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

特許第4841095号
(P4841095)

(45)発行日　平成23年12月21日(2011.12.21)　(24)登録日　平成23年10月14日(2011.10.14)

(51)Int.Cl.			F I		
H04N	7/16	(2011.01)	H04N	7/16	Z
H04L	9/32	(2006.01)	H04L	9/00	675D
H04N	7/167	(2011.01)	H04N	7/167	Z
			H04L	9/00	673B

請求項の数 11　(全 8 頁)

(21)出願番号　特願2001-531313 (P2001-531313)
(86)(22)出願日　平成12年10月19日 (2000.10.19)
(65)公表番号　特表2003-512786 (P2003-512786A)
(43)公表日　平成15年4月2日 (2003.4.2)
(86)国際出願番号　PCT/US2000/028942
(87)国際公開番号　WO2001/030083
(87)国際公開日　平成13年4月26日 (2001.4.26)
審査請求日　平成19年10月16日 (2007.10.16)
(31)優先権主張番号　60/160,355
(32)優先日　平成11年10月19日 (1999.10.19)
(33)優先権主張国　米国(US)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫

最終頁に続く

(54)【発明の名称】保護された内容を伝送する許可を確認するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
保護されたコンテンツを受信することが可能なソース装置が前記保護されたコンテンツを、当該保護されたコンテンツをデスクランブルすることが可能なシンク装置に伝送するのを許可されていることを確認する方法であって、
前記ソース装置およびシンク装置に関連する承認コードを前記ソース装置において受信するステップを含み、
前記承認コードは、前記ソース装置および前記シンク装置に独自に関連する識別子を使用して決定され、更に、
前記ソース装置において、前記ソース装置およびシンク装置に関連するデータを使用するローカル・コードを決定するステップを含み、
前記ローカル・コードは、前記シンク装置からのデータおよび前記ソース装置内に予め貯えられたソース識別子を使用して決定され、更に、
前記ソース装置において、前記承認コードの少なくとも一部を前記ローカル・コードの少なくとも一部と比較するステップと、
当該比較に応答して前記ソース装置からの前記保護されたコンテンツを前記シンク装置が受信することが許可されていることを確認するステップと、
前記確認するステップに応答して前記シンク装置に対して前記保護されたコンテンツに対するアクセスを提供するステップと、から成る前記方法。
【請求項２】

ハッシュ計算に基づいて前記承認コードおよび前記ローカル・コードが決定される、請求項１記載の方法。

【請求項３】

前記ソース装置およびシンク装置に関連する前記識別子が一連番号またはユーザがアクセスできる他の識別コードであり、前記ハッシュ計算で使用される前記シンク装置からのデータが公開キーである、請求項２記載の方法。

【請求項４】

保護されたコンテンツを受信することが可能なソース装置が前記保護されたコンテンツを、当該保護されたコンテンツをデスクランブルすることが可能なシンク装置に伝送するのを許可されていることを確認する方法であって、

前記ソース装置およびシンク装置に関連する独自の識別子を認可当局に提供するステップと、

前記認可当局によって伝送された、前記識別子に対応するデータを使用する承認コードを前記認可当局から受信するステップを含み、

前記ソース装置において、前記ソース装置およびシンク装置に関連する前記データを使用するローカル・コードを決定するステップと、

前記承認コードの少なくとも一部を前記ローカル・コードの少なくとも一部と比較するステップと、

当該比較に応答して前記ソース装置からの前記保護されたコンテンツを前記シンク装置が受信することが許可されていることを確認するステップと、

前記確認するステップに応答して前記シンク装置に対して前記保護されたコンテンツに対するアクセスを提供するステップと、から成る前記方法。

【請求項５】

前記ソース装置がアクセス装置と媒体プレーヤのうちの１つから選択され、前記シンク装置がディジタル・テレビジョン受像機である、請求項４記載の方法。

【請求項６】

前記ソース装置に関連する前記データが、ユーザによって容易に確かめられないようセキュリティを保障される、請求項４記載の方法。

【請求項７】

前記ソース装置およびシンク装置に関連する前記データが、前記ソース装置を表示する独自の識別子と前記シンク装置に関連する公開暗号化キーとから成る、請求項４記載の方法。

