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

特許第4621359号
(P4621359)

(45)発行日　平成23年1月26日(2011.1.26)　(24)登録日　平成22年11月5日(2010.11.5)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06K 19/07	(2006.01)	G06K	19/00	N
G06F 21/24	(2006.01)	G06F	12/14	550A
G06F 21/20	(2006.01)	G06F	15/00	330A
G06K 19/00	(2006.01)	G06K	19/00	Q

請求項の数 7　(全 12 頁)　最終頁に続く

(21)出願番号　特願2000-611462 (P2000-611462)
(86)(22)出願日　平成12年3月31日 (2000.3.31)
(65)公表番号　特表2002-542672 (P2002-542672A)
(43)公表日　平成14年12月10日 (2002.12.10)
(86)国際出願番号　PCT/EP2000/002918
(87)国際公開番号　WO2000/062505
(87)国際公開日　平成12年10月19日 (2000.10.19)
審査請求日　平成19年3月8日 (2007.3.8)
(31)優先権主張番号　99/04767
(32)優先日　平成11年4月13日 (1999.4.13)
(33)優先権主張国　フランス(FR)

(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　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】デジタルホームネットワークとデジタルホームネットワークの作成及び更新方法

(57)【特許請求の範囲】

【請求項１】

ローカルデジタルネットワークに接続されるよう適応された、該ローカルデジタルネットワーク内を流れるデータを受信する提示装置であって、前記データは前記ローカルデジタルネットワークに接続されたアクセス装置において暗号化されており、当該提示装置は状態インジケータを含んでおり、該状態インジケータは、当該提示装置が、前記受信されたデータを復号するための、前記ローカルデジタルネットワークに固有の復号鍵（$K_{PRI.LOC}$）を含んでいるかどうか、および、当該提示装置が、前記ローカルデジタルネットワークに接続されるのに適した任意の新しい提示装置に前記復号鍵を送信することが許可されているかどうかを示すものである、提示装置。

【請求項２】

請求項１記載の提示装置であって、当該提示装置の第１の状態であるバージン状態（ＩＥ＝００）が、当該提示装置がローカルデジタルネットワークに初めて接続されたのであり、該ローカルデジタルネットワークに固有の復号鍵を含んでいないことを示す、提示装置。

【請求項３】

請求項２記載の提示装置であって、当該提示装置の第２の状態である親状態（ＩＥ＝０１）が、当該提示装置が前記ローカルデジタルネットワークに固有の復号鍵を含んでおり、前記ローカルデジタルネットワークに接続されるのに適した任意の新しい提示装置に前記復号鍵を送信することが許可されていることを示す、提示装置。

【請求項４】
請求項３記載の提示装置であって、当該提示装置の第３の状態である無効状態（ＩＥ＝１０）が、当該提示装置が前記ローカルデジタルネットワークに固有の復号鍵を含んでおり、前記ローカルデジタルネットワークに接続されるのに適した任意の新しい提示装置に前記復号鍵を送信することは許可されていないことを示す、提示装置。
【請求項５】
状態の変化が、
・バージン状態から親状態へ、または、
・親状態から無効状態へ、または、
・バージン状態から無効状態へ、
移行するようにのみ起こるよう適応されている、請求項４記載の提示装置。
【請求項６】
請求項５記載の提示装置であって、当該装置が親状態にある場合は、当該装置が前記ローカルデジタルネットワークに接続された親状態にある唯一の提示装置であることを特徴とする、提示装置。
【請求項７】
請求項１ないし６のうちいずれか一項記載の提示装置であって、前記状態インジケータが、当該提示装置に挿入されることのできるスマートカードに含まれることを特徴とする、提示装置。
【発明の詳細な説明】
【０００１】
本発明は、一般的には、ローカルデジタルネットワークの分野に係り、特に、デジタルホームネットワークの分野に関する。
【０００２】
このようなネットワークは、たとえば、IEEE 1394標準に準拠したバスのようなデジタルバスによって相互連結された装置の組により構成される。ネットワークは、２種類の装置、すなわち、
ローカルネットワークの外部から発したデータを受信し、そのデータを、接続されているネットワークのあるポイントに送信することができるアクセス装置と、
ネットワーク内を流れるデータを、接続されているネットワークの別のポイントにて提示するために受信するよう適合された提示装置と、
を有する。上記第２のタイプの装置は、ローカルネットワークの外部とのリンクを具備していない。
【０００３】
オーディオ及び／又はビデオデータを住宅の種々の部屋へ伝達することを目的としたデジタルホームネットワークの一例を考えると、アクセス装置は、ネットワークの外部から衛星アンテナ若しくはケーブルコネクションを介してビデオ番組を受信するデジタルデコーダ又はセットトップ・ボックス、或いは、光ディスクから読み出したデータ（オーディオ及び／又はビデオ）をデジタル形式でネットワーク上でブロードキャストする光ディスクの読取装置である（本例の場合に、ディスクはネットワークの外部から発したデータを収容する）。提示装置は、たとえば、ネットワークから受信したビデオ番組を見ることができるようにするテレビジョン受像機、或いは、より一般的には、受信したデジタル情報をエンドユーザへブロードキャストするため、受信したデジタル信号をアナログ形式に変換することができる装置である。
【０００４】
上述のタイプのホームネットワークは、ネットワークの外部とのリンクを具備せず、ネットワーク内を流れるデータを記録する機能を有する第３のタイプの装置を含む。この第３のタイプの装置の一例として、特に、デジタルビデオレコーダ、又は、ＤＶＤ（デジタル汎用ディスク）タイプの光ディスクを記録できる装置を挙げることができる。
【０００５】

