

(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
2022年11月17日(17.11.2022)



(10) 国際公開番号

WO 2022/239162 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

武蔵野市緑町3丁目9-11 NTT 知的財産センタ内 Tokyo (JP).

(21) 国際出願番号: PCT/JP2021/018118

(22) 国際出願日: 2021年5月12日(12.05.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(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).

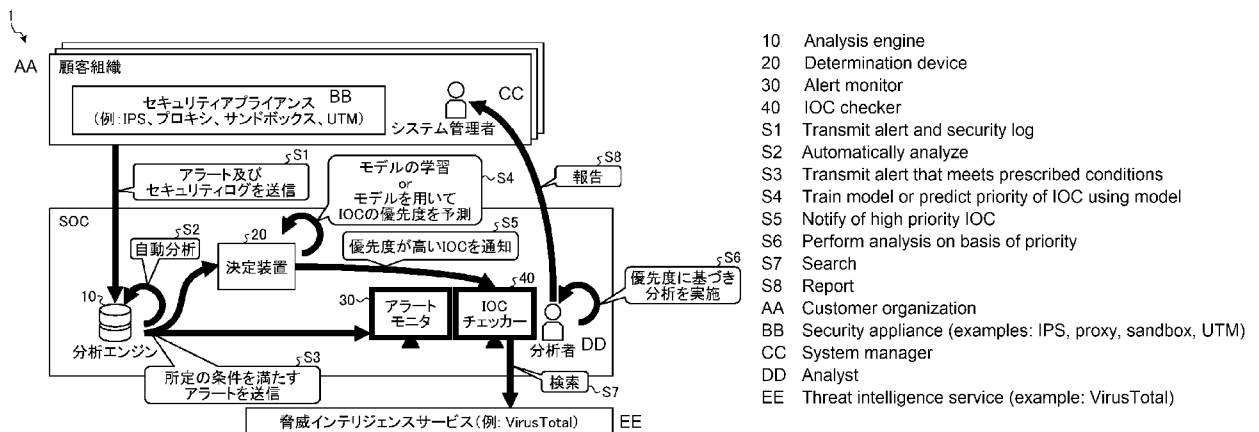
(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング Tokyo (JP).

(72) 発明者: 千葉 大紀 (CHIBA, Daiki); 〒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). 秋山 満昭 (AKIYAMA, Mitsuaki); 〒1808585 東京都

(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, IT, JO, JP, KE, KG, KH, 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,

(54) Title: DETERMINATION METHOD, DETERMINATION DEVICE, AND DETERMINATION PROGRAM

(54) 発明の名称: 決定方法、決定装置及び決定プログラム



(57) Abstract: A feature information extraction unit (21) extracts feature information from IOCs included in information relating to cyber security. A label assignment unit (22) assigns a label to each IOC in accordance with the actual amount of operation that was required to handle an alert associated with the IOC. A training unit (23) trains a model that outputs a label from IOC feature information, using training data that combines the feature information extracted by the feature information extraction unit (21) with the labels assigned by the label assignment unit (22).

(57) 要約: 特徴情報抽出部(21)は、サイバーセキュリティに関する情報に含まれるIOCから特徴情報を抽出する。ラベル付与部(22)は、IOCのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与する。学習部(23)は、特徴情報抽出部(21)によって抽出された特徴情報及びラベル付与部(22)によって付与されたラベルを組み合わせた学習データを用いて、IOCの特徴情報からラベルを出力するモデルの学習を行う。

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))

明 細 書

発明の名称： 決定方法、決定装置及び決定プログラム

技術分野

[0001] 本発明は、決定方法、決定装置及び決定プログラムに関する。

背景技術

[0002] 企業や組織ではサイバーセキュリティを担保するために、セキュリティ管理や脅威を検知するためのシステムが導入されている。セキュリティオペレーションセンタ（SOC：Security Operation Center）は、このようなシステムの運用を行う組織である。SOCのアナリスト（分析者）は、システムから出力される大量のログやアラートを監視、分析し、必要な対処を行う。

[0003] 一方で、下記の参考文献1、2によると、日々大量に発生するアラートを処理するアナリストが、アラート疲労と呼ばれる状況を起こし、アナリストの燃え尽きにつながるものが問題視されている。

参考文献1：S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, “A human capital model for mitigating security analyst burnout,” Proc. SOUPS, 2015.

参考文献2：Ponemon Institute, “Improving the Effectiveness of the Security Operations Center,” 2019.

[0004] また、上記の問題を解決するために必要なことは、よりすぐれた自動化を実現してアナリストの稼働を削減することである。実際、参考文献3によると、多くのSOCのマネージャは、SOCコンポーネントの自動化レベルが不十分であることが現在のSOC組織における最重要課題であるにとらえている。

参考文献3：F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupe, and G.-J. Ahn, “Matched and Mismatched,”

tched SOC's: A Qualitative Study on Security Operations Center Issues," Proc. ACM CCS, 2019.

[0005] これに対し、例えば、セキュリティに関する各アラートの異常スコアや悪性度スコアを過去のアラートから推定することで、真に悪質なアラートと誤検知となる本来非悪性のアラートとを識別する技術が提案されている（例えば、非特許文献1から5を参照）。

[0006] また、セキュリティに関する各アラートと最も関連性の高い情報を抽出してくることで、アナリストのその後のプロセスをサポートする技術が知られている（例えば、非特許文献6から8を参照）。

先行技術文献

非特許文献

[0007] 非特許文献1: W. U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, and A. Bates, "NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage," Proc. NDSS, 2019.

非特許文献2: A. Oprea, Z. Li, R. Norris, and K. Bowers, "MADE: Security Analytics for Enterprise Threat Detection," Proc. ACSAC, 2018.

非特許文献3: K. A. Roundy, A. Tamersoy, M. Spertus, M. Hart, D. Kats, M. Dell'Amico, and R. Scott, "Smoke Detector: Cross-Product Intrusion Detection With Weak Indicators," Proc. ACSAC, 2017.

非特許文献4: Y. Liu, M. Zhang, D. Li, K. Jee, Z. Li, Z. Wu, J. Rhee, and P. Mittal, "Towards a Timely Causality Analysis for Enterprise Security," Proc. NDSS, 2018.

非特許文献5: P. Najafi, A. Muhle, W. Punter, F. Cheng, and C. Meinel, "MalRank: a measure of maliciousness in SIEM-based knowledge graphs," Proc. ACSAC, 2019.

非特許文献6: C. Zhong, J. Yen, P. Liu, and R. F. Erbacher,

“Automate Cybersecurity Data Triage by Leveraging Human Analysts’ Cognitive Process,” Proc. IEEE IDS, 2016.

非特許文献7: C. Zhong, T. Lin, P. Liu, J. Yen, and K. Chen,

“A cyber security data triage operation retrieval system,”

Comput. Secur., vol.76, pp.12–31, 2018.

非特許文献8: S. T. Chen, Y. Han, D. H. Chau, C. Gates, M.

Hart, and K. A. Roundy, “Predicting Cyber Threats with Virtual Security Products,” Proc. ACSAC, 2017.

