(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-214219
(P2013-214219A)
(43)公開日　平成25年10月17日(2013.10.17)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/62	(2013.01)	G06F 21/24	163G	
		G06F 21/24	163C	
		G06F 21/24	165E	

審査請求 未請求　請求項の数 7　ＯＬ　（全 12 頁）

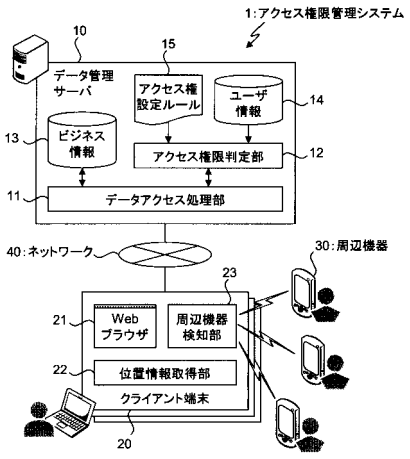
(21)出願番号　特願2012-84509(P2012-84509)
(22)出願日　平成24年4月3日(2012.4.3)

(71)出願人　000155469
株式会社野村総合研究所
東京都千代田区丸の内一丁目６番５号
(74)代理人　100080001
弁理士　筒井　大和
(74)代理人　100093023
弁理士　小塚　善高
(74)代理人　100117008
弁理士　筒井　章子
(72)発明者　近藤　俊明
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

(54)【発明の名称】アクセス権限管理システム

(57)【要約】
【課題】ユーザが存在する位置や、その周辺の環境や状況、意味内容などの情報に対応する周辺コンテキストの内容に応じて、当該ユーザに対する各データへのアクセス権限を動的に設定・変更することができるアクセス権限管理システムを提供する。
【解決手段】ビジネス情報１３を保管するデータ管理サーバ１０と、データ管理サーバ１０とネットワーク４０を介して接続可能な１つ以上のクライアント端末２０とからなるアクセス権限管理システム１であって、データ管理サーバ１０は、クライアント端末２０を介して第１のユーザからビジネス情報１３内のデータに対するアクセス要求を受けた場合に、クライアント端末２０の存在場所についての周辺コンテキストの情報を取得し、これに基づいて前記アクセス要求に係るビジネス情報１３内のデータへのアクセス権限を判定するアクセス権限判定部１２を有する。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
データを保管するデータ管理サーバと、前記データ管理サーバとネットワークを介して接続可能な１つ以上のクライアント端末とからなるアクセス権限管理システムであって、
前記データ管理サーバは、前記クライアント端末を介して第１のユーザから前記データに対するアクセス要求を受けた場合に、前記クライアント端末の存在場所についての周辺コンテキストの情報を取得し、これに基づいて前記アクセス要求に係る前記データへのアクセス権限を判定するアクセス権限判定部を有することを特徴とするアクセス権限管理システム。
【請求項２】
請求項１に記載のアクセス権限管理システムにおいて、
前記クライアント端末は、相互に近距離無線通信を行うことによって通信可能範囲に存在する周辺機器を検知し、検知した前記周辺機器の識別情報を取得する周辺機器検知部を有して、前記データ管理サーバに対して送信する前記アクセス要求に、前記周辺機器検知部によって取得した前記周辺機器の識別情報からなる周辺機器情報を付加し、
前記データ管理サーバの前記アクセス権限判定部は、前記クライアント端末から受信した前記アクセス要求に付加された前記周辺機器情報と、前記データ管理サーバが保持する、各ユーザが保有する前記周辺機器の識別情報に係る情報とに基づいて、前記周辺コンテキストとして、前記クライアント端末の前記通信可能範囲に、前記アクセス要求に係る前記データへのアクセスについての承認権限を有さないが、前記第１のユーザより上位の役割を有する所定の数以上の第２のユーザがそれぞれ保有する前記周辺機器が存在すると判断した場合に、前記アクセス要求に対して対応する前記データへのアクセスを許可する、もしくはアクセス権限を強化することを特徴とするアクセス権限管理システム。
【請求項３】
請求項２に記載のアクセス権限管理システムにおいて、
前記データ管理サーバは、前記アクセス権限判定部により、前記アクセス要求に対して対応する前記データへのアクセスを許可し、もしくはアクセス権限を強化した場合に、その旨を、前記アクセス要求に係る前記データへのアクセスについての承認権限を有する第２のユーザに対して通知することを特徴とするアクセス権限管理システム。
【請求項４】
請求項２に記載のアクセス権限管理システムにおいて、
前記データ管理サーバは、前記アクセス権限判定部により、前記アクセス要求に対して対応する前記データへのアクセスを許可し、もしくはアクセス権限を強化した場合に、前記アクセス要求に係る処理履歴を、通常時より長期間保持する、および／または通常時より詳細な内容を記録することを特徴とするアクセス権限管理システム。
【請求項５】
請求項１に記載のアクセス権限管理システムにおいて、
前記クライアント端末は、相互に近距離無線通信を行うことによって通信可能範囲に存在する周辺機器を検知し、検知した前記周辺機器の識別情報を取得する周辺機器検知部を有して、前記データ管理サーバに対して送信する前記アクセス要求に、前記周辺機器検知部によって取得した前記周辺機器の識別情報からなる周辺機器情報を付加し、
前記データ管理サーバの前記アクセス権限判定部は、前記クライアント端末から受信した前記アクセス要求に付加された前記周辺機器情報と、前記データ管理サーバが保持する、各ユーザが保有する前記周辺機器の識別情報に係る情報とに基づいて、前記周辺コンテキストとして、前記クライアント端末の前記通信可能範囲に、前記アクセス要求に係る前記データへのアクセスについての承認権限を有する第３のユーザが保有する前記周辺機器が存在すると判断した場合に、前記アクセス要求に対して対応する前記データへのアクセスを許可する、もしくはアクセス権限を強化することを特徴とするアクセス権限管理システム。
【請求項６】

