(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-506584
(P2009-506584A)
(43)公表日　平成21年2月12日(2009.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5B285
G06F 21/00	(2006.01)	H04L	9/00	601E	5J104
		G06F	15/00	330Z	

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

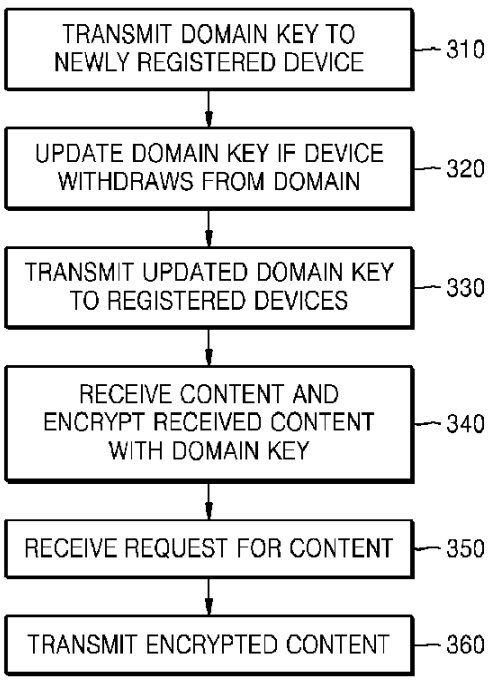
(21)出願番号	特願2008-507560 (P2008-507560)
(86)(22)出願日	平成18年4月25日 (2006.4.25)
(85)翻訳文提出日	平成19年10月16日 (2007.10.16)
(86)国際出願番号	PCT/KR2006/001543
(87)国際公開番号	WO2006/115362
(87)国際公開日	平成18年11月2日 (2006.11.2)
(31)優先権主張番号	60/674,333
(32)優先日	平成17年4月25日 (2005.4.25)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	10-2005-0065669
(32)優先日	平成17年7月20日 (2005.7.20)
(33)優先権主張国	韓国 (KR)

(71)出願人　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】ドメイン管理方法及びそのための装置

(57)【要約】
本発明はドメイン内でデジタルコンテンツを保護する方法及び装置に係り、ドメインに登録された任意のデバイスが前記ドメインから脱退するにつれて、前記脱退前に使われたドメインキーは、脱退したデバイスが使用できないドメインキーにアップデートし、脱退したデバイスに露出されていないかかるドメインキーは、現在ドメインに登録されているデバイスに伝送して、ドメインに登録されたデバイスのみ最新のドメインキーを持つようにすることによって、ドメイン内で共有されるデジタルコンテンツを、ドメインに属していないデバイスはもとよりドメインに属していて脱退したデバイスも、現在ドメイン内で共有されているデジタルコンテンツを使用不可にする。また、ホームドメインから脱退したデバイスは、ホームドメインから脱退する前に正当にダウンロードしたデジタルコンテンツを利用できる。



【特許請求の範囲】
【請求項１】
ドメインを管理する方法において、
前記ドメインに登録されたデバイスのうち一つが前記ドメインから脱退するにつれて、前記脱退前に使われた第１ドメインキーを、前記脱退したデバイスに露出されていない第２ドメインキーにアップデートするステップと、
前記ドメインに登録された複数のデバイスに前記第２ドメインキーを伝送するステップと、を含むことを特徴とする方法。
【請求項２】
外部から所定コンテンツが受信された場合、前記コンテンツを前記第２ドメインキーでのみ復号化するように暗号化するステップと、
前記暗号化されたコンテンツを、前記コンテンツを要請するデバイスに伝送するステップと、をさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記アップデート以後、前記ドメインに新規登録するデバイスに前記第１ドメインキー及び前記第２ドメインキーを伝送するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記第１ドメインキー及び前記第２ドメインキーを伝送するステップは、
前記第１ドメインキー及び前記第２ドメインキーを、前記アップデート以後に前記ドメインに新規登録したデバイスの公開キーで暗号化するステップと、
前記暗号化された第１ドメインキー及び前記第２ドメインキーを、前記新規登録したデバイスに伝送するステップと、を含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記暗号化ステップは、
前記コンテンツをコンテンツキーで暗号化するステップを含み、
前記暗号化されたコンテンツキーは、前記第１ドメインキー及び前記第２ドメインキーのうち、前記コンテンツが受信される当時のドメインキーのみで復号化できることを特徴とする請求項２に記載の方法。
【請求項６】
前記第１ドメインキー及び前記第２ドメインキーは対称キーであることを特徴とする請求項１に記載の方法。
【請求項７】
前記第１ドメインキー及び前記第２ドメインキーは、ＰＫＩ基盤の個人キーまたはＰＫＩ基盤の公開キーであることを特徴とする請求項１に記載の方法。
【請求項８】
ドメインを管理する装置において、
前記ドメインに登録されたデバイスのうち一つが前記ドメインから脱退する場合、既存のドメインキーである第１ドメインキーを、前記脱退したデバイスに露出されていない第２ドメインキーにアップデートするドメインキーアップデート部と、
前記ドメインキーアップデート部が前記第１ドメインキーを前記第２ドメインキーにアップデートした場合、前記第２ドメインキーを前記ドメインに登録された複数のデバイスに伝送するドメインキー伝送部と、を備えることを特徴とする装置。
【請求項９】
前記ドメインキー伝送部は、前記第１ドメインキーが前記第２ドメインキーにアップデートされた後、前記ドメインに新規登録するデバイスに前記第１ドメインキー及び前記第２ドメインキーを伝送することを特徴とする請求項８に記載の装置。
【請求項１０】
前記アップデート後に所定コンテンツが前記ドメインの外部から受信された場合、前記第２ドメインキーのみにより復号化されるように前記コンテンツを暗号化して、前記コン

