(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3872689号
(P3872689)
(45)発行日　平成19年1月24日(2007.1.24)　(24)登録日　平成18年10月27日(2006.10.27)

(51)Int.Cl.　　F I
G06Q 10/00 (2006.01)　　G06F 17/60　174
G06F 21/20 (2006.01)　　G06F 15/00　330A

請求項の数 18　(全 23 頁)

(21)出願番号　特願2001-398244(P2001-398244)
(22)出願日　平成13年12月27日(2001.12.27)
(65)公開番号　特開2003-196476(P2003-196476A)
(43)公開日　平成15年7月11日(2003.7.11)
審査請求日　平成15年10月23日(2003.10.23)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100084032
弁理士　三品　岩男
(72)発明者　藤山　達也
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内
(72)発明者　永井　康彦
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】セキュリティポリシーの作成支援システムおよびセキュリティ対策決定支援システム

(57)【特許請求の範囲】
【請求項１】
情報資産毎に、該情報資産を識別するための資産ＩＤ、を有する資産要素からなる第一の要素データと、
前記情報資産が曝される脅威毎に、該脅威を識別するための脅威ＩＤ、該脅威の内容を示す攻撃方法、および、該脅威による損失額を単位時間当たりの割合で特定した基準リスク、を有する脅威要素からなる第二の要素データと、
前記脅威への対策毎に、該対策を識別するための対策ＩＤ、該対策の具体的な内容を示す対策の内容、該対策に要するコスト額を単位時間当たりの割合で特定した基準コスト、および、該対策による前記基準リスクの削減額を単位時間当たりの割合で特定した基準削減効果、を有する対策要素からなる第三の要素データと、
資産ＩＤ、および、該資産ＩＤにより特定される情報資産に関連するキーワードを識別するためのキーワードＩＤ、を該資産ＩＤ毎に有する資産要素実績からなる第一の要素実績データと、
脅威ＩＤ、および、該脅威ＩＤにより特定される脅威に関連するキーワードを識別するためのキーワードＩＤ、を該脅威ＩＤ毎に有する脅威要素実績からなる第二の要素実績データと、
対策ＩＤ、および、該対策ＩＤにより特定される対策に関連するキーワードを識別するためのキーワードＩＤ、を該対策ＩＤ毎に有する対策要素実績からなる第三の要素実績データと、

キーワード、および、該キーワードを識別するためのキーワードＩＤ、を該キーワード毎に有するキーワードデータと、
を記憶する記憶部、制御部、表示部、および、入力部、を備えるセキュリティポリシーの作成支援システムであって、
前記制御部は、
前記入力部を介して、キーワードの入力を受け付けるキーワード受付処理と、
前記キーワード受付処理で受け付けたキーワードに対応するキーワードＩＤを前記キーワードデータから抽出するキーワードＩＤ抽出処理と、
前記キーワードＩＤ抽出処理で抽出したキーワードＩＤに関連する資産ＩＤ、脅威ＩＤ、および、対策ＩＤをそれぞれ前記第一の要素実績データ、前記第二の要素実績データ、および、前記第三の要素実績データ、から抽出する要素抽出処理と、
前記要素抽出処理で抽出された資産ＩＤ毎に、該資産ＩＤにより特定される情報資産が曝される脅威を、前記要素抽出処理で抽出された脅威ＩＤにより特定される脅威の中から前記入力部を介して特定する処理を受け付ける脅威特定処理と、
前記脅威抽出処理で特定された脅威毎に、該脅威に対して採用する対策を、前記要素抽出処理で抽出された対策ＩＤにより特定される対策の中から前記入力部を介して特定する処理を受け付ける対策特定処理と、
前記脅威特定処理で特定された脅威毎に、前記第二の要素データから前記基準リスクを抽出して加算することで、該資産毎の合計値であるリスク合計値を算出するとともに、前記脅威抽出処理で脅威を抽出した資産毎に、前記対策特定処理で特定された対策に対応する基準削減効果を前記第三の要素データから抽出し、該基準削減効果を前記リスク合計値から各々減算することで、残存リスク額を算出する残存リスク算出処理と、
前記脅威抽出処理で脅威を抽出した資産毎に、前記対策特定処理で特定された対策に対応する基準コストを前記第三の要素データから抽出し、該基準コストを各々加算することにより所用コスト額を算出する所用コスト算出処理と、
前記脅威抽出処理で脅威を抽出した資産毎に、前記残存リスク額、前記所用コスト額、および、前記対策特定処理で特定された対策、を特定したセキュリティポリシーを作成し、該セキュリティポリシーを前記表示部に表示する表示処理と、
を行うことを特徴とするセキュリティポリシーの作成支援システム。
【請求項２】
請求項１に記載のセキュリティポリシーの作成支援システムであって、
前記脅威特定処理は、前記要素抽出処理で抽出された資産ＩＤ毎に、前記要素抽出処理で抽出された脅威ＩＤに対応する前記第二の要素データに含まれる少なくとも一つの情報をリストにして前記表示部に表示し、該リストの中から前記入力部を介して特定するものであること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項３】
請求項２に記載のセキュリティポリシーの作成支援システムであって、
前記第二の要素実績データには、脅威毎に、前記セキュリティポリシーを作成する際に前記脅威特定処理で特定された回数がカウントされており、
前記リストは、前記回数が多いものから順に上位に位置するようにされていること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項４】
請求項１に記載のセキュリティポリシーの作成支援システムであって、
前記対策特定処理は、前記脅威抽出処理で特定された脅威毎に、前記要素抽出処理で抽出された対策ＩＤに対応する前記第三の要素データに含まれる少なくとも一つの情報をリストにして前記表示部に表示し、該リストの中から前記入力部を介して特定するものであること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項５】
請求項４に記載のセキュリティポリシーの作成支援システムであって、
前記第三の要素実績データには、対策毎に、前記セキュリティポリシーを作成する際に

前記対策特定処理で特定された回数がカウントされており、
前記リストは、前記回数が多いものから順に上位に位置するようにされていること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項６】
請求項４に記載のセキュリティポリシーの作成支援システムであって、
前記記憶部には、脅威を識別するための脅威ＩＤ、該脅威への対策を識別するための対策ＩＤ、および、該脅威ＩＤにより特定される脅威に対して該対策ＩＤにより特定される対策が前記セキュリティポリシーを作成する際に前記対策特定処理で特定された第一の回数、を有するリンクデータがさらに記憶されており、
前記リストは、前記第一の回数が多いものから順に上位に位置するようにされていること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項７】
請求項６に記載のセキュリティポリシーの作成支援システムであって、
前記第三の要素実績データには、対策毎に、前記セキュリティポリシーを作成する際に前記対策特定処理で特定された第二の回数がカウントされており、
前記リストは、前記第一の回数が同じ場合には、前記第二の回数が多いものから順に上位に位置するようにされていること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項８】
請求項７に記載のセキュリティポリシーの作成支援システムであって、
前記リンクデータは、前記脅威ＩＤにより特定される脅威又は前記対策ＩＤにより特定される対策に関連するキーワードを識別するためのキーワードＩＤ、および、該キーワードＩＤにより特定されるキーワードが前記セキュリティポリシーを作成する際に使用された第三の回数、をさらに有しており、
前記リストは、前記第一の回数及び前記第二の回数が同じ場合には、前記第三の回数が多いものから順に上位に位置するようにされていること、を特徴とするセキュリティポリシーの作成支援システム。
【請求項９】
請求項１に記載のセキュリティポリシーの作成支援システムであって、
前記制御部は、
前記入力部を介してユーザＩＤの入力を受け付けるユーザＩＤ入力処理と、
前記入力部を介して、前記第一の要素実績データ、前記第二の要素実績データ、または、前記第三の要素実績データに、それぞれ新たな資産要素実績、脅威要素実績、または、対策要素実績、を追加する更新処理と、
前記更新処理において追加を行ったユーザのユーザＩＤを前記資産要素実績、前記脅威要素実績、または、前記対策要素実績、に追加するユーザＩＤ追加処理と、
前記更新処理により追加された前記資産要素実績、前記脅威要素実績、または、前記対策要素実績が、前記セキュリティポリシーを作成する際に前記対策特定処理で特定された回数に所定の金額を乗算することにより、前記ユーザＩＤ毎にノウハウ提供料を算出するノウハウ提供料算出処理と、
をさらに行うことを特徴とするセキュリティポリシーの作成支援システム。
【請求項１０】
入力手段、および、表示手段を備えるコンピュータを、
情報資産毎に、該情報資産を識別するための資産ＩＤ、を有する第一の要素データと、
前記情報資産が曝される脅威毎に、該脅威を識別するための脅威ＩＤ、該脅威の内容を示す攻撃方法、および、該脅威による損失額を単位時間当たりの割合で特定した基準リスク、を有する第二の要素データと、
前記脅威への対策毎に、該対策を識別するための対策ＩＤ、該対策の具体的な内容を示す対策の内容、該対策に要するコスト額を単位時間当たりの割合で特定した基準コスト、および、該対策による前記基準リスクの削減額を単位時間当たりの割合で特定した基準削

