(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10月20日(20.10.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/219819 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2021/015759

(22) 国際出願日： 2021年4月16日(16.04.2021)

(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).

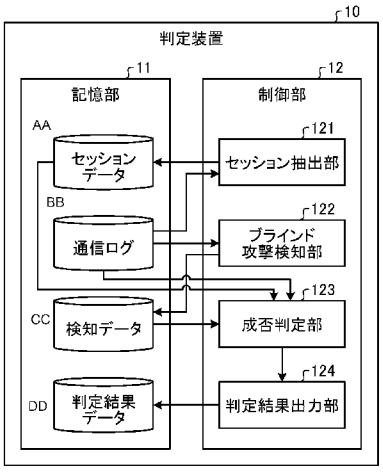
(72) 発明者: 鐘本 楊 (**KANEMOTO, Yo**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

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

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

(54) 発明の名称： 判定装置、判定方法、および、判定プログラム



10 Determination device
11 Storage unit
12 Control unit
121 Session extraction unit
122 Blind attack detection unit
123 Success or failure determination unit
124 Determination result output unit
AA Session data
BB Communication log
CC Detection data
DD Determination result data

(57) **Abstract:** This determination device (10) extracts a series of communication logs of the same session, from among attack detection target communication logs, and detects a blind attack by an attack detection signature. Further, the determination device (10) identifies the location of the attack target of the blind attack and the details of the attack, from the communication log in which the blind attack is detected. Next, the determination device (10) extracts, from among the series of communication logs of the same session, communication logs in which the locations of the attack target match, with respect to the communication log in which the blind attack is detected. Next, when it is determined that the extracted communication log has a plurality of types of attack details and a plurality of response status codes and response sizes, the determination device (10) determines that the blind attack due to communication indicated by the series of communication logs was successful.

(57) 要約：判定装置（１０）は、攻撃の検知対象の通信ログから、同じセッションの一連の通信ログを抽出し、攻撃検知シグネチャにより、ブラインド攻撃を検知する。また、判定装置（１０）は、ブラインド攻撃を検知した通信ログから、ブラインド攻撃の攻撃対象の箇所および攻撃の内容を特定する。次に、判定装置（１０）は、同じセッションの一連の通信ログのうち、ブラインド攻撃を検知した通信ログについて、攻撃対象の箇所が一致する通信ログを抽出する。次に、判定装置（１０）は、抽出した通信ログに、攻撃の内容が複数種類あり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、一連の通信ログの示す通信によるブラインド攻撃が成功したと判定する。

WO 2022/219819 A1

［続葉有］

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:

一　国際調査報告（条約第21条(3)）

明　細　書

発明の名称 ： 判定装置、判定方法、および、判定プログラム

技術分野

[0001] 本発明は、ブラインド攻撃が成功したか否かを判定するための、判定装置、判定方法、および、判定プログラムに関する。

背景技術

[0002] 従来、ウェブサーバ等への攻撃を検知する技術が提案されている。しかし、すべての攻撃を検知してアラートを発すると、保守者や監視者がアラートを見逃してしまう場合がある。したがって、攻撃が成功した場合のみ、アラートを発することが好ましい。ここで、従来、攻撃が成功したか否かを、ウェブサーバ等へ攻撃を行った際のレスポンスを検査することにより判定する技術がある（特許文献１参照）。

先行技術文献

特許文献

[0003] 特許文献1：特許第６７０８７９４号公報

発明の概要

発明が解決しようとする課題

[0004] しかし、従来技術は、攻撃による痕跡がウェブサーバ等へ攻撃を行った際のレスポンスに出現することを前提としている。例えば、ブラインドSQLインジェクション、ブラインドOSコマンドインジェクション等、攻撃対象に対し、それぞれ異なるパラメタを設定したリクエストを送信し、そのレスポンスの違いから、情報を探る攻撃（ブラインド攻撃）の場合、攻撃の痕跡が明示的にレスポンスに出現しない。このため、従来技術では、攻撃が成功したか否かが判定できなかった。

[0005] [例１：ブラインドSQLインジェクションの場合]

例えば、ウェブアプリケーション/index.phpにSQLインジェクションの脆弱性が存在し、以下のようなブラインド攻撃を受けた場合を考える。

[0006] GET /index.php?id=“1 AND user() = ‘admin’ #”

GET /index.php?id=“1 AND user() != ‘admin’ #”

[0007] このブラインド攻撃が成功すると、DB（データベース）に接続しているユーザがadminであるという情報が漏洩する。この攻撃は成功しても、レスポンスの内容に攻撃の痕跡（例えば、adminという文字列）が出現しない。

[0008] [例２：ブラインドOSコマンドインジェクション]

また、以下のようなブラインド攻撃を受けた場合を考える。

[0009] GET /index.php?name=x; X=$(cat /etc/passwd|tail -n 1|cut -f 1 -d”:”);test $X = ” admin”

GET /index.php?name=x; X=$(cat /etc/passwd|tail -n 1|cut -f 1 -d”:”);test $X != ” admin”

[0010] このブラインド攻撃が成功すると、最近作成されたユーザ名がadminであるという情報が漏洩する。例1と同様に、この攻撃も成功しても、レスポンスの内容に攻撃の痕跡（例えば、adminという文字列）が出現しない。

