

(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)



(10) 国際公開番号

WO 2022/219792 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号: PCT/JP2021/015645

(22) 国際出願日: 2021年4月15日(15.04.2021)

(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 N T 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).

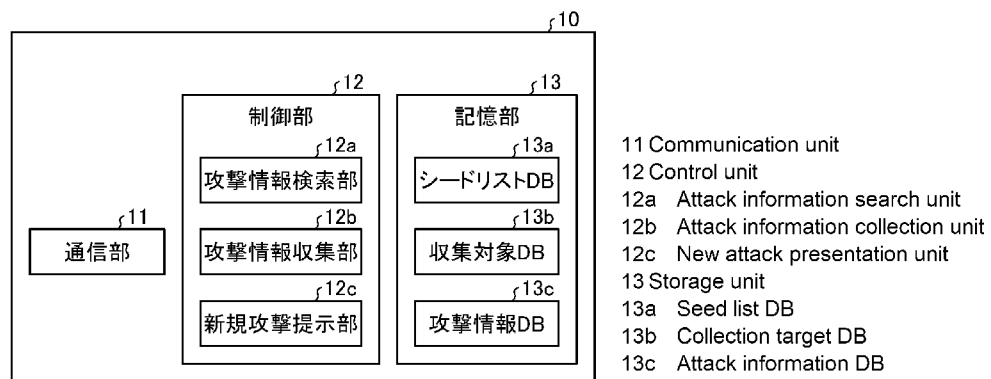
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, 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,

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

(54) 発明の名称: 収集装置、収集方法、および、収集プログラム

[図2]



(57) Abstract: A collection device (10) searches the Internet space for web site information by using a search engine with a keyword indicating the characteristic of a cyberattack serving as a search key, accesses each retrieved web site to collect information on a cyberattack, and presents a newly detected cyberattack from the collected information on a cyberattack.

(57) 要約: 収集装置 (10) は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジンを用いて、インターネット空間からWebサイトの情報を検索し、検索された各Webサイトにアクセスし、サイバー攻撃に関する情報を収集し、収集したサイバー攻撃に関する情報から新規に発見されたサイバー攻撃を提示する。

[続葉有]

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： 収集装置、収集方法、および、収集プログラム

技術分野

[0001] 本発明は、サイバー攻撃に関する情報を収集する、収集装置、収集方法、および、収集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ている一方で、不特定多数からのアクセスが可能である。そのため、Webアプリケーションが脆弱なシステムを有すれば、攻撃に晒されやすいという性質がある。

[0003] 攻撃者は、Webアプリケーションに脆弱性があること発見した場合、インターネット空間に存在する脆弱性を有するWebアプリケーションを事前に探索し、攻撃する傾向にある。そのため、いち早くこの探索および攻撃活動を検知することで、攻撃をあらかじめ遮断するなど早期に対策を行うことが可能となる。

[0004] ここで、Web攻撃を収集する手法は大きく分けて二つある。例えば、ハニーポットを配置し攻撃に関する情報を収集する技術（例えば、非特許文献1参照）がある。また、例えば、通常運用しているWebサーバに対するアクセスログを観測し、アクセスするURLが共起することを利用し、脆弱性スキャンを検知する技術（例えば、非特許文献2参照）がある。

先行技術文献

非特許文献

[0005] 非特許文献1：高対話型 Webハニーポットにおける攻撃情報収集方式の改善、八木 毅、谷本 直人、針生 剛男、伊藤 光恭、CSS、2009

非特許文献2：URLの共起性検知に基づくWebスキャンの実態調査、鐘 揚、折原 慎吾、谷川 真樹、嶋田 創、村瀬 勉、高倉 弘喜、大嶋 嘉人、ICSS、2016

発明の概要

発明が解決しようとする課題

[0006] しかし、従来の技術は、W e b 攻撃に関する情報を効率よく収集することが難しく、早期に攻撃者による未知攻撃を検知することが課題である。例えば、従来の技術は、攻撃の観測環境の規模に依存しており、観測環境の大きさが限られているため、攻撃の最新の動向を効率よく収集できない。また、従来のハニーポットやW e b サーバにおける観測技術では、その観測環境に攻撃が到達した時に攻撃を認識することが可能であるが、攻撃の検知が攻撃開始からどうしても時間が経過してしまうため、早期に攻撃を検知することが困難である。

[0007] そこで、本発明は、前述した問題を解決し、W e b 攻撃に関する情報を効率よく収集し、早期に攻撃者による未知攻撃を検知することを課題とする。

課題を解決するための手段

[0008] 前術した課題を解決するため、本発明の収集装置は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジンを用いて、インターネット空間からW e b サイトの情報を検索する攻撃情報検索部と、検索された各W e b サイトにアクセスし、前記サイバー攻撃に関する情報を収集する攻撃情報収集部と、収集された前記サイバー攻撃に関する情報から新規の前記サイバー攻撃を提示する新規攻撃提示部と、を備えることを特徴とする。

発明の効果

[0009] 本発明によれば、W e b 攻撃に関する情報を効率よく収集し、早期に攻撃者による未知攻撃を提示することができる。

図面の簡単な説明

[0010] [図1]図 1 は、第 1 の実施形態の収集装置を含むシステムの構成例を示す図である。

[図2]図 2 は、第 1 の実施形態の収集装置の構成を示すブロック図である。

[図3]図 3 は、シードリストデータベースに記憶されるシードリストの一例を示す図である。

[図4]図4は、収集対象データベースに記憶される対象Webサイトの検索結果の一例を示す図である。

[図5]図5は、シードリストキーワード毎に収集対象データベースに記憶される検索結果の一例を示す図である。

[図6]図6は、攻撃情報データベースに記憶される攻撃情報の一例を示す図である。

[図7]図7は、攻撃情報検索部の処理の流れの一例を示す図である。

[図8]図8は、攻撃情報収集部の処理の流れの一例を示す図である。

[図9]図9は、異なるアクセスログ形式から攻撃情報を取得する攻撃情報収集部の処理の流れの一例を示す図である。

[図10]図10は、新規攻撃提示部がシードリストを更新する処理の流れの一例を示す図である。

[図11]図11は、収集装置10の処理手順の一例を示すフローチャートである。

[図12]図12は、収集装置10の処理の流れの一例を示す図である。

[図13]図13は、収集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

[0011] 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）である第1の実施形態を説明する。本発明は、実施形態に限定されない。

[0012] [第1の実施形態]

まず、図1を用いて第1の実施形態の収集装置10を含むシステムの構成例を説明する。収集システムは、例えば、ネットワーク1を介して接続される、サーバ上のWebサイト2aと、サーバ上の検索エンジン2bと、端末3と、収集装置10とを備える。

[0013] ネットワーク1は、複数のコンピュータや電子機器などを繋いで信号やデータ、情報をやりとりすることができるコンピュータネットワークのことである。また、ネットワーク1は、有線接続または無線接続のどちらでもよい

。Webサイト2aは、サーバ上に保存されているWebページ群のことを示す。

[0014] 検索エンジン2bは、一般的なあるシステムに存在するデータやファイルを、利用者がキーワードや条件を入力して検索できるようにしたシステムのことを指す。検索エンジン2bの例として、Google社の提供する「Chrome」（登録商標）や、Microsoft社の提供する「Bing」（登録商標）などがあげられる。

[0015] 端末3は、操作者またはサイバー攻撃情報の監視者が操作する電子機器端末である。例えば、端末3は、デスクトップ型PC（Personal Computer）や、ノート型PCや、タブレット端末や、携帯電話機や、PDA（Personal Digital Assistant）等である。

[0016] 収集装置10は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジン2bを用いて、インターネット空間からWebサイト2aの情報を検索し、検索された各Webサイト2aにアクセスし、サイバー攻撃に関する情報を収集し、収集されたサイバー攻撃に関する情報から新規のサイバー攻撃を提示する。

[0017] これにより収集装置10は、検索エンジン2b等を利用してインターネット空間からWeb攻撃に関する情報を効率よく収集し、早期に攻撃者による未知攻撃を提示することができる。

[0018] 次に、図2を用いて、収集装置10の構成例を説明する。同図に示すように、この収集装置10は、通信部11と、制御部12と、記憶部13とを有する。以下に収集装置10が有する各部の処理を説明する。

