(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
2020年8月27日(27.08.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/170911 A1

(51) 国際特許分類:
G06F 21/55 (2013.01) *G06F 16/28* (2019.01)

(21) 国際出願番号： PCT/JP2020/005377

(22) 国際出願日： 2020年2月12日(12.02.2020)

(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 2019-028716 2019年2月20日(20.02.2019) JP

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 風戸 雄太(**KAZATO, Yuta**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

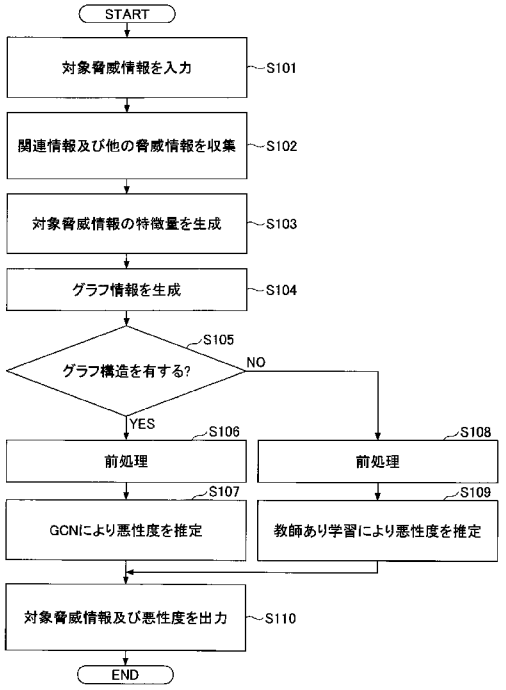
(74) 代理人: 伊東 忠重, 外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 Tokyo (JP).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** ESTIMATION DEVICE, ESTIMATION METHOD, AND PROGRAM

(54) 発明の名称： 推定装置、推定方法及びプログラム

[図3]



S101 Input subject threat information
S102 Collect related information and other threat information
S103 Generate feature amount of subject threat information
S104 Generate graph information
S105 Does graph structure exist?
S106, S108 Preprocessing
S107 Estimate degree of maliciousness by means of GCN
S109 Estimate degree of maliciousness by means of supervised learning
S110 Output subject threat information and degree of maliciousness

(57) **Abstract:** An estimation device characterized by having: a collection means that, when threat information for which a degree of maliciousness is to be estimated is input, collects related information related to the threat information, and other threat information different from the threat information; a feature amount generation means for generating a feature amount indicating a feature of the threat information, on the basis of the related information; a graph information generation means for generating, on the basis of the related information and the other threat information, graph information indicating

WO 2020/170911 A1

［続葉有］

MA, MD, ME, MG, MK, MN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))

a graph in which each item of threat information and the other threat information is a node and a relationship between the nodes is an edge; and an estimation means that, when a graph structure exists between the threat information and the other threat information on the graph indicated by the graph information, uses the feature amount of the threat information to estimate a degree of maliciousness for the threat information by means of a graph convolutional neural network.

(57) 要約:悪性度の推定対象の脅威情報が入力されると、前記脅威情報に関連する関連情報と、前記脅威情報とは異なる他の脅威情報とを収集する収集手段と、前記関連情報に基づいて、前記脅威情報の特徴を表す特徴量を生成する特徴量生成手段と、前記関連情報と前記他の脅威情報とに基づいて、前記脅威情報及び前記他の脅威情報のそれぞれをノード、該ノード間の関連をエッジとするグラフを示すグラフ情報を生成するグラフ情報生成手段と、前記グラフ情報により示されるグラフ上で前記脅威情報と前記他の脅威情報の間にグラフ構造が存在する場合、前記脅威情報の特徴量を用いて、グラフ畳み込みニューラルネットワークにより、前記脅威情報の悪性度を推定する推定手段と、を有することを特徴とする。

明　細　書

発明の名称 ： 推定装置、推定方法及びプログラム

技術分野

[0001] 本発明は、推定装置、推定方法及びプログラムに関する。

背景技術

[0002] 近年、脅威情報（ＣＴＩ：Cyber Threat Intelligence）を活用したセキュリティオペレーションが行われている。脅威情報とは、サイバー攻撃や脅威に関連する攻撃者、攻撃目的、攻撃手法等に関する情報を収集・蓄積し、その分析を行うことで、攻撃検知や対処等のセキュリティオペレーションに活用可能な情報のことである。脅威情報としては、例えば、攻撃者が利用したＩＰ（Internet Protocol）アドレスやドメイン名、ＵＲＬ（Uniform Resource Locator）等のＩｏＣ（Indicator of Compromise）情報、攻撃への対処方法（Course of Action）に関する情報、マルウェアのハッシュ値等が挙げられる。

[0003] このような脅威情報の指標の１つとして、悪性度（Maliciousness）が知られており、脅威情報に対する優先度の決定や意思決定の判断等に用いられている。悪性度とは、ドメイン名やＵＲＬ等の脅威情報がサイバー攻撃に使用されている可能性の度合いを示す指標であり、例えば、当該脅威情報が悪性である確率で表される。このため、悪性度が正確である程、迅速かつ正確なセキュリティオペレーション等が実現可能となる。なお、脅威情報の情報源としては、例えば、セキュリティ企業の脅威情報提供サービス、攻撃通信を検知する攻撃検知装置からのアラート情報、オープンソースインテリジェンス（ＯＳＩＮＴ：open-source intelligence）等が挙げられる。

[0004] 脅威情報の悪性度を算出する従来技術として、脅威情報を「ノード」、互いに関連する脅威情報間の接続を「エッジ」としたグラフを用いて、グラフ分析手法によって悪性度を推定する技術が知られている。例えば、ページランク手法を用いて悪性度を計算する技術（非特許文献１）やグラフ伝播手法

によって悪性度を推定する技術（非特許文献２）が知られている。また、２部グラフ上での確率伝搬法を用いて、脅威スコアを算出する技術も知られている（非特許文献３）。

先行技術文献

非特許文献

[0005] 非特許文献1：Boukhtouta, Amine, et al. "Graph-theoretic characterization of cyber-threat infrastructures." Digital Investigation 14 (2015): S3-S15

非特許文献2：WANG, Xin, et al. "Poster: An Approach to Verifying Threat Intelligence Based on Graph Propagation." IEEE S&P 2018 Poster

非特許文献3：風戸雄太，福田健介，菅原俊治．"DNS グラフ上でのグラフ分析と脅威スコア伝播による悪性ドメイン特定." コンピュータ ソフトウェア 33.3 (2016): 3_16-3_2

発明の概要

発明が解決しようとする課題

[0006] しかしながら、従来技術では、脅威情報自体の特徴を利用できないため、悪性度の推定精度が高くない場合があった。

[0007] 本発明は、上記の点に鑑みてなされたもので、脅威情報の悪性度を高い精度で推定することも目的とする。

課題を解決するための手段

[0008] 上記目的を達成するため、本発明の実施の形態は、悪性度の推定対象の脅威情報が入力されると、前記脅威情報に関連する関連情報と、前記脅威情報とは異なる他の脅威情報とを収集する収集手段と、前記関連情報に基づいて、前記脅威情報の特徴を表す特徴量を生成する特徴量生成手段と、前記関連情報と前記他の脅威情報とに基づいて、前記脅威情報及び前記他の脅威情報のそれぞれをノード、該ノード間の関連をエッジとするグラフを示すグラフ情報を生成するグラフ情報生成手段と、前記グラフ情報により示されるグラ

