

(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.C1.

F 1

G06Q 10/00 (2006.01)
G06F 21/20 (2006.01)G06F 17/60 174
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、

10

20

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

10

20

30

40

50

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。

10

【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、

20

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、

30

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 每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、

40

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

50

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。

10

20

30

40

50

【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】

10

20

30

40

50

【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 (GM ITS: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

10

20

30

40

50

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。

10

【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】

以下、本発明の実施形態について、図面を用いて説明する。

20

【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。

30

【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。

40

【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

50

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、CPU 31 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。CPU 10 31 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、CPU 31 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。

20

【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 ID 411 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。

30

【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 ID 421 と、脅威の種別を識別するための脅威種別 ID 422 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、隨時、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 ID 431 と、対策の種別を識別するための対策種別 ID 432 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、隨時、更新することができる。

40

【0023】

脅威の種別を定義する定義情報 44 は、脅威種別 ID 441 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 ID 451 と、対策種別 452 とを対応

50

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。 10

【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。 20

【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。 30

【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。 40

【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 50

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)

10

20

30

40

50

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形をする(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、雛形データの場合、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形一覧を表示させる。ユーザは、この画面110を利用して、雛形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

10

20

30

40

50

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離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、脅威離型一覧をユーザに提示する。ここで示された脅威の離型をベースに、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に脅威の離型が表示され、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

10

20

30

40

50

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”的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。

10

【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。

20

【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。

30

【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）

40

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。

50

【 0 0 7 3 】

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。

【 0 0 7 4 】

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。 10

【 0 0 7 5 】

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。 20

【 0 0 7 6 】

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。 30

【 0 0 7 7 】

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。 30

【 0 0 7 8 】

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。

【 0 0 7 9 】

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。 40

【 0 0 8 0 】

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。

【 0 0 8 1 】

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。

【 0 0 8 2 】

【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。 10

【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。 20

【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。 30

【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】

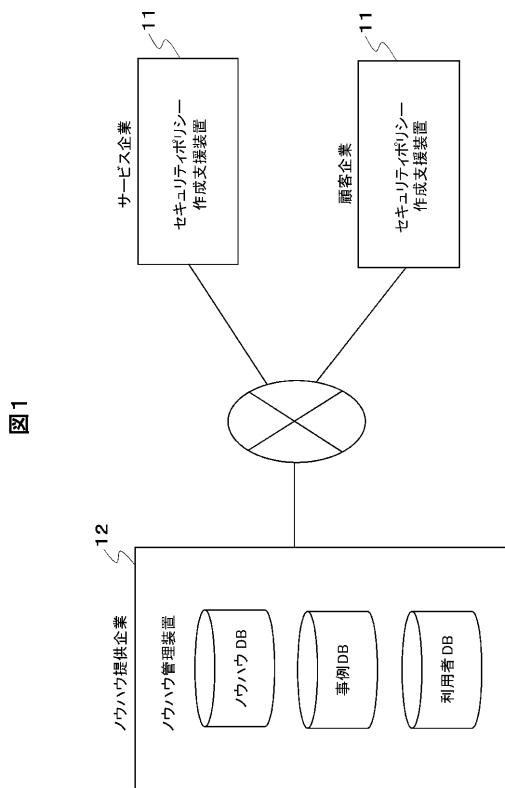
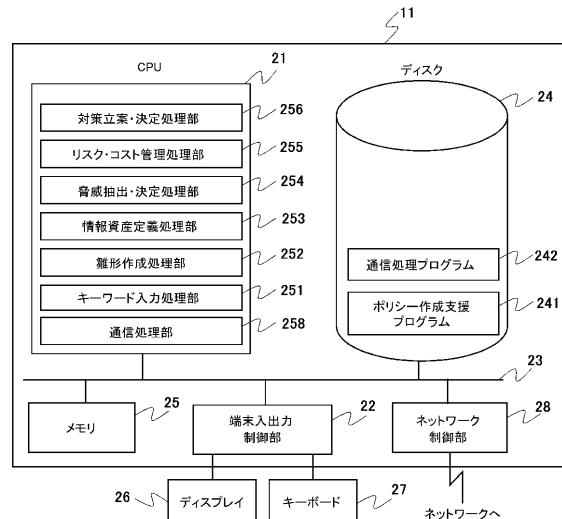


図1

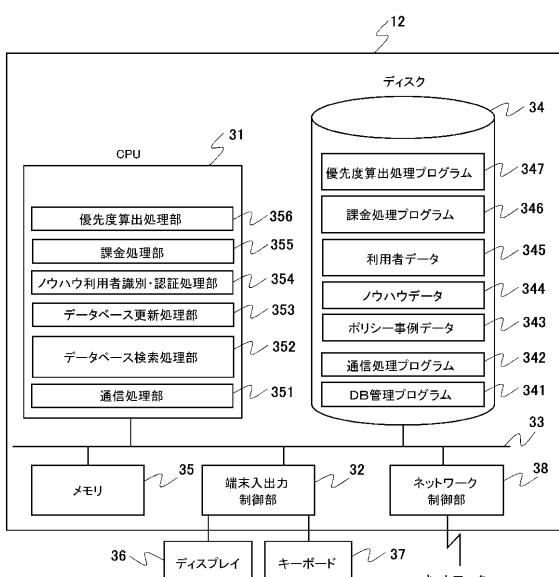
【図2】

図2



【図3】

図3

36 37
ネットワークへ

【図4】

図4

(a)

資産ID	分類項目	情報資産名	存在場所	資産形態
001	機密情報	企業機密情報	機器	電子データ

脅威ID	脅威種別ID	攻撃者/要因	攻撃方法	基準リスク(万円/年)
001	01	第三者	正規権限者	100

対策ID	対策種別ID	対策内容	基準コスト(万円/年)	基準削減効果(万円/年)
001	01	...	50	100

脅威種別ID	脅威種別
01	機密性の侵害
02	完全性の侵害
03	可用性の侵害
...	...

