(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12月22日(22.12.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/264239 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2021/022590

(22) 国際出願日： 2021年6月14日(14.06.2021)

(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).

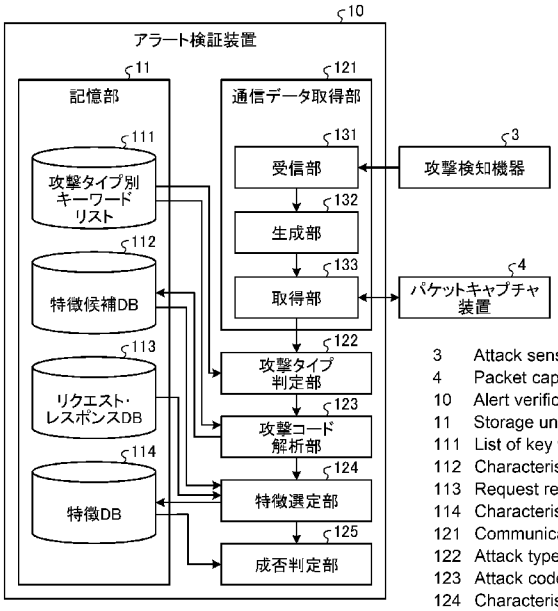
(72) 発明者: 宮本 国雄 (**MIYAMOTO, Kunio**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 岩城 悠太 (**IWAKI, Yuta**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 鐘本 楊(**KANEMOTO, Yo**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 黒木 琴海(**KUROKI, Kotomi**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 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,

(54) **Title:** ALERT VERIFICATION DEVICE, ALERT VERIFICATION METHOD, AND ALERT VERIFICATION PROGRAM

(54) 発明の名称： アラート検証装置、アラート検証方法及びアラート検証プログラム



3 Attack sensing apparatus
4 Packet capture device
10 Alert verification device
11 Storage unit
111 List of key words by attack type
112 Characteristics candidate database
113 Request response database
114 Characteristics database
121 Communication data acquisition unit
122 Attack type determination unit
123 Attack code analysis unit
124 Characteristics selection unit
125 Feasibility determination unit
131 Receiving unit
132 Generation unit
133 Acquisition unit

(57) **Abstract:** In the present invention, a receiving unit (131) receives an alert transmitted from an attack sensing apparatus (3) that senses attacks on a device to be monitored. A generation unit (132) generates, on the basis of the alert received by the receiving unit (131), acquisition conditions for communication data to be acquired. The acquisition unit (133) acquires the communication data that matches the acquisition conditions generated by the generation unit (132) from a packet capture device (4) that retains data transmitted from and received by the device to be monitored. A success/failure

WO 2022/264239 A1

[続葉有]

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, 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：

— 国際調査報告（条約第21条(3)）

determination unit (125) determines the feasibility of an attack on the basis of the communication data acquired by the acquisition unit (133).

(57) 要約：受信部（１３１）は、監視対象装置に対する攻撃を検知する攻撃検知機器（３）から送信されたアラートを受信する。生成部（１３２）は、受信部（１３１）により受信されたアラートを基に、取得する通信データの取得条件を生成する。取得部（１３３）は、監視対象装置により送受信されたデータを保持するパケットキャプチャ装置（４）から、生成部（１３２）により生成された取得条件にマッチする前記通信データを取得する。成否判定部（１２５）は、取得部（１３３）により取得された通信データを基に攻撃の成否を判定する。

明　細　書

発明の名称 ：

アラート検証装置、アラート検証方法及びアラート検証プログラム

技術分野

[0001] 本発明は、アラート検証装置、アラート検証方法及びアラート検証プログラムに関する。

背景技術

[0002] Ｗｅｂアプリケーションは、多くのサービスで利用される一方で、不特定多数からアクセス可能である。そのため、Ｗｅｂアプリケーションは、攻撃にも晒されやすいという性質を有する。Ｗｅｂアプリケーションへの攻撃は、日々大量に発生しており、セキュリティ機器などによって検知される。

[0003] 攻撃検知技術としては、ＷＡＦ（Web Application Firewall）や、ＮＩＤＳ（Network-based Intrusion Detection System）といった技術が存在する。これらは、事前に保持する攻撃コードの特徴とマッチングする通信をネットワーク通信の中から攻撃として検知する技術である。ただし、これらの技術では、攻撃を検知することは可能であるが、検知した攻撃が成功したか否かを自動で判定することは困難であり、大量のアラートを人手で調査することで攻撃の成否が判明する。

[0004] そのため、攻撃の成否を検証する様々な技術が研究されている。例えば、ファイルアクセスやＤＢ（Data Base）アクセスといったサーバ内の特徴などを用いる異常検知技術を応用して攻撃を検知し且つ異常を検知した際は攻撃が成功したことを示すＨＩＤＳ（Host-based Intrusion Detection System）と呼ばれる技術がある。また、攻撃が成功した際の状態遷移を定義し、攻撃によってシステムが定義された状態遷移を行うと攻撃が成功したとして検知するStateful ＩＤＳと呼ばれる技術がある（A Stateful Intrusion Detection System for World-WideWeb Servers, ACSAC, 2003、Enhancing Byte-Level Network Intrusion Detection Signatures with C

ontext, CCS, 2003、Verify Results of Network Intrusion Alerts Using Lightweight Protocol Analysis, ACSAC, 2005参照）。また、攻撃が対処とするアプリケーション及びバーションが利用されているかを事前にチェックし、利用されていると判定した場合、攻撃が成功したとして検知する、脆弱性情報との相関部積と呼ばれる手法がある（Alert Verification Determining the Success of Intrusion Attempts, DIMVA, 2004参照）。さらに、攻撃コードのエミュレートを行い、実行時に同じ挙動を観測した場合、攻撃が成功してとして検知する攻撃コードのエミュレーションと呼ばれる技術がある（On Emulation-Based Network Intrusion Detection Systems, RAID, 2014参照）。

[0005] また、攻撃コードによるサーバへの攻撃が成功したか否かを判定する従来技術として以下のような技術が提案されている。１つは、判定した攻撃タイプに応じてサーバへの攻撃のエミュレーションを実施してサーバへの攻撃に成功した場合にレスポンスに現れる特徴を抽出し、サーバからのレスポンスが抽出した特徴を有する場合に攻撃コードによる攻撃が成功したと判定する技術である。他にも、攻撃タイプに応じてサーバへの攻撃のエミュレーションを実施して攻撃が成功した場合のレスポンスの特徴を抽出し、攻撃リクエスト以降の複数のレスポンスのうち少なくとも１つが抽出した特徴を有する場合に、攻撃が成功したと判定する技術が存在する。

[0006] これらの従来技術における処理は、例えば以下のように実行される。まず、リクエストは攻撃か否かが判定される。リクエストが攻撃でなければ、攻撃成否判定不能と判定される。また、リクエストが攻撃の場合、攻撃タイプの判定処理を行い、攻撃タイプが判定可能か否かの判定が行われる。攻撃タイプが判定不能であれば、攻撃成否判定不能と判定される。これに対して、攻撃タイプが判定可能の場合、攻撃コードの解析が行われ、レスポンスに表れる特徴の中からその攻撃コードに対応する特徴の選定処理が行われる。次に、選択された特徴が存在するか否かが判定される。選択された特徴が存在しなければ、攻撃成否判定不能と判定される。これに対して、選択された特

徴が存在する場合、特徴の検査処理が行われ、攻撃が成功したか否かが判定され、判定結果により攻撃の成否が通知される。

[0007] 以上のような攻撃の成否判定処理を行う装置は、例えば、攻撃検知部、攻撃タイプ判定部、攻撃コード解析部、特徴選定部及び特徴検査部を備える。攻撃検知部は、リクエストが攻撃か否かの検知を行う。攻撃タイプ判定部は、予め保持するキーワードリストを用いて、攻撃コードのプログラミング言語や攻撃の手法から攻撃のタイプを判定する。攻撃コード解析部は、予め保持するキーワードリスト及び特徴候補ＤＢを用いて、攻撃タイプに応じて攻撃コードを実行できるエミュレータを用意し、そのエミュレータで攻撃コードを実行する。特徴選定部は、レスポンスの情報が格納されたレスポンスＤＢ及び攻撃成功時の特徴の情報を格納する特徴ＤＢを用いて、得られた特徴候補から攻撃成功時の特徴として扱うのにふさわしくない特徴を除外する。特徴検査部は、特徴ＤＢを用いて、攻撃コード解析部で得られた攻撃コードが実行された際に出力する特徴が通信などに含まれているか否かを検査する。このような、攻撃コードによるサーバへの攻撃が成功したか否かを判定する技術を以下では、アラート検証技術と呼ぶ。

先行技術文献

特許文献

[0008] 特許文献1：国際公開第２０１９／０１３２６６号

特許文献2：国際公開第２０１９／２２５２１６号

発明の概要

発明が解決しようとする課題

[0009] しかしながら、アラート検証技術には、以下のような問題が存在する。攻撃として検知されていない通信のパケットもアラート検証技術の実施装置でＨＴＴＰリクエスト又はＨＴＴＰレスポンスへのパース処理が行われる。すなわち、アラート検証技術の実施装置では、通信パケットをＨＴＴＰリクエスト又はＨＴＴＰレスポンスへのパース処理が行われ、攻撃通信であるか否

かがＷＡＦなどの攻撃検知機器の情報を用いて判定される。そのため、大量トラフィック環境ではパース処理の負荷が大きくなり、アラート検証技術の処理が大幅に遅延する。この場合、全ての通信パケットが、ＨＴＴＰリクエスト又はＨＴＴＰレスポンスにパースされるが、アラート検証技術での攻撃成否判定の対象となる通信は、攻撃と判定された通信である。

[0010] 本発明は、上記に鑑みてなされたものであって、通信パケットのパース処理を軽減し、攻撃判定処理の処理負荷を低減することを目的とする。

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、受信部は、監視対象装置に対する攻撃を検知する攻撃検知機器から送信されたアラートを受信する。生成部は、前記受信部により受信された前記アラートを基に、取得する通信データの取得条件を生成する。取得部は、前記監視対象装置により送受信されたデータを保持するパケットキャプチャ装置から、前記生成部により生成された前記取得条件にマッチする前記通信データを取得する。成否判定部は、前記取得部により取得された前記通信データを基に前記攻撃の成否を判定する。

発明の効果

[0012] 本発明によれば、通信パケットのパース処理を軽減し、攻撃判定処理の処理負荷を低減することができる。

図面の簡単な説明

[0013] [図1]図１は、アラート検証装置が配置されたシステムの概略構成図である。

[図2]図２は、第１の実施形態に係る判定装置のブロック図である。

[図3]図３は、攻撃タイプ別キーワードリストの一例を示す図である。

[図4]図４は、第１の実施形態に係る判定装置による攻撃成否の判定処理のフローチャートある。

[図5]図５は、第２の実施形態におけるセカンドオーダ攻撃を示す図である。

[図6]図６は、第３の実施形態における複数のセッションにまたがる攻撃を示す図である。

[図7]図７は、第４の実施形態におけるログインバイパス攻撃を示す図である。

[図8]図８は、第６の実施形態に係るシステム構成図である。

[図9]図９は、攻撃成否判定処理のためのアラート検証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、本願の開示するアラート検証装置、アラート検証方法及びアラート検証プログラムの一実施形態を図面に基づいて詳細に説明する。なお、以下の実施形態により本願の開示するアラート検証装置、アラート検証方法及びアラート検証プログラムが限定されるものではない。