請求項１に記載のアクセス権限管理システムにおいて、
前記クライアント端末は、相互に近距離無線通信を行うことによって通信可能範囲に存在する周辺機器を検知し、検知した前記周辺機器の識別情報を取得する周辺機器検知部を有して、前記データ管理サーバに対して送信する前記アクセス要求に、前記周辺機器検知部によって取得した前記周辺機器の識別情報からなる周辺機器情報を付加し、
前記データ管理サーバの前記アクセス権限判定部は、前記クライアント端末から受信した前記アクセス要求に付加された前記周辺機器情報と、前記データ管理サーバが保持する、各ユーザが保有する前記周辺機器の識別情報に係る情報とに基づいて、前記周辺コンテキストとして、前記クライアント端末の前記通信可能範囲に、前記第１のユーザと同程度の役割を有する所定の数以上の第４のユーザがそれぞれ保有する前記周辺機器が存在すると判断した場合に、前記アクセス要求に対して対応する前記データの参照可能数の制限を緩和することを特徴とするアクセス権限管理システム。
【請求項７】
請求項１～６のいずれか１項に記載のアクセス権限管理システムにおいて、
前記データ管理サーバは、前記クライアント端末を介して登録された前記第１のユーザの行動予定の情報を保持し、
前記クライアント端末は、自身の位置に関する情報である位置情報を取得する位置情報取得部を有して、前記データ管理サーバに対して送信する前記アクセス要求に、前記位置情報取得部によって取得した前記位置情報を付加し、
前記データ管理サーバの前記アクセス権限判定部は、前記クライアント端末から受信した前記アクセス要求に付加された前記位置情報と、当該処理時の時刻情報、および、前記データ管理サーバが保持する前記第１のユーザの前記行動予定の情報とに基づいて、前記周辺コンテキストとして、前記第１のユーザが、前記行動予定に係る時間帯に前記行動予定に係る場所に存在すると判断した場合に、前記アクセス要求に対して前記行動予定に対応する前記データへのアクセスを許可する、もしくはアクセス権限を強化することを特徴とするアクセス権限管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データに対するアクセス権限を管理する技術に関し、特に、アクセス権限を動的に変更することを可能とするアクセス権限管理システムに適用して有効な技術に関するものである。
【背景技術】
【０００２】
一般的に、複数のユーザからアクセスされる可能性があるデータについては、アクセス権限が設定され、適切なユーザに適切な態様（例えば、読み取り、変更、実行など）でのアクセスのみ許可するようデータへのアクセスが制御される。特に、例えば、企業におけるＣＲＭ（Customer Relationship Management）システムなどでは、複数の顧客に関するビジネス情報に係るデータを大量に保持して一元的に管理し、複数の部署や社員などが業務上の必要に応じてこれらのデータにアクセスする形態がとられるため、各社員等が許可された範囲（顧客やデータの種別等）のデータを許可された態様でのみ利用可能となるよう、各データに対するアクセス権限を管理することは重要となる。
【０００３】
従来は、このようなデータのアクセス権限については、通常、データ毎にアクセス権限を個別に設定しており、この場合、アクセス権限の設定が必要となる数は、単純にはデータ（もしくはデータ種別）とユーザ（もしくはユーザグループ等）の数の乗算となって非常に多数となることから、管理が煩雑となる。特に、ユーザの異動や業務上の役割の変更などに伴ってアクセス権限の見直しや変更を行うことは、対象ユーザの数が多くなると管理者等にとって非常に大きな負荷となる。
【０００４】