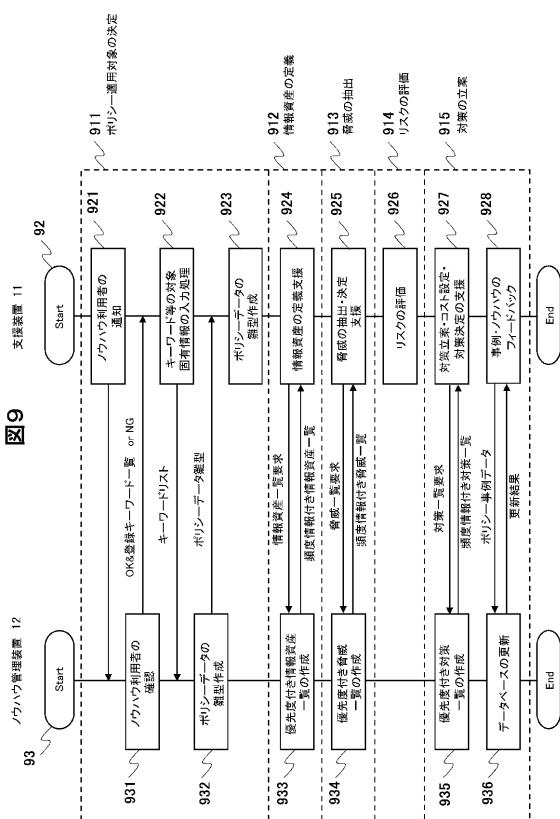
対策種別ID	対策種別
01	物理/電源設備
02	論理/識別・認証
03	運用/組織・体制
...	...

(b)

脅威-資産リンクID	脅威ID	資産ID
001	001	024

対策-脅威リンクID	対策ID	脅威ID
001	001	001

【 図 9 】



【 図 1 1 】

图 11

情報資産の定義				
分類項目	情報資産一般名称	情報資産固有名称	場所/形態	▲ 追加/編集 ▼ 削除
機密情報	予算情報	XYZ支店予算情報	外部記憶媒体/ 電子データ	
機密情報	決算情報	XYZ支店決算情報	社内業務DB/ 電子データ	
プライバシー情報	顧客プライバシー情報	顧客プライバシー情報	社内業務DB/ 電子データ	
プライバシー情報	社員プライバシー情報		社内業務DB/ 電子データ	
ハードウェア	Web サーバ		情報システム室/ ハードウェア	

【 図 1 0 】

図10

100

ポリシー適用対象固有情報の入力

S

会社／組織名	ABC銀行	対象識別子
適用対象名	銀行業務システム	ABC_1
キーワード (最大4個)	金融	業務ネットワークシステム
	新規追加	
	金融 官公庁 全社共通 情報システム部門 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 業務ネットワークシステム 顧客プライバシー情報	101 102
OK		キャンセル