[0019] 通信部11は、サイバー攻撃を含む各種情報に関する通信を制御する。例えば、通信部11は、ネットワーク1を介して接続される収集装置10、Webサイト2a、検索エンジン2b、および端末3との間でやり取りする各種情報に関する通信を制御する。例えば、通信部11は、サイバー攻撃に関する各種情報を端末3へ送信する。

[0020] 記憶部13は、制御部12による各種処理に必要なデータおよびプログラ

ムを格納する。また、記憶部13は、シードリストデータベース13a（図示では、シードリストDB）、収集対象データベース13b（図示では、収集対象DB）、および攻撃情報データベース13c（図示では、攻撃情報DB）を有する。例えば、記憶部13は、RAM（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、又は、ハードディスク、光ディスク等の記憶装置などである。

[0021] 次に、記憶部13のシードリストデータベース13aについて説明する。シードリストデータベース13aは、サイバー攻撃の特徴を示すキーワードが予め記憶されたシードリストを記憶する。

[0022] シードリストとは、サイバー攻撃の特徴を示す情報であり、シードリストキーワードをリスト上に記憶したもの示すものである。ここで、シードリストキーワードとは、例えば、攻撃者が事前に脆弱性を有するWebアプリケーションを調べる際に用いる検索キーのキーワードを指す。例えば、シードリストキーワードは、OS情報の検索に用いられる「/.env」、ルータ情報の検索に用いられる「/HNAP1」があげられる。

[0023] 図3は、シードリストデータベース13aに記憶されるシードリストの一例を示す図である。例えば、図3に示すように、シードリストデータベース13aは、Webサイト2aの管理システムのURLの一部として用いられる「/phpMyAdmin」を、シードリストキーワードとしてシードリストデータベース13aに記憶する。

[0024] 例えば、シードリストデータベース13aは、予め設定されたシードリストを記憶する。また、シードリストデータベース13aは、後述する新規攻撃提示部12cが提示する新規のシードリストキーワードを、予め設定されたシードリストに上書きして記憶してもよい。

[0025] 次に、記憶部13の収集対象データベース13bについて説明する。収集対象データベース13bは、後述する攻撃情報検索部12aによって定期的に取得されるWebサイト情報を記憶する。

[0026] 収集対象データベース13bは、シードリストキーワード、検索内容、お

よび対象Webサイトを紐づけて記憶する。例えば、収集対象データベース13bは、シードリストデータベース13aから取得するシードリストキーワードの情報を、「シードリストキーワード」の項目（以下、シードリストキーワード項目）に記憶する。また、収集対象データベース13bは、後述する攻撃情報検索部12aが検索エンジン2bに入力した検索キーワード情報を、「検索内容」の項目（以下、検索内容項目）に記憶する。また、収集対象データベース13bは、攻撃対象となり得るWebサイト2aのURL情報を「対象Webサイト」の項目（以下、対象Webサイト項目）に記憶する。

[0027] 図4は、収集対象データベース13bに記憶される対象Webサイトの検索結果の一例を示す図である。例えば、図4に示すように、収集対象データベース13bは、「/phpMyAdmin」をシードリストキーワード項目に記憶する。また、収集対象データベース13bは、検索キーワードである「GET/phpMyAdmin HTTP/1.1」を、検索内容項目に記憶する。また、収集対象データベース13bは、攻撃対象となり得るWebサイト2aのURL情報である「aaa.com/access_log/2021-01-01」を、対象Webサイト項目に記憶する。

[0028] 図5は、シードリストキーワード毎に収集対象データベース13bに記憶される検索結果の一例を示す図である。例えば、図5に示すように、収集対象データベース13bは、シードリストキーワード毎に検索結果を記憶してもよい。

[0029] 例えば、図5に示すように、収集対象データベース13bは、「/HNAP1」をシードリストキーワード項目に記憶し、検索キーワードである「GET/HNAP1 HTTP/1.1」を検索内容項目に記憶し、シードリストキーワード「/HNAP1」の検索結果として、攻撃対象となり得るWebサイト2aのURL情報である「bbb.com/access_log/2021-01-01」を対象Webサイト項目に記憶する。

[0030] 例えば、図5に示すように、収集対象データベース13bは、「/.env」をシードリストキーワード項目に記憶し、検索キーワードである「GET/.env HTTP/1.1」を検索内容項目に記憶し、シードリストキーワード「/.env」の検

索結果として、攻撃対象となり得るWebサイト2aのURL情報である「cc.com/access_log/2021-01-01」を対象Webサイト項目に記憶する。

[0031] 次に、記憶部13の攻撃情報データベース13cについて説明する。攻撃情報データベース13cは、後述する攻撃情報収集部12bによって取得されるWebサイト情報へのサイバー攻撃情報を記憶する。

[0032] 図6は、攻撃情報データベース13cに記憶される攻撃情報の一例を示す図である。例えば、攻撃情報データベース13cは、メソッド情報である「GET」を攻撃情報のメソッドの項目に記憶する。また、攻撃情報データベース13cは、検索キーワードである「/phpMyAdmin」を、攻撃情報の検索キーワード項目に記憶する。

[0033] また、攻撃情報データベース13cは、サイバー攻撃を受けたWebサイト2aのURL情報である「aaa.com/access_log/2021-01-01」を、URLの項目に記憶する。また、攻撃情報データベース13cは、サイバー攻撃情報を受けた時刻を示す攻撃時刻である「2021-01-01」を、攻撃時刻の項目に記憶する。

[0034] 攻撃情報データベース13cは、HTTPリクエストで用いられたメソッド情報、攻撃対象のWebサイト2aのURL情報、サイバー攻撃情報を受けた時刻を示す攻撃時刻、を紐づけて記憶する。

[0035] 続いて、制御部12について説明する。制御部12は、収集装置10全体の制御を司る。制御部12は、攻撃情報検索部12aと、攻撃情報収集部12bと、新規攻撃提示部12cと、を備える。制御部12は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行する。

[0036] 例えば、制御部12は、攻撃情報検索部12aと、攻撃情報収集部12bと、新規攻撃提示部12cとを有する。ここで、制御部12は、CPU (Central Processing Unit) やMPU (Micro Processing Unit) などの電子回路やASIC (Application Specific Integrated Circuit) やFPGA (Field Programmable Gate Array) などの集積回路である。

[0037] まず、制御部 12 の攻撃情報検索部 12 a について説明する。攻撃情報検索部 12 a は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジン 2 b を用いて、インターネット空間から Web サイト 2 a の情報を検索する。

[0038] 例えば、攻撃情報検索部 12 a は、サイバー攻撃の特徴を示すキーワードが予め記憶されたシードリストに基づいて、シードリストのキーワード毎に検索キーワードを作成し、作成した検索キーワード毎に、検索エンジン 2 b を用いて Web サイト 2 a の情報を検索する。また、攻撃情報検索部 12 a は、収集した Web サイト 2 a の URL 情報および検索キーワードを、収集対象データベース 13 b に格納する。

[0039] 図 7 は、攻撃情報検索部 12 a の処理の流れの一例を示す図である。例えば、攻撃情報検索部 12 a は、シードリストデータベース 13 a から一つのシードリストキーワードを取得する。

[0040] そして、攻撃情報検索部 12 a は、予め記憶されたキーワードを組み合わせ、一つのシードリストキーワードに対して複数の検索キーワードを作成する。例えば、攻撃情報検索部 12 a は、取得したシードリストキーワードの前後に、メソッド情報等である「GET」、「HTTP /1.1」を追加し、検索キーワードを作成する。

[0041] 検索キーワードとは、攻撃情報検索部 12 a が検索エンジン 2 b に入力、および検索をかける際に用いるキーワードのことを指す。検索キーワードを作成する際に用いられる、予め設定された組み合わせのキーワードの例として、「GET」、「POST」、「HTTP /1.0」、「HTTP /2」、などがあげられる。このとき、シードリストキーワードと検索キーワードの総数比は、1 : N の関係である。

[0042] そして、攻撃情報検索部 12 a は、作成した検索キーワード毎に検索エンジン 2 b で該当する Web サイト 2 a を定期的に検索する。攻撃情報検索部 12 a は、検索キーワード毎に Web サイト 2 a の URL 情報を記憶する。このとき、検索キーワードと検索された Web サイト 2 a の総数比は、1 :

