

(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
2021年9月23日(23.09.2021)



(10) 国際公開番号

WO 2021/186515 A1

(51) 国際特許分類:
G06F 21/57 (2013.01)

(21) 国際出願番号: PCT/JP2020/011557

(22) 国際出願日: 2020年3月16日(16.03.2020)

(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: 渡邊 卓弥 (**WATANABE, Takuya**); 〒1808585 東京都武蔵野市緑町3丁目9-1 N T T 知的財産センタ内 Tokyo (JP). 塩治 榮太

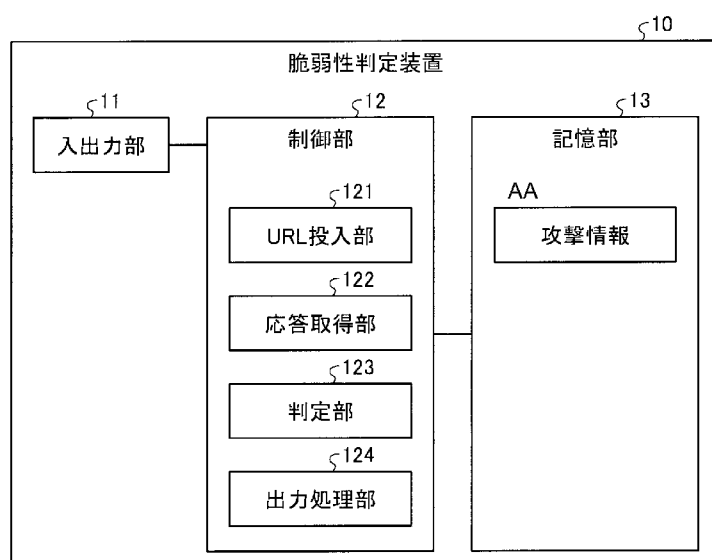
朗(**SHIOJI, Eitaro**); 〒1808585 東京都武蔵野市緑町3丁目9-1 N T T 知的財産センタ内 Tokyo (JP). 秋山 満昭(**AKIYAMA, Mitsuaki**); 〒1808585 東京都武蔵野市緑町3丁目9-1 N T T 知的財産センタ内 Tokyo (JP).

(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,

(54) **Title:** VULNERABILITY ASSESSMENT DEVICE, VULNERABILITY ASSESSMENT METHOD AND VULNERABILITY ASSESSMENT PROGRAM

(54) 発明の名称: 脆弱性判定装置、脆弱性判定方法、および、脆弱性判定プログラム



10 Vulnerability assessment device
11 Input/output unit
12 Control unit
13 Storage unit
121 URL-issuing unit
122 Response acquisition unit
123 Assessment unit
124 Output processing unit
AA Attack information

(57) **Abstract:** A vulnerability assessment device (10) obtains, from a web rehosting device, the content and URL of each of a plurality of websites after rehosting by the web rehosting device. Thereafter, on the basis of the content and URL of the plurality of obtained rehosted websites, the vulnerability assessment device (10) identifies one or more of the following: the URL set for each of the plurality of rehosted websites; the presence/absence of a setting for writing a Cookie in the plurality of websites; and the presence/absence of a code for accessing a prescribed browser function of the plurality of websites. The vulnerability assessment device (10) assesses an attack which could occur as a result of rehosting the plurality of websites by using the identified results, and outputs the assessment results.

HN, HR, HU, ID, IL, IN, IR, IS, 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：

- 一 国際調査報告 (条約第21条(3))

(57) 要約：脆弱性判定装置（10）は、ウェブ再ホスティング装置から、当該ウェブ再ホスティング装置による再ホスト後の複数のウェブサイトそれぞれのコンテンツおよびURLを取得する。その後、脆弱性判定装置（10）は、取得した再ホスト後の複数のウェブサイトコンテンツおよびURLに基づき、再ホスト後の複数のウェブサイトそれぞれに設定されたURL、複数のウェブサイトにおけるCookieを書き込む設定の有無、および、複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無の少なくともいずれかを特定する。そして、脆弱性判定装置（10）は、特定した結果を用いて、複数のウェブサイトの再ホストにより発生しうる攻撃を判定し、その判定結果を出力する。

明 細 書

発明の名称：

脆弱性判定装置、脆弱性判定方法、および、脆弱性判定プログラム

技術分野

[0001] 本発明は、脆弱性判定装置、脆弱性判定方法、および、脆弱性判定プログラムに関する。

背景技術

[0002] 例えば、翻訳サービスの提供や、ウェブサイトのコンテンツの検閲回避等の目的で、ウェブサイトを別のウェブサイトで再ホストしてユーザに表示するサービスがある。以下、このようなサービスをWeb Rehosting（ウェブ再ホスティング）と呼ぶ。例えば、Google翻訳（登録商標）、Wayback Machine、ProxySite等が上記のウェブ再ホスティングに該当する。

[0003] 上記のウェブ再ホスティングにおいて、再ホストの対象となるウェブサイト群が異なるオリジン（例えば、ドメイン、ポート、スキーム）であったとしても、再ホスト後これらのウェブサイト群は同じオリジンに配置される。このため、再ホストの対象となるウェブサイト群に悪性ウェブサイトが含まれていた場合、ウェブ再ホスティングにおいて、当該ウェブサイトがセキュリティ上の境界を破って他のウェブサイトを攻撃するおそれがある。

[0004] 例えば、図1に示すように、再ホストの対象となるウェブサイトA，B，CのURL（Uniform Resource Locator）のドメインがそれぞれ異なっていたとしても、ウェブ再ホスティングにより、ウェブサイトA，B，CのURLのドメインが同じドメイン（rehosted.example）になることがある。このような場合において、再ホストの対象となるウェブサイトに攻撃者サイト（例えば、ウェブサイトC）が含まれていると、再ホスト後、攻撃者サイト（ウェブサイトC）からウェブサイトA，Bへの攻撃が成立してしまうおそれがある。よって、上記のような攻撃を防止するため、ウェブ再ホスティングサービスの脆弱性を調査することが重要である。

先行技術文献

非特許文献

- [0005] 非特許文献1: D. Martin and A. Schulman, “DEANONYMIZING USERS OF THE SAFEWEB ANONYMIZING SERVICE”, in 11th USENIX Security Symposium (USENIX Security 02), 2002.