S

103

【 図 1 2 】

図12

情報資産の追加 / 編集

<p>分類項目</p> <p>機密情報 プライバシー情報 ...</p> <p>資産固有名</p> <p>場所・形態</p> <p>建物・部屋等</p> <p>管理責任者</p> <p>用途・目的</p> <p>重要性</p> <p>その他</p>	<p>資産一般</p> <p>名前(権限) 先度順</p> <p>新規追加</p> <p>決済情報 5 予算情報 5 顧客取引情報 3 経営方針情報 1</p> <p>新規追加</p> <p>社内業務DB / 電子データ 外部記憶媒体 / 電子データ プリンター-排紙口 / 紙 キヤビネット / 紙</p> <p>用者</p>	<p>1201</p> <p>1202</p> <p>1203</p> <p>1204</p> <p>1205</p> <p>1206</p> <p>1207</p> <p>1208</p> <p>1209</p> <p>1210</p> <p>1211</p> <p>1212</p> <p>1213</p> <p>1214</p> <p>1215</p> <p>1216</p> <p>1217</p> <p>1218</p> <p>1219</p> <p>1220</p> <p>1221</p> <p>1222</p> <p>1223</p> <p>1224</p> <p>1225</p> <p>1226</p> <p>1227</p> <p>1228</p> <p>1229</p> <p>1230</p> <p>1231</p> <p>1232</p> <p>1233</p> <p>1234</p> <p>1235</p> <p>1236</p> <p>1237</p> <p>1238</p> <p>1239</p> <p>1240</p> <p>1241</p> <p>1242</p> <p>1243</p> <p>1244</p> <p>1245</p> <p>1246</p> <p>1247</p> <p>1248</p> <p>1249</p> <p>1250</p> <p>1251</p> <p>1252</p> <p>1253</p> <p>1254</p> <p>1255</p> <p>1256</p> <p>1257</p> <p>1258</p> <p>1259</p> <p>1260</p> <p>1261</p> <p>1262</p> <p>1263</p> <p>1264</p> <p>1265</p> <p>1266</p> <p>1267</p> <p>1268</p> <p>1269</p> <p>1270</p> <p>1271</p> <p>1272</p> <p>1273</p> <p>1274</p> <p>1275</p> <p>1276</p> <p>1277</p> <p>1278</p> <p>1279</p> <p>1280</p> <p>1281</p> <p>1282</p> <p>1283</p> <p>1284</p> <p>1285</p> <p>1286</p> <p>1287</p> <p>1288</p> <p>1289</p> <p>1290</p> <p>1291</p> <p>1292</p> <p>1293</p> <p>1294</p> <p>1295</p> <p>1296</p> <p>1297</p> <p>1298</p> <p>1299</p> <p>1300</p> <p>1301</p> <p>1302</p> <p>1303</p> <p>1304</p> <p>1305</p> <p>1306</p> <p>1307</p> <p>1308</p> <p>1309</p> <p>1310</p> <p>1311</p> <p>1312</p> <p>1313</p> <p>1314</p> <p>1315</p> <p>1316</p> <p>1317</p> <p>1318</p> <p>1319</p> <p>1320</p> <p>1321</p> <p>1322</p> <p>1323</p> <p>1324</p> <p>1325</p> <p>1326</p> <p>1327</p> <p>1328</p> <p>1329</p> <p>1330</p> <p>1331</p> <p>1332</p> <p>1333</p> <p>1334</p> <p>1335</p> <p>1336</p> <p>1337</p> <p>1338</p> <p>1339</p> <p>1340</p> <p>1341</p> <p>1342</p> <p>1343</p> <p>1344</p> <p>1345</p> <p>1346</p> <p>1347</p> <p>1348</p> <p>1349</p> <p>1350</p> <p>1351</p> <p>1352</p> <p>1353</p> <p>1354</p> <p>1355</p> <p>1356</p> <p>1357</p> <p>1358</p> <p>1359</p> <p>1360</p> <p>1361</p> <p>1362</p> <p>1363</p> <p>1364</p> <p>1365</p> <p>1366</p> <p>1367</p> <p>1368</p> <p>1369</p> <p>1370</p> <p>1371</p> <p>1372</p> <p>1373</p> <p>1374</p> <p>1375</p> <p>1376</p> <p>1377</p> <p>1378</p> <p>1379</p> <p>1380</p> <p>1381</p> <p>1382</p> <p>1383</p> <p>1384</p> <p>1385</p> <p>1386</p> <p>1387</p> <p>1388</p> <p>1389</p> <p>1390</p> <p>1391</p> <p>1392</p> <p>1393</p> <p>1394</p> <p>1395</p> <p>1396</p> <p>1397</p> <p>1398</p> <p>1399</p> <p>1400</p> <p>1401</p> <p>1402</p> <p>1403</p> <p>1404</p> <p>1405</p> <p>1406</p> <p>1407</p> <p>1408</p> <p>1409</p> <p>1410</p> <p>1411</p> <p>1412</p> <p>1413</p> <p>1414</p> <p>1415</p> <p>1416</p> <p>1417</p> <p>1418</p> <p>1419</p> <p>1420</p> <p>1421</p> <p>1422</p> <p>1423</p> <p>1424</p> <p>1425</p> <p>1426</p> <p>1427</p> <p>1428</p> <p>1429</p> <p>1430</p> <p>1431</p> <p>1432</p> <p>1433</p> <p>1434</p> <p>1435</p> <p>1436</p> <p>1437</p> <p>1438</p> <p>1439</p> <p>1440</p> <p>1441</p> <p>1442</p> <p>1443</p> <p>1444</p> <p>1445</p> <p>1446</p> <p>1447</p> <p>1448</p> <p>1449</p> <p>1450</p> <p>1451</p> <p>1452</p> <p>1453</p> <p>1454</p> <p>1455</p> <p>1456</p> <p>1457</p> <p>1458</p> <p>1459</p> <p>1460</p> <p>1461</p> <p>1462</p> <p>1463</p> <p>1464</p> <p>1465</p> <p>1466</p> <p>1467</p> <p>1468</p> <p>1469</p> <p>1470</p> <p>1471</p> <p>1472</p> <p>1473</p> <p>1474</p> <p>1475</p> <p>1476</p> <p>1477</p> <p>1478</p> <p>1479</p> <p>1480</p> <p>1481</p> <p>1482</p> <p>1483</p> <p>1484</p> <p>1485</p> <p>1486</p> <p>1487</p> <p>1488</p> <p>1489</p> <p>1490</p> <p>1491</p> <p>1492</p> <p>1493</p> <p>1494</p> <p>1495</p> <p>1496</p> <p>1497</p> <p>1498</p> <p>1499</p> <p>1500</p> <p>1501</p> <p>1502</p> <p>1503</p> <p>1504</p> <p>1505</p> <p>1506</p