【請求項８】

前記ソース装置が前記コンテンツを前記シンク装置に供給するのを許可されているかどうかの指示を提供するステップと、前記比較された承認コードとローカル・コードが一致しているかどうかを伝えるのを故意に遅延させるステップを更に含む、請求項１記載の方法。

【請求項９】

選択された装置が保護されたコンテンツを受信することを許可されていることを確認し、保護されたコンテンツにアクセスするのに使用される少なくとも１つのセキュリティ・キーおよび少なくとも１つのインデックス識別子を選択する方法であって、

第１の装置において、前記選択された装置に関連する複数のセキュリティ・キーを受信するステップと、

前記第１の装置および前記選択された装置に関連する承認コードであって、前記第１の装置、前記選択された装置、および前記インデックス識別子に一意に関連する識別子を使用して決定される、承認コードを受信するステップと、

前記第１の装置および前記選択された装置に関連するデータを使用して前記第１の装置におけるローカル・コードを決定するステップであって、該ローカル・コードは、第１の装置、前記選択された装置および前記インデックス識別子からのデータを使用して決定される、ステップと、

前記承認コードを前記ローカル・コードと比較し、当該比較に応答して前記保護されたコンテンツを前記選択された装置が受信することが許可されていることを確認するステップと、

前記第１の装置を用いて前記インデックス識別子に関連する前記複数のセキュリティ・キーのうちの１つを選択するステップとを含み、

前記複数のセキュリティ・キーは、キー・テーブル内でインデックスされ、前記インデックス識別子は、前記キー・テーブル内の前記選択されたキーのインデックスであり且つ前記インデックス識別子および前記選択された装置に関連する識別子のハッシュ関数の結果であり、更に、

前記保護されたコンテンツを前記選択された装置が受信することが許可されていることを確認すると、前記第１の装置および選択されたセキュリティ・キーを使用して、前記コンテンツを前記選択された装置に供給するステップと、から成る、前記方法。

【請求項１０】

前記コンテンツにアクセスするために前記選択された装置を表示する連番識別子を認可当局に提供するステップを更に含む、請求項９記載の方法。

【請求項１１】

前記連番識別子を使用して前記選択された装置に関連する識別子を決定するステップを更に含む、請求項１０記載の方法。

【発明の詳細な説明】

【０００１】

（産業上の利用分野）

一般に、本発明は、ディジタル・オーディオ／ビデオ送信システムに関し、特に、保護された内容（コンテンツ：ｃｏｎｔｅｎｔ）へのアクセスを検証する方法およびシステムに関する。

【０００２】

（発明の背景）

拡張された条件付きアクセス（Ｅｘｔｅｎｄｅｄ　Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ：ＸＣＡ）は、送信および蓄積の間、符号化されたディジタル・オーディオ／ビデオ（Ａ／Ｖ）の内容（コンテンツ）を保護するシステムである。拡張された条件付きアクセス・システムの下で、経済的価値のある内容は無許可のアクセスを防止するためにスクランブル（ｓｃｒａｍｂｌｅ：暗号化、混乱、変調）される。拡張された条件付きアクセスでは、スクランブルされた内容の収録を許可するが、合法的でない内容のデスクランブル（ｄｅｓｃｒａｍｂｌｅ：スクランブル解除：解読）を許可しない。合法的内容とは、オリジナルなもの、または著作権所有者によって許可（ａｕｔｈｏｒｉｚｅ）されたものである。勿論、デスクランブルとは暗号解読のプロセスをいう。非合法的内容はデスクランブルされないので視聴できない。

【０００３】

拡張された条件付きアクセス・アーキテクチャの著しい特徴は、条件付きアクセス（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ：ＣＡ）およびローカル（ｌｏｃａｌ）保護の考え方である。条件付きアクセスは番組のような保護された内容へのアクセスを特定する。取外し可能なセキュリティ装置はセキュリティに関連する機能を遂行する。経済的に価値のある内容は条件付きアクセス・サービスを使用して伝送される。例えば、ディジタル衛星システムは、加入者への大量配信のために、デスクランブル・キーおよびビデオ・コンテンツをスクランブルする。何人かの加入者はそのコンテンツを購入することに決めるであろう。その場合、加入者はデスクランブル・キーを再生／獲得するために必要なキー（ｋｅｙ）を与えられる。そのコンテンツを購入しない加入者はそのようなキーを入手することができない。これは拡張された条件付きアクセスの用語では条件付きアクセスというプロセスである。