フ上で前記脅威情報と前記他の脅威情報の間にグラフ構造が存在する場合、前記脅威情報の特徴量を用いて、グラフ畳み込みニューラルネットワークにより、前記脅威情報の悪性度を推定する推定手段と、を有することを特徴とする。

発明の効果

[0009] 脅威情報の悪性度を高い精度で推定することができる。

図面の簡単な説明

[0010] [図1]本発明の実施の形態における悪性度推定システムの全体構成の一例を示す図である。

[図2]本発明の実施の形態における悪性度推定装置のハードウェア構成の一例を示す図である。

[図3]本発明の実施の形態における悪性度推定処理の一例を示すフローチャートである。

発明を実施するための形態

[0011] 以下、本発明の実施の形態について説明する。本発明の実施の形態では、脅威情報の特徴を表す特徴量と、悪性度の推定対象の脅威情報（以降、「対象脅威情報」とも表す。）と他の脅威情報との関連性（グラフ構造）とを用いて、グラフ畳み込みニューラルネットワーク（ＧＣＮ：Graph Convolutional Networks又はGraph Convolutional Neural Networks）によって対象脅威情報の悪性度を推定する。また、本発明の実施の形態では、対象脅威情報が他の脅威情報と関連性がない場合（すなわち、対象脅威情報がグラフ上で単独であり、他の脅威情報との間でグラフ構造を有しない場合）には、特徴量を用いて、教師あり学習で学習した所定のモデルによって対象脅威情報の悪性度を推定する。

[0012] そこで、以降の本発明の実施の形態では、各脅威情報の特徴を用いて、対象脅威情報が他の脅威情報との間でグラフ構造を有する場合にはグラフ畳み込みニューラルネットワークによって悪性度を推定し、対象脅威情報が他の脅威情報との間でグラフ構造を有しない場合には教師あり学習で学習した所

定のモデルによって悪性度を推定する悪性度推定システム１について説明する。

[0013] ＜悪性度推定システム１の全体構成＞

まず、本発明の実施の形態における悪性度推定システム１の全体構成について、図１を参照しながら説明する。図１は、本発明の実施の形態における悪性度推定システム１の全体構成の一例を示す図である。

[0014] 図１に示すように、本発明の実施の形態における悪性度推定システム１には、悪性度推定装置１０と、各種の外部装置２０とが含まれる。悪性度推定装置１０と、各種の外部装置２０とは、任意のネットワーク（例えば、インターネットや社内ＬＡＮ（Local Area Network）等）を介して通信可能に接続される。ここで、外部装置２０としては、例えば、脅威情報管理装置２１、フロー観測情報管理装置２２、攻撃検知装置２３、ＯＳＩＮＴサーバ２４、ＤＮＳサーバ２５、及びＷＨＯＩＳ／ＲＤＡＰサーバ２６等が挙げられる。

[0015] 悪性度推定装置１０は、対象脅威情報が入力されると、対象脅威情報に関連する情報（以降、「関連情報」とも表す。）や他の脅威情報等を収集した上で、これら対象脅威情報や関連情報、他の脅威情報等を用いて、対象脅威情報の悪性度を推定する。このとき、悪性度推定装置１０は、対象脅威情報の特徴量を生成すると共に、対象脅威情報が他の脅威情報とグラフ構造を有するか否かを判定した上で、この判定結果に応じて、グラフ畳み込みニューラルネットワーク又は教師あり学習で学習した所定のモデルのいずれかによって対象脅威情報の悪性度を推定する。なお、他の脅威情報とは、対象脅威情報以外の脅威情報のことを意味する。

[0016] 脅威情報管理装置２１は、過去に登録、共有、分析、又は利用（以降、登録、共有、分析、利用をまとめて「利用等」とも表す。）された脅威情報を蓄積・管理するＤＢ（データベース）である。脅威情報管理装置２１には、脅威情報に加えて、この脅威情報の悪性度（過去に推定又は設定された悪性度）と特徴量（過去に生成された特徴量）も蓄積・管理されているものとす

る。

[0017] フロー観測情報管理装置２２は、ネットワーク上に存在するフローエクスポータやフローコレクタ等から収集したフロー観測情報を格納・管理するＤＢである。

[0018] 攻撃検知装置２３は、ファイアウォールやＩＤＳ（Intrusion Detection System）／ＩＰＳ（Intrusion Prevention System）等のサイバー攻撃を検知・遮断するためのソフトウェア又はネットワーク機器である。

[0019] ＯＳＩＮＴサーバ２４は、オープンソースインテリジェンスの公開情報を提供するサーバである。ＯＳＩＮＴサーバ２４は、例えばＷｅｂページ等の形態で、オープンソースインテリジェンスの公開情報を提供する。

[0020] ＤＮＳサーバ２５は、ドメイン名とＩＰアドレスとの間の名前解決（又は「アドレス解決」とも称される。）を行うサーバである。

[0021] ＷＨＯＩＳ／ＲＤＡＰサーバ２６は、ＩＰアドレスやドメイン名の所有者情報を提供するサーバである。

[0022] ここで、図１に示すように、悪性度推定装置１０は、機能部として、入力部１０１と、情報収集部１０２と、特徴量生成部１０３と、グラフ情報生成部１０４と、悪性度計算部１０５と、出力部１０６とを有する。

[0023] 入力部１０１は、対象脅威情報を入力する。なお、入力部１０１は、予め決められた任意の入力元から対象脅威情報を入力すればよい。例えば、入力部１０１は、メモリ等の記憶装置に格納されている対象脅威情報を入力してもよいし、ネットワークを介して接続された他の装置から受信した対象脅威情報を入力してもよい。

[0024] 情報収集部１０２は、関連情報や他の脅威情報を収集する。ここで、情報収集部１０２には、ＮＷ情報収集部１１１と、ＯＳＩＮＴ収集部１１２と、脅威情報収集部１１３とが含まれる。

[0025] ＮＷ情報収集部１１１は、ネットワークで観測可能な関連情報を収集する。例えば、ＮＷ情報収集部１１１は、フロー観測情報管理装置２２に問い合わせて、対象脅威情報に関連するフロー観測情報を収集する。また、例えば

、ＮＷ情報収集部１１１は、ＤＮＳサーバ２５に問い合わせて、対象脅威情報に含まれるドメイン名やＩＰアドレスを名前解決した情報（名前解決結果情報）を収集する。同様に、例えば、ＮＷ情報収集部１１１は、ＷＨＯＩＳ／ＲＤＡＰサーバ２６に問い合わせて、対象脅威情報に含まれるドメイン名やＩＰアドレスの所有者情報を収集する。

[0026] なお、例えば、ＮＷ情報収集部１１１は、攻撃検知装置２３に問い合わせて、対象脅威情報に関連するアラート情報を関連情報として収集してもよい。アラート情報も関連情報として収集されることで、例えば、各脅威情報（対象脅威情報及び他の脅威情報）の関連を表すグラフ構造からグラフ情報を生成する際に利用したり、推定された悪性度（つまり、対象脅威情報の悪性度）の根拠情報として利用したりすることが可能となる。