> <p>1507</p> <p>1508</p> <p>1509</p> <p>1510</p> <p>1511</p> <p>1512</p> <p>1513</p> <p>1514</p> <p>1515</p> <p>1516</p> <p>1517</p> <p>1518</p> <p>1519</p> <p>1520</p> <p>1521</p> <p>1522</p> <p>1523</p> <p>1524</p> <p>1525</p> <p>1526</p> <p>1527</p> <p>1528</p> <p>1529</p> <p>1530</p> <p>1531</p> <p>1532</p> <p>1533</p> <p>1534</p> <p>1535</p> <p>1536</p> <p>1537</p> <p>1538</p> <p>1539</p> <p>1540</p> <p>1541</p> <p>1542</p> <p>1543</p> <p>1544</p> <p>1545</p> <p>1546</p> <p>1547</p> <p>1548</p> <p>1549</p> <p>1550</p> <p>1551</p> <p>1552</p> <p>1553</p> <p>1554</p> <p>1555</p> <p>1556</p> <p>1557</p> <p>1558</p> <p>1559</p> <p>1560</p> <p>1561</p> <p>1562</p> <p>1563</p> <p>1564</p> <p>1565</p> <p>1566</p> <p>1567</p> <p>1568</p> <p>1569</p> <p>1570</p> <p>1571</p> <p>1572</p> <p>1573</p> <p>1574</p> <p>1575</p> <p>1576</p> <p>1577</p> <p>1578</p> <p>1579</p> <p>1580</p> <p>1581</p> <p>1582</p> <p>1583</p> <p>1584</p> <p>1585</p> <p>1586</p> <p>1587</p> <p>1588</p> <p>1589</p> <p>1590</p> <p>1591</p> <p>1592</p> <p>1593</p> <p>1594</p> <p>1595</p> <p>1596</p> <p>1597</p> <p>1598</p> <p>1599</p> <p>1600</p> <p>1601</p> <p>1602</p> <p>1603</p> <p>1604</p> <p>1605</p> <p>1606</p> <p>1607</p> <p>1608</p> <p>1609</p> <p>1610</p> <p>1611</p> <p>1612</p> <p>1613</p> <p>1614</p> <p>1615</p> <p>1616</p> <p>1617</p> <p>1618</p> <p>1619</p> <p>1620</p> <p>1621</p> <p>1622</p> <p>1623</p> <p>1624</p> <p>1625</p> <p>1626</p> <p>1627</p> <p>1628</p> <p>1629</p> <p>1630</p> <p>1631</p> <p>1632</p> <p>1633</p> <p>1634</p> <p>1635</p> <p>1636</p> <p>1637</p> <p>1638</p> <p>1639</p> <p>1640</p> <p>1641</p> <p>1642</p> <p>1643</p> <p>1644</p> <p>1645</p> <p>1646</p> <p>1647</p> <p>1648</p> <p>1649</p> <p>1650</p> <p>1651</p> <p>1652</p> <p>1653</p> <p>1654</p> <p>1655</p> <p>1656</p> <p>1657</p> <p>1658</p> <p>1659</p> <p>1660</p> <p>1661</p> <p>1662</p> <p>1663</p> <p>1664</p> <p>1665</p> <p>1666</p> <p>1667</p> <p>1668</p> <p>1669</p> <p>1670</p> <p>1671</p> <p>1672</p> <p>1673</p> <p>1674</p> <p>1675</p> <p>1676</p> <p>1677</p> <p>1678</p> <p>1679</p> <p>1680</p> <p>1681</p> <p>1682</p> <p>1683</p> <p>1684</p> <p>1685</p> <p>1686</p> <p>1687</p> <p>1688</p> <p>1689</p> <p>1690</p> <p>1691</p> <p>1692</p> <p>1693</p> <p>1694</p> <p>1695</p> <p>1696</p> <p>1697</p> <p>1698</p> <p>1699</p> <p>1700</p> <p>1701</p> <p>1702</p> <p>1703</p> <p>1704</p> <p>1705</p> <p>1706</p> <p>1707</p> <p>1708</p> <p>1709</p> <p>1710</p> <p>1711</p> <p>1712</p> <p>1713</p> <p>1714</p> <p>1715</p> <p>1716</p> <p>1717</p> <p>1718</p> <p>1719</p> <p>1720</p> <p>1721</p> <p>1722</p> <p>1723</p> <p>1724</p> <p>1725</p> <p>1726</p> <p>1727</p> <p>1728</p> <p>1729</p> <p>1730</p> <p>1731</p> <p>1732</p> <p>1733</p> <p>1734</p> <p>1735</p> <p>1736</p> <p>1737</p> <p>1738</p> <p>1739</p> <p>1740</p> <p>1741</p> <p>1742</p> <p>1743</p> <p>1744</p> <p>1745</p> <p>1746</p> <p>1747</p> <p>1748</p> <p>1749</p> <p>1750</p> <p>1751</p> <p>1752</p> <p>1753</p> <p>1754</p> <p>1755</p> <p>1756</p> <p>1757</p> <p>1758</p> <p>1759</p> <p>1760</p> <p>1761</p> <p>1762</p> <p>1763</p> <p>1764</p> <p>1765</p> <p>1766</p> <p>1767</p> <p>1768</p> <p>1769</p> <p>1770</p> <p>1771</p> <p>1772</p> <p>1773</p> <p>1774</p> <p>1775</p> <p>1776</p> <p>1777</p> <p>1778</p> <p>1779</p> <p>1780</p> <p>1781</p> <p>1782</p> <p>1783</p> <p>1784</p> <p>1785</p> <p>1786</p> <p>1787</p> <p>1788</p> <p>1789</p> <p>1790</p> <p>1791</p> <p>1792</p> <p>1793</p> <p>1794</p> <p>1795</p> <p>1796</p> <p>1797</p> <p>1798</p> <p>1799</p> <p>1800</p> <p>1801</p> <p>1802</p> <p>1803</p> <p>1804</p> <p>1805</p> <p>1806</p> <p>1807</p> <p>1808</p> <p>1809</p> <p>1810</p> <p>1811</p> <p>1812</p> <p>1813</p> <p>1814</p> <p>1815</p> <p>1816</p> <p>1817</p> <p>1818</p> <p>1819</p> <p>1820</p> <p>1821</p> <p>1822</p> <p>1823</p> <p>1824</p> <p>1825</p> <p>1826</p> <p>1827</p> <p>1828</p> <p>1829</p> <p>1830</p> <p>1831</p> <p>1832</p> <p>1833</p> <p>1834</p> <p>1835</p> <p>1836</p> <p>1837</p> <p>1838</p> <p>1839</p> <p>1840</p> <p>1841</p> <p>1842</p> <p>1843</p> <p>1844</p> <p>1845</p> <p>1846</p> <p>1847</p> <p>1848</p> <p>1849</p> <p>1850</p> <p>1851</p> <p>1852</p> <p>1853</p> <p>1854</p> <p>1855</p> <p>1856</p> <p>1857</p> <p>1858</p> <p>1859</p> <p>1860</p> <p>1861</p> <p>1862</p> <p>1863</p> <p>1864</p> <p>1865</p> <p>1866</p> <p>1867</p> <p>1868</p> <p>1869</p> <p>1870</p> <p>1871</p> <p>1872</p> <p>1873</p> <p>1874</p> <p>1875</p> <p>1876</p> <p>1877</p> <p>1878</p> <p>1879</p> <p>1880</p> <p>1881</p> <p>1882</p> <p>1883</p> <p>1884</p> <p>1885</p> <p>1886</p> <p>1887</p> <p>1888</p> <p>1889</p> <p>1890</p> <p>1891</p> <p>1892</p> <p>1893</p> <p>1894</p> <p>1895</p> <p>1896</p> <p>1897</p> <p>1898</p> <p>1899</p> <p>1900</p> <p>1901</p> <p>1902</p> <p>1903</p> <p>1904</p> <p>1905</p> <p>1906</p> <p>1907</p> <p>1908</p> <p>1909</p> <p>1910</p> <p>1911</p> <p>1912</p> <p>1913</p> <p>1914</p> <p>1915</p> <p>1916</p> <p>1917</p> <p>1918</p> <p>1919</p> <p>1920</p> <p>1921</p> <p>1922</p> <p>1923</p> <p>1924</p> <p>1925</p> <p>1926</p> <p>1927</p> <p>1928</p> <p>1929</p> <p>1930</p> <p>1931</p> <p>1932</p> <p>1933</p> <p>1934</p> <p>1935</p> <p>1936</p> <p>1937</p> <p>1938</p> <p>1939</p> <p>1940</p> <p>1941</p> <p>1942</p> <p>1943</p> <p>1944</p> <p>1945</p> <p>1946</p> <p>1947</p> <p>1948</p> <p>1949</p> <p>1950</p> <p>1951</p> <p>1952</p> <p>1953</p> <p>1954</p> <p>1955</p> <p>1956</p> <p>1957</p> <p>1958</p> <p>1959</p> <p>1960</p> <p>1961</p> <p>1962</p> <p>1963</p> <p>1964</p> <p>1965</p> <p>1966</p> <p>1967</p> <p>1968</p> <p>1969</p> <p>1970</p> <p>1971</p> <p>1972</p> <p>1973</p> <p>1974</p> <p>1975</p> <p>1976</p> <p>1977</p> <p>1978</p> <p>1979</p> <p>1980</p> <p>1981</p> <p>1982</p> <p>1983</p> <p>1984</p> <p>1985</p> <p>1986</p> <p>1987</p> <p>1988</p> <p>1989</p> <p>1990</p> <p>1991</p> <p>1992</p> <p>1993</p> <p>1994</p> <p>1995</p> <p>1996</p> <p>1997</p> <p>1998</p> <p>1999</p> <p>2000</p> <p>2001</p> <p>2002</p> <p>2003</p> <p>2004</p> <p>2005</p> <p>2006</p> <p>2007</p> <p>2008</p> <p>2009</p> <p>2010</p> <p>2011</p> <p>2012</p> <p>2013</p> <p>2014</p> <p>2015</p> <p>2016</p> <p>2017</p> <p>2018</p> <p>2019</p> <p>2020</p> <p>2021</p> <p>2022</p> <p>2023</p> <p>2024</p> <p>2025</p> <p>2026</p> <p>2027</p> <p>2028</p> <p>2029</p> <p>2030</p> <p>2031</p> <p>2032</p> <p>2033</p> <p>2034</p> <p>2035</p> <p>2036</p> <p>2037</p> <p>2038</p> <p>2039</p> <p>2040</p> <p>2041</p> <p>2042</p> <p>2043</p> <p>2044</p> <p>2045</p> <p>2046</p> <p>2047</p> <p>2048</p> <p>2049</p> <p>2050</p> <p>2051</p> <p>2052</p> <p>2053</p> <p>2054</p> <p>2055</p> <p>2056</p> <p>2057</p> <p>2058</p> <p>2059</p> <p>2060</p> <p>2061</p> <p>2062</p> <p>2063</p> <p>2064</p> <p>2065</p> <p>2066</p> <p>2067</p> <p>2068</p> <p>2069</p> <p>2070</p> <p>2071</p> <p>2072</p> <p>2073</p> <p>2074</p> <p>2075</p> <p>2076</p> <p>2077</p> <p>2078</p> <p>2079</p> <p>2080</p> <p>2081</p> <p>2082</p> <p>2083</p> <p>2084</p> <p>2085</p> <p>2086</p> <p>2087</p> <p>2088</p> <p>2089</p> <p>2090</p> <p>2091</p> <p>2092</p> <p>2093</p> <p>2094</p> <p>2095</p> <p>2096</p> <p>2097</p> <p>2098</p> <p>2099</p> <p>2100</p> <p>2101</p> <p>2102</p> <p>2103</p> <p>2104</p> <p>2105</p> <p>2106</p> <p>2107</p> <p>2108</p> <p>2109</p> <p>2110</p> <p>2111</p> <p>2112</p> <p>2113</p> <p>2114</p> <p>2115</p> <p>2116</p> <p>2117</p> <p>2118</p> <p>2119</p> <p>2120</p> <p>2121</p> <p>2122</p> <p>2123</p> <p>2124</p> <p>2125</p> <p>2126</p> <p>2127</p> <p>2128</p> <p>2129</p> <p>2130</p> <p>2131</p> <p>2132</p> <p>2133</p> <p>2134</p> <p>2135</p> <p>2136</p> <p>2137</p> <p>2138</p> <p>2139</p> <p>2140</p> <p>2141</p> <p>2142</p> <p>2143</p> <p>2144</p> <p>2145</p> <p>2146</p> <p>2147</p> <p>2148</p> <p>2149</p> <p>2150</p> <p>2151</p> <p>2152</p> <p>2153</p> <p>2154</p> <p>2155</p> <p>2156</p> <p>2157</p> <p>2158</p> <p>2159</p> <p>2160</p> <p>2161</p> <p>2162</p> <p>2163</p> <p>2164</p> <p>2165</p> <p>2166</p> <p>2167</p> <p>2168</p> <p>2169</p> <p>2170</p> <p>2171</p> <p>2172</p> <p>