[0011] そこで、本発明は、前記した問題を解決し、ブラインド攻撃が成功したか否かを判定することを課題とする。

課題を解決するための手段

[0012] 前記した課題を解決するため、本発明は、攻撃の検知対象の通信ログから、同じセッションの一連の通信ログを抽出するセッション抽出部と、前記通信ログのリクエスト先のURLを用いて、ブラインド攻撃の通信ログを検知し、ブラインド攻撃を検知した前記通信ログから、ブラインド攻撃の攻撃対象の箇所および攻撃の内容を特定する攻撃検知部と、抽出された前記同じセッションの一連の通信ログのうち、前記攻撃対象の箇所が一致する通信ログを抽出し、抽出した前記通信ログに、攻撃の内容が複数種類あり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、前記一連の通信ログの示す通信によりブラインド攻撃が成功したと判定する成否判定部と、前記判定の結果を出力する判定結果出力部とを備えることを特徴とする。

発明の効果

[0013] 本発明によれば、ブラインド攻撃が成功したか否かを判定することができる。

図面の簡単な説明

[0014] [図1]図１は、判定装置の動作概要を説明するための図である。

[図2]図２は、判定装置の構成例を示す図である。

[図3]図３は、図２の通信ログの例を示す図である。

[図4]図４は、図２の検知データの例を示す図である。

[図5]図５は、図２の成否判定部による成否判定を説明するための図である。

[図6]図６は、判定装置の処理手順の例を示すフローチャートである。

[図7]図７は、判定装置を含むシステムの構成例を示す図である。

[図8]図８は、判定プログラムを実行するコンピュータの構成例を示す図である。

発明を実施するための形態

[0015] 以下、図面を参照しながら、本発明を実施するための形態（実施形態）について説明する。本発明は、以下に説明する実施形態に限定されない。

[0016] [概要]

本実施形態の判定装置１０の概要を説明する。なお、以下の説明において、ブラインド攻撃とは、攻撃対象に対し、異なるパラメタを設定したリクエストを送信し、そのリクエストに対するレスポンスの違いから、情報を探る攻撃である。

[0017] 例えば、図１に示すように、判定装置１０は、ウェブサーバとの通信の通信ログから、ウェブサーバへのリクエスト（（１））と、そのリクエストに対するレスポンスのステータスコードおよびレスポンスサイズ（（２））とを取得する。そして、判定装置１０は、取得したデータに基づき、同じセッション間でブラインド攻撃を特定し、ステータスコードやレスポンスサイズから攻撃の成否を判定する（（３））。

[0018] 例えば、判定装置１０は、取得した通信ログの中から、同じセッションの

一連の通信ログ（図１の符号１０１参照）を抽出する。そして、判定装置１０は、抽出した一連の通信ログのリクエスト先のURL等から、一連の通信がブラインド攻撃であるか否かを判定する。

[0019] ここで判定装置１０が、一連の通信をブラインド攻撃と判定し、攻撃対象箇所が同じ（例えば、URLのパラメタid）であり、攻撃の内容（例えば、リクエストに設定されたパラメタ等）が異なり、かつ、レスポンスのステータスコードおよびレスポンスサイズが異なる場合、判定装置１０は、符号１０１に示す一連の通信によるブラインド攻撃は成功したと判定する。

[0020] このようにすることで、判定装置１０は、ブラインド攻撃を検知し、そのブラインド攻撃が成功したか否かを判定することができる。

[0021] [構成例]

次に、図２を用いて、判定装置１０の構成例を説明する。判定装置１０は、記憶部１１と、制御部１２とを備える。記憶部１１は、制御部１２が各種処理を実行する際に参照するデータや、各種処理の実行により生成されたデータを記憶する。

[0022] 例えば、記憶部１１は、攻撃の検知対象の通信ログである通信ログ、制御部１２により抽出されたセッションデータ（詳細は後記）、検知データ（詳細は後記）、攻撃が成功したか否かの判定結果データ等を記憶する。

[0023] 通信ログは、例えば、図３に示すように、攻撃の検知対象の通信ログの識別情報（No.）ごとに、通信の発生時刻、リクエストの送信元および送信先、リクエスト先のURLと、レスポンスのステータスコード、レスポンスサイズ等を含む。なお、通信ログは、例えば、判定装置１０の入出力部（図示省略）経由で入力される。

[0024] 制御部１２は、判定装置１０全体の制御を司る。制御部１２は、セッション抽出部１２１と、ブラインド攻撃検知部１２２と、成否判定部１２３と、判定結果出力部１２４とを備える。

[0025] セッション抽出部１２１は、通信ログから同じセッションの通信ログを抽出する。例えば、セッション抽出部１２１は、通信ログから、送信元および

送信先が同じで所定時間以内に行われた一連の通信の通信ログを、同じセッションの通信ログとして抽出する。

[0026] 例えば、セッション抽出部１２１は、図３に示す通信ログから、送信元および送信先が同じで、T=5以内に通信が行われた[1,2,5]、[3,4]、[6]の通信ログを、それぞれ同じセッションの通信の通信ログとして抽出する。そして、セッション抽出部１２１は、抽出した通信ログそれぞれにセッションの識別情報（例えば、S1,S2,S3）を付与する。

