

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-163379
(P2000-163379A)

(43) 公開日 平成12年6月16日 (2000.6.16)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D
G 0 1 S 5/14		G 0 1 S 5/14	
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 A
	12/14		3 1 0 K
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D

審査請求 未請求 請求項の数28 OL (全 11 頁) 最終頁に続く

(21) 出願番号 特願平11-308358

(22) 出願日 平成11年10月29日 (1999. 10. 29)

(31) 優先権主張番号 0 9 / 1 8 2 3 4 2

(32) 優先日 平成10年10月29日 (1998. 10. 29)

(33) 優先権主張国 米国 (U S)

(71) 出願人 599153541

デイトム インコーポレイテッド
アメリカ合衆国 マサチューセッツ州 ベ
ッドフォード ミドルセックスターンパイ
ク 54

(72) 発明者 トーマス マーク ヘイスティングス
アメリカ合衆国 マサチューセッツ州
02420 レキシントン メリアムストリー
ト 38

(74) 代理人 100079119
弁理士 藤村 元彦 (外1名)

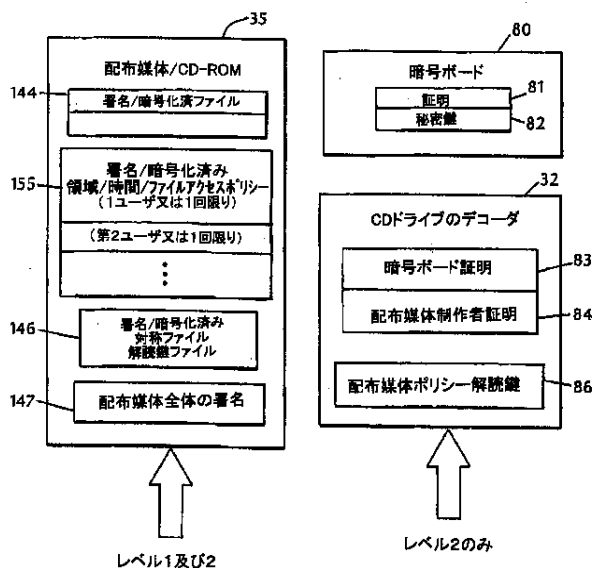
最終頁に続く

(54) 【発明の名称】 格納情報へのアクセス制御

(57) 【要約】 (修正有)

【課題】 情報の使用を指定された地理的領域に制限で
きる格納された情報へのアクセス制御方法。

【解決手段】 ユーザによる格納情報へのアクセスは、
実際の地理的位置又は実際の日/時を格納情報へのア
クセスが許可された地理的領域又は期間と比較すること
によって制御される。格納情報が位置する実際の地理的
位置及び実際の日/時は、例えば、GPS受信機などの信
頼できる位置及び時間情報を供給する受信機で受信され
た信号に基づいて確定される。実際の地理的位置又は日
/時が許可された地理的領域又は期間内である場合に格
納情報へのアクセスが許可される。受信機から供給され
る位置及び日/時の情報は、暗号法により署名及び暗号
化されてもよい。



【特許請求の範囲】

【請求項1】 格納情報へのアクセスを制御する方法であって、
信頼できる位置情報を供給する受信機で受信した信号に基づいて前記格納情報が位置する実際の地理的位置を確定するステップと、
前記実際の地理的位置を前記格納情報へのアクセスが許可された地理的領域と比較するステップと、
前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

【請求項2】 請求項1に記載の方法であって、前記受信機はGPS受信機からなることを特徴とする方法。

【請求項3】 請求項1に記載の方法であって、前記格納情報はコンピュータ可読の媒体に格納されることを特徴とする方法。

【請求項4】 請求項3に記載の方法であって、前記コンピュータ可読の媒体は可搬型であることを特徴とする方法。

【請求項5】 請求項3に記載の方法であって、前記コンピュータ可読の媒体は大容量ディスクからなることを特徴とする方法。

【請求項6】 請求項1に記載の方法であって、前記格納情報は、各々がアクセスが許可される関連した地理的領域を含むファイルからなり、前記実際の地理的位置が前記ファイルの該許可された地理的領域内に位置する場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。

【請求項7】 請求項6に記載の方法であって、前記実際の地理的位置が前記許可された地理的領域に一致しない場合に、前記格納情報へのアクセスを拒否するステップを更に有することを特徴とする方法。

【請求項8】 請求項1に記載の方法であって、暗号鍵を用いて前記格納情報を暗号化するステップと、前記実際の地理的位置が前記許可された地理的領域内に位置する場合に、前記格納情報の解読を許す解読キーを提供するステップと、を更に有することを特徴とする方法。

【請求項9】 請求項1に記載の方法であって、暗号法により前記実際の地理的位置に受信機の暗号鍵で署名するステップと、
実際の地理的位置が前記許可された地理的領域と比較される前に受信機の解読キーで前記受信機の署名を検証するステップと、を更に有することを特徴とする方法。

【請求項10】 請求項1に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも1つは他のサブセットと異なる許可された地理的領域を有し、該許可された地理的領域が実際の地理的位置内に位置するサブセットへのアクセスは許可され、前記許可された地理的領域が実際の地理的位置内

