(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-4236
(P2017-4236A)
(43)公開日　平成29年1月5日(2017.1.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/55	(2013.01)	G06F	21/55		5B089
G06F 13/00	(2006.01)	G06F	13/00	351N	

審査請求 未請求　請求項の数 6　ＯＬ　（全 18 頁）

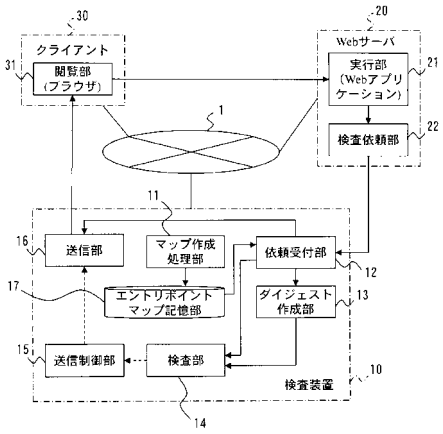
(21)出願番号　特願2015-117141 (P2015-117141)
(22)出願日　平成27年6月10日 (2015.6.10)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110001210
特許業務法人ＹＫＩ国際特許事務所
(72)発明者　長田　元気
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内

Ｆターム(参考)　5B089 GA11 GA21 GB02 HA10 HB05 JA22 JB02 KA17 KB13

(54)【発明の名称】情報処理装置、ネットワークシステム及びプログラム

(57)【要約】
【課題】既知でないクロスサイトスクリプティング攻撃をも防御する。
【解決手段】検査装置１０は、リクエストに応じて想定されるレスポンス（想定レスポンス）からタブの並びを抽出した想定ダイジェストを予め作成してエントリポイントに対応付けして記憶するエントリポイントマップ記憶部１７と、クライアント３０からの実際のリクエスト及び当該リクエストに応じてＷｅｂサーバ２０が作成した実レスポンスの組を受け付ける依頼受付部１２と、実レスポンスからタグの並びを抽出して実ダイジェストを作成するダイジェスト作成部１３と、実ダイジェストの記述内容が、対応する想定ダイジェストの様式に合致することで実レスポンスが正常と判断する検査部１４と、実レスポンスが正常の場合にはＷｅｂサーバ２０はＸＳＳ攻撃の被害を受けていないとして、送信部１６に実レスポンスをクライアント３０へ送信させる送信制御部１５と、を有する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ウェブページ毎に、当該ウェブページの閲覧要求に応じてウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応答パターンを記憶する記憶手段と、
クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答であってマークアップ言語により記述された応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段と、
前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記想定応答パターンには、前記ウェブサーバにより作成される応答に繰り返し含まれる可能性のある要素が所定の記述規則に従い記号化され記述されていることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記作成手段は、前記ウェブサーバにより作成される応答に記述内容が固定された記述部分が所定の記述規則に従い暗号化されて前記想定応答パターンに記述される場合において、前記クライアントからの閲覧要求に応じて前記ウェブサーバにより作成された応答に記述内容が固定された記述部分が含まれている場合、当該固定された記述部分を前記記述規則に従い暗号化して前記応答パターンを作成することを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記送信制御手段は、前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応する想定応答パターンの様式に該当しない場合、前記ウェブサーバにより作成された応答に代えて、前記ウェブサーバが攻撃された可能性がある旨を示す通知情報を前記クライアントへ送信させるよう制御することを特徴とする請求項１に記載の情報処理装置。
【請求項５】
ウェブページの閲覧要求を送信するクライアントと、
前記クライアントから送られてきたウェブページの閲覧要求に応じてマークアップ言語により記述された応答を作成するウェブサーバと、
情報処理装置と、
ウェブページ毎に、当該ウェブページの閲覧要求に応じて前記ウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応答パターンを記憶する記憶手段と、
を有し、
前記ウェブサーバは、前記クライアントから送られてきたウェブページの閲覧要求及び当該閲覧要求に応じて作成した応答を前記情報処理装置へ送信することで、前記ウェブサーバの検査を依頼する検査依頼手段を有し、
前記情報処理装置は、
前記ウェブサーバからの検査の依頼時に送信された閲覧要求及び応答を受け付ける依頼受付手段と、
前記依頼受付手段により受け付けられた応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段と、

前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段と、

を有することを特徴とするネットワークシステム。

【請求項６】

ウェブページ毎に、当該ウェブページの閲覧要求に応じてウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応答パターンを記憶する記憶手段をアクセス可能なコンピュータを、

クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答であってマークアップ言語により記述された応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段、

前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段、

として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置、ネットワークシステム及びプログラムに関する。

【背景技術】

【０００２】

インターネットを通じた攻撃手法の一つとして、クロスサイトスクリプティング攻撃（以下、「ＸＳＳ攻撃」と称する）がある。ＸＳＳ攻撃は、悪意のある第三者が保安上の弱点（脆弱性）のあるＷｅｂサイトを踏み台に、悪意のあるプログラムをそのＷｅｂサイトの訪問者（クライアント端末）に送り込むことで、情報の漏洩やクライアント端末の誤動作を生じさせる攻撃である。

【０００３】

ＸＳＳ攻撃からＷｅｂサイトを守る手法として、従来では、ＸＳＳ攻撃の実績（疑わしい文字列）をパターン化し、そのパターンを参照し攻撃の可能性のある外部アクセスを無効にする技術が提案されている（例えば、特許文献１，２）。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００６－０９９４６０号公報

【特許文献２】特開２０１３－２４２９２４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

本発明は、既知でないクロスサイトスクリプティング攻撃をも防御することを目的とする。

【課題を解決するための手段】

【０００６】

本発明に係る情報処理装置は、ウェブページ毎に、当該ウェブページの閲覧要求に応じてウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応

答パターンを記憶する記憶手段と、クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答であってマークアップ言語により記述された応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段と、前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段と、を有することを特徴とする。

【０００７】

また、前記想定応答パターンには、前記ウェブサーバにより作成される応答に繰り返し含まれる可能性のある要素が所定の記述規則に従い記号化され記述されていることを特徴とする。

【０００８】

また、前記作成手段は、前記ウェブサーバにより作成される応答に記述内容が固定された記述部分が所定の記述規則に従い暗号化されて前記想定応答パターンに記述される場合において、前記クライアントからの閲覧要求に応じて前記ウェブサーバにより作成された応答に記述内容が固定された記述部分が含まれている場合、当該固定された記述部分を前記記述規則に従い暗号化して前記応答パターンを作成することを特徴とする。

【０００９】

また、前記送信制御手段は、前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応する想定応答パターンの様式に該当しない場合、前記ウェブサーバにより作成された応答に代えて、前記ウェブサーバが攻撃された可能性がある旨を示す通知情報を前記クライアントへ送信させるよう制御することを特徴とする。

【００１０】

本発明に係るネットワークシステムは、ウェブページの閲覧要求を送信するクライアントと、前記クライアントから送られてきたウェブページの閲覧要求に応じてマークアップ言語により記述された応答を作成するウェブサーバと、情報処理装置と、ウェブページ毎に、当該ウェブページの閲覧要求に応じて前記ウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応答パターンを記憶する記憶手段と、を有し、前記ウェブサーバは、前記クライアントから送られてきたウェブページの閲覧要求及び当該閲覧要求に応じて作成した応答を前記情報処理装置へ送信することで、前記ウェブサーバの検査を依頼する検査依頼手段を有し、前記情報処理装置は、前記ウェブサーバからの検査の依頼時に送信された閲覧要求及び応答を受け付ける依頼受付手段と、前記依頼受付手段により受け付けられた応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段と、前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段と、を有することを特徴とする。