[0015] ［第１の実施形態］

［概要］

図１は、アラート検証装置が配置されたシステムの概略構成図である。図１に示すように、インターネットからＷｅｂサーバ１に繋がる通信経路上に、通信複製機器２及び攻撃検知機器３が配置される。さらに、通信複製機器２には、パケットキャプチャ装置４が接続される。そして、アラート検証装置１０は、パケットキャプチャ装置４及びＷｅｂサーバ１に繋がる通信経路上に配置された攻撃検知機器３に接続される。このようにアラート検証装置１０がＷｅｂサーバ１に繋がる経路とは異なる経路で攻撃検知機器３に接続された構成は、タップ構成と呼ばれる。

[0016] Ｗｅｂサーバ１で動作するＷｅｂアプリケーションは、インターネットに接続されたＰＣなどとの間でリクエストの受信及びレスポンスの送信、並びに、リクエストの送信及びレスポンスの受信といった通信を行う。本実施形態では、Ｗｅｂアプリケーションに対する通信について説明するが、以下の説明では、Ｗｅｂサーバ１で動作するＷｅｂアプリケーションに対する通信を単にＷｅｂサーバ１に対する通信と呼ぶ。Ｗｅｂサーバ１に対するインターネットからのリクエストには、攻撃リクエストが含まれる場合がある。

[0017] 通信複製機器２は、Ｗｅｂサーバ１へのトラフィックを複製する。言い換

えれば、通信複製機器２は、インターネットに接続されたＰＣなどとＷｅｂサーバ１の間で送受信される通信データを受信して複製を生成する。そして、通信複製機器２は、複製した通信データをパケットキャプチャ装置４へ送信する。

[0018] パケットキャプチャ装置４は、通信複製機器２で生成されたインターネットに接続されたＰＣなどとＷｅｂサーバ１との間で送受信される通信データの複製を受信する。そして、パケットキャプチャ装置４は、取得した通信データを蓄積して保持する。

[0019] 攻撃検知機器３は、例えばＷＡＦなどの技術を用いてネットワーク通信の中から攻撃リクエストを検知する機能を備えた装置である。攻撃検知機器３は、インターネットからＷｅｂサーバ１へ送信される攻撃リクエストを受信すると、この攻撃リクエストを示すアラートを生成してアラート検証装置１０へ送信する。アラートには、例えば、攻撃リクエストの送信元のＩＰ（Internet Protocol）アドレスやポート番号及びＵＲＬ（Uniform Resource Locator）のパス部などが含まれる。

[0020] アラート検証装置１０は、攻撃が検知された場合、攻撃検知を示すアラートを攻撃検知機器３から受信する。そして、アラート検証装置１０は、アラートと紐づく通信データをパケットキャプチャ装置４から取得する。そして、アラート検証装置１０は、取得した通信データから特定した攻撃タイプ（例えば、ＯＳ（Operating System）コマンドを悪用する攻撃タイプ）に応じたエミュレータで攻撃コードを実行し、実行の結果をＷｅｂサーバ１から出力される情報を攻撃の成功時に出力される特徴として抽出する。

[0021] その後、アラート検証装置１０は、Ｗｅｂサーバ１からのレスポンスを検査し、レスポンスに、抽出した特徴が含まれている場合、攻撃は成功したと判定する。ここで、アラート検証装置１０では、Ｗｅｂサーバ１に対する攻撃リクエストがあった際、抽出された特徴を攻撃リクエストに対するレスポンスだけでなく、それ以後のレスポンスであって、所定の条件に合致した全てのレスポンスを検査対象としてもよい。

[0022] このように、アラート検証装置１０は、攻撃成否判定を行う対象とする通信データをパケットキャプチャ装置４から取得し、その他の通信データの取得を抑制することで、通信パケットのパース処理負荷を低減できる。

[0023] ［判定装置の構成］

図２は、第１の実施形態に係る判定装置のブロック図である。図２に示すように、本実施形態に係るアラート検証装置１０は、記憶部１１、通信データ取得部１２１、攻撃タイプ判定部１２２、攻撃コード解析部１２３、特徴選定部１２４及び成否判定部１２５を備える。記憶部１１は、攻撃タイプ別キーワードリスト１１１、特徴候補ＤＢ１１２、リクエスト・レスポンスＤＢ１１３及び特徴ＤＢ１１４を格納する。

[0024] 攻撃タイプ別キーワードリスト１１１は、攻撃タイプ毎に、各攻撃タイプの攻撃コードに含まれるキーワードを示した情報である。図３は、攻撃タイプ別キーワードリストの一例を示す図である。この攻撃タイプ別キーワードリスト１１１は、攻撃タイプ判定部１２２が、攻撃コードに含まれるキーワードから攻撃タイプを判定する際に参照される。

[0025] なお、攻撃タイプは、例えば、Ａ．ＯＳコマンドを悪用する攻撃タイプ、Ｂ．プログラムコードを悪用する攻撃タイプ、Ｃ．ＤＢの機能であるＳＱＬ（Structured Query Language）コマンドを悪用する攻撃タイプ（例えば、ＳＱＬ Injection等）、Ｄ．ＨＴＴＰ（Hyper Text Transfer Protocol）レスポンスを悪用する攻撃タイプ（例えば、ＸＳＳ（Cross Site Scripting）、Header Injection等）、Ｅ．ファイル操作を悪用する攻撃タイプ（例えば、ディレクトリトラバーサル等）の５つのタイプに分けられる。

[0026] なお、図３に例示するように、上記のＡ．の攻撃タイプではＯＳコマンドの名前をキーワードとする。また、Ｂ．の攻撃タイプではプログラミング言語で利用する固有表現をキーワードとする。例えば、PHP（Hypertext Preprocessor）であればprint_r、var_dump、base64_decode等のPHPに固有の関数あるいはPHPの固有表現等（$_GET、$_POST等）をキーワードとする。その他のプログラミング言語（Java（登録商標）、Perl、Ruby、Python等）におい

ても同等である。そのため、Ｂ．の攻撃タイプではプログラミング言語毎に攻撃タイプ別キーワードリスト１１１を保持する。このとき、どのプログラミング言語に当たるかの情報は、例えば、図３に示すように、サブ攻撃タイプとして保持する。

[0027] また、Ｃ．の攻撃タイプではＳＱＬコマンドの名前（select、update、insert、drop等）やＤＢアクセスの際の特徴的な表現をキーワードとする。例えば、ＭｙＳＱＬの場合、information_schema、@@version、mysql等である。さらに、Ｄ．の攻撃タイプではＨＴＭＬ（HyperText Markup Language）やJavascript（登録商標）で利用される固有表現（alert、onclick等）をキーワードとする。また、Ｅ．の攻撃タイプではディレクトリトラバーサル攻撃で利用される固有表現（../等）をキーワードとする。

[0028] 図２に戻って説明を続ける。特徴候補ＤＢ１１２は、攻撃コード解析部１２３よる攻撃コードのエミュレーションの結果、エミュレータから出力された情報（特徴候補）を記憶する。

[0029] リクエスト・レスポンスＤＢ１１３は、Ｗｅｂサーバ１への様々なリクエスト及びＷｅｂサーバ１からの様々なレスポンスを記憶する。なお、このリクエスト・レスポンスＤＢ１１３は、特徴選定部１２４が、特徴候補から、通常のレスポンスに頻繁に登場する語（普遍的な語）を除外する際に参照されるための情報も記憶してもよい。この場合には、リクエスト・レスポンスＤＢ１１３は、例えば、攻撃が来ないことが保証されている試験環境でレスポンスを取得して作成される。あるいは、攻撃検知機器３で検知されなかったリクエストに対応するレスポンスを用いて作成される。

[0030] 特徴ＤＢ１１４は、攻撃コードによる攻撃の成功時にＷｅｂサーバ１から出力される特徴を記憶する。具体的には、特徴ＤＢ１１４は、特徴候補ＤＢ１１２に記憶される特徴候補の中から特徴選定部１２４により選定された特徴を記憶する。この特徴ＤＢ１１４に記憶される特徴は、成否判定部１２５が、Ｗｅｂサーバ１からのレスポンスに基づき、攻撃が成功したか否かを判定する際に参照される。

[0031] 通信データ取得部１２１は、以下に示すアラート受信処理を実行する。通信データ取得部１２１は、攻撃検知機器３により発行されたアラートを受信してそのアラートに紐づく通信データの取得条件を生成するアラート受信処理を実行する。次に、通信データ取得部１２１は、生成した取得条件に応じた通信データをパケットキャプチャ装置４から取得する通信データ取得処理を実行する。より詳しくは、通信データ取得部１２１は、受信部１３１、生成部１３２及び取得部１３３を有する。

[0032] 受信部１３１は、攻撃検知機器３によりＷｅｂサーバ１への攻撃が検知された場合、その攻撃検知を通知するアラートを攻撃検知機器３から受信する。すなわち、受信部１３１は、監視対象装置であるＷｅｂサーバ１に対する攻撃を検知してアラートを発生する攻撃検知機器３から送信されたアラートを受信する。そして、受信部１３１は、受信したアラートを生成部１３２へ出力する。

[0033] 生成部１３２は、攻撃検知機器３により発行されたアラートの入力を受信部１３１から受ける。次に、生成部１３２は、アラートに紐づく通信データを特定可能な情報をアラートから抽出する。例えば、生成部１３２は、アラートに含まれる、攻撃リクエストの送信元のＩＰアドレス及びポート番号、並びに、ＵＲＬのパス部などの一部もしくは全てを抽出する。

[0034] 次に、生成部１３２は、アラートに紐づく通信データを特定可能な情報を用いて通信データの取得条件を生成する。例えば、生成部１３２は、アラートに含まれる、攻撃リクエストの送信元のＩＰアドレス及びポート番号、並びに、ＵＲＬのパス部などの一部もしくは全てを使用して、それらに関連する通信データを取得するための取得条件を生成する。その後、生成部１３２は、生成した取得条件を取得部１３３へ出力する。すなわち、生成部１３２は、受信部１３１により受信されたアラートを基に、取得する通信データの取得条件を生成する。