テンツを要請するデバイスに伝送するコンテンツ処理部をさらに備えることを特徴とする請求項８に記載の装置。
【請求項１１】
前記ドメインキー伝送部は、
前記ドメインに新規登録するデバイスの公開キーを利用して、前記第１ドメインキー及び前記第２ドメインキーを暗号化する暗号化部と、
前記暗号化されたドメインキーを前記ドメインに新規登録するデバイスに伝送する伝送部と、を備えることを特徴とする請求項９に記載の装置。
【請求項１２】
前記ドメインキー伝送部は、前記第１ドメインキー及び前記第２ドメインキーと共に前記第１ドメインキー及び前記第２ドメインキーのアップデートバージョン情報を、前記コンテンツ処理部は、前記暗号化されたコンテンツと共に前記アップデートバージョン情報を共に伝送することを特徴とする請求項１０に記載の装置。
【請求項１３】
前記ドメインキー伝送部は、新規登録するデバイスに以前のあらゆるドメインキーを共に伝送することを特徴とする請求項９に記載の装置。
【請求項１４】
前記コンテンツ処理部は、
前記コンテンツをコンテンツキーで暗号化する第１暗号化部と、
前記コンテンツキーを、第１ドメインキー及び第２ドメインキーのうち、前記コンテンツが外部から受信される当時のドメインキーのみで復号化されるように暗号化する第２暗号化部と、を備えることを特徴とする請求項１０に記載の装置。
【請求項１５】
前記第１ドメインキー及び前記第２ドメインキーは、対称キーであることを特徴とする請求項８に記載の装置。
【請求項１６】
前記第１ドメインキー及び前記第２ドメインキーは、ＰＫＩ基盤のキーであることを特徴とする請求項８に記載の装置。
【請求項１７】
ドメイン管理方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体であり、
前記方法は、
前記ドメインに登録された複数のデバイスのうち一つが前記ドメインから脱退することによって、前記脱退前に使われた第１ドメインキーを、前記脱退したデバイスに露出されていない第２ドメインキーにアップデートするステップと、
前記ドメインに登録された複数のデバイスに前記第２ドメインキーを伝送するステップと、を含むことを特徴とする記録媒体。
【請求項１８】
デバイスをドメインに登録する方法において、
前記ドメインを管理するドメイン管理装置に前記デバイスの登録を要請するステップと、
前記デバイスの公開キーで暗号化された前記ドメインの現在及び以前のあらゆるドメインキーを受信するステップと、を含むことを特徴とする方法。
【請求項１９】
前記デバイスの公開キーを前記ドメイン管理装置に伝送するステップをさらに含むことを特徴とする請求項１８に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ドメイン管理方法に係り、より詳細には、ドメイン内でデジタルコンテンツ

を保護する方法に関する。
【背景技術】
【０００２】
最近、インターネット、地上波 、ケーブル、衛星などの多様な通信媒体を利用したデジタルコンテンツの伝送が急増しており、ＣＤ（コンパクトディスク）、ＤＶＤ（デジタル　ヴァーサタイル　ディスク）などの大容量記録媒体を利用したデジタルコンテンツの販売及びレンタルが急増している。これにより、デジタルコンテンツの著作権を保護するためのソリューションであるＤＲＭ（デジタル　ライツ　マネージメント）が重要な問題として浮び上がっている。特に、あるホームドメインの正当なユーザが、このホームドメインに属しているデバイスを通じて多様なコンテンツサービスを自由に提供されるようにする分野についての研究が活発に進んでいるが、これによれば、同じドメインに属するデジタルＴＶやＰＤＡなどのデバイスは、各自保存しているコンテンツを他のデバイスと共有できるようになる。
【０００３】
しかし、コンテンツを理想的に保護するためには、ドメイン内のコンテンツをドメインに登録されたデバイスのみ使用でき、ドメインに登録されていないデバイスはもとより、ドメインに登録されてから脱退したデバイスの場合、これ以上ドメインの新規コンテンツを利用できなくするが、ドメインに登録された当時に既に正当にダウンロードしたコンテンツは利用可能にし続けることが望ましいが、まだこのような方法を具現するための具体的な技術が提示されていない。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
本発明は、一つのドメイン内で共有されるコンテンツをドメインに属するデバイスのみ使用可能にするが、脱退したデバイスも脱退前に正当にダウンロードしたコンテンツを使用できるようにドメインを管理する装置及び方法を提供するところにその目的がある。
【課題を解決するための手段】
【０００５】
このような目的を達成するための本発明は、ドメインを管理する方法において、前記ドメインに登録されたデバイスのうち一つが前記ドメインから脱退するにつれて、前記脱退前に使われた第１ドメインキーを、前記脱退したデバイスに露出されていない第２ドメインキーにアップデートするステップと、前記ドメインに登録された複数のデバイスに前記第２ドメインキーを伝送するステップと、を含むことを特徴とする。
【０００６】
前記ドメイン管理方法は、外部から所定コンテンツが受信された場合、前記コンテンツを前記第２ドメインキーでのみ復号化するように暗号化するステップと、前記暗号化されたコンテンツを、前記コンテンツを要請するデバイスに伝送するステップと、をさらに含むことが望ましい。
【０００７】
また本発明は、前記ドメイン管理方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体を提供する。
【０００８】
また本発明は、ドメインを管理する装置において、前記ドメインに登録されたデバイスのうち一つが前記ドメインから脱退する場合、既存のドメインキーである第１ドメインキーを、前記脱退したデバイスに露出されていない第２ドメインキーにアップデートするドメインキーアップデート部と、前記ドメインキーアップデート部が前記第１ドメインキーを前記第２ドメインキーにアップデートした場合、前記第２ドメインキーを前記ドメインに登録された複数のデバイスに伝送するドメインキー伝送部と、を備えることを特徴とする。
【発明の効果】

【０００９】
本発明によれば、一つのドメインに登録されたデバイス同士で共有するドメインキーを利用してドメイン内で共有されるデジタルコンテンツを、ドメインに属していないデバイスはもとよりドメインに属していて脱退したデバイスも利用できないようにすると同時に、ドメインから脱退したデバイスの場合、ドメインに属した時に正当にダウンロードしたデジタルコンテンツは利用可能にすることによって、デジタルコンテンツが共有される範囲が現在ドメインに登録されたデバイスに限定されるようにドメインを効率的に管理できる。

