

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2024年12月19日(19.12.2024)



(10) 国際公開番号

WO 2024/257507 A1

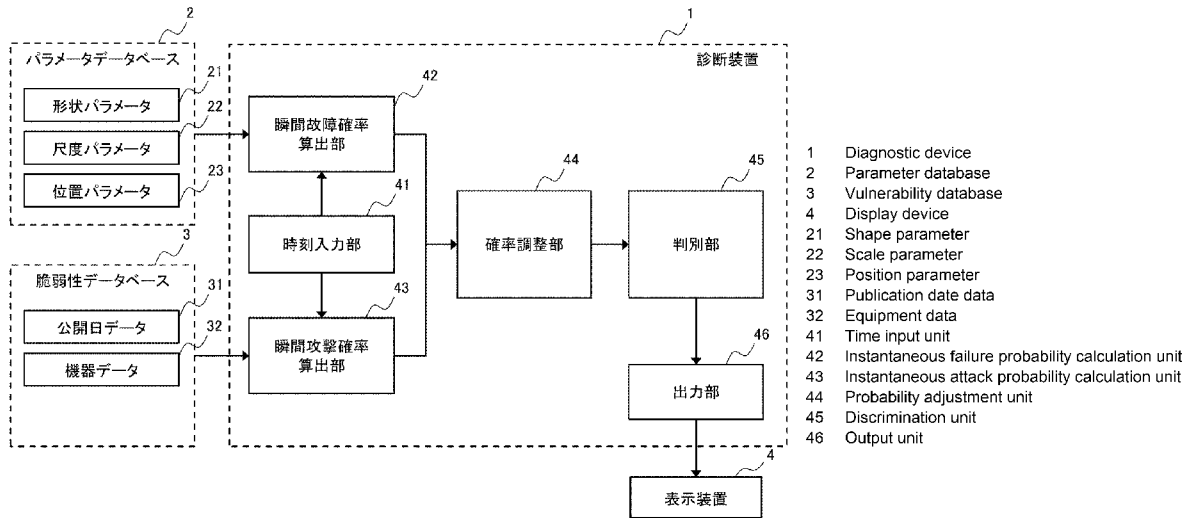
- (51) 国際特許分類:
G05B 23/02 (2006.01) G06F 21/55 (2013.01)
- (21) 国際出願番号: PCT/JP2024/017050
- (22) 国際出願日: 2024年5月8日(08.05.2024)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2023-096396 2023年6月12日(12.06.2023) JP
- (71) 出願人: 株式会社日立製作所(HITACHI, LTD.)
[JP/JP]; 〒1008280 東京都千代田区丸の内一丁目6番6号 Tokyo (JP).
- (72) 発明者: 阪田 恒晟(SAKATA Kosei); 〒1008280
東京都千代田区丸の内一丁目6番6号 株式会

社日立製作所内 Tokyo (JP). 小倉 貴志(OGURA Takashi); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP). 松本 典剛(MATSUMOTO Noritaka); 〒1008280 東京都千代田区丸の内一丁目6番6号 株式会社日立製作所内 Tokyo (JP).

- (74) 代理人: 弁理士法人開知 (KAICHI IP);
〒1030022 東京都中央区日本橋室町四丁目3番16号 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH,

(54) Title: DIAGNOSTIC DEVICE AND DIAGNOSTIC METHOD

(54) 発明の名称: 診断装置および診断方法



(57) Abstract: This diagnostic device is provided with a calculation device that: calculates an instantaneous attack probability, which is the probability that a cyber attack was performed on equipment to be diagnosed at a prescribed time; calculates an instantaneous failure probability, which is the probability that a failure occurred in the equipment to be diagnosed at the prescribed time; and determines whether or not there was a cyber attack on the equipment to be diagnosed and whether or not there was a failure in the equipment to be diagnosed at the prescribed time on the basis of the instantaneous attack probability and the instantaneous failure probability.

(57) 要約: 診断装置が備える演算装置は、診断対象機器に対して所定の時刻にサイバー攻撃が実施された確率である瞬間攻撃確率を算出し、診断対象機器において所定の時刻に故障が生じた確率である瞬間故障確率を算出し、瞬間攻撃確率と瞬間故障確率とに基づき、所定の時刻における、診断対象機器に対するサイバー攻撃の有無および診断対象機器における故障の有無を判定する。

KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

明 細 書

発明の名称：診断装置および診断方法

技術分野

[0001] 本発明は、診断装置および診断方法に関する。

背景技術

[0002] 安定した稼働が求められる制御システムは、機器の故障とサイバー攻撃の両方に対処を行う必要がある。機器の状態を正常と異常の二値で診断する、いわゆる二値診断には、異常をサイバー攻撃と機器の故障に判別することができない、正常と思われるサイバー攻撃を判別できない、等の問題がある。特許文献1には、機器の状態を二値診断以外で診断する診断方法が記載されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2019-194830号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献1に記載の技術では、サイバー攻撃を受けている確率と機器が故障した確率の相互に依存関係があるため、正確な診断ができないという問題があった。

[0005] 本発明は、サイバー攻撃の有無および機器の故障の有無を適切に判別可能な診断装置および診断方法の提供を目的とする。

課題を解決するための手段

[0006] 本発明の一態様による診断装置は、演算装置を備え、前記演算装置は、診断対象機器に対して所定の時刻にサイバー攻撃が実施された確率である瞬間攻撃確率を算出し、前記診断対象機器において前記所定の時刻に故障が生じた確率である瞬間故障確率を算出し、前記瞬間攻撃確率と前記瞬間故障確率とに基づき、前記所定の時刻における、前記診断対象機器に対するサイバー

攻撃の有無および前記診断対象機器における故障の有無を判定する。

発明の効果

[0007] 本発明によれば、サイバー攻撃の有無および機器の故障の有無を適切に判別できる。

図面の簡単な説明

[0008] [図1]図1は、第1実施形態に係る診断装置のハードウェア構成を模式的に示すブロック図である。

[図2]図2は、第1実施形態に係る診断装置の機能構成を示すブロック図である。

[図3]図3は、瞬間故障確率算出部が実行する瞬間故障確率算出処理のフローチャートである。

[図4]図4は、瞬間攻撃確率算出部が実行する瞬間攻撃確率算出処理のフローチャートである。

[図5]図5は、確率調整部が実行する確率調整処理のフローチャートである。

[図6]図6は、調整後瞬間故障確率および調整後瞬間攻撃確率を例示するグラフである。

[図7]図7は、判別部が実行する判別処理のフローチャートである。

[図8]図8は、表示装置の表示画面を例示する模式図である。

[図9]図9は、第2実施形態に係る診断装置の機能構成を示すブロック図である。

[図10]図10は、瞬間攻撃確率算出部が実行する瞬間攻撃確率算出処理のフローチャートである。

[図11]図11は、調整後瞬間故障確率および調整後瞬間攻撃確率を例示するグラフである。

[図12]図12は、第3実施形態に係る診断装置の機能構成を示すブロック図である。

[図13]図13は、調整後瞬間故障確率および調整後瞬間攻撃確率を例示するグラフである。

発明を実施するための形態

[0009] 図1～図8を参照して、本発明の実施形態に係る診断装置について説明する。

[0010] <第1実施形態>

図1は、第1実施形態に係る診断装置1のハードウェア構成を模式的に示すブロック図である。診断装置1は、不図示の診断対象機器（例えば制御システムに含まれる制御装置等）の健全性を診断し、診断結果をユーザに報知する装置である。ユーザは任意のタイミング（例えば毎日の特定の時刻等）で診断装置1を用いて診断対象機器の診断を行い、診断結果を参照して診断対象機器に必要な処置を施すことができる。

[0011] 診断装置1は、CPU（Central Processing Unit）、MPU（Micro Processing Unit）、DSP（Digital Signal Processor）等の演算装置11、ROM（Read Only Memory）、フラッシュメモリ、ハードディスクドライブ等の不揮発性メモリ12、所謂RAM（Random Access Memory）と呼ばれる揮発性メモリ13、入出力インタフェース14、および、その他の周辺回路を備えたコンピュータで構成される。これらのハードウェアは、協働してソフトウェアを動作させ、複数の機能を実現する。なお、診断装置1は、1つのコンピュータで構成してもよいし、複数のコンピュータで構成してもよい。また、演算装置11としては、ASIC（application specific integrated circuit）、FPGA（Field Programmable Gate Array）などを用いることができる。

[0012] 不揮発性メモリ12には、各種演算が実行可能なプログラムが格納されている。すなわち、不揮発性メモリ12は、本実施形態の機能を実現するプログラムを読み取り可能な記憶媒体（記憶装置）である。揮発性メモリ13は、演算装置11による演算結果および入力インタフェース14から入力された信号を一時的に記憶する記憶媒体（記憶装置）である。演算装置11は、不揮発性メモリ12に記憶されたプログラムを揮発性メモリに展開して演算実行する装置であって、プログラムに従って入力インタフェース14、不

揮発性メモリ 12 および揮発性メモリ 13 から取り入れたデータに対して所定の演算処理を行う。

[0013] 診断装置 1 は、入出力インタフェース 14 を介して、パラメータデータベース 2、脆弱性データベース 3、および表示装置 4 に接続される。パラメータデータベース 2 および脆弱性データベース 3 は、所定のデータが格納された記憶装置である。パラメータデータベース 2 および脆弱性データベース 3 に格納されるデータについては後に詳述する。表示装置 4 は、例えば液晶モニタ等の表示画面を有する装置である。

[0014] 入出力インタフェース 14 の入力部は、パラメータデータベース 2 および脆弱性データベース 3 から入力された信号を演算装置 11 で演算可能なデータに変換する。また、入出力インタフェース 14 の出力部は、演算装置 11 での演算結果に応じた出力用の信号を生成し、その信号を表示装置 4 に出力する。

[0015] 図 2 は、第 1 実施形態に係る診断装置 1 の機能構成を示すブロック図である。診断装置 1 は、時刻入力部 41、瞬間故障確率算出部 42、瞬間攻撃確率算出部 43、確率調整部 44、判別部 45、および出力部 46 を備える。時刻入力部 41 は、瞬間故障確率算出部 42 および瞬間攻撃確率算出部 43 に診断時刻を入力する。瞬間故障確率算出部 42 は、診断時刻における診断対象機器の瞬間故障確率を算出する。瞬間攻撃確率算出部 43 は、診断時刻における診断対象機器の瞬間攻撃確率を算出する。確率調整部 44 は、瞬間故障確率および瞬間攻撃確率を同次元化する調整を実施する。判別部 45 は、確率調整部 44 により調整された瞬間故障確率および瞬間攻撃確率を用いて、診断対象機器へのサイバー攻撃の可能性の有無、および、診断対象機器の故障の可能性の有無を判別する。出力部 46 は、判別部 45 による判別の結果を表示装置 4 に出力し、その内容をユーザに報知する。

[0016] パラメータデータベース 2 には、形状パラメータ 21、尺度パラメータ 22、および位置パラメータ 23 が格納される。また、脆弱性データベース 3 には、公開日データ 31、および機器データ 32 が格納される。これらのデ

ータについては当該データを使用する処理と合わせて説明する。

[0017] 診断装置 1 による診断対象機器の診断は、瞬間故障確率算出処理、瞬間攻撃確率算出処理、確率調整処理、および判別処理により実現される。以下、これらの処理について順に説明する。

[0018] [瞬間故障確率算出処理]