Nの関係である。また、シードリストキーワードと検索キーワードと検索されたWebサイト2aの総数比は、 $1 : N : N^2$ の関係である。

[0043] 続いて、攻撃情報検索部12aは、シードリストキーワードの項目として、シードリストデータベース13aから取得したシードリストキーワードの情報を格納し、検索内容の項目として、作成した検索キーワード情報を格納し、対象Webサイトの項目として、Webサイト2aのURL情報を収集対象データベース13bに格納する。つまり、攻撃情報検索部12aは、シードリストキーワードと検索内容と対象Webサイトを紐づけて格納する。

[0044] 例えば、図7に示すように、攻撃情報検索部12aは、シードリストデータベース13aから取得する複数のシードリストキーワードとして「/phpMyAdmin」、「/.env」、「/HNAP1」、を取得する。次に、攻撃情報検索部12aは、シードリストキーワード“/phpMyAdmin”の検索キーワードとして「GET /phpMyAdmin HTTP /1.1」を作成する。攻撃情報検索部12aは、検索キーワード「GET /phpMyAdmin HTTP /1.1」を用いて、インターネット空間に存在する公開されたアクセスログからWeb攻撃の対象となり得るWebサイト2aを検索する。

[0045] そして、攻撃情報検索部12aは、検索キーワード「GET /phpMyAdmin HTTP /1.1」の検索結果からヒットしたWebサイト2aを、対象Webサイトとして収集対象データベース13bに格納する。例えば、攻撃情報検索部12aは、Webサイト2aのURL情報である「aaa.com/access_log/2021-01-01」、「bbb.com/blog/bbb.html」、「ccc.com/stats/index.html」、「ddd.com/」を対象Webサイトの項目に格納し、検索キーワード「GET /phpMyAdmin HTTP /1.1」と紐づけて格納する。

[0046] また、例えば、攻撃情報検索部12aが、シードリストキーワード“/phpMyAdmin”を用いて、検索キーワード「POST /phpMyAdmin HTTP/1.0」を作成した場合、攻撃情報検索部12aは、検索キーワード「POST /phpMyAdmin HTTP/1.0」を用いて、インターネット空間に存在する公開されたアクセスログからWeb攻撃の対象となり得るWebサイト2aを検索する。

- [0047] そして、攻撃情報検索部 12a は、検索キーワード「POST /phpMyAdmin HTTP/1.0」の検索結果からヒットしたWebサイト 2a を、対象Webサイトとして収集対象データベース 13b に格納する。例えば、収集対象データベース 13b は、対象Webサイトの項目として、Webサイト 2a のURL 情報である「eee.com/access_log/2021-01-01」、「ggg.com/blog/bbb.html」を、検索キーワード「POST /phpMyAdmin HTTP/1.0」と紐づけて格納する。
- [0048] また、例えば、攻撃情報検索部 12a が、シードリストキーワード“/phpMyAdmin”を用いて、検索キーワード「GET /phpMyAdmin HTTP/2」を作成した場合、攻撃情報検索部 12a は、検索キーワード「GET /phpMyAdmin HTTP/2」を用いて、インターネット空間に存在する公開されたアクセスログからWeb攻撃の対象となり得るWebサイト 2a を検索する。
- [0049] 攻撃情報検索部 12a は、検索キーワード「GET /phpMyAdmin HTTP/2」の検索結果からヒットしたWebサイト 2a を、対象Webサイトとして収集対象データベース 13b に格納する。例えば、収集対象データベース 13b は、対象Webサイトの項目として、Webサイト 2a のURL 情報である「hhh.com/stats/index.html」、「kkk.com/」を、検索キーワード「GET /phpMyAdmin HTTP/2」と紐づけて格納する。
- [0050] 次に、制御部 12 の攻撃情報収集部 12b について説明する。攻撃情報収集部 12b は、収集された各Webサイト 2a にアクセスし、サイバー攻撃に関する情報を収集する。
- [0051] 例えば、攻撃情報収集部 12b は、Webサイト 2a にアクセスし、Webサイト 2a のアクセスログからサイバー攻撃に関する情報を収集し、アクセスログに記されたステータスコードにより攻撃の有無を判定し、判定結果に応じて、攻撃情報より攻撃した日時を示す攻撃時刻および検索キーワードの情報を収集する。
- [0052] また、例えば、攻撃情報収集部 12b は、攻撃情報より攻撃時刻および検索キーワードの情報を定期的に収集し、攻撃時刻が最新の日時に更新される

まで最新のアクセスログ情報を収集し、収集した各攻撃情報を予め定めた形式に整形し、攻撃情報を収集する攻撃情報データベース 13c に格納する。

[0053] 図8は、攻撃情報収集部 12b の処理の流れの一例を示す図である。図8に示すように、攻撃情報収集部 12b は、対象Webサイト「aaa.com/access_log/2021-01-01」にアクセスし、アクセスログから攻撃情報を取得する。掲載されるアクセスログ情報には、攻撃を意図しない正常のアクセスも含まれる。そのため、攻撃情報収集部 12b は、例えば、アクセスログに記されたステータスコードが400番台の場合を攻撃として判定する。

[0054] 攻撃の有無の判定方法は、予め設定されているものとし、後から条件を変更することも可能である。攻撃情報収集部 12b は、攻撃と判定したアクセスログ情報を収集し、攻撃情報データベース 13c に格納する。

[0055] 例えば、Webサイト 2a のURLに「2021-01-01」や「2021/01/01」のような日付が存在する場合、攻撃情報収集部 12b は、日付部分の情報を整形し、さらに、最新の日付になるまでアクセスログ情報を収集する。

[0056] 例えば、攻撃情報収集部 12b は、メソッド情報である「GET」を攻撃情報データベース 13c の攻撃情報のメソッドの項目に格納する。また、攻撃情報収集部 12b は、検索キーワードである「/phpMyAdmin」を、攻撃情報データベース 13c の攻撃情報の検索キーワード項目に格納する。

[0057] また、攻撃情報収集部 12b は、サイバー攻撃を受けたWebサイト 2a のURL情報である「aaa.com/access_log/2021-01-01」を、攻撃情報データベース 13c のURLの項目に格納する。また、攻撃情報収集部 12b は、サイバー攻撃を受けた時刻を示す攻撃時刻である「2021-01-01」を、攻撃情報データベース 13c の攻撃時刻の項目に格納する。

[0058] また、Webページの掲載内容には、ログの形式で記されている場合や、整形されたテーブルやリストのような形式で掲載されている場合もある。図9は、異なるアクセスログ形式から攻撃情報を取得する攻撃情報収集部 12b の処理の流れの一例を示す図である。

[0059] 図9に示すように、攻撃情報収集部 12b は、テーブルやリスト形式の値

から、攻撃情報に相当する部分を切り出して取得する。例えば、攻撃情報収集部 12 b は、メソッド情報である「GET」を攻撃情報データベース 13 c の攻撃情報のメソッドの項目に格納する。また、攻撃情報収集部 12 b は、検索キーワードである「/CFIDE/administrator/」を、攻撃情報データベース 13 c の攻撃情報の検索キーワード項目に格納する。

[0060] また、攻撃情報収集部 12 b は、サイバー攻撃を受けた Web サイト 2 a の URL 情報である「bbb.com/blog/bbb.html」を、攻撃情報データベース 13 c の URL の項目に格納する。また、攻撃情報収集部 12 b は、サイバー攻撃を受けた時刻を示す攻撃時刻である「2021-01-01」を、攻撃情報データベース 13 c の攻撃時刻の項目に格納する。

[0061] このように、攻撃情報収集部 12 b は、異なるアクセスログ形式から攻撃情報に相当する部分を切り出して取得することができる。

[0062] 次に、制御部 12 の新規攻撃提示部 12 c について説明する。新規攻撃提示部 12 c は、収集されたサイバー攻撃に関する情報から新規のサイバー攻撃を提示する。

[0063] 例えば、新規攻撃提示部 12 c は、収集された攻撃情報から新規に発見されたサイバー攻撃をユーザに提示し、新規の検索キーワードに関する情報を検出すると、未知の攻撃と判定し、シードリストに新規の検索キーワードの情報を更新する。

[0064] 図 10 は、新規攻撃提示部 12 c がシードリストを更新する処理の流れの一例を示す図である。例えば、図 10 に示すように、新規攻撃提示部 12 c は、収集した攻撃情報から既存の攻撃情報と照合し、新規に発見された攻撃である「/CFIDE/administrator/」を検出する。新規攻撃提示部 12 c は、新規に発見された攻撃を検出すると、攻撃情報データベース 13 c の該当する項目を「未知攻撃」として情報を更新する。

