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

特許第4887735号
(P4887735)

(45)発行日　平成24年2月29日(2012.2.29)　(24)登録日　平成23年12月22日(2011.12.22)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330D
G06F 21/22	(2006.01)	G06F	9/06	660E
G09C 1/00	(2006.01)	G09C	1/00	640E

請求項の数 8　(全 20 頁)

(21)出願番号　特願2005-316772 (P2005-316772)
(22)出願日　平成17年10月31日 (2005.10.31)
(65)公開番号　特開2007-122598 (P2007-122598A)
(43)公開日　平成19年5月17日 (2007.5.17)
審査請求日　平成20年10月17日 (2008.10.17)

(73)特許権者　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(74)代理人　110001254
特許業務法人光陽国際特許事務所
(74)代理人　100090033
弁理士　荒船　博司
(74)代理人　100093045
弁理士　荒船　良男
(72)発明者　高橋　英士朗
東京都八王子市石川町２９５１番地５　カシオ計算機株式会社　八王子技術センター内

審査官　石田　信行

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム及びプログラム

(57)【特許請求の範囲】
【請求項１】
アプリケーションの動作を複数の動作処理にグループ分けした場合の各動作グループ毎のセキュリティ制御条件を、複数の動作グループ毎に複数記憶するセキュリティ情報記憶手段と、
前記各動作グループ毎の複数のセキュリティ制御条件の内の何れのセキュリティ制御条件を利用するかを示す第一インデックス情報を前記各動作グループ毎に一つずつ定義し、一括して管理するロール情報を複数記憶するロール情報記憶手段と、
認証されるユーザ毎に、前記ロール情報の内のいずれのロール情報を利用するかを示す第二インデックス情報を対応付けて定義したユーザ定義記憶手段と、
認証されたユーザに対応付けて定義された第二インデックス情報を前記ユーザ定義情報手段から取得し、その取得した第二インデックス情報に対応するロール情報を前記ロール情報記憶手段から取得し、その取得したロール情報で一括して管理された各動作グループ毎の第一インデックス情報に基づいて、前記認証されたユーザに対応付けて定義された前記各動作グループ毎のセキュリティ制御条件を前記セキュリティ情報記憶手段から読み出す条件読出手段と、
前記条件読出手段で読み出された各セキュリティ制御条件に基づいて、前記各動作グループ毎のセキュリティ動作を実行制御する制御手段と、
を備えることを特徴とする情報処理装置。
【請求項２】

前記ロール情報は、対応するユーザに当該ロール情報を適用する日付に関する情報を含み、
前記条件読出手段は、前記日付に関する情報に応じてユーザに対応するロール情報を取得することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記ロール情報と前記セキュリティ制御条件を編集する編集手段を更に備えることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記セキュリティ制御条件は、ロール情報毎のアプリケーションプログラムの起動条件であるメニューセキュリティ情報であり、
前記制御手段は、前記取得されたロール情報及び前記メニューセキュリティ情報に基づいてメニュー表示に関する制御を行うことを特徴とする請求項１～３のいずれか一項に記載の情報処理装置。
【請求項５】
前記セキュリティ制御条件は、ロール情報毎のアプリケーションプログラムの参照項目に対応した制御条件である項目セキュリティ情報であり、
前記制御手段は、前記取得されたロール情報及び前記項目セキュリティ情報に基づいて表示項目に関する制御を行うことを特徴とする請求項１～３のいずれか一項に記載の情報処理装置。
【請求項６】
前記セキュリティ制御条件は、ロール情報毎の業務アプリケーションで使用する参照レコードに対応した制御条件であるレコードセキュリティ情報であり、
前記制御手段は、前記取得されたロール情報及び前記レコードセキュリティ情報に基づいて表示レコードに関する制御を行うことを特徴とする請求項１～３のいずれか一項に記載の情報処理装置。
【請求項７】
端末装置及び情報処理装置が互いに通信可能に接続され、端末装置から情報処理装置へのログイン時にユーザを認証し、この認証されたユーザに応じて情報処理装置が複数のアプリケーションの動作を行う情報処理システムにおいて、
アプリケーションの動作を複数の動作処理にグループ分けした場合の各動作グループ毎のセキュリティ制御条件を、複数の動作グループ毎に複数記憶するセキュリティ情報と、前記各動作グループ毎の複数のセキュリティ制御条件の内の何れのセキュリティ制御条件を利用するかを示す第一インデックス情報を前記各動作グループ毎に一つずつ定義し、一括して管理するロール情報を複数記憶するロール記憶情報と、認証されるユーザ毎に、前記ロール情報の内のいずれのロール情報を利用するかを示す第二インデックス方法を対応付けて定義したユーザ定義情報と、を記憶するデータベースサーバを更に有し、
前記情報処理装置は、
認証されたユーザに対応付けて定義された第二インデックス情報を前記データベースに記憶された前記ユーザ定義情報から取得し、その取得した第二インデックス情報に対応するロール情報を前記データベースに記憶された前記ロール情報記憶から取得し、その取得したロール情報で一括して管理された各動作グループ毎の第一インデックス情報に基づいて、前記認証されたユーザに対応付けて定義された前記各動作グループ毎のセキュリティ制御条件を前記データベースから読み出す条件読出手段と、
前記条件読出手段で読み出された各セキュリティ制御条件に基づいて、前記各動作グループ毎のセキュリティ動作を実行制御する制御手段と、
を備えることを特徴とする情報処理システム。
【請求項８】
ログイン時にユーザを認証し、この認証されたユーザに応じて複数のアプリケーションプログラムからなる業務アプリケーションの動作を行う情報処理装置のコンピュータに、
アプリケーションの動作を複数の動作処理にグループ分けした場合の各動作グループ毎

のセキュリティ制御条件を、複数の動作グループ毎に複数記憶するセキュリティ情報記憶機能と、
前記各動作グループ毎の複数のセキュリティ制御条件の内の何れのセキュリティ制御条件を利用するかを示す第一インデックス情報を前記各動作グループ毎に一つずつ定義し、一括して管理するロール情報を複数記憶するロール情報記憶機能と、
認証されるユーザ毎に、前記ロール情報の内のいずれのロール情報を利用するかを示す第二インデックス情報を対応付けて定義したユーザ定義記憶機能と、
認証されたユーザに対応付けて定義された第二インデックス情報を前記ユーザ定義情報機能から取得し、その取得した第二インデックス情報に対応するロール情報を前記ロール情報記憶機能から取得し、その取得したロール情報で一括して管理された各動作グループ毎の第一インデックス情報に基づいて、前記認証されたユーザに対応付けて定義された前記各動作グループ毎のセキュリティ制御条件を前記セキュリティ情報記憶機能から読み出す条件読出機能と、
前記条件読出手段で読み出された各セキュリティ制御条件に基づいて、前記各動作グループ毎のセキュリティ動作を実行制御する動作制御機能と、
を実現することを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザごとの権限に応じたセキュリティ制御を行う情報処理装置、情報処理システム及びプログラムに関する。
【背景技術】
【０００２】
従来から、企業などにおける情報処理装置では、見積書の作成や給与明細書の作成などを業務の内容に応じた業務アプリケーションを実行して業務処理を行っている。その業務アプリケーションでは、企業の社員であるユーザ（利用者、社員）をパスワードなどで認証し、その認証されたユーザの権限に応じて動作の制御を行うセキュリティ制御を行うことが一般的である。このため、企業の人事情報を元にユーザ毎の業務処理のセキュリティ制御を設定する場合は、営業、経理、人事などの各部門における様々な業務アプリケーションに対して行う必要があり、企業の規模が大きくなるほど煩雑なものであった。
【０００３】
この業務処理を行う情報処理装置におけるユーザ毎のセキュリティ制御の設定を容易に行う技術としては、例えば、人事情報と業務アプリケーション毎の権限情報を参照して、ユーザ個人の業務アプリケーションに対する権限を認証することで、人事情報や権限情報が更新された場合でも認証のための設定の更新を必要としない技術が特許文献１に開示されている。
【特許文献１】特開２００５－１０７９８４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、業務処理におけるセキュリティ制御では各業務アプリケーションの細部動作においてもユーザの属性に応じて実行規制や情報の秘匿などを行う場合があるが、上述した特許文献１などの従来技術では人事情報や権限情報などに応じて起動した後のセキュリティ制御を行う場合には業務アプリケーション毎に設定する必要があった。このため、より容易にセキュリティ制御を管理するには十分なものではなく、さらなる開発が望まれていた。
【０００５】
本発明は、このような課題に鑑みてなされたものであり、その目的とするところは、業務処理におけるユーザ毎のセキュリティ制御の管理を容易に行う技術を提供することである。