減効果、を有する第三の要素データと、
資産ＩＤ、および、該資産ＩＤにより特定される情報資産に関連するキーワードを識別するためのキーワードＩＤ、を該資産ＩＤ毎に有する資産要素実績からなる第一の要素実績データと、
脅威ＩＤ、および、該脅威ＩＤにより特定される脅威に関連するキーワードを識別するためのキーワードＩＤ、を該脅威ＩＤ毎に有する脅威要素実績からなる第二の要素実績データと、
対策ＩＤ、および、該対策ＩＤにより特定される対策に関連するキーワードを識別するためのキーワードＩＤ、を該対策ＩＤ毎に有する対策要素実績からなる第三の要素実績データと、
キーワード、および、該キーワードを識別するためのキーワードＩＤ、を該キーワード毎に有するキーワードデータと、
を記憶する記憶手段、
前記入力手段を介して、キーワードの入力を受け付けるキーワード受付処理と、
前記キーワード受付処理で受け付けたキーワードに対応するキーワードＩＤを前記キーワードデータから抽出するキーワードＩＤ抽出処理と、
前記キーワードＩＤ抽出処理で抽出したキーワードＩＤに関連する資産ＩＤ、脅威ＩＤ、および、対策ＩＤをそれぞれ前記第一の要素実績データ、前記第二の要素実績データ、および、前記第三の要素実績データ、から抽出する要素抽出処理と、
前記要素抽出処理で抽出された資産ＩＤ毎に、該資産ＩＤにより特定される情報資産が曝される脅威を、前記要素抽出処理で抽出された脅威ＩＤにより特定される脅威の中から前記入力手段を介して特定する処理を受け付ける脅威特定処理と、
前記脅威抽出処理で特定された脅威毎に、該脅威に対して採用する対策を、前記要素抽出処理で抽出された対策ＩＤにより特定される対策の中から前記入力手段を介して特定する処理を受け付ける対策特定処理と、
前記脅威特定処理で特定された脅威毎に、前記第二の要素データから前記基準リスクを抽出して加算することで、該資産毎の合計値であるリスク合計値を算出するとともに、前記脅威抽出処理で脅威を抽出した資産毎に、前記対策特定処理で特定された対策に対応する基準削減効果を前記第三の要素データから抽出し、該基準削減効果を前記リスク合計値から各々減算することで、残存リスク額を算出する残存リスク算出処理と、
前記脅威抽出処理で脅威を抽出した資産毎に、前記対策特定処理で特定された対策に対応する基準コストを前記第三の要素データから抽出し、該基準コストを各々加算することにより所用コスト額を算出する所用コスト算出処理と、
前記脅威抽出処理で脅威を抽出した資産毎に、前記残存リスク額、前記所用コスト額、および、前記対策特定処理で特定された対策、を特定したセキュリティポリシーを作成し、該セキュリティポリシーを前記表示手段に表示する表示処理と、
を行う制御手段、
として機能させることを特徴とするプログラム。
【請求項１１】
請求項１０に記載のプログラムであって、
前記脅威特定処理は、前記要素抽出処理で抽出された資産ＩＤ毎に、前記要素抽出処理で抽出された脅威ＩＤに対応する第二の要素データに含まれる少なくとも一つの情報をリストにして前記表示手段に表示し、該リストの中から前記入力手段を介して特定するものであること、を特徴とするプログラム。
【請求項１２】
請求項１１に記載のプログラムであって、
前記第二の要素実績データには、脅威毎に、前記セキュリティポリシーを作成する際に前記脅威特定処理で特定された回数がカウントされており、
前記リストは、前記回数が多いものから順に上位に位置するようにされていること、を特徴とするプログラム。

【請求項１３】
請求項１０に記載のプログラムであって、
前記対策特定処理は、前記脅威抽出処理で特定された脅威毎に、前記要素抽出処理で抽出された対策ＩＤに対応する第三の要素データに含まれる少なくとも一つの情報をリストにして前記表示手段に表示し、該リストの中から前記入力手段を介して特定するものであること、を特徴とするプログラム。
【請求項１４】
請求項１３に記載のプログラムであって、
前記第三の要素実績データには、対策毎に、前記セキュリティポリシーを作成する際に前記対策特定処理で特定された回数がカウントされており、
前記リストは、前記回数が多いものから順に上位に位置するようにされていること、を特徴とするプログラム。
【請求項１５】
請求項１３に記載のプログラムであって、
前記記憶手段には、脅威を識別するための脅威ＩＤ、該脅威への対策を識別するための対策ＩＤ、および、該脅威ＩＤにより特定される脅威に対して該対策ＩＤにより特定される対策が前記セキュリティポリシーを作成する際に前記対策特定処理で特定された第一の回数、を有するリンクデータがさらに記憶されており、
前記リストは、前記第一の回数が多いものから順に上位に位置するようにされていること、を特徴とするプログラム。
【請求項１６】
請求項１５に記載のプログラムであって、
前記第三の要素実績データには、対策毎に、前記セキュリティポリシーを作成する際に前記対策特定処理で特定された第二の回数がカウントされており、
前記リストは、前記第一の回数が同じ場合には、前記第二の回数が多いものから順に上位に位置するようにされていること、を特徴とするプログラム。
【請求項１７】
請求項１６に記載のプログラムであって、
前記リンクデータは、前記脅威ＩＤにより特定される脅威又は前記対策ＩＤにより特定される対策に関連するキーワードを識別するためのキーワードＩＤ、および、該キーワードＩＤにより特定されるキーワードが前記セキュリティポリシーを作成する際に使用された第三の回数、をさらに有しており、
前記リストは、前記第一の回数及び前記第二の回数が同じ場合には、前記第三の回数が多いものから順に上位に位置するようにされていること、を特徴とするプログラム。
【請求項１８】
請求項１０に記載のプログラムであって、
前記制御手段に、
前記入力手段を介してユーザＩＤの入力を受け付けるユーザＩＤ入力処理と、
前記入力手段を介して、前記第一の要素実績データ、前記第二の要素実績データ、または、前記第三の要素実績データに、それぞれ新たな資産要素実績、脅威要素実績、または、対策要素実績、を追加する更新処理と、
前記更新処理において追加を行ったユーザのユーザＩＤを前記資産要素実績、前記脅威要素実績、または、前記対策要素実績、に追加するユーザＩＤ追加処理と、
前記更新処理により追加された前記資産要素実績、前記脅威要素実績、または、前記対策要素実績が、前記セキュリティポリシーを作成する際に前記対策特定処理で特定された回数に所定の金額を乗算することにより、前記ユーザＩＤ毎にノウハウ提供料を算出するノウハウ提供料算出処理と、
をさらに行わせることを特徴とするプログラム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
本発明は、情報システムのセキュリティポリシーの作成を支援するシステムに関し、特に、過去の事例データに基づいてセキュリティポリシーの作成を支援するシステムに関する。
【０００２】
【従来の技術】
従来より、情報セキュリティポリシーの策定手法・手順としては、ISO/IEC TR 13335 (GMITS:Guidelines for the management of IT Security)やISO/IEC 17799 (BS7799)等の国際標準により規定され推奨される手法・手順がある。この手法・手順では、(1)適用対象・範囲の決定、(2)情報資産の定義、(3)脅威の抽出、(4)リスク評価、(5)ポリシー（対策）の策定、の各ステップをこの順に正確に実施する。また、情報技術製品や情報システムのセキュリティ機能の設計・評価に関する国際標準としてISO/IEC 15408 (CC:Common Criteria)があり、前述のISO/IEC TR 13335やISO/IEC 17799等と同様の手順でのセキュリティ設計を推奨している。この手法・手順では、まず最初に対象となる情報システムの固有性を定義し、その定義をもとにして対象システムに固有の脅威を洗い出すことにより、対象システム固有の対策を策定できる。つまり、この手法・手順は、対象となる情報システムに適したセキュリティポリシー、あるいはセキュリティに関する対策を策定するために有効なものである。
【０００３】
また、簡易なポリシー策定方法としては、セキュリティポリシーの作成事例を利用するものがあり、例えば、特開２００１－１０１１３５号公報「セキュリティ評価方法および装置、セキュリティ施策の作成支援方法および装置」がある。この先行技術文献では、各情報機器タイプのポリシー事例を事前にデータベースに格納しておき、対象システム構成に応じて、各構成機器のポリシー事例を組み合わせることにより、対象システム全体のポリシーを策定するものである。
【０００４】
【発明が解決しようとする課題】
しかしながら、前述の国際標準で推奨されているセキュリティポリシー策定手法・手順の実施には、リスク分析等、高度な専門知識や技術に加えて、脅威や対策事例の豊富な知識と、どの脅威に対してどの対策が有効であるかといったセキュリティに関するノウハウが必要となる。このため、限られた専門家が時間およびコストをかけなければ実施できないという問題点がある。
【０００５】
一方、前述の先行技術文献の手法では、構成機器からセキュリティポリシーを導出するノウハウをデータベース化しているが、インターネット接続システム等のような各構成要素の固有性が小さい情報システムを対象としており、適用範囲が限定されている。
【０００６】
そこで、本発明は、ノウハウを有しない者であっても、対象となる情報システムに適したセキュリティに関する対策の決定、あるいはセキュリティポリシーを作成することができるように支援するシステムを提供することを目的とする。
【０００７】
また、本発明は、セキュリティポリシーの作成に対してノウハウを提供して、それに対する課金を行うシステムを提供することを別の目的とする。
【０００８】
また、セキュリティポリシーの作成事例データを収集して、効率的にノウハウを蓄積することをさらに別の目的とする。
【０００９】
【課題を解決するための手段】
本発明の一つの形態に従うセキュリティポリシーの作成支援システムによれば、情報システムを構成する情報資産と、前記情報資産に関連するキーワードとを対応付けて記憶する

第１の記憶手段と、前記情報資産が曝される脅威と、前記脅威に関連するキーワードとを対応付けて記憶する第２の記憶手段と、前記脅威に対する対策と、前記対策に関連するキーワードとを対応付けて記憶する第３の記憶手段と、セキュリティポリシーの作成対象となる情報システムに関するキーワードの入力を受け付ける受付手段と、前記受付手段が受け付けたキーワードに基づいて、情報資産と脅威と対策とを抽出する抽出手段と、前記抽出手段による抽出結果を表示する表示手段とを備える。