に位置しないサブセットへのアクセスは許可されないことを特徴とする方法。

【請求項11】 請求項6に記載の方法であって、前記許可された地理的領域との該関連はポリシーファイルとして前記格納情報と共に格納されることを特徴とする方法。

【請求項12】 格納情報へのアクセスを制御するための装置であって、
信頼できる位置情報を供給して前記格納情報が位置する実際の地理的位置を確定する受信機と、
前記実際の地理的位置を前記格納情報へのアクセスが許可される地理的領域と比較するコンピュータと、を有し、
前記コンピュータは、前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すことを特徴とする装置。

【請求項13】 請求項12に記載の装置であって、前記受信機はGPS受信機であることを特徴とする装置。

【請求項14】 請求項12に記載の装置であって、前記受信機は、前記実際の地理的位置に暗号法により署名するための受信機暗号鍵を提供する受信機暗号メカニズムを更に有することを特徴とする装置。

【請求項15】 請求項14に記載の装置であって、前記格納情報を読み取る読取装置を更に有し、前記読取装置は、該暗号法により署名された実際の位置を検証する受信機解読キーを含むことを特徴とする装置。

【請求項16】 請求項15に記載の装置であって、前記読取装置は、前記受信機に送信されて前記実際の地理的位置に加えられる位置オフセットを提供する初期化ベクトルを生成することを特徴とする装置。

【請求項17】 請求項16に記載の装置であって、前記位置オフセットに暗号法により署名するための読取装置暗号鍵を提供する読取装置暗号メカニズムを更に有し、前記位置オフセットが前記実際の地理的位置に加えられる前に、該位置オフセット署名は前記受信機によって対応する読取装置解読キーにより検証されることを特徴とする装置。

【請求項18】 格納情報のより大規模なファイルセットに属するファイルサブセットへのアクセスを制御する方法であって、
該大規模ファイルセットのファイルの各々に一意のファイル暗号鍵を関連付けて、該関連暗号鍵を用いて前記ファイルを暗号化するステップと、
前記格納情報へのアクセスが許可される少なくとも1つの許可された地理的領域を前記大規模ファイルセットのファイルの各々に関連付けるステップと、
信頼できる位置情報を供給する受信機で受信された信号に基づいて、前記格納情報が位置する実際の地理的位置を確定するステップと、
前記実際の地理的位置を前記許可された地理的領域と比

較するステップと、
実際の地理的位置が前記ファイルサブセットに属するファイルの前記許可された地理的領域内に位置する場合には、前記ファイルサブセットに属する前記ファイルへのアクセスを許可し解読を許すファイル解読キーを供給するステップと、を有することを特徴とする方法。

【請求項19】 請求項18に記載の方法であって、前記ファイルと前記許可された地理的領域との前記関連はポリシーファイルを含むポリシーとして格納され、前記ポリシーファイルの各々は、ユーザ・パスワードによりアクセスでき、実際の地理的位置が前記ファイルに関連した前記許可された地理的領域内に位置しユーザ・パスワードが有効な場合に前記ポリシーファイルにリストされたファイルへのアクセスを許可することを特徴とする方法。

【請求項20】 請求項19に記載の方法であって、前記ポリシーは前記格納情報と共に格納されることを特徴とする方法。

【請求項21】 格納情報へのアクセスを制御する方法であって、
信頼できる時間情報を供給する受信機で受信された信号に基づいて前記格納情報の位置における実際の日付又は時間を確定するステップと、
前記実際の日付又は時間を前記格納情報へのアクセスが許可される所定の日付又は時間の期間と比較するステップと、
前記実際の日付又は時間が該許可された日付又は時間の期間内に発生した場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

【請求項22】 請求項21に記載の方法であって、前記実際の日付又は時間が前記許可された日付又は時間の期間内に発生しなかった場合に前記格納情報へのアクセスを拒否するステップ、を更に有することを特徴とする方法。

【請求項23】 請求項21に記載の方法であって、前記情報は、各々がアクセスが許される関連した許可された日付又は時間の期間を有するファイルを有し、前記実際の日付又は時間が該関連した許可された日付又は時間の期間内に発生した場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。

【請求項24】 請求項21に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも1つは他のサブセットと異なる許可された日付又は時間の期間を有し、前記実際の日付又は時間に一致する許可された日付又は時間の期間を有するサブセットへのアクセスは許可され、前記実際の日付又は時間に一致しないサブセットへのアクセスは許可されないことを特徴とする方法。

【請求項25】 格納された情報へのアクセスを制御する方法であって、

前記情報を許可された地理的領域及び許可された期間と関連付けたポリシーを形成するステップと、
暗号法により前記ポリシー及び前記情報に署名を行うステップと、
該署名されたポリシーを該署名された情報と共に格納するステップと、
前記ポリシーのロックを解除するパスワードを供給するステップと、

信頼できる位置情報を供給する受信機で受信された信号に基づいて、該格納された情報が位置する実際の地理的位置を確定するステップと、
実際の時間を確定するステップと、
前記実際の地理的位置及び前記実際の時間を前記ポリシーの前記許可された地理的領域及び前記許可された期間と比較するステップと、
前記実際の地理的位置及び前記実際の時間が前記ポリシーの前記許可された地理的領域及び前記許可された期間内である場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。

【請求項26】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は全地球周回ナビゲーション衛星システムであることを特徴とする方法。

【請求項27】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は慣性航法システムであることを特徴とする方法。