【００１１】

本発明に係るプログラムは、ウェブページ毎に、当該ウェブページの閲覧要求に応じてウェブサーバにより作成される応答であってマークアップ言語により記述される応答の想定される記述内容を解析することによって作成された当該応答の文書構造を示す想定応答パターンを記憶する記憶手段をアクセス可能なコンピュータを、クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答であってマークアップ言語により記述された応答の記述内容を解析することによって当該応答の文書構造を示す応答パターンを作成する作成手段、前記作成手段により作成された応答パターンが、前記クライアントにより閲覧要求されたウェブページに対応して前記記憶手段に

記憶された想定応答パターンの様式に合致する場合、前記クライアントから送られてきたウェブページの閲覧要求に応じて前記ウェブサーバにより作成された応答を前記クライアントへ送信させるよう制御する送信制御手段、として機能させる。

【発明の効果】

【００１２】

請求項１に記載の発明によれば、既知でないクロスサイトスクリプティング攻撃をも防御することができる。

【００１３】

請求項２に記載の発明によれば、応答パターンに要素が繰り返し記述される場合に対応することができる。

【００１４】

請求項３に記載の発明によれば、応答パターンに記述内容が固定された記述部分が含まれる場合に便宜を図ることができる。

【００１５】

請求項４に記載の発明によれば、ウェブサーバが攻撃された可能性がある旨をクライアントに通知することができる。

【００１６】

請求項５に記載の発明によれば、既知でないクロスサイトスクリプティング攻撃をも防御することができる。

【００１７】

請求項６に記載の発明によれば、既知でないクロスサイトスクリプティング攻撃をも防御することができる。

【図面の簡単な説明】

【００１８】

【図１】本発明に係る情報処理装置の一実施の形態である検査装置を示したブロック構成図である。

【図２】本実施の形態における検査装置を形成するコンピュータのハードウェア構成図である。

【図３】本実施の形態におけるエントリポイントマップ記憶部に記憶されたエントリポイントマップのデータ構成の一例を示した図である。

【図４】本実施の形態におけるエントリポイントマップ作成処理を示したフローチャートである。

【図５】本実施の形態におけるダイジェストの作成処理を示したフローチャートである。

【図６】（ａ）は、想定レスポンスの記述内容の一例を示した図、（ｂ）は（ａ）の想定レスポンスから作成される想定ダイジェストの例を示した図である。

【図７】本実施の形態におけるＤＯＭ構造パターンの作成処理を示したフローチャートである。

【図８】本実施の形態における検査装置が行う検査処理を示したフローチャートである。

【図９】（ａ）は、実レスポンスの記述内容の一例を示した図、（ｂ）は（ａ）の実レスポンスから作成される想定ダイジェストの例を示した図である。

【図１０】（ａ）は、繰り返しパターンを含む想定レスポンスの記述内容の一例を示した図、（ｂ）は（ａ）の想定レスポンスから作成される想定ダイジェスト、（ｃ）は（ｂ）を記号化して表した想定ダイジェスト、（ｄ）は（ｃ）に含まれる繰り返し部分を圧縮して記述したときの想定ダイジェストの一例、（ｅ）は（ｃ）に含まれる繰り返し部分を圧縮して記述したときの想定ダイジェストの他の例、（ｆ）は（ｄ）を復号して得られる想定ダイジェストの一例、（ｇ）は（ｅ）を復号して得られる想定ダイジェストの他の例、をそれぞれ示した図である。

【図１１】（ａ）は、繰り返しパターンを含む想定レスポンスの記述内容の他の例を示した図、（ｂ）は（ａ）の想定レスポンスから作成される想定ダイジェスト、（ｃ）は（ｂ）を記号化して表した想定ダイジェスト、（ｄ）は（ｃ）を復号して得られる想定ダイジ

ェストの例を示した図である。
【図１２】（ａ）は、記述の固定部分と変動部分とを含む想定レスポンスの記述内容の例を示した図、（ｂ）は（ａ）の想定レスポンスから作成される想定ダイジェストを示した図である。
【図１３】（ａ）は、記述の固定部分と変動部分とを含む実レスポンスの記述内容の例を示した図、（ｂ）は（ａ）の実レスポンスから作成される実ダイジェストを示した図である。
【発明を実施するための形態】
【００１９】
以下、図面に基づいて、本発明の好適な実施の形態について説明する。
【００２０】
図１は、本発明に係る情報処理装置の一実施の形態である検査装置１０を含むネットワークシステムの全体構成及びブロック構成を示した図である。図１には、検査装置１０、Ｗｅｂサーバ２０及びクライアント３０をインターネット等の公衆網（以下、「ネットワーク」）１に接続した構成が示されている。なお、ネットワーク１には、複数のＷｅｂサーバ２０及びクライアント３０を接続してもよいが、それぞれは同じ構成でよいため、図１にはそれぞれ１台のみを図示した。Ｗｅｂサーバ２０は、汎用的なサーバコンピュータにより実現され、１又は複数のＷｅｂアプリケーションが実行可能に搭載されている。クライアント３０は、パーソナルコンピュータ（ＰＣ）等汎用的なコンピュータにより実現される端末であり、Ｗｅｂサーバ２０のＷｅｂアプリケーションが提供するＷｅｂページを閲覧するためのブラウザが搭載されている。検査装置１０は、汎用的なコンピュータにより実現される。本実施の形態におけるネットワークシステムは、従前からあるハードウェア構成により実現してよい。
【００２１】
図２は、本実施の形態における検査装置１０を形成するコンピュータのハードウェア構成図である。本実施の形態において検査装置１０を形成するコンピュータは、ＣＰＵ４１、ＲＯＭ４２、ＲＡＭ４３、ハードディスクドライブ（ＨＤＤ）４４、入力手段として設けられたマウス４５とキーボード４６、及び表示装置として設けられたディスプレイ４７をそれぞれ接続する入出力コントローラ４８、通信手段として設けられたネットワークコントローラ４９を内部バス５０に接続して構成される。なお、Ｗｅｂサーバ２０及びクライアント３０もコンピュータであることから、各ハードウェア構成は、図２と同様に図示できる。
【００２２】
図１に戻り、クライアント３０は、ブラウザにより実現され、Ｗｅｂサーバ２０が提供するＷｅｂページを閲覧する閲覧部３１を有している。Ｗｅｂサーバ２０は、クライアント３０からのリクエストに応じてＷｅｂアプリケーションを実行する実行部２１と、当該リクエストに応じてＷｅｂアプリケーションによりレスポンスが作成されると、そのリクエスト及びレスポンスの組を検査装置１０へ送信することで、Ｗｅｂサーバ２０がＸＳＳ攻撃を受けているかいないかの検査を依頼する検査依頼部２２と、を有する。各構成要素３１，２１，２２は、各コンピュータと当該コンピュータに搭載されたＣＰＵで動作するプログラムとの協調動作により実現される。
【００２３】
本実施の形態における検査装置１０は、マップ作成処理部１１、依頼受付部１２、ダイジェスト作成部１３、検査部１４、送信制御部１５、送信部１６及びエントリポイントマップ記憶部１７を有している。なお、本実施の形態の説明に用いない構成要素については、図から省略している。Ｗｅｂサーバ２０及びクライアント３０においても同様に適宜省略している。
【００２４】
検査装置１０は、クライアント３０から送信されてきたＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）リクエスト（以下、単に「リクエスト」という

