

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7052602号
(P7052602)

(45)発行日 令和4年4月12日(2022.4.12)

(24)登録日 令和4年4月4日(2022.4.4)

(51)国際特許分類	F I
H 0 4 L 43/00 (2022.01)	H 0 4 L 43/00
G 0 6 F 21/56 (2013.01)	G 0 6 F 21/56 3 6 0

請求項の数 6 (全17頁)

(21)出願番号	特願2018-126189(P2018-126189)	(73)特許権者	000004226 日本電信電話株式会社 東京都千代田区大手町一丁目5番1号
(22)出願日	平成30年7月2日(2018.7.2)	(74)代理人	110002147 特許業務法人酒井国際特許事務所
(65)公開番号	特開2020-5234(P2020-5234A)	(72)発明者	中津留 毅 東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
(43)公開日	令和2年1月9日(2020.1.9)	(72)発明者	佐藤 友康 東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
審査請求日	令和2年10月26日(2020.10.26)	(72)発明者	南 拓也 東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
		(72)発明者	藤木 直人 最終頁に続く

(54)【発明の名称】 生成装置、生成方法及び生成プログラム

(57)【特許請求の範囲】

【請求項1】

ネットワークにおける通信に関する複数の項目を持つ情報を基に、前記ネットワークの異常を検知する検知部と、
前記検知部によって異常が検知された場合、前記情報のそれぞれに対応する異常原因としてIDSシグネチャを特定する特定部と、
前記情報が持つ項目の値と、発アドレス分類及び着アドレス分類と、前記特定部によって特定された異常原因とを基に、前記情報の所定の集合ごとの異常原因のパターンを生成するパターン生成部と、
を有することを特徴とする生成装置。

【請求項2】

前記パターン生成部は、前記情報が持つ項目の値から生成されたメタ情報を基に、前記情報に対応するフローごとの異常原因の組み合わせを表すパターンであって、各異常原因に対応するフローの数が複数であることを表現可能なパターンを生成することを特徴とする請求項1に記載の生成装置。

【請求項3】

前記パターン生成部によって生成されたパターンを記憶する記憶部を参照し、前記パターン生成部が第1のパターンを生成した場合、前記第1のパターンと前記記憶部に記憶されたパターンとが一致するか否かを判定する判定部をさらに有することを特徴とする請求項1に記載の生成装置。

【請求項 4】

ネットワークの正常動作時の通信に関する情報を基に、前記ネットワークの異常を検知するための検知モデルを生成する検知モデル生成部と、
前記ネットワークの通信に関する情報を基に、前記ネットワークの異常原因を特定するための特定モデルを生成する特定モデル生成部と、
をさらに有し、
前記検知部は、検知対象の情報を基に、前記検知モデルを用いて前記ネットワークの異常を検知し、
前記特定部は、前記検知部によって異常が検知された場合、前記特定モデルを用いて、前記検知対象の情報のそれぞれに対応する異常原因を特定し、
前記パターン生成部は、前記検知対象の情報のフロー単位の集合ごとの異常原因のパターンを生成することを特徴とする請求項 1 に記載の生成装置。

10

【請求項 5】

コンピュータによって実行される生成方法であって、
ネットワークにおける通信に関する複数の項目を持つ情報を基に、前記ネットワークの異常を検知する検知工程と、
前記検知工程によって異常が検知された場合、前記情報のそれぞれに対応する異常原因として IDS シグネチャ を特定する特定工程と、
前記情報が持つ項目の値と、発アドレス分類及び着アドレス分類と、前記特定工程によって特定された異常原因とを基に、前記情報の所定の集合ごとの異常原因のパターンを生成するパターン生成工程と、
を含むことを特徴とする生成方法。

20

【請求項 6】

コンピュータを、請求項 1 から 4 のいずれか 1 項に記載の生成装置として機能させるための生成プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、生成装置、生成方法及び生成プログラムに関する。

【背景技術】

30

【0002】

PC (Personal Computer) 等の機器におけるマルウェア感染等による異常を検知する方法として、機器の挙動パターンと既知の異常パターンを比較して異常を検知するブラックリスト方式と、機器の挙動パターンと正常状態の挙動パターンを比較して異常を検知するホワイトリスト方式とが従来から実用化されている。

【0003】

また、システム負荷情報を基に異常判定を行い、異常が発生した機器で実行されている機能を特定しブラックリストに登録する一方、異常が発生していない機器で実行されている機能をホワイトリストに登録する技術が知られている。

【先行技術文献】

40

【特許文献】

【0004】

【文献】特開 2017-84296 号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、従来の技術には、異常原因の特定を効率的に行うことができない場合があるという問題がある。例えば、ブラックリスト方式では予め異常パターンが定められているため、定められた異常パターンと合致した場合に異常原因を特定可能であるが、未知マルウェア等による異常の検知は困難である。一方、ホワイトリスト方式では正常状態と合

50

致しない挙動パターンは全て異常として検知可能であるが、異常原因の特定は困難である。

【０００６】

また、異常が発生した機器で実行されている機能を特定しブラックリストに登録し、異常が発生していない機器で実行されている機能をホワイトリストに登録する技術では、異常動作をしている機能を特定できるに過ぎず、異常原因を特定することは困難である。

【課題を解決するための手段】

【０００７】

上述した課題を解決し、目的を達成するために、本発明の生成装置は、ネットワークにおける通信に関する複数の項目を持つ情報を基に、前記ネットワークの異常を検知する検知部と、前記検知部によって異常が検知された場合、前記情報のそれぞれに対応する異常原因を特定する特定部と、前記情報が持つ項目の値と、前記特定部によって特定された異常原因とを基に、前記情報の所定の集合ごとの異常原因のパターンを生成するパターン生成部と、を有することを特徴とする。

【発明の効果】

【０００８】

本発明によれば、異常原因の特定を効率的に行うことができる。

【図面の簡単な説明】

【０００９】

【図１】図１は、第１の実施形態に係る生成システムの構成の一例を示す図である。

【図２】図２は、第１の実施形態に係る生成装置の構成の一例を示す図である。

【図３】図３は、第１の実施形態に係るＲow情報の一例を示す図である。

【図４】図４は、第１の実施形態に係るインシデントパターンの生成について説明するための図である。

【図５】図５は、第１の実施形態に係るインシデントパターンの判定について説明するための図である。

【図６】図６は、第１の実施形態に係るインシデントパターンの要素の一例を示す図である。

【図７】図７は、第１の実施形態に係る生成装置の初期設定フェーズにおける処理の流れを示すフローチャートである。

【図８】図８は、第１の実施形態に係る生成装置の運用フェーズにおける処理の流れを示すフローチャートである。

【図９】図９は、第１の実施形態に係るインシデントパターンを生成する処理の流れを示すフローチャートである。

【図１０】図１０は、生成プログラムを実行するコンピュータの一例を示す図である。

【発明を実施するための形態】

【００１０】

以下に、本願に係る生成装置、生成方法及び生成プログラムの実施形態を図面に基づいて詳細に説明する。なお、本発明は、以下に説明する実施形態により限定されるものではない。

