

(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
2017年4月13日(13.04.2017)



(10) 国際公開番号
WO 2017/061469 A1

- (51) 国際特許分類:
H04L 12/70 (2013.01) G06F 21/56 (2013.01)
- (21) 国際出願番号: PCT/JP2016/079620
- (22) 国際出願日: 2016年10月5日(05.10.2016)
- (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 2015-198753 2015年10月6日(06.10.2015) 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: 寺本 泰大(TERAMOTO, Yasuhiro); 〒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). 胡 博(HU, Bo); 〒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). 岸 寿春(KISHI, Toshiharu); 〒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). 永渕 幸雄(NAGAFUCHI, Yukio); 〒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). 小山 高明(KOYAMA, Takaaki); 〒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). 北爪 秀雄(KITAZUME, Hideo); 〒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: 特許業務法人酒井国際特許事務所(SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号虎の門三井ビルディング 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, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[続葉有]

(54) Title: IDENTIFICATION SYSTEM, IDENTIFICATION DEVICE AND IDENTIFICATION METHOD

(54) 発明の名称: 特定システム、特定装置および特定方法

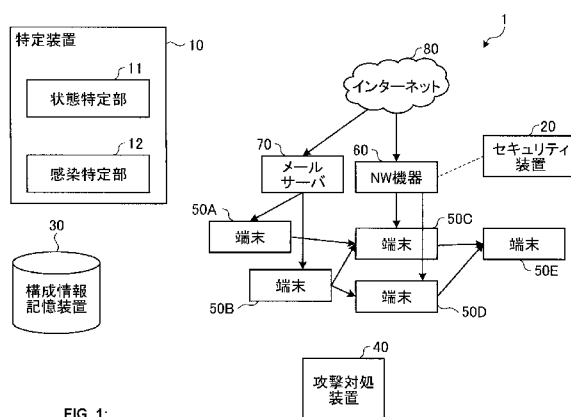


FIG. 1:
10 Identification device
11 State identification unit
12 Infection identification unit
20 Security device
30 Configuration information storage device
40 Attack coping device
50A-50E Terminal
60 NW equipment
70 Mail server
80 Internet

(57) Abstract: An identification device (10) receives detection information from a security device (20) which detects activity relating to an illegal intrusion into a network or an infection of a terminal (50), and identifies the state of the terminal (50) from the activity of the terminal (50) and terminal (50) information included in the detection information. If the state of a terminal (50) is identified by a state identification unit (11) as being a malware-infected state, the identification device (10) identifies, on the basis of connection information stored by a configuration information storage device (30), a terminal (50) suspected of having been infected up to the terminal (50) activity included in the detection information, and identifies, as an infected terminal candidate which might be infected, a terminal (50) positioned on a path the infected terminal might use in a future illegal intrusion or terminal infection.

(57) 要約: 特定装置(10)は、ネットワーク内への不正侵入または端末(50)の感染に関する活動を検知するセキュリティ装置20から検知情報を受信し、該検知情報に含まれる端末(50)の情報および該端末(50)の活動内容から当該端末(50)の状態を特定する。そして、特定装置(10)は、状態特定部(11)によって端末(50)の状態がマルウェアに感染した状態であると特定された場合には、

構成情報記憶装置(30)によって記憶された接続情報に基づいて、検知情報に含まれる端末(50)の活動内容に至るまでに感染した疑いがある端末(50)を特定し、感染した端末(50)が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末(50)を感染する可能性がある感染端末の候補と特定する。



MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, 添付公開書類:
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, — 国際調査報告 (条約第 21 条(3))
KM, ML, MR, NE, SN, TD, TG).

明 細 書

発明の名称： 特定システム、特定装置および特定方法

技術分野

[0001] 本発明は、特定システム、特定装置および特定方法に関する。

背景技術

[0002] 従来、マルウェアと呼ばれる、コンピュータウィルス、スパイウェア、ボット等の不正かつ有害な動作を行う意図で作成された悪意のソフトウェアやプログラムコード等の不正なソフトウェアの存在が知られている。

[0003] 例えば、このようなマルウェアによる標的型攻撃やAPT (Advanced Persistent Threat) 攻撃の伝播経路候補を算出するための技術として、Attack Graphが存在する。Attack Graphは、ネットワークシステム構成、端末のOS・アプリケーション情報を収集し、外部攻撃者の侵入経路候補を静的に算出する事で、ネットワークの脅威を評価する技術である。

先行技術文献

非特許文献

[0004] 非特許文献1: Subil Abraham, Suku Nair, “A Predictive Framework for Cyber Security Analytics using Attack Graphs”, IJCNC 2015.

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、従来の技術では、感染の疑いがある端末や今後感染する可能性がある感染端末の候補を適切に特定することができないという課題があった。例えば、標的型攻撃やAPT攻撃では、不正侵入されたもしくはマルウェアに感染した端末を介して、同一ネットワークシステム内の複数の端末への侵入または感染を拡大するという特徴があり、セキュリティ装置の検知した感染端末に対して、遮断等の対処を行っても、検知されていない他の感染端末が存在した場合、当該端末を介し、攻撃が継続される。このような場

合に、従来の技術では、検知した端末への経路上にある感染の疑いがある端末や今後感染する可能性がある感染端末の候補を適切に特定することができなかった。

課題を解決するための手段

[0006] 上述した課題を解決し、目的を達成するために、本発明の特定システムは、ネットワーク内の端末に関する情報を記憶する構成情報記憶装置と、前記端末の状態を特定する特定装置とを有する特定システムであって、前記構成情報記憶装置は、前記ネットワーク内における端末同士の接続関係を示す接続情報を記憶し、前記特定装置は、前記ネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定部と、前記状態特定部によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、前記構成情報記憶装置によって記憶された接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定部とを有することを特徴とする。

[0007] また、本発明の特定装置は、複数の端末を含むネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知に関する検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定部と、前記状態特定部によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、ネットワーク内の端末同士の接続関係を示す接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定部とを有することを特徴とする。

[0008] また、本発明の特定方法は、特定装置によって実行される特定方法であって、複数の端末を含むネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知に関する検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定工程と、前記状態特定工程によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、ネットワーク内の端末同士の接続関係を示す接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定工程とを含んだことを特徴とする。

発明の効果

[0009] 本発明によれば、感染の疑いがある端末や今後感染する可能性がある感染端末の候補を適切に特定することが可能であるという効果を奏する。

図面の簡単な説明

[0010] [図1]図1は、第一の実施の形態に係る特定システムの構成の一例を示す図である。

[図2]図2は、第一の実施の形態に係る構成情報記憶装置が記憶する端末の接続情報の一例を示す図である。

[図3]図3は、第一の実施の形態に係る構成情報記憶装置が記憶する端末の状態情報の一例を示す図である。

[図4]図4は、第一の実施の形態に係る特定装置において端末の状態を特定する処理を説明する図である。

[図5]図5は、第一の実施の形態に係る特定装置において感染の疑いがある端末および感染端末の候補を特定する処理を説明する図である。

[図6]図6は、第一の実施の形態に係る攻撃対処装置において感染が確定した端末に対する対処を説明する図である。

[図7]図7は、第一の実施の形態に係る特定装置において感染の疑いがある端

末および感染端末の候補を特定する処理を説明する図である。

[図8]図8は、第一の実施の形態に係る攻撃対処装置において感染の可能性が高い端末に対する対処を説明する図である。

[図9]図9は、第一の実施の形態に係る特定装置の処理の流れを示すフローチャートである。

[図10]図10は、第一の実施の形態に係る特定システムの処理の流れを示すシーケンス図である。

[図11]図11は、特定プログラムを実行するコンピュータを示す図である。

発明を実施するための形態

[0011] 以下に、本願に係る特定システム、特定装置および特定方法の実施形態を図面に基づいて詳細に説明する。なお、この実施形態により本願に係る特定システム、特定装置および特定方法が限定されるものではない。

[0012] [第一の実施の形態]

以下の実施の形態では、第一の実施の形態に係る特定システムの構成、特定装置および特定システムの処理の流れを順に説明し、最後に第一の実施の形態による効果を説明する。

[0013] [特定システムの構成]

図1は、第一の実施の形態に係る特定システムの構成の一例を示す図である。第一の実施の形態に係る特定システム1は、感染の疑いがある端末や今後感染する可能性のある端末の候補を特定する特定装置10、通信を監視するセキュリティ装置20、ネットワーク内の端末50A～50Eに関する情報を記憶する構成情報記憶装置30、通信の監視や通信の制限を行う攻撃対処装置40、複数の端末50A～50E、ファイアーウォール、ルーター、スイッチ等のNW（Network）機器60、ネットワークサービスを提供するメールサーバ70を有する。