）に応じてＷｅｂサーバ２０が作成するＨＴＴＰレスポンス（以下、単に「レスポンス」という）の正当性を検証することでＷｅｂサーバ２０がＸＳＳ攻撃により被害を受けているかいないかの検査を行う。マップ作成処理部１１は、その検査に用いるエントリポイントマップを事前に作成し、エントリポイントマップ記憶部１７に登録する。エントリポイントマップに関しては後述する。依頼受付部１２は、Ｗｅｂサーバ２０から送られてくるリクエスト及びレスポンスの組を検査依頼として受け付ける。ダイジェスト作成部１３は、作成手段として設けられ、依頼受付部１２により受け付けられたレスポンス、すなわちクライアント３０から実際に送られてきたＷｅｂページの閲覧要求（リクエスト）に応じてＷｅｂサーバ２０により作成されたレスポンスの記述内容を解析することによって当該レスポンスの記述内容のＤＯＭ（Ｄｏｃｕｍｅｎｔ　Ｏｂｊｅｃｔ　Ｍｏｄｅｌ）構造パターンを作成する。本実施の形態においては、レスポンスのＤＯＭ構造パターン（レスポンスの文書構造を示す応答パターン）を「ダイジェスト」と称している。レスポンスは、ＨＴＭＬ（Ｈｙｐｅｒｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）などのマークアップ言語により記述される。

【００２５】

検査部１４は、依頼受付部１２により受け付けられたレスポンスのダイジェストと、エントリポイントマップ記憶部１７に登録されているエントリポイントマップを用いて、当該レスポンスの正当性を検証する。具体的には、検査部１４は、ダイジェストが、当該エントリポイントに対応してエントリポイントマップ記憶部１７に記憶された想定ダイジェストの様式に合致する場合、レスポンスが正常である、すなわちＷｅｂサーバ２０は、ＸＳＳ攻撃を受けていないと判断する。

【００２６】

ところで、Ｗｅｂサーバ２０は、クライアント３０からのリクエストに応じてＷｅｂページをクライアント３０に表示させるためにレスポンスを返すが、そのレスポンスの記述内容はＷｅｂアプリケーションの記述内容から想定可能である。このＷｅｂアプリケーションの記述内容から想定して作成されるレスポンスを「想定レスポンス」と称することにする。また、想定レスポンスのＤＯＭ構造パターン（想定応答パターン）もダイジェストであるが、ダイジェスト作成部１３が作成するダイジェストと区別するために、本実施の形態では、想定レスポンスのＤＯＭ構造パターンを「想定ダイジェスト」と称することにする。また、クライアント３０からのリクエストに応じて実際に作成されるレスポンスを「実レスポンス」とも称することにする。そして、ダイジェスト作成部１３が実レスポンスに基づき作成するダイジェストを「実ダイジェスト」とも称することにする。詳細は後述するが、エントリポイントマップには、想定ダイジェストが設定される。

【００２７】

送信制御部１５は、送信制御手段として設けられ、検査部１４によりレスポンスが正常であると判断された場合、当該レスポンスをクライアント３０へ送信させるよう制御する。一方、レスポンスが正常でないと判断された場合、Ｗｅｂサーバ２０により作成されたレスポンスに代えて、Ｗｅｂサーバ２０がＸＳＳ攻撃された可能性がある旨を示す通知情報をクライアント３０へ送信させるよう制御する。送信部１６は、送信制御部１５による制御に従いレスポンス又は通知情報をクライアント３０へ送信する。

【００２８】

検査装置１０における各構成要素１１～１６は、検査装置１０を形成するコンピュータと、コンピュータに搭載されたＣＰＵ４１で動作するプログラムとの協調動作により実現される。また、エントリポイントマップ記憶部１７は、検査装置１０に搭載されたＨＤＤ４４にて実現される。あるいは、ＲＡＭ４３又は外部にある記憶手段をネットワーク経由で利用してもよい。

【００２９】

また、本実施の形態で用いるプログラムは、通信手段により提供することはもちろん、ＣＤ－ＲＯＭやＵＳＢメモリ等のコンピュータ読み取り可能な記録媒体に格納して提供することも可能である。通信手段や記録媒体から提供されたプログラムはコンピュータにイ

ンストールされ、コンピュータのＣＰＵがプログラムを順次実行することで各種処理が実現される。

【００３０】

図３は、本実施の形態におけるエントリポイントマップ記憶部１７に記憶されたエントリポイントマップのデータ構成の一例を示した図である。また、図４は、本実施の形態におけるマップ作成処理部１１により実施されるエントリポイントマップ作成処理を示したフローチャートである。以下、図３及び図４を用いてエントリポイントマップ及びエントリポイントマップの作成処理について説明する。マップ作成処理部１１は、検査装置１０が検査を開始する前にエントリポイントマップを作成しておく必要がある。

【００３１】

エントリポイントマップには、Ｗｅｂアプリケーションのエントリポイントと想定ダイジェストとが組にして設定される。エントリポイントは、プログラム等の実行開始位置を示す情報であるが、本実施の形態においては、アクセス先を示すＵＲＩ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｔｉｆｉｅｒ）、クッキー（Ｃｏｏｋｉｅ）の有無等のアクセス時の状態を示す認証状態及び１又は複数のリクエストパラメータの組合せによってエントリポイントを表す。

【００３２】

マップ作成処理部１１は、Ｗｅｂサーバ２０が実行するＷｅｂアプリケーションを取得し、解析することでＷｅｂアプリケーションに含まれているエントリポイントを抽出する（ステップ１１０）。ところで、クライアント３０からリクエストが送信されてくると、Ｗｅｂサーバ２０の実行部２１は、そのリクエストの記述からＷｅｂアプリケーションの中のエントリポイントを特定し、エントリポイント以降の記述内容に基づきレスポンスを作成することになる。従って、マップ作成処理部１１は、各エントリポイントに対応するリクエストがそれぞれ送信されてくることを想定し、各エントリポイント以降の記述内容を解析することで想定されるレスポンスのＤＯＭ構造パターン、すなわち想定ダイジェストをエントリポイント毎に作成する（ステップ１２０）。そして、マップ作成処理部１１は、エントリポイントと想定ダイジェストとを組にしてエントリポイントマップ記憶部１７に登録する（ステップ１３０）。

【００３３】

続いて、ステップ１２０における想定ダイジェストの作成処理の詳細について図５に示したフローチャートを用いて説明する。

【００３４】

マップ作成処理部１１は、Ｗｅｂアプリケーションに含まれている各エントリポイントからの記述内容を想定レスポンスとして抽出して取得する（ステップ１２１）。そして、マップ作成処理部１１は、想定レスポンスをディスプレイ４７に表示する。ここで、エントリポイントマップを設定する開発者は、表示された想定レスポンスを参照してハッシュを利用するかどうかを判断する。なお、ハッシュについては後述するとし、ここでは、開発者はハッシュを利用しないことを選択したものとして説明する。

【００３５】

開発者によりハッシュ利用をしないという選択を受け付けると（ステップ１２２でＮ）、マップ作成処理部１１は、その想定レスポンスからＤＯＭ構造パターン、すなわち、想定ダイジェストを作成する（ステップ１２３）。この想定ダイジェストの作成方法について図６及び図７を用いて詳述する。