【００１０】

本発明の他の形態に従うセキュリティポリシーの作成支援システムによれば、情報システムを構成する情報資産と、前記情報資産が曝される脅威との関連を記憶する記憶手段と、セキュリティポリシーの作成対象となる情報システムに含まれる情報資産を決定する資産決定手段と、前記資産決定手段により決定された情報資産に対する脅威の候補を抽出する抽出手段と、前記抽出手段による抽出結果を表示する表示手段とを備える。

【００１１】

本発明の他の形態に従うセキュリティ対策決定支援システムによれば、情報システムが曝される脅威と、前記脅威に対する対策との関連を記憶する記憶手段と、セキュリティに関する対策を決定する対象となる情報システムが曝される脅威を決定する脅威決定手段と、前記脅威決定手段により決定された脅威に対する対策の候補を抽出する抽出手段と、前記抽出手段による抽出結果を表示する表示手段とを備える。

【００１２】

【発明の実施の形態】

以下、本発明の実施形態について、図面を用いて説明する。

【００１３】

図１は、本発明を適用した第一の実施形態に係るセキュリティポリシー作成支援システムの全体構成を示す図である。本システムは、セキュリティポリシーの作成を支援するセキュリティポリシー作成支援装置（以下、支援装置）１１と、セキュリティポリシーの作成時に使用するノウハウを管理するノウハウ管理装置１２とを有する。ノウハウ管理装置１２は、セキュリティポリシーを作成する際に利用するノウハウを保持したノウハウデータベース１３と、複数のセキュリティポリシー作成事例データからなる事例データベース１５と、ノウハウデータベース１３の利用者の情報を管理する利用者データベース１６とを有する。

【００１４】

支援装置１１の詳細な構成を図２に示す。支援装置１１は、汎用のパーソナルコンピュータ等で構成することができる。例えば、支援装置１１は、ＣＰＵ２１と、入出力制御部２２と、バス２３と、外部記憶装置２４と、主記憶装置（メモリ）２５と、端末入出力制御部２２に接続されたディスプレイ２６およびキーボード２７と、他の装置との間のネットワーク回線を制御するネットワーク制御部２８とを有する。

【００１５】

外部記憶装置２４には、セキュリティポリシーの作成支援プログラム２４１と、通信処理プログラム２４２とが記憶されている。ＣＰＵ２１が、作成支援プログラム２４１と通信処理プログラム２４２とを読み込んで、実行することにより以下の各処理部２５０１～２５８が実現する。つまり、ＣＰＵ２１上には、セキュリティポリシーを作成する対象システムのキーワード入力処理部２５１と、対象システムのキーワードに基づいて情報資産、脅威、対策等のポリシー作成に関わるデータ群（以降、事例データと呼ぶ）の雛型を作成する雛型作成処理部２５２と、情報資産の定義を支援する情報資産定義処理部２５３と、情報資産に対する脅威を洗い出し、対策を取るべき脅威の決定を支援する脅威抽出・決定処理部２５４と、リスク及び対策に要するコストを評価するリスク・コスト管理処理部２５５と、脅威に対する対策の決定を支援する対策立案・決定処理部２５６と、ネットワーク回線を介した通信を行うための通信処理部２５８とを備える。

【００１６】

ノウハウ管理装置１２の詳細な構成を図３に示す。ノウハウ管理装置１２は、汎用のパー

ソナルコンピュータ等で構成することができる。例えば、ノウハウ管理装置１２は、ＣＰＵ３１と、入出力制御部３２と、バス３３と、外部記憶装置３４と、主記憶装置（メモリ）３５と、端末入出力制御部３２に接続されたディスプレイ３６およびキーボード３７と、他の装置との間のネットワーク回線を制御するネットワーク制御部３８とを有する。

【００１７】

外部記憶装置３４には、ノウハウデータベース等を管理するデータベース管理プログラム３４１と、ネットワーク回線を介して通信を行うための通信制御処理プログラム３４２と、事例データベースを構成する事例データ３４３と、ノウハウデータベースを構成するノウハウデータ３４４と、利用者管理データベースを構成する利用者データ３４５と、課金処理プログラム３４６と、優先度算出処理プログラム３４７とが記憶されている。ＣＰＵ３１が、データベース管理プログラム３４１、通信処理プログラム２４２、課金処理プログラム３４６、及び優先度算出処理プログラム３４７を読み込んで、実行することにより以下の各処理部３５１～３５６が実現する。つまり、ＣＰＵ３１上には、通信処理部３５１と、データベース検索処理部３５２と、データベース更新処理部３５３と、ノウハウ利用者識別・認証処理部３５４と、課金処理部３５５と、優先度算出処理部３５６とを備える。

【００１８】

つぎに、ノウハウデータベース１３が有するデータ項目を図４及び図５に示す。ノウハウデータベース１３は、要素データ１３１と、要素間リンクデータ１３２と、実績データ１３３、１３４と、キーワードデータ１３５とを有する。

【００１９】

要素データ１３１は、セキュリティポリシーの作成に必要な要素を定義する。要素データには、対象となるシステムが保有する情報資産（以下、単に資産という）の種類に関する情報４１と、対象となるシステムが曝される脅威の種類に関する情報４２と、脅威に対する対策の種類に関する情報４３と、脅威の種別を定義する定義情報４４と、対策の種別を定義する定義情報４５とが含まれる。

【００２０】

資産の種類に関する情報４１は、資産を識別するための資産ＩＤ４１１と、資産の分類項目４１２と、情報資産名４１３と、資産の存在場所４１４と、資産の形態４１５とを含む。

【００２１】

脅威の種類に関する情報４２は、脅威を識別するための脅威ＩＤ４２１と、脅威の種別を識別するための脅威種別ＩＤ４２２と、攻撃者または脅威の要因４２３と、攻撃方法４２４と、基準リスク４２５とを含む。基準リスク４２５とは、脅威の度合い（その脅威が起こったときの損失の度合い）を示すものであり、他の脅威と比較するための指標である。例えば、基準リスク４２５は、脅威が起こったときに予想される損失額と、その脅威の起こる確率の積で求めることができる。基準リスク４２５は、随時、更新することができる。

【００２２】

脅威に対する対策の種類に関する情報４３は、対策を識別するための対策ＩＤ４３１と、対策の種別を識別するための対策種別ＩＤ４３２と、対策の内容４３３と、基準コスト４３４と、基準削減効果４３５とを含む。基準コスト４３４とは、その対策を実施するのに要するコストである。基準削減効果４３５は、対策を実施することにより期待できる基準リスク４２５の削減効果であり、他の対策と比較するための指標である。基準コスト４３４および基準削減効果４３５は、随時、更新することができる。

【００２３】

脅威の種別を定義する定義情報４４は、脅威種別ＩＤ４４１と、脅威種別４４２とを対応付ける。

【００２４】

対策の種別を定義する定義情報４５は、対策種別ＩＤ４５１と、対策種別４５２とを対応

付ける。
【００２５】
要素間リンクデータ１３２は、要素間の関連を定義する。具体的には、要素間リンクデータ１３２は、資産と、その資産に対して生じ得る脅威とを関連付ける脅威－資産リンク４７と、脅威と、その脅威に対する対策とを関連付ける対策－脅威間リンク４８とを含む。
【００２６】
脅威－資産リンク４７は、脅威－資産リンクＩＤ４７１と、脅威ＩＤ４２１と、資産ＩＤ４１１とをそれぞれ対応付ける。
【００２７】
対策－脅威間リンク４８は、対策－脅威間リンクＩＤ４８１と、対策ＩＤ４３１と、脅威ＩＤ４２１とをそれぞれ対応付ける。
【００２８】
キーワードデータ１３５は、セキュリティポリシーの適用対象システムの特徴を表すキーワードとして使用できるものが登録されている。キーワードは、例えば、業種（例えば金融、証券、官公庁等）、システム種別（例えばインターネット接続システム、リモートアクセスシステム、ATMシステム等）、部門種別（例えば全社、人事部門、開発部門等）等を含む。キーワードデータ１３５は、キーワードＩＤ５６１と、キーワード５６２と、上位キーワード５６３とが対応付けられている。キーワード同士が階層的な関係を有する場合、上位キーワード５６３には、キーワード５６２の上位となるキーワードのＩＤが登録される。
【００２９】
実績データ１３３、１３４は、要素データの実績データ１３３と要素間リンクデータの実績データ１３４とがあり、要素データ１３１または要素間リンクデータ１３２が、セキュリティポリシーの作成に使用された回数の実績を示す。さらに、要素実績データ１３３および要素間リンク実績データ１３４は、要素データまたは要素間リンクデータとキーワードとを対応付ける。
【００３０】
要素データの実績データ１３３は、資産の実績データ５１と、脅威の実績データ５２と、対策の実績データ５３とを含む。要素間リンクの実績データ１３４は、脅威－資産間リンクの実績データ５４と、対策－脅威間リンクの実績データ５５とを含む。
【００３１】
資産実績データ５１は、資産ＩＤ４１１と、その資産が使用された使用総数５１２と、この資産を登録した登録者のＩＤ５１６とを含む。さらに、資産実績データ５１は、資産ＩＤ４１１に対応付けられたキーワード５１３と、そのキーワードの使用回数５１４との組み合わせを複数含む。使用総数５１２は、資産がセキュリティポリシーの作成時に使用された総数である。キーワード別の使用回数５１４は、そのキーワードに基づいて資産が使用された回数を示す。
【００３２】
脅威の実績データ５２、対策の実績データ５３、脅威－資産間リンクの実績データ５４、および対策－脅威間リンクの実績データ５５についても、同様の構造を有する。
【００３３】
次に、事例データベース１５が有するデータ項目を図６に示す。事例データベース１５は、本システムがセキュリティポリシーの作成を行った事例に関するデータを蓄積したデータベースである。事例データベース１５は、セキュリティポリシーの作成対象システムの事例データ６１と、要素データの事例データ６２、６３、６４と、要素間リンクデータの事例データ６５、６６とを含む。
【００３４】
セキュリティポリシーの作成対象システムの事例データ６１は、対象となる事例の事例ＩＤ６０１と、キーワード６０２と、作成者ＩＤ６０３とを含む。キーワード６０２は、ここでは４つ登録することができる。作成者ＩＤ６０３は、事例を作成して登録した者のＩ

