



PCT

特許協力条約に基づいて公開された国際出願

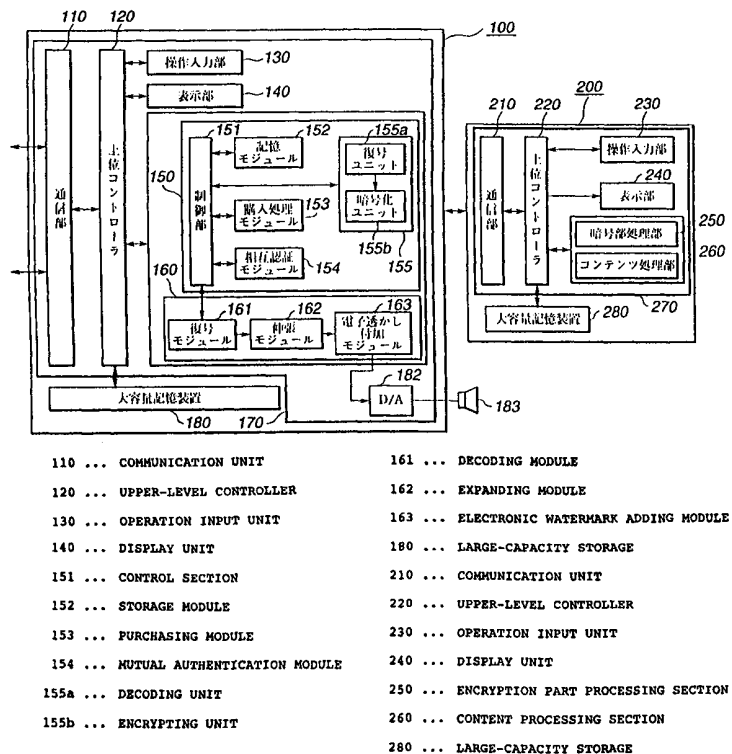
(51) 国際特許分類6 H04L 9/32, G09C 1/00, 5/00, G06F 17/60	A1	(11) 国際公開番号 WO00/07329 (43) 国際公開日 2000年2月10日(10.02.00)
(21) 国際出願番号 PCT/JP99/04132 (22) 国際出願日 1999年7月30日(30.07.99) (30) 優先権データ 特願平10/215809 1998年7月30日(30.07.98) JP (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ) 石橋義人(ISHIBASHI, Yoshihito)[JP/JP] 大石丈於(OISHI, Tateo)[JP/JP] 浅野智之(ASANO, Tomoyuki)[JP/JP] 大澤義知(OSAWA, Yoshitomo)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) (74) 代理人 小池 晃, 外(KOIKE, Akira et al.) 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo, (JP)		(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE) 添付公開書類 国際調査報告書

(54)Title: CONTENT PROCESSING SYSTEM

(54)発明の名称 コンテンツ処理システム

(57) Abstract

A first information processor (100) stores identification information in a storage module (152), stores an encrypted content signal in a large-capacity storage (180), and supplies the encrypted content signal and identification information to a second information processor (200) through a communication unit (110). The first information processor (100) also stores log information generated by a purchasing module (153) of a receiver (170) each time a content key is decoded in the storage module (152) and sends the log information to a key managing center (30) through a transmitter (110) at a predetermined timing. A second information processor (200) has a communication unit (210) which receives the encrypted content signal and the identification information and a content processing section (260) which decodes the encrypted content signal and adds the identification information.



(57)要約

第1の情報処理装置100は、記憶モジュール152に識別情報を記憶し、被暗号化コンテンツ信号を大容量記憶装置180に記憶しておき、被暗号化コンテンツ信号及び識別情報を通信部110を介して第2の情報処理装置200に供給する。第1の情報処理装置100は、受信装置170において、コンテンツ鍵を復号する毎に購入処理モジュール153により生成されるログ情報を記憶モジュール152に記憶しておき、所定のタイミングでログ情報を送信部110を介して鍵管理センタ30に送信する。第2の情報処理装置200は、通信部210を介して被暗号化コンテンツ信号及び上記識別情報を受信し、コンテンツ処理部260により、被暗号化コンテンツ信号を復号し上記識別情報を付加する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AL アルバニア	EE エストニア	LC セントルシア	SD スーダン
AM アルメニア	ES スペイン	LI リヒテンシュタイン	SE スウェーデン
AT オーストリア	FI フィンランド	LK スリ・ランカ	SG シンガポール
AU オーストラリア	FR フランス	LR リベリア	SI スロヴェニア
AZ アゼルバイジャン	GA ガボン	LS レソト	SK スロヴァキア
BA ボスニア・ヘルツェゴビナ	GB 英国	LT リトアニア	SL シエラ・レオネ
BB バルバドス	GD グレナダ	LU ルクセンブルグ	SN セネガル
BE ベルギー	GE グルジア	LV ラトヴィア	SZ スワジランド
BF ブルギナ・ファソ	GH ガーナ	MA モロッコ	TD チャード
BG ブルガリア	GM ガンビア	MC モナコ	TG トーゴ
BJ ベナン	GN ギニア	MD モルドヴァ	TJ タジキスタン
BR ブラジル	GW ギニア・ビサウ	MG マダガスカル	TZ タンザニア
BY ベラルーシ	GR ギリシャ	MK マケドニア旧ユーゴスラヴィア	TM トルクメニスタン
CA カナダ	HR クロアチア	共和国	TR トルコ
CF 中央アフリカ	HU ハンガリー	マリ	TT トリニダード・トバゴ
CG コンゴ	ID インドネシア	ML モンゴル	UA ウクライナ
CH スイス	IE アイルランド	MN モーリタニア	UG ウガンダ
CI コートジボアール	IL イスラエル	MR マラウイ	US 米国
CM カメルーン	IN インド	MX メキシコ	UZ ウズベキスタン
CN 中国	IS アイスランド	NE ニジェール	VN ヴィエトナム
CR コスタ・リカ	IT イタリア	NL オランダ	YU ユーゴスラビア
CU キューバ	JP 日本	NO ノールウェー	ZA 南アフリカ共和国
CY キプロス	KE ケニア	NZ ニュー・ジールランド	ZW ジンバブエ
CZ チェッコ	KG キルギスタン	PL ポーランド	
DE ドイツ	KP 北朝鮮	PT ポルトガル	
DK デンマーク	KR 韓国	RO ルーマニア	

明 細 書

コンテンツ処理システム

技 術 分 野

本発明は、ユーザが電子配信により暗号化されたコンテンツデータ (content data) を取得するためのコンテンツ処理システムに関する。

背 景 技 術

近年、衛星放送やインターネット等を用いた電子配信により、暗号化したコンテンツデータ (Content Data) をユーザに提供するデータ配信が行われている。

衛星放送やインターネット等を用いた電子配信では、データが第三者へ漏れることを防止するために、暗号化を施してデータ送信装置、受信装置間でデータの送受信を行っている。電子配信されるコンテンツデータには、例えば、音楽、映像、プログラムやテキスト等の著作物が挙げられる。

音楽、映像等のコンテンツデータ (Content Data) で著作権があるものについては、これを個人で使用する場合であっても、自由に複製することは著作権保護に反することがある。特に、デジタルデ

ータのままでの複製、いわゆるデジタルコピーあるいはデジタルダビングについては、信号劣化なくコンテンツデータを複製できるため、何らかの制限を設ける必要があり、例えば、I E C 9 5 8 で規定されているオーディオのデジタルインタフェースでは、現在のC D (Compact Disc)、D A T (Digital Audio Tape)、M D (Mini Disc) 等で用いられているS C M S (Serial Copy Management System) というコピーの世代制限方式が採用されている。この方式は、所定の記録媒体に1回目(1世代目)のコピーを実行する際に、これ以上すなわち2世代目以降のコピーを禁止するコピー制御コードをデジタルインタフェース上のビットに記述するというものである。すなわち、S C M Sでは、「親」のコンテンツデータに付加されたあるいは埋め込まれたS C M Sのコピー制御コードが1世代コピー可とされており、これを複製先の機器に送ってデジタル複製して得られる「子」のコンテンツデータでは、S C M Sのコピー制御コードがコピー不可(コピー禁止)に書き換えられるようなシステムである。

ここで、音楽データ等のコンテンツデータについて、インターネットや衛星通信等の電子配信によってサービスを行う場合を考える際に、音楽データ等のコンテンツデータは一般に暗号化され、その暗号化に使用された鍵(コンテンツ鍵(Content Key))も、別の鍵(配送鍵(Distribution Key))で暗号化されるのが一般的である。

ところで、このような音楽データ等のコンテンツデータの複製に関して、今までと同様に1世代のデジタル複製ができるものとするとき、「親」のコンテンツデータのコピー制御コードが1世代コピー可とされ、複製先の機器での「子」のコンテンツデータの копи

一制御コードがコピー禁止に書き換えられていなければならない。

ここで、「親」のコンテンツデータが暗号化されている場合に、複製先の機器が暗号化されたコンテンツデータを復号化する機能を備えていれば、コンテンツデータは復号化することなく複製先の機器に送るのが、処理時間や手間の上からも好ましいが、SCMS等のコピー制御コードもコンテンツデータとともにあるいはコンテンツデータに埋め込まれた形態で暗号化されているので、コンテンツデータに埋め込まれて暗号化されているコピー制御コードの値が変更されないままで複製先の機器に供給されることになる。これに対して、供給側の機器でコピー制御コードをコピー禁止に書き換えてコンテンツデータに埋め込み複製先の機器へ送ろうとした場合、コンテンツデータの暗号を解いて、コピー制御コードをコピー禁止に書き換えた後に、再暗号化しなくてはならず、処理が面倒で手間がかかることになる。