このような課題に対し、アクセス権限を自動的に設定したり変更したりする技術が提案されている。例えば、特開２００６－９２１７０号公報（特許文献１）には、ユーザの位置およびユーザがアクセス先としたリソースを検出する階層型位置検出装置と、階層型位置検出装置が検出したユーザの位置およびアクセス先のリソースに関する情報を蓄積する位置検出・ファイルアクセスＤＢサーバと、ユーザの位置に応じて設定されたリソースへの権限を管理すると共に、リソースへアクセスしたユーザの位置とユーザの位置に応じて設定されたリソースへの権限とに基づいて、ユーザからの当該リソースへの行為を認証するユーザ位置依存ファイル権限認証用サーバとを有することで、セキュリティを向上し、ファイルやデータの漏洩を防止することができるリソースアクセス管理システムが記載されている。

【０００５】

また、特開２００９－２１１６２７号公報（特許文献２）には、時間と前記時間におけるユーザの属性情報を記憶する属性情報記憶手段と、コンテンツにアクセスできるアクセス制御を行うための、コンテンツに対応付けられた時間とその時間におけるコンテンツの属性情報と、属性情報記憶手段に記憶された時間とユーザの属性情報とを比較した結果に基づいて、コンテンツにアクセスできるユーザのアクセス権の設定を動的に変更するアクセス権制御手段とを備えることで、時間とその時間におけるユーザの状況に応じて、ユーザに負担をかけることなく、ユーザのコンテンツへのアクセス制限を動的に設定変更することができるコンテンツアクセス制御システムが記載されている。

【０００６】

また、特開２００９－２９４８１７号公報（特許文献３）には、アクセス権限の付与されているファイルが記録されている記憶装置とは別の別記録媒体であって相手装置（受信側装置）が利用可能な別記録媒体（ファイルサーバ、リムーバブル媒体など）にファイルを記録する記録手段と、前記記録手段によって上記ファイルを上記別記録媒体に記録する際、上記別記録媒体に記録したファイルに付与されているアクセス権限をファイルの記録先に応じて変更するアクセス権限再設定手段と、別記録媒体に記録されたファイルに対するアクセスを、上記変更されたアクセス権限に従って制御する受信側装置とを有し、ファイルに付与されているアクセス権限を、ファイルの送信先、アップロード先、コピー先といったファイルの記録先に応じて自動的に変更するアクセス権限管理装置が記載されている。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２００６－９２１７０号公報

【特許文献２】特開２００９－２１１６２７号公報

【特許文献３】特開２００９－２９４８１７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上記の特許文献１～３に記載されたような技術を利用することで、例えば、ユーザの位置や時間、データの記録先などに応じてアクセス権限をある程度自動で設定・変更することが可能となる。

【０００９】

一方で、近年、いわゆるスマートフォンやタブレット型端末などの高性能の携帯型端末が広く普及してきており、ビジネスにおいても活用される場面が増えてきている。企業の社員等のユーザは、これらの端末を社内に限らず移動中や外出先なども含めて常に携帯し、通信機能を利用してリモートのロケーションから社内のビジネス情報などのデータにアクセスすることが可能である。すなわち、ユーザがデータにアクセスする際の場所は様々であり、これに伴い、周辺の環境（周辺に存在する人や物等）も様々である。従って、自身が存在する位置や、その周辺の環境や状況、その意味内容（以下では、これらを総称し

