(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6252268号
(P6252268)

(45)発行日　平成29年12月27日(2017.12.27)　(24)登録日　平成29年12月8日(2017.12.8)

(51)Int.Cl.　F I
G06Q 10/06 (2012.01)　G06Q 10/06　３２６
G06F 21/00 (2013.01)　G06F 21/00

請求項の数 6　(全 15 頁)

(21)出願番号　特願2014-52693(P2014-52693)
(22)出願日　平成26年3月14日(2014.3.14)
(65)公開番号　特開2015-176375(P2015-176375A)
(43)公開日　平成27年10月5日(2015.10.5)
審査請求日　平成28年8月4日(2016.8.4)

（出願人による申告）平成２５年度、総務省、「サイバー攻撃の解析・検知に関する研究開発」研究開発委託契約に基づく開発項目「利用者の行動特性に基づくサイバー攻撃検知技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　寺田　剛陽
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　片山　佳則
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　森永　正信
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】管理方法、管理装置および管理プログラム

(57)【特許請求の範囲】
【請求項１】
管理装置が
特定の事例経験者に特徴的な心理特性を抽出し、
特定の事例経験者に特徴的な行動特性を抽出し、
抽出された心理特性の項目それぞれについて、行動特性として抽出された複数の項目との関係式を求め、
各ユーザについて、心理特性の項目それぞれの前記関係式と、ログデータの値とから心理特性の値を計算し、当該心理特性の値が所定の値を超過したユーザに対して、超過した心理特性に対応する対策を配信する
処理を実行することを特徴とする管理方法。
【請求項２】
前記行動特性を抽出する処理は、
前記特定の事例経験者における、予め設定された期間内のログに基づいて行動特性を抽出する
ことを特徴とする請求項１に記載の管理方法。
【請求項３】
前記対策を配信する処理は、
前記計算された心理特性の値が、複数のユーザについて計算された心理特性の値の分布において、特定の事例経験者が属する側の上位である場合のユーザに対して、心理特性に

対応する対策を配信する
ことを特徴とする請求項１又は２に記載の管理方法。
【請求項４】
前記関係式を求める処理は、
前記特定の事例経験者と、前記特定の事例経験者以外の人との間に、所定量以上の差のある心理特性及び行動特性の項目についての関係式を求める、
ことを特徴とする請求項１乃至３のいずれか一項に記載の管理方法。
【請求項５】
特定の事例経験者に特徴的な心理特性を抽出する心理特性抽出部と、
特定の事例経験者に特徴的な行動特性を抽出する行動特性抽出部と、
抽出された心理特性の項目それぞれについて、行動特性として抽出された複数の項目との関係式を求める計算部と、
計算された関係式を示すデータを記録する記録部と、
各ユーザについて、特定の事例経験者に特徴的な心理特性の項目それぞれについて前記特定の事例経験者に特徴的な行動特性として抽出された複数の項目との関係式と、ログデータの値とから心理特性の値を計算し、当該心理特性の値が所定の値を超過したユーザを検知する検知部と、
前記検知されたユーザに対して、超過した心理特性に対応する対策を配信する配信部と
を有することを特徴とする管理装置。
【請求項６】
管理装置のコンピュータに、
特定の事例経験者に特徴的な心理特性を抽出し、
特定の事例経験者に特徴的な行動特性を抽出し、
抽出された心理特性の項目それぞれについて、行動特性として抽出された複数の項目との関係式を求め、
計算された関係式を示すデータを記録し、
各ユーザについて、特定の事例経験者に特徴的な心理特性の項目それぞれについて前記特定の事例経験者に特徴的な行動特性として抽出された複数の項目との関係式と、ログデータの値とから心理特性の値を計算し、当該心理特性の値が所定の値を超過したユーザを検知し、
前記検知されたユーザに対して、超過した心理特性に対応する対策を配信する
処理を実行させることを特徴とする管理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、管理方法、管理装置および管理プログラムに関する。
【背景技術】
【０００２】
従来、各種サービスをユーザに提供する業務用又は商用のシステムにおいては、ユーザがクラッキングの被害を受けないように、ユーザの過去の行動データであるログをもとにセキュリティについての注意喚起を行うことで、システムのセキュリティを向上させている。このクラッキングの被害については、一例として標準型攻撃メールによるものがある。標準型攻撃メールによるクラッキングでは、電子メールに添付されたプログラム（実行ファイル）の起動をユーザに促し、起動されたプログラムを足がかりにシステムへの侵入等を行う。このため、電子メールに添付されたプログラムを不用意に起動しないよう、ユーザのログから電子メールに添付されたプログラムの実行経験のあるユーザなどに対して注意喚起を行う。
【先行技術文献】
【特許文献】
【０００３】