発明の概要

発明が解決しようとする課題

- [0006] ここで、従来、例えば、ウェブサイトに対し個別に脆弱性を調査する技術はあった。しかし、上記のウェブ再ホスティングサービスに対して統一的に脆弱性を調査することは行われていなかった。そこで、本発明は、ウェブ再ホスティングサービスに対して統一的に脆弱性を調査することを課題とする。

課題を解決するための手段

- [0007] 前記した課題を解決するため、本発明は、複数のウェブサイトを再ホストしてユーザ端末に表示させる再ホスティング装置に、再ホストの対象となる複数のウェブサイトのURLを投入するURL投入部と、前記再ホスティング装置から、前記再ホスト後の前記複数のウェブサイトそれぞれのコンテンツおよびURLを含む、前記URLの投入に対する応答を取得する応答取得部と、前記取得した応答に基づき、前記再ホスト後の複数のウェブサイトそれぞれに設定されたURL、前記複数のウェブサイトにおけるCookieを書き込む設定の有無、および、前記複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無の少なくともいずれかを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定する判定部とを備えることを特徴とする。

発明の効果

- [0008] 本発明によれば、ウェブ再ホスティングサービスに対して統一的に脆弱性を調査することができる。

図面の簡単な説明

[0009] [図1]図 1 は、ウェブ再ホスティングを説明するための図である。

[図2]図 2 は、ウェブ再ホスティングにおいて発生しうる攻撃の例を示す図である。

[図3]図 3 は、ユーザ端末が攻撃者サイトにアクセスした後、正常サイトにアクセスすることによる攻撃の例を示す図である。

[図4]図 4 は、ユーザ端末が正常サイトにアクセスした後、攻撃者サイトにアクセスすることによる攻撃の例を示す図である。

[図5]図 5 は、脆弱性判定装置によるウェブ再ホスティングの脆弱性の判定の概要を説明する図である。

[図6]図 6 は、調査用サイト X の例を示す図である。

[図7]図 7 は、脆弱性判定装置の構成例を示す図である。

[図8]図 8 は、図 7 に示す攻撃判定情報の例を示す図である。

[図9]図 9 は、脆弱性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10]図 10 は、脆弱性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

[0010] 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。なお、本発明は、以下に説明する実施形態に限定されない。

[0011] [攻撃について]

まず、本実施形態の脆弱性判定装置が判定の対象とする攻撃について説明する。なお、本実施形態において、脆弱性判定装置が判定の対象とする攻撃は、ユーザ端末がウェブ再ホスティングサービスにより、攻撃者サイトを閲覧することにより発生する攻撃であるものとする。

[0012] 上記の攻撃は、例えば、図 2 に示すAtk#1～Atk#5の攻撃が考えられる。

[0013] ・Atk#1：ブラウザのService Worker (SW)、Application Cache (AppCache) の機能を悪用し、他のウェブサイトへのアクセスを永続的に傍受、改竄す

る。

- ・ Atk#2：ブラウザにおいてパーミッション保護されたリソース（Camera、Microphone、Location等）を悪用し、過去に許可された権限を再利用する。

- ・ Atk#3：ブラウザのPassword Managerの機能を悪用し、ブラウザに保存されたID、パスワードを窃取する。

- ・ Atk#4：ブラウザのCookie、localStorageを悪用し、ブラウザの閲覧履歴の推定を行う。

- ・ Atk#5：ブラウザのCookieを悪用し、ブラウザのログインセッションの窃取、上書きを行う。

[0014] 上記の攻撃は、ユーザ端末が攻撃者サイトにアクセスした後、正常サイトにアクセスすることによるもの（図3参照）と、ユーザ端末が正常サイトにアクセスした後、攻撃者サイトにアクセスすることによるもの（図4参照）とに分けられる。

[0015] 上記のAtk#1は、ユーザ端末が攻撃者サイトにアクセスした後、正常サイトにアクセスすることによる攻撃である。また、Atk#2～Atk#5は、ユーザ端末が正常サイトにアクセスした後、攻撃者サイトにアクセスすることによる攻撃である。これらの攻撃について、図3および図4を用いて説明する。

[0016] まず、図3を用いて、ユーザ端末が攻撃者サイトにアクセスした後、正常サイトにアクセスすることによる攻撃について説明する。例えば、ユーザ端末がウェブ再ホスティングを通して攻撃者サイトを訪問すると（図3の（1））、悪意あるSW（Service Worker）、Application Cacheがユーザ端末のブラウザに登録される（図3の（2））。その後、ユーザ端末がウェブ再ホスティングを通して正常サイトにアクセスすると、上記のSW、Application Cacheによって正常サイトへのアクセスが傍受、改竄される（図3の（3））。

[0017] 次に、図4を用いて、ユーザ端末が正常サイトにアクセスした後、攻撃者サイトにアクセスすることによる攻撃について説明する。例えば、ユーザ端末がウェブ再ホスティングを通して正常サイトを利用すると（図4の（1）

）、ユーザ端末のブラウザに機密データ（例えば、ログイン情報等）が保存される（図４の（２））。その後、ユーザ端末が攻撃者サイトにアクセスすると、ブラウザに保存された機密データが窃取される（図４の（３））。

[0018] [概要]

次に、図５を用いて、脆弱性判定装置によるウェブ再ホスティングの脆弱性の判定の概要を説明する。

[0019] まず、脆弱性判定装置１０を含むシステムの構成例を説明する。システムは、ウェブ再ホスティング装置（再ホスティング装置）１と脆弱性判定装置１０とを含む。

[0020] ウェブ再ホスティング装置１は、複数のウェブサイトの再ホスティングを行う。例えば、ウェブ再ホスティング装置１は、複数のウェブサイトを再ホストしてユーザ端末に表示させる。

[0021] 脆弱性判定装置１０は、ウェブ再ホスティング装置１によるウェブ再ホスティングの脆弱性の判定を行う。このウェブ再ホスティング装置１と脆弱性判定装置１０とは、例えば、インターネット等のネットワーク経由で通信可能に接続される。

[0022] 脆弱性判定装置１０においてウェブ再ホスティングの脆弱性の判定を行うため、システムの管理者等は、調査用サイトＸ，Ｙ（後記）を用意しておく。そして、脆弱性判定装置１０は、ウェブ再ホスティング装置１に、上記の調査用サイトＸ，ＹのＵＲＬを投入する。その後、ウェブ再ホスティング装置１は、投入された調査用サイトＸ，Ｙのウェブ再ホスティングを行うため、調査用サイトＸ，Ｙの内部変換を行う。例えば、ウェブ再ホスティング装置１は、調査用サイトＸ，ＹのＵＲＬの変換等を行う。そして、ウェブ再ホスティング装置１は、調査用サイトＸ，ＹのＵＲＬの投入の応答を脆弱性判定装置１０に返す。例えば、ウェブ再ホスティング装置１は、再ホスト後の調査用サイトＸ，Ｙ（調査用サイトＸ′，Ｙ′）それぞれのＵＲＬ、コンテンツ等を脆弱性判定装置１０へ返す。そして、脆弱性判定装置１０は、当該応答に基づき、調査用サイトＸ′，Ｙ′に発生しうる攻撃を判定する。

[0023] [調査用サイト]

ここで、上記の調査用サイトX、Yについて説明する。例えば、調査用サイトXは、図6に示すように、トップページをhttps://x.example/とし、このトップページの配下にService Workerに関するコード (sw.js) と、Application Cache Manifest (manifest) とが配置されるよう設定する。

[0024] なお、調査用サイトXのトップページは、当該トップページからのHTTP応答が以下の内容となるよう設定されているものとする。以下に示すAtk#1~Atk#5は、図2に示す攻撃パターンに対応する。

[0025] 例えば、図6に示すように、HTTP応答ヘッダにはCookieを書き込むHTTPヘッダ (例えば、Set-Cookie:abc=123) が設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#4、Atk#5のCookieを用いた攻撃が発生しうるか否かを判定することができる。

