

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4034653号
(P4034653)

(45) 発行日 平成20年1月16日(2008.1.16)

(24) 登録日 平成19年11月2日(2007.11.2)

(51) Int. Cl.	F I
H O 4 L 9/08 (2006.01)	H O 4 L 9/00 G O 1 C
	H O 4 L 9/00 G O 1 E

請求項の数 41 (全 30 頁)

(21) 出願番号	特願2002-556356 (P2002-556356)	(73) 特許権者	503161028
(86) (22) 出願日	平成14年1月10日(2002.1.10)		ゲオコデックス・エルエルシー
(65) 公表番号	特表2004-528739 (P2004-528739A)		アメリカ合衆国、カリフォルニア州 9 1
(43) 公表日	平成16年9月16日(2004.9.16)		4 3 6 - 1 7 6 3、エンシーノ、スイート
(86) 国際出願番号	PCT/US2002/000956		3 0 1、ペントウーラ・プールバード
(87) 国際公開番号	W02002/056162		1 6 8 6 1
(87) 国際公開日	平成14年7月18日(2002.7.18)	(74) 代理人	100058479
審査請求日	平成16年12月9日(2004.12.9)		弁理士 鈴江 武彦
(31) 優先権主張番号	09/758,637	(74) 代理人	100091351
(32) 優先日	平成13年1月10日(2001.1.10)		弁理士 河野 哲
(33) 優先権主張国	米国 (US)	(74) 代理人	100088683
			弁理士 中村 誠
		(74) 代理人	100108855
			弁理士 蔵田 昌俊

最終頁に続く

(54) 【発明の名称】 デジタル情報をジェオロックし、機密保護するための暗号化システムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

特定の地理的領域を識別する位置識別属性を検索する機能と、

特定の地理的領域の位置を識別せずに、特定の地理的領域の中の全ての座標を共通値に写像する位置識別属性から形状パラメータを導出する機能と、

位置識別属性と形状パラメータを入力として使用して暗号化キーを生成する機能と、

暗号化キーを使用してデジタル情報を暗号化する機能と、

形状パラメータと暗号化されたデジタル情報を送信する機能と

をプロセッサに実行させるように動作するソフトウェア命令を記憶するように構成されたメモリを有しているプロセッサを含んでいる第1の情報処理装置と、

形状パラメータと暗号化されたデジタル情報を受信する機能と、

第2の情報処理装置の現在位置を決定する機能と、

現在位置と形状パラメータを入力として使用して解読キーを生成する機能と、

解読キーを使用してデジタル情報を解読する機能と

をプロセッサに実行させるように動作するソフトウェア命令を記憶するように構成されたメモリを有しているプロセッサを含んでいる第2の情報処理装置とを備えており、

前期位置識別属性は、地理的領域の中の固有位置を識別する位置値と固有位置を囲むエリアを識別する近接値を含んでおり、前記解読キーは、現在位置が特定の地理的領域の中にある場合には暗号化キーと一致し、前記デジタル情報は、解読キーが暗号化キーと一致する場合にのみ解読されることが出来るデジタル情報へのアクセスを制御するシステム。

10

20

【請求項 2】

導出する機能は、式： $f(x) = \text{int}(x / \text{境界})$ に従うマッピング関数 $f(x)$ をさらに含んでおり、 x は、位置値の対応する緯度または経度であり、 境界 は、境界をなす緯度または経度間の辺の長さであり、 int は、 $x / \text{境界}$ の整数部分を戻す関数である請求項 1 記載のシステム。

【請求項 3】

近接値は、境界を付けられた方形エリアを規定する請求項 1 記載のシステム。

【請求項 4】

近接値は、円形の境界を付けられたエリアを規定する請求項 1 記載のシステム。

【請求項 5】

暗号化キーを生成する機能は、位置値と形状パラメータを入力として使用して初期キーを生成する機能をさらに含んでいる請求項 1 記載のシステム。

10

【請求項 6】

暗号化キーを生成する機能は、暗号化キーを算出するために初期キーを変換する機能をさらに含んでいる請求項 1 記載のシステム。

【請求項 7】

位置値は、固有位置のために緯度および経度測定をさらに規定する請求項 1 記載のシステム。

【請求項 8】

位置値は、固有位置のために高度測定をさらに規定する請求項 1 記載のシステム。

20

【請求項 9】

第 2 の情報処理装置によって実行される位置を決定する機能は、第 2 の情報処理装置のために街路アドレスから位置を解く機能をさらに含んでいる請求項 1 記載のシステム。

【請求項 10】

第 2 の情報処理装置によって実行される位置を決定する機能は、第 2 の情報処理装置のメモリの中に記憶されているファイルから位置を検索する機能をさらに含んでいる請求項 1 記載のシステム。

【請求項 11】

第 2 の情報処理装置は、GPS 受信機をさらに備えており、第 2 情報処理装置によって実行される位置を決定する機能は、GPS 受信機によって受信される信号から位置を復元する機能をさらに含んでいる請求項 1 記載のシステム。

30

【請求項 12】

第 2 の情報処理装置によって実行される位置を決定する機能は、第 2 の情報処理装置によって受信される RF 信号を三角測量することによって（現在）位置を復元する機能をさらに含んでいる請求項 1 記載のシステム。

【請求項 13】

第 2 の情報処理装置は、特定の地理的位置でのみソフトウェアアプリケーションによってデジタル情報へのアクセスを許可する機能をさらに実行する請求項 1 記載のシステム。

【請求項 14】

第 2 の情報処理装置は、特定の地理的位置でのみメモリからデジタル情報の検索を許可する機能をさらに実行する請求項 1 記載のシステム。

40

【請求項 15】

第 2 の情報処理装置は、特定の地理的位置でのみデジタル情報のビジュアル表示を許可する機能をさらに実行する請求項 1 記載のシステム。

【請求項 16】

第 1 の情報処理装置は、形状パラメータを暗号化されたデジタル情報に付加する機能をさらに実行する請求項 1 記載のシステム。

【請求項 17】

第 2 の情報処理装置によって実行される受信する機能は、付加された形状パラメータを復元する機能をさらに含んでいる請求項 1 記載のシステム。

50

【請求項 18】

第2の情報処理装置によって実行される受信する機能は、形状パラメータと暗号化されたデジタル情報を第1の情報処理装置から受信する機能をさらに含んでいる請求項1記載のシステム。

【請求項 19】

第1の情報処理装置は、形状パラメータと暗号化されたデジタル情報を第2の情報処理装置に伝送する機能をさらに実行する請求項1記載のシステム。

【請求項 20】

特定の地理的領域を識別する位置識別属性を検索する機能と、
 特定の地理的領域の位置を識別せずに、特定の地理的領域の中の全ての座標を共通値に
 10 写像する位置識別属性から形状パラメータを導出する機能と、
 位置識別属性と形状パラメータを入力として使用して暗号化キーを生成する機能と、
 暗号化キーを使用してデジタル情報を暗号化する機能と、
 形状パラメータと暗号化されたデジタル情報を受信者に送信する機能と
 をプロセッサに実行させるように動作するソフトウェア命令を記憶するように構成された
 メモリを有しているプロセッサを備えており、
 前期位置識別属性は、地理的領域の中の固有位置を識別する位置値と固有位置を囲むエリ
 アを識別する近接値を含んでおり、暗号化されたデジタル情報は、特定の地理的領域の中
 に設置され形状パラメータへのアクセスができる受信者装置によってのみ解読される情報
 20 処理装置。

【請求項 21】

導出する機能は、式： $f(x) = \text{int}(x / \text{boundary})$ に従うマッピング関数 $f(x)$ をさらに含んでおり、 x は、位置値の対応する緯度または経度であり、 boundary は、境界をなす緯度または経度間の辺の長さであり、 int は、 $x / \text{boundary}$ の整数部分を戻す関数である請求項20記載の情報処理装置。

【請求項 22】

近接値は、境界を付けられた方形エリアを規定する請求項20記載の情報処理装置。

【請求項 23】

近接値は、円形の境界を付けられたエリアを規定する請求項20記載の情報処理装置。

【請求項 24】

暗号化キーを生成する機能は、位置値と形状パラメータを入力として使用して初期キーを生成する機能をさらに含んでいる請求項20記載の情報処理装置。

【請求項 25】

暗号化キーを生成する機能は、暗号化キーを算出するために初期キーを変換する機能をさらに含んでいる請求項20記載の情報処理装置。

【請求項 26】

近接値は、方形領域、多角形領域、円形領域、楕円形領域の少なくとも1つを規定する請求項20記載の情報処理装置。

【請求項 27】

特定の地理的領域は、郵便番号、州、市、群、電話加入区域コード、国の少なくとも1
 40 つを含んでいる請求項20記載の情報処理装置。

【請求項 28】

受信する機能は、時間値を受信する機能をさらに含んでいる請求項20記載の情報処理装置。

【請求項 29】

位置値は、特定の地理的領域のために緯度および経度測定をさらに規定する請求項20記載の情報処理装置。

【請求項 30】

プロセッサは、形状パラメータを暗号化されたデジタル情報に付加する機能をさらに実行する請求項20記載の情報処理装置。

【請求項 3 1】

プロセッサは、暗号化されたデジタル情報を適切な記憶媒体に記憶する機能をさらに実行する請求項 2 0 記載の情報処理装置。

【請求項 3 2】

位置識別属性と形状パラメータを入力として使用して生成された暗号化キーを使用して暗号化されたデジタル情報を受信する機能と、

形状パラメータを受信する機能と、

情報処理装置の現在位置を決定する機能と、

現在位置と形状パラメータを入力として使用して解読キーを生成する機能と、

解読キーを使用してデジタル情報を解読する機能と

10

をプロセッサに実行させるように動作するソフトウェア命令を記憶するように構成されたメモリを有しているプロセッサを備えており、

前期位置識別属性は特定の地理的領域を識別し、前期位置識別属性は地理的領域の中の固有位置を識別する位置値と固有位置を囲むエリアを識別する近接値を含んでおり、形状パラメータは特定の地理的領域の位置を識別せずに、特定の地理的領域の中の全ての座標を共通値にマッピングし、前記解読キーは、現在位置が特定の地理的領域の中にある場合には暗号化キーと一致し、前記デジタル情報は、解読キーが暗号化キーと一致する場合にのみ解読されることができると、情報処理装置。

【請求項 3 3】

位置値は、特定の地理的位置のために緯度および経度測定をさらに規定する請求項 3 2 記載の情報処理装置。

20

【請求項 3 4】

位置値は、特定の地理的位置のために高度測定をさらに規定する請求項 3 2 記載の情報処理装置。

【請求項 3 5】

位置を決定する機能は、情報処理装置のために街路アドレスから位置を解く機能をさらに含んでいる請求項 3 2 記載の情報処理装置。

【請求項 3 6】

位置を決定する機能は、情報処理装置のメモリの中に記憶されているファイルから位置を検索する機能をさらに含んでいる請求項 3 2 記載の情報処理装置。

30

【請求項 3 7】

G P S 受信機をさらに備えており、位置を決定する機能は、G P S 受信機によって受信される信号から位置を復元する機能をさらに含んでいる請求項 3 2 記載の情報処理装置。

【請求項 3 8】

位置を決定する機能は、情報処理装置によって受信される R F 信号を三角測量することによって位置を復元する機能をさらに含んでいる請求項 3 2 記載の情報処理装置。

【請求項 3 9】

プロセッサは、特定の地理的位置でのみプロセッサによってデジタル情報へのアクセスを許可する機能をさらに実行する請求項 3 2 記載の情報処理装置。

【請求項 4 0】

40

プロセッサは、特定の地理的位置でのみメモリからデジタル情報の検索を許可する機能をさらに実行する請求項 3 2 記載の情報処理装置。

【請求項 4 1】

プロセッサに有効に結合されているビジュアル表示モニタを備えており、プロセッサは特定の地理的位置でのみビジュアル表示モニタにデジタル情報のビジュアル表示を許可する機能をさらに実行する請求項 3 2 記載の情報処理装置。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、デジタル情報の通信に関し、とくに、位置保全属性を使用してデジタル情報