[0014] また、NW機器60およびメールサーバ70は、インターネット80と接続されている。また、複数の端末50A～50Eを含むネットワークは、ファイアーウォールのACL（Access Control List）等を用いて業務遂行に

必要な通信のみを許可しているものとする。図1では、ファイヤーウォールにより許可されている通信および、サービスの接続性（メール、HTTP Proxy、認証システム等）の論理的通信を機器接続の矢印として示す。なお、図1に示す各装置や機能の数は、あくまで一例であり、これに限られるものではない。また、複数の端末50A～50Eについて、特に区別なく説明する場合には、適宜端末50と記載する。

[0015] セキュリティ装置20は、ネットワーク内における各端末50A～50EやNW機器60の通信を監視し、不正通信等を検知した場合には、検知情報を特定装置10に送信する。検知情報には、不正通信を行った端末50の情報や端末50の活動内容等が含まれている。

[0016] 構成情報記憶装置30は、ネットワーク内における端末同士の接続関係を示す接続情報を記憶する。例えば、構成情報記憶装置30は、図2に例示するように、端末の名称を示す「端末名」と、端末のIPアドレスを示す「IPアドレス」と端末のMACアドレスを示す「MACアドレス」と端末同士の接続関係を示す「接続情報」とを対応付けて記憶する。

[0017] 図2の例を挙げて説明すると、構成情報記憶装置30は、端末名「端末1」とIPアドレス「10.1.1.1」とMACアドレス「70:58:12:27:B7:17」と接続情報「メールサーバ→端末1、端末1→端末3」とを対応付けて記憶する。これは、端末1のIPアドレスが「10.1.1.1」であり、MACアドレス「70:58:12:27:B7:17」であって、メールサーバ70と端末3と接続関係にあることを意味する。

[0018] また、構成情報記憶装置30は、後述する状態特定部11によって特定された端末50の状態を示す端末の状態情報、後述する感染特定部12によって特定された感染の疑いがある端末および感染端末の候補を記憶する。例えば、構成情報記憶装置30は、図3に例示するように、端末の名称を示す「端末名」と、端末の状態を示す「端末状態」と、感染の疑いの度合いを示す「感染疑いスコア」と、感染するリスクの度合いを示す「感染リスクスコア」とを対応付けて記憶する。

[0019] ここで、端末状態には、「感染疑い」、「感染」、「非感染」、「感染拡大候補」、「被攻撃」がある。「感染疑い」は、感染の疑いがある状態である。「感染」は、感染が確定した状態である。「非感染」は、感染していない状態である。「感染拡大候補」は、今後感染する可能性がある状態である。「被攻撃」は、感染した端末等から攻撃を受けた状態である。なお、感染疑いスコアは、数値が高いほど感染の疑いが強く、また、感染リスクスコアは、数値が高いほど今後感染する可能性が高いものとする。

[0020] 図3の例を挙げて説明すると、構成情報記憶装置30は、端末名「端末1」と端末状態「感染疑い」と感染疑いスコア「0.33」と感染リスクスコア「0.1」とを対応付けて記憶する。これは、端末1の現在の状態が感染の疑いがある状態であり、感染疑いスコアが「0.33」であり、感染リスクスコアが「0.1」であることを意味する。

[0021] なお、ここでは、端末名「端末1」は、図1における端末50Aに対応しており、端末名「端末2」は、図1における端末50Bに対応しており、端末名「端末3」は、図1における端末50Cに対応しており、端末名「端末4」は、図1における端末50Dに対応しており、端末名「端末5」は、図1における端末50Eに対応しているものとする。

[0022] また、攻撃対処装置40は、後述する状態特定部11によって特定された感染端末と、後述する感染特定部12によって特定された感染の疑いがある端末のうち感染の疑いが高い端末とに対して、通信の遮断、通信の監視または通信の制限を行う。

[0023] 特定装置10は、端末の状態を特定するとともに、感染の疑いがある端末および今後感染する可能性のある端末の候補を特定する。図1に示すように、特定装置10は、状態特定部11および感染特定部12を有する。

[0024] 状態特定部11は、ネットワーク内への不正侵入または端末50の感染に関する活動を検知するセキュリティ装置20から検知情報を受信し、該検知情報に含まれる端末50の情報および該端末の活動内容から当該端末50の状態を特定する。例えば、状態特定部11は、検知情報が通信に関する情報

である場合には、該通信の送信元アドレスおよび送信先アドレスに対応する端末50の状態を特定し、検知情報が端末50に関する情報である場合には、該端末50の状態を特定する。

[0025] 具体的な例を挙げて説明すると、状態特定部11は、例えば、検知情報が「端末4」が「端末5」と通信を行うことによって「端末4」が「端末5」へ攻撃を行った旨の情報である場合には、通信に関する情報である場合として、該通信の送信元アドレスに対応する「端末4」と送信先アドレスに対応する「端末5」の状態を特定する。また、状態特定部11は、例えば、検知情報が、「端末3」がマルウェアに感染した旨の情報である場合には、端末50に関する情報である場合として、「端末3」の状態を特定する。

[0026] ここで、図4の例を用いて、特定装置10において端末の状態を特定する処理を説明する。図4は、第一の実施の形態に係る特定装置において端末の状態を特定する処理を説明する図である。なお、図4において、各端末50A～50Eの横の数字は当該端末の感染疑いスコアおよび感染リスクスコアの数値例である。攻撃を受けていない状態では、感染疑い数値は全ての端末50において「0」である。また、感染リスクについてはインターネット80との接続性のある端末50に一定のルールにより設定する。図4の例では、数値は、インターネット80および感染端末と直接的な接続性のある端末に対して「0.1」を付加しているが、これに限定されるものではなく、数値の決定方法は任意に設定可能である。

[0027] 図4の例では、端末の名称「端末3」である端末50Cがマルウェアに感染し、感染端末を外部から制御するために外部ネットワークのサーバと行われる通信であるC&C通信をネットワーク内に設置されたセキュリティ装置20が検知した場合の処理を説明する。図4に例示するように、特定装置10の状態特定部11は、セキュリティ装置20から受信した検知情報に含まれる端末3が外部とのC&C通信を行った旨の情報をもとに、端末50Cの状態を特定する。ここで、状態特定部11は、端末3のC&C通信を検知した場合には、端末3がマルウェアに感染していることが確定であると判断可

能なため、端末3の状態を感染状態と特定し、感染疑いスコアを「1.0」とする。

[0028] 感染特定部12は、状態特定部11によって端末50の状態がマルウェアに感染した状態であると特定された場合には、構成情報記憶装置30によって記憶された接続情報に基づいて、検知情報に含まれる端末50の活動内容に至るまでに感染した疑いがある端末50を特定し、感染した端末50が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末50を感染する可能性がある感染端末の候補と特定する。

[0029] 例えば、感染特定部12は、状態特定部11によって特定された感染端末の感染経路となりうる通信経路に含まれる端末50を感染の疑いがある端末50と特定し、感染経路となりうる通信経路の数と、過去の端末の状態とに基づいて、感染の疑いがある各端末50について、感染の疑いの度合いを示す数値を算出する。

[0030] また、例えば、感染特定部12は、状態特定部11によって特定された感染端末を起点に、接続情報を用いて、感染端末からの感染が可能である端末50を感染する可能性がある感染端末の候補と特定する。

[0031] ここで、図5の例を用いて、特定装置10において感染の疑いがある端末50および感染端末の候補を特定する処理を説明する。図5は、第一の実施の形態に係る特定装置において感染の疑いがある端末および感染端末の候補を特定する処理を説明する図である。図5の例では、状態特定部11により「端末3」の状態が感染状態と特定され、感染疑いスコアが「1.0」となったものとする。

[0032] 特定装置10の感染特定部12は、検知情報に含まれる「端末3」の状態が特定された場合に、構成情報記憶装置30の接続情報を用いて、まず端末3の感染経路の特定を行う。図5の例では、端末3への感染経路候補として、インターネット80よりNW機器60を介して直接行われた攻撃、端末1を介した攻撃または端末2を介した攻撃の合計3通りの経路が考えられる。

[0033] このため、感染経路となりうる通信経路の数「3」から加算する感染疑い

スコアを「0.33 (1/3)」とし、端末1および端末2の過去の感染疑いスコアに加算して、感染の疑いの度合いを示す数値である感染疑いスコアを算出する。なお、感染経路が複数存在する場合の感染疑いスコアの割り振りについては、経路単位で均等に配分する場合を説明したが、統計情報を用いた重みを付けた割り振りも可能であり、数値の決定方法はこれに限定されるものではない。