発明の概要

発明が解決しようとする課題

[0008] しかしながら、従来の技術には、SOCのアナリストの稼働量を十分に減らすことができない場合があるという問題がある。

[0009] 例えば、上記の先行技術文献に記載された技術は、いずれもアナリストが個々のアラートを分析することを前提としている点で共通している。

[0010] ここで、複数のアナリストを擁するSOC拠点では、各アナリストが異なった観点から分析を行う場合がある。この場合、個々のアラートに関する情報が得られる従来の技術では、個々のアラートに対する分析処理を効率化できるものの、分析回数自体を減らすことはできず、SOC拠点全体として十分に稼働量を削減することは困難な場合がある。

課題を解決するための手段

[0011] 上述した課題を解決し、目的を達成するために、決定方法は、決定装置によって実行される決定方法であって、サイバーセキュリティに関する情報に含まれるIOC (Indicator of Compromise) から特徴情報を抽出する特徴情報抽出工程と、前記IOCのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与するラベル付与工程と、前記特徴情報抽出部によって抽出された特徴情報及び前記ラベル付与工程によって付与されたラベルを組み合わせた学習データを用いて、IOCの特徴情報からラベルを出力するモデルの学習を行う学習工程と、を含むことを特徴とす

る。

発明の効果

[0012] 本発明によれば、SOCのアナリストの稼働量を十分に減らすことができる。

図面の簡単な説明

[0013] [図1]図1は、セキュリティシステムについて説明する図である。

[図2]図2は、アラートモニタの画面の例を示す図である。

[図3]図3は、IOCチェッカーの画面の例を示す図である。

[図4]図4は、第1の実施形態に係る決定装置の構成例を示す図である。

[図5]図5は、特徴情報の抽出及びラベルの付与を行う期間を説明する図である。

[図6]図6は、学習処理の流れを示すフローチャートである。

[図7]図7は、ラベルを付与する処理の流れを示すフローチャートである。

[図8]図8は、予測処理の流れを示すフローチャートである。

[図9]図9は、決定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

[0014] 以下に、本願に係る決定方法、決定装置及び決定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。

[0015] [第1の実施形態の構成]

まず、図1を用いて、第1の実施形態に係る決定装置を含むセキュリティシステムについて説明する。図1は、セキュリティシステムについて説明する図である。

[0016] セキュリティシステム1は、顧客組織のセキュリティプライアンスにおいて生じた所定の情報を基に、分析エンジンによる自動分析、又は分析者による分析が行われる。

[0017] セキュリティプライアンスは、例えば侵入防御システム（IPS：Intrusi

on Prevention System)、プロキシ、サンドボックス、統合脅威管理 (U T M : Unified Threat Management) 等である。

[0018] S O Cでは、セキュリティアプライアンスから取得したセキュリティに関する情報をリアルタイムに分析する。例えば、セキュリティに関する情報にはセキュリティログ及びアラートが含まれる。

[0019] 図1の例では、S O Cは大規模なM S S P (Managed Security Service Provider) で提供されるアウトソースS O Cとして利用されている。一方で、本実施形態は、インハウスS O Cにも適用可能である。

[0020] アウトソースS O CとインハウスS O Cは組織的な違いはあるが、全体的なワークフローは類似している。このため、スケールメリットを十分に発揮できる規模の組織のインハウスS O Cであれば、本実施形態の効果が得られやすい。

[0021] セキュリティシステム1における処理の流れを説明する。図1に示すように、まず、顧客組織のセキュリティアプライアンスは、アラート及びセキュリティログをS O Cの分析エンジン10に送信する(ステップS1)。

[0022] 以下、アラートについて処理を行う場合の例を説明する。セキュリティシステム1は、セキュリティログについても、アラートと同様に処理することができる。

[0023] 分析エンジン10は自動分析を行う(ステップS2)。分析エンジン10は、既知の悪意のある特性や、事前に定義されたルールやブラックリストに基づいて分析を行うことで、アラートに対応する。

[0024] 分析エンジン10は、S O A R (Security Orchestration, Automation, and Response) と呼ばれる機能を用いて分析を行ってもよい。

[0025] 分析エンジン10は、所定の条件を満たすアラートを決定装置20、アラートモニタ30又はI O Cチェッカー40に送信する(ステップS3)。

[0026] このとき、図2に示すように、アラートモニタ30は、アラートに関する情報を表示する。図2は、アラートモニタの画面の例を示す図である。

[0027] 例えば、アラートモニタ30には、アラートの原因となったイベントの日

付 (Date)、顧客名 (Customer)、アラートを送信したデバイス (Device)、アラートの名前 (Alert Name)、アラートのトリガーとなった状況の概要等が表示される。

[0028] また、図3に示すように、I O Cチェッカー40は、アラートに含まれるI O C (Indicator of Compromise) に関する情報を表示する。図3は、I O Cチェッカーの画面の例を示す図である。

[0029] 例えば、I O Cには、ドメイン名、I Pアドレス、URL、ファイルハッシュ値等が含まれる。

[0030] 図3に示すように、例えば、I O Cチェッカー40は、S O Cでの調査状況 (Status)、I O Cの悪性度に関するS O Cの直近の判断 (S O C Last Decision)、そのI O Cの最新の脅威インテリジェンス結果 (Detection in TI) 等を表示する。

[0031] 例えば、分析者は、アラートモニタ30及びI O Cチェッカー40といった、I O C評価専用のツールを使って、分析エンジン10によって処理できなかったアラートについてI O Cのトリアージ (評価) を行う。

[0032] S O Cの分析者は日頃のS O Cワークフローで大量のアラートを処理する。そこで、決定装置20は、優先度が高いI O Cを決定し、分析者に通知する。これにより、S O Cにおいて複数の分析者が同じI O Cを手動で評価することを防止することができる。

[0033] また、決定装置20によれば、優先度が高いI O Cを優先して分析することができるため、分析者の稼働量に対する効果を向上させることができる。

[0034] 決定装置20は、モデルの学習、又はモデルを用いてI O Cの優先度の予測を行う (ステップS4)。そして、決定装置20は、予測結果に基づき優先度が高いI O Cを決定し、当該決定したI O Cを通知する (ステップS5)。

[0035] 例えば、決定装置20は、決定したI O Cを、I O Cチェッカー40を介して分析者に通知する。

[0036] 分析者は、通知された優先度に基づき分析を実施する (ステップS6)。

また、分析者は、分析の過程で脅威インテリジェンスサービス（例えば、Virus Total）の検索を行ってもよい（ステップS7）。

[0037] 脅威インテリジェンスサービスの中には、脅威のレベルや悪性度に関するスコアを提供するものがある。しかしながら、本来そのようなスコアは必ずしも分析者の次のアクションを決定するものではない。

[0038] 例えば、既にパッチが展開されている脆弱性を利用した攻撃に関連したＩＯＣは、悪性であるスコアが高いかもしれないが、顧客組織を守るという観点では差し迫った脅威ではない。

[0039] このように、ＳＯＣにおけるアラート分析は単純ではないため、アラート分析を完全自動化することは難しく、分析者による判断が必要になる場合がある。

[0040] このため、決定装置２０による優先度が高いＩＯＣの決定は、分析者の判断の時間を確保し、また各ＩＯＣの調査稼働を削減するために有用であるといえることができる。

[0041] 分析者は、最終的に分析対象のアラート及び当該アラートに含まれたＩＯＣが悪性か非悪性かを判断し、さらに顧客への報告が必要かどうかを判断し、顧客への報告が必要な場合、顧客組織のシステム管理者等に報告を行う（ステップS8）。