【００３６】

図６（ａ）は、あるエントリポイントにおける記述内容の一例であり、想定レスポンスに相当する。想定レスポンスは、ＨＴＭＬで記述されているため、“＜ｈｔｍｌ＞”などのタグを含んでいる。マップ作成処理部１１は、想定レスポンスに含まれている全てのタグを、想定レスポンスにおける出現順に抽出する（ステップ１４１）。この抽出したタグをカンマで区切って表した情報を図６（ｂ）に示すが、本実施の形態では、図６（ｂ）に示したタグの並びをダイジェストとして作成する。なお、図６（ａ）に例示した想定レス

ポンスには繰り返しパターンが含まれていない。繰り返しパターンが含まれている場合に関しては後述する。

【００３７】

このようにして、マップ作成処理部１１は、想定レスポンスからダイジェストを「想定ダイジェスト」として作成する。なお、ダイジェスト作成部１３は、クライアント３０からのリクエストに応じて作成されたレスポンスからダイジェストを作成するが、このダイジェスト作成部１３におけるダイジェスト作成処理も図７に示した処理手順に従って「実ダイジェスト」を作成する。

【００３８】

本実施の形態では、以上のようにしてエントリポイントマップを作成する。これにより、検査装置１０は、クライアント３０により実際に送信されたリクエストに応じてＷｅｂサーバ２０により作成されたレスポンスの正当性の検証を行えるようになる。

【００３９】

次に、クライアント３０がリクエストをＷｅｂサーバ２０へ送信してからレスポンスを取得するまでの基本的な処理の流れについて説明する。

【００４０】

Ｗｅｂサーバ２０がクライアント３０から送信されてきたリクエストを受け付けると、実行部２１は、そのリクエストの記述形式からＷｅｂアプリケーションにおけるエントリポイントを特定する。そして、その特定されたエントリポイント以降の記述内容に従ってレスポンスを作成する。レスポンスが作成されると、検査依頼部２２は、リクエスト及びレスポンスを組にして検査装置１０へ送信することでレスポンスの正当性の検証、換言するとＷｅｂサーバ２０がＸＳＳ攻撃の被害を受けているかいないかの検査を依頼する。

【００４１】

以下、本実施の形態における検査装置１０が行う検査処理について図８に示したフローチャートを用いて説明する。

【００４２】

依頼受付部１２は、Ｗｅｂサーバ２０からリクエスト及びレスポンスの組を受信することで検査の依頼を受け付けると（ステップ１５１）、エントリポイントマップの中から、受け付けたリクエストに対応するエントリポイントを特定する（ステップ１５２）。そして、依頼受付部１２は、特定したエントリポイントに対応した想定ダイジェストをエントリポイントマップから読み出し取得する（ステップ１５３）。

【００４３】

ダイジェスト作成部１３は、依頼受付部１２が受け付けたリクエスト、すなわちクライアント３０が実際に発したリクエストに基づき作成されたレスポンスの実ダイジェストを作成する（ステップ１５４）。ダイジェストの作成方法については、図４～図７を用いてすでに説明しているので説明を省略する。

【００４４】

ダイジェスト作成部１３により実ダイジェストが作成されると、検査部１４は、ステップ１５３により取得された想定ダイジェストと、ステップ１５４により作成された実ダイジェストと、を比較する。ここで、実ダイジェストが想定ダイジェストの様式に合致する場合（ステップ１５５でＹ）、検査部１４は、Ｗｅｂサーバ２０において実レスポンスが正常に作成されたと判断する（ステップ１５６）。この基本的な検査処理において、実ダイジェストが想定ダイジェストの様式に合致する場合というのは、実ダイジェストと想定ダイジェストの各記述内容が一致している場合のことをいう。正常と判断された場合、つまり、実レスポンスの正当性が検証されると、送信制御部１５は、実レスポンスをクライアント３０へ送信するよう送信部１６に指示する。送信部１６は、この指示に応じて、依頼受付部１２により受け付けられたレスポンスを、リクエストを送信したクライアント３０へ送信する。

【００４５】

一方、実ダイジェストが想定ダイジェストの様式に合致しない場合（ステップ１５５で

Ｎ）、検査部１４は、Ｗｅｂサーバ２０において作成されたレスポンスは異常と判断する（ステップ１５７）。異常と判断された場合、送信制御部１５は、Ｗｅｂサーバ２０がＸＳＳ攻撃された可能性がある旨を示す通知情報をクライアント３０へ送信するよう送信部１６に指示する。送信部１６は、この指示に応じてその通知情報を、リクエストを送信したクライアント３０へ送信する。

【００４６】

クライアント３０は、リスエストをＷｅｂサーバ２０へ送信した後、レスポンスが検査装置１０を介して返信されてくると、ブラウザがそのレスポンスの記述内容を解釈してＷｅｂページをディスプレイに表示する。一方、リスエストに応じて通知情報が返信されてくると、ブラウザは、その通知情報をディスプレイに表示することによって、Ｗｅｂサーバ２０がＸＳＳ攻撃された可能性がある旨をユーザに知らせる。

【００４７】

以下、前述した検査処理について、ダイジェストの具体例を用いて詳述する。

【００４８】

例えば、ステップ１５１において受け付けたリクエストから得られる想定レスポンスが図６（ａ）だとする。マップ作成処理部１１は、この想定レスポンスに基づき図６（ｂ）に示した想定ダイジェストを作成する。ここで、ステップ１５１において受け付けた実レスポンスの記述内容が、図６（ａ）に示した想定ダイジェストと同一であったとする。この場合、ダイジェスト作成部１３は、当該実レスポンスのダイジェストを図６（ｂ）のように作成する。この結果、実ダイジェストの記述内容は、想定ダイジェストと一致するので（ステップ１５５でＹ）、当該実レスポンスは正常と判断される（ステップ１５６）。

【００４９】

このように、レスポンスがＷｅｂサーバ２０によって正常に作成されているのであれば、当該レスポンスの記述内容は、対応する想定レスポンスと一致するはずである。これにより、実レスポンスの正当性は証明される。

【００５０】

ここで、クライアント３０からの実際のリクエストに応じて作成されたレスポンスが図９（ａ）であるとする。図６（ａ）と図９（ａ）を比較すると明らかなように、作成されたレスポンスには、想定レスポンスの“ｈｅｎｓｕ”に代えて＜ｓｃｒｉｐｔ＞タグによる記述５１が挿入されていることがわかる。従って、ダイジェスト作成部１３は、図９（ａ）に示した実レスポンスから図９（ｂ）に示した実ダイジェストを作成することになる（ステップ１５４）。ここで、図６（ｂ）及び図９（ｂ）の各ダイジェストを比較すれば明らかなように、ダイジェスト作成部１３が作成した実ダイジェストには、想定ダイジェストに含まれていない“ｓｃｒｉｐｔ”及び“／ｓｃｒｉｐｔ”が含まれており、このため、両者は合致しない。このような場合、検査部１４は、実ダイジェストが想定ダイジェストの様式に合致しないと判断して（ステップ１５５でＮ）、Ｗｅｂサーバ２０において作成された実レスポンスは異常と判断する（ステップ１５７）。

【００５１】

本実施の形態においては、以上説明したように、各エントリポイントからの記述内容に基づきエントリポイント毎、すなわちＷｅｂページ毎に想定ダイジェストを予め用意しておき、実際に送信されたリクエストのレスポンスから作成されたダイジェストを、対応する想定ダイジェストと比較することによってＷｅｂサーバ２０がＸＳＳ攻撃の被害を受けている可能性があるかどうかを判断するようにした。つまり、ＸＳＳ攻撃を実際に受けたときの実績（疑わしい文字列等）を参照しなくてもＸＳＳ攻撃の有無を判定できるようにした。従って、本実施の形態においては、反射型ＸＳＳに限らず、格納型ＸＳＳ及びＤＯＭベースのＸＳＳにも対処可能である。

