば、学習モデル構築部１２は、メール相手（ｘ）のメール受信ごとの、各部分のアノマリ・パターンを時間順に結合（統合）してメール相手（ｘ）の学習モデル１３を構築する。同様にメール相手（ａ、ｂ、…）についても、学習モデル構築部１２は、メール受信ごとの各部分のアノマリ・パターンを時間順に結合（統合）してメール相手（ａ、ｂ、…）の学習モデル１３を構築する。

【００２８】

なお、メール相手（ｘ）はやり取り型標的型メール攻撃を行う相手である。よって、教師付き学習である場合、学習モデル構築部１２は、メール相手（ｘ）について各部分を時間順に結合（統合）した学習モデル１３を、アノマリ検知すべきパターン（検知パータン）として構築する。また、学習モデル構築部１２は、メール相手（ａ、ｂ、…）について各部分を時間順に結合（統合）した学習モデル１３を、アノマリ検知から除外すべき定常のパターン（除外パータン）として構築する。

【００２９】

図３は、学習モデル１３を説明する説明図である。図３に示すように、学習モデル１３は、特定事象ごとの部分群（各部分）を管理する部分群管理表１３１と、部分ごとの情報を管理する部分管理表１３２と、各部分のアノマリ・パターン１３３とを有する。

【００３０】

部分群管理表１３１は、メール相手（ａ、ｂ、…、ｘ）からのメール受信という特定事象（主軸）ごとの、各部分の情報を統括管理するテーブルであり、例えばポインタ情報、主軸の部分識別子、アノマリ度、部分管理表アドレスを有する。

【００３１】

ポインタ情報には、各部分群管理表１３１のアドレスを示す情報が格納される。例えば、やり取り型標的型メール攻撃を行うメール相手（ｘ）についての部分群管理表１３１には、検知パターンとして参照されるアドレスがポインタ情報に記述される。また、通常のメールをやり取りするメール相手（ａ、ｂ、…）についての部分群管理表１３１には、除外パターンとして参照されるアドレスがポインタ情報に記述される。

【００３２】

主軸の部分識別子には、特定事象（主軸）を識別するためにユニークに割り当てられた値が格納される。例えば、部分識別子には、メール相手のＩＤ（例えばメールアドレス）とメール命題のＩＤ（例えばメールタイトル）とを組み合わせた値が格納される。これにより、例えば、やり取り型標的型メール攻撃においてやり取りされるメールについては、

同一の部分識別子が格納されることとなる。アノマリ度には、過去ログ２０の中で特定事象が出現した出現頻度を示す値が格納される。部分管理表アドレスには、部分ごとの情報を管理する部分管理表１３２を示すアドレスが格納される。

【００３３】

部分管理表１３２は、部分ごとの情報を統括管理するテーブルであり、例えば、ポインタ情報、主軸の部分識別子、部分の出現頻度、アノマリ・パターンのアドレスを有する。ポインタ情報には、時間順に結合された次の部分を示すアドレスが格納される。これにより、部分管理表１３２のポインタ情報を参照することで、時間順に結合された部分ごとの情報を、時間軸に沿って順次参照することができる。部分の出現頻度には、過去ログ２０の中で部分が出現した出現頻度を示す値が格納される。アノマリ・パターンのアドレスには、対象の部分におけるアノマリ・パターン１３３を示すアドレスが格納される。

【００３４】

図２に戻り、アノマリ検知部１４は、構築された学習モデル１３について、時間軸に沿って、順次、発生した事象に応じて入力されるイベントデータ３０との比較、すなわちシステムの現状との比較（照合）を行い、アノマリ（異常）を検知する。例えば、アノマリ検知部１４は、システムの現状が検知パターンとして構築された学習モデル１３と照合する場合には検知パターンに対応するアノマリが発生したことを検知する。また、アノマリ検知部１４は、システムの現状が除外パターンとして構築された学習モデル１３と照合しない場合には、定常から外れた何らかのアノマリが発生したことを検知する。一例として、やり取り型標的型メール攻撃を行うメール相手（ｘ）についての部分を統合した学習モデル１３と、システムの現状とが合う場合には、やり取り型標的型メール攻撃にかかるアノマリ検知を行う。

【００３５】

ここで、学習モデル１３の構築にかかる処理の詳細を説明する。図４－１および図４－２は、学習モデル１３の構築にかかる処理の一例を示すフローチャートである。なお、図４－２は、図４－１に続く処理のフローチャートである。

【００３６】

図４－１に示すように、処理が開始されると、学習モデル構築部１２は、メモリなどに格納された定義・ルール情報１１の読込みを行う（Ｓ１）。

【００３７】

図５は、定義・ルール情報１１を説明する説明図である。図５に示すように、定義・ルール情報１１は、主軸となる特定事象および特定事象と関連する関連事象について（１～Ｎの事象）、各事象への適用ルールなどの情報を含む。

【００３８】

例えば、各事象への適用ルールには、事象の発生を示す起点および事象の終了を示す終点のルールがあり、事象に対応したものが予め設定される。また、適用ルールには、各事象においてアノマリ・パターンを時間的に整合した形とするためのマスキングについてのルール（マスキング・パターン）がある。マスキングのルールについては、例えば、（ａ）：ワイルドカード（合致）、（ｂ）：パディング（直前を延長）、（ｃ）：０（ＮＵＬＬ）の適用などがあり、事象に対応したものが予め設定される。適用ルールには、各事象においてアノマリ算出（出現頻度の算出）を行うためのルールがあり、事象に対応した算出方法が予め設定される。

【００３９】

次いで、学習モデル構築部１２は、過去ログ２０の読込みを行い（Ｓ２）、過去ログ２０において事象ごとに記述された処理のプロセス名などを参照することで、定義・ルール情報１１に示された主軸の各事象（特定事象の各々）を過去ログ２０より抽出する（Ｓ３）。次いで、学習モデル構築部１２は、Ｓ３で抽出された主軸の各事象を起点として、定義・ルール情報１１に示された主軸の関連事象を過去ログ２０より抽出する（Ｓ４）。

