

明 細 書

発明の名称：

ウェブサイトの脆弱性を検査するためのシステム、方法、及びプログラム
技術分野

[0001] 本発明は、ウェブサイトの自動巡回を伴って、当該ウェブサイトの脆弱性を検査するためのシステム、方法、及びプログラムに関するものである。

背景技術

[0002] 従来、ウェブサイトの脆弱性を検査するための様々なサービスが提供されている（例えば、下記特許文献 1 を参照）。こうしたサービスでは、ウェブサイトの自動巡回が行われる場合があり、こうした自動巡回では、典型的には、ウェブページの HTML データから、リンク及びフォーム等を抽出し、これらに順次にアクセスするという処理が繰り返される。

先行技術文献

特許文献

[0003] 特許文献1：特開 2 0 1 2 - 1 3 3 4 0 6 号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、上述したような自動巡回において、例えば、アクセスするウェブページの数、階層数、及び、経過時間等の上限を設定する場合には、ウェブサイトの全てのページを巡回するよりも前に自動巡回が停止することになり、この結果、ウェブサイトが有する複数の機能の一部について、脆弱性検査の対象から漏れてしまう場合があった。例えば、ECサイトにおける商品購入機能等のように、重点的に検査を行うべき機能については、自動巡回の対象外となってしまうのを防止するのが望ましい。

[0005] 本発明の実施形態は、ウェブサイトの脆弱性検査において、重要な機能の検査漏れを抑制することを目的の一つとする。本発明の実施形態の他の目的は、本明細書全体を参照することにより明らかとなる。

課題を解決するための手段

- [0006] 本発明の一実施形態に係るシステムは、1又は複数のコンピュータプロセッサを備え、ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するためのシステムであって、前記1又は複数のコンピュータプロセッサは、前記ウェブサイトに含まれる第1ウェブページを取得するステップと、前記第1ウェブページに関する第1ページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するステップと、前記第1ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、前記複数の実行可能操作のうち、前記関連度に基づいて特定される第1操作を実行するステップと、前記第1操作の実行に応じて第2ウェブページを取得するステップと、を実行する。
- [0007] 本発明の一実施形態に係る方法は、1又は複数のコンピュータによって実行され、ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するための方法であって、前記ウェブサイトに含まれる第1ウェブページを取得するステップと、前記第1ウェブページに関する第1ページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するステップと、前記第1ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、前記複数の実行可能操作のうち、前記関連度に基づいて特定される第1操作を実行するステップと、前記第1操作の実行に応じて第2ウェブページを取得するステップと、を備える。
- [0008] 本発明の一実施形態に係るプログラムは、ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するためのプログラムであって、1又は複数のコンピュータに、前記ウェブサイトに含まれる第1ウェブページを取得するステップと、前記第1ウェブページに関する第1ページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するステップと、前記第1ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、

前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、前記複数の実行可能操作のうち、前記関連度に基づいて特定される第1操作を実行するステップと、前記第1操作の実行に応じて第2ウェブページを取得するステップと、を実行させる。

発明の効果

[0009] 本発明の様々な実施形態は、ウェブサイトの脆弱性検査において、重要な機能の検査漏れを抑制する。

図面の簡単な説明

[0010] [図1]本発明の一実施形態に係る脆弱性検査サーバ10を含むネットワークの構成を概略的に示す構成図。

[図2]検査管理テーブル152が管理する情報を例示する図。

[図3]ページ管理テーブル154が管理する情報を例示する図。

[図4]操作管理テーブル156が管理する情報を例示する図。

[図5]ウェブサイトの脆弱性を検査する際に脆弱性検査サーバ10が実行する処理を例示するフローチャート。

[図6]対象サイト設定画面50を例示する図。

[図7]ウェブサイトの自動巡回の際に脆弱性検査サーバ10が実行する処理を例示するフローチャート。

[図8]機能関連度スコアを取得する際の大規模言語モデルにおける入出力情報の一例を示す図。

[図9]操作管理テーブル156の登録内容の一例を示す図。

[図10]機能関連度スコアを取得する際の大規模言語モデルにおける入出力情報の一例を示す図。

[図11]操作管理テーブル156の登録内容の一例を示す図。

[図12]検査結果確認画面60を例示する図。

[図13]目標機能（検査必要機能）を設定する際の大規模言語モデルにおける入出力情報の一例を示す図。

[図14]機能関連度スコアを取得する際の大規模言語モデルにおける入出力情

報の他の例を示す図。

発明を実施するための形態

[0011] 以下、図面を参照しながら、本発明の実施形態について説明する。各図面において、同一の又は類似する構成要素に対しては同一の参照符号が付され得る。

[0012] 図1は、本発明の一実施形態に係る脆弱性検査サーバ10を含むネットワークの構成を概略的に示す構成図である。サーバ10は、図示するように、インターネット等の通信ネットワーク20を介してユーザ端末30と通信可能に接続されている。図1においては、1つのユーザ端末30のみが図示されているが、サーバ10は、複数のユーザ端末30と通信可能に接続されている。脆弱性検査サーバ10は、ユーザ端末30を操作するユーザに対して、当該ユーザによって指定されるウェブサイト22等の脆弱性（情報セキュリティ上の欠陥）を検査する脆弱性検査サービスを提供する。脆弱性検査サーバ10は、本発明のシステムの全部又は一部を実装する装置の一例である。