て「周辺コンテキスト」と記載する場合がある）は様々に異なる。
【００１０】
そこで、自身が存在する位置における周辺コンテキストに対応する情報を取得して、これに応じてアクセス権限を動的に変更することで、より柔軟かつ精緻なアクセス権限の動的設定や変更が可能になると考えられる。近年普及している携帯型端末では、通常、近距離無線通信機能を有しており、周辺の携帯型端末を含む情報処理装置と無線通信することができるため、周辺コンテキストの情報の一つとして、周辺に存在する機器の情報を把握することは容易に可能となっている。また、これらの通信機能や、ＧＰＳ（Global Positioning System）機能などにより、携帯型端末の位置情報を把握することも容易となっている。
【００１１】
一方で、上記の特許文献１～３に記載されたような従来技術では、ユーザの位置や時間といったユーザ自身のコンテキストに応じたアクセス権限の動的設定は可能であるが、上記のような周辺コンテキストを利用することまでは考慮されていない。
【００１２】
そこで本発明の目的は、ユーザが存在する位置や、その周辺の環境や状況、意味内容などの情報に対応する周辺コンテキストの内容に応じて、当該ユーザに対する各データへのアクセス権限を動的に設定・変更することができるアクセス権限管理システムを提供することにある。本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。
【課題を解決するための手段】
【００１３】
本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。
【００１４】
本発明の代表的な実施の形態によるアクセス権限管理システムは、データを保管するデータ管理サーバと、前記データ管理サーバとネットワークを介して接続可能な１つ以上のクライアント端末とからなるアクセス権限管理システムであって、前記データ管理サーバは、前記クライアント端末を介して第１のユーザから前記データに対するアクセス要求を受けた場合に、前記クライアント端末の存在場所についての周辺コンテキストの情報を取得し、これに基づいて前記アクセス要求に係る前記データへのアクセス権限を判定するアクセス権限判定部を有することを特徴とするものである。
【発明の効果】
【００１５】
本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば以下のとおりである。
【００１６】
すなわち、本発明の代表的な実施の形態によれば、ユーザが存在する位置や、その周辺の環境や状況、意味内容などの情報に対応する周辺コンテキストの内容に応じて、当該ユーザに対する各データへのアクセス権限を動的に設定・変更することが可能となり、これにより、アクセス権限の設定がより柔軟に行えるようになるとともに、アクセス権限の管理負荷を低減させることが可能となる。
【図面の簡単な説明】
【００１７】
【図１】本発明の一実施の形態であるアクセス権限管理システムの構成例について概要を示した図である。
【図２】本発明の一実施の形態における周辺コンテキストを考慮しないアクセス権限の判定の例について概要を示した図である。
【図３】本発明の一実施の形態における周辺コンテキストを考慮したアクセス権限の判定の例について概要を示した図である。

【図４】本発明の一実施の形態における周辺コンテキストを考慮したアクセス権限の判定の他の例について概要を示した図である。
【図５】本発明の一実施の形態における周辺コンテキストを考慮しないアクセス権限の判定の他の例について概要を示した図である。
【図６】本発明の一実施の形態における周辺コンテキストを考慮したアクセス権限の判定の他の例について概要を示した図である。
【図７】本発明の一実施の形態における周辺コンテキストを考慮したアクセス権限の判定の他の例について概要を示した図である。
【発明を実施するための形態】
【００１８】
以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一部には原則として同一の符号を付し、その繰り返しの説明は省略する。
【００１９】
本発明の一実施の形態であるアクセス権限管理システムは、例えば、企業の社内のＣＲＭシステム等においてサーバ上に保管されたビジネス情報などのデータに対して、社員等のユーザがクライアント端末を介してアクセスした場合に、クライアント端末によって取得されたその位置や、周辺の環境や状況等の情報、その意味内容（例えば、「近くに部長がいる」や「○○人集まって作業中」、「顧客の場所に訪問中」や「○○へ出張中」等）などの情報に対応する周辺コンテキストの情報を取得し、この内容に応じて当該ユーザに対する各データへのアクセス権限を動的に設定・変更するというシステムである。
【００２０】
＜システム構成＞
図１は、本発明の一実施の形態であるアクセス権限管理システムの構成例について概要を示した図である。アクセス権限管理システム１は、例えば、ＣＲＭシステム等の社内システムにおいてビジネス情報などのデータを保管するサーバシステムであるデータ管理サーバ１０と、インターネットやイントラネット等のネットワーク４０を介してデータ管理サーバ１０に接続することが可能な１つ以上のクライアント端末２０とを有する構成をとる。なお、本実施の形態では、ＣＲＭシステム等の社内システムにおいてビジネス情報などのデータに対してアクセス権限を設定し管理するシステムを対象として説明するが、これに限るものではなく、データを保管してこれに対するアクセス権限を設定して管理するシステムであれば適用することが可能である。
【００２１】
データ管理サーバ１０は、例えば、ＯＳ（Operating System）等のミドルウェアもしくはアプリケーションプログラム等のソフトウェアにより実装されるデータアクセス処理部１１、およびアクセス権限判定部１２などの各部を有する。また、データベースやファイル等として保管されているビジネス情報１３と、ビジネス情報１３内の各データにアクセスし得るユーザ（データ管理サーバ１０を保有する企業の社員等）の情報を保持するデータベースであるユーザ情報１４を有する。また、ファイルやデータベース等として実装され、ビジネス情報１３内のデータに対するアクセス権限を動的に設定・変更するためのルールを定義・設定したアクセス権設定ルール１５を有する。
【００２２】
データアクセス処理部１１は、クライアント端末２０を介したユーザからのビジネス情報１３へのアクセス（読み込み、書き込み、実行など）の要求に対して、後述するアクセス権限判定部１２により、当該ユーザに対するビジネス情報１３内の各データへのアクセス権限を判定して動的に設定・変更し、アクセスが許可される場合には対象データをクライアント端末２０に送信する一方、アクセスが許可されない場合はその旨をクライアント端末２０に応答する。各種のクライアント端末２０からのアクセス要求を受け付けられるようにするため、例えば、図示しないＷｅｂサーバプログラム上で稼働するサービスとして実装してもよい。