【発明を実施するための最良の形態】

【００１０】
以下では、図面を参照して本発明の望ましい実施形態を詳細に説明する。

【００１１】
図１は、本発明によるリンク情報のフォーマットを示す図である。

【００１２】
本発明によるドメイン管理装置は、ドメインに登録されたデバイスそれぞれのＰＫＩ（パブリック　キー　インフラストラクチャー）基盤の公開キーを利用して、ドメイン内で共有される復号化キーのドメインキーを暗号化してリンク情報を生成して保存し、ドメインに登録されたデバイスに伝送する。図１を参照するに、リンク情報は、有効性情報１１０、メジャーバージョン１２０、マイナーバージョン１３０、リンクデータ１４０を表すフィールドを含む。有効性情報１１０は、本リンク情報が以前のものであるか現在のものであるかを表示するビットである。本リンク情報が現在のものであるか以前のものであるかは、後述するリンクデータ１４０に含まれたドメインキーが現在使われているものであるかどうかによって決定される。

【００１３】
メジャーバージョン１２０は、リンクデータ１４０に含まれたドメインキーのバージョン情報であり、ドメインに登録されたデバイスが脱退する場合に増加し、マイナーバージョン１３０は、新規デバイスがドメインに登録する時に増加するものであって、本発明によるドメイン管理装置は、これを利用してメジャーバージョン１２０が同じ複数のリンク情報のうち最新リンク情報を区分できる。

【００１４】
リンクデータ１４０は、ドメインに属するデバイスの公開キーを利用してドメインキーを暗号化したものである。リンク情報を受信したデバイスは、リンクデータ１４０を自身の個人キーで復号化してドメインキーを獲得できる。メジャーバージョン１２０またはマイナーバージョン１３０の変動がある場合、すなわち、デバイスの出入がある場合、本発明によるドメイン管理装置は、アップデートされたあらゆるリンク情報をドメインに登録されたデバイスに伝送することによって、デバイスは、ドメイン内のデバイス及びドメインキーに関する情報を最新の情報に保持できる。

【００１５】
図２は、本発明によるコンテンツ情報のフォーマットを示す図である。

【００１６】
バージョン２１０は、リンク情報でのメジャーバージョン１２０と同じくドメインキーのバージョンを表すデータであるが、ドメイン管理装置が外部からデジタルコンテンツを受信する場合、受信当時のドメインキーのバージョンが記録される。コンテンツ２２０は、本発明によるドメイン管理装置が外部から受信したデジタルコンテンツをドメインキーで復号化できるように暗号化したデータである。このようなコンテンツ情報を受信したデバイスは正当な権限がある場合、コンテンツ２２０をドメインキーで復号化して、ドメイン管理装置が受信したデジタルコンテンツを利用できる。

【００１７】
図３は、本発明によるドメイン管理方法が行われる過程を簡略に示すフローチャートである。

【００１８】
新たなデバイスが登録されれば、ドメイン管理装置は、その新規デバイスの公開キーを利用して現在のドメインキーを暗号化してリンク情報を生成した後、新規デバイスに伝送する（３１０）。この時、現在のドメインキーを暗号化して生成したリンク情報だけでなく、以前のリンク情報、すなわち、以前バージョンのドメインキーが存在すれば、これらをいずれも伝送することによって、ドメインに登録されたデバイスが、ドメイン管理装置が保存しているあらゆるデジタルコンテンツを利用可能にする。
【００１９】
もし、ドメインから脱退するデバイスがある場合には現在のドメインキーをアップデートし（３２０）、アップデートされたドメインキーをドメインに登録されたデバイスに伝送して（３３０）、登録されたデバイスが常に最新のドメインキーを持つようにする。以後、ドメイン管理装置が外部からデジタルコンテンツを受信すれば、受信当時のドメインキーで受信したデジタルコンテンツを暗号化し（３４０）、以後にドメインに登録されたデバイスから該当コンテンツについての要請を受信すれば（３５０）、暗号化されたコンテンツを該当デバイスに伝送する（３６０）。暗号化されたコンテンツを受信したデバイスは、自身が持っているドメインキーを利用してこれを復号化できる。
【００２０】
図４は、本発明の一実施形態によってドメインに新規デバイスが登録される時の情報フローを示す図である。
【００２１】
図示されたように、まだドメインに属するデバイスがない状態で、デバイスＡ　４１０がドメイン管理装置４００に自身の公開キーであるｐｕｂ＿ｃｏｎｆ＿ｄｅｖ＿Ａを伝送しつつドメインへの登録を要請すれば、ドメイン管理装置４００は、これを利用してドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１を暗号化し、暗号化したドメインキーが現在の最新ドメインであることを表す“Ｃ”を有効性情報フィールドに記録し、ドメインキーのメジャーバージョンを表す１をメジャーバージョンフィールドに記録してリンク情報を生成する。ドメイン管理装置４００は、生成したリンク情報をデバイスＡ　４１０に伝送し、デバイスＡ４００はこれを受信して保存する。これにより、ドメインキーは、デバイスＡのみ自身の個人キーを利用して復号化可能になる。
【００２２】
図５は、図４での過程以後、他の新規デバイスが登録される時の情報フローを示す図である。
【００２３】
図示されたように、図４での過程以後、デバイスＢ　４２０がドメイン管理装置４００に自身の公開キーであるｐｕｂ＿ｃｏｎｆ＿ｄｅｖ＿Ｂを伝送しつつドメインへの登録を要請すれば、ドメイン管理装置４００は、Ｂに関するリンク情報を生成して既存のＡに関するリンク情報に新たに生成したリンク情報を付加すると同時に、これらのマイナーバージョンを１に増加させる。すなわち、本発明で新たなデバイスがドメインに新規登録される場合、ドメインキナメジャーバージョンの変動はなくマイナーバージョンのみ増加する。以後、ドメイン管理装置４００は、リンク情報をドメインに登録されたあらゆる装置、すなわち、デバイスＡ　４１０及びデバイスＢ　４２０に伝送する。これにより、デバイスＢ　４２０もデバイスＡ　４１０と同じく自身の個人キーを利用してドメインキーを復号化できる。
【００２４】
図６は、図５での過程以後、本発明によるドメイン管理装置が第１コンテンツを受信してドメインに登録されたデバイスに提供する過程を示す図である。
【００２５】
ドメイン管理装置４００は、外部から第１コンテンツ４０１を受信し、第１コンテンツ４０１についての対称キーであるＫｅｙ＿ｃｏｎｔｅｎｔ１を利用して暗号化し、またＫｅｙ＿ｃｏｎｔｅｎｔ１を、第１コンテンツ４０１が受信される時のドメインキーを利用