[0013] まず、脆弱性検査サーバ10のハードウェア構成について説明する。脆弱性検査サーバ10は、一般的なコンピュータとして構成されており、図1に示すように、コンピュータプロセッサ11と、メインメモリ12と、入出力I/F13と、通信I/F14と、ストレージ（記憶装置）15とを備え、これらの各構成要素が図示しないバス等を介して電氣的に接続されている。

[0014] コンピュータプロセッサ11は、CPU又はGPU等として構成され、ストレージ15等に記憶されている様々なプログラムをメインメモリ12に読み込んで、当該プログラムに含まれる各種の命令を実行する。メインメモリ12は、例えば、DRAM等によって構成される。

[0015] 入出力I/F13は、操作者等との間で情報をやり取りするための各種の入出力装置を含む。入出力I/F13は、例えば、キーボード、ポインティングデバイス（例えば、マウス、タッチパネル等）等の情報入力装置、マイクロフォン等の音声入力装置、カメラ等の画像入力装置を含む。また、入出

力 I / F 1 3 は、ディスプレイ等の画像出力装置、スピーカー等の音声出力装置を含む。

[0016] 通信 I / F 1 4 は、ネットワークアダプタ等のハードウェア、各種の通信用ソフトウェア、又はこれらの組み合わせとして実装され、通信ネットワーク 2 0 等を介した有線又は無線の通信を実現できるように構成されている。

[0017] ストレージ 1 5 は、例えば、磁気ディスク又はフラッシュメモリ等によって構成される。ストレージ 1 5 は、オペレーティングシステムを含む様々なプログラム及び各種データ等を記憶する。例えば、ストレージ 1 5 は、図 1 に示すように、脆弱性の検査に関する情報を管理する検査管理テーブル 1 5 2 と、検査対象のウェブサイト 2 2 に含まれるウェブページに関する情報を管理するページ管理テーブル 1 5 4 と、各ウェブページにおいて実行される操作に関する情報を管理する操作管理テーブル 1 5 6 とを有する。これらのテーブルは、その一部が 1 つのテーブルに統合されてもよいし、複数のテーブルに分割されてもよい。

[0018] また、例えば、ストレージ 1 5 は、本発明の一実施形態に係るサーバ側プログラム 4 0 を記憶する。当該プログラム 4 0 は、サーバ 1 0 を、脆弱性検査サービスを提供するためのシステムの全部又は一部として機能させるためのプログラムである。サーバ側プログラム 4 0 の少なくとも一部は、後述する端末側プログラム 4 2 を介して、ユーザ端末 3 0 側において実行されるように構成され得る。

[0019] 本実施形態において、脆弱性検査サーバ 1 0 は、それぞれが上述したハードウェア構成を有する複数のコンピュータを用いて構成され得る。例えば、サーバ 1 0 は、複数のサーバ装置によって構成される。

[0020] このように構成された脆弱性検査サーバ 1 0 は、ウェブサーバ及びアプリケーションサーバとしての機能を有するように構成することができ、ユーザ端末 3 0 からの要求に応答して各種の処理を実行し、当該処理の結果に応じた画面データ（例えば、HTML データ）及び制御データ等をユーザ端末 3 0 に対して送信する。ユーザ端末 3 0 では、受信したデータに基づくウェブ

ページ又はその他の画面が出力される。

- [0021] 次に、ユーザ端末30のハードウェア構成について説明する。ユーザ端末30は、一般的なコンピュータとして構成されており、図1に示すように、コンピュータプロセッサ31と、メインメモリ32と、入出力I/F33と、通信I/F34と、ストレージ（記憶装置）35とを備え、これらの各構成要素が図示しないバス等を介して電氣的に接続されている。
- [0022] コンピュータプロセッサ31は、CPU又はGPU等として構成され、ストレージ35等に記憶されている様々なプログラムをメインメモリ32に読み込んで、当該プログラムに含まれる各種の命令を実行する。メインメモリ32は、例えば、DRAM等によって構成される。
- [0023] 入出力I/F33は、操作者等との間で情報をやり取りするための各種の入出力装置を含む。入出力I/F33は、例えば、キーボード、ポインティングデバイス（例えば、マウス、タッチパネル等）等の情報入力装置、マイクロフォン等の音声入力装置、カメラ等の画像入力装置を含む。また、入出力I/F33は、ディスプレイ等の画像出力装置、スピーカー等の音声出力装置を含む。
- [0024] 通信I/F34は、ネットワークアダプタ等のハードウェア、各種の通信ソフトウェア、及びこれらの組み合わせとして実装され、通信ネットワーク20等を介した有線又は無線の通信を実現できるように構成されている。
- [0025] ストレージ35は、例えば、磁気ディスク又はフラッシュメモリ等によって構成される。ストレージ35は、オペレーティングシステムを含む様々なプログラム及び各種データ等を記憶する。ストレージ35が記憶するプログラムは、アプリケーションマーケット等からダウンロードされてインストールされ得る。また、ストレージ35は、上述した端末側プログラム42を記憶する。当該プログラム42は、ウェブブラウザ、又は、その他のアプリケーション（例えば、本実施形態の脆弱性検査サービス用の端末側アプリケーション等）として構成され、上述したように、サーバ側プログラム40の少なくとも一部を実行するように構成され得る。