同一の装置が、上述の二つ以上の異なる装置カテゴリーに属し得ることに注意する必要がある。たとえば、光ディスクを記録する装置は、商業的に予め記録されたディスクを読み取ることも可能なので、上述の第１の装置のカテゴリーと第３の装置のカテゴリーに同時に属している。

【０００６】

ローカルネットワークの外部から発したデータを供給するコンテンツプロバイダ、特に、有料テレビ番組をブロードキャストするサービスプロバイダ、若しくは、たとえば、その他の光ディスクの発行元の立場を考えると、これらの伝送されたデータがコピーされること、及び、（たとえば、光ディスク若しくはその他の記録媒体へコピーされることによって）あるローカルネットワークから別のローカルネットワークへ容易に流出し得ることを防止する必要がある。

【０００７】

このため、実際には、鍵を使用する暗号化アルゴリズムを用いてデータを暗号化することにより、データを秘密形式で伝送することが知られている。この鍵は、これらのデータを受信することが許可されている装置に対し事前に公開されているか、或いは、コンテンツプロバイダとそれらの装置との間で特定の安全なプロトコルに従って交換される。

【０００８】

デジタルホームネットワークを保有するユーザの立場を考えると、これらのデータは、ネットワーク内の１台の装置がコンテンツプロバイダからデータを受信する権利を付与されているときには、ネットワークの他の全ての装置へ送信可能であることが望ましい。したがって、有料テレビサービスの加入者であり、かつ、（暗号形式で送信された）番組をラウンジに設置された（番組の復号化を許可された）セットトップ・ボックスで受信するユーザは、これらの番組を、たとえば、寝室に設置されたテレビジョンで視聴できることを希望する。さらに、ユーザは、受信した番組を記録し、後で、たとえ、その有料テレビサービスの加入者ではなくなったときでも、ネットワークの数台の装置でその番組を視聴できることに関心がある。

【０００９】

コンテンツプロバイダの要望と、ユーザの要望とを考慮することにより、本発明は、ローカルデジタルネットワークで受信されたデータがネットワークの種々の装置の間で自由に流れつつも、そのデータがあるローカルネットワークから別のローカルネットワークへ流れることは阻止される手段を提供することを目的とする。

【００１０】

この目的を達成するため、本発明が提案するローカルデジタルネットワーク、特に、デジタルホームネットワークは、

ネットワークの外部から発するデータを受信し、そのデータをネットワークのあるポイントへ送信することができる少なくとも一台のアクセス装置と、

データが暗号形式だけで流れるように適応したネットワーク内を流れるデータを受信するよう適応し、ネットワークのあるポイントでそのデータを提示する少なくとも一台の提示装置と、

を有する。本発明によれば、ネットワークの全ての装置は、ネットワークを流れるデータの暗号化及び復号化のため、ネットワークに特有の単一の暗号鍵、すなわち、ネットワークのローカル鍵を使用する。

【００１１】

各ローカルネットワークは、他のローカルネットワークのローカル鍵とは異なる固有のローカル鍵を保有するので、ローカルネットワークへ入った情報は、ネットワークの全ての装置が同じように読むことができるが、他のローカルネットワークで読むためにコピーすることはできない。より正確に表現すると、情報は、暗号形式でコピーすることができるが、その情報がコピーされたローカルネットワークとは異なる別のローカルネットワークにおいてはその情報を再生できない。したがって、本発明は、コンテンツプロバイダの要望と、ユーザの要望の両方を満たす。