[0027] ＯＳＩＮＴ収集部１１２は、オープンソースインテリジェンスの公開情報を収集する。すなわち、ＯＳＩＮＴ収集部１１２は、ＯＳＩＮＴサーバ２４に問い合わせて、対象脅威情報に関連する公開情報を収集する。なお、ＯＳＩＮＴ収集部１１２によって収集される公開情報としては、例えば、ＡＳ（Autonomous System）番号結果を示す情報、ＧｅｏＩＰの検索結果を示す情報、レピュテーションサービスから得られる情報等が挙げられる。

[0028] 脅威情報収集部１１３は、他の脅威情報を収集する。すなわち、脅威情報収集部１１３は、脅威情報管理装置２１に問い合わせて、過去に利用等された他の脅威情報を収集する。なお、他の脅威情報の関連情報も脅威情報管理装置２１に蓄積・管理されていてもよく、この場合には、脅威情報収集部１１３は、他の脅威情報に加えて、他の脅威情報の関連情報を収集してもよい。

[0029] 特徴量生成部１０３は、対象脅威情報に含まれるドメイン名やＵＲＬ等と、ＮＷ情報収集部１１１やＯＳＩＮＴ収集部１１２により収集された関連情報とを用いて、対象脅威情報の特徴量を生成する。

[0030] グラフ情報生成部１０４は、対象脅威情報と、情報収集部１０２により収集された関連情報及び他の脅威情報とを用いて、各脅威情報（対象脅威情報

及び他の脅威情報）の関連を表すグラフ構造からグラフ情報（ノード情報及びグラフ情報）を生成する。

[0031] 悪性度計算部１０５は、グラフ情報生成部１０４により生成されたグラフ情報を用いて、対象脅威情報が他の脅威情報との間でグラフ構造を有するか否かを判定する。そして、この判定結果に応じて、悪性度計算部１０５は、各脅威情報（対象脅威情報及び他の脅威情報）の特徴量を用いて、グラフ畳み込みニューラルネットワーク又は教師あり学習で学習した所定のモデルのいずれかによって対象脅威情報の悪性度を推定する。ここで、悪性度計算部１０５には、前処理部１２１と、グラフ畳み込み計算部１２２と、教師あり学習計算部１２３とが含まれる。

[0032] 前処理部１２１は、前処理として、各脅威情報の特徴量のそれぞれを示すデータ（以降、「特徴量データ」とも表す。）の集合を、例えば、教師用集合と、検証用集合と、テスト用集合とに分割する。ここで、教師用集合とは、グラフ畳み込みニューラルネットワークや教師あり学習で学習するモデルの学習に用いられる特徴量データの集合である。また、検証用集合とは、当該学習結果の検証に用いられる特徴量データの集合である。一方で、テスト用集合とは、悪性度の推定に用いられる特徴量データの集合であり、対象脅威情報の特徴量データはテスト用集合に含まれる。

[0033] そして、前処理部１２１は、教師用集合から複数の教師データを作成すると共に、検証用集合から複数の検証用データを作成する。また、前処理部１２１は、テスト用集合からテスト用データを作成する。ここで、教師データ及び検証用データとは、グラフ畳み込みニューラルネットワークや教師あり学習で学習するモデルに入力される入力データに対して、悪性度を示すラベルを付与したデータである。このとき、教師データ及び検証用データに含まれるラベルは、教師データ及び検証用データをそれぞれ構成する特徴量データの悪性度から算出されればよい。一方で、テスト用データとは、グラフ畳み込みニューラルネットワークや教師あり学習で学習するモデルに入力される入力データのことである（つまり、テスト用データにはラベルは付与され

ない）。なお、他の脅威情報の特徴量データと、教師データ及び検証用データにラベルを付与するための悪性度とは、脅威情報管理装置２１に蓄積・管理されているものを用いる。

[0034] グラフ畳み込み計算部１２２は、前処理部１２１により作成された入力データ（教師データ、検証用データ及びテスト用データ）と、グラフ情報生成部１０４により生成されたグラフ情報とを用いて、グラフ畳み込みニューラルネットワークによって対象脅威情報の悪性度を計算（推定）する。

[0035] 教師あり学習計算部１２３は、前処理部１２１により作成された入力データ（教師データ、検証用データ及びテスト用データ）を用いて、教師あり学習の手法によって対象脅威情報の悪性度を計算（推定）する。

[0036] 出力部１０６は、対象脅威情報と、悪性度計算部１０５により計算（推定）された悪性度とを出力する。なお、出力部１０６は、予め決められた任意の出力先に対象脅威情報と悪性度とを出力すればよい。例えば、出力部１０６は、ディスプレイ等を出力先としてもよいし、メモリ等の記憶装置を出力先としてもよいし、ネットワークを介して接続される他の装置（例えば、脅威情報管理装置２１等）を出力先としてもよい。

[0037] ＜悪性度推定装置１０のハードウェア構成＞

次に、本発明の実施の形態における悪性度推定装置１０のハードウェア構成について、図２を参照しながら説明する。図２は、本発明の実施の形態における悪性度推定装置１０のハードウェア構成の一例を示す図である。

[0038] 図２に示すように、本発明の実施の形態における悪性度推定装置１０は、ハードウェアとして、入力装置２０１と、表示装置２０２と、外部Ｉ／Ｆ２０３と、ＲＡＭ（Random Access Memory）２０４と、ＲＯＭ（Read Only Memory）２０５と、プロセッサ２０６と、通信Ｉ／Ｆ２０７と、補助記憶装置２０８とを有する。これら各ハードウェアは、それぞれがバスＢを介して通信可能に接続されている。

[0039] 入力装置２０１は、例えばキーボードやマウス、タッチパネル等であり、ユーザが各種操作を入力するのに用いられる。表示装置２０２は、例えばデ

ィスプレイ等であり、悪性度推定装置１０の処理結果（例えば、推定された悪性度等）を表示する。なお、悪性度推定装置１０は、入力装置２０１及び表示装置２０２の少なくとも一方を有していなくてもよい。

[0040] 外部Ｉ／Ｆ２０３は、記録媒体２０３ａ等の外部記録媒体とのインタフェースである。悪性度推定装置１０は、外部Ｉ／Ｆ２０３を介して、記録媒体２０３ａの読み取りや書き込み等を行うことができる。記録媒体２０３ａには、悪性度推定装置１０が有する各機能部（例えば、入力部１０１、情報収集部１０２、特徴量生成部１０３、グラフ情報生成部１０４、悪性度計算部１０５及び出力部１０６等）を実現する１以上のプログラム等が記録されていてもよい。

[0041] 記録媒体２０３ａには、例えば、フレキシブルディスク、ＣＤ（Compact Disc）、ＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等がある。

[0042] ＲＡＭ２０４は、プログラムやデータを一時保持する揮発性の半導体メモリである。ＲＯＭ２０５は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリである。ＲＯＭ２０５には、例えば、ＯＳ（Operating System）に関する設定情報や通信ネットワークに関する設定情報等が格納されている。