[0027] その後、セッション抽出部１２１は、セッションの識別情報と当該セッションに対応する通信ログの識別情報とを示した情報（例えば、S1=[1,2,5]、S2=[3,4]、S3=[6]）をセッションデータとして記憶部１１に格納する。

[0028] 図２の説明に戻る。ブラインド攻撃検知部１２２は、例えば、既存のシグネチャ検知を利用して、通信ログの示すリクエストがブラインド攻撃か否かを判定する。

[0029] 例えば、検知シグネチャを、正規表現“AND .* [!=<>]+ .* #”とした場合を考える。この場合、ブラインド攻撃検知部１２２は、図３に示す通信ログから、上記の検知シグネチャを持つ[2,3,4,5]を、ブラインド攻撃の通信ログとして検知する（図４参照）。

[0030] なお、ブラインド攻撃検知部１２２は、例えば、図４に示すように、ブラインド攻撃の通信ログから、ブラインド攻撃の対象箇所およびブラインド攻撃の内容の特定も行う。そして、ブラインド攻撃検知部１２２は、ブラインド攻撃を検知した通信ログの識別情報（No.）、ブラインド攻撃の対象箇所、ブラインド攻撃の内容等を示した情報（図４参照）を検知データとして記憶部１１に格納する。

[0031] なお、ブラインド攻撃検知部１２２がブラインド攻撃の検知に用いるシグネチャは、上記の正規表現“AND .* [!=<>]+ .* #”の他、正規表現“test ¥$.+ !?= ”、正規表現“test ¥$.+ -(z|n|eq|ne|gt|ge|lt|le)”等であってもよい。ブラインド攻撃検知部１２２が、ブラインド攻撃シグネチャとして、正規表現“test ¥$.+ !?= ”、正規表現“test ¥$.+ -(z|n|

eq|ne|gt|ge|lt|le)”を用いることで、ブラインドOSコマンドインジェクションによる攻撃を検知することができる。

[0032] 図２の説明に戻る。成否判定部１２３は、同じセッションの通信ログのうち、攻撃対象の箇所が一致する通信ログを抽出する。そして、成否判定部１２３は、抽出した通信ログの攻撃の内容が複数種類であり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、ブラインド攻撃に成功したと判定する。一方、成否判定部１２３は、抽出した通信ログの攻撃の内容が複数種類ではない、レスポンスのステータスコードが複数ない、または、レスポンスサイズが複数ないと判定した場合、ブラインド攻撃に失敗したと判定する。

[0033] 例えば、成否判定部１２３は、セッションデータを参照して、通信ログから同じセッションの通信ログを抽出する。そして、成否判定部１２３は、検知データを参照して、抽出した通信ログから、ブラインド攻撃が検知され、かつ、攻撃対象の箇所が一致する通信ログを特定する。

[0034] 例えば、図５に示す通信ログにおいて、No.2,5の通信ログのブラインド攻撃は、セッションS1に属し、攻撃対象箇所がパラメタidで一致する。また、No.2,5の通信ログのブラインド攻撃の内容がそれぞれ異なり、かつ、ステータスコードおよびレスポンスサイズがそれぞれ異なることから、成否判定部１２３は攻撃に成功したと判定する。

[0035] 一方、図５に示す通信ログにおいて、No.3,4の通信ログのブラインド攻撃は、セッションS2に属し、攻撃対象箇所がパラメタpwで一致する。また、No.3,4の通信ログのブラインド攻撃の内容はそれぞれ異なるが、ステータスコードおよびレスポンスサイズがそれぞれ同じであるので、成否判定部１２３は攻撃に失敗した判定する。

[0036] 図２の説明に戻る。判定結果出力部１２４は、成否判定部１２３による判定結果を出力する。判定結果出力部１２４は、通信ログのうち、No.2,5の通信ログは、パラメタidに対するブラインド攻撃を示し、攻撃に成功したという判定結果を出力する。

[0037] このようにすることで、判定装置１０は、既存のシステムを改変することなく、ブラインド攻撃を検知し、攻撃が行われているセッション間の通信の挙動からブラインド攻撃が成功したか否かを判定することができる。

[0038] ［処理手順の例］

次に、図６を用いて判定装置１０の処理手順の例を説明する。まず、判定装置１０が新たな通信ログを取得すると（Ｓ１１）、セッション抽出部１２１でセッションデータをもとに通信ログが新たなセッションか既存のセッションの一部かを判定し、判定の結果に応じて、セッションデータを更新する（Ｓ１２）。

[0039] Ｓ１２の後、Ｓ１１で取得した新たな通信ログが、ブラインド攻撃検知部１２２でブラインド攻撃として検知されたか否かを判定する（Ｓ１３）。ブラインド攻撃検知部１２２で当該新たな通信ログがブラインド攻撃として検知された場合（Ｓ１３でＹｅｓ）、成否判定部１２３でセッションデータをもとにブラインド攻撃の成否を判定する（Ｓ１４）。そして、判定結果出力部１２４で、Ｓ１４の判定の結果を出力する（Ｓ１５）。一方、ブラインド攻撃検知部１２２で当該新たな通信ログがブラインド攻撃として検知されなかった場合（Ｓ１３でＮｏ）、処理を終了する。

