(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2013-109601
(P2013-109601A)
(43)公開日　平成25年6月6日(2013.6.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/34	(2013.01)	G06F	21/20	134	5J104
G06F 21/44	(2013.01)	G06F	21/20	144C	5K067
G06F 21/40	(2013.01)	G06F	21/20	140	5K127
H04L 9/32	(2006.01)	H04L	9/00	673E	5K201
H04M 11/00	(2006.01)	H04M	11/00	302	

審査請求 未請求　請求項の数 10　ＯＬ　（全 17 頁）　最終頁に続く

(21)出願番号　特願2011-254482 (P2011-254482)
(22)出願日　平成23年11月22日 (2011.11.22)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成２２年度　総務省「ユビキタス・プラットフォーム技術の研究開発（ユビキタス端末技術）に関する研究開発」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）

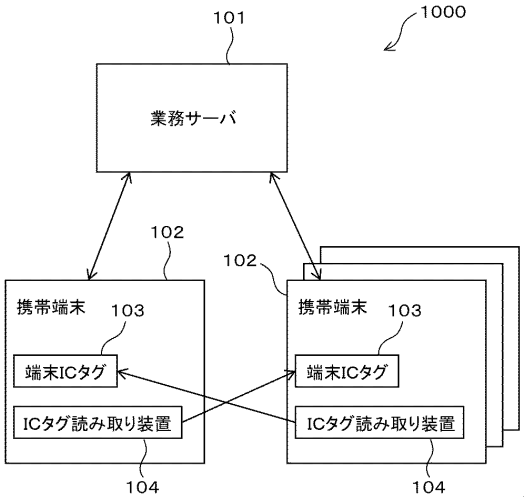
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　廣瀬　隆裕
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所セキュリティ・トレーサビリティ事業部内
(72)発明者　福島　真一郎
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所セキュリティ・トレーサビリティ事業部内

最終頁に続く

(54)【発明の名称】携帯端末認証システム、および携帯端末認証方法

(57)【要約】　（修正有）
【課題】携帯端末の利用者への利便性を損なうことなく、セキュリティリスクを回避することが可能な携帯端末認証システム、および携帯端末認証方法を提供する。
【解決手段】携帯端末からの要求に応じて利用者を認証する携帯端末認証システム１０００であって、利用者が認証のために利用する被認証用携帯端末１０２と、認証者が利用者を認証するための認証用携帯端末１０２と、を備え、業務サーバ１０１は、被認証用携帯端末１０２から通信パケットを受信するパケット受信部と、認証用携帯端末１０２からアクセス要求を受信する要求受信部と、パケット受信部が受信した通信パケットに被認証用タグＩＤと認証用タグＩＤとが含まれている場合に、要求受信部が受信したアクセス要求を許可する利用者認証部と、を備える。
【選択図】図１

図１



【特許請求の範囲】
【請求項１】
携帯端末からの要求に応じて利用者を認証する携帯端末認証システムであって、
前記利用者が認証のために利用する被認証用携帯端末は、
被認証用ＩＣ（Integrated Circuits）タグと、
前記利用者によるアクセス要求をサーバに送信する被認証制御部と、を備え、
認証者が前記利用者を認証するための認証用携帯端末は、
認証用ＩＣタグと、
前記被認証用ＩＣタグを読み取るための被認証用ＩＣタグ読み取り部と、
前記認証用ＩＣタグを識別するための認証用ＩＣタグ識別情報と前記被認証用ＩＣタグを識別するための被認証用ＩＣタグ識別情報とを含む通信パケットを、前記サーバに送信する認証制御部と、を備え、
前記サーバは、
前記被認証用携帯端末から前記通信パケットを受信するパケット受信部と、
前記認証用携帯端末から前記アクセス要求を受信する要求受信部と、
前記パケット受信部が受信した前記通信パケットに前記被認証用タグＩＤと前記認証用タグＩＤとが含まれている場合に、前記要求受信部が受信した前記アクセス要求を許可する利用者認証部と、
を備えることを特徴とする携帯端末認証システム。
【請求項２】
前記サーバは、前記被認証用ＩＣタグＩＤと前記利用者と、および前記認証用ＩＣタグＩＤと前記認証者とを対応付けた利用者情報テーブルと、前記利用者と前記認証者との両者の関係を示す関係区分とを対応付けた関係情報テーブルと、前記アクセス要求されたアプリケーションと前記関係区分とを対応付けて記憶するポリシーテーブルと、をあらかじめ記憶する記憶部をさらに備え、
前記利用者認証部は、前記パケット受信部が受信した前記通信パケット含まれる前記被認証用タグＩＤおよび前記認証用タグＩＤと、前記利用者情報テーブルと、前記関係情報テーブルとに基づいて、前記利用者と前記認証者とが前記関係区分に示された関係を満たしているか否かを判定し、前記利用者と前記認証者とが前記関係区分に示された関係を満たしていると判定した場合に、前記アクセス要求されたアプリケーションに対する前記アクセス要求を許可する、
ことを特徴とする請求項１に記載の携帯端末認証システム。
【請求項３】
前記ポリシーテーブルは、さらに前記関係区分に対応付けて前記アクセス要求を許可するための認証条件を記憶し、
前記利用者認証部は、さらに前記認証条件として前記被認証用ＩＣタグが前記認証用携帯端末の前記被認証用ＩＣタグ読取部によって読み取られている場合に、前記アクセス要求されたアプリケーションに対する前記アクセス要求を許可する、
ことを特徴とする請求項２に記載の携帯端末認証システム。
【請求項４】
前記通信パケットには、前記被認証用ＩＣタグが前記認証用携帯端末によって読み取った時刻を含み、
前記ポリシーテーブルは、さらに前記認証条件に対応付けて前記認証条件を満たすべき時間の間隔を示す有効時間を記憶し、
前記利用者認証部は、前記被認証用ＩＣタグが読み取られた時刻と、タイマにより計時される現在時刻とを比較し、両者の差が前記有効時間内である場合に、前記アクセス要求されたアプリケーションに対する前記アクセス要求を許可する、
ことを特徴とする請求項３に記載の携帯端末認証システム。
【請求項５】
前記認証用携帯端末の認証制御部は、前記通信パケットを繰り返し前記サーバに送信し