【００４０】

次いで、学習モデル構築部１２は、主軸の事象（特定事象）ごとに、主軸の事象および

関連事象の全ての事象が終了するまでの関連期間、すなわち各部分の時間幅を算出する（Ｓ５）。具体的には、学習モデル構築部１２は、プロセス切換などの処理の論理関係を調べ、主軸の事象および関連事象におけるプロセスを追跡する。次いで、学習モデル構築部１２は、定義・ルール情報１１において事象ごとに示された終点のルールをもとに、主軸の事象および関連事象の各事象におけるプロセスの終点を求める。次いで、学習モデル構築部１２は、求めた終点の中で起点に対する終点が最も長いものを関連期間の終点とする。学習モデル構築部１２は、Ｓ３、Ｓ４において抽出された事象を算出された関連期間内のものに絞り込み、部分ごとの事象を抽出する。

【００４１】

次いで、学習モデル構築部１２は、定義・ルール情報１１に基づき、各部分における事象ごとのマスキング・パターンを作成する（Ｓ６）。具体的には、学習モデル構築部１２は、定義・ルール情報１１における事象ごとのマスキングのルール（（ａ）、（ｂ）または（ｃ））を参照し、事象に対応したルールでマスキング・パターンを作成する。これにより、関連期間内の各事象について、実体がない期間のアノマリ・パターン１３３については、Ｓ６で作成されたマスキング・パターンで補填される。これにより、アノマリ・パターン１３３の各事象を時間的に整合した形とすることができる。

【００４２】

次いで、学習モデル構築部１２は、全部分についてＳ３～Ｓ６の処理が完了したか否かを判定する（Ｓ７）。全部分の処理が完了していない場合（Ｓ７：ＮＯ）、学習モデル構築部１２は、Ｓ３へ処理を戻し、処理が完了していない次の部分についての処理を実施する。

【００４３】

全部分の処理が完了した場合（Ｓ７：ＹＥＳ）、学習モデル構築部１２は、定義・ルール情報１１のアノマリ算出のルールに基づき、部分の事象別（１～Ｎ）のアノマリ度（出現頻度）を算出する（Ｓ８）。次いで、学習モデル構築部１２は、部分毎に抽出した事象の内容を前処理により数値や文字で変換した値を時間順に並べ、部分毎のアノマリ・パターン１３３を作成する（Ｓ９）。なお、学習モデル構築部１２は、実体がない期間についてはＳ６において作成されたマスキング・パターンで補填してアノマリ・パターン１３３を作成する。

【００４４】

ここで、学習モデル構築部１２は、部分毎に部分識別子を付与した部分管理表１３２を作成し、Ｓ９で作成したアノマリ・パターン１３３のアドレスを部分管理表１３２に格納する。

【００４５】

図６は、部分管理表１３２とアノマリ・パターン１３３を説明する説明図である。図６に示すように、学習モデル構築部１２は、メール相手のＩＤ（例えばメールアドレス）とメール命題のＩＤ（例えばメールタイトル）とを組み合わせた部分識別子を付与した部分管理表１３２を作成する。次いで、学習モデル構築部１２は、Ｓ９で作成したアノマリ・パターン１３３のアドレスを部分管理表１３２に格納する。

【００４６】

なお、学習モデル構築部１２は、部分毎のアノマリ・パターン１３３を時間軸で圧縮し、圧縮後のアノマリ・パターン１３３のアドレスを部分管理表１３２に格納してもよい。図７は、アノマリ・パターン１３３の圧縮を説明する説明図である。

【００４７】

なお、図７において、アノマリ・パターン１３３ａは圧縮前のアノマリ・パターンを示し、アノマリ・パターン１３３ｂは圧縮後のアノマリ・パターンを示すものとする。また、アノマリ・パターンにかかる事象については、Ａ～Ｃの３つの事象があるものとする。事象Ａについては、グループ分けにより０、１、２のいずれかの値に変換されるものとし、変換後の値（事象Ａのアノマリ・パターン）は時間順に１、１、０、０、１、２、２となるものとする。また、事象Ｂについては、グループ分けにより０、１のいずれかの値に

変換されるものとし、事象Ｂのアノマリ・パターンは時間順に０、０、０、０、０、０、１となるものとする。また、事象Ｃについては、グループ分けにより０、１、２のいずれかの値に変換されるものとし、事象Ｃのアノマリ・パターンは１、１、１、１、１、１、１となるものとする。

【００４８】

圧縮前のアノマリ・パターン１３３ａでは、事象Ａ、Ｂ、Ｃのパターンが（１、０、１）または（０、０、１）である、連続した時間幅の部分がある。学習モデル構築部１２は、このように時間軸において連続したパターンの部分を時間幅を示す情報を変更（図示例では１から２に変更）して圧縮する。このように、学習モデル構築部１２は、アノマリ・パターン１３３を時間軸で圧縮することで、アノマリ・パターン１３３のデータ量を削減してもよい。

【００４９】

図４－１に戻り、Ｓ９に次いで、学習モデル構築部１２は、全部分についてＳ８、Ｓ９の処理が完了したか否かを判定する（Ｓ１０）。全部分の処理が完了していない場合（Ｓ１０：ＮＯ）、学習モデル構築部１２は、Ｓ８へ処理を戻し、処理が完了していない次の部分についての処理を実施する。

【００５０】

全部分の処理が完了した場合（Ｓ１０：ＹＥＳ）、学習モデル構築部１２は、全ての部分に対して出現頻度を算出し、算出した出現頻度を部分管理表１３２に反映する（Ｓ１１）。具体的には、学習モデル構築部１２は、１／母数（＝全部分数）として出現頻度を算出し、算出した出現頻度を部分管理表１３２における部分の出現頻度に格納する。

