

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7463021号
(P7463021)

(45)発行日 令和6年4月8日(2024.4.8)

(24)登録日 令和6年3月29日(2024.3.29)

(51)国際特許分類

F I

G 0 6 F 21/57 (2013.01)

G 0 6 F 21/57 3 7 0

請求項の数 8 (全17頁)

(21)出願番号	特願2020-176277(P2020-176277)	(73)特許権者	520409888
(22)出願日	令和2年10月20日(2020.10.20)		株式会社Flat Security
(65)公開番号	特開2022-67533(P2022-67533A)		東京都文京区本郷3丁目43番16号コ
(43)公開日	令和4年5月6日(2022.5.6)		ア本郷ビル2階A室
審査請求日	令和5年9月19日(2023.9.19)	(74)代理人	230121016
特許法第30条第2項適用 (1) 公開1 ▲1▼公開			弁護士 小笠原 匡隆
日:2020年9月17日 ▲2▼配信場所:https://signal.diamond.jp/articles/-/286 ▲3▼公開者:株式会社ダイヤモンド社 ▲4▼配信した内容:公開者が、上記配信場所に		(72)発明者	米内 貴志
記載のウェブサイトを通じて米内貴志が発明したトレーニングシステムを用いたサービスについて公開した。(			東京都文京区本郷3丁目43番16号コ
2) 公開2 ▲1▼公開日:2020年9月17日 ▲2			ア本郷ビル2階A室 株式会社Flat Security内
▼配信場所:https://flatt.tech/learning_platform/ ▲3▼公開者:		審査官	平井 誠
最終頁に続く			

最終頁に続く

(54)【発明の名称】 サーバー装置、プログラム及び方法

(57)【特許請求の範囲】

【請求項1】

ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をするように構成された通信インターフェイスと、

所定の指示命令に加え、あらかじめ運営者によって意図的に1又は複数の脆弱性が含まれた修正対象ソースコードと、前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリと、

前記所定の指示命令に基づいて、

前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信し、

前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象ソースコードを前記端末装置から受信し、

受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する、

ための処理をするように構成されたプロセッサと、

を含むサーバー装置。

【請求項2】

前記プロセッサは、前記評価の結果を、前記通信インターフェイスを介して、前記端末装置に対して送信するための処理をするように構成された、請求項1に記載のサーバー装置。

【請求項 3】

前記修正の程度は、前記運営者によって意図的に含まれた前記脆弱性が前記修正対象ソースコードにおいて解消されたか否かである、請求項 1 又は 2 に記載のサーバー装置。

【請求項 4】

前記修正対象ソースコードは、前記運営者によって意図的に含まれた複数の脆弱性を含み、

前記評価の程度は、前記複数の脆弱性のうち前記修正対象ソースコードにおいて解消した脆弱性の数に基づく、

請求項 1 ～ 3 のいずれか一項に記載のサーバー装置。

【請求項 5】

前記修正対象ソースコードは、既存のウェブサービス又はアプリケーションにおいて用いられるコードの少なくとも一部に基づくものである、請求項 1 ～ 4 のいずれか一項に記載のサーバー装置。

【請求項 6】

前記修正対象ソースコードは、前記既存のウェブサービス又はアプリケーションにおけるログインに係る処理を実行するためのものである、請求項 5 に記載のサーバー装置。

【請求項 7】

ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をるように構成された通信インターフェイスと、あらかじめ運営者によって意図的に 1 又は複数の脆弱性が含まれた修正対象ソースコードと前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリと、を含むコンピュータを、

前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信し、

前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象ソースコードを前記端末装置から受信し、

受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する、

ための処理をするように構成されたプロセッサ

として機能させるプログラム。

【請求項 8】

ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をるように構成された通信インターフェイスと、所定の指示命令に加えあらかじめ運営者によって意図的に 1 又は複数の脆弱性が含まれた修正対象ソースコードと前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリとを含むコンピュータにおいて、プロセッサが前記所定の指示命令を実行することによりなされる方法であって、

前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信する段階と、

前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象ソースコードを前記端末装置から受信する段階と、

受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する段階と、

を含む方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、脆弱性を含むソースコードの修正の程度を評価するためのサーバー装置、プログラム及び方法に関する。

【背景技術】

【0002】

従来より、ウェブアプリケーションやスマートフォン向けアプリケーションを介して行われるウェブサービスを実行するためのソースコードにおいて、脆弱性が含まれるか否かを検査するシステムが知られていた。例えば、特許文献1は、ブロックチェーンの仕様に基づき予め定められた評価項目にしたがってコントラクトのソースコードの脆弱性を検出することで、ブロックチェーンに関連するソースコードの脆弱性を検出する精度を向上させたシステムが記載されている。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2019-003309号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

そこで、上記のような技術を踏まえ、本開示では、ソースコードに含まれた脆弱性の修正の程度を評価することが可能なサーバー装置、プログラム及び方法を提供する。

【課題を解決するための手段】

【0005】

本開示の一態様によれば、「ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をするように構成された通信インターフェイスと、所定の指示命令に加え、あらかじめ運営者によって意図的に1又は複数の脆弱性が含まれた修正対象ソースコードと、前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリと、前記所定の指示命令に基づいて、前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信し、前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象ソースコードを前記端末装置から受信し、受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する、ための処理をするように構成されたプロセッサと、を含むサーバー装置」が提供される。

【0006】

本開示の一態様によれば、「ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をするように構成された通信インターフェイスと、あらかじめ運営者によって意図的に1又は複数の脆弱性が含まれた修正対象ソースコードと前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリと、を含むコンピュータを、前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信し、前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象ソースコードを前記端末装置から受信し、受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する、ための処理をするように構成されたプロセッサとして機能させるプログラム」が提供される。

【0007】

本開示の一態様によれば、「ネットワークを介して通信可能に接続された端末装置との間で所定の情報の送受信をするように構成された通信インターフェイスと、所定の指示命令に加えあらかじめ運営者によって意図的に1又は複数の脆弱性が含まれた修正対象ソースコードと前記修正対象ソースコードに関連付けられた攻撃コードとを記憶するように構成されたメモリとを含むコンピュータにおいて、プロセッサが前記所定の指示命令を実行することによりなされる方法であって、前記通信インターフェイスを介して、前記端末装置に前記修正対象ソースコードを送信する段階と、前記通信インターフェイスを介して、前記端末装置を保持するユーザによって前記脆弱性に対する修正がなされた前記修正対象