、
前記サーバの記憶部は、さらに前記利用者を識別するための認証対象者ＩＤと、前記認証者を識別するための読み取り者ＩＤと前記認証用携帯端末が前記被認証者ＩＣタグを読み取った時刻を示す読み取り時刻とを対応付けた読み取り者ＩＤ情報と、を対応付けて記憶する受信情報データベースをあらかじめ記憶し、
前記利用者認証部は、前記認証用携帯端末から前記通信パケットを受信する都度、前記通信パケットに含まれる前記被認証用タグＩＤおよび前記認証用タグＩＤと、前記利用者情報テーブルとに基づいて、前記受信情報データベースの中からアクセス要求された前記利用者に対応する前記読み取り者ＩＤ情報を特定し、特定した前記読み取り者ＩＤ情報に含まれる前記読み取り時刻を前記被認証用ＩＣタグが読み取られた時刻に更新する、
ことを特徴とする請求項４に記載の携帯端末認証システム。
【請求項６】
前記有効時間は、前記アクセス要求されたアプリケーションにより行われる業務の重要性に応じて間隔が定められている、
ことを特徴とする請求項４または５に記載の携帯端末認証システム。
【請求項７】
前記有効時間は、前記アクセス要求されたアプリケーションにより行われる業務の処理時間に応じて間隔が定められている、
ことを特徴とする請求項４～６のいずれか１項に記載の携帯端末認証システム。
【請求項８】
前記受信情報ＤＢの前記読み取り者ＩＤ情報には、さらに前記読み取り時刻に対応付けて前記利用者の認証回数を対応付けて記憶し、
前記利用者認証部は、前記アクセス要求されたアプリケーションに対する前記アクセス要求を許可した場合に前記認証回数を更新し、前記認証回数が多い順に前記受信情報ＤＢに記憶された前記読み取り者ＩＤ情報を並べ替える、
ことを特徴とする請求項５～７のいずれか１項に記載の携帯端末認証システム。
【請求項９】
前記受信情報ＤＢは、インデックスが付された前記認証対象者ＩＤを上位とし、前記読み取り者ＩＤ情報を下位とした階層構造により構成されている、
ことを特徴とする請求項５～８のいずれか１項に記載の携帯端末認証システム。
【請求項１０】
携帯端末からの要求に応じて利用者を認証する携帯端末認証システムにおいて行われる携帯端末認証方法であって、
前記利用者が認証のために利用され被認証用ＩＣタグを有した被認証用携帯端末が、前記利用者によるアクセス要求をサーバに送信する被認証ステップと、
認証者が前記利用者を認証し認証用ＩＣタグを有した認証用携帯端末が、前記被認証用ＩＣタグを読み取るための被認証用ＩＣタグ読み取りステップと、
前記認証用ＩＣタグを識別するための認証用ＩＣタグ識別情報と前記被認証用ＩＣタグを識別するための被認証用ＩＣタグ識別情報とを含む通信パケットを、前記サーバに送信する認証ステップと、
前記サーバが、前記被認証用携帯端末から前記通信パケットを受信するパケット受信ステップと、
前記認証用携帯端末から前記アクセス要求を受信する要求受信ステップと、
前記パケット受信ステップにおいて受信した前記通信パケットに前記被認証用タグＩＤと前記認証用タグＩＤとが含まれている場合に、前記要求受信部が受信した前記アクセス要求を許可する利用者認証ステップと、
を含むことを特徴とする携帯端末認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、携帯端末を認証する携帯端末認証システム、および携帯端末認証方法に関する。

【背景技術】

【０００２】

スマートフォン等の高機能な携帯端末が普及するに従って、重要な業務が携帯端末で実行されるようになっている。携帯端末は持ち歩かれるので、紛失や盗難のセキュリティリスクが避けられない。紛失に気付いた場合には、アカウントを無効化するなどの対抗策も取ることができるが、気付くまでの間に情報がリスクに曝され続ける。

【０００３】

最近の携帯端末はＧＰＳ（Global Positioning System）などの測位機能を備えているため、このようなリスクを回避するものとして、端末の位置によって、業務の利用を制限する方法が考案されている（例えば、特許文献１、２）。これらの技術では、業務サーバにアクセスしたときに端末の測位を行い、予め登録した事務所以外からアクセス接続できないようにするなどの方法により、上述したリスクを回避している。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１０－５５２９７号公報

【特許文献２】特開２００７－１０４４６４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

上述した技術では、端末が持ち去られた場合であっても、予め登録した事務所以外からアクセス接続できないため、その端末を使用することはできない。しかし、これらの技術を用いた場合、その端末を使える場所が制限されてしまうため、利用者が自由に持ち歩いて利用できるという携帯端末の利点が大幅に削がれてしまう問題がある。

【０００６】

本発明は、上記に鑑みてなされたものであって、携帯端末の利用者への利便性を損なうことなく、セキュリティリスクを回避することが可能な携帯端末認証システム、および携帯端末認証方法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】

【０００７】

上述した課題を解決し、目的を達成するために、本発明にかかる携帯端末認証システムは、携帯端末からの要求に応じて利用者を認証する携帯端末認証システムであって、前記利用者が認証のために利用する被認証用携帯端末は、被認証用ＩＣ（Integrated Circuits）タグと、前記利用者によるアクセス要求をサーバに送信する被認証制御部と、を備え、認証者が前記利用者を認証するための認証用携帯端末は、認証用ＩＣタグと、前記被認証用ＩＣタグを読み取るための被認証用ＩＣタグ読み取り部と、前記認証用ＩＣタグを識別するための認証用ＩＣタグ識別情報と前記被認証用ＩＣタグを識別するための被認証用ＩＣタグ識別情報とを含む通信パケットを、前記サーバに送信する認証制御部と、を備え、前記サーバは、前記被認証用携帯端末から前記通信パケットを受信するパケット受信部と、前記認証用携帯端末から前記アクセス要求を受信する要求受信部と、前記パケット受信部が受信した前記通信パケットに前記被認証用タグＩＤと前記認証用タグＩＤとが含まれている場合に、前記要求受信部が受信した前記アクセス要求を許可する利用者認証部と、を備えることを特徴とする。

