明細書

発明の名称

セキュリティ検証装置及びセキュリティ検証方法

技術分野

本発明は、システムのセキュリティに関し、特にセキュリティ設計の検証を行うセキュリティ検証装置、セキュリティ検証方法、及びそのためのプログラムに関する。

背景技術

セキュリティ技術に関し、さまざまな関連技術が知られている。

特許文献1は、以下に示す情報セキュリティ対策決定支援装置を開示する。

その情報セキュリティ対策決定支援装置は、診断対象システムの属性情報の入力を受ける。続けて、その情報セキュリティ対策決定支援装置は、脅威一覧や、その脅威とセキュリティ対策（以下、単に「対策」と記載）との関係等を参照して、その診断対象システムに含まれる情報セキュリティ上の問題点を洗い出す。ここで、その脅威一覧は、不正アクセス行為の手順を構造化したセキュリティ・イベント遷移モデルに基づいて生成されたものである。

次に、その情報セキュリティ対策決定支援装置は、診断対象システムの情報セキュリティを保つための対策パターンを提示する。

また、その情報セキュリティ対策決定支援装置は、その各対策のコストや効果を示す対策一覧を参照し、洗い出したその各対策について、その対策に掛かるコスト、その対策を施した場合の効果、及び残存リスク等を計算する。 そして、その情報セキュリティ対策決定支援装置は、この計算結果に基づいて、そのコストを最小にし、求める対策の強度を担保できる対策例、コスト対効果を最大にする対策例、コストを度外視してセキュリティ対策の強度を最大にする対策例など、要望にあった対策を選び出して提示する。

特許文献2は、以下に示す統合システムセキュリティ設計方法を開示する。

特許文献2の統合システムセキュリティ設計方法は、国際セキュリティ基準ISO17799（ISMS（Information Security Management System））とISO15408（CC

(Common Criteria))との両基準に準拠するサイト及び情報システムに関するセキュリティ設計方法である。

統合システムセキュリティ設計方法を実現するセキュリティ設計支援装置は、あるサイトについて、セキュリティの対象となる資産グループの情報の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その入力された資産グループの情報を表示し、各資産グループに対応する情報システムの「資産の情報」の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その入力された資産グループの情報を表示し、その各資産グループについて、「サイトの脅威の情報」の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その資産グループとその資産との対応関係に基づいて、その資産グループについてその入力された「サイトの脅威の情報」とその「資産の情報」とを表示し、その資産について「情報システムの脅威の情報」の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その入力された「サイトの脅威の情報」を表示し、その各サイトの脅威について「サイトの対策方針」の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、「サイトの脅威の情報」と「情報システムの脅威の情報」との対応関係に基づいて、その「サイトの脅威の情報」に対応して入力されたその「サイトの対策方針」とその「情報システムの脅威の情報」とを表示し、その各情報システムの脅威について「情報システムの対策方針」の入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その入力された「サイトの対策方針」を表示し、対策基準マッピングテーブルを参照して上位レベル対策基準を表示し、選択されたその「サイトの対策方針」について上位レベル対策基準の選択入力を受け付ける。ここで、その対策基準マッピングテーブルは、ISMSに準拠する上位レベル対策基準とCCに準拠する下位レベル対策基準との対応関係を格納するテーブルである。

次に、そのセキュリティ設計支援装置は、その「サイトの対策方針」とその「情報システムの対策方針」との対応関係に基づいて、選択されたその「サイトの対策方針」に対応するその「情報システムの対策方針」を表示する。次に、そのセキュリティ設計支援装置は、その「選択されたサイトの対策方針」に対応して選択された、上位レベル対策基準とその対策基準マッピングテーブル上で対応関係をもつ下位レベル対策基準とを表示し、選択されたその「情報システムの対策方針」について下位レベル対策基準の選択入力を受け付ける。

次に、そのセキュリティ設計支援装置は、その資産グループの情報とその資産の情報との対応から、選択された上位レベル対策基準と選択された下位レベル対策基準との対応に至るまでの、それらの対応を含む対応関係に従ってISMS準拠セキュリティ設計書とCC準拠セキュリティ設計書を作成して出力する。

[特許文献]

[特許文献1]特開2009－110177号公報

[特許文献2]特開2005－258512号公報

発明の概要

[発明が解決しようとする課題]

しかしながら、上述した特許文献に記載された技術においては、システムに必要なセキュリティ対策を実現するための、要素(例えば、機器、ソフトウェア)を漏れなく用意可能であることを検証することができないという問題点がある。

検証することができない理由は、以下のとおりである。

システムのセキュリティ設計において、そのシステムのセキュリティ要件(例えば、顧客の運用する資産の機密性/完全性保護)を満たすIT(Information Technology)セキュリティ対策を、そのシステムを構成する機器やソフトウェアで実現する必要がある。