【００１１】

〔第１の実施形態の構成〕

まず、図１を用いて、第１の実施形態に係る生成システムの構成について説明する。図１は、第１の実施形態に係る生成システムの構成の一例を示す図である。図１に示すように、生成システム１は、生成装置１０、ゲートウェイ装置２０及び機器３０を有する。また、生成装置１０及びゲートウェイ装置２０は、ネットワーク２を介して通信可能に接続されている。また、機器３０は、ゲートウェイ装置２０と通信可能に接続されている。

【００１２】

例えば、機器３０は、ＰＣ、スマートフォン等の端末装置である。ネットワーク２は、例えばインターネットである。また、ゲートウェイ装置２０は、機器３０と同一のＬＡＮ（Local Area Network）に接続され、機器３０によって行われた通信の通信ログ又は機

10

20

30

40

50

器 3 0 の動作ログをキャプチャする。また、生成装置 1 0 は、ネットワーク 2 における通信に関する情報を取得し、異常の検知及び異常原因の特定を行う。以降の説明では、通信に関する情報を通信特徴量と表記する場合がある。

【 0 0 1 3 】

生成装置 1 0 が取得する通信特徴量には、例えば、通信におけるデータの送信元又は宛先のアドレス及びポート番号が含まれる。また、通信特徴量には、通信の継続時間及びバイト数が含まれていてもよい。

【 0 0 1 4 】

図 2 を用いて、第 1 の実施形態に係る生成装置の構成について説明する。図 2 は、第 1 の実施形態に係る生成装置の構成の一例を示す図である。図 2 に示すように、生成装置 1 0 は、通信部 1 1、入力部 1 2、出力部 1 3、記憶部 1 4 及び制御部 1 5 を有する。

【 0 0 1 5 】

通信部 1 1 は、ネットワークを介して、他の装置との間でデータ通信を行う。例えば、通信部 1 1 は N I C (Network Interface Card) である。入力部 1 2 は、ユーザからのデータの入力を受け付ける。入力部 1 2 は、例えば、マウスやキーボード等の入力装置である。出力部 1 3 は、画面の表示等により、データを出力する。出力部 1 3 は、例えば、ディスプレイ等の表示装置である。

【 0 0 1 6 】

また、入力部 1 2 及び出力部 1 3 は、それぞれ、入力インタフェース及び出力インタフェースであってもよい。例えば、入力部 1 2 及び出力部 1 3 は、生成装置 1 0 に接続された他の装置及びメモリカードや U S B (Universal Serial Bus) メモリ等のメディアとの間でデータの入力及び出力を行う。また、入力部 1 2 は、通信部 1 1 が受信したデータを入力データとして受け付けてもよい。また、出力部 1 3 は、通信部 1 1 に対してデータを出力してもよい。

【 0 0 1 7 】

記憶部 1 4 は、H D D (Hard Disk Drive)、S S D (Solid State Drive)、光ディスク等の記憶装置である。なお、記憶部 1 4 は、R A M (Random Access Memory)、フラッシュメモリ、N V S R A M (Non Volatile Static Random Access Memory) 等のデータを書き換え可能な半導体メモリであってもよい。記憶部 1 4 は、生成装置 1 0 で実行される O S (Operating System) や各種プログラムを記憶する。さらに、記憶部 1 4 は、プログラムの実行で用いられる各種情報を記憶する。また、記憶部 1 4 は、検知モデル 1 4 1、特定モデル 1 4 2 及び異常原因 D B 1 4 3 を記憶する。

【 0 0 1 8 】

検知モデル 1 4 1 は、ネットワーク 2 の異常を検知するためのモデルである。検知モデル 1 4 1 は、機器 3 0 が異常状態であることを検知するためのモデルであってもよい。例えば、検知モデル 1 4 1 は、セキュリティ製品 (I P S (Intrusion Prevention System), I D S (Intrusion Detection and Prevention), W A F (Web Application Firewall) 等) のシグネチャを利用して検知することや、通信特徴量からアノマリスコアを計算する関数及びパラメータを含む。

【 0 0 1 9 】

特定モデル 1 4 2 は、機器 3 0 の異常原因を特定するためのモデルである。例えば、セキュリティ製品 (I P S, I D S, W A F 等) のシグネチャや、異常原因及び異常原因を特定するための通信特徴量が記載された機械学習の学習済みのモデルである。

【 0 0 2 0 】

異常原因 D B 1 4 3 は、異常原因を特定するための情報を記憶する。異常原因 D B 1 4 3 は、特定モデル 1 4 2 による異常原因の特定に用いられるデータ及び後述するインシデントパターンを記憶する。

【 0 0 2 1 】

例えば、異常原因 D B 1 4 3 は、図 3 に示す R o w 情報を含む情報を記憶する。図 3 は、第 1 の実施形態に係る R o w 情報の一例を示す図である。図 3 に示すように、R o w 情報

10

20

30

40

50

には、発アドレス、着アドレス、発ポート、着ポート、継続時間、プロトコル、登りバイト数、下りバイト数、通信タイプが含まれる。例えば、Row情報は、通信特徴量に含まれるデータそのものである。なお、Row情報は、ネットワーク2における通信に関する複数の項目を持つ情報の一例である。

【0022】

また、異常原因DB143は、Row情報のそれぞれに対応する異常原因であるIDSシグネチャを記憶する。IDSシグネチャは、生成装置10が、特定モデル142を用いてRow情報を基に生成したものであってもよいし、他の装置等から取得したものであってもよい。例えば、IDSシグネチャは、IPアドレスがインターネットネットワークのものであるか外部のものであるかを、構成管理情報を基に特定した情報である。また、例えば、IDSシグネチャは、脅威のあるIPアドレスを記したブラックリストDBから取得した情報である。

10

【0023】

さらに、異常原因DB143は、環境の変化等で変化しない項目の値から生成されたメタ情報を記憶する。例えば、同じマルウェアが複数のサイトに感染する場合を考える。このとき、感染の拡大又はマルウェアの駆除等の影響で、感染端末があるローカルの情報は変化することが考えられる。一方で、同じマルウェアであれば、アクセスする先は頻繁には変化しないことが考えられる。例えば、図3の(2)、(3)及び(4)では、感染した端末11.11.11.1から11.11.11.2~4へのログインが試行されている。このような場合、感染した端末のIPアドレスや、ログインを試みる端末はマルウェアの入り込んだ環境に依存しており、同じでないことが多い。一方で、(7)及び(8)では、感染した端末は、端末99.99.99.3からマルウェアをダウンロードしている。このような場合、感染した端末は環境依存だが、マルウェアのダウンロード先のURLやIPアドレスは同じアドレスになることが多い。このように、アドレスの分類によって、IPアドレス自体に意味があるかが変化することが知られている。