【請求項28】 請求項1に記載の方法であって、前記信頼できる位置及び時間の供給源は衛星ベースの位置確定システムであることを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、格納された情報へのアクセス制御に関する。

【0002】

【従来の技術】例えばCD-ROM等のデータ配布媒体には多数のファイルを格納することができる。CD-ROMの製作者は、秘密扱いである、又はユーザによる支払いを要するという理由から特定のファイルへのユーザのアクセスを制御することを望む場合がある。

【0003】ユーザに対しCD-ROM製作者から得られるパスワードの入力を要求することによってアクセスを制御してもよい。異なるパスワードによって、異なるファイル又は異なるファイルのサブセットのロックが解除（アンロック）されてもよい。ファイルは、暗号によって署名され、更に保護のために暗号化されてもよい。製作者がその製作者だけが知っている一意の鍵（キー）によって各ファイルを暗号化する方法について記載された米国特許第5,646,992号を参考文献としてここに挙げる。ユーザが暗号化されたアイテムを受け取り、製作者がそのユーザのアクセス要求を処理した後、ユーザは暗号化された各ファイルの解読に用いられる解読鍵（すな

わち、パスワード)を受け取る。パスワードは、アクセスが要求されたファイルのみロックを解除する。

【0004】

【発明の概要】本発明は、信頼できる位置情報を供給する受信機により受信した信号に基づいて配置される格納情報の実際の地理的位置を確定することによって格納情報へのアクセスを制御することを一つの特徴としている。次に、実際の地理的位置は、格納情報に対するアクセスが許可される地理的な領域と比較される。実際の地理的位置が許可された地理的領域内に位置する場合、ユーザは格納情報へのアクセスを許される。

【0005】本発明の実施例は、以下の特徴を含んでいる。位置情報を供給する受信機は、衛星ベースの位置確定システム又は慣性航法装置から位置情報を受信することができる。その情報は、コンピュータ可読の媒体(例えば、大容量ディスク)に格納される。格納情報はファイルを含み、これらのファイルの各々はアクセスが許される関連した地理的領域を含む。実際の地理的位置がファイルに許可された地理的領域内に位置する場合、ユーザはその特定のファイルにアクセスできる。格納情報は暗号化することができ、実際の地理的位置が許可された地理的領域内に位置する場合だけ、ユーザは解読鍵にアクセスできる。また、格納情報は情報のサブセットに分割することができ、少なくとも1つのサブセットは他のサブセットとは異なる許可領域を有する。許可された地理的領域とファイルとの対応は、ポリシーファイル(policy file)として格納情報と共に格納される。

【0006】本発明は他の特徴として、信頼できる時間情報を供給する受信機により受信された信号に基づいて格納情報の位置における実際の日付又は時間を確定する。実際の日付又は時間は、格納情報に対するアクセスが許可された所定の日付又は時間の期間と比較される。実際の日付又は時間が許可された期間内にある場合、ユーザは格納情報にアクセスすることができる。

【0007】本発明は他の特徴として、格納情報が位置する実際の地理的位置を確定するために信頼できる位置情報を供給する受信機を含む。コンピュータは、格納情報へのアクセスが許可される地理的領域と位置情報を受信し、実際の地理的位置が許可された地理的領域内に位置する場合にアクセスを許可する。本発明の実施例は以下の特徴を有している。受信機は、暗号法により実際の地理的位置に受信機暗号鍵で署名して、実際の地理的位置が許可された地理的領域と比較される前に、その受信機署名を受信機解読鍵で検証する受信機暗号メカニズムを含む。

【0008】更に他の特徴として、本発明は、暗号によって署名された実際の位置を検証するための対応する受信機解読鍵を有する読取装置を含む。本発明の実施例は、以下の特徴を含む。読取装置は、受信機に送信されて実際の地理的位置に加えらる位置オフセットを提供

する初期化ベクトルを生成する。読取装置は、読取装置暗号鍵によって位置オフセットに暗号署名する。受信機は、位置オフセットが実際の地理的位置に加えらる前に、対応する読取装置解読鍵により位置オフセットの署名を検証する。

【0009】本発明の他の特徴として、情報と許可された地理的領域及び許可された期間とを関連させるポリシーを形成し、暗号によってその情報及びポリシーに署名する。署名されたポリシーは、署名された情報と共に格納される。ユーザは、実際の地理的位置及び実際の時間がそれぞれ許可された地理的領域及び許可された期間内にある場合に、製作者からポリシーのロックを解くためのパスワードを得て、格納情報にアクセスすることができる。

【0010】本発明の利点について以下に述べる。格納情報の製作者は、その情報の使用を指定された地理的領域に制限するか、又は使用が許されない指定領域を除外することができる。例えば、CD-ROMに格納される自動車のサービス・マニュアルは、対応する特定の国及び/又は領域に適用できる異なるセクションの情報を含んでいてもよい。ユーザは、現在の地理的位置に適用できる一部の情報のみを見ることが許されてもよい。同様に、機密に関わる会社のレポートへのアクセスは、特定の施設位置に限られていてもよい。時間に敏感な情報に対するアクセスは、一定の日の前又は後に拒否されるか、又は許された期間に限られてもよい。許可された地理的領域及び期間についての情報を、CD-ROMに格納されユーザ・パスワードによってアクセスされるポリシー・ファイルと関連させることによって、CD-ROMの製作者は、ユーザが特定のポリシー・ファイルの一式、従って、対応する領域及び日/時間で許可された情報にアクセスすることを許可する新たなパスワードを発行することができる。