そのシステムのセキュリティ要件は、例えば、ユーザからの要求にそったそのシステムの構成/動作要件である。そのシステムのセキュリティ要件は、また、ユーザ指定の各種セキュリティ規定(NISC(National Information Security Center、内閣官房情報セキュリティーセンター)統一基準等、業界で定められたセキュリティ要件)に対応するものである。

そのITセキュリティ対策は、それらのシステムのセキュリティ要件を、そのシステムを構成する要素でどのように実現するかについて、確実に設計できているかどうかを検証される必要がある。

特許文献1の情報セキュリティ対策決定支援装置は、システムによるセキュリティ対策の実現手段と、各構成要素との整合性を検証していない。そのため、その情報セキュリティ対策決定支援装置による設計では、セキュリティ設計に必要な製品が漏れなく含まれているかどうかを保証できず、システム構築時の製品調達漏れ等が発生する可能性がある。

同じく、特許文献2の統合システムセキュリティ設計方法も、システムによるセキュリティ対策の実現手段と、各構成要素との整合性を検証していない。

本発明の目的は、上述した問題点を解決できるセキュリティ検証装置、セキュリティ検証方法、及びそのためのプログラムを提供することにある。

[課題を解決するための手段]

本発明のセキュリティ検証装置は、セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶する検証アイテム記憶手段と、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶する機能アイテム記憶手段と、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記検証アイテム記憶手段から前記検証アイテムを選択して出力し、前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力する要件モデル生成手段と、

前記要件モデル生成手段が選択した前記検証アイテムに含まれる実現方式に基づいて、前記機能アイテム記憶手段から前記機能アイテムを抽出し、前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力する保有機能モデル生成手段と、

前記対象パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証し、前記比較検証の検証結果を、出力する検証手段と、を含む。

本発明のセキュリティ検証方法は、セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶し、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶している、コンピュータが、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記1以上記憶している検証アイテムの内から前記検証アイテムを選択して出力し、

前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力し、

前記選択した前記検証アイテムに含まれる実現方式に基づいて、前記1以上記憶している機能アイテムの内から前記機能アイテムを抽出し、

前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力し、

前記対象パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証し、

前記比較検証の検証結果を、出力する。

本発明の不揮発性記憶媒体に記録されたプログラムは、セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶し、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶している、コンピュータに、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記1以上記憶している検証アイテムの内から前記検証アイテムを選択して出力する処理と、

前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力する処理と、

前記選択した前記検証アイテムに含まれる実現方式に基づいて、前記1以上記憶し

ている機能アイテムの内から前記機能アイテムを抽出する処理と、

前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力する処理と、

前記対象パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証する処理と、

前記比較検証の検証結果を、出力する処理と、を実行させる。

[発明の効果]

本発明は、システムに必要なセキュリティ対策を実現するための要素を、漏れなく用意可能であることを検証することが可能になるという効果がある。

図面の簡単な説明

[図1] 図1は、第1の実施の形態の構成を示すブロック図である。

[図2] 図2は、第1の実施の形態におけるシステム要件の一例を示す図である。

[図3] 図3は、第1の実施の形態におけるセキュリティ対象モデルの一例を示す図である。

[図4] 図4は、第1の実施の形態における検証アイテムデータベースの一例を示す図である。

[図5] 図5は、第1の実施の形態における検証アイテムの一例を示す図である。

[図6] 図6は、第1の実施の形態における要件モデルの一例を示す図である。

[図7] 図7は、第1の実施の形態における機能アイテムデータベースの一例を示す図である。

[図8] 図8は、第1の実施の形態における機能アイテムの一例を示す図である。

[図9] 図9は、第1の実施の形態における保有機能モデルの一例を示す図である。

[図10] 図10は、第1の実施の形態のハードウェア構成を示す図である。

[図11] 図11は、第1の実施の形態におけるセキュリティ検証装置101の動作を示すフローチャートである。

[図12] 図12は、第2の実施の形態の構成を示すブロック図である。

[図13] 図13は、第2の実施の形態におけるシステムモデルの一例を示す図である。

[図14] 図14は、第3の実施の形態の構成を示すブロック図である。

[図15] 図15は、第3の実施の形態におけるセキュリティ規定データベースの一例を示す図である。

[図16] 図16は、プログラムを記録した不揮発性記憶媒体の例を示すブロック図である。

発明を実施するための形態

本発明を実施するための形態について図面を参照して詳細に説明する。

[第1の実施の形態]

図1は、本発明の第1の実施形態の構成を示すブロック図である。

図1を参照すると、本実施形態に係るセキュリティ検証装置101は、要件モデル生成部200、検証アイテムデータベース(検証アイテム記憶手段とも呼ばれる)210、保有機能モデル生成部300、機能アイテムデータベース(機能アイテム記憶手段とも呼ばれる)310及び検証部400を含む。