[0040] 判定装置１０が上記の処理を行うことで、既存のシステムを改変することなく、ブラインド攻撃を検知し、攻撃が行われているセッション間の通信の挙動からブラインド攻撃が成功したか否かを判定することができる。その結果、保守者や管理者は、上記の攻撃に関し、優先すべきアラートとそうでないアラートを分別できるので、セキュリティオペレーションを効率的に行うことができる。

[0041] ［その他の実施形態］

なお、判定装置１０におけるブラインド攻撃検知部１２２は、判定装置１０の外部に設置されていてもよい。例えば、ブラインド攻撃検知部１２２は、図７の（１）および（２）に示すように、判定装置１０の外部に設置されるWAF（Web Application Firewall）等の攻撃検知機器により実現されても

よい。また、判定装置１０は、図７の（１）に示すように、攻撃の成否の判定対象となるウェブサーバと直接接続する構成（インライン構成）としてもよいし、図７の（２）に示すように、ウェブサーバとWAF等の攻撃検知機器経由で接続する構成（タップ構成）としてもよい。

[0042] ［システム構成等］

また、図示した各部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・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・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及び当該ＣＰＵにて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。

[0043] また、前記した実施形態において説明した処理のうち、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。

[0044] ［プログラム］

前記した判定装置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、情報処理装置を判定装置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、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）等の端末等がその範疇に含

まれる。

[0045] また、判定装置１０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。この場合、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。

[0046] 図８は、判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。

[0047] 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。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。

[0048] 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、上記の判定装置１０が実行する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１

０９３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、判定装置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。

[0049] また、上述した実施形態の処理で用いられるデータは、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が、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に読み出して実行する。

[0050] 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）を介して接続される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

[0051] １０ 判定装置

１１ 記憶部

１２ 制御部

１２１ セッション抽出部

１２２ ブラインド攻撃検知部

１２３ 成否判定部

１２４ 判定結果出力部

請求の範囲

[請求項1] 攻撃の検知対象の通信ログから、同じセッションの一連の通信ログを抽出するセッション抽出部と、

前記通信ログのリクエスト先のURLを用いて、ブラインド攻撃の通信ログを検知し、ブラインド攻撃を検知した前記通信ログから、ブラインド攻撃の攻撃対象の箇所および攻撃の内容を特定する攻撃検知部と、

抽出された前記同じセッションの一連の通信ログのうち、前記ブラインド攻撃の攻撃対象の箇所が一致する通信ログを抽出し、抽出した前記通信ログに、攻撃の内容が複数種類あり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、前記一連の通信ログの示す通信によりブラインド攻撃が成功したと判定する成否判定部と、

前記判定の結果を出力する判定結果出力部と

を備えることを特徴とする判定装置。

[請求項2] 前記攻撃検知部は、

前記通信ログのリクエスト先のURLに対し、攻撃検知シグネチャを適用することにより、ブラインド攻撃の通信ログを検知する

ことを特徴とする請求項１に記載の判定装置。

[請求項3] 前記攻撃検知部は、

正規表現“AND.*[!=<>]+.*#”、“test ¥$.+ !?=”、および、正規表現“test ¥$.+ -(z|n|eq|ne|gt|ge|lt|le)”のうち、少なくともいずれか１つを攻撃検知シグネチャとして用いて、ブラインド攻撃の通信ログを検知する

ことを特徴とする請求項１に記載の判定装置。

[請求項4] 判定装置により実行される判定方法であって、

攻撃の検知対象の通信ログから、同じセッションの一連の通信ログを抽出する工程と、

前記通信ログのリクエスト先のURLを用いて、ブラインド攻撃の通信ログを検知し、ブラインド攻撃を検知した前記通信ログから、ブラインド攻撃の攻撃対象の箇所および攻撃の内容を特定する工程と、

抽出された前記同じセッションの一連の通信ログのうち、前記ブラインド攻撃の攻撃対象の箇所が一致する通信ログを抽出し、抽出した前記通信ログに、攻撃の内容が複数種類あり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、前記一連の通信ログの示す通信によりブラインド攻撃が成功したと判定する工程と、