一般に、コンテンツ鍵の大きさは数バイト程度であり、各コンテンツデータの大きさは数百キロバイトから数メガバイト、数ギガバイトに及ぶため、鍵をかけ直す場合には非常に多くの処理時間がかかることになる。

発 明 の 開 示

本発明は、このような従来の実情を鑑みてなされたものであり、ユーザが電子配信により暗号化されたコンテンツ信号を取得した後このコンテンツを復号して出力する際に、取得時に用いた機器の識

別情報を効率よくコンテンツに埋め込むことができるようにしたコンテンツ信号受信装置及びコンテンツ処理システムを提供することを目的とする。

また、本発明は、ユーザが電子配信により暗号化されたコンテンツ信号を取得して復号する際に、確実に課金処理を行うことができるようにしたコンテンツ処理装置、暗号処理装置及びコンテンツ処理システムを提供することを目的とするものである。

また、本発明は、ユーザが電子配信により暗号化されたコンテンツ信号を取得した後このコンテンツを復号して出力する際に、取得時に用いた機器の識別情報を効率よくコンテンツに埋め込むことができるようにしたコンテンツ信号受信方法を提供することを目的とする。

また、本発明は、ユーザが電子配信により暗号化されたコンテンツ信号を取得して復号する際に、確実に課金処理を行うことができるようにしたコンテンツ処理方法を提供することを目的とするものである。

本発明に係るコンテンツ信号受信装置は、被暗号化コンテンツ信号を受信する受信手段と、上記受信手段で受信した被暗号化コンテンツ信号を記憶する記憶手段と、ユーザ指示情報として、上記記憶手段に記憶された上記被暗号化コンテンツ信号を復号する指示が与えられたときに、上記記憶手段に記憶された上記被暗号化コンテンツ信号を復号する復号手段と、上記復号手段により復号されたコンテンツ信号に識別情報を付加する識別情報付加手段とを備えること特徴とする。

さらに、本発明に係るコンテンツ信号受信装置は、外部装置から

被暗号化コンテンツ信号及び識別情報を受信する受信手段と、上記被暗号化コンテンツ信号を復号する復号手段と、上記復号手段により復号されたコンテンツ信号に識別情報を付加する識別情報付加手段とを備えること特徴とする。

また、本発明に係るコンテンツ処理装置は、コンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号する復号手段と、上記復号手段により上記コンテンツ鍵を復号するごとにログ情報を生成するログ情報生成手段と、上記ログ情報を記憶する記憶手段と、所定のタイミングで上記ログ情報を送信する送信手段とを備えること特徴とする。

また、本発明に係るコンテンツ処理装置は、被暗号化コンテンツ信号を復号するためのコンテンツ鍵を所定期間毎に更新される配送鍵で暗号化して得た被暗号化コンテンツ鍵を受信する受信手段と、上記コンテンツ鍵によって上記被暗号化コンテンツ信号を復号する復号手段と、上記被暗号化コンテンツ信号の使用に関する課金情報を生成する課金情報生成手段と、上記課金情報を記憶する記憶手段と、上記配送鍵が更新されたときに、上記課金情報を送信する送信手段とを備えること特徴とする。

また、本発明に係るコンテンツ処理装置は、被暗号化コンテンツ信号を復号するための鍵であり、所定期間毎に更新される配送鍵を受信する受信手段と、上記配送鍵に基づいて、上記被暗号化コンテンツ信号を復号する復号手段と、上記被暗号化コンテンツ信号の使用に関する課金情報を生成する課金情報生成手段と、上記課金情報を記憶する記憶手段と、上記配送鍵が更新されたときに、上記課金情報を送信する送信手段とを備えること特徴とする。

また、本発明に係る暗号処理装置は、コンテンツ信号を復号するためのコンテンツ鍵が暗号化されてなる被暗号化コンテンツ鍵を復号する復号手段と、上記コンテンツ鍵を復号する毎にログ情報を生成するログ情報生成手段と、上記コンテンツ鍵を保存鍵で暗号化する暗号化手段と、上記復号手段、上記ログ情報生成手段及び上記暗号化手段を内蔵する1チップモジュールとからなることを特徴とする。

また、本発明に係るコンテンツ処理システムは、被暗号化コンテンツ信号を記憶する記憶手段と、識別情報を記憶する記憶手段と、上記被暗号化コンテンツ信号及び上記識別情報を送信する送信手段とを備える第1のコンテンツ処理装置と、上記被暗号化コンテンツ信号及び上記識別情報を受信する受信手段と、上記被暗号化コンテンツ信号を復号する復号手段と、上記復号手段によって復号されたコンテンツ信号に上記識別情報を付加する識別情報付加手段とを備える第2のコンテンツ処理装置とを備えることを特徴とする。

さらに、本発明に係るコンテンツ処理システムは、コンテンツ鍵によって被暗号化コンテンツ信号を復号する復号手段と、上記復号手段によって上記コンテンツ鍵を復号する毎にログ情報を生成するログ情報生成手段と、上記ログ情報を記憶する記憶手段と、所定のタイミングで上記ログ情報を送信する送信手段とを備えるコンテンツ処理装置と、上記ログ情報を受信する受信手段と、上記ログ情報に基づいて課金処理を行う課金手段とを備える課金処理装置とからなることを特徴する。

また、本発明に係るコンテンツ信号受信方法は、被暗号化コンテンツ（Content）信号を受信し、受信した被暗号化コンテンツ信号を

記憶し、ユーザ指示情報として、記憶した上記被暗号化コンテンツ信号を復号する指示が与えられたときに、記憶した上記被暗号化コンテンツ信号を復号し、復号したコンテンツ信号に識別情報を付加するステップからなることを特徴とする。

さらに、本発明に係るコンテンツ受信方法は、外部から被暗号化コンテンツ信号及び識別情報を受信し、上記被暗号化コンテンツ信号を復号し、復号した上記コンテンツ信号に識別情報を付加するステップからなることを特徴とする。

また、本発明に係るコンテンツ処理方法は、コンテンツ鍵を用いて、被暗号化コンテンツ信号を復号し、上記コンテンツ鍵を復号するごとにログ情報を生成し、上記ログ情報を記憶し、所定のタイミングで上記ログ情報を送信するステップからなることを特徴とする。

また、本発明に係るコンテンツ処理方法は、被暗号化コンテンツ信号を復号するためのコンテンツ鍵を所定期間毎に更新される配送鍵で暗号化して得た被暗号化コンテンツ鍵を受信し、上記コンテンツ鍵によって上記被暗号化コンテンツ信号を復号し、上記被暗号化コンテンツ信号の使用に関する課金情報を生成し、上記課金情報を記憶し、上記配送鍵が更新されたときに、上記課金情報を送信するステップからなること特徴とする。

また、本発明に係るコンテンツ処理方法は、被暗号化コンテンツ信号を復号するための鍵であり、所定期間毎に更新される配送鍵を受信し、上記配送鍵に基づいて、上記被暗号化コンテンツ信号を復号し、上記被暗号化コンテンツ信号の使用に関する課金情報を生成し、上記課金情報を記憶し、上記配送鍵が更新されたときに、上記課金情報を送信するステップからなること特徴とする。

図面の簡単な説明

図 1 は、本発明を適用したコンテンツ配信システム全体の基本構成を示すブロック図である。

図 2 は、上記第 1 の情報処理装置及び第 2 の情報処理装置の構成を示すブロック図である。

図 3 は、上記コンテンツ配信システムにおいて、保存鍵のみを保持している第 1 の情報処理装置がコンテンツデータを受信して大容量記憶装置に保存する場合の概略構成を示すブロック図である。

図 4 は、公開鍵暗号による相互認証処理の手順を説明するための図である。

図 5 は、上記コンテンツ配信システムにおいて、配送鍵を保持している第 1 の情報処理装置がコンテンツデータを受信して大容量記憶装置に保存する場合の概略構成を示すブロック図である。

図 6 は、上記第 1 の情報処理装置により行われる課金処理のフローチャートである。

図 7 は、本発明の第 1 の実施の形態での上記コンテンツ配信システムにおける第 1 の情報処理装置の受信装置の要部構成を示すブロック図である。

図 8 は、本発明の第 1 の実施の形態での上記コンテンツ配信システムにおける第 2 の情報処理装置の受信装置の要部構成を示すブロック図である。

図 9 は、第 1 の情報処理装置の大容量記憶装置に記憶されたコンテンツデータを第 2 の情報処理装置に第 1 の手順により転送する場

合を示す図である。

図 1 0 は、第 1 の情報処理装置の大容量記憶装置に記憶されたコンテンツデータを第 2 の情報処理装置に第 2 の手順により転送する場合を示す図である。

図 1 1 は、第 1 の情報処理装置の大容量記憶装置に記憶されたコンテンツデータを第 2 の情報処理装置に第 3 の手順により転送する場合を示す図である。

図 1 2 は、本発明の第 2 の実施の形態での上記コンテンツ配信システムにおける第 1 の情報処理装置の受信装置の要部構成を示すブロック図である。

図 1 3 は、本発明の第 2 の実施の形態での上記コンテンツ配信システムにおける第 2 の情報処理装置の受信装置の要部構成を示すブロック図である。

図 1 4 は、本発明の第 3 の実施の形態での上記コンテンツ配信システムにおける第 1 の情報処理装置の受信装置の要部構成を示すブロック図である。

図 1 5 は、本発明の第 3 の実施の形態での上記コンテンツ配信システムにおける第 2 の情報処理装置の受信装置の要部構成を示すブロック図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を参照しながら詳細に説明する。