まず、本実施形態に係るセキュリティ検証装置101の動作の概要を説明する。

セキュリティ検証装置101は、外部装置(不図示)或いは操作者(不図示)から、被検証システムのセキュリティの要件を示す情報を受け取る。また、セキュリティ検証装置101は、被検証システムの内そのセキュリティの要件に対応するセキュリティ対象部分の構成を示す情報を受け取る。そして、セキュリティ検証装置101は、これらの受け取った情報に基づいて、その被検証システムのセキュリティ(安全性)を検証し、結果を出力する。

図2は、被検証システムのセキュリティの要件を示す情報である、システム要件110の一例を示す図である。図2に示すようにシステム要件110は、セキュリティ要件に係わるキーワードとして、例えば、「主体認証」、「WEB(ウェブ、ワールドワイドウェブのこと)」、「AP(APPRICATION)」及び「DB(DATABASE)」を含む。尚、図2に示すシステム要件110は、セキュリティの要件を1件示している。しかし、システム要件110は、任意の数のセキュリティ要件を示すものであってよい。

図3は、被検証システムのセキュリティ対象部分の構成を示す情報である、セキュリティ対象モデル140の一例を示す図である。図3に示すようにセキュリティ対象モデル140は、被検証システムのセキュリティ対象部分の構成を示す情報として、接続元識別情報(例えば、装置名、機能ブロック名)142と接続先識別情報143とを含む。尚、

図3に示すセキュリティ対象モデル140は、図2に示すシステム要件110に対応する、被検証システムのセキュリティ対象部分の構成を示す情報である。システム要件110が複数の件数のセキュリティ要件を示している場合、セキュリティ対象モデル140は、そのセキュリティ要件に対応する被検証システムのセキュリティ対象部分の構成の種類の数だけ存在する。

被検証システムのセキュリティの検証の結果は、セキュリティ対象モデル140の保有する機能が、システム要件110で示されるセキュリティの要件を満足するか否かを示す情報である。尚、その結果は、他の情報(例えば、セキュリティ機能の運用条件、セキュリティを満足するための設定情報)を含んでいてもよい。

次に、第1の実施の形態におけるセキュリティ検証装置101が備える各構成要素について説明する。尚、図1に示す構成要素は、ハードウェア単位の構成要素ではなく、機能単位の構成要素を示している。

＝＝＝要件モデル生成部200＝＝＝

要件モデル生成部200は、被検証システムのシステム要件110に基づいて、検証アイテムデータベース210の内容を参照し、セキュリティ機能と実現方式と対象パーツとが関連付けられた検証アイテムを選択して出力する。また、要件モデル生成部200は、セキュリティ対象モデル140に基づいて、選択した検証アイテムに含まれる対象パーツそれぞれのセキュリティの要件を示す情報を生成し、出力する。

具体的には、第1に要件モデル生成部200は、検証アイテムデータベース210を参照し、受け取ったシステム要件110に対応する検証アイテムを選択し、出力する。

図4は、検証アイテムデータベース210の一例を示す図である。図4に示すように、検証アイテムデータベース210は、セキュリティ機能名212と実現方式213とパーツ情報214とが関連付けられたレコード(検証アイテム)を1以上含む。セキュリティ機能名212は、セキュリティの内容(例えば、主体認証)を特定する情報である。実現方式213は、セキュリティ機能名212で特定されるセキュリティの実現方式(例えば、ID(IDENTIFICATION)／パスワード方式)を示す情報である。パーツ情報214は、そのセキュリティを実現する1以上のパーツ(例えば、装置、機能ブロック)それぞれの識別情報(例えば、WWWサーバ、APサーバ、DBサーバ)を含む。

図5は、要件モデル生成部200が選択した検証アイテム211の一例を示す図である。尚、図5は、システム要件110に対応して、検証アイテムデータベース210から1レコー

ドが選択された場合の例を示している。しかし、システム要件１１０が複数のセキュリティの内容を指定している場合、選択されるレコードも複数であってよい。

第２に、要件モデル生成部２００は、受け取ったセキュリティ対象モデル１４０と、検証アイテム２１１とからパーツ毎のセキュリティ検証の要件を示すモデルを生成する。

図６は、パーツ毎のセキュリティ検証の要件を示すモデルである、要件モデル２３０の例を示す図である。図６に示すように、要件モデル２３０は、パーツ識別情報２３２、セキュリティ機能名２３３及び実現方式２３４とから構成されるレコードを１以上含む。パーツ識別情報２３２は、各パーツを識別する情報である。このパーツ識別情報２３２は、検証アイテム２１１のパーツ情報２１４で示されるパーツの識別情報と、受け取ったセキュリティ対象モデル１４０に含まれる接続先識別情報１４３と、が一致している識別情報である。セキュリティ機能名２３３は、検証アイテム２１１のセキュリティ機能名２１２のコピーである。実現方式２３４は、検証アイテム２１１の実現方式２１３のコピーである。

即ち、要件モデル生成部２００は、検証アイテム２１１のパーツ情報２１４で示されるパーツの識別情報の内、受け取ったセキュリティ対象モデル１４０に含まれる接続先識別情報１４３と一致する識別情報で特定されるパーツを抽出する。続けて、要件モデル生成部２００は、抽出したパーツ毎のセキュリティの要件を示す、要件モデル２３０を生成する。