【００１２】
本発明の好ましい一局面によれば、データは、非対称暗号システムと呼ばれる、公開鍵による暗号システムを用いて暗号化される。ネットワークのローカル鍵は、本例の場合に、公開鍵と秘密鍵のペア、すなわち、ネットワークのローカル公開鍵とローカル秘密鍵とによって構成される。
【００１３】
好ましくは、ネットワークに接続された提示装置だけがローカル秘密鍵を知っている。
【００１４】
具体的な一実施例によれば、所与の時点においては、ネットワークのある単一の提示装置が、ローカル秘密鍵を、ネットワークに接続するのに適した新しい提示装置へ送信することを許可される。この装置は、以後、ネットワークの「親」と呼ばれる。
【００１５】
ネットワークの「親」である装置が、特に、最初のローカルネットワークと同じローカル鍵を保有する不正ローカルネットワークを作成するために、ローカルネットワークから取り外された場合には、最初のローカルネットワークのどの装置も、ローカル秘密鍵を、最初のローカルネットワークに接続するのに適した新しい提示装置へ送信し得なくなるので、最初のローカルネットワークは変更できなくなる。
【００１６】
本発明のもう一つの局面によれば、ある所与の時点で、提示装置は、以下の状態の中でただ一つの状態だけを取ることができる。
【００１７】
ｉ）提示装置が最初にネットワークへ接続されたときのバージン状態である第１の状態。
【００１８】
ｉｉ）提示装置が、ネットワークのローカル秘密鍵を、該ネットワークに接続するのに適した任意の新しい提示装置へ送信することが許可された親状態である第２の状態。
【００１９】
ｉｉｉ）提示装置が、ネットワークのローカル秘密鍵を、該ネットワークに接続するのに適した任意の新しい提示装置へ送信することがもはや許可されなくなる無効状態である第３の状態。
【００２０】
提示装置は、上位ランクの状態へ移る場合に限り、すなわち、バージン状態から親状態へ、或いは、親状態から無効状態へ移る場合に限り、状態を変更することができる。
【００２１】
本発明の好ましい一局面によれば、ネットワークのある単一の提示装置が第２の状態、すなわち、ネットワークの親である親状態にある。
【００２２】
具体的な一実施例によれば、所与の時点で、ネットワークの親は、ネットワークに最後に接続された提示装置である。
【００２３】
したがって、ネットワークの親の称号は、ローカルネットワークに接続された新しい提示装置へ渡される。これにより、単一の親提示装置から始めて、同じローカル鍵を有する一連のローカルネットワークを作成する不正行為を可能にすることが阻止される。
【００２４】
また、本発明は、上述のように、デジタルネットワークに接続されるよう適応し、所与の時点で、上述のバージン状態、親状態又は無効状態の中のいずれか一つの状態だけを取ることができ、上位ランクの状態へ移るような状態の変更だけを行うように適応した提示装置に関する。
【００２５】
本発明の一局面によれば、提示装置がバージン状態にあるとき、提示装置は、固有の公

開鍵と秘密鍵のペアを保有しており、接続されるのに適したネットワークのローカル鍵のペアを受信し、固有の鍵のペアの代わりに受信したローカル鍵のペアを保持することが許可される。

【００２６】

本発明のもう一つの局面によれば、提示装置が無効状態にあるとき、提示装置は、接続されるのに適したネットワークのローカル鍵のペアを受信することが許可されなくなる。

【００２７】

本発明のもう一つの局面によれば、提示装置は、上記提示装置が占める状態を保持する手段を有し、この記憶手段はスマートカードに統合されている。

【００２８】

本発明の更に別の局面によれば、ネットワークのローカル鍵のペアは、上記提示装置に装備されたスマートカード内に収容されている。

【００２９】

また、本発明は、上述のネットワークのようなネットワークを作成し、更新する方法に関する。この方法については後述する。

【００３０】

本発明のその他の特徴及び利点は、添付図面と共に、以下の本発明の具体的、例示的な実施例の説明から明らかになるであろう。

【００３１】

添付図面を通じて、本発明と、以下に説明する本発明の具体的な実施例とを理解するために重要な要素だけが示されている。

【００３２】

アクセス装置１と、２台の提示装置２と、一般的にＤＶＣＲ（デジタルビデオカセットレコーダの略）と称されるデジタルビデオレコーダ４とを含むデジタルホームネットワークが図１に示されている。装置１、２、３及び４の組立体は、たとえば、ＩＥＥＥ１３９４標準に準拠した家庭用デジタルバスＢに接続される。