[0042] 例えば、分析者があるＩＯＣの評価を完了すると、その結果に基づいて、分析エンジン１０におけるアラートのトリガーされる条件を変更することができる。

[0043] 例えば、分析者による評価で明らかに悪性のＩＯＣが特定された場合、カスタムブラックリスト又はカスタムシグネチャとして当該ＩＯＣを分析エンジン１０において使用することができる。

[0044] その場合、同一ＩＯＣを含むログをＳＯＣの他の顧客でも自動的に検知できるようにすることができる。また、評価で誤検知や脅威レベルが少ないＩＯＣが特定された場合、アラートをトリガーするＳＩＥＭロジックが変更され、同じ誤検知アラートが再び発生するのを防ぐことができ、分析者の稼働

削減につながる。

[0045] 以降、決定装置 20 が優先度の高い IOC を決定する処理について、決定装置 20 の構成とともに詳細に説明する。

[0046] 図 4 は、第 1 の実施形態に係る決定装置の構成例を示す図である。図 4 に示すように、決定装置 20 は、特徴情報抽出部 21、ラベル付与部 22、学習部 23、予測部 24 及びモデル情報 25 を有する。

[0047] 決定装置 20 は、機械学習手法によるモデルの学習処理、及び学習済みのモデルを使った予測処理を行う。

[0048] 学習処理では、特徴情報抽出部 21、ラベル付与部 22 及び学習部 23 が用いられる。また、予測処理では、特徴情報抽出部 21 及び予測部 24 が用いられる。

[0049] 特徴情報抽出部 21 は、サイバーセキュリティに関する情報に含まれる IOC から特徴情報を抽出する。例えば、サイバーセキュリティに関する情報は、分析エンジン 10 から取得するアラートである。

[0050] 特徴情報抽出部 21 は、分析エンジン 10 から入手した過去のアラートに含まれる IOC から、当該 IOC の特性を特徴づける情報（以後、特徴情報）を抽出する。

[0051] 特徴情報は、IOC に含まれるドメイン名、IP アドレス、URL、ファイルハッシュ値等であってもよい。

[0052] 例えば、特徴情報抽出部 21 は、あらかじめ定められた一定の日数の間に発生したアラートから特徴情報を抽出する。

[0053] ラベル付与部 22 は、IOC のそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与する。

[0054] ここでは、ラベルは優先度が高いか否かを表す二値データであるものとする。例えば、ラベル付与部 22 は、過去に分析者の稼働を多く消費した IOC については、優先度が高いことを示すラベルを付与し、そうでないものについては優先度が低いことを示すラベルを付与する。

[0055] なお、従来技術（例えば、非特許文献 4 から 8 に記載の技術）では、IOC

Cが悪性のもの（又は悪意があるもの）であるか否かを示すラベルが付与されていた。一方で、本実施形態では、分析者の稼働量に基づきラベルが付与される。

[0056] ラベル付与部22は、IOCのうち、関連するアラートに対して一定期間内に発生した手動調査の回数が所定値以上であるIOCについて、優先度が高いことを示すラベルを付与し、手動調査の回数が所定値未満であるIOCについて、優先度が低いことを示すラベルを付与する。

[0057] 以降の説明では、優先度が高いことを示すラベルを「優先」、優先度が低いことを示すラベルを「非優先」と表記する。

[0058] 例えば、ラベル付与部22は、ラベル付与時点の前のL日間にK回以上の分析者による手動調査が発生したIOCを「優先」とラベル付けし、それ以外は「非優先」とラベル付けする（ただし、K及びLは整数）。

[0059] 図5に示す学習処理のタイムラインは、ラベル付与部22がいつのデータをラベルの付与に利用するかを示している。図5は、特徴情報の抽出及びラベルの付与を行う期間を説明する図である。

[0060] 例えば、ラベル付与時点が「現在」と表記した時点である場合、ラベル付与部22は、その直近L日間に当該IOCが分析者によってK回以上調査されたか否かを判定する。

[0061] これにより、ラベル付与部22は、過去から直近までのSOCのデータを使って自動的にラベルを付与することができる。

[0062] さらに、ラベル付与部22は、ラベル付与の動作を一定の期間が経過するたびに繰り返すことで、教師あり機械学習に必要な正解ラベル付きのデータを追加し続けることができる。

[0063] また、ラベル付与部22は、分析者による作業を要求することなく自動的にラベルの付与を行うことができるため、分析者の日頃の業務を妨げることがない。

[0064] この点について、SOCやセキュリティ現場で追加される新たなツールは、そのメンテナンスに分析者の追加作業を要求するような個別のソリューション

ョンになりがちであることが、参考文献4で指摘されている。

参考文献4：M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," IEEE Access, vol.8, pp.227756-227779, 2020.

[0065] 本実施形態のラベル付与機能は、自動的に処理を実行し、メンテナンスフリーであるため、ツールの追加による分析者の稼働量の増加という問題を解決しているといえることができる。

[0066] なお、ラベル付与部22は、手動調査の回数ではなく、手動調査に要した時間を基にラベルを付与してもよい。

[0067] その場合、ラベル付与部22は、IOCのうち、関連するアラートに対して一定期間内に発生した手動調査に要した時間が所定値以上であるIOCについて、優先度が高いことを示すラベルを付与し、時間が所定値未満であるIOCについて、優先度が低いことを示すラベルを付与するようにしてもよい。

[0068] 例えば、ラベル付与部22は、ラベル付与時点の前のL日間にT時間以上の分析者による手動調査が発生したIOCを「優先」とラベル付けし、それ以外は「非優先」とラベル付けする（ただし、Tは実数）。

[0069] 学習部23は、特徴情報抽出部21によって抽出された特徴情報及びラベル付与部22によって付与されたラベルを組み合わせた学習データを用いて、IOCの特徴情報からラベルを出力するモデルの学習を行う。

[0070] 学習部23は、教師あり機械学習により、モデルの作成及び更新を行う。モデル情報25は、モデルを構築するためのパラメータ等を含む情報である。学習部23は、モデル情報25の作成及び更新を行う。

[0071] 学習部23は、既知の任意の教師あり機械学習のアルゴリズムを採用することが可能である。本実施形態では、学習部23は標準的なロジスティック回帰を採用するものとする。

[0072] ロジスティック回帰は、スケーラブルで高速なので、SOC環境のように多くの顧客からの大量のアラートに含まれるIOCを予測するのに適してい

る。

[0073] また、ロジスティック回帰は解釈可能性が高いことが知られている。ロジスティック回帰の出力は、その性質上、入力された I O C が優先される確率として解釈でき、さらに各 I O C に対応する特徴情報のうちどの特徴が結果に貢献しているかを示すことができる。このように、ロジスティック回帰には解釈可能性が高いという利点がある。

[0074] ここでは、学習部 2 3 は、特に L 1 正則化つきロジスティック回帰を利用するものとする。

[0075] まず、学習部 2 3 は、特徴情報抽出部 2 1 によって抽出された特徴情報を表すベクトル $\mathbf{x}$ が与えられたとき、(1) 式に示すラベルの条件付き確率 y を、(2) 式のようにモデル化する。

[0076] [数1]

$$y \in \{0(\text{non-priority}), 1(\text{priority})\} \quad \dots (1)$$

[0077] [数2]

$$p(y = 1|\mathbf{x}; \theta) = \sigma(\theta^T \mathbf{x}) = 1/(1 + \exp(-\theta^T \mathbf{x})) \quad \dots (2)$$