＝＝＝検証アイテムデータベース２１０＝＝＝

検証アイテムデータベース２１０は、複数の検証アイテム２１１を記憶し、要求に応答して出力する。

＝＝＝保有機能モデル生成部３００＝＝＝

保有機能モデル生成部３００は、要件モデル生成部２００が出力した検証アイテム２１１に含まれる実現方式２１３に基づいて、機能アイテムデータベース３１０から機能アイテムを抽出する。続けて、保有機能モデル生成部３００は、抽出した機能アイテムに基づいて、セキュリティ対象モデル１４０に含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力する。

具体的には、第１に保有機能モデル生成部３００は、受け取った検証アイテム２１１の実現方式２１３に基づいて、機能アイテムデータベース３１０から機能アイテムを抽出する。

図7は、機能アイテムデータベース310の一例を示す図である。図7に示すように機能アイテムデータベース310は、パーツ識別情報312とセキュリティ機能名313と実現手段314とが関連付けられたレコード(機能アイテム)を1以上含む。パーツ識別情報312は、各パーツを識別する情報である。セキュリティ機能名313は、セキュリティの内容(例えば、識別認証)を特定する情報である。実現手段314は、パーツ識別情報312で特定されるパーツのセキュリティ機能名313で特定されるセキュリティの実現手段(例えば、ID(IDENTIFICATION)／パスワード方式)を示す情報である。

図8は、機能アイテム320の一例を示す図である。図8に示すように機能アイテム320は、検証アイテムデータベース210から選択されたレコードを1以上含む。

第2に、保有機能モデル生成部300は、受け取ったセキュリティ対象モデル140と、機能アイテム320とから、パーツ毎のセキュリティ検証の保有機能を示すモデルを生成する。

図9は、パーツ毎のセキュリティ検証の保有機能を示すモデルである、保有機能モデル330の例を示す図である。図9に示すように、保有機能モデル330は、パーツ識別情報332、セキュリティ機能名333及び実現手段334とから構成されるレコードを1以上含む。パーツ識別情報332は、各パーツを識別する情報である。このパーツ識別情報332は、機能アイテム320のパーツ識別情報312と、受け取ったセキュリティ対象モデル140に含まれる接続先識別情報143と、が一致している識別情報である。セキュリティ機能名333は、セキュリティ機能名313のコピーである。実現手段334は、機能アイテム320の実現手段314のコピーである。

即ち、保有機能モデル生成部300は、機能アイテム320のパーツ識別情報312の内、受け取ったセキュリティ対象モデル140に含まれる接続先識別情報143と一致する、パーツ識別情報312を含むレコードを抽出する。続けて、保有機能モデル生成部300は、抽出したパーツ毎の保有機能を示す、保有機能モデル330を生成する。

＝＝＝機能アイテムデータベース310＝＝＝

機能アイテムデータベース310は、複数の機能アイテム320を記憶し、要求に応答して出力する。

＝＝＝検証部400＝＝＝

検証部400は、要件モデル230と保有機能モデル330とを比較検証し、その検証結果を、出力する。

具体的には、第1に検証部400は、要件モデル230に含まれるパーツ識別情報232の内、保有機能モデル330に含まれるパーツ識別情報332のいずれにも一致しないパーツ識別情報232が存在するか否かを検証する。

第2に、検証部400は、検証した結果を出力する。この、検証結果は、セキュリティ対象モデル140がシステム要件110を満足していることを示す情報、或いは、満足していないことを示す情報である。

尚、検証部400は、検証結果に加えて、セキュリティ機能名233及び保有機能モデル330を出力してもよい。

以上が、セキュリティ検証装置101の機能単位の各構成要素についての説明である。

次に、セキュリティ検証装置101のハードウェア単位の構成要素について説明する。

図10は、本実施形態におけるセキュリティ検証装置101とその周辺装置のハードウェア構成を示す図である。図10に示されるように、セキュリティ検証装置101は、CPU(Central Processing Unit)1070、記憶部1071、記憶装置1072、入力部1073、出力部1074及び通信部1075を含む。

図16は、プログラムを記録した不揮発性記憶媒体1077の例を示すブロック図である。

CPU1070は、オペレーティングシステム(不図示)を動作させて、本実施形態に係るセキュリティ検証装置101の全体の動作を制御する。また、CPU1070は、例えば記憶装置1072に装着された不揮発性記録媒体1077(または記憶媒体)から、プログラムやデータを読み込み、読み込んだプログラムやデータを記憶部1071に書き込む。そして、CPU1070は、読み込んだプログラムに従って、また読み込んだデータに基づいて、図1に示す要件モデル生成部200、保有機能モデル生成部300及び検証部400として各種の処理を実行する。