【００２３】
アクセス権限判定部１２は、データアクセス処理部１１を介して受け取った、ユーザからのビジネス情報１３へのアクセス要求に対して、アクセス要求に付されているクライアント端末２０の位置情報、および後述する周辺機器情報と、ユーザ情報１４に保持されている当該ユーザの属性や行動予定の情報に基づいて、当該ユーザ（クライアント端末２０の所在場所）についての周辺コンテキストの情報を得るとともに、これにアクセス権設定ルール１５を適用してアクセス権限を判定し、設定もしくは変更する。
【００２４】
ユーザ情報１４には、例えば、ユーザ毎の所属部署やグループの情報、役職や役割、担当顧客の情報など、周辺コンテキストの情報とは関係なく当該情報に基づいてアクセス権限を判定できる情報が含まれる。また、各ユーザ（社員）が保有する後述する周辺機器３０の識別情報についても保持する。また、これらに加えて、例えば、各ユーザの外出予定や出張申請の内容など、ユーザの存在場所に関わる行動予定の情報を保持する。これにより、周辺コンテキストの情報として、ユーザの存在場所についての意味内容を判定することができる。
【００２５】
アクセス権設定ルール１５には、形式は特に限定されないが、例えば、ビジネス情報１３内のデータ（もしくはデータ種別）毎、もしくはユーザ情報１４に登録されたユーザ（もしくはグループ等）毎に、データへのアクセス権限を設定するためのルールを管理者等が予め設定しておく。ルールとしては、例えば、デフォルトのアクセス権限に加えて、アクセス権限をデフォルト値から変更する場合の条件を定義する。条件としては、例えば、上述したような、ユーザ毎の所属部署やグループの情報、役職や役割、担当顧客の情報などに基づいてデフォルトのアクセス権限を決定するものや、後述するような周辺コンテキストの内容に基づいてアクセス権限をデフォルト値から動的に変更するものなどを適宜設定することができる。
【００２６】
クライアント端末２０は、ＰＣ（Personal Computer）や、タブレット型端末、スマートフォン、携帯電話などの情報処理端末であるが、可搬な携帯型端末であるのが望ましい。クライアント端末２０は、データ管理サーバ１０のデータアクセス処理部１１に対してデータへのアクセス要求を行うためのインタフェースを提供するソフトウェアとして、例えば、一般的なＷｅｂブラウザ２１を有している。また、デバイス等として、自身の位置に関する情報を取得する位置情報取得部２２と、周辺に存在する周辺機器３０に関する情報を取得する周辺機器検知部２３とを有する。
【００２７】
位置情報取得部２２は、特に限定しないが、例えば、ＧＰＳセンサによる緯度・経度情報を取得する機能や、Ｆｅｌｉｃａ（登録商標）等の近距離無線通信機能によりリーダとの関係での位置を把握する機能（例えば、社員証による入館システムなど）、無線ＬＡＮ機能において検知できるアクセスポイントのＳＳＩＤ（Service Set IDentifier）の情報を取得することで、アクセスポイントとの関係での概略の位置を把握する機能、クライアント端末２０のＩＰアドレスの情報から概略の位置を把握する機能などにより、周辺コンテキスト（もしくはこれを得るための情報の一つ）としての位置情報を取得する。様々な場所や状況において位置情報を把握可能とするため、これらのうち複数の機能・デバイスを状況に応じて使い分けたり、組み合わせたりするものであってもよい（例えば、ＧＰＳの電波状況が悪い地下等では無線ＬＡＮのＳＳＩＤを利用するなど）。
【００２８】
周辺機器検知部２３は、周辺に存在する周辺機器３０との間で相互に、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）やＲＦＩＤ（Radio Frequency IDentification）などの近距離無線通信を行うことで、周辺（すなわち電波の届く通信可能範囲）に周辺機器３０が存在することの検知と、存在する各周辺機器３０の識別を行うことで、周辺コンテキストとしての周辺機器情報（周辺に存在する周辺機器３０の識別情報）を取得する。