[0078] ここで、 θ はロジスティック回帰モデルのパラメータである。また、 σ はシグモイド関数である。また、 $\mathbf{x}$ の全ての特徴は、 $[0, 1]$ の範囲に正規化されるものとする。

[0079] 学習部 2 3 は、正則化の度合いを決定するハイパーパラメータ λ を導入した (4) 式の目的関数を最小化する際のパラメータ θ を求めるために、(3) 式に示す n 個のラベル付きの学習用データの集合を使用する。

[0080] [数3]

$$\{(x_i, y_i)\}_{i=1}^n \quad \dots (3)$$

[0081] [数4]

$$\min_{\theta} \sum_{i=1}^n -\log p(y_i|x_i; \theta) + \lambda \|\theta\|_1 \quad \dots (4)$$

[0082] (4) 式のうち、L 1 正則化部分 $\lambda \|\theta\|_1$ は、目的関数にペナルティを加えており、有意に寄与しない特徴情報を識別して削減する効果がある。

[0083] このような特徴量の削減は必要以上に学習データに合わせてしまうオーバーフィッティングの防止に寄与するだけでなく、メモリ使用量の削減や、SOCアナリストに提示する結果をより簡潔で解釈しやすいものにする効果がある。

[0084] 予測部24は、学習部23による学習が行われたモデルを用いて、IOCの特徴情報からラベルを予測する。

[0085] 予測部24は、学習部23によって学習が行われたモデルを利用して、新たにリアルタイムで発生したアラートに含まれるIOCと対応する特徴情報を入力し、どのIOCが将来的に分析者の稼働を多く消費することになるのかを予測する。

[0086] 例えば、予測部24は、モデル情報25を基に構築したロジスティック回帰モデルを使って予測を行う。

[0087] 例えば、予測部24は、分析者が対象のIOCをP日以内にK回以上手動で分析する確率を予測することである（ただし、Pは整数）。

[0088] 予測部24は、学習部23によって決定されたパラメータ θ を用いて、IOCに対応する特徴情報のベクトル x が「優先」である確率 p を求め、予測するラベル $\hat{y}$ （ y の直上に $\hat{}$ ）を（5）式で定義する。

[0089] [数5]

$$\hat{y} = \begin{cases} 1, & \text{if } p(y|x; \theta) \geq 0.5 \\ 0, & \text{otherwise} \end{cases} \quad \dots (5)$$

[0090] 決定装置20は、予測部24によって予測されたラベルを基に、SOCの分析者による繰り返しの調査につながると考えられるIOC、すなわち「優先」ラベルが予測されたIOCを、確率 p が高い順に出力し、分析者に提示する。

[0091] このとき、分析者は、決定装置20によって提示された情報を利用して、調査対象の優先順位付けを行い、効率的にトリアージや詳細分析を行うことができる。

[0092] SOCの分析者は、IOCに対してどのようなアクションを取るべきかを

可能な限り決定し記録することが求められる。

[0093] 本実施形態によれば、分析者は優先度が高い I O C を調査し、その結果を分析エンジン 10 に反映させることができる。それによって、分析エンジン 10 は同じ I O C を含むアラートを自動処理できるようになるため、分析者が毎回当該 I O C を手動で調査することを回避し、S O C 全体としての稼働量の削減を図ることができる。

[0094] 例えば、分析者は優先度が高いと決定された I O C を調査し、その結果を基に分析エンジン 10 に当該 I O C を自動分析させるようにする。これにより、当該 I O C は他の分析者に受け渡されることがなくなるため、稼働量が削減される。

[0095] なお、決定装置 20 は、学習処理をオフラインで定期的（例えば 1 日に 1 回）に再実行し、モデル情報 25 を更新する。決定装置 20 は、図 5 に示すように、F + L 日間のデータを利用して学習処理を行う。

[0096] 一方、決定装置 20 が、顧客組織からのアラートに含まれる I O C をリアルタイムに処理する際、すなわち予測処理を行う際には、当該 I O C に対して、過去 F 日間分のデータを利用して特徴情報を抽出する。

[0097] そして、決定装置 20 は、抽出した特徴情報から、未来の P 日間に分析者による K 回以上の手動調査が実施される確率 p を計算する。

[0098] 決定装置 20 は、上記の予測処理をリアルタイムに受信する I O C ごとに繰り返す。その結果、分析者が優先的に調査すべき I O C のリストが、図 3 のように I O C チェッカー 40 の画面に表示され継続的に更新される。

[0099] [第 1 の実施形態の処理]

図 6 は、学習処理の流れを示すフローチャートである。図 6 に示すように、まず、決定装置 20 は、過去のアラートの入力を受け付ける（ステップ S 101）。

[0100] 次に、決定装置 20 は、入力されたアラートに含まれる I O C から特徴情報を抽出する（ステップ S 102）。続いて、決定装置 20 は、各 I O C に対する分析者の稼働量に基づいて優先度に関する正解ラベルを付与する（ス

テップS103)。

[0101] そして、決定装置20は、正解ラベルを用いて、特徴情報から優先度に関するラベルを出力するモデルを学習する(ステップS104)。

[0102] 図7は、ラベルを付与する処理の流れを示すフローチャートである。図7の処理は、図6のステップS103に相当する。

[0103] まず、図7に示すように、決定装置20は、kに現在からL日前までの調査回数を代入する(ステップS103a)。

[0104] ここで、kが定数K以上であれば(ステップS103b、Yes)、決定装置20は正解ラベル「優先」を付与する(ステップS103c)。

[0105] 一方、kが定数K未満であれば(ステップS103b、No)、決定装置20は正解ラベル「非優先」を付与する(ステップS103d)。

[0106] 図8は、予測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、決定装置20は、直近のアラートの入力を受け付ける(ステップS201)。

[0107] 次に、決定装置20は、入力されたアラートに含まれるIOCから特徴情報を抽出する(ステップS202)。続いて、決定装置20は、各IOCに対する分析者の稼働量に基づいて正解ラベルを抽出する(ステップS203)。

[0108] そして、決定装置20は、特徴情報を学習済みのモデルに入力して、優先度に関するラベルを予測する(ステップS204)。

[0109] 決定装置20は、予測したラベルに基づき優先度の高いIOCをSOCの分析者に通知することができる。

[0110] [第1の実施形態の効果]

これまで説明してきたように、特徴情報抽出部21は、サイバーセキュリティに関する情報に含まれるIOCから特徴情報を抽出する。ラベル付与部22は、IOCのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与する。学習部23は、特徴情報抽出部21によって抽出された特徴情報及びラベル付与部22によって付与されたラベル

を組み合わせた学習データを用いて、ＩＯＣの特徴情報からラベルを出力するモデルの学習を行う。

[0111] これにより、決定装置２０によって学習が行われたモデルを用いることで、優先度の高いＩＯＣを分析者に通知し、ＳＯＣ全体の稼働量を減らすことができる。

[0112] ラベル付与部２２は、ＩＯＣのうち、関連するアラートに対して一定期間内に発生した手動調査の回数が所定値以上であるＩＯＣについて、優先度が高いことを示すラベルを付与し、手動調査の回数が所定値未満であるＩＯＣについて、優先度が低いことを示すラベルを付与する。