- [0026] 本実施形態において、ユーザ端末30は、スマートフォン、タブレット端末、又はパーソナルコンピュータ等として構成され得る。
- [0027] このように構成されたユーザ端末30を操作するユーザは、ストレージ35等にインストールされている端末側プログラム42を介したサーバ10との通信を実行することによって、当該サーバ10が提供する脆弱性検査サービスを利用することができる。
- [0028] 次に、このように構成された脆弱性検査サーバ10が有する機能について説明する。サーバ10のコンピュータプロセッサ11は、図1に示すように、メインメモリ12に読み込まれたプログラム（例えば、サーバ側プログラム40の少なくとも一部）に含まれる命令を実行することによって、管理機能制御部112、自動巡回制御部114、及び、検査制御部116として機能するように構成されている。
- [0029] 管理機能制御部112は、脆弱性検査サービスの管理機能の制御に関する様々な処理を実行するように構成されている。例えば、管理機能制御部112は、当該管理機能に関する様々な画面の画面データ及び制御データ等をユーザ端末30に対して送信し、ユーザ端末30において出力される当該画面を介したユーザによる操作入力に応答して様々な処理を実行し、当該処理の結果に応じた画面データ及び制御データ等をユーザ端末30に対して送信する。管理機能制御部112によって制御される管理機能は、例えば、ログイン処理（ユーザ認証）、課金制御、及び、ユーザアカウントの管理等を含む。
- [0030] 自動巡回制御部114は、ウェブサイト22の自動巡回の制御に関する様々な処理を実行するように構成されている。例えば、自動巡回制御部114は、ウェブサイト22に含まれるウェブページを取得し、当該ウェブページにおいて実行可能な操作（遷移対象要素（例えば、リンク又はスクリプト等が設定された様々な種類のオブジェクト（ボタン、画像、及び、テキスト等）を含む。）のクリック等）を実行して遷移先のウェブページを取得し、これらを繰り返すことによって、ウェブサイト22を巡回する。

- [0031] 本実施形態において、自動巡回制御部 114 は、ウェブページに関するページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するように構成されている。例えば、自動巡回制御部 114 は、ウェブページの HTML データに基づいて、検査必要機能を判定する。
- [0032] また、自動巡回制御部 114 は、ウェブページにおいて実行可能な複数の実行可能操作を特定し、各実行可能操作と検査必要機能との間の関連度を判定するように構成されている。例えば、自動巡回制御部 114 は、ウェブページの HTML データ等に基づいて、予め定められた複数の操作のうち、当該ウェブページにおいて実行可能な操作を特定する。予め定められた操作は、例えば、「商品のリンクをクリックする」、「ログインのリンクをクリックする」、及び、「ログインフォームを入力して送信する」等の操作を含む。
- [0033] 本実施形態において、ウェブページにおいて実行される操作は、各実行可能操作と検査必要機能との間の関連度に基づいて特定される。つまり、自動巡回制御部 114 は、複数の実行可能操作のうち、関連度に基づいて特定される操作を実行し、当該操作の実行に応じて、遷移先のウェブページを取得するように構成されている。例えば、複数の実行可能操作のうち、検査必要機能との間の関連度が高い操作が優先して実行される。
- [0034] 検査制御部 116 は、ウェブサイト 22 の脆弱性の検査の制御に関する様々な処理を実行するように構成されている。例えば、検査制御部 116 は、ウェブサイト 22 を自動巡回する際に、予め定められた検査項目を検査するための様々なリクエストを送信し、当該ウェブサイト 22 から受信したレスポンスの内容に基づいて、対応する検査項目について判断する。
- [0035] このように、本実施形態における脆弱性検査サーバ 10 は、ウェブサイト 22 を自動巡回する際に、脆弱性の検査が必要な検査必要機能を判定し、ウェブページにおいて実行可能な複数の実行可能操作の各々と検査必要機能との間の関連度を判定し、これらの複数の実行可能操作のうち、当該関連度に基づいて特定される操作を実行するから、検査が必要な機能との間の関連度