Ｄである。
【００３５】
要素データの事例データは、資産の事例データ６２と、脅威の事例データ６３と、対策の事例データ６４とを有する。
【００３６】
資産の事例データ６２は、資産事例ＩＤ６２１と、具体的資産名６２２と、資産ＩＤ４１１と、分類項目４１２と、情報資産名４１３と、存在場所４１４と、資産形態４１５とを有する。
【００３７】
脅威の事例データ６３は、脅威事例ＩＤ６３１と、具体的脅威記述６３２と、設定リスク６３３と、脅威ＩＤ４２１と、脅威種別４２２と、攻撃者／要因４２３と、攻撃方法４２４とを有する。
【００３８】
対策の事例データ６４は、対策事例ＩＤ６４１と具体的対策記述６４２と、設定コスト６４３と、リスク削減効果６４４と、対策ＩＤ４３１と、対策種別ＩＤ４３２と、対策内容４３３とを有する。
【００３９】
要素間リンクデータの事例データは、脅威－資産間リンクの事例データ６５と、対策－脅威間リンクの事例データ６６とを含む。
【００４０】
脅威－資産間リンクの事例データ６５は、脅威－資産事例リンクＩＤ６５１と、脅威事例ＩＤ６３１と、資産事例ＩＤ６２１と、脅威－資産間リンクＩＤ４７１とを含む。
【００４１】
対策－脅威間リンクの事例データ６６は、対策－脅威事例リンクＩＤ６６１と、対策事例ＩＤ６４１と、脅威事例ＩＤ６３１と、対策－脅威リンクＩＤ４８１とを含む。
【００４２】
つぎに、利用者データベース１６のデータ項目を、図７に示す。利用者データベース１６は、ユーザＩＤ７１１と、利用者を認証するためのパスワード７１２と、利用者の人名や会社名等のユーザ詳細情報７１３と、課金総額７１４と、ポリシー事例データの作成回数７１５と、ポリシー事例データの提供回数７１６と、各ポリシー事例データの利用回数の総和７１７とを含む。
【００４３】
次に、新規にセキュリティポリシーを作成するときの処理手順について、説明する。
【００４４】
図９は、標準的なセキュリティポリシー作成手順を示すフローチャートである。セキュリティポリシーの作成は、支援装置１１とノウハウ管理装置１２とがそれぞれ処理を実行し、セキュリティポリシーの適用対象の決定９１１、保護すべき情報資産の定義９１２、定義した情報資産に対する脅威の抽出９１３、脅威に対するリスクの評価９１４、および対策の立案９１５の順に行われる。
【００４５】
まず、ポリシー作成支援プログラム２４１が表示するメニュー画面の例を図１８に示す。ここで、適用対象の決定ボタン１８０１が押下されると、後述するステップＳ９２２、Ｓ９２３の処理が実行される。情報資産の定義ボタン１８０２が押下されると、後述するステップＳ９２４の処理が実行される。脅威抽出＆リスク評価ボタン１８０３が押下されると、後述するステップＳ９２５、Ｓ９２６が実行される。対策立案ボタン１８０４が押下されると、後述するステップＳ９２７が実行され、ユーザがセキュリティポリシーの作成が完了したと判断して、完了ボタン１８０６が押下されると、後述するステップＳ９２８の処理が実行される。
【００４６】
（セキュリティポリシーの適用対象の決定９１１）

まず、ユーザが支援装置１１へログインする。ユーザのログインは、例えば、図２２に示すような、利用者を識別するためのユーザＩＤ２２０１と、パスワードの入力領域２２０２を備えたログイン２２０画面を利用してもよい。支援装置１１は、受け付けたユーザＩＤとパスワードをノウハウ管理装置１２へ通知する（Ｓ９２１）。

【００４７】

ノウハウ管理装置１２のノウハウ利用者識別・認証処理部３５４は、通知されたユーザＩＤとパスワードを利用者データベース１６の登録内容と照らし合わせることにより利用可否を決定する。登録ユーザの場合はノウハウデータベース１３のキーワードデータ１３５に登録されているキーワード一覧を送信する（Ｓ９３１）。

【００４８】

支援装置１１の対象システムのキーワード入力処理部２５１は、図１０に示すセキュリティポリシー適用対象のキーワード情報入力画面１００を表示し、ユーザからキーワード等の入力を受け付ける。キーワードは、新規追加１０１を選択して入力するか、または受信したキーワード一覧１０２から選択できる。入力完了後にキーワードをノウハウ管理装置１２に送信する（Ｓ９２２）。

【００４９】

ノウハウ管理装置１２のデータベース検索・データ取得処理部３５２は、受信したキーワードに基づいて、セキュリティポリシーの雛形を作成し、支援装置１１へ送信される（Ｓ９３２）。雛形作成の詳細な処理手順は、図１９に示す。

【００５０】

すなわち、データベース検索・データ取得処理部３５２は、受信したキーワードのうちキーワードデータ１３５に登録されているものを抽出し、キーワードリストを作成する（Ｓ１９０１）。さらに、データベース検索・データ取得処理部３５２は、キーワードリストに含まれる各キーワードの上位キーワード５６３を抽出する（Ｓ１９０２）。そして、１３３を検索して、キーワードリストの各キーワードが関連する資産、脅威、対策、および、脅威－資産リンク、対策－脅威リンクを抽出する（Ｓ１９０３）。最後に、要素間リンクデータ１３２を参照し、対応付けられている資産、脅威、対策のみを残し、セキュリティポリシーの雛型をする（Ｓ１９０４）。なお、ステップＳ１９０３の具体的な処理としては、関連するキーワードに対して少なくとも１回以上使用されているものを抽出してもよいし、事前に設定した使用回数（例えば１０回）以上使用されているものを抽出してもよい。

【００５１】

支援装置１１のポリシーデータ雛形作成処理部２５２が、受信した情報資産、脅威、対策、脅威－資産リンク、対策－脅威リンクを含む雛形データを事例データベース１５へ格納する。ただし、雛型データの場合、事例ＩＤ（６２１、６３１、６４１、６５１、６６１）および具体的記述（６２２、６３２、６４２、６５２、６６２）は空欄とし、設定リスク６３３、設定コスト６４３にはそれぞれ基準リスク４２５、基準コスト４３４を設定する。この雛形データをベースにして以降の処理を行う。

【００５２】

（資産の定義９１２）

支援装置１１の情報資産定義処理部２５３は、図１１に示す資産の定義画面１１０に、初期状態として資産雛型一覧を表示させる。ユーザは、この画面１１０を利用して、雛型をベースに資産の追加/編集、削除を行う（Ｓ９２４）。

【００５３】

資産の定義画面１１０は、抽出された資産の分類項目１１０１と、一般名称１１０２と、固有名称１１０３と、資産の所在する場所および形態１１０４の表示領域を有し、さらに、雛形に含まれる資産の追加及び編集を行うための追加／編集ボタン１１０５と、削除するための削除ボタン１１０６とを有する。追加／編集ボタン１１０５が押されると、図１２に示す追加／編集画面１２０が表示される。追加／編集画面１２０では、雛形には含まれていない新たな資産を追加することができる。追加／編集画面１２０は、分類項目１２

０１、資産一般名称１２０２、資産固有名称１２０４、場所／形態１２０５等の入力欄を有する。

【００５４】

支援装置１１の情報資産定義処理部２５３は、ノウハウ管理装置１２に対して資産一覧を要求し、ノウハウ管理装置１２のデータベース検索・データ取得処理部３５２は実績データを含む情報資産一覧を支援装置１１に送信する。情報資産定義処理部２５３は受信した資産一覧を、分類項目１２０１、資産一般名称１２０２、および場所/形態１２０５の入力領域における選択肢として表示する。ここで、一般名称１２０２は、その資産名がこれまでに使用された回数に基づいて資産の選択優先度１２０３を決定し、その優先度順に一覧表示する。優先度１２０３は、例えば、使用回数が多いほど優先度を高くする。具体的には、(a)総使用回数の大きい順に優先度を割り振る、(b)キーワードに関連するが雛型として採用されなかった資産を使用回数順に優先付けした後、キーワードに関連しない資産を総使用回数順に優先付けする等の方法がある。

【００５５】

本システムは、上記のような画面を用いて、ユーザによる資産定義を支援する。

【００５６】

（脅威の抽出９１３）

ユーザが資産の定義を終わると、本システムは、ユーザによる脅威の定義を支援する。すなわち、支援装置１１の脅威抽出・決定処理部２５４は、図１３に示す脅威抽出・リスク評価画面１３０で、脅威雛型一覧をユーザに提示する。ここで示された脅威の雛型をベースに、ユーザは脅威の追加、編集、削除を行う（Ｓ９２５）。脅威抽出・リスク評価画面１３０は、定義した資産ごとに脅威を抽出、決定するための画面であり、脅威種別１３０１と、セキュリティポリシー作成のために採用した脅威リスト１３０２と、使用回数に基づく優先度１３０３と、リスク１３０４と、追加候補のリスト１３０５と、追加ボタン１３０６と、削除ボタン１３０７と、新規追加ボタン１３０８と、リスク評価ボタン１３０９とを有する。脅威抽出・リスク評価画面１３０を開いたとき、採用脅威１３０２に脅威の雛型が表示され、追加候補リスト１３０５にノウハウデータベース１３から取得した脅威の一覧が表示される。ここで、追加候補リスト１３０５は、脅威の選択優先度１３０３の順に表示される。優先度１３０３は、その脅威がこれまでに使用された回数に基づいて算出される。例えば、優先度１３０３は、使用回数が多いほど優先度を高くする。具体的には、(a)総使用回数の大きい順に優先度を割り振る、(b)対象とする情報資産が関わる脅威－資産リンクの総使用回数の大きい順に優先度を割り振る、(c)まず(b)の方法で優先度を割り振り、同じ使用回数のものについてはさらに(a)の方法で順位をつける、(d)(c)の方法でもなお同じ順位となる場合はさらにキーワードとの関連の有無やキーワードに使用回数の大小で判断する等の方法がある。