[0026] また、HTTP応答ボディには、ブラウザの各機能にアクセスするコード (HTML、JavaScript (登録商標) を用いたコード) が設定される。

[0027] 例えば、図6に示すように、HTTP応答ボディには、<html manifest="...">が設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#1のAppCacheを用いた攻撃が発生しうるか否かを判定することができる。

[0028] また、HTTP応答ボディには、ID/パスワード入力フォームである<form>が設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#3のID、パスワードを用いた攻撃が発生しうるか否かを判定することができる。

[0029] さらに、HTTP応答ボディには、navigator.serviceWorker.registerが設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#1のSWを用いた攻撃が発生しうるか否かを判定することができる。

[0030] また、HTTP応答ボディには、navigator.geolocation.getCurrentPositionが設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#2のパーミッション保護されたリソース (例えば、location) を

用いた攻撃が発生しうるか否かを判定することができる。

[0031] また、HTTP応答ボディには、例えば、localStorageが設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#4のlocalStorageを用いた攻撃が発生しうるか否かを判定することができる。

[0032] また、HTTP応答ボディには、例えば、document.cookie;が設定される。これにより、脆弱性判定装置10は、調査用サイトXの再ホスト後にAtk#4およびAtk#5のCookieを用いた攻撃が発生しうるか否かを判定することができる。

[0033] また、HTTP応答ボディには、SWとAppCacheを参照する以下のHTMLコードも設定される。

[0034] <script src="./sw.js">

[0035] これにより、脆弱性判定装置10は、再ホスト後に調査用サイトXに配置される、sw.jsおよびmanifestがどのようなURLに変換されるかを確認することができる。

[0036] また、上記のsw.js (https://x.example/sw.js) のHTTP応答ヘッダには、Content-typeとしてtext/javascriptが設定される。さらに、上記のmanifest (https://x.example/manifest) のHTTP応答ヘッダには、Content-typeとしてtext/cache-manifestが設定される。これにより、脆弱性判定装置10は、再ホスト後の調査用サイトXにAtk#1のSW、AppCacheを用いた攻撃が発生しうるか否かを判定することができる。

[0037] なお、調査用サイトYは、ウェブ再ホスティング装置1による再ホスト後にどのようなURLに変換されるかを確認するために用いられるので、調査用サイトXとは異なるドメインのURLがされれば、コンテンツはどのようなものでもよい。例えば、調査用サイトYのトップページのURLとして、調査用サイトXとは異なるドメインのURLである「https://y.example/」等を設定する。

[0038] [構成]

次に図7を用いて脆弱性判定装置10の構成例を説明する。脆弱性判定装

置 1 0 は、入出力部 1 1 と、制御部 1 2 と、記憶部 1 3 とを備える。

[0039] 入出力部 1 1 は、外部装置から各種データの入力を受け付けたり、外部装置へ各種データを出力したりするためのインタフェースである。この入出力部 1 1 は、例えば、ウェブ再ホスティング装置 1 に対し、再ホストの対象となるウェブサイトの URL を出力したり、当該ウェブ再ホスティング装置 1 からの応答の入力を受け付けたりする。

[0040] 制御部 1 2 は、脆弱性判定装置 1 0 全体の制御を司る。制御部 1 2 は、各種の処理手順等を規定したプログラム及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。例えば、制御部 1 2 は、CPU (Central Processing Unit) や MPU (Micro Processing Unit) 等の電子回路である。制御部 1 2 は、各種のプログラムが動作することにより各種の処理部として機能する。

[0041] 制御部 1 2 は、URL 投入部 1 2 1 と、応答取得部 1 2 2 と、判定部 1 2 3 と、出力処理部 1 2 4 とを備える。

[0042] URL 投入部 1 2 1 は、ウェブ再ホスティング装置 1 に対し、再ホストの対象となるウェブサイト（例えば、調査用サイト X, Y）の URL を投入する。

[0043] 応答取得部 1 2 2 は、ウェブ再ホスティング装置 1 から、上記の URL の投入に対する応答（例えば、当該ウェブ再ホスティング装置 1 による再ホスト後の複数のウェブサイトそれぞれのコンテンツ、URL 等）を取得する。

[0044] 判定部 1 2 3 は、応答取得部 1 2 2 により取得された応答に基づき、複数のウェブサイトの再ホストにより発生しうる攻撃を判定する。

[0045] 例えば、判定部 1 2 3 は、応答取得部 1 2 2 により取得された応答（例えば、当該ウェブ再ホスティング装置 1 による再ホスト後の複数のウェブサイトそれぞれのコンテンツおよび URL）に基づき、例えば、再ホスト後の複数のウェブサイトそれぞれに設定された URL、当該複数のウェブサイトにおける Cookie を書き込む設定の有無、当該複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無等を特定する。そして、判定

部 1 2 3 は、特定した結果と、記憶部 1 3 の攻撃情報（図 8 参照）とを用いて、当該複数のウェブサイトの再ホストにより発生しうる攻撃を判定する。出力処理部 1 2 4 は、上記の判定部 1 2 3 の判定結果を入出力部 1 1 経由で出力する。

[0046] 例えば、判定部 1 2 3 は、前記した再ホスト後の調査用サイト X´, Y´ のコンテンツ、URL について、以下の（１）～（６）に示す項目をチェックする。

[0047] （１）スキーマチェック：調査用サイト X´ の URL のスキーマは https であるか否か。

（２）ドメインチェック：調査用サイト X´ および調査用サイト Y´ の URL のドメインは同じであるか否か。

（３）パスチェック：調査用サイト X´ および調査用サイト Y´ の URL のパスはそれぞれ同じ階層であるか否か。

（４）応答ヘッダチェック：調査用サイト X´ の HTTP 応答ヘッダにおいて Cookie を書き込む設定が有効であるか否か。

（５）応答ボディチェック：調査用サイト X´ の HTTP 応答ボディにおいてブラウザの各機能にアクセスするコードが有効であるか否か。

（６）追加リソースチェック：調査用サイト X´ の配下の sw.js および manifest に正しい Content-type が設定されているか否か。

[0048] 判定部 1 2 3 は、URL 投入に対する応答に関する上記の（１）～（６）の項目のチェック結果に基づき、調査用サイト X, Y の再ホストにより発生しうる攻撃を判定する。例えば、判定部 1 2 3 は、上記の（１）～（６）に示す項目のチェックの結果（チェック結果）と、図 8 に示す攻撃判定情報とを参照して、調査用サイト X, Y の再ホストにより発生しうる攻撃の種類（例えば、図 2 に示す Atk#1～Atk#5）を判定する。

[0049] 上記の攻撃判定情報は、発生しうる攻撃の種類ごとに、当該種類の攻撃が発生しうる（１）～（６）の項目のチェック結果の組み合わせを示した情報である。なお、図 8 において空欄になっている項目は、当該項目に該当して

もよいし（Yesでもよいし）、該当しなくてもよい（Noでもよい）ことを示す。

[0050] 例えば、図8に示す攻撃判定情報の1行目の情報は、（1）調査用サイトX'のURLのスキーマがhttpsであり、（2）調査用サイトX'および調査用サイトY'のURLのドメインが同じであり、（3）調査用サイトX'および調査用サイトY'のURLのパスがそれぞれ同じ階層であり、（5）調査用サイトX'のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効であり、かつ、（6）調査用サイトX'の配下のsw.jsおよびmanifestに正しいContent-typeが設定されている場合、調査用サイトX，Yの再ホストにより、SWに関するAtk#1の攻撃が発生しうることを示す。