に基づいて特定される操作の実行が可能となり、重要な機能に対応するウェブページへの巡回が促進され得る。つまり、脆弱性検査サーバ10は、ウェブサイトの脆弱性検査において、重要な機能の検査漏れを抑制する。

[0036] 本実施形態において、検査必要機能の判定は、様々な手法を用いて実現され得る。例えば、検査必要機能の判定は、ルールベースの手法を用いて実現される。この場合、例えば、ウェブページにおけるラベル名に基づいて検査必要機能を判定する（例えば、対応するHTMLデータにおいて、「ログイン」、「login」、「パスワード」、及び「アカウント」等のラベル名が含まれる場合に、検査必要機能として「ログイン機能」が判定される。）ようにしてもよい。

[0037] また、検査必要機能の判定は、機械学習によって生成される学習済みモデルを用いて実現されてもよい。例えば、自動巡回制御部114は、ページ情報を含む入力情報を、検査必要機能を判定するための学習済みモデルに入力し、当該学習済みモデルから出力される、検査必要機能を特定するための出力情報に基づいて、当該検査必要機能を判定するように構成され得る。こうした構成は、学習済みモデルを用いた検査必要機能の判定を可能とする。

[0038] 本実施形態において、検査必要機能を判定するための学習済みモデルは、様々な情報を出力するように構成され得る。例えば、当該学習済みモデルは、検査必要機能を特定する情報を出力するように構成される。例えば、当該学習済みモデルは、ウェブページのHTMLデータと共に、予め定められた複数の機能の中からの検査必要機能の選択を指示する情報が入力されると、選択された検査必要機能の情報を出力する大規模言語モデル（LLM）として構成される。こうした構成は、学習済みモデルから出力される検査必要機能を特定する情報に基づいて、検査必要機能を判定することを可能とする。

[0039] また、こうした学習済みモデルは、例えば、予め定められた複数の機能の各々の、脆弱性の検査が必要な可能性を示す検査必要可能性情報を出力するように構成される。こうした学習済みモデルは、例えば、多量の訓練データ（例えば、ウェブサイトに含まれるウェブページのページ情報（HTMLデ

ータ等)、及び、当該ウェブサイトにおける検査必要機能を特定する情報等)を用いた機械学習を介して生成され、検査必要可能性情報として、検査が必要な可能性を示すスコア等を入力するように構成される。この場合、自動巡回制御部114は、当該学習済みモデルから出力される検査必要可能性情報に基づいて、脆弱性の検査が必要な可能性が高い機能が優先されるように、検査必要機能を判定する。こうした構成は、学習済みモデルから出力される検査必要可能性情報に基づく検査必要機能の判定を可能とする。

[0040] また、自動巡回制御部114は、遷移先のウェブページのページ情報にさらに基づいて、検査必要機能を再度判定するように構成され得る。例えば、自動巡回制御部114は、第1ウェブページの第1ページ情報に基づいて、第1機能を検査必要機能として判定し、その後、第1ページ情報に加えて、遷移先の第2ウェブページの第2ページ情報にさらに基づいて、第1機能に代えて、又は、これに加えて、第2機能を検査必要機能として判定する。こうした構成は、複数のウェブページのページ情報に基づいて検査必要機能を繰り返し判定することを可能とする。

[0041] 本実施形態において、実行可能操作と検査必要機能との間の関連度の判定は、様々な手法を用いて実現され得る。例えば、当該関連度の判定は、ルールベースの手法を用いて実現される。この場合、例えば、操作に対応するラベル名に基づいて関連度を判定する(例えば、対応するラベル名が「ログイン」である場合に、ログイン機能との関連度が「100」に設定され、対応するラベル名が「アカウント」である場合に、ログイン機能との関連度が「50」に設定される。)ようにしてもよい。

[0042] また、関連度の判定は、機械学習によって生成される学習済みモデルを用いて実現されてもよい。例えば、自動巡回制御部114は、ウェブページのページ情報(HTMLデータ等)、及び、実行可能操作と検査必要機能との組合せを含む情報を、関連度を判定するための学習済みモデルに入力し、当該学習済みモデルから出力される関連度を判定するための情報(関連度を示すスコア等を含む。)に基づいて、当該関連度を判定するように構成され得る。

る。こうした学習済みモデルは、例えば、多量の訓練データ（例えば、ウェブページのページ情報（HTMLデータ等）、当該ウェブページにおける実行可能操作、及び、当該操作に関連する検査必要機能等）を用いた機械学習を介して生成される。また、この場合、学習済みモデルに対する入力情報として、過去の操作実績（対応するウェブページに到達するまでに行われた操作）が含まれるようにしてもよい。こうした構成は、学習済みモデルを用いた関連度の判定を可能とする。