【００３３】

アクセス装置１は、スマートカード１１を装備したスマートカードリーダを具備したデジタルレコーダ１０を含む。このデジタルレコーダ１０は、衛星アンテナ、又は、ケーブルネットワークに接続され、サービスプロバイダによって配信されるビデオ番組を受信する。これらの番組は、たとえば、ＭＰＥＧ２フォーマットのデータのストリームＦで受信される。公知の方法で、これらの番組は、スクランブルをかけられた形式で伝送され、そのコンテンツは、制御語ＣＷによってスクランブルされている。これらの制御語は、それ自体が、伝送中に秘密の状態を保ったままとなるような仕方で、ある所与の暗号化アルゴリズムに従って鍵Ｋを用いて暗号化された形式で、データストリームＦ中で伝送される。

【００３４】

かくして、サービスプロバイダによって許可されたユーザだけが（たとえば、申込料金の対価として）伝送されたデータを復号化する権能を付与される。このため、プロバイダは、許可されたユーザに、制御語ＣＷを復号化するため役立つ鍵Ｋを供給する。非常にしばしば、番組を受信する権能は、ユーザが自分の申込料金を支払う間に限られた一時的な権能である。したがって、鍵Ｋは、サービスプロバイダによって定期的に変更される。

【００３５】

本発明によれば、以下に説明するように、ユーザは、自分が加入している間に伝送された番組を記録し、自分が加入者ではなくなった場合でも、その番組を自分のネットワーク上で好きなだけしばしば再生することができる。これに対し、データは、暗号形式で記録されるので、そのデータを記録したユーザのネットワーク以外のネットワークではそのデータを再生することができない。

【００３６】

図１において、ネットワークの状態は、全ての装置が図２及び３を参照して後述する処理に応じて接続されている状態である。

【００３７】
次に、デコーダ１０によって受信されたストリームＦで伝送されたデータが処理される様子を説明する。当業者には公知のように、ＭＰＥＧ２フォーマットに従って伝送されたデータの場合、データストリームＦは、一連のビデオデータパケット、オーディオデータパケット、及び、管理データパケットを含む。管理データパケットは、特に、制御メッセージＥＣＭ（権利制御メッセージの略）を含む。制御メッセージＥＣＭでは、ビデオパケット及びオーディオパケットで伝送されたデータにスクランブルをかけるため利用される制御語ＣＷが、鍵Ｋを用いた暗号形式で伝送される。
【００３８】
このデータストリームＦは、スマートカード１１へ送信され、スマートカード内で処理される。データストリームＦは、デマルチプレクサ回路（ＤＥＭＵＸ）１２によって受信され、デマルチプレクサ回路は、ＥＣＭをアクセス制御回路ＣＡ１３へ送信し、スクランブルをかけられたビデオデータ及びオーディオデータのパケットＤＥをマルチプレクシング回路（ＭＵＸ）１５へ送信する。回路ＣＡは、鍵Ｋを保持し、ＥＣＭに収容された制御語ＣＷを復号化することが可能である。回路ＣＡは、これらの制御語ＣＷを変換器回路１４へ送信する。本発明によれば、変換器回路１４は、ネットワークのローカル公開鍵$K_{PUB.LOC}$を保持する。変換器回路１４は、この鍵$K_{PUB.LOC}$を使用し、制御語ＣＷを暗号化し、ローカル公開鍵を使用して暗号化されたこれらの制御語を、制御メッセージＬＥＣＭでマルチプレクシング回路１５へ送信する。これらのメッセージＬＥＣＭは、初期データストリームＦで受信されたメッセージＥＣＭと同じ機能を備えているが、メッセージＬＥＣＭの場合、制御語ＣＷは、サービスプロバイダの鍵Ｋを用いて暗号化されるのではなく、ローカル公開鍵$K_{PUB.LOC}$を用いて暗号化されている点が相違する。
【００３９】
マルチプレクシング回路１５は、データパケットＤＥと、変換された制御メッセージＬＥＣＭを、データストリームＦ’として送信し、データストリームＦ’はデコーダ１０によって受信される。家庭用バスＢのあちらこちらを流れるデータストリームは、このデータストリームＦ’であり、データストリームＦ’は、いずれか１台の提示装置２又は３によって受信され、或いは、デジタルビデオレコーダ４によって受信され、記録される。本発明によれば、データは、バスＢ内を常に暗号形式で流れ、ネットワークのローカル秘密鍵$K_{PRI.LOC}$を収容する装置だけが制御語ＣＷを復号化し、データＤＥを復号化し得る。したがって、これは、図１の家庭用ネットワークで作成されたいかなるコピーが他のローカルネットワークへブロードキャストされることをも阻止する。
【００４０】
図１の例の場合に、回路１２乃至１５は、スマートカード１１と一体化してもよいが、他の変形例では、回路ＤＥＭＵＸ及び回路ＭＵＸはデコーダ１０に収容し、残りの回路１３及び回路１４がスマートカードに一体化される。特に、回路ＣＡ１３及び変換器回路１４は、復号鍵及び暗号鍵を収容するので、これらの回路は、スマートカードのような安全な媒体に組み込まれる。
【００４１】
提示装置２は、スマートカード２１を搭載したスマートカードリーダを具備したデジタルテレビジョン受像機（ＤＴＶ１）２０を含む。受像機２０は、バスＢを介して、デコーダ１０、若しくは、デジタルビデオレコーダ４から発生されたデータストリームＦ’を受信する。データストリームＦ’は、スマートカード２１へ送信される。データストリームＦ’は、デマルチプレクサ回路（ＤＭＵＸ）２２で受信され、デマルチプレクサ回路（ＤＭＵＸ）２２は、スクランブルをかけられたビデオデータパケット及びオーディオデータパケットＤＥを、スクランブル解除回路（ＤＥＳ．）２４へ送信し、変換された制御メッセージＬＥＣＭを端末モジュール２３へ送信する。端末モジュールは、ネットワークの公開鍵（$K_{PUB.LOC}$）と秘密鍵（$K_{PRI.LOC}$）のペアを収容する。制御メッセージＬＥＣＭは、ネットワークのローカル公開鍵$K_{PUB.LOC}$を用いて暗号化された