【００５２】

ところで、上記説明においては、繰り返しのない簡単な記述内容のレスポンスを例にして本実施の形態における基本的な検査処理について説明した。以下、繰り返しのある記述内容のレスポンスに対応する場合の検査処理について説明する。具体的には、上記におい

て説明していない図７のステップ１４３～１４５の処理について説明する。
【００５３】
掲示板、検索結果あるいは表（テーブル）の表示に関するリクエストの場合、該当する各データは、通常は同じ表示形式にて繰り返し表示される。そして、リクエストを発するタイミングや検索条件によって、該当するデータ数（表示件数）は変動する。
【００５４】
図１０（ａ）は、繰り返しのある想定レスポンスの一例を示した図である。この想定レスポンスから想定ダイジェストを作成するマップ作成処理部１１における処理について説明する。
【００５５】
マップ作成処理部１１は、Ｗｅｂアプリケーションから抽出したエントリポイントからの記述内容を解析することで想定レスポンスを取得すると（図４のステップ１１０，１２０、図５のステップ１２１～１２３）、その想定レスポンスからタグを抽出する（ステップ１４１）。想定ダイジェストが図１０（ａ）の場合、マップ作成処理部１１は、図１０（ｂ）に示した想定ダイジェストが得られる。
【００５６】
ここで、想定レスポンスの記述５２は、表において同じ形式にて表示されるデータ（レコード）の繰り返し部分であることから、この想定レスポンスから抽出したタグの並びを解析するとタグの並びが同じパターンが繰り返し現れてくる。このように、想定ダイジェストに繰り返しパターンが含まれていると（ステップ１４２でＹ）、マップ作成処理部１１は、図１０（ｂ）に示したようにタグの並びが同じ繰り返しパターンを１つにまとめ、それぞれに記号を割り振る。図１０（ｂ）に示した記号の例によると、“ｔｒ，ｔｄ，／ｔｄ，ｔｄ，ａ，／ａ，／ｔｄ，／ｔｒ”というパターンが繰り返し現れているので、このパターンに“Ｃ”という記号を割り振る。なお、“ｈｔｍｌ”や“ｔａｂｌｅ”など繰り返しパターンに含まれないタグに対しては、記号を個々に割り振る。このようにして、マップ作成処理部１１は、想定レスポンスから得られた想定ダイジェストに含まれるタグを記号化する（ステップ１４３）。記号化後の想定ダイジェストを図１０（ｃ）に示す。
【００５７】
続いて、マップ作成処理部１１は、記号化された想定ダイジェストを解析することで記号を必要により圧縮する（ステップ１４４）。図１０（ｃ）に示した記号化された想定ダイジェストによると、“Ｃ”が３回繰り返し連続して登場している。そこで、本実施の形態では、１つのパターンとして図１０（ｄ）に示したように３つの“Ｃ”を“Ｃ３”と圧縮する。その後、マップ作成処理部１１は、記号を復号してタグに展開する（ステップ１４５）。
【００５８】
以上説明したように、想定レスポンスから得られる想定ダイジェスト（図１０（ｂ））にタグの繰り返しパターンが存在する場合、マップ作成処理部１１は、その想定ダイジェストを編集し、上記のように繰り返しパターンを圧縮し、図１０（ｆ）に例示したように繰り返し部分要素を記号化して想定ダイジェストを作成する。図１０（ｆ）を参照すれば明らかなように、本実施の形態では、繰り返し部分を小括弧“（）”で囲み、その繰り返し回数を“）”に続けて記述するという所定の記述規則に従って記述している。
【００５９】
また、ステップ１４４において、記号化された想定ダイジェストを圧縮する他のパターンとして、図１０（ｅ）に示したように３つの“Ｃ”を 、“Ｃ”が３回と限定せずに複数回登場していることを示す“Ｃ＋”と圧縮してもよい。これを復号した結果、作成される想定ダイジェストを図１０（ｇ）に示す。図１０（ｇ）を参照すれば明らかなように、繰り返し部分を、図１０（ｆ）のように繰り返し回数を“３”と数値にて固定化せずに、“）”に続けて１回以上繰り返されていることを表す“＋”で表すという所定の記述規則に従って記述している。
【００６０】

図１０（ａ）に例示した想定レスポンスでは、３回の繰り返しが存在している。ただ、検索条件等によってヒットするデータ数が異なってくることは容易に想像しうる。そこで、“Ｃ３”と繰り返し回数を３回と明示せずに、１回以上出現することを示す“＋”という記号を付加することで、繰り返しパターンの回数は変動してもよい、可変であるという形式にて想定ダイジェストを作成する。

【００６１】

一方、“Ｃ３”のように“Ｃｎ”（ｎは自然数）と繰り返し回数を明示することにも長所がある。例えば、血液型や都道府県等繰り返しの数が固定的なデータを表示するのであれば、“Ｃｎ”と繰り返し回数を固定して想定ダイジェストを作成するのが好適である。例えば、血液型は、Ａ，Ｂ，Ｏ，ＡＢと４タイプと固定されているので“Ｃ４”とする。この場合において、血液型に対するデータを表示するための実ダイジェストにおける繰り返し回数が５回などと４回以外になっていれば、Ｗｅｂサーバ２０はＸＳＳ攻撃の被害を受けていると推定できる。

【００６２】

なお、上記説明では、タグ及び繰り返しパターンに英字を割り振り、繰り返しパターンに対しては“＋”という記号を付加して表すようにしたが、これらの記号は一例であって所定の記述規則に従い異なる記号を用いるようにしてもよい。また、本実施の形態では、繰り返し回数が固定である場合と変動である場合との例を示したが、繰り返し回数として上下限値や範囲を指定できるようにしてもよい。この場合、エントリポイントマップを作成する際に、図１０（ｆ）あるいは図１０（ｇ）のようにマップ作成処理部１１が自動作成した想定ダイジェストをディスプレイ４７に表示して、開発者に編集させるようにしてもよい。

【００６３】

次に、クライアント３０から実際に送信されたリクエストに応じて作成されたレスポンスに繰り返しパターンが存在する場合における検査装置１０における検査処理について図８を用いて説明する。なお、すでに説明した処理については適宜省略する。

【００６４】

依頼受付部１２は、受け付けたリクエスト及びレスポンスの組に基づき想定ダイジェストを取得する（ステップ１５１～１５３）。そして、ダイジェスト作成部１３は、依頼受付部１２が受け付けたレスポンスの実ダイジェストを作成する（ステップ１５４）。

【００６５】

続いて、検査部１４は、ステップ１５３により取得された想定ダイジェストと、ステップ１５４により作成された実ダイジェストと、を比較するが、想定ダイジェスト（例えば図１０（ｇ））を参照することで繰り返しパターンが含まれていることを認識できる。この場合、検査部１４は、想定ダイジェストの繰り返し部分に対応するタグの並びを実ダイジェストの中から見つけ、前述した“）”に続く“３”や“＋”の記号に基づいて実ダイジェストにおける繰り返し部分の記述の正当性を検証する。

【００６６】

例えば、実ダイジェストにおいて、図１０（ｂ）における記号“Ｃ”に対応するタグの並びが５回繰り返されている場合において、想定ダイジェストが図１０（ｆ）のように作成されている場合、タグの並びは一致しているものの繰り返し回数が３回でないため、実ダイジェストは異常と判断される。一方、想定ダイジェストが図１０（ｇ）のように作成されている場合、繰り返しパターンと指定された部分のタグの並びが一致しているため、実ダイジェストは正常と判断される。