[0043] 次に、このような機能を有する本実施形態の脆弱性検査サーバ10の一態様としての具体例について説明する。まず、この例において、各テーブルが管理する情報について説明する。図2は、この例において、検査管理テーブル152が管理する情報を例示する。この例における検査管理テーブル152は、個別の検査に関する情報を管理し、図示するように、個別の検査（案件）を識別する「検査ID」に対応付けて、検査対象のウェブサイトの検査の起点となるトップ画面（トップページ）のURLである「トップ画面URL」、画面遷移の設定日時である「画面遷移設定日時」、脆弱性検査の実行日時である「検査実行日時」等の情報を管理する。

[0044] 図3は、この例において、ページ管理テーブル154が管理する情報を例示する。この例におけるページ管理テーブル154は、検査対象のウェブサイトに含まれる各ウェブページ（画面）に関する情報を管理し、図示するように、個別の検査を識別する「検査ID」、及び、当該検査において個別の画面を識別する「画面ID」の組合せに対応付けて、当該画面のURLである「画面URL」、当該画面の画面キャプチャに関する情報である「画面キャプチャ情報」、当該画面の「HTMLデータ」、当該画面の遷移元の画面を識別する「遷移元画面ID」、当該画面の遷移元の操作（当該画面に遷移する際の操作）を識別する「遷移元操作ID」、遷移元の画面において、入力項目に対して入力された入力値に関する情報である「遷移元入力情報」、当該画面における検査結果に関する情報である「検査結果情報」等の情報を管理する。

[0045] 図4は、この例において、操作管理テーブル156が管理する情報を例示する。この例における操作管理テーブル156は、各画面において実行される操作に関する情報を管理し、個別の検査を識別する「検査ID」、当該検査において個別の画面を識別する「画面ID」、及び、当該画面において実行される個別の操作を識別する「操作ID」の組合せに対応付けて、当該操作に対応する画面構成要素に関する情報（ラベル名等）である「要素情報」、当該操作に関連付けられた検査必要機能を識別する「機能ID」、当該操作と検査必要機能との間の関連度スコアを示す「機能関連度スコア」、当該操作を実行済みであるか否かを示す「実行済みフラグ」等の情報を管理する。

[0046] 以上、この例において、各テーブルが管理する情報について説明した。次に、この例において、脆弱性検査サーバ10が実行する処理、及び、ユーザ端末30において出力される画面等について説明する。

[0047] 図5は、この例において、ウェブサイトの脆弱性を検査する際に脆弱性検査サーバ10が実行する処理を例示するフローチャートである。サーバ10は、まず、図示するように、脆弱性を検査する対象のウェブサイトの設定を受け付ける（ステップS100）。こうした設定の受付は、ユーザ端末30において出力される画面を介して行われる。

[0048] 図6は、ユーザ端末30において出力される、検査対象のウェブサイトの設定を受け付けるための対象サイト設定画面50を例示する。当該画面50は、図示するように、検査対象のウェブサイトのトップ画面（トップページ）のURLを入力するためのURL入力領域52と、当該ウェブサイトへのログインに用いられるログインIDを入力するためのログインID入力領域54と、当該ウェブサイトへのログインに用いられるパスワードを入力するためのパスワード入力領域56と、「巡回・検査開始」というテキストが付加された続行ボタン58とを有する。このように、この例では、検査対象のウェブサイトの設定情報として、トップ画面のURL、ログインID、及び、パスワードが受け付けられる。

- [0049] 続行ボタン58は、検査対象のウェブサイトの自動巡回及び検査を指示するためのオブジェクトである。図5のフローチャートに戻り、続行ボタン58が選択されると、サーバ10は、次に、検査対象のウェブサイトを自動巡回し、検査の際の画面遷移を設定する（ステップS110）。
- [0050] 図7は、ウェブサイトの自動巡回の際にサーバ10が実行する処理を例示するフローチャートである。サーバ10は、まず、図示するように、検査対象のウェブサイトのトップ画面にアクセスし、当該トップ画面を画面遷移に追加する（ステップS200）。具体的には、サーバ10において、ウェブブラウザが起動され、対象サイト設定画面50を介して入力されたURLによって特定されるトップ画面へのアクセス（対応するウェブページの取得）が行われる。また、ページ管理テーブル154において、当該トップ画面に関する情報が登録され、具体的には、検査ID、画面ID、画面URL、画面キャプチャ情報、及び、HTMLデータが設定される。
- [0051] 続いて、サーバ10は、脆弱性検査の目標機能（検査必要機能）を判定する（ステップS210）。目標機能は、この例では、学習済みモデルを用いて判定され、具体的には、対応する画面（ここでは、トップ画面）のHTMLデータが当該学習済みモデルに入力されると、当該学習済みモデルから、予め定められた複数の機能の各々について、検査が必要である可能性を示す検査必要性スコアが出力され、当該スコアの値が最も大きい機能が、目標機能として判定される。こうした学習済みモデルは、多量の訓練データ（HTMLデータに対して、検査が必要な機能を特定する情報が付加されたデータ等）を用いた機械学習を介して生成される。予め定められる複数の機能は、脆弱性検査サービスの提供者によって設定され、例えば、「ユーザ新規登録」、「ログイン」、「商品購入」、「問い合わせ」等を含む。
- [0052] 次に、サーバ10は、実行可能操作を特定する（ステップS220）。具体的には、対応する画面（ここでは、トップ画面）のHTMLデータに基づいて、1又は複数の実行可能操作が特定される。実行可能操作は、リンク又はスクリプト等が設定された画面構成要素（ボタン、画像、及び、テキスト