[0113] これにより、決定装置２０は、学習済みのモデルを用いて、手動調査の回数に基づく優先度を予測し分析者に知らせることができる。

[0114] ラベル付与部２２は、ＩＯＣのうち、関連するアラートに対して一定期間内に発生した手動調査に要した時間が所定値以上であるＩＯＣについて、優先度が高いことを示すラベルを付与し、時間が所定値未満であるＩＯＣについて、優先度が低いことを示すラベルを付与する。

[0115] これにより、決定装置２０は、学習済みのモデルを用いて、手動調査の時間に基づく優先度を予測し分析者に知らせることができる。

[0116] 予測部２４は、学習部２３による学習が行われたモデルを用いて、ＩＯＣの特徴情報からラベルを予測する。また、予測部２４は、優先度が高いことを示すラベルが予測されたＩＯＣに関する情報を分析者に通知する。

[0117] これにより、決定装置２０は、優先度の高いＩＯＣを分析者に通知し、ＳＯＣ全体の稼働量を減らすことができる。

[0118] [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、各装置の分散及び統合の具体的形態は図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又は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 (Central Processing Unit) 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。なお、プログラムは、CPUだけでなく、GPU等の他のプロセッサによって実行されてもよい。

[0119] 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。

[0120] [プログラム]

一実施形態として、決定装置20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決定処理を実行する決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、上記の決定プログラムを情報処理装置に実行させることにより、情報処理装置を決定装置20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。

[0121] また、決定装置20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決定処理に関するサービスを提供する決定サーバ装置として実装することもできる。例えば、決定サーバ装置は、セキュリティに関するアラートを入力とし、優先度の高いIOCを出力とする決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、決定サーバ装置は、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決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。

[0122] 図9は、決定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バインタフェース1030、ディスクドライバインタフェース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。

[0123] メモリ1010は、ROM (Read Only Memory) 1011及びRAM (Random Access Memory) 1012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バインタフェース1030は、ハードディスクドライブ1090に接続される。ディスクドライバインタフェース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。

[0124] 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。すなわち、決定装置20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、決定装置20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 (Solid State Drive) により代替されてもよい。

[0125] 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、CPU1020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RAM1012に読み出して、上述した実施形態の処理を実行する。

[0126] 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 Network）、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

- [0127] 1 セキュリティシステム
- 10 分析エンジン
- 20 決定装置
- 21 特徴情報抽出部
- 22 ラベル付与部
- 23 学習部
- 24 予測部
- 25 モデル情報
- 30 アラートモニタ
- 40 I/Oチェッカー

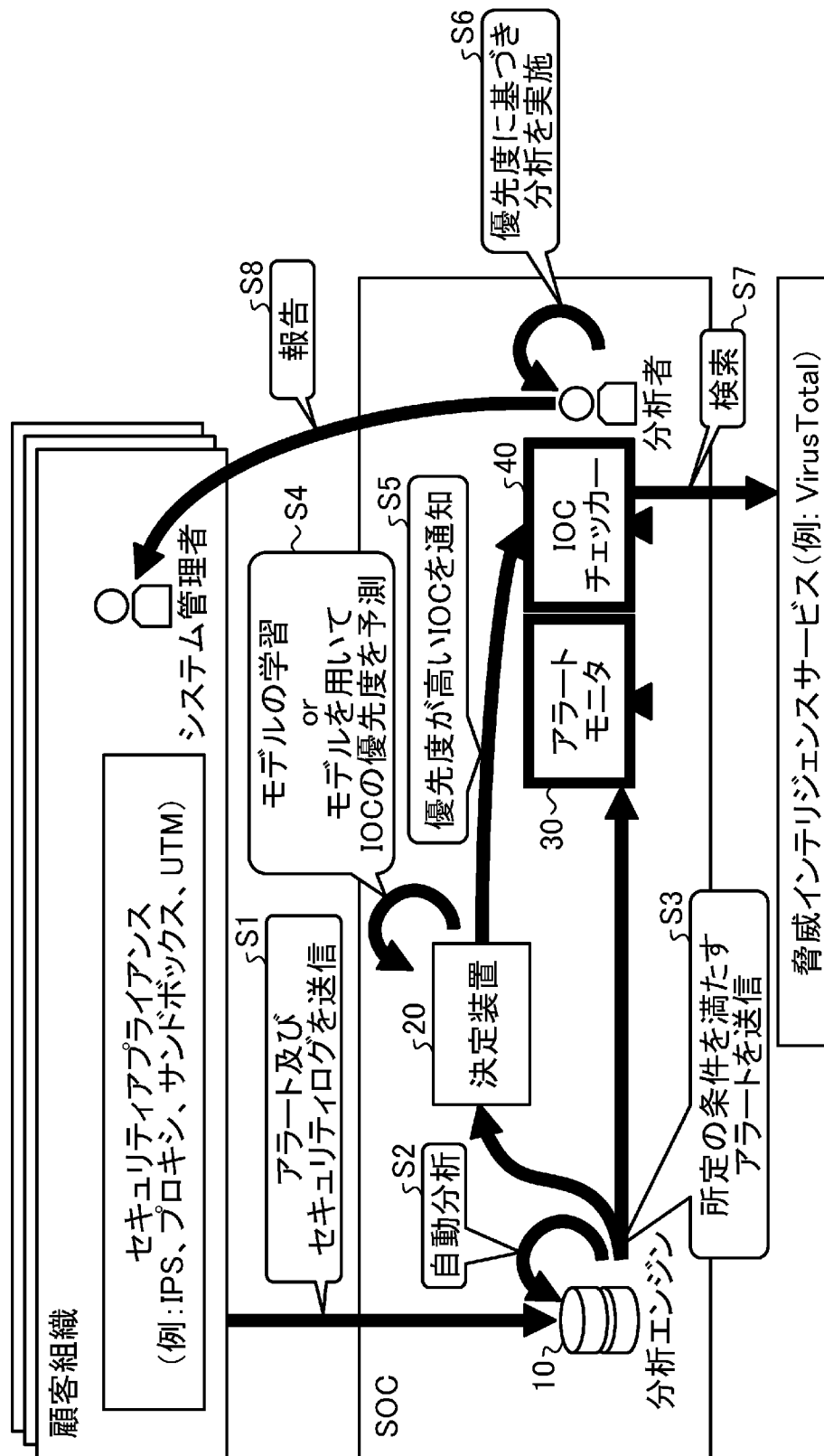
請求の範囲

- [請求項1] 決定装置によって実行される決定方法であって、
サイバーセキュリティに関する情報に含まれるＩＯＣ（Indicator of Compromise）から特徴情報を抽出する特徴情報抽出工程と、
前記ＩＯＣのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与するラベル付与工程と、
前記特徴情報抽出工程によって抽出された特徴情報及び前記ラベル付与工程によって付与されたラベルを組み合わせた学習データを用いて、ＩＯＣの特徴情報からラベルを出力するモデルの学習を行う学習工程と、
を含むことを特徴とする決定方法。
- [請求項2] 前記ラベル付与工程は、前記ＩＯＣのうち、関連するアラートに対して一定期間内に発生した手動調査の回数が所定値以上であるＩＯＣについて、優先度が高いことを示すラベルを付与し、前記手動調査の回数が前記所定値未満であるＩＯＣについて、優先度が低いことを示すラベルを付与することを特徴とする請求項１に記載の決定方法。
- [請求項3] 前記ラベル付与工程は、前記ＩＯＣのうち、関連するアラートに対して一定期間内に発生した手動調査に要した時間が所定値以上であるＩＯＣについて、優先度が高いことを示すラベルを付与し、前記時間が前記所定値未満であるＩＯＣについて、優先度が低いことを示すラベルを付与することを特徴とする請求項１に記載の決定方法。
- [請求項4] 前記学習工程による学習が行われたモデルを用いて、ＩＯＣの特徴情報からラベルを予測する予測工程をさらに含むことを特徴とする請求項１から３のいずれか１項に記載の決定方法。
- [請求項5] 前記予測工程において、優先度が高いことを示すラベルが予測されたＩＯＣに関する情報を通知する通知工程をさらに含むことを特徴とする請求項４に記載の決定方法。