[0065] 例えば、図 10 に示すように、新規攻撃提示部 12 c は、新規に発見された攻撃である「/CFIDE/administrator/」の行の「未知攻撃」の項目に「YES」の値を追記する。

[0066] そして、新規攻撃提示部 12c は、新規に発見された攻撃である「/CFIDE/administrator/」を未知の攻撃として、操作者または監視者の端末 3 に攻撃情報を提示する。また、新規攻撃提示部 12c は、新規に発見された攻撃である「/CFIDE/administrator/」をシードリストキーワードと認定し、シードリストデータベース 13a に更新する。

[0067] このように、収集装置 10 は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジン 2b を用いて、インターネット空間から Web サイト 2a の情報を検索し、検索された各 Web サイト 2a にアクセスし、サイバー攻撃に関する情報を収集し、収集されたサイバー攻撃に関する情報から新規のサイバー攻撃を提示する。

[0068] また、収集装置 10 は、予め設定されるシードリストキーワードを用いて、多様に検索キーワードを作成することで、サイバー攻撃の対象となり得る Web サイト 2a を効果的に収集することができる。さらに、収集装置 10 は、シードリストを更新することで、常に最新のアクセスログ情報を収集し、汎用的な攻撃情報およびシードリストを取得することができる。加えて、収集装置 10 は、ハニーポットや Web サーバなどの観測環境に依存せずに、インターネット空間上の検索エンジン 2b を用いて、攻撃情報を収集することができる。

[0069] つまり、収集装置 10 は、サイバー攻撃の対象となり得る Web サイト 2a を事前に把握し、監視対象の Web サイト 2a を限定することで、早期に、攻撃者による未知攻撃を検出し、監視者の最新の攻撃動向の把握に貢献することができるという効果を奏する。

[0070] [収集装置の処理の一例]

次に、図 11 を用いて、収集装置 10 の処理について説明する。図 11 は、収集装置 10 の処理手順の一例を示すフローチャートである。

[0071] 図 11 に示すように、収集装置 10 の攻撃情報検索部 12a は、シードリストに基づき、検索エンジン 2b で攻撃情報を掲載する Web サイト 2a の情報を取得する（S1）。

[0072] 例えば、攻撃情報検索部 12a は、シードリストデータベース 13a から一つのシードリストキーワードを取得する。そして、収集装置 10 は、予め記憶されたキーワードを組み合わせ、一つのシードリストキーワードに対して複数の検索キーワードを作成する。そして、攻撃情報検索部 12a は、作成した検索キーワード毎に検索エンジン 2b で該当する Web サイト 2a を検索する。

[0073] そして、攻撃情報収集部 12b は、S1 で収集された Web サイト 2a の URL 情報に基づき、Web サイト 2a の攻撃情報を取得する (S2)。

[0074] 例えば、攻撃情報収集部 12b は、インターネット空間に公開されたアクセスログからサイバー攻撃に関する情報を収集し、アクセスログに記されたステータスコードにより攻撃の有無を判定し、判定結果に応じて、攻撃情報より攻撃した日時を示す攻撃時刻および検索キーワードの情報を収集する。

[0075] 続いて、新規攻撃提示部 12c は、S2 で取得した攻撃情報を端末 3 に出力し、新規の検索キーワードをシードリストデータベース 13a に更新する (S3)。収集装置 10 は、S1 から S3 の一連の処理の流れを繰り返し、最新の攻撃情報を取得する。つまり、収集装置 10 は、シードリストデータベース 13a が更新された後、新規の検索キーワードを用いて、新に Web サイト 2a を検索し、最新の攻撃情報を取得する処理を繰り返す。

[0076] 図 12 は、収集装置 10 の処理の流れの一例を示す図である。例えば、図 12 に示すように、収集装置 10 は、シードリストデータベース 13a を用いて、脆弱性を有する Web アプリケーションのキーワードを検索キーとして、検索エンジン 2b から Web サイト 2a を検索する。

[0077] そして、収集装置 10 は、サイバー攻撃の対象となり得る Web サイト 2a のアクセスログを取得して、攻撃情報を収集装置 10 の保有するデータベースに蓄積する。続いて、収集装置 10 は、蓄積した攻撃情報を用いて定期的に対象の Web サイト 2a を監視し、新しい攻撃情報を検知した場合は、監視者の端末 3 へ提示する。

[0078] [実施の形態 1 の効果]

収集装置 10 は、サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジン 2 b を用いて、インターネット空間から Web サイト 2 a の情報を検索し、検索された各 Web サイト 2 a にアクセスし、サイバー攻撃に関する情報を収集し、収集されたサイバー攻撃に関する情報から新規のサイバー攻撃を提示する。

[0079] これにより収集装置 10 は、検索エンジン 2 b 等を利用してインターネット空間から Web 攻撃に関する情報を効率よく収集し、早期に攻撃者による未知攻撃を提示することができる。

[0080] また、収集装置 10 は、サイバー攻撃の特徴を示すキーワードが予め記憶されたシードリストに基づいて、シードリストのキーワード毎に検索キーワードを作成し、作成した検索キーワード毎に、検索エンジン 2 b を用いて Web サイト 2 a の情報を検索することができる。

[0081] これにより収集装置 10 は、予め設定されるシードリストキーワードを用いて、多様に検索キーワードを作成し、サイバー攻撃の対象となり得る Web サイト 2 a を効果的に収集することができる。

[0082] また、収集装置 10 は、Web サイト 2 a にアクセスし、Web サイト 2 a のアクセスログからサイバー攻撃に関する情報を収集し、アクセスログに記されたステータスコードにより攻撃の有無を判定し、判定結果に応じて、攻撃情報より攻撃した日時を示す攻撃時刻および検索キーワードに関する情報を収集することができる。

[0083] これにより収集装置 10 は、異なるアクセスログ形式から、アクセスログに記されたステータスコードを用いて、攻撃時刻を含む詳細な攻撃情報を収集することができる。

[0084] また、収集装置 10 は、攻撃情報より攻撃時刻および検索キーワードの情報を定期的に収集し、攻撃時刻が最新の日時に更新されるまで最新のアクセスログ情報を収集し、収集した各攻撃情報を予め定めた形式に整形し、攻撃情報を収集する攻撃情報データベース 13 c に格納することができる。

[0085] これにより収集装置 10 は、日常的に最新のアクセスログ情報を収集し、

汎用的な攻撃情報およびシードリストを取得することができる。

[0086] また、収集装置 10 は、収集した攻撃情報から新規に発見されたサイバー攻撃をユーザに提示し、新規の検索キーワードを検出すると、未知の攻撃と判定し、シードリストに新規の検索キーワードの情報を更新することができる。

[0087] これにより収集装置 10 は、早期に攻撃者による未知攻撃を監視者に提示することで、監視者は最新の攻撃動向を把握することができる。

[0088] [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。

[0089] 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。

[0090] [プログラム]

前記した収集装置 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、情報処理装置を各実施形態の収集装置 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。

[0091] また、収集装置 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。

[0092] 図 13 は、収集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、CPU 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。

[0093] 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。

[0094] ハードディスクドライブ 1090 は、例えば、OS 1091、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 1 0 9 4 を記憶する。すなわち、上記の収集装置 1 0 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 1 0 9 3 として実装される。プログラムモジュール 1 0 9 3 は、例えばハードディスクドライブ 1 0 9 0 に記憶される。例えば、収集装置 1 0 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 1 0 9 3 が、ハードディスクドライブ 1 0 9 0 に記憶される。なお、ハードディスクドライブ 1 0 9 0 は、SSDにより代替されてもよい。

[0095] また、上述した実施形態の処理で用いられる各データは、プログラムデータ 1 0 9 4 として、例えばメモリ 1 0 1 0 やハードディスクドライブ 1 0 9 0 に記憶される。そして、CPU 1 0 2 0 が、メモリ 1 0 1 0 やハードディスクドライブ 1 0 9 0 に記憶されたプログラムモジュール 1 0 9 3 やプログラムデータ 1 0 9 4 を必要に応じて RAM 1 0 1 2 に読み出して実行する。