図 3 は、瞬間故障確率算出部 4 2 が実行する瞬間故障確率算出処理のフローチャートである。ステップ S 1 0 0 において、時刻入力部 4 1 が瞬間故障確率算出部 4 2 に診断時刻を入力する。ステップ S 1 1 0 において、瞬間故障確率算出部 4 2 がパラメータデータベース 2 から形状パラメータ 2 1、尺度パラメータ 2 2、および位置パラメータ 2 3 を取得する。これらの各パラメータは、診断対象機器の過去の故障回数や故障に至るまでの時間に応じて、あらかじめ決まった値が設定される。ステップ S 1 2 0 において、瞬間故障確率算出部 4 2 が故障密度関数 $f(t)$ に形状パラメータ 2 1、尺度パラメータ 2 2、および位置パラメータ 2 3 を代入する。

[0019] 故障密度関数 $f(t)$ は、時間の経過に対する診断対象機器の故障確率を表す関数である。すなわち故障密度関数 $f(t)$ は、時間変化する確率分布を表す関数である。故障密度関数 $f(t)$ は、ハザード関数 $h(t)$ と信頼度関数 $R(t)$ の積で表現される。ここで変数 t は診断対象機器の稼働時間を表し、 $t = 0$ は診断対象機器が稼働を開始した時刻に対応する。ハザード関数 $h(t)$ は、診断対象機器が時刻 t までに実際に故障したことがあるか否かに関係なく、時刻 t の時点で診断対象機器に故障が発生する確率を表す関数である。換言すると、ハザード関数 $h(t)$ は、診断対象機器が時刻 t まで故障しなかったという条件のもとで、その時刻に診断対象機器が故障する条件付き確率密度である。形状パラメータ 2 1 を m 、尺度パラメータ 2 2 を n 、位置パラメータ 2 3 を Γ という記号でそれぞれ表すと、ハザード関数 $h(t)$ は次式 (1) で表される。

$$h(t) = m/n \cdot \{(t - \Gamma)/n\}^{m-1} \cdots (1)$$

信頼度関数 $R(t)$ は、診断対象機器に時刻 t まで故障が起こらない確率

を表す関数であり、次式（２）で表される。

$$R(t) = \exp \{ - (t - \Gamma / n)^m \} \quad \cdots (2)$$

故障密度関数 $f(t)$ は、診断対象機器に時刻 t で最初に故障が起こる確率を表す関数であり、次式（３）で表される。

$$f(t) = h(t) \cdot R(t) \quad \cdots (3)$$

故障密度関数 $f(t)$ は、例えばワイブル分布のように、一般に時間経過に伴い下に凸の関数となる。

[0020] 文字 m で表した形状パラメータ 21 は、故障密度関数 $f(t)$ の時間経過に伴う増減、すなわち故障密度関数 $f(t)$ が表す確率分布の形状を定めるパラメータである。例えば $m < 1$ のとき、故障密度関数 $f(t)$ は時間経過に従って減少する形状となる。また $m > 1$ のとき、故障密度関数 $f(t)$ は時間経過に従って増加する形状となる。また $m = 0$ のとき、故障確率は時間経過によらず一定になる。文字 n で表した尺度パラメータ 22 は、故障密度関数 $f(t)$ の大小、すなわち故障密度関数 $f(t)$ が表す確率分布の尺度を定めるパラメータである。例えば $n = 1$ の時の故障密度関数 $f(t)$ の最大値は、 $n = 2$ の時の故障密度関数 $f(t)$ の最大値の 2 倍となる。文字 Γ で表した位置パラメータ 23 は、故障密度関数 $f(t)$ の位相、すなわち故障密度関数 $f(t)$ が表す確率分布の位置を定めるパラメータである。例えば $\Gamma = 2$ の時の故障密度関数 $f(t)$ の横軸上の初期位置は、 $\Gamma = 0$ の時の故障密度関数 $f(t)$ の初期位置と比べ 2 だけ平行移動している。

[0021] 図 3 のステップ S120 において、瞬間故障確率算出部 42 が上式（３）の故障密度関数 $f(t)$ に形状パラメータ 21、尺度パラメータ 22、および位置パラメータ 23 を代入する。続くステップ S130 において瞬間故障確率算出部 42 は、各パラメータを代入した後の故障密度関数 $f(t)$ と診断時刻 t を用いて、瞬間故障確率を算出する。次式（４）のように定義される累積故障分布関数 $F(t)$ を導入する。

$$F(t) = \int f(t) dt \quad \cdots (4)$$

診断時刻を t_1 とすると、瞬間故障確率算出部 42 は累積故障分布関数 F

(t) を $t = 0$ から $t = t_1$ まで時間積分することにより瞬間故障確率を算出する。

[0022] [瞬間攻撃確率算出処理]

図4は、瞬間攻撃確率算出部43が実行する瞬間攻撃確率算出処理のフローチャートである。ステップS200において、時刻入力部41が瞬間攻撃確率算出部43に診断時刻を入力する。ステップS210において、瞬間攻撃確率算出部43が脆弱性データベース3から公開日データ31および機器データ32を取得する。

[0023] 脆弱性データベース3は、診断対象機器を構成するソフトウェアやハードウェアの脆弱性情報を保持する。公開日データ31は、診断対象機器に関連するソフトウェアやハードウェアの脆弱性情報が公開された日付を示す。機器データ32は、診断対象機器のネットワーク接続情報や診断対象機器の内部で保持および使用しているプログラム情報を示す。これらのデータは、例えば各国のセキュリティ関連団体が公開している脆弱性情報をインターネットなどを用いて予め収集して設定される。例えば、共通脆弱性評価システムとして知られるCVSS (Common Vulnerability Scoring System) に基づき公表されている脆弱性情報から公開日データ31を生成して脆弱性データベース3に格納する。また、そのような脆弱性情報を機器データ32と比較することで、診断対象機器に影響のある脆弱性を特定することができる。

[0024] ステップS220において、瞬間攻撃確率算出部43が診断対象機器のセキュリティ評価値を算出する。セキュリティ評価値は、診断対象機器のサイバー攻撃に対するリスクの高さを表す数値であり、例えば診断対象機器のサイバー攻撃への耐性が高いほど、診断対象機器がサイバー攻撃を受けたときの被害が大きいほど、その値は大きくなるように設定する。

[0025] 第1実施形態の瞬間攻撃確率算出部43は、セキュリティ評価値 $Risk$ を次式(5)により算出する。

$$Risk = Impact \cdot Likelihood \quad \dots (5)$$

ここで、 $Impact$ は、診断対象機器への影響度合い（影響の大きさ）

を表し、Likelihoodは、診断対象機器への攻撃容易性を表している。

[0026] 例えば、前述したCVSSでは脆弱性公開日におけるセキュリティ評価値を脆弱性そのものの基本特性から以下のように定めている。脆弱性そのものの基本特性には、攻撃容易性を測るものとして、脆弱性のあるコンポーネントをどこから攻撃可能であるかの指標である攻撃元区分X、脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さの指標であるY、脆弱性のあるコンポーネントを攻撃する際に必要な特権レベルZ、脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルWがある。また、診断対象機器への影響度合を測るものとして、機密性への影響レベルCや完全性への影響I、可用性への影響Aがある。

[0027] ここでImpactは可用性A、完全性I、機密性Cを用いて次式(6)のように表すことができる。

$$\text{Impact} = 1 - (1 - A) \times (1 - I) \times (1 - C) \quad \dots (6)$$

またLikelihoodは、攻撃元区分X、攻撃条件の複雑さY、必要な特権レベルZ、必要なユーザ関与レベルWを用いて、次式(7)のように表すことができる。

$$\text{Likelihood} = 8.22 \times X \times Y \times Z \times W \quad \dots (7)$$

式(5)に式(6)と式(7)を代入し、セキュリティ評価値Riskを算出する次式(8)を得る。

$$\text{Risk} = (1 - (1 - A) \times (1 - I) \times (1 - C)) \times 8.22 \times X \times Y \times Z \times W \quad \dots (8)$$

図4のステップS220において、瞬間攻撃確率算出部43は、式(8)を用いてセキュリティ評価値Riskを算出する。

[0028] ステップS230において、瞬間攻撃確率算出部43が攻撃密度関数a(t)を決定する。攻撃密度関数a(t)は、時刻tで最初にサイバー攻撃を受ける確率を表す関数である。すなわち攻撃密度関数a(t)は、時間変化

する確率分布を表す関数である。攻撃密度関数 $a(t)$ は、故障密度関数 $f(t)$ とは個別に（独立に）設定されるので、通常、両者には相関がない。換言すると、攻撃密度関数 $a(t)$ および故障密度関数 $f(t)$ は、それぞれ異なる確率分布を表す関数である。瞬間攻撃確率算出部 43 は、前述したセキュリティ評価値をパラメータとして持つ確率分布を想定し、その確率分布を表す攻撃密度関数 $a(t)$ を決定する。例えば攻撃密度関数 $a(t)$ は、時間に対して上に凸の関数や単調に減少する関数などであり、そのような関数としてはガウス分布などが挙げられる。

[0029] 第1実施形態の瞬間攻撃確率算出部 43 は、次式（9）で表現される攻撃密度関数 $a(t)$ を用いる。

$$a(t) = 1 / \sqrt{2\pi\sigma} \exp\{- (t - \mu)^2 / 2\sigma^2\} \quad \dots (9)$$

ここで μ は平均を、 σ は標準偏差を、 $2\sigma^2$ は分散を表す。

[0030] ステップ S240 において瞬間攻撃確率算出部 43 は、ステップ S200 で入力された診断時刻とステップ S230 で決定した攻撃密度関数 $a(t)$ とを用いて、瞬間攻撃確率を算出する。次式（10）のように定義される累積攻撃分布関数 $A(t)$ を導入する。

$$A(t) = \int a(t) dt \quad \dots (10)$$

診断時刻を t_1 とすると、瞬間攻撃確率算出部 43 は累積攻撃分布関数 $A(t)$ を $t=0$ から $t=t_1$ まで時間積分することにより瞬間攻撃確率を算出する。

[0031] [確率調整処理]

図5は、確率調整部 44 が実行する確率調整処理のフローチャートである。確率調整処理において確率調整部 44 は、診断時刻における故障とサイバー攻撃それぞれの確率分布を同次元化して比較可能にする。第1実施形態では、異なる確率分布を同次元化する方法として、確率距離尺度を用いる方法を採用している。

[0032] ステップ S300 において確率調整部 44 は、瞬間故障確率算出部 42 が

瞬間故障確率算出処理で導出した累積故障分布関数 $F(t)$ と、瞬間攻撃確率算出部 43 が瞬間攻撃確率算出処理で導出した累積攻撃分布関数 $A(t)$ と、を取得する。ステップ S310 において確率調整部 44 は、累積故障分布関数 $F(t)$ と累積攻撃分布関数 $A(t)$ との間の確率距離尺度を算出する。

[0033] 確率距離尺度は、例えばカルバック&ライブラー情報量など、異なる確率分布（例えばワイブル分布とガウス分布）間の距離を意味する。確率距離尺度 DKL は次式 (11) により算出される。

$$DKL(F(t) || A(t)) = \int F(t) \log \{A(t) / F(t)\} dt \quad \dots (11)$$

このように、第 1 実施形態では確率距離尺度としてカルバック&ライブラー情報量を採用する。

[0034] ステップ S320 において確率調整部 44 は、診断時刻における調整後瞬間故障確率および調整後瞬間攻撃確率を算出する。確率調整部 44 は、診断時刻における瞬間故障確率（図 3 のステップ S130 で算出した値）にステップ S310 で算出した確率距離尺度を乗算し、調整後瞬間故障確率とする。同様に確率調整部 44 は、診断時刻における瞬間攻撃確率（図 4 のステップ S240 で算出した値）にステップ S310 で算出した確率距離尺度を乗算し、調整後瞬間攻撃確率とする。