等)をクリックする操作として特定される。

[0053] 続いて、サーバ10は、特定された実行可能操作について、目標機能との間の関連度を示す機能関連度スコアを判定する(ステップS230)。機能関連度スコアは、具体的には、学習済みモデルを用いて取得される。当該学習済みモデルは、この例では、大規模言語モデルとして構成され、対応する画面のHTMLデータと共に、実行可能操作と目標機能との間の機能関連度スコアの提示を指示する情報が入力されると、当該スコアを出力するように構成されている。こうした大規模言語モデルとして、例えば、米国OpenAI社が提供するGPT-4が適用され得る。

[0054] 図8は、大規模言語モデルにおける入出力情報の一例を示す。こうした入力情報が、サーバ10によって自動的に生成される。

[0055] 図7のフローチャートに戻り、次に、サーバ10は、機能関連度スコアが閾値以上である操作を登録する(ステップS235)。具体的には、操作管理テーブル156において、検査ID、画面ID、操作ID、要素情報、機能ID、及び、機能関連度スコアが設定される。要素情報には、クリックの対象となる画面構成要素を特定する情報(ラベル名等)が設定される。このように、この例では、目標機能との間の機能関連度スコアが閾値以上である(目標機能との間の関連性が高い)操作が、当該目標機能と関連付けられて、操作管理テーブル156に登録される。

[0056] 図9は、この時点における操作管理テーブル156の内容の一例を示す。図示するように、図9の例では、画面IDが「S01」である画面(トップ画面)における実行可能操作のうち、目標機能(機能IDが「F01」)との間の機能関連度が閾値以上である2つの操作(操作IDが「O01」及び「O02」)が、当該目標機能と関連付けて登録されている。

[0057] 図7のフローチャートに戻り、次に、登録済みの操作について、未実行の操作がある場合(ステップS240においてYES)、サーバ10は、実行対象操作を決定して実行する(ステップS250)。具体的には、未実行の登録済みの操作(操作管理テーブル156の実行済みフラグを参照すること

によって特定される。)のうち、所定ルールに従って特定される(例えば、機能関連度スコアが最も大きい)操作が、実行対象操作として決定される。なお、対応する画面に入力項目(例えば、入力可能なフォーム要素)が存在する場合には、当該入力項目に対する入力値を設定した上で、操作の実行が行われる。入力値は、所定ルールに従って自動的に設定される。

[0058] 続いて、サーバ10は、操作の実行に応じた遷移先画面への遷移を画面遷移に追加する(ステップS260)。具体的には、ページ管理テーブル154において、遷移先の画面に関する情報が登録され、つまり、検査ID、画面ID、画面URL、画面キャプチャ情報、HTMLデータ、遷移元画面ID、遷移元操作ID、及び、遷移元入力情報が設定される。遷移元操作IDには、直前に実行された操作を識別する値が設定される。また、遷移元入力情報には、入力項目及び入力値の組合せが設定される。

[0059] ここで、遷移先の画面が、画面遷移への追加対象外の画面である場合には、画面遷移への追加が行われないようにしてもよい。例えば、検査対象のウェブサイトの外部のサイトの画面、及び、既に画面遷移に含まれる画面と重複する画面(例えば、画面の類似度に基づいて判断される。)等については、画面遷移への追加対象外と判断される。

[0060] 次に、サーバ10は、ステップS210へと戻り、遷移先の画面を対象に、目標機能の設定(ステップS210)、実行可能操作の特定(ステップS220)、各操作の機能関連度スコアの判定(ステップS230)、及び、機能関連度スコアが閾値以上である操作の登録(ステップS235)を行う。

[0061] ここで、2回目以降の機能関連度スコアの判定の際には、対応する画面のHTMLデータに基づいて判定された目標機能(現在の画面に基づく目標機能)に加えて、操作管理テーブル156において、直前に実行された操作と関連付けて登録されている目標機能(直前に実行された操作との間の関連性が高い目標機能)が判定対象となる。つまり、これらの2つの目標機能が異なる場合には、1つの実行可能操作について、2つの目標機能との間の2つ

の機能関連度スコアが判定される。そして、2つの機能関連度スコアの両方が閾値以上である場合、操作の登録の際には、所定ルールに従って選択された1つの目標機能が関連付けられる。