10

20

30

40

50

ソースコードを前記端末装置から受信する段階と、受信した前記修正対象ソースコードに対して、前記修正対象ソースコードに関連付けられた前記攻撃コードによる攻撃を実行することによって、前記修正の程度を評価する段階と、を含む方法」が提供される。

【発明の効果】

【0008】

本開示によれば、ソースコードに含まれた脆弱性の修正の程度を評価することが可能なサーバー装置、プログラム及び方法を提供することができる。

【0009】

なお、上記効果は説明の便宜のための例示的なものであるにすぎず、限定的なものではない。上記効果に加えて、又は上記効果に代えて、本開示中に記載されたいかなる効果や当業者であれば明らかな効果を奏することも可能である。

【図面の簡単な説明】

【0010】

【図1】図1は、本開示に係るシステム1の構成を概略的に示す概念図である。

【図2】図2は、本開示に係るサーバー装置100の構成の例を示すブロック図である。

【図3】図3は、本開示に係る端末装置200の構成の例を示すブロック図である。

【図4A】図4Aは、本開示に係るサーバー装置100に記憶されるユーザ情報テーブルを概念的に示す図である。

【図4B】図4Bは、本開示に係るサーバー装置100に記憶されるソースコード情報テーブルを概念的に示す図である。

【図5】図5は、本開示に係るシステム1において実行される処理シーケンスを示す図である。

【図6】図6は、本開示に係る端末装置200において実行される処理フローを示す図である。

【図7】図7は、本開示に係るサーバー装置100において実行される処理フローを示す図である。

【図8A】図8Aは、本開示に係る端末装置200に表示される画面の例を示す図である。

【図8B】図8Bは、本開示に係る端末装置200に送信される修正対象ソースコードの例を示す図である。

【図9】図9は、本開示に係る端末装置200から送信される修正後の修正対象ソースコードの例を示す図である。

【発明を実施するための形態】

【0011】

添付図面を参照して本開示の様々な実施形態を説明する。なお、図面における共通する構成要素には同一の参照符号が付されている。

【0012】

1. 本開示に係るシステムの概要

本開示に係るシステムは、主にサーバー装置及び当該サーバー装置にネットワークを通じて通信可能に接続された端末装置を含む。当該システムは、一例としては、端末装置がサーバー装置からダウンロードした脆弱性を含む修正対象のソースコードに対して修正を行い、その修正後のソースコードがアップロードされたサーバー装置において修正ができているか否かを評価するためのセキュリティリスクに対するトレーニングサービスに利用される。なお、当該トレーニングサービスは本開示に係るシステムの適用例の一例である。

【0013】

なお、本開示において、「運営者」という用語は、端末装置を保持するユーザとの区別のために用いているにすぎない。したがって、特定の一個人を指すことを明記している場合を除き、特定の一個人を指す場合もあれば、当該個人に関連する組織（例えば、会社や組合、団体、集団など）を指す場合もある。

【0014】

また、本開示において、修正対象ソースコードには、「意図的に」運営者によって脆弱

10

20

30

40

50

性が含まれているが、この「意図的」というのは運営者自らが、脆弱性があるコードを作成したことを意味するものではない。例えば、善意又は悪意のある第三者が作成したソースコードであっても、運営者が脆弱性があることを把握したうえで本開示に係る修正対象ソースコードとして利用することが可能である。また、善意又は悪意のある第三者が作成したソースコードにおいて運営者自らが脆弱性がある箇所を特定可能に把握しておらずとも、本開示に係る修正対象ソースコードとして利用することが可能である。

【0015】

2. 本開示に係るシステム1の構成

図1は、本開示に係るシステム1の構成を概略的に示す概念図である。図1を参照すると、システム1は、サーバー装置100及び端末装置200を含む。そして、サーバー装置100及び端末装置200は、互いにネットワークを通じて通信可能に接続される。

【0016】

なお、本開示においては、端末装置200は、1台しか記載されていないが、当然2台又は3台以上の端末装置を含むことも可能である。また、サーバー装置100は単一のものとして記載されているが、各構成要素及び処理を複数のサーバー装置に分配したり、各種データベースと接続することも可能である。

【0017】

3. サーバー装置100の構成

図2は、本開示に係るサーバー装置100の構成の例を示すブロック図である。サーバー装置100は、図2に示す構成要素の全てを備える必要はなく、一部を省略した構成をとることも可能であるし、他の構成要素を加えることも可能である。

【0018】

図2によると、サーバー装置100は、RAM、ROM、及び不揮発性メモリ、HDD等を含むメモリ111、CPU等から構成されるプロセッサ112、出力インターフェイス113、及び通信インターフェイス114を含む。そして、これらの各構成要素が制御ライン及びデータラインを介して互いに電氣的に接続される。なお、メモリ111には、通信インターフェイス等を介して接続されたデータベースや外部記憶装置なども含む。

【0019】

メモリ111は、RAM、ROM、不揮発性メモリ、HDDを含み、記憶部として機能する。当該メモリ111は、本開示に係るアプリケーションやOSを実行するための指示命令をプログラムとして記憶する。このようなプログラムは、プロセッサ112によってロードされ実行される。また、メモリ111は、ユーザ情報テーブル(図4A)及びソースコード情報テーブル等の各種テーブルを記憶する。さらに、メモリ111(特にRAM)は、上記プログラムがプロセッサ112によって実行される間、データの書き込み及び読み込みを実行するために一時的に用いられる。本開示においては、メモリ111は、特に、端末装置200からの要求を受けて通信インターフェイス114を介して端末装置200に修正対象ソースコードを送信する処理、通信インターフェイス114を介して端末装置200を保持するユーザによって脆弱性に対する修正がなされた修正対象ソースコードを端末装置200から受信する処理、受信した修正対象ソースコードに対して当該修正対象ソースコードに関連付けられた攻撃コードによる攻撃を実行する処理、攻撃の実行の結果脆弱性が解消しているか否かを判断してその修正の程度を評価する処理、評価の結果を通信インターフェイスを介して端末装置200に送信する処理等を実行するためのプログラムを記憶する。