[0035] 取得部１３３は、生成部１３２により生成された取得条件をパケットキャプチャ装置４に送信して、取得条件にマッチする通信データの取得要求を行

う。そして、取得部１３３は、送信した取得条件にマッチする通信データをパケットキャプチャ装置４から受信する。すなわち、取得部１３３は、監視対象装置であるＷｅｂサーバ１により送受信されたデータを保持するパケットキャプチャ装置４から、生成部１３２により生成された取得条件にマッチする通信データを取得する。その後、取得部１３３は、取得条件にマッチする通信データ、すなわち、アラートに紐づく通信データを攻撃タイプ判定部１２２へ出力する。

[0036] 攻撃タイプ判定部１２２は、アラートに紐づく通信データの入力を通信データ取得部１２１の取得部１３３から受ける。そして、攻撃タイプ判定部１２２は、取得した通信データに含まれる攻撃コードを抽出する。その後、攻撃タイプ判定部１２２は、抽出した攻撃コードを用いて攻撃タイプの判定を行う。

[0037] ここで、攻撃タイプ判定部１２２は、例えば、Ｗｅｂサーバ１に対する攻撃の中でも特に重要と思われる、上記のＡ．～Ｅ．の攻撃タイプの５つの攻撃タイプのいずれであるかを判定する。具体的には、攻撃タイプ判定部１２２は、攻撃コードに含まれるキーワードが、攻撃タイプ別キーワードリスト１１１に示されるどの攻撃タイプのキーワードとマッチするかにより判定を行う。

[0038] 例えば、攻撃タイプ判定部１２２は、攻撃タイプ別キーワードリスト１１１を参照して、攻撃コードに「cat」が含まれていれば、当該攻撃コードをＡ．の攻撃タイプ（ＯＳコマンドを悪用する攻撃タイプ）と判定する。また、攻撃タイプ判定部１２２は、攻撃コードに「print_r」が含まれていれば、当該攻撃コードをＢ．の攻撃タイプ（プログラムコードを悪用する攻撃タイプ）であり、その中でもphpを用いた攻撃タイプであると判定する。

[0039] なお、攻撃タイプ判定部１２２は、攻撃コードが、攻撃タイプ別キーワードリスト１１１に示される複数の攻撃タイプのキーワードとマッチした場合、予め決められた条件にしたがって攻撃タイプの判定を行う。例えば、攻撃タイプ判定部１２２は、攻撃コードの最初にあたる攻撃コード内で最も左の

位置に出現したキーワードの攻撃タイプであると判定する。

[0040] 一例を挙げると、攻撃コードが「;php -e “$i=123456789;var_dump($1)”;」の場合、攻撃タイプ別キーワードリスト１１１において、Ａ．の攻撃タイプのキーワードである「php」と、Ｂ．の攻撃タイプのキーワードである「var_dump」とが出現する。このような場合、攻撃タイプ判定部１２２は、上記の攻撃コードにおいて「php」の方が「var_dump」よりも初めに出現しているので、Ａ．の攻撃タイプと判定する。

[0041] なお、攻撃タイプ判定部１２２は、攻撃タイプ別キーワードリスト１１１を参照して、攻撃コードがどの攻撃タイプともマッチしなかった場合は判定不可とする。その後、攻撃タイプ判定部１２２は、攻撃リクエストに含まれる攻撃コード及びその攻撃コードの攻撃タイプを攻撃コード解析部１２３に通知する。

[0042] 攻撃コード解析部１２３は、攻撃コードについてエミュレータを用いた動的解析を行うことにより、当該攻撃コードを実行した際にＷｅｂサーバ１からのレスポンスに現れる特徴を抽出する。

[0043] 具体的には、攻撃コード解析部１２３は、攻撃タイプ判定部１２２で判定された攻撃コードの攻撃タイプに応じたエミュレータを用いて、その攻撃コードによるＷｅｂサーバ１への攻撃のエミュレーションを実施する。そして、攻撃コード解析部１２３は、攻撃コードのエミュレーションにおいて攻撃に対するレスポンスに現れる出力を、攻撃の成功時に現れる特徴候補として抽出する。

[0044] なお、上記の各攻撃タイプに応じたエミュレータは、例えば、デバッガやインタープリタを応用して事前に作成され、攻撃コード解析部１２３は、事前作成されたエミュレータから、攻撃タイプに応じたエミュレータを選択する。

[0045] 次に、攻撃コード解析部１２３は、例えば、以下のようにして攻撃コードを実行した際のリクエストに対するレスポンスに現れる特徴を抽出する。

[0046] 例えば、攻撃コードの攻撃タイプがＡ．ＯＳコマンドを悪用する攻撃タイ

プである場合、攻撃コード解析部１２３は、ＯＳコマンドを実行できる環境を用いて、当該攻撃コードをコマンドとして実行する。ＯＳコマンドを実行できる環境として、例えば、Windows（登録商標）のコマンドプロンプト、Linux（登録商標）のbash、あるいはコマンドをエミュレートできるエミュレータなどが利用可能である。

[0047] 一例を挙げると、攻撃コード解析部１２３は、「bash -c ”cat /etc/passwd;”」というように、bashコマンドに-c引数で指定したコマンドを実行させる。そして、攻撃コード解析部１２３は、コマンドの実行による標準出力、標準エラー出力の内容を特徴候補として抽出する。例えば、攻撃コード解析部１２３は、攻撃コード「cat /etc/passwd;」に対し、標準出力：「root:*:0:/bin/sh …」、標準エラー出力「なし」という情報を特徴候補として抽出する。

[0048] また、例えば、攻撃コードの攻撃タイプが、Ｂ．プログラムコードを悪用する攻撃タイプである場合、攻撃コード解析部１２３は、プログラミング言語に対して適切なインタープリタあるいはエミュレータを用いて、当該攻撃コードを実行する。

[0049] 一例を挙げると、攻撃コードが、phpコードの場合、攻撃コード解析部１２３は、「php -r ”print(‘123456789’);die();”」というように、phpインタープリタに-r引数で指定したコードを実行させる。また、攻撃コードがpythonコードの場合、攻撃コード解析部１２３は、「python -c “import sys;print 123456789;sys.exit()”」というように、pythonインタープリタに-c引数で指定したコードを実行させる。

[0050] そして、攻撃コード解析部１２３は、コードの実行後、標準出力、標準エラー出力の内容を特徴候補として抽出する。例えば、phpコードの場合、攻撃コード解析部１２３は、攻撃コード「print(‘123456789’);die();」に対し、標準出力「123456789」、標準エラー出力「なし」という情報を特徴候補として抽出する。

[0051] また、攻撃コードの攻撃タイプが、Ｃ．ＳＱＬコマンドを悪用する攻撃タ

イプである場合、攻撃コード解析部１２３は、ＤＢに対してＳＱＬ文を実行できるターミナルあるいはエミュレータを用いて、攻撃コードを実行する。

[0052] なお、ＳＱＬ Injection攻撃によって挿入されるＳＱＬ文（ＳＱＬコマンド）は部分的なものであり、そのままでは実行できない。よって、攻撃コード解析部１２３は、ＳＱＬ文の整形を行う。例えば、攻撃コード解析部１２３は、ＳＱＬ文のSELECT句等より前の部分を消去することにより、ＳＱＬ文をSELECT句等が攻撃コードの最初に現れるように変更する。なお、攻撃コード解析部１２３が、ＳＱＬ文の句のうち、最初に現れるように調整するキーワードは、SELECT句以外の例えばupdate、delete、drop等の句であってもよく、これらの句は攻撃タイプ別キーワードリスト１１１で与えられているものとする。

[0053] 攻撃コード解析部１２３は、整形後のＳＱＬ文の実行による標準出力、標準エラー出力の内容を特徴候補として抽出する。例えば、攻撃コード解析部１２３は、攻撃コード「’ union select 123456789 -」を「select 123456789」に整形する。そして、攻撃コード解析部１２３は、整形後の攻撃コードの実行による標準出力「123456789」、標準エラー出力「なし」という情報を特徴候補として抽出する。

[0054] また、攻撃コードの攻撃タイプが、Ｄ．ＨＴＴＰレスポンスを悪用する攻撃タイプである場合、攻撃コード解析部１２３は、攻撃の性質上、攻撃コードそのものがレスポンスとしてクライアントに送られるため、攻撃コードそのものを特徴候補として抽出する。

[0055] 例えば、攻撃コードがXSSによる攻撃コード「<script>alert(1)</script>」である場合、攻撃コード解析部１２３は、「<script>alert(1)</script>」を特徴候補として抽出する。また、攻撃コードがHeader Injectionによる攻撃コード「¥r¥nSet-Cookie:1234;」である場合、攻撃コード解析部１２３は、「¥r¥nSet-Cookie:1234;」を特徴候補として抽出する。

[0056] また、攻撃コードの攻撃タイプが、Ｅ．ファイル操作を悪用する攻撃タイプ（例えば、ディレクトリトラバーサル等）である場合、攻撃コード解析部

１２３は、攻撃コードに現れるファイル名をＯＳ内で検索し、そのファイル名のファイルの内容を特徴候補として抽出する。

[0057] 例えば、攻撃コードが「../../../../etc/passwd」である場合、攻撃コード解析部１２３は、ＯＳ内から検索された、当該攻撃コードに現れるファイル名のファイルの内容である「root:*:0:/bin/sh …」を特徴候補として抽出する。

[0058] このようにすることで、攻撃コード解析部１２３は、攻撃コードの攻撃タイプに応じたエミュレーションを実行し、当該攻撃コードによる攻撃の成功時の特徴である特徴候補を抽出することができる。そして、攻撃コード解析部１２３は、抽出した特徴候補を特徴候補ＤＢ１１２に記憶させる。

[0059] 特徴選定部１２４は、攻撃コード解析部１２３により抽出された特徴候補の中から、特徴としては不適切な候補を除外する。具体的には、特徴選定部１２４は、特徴候補ＤＢ１１２に記憶される特徴候補の中から、普遍的過ぎて攻撃の成否の判定に利用できない可能性の高い特徴候補を除外する。

[0060] 例えば、特徴選定部１２４は、特徴候補ＤＢ１１２に記憶される特徴候補のうち、文字列長が２以下といった文字列長が極端に短い特徴候補を除外する。さらに、特徴選定部１２４は、通常のレスポンスにも現れる普遍的な語の特徴候補を特徴候補から除外する。そして、特徴選定部１２４は、残った特徴候補を攻撃成功時の特徴として、特徴ＤＢ１１４に記憶させる。

[0061] 例えば、特徴選定部１２４は、特徴候補「1、2、title、page、123456789」の中から、文字列長が所定値（例えば、２）以下の特徴候補「1、2」を除外する。その後、特徴選定部１２４は、文字列長が所定値以下の特徴候補を除外した「title、page、123456789」から普遍的な語を除外する。

[0062] ここでの普遍的な語は、例えば、攻撃でないリクエストに対するレスポンスに含まれる語であるものとする。したがって、特徴選定部１２４は、リクエスト・レスポンスＤＢ１１３を参照して、特徴候補「title、page、123456789」のうち、リクエスト・レスポンスＤＢ１１３における出現回数が１以上の特徴候補を除外する。そして、特徴選定部１２４は、除外の結果の残った