図 1 は、本発明を適用したコンテンツ配信システム全体の基本構成を示すブロック図である。この図 1 に示すコンテンツ(Contents)配信システムは、音楽データ、動画データ、書籍等の文書データ、静止画データ等のコンテンツデータ(Content Data)を保持するコンテンツプロバイダ(Contents Provider) 10 と、コンテンツプロバイダ 10 からのコンテンツデータをユーザに供給するサービスプロバイダ 20 と、コンテンツ(Content)配送のための鍵（配送鍵(Distribution Key)）を配送する鍵配送センタ 30 と、コンテンツデータを伝送するための衛星やケーブルやインターネット等の伝送系 50 と、ユーザ側の第 1 の情報処理装置 100 と、この第 1 の情報処理装置 100 からコンテンツデータが転送される第 2 の情報処理装置 200 から構成されている。

コンテンツプロバイダ 10 は、コンテンツデータを保持しており、必要に応じてコンテンツデータに電子透かし(Watermark: ウォーターマーク)を挿入し、さらにコンテンツデータの圧縮、暗号化を行う。またコンテンツプロバイダ 10 は、暗号化されたコンテンツデータを復号するためのコンテンツ鍵(Content Key)を、配送鍵で暗号化する。なお、コンテンツプロバイダ 10 は、コンテンツデータに加え、別途メタデータ(Meta Data)を持つこともある。これらのデータはサービスプロバイダ 20 に送られる。

サービスプロバイダ 20 は、コンテンツプロバイダ 10 からの暗号化されたコンテンツデータや暗号化されたコンテンツ鍵等を受信し、コンテンツデータの値付けを行い（価格を決め）、通信路を確保して、伝送系 50 を介してユーザ側の第 1 の情報処理装置 100 に暗号化されたコンテンツデータ等を送信する。

鍵配送センタ 30 は、コンテンツプロバイダ 10 に配送鍵(Distribution Key)を配送し、ユーザ側の情報処理装置 100 から課金情報を入手して決済処理を行い、その結果に応じてコンテンツプロバイダ 10、サービスプロバイダ 20 に利益配分を行う。

第 1 の情報処理装置 100 は、ユーザが保有する機器であり、図 2 に示すように、サービスプロバイダ 20 から伝送系 50 を介して供給される暗号化された被暗号化コンテンツデータ等の情報を受信する受信装置 170 と、供給された被暗号化コンテンツデータ等の情報を保存する大容量記憶装置 180 等を有している。

第 2 の情報処理装置 200 は、ユーザが保有する機器であり、第 1 の情報処理装置 100 から転送される暗号化された被暗号化コンテンツデータ等の情報を受信する受信装置 270 と、供給された被暗号化コンテンツデータ等の情報を保存する大容量記憶装置 280 等を有している。

すなわち、このコンテンツ配信システムにおいて、コンテンツを視聴等するユーザが持つ第 1 の情報処理装置 100 及び第 2 の情報処理装置 200 は、図 2 に示すように、サービスプロバイダ 20 又は他の情報処理装置から送られてくる被暗号化コンテンツデータ等を受信する受信装置 170、270 と、それぞれ受信装置 170、270 により受信した被暗号化コンテンツデータ等を記憶しておく大容量記憶装置 180、280 からなる。

上記受信装置 170、270 は、それぞれ外部とデータの送信／受信を行う通信部 110、210、通信部 110、210 に接続された上位コントローラ 120、220、上位コントローラ 120、220 に接続された操作入力部 130、230、表示部 140、2

40、暗号処理部150、250やコンテンツ処理部(Content Processing Section)160、260などからなる。

この第1の情報処理装置100の受信装置170において、通信部110は、上記サービスプロバイダ20や鍵配送センタ30と通信し、コンテンツデータ又は鍵等の所定の情報を送信／受信する。また、第2の情報処理装置100の受信装置170において、通信部210は、上記第1の情報処理装置100と通信し、所定の情報を送信／受信する。そして、上位コントローラ120、220は、それぞれ上記通信部110、210を介して受信したデータや操作入力部130、230からの操作入力データに応じて、所定のメッセージ等を表示部140、240に表示し、暗号処理部150、250を利用してコンテンツデータの利用権購入処理や転送処理等を行い、暗号化されたコンテンツデータ等を大容量記憶装置180、280に記憶し、また、被暗号化コンテンツデータを大容量記憶装置180、280から読み出してコンテンツ処理部160、260に供給するなどの制御を行う。

上記操作入力部130、230は、それぞれ図示しないリモートコントローラからの信号や図示しない入力ボタンの操作などによる操作入力データすなわちユーザ指示情報を上記上位コントローラ120、220に供給する。また、上記表示部140、240は、それぞれ上記上位コントローラ120、220により制御される液晶表示器のような表示デバイスで構成されており、指示を出したり、情報を表示したりする。上記入力操作部130、230及び表示部140、240は、必要に応じてタッチパネル式液晶表示器などになり、それぞれ一つにまとめられる。

また、第1の情報処理装置100の受信装置170において、暗号処理部150は、サービスプロバイダ20、鍵配送センタ30と相互認証し、コンテンツ利用権を購入するとともに購入処理をし、所定のデータの暗号化／復号化を行い、コンテンツ鍵Kc及び使用許諾条件情報を保持する記憶モジュール152を管理し、さらに配送鍵Kdや課金情報等を上記記憶モジュール152に記憶する。この暗号処理部150は、制御部151、記憶モジュール152、購入処理モジュール153、相互認証モジュール154、暗号化／復号モジュール155などからなる。

上記暗号処理部150において、制御部151は、上位コントローラ120からのコマンドに応じて各モジュールを制御するとともに、各モジュールからの結果を上位コントローラ120に送信する。また、記憶モジュール152は、購入処理モジュール153から供給された課金情報及び配送鍵Kd等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送鍵Kd等のデータを供給する。購入処理モジュール153は、サービスプロバイダ20から受信した取扱方針や価格情報から、新たに使用許諾条件情報及び課金情報を生成して記憶モジュール152に出力する。相互認証モジュール154は、外部装置との相互認証を実行し、必要に応じて、一時鍵Kt（セッション鍵）を生成して暗号化／復号モジュール155に供給する。暗号化／復号モジュール155は、復号ユニット155a及び暗号化ユニット155bから構成される。復号ユニット155aは、配送鍵Kdで暗号化されたコンテンツ鍵Kcを復号したり、セッション鍵Ktで暗号化された各種データを復号したりする。暗号化ユニット155bは、復号されたコンテンツ鍵Kcを

記憶モジュール 152 に保持されている保存鍵 K_s で暗号化し、制御部 151 を介して記憶モジュール 152 に出力したり、セッション鍵 K_t で各種データを暗号化したりする。

また、コンテンツ処理部 160 は、上記暗号処理部 150 と相互認証してコンテンツ鍵 K_c を受信し、このコンテンツ鍵 K_c を用いて上位コントローラ 120 から供給された暗号化されたコンテンツデータを復号し、圧縮されているコンテンツデータを伸張し、さらに電子透かしをコンテンツデータに埋め込む。このコンテンツ処理部 160 は、復号モジュール 161、伸張モジュール 162、電子透かし埋め込みモジュール 163 などからなる。

上記コンテンツ処理部 160 において、復号モジュール 161 は、大容量記憶部 180 に記憶されたコンテンツデータをコンテンツ鍵 K_c で復号し、伸張モジュール 162 に出力する。伸張モジュール 162 は、圧縮されているコンテンツデータを例えば ATRAC (Adaptive Transform Acoustic Coding) 方式で伸張し、電子透かし埋め込みモジュール 163 に出力する。電子透かし埋め込みモジュール 163 は、購入処理を行った暗号処理部の個別 ID を電子透かし技術を用いてコンテンツデータに埋め込み、D/Aコンバータ 182 によりアナログ化されてスピーカ 183 から出力される。

上記第 1 の情報処理装置 100 の受信装置 170 における暗号処理部 150 及びコンテンツ処理部 160 は、シングルチップの暗号処理 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧又は周波数の幅が狭いなど、外部から不正にデータを読み出し難い特性（耐タンパ性）を有するシングルチップ IC として構成されている。

また、第2の情報処理装置200の受信装置270に設けられている暗号処理部250及びコンテンツ処理部260は、上記第1の情報処理装置100の受信装置170の暗号処理部150及びコンテンツ処理部160と同様な機能を有するもので、耐タンパ性を有するシングルチップICとして構成されている。

さらに、上記大容量記憶部180、280は、ハードディスクや光ディスク等の記憶デバイスで、コンテンツ鍵Kcで暗号化されたコンテンツデータ、配送鍵Kdで暗号化されたコンテンツ鍵Kc、使用許諾情報、価格情報、公開鍵証明書、登録情報等が保存されている。