【特許文献１】特開２００１－１３４７０６号公報
【特許文献２】特開２０１３－２０５８７号公報
【特許文献３】特開２０１２－９４０５６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上述した従来技術では、ログによる表面的なユーザの行動をもとにセキュリティについての注意喚起を行っているに過ぎず、ユーザの心理面を考慮したものではなかった。例えば、クラッキングに対する警戒心の低下したユーザ等、セキュリティ意識の低いユーザを対象にしての注意喚起を行うことはできなかった。
【０００５】
１つの側面では、本発明は、セキュリティを向上できる管理方法、管理装置および管理プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
一実施形態の管理方法は、管理装置が特定の事例経験者に特徴的な心理特性を抽出し、特定の事例経験者に特徴的な行動特性を抽出し、抽出された心理特性の項目それぞれについて、行動特性として抽出された複数の項目との関係式を求め、各ユーザについて、心理特性の項目それぞれの前記関係式と、ログデータの値とから心理特性の値を計算し、当該心理特性の値が所定の値を超過したユーザに対して、超過した心理特性に対応する対策を配信する処理を実行する。
【発明の効果】
【０００７】
一実施形態によれば、セキュリティを向上できる、という効果を奏する。
【図面の簡単な説明】
【０００８】
【図１】図１は、実施形態にかかる管理装置の機能構成を例示するブロック図である。
【図２】図２は、実施形態にかかる管理装置の処理の工程を例示するフローチャートである。
【図３】図３は、心理特性抽出工程を例示するフローチャートである。
【図４】図４は、心理状態データテーブルの一例を説明する説明図である。
【図５】図５は、心理特性データテーブルの一例を説明する説明図である。
【図６】図６は、行動特性抽出工程を例示するフローチャートである。
【図７】図７は、行動ログデータテーブルの一例を説明する説明図である。
【図８】図８は、行動特性データテーブルの一例を説明する説明図である。
【図９】図９は、計算工程を例示するフローチャートである。
【図１０】図１０は、関係式データの一例を説明する説明図である。
【図１１】図１１は、ユーザ検知工程を例示するフローチャートである。
【図１２】図１２は、ユーザ検知テーブルの一例を説明する説明図である。
【図１３】図１３は、ユーザ検知の一例を説明する説明図である。
【図１４】図１４は、対策の配信の一例を説明する説明図である。
【図１５】図１５は、管理装置のハードウエア構成を例示するブロック図である。
【図１６】図１６は、管理装置を用いるシステムの一例を説明する説明図である。
【図１７】図１７は、管理装置を用いるシステムの一例を説明する説明図である。
【発明を実施するための形態】
【０００９】
以下、図面を参照して、実施形態にかかる管理方法、管理装置および管理プログラムを説明する。実施形態において同一の機能を有する構成には同一の符号を付し、重複する説明は省略する。なお、以下の実施形態で説明する管理方法、管理装置および管理プログラムは、一例を示すに過ぎず、実施形態を限定するものではない。また、以下の各実施形態

は、矛盾しない範囲内で適宜組みあわせてもよい。

【００１０】

図１は、実施形態にかかる管理装置１００の機能構成を例示するブロック図である。図２は、実施形態にかかる管理装置１００の処理の工程を例示するフローチャートである。図１に示すように、管理装置１００は、心理特性抽出部１０と、行動特性抽出部２０と、計算部３０と、ユーザ検知部４０と、配信部５０とを有する。管理装置１００は、ＰＣ（Personal Computer）、ワークステーションなどの情報処理装置などであってよい。管理装置１００は、ＣＰＵ（Central Processing Unit）がプログラムを実行することで、上述した機能構成を実現する（ハードウエア構成の詳細は後述する）。

【００１１】

心理特性抽出部１０は、ＩＴ（インターネット）被害経験者に特徴的な心理特性を抽出する処理を行う。具体的には、図２に示す心理特性抽出工程（Ｓ１０）において、心理特性抽出部１０は、サンプルとするユーザについての情報であるアンケート回答データ１、ＩＴ被害経験データ２を参照して、ＩＴ被害経験者に特徴的な心理特性を抽出する。なお、サンプルとするユーザについては、システム内のユーザよりシステム管理者が任意又は無作為に抽出してよい。例えば、システム内の全ユーザを対象としてもよく、一部のユーザを対象としてもよい。

【００１２】

ここで、ＩＴ被害経験者とは、インターネットなどのネットワークを介したクラッキング等の被害に対するセキュリティ意識の低い人の総称であってよい。例えば、ＩＴ被害経験者は、クラッキング等の被害を受けた人（実害のあった人）に限定しない。ＩＴ被害経験者は、標準型攻撃メールについての訓練メールでプログラムを開いてしまった人など、セキュリティに対する意識の低さに起因する特定の事例に該当する者を含めてよい。

【００１３】

アンケート回答データ１は、サンプルとするユーザに対して行った、心理状態に関する質問項目を含むアンケートの回答が記録されたデータである。サンプルとするユーザに対して行うアンケートには、標準型攻撃メールについての訓練メールでの開封経験（プログラムの実行経験）、ウイルスの感染経験、自信過剰度を評価する質問項目、目先の利益の優先度を評価する質問項目、クラッキングの被害に遭う可能性を問う質問項目などがある。自信過剰度を評価する質問項目、目先の利益の優先度を評価する質問項目などの心理状態に関する質問項目については、例えば、ユーザの回答を数値化した（段階別に評価した）ものなどであってよい。また、アンケートには、心理状態に関する質問項目だけでなく、訓練メールでの開封経験、ウイルスの感染経験など、セキュリティに対する意識の低い人か否かを判定するための質問項目を含めてもよい。アンケート回答データ１には、サンプルとするユーザを識別するユーザＩＤごとに、上述したアンケートの回答結果が記述されている。

【００１４】

ＩＴ被害経験データ２は、サンプルとするユーザごとのＩＴ被害経験（クラッキング被害）の有無が記録されたデータである。具体的には、ＩＴ被害経験データ２には、サンプルとするユーザを識別するユーザＩＤごとに、ＩＴ被害経験の有無が記述されている。

【００１５】

心理特性抽出部１０は、上述したアンケート回答データ１、ＩＴ被害経験データ２を参照し、ＩＴ被害経験者に特徴的な心理特性を抽出する構成として、心理情報収集部１１と、統計分析部１３とを有する。ここで、心理特性抽出工程における心理情報収集部１１と、統計分析部１３との処理の詳細を説明する。図３は、心理特性抽出工程を例示するフローチャートである。

【００１６】

図３に示すように、心理情報収集部１１は、アンケート回答データ１、ＩＴ被害経験データ２を参照し、サンプルとする全ユーザについて、ユーザごとにセキュリティ意識の低い低意識群と、セキュリティ意識の高い高意識群とに振り分ける（Ｓ１１）。具体的には

、心理情報収集部１１は、ユーザＩＤごとに、アンケート回答データ１におけるセキュリティに対する意識の低い人か否かを判定するための質問項目、ＩＴ被害経験データ２におけるＩＴ被害経験の有無を読み出す。次いで、心理情報収集部１１は、読み出した内容をもとに、例えば、ＩＴ被害経験が有る場合は低意識群へ、ＩＴ被害経験が無い場合は高意識群へ振り分ける。ユーザごとに低意識群又は高意識群に振り分けた、アンケート回答データ１、ＩＴ被害経験データ２のデータは、心理状態データテーブル１２に格納される。

