(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5999191号
(P5999191)
(45)発行日　平成28年9月28日(2016.9.28)　(24)登録日　平成28年9月9日(2016.9.9)

(51)Int.Cl.　F I
G06F 21/57 (2013.01)　G06F 21/57 370

請求項の数 7 (全 20 頁)

(21)出願番号　特願2014-541976(P2014-541976)
(86)(22)出願日　平成25年7月18日(2013.7.18)
(86)国際出願番号　PCT/JP2013/069557
(87)国際公開番号　WO2014/061326
(87)国際公開日　平成26年4月24日(2014.4.24)
審査請求日　平成28年6月16日(2016.6.16)
(31)優先権主張番号　特願2012-228074(P2012-228074)
(32)優先日　平成24年10月15日(2012.10.15)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100124154
弁理士　下坂　直樹
(72)発明者　芦野　佑樹
東京都港区芝五丁目７番１号
日本電気株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】セキュリティ機能設計支援装置、セキュリティ機能設計支援方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
システムの構成を表示装置に表示するシステム構成データ表示部と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する実現方式設定支援部と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する付随機能要素設定支援部と、
ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する付随機能要素評価部と、
前記付随機能要素評価部による判定の結果を出力する評価結果出力部と、を含むセキュリティ機能設計支援装置。
【請求項２】
前記付随機能要素評価部は、
ユーザ操作によって設定された前記付随機能要素のデータを取得し、
前記妥当性を判定するための条件に基づいて、システム構成データおよびユーザ操作に

よって設定された前記セキュリティ実現方式の情報を参照しながら付随機能要素の妥当性を判定する、請求項１に記載のセキュリティ機能設計支援装置。
【請求項３】
前記評価結果出力部は、
ユーザが必須の付随機能要素を設定しなかった場合には、必須要素であることを知らせる画像を表示する、請求項１または２に記載のセキュリティ機能設計支援装置。
【請求項４】
前記評価結果出力部は、
ある付随機能要素を機能させるために必要な副実現方式が設定されていない場合には、その付随機能要素が設定されている実現方式を含めて不合格であることを知らせる画像を表示する、請求項１から３のいずれか１項に記載のセキュリティ機能設計支援装置。
【請求項５】
前記評価結果出力部は、
設定された各々の実現方式にかかるコストの情報を表示する、請求項１から４のいずれか１項に記載のセキュリティ機能設計支援装置。
【請求項６】
システムの構成を表示装置に表示する工程と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する工程と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する工程と、
ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する工程と、
前記判定の結果を出力する工程と、を含むセキュリティ機能設計支援方法。
【請求項７】
コンピュータを、
システムの構成を表示装置に表示するシステム構成データ表示部と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する実現方式設定支援部と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する付随機能要素設定支援部と、
ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する付随機能要素評価部と、
前記付随機能要素評価部による判定の結果を出力する評価結果出力部と、
して機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティ機能設計支援装置、セキュリティ機能設計支援方法、およびプログラムに関する。
【背景技術】
【０００２】
コンピュータシステムのセキュリティ機能設計の要素には、あるセキュリティ機能（例

えば主体認証）を実現するための具体的な方策（セキュリティ実現方式）と、そのセキュリティ実現方式を機能させる上で必要となる付随的な方策（付随機能要素）が含まれる。付随機能要素は、システム構成によって変化する。例えば、セキュリティ実現方式としてユーザＩＤとパスワードを用いた認証方式を採用する際、ユーザＩＤとパスワードが送受信される通信経路の暗号化が必要か否かは、システムがオンラインかオフラインかによって変化する。すなわち、この例では通信路の暗号化が付随機能要素となる。システムの設計者は、システム構成を考慮して付随機能要素を選択し、過不足が無いように設計する必要がある。そのためには、システム設計者は、システム全体の知識の他、セキュリティ全般の知識が必要となり、大変な労力が必要となる。また、付随機能要素の設計が不十分であると、それが原因でシステム全体のセキュリティ機能が有効に働かなくなり、結果としてセキュリティ事故が発生する要因となり得る。

【０００３】

特許文献１に記載されたセキュリティ設計支援方法では、設計対象システムに想定される脅威の原因となるエージェントの場所から当該脅威により被害を受ける資産の場所までの経路上の場所をセキュリティ機能要件の配置候補とする。さらに予め定めた配置ルールに従い、各配置候補の優先度を判定することにより、セキュリティ機能要件の配置を容易にしている。

【０００４】

特許文献２に記載されたセキュリティ設計支援方法では、情報システムの脅威のリスク値と、当該脅威に対する対策方針と、当該脅威に対する対策方針のセキュリティ機能要件から、当該セキュリティ機能要件の重要度を取得する。また、セキュリティ機能要件の重要度と、当該セキュリティ機能要件と既存の情報関連製品のセキュリティ機能との関連度と、当該情報関連製品のセキュリティ機能の満足度とから、情報システムへ導入する情報関連製品を導出する。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００６－２７６９９３号公報

【特許文献２】特開２００６－３５０３９９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかし、特許文献１に記載の方法では、セキュリティ機能要件の配置を支援することはできるが、セキュリティ機能を実現するための付随機能要素の配置の妥当性を判定することはできない。

【０００７】

また、特許文献２に記載の方法では、セキュリティ機能要件の重要度や、情報関連製品のセキュリティ機能との関連度、情報関連製品のセキュリティ機能の満足度などのデータに基づいてセキュリティ設計を支援しているが、システム構成などの条件に基づいて付随機能要素の妥当性を判定することはできなかった。

【０００８】

以上のように、特許文献１，２に記載の方法では、セキュリティ機能の実現方式を機能させるための付随機能要素の設定を支援することはできなかった。

【０００９】

本発明は、システム構成によって異なる、セキュリティ実現方式に必要な付随機能要素の配置の妥当性を評価し、付随機能要素の設計を支援することである。

【００１０】

本発明に係るセキュリティ機能設計支援装置は、システムの構成を表示装置に表示するシステム構成データ表示部と、セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作

によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する実現方式設定支援部と、前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する付随機能要素設定支援部と、ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する付随機能要素評価部と、前記付随機能要素評価部による判定の結果を出力する評価結果出力部と、を含む。

【発明の効果】

【００１１】

本発明によれば、システム構成によって異なる、セキュリティ実現方式に必要な付随機能要素の配置の妥当性を評価し、付随機能要素の設計を支援することができる。

【図面の簡単な説明】

【００１２】

【図１】本発明の実施の形態による、セキュリティ機能設計支援装置の構成を示すブロック図。

【図２】本発明の実施の形態による、システム構成データ記憶部に記憶されるデータの例を示す図。

【図３】本発明の実施の形態による、実現方式記憶部に記憶されるデータの例を示す図。

【図４】本発明の実施の形態による、付随機能要素記憶部に記憶されるデータの例を示す図。

【図５】本発明の実施の形態による、付随機能要素定義記憶部に記憶されるデータの例を示す図。

【図６】本発明の実施の形態による、セキュリティ機能設計支援装置の動作のフローチャート。

【図７】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図８】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図９】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１０】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１１】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１２】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１３】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１４】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１５】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１６】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１７】本発明の実施の形態による、表示装置に表示される画面の例を示す図。