特徴候補を攻撃成功時の特徴として、特徴ＤＢ１１４に記憶させる。

[0063] 一例として、リクエスト・レスポンスＤＢ１１３にレスポンス「<html><title>My blog page</title> Hello world ！ Date : 2017/4/1 </html>」が記憶されている場合で説明する。この場合、特徴選定部１２４は、特徴候補「title、page、123456789」のうち、当該レスポンスに出現する特徴候補「title、page」を除外する。そして、特徴選定部１２４は、除外の結果の残った特徴候補「123456789」を攻撃成功時の特徴として、特徴ＤＢ１１４に記憶させる。

[0064] ここで、本実施形態では、特徴選定部１２４は、特徴候補ＤＢ１１２から普遍的な語を除外する際、リクエスト・レスポンスＤＢ１１３を用いたが、予め用意された普遍的な語のリストを用いてもよい。また、特徴選定部１２４は、攻撃コード解析部１２３により抽出された特徴候補に対し、上記のように、文字列長が極端に短い特徴候補の除外及び普遍的な語の特徴候補の除外の双方を行ってもよいし、いずれか一方のみを行ってもよい。

[0065] 成否判定部１２５は、特徴ＤＢ１１４を参照して、Ｗｅｂサーバ１からのレスポンスが攻撃の成功を示すものか否かを判定する。つまり、成否判定部１２５は、レスポンスに、特徴ＤＢ１１４に記憶される特徴が含まれる場合、攻撃が成功したと判定する。一方、成否判定部１２５は、レスポンスに、特徴ＤＢ１１４に記憶される特徴が含まれない場合、攻撃は失敗したと判定する。すなわち、成否判定部１２５は、取得部１３３により取得された通信データを基に攻撃の成否を判定する。そして、成否判定部１２５は、攻撃の成否の判定結果を出力する。

[0066] ここで、成否判定部１２５は、攻撃リクエスト以降のＷｅｂサーバ１への複数のリクエストにそれぞれ対応する複数のレスポンスが、抽出した特徴を有するかそれぞれ検査し、複数のレスポンスのうち少なくともいずれか一つが、抽出した特徴を有する場合、攻撃コードによる攻撃が成功したと判定してもよい。

[0067] ［攻撃成否の判定処理の処理手順］

図４は、第１の実施形態に係る判定装置による攻撃成否の判定処理のフローチャートである。次に、図４を参照して、本実施形態に係るアラート検証装置１０による攻撃成否の判定処理の流れを説明する。

[0068] 通信データ取得部１２１の受信部１３１は、攻撃検知機器３によりＷｅｂサーバ１への攻撃が検知された場合、攻撃検知機器３からアラートを受信する。通信データ取得部１２１の生成部１３２は、受信部１３１により取得されたアラートから通信データの取得条件を生成する（ステップＳ１）。

[0069] 次に、通信データ取得部１２１の取得部１３３は、生成部１３２により生成された取得条件とマッチする通信データをパケットキャプチャ装置４から取得する（ステップＳ２）。その後、通信データ取得部１２１の取得部１３３は、取得した通信データをアラートに紐づく通信データとして攻撃タイプ判定部１２２へ出力する。

[0070] 攻撃タイプ判定部１２２は、攻撃タイプ別キーワードリスト１１１を参照して、通信データ取得部１２１により取得された通信データに含まれる攻撃コードの攻撃タイプを判定する（ステップＳ３）。

[0071] 攻撃タイプ判定部１２２は、攻撃タイプの判定結果から、攻撃タイプが判定可能か否かを判定する（ステップＳ４）。

[0072] 攻撃タイプが判定可能な場合（ステップＳ４：肯定）、攻撃コード解析部１２３は、攻撃タイプ判定部１２２により判定された攻撃タイプに基づき、攻撃コードのエミュレーションを実行する。そして、攻撃コード解析部１２３は、エミュレーションの結果出力された情報を、攻撃成功時の特徴候補として抽出する攻撃コード解析処理を行う（ステップＳ５）。その後、攻撃コード解析部１２３は、抽出した特徴候補を特徴候補ＤＢ１１２に記憶させる。

[0073] 特徴選定部１２４は、特徴候補ＤＢ１１２に格納された特徴候補の中から、特徴としては不適切な特徴候補を除外した特徴候補を、攻撃の成否の判定に用いる特徴として選定する（ステップＳ６）。

[0074] そして、特徴選定部１２４は、特徴の選定結果に応じて特徴が存在するか

否かを判定する（ステップＳ７）。例えば、特徴候補が全て除外された場合は、特徴選定部１２４は、特徴が存在しないと判定することになる。

[0075] 特徴が存在する場合（ステップＳ７：肯定）、特徴選定部１２４は、選定した攻撃の成否の判定に用いる特徴を特徴ＤＢ１１４に記憶させる。成否判定部１２５は、Ｗｅｂサーバ１からのレスポンスに特徴ＤＢ１１４に記憶された特徴が含まれるか否かを判定する（ステップＳ８）。成否判定部１２５は、特徴ＤＢ１１４に記憶される特徴と、攻撃の成否の判定対象となるＷｅｂサーバ１からのレスポンスとを照合することにより、攻撃が成功したか否かを判定する。

[0076] Ｗｅｂサーバ１からのレスポンスに特徴ＤＢ１１４に記憶された特徴が含まれている場合（ステップＳ８：肯定）、成否判定部１２５は、Ｗｅｂサーバ１への攻撃が成功したと判定する。そして、成否判定部１２５は、Ｗｅｂサーバ１への攻撃の成功を通知するメッセージを管理者端末などの外部装置（不図示）へ送信して、Ｗｅｂサーバ１の管理者に通知する（ステップＳ９）。

[0077] これに対して、Ｗｅｂサーバ１からのレスポンスに特徴ＤＢ１１４に記憶された特徴が含まれていない場合（ステップＳ８：否定）、成否判定部１２５は、Ｗｅｂサーバ１への攻撃は失敗したと判定する。そして、成否判定部１２５は、Ｗｅｂサーバ１への攻撃の失敗を通知するメッセージを管理者端末などの外部装置（不図示）へ送信して、Ｗｅｂサーバ１の管理者に通知する（ステップＳ１０）。

[0078] 一方、攻撃タイプの判定不可能な場合（ステップＳ４：否定）又は特徴が存在しない場合（ステップＳ７：否定）、成否判定部１２５は、攻撃の成否判定は不可として、管理者に通知する（ステップＳ１１）。

[0079] ［情報収集処理による効果］

以上に説明したように、本実施形態に係るアラート検証装置１０は、ＷＡＦなどの攻撃検知機器３による攻撃検知時のアラートを受信して、受信したアラートから生成した取得条件を満たす通信データを、通信データの複製を

保持するパケットキャプチャ装置４から取得する。そして、アラート検証装置１０は、取得したアラートに紐づく通信データを用いて攻撃タイプを判定し、攻撃コードをエミュレートしてレスポンスの特徴を抽出し、抽出した特徴を有するレスポンスがＷｅｂサーバ１から出力された場合、攻撃が成功したと判定する。これにより、アラート検証装置１０は、アラートに紐づく通信データのパースを行い攻撃の成否の判定ができるので、Ｗｅｂサーバ１に対する全ての通信データのパース処理に比べて少ないパース処理で攻撃の成否の判定ができる。したがって、アラート検証装置１０は、既存のシステムの改変や、攻撃の定義や脆弱性情報の収集を行うことなく、通信パケットのパース処理負荷を低減しつつ、Ｗｅｂサーバ１に対する攻撃の成否を判定することが可能となる。

[0080] ［第２の実施形態］

図５は、第２の実施形態におけるセカンドオーダ攻撃を示す図である。Ｗｅｂサーバ１への攻撃には、登録機能と参照機能をまたいで確認する必要のある脆弱性を対象とするセカンドオーダ攻撃が存在する。例えば、図５に示すようなセカンドオーダ攻撃を分析する場合について説明する。セッション＃１では、ＷＡＦ等の攻撃検知機器３は、攻撃リクエスト２０１が検知されるが、セッション＃２ではリクエストを攻撃と判定しないことが考えられる。この場合、攻撃リクエスト２０１とレスポンス２０２とが攻撃者が意図した攻撃であるが、第１の実施形態で説明したアラート検証装置１０では、レスポンス２０２がアラート検証技術の攻撃成否判定の対象とならないことがある。

[0081] そこで、本実施形態に係る通信データ取得部１２１は、アラートから通信データの取得条件を生成して、生成した取得条件を満たす通信データをパケットキャプチャ装置４から取得する処理に加えて、以下の処理を行う。ただし、通信データ取得部１２１は、アラートから生成した通信データの取得条件を満たす通信データを取得する処理に変えて、以下の処理を行ってもよい。

[0082] 生成部１３２は、受信部１３１により取得されたアラートから、その攻撃が検知されたセッションを特定する。次に、生成部１３２は、特定したセッションにおけるＩＰアドレスなどの通信元や通信先を特定できる情報を利用して取得条件を生成する。すなわち、生成部１３２は、アラートが発生した第１セッションにおける通信元又は通信先を特定する情報を基に取得条件を生成する。

[0083] 取得部１３３は、生成部１３２により生成された取得条件に応じてアラート発生から一定時間の間の通信データを取得する。すなわち、取得部１３３は、第１セッション及び第１セッション以降の第２セッションについても取得条件にマッチする通信データをパケットキャプチャ装置４から取得する。

[0084] 例えば、攻撃リクエスト２０１による攻撃を検知して攻撃検知機器３がアラートを発行した場合、生成部１３２は、アラートから攻撃が検出された際の攻撃リクエスト２０１によるセッション＃１を特定する。そして、生成部１３２は、セッション＃１における通信対象装置５のＩＰアドレスなどのＷｅｂサーバ１の通信相手を特定する情報を記憶する。例えば、生成部１３２は、セッション＃１における「送信元ＩＰアドレス１９２．１６８．０．１及び送信先ＩＰアドレス１０．０．０．１」を記憶する。

[0085] そして、取得部１３３は、アラート発生から一定時間の間に一定間隔でパケットキャプチャ装置４から通信対象装置５を特定する情報に一致する通信データを取得し、攻撃タイプ判定部１２２へ送信する。例えば、取得部１３３は、１時間の間、５分間隔でパケットキャプチャ装置４から「送信元ＩＰアドレス１９２．１６８．０．１及び送信先ＩＰアドレス１０．０．０．１」のＨＴＴＰリクエスト及びＨＴＴＰレスポンスを取得する。

[0086] ここで、通信データ取得部１２１は、成否判定部１２５によりセッション＃１について攻撃失敗と判定された場合に以上の処理を行ってもよい。

[0087] これにより、アラート検証装置１０は、攻撃リクエスト２０１が検知されたセッション＃１で攻撃失敗と判定した場合でも、攻撃リクエストが検知されないセッション＃２におけるレスポンス２０２により攻撃成功と判定する