【０００４】

拡張された条件付きアクセス・システムではリターン・チャンネルを使用し、内容にアク

セスするために使用するローカル・キーおよび識別子の検証を受ける。これを行うために、たいていの装置は何らかのリターン・パス（ｒｅｔｕｒｎ　ｐａｔｈ：戻り道）を必要とするので、問題を生じる。

【０００５】

拡張された条件付きアクセス・システム、および拡張された条件付きアクセスを呈する他のシステムにおいて保護された内容にアクセスするために使用される識別子およびキーを検証する改良された方法が望まれる。

【０００６】

（発明の概要）

条件付きアクセス・システムで保護された内容（例えば、スクランブルされたサービス）をソース（ｓｏｕｒｃｅ）装置がシンク（ｓｉｎｋ）装置に伝送するのを許可されていることを確認する方法であって、この方法は、ソース装置とシンク装置に関連するユニークな識別子を認可当局に提供するステップを含む。認可当局（ｖａｌｉｄａｔｉｏｎ　ａｕｔｈｏｒｉｔｙ）は、ソース装置およびシンク装置に関連するデータ（伝送された識別子に対応する）を使用して、承認されたコード（ａｐｐｒｏｖａｌ　ｃｏｄｅ）を決定し：ソース装置は、ソース装置およびシンク装置に関連するデータを使用してローカル・コード（ｌｏｃａｌ　ｃｏｄｅ）を決定し、承認されたコードの少なくとも一部をローカル・コードの少なくとも一部と比較して、ソース装置がその内容（コンテンツ）をシンク装置に伝送するのを許可されていることを確認する。

【０００７】

（発明の実施の形態）

本発明によれば、拡張された条件付きアクセス・システムにおける装置の所有者、使用者または操作者はリターン・パス（戻り道）の一部として利用される。しかしながら、装置の操作者をリターン・チャンネルとして利用しているとき、主要な問題に直面する。７６８ビットの数字をユーザが正確に読み取りあるいは入力することは期待できない。しかしながら、盲目的な暗号解読の攻撃（すなわち、あらゆる可能な署名を、うまく働くまで、試みること）を防止するために多くの数が必要とされる。問題は、受信されたメッセージ（例えば、公開キー）が有効であるのを確かめることである。これを行うために使用される証明書または署名（ｓｉｇｎａｔｕｒｅ）は、少なくとも長さが２０バイトで、通例、１００バイトに近い。署名は盲目的な攻撃を実行不可能にするのに十分な値を持たなければならない。本発明によれば、盲目的な攻撃を行うのに使用できるリソース（ｒｅｓｏｕｒｃｅｓ）を制限することにより、ずっと小さいキー（ｋｅｙ）スペースで同じ目的を達成することができる。

【０００８】

図１は、保護されている内容（コンテンツ：ｃｏｎｔｅｎｔ）へのアクセスを検証するシステム１０を示す。システム１０は、関連するソース識別子（ＳＯＵＲＣＥ　ＩＤ）を有するソース装置２０、関連するディジタル公開キー（ＰＵＢＬＩＣ　ＫＥＹ）を有するシンク装置、ソース装置２０のユーザ（使用者）またはオペレータ（操作者）５０、およびヘッドエンド（ｈｅａｄ　ｅｎｄ）条件付きアクセス（または信頼される第三者：Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ：ＴＴＰ）システム４０を備える。

【０００９】

ソース装置２０は、アクセス装置、例えば、衛星セットトップ・ボックス（Ｓｅｔ‐Ｔｏｐ　Ｂｏｘ：ＳＴＢ）または媒体プレーヤ、例えば、ディジタル・ビデオカセット（ＤＶＨＳ）プレーヤまたはディジタル多用途ディスク（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ：ＤＶＤ）プレーヤの形式をとり、シンク装置はディジタル・テレビジョン受像機（ＤＴＶ）の形式をとることができる。本発明の別の態様によれば、ソース装置２０とシンク装置３０は何れも公然とアクセスできる一連番号（シリアル　ナンバー：ｓｅｒｉａｌ　ｎｕｍｂｅｒ）を有する。