[請求項6] サイバーセキュリティに関する情報に含まれるＩＯＣ（Indicator of Compromise）から特徴情報を抽出する特徴情報抽出部と、
前記ＩＯＣのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与するラベル付与部と、
前記特徴情報抽出部によって抽出された特徴情報及び前記ラベル付与部によって付与されたラベルを組み合わせた学習データを用いて、
ＩＯＣの特徴情報からラベルを出力するモデルの学習を行う学習部と、
、
を有することを特徴とする決定装置。

[請求項7] コンピュータに、
サイバーセキュリティに関する情報に含まれるＩＯＣ（Indicator of Compromise）から特徴情報を抽出する特徴情報抽出手順と、
前記ＩＯＣのそれぞれについて、関連するアラートの対応に要した稼働量の実績に応じたラベルを付与するラベル付与手順と、
前記特徴情報抽出手順によって抽出された特徴情報及び前記ラベル付与手順によって付与されたラベルを組み合わせた学習データを用いて、
ＩＯＣの特徴情報からラベルを出力するモデルの学習を行う学習手順と、
を実行させることを特徴とする決定プログラム。

[図1]



[図2]

5 30

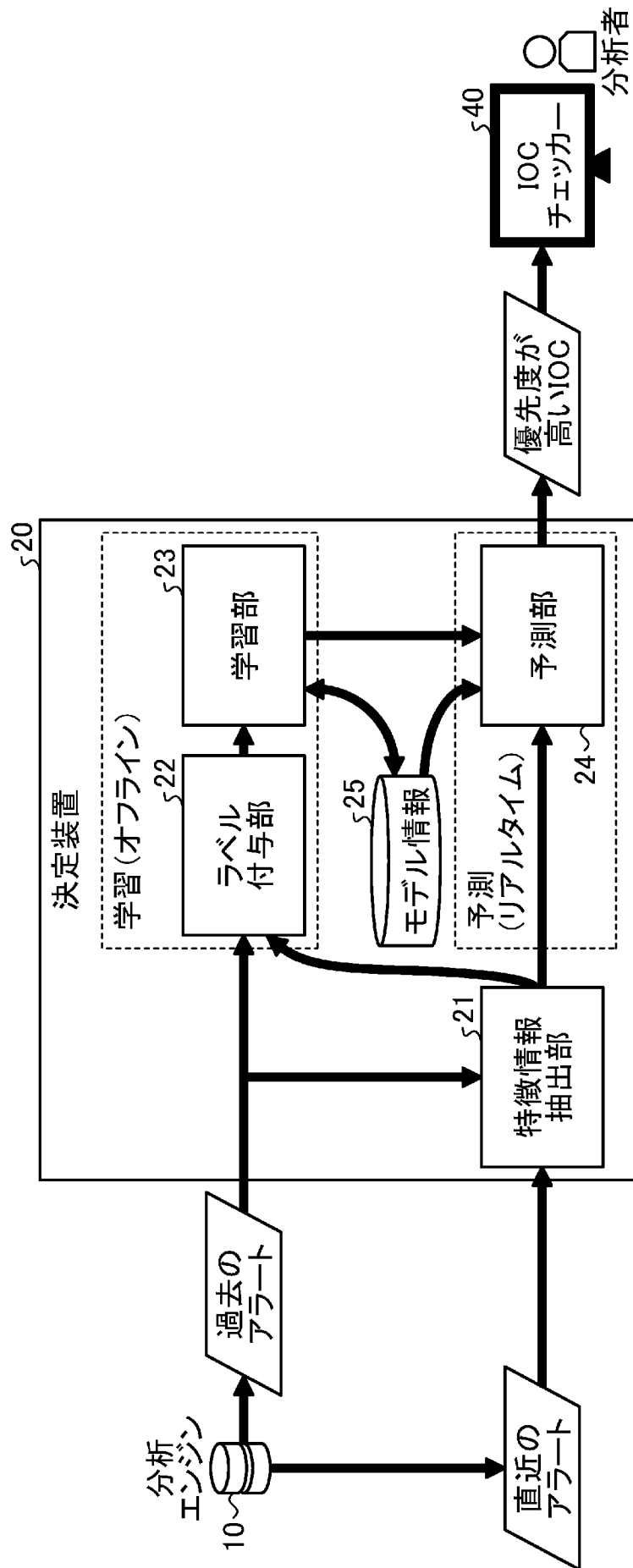
Data	Customer	Device	Alert Name	...
2020-06-01 10:04:00	Foo Corp.	Sandbox	Malware Callback	...
2020-06-01 10:05:30	Bar Inc.	Proxy	Phishing Website	...
2020-06-01 10:06:50	Baz Ltd.	UTM	Suspicious DNS Query	...
...	...	...	...	...

[図3]

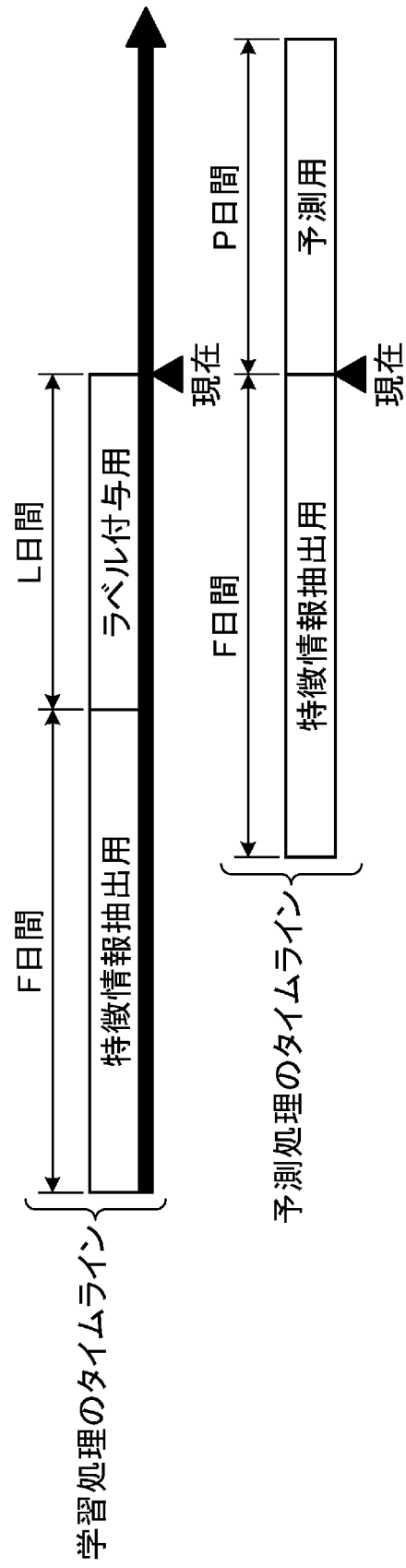
5 40

Domain Name	Status	SOC Last Decision	# Detection in TI	...
malware.example	Completed	Report Sent	20/80	...
phishing.example	New	Undecided	10/80	...
example.com	Pending	Undecided	2/80	...
...	...	...	...	...