20

【0024】

また、異常原因DB143は、フロー単位のインシデントパターンを記憶する。ここで、図3の(1)~(10)をフロー単位のRow情報であるとする。このとき、例えば、異常原因DB143は、(1)~(10)のRow情報に対応して一意に生成されるインシデントパターンを記憶する。なお、インシデントパターンは、後述するパターン生成部155によって生成される。

30

【0025】

制御部15は、生成装置10全体を制御する。制御部15は、例えば、CPU (Central Processing Unit)、GPU (Graphics Processing Unit)、TPU (Tensor Processing Unit)、MPU (Micro Processing Unit)等の電子回路や、ASIC (Application Specific Integrated Circuit)、FPGA (Field Programmable Gate Array)等の集積回路である。また、制御部15は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、内部メモリを用いて各処理を実行する。また、制御部15は、各種のプログラムが動作することにより各種の処理部として機能する。例えば、制御部15は、検知モデル生成部151、検知部152、特定モデル生成部153、特定部154、パターン生成部155及び判定部156を有する。

40

【0026】

検知モデル生成部151は、ネットワーク2の正常動作時の通信に関する情報を基に、ネットワーク2の異常を検知するための検知モデル141を生成する。例えば、検知モデル生成部151は、検知モデル141が、入力された検知対象のデータと正常データとが類似していないほど高いアノマリスコアを出力するように学習を行う。

【0027】

検知部152は、ネットワーク2における通信に関する複数の項目を持つ情報を基に、ネットワーク2の異常を検知する。例えば、検知部152は、検知対象の情報を基に、検知モデル141を用いてネットワーク2の異常を検知する。ここで、検知対象の情報は、R

50

ow情報であってもよい。

【0028】

例えば、検知部152は、検知対象の情報を検知モデル141に入力し、検知モデル141によって出力されたアノマリスコアが閾値以上である場合、ネットワーク2の異常を検知する。また、検知モデル141がシグネチャである場合は、検知部152は、シグネチャマッチングにより異常を検知することができる。また、図3に示すように、検知部152は、異常を検知した際のメタ情報を、IDSシグネチャとして異常原因DB143に格納する。例えば、前述のセキュリティ製品又は検知モデル141は、フローごとに、検知した異常を分類することができる。検知部152は、そのような分類をIDSシグネチャとすることができる。

10

【0029】

特定モデル生成部153は、ネットワーク2の通信に関する情報を基に、ネットワーク2の異常原因を特定するための特定モデル142を生成する。例えば、特定モデル生成部153は、異常原因DB143を基に、特定モデル142が、入力された通信特徴量と類似する通信特徴量に対応付けられた異常原因を出力するように学習を行う。

【0030】

特定部154は、検知部152によって異常が検知された場合、情報のそれぞれに対応する異常原因を特定する。例えば、特定部154は、検知部152によって異常が検知された場合、特定モデル142を用いて、検知対象の情報のそれぞれに対応する異常原因を特定する。例えば、特定部154は、検知部152によって異常が検知された場合、検知対象の情報を特定モデル142に入力し、特定モデル142によって出力された異常原因を取得する。また、特定モデル142がシグネチャである場合は、特定部154は、シグネチャマッチングにより異常原因を特定することができる。

20

【0031】

パターン生成部155は、通信特徴量を持つ項目の値と、特定部154によって特定された異常原因とを基に、通信特徴量の所定の集合ごとの異常原因のパターンを生成する。このとき、パターン生成部155は、情報が持つ項目の値から生成されたメタ情報を基にパターンを生成してもよい。また、パターン生成部155は、検知対象の情報のフロー単位の集合ごとの異常原因のパターンを生成することができる。以降の説明では、パターン生成部155によって生成されるパターンをインシデントパターンと表記する場合がある。

30

【0032】

ここで、図4を用いて、インシデントパターンの生成について説明する。図4は、第1の実施形態に係るインシデントパターンの生成について説明するための図である。図4は、フローに含まれる通信の内容を模式的に表したものである。

【0033】

図4の(1)は、機器30が、C2サーバであるC2-1に対してhttpによる通信を行ったことを示している。また、(2)～(4)は、機器30のうちの1つが、他の機器30に対してtelnetによるログインの試みを行ったことを示している。また、(5)及び(6)は、機器30が、C2サーバであるC2-2との間でtelnetによる通信を行ったことを示している。また、(7)及び(8)は、機器30が、マルウェア配信サイトを提供する配布サーバとの間でhttpによる通信を行ったことを示している。また、(9)及び(10)は、機器30が、一般WebサーバであるTaagetとの間でhttpによる通信を行ったことを示している。

40

【0034】

ここで、検知部152が、図4に示すフローに含まれる通信が行われた際の通信特徴量を基に異常を検知したものとする。このとき、特定部154は、(1)～(10)の通信に対応する通信特徴量のそれぞれについて、異常原因を特定する。

【0035】

そして、図3に示すように、パターン生成部155は、通信特徴量及び特定された異常原因を収集し、Row情報及びIDSシグネチャとして異常原因DB143に格納する。さ

50

らに、パターン生成部 155 は、所定の情報を基にメタ情報を生成する。

【0036】

ここで、例えば、図 3 の (1) の I D S シグネチャ、発アドレス分類及び着アドレス分類は、それぞれ「C 2 通信」、「網内アドレス」及び「C 2 サーバ」である。また、(2) 及び (3) の I D S シグネチャ、発アドレス分類及び着アドレス分類は、それぞれ「ログイン試行／成功」、「網内アドレス」及び「網内アドレス」である。また、(4) の I D S シグネチャ、発アドレス分類及び着アドレス分類は、それぞれ「ログイン試行／失敗」、「網内アドレス」及び「網内アドレス」である。これにより、パターン生成部 155 は、(1)～(4)を、C 2 サーバの指示によるスキャン (C 2 - S c a n) によるものと判定する。

10

【0037】

同様に、パターン生成部 155 は、(5)～(8)を、C 2 サーバの指示によるダウンロード (C 2 - D o w n l o a d) によるものと判定する。また、パターン生成部 155 は、(9)及び(10)を、C 2 サーバの指示による D o s 攻撃 (C 2 - D o s) によるものと判定する。