【００１０】

一般に、ソース装置２０からシンク装置３０に送信される内容を、それが違法に再生され

たり不正に使用されないよう保護するために、シンク装置３０の公開キーはソース装置２０に伝送される。ソース装置から供給される内容はシンク装置３０の公開キー（ＰＵＢＬＩＣ　ＫＥＹ）を使用してスクランブルされ、スクランブルされた形式でシンク装置３０に送信される。シンク装置３０は、それに対応する非公開キーを使用して、その内容をデスクランブル（ｕｎｓｃｒａｍｂｌｅ）し、シンク装置３０によるその適正な内容表示を可能にする。上述した事項は２段階のプロセスで行われ、内容は対称アルゴリズムを使用してスクランブルされ、このスクランブルのための制御ワードは公開キー（ＰＵＢＬＩＣ　ＫＥＹ）を使用して送られる。

【００１１】

シンク装置３０の公開キーとソース装置２０のソース拡張子はそれぞれ、これらの装置の一連番号を使用して信頼される第三者によって決定される。決定された公開キー（ＰＵＢＬＩＣ　ＫＥＹ）とソース識別子（ＳＯＵＲＣＥ　ＩＤ）は次に、装置２０と装置３０および信頼される第三者によって別々に使用され、内容にアクセスするために装置２０と装置３０とが組み合って動作できることを検証する。

【００１２】

ユーザ５０はソース装置およびシンク装置２０、３０から一連番号を（これらの装置から読み取って）獲得し、ヘッドエンド（ｈｅａｄ　ｅｎｄ）条件付きアクセス・システムにコール（ｃａｌｌ）して、ソース装置２０とシンク装置３０とが組み合って使用できるようにする。ユーザ５０は一連番号（図に５２で示す）をヘッドエンド条件付きアクセス・システム４０に供給する。これらの一連番号は、例えば、音声で、あるいは電子的に、あるいは音響的に供給することができる。ヘッドエンド条件付きアクセス・システム４０は、供給された一連番号をソース識別子（ＳＯＵＲＣＥ　ＩＤ）と公開キー（ＰＵＢＬＩＣ　ＫＥＹ）データに変換するデータベースにアクセスできる。従って、ヘッドエンド条件付きアクセス・システム４０は、例えば、ルックアップ・テーブルを利用して、伝送されたこれらの一連番号から、ソース装置２０のソース拡張子データとシンク装置３０の公開キー・データを識別する。本発明の別の態様によれば、一連番号とソース拡張子との関係は公開のものでなく容易に確かめられない、ということは重要である。

【００１３】

図１で、ヘッドエンド条件付きアクセス・システム４０は、これら２つの値（例えば、ソース拡張子と公開キー）のハッシュ・コード（ｈａｓｈ　ｃｏｄｅ）を承認ハッシュ（ａｐｐｒｏｖａｌ　ｈａｓｈ）として計算して、それをパーソナル識別番号（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ：ＰＩＮ：図に４２で示す）としてユーザ５０に供給する。ユーザ５０は、次に、このパーソナル識別番号（図に５４で示す）をソース装置２０の中に入力する。ソース装置２０は、同じハッシュを、ソース装置２０内に在るソース識別子（ＳＯＵＲＣＥ　ＩＤ）およびシンク装置３０から供給される公開キー（ＰＵＢＬＩＣ　ＫＥＹ：３４で示す）を使用してローカル・ハッシュとして計算している。パーソナル識別番号がそのハッシュとマッチ（ｍａｔｃｈ）すれば、ソース装置２０は、シンク装置３０から供給された公開キー（３４）が有効であり且つヘッドエンド条件付きアクセス・システム４０がこのキーを与えられたことを認めると共に、ソース装置２０とシンク装置３０とが互いに組み合って動作することを許可するように、ヘッドエンド条件付きアクセス・システムがそのキーの使用を承認することを認める。

【００１４】

本発明の別の態様によれば、ソース識別子および／またはハッシュ計算のアルゴリズムは秘密にされる。当業者に理解されるように、潜在的な「盗用：ｐｉｒａｔｅ」はこれをハッシュ機能（ｈａｓｈ　ｆｕｎｃｔｉｏｎ）に入力しないという事実は、より強力なコンピュータを使用する盲目的な攻撃を効果的に防止する。

【００１５】

本発明の別の態様によれば、パーソナル識別番号コードは大きなスペースを有するので、有効な署名の検索は長時間を要する。これを達成する１つの方法は、複雑な計算で、あるいは計算後の待ち時間で、パーソナル識別番号コードを承認するために、ソース装置２０