制御語ＣＷを収容するので、端末モジュールは、ネットワークのローカル秘密鍵$K_{PRI.LOC}$を用いて、これらの制御語を復号化することができ、制御語ＣＷを平文で取得することができる。これらの制御語ＣＷは、スクランブル解除回路２４へ送信され、スクランブル解除回路２４は、データパケットＤＥのスクランブルを外すためこれらの制御語ＣＷを使用し、平文のデータパケットＤＣをテレビジョン受像機２０へ出力する。

【００４２】

平文データＤＣがスマートカード２１と、テレビジョン受像機２０のディスプレイ回路との間で最終的に伝送されることを確保するため、スマートカードと、受像機２０のカードリーダとの間のインタフェースＩは、スマートカードの安全性を確保するため、たとえば、米国ＮＲＳＳ標準（ナショナル・リニューワブル・セキュリティ・スタンダード）に準拠して作成される。

【００４３】

第２の提示装置３は、スマートカード３１が搭載されたスマートカードリーダを具備したデジタルテレビジョン受像機（ＤＴＶ２）３０を含み、第１の提示装置２と全く同様に動作するので、これ以上の説明を加えない。

【００４４】

上述のローカルデジタルネットワークを用いることにより、コンテンツプロバイダから生じたデータストリームＦは、データストリームＦを受信するアクセス装置によって、ネットワークのローカル公開鍵$K_{PUB.LOC}$を用いてデータストリームＦ’へ変換される。このデータストリームＦ’は、ローカルネットワークに特有のフォーマットを有し、このデータは、ローカルネットワークのローカル秘密鍵を保持するこのローカルネットワークの提示装置以外の装置では復号化し得ない。

【００４５】

次に、図１のローカルデジタルネットワークが作成される態様、及び、ネットワークの全ての装置がネットワークの固有のローカル鍵のペアを共用することを保証するように、新しい装置のこのローカルネットワークへの接続が管理される態様を説明する。

【００４６】

本発明によるデジタルネットワークを作成するため、アクセス装置と提示装置を一体的に接続する必要がある。

【００４７】

図２では、最初に、ネットワークは、デジタルバスＢを用いて、アクセス装置１と提示装置２を接続することにより作成される場合を考える。ネットワークを作成する処理の種々の手順は、二つの装置の間で行われるやり取りを示すような形で時間軸ｔに沿って表わされている。

【００４８】

この処理の第１のステップ１００において、２台の装置が一つに接続されたとき、提示装置は、公開鍵K_{PUB2}と秘密鍵K_{PRI2}のペアを収容し、本発明によれば、バージン状態にある。

【００４９】

装置の状態は、好ましくは、提示装置の端末モジュール２３（図１）に設けられた２ビットのレジスタである状態インジケータＩＥによって記憶される。慣例的に、装置がバージン状態であるとき、状態インジケータＩＥは００に一致し、装置が親状態であるとき、ＩＥ＝０１であり、装置が無効状態であるとき、ＩＥ＝１０であるとする。