【０００８】

また、本発明は、上記携帯端末認証システムで行われる携帯端末認証方法である。

【発明の効果】

【０００９】

本発明によれば、携帯端末の利用者への利便性を損なうことなく、セキュリティリスク

を回避することが可能となる。
【図面の簡単な説明】
【００１０】
【図１】本実施の形態における認証システムの全体構成を示す図である。
【図２】業務サーバの構成を示す図である。
【図３】受信情報ＤＢの構成を示す図である。
【図４Ａ】利用者情報テーブルの構成を示す図である。
【図４Ｂ】利用者情報テーブルの構成を示す図である（具体例）。
【図５Ａ】関係情報テーブルの構成を示す図である。
【図５Ｂ】関係情報テーブルの構成を示す図である（具体例）。
【図６Ａ】ポリシーテーブルの構成を示す図である。
【図６Ｂ】ポリシーテーブルの構成を示す図である（具体例）。
【図７】通信パケットの構成を示す図である。
【図８】読取情報設定処理の処理手順を示すフローチャートである。
【図９】受信データ反映処理の処理手順を示すフローチャートである。
【図１０】利用者認証処理の処理手順を示すフローチャートである。
【図１１】ノード整列処理の処理手順を示すフローチャートである。
【発明を実施するための形態】
【００１１】
以下に添付図面を参照して、本発明にかかる携帯端末の認証方法の実施の形態を詳細に説明する。
【００１２】
図1は、本実施の形態における認証システム１０００の全体構成を示している。図１に示すように、認証システム１０００は、業務サーバ１０１と、複数の携帯端末１０２と、を有して構成されている。
【００１３】
業務サーバ１０１は、複数の携帯端末１０２と通信を行う装置である。また、携帯端末１０２は、ＩＣ（Integrated Circuits）タグ１０３の読み取り装置１０４を備えており、各携帯端末１０２のそれぞれにユニークなＩＣタグ１０３が貼付されている。ＩＣタグ１０３は、読み取り装置１０４によって、相対的に互いの端末が読み取り可能な位置関係（範囲）にある場合に携帯端末１０２同士で互いのＩＣタグ１０３を読み取ることができ、読み取った情報は業務サーバ１０１に自動的に送信される。なお、以下では特に図示していないが、業務サーバ１０１や携帯端末１０２は、後述する各種の処理を行うためのＣＰＵ（Central Processing Unit）等から構成される演算装置や、他の端末と通信するための一般的な通信装置を有しているものとする。
【００１４】
図２は、業務サーバ１０１の構成を示している。図２に示すように、業務サーバ１０１は、受信情報ＤＢ２０１と、利用者情報テーブル２０２と、関係情報テーブル２０３と、業務アプリケーション２０４と、利用者認証装置２０５と、タグＩＤ受信装置２０６と、ポリシーテーブル２０７と、を有して構成されている。なお、受信情報ＤＢ２０１、利用者情報テーブル２０２、関係情報テーブル２０３、業務アプリケーション２０４、ポリシーテーブル２０７は、実際にはＨＤＤ（Hard Disk Drive）等の記憶装置に記憶されているものとする。まず、受信情報ＤＢ２０１について説明する。
【００１５】
図３は、受信情報ＤＢ２０１の構成を示す図である。図３に示すように、受信情報ＤＢ２０１は、認証を高速化するため、ツリー構造により構成されたＤＢとなっている。利用者が認証される際に必要な情報は、すべて最上位ノードである認証対象者ＩＤ３０１の下位階層である子ノードに格納されており、検索時にＪＯＩＮ処理のような負荷の重い処理を必要としない構造となっている。
【００１６】

最上位の階層である１階層目の認証対象者ＩＤ３０１は、認証を受けようとする利用者を一意に識別するためのＩＤ（IDentifier）である。ＩＣタグの読み取りという面から見ると、認証対象者は、ＩＣタグ１０３を読み取られた側の携帯端末１０２の利用者である。最上位ノードである認証対象者ＩＤ３０１には索引が付けられており、認証対象者ＩＤ３０１は一意なＩＤの並びであるため、ハッシュインデックス等の一般的な手法で効率的に検索可能となっている。

【００１７】

次の下位階層である２階層目の読み取り者ＩＤ情報３０２は、認証を与える側の利用者を一意に識別するためのＩＤを含む情報である。ＩＣタグの読み取りという面から見ると、読み取り者は、ＩＣタグ１０３を読み取った側の携帯端末１０２の利用者である。下位ノードである読み取り者ＩＤ情報３０２の中には、読み取り者ＩＤ３０２１と、読み取り時刻３０２２と、認証回数３０２３とが対応付けて格納されている。これらの情報は、認証回数の多い順（例えば、認証が成功した回数の多い順）に従って整列されている。読み取り時刻３０２２は、ＩＣタグ１０３が読み取られるたびに、利用者認証装置２０５によってＩＣタグ１０３が読み取られた最新の時刻（利用者の携帯端末１０２から受信した通信パケットに含まれる受信時刻）に更新される。認証回数３０２３は、そのノードが認証に利用されると、利用者認証装置２０５がカウンタ（不図示）をカウントアップする。したがって、認証によく利用されるノードほど認証回数が多くなる。ただし、認証を行うたびにノードの並べ替えを行うと、負荷が重くなってしまうため、認証時は認証回数３０２３をカウントアップするのみとし、システムの負荷が軽い時間帯に、利用者認証装置２０５は、バッチ処理によって読み取り者ＩＤ情報３０２の並べ替え処理を行う。

【００１８】

さらに次の下位階層である３階層目の認証対象者と読み取り者の関係を示す関係情報３０３は、１つの読み取り者ＩＤ情報３０２に対して複数存在する。例えば、部下の携帯端末１０２のＩＣタグ１０３を、その部下が所属する部署の上長の携帯端末１０２が読み取った場合、利用者認証装置２０５により、「上長」という関係および「同一部署」という２つの関係が設定される。より具体的には、業務アプリケーション２０４を実行する利用者に対する認証条件によって、例えば、「上長や上位上長の携帯端末が読み取ること」という条件が設定される場合と、「同じ職場の人員の携帯端末が読み取ること」という条件が設定される場合が考えられる。そして、設定されたこれらの関係情報やこれらの関係情報の組み合わせを認証条件の１つとして、後述するような利用者の認証処理を行う際に使用される。続いて、利用者情報テーブル２０２について説明する。

【００１９】

図４Ａは、利用者情報テーブル２０２の構成を示す図である。図４Ａに示すように、利用者情報テーブル２０２は、複数の利用者情報レコード４０１を有して構成されている。利用者情報レコード４０１のそれぞれは、携帯端末１０２を一意に識別するための端末ＩＤ４０１１と、その携帯端末が有するＩＣタグを一意に識別するための端末タグＩＤ４０１２と、その携帯端末の利用者を一意に識別するための利用者ＩＤとが対応付けて記憶され、携帯端末１０２と貼付されているＩＣタグ１０３と利用者の３つを結びつける役割を有している。例えば、図４Ｂでは、利用者情報テーブル２０２は、端末ＩＤ４０１１が「０００Ａ」、「０００Ｂ」の２台の携帯端末１０２が登録され、それぞれの端末タグＩＤ４０１２および利用者ＩＤ４０１３は、「０００ａ」および「０００１」、「０００ｂ」および「０００２」であることを示している。続いて、関係情報テーブル２０３について説明する。

【００２０】

図５Ａは、関係情報テーブル２０３の構成を示す図である。図５Ａに示すように、関係情報テーブル２０３は、複数の関係情報レコード５０１を有して構成されている。関係情報レコード５０１のそれぞれは、認証を受ける利用者を一意に識別するための被認証者ＩＤ５０１１と、被認証者に認証を与える認証者ＩＤ５０１２と、利用者と認証者との間の関係を示す関係区分５０１３とが対応付けて記憶されている。たとえば、被認証者ＩＤ５

０１１として社員（部下）のＩＤが設定され、認証者ＩＤ５０１２としてその上長のＩＤが設定され、利用者と認証者の関係区分として「上長」が設定される。例えば、図５Ｂでは、被認証者ＩＤ５０１１には、部下の利用者ＩＤ「０００２」が設定され、認証者ＩＤ５０１２には、その上司の利用者ＩＤ「０００１」が設定され、利用者と認証者の関係区分５０１３には、上司と部下の関係を示す「上長」が設定されていることを示している。続いて、関係情報テーブル２０３について説明する。