尚、CPU1070は、通信網(不図示)に接続されている外部コンピュータ(不図示)から、記憶部1071にプログラムやデータをダウンロードするようにしてもよい。

記憶部1071は、プログラムやデータを記憶する。

記憶装置1072は、例えば、光ディスク、フレキシブルディスク、磁気光ディスク、外付けハードディスク及び半導体メモリであって、不揮発性記憶媒体1077を含む。記憶装置1072は、プログラムをコンピュータ読み取り可能に記録する。また、記憶装置107

2は、データをコンピュータ読み取り可能に記録してもよい。記憶装置1072は、検証アイテムデータベース210及び機能アイテムデータベース310を含んでもよい。

入力部1073は、例えばマウスやキーボード、内蔵のキーボタンなどで実現され、入力操作に用いられる。入力部1073は、マウスやキーボード、内蔵のキーボタンに限らず、例えばタッチパネル、加速度計、ジャイロセンサ、カメラなどでもよい。

出力部1074は、例えばディスプレイで実現され、出力を確認するために用いられる。

通信部1075は、セキュリティ検証装置101と外部装置(不図示)とのインタフェースを実現する。通信部1075は、要件モデル生成部200、保有機能モデル生成部300及び検証部400の一部として含まれる。

以上が、セキュリティ検証装置101のハードウェア単位の各構成要素についての説明である。

以上説明したように、図1に示す機能単位のブロックは、図10に示すハードウェア構成によって実現される。但し、セキュリティ検証装置101が備える各部の実現手段は、上記に限定されない。すなわち、セキュリティ検証装置101は、物理的に結合した一つの装置により実現されてもよいし、物理的に分離した2つ以上の装置を有線または無線で接続し、これら複数の装置により実現されてもよい。

また、前述のプログラムを記録した不揮発性記録媒体1077がセキュリティ検証装置101に供給され、セキュリティ検証装置101は、不揮発性記録媒体1077に格納されたプログラムを読み込み、実行してもよい。すなわち、本実施形態は、セキュリティ検証装置101が実行するプログラムを、一時的にまたは非一時的に、記憶する記録媒体の実施形態を含む。図

次に本実施形態の動作について、図1～図11を参照して詳細に説明する。

図11は、セキュリティ検証装置101の動作を示すフローチャートである。尚、このフローチャートによる処理は、前述したCPUによるプログラム制御に基づいて、実行されても良い。また、処理のステップ名については、S601のように、記号で記載する。

セキュリティ検証装置101は、外部装置(不図示)から、システム要件110とセキュリティ対象モデル140とを受け取る(S610)。

例えば、セキュリティ検証装置101は、図10に示す通信部1075を介して、外部のサーバ(不図示)から、システム要件110とセキュリティ対象モデル140とを受け取る。

また、セキュリティ検証装置101は、図10に示す入力部1073から操作者が入力するシステム要件110とセキュリティ対象モデル140とを受け取るようにしてもよい。

次に、セキュリティ検証装置101の要件モデル生成部200は、受け取ったシステム要件110に含まれるセキュリティ機能を示すキーワード(図2に示すシステム要件110の場合、「主体認証」)を抽出する(S612)。

次に、要件モデル生成部200は、検証アイテムデータベース210を検索し、抽出したキーワードに一致するセキュリティ機能名212を含むレコード(検証アイテム211)を選択し、出力する(S614)。

次に、要件モデル生成部200は、選択した検証アイテム211のパーツ情報214に含まれるパーツの識別情報(ここでは、「WWWサーバ」、「APサーバ)及び「DBサーバ」)と一致する、セキュリティ対象モデル140の接続先識別情報143を選択する(S616)。

続けて、要件モデル生成部200は、次の第1、第2及び第3の手順で、要件モデル230を生成する。第1に、要件モデル生成部200は、選択した接続先識別情報143をパーツ識別情報232とする。第2に、要件モデル生成部200は、検証アイテムデータベース210のセキュリティ機能名212をセキュリティ機能名233とする。第3に、要件モデル生成部200は、検証アイテムデータベース210の実現方式213を実現方式234とする。(S618)。

次に、保有機能モデル生成部300は、受け取った検証アイテム211から実現方式213を取得する(S620)。

次に、保有機能モデル生成部300は、機能アイテムデータベース310を検索し、取得した実現方式213に一致する実現手段314を含むレコードを機能アイテム320として取得する(S622)。

次に、保有機能モデル生成部300は、受け取ったシステム要件110に含まれるパーツを示すキーワード(図2に示すシステム要件110の場合、「WEB」、「AP」及び「DB」)を抽出する(S624)。

次に、保有機能モデル生成部300は、機能アイテム320の内、抽出したキーワードに対応するパーツ識別情報312を含むレコードを選択する(S626)。

続けて、保有機能モデル生成部300は、選択したレコードのパーツ識別情報312をパーツ識別情報332とし、実現手段314を実現手段334として保有機能モデル330を生成する(S628)。