【0011】本発明の他の利点及び特徴は、下記の記載及び特許請求の範囲から明らかになる。

【0012】

【発明の実施の形態】図1ないし図3に示すように、データ配布媒体35として用いられる携帯用のコンピュータ可読のCD-ROMに格納された情報へのアクセスは、情報へのアクセスがなされるコンピュータ・システム10の実際の地理的位置及びアクセスされる時間に基づいて制御されてもよい。

【0013】コンピュータ・システム10において、コンピュータ20はキーボード50、マウス60、モニター40及びCD-ROMドライブ30に接続されている。GPS受信機70は、信頼できる位置情報及び時間情報の供給源として機能する。受信機70は、コンピュータ・システム10の実際の地理的位置に位置し、周囲するGPS衛星90(1つのみを示す)から信号75を受信する。受信機70は、受信信号75を経度、緯度及

び高度について数メートルの精度の地理的位置データ71、及びマイクロ秒の精度の日/時データ71に変換する。データ71は、デバイス・ドライバ72を経てコンピュータ20に送信される。

【0014】図6に示すように、受信機暗号ボード80は、製作者によって署名された公開鍵証明書81及び対応する秘密鍵82を含んでもよい。また、地理的位置及び日/時データ71は、データを認証するために秘密鍵82によって署名されてもよい。また、図6に示すように、CD-ROMドライブ30は、ハードウェア又はソフトウェアとして組み込まれた暗号及び署名機能（デコーダ32）を含んでもよい。デコーダ32は、証明書81と同一の暗号ボード公開鍵証明書83、製作者の身元確認のための製作者証明84、及びその製作者によって署名された配布媒体ポリシー解読鍵86を含む。暗号ボード証明83は、秘密鍵82によって署名された暗号ボード80の署名を検証する。ポリシー解読鍵86は、CD-ROM35に格納されたアクセス・ポリシー155を解読する。

【0015】下記の実施例に記載するように、コンピュータ・システム10は、レベル1及びレベル2等の数レベルのセキュリティを有することができる。レベル1のセキュリティを有するシステムにおいて、受信機70は従来のデバイス・ドライバ72を介してコンピュータ20と通信する。また、CD-ROMドライブ30は従来のCD-ROMである。受信機70及びCD-ROMドライブ30は、付属の暗号/解読機能を有していない。セキュリティを高めるため、レベル1のシステムのコンピュータ20は、データを認証及び/又は暗号化することができる「信頼できる」コンピュータである。さらに安全のため、レベル2のシステムにおいては、受信機70は暗号ボード80を含み、CD-ROMドライブ30はデコーダ32を含んでもよい。レベル2のシステムは、データ認証、及び受信機70とデコーダ32との間のデータ伝送の暗号化を行うように設計される。また、コンピュータ20は、データ認証及び暗号化を行わない市販のコンピュータであってもよい。

【0016】キーボード50及びマウス60からの入力データは、ユーザ・インタフェース95を介して入力された通常のコマンド及びデータ入力130（アプリケーション・プログラム34によって提供される）、及びユーザがデータ配布媒体35に格納された情報にアクセスするための一つ以上のパスワード130を含んでもよい。

【0017】CD-ROM35は、情報ファイル144、許可された地理的領域のリスト150、許可された日/時の期間のリスト154、一つ以上のファイル解読鍵ファイル146、一つ以上のポリシー・ファイル152及びCD-ROM35全体の署名147等の種々の情報を格納する。図3に示すように、ファイル144、1

46、150、152、154及び155は署名及び暗号化されてもよい。

【0018】ファイル144は、サブセット141、142及び143にグループ化されてもよい。また、ファイルは複数のサブセットに属していてもよい。（以下の説明において、ファイルの語は、ファイル及びファイル・サブセットの両者を意味する）。ファイル141、142及び143のそれぞれは、一意的なファイル暗号鍵51（E1、E2、E3）によって暗号化されてもよい。対応するファイル解読鍵52（K1、K2、K3）は、CD-ROM35のファイル解読鍵ファイル146に格納される。解読鍵及び解読鍵ファイルに関する更なる情報は、米国特許第5,646,992号に記載されている。

【0019】CD-ROM35上のファイル141、142及び143の各々は、許可された地理的領域のリスト150に格納された許可された地理的領域のうちゼロ又は1つ以上と関連付けられている。例えば、ニューヨーク市のエンパイアステートビルに対応する緯度及び経度、及び50ないし60メートルの高度で領域が区切られ、その領域に関連するファイルは、受信機70がエンパイアステートビルのある一定のオフィス領域内に位置する場合にのみ開くことができる。

【0020】同様に、ファイル141、142及び143の各々は、許可された日/時の期間のリスト154に格納された許可された期間のうちゼロ又は1つ以上と関連付けられる。GPS衛星90のそれぞれは、極めて高精度のクロックを維持する。受信機70は信号75の一部としてGPSクロック信号を受信するか、又は、ローカルな原子時計が同様のクロック信号を提供する。情報へのアクセスが試みられているときに、クロック信号によって実際の時間に基づいた情報へのアクセスが制御可能になる。例えば、製作者は、(1)所定の日/時の前、(2)所定の日/時の後、又は、(3)所定の日/時の期間の間だけアクセスが許されるように指定することができる。