このコンテンツ配信システムにおける本発明の第1の実施の形態について図1ないし図11を参照して説明する。

先ず、このコンテンツ配信システムにおいて、コンテンツプロバイダ10から提供されたコンテンツデータが、ユーザの情報処理装置100の受信装置170を介して大容量受信装置180に記憶されるまでの手順①～⑥について、図3を参照しながら説明する。

暗号化されていないコンテンツデータを保持するコンテンツプロバイダ10は、図示しない乱数生成器でコンテンツ鍵（例えば共通鍵）Kcを生成し、このコンテンツ鍵KcでコンテンツデータContを暗号化する。次に、コンテンツプロバイダ10は、あらかじめ鍵管理センタ30から供給された配送鍵（例えば共通鍵、公開鍵であってもよい）Kdを用いて（手順①）、コンテンツ鍵Kc及び使用許諾情報等のその他の情報を暗号化する。そして、コンテンツプロバイダ10は、これらの被暗号化コンテンツデータKc(Cont)及び被暗号化コンテンツ鍵Kd(Kc)をサービスプロバイダ20に供給す

る（手順②）。

ユーザが持つ第1の情報処理装置100の受信装置170は、衛星通信やケーブル通信、インターネット等を介してサービスプロバイダ20から被暗号化コンテンツデータKc(Cont)及び被暗号化コンテンツ鍵Kd(Kc)を受信する（手順③）。これらを受信した受信装置170は、ユーザがこのコンテンツを楽しむために暗号を解かなくてはならない。そのために、受信装置170は、復号された状態のコンテンツ鍵Kcを次のようにして入手する。

第1の情報処理装置100の受信装置170は、暗号化されたコンテンツ鍵Kd(Kc)を直接鍵管理センタ30に送信する（手順④）。ここで、受信装置170は、手順③で受信した被暗号化コンテンツ鍵Kd(Kc)を一度大容量受信装置180に記憶してもよく（手順⑤）、また、しなくてもよい。すなわち、受信装置170は、コンテンツ鍵Kcの暗号化に使用している配送鍵Kdを持っておらず、このままでは、受信装置170は、被暗号化コンテンツ鍵Kd(Kc)を復号できないので、この被暗号化コンテンツ鍵Kd(Kc)を一旦鍵管理センタ30に送信する。

このとき、第1の情報処理装置100の受信装置170は、自己の識別情報IDや自己の保存鍵Ksも被暗号化コンテンツ鍵Kd(Kc)と一緒に送信する。これらを受信した鍵管理センタ30は、自己の保持する配送鍵Kdで被暗号化コンテンツ鍵Kd(Kc)からコンテンツ鍵Kcを復号し、ユーザの受信装置170から受け取った保存鍵Ksでコンテンツ鍵Kcを再度暗号化する。この時、さらに、鍵管理センタ30は、ユーザの識別情報に従って課金処理を行う。そして、鍵管理センタ30は、保存鍵Ksで暗号化された被暗号化コ

ンテンツ鍵 $K_s(K_c)$ を受信装置に返送する（手順⑥）。

鍵管理センタ 30 は、これらのデータを受信装置 170 との間の相互認証で確立されたセッション鍵で暗号化した上で送っても良い。すなわち、セッション鍵によりコンテンツ鍵等を暗号化する場合、受信装置 170 は、保存鍵 K_s を鍵管理センタ 30 に送信せず、鍵管理センタ 30 は、コンテンツ鍵 K_c をセッション鍵で暗号化し、受信装置 170 に送信する。受信装置 170 は、セッション鍵で暗号化された被暗号化コンテンツ鍵等を受信した後、このセッション鍵を用いてコンテンツ鍵 K_c などを一旦復号し、復号したコンテンツ鍵 K_c など自己の持つ保存鍵 K_s で暗号化する。

保存鍵 K_s により暗号化された被暗号化コンテンツ鍵 $K_s(K_c)$ を受信した受信装置 170 は、その被暗号化コンテンツ鍵 $K_s(K_c)$ を大容量受信装置 180 に保存する。受信装置 170 の記憶モジュール 152 には、保存鍵 K_s が保存されているため、受信装置 170 は、いつでもコンテンツ鍵 K_c を復号することができ、また、このコンテンツ鍵 K_c を用いて、被暗号化コンテンツデータ $K_c(Cont)$ からコンテンツデータ $Cont$ を復号することができる。なお、図 3 中には、大容量受信装置 180 に 1 つしか鍵が記憶されていないが、実際には数多くの暗号化されたコンテンツやコンテンツ鍵が保存されていてもよい。

以上のように、本発明を適用したコンテンツ配信システムでは、コンテンツプロバイダ 10 が有するコンテンツデータ $Cont$ をコンテンツ鍵 K_c で暗号化してユーザの受信装置 170 に提供することができるとともに、このコンテンツデータ $Cont$ の暗号化に用いたコンテンツ鍵 K_c も暗号化してユーザの受信装置 170 に提供すること

ができる。そして、ユーザの受信装置 170 は、提供された被暗号化コンテンツ鍵 K_c を復号して、コンテンツデータ $Cont$ を復号することが可能となる。

なお、暗号アルゴリズムは、第三者に内容がわからないようにデータを暗号化するアルゴリズムであればどのようなアルゴリズムであってもよい。例えば、暗号アルゴリズムとしては、公開鍵暗号方式や共通鍵暗号方式が一般に知られている。公開鍵暗号方式は、暗号化に使用する鍵と復号に使用する鍵とが異なる暗号アルゴリズムであり、例えば RSA 暗号や、楕円曲線暗号が知られている。この公開鍵暗号方式では、2つの鍵の内、一般に公開される鍵が公開鍵、ユーザが秘密に保持している鍵が秘密鍵と呼ばれる。一方、共通鍵暗号方式は、暗号化する際に使用する鍵と復号する際に使用する鍵が同じである暗号アルゴリズムであり、例えば DES (Data Encryption Standard) 暗号や、FEAL (Fast Encryption Algorithm) (NTT)、Misty (三菱電機) などが知られている。この共通鍵暗号方式では、使用する鍵が共通鍵と呼ばれる。

ここで、機器 A と機器 B とが、公開鍵暗号により互いに正当な相手であるか相互認証する場合について、図 4 を用いて説明する。

なお、機器 A の公開鍵を K_{pa} 、秘密鍵を K_{sa} 、識別情報を ID_a とする。また、機器 B の公開鍵を K_{pb} 、秘密鍵を K_{sb} 、識別情報を ID_b とする。そして、認証局の公開鍵を K_{pc} 、秘密鍵を K_{sc} とする。

また、機器 A の公開鍵 K_{pa} の正当性を示すための証明書 Ca は、以下の式(1)のようになる。

$$Ca = ID_a + (\text{その他の情報}) + K_{pa} + Siga \quad \dots(1)$$

この式(1)における $Siga$ は、署名データであって以下の式(2)の

ようになる。

$$\text{Siga} = \text{Enc}(\text{Hash}(\text{IDa} + (\text{その他の情報}) + \text{Kpa}), \text{Ksc}) \cdots (2)$$

この式(2)において、Hash()は、ハッシュ関数と呼ばれる一方方向性関数である。このハッシュ関数は、データ長が長いデータを短い固定のビット長のデータに圧縮する関数で、出力からは入力がかかりにくい関数である。このハッシュ関数の代表的なものとしてMD(Message Digest)5やSHA(Secure Hash Algorithm)-1などが知られている。このhash関数については、Bruce Schneier著「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。また、“+”は、データを連結することを意味する。例えば、16ビットデータ+16ビットデータは、連続して並べた32ビットデータであることを意味する。“Enc()”は、暗号化処理を表し、Enc(x, y)はデータxを暗号鍵yで暗号化することを示す。ここでは公開鍵暗号(例えばRSA暗号)を使用すると仮定する。また、この式(2)では用いていないが、Dec()は、復号処理を表し、Dec(x, z)はデータxを復号鍵zで復号することを示す。機器Bの公開鍵Kpbの正当性を示すための証明書Cbも、この証明書Caと同様である。

相互認証は、図4に示すステップS1からステップS4の手順により行われる。なお、機器A及び機器Bは、自らの鍵や識別情報に加え、それぞれ自己の公開鍵の証明書Ca, Cbと認証局の公開鍵Kpcを保持している。

まず、ステップS1において、機器Aは、乱数R1を生成する。さらに、以下の式(3)に示すように、この乱数R1を秘密鍵Ksaで暗号化して、認証データR2を生成する。

$$R2 = \text{Enc}(R1, Ksa) \quad \dots(3)$$

そして、証明書Ca及び認証データR2を機器Bに送る。

続いて、ステップS2において、機器Bは、機器Aから送られてきた証明書Ca(=IDa+(その他の情報)+Kpa+SigA)が正しいかどうか検証する。すなわち、機器Bは、まず、 $D1 = \text{Hash}(IDa + (\text{その他の情報}) + Kpa)$ を生成する。そして、このD1と $\text{Dec}(\text{SigA}, Kpc)$ とを比較し、一致していれば公開鍵Kpaは正当であると判断する。