2173</p> <p>2174</p> <p>2175</p> <p>2176</p> <p>2177</p> <p>2178</p> <p>2179</p> <p>2180</p> <p>2181</p> <p>2182</p> <p>2183</p> <p>2184</p> <p>2185</p> <p>2186</p> <p>2187</p> <p>2188</p> <p>2189</p> <p>2190</p> <p>2191</p> <p>2192</p> <p>2193</p> <p>2194</p> <p>2195</p> <p>2196</p> <p>2197</p> <p>2198</p> <p>2199</p> <p>2200</p> <p>2201</p> <p>2202</p> <p>2203</p> <p>2204</p> <p>2205</p> <p>2206</p> <p>2207</p> <p>2208</p> <p>2209</p> <p>2210</p> <p>2211</p> <p>2212</p> <p>2213</p> <p>2214</p> <p>2215</p> <p>2216</p> <p>2217</p> <p>2218</p> <p>2219</p> <p>2220</p> <p>2221</p> <p>2222</p> <p>2223</p> <p>2224</p> <p>2225</p> <p>2226</p> <p>2227</p> <p>2228</p> <p>2229</p> <p>2230</p> <p>2231</p> <p>2232</p> <p>2233</p> <p>2234</p> <p>2235</p> <p>2236</p> <p>2237</p> <p>2238</p> <p>2239</p> <p>2240</p> <p>2241</p> <p>2242</p> <p>2243</p> <p>2244</p> <p>2245</p> <p>2246</p> <p>2247</p> <p>2248</p> <p>2249</p> <p>2250</p> <p>2251</p> <p>2252</p> <p>2253</p> <p>2254</p> <p>2255</p> <p>2256</p> <p>2257</p> <p>2258</p> <p>2259</p> <p>2260</p> <p>2261</p> <p>2262</p> <p>2263</p> <p>2264</p> <p>2265</p> <p>2266</p> <p>2267</p> <p>2268</p> <p>2269</p> <p>2270</p> <p>2271</p> <p>2272</p> <p>2273</p> <p>2274</p> <p>2275</p> <p>2276</p> <p>2277</p> <p>2278</p> <p>2279</p> <p>2280</p> <p>2281</p> <p>2282</p> <p>2283</p> <p>2284</p> <p>2285</p> <p>2286</p> <p>2287</p> <p>2288</p> <p>2289</p> <p>2290</p> <p>2291</p> <p>2292</p> <p>2293</p> <p>2294</p> <p>2295</p> <p>2296</p> <p>2297</p> <p>2298</p> <p>2299</p> <p>2300</p> <p>2301</p> <p>2302</p> <p>2303</p> <p>2304</p> <p>2305</p> <p>2306</p> <p>2307</p> <p>2308</p> <p>2309</p> <p>2310</p> <p>2311</p> <p>2312</p> <p>2313</p> <p>2314</p> <p>2315</p> <p>2316</p> <p>2317</p> <p>2318</p> <p>2319</p> <p>2320</p> <p>2321</p> <p>2322</p> <p>2323</p> <p>2324</p> <p>2325</p> <p>2326</p> <p>2327</p> <p>2328</p> <p>2329</p> <p>2330</p> <p>2331</p> <p>2332</p> <p>2333</p> <p>2334</p> <p>2335</p> <p>2336</p> <p>2337</p> <p>2338</p> <p>2339</p> <p>2340</p> <p>2341</p> <p>2342</p> <p>2343</p> <p>2344</p> <p>2345</p> <p>2346</p> <p>2347</p> <p>2348</p> <p>2349</p> <p>2350</p> <p>2351</p> <p>2352</p> <p>2353</p> <p>2354</p> <p>2355</p> <p>2356</p> <p>2357</p> <p>2358</p> <p>2359</p> <p>2360</p> <p>2361</p> <p>2362</p> <p>2363</p> <p>2364</p> <p>2365</p> <p>2366</p> <p>2367</p> <p>2368</p> <p>2369</p> <p>2370</p> <p>2371</p> <p>2372</p> <p>2373</p> <p>2374</p> <p>2375</p> <p>2376</p> <p>2377</p> <p>2378</p> <p>2379</p> <p>2380</p> <p>2381</p> <p>2382</p> <p>2383</p> <p>2384</p> <p>2385</p> <p>2386</p> <p>2387</p> <p>2388</p> <p>2389</p> <p>2390</p> <p>2391</p> <p>2392</p> <p>2393</p> <p>2394</p> <p>2395</p> <p>2396</p> <p>2397</p> <p>2398</p> <p>2399</p> <p>2400</p> <p>2401</p> <p>2402</p> <p>2403</p> <p>2404</p> <p>2405</p> <p>2406</p> <p>2407</p> <p>2408</p> <p>2409</p> <p>2410</p> <p>2411</p> <p>2412</p> <p>2413</p> <p>2414</p> <p>2415</p> <p>2416</p> <p>2417</p> <p>2418</p> <p>2419</p> <p>2420</p> <p>2421</p> <p>2422</p> <p>2423</p> <p>2424</p> <p>2425</p> <p>2426</p> <p>2427</p> <p>2428</p> <p>2429</p> <p>2430</p> <p>2431</p> <p>2432</p> <p>2433</p> <p>2434</p> <p>2435</p> <p>2436</p> <p>2437</p> <p>2438</p> <p>2439</p> <p>2440</p> <p>2441</p> <p>2442</p> <p>2443</p> <p>2444</p> <p>2445</p> <p>2446</p> <p>2447</p> <p>2448</p> <p>2449</p> <p>2450</p> <p>2451</p> <p>2452</p> <p>2453</p> <p>2454</p> <p>2455</p> <p>2456</p> <p>2457</p> <p>2458</p> <p>2459</p> <p>2460</p> <p>2461</p> <p>2462</p> <p>2463</p> <p>2464</p> <p>2465</p> <p>2466</p> <p>2467</p> <p>2468</p> <p>2469</p> <p>2470</p> <p>2471</p> <p>2472</p> <p>2473</p> <p>2474</p> <p>2475</p> <p>2476</p> <p>2477</p> <p>2478</p> <p>2479</p> <p>2480</p> <p>2481</p> <p>2482</p> <p>2483</p> <p>2484</p> <p>2485</p> <p>2486</p> <p>2487</p> <p>2488</p> <p>2489</p> <p>2490</p> <p>2491</p> <p>2492</p> <p>2493</p> <p>2494</p> <p>2495</p> <p>2496</p> <p>2497</p> <p>2498</p> <p>2499</p> <p>2500</p>
----------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