【００２９】
周辺機器３０は、例えば、対象の企業等に属する各社員がそれぞれ保有するＰＣやタブレット型端末、スマートフォン等の携帯型端末であり、クライアント端末２０の周辺機器検知部２３との間で近距離無線通信を行うことができる通信手段を備えたものである。従って、クライアント端末２０は、近距離無線通信により周辺機器３０の存在を検知することで、周辺に存在する他の社員の情報を把握することができる。なお、各社員は、保有する周辺機器３０を自身にとってのクライアント端末２０として用いることで、存在場所の把握のためだけに専用の機器を保有するという負荷を回避することができる。
【００３０】
なお、クライアント端末２０と周辺機器３０との間の近距離無線通信の通信プロトコル等については特に限定されず、例えば、各機器（クライアント端末２０および周辺機器３０）が定期的に自身の機器の識別情報等を発信して存在を通知する一方で、周辺の他の機器からの通知を待ち受けるなど種々の手法を適宜採用することができる。
【００３１】
クライアント端末２０を使用するユーザが、データ管理サーバ１０上のビジネス情報１３内のデータにアクセスするため、Ｗｅｂブラウザ２１を介して操作を行うと、例えば、Ｗｅｂブラウザ２１上で稼働するクライアントプログラムが、位置情報取得部２２および周辺機器検知部２３からクライアント端末２０の位置情報および周辺機器情報をそれぞれ取得し、データへのアクセス要求に付加して、データ管理サーバ１０のデータアクセス処理部１１に送信する。
【００３２】
アクセス要求を受信したデータアクセス処理部１１では、アクセス権限判定部１２により、アクセス権設定ルール１５に設定された対象のデータもしくはユーザについてのルールに従って、例えば、ユーザ毎の所属部署やグループの情報、役職や役割、担当顧客の情報などに基づいてアクセス権限を判定する。また、アクセス要求に付加された周辺機器３０の識別情報に基づいてユーザ情報１４から取得した、周辺に存在する他の社員の情報や、ユーザ情報１４に登録されたユーザの行動予定の情報等から把握できる周辺コンテキストの情報を取得し、その内容に基づいて、アクセス権設定ルール１５に設定されたルールに従って、後述するようにアクセス権限を判定する。これらの結果、アクセスが許可される場合には、ビジネス情報１３内の対象データを取得してクライアント端末２０に応答する。
【００３３】
＜アクセス権限の判断＞
以下では、データ管理サーバ１０のアクセス権限判定部１２におけるアクセス権限の判定処理の内容の例について説明する。図２は、周辺コンテキストを考慮しないアクセス権限の判定の例について概要を示した図である。当該アクセス権限は、例えば、ユーザ毎の所属部署やグループの情報、役職や役割、担当顧客の情報などに基づいて決定されるデフォルトのアクセス権限である。図２の例では、クライアント端末２０からのアクセス要求に対して、ビジネス情報１３内の対象のデータへのアクセスを拒否した場合を示している。ここでは例えば、アクセス権設定ルール１５において、対象のユーザ自身、もしくは所属する部署や役割、担当顧客などの属性情報が、ビジネス情報１３内の対象のデータへのアクセスが許可される条件に合致していない、もしくはアクセスが拒否される条件に合致していることから、アクセス権限がないと判定している。
【００３４】
本実施の形態では、上記のような場合であっても、ユーザについての周辺コンテキストを考慮して、アクセス権限を強化・格上げする（もしくは格下げする）ことを可能とする。図３、図４は、周辺コンテキストを考慮したアクセス権限の判定の例について概要を示した図である。図３に示すように、データにアクセスしようとしている社員等のユーザ（クライアント端末２０）の周辺に、当該データへのアクセスについての承認権限を有する上司等の社員（例えば部長等）が存在することを当該上司等が保有する周辺機器３０との

間の近距離無線通信により検知した場合には、セキュリティ上のリスクは減少すると考えて、アクセス権限を格上げし、同一のデータでもアクセス可能とする。

【００３５】

なお、このとき、上司等がユーザ（クライアント端末２０）の周辺を通り過ぎただけというような場合を考慮して、例えば、クライアント端末２０の周辺機器検知部２３において、対象の周辺機器３０がクライアント端末２０の周辺に所定の時間（例えば５分間）以上連続して存在したことを検知した場合にのみ、対象の周辺機器３０（上司等の他の社員）がクライアント端末２０の周辺に存在したものと判断するようにしてもよい。

【００３６】

一方で、図３に示すような方式をとった場合であっても、例えば、部長等が外出や会議等により不在で、ユーザの周辺に存在しないという場合には、アクセス権限を格上げすることはできない。このように、部長等の承認権限を有する上司が周辺に存在しない場合であっても、本実施の形態では、図４に示すように、例えば、課長やリーダー等の所定の役職・役割以上の社員が周辺に一定人数以上（図４の例では３人）存在していれば、部長等の承認権限を有する上司が周辺に存在する場合と同様に、アクセス権限を格上げすることを可能とする。