【００１７】

図４は、心理状態データテーブル１２の一例を説明する説明図である。図４に示すように、心理状態データテーブル１２には、ユーザＩＤごとに、心理状態などの各質問項目における回答と、低意識群又は高意識群を示す所属グループとが記述される。

【００１８】

次いで、統計分析部１３は、低意識群又は高意識群の２群に分けたデータについて、質問項目ごとに統計値（総数、平均値、標準偏差など）を算出し、それぞれのデータの正規性をチェックする（Ｓ１２）。具体的には、算出した統計値をもとに低意識群又は高意識群の２群に分けたデータが正規分布に近いか否かをチェックする。

【００１９】

次いで、統計分析部１３は、低意識群又は高意識群の２群に分けたデータについて、質問項目ごとに統計値（総数、平均値、標準偏差など）を算出し、それぞれのデータの等分散性をチェックする（Ｓ１３）。具体的には、低意識群のデータと高意識群のデータとの間の等分散性（２群のデータの分散は同じくらいであるか）をチェックする。

【００２０】

次いで、統計分析部１３は、チェックした正規性、等分散性をもとに、低意識群のデータと高意識群のデータとの間で差が有るかを検定するための統計的検定手法を選択する（Ｓ１４）。ここで選択する統計的検定手法には、例えば、ウェルチのｔ検定、マン・ホイットニーのＵ検定などがある。Ｓ１４では、チェックした正規性、等分散性に対応する統計的検定手法が適宜選択される。

【００２１】

次いで、統計分析部１３は、選択された統計的検定手法を用いて低意識群のデータと高意識群のデータとの間で差がある質問項目を抽出し、抽出した質問項目のデータ（例えば低意識群の統計値）を心理特性（Ｙ＿ｉ）とする（Ｓ１５）。抽出された心理特性（Ｙ＿ｉ）は、心理特性データテーブル１４に格納される。

【００２２】

図５は、心理特性データテーブル１４の一例を説明する説明図である。図５に示すように、心理特性データテーブル１４には、質問項目（Ｑ３、Ｑ４…）ごとに、低意識群（ｇ１）の統計値、高意識群（ｇ２）の統計値、検定値（ｔ値）、判定基準値、判定結果が記述されている。図５では、統計的検定手法としてｔ検定が選択された場合が例示されているが、Ｕ検定であってもよい。

【００２３】

検定値（ｔ値）は、Ｓ１４において選択された統計的検定手法に従って算出される値である。ｔ検定では、次の式（１）に従って質問項目ごとのｔ値が算出される。

【００２４】

【数１】

$$t_{\_Qi} = \left(m_{g1} - m_{g2}\right) \Big/ \left(\sigma_{g1} / \sqrt{n_{g1}}\right) \quad (i = 1,2,\cdots) \qquad \cdots \ (1)$$

【００２５】

式（１）において、添字のＱｉは質問項目（ｉ＝１、２、…）を示す。また、添字のｇ１は低意識群のデータであることを示す。添字のｇ２は高意識群のデータであることを示す。

【００２６】

判定基準値は、２群のデータに有意差ありと判定できる、ｔ値の絶対値の最小値を示す

値である。本実施形態では一律に有意水準（約５％）とするための値（２．０４）が設定されているが、この値は任意に設定してよい。

【００２７】

判定は、ｔ値が判定基準値を満たすか否かの判定結果を示す。例えば、Ｑ３、Ｑ４については、ｔ値の絶対値（２．７４、２．３５）が判定基準値（最小値）を上回ることから、低意識群のデータと高意識群のデータとの間で有意差あり（○）と判定された判定結果が記述される。すなわち、Ｑ３、Ｑ４のデータについては、抽出された心理特性（Ｙ＿ｉ）とされる。また、Ｑ５については、ｔ値の絶対値（１．３６）が判定基準値（最小値）を下回ることから、低意識群のデータと高意識群のデータとの間で有意差なし（×）と判定された判定結果が記述される。このため、Ｑ５については、心理特性（Ｙ＿ｉ）として抽出されなかったデータとされる。

【００２８】

図１、２に戻り、行動特性抽出部２０は、ＩＴ被害経験者に特徴的な行動特性を抽出する処理を行う。具体的には、図２に示す行動特性抽出工程（Ｓ２０）において、行動特性抽出部２０は、サンプルとするユーザについての情報であるＩＴ被害経験データ２、ログデータ３を参照して、ＩＴ被害経験者に特徴的な行動特性を抽出する。

【００２９】

ログデータ３は、ユーザの過去の行動（操作内容、表示内容等）を逐次記録したデータである。具体的には、ログデータ３には、ユーザ（ユーザＩＤ）とそのユーザが行った行動項目が日時とともに記録されている。ログデータ３が記録する行動項目には、マウス、キーボードの操作の他、各種画面（例えば警告画面）の表示時間、メールの送受信、パッチを適用した時刻などがある。

【００３０】

行動特性抽出部２０は、ＩＴ被害経験データ２、ログデータ３を参照し、ＩＴ被害経験者に特徴的な行動特性を抽出する構成として、行動情報収集部２１と、統計分析部２３とを有する。ここで、行動特性抽出工程における行動情報収集部２１と、統計分析部２３との処理の詳細を説明する。図６は、行動特性抽出工程を例示するフローチャートである。

【００３１】

図６に示すように、行動情報収集部２１は、心理状態データテーブル１２の所属グループを参照し、サンプルとする全ユーザについて、ユーザごとにセキュリティ意識の低い低意識群と、セキュリティ意識の高い高意識群とのどちらに属するかを取得する（Ｓ２１）。なお、低意識群又は高意識群のどちらに属するかについては、ＩＴ被害経験データ２を参照して得てもよい。