次に、検証部400は、要件モデル230に含まれる各レコードに対応するレコードを保有機能モデル330が含むか否かを判定する(S630)。ここで、要件モデル230に含まれる各レコードに対応する、保有機能モデル330に含まれるレコードは、以下の第1、第2及び第3の条件を満たす。第1に、要件モデル230に含まれるレコードのパーツ識別情報232と保有機能モデル330に含まれるレコードのパーツ識別情報332とが一致する。第2に、要件モデル230に含まれるレコードのセキュリティ機能名233と保有機能モデル330に含まれるレコードのセキュリティ機能名333とが対応する。第3に、要件モデル230に含まれるレコードの実現方式234と保有機能モデル330に含まれるレコードの実現手段334とが一致する。尚、セキュリティ機能名233に対応するセキュリティ機能名333は、例えば、同じ認証機能を表す、「主体認証」に対する「識別認証」である。

要件モデル230に含まれる全てのレコードに対応するレコードを保有機能モデル330が含む場合(S630でYES)、検証部400は、セキュリティ対象モデル140がシステム要件110を満足していることを示す情報を出力する(S632)。

要件モデル230に含まれるいずれかのレコードに対応するレコードを保有機能モデル330が含んでいない場合(S630でNO)、検証部400は、セキュリティ対象モデル140がシステム要件110を満足していないことを示す情報を出力する(S634)。

上述した本実施形態における第1の効果は、システムに必要なセキュリティ対策を実現するための要素を、漏れなく用意可能であることを検証することを可能にする点である。

その理由は、以下のような構成を含むからである。即ち、要件モデル生成部200が、被検証システムのセキュリティ要件に対応する、パーツ毎のセキュリティ要件を示す要件モデル230を生成する。第2に、保有機能モデル生成部300が被検証システムのセキュリティ対象部分を構成するパーツ毎の、セキュリティに関する保有機能を示す保有機能モデル330を生成する。第3に、検証部400が要件モデル230と保有機能モデル330とを比較検証する。

上述した本実施形態における第2の効果は、システム要件110が被検証システムの構成要素によりどのように実現されているかの提示を可能にする点である。

その理由は、検証部400が、検証結果に加えて、セキュリティ機能名233及び保有機能モデル330を出力するようにしたからである。

[第2の実施形態]

次に、本発明の第2の実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

図12は、本発明の第2の実施形態に係るセキュリティ検証装置102の構成を示すブロック図である。

図12を参照すると、本実施形態のセキュリティ検証装置102は、第1の実施形態のセキュリティ検証装置101と比べて、セキュリティ対象モデル抽出部500を更に含む。

セキュリティ検証装置102は、第1の実施形態のセキュリティ検証装置101が受け取るセキュリティ対象モデル140に替えて、図13に示すようなシステムモデル120を受け取る。システムモデル120は、セキュリティ対象モデル140の構成を、全体の構成の一部として含む。例えば、システムモデル120は、被検証システム全体の構成を示す情報である。

図13は、システムモデル120の一例を示す図である。図13に示すようにシステムモデル120は、被検証システム全体の構成を示す情報として、接続元識別情報142と接続先識別情報143とを含む。

＝＝＝セキュリティ対象モデル抽出部500＝＝＝

セキュリティ対象モデル抽出部500は、受け取ったシステムモデル120から、システム要件110に基づいて、セキュリティ対象モデル140を生成し、出力する。

例えば、セキュリティ対象モデル抽出部500は、システム要件110に含まれるキーワード「WEB」に基づいて、「外部WWWサーバ」から「インターネット」までの経路に係わるレコードを、システムモデル120から抽出する。更に、セキュリティ対象モデル抽出部500は、システム要件110に含まれるキーワード「AP」に基づいて、「APサーバ」から「インターネット」までの経路に係わるレコードを、システムモデル120から抽出する。更に、セキュリティ対象モデル抽出部500は、システム要件110に含まれるキーワード「DB」に基づいて、「DBサーバ」から「インターネット」までの経路に係わるレコードを、シ

ステムモデル120から抽出する。次に、セキュリティ対象モデル抽出部500は、これらの抽出したレコードをセキュリティ対象モデル140として出力する。

上述した本実施形態における効果は、セキュリティ対象モデル140を正確に生成することを可能にする点である。

その理由は、セキュリティ対象モデル抽出部500が、システム要件110に基づいてセキュリティ対象モデル140を生成するようにしたからである。

[第3の実施形態]

次に、本発明の第3の実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

図14は、本発明の第3の実施形態に係るセキュリティ検証装置103の構成を示すブロック図である。

図14を参照すると、本実施形態のセキュリティ検証装置103は、第1の実施形態のセキュリティ検証装置101と比べて、セキュリティ規定データベース(セキュリティ規定記憶手段とも呼ばれる)410を更に含む。また、セキュリティ検証装置103は、第1の実施形態のセキュリティ検証装置101と比べて、検証部400に替えて検証部403を含む。