【課題を解決するための手段】
【０００６】
上記課題を解決するために、請求項１に記載の発明は、アプリケーションの動作を複数の動作処理にグループ分けした場合の各動作グループ毎のセキュリティ制御条件を、複数の動作グループ毎に複数記憶するセキュリティ情報記憶手段と、前記各動作グループ毎の複数のセキュリティ制御条件の内の何れのセキュリティ制御条件を利用するかを示す第一インデックス情報を前記各動作グループ毎に一つずつ定義し、一括して管理するロール情報を複数記憶するロール情報記憶手段と、認証されるユーザ毎に、前記ロール情報の内のいずれのロール情報を利用するかを示す第二インデックス情報を対応付けて定義したユーザ定義記憶手段と、認証されたユーザに対応付けて定義された第二インデックス情報を前記ユーザ定義情報手段から取得し、その取得した第二インデックス情報に対応するロール情報を前記ロール情報記憶手段から取得し、その取得したロール情報で一括して管理された各動作グループ毎の第一インデックス情報に基づいて、前記認証されたユーザに対応付けて定義された前記各動作グループ毎のセキュリティ制御条件を前記セキュリティ情報記憶手段から読み出す条件読出手段と、前記条件読出手段で読み出された各セキュリティ制御条件に基づいて、前記各動作グループ毎のセキュリティ動作を実行制御する制御手段と、を備えることを特徴とする。
【０００８】
請求項２に記載の発明は、請求項１に記載の発明において、前記ロール情報は、対応するユーザに当該ロール情報を適用する日付に関する情報を含み、前記条件読出手段は、前記日付に関する情報に応じてユーザに対応するロール情報を取得することを特徴とする。
【０００９】
請求項３に記載の発明は、請求項１又は２に記載の発明において、前記複数のロール情報と前記セキュリティ制御条件を編集する編集手段を更に備えることを特徴とする。
【００１０】
請求項４に記載の発明は、請求項１～３のいずれか一項に記載の発明において、前記セキュリティ制御条件は、ロール情報毎の様々なアプリケーションプログラムの起動条件であるメニューセキュリティ情報であり、前記制御手段は、前記取得されたロール情報及び前記メニューセキュリティ情報に基づいてメニュー表示に関する制御を行うことを特徴とする。
【００１１】
請求項５に記載の発明は、請求項１～３のいずれか一項に記載の発明において、前記セキュリティ制御条件は、ロール情報毎の様々な参照項目に対応した制御条件である項目セキュリティ情報であり、前記制御手段は、前記取得されたロール情報及び前記項目セキュリティ情報に基づいて表示項目に関する制御を行うことを特徴とする。
【００１２】
請求項６に記載の発明は、請求項１～３のいずれか一項に記載の発明において、前記セキュリティ制御条件は、ロール情報毎の業務アプリケーションで使用する参照レコードに対応した制御条件であるレコードセキュリティ情報であり、前記制御手段は、前記取得されたロール情報及び前記レコードセキュリティ情報に基づいて表示レコードに関する制御を行うことを特徴とする。
【００１３】
請求項７に記載の発明は請求項１に記載の発明に示した主要な機能を有する情報処理システムであり、請求項８に記載の発明は請求項１に記載の発明に示した主要な機能を実現するプログラムである。
【発明の効果】
【００１４】
請求項１、７、８に記載の発明によれば、ユーザ定義記憶手段にユーザに対応するロール情報を第二インデックス情報として定義し、そのロール情報は、アプリケーションの動作処理をグループ分けした複数のグループから、各グループごとに利用するセキュリテ

ィ制御条件を第一インデックス情報によって一括で管理しているため、前記第二インデックス情報を基にロール情報を取得し、その取得されたロール情報に対応付けられたセキュリティ制御条件を前記各第一インデックス情報に基づき取得することで、アプリケーションの動作の制御を容易に行うことができる。

【００１６】

請求項２に記載の発明によれば、ロール情報は、対応するユーザに当該ロール情報を適用する日付情報を含み、その日付に関する情報に応じてユーザに対応する権限を取得する構成であるため、日付に応じた柔軟なセキュリティ制御の設定を行うことができる。

【００１７】

請求項３に記載の発明によれば、ロール情報とセキュリティ制御条件を編集する編集手段を更に備えるため、セキュリティ制御に応じた機器の設定を行うことができる。

【００１８】

請求項４に記載の発明によれば、ロール情報毎の様々なアプリケーションプログラムの起動条件であるメニューセキュリティ情報に基づいたメニュー表示に関する制御を行うことができ、ユーザの権限に応じたメニュー構成で画面表示することができる。

【００１９】

請求項５に記載の発明によれば、ロール情報毎の様々な参照項目に対応した制御条件であるセキュリティ情報に基づいた表示項目に関する制御を行うことができ、ユーザの権限に応じた項目を画面表示することができる。

【００２０】

請求項６に記載の発明によれば、ロール情報毎の様々な参照レコードに対応した制御条件であるレコードセキュリティ情報に基づいて表示レコードに関する制御を行うことができ、ユーザの権限に応じたデータレコードを画面表示することができる。

【発明を実施するための最良の形態】

【００２１】

以下、図を参照して本発明の実施形態について詳細に説明するが、この発明は、この実施の形態に限定されない。また、この発明の実施の形態は発明の最も好ましい形態を示すものであり、発明の用途はこれに限定しない。

【００２２】

［第１の実施の形態］

先ず、図１～図７を参照して、本発明の第１の実施形態について説明する。

【００２３】

図１は、本発明である情報処理装置１の機能的構成を模式的に示したブロック図であり、図２は、記憶装置１３に格納されるファイル構成を模式的に示した図であり、図３（ａ）は、ユーザ情報定義ファイル１３１の内容を例示する図であり、図３（ｂ）は、システムセキュリティ情報定義ファイル１３２の内容を例示する図であり、図３（ｃ）は、レコードセキュリティ情報設定ファイル１３３の内容を例示する図であり、図３（ｄ）は、メニューセキュリティ情報設定ファイル１３４の内容を例示する図であり、図３（ｅ）は、社員属人情報管理ファイル１３７の内容を例示する図であり、図４は、情報処理装置１における動作処理を示したフローチャートであり、図５は、情報処理装置１における社員情報更新処理を示したフローチャートであり、図６は、情報処理装置１における業務処理の概要を例示する図であり、図７（ａ）は、ユーザの属人情報に対応したセキュリティ制御を例示する表であり、図７（ｂ）は、ユーザの属人情報の更新に応じたセキュリティ制御を例示する図である。

【００２４】

図１に示すように、情報処理装置１は、ＣＰＵ１１、ＲＡＭ１２、記憶装置１３、表示装置１４及び入力装置１５を備え、各部はバス１６により互いに電気的に接続される構成であるＰＣ（Personal Computer）やＷＳ（Work Station）等の情報機器である。

【００２５】

ＣＰＵ１１（Central Processing Unit）は、特に図示しないＲＯＭ（Read Only M

emory）や内部ＲＡＭ（Randam Access Memory）を備え、当該ＲＯＭや記憶装置１３に格納された各種制御プログラムやデータを読み出し、その内部ＲＡＭやＲＡＭ１２に形成された作業領域に展開して、該各種制御プログラムやデータに応じた処理を実行することで情報処理装置１の各部を統括制御する。また、ＣＰＵ１１は、特に図示しない常時一定周波数を発信する水晶発振器によるクロック信号を基準に動作するとともに、当該クロック信号を計数して現在の日付や時刻を計時する機能を有する。

【００２６】

ＲＡＭ１２は、格納先であるアドレスを指定することでデータの読み書きを自在に行い、上述したＣＰＵ１１により実行制御される各種制御プログラムやデータを一時的に格納する作業領域を形成する。具体的には、ＲＡＭ１２は、後述する処理で作成されるユーザセキュリティ情報１２１を作業領域に格納する。

【００２７】

記憶装置１３は、ＣＰＵ１１からの指示に応じて読み書き可能な磁気的又は光学的記録媒体、若しくは半導体等の不揮発性メモリであり、ユーザ情報定義ファイル１３１、システムセキュリティ情報定義ファイル１３２、レコードセキュリティ情報設定ファイル１３３、メニューセキュリティ情報設定ファイル１３４、項目セキュリティ情報設定ファイル１３５、社員情報管理ファイル１３６、社員属人情報管理ファイル１３７及び情報履歴管理ファイル１３８等の各種データファイルを格納する。具体的には、記憶装置１３は、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、ＤＶＤ－Ｒ、ＤＶＤ－Ｒ／Ｗ、ＤＶＤ＋Ｒ／Ｗ、ＤＶＤ－ＲＡＭ、ブルーレイディスク、ＭＯディスク、ＰＣカード、ＳＤカード、メモリースティック（登録商標）、スマートメディア、コンパクトフラッシュ（登録商標）、ｘＤ－Ｐｉｃｔｕｒｅカード、ＨＤＤ、及びＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）などである。

【００２８】

記憶装置１３が格納する各種データファイルについては、図２に示すように、各データファイルにおけるテーブルの一つの項目と他のデータファイルにおけるテーブルの一つの項目とが関連付けられて構成される。具体的には、ユーザ情報定義ファイル１３１とシステムセキュリティ情報定義ファイル１３２とがロールＩＤで、システムセキュリティ情報定義ファイル１３２とレコードセキュリティ情報設定ファイル１３３とがレコードグループＩＤで、システムセキュリティ情報定義ファイル１３２とメニューセキュリティ情報設定ファイル１３４とがメニューグループＩＤで、システムセキュリティ情報定義ファイル１３２と項目セキュリティ情報設定ファイル１３５とが項目グループＩＤで、ユーザ情報定義ファイル１３１と社員情報管理ファイル１３６、社員属人情報管理ファイル１３７及び情報履歴管理ファイル１３８とが社員番号でそれぞれ関連付けられている。