[0043] プロセッサ２０６は、例えばＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics Processing Unit）等であり、ＲＯＭ２０５や補助記憶装置２０８等からプログラムやデータをＲＡＭ２０４上に読み出して処理を実行する演算装置である。悪性度推定装置１０が有する各機能部は、ＲＯＭ２０５や補助記憶装置２０８等に格納されている１以上のプログラムをＲＡＭ２０４上に読み出してプロセッサ２０６が処理を実行することで実現される。

[0044] 通信Ｉ／Ｆ２０７は、悪性度推定装置１０を通信ネットワークに接続するためのインタフェースである。悪性度推定装置１０が有する各機能部を実現する１以上のプログラムは、通信Ｉ／Ｆ２０７を介して、所定のサーバ等か

ら取得（ダウンロード）されてもよい。

[0045] 補助記憶装置２０８は、例えばＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）等であり、プログラムやデータを格納している不揮発性の記憶装置である。補助記憶装置２０８に格納されているプログラムやデータには、例えば、ＯＳ，当該ＯＳ上で各種機能を実現するアプリケーションプログラム、悪性度推定装置１０が有する各機能部を実現する１以上のプログラム等がある。

[0046] 本発明の実施の形態における悪性度推定装置１０は、図２に示すハードウェア構成を有することにより、後述する各種処理を実現することができる。なお、図２に示す例では、本発明の実施の形態における悪性度推定装置１０が１台の装置（コンピュータ）で実現されている場合を示したが、これに限られない。本発明の実施の形態における悪性度推定装置１０は、複数台の装置（コンピュータ）で実現されていてもよい。また、１台の装置（コンピュータ）には、複数のプロセッサ２０６や複数のメモリ（ＲＡＭ２０４やＲＯＭ２０５、補助記憶装置２０８等）が含まれていてもよい。

[0047] ＜悪性度推定処理＞

次に、対象脅威情報の悪性度を推定する処理（悪性度推定処理）について、図３を参照しながら説明する。図３は、本発明の実施の形態における悪性度推定処理の一例を示すフローチャートである。

[0048] ステップＳ１０１：まず、入力部１０１は、対象脅威情報を入力する。

[0049] ステップＳ１０２：次に、情報収集部１０２は、関連情報と他の脅威情報とを収集する。すなわち、情報収集部１０２は、ＮＷ情報収集部１１１によってネットワークで観測可能な関連情報をフロー観測情報管理装置２２や攻撃検知装置２３、ＤＮＳサーバ２５、ＷＨＯＩＳ／ＲＤＡＰサーバ２６等から収集すると共に、ＯＳＩＮＴ収集部１１２によってオープンソースインテリジェンスの公開情報を関連情報としてＯＳＩＮＴサーバ２７から収集する。また、情報収集部１０２は、脅威情報収集部１１３によって他の脅威情報を脅威情報管理装置２１から収集する。

[0050] なお、上記のステップＳ１０２で収集された関連情報及び他の脅威情報は、例えば、悪性度推定装置１０の補助記憶装置２０８等に格納される。

[0051] ステップＳ１０３：次に、特徴量生成部１０３は、対象脅威情報に含まれるドメイン名やＵＲＬ等と、ＮＷ情報収集部１１１やＯＳＩＮＴ収集部１１２により収集された関連情報とを用いて、対象脅威情報の特徴量を生成する。ここで、特徴量は、例えば、脅威情報の様々な特徴を数値化した値を各要素するベクトルで表される。

[0052] 脅威情報の特徴としては、一例として、以下に示すものが挙げられる。

[0053] ・脅威情報に含まれるドメイン名やＵＲＬの文字列の長さ

・脅威情報に含まれるドメイン名やＵＲＬ中の数字の割合

・脅威情報に含まれるドメイン名やＵＲＬ中の子音の割合

・脅威情報に含まれるドメイン名やＵＲＬに所定の特徴的な文字列（例えば、文字列「exe」等）が含まれるか否か

・名前解決結果情報に含まれるＡレコード数やＮＳレコード数

・脅威情報に含まれるＩＰアドレスの国別情報

これらの各特徴を数値化するにあたっては、関連情報が用いられる場合もある。例えば、脅威情報に含まれるＩＰアドレスの国別情報を数値化する際には、ＧｅｏＩＰの検索結果を示す情報等が用いられる。

[0054] これにより、例えば、対象脅威情報の各特徴を数値化した値をx_1，x_2，・・・，x_Nとすれば、これらx_1，x_2，・・・，x_Nを各要素とするベクトル［x_1，x_2，・・・，x_N］が対象脅威情報の特徴量として生成される。ここで、Ｎは、予め決められた値であり、脅威情報の特徴数を表す。なお、例えば、ドメイン名やＵＲＬに所定の特徴的な文字列が含まれるか否かを数値化する場合等には、Ｏｎｅ－ｈｏｔ　Ｅｎｃｏｄｅｒ等が用いられればよい。

[0055] なお、上記の脅威情報の特徴は一例であって、上記に挙げた特徴以外にも種々の特徴が用いられてもよい。

[0056] ステップＳ１０４：次に、グラフ情報生成部１０４は、対象脅威情報と、

上記のステップＳ１０２で収集された関連情報及び他の脅威情報とを用いて、各脅威情報（対象脅威情報及び他の脅威情報）の関連を表すグラフ構造からグラフ情報を生成する。ここで、グラフ情報生成部１０４は、各脅威情報（対象脅威情報及び他の脅威情報）をノード、脅威情報（ノード）間の関連をエッジとして、グラフ情報を生成する。なお、他の脅威情報の関連情報は、例えば、上記のステップＳ１０２で脅威情報管理装置２１から収集されてもよいし、本ステップで脅威情報管理装置２１に蓄積・管理されている関連情報を参照又は収集されてもよい。

[0057] 関連がある脅威情報としては、一例として、以下に示すものが挙げられる。

[0058] ・同一ドメイン名の正引き結果として得られるＩＰアドレスが含まれる脅威情報同士

例えば、或るドメイン名の正引き結果としてＩＰアドレスＡとＩＰアドレスＢとが得られる場合、ＩＰアドレスＡが含まれる脅威情報Ａと、ＩＰアドレスＢが含まれる脅威情報Ｂとは関連がある脅威情報となる。

[0059] ・同一ＩＰアドレスを共有しているドメイン名が含まれる脅威情報同士

例えば、ドメイン名Ｃとドメイン名Ｄとが同一のＩＰアドレスを共有している場合、ドメイン名Ｃが含まれる脅威情報Ｃと、ドメイン名Ｄが含まれる脅威情報Ｄとは関連がある脅威情報となる。

[0060] ・ＷＨＯＩＳ又はＲＤＡＰの問い合わせ結果として得られる企業名やレジスタ名が同じであるドメイン名が含まれる脅威情報同士

例えば、ドメイン名Ｅ及びドメイン名ＦのＷＨＯＩＳ又はＲＤＡＰの問い合わせ結果が同一企業名である場合、ドメイン名Ｅが含まれる脅威情報Ｅと、ドメイン名Ｆが含まれる脅威情報Ｆとは関連がある脅威情報となる。

[0061] これにより、各脅威情報をノードとし、関連がある脅威情報のノード間にエッジを有するグラフ構造を得ることができ、グラフ情報生成部１０４は、このグラフ構造を示すグラフ情報を生成することができる。グラフ情報としては、例えば、隣接行列（adjacency matrix）やグラフラプラシアン等が挙