【００３７】

なお、この場合は、図３に示すような、部長等の本来の承認権限を有する他の社員が周辺に存在するという場合とは異なるため、アクセス権限の内容に差を設ける（例えば、参照のみ可能とするなど）ようにしてもよい。また、アクセス権限の変更を行った旨の電子メール等を部長等に対して自動的に送付して通知したり、データ管理サーバ１０において当該アクセスに係るログデータを通常よりも長期間保持したり、より詳細な内容を保持したりすることで、監査等のための証跡を適切に保持できるようにしてもよい。

【００３８】

また、本実施の形態では、周辺機器３０は、他の社員等が保有する携帯型端末としているが、これに限らず、所定の場所に固定的に設置されている機器（例えば、サーバ機器やプリンター、ネットワーク機器等）であってもよい。この場合は、例えば、図３に示すような承認権限を有する上司等の社員が周辺に存在するという場合の代替として、ユーザが所定の場所（例えば、オフィスの所定のエリアなど）の周辺に存在していることを、対象のデータへのアクセスの条件とすることになる。

【００３９】

図５は、周辺コンテキストを考慮しないアクセス権限の判定の他の例について概要を示した図である。図２の例と同様に、当該アクセス権限は、例えば、ユーザ毎の所属部署やグループの情報、役職や役割、担当顧客の情報などに基づいて決定されるデフォルトのアクセス権限である。図５の例では、図２の例と異なり、ビジネス情報１３内の対象のデータへのアクセスは許可しているが、アクセス権限の制約として、参照可能なデータの数を１００件に制限していることを示している。

【００４０】

本実施の形態では、上記のような場合であっても、ユーザについての周辺コンテキストを考慮して、アクセス権限を格上げする（もしくは格下げする）ことを可能とする。図６は、周辺コンテキストを考慮したアクセス権限の判定の他の例について概要を示した図である。図６に示すように、データにアクセスしようとしている社員等のユーザ（クライアント端末２０）の周辺に役職や役割、権限等が同程度の他の社員（ユーザ）が一定人数以上（図６の例では合計３人）存在していれば、例えば、提案書作成等の共通の作業のために集まっているものと判断して、参照可能なデータの数の制限を１０００件に緩和する（アクセス権限を強化する）ことを示している。この場合、図３、図４に示した例のように、役職や役割、権限等が上位の他の社員が一定人数以上周辺に存在する場合に参照可能なデータの数の制限を緩和するようにしてもよい。

【００４１】

図７は、周辺コンテキストを考慮したアクセス権限の判定の他の例について概要を示し

た図である。ここでは、ユーザが予めデータ管理サーバ１０のユーザ情報１４に登録しておいた行動予定の情報に基づいて、ユーザがいる位置やその周辺についての意味内容（周辺コンテキスト）を判定し、これに基づいてアクセス権限を格上げ（もしくは格下げ）することを可能とする。

【００４２】

図７の例では、ユーザがクライアント端末２０を介してデータ管理サーバ１０のユーザ情報１４に対して予め顧客への訪問予定（日時と訪問先の顧客）等の行動予定を登録しておく。出張申請などの情報であってもよい。その後、当該ユーザから、通常は外出先等の社外のロケーションからのアクセスは許可されないようなビジネス情報１３内の対象の顧客に関連するデータに対するアクセス要求がされると、当該ユーザが対象の顧客の所在地周辺にいると判断した場合にのみ、アクセス権限を格上げしてアクセスを許可するよう制御する。

【００４３】

このとき、当該ユーザが対象の顧客の所在地周辺に業務として存在していることを判断するため、クライアント端末２０からは、データへのアクセス要求に対して位置情報取得部２２により取得したクライアント端末２０の位置情報を付加する。この位置情報と、当該処理時の時刻情報とを、ユーザ情報１４に登録された当該ユーザについての行動予定の情報（行動場所と時間帯の情報）と突合することで、当該ユーザが顧客の所在地に業務として存在しているのか否かを判断することができる。このような判断を可能とするため、データ管理サーバ１０は、図示しない顧客情報データベース等に、顧客の所在地の情報（例えば、住所、緯度・経度、周辺の無線ＬＡＮアクセスポイントのＳＳＩＤなど）を保持していてもよい。

【００４４】

このように、ユーザが訪問予定の顧客の所在地周辺に業務として存在している場合にアクセス権限を格上げするのに加えて、顧客への訪問回数を考慮するようにしてもよい。例えば、図示しない行動履歴等を保持するデータベース等を参照して、当該顧客への訪問回数を判定し、初回訪問の場合には、一般的な情報からなるデータへのアクセスのみ許可し、２回目以降の訪問の場合には、例えば、訪問回数に応じてより重要なデータや開示が制限されているデータへのアクセスについても許可するよう制御してもよい。