[0035] 例えば、調整後瞬間故障確率を $F'(t)$ 、調整後瞬間攻撃確率を $A'(t)$ とすると、調整後瞬間故障確率および調整後瞬間攻撃確率は次式 (12)、(13) により算出できる。

$$F'(t) = DKL(F(t) || A(t)) \cdot F(t) \quad \dots (12)$$

$$A'(t) = DKL(F(t) || A(t)) \cdot A(t) \quad \dots (13)$$

ステップ S320 で調整後瞬間故障確率 $F'(t)$ 、および調整後瞬間攻撃確率 $A'(t)$ が算出されると、処理がステップ S330 に進む。

[0036] ステップS 3 3 0において確率調整部4 4は、ステップS 3 2 0で算出した診断時刻 t_1 における調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を判別部4 5に出力する。

[0037] 図6は、調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を例示するグラフである。図6において、符号6 2が調整後瞬間故障確率 $F'(t)$ を、符号6 3が調整後瞬間攻撃確率 $A'(t)$ を、それぞれ表す。図6において、横軸は経過時間 t を表し縦軸は経過時間におけるそれぞれの確率を表す。図6では、横軸の経過時間 t を初期運用、中期運用、最終運用の3つのフェイズに区切っている。これは、診断対象機器を導入し運用を開始してからのフェイズをそれぞれ意味している。すなわち、初期運用フェイズは診断対象機器の稼働直後からしばらくの間を、中期運用フェイズは運用が軌道に乗ってからしばらくの間を、最終運用フェイズは運用の終盤をそれぞれ表している。符号6 0は診断対象機器に脆弱性が発覚した日時を表し、符号6 1は診断装置1による診断を行った時刻（診断時刻 t_1 ）を表す。符号6 4は診断時刻における調整後瞬間故障確率 $F'(t)$ を、符号6 5は診断時刻における調整後瞬間攻撃確率 $A'(t)$ をそれぞれ表す。例えば図6では、診断時刻 t_1 において、調整後瞬間故障確率 $F'(t) = 0.3$ であり、調整後瞬間攻撃確率 $A'(t) = 0.2$ である。

[0038] [判別処理]

図7は、判別部4 5が実行する判別処理のフローチャートである。判別部4 5は、確率調整部4 4が出力する調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を所定のしきい値 f 、 a とそれぞれ比較することにより、故障およびサイバー攻撃の有無を出力する。所定のしきい値 f は故障密度関数 $f(t)$ に基づく値であり、所定のしきい値 a は攻撃密度関数 $a(t)$ に基づく値である。これらのしきい値 f 、 a は、例えば故障密度関数 $f(t)$ や攻撃密度関数 $a(t)$ の最頻値、平均値、中央値などの統計値であってもよいし、それらの統計値とは別に診断装置1の設計者が指定する値であってもよい。

[0039] ステップS400において判別部45は、調整後瞬間故障確率 $F'(t)$ の値をしきい値 f と比較する。調整後瞬間故障確率 $F'(t)$ の値がしきい値 f 以上である場合、処理はステップS410に進む。ステップS410において判別部45は、調整後瞬間攻撃確率 $A'(t)$ の値をしきい値 a と比較する。調整後瞬間攻撃確率 $A'(t)$ の値がしきい値 a 以上である場合、処理はステップS420に進む。ステップS420において判別部45は、故障およびサイバー攻撃の両方が同時に生じた可能性が高いと判別する。ステップS410において調整後瞬間攻撃確率 $A'(t)$ の値がしきい値 a 未満である場合、処理はステップS430に進む。ステップS430において判別部45は、故障が生じた可能性が高いと判別する。ステップS400において調整後瞬間故障確率 $F'(t)$ の値がしきい値 f 未満である場合、処理はステップS440に進む。ステップS440において判別部45は、調整後瞬間攻撃確率 $A'(t)$ の値をしきい値 a と比較する。調整後瞬間攻撃確率 $A'(t)$ の値がしきい値 a 以上である場合、処理はステップS450に進む。ステップS450において判別部45は、サイバー攻撃が生じた可能性が高いと判別する。ステップS440において調整後瞬間攻撃確率 $A'(t)$ の値がしきい値 a 未満である場合、処理はステップS460に進む。ステップS460において判別部45は、故障が生じた可能性もサイバー攻撃が生じた可能性もいずれも低い、すなわち診断対象機器は正常な状態であると判別する。

[0040] 例えば、設計者により $f = 0.4$ 、 $a = 0.3$ というしきい値が与えられており、図6に示すように調整後瞬間故障確率 $F'(t) = 0.3$ 、調整後瞬間攻撃確率 $A'(t) = 0.2$ である場合を考える。この場合、ステップS400で調整後瞬間故障確率 $F'(t)$ がしきい値 f 未満であるためステップS440に進み、調整後瞬間攻撃確率 $A'(t)$ がしきい値 a 未満であるためステップS460に進む。その結果、判別部45は診断対象機器が正常な状態である（故障も生じていないしサイバー攻撃も受けていない）と判別する。

- [0041] 図8は、表示装置4の表示画面を例示する模式図である。出力部46は、判別部45による判別の結果、すなわち診断結果を表示装置4に出力する。表示装置4は、この診断結果に基づき、図8に例示するような画面を表示する。
- [0042] 表示装置4の表示画面には、診断日時表示領域90、診断結果表示領域91、診断結果詳細表示領域92、診断グラフ表示領域93、および再診断ボタン94が設けられる。診断日時表示領域90は、診断を実施した日時（診断時刻 t_1 ）を表示する。診断結果表示領域91は、診断対象機器の診断結果を表示する領域である。診断結果表示領域91には、診断結果が正常、故障、攻撃（サイバー攻撃）、故障&攻撃、のいずれかの形で表示される。診断結果詳細表示領域92は、診断結果表示領域91に表示される結果の内訳（詳細）を表示する領域である。診断グラフ表示領域93は、診断時刻までの故障確率分布および攻撃確率分布を表示するものであり、例えば図6に例示したグラフのように確率分布が表示されるものとする。再診断ボタン94は、再診断を実行するためのボタンである。再診断ボタン94を押すことで、ボタンが押された時刻における診断対象機器の診断が再度実行され、再診断の結果を表示装置4の表示画面に表示することができる。
- [0043] 上述した第1実施形態によれば、次の作用効果を奏する。
- [0044] （1）瞬間攻撃確率算出部43（演算装置）が診断対象機器に対して診断時刻（所定の時刻）にサイバー攻撃が実施された確率である瞬間攻撃確率を算出し、瞬間故障確率算出部42（演算装置）が診断対象機器において診断時刻（所定の時刻）に故障が生じた確率である瞬間故障確率を算出する。その後、判別部45（演算装置）が、瞬間攻撃確率と瞬間故障確率とに基づき、診断時刻（所定の時刻）における、診断対象機器に対するサイバー攻撃の有無および診断対象機器における故障の有無を判定する。このようにしたので、サイバー攻撃の有無および機器の故障の有無を適切に判別できる。また、瞬間攻撃確率と瞬間故障確率は別々に算出され、お互いに相関がないので、一方が他方に影響されることがなく、サイバー攻撃の確率と故障の確率と

を独立に判断することができる。

[0045] (2) 判別部 4 5 (演算装置) は、瞬間攻撃確率および瞬間故障確率をそれぞれ所定の閾値と比較することにより、診断対象機器に対するサイバー攻撃の有無および診断対象機器における故障の有無を判定する。このようにしたので、サイバー攻撃の有無と故障の有無とを、一方が他方に影響されることなく独立に判断することができる。

[0046] (3) 瞬間攻撃確率算出部 4 3 (演算装置) は、時間変化する確率分布を表した攻撃密度関数 $a(t)$ (第 1 の確率分布) を用いて瞬間攻撃確率を算出する。また、瞬間故障確率算出部 4 2 (演算装置) は、時間変化する確率分布を表し攻撃密度関数 $a(t)$ (第 1 の確率分布) とは異なる故障密度関数 $f(t)$ (第 2 の確率分布) を用いて瞬間故障確率を算出する。このようにしたので、サイバー攻撃の有無と故障の有無とを、一方が他方に影響されることなく独立に判断することができる。

[0047] (4) 瞬間故障確率算出部 4 2 (演算装置) は、診断対象機器が故障する確率の確率分布の形状、尺度、および位置の特徴を表す形状パラメータ 2 1、尺度パラメータ 2 2、および位置パラメータ 2 1 の少なくとも一つを用いて瞬間故障確率を算出する。このようにしたので、診断対象機器の故障の有無を精度よく判別することが可能になる。

[0048] (5) 瞬間攻撃確率算出部 4 3 (演算装置) は、診断対象機器を構成するハードウェアまたはソフトウェアに関連する脆弱性データベース 3 (脆弱性情報) を用いて瞬間攻撃確率を算出する。このようにしたので、診断対象機器へのサイバー攻撃の有無を精度よく判別することが可能になる。

[0049] (6) 確率調整部 4 4 (演算装置) は、瞬間攻撃確率および瞬間故障確率を同次元化する調整を行う。このようにしたので、瞬間攻撃確率および瞬間故障確率をそれぞれ比較するしきい値を共通の尺度で決定することができ、しきい値の設定が簡便になる。

[0050] (7) 出力部 4 6 (演算装置) は、判別部 4 5 (演算装置) により判定された診断対象機器に対するサイバー攻撃の有無、および、判別部 4 5 (演算

装置)により判定された診断対象機器における故障の有無を表示装置4に表示させる。このようにしたので、診断装置1の使用者が診断結果を的確に把握することが可能になる。

[0051] <第2実施形態>

図9～図11を参照して、本発明の第2実施形態に係る診断装置について説明する。なお、第1実施形態で説明した構成と同一もしくは相当する構成には同一の参照記号を付し、相違点を主に説明する。

[0052] 図9は、図2と同様の図であり、第2実施形態に係る診断装置100の機能構成を示すブロック図である。診断装置100は、第1実施形態に係る診断装置1の各部に加えて、保守リスク評価値算出部47を備える。保守リスク評価値算出部47は、診断対象機器の保守に関連するリスクを定量化した数値である保守リスク評価値を算出する。診断装置100には、第1実施形態と同様のパラメータデータベース2および脆弱性データベース3に加えて、保守点検データベース5が接続される。

[0053] 保守点検データベース5は、保守点検データ51、保守員データ52、および操作ログデータ53を格納する。保守点検データ51は、例えば保守員による診断対象機器の保守点検日や点検場所に関する情報である。保守員データ52は、例えば保守員の年齢、勤務年数といった保守員自身に関する情報である。操作ログデータ53は、例えば保守時間や操作コマンド数に関する情報である。

[0054] 保守リスク評価値算出部47による保守リスク評価値の算出方法の一例を説明する。保守リスク評価値Lは次式(14)のように表される。

$$L = T \cdot C \quad \cdots (14)$$

ここで、Tは規定操作時間に対する実際の操作時間の割合を表し、Cは規定操作コマンド数に対する実際の操作コマンド数の割合を表している。

[0055] 操作時間の割合Tや操作コマンド数の割合Cの値を所定の値と比較することで、保守員の操作への精通の度合を定量的に測ることができる。例えば、Cが1より大きい場合、その保守員は保守操作に精通していないと判定した

り、Cが1未満であれば保守操作に精通していると判定したりすることができる。また、Tについても同様に、Tが1より大きい場合、その保守員は保守操作に精通していないと判定したり、Tが1未満であれば保守操作に精通していると判定したりすることができる。

[0056] なお、保守員が保守操作に精通しているか否かの判別は、上述したルールのベースの指標の他に、保守員データ52に含まれる保守員の年齢、勤務年数や、操作ログデータ53に含まれる操作時間などを入力データセットとする機械学習により行うことも可能である。

[0057] 図10は、図4と同様の図であり、瞬間攻撃確率算出部43が実行する瞬間攻撃確率算出処理のフローチャートである。図10のフローチャートでは、図4のフローチャートのステップS220とステップS230の間に、ステップS225の処理が追加されている。ステップS225において瞬間攻撃確率算出部43は、ステップS220で決定したセキュリティ評価値に対して、保守リスク評価値算出部47が算出した保守リスク評価値を合算する。これにより、これ以降のセキュリティ評価値を対象とする処理は、保守リスク評価値を加味した処理となる。