前記判定の結果を出力する工程と

を含むことを特徴とする判定方法。

[請求項5] 攻撃の検知対象の通信ログから、同じセッションの一連の通信ログを抽出する工程と、

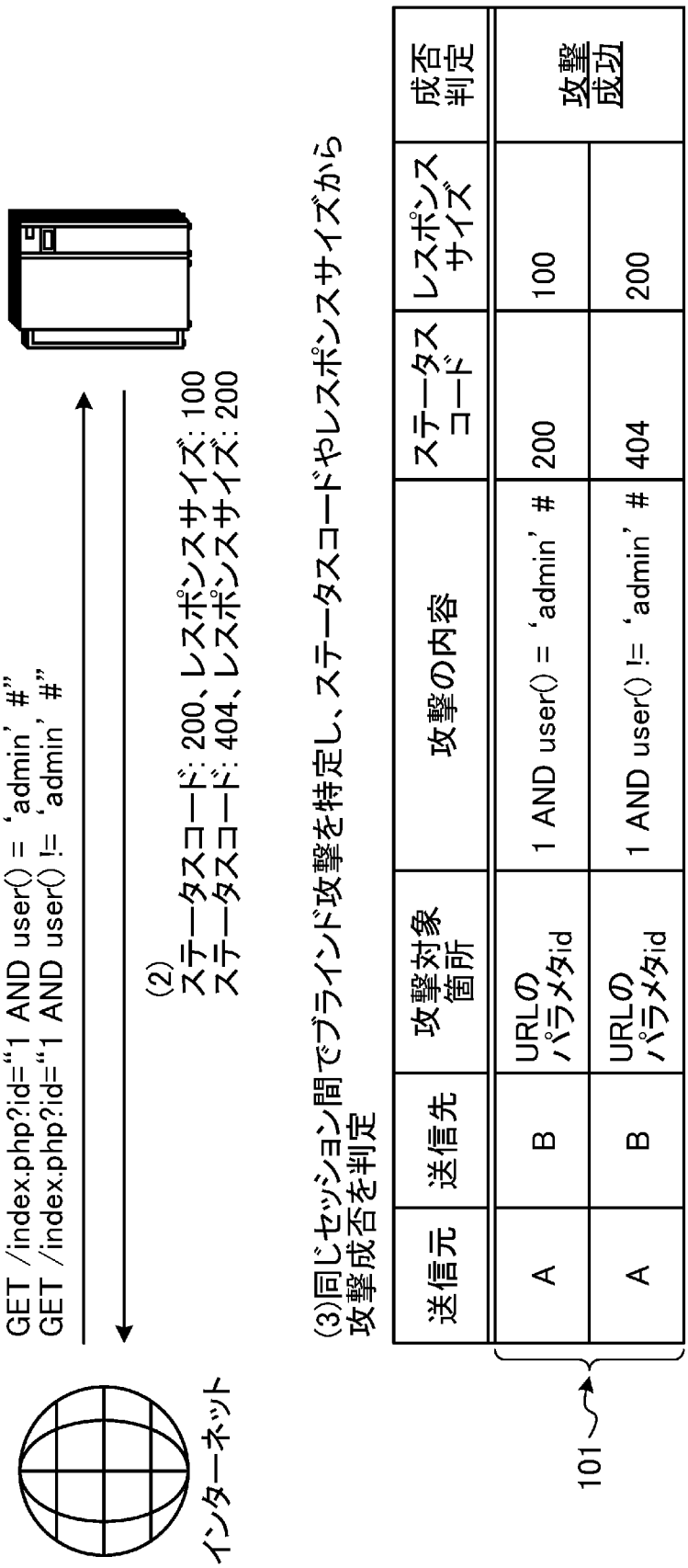
前記通信ログのリクエスト先のURLを用いて、ブラインド攻撃の通信ログを検知し、ブラインド攻撃を検知した前記通信ログから、ブラインド攻撃の攻撃対象の箇所および攻撃の内容を特定する工程と、

抽出された前記同じセッションの一連の通信ログのうち、前記ブラインド攻撃の攻撃対象の箇所が一致する通信ログを抽出し、抽出した前記通信ログに、攻撃の内容が複数種類あり、かつ、レスポンスのステータスコードおよびレスポンスサイズが複数あると判定した場合、前記一連の通信ログの示す通信によりブラインド攻撃が成功したと判定する工程と、

前記判定の結果を出力する工程と

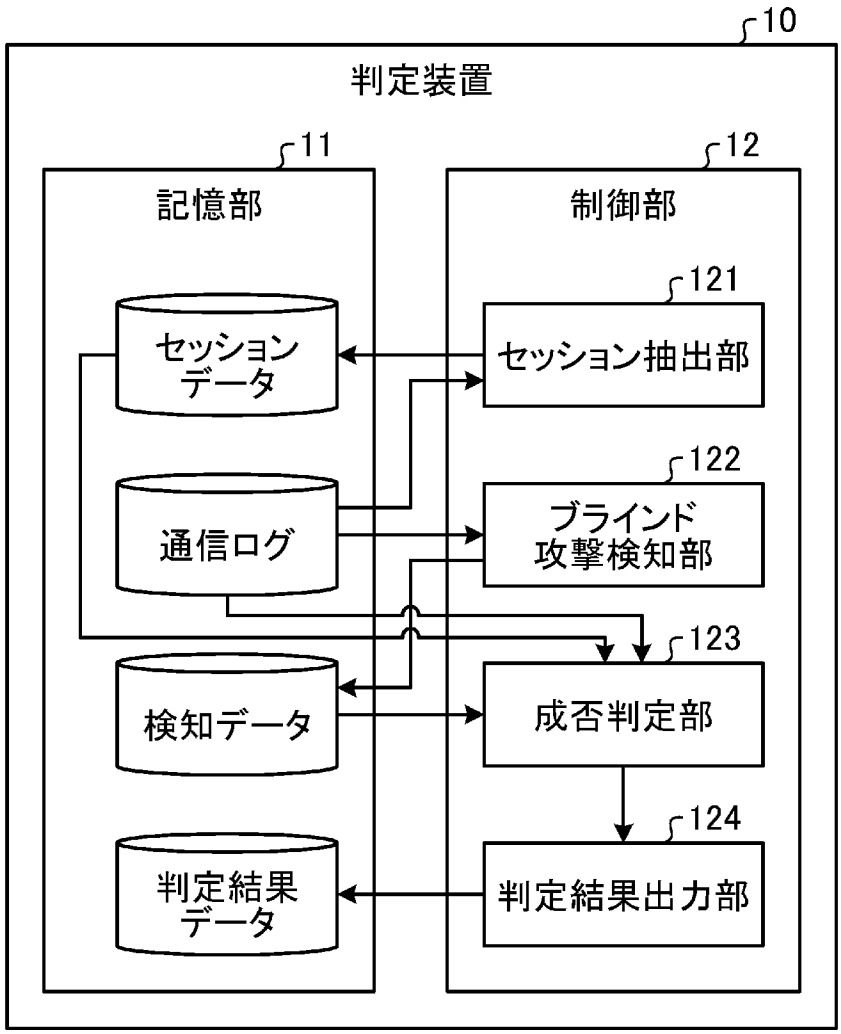
をコンピュータに実行させるための判定プログラム。

[図1]