【0038】

パターン生成部 155 は、情報が持つ項目の値から生成されたメタ情報を基に、情報に対応するフローごとの異常原因の組み合わせを表すパターンであって、各異常原因に対応するフローの数が複数であることを表現可能なパターンを生成する。例えば、パターン生成部 155 は、「C 2 - S c a n * C 2 - D o w n l o a d C 2 - D o s *」というインシデントパターンを生成する。

20

【0039】

ここで、「*」は、複数のフローが存在することを示している。例えば、C 2 によるスキャンでは、スキャンするポート数やネットワークに存在する機器の台数によりフローが変化することがある。また、D o S 攻撃では、発生する H T T P フローの数は、機器の性能等により一定ではない。このため、インシデントパターンにおいてフローの数を限定してしまうと、同様のインシデントパターンが存在したとしても、フローの数の違いにより比較及び検索ができないことが考えられる。そこで、パターン生成部 155 は、インシデントパターンの比較及び検索を容易にするため、複数のフローを束ね抽象化したインシデントパターンを生成する。なお、「C 2 - S c a n * C 2 - D o w n l o a d C 2 - D o s *」は、「複数の送信元からのスキャンが発生した後、C 2 サーバからのダウンロードが行われ、複数の送信元からの D o s 攻撃が始まった」ということを意味している。なお、「*」は、1を含む任意の数のフローが存在することを示すものであってもよい。

30

【0040】

判定部 156 は、パターン生成部 155 によって生成されたパターンを記憶する記憶部 14 を参照し、パターン生成部 155 が第 1 のパターンを生成した場合、第 1 のパターンと記憶部 14 に記憶されたパターンとが一致するか否かを判定する。つまり、判定部 156 は、パターン生成部 155 によって新たに生成されたインシデントパターンが、過去に生成されたインシデントパターンと一致するか否かを判定することができる。

【0041】

図 5 は、第 1 の実施形態に係るインシデントパターンの判定について説明するための図である。図 5 の (11) は、機器 30 が、C 2 サーバである C 2 - 3 に対して h t t p による通信を行ったことを示している。また、(12) は、機器 30 のうちの 1 つが、他の機器 30 に対して t e l n e t によるログインの試みを行ったことを示している。また、(13) は、機器 30 が、C 2 サーバである C 2 - 4 との間で t e l n e t による通信を行ったことを示している。また、(14) は、機器 30 が、マルウェア配信サイトを提供する W e b s e r v e r 2 との間で h t t p による通信を行ったことを示している。また、(16) は、機器 30 が、一般 W e b サーバである T a e g e t 2 との間で h t t p による通信を行ったことを示している。

40

【0042】

50

図4と図5を比較すると、ログインを試みられた機器30の数、C2サーバやマルウェア配信サイトを提供するサーバが異なる。一方で、「任意の送信元からのスキャンが発生した」こと、「C2サーバからのダウンロードが行われた」こと等は共通している。このため、パターン生成部155は、図5の例からも、図4の例からと同様に、「C2-Scan* C2-Download C2-Dos*」というインシデントパターンを生成する。このため、判定部156は、図5の例から生成されたインシデントパターンが、過去に図4の例から生成されたインシデントパターンと一致するものであると判定することができる。

【0043】

ここで、パターン生成部155は、図6に示すような情報を参照することで、「C2-Scan」、「C2-Download」、「C2-Dos」といったインシデントパターンの要素を判定することができる。図6は、第1の実施形態に係るインシデントパターンの要素の一例を示す図である。例えば、図6の(b)は、「C2-Scan*」というパターンが、C2との通信後に複数回のScanが発生するものであることを示している。また、図6の(c)は、「C2-Upload」というパターンが、C2との通信後にUploadが発生するものであることを示している。

【0044】

また、出力部13は、検知対象の通信特徴量及び異常原因を出力する。このとき、出力部13は、パターン生成部155によって生成されたインシデントパターンを異常原因に含めて出力する。ここで、出力部13によって出力された情報に対しては、インシデントレスポンスが行われる。例えば、インシデントレスポンスは、システムの管理者が出力部13によって出力された情報を参考に、異常原因を特定することである。そして、入力部12は、インシデントレスポンスによって特定された異常原因の入力を受け付ける。インシデントレスポンスによって特定される異常原因は、インシデントパターンと同様のデータ形式で表されていてもよい。

【0045】

ここで、生成装置10が特定した異常原因と、インシデントレスポンスによって特定された異常原因とが同一である場合と同一でない場合とが考えられる。このとき、生成装置10は、インシデントレスポンスによって特定された異常原因を優先して異常原因DB143に格納する。

【0046】

そして、特定モデル生成部153は、さらに特定モデル142の生成を行う。これにより、生成装置10は、インシデントレスポンスの結果を特定モデル142に反映させることができる。

【0047】

【第1の実施形態の処理】

図7及び8を用いて、生成装置10の処理の流れを説明する。生成装置10の処理は、大きく初期設定フェーズと運用フェーズに分けられる。初期設定フェーズにおいて、生成装置10は、主に収集又は初期学習を行う。また、運用フェーズにおいて、生成装置10は、主に機器の異常検知及び異常原因の特定を行う。また、検知モデル141及び特定モデル142は、通信特徴量だけでなく、機器30の動作ログを用いた異常の検知及び異常原因の特定を行うことができるものとする。また、動作ログは、通信特徴量と同様に異常原因DB143に記憶されるものとする。

【0048】

図7は、第1の実施形態に係る生成装置の初期設定フェーズにおける処理の流れを示すフローチャートである。図8に示すように、まず、特定モデル生成部153は、異常原因DB143に異常原因の通信特徴量又は動作ログが存在するか否かを確認する(ステップS101)。

【0049】

ここで、異常原因DB143に異常原因の通信特徴量又は動作ログが存在する場合(ステ

10

20

30

40

50

ップ S 1 0 1、Y e s)、特定モデル生成部 1 5 3 は、異常原因の収集又は初期学習を行い、特定モデル 1 4 2 を生成する(ステップ S 1 0 2)。一方、異常原因 D B 1 4 3 に異常原因の通信特徴量又は動作ログが存在しない場合(ステップ S 1 0 1、N o)、特定モデル生成部 1 5 3 は、異常原因の収集又は初期学習を行わない。このように、特定モデル生成部 1 5 3 は、異常原因 D B 1 4 3 に異常原因と通信特徴量又は動作ログとが記憶されている場合にのみ特定モデル 1 4 2 を生成することとしてもよい。

【0050】

次に、検知モデル生成部 1 5 1 は、機器の正常動作時の通信特徴量又は動作ログを基に、正常動作の収集又は初期学習を行い、検知モデル 1 4 1 を生成する(ステップ S 1 0 3)。なお、例えば、初期学習は、正常データ又は異常原因 D B 1 4 3 に記憶された異常原因と通信特徴量又は動作ログとを基に、検知モデル 1 4 1 又は特定モデル 1 4 2 を新規生成する処理である。これに対して、例えば、再学習は、異常原因 D B 1 4 3 に記憶された異常原因と通信特徴量又は動作ログとであって、初期学習の際に記憶されていなかった異常原因と通信特徴量又は動作ログとを基に、特定モデル 1 4 2 を更新する処理である。