【0020】

プロセッサ112は、CPU(マイクロコンピュータ:マイコン)から構成され、メモリ111に記憶された各種プログラムに基づいて、接続された他の構成要素を制御するための制御部として機能する。本開示においては、特に、プロセッサ112は、端末装置200からの要求を受けて通信インターフェイス114を介して端末装置200に修正対象ソースコードを送信する処理、通信インターフェイス114を介して端末装置200を保持するユーザによって脆弱性に対する修正がなされた修正対象ソースコードを端末装置2

10

20

30

40

50

00から受信する処理、受信した修正対象ソースコードに対して当該修正対象ソースコードに関連付けられた攻撃コードによる攻撃を実行する処理、攻撃の実行の結果脆弱性が解消しているか否かを判断してその修正の程度を評価する処理、評価の結果を通信インターフェイスを介して端末装置200に送信する処理等を実行する。プロセッサ112は、単一のCPUで構成されても良いが、複数のCPUで構成しても良い。

【0021】

通信インターフェイス114は、一例として、端末装置200、依頼者端末装置300及び／又は他のサーバー装置とネットワークを介して、本開示に係るシステム1において用いられるプログラム、各種情報等を送受信するために、変調や復調などの処理を行う通信部として機能する。通信インターフェイス114は、上記の無線通信方式や公知の有線通信方式にしたがって、端末装置200及び／又は他のサーバー装置と通信する。本開示においては、通信インターフェイス114を介して、端末装置200から修正対象ソースコードの送信要求、修正後の修正対象ソースコードなどが受信され、端末装置200に修正対象ソースコード、評価結果などが送信される。

10

【0022】

出力インターフェイス113は、特に図示はしていないが、プリンタやディスプレイ等の様々な外部機器との間で情報の入出力をするための情報入出力部として機能する。出力インターフェイス113は、シリアルポート、パラレルポート、USB等、所望に応じて公知の接続形式を採用することが可能である。

20

【0023】

4. 端末装置200の構成

図3は、本開示に係る端末装置200の構成の例を示すブロック図である。端末装置200は、図3に示す構成要素の全てを備える必要はなく、一部を省略した構成をとることも可能であるし、他の構成要素を加えることも可能である。

【0024】

端末装置200は、一例としては、ラップトップパソコンに代表される無線通信可能な携帯型の端末装置が挙げられる。しかし、それ以外にも、スマートフォン、フィーチャーフォン、携帯情報端末、PDA、デスクトップパソコン、携帯型ゲーム機、据え置き型ゲーム機など、本開示に係るプログラムを実行可能な装置であれば、いずれでも好適に適用することが可能である。また、本開示に係るプログラムが複数の端末装置200で実行される場合、必ずしも各端末装置200が同じか同種のものである必要はない。例えば、ある端末装置200はデスクトップパソコンで、その他の端末装置200はラップトップパソコンであってもよい。

30

【0025】

図3によると、端末装置200は、ディスプレイ211、プロセッサ212、RAM、ROM、又は不揮発性メモリ（場合によっては、HDD）等を含むメモリ213、通信処理回路215及びアンテナを含む通信インターフェイス214、タッチパネル217及びハードキー218を含む入力インターフェイス216を含む。そして、これらの各構成要素が制御ライン及びデータラインを介して互いに電氣的に接続される。

【0026】

ディスプレイ211は、プロセッサ212の指示に応じて、メモリ213に記憶された画像情報を読み出して、本開示に係るプログラムを実行することによって出力される各種表示（例えば、図8A）を行う表示部として機能する。ディスプレイ211は、例えば液晶ディスプレイ、有機ELディスプレイ又は電子ペーパー等から構成される。

40

【0027】

入力インターフェイス216は、タッチパネル217、ハードキー218、マウス（図示しない）等から構成され、本開示に係るプログラムの実行や、修正対象ソースコードに対する修正などの各種指示入力を受け付ける。タッチパネル217は、ディスプレイ211の表示する画像データに対応する位置座標の情報をプロセッサ212に出力する。タッチパネル方式としては、抵抗膜方式、静電容量結合方式、超音波表面弾性波方式など、公

50

知の方式を利用することができる。本開示においては、タッチパネル 217 は、指示体によりディスプレイ 211 に表示された各アイコン等に対する操作をするためのポインタの移動操作や、各アイコンに対する選択操作を検出する。また、ハードキー 218 は、例えばキーボード等を含み、修正対象ソースコードに対する修正コードの入力やユーザ ID 情報の入力など、文字やテキスト情報などの入力に用いられる。

【0028】

プロセッサ 212 は、CPU（マイクロコンピュータ：マイコン）から構成され、メモリ 213 に記憶された各種プログラムに基づいて、接続された他の構成要素を制御する制御部として機能する。具体的には、プロセッサ 212 は、本開示に係るアプリケーションを実行するためのプログラムや OS を実行するためのプログラムをメモリ 213 から読み出して実行する。本開示においては、本開示に係るアプリケーションの起動の指示入力を入力インターフェイス 216 で受け付けると当該アプリケーションを起動する処理、入力インターフェイス 216 で受け付けた指示入力に応じて修正対象ソースコードの送信要求を通信インターフェイス 214 を介してサーバ装置 100 に送信する処理、修正対象ソースコードを通信インターフェイス 214 を介してサーバ装置 100 から受信する処理、修正対象ソースコードに対してユーザによる修正がなされた修正後の修正対象ソースコードの入力を受け付ける処理、受け付けられた修正対象ソースコードを通信インターフェイス 214 を介してサーバ装置 100 に送信する処理、通信インターフェイス 214 を介してサーバ装置 100 から修正対象ソースコードに対する修正の評価結果を受信し、それを出力する処理等を実行する。なお、プロセッサ 212 は、単一の CPU で構成されても良いが、複数の CPU で構成しても良い。また、画像処理に特化した GPU 等、他の種類のプロセッサを適宜組み合わせてもよい。