【００５７】

（リスクの評価９１４）

そして、採用した脅威リスト１３０２には、ユーザが採用した脅威がリストアップされる。ここでリスク評価ボタン１３０９が押されると、リスク・コスト管理処理部２５５がリスクを評価する（Ｓ９２６）。リスク表示領域１３０４には、リスク評価結果の値が表示される。なお、リスク評価手法は公知の定量手法、定性手法等があり、いずれかの方式に基づいて別途算出する。

【００５８】

（対策の立案９１５）

最後に、図１４に示す対策決定・コスト設定画面１４０、図１５に示す対策立案・コスト設定画面１５０および図１６に示す対策選択画面１６０で、脅威に対する対策を洗い出し、設定した許容リスク、許容コストを満足するようにコスト効果の高い対策を選択する（Ｓ９２７）。対策決定・コスト設定画面１４０は、各資産別に対策をとるべき脅威一覧１４０７と、資産別残存リスク１４０２と、対策にかかる所要コスト１４０４と、許容リスクの入力領域１４０１と、許容コストの入力領域１４０３と、対策候補作成ボタン１４０

５と、対策選択ボタン１４０６とを有する。

【００５９】

ユーザが脅威一覧１４０７から脅威を選択後、対策候補作成ボタン１４０５を押下すると、対策立案・コスト設定画面１５０が開き、脅威に対する対策の洗い出しと各対策の所要コストの設定を行う。対策立案・コスト設定画面１５０は、選択した脅威に対する対策案を洗い出し、各対策のコストを設定するための画面であり、対策候補リスト１５０２、使用回数に基づく優先度１５０３と、コスト１５０４と、追加候補リスト１５０６、追加ボタン１５０７と、削除ボタン１５０８と、新規追加ボタン１５０９とを有する。この画面１５０が開いたときには、対策候補１５０２に対策の雛型が表示され、追加候補リスト１５０６にノウハウデータベース１３から取得した対策の一覧が表示される。ここで、追加候補リスト１５０６は、対策の優先度１５０３の順に表示される。優先度１５０３は、その対策がこれまでに使用された回数に基づいて算出される。具体的には、(a)各対策の総使用回数の大きい順に優先度を割り振る、(b)対象とする脅威が関わる対策－脅威リンクの総使用回数の大きい順に優先度を割り振る、(c)まず(b)の方法で優先度を割り振り同じ使用回数のものについてはさらに(a)の方法で順位をつける、(d)(c)の方法でもなお同じ順位となる場合はさらにキーワードとの関連の有無やキーワードに使用回数の大小で判断する、等の方法がある。

【００６０】

次に、ユーザが対策選択ボタン１４０６を押下すると、対策選択画面１６０が開き、各資産について許容リスク、許容コストを満足する対策を選択する。対策選択画面１６０は、残存リスク、所要コストが許容範囲に収まり、脅威に対して抜け漏れなく対処する対策を選択するための画面であり、脅威一覧リスト１６０１、対策一覧リスト１６０２、対策の選択領域１６０３と、未対策脅威の有無の表示領域１６０４と、残存リスクと所要コスト表示領域１６０６とを有する。ユーザが対策の選択領域１６０３にチェックを入れて選択することにより、残存リスクと所要コスト表示領域１６０６および未対策脅威の有無の表示領域１６０４に、その時の状況が表示される。

【００６１】

以上によりセキュリティポリシーの作成は完了する。本方式のセキュリティポリシー作成支援方法および装置ではさらに、支援装置１１の通信処理部２５８が、ポリシー作成完了時に、事例データ全体あるいは一部をノウハウ管理装置１２に送信する（Ｓ９２８）。

【００６２】

一方、ノウハウ管理装置１２のデータベース自動更新処理部３５３は、受信した事例データの全体、または一部に基づいてノウハウデータベース１３を更新する。

【００６３】

図２１にデータベース自動更新処理部３５３が行う更新処理の手順を示す。図８は更新前後の事例データベース１５、およびノウハウデータベース１３を示す。データベース自動更新処理部３５３は、受信するポリシー事例データの形式に基づいて処理２１１と処理２１２に分岐する。ポリシー事例データ全体（フォーマット６１、６２、６３、６４、６５、６６）を受信した場合、まず受信したデータをポリシー事例データ３４３に保存する（Ｓ３１１１）。次に、受信した事例データが、ノウハウデータベースに登録されている既存データに基づいて作成されたもの（資産ＩＤ８１１に識別子あり）か、ノウハウデータベースに存在せず新規に作成されたもの（資産ＩＤ８１２に“－”あり）かを識別する（Ｓ２１１２２）。次に、事例データが既存データに基づいている場合、ノウハウデータベースの要素実績データ１３３及び要素間リンク実績データ１３４の総使用回数とキーワードが関連する場合の使用回数とを１増加させる。新規作成データである場合、ノウハウデータベースに追加し、新しいＩＤを付与する（Ｓ２１１３）。例えば、図８の場合、資産ＩＤ“０２４”の事例データについては、更新前の資産使用実績記録部８３の総使用回数“１５６"とキーワード”K００１“に関連する使用回数”６３“が、更新後にそれぞれ”１５７“ ”６４“と１ずつ増加する。また、資産ＩＤ”-“の新規作成の事例データについては、資産定義部８２に新規の資産８２１が追加され、資産ＩＤ”１００“が付与され

る。最後に、付与された新規IDを事例データベースに反映させる（Ｓ２１１４）。
【００６４】
例えば、図８の場合、更新前に”-“であった資産ＩＤ８１２が更新後に”１００“となる。ポリシー事例データ個別（フォーマット５１、５２、５３、５４、５５）に受信した場合、受信したポリシー事例データについて、ステップＳ２１１２、２１１３、２１１４を実施する。
【００６５】
これにより、データベースの規模（データ数）とデータ品質を示す指標（使用実績）の信頼性を効率よく向上することができる。
【００６６】
次に、本システムにおけるノウハウ使用に対する課金処理について説明する。
【００６７】
図１７は、本システムを利用するノウハウ提供企業１７１、およびノウハウ利用企業（セキュリティポリシー作成支援サービスを提供する企業あるいはセキュリティポリシーを必要とする顧客企業等）１７２との間におけるノウハウの流れと課金の仕組みを示す図である。
【００６８】
ノウハウ提供企業１７１は、事例データ１７０１を保持している。ノウハウ利用企業１７２は、ノウハウ提供企業１７１が提供する既存事例データ１７０１と新規に作成した新規事例データ１７０２とを合わせてセキュリティポリシーを作成する。そして、ノウハウ利用企業１７２は、新規事例データ１７０２と既存事例データ使用実績１７０３をノウハウ提供企業に提供する。これにより、ノウハウ提供企業１７１はノウハウデータベースの規模（データ数）を拡大できるとともに、事例データの有用度の尺度として利用可能な使用実績データを更新して使用頻度データの信頼性を高めることができる。
【００６９】
これらのノウハウの流れに対して、ノウハウ提供企業１７１は、ノウハウ利用企業１７２に対してノウハウ使用料を請求する。ノウハウ利用企業１７２は、提供を受けたノウハウの有用度に応じた代価を支払う。一方、ノウハウ利用企業１７２が新規事例データを提供したときは、ノウハウ提供企業１７１が、その有用度に応じた対価を支払う。この仕組みにより、ノウハウ利用企業１７２は、より多く、より品質の高い新規事例データを提供することでノウハウ使用料を削減できる。また、ノウハウ提供企業はより多く、より品質の高い事例データを獲得することでノウハウデータベースの品質を高め、より質の高いノウハウを提供できる。
【００７０】
この課金システムにおける課金計算式の一例を、次に示す。
【００７１】
ノウハウ使用料（Ｋ円）＝既存事例データ情報料（Ｋ円／回）×事例データ作成回数…（１）
ノウハウ提供料（Ｋ円）＝新規事項データ情報料（Ｋ円／回）×事例データ作成回数…（２）
提供ノウハウ付加価値料（Ｋ円）＝付加価値料（Ｋ円／回）×新規事例データ合計使用回数…（３）
課金額（Ｋ円）＝ノウハウ使用料－ノウハウ提供料－提供ノウハウ付加価値料…（４）
【００７２】
ここで、既存事例データ情報料、新規事例データ情報料および付加価値料は、予め設定しておく。ポリシー事例作成回数およびポリシー事例提供回数は利用者管理データベース１６に記録される。また、ノウハウデータベース１３にノウハウデータを記録する場合、それぞれのデータ登録者ID（５１６、５２６、５３６、５４６、５５６）を記録し、各データ登録者ID毎のノウハウデータ使用回数（５１２、５２２、５３２、５４２、５５２）の総和を新規事例データ合計使用回数とすることにより、課金額を計算できる。