[0096] なお、プログラムモジュール 1 0 9 3 やプログラムデータ 1 0 9 4 は、ハードディスクドライブ 1 0 9 0 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 1 1 0 0 等を介して CPU 1 0 2 0 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 1 0 9 3 及びプログラムデータ 1 0 9 4 は、ネットワークされたーク (LAN (Local Area Network)、WAN (Wide Area Network) 等) を介して接続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 1 0 9 3 及びプログラムデータ 1 0 9 4 は、他のコンピュータから、ネットワークインタフェース 1 0 7 0 を介して CPU 1 0 2 0 によって読み出されてもよい。

符号の説明

- [0097] 1 ネットワーク
- 2 a Web サイト (サーバ)
- 2 b 検索エンジン (サーバ)
- 3 端末
- 1 0 収集装置
- 1 1 通信部

- 1 2 制御部
 - 1 2 a 攻撃情報検索部
 - 1 2 b 攻撃情報収集部
 - 1 2 c 新規攻撃提示部
- 1 3 記憶部
 - 1 3 a シードリストデータベース
 - 1 3 b 収集対象データベース
 - 1 3 c 攻撃情報データベース

請求の範囲

- [請求項1] サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジンを用いて、インターネット空間からWebサイトの情報を検索する攻撃情報検索部と、
- 検索された各Webサイトにアクセスし、前記サイバー攻撃に関する情報を収集する攻撃情報収集部と、
- 収集された前記サイバー攻撃に関する情報から新規のサイバー攻撃を提示する新規攻撃提示部と、
- を備えることを特徴とする収集装置。
- [請求項2] 前記攻撃情報検索部が、
- 前記サイバー攻撃の特徴を示すキーワードが予め記憶されたシードリストに基づいて、前記シードリストのキーワード毎に検索キーワードを作成し、
- 作成した前記検索キーワード毎に、検索エンジンを用いて前記Webサイトの情報を検索することを特徴とする請求項1に記載の収集装置。
- [請求項3] 前記攻撃情報収集部が、
- 前記Webサイトにアクセスし、前記Webサイトのアクセスログから前記サイバー攻撃に関する情報を収集し、
- 前記アクセスログに記されたステータスコードにより攻撃の有無を判定し、判定結果に応じて、前記サイバー攻撃に関する情報より攻撃した日時を示す攻撃時刻および検索キーワードに関する情報を収集する
- ことを特徴とする請求項1に記載の収集装置。
- [請求項4] 前記攻撃情報収集部が、
- 前記サイバー攻撃に関する情報より攻撃した日時を示す攻撃時刻および検索キーワードに関する情報を定期的に収集し、
- 前記攻撃時刻が最新の日時に更新されるまで最新のアクセスログ情

報を収集し、

収集した前記サイバー攻撃に関する情報を予め定めた形式に整形し

、

攻撃情報を収集する攻撃情報データベースに格納する

ことを特徴とする請求項 1 に記載の収集装置。

[請求項5]

前記新規攻撃提示部が、

収集された前記サイバー攻撃に関する情報から新規の前記サイバー攻撃をユーザに提示し、

新規の検索キーワードに関する情報を検出すると、未知の攻撃と判定し、

前記サイバー攻撃の特徴を示すキーワードが予め記憶されたシードリストに前記新規の検索キーワードの情報を更新する

ことを特徴とする請求項 1 に記載の収集装置。

[請求項6]

収集装置により実行される収集方法であって、

サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジンを用いて、インターネット空間からWebサイトの情報を検索する工程と、

検索された各Webサイトにアクセスし、前記サイバー攻撃に関する情報を収集する工程と、

収集した前記サイバー攻撃に関する情報から新規に発見された前記サイバー攻撃を提示する工程と、

を含むことを特徴とする収集方法。

[請求項7]

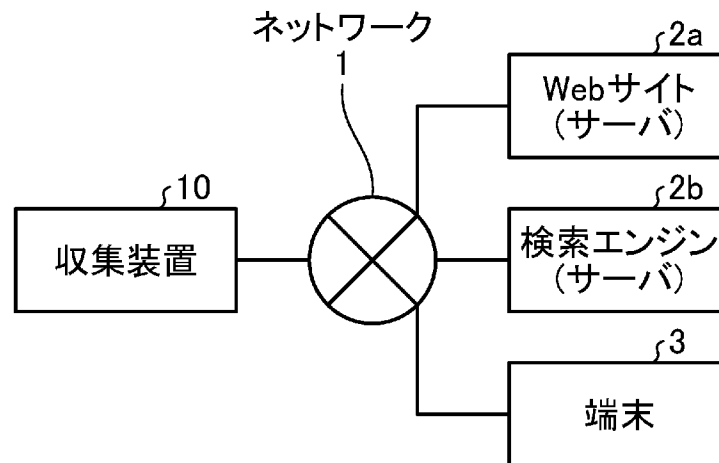
サイバー攻撃の特徴を示すキーワードを検索キーとして、検索エンジンを用いて、インターネット空間からWebサイトの情報を検索する工程と、

検索された各Webサイトにアクセスし、前記サイバー攻撃に関する情報を収集する工程と、

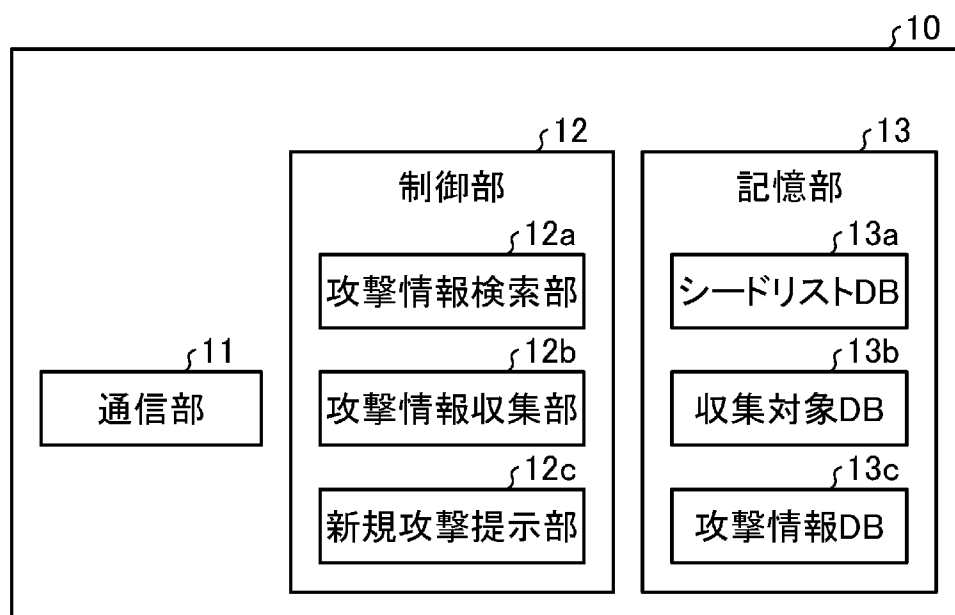
収集した前記サイバー攻撃に関する情報から新規に発見された前記

サイバー攻撃を提示する工程と、
をコンピュータに実行させることを特徴とする収集プログラム。

[図1]



[図2]



[図3]

シードリスト
/phpMyAdmin
/.env
/HNAP1
...

[図4]

シードリスト キーワード	検索内容	対象Webサイト
/phpMyAdmin	GET /phpMyAdmin HTTP/1.1	aaa.com/access_log/2021-01-01
		bbb.com/blog/bbb.html
		ccc.com/stats/index.html
		ddd.com/
...		...
	POST /phpMyAdmin HTTP/1.0	eee.com/access_log/2021-01-01
		ggg.com/blog/bbb.html
...		...
	GET /phpMyAdmin HTTP/2	hhh.com/stats/index.html
		kkk.com/
	...	...