【0021】ユーザがキーボード50から入力するパスワード130によって、製作者はファイル141、142及び143とリスト150及び154の特定のアイテムとを関連付けることができる。パスワード130は、複数のアクセスに有効なユーザ・パスワード、又は1回限りのパスワードであってもよい。または、製作者は、ポリシー・ファイル152によってリスト150及び154の特定の地理的領域/日/時の情報とファイル141、142及び143とを関連付けることができる。有効なユーザ・パスワード130は、一つ以上のポリシー・ファイル152のロックを解除するものであってもよい。ユーザの実際の地理的位置及び現在の日付及び時間がユーザ・パスワード150に対応する許可された地理的領域及び許可された日/時内である場合、ユーザはユーザ・インタフェース95を介して選択したファイルに

アクセスすることができる。次に、選択された情報は出力装置40上に表示される。

【0022】表1は、1例として、CD-ROM35に格納され、対応する許可された地理的領域及び日/時と関連付けられた5つの暗号化済みファイルAないしFにどのようにアクセスすることができるかを示している。各ファイルは、4つの異なるファイル解読鍵K1ないしK4のうちの1つと関連付けられている。L1及びL2は2つの異なる許可された地理的領域であり、T1、T2及びT3は3つの異なる許可された日/時の期間である。ファイル解読鍵K1（例えば、パスワード）を所有するユーザは、時刻T1において地理的領域L1及びL

3内のマニュアルAを解読することができる。同じユーザは、また、領域L2及びL3内で同一の時刻T1においてマニュアルDを解読することができるが、領域L1内では解読できない。同様に、鍵K2を有するユーザは、領域L2内で画像B及び画像Eを解読できるが、同じ時刻では解読できない。図面Cは、時刻T3ではいかなる位置においても解読することができるが、業務報告書Fは鍵K4を必要とし、領域L1内であればいつでも解読することができる。

【0023】

【表1】

暗号化されたファイル	ファイル解読鍵	許可された地理的領域	許可された日/時の期間
マニュアルA	K1	L1, L3	T1
画像B	K2	L2	T1, T3
図面C	K3	--	T3
マニュアルD	K1	L2, L3	T1
画像E	K2	L2	T2
報告書F	K4	L1	--

図3に示すように、任意の暗号による暗号署名のために、製作者はCD-ROM35に書くべきソース・ファイル144'を選択し、許可された地理的領域150'のリスト及び許可された日時の期間154'のリストを指定する。製作者は、各ファイル又はファイル・サブセットをゼロ又は1つ以上の地理的領域150'、及びゼロ又は1つ以上の日時の期間154'と関連付けて（表1参照）、この関連付けをポリシーファイル152'に格納する。ファイル144'、150'、152'、154'の各々は、ステップ53、340、350及び360において対応する暗号鍵51、345、355及び365によって署名、暗号化される。対応する暗号化されたファイル150、152及び154は、署名、暗号化された領域/時間/ファイルアクセス・ポリシー155として格納される。上述した如く、署名/暗号化されたファイル144、署名/暗号化された対称ファイル解読キーファイル146、及び製作者がCD-ROM35全体に署名するために用いられる署名147もまたCD-ROM35に格納される。

【0024】図4及び図5に示すように、署名/暗号化ファイル144にアクセスするために、ユーザは製作者からパスワード130（図2）を得て（ステップ400）、キーボード50からパスワード130を入力する（ステップ410）。パスワード130は1回限りの（ワンタイム）パスワードであると仮定される。但し、複数のセッションに有効なユーザ・パスワードを用いる

こともできる。

【0025】図4に示すように、レベル1及びレベル2に関するプロセス・フローの初期の部分はほとんど同一である。ステップ420においてパスワード130をチェックし、システム構成に従い、ステップ440（レベル1の場合、追加のセキュリティなし）又はステップ450（レベル2の場合、受信機/CD-ROMドライブのセキュリティ有り）を実行する。図5に示されるステップ440及びステップ450の詳細について以下に説明する。

【0026】図5に示すように、プロセス440において、ユーザのパスワード130はデバイス・ドライバ72に送られる（ステップ510）。デバイス・ドライバ72は、ワンタイム・パスワード130に応答して、それ自身のワンタイム・パスワードをユーザ・パスワード130から生成し（ステップ520）、ユーザが実際に正しいワンタイム・パスワード130を入力したことを検証し（ステップ530）、ユーザにインタラクティブ・セッションを認証する（ステップ532）。さもなければ、アクセスは拒否される（ステップ535）。

【0027】一度、パスワード130によってユーザが認証されると、デバイス・ドライバ72は現在の位置及び日/時を受信機70に問い合わせる（ステップ540）。次に、デバイス・ドライバ72は、受信機70から戻された時間及び位置データと、ファイル144又はファイル・サブセット141、142及び143に適用

するポリシー155を比較する(ステップ460)。ユーザがファイル144へのアクセスを許可されると、次に、データは解読鍵52によってロックが解かれて(ステップ470、図3)解読され(ステップ480)、ユーザのアプリケーション・プログラム34に供給され表示される(ステップ490)。