【0051】

図 8 は、第 1 の実施形態に係る生成装置の運用フェーズにおける処理の流れを示すフローチャートである。図 8 に示すように、まず、検知部 1 5 2 は、検知対象の機器 3 0 の通信特徴量又は動作ログを取得する(ステップ S 2 0 1)。次に、検知部 1 5 2 は、取得した通信特徴量又は動作ログを検知モデル 1 4 1 に入力する(ステップ S 2 0 2)。ここで、検知部 1 5 2 によって異常が検知されなかった場合(ステップ S 2 0 2、N o)、処理がステップ S 2 0 1 に戻され、検知部 1 5 2 は、次の検知対象の機器 3 0 の通信特徴量又は動作ログを取得する(ステップ S 2 0 1)。

【0052】

一方、検知部 1 5 2 によって異常が検知された場合(ステップ S 2 0 2、Y e s)、特定部 1 5 4 は、検知対象の機器 3 0 の通信特徴量又は動作ログを特定モデル 1 4 2 に入力し、異常原因を特定する(ステップ S 2 0 3)。なお、異常原因の特定処理については、後に図 9 を用いて説明する。

【0053】

そして、出力部 1 3 は、検知対象の機器 3 0 の通信特徴量又は動作ログと特定部 1 5 4 によって特定された異常原因を出力する(ステップ S 2 0 4)。そして、入力部 1 2 は、インシデントレスポンス結果の入力を受け付ける(ステップ S 2 0 5)。

【0054】

ここで、特定部 1 5 4 が特定した異常原因とインシデントレスポンス結果の異常原因が同一である場合(ステップ S 2 0 6、Y e s)、処理がステップ S 2 0 1 に戻され、検知部 1 5 2 は、次の検知対象の機器 3 0 の通信特徴量及び動作ログを取得する(ステップ S 2 0 1)。

【0055】

一方、特定部 1 5 4 が特定した異常原因とインシデントレスポンス結果の異常原因が同一でない場合(ステップ S 2 0 6、N o)、特定モデル生成部 1 5 3 は、インシデントレスポンス結果の異常原因を検知対象の機器 3 0 の通信特徴量又は動作ログとともに異常原因 D B 1 4 3 に格納する(ステップ S 2 0 7)。

【0056】

ここで、初期設定フェーズにおける異常原因の収集又は初期学習(図 7 のステップ S 1 0 2)が実行済みである場合(ステップ S 2 0 8、Y e s)、特定モデル生成部 1 5 3 は、異常原因 D B 1 4 3 から異常原因と通信特徴量又は動作ログとを取得し、異常原因の収集又は再学習を行う(ステップ S 2 0 9)。

【0057】

一方、初期設定フェーズにおける異常原因の初期学習(図 7 のステップ S 1 0 2)が実行済みでない場合(ステップ S 2 0 8、N o)、特定モデル生成部 1 5 3 は、異常原因 D B 1 4 3 から異常原因と通信特徴量又は動作ログとを取得し、異常原因の収集又は初期学習

10

20

30

40

50

を行う（ステップ S 2 1 0）。

【 0 0 5 8 】

異常原因の収集又は再学習（ステップ S 2 0 9）もしくは収集又は初期学習（ステップ S 2 1 0）が行われると、処理がステップ S 2 0 1 に戻され、検知部 1 5 2 は、次の検知対象の機器 3 0 の通信特徴量又は動作ログを取得する（ステップ S 2 0 1）。

【 0 0 5 9 】

図 9 を用いて、異常原因を特定する処理（図 8 のステップ S 2 0 3）について説明する。ここでは、生成装置 1 0 は、異常原因として、各通信特徴量の個別の異常原因と、インシデントパターンとを特定するものとする。図 9 は、第 1 の実施形態に係るインシデントパターンを生成する処理の流れを示すフローチャートである。

【 0 0 6 0 】

図 9 に示すように、まず、特定部 1 5 4 は、特定モデル 1 4 2 を用いて、各通信特徴量の個別の異常原因を特定する（ステップ S 3 0 1）。例えば、特定部 1 5 4 は、図 3 に示す IDS シグネチャを特定する。

【 0 0 6 1 】

次に、パターン生成部 1 5 5 は、検知対象の情報から Row 情報を収集し（ステップ S 3 0 2）、インシデントパターンを生成する（ステップ S 3 0 3）。さらに、判定部 1 5 6 は、パターン生成部 1 5 5 によって生成されたインシデントパターンが、過去に生成されたインシデントパターンのそれぞれと同一であるか否かを判定する（ステップ S 3 0 4）。そして、特定部 1 5 4 は、判定部 1 5 6 によって同一であると判定されたインシデントパターンを、異常原因として特定する（ステップ S 3 0 5）。

【 0 0 6 2 】

〔第 1 の実施形態の効果〕

生成装置 1 0 の検知部 1 5 2 は、ネットワーク 2 における通信に関する複数の項目を持つ情報を基に、ネットワーク 2 の異常を検知する。また、特定部 1 5 4 は、検知部 1 5 2 によって異常が検知された場合、情報のそれぞれに対応する異常原因を特定する。また、パターン生成部 1 5 5 は、情報が持つ項目の値と、特定部 1 5 4 によって特定された異常原因とを基に、情報の所定の集合ごとの異常原因のパターンを生成する。このように、生成装置 1 0 は、異常が検知された場合、所定の集合ごとのインシデントパターンを生成することができる。この結果、生成装置 1 0 によれば、異常原因の特定を効率的に行うことが可能になる。

【 0 0 6 3 】

例えば、生成装置 1 0 によって生成されたインシデントパターンは、システム管理者によるインシデントレスポンスの作成に役立つ。例えば、インシデントパターンが作成されず、通信特徴量ごとに特定された異常原因がシステム管理者に提供される場合を考える。このとき、システム管理者は、提供された異常原因を基に、過去に作成されたインシデントレスポンスの説明や対処法が記載されたレポートを検索する。ここで、提供された異常原因に、重複や検索に寄与しないものが含まれている場合、システム管理者はレポートの検索を効率的に行うことができない。