【００５１】

次いで、学習モデル構築部１２は、過去ログ２０に出現した時間順に部分をソートし（Ｓ１２）、同一の部分識別子が付与された部分を統合（結合）する（Ｓ１３）。具体的には、各部分を管理する部分管理表１３２のポインタ情報をＳ１２でソートした順序で参照するように設定する。これにより、例えばメール相手ごとのメール受信という特定事象ごとに抽出された部分が統合される。

【００５２】

部分識別子には、一例として、メール相手のＩＤ（例えばメールアドレス）とメール命題のＩＤ（例えばメールタイトル）とを組み合わせた値が格納される。よって、Ｓ１３では、同じメール相手との同じ命題のメールのやり取りについての部分であり、例えばやり取り型標的型メール攻撃で想定されるメールのやり取りの部分が時間順に統合されることとなる。これにより、やり取り型標的型メール攻撃で想定されるメールのやり取り間に生じた数々の別事象が学習モデル１３に混じることを抑止できる。また、メールのやり取り開始から終了するまでの長期にわたる事象をもとに学習モデル１３を構築する場合に比べて、学習モデル１３のデータ量を削減することができる。

【００５３】

次いで、学習モデル構築部１２は、Ｓ１３で統合した部分間の接続部においてアノマリ・パターン１３３が同一の時は、同一する部分をマージしてデータ量を圧縮する（Ｓ１４）。具体的には、図７に例示したアノマリ・パターン１３３の圧縮と同様に、アノマリ・パターン１３３が同一である部分の圧縮を行う。

【００５４】

次いで、学習モデル構築部１２は、「定常」の除外パターンの学習であるか、教師付き学習による「異常」の検知パターンの学習であるかを判定する（Ｓ１５）。具体的には、学習モデル構築部１２は、過去ログ２０を読み込んだ教師付き学習であるか否かをもとに「定常」または「異常」の判定を行う。

【００５５】

Ｓ１５において「定常」の場合、すなわちメール相手（ａ、ｂ、…）より学習モデル１３を構築した場合、学習モデル構築部１２は、構築した学習モデル１３を除外パターンとして登録する（Ｓ１６）。また、Ｓ１５において「異常」の場合、すなわちメール相手（

ｘ）より学習モデル１３を構築した場合、学習モデル構築部１２は、構築した学習モデル１３を検知パターンとして登録する（Ｓ１７）。

【００５６】

次いで、学習モデル構築部１２は、全部分についてＳ１３～Ｓ１７の処理が完了したか否かを判定する（Ｓ１８）。全部分の処理が完了していない場合（Ｓ１８：ＮＯ）、学習モデル構築部１２は、Ｓ１３へ処理を戻し、処理が完了していない次の部分についての処理を実施する。

【００５７】

全部分の処理が完了した場合（Ｓ１８：ＹＥＳ）、学習モデル構築部１２は、除外パターンまた検知パターンごとに学習モデル１３の部分群同士を比較し（Ｓ１９）、部分群同士での共通性・重複の有無を判定する（Ｓ２０）。具体的には、学習モデル構築部１２は、互いの部分群のアノマリ・パターン１３３を比較し、部分群の全体または部分群の途中までの部分で一致する部分を共通性・重複のある共通部と判定する。

【００５８】

共通性・重複がある場合（Ｓ２０：ＹＥＳ）、学習モデル構築部１２は、共通性・重複があると判定された共通部をマージし、マージされた部分のアノマリ度（出現頻度）を変更する（Ｓ２１）。具体的には、学習モデル構築部１２は、マージ前の互いの共通部における出現頻度を合算するなどして、マージされた部分のアノマリ度を求め、新たなアノマリ度に変更する。共通性・重複がない場合（Ｓ２０：ＮＯ）、学習モデル構築部１２は、Ｓ２１をスキップしてＳ２２へ処理を進める。

【００５９】

図８は、共通部のマージを説明する説明図である。具体的には、部分群管理表１３１Ａ、部分管理表１３２Ａおよびアノマリ・パターン１３３Ａにおける部分群（Ａ）と、部分群管理表１３１Ｂ、部分管理表１３２Ｂおよびアノマリ・パターン１３３Ｂにおける部分群（Ｂ）とにおける共通部のマージを例示する図である。

【００６０】

一例として、図８の例は、メール相手（ｘ）より構築した検知パターンの学習モデル１３における部分群（Ａ、Ｂ）であるものとする。また、部分群（Ａ）は、３通のメールをやり取りした後に攻撃メールを受けた部分群とする。また、部分群（Ｂ）は、３通目までは部分群（Ａ）と同じであり、４通目に部分群（Ａ）とは異なるメールを受けてから攻撃メールを受けた部分群とする。

【００６１】

このように、３通のメールをやり取りした共通のアノマリ・パターン１３３（共通部）がある場合、学習モデル構築部１２は、学習モデル１３における部分群（Ａ、Ｂ）をマージして共通部の重複を除去した部分群管理表１３１Ｃ、部分管理表１３２Ｃおよびアノマリ・パターン１３３Ｃを作成する。なお、部分群管理表１３１Ｃ、部分管理表１３２Ｃおよびアノマリ・パターン１３３Ｃの識別子については、共通の識別子（例えば部分群（Ａ）の部分識別子＋部分群（Ｂ）の部分識別子）を新たに付与する。このように、学習モデル構築部１２は、部分群における共通のアノマリ・パターン１３３をマージすることで、学習モデル１３のデータ量を削減することができる。

【００６２】

次いで、学習モデル構築部１２は、全部分についてＳ１９～Ｓ２１の処理が完了したか否かを判定する（Ｓ２２）。全部分の処理が完了していない場合（Ｓ２２：ＮＯ）、学習モデル構築部１２は、Ｓ１９へ処理を戻し、処理が完了していない次の部分についての処理を実施する。全部分の処理が完了した場合（Ｓ２２：ＹＥＳ）、学習モデル構築部１２は学習モデル１３の構築にかかる処理を終了する。