【0028】レベル2のシステムにおいて、受信機70は、以下において「暗号ボード」と称される暗号の受信機ボード80を含む。前述のように、暗号ボード80はメッセージの署名及び暗号化/解読を行うことができる。CD-ROMドライブ30は、暗号ボード80により署名され暗号ボード80から受信される位置データを復号するためのデコーダ32を含む。

【0029】図5に示すように、プロセス450において、ユーザ・パスワード130は、パスワード130を受付けそれを変更せずにデコーダ32に渡すデバイス・ドライバ72に送られる(ステップ550)。次に、ドライバ32は、ユーザ・パスワードに対応するそれ自身のワンタイム・パスワードを秘密鍵86によって内部で生成し(ステップ560)、正しいパスワード130がデバイス・ドライバ72に送信されたことを検証し(ステップ570)、ユーザにインタラクティブ・セッションを認証する(ステップ572)。さもなければ、アクセスは拒否される(ステップ575)。

【0030】一度、暗号回路32がユーザを認証すると、ドライバ32はデバイス・ドライバ72を介して暗号ボード80に受信機70からの現在の時刻及び位置情報について問い合わせる(ステップ580)。デコーダ装置30は、暗号ボード80に「初期化ベクトル」、すなわち、デバイス・ドライバ72が時間及び位置についての要求とともに暗号ボード80に渡す位置オフセットを形成する(ステップ590)ための署名されたランダム又は他のビット・パターンを供給する(ステップ590)。

【0031】暗号ボード80は、現在の時刻及び緯度、経度、高度による実際の地理的位置を含む予め確立されたデータ・フォーマットに応じたパケットを準備することによって応答する(ステップ600)。また、計算に必要な他のデータと同様に位置データを送信する衛星の識別情報が含まれていてもよい。暗号ボード80は、また、供給された初期化ベクトルをパケット内に既知のオフセットで格納し、パケット内容に暗号署名を適用する。暗号の署名は、例えば、メッセージ・ダイジェスト/パケット・データの寄せ集め(ハッシュ)、さらにある所定鍵によるメッセージ・ダイジェストの暗号であってもよく、あるいは暗号ボード80に格納された証明又は鍵に応じて対称又は非対称であってもよい。

【0032】次に、暗号ボード80は、パケットをデコーダ32/CD-ROMドライブ30に中継するデバイス・ドライバ72に署名された時間/位置パケットを送

信する(ステップ605)。デコーダ32は、暗号ボード80から受信したパケットの署名をデコーダ32に格納された署名と比較する(ステップ610)。その署名が適切に検証されると(ステップ620)、パケット内の初期化ベクトルが調べられ、ステップ590においてデコーダ32が暗号ボード80に実際に供給した初期化ベクトルと同一の初期化ベクトルであるかを確定する。これが本当ならば、デコーダ32が受信したパケットは最近のもので真性なものであり、時間及び位置データは有効であるとして受け付けられる。

【0033】一度、暗号ボード80からのパケットが署名及び初期化ベクトルに基づいて許可されると、デコーダ32は、暗号ボード80から受信した時間及び位置データをファイル144又はファイル・サブセット144に適用されるポリシー155と比較する(ステップ460)。ユーザがファイル144へアクセスすることが許可されると、データのロックは解かれ(ステップ470)、解読鍵52により解読されて(ステップ480)、ユーザ・アプリケーション・プログラム34に供給され表示される(ステップ490)。

【0034】他の実施例は、特許請求の範囲内である。例えば、GPS受信機は正確にデータ配布媒体読取装置の位置に配置されている必要はなく、読取装置に対して既知の位置(例えば、建物のローカルエリア・ネットワークにコンピュータ・サービスを提供するコントロール・サーバを含む部屋など)に配置されていればよい。また、ポリシー・ファイル152'は、一定のファイル144に対するアクセスが拒否される地理的領域を指定してもよい。

【0035】ファイルに対するアクセスの制限は、製作者によりキーボードから入力されるパスワードに限定されない。例えば、顔の特徴、指紋及び/又は声紋などの一定の生物測定学的属性をパスワードに加えて、又はパスワードの代りに用いてもよい。

【図面の簡単な説明】

【図1】コンピュータ・システムの斜視図である。

【図2】格納情報へのアクセスを制御するコンピュータベースのシステムのブロック図である。

【図3】フローチャートである。

【図4】フローチャートである。

【図5】フローチャートである。

【図6】暗号の構成要素を示すブロック図である。

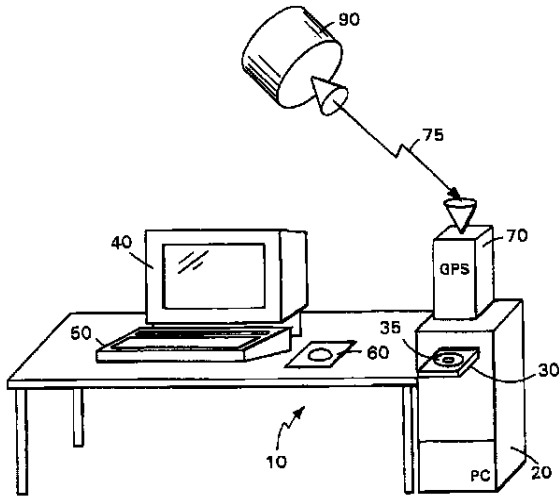
【主要部分の符号の説明】

- 10 コンピュータ・システム
- 20 コンピュータ
- 32 デコーダ
- 35 データ配布媒体
- 70 GPS受信機
- 80 暗号ボード
- 81 証明書