【 0 0 6 4 】

例えば、図 3 の（１）～（４）の IDS シグネチャに基づいて、「C 2 通信」、「ログイン試行」、「ログイン試行」、「ログイン試行」という一連の異常原因がシステム管理者に提供されたとする。このとき、過去に「C 2 通信」、「ログイン試行」、「ログイン試行」、「ログイン試行」という一連の異常原因が存在せず、「C 2 通信」、「ログイン試行」、「ログイン試行」という一連の異常原因のみが存在していたとする。この場合、システム管理者は、提供された一連の異常原因に完全一致するものを検索することができない。一方、生成装置 1 0 によれば、前述の一連の異常原因をいずれも同一のインシデントパターンとして提供することができる。このように、生成装置 1 0 は、システム管理者によるインシデントレスポンスを支援することができる。

【 0 0 6 5 】

パターン生成部 155 は、情報が持つ項目の値から生成されたメタ情報を基に、情報に対応するフローごとの異常原因の組み合わせを表すパターンであって、各異常原因に対応するフローの数が複数であることを表現可能なパターンを生成する。これにより、生成装置 10 は、フローの数が抽象化されたインシデントパターンを生成することができる。特に、異常原因の組み合わせが共通していて、フローの数が異なるインシデントパターン同士の比較及び検索が容易になる。

【0066】

判定部 156 は、パターン生成部 155 によって生成されたパターンを記憶する記憶部を参照し、パターン生成部 155 が第 1 のパターンを生成した場合、第 1 のパターンと記憶部に記憶されたパターンとが一致するか否かを判定する。これにより、生成装置 10 は、過去に生成した同一のインシデントパターンの存在をシステム管理者に通知することができるため、インシデントレスポンスを支援することができる。

10

【0067】

検知モデル生成部 151 は、ネットワーク 2 の正常動作時の通信に関する情報を基に、ネットワーク 2 の異常を検知するための検知モデル 141 を生成する。また、特定モデル生成部 153 は、ネットワーク 2 の通信に関する情報を基に、ネットワーク 2 の異常原因を特定するための特定モデル 142 を生成する。また、検知部 152 は、検知対象の情報を基に、検知モデル 141 を用いてネットワーク 2 の異常を検知する。また、特定部 154 は、検知部 152 によって異常が検知された場合、特定モデル 142 を用いて、検知対象の情報のそれぞれに対応する異常原因を特定する。また、パターン生成部 155 は、検知対象の情報のフロー単位の集合ごとの異常原因のパターンを生成する。このように、生成装置 10 は、異常が検知された場合、フロー単位でインシデントパターンを生成することができる。この結果、生成装置 10 は、システム管理者が解釈しやすいインシデントパターンを提供することができる。また、生成装置 10 は、インシデントパターンを生成しつつ、各モデルを強化していくことができる。

20

【0068】

〔その他の実施形態〕

生成システム 1 の装置構成は、図 1 のものに限られない。例えば、生成システム 1 は、検知モデル生成部 151 及び検知部 152 に相当する機能を備えた検知装置と、特定モデル生成部 153 及び特定部 154 に相当する機能を備えた生成装置とを有するものであってもよい。また、生成装置 10 は、ゲートウェイ装置 20 を経由せずに、直接機器 30 の通信特微量又は動作ログを取得してもよい。

30

【0069】

また、これまでの説明における「通信特微量又は動作ログ」は、「通信特微量」、「動作ログ」又は「通信特微量及び動作ログ」に置き換えてもよい。例えば、検知モデル 141 は、通信特微量及び動作ログの両方から生成されたものであってもよい。また、例えば、異常原因 DB 143 には、異常原因と動作ログが記憶されていてもよい。

【0070】

例えば、検知モデル生成部 151 は、機器 30 の正常動作時の動作ログを学習し、機器 30 が異常状態であることを検知するための検知モデル 141 を生成する。特定モデル生成部 153 は、機器 30 の異常原因ごとの通信特微量を収集又は学習し、機器 30 の異常原因を特定するための特定モデル 142 を生成する。検知部 152 は、検知モデル 141 と機器 30 から取得した動作ログとを基に、機器 30 が異常状態であることを検知する。特定部 154 は、検知部 152 によって機器 30 が異常状態であることが検知された場合、特定モデル 142 と機器 30 から取得した通信特微量とを基に、機器 30 の異常原因を特定する。

40

【0071】

〔システム構成等〕

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように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

50

示のものに限られず、その全部又は一部を、各種の負荷や使用状況等に応じて、任意の単位で機能的又は物理的に分散・統合して構成することができる。さらに、各装置にて行われる各処理機能は、その全部又は任意の一部が、CPU及び当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【0072】

また、本実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

10

【0073】

〔プログラム〕

一実施形態として、生成装置10は、パッケージソフトウェアやオンラインソフトウェアとして上記の異常検知処理及び異常原因の特定処理を実行する生成プログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記の生成プログラムを情報処理装置に実行させることにより、情報処理装置を生成装置10として機能させることができる。ここで言う情報処理装置には、デスクトップ型又はノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはサーバ機器、スマートフォン、携帯電話機やPHS（Personal Handyphone System）等の移動体通信端末、さらには、PDA（Personal Digital Assistant）等のスレート端末等がその範疇に含まれる。

20

【0074】

また、生成装置10は、ユーザが使用する端末装置をクライアントとし、当該クライアントに上記の異常検知処理及び異常原因の特定処理に関するサービスを提供する特定サーバ装置として実装することもできる。例えば、特定サーバ装置は、機器の通信特徴量及び動作ログを入力とし、異常状態であるか否か及び異常状態であった場合の異常原因を出力とする特定サービスを提供するサーバ装置として実装される。この場合、特定サーバ装置は、Webサーバとして実装することとしてもよいし、アウトソーシングによって上記の異常検知処理及び異常原因の特定処理に関するサービスを提供するクラウドとして実装することとしてもかまわない。

30

【0075】

図10は、生成プログラムを実行するコンピュータの一例を示す図である。コンピュータ1000は、例えば、メモリ1010、CPU1020を有する。また、コンピュータ1000は、ハードディスクドライブインタフェース1030、ディスクドライブインタフェース1040、シリアルポートインタフェース1050、ビデオアダプタ1060、ネットワークインタフェース1070を有する。これらの各部は、バス1080によって接続される。

【0076】

メモリ1010は、ROM（Read Only Memory）1011及びRAM1012を含む。ROM1011は、例えば、BIOS（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース1030は、ハードディスクドライブ1090に接続される。ディスクドライブインタフェース1040は、ディスクドライブ1100に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ1100に挿入される。シリアルポートインタフェース1050は、例えばマウス1110、キーボード1120に接続される。ビデオアダプタ1060は、例えばディスプレイ1130に接続される。

40

【0077】

ハードディスクドライブ1090は、例えば、OS1091、アプリケーションプログラム1092、プログラムモジュール1093、プログラムデータ1094を記憶する。す

50

なわち、生成装置 10 の各処理を規定するプログラムは、コンピュータにより実行可能なコードが記述されたプログラムモジュール 1093 として実装される。プログラムモジュール 1093 は、例えばハードディスクドライブ 1090 に記憶される。例えば、生成装置 10 における機能構成と同様の処理を実行するためのプログラムモジュール 1093 が、ハードディスクドライブ 1090 に記憶される。なお、ハードディスクドライブ 1090 は、SSD により代替されてもよい。