して始めて復号化できる暗号キーであるｐｕｂ＿ｓｈａｒ＿ｕｓｅｒ１を利用して、暗号化してコンテンツ情報４０２を生成する。前述したようにコンテンツ情報４０２のバージョンは、第１コンテンツ４０１が受信される時のドメインキーバージョンと同一であるので、この場合に１になる。

【００２６】

以後、デバイスＡ　４１０及びデバイスＢ　４２０の要請に応じてドメイン管理装置４００は、生成したコンテンツ情報を両デバイスに伝送する。これにより、ドメインに登録されたデバイスであるデバイスＡ　４１０及びデバイスＢ　４２０は、自身が保存しているリンク情報で自身の個人キーを利用してドメインキーを復号化した後、ドメインキーを利用してコンテンツキーを復号化し、最後にコンテンツキーを利用して第１コンテンツを復号化できる。

【００２７】

ここで、コンテンツキーを暗号化する暗号キーであるｐｕｂ＿ｓｈａｒ＿ｕｓｅｒ１は、復号化キーであるドメインキーｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１と対応するものであり、両者はＰＫＩ基盤の公開キーと個人キーとの関係にあるが、暗号化方法は、これに限定されず、ｐｕｂ＿ｓｈａｒ＿ｕｓｅｒ１とｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１とが同じキーである場合、すなわち、ドメインキーが対称キーである場合にも本発明に適用できる。

【００２８】

図７は、図６での過程以後ドメインに登録されたデバイスがドメインから脱退する場合の情報フローを示す図である。

【００２９】

図示されたように、デバイスＡ　４１０がドメインから脱退すれば、ドメイン管理装置４００は、保存していたリンク情報のうちデバイスＡ　４１０のリンク情報を削除し、ドメインキーをアップデートする。

【００３０】

すなわち、まだドメインに登録されているＢのリンク情報に含まれた有効性情報を、リンク情報が現在のものであることを表す“Ｂ”から以前のものであることを表す“Ｐ”に入れ替え、新たなドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２を再びデバイスＢ　４２０の公開キーであるｐｕｂ＿ｃｏｎｆ＿ｄｅｖ＿Ｂで暗号化して新たなリンク情報を生成する。新たに生成されたリンク情報の有効性情報は現在を表す“Ｃ”になり、ドメインキーがアップデートされたので、メジャーバージョンは２に増加する。すなわち、本発明によるメジャーバージョンは、ドメインに登録されたデバイスが脱退すれば増加する。一方、メジャーバージョンの増加と共にマイナーバージョンは０にリセットされる。

【００３１】

ドメイン管理装置４００は、変更されたリンク情報をデバイスＢ　４２０に伝送し、デバイスＢ　４２０は、ドメイン管理装置４００と同一に自身が保存しているリンク情報を受信したリンク情報に代替する。

【００３２】

前記の過程を経た結果、デバイスＡ　４１０はドメインから脱退したが、自身が保存しているリンク情報には、第１コンテンツを復号化できるバージョンのドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１が自身の公開キーで暗号化されているので、正当にダウンロードしたデジタルコンテンツである第１コンテンツは依然として利用できる。しかし、以後に受信されるコンテンツは、メジャーバージョンが２であるドメインキーｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２を利用して始めて復号化できるように暗号化されるので、デバイスＡ　４１０は利用できなくなる。一方、デバイスＢ　４２０は、ｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１が暗号化されて含まれた以前のリンク情報を依然として持っているので、第１コンテンツを利用するのには何の支障もなく、現在のリンク情報に最新バージョンのドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２を暗号化して持っているので、以後に受信されるデジタルコンテンツも利用できる。

【００３３】

図８は、図７での過程以後、本発明によるドメイン管理装置が第２コンテンツを受信してドメインに登録されたデバイスに提供する過程を示す図である。

【００３４】

ドメイン管理装置４００は第２コンテンツ４０３を受信すれば、第２コンテンツ４０３についての対称キーであるＫｅｙ＿ｃｏｎｔｅｎｔ２を利用して暗号化し、Ｋｅｙ＿ｃｏｎｔｅｎｔ２は、受信当時のドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２のみで復号化できるように、ｐｕｂ＿ｓｈａｒ＿ｕｓｅｒ２を利用して暗号化することによって新たなコンテンツ情報４０４を生成する。このコンテンツ情報４０４のバージョンはもちろん、第２コンテンツの受信当時の最新リンク情報のメジャーバージョンによって２となる。ドメイン管理装置４００がデバイスＢ　４２０の要請によりコンテンツ情報４０４をデバイスＢ　４２０に伝送すれば、デバイスＢ　４２０は第１コンテンツはもとより、自身の最新リンク情報に含まれたドメインキーｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２を利用して第２コンテンツも利用できるようになる。

【００３５】

ここで、二つのコンテンツを持つデバイスＢ　４２０は、コンテンツ情報に含まれたバージョン情報を見ていかなるリンク情報のドメインキーを暗号化せねばならないかが分かる。例えば、メジャーバージョンが２であるｃｏｎｔｅｎｔ２を利用しようとすれば、メジャーバージョンが２であるリンク情報を探してデバイスＢ　４２０の個人キーを入力することによって復号化されたｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２を得て、これを利用してＫｅｙ＿ｃｏｎｔｅｎｔ２を復号化した後、再びＫｅｙ＿ｃｏｎｔｅｎｔ２を利用してｃｏｎｔｅｎｔ２を復号化できる。

【００３６】

図９は、図８での過程以後、さらに他の新規デバイスがドメインに登録される時の情報フローを示す図である。

【００３７】

以前と同じ方法でデバイスＣ　４２０がドメイン管理装置４００に登録を要請すれば、ドメイン管理装置４００は、自身が保存しているリンク情報をアップデートし、アップデートされたリンク情報をデバイスＢ　４２０及びデバイスＣ　４３０に伝送する。

【００３８】

ここで、ドメイン管理装置４００は、現在のドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ２だけでなく、以前バージョンのドメインキーであるｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１も同じくデバイスＣ　４３０の公開キーで暗号化してリンク情報を生成するという点に注目せねばならない。このようなリンク情報の場合、ｐｒｉｖ＿ｓｈａｒ＿ｕｓｅｒ１のバージョンによってメジャーバージョンは１になり、これは現在使われているドメインキーではないので、有効性情報には“Ｐ”が記録される。このように生成されたリンク情報はデバイスＣ　４３０に伝送されるので、デバイスＣ　４３０は、ドメイン管理装置４００への要請を通じて第２コンテンツ４０３だけでなく第１コンテンツ４０１も利用できるようになる。また、以後に受信されるコンテンツももちろん利用できる。