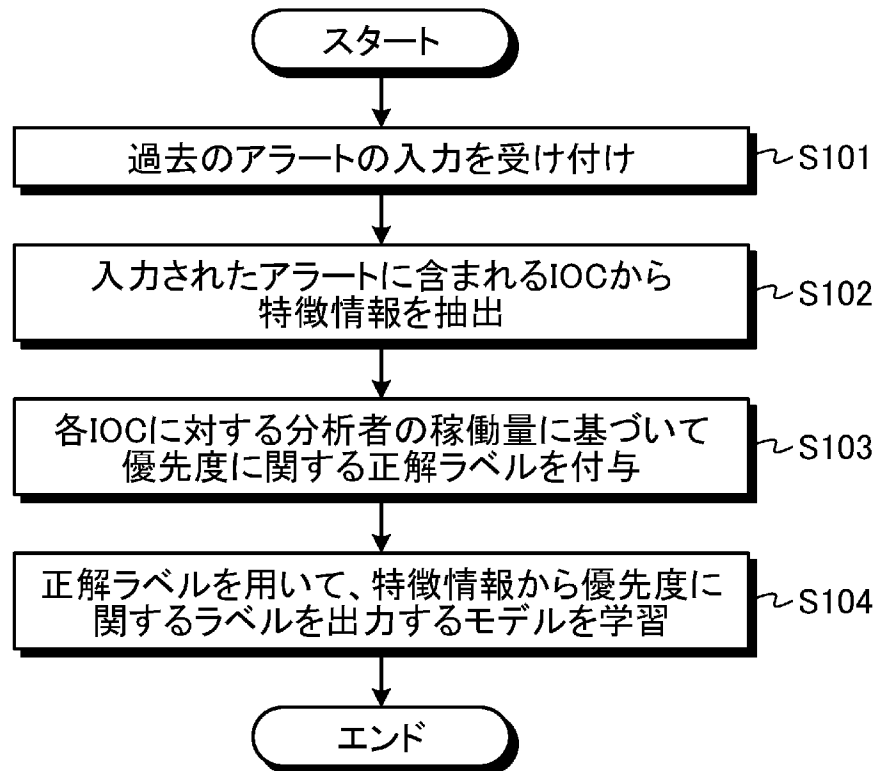
[図4]



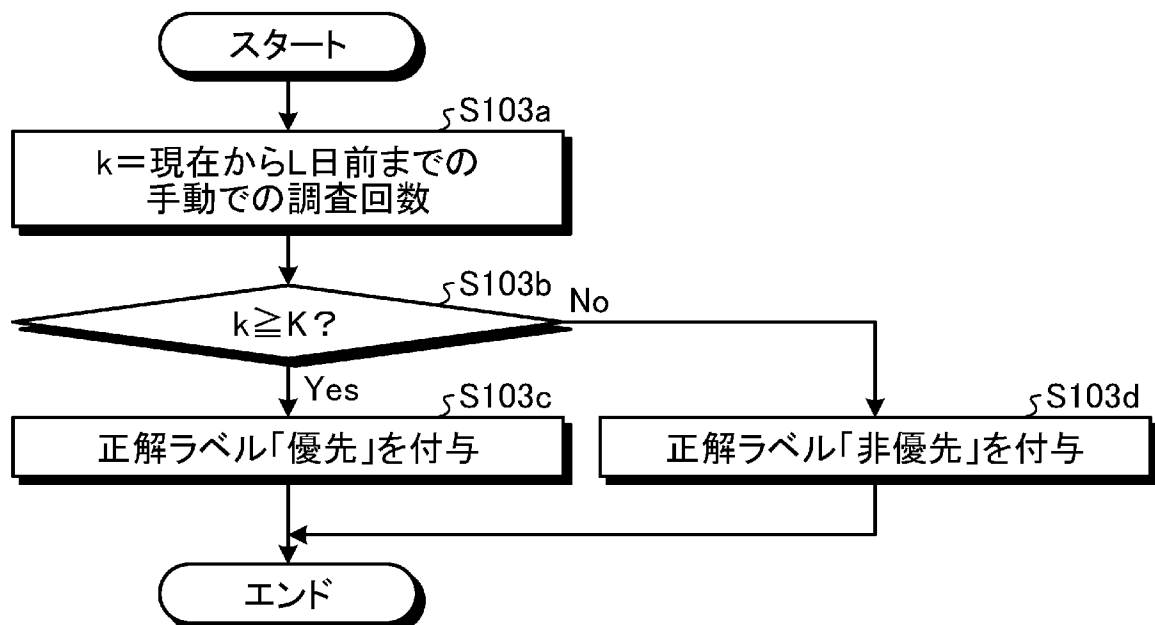
[図5]



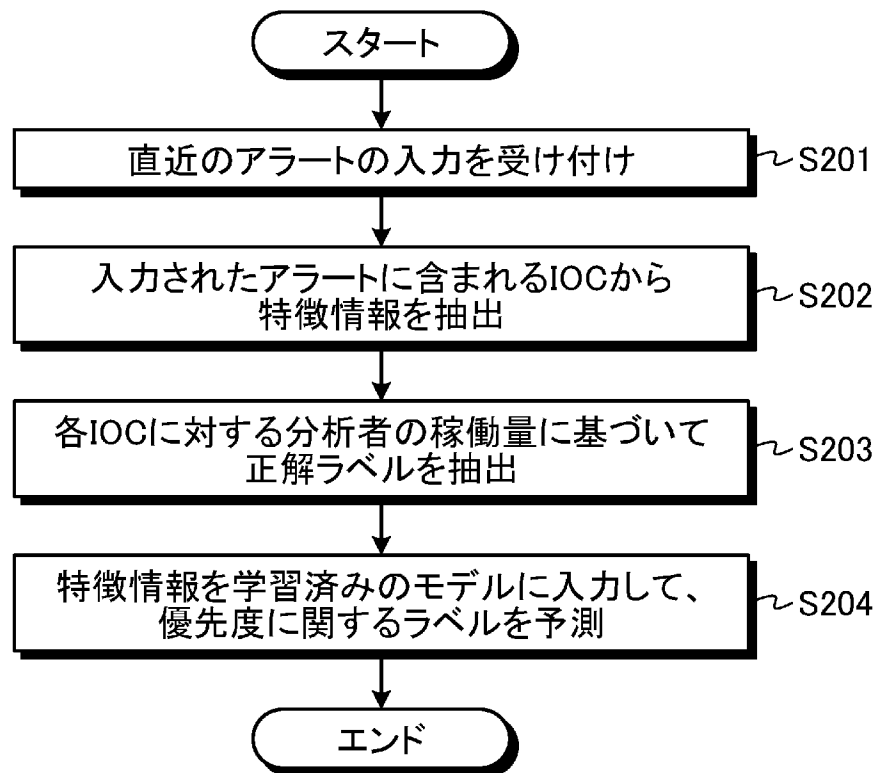
[図6]