【００７３】
これにより、作成結果のポリシー事例データのノウハウデータベースへの提供回数、提供データ数、および、提供データの利用頻度に基づいてノウハウ使用に対する課金を減額することができる。その結果、事例データの提供と、利用頻度が高い高品質なセキュリティポリシーの作成を促進することができる。さらに、ユーザ（課金支払い者）のセキュリティポリシー作成コストを削減できると同時に、ノウハウデータベースの拡充・高品質化を図ることができる。
【００７４】
次に、本発明の第二の実施形態について説明する。第二の実施形態は、ポリシー作成支援装置１１がネットワーク上の配置したノウハウデータベースにアクセスすることなく単独で動作する形態である。
【００７５】
図２０は、セキュリティポリシー作成支援システムの第二の実施形態の構成を示す図である。第二の実施形態における支援装置１１は、図２に示す構成に加えて、FDD、CD-ROM、DVD等の外部記憶媒体を制御する外部記憶媒体制御部２０１を備え、外部記憶装置２４にはノウハウデータベース管理機能付きのポリシー作成支援プログラム２０２、ノウハウデータ３４４、利用者管理データ３４５が格納される。なお、ポリシー作成支援プログラム２０２、ノウハウデータ３４４、利用者管理データ３４５は、ネットワーク経由または外部記憶媒体２０３経由で別途読み込まれる。ただし、ノウハウデータ３４４、利用者管理データ３４５は、支援装置に接続された外部記憶媒体２０３上に格納された状態でもよい。さらに、ディスク上のプログラムを実行することにより、ＣＰＵ上２１には図に示す各処理部が実現される。
【００７６】
支援装置１１が図２０に示す構成の場合、図９に示すポリシー作成支援装置―ノウハウ管理装置間のネットワーク経由の処理全体を、内部バス２３を介した支援装置１１内部の処理として置き換えることができる。
【００７７】
また、作成結果のポリシー事例データをネットワーク経由または外部記憶媒体２０３経由でノウハウ管理装置１２に送り込むことにより、第二の実施形態においても、ノウハウ管理装置１２に接続されるノウハウデータベースを更新可能であり、それに伴う課金の仕組み（図１７）もまた実現可能である。
【００７８】
以上説明した実施形態によれば、資産、脅威、対策の各要素間の対応関係情報を設けることにより、各要素間の対応関係を常に維持することが可能となる。これにより、抜け漏れのないセキュリティに関する対策を策定できる。
【００７９】
さらに、資産、脅威、対策の各要素データの使用実績データを備えることにより、使用回数の多い事例データを、多くのセキュリティポリシーの作成に利用されるより重要なデータとして、優先的に利用することができる。加えて、各要素間リンクの使用実績データを設けることにより、使用頻度の高い対応関係を、より結び付きの強い重要な関係であるとして優先的に利用することができる。
【００８０】
また、対象システムの特徴を表すキーワードを利用してポリシー事例データの雛型を作成することにより、対象システムに適した雛型をベースにして効率よくセキュリティポリシーを策定できる。
【００８１】
上述した本発明の実施形態は、本発明の説明のための例示であり、本発明の範囲をそれらの実施形態にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施することができる。
【００８２】

【発明の効果】
本発明によれば、ノウハウを有しない者であっても、対象となる情報システムに適したセキュリティに関する対策の決定、あるいはセキュリティポリシーを作成することができる。
【図面の簡単な説明】
【図１】本発明を適用した第一の実施形態に係るセキュリティポリシー作成支援システムの全体構成を示す図である。
【図２】支援装置１１の詳細な構成を示す図である。
【図３】ノウハウ管理装置１２の詳細な構成を示す図である。
【図４】ノウハウデータベース１３が有するデータ項目を示す図である。
【図５】ノウハウデータベース１３が有するデータ項目を示す図である。
【図６】事例データベース１５が有するデータ項目を示す図である。
【図７】利用者データベース１６が有するデータ項目を示す図である。
【図８】事例データベース１５およびノウハウデータベース１３の更新前後の様子を示す図である。
【図９】標準的なセキュリティポリシー作成手順を示すフローチャートである。
【図１０】セキュリティポリシー適用対象のキーワード情報入力画面１００を示す図である。
【図１１】資産の定義画面１１０を示す図である。
【図１２】追加／編集画面１２０を示す図である。
【図１３】脅威抽出・リスク評価画面１３０を示す図である。
【図１４】対策決定・コスト設定画面１４０を示す図である。
【図１５】対策立案・コスト設定画面１５０を示す図である。
【図１６】対策選択画面１６０を示す図である。
【図１７】本実施形態におけるノウハウの流れと課金の仕組みを示す図である。
【図１８】メニュー画面の例を示す図である。
【図１９】雛形作成の詳細な処理手順を示すフローチャートである。
【図２０】本発明を適用した第二の実施形態に係るセキュリティポリシー作成支援システムの全体構成を示す図である。
【図２１】データベース自動更新処理部３５３が行う更新処理の手順を示すフローチャートである。
【図２２】ログイン２２０画面を示す図である。
【符号の説明】
１１…セキュリティポリシー作成支援装置、１２…ノウハウ提供装置、１３…ノウハウデータベース、１５…事例データベース、１６…利用者データベース、１３１…要素データ、１３２…要素間リンクデータ、１３３…要素実績データ、１３４…要素間リンク実績データ、１３５…キーワードデータ。

【図１】

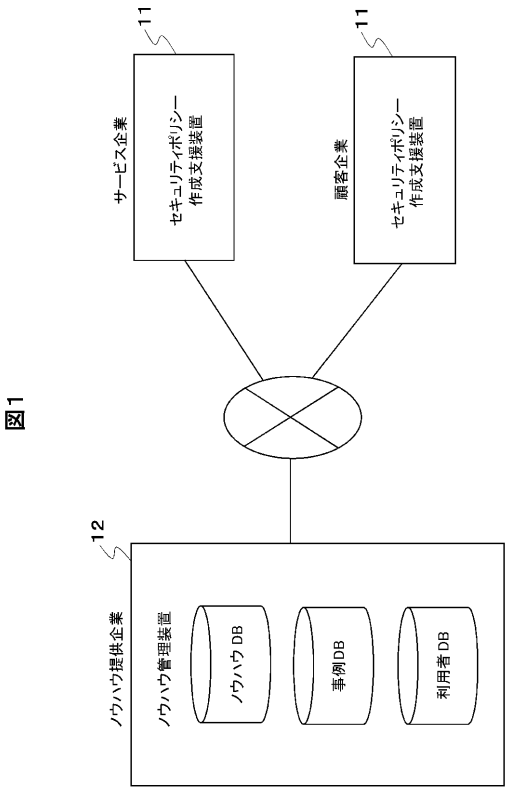
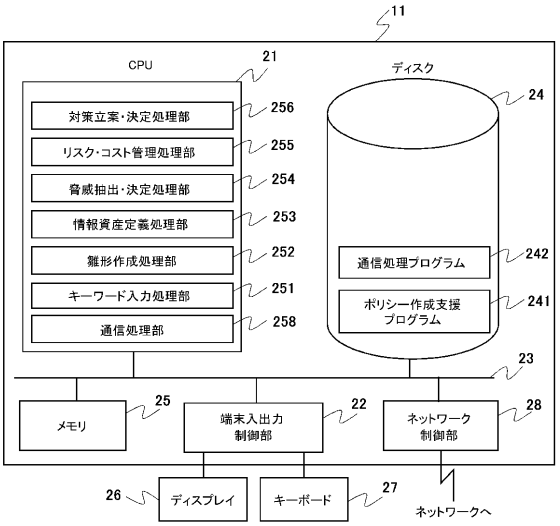


図1

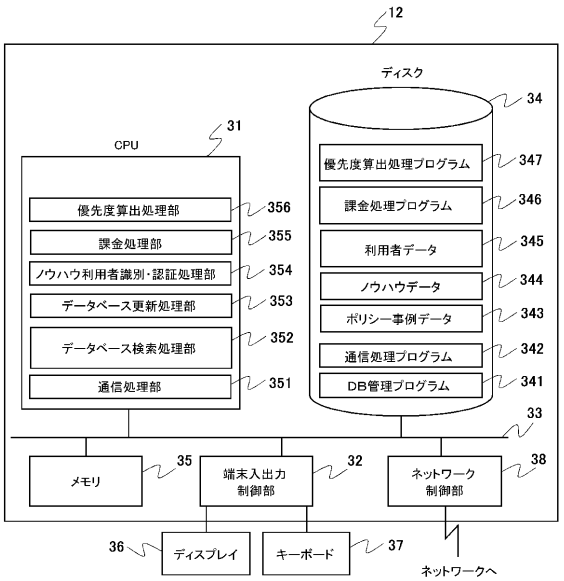
【図２】

図2



【図３】

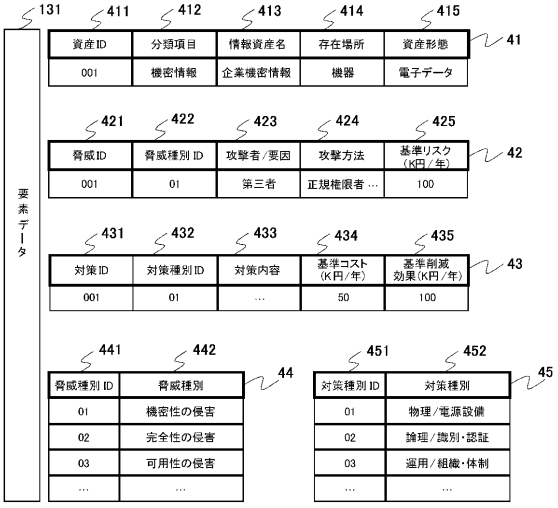
図3



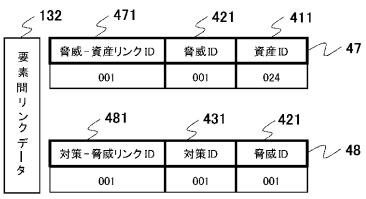
【図４】

図4

(a)



(b)



【図５】

図5

(a)