【００２１】

なお、本実施の形態においては、利用者と認証者の関係区分６０１２には、本システムの利用者が企業の社員等であることを前提として、「上長」と設定しているが、これに限らず、例えば、家族や親族と設定し、利用者が３親等以内の親族に限り、家族のスケジュールを管理するシステムに接続させるというような制御を行うことも可能である。続いて、ポリシーテーブル２０７について説明する。

【００２２】

図６Ａは、ポリシーテーブル２０７の構成を示す図である。図６Ａに示すように、ポリシーテーブル２０７は、複数のポリシーレコード６０１を有して構成されている。ポリシーレコード６０１のそれぞれは、認証が行われて業務アプリケーションによって行われる業務を一意に識別するための業務ＩＤ６０１１と、利用者と認証者との間の関係を示す関係区分６０１２と、利用者が業務アプリケーション２０４を利用するための認証条件を示す認証条件区分６０１２と、認証条件区分に示されている条件を満たすべき時間（間隔）を示す有効時間６０１３とが対応付けて記憶されている。このポリシーレコード６０１は、業務アプリケーション２０４ごとに作成され、認証の利用を許可する条件が設定される。たとえば、ある業務アプリケーション２０４を利用する際には「上長の携帯端末で読み取られていること」を認証の条件とし、別の業務アプリケーション２０４を利用する際には「同じ職場の２名以上の携帯端末で読み取られること」を認証の条件とするように設定される。例えば、図６Ｂでは、業務ＩＤ「アプリＸ」で識別される業務アプリケーション２０４は、そのアプリケーションを利用する直前の少なくとも１０分の間に、上長の携帯端末１０２で、上長の部下の携帯端末１０２のＩＣタグ１０３が読み取られていることを条件として、利用者に対する認証を許可することを示している。

【００２３】

なお、上述した有効時間６０１３は、業務アプリケーション２０４の重要度に応じて設定することとしてもよい。例えば、企業の機密情報や社員や顧客の個人情報に関する業務アプリケーション２０４を使用する場合には、常に上司の監視下で利用者が業務アプリケーション２０４を利用することが望ましいため、短い間隔で繰り返し（例えば、１分毎に繰り返し）部下の携帯端末１０２のＩＣタグ１０３が読み取られていることを条件としたり、あるいは社内備品の在庫管理に関する業務アプリケーション２０４を使用する場合には、比較的上司の監視下で利用者が業務アプリケーションを利用する必要はないため、長い間隔で（例えば、３０分前に１度だけ）部下の携帯端末１０２のＩＣタグ１０３が読み取られていることを条件とすることも可能である。このような設定とすることにより、業務の重要度の応じた柔軟なセキュリティ管理を実現することができる。

【００２４】

さらに、例えば、処理時間が膨大であるために業務アプリケーション２０４を使用した業務を遂行する時間も長時間に及ぶような場合には、長い間隔（例えば、１時間前に１度だけ）部下の携帯端末１０２のＩＣタグ１０３が読み取られていることを条件としたり、その逆に業務アプリケーション２０４を使用した業務を遂行する時間が短時間で済むような場合には、短い間隔（例えば、３０秒前に１度だけ）部下の携帯端末１０２のＩＣタグ１０３が読み取られていることを条件とすることとしてもよい。このような設定とすることにより、効率的なセキュリティ管理を実現することができる。なお、上述した業務の重要度に応じた設定と業務の時間に応じた設定とを組み合わせた条件を設定することももちろん可能である。

【００２５】

タグＩＤ受信装置２０６は、携帯端末１０２から送信された通信パケットを受信して、その情報を利用者認証装置２０５に送る。利用者認証装置２０５は、利用者情報テーブル２０２と関係情報テーブル２０３を参照しながら、受信情報ＤＢ２０１にレコードを追加する。業務アプリケーション２０４は、携帯端末１０２からアクセスを受けると、受信情報ＤＢ２０１とポリシーテーブル２０７とを参照して、利用者の認証を行う。これらの各部の具体的な処理についてはフローチャートを用いて後述する。

【００２６】

図７は、携帯端末１０２から業務サーバ１０１に送信される通信パケットの構成を示す図である。通信パケットはＴＬＶ（Tag Length Value）形式である。識別子７０１は、送信される通信パケットの中に含まれるデータ部分の種別を示す１バイトの値である。通信パケットの受信者情報の中には、1つだけ受信端末タグＩＤ７０２が設定される。これは文字通り、ＩＣタグ１０３を読み取った携帯端末１０２（例えば、上司の携帯端末）に貼付されているＩＣタグ１０３のＩＤである。

【００２７】

読み取りタグＩＤ７０３は、ＩＣタグ１０３を読み取られた携帯端末１０２（例えば、部下の携帯端末）に貼付されているＩＣタグ１０３のＩＤであり、その数は読み取った個数に応じて可変である。例えば、上司と部下以外の他人が所持する携帯端末が通信範囲内に存在する場合には、受信端末タグＩＤ７０２には、上司の携帯端末１０２のＩＣタグ１０３のＩＤが設定され、複数の読み取りタグＩＤ７０３のうちの１つに部下の携帯端末１０２のＩＣタグ１０３が設定された状態となっている。そして、このような通信パケットが、繰り返し定期的に携帯端末１０２（例えば、上司の携帯端末）から業務サーバ１０１に送信される。続いて、認証システム１０００で行われる各種処理の処理手順について説明する。

【００２８】

図８は、業務サーバ１０１が携帯端末１０２から受信した通信パケットに従って読み取り情報を設定する処理（読取情報設定処理）の処理手順を示すフローチャートである。図８に示すように、まず、業務サーバ１０１のタグＩＤ受信装置２０６は、携帯端末１０２から通信パケットを受信すると（ステップ８０１）、受信した通信パケットを解析し、その中に含まれている受信端末タグＩＤ７０２を取り出す（ステップ８０２）。

【００２９】

そして、利用者認証装置２０５は、タグＩＤ受信装置２０６が取り出した受信端末タグＩＤ７０２をキーとして利用者情報テーブル２０２を検索し（ステップ８０３）、利用者情報テーブル２０２に記憶されているレコードの中で、タグＩＤ受信装置２０６が取り出した受信端末タグＩＤ７０２と同じ端末タグＩＤ４０１２を含むレコードがあるか否かを判定する（ステップ８０４）。

【００３０】

利用者認証装置２０５は、利用者情報テーブル２０２に記憶されているレコードの中で、タグＩＤ受信装置２０６が取り出した受信端末タグＩＤ７０２と同じ端末タグＩＤ４０１２を含むレコードがないと判定した場合（ステップ８０４；Ｎｏ）、元々登録されていない利用者の携帯端末からの通信パケットであると判定し、通信パケットを廃棄して、次の通信パケットを待つ。

【００３１】

一方、利用者認証装置２０５は、利用者情報テーブル２０２に記憶されているレコードの中で、タグＩＤ受信装置２０６が取り出した受信端末タグＩＤ７０２と同じ端末タグＩＤ４０１２を含むレコードがあると判定した場合（ステップ８０４；Ｙｅｓ）、そのレコードから利用者ＩＤ４０１３を取り出すとともに、通信パケットの中から読み取りタグＩＤ７０３を1つずつ取り出す（ステップ８０５）。