【００３２】

次いで、行動情報収集部２１は、ログデータ３を参照し、行動項目について、一定期間内の代表値（総数、平均値、標準偏差、中央値などの統計値）をユーザごとに計算する（Ｓ２２）。具体的には、行動情報収集部２１は、ユーザＩＤごとに、一定期間内において該当する行動項目を抽出し、抽出した行動項目における代表値を計算する。なお、抽出する期間については、管理者などが入力装置などを介して、１ヶ月、１週間などの単位で任意に設定したものであってよい。Ｓ２１、Ｓ２２においてユーザごとに取得・計算されたデータは、行動ログデータテーブル２２に格納される。

【００３３】

図７は、行動ログデータテーブル２２の一例を説明する説明図である。図７に示すように、行動ログデータテーブル２２は、ユーザＩＤごとに、所属グループ、行動項目（警告画面表示時間、送信メール数／日、パッチ適用間隔…）における代表値（計測回数、平均値、標準偏差など）が記述される。

【００３４】

次いで、統計分析部２３は、低意識群又は高意識群の２群に分けたデータについて、ログデータ３の行動項目ごとに、統計値（総数、平均値、標準偏差など）に基づいて、それぞれのデータの正規性をチェックする（Ｓ２３）。具体的には、統計値をもとに低意識群

又は高意識群の２群に分けたデータが正規分布に近いか否かをチェックする。

【００３５】

次いで、統計分析部２３は、低意識群又は高意識群の２群に分けたデータについて、ログデータ３の行動項目ごとに、統計値に基づいて、それぞれのデータの等分散性をチェックする（Ｓ２４）。具体的には、低意識群のデータと高意識群のデータとの間の等分散性（２群のデータの分散は同じくらいであるか）をチェックする。

【００３６】

次いで、統計分析部２３は、チェックした正規性、等分散性をもとに、低意識群のデータと高意識群のデータとの間で差が有るかを検定するための統計的検定手法を選択する（Ｓ２５）。ここで選択する統計的検定手法には、例えば、ウェルチのｔ検定、マン・ホイットニーのＵ検定などがある。Ｓ２５では、チェックした正規性、等分散性に対応する統計的検法が適宜選択される。

【００３７】

次いで、統計分析部２３は、選択された統計的検定手法を用いて低意識群のデータと高意識群のデータとの間で差があるログデータ３の行動項目を抽出し、抽出した行動項目のデータ（例えば低意識群の統計値）を行動特性（Ｘ＿ｋ）とする（Ｓ２６）。抽出された行動特性（Ｘ＿ｋ）は、行動特性データテーブル２４に格納される。

【００３８】

図８は、行動特性データテーブル２４の一例を説明する説明図である。図８に示すように、行動特性データテーブル２４には、行動項目（警告画面表示時間、送信メール数／日…）ごとに、低意識群（ｇ１）の統計値、高意識群（ｇ２）の統計値、検定値（ｔ値）、判定基準値、判定結果が記述されている。図８では、統計的検定手法としてｔ検定が選択された場合が例示されているが、Ｕ検定であってもよい。

【００３９】

検定値（ｔ値）は、Ｓ２５において選択された統計的検定手法に従って算出される値である。ｔ検定では、次の式（２）に従って行動項目ごとのｔ値が算出される。

【００４０】

【数２】

$$t\_Bj=\left(m_{g1}-m_{g2}\right)\Big/\left(\sigma_{g1}/\sqrt{n_{g1}}\right)\quad\left(j=1,2,\cdots\right)\qquad\cdots\ (2)$$

【００４１】

式（２）において、添字のＢｊは行動項目（ｊ＝１、２、…）を示す。また、添字のｇ１は低意識群のデータであることを示す。添字のｇ２は高意識群のデータであることを示す。

【００４２】

判定基準値は、２群のデータに有意差ありと判定できる、ｔ値の絶対値の最小値を示す値である。本実施形態では行動項目ごとに有意水準（約５％）とするための値（２．０５、２．０３、２．０４）が設定されているが、この値は任意に設定してよい。

【００４３】

判定は、ｔ値が判定基準値を満たすか否かの判定結果を示す。例えば、警告画面表示時間（Ｂ１）、パッチ適用間隔（Ｂ３）については、ｔ値の絶対値（２．１９、２．３０）が判定基準値（最小値）を上回ることから、低意識群のデータと高意識群のデータとの間で有意差あり（○）と判定された判定結果が記述される。すなわち、Ｂ１、Ｂ３のデータについては、抽出された行動特性（Ｘ＿ｋ）とされる。また、送信メール数／日（Ｂ２）については、ｔ値の絶対値（１．３１）が判定基準値（最小値）を下回ることから、低意識群のデータと高意識群のデータとの間で有意差なし（×）と判定された判定結果が記述される。このため、Ｂ２については、行動特性（Ｘ＿ｋ）として抽出されなかったデータとされる。

【００４４】

図１、２に戻り、計算部３０は、図２に示す計算工程（Ｓ３０）において、心理特性抽

出部１０より抽出された心理特性の項目それぞれについて、行動特性抽出部２０より行動特性として抽出された複数の項目との関係式を求める処理を行う。この関係式は、低意識群と高意識群との間に有意差のある心理特性と、行動特性との相関性を示していることから、セキュリティ意識の低いユーザにおける心理特性と行動特性との間の相関性を示すデータでもある。

【００４５】

計算部３０は、上述した関係式を求める構成として、統計分析部３１を有する。ここで、計算工程における統計分析部３１の処理の詳細を説明する。図９は、計算工程を例示するフローチャートである。

【００４６】

図９に示すように、統計分析部３１は、心理特性データテーブル１４、行動特性データテーブル２４を参照し、心理特性Ｙ＿ｉ（ｉ＝１，２，…）および行動特性Ｘ＿ｋ（ｋ＝１，２，…）のすべてについて、データの正規性をチェックする。具体的には、心理特性Ｙ＿ｉ、行動特性Ｘ＿ｋのすべてのデータが、正規分布に近いか否かをチェックする。