にかなりの時間を取らせることである。このアプリケーション（例えば、家庭用Ａ／Ｖネットワークのコピー保護）に提案される値は、９桁または１０桁のパーソナル識別番号、および１秒の計算時間である。これによって、平均検索時間は５×１０^{8}秒または５×１０^{9}秒、すなわち約１６年乃至１６０年が強いられるであろう。

【００１６】

本発明の別の態様によれば、ハッシュ機能への別の入力は、タイトル・コード（ｔｉｔｌｅ　ｃｏｄｅ）または媒体（例えば、テープまたはＤＶＤ）の一連番号である。これにより、個々のタイトルまたはテープは承認されるかまたは承認されない。一定のユーザ５０に対する一連番号をヘッドエンド条件付きアクセス・システム４０内に貯えることにより時間を著しく節約することができ、ユーザ５０は各トランザクション（ｔｒａｎｓａｃｔｉｏｎ：処理、取引）ごとにそれら（一連番号）を備える必要がない。

【００１７】

本発明の別の態様によれば、ハッシュ機能への別の入力は、最初の承認以来の全ランニング・タイムまたは経過時間を表示することができる。これにより、一定の時間後または使用後に承認は自動的に失効する。もし追加のタイム・コードが必要とされるなら、これはソース装置２０からユーザ５０に合図することができる。タイム・コードは、次のタイム・コードが何であるかをユーザ５０が効果的に推測または予測できないようにランダムにすべきである。もしこれをすることがユーザ５０にできたなら、ユーザは前もってコールイン（ｃａｌｌ　ｉｎ）し、パーソナル識別番号コードをそれが必要とされる前に得ることによって自分のシステムに事前に許可を与えることができるであろう。

【００１８】

本発明の更に別の態様によれば、別のパーソナル識別番号コードに基づくシステムは、ネットワークごとに独自のキーを使用するというセキュリティの極限にまで至らずに、ローカル・ネットワークのキー（ｋｅｙ）スペースをより小さいセグメントに分割することに基づいている。

【００１９】

図２は、保護された内容へのアクセスに使用されるキーおよび識別子を検証するのに適する別のシステム１００を示す。システム１００は、関連するソース識別子（ＳＯＵＲＣＥ　ＩＤ）を有するソース装置１２０、関連する公開キー（ＰＵＢＬＩＣ　ＫＥＹ）を有するシンク装置１３０、ソース装置１２０のユーザまたはオペレータ１５０、およびヘッドエンド条件付きアクセス・システム１４０を備える。

【００２０】

比較的少数（例えば、１０，０００）の非公開キーを有するシンク装置を作ることができる。ユーザはシンク装置１３０とソース装置１２０の一連番号（図にそれぞれ、１３２、１２２で示す）を読み取る。ユーザ１５０は、次に、ヘッドエンド条件付きアクセス・システム１４０の中にコール（ｃａｌｌ）し、シンク装置１３０とソース装置１２０の一連番号（１５２）を供給し、このシンク装置１３０のパーソナル識別番号コード（１４２）を受信する。パーソナル識別番号コードはルックアップ・テーブルにより、または計算により決定される。ユーザ１５０は、次に、このパーソナル識別番号コード（１５４で示す）をソース装置１２０の中に入力し、ソース装置１２０は、公開キー・テーブル１６０を使用して、シンク装置１３０に使用する正確な公開キーにインデックス（ｉｎｄｅｘ）する。

【００２１】

公開キー・テーブル１６０はソース装置１２０の蓄積容量に比較して大きい。テーブル１６０は暗号化されており、予め記録された媒体（例えば、テープ）の開始時に貯えられる。これにより、予め記録されたテープはネットワークを初期設定するのに使用されるので、公開キー（ＰＵＢＬＩＣ　ＫＥＹ）を必要なときに獲得するための容易な機構が得られる。その後、シンク装置１３０に使用する適正なキーをソース装置１２０が記憶するので、システム１００は自力で働く。