【図１８】本発明の実施の形態による、付随機能要素の評価の動作のフローチャート。

【図１９】本発明の実施の形態による、付随機能要素の評価の動作のフローチャート。

【図２０】本発明の変形例による、表示装置に表示される画面の例を示す図。

【発明を実施するための形態】

【００１３】

（セキュリティ機能設計）

コンピュータシステムが提供する機能（提供機能）には、例えば、特定の利用者のみに情報を提供するものがある。しかし、悪意を持った第三者（攻撃者）は、この提供機能に対して不正な操作などを行う（攻撃）ことによって、本来手に入れることのできない情報を入手することがある。

【００１４】

そのため、攻撃者から提供機能を守るためには、提供機能を守る機能（セキュリティ機能）が必要である。システム設計時には、そのセキュリティ機能をどこにどのように配置するかを設計すること（セキュリティ機能設計）が必要である。

【００１５】
セキュリティ機能設計においては、まず守るべき情報資産を決める。例えば、特定のユーザに提供する情報が情報資産として挙げられる。
次に、この情報資産を守るために必要なセキュリティ機能を検討する必要がある。例えば、特定のユーザを認証できるようにすること（主体認証）が挙げられる。
【００１６】
次に、このセキュリティ機能を実現するために必要なソフトウェアなどの方式（セキュリティ実現方式）を選定する。例えば、ユーザを識別するための識別符号であるＩＤと、ユーザしか知りえないパスワードを用いた認証方式（ＩＤ／ＰＷ認証）を選定することができる。
【００１７】
次に、このセキュリティ実現方式そのものが攻撃者によって攻撃を受ける可能性があるため、セキュリティ実現方式を保護するための機能（付随機能要素）も必要となる。例えば、上述のＩＤ／ＰＷ認証では、通信経路上をＩＤとＰＷが行き来するため、付随機能として通信路の暗号化が必要である。ただし、付随機能はシステム構成によっては必須ではない。例えば、通信機能を一切持たないコンピュータシステムでは、通信路の暗号化機能は不要となる。このように、セキュリティ機能設計においては、システム構成によって変化する付随機能要素を過不足なく適切に設定する必要がある。
【００１８】
（セキュリティ機能設計支援装置の構成）
以下、本発明の実施の形態によるセキュリティ機能設計支援装置の構成について説明する。
図１は、本発明の実施の形態によるセキュリティ機能設計支援装置１００の構成を示すブロック図である。図に示すように、セキュリティ機能設計支援装置１００は、システム構成データ表示部１１１、実現方式設定支援部１１２、付随機能要素設定支援部１１３、付随機能要素評価部１１４、評価結果出力部１１５、システム構成データ記憶部３０１、実現方式記憶部３０２、付随機能要素記憶部３０３、付随機能要素定義記憶部３０４、表示装置１３０、入力装置１４０を備えている。
【００１９】
セキュリティ機能設計支援装置１００は、ＣＰＵ、ＲＯＭやＲＡＭ等のメモリ、各種の情報を格納する外部記憶装置、入力インタフェース、出力インタフェース、通信インタフェース及びこれらを結ぶバスを備える専用又は汎用のコンピュータを適用することができる。なお、セキュリティ機能設計支援装置１００は、単一のコンピュータにより構成されるものであっても、通信回線を介して互いに接続された複数のコンピュータにより構成されるものであってもよい。
【００２０】
システム構成データ表示部１１１、実現方式設定支援部１１２、付随機能要素設定支援部１１３、付随機能要素評価部１１４、評価結果出力部１１５は、ＣＰＵがＲＯＭ等に格納された所定のプログラムを実行することにより実現される機能のモジュールに相当する。システム構成データ記憶部３０１、実現方式記憶部３０２、付随機能要素記憶部３０３、付随機能要素定義記憶部３０４は外部記憶装置により実装される。外部記憶装置は、セキュリティ機能設計支援装置１００とネットワーク等を介して接続されていてもよい。
【００２１】
表示装置１３０は、ディスプレイ等の表示装置であり、セキュリティ機能設計支援装置１００のＣＰＵから出力される画像信号を受けて、各種画像を表示するものである。
【００２２】
入力装置１４０は、マウスやキーボード等を含む各種デバイスであり、ユーザがセキュリティ機能設計支援装置１００に対して各種情報の入力を行う際に使用される。
【００２３】
システム構成データ記憶部３０１は、システムの構成の情報を記憶する。図２は、シス

テム構成データ記憶部３０１に記憶されるシステム構成データの例を示す図である。図２に示すように、システム構成データは、構成要素名４０１と接続先４０２をデータ項目として含んでいる。構成要素名４０１は、セキュリティ機能設計の対象となるシステムを構成する構成要素の名称である。接続先４０２は、それぞれの構成要素と通信回線を介して接続された構成要素を表している。

【００２４】

図２の例におけるシステムは、３つの構成要素（クライアント、ＷＷＷ／ＡＰサーバ、ＤＢサーバ）によって構成され、クライアントとＷＷＷ／ＡＰサーバ、ＷＷＷ／ＡＰサーバとＤＢサーバにそれぞれ無方向の接続関係がある。このシステムのシステム構成データは、図２に示すように、構成要素名４０１として（クライアント、ＷＷＷ／ＡＰサーバ、ＤＢサーバ）が設けられ、それぞれの構成要素の接続先４０２が記録される。この例では、クライアントとＤＢサーバはＷＷＷ／ＡＰサーバを介して接続されていることが分かる。

【００２５】

実現方式記憶部３０２は、システムの構成要素に対して設定されたセキュリティ機能を実現するためのセキュリティ実現方式のデータを記憶する。図３は、実現方式記憶部３０２に記憶されるデータの例を示す図である。図３に示すように、実現方式記憶部３０２は、構成要素名４１１、採用した実現方式名４１２、実現方式が取り扱う保護資産４２０、実現方式が取り扱う保護資産の送信元４１３、実現方式が取り扱う保護資産の受信先４１４を含むテーブル４１５を含んでいる。

【００２６】

テーブル４１５は階層構造を持つことができる。例えば、あるセキュリティ実現方式を保護するための付随機能要素が、他のセキュリティ実現方式によって実現されている場合は、テーブル４１５のレコード４１８を親としてテーブル４１６を作成し、その親のレコード４１８からテーブル４１６を辿れるようにリンク構造４１７を設ける。

【００２７】

図３の例では、ＷＷＷ／ＡＰサーバにおいて、ＩＤ／ＰＷ認証というセキュリティ実現方式を採用している。さらに、ＩＤ／ＰＷ認証で取り扱う保護資産はＩＤ／ＰＷであり、保護資産の送信元はクライアントであり、保護資産の受信先はＷＷＷ／ＡＰサーバである（テーブル４１５）。また、ＩＤ／ＰＷ認証の付随機能要素を実現するセキュリティ実現方式がＳＳＬであり、ＳＳＬが取り扱う保護資産の送信元がクライアントで、その保護資産の受信先がＷＷＷ／ＡＰサーバである（テーブル４１６）。また、親レコード４１８からテーブル４１６が辿れるようにリンク構造４１７が設定されている。