50

を暗号化する方法およびシステムに関する。

【背景の技術】

【0002】

コンピュータ、通信およびネットワークテクノロジーの急速な進歩により、数年前には不可能だった新しい機会やアプリケーションがどっと雪崩のように可能になってきている。これらの進歩は、インターネットの爆発的な普及によって例証される。技術的に知られているように、インターネットは、あらゆる種類のコンピュータが互いに通信し、情報を共用することを可能にするコンピュータネットワークの相互接続である。あらゆる規模の企業、個人、政府機関、慈善団体および学術センターがインターネットを常に使用して情報を共用し、サービスを配信し、広範囲にわたってコンテンツを交換している。インターネットは、何れの機関からも制御されず管理もされないシステムの分布形ネットワークとして機能する。情報の交換を容易にする物理的および論理的通路がこれらのネットワークを互いに結び付けている。

10

【0003】

この情報アクセスが社会にもたらされたことには非常に高い価値があるにもかかわらず、機密性、本物であること、完全性、無許可の使用、取引の秘密保持、サイトの保護等を含む情報のセキュリティの制御は重要な問題として残されている。インターネットの著しい開放性のために、その情報が保護されていることを確実に知ることが非常に困難なものとなる。その結果、インターネットのユーザは彼らが送信または受信したデータの真実性または使用に関して何等仮定を行わないに違いない。

20

【0004】

この問題の根源は、インターネットの固有の構成に由来する。インターネットがその基礎を置くTCP/IPプロトコルの目的は、ネットワーク中においてデータパケットがとる経路を指図することなく、そのインターネットに接続された任意のコンピュータ間において情報のパケットを単に配信することである。コンピュータおよび基本的なインターネットソフトウェアを有する誰もが十分に有能なホストとしてインターネットに接続し、インターネットサービスを別のユーザに提供することができる。インターネットを横断した情報はその通路に沿った多くのコンピュータを通過し、各コンピュータはその情報にアクセスすることができる。インターネットに対する新しいネットワーク接続（広域携帯電話、ブロードバンドケーブル、レーザおよびマイクロ波ネットワーク等）が普及されるため、将来的にこの問題は悪化し続けるであろう。

30

【0005】

情報セキュリティおよびアクセス制御を歴史的に行ってきた暗号システムは、インターネットの成長に遅れをとっている。暗号化システムにおいて、送信側は暗号化アルゴリズムを使用して元のデータ、または“平文”を、“暗号テキスト”と呼ばれる符号化された等価なものに変換する。その後、暗号テキストは受信機によって復号（または解読）され、それによって平文に戻されることができる。暗号化アルゴリズムは、典型的に長さが40乃至128ビットの2進数であるキーを使用する。キー中のビット数が大きくなると、それだけ一層キーの組合せが可能になり、そのコードを解明するのに要する時間が長くなる。データは、キーの中のビットを数学的にデータビットと組合せることにより暗号化され、あるいは“ロック”される。受信端においては、コードを“ロック解除”して、元のデータを復元するためにこのキーが使用される。

40

【0006】

インターネットの前に、暗号法は主に、送信者および受信者の両者が秘密キー（対称キーとしても知られている）を使用して平文の暗号化および解読を行う秘密キーシステムに依存していた。セキュリティは秘密キーを知っている送信者および受信者に依存しており、政府および大企業がその機密情報を保護するのに十分であることが証明されている。秘密キーシステムは、主として危険にさらすことなくユーザに秘密キーを分配することが困難であるために、インターネット上における情報トラフィック量へのアクセスの制御にはあまり効果的ではない。

50

【 0 0 0 7 】

このような専用キーシステムに代わるものは、専用キーおよび公開キーとして知られている2つのキーを使用する公開キー暗号法である。各パーティは、秘密を保持されて共有されない専用キーと、公に利用可能にされている公開キーとを有している。公開キーは平文情報を暗号化するために使用され、専用キーは暗号文メッセージを解読するために使用される。専用キーは、公開キーから数学的に導出されてはならない。通信を行っているパーティは、インターネットのような機密保護されていない通信チャンネルによって彼等の公開キーを交換し、その後彼等のメッセージを暗号化するために公開キーを使用してもよい。その後、受信者はそのメッセージを解読するために専用キーを使用する。それでもなお、公開キー暗号法に関する欠点は残っている。公開キー暗号化は計算が集中的なものであり、したがって使用に時間がかかる。いくつかの推測によれば、公開キーシステムは典型的にそれらの対応した専用キーより100倍遅く、したがってそれらは計算集中的な圧縮/圧縮復元もまた行われなければならないオーディオおよびビデオシステムに対して実際的ではない。公開キーの分配により別の問題が発生し、それによって公開キーにアクセスしてその妥当性を検査する中央化された登録または署名機関として機能する企業（たとえば、Verisign社）を大きく成長させる。このような欠点を考慮して、公開キー暗号化はインターネット通信全体のごく僅かな部分に対してのみ使用されている。大部分のこのような通信に対しては、セキュリティ問題は公開キー管理の不便さおよび費用を是認するほど深刻なものではないようである。

10

【 0 0 0 8 】

これらの欠点のいくつかを克服している公開キー暗号法の1つの形態は、“非常に優れた機密”を意味するPGPである。PGPにより、個人は互いのキー証明書に署名することが可能になり、それによって中央型署名機関に頼らなくなる。PGPはますます容認されてきているが、キー分配および管理が困難であるために、それは依然としてインターネットトラフィックの一部に対してしか使用されていない。したがって、インターネット上での暗号化の広範囲にわたる使用は、それがユーザにとって透明に思える方式で実施された場合にのみ広く受入れられるであろう。

20

【 0 0 0 9 】

通信システムに対する別の重要な考慮事項は、著作権保護されたデジタルコンテンツの無許可コピーの防止である。通常の計算および通信システムに関して、良心を欠いた者はデジタル形態の著作権のある作品（たとえば、音楽、著作物、写真、ビデオ、ソフトウェア等）の無数の同一コピーを容易に作成して分配することができる。さらに、商業的に利用可能なファイル指標付けサービスにより、コンピュータユーザは別のユーザのコンピュータシステム上のデジタルファイルの位置を突き止め、それにアクセスすることが容易に可能となり、それによって広範囲に及ぶ著作権侵害の可能性が著しく増加している。Napster社（San Mateo, CA）によって提供されている1つのこのようなサービスは、現在インターネットにログオンされている別のコンピュータ上に存在する一般的なMP3フォーマットの音楽ファイルの位置を突き止めるようにNapsterウェブサイトと共同して動作するファイル共用アプリケーションを提供する。グヌーテラ（Gnutella）として知られている同様のサービスは、種々の情報が世界全体で利用可能なものにするユーザおよび組織のゆるやかな自由な連合体であるグヌーテラ・ネット上のソフトウェアおよびドキュメントをユーザがサーチすることを可能にするファイル共用システムを提供する。グヌーテラは、音楽ファイル用に調整され、中央化されたリスティングを与えるナプスター（Napster）とは異なり、グヌーテラ・ネットは、全ての種類のファイルを含むピア・ツー・ピアネットワークである。これらのファイル共用システムはまた、著作権保護されていないファイルをユーザが共用することを可能にする際はその目的は合法的なものであるが、それらはまた著作権法に違反して著作権保護されたファイルを手に入れるために広く使用されている。これらのファイル共用システムの違法使用は、著作権の所有者に対する深刻な脅威を表す。

30

40

【 0 0 1 0 】

50

インターネットの積極的な保安管理は、著作権保有者にとって有効なソリューションではない。インターネットの著作権侵害の広範囲で匿名の性質を仮定すると、このような管理努力は論理的に困難である。さらに、インターネット上で交換される情報コンテンツは自由でなければならないという世論のために、大規模な保安管理努力は公的関係の観点から魅力のないものになる。この問題を解決するために、予防措置に焦点を合わせることによって配布されるデジタルコンテンツの著作権を保護する種々のデジタル権利管理(DRM)システムが生成されてきた。たとえば、Secure Digital Music Initiative(SDMI)として知られているレコード産業向けに提案されたDRMシステムは、デジタル音楽をインターネットによって安全に配布するための1組のルールを明らかにしている。SDMIは、ソフトウェアおよびハードウェアのプレーヤがマテリアルを再生するためにサポートしなければならないコンテナフォーマットを含むコンプライアントなDRMシステムを開発するためのガイドラインを提供している。SDMIは米国レコード産業協会(RIAA)ならびにソニー、ワーナー、BMG、EMIおよびユニバーサルの上位5社の音楽製作会社により支援されることが1999年2月に発表された。

10

【0011】

これらの努力にもかかわらず、DRMシステムはいくつかの理由のためにせいぜい不完全なソリューションしか提供しない。第1に、インターネット上で著作権侵害されたコンテンツの利用可能性を仮定すると、通常の売買経路を介してマテリアルのコピーを合法的に購入するよりもインターネットによってデジタルファイルを違法にダウンロードするほうが、ユーザにとってははるかに便利で廉価である。違法に入手したマテリアルは合法的なコピーと比較して品質は低いかもしれないが、便利さおよびごく僅かな費用がこの欠点を補償することが多い。第2に、大部分のDRMテクノロジーは、デジタル情報を保護するためにある形態の暗号化に依存している。非常に有効であるために、暗号化方式に関する利害関係者は共に暗号化された情報の秘密を保持する利権を有していなければならない。コンテンツの法的購入者はそのコンテンツを見る権利を有しているが、暗号化によって与えられる秘密が確実に保持されるようにする利権は有しない。このために、多くのDRMソリューションにおいて、暗号解読キーをユーザから隠蔽しようと試みるデジタル証明書またはライセンスが使用される。このようなシステムでは、コンテンツの全てのコピーは同じ方法で暗号化され、メディアプレーヤーは解読されたコンテンツを表示するか、あるいは再生するためにユーザの権利の妥当性を検査する。しかしながら、暗号化されたコンテンツおよび暗号解読キーは隠蔽されているにもかかわらず、ユーザはそれにアクセスすることが可能であるため、高度な知識を有するユーザは、DRMソリューションを逆処理してその暗号化を解読し、それによって解読されたコンテンツを何等妨害を受けずにコピーして配布することができる。これより技術的に劣るが、コンテンツの暗号化されていないコピーを入手する別の方法、たとえば、コンテンツが再生中に合法的に表示されているときにそのデジタルビデオデータファイルの各フレームをビデオテープ撮りする等もまた、良心のないユーザが利用することが可能である。

20

30

【発明の開示】

【発明が解決しようとする課題】

40

【0012】

したがって、これらおよびその他の欠点を克服したデジタル情報交換の制御方法を提供することが非常に望ましい。とくに、セキュリティおよび情報へのアクセスに対する制御を可能にすると共に著作権保護されたコンテンツの無許可コピーを阻止する情報交換システムおよび方法を提供することが望まれている。

【課題を解決するための手段】

【0013】

本発明によるデジタル情報へのアクセスを制御する方法および装置は、特定の地理的位置を規定する位置識別属性を使用する。位置識別属性は、その特定の地理的な位置でのみデジタル情報がアクセスされることができるようこのデジタル情報に関連付けられてい

50

る。位置識別属性はさらに位置値と近接値とを含んでいる。位置値はデジタル情報の予定された受信アプライアンスの位置に対応し、緯度、経度および高度ディメンションに関してさらに規定されることができる。近接値は、その位置を囲むゾーンに対応している。位置識別属性はさらに、特定の地理的な位置および特定の時間期間中にのみデジタル情報がアクセスされることができるように、時間値を含んでいてもよい。

【0014】

本発明の1実施形態において、デジタル情報は位置識別属性に基づいたジェオロック (geolocking) キーを使用して暗号化され、解読される。このジェオロックキーは位置識別属性から決定される形状パラメータに基づいており、暗号化されたデジタル情報と共に含まれている。形状パラメータは地理的エリアの形状を記述しているが、しかしその地理的エリアがどこに位置しているかは識別しない。暗号化されたデジタル情報を受取ったアプライアンスは、受取られた形状パラメータおよびそのアプライアンス位置に基づいてデジタル情報を解読するためのジェオロックキーを生成することができる。アプライアンス位置が位置識別属性の近接エリア内にない場合、そのアプライアンスはデジタル情報を解読するためのジェオロックキーを生成することができない。したがって、位置識別性は、特定の地理的位置のみでのデジタル情報の解読を可能にすることにより強化される。