[0051] また、図8に示す攻撃判定情報の2行目の情報は、（1）調査用サイトX'のURLのスキーマがhttpsであり、（2）調査用サイトX'および調査用サイトY'のURLのドメインが同じであり、（5）調査用サイトX'のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効であり、かつ、（6）調査用サイトX'の配下のsw.jsおよびmanifestに正しいContent-typeが設定されている場合、調査用サイトX，Yの再ホストにより、AppCacheに関するAtk#1の攻撃が発生しうることを示す。

[0052] さらに、図8に示す攻撃判定情報の3行目の情報は、（1）調査用サイトX'のURLのスキーマがhttpsであり、（2）調査用サイトX'および調査用サイトY'のURLのドメインが同じであり、（5）調査用サイトX'のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効である場合、調査用サイトX，Yの再ホストにより、Atk#2の攻撃が発生しうることを示す。

[0053] また、図8に示す攻撃判定情報の4行目の情報は、（2）調査用サイトX'および調査用サイトY'のURLのドメインが同じであり、（4）調査用サイトX'のHTTP応答ヘッダにおいてCookieを書き込む設定が有効であり、（5）調査用サイトX'のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効である場合、調査用サイトX，Yの再ホストにより、A

tk#3の攻撃が発生しうることを示す。

[0054] また、図8に示す攻撃判定情報の5行目の情報は、(2)調査用サイトX[′]および調査用サイトY[′]のURLのドメインが同じであり、(5)調査用サイトX[′]のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効である場合、調査用サイトX、Yの再ホストにより、Atk#4の攻撃が発生しうることを示す。

[0055] また、図8に示す攻撃判定情報の6行目の情報は、(2)調査用サイトX[′]および調査用サイトY[′]のURLのドメインが同じであり、(4)調査用サイトX[′]のHTTP応答ヘッダにおいてCookieを書き込む設定が有効であり、(5)調査用サイトX[′]のHTTP応答ボディにおいてブラウザの各機能にアクセスするコードが有効である場合、調査用サイトX、Yの再ホストにより、Atk#5の攻撃が発生しうることを示す。

[0056] なお、上記の攻撃判定情報は、脆弱性判定装置10の管理者等により適宜変更可能である。

[0057] 図7の記憶部13は、例えば、RAM(Random Access Memory)、フラッシュメモリ(Flash Memory)等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現され、脆弱性判定装置10を動作させる処理プログラムや、処理プログラムの実行中に使用されるデータ等が記憶される。記憶部13には、例えば、上記の攻撃判定情報(図8参照)が記憶される。

[0058] [処理手順]

次に図9を用いて脆弱性判定装置10の処理手順の例を説明する。なお、調査用サイトX、Yは事前に用意されているものとする。

[0059] まず、脆弱性判定装置10のURL投入部121はウェブ再ホスティング装置1に調査用サイトのURLを投入する(S1)。その後、応答取得部122は、ウェブ再ホスティング装置1から、S1におけるURLの投入に対する応答(例えば、再ホスト後の調査用サイトX、YそれぞれのコンテンツおよびURL)を取得する(S2)。

[0060] S 2 の後、判定部 1 2 3 は、S 2 で取得された応答に基づき、ウェブサイト（調査用サイト X，Y）の再ホストにより発生しうる攻撃を判定する（S 3）。そして、出力処理部 1 2 4 は、S 3 の判定結果を出力する（S 4）。

[0061] このような脆弱性判定装置 1 0 によれば、ウェブ再ホスティングサービスの脆弱性を判定することができる。

[0062] [プログラム]

また、上記の実施形態で述べた脆弱性判定装置 1 0 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コンピュータに実行させることにより、コンピュータを脆弱性判定装置 1 0 として機能させることができる。ここで言うコンピュータには、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、ラック搭載型のサーバコンピュータ等が含まれる。また、その他にも、コンピュータにはスマートフォン、携帯電話機や P H S（Personal Handyphone System）等の移動体通信端末、さらには、P D A（Personal Digital Assistants）等がその範疇に含まれる。また、脆弱性判定装置 1 0 の機能を、クラウドサーバに実装してもよい。

[0063] 図 1 0 を用いて、上記のプログラム（脆弱性判定プログラム）を実行するコンピュータの一例を説明する。図 1 0 に示すように、コンピュータ 1 0 0 0 は、例えば、メモリ 1 0 1 0 と、CPU 1 0 2 0 と、ハードディスクドライバインタフェース 1 0 3 0 と、ディスクドライバインタフェース 1 0 4 0 と、シリアルポートインタフェース 1 0 5 0 と、ビデオアダプタ 1 0 6 0 と、ネットワークインタフェース 1 0 7 0 とを有する。これらの各部は、バス 1 0 8 0 によって接続される。

[0064] メモリ 1 0 1 0 は、ROM（Read Only Memory）1 0 1 1 および RAM 1 0 1 2 を含む。ROM 1 0 1 1 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 1 0 3 0 は、ハードディスクドライブ 1 0 9 0 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。

[0065] ここで、図１０に示すように、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およびプログラムデータ１０９４を記憶する。前記した実施形態で説明した記憶部１３は、例えばハードディスクドライブ１０９０やメモリ１０１０に装備される。

[0066] そして、ＣＰＵ１０２０が、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、上述した各手順を実行する。

[0067] なお、上記の脆弱性判定プログラムに係る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れず、例えば、着脱可能な記憶媒体に記憶されて、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、上記のプログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ＬＡＮやＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、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

[0068] １ ウェブ再ホスティング装置

１０ 脆弱性判定装置

１１ 入出力部

１２ 制御部

１３ 記憶部

1 2 1 U R L 投入部

1 2 2 応答取得部

1 2 3 判定部

1 2 4 出力処理部

請求の範囲

【請求項1】 複数のウェブサイトを再ホストしてユーザ端末に表示させる再ホスティング装置に、再ホストの対象となる複数のウェブサイトのURLを投入するURL投入部と、

前記再ホスティング装置から、前記再ホスト後の前記複数のウェブサイトそれぞれのコンテンツおよびURLを含む、前記URLの投入に対する応答を取得する応答取得部と、

前記取得した応答に基づき、前記再ホスト後の複数のウェブサイトそれぞれに設定されたURL、前記複数のウェブサイトにおけるCookieを書き込む設定の有無、および、前記複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無の少なくともいずれかを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定する判定部と

を備えることを特徴とする脆弱性判定装置。

【請求項2】 前記判定部は、さらに、

前記取得した応答に基づき、前記再ホスト後の複数のウェブサイトそれぞれに設定されたURLにおけるドメインが同じか否か、および、パスの階層が同じか否かを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定することを特徴とする請求項1に記載の脆弱性判定装置。

【請求項3】 前記判定部は、さらに、

前記取得した応答に基づき、前記再ホスト後の複数のウェブサイトのいずれかのService WorkerおよびApplication Cache Manifestそれぞれに正しいContent-Typeが設定されているか否かを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定する