[0034] 次に、感染特定部12は、感染端末および感染と疑われる端末50から、次の感染拡大先端末の候補を特定する。図5の例では、感染端末である端末3を起点に、端末3と接続する端末5が感染可能であり、端末5を感染拡大先端末の候補と特定するとともに、感染リスクスコアに「0.1」を加算する。また、端末1および端末2の感染疑いスコアが「0.33」であり、端末2から感染拡大可能な端末4に対して「0.33」に「0.1」を乗算し、小数点第3位以下を切り捨てたスコア「0.03」を感染リスクスコアに加算する。

[0035] この結果、図5に例示するように、端末4の感染リスクスコアが「0.13」となる。このように、感染特定部12は、端末の状態が変化したり、感染疑いスコアや感染リスクスコアが変化したりした場合には、構成情報記憶装置30に記憶された端末の状態情報と、感染疑いスコアおよび感染リスクスコアとを更新する。

[0036] 次に、図6を用いて、攻撃対処装置40において感染が確定した端末に対する対処を説明する。図6は、第一の実施の形態に係る攻撃対処装置において感染が確定した端末に対する対処を説明する図である。攻撃対処装置40は、端末3の感染疑いスコアが第一の閾値（例えば、「0.9」）を超えた場合には、端末3に対する対処を決定する。図6に例示するように、端末3の感染疑いスコアが「1.0」となっており、第一の閾値を超えているので、端末3への対処を決定する。図6の例では、端末3は感染が確定した端末であるため、対処の内容としては、端末3の隔離を行い、端末3に関する通信を遮断する。

[0037] 次に、図7および図8を用いて、新たな事象として、端末4から端末5への攻撃をセキュリティ装置20が検知した場合における特定装置10および攻撃対処装置40の処理について説明する。図7は、第一の実施の形態に係る特定装置において感染の疑いがある端末および感染端末の候補を特定する処理を説明する図である。図8は、第一の実施の形態に係る攻撃対処装置において感染の可能性が高い端末に対する対処を説明する図である。

[0038] 図7に例示するように、特定装置10の状態特定部11は、セキュリティ装置20から受信した検知情報（端末4から端末5への攻撃）をもとに、端末4および端末5の状態を特定する。ここで、端末4から端末5への攻撃を検知した場合、端末4がマルウェアに感染したことが確定しているものと判断可能なため、端末4の状態を感染状態と特定し、感染疑いスコアに「1.0」を加算し、端末4の感染疑いスコア「1.0」とする。また、図7の例では、端末4への感染経路候補として、インターネット80よりNW機器60を介して直接行われた攻撃、端末2を介した攻撃の合計2通りの経路が考えられる。このため、感染経路となりうる通信経路の数「2」から加算する感染疑いスコアを「0.5（1／2）」とし、感染経路候補上に位置する端末2の感染疑いスコアに「0.5」を加算する。この結果、端末2の感染疑いスコアが「0.83」となる。

[0039] また、端末5は、端末4から端末5への攻撃を受けているので、端末5の状態を被攻撃状態と特定し、ここでは、感染疑いスコアに「0.5」を加算し、感染リスクスコアに「1.0」を加算する。この結果、端末5の感染疑いスコアが「0.5」となり、感染リスクスコアが「1.1」となる。

[0040] そして、図8に例示するように、攻撃対処装置40は、感染疑いスコアが第二の閾値（例えば、「0.7」）を超えた場合には、端末2に対する対処として、通信監視および通信制限を決定する。図8に例示するように、端末2の感染疑いスコアが「0.83」となっており、第二の閾値を超えているので、端末2への対処を決定する。図8の例では、端末2は感染している可能性が高い端末であるため、対処の内容としては、通信監視および通信制限

の対処を行う。このように、感染している可能性が高い端末に対して、通信監視および通信制限の対処を行うことで、端末２が感染していた場合の新たな端末５０への感染拡大および端末２から外部Ｃ＆Ｃ通信接続等を防ぐことができる。

[0041] このように、特定システム１では、セキュリティ装置２０が攻撃を検知する度に、上記したように特定装置１０が感染の疑いがある端末や今後感染する可能性のある端末の候補を特定する処理を繰り返す事により、感染疑い端末の候補を特定し、さらに例えば候補端末に対して候補となった回数や感染疑いを数値化した情報を累積演算する事により、検知した端末以外の感染端末を特定および、感染していた場合の侵入拡大・被害発生の低減を行う事が可能となる。

[0042] [特定装置の処理の流れ]

次に、図９を用いて、第一の実施の形態に係る特定装置１０の処理の流れを説明する。図９は、第一の実施の形態に係る特定装置の処理の流れを示すフローチャートである。

[0043] 図９に示すように、特定装置１０の状態特定部１１は、セキュリティ装置２０から検知情報を受信すると（ステップＳ１０１肯定）、該検知情報に含まれる端末５０の情報および該端末の活動内容から当該端末５０の状態を特定する（ステップＳ１０２）。

[0044] そして、特定装置１０の感染特定部１２は、状態特定部１１によって端末５０の状態がマルウェアに感染した状態であると特定された際に、構成情報記憶装置３０に記憶された接続情報を参照し、感染端末と接続関係にある端末が存在するか否かを判定する（ステップＳ１０３）。

[0045] この結果、特定装置１０の感染特定部１２は、感染端末と接続関係にある端末が存在しないと判定した場合には（ステップＳ１０３否定）、構成情報記憶装置３０の端末の状態情報を更新して（ステップＳ１０５）、処理を終了する。

[0046] また、特定装置１０の感染特定部１２は、感染端末と接続関係にある端末

が存在すると判定した場合には（ステップS 1 0 3 肯定）、感染端末と接続関係にある各端末5 0 について、感染端末へ至る経路上にある端末5 0 を感染疑い端末と特定し、感染端末の先に位置する端末を感染候補端末と特定する（ステップS 1 0 4）。構成情報記憶装置3 0 の端末の状態情報を更新して（ステップS 1 0 5）、処理を終了する。

[0047] [特定システムの処理の流れ]

次に、図1 0 を用いて、第一の実施の形態に係る特定システム1 の処理の流れを説明する。図1 0 は、第一の実施の形態に係る特定システムの処理の流れを示すシーケンス図である。

[0048] 図1 0 に示すように、セキュリティ装置2 0 は、不正通信等を検知すると（ステップS 2 0 1）、検知情報を特定装置1 0 へ送信する（ステップS 2 0 2）。特定装置1 0 は、検知情報を受信すると、検知情報を用いて、端末5 0 の状態を特定する（ステップS 2 0 3）。具体的には、特定装置1 0 は、該検知情報に含まれる端末5 0 の情報および該端末の活動内容から端末5 0 の状態を特定する。

[0049] そして、特定装置1 0 は、端末5 0 の状態がマルウェアに感染した状態であると特定した際には、構成情報記憶装置3 0 に記憶された接続情報を要求する（ステップS 2 0 4）。続いて、特定装置1 0 は、要求した接続情報を参照し（ステップS 2 0 5）、感染端末と接続関係にある各端末5 0 について、感染端末へ至る経路上にある端末5 0 を感染疑い端末と特定し、感染端末の先に位置する端末を感染候補端末と特定する（ステップS 2 0 6）。その後、特定装置1 0 は、構成情報記憶装置3 0 の端末の状態情報を更新して（ステップS 2 0 7）、処理を終了する。

[0050] [第一の実施の形態の効果]

このように、第一の実施の形態に係る特定装置1 0 は、ネットワーク内への不正侵入または端末5 0 の感染に関する活動を検知するセキュリティ装置2 0 から検知情報を受信し、該検知情報に含まれる端末5 0 の情報および該端末5 0 の活動内容から当該端末5 0 の状態を特定する。そして、特定装置

１０は、状態特定部１１によって端末５０の状態がマルウェアに感染した状態であると特定された場合には、構成情報記憶装置３０によって記憶された接続情報に基づいて、検知情報に含まれる端末５０の活動内容に至るまでに感染した疑いがある端末５０を特定し、感染した端末５０が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末５０を感染する可能性がある感染端末の候補と特定する。このため、感染端末を検知するだけでなく、感染の疑いがある端末や今後感染する可能性がある感染端末の候補を特定することが可能となる。