【0029】

メモリ 213 は、ROM、RAM、不揮発性メモリ、HDD 等から構成され、記憶部として機能する。ROM は、本開示に係るアプリケーションや OS を実行するための指示命令をプログラムとして記憶する。RAM は、ROM に記憶されたプログラムがプロセッサ 212 により処理されている間、データの書き込み及び読み込みをするために用いられるメモリである。不揮発性メモリは、当該プログラムの実行によってデータの書き込み及び読み込みが実行されるメモリであって、ここに書き込まれたデータは、当該プログラムの実行が終了した後も保存される。本開示においては、メモリ 213 は、特に、本開示に係るアプリケーションの起動の指示入力を入力インターフェイス 216 で受け付けると当該アプリケーションを起動する処理、入力インターフェイス 216 で受け付けた指示入力に応じて修正対象ソースコードの送信要求を通信インターフェイス 214 を介してサーバ装置 100 に送信する処理、修正対象ソースコードを通信インターフェイス 214 を介してサーバ装置 100 から受信する処理、修正対象ソースコードに対してユーザによる修正がなされた修正後の修正対象ソースコードの入力を受け付ける処理、受け付けられた修正対象ソースコードを通信インターフェイス 214 を介してサーバ装置 100 に送信する処理、通信インターフェイス 214 を介してサーバ装置 100 から修正対象ソースコードに対する修正の評価結果を受信し、それを出力する処理等のためのプログラムを記憶する。

【0030】

通信インターフェイス 214 は、通信処理回路 215 及びアンテナを介して、遠隔に設置されたサーバ装置 100 や他の端末装置との間で情報の送受信をする通信部として機能する。通信処理回路 215 は、本開示に係るシステムにおいて用いられるプログラムや各種情報等を処理の進行に応じて、サーバ装置 100 から受信するための処理をする。本開示においては、特に、通信インターフェイス 214 を介して、サーバ装置 100 に対して修正対象ソースコードの送信要求や修正済みの修正対象ソースコードなどが送信され、サーバ装置 100 から修正対象ソースコードやユーザが行った修正に対する評価結果などが受信される。

【0031】

通信処理回路 215 は、LTE 方式に代表されるような広帯域の無線通信方式に基づいて処理されるが、IEEE 802.11 に代表されるような無線 LAN や Bluetooth (登録商標) のような狭帯域の無線通信に関する方式に基づいて処理することも可能である。また、無線通信に代えて、又は加えて、有線通信を用いることも可能である。

【0032】

5. メモリ等に記憶される情報

図 4A は、本開示に係るサーバー装置 100 に記憶されるユーザ情報テーブルを概念的に示す図である。一例としては、当該テーブルには、端末装置 200 で本開示のプログラムを起動しユーザ登録を行うことによって生成又は入力される情報が記憶される。これらの情報は、各ユーザや運営者からの指示入力などに応じて適宜更新されうる。

【0033】

図 4A によると、ユーザ ID 情報に対応付けて、ユーザ名情報、ランク情報、修正後のソースコード情報、評価情報等が記憶される。「ユーザ ID 情報」は、各ユーザに付与された固有の情報で、各ユーザを特定するための情報である。当該情報は、新たなユーザが新規のユーザ登録を行うたびに生成され記憶される。「ユーザ名情報」は、ユーザの呼称に関する情報で、各ユーザが任意に入力することも可能である。「ランク情報」は各ユーザの脆弱性の修正に対する習熟度を示す情報である。その一例としては、「初級」、「中級」、「上級」等の分類であったり、「レベル 1」、「レベル 2」、「レベル 3」などの数値などが挙げられる。「修正後のソースコード情報」は、各ユーザが保持する端末装置 200 から送信された修正済みの修正対象ソースコードである。「評価情報」は、修正済みの修正対象ソースコードに対して攻撃コードを実行して脆弱性が解消したか否かなどの各ユーザに対する評価に関する情報である。一例としては、脆弱性が解消したか否かに関する情報や、修正対象ソースコードに含まれる複数の脆弱性のうち解消した数に関する情報や、それらに基づいて分類（例えば、「優」、「良」、「可」、「不可」など）した情報やスコア化した情報などが挙げられる。

【0034】

図 4B は、本開示に係るサーバー装置 100 に記憶されるソースコード情報テーブルを概念的に示す図である。一例としては、当該テーブルには、運営者によって修正対象となる修正対象ソースコードが新たに登録されるごとに記憶される。これらの情報は、運営者からの指示入力などに応じて適宜更新されうる。

【0035】

図 4B によると、ソースコード ID 情報に対応付けて、修正対象ソースコード情報と攻撃コード情報とが記憶される。「ソースコード ID 情報」は、各ソースコードに付与された固有の情報で、各ソースコードを特定するための情報である。当該情報は、新たに修正対象ソースコードが運営者によって登録されるごとに生成され記憶される。「修正対象ソースコード情報」は、ユーザが修正すべきソースコードそのもの、又は当該ソースコードが記憶されたリンク先の情報が記憶される。当該修正対象ソースコードには、運営者によって意図的に含まされた一又は複数の脆弱性が含まれている。「攻撃コード情報」は、対応する修正対象ソースコード情報により特定される修正対象ソースコードに含まれる脆弱性に対して攻撃を実行するためのコード又は当該コードのリンク先の情報が記憶される。当該攻撃コードを修正後の修正対象ソースコードに対して実行することによって、修正対象ソースコードに含まれる脆弱性が解消しているか否かを判断することが可能となる。

【0036】

なお、本開示においては、このようなソースコード情報テーブルをランクごとに対応付けて用意する。このように、ランクに分けて用意することによって、ユーザの習熟度に応じて脆弱性解消の困難度を変更することができ、ユーザの習熟度に応じた柔軟な対応が可能となる。

【0037】

6. システム 1 において実行される処理シーケンス

図 5 は、本開示に係るシステム 1 において実行される処理シーケンスを示す図である。

具体的には、図 5 は、サーバー装置 100 及び端末装置 200 の間で実行される様々な処理の処理シーケンスの一部を示す。

【0038】

図 5 によると、サーバー装置 100 は、あらかじめメモリ 111 のソースコード情報テーブルに修正対象ソースコードをソースコード ID 情報に対応付けて記憶する (S11)。記憶される修正対象ソースコードには、あらかじめ運営者によって意図的に一又は複数の脆弱性が含まれている。