【００６７】

図６（ａ）に例示したように繰り返しのない簡単な想定レスポンスの場合は、実ダイジェストが想定ダイジェストと完全に一致する必要があるが、ここで説明しているダイジェストに繰り返しパターンが含まれる場合、実ダイジェストの記述内容は想定ダイジェストと完全に一致しない。しかしながら、実ダイジェストの記述内容は、想定ダイジェストの記述規則によって意図している記述に合致している。このように、本実施の形態では、実

ダイジェストの記述内容が、所定の記述規則によって示されている想定ダイジェストが意図する内容である場合、実ダイジェストの記述内容は想定ダイジェストの様式に合致していると解釈する。

【００６８】

このように、検査部１４は、実ダイジェストの記述内容が想定ダイジェストの様式に合致している場合（ステップ１５５でＹ）、詳細には、実ダイジェストにおける繰り返し部分以外の記述内容は想定ダイジェストと一致し、実ダイジェストにおける繰り返し部分の記述内容は想定ダイジェストにおける所定の記述規則に合致している場合、検査部１４は、Ｗｅｂサーバ２０においてレスポンスが正常に作成されたと判断する（ステップ１５６）。一方、実ダイジェストの記述内容が想定ダイジェストの様式に合致していない場合（ステップ１５５でＮ）、検査部１４は、Ｗｅｂサーバ２０において作成されたレスポンスは異常と判断する（ステップ１５７）。

【００６９】

なお、本実施の形態では、ステップ１４４において圧縮した後にステップ１４５で復号した想定ダイジェストを用いて実ダイジェストと比較するようにしたが、実レスポンスに対してステップ１４３，１４４を施して、記号化、圧縮化した状態で実ダイジェストと想定ダイジェストとを比較するようにしてもよい。

【００７０】

以下、レスポンスに繰り返しパターンを含む場合の変形例について説明する。

【００７１】

図１１（ａ）は、図１０（ａ）と同様に繰り返しパターンを含む想定レスポンスを示した図である。但し、図１１（ａ）は、想定レスポンスにおける繰り返し部分の一部に他の繰り返し部分には含まれない記述が含まれている場合である。具体的には、繰り返し部分の１箇所に“ｉｍｇ”タグによる記述５３が含まれている。この記述５３を除外すると、図１１（ａ）に示した想定レスポンスには、“ｔｒ，ｔｄ，／ｔｄ，ｔｄ，ａ，／ａ，／ｔｄ，／ｔｒ”という繰り返しパターンが含まれている。基本的には、図１０を用いて説明したのと同様に処理して想定ダイジェストを作成すればよい。ただ、この例の場合、図１１（ｄ）に示したように一部に現れる可能性のあるタグ“ｉｍｇ”を“（ｉｍｇ）？”というように“（）”で囲み、“）”に続けて“？”を付けるという所定の記述規則に従って想定ダイジェストを作成する。これは、例えば、エントリポイントマップを作成する際に、図１１（ｂ）のようにマップ作成処理部１１が自動作成した想定ダイジェストをディスプレイ４７に表示して、開発者に編集させるようにして、図１１（ｄ）に示した想定ダイジェストを完成させるようにしてもよい。

【００７２】

続いて、ダイジェストを作成する他の例について説明する。具体的には、上記において説明していない図５のステップ１２４～１２７の処理について説明する。

【００７３】

前述した繰り返しパターンのように、レスポンスにおける記述内容に変動する部分とは別に固定する部分は存在しうる。図１２（ａ）は、想定レスポンスの一例を示した図であるが、図１２（ａ）に例示したように、想定レスポンスには、固定された記述５４と変動する記述５５とが混在する場合がある。前述したように想定レスポンスから全てのタグを抽出して想定ダイジェストを作成してもよいが、記述の固定部分に関しては、まとめて処理することで想定ダイジェストを作成してもよい。

【００７４】

以下、想定レスポンスを記述の固定部分と変動部分とに分けてマップ作成処理部１１がエントリポイントマップを作成処理について説明する。

【００７５】

マップ作成処理部１１は、Ｗｅｂアプリケーションから抽出したエントリポイントからの記述内容を解析することで想定レスポンスを取得する（図４のステップ１１０，１２０、図５のステップ１２１）。

【００７６】
ここで、開発者によりハッシュを利用するという選択を受け付けると（ステップ１２２でＹ）、マップ作成処理部１１は、想定レスポンスをディスプレイ４７に表示して、開発者に固定部分と変動部分とを指定させる。指定された内容を受け付けることで、想定レスポンスにおける固定部分と変動部分とをそれぞれ抽出する（ステップ１２４）。図１２（ａ）に例示した想定レスポンスによると、記述５４，５６が固定部分に、記述５５が変動部分に、それぞれ該当するものとする。続いて、マップ作成処理部１１は、固定部分の記述５４，５６それぞれを対象としてハッシュ値を算出する（ステップ１２５）。本実施の形態では、固定部分の記述に対してハッシュ対象とする直前のタグ（ダイジェスト）からのバイト数とハッシュ値とを当該固定部分におけるダイジェストして作成する。記述５４は、想定レスポンスの先頭なので、その先頭位置からのバイト数“８５”と、８５バイト分の記述５４をハッシュ対象として算出されたハッシュ値（Ｈａｓｈ値１）と、で当該固定部分のダイジェストを作成する。記述５６は、直前のタグ（ダイジェスト）“／ｄｉｖ”からのバイト数“４１”と、４１バイト分の記述５６をハッシュ対象として算出されたハッシュ値（Ｈａｓｈ値２）と、で当該固定部分のダイジェストを作成する。

【００７７】
続いて、マップ作成処理部１１は、変動部分の記述５５に対しては、ステップ１２３において説明したように全てのタグを抽出してＤＯＭ構造パターンを作成する（ステップ１２６）。この作成したＤＯＭ構造パターンが対応する変動部分のダイジェストとなる。以上のようにして、固定部分と変動部分とに対してそれぞれダイジェストを作成すると、これらをマージして想定ダイジェストを完成させる（ステップ１２７）。なお、ステップ１２５とステップ１２６は、処理順を逆にして実行してもよい。

【００７８】
図１２（ｂ）は、以上の処理により作成された想定ダイジェストを示した図である。想定ダイジェストに含まれる各記述５７，５８，５９は、それぞれ想定レスポンスの各記述５４，５５，５６に対応する。

【００７９】
次に、ハッシュ値を含む想定ダイジェストを用いた検査装置１０における検査処理について図８を用いて説明する。なお、すでに説明した処理については適宜省略する。

【００８０】
依頼受付部１２は、受け付けたリクエスト及びレスポンスの組に基づき想定ダイジェストを取得する（ステップ１５１～１５３）。そして、ダイジェスト作成部１３は、依頼受付部１２が受け付けたレスポンスのダイジェストを作成する。このとき、ダイジェスト作成部１３は、想定ダイジェスト（例えば図１２（ｂ））を参照することでハッシュ値が含まれていることを認識できるので、図５のステップ１２４～１２７を説明したのと同様に処理して、実レスポンスからハッシュを利用した実ダイジェストを作成する（ステップ１５４）。