[0062] 図10は、2回目の機能関連度スコアの判定の際の大規模言語モデルにおける入出力情報の一例を示す。この場合、図示するように、大規模言語モデルにおける入力情報には、過去の操作として、直前に実行された操作に関する情報が設定され、過去の操作によって到達したページのURL及びHTMLとして、過去の画面（トップ画面）に関する情報が設定されている。こうした情報は、ページ管理テーブル154及び操作管理テーブル156において管理されている情報に基づいて、サーバ10によって自動的に生成される。

[0063] 図11は、この時点における操作管理テーブル156の内容の一例を示す。図示するように、図11の例では、画面IDが「S01」である画面（トップ画面）における操作IDが「O01」である操作が実行されており（実行済みフラグが「1」）、遷移先の画面IDが「S02」である画面における実行可能操作のうち、操作IDが「O01」の操作が、機能IDが「F01」の目標機能と関連付けて登録されており、さらに、操作IDが「O02」の操作が、機能IDが「F02」の目標機能（遷移先の画面に基づく目標機能）と関連付けて登録されている。

[0064] 図7のフローチャートに戻り、そして、その時点で未実行の登録済みの操作の中から、所定ルールに従って特定される操作が、実行対象操作として決定及び実行され（ステップS250）、当該操作の実行に応じた遷移先画面への遷移が画面遷移に新たに追加される（ステップS260）。これらの処理は、未実行の登録済みの操作がなくなるまで（ステップS240においてNO）の間、繰り返される。

[0065] 図5のフローチャートに戻り、こうして画面遷移が設定されると、続いて、サーバ10は、設定された画面遷移に従って、脆弱性の検査を実行する（ステップS120）。具体的には、ウェブブラウザを起動し、ページ管理テ

ーブル154において管理されている情報に従って、画面遷移に含まれる各画面を順に訪れて、予め定められた脆弱性の検査項目の検査を行う。脆弱性の検査項目は、例えば、OWASP Top10において規定されている項目を含む。検査結果は、ページ管理テーブル154の検査結果情報に登録される。なお、ウェブサイトの自動巡回の際に（つまり、画面遷移の設定の際に）、各画面において、検査項目の検査を行うようにしてもよい。

[0066] 図12は、ユーザ端末30において出力される、検査結果を確認するための検査結果確認画面60を例示する。当該画面60は、図示するように、脆弱性の検査結果を一覧表示する一覧表示領域62を有する。当該領域62は、各画面の脆弱性の検査結果（深刻度、脆弱性名、検出箇所、及び、脆弱箇所等）を一覧表示する。これらの情報は、ページ管理テーブル154の検査結果情報において管理されている。

[0067] 上述した例では、脆弱性検査の目標機能（検査必要機能）を設定する際に、対応する画面のHTMLデータが入力されると、各機能の検査必要性スコアを出力する学習済みモデルを用いるようにしたが、大規模言語モデルを用いて目標機能を設定するようにしてもよい。図13は、目標機能を設定する際の大規模言語モデルにおける入出力情報の一例を示す。この場合、図示するように、入力情報として、現在の画面のHTMLデータに加えて、他の画面（遷移元の画面等）のHTMLデータが設定され得る。さらに、こうした目標機能の設定を、ルールベースの手法で実現してもよい。

[0068] 上述した例において、大規模言語モデルを用いて機能関連度スコアを取得する際に、当該スコアに加えて、当該スコアの根拠を取得するようにしてもよい。図14は、この場合の大規模言語モデルにおける入出力情報の一例を示す。こうした根拠の情報は、例えば、操作管理テーブル156において管理することができ、スコアの妥当性の検証、及び、操作実績の一部として利用することができる。また、こうした機能関連度の判定を、ルールベースの手法で実現してもよい。

[0069] 以上説明した本実施形態に係る脆弱性検査サーバ10は、ウェブサイト2

2を自動巡回する際に、脆弱性の検査が必要な検査必要機能を判定し、ウェブページにおいて実行可能な複数の実行可能操作の各々と検査必要機能との間の関連度を判定し、これらの複数の実行可能操作のうち、当該関連度に基づいて特定される操作を実行するから、検査が必要な機能との間の関連度に基づいて特定される操作の実行が可能となり、重要な機能に対応するウェブページへの巡回が促進され得る。つまり、脆弱性検査サーバ10は、ウェブサイトの脆弱性検査において、重要な機能の検査漏れを抑制する。

[0070] 本発明の他の実施形態において、上述した実施形態における脆弱性検査サーバ10が有する機能の一部又は全部は、脆弱性検査サーバ10及びユーザ端末30が協働することによって実現され、又は、ユーザ端末30によって実現され得る。

[0071] 本明細書で説明された処理及び手順は、明示的に説明されたもの以外にも、ソフトウェア、ハードウェアまたはこれらの任意の組み合わせによって実現される。例えば、本明細書で説明される処理及び手順は、集積回路、揮発性メモリ、不揮発性メモリ、磁気ディスク等の媒体に、当該処理及び手順に相当するロジックを実装することによって実現される。また、本明細書で説明された処理及び手順は、当該処理・手順に相当するコンピュータプログラムとして実装し、各種のコンピュータに実行させることが可能である。