[0058] 式(5)に示した通り、セキュリティ評価値は診断対象機器への影響度合い(影響の大きさ)Impact、診断対象機器への攻撃容易性Likelihoodにより決定される。保守リスク評価値はそれらの値のうち攻撃容易性Likelihoodに反映される。式(7)に示した通り、Likelihoodは攻撃元区分X、攻撃条件の複雑さY、必要な特権レベルZ、必要なユーザ関与レベルWに基づく値である。瞬間攻撃確率算出部43は、攻撃元区分Xや必要な特権レベルZの値を保守リスク評価値に応じで変動させることにより、保守リスク評価値をセキュリティ評価値に合算(反映)する。例えば、保守リスク評価値が大きいほど攻撃元区分Xや必要な特権レベルZの値を上げたり、保守リスク評価値が小さいほど攻撃元区分Xや必要な特権レベルZの値を下げたりする。

[0059] なお、保守リスク評価値をセキュリティ評価値に合算する方法は上述の方

法に限定されない。例えば保守リスク評価値をセキュリティリスク評価値のように同じ10段階で評価し、セキュリティリスク評価値に足し合わせるようにしてもよい。

[0060] 図11は、図6と同様の図であり、調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を例示するグラフである。符号1360は調整後瞬間故障確率 $F'(t)$ を、符号1370は調整後瞬間攻撃確率 $A'(t)$ を、それぞれ表す。図11において、横軸は経過時間 t を表し縦軸は経過時間におけるそれぞれの確率を表す。符号1300は診断対象機器に脆弱性が発覚した日時を表し、符号1310は診断装置1による診断を行った時刻（診断時刻 t_1 ）を表す。符号1330は診断時刻における保守リスク評価値を加味しない調整後瞬間攻撃確率 $A'(t)$ を表し、符号1340は診断時刻における保守リスク評価値を加味した調整後瞬間攻撃確率 $A'(t)$ を表す。符号1350は診断時刻における調整後瞬間故障確率 $F'(t)$ を表す。

[0061] 調整後瞬間攻撃確率 $A'(t)$ は、従来のセキュリティ要素に起因するものの以外に、保守員による保守点検作業にも起因して変動する。例えば図6においては、診断時刻における調整後瞬間攻撃確率 $A'(t) = 0.2$ であるケースを考えたが、図11においては $A'(t) = 0.3$ となるケースを考える。これは、脆弱性要因に加え、保守要因が調整後瞬間攻撃確率 $A'(t)$ に反映されたことを考慮するためである。この保守要因が反映された調整後瞬間攻撃確率 $A'(t)$ において、例えば、 $A'(t) = 0.3$ 、しきい値 $a = 0.2$ の場合の出力結果を考える。ただし、調整後瞬間故障確率 $F'(t) = 0.3$ およびしきい値 $f = 0.4$ は図6と同様とする。このとき判別部45は、まず $F'(t)$ が f より小さいことから故障の可能性は低いと判別する。その後、判別部45は、 $A'(t)$ が a 以上であることからサイバー攻撃の可能性が高いと判別する。これにより診断結果はサイバー攻撃の可能性が高い、ということになる。このように、保守リスク評価値が加味されたことにより調整後瞬間攻撃確率 $A'(t)$ の値が大きくなり、その結果

、図 6 で説明した内容から診断結果が変化している。

[0062] 上述した第 2 実施形態によれば、次の作用効果を奏する。

[0063] (1) 瞬間攻撃確率算出部 4 3 (演算装置) は、診断対象機器の保守点検に関する情報である保守点検データ 5 1、診断対象機器の保守点検を行う保守員に関する情報である保守員データ 5 2、および診断対象機器の保守点検において成された操作の操作ログに関する情報である操作ログデータ 5 3 の少なくとも一つに基づく保守リスク評価値を用いて瞬間攻撃確率を算出する。このようにすることで、診断対象機器のライフサイクルを加味した診断ができるようになる。

[0064] <第 3 実施形態>

図 1 2 および図 1 3 を参照して、本発明の第 3 実施形態に係る診断装置について説明する。なお、第 1 実施形態で説明した構成と同一もしくは相当する構成には同一の参照記号を付し、相違点を主に説明する。

[0065] 図 1 2 は、図 2 と同様の図であり、第 3 実施形態に係る診断装置 2 0 0 の機能構成を示すブロック図である。診断装置 2 0 0 には、第 1 実施形態と同様のパラメータデータベース 2 および脆弱性データベース 3 に加えて、物理情報データベース 7 およびアクセス情報データベース 8 が接続される。

[0066] 物理情報データベース 7 には、温度データ 7 1、湿度データ 7 2、および振動データ 7 3 が格納される。温度データ 7 1 は、例えば診断対象機器が高温下で稼働している、あるいは冷却下で稼働している、といった診断対象機器の環境の温度に関するデータである。湿度データ 7 2 は、例えば診断対象機器が設置されている環境が多湿あるいは低湿である、といった診断対象機器の環境の湿度に関するデータである。振動データ 7 3 は、例えば診断対象機器が設置されている環境の振動の大きさに関するデータである。なお、これら以外にも、例えば、診断対象機器の環境の風（風量および風速）、放射能、塵などに関するデータを物理情報データベース 7 に格納してもよい。

[0067] アクセス情報データベース 8 には、物理アクセスデータ 8 1 およびネットワークデータ 8 2 が格納される。物理アクセスデータ 8 1 は、診断対象機器

の設置場所のセキュリティ状況に関するデータ、すなわち、診断対象機器が設置されている環境の物理的な安全性を示すデータであり、例えば診断対象機器の設置されている部屋が施錠されている、あるいは特定の人物しか入室できないような物理的セキュリティが構築されている、診断対象機器がワイヤーロック等で固定されている、といったデータである。ネットワークデータ 82 は、診断対象機器に外部からネットワーク経由でアクセスする経路のセキュリティ状況に関するデータ、すなわち、外部から診断対象機器への侵入のしやすさを示すデータであり、例えば診断対象機器のデバックポートの情報やシェル情報、ネットワーク通信に用いるポート情報などである。

[0068] 第3実施形態の瞬間故障確率算出部 42 は、パラメータデータベース 2 内の各種パラメータだけではなく、物理情報データベース 7 内の各種データをも用いて瞬間故障確率を算出する。第3実施形態の瞬間攻撃確率算出部 43 は、脆弱性データベース 3 内の各種データだけではなく、アクセス情報データベース 8 内の各種データをも用いて瞬間攻撃確率を算出する。

[0069] 図 13 は、図 6 と同様の図であり、調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を例示するグラフである。符号 1550 は調整後瞬間故障確率 $F'(t)$ を、符号 1540 は調整後瞬間攻撃確率 $A'(t)$ を、それぞれ表す。図 13 において、横軸は経過時間 t を表し縦軸は経過時間におけるそれぞれの確率を表す。符号 1500 は診断対象機器に脆弱性が発覚した日時を表し、符号 1510 は診断装置 200 による診断を行った時刻（診断時刻 t_1 ）を表す。符号 1530 は診断時刻における物理情報データベース 7 内の各種データを加味した調整後瞬間故障確率 $F'(t)$ を表し、符号 1520 は診断時刻におけるアクセス情報データベース 8 内の各種データを加味した調整後瞬間攻撃確率 $A'(t)$ を表す。

[0070] 例えば図 6 においては、診断時刻における調整後瞬間故障確率 $F'(t) = 0.3$ であるケースを考えたが、図 13 においては調整後瞬間故障確率 $F'(t) = 0.45$ となるケースを考える。また図 6 においては、診断時刻における調整後瞬間攻撃確率 $A'(t) = 0.2$ であるケースを考えたが、

図13においては $A'(t) = 0.25$ となるケースを考える。これらは、診断対象機器に対する物理的要因（物理情報データベース7内の各種データ）の影響が大きい一方、診断対象機器に対する外部アクセスによるセキュリティ要因（アクセス情報データベース8内の各種データ）が少ないことを意味する。このように、確率分布自体に物理的要因および外部アクセスによるセキュリティ要因に基づくバイアスをかけることで、より正確な診断を実施できる。

[0071] 例えば、 $F'(t) = 0.45$ 、しきい値 $f = 0.4$ 、 $A'(t) = 0.25$ 、しきい値 $a = 0.35$ の場合の出力結果を考える。このとき判別部45は、まず $F'(t)$ が f 以上であることから故障の可能性が高いと判別する。その後、判別部45は、 $A'(t)$ が a 未満であることからサイバー攻撃の可能性は低いと判別する。これにより診断結果は故障の可能性が高い、ということになる。このように、物理的要因や外部アクセスによるセキュリティ要因が加味されたことにより、図6で説明した内容から診断結果が変化している。

[0072] 上述した第3実施形態によれば、次の作用効果を奏する。

[0073] (1) 瞬間故障確率算出部42（演算装置）は、診断対象機器が稼働する物理環境の温度、湿度、振動、風、放射能、塵のうち少なくとも一つに関する情報である物理情報データベース7を用いて瞬間故障確率を算出する。このようにしたので、瞬間故障確率の精度が向上し、故障の有無をより正確に診断することができる。

[0074] (2) 瞬間攻撃確率算出部43（演算装置）は、診断対象機器の設置場所のセキュリティ状況に関する情報である物理アクセスデータ81、および診断対象機器に外部からネットワーク経由でアクセスする経路のセキュリティ状況に関する情報であるネットワークデータ82を用いて瞬間攻撃確率を算出する。物理アクセスデータ81およびネットワークデータ82のうち少なくとも一つの情報を用いて瞬間攻撃確率を算出ことで、算出される瞬間攻撃確率の精度が向上し、サイバー攻撃の有無をより正確に診断することができる。

る。

[0075] 次のような変形例も本発明の範囲内であり、変形例に示す構成と上述の実施形態で説明した構成を組み合わせたり、上述の異なる実施形態で説明した構成同士を組み合わせたり、以下の異なる変形例で説明する構成同士を組み合わせることも可能である。

[0076] <変形例 1>

累積故障分布関数 $F(t)$ は、式 (4) で説明したものと異なってもよい。例えば故障密度関数 $f(t)$ ではなく、信頼度関数 $R(t)$ を用いて累積故障分布関数 $F(t)$ をしてもよい。この場合、累積故障分布関数 $F(t)$ は $1 - R(t)$ と定義し、瞬間故障確率は診断時刻 t_1 を用いて $1 - R(t_1)$ という形で算出すればよい。他にも、例えば、パラメータデータベース 2 内の各種パラメータと時間を変数として持つ関数を診断対象機器の特性から事前に算出しておき、診断時刻 t_1 をその関数に代入し確率を算出するようにしてもよい。

[0077] <変形例 2>

セキュリティ評価値 $Risk$ は、式 (8) で説明したものと異なってもよい。例えば脆弱性そのものの基本特性以外に、現在の脆弱性の深刻度を加味したり、ユーザの利用環境を含めた最終的な脆弱性を用いてセキュリティ評価値 $Risk$ を算出してもよい。

[0078] <変形例 3>

上述の説明では、故障密度関数 $f(t)$ の例としてワイブル分布を、攻撃密度関数 $a(t)$ の例としてガウス分布を挙げたが、確率分布の種類はこれに限るものではない。他の確率分布を故障密度関数 $f(t)$ や攻撃密度関数 $a(t)$ として用いてもよい。

[0079] <変形例 4>

調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ の算出方法は、式 (12) および式 (13) で例示したものと異なってもよい。例えば、距離尺度を演算後、故障密度関数 $f(t)$ および攻撃密度関数