【００２９】

ユーザ情報定義ファイル１３１は、情報処理装置１のユーザを識別するためにユーザ毎に「ユーザＩＤ」を格納し、その「ユーザＩＤ」毎にログインを認証するための「パスワード」、各種セキュリティ情報のインデックスである「ロールＩＤ」及び社員情報のインデックスである「社員番号」等のシステム情報を設定するファイルである。例えば図３（ａ）に示すように、「ユーザＩＤ」が「test」であるユーザのシステム情報がテーブル形式で格納される。

【００３０】

システムセキュリティ情報定義ファイル１３２は、「ロールＩＤ」毎に、セキュリティ動作を実施する会社を示す「操作会社」、業務システムの種別を示す「システム種別」、業務操作が可能な範囲を示す「操作範囲区分」、セキュリティ動作を発動する基準日に関する情報である「基準日情報」及び各セキュリティ動作に関する情報のインデックスである「メニューグループＩＤ」・「レコードグループＩＤ」・「項目グループＩＤ」等を設定するファイルである。例えば図３（ｂ）に示すように、「ロールＩＤ」が「jinji」である各種セキュリティ情報がテーブル形式で格納される。

【００３１】

レコードセキュリティ情報設定ファイル１３３は、情報処理に関するデータレコードを識別する「レコードグループＩＤ」毎に、参照するユーザの情報（属人情報）の項目名を設定する「セキュリティ項目名」、セキュリティ制御を設定する際の条件などを演算するための「演算子」、この「レコードグループＩＤ」に関するセキュリティ情報である「セキュリティ項目値」及び他の「レコードグループＩＤ」などとの論理条件を指定する「条件接続詞」等を設定し、データのレコードに対するアクセス権限の有無などのセキュリティ制御を設定するファイルである。

【００３２】

「演算子」としては、例えば「＝」・「＞」・「＜」などの比較演算子があり、「セキュリティ項目値」と対象となるレコードとの間でセキュリティ制御の有無の判定に用いられる。「セキュリティ項目値」としては、アクセス制御を判定する際の値を直に格納する構成以外に、「セキュリティ項目名」に格納された参照先であるユーザに関する情報を参照するように指示する所定のリテラルを格納する構成であってもよい。

【００３３】

レコードセキュリティ情報設定ファイル１３３は、例えば図３（ｃ）に示すように、レコードグループＩＤが「２００」である場合のユーザに関する情報の参照先として社員属人情報管理ファイル１３７の「所属」や、セキュリティ制御を判定する際の比較演算子として「＝」及びユーザに関する情報を参照することを示すリテラルである「自」がテーブル形式で格納される。なお、このユーザに関する情報を参照することを示すリテラルやその参照先に関する情報は、レコードセキュリティ情報設定ファイル１３３だけでなく他のセキュリティ情報設定ファイルにも設けられる構成であって良い。

【００３４】

メニューセキュリティ情報設定ファイル１３４は、「メニューグループＩＤ」に対し、メニューを識別する「メニューＩＤ」及びそのメニューによる処理の起動情報などを格納する「起動コマンド」等を設定することで、「メニューグループＩＤ」毎にメニューを登録してメニューの表示／非表示や起動の可否などを制御するファイルである。例えば図３（ｄ）に示すように、「メニューグループＩＤ」が「１００」である場合の「メニューＩＤ」である「１０００１」や「１０００２」に対して、「起動コマンド」として「登録」や「閲覧」がテーブル形式で格納される。

【００３５】

項目セキュリティ情報設定ファイル１３５は、「項目グループＩＤ」に対し、「項目群コード」及び「参照区分」等を設定して、各項目群コードで設定されるデータ項目の表示／非表示などのセキュリティ制御を指定するファイルである。なお、項目毎のセキュリティ制御の設定には、表示／非表示以外にその項目に関するデータ変更／登録の禁止などでもよく、特に限定しない。

【００３６】

社員情報管理ファイル１３６は、ユーザ情報定義ファイル１３１における「社員番号」をインデックスとしてユーザＩＤで識別される社員の個人情報を「氏名」や「住所」等に格納するファイルであり、同様に社員属人情報管理ファイル１３７は、「社員番号」をインデックスとして社員の所属や役職を示す情報を「所属」又は「役職」等に格納するファイルであり、情報履歴管理ファイル１３８は「社員番号」をインデックスとして社員の人事経歴や将来の人事異動の予定などの情報を「履歴情報１Ａ」、「履歴情報１Ｂ」…に格納するファイルである。これらのファイルは、ユーザの属人情報を記憶するものであり、例えば図３（ｅ）に示すように、社員属人情報管理ファイル１３７には「社員番号」として「１０」等の数値が格納され、それに対応する「所属」を示す値として「５００」等の数値が格納される。

【００３７】

表示装置１４は、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などのディスプレイであり、画面上にＣＰＵ１１からの画像信号に応じた画像を表示する。

【００３８】
入力装置１５は、情報処理装置１に対する操作指示を入力するための数字キー、文字キー、各種機能キー等から構成されるキーボードや、マウス、タッチパネル等のポインティングデバイスであり、ユーザの操作に応じた操作信号をＣＰＵ１１に出力する。
【００３９】
次に、ＣＰＵ１１が制御して行う情報処理装置１の動作処理について説明する。図４に示すように、ＣＰＵ１１は、入力装置１５からのＩＤやパスワードの入力などによる起動操作を受け付け（ステップＳ１１）、その入力された情報とユーザ情報定義ファイル１３１に格納された情報とを照合して認証するシステムログイン処理を行う（ステップＳ１２）。
【００４０】
次いで、ステップＳ１２で認証されたユーザの「ユーザＩＤ」を元に前述した「ロールＩＤ」をキーとしてシステムセキュリティ情報定義ファイル１３２に格納された各種セキュリティを参照する際に必要な情報（「メニューグループＩＤ」、「レコードグループＩＤ」、「項目グループＩＤ」）が取得され、その取得された情報とユーザ情報定義ファイル１３１の情報とを合わせた情報がＲＡＭ１２の所定領域にユーザセキュリティ情報１２１として格納されるユーザセキュリティ情報取得処理が行われる（ステップＳ１３）。
【００４１】
次いで、ユーザセキュリティ情報１２１の「レコードグループＩＤ」を元にしてレコードセキュリティ情報設定ファイル１３３からデータレコード毎のセキュリティ制御に関する情報が取得され、ユーザの属性情報等に応じたデータレコードの参照やデータレコードへのデータの登録などのレコード毎のセキュリティ制御に関する条件が作成されてユーザセキュリティ情報１２１に格納される（ステップＳ１４）。
【００４２】
なお、このステップＳ１４においては、レコードセキュリティ情報設定ファイル１３３にユーザの属人情報などの参照を示すリテラル（例えば前述の「自」）などが格納されている場合は、情報の参照先である社員情報管理ファイル１３６、社員属人情報管理ファイル１３７又は情報履歴管理ファイル１３８の値（例えば前述の「所属」の場合は社員属人情報管理ファイル１３７の「所属」に格納される値）が格納される。
【００４３】
次いで、ユーザセキュリティ情報１２１の「メニューグループＩＤ」を元にしてメニューセキュリティ情報設定ファイル１３４から起動可能なメニューの情報が取得されるメニューセキュリティ処理が行われ（ステップＳ１５）、その取得された情報に基づき、例えば起動可能なメニューのみの表示を指示するメニュー表示処理が行われて（ステップＳ１６）、表示装置１４にメニュー画面が表示される。
【００４４】
次いで、表示装置１４に表示されたメニュー画面を元にして行われるユーザのメニュー選択などによる業務処理画面の起動指示が入力装置１５から受け付けられ（ステップＳ１７）、ユーザセキュリティ情報１２１の「項目グループＩＤ」を元にして起動する業務処理に係る項目の表示／非表示などのセキュリティ制御に関する情報が項目セキュリティ情報設定ファイル１３５から取得される項目セキュリティ処理が行われ（ステップＳ１８）、その項目毎のセキュリティ制御に応じてデータ項目を表示する業務画面表示処理が行われる（ステップＳ１９）。
【００４５】
次いで、表示装置１４に表示された業務処理画面を元にして行われる社員レコード（社員番号）などを指定したレコードへのアクセス指示が入力装置１５から受け付けられ（ステップＳ２０）、ユーザセキュリティ情報１２１に格納されたレコード毎のセキュリティ制御に関する条件を元に、アクセス指示されたレコードに関するセキュリティ制御の条件が取得されるレコードセキュリティ処理が行われ（ステップＳ２１）、その取得されたセキュリティ制御の条件に応じてデータに対するアクセス（閲覧）権の有無が判断されて、

アクセスが可能なデータが取得されるデータアクセス処理が行われ（ステップＳ２２）、その取得されたデータを表示装置１４に表示するデータ表示処理が行われて（ステップＳ２３）、終了する。