【００５０】

状態インジケータＩＥは、耐タンパー性が保証されるように、スマートカード内の集積回路に収容される。

【００５１】

提示装置が製造元によって販売されたとき、本発明のタイプの既設のローカルネットワークに接続可能でなければならない。また、提示装置は、新しいネットワークを作成するようにアクセス装置へ接続可能でなければならない。そのため、本発明に従って製造され

た提示装置は、提示装置毎に固有であり、他の提示装置のものとは異なる公開鍵と秘密鍵のペアを必ず保持し、これにより、本発明に従って作成された各ローカルネットワークが、ユニークな鍵のペアを保持することを保証する。さらに、やり取りの機密性を保証するため、使用される全ての秘密鍵／公開鍵のペアは、当業者に公知の方法に応じて認証される。

【００５２】

アクセス装置は、暗号鍵／復号鍵を保持しない状態で製造、販売される。アクセス装置は、好ましくは、図１に関して説明したように、本発明による（スマートカードに収容された）変換器回路を含み、接続されるネットワークのローカル鍵を記憶することができる。

【００５３】

図２を参照するに、この処理のステップ１０１において、提示装置２は、バス２を介して、バスＢに接続される資格のある全てのアクセス装置、本例ではアクセス装置１を宛先として、公開鍵K_{PUB2}を配布する。

【００５４】

ステップ１０２において、アクセス装置１は、公開鍵K_{PUB2}を受信し、ネットワークの新しいローカル公開鍵（$K_{PUB.LOC}=K_{PUB2}$）として記憶する。

【００５５】

ステップ１０３において、アクセス装置１は、バスＢを介して、提示装置２を宛先として、状態変更信号を配布する。このステップは、提示装置２に対して、該提示装置２がネットワークに接続される最初であること、したがって、該提示装置２がネットワークの親になるべきことを報せることを目的とする。換言すると、この提示装置２が、秘密鍵K_{PRI2}（これがネットワークのローカル秘密鍵$K_{PRI.LOC}$になる）をネットワークに接続されるべき任意の新しい提示装置に送信することが許可された唯一の提示装置である旨を提示装置２へ報せるのである。

【００５６】

ステップ１０４において、提示装置２は、状態変更信号を受信し、親状態（ＩＥ＝０１）へ移るように状態インジケータを変更する。

【００５７】

この処理の最後に、ネットワーク中の装置に公開された（提示装置２の初期公開鍵K_{PUB2}と等しい）固有のローカル公開鍵$K_{PUB.LOC}$と、提示装置２だけが知っている固有のローカル秘密鍵$K_{PRI.LOC}$を有する本発明によるローカルデジタルネットワークが得られる。ネットワークは、本発明によれば、新しい提示装置の接続を許可することによりネットワークを変更することができる親提示装置を含む。

【００５８】

次に、図３を参照して、本例の場合に提示装置３である新しい提示装置を、図２の処理に従って作成されたネットワークへ接続する処理を説明する。

【００５９】

この処理の最初のステップ２００、２００’及び２００”において、提示装置３を、デジタルバスＢを介して、既存のローカルネットワークへ接続する。提示装置３は、固有の公開鍵K_{PUB3}と秘密鍵K_{PRI3}のペアを収容しており、バージン状態（ＩＥ＝００）である。アクセス装置１及び提示装置２は、図２の処理の最後の状態と同じ状態であり、アクセス装置１は、ネットワークのローカル公開鍵$K_{PUB.LOC}$を保持し、提示装置は、ネットワークの親状態（ＩＥ＝０１）であり、ネットワークのローカル鍵のペア$K_{PUB.LOC}$及び$K_{PRI.LOC}$を保持している。

【００６０】

第２のステップ２０１において、提示装置３は、バスＢを介して、バスＢへ接続する資格のある全てのアクセス装置、本例の場合にはアクセス装置１へ向けられた公開鍵K_{PUB3}を配布する。このステップは、作成処理のステップ１０１（図２）と同じステップである。