【００８１】
続いて、検査部１４は、ステップ１５３により取得された想定ダイジェストと、ステップ１５４により作成された実ダイジェストと、を比較し、実ダイジェストが想定ダイジェストの様式に合致する場合（ステップ１５５でＹ）、検査部１４は、Ｗｅｂサーバ２０においてレスポンスが正常に作成されたと判断する（ステップ１５６）。実ダイジェストが想定ダイジェストの様式に合致する場合というのは、ハッシュを利用した記述に関しては、対応する記述と一致する場合である。ハッシュを利用していない記述に関しては、レスポンスが簡単な記述及び繰り返すパターンを含む場合において説明したように、当該記述の実ダイジェストが、対応する記述の想定ダイジェストの様式に合致する場合である。一方、実ダイジェストが想定ダイジェストの様式に合致しない場合（ステップ１５５でＮ）、検査部１４は、Ｗｅｂサーバ２０において作成されたレスポンスは異常と判断する（ステップ１５７）。

【００８２】

図１３（ａ）は、Ｗｅｂサーバ２０において作成された実レスポンスの例を示した図である。図１２（ａ）に示した想定レスポンスと比較すると明らかなように、図１３（ａ）に示した実レスポンスにおける記述５４には、想定レスポンスに含まれている記述６１が含まれている。この記述６１によって実レスポンスにおける記述５４に対して算出されるバイト数及びハッシュ値は、想定レスポンスとは異なってくる。図１３（ｂ）に例示したように記述５４に対するダイジェスト６２は、対応する想定ダイジェスト５７と異なってくる。

【００８３】

本実施の形態によれば、クライアント３０からのリクエストに応じて作成したレスポンスの実ダイジェストを、事前に用意しておいた想定ダイジェストと比較し検証することで、Ｗｅｂサーバ２０がＸＳＳ攻撃の被害を受けているかどうかを検査できるようにした。

【００８４】

なお、本実施の形態では、送信制御部１５は送信部１６に指示することで、Ｗｅｂサーバ２０が作成したレスポンスを検査装置１０からクライアント３０へ送信するようにした。これを、送信制御部１５は、レスポンスの送信指示をＷｅｂサーバ２０にすることで、Ｗｅｂサーバ２０からクライアント３０へレスポンスを返信させるようにしてもよい。通知情報についても同様である。

【００８５】

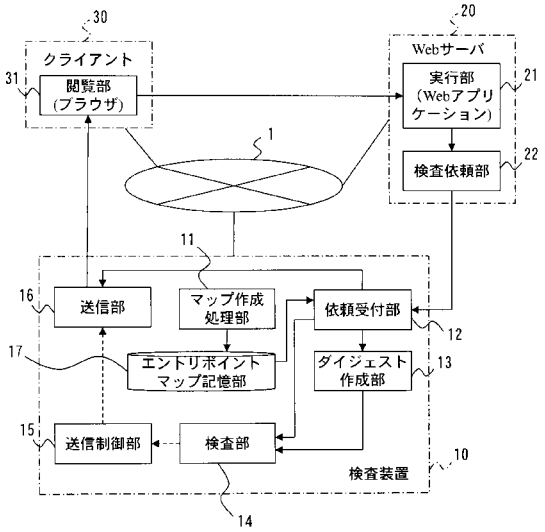
また、本実施の形態では、検査装置１０をＷｅｂサーバ２０とは別に設けたが、検査装置１０が持つ処理機能をＷｅｂサーバ２０に持たせることで一体に形成してもよい。あるいは、Ｗｅｂサーバ２０と検査装置１０とを１対１に対応付けずに、検査装置１０が複数のＷｅｂサーバ２０の検査を行うようにしてもよい。

【符号の説明】

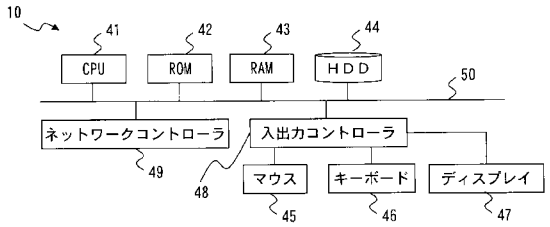
【００８６】

１　ネットワーク、１０　検査装置、１１　マップ作成処理部、１２　依頼受付部、１３　ダイジェスト作成部、１４　検査部、１５　送信制御部、１６　送信部、１７　エントリポイントマップ記憶部、２０　Ｗｅｂサーバ、２１　実行部、２２　検査依頼部、３０　クライアント、３１　閲覧部、４１　ＣＰＵ、４２　ＲＯＭ、４３　ＲＡＭ、４４　ハードディスクドライブ（ＨＤＤ）、４５　マウス、４６　キーボード、４７　ディスプレイ、４８　入出力コントローラ、４９　ネットワークコントローラ、５０　内部バス。

【図１】



【図２】

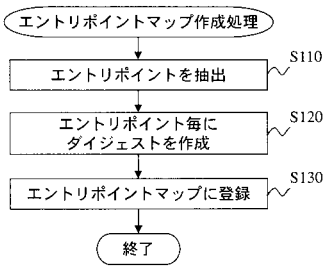


【図３】

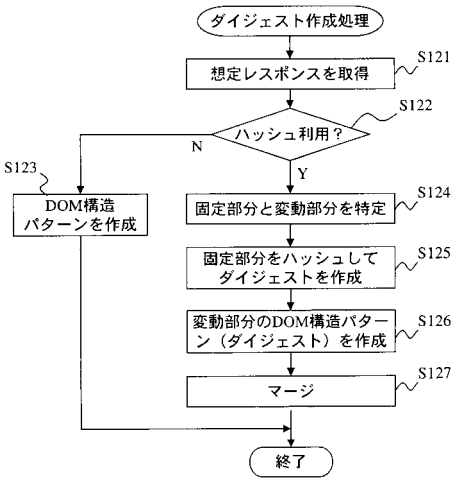
エントリポイントマップ

エントリポイント URI	認証状態 cookie	Param1 - action	Param2 - xxxxx	想定ダイジェスト
/jsw/top	N/A	N/A	..	N/A
/jsw/client/	N/A	N/A	..	html, script, /script, img, div, /div, /html
/jsw/client/sw	無	N/A	..	html, table, tr, td, td, a, /a, /td, /td, /tr, /table, /html
/jsw/client/sw	有	N/A	..	html, table, (tr, td, td, a, (img)?, /a, /td, /td, /tr)+, /table, /html
/jportal/jsapi	無	N/A	..	..
/jportal/jsapi	有	confirm	..	..
/jportal/jsapi	有	submit	..	..
..	..	..	..	..