【００４７】

次いで、統計分析部３１は、正規性のチェックの結果、正規性を満たさないか否か、すなわち正規分布から外れているか否かを判定する（Ｓ３２）。心理特性Ｙ＿ｉ、行動特性Ｘ＿ｋにおいて、正規性を満たさない場合（Ｓ３２：ＹＥＳ）、統計分析部３１は、変数変換を行って、データを正規分布に近づける（Ｓ３３）。これにより、心理特性及び行動特性の関係式（相関性）を求める前に、心理特性及び行動特性のデータの条件を整える。心理特性Ｙ＿ｉ、行動特性Ｘ＿ｋにおいて、正規性を満たす場合（Ｓ３２：ＮＯ）、統計分析部３１は、Ｓ３３をスキップしてＳ３４へ処理を進める。

【００４８】

Ｓ３４において、統計分析部３１は、心理特性Ｙ＿ｉそれぞれについて、従来の回帰分析手法を用いて、行動特性Ｘ＿ｋ（ｋ＝１，２，…）との関係式（相関性）を計算する。具体的には、次の式（３）に示すように、重回帰分析などの回帰式により関係式が計算される。

【００４９】

【数３】

$$Y_i = a_1X_1 + a_2X_2 + \cdots + a_kX_k \qquad \cdots (3)$$

【００５０】

式（３）において、Ｙは心理特性であり、添字のｉ（ｉ＝１，２，…）は心理特性の項目を示す。Ｘは行動特性であり、添字のｋ（ｋ＝１，２，…）は行動特性の項目を示す。行動特性の各項目におけるａは、回帰係数であり、心理特性に対する行動特性の影響度を示す。

【００５１】

計算された関係式を示すデータは、関係式データ３２に格納される。図１０は、関係式データ３２の一例を説明する説明図である。図１０に示すように、関係式データ３２には、心理特性Ｙ＿ｉそれぞれについて、各行動特性の影響度である回帰係数が格納される。

【００５２】

図１、２に戻り、ユーザ検知部４０は、図２に示すユーザ検知工程（Ｓ４０）において、各ユーザについて、心理特性の項目それぞれの関係式と、ログデータ３の値とから心理特性の値（Ｙ＿ｉ）を計算する。具体的には、ユーザ検知部４０は、関係式データ３２と行動ログデータテーブル２２とを参照し、各ユーザについて、定期的に心理特性の値を計算する。なお、心理特性の値を計算する定期的な間隔は、管理者が入力装置などを介して、１ヶ月、１週間などの単位で任意に設定したものであってよい。次いで、ユーザ検知部４０は、計算した心理特性の値（Ｙ＿ｉ）が所定の値を超過したユーザ、すなわちセキュリティ意識の低いユーザを検知する。

【００５３】

ユーザ検知部４０は、ユーザを検知する構成として、検知部４１を有する。ここで、ユーザ検知工程における検知部４１の処理の詳細を説明する。図１１は、ユーザ検知工程を例示するフローチャートである。

【００５４】

図１１に示すように、検知部４１は、関係式データ３２と行動ログデータテーブル２２とを参照し、各ユーザの心理特性の値（Ｙ＿ｉ）を、関係式と行動特性（Ｘ＿ｋ）に対応するログの値をもとに計算する（Ｓ４１）。具体的には、Ｙ＿ｉにおける関係式の回帰係数を関係式データ３２より読み出し、行動特性（Ｘ＿ｋ）に対応するログの値を回帰係数に掛け合わせることで、心理特性の値を求める。

【００５５】

次いで、検知部４１は、計算された心理特性の値が、セキュリティ意識の低い、低意識のユーザとする条件を満たすか否かを判定する（Ｓ４２）。この検知部４１における判定結果は、ユーザ検知テーブル４２に格納される。

【００５６】

図１２は、ユーザ検知テーブル４２の一例を説明する説明図である。図１２に示すように、ユーザ検知テーブル４２には、ユーザＩＤごとに、そのユーザの心理特性の値と、判定（判定結果）が格納される。判定には、低意識のユーザとする条件を満たすと判定された心理特性の項目が格納される。例えば、ユーザＩＤが「ｕ０００１」のユーザについては、Ｙ＿１（自信過剰度）の判定結果が低意識のユーザとする条件を満たすものと判定されている。

【００５７】

単純な構成としては、検知部４１は、計算された心理特性の値が、所定の閾値を超えるか否かにより判定する。また、検知部４１は、計算された心理特性の値が、複数のユーザについて計算された心理特性の値の分布（例えばユーザ全体のデータ分布）において、低意識群が属する側の上位であるか否かを判定する。例えば、計算された心理特性の値が、ユーザ全体のデータ分布の両端のうち、統計的検定手法によって決定される、低意識群側の上位α％に属するか否かを判定する。ここで、αの値は管理者が入力装置などを介して適宜設定してよい。

【００５８】

図１３は、ユーザ検知の一例を説明する説明図である。図１３に示すグラフは、ユーザ全体の心理特性の得点分布をユーザ数の割合で示している。また、低意識群が属する側は、心理特性の得点の高得点側であるとする。この場合、行動特性（Ｘ＿ｋ）に対応するログの値を回帰係数に掛け合わせて求めた心理特性の値（Ｙ＿ｉ）の得点が、上位のα％に該当する領域Ｒに入るユーザを検知する。

【００５９】

検知部４１は、ユーザ検知テーブル４２を参照し、計算された心理特性の値が低意識のユーザとする条件を満たすか否かを判定し（Ｓ４２）、満たす場合（Ｓ４２：ＹＥＳ）、検知したユーザを配信部５０に通知する（Ｓ４３）。具体的には、検知部４１は、検知したユーザを示すユーザＩＤとともに、条件を満たすと判定された心理特性とその値を通知する。

【００６０】

図１、２に戻り、配信部５０は、図２に示す配信工程（Ｓ５０）において、Ｓ４０で計算した心理特性の値（Ｙ＿ｉ）が所定の値を超過したユーザ、すなわちセキュリティ意識の低いユーザに対して、超過した心理特性に対応する対策を配信する。具体的には、配信部５０は、検知部４１よりユーザＩＤとともに通知された、条件を満たすと判定された心理特性とその値に基づいて、その心理特性に対応する対策を配信する。