$a(t)$ に算出した距離尺度を乗算したものを時刻 0 から診断時刻 t_1 までそれぞれ積分することにより、調整後瞬間故障確率 $F'(t)$ および調整後瞬間攻撃確率 $A'(t)$ を算出するようにしてもよい。また、上述の各実施形態では、式 (11) に示した確率距離尺度を用いて瞬間故障確率と瞬間攻撃確率とを同次元化していたが、それ以外の方法で、瞬間故障確率と瞬間攻撃確率とを比較可能にしてもよい。

[0080] <変形例 5>

上述した各種のデータベース（パラメータデータベース 2、脆弱性データベース 3、保守点検データベース 5、物理情報データベース 7、およびアクセス情報データベース 8）に格納するデータは、上述したデータと異なってもよい。また、その利用方法についても、上述した各実施形態と異なってもよい。

[0081] 以上、本発明の実施形態について説明したが、上記実施形態は本発明の適用例の一部を示したに過ぎず、本発明の技術的範囲を上記実施形態の具体的構成に限定する趣旨ではない。

符号の説明

[0082] 1、100、200…診断装置、2…パラメータデータベース、3…脆弱性データベース、4…表示装置、5…保守点検データベース、7…物理情報データベース、8…アクセス情報データベース、11…演算装置、12…不揮発性メモリ、13…揮発性メモリ、14…入出力インタフェース、21…形状パラメータ、22…尺度パラメータ、23…位置パラメータ、31…公開日データ、32…機器データ、41…時刻入力部、42…瞬間故障確率算出部、43…瞬間攻撃確率算出部、44…確率調整部、45…判別部、46…出力部、47…保守リスク評価値算出部、51…保守点検データ、52…保守員データ、53…操作ログデータ、71…温度データ、72…湿度データ、73…振動データ、81…物理アクセスデータ、82…ネットワークデータ

請求の範囲

- [請求項1] 演算装置を備えた診断装置であって、
前記演算装置は、
診断対象機器に対して所定の時刻にサイバー攻撃が実施された確率である瞬間攻撃確率を算出し、
前記診断対象機器において前記所定の時刻に故障が生じた確率である瞬間故障確率を算出し、
前記瞬間攻撃確率と前記瞬間故障確率とに基づき、前記所定の時刻における、前記診断対象機器に対するサイバー攻撃の有無および前記診断対象機器における故障の有無を判定する、
診断装置。
- [請求項2] 請求項1に記載の診断装置において、
前記演算装置は、
前記瞬間攻撃確率および前記瞬間故障確率をそれぞれ所定の閾値と比較することにより、前記診断対象機器に対するサイバー攻撃の有無および前記診断対象機器における故障の有無を判定する診断装置。
- [請求項3] 請求項1に記載の診断装置において、
前記演算装置は、
時間変化する第1の確率分布を用いて前記瞬間攻撃確率を算出し、時間変化した前記第1の確率分布とは異なる第2の確率分布を用いて前記瞬間故障確率を算出する診断装置。
- [請求項4] 請求項1に記載の診断装置において、
前記演算装置は、
前記診断対象機器が故障する確率の確率分布の形状、尺度、および位置の特徴を表すパラメータの少なくとも一つを用いて前記瞬間故障確率を算出する診断装置。
- [請求項5] 請求項1に記載の診断装置において、
前記演算装置は、

前記診断対象機器を構成するハードウェアまたはソフトウェアに関連する脆弱性情報を用いて前記瞬間攻撃確率を算出する診断装置。

[請求項6] 請求項1に記載の診断装置において、
前記演算装置は、
前記瞬間攻撃確率および前記瞬間故障確率を同次元化する調整を行う診断装置。

[請求項7] 請求項1に記載の診断装置において、
前記演算装置は、
前記演算装置により判定された前記診断対象機器に対するサイバー攻撃の有無、および、前記演算装置により判定された前記診断対象機器における故障の有無を表示装置に表示させる診断装置。

[請求項8] 請求項1に記載の診断装置において、
前記演算装置は、
前記診断対象機器の保守点検に関する情報、前記診断対象機器の保守点検を行う保守員に関する情報、および前記診断対象機器の保守点検において成された操作の操作ログに関する情報の少なくとも一つを用いて前記瞬間攻撃確率を算出する診断装置。

[請求項9] 請求項1に記載の診断装置において、
前記演算装置は、
前記診断対象機器が稼働する物理環境の温度、湿度、振動、風、放射能、塵のうち少なくとも一つに関する情報を用いて前記瞬間故障確率を算出する診断装置。

[請求項10] 請求項1に記載の診断装置において、
前記演算装置は、
前記診断対象機器の設置場所のセキュリティ状況に関する情報、および前記診断対象機器に外部からネットワーク経由でアクセスする経路のセキュリティ状況に関する情報のうち少なくとも一つの情報を用いて前記瞬間攻撃確率を算出する診断装置。

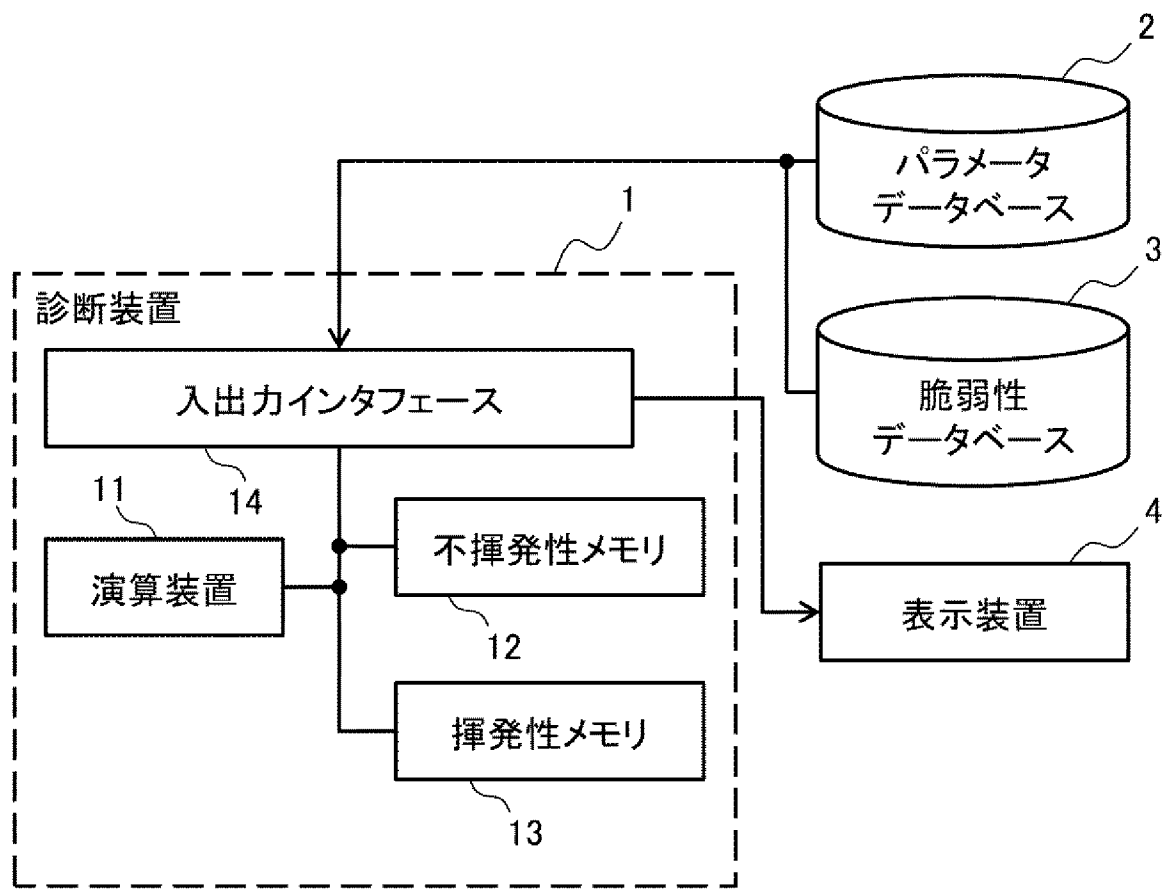
[請求項11] 診断対象機器に対して所定の時刻にサイバー攻撃が実施された確率である瞬間攻撃確率を算出し、

 前記診断対象機器において前記所定の時刻に故障が生じた確率である瞬間故障確率を算出し、

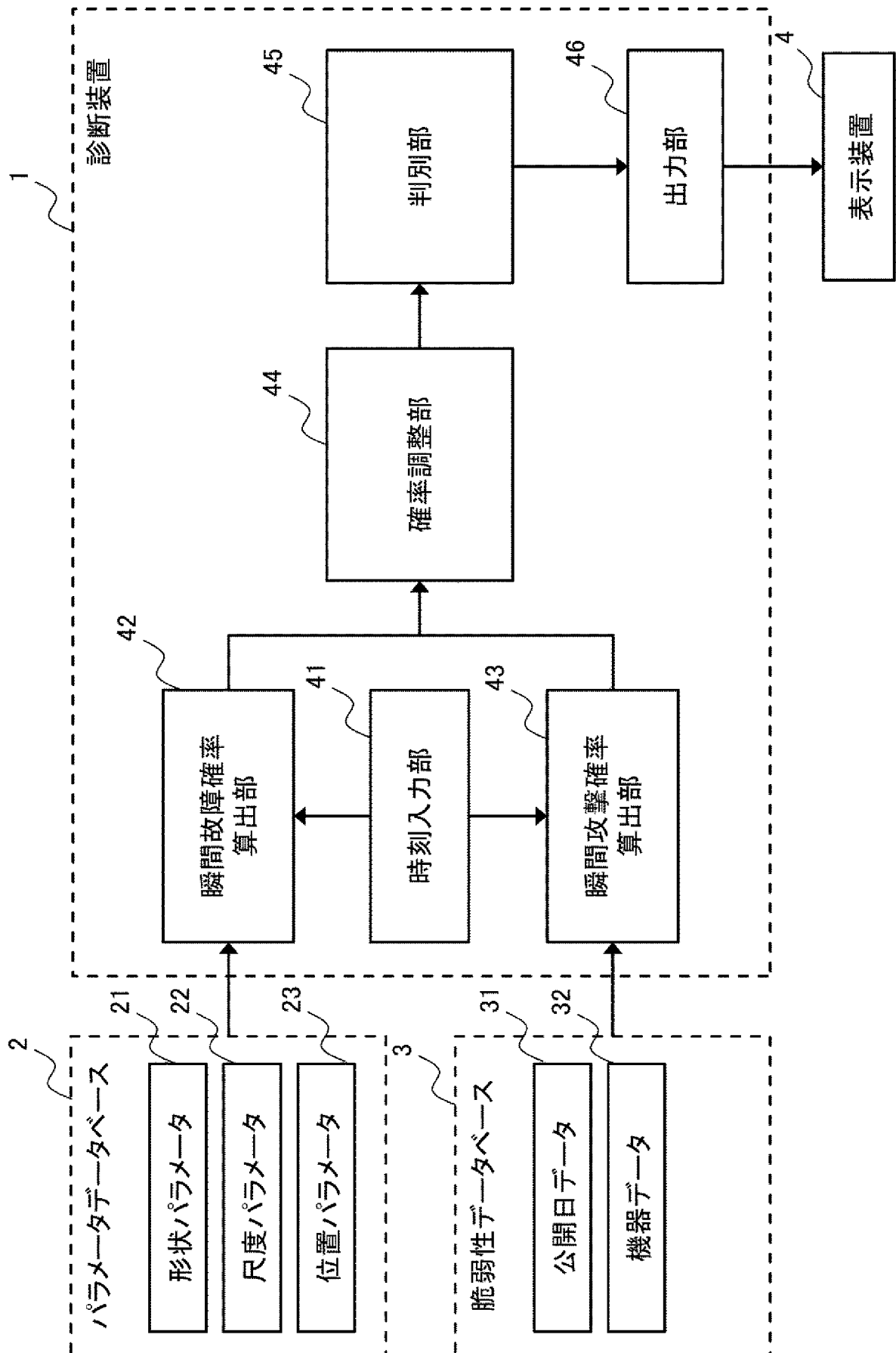
 前記瞬間攻撃確率と前記瞬間故障確率とに基づき、前記所定の時刻における、前記診断対象機器に対するサイバー攻撃の有無および前記診断対象機器における故障の有無を判定する、