【００４６】

ここで、業務処理におけるデータ表示以外に、ステップＳ１６までの処理により表示装置１４に表示されるメニュー画面の後に、ユーザからの指示でＣＰＵ１１が行う社員情報更新処理について説明する。

【００４７】

図５に示すように、ＣＰＵ１１は、ステップＳ１６以降の処理において、社員情報の更新画面表示の指示を入力装置１５から受け付け（ステップＳ３０）、ステップＳ１８と同様に起動する更新処理に係る項目のセキュリティ制御に関する情報を項目セキュリティ情報設定ファイル１３５から取得する項目セキュリティ処理を行い（ステップＳ３１）、その情報に応じたデータ項目による社員情報の更新画面を表示装置１４に表示する（ステップＳ３２）。

【００４８】

次いで、更新する社員に関して社員番号の入力による社員レコードへのアクセス指示が入力装置１５から受け付けられ（ステップＳ３３）、前述したレコードセキュリティ処理（ステップＳ２１）、データアクセス処理（ステップＳ２２）及びデータ表示処理（ステップＳ２３）と同様の処理が行われて更新対象の社員に関するデータが表示装置１４に表示される（ステップＳ３４～Ｓ３６）。

【００４９】

次いで、所属変更や役職変更など更新する社員情報と共に、その情報が発令される人事上の基準日やセキュリティ上の基準日の更新指示が入力装置１５から受け付けられ（ステップＳ３７）、その受け付けられた情報に基づいてシステムセキュリティ情報定義ファイル１３２の「基準日情報」や情報履歴管理ファイル１３８の履歴情報の更新による社員情報基準日の設定が行われて（ステップＳ３８）、終了する。

【００５０】

以上に示した構成・動作により、情報処理装置１は、図６に示すように、ログイン時に認証したユーザが操作する場合に各種処理において行うセキュリティ制御に関する情報であるユーザセキュリティ情報１２１を作成し、それに基づいてそのユーザの権限に応じたメニューの表示の有無や業務処理画面におけるレコードデータや項目データの表示の可否等のセキュリティ制御を行う構成である。このため、情報処理装置１は、ユーザ毎のセキュリティ制御に関する権限を一元的に設定し、ユーザセキュリティ情報１２１により様々な動作制御に対応付けて管理することが可能となり、容易にセキュリティ制御の管理を行うことができる。

【００５１】

また、情報処理装置１は、ユーザセキュリティ情報１２１の操作範囲やメニューグループＩＤに応じてアプリケーションプログラムの起動などを指示するメニューを表示する構成であるため、ユーザに応じて操作可能なメニューだけを表示するセキュリティ制御を行うことができる。

【００５２】

また、情報処理装置１は、ユーザセキュリティ情報１２１のレコードグループＩＤや項目グループＩＤに応じてデータレコードやデータ項目の表示／非表示を制御し、ユーザの権限に応じた情報だけを表示するセキュリティ制御を行うことができる。

【００５３】

また、情報処理装置１は、社員情報更新処理により、セキュリティ制御の設定を行うことができる。更にユーザセキュリティ情報１２１によるセキュリティ制御に応じて社員情報更新処理を行う構成であり、登録や変更などの権限を持つユーザのみが行えるため、システム管理者以外の人事担当者などが設定を行うことができるとともに、セキュリティの設定を安全に管理することができる。

【００５４】
具体的には、情報処理装置１は、図７（ａ）に示すように、ログイン時のユーザに対応する「人事担当者」・「経理担当者」・「システム管理者」などの権限ごとに、「社員登録」・「権限、人事情報設定」・「パスワード設定」・「社員給与閲覧」・「社員給与設定」などの動作条件に応じた実行制御を行うことができる。
【００５５】
また、情報処理装置１は、システムセキュリティ情報定義ファイル１３２にセキュリティに関する日付情報と情報履歴管理ファイル１３８に人事異動などの履歴に関する情報（属人情報）とを格納する構成であり、前述したステップＳ１４、Ｓ１５、Ｓ１８、Ｓ２１又はＳ２２において、その履歴に関する情報に基づいたユーザの人事異動などの発令日に前後してセキュリティに関する日付情報に応じた幅でユーザの権限を調整する。
【００５６】
このため、情報処理装置１は、図７（ｂ）に示すように、現実のユーザの人事扱いが発令日を境に人事から経理に移行する場合においても、そのユーザのセキュリティに関する制御に幅を持たせて柔軟に対応することができ、人事異動に伴うセキュリティ制御の変更によりデータの引き継ぎを困難にさせることがない。
【００５７】
［第２の実施の形態］
次に、図８～図１６を参照して、本発明の第２の実施形態について説明する。ただし、前述した第１の実施形態と同一な構成や動作についての説明は省略する。
【００５８】
図８は、本発明である情報処理システム１００の概略を示した概略図であり、図９は、端末２、データベースサーバ４の機能的構成を模式的に示したブロック図であり、図１０は、サーバ３の機能的構成を模式的に示したブロック図であり、図１１は、データベースサーバ４におけるデータベース（ＤＢ）の構成を模式的に示した図であり、図１２は、情報処理システム１００における動作処理を示したラダーチャートであり、図１３は、情報処理システム１００における社員情報更新処理を示したラダーチャートであり、図１４は、情報処理システム１００における業務処理の概要を例示する図であり、図１５は、ユーザの所属する会社の更新に対応したセキュリティ制御を例示する図である。
【００５９】
図８に示すように、情報処理システム１００は、端末２、サーバ３及びデータベースサーバ４がインターネットやイントラネットなどである通信ネットワークＮにより有線又は無線で互いに通信可能に接続する構成である。なお、端末２は、図示した端末２ａ、２ｂ、２ｃ…のように複数備える構成であって良い。
【００６０】
端末２、データベースサーバ４の内部構成については、図９に示すように、前述した情報処理装置１と同様の各部（ＣＰＵ２１、ＲＡＭ２２、記憶装置２３、表示装置２４及び入力装置２５）及び通信装置２６を備え、各部はバス２７により互いに電気的に接続される構成の情報機器である。
【００６１】
通信装置２６は、無線通信回路及びアンテナや、有線で通信を行うための通信インターフェイスを備えた回路部であり、ＣＰＵ２１の指示に基づいて通信ネットワークＮに接続する情報機器との間でデータの送受信を行う。
【００６２】
上記構成により、端末２は、例えばＰＣやＷＳなどであり、通信ネットワークＮに接続するサーバ３が提供するデータやサービスを利用する操作端末として動作する。また、データベースサーバ４は、リレーショナルデータベースとしての機能を通信ネットワークＮに接続する機器に提供する情報処理装置として動作する。具体的には、データベースサーバ４は、業務処理などに係る各種データを複数のテーブル（ＤＢ）で管理し、他の機器からのＳＱＬ（Structured Query Language）によりＩＤ番号や名前などのキーとなるデ

ータを指定した指示に応じてデータの登録、結合、抽出などを行い、その結果を返信する。

【００６３】

サーバ３の内部構成については、図１０に示すように、前述の情報処理装置１と同様の各部（ＣＰＵ３１、ＲＡＭ３２、記憶装置３３、表示装置３４及び通信装置３６）及び前述の通信装置２６と同様に通信ネットワークＮに接続する情報機器との間でデータの送受信を行う通信装置３６を備え、各部はバス３７により互いに電気的に接続される構成の情報機器である。また、サーバ３は、後述する動作処理により作成されるユーザセキュリティ情報１２１をＲＡＭ３２に格納する。

【００６４】

上記構成により、サーバ３は、通信ネットワークＮを介して接続するクライアントである端末２に対してデータベースサーバ４を利用した業務処理などのサービスを提供する。例えば、サーバ３は、通信ネットワークＮを介したＨＴＴＰ（HyperText Transfer Protocol）により端末２で実行されるブラウザから引数などを伴って呼び出されることでプログラムを起動して処理するＣＧＩ（Common Gateway Interface）やＳＳＩ（Server Side Include）の機能や、ＡＳＰ（Active Server Pages）、ＪＳＰ（Java(登録商標) Server Pages）及びＰＨＰ（PHP:Hypertext Preprocessor）などの前記ＣＧＩの機能をサーバに組み込んでスクリプト処理をするサーバサイドスクリプティング技術（Server Side Scripting）による機能を利用した業務処理Ｗｅｂサーバとして動作し、ＳＱＬによる指示をデータベースサーバ４に送って得られるデータに基づいた業務情報をＷｅｂページとして端末２のブラウザに送信する情報処理装置である。

【００６５】

データベースサーバ４が扱うＤＢの構成については、図１１に示すように、
ユーザ情報定義ＤＢ４３１とシステムセキュリティ情報定義ＤＢ４３２とがロールＩＤをキーとして、システムセキュリティ情報定義ＤＢ４３２とレコードセキュリティ情報設定ＤＢ４３３とがレコードグループＩＤをキーして、システムセキュリティ情報定義ＤＢ４３２とメニューセキュリティ情報設定ＤＢ４３４とがメニューグループＩＤをキーとして、システムセキュリティ情報定義ＤＢ４３２と項目セキュリティ情報設定ＤＢ４３５とが項目グループＩＤをキーとして、ＶＩＥＷ社員情報４４０、社員情報管理ＤＢ４３６、社員属人情報管理ＤＢ４３７、情報履歴管理ＤＢ４３８及び社員所属会社管理ＤＢ４３９とユーザ情報定義ＤＢ４３１とが社員番号をキーとして関連付けられる。