【0015】

以下の好ましい実施形態の詳細な説明を考慮することにより、当業者はデジタル情報へのアクセスを制御するために位置識別性を使用するシステムおよび方法をさらに完全に理解し、その付加的な利点および目的を認識するであろう。この明細書の最後に添付され簡単な説明が示されている図面を参照とする。

【発明を実施するための最良の形態】

【0016】

本発明は、情報に対するセキュリティおよびアクセスに対する制御を可能にすると共に著作権保護されたコンテンツの無許可コピーを阻止するデジタル情報交換制御方法に対する必要性を満足させるものである。以下の詳細な説明において、1以上の図面に示されている同じ構成要素を表すために同じ構成要素符号が使用されている。この詳細な説明では、以下を含む種々の用語が使用されている。

【0017】

アプライアンス：デジタル情報および位置情報を獲得するための最小容量を備えた電子デバイス、システム、ネットワーク、およびそれに類似したもの。これらの電子デバイスは、プログラム命令を実行するための処理機能、および短期および長期データ記憶用のメモリ容量を含んでいることが多く、さらに情報を送信する能力を含んでいてもよい。

【0018】

位置識別属性を関連付ける：デジタル情報に位置識別属性をマークする方法。

【0019】

座標系：位置は、地球上の任意の位置を特有に識別する程度に基づいた座標系である緯度および経度によって示される。緯度は地球の赤道 (0°) から北極 (90°北) または南極 (90°南) までの角度として測定される。緯度線は、赤道平面と平行に走る円により形成される。全ての整数の緯度線は互いから等距離である。ある位置の緯度は、赤道平面と地球の中心から投影された線との間の角度の尺度である。経度線は、北極および南極の両者と交差する大きい円により形成される。各経度は地球を半分に分けて考えることができる。経度は、英国のグリニッジの王立グリニッジ天文台から東に0°から180°までおよび西に0°から180°までの半分の円で測定される。0°の経度線は本初子午線と呼ばれている。ある位置の経度は、その大きい円により形成された平面と本初子午線との間の角度の尺度である。この詳細な説明において、メリーランド内の位置に対する緯度および経度座標が、ある図面に関する例として使用されている。10進法として表された場合、メリーランドにおける経度座標は通常負の数として表される。しかしながら、以下の説明では、本発明の基礎をなす方法の説明を容易にするために、これらの経度座標は一

10

20

30

40

50

貫して正の数として表されている。

【0020】

デジタル情報：デジタル情報はデジタルフォーマットで表された情報である。デジタル的に表されることのできる情報の例には、テキスト、データ、ソフトウェア、音楽、ビデオ、グラフィックス等が含まれる。

【0021】

位置識別性の実施：デジタル情報の関連した位置識別属性によってそのデジタル情報へのアクセスを行うか、あるいは拒否する方法。

【0022】

ジオコード (geocode)：通常座標系に関連した地球上の位置の特有の符号化。いくつかのジオコードは、ある場所がその緯度および経度によって何時識別されたかのような、ポイント位置を識別する。別のジオコードは、郵便番号のような領域を識別してもよい。

10

【0023】

ジェオロック：デジタル情報と、位置識別属性により規定された地理的エリアとの間において実施された関連付け。

【0024】

ジェオロックされた情報：位置識別属性と関連付けられており、位置識別属性により規定されたエリア内においてのみアクセス可能なデジタル情報。

【0025】

20

位置：任意の地理的な場所。それは、正確な地点、エリアまたは領域の位置、近接エリア内に含まれている地点、または地球上の場所の組合せであることができるが、それに限定されない。位置はまた、地球の表面より高いか、または低いポジションを識別するための高さ（または高度）、あるいは時間的なディメンションでポジションを識別するための時間を含むことができる。

【0026】

位置識別性：位置の正確な符号化。情報がアクセスされる位置を正確に規定するためにその情報の属性が使用されることができ、それに限定されない。位置識別性は、ある地点、ある領域、関連付けられた地点を有する領域、回廊地帯（すなわち、中心線の両側に長さを有するその中心線）の符号化であってもよいし、あるいはある位置の任意の他の正確な空間的および時間的識別により行われてもよい。

30

【0027】

位置分散：ある位置のジオコードがそれと隣接した位置とを正確に区別できない可能性のある最小分解能。たとえば、軍用方眼地点指示方式が精度の2つのキャラクタと共に使用された場合、任意の位置の精度はわずか10キロメートル以内である。

【0028】

再生位置：デジタル情報へのアクセスが許可されるであろう位置識別属性の位置部分。

【0029】

プレーヤ位置：ジェオロックされたファイルの再生を試みるアプライアンスの位置。

【0030】

40

近接：その位置を含んでいるゾーンまたはエリア。

【0031】

上記の定義は本発明の技術的範囲を制限するものではなく、それはむしろ本発明を説明するときに使用される用語を明確にするものである。定義された用語はまた、当業者には別の意味があることを認識すべきである。以下の詳細な説明において、これらおよびその他の用語が使用される。

図1を参照とすると、位置識別性によって決定されたデジタル情報へのアクセスを表す本発明の概略図が示されている。位置識別性とは、情報がアクセス可能な地理的エリアまたは領域を正確に決定するその情報の属性のことである。AおよびBで示された2つの地理的エリアがマップ101上のアメリカ大陸内に示されている。情報130はデジタルフォーマ

50

ットで表され、そのデジタル情報がアクセスされることのできる領域として地理的エリアAを正確に規定する関連した位置識別属性131を有している。アプライアンス112がこの地理的領域A内に位置している場合、デジタル情報130はそのアプライアンスによってアクセス可能となる。反対に、アプライアンス122が地理的領域B（または地理的領域A以外の他のどこかの場所）内に位置している場合、デジタル情報130はアクセス不可能となるであろう。したがって、位置識別性は、デジタル情報がアクセスされることのできる正確な地理的領域を決定するそのデジタル情報の属性を表している。位置識別性を有するデジタル情報は“ジオロックされている”と呼ばれ、位置識別属性を実施するシステムは関連付けられたデジタル情報を、位置識別属性により規定された地理的領域にジオロックする。

10

【0032】

図2には、位置識別属性140が情報の2つの項目、すなわち位置値142および近接値143を含むものとして示されている。位置値142は特定の場所の特有のポジションに対応している。任意の位置が特有に数値で識別される緯度および経度のような多くの異なった座標系が開発されている。本発明の目的のために、ある場所を特有に識別する任意の座標系が位置識別属性140の位置値142として使用されることができる。近接値143は、その位置を囲むゾーンまたはエリアの範囲に対応している。位置識別属性140は、近接値143がゼロ、ナル、空等、または位置識別属性により参照されたエリアが特有の地点であることを示する別の値に設定されている場合、ある地点または正確な位置を含んでいてもよい。近接値143は、位置分散とは異なっていることを認識すべきである。近接値143はエリアまたは領域を表わすものであり、一方位置分散は、ジオコードまたはある位置がそれと隣接した位置と正確に区別できない可能性のある最小分解能である。

20

【0033】

図3は、位置値142をさらに詳細に示している。上述のように、座標系内の全ての各位置を特有に識別する1組の数が得られる多くの種々の座標系が一般的に使用されている。本発明において、位置値142は、142aで示されているように特有の位置表示またはジオコードに関して規定されている。それ故、通常の座標系を使用する緯度144および経度145がさらにジオコードを規定することができる。地球中心方式(Earth Centered)、地球固定ガウス座標系、ユニバーサル・トランスバース・メルカトル(UTM)、軍用方眼地点指示方式(MGRS)、ワールド・ジオグラフィック・リファレンス・システム(GEOREF)等のような既知の別のシステムもまた便利に使用されることができる。緯度144および経度145に加えて、位置値はさらに、142bで示されているように高度146を含むことが可能であり、この高度146は海水面より上方の位置の高さに対応している。その代りに、位置値はさらに142cで示されている時間値147を含むことができ、この時間値147は日付および、または時間範囲に関して規定されてもよい。これによって、位置識別属性の定義は情報に対する地理的および、または時間的アクセスの両者を考慮することが可能になる。

30

【0034】

位置識別性の位置値142を含む地理的領域またはエリアはいずれも位置識別属性140に対する近接値143として機能することができる。近接値143は、2つの隣接した経度線（水平線のエッジを示す）と2つの隣接した緯度線（垂直線のエッジを示す）とにより規定された方形領域を含んでいてもよい。その代りに、近接値143は、その位置の周囲の半径を規定する単一の数により表された円形領域を含んでいてもよい。円形領域はさらに、その位置を中心とした楕円形エリアか、あるいは必ずしも質量中心としてではないがその位置を含んでいる円形または楕円形エリアのいずれかとして規定されることができる。別の形態では、近接値143は不規則的な閉じた多角形または回廊を含んでいてもよい。さらに別の形態においては、近接値143はブラジルの国のような既知の地理的領域に対応していてもよい。近接値143を規定することのできる既知の地理的領域の別のタイプには、郵便番号、州、郡、合併された市等が含まれる。

40

【0035】

50

本発明によると、ジェオロックされたデジタル情報が保存されるか、記憶されるか、あるいはコピーされた場合には常に、デジタル情報の後のアクセスが位置識別属性140により規定された地理的エリアに制限されるように、位置識別属性140がそのデジタル情報と関連付けられる。図4は、デジタル情報のアクセスまたは再生が可能にされるであろう領域を正確に規定する位置識別属性140とそのデジタル情報を関連付ける一般的な方法を示している。この方法は、コンピュータファイルが保存される場合のそのファイルに対する読み出し専用属性のようなファイル属性の設定に類似していることを認識すべきである。この方法は、パーソナルコンピュータ、サーバ、パーソナル・デジタル・アシスタント(PDA)、ラップトップ、ワークステーション、ネットワーク、広域携帯電話およびそれに類似したもののような端末使用、別のパーティへの通信または配信のためにデジタル情報を生成し、操作し、処理するのに十分なデータ処理能力およびメモリを有するシステムまたはデバイスによって行われる。システムまたはデバイス上で動作するソフトウェアまたは埋込み型ファームウェア命令はこの方法が行われるようにする。

10

【0036】

とくに、この方法は、位置識別属性と共にデジタル情報を保存または記憶するコマンドによりステップ200からスタートする。ステップ202において、デジタル情報に対する位置値142は、後で使用するために検索され、記憶される。位置値142は、必ずしも、この方法がそのアプライアンスに呼出される地理的位置とは限らず、むしろデジタル情報に対するアクセスが許されることとなるアプライアンスに対する位置識別属性(上述した)に対応する。ステップ204において、アプライアンスの位置識別属性の近接値143が後で使用するために検索されて記憶される。以下、位置および近接値142、143を生成する種々の方法をさらに詳細に説明する。このような方法に加えて、位置および近接値142、143はまたメモリ中に予め記憶され、そこから検索されてもよいし、あるいはエンドユーザがその情報を提供するように問合せられてもよい。ステップ206において、検索された位置および近接値142、143は、位置識別属性140を生成するために使用される。その後、ステップ210において、デジタル情報216は、ジェオロックされたデジタル情報218を提供するように位置識別属性140と関連付けられる。

20

【0037】

再生アプライアンスが有効な位置識別属性を確認しない限り、そのアプライアンスより行われる読み出しまたはコピー動作によってジェオロックされた情報にアクセスしようとする試みは、拒否されるであろう。これは、デジタル情報の関連付けられた位置識別性を再生アプライアンスの位置に対して評価して一致するか否かを決定することにより行われる。図5は、デジタル情報へのアクセスを位置識別属性により実施するための一般的な方法を示している。論理的には、この方法は、オペレーティングシステムが現在ファイル上で読み出し専用属性を実施している方式、すなわちユーザが読み出しのためにそのファイルにアクセスすることを許すが、書き込みのためのアクセスを拒否する方式に類似している。この方法は、パーソナルコンピュータ、サーバ、ルータ、パーソナル・デジタル・アシスタント(PDA)、ワークステーション、ネットワーク、広域携帯電話、ラップトップ等の別のパーティにより通信され、あるいは配信されたデジタル情報の受信を可能にするのに十分なデータ処理能力およびメモリを有するシステムまたはデバイスによって行われる。システムまたはデバイス上で動作するソフトウェアまたは埋込み型ファームウェア命令はこの方法が行われるようにする。