【００６３】

次に、アノマリ検知にかかる処理の詳細を説明する。図９は、アノマリ検知にかかる処理の一例を示すフローチャートである。

【００６４】

図９に示すように、処理が開始されると、アノマリ検知部１４は、前処理後のイベントデータ３０をもとに、監視対象のシステムにおいてリアルタイムに発生した事象に対応するパターンデータ（アノマリ・パターン）を作成する（Ｓ３０）。このアノマリ・パターンについては、定義・ルール情報１１をもとにマスキングを施したものとする。次いで、アノマリ検知部１４は、Ｓ３０で作成したアノマリ・パターンについて、時系列順に同一命題の事象（例えば、メール相手（ａ、ｂ、…、ｘ）ごとのメール受信）を連結する（Ｓ３１）。

【００６５】

次いで、アノマリ検知部１４は、Ｓ３０、Ｓ３１で作成した今回のアノマリ・パターンは一つ前のパターンと同一であるか否かを判定する（Ｓ３２）。同一である場合（Ｓ３２：ＹＥＳ）、アノマリ検知部１４は、一致するアノマリ・パターンをマージする（Ｓ３３）。同一でない場合（Ｓ３２：ＮＯ）、アノマリ検知部１４は、Ｓ３３の処理をスキップする。

【００６６】

次いで、アノマリ検知部１４は、現アノマリ・パターンの要素と同一要素分だけを学習モデル１３と比較する（Ｓ３４）。次いで、アノマリ検知部１４は、Ｓ３４の比較において一致する学習モデル１３があるか否かを判定する（Ｓ３５）。一致する学習モデル１３がない場合（Ｓ３５：ＮＯ）、アノマリ検知部１４は、Ｓ４０へ処理を進める。

【００６７】

一致する学習モデル１３がある場合（Ｓ３５：ＹＥＳ）、アノマリ検知部１４は、現アノマリ・パターンと途中（同一要素分）まで一致した学習モデル１３全体とを比較する（Ｓ３６）。次いで、アノマリ検知部１４は、Ｓ３６の比較において最後まで一致したか否かを判定する（Ｓ３７）。最後まで一致しない場合（Ｓ３７：ＮＯ）、学習モデル１３との比較においてシステムに異常が生じていることの確認が取れないことから、異常検知のアラームを出すことなく、処理を終了する。

【００６８】

最後まで一致する場合（Ｓ３７：ＹＥＳ）、アノマリ検知部１４は、一致した学習モデル１３は、「いつも」の状態を示す除外パターンであるか、「異常」の状態を示す検知パターンであるかを判定する（Ｓ３８）。Ｓ３８において「いつも」である場合、異常検知のアラームを出すことなく、処理を終了する。

【００６９】

Ｓ３８において「異常」である場合、アノマリ検知部１４は、異常検知のアラームを出力部１６に発信し（Ｓ３９）、処理を終了する。異常検知のアラームを受けた出力部１６は、端末装置２や所定のアプリなどに異常検知を出力する。

【００７０】

Ｓ４０に処理を進める場合は、現アノマリ・パターンと一致する学習モデル１３がないので、「異常」の状態を示す検知パターンだけでなく、「いつも」の状態を示す除外パターンとの一致もないこととなる。したがって、Ｓ４０において、アノマリ検知部１４は、異常とまでは言えないが、不審な状態であることを示す不審アラームを出力部１６に発信する。不審アラームを受けた出力部１６は、端末装置２や所定のアプリなどに不審アラームを出力する。

【００７１】

次いで、アノマリ検知部１４は、学習モデル１３における除外パターン・検知パターンの各々と、Ｓ３０、Ｓ３１で作成したアノマリ・パターンとの類似性を算出する（Ｓ４１）。具体的には、パターンマッチにかかる公知の手法を用いることで、互いのパターンの類似度合いを求める。

【００７２】

次いで、アノマリ検知部１４は、算出された類似度合いをもとに、Ｓ３０、Ｓ３１で作成したアノマリ・パターンが除外パターン・検知パターンのどちらに近いかを判定する（Ｓ４２）。Ｓ４２において除外パターンに近い場合、システムの現状が定常とするパター

ンに類似していることから、アノマリ検知部１４は、定常に対する不審回数を増加する（Ｓ４３）。

【００７３】

次いで、アノマリ検知部１４は、定常に対する不審回数が予め定められた閾値を超過するか否かを判定する（Ｓ４４）。超過する場合（Ｓ４４：≧閾値）、アノマリ検知部１４は、異常の度合いが高いことから定常起因の異常検知アラームを出力部１６に発信する（Ｓ４５）。異常検知アラームを受けた出力部１６は、端末装置２や所定のアプリなどに異常検知を出力する。

【００７４】

Ｓ４２において検知パターンに近い場合、システムの現状が異常とするパターンに類似していることから、アノマリ検知部１４は、異常に対する不審回数を増加する（Ｓ４６）。次いで、アノマリ検知部１４は、異常に対する不審回数が予め定められた閾値を超過するか否かを判定する（Ｓ４７）。超過する場合（Ｓ４７：≧閾値）、アノマリ検知部１４は、異常の度合いが高いことから異常起因の異常検知アラームを出力部１６に発信する（Ｓ４８）。異常検知アラームを受けた出力部１６は、端末装置２や所定のアプリなどに異常検知を出力する。

【００７５】

図１０は、異常検知の一例を説明する説明図である。図１０において、上段には除外パターンの学習モデル１３に含まれるアノマリ・パターン１３３の一例が示されている。また、下段にはＳ３０、Ｓ３１で作成したアノマリ・パターン３１の一例が示されている。図１０に示すように、例えば、Ｓ３０、Ｓ３１で作成したシステムの現状を示すアノマリ・パターン３１と、除外パターンのアノマリ・パターン１３３とが不一致である場合（非該当時）、アノマリ検知部１４はシステムにおける不審アラームを出力する。そして、定常に対する不審回数が予め定められた閾値を超過したところで、定常起因の異常検知アラームを出力する。