【００２２】

テープのような予め記録された媒体は、従来、より強力な何か他の暗号化システムで暗号化されている。本発明においては、ソース装置１２０からシンク装置１３０へのディジタル・リンクのみが、この比較的弱いローカル・キーで暗号化されている。ローカル・キーが、このネットワークに独自のものでない限り、もし各タイトルごとにそのテープにつき１０，０００の異なるバージョンが必要とされるなら、素材のコピーを１０，０００作って利益を得るのは非常に困難であろう。

【００２３】

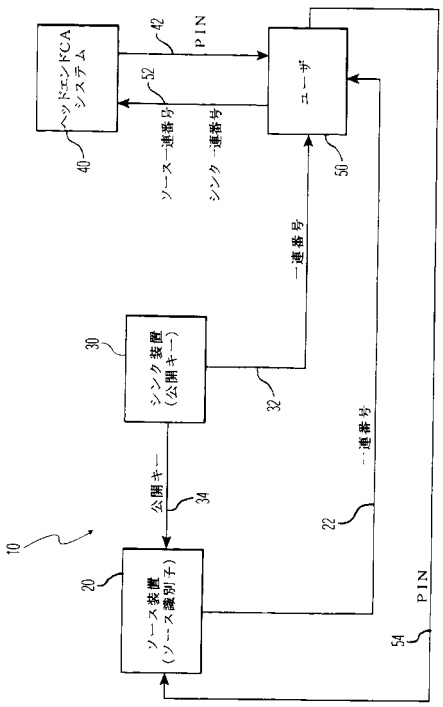
上記のシステム１００のローカル・キー１０，０００のうち１つが知られると、「盗用：ｐｉｒａｔｅ」ユーザは、任意のソース装置１２０を使用してコンテンツをプレー（ｐｌａｙ）できるようにするために、同じパーソナル識別番号コードを絶えず使用するかもしれない。システム１００は、パーソナル識別番号コードをソース識別子（ＳＯＵＲＣＥＩＤ）のハッシュ機能にすることにより、また公開キー・テーブル１６０の中にインデックスすることにより、改善される。これにより、ユーザ５０は各ソース装置１２０について独自のパーソナル識別番号を獲得することを強いられる。もしインデックス・テーブル１６０内の一定の公開キーについて圧倒的に多数のリクエストが入ってくるなら、それは非公開キーが危うくなっていることの合図とされる。

【図面の簡単な説明】

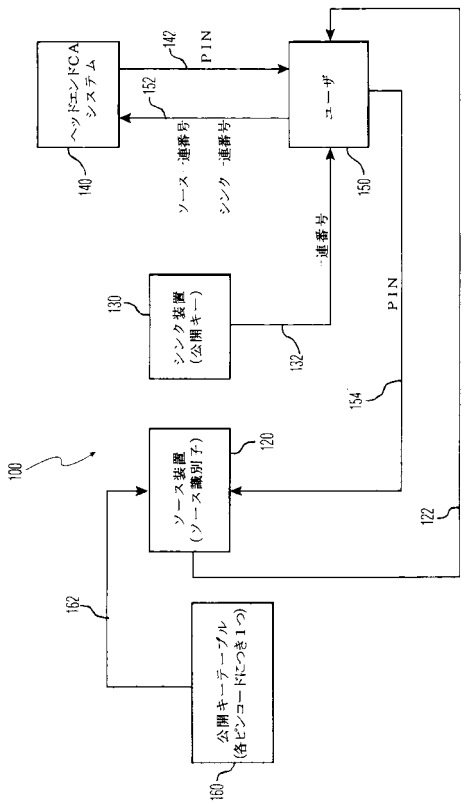
【図１】　本発明の第１の態様に従うシステムを例示する。

【図２】　本発明の第２の態様に従うシステムを例示する。

【図１】



【図２】



フロントページの続き

(72)発明者　ダフイールド，デイビツド　ジエイ
アメリカ合衆国　インデイアナ州　インデイアナポリス　フオール・クリーク・ロード　５４５９
(72)発明者　デイース，マイケル　スコット
アメリカ合衆国　インデイアナ州　ザイオンズビル　インデイアン・パイプ・レーン　１１０３

審査官　三森　雄介

(56)参考文献　特開平１１－２０５３０５（ＪＰ，Ａ）
特開平１１－１６８４５９（ＪＰ，Ａ）
特開平１１－２６１７３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 7/14- 7/173
H04N 5/38- 5/46
H04L 9/00- 9/38
G06F 12/14,21/24
G06F 21/02-21/06