【００３２】

利用者認証装置２０５は、通信パケットの中から全ての読み取りタグＩＤ７０３を取り出したか否かを判定し（ステップ８０６）、通信パケットの中から全ての読み取りタグＩ

Ｄ７０３を取り出したと判定した場合（ステップ８０６；Ｙｅｓ）、処理を終了させる。
【００３３】
一方、利用者認証装置２０５は、通信パケットの中から全ての読み取りタグＩＤ７０３を取り出していないと判定した場合（ステップ８０６；Ｎｏ）、さらに、読み取りタグＩＤ７０３をキーとして利用者情報テーブル２０２を検索し（ステップ８０７）、その読み取りタグＩＤ７０３と同じ端末タグＩＤ４０１１を含むレコードがあるか否かを判定する（ステップ８０８）。
【００３４】
利用者認証装置２０５は、その読み取りタグＩＤ７０３と同じ端末タグＩＤ４０１１を含むレコードがないと判定した場合（ステップ８０８；Ｎｏ）、本認証システム１０００とは関係のない別のＩＣタグを読み取ってしまったものと判定し、データを破棄して、ステップ８０５に戻って次の読み取りタグＩＤの処理に移る。
【００３５】
一方、利用者認証装置２０５は、その読み取りタグＩＤ７０３と同じ端末タグＩＤ４０１１を含むレコードがあると判定した場合（ステップ８０８；Ｙｅｓ）、そのレコードから利用者ＩＤ（すなわち、読み取られた側の利用者ＩＤ）４０１３を取り出し、受信情報ＤＢ２０１に受信データを反映させる処理（受信データ反映処理）を行い（ステップ８０９）、ステップ８０５に戻って以降の処理を繰り返し行う。
【００３６】
図９は、受信データ反映処理の処理手順を示すフローチャートである。図９に示すように、利用者認証装置２０５は、受信情報ＤＢ２０１にアクセスし、受信情報ＤＢ２０１の索引を用いて、認証対象者ＩＤ３０１と図８のステップ８０９で読み取られた利用者ＩＤ（読み取られた側の利用者ＩＤ）４０１３が等しい１階層ノード（最上位の階層である１階層目の認証対象者ＩＤ３０１）を検索する（ステップ９０１）。
【００３７】
利用者認証装置２０５は、該当するノードが存在するか否かを判定し（ステップ９０２）、該当するノードが存在すると判定した場合（ステップ９０２；Ｙｅｓ）、そのノードのデータを更新すれば良い。一方、利用者認証装置２０５は、該当するノードが存在しないと判定した場合（ステップ９０２；Ｎｏ）、新たに認証対象者のノードを作成し（ステップ９０３）、以降の処理で必要な情報を書き込む。
【００３８】
そして、利用者認証装置２０５は、当該ノードの子ノードを調べ、その子ノードに含まれる読み取り者ＩＤ３０２１と利用者ＩＤ（読み取った側の利用者ＩＤ）４０１３とが等しい２階層ノード（下位ノードである読み取り者ＩＤ情報３０２）を検索する（ステップ９０４）。
【００３９】
利用者認証装置２０５は、該当するノードが存在するか否かを判定し（ステップ９０５）、該当するノードが存在すると判定した場合（ステップ９０５；Ｙｅｓ）、ノードのデータを更新すれば良い。一方、利用者認証装置２０５は、該当するノードが存在しないと判定した場合（ステップ９０５；Ｎｏ）、新たに読み取り者のノードを作成し、リンクの末端にノードを追加する（ステップ９０６）。
【００４０】
さらに、利用者認証装置２０５は、読み取り者ＩＤ情報３０２に含まれる読み取り時刻３０２２と認証回数３０２３とを更新する（ステップ９０７）。このとき、その読み取り者ＩＤ情報３０２が新規に作成されたものである場合には認証回数は「０回」として設定し、既存の読み取り者ＩＤ情報３０２である場合には認証回数は変更しない。読み取り者ＩＤ情報３０２の並び（順序）が認証回数の順序となっていない場合もあるが、この時点では何もせずに、並び替えの処理を行わないものとする。リンク並べ替えの負荷を軽減するため、システムの負荷が軽い時間帯を選んで、バッチ処理等によりまとめてリンクの並べ替え処理を行う。

【００４１】
利用者認証装置２０５は、関係情報テーブル２０３を検索し、利用者ＩＤ（読まれた側の利用者ＩＤ）４０１３と被認証者ＩＤ５０１１が等しく、かつ、利用者ＩＤ（読んだ側の利用者ＩＤ）４０１３と認証者ＩＤ５０１２が一致するレコードを検索し、そのレコードに含まれる関係情報を取り出す（ステップ９０８）。利用者認証装置２０５は、読み取りＩＤノードの子ノードを辿って、関係情報レコード５０１と一致する関係を保持する３階層ノード（３階層目の認証対象者と読み取り者の関係を示す関係情報３０３）が存在するかどうかを調べる。
【００４２】
そして、利用者認証装置２０５は、関係情報レコード５０１と一致する関係を保持する３階層ノード（子ノード）が存在するか否かを判定し（ステップ９０９）、関係情報レコードと一致する関係を保持する３階層ノードが存在すると判定した場合（ステップ９０９；Ｙｅｓ）、処理を終了させる。
【００４３】
一方、利用者認証装置２０５は、関係情報レコードと一致する関係を保持する３階層ノードが存在しないと判定した場合（ステップ９０９；Ｎｏ）、新しく認証対象者と読み取り者の関係のノードを作成して、読み取り者ＩＤ情報３０２の下位ノードに追加する（ステップ９１０）。このステップ９１０の処理が終了すると、図９に示した受信データ反映処理の全ての処理が終了する。そして、図８および図９に示した処理を繰り返し定期的に行うことによって、業務サーバ１０１は携帯端末１０２の位置を管理する必要がなく、単に携帯端末１０２が読み取ったＩＣタグのみ報告を受ければよいため、利用者の認証のための管理が容易となる。
【００４４】
続いて、業務アプリケーション２０４にアクセスする利用者を認証する際に行われる処理（利用者認証処理）について説明する。図１０は、利用者認証処理の処理手順を示すフローチャートである。なお、以下の処理を行う前提として、利用者は、あらかじめシステムにログイン等する際に、使用する業務の業務ＩＤおよび自身の利用者ＩＤを携帯端末１０２から入力し、業務サーバ１０１に送信しているものとする。
【００４５】
図１０に示すように、利用者認証装置２０５は、まず、業務ＩＤ６０１１をキーとしてポリシーテーブル２０７を検索し、携帯端末１０２から受信した業務ＩＤに一致する業務ＩＤ６０１１を有したポリシーレコード６０１から認可に必要な条件を取得する（ステップ１００１）。利用者が利用する業務によって許可する条件が異なるため、まず認証のポリシーを明確にしなければならないためである。
【００４６】
次に、利用者認証装置２０５は、受信情報ＤＢ２０１を検索して、アクセスを要求してきた利用者ＩＤと一致する認証対象者ＩＤ３０１含む１階層ノードを検索し（ステップ１００２）、一致するノードが存在するか否かを判定する（ステップ１００３）。
【００４７】
利用者認証装置２０５は、一致するノードが存在しないと判定した場合（ステップ１００３；Ｎｏ）、当該利用者のＩＣタグが読み取られていないことを意味するため、利用者に認証失敗の応答を返し、処理を終了させる。
【００４８】
一方、利用者認証装置２０５は、一致するノードが存在すると判定した場合（ステップ１００３；Ｙｅｓ）、そのノードの子ノードを順にスキャンし（ステップ１００４）、以降の処理で認証ポリシーに一致するノードがあるかどうか調べる。
【００４９】
利用者認証装置２０５は、ステップ１００５において、スキャンすべきノードはまだ残っているか否かを判定し（ステップ１００５）、スキャンすべきノードはもう残っていない、すなわち、認証ポリシーに一致するノードがないと判定した場合（ステップ１００５