【００６１】

図１４は、対策の配信の一例を説明する説明図である。図１４に示すように、関係式データ３２及びログデータ３より求めた心理特性の値が所定の値を超過した場合、管理装置１００は、その超過した心理特性の値に応じた対策、すなわち、ユーザの心理面を考慮し

た対策をユーザに対して配信する。具体的には、他のユーザと比べて値が悪かった心理特性についての対策を配信する。例えば、心理特性として自信過剰度の判定結果が条件を満たすものと判定された場合、自信過剰度に対応した対策を配信する。これにより、ユーザには、自身の心理特性にあった対策が配信されることから、ユーザのセキュリティに対する意識を効果的に向上させることができる。したがって、システムのセキュリティを向上できる。

【００６２】

管理装置１００で行われる各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ（Micro Controller Unit）等のマイクロ・コンピュータ）上で、その全部または任意の一部を実行するようにしてもよい。また、各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ等のマイクロ・コンピュータ）で解析実行されるプログラム上、またはワイヤードロジックによるハードウェア上で、その全部または任意の一部を実行するようにしてもよいことは言うまでもない。

【００６３】

ところで、上記の実施形態で説明した各種の処理は、予め用意されたプログラムをコンピュータで実行することで実現できる。そこで、以下では、上記の実施例と同様の機能を有するプログラムを実行するコンピュータ（ハードウエア）の一例を説明する。図１５は、管理装置１００のハードウエア構成を例示するブロック図である。

【００６４】

図１５が示すように、管理装置１００は、各種演算処理を実行するＣＰＵ１０１と、データ入力を受け付ける入力装置１０２と、モニタ１０３と、スピーカ１０４とを有する。また、管理装置１００は、記憶媒体からプログラム等を読み取る媒体読取装置１０５と、各種装置と接続するためのインタフェース装置１０６と、有線または無線により外部機器と通信接続するための通信装置１０７とを有する。また、管理装置１００は、各種情報を一時記憶するＲＡＭ１０８と、ハードディスク装置１０９とを有する。また、管理装置１００内の各部（１０１～１０９）は、バス１１０に接続される。

【００６５】

ハードディスク装置１０９には、心理特性抽出部１０、行動特性抽出部２０、計算部３０、ユーザ検知部４０および配信部５０の各処理部と同様の機能を有するプログラム（管理プログラム）が記憶される。また、ハードディスク装置１０９には、プログラムを実現するための各種データが記憶される。入力装置１０２は、例えば管理装置１００の操作者から操作情報の入力を受け付ける。モニタ１０３は、例えば操作者が操作する各種画面を表示する。インタフェース装置１０６は、例えば印刷装置等が接続される。通信装置１０７は、ＬＡＮ（Local Area Network）等の通信ネットワークと接続され、通信ネットワークを介した外部機器との間で各種情報をやりとりする。

【００６６】

ＣＰＵ１０１は、ハードディスク装置１０９に記憶された各プログラムを読み出して、ＲＡＭ１０８に展開して実行することで、各種の処理を行う。また、これらのプログラムは、管理装置１００を心理特性抽出部１０、行動特性抽出部２０、計算部３０、ユーザ検知部４０および配信部５０として機能させることができる。

【００６７】

なお、上記のプログラムは、必ずしもハードディスク装置１０９に記憶されている必要はない。例えば、管理装置１００が読み取り可能な記憶媒体に記憶されたプログラムを、管理装置１００が読み出して実行するようにしてもよい。管理装置１００が読み取り可能な記憶媒体は、例えば、ＣＤ－ＲＯＭやＤＶＤディスク、ＵＳＢ（Universal Serial Bus）メモリ等の可搬型記録媒体、フラッシュメモリ等の半導体メモリ、ハードディスクドライブ等が対応する。また、公衆回線、インターネット、ＬＡＮ（Local Area Network）等に接続された装置にこのプログラムを記憶させておき、管理装置１００がこれらからプログラムを読み出して実行するようにしてもよい。

【００６８】

図１６、図１７は、管理装置を用いるシステムの一例を説明する説明図である。図１６に示すように、管理装置１００は、通信ネットワークＮに接続された複数の端末装置２００におけるユーザを管理するサーバ装置などであってよい。管理装置１００は、日常的に端末装置２００を介したユーザの操作をログデータ３として蓄積し、セキュリティ意識の低いユーザとして検知されたユーザや、そのユーザに関連する人物（上司や人事部）などに対策を配信してもよい。

【００６９】

また、図１７に示すように、関係式データ３２を算出するまでの準備フェーズで用いる管理装置１００ａと、算出された関係式データ３２を活用する運用フェーズで用いる管理装置１００ｂとを別に構成するシステムであってもよい。管理装置１００ａでは、プログラムを実行することで、心理特性抽出部１０、行動特性抽出部２０、計算部３０としての機能を実現し、関係式データ３２の算出までを行う。管理装置１００ｂでは、プログラムを実行することで、ユーザ検知部４０、配信部５０としての機能を実現し、算出された関係式データ３２と、ログデータ３ａとをもとにしたシステムの運用を行う。具体的には、管理装置１００ｂは、日常的に端末装置２００を介したユーザの操作をログデータ３ａとして蓄積し、セキュリティ意識の低いユーザとして検知されたユーザや、そのユーザに関連する人物（上司や人事部）などに対策を配信する。