【００３９】

図１０は、図９での過程以後、さらに他の新規デバイスがドメインに登録される時の情報フローを示す図である。

【００４０】

デバイスＤ　４３０がドメイン管理装置４００に登録を要請すれば、図９と同じくリンク情報のアップデートが行われる。リンク情報のうち、最新ドメインキーが暗号化されて含まれたリンク情報のマイナーバージョンは、以前の１からデバイスＤ　４４０の登録により２になる。また、登録されたデバイスの脱退はなかったので、メジャーバージョン、すなわち、ドメインキーのアップデートはない。この場合、図９と同じくデバイスＤ　４４０は、第１コンテンツ及び第２コンテンツはもとより以後に受信されるデジタルコンテンツをいずれも利用できる。

【００４１】

図１１は、本発明によるドメイン管理装置の構成を示す図である。図１１を参照するに、本発明によるドメイン管理装置４００は、Ｉ／Ｏインターフェース５１０、ドメインキーアップデート部５２０、ドメインキー伝送部５３０、コンテンツ処理部５４０及び保存部５５０を備え、ドメインキー伝送部５３０は、リンク情報生成部５３１、暗号化部５３２及び伝送部５３３を、コンテンツ処理部５４０は、第１暗号化部５４１及び第２暗号化部５４２を備える。

【００４２】

Ｉ／Ｏインターフェース５１０は、ドメイン管理装置４００がドメイン外部または内部のデバイスとデータを交換するための手段であり、保存部５５０は、リンク情報、ドメインキー、コンテンツなどを保存するための手段である。

【００４３】

ドメインキーアップデート部５２０は、ドメインに登録された任意のデバイスがドメインから脱退する場合、アップデートされたドメインキーを生成してドメインキー伝送部５３０に送る。

【００４４】

ドメインキー伝送部５３０は、ドメインに新規登録するデバイスにリンク情報を通じてドメインキーを伝送し、ドメインキーのアップデートがある場合、アップデートされたドメインキーをリンク情報を通じてドメインに登録されたデバイスに伝送する。新規登録するデバイスに伝送するドメインキーを伝送する場合、ドメインキーが少なくても１回以上アップデートされたものであれば、以前のあらゆるアップデートバージョンのドメインキーを共に伝送して、新規登録するデバイスが以前のあらゆるコンテンツを利用可能にすることが望ましい。

【００４５】

暗号化部５３２は、デバイスの公開キーを利用してドメインキーを暗号化し、リンク情報生成部５３１は、暗号化されたドメインキーに有効性情報、メジャーバージョン及びマイナーバージョンを付加してリンク情報を生成し、伝送部５３３は、このようなリンク情報をドメインに登録されたデバイスに伝送することによって、デバイスがドメインキーを持つようにする。

【００４６】

コンテンツ処理部５４０は、デジタルコンテンツが外部から受信されれば、受信される当時バージョンのドメインキーのみで復号化できるように、デジタルコンテンツを暗号化して要請デバイスに伝送する。第１暗号化部５４１は、受信されたデジタルコンテンツをそのコンテンツに対する対称キーであるコンテンツキーで暗号化し、第２暗号化部５４２は、そのコンテンツキーを、該当デジタルコンテンツが外部から受信される当時バージョンのドメインキーのみで復号化できるように暗号化してコンテンツ情報を生成する。コンテンツ情報伝送部５４３は、生成されたコンテンツ情報を該当デジタルコンテンツを要請したデバイスに伝送する。

【００４７】

ここで、ドメインキー伝送部５３０は、ドメインキーを伝送する時にそのドメインキーのアップデートバージョン情報を、コンテンツ処理部５４０は、暗号化されたコンテンツと共にその暗号化されたコンテンツを復号化できるドメインキーのアップデートバージョン情報を共に伝送して、二つ以上のコンテンツを受信したデバイスがコンテンツの復号化のためのドメインキーを容易に検索可能にすることが望ましい。

【００４８】

一方、前述した本発明の実施形態は、コンピュータで実行できるプログラムで作成可能であり、コンピュータで読み取り可能な記録媒体を利用して前記プログラムを動作させる汎用ディジタルコンピュータで具現されうる。

【００４９】

前記コンピュータで読み取り可能な記録媒体は、マグネチック記録媒体（例えば、ロム、フロッピー（登録商標）ディスク、ハードディスクなど）、光学的判読媒体（例えば、

ＣＤ－ＲＯＭ、ＤＶＤなど）及びキャリアウェーブ（例えば、インターネットを通じる伝送）のような記録媒体を含む。

【００５０】

これまで本発明についてその望ましい実施形態を中心に説明した。当業者ならば、本発明が本発明の本質的な特性から逸脱しない範囲で変形された形態で具現されうるということが理解できるであろう。したがって、開示された実施形態は限定的な観点ではなく説明的な観点で考慮されねばならない。本発明の範囲は前述した説明ではなく特許請求の範囲に現れており、それと同等な範囲内にあるあらゆる差異点は本発明に含まれていると解釈されねばならない。

【図面の簡単な説明】

【００５１】

【図１】本発明によるリンク情報のフォーマットを示す図である。

【図２】本発明によるコンテンツ情報のフォーマットを示す図である。

【図３】本発明によるドメイン管理方法が行われる過程を簡略に示すフローチャートである。

【図４】本発明の一実施形態によってドメインに新規デバイスが登録される時の情報フローを示す図である。

【図５】図４での過程以後に他の新規デバイスが登録される時の情報フローを示す図である。

【図６】図５での過程以後、本発明によるドメイン管理装置が第１コンテンツを受信してドメインに登録されたデバイスに提供する過程を示す図である。

【図７】図６での過程以後、ドメインに登録されたデバイスがドメインから脱退する場合の情報フローを示す図である。

【図８】図７での過程以後、本発明によるドメイン管理装置が第２コンテンツを受信してドメインに登録されたデバイスに提供する過程を示す図である。

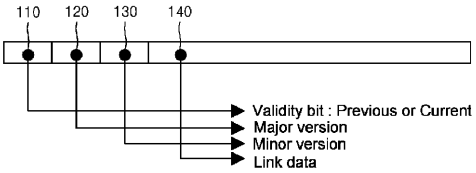
【図９】図８での過程以後、さらに他の新規デバイスがドメインに登録される時の情報フローを示す図である。