【００７６】

以上のように、検知装置１の定義・ルール情報１１は、過去ログ２０に含まれる事象の中から、特定事象を抽出し、特定事象ごとに、特定事象と関連する複数の関連事象を特定事象を起点とする所定の時間幅にわたって抽出する。また、定義・ルール情報１１は、特定事象ごとに、特定事象および関連事象に対応するアノマリ・パターン１３３を作成する。また、定義・ルール情報１１は、特定事象ごとに作成されたアノマリ・パターン１３３を特定事象の時間順に結合した学習モデル１３を構築する。検知装置１のアノマリ検知部１４は、学習モデル１３と、発生した事象に応じて入力されるイベントデータ３０との照合結果をもとに異常（アノマリ）の検知を行う。

【００７７】

このように、過去ログ２０から特定事象と、特定事象を起点とする所定の時間幅にわたる関連事象とを抽出してアノマリ検知にかかる学習モデル１３を構築するため、特定事象間に生じた数々の別事象が学習モデル１３に混じることを抑止できる。よって、検知装置１は、構築された学習モデル１３と、イベントデータ３０との照合結果をもとにアノマリ検知を行うことで、間欠的で長期間にわたる事象を伴うアノマリを精度よく検知できる。

【００７８】

図１１は、やり取り型標的型メール攻撃における異常検知を説明する説明図である。図１１に示すように、検知装置１では、間欠的で長期間にわたる事象を伴うやり取り型標的型メール攻撃における異常（アノマリ）を精度よく検知できる。

【００７９】

なお、図示した各装置の各構成要素は、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。

【００８０】

例えば、本実施形態では検知装置１単体の装置構成を例示したが、複数のストレージ装置やサーバ装置などをネットワークで接続したクラウドコンピューティングとしてもよい。

【００８１】

また、検知装置１で行われる各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ（Micro Controller Unit）等のマイクロ・コンピュータ）上で、その全部または任意の一部を実行するようにしてもよい。また、各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ等のマイクロ・コンピュータ）で解析実行されるプログラム上、またはワイヤードロジックによるハードウエア上で、その全部または任意の一部を実行するようにしてもよいことは言うまでもない。

【００８２】

ところで、上記の実施形態で説明した各種の処理は、予め用意されたプログラムをコンピュータで実行することで実現できる。そこで、以下では、上記の実施例と同様の機能を有するプログラムを実行するコンピュータ（ハードウエア）の一例を説明する。図１２は、実施形態にかかる検知装置１のハードウエア構成の一例を示すブロック図である。

【００８３】

図１２に示すように、検知装置１は、各種演算処理を実行するＣＰＵ１０１と、データ入力を受け付ける入力装置１０２と、モニタ１０３と、スピーカ１０４とを有する。また、検知装置１は、記憶媒体からプログラム等を読み取る媒体読取装置１０５と、各種装置と接続するためのインタフェース装置１０６と、有線または無線により外部機器と通信接続するための通信装置１０７とを有する。また、検知装置１は、各種情報を一時記憶するＲＡＭ１０８と、ハードディスク装置１０９とを有する。また、検知装置１内の各部（１０１～１０９）は、バス１１０に接続される。

【００８４】

ハードディスク装置１０９には、上記の実施形態で説明した前処理部１０ａ、１０ｂ、学習モデル構築部１２、アノマリ検知部１４、分散・並列処理部１５および出力部１６における各種の処理を実行するためのプログラム１１１が記憶される。また、ハードディスク装置１０９には、プログラム１１１が参照する各種データ１１２（学習モデル１３、過去ログ２０およびイベントデータ３０など）が記憶される。入力装置１０２は、例えば、検知装置１の操作者から操作情報の入力を受け付ける。モニタ１０３は、例えば、操作者が操作する各種画面を表示する。インタフェース装置１０６は、例えば印刷装置等が接続される。通信装置１０７は、ＬＡＮ（Local Area Network）等の通信ネットワークと接続され、通信ネットワークを介した外部機器との間で各種情報をやりとりする。

【００８５】

ＣＰＵ１０１は、ハードディスク装置１０９に記憶されたプログラム１１１を読み出して、ＲＡＭ１０８に展開して実行することで、各種の処理を行う。なお、プログラム１１１は、ハードディスク装置１０９に記憶されていなくてもよい。例えば、検知装置１が読み取り可能な記憶媒体に記憶されたプログラム１１１を読み出して実行するようにしてもよい。検知装置１が読み取り可能な記憶媒体は、例えば、ＣＤ－ＲＯＭやＤＶＤディスク、ＵＳＢ（Universal Serial Bus）メモリ等の可搬型記録媒体、フラッシュメモリ等の半導体メモリ、ハードディスクドライブ等が対応する。また、公衆回線、インターネット、ＬＡＮ等に接続された装置にこのプログラム１１１を記憶させておき、検知装置１がこれらからプログラム１１１を読み出して実行するようにしてもよい。