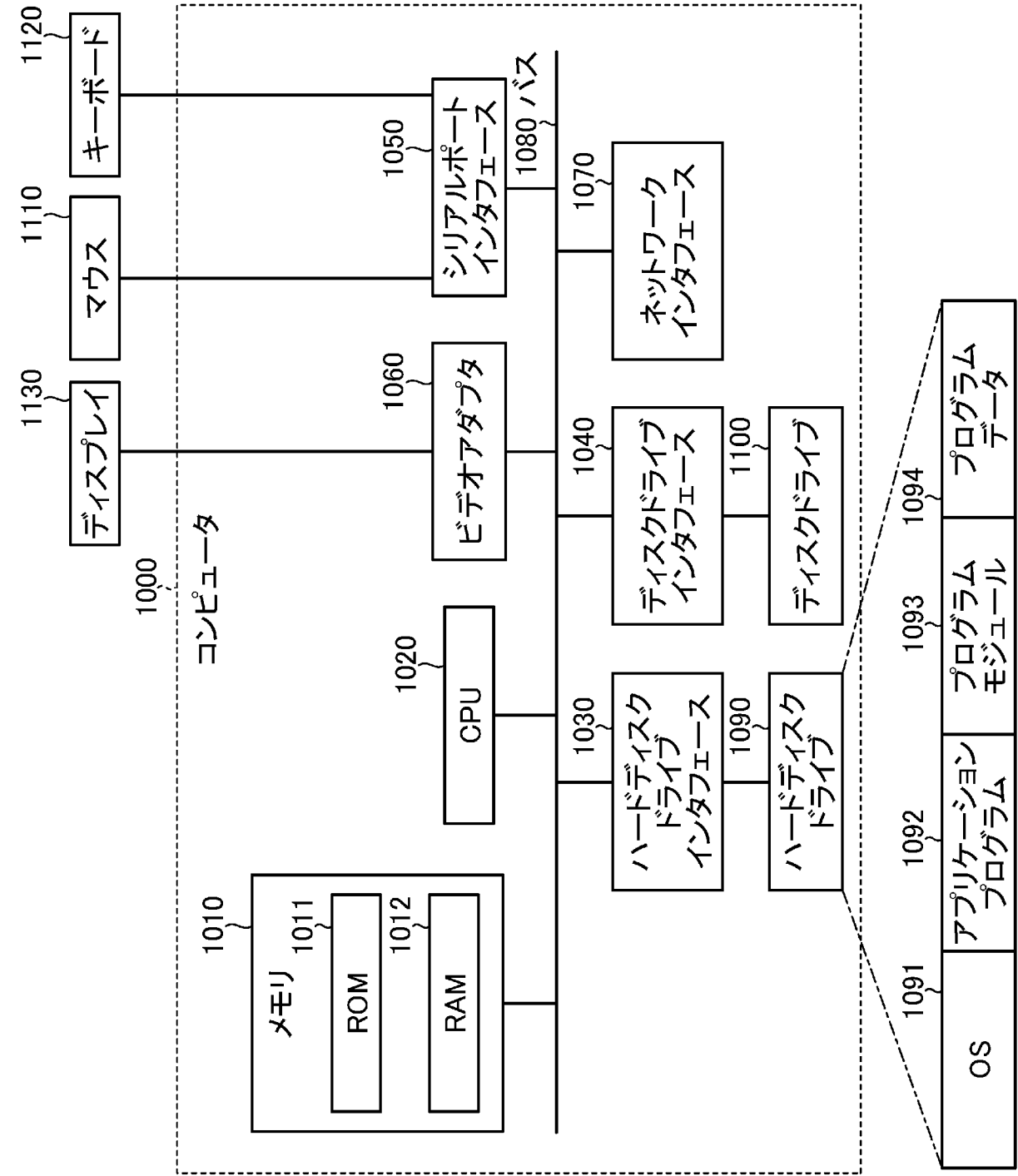
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/018118

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/55(2013.01)i

FI: G06F21/55340

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)

Int.Cl. 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 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

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	WO 2018/235252 A1 (NEC CORP.) 27 December 2018 (2018-12-27), paragraphs [0027], [0028], [0076], [0080], [0081], [0091], [0092], [0095], [0096], [0101], [0107], [0108], [0148], [0152], fig. 9, 10, 17	1-7
A	WO 2016/117132 A1 (UBIC KK) 28 July 2016 (2016-07-28), paragraphs [0033], [0035], [0060], [0073], [0104], fig. 1	1-7
A	US 2019/0230098 A1 (T-MOBILE USA, INC.) 25 July 2019 (2019-07-25), paragraph [0060]	1-7
A	JP 2018-521430 A (HASAN, S. K.) 02 August 2018 (2018-08-02), paragraph [0060]	1-7



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

14 June 2021

Date of mailing of the international search report

22 June 2021

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/JP2021/018118

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2020/148934 A1 (HITACHI, LTD.) 23 July 2020 (2020-07-23), paragraphs [0003], [0014], [0022], fig. 1	1 - 7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/018118

WO 2018/235252 A1 27 December 2018	US 2020/0184072 A1 paragraphs [0055], [0056], [0104], [0108], [0109], [0119], [0120], [0123], [0124], [0129], [0135], [0136], [0176], [0180], fig. 9, 10, 17
WO 2016/117132 A1 28 July 2016	(Family: none)
US 2019/0230098 A1 25 July 2019	(Family: none)
JP 2018-521430 A 02 August 2018	WO 2017/014823 A2 paragraph [0058]
WO 2020/148934 A1 23 July 2020	JP 2020-113216 A

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 FI: G06F21/55 340														
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 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
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	WO 2018/235252 A1（日本電気株式会社）27.12.2018（2018 - 12 - 27） 段落[0027]-[0028], [0076], [0080]-[0081], [0091]-[0092], [0095]-[0096], [0101], [0107]-[0108], [0148], [0152], 図9-10, 17	1-7												
A	WO 2016/117132 A1（株式会社U B I C）28.07.2016（2016 - 07 - 28） 段落[0033], [0035], [0060], [0073], [0104], 図1	1-7												
A	US 2019/0230098 A1（T-Mobile USA, Inc.）25.07.2019（2019 - 07 - 25） 段落[0060]	1-7												
A	JP 2018-521430 A（ハサン・シェド・カムラン）02.08.2018（2018 - 08 - 02） 段落[0060]	1-7												
A	WO 2020/148934 A1（株式会社日立製作所）23.07.2020（2020 - 07 - 23） 段落[0003], [0014], [0022], 図1	1-7												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 14.06.2021	国際調査報告の発送日 22.06.2021													
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） 小林 秀和 5S 3449 電話番号 03-3581-1101 内線 3546													

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/JP2021/018118

引用文献			公表日	パテントファミリー文献	公表日
WO	2018/235252	A1	27.12.2018	US 2020/0184072 A1 段落[0055]-[0056], [0104], [0108]-[0109], [0119]-[0120], [0123]- [0124], [0129], [0135]- [0136], [0176], [0180], 図9-10, 17	
WO	2016/117132	A1	28.07.2016	(ファミリーなし)	
US	2019/0230098	A1	25.07.2019	(ファミリーなし)	
JP	2018-521430	A	02.08.2018	WO 2017/014823 A2 段落[0058]	
WO	2020/148934	A1	23.07.2020	JP 2020-113216 A	