送信元	送信先	攻撃対象箇所	攻撃の内容	ステータスコード	レスポンスサイズ	成否判定
A	B	URLのパラメタid	1 AND user() = 'admin' #	200	100	攻撃成功
A	B	URLのパラメタid	1 AND user() != 'admin' #	404	200	

[図2]


10
判定装置
11
記憶部
12
制御部
121
セッション抽出部
122
ブラインド攻撃検知部
123
成否判定部
124
判定結果出力部
セッションデータ
通信ログ
検知データ
判定結果データ

[図3]

No.	時刻	送信元	送信先	URL	ステータスコード	レスポンスサイズ	セッション
1	0	A	B	/index.php	200	100	S1
2	1	A	B	/index.php?id=1 AND user() = 'admin' #	200	100	S1
3	2	C	B	/index.php?pw='test' AND user() = 'admin' #	200	100	S2
4	3	C	B	/index.php?pw='test' AND user() != 'admin' #	200	100	S2
5	4	A	B	/index.php?id="1 AND user() != 'admin' #"	404	200	S1
6	10	A	B	/home.php	200	150	S3

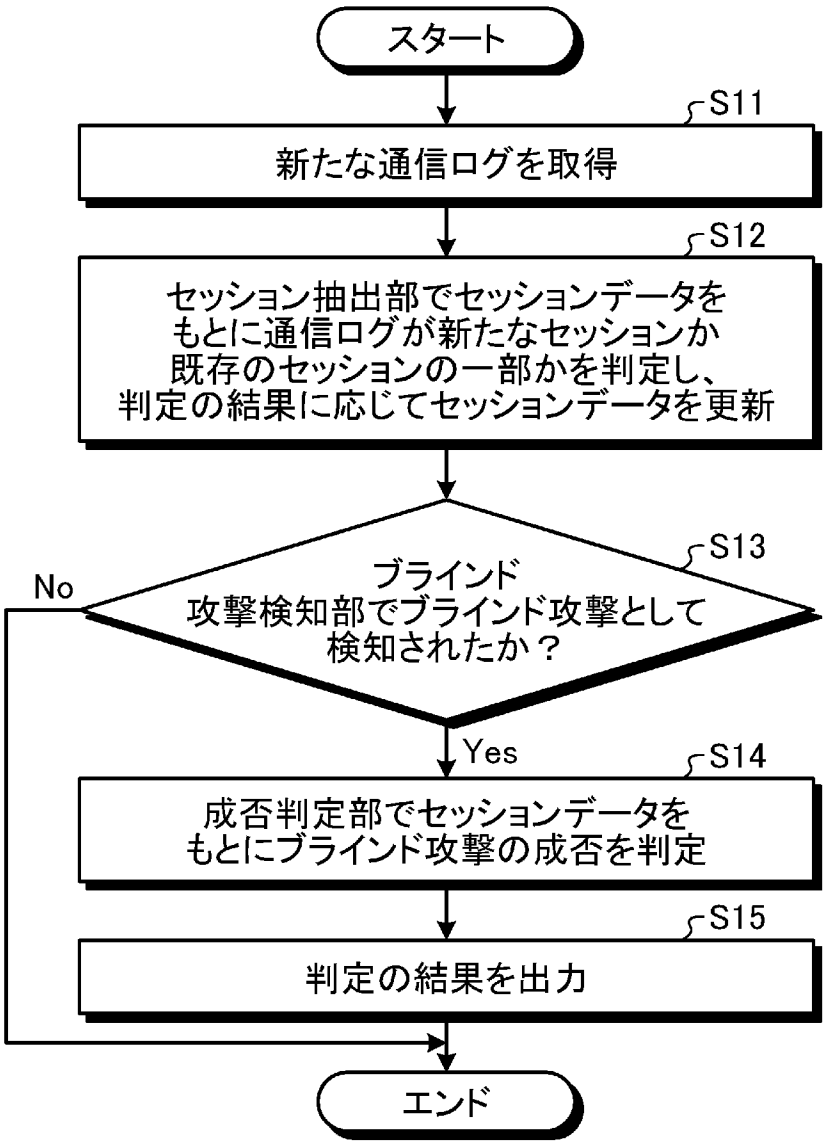
[図4]

No.	攻撃検知	対象箇所	ブラインド攻撃の内容
1			
2	攻撃	パラメタid	AND user() = ‘admin’ #
3	攻撃	パラメタpw	AND user() = ‘admin’ #
4	攻撃	パラメタpw	AND user() != ‘admin’ #
5	攻撃	パラメタid	AND user() != ‘admin’ #
6			