ことができる。

[0088] 以上に説明したように、本実施形態に係るアラート検証装置１０は、攻撃が検知されたセッション以降のセッションについても攻撃の通信対象装置５との間の通信データを取得して、攻撃の成否を判定する。これにより、セカンドオーダ攻撃についても攻撃の成否を判定することが可能となり、Ｗｅｂサーバ１のセキュリティを向上させることができる。

[0089] ［第３実施形態］

図６は、第３の実施形態における複数のセッションにまたがる攻撃を示す図である。Ｗｅｂサーバ１への攻撃には、ブラインドＳＱＬインジェクションなどの複数のセッションにまたがる攻撃が存在する。例えば、図６に示すような複数のセッションにまたがる攻撃を分析する場合について説明する。この場合、セッション＃１及び＃２のいずれにおいても、攻撃検知機器３は、リクエスト２１１及び２１２を攻撃リクエストとして検知しないことが考えられる。この場合、第１の実施形態で説明したアラート検証装置１０では、セッション＃１及び＃２の通信が攻撃成否判定の対象とならないことがある。

[0090] そこで、本実施形態に係る通信データ取得部１２１は、アラートから通信データの取得条件を生成して、生成した取得条件を満たす通信データをパケットキャプチャ装置４から取得する処理に加えて、以下の処理を行う。ただし、通信データ取得部１２１は、アラートから生成した通信データの取得条件を満たす通信データを取得する処理に変えて、以下の処理を行ってもよい。

[0091] 生成部１３２は、事前に定義された攻撃コードを基に取得条件を生成する。そして、取得部１３３は、生成部１３２により生成された取得条件に応じた通信データをパケットキャプチャ装置４から取得して攻撃タイプ判定部１２２へ送信する。

[0092] 例えば、生成部１３２は、事前に定義された正規表現（例えば、”¥d+=¥d+”（¥d+は数字が１文字以上続くことを表す）など）とマッチするＨＴＴＰリ

クエスト及びＨＴＴＰレスポンスを取得するための取得条件を生成する。取得部１３３は、５分間隔などの一定間隔で、事前に定義された正規表現とマッチするＨＴＴＰリクエスト及びＨＴＴＰレスポンスをパケットキャプチャ装置４から取得して攻撃タイプ判定部１２２へ送信する。

[0093] 以上に説明したように、本実施形態に係るアラート検証装置１０は、攻撃検知機器３によりリクエスト２１１及び２１２が攻撃と検知されないセッション＃１及び＃２についても、攻撃成否判定処理の対象とすることができる。これにより、ブラインドＳＱＬインジェクションなどの複数のセッションにまたがる攻撃についても攻撃の成否を判定することが可能となり、Ｗｅｂサーバ１のセキュリティを向上させることができる。

[0094] ［第４の実施形態］

図７は、第４の実施形態におけるログインバイパス攻撃を示す図である。Ｗｅｂサーバ１への攻撃には、認証をバイパスしてログインするログインバイパス攻撃が存在する。例えば、図７に示すようなログイン攻撃を分析する場合について説明する。この場合、リクエスト２２１で入力される情報はログインページにとっては攻撃となるが、一般的には攻撃とならない情報である。さらに、ログイン後のページにアクセスするためのリクエスト２２２も攻撃検知機器３では攻撃とは判定されない。そのため、ログインページを特定しておかなければ、第１の実施形態で説明したアラート検証装置１０では、通信が攻撃成否判定の対象とならないことがある。

[0095] そこで、本実施形態に係る通信データ取得部１２１は、アラートから通信データの取得条件を生成して、生成した取得条件を満たす通信データをパケットキャプチャ装置４から取得する処理に加えて、以下の処理を行う。ただし、通信データ取得部１２１は、アラートから生成した通信データの取得条件を満たす通信データを取得する処理に変えて、以下の処理を行ってもよい。

[0096] 生成部１３２は、事前に定義されたログインページのＵＲＬのパス部などから取得条件を生成する。すなわち、生成部１３２は、監視対象装置である

Ｗｅｂサーバ１におけるログインページの情報を基に取得条件を生成する。そして、取得部１３３は、生成部１３２により生成された取得条件に応じて、ログインページに関連する通信データをパケットキャプチャ装置４から取得して攻撃タイプ判定部１２２へ送信する。

[0097] 例えば、生成部１３２は、事前にログインページの候補となるパス部（例えば、/login.php）などの指定を受ける。そして、生成部１３２は、ＵＲＬのパス部に”/login.php”を含むＨＴＴＰリクエスト及びＨＴＴＰレスポンスを取得するための取得条件を生成する。取得部１３３は、生成部１３２により生成された取得条件にしたがって、ＵＲＬのパス部に”/login.php”を含むＨＴＴＰリクエスト及びＨＴＴＰレスポンスをパケットキャプチャ装置４から取得して攻撃タイプ判定部１２２へ送信する。

[0098] なお、生成部１３２は、事前にログインページのＵＲＬのパス部などの指定を受けずに、以下の方法でログインページの情報を取得してもよい。例えば、生成部１３２は、アラートから生成した取得条件を満たす通信データを用いて攻撃成否判定が行われた際に、ログインページであると判定できたＵＲＬのパス部などを記憶する。そして、生成部１３２は、記憶したＵＲＬのパス部などから取得条件を生成してもよい。

[0099] 以上に説明したように、本実施形態に係るアラート検証装置１０は、攻撃検知機器３により攻撃と検知されないログインバイパス攻撃における通信についても、攻撃成否判定処理の対象とすることができる。これにより、ログインバイパス攻撃についても攻撃の成否を判定することが可能となり、Ｗｅｂサーバ１のセキュリティを向上させることができる。

[0100] ［第５の実施形態］

次に、第５の実施形態ついて説明する。攻撃検知機器３のアラート情報を使用せず、事前に定義された特定のＨＴＴＰリクエスト及びＨＴＴＰレスポンス、すなわち、事前に定義された特定の通信データについて攻撃成否判定を行いたい場合が存在する。

[0101] そこで、本実施形態に係る通信データ取得部１２１の生成部１３２は、事

前に定義された情報、すなわち、事前に定義された特定の通信データを抽出するための情報から取得条件を生成する。そして、通信データ取得部１２１の取得部１３３は、生成部１３２により生成された取得条件に応じた通信データをパケットキャプチャ装置４から取得して攻撃タイプ判定部１２２へ送信する。

[0102] 例えば、特定のＵＲＬのパス部（例えば、/example.html）などへのアクセスをアラート検証技術の攻撃成否判定の対象としたい場合、生成部１３２は、特定のＵＲＬのパス部である”/example.html”の情報を事前に取得する。そして、生成部１３２は、ＵＲＬのパス部に”/example.html”を含むＨＴＴＰリクエスト及びＨＴＴＰレスポンスを取得するための取得条件を生成する。取得部１３３は、生成部１３２により生成された取得条件にしたがい、ＵＲＬのパス部に”/example.html”を含むＨＴＴＰリクエスト及びＨＴＴＰレスポンスをパケットキャプチャ装置４から取得する。

[0103] 以上に説明したように、本実施形態に係るアラート検証装置１０は、事前に定義された情報に基づいて通信データを取得する。これにより、事前に定義された特定のＨＴＴＰリクエスト及びＨＴＴＰレスポンスについて攻撃成否判定を行うことが可能となり、Ｗｅｂサーバ１のセキュリティを向上させることができる。

[0104] ［第６の実施形態］

図８は、第６の実施形態に係るシステム構成図である。本実施形態に係るシステムには、図８に示すように、負荷分散装置６が設けられ、複数のパケットキャプチャ装置４が複数配置される。本実施例に係るシステムでは、通信データの取得処理が分散して行われる。

[0105] 負荷分散装置６は、複数のパケットキャプチャ装置４が接続される。負荷分散装置６は、通信複製機器２で生成されたインターネットからＷｅｂサーバ１へ送信される通信データの複製を受信する。そして、負荷分散装置６は、各パケットキャプチャ装置４におおよそ均等に送られるように分散して通信データの複製を送信する。

[0106] パケットキャプチャ装置４は、それぞれが負荷分散装置６から通信データの複製を受信する。そして、パケットキャプチャ装置４は、それぞれで取得した通信データを蓄積して保管する。

[0107] アラート検証装置１０は、複数のパケットキャプチャ装置４のそれぞれと接続される。アラート検証装置１０における通信データ取得部１２１の取得部１３３は、アラートに基づいて作成したデータの取得条件とマッチする通信データを各パケットキャプチャ装置４が保持する通信データの中から特定して取得する。すなわち、取得部１３３は、監視対象装置であるＷｅｂサーバ１が行う通信における通信データを分散して保持する複数のパケットキャプチャ装置４から通信データを取得する。

[0108] 以上に説明したように、本実施形態に係るシステムは、複製された通信データを複数のパケットキャプチャ装置４に分散して送信し格納させる。これにより、より大量のトラフィックが流れる環境において迅速に攻撃成否判定処理を行うことができ、トラフィックが大量に流れるＷｅｂサーバ１であってもセキュリティを向上させることができる。

[0109] （変形例）

以上の各実施例では、攻撃成否判定の監視対象とする通信をＨＴＴＰリクエスト及びＨＴＴＰレスポンスを例に説明したが、攻撃の成否を判定する情報を有する通信であれば特に制限はない。例えば、アラート検証装置１０は、ＦＴＰ（File Transfer Protocol）などの他のプロトコルを監視対象として攻撃成否判定処理を行ってもよい。

[0110] ［システム構成等］

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Ｃ

ＰＵ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。

[0111] また、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。

[0112] また、以上の各実施形態では、タップ構成のシステムを例に説明したが、これに限らず攻撃検知機器３とＷｅｂサーバ１との間にアラート検証装置１０が配置して、アラート検証装置１０が攻撃の成否の判定対象となるＷｅｂサーバ１に直接接続されるインライン構成を採用してもよい。また、以上の各実施例では、ＴＡＰなどの通信データをコピーするために通信複製機器２を配置したが、攻撃検知機器３が通信データの複製機能を有する場合、攻撃検知機器３にパケットキャプチャ装置４を接続し、攻撃検知機器３が、通信データを複製してパケットキャプチャ装置４に送信してもよい。

[0113] ［プログラム］

また、上記の実施形態で述べたアラート検証装置１０の機能を実現するプログラムを所望の情報処理装置（コンピュータ）にインストールすることによって実装できる。例えば、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提供される上記のプログラムを情報処理装置に実行させることにより、情報処理装置をアラート検証装置１０として機能させることができる。ここで言う情報処理装置には、デスクトップ型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、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 Assistants）等がその範疇に含まれる。また、アラート検証装置１０を、クラウドサーバに実装してもよい。

[0114] 図９は、攻撃成否判定処理のためのアラート検証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。図９に示すように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

[0115] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１および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ブインタフェース１０３０は、ハードディスクドライブ１０９０に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１１００に接続される。ディスクドライブ１１００には、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挿入される。シリアルポートインタフェース１０５０には、例えば、マウス１１１０およびキーボード１１２０が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１１３０が接続される。