げられる。

[0062] ステップＳ１０５：次に、悪性度計算部１０５は、上記のステップＳ１０４で作成されたグラフ情報を用いて、対象脅威情報が他の脅威情報との間でグラフ構造を有するか否かを判定する。すなわち、悪性度計算部１０５は、対象脅威情報を示すノードが、他のノード（つまり、他の脅威情報を示すノード）とエッジで接続されているか否かを判定する。

[0063] ステップＳ１０５で対象脅威情報が他の脅威情報との間でグラフ構造を有すると判定された場合、悪性度計算部１０５は、ステップＳ１０６に進む。一方で、対象脅威情報が他の脅威情報との間でグラフ構造を有しないと判定された場合（つまり、対象脅威情報を示すノードがグラフ上で単独である場合）、悪性度計算部１０５は、ステップＳ１０８に進む。

[0064] ステップＳ１０６：上記のステップＳ１０５で対象脅威情報が他の脅威情報との間でグラフ構造を有すると判定された場合、悪性度計算部１０５は、前処理部１２１により、各脅威情報の特徴量データを、教師用集合と、検証用集合と、テスト用集合とに分割する。ここで、前処理部１２１は、例えば、教師用集合に含まれる特徴量データ数と、検証用集合に含まれる特徴量データ数と、テスト用集合に含まれる特徴量データ数とが、それぞれ予め設定された割合（全特徴量データ数に対する割合）となるように、ランダムに分割すればよい。なお、上述したように、テスト用集合には、対象脅威情報の特徴量データ（すなわち、上記のステップＳ１０４で生成された特徴量を示すデータ）が含まれる。

[0065] そして、前処理部１２１は、教師用集合から複数の教師データを作成すると共に、検証用集合から複数の検証用データを作成する。また、前処理部１２１は、テスト用集合からテスト用データを作成する。なお、或る１つの教師データに付与されるラベルの悪性度は、例えば、この教師データを構成する特徴量データの悪性度の平均等とすればよい。検証用データについても同様である。

[0066] ステップＳ１０７：次に、悪性度計算部１０５は、グラフ畳み込み計算部

１２２により、上記のステップＳ１０６で作成された入力データ（教師データ、検証用データ及びテスト用データ）と、上記のステップＳ１０４で生成されたグラフ情報とを用いて、グラフ畳み込みニューラルネットワークによって対象脅威情報の悪性度を計算（推定）する。グラフ畳み込みニューラルネットワークでは、ｔをグラフ畳みニューラルネットワークの層を示すインデックス、ｔ＝０を入力層、ｔ＝Ｔ－１を出力層として、ｔ＝０，・・・，Ｔ－１に対して、以下の式（１）により悪性度を推定する。

[0067] $H^{(t+1)}=\sigma(AH^{(t)}W^{(t)})$ ・・・（１）

ここで、Ａはグラフ情報、$W^{(t)}$はｔ層目のパラメータ（重み）、σは活性化関数である。また、$X=H^{(0)}$は入力データであり、所定の個数の特徴量データで構成される行列（例えば、所定の個数をＭ、特徴量データがＮ次の横ベクトルとすれば、Ｍ×Ｎ行列）である。なお、活性化関数σとしては、例えば、出力層以外ではＲｅＬＵ等を用いて、出力層では悪性度を出力するｓｏｆｔｍａｘ関数（つまり、悪性度をｐとして、ｐと１－ｐとを出力するｓｏｆｔｍａｘ関数）を用いる。

[0068] このとき、グラフ畳み込み計算部１２２は、以下の（１－１）～（１－３）により悪性度を推定する。

[0069] （１－１）まず、グラフ畳み込み計算部１２２は、複数の教師データのそれぞれを入力データとして、グラフ畳み込みニューラルネットワークの各パラメータ（重み）$W^{(t)}$を更新する。すなわち、悪性度計算部１０５は、教師データに付与されたラベルと、当該教師データを入力データとした場合のグラフ畳み込みニューラルネットワークの出力結果とを用いて、所定の誤差関数（誤差関数は「目的関数」や「損失関数」等と称されてもよい。）が最小となるように、既知の最適化手法により各パラメータ$W^{(t)}$を更新する。

[0070] （１－２）次に、グラフ畳み込み計算部１２２は、複数の検証用データのそれぞれを入力データとして、グラフ畳み込みニューラルネットワークの推定精度を検証する。すなわち、悪性度計算部１０５は、検証用データに付与されたラベルと、当該検証用データを入力データとした場合のグラフ畳み込

みニューラルネットワークの出力結果とを用いて、既知の検証手法によりグラフ畳み込みニューラルネットワークの推定精度を検証する。なお、例えば、この検証結果、グラフ畳み込みニューラルネットワークの推定精度が十分でない場合には、学習用集合及び検証用集合の割合を変更して、上記のステップＳ１０６から再度実行することが考えられる。

[0071] （１－３）最後に、グラフ畳み込み計算部１２２は、テスト用データを入力データとして、グラフ畳み込みニューラルネットワークの出力結果を得る。この出力結果が、対象脅威情報の悪性度の推定結果である。

[0072] なお、上記の（１－２）は必ずしも行われなくてもよい。この場合は、上記のステップＳ１０６で検証用データが作成されなくてもよい。

[0073] ステップＳ１０８：上記のステップＳ１０５で対象脅威情報が他の脅威情報との間でグラフ構造を有しないと判定された場合、悪性度計算部１０５は、上記のステップＳ１０６と同様に、前処理部１２１により、各脅威情報の特徴量データを、教師用集合と、検証用集合と、テスト用集合とに分割し、複数の教師データと、複数の検証用データと、テスト用データとを作成する。

[0074] ただし、例えば、教師用集合に含まれる特徴量データ数と、検証用集合に含まれる特徴量データ数と、テスト用集合に含まれる特徴量データ数との割合が、上記のステップＳ１０５と異なっていてもよい（すなわち、上記のステップＳ１０５と本ステップとで、異なる値が割合として設定されていてもよい）。例えば、教師あり学習の手法で用いるモデルによっては各脅威情報の特徴量データそのものが入力データとなる。このような場合、テスト用集合に含まれる特徴量データ数が「１」となるように割合が設定される。

[0075] ステップＳ１０９：次に、悪性度計算部１０５は、教師あり学習計算部１２３により、上記のステップＳ１０８で作成された入力データ（教師データ、検証用データ及びテスト用データ）を用いて、教師あり学習の手法によって対象脅威情報の悪性度を計算（推定）する。

[0076] ここで、教師あり学習の手法に用いるモデル（学習モデル）としては任意

の学習モデルを用いることができる。例えば、学習モデルとしては、サポートベクターマシンや決定木、アンサンブル学習（バギング、ブースティング）に適用される学習モデル等が挙げられる。

[0077] このとき、教師あり学習計算部１２３は、以下の（２－１）～（２－３）により悪性度を推定する。

[0078] （２－１）まず、教師あり学習計算部１２３は、複数の教師データのそれぞれを入力データとして、教師あり学習の手法により学習モデルを学習する。

[0079] （２－２）次に、教師あり学習計算部１２３は、複数の検証用データのそれぞれを入力データとして、既知の検証手法により学習モデルの推定精度を検証する。なお、例えば、この検証結果、学習モデルの推定精度が十分でない場合には、学習用集合及び検証用集合の割合を変更して、上記のステップＳ１０８から再度実行することが考えられる。