【0078】

また、上述した実施形態の処理で用いられる設定データは、プログラムデータ 1094 として、例えばメモリ 1010 やハードディスクドライブ 1090 に記憶される。そして、CPU 1020 は、メモリ 1010 やハードディスクドライブ 1090 に記憶されたプログラムモジュール 1093 やプログラムデータ 1094 を必要に応じて RAM 1012 に読み出して、上述した実施形態の処理を実行する。

【0079】

なお、プログラムモジュール 1093 やプログラムデータ 1094 は、ハードディスクドライブ 1090 に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ 1100 等を介して CPU 1020 によって読み出されてもよい。あるいは、プログラムモジュール 1093 及びプログラムデータ 1094 は、ネットワーク（LAN、WAN（Wide Area Network）等）を介して接続された他のコンピュータに記憶されてもよい。そして、プログラムモジュール 1093 及びプログラムデータ 1094 は、他のコンピュータから、ネットワークインタフェース 1070 を介して CPU 1020 によって読み出されてもよい。

【符号の説明】

【0080】

- 1 生成システム
- 2 ネットワーク
- 10 生成装置
- 11 通信部
- 12 入力部
- 13 出力部
- 14 記憶部
- 15 制御部
- 20 ゲートウェイ装置
- 30 機器
- 141 検知モデル
- 142 特定モデル
- 143 異常原因DB
- 151 検知モデル生成部
- 152 検知部
- 153 特定モデル生成部
- 154 特定部
- 155 パターン生成部
- 156 判定部

10

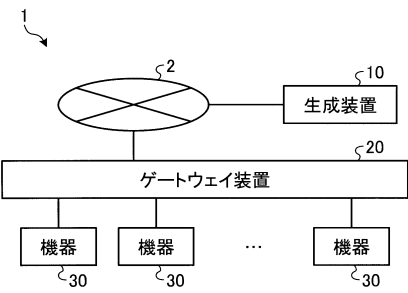
20

30

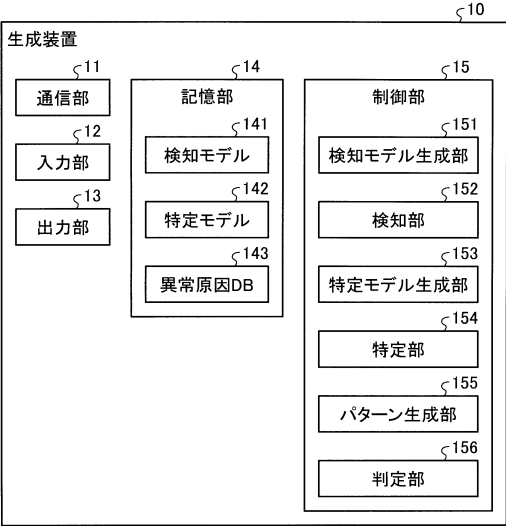
40

50

【図面】
【図 1】



【図 2】



10

20

【図 3】

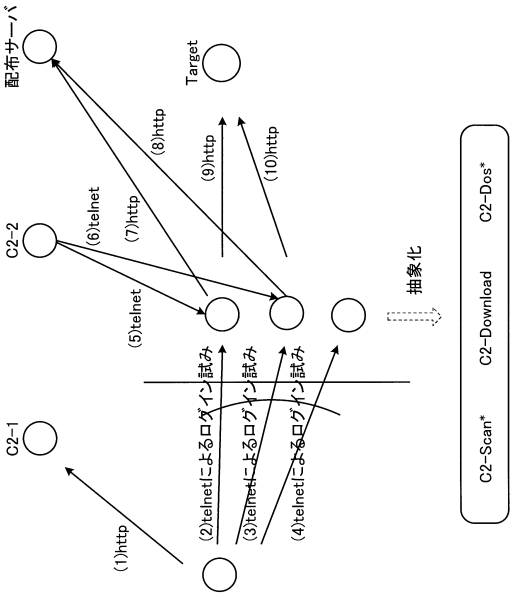
Row情報									
No	発アドレス	着アドレス	発ポート	着ポート	接続時間 ms	プロトコル	発り バイト数	下り バイト数	通信 タイプ
(1)	11.11.11.1	99.99.99.1	6332	80	300	TCP	100	10	HTTP
(2)	11.11.11.1	11.11.11.2	6600	23	100	TCP	10	10	TELNET
(3)	11.11.11.1	11.11.11.3	6500	23	105	TCP	19	10	TELNET
(4)	11.11.11.1	11.11.11.4	6700	23	98	TCP	10	10	TELNET
(5)	99.99.99.2	11.11.11.2	1235	23	90	TCP	10	10	TELNET
(6)	99.99.99.2	11.11.11.3	46543	23	60	TCP	11	11	TELNET
(7)	11.11.11.2	99.99.99.3	6500			TCP	10	10	HTTP
(8)	11.11.11.3	99.99.99.3	6700			TCP	10	10	HTTP
(9)	11.11.11.2	100.88.99.11	1235	80	80	TCP	10	10	HTTP
(10)	11.11.11.3	100.88.99.11	32353	80	80	TCP	10	10	HTTP

発アドレス	着アドレス	発ポート	着ポート	通信タイプ	検知アドレス	検知アドレス	検知アドレス
11.11.11.1	99.99.99.1	6332	80	HTTP	検知アドレス	検知アドレス	検知アドレス
11.11.11.1	11.11.11.2	6600	23	TELNET	検知アドレス	検知アドレス	検知アドレス
11.11.11.1	11.11.11.3	6500	23	TELNET	検知アドレス	検知アドレス	検知アドレス
11.11.11.1	11.11.11.4	6700	23	TELNET	検知アドレス	検知アドレス	検知アドレス
99.99.99.2	11.11.11.2	1235	23	TELNET	検知アドレス	検知アドレス	検知アドレス
99.99.99.2	11.11.11.3	46543	23	TELNET	検知アドレス	検知アドレス	検知アドレス
11.11.11.2	99.99.99.3	6500		HTTP	検知アドレス	検知アドレス	検知アドレス
11.11.11.3	99.99.99.3	6700		HTTP	検知アドレス	検知アドレス	検知アドレス
11.11.11.2	100.88.99.11	1235	80	HTTP	検知アドレス	検知アドレス	検知アドレス
11.11.11.3	100.88.99.11	32353	80	HTTP	検知アドレス	検知アドレス	検知アドレス