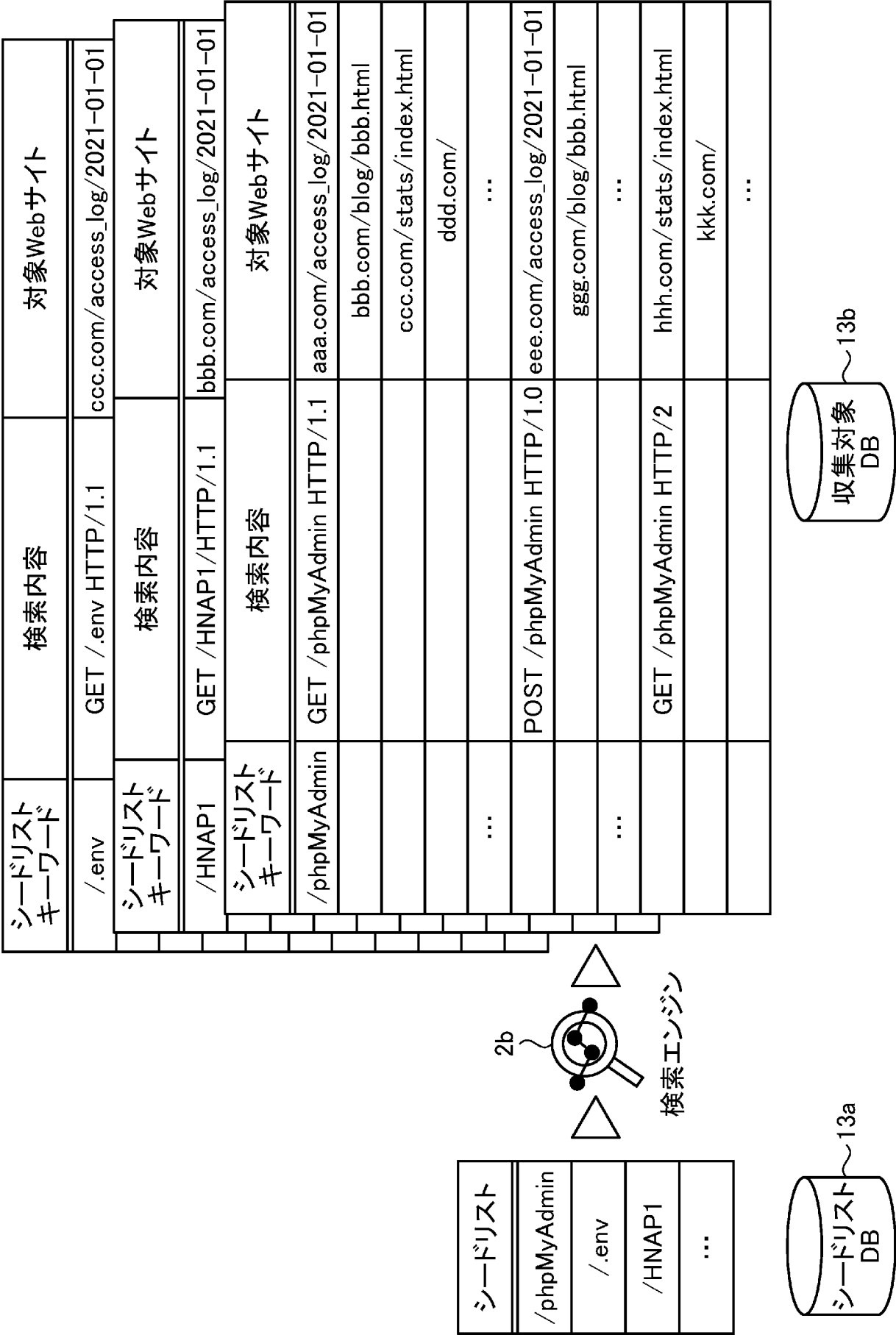
[図5]

シードリスト キーワード	検索内容	対象Webサイト
/ .env	GET /.env HTTP/1.1	ccc.com/access_log/2021-01-01
シードリスト キーワード	検索内容	対象Webサイト
/HNAP1	GET /HNAP1/HTTP/1.1	bbb.com/access_log/2021-01-01
シードリスト キーワード	検索内容	対象Webサイト
/phpMyAdmin	GET /phpMyAdmin HTTP/1.1	aaa.com/access_log/2021-01-01
		bbb.com/blog/bbb.html
		ccc.com/stats/index.html
		ddd.com/
...		...
	POST /phpMyAdmin HTTP/1.0	eee.com/access_log/2021-01-01
		ggg.com/blog/bbb.html
...		...
	GET /phpMyAdmin HTTP/2	hhh.com/stats/index.html
		kkk.com/
		...

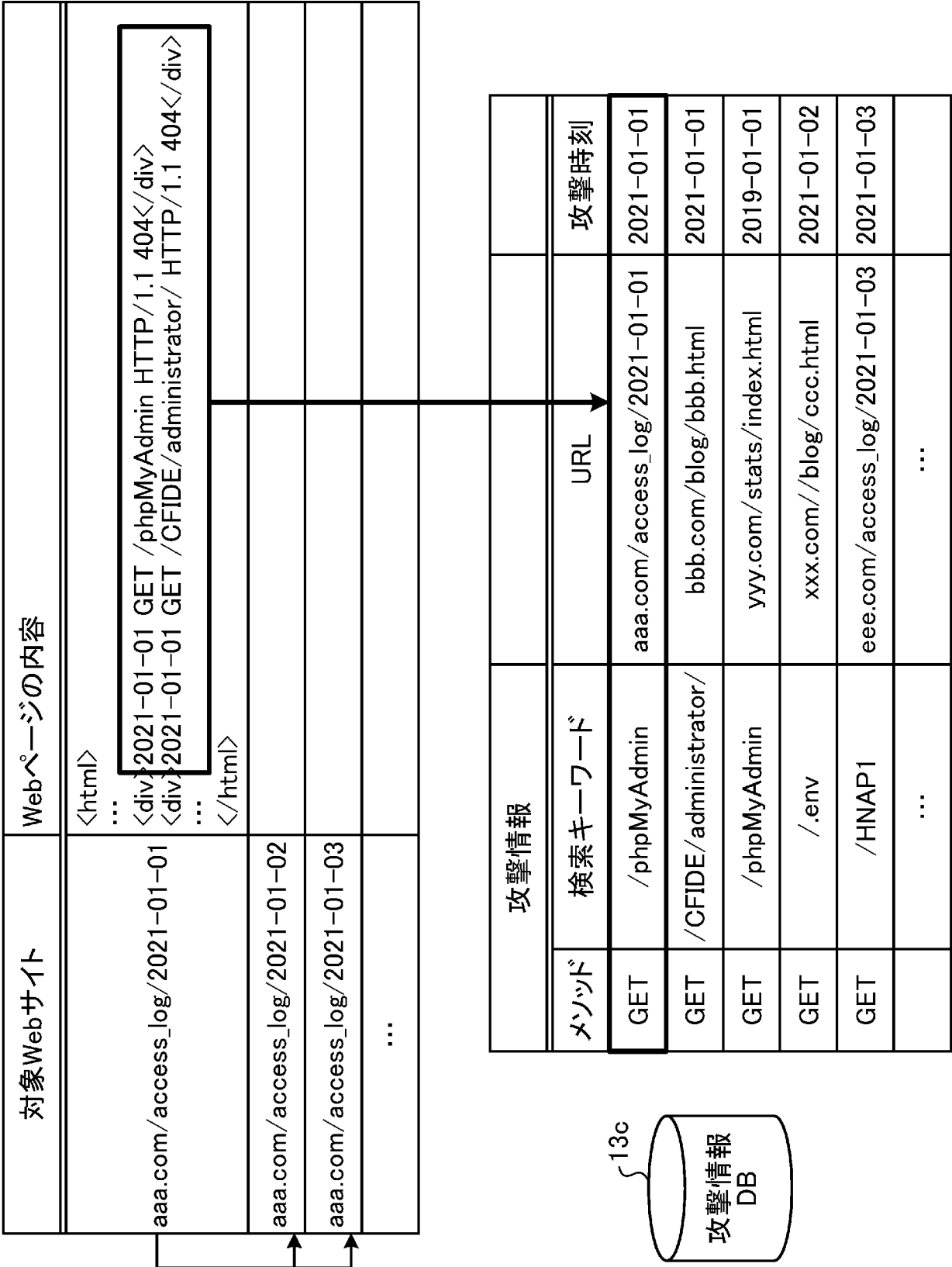
[図6]

攻撃情報			
メソッド	検索キーワード	URL	攻撃時刻
GET	/phpMyAdmin	aaa.com/access_log/2021-01-01	2021-01-01
GET	/CFIDE/administrator/	bbb.com/blog/bbb.html	2021-01-01
GET	/phpMyAdmin	yyy.com/stats/index.html	2019-01-01
GET	/.env	xxx.com//blog/ccc.html	2021-01-02
GET	/HNAP1	eee.com/access_log/2021-01-03	2021-01-03
	...	...	