ことを特徴とする請求項1に記載の脆弱性判定装置。

【請求項4】 前記複数のウェブサイトの再ホストにより発生しうる攻撃は、

ブラウザのService WorkerまたはApplication Cacheを用いた他のウェブサイトへのアクセスの傍受または改ざん、ブラウザにおいて過去に利用が許可された権限の再利用、ブラウザに保存されたID、パスワードの窃取、ブラウザによる閲覧履歴の推定、および、他のウェブサイトへのログインセッションの窃取または上書き、のいずれかまたはこれらの組み合わせである

ことを特徴とする請求項1に記載の脆弱性判定装置。

[請求項5]

脆弱性判定装置により実行される脆弱性判定方法であって、

複数のウェブサイトを再ホストしてユーザ端末に表示させる再ホスティング装置に、再ホストの対象となる複数のウェブサイトのURLを投入する工程と、

前記再ホスティング装置から再ホスト後の前記複数のウェブサイトそれぞれのコンテンツおよびURLを含む、前記URLの投入に対する応答を取得する工程と、

前記取得した応答に基づき、前記再ホスト後の複数のウェブサイトそれぞれに設定されたURL、前記複数のウェブサイトにおけるcookieを書き込む設定の有無、および、前記複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無の少なくともいずれかを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定する工程と

を含むことを特徴とする脆弱性判定方法。

[請求項6]

複数のウェブサイトを再ホストしてユーザ端末に表示させる再ホスティング装置に、再ホストの対象となる複数のウェブサイトのURLを投入する工程と、

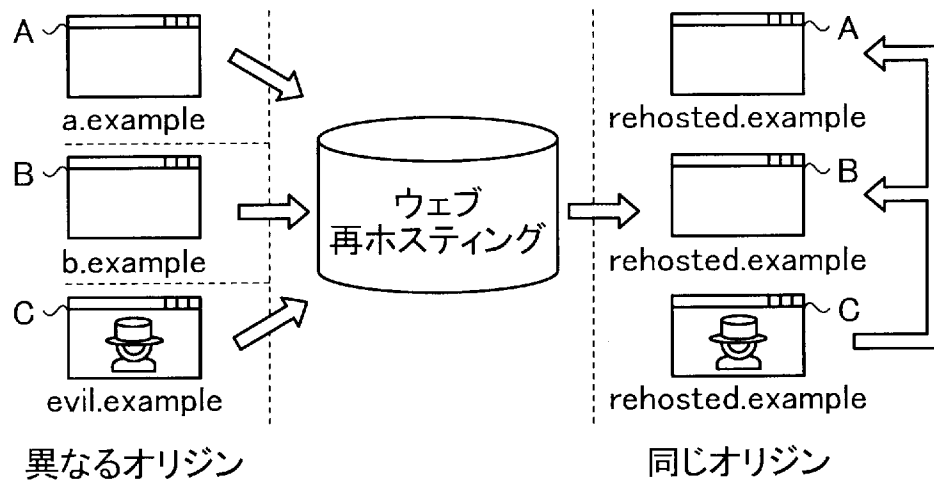
前記再ホスティング装置から、前記再ホスト後の前記複数のウェブサイトそれぞれのコンテンツおよびURLを含む、前記URLの投入に対する応答を取得する工程と、

前記取得した応答に基づき、前記再ホスト後の複数のウェブサイト

それぞれに設定されたURL、前記複数のウェブサイトにおけるcookieを書き込む設定の有無、および、前記複数のウェブサイトにおけるブラウザの所定の機能にアクセスするコードの有無の少なくともいずれかを特定し、前記特定した結果を用いて、前記複数のウェブサイトの再ホストにより発生しうる攻撃を判定する工程と

をコンピュータに実行させることを特徴とする脆弱性判定プログラム。

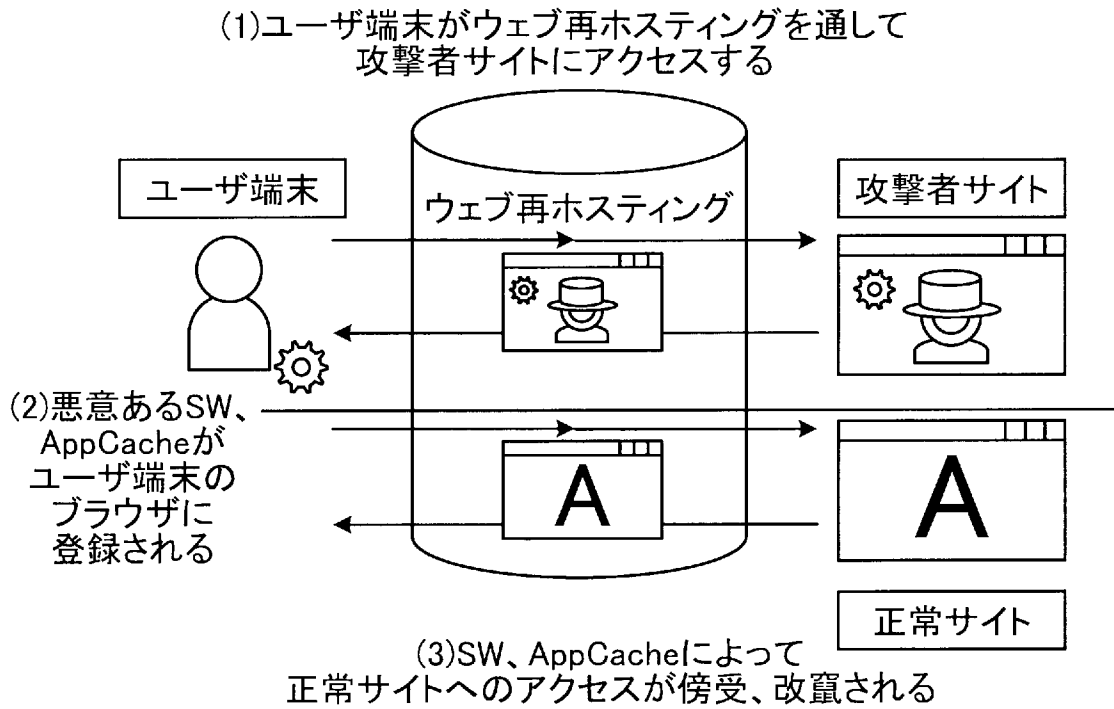
[図1]