機器Bは、公開鍵Kpaが正当であると判断すると、以下の式(4)に示すように、認証データR2を公開鍵Kpaで復号して、乱数R1を再生する。

$$R1 = \text{Dec}(R2, Kpa) \quad \dots(4)$$

次に、機器Bは、以下の式(5)に示すように、この乱数R1を秘密鍵Ksbで暗号化し、認証データR3を生成する。

$$R3 = \text{Enc}(R1, Ksb) \quad \dots(5)$$

そして、機器Bは、証明書Cb及び認証データR3を機器Aに送る。

続いて、ステップS3において、機器Aは、ステップS2と同様に機器Bから送られてきた証明書Cbの検証を行い、公開鍵Kpbが正当であるか判断する。機器Aは、公開鍵Kpbが正当であると判断すると、以下の式(6)に示すように、認証データR3を公開鍵Kpbで復号して検証データR4を生成し、この検証データR4と乱数R1とを比較する。

$$R4 = \text{Dec}(R3, Kpb) \quad \dots(6)$$

乱数R1と検証データR4とが一致していれば、機器Bは正当な秘密鍵Ksbを持っていることになり、機器Bの正当性が確認できる。もし、一致していなければ、機器Bは証明書Cbを盗み見た不正な機器

であると判断できる。

次に、機器Aは、以下の式(7)に示すように、ハッシュ関数を用いて、乱数R1と認証データR2とから認証データR5を生成する。

$$R5 = \text{Hash}(R1 + R2) \quad \dots(7)$$

そして、機器Aは、以下の式(8)に示すように、この認証データR5を秘密鍵Ksaで暗号化し、R6を生成する。

$$R6 = \text{Enc}(R5, Ksa) \quad \dots(8)$$

そして、機器Aは、R6を機器Bに送る。

続いて、ステップS4において、機器Bは、以下の式(9)に示すように、ハッシュ関数を用いて、乱数R1と認証データR2から検証データR7を生成する。

$$R7 = \text{Hash}(R1 + R2) \quad \dots(9)$$

次に、機器Bは、以下の式(10)に示すように、送られてきたR6を公開鍵Kpaで復号して検証データR8を生成する。

$$R8 = \text{Dec}(R6, Kpa) \quad \dots(10)$$

そして、機器Bは、検証データR7と検証データR8とを比較し、一致していれば機器Aは正当な秘密鍵Ksaを持っていることになり、機器Aの正当性が確認できる。もし、一致していなければ、機器Aは証明書Caを盗み見た不正な機器であると判断できる。

以上のように、機器Aと機器Bとは、両者が互いに正当であることを確認し合う相互認証を行うことができる。なお、乱数R1などのデータをその時限りの一時的な鍵として使用することがあり、この鍵のことをセッション鍵と呼ぶ。

コンテンツ配信システムにおけるコンテンツの復号処理は、以上説明したコンテンツ鍵の暗号化を解き、使用条件等を取り出して、

この使用条件に応じて暗号化されたコンテンツを復号することになる。例えば、コンテンツを10回だけ復号可能であるという条件であれば、コンテンツ鍵を1回復号する毎にコンテンツ鍵に付随する使用条件の使用回数を減らす。また、例えばコピー禁止であるという条件があれば、他の機器へコンテンツの転送をしようとした場合には、コンテンツデータの復号を禁止する等のコピー制限がなされる。

なお、このコンテンツ配信システムにおいて、鍵管理センタ30の課金処理は次の1.～3.の処理が考えられる。

1. 鍵管理センタ30は、識別情報に関係づけられた口座番号やクレジットカード番号を保持しておき、この番号に応じて銀行やカード会社から代金を徴収する。
2. 鍵管理センタ30は、鍵を送る毎に口座番号やクレジットカード番号を併せて送らせ決済する。
3. 鍵管理センタ30は、受信装置170の内部の記憶モジュール152に蓄えられた電子マネーから代金を引く。

また、このコンテンツ配信システムにおいては、図5に示すように、第1の情報処理装置100の受信装置170の記憶モジュール152に配送鍵Kdをあらかじめ保持させておき、この配送鍵Kdを用いて被暗号化コンテンツ鍵Kd(Kc)からコンテンツ鍵Kcを復号してもよい。

この場合、ユーザが持つ第1の情報処理装置100の受信装置170は、衛星通信やケーブル通信、インターネット等を介してサービスプロバイダ20から被暗号化コンテンツデータKc(Cont)及び被暗号化コンテンツ鍵Kd(Kc)を受信すると(手順③)、記憶モジ

ジュール 152 に保持している配送鍵 Kd を用いて被暗号化コンテンツ鍵 Kd(Kc) からコンテンツ鍵 Kc を復号し、このコンテンツ鍵 Kc を自己が独自に保持する保存鍵 Ks で暗号化し直し、Ks(Kc) として大容量受信装置 180 に保存する（手順④）。更に、受信装置 170 は、コンテンツ鍵 Kc を復号する毎にログ情報 log を作成し、このログ情報 log を記憶モジュール 152 に蓄積する。そして、課金は、一定期間経過した時や配送鍵 Kd の復号を所定回数行った時や配送鍵 Kd の更新を行う時等に、受信装置 170 が鍵管理センタ 30 にログ情報 log を送信する（手順⑤）ことにより、処理される。

すなわち、第 1 の情報処理装置 100 の受信装置 170 は、図 6 に課金処理のフローチャートを示してあるように、前回課金処理を行ってから、一定期間経過したか否か（ステップ S11）、被暗号化配送鍵 Kd の復号を所定回数行ったか否か（ステップ S12）、配送鍵 Kd の更新を行うか否か（ステップ S13）を繰り返し判定しており、上記各ステップ S11～S13 のいずれかの判定結果が YES の場合に、鍵管理センタ 30 にログ情報 log を送信する（ステップ S14）ことにより課金処理を行う。そして、上記ステップ S14 でログ情報 log を送信したら、今回の課金処理をリセットして上記ステップ S11 に戻り、次の課金処理に入る。

なお、図 5 に示すように、上記コンテンツプロバイダ 10 にはあらかじめ鍵管理センタ 30 から配送鍵 Kd が与えられ（手順①）、コンテンツプロバイダ 10 から被暗号化コンテンツデータ Kc(Cont) 及び被暗号化コンテンツ鍵 Kd(Kc) がサービスプロバイダ 20 に供給されている（手順②）。

このように第 1 の情報処理装置 100 の記憶モジュール 152 に

配送鍵 Kd をあらかじめ保存しておく場合には、コンテンツプロバイダ 10 が使用する配送鍵 Kd は一定期間（例えば 1 ヶ月）毎に更新され、第 1 の情報処理装置 100 もそれに応じて鍵管理センタ 30 から配送鍵 Kd が供給されるものとする（手順⑥）。つまり、配送鍵 Kd は、全ての機器に対して共通であるため、安全性を鑑み時々変更する。

次に、上記第 1 の情報処理装置 100、及び、この第 1 の情報処理装置 100 に接続された第 2 の情報処理装置 200 について、図 7 及び図 8 を参照して、さらに詳細に説明する。

この第 1 の情報処理装置 100 の受信装置 170 における暗号化／復号モジュール 155 は、図 7 に示すように、記憶モジュール 152 と、配送鍵 Kd により暗号化された被暗号化コンテンツ鍵 Kd (Kc) からコンテンツ鍵 Kc を復号するコンテンツ鍵復号部 23 と、復号されコンテンツ鍵 Kc にこの受信装置 170 固有の識別情報 ID を付加する識別情報付加部 24 と、第 2 の情報処理装置 200 の保存鍵 Ks' を配送鍵として用いて識別情報 ID が付加されたコンテンツ鍵 (Kc + ID) を暗号化するコンテンツ鍵暗号化部 25 とを備え、被暗号化コンテンツデータ Kc (Cont) と被暗号化コンテンツ鍵 Ks' (Kc + ID) を通信部 110 を介して第 2 の情報処理装置 200 に送信するようになっている。また、この受信装置 170 は、IEEE 1394 インターフェース等により大容量受信装置 180 と接続されている。

この第 1 の情報処理装置 100 の受信装置 170 において、記憶モジュール 152 は、IC チップ内のフラッシュメモリ等から構成され、コンテンツ鍵復号部 23、識別情報付加部 24、コンテンツ

鍵暗号部 25 は、IC チップ内の ASIC やプログラムにより構成される。

上記記憶モジュール 152 は、第 1 の受信装置 170 内に組み込まれた耐タンパー性のあるシングルチップ IC 内のメモリ（フラッシュメモリ、EEPROM 等）や、第 1 の受信装置 170 とデータの授受ができる IC カード等、第 3 者が簡単に中身を確認できないような記憶媒体であればどのようなものであっても良い。

また、上記大容量記憶装置 180 は、リムーバブル型あるいは固定型のハードディスク、光ディスク、テープメディア、半導体メモリ等のどのような記憶媒体や記憶装置等であってもよく、また、第 1 の受信装置 170 に外部接続あるいは内蔵されたものであってもよい。なお、これらの大容量受信装置 180 には、それぞれを識別するための識別情報（ID）が書き込まれていてもよく、この識別情報は書換え不能になっていてもよい。