[0080] （２－３）最後に、教師あり学習計算部１２３は、テスト用データを入力データとして、学習モデルの出力結果を得る。この出力結果が、対象脅威情報の悪性度の推定結果である。

[0081] なお、上記の（２－２）は必ずしも行われなくてもよい。この場合は、上記のステップＳ１０８で検証用データが作成されなくてもよい。

[0082] ステップＳ１１０：ステップＳ１０７又はステップＳ１０９に続いて、出力部１０６は、対象脅威情報と、上記のステップＳ１０７又は上記のステップＳ１０９で推定された悪性度とを出力する。なお、例えば、上記のステップＳ１０７又は上記のステップＳ１０９で推定された悪性度が所定の閾値を超えている場合にのみ、出力部１０６は、本ステップを実行するようにしてよい。

[0083] また、例えば、上記のステップＳ１０７又は上記のステップＳ１０９で推定された悪性度が、予め設定された所定の閾値を超えている場合には、出力部１０６は、セキュリティ運用者の端末等に所定の通知を送信してもよい。

[0084] 更に、出力部１０６は、対象脅威情報及び悪性度に加えて、例えば、対象

脅威情報を示すノードを含むグラフや対象脅威情報の特徴量等を出力してもよい。このとき、出力部１０６は、脅威情報を所定の形式（例えば、ＳＴＩＸ（Structured Threat Information Expression）形式等の標準記述形式）で出力してもよい。

[0085] ＜まとめ＞

以上のように、本発明の実施の形態における悪性度推定装置１０は、様々な関連情報や脅威情報を収集した上で、対象脅威情報が他の脅威情報との間でグラフ構造を有するか否かを判定し、この判定結果に応じて、グラフ畳み込みニューラルネットワーク又は教師あり学習で学習した所定のモデルと、各脅威情報の特徴量とを用いて、対象脅威情報の悪性度を推定する。これにより、対象脅威情報が他の脅威情報との間でグラフ構造を有する場合には、対象脅威情報の特徴と、グラフ構造とを利用して、極めて高い精度で悪性度を推定することが可能となる。一方で、対象脅威情報が他の脅威情報との間でグラフ構造を有しない場合であっても、対象脅威情報の特徴を利用して、高い精度で悪性度を推定することが可能となる。

[0086] このため、本発明の実施の形態における悪性度推定装置１０を用いることで、より早期に、かつ、より高い精度で様々なサイバー攻撃を検知及び対処可能となる。また、多数の脅威情報の分析・選別に要する運用者の負担軽減や誤検知の削減による効率的なセキュリティオペレーションも可能となる。

[0087] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

符号の説明

[0088]

１	悪性度推定システム
１０	悪性度推定装置
２０	外部装置
２１	脅威情報管理装置
２２	フロー観測情報管理装置
２３	攻撃検知装置

２４　　ＯＳＩＮＴサーバ

２５　　ＤＮＳサーバ

２６　　ＷＨＯＩＳ／ＲＤＡＰサーバ

１０１　入力部

１０２　情報収集部

１０３　特徴量生成部

１０４　グラフ情報生成部

１０５　悪性度計算部

１０６　出力部

１１１　ＮＷ情報収集部

１１２　ＯＳＩＮＴ収集部

１１３　脅威情報収集部

１２１　前処理部

１２２　グラフ畳み込み計算部

１２３　教師あり学習計算部

請求の範囲

[請求項1] 悪性度の推定対象の脅威情報が入力されると、前記脅威情報に関連する関連情報と、前記脅威情報とは異なる他の脅威情報とを収集する収集手段と、

前記関連情報に基づいて、前記脅威情報の特徴を表す特徴量を生成する特徴量生成手段と、

前記関連情報と前記他の脅威情報とに基づいて、前記脅威情報及び前記他の脅威情報のそれぞれをノード、該ノード間の関連をエッジとするグラフを示すグラフ情報を生成するグラフ情報生成手段と、

前記グラフ情報により示されるグラフ上で前記脅威情報と前記他の脅威情報の間にグラフ構造が存在する場合、前記脅威情報の特徴量を用いて、グラフ畳み込みニューラルネットワークにより、前記脅威情報の悪性度を推定する推定手段と、

を有することを特徴とする推定装置。

[請求項2] 前記収集手段は、

フローエクスポータ又は／及びフローコレクタから収集可能なフロー観測情報と、オープンソースインテリジェンスを提供するサーバ又はＷｅｂサイトから収集可能な公開情報と、ＤＮＳサーバから収集可能な名前解決情報と、ＷＨＯＩＳサーバ又はＲＤＡＰサーバから収集可能な所有者情報とのうちの少なくとも１つ以上の情報を前記関連情報として収集し、

前記特徴量生成手段は、

収集された前記１つ以上の情報に基づいて、前記特徴量を生成する、ことを特徴とする請求項１に記載の推定装置。

[請求項3] 前記推定手段は、

前記グラフ情報により示されるグラフ上で前記脅威情報と前記他の脅威情報の間にグラフ構造が存在しない場合、前記脅威情報の特徴量を用いて、教師あり学習の手法で学習された所定の学習モデルにより

、前記脅威情報の悪性度を推定する、ことを特徴とする請求項１又は２に記載の推定装置。

[請求項4] 前記特徴量には、

前記脅威情報に含まれるドメイン名の文字列の長さと、前記脅威情報に含まれるＵＲＬの文字列の長さと、前記脅威情報に含まれるドメイン名中の数字の割合と、前記脅威情報に含まれるＵＲＬ中の数字の割合と、前記脅威情報に含まれるドメイン名中の子音の割合と、前記脅威情報に含まれるＵＲＬ中の子音の割合と、前記脅威情報に含まれるドメイン名に所定の文字列が含まれるか否かを示す情報と、前記脅威情報に含まれるＵＲＬに所定の文字列が含まれるか否かを示す情報と、前記脅威情報に含まれるＩＰアドレスの国別情報と、前記脅威情報に含まれるＩＰアドレス又はドメイン名を名前解決した場合におけるＡレコード数及びＮＳレコード数と、のうちの少なくとも１つ以上が含まれる、ことを特徴とする請求項１乃至３の何れか一項に記載の推定装置。