【 図 1 3 】

図13

脅威抽出・リスク評価

XYZ支店
決算情報

脅威種別

機密性侵害	▼	攻撃者 / 要因	外部第三者	▼
攻撃方法記述		後	リスク	▲
情報を見る正規権限者をだまして聞き出す		4	150K	
1306	1307	1308		
<div style="text-align: center;"> 追加 ↑ ↓ 削除 新規追加 </div>				
<p>正規権限者になりすまして、データに不正アクセスする ネットワーク上のデータを盗聴する 不用意に放置または座薬された紙類を見る 与えられたアクセス権限を不正の目的に利用する ソフトウェアの裏表の脆弱性を利用してアクセス権を取得</p>				
5	200K	▲		
5	300K			
5	50K			
4	100K			
3	150K	▼		
編集 リスク評価				
OK		キャンセル		

1301 1302 1303 1304

1305 1309

【 図 1 4 】

図 14

対策決定・コスト設定			
XYZ支店 決算情報			1407
脅威一覧			
脅威種別	攻撃者/要因	攻撃方法	リスク
機密性侵害 機密性侵害 機密性侵害 機密性侵害 完全性侵害 完全性侵害	外部第三者 内部第三者 ... 正規権限者 外部第三者 正規権限者	情報を知る正規権限者をだまして聞き出す 不用意に放散または廃棄された紙等を見る ... 与えられたアクセス権限を不正な目的に利用する ソフトウェアの実装上の脆弱性を利用してアクセス 与えられたアクセス権限を不正な目的に利用する	150K 200K ... 300K 50K 100K
対策選択			
許容リスク 残存リスク 許容コスト 所要コスト	[合計: 30,000円/年, 資産別: 2,000円/年]		1401
	[合計: 50,000円/年, 資産別: 7,500円/年]		1402
	[合計: 10,000円/年]		1403
	[合計: 10,000円/年]		1404
完了		キャンセル	

【 図 15 】

15

		対策立案・コスト設定			
攻撃種別		機密性侵害	攻撃者/要因	外部第三者	
攻撃方法		情報を知る正規権限者をだまして聞き出す			
対策候補	対策種別	対策内容	優	コスト	▲
	物理/建物	機密情報を含む部屋には入退室制御機構を備える	5	150K	
	論理/暗号化	重要データは暗号化して保存する	2	200K	
追加候補	運用/組織・体制	従業員は情報セキュリティに関する誓約書に署名する	5	200K	▼
		追加	↑	↓	削除
				新規追加	1509
追加候補	物理/建物	重要な情報は施設された保管庫で管理する	5	150K	▲
	論理/識別・認証	重要な情報へアクセスする利用者を識別する	4	200K	
	論理/アクセス制御	重要な情報へは正規の権限を持つ利用者のみアクセス許可	5	200K	▼
			OK	キャンセル	
1506	1507		1508		