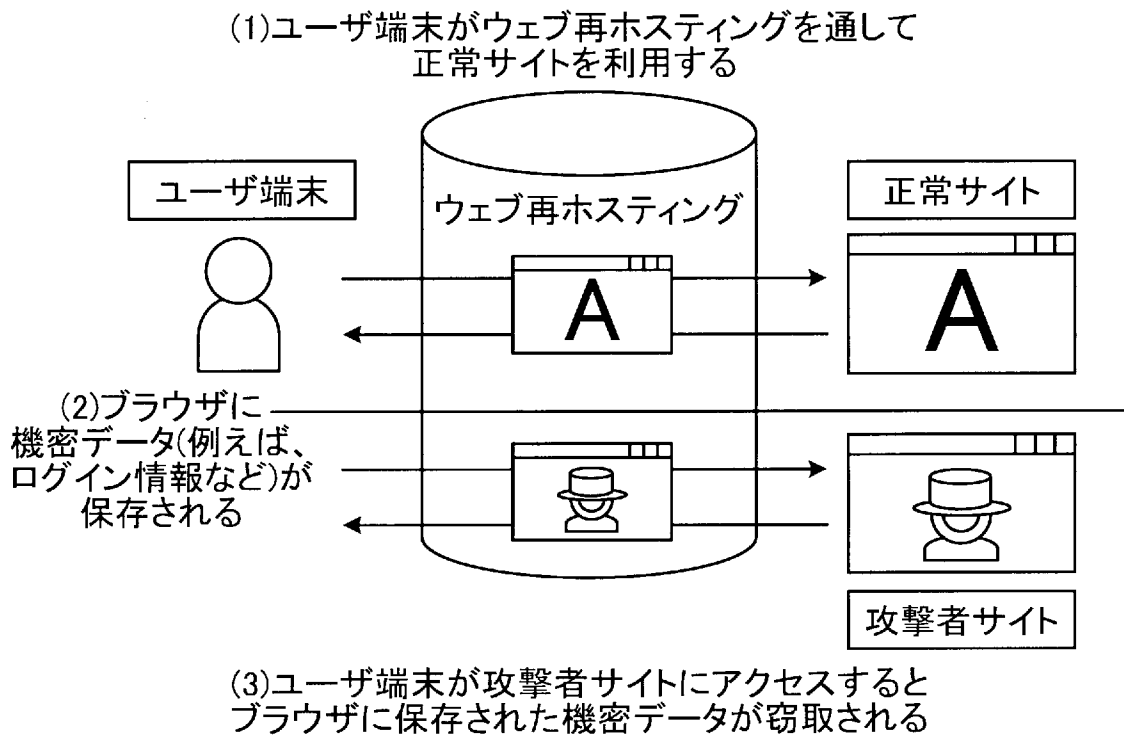
[図2]

	悪用するブラウザ機能	攻撃内容
Atk#1	Service Worker(SW)、 Application Cache(AppCache)	永続的な傍受、改竄
Atk#2	パーミッション保護されたリソース (Camera, Microphone, Location, etc.)	過去に許可された 権限の再利用
Atk#3	Password Manager	保存されたID、 パスワード窃取
Atk#4	Cookie、localStorage	閲覧履歴の推定
Atk#5	Cookie	ログインセッションの窃取、 上書き

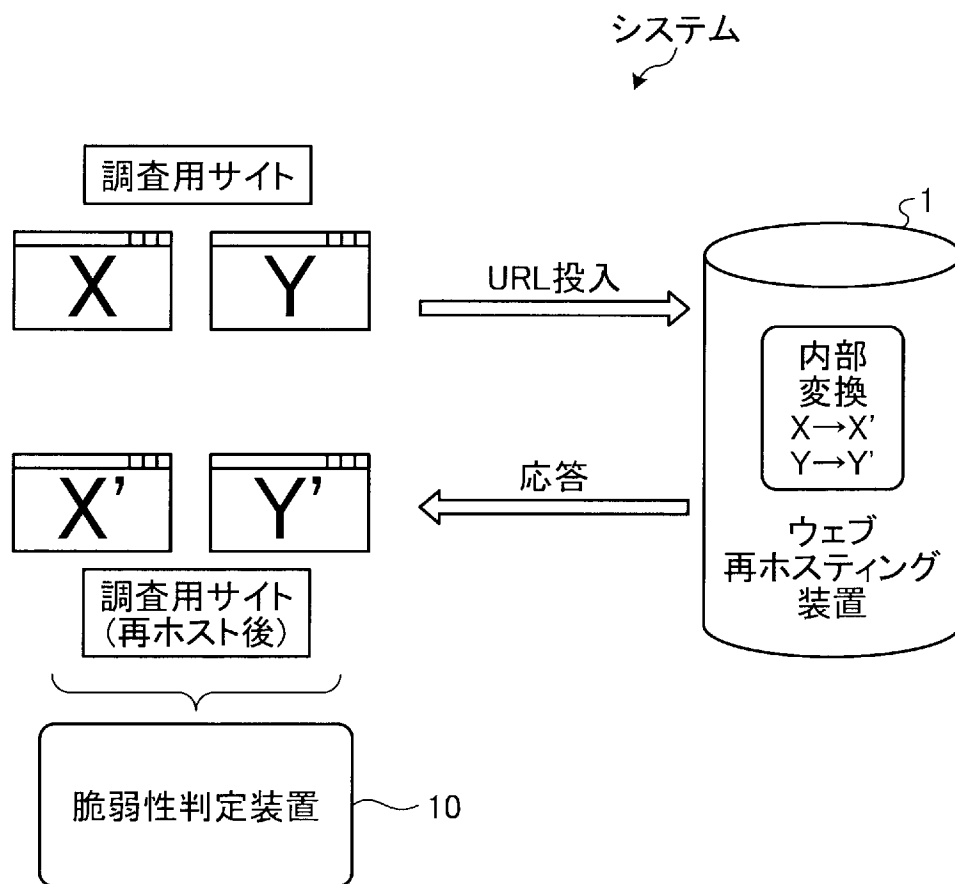
[図3]