 診断方法。

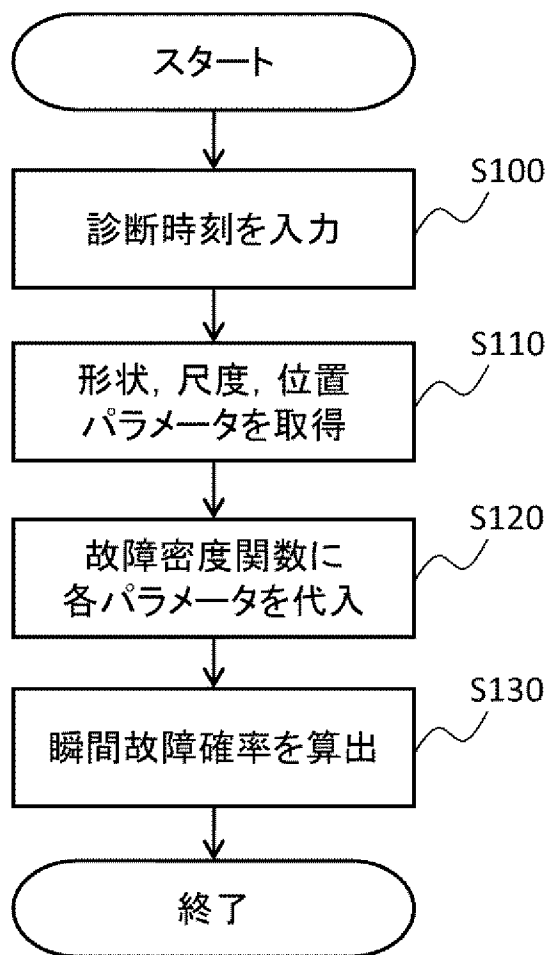
[図1]



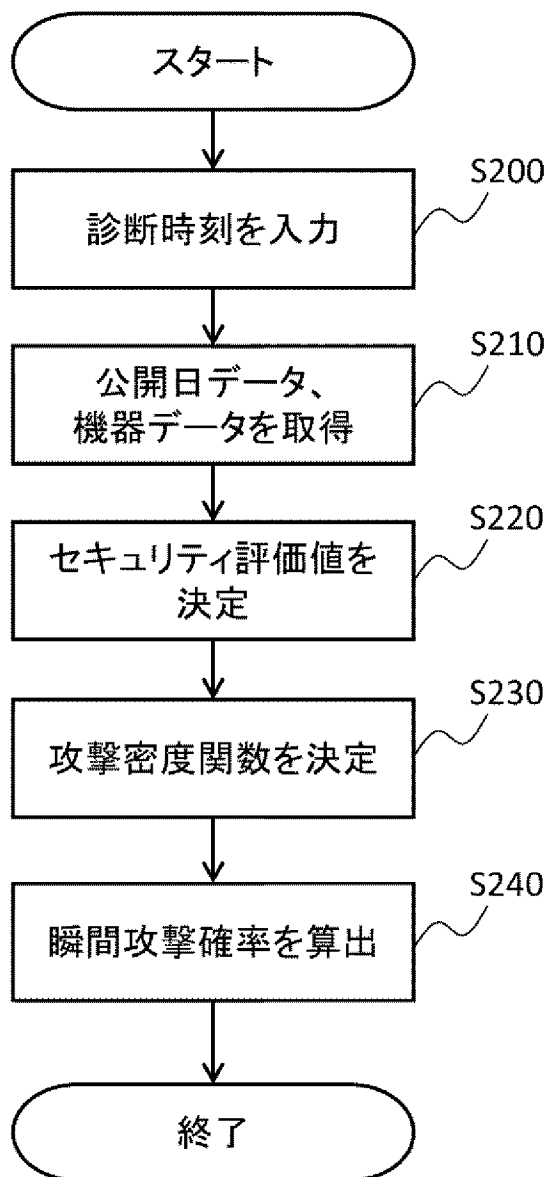
[図2]



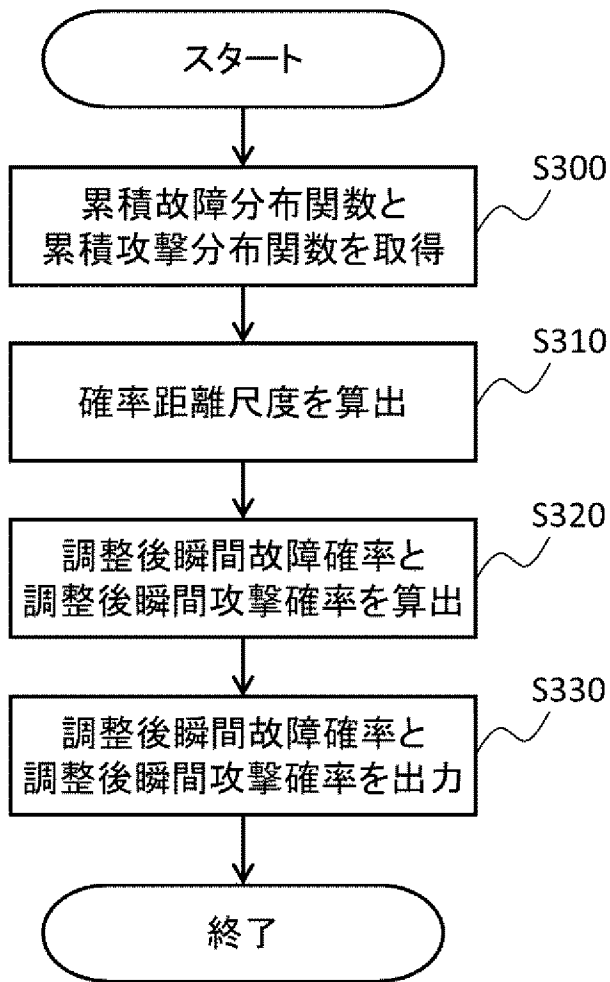
[図3]



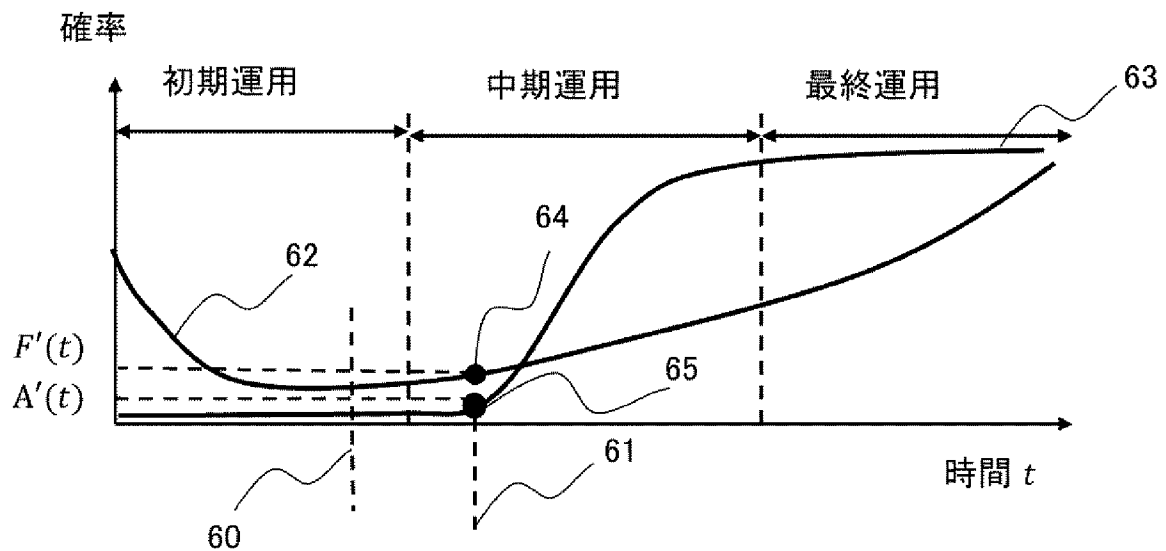
[図4]



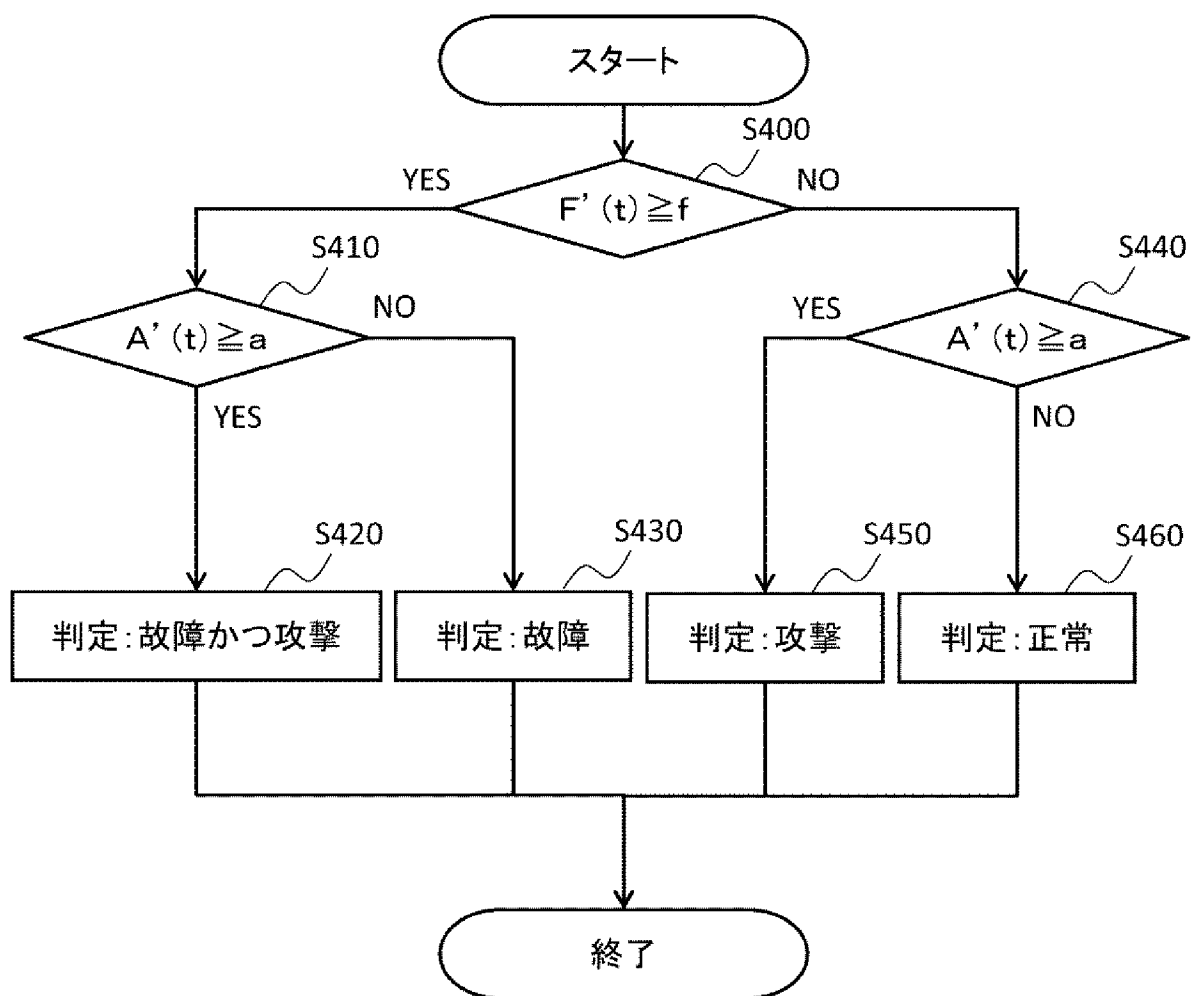
[図5]