[0116] 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、アラート検証装置１０と同等の機能を持つアラート検証装置１０の各処理を規定するアラート検証プログラムは、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、アラート検証装置１０における機能構成と同様の処理を実行するためのプログラムモジュール１０９３が、ハードディスクドライブ１０９０に記憶される。なお、ハードディスクドライブ１０９０は、ＳＳＤ（Solid State Drive）により代替されてもよい。

[0117] 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。

[0118] 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）や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

[0119] １ Ｗｅｂサーバ

２ 通信複製機器

３ 攻撃検知機器

４ パケットキャプチャ装置

１０ アラート検証装置

１１ 記憶部

１１１ 攻撃タイプ別キーワードリスト

１１２ 特徴候補ＤＢ

１１３ リクエスト・レスポンスＤＢ

１１４ 特徴ＤＢ

１２１ 通信データ取得部

１２２ 攻撃タイプ判定部

１２３　攻撃コード解析部

１２４　特徴選定部

１２５　成否判定部

請求の範囲

[請求項1] 監視対象装置に対する攻撃を検知する攻撃検知機器から送信されたアラートを受信する受信部と、

前記受信部により受信された前記アラートを基に、取得する通信データの取得条件を生成する生成部と、

前記監視対象装置により送受信されたデータを保持するパケットキャプチャ装置から、前記生成部により生成された前記取得条件にマッチする前記通信データを取得する取得部と、

前記取得部により取得された前記通信データを基に前記攻撃の成否を判定する成否判定部と

を備えたことを特徴とするアラート検証装置。

[請求項2] 前記生成部は、前記アラートが発生した第１セッションにおける通信元又は通信先を特定する情報を基に前記取得条件を生成し、

前記取得部は、前記第１セッション及び第２セッション以降についても前記取得条件にマッチする通信データを前記パケットキャプチャ装置から取得する

ことを特徴とする請求項１に記載のアラート検証装置。

[請求項3] 前記生成部は、事前に定義された攻撃コードを基に前記取得条件を生成することを特徴とする請求項１又は２に記載のアラート検証装置。

[請求項4] 前記生成部は、前記監視対象装置におけるログインページの情報を基に前記取得条件を生成することを特徴とする請求項１～３のいずれか一つに記載のアラート検証装置。

[請求項5] 前記生成部は、事前に定義された特定の通信データを抽出するための情報を基に前記取得条件を生成することを特徴とする請求項１～４のいずれか一つに記載のアラート検証装置。

[請求項6] 前記取得部は、前記監視対象装置が行う通信における通信データを分散して受信してそれぞれで保持する複数のパケットキャプチャ装置

から前記通信データを取得することを特徴とする請求項１～５のいずれか一つに記載のアラート検証装置。

[請求項7] 監視対象装置に対する攻撃を検知する攻撃検知機器から送信されたアラートを受信する受信工程と、

前記受信工程において受信された前記アラートを基に、取得する通信データの取得条件を生成する生成工程と、

前記監視対象装置により送受信されたデータを保持するデータを保持するパケットキャプチャ装置から、前記生成工程において生成された前記取得条件にマッチする前記通信データを取得する取得工程と

前記取得工程において取得された前記通信データを基に前記攻撃の成否を判定する成否判定工程と

を備えたことを特徴とするアラート検証方法。

[請求項8] 監視対象装置に対する攻撃を検知する攻撃検知機器から送信されたアラートを受信し、

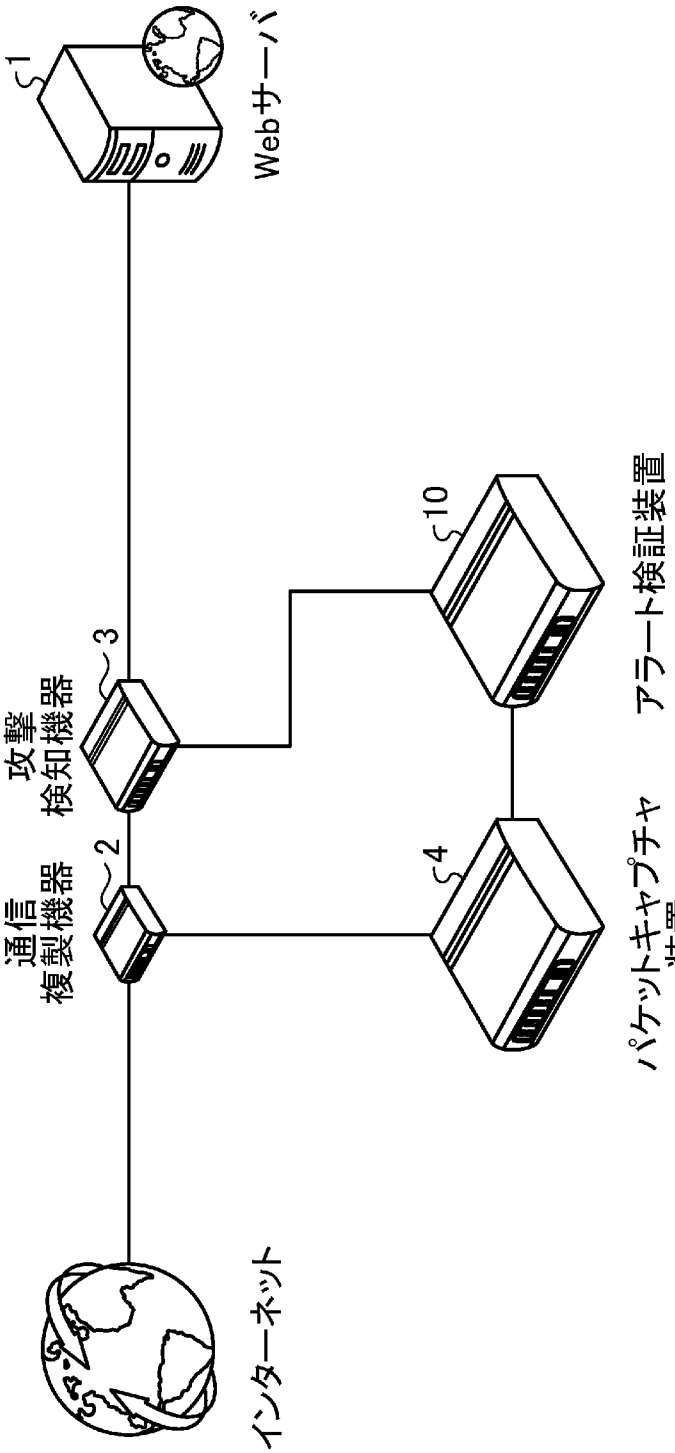
受信した前記アラートを基に、取得する通信データの取得条件を生成し、

前記監視対象装置により送受信されたデータを保持するパケットキャプチャ装置から、生成した前記取得条件にマッチする前記通信データを取得し、

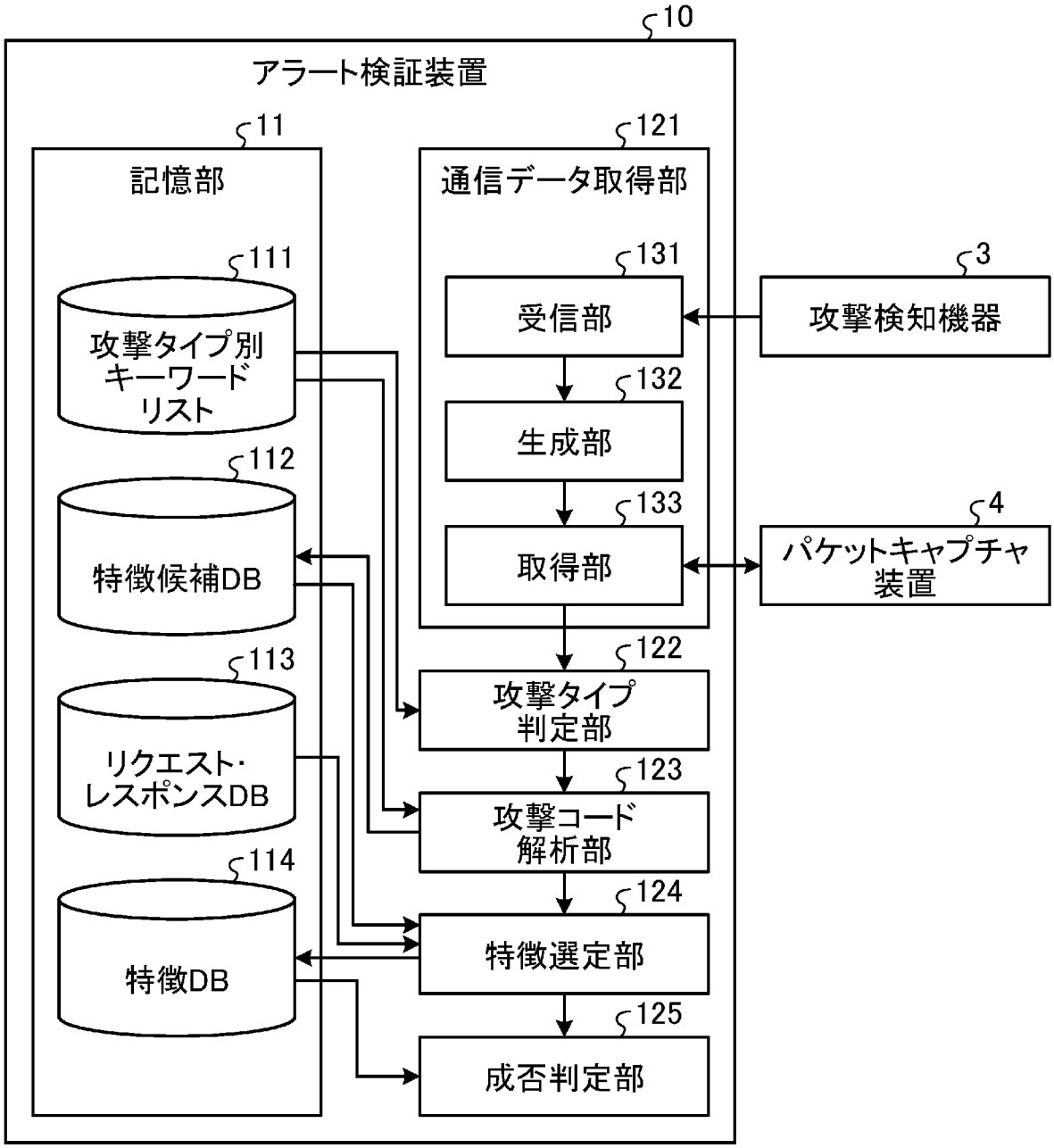
取得した前記通信データを基に前記攻撃の成否を判定する

処理をコンピュータ実行させることを特徴とするアラート検証プログラム。

[図1]