【0039】

他方、端末装置 200 においては、プロセッサ 212 が、入力インターフェイス 216 でユーザの指示入力を受け付けることで、本開示に係るアプリケーションを起動する (S12)。その後、プロセッサは端末装置 200 のディスプレイ 211 に当該アプリケーションに係る表示を行う。具体的には予め登録されたユーザ ID やパスワードの入力を行い、適宜サーバー装置 100 と通信を行ってユーザの認証を行う。その後、プロセッサ 212 は、ディスプレイ 211 にユーザの脆弱性解消に関する画面を表示し、当該画面において入力インターフェイス 216 を介して、ユーザによる修正対象ソースコードが含まれたファイルのダウンロードに関する指示入力を受け付ける (S13)。そして、プロセッサ 212 は、通信インターフェイス 214 を介して、サーバー装置 100 に修正対象ソースコードが含まれたファイルの送信要求 (T11) と当該ユーザのユーザ ID 情報等を送信する。

【0040】

サーバー装置 100 において通信インターフェイス 114 を介して送信要求等を受信すると、プロセッサ 112 は、メモリ 111 のユーザ情報テーブル及びソースコード情報テーブルを参照し、ユーザ ID 情報に対応付けられたランク情報のソースコード情報テーブルから当該ユーザに対して出題する修正対象ソースコードを読み出す (S14)。具体的には、プロセッサ 112 は、ランク情報に基づいてそのランクに応じたソースコード情報テーブルが特定されると、特定されたソースコード情報テーブル内に含まれるソースコードから、ランダムに、又は予め決められた順序に従って一又は複数のソースコードを修正対象ソースコードとして選択する。そして、プロセッサ 112 は、通信インターフェイス 114 を介して、読み出された一又は複数の修正対象ソースコード (T12) とそれに対応付けられたソースコード ID 情報とを、送信要求を送信してきた端末装置 200 に対して送信する。

【0041】

端末装置 200 において通信インターフェイス 214 を介して修正対象ソースコード等が受信されると、プロセッサ 212 は、メモリ 213 に記憶するとともに、受信した修正対象ソースコードをディスプレイ 211 の画面に表示する。そして、プロセッサ 212 は、入力インターフェイス 216 を介して受け付けられたユーザによる、修正対象ソースコードに対する脆弱性の修正指示、すなわち堅牢化指示を受け付け、その修正後の修正対象ソースコードをメモリ 213 に記憶する (S15)。なお、修正対象ソースコードに対する脆弱性の修正は、修正対象ソースコードを受信した端末装置 200 で行ってもよいし、他の端末装置を用いて修正を行ったうえで、修正後の修正対象ソースコードを当該端末装置 200 にダウンロードして記憶するようにしてもよい。そして、プロセッサ 112 は、修正後の修正対象ソースコードが記憶されると、メモリ 213 から読み出して修正後の修正対象ソースコード (T13) と、当該ソースコードに対応付けられたソースコード ID 情報、及びユーザ ID 情報を通信インターフェイス 214 を介してサーバー装置 100 に送信する。

【0042】

サーバー装置 100 において修正後の修正対象ソースコードが通信インターフェイス 114 を介して受信されると、プロセッサ 112 は、受信したソースコード ID 情報に対応付けられた攻撃コードを特定し、修正後の修正対象ソースコードに対して当該攻撃コードを用いて疑似的な攻撃を実行する (S16)。そして、プロセッサ 112 は、実行した疑

10

20

30

40

50

似的な攻撃の結果を受けて、修正後の修正対象ソースコードに対して評価を行う（S 1 7）。このような評価は、一例としては、予め意図的に運営者によって含まれた脆弱性が解消したか否か、そのような脆弱性が複数ある場合にはそのうち何個の脆弱性を解消することができたか、そのような脆弱性がある箇所を正確に特定することができたか否か、及びそれらの組み合わせによって少なくとも行われる。プロセッサ 1 1 2 は、脆弱性に対する修正の評価が行われると、その評価結果をユーザ ID 情報に対応付けてユーザ情報テーブルに記憶する（S 1 8）。そして、プロセッサ 1 1 2 は、通信インターフェイス 1 1 4 を介して記憶した評価結果（T 1 4）を端末装置 2 0 0 に送信する。なお、上記評価には、例示したものに加えて、正常系における動作結果なども加えてもよい。

【0 0 4 3】

端末装置 2 0 0 において通信インターフェイス 2 1 4 を介して評価結果が受信されると、プロセッサ 2 1 2 は、メモリ 2 1 3 にその評価結果を記憶するとともに、ディスプレイ 2 1 1 に表示する。これによって、当該処理シーケンスは終了する。

【0 0 4 4】

7. 端末装置 2 0 0 で行われる処理フロー

図 6 は、本開示に係る端末装置 2 0 0 において実行される処理フローを示す図である。具体的には、図 6 は、図 5 の処理シーケンスのうち S 1 3 ～ S 1 5 において端末装置 2 0 0 が行う処理フローである。当該処理フローは、端末装置 2 0 0 のプロセッサ 2 1 2 がメモリ 2 1 3 に記憶されたプログラムを読み出して実行することにより行われる。

【0 0 4 5】

図 6 によると、プロセッサ 2 1 2 は、セキュリティに関する画面において、入力インターフェイス 2 1 6 を介してユーザによる修正対象ソースコードのダウンロードに係る指示入力を受け付けたことによる割込み信号を受信することで開始される（S 1 0 1）。ダウンロードの指示入力が受け付けられると、プロセッサ 2 1 2 は、通信インターフェイス 2 1 4 を制御して、当該端末装置 2 0 0 を保持するユーザのユーザ ID 情報とともに修正対象ソースコードの送信要求を送信する（S 1 0 2）。

【0 0 4 6】

次に、プロセッサ 2 1 2 は、通信インターフェイス 2 1 4 を介してサーバー装置 1 0 0 から修正対象ソースコード及び当該ソースコードに対応付けられたソースコード ID 情報を受信したことによる割込み信号を受信したか否かを判定する（S 1 0 3）。そして、当該割込み信号を受信した場合には、受信した修正対象ソースコードをディスプレイ 2 1 1 に出力する（S 1 0 4）。