【００６６】

ユーザ情報定義ＤＢ４３１、システムセキュリティ情報定義ＤＢ４３２、レコードセキュリティ情報設定ＤＢ４３３、メニューセキュリティ情報設定ＤＢ４３４、項目セキュリティ情報設定ＤＢ４３５、社員情報管理ＤＢ４３６及び社員属人情報管理ＤＢ４３７のデータ構成については、システムセキュリティ情報定義ＤＢ４３２に操作会社に関する情報である「操作会社」を格納すること以外、前述した情報処理装置１におけるユーザ情報定義ファイル１３１、システムセキュリティ情報定義ファイル１３２、レコードセキュリティ情報設定ファイル１３３、メニューセキュリティ情報設定ファイル１３４、項目セキュリティ情報設定ファイル１３５、社員情報管理ファイル１３６、社員属人情報管理ファイル１３７と同様な情報をＤＢとして保持する構成以外は同一であるため説明を省略する。

【００６７】

情報履歴管理ＤＢ４３８は、前述した情報履歴管理ファイル１３８と同一なデータ構成であり、社員の人事経歴や将来の人事異動の予定などの情報を情報処理システム１００を利用する会社毎（系列・関連会社）に仕分けた情報履歴管理ＤＢ４３８ａ、４３８ｂとして保持する。

【００６８】

社員所属会社管理ＤＢ４３９は、「社員番号」をキー値として、所属する系列・関連会社などを示す情報である「会社」、人事・経理などの利用するシステム種別を示す情報である「システム種別」、他の業務を兼務する場合の情報である「兼務区分」、社員属人情

報管理ＤＢ４３７の所属や役職に対応したセキュリティ制御の情報である「Ｓ所属」・「Ｓ役職」を格納する構成である。

【００６９】

ＶＩＥＷ社員情報４４０は、社員番号をキー値として、ＳＱＬコマンドにより社員情報管理ＤＢ４３６、社員属人情報管理ＤＢ４３７及び社員属人情報管理ＤＢ４３７からデータを抽出したＶＩＥＷテーブルである。

【００７０】

次に、情報処理システム１００における動作処理の詳細を図１２を参照して説明する。なお、図１２において、ステップＳ２０１～Ｓ２０６の各処理については端末２のＣＰＵ２１が行い、ステップＳ３０１～Ｓ３１０の各処理についてはサーバ３のＣＰＵ３１が行い、ステップＳ４０１～Ｓ４０６の各処理についてはデータベースサーバ４のＣＰＵ２１が行う。

【００７１】

先ず、ユーザからの「ユーザＩＤ」や「パスワード」の入力などによる起動操作が端末２の入力装置２５から受け付けられてサーバ３に送信され（ステップＳ２０１）、その入力された「ユーザＩＤ」を元にしてユーザ情報定義ＤＢ４３１をデータベースサーバ４から受け取られ、入力された「パスワード」とユーザ情報定義ＤＢ４３１に格納された「パスワード」とを照合して認証するシステムログイン処理が行われる（ステップＳ３０１、Ｓ４０１）。

【００７２】

次いで、認証された「ユーザＩＤ」を元に「ロールＩＤ」をキーとしたシステムセキュリティ情報定義ＤＢ４３２をデータベースサーバ４から受け取り、前述したステップＳ１３と同様にユーザセキュリティ情報１２１がＲＡＭ３２に格納されるユーザセキュリティ情報取得処理がサーバ３で行われる（ステップＳ３０２、Ｓ４０２）。

【００７３】

次いで、ユーザセキュリティ情報１２１の「レコードグループＩＤ」をキー値とてレコードセキュリティ情報設定ＤＢ４３３をデータベースサーバ４から受け取り、前述したステップＳ１４と同様にレコード毎のセキュリティ制御に関する条件がサーバ３で作成されてユーザセキュリティ情報１２１に格納されるレコードセキュリティ条件作成処理がサーバ３で行われる（ステップＳ３０３、Ｓ４０３）。

【００７４】

次いで、ユーザセキュリティ情報１２１の「メニューグループＩＤ」をキー値としてメニューセキュリティ情報設定ＤＢ４３４をデータベースサーバ４から受け取り、前述したステップＳ１５と同様にメニューセキュリティ処理がサーバ３で行われ（ステップＳ３０４、Ｓ４０４）、サーバ３からそのメニューセキュリティ処理に応じたメニュー情報が端末２に送信され、端末２の表示装置２４にメニュー画面が表示される（ステップＳ３０５、Ｓ２０２）。

【００７５】

次いで、ユーザからの業務処理画面の起動指示が端末２の入力装置２５から受け付けられ（ステップＳ２０３）、ユーザセキュリティ情報１２１の「項目グループＩＤ」をキー値として項目セキュリティ情報設定ＤＢ４３５をデータベースサーバ４から受け取り、前述したステップＳ１８と同様に項目セキュリティ処理がサーバ３で行われ（ステップＳ３０６、Ｓ４０５）、サーバ３からその項目セキュリティ処理に応じてデータ項目を表示する業務画面情報が端末２に送信され、端末２の表示装置２４に業務画面が表示される（ステップＳ３０７、Ｓ２０４）。

【００７６】

次いで、「社員番号」を指定した社員レコードへのアクセス指示が端末２の入力装置２５から受け付けられ（ステップＳ２０５）、前述したステップＳ２１と同様なレコードセキュリティ処理が行われ（ステップＳ３０８）、「社員番号」をキー値としたＶＩＥＷ社員情報４４０をデータベースサーバ４から受け取り、前述したステップＳ２２と同様にア

クセスが可能なデータが取得されるデータアクセス処理が行われ（ステップＳ３０９、Ｓ４０６）、その取得されたデータが端末２に送信され、端末２の表示装置２４に表示されて（ステップＳ３１０、Ｓ２０６）、終了する。

【００７７】

ここで、情報処理システム１００において、メニュー画面が表示された後（ステップＳ２０２）に行われる社員情報更新処理について、図１３を参照して説明する。なお、図１３において、ステップＳ２１１～Ｓ２１５の各処理については端末２のＣＰＵ２１が行い、ステップＳ３１１～Ｓ３１６の各処理についてはサーバ３のＣＰＵ３１が行い、Ｓ４１１～Ｓ４１３の各処理についてはデータベースサーバ４のＣＰＵ２１が行う。

【００７８】

先ず、社員情報の更新画面表示の指示が端末２の入力装置２５から受け付けられてサーバ３に送信され（ステップＳ２１１）、項目セキュリティ情報設定ＤＢ４３５をデータベースサーバ４から受け取り、前述したステップＳ３１と同様に更新処理に係る項目セキュリティ処理が行われ（ステップＳ３１１、Ｓ４１１）、その情報に応じたデータ項目による社員情報の更新画面情報が端末２に送信され、端末２の表示装置２４に更新画面が表示される（ステップＳ３１２、Ｓ２１２）。

【００７９】

次いで、更新する社員に関して社員番号の入力による社員レコードへのアクセス指示が端末２の入力装置２５から受け付けられてサーバ３に送信され（ステップＳ２１３）、前述したステップＳ３０８～Ｓ３１０、Ｓ４０６及びＳ２０６に示した処理と同一の処理が行われて更新対象の社員に関するデータが端末２の表示装置２４に表示される（ステップＳ３１３～Ｓ３１５、Ｓ４１２及びＳ２１４）。

【００８０】

次いで、所属・役職・所属会社変更などの更新する社員情報と共に、その情報が発令される人事上の基準日やセキュリティ上の基準日の更新指示が端末２の入力装置２５から受け付けられてサーバ３に送信され（ステップＳ２１５）、その送信された情報に基づいたＳＱＬ文による更新コマンドがデータベースサーバ４に送信されて（ステップＳ３１６）、社員情報やその情報が発令される人事上の基準日やセキュリティ上の基準日などを格納するシステムセキュリティ情報定義ＤＢ４３２、社員属人情報管理ＤＢ４３７又は社員所属会社管理ＤＢ４３９などが更新され（ステップＳ４１３）、終了する。

【００８１】

以上に示した構成・動作により、端末２、サーバ３及びデータベースサーバ４が通信ネットワークＮにより通信可能に接続される情報処理システム１００においても、業務処理におけるユーザ毎のセキュリティ制御の管理を容易に行うことができる。具体的には、図１４に示すように、端末２からの操作指示により、ログイン時に認証したユーザが操作する場合に各種処理において行うセキュリティ制御に関する情報であるユーザセキュリティ情報１２１を作成し、それに基づいてそのユーザの権限に応じたメニューの表示の有無や業務処理画面におけるレコードデータや項目データの表示の可否等のセキュリティ制御を行う構成である。