30

40

【0038】

とくに、この方法は、デジタル情報にアクセスするコマンドによりステップ220からスタートする。ステップ222において、ジェオロックされたデジタル情報218は、関連付けられた位置識別属性140を読み出しおよび記憶するためにアクセスされる。デジタル情報それ自身ではなく、ジェオロックされた情報の位置識別部分だけがアクセスされることを認識すべきである。ジェオロックされた情報の位置識別属性140はこの方法においてさらに使用されるために記憶される。ステップ224において、この方法は、デジタル情報にアクセスするアプライアンスの位置を決定する。以下に説明するように、アプライアンス位置16

50

0を決定するための種々の可能な方法が存在する。アプライアンス位置160はこの方法においてさらに使用されるために記憶される。ステップ226において、この方法は、アプライアンスの位置が位置識別性140により規定された領域と一致するか否かを決定する。アプライアンス位置160が位置識別属性140と一致した場合、ステップ228においてジェオロックされたデジタル情報218へのアクセスが可能にされる。反対に、アプライアンス位置160が位置識別属性140と一致しない場合、ステップ230においてアクセスは拒否される。

【0039】

図6A乃至6Dは、ジェオロックされたデジタル情報へのアクセスを試みているアプライアンスの再生位置を決定するための複数の例示的な方法を示している。これらの方法は、図5に関して上述したように、デジタル情報による位置識別属性を実施する処理手順の一部としてシステムにより行われる。アプライアンスの再生位置を決定する別の方法もまた有効に使用されることが可能であることを認識すべきである。

【0040】

図6Aは、ジェオロックされたデジタル情報を受信することとなるアプライアンスに対する街路アドレスからジオコードが解かれるアドレスデコーディング方法240を示している。ステップ242において、アプライアンスに対するアドレスが検索される。アドレス情報は、アドレスが獲得されたそのアプライアンスとの前の通信に基づいてメモリから再現されることができる。その代わりに、アプライアンスは情報トランザクションの最初の部分としてアドレス情報を提供するように促してもよい。アドレス情報は一度検索されると、ステップ244において特定のジオコードを導くために復号される。このステップは、Mapinfo社(Troy, New York)製のMapMarker OCXコンポーネントバージョン4.2のような、アドレスから座標特定ジオコードを生成することのできる市販のソフトウェアプログラムを使用してもよい。位置識別属性に関して時間要素を含むことが所望された場合、ステップ246において、アプライアンスシステムクロックから時間を読み出す等によりそのアプライアンスから現在の時間が検索される。このステップ246は随意であり、多くのアプリケーションにおいて、時間要素は必要とされないことを認識すべきである。最後に、ステップ248において、ジオコードおよび時間は、位置識別属性140に対する位置値142として使用可能なフォーマットに変換される。

【0041】

図6Bは、アプライアンス上に記憶されたライセンスから位置値が導かれるアプライアンスライセンス方法250を示している。ライセンスパックは多くのシステムによく知られている特徴であり、一般にアプライアンスプログラムへのアクセスの妥当性を検査するために使用されている。ライセンスパックは、ユーザ/免許された者に関する情報を含むデジタルファイルである。それらは解読不可能ではないが、ユーザの妥当性を検査する信頼性の高い方法のものとなるように編成され、暗号化されている。本発明のこの実施形態において、ライセンスパックは、アプライアンスの位置を識別する座標特定ジオコードを含んでいる。ステップ252において、アプライアンス上に記憶されたライセンスパックがアクセスされ検索される。その後、ステップ254においてジオコードがそのライセンスから復元される。位置識別属性に関して時間要素を含むことが所望された場合、ステップ256において、アプライアンスシステムクロックから時間を読み出す等によりそのアプライアンスから現在の時間が検索される。このステップ256は随意であり、多くのアプリケーションにおいて、時間要素は必要とされないことを認識すべきである。最後に、ステップ258において、ジオコードおよび時間は、位置識別属性140に対する位置値142として使用可能なフォーマットに変換される。

【0042】

図6Cは、アプライアンス内に埋込まれたGPS受信機から位置値が復元されるGPSデータ復元方法260を示している。技術的に知られているように、グローバル・ポジショニング・システム(GPS)は、米国防省により開発されて運用されている衛星ベースの無線航法システムである。GPSにより、地上、海上および航空機上のユーザは一日24時間にわたって、全天候の下に、世界中のどこでも彼等の3次元位置、速度および時間

10

20

30

40

50

を判断して決定することが可能となる。このGPSシステムは世界中の民間ユーザに100m未満の正確度を提供し、一方米国の軍事および民間ユーザははるかに高い正確度を有している。GPS位置情報は、World Geodetic System 1984 (WGS 84) と呼ばれる座標系に基づいており、緯度および経度座標系に類似している。GPS受信機の商業的可用性は、一般的に増加を続けており、この実施形態では、アプライアンスは組み込み型GPS受信機を含んでいることが予想される。たとえば、GPS受信機は、Rockwell社製のNavCardまたはTrimble Navigation社製のGPS cardのようなPCMCIAカードとして利用可能であり、Novale社は汎用IBM PC用のGPS受信機を製造している。ステップ262において、アプライアンス内に組み込まれたGPS受信機がアクセスされる。ステップ264において、組み込まれたGPS受信機からジオコードが復元される。随意に、時間値もまたGPS受信機から復元されてもよい。最後に、ステップ266において、ジオコードおよびオプションの時間値は、位置識別属性140に対する位置値142として使用可能なフォーマットに変換される。

10

【0043】

図6Dはアプライアンスの位置を決定するための三角測量データ復元方法270を示している。技術的に知られているように、三角測量は、正確な位置情報を提供するために衛星、広域携帯電話、航法システムおよびその他の無線信号オペレータによってよく使用される方法である。ロラン-Cシステムは、複数の固定された位置のRF送信機からのRF信号を三角測量することによって位置情報を提供する商用として利用可能な航法システムの一例である。ステップ272において、システムはアプライアンスにより伝達されたRF信号にアクセスすることによりそのアプライアンスの方向を決定する。ステップ274において、三角測量アルゴリズムを使用してRF信号からジオコードが計算される。最後に、ステップ276において、ジオコードは、位置識別属性140に対する位置値142として使用可能なフォーマットに変換される。位置識別属性140において時間要素が必要とされた場合、上述した同じ方法でアプライアンスのシステムクロックから現在の時間が読出される。

20

【0044】

本発明の1実施形態によると、デジタル情報はアプライアンスへの転送前に暗号化され、位置識別属性140は、デジタル情報を暗号化するために使用される位置識別属性ベースのキーを生成するために使用される。デジタル情報に追加される暗号の層は、位置識別属性140により規定されたアクセスに対する制限を実施する。図7は、平文のデジタル情報（メディア）をジェオロックされた暗号化されたデジタル情報に変換するために使用される位置識別属性140に、デジタル情報を関連付ける暗号化方法を示している。この方法は、ネットワークに接続されたユーザに暗号化されたデジタル情報を分配するために、インターネットのようなネットワークに結合されたサーバによって行われることができる。デジタル情報は、メディア記憶メモリ152からサーバによりアクセスされる。広告またはデジタル形態の他の類似したマテリアルのようなプレビュー情報はまた、プレビュー記憶メモリ154からサーバによりアクセスされてもよい。デジタル情報およびプレビュー情報は平文形態でメディア記憶メモリ152およびプレビュー記憶メモリ154中に記憶される。ジェオロックされるべき特定のデジタル情報は、メディア記憶メモリ152内の平文のデジタル情報にインデックスを付けるために使用される特有のメディアID 150を割当てられる。

30

40

【0045】

この方法は、位置識別属性にしたがって暗号化されたジェオロックされたデジタル情報を生成するコマンドによりステップ300からスタートする。ステップ302において、リクエストされたデジタル情報（またはメディア）はメディア記憶メモリ152から対応したメディアID 150に関連してアクセスされる。デジタル情報は近接地理的エリアに対してカスタム暗号化されているので、プレビュー情報は参照された最も近い地理的エリアに対してカスタム調整され、暗号化されたメディアと共に含まれることができる。その代わりに、ターゲットの顧客に関する人口統計情報が知られてもよく、含まれているプレビュー情報をさらに改善するために使用されることができる。追加のプレビューが含まれることになる

50

場合、ステップ304においてそれはプレビュー記憶メモリ154からアクセスされ、リクエストされたデジタル情報と連結される。平文のデジタル情報および連結されたプレビュー情報は、ステップ306において行われる暗号処理への入力として使用される。

【0046】

ステップ306における暗号処理は、位置および近接値により規定される地理的領域の形状を規定する位置識別属性140を使用する。位置識別属性140は、以下においてさらに詳細に説明するように暗号化のために使用されるジェオロックキー166を生成するために使用される。その後、ステップ308において、形状パラメータ（形状 *parm*）と呼ばれるパラメータを暗号テキストの前部に付加することにより、平文が暗号化されると共にジェオロックされた情報がパッケージ化される。とくに、ジェオロックキーは、ジェオロックされたデジタル情報156を提供するように暗号化アルゴリズムを使用して平文情報および連結されたプレビュー情報を決定論的に修正するために使用され、このジェオロックされたデジタル情報156には暗号テキスト形態158のデジタル情報および連結されたプレビュー情報と、平文形態の形状 *parm* 157とが含まれている。形状 *parm* は重要なエリアの形状を、この重要なエリアに対応した特定の位置を識別せずに規定する。形状 *parm* は、位置識別属性140の近接部分の無位置変換である。無位置とは、実際の位置を参照せずに近接エリアの形状を規定する形状 *parm* の特性のことである。

【0047】

位置識別属性140が規定する近接エリアが円形であるか、あるいは境界を付けられた方形であるかに応じて、各形状 *parm* は特性上サイズが異なったものとなる。この種々サイズを使用して、ジェオロックされたデジタル情報156を受取ったクライアントは、円形または境界を付けられた方形のどちらの近接エリアに対してファイルを処理すべきかを決定する。その代り、形状 *parm* のフォーマットは、ジェオロックされたデジタル情報中のフィールドとして含まれていてもよい。

【0048】

本発明の好ましい実施形態において、近接エリア内の異なった座標を同じ値にマップするためにマッピング関数が使用される。マッピング関数は次式で表される：

$$f(x) = \Delta * \text{int}(x / \Delta)$$

ここで、*int* は括弧内のその引数の整数部分を戻す関数である。x をジオコード位置の緯度として使用し、 Δ を境界をなす緯度間の辺の長さとして使用することによって、または x をジオコード位置の経度として使用し、 Δ を境界をなす経度間の辺の長さとして使用することによって、グリッドは緯度／経度座標系全体に対して構成されることができる。グリッドセル内のあらゆるジオコードは、上記の関数とその緯度および経度に適用されたときに同じ値に変換されることとなる。“大きい方形”の境界は、境界をなす辺の長さの正確な倍数である境界上に直接位置しなくてもよいので、無位置オフセット尺度が境界の下方の辺を使用して計算され、グリッドを線形的にシフトするために使用される。

【0049】

図8は、境界を付けられた方形近接エリアに対する位置識別属性からのパラメータ形状 *parm* の決定を示している。図中の水平線は緯度線に対応し、垂直線は経度線に対応している。赤道（緯度）およびグリニッジ（経度）が示されている。点線のグリッドは、方形近接エリアのサイズと同じサイズの方形グリッドに対する緯度および経度の線を表している。グリッドは0度の緯度（すなわち、赤道）および0度の経度（すなわち、グリニッジ）を中心と定められている。境界を付けられた方形に対する位置識別性は、再生位置の緯度（*lat*）および経度（*lng*）である位置部分を含んでいる。近接部分は、2つのセットの座標により表される。第1の座標セットは、方形の下方部分を規定する緯度線と方形の左辺を規定する経度線とを提供し、（ $\beta \text{lat} 1$, $\beta \text{lng} 1$ ）によって表される。第2の座標セットは、方形の上部を規定する緯度線と方形の右辺を規定する経度線とを提供し、（ $\beta \text{lat} 2$, $\beta \text{lng} 2$ ）によって表される。位置識別性から、形状 *parm* は、最初に境界を付けられた方形の辺の長さを計算することによって計算される。緯度線の間の距離は Δlat で示され、 $\beta \text{lat} 2$ と $\beta \text{lat} 1$ との間の絶対差 [すなわち *a b*