[請求項5] 悪性度の推定対象の脅威情報が入力されると、前記脅威情報に関連する関連情報と、前記脅威情報とは異なる他の脅威情報とを収集する収集手順と、

前記関連情報に基づいて、前記脅威情報の特徴を表す特徴量を生成する特徴量生成手順と、

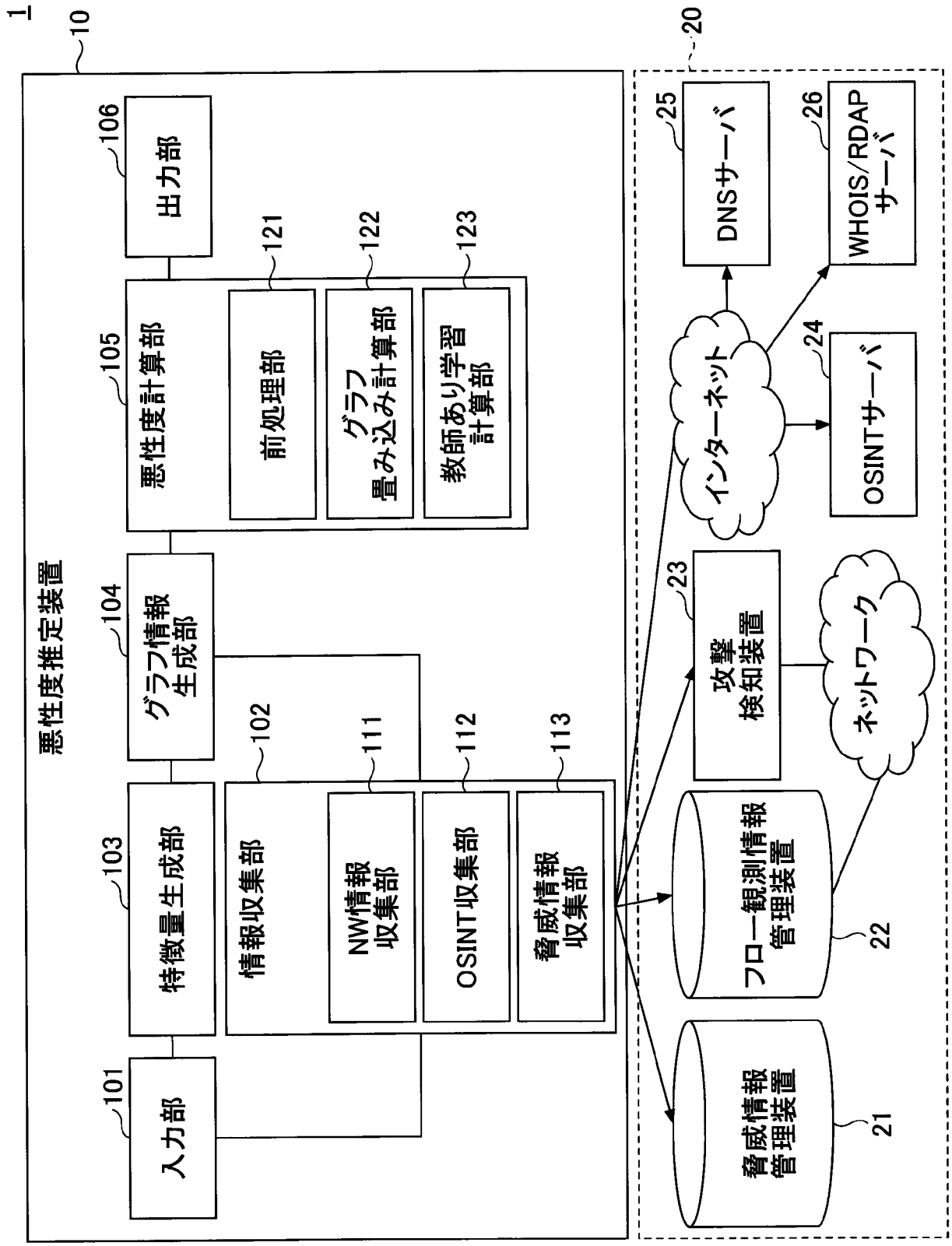
前記関連情報と前記他の脅威情報とに基づいて、前記脅威情報及び前記他の脅威情報のそれぞれをノード、該ノード間の関連をエッジとするグラフを示すグラフ情報を生成するグラフ情報生成手順と、

前記グラフ情報により示されるグラフ上で前記脅威情報と前記他の脅威情報の間にグラフ構造が存在する場合、前記脅威情報の特徴量を用いて、グラフ畳み込みニューラルネットワークにより、前記脅威情報の悪性度を推定する推定手順と、