一方、第 2 の情報処理装置 200 の受信装置 270 は、図 8 に示すように、この受信装置 270 が独自に保持する保存鍵 Ks' により暗号化された被暗号化コンテンツ鍵 Ks' ($Kc + ID$) を復号するコンテンツ鍵復号部 33 を上記暗号処理部 250 に備えけるとともに、上記コンテンツ処理部 260 における復号モジュール及び電子透かし埋め込みモジュールとして、コンテンツ鍵 Kc により暗号化された被暗号化コンテンツデータ $Kc(Cont)$ を復号するコンテンツ復号部 34 と、コンテンツ復号部 34 により復号されたコンテンツデータを伸張する伸張部 35 と、伸張部 35 により伸張されたコンテンツデータに対して電子透かし処理により第 1 の情報処理装置 100 固有の識別情報 $ID1$ を埋め込む電子透かし埋込部 36 とを備え、

電子透かしにより識別情報 I D 1 が埋め込まれたコンテンツデータを出力端子 3 7 から出力するようになっている。また、この受信装置 2 7 0 は、第 1 の情報処理装置 1 0 0 から被暗号化コンテンツデータ K c (Cont) と被暗号化コンテンツ鍵 K s' (K c + I D) を通信部 2 1 0 介して受信するようになっている。さらに、この受信装置 2 7 0 は、I E E E 1 3 9 4 インターフェース等により大容量記憶装置 2 8 0 と接続されている。

なお、伸張部 3 5 としては、例えば、M P E G (Moving Picture Experts Group) 規格で符号化されたデータをデコードする M P E G デコーダや、いわゆる A T R A C (Adaptive Transform Acoustic Coding) 規格で符号化されたデータをデコードする A T R A C デコーダ等が挙げられる。

この第 2 の情報処理装置 2 0 0 における受信装置 2 7 0 の記憶モジュール 2 5 2 は、上記第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 における記憶モジュール 1 5 2 と同様に I C チップ内のフラッシュメモリ等から構成され、また、コンテンツ鍵復号部 3 3、コンテンツ復号部 3 4、電子透かし埋込部 3 6、伸張部 3 5 は、I C チップ内の A S I C やプログラムにより構成される。

また、第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 と第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 とは、それぞれ、固有の識別情報 (I D 1, I D 2) を有し、また、独自の保存鍵 K s, K s' を保持している。第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 が独自に保持している保存鍵を以下第 1 の保存鍵 K s と呼び、第 2 の受信装置 2 7 0 が独自に保持している保存鍵を以下第 2 の保存鍵 K s' と呼ぶ。

また、第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 の電子透かし

埋込部 36 は、コンテンツデータに対して電子透かし情報(Water Mark)を埋め込むものである。この電子透かし処理により情報を埋め込んだ音声データや画像データ等は、埋め込んだ情報が除去しにくく、フィルタリング処理や圧縮／伸張処理を繰り返し行った後もこの情報を取り出すことができる。

次に、第 1 の情報処理装置 100 の大容量受信装置 180 に記憶されたコンテンツデータを第 2 の情報処理装置 200 に転送する手順について説明する。

まず、第 1 の情報処理装置 100 の大容量受信装置 180 に記憶されたコンテンツデータを第 2 の情報処理装置 200 に転送する場合の第 1 の手順①～⑭について、図 9 を参照して説明する。

この第 1 の手順で第 1 の情報処理装置 100 から第 2 の情報処理装置 200 にコンテンツデータを転送する場合、第 1 の情報処理装置 100 の受信装置 170 の記憶モジュール 152 には、配送鍵 Kd と、この第 1 の情報処理装置の固有の識別情報 ID1 があらかじめ保存されている。そして、第 1 の情報処理装置 100 は、衛星通信やインターネットを介してサービスプロバイダ 20 から送られてくるコンテンツ鍵 Kc で暗号化された被暗号化コンテンツデータ Kc(Cont) と、配送鍵 Kd で暗号化された被暗号化コンテンツ鍵 Kd(Kc)を受信装置 170 により受信し(手順①)、受信した被暗号化コンテンツデータ Kc(Cont) と被暗号化コンテンツ鍵 Kd(Kc)を大容量受信装置 180 に保存している(手順②)。

そして、この第 1 の手順では、第 2 の情報処理装置 200 から第 1 の情報処理装置 100 へコンテンツの転送要求を行うために、先ず第 1 の情報処理装置 100 と第 2 の情報処理装置 200 との間で

相互認証を行う（手順③）。この相互認証は、例えば図2に示した第2の情報処理装置200の受信装置270において、操作入力部230から上位コントローラ220に入力されるユーザ指示情報に応じて、第1の情報処理装置100へコンテンツの転送要求を行うために、先ず第1の情報処理装置100と第2の情報処理装置200との間で行う。なお、上記相互認証処理は、図2に示した第1の情報処理装置100の受信装置170において、図示しないリモートコントローラからの信号や図示しない入力ボタンの操作などによる操作入力データすなわちユーザ指示情報が操作入力部130から上位コントローラ120に入力されることにより、第1の情報処理装置100と第2の情報処理装置200との間で各通信部110、210を介して実行するようにしてもよい。

続いて第2の情報処理装置200の受信装置270は、第1の情報処理装置100からコピーしたいコンテンツのコンテンツ番号と第2の保存鍵Ks'を含むコンテンツ要求コマンドを、セッション鍵で暗号化して第1の情報処理装置100の受信装置170へ送る（手順④）。

コンテンツ要求コマンドを受信した第1の情報処理装置100の受信装置170は、受信したデータをセッション鍵で復号し、コンテンツ番号と第2の保存鍵Ks'を取得する。そして、上記受信装置170は、大容量受信装置180からコンテンツ番号に応じたコンテンツ及びコンテンツ鍵を検索して取り出す（手順⑤）。続いて第1の情報処理装置100の受信装置170は、コンテンツ鍵復号部23により記憶モジュール152内に保持している配送鍵Kdでコンテンツ鍵Kcを復号し（手順⑥）、復号したコンテンツ鍵Kcに

自己の識別情報 I D 1 を識別情報付加部 2 4 により付加する（手順⑦）。例えば、コンテンツ鍵 K c が “0 1 2 3 4 5 6 7 8 9 A B C D E F” であったとし、第 1 の情報処理装置 1 0 0 の識別情報 I D 1 が “0 0 0 0 1 1 1 1 2 2 2 2 3 3 3 3” であったとすると、識別情報が付加された鍵データは 0 1 2 3 4 5 6 7 8 9 A B C D E F 0 0 0 0 1 1 1 1 2 2 2 2 3 3 3 3 となる。

続いて、第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 は、コンテンツ鍵暗号化部 2 5 により、自己の識別情報 I D 1 を付加したコンテンツ鍵 K c を第 2 の保存鍵 K s' を用いて暗号化する（手順⑧）。そして、第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 は、識別情報 I D 1 が付加されて暗号化された被暗号化コンテンツ鍵 K s' (K c + I D 1) 及び被暗号化コンテンツデータ K c (Cont) を、通信部 1 1 0 を介して第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 へ送信する（手順⑨）。

第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 は、第 1 の情報処理装置 1 0 0 から送信された被暗号化コンテンツ鍵 K s' (K c + I D) と被暗号化コンテンツデータ K c (Cont) を、通信部 2 1 0 を介して受信し、大容量記憶装置 2 8 0 に保存する（手順⑩）。

そして、第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 は、コンテンツ鍵復号部 3 3 により、記憶モジュール 2 5 2 に記憶された第 2 の保存鍵 K s' を用いて、受信した被暗号化コンテンツ鍵 K s' (K c + I D) を復号する（手順⑪）。第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 は、被暗号化コンテンツ鍵 K s' (K c + I D 1) を復号することによって、コンテンツ鍵 K c と第 1 の情報処理装置 1 0 0 の識別情報 I D 1 を得ることができる。また、第 2 の情報処理装置 2 0

0の受信装置270は、コンテンツ復号部34により、このコンテンツ鍵 K_c を用いて、受信した被暗号化コンテンツデータ $K_c(Con t)$ を復号する(手順⑫)。伸張部35は、上記コンテンツ復号部34により復号されたコンテンツデータに対して、所定の伸張処理、例えば、コンテンツデータがA T R A Cで圧縮された音楽データである場合、A T R A Cの伸張処理を行いP C Mデータに変換する(手順⑬)。そして、電子透かし埋込部36は、上記コンテンツ鍵復号部33により被暗号化コンテンツ鍵 $K_s'(K_c + I D 1)$ を復号して得られた第1の情報処理装置100固有の識別情報I D 1を、上記伸張部35により伸張されたコンテンツデータに対して、電子透かし処理により埋め込み、出力端子37を介して出力する(手順⑭)。

以上が第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送して再生する第1の手順である。

次に、第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送して再生する第2の手順について、図10を参照して説明する。

上述した第1の手順①～⑭では、手順④でコピーしたいコンテンツのコンテンツ番号と第2の保存鍵 K_s' を含むコンテンツ要求コマンドを第2の情報処理装置200から第1の情報処理装置100に送信していたが、以下に説明する第2の手順①～⑯では、第2の保存鍵 K_s' をあらかじめ第1の情報処理装置100の受信装置170の記憶モジュール152に登録しておく。