$s(\beta_{lat}2 - \beta_{lat}1)]$ である。経度線の間の距離は Δlng で示され、 $\beta_{lng}2$ と $\beta_{lng}1$ との間の絶対差[すなわち $abs(\beta_{lng}2 - \beta_{lng}1)]$ である。

【0050】

次に、上述したマッピング関数を使用して変換係数が計算される。緯度変換係数($olat$)は、以下の式にしたがって計算される：

$$olat = \beta_{lat}1 - \Delta lat * int(\beta_{lat}1 / \Delta lat)$$

経度変換係数($olng$)は、以下の式にしたがって計算される：

$$olng = \beta_{lng}1 - \Delta lng * int(\beta_{lng}1 / \Delta lng)$$

これらの式は、座標値を線形的にシフトするために使用される。形状 $parm$ は2つのセットの数(Δlat , Δlng)および($olat$, $olng$)である。形状 $parm$ は無位置である、すなわち、それは方形近接エリアのサイズだけに依存し、方形近接エリアの正確な位置には依存しないことは注目に値する。マッピング関数が形状 $parm$ により使用されたとき、以下の関数は方形近接エリア内の任意の緯度/経度座標($plat$, $plng$)に対して同じ値を有することとなる：

$$f(plat) = \Delta lat * (int((plat - olat) / \Delta lat))$$

$$f(plng) = \Delta lng * (int((plng - olng) / \Delta lng))$$

とくに、値の対($f(plat)$, $f(plng)$)は、境界をなす方形の下辺および左辺の上およびその内部の全ての座標に対して同じ値を有することとなり、また、値は形状 $parm$ と、座標($plat$, $plng$)とにのみ依存するであろう。これらの関数は、デジタル情報をジェオロックするために使用される暗号化キーを構成するために使用されるであろう。

【0051】

図9は、円形の近接エリアに対する位置識別性からの形状 $parm$ パラメータの決定を示している。前の図面のように、水平線は緯度線に対応し、垂直線は経度線に対応している。点線のグリッドは、円形の近接エリアを正確に囲む方形と同じサイズの方角グリッドに対する緯度および経度の線を表している。円形の近接エリアに対する位置識別性は、再生位置の緯度(lat)および経度(lng)により規定される位置部分と、単一の数、すなわち、円形近接エリアの半径により規定される近接部分とを含んでいる。位置識別属性から、形状 $parm$ は最初に円形近接エリアの半径の2倍として直径を決定することにより計算される。この値から、図9に示されているように方形グリッドに対するサイズが得られる。次に、変換係数が計算され、上述したマッピング関数を使用する。緯度変換係数($olat$)および経度変換係数($olng$)は、以下の式にしたがって計算される：

$$olat = lat - \text{半径} - (\Delta lat * int(lat / \Delta lat))$$

$$olng = lng - \text{半径} - (\Delta lng * int(lng / \Delta lng))$$

ここで、 Δlat Δlng は円形の近接エリアの直径に対応する。これらの式は、座標値を線形的にシフトするために使用される。形状 $parm$ は2つのセットの数($olat$, $olng$)および半径である。マッピング関数が形状 $parm$ により使用されたとき、以下の関数は、円形近接エリアに境界を付ける方形内の任意の緯度/経度座標($plat$, $plng$)に対して同じ値を有することとなる：

$$f(plat) = \Delta lat * (int((plat - olat) / \Delta lat))$$

$$f(plng) = \Delta lng * (int((plng - olng) / \Delta lng))$$

とくに、値の対は($f(plat)$, $f(plng)$)は、グリッド正方形の下辺および左辺の上およびその内部の全ての座標に対して同じ値を有し、値は形状 $parm$ と、座標($plat$, $plng$)とにのみ依存するであろう。これらの関数は、デジタル情報を暗号化するために使用されるジェオロックキーを構成するために使用されるであろう。最後

10

20

30

40

50

に、以下の式を使用してそれが円形近接エリア内に入っているか否かを決定するために座標 (p l a t , p l n g) が評価されることができる：

$$d i s t = s q r t ((p l a t - (f (p l a t) + \text{半径} + o l a t)) ^ 2 + (p l n g - (f (p l n g) + \text{半径} + o l n g)) ^ 2$$

これに対して d i s t は半径以下であり、円形近接エリアの円周上であるか、または円周内に入っている。

【 0 0 5 2 】

本発明の別の実施形態によると、デジタル情報は、アプライアンスによる転送または記憶される前に暗号化され、位置識別属性140は、デジタル情報を暗号化するために使用される位置識別性ベースのジェオロックキーを生成するために使用される。デジタル情報に追加された暗号化の層は、位置識別属性140により規定されたアクセスに関する制限を実施する。

10

【 0 0 5 3 】

図 1 0 は、平文のデジタル情報 (メディア) をジェオロックされた暗号化されたデジタル情報に変換するために使用される、デジタル情報を位置識別属性140と関連付けるための暗号化方法を示している。この方法は、アプライアンスにより、デジタル情報をローカルメモリ (たとえば、ハードディスク) 中に記憶する前、あるいはデジタル情報を別のアプライアンスまたはネットワークに伝送する前に行われてもよい。

【 0 0 5 4 】

平文のデジタル情報170をジェオロックするために使用されることとなる位置識別属性140は、(a) 再生位置パラメータ162と、(b) 形状 p a r m パラメータ157の2つのパラメータを計算するために使用される。再生位置パラメータ162は、位置識別属性140の位置部分である。形状 p a r m パラメータ157は、上述した方形または円形の境界を付けられた領域に対して計算された位置識別属性の近接部分の無位置変換である。位置および形状 p a r m の両パラメータは、道理上推測または再構成されることのできないジェオロックキー166を構成するためにキー生成プロセス310への入力として使用される。本発明の好ましい実施形態において、ジェオロックキー166は長さが64ビットであるが、任意の長さが有効に使用されることができるとを認識すべきである。結果的に得られるシーケンスは、暗号化プロセス312によってビット的排他的オアを行うことにより平文データ170を暗号化するために使用される。この結果、平文170の中のデータバイトの数に等しい長さの暗号化されたバイトが得られる。暗号化されたデータ (または暗号テキスト) 158は、形状 p a r m 157パラメータに連結され、ジェオロックされたデジタル情報156として記憶される。別の既知の暗号化アルゴリズムもまた有効に使用されることができるとを認識すべきである。

20

30

【 0 0 5 5 】

例示的な暗号化プロセス312は広く使用されている別の暗号化方法に類似しているが、1つの大きな相違を有している。排他的オア機能 (すなわち、X O R) を使用して平文と組合せられた64ビットの暗号化キーは、商業的には、W i r e d E q u i v a l e n t P r i v a c y (W E P) のようなプロトコルにおいて使用される。W E P の実施は、会話に参加しているステーションにキーをどのように分配すべきかというキー管理問題を考えなければならず、そのようにして暗号化 / 解読が行われることができる。しかしながら、本発明にはキー分配問題は存在しない。暗号化 / 解読キーは、デジタル情報と共に含まれている無位置情報およびそのアプライアンスに対する再生位置のみから構成されることができる。ファイルが暗号化されたときに位置識別属性より規定された近接エリア内に位置しているアプライアンスだけが、デジタル情報を見るか、あるいは再生することができる。その代りに、暗号化キーを構成するために位置識別属性140の時間パラメータが近接パラメータの代りに、あるいはそれと共に使用されてもよい。

40

【 0 0 5 6 】

図 1 1 には、ジェオロックキー166を形状 p a r m 値および再生位置 (l a t , l n g) 値から生成するために使用される上述のキ - 生成プロセス310がさらに詳細に示されて

50

いる。初期キ - 生成プロセス322は、形状 `parm`157および位置パラメータ162を使用して初期 64 ビット暗号化キー174を生成する。その後、この初期キー174は、初期キー174の決定論的数学的変換を使用してさらにジェオロックキー166の秘密保護および生成を行う秘密キー生成プロセス324（すなわち、隠蔽機能）において使用される。以下、図 13 に関して初期キーを生成するために使用される初期キ - 生成プロセス322および秘密キー生成プロセス324をさらに詳細に説明する。

【0057】

デジタル情報が本発明の上記の実施形態のいずれかにしたがって暗号化された後、アプライアンスは平文のデジタル情報を復元し、それによってデジタル情報を観察し、または再生することを可能にするために暗号解読プロセスを行う。図 12 は、平文のデジタル情報をジェオロックされたデジタル情報から復元するための暗号解読方法を示している。この方法は、位置識別属性にしたがって暗号化されたジェオロックされたデジタル情報にアクセスするコマンドによりステップ320から始まる。ステップ322において、図 6 A 乃至 6 D に関して上述した方法の 1 つを使用してアプライアンス位置160が決定される。アプライアンス位置160はこの方法でさらに使用するためにアプライアンスにより記憶されてもよい。ステップ324において、ジェオロックされたデジタル情報156がアクセスされる。上述したように、ジェオロックされたデジタル情報156は形状 `parm`パラメータ157と暗号テキスト158とを含んでいる。ステップ326において暗号解読処理が行われ、このとき、暗号化された情報を解読して、平文のデジタル情報170を生成するために使用されるジェオロックキーを決定するために形状 `parm`パラメータ157およびプレーヤ位置160が使用される。その後、平文のデジタル情報170は、たとえば、デジタル情報をプリンタにスプールし、そのデジタル情報を表示装置 / 再生装置上で観察する等の、任意の所望の方法でアプライアンスにより使用されてもよい。以下、図 15 に関して解読処理ステップ326をさらに詳細に説明する。

【0058】

図 13 を参照とすると、暗号化または暗号解読のいずれかに対して使用されるジェオロックキーを生成する例示的なプロセスが示されている。上記において方形および円形の近接エリアに対してそれぞれ計算された値（`flat (plat)`）、（`flng (plng)`）は、ジェオロックキーを生成するために入力として使用される。図 8 および 9 に関して上述したように、これらの値は形状 `parm`および位置値から計算される。緯度値 `flat (plat)` は、フォーマット `sll . d d d d d d` が生成されるようにプロセスステップ332において 10 文字の緯度ストリング184としてフォーマット化され、ここで `s` は符号である。同様に、経度値 `flng (plng)` 183は、フォーマット `sll l l . d d d d d d` が生成されるようにプロセスステップ334で 11 文字の経度ストリング185としてフォーマット化される。その後、プロセスステップ336において、全ての非数値文字（すなわち、符号および 10 進小数点）が緯度ストリング184および経度ストリング185から除去され、結果的に得られた経度ストリング185は結果的に得られた緯度ストリング184に連結されて、フォーマット `l l d d d d d d l l l d d d d d d` を有する 17 文字ストリング186が生成される。プロセスステップ338において、17 文字ストリング186は 64 ビット 2 進ストリングに変換される。とくに、17 文字ストリングの最後の文字はドロップされ、その結果全ての文字が数値である 16 文字ストリングとなる。各数字の文字は 4 ビットオクテット（たとえば、“1”はオクテット“0001”であり、“2”はオクテット“0010”である等）により表されることができ、16 文字ストリング中の各文字に対するオクテット表現が連結されて、64 ビットの 2 進ストリングが生成される。この 64 ビットの 2 進ストリングは、上述したようにデジタル情報を暗号化するために使用される初期キー174を提供する。

【0059】

その後、この初期キー174は、それを機密またはジェオロックキー166に変換する隠蔽機能340により処理される。本発明の好ましい実施形態では、別のさらに複雑な隠蔽機能もまた使用されることができ、比較的に簡単な隠蔽機能が使用さ

10

20

30

40

50

れる。隠蔽機能340にしたがって、初期キー174は、排他的オア機能（すなわち、X O R）を使用して16文字のストリングのオクテット展開1234567890123456と関連付けられた64ビットの2進ストリングと組合せられる。これによって、暗号化および解読の両方に使用されるジェオロックキー166が生成される。重要なことには、このジェオロックキー166の値は、ジェオロックされたデジタル情報に対応した近接エリア内の全ての位置に対して同じになる。本発明の好ましい実施形態において、隠蔽機能はソフトウェアルーチンとして実行されるが、しかし、電子回路において隠蔽機能を含む全暗号化アルゴリズムを実施することにより結果的に強い暗号化が行われることを認識すべきである。