【0 0 4 7】

ここで、図 8 A は、本開示に係る端末装置 2 0 0 に表示される画面の例を示す図である。図 8 A によると、受信した修正対象ソースコードが画面右側のソースコード表示領域 1 4 に表示されている。また、画面左側のブラウザ表示画領域 1 3 においては、受信した修正対象ソースコードを例えばブラウザアプリケーションで読み込んだときに表示される画面の一例が表示される。図 8 A の例においては、e コマースなどの既存のウェブサービスにおけるログイン処理を行うためのソースコードに基づいて生成されたソースコードが修正対象ソースコードとして送信され、当該ソースコードを読み込むことでログイン画面が表示されるようになっている。なお、ログイン処理のためのソースコードは修正対象ソースコードの一例であって、他に既存のニュースサイトや SNS などのウェブアプリケーションやスマートフォン向けアプリケーション、PC 向けのソフトウェアなど、様々なソースコードに基づいて修正対象ソースコードを生成することが可能である。

【0 0 4 8】

また、図 8 B は、本開示に係る端末装置 2 0 0 に送信される修正対象ソースコードの例を示す図である。図 8 B によれば、上記のとおり e コマースなどのウェブサービスにおけるログイン処理を行うためのソースコードの一例が示されている。当該ソースコードからも明らかなように、コード 1 5 A、1 6 A 及び 1 7 A の箇所において、当該修正対象ソースコードは運営者によって意図的に含まれた脆弱性を有している。具体的には、コード

10

20

30

40

50

15AはSQLインジェクションの例であり、データベースへの不正アクセス等の原因となりうる。コード16Aはクロスサイトスクリプティング(XSS)の例であり、コード中にHTMLやJavaScriptを埋め込むことでウェブサイト管理者が意図しない行動等の原因となりうる。コード17Aはオープンリダイレクトの例であり、URLを入力したサイトから自動的に悪意のある他のサイトへ移動させる等の原因になりうる。これらの脆弱性を利用することによって、個人情報や秘密情報の漏洩、サイトの不正改ざん等の種々の問題が引き起こされる。

【0049】

再び図6に戻り、プロセッサ212は、図8A及び図8Bに例示された修正対象ソースコードに対して、脆弱性に対する修正がなされた修正後の修正対象ソースコードの入力がなされたことによる割込み信号を受信したか否かを判定する(S105)。ここで、「脆弱性に対する修正」は、完全な堅牢化がなされ脆弱性が完全に解消されたものである必要はない。つまり、「脆弱性に対する修正」とは、ユーザが脆弱性に対して何かしらの対処を行ったか、対処を検討したことを広く意味している。

【0050】

また、修正対象ソースコードに対する修正は、端末装置200の入力インターフェイス216においてユーザの指示入力を受け付けて行ってもよい。また、修正対象ソースコードに対する修正は、他の端末装置で行って、修正後の修正対象ソースコードを端末装置200に入力することで行ってもよい。

【0051】

ここで、図9は、本開示に係る端末装置200から送信される修正後の修正対象ソースコードの例を示す図である。図9によると、図8Bに示された修正前の修正対象ソースコードに対して、ユーザによる指示入力を受け付けることで脆弱性の修正がなされ堅牢化されたのちの修正対象ソースコードが示されている。具体的には、図8Bにおいて示されたコード15A、16A及び17Aの箇所において運営者によって意図的に脆弱性が含まれていたところ、当該コード部分がそれぞれコード15B、16B及び17Bのとおり修正され、脆弱性が解消されている。具体的には、SQLインジェクションの脆弱性を有するコード15Aに対しては、コード15Bに示されているように、バインド変数(bind Value)を使用する修正がなされている。また、XSSの脆弱性を有するコード16Aに対しては、コード16Bに示されているように、htmlspecialchars関数を使用する修正がなされている。また、オープンリダイレクトの脆弱性を有するコード17Aに対しては、コード17Bに示されているように、isset関数を使用する修正がなされている。なお、これらの修正は一例であり、当然他の修正であってもよい。また、解消されたか否かについてはユーザによって修正がなされた時には判断をしておらず、サーバー装置100に送信された後攻撃コードを実行することによって判断される。

【0052】

なお、修正対象ソースコードに対する修正は、図9の例では、脆弱性が全て解消し完全な堅牢化がなされたのちのソースコードが示されている。しかし、これに限らず、修正対象ソースコードに対する修正は、脆弱性が含まれた箇所を特定したり、一部のみの脆弱性を修正するだけであってもよい。また、修正対象ソースコードに対する修正は、必ずしも「正解」している必要はなく、修正しても依然として脆弱性が解消できていないようなものであってもよい。

【0053】

再び図6に戻り、プロセッサ212は修正後の修正対象ソースコードの入力がなされると、入力された修正後の修正対象ソースコード、ユーザID情報、及び受信した修正対象ソースコードに対応するソースコードID情報を通信インターフェイス214を介してサーバー装置100に送信する(S106)。これによって、図5の処理シーケンスのうちS13～S15において端末装置200が行う処理フローは終了する。

【0054】

8. サーバー装置100で行われる処理フロー

10

20

30

40

50

図 7 は、本開示に係るサーバー装置 100 において実行される処理フローを示す図である。具体的には、図 7 は、図 5 の処理シーケンスのうち S 16～S 18 においてサーバー装置 100 が行う処理フローである。当該処理フローは、サーバー装置 100 のプロセッサ 112 がメモリ 111 に記憶されたプログラムを読み出して実行することにより行われる。

【0055】

図 7 によると、プロセッサ 112 は、通信インターフェイス 114 において端末装置 200 から修正後の修正対象ソースコード等が受信されたことによる割込み信号を受信することで当該処理フローを開始する（S 201）。次に、プロセッサ 112 は、ソースコード情報テーブルを参照して、修正後の修正対象ソースコードとともに受信したソースコード ID 情報に基づいて、当該ソースコード ID 情報に対応する攻撃コードを読み出す（S 202）。そして、プロセッサ 112 は、受信した修正後の修正対象ソースコードに対して、読み出された攻撃コードを適用して、疑似的な攻撃を実行する（S 203）。これによって、プロセッサ 112 は、修正後の修正対象ソースコードにおいて脆弱性がどの程度解消されたのかを評価する（S 204）。