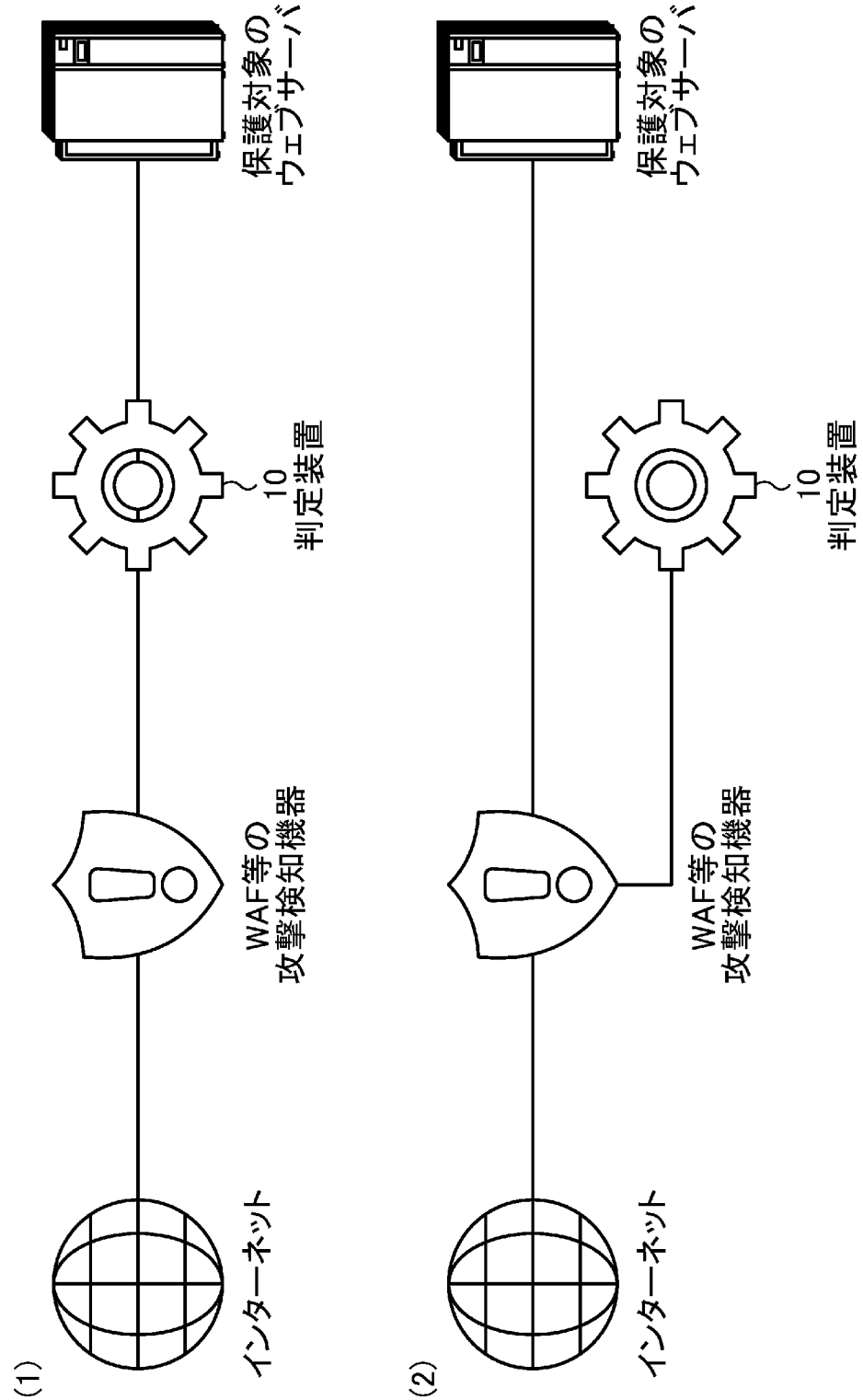
[図5]

No.	攻撃検知	対象箇所	ブラインド攻撃の内容	ステータスコード	レスポンスサイズ	セッション	成否判定
1							
2	攻撃	パラメタid	AND user() = ‘admin’ #	200	100	S1	成功
3	攻撃	パラメタpw	AND user() = ‘admin’ #	200	100	S2	失敗
4	攻撃	パラメタpw	AND user() != ‘admin’ #	200	100	S2	失敗
5	攻撃	パラメタid	AND user() != ‘admin’ #	404	200	S1	成功
6							