【００２８】

付随機能要素記憶部３０３は、システムの構成要素に対して設定され、セキュリティ実現方式の機能を保護するために設定された付随機能要素のデータを記憶する。図４は、付随機能要素記憶部３０３に記憶されるデータの例を示す図である。図４に示すように、付随機能要素記憶部３０３は、構成要素名４２１、構成要素に対して配置されたセキュリティ機能の実現方式名４２２、付随機能要素名４２３、その付随機能要素を実現するためのセキュリティ機能の実現方式（副実現方式）４２４を含むテーブル４２５を含んでいる。

【００２９】

テーブル４２５は階層構造を持つことができる。例えば、一つの付随機能要素が他のセキュリティ実現方式によって実現されている場合は、テーブル４２５の該当するレコード４２９を親としてテーブル４２６を作成し、親レコード４２９から子テーブル４２６が辿れるようにリンク構造４２７を設定する。

【００３０】

図４の例では、ＷＷＷ／ＡＰサーバに対し、セキュリティ実現方式としてＩＤ／ＰＷ認証が採用されている。ＩＤ／ＰＷ認証に対し、付随機能要素である「機能主体」および「通信路暗号化」が配置されている（テーブル４２５）。また、通信路暗号化は、他のセキュリティ実現方式「ＳＳＬ」によって実現されるため、副実現方式４２４としてＳＳＬが

登録されている。さらに、レコード４２９を親として、子テーブル４２６にリンク構造４２７が設定されている。テーブル４２６には、セキュリティ実現方式「ＳＳＬ」の付随機能要素に関する情報が格納されている。

【００３１】

付随機能要素定義記憶部３０４は、あるセキュリティ実現方式の機能を保護するための付随機能要素の情報を記憶する。図５は、付随機能要素定義記憶部３０４に記憶されるデータの例を示す図である。図５に示すように、付随機能要素定義記憶部３０４は、セキュリティ実現方式名４３１、セキュリティ実現方式を保護するための付随機能要素名４３２、その付随機能要素が取り扱う保護資産名（取扱い資産）４３３、付随機能要素の合否を判定するための判定ルール４３４、付随機能要素を実現するための他のセキュリティ実現方式があるか否かを示す情報（副実現方式）４３５を含むテーブル４３６を含んでいる。判定ルール４３４には、副テーブル４３９がリンクしている。副テーブル４３９は、判定ルールインデックス４３７、合格条件４３８を含んでおり、判定ルール４３４から副テーブル４３９が辿れるようにリンク構造４４０が設定されている。

【００３２】

図５の例では、例えばＩＤ／ＰＷ認証の場合、機能主体と通信路暗号化の２つが付随機能として定義されている。機能主体のレコード４４２を見ると、取扱い資産４３３は機能主体である。これは、セキュリティ実現方式であるＩＤ／ＰＷ認証の機能そのものを意味している。なお、取扱い資産４３３が「指定」の場合は、実現方式記憶部３０２で指定されている保護資産が充てられる。また、判定ルールについては、例えば「１」とされている場合には、リンク構造４４０を辿り、副テーブル４３９の中の判定ルールインデックス４３７が「１」を含むレコードを参照する。図５の例では、「システム構成上に配置されて、システム構成に矛盾が無い」が判定ルールとなる。副実現方式４３５については、「ある」の場合は付随機能が他の実現方式によって実現されることを示し、「ない」の場合は他の実現方式によって実現されるものではないことを示す。

【００３３】

（セキュリティ機能設計支援装置の動作）

次に、本発明の実施の形態によるセキュリティ機能設計支援装置の動作について説明する。

【００３４】

ここで、システム構成データ記憶部３０１には、対象となるシステムのシステム構成データが記憶されている。また、付随機能要素定義記憶部３０４には、各種のセキュリティ規定に基づいて定められた付随機能要素の定義情報が記憶されている。

【００３５】

図６は、実施の形態１によるセキュリティ機能設計支援装置１００の動作のフローチャートである。また、図７～１７は、表示装置１３０に表示される画面の例を示す図である。

【００３６】

まず、システム構成データ表示部１１１が、システム構成データ記憶部３０１を参照し、システム構成を表示装置１３０に表示する（ステップＳ１１）。

【００３７】

次に、実現方式設定支援部１１２が、ユーザが入力装置１４０を用いて行った操作に基づいて、システムの構成要素に対し実現方式を配置する（ステップＳ１２）。配置された実現方式は実現方式記憶部３０２に登録される。

【００３８】

図７は、ステップＳ１１、Ｓ１２における表示装置１３０の画面の例を示している。図に示すように、画面にはシステムの構成要素であるクライアント（Ａ）、ＷＷＷ／ＡＰサーバ（Ｂ）、ＤＢサーバ（Ｃ）が表示される。また、各々の構成要素間の接続関係が矢印で示されている。

【００３９】

ユーザは、実現方式の一覧が表示されたリスト（Ｐ）から、入力装置１４０を用いて所望の実現方式（方式１）を指定し、ドラッグアンドドロップを行う。この操作により、図７に示すように方式１がＷＷＷ／ＡＰサーバに配置される。

【００４０】

次に、実現方式設定支援部１１２は、ユーザが入力装置１４０を用いて行った操作に基づいて、ステップＳ１３で配置した実現方式における保護資産、保護資産の送信元および受信先を設定する（ステップＳ１３）。設定された保護資産、保護資産の送信元および受信先は実現方式記憶部３０２に登録される。

【００４１】

図８は、ステップＳ１３における表示装置１３０の画面の例を示している。ユーザは、保護資産、保護資産の送信元、受信先の一覧が表示されるリストボックスから、入力装置１４０を用いて所望の保護資産、送信元および受信先を選択する。各々の選択肢は、システム構成データ記憶部３０１の内容に基づいて提示されるようにしてもよい。

【００４２】

次に、実現方式設定支援部１１２は、ステップＳ１３で設定された情報に基づいて、保護資産（情報）の構成要素間での流れを表示装置１３０に表示する（ステップＳ１４）。

【００４３】

図９は、ステップＳ１４における表示装置１３０の画面の例を示している。図９に示すように、ユーザが指定した「資産１」がクライアントからＷＷＷ／ＡＰサーバに送信されることが点線の矢印で示されている。

【００４４】

次に、付随機能要素設定支援部１１３は、付随機能要素定義記憶部３０４を参照し、付随機能要素の候補を表示装置１３０に表示する（ステップＳ１５）。

【００４５】

図１０は、ステップＳ１５における表示装置１３０の画面の例を示している。図に示すように、付随機能要素の候補Ｆ１～Ｆ８が表示される。付随機能要素の候補の数が多い場合は、入力装置１４０の操作に基づいて特定の要素（図９ではＦ４とＦ５）が大きく表示されるようにしてもよい。例えばマウスのホイールを回すことにより大きく表示される要素が変化するようにしてもよい。