【0056】

このような評価の一例としては、疑似的な攻撃の実行の結果、脆弱性に起因するセキュリティリスクが依然として生じた場合には、「脆弱性が解消できていない」という評価がなされ、脆弱性に起因するセキュリティリスクが生じなかった場合には「脆弱性が解消できた」という評価がなされる。また、修正対象ソースコードにおいて複数の脆弱性が含まれていた場合には、脆弱性が解消できた数もその評価の対象とする。なお、評価は、あらかじめ運営者が作成した模範的な修正後のコードとの一致／不一致を判定することによって行うことも可能である。しかし、実際には脆弱性の解消方法はユーザごとに様々な方法が想定されうるため、S 202 及び S 203 のように攻撃コードを読み出し疑似的な攻撃を実行することによって行うことが好ましい。このようにすることによって、より柔軟性のある評価が可能となる。

【0057】

プロセッサ 112 は、修正後の修正対象ソースコードに対して修正の程度が評価されると、その評価結果をメモリ 111 のユーザ情報テーブルに受信したユーザ ID 情報に対応付けて記憶する。そして、プロセッサ 112 は、記憶した評価結果を、ユーザ ID 情報に対応付けられたユーザが保持する端末装置 200 に対して、通信インターフェイス 114 を介して送信する（S 205）。なお、プロセッサ 112 は、例えば、評価結果をスコア化し、これまで得られたスコア値に累積し、その累積値に応じてランク情報を更新してもよい。例えば、累積値があらかじめ決められた中級の閾値を越えた場合には、プロセッサ 112 は、ユーザ ID 情報に対応付けられたランク情報を、初級から中級に更新して記憶する。これによって、図 5 の処理シーケンスのうち S 16～S 18 において端末装置 200 が行う処理フローは終了する。

【0058】

以上、本開示においては、ソースコードに含まれた脆弱性の修正の程度を評価することが可能なサーバー装置、プログラム及び方法を提供することができる。特に、修正の程度の評価において、修正対象ソースコードに対してあらかじめ対応付けられた攻撃コードを実行し、脆弱性が解消したか否かに基づいて評価するため、柔軟な評価が可能となる。

【0059】

本明細書で説明される処理及び手順は、開示において明示的に説明されたものによってのみならず、ソフトウェア、ハードウェア又はこれらの組み合わせによっても実現可能である。具体的には、本明細書で説明された処理及び手順は、集積回路、揮発性メモリ、不揮発性メモリ、磁気ディスク、光ストレージ等の媒体に、当該処理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る処理及び手順は、それらの処理・手順をコンピュータプログラムとして実装し、端末装置やサーバー装置を含む各種のコンピュータに実行させることが可能である。

10

20

30

40

50

【0060】

本明細書中で説明される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、そのような処理又は手順は、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るものとすることができる。また、本明細書中で説明される各種情報が単一のメモリや記憶部に格納される旨が説明されたとしても、そのような情報は、単一の装置に備えられた複数のメモリ又は複数の装置に分散して配置された複数のメモリに分散して格納されるものとすることができる。さらに、本明細書において説明されるソフトウェア及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、又は、より多い構成要素に分解することによって実現されるものとすることができる。

10

【符号の説明】

【0061】

100 サーバ装置

200 端末装置

20

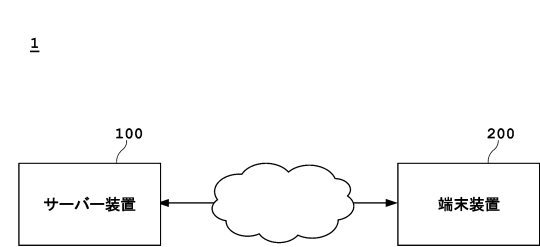
30

40

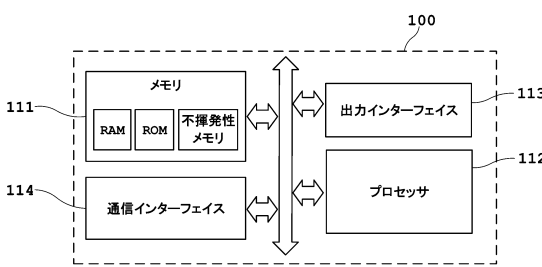
50

【図面】

【図 1】

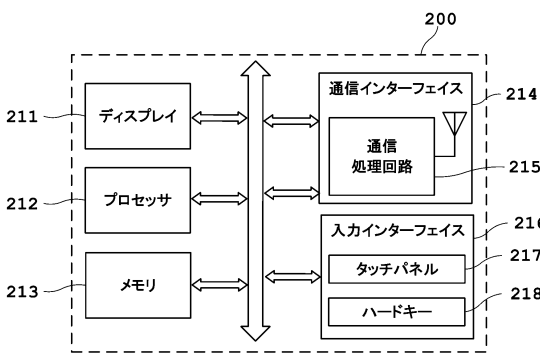


【図 2】



10

【図 3】



【図 4 A】

ユーザID	ユーザ名	ランク	修正後の ソースコード	評価
U1	N1	R1	C1	E1
U2	N2	R2	C2	E2
U3	N3	R3	C3	E3
U4	N4	R4	C4	E4
U4	N5	R5	C5	E5
...	...	...	...	...

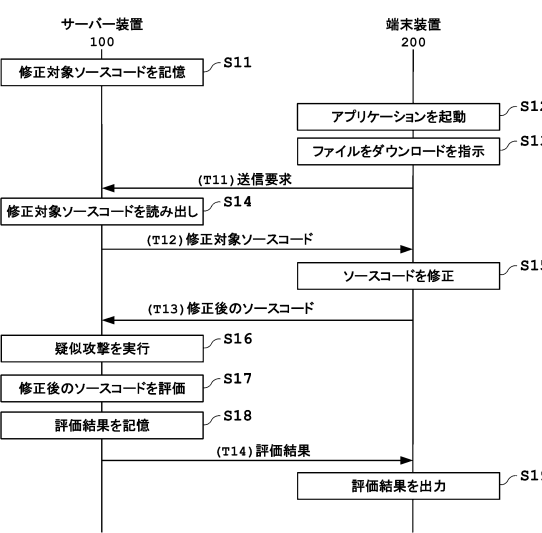
20

【図 4 B】

ランク＝初級

ソースコード ID	修正対象 ソースコード	攻撃コード
D1	S1	A1
D2	S2	A2
D3	S3	A3
D4	S4	A4
D5	S5	A5
...	...	...