133 要素実績データ

411 資産ID	512 総使用回数	513 キーワード	514 使用回数	[キーワード,使用回数],…	516 データ登録者ID
001	123	K001	32	…	AAA

51

421 脅威ID	522 総使用回数	523 キーワード	524 使用回数	[キーワード,使用回数],…	526 データ登録者ID
001	100	K001	38	…	BBB

52

431 対策ID	532 総使用回数	533 キーワード	534 使用回数	[キーワード,使用回数],…	536 データ登録者ID
001	105	K001	42	…	–

53

(b)

134 要素間リンク実績データ

471 脅威-資産リンクID	542 総使用回数	543 キーワード	544 使用回数	[キーワード,使用回数],…	546 データ登録者ID
001	55	K001	4	…	CCC

54

481 対策-脅威リンクID	552 総使用回数	553 キーワード	554 使用回数	[キーワード,使用回数],…	556 データ登録者ID
001	29	K001	18	…	–

55

(c)

135 キーワードデータ

561 キーワードID	562 キーワード	563 上位キーワードID	
K001	金融	–	–
K002	証券	–	–
K003	ATMシステム	K001	–
K004	自動振替システム	K001	K002

【図６】

図6

(a)

対象システム

601 事例ID	602 適用対象固有情報（業種,対象部門,対象システム,情報資産等）=キーワード				603 作成者ID
ABC_1	金融	口座振替システム	プライバシー情報		AAA

61

(b)

参考データ

621 資産事例ID	622 具体的資産名	411 資産ID	6211 分類項目	412 情報資産名	413 存在場所	414 資産形態	415
ABC_1-A01	顧客プライバシー情報	024	プライバシー情報	顧客情報	機器	電子データ	62
ABC_1-A02	全社経営情報	–	機密情報	経営情報	機器	電子データ	

6212

631 脅威事例ID	632 具体的脅威記述	633 設定リスク(K円/年)	421 脅威ID	422 脅威種別	423 攻撃者/要因	424 攻撃方法	63
ABC_1-T01	顧客情報の管理者を騙して…	1000	011	機密性	第三者	…	
ABC_1-T02	システム管理者のふりを…	100	–	機密性	内部者	…	

641 対策事例ID	642 具体的対策記述	643 設定コスト(K円/年)	644 リスク削減効果(%/年)	431 対策ID	432 対策種別ID	433 対策内容	64
ABC_1-P01	…	50	10	033	001	…	
ABC_1-P02	…	100	20	–	001	…	

(c)

要素間リンクデータ

651 脅威-資産事例リンクID	631 脅威事例ID	621 資産事例ID	471 脅威-資産リンクID	65
ABC_1-TA01	ABC_1-T02	ABC_1-A01	005	
ABC_1-TA02	ABC_1-T05	ABC_1-A03	–	

661 対策-脅威事例リンクID	641 対策事例ID	631 脅威事例ID	481 対策-脅威リンクID	66
ABC_1-PT01	ABC_1-P01	ABC_1-T01	023	
ABC_1-PT02	ABC_1-P01	ABC_1-T03	–	

【図７】

図7

71

711 ユーザID	712 パスワード	713 ユーザ詳細情報	714 課金総額(K円)	715 ポリシー事例作成回数	716 ポリシー事例提供回数	717 ポリシー事例データ利用回数総和
AAA	********	AAAコンサル	700	4	3	500
BBB	********	BBB SI会社	-200	1	1	300
CCC	********	CCC銀行	900	2	0	50

【図８】

図8

ノウハウデータベース 13

82

資産ID	情報資産名	存在場所	資産形態
…	…	…	…
099	メールサーバ	システム室	ハードウェア

83

資産ID	総使用回数	キーワード	使用回数
024	156	K001	63

831 832

82

資産ID	情報資産名	存在場所	資産形態
…	…	…	…
099	企業機密情報	機器	電子データ
100	経営情報	機器	電子データ

821

83

資産ID	総使用回数	キーワード	使用回数
024	157	K001	64

833 834

事例データベース 15

811

81

更新前

資産事例ID	具体的資産名	資産ID	情報資産名	存在場所	資産形態
ABC_1-A01	顧客プライバシー情報	024	プライバシー情報	機器	電子データ
ABC_1-A02	全社経営情報	–	経営情報	機器	電子データ

812 813 814 815

81

更新後

資産事例ID	具体的資産名	資産ID	情報資産名	存在場所	資産形態
ABC_1-A01	顧客プライバシー情報	024	プライバシー情報	機器	電子データ
ABC_1-A02	全社経営情報	100	経営情報	機器	電子データ

816

【図９】

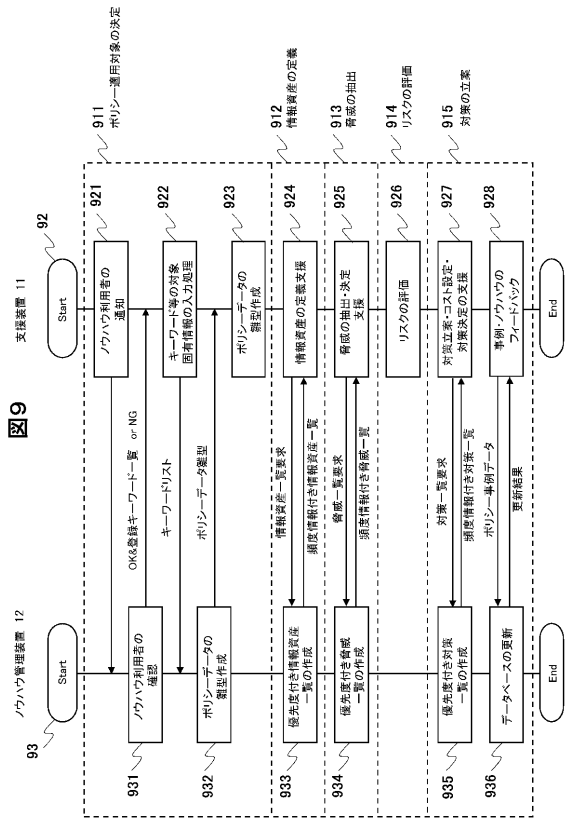
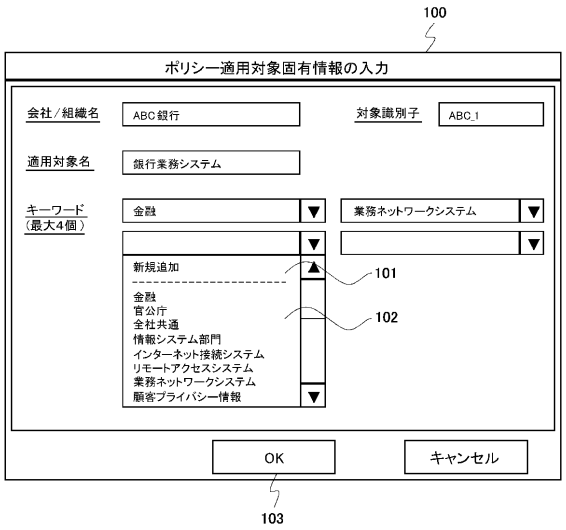