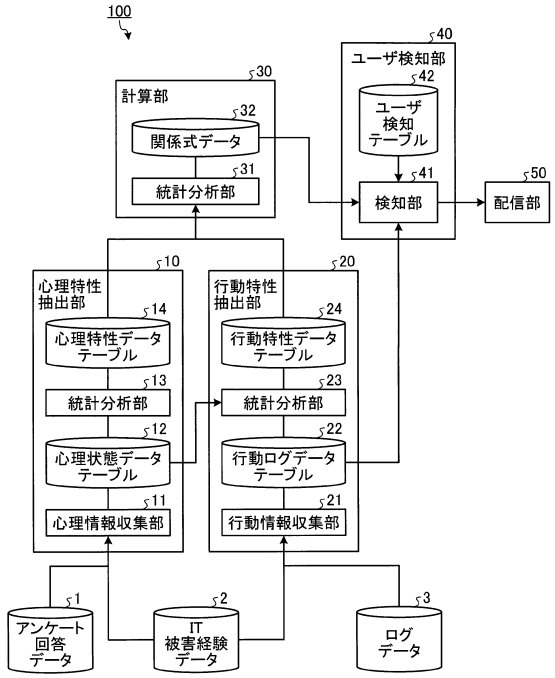
【符号の説明】

【００７０】

１　アンケート回答データ
２　ＩＴ被害経験データ
３、３ａ　ログデータ
１０　心理特性抽出部
１１　心理情報収集部
１２　心理状態データテーブル
１３、２３、３１　統計分析部
１４　心理特性データテーブル
２０　行動特性抽出部
２１　行動情報収集部
２２　行動ログデータテーブル
２４　行動特性データテーブル
３０　計算部
３２　関係式データ
４０　ユーザ検知部
４１　検知部
４２　ユーザ検知テーブル
５０　配信部
１００、１００ａ、１００ｂ　管理装置
２００　端末装置
Ｎ　通信ネットワーク
Ｒ　領域

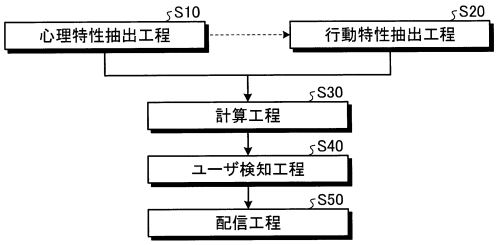
【図１】

実施形態にかかる管理装置の機能構成を例示するブロック図



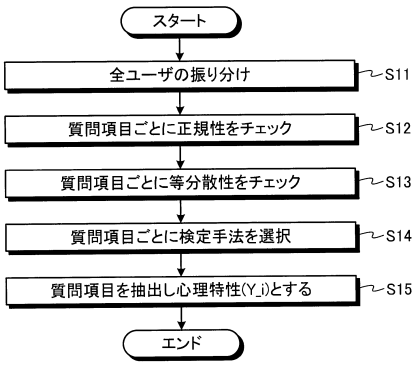
【図２】

実施形態にかかる管理装置の処理の工程を例示するフローチャート



【図３】

心理特性抽出工程を例示するフローチャート



【図４】

心理状態データテーブルの一例を説明する説明図

12

	ユーザID			
	u0001	u0002	u0003	…
Q1(訓練メールの開封経験)	1(あり)	0(なし)	0(なし)	
Q2(ウィルス感染経験)	0(あり)	0(なし)	1(なし)	
Q3(自信過剰度 5段階評価)	5	3	4	
Q4(目先の利益の優先度 7段階評価)	7	4	2	
Q5(今後被害に遭う可能性 %で回答)	20	50	50	
⋮				⋮
所属グループ	低意識群	高意識群	低意識群	…

【図５】

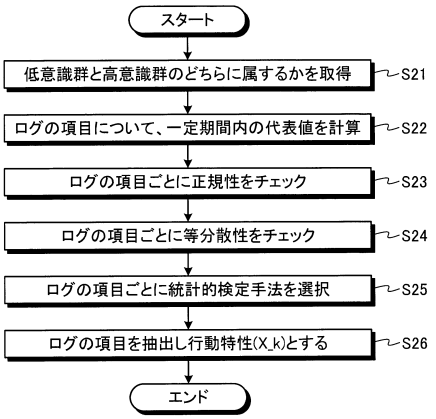
心理特性データテーブルの一例を説明する説明図

14

		低意識群 g1	高意識群 g2	t値	判定基準値	判定
Q3 (自信過剰度)	人数 n	30	270	2.74	2.04	○
	平均値 m	3.5	3.0			
	標準偏差 σ	1.0	2.0			
Q4 (目先の利益の優先度)	人数 n	30	270	2.35	2.04	○
	平均値 m	4.3	4.0			
	標準偏差 σ	0.7	2.0			
Q5 (被害に遭う可能性予想)	人数 n	30	270	−1.36	2.04	×
	平均値 m	45.0	50.0			
	標準偏差 σ	20.0	21.0			

【図６】

行動特性抽出工程を例示するフローチャート



【図７】

行動ログデータテーブルの一例を説明する説明図

22

		ユーザID			…
		u0001	u0002	u0003	
所属グループ		低意識群	高意識群	低意識群	
警告画面表示時間	計測回数 c	5	3	4	
	平均値 m	2.1秒	4.1秒	2.5秒	
	標準偏差 σ	5.2秒	6.3秒	5.0秒	
送信メール数/日	計測回数 c	20	19	20	
	平均値 m	3.1通	2.2通	2.0通	
	標準偏差 σ	4.2通	5.1通	5.0通	
パッチ適用間隔	計測回数 c	4	4	4	
	平均値 m	14.1日	13.3日	15.0日	
	標準偏差 σ	2.2日	3.2日	3.0日	
…	…	…	…	…	…

【図８】

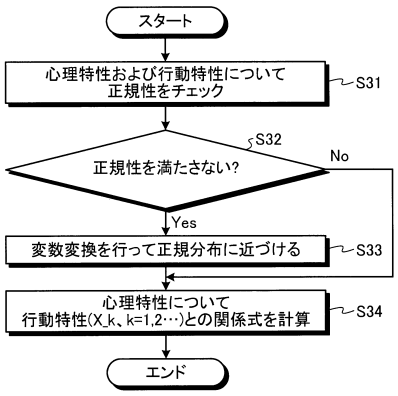
行動特性データテーブルの一例を説明する説明図

24

		低意識群 g1	高意識群 g2	t値	判定基準値	判定
警告画面表示時間	人数 n	30	270	-2.19	2.05	○
	平均値 m	2.0秒	4.0秒			
	標準偏差 σ	5.0秒	6.0秒			
送信メール数/日	人数 n	35	280	1.31	2.03	×
	平均値 m	3.0通	2.0通			
	標準偏差 σ	4.5通	5.0通			
パッチ適用間隔	人数 n	33	275	2.30	2.04	○
	平均値 m	14.0日	13.0日			
	標準偏差 σ	2.5日	3.0日			
…	…	…	…	…	…	…