【００４６】

次に、付随機能要素設定支援部１１３は、ユーザが入力装置１４０を用いて行った操作に基づいて、付随機能要素を設定する（ステップＳ１６）。

【００４７】

図１１，１２は、ステップＳ１６における表示装置１３０の画面の例を示している。ユーザが入力装置１４０を用いて特定の付随機能要素（Ｆ４）を選択すると、その付随機能要素を配置するかしないかを選択させるダイアログが表示される（図１１）。ユーザが「配置しない」を選択するとその付随機能要素は小さく表示される（図１２）。「配置する」が選択された場合には、実現方式記憶部３０２および付随機能要素記憶部３０３に選択された付随機能要素が登録される。

【００４８】

次に、付随機能要素設定支援部１１３は、付随機能要素定義記憶部３０４を参照し、ステップＳ１６で選択された付随機能要素を実現するための他の実現方式（副実現方式）があるか否かを判定する（ステップＳ１７）。

【００４９】

副実現方式が無い場合は（ＮＯ）、ステップＳ１８に移行し、付随機能要素評価部１１４が設定された付随機能要素の妥当性を評価する。付随機能要素の評価処理については後述する。評価処理が終了したらステップＳ１９へ移行し、評価結果出力部１１５が評価結果を出力する。結果が合格の場合は図１３に示すように、設定した付随機能要素が合格であることが表示される。

【００５０】

ステップＳ１７において副実現方式があると判定された場合は（ＹＥＳ）、ステップＳ２０へ移行する。ステップＳ２０では、実現方式設定支援部１１２は、図１４に示すように副実現方式の選択肢をリストボックス等で表示する。

【００５１】

次に、ステップＳ２１において、実現方式設定支援部１１２は副実現方式を設定する。図１５に示すように、ユーザによって副実現方式（実現方式２）を選択すると、「方式２」がＷＷＷ／ＡＰサーバに配置される。また、「方式１」との親子関係（方式１が親で方式２が子）が矢印で表示される。副実現方式が選択されると、実現方式記憶部３０２および付随機能要素記憶部の情報が更新される。

【００５２】

次に、ステップＳ２２において、付随機能要素設定支援部１１３は、ステップＳ２１で設定された副実現方式に対する付随機能要素の候補を表示装置１３０に表示する（図１６）。

【００５３】

次に、ステップＳ２３において、付随機能要素設定支援部１１３は、ユーザが入力装置１４０を用いて行った操作に基づいて、付随機能要素を設定する。図１７に示すように、ユーザが入力装置１４０を用いて特定の付随機能要素（Ｆ１４）を選択すると、その付随機能要素を配置するかしないかを選択させるダイアログが表示される。ユーザが「配置しない」を選択するとその付随機能要素は小さく表示され、「配置する」を選択すると、実現方式記憶部３０２および付随機能要素記憶部３０３が更新される。以降、ステップＳ１７へ戻って処理が繰り返される。

【００５４】

次に、付随機能要素評価部１１４による付随機能要素の評価について、図１８，１９のフローチャートを用いて詳しく説明する。ここでは、ステップＳ１２～Ｓ２３の処理によって、実現方式記憶部３０２と付随機能要素記憶部３０３には、図３，４に示す内容のデータが登録されたものとして説明する。

【００５５】

まず、付随機能要素評価部１１４は、実現方式記憶部３０２より、未検証の実現方式を１つ取得する（ステップＳ１００１）。具体的には、図３に示すテーブル４１５から、未検証のレコード４１８（以下、構成要素に対して採用した実現方式レコードと記す。）を選択する。

【００５６】

次に、付随機能要素評価部１１４は、付随機能要素定義記憶部３０４から、ステップＳ１００１で選択した実現方式の付随機能要素の定義レコードを取得する（ステップＳ１００２）。例えば、ステップＳ１００１で取得したレコードの採用した実現方式名４１２が「ＩＤ／ＰＷ認証」だった場合には、図５に示すテーブル４３６から、実現方式名４３１が「ＩＤ／ＰＷ認証」であるレコード群４４１（以下、付随機能要素定義レコード群と記す。）を取得する。

【００５７】

次に、付随機能要素評価部１１４は、付随機能要素記憶部３０３のテーブル４２５から、ステップＳ１００１で取得したレコードの採用した実現方式名４１２と実現方式名４２２の内容が同一のレコード群（以下、配置された付随機能要素レコード群と記す。）を取得する（ステップＳ１００３）。具体的には、ステップＳ１００１で取得したレコードの採用した実現方式名４１２が「ＩＤ／ＰＷ認証」だった場合には、図４に示すレコード群４３０が取得される。

【００５８】

次に、ステップＳ１００２とステップＳ１００３で取得したデータを基に、付随機能要素評価部１１４は付随機能要素の評価を行う（ステップＳ１００４）。

【００５９】

ステップＳ１００４の処理について図１９のフローチャートを用いて詳しく説明する。

まず、付随機能要素評価部１１４は、図６のステップＳ１００２で取得した付随機能要素定義レコード群の中から、レコード（以下、評価対象付随機能要素レコードと記す。）を１つ取得する（ステップＳ１１０１）。

【００６０】

次に、ステップＳ１００３で取得した配置された付随機能要素レコード群の中に、実現方式名４２２と付随機能要素名４２３が、ステップＳ１１０１で取得した評価対象付随機能要素レコードの実現方式名４３１および付随機能要素名４３２と一致するレコード（以下、配置済み付随機能要素レコードと記す。）が存在するか否かを判定する（ステップ１１０２）。配置済み付随機能要素レコードが存在する場合はステップＳ１１０３に移行し、存在しない場合はステップＳ１１０８に移行する。

【００６１】

図４、５を用いて具体的に説明する。ステップＳ１１０１において、評価対象付随機能要素レコード４４２が選択される。レコード４４２の実現方式名４３１は「ＩＤ／ＰＷ認証」であり、付随機能要素名４３２は「機能主体」である。これと同じ内容の実現方式名４２２と付随機能要素名４２３を持つレコードを、ステップＳ１００３で取得した配置された付随機能要素レコード群の中から取得する。図４の例ではレコード４２８が該当する。したがって、レコード４２８が配置済み付随機能要素レコードとなる。

【００６２】

ステップＳ１１０３では、ステップＳ１１０１で取得した評価対象付随機能要素レコードの判定ルール４３４に基づいてリンク構造４４０を辿り、テーブル４３９から合格条件が記述された１つ以上のレコード（以下、判定ルールレコード群と記す。）を取得する。

【００６３】

図５を用いて具体的に説明する。ステップＳ１１０１で取得されたレコード４４２の判定ルール４３４は「１」である。評価結果出力部１１５は、リンク構造４４０を辿って、テーブル４３９の中から判定ルールインデックス４３７が判定ルール４３４とおなじ内容のレコード４４５を取得する。付随機能要素評価部１１４は、レコード４４５の合格条件４３８の内容「システム構成上に配置されて、システム構成に矛盾が無い」を判定ルールとして取得する。