[0051] つまり、特定装置１０は、例えば、標的型攻撃やＡＰＴ攻撃に関する事象等を検知した際に、検知した端末だけでなく、検知した端末への経路となった端末や侵入・感染拡大先端末の候補を特定する事が可能となり、これらの端末の監視強化や通信制限、通信遮断等の対処を行う事が可能となる。

[0052] [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。例えば、特定装置１０の状態特定部１１と感染特定部１２の機能について、それぞれの機能を別々の装置が有するようにしてもよい。また、例えば、特定装置１０が、構成情報記憶装置３０の情報を記憶するようにしてもよいし、攻撃対処装置４０の機能を有するようにしてもよい。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該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。

[0053] また、本実施形態において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部

を公知の方法で自動的におこなうこともできる。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。

[0054] [プログラム]

また、一実施形態として、特定装置 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特定処理を実行する特定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、上記の特定プログラムを情報処理装置に実行させることにより、情報処理装置を特定装置 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、例えば、デスクトップ型またはノート型のパーソナルコンピュータが含まれる。また、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特定処理に関するサービスを提供するサーバ装置として実装することもできる。例えば、特定装置 10 は、感染端末を検知するだけでなく、感染の疑いがある端末や今後感染する可能性がある感染端末の候補を特定する処理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、特定装置 10 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。

[0055] 図 11 は、特定プログラムを実行するコンピュータを示す図である。コンピュータ 1000 は、例えば、メモリ 1010、CPU (Central Processing Unit) 1020 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。

[0056] メモリ 1010 は、ROM (Read Only Memory) 1011 及び RAM (Random Access Memory) 1012 を含む。ROM 1011 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１０３１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１０４１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１０４１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１０５１、キーボード１０５２に接続される。ビデオアダプタ１０６０は、例えばディスプレイ１０６１に接続される。

[0057] ハードディスクドライブ１０３１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。すなわち、特定装置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１０３１に記憶される。例えば、特定装置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１０３１に記憶される。なお、ハードディスクドライブ１０３１は、SSD (Solid State Drive) により代替されてもよい。

[0058] 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１０３１に記憶される。そして、CPU１０２０が、メモリ１０１０やハードディスクドライブ１０３１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RAM１０１２に読み出して実行する。

[0059] 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１０３１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１０４１等を介してCPU１０２０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 (Local Area Ne

work)、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CPU1020によって読み出されてもよい。

符号の説明

- [0060] 1 特定システム
- 10 特定装置
- 11 状態特定部
- 12 感染特定部
- 20 セキュリティ装置
- 30 構成情報記憶装置
- 40 攻撃対処装置
- 50、50A～50E 端末
- 60 NW機器
- 70 メールサーバ
- 80 インターネット

請求の範囲

- [請求項1] ネットワーク内の端末に関する情報を記憶する構成情報記憶装置と、前記端末の状態を特定する特定装置とを有する特定システムであって、
- 前記構成情報記憶装置は、前記ネットワーク内における端末同士の接続関係を示す接続情報を記憶し、
- 前記特定装置は、
- 前記ネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定部と、
- 前記状態特定部によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、前記構成情報記憶装置によって記憶された接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定部と
- を有することを特徴とする特定システム。
- [請求項2] 前記状態特定部は、前記検知情報が通信に関する情報である場合には、該通信の送信元アドレスおよび送信先アドレスに対応する端末の状態を特定し、前記検知情報が端末に関する情報である場合には、該端末の状態を特定することを特徴とする請求項1に記載の特定システム。
- [請求項3] 前記構成情報記憶装置は、前記ネットワーク内の端末のアドレス情報、前記状態特定部によって特定された端末の状態を示す端末状態情報、前記感染特定部によって特定された感染の疑いがある端末および感染端末の候補を記憶することを特徴とする請求項1または2に記載の特定システム。

- [請求項4] 前記感染特定部は、前記状態特定部によって特定された感染端末の感染経路となりうる通信経路に含まれる端末を感染の疑いがある端末と特定し、前記感染経路となりうる通信経路の数と、過去の端末の状態とに基づいて、感染の疑いがある各端末について、感染の疑いの度合いを示す数値を算出することを特徴とする請求項1または2に記載の特定システム。
- [請求項5] 前記感染特定部は、前記状態特定部によって特定された感染端末を起点に、前記接続情報を用いて、前記感染端末からの感染が可能である端末を感染する可能性がある感染端末の候補と特定することを特徴とする請求項1または2に記載の特定システム。
- [請求項6] 前記特定システムは、さらに攻撃対処装置を有し、
前記攻撃対処装置は、前記状態特定部によって特定された感染端末と、前記感染特定部によって特定された感染の疑いがある端末のうち感染の疑いが高い端末とに対して、通信の遮断、通信の監視または通信の制限を行うことを特徴とする請求項1または2に記載の特定システム。
- [請求項7] 前記攻撃対処装置は、前記端末の感染の疑いの度合いを示す感染疑いスコアが第1の閾値を超えた場合は、当該端末の通信を遮断し、第2の閾値を超えた場合は、当該端末の通信監視および通信制限を行うことを特徴とする請求項6に記載の特定システム。
- [請求項8] 複数の端末を含むネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知に関する検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定部と、
前記状態特定部によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、ネットワーク内の端末同士の接続関係を示す接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今

後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定部とを有することを特徴とする特定装置。

[請求項9]

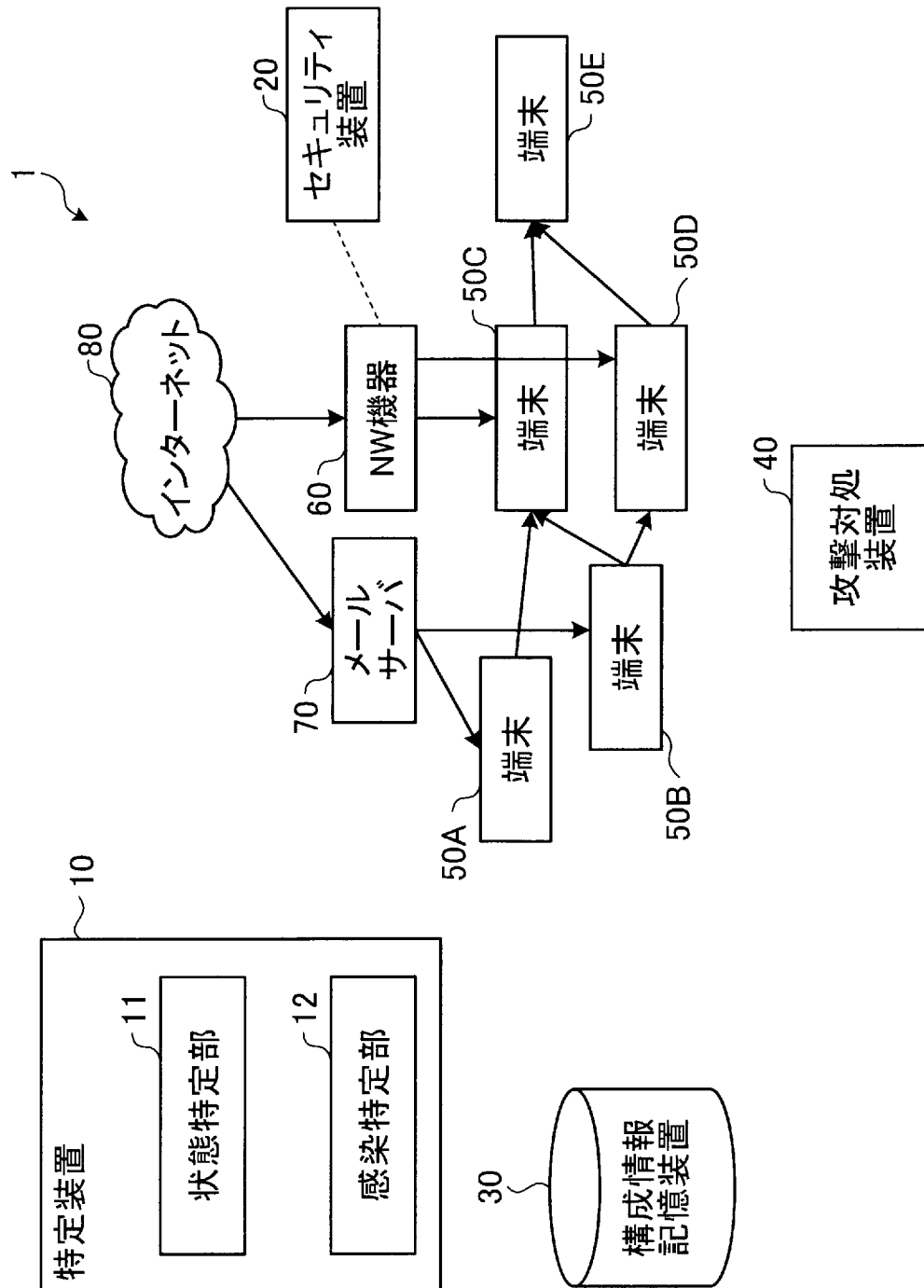
特定装置によって実行される特定方法であって、

複数の端末を含むネットワーク内への不正侵入または端末の感染に関する活動を検知するセキュリティ装置から検知に関する検知情報を受信し、該検知情報に含まれる端末の情報および該端末の活動内容から当該端末の状態を特定する状態特定工程と、