【００８２】

また、情報処理システム１００は、社員情報管理ＤＢ４３６、社員属人情報管理ＤＢ４３７及び社員が所属する系列・関連会社などの情報を格納する社員所属会社管理ＤＢ４３９をＶＩＥＷ社員情報４４０として抽出し、レコードセキュリティ動作を行う構成であり、所属する会社が違う場合においても同一のユーザセキュリティ情報１２１で管理することができる。

【００８３】

また、情報処理システム１００は、情報処理装置１と同様にセキュリティに関する日付情報と人事異動などの履歴に関する情報をデータベースサーバ４に格納する構成であり、前述したステップＳ３０３、Ｓ３０４、Ｓ３０６、Ｓ３０８又はＳ３０９において、その履歴に関する情報に基づいたユーザの所属会社変更などの人事発令日前後してセキュリテ

ィに関する日付情報に応じた幅でユーザの権限を調整する。

【００８４】

このため、情報処理システム１００は、図１５に示すように、現実のユーザの所属会社が発令日を境に変更する場合に場合においても、そのユーザのセキュリティに関する制御に幅を持たして柔軟に対応することができ、所属会社の変更に伴うセキュリティ制御の変更でデータの引き継ぎを困難にさせることがない。

【００８５】

なお、本実施の形態における記述は、本発明の一例を示すものであり、これに限定しない。本発明における情報処理装置１又は情報処理システム１００の細部構成及び細部動作に関しては、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。例えば、例示した各種情報ファイルにおける数値等は、他のリテラルであって良く特に限定しない。

【００８６】

また、ユーザを識別するために入力装置１５から受け付ける情報は、本実施の形態ではキーボードなどから入力されるユーザ名やパスワード等とする構成を示したが、入力装置１５としてカードリーダを備えてユーザが所持する磁気カード又はＩＣカードを読み取って得られる情報や、更に、入力装置１５として静電容量方式の半導体チップ、ＣＣＤカメラ、赤外線カメラ又はマイクなどを備え、それらから得られる指紋情報、顔画像情報、目の光彩情報、手のひら静脈情報又は音声情報などの生体情報であってもよく、特に限定しない。

【図面の簡単な説明】

【００８７】

【図１】本発明である情報処理装置１の機能的構成を模式的に示したブロック図である。

【図２】記憶装置１３に格納されるファイル構成を模式的に示した図である。

【図３】（ａ）は、ユーザ情報定義ファイル１３１の内容を例示する図であり、（ｂ）は、システムセキュリティ情報定義ファイル１３２の内容を例示する図であり、（ｃ）は、レコードセキュリティ情報設定ファイル１３３の内容を例示する図であり、（ｄ）は、メニューセキュリティ情報設定ファイル１３４の内容を例示する図であり、（ｅ）は、社員属人情報管理ファイル１３７の内容を例示する図である。

【図４】情報処理装置１における動作処理を示したフローチャートである。

【図５】情報処理装置１における社員情報更新処理を示したフローチャートである。

【図６】情報処理装置１における業務処理の概要を例示する図である。

【図７】（ａ）は、ユーザの属人情報に対応したセキュリティ制御を例示する表であり、（ｂ）は、ユーザの属人情報の更新に応じたセキュリティ制御を例示する図である。

【図８】本発明である情報処理システム１００の概略を示した概略図である。

【図９】端末２、データベースサーバ４の機能的構成を模式的に示したブロック図である。

【図１０】サーバ３の機能的構成を模式的に示したブロック図である。

【図１１】データベースサーバ４におけるデータベースの構成を模式的に示した図である。

【図１２】情報処理システム１００における動作処理を示したラダーチャートである。

【図１３】情報処理システム１００における社員情報更新処理を示したラダーチャートである。

【図１４】情報処理システム１００における業務処理の概略を例示する図である。

【図１５】ユーザの所属する会社の更新に対応したセキュリティ制御を例示する図である。

【符号の説明】

【００８８】

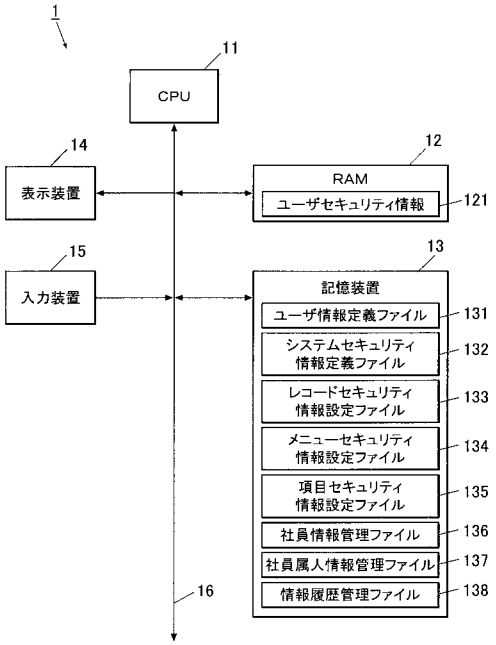
１　情報処理装置

１００　情報処理システム

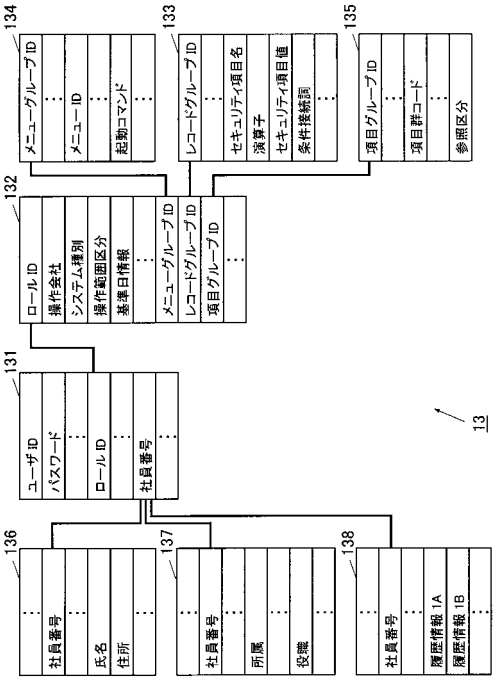
２、２ａ、２ｂ、２ｃ　端末

３　サーバ
４　データベースサーバ
Ｎ　通信ネットワーク
１１　ＣＰＵ（取得手段、制御手段）
１２　ＲＡＭ
１３　記憶装置（記憶手段）
１４　表示装置
１５　入力装置（編集手段）
１６　バス
２１　ＣＰＵ
２２　ＲＡＭ
２３　記憶装置
２４　表示装置
２５　入力装置
２６　通信装置
２７　バス
３１　ＣＰＵ（取得手段、制御手段）
３２　ＲＡＭ
３３　記憶装置
３４　表示装置
３５　入力装置
３７　バス
１２１　ユーザセキュリティ情報
１３１　ユーザ情報定義ファイル
１３２　システムセキュリティ情報定義ファイル（複数の権限情報）
１３３　レコードセキュリティ情報設定ファイル（レコードセキュリティ情報）
１３４　メニューセキュリティ情報設定ファイル（メニューセキュリティ情報）
１３５　項目セキュリティ情報設定ファイル（項目セキュリティ情報）
１３６　社員情報管理ファイル（属人情報）
１３７　社員属人情報管理ファイル（属人情報）
１３８　情報履歴管理ファイル（属人情報）
４３１　ユーザ情報定義ＤＢ
４３２　システムセキュリティ情報定義ＤＢ（複数の権限情報）
４３３　レコードセキュリティ情報設定ＤＢ（レコードセキュリティ情報）
４３４　メニューセキュリティ情報設定ＤＢ（メニューセキュリティ情報）
４３５　項目セキュリティ情報設定ＤＢ（項目セキュリティ情報）
４３６　社員情報管理ＤＢ（属人情報）
４３７　社員属人情報管理ＤＢ（属人情報）
４３８、４３８ａ、４３８ｂ　情報履歴管理ＤＢ（属人情報）
４３９　社員所属会社管理ＤＢ（属人情報）
４４０　ＶＩＥＷ社員情報

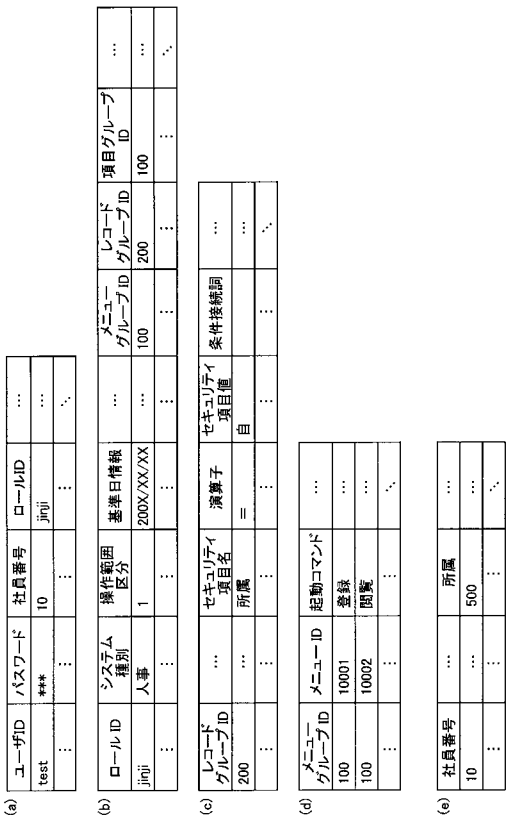
【図１】


1
CPU
11
表示装置
14
RAM
12
ユーザセキュリティ情報
121
入力装置
15
記憶装置
13
ユーザ情報定義ファイル
131
システムセキュリティ情報定義ファイル
132
レコードセキュリティ情報設定ファイル
133
メニューセキュリティ情報設定ファイル
134
項目セキュリティ情報設定ファイル
135
社員情報管理ファイル
136
社員属人情報管理ファイル
137
情報履歴管理ファイル
138
16