【００６４】

次に、付随機能要素評価部１１４は、ステップＳ１１０３で取得した判定ルールに基づいて、付随機能要素の合否判定を行う。判定ルールが複数ある場合は、全ての判定ルールについて評価を行う（ステップＳ１１０４）。

【００６５】

付随機能要素の合否判定について、図４、５を用いて具体的に説明する。ステップＳ１１０１では評価対象付随機能要素レコード４４２が取得され、ステップＳ１１０２では配置済み付随機能要素レコード４２８が取得される。また、ステップＳ１１０３では判定ルールレコード群としてレコード４４５が取得される。この結果、判定ルールは１つのみで、「システム構成上に配置されて、システム構成に矛盾が無い」である。

【００６６】

「システム構成上に配置されて、システム構成に矛盾が無い」とは、配置済み付随機能要素レコードが存在し、ステップＳ１００１で取得したレコードの構成要素名４１１が、システム構成データ記憶部３０１の構成要素名４０１に存在し、且つ、保護資産の送信元４１３と保護資産の受信先４１４が通信可能であれば合格という意味である。

【００６７】

ここで、配置済み付随機能要素レコード４２８の構成要素名４２１は「ＷＷＷ／ＡＰサーバ」である。図２のシステム構成データ記憶部３０１を参照すると、構成要素名４０１が「ＷＷＷ／ＡＰサーバ」のレコードが存在する。また、図２より「クライアント」と「ＷＷＷ／ＡＰサーバ」は接続されているため通信可能である。

【００６８】

また、ステップＳ１１０１で評価対象付随機能要素レコード４４３が取得された場合に

は、ステップＳ１１０２では配置済み付随機能要素レコード４２９が取得される。そして、レコード４４３の判定ルール４３４は「２，３，４，５」であるため、ステップＳ１１０３では判定ルールとして「副実現方式が選択されている」、「実現方式と同じ構成要素に配置されている」、「副実現方式の取り扱い保護資産、送信元、受信先が同じである」、「副実現方式が合格している」が取得される。

【００６９】

付随機能要素評価部１１４は、それぞれの判定ルールに基づいて評価を行う。まず、「副実現方式が選択されている」の評価について説明する。レコード４２９の副実現方式４２４にはＳＳＬが設定されている。この場合、構成要素に対して採用した実現方式レコード４１８から子テーブル４１６へのリンク構造４１７を辿る。子テーブル４１６に、採用した実現方式名４１２が「ＳＳＬ」のレコード（以下、副実現方式レコードと記す。）が存在している場合は合格とする。

【００７０】

次に、「実現方式と同じ構成要素に配置されている」の評価について説明する。ステップ１００１で取得した「構成要素が採用した実現方式レコード（４１８）」からから子テーブル４１６へのリンク構造４１７を辿る。「配置済み付随機能要素レコード（４２９）」の副実現方式４２４と同一の実現方式名４２２を持つレコードが、子テーブル４１６に存在する場合は合格と判断する。

【００７１】

次に、「副実現方式の取り扱い保護資産、送信元、受信先が同じである」の評価について説明する。まず、「評価対象付随機能要素レコード（４４３）」の取扱い資産４３３が「指定」となっている場合、「構成要素が採用した実現方式レコード（４１８）」の取扱い保護資産４２０に記述された保護資産と同値とする。例えば、この値が「ＩＤ／ＰＷ」の場合は、「副実現方式レコード（４１９）」の実現方式名４１２が「ＩＤ／ＰＷ」であり、「副実現方式レコード（４１９）」の保護資産の送信元４１３と保護資産の受信先４１４が、「構成要素が採用した実現方式レコード（４１８）」の保護資産の送信元４１３と保護資産の受信先４１４と同じであれば合格と判断する。

【００７２】

次に、「副実現方式が合格している」の評価について説明する。検証する実現方式をＳＳＬとしてステップＳ１００１から動作を実行し、その結果が合格と判定されれば合格となる。

なお、判定ルールは図５に記載されているものに限られない。

【００７３】

ステップＳ１１０５では、ステップＳ１００２で取得した「付随機能要素定義レコード群」の中に未評価の付随機能要素がある場合は、ステップＳ１１０１へ移行する。未評価の付随機能要素がない場合は、ステップＳ１１０６へ移行する。

【００７４】

ステップＳ１１０６では、全ての付随機能要素についての評価が合格だった場合はステップＳ１１０７へ移行し、不合格の付随機能要素がある場合はステップＳ１１０８へ移行する。

【００７５】

ステップＳ１１０７では、本実現方式についての付随機能要素の設計が妥当であると判断して処理を終了する（ステップＳ１１０７）。

ステップＳ１１０８では、本実現方式についての付随機能要素の設計が妥当でないと判断して処理を終了する（ステップＳ１１０８）。

【００７６】

図１８のステップＳ１００５に戻り、未検証の実現方式がある場合は再びステップＳ１００１に戻る。全ての実現方式の検証が終わった場合はステップＳ１００６に移行する。

【００７７】

ステップＳ１００６では、付随機能要素評価部１１４が、実現方式記憶部３０２に記述

されている実現方式毎に評価結果を出力する。
以上で、付随機能要素評価部１１４による付随機能要素の評価処理が終了する。
【００７８】
なお、ステップＳ１９の評価結果出力については、例えば、全ての付随機能要素が合格と判定された場合には、親子関係にある実現方式全体を特定の色（緑色等）で表示するようにしてもよい。これにより、ユーザは、そのセキュリティ機能を実現させるための実現方式全体が正しく設定されていることが分かる。また、不合格の付随機能要素がある場合には他の色（赤色等）で表示する。
【００７９】
また、設定途中でユーザに誤った選択操作を警告するようにしてもよい。例えば、図１２（ステップＳ１６）において、必須の付随機能要素であるにもかかわらず、ユーザが配置しないを選択した場合には、特定の色（黄色等）でその付随機能要素や対象となる構成要素を表示するようにしてもよい。
【００８０】
また、図１６（ステップＳ２２）において、子の実現方式が配置された段階で、親の実現方式についても設定が不十分であることが確定するため、このタイミングで親子関係にある実現方式全体を不合格の色（赤色等）で表示するようにしてもよい。これにより、セキュリティ機能の設定において、具体的にどの付随機能要素に問題があるのかが明確になり、ユーザが対応しやすくなる。
【００８１】
以上のように、本実施形態によれば、実現方式設定支援部１１２および付随機能要素設定支援部１１３によって、ユーザがセキュリティ機能設計を視覚的に行えるようにすると共に、付随機能要素評価部１１４が、ユーザが設定した付随機能要素の妥当性を判定し、ユーザが判定結果を視覚的に確認できるようにした。
これにより、ユーザは、具体的にどの付随機能要素の設定に問題があるのか把握できるので、セキュリティ機能設計を効率的に行うことができる。
【００８２】
（変形例）
なお、各々の実現方式にかかるコストを予め登録しておき、図２０に示すように、配置した実現方式毎にコストを表示するようにしてもよい。図２０の例では、円グラフを用いて、全ての必要な付随機能要素を配置した場合を１００％とし、既に配置済みの付随機能要素の割合を視覚的に表示している。このように表示することにより、ユーザは付随機能要素がどれぐらい不足しているか把握することができる。また、グラフをクリックすると、不足している付随機能要素名が表示されるようにしてもよい。
【００８３】
この出願は、２０１２年１０月１０日に出願された日本出願特願２０１２－２２８０７４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。
【００８４】
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様々な変更をすることができる。
【産業上の利用可能性】
【００８５】
本発明は、例えばシステム開発の設計時におけるセキュリティ機能設計に適用できる。
【００８６】
上記の実施の形態の一部または全部は、以下の付記のようにも記載されうるが、以下には限られない。
（付記１）システムの構成を表示装置に表示するシステム構成データ表示部と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリ

ティ実現方式を、ユーザの操作によって選択された構成要素に設定する実現方式設定支援部と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する付随機能要素設定支援部と、
ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する付随機能要素評価部と、
前記付随機能要素評価部による判定の結果を出力する評価結果出力部と、を含むセキュリティ機能設計支援装置。
【００８７】
（付記２）前記付随機能要素評価部は、
ユーザ操作によって設定された前記付随機能要素のデータを取得し、
前記妥当性を判定するための条件に基づいて、システム構成データおよびユーザ操作によって設定された前記セキュリティ実現方式の情報を参照しながら付随機能要素の妥当性を判定する、付記１に記載のセキュリティ機能設計支援装置。
【００８８】
（付記３）前記評価結果出力部は、
ユーザが必須の付随機能要素を設定しなかった場合には、必須要素であることを知らせる画像を表示する、付記１または２に記載のセキュリティ機能設計支援装置。
【００８９】
（付記４）前記評価結果出力部は、
ある付随機能要素を機能させるために必要な副実現方式が設定されていない場合には、その付随機能要素が設定されている実現方式を含めて不合格であることを知らせる画像を表示する、付記１から３のいずれか１項に記載のセキュリティ機能設計支援装置。
【００９０】
（付記５）前記評価結果出力部は、
設定された各々の実現方式にかかるコストの情報を表示する、付記１から４のいずれか１項に記載のセキュリティ機能設計支援装置。
【００９１】
（付記６）システムの構成を表示装置に表示する工程と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する工程と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付随機能要素を、ユーザの操作によって選択された構成要素に設定する工程と、
ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する工程と、
前記判定の結果を出力する工程と、を含むセキュリティ機能設計支援方法。
【００９２】
（付記７）コンピュータを、
システムの構成を表示装置に表示するシステム構成データ表示部と、
セキュリティ機能を実現するために、前記システムの構成要素に対して設定可能なセキュリティ実現方式の候補を提示するとともに、ユーザの操作によって選択されたセキュリティ実現方式を、ユーザの操作によって選択された構成要素に設定する実現方式設定支援部と、
前記セキュリティ実現方式の機能を保護するために、前記システムの構成要素に対して設定可能な付随機能要素の候補を提示するとともに、ユーザの操作によって選択された付

随機能要素を、ユーザの操作によって選択された構成要素に設定する付随機能要素設定支援部と、

ある付随機能要素の設定の妥当性を判定するための条件に基づいて、前記システムの構成要素に対して設定された付随機能要素が妥当であるか否かを判定する付随機能要素評価部と、

前記付随機能要素評価部による判定の結果を出力する評価結果出力部と、

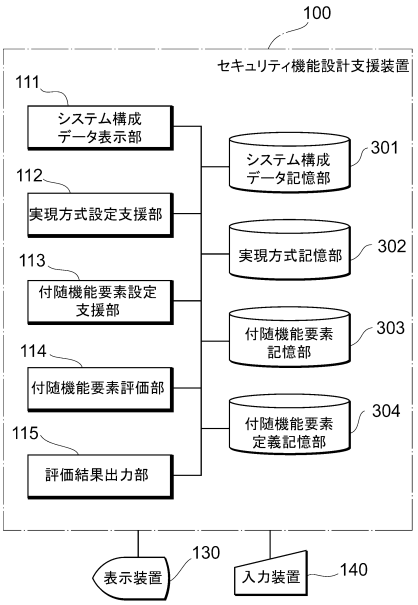
して機能させるプログラム。

【符号の説明】

【００９３】

１００　セキュリティ機能設計支援装置
１１１　システム構成データ表示部
１１２　実現方式設定支援部
１１３　付随機能要素設定支援部
１１４　付随機能要素評価部
１１５　評価結果出力部
１３０　表示装置
１４０　入力装置
３０１　システム構成データ記憶部
３０２　実現方式記憶部
３０３　付随機能要素記憶部
３０４，付随機能要素定義記憶部
４０１，４１１，４２１　構成要素名
４０２　接続先
４１２　採用した実現方式名
４２０　取扱い保護資産
４１３　保護資産の送信元
４１４　保護資産の受信先
４１５，４１６，４２５，４２６，４３６　テーブル
４１７，４２７，４４０　リンク構造
４１８，４１９，４２８，４２９，４４２，４４３，４４４，４４５　レコード
４２２，４３１　実現方式名
４２３，４３２　付随機能要素名
４２４，４３５　副実現方式
４３０，４４１　レコード群
４３３　取扱い資産
４３４　判定ルール
４３７　判定ルールインデックス
４３８　合格条件
４３９　副テーブル