【0060】

10

図14は、ジェオロックされたものの検索を試みているアプライアンスに適応可能な解読方法を示すフローチャートである。この方法において、プレーヤ位置160は知られていてもよく、あるいはメモリから検索されるか、もしくは図6A乃至6Dに関して前に示されたように決定されることができる。この方法は、ジェオロックキー166を生成するためにジェオロックされたデジタル情報156からの形状p a r m 157がプレーヤ位置160と共に使用されるステップ342から始まる。その後、ステップ344において平文のデジタル情報170が得られるようにジェオロックキー166を使用して暗号テキストデジタル情報158が解読される。上述したように、解読ステップ344はジェオロックキー166と暗号テキストデジタル情報158との間で排他的オア機能を行ってもよい。

【0061】

20

次に、図15乃至17を参照とすると、境界を付けられた方形近接エリアの種々の例が示されている。これらの図面は図8（上述された）に類似しているが、しかし境界を付けられた方形近接エリアに対するジェオロックキーを上記に示された好ましい方法を使用して計算するために使用される。図15は、ジェオロックキーを生成するために使用される境界を付けられた第1の方形近接エリアを示している。位置識別属性は以下のとおりである：

位置識別性 = (位置, 近接) =

((39.102479, 77.235771), ((39.102100, 77.235000), (39.103100, 77.237000)))

形状p a r mパラメータは位置識別属性から以下のように導かれる：

形状p a r m = ((Δlat, Δlng), (olat, olng)) = ((0.001, 0.002), (0.0001, 0.001))

30

その後、形状p a r mは、f(plat)およびf(plng)を決定するために上述したマッピング関数において使用される：

【数1】

$$f(\text{plat}) = .001 * (\text{int}(\text{plat} - .0001) / .001)$$

$$f(\text{plat}) = .001 * (\text{int}(39.102479 - .0001) / .001) = 39.102000$$

40

$$f(\text{plng}) = .002 * (\text{int}(\text{plng} - .001) / .0001)$$

$$f(\text{plng}) = .002 * (\text{int}(77.235771 - .001) / .0001) = 77.234000$$

f(plat)およびf(plng)からの8つの最上位桁の文字が使用されて、16文字ストリング3910200007723400が生成される。次に16文字ストリングの個々の文字はそれぞれ4ビットオクテットに変換され、以下の64ビットストリング初期キーが生成される：

50

【数 2】

00111001000100000010000000000000000011101110010001101000000000

その後、64ビットストリング初期キーは、ジェオロックキーを生成するために排他的オア機能（すなわち、XOR）を使用して16文字ストリングのオクテット展開1234567890123456と組合せられる。とくに、16文字ストリングのオクテット展開1234567890123456は以下のとおりである：

【数 3】

0001001000110100010101100111100010010000000100100011010001010110

排他的オア機能を使用して2つの64ビットストリングを組合せることにより生成されたジェオロック暗号化キーは以下のとおりである：

【数 4】

001010110010010001110110011110001001011101100000000000001010110

【0062】

図16は、プレーヤ位置がジェオロックされたデータの位置識別性と一致した、すなわち近接エリア内に入っているときの、境界を付けられた方形近接エリアに対するジェオロックキーの生成を示している。この例において、プレーヤ位置（すなわち、39.102120, 77.236120）は、図15に関する上記の例において与えられた再生位置とは異なっている。しかしながら、示されるように、両計算セットにより同じ暗号化キーが生成され、方形の近接エリア内の任意のプレーヤ位置から暗号テキストデジタル情報が復元されることができることが証明される。特定されたプレーヤ位置に対して、形状パラメータは上述されたものと同じである。マッピング関数 $f(plat)$ および $f(plng)$ は以下のとおりである：

【数 5】

$$f(plat) = .001 * (int(plat - .0001) / .001)$$

$$f(plat) = .001 * (int(39.102120 - .0001) / .001) = 39.102000$$

$$f(plng) = .002 * (int(plng - .001) / .0001)$$

$$f(plng) = .002 * (int(77.236120 - .001) / .0001) = 77.234000$$

このプレーヤ位置について、マッピング関数 $f(plat)$ および $f(plng)$ は上述された位置識別属性に対するものと同じであることを認識すべきである。したがって、初期キーおよびジェオロックキーはまた前に計算されたものと同じになる。したがって、プレーヤはジェオロックされたデジタル情報を特定されたプレーヤ位置から成功的に解読することができるであろう。

【0063】

対照的に、図17はプレーヤ位置がジェオロックされたデータの位置識別性と一致していない、すなわち位置識別性により規定された近接エリア外であるときの、境界を付けられた方形近接エリアに対するジェオロックキーの生成を示している。プレーヤ位置（すな

10

20

30

40

50

わち、28.543212, 73.543456) は、前の例で与えられた再生位置とは異なっている。この特定されたプレーヤ位置に対して、再び形状 parm は前の例のものと同じであるが、しかしマッピング関数値は $f(\text{plat})$ および $f(\text{plng})$ に対して異なった値を与える。とくに、マッピング関数 $f(\text{plat})$ および $f(\text{plng})$ は以下のとおりである：

【数 6】

$$\begin{aligned} f(\text{plat}) &= .001 * (\text{int}(\text{plat} - .0001) / .001) \\ f(\text{plat}) &= .001 * (\text{int}(28.543212 - .0001) / .001) = 28.543000 \end{aligned}$$

10

$$\begin{aligned} f(\text{plng}) &= .002 * (\text{int}(\text{plng} - .001) / .0001) \\ f(\text{plng}) &= .002 * (\text{int}(73.543456 - .001) / .0001) = 73.542000 \end{aligned}$$

$f(\text{plat})$ および $f(\text{plng})$ からの 8 つの最上位桁の文字が使用されて、16 文字ストリング 2854300007354200 が生成される。次に 16 文字ストリングの個々の文字はそれぞれ 4 ビットオクテットに変換され、以下の 64 ビットストリングの初期キーが生成される：

20

【数 7】

001010000101010000110000000000000000111001101010100001000000000

前のように、64 ビットストリングの初期キーはその後、排他的オア機能（すなわち、XOR）を使用して 16 文字ストリングのオクテット展開 1234567890123456 と組合せられ、以下のようなジェオロッキキーが生成される：

30

【数 8】

0011101001100000011001100111100010010111001001110111011001010110

40

初期キーおよび、したがってジェオロッキキーは前に計算されたものと同じでないことは注目に値する。したがって、プレーヤは特定されたプレーヤ位置からジェオロックされたデジタル情報を解読することができないであろう。

【0064】

以下図 18 および 19 を参照とすると、円形の近接エリアに対する暗号化 / 解読キーの計算の例が示されている。これらの図面は図 9（上述された）に類似しているが、上記の好ましい方法を使用して円形の近接エリアに対する暗号化 / 解読キーの計算を示すために使用される。図 18 は、円形の近接エリアに対する暗号化キーの生成を示している。位置識別属性は以下のとおりである：

$$\text{位置識別属性} = (\text{位置}, \text{近接}) = ((\text{lat}, \text{lng}), (\text{半径})) =$$

50

((39.102479, 77.235711), 0.0001)

形状 p a r m パラメータは位置識別性から以下のように導かれる：

形状 p a r m = ((o l a t , o l n g) , 半径) = ((- 0.000021 , 0.000071) , 0.0001)

円形近接エリアの直径 Δ l a t l n g は 0 . 0 0 0 2 である。その後、形状 p a r m は、 $f(p l a t)$ および $f(p l n g)$ を決定するために上述したマッピング関数において使用される：

【数 9】

$$f(plat) = .0002 * (int(plat - (-.000021) / .0002)$$

$$f(plat) = .0002 * (int(39.102479 + .000021) / .0002) = 39.102400$$

$$f(plng) = .0002 * (int(plng - .000071) / .0002)$$

$$f(plng) = .0002 * (int((77.235711 - .000071) / .0002) = 77.235600$$

$f(p l a t)$ および $f(p l n g)$ からの 8 つの最上位桁の文字が使用されて、16 文字ストリング 3910240007723560 が生成される。次に 16 文字ストリングの個々の文字はそれぞれ 4 ビットオクテットに変換され、以下の 64 ビットストリング初期キーが生成される：

【数 10】

001110010001000000100100000000000000111011100100011010101100000

その後、64 ビットストリング初期キーは排他的オア機能（すなわち、X O R）を使用して 16 文字ストリングのオクテット展開 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 と組合せられ、以下のジェオロックキーが生成される：

【数 11】

0010101100100100011100100111100010010111011000000000000100110110

図 19 は、プレーヤ位置がジェオロックされたデータの位置識別属性内である、すなわち、円形の近接エリア内に入っているときの、円形近接エリアに対するジェオロックキーの生成を示している。プレーヤ位置（すなわち、39.102420, 77.235699）は、図 18 に関して上記に示された位置識別性で規定された再生位置とは異なっている。しかしながら、示されるように、両計算セットから同じ暗号化キーが得られる。特定されたプレーヤ位置に対して、形状 p a r m パラメータは図 18 に関して上述したのと同じである。その後、形状 p a r m パラメータは、 $f(p l a t)$ および $f(p l n g)$ を決定するために上述したマッピング関数において使用される：

10

20

30

40

【数 1 2】

$$f(plat) = .0002 * (int(plat - (-.000021)/.0002)$$

$$f(plat) = .0002 * (int(39.102420 + .000021)/.0002) = 39.102400$$

$$f(plng) = .0002 * (int(plng - .000071)/.0002)$$

$$f(plng) = .0002 * (int(77.235699 - .000071)/.0002) = 77.235600$$

10

このマッピング関数は、特定されたプレーヤ位置に関して、それらが位置識別性の位置部分を使用した場合と同じ結果を生じさせる。次に、以下の式を使用してそれが円形の近接エリア内に入っているか否かを決定するために座標 (p l a t , p l n g) が評価される：

$$dist = \sqrt{(plat - (f(plat) + 半径 + olat))^2 + (plng - (f(plng) + 半径 + olng))^2}$$

$$dist = \sqrt{(39.102420 - (39.102400 + 0.00001 - 0.000021))^2 + (77.235699 - (77.235600 + 0.00001 + 0.000071))^2}$$

$$dist = 0.00008414$$

20

距離関数は半径以下である値を戻したので、プレーヤは円形領域の円周内に入っているか、あるいは円周上に位置している。反対に、距離関数が半径より大きい場合、ジェオロックキーは、無効キーである全て0の64ビットストリングに設定され、ジェオロックされたデジタル情報を正しく解読しないであろう。上述したように、このプレーヤ位置に関して、マッピング関数 $f(plat)$ および $f(plng)$ は位置識別属性に対するものと同じである。したがって、プレーヤはジェオロックされたデジタル情報を特定されたプレーヤ位置から成功的に解読することができるであろう。

30

【0065】

上述の位置識別属性暗号化システムおよび方法には多くの利点がある。位置識別性は、デジタル情報セキュリティ問題を克服し、ユーザに完全に透明な方式で暗号化キーを管理する手段を提供する。これによって、暗号化されたデジタル情報はインターネットのような公衆ネットワークを横切って容易に通信されることが可能になる。デジタル情報の準備が整えられた近接エリア内のユーザは、この情報にアクセスし、これを使用することができ、一方このエリア外のユーザはアクセスを拒否されるであろう。この点において、デジタル情報は、それが再生されることとなるターゲット位置に対して特定の暗号化されるため、本発明は“カスタム”または“1対1”暗号化を行なう。また、カスタム暗号化によって、デジタル情報は、ジェオロックされた情報と共に含まれているターゲットのプレビューおよび広告マテリアルに対して正しい順序でカスタム化されることが可能となる。特定の位置に対してファイルが暗号化されたとき、カスタムプレビューマテリアルを含むようにそのエリアの人口統計が使用されることができ。たとえば、メキシコシティに対して暗号化されたマテリアルは、スペイン語のプレビューマテリアルを含んでいてもよく、一方メリーランド州のゲイザースバーグに対する類似のマテリアルは英語である。