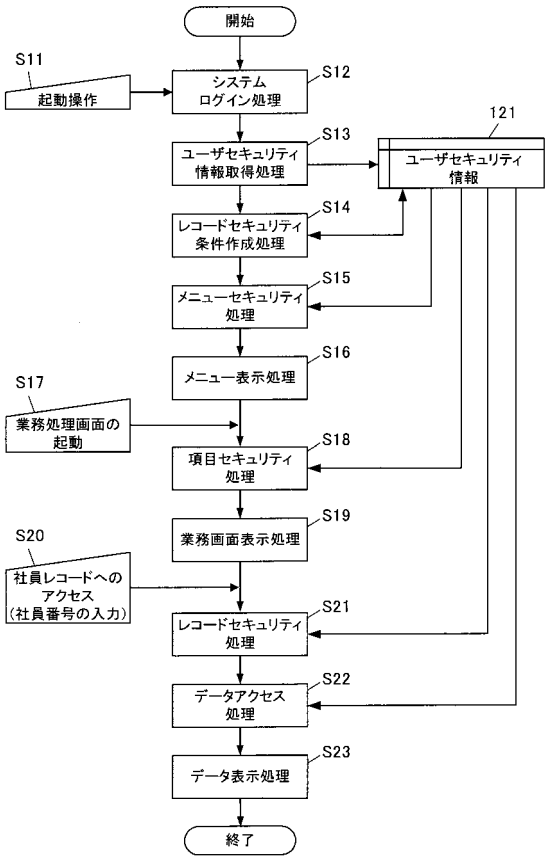
【図２】


134
メニューグループID
メニューID
起動コマンド
133
レコードグループID
セキュリティ項目名
演算子
セキュリティ項目値
条件接続詞
135
項目グループID
項目群コード
参照区分
132
ロールID
操作会社
システム種別
操作範囲区分
基準日情報
メニューグループID
レコードグループID
項目グループID
131
ユーザID
パスワード
ロールID
社員番号
13
136
社員番号
氏名
住所
137
社員番号
所属
役職
138
社員番号
履歴情報1A
履歴情報1B

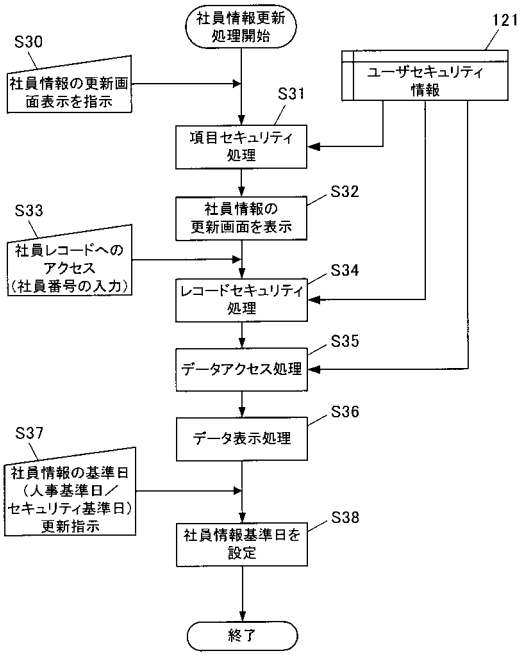
【図３】


(a)
ユーザID
パスワード
社員番号
ロールID
test
****
10
jinji
(b)
ロールID
システム種別
操作範囲区分
基準日情報
メニューグループID
レコードグループID
項目グループID
jinji
人事
1
200X/XX/XX
100
200
100
(c)
レコードグループID
セキュリティ項目名
演算子
セキュリティ項目値
条件接続詞
200
所属
=
自
(d)
メニューグループID
メニューID
起動コマンド
100
10001
登録
100
10002
閲覧
(e)
社員番号
所属
10
500

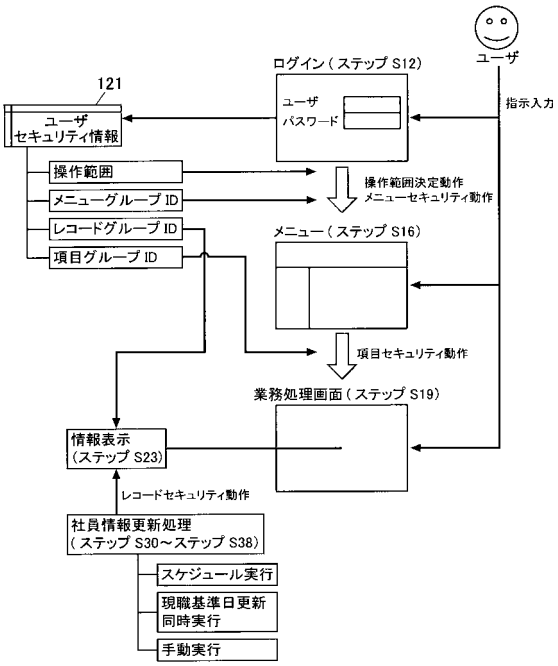
【図４】


開始
S11
起動操作
システム
ログイン処理
S12
121
ユーザセキュリティ
情報取得処理
S13
ユーザセキュリティ
情報
レコードセキュリティ
条件作成処理
S14
メニューセキュリティ
処理
S15
メニュー表示処理
S16
S17
業務処理画面の
起動
項目セキュリティ
処理
S18
業務画面表示処理
S19
S20
社員レコードへの
アクセス
(社員番号の入力)
レコードセキュリティ
処理
S21
データアクセス
処理
S22
データ表示処理
S23
終了

【図５】



【図６】

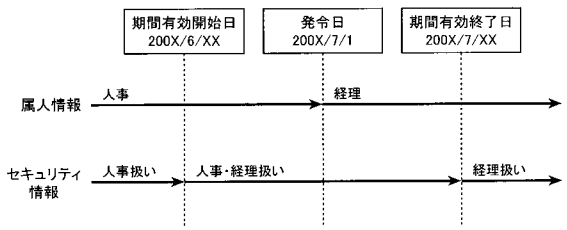


【図７】

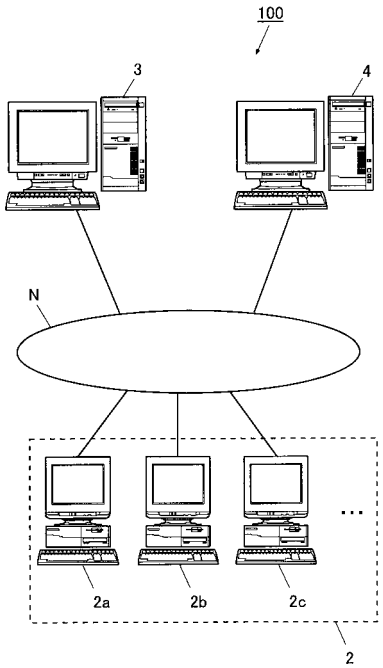
(a)

	社員登録	権限，人事情報設定	パスワード設定	社員給与閲覧	社員給与設定
人事担当者	○	○	×	○	×
経理担当者	×	×	×	○	○
システム管理者	○	×	○	×	×

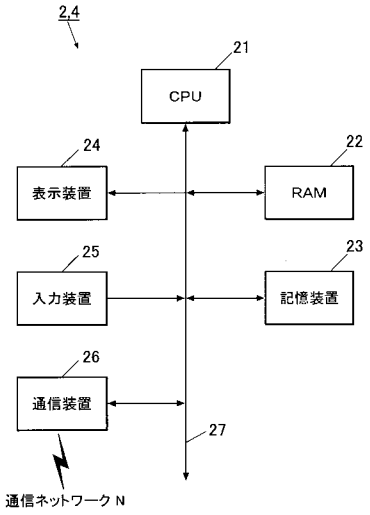
(b)