前記状態特定工程によって前記端末の状態がマルウェアに感染した状態であると特定された場合には、ネットワーク内の端末同士の接続関係を示す接続情報に基づいて、前記検知情報に含まれる端末の活動内容に至るまでに感染した疑いがある端末を特定し、感染した端末が今後不正侵入または端末の感染に用いる可能性がある経路上に位置する端末を感染する可能性がある感染端末の候補と特定する感染特定工程と

を含んだことを特徴とする特定方法。

[図1]



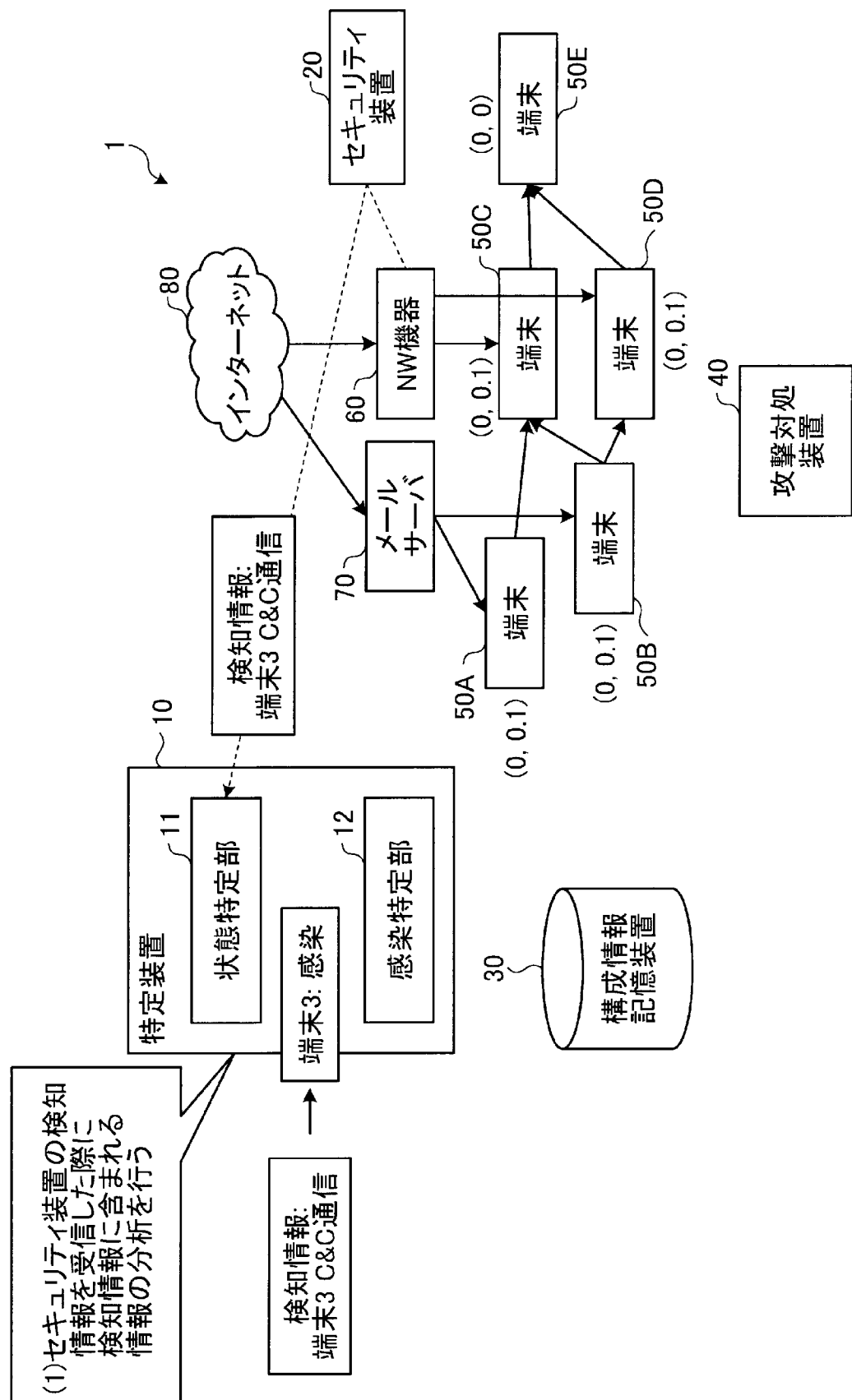
[図2]

端末名	IPアドレス	MACアドレス	接続情報
端末1	10.1.1.1	70:58:12:27:B7:17	メールサーバ→端末1、 端末1→端末3
端末2	10.1.2.1	70:58:12:27:B7:16	メールサーバ→端末2、 端末2→端末3、 端末2→端末4

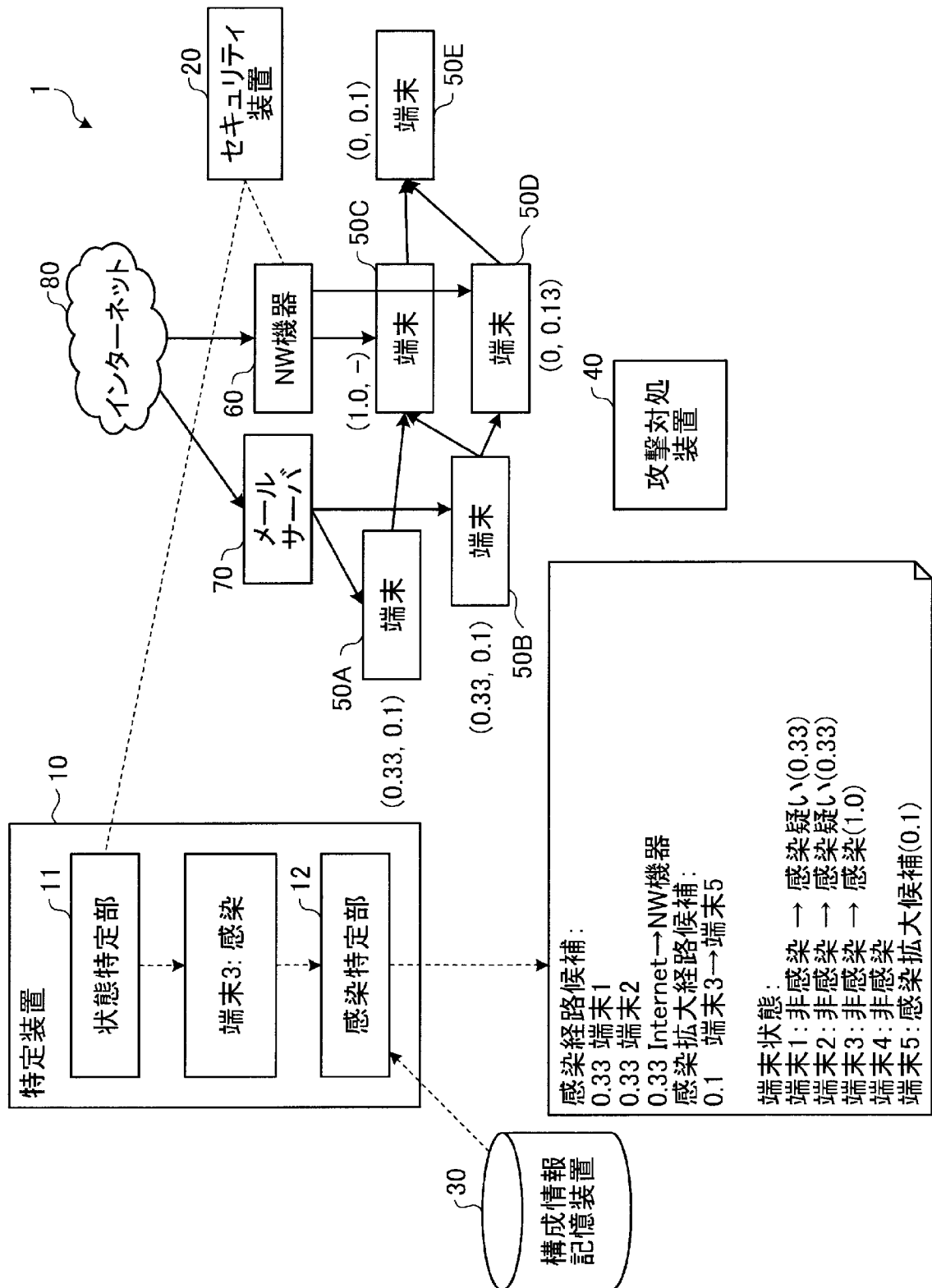
[図3]