【図１】

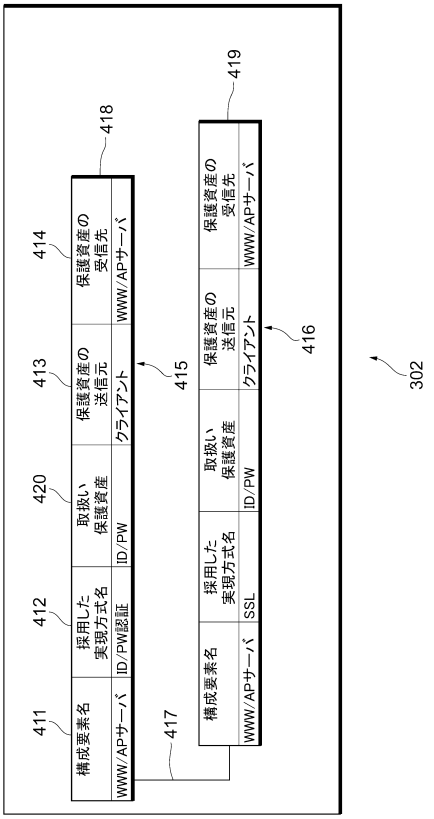


【図２】

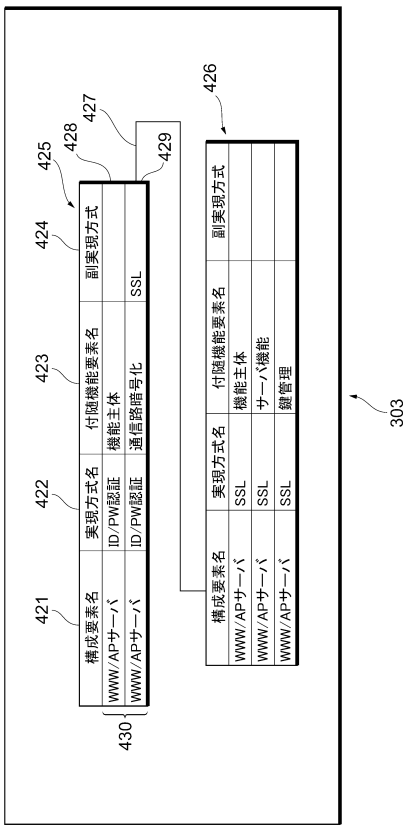
401　402　301

構成要素名	接続先
クライアント	WWW/APサーバ
WWW/APサーバ	クライアント
WWW/APサーバ	DBサーバ
DBサーバ	WWW/APサーバ

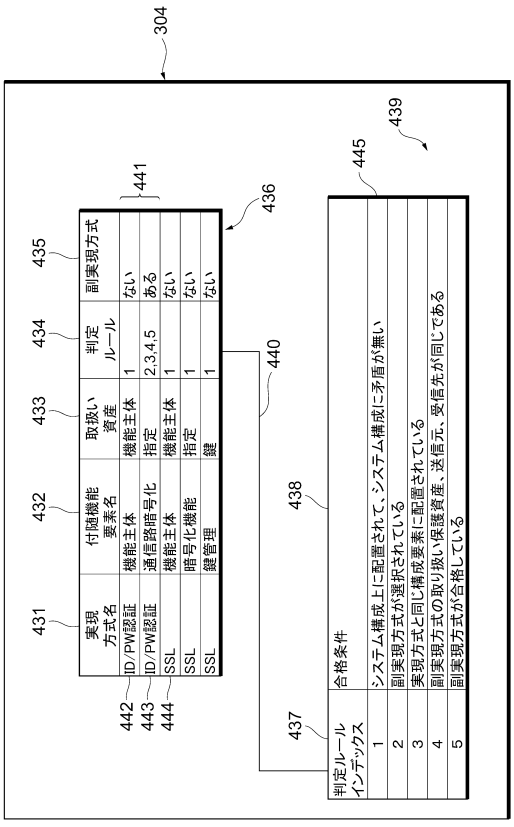
【図３】



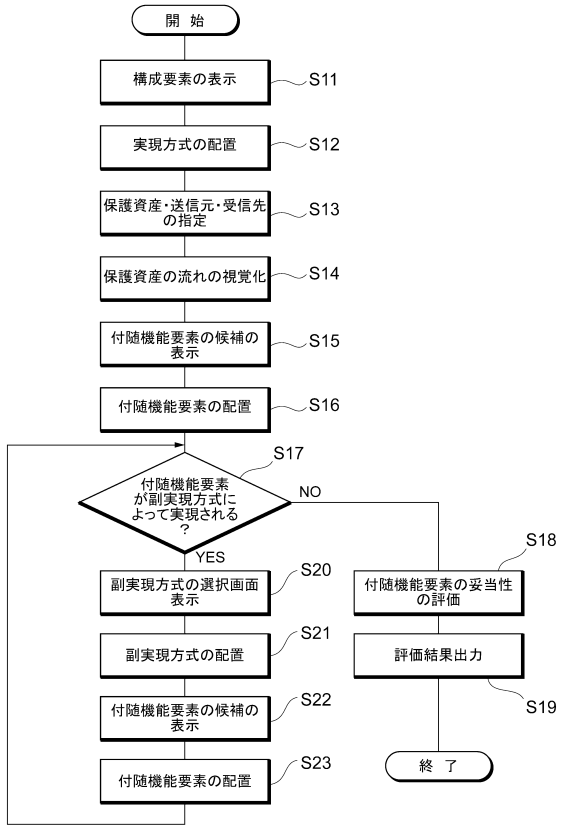
【図４】



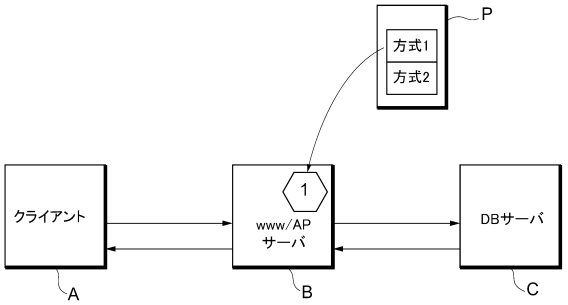
【図５】



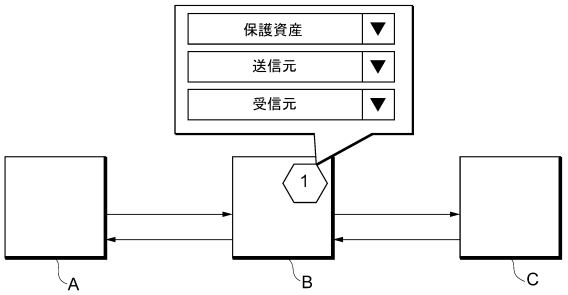
【図６】



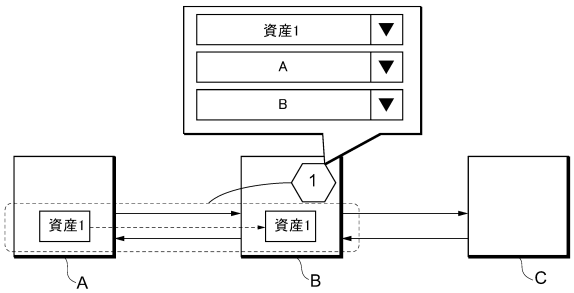
【図７】



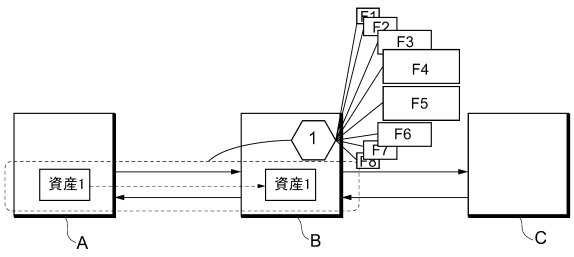
【図８】



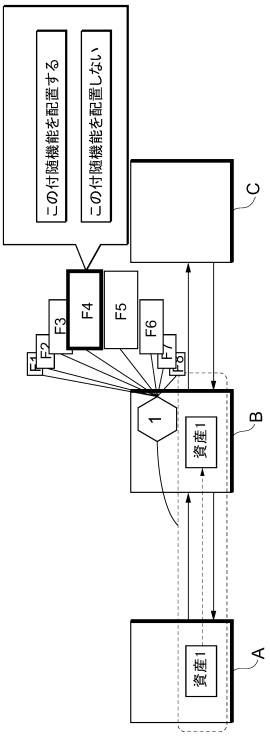
【図９】



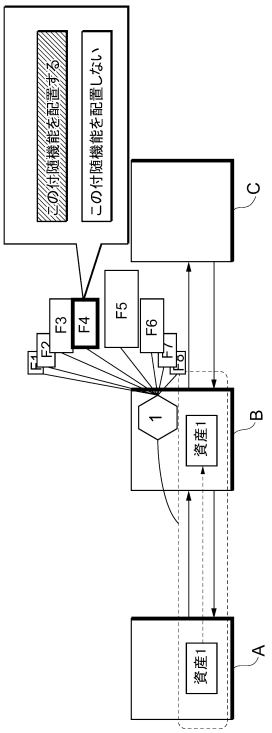