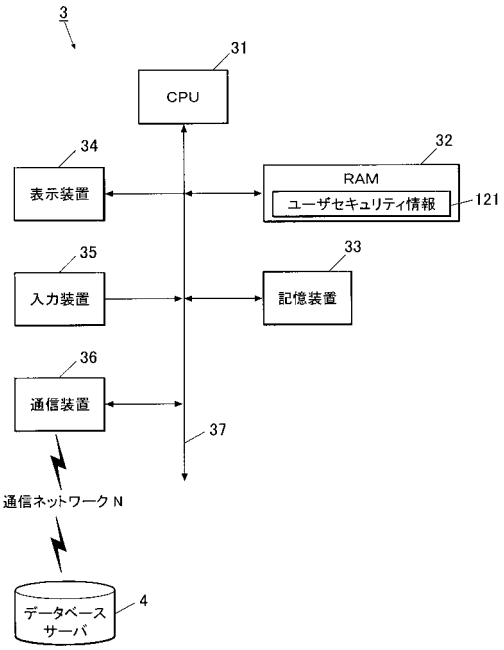
【図８】



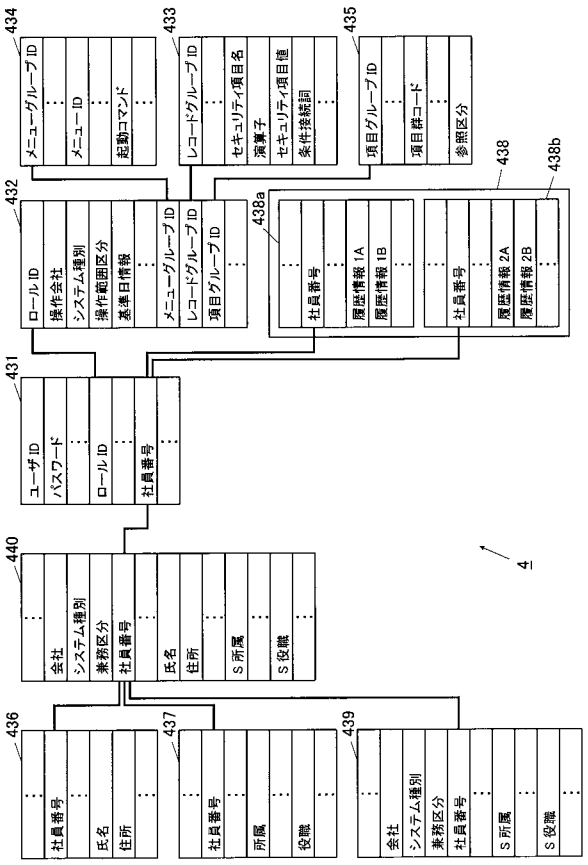
【図９】



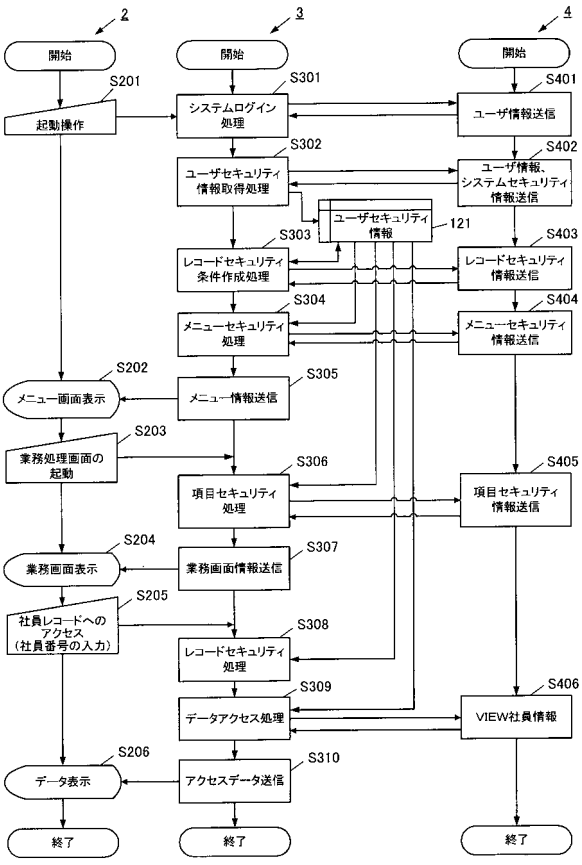
【図１０】



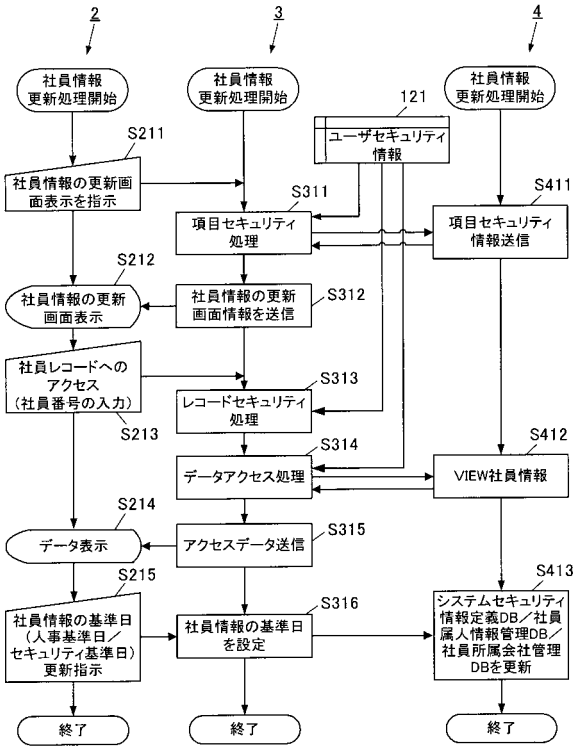
【図１１】



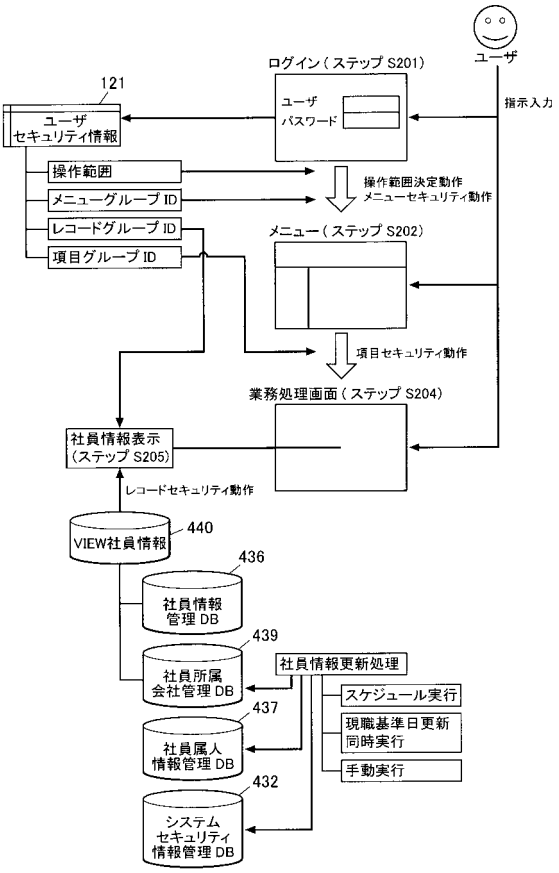
【図１２】



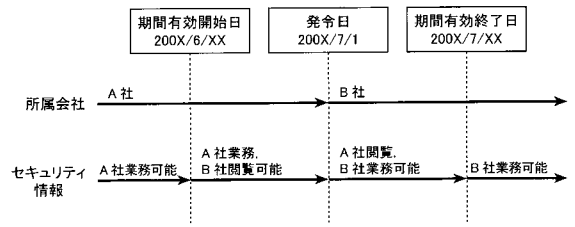
【図１３】


2
3
4
社員情報更新処理開始
社員情報更新処理開始
社員情報更新処理開始
121
ユーザセキュリティ情報
S211
社員情報の更新画面表示を指示
S311
項目セキュリティ処理
S411
項目セキュリティ情報送信
S212
社員情報の更新画面表示
社員情報の更新画面情報を送信
S312
社員レコードへのアクセス（社員番号の入力）
S313
レコードセキュリティ処理
S213
S314
S412
データアクセス処理
VIEW社員情報
S214
データ表示
アクセスデータ送信
S315
S215
S413
社員情報の基準日（人事基準日／セキュリティ基準日）更新指示
S316
社員情報の基準日を設定
システムセキュリティ情報定義DB／社員属人情報管理DB／社員所属会社管理DBを更新
終了
終了
終了

【図１４】


ユーザ
ログイン（ステップ S201）
121
ユーザセキュリティ情報
ユーザ
パスワード
指示入力
操作範囲
メニューグループ ID
レコードグループ ID
項目グループ ID
操作範囲決定動作
メニューセキュリティ動作
メニュー（ステップ S202）
項目セキュリティ動作
業務処理画面（ステップ S204）
社員情報表示（ステップ S205）
レコードセキュリティ動作
VIEW社員情報
440
436
社員情報管理 DB
439
社員所属会社管理 DB
社員情報更新処理
スケジュール実行
現職基準日更新同時実行
手動実行
437
社員属人情報管理 DB
432
システムセキュリティ情報管理 DB

【図１５】


期間有効開始日
200X/6/XX
発令日
200X/7/1
期間有効終了日
200X/7/XX
所属会社
A 社
B 社
セキュリティ情報
A 社業務可能
A 社業務，B 社閲覧可能
A 社閲覧，B 社業務可能
B 社業務可能

フロントページの続き

(56)参考文献 特開２００３－０６７３３６（ＪＰ，Ａ）
特開２００５－１０７９８４（ＪＰ，Ａ）
特開２００３－００６３９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｆ　２１／２２
Ｇ０９Ｃ　１／００