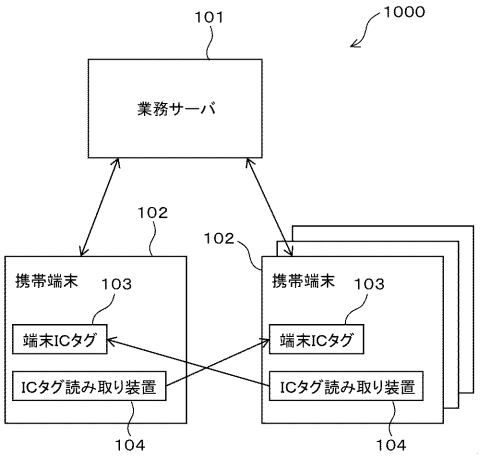
；Ｎｏ）、利用者に認証失敗の応答を返し、処理を終了させる。
【００５０】
一方、利用者認証装置２０５は、スキャンすべきノードがあると判定した場合（ステップ１００５；Ｙｅｓ）、そのノードが認証ポリシーに一致するノードであるか調べ（ステップ１００６）、両者が一致するか否かを判定する（ステップ１００７）。
【００５１】
そして、利用者認証装置２０５は、両者が一致しないと判定した場合（ステップ１００７；Ｎｏ）、ステップ１００４に戻って、以降の処理を繰り返す。一方、利用者認証装置２０５は、両者が一致すると判定した場合（ステップ１００７；Ｙｅｓ）、認証成功と判断して、利用者のアクセスを許可し、認証ポリシーに一致したノードの認証回数３０２３をカウントアップし（ステップ１００８）、処理を終了させる。
【００５２】
上述した認証ポリシーが一致するか否かの判定のレベルは、利用者が利用しようとする業務の業務アプリケーション２０４の種類によって異なるが、主に、読み取り時刻３０２に関する条件と、関係情報３０３に関する条件とがある。読み取り時刻３０２に関する条件としては、例えば、利用者認証装置２０５は、受信情報ＤＢ２０１の読み取り者ＩＤ情報３０２に含まれる読み取り時刻３０２２とタイマ（不図示）により計時される現在時刻とを比較して、その差が有効時間６０１４として設定された時間以内であれば認証を許可する。この場合、業務の重要性等のセキュリティ要件によって、数分に設定される場合もあれば、３０分や１時間程度に設定されることもある。
【００５３】
また、関係情報３０３に関する条件としては、例えば、利用者認証装置２０５は、３階層ノード（３階層目の認証対象者と読み取り者の関係を示す関係情報３０３）およびポリシーテーブル２０７を参照し、関係情報３０３に設定されている認証対象者と読み取り者との関係３０３１、３０３２に利用者が利用しようとしている業務ＩＤ６０１１の業務で必要とされている利用者と認証者の関係区分６０１２が含まれているか否か（例えば、「上長」として設定されているか否か）を判定し、そのような設定がされている場合には認証を許可する。もちろん、上述した読み取り時刻３０２に関する条件と関係情報３０３に関する条件とを組み合わせて利用者を認証することも可能である。
【００５４】
なお、認証に使われる回数が多いノードは、例えば、いつも一緒に行動している上長や同僚である可能性が高く、近い将来にまた使われる可能性も高い。したがって、利用者認証装置２０５が、後述するノード整列処理を行ってリンクの上位に並べておくことにより、検索を効率化することができる。
【００５５】
図１１は、２階層のノードを整列する処理（ノード整列処理）の処理手順を示すフローチャートである。図１１に示すように、利用者認証装置２０５は、あらかじめ定められた規定時間だけスリープ時間が経過すると（ステップ１１０１）、業務サーバ１０１のシステム負荷を調べ、システム負荷が高いか否か（所定の上限値を超えているか否か）を判定する（ステップ１１０２）。
【００５６】
なお、システム負荷は、例えば、ＣＰＵ利用率、メモリの使用状況、ディスク使用率、回線負荷などを監視して定められるものとし、ＣＰＵ使用率またはディスク使用率のいずれかが５０％を超えている場合には負荷が高いと判断し、本ノード整列処理は控える判断をする。また、スリープ時間は、認証業務の要件やシステム負荷を考慮して、例えば５分などに設定する。
【００５７】
そして、利用者認証装置２０５は、システム負荷が高い（所定の上限値を超えている）と判定した場合（ステップ１１０２；Ｙｅｓ）、ステップ１１０１に戻って再びスリープ状態となる。