【００６１】
ステップ２０２において、アクセス装置１は、公開鍵K_{PUB3}を受信し、アクセス装置１が既に公開鍵を保持しているかどうかを照合する。
【００６２】
本例のように照合結果が肯定的である場合、次のステップ２０３において、アクセス装置１は、バスＢを介して、新しい提示装置３へ向けてローカル公開鍵$K_{PUB.LOC}$を配布する。
【００６３】
ステップ２０４において、提示装置３は、ローカル公開鍵$K_{PUB.LOC}$を受信し、そのローカル公開鍵を好ましくは端末モジュールに記憶する。
【００６４】
ステップ２０５において、提示装置３は、バスＢを介して、ネットワークの全ての提示装置へ、ネットワークの親装置が応答することを要求するメッセージの形式（Ｇｅｎｉｔｏｒ？）で信号を配布する。
【００６５】
ステップ２０６において、ネットワークの親装置、本例の場合には提示装置２は、このメッセージを受信し、提示装置２と提示装置３の間で信頼できる形で通信が確立された後、提示装置２は、無効状態（ＩＥ＝１０）へ移るように状態を変更する。
【００６６】
ステップ２０７において、提示装置２は、ネットワークのローカル秘密鍵を、提示装置３によって復号化可能な暗号形式（$E(K_{PRI.LOC})$）で配布する。特に、提示装置２と提示装置３の間におけるこのローカル秘密鍵の安全な伝送は、ローカル秘密鍵を暗号化するための提示装置３の初期公開鍵K_{PUB3}を用いて行われ、提示装置３は、この秘密鍵K_{PRI3}を用いてこのメッセージを復号化することができる。鍵K_{PUB3}は、たとえば、ステップ２０５の間に提示装置２へ送信される。
【００６７】
ステップ２０８において、提示装置３は、このローカル秘密鍵を受信し、好ましくは、スマートカード３１（図１）と一体化された端末モジュールへ記憶させる。
【００６８】
ステップ２０９において、提示装置３は、ローカル秘密鍵の受信を承認する信号を、バスＢを介して提示装置２へ配布する。
【００６９】
ステップ２１０において、提示装置２は、この受信承認信号を受信し、これに応答して、状態変更信号を新しい提示装置３へ配布し、ステップ２１１において、提示装置３は、この信号を受信し、ネットワークの新しい親になるように状態を変更する（ＩＥ＝０１）。
【００７０】
提示装置２は、これ以降、無効状態になるので、ネットワークのローカル公開鍵を他の提示装置へ送信することが許可されなくなる。これにより、上述のネットワークと同じローカル鍵のペアを保有する別の不正なローカルネットワークを作成するため、この装置２をネットワークから取り除くことが阻止できるようになる。
【００７１】
この処理の終わりには、２台の提示装置２及び３と１台のアクセス装置１とが、ローカルネットワークに接続されている。これらは、ネットワークのローカル鍵のペア$K_{PUB.LOC}$及び$K_{PRI.LOC}$を共用する。ネットワークには、常に、ネットワークに最後に接続された提示装置、すなわち、固有の親装置が存在する。
【００７２】
本発明によるアクセス装置が鍵を備えることなく販売されるので、新しいアクセス装置のローカルネットワークへの接続は、非常に簡単である。特に、新しいアクセス装置がネットワークにプラグインされたとき、新しいアクセス装置が、バスＢを介して、ネットワ

ークの公開鍵を受信することを要求するメッセージを配布するよう構成することが可能である。このメッセージを受信する第１のネットワーク装置、或いは、親装置だけが、このメッセージに応答して、ネットワークの公開鍵を新しいアクセス装置へ配布するよう構成することが可能である。