この第2の手順で第1の情報処理装置100から第2の情報処理

装置 2 0 0 にコンテンツデータを転送する場合にも、第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 の記憶モジュール 1 5 2 には、配送鍵 K_d と、この第 1 の情報処理装置の固有の識別情報 ID_1 があらかじめ保存されている。そして、第 1 の情報処理装置 1 0 0 は、衛星通信やインターネットを介してサービスプロバイダ 2 0 から送られてくるコンテンツ鍵 K_c で暗号化された被暗号化コンテンツデータ $K_c(Cont)$ と、配送鍵 K_d で暗号化された被暗号化コンテンツ鍵 $K_d(K_c)$ を受信装置 1 7 0 により受信し（手順①）、受信した被暗号化コンテンツデータ $K_c(Cont)$ と被暗号化コンテンツ鍵 $K_d(K_c)$ を大容量受信装置 1 8 0 に保存している（手順②）。

そして、この第 2 の手順では、第 2 の保存鍵 $K_{s'}$ を第 1 の受信装置 1 7 0 に登録する登録作業を行う。登録作業を始めるに当たり、上述の図 2 に示した第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 において、図示しないリモートコントローラからの信号や図示しない入力ボタンの操作などによる操作入力データすなわちユーザ指示情報が操作入力部 2 3 0 から上位コントローラ 2 2 0 に入力されることにより、第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 から第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 に対し相互認証要求が送られる（手順③）。その後、両者の間で相互認証が行われ、セッション鍵が共有される（手順④）。続いて、第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 は、第 2 の保存鍵 $K_{s'}$ を含む登録要求命令をこのセッション鍵で暗号化して、第 1 の受信装置 1 7 0 へ送る。これらを受信した第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 は、記憶モジュール 1 5 2 へ第 2 の情報処理装置 2 0 0 の第 2 の保存鍵 $K_{s'}$ を登録する（手順⑤）。

続いて、第2の情報処理装置200の受信装置270は、第1の情報処理装置100からコピーしたいコンテンツのコンテンツ番号を含むコンテンツ要求コマンドをセッション鍵で暗号化して第1の情報処理装置100の受信装置170へ送る（手順⑥）。これを受信した第1の情報処理装置100の受信装置170は、セッション鍵で受信データを復号し、コンテンツ番号を取得する。そして、第1の情報処理装置100の受信装置170は、大容量受信装置180からコンテンツ番号に応じた被暗号化コンテンツデータ $K_c(\text{Cont})$ 及び被暗号化コンテンツ鍵 $K_d(K_c)$ を検索して取り出す（手順⑦）。

続いて、第1の情報処理装置100の受信装置170は、記憶モジュール152内の配送鍵 K_d により被暗号化コンテンツ鍵 $K_d(K_c)$ からコンテンツ鍵 K_c を復号し（手順⑧）、復号したコンテンツ鍵 K_c に自己の識別情報 $ID1$ を付加する（手順⑨）。続いて、このデータ $(K_c + ID1)$ を、記憶モジュール152に登録されている第2の保存鍵 K_s' を用いて暗号化する（手順⑩）。そして、第1の情報処理装置100の受信装置170は、識別情報 $ID1$ が付加されて暗号化された被暗号化コンテンツ鍵 $K_s'(K_c + ID1)$ 及び被暗号化コンテンツデータ $K_c(\text{Cont})$ を、通信部110を介して第2の情報処理装置200の受信装置270へ送信する（手順⑪）。

続いて、第2の情報処理装置200の受信装置270は、第1の情報処理装置100の受信装置170から送信された被暗号化コンテンツ鍵 $K_s'(K_c + ID1)$ と被暗号化コンテンツデータ $K_c(\text{Cont})$ を受信して大容量記憶装置32に取り込む（手順⑫）。そして、上記受信装置270は、記憶モジュール252に記憶されている第

2の保存鍵 Ks' を用いて、受信した被暗号化コンテンツ鍵 Ks' ($Kc + ID1$)からコンテンツ鍵 Kc と識別情報 $ID1$ をコンテンツ鍵復号部33により復号する(手順⑬)。第2の情報処理装置200の受信装置270は、被暗号化コンテンツ鍵 Ks' ($Kc + ID1$)を復号することによって、コンテンツ鍵 Kc と第1の情報処理装置100の受信装置170の識別情報 $ID1$ を得ることができる。第2の情報処理装置200の受信装置270は、このコンテンツ鍵 Kc を用いてコンテンツ復号部34により、被暗号化コンテンツデータ $Kc(Cont)$ からコンテンツデータを復号する(手順⑭)。伸張部35は、上記コンテンツ復号部34により復号されたコンテンツデータに対して伸張処理を行う。伸張部35は、例えばATRA Cの伸張処理を行い、PCMデータにする(手順⑮)。そして、電子透かし埋込部36は、上記コンテンツ鍵復号部33で被暗号化コンテンツ鍵 Ks' ($Kc + ID1$)を復号することにより得られた上記第1の情報処理装置100固有の識別情報 $ID1$ を、伸張部35により伸張されたコンテンツデータに対して、電子透かし処理により埋め込み、を出力端子37から出力する(手順⑯)。

以上が第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送して再生する第2の手順である。

次に、第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送して再生する第3の手順について、図11を参照して説明する。

上述した第1の手順では、第2の情報処理装置200にコピー(転送)する際に第1の情報処理装置100の識別情報 $ID1$ をコ

ンテンツ鍵 Kc に付加していたが、以下に説明する第 3 の手順では、コンテンツ鍵 Kc にあらかじめ第 1 の情報処理装置 100 の識別情報 ID 1 を付加して大容量受信装置 180 に保存しておく。

すなわち、この第 3 の手順で第 1 の情報処理装置 100 から第 2 の情報処理装置 200 にコンテンツデータを転送する場合、第 1 の情報処理装置 100 の受信装置 170 の記憶モジュール 152 には、配送鍵 Kd と、この第 1 の情報処理装置の固有の識別情報 ID 1 があらかじめ保存されている。そして、第 1 の情報処理装置 100 は、衛星通信やインターネットを介してサービスプロバイダ 20 から送られてくるコンテンツ鍵 Kc で暗号化された被暗号化コンテンツデータ Kc(Cont) と、配送鍵 Kd で暗号化された被暗号化コンテンツ鍵 Kd(Kc)を受信装置 170 により受信し（手順①）、受信した被暗号化コンテンツデータ Kc(Cont) と被暗号化コンテンツ鍵 Kd(Kc)を大容量受信装置 180 に保存する（手順②）。

この第 3 の手順では、第 1 の情報処理装置 100 の受信装置 170 において、コンテンツ鍵復号部 23 は、上記配送鍵 Kd で暗号化された被暗号化コンテンツ鍵 Kd(Kc)を記憶モジュール 152 に保持されている配送鍵 Kd を用いて復号する（手順③）。識別情報付加部 24 は、上記コンテンツ鍵復号部 23 により復号されたコンテンツ鍵 Kc に第 1 の情報処理装置 100 の識別情報 ID 1 を付加する（手順④）、コンテンツ鍵暗号部 25 は、上記識別情報付加部 24 により識別情報 ID 1 が付加されたコンテンツ鍵 Kc+ID 1 を、第 1 の保存鍵 Ks を用いて暗号化する（手順⑤）。

そして、この第 3 の手順では、上記コンテンツ鍵暗号部 25 により暗号化された被暗号化コンテンツ鍵 Ks(Kc+ID 1)が大容量受

信装置 180 に保存される（手順⑥）。

このようにコンテンツ鍵 K_c で暗号化された被暗号化コンテンツデータ $K_c(\text{Cont})$ と、第 1 の保存鍵 K_s で暗号化された被暗号化コンテンツ鍵 $K_s(K_c + ID1)$ が大容量受信装置 180 に保存されている状態で、上述の図 2 に示した第 2 の情報処理装置 200 の受信装置 270 の操作入力部 230 から操作入力データすなわちユーザ指示情報が上位コントローラ 220 に入力されることにより、第 2 の情報処理装置 200 から第 1 の情報処理装置 100 へコンテンツの転送要求を行うためにコンテンツ(Content) 要求コマンドが送信されると（手順⑦）、第 1 の情報処理装置 100 と第 2 の情報処理装置 200 との間で相互認証を行う（手順⑧）。

上記手順⑦において、第 2 の情報処理装置 200 の受信装置 270 は、第 1 の情報処理装置 100 からコピー（転送）したいコンテンツデータのコンテンツ番号を含むコンテンツ要求コマンドをセッション鍵で暗号化して第 1 の情報処理装置 100 の受信装置 170 へ送る。上記コンテンツ要求コマンドを受信した第 1 の情報処理装置 100 の受信装置 170 は、手順⑧の相互認証を行を完了すると、セッション鍵で受信データを復号することによりコンテンツ番号を得て、大容量受信装置 180 からコンテンツ番号に応じた被暗号化コンテンツデータ $K_c(\text{Cont})$ 及び被暗号化コンテンツ鍵 $K_s(K_c + ID1)$ を検索して取り出す（手順⑨）。

続いて、第 1 の情報処理装置 100 の受信装置 170 は、記憶モジュール 152 内の第 1 の保存鍵 K_s を用いてコンテンツ鍵復号部 23 により上記被暗号化コンテンツ鍵 $K_s(K_c + ID1)$ から識別情報 $ID1$ が付加されたコンテンツ鍵 $(K_c + ID1)$ を復号し（手順