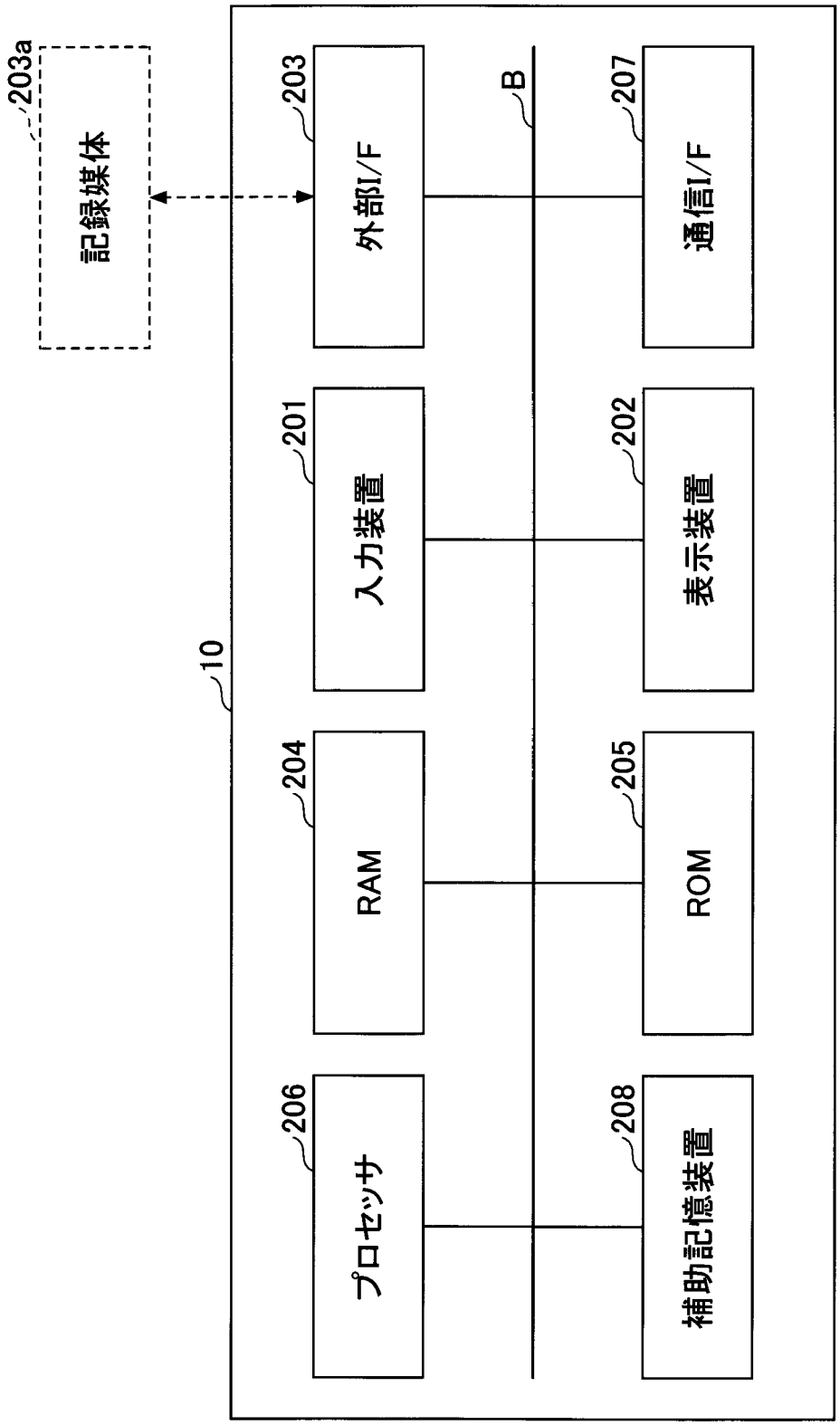
をコンピュータが実行することを特徴とする推定方法。

[請求項6] コンピュータを、請求項１乃至４の何れか一項に記載の推定装置における各手段として機能させるためのプログラム。

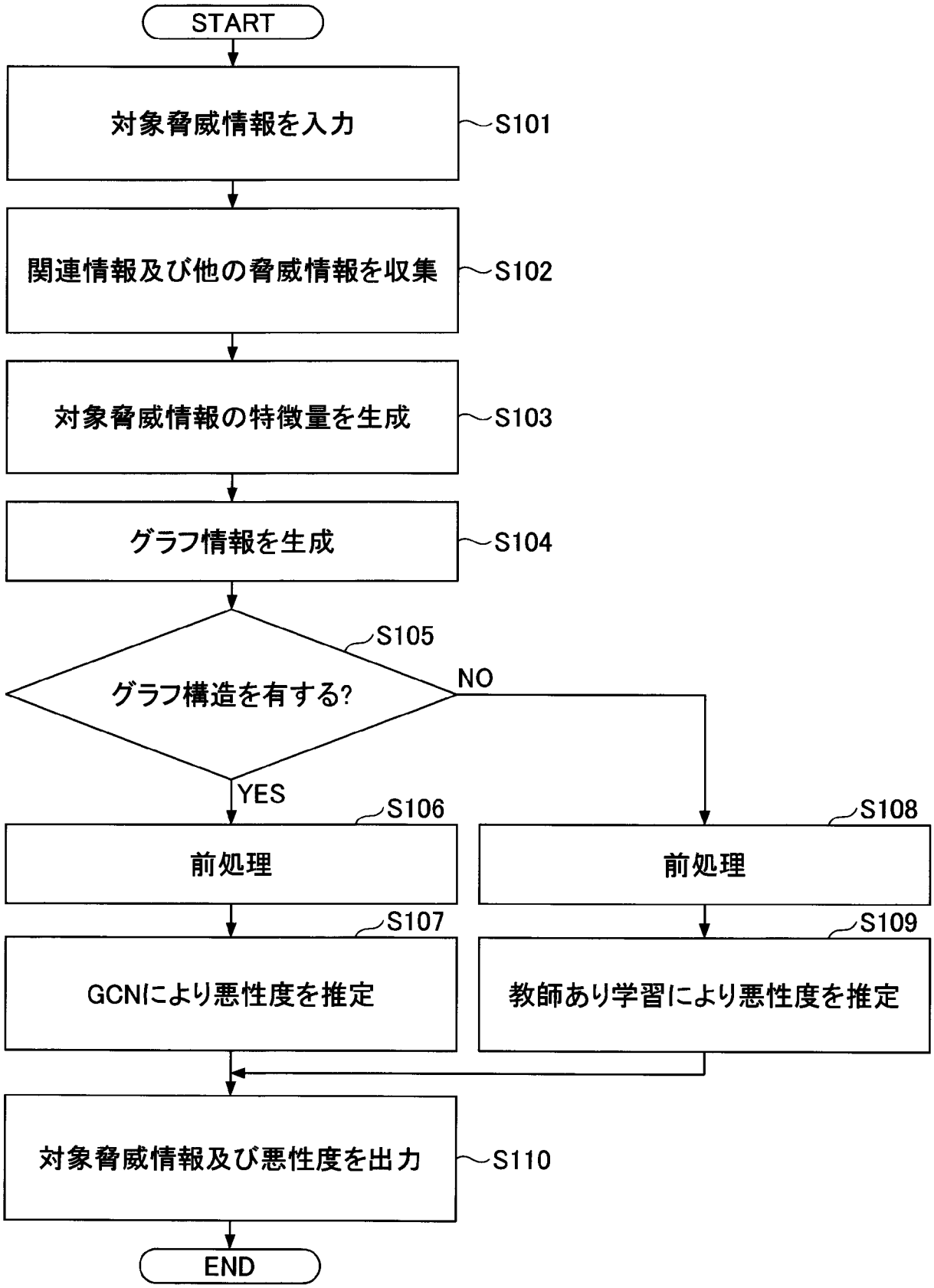
[図1]


1
10
悪性度推定装置
101
入力部
103
特徴量生成部
104
グラフ情報生成部
105
悪性度計算部
106
出力部
102
情報収集部
111
NW情報収集部
112
OSINT収集部
113
脅威情報収集部
121
前処理部
122
グラフ畳み込み計算部
123
教師あり学習計算部
20
21
脅威情報管理装置
22
フロー観測情報管理装置
23
攻撃検知装置
24
OSINTサーバ
25
DNSサーバ
26
WHOIS/RDAPサーバ
インターネット
ネットワーク

[図2]


203a
記録媒体
10
203
外部I/F
B
207
通信I/F
201
入力装置
202
表示装置
204
RAM
205
ROM
206
プロセッサ
208
補助記憶装置

[図3]


START
対象脅威情報を入力
S101
関連情報及び他の脅威情報を収集
S102
対象脅威情報の特徴量を生成
S103
グラフ情報を生成
S104
S105
グラフ構造を有する?
NO
YES
S106
前処理
S108
前処理
S107
GCNにより悪性度を推定
S109
教師あり学習により悪性度を推定
対象脅威情報及び悪性度を出力
S110
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/005377

A. CLASSIFICATION OF SUBJECT MATTER
G06F 21/55(2013.01)i; G06F 16/28(2019.01)i
FI: G06F21/55; G06F16/28

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)
G06F21/55; G06F16/28

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
A	風戸 雄太ほか, 確率伝播法を用いた脅威情報の信頼度算出方式の一検討, 電子情報通信学会 2018 年通信ソサイエティ大会講演論文集 2, 28 August 2018, p. 89, in particular, page 89, left column, lines 9-12, non-official translation (KAZATO, Yuta et al., "A study on the reliability calculation method of threat information using belief propagation", Lecture proceedings 2 of the 2018 communication society conference of IEICE)	1-6

☐ 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
"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	Date of mailing of the international search report
31 March 2020 (31.03.2020)	14 April 2020 (14.04.2020)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

国際調査報告

国際出願番号
PCT/JP2020/005377

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/55(2013.01)i; G06F 16/28(2019.01)i
FI: G06F21/55; G06F16/28

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））

G06F21/55; G06F16/28

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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
A	風戸 雄太ほか，確率伝播法を用いた脅威情報の信頼度算出方式の一検討，電子情報通信学会２０１８年通信ソサイエティ大会講演論文集２，2018.08.28，p.89 特に第89ページ左欄第9-12行目	1-6

☐ 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、一般的技術水準を示すもの
“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	国際調査報告の発送日
31.03.2020	14.04.2020

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）
平井　誠 5S 9071
電話番号 03-3581-1101 内線 3546