図9

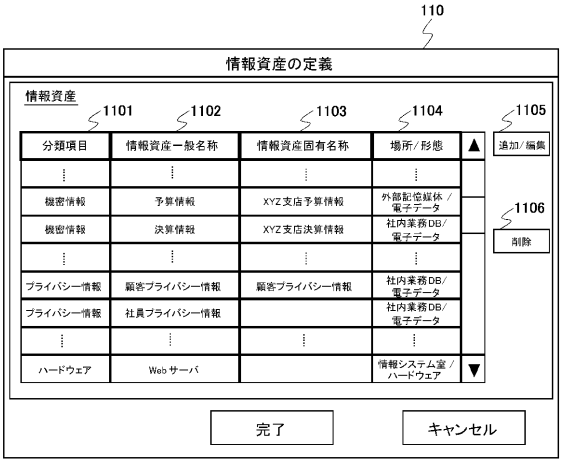
【図１０】

図10



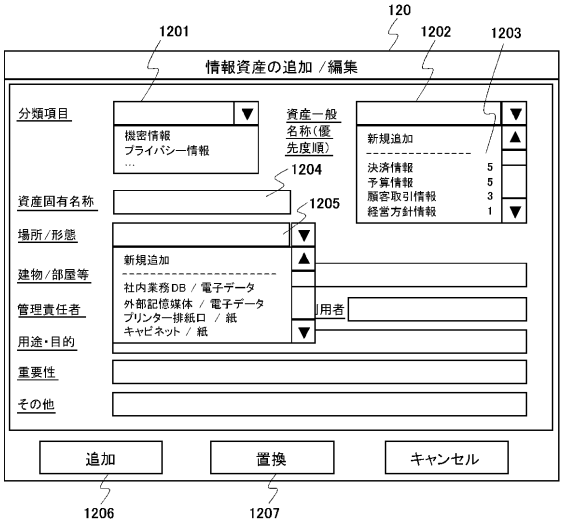
【図１１】

図11



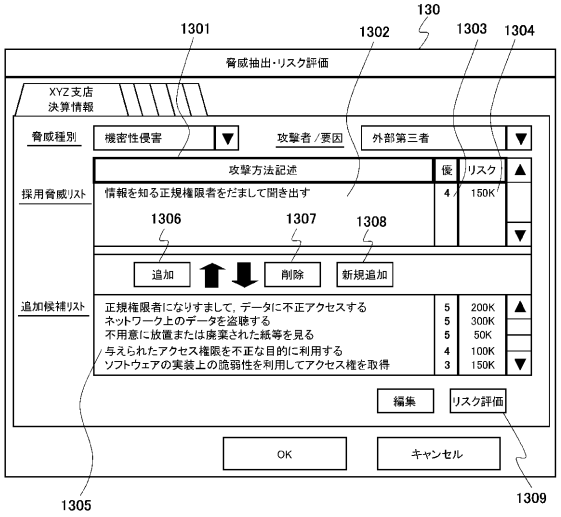
【図１２】

図12



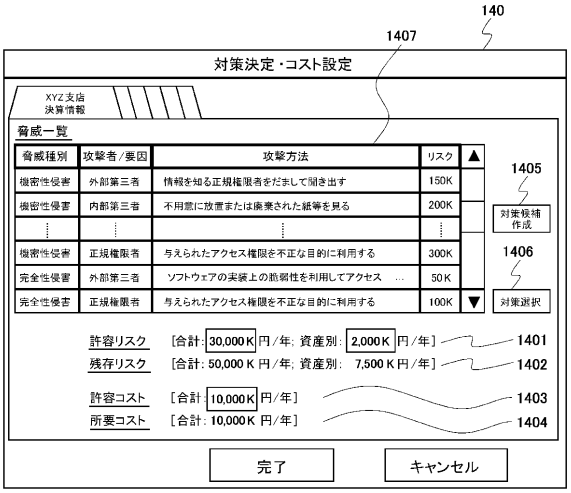
【図１３】

図13



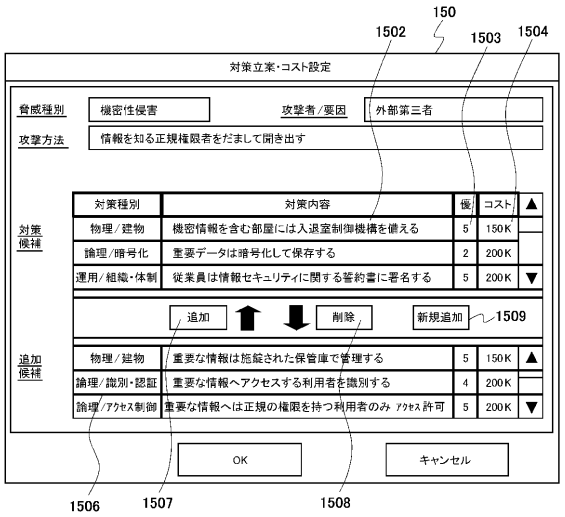
【図１４】

図14



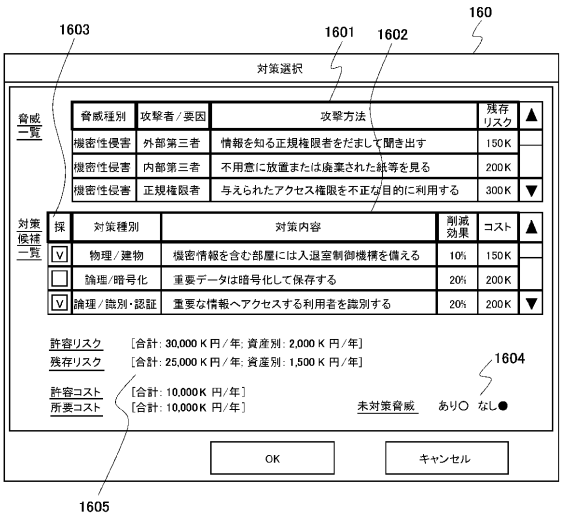
【図１５】

図15



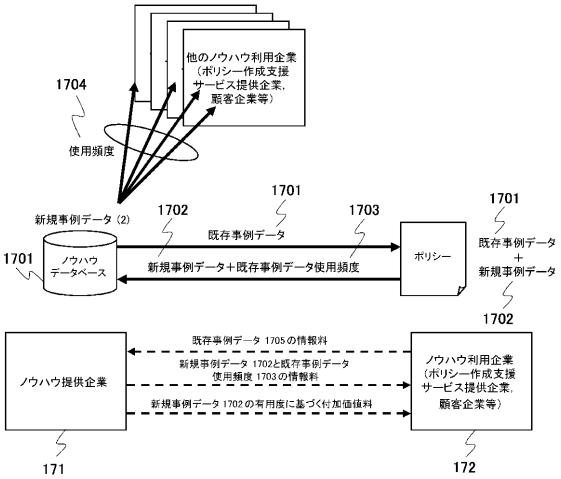
【図１６】

図16



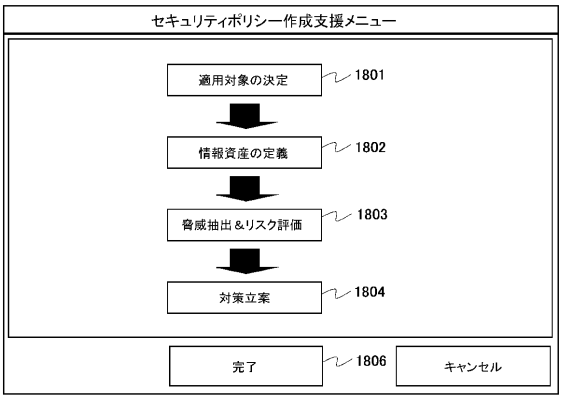
【図１７】

図17



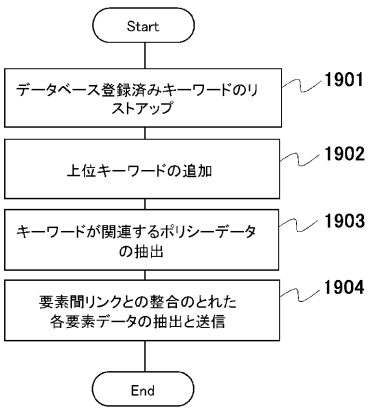
【図１８】

図18



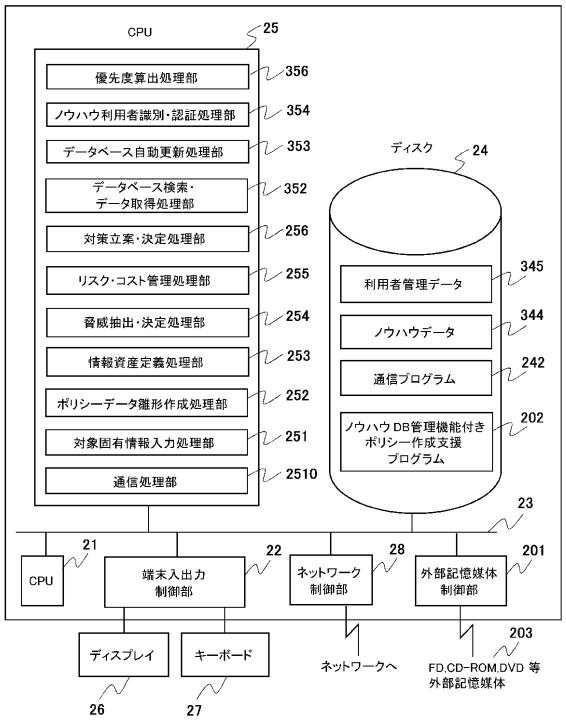
【図１９】

図19



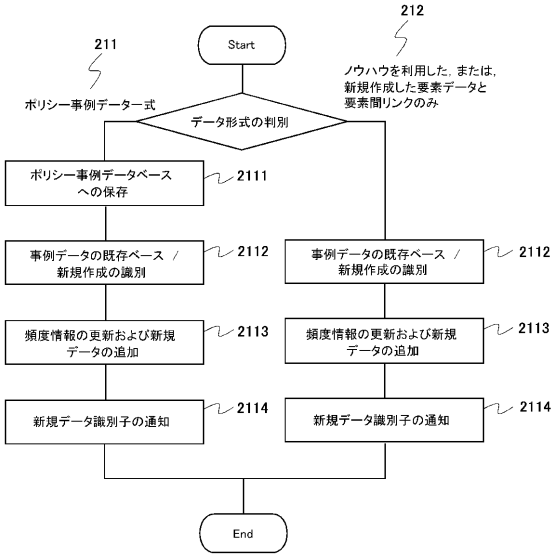
【図２０】

図20



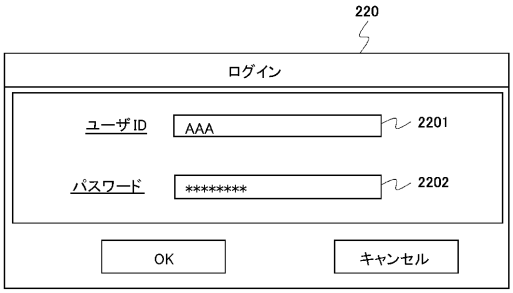
【図２１】

図21



【図２２】

図22



フロントページの続き

(72)発明者 諸橋 政幸
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内
(72)発明者 相羽 律子
神奈川県川崎市幸区鹿島田８９０番地 株式会社日立製作所 情報サービス事業部内

審査官 金子 幸一

(56)参考文献 特開２００１－１０１１３５（ＪＰ，Ａ）
特開２００１－１５５０８１（ＪＰ，Ａ）
特開平０９－２４５０４６（ＪＰ，Ａ）
萱島 信，石田育士，ポリシーベースセキュリティ構築支援システムの提案，情報処理学会研究報告，日本，社団法人情報処理学会，２００１年 2月２１日，第２００１巻，第１５号，第１９－２４頁
永井康彦，藤山達也，佐々木良一，セキュリティ対策目標尾の最適決定技法の提案，情報処理学会論文誌，日本，社団法人情報処理学会，２０００年 8月１５日，第４１巻，第8号，第２２６４－２２７１頁
小澤隆一，小熊圭一郎，雨宮俊一，セキュリティポリシー実現へのステップ，ＩＮＴＥＲＯＰ ＭＡＧＡＺＩＮＥ，日本，ソフトバンクパブリッシング株式会社，２０００年１０月 1日，第１０巻，第１０号，第１５２－１５６頁

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q 10/00
G06F 21/20