【図１０】



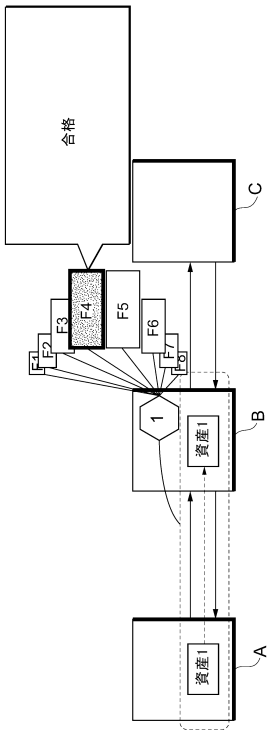
【図１１】



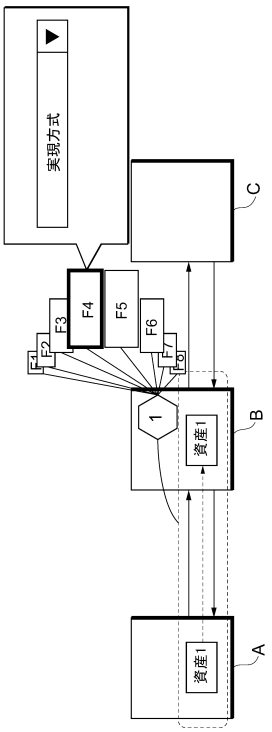
【図１２】



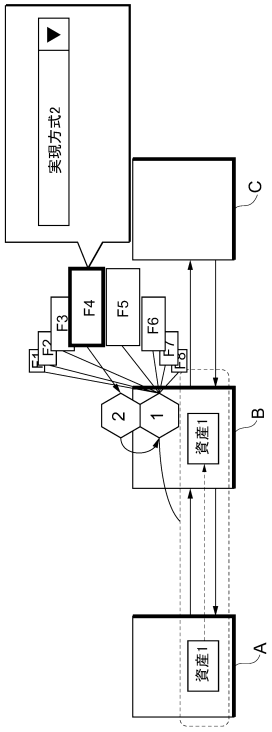
【図１３】



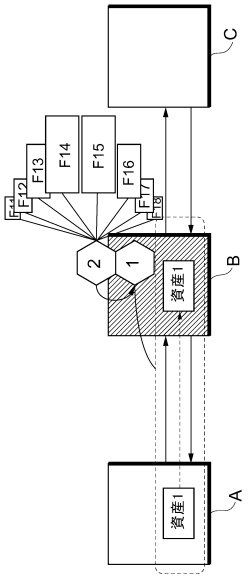
【図１４】



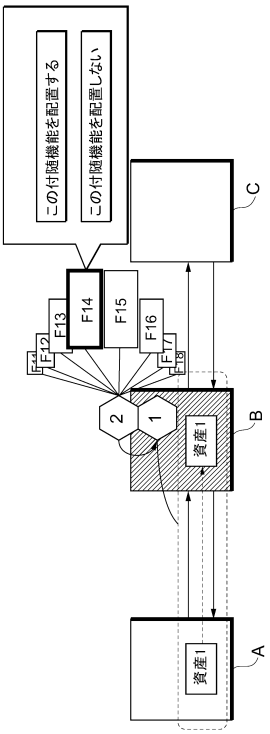
【図１５】



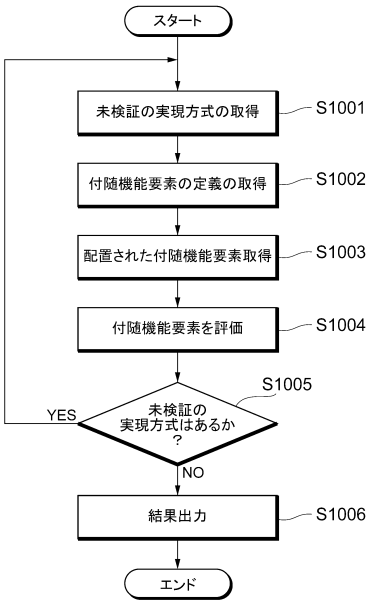
【図１６】



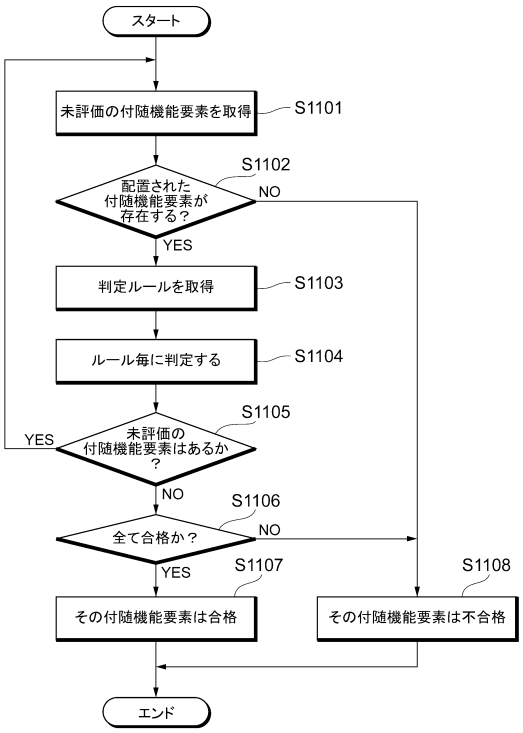
【図１７】



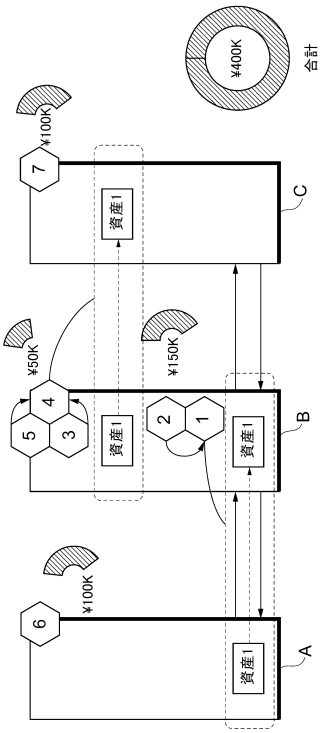
【図１８】



【図１９】



【図２０】



フロントページの続き

(56)参考文献 特開２０１１－１９７７９９（ＪＰ，Ａ）
特開２０１２－０３８１０８（ＪＰ，Ａ）
特開２００６－３５０３９９（ＪＰ，Ａ）
特開２０１１－２３２８７４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７