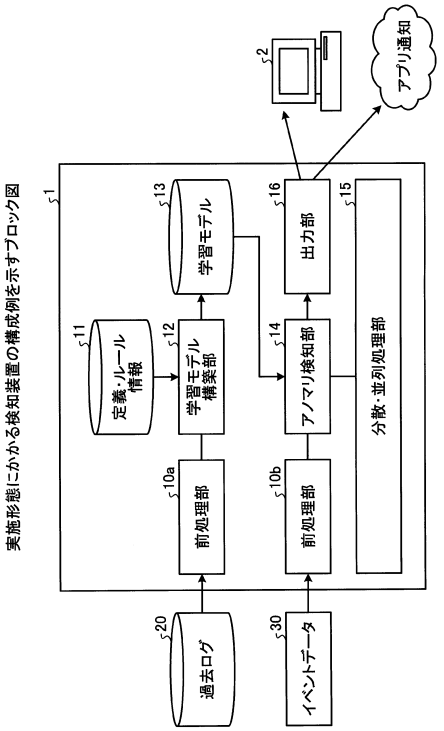
【符号の説明】

【００８６】

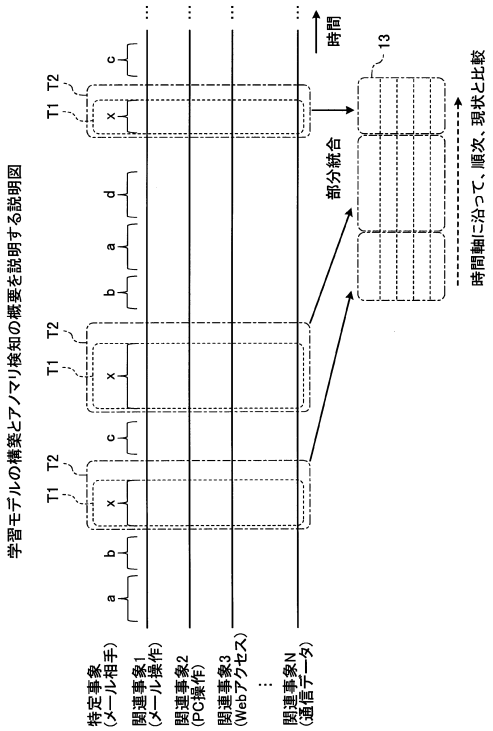
１…検知装置
２…端末装置
１０ａ、１０ｂ…前処理部
１１…定義・ルール情報
１２…学習モデル構築部

１３…学習モデル
１４…アノマリ検知部
１５…分散・並列処理部
１６…出力部
２０…過去ログ
３０…イベントデータ
３１、１３３、１３３Ａ、１３３Ｂ、１３３Ｃ、１３３ａ、１３３ｂ…アノマリ・パターン
１０１…ＣＰＵ
１１１…プログラム
１３１、１３１Ａ、１３１Ｂ、１３１Ｃ…部分群管理表
１３２、１３２Ａ、１３２Ｂ、１３２Ｃ…部分管理表
Ｔ１、Ｔ２…期間