端末名	端末状態	感染疑いスコア	感染リスクコア
端末1	感染疑い	0.33	0.1
端末2	感染疑い	0.33	0.1
端末3	感染	1.0	0.1
端末4	非感染	0	0.13
端末5	感染拡大候補	0	0.1

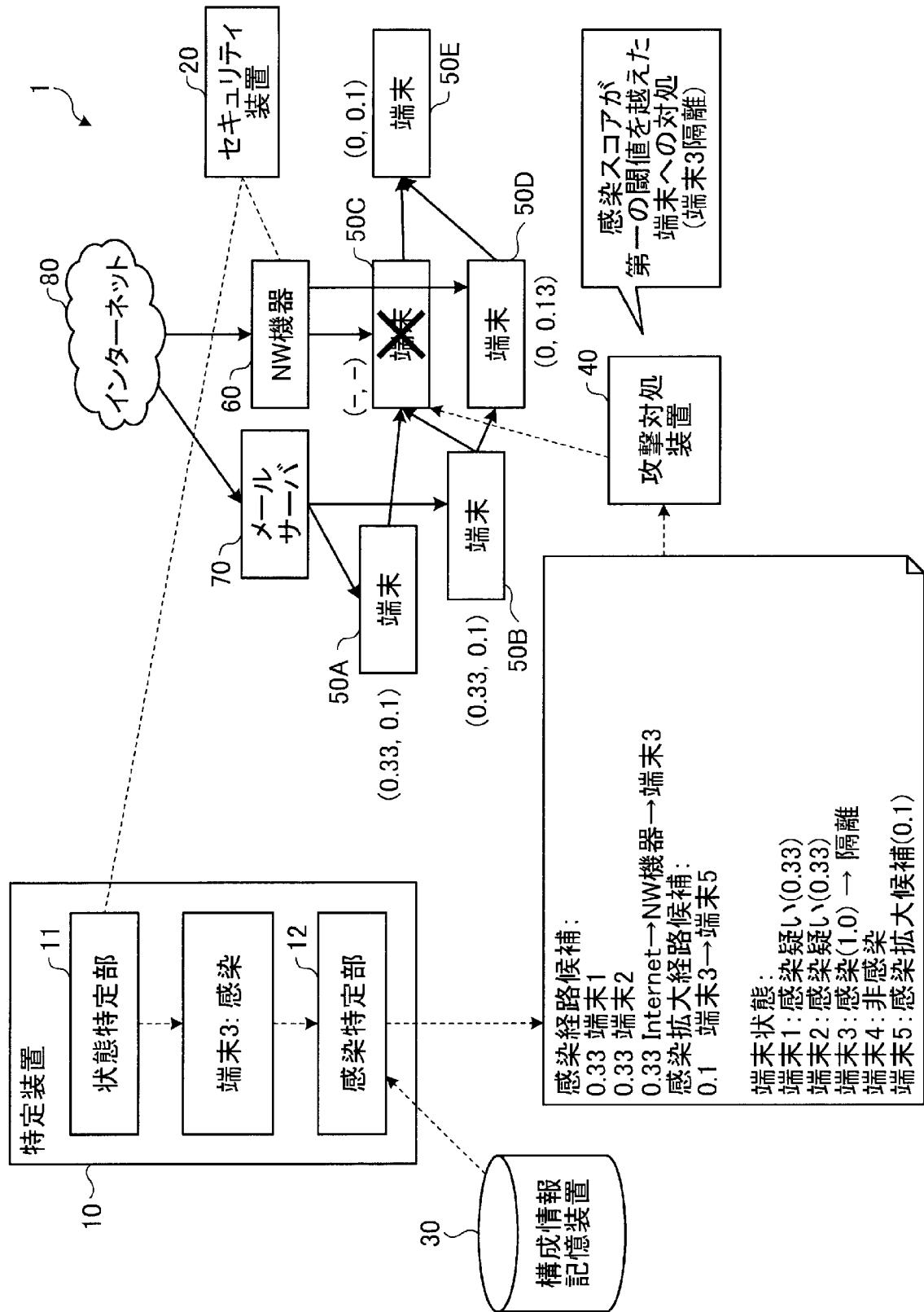
[図4]



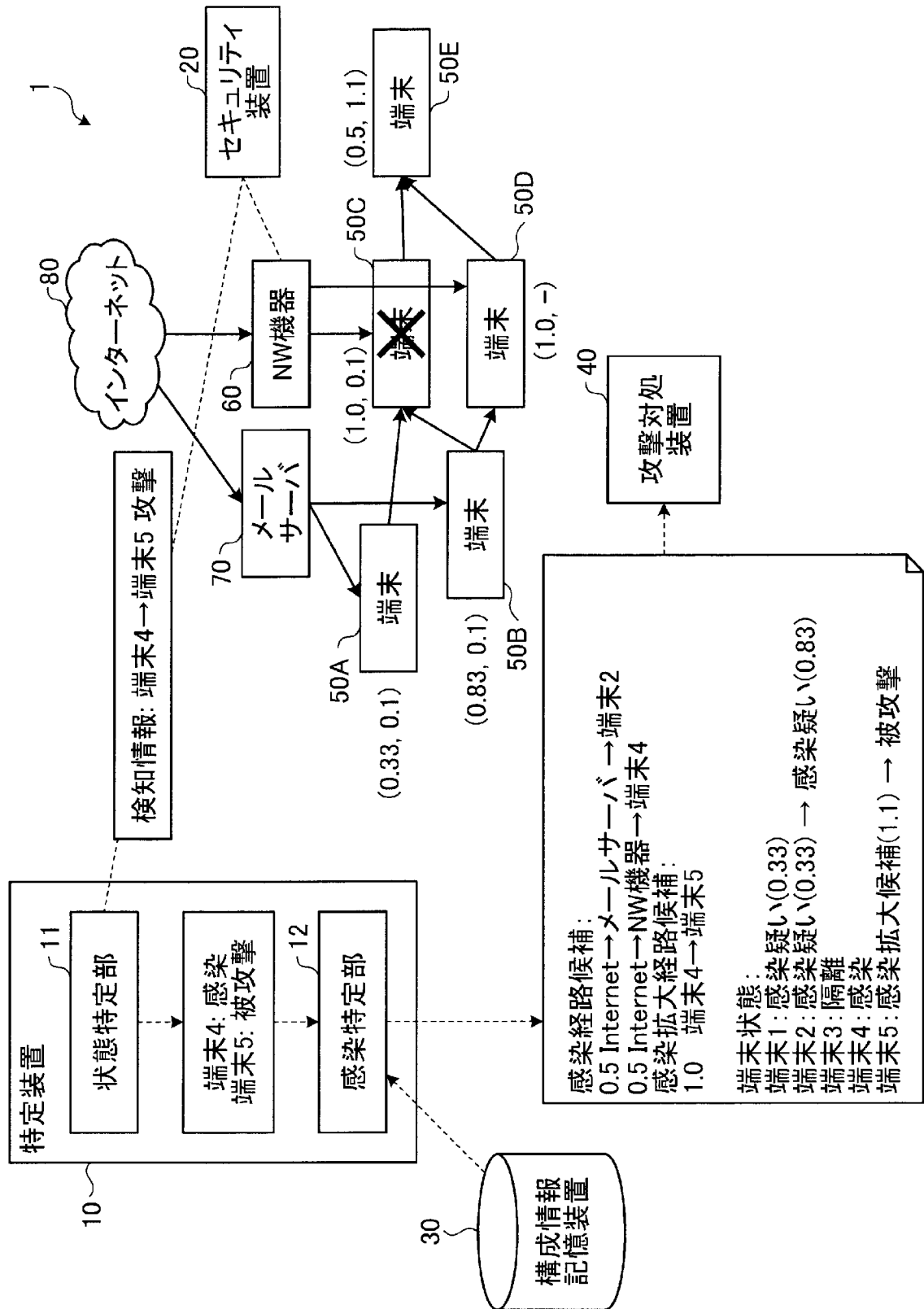
[図5]