===セキュリティ規定データベース410===

図15は、セキュリティ規定データベース410の一例を示す図である。図15に示すように、セキュリティ規定データベース410は、セキュリティ機能名412と規定識別情報413とが関連付けられたレコードを1以上含む。セキュリティ機能名412は、セキュリティの内容を特定する情報である。規定識別情報413は、セキュリティ機能名412で特定されるセキュリティの内容に対応する、予め定められたセキュリティ基準における各規定を1つ以上特定する情報である。ここで、予め定められたセキュリティ基準は、例えば、公的セキュリティ基準(例えば、「政府機関の情報セキュリティ対策のための統一基準」)である。また、各規定を特定する情報は、例えば、「政府機関の情報セキュリティ対策のための統一基準」の見出し番号である。また、各規定を特定する情報は、基準名(例えば、ISMS)とその基準名で特定される基準で規定される各セキュリティ機能の識別情報との組(例えば、ISMS:12.1.4)であってもよい。

===検証部403===

検証部403は、検証部400が出力する検証結果に加えて、その検証結果の対象であるセキュリティ機能に対応する規定識別情報413を、出力する。

例えば、検証部403は、セキュリティ機能名233が「主体認証」の要件モデル230について検証を行った場合、セキュリティ規定データベース410を参照して規定識別情報413の「2.2.1.1(1)(a)」を取得し、検証結果と合わせて出力する。

更に、検証部403は、他のデータベース(不図示)を参照し、関連する情報(例えば、パーツ識別情報332で特定されるパーツの設定情報)を検証結果と合わせて出力するようにしてもよい。

また、検証部403は、第1の実施形態と同様に、検証結果に加えて、セキュリティ機能名233及び保有機能モデル330を出力するようにしてもよい。

尚、検証部403は、第2の実施形態に適用してもよい。

上述した本実施形態における第1の効果は、政府/業界で定められているセキュリティ規定の各項目に対して、被検証システムが規定を満足しているか否かを示すことを、可能にする点である。

その理由は、検証部403が、セキュリティ規定データベース410を参照して、規定識別情報413を、出力するようにしたからである。

上述した本実施形態における第2の効果は、予め定められたセキュリティ基準が、被検証システムの構成要素によりどのように実現されているかの提示を可能にする点である。

その理由は、検証部400が、検証結果に加えて、セキュリティ機能名233及び保有機能モデル330を出力するようにしたからである。

尚、上述の各実施形態においては、1つのセキュリティ機能に関して入力情報が各セキュリティ検証装置に入力され、各セキュリティ検証装置からそれに対応する1つの検証結果を出力する場合を説明した。しかし、各セキュリティ検証装置は、複数のセキュリティ機能に関して入力情報が入力され、それに対応する複数の検証結果を出力するようにしてもよい。この場合検証結果及びその他の関連情報は、表の形式で出力されてもよい。

また、実施形態3の場合、その表は、予め定められたセキュリティ基準の各項目と、その項目それぞれに対応する一覧表であってもよい。

以上の各実施形態で説明した各構成要素は、必ずしも個々に独立した存在である必要はない。例えば、各構成要素は、複数の構成要素が1個のモジュールとして実現されたり、1つの構成要素が複数のモジュールで実現されたりしてもよい。また、各構成要素は、ある構成要素が他の構成要素の一部であったり、ある構成要素の一部と他の構成要素の一部とが重複していたり、といったような構成であってもよい。

以上説明した各実施形態における各構成要素及び各構成要素を実現するモジュールは、必要に応じ可能であれば、ハードウェア的に実現されても良いし、コンピュータ及びプログラムで実現されても良いし、ハードウェア的なモジュールとコンピュータ及びプログラムとの混在により実現されても良い。プログラムは、磁気ディスクや半導体メモリなど、不揮発性のコンピュータ可読記録媒体に記録されて提供され、コンピュータの立ち上げ時などにコンピュータに読み取られる。この読み取られたプログラムは、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施形態における構成要素として機能させる。

また、以上説明した各実施形態では、複数の動作をフローチャートの形式で順番に記載してあるが、その記載の順番は複数の動作を実行する順番を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の順番は内容的に支障しない範囲で変更することができる。

更に、以上説明した各実施形態では、複数の動作は個々に相違するタイミングで実行されることに限定されない。例えば、ある動作の実行中に他の動作が発生したり、ある動作と他の動作との実行タイミングが部分的に乃至全部において重複していたりしていてもよい。

更に、以上説明した各実施形態では、ある動作が他の動作の契機になるように記載しているが、その記載はある動作と他の動作の全ての関係を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の関係は内容的に支障のない範囲で変更することができる。また各構成要素の各動作の具体的な記載は、各構成要素の各動作を限定するものではない。このため、各構成要素の具体的な各動作は、各実施形態を実施する上で機能的、性能的、その他の特性に対して支障をきたさない範囲内で変更されて良い。