【００５８】
一方、利用者認証装置２０５は、システム負荷が高くない（所定の上限値を超えていない）と判定した場合（ステップ１１０２；Ｎｏ）、予め定められた数の１階層ノードをスキャンし（ステップ１１０３）、全てのノードのスキャンが終了せず、１階層ノードがまだ残っているか否かを判定する（ステップ１１０４）。
【００５９】
利用者認証装置２０５は、１階層ノードがもう残っていないと判定した場合（ステップ１１０４；Ｎｏ）、ステップ１１０１に戻ってスリープ状態となる。一方、利用者認証装置２０５は、１階層ノードがまだ残っていると判定した場合（ステップ１１０４；Ｙｅｓ）、実際に認証回数順に２階層ノードの整列処理を行う。
【００６０】
本ノード整列処理において、１回ですべてのノードを整列するのではなく、一定数のノードを整列したところで処理を終了し、次回の処理で続きの整列を行うこととしてもよい。大規模なシステムでは、登録されているノード数も膨大となるため、すべてのノードを処理すると長い時間がかかってしまう。したがって、整列処理を小分けにして、少しずつ整列を実行することで、システム全体のレスポンスが低下することを回避することが可能となる。具体的には、処理するノードの規定数を、整列にかかる時間と、業務要件を考慮して、例えば、１回に１０００ノードずつ処理するというように定め、当該１階層ノード直下の２階層ノードを、認証回数が多い順に並べ替える。この場合、規定の件数を処理するか、すべてのノードを処理したら、再びスリープ状態に戻ることとなる。
【００６１】
このように、本実施の形態においては、単純に端末の位置で制限するのではなく、他の端末との位置関係を元にアクセス制限を行い、例えば、携帯端末にＩＣタグを貼付して、他の携帯端末から当該ＩＣタグを読み取り、業務サーバに繰り返し定期的に報告する。そして、利用者からアクセス要求が届いた場合に、当該利用者の携帯端末に貼付されたＩＣタグが関係者の携帯端末から読めているかどうか確認する。例えば、同じ部門の社員の端末からタグが読み取れていれば、業務サーバへのアクセスを許可するというような制御を行っているので、出張する度に、利用場所を登録する手間は不要となり、また、携帯端末が盗難に遭って持ち去られたとしても、その携帯端末のＩＣタグが読み取れなければ業務アプリケーションに接続することはできないため、そのような場合であっても高度なセキュリティを保つことが可能となる。さらに、副次的な効果として、利用者本人の不正を抑制させ、また、通常、不正は人目を避けて実行されるため、本システムによれば、必ず近くに上長や同僚の目があることが保証され、その意味でも高度なセキュリティを保つことが可能となる。
【００６２】
なお、本発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化することができる。例えば、業務サーバ１０１のうち、その容量が膨大となる場合には、受信情報ＤＢ２０１や利用者情報テーブル２０２等のデータのみを他のサーバとして構成する等、構成要素を適宜組み合わせても良い。
【符号の説明】
【００６３】
１０００　認証システム
１０１　業務サーバ
１０２　携帯端末
１０３　ＩＣタグ
１０４　読み取り装置
２０１　受信情報ＤＢ
２０２　利用者情報テーブル
２０３　関係情報テーブル