【図１０】図９での過程以後、さらに他の新規デバイスがドメインに登録される時の情報フローを示す図である。

【図１１】本発明によるドメイン管理装置の構成を示す図である。

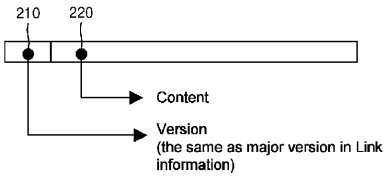
【図１】

FIG. 1

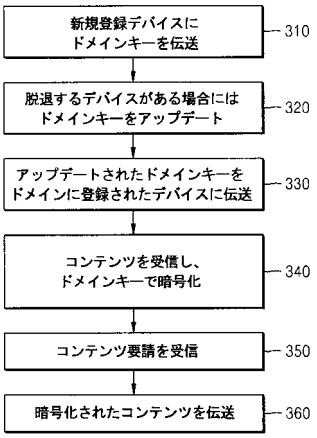


【図２】

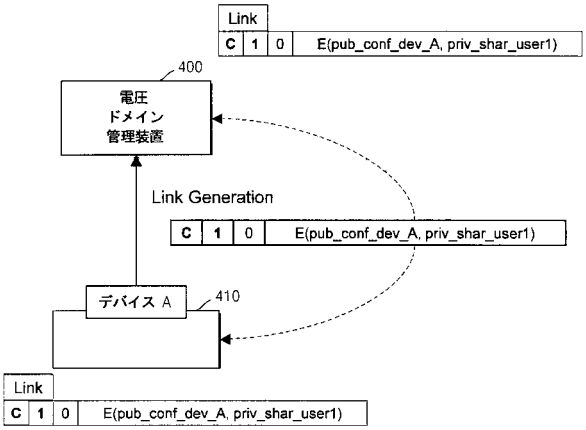
FIG. 2



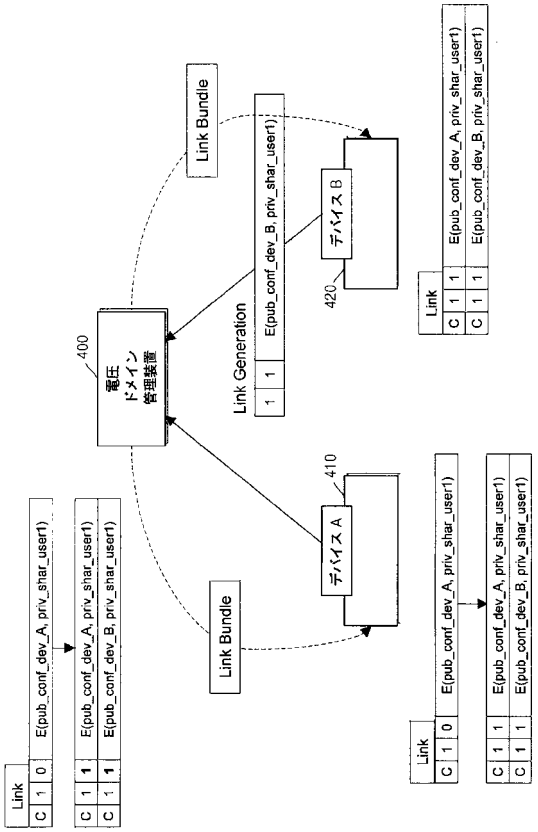
【図３】



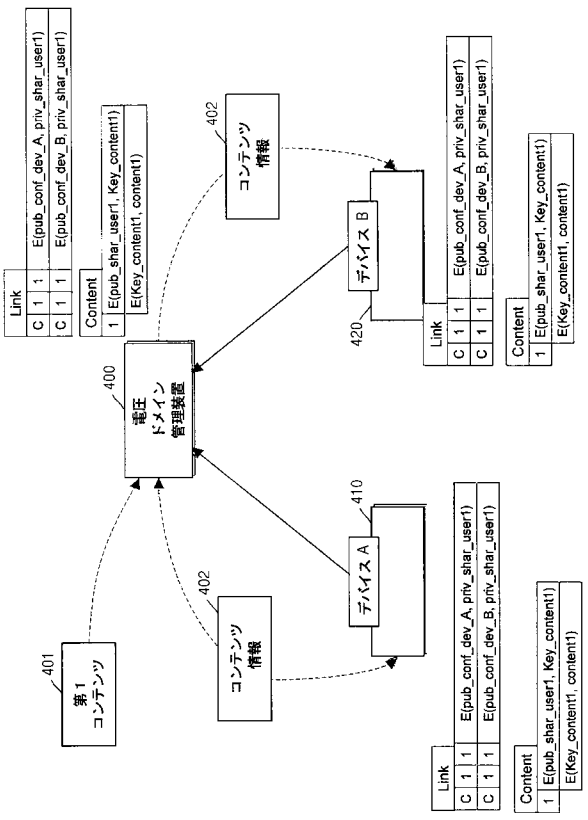
【図４】



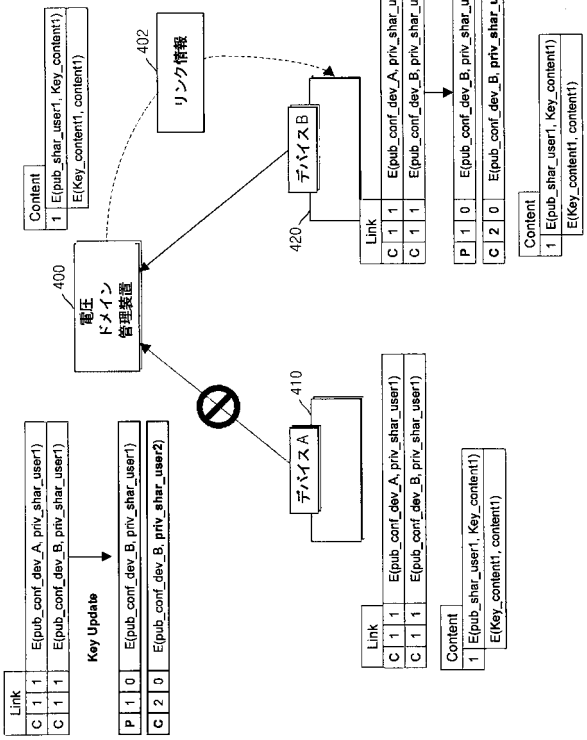
【図５】



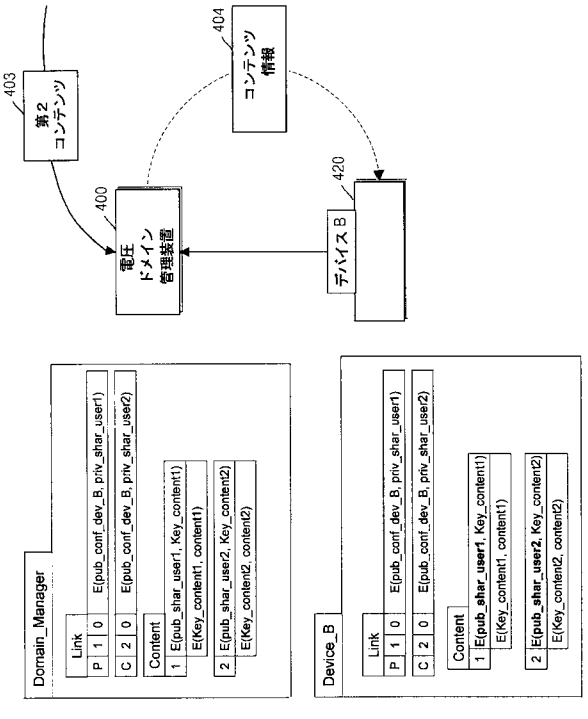
【図６】


401
第１
コンテンツ
400
電圧
ドメイン
管理装置
402
コンテンツ
情報
410
デバイス A
420
デバイス B
Link
C 1 1 E(pub_conf_dev_A, priv_shar_user1)
C 1 1 E(pub_conf_dev_B, priv_shar_user1)
Content
1 E(pub_shar_user1, Key_content1)
E(Key_content1, content1)

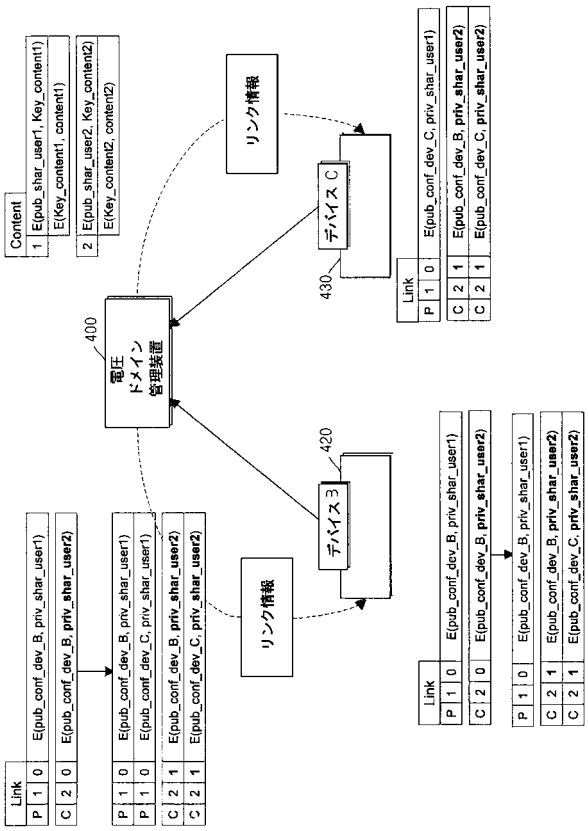
【図７】


400
電圧
ドメイン
管理装置
402
リンク情報
410
デバイス A
420
デバイス B
Key Update
Link