以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者

が理解し得るさまざまな変更をすることができる。

この出願は、2011年12月1日に出願された日本出願特願2011－263754を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

101 セキュリティ検証装置
102 セキュリティ検証装置
103 セキュリティ検証装置
110 システム要件
120 システムモデル
140 セキュリティ対象モデル
142 接続元識別情報
143 接続先識別情報
200 要件モデル生成部
210 検証アイテムデータベース
211 検証アイテム
212 セキュリティ機能名
213 実現方式
214 パーツ情報
230 要件モデル
232 パーツ識別情報
233 セキュリティ機能名
234 実現方式
300 保有機能モデル生成部
310 機能アイテムデータベース
312 パーツ識別情報
313 セキュリティ機能名
314 実現手段
320 機能アイテム
330 保有機能モデル

332 パーツ識別情報
333 セキュリティ機能名
334 実現手段
400 検証部
403 検証部
410 セキュリティ規定データベース
412 セキュリティ機能名
413 規定識別情報
500 セキュリティ対象モデル抽出部
1070 CPU
1071 記憶部
1072 記憶装置
1073 入力部
1074 出力部
1075 通信部

請求の範囲

[請求項1]

セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶する検証アイテム記憶手段と、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶する機能アイテム記憶手段と、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記検証アイテム記憶手段から前記検証アイテムを選択して出力し、前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力する要件モデル生成手段と、

前記要件モデル生成手段が選択した前記検証アイテムに含まれる実現方式に基づいて、前記機能アイテム記憶手段から前記機能アイテムを抽出し、前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力する保有機能モデル生成手段と、

前記パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証し、前記比較検証の検証結果を、出力する検証手段と、を含む

セキュリティ検証装置。

[請求項2]

前記システム要件と前記セキュリティ対象モデルの構成を全体の構成の一部として含むシステムモデルとに基づいて、前記セキュリティ対象モデルを生成し、出力するセキュリティ対象モデル抽出手段を更に含む、

ことを特徴とする請求項1記載のセキュリティ検証装置。

[請求項3]

前記セキュリティ機能名と前記セキュリティ機能名で特定されるセキュリティの内容に対応する、予め定められたセキュリティ基準における各規定を1つ以上特定する情報である規定識別情報とが関連付けられたレコードを1以上含むセキュリティ規定記憶手段を更に含み、

前記検証手段は、セキュリティ規定記憶手段を参照し、前記検証結果の対象であるセキュリティ機能に対応する規定識別情報を、出力する

ことを特徴とする請求項1または2記載のセキュリティ検証装置。

[請求項4]

前記検証手段は、前記パーツそれぞれのセキュリティの要件を示す情報及び前記パーツそれぞれのセキュリティの保有機能を示す情報の内の、任意の情報を更に出力する

ことを特徴とする請求項1乃至3のいずれか1項に記載のセキュリティ検証装置。

[請求項5]

セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶し、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶している、コンピュータが、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記1以上記憶している検証アイテムの内から前記検証アイテムを選択して出力し、

前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力し、

前記選択した前記検証アイテムに含まれる実現方式に基づいて、前記1以上記憶している機能アイテムの内から前記機能アイテムを抽出し、

前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力し、

前記対象パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証し、

前記比較検証の検証結果を、出力する

セキュリティ検証方法。

[請求項6]

セキュリティの内容を特定する情報であるセキュリティ機能名と前記セキュリティの実現方式を示す情報である実現方式と前記セキュリティを実現する1以上のパーツそれぞれの識別情報であるパーツ識別情報を含むパーツ情報とを少なくとも含む検証アイテムを1以上記憶し、

前記パーツ識別情報と前記セキュリティ機能名と前記パーツ識別情報で特定されるパーツの前記セキュリティ機能名で特定されるセキュリティの実現手段を示す情報である実現手段とを少なくとも含む機能アイテムを1以上記憶している、コンピュータに、

被検証システムのセキュリティの要件を示す情報であるシステム要件に基づいて、前記1以上記憶している検証アイテムの内から前記検証アイテムを選択して出力する処理と、

前記被検証システムのセキュリティ対象部分の構成を示す情報であるセキュリティ対象モデルに基づいて、前記選択した検証アイテムのパーツ情報に含まれるパーツ識別情報で特定されるパーツそれぞれのセキュリティの要件を示す情報を生成し、出力する処理と、

前記選択した前記検証アイテムに含まれる実現方式に基づいて、前記1以上記憶している機能アイテムの内から前記機能アイテムを抽出する処理と、

前記抽出した機能アイテムに基づいて、前記セキュリティ対象モデルに含まれるパーツそれぞれのセキュリティの保有機能を示す情報を生成し、出力する処理と、

前記対象パーツそれぞれのセキュリティの要件を示す情報と前記パーツそれぞれのセキュリティの保有機能を示す情報とを比較検証する処理と、

前記比較検証の検証結果を、出力する処理と、を実行させる

プログラムを記録した不揮発性記憶媒体。