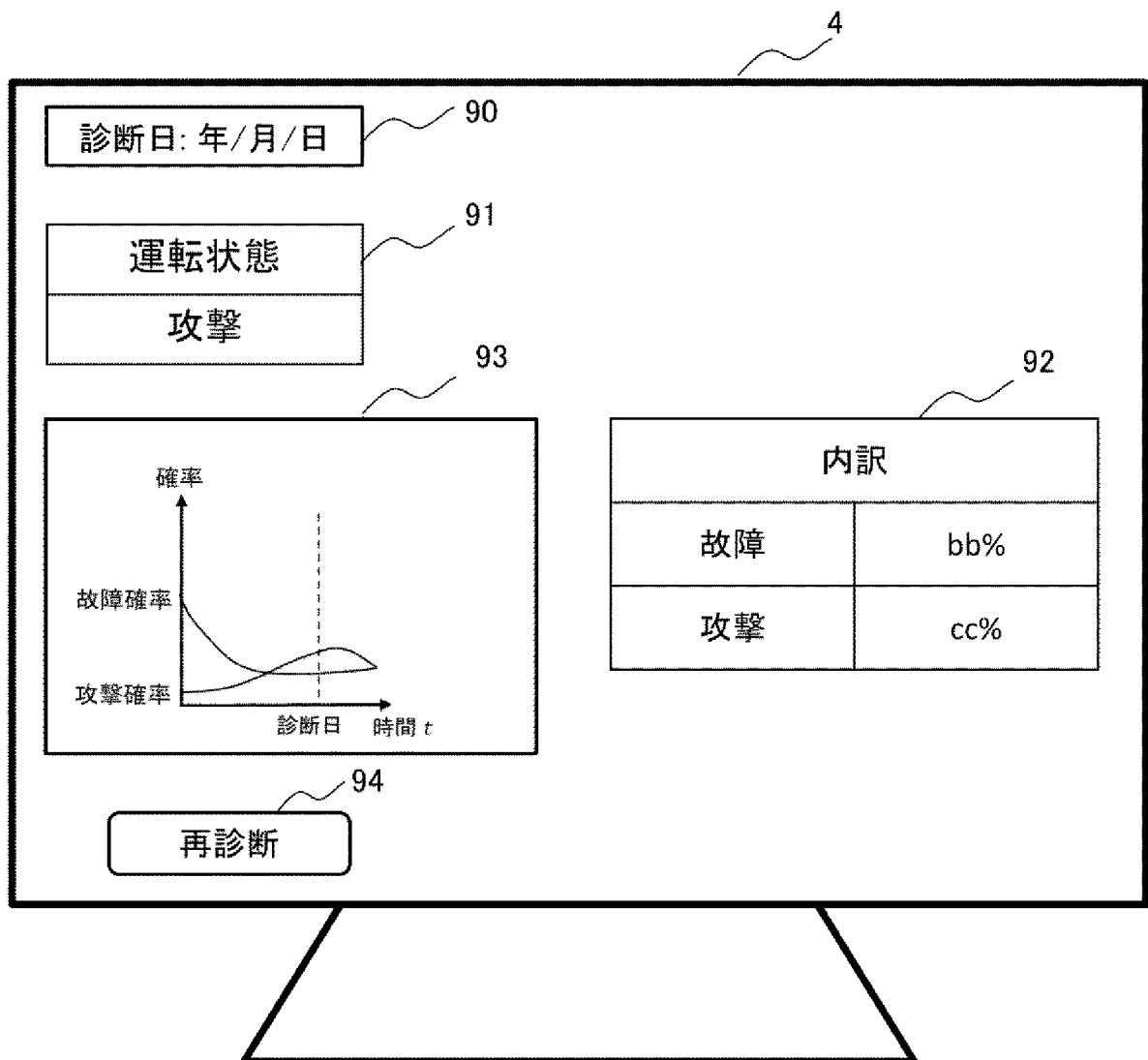
[図6]



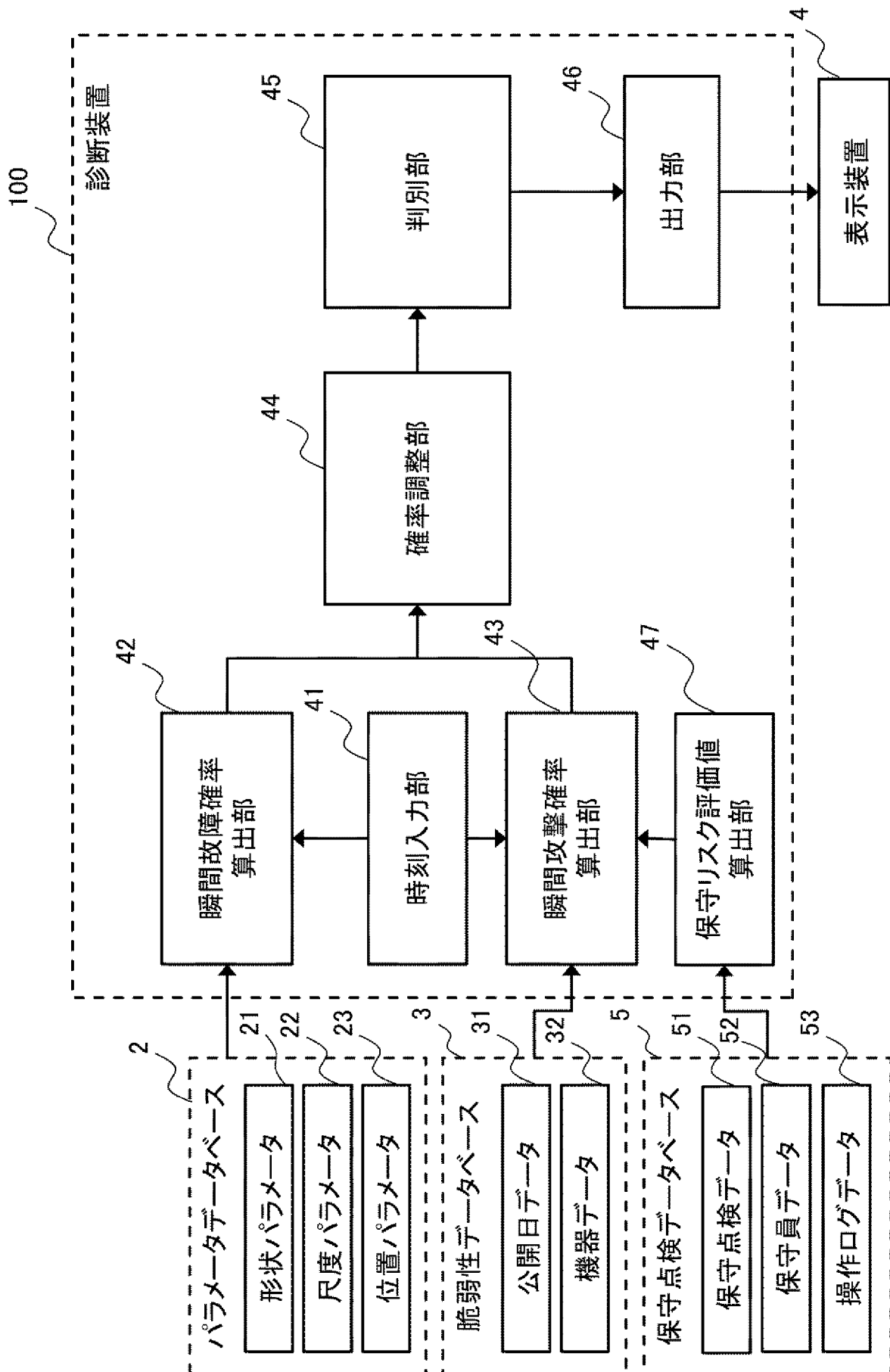
[図7]



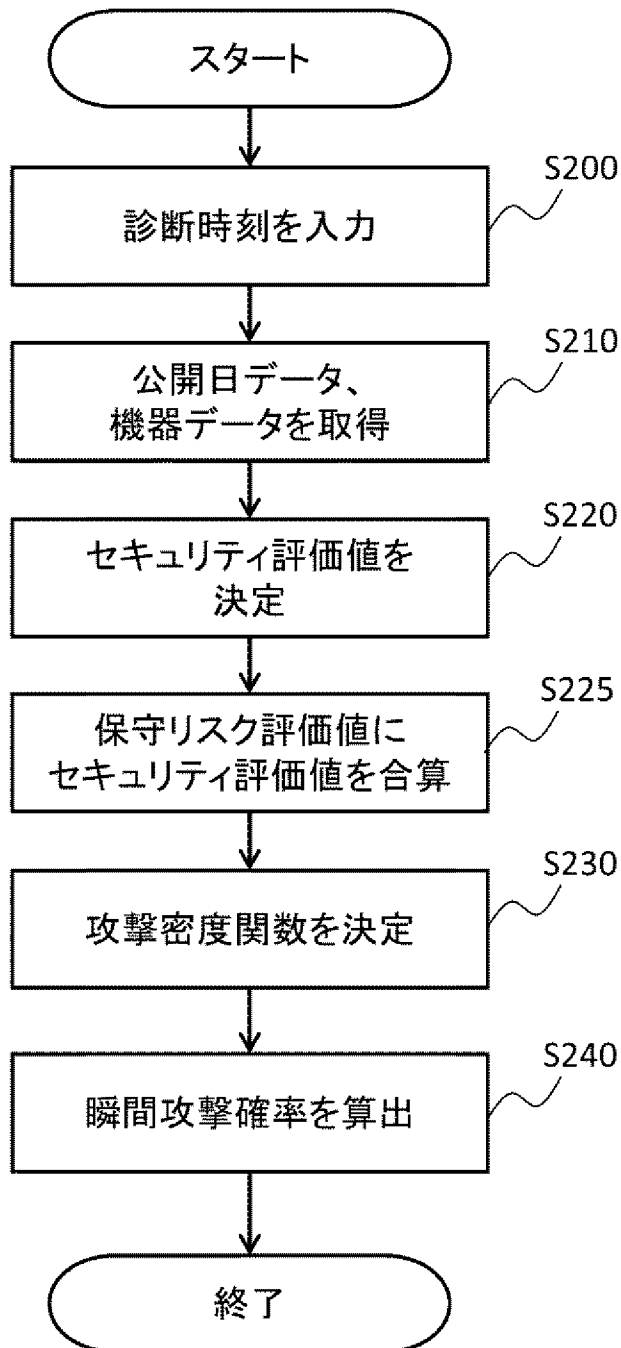
[図8]