２０４　　業務アプリケーション
２０５　　利用者認証装置
２０６　　タグＩＤ受信装置
２０７　　ポリシーテーブル。

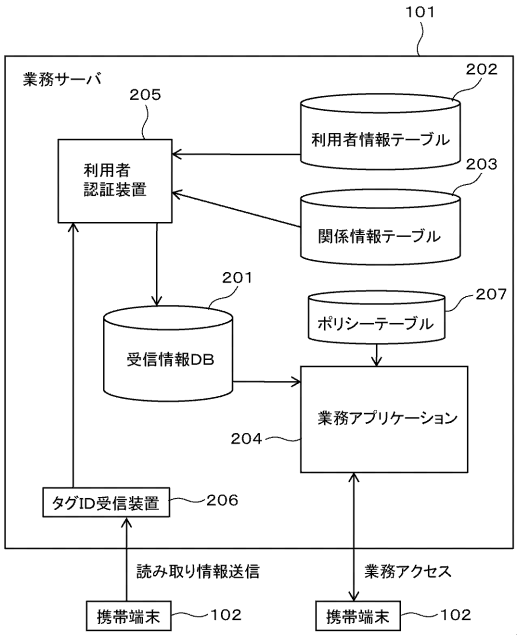
【図１】

図１



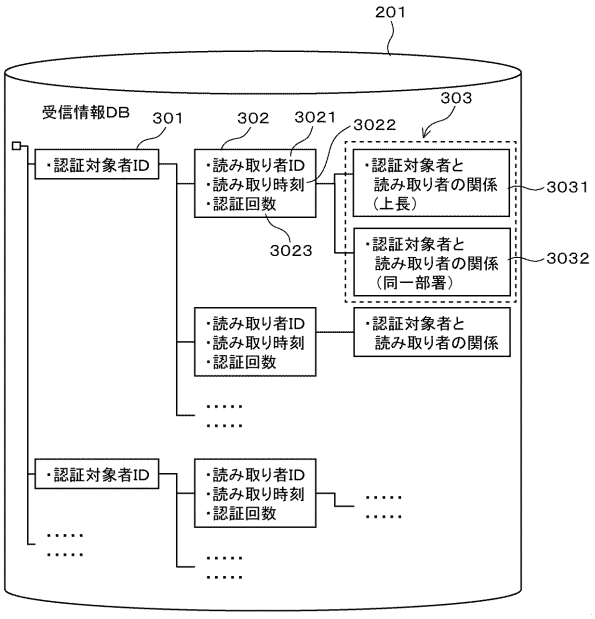
【図２】

図２



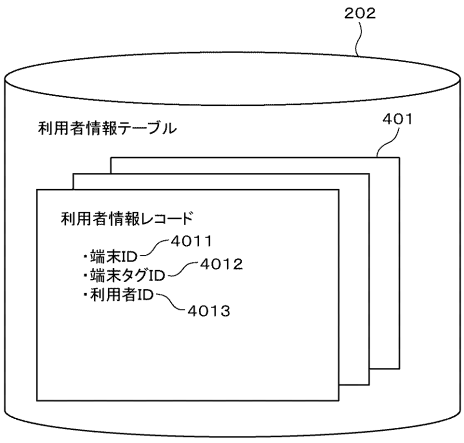
【図３】

図３



【図４Ａ】

図４Ａ



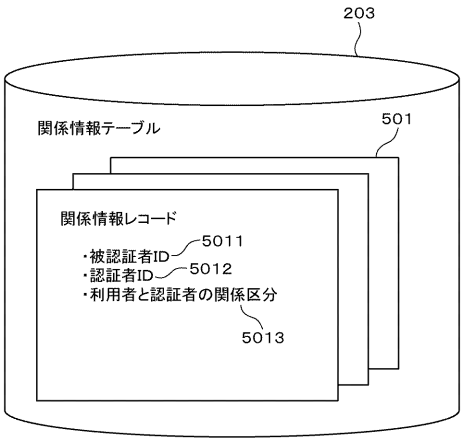
【図４Ｂ】

図４Ｂ

4011 端末ID	4012 端末タグID	4013 利用者ID
000A	000a	0001
000B	000b	0002
⋮	⋮	⋮

【図５Ａ】

図５Ａ



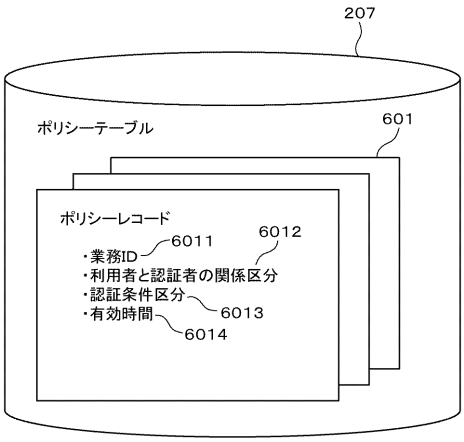
【図５Ｂ】

図５Ｂ

5011 被認証者ID	5012 認証者ID	5013 利用者と認証者の関係区分
0002	0001	上長
⋮	⋮	⋮

【図６Ａ】

図６Ａ



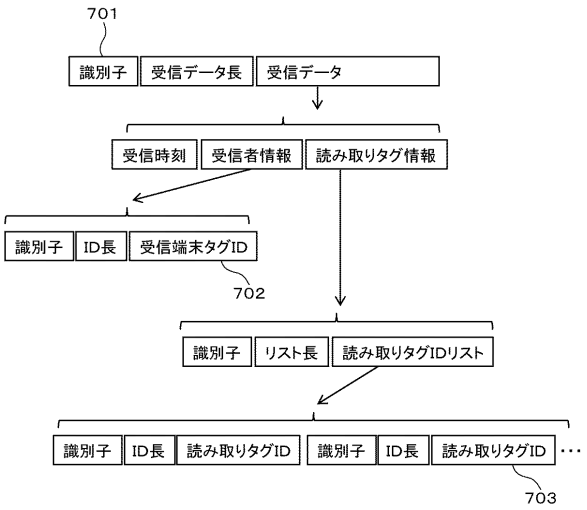
【図６Ｂ】

図６Ｂ

6011 業務ID	6012 利用者と認証者の関係区分	6013 認証条件区分	6014 有効時間
アプリX	上長	上長の携帯端末で ICタグが読み取られている	10分
⋮	⋮	⋮	⋮

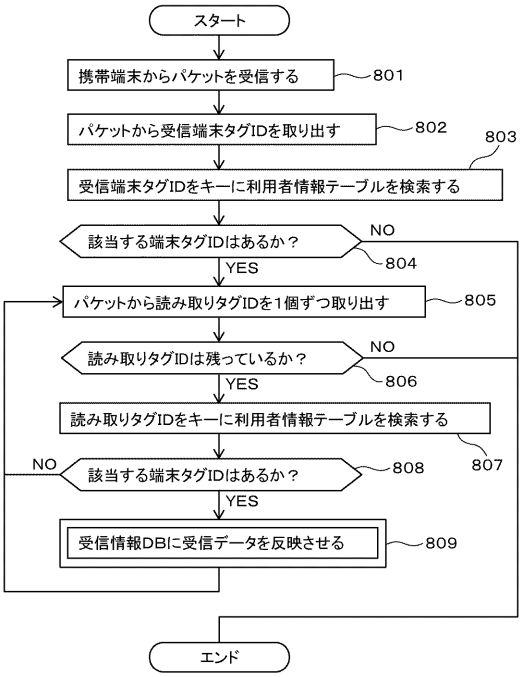
【図７】

図７



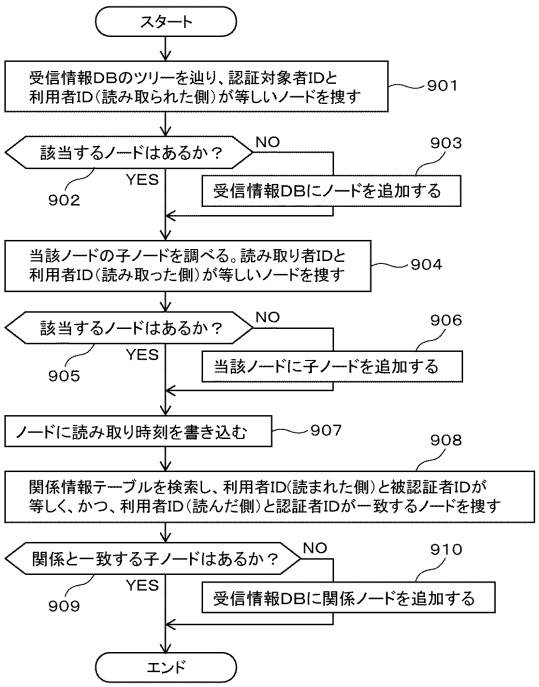
【図８】

図８



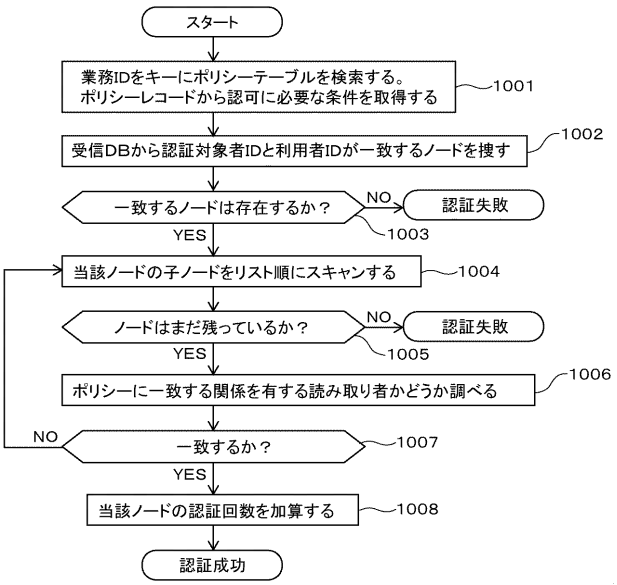
【図９】

図９



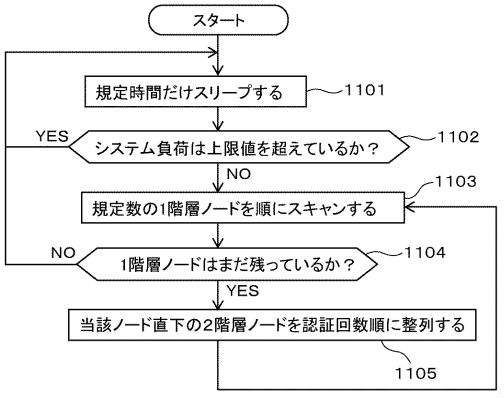
【図１０】

図１０



【図１１】

図１１


スタート
規定時間だけスリープする
1101
YES
システム負荷は上限値を超えているか？
1102
NO
1103
規定数の1階層ノードを順にスキャンする
NO
1階層ノードはまだ残っているか？
1104
YES
当該ノード直下の2階層ノードを認証回数順に整列する
1105

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
H04M 1/67	***(2006.01)***	H04M	1/67		
H04W 12/06	***(2009.01)***	H04Q	7/00	１８３	

(72)発明者 日森 由樹
神奈川県川崎市幸区鹿島田８９０番地 株式会社日立製作所セキュリティ・トレーサビリティ事業部内
(72)発明者 堀 健太郎
神奈川県川崎市幸区鹿島田８９０番地 株式会社日立製作所セキュリティ・トレーサビリティ事業部内
(72)発明者 井上 健
神奈川県川崎市幸区鹿島田８９０番地 株式会社日立製作所セキュリティ・トレーサビリティ事業部内

Ｆターム(参考) 5J104 AA07 AA16 EA08 EA16 KA02 NA33 NA36 PA07
5K067 AA32 AA33 BB21 DD17 EE02 EE10 EE35 HH22 HH23 KK15
5K127 AA21 BA03 BB23 BB33 DA14 GA12 GE03 JA14 JA42 JA56 JA57
5K201 AA09 BB07 CB10 CC03 EC06