30

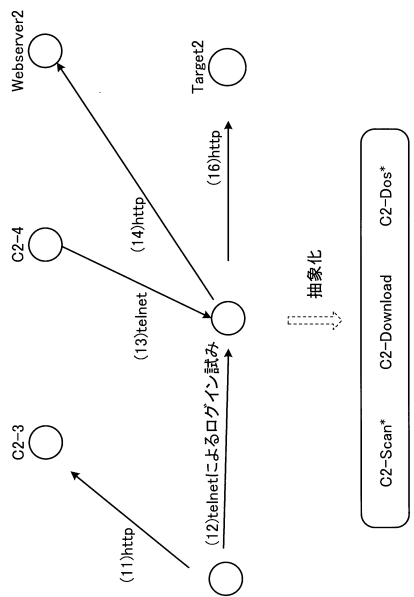
40

【図 4】

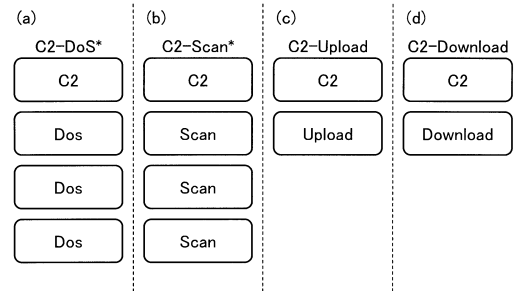


50

【図 5】



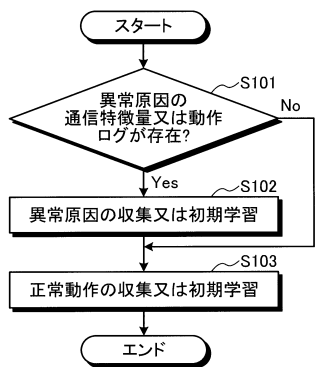
【図 6】



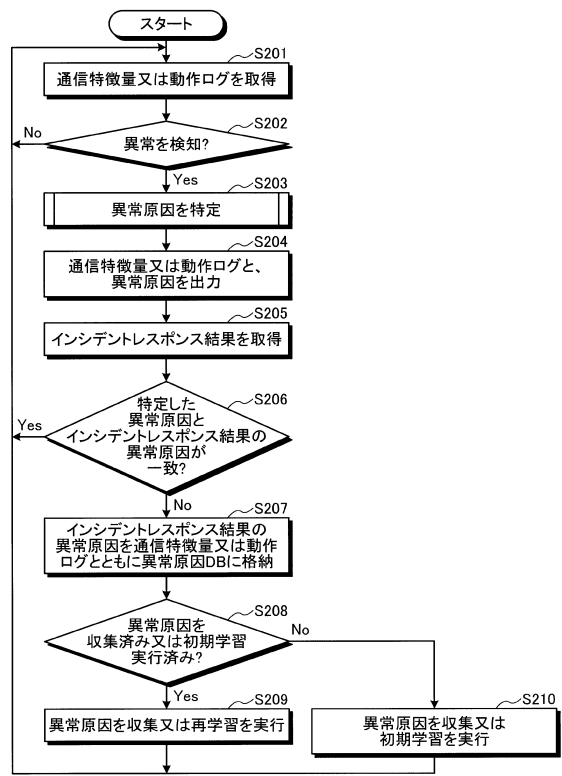
10

20

【図 7】



【図 8】

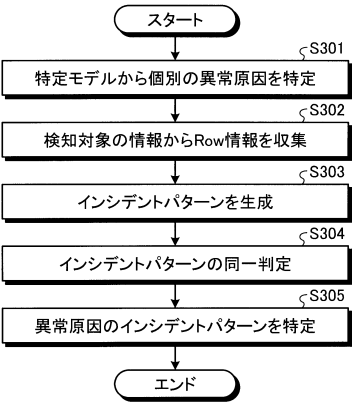


30

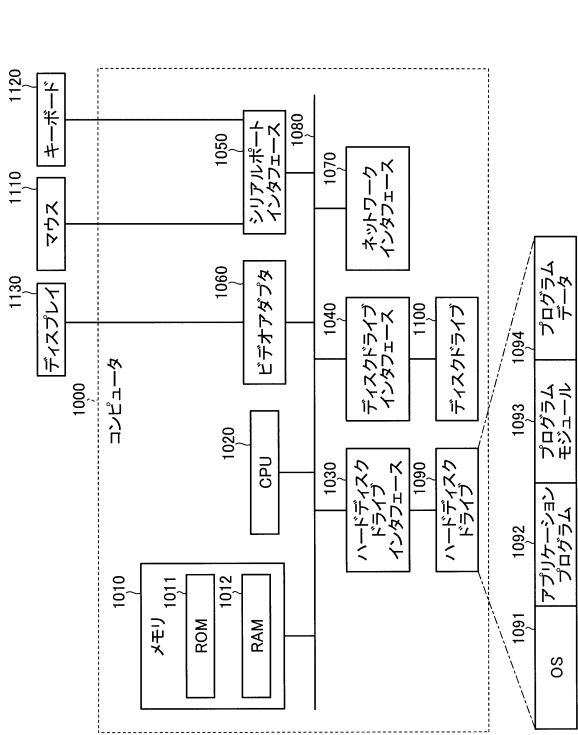
40

50

【図 9】



【図 10】



10

20

30

40

50

フロントページの続き

東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内

(72)発明者 泉 雅巳

東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内

審査官 中川 幸洋

(56)参考文献 特開2013-011949(JP, A)

特開2006-041969(JP, A)

中田 健介 Kensuke Nakata, 動的解析結果に基づく共通的なマルウェア通信パターン抽出技術の検討 A Method of Extracting Common Malware Communication Patterns from Dynamic Analysis Result, C S S 2015 コンピュータセキュリティシンポジウム2015 論文集 合同開催 マルウェア対策研究人材育成ワークショップ2015 プライバシーワークショップ2015 情報処理学会シンポジウムシリーズ V o l . 2015 N o . 3 [C D - R O M] , 日本, 一般社団法人情報処理学会 コンピュータセキュリティ研究会 セキュリティ心理学とトラスト研究会, 2015年10月14日, 第2015巻, pp.318-325

今井 康平 Kohei IMAI, シグネチャ型IDSを考慮したトラフィック特徴量のクラスタリングに基づく未知の異常検出 Anomaly Detection Based on Clustering of Network Traffic Characteristics Considering Results of Signature Based IDS Evaluation, 電子情報通信学会技術研究報告 V o l . 114 N o . 489 IEICE Technical Report, 日本, 一般社団法人電子情報通信学会 The Institute of Electronics, Information and Communication Engineers, 2015年02月24日, 第114巻

(58)調査した分野 (Int.Cl., DB名)

H04L 43/00

G06F 21/56