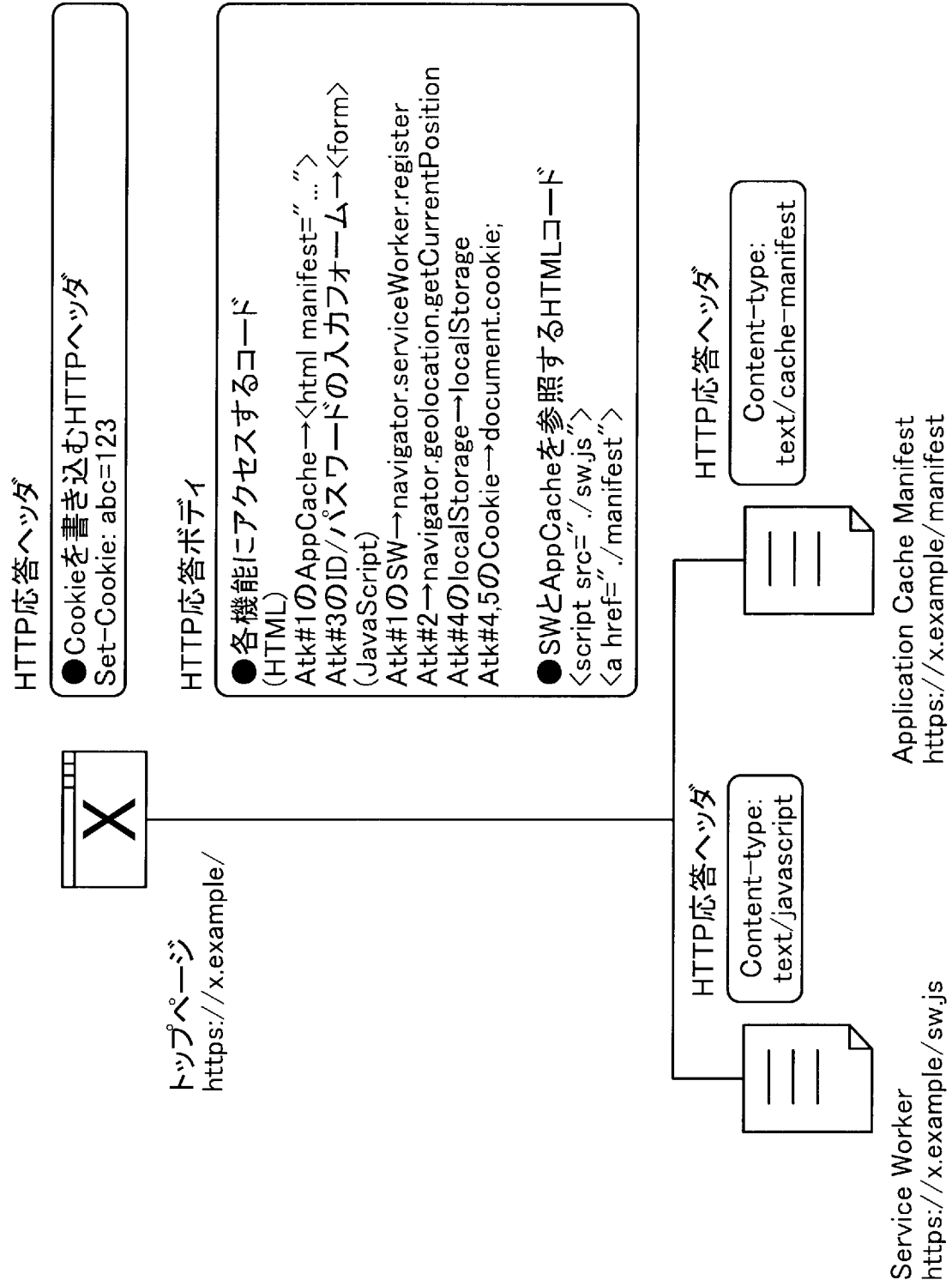
[図4]



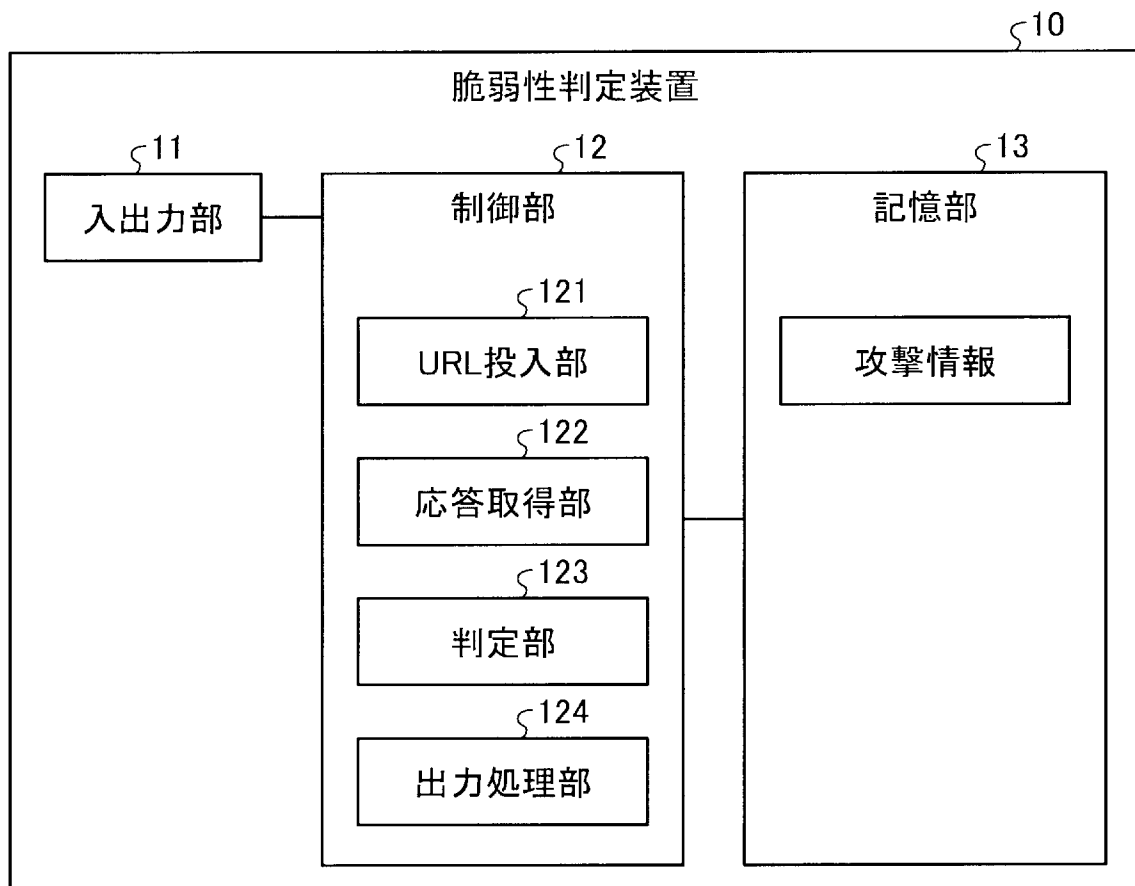
[図5]



[図6]



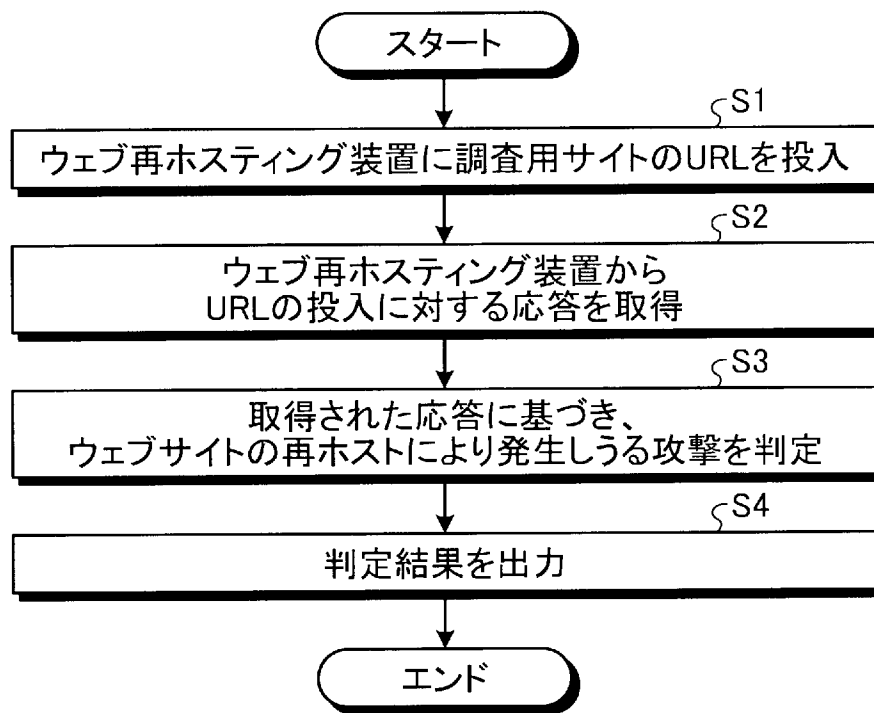
[図7]