【図９】

計算工程を例示するフローチャート



【図１０】

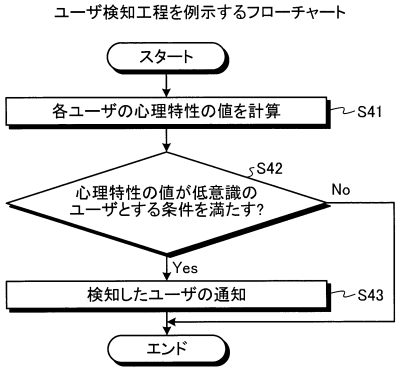
関係式データの一例を説明する説明図

32

心理特性(Y_i)	第1成分		第2成分		…
	行動特性(X_1)	回帰係数(a_1)	行動特性(X_2)	回帰係数(a_2)	
自信過剰度(Y_1)	警告画面表示時間	-3.1	パッチ適用間隔	2.2	
目先の利益優先度(Y_2)	警告画面表示時間	-2.3	パッチ適用間隔	1.4	
…	…	…	…	…	…

【図１１】

ユーザ検知工程を例示するフローチャート



【図１２】

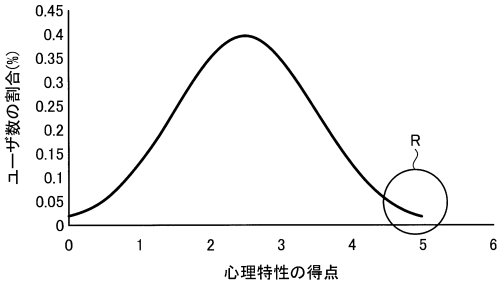
ユーザ検知テーブルの一例を説明する説明図

42

ユーザID	心理特性			…	判定
	Y_1 (自信過剰度 5段階評価)	Y_2 (目先の利益優先度 7段階評価)	Y_3 (情報共有度 6段階評価)		
u0001	4.8	3.1	3.2	…	Y_1
u0002	2.5	6.6	5.9	…	Y_2, Y_3
u0003	2.5	3.3	2.9	…	なし
…	…	…	…	…	…

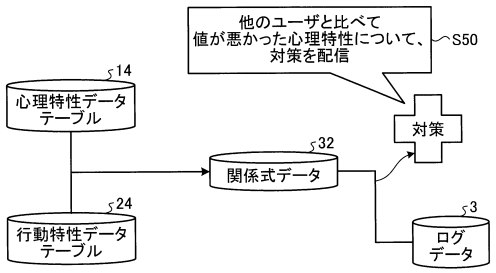
【図１３】

ユーザ検知の一例を説明する説明図



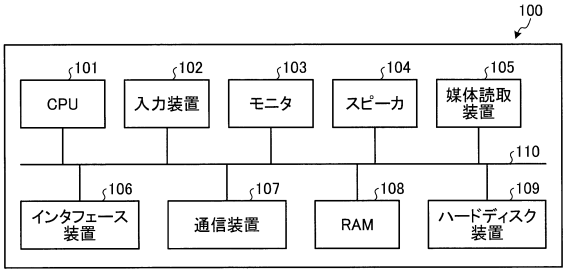
【図１４】

対策の配信の一例を説明する説明図



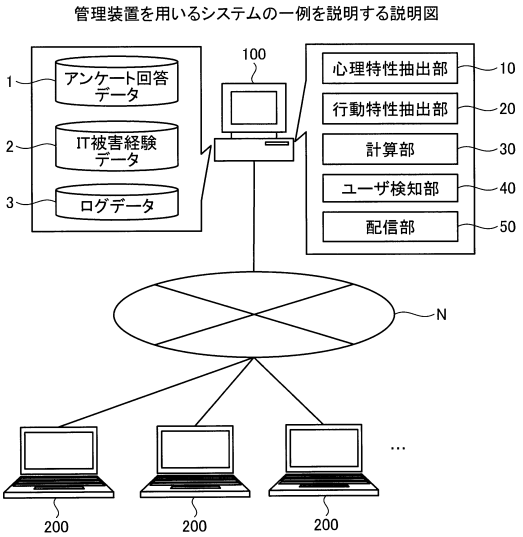
【図１５】

管理装置のハードウエア構成を例示するブロック図



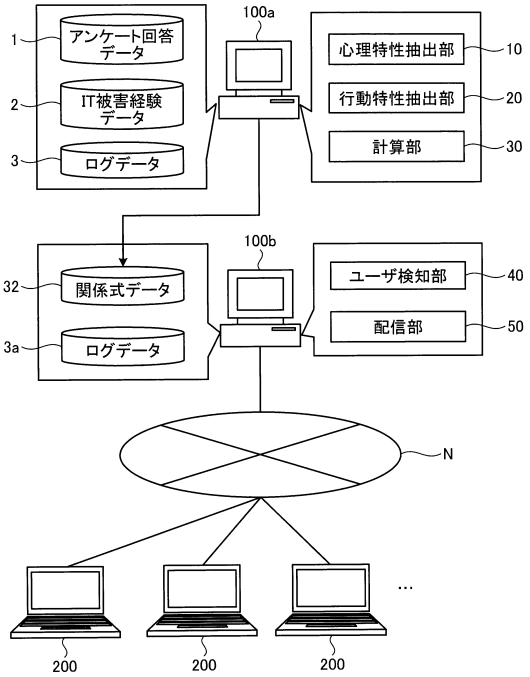
【図１６】

管理装置を用いるシステムの一例を説明する説明図



【図１７】

管理装置を用いるシステムの一例を説明する説明図



フロントページの続き

(72)発明者　武仲　正彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　佐藤　裕子

(56)参考文献　特開２０１２－０９４０５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　９９／００
Ｇ０６Ｆ　２１／００