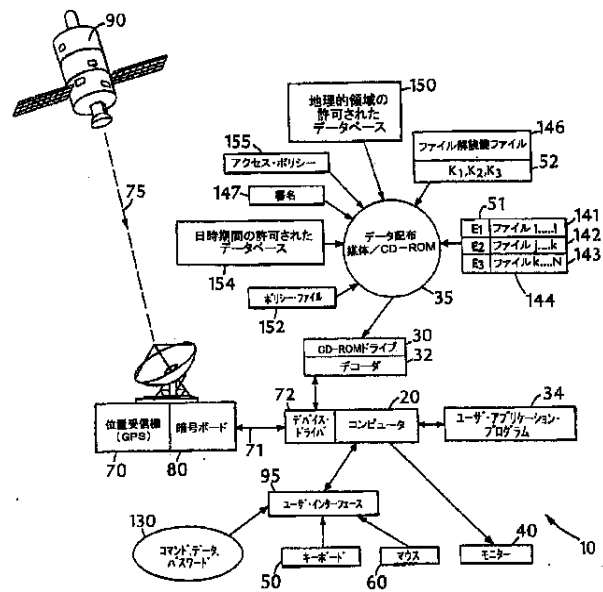
- 82 秘密鍵
- 83 暗号ボード公開鍵証明
- 84 製作者証明
- 86 配布媒体ポリシー解読鍵
- 90 GPS衛星