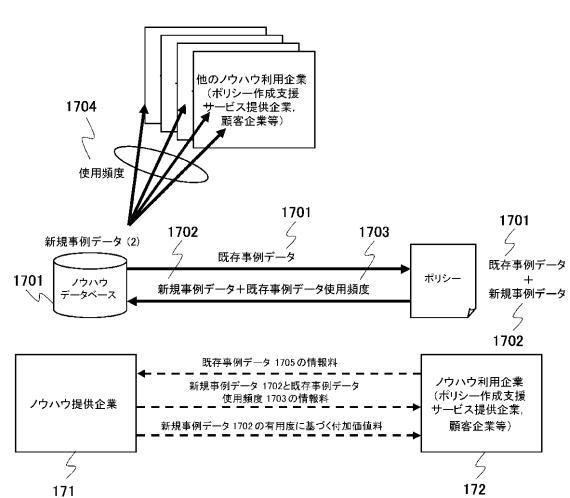
【 図 1 6 】

16

対策選択		1601	1602	1603
脅威一覧				
脅威種別	攻撃者／要因	攻撃方法	残存リスク	▲
機密性侵害	外部第三者	情報を知る正規権限者をだまして聞き出す	150K	▼
機密性侵害	内部第三者	不用意に放置または廃棄された紙等を見る	200K	▼
機密性侵害	正規権限者	与えられたアクセス権限を不正／目的に利用する	300K	▼
対策候補一覧	採択	対策内容	削減効果	コスト
	<input checked="" type="checkbox"/> 物理／建物	機密情報を含む部屋には入退室制御機器を備える	10%	150K
	<input type="checkbox"/> 理論／暗号化	重要データは暗号化して保存する	20%	200K
	<input checked="" type="checkbox"/> 認証／識別・認証	重要な情報へアクセスする利用者を識別する	20%	200K
許容リスク	[合計: 30,000 K 円／年、資産別: 2,000 K 円／年]			
残存リスク	[合計: 25,000 K 円／年、資産別: 1,500 K 円／年]			
許容コスト	[合計: 10,000 K 円／年]			
所要コスト	[合計: 10,000 K 円／年]			
	未対策脅威 あり○ なし●			
OK		キャンセル		

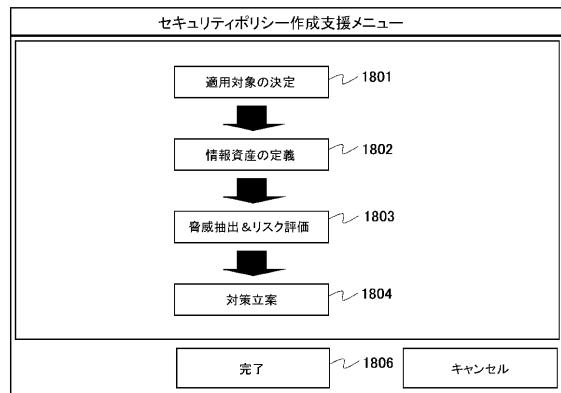
【図17】

図17



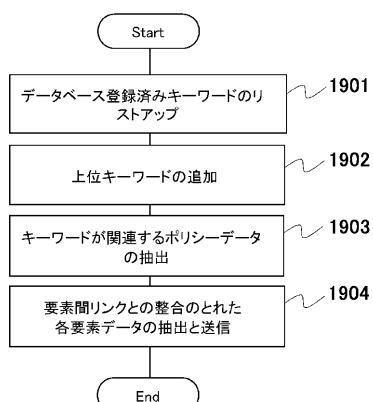
【図18】

図18



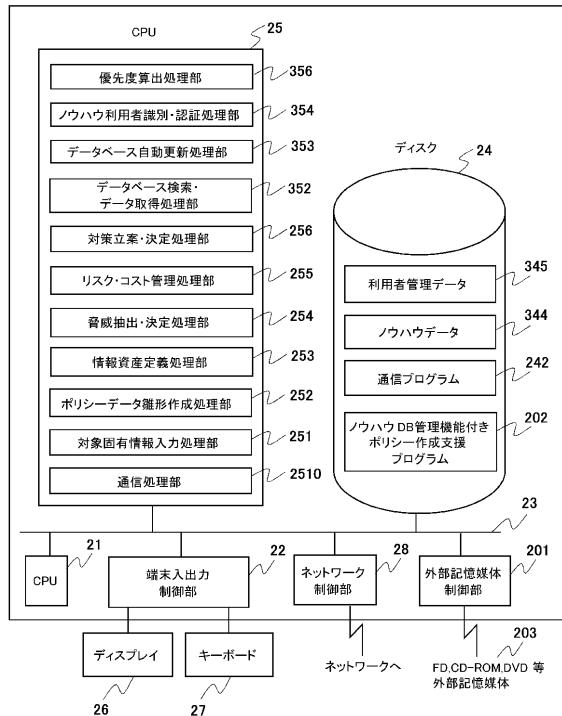
【図19】

図19



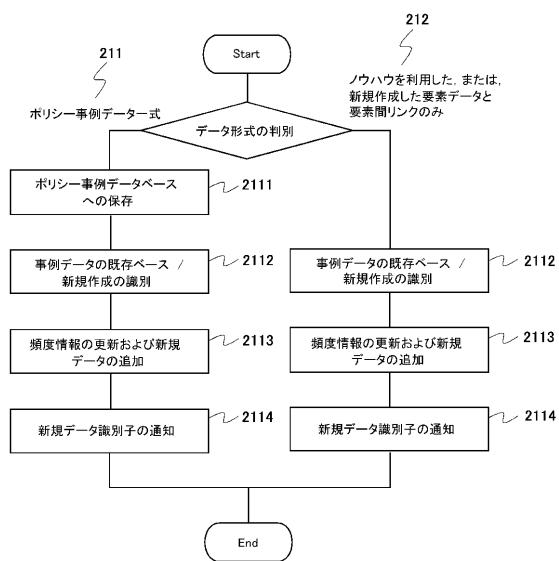
【図20】

図20



【図21】

図21



【図22】

図22

ログイン	
ユーザID	<input type="text" value="AAA"/> 2201
パスワード	<input type="password" value="*****"/> 2202
OK	キャンセル

Form description: A login interface titled 'ログイン'. It contains fields for 'ユーザID' (User ID) with value 'AAA' (2201) and 'パスワード' (Password) with value '*****' (2202). It also includes 'OK' and 'キャンセル' (Cancel) buttons.

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