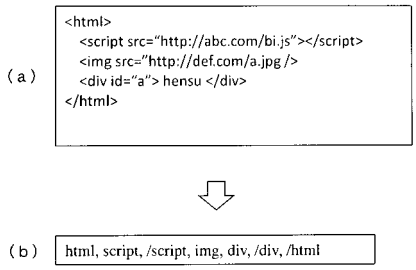
【図４】



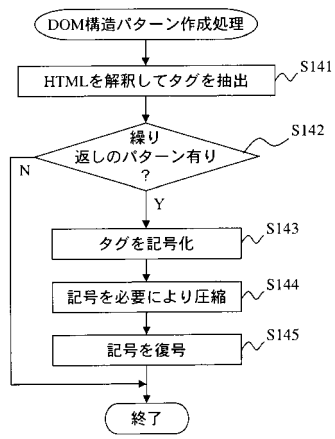
【図５】



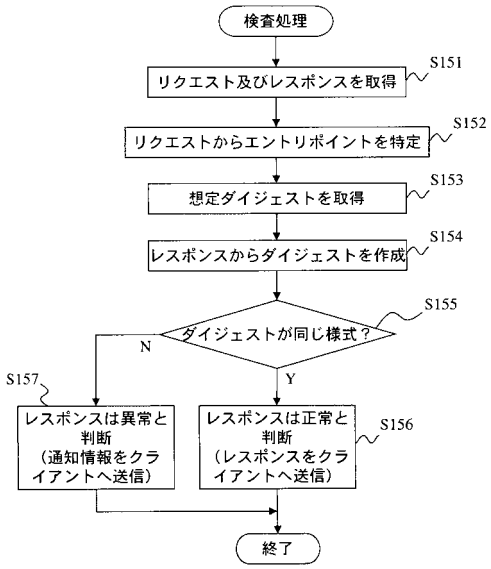
【図６】



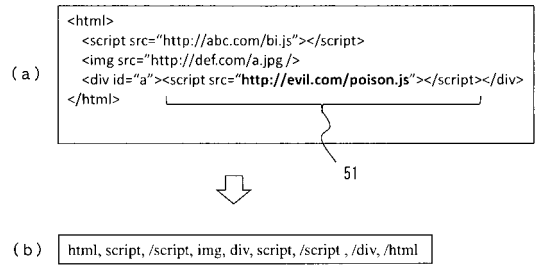
【図７】



【図８】

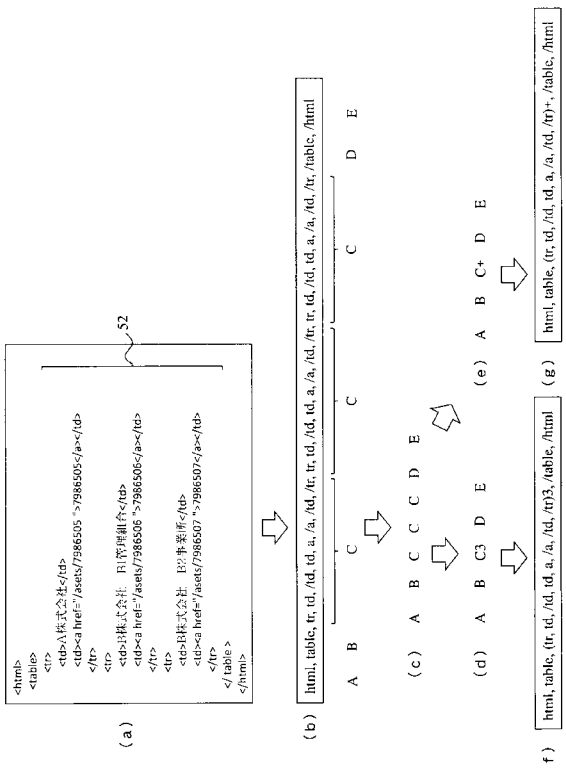

検査処理
リクエスト及びレスポンスを取得
S151
リクエストからエントリポイントを特定
S152
想定ダイジェストを取得
S153
レスポンスからダイジェストを作成
S154
ダイジェストが同じ様式？
S155
N
Y
S157
レスポンスは異常と判断（通知情報をクライアントへ送信）
レスポンスは正常と判断（レスポンスをクライアントへ送信）
S156
終了

【図９】

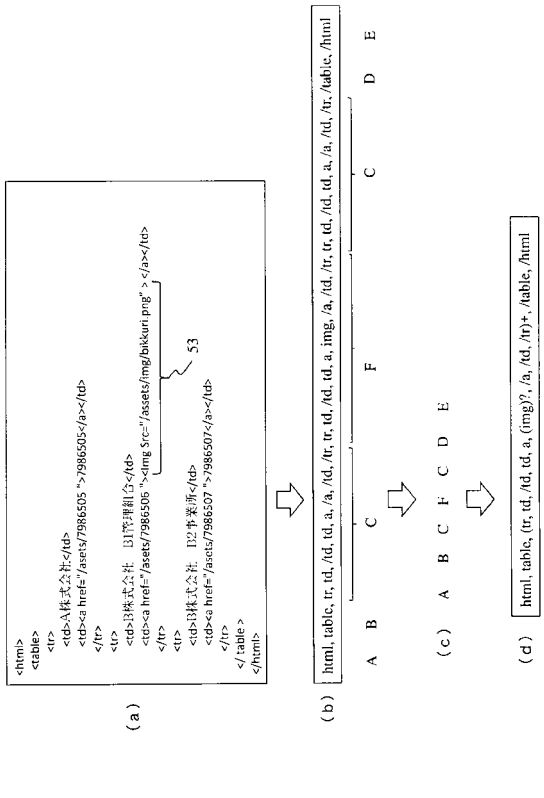

(a)
<html>
<script src="http://abc.com/bi.js"></script>

<script src="http://evil.com/poison.js"></script>
</html>
51
(b)
html, script, /script, img, div, script, /script , /div, /html

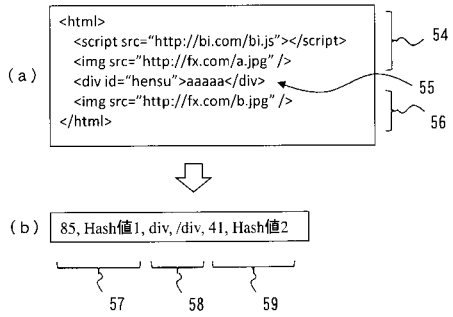
【図１０】


(a)
52
(b)
html, table, (tr, td, /td, td, a, /a, /td, /tr, tr, td, /td, td, a, /a, /td, /tr, tr, td, /td, td, a, /a, /td, /tr, /table, /html
A B C C C D E
(c) A B C C C D E
(d) A B C3 D E
(e) A B C+ D E
(f) html, table, (tr, td, /td, td, a, /a, /td, /tr)3, /table, /html
(g) html, table, (tr, td, /td, td, a, /a, /td, /tr)+, /table, /html

【図１１】


(a)
<html>
<table>
<tr>
<td>A株式会社</td>
<td>7986505</td>
</tr>
<tr>
<td>B株式会社 B1営業組合</td>
<td><img Src="/assets/img/bikkuri.png" ></td>
</tr>
<tr>
<td>B株式会社 B2営業所</td>
<td>7986507</td>
</tr>
</table>
</html>
53
(b) html, table, tr, td, /td, td, a, /a, /td, /tr, tr, td, /td, td, a, img, /a, /td, /tr, tr, td, /td, td, a, /a, /td, /tr, /table, /html
A B C F C D E
(c) A B C F C D E
(d) html, table, (tr, td, /td, td, a, (img)?, /a, /td, /tr)+, /table, /html

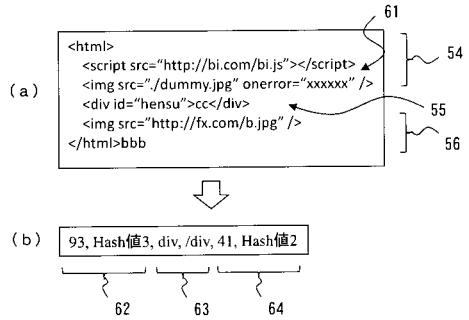
【図１２】


(a)
<html>
<script src="http://bi.com/bi.js"></script>

aaaaa

</html>
54
55
56
(b)
85, Hash値1, div, /div, 41, Hash値2
57
58
59

【図１３】


61
(a)
<html>
<script src="http://bi.com/bi.js"></script>

cc

</html>bbb
54
55
56
(b)
93, Hash値3, div, /div, 41, Hash値2
62
63
64