- 144 情報ファイル
- 146 ファイル解読鍵ファイル
- 147 配布媒体の署名
- 155 アクセス・ポリシー

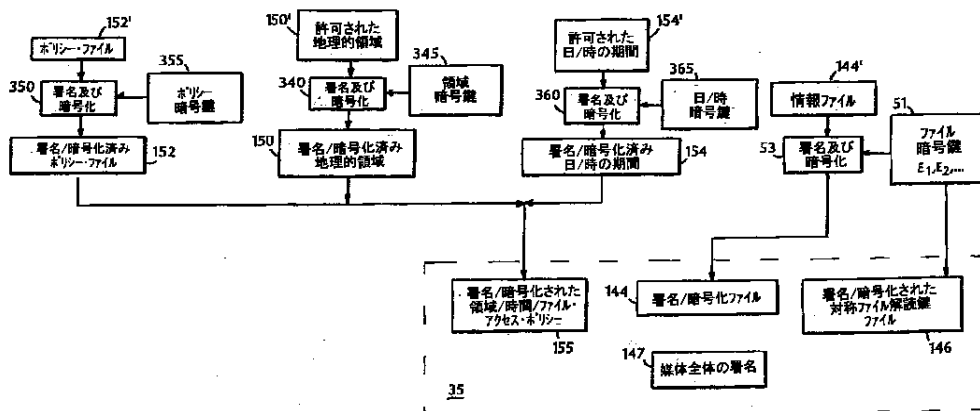
【図1】



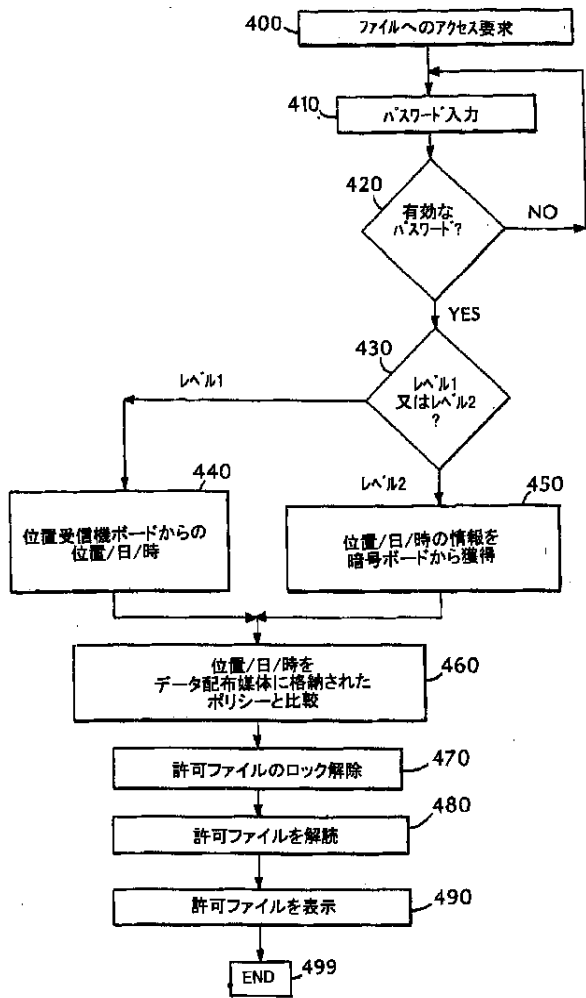
【図2】



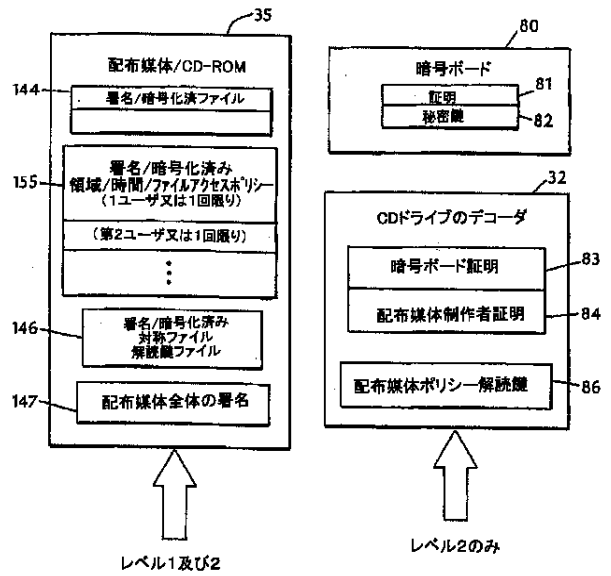
【図3】



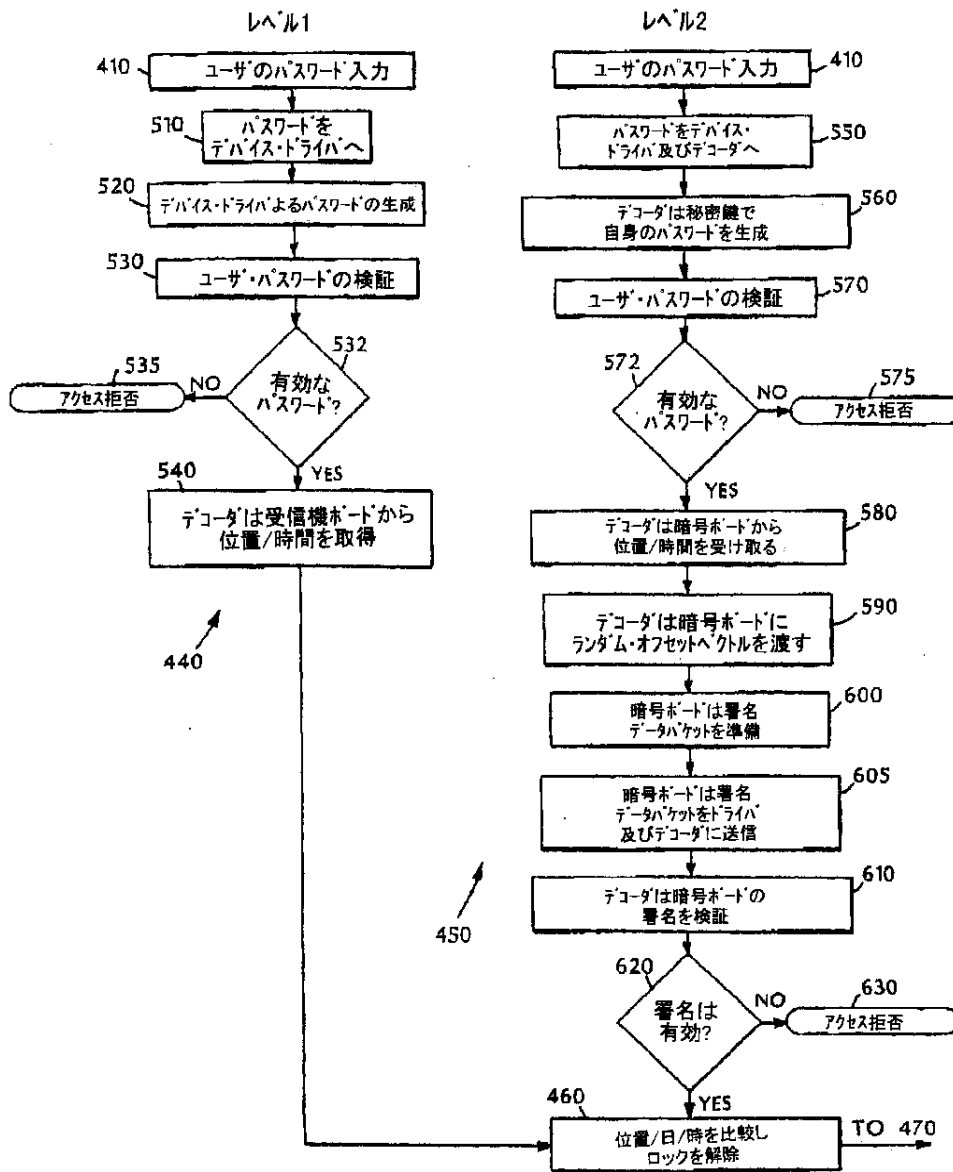
【図4】



【図6】



【図5】



フロントページの続き

(51)Int.Cl.⁷
H04L 9/14

識別記号

F I
H04L 9/00

テマコード(参考)

641

(72)発明者 マイケル イー. マックニール
アメリカ合衆国 カリフォルニア州
95018 フェルトン ロストエイカードラ
イブ 1271

(72)発明者 トッド エス. グラッシィ
アメリカ合衆国 カリフォルニア州
95066 スコッツバリー ブルーボネット
レーン 109エイ

(72)発明者 ジェラルド エル. ウィレット
アメリカ合衆国 マサチューセッツ州
02148 マルデン#1 ハーバードストリ
ート 189