C 1 1 E(pub_conf_dev_A, priv_shar_user1)
C 1 1 E(pub_conf_dev_B, priv_shar_user1)
P 1 0 E(pub_conf_dev_B, priv_shar_user2)
C 2 0 E(pub_conf_dev_B, priv_shar_user2)
Content
1 E(pub_shar_user1, Key_content1)
E(Key_content1, content1)

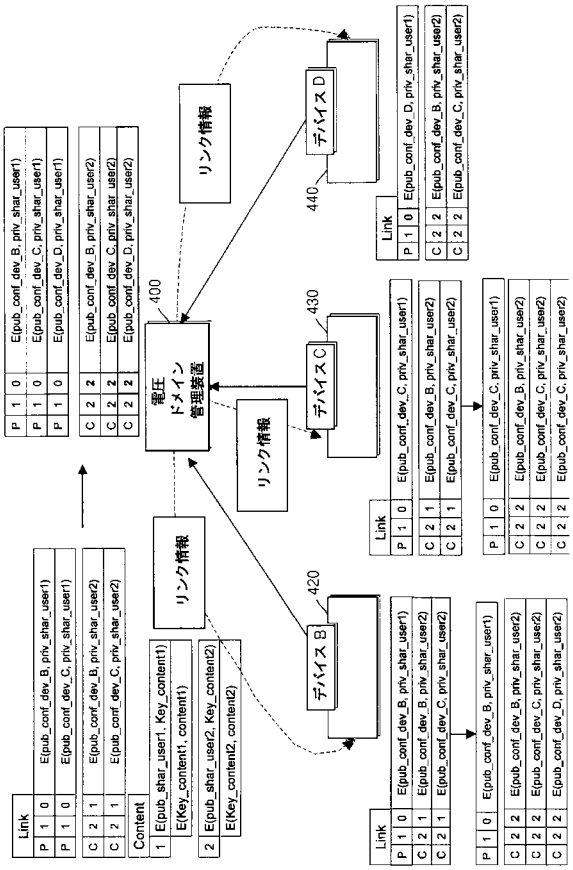
【図８】


403
第２
コンテンツ
400
電圧
ドメイン
管理装置
404
コンテンツ
情報
420
デバイス B
Domain_Manager
Link
P 1 0 E(pub_conf_dev_B, priv_shar_user1)
C 2 0 E(pub_conf_dev_B, priv_shar_user2)
Content
1 E(pub_shar_user1, Key_content1)
E(Key_content1, content1)
2 E(pub_shar_user2, Key_content2)
E(Key_content2, content2)
Device_B
Link
P 1 0 E(pub_conf_dev_B, priv_shar_user1)
C 2 0 E(pub_conf_dev_B, priv_shar_user2)
Content
1 E(pub_shar_user1, Key_content1)
E(Key_content1, content1)
2 E(pub_shar_user2, Key_content2)
E(Key_content2, content2)