【図１】

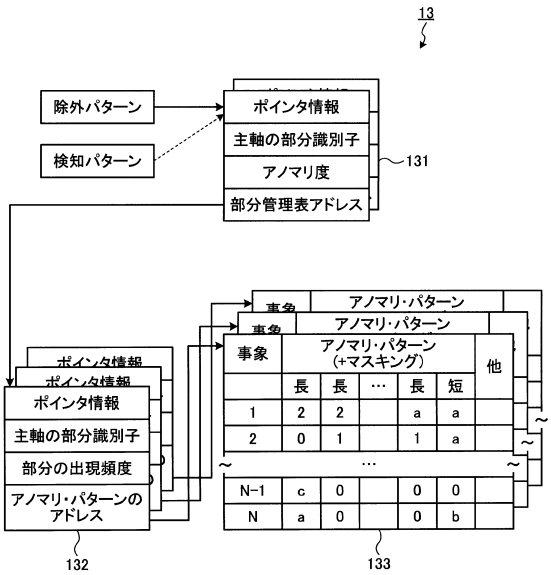


【図２】



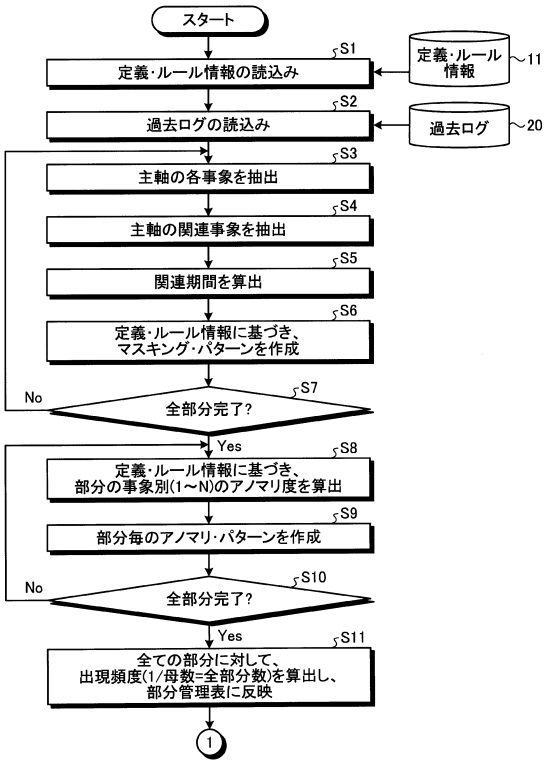
【図３】

学習モデルを説明する説明図



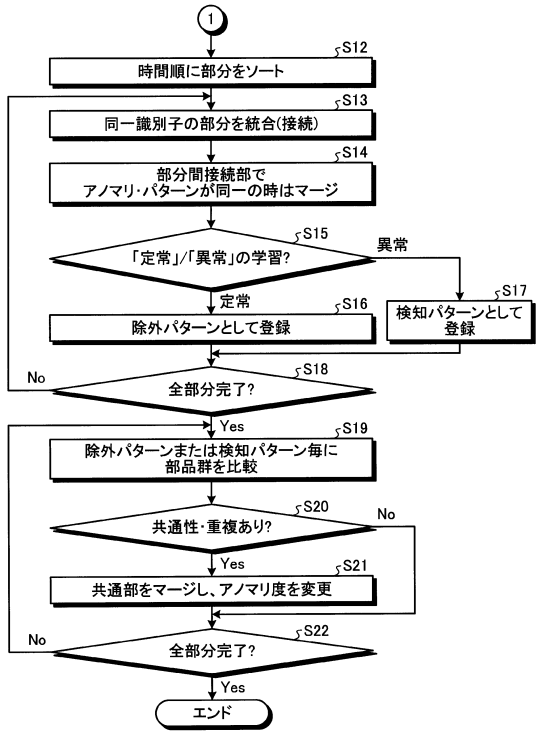
【図４－１】

学習モデルの構築にかかる処理の一例を示すフローチャート



【図４－２】

学習モデルの構築にかかる処理の一例を示すフローチャート



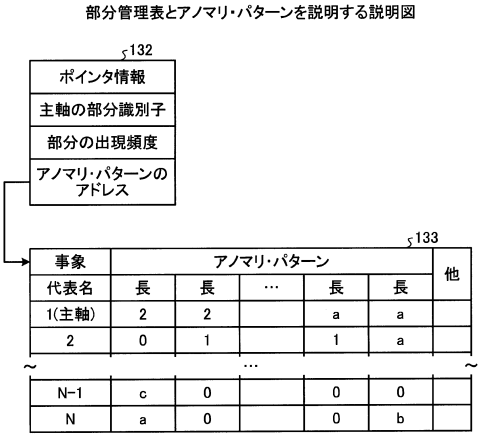
【図５】

定義・ルール情報を説明する説明図

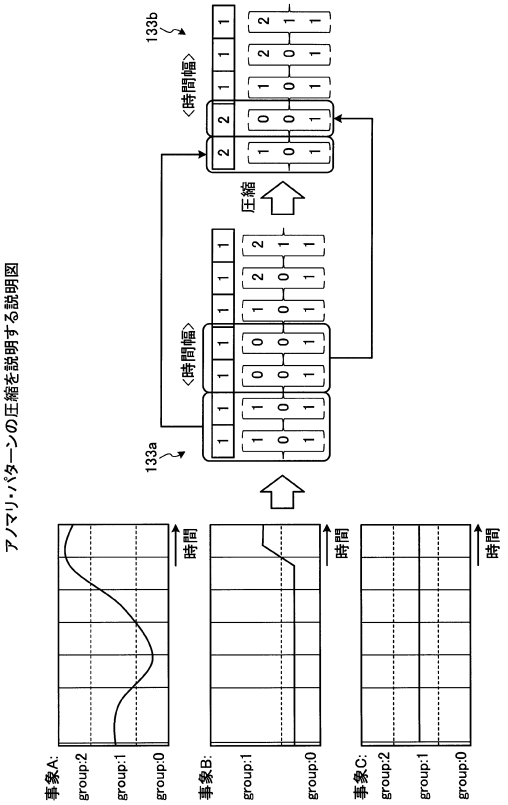
11

事象	各事象への適用ルール				他
	起点	終点	マスキング	アノマリ算出	
1=主軸	メール操作ログ	同左	(a)	ルール1	
2	プロセスログ等	同左	(a)	ルール2	
3	クリック等	同左	(b)	頻度	
～		…			～
N-1	Webアクセス等	同左	(c)	アクセス先	
N	通信パケット等	同左	(a)	長さ混在	

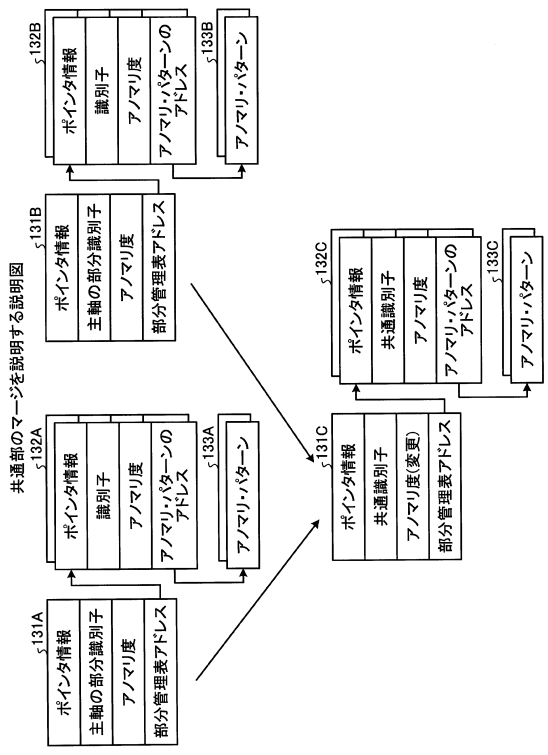
【図６】


部分管理表とアノマリ・パターンを説明する説明図
132
ポインタ情報
主軸の部分識別子
部分の出現頻度
アノマリ・パターンのアドレス
133
事象
アノマリ・パターン
他
代表名
長
1(主軸)
2
0
1
a
N-1
c
N
a
b

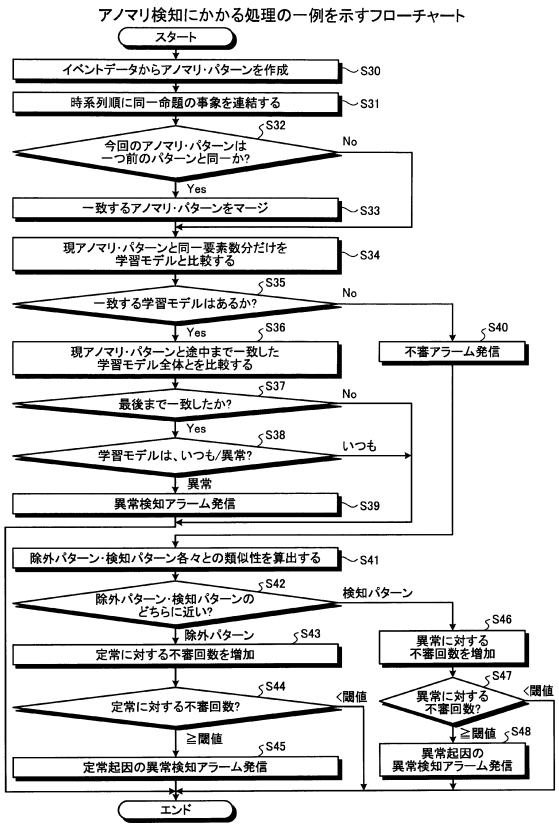
【図７】


アノマリ・パターンの圧縮を説明する説明図
133b
〈時間幅〉
圧縮
133a
時間
事象A:
group:2
group:1
group:0
事象B:
group:1
group:0
事象C:
group:2
group:1
group:0