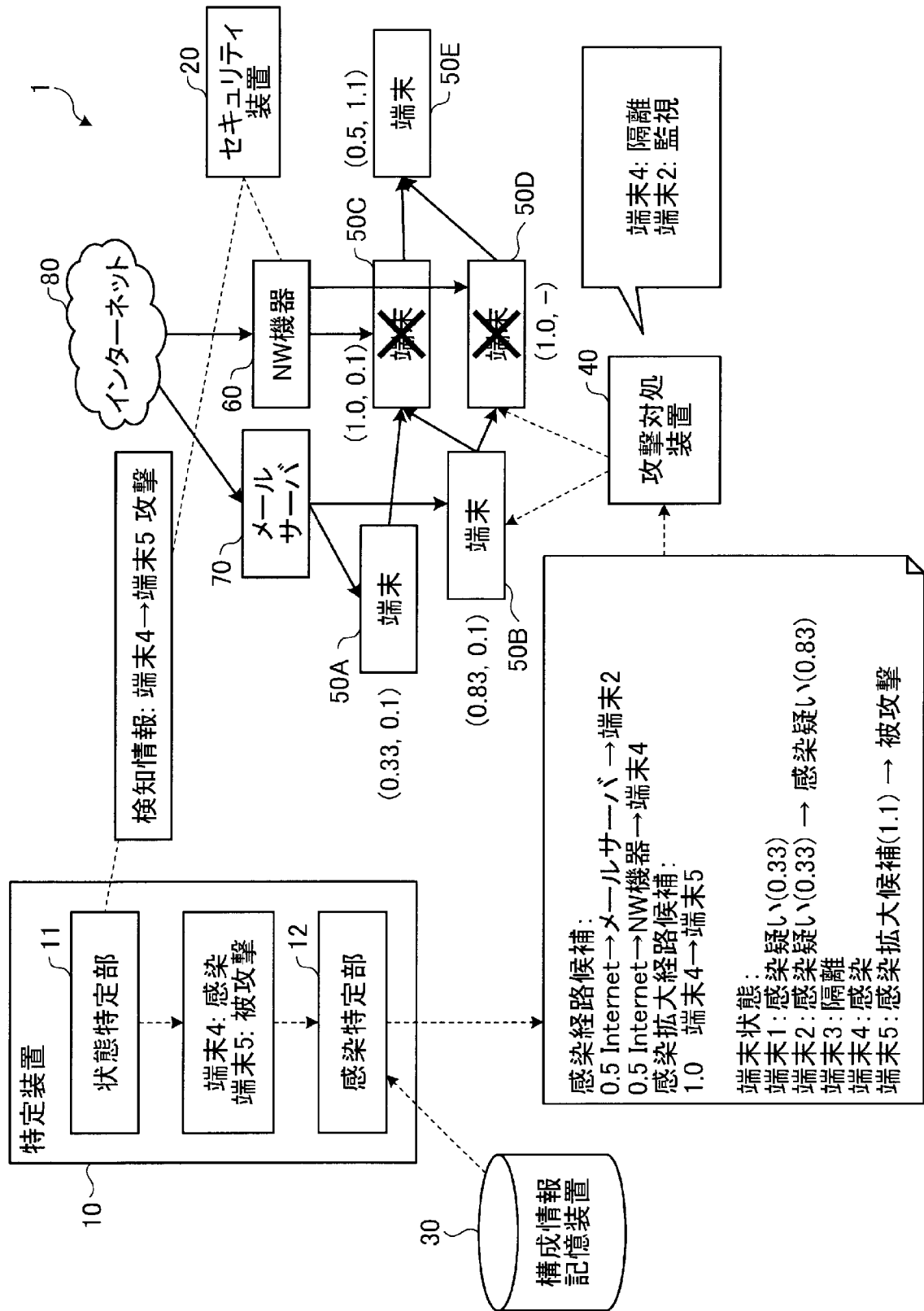
[図6]



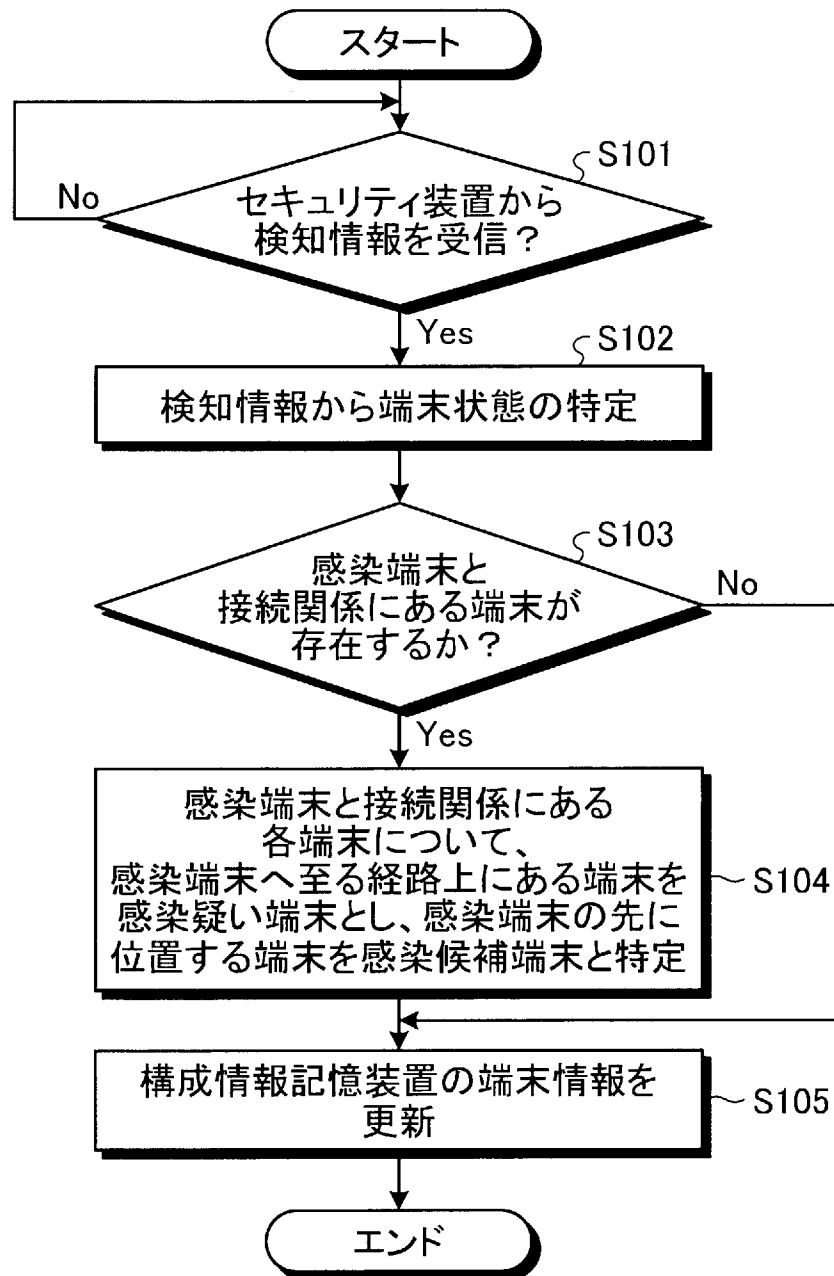
[図7]