[図7]



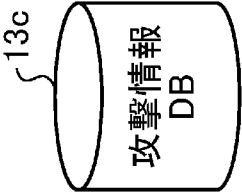
[図8]



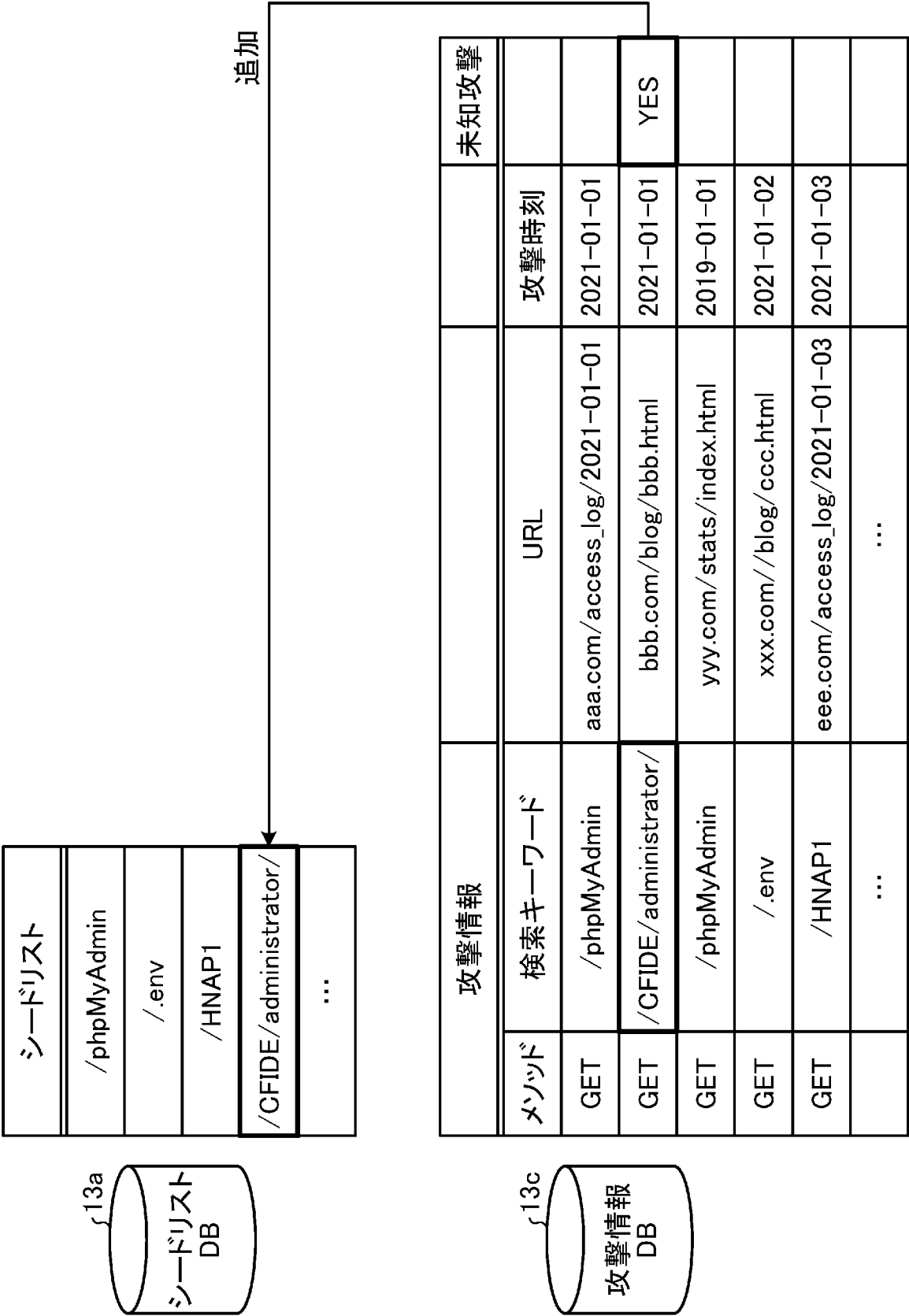
[図9]

対象Webサイト	Webページの内容
bbb.com/blog/bbb.html	<html> ... <table> <tr><td>2021-01-01</td><td>GET</td> <td>/phpMyAdmin </td><td>HTTP/1.1</td><td>404</td></tr> <tr><td>2021-01-01</td><td>GET</td> <td>/CFIDE/administrator/</td><td>HTTP/1.1</td><td>404</td></tr> ... </table> </html>
...	

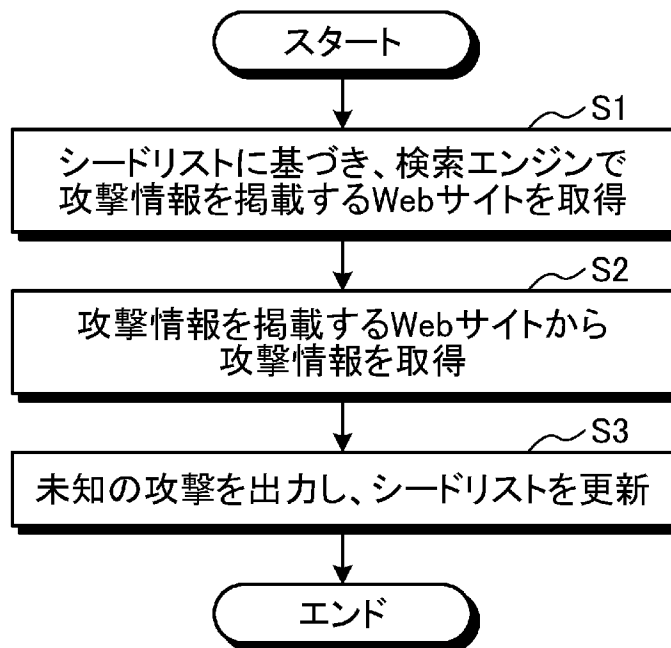
攻撃情報			
メソッド	検索キーワード	URL	攻撃時刻
GET	/phpMyAdmin	aaa.com/access_log/2021-01-01	2021-01-01
GET	/CFIDE/administrator/	bbb.com/blog/bbb.html	2021-01-01
GET	/phpMyAdmin	yyy.com/stats/index.html	2019-01-01
GET	/env	xxx.com//blog/ccc.html	2021-01-02
GET	/HNAP1	eee.com/access_log/2021-01-03	2021-01-03
	...	...	