40

【0066】

位置識別属性ベースの暗号化は特性上、暗号化キーの共用に関して前の暗号化方法とは異なったアプローチを採用する。対称的な解読キーを構成するために不可欠な情報の2つの部分は、(a)再生装置に知られている再生位置と、および(b)暗号化されたデジタル情報内と共に含まれている形状 *parm* パラメータとを含んでいる。いずれか一方の情

50

報部分だけでは、解読キーを構成するのに不十分である。暗号化は地理的エリアに特定されており、暗号化アルゴリズムはその解読が行われるユーザまたは装置に関して何も知る必要がない。同じデジタル情報の暗号解読は、位置識別属性により規定された領域内にその位置が入っていると識別された任意のマシン上で行われることができる。位置識別暗号化は、それが従来技術の方法の有用性を制限するキー分配問題を回避するという点で、以前の暗号化アルゴリズムとは異なっている。Wired Equivalent Privacy (WEP) のような対称的な暗号化方法、または Diffie-Hellman のような非対称的な方法によるように暗号化キーの分配または共用を行う必要がない。また、セキュア・ソケット・レーヤ (SSL) またはマルチパーパス・インターネット・メール・エクスチェンジ (S/MIME) におけるように秘密キー交換を交渉する必要がない。

10

【0067】

デジタル情報へのアクセスを制御するために位置識別属性が使用されることのできる多くのアプリケーションおよびデータフォーマットが存在している。ユーザは電話線、光ファイバ、ケーブルテレビジョン、衛星放送、無線またはその他のメディアを含む任意の都合のよい方法を使用して、ジェオロックされたデジタル情報を電子形態で受取ることができる。ユーザはまたカスタム生成されたジェオロックされたデジタル情報を、たとえば、CD-ROM、ディスク、ビデオカセットまたはテープ等の磁気またはその他の符号化されたメディアの形態で店またはベンダーから物理的に受取ってもよい。同様に、ジェオロックされたデジタル情報は、インターネットのような広域ネットワーク、イントラネットのようなローカルネットワーク、eメールへの接続のような個人とサーバコンピュータとの間のダイヤルアップアクセスを含むネットワークによって、あるいはデジタル広域携帯電話または別の無線デバイスによって伝送されることができる。ジェオロックされたデジタル情報は、ディスク、CD-ROM、テープ、固定されたまたは取外し可能なハードディスク、DVD/CD-ROM、フラッシュメモリ/ディスク、EEPROM等に記憶されることができる。この方式で保護されることのできるデジタル情報のタイプには、いくつかの名をあげれば、音楽ファイル（たとえば、MP3）、ソフトウェア、文学作品、商取引ファイル、テキストファイル、ビデオ/グラフィックス、ページングメッセージ、広域携帯電話の会話および取引、ならびにデジタルファイルが含まれることができる。

20

30

【0068】

例示的なアプリケーションにおいて、顧客はデジタルフィルムまたはオーディオをベンダーのカatalogから注文する。このCatalogはハードコピーまたはインターネットベースのものであってよく、その注文は郵便投函、電話、ファクシミリ送信またはインターネットベースの取引によって行われることができる。何れの発注方法でも、顧客の注文は再生位置を示している。この注文がベンダーによって調達されたときに、その顧客に関連した位置識別属性が決定され、暗号キーを生成するために使用され、後にこの暗号キーはそのメディアに対するデジタル情報ファイルを暗号化するために使用される。その後、購入されたメディアはその注文に対してカスタム暗号化され、DVDまたはCD-ROMのようなフォーマットにコピーされ、ビューアと共にパッケージ化され、このビューアもまた位置識別属性に対してカスタム化されている。購入されたメディアの内容全体がコピーされた場合でさえ、その位置識別属性に対してカスタム化されたビューアおよびメディアが許容領域外での視聴を阻止する。この例示的なアプリケーションでは、位置識別性ならびにカスタム化された暗号およびビューアの使用により、デジタルメディアの著作権侵害および無許可使用ならびにコピーの問題に対して抵抗力の強い解決方法が提供される。

40

【0069】

本発明の別の例示的なアプリケーションにおいて、位置識別性は、公衆ネットワークによって情報を“有線放送 (narrowcast)” するために使用される。有線放送とは、この文脈では、ポイント・ツー・ポイント伝送、あるいは無制限の位置に対する放送とは対照的に、限られた視聴者に対する情報の伝送のことである。たとえば、局地的天候、交通情報

50

、映画上映スケジュール、店舗情報等の多くのタイプの情報は、ある位置関係の範囲内でのみ使用可能である。このような位置依存性情報を使用するアプリケーションは、位置ベースアプリケーションと呼ばれることができる。位置識別性は、たとえば、天候に対するローカル地域、販売に対する店舗の位置および広告情報等の、それが関連する位置で識別されるネットワークによって情報を送信するために放送タイプのプロトコルを使用する方法を提供する。クライアントのアプライアンスの位置を使用することにより、そのクライアントのアプリケーションは情報に付与された位置識別性を使用して、それらの現在の位置に基づいて情報を選択的にスクリーンすることができる。それはまた、地理的に制限された有線放送アプリケーションに対して、機密保護されて安全な秘密通信を維持するために特有の位置ベースの共用暗号キーを設定する方法を提供することができる。

10

【 0 0 7 0 】

本発明の別の例示的なアプリケーションにおいて、位置識別性は、無線ネットワーク連結性に対する機密性およびセキュリティを強化するために使用される。無線ネットワークは、無線ポータブルまたはワークステーションがネットワークに接続することを可能にする“ブルートゥース”テクノロジーのようなネットワーク装置およびプロトコルの出現と共に成年に達した。“ブルートゥース”は移動デバイス（たとえば、ラップトップ、PDA、広域携帯電話等）とポイント・ツー・ポイントおよびマルチポイントアプリケーションをサポートするデスクトップデバイスとの間におけるデジタル音声およびデータの短距離送信用の公衆の標準規格である。ネットワークによって通信しているあらゆる無線アプライアンスは特有の位置を有するため、位置識別性は、公衆ネットワークによっ

20

【 0 0 7 1 】

上述した実施形態および例示的なアプリケーションのそれぞれにおいて、ジェオロックされたデジタル情報にアクセスするアプリケーションプログラムとこれらのアプリケーションが動作する周辺およびネットワーク環境との間には少なくとも4つの論理的な境界が存在する。これらの境界には、(1)データ獲得/アプライアンスの境界、(2)記憶/アプライアンスの境界、(3)ユーザインターフェース/アプライアンスの境界、および(4)アプライアンス/位置の獲得の境界が含まれる。データ獲得/アプライアンスの境界とは、たとえば、位置識別属性が満足されない限り別のソースからデジタル情報を獲得できないアプライアンスのようなアプライアンスがデジタル情報を獲得した時点で位置識別性を実施することである。記憶/アプライアンスの境界とは、たとえば、位置識別性が満足されない限り、アプライアンスは記憶されたファイルをメモリから呼出すことができない等の、アプライアンスがデジタル情報を記憶した時点で位置識別属性を実施することである。ユーザインターフェース/アプライアンスの境界とは、たとえば、位置識別属性が満足されない限り、ユーザはアプライアンスのモニタ上でデジタル情報を見ることができない等の、ユーザに情報を与えた時点で位置識別属性を実施することである。アプライアンス/位置の獲得の境界とは、たとえば、組込み型GPS受信機を使用してそのアプライアンス位置が獲得されない限り、ユーザが如何なる方法でもそのデジタル情報を見たり、記憶したり、検索したりする、あるいはそうでなければ使用することができない等の、アプライアンス位置の妥当性を検査することによってジェオロックされたデータへのアクセスを制限することである。本発明の任意の特定の実施形態により提供される相対的なセキュリティは、アクセス制御が実施される境界に関連していることを認識すべきである。

30

40

【 0 0 7 2 】

以上、デジタル情報へのアクセスを制御するために位置識別属性を使用するシステムおよび方法の好ましい実施形態を説明してきたが、当業者には、本発明の利点が達成されていることが明らかであろう。本発明の技術的範囲内において種々の修正、適応および別の実施形態が可能であることもまた認識しなければならない。さらに、本発明は添付された請求の範囲によって制限されている。

【 図面の簡単な説明 】

50

【 0 0 7 3 】

【図 1】本発明の 1 実施形態にしたがって位置識別性により決定されたデジタル情報へのアクセスを示す概略図。

【図 2】位置識別属性の構成要素を示すブロック図。

【図 3】位置識別属性の位置決定値の構成要素を示すブロック図。

【図 4】位置識別属性をデジタル情報と関連付けるための方法を示すフローチャート。

【図 5】位置識別属性を使用してジェオロックされたデジタル情報へのアクセスを強化するための方法を示すフローチャート。

【図 6 A】アプライアンスに対する位置識別性を決定するための方法を示すフローチャート。

10

【図 6 B】アプライアンスに対する位置識別性を決定するための別の方法を示すフローチャート。

【図 6 C】アプライアンスに対する位置識別性を決定するための別の方法を示すフローチャート。

【図 6 D】アプライアンスに対する位置識別性を決定するための別の方法を示すフローチャート。

【図 7】ジェオロックされたデジタル情報をサーバ透視図から生成する方法を示すフローチャート。

【図 8】境界を付けられた方形の近接エリアに対する位置識別性からの、暗号化パラメータの計算を示す図。

20

【図 9】円形の近接エリアに対する位置識別性からの、暗号化パラメータの計算を示す図。

【図 1 0】位置識別性暗号化処理の方法を示すフローチャート。

【図 1 1】ジェオロックキーを発生する方法を示すフローチャート。

【図 1 2】ジェオロックされたデジタル情報をクライアント透視図から見る、または再生するための方法を示すフローチャート。

【図 1 3】ジェオロックキーを発生する方法を示すフローチャート。

【図 1 4】位置識別性ベースの解読処理の方法を示すフローチャート。

【図 1 5】対応したジェオロックキーを計算するために使用される境界を付けられた方形の近接エリアの一例を示す図。

30

【図 1 6】再生装置の位置がジェオロックされたデータの位置識別性と一致している、対応したジェオロックキーを計算するために使用される境界を付けられた方形の近接エリアの一例を示す図。

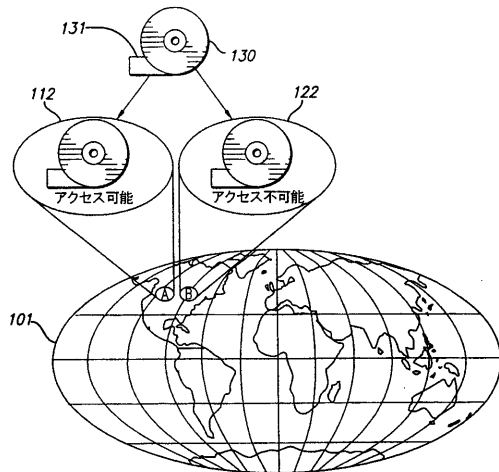
【図 1 7】再生装置の位置がジェオロックされたデータの位置識別性と一致していない、対応したジェオロックキーを計算するために使用される境界を付けられた方形の近接エリアの一例を示す図。

【図 1 8】対応したジェオロックキーを計算するために使用される円形の近接エリアの一例を示す図。

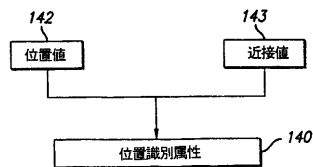
【図 1 9】対応したジェオロックキーを計算するために使用される円形の近接エリアの一例を示す図。