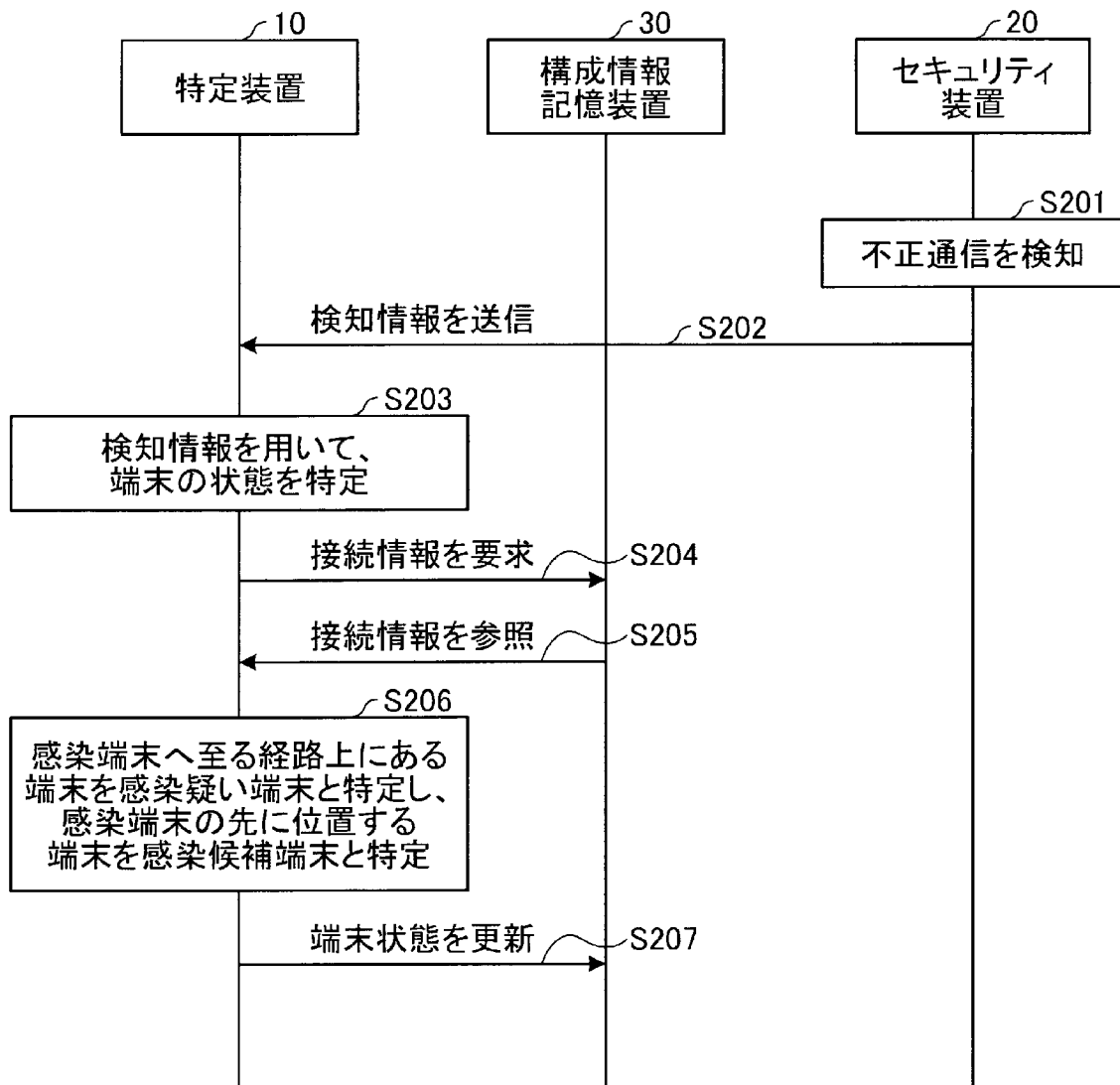
[図8]



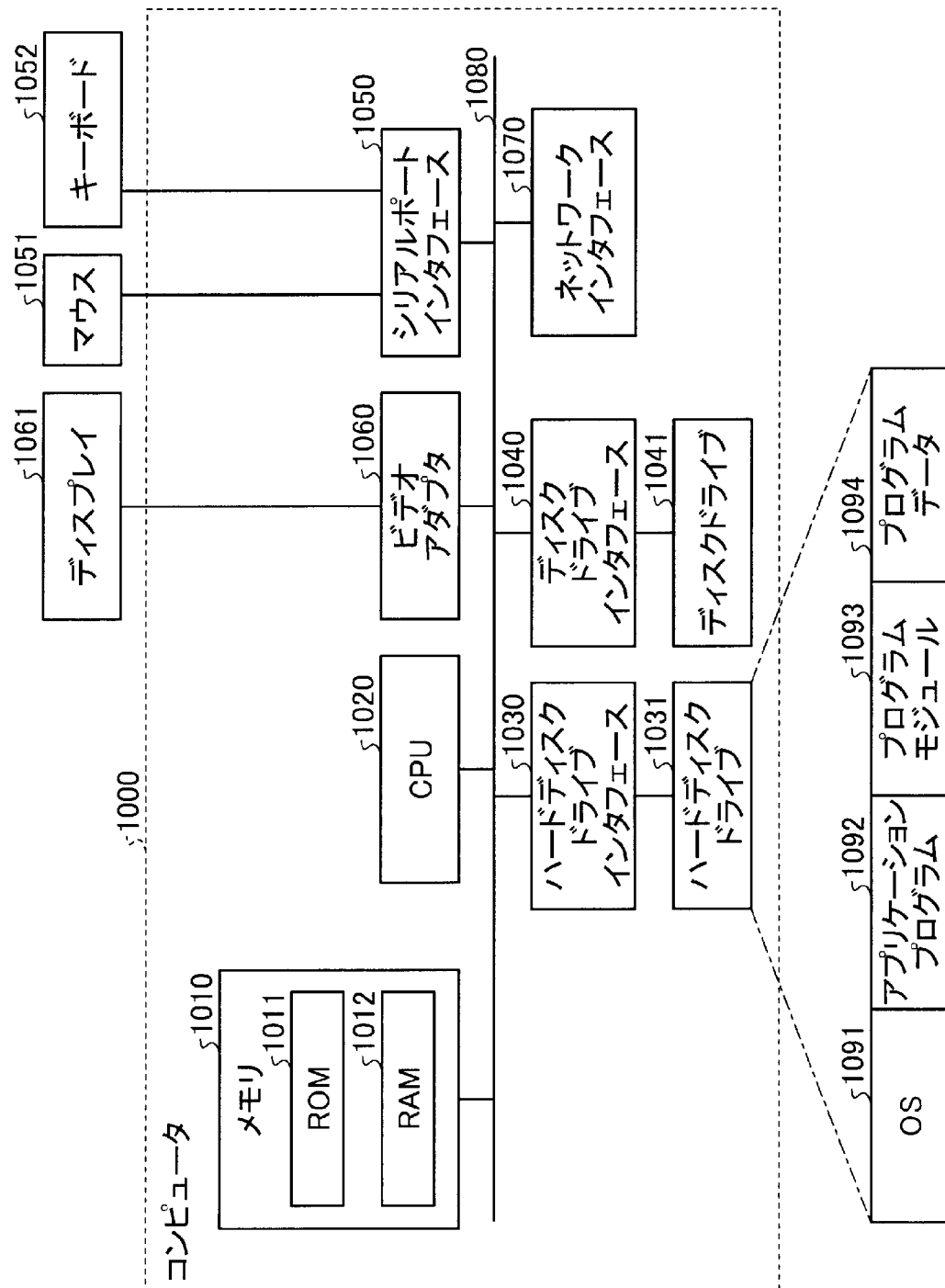
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/079620

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/70(2013.01)i, G06F21/56(2013.01)i

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)

H04L12/70, G06F21/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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 2015-95159 A (Nippon Telegraph and Telephone Corp.), 18 May 2015 (18.05.2015), 0013, 0030, 0082; fig. 2, 3, 7 (Family: none)	1-6, 8, 9 7
Y A	JP 2011-101172 A (NEC Corp.), 19 May 2011 (19.05.2011), 0012 to 0018; fig. 1 to 4 (Family: none)	1-6, 8, 9 7
A	JP 2008-141398 A (Mitsubishi Electric Corp.), 19 June 2008 (19.06.2008), entire text; all drawings (Family: none)	1-9

☒ 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
13 December 2016 (13.12.16)

Date of mailing of the international search report
27 December 2016 (27.12.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/079620

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-117929 A (Nippon Telegraph and Telephone Corp.), 28 May 2009 (28.05.2009), entire text; all drawings (Family: none)	1-9

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L12/70(2013.01)i, G06F21/56(2013.01)i

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））

Int.Cl. H04L12/70, G06F21/56

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016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 A	JP 2015-95159 A（日本電信電話株式会社）2015.05.18, 0013, 0030, 0082, 図2, 図3, 図7（ファミリーなし）	1-6, 8, 9 7
Y A	JP 2011-101172 A（日本電気株式会社）2011.05.19, 0012-0018, 図1-4（ファミリーなし）	1-6, 8, 9 7
A	JP 2008-141398 A（三菱電機株式会社）2008.06.19, 全文、全図（ファミリーなし）	1-9

☒ 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矛盾するものではなく、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

13.12.2016

国際調査報告の発送日

27.12.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

宮島 郁美

5X

8523

電話番号 03-3581-1101 内線 3596

C (続き) . 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	JP 2009-117929 A (日本電信電話株式会社) 2009.05.28, 全文、全図 (ファミリーなし)	1-9