[0072] 本明細書中で説明された処理及び手順が単一の装置、ソフトウェア、コンポーネント、モジュールによって実行される旨が説明されたとしても、そのような処理または手順は複数の装置、複数のソフトウェア、複数のコンポーネント、及び／又は複数のモジュールによって実行され得る。また、本明細書において説明されたソフトウェアおよびハードウェアの要素は、それらをより少ない構成要素に統合して、またはより多い構成要素に分解することによって実現することも可能である。

[0073] 本明細書において、発明の構成要素が単数もしくは複数のいずれか一方として説明された場合、又は、単数もしくは複数のいずれとも限定せずに説明された場合であっても、文脈上別に解すべき場合を除き、当該構成要素は単

数又は複数のいずれであってもよい。

請求の範囲

- [請求項1] 1又は複数のコンピュータプロセッサを備え、ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するためのシステムであって、前記1又は複数のコンピュータプロセッサは、
- 前記ウェブサイトに含まれる第1ウェブページを取得するステップと、
- 前記第1ウェブページに関する第1ページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するステップと、
- 前記第1ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、
- 前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、
- 前記複数の実行可能操作のうち、前記関連度に基づいて特定される第1操作を実行するステップと、
- 前記第1操作の実行に応じて第2ウェブページを取得するステップと、を実行する、
- システム。
- [請求項2] 前記第1操作は、前記複数の実行可能操作のうち、前記関連度が高い実行可能操作が優先して特定される、
- 請求項1のシステム。
- [請求項3] 前記検査必要機能を判定するステップは、前記第1ページ情報を含む第1入力情報を第1学習済みモデルに入力し、前記第1学習済みモデルから出力される、前記検査必要機能を特定するための第1出力情報に基づいて、前記検査必要機能を判定することを含む、
- 請求項1のシステム。
- [請求項4] 前記第1出力情報は、前記検査必要機能を特定する情報を含む、
- 請求項3のシステム。
- [請求項5] 前記第1出力情報は、所定の複数の機能の各々の、脆弱性の検査が

必要な可能性を示す可能性情報を含み、

前記検査必要機能を判定するステップは、前記所定の複数の機能のうち、脆弱性の検査が必要な可能性が高い機能が優先されるように、前記検査必要機能を判定する、

請求項 3 のシステム。

[請求項 6] 前記 1 又は複数のコンピュータプロセッサは、さらに、前記第 1 ページ情報に加えて、前記第 2 ウェブページに関する第 2 ページ情報にさらに基づいて、前記検査必要機能を再度判定するステップを実行する、

請求項 1 のシステム。

[請求項 7] 前記関連度を判定するステップは、前記第 1 ページ情報、及び、前記複数の実行可能操作の各々と前記検査必要機能との組合せを含む第 2 入力情報を第 2 学習済みモデルに入力し、前記第 2 学習済みモデルから出力される、前記関連度を判定するための第 2 出力情報に基づいて、前記関連度を判定する、

請求項 1 のシステム。

[請求項 8] 前記第 2 出力情報は、前記関連度を含む、

請求項 7 のシステム。

[請求項 9] 前記第 1 ウェブページを取得するステップは、第 2 操作の実行に応じて前記第 1 ウェブページを取得し、

前記第 2 入力情報は、前記第 2 操作を特定する情報をさらに含む、

請求項 7 のシステム。

[請求項 10] 1 又は複数のコンピュータによって実行され、ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するための方法であって、

前記ウェブサイトに含まれる第 1 ウェブページを取得するステップと、

前記第 1 ウェブページに関する第 1 ページ情報に基づいて、脆弱性

の検査が必要な検査必要機能を判定するステップと、

前記第 1 ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、

前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、

前記複数の実行可能操作のうち、前記関連度に基づいて特定される第 1 操作を実行するステップと、

前記第 1 操作の実行に応じて第 2 ウェブページを取得するステップと、を備える、

方法。

[請求項11]

ウェブサイトの自動巡回を伴って前記ウェブサイトの脆弱性を検査するためのプログラムであって、1 又は複数のコンピュータに、

前記ウェブサイトに含まれる第 1 ウェブページを取得するステップと、

前記第 1 ウェブページに関する第 1 ページ情報に基づいて、脆弱性の検査が必要な検査必要機能を判定するステップと、

前記第 1 ウェブページにおいて実行可能な複数の実行可能操作を特定するステップと、

前記複数の実行可能操作の各々と前記検査必要機能との間の関連度を判定するステップと、

前記複数の実行可能操作のうち、前記関連度に基づいて特定される第 1 操作を実行するステップと、

前記第 1 操作の実行に応じて第 2 ウェブページを取得するステップと、を実行させる、

プログラム。