【図 5】

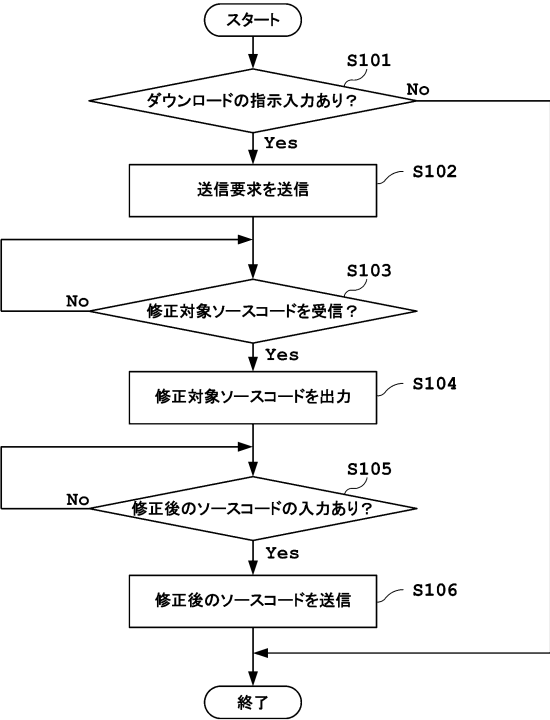


30

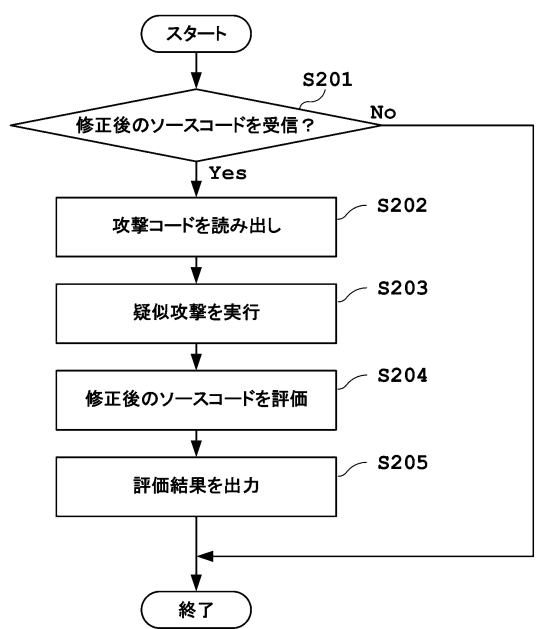
40

50

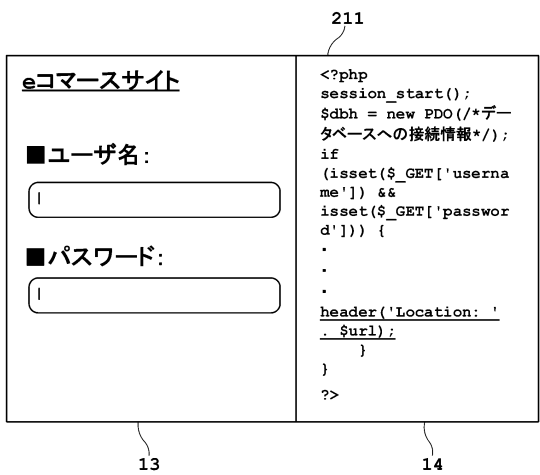
【図 6】



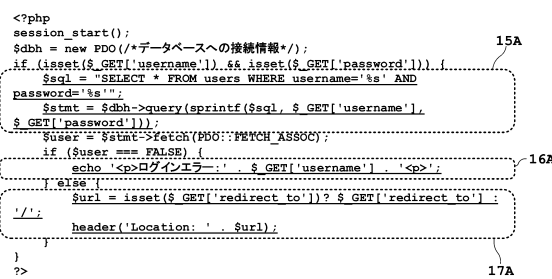
【図 7】



【図 8 A】



【図 8 B】



10

20

30

40

50

【図 9】

```
<?php
session_start();
$dbh = new PDO(/*データベースへの接続情報*/);
if (isset($_GET['username']) && isset($_GET['password'])) {
    $sql = "SELECT * FROM users WHERE username=:username AND
    password=:password";
    $stmt = $dbh->prepare($sql);
    $stmt->bindValue(":username", $_GET["username"],
    PDO::PARAM_STR);
    $stmt->bindValue(":password", $_GET["password"],
    PDO::PARAM_STR);
    $stmt->execute();
    $user = $stmt->fetch(PDO::FETCH_ASSOC);
    if ($user == FALSE) {
        echo "<p>ログインエラー:</p>";
        htmlspecialchars($_GET['username'], ENT_QUOTES, 'UTF-8') . '<p>';
    } else {
        $url = in_array($_GET['redirect_to'], ['/','/home','/
        cart'], true)? $_GET['redirect_to'] : '/';
        header('Location: ' . $url);
    }
}
?>
```

15B

16B

17B

10

20

30

40

50

フロントページの続き

株式会社Flat Security ▲4▼配信した内容：公開者が、上記配信場所に記載のウェブサイトを通じて米内貴志が発明したトレーニングシステムを用いたサービスの提供を開始した。（3）公開3 ▲1▼配信日：2020年9月17日 ▲2▼配信場所：<https://prtimes.jp/main/html/rd/p/000000017.000027502.html> ▲3▼公開者：株式会社Flat Security ▲4▼配信した内容：公開者が、上記配信場所に記載のウェブサイトを通じて米内貴志が発明したトレーニングシステムを公開した。

(56)参考文献

特開2003-108521 (JP, A)

米国特許出願公開第2018/0121657 (US, A1)

何 賽 sai HE, Javaプログラミング学習支援システムのテストコード学習のためのコード修正問題の提案 A Proposal of Code Correction Problem for Test Code Study in Java Programming Learning Assistant System, 電子情報通信学会技術研究報告 Vol. 117 No. 380 IEICE Technical Report, 日本, 一般社団法人電子情報通信学会 The Institute of Electronics, Information and Communication Engineers, 2018年01月11日, 第117巻, pages 161-166

(58)調査した分野 (Int.Cl., DB名)

G06F 21/57