1
Webサーバ
3
攻撃
検知機器
2
通信
複製機器
10
アラート検証装置
4
パケットキャプチャ
装置
インターネット

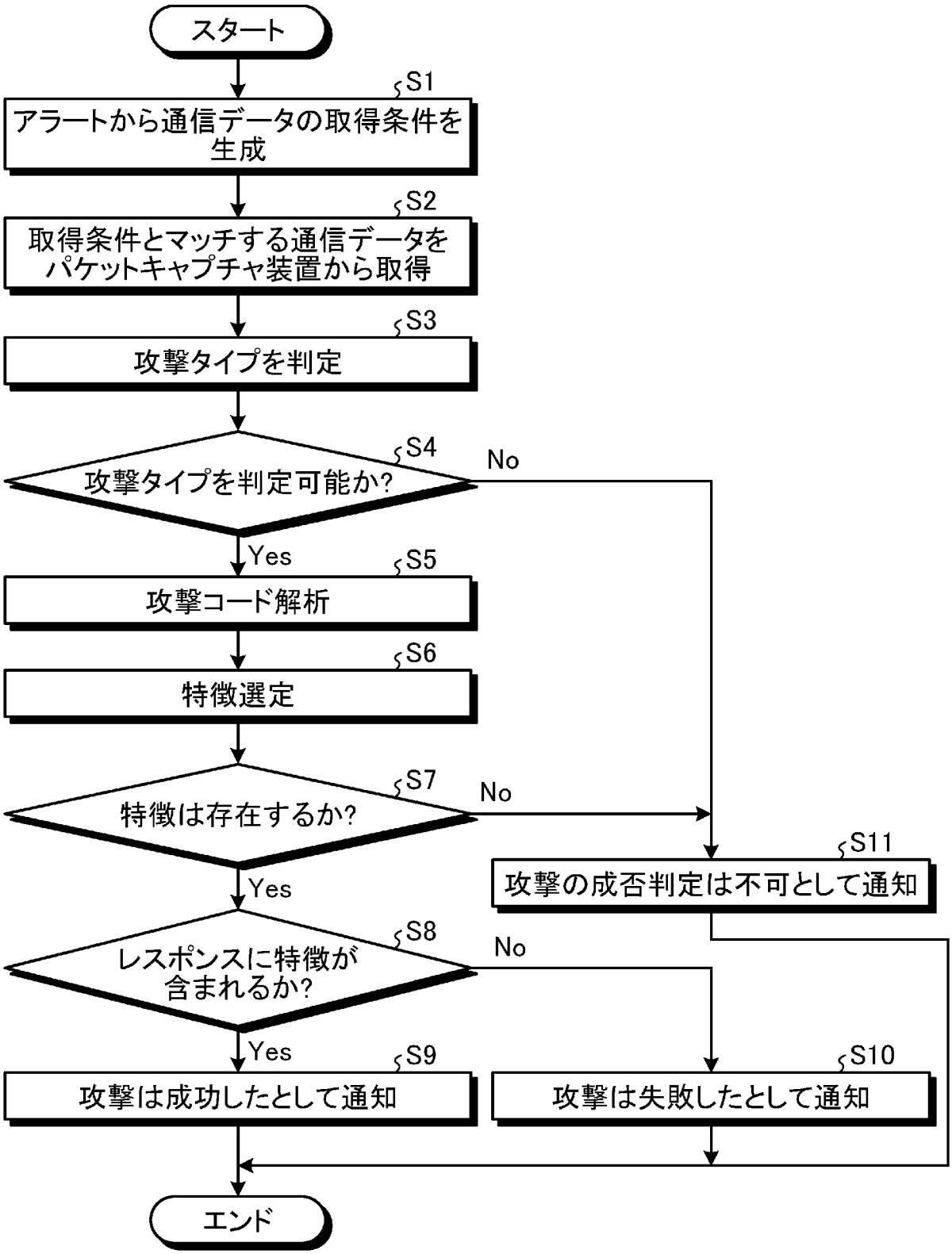
[図2]


10
アラート検証装置
11
記憶部
111
攻撃タイプ別
キーワード
リスト
112
特徴候補DB
113
リクエスト・
レスポンスDB
114
特徴DB
121
通信データ取得部
131
受信部
132
生成部
133
取得部
122
攻撃タイプ
判定部
123
攻撃コード
解析部
124
特徴選定部
125
成否判定部
3
攻撃検知機器
4
パケットキャプチャ
装置

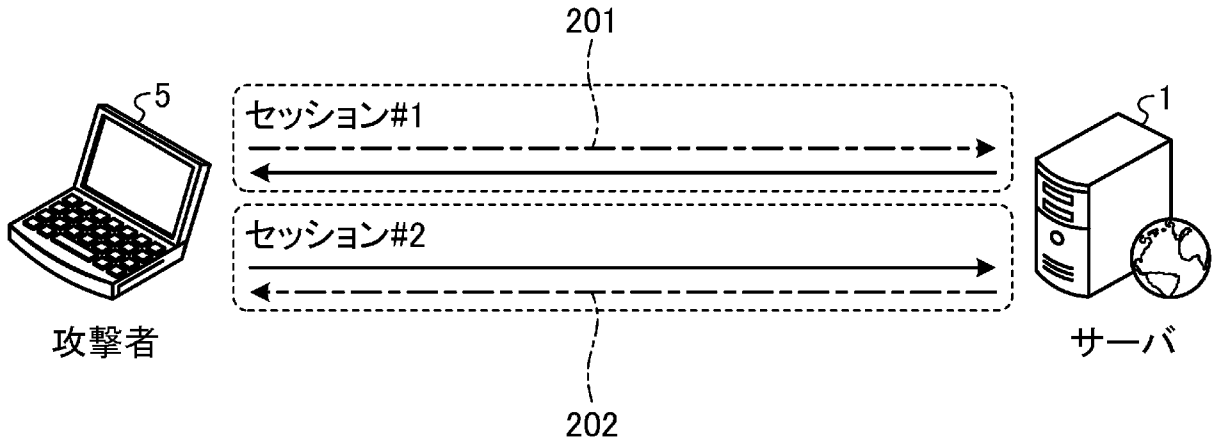
[図3]

攻撃タイプ	サブ攻撃タイプ	キーワード
A		cat, ls, wget, curl, echo, print, exec, php, python, ruby, …
B	PHP	print_r, var_dump, base64_decode, … $_GET, $_POST, …
	Java	java., javax., @ognl. など
	Perl	…
	…	…
C		select, update, insert, drop, … information_schema, @@version, mysql., …
D		<, >, script, iframe, document., window., onmouse, onclick, alert(, …
E		../, ./.../, …

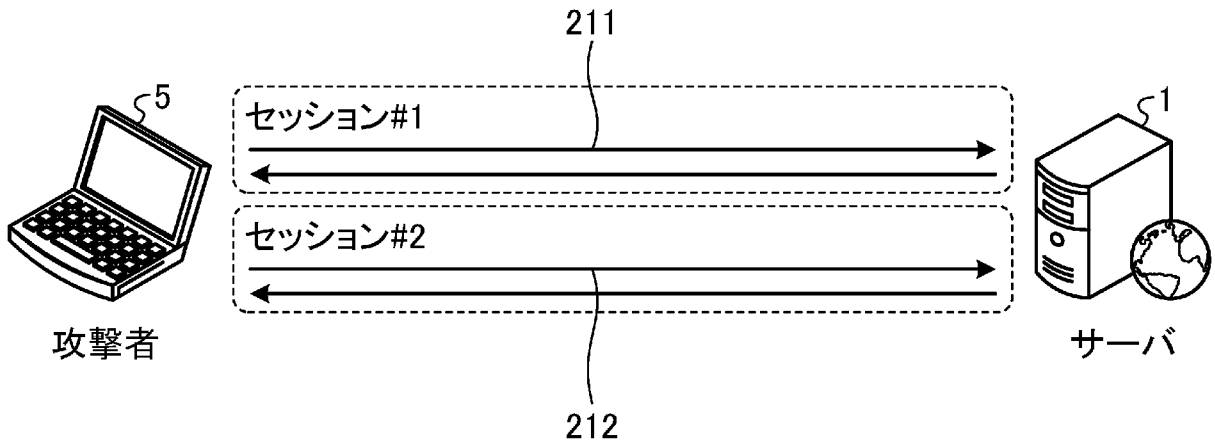
[図4]


スタート
S1
アラートから通信データの取得条件を生成
S2
取得条件とマッチする通信データをパケットキャプチャ装置から取得
S3
攻撃タイプを判定
S4
攻撃タイプを判定可能か?
No
Yes
S5
攻撃コード解析
S6
特徴選定
S7
特徴は存在するか?
No
Yes
S11
攻撃の成否判定は不可として通知
S8
レスポンスに特徴が含まれるか?
No
Yes
S9
攻撃は成功したとして通知
S10
攻撃は失敗したとして通知
エンド

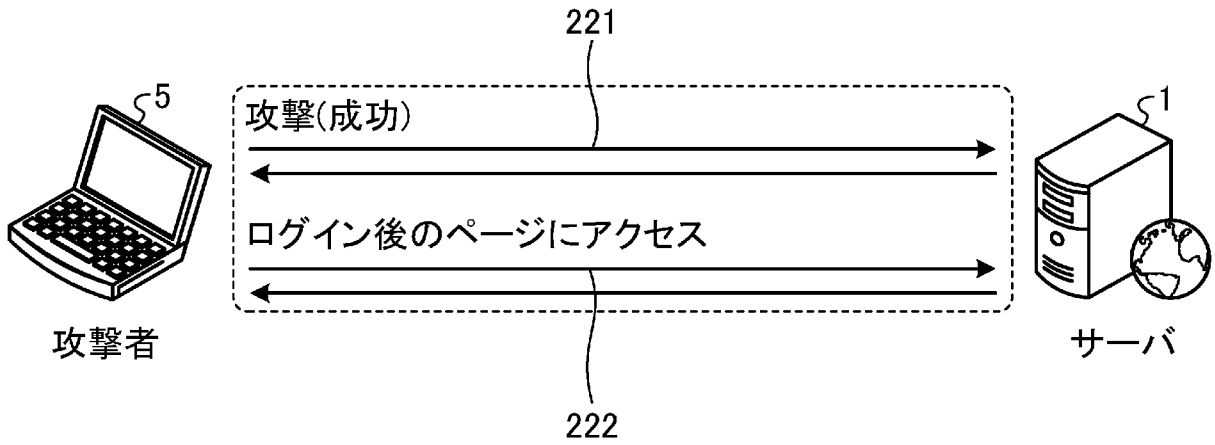
[図5]