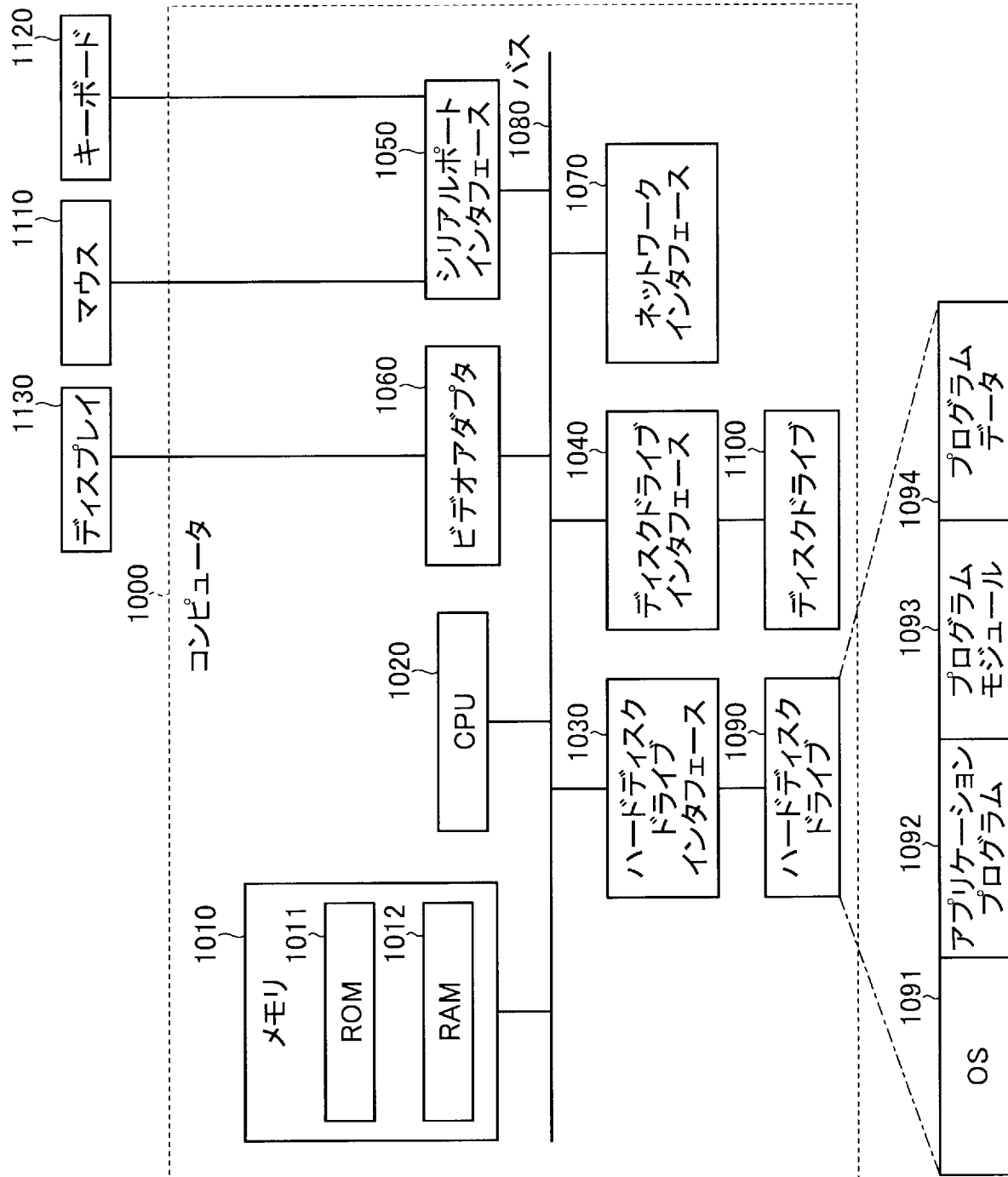
[図8]

(1)スキーマ チェック	(2)ドメイン チェック	(3)パスチェック	(4)応答 ヘッダチェック	(5)応答 ボディチェック	(6)追加 リソースチェック	発生しうる攻撃
Yes	Yes	Yes		Yes	Yes	Atk#1(SW)
Yes	Yes			Yes	Yes	Atk#1(AppCache)
Yes	Yes			Yes		Atk#2
	Yes		Yes	Yes		Atk#3
	Yes			Yes		Atk#4
	Yes		Yes	Yes		Atk#5

[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/011557

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06F21/57 (2013.01) i

FI: G06F21/57 370

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. G06F21/57

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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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	US 2013/0160131 A1 (MADOU, Matias) 20 June 2013	1-6
A	JP 2017-224150 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 21 December 2017	1-6
A	US 8856869 B1 (NEXWAVSEC SOFTNIARE INC.) 07 October 2014	1-6
A	JP 2019-517088 A (SITELOCK LLC) 20 June 2019	1-6



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

14.09.2020

Date of mailing of the international search report

24.09.2020

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/JP2020/011557

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
US 2013/0160131 A1	20.06.2013	(Family: none)	
JP 2017-224150 A	21.12.2017	(Family: none)	
US 8856869 B1	07.10.2014	US 10289857 B1	
		US 2019/0354709 A1	
JP 2019-517088 A	20.06.2019	US 2017/0324760 A1	
		WO 2017/193027 A1	
		CA 3023254 A1	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/57(2013.01)i FI: G06F21/57 370														
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）） G06F21/57 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 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020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 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020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 - 2020年													
日本国実用新案登録公報	1996 - 2020年													
日本国登録実用新案公報	1994 - 2020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	US 2013/0160131 A1 (MADOU, Matias) 20.06.2013 (2013 - 06 - 20)	1-6												
A	JP 2017-224150 A (日本電信電話株式会社) 21.12.2017 (2017 - 12 - 21)	1-6												
A	US 8856869 B1 (NEXWAVSEC SOFTWARE INC.) 07.10.2014 (2014 - 10 - 07)	1-6												
A	JP 2019-517088 A (サイトロック リミテッド ライアビリティ カンパニー) 20.06.2019 (2019 - 06 - 20)	1-6												
☐ 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>* 参考文献のカテゴリー</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>			* 参考文献のカテゴリー	“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	
* 参考文献のカテゴリー	“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 14.09.2020	国際調査報告の発送日 24.09.2020													
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） 岸野 徹 5S 3983 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/JP2020/011557

引用文献			公表日	パテントファミリー文献	公表日
US	2013/0160131	A1	20.06.2013	(ファミリーなし)	
JP	2017-224150	A	21.12.2017	(ファミリーなし)	
US	8856869	B1	07.10.2014	US	10289857 B1
				US	2019/0354709 A1
JP	2019-517088	A	20.06.2019	US	2017/0324760 A1
				WO	2017/193027 A1
				CA	3023254 A1