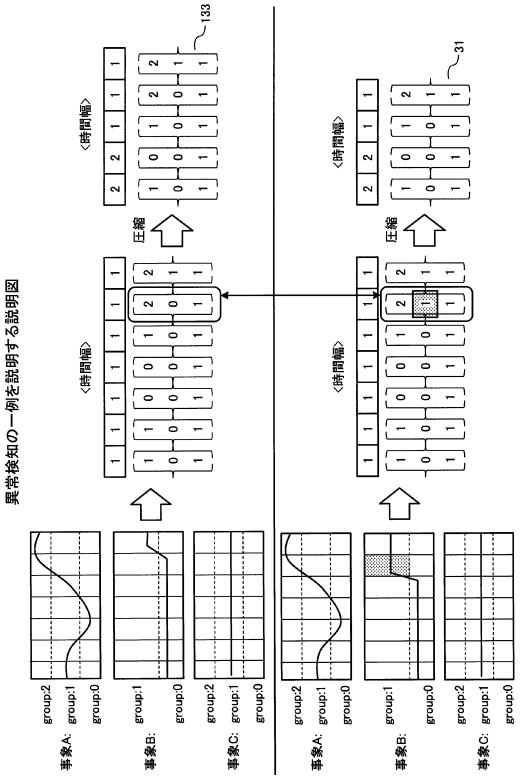
【図８】


共通部のマージを説明する説明図
132B
ポインタ情報
識別子
アノマリ度
アノマリ・パターンのアドレス
133B
アノマリ・パターン
131B
ポインタ情報
主軸の部分識別子
アノマリ度
部分管理表アドレス
132C
ポインタ情報
共通識別子
アノマリ度
アノマリ・パターンのアドレス
133C
アノマリ・パターン
132A
ポインタ情報
識別子
アノマリ度
アノマリ・パターンのアドレス
133A
アノマリ・パターン
131C
ポインタ情報
共通識別子
アノマリ度(変更)
部分管理表アドレス
131A
ポインタ情報
主軸の部分識別子
アノマリ度
部分管理表アドレス

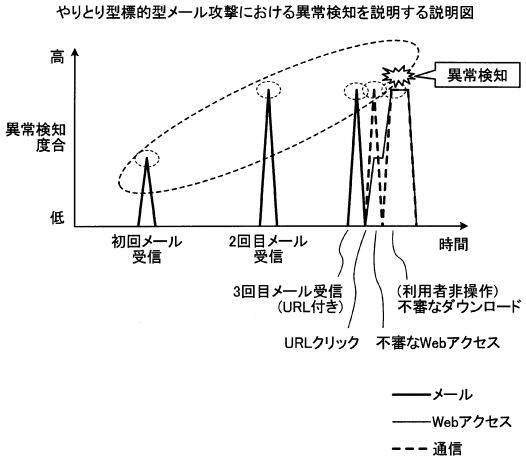
【図９】


アノマリ検知にかかる処理の一例を示すフローチャート
スタート
イベントデータからアノマリ・パターンを作成
S30
時系列順に同一命題の事象を連結する
S31
S32
今回のアノマリ・パターンは一つ前のパターンと同一か?
No
Yes
一致するアノマリ・パターンをマージ
S33
現アノマリ・パターンと同一要素数分だけを学習モデルと比較する
S34
S35
一致する学習モデルはあるか?
No
Yes
S36
現アノマリ・パターンと途中まで一致した学習モデル全体とを比較する
S40
不審アラーム発信
S37
最後まで一致したか?
No
Yes
S38
学習モデルは、いつも/異常?
いつも
異常
異常検知アラーム発信
S39
除外パターン・検知パターン各々との類似性を算出する
S41
S42
除外パターン・検知パターンのどちらに近い?
検知パターン
除外パターン
S43
定常に対する不審回数を増加
S46
異常に対する不審回数を増加
S44
定常に対する不審回数?
<閾値
≧閾値
S47
異常に対する不審回数?
<閾値
≧閾値
S48
異常起因の異常検知アラーム発信
S45
定常起因の異常検知アラーム発信
エンド

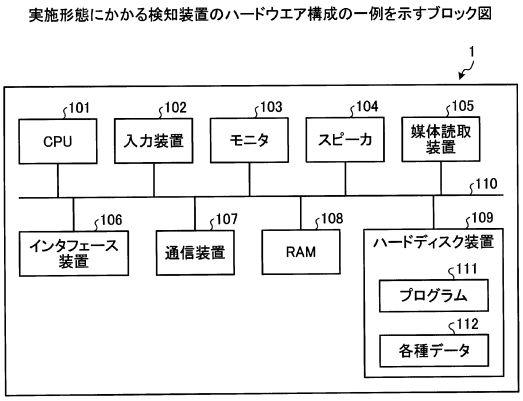
【図１０】


異常検知の一例を説明する説明図
133
31
〈時間幅〉
圧縮
group:2
group:1
group:0
事象A:
事象B:
事象C:

【図１１】


やりとり型標的型メール攻撃における異常検知を説明する説明図
高
異常検知度合
低
異常検知
初回メール受信
2回目メール受信
時間
3回目メール受信（URL付き）
（利用者非操作）不審なダウンロード
URLクリック
不審なWebアクセス
メール
Webアクセス
通信

【図１２】


実施形態にかかる検知装置のハードウエア構成の一例を示すブロック図
1
101 CPU
102 入力装置
103 モニタ
104 スピーカ
105 媒体読取装置
110
106 インタフェース装置
107 通信装置
108 RAM
109 ハードディスク装置
111 プログラム
112 各種データ

フロントページの続き

(72)発明者　小▲柳▼　佑介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

合議体
審判長　田中　秀人
審判官　山崎　慎一
審判官　須田　勝巳

(56)参考文献　特表２０１４－５３１６４７（ＪＰ，Ａ）
特開２０１１－６５４４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/55
G06F11/34