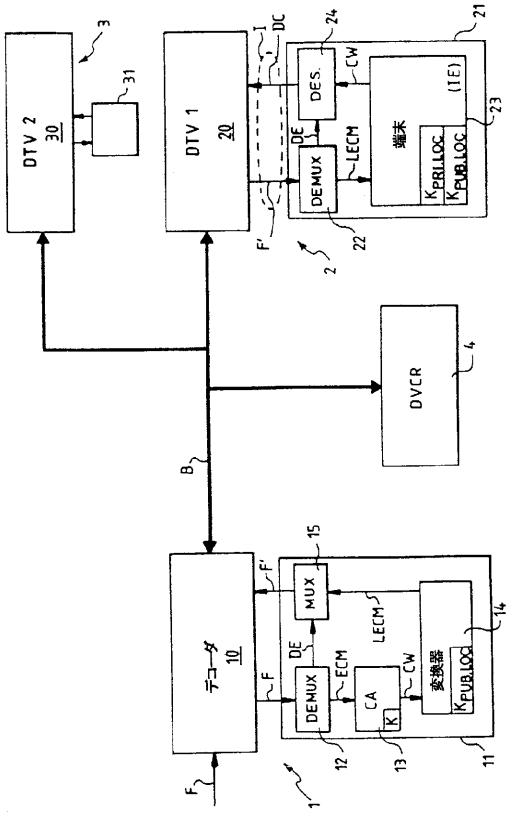
【図面の簡単な説明】

【図１】　本発明によるローカルデジタルネットワークの説明図である。

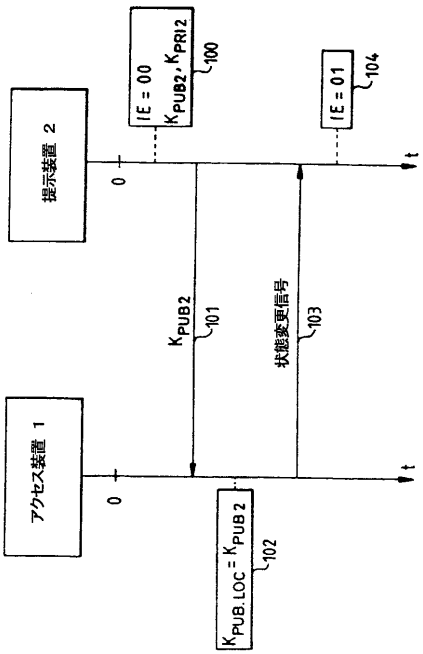
【図２】　図１に示されたローカルデジタルネットワークのようなデジタルネットワークを作成する方法の説明図である。

【図３】　新しい提示装置を、たとえば、図２に示された方法に従って作成されたローカルデジタルネットワークへ接続する方法の説明図である。

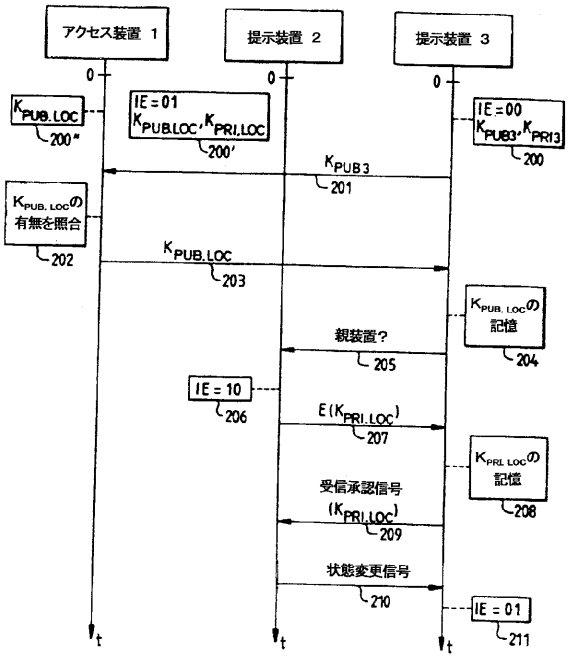
【図１】



【図２】



【図３】


アクセス装置 1
提示装置 2
提示装置 3
0
0
0
$K_{PUB.LOC}$
200"
IE=01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE=00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
$K_{PUB.LOC}$の有無を照合
202
$K_{PUB.LOC}$
203
$K_{PUB.LOC}$の記憶
204
親装置?
205
IE=10
206
$E(K_{PRI.LOC})$
207
$K_{PRI.LOC}$の記憶
208
受信承認信号
$(K_{PRI.LOC})$
209
状態変更信号
210
IE=01
211
t
t
t

フロントページの続き

(51)Int.Cl.			F I		
G09C	*1/00*	*(2006.01)*	H04L	9/00	601F
			G09C	1/00	660G

(72)発明者 ケ, フロランス
フランス国, １３００６ マルセイユ, リュ・ド・ブルトゥイユ １６９, レ・オー・ド・ブルトゥイユ アパルトマン６２ バティマン アー
(72)発明者 アンドル, ジャン－ピエール
フランス国, ３５０００ レンヌ, リュ・ド・ロンジェニル ２０
(72)発明者 フュロン, テディ
フランス国, ３５０００ レンヌ, リュ・ド・ラ・サンテ １３

審査官 新田 亮

(56)参考文献 特開平０４－３４８４３８（ＪＰ, Ａ）
特開平１０－２７１０１１（ＪＰ, Ａ）
国際公開第００／０２０９５０（WO, Ａ１）
特開平０８－０４６９４８（ＪＰ, Ａ）
特開平１０－０４０１５４（ＪＰ, Ａ）
特開平０２－２５０４３９（ＪＰ, Ａ）
特開平０９－１８５５０１（ＪＰ, Ａ）
Shahid Rahman et.al., AFRTS COMMERCIAL OFF THE SHELF(COTS) WORLDWIDE DIGITAL VIDEO BROADCCAST NETWORK, Digital Object Identifier 10.1109/MILCOM, １９９７年, p.640-644, ＵＲＬ, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00646699

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/08
G06F 21/20
G06F 21/24
G06K 19/00
G06K 19/07
G09C 1/00