201
5
セッション#1
1
セッション#2
攻撃者
サーバ
202

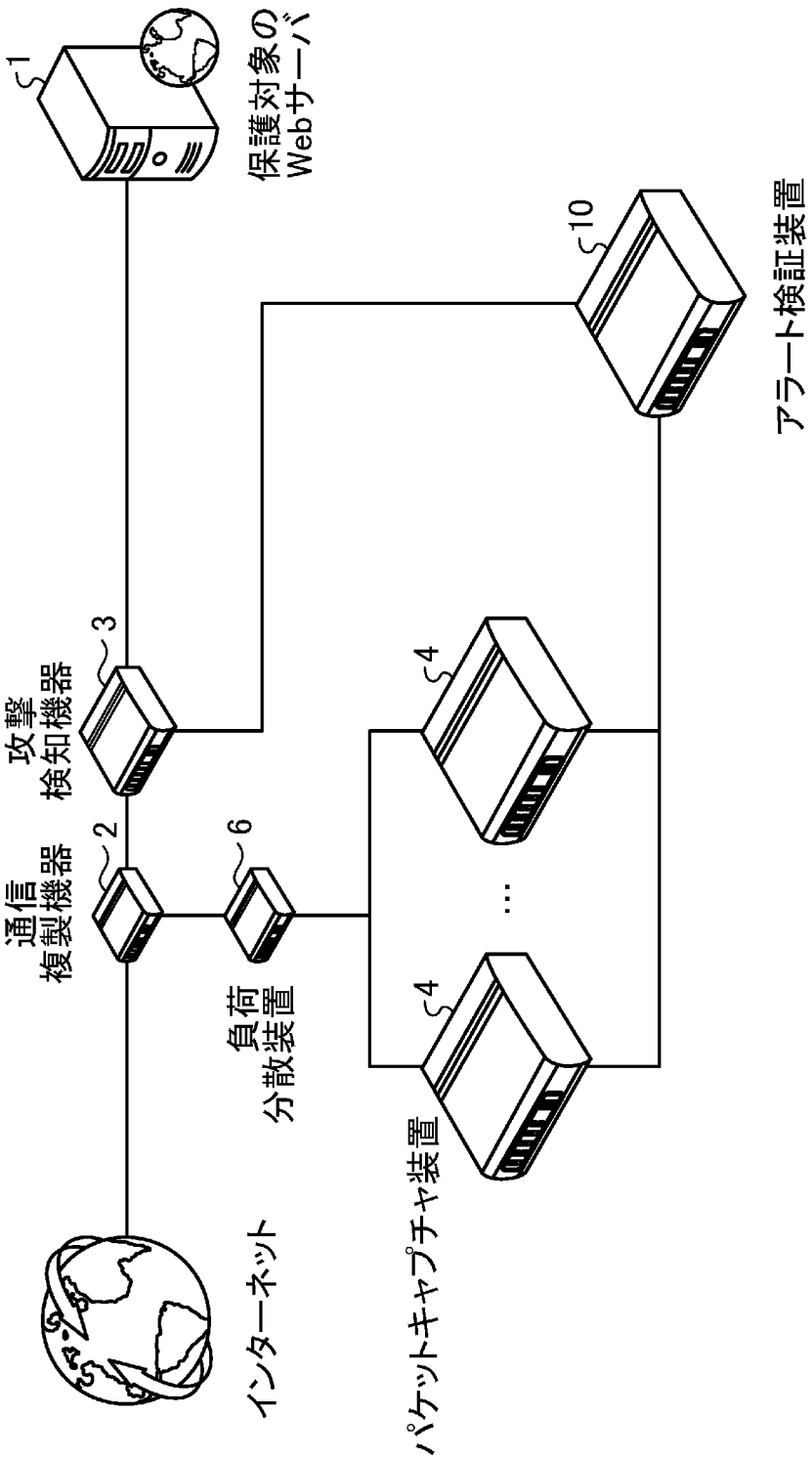
[図6]


211
5
セッション#1
1
セッション#2
攻撃者
サーバ
212

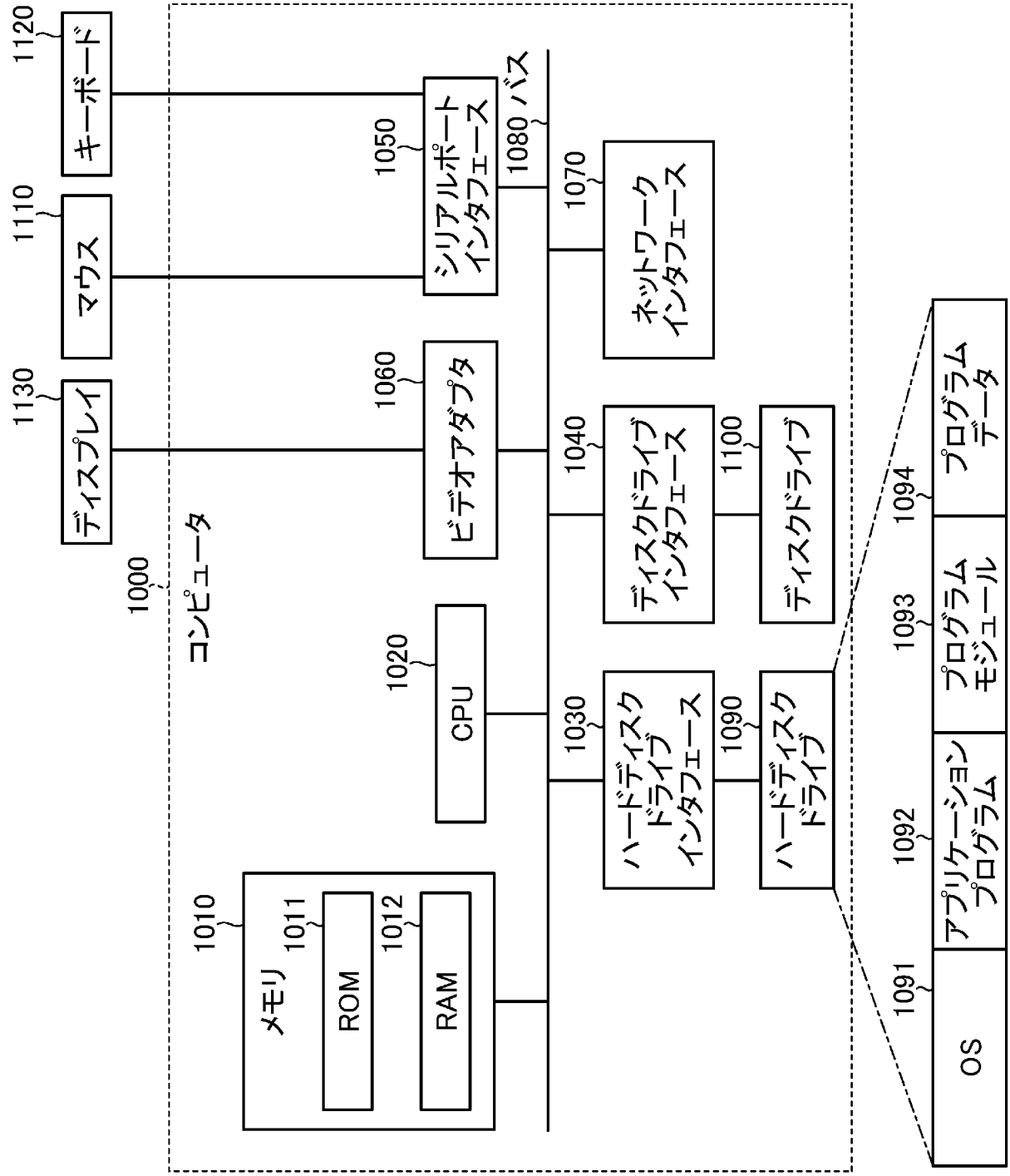
[図7]



[図8]


1
保護対象の
Webサーバ
10
アラート検証装置
攻撃
検知機器
3
通信
複製機器
2
6
4
4
負荷
分散装置
インターネット
パケットキャプチャ装置

[図9]


1120
キーボード
1110
マウス
1130
ディスプレイ
1000
コンピュータ
1050
シリアルポート
インタフェース
1080 バス
1070
ネットワーク
インタフェース
1060
ビデオアダプタ
1040
ディスクドライブ
インタフェース
1100
ディスクドライブ
1020
CPU
1030
ハードディスク
ドライブ
インタフェース
1090
ハードディスク
ドライブ
1010
メモリ
1011
ROM
1012
RAM
1091
OS
1092
アプリケーション
プログラム
1093
プログラム
モジュール
1094
プログラム
データ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/022590

A. CLASSIFICATION OF SUBJECT MATTER
G06F 21/55(2013.01)i
FI: 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)
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.
X	JP 2010-152773 A (MITSUBISHI ELECTRIC CORP) 08 July 2010 (2010-07-08) in particular, paragraphs [0009]-[0016], [0035]-[0049], etc.	1, 5, 7-8
A	all pages, all drawings	2, 4
Y	in particular, paragraphs [0009]-[0016], [0035]-[0049], etc.	3, 6
Y	WO 2019/225216 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 28 November 2019 (2019-11-28) in particular, paragraph [0061], etc.	3
A	all pages, all drawings	2, 4
Y	WO 2019/013266 A1 (NIPPON TELEGRAPH & TELEPHONE) 17 January 2019 (2019-01-17) in particular, paragraph [0056], etc.	3
A	all pages, all drawings	2, 4

☒ 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
24 August 2021 (2.08.2021)	31 August 2021 (31.08.2021)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/022590

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2015/189971 A1 (ARTIZA NETWORKS INC) 17 December 2015 (2015-12-17) in particular, paragraph [0018], etc.	6
A	all pages, all drawings	2, 4

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/022590

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2010-152773 A	08 Jul. 2010	(Family: none)	
WO 2019/225216 A1	28 Nov. 2019	(Family: none)	
WO 2019/013266 A1	17 Jan. 2019	EP 3637292 A1 in particular, paragraph [0056], etc.	
WO 2015/189971 A1	17 Dec. 2015	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/022590

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

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
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

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
X	JP 2010-152773 A（三菱電機株式会社）08.07.2010（2010-07-08） 特に段落０００９－００１６、００３５－００４９等	1, 5, 7-8
A	全頁、全図	2, 4
Y	特に段落０００９－００１６、００３５－００４９等	3, 6
Y	WO 2019/225216 A1（日本電信電話株式会社）28.11.2019（2019-11-28） 特に段落００６１等	3
A	全頁、全図	2, 4
Y	WO 2019/013266 A1（日本電信電話株式会社）17.01.2019（2019-01-17） 特に段落００５６等	3
A	全頁、全図	2, 4
Y	WO 2015/189971 A1（株式会社アルチザネットワークス）17.12.2015（2015-12-17） 特に段落００１８等	6
A	全頁、全図	2, 4

☐ 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
24.08.2021	31.08.2021

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）
児玉　崇晶 5S 3651
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/JP2021/022590

引用文献	公表日	パテントファミリー文献	公表日
JP 2010-152773 A	08.07.2010	（ファミリーなし）	
WO 2019/225216 A1	28.11.2019	（ファミリーなし）	
WO 2019/013266 A1	17.01.2019	EP 3637292 A1 特に段落００５６等	
WO 2015/189971 A1	17.12.2015	（ファミリーなし）	