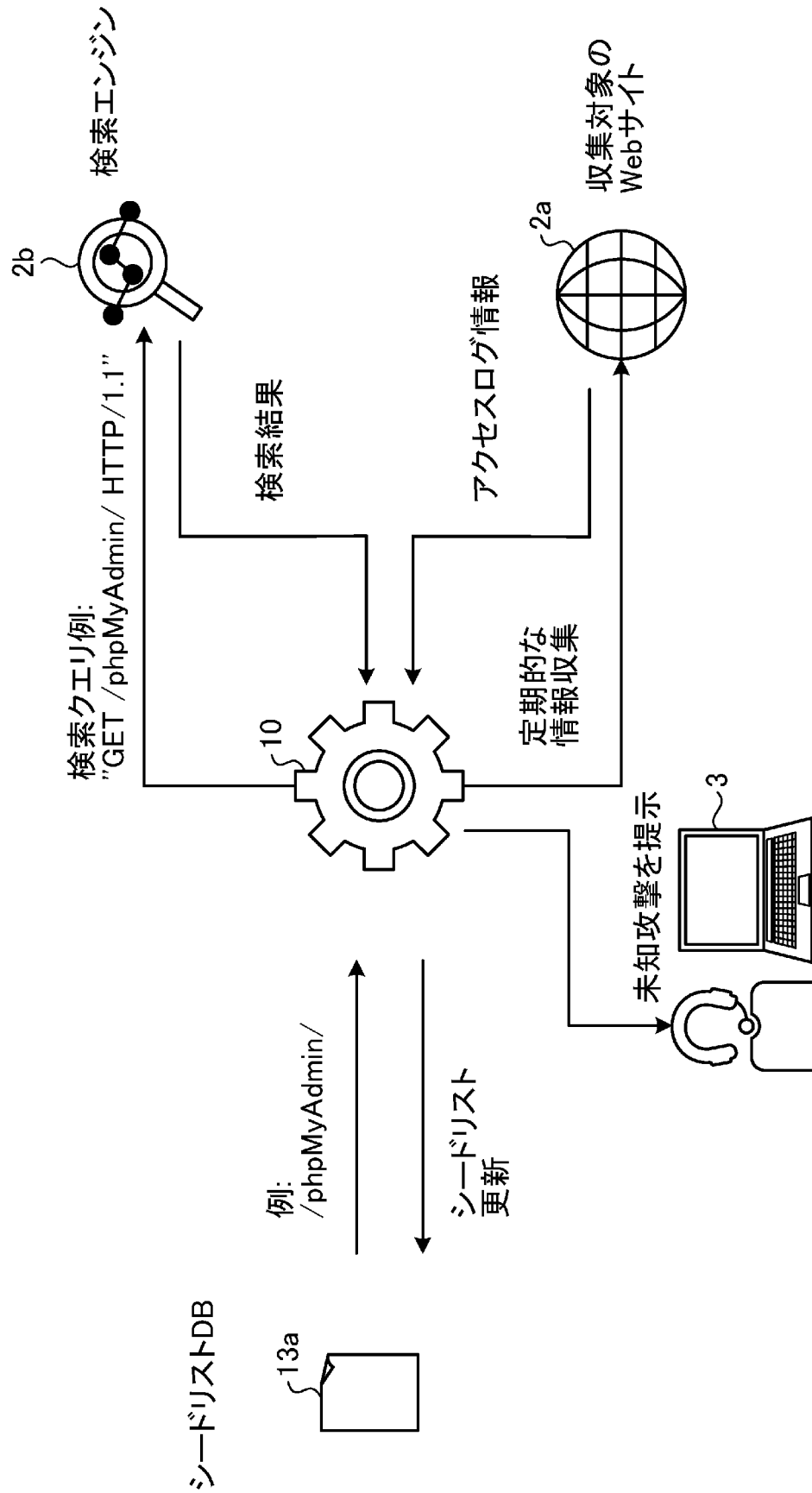
[図10]



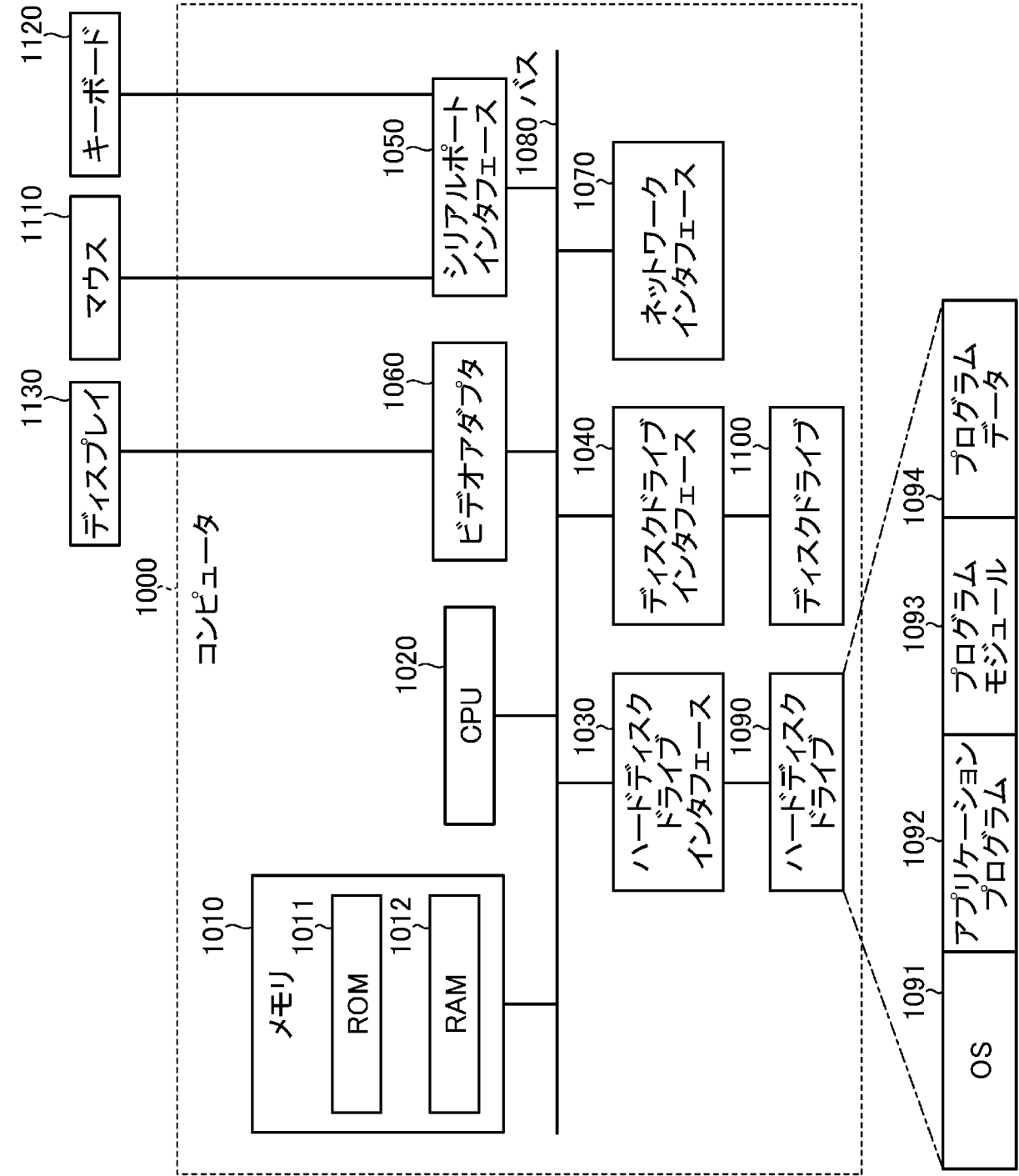
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/015645

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.
Y	WO 2019/142399 A1 (NIPPON TELEGRAPH & TELEPHONE) 25 July 2019 (2019-07-25) paragraphs [0021], [0098]-[0099], fig. 1	1-2, 6-7
A	entire text, all drawings	3-5
Y	JP 2015-106336 A (NIPPON TELEGRAPH & TELEPHONE) 08 June 2015 (2015-06-08) paragraphs [0014]-[0015], [0019], [0046]	1-2, 6-7
A	entire text, all drawings	3-5
A	JP 2016-006700 A (NTT DATA CORP) 14 January 2016 (2016-01-14) abstract	1-7
A	JP 2005-070961 A (NIPPON TELEGR & TELEPH CORP <NTT>) 17 March 2005 (2005-03-17) abstract	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
06 July 2021 (06.07.2021)

Date of mailing of the international search report
20 July 2021 (20.07.2021)

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
Information on patent family members

International application No.

PCT/JP2021/015645

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2019/142399 A1	25 Jul. 2019	(Family: none)	
JP 2015-106336 A	08 Jun. 2015	(Family: none)	
JP 2016-006700 A	14 Jan. 2016	(Family: none)	
JP 2005-070961 A	17 Mar. 2005	(Family: none)	

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 <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								
Y	WO 2019/142399 A1（日本電信電話株式会社）25.07.2019（2019 - 07 - 25） 段落0021, 0098-0099及び図1	1-2, 6-7								
A	全文, 全図	3-5								
Y	JP 2015-106336 A（日本電信電話株式会社）08.06.2015（2015 - 06 - 08） 段落0014-0015, 0019, 0046	1-2, 6-7								
A	全文, 全図	3-5								
A	JP 2016-006700 A（株式会社エヌ・ティ・ティ・データ）14.01.2016（2016 - 01 - 14） 要約	1-7								
A	JP 2005-070961 A（日本電信電話株式会社）17.03.2005（2005 - 03 - 17） 要約	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。										
* 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 06.07.2021		国際調査報告の発送日 20.07.2021								
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） 吉田 歩 5S 1206 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/JP2021/015645

引用文献			公表日	パテントファミリー文献	公表日
WO	2019/142399	A1	25.07.2019	(ファミリーなし)	
JP	2015-106336	A	08.06.2015	(ファミリーなし)	
JP	2016-006700	A	14.01.2016	(ファミリーなし)	
JP	2005-070961	A	17.03.2005	(ファミリーなし)	