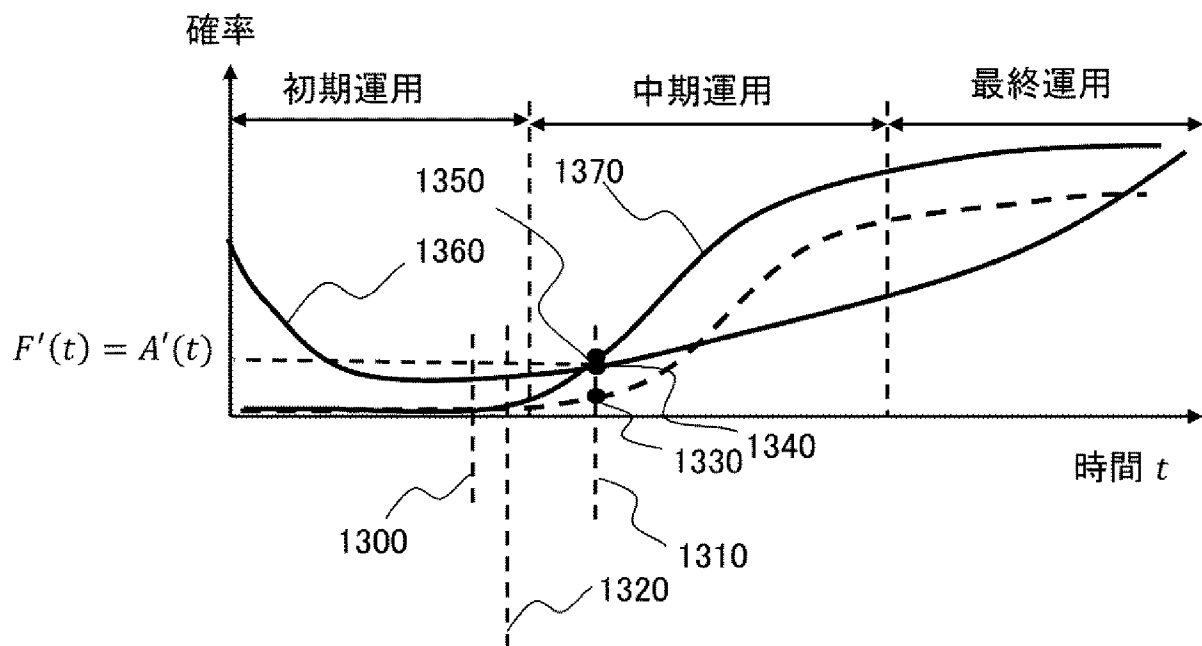
[図9]



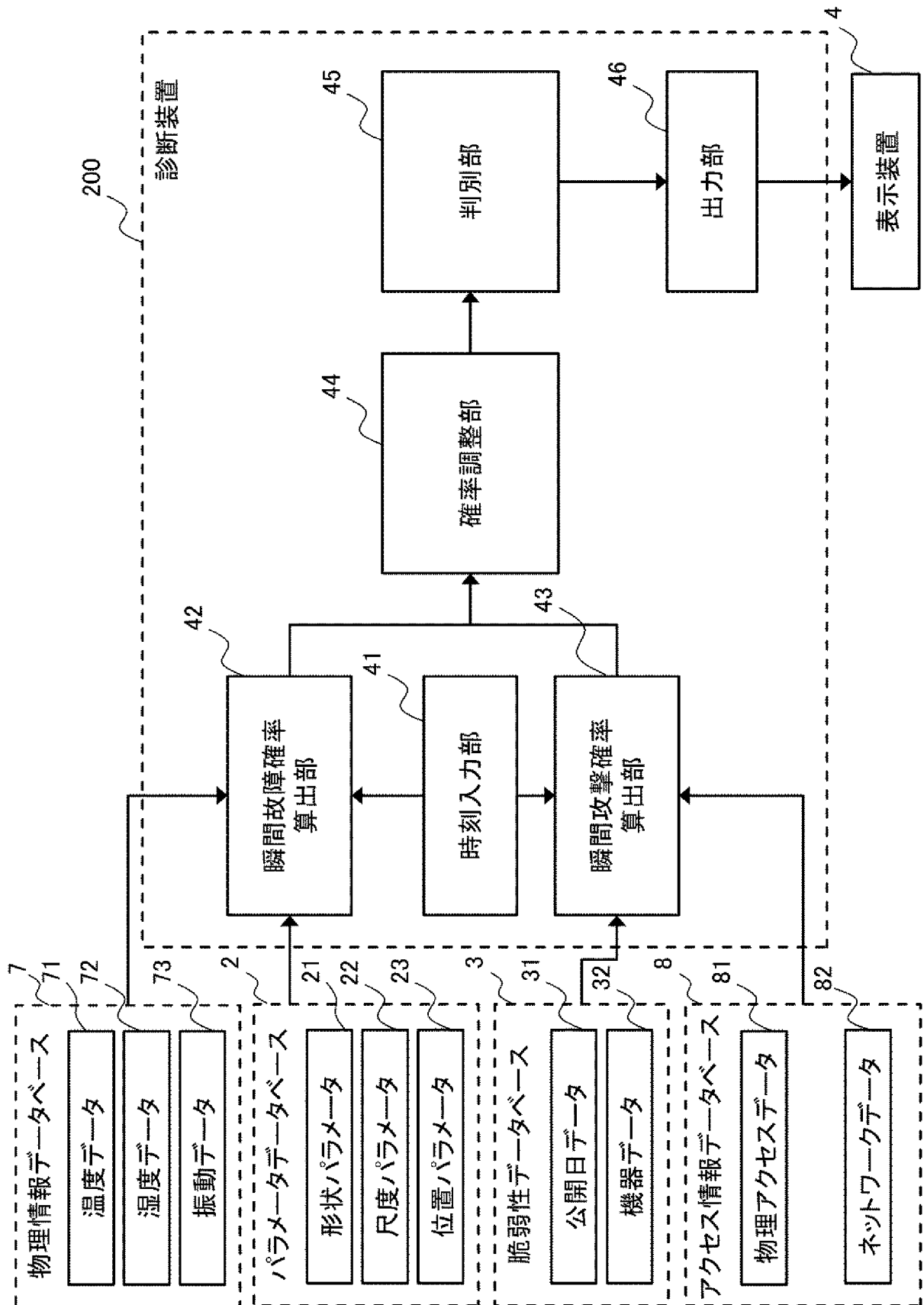
[図10]



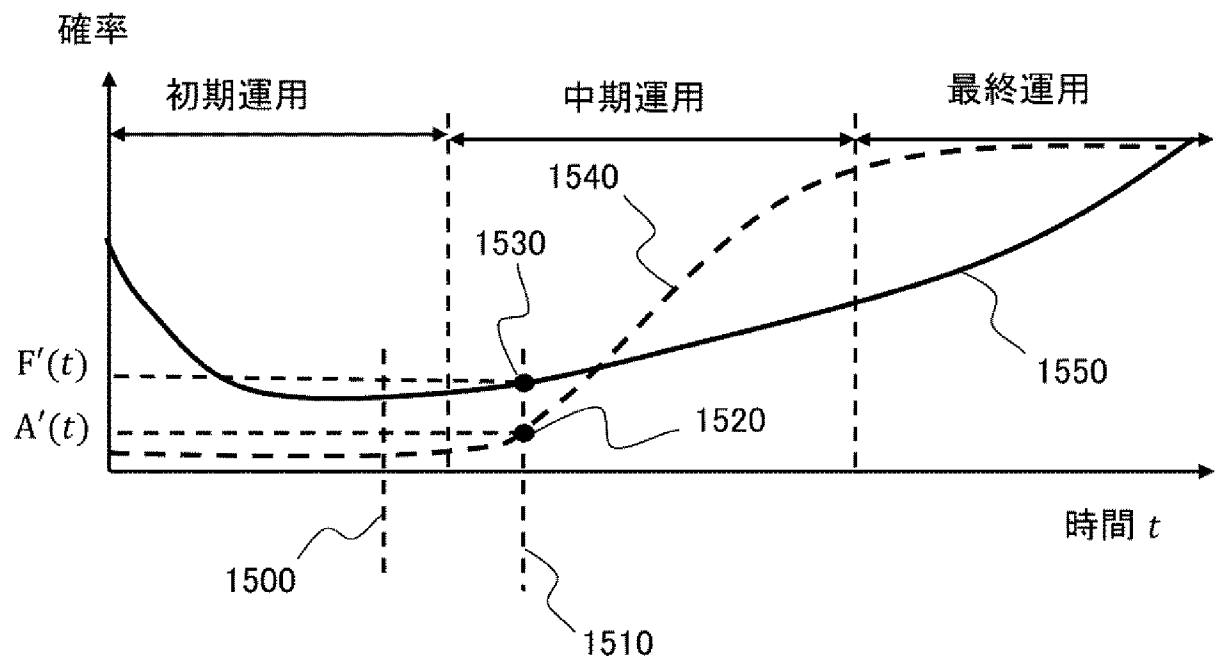
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/017050

A. CLASSIFICATION OF SUBJECT MATTER <i>G05B 23/02</i> (2006.01)i; <i>G06F 21/55</i> (2013.01)i FI: G05B23/02 T; G05B23/02 302Z; G06F21/55 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G05B23/02; G06F21/55 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2024 Registered utility model specifications of Japan 1996-2024 Published registered utility model applications of Japan 1994-2024 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2020-61717 A (KABUSHIKI KAISHA TOSHIBA) 16 April 2020 (2020-04-16) paragraphs [0005]-[0007], [0012]-[0046], fig. 1-8	1-5, 7-11 6
Y	JP 2019-61565 A (PANASONIC IP CORP. AMERICA) 18 April 2019 (2019-04-18) paragraphs [0011]-[0012], [0033]-[0073], fig. 1-4	1-5, 7-11
Y	JP 2019-212143 A (HITACHI, LTD.) 12 December 2019 (2019-12-12) paragraph [0018]	3, 5
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “D” document cited by the applicant in the international application “E” earlier application or patent but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family		
Date of the actual completion of the international search 28 June 2024		Date of mailing of the international search report 09 July 2024
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/017050

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2020-61717	A	16 April 2020	(Family: none)	
JP	2019-61565	A	18 April 2019	US 2019/0095300 A1 paragraphs [0018]-[0019], [0041]-[0081], fig. 1-4 EP 3462267 A1 CN 109558293 A	
JP	2019-212143	A	12 December 2019	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC））

G05B 23/02(2006.01)i; G06F 21/55(2013.01)i

FI: G05B23/02 T; G05B23/02 302Z; G06F21/55

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

G05B23/02; G06F21/55

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報

1922 - 1996年

日本国公開実用新案公報

1971 - 2024年

日本国実用新案登録公報

1996 - 2024年

日本国登録実用新案公報

1994 - 2024年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2020-61717 A（株式会社東芝）16.04.2020（2020 - 04 - 16） 段落[0005]-[0007], [0012]-[0046], 図1-8	1-5, 7-11
A		6
Y	JP 2019-61565 A（パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ）18.04.2019（2019 - 04 - 18） 段落[0011]-[0012], [0033]-[0073], 図1-4	1-5, 7-11
Y	JP 2019-212143 A（株式会社日立製作所）12.12.2019（2019 - 12 - 12） 段落[0018]	3, 5

☐ C欄の続きにも文献が列挙されている。

☒ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

“A” 特に関連のある文献ではなく、一般的技术水準を示すもの

“D” 国際出願で出願人が先行技術文献として記載した文献

“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

“O” 口頭による開示、使用、展示等に言及する文献

“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの

“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

“&” 同一パテントファミリー文献

国際調査を完了した日

28.06.2024

国際調査報告の発送日

09.07.2024

名称及びあて先

日本国特許庁(ISA/JP)

〒100-8915

日本国

東京都千代田区霞が関三丁目4番3号

権限のある職員（特許庁審査官）

影山 直洋 3U 5785

電話番号 03-3581-1101 内線 3364

様式 PCT/ISA/210（第2ページ）（2022年7月）

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2024/017050

引用文献			公表日	パテントファミリー文献	公表日
JP	2020-61717	A	16.04.2020	(ファミリーなし)	
JP	2019-61565	A	18.04.2019	US 2019/0095300 A1 段落[0018]-[0019], [0041]- [0081], 図1-4	
				EP 3462267 A1	
				CN 109558293 A	
JP	2019-212143	A	12.12.2019	(ファミリーなし)	