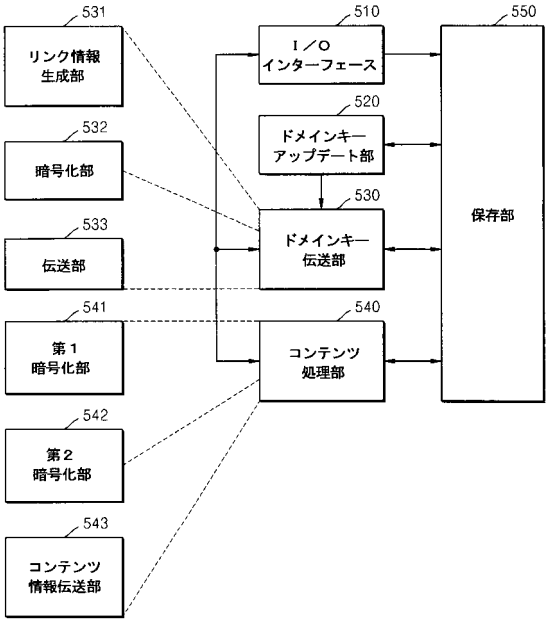
【図９】


400
電圧
ドメイン
管理装置
リンク情報
420
デバイス 3
430
デバイス C
Content
1 E(pub_shar_user1, Key_content1)
E(Key_content1, content1)
2 E(pub_shar_user2, Key_content2)
E(Key_content2, content2)
Link
P 1 0 E(pub_conf_dev_B, priv_shar_user1)
C 2 1 E(pub_conf_dev_B, priv_shar_user2)
C 2 1 E(pub_conf_dev_C, priv_shar_user2)
P 1 0 E(pub_conf_dev_C, priv_shar_user1)

【図１０】


電圧
ドメイン
管理装置
400
リンク情報
リンク情報
リンク情報
デバイス B
420
デバイス C
430
デバイス D
440
Link
Content
E(pub_conf_dev_B, priv_shar_user1)
E(pub_conf_dev_C, priv_shar_user1)
E(pub_conf_dev_D, priv_shar_user1)
E(pub_conf_dev_B, priv_shar_user2)
E(pub_conf_dev_C, priv_shar_user2)
E(pub_conf_dev_D, priv_shar_user2)
E(pub_shar_user1, Key_content1)
E(Key_content1, content1)
E(pub_shar_user2, Key_content2)
E(Key_content2, content2)

【図１１】


531
リンク情報
生成部
532
暗号化部
533
伝送部
541
第１
暗号化部
542
第２
暗号化部
543
コンテンツ
情報伝送部
510
Ｉ／Ｏ
インターフェース
520
ドメインキー
アップデート部
530
ドメインキー
伝送部
540
コンテンツ
処理部
550
保存部

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2006/001543

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC8 G06F17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Patents and applications for inventions since 1975
Korean Utility models and applications for Utility models since 1975
Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS "domain, content, update, encrypt"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004-70612 A1 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 19 AUGUST 2004 See abstract; figures 2, 10, 13. claims 1-2.	1, 8
A	WO 2002-86725 A1 (MOTOROLA INC.) 31 OCTOBER 2002 See abstract; figures 1, 2, 4.	1, 8
A	KR 2005-7830 A (SAMSUNG ELEC. CO., LTD.) 21 JANUARY 2005 See abstract. claims 1-14.	1, 8
A	WO 2001-95206 A1 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 13. DEC. 2001 See abstract; figure 1.	1, 8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 JULY 2006 (26.07.2006)	**26 JULY 2006 (26.07.2006)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer KIM, Jung Jin Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2006/001543

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO2004070612A1	19.08.2004	CA2502605A1	19.08.2004
		CN1748206A	15.03.2006
		EP01603044A1	07.12.2005
		JP2004259262A2	16.09.2004
WO2002086725A1	31.10.2002	CN1503944A	09.06.2004
		EP01390851A1	25.02.2004
		JP16535623	25.11.2004
		RU2003133468A	10.05.2005
		US2002157002A1	24.10.2002
		KR1020040005922	16.01.2004
KR 2005007830 A	21.01.2005	US2005010769A1	13.01.2005
WO200195206A1	13.12.2001	AU200168105A1	17.12.2001
		CN1386238A	18.12.2002
		EP01290610A1	12.03.2003
		JP2003536144T2	02.12.2003
		MXPA02001182A	02.07.2002
		US20020165825A1	07.11.2002
		KR1020020020953	16.03.2002

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 キム，ボン－ソン
大韓民国 ４６３－７２４ キョンギード ソンナム－シ ブンダン－グ グムゴック－ドン ジュゴン ９－ダンジ・アパート ９０３－４１１（番地なし）
(72)発明者 キム，ミョン－ソン
大韓民国 ４３７－７６９ キョンギード ウィワン－シ サム－ドン デーウー・アパート １０５－１０４（番地なし）
(72)発明者 ハン，ソン－ヒュー
大韓民国 １３８－７６７ ソウル ソンパ－グ ムンジョン ２－ドン ファミリー １－ダンジ・アパート １０２－１００６（番地なし）
(72)発明者 ユン，ヨン－ソン
大韓民国 ４４１－７４２ キョンギード スウォン－シ グォンソン－グ グォンソン－ドン サンロク・アパート ５１１－７０４（番地なし）
(72)発明者 リー，ソン－ナム
大韓民国 ４４３－８４８ キョンギード スウォン－シ ヨントン－グ メタン－ドン １２５４－７
(72)発明者 リー，ジェ－フン
大韓民国 ４４３－８４８ キョンギード スウォン－シ ヨントン－グ メタン ３－ドン １２５０－８ ２０６号

Ｆターム(参考) 5B285 AA02 BA09 CA05 CA41 CA43 CB53 CB58
5J104 AA16 EA16 PA07