【００４５】

また、例えば、東京や北海道などの地域毎の業務に関連するデータへのアクセスは、当該地域に属するユーザにのみ許可し、他の地域のユーザからのアクセスは許可しないよう制御しているところ、北海道にいるユーザが出張で東京地域の事業所に来るような場合は、当該ユーザの行動予定として予め東京地域への出張申請が提出・登録されていれば、当該出張期間、もしくは、当該ユーザが東京地域の事業所等に最後に入館してから一定期間（例えば１ヶ月など）が経過するまでは、東京地域のデータへのアクセスについても許可するようアクセス権限を格上げするような制御を行うことも可能である。

【００４６】

このように、ユーザ（クライアント端末２０）の位置情報および時刻情報と、予めシステムに登録等されているユーザの行動予定等の情報という、当該ユーザの存在位置における意味内容を把握することが可能な周辺コンテキストの情報を取得し、これに基づいてデータへのアクセス権限を設定・変更することが可能である。

【００４７】

以上に説明したように、本発明の一実施の形態であるアクセス権限管理システム１によれば、データ管理サーバ１０上に保管されたビジネス情報１３などのデータに対して、社員等のユーザがクライアント端末２０を介してアクセスした場合に、クライアント端末２０によって取得されたその位置や、周辺の環境や状況等の情報、その意味内容などの情報に対応する周辺コンテキストの情報を取得し、この内容に応じて当該ユーザに対する各データへのアクセス権限を動的に設定・変更することが可能となる。これにより、アクセス権限の設定がより柔軟に行えるようになるとともに、アクセス権限の管理負荷を低減させ

ることが可能となる。

【００４８】

以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【産業上の利用可能性】

【００４９】

本発明は、アクセス権限を動的に変更することを可能とするアクセス権限管理システムに利用可能である。

【符号の説明】

【００５０】

１…アクセス権限管理システム、

１０…データ管理サーバ、１１…データアクセス処理部、１２…アクセス権限判定部、１３…ビジネス情報、１４…ユーザ情報、１５…アクセス権設定ルール、

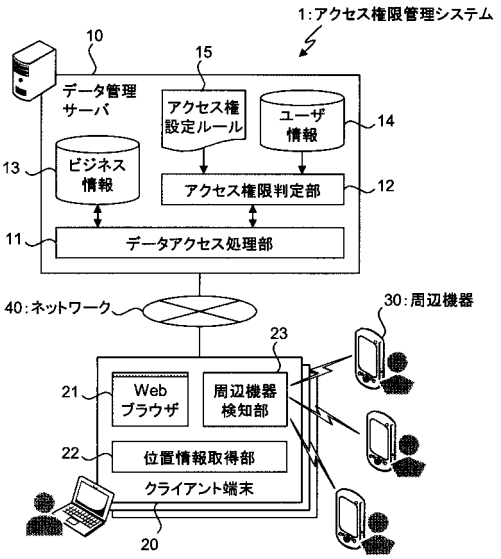
２０…クライアント端末、２１…Ｗｅｂブラウザ、２２…位置情報取得部、２３…周辺機器検知部、

３０…周辺機器、

４０…ネットワーク。

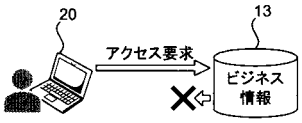
【図１】

図1



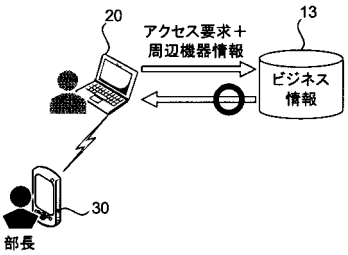
【図２】

図2



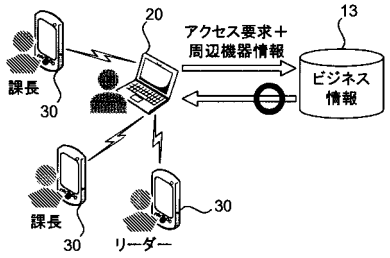
【図３】

図3



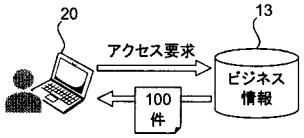
【図４】

図４



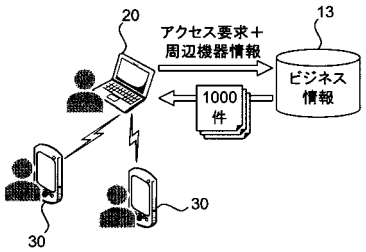
【図５】

図５



【図６】

図６



【図７】

図７