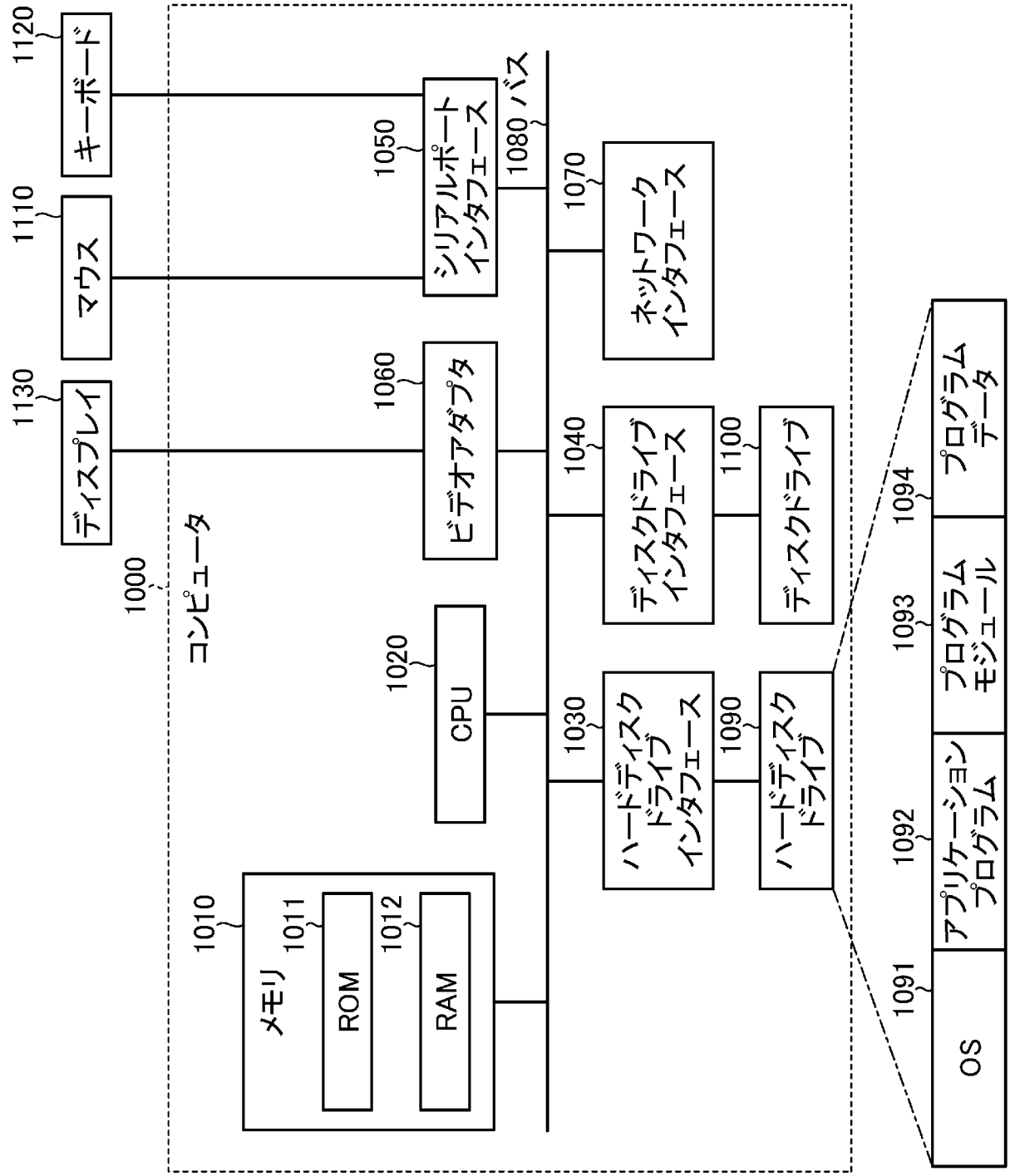
[図6]


スタート
S11
新たな通信ログを取得
S12
セッション抽出部でセッションデータを
もとに通信ログが新たなセッションか
既存のセッションの一部かを判定し、
判定の結果に応じてセッションデータを更新
S13
ブラインド
攻撃検知部でブラインド攻撃として
検知されたか？
No
Yes
S14
成否判定部でセッションデータを
もとにブラインド攻撃の成否を判定
S15
判定の結果を出力
エンド

[図7]


(1)
インターネット
WAF等の
攻撃検知機器
10
判定装置
保護対象の
ウェブサーバ
(2)
インターネット
WAF等の
攻撃検知機器
10
判定装置
保護対象の
ウェブサーバ

[図8]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
バス
1090
ハードディスクドライブ
1100
ディスクドライブ
1110
マウス
1120
キーボード
1130
ディスプレイ
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/JP2021/015759

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)
C06F21/55

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	JP 2002-318734 A (TEAMGIA:KK) 31 October 2002 (2002-10-31) paragraphs [0015]-[0016], [0060]-[0071]	1-5
A	US 2018/0349602 A1 (SAP SE) 06 December 2018 (2018-12-06) paragraphs [0003], [0059], [0240], [0275], fig. 2, 9	1-5

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"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
25 May 2021 (25.05.2021)	08 June 2021 (08.06.2021)

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
Information on patent family members

International application No.
PCT/JP2021/015759

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2002-318734 A	31 Oct. 2002	TW 226984 B	
US 2018/0349602 A1	06 Dec. 2018	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/015759

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
A	JP 2002-318734 A (株式会社チームガイア) 31.10.2002 (2002-10-31) 段落0015-0016,0060-0071	1-5
A	US 2018/0349602 A1 (SAP SE) 06.12.2018 (2018-12-06) 段落0003,0059,0240,0275,図2,9	1-5

☐ C欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“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
25.05.2021	08.06.2021

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）
松平　英 5S 1594
電話番号 03-3581-1101 内線 3545

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/JP2021/015759

引用文献	公表日	パテントファミリー文献	公表日
JP 2002-318734 A	31.10.2002	TW 226984 B	
US 2018/0349602 A1	06.12.2018	（ファミリーなし）	