40

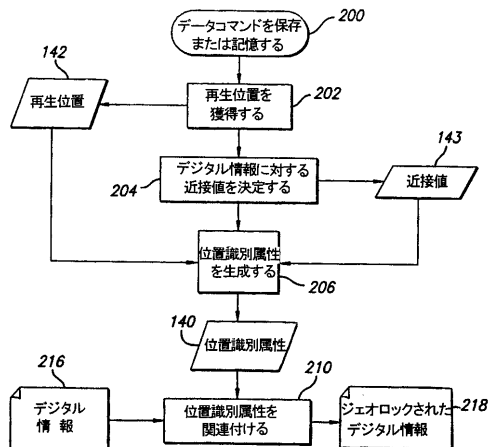
【図 1】



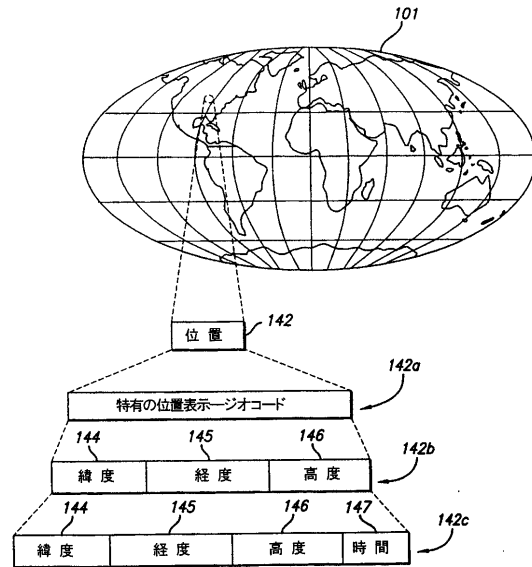
【図 2】



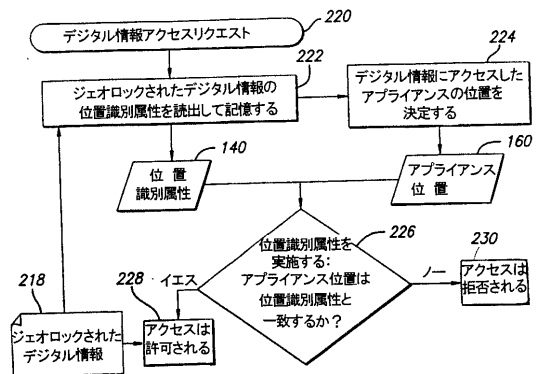
【図 4】



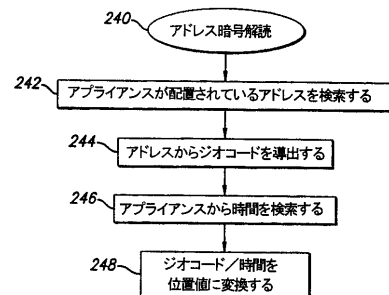
【図 3】



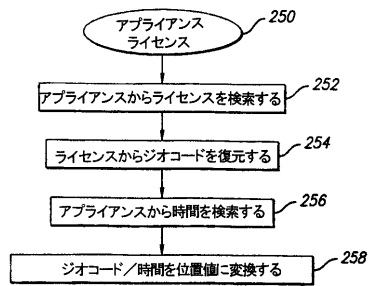
【図 5】



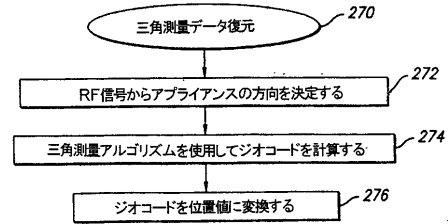
【図 6 A】



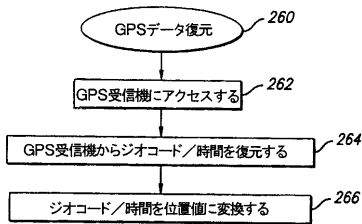
【図 6 B】



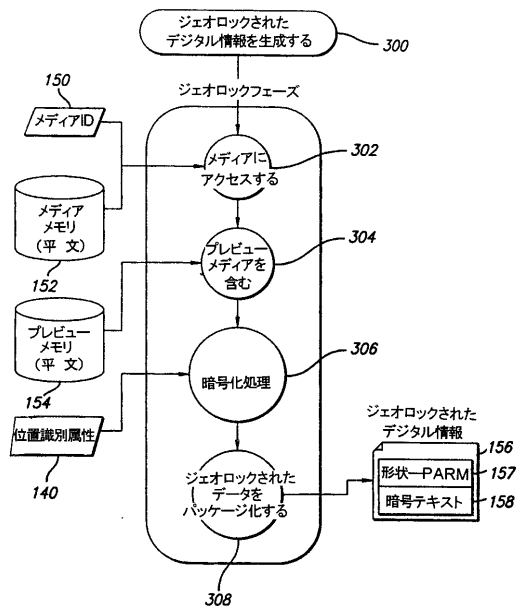
【図 6 D】



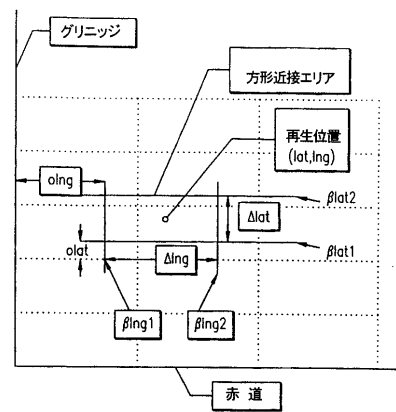
【図 6 C】



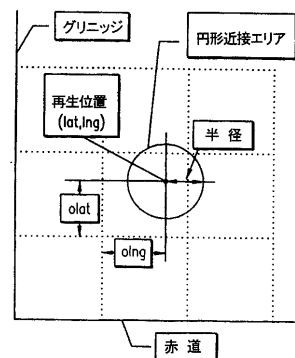
【図 7】



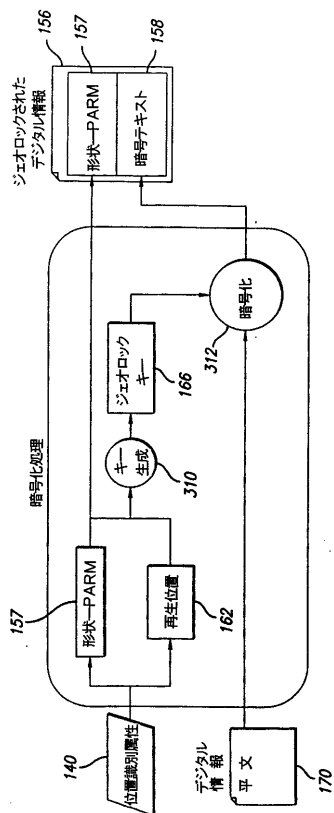
【図 8】



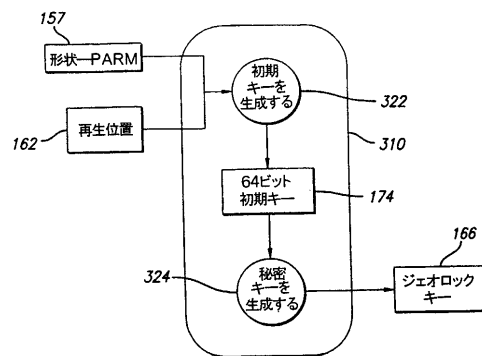
【図 9】



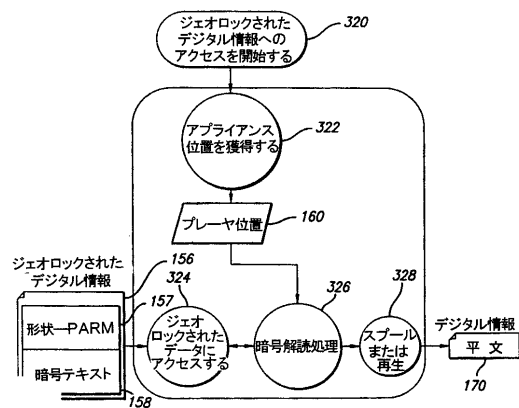
【 図 1 0 】



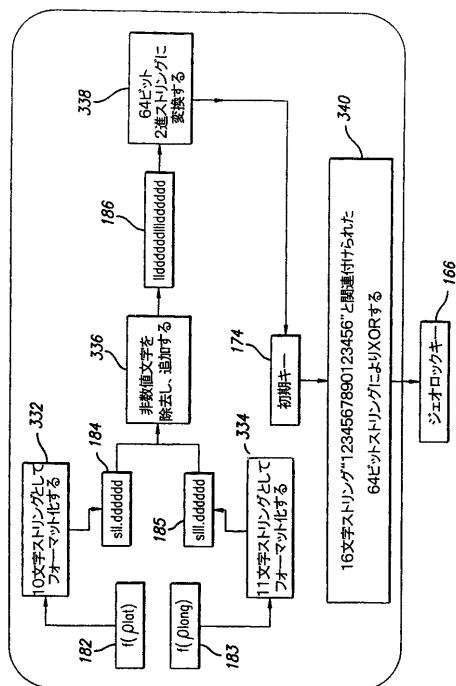
【 図 1 1 】



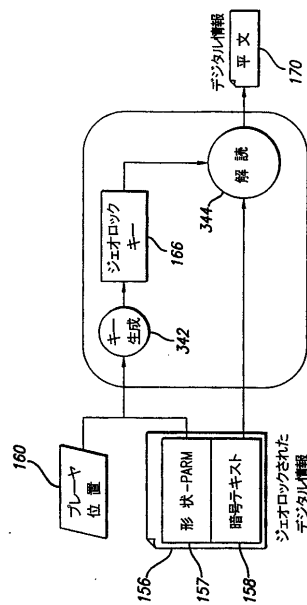
【 図 1 2 】



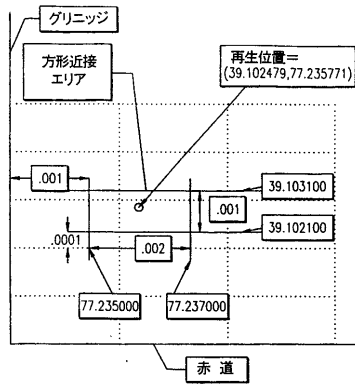
【 図 1 3 】



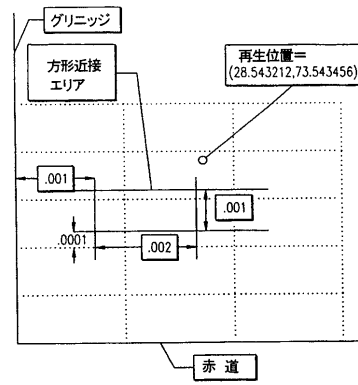
【 図 1 4 】



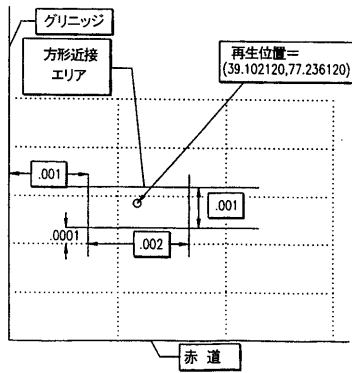
【図 15】



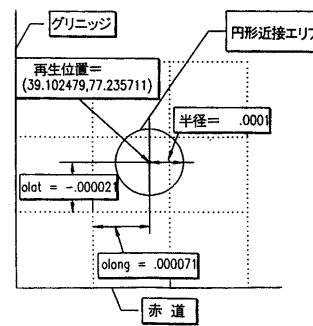
【図 17】



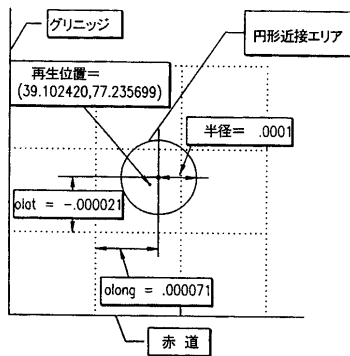
【図 16】



【図 18】



【図 19】



フロントページの続き

- (74)代理人 100075672
弁理士 峰 隆司
- (74)代理人 100109830
弁理士 福原 淑弘
- (74)代理人 100084618
弁理士 村松 貞男
- (74)代理人 100092196
弁理士 橋本 良郎
- (72)発明者 セイラー、マーク・イー
アメリカ合衆国、カリフォルニア州 90068、ロス・アンジェルス、ブレア・ドライブ 3480
- (72)発明者 グリック、バリー・ジェイ
アメリカ合衆国、ワシントン州 ディーシー 20008、キャシードラル・アベニュー・エヌダブリュ 2710
- (72)発明者 カーフ、ロナルド・エス
アメリカ合衆国、メリーランド州 20878、ガイサースバーグ、ブランディ・ホール・レーン 11425

審査官 石田 信行

- (56)参考文献 特開平11-331144(JP,A)
特開2000-163379(JP,A)
特開2000-011538(JP,A)
特開平10-040100(JP,A)
特開2002-123172(JP,A)
特開2001-053741(JP,A)
特開2002-268549(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/08
G09C 1/00
G06F 21/24