⑩)、復号したコンテンツ鍵($K_c + ID1$)を、記憶モジュール152に登録されている第2の保存鍵 K_s' を用いてコンテンツ鍵暗号化部25により暗号化する(手順⑪)。そして、識別情報 $ID1$ が付加されて暗号化された被暗号化コンテンツ鍵 K_s' ($K_c + ID1$)及び被暗号化コンテンツデータ $K_c(Cont)$ を通信部110を介して第2の情報処理装置200の受信装置270へ送信する(手順⑫)。

続いて、第2の情報処理装置200の受信装置270は、第1の情報処理装置100の受信装置170から送信された被暗号化コンテンツ鍵 K_s' ($K_c + ID1$)と被暗号化コンテンツデータ $K_c(Cont)$ を受信して大容量記憶装置280に取り込む(手順⑬)。そして、上記受信装置270は、記憶モジュール252に記憶されている第2の保存鍵 K_s' を用いて、受信した被暗号化コンテンツ鍵 K_s' ($K_c + ID1$)から識別情報が付加されたコンテンツ鍵($K_c + ID1$)をコンテンツ鍵復号部33により復号する(手順⑭)。なお、識別情報は、ともに伝送すればコンテンツ鍵に付加するのではなくしていなくてもよい。第2の情報処理装置200の受信装置270は、被暗号化コンテンツ鍵 K_s' ($K_c + ID1$)を復号することによって、コンテンツ鍵 K_c と第1の情報処理装置100の受信装置170の識別情報 $ID1$ を得ることができる。第2の情報処理装置200の受信装置270は、このコンテンツ鍵 K_c を用いてコンテンツ復号部34により、被暗号化コンテンツデータ $K_c(Cont)$ からコンテンツデータを復号する(手順⑮)。

続いて、第2の情報処理装置200の受信装置270は、伸張部35が、上記コンテンツ復号部34により復号されたコンテンツデータに対して、伸張処理を行う。例えば、伸張部35は、コンテン

ッデータに対してA T R A Cの伸張処理により、P C Mデータにする（手順⑯）。そして、電子透かし埋込部36は、上記コンテンツ鍵復号部33で被暗号化コンテンツ鍵 Ks' ($Kc + ID1$) から識別情報が付加されたコンテンツ鍵 ($Kc + ID1$) を復号することにより得られた上記第1の情報処理装置100固有の識別情報ID1を、伸張部35により伸張されたコンテンツデータに対して、電子透かし処理により埋め込み、出力端子37から出力する（手順⑰）。

以上が第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送して再生する第3の手順である。

以上のような手順で、第1の情報処理装置100の大容量受信装置180に記憶されたコンテンツデータを第2の情報処理装置200に転送することにより、コピーされたコンテンツデータには、コンテンツデータを買取った第1の情報処理装置100の固有の識別情報ID1が電子透かし処理により埋め込まれる。したがって、例えば、悪意を持ったユーザがコンテンツデータを複製して販売しようとしても、コンテンツデータには買取ったユーザの第1の情報処理装置100の識別情報が書き込まれ、契約外の違法な複製等をしたユーザの追跡が可能となり、犯罪抑止力が向上する。また、この第1の情報処理装置100及び第2の情報処理装置200では、その構成が簡易になり、効率よく第1の情報処理装置100の識別情報ID1をコンテンツデータに埋め込むことができる。

なお、以上の第1から第3の手順では、衛星通信やインターネットで受信したコンテンツデータ及びコンテンツ鍵は、一度第1の情報処理装置100の大容量受信装置180に保存していたが、以上

の第 1 から第 3 の手順に従いコンテンツデータをそのまま第 2 の情報処理装置 200 へ転送してもよい。

また、コンテンツ鍵が第 2 の情報処理装置 200 へ送信される前の第 2 の保存鍵 K_s' による暗号化の際に、暗号化をするコンテンツ鍵 K_c がコピー（転送）されたものであるという情報を付加してもよい。このことにより、このコンテンツ鍵を受信した第 2 の情報処理装置 200 では、このコンテンツ鍵 K_c の使用条件を制限することができる。例えば、そのコンテンツの著作権情報としてコピー（転送）不可を示す情報が付加されていた場合、第 2 の情報処理装置 200 で、そのコンテンツデータのデジタル出力を停止することができる。

さらに、上述の第 1 の実施の形態においては被暗号化コンテンツデータをインターネットや衛星通信等により電子配信しているが、被暗号化コンテンツデータは $CR-ROM$ などの情報記録媒体により供給するようにしても良い。

次に、本発明を適用した第 2 の実施の形態について図 1 及び図並びに図 12 及び図 13 を参照して説明する。

なお、この第 2 の実施の形態を説明するに当たり、上記第 1 の実施の形態で説明した構成要素と同一の構成要素については、図面中に同一の符号を付け、その詳細な説明を省略する。

この第 2 の実施の形態において、第 1 の情報処理装置 100 の受信装置 170 は、図 12 に示すように、上記暗号処理部 150 の相互認証モジュール 154 として、第 2 の情報処理装置 200 の受信装置 270 と相互認証用のインタフェース 45 を介して相互認証を行う相互認証部 43 と、相互認証に用いるセッション鍵を生成する

セッション鍵生成部 4 4 とを備えている。そして、この受信装置 1 7 0 は、上記暗号処理部 1 5 0 の暗号化／復号モジュール 1 5 5 として、配送鍵 K_d により暗号化された被暗号化コンテンツ鍵 K_d(K_c) からコンテンツ鍵 K_c を復号するコンテンツ鍵復号部 2 3 と、復号したコンテンツ鍵 K_c にこの第 1 の情報処理装置 1 0 0 固有の識別情報 I D 1 を付加する識別情報付加部 2 4 と、セッション鍵 K_t によりコンテンツ鍵 K_c を暗号化するコンテンツ鍵暗号化部 4 2 を備え、上記コンテンツ鍵暗号化部 4 2 により暗号化した被暗号化コンテンツ鍵 K_t(K_c) を通信部 1 1 0 を介して第 2 の情報処理装置 2 0 0 に送信するようになっている。この第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 の記憶モジュール 1 5 2 には、配送鍵 K_d、第 1 の保存鍵 K_s、この第 1 の情報処理装置 1 0 0 の固有の識別情報 I D 1 が保存されており、大容量記憶装置 1 8 0 には、コンテンツ鍵 K_c で暗号化されたコンテンツデータ K_c(Cont) と、配送鍵 K_d で暗号化された被暗号化コンテンツ鍵 K_d(K_c) が保存される。

また、第 2 の情報処理装置 2 0 0 の受信装置 2 7 0 は、図 1 3 に示すように、上記暗号処理部 2 5 0 の相互認証モジュールとして、第 1 の情報処理装置 1 0 0 の受信装置 1 7 0 と相互認証用のインタフェース 5 6 を介して相互認証を行う相互認証部 5 3 と、相互認証後の暗号化に用いるセッション鍵 K_t を生成するセッション鍵生成部 5 4 とを備えているとともに、セッション鍵 K_t により暗号化された被暗号化コンテンツ鍵 K_t(K_c) を復号するコンテンツ鍵復号部 5 2 と、この第 2 の情報処理装置 2 0 0 が独自に保持する第 2 の保存鍵 K_s' により、復号したコンテンツ鍵 K_c を暗号化して大容量記憶装置 2 8 0 に保存するコンテンツ鍵暗号化部 5 5 を備えている。

そして、この第2の情報処理装置200の受信装置270は、上記コンテンツ処理部260における復号モジュール及び電子透かし埋め込みモジュールとして、コンテンツ鍵Kcにより暗号化された被暗号化コンテンツデータKc(Cont)からコンテンツデータを復号するコンテンツ復号部34と、コンテンツ復号部34により復号されたコンテンツデータを伸張する伸張部35と、伸張部35により伸張されたコンテンツデータに対して電子透かし処理により第1の情報処理装置100固有の識別情報ID1を埋め込む電子透かし埋込部36とを備え、上記電子透かし埋込部36により識別情報ID1が埋め込まれたコンテンツデータを出力端子37から出力するようになっている。

この第2の実施の形態において、第1の情報処理装置100は、衛星通信やインターネットを介してサービスプロバイダ20から送られてくるコンテンツ鍵Kcで暗号化された被暗号化コンテンツデータKc(Cont)と、配送鍵Kdで暗号化された被暗号化コンテンツ鍵Kd(Kc)を受信装置170により受信し(手順①)、受信した被暗号化コンテンツデータKc(Cont)と被暗号化コンテンツ鍵Kd(Kc)を大容量記憶装置180に保存する(手順②)。

そして、第1の情報処理装置100から第2の情報処理装置200に被暗号化コンテンツデータKc(Cont)を転送(コピー)するに当たり、例えば上述の図2に示した第2の情報処理装置200の受信装置270の操作入力部230から操作入力データすなわちユーザ指示情報が上位コントローラ220に入力されることにより、第1の情報処理装置100の受信装置170の相互認証部43と第2の情報処理装置200の受信装置270の相互認証部53とで相互

認証を行う（手順③）。その際、第1の情報処理装置100の受信装置170のセッション鍵生成部44及び第2の情報処理装置200の受信装置270のセッション鍵生成部54で、セッション鍵 K_t が生成され、このセッション鍵 K_t が共有される（手順④）。

続いて第2の情報処理装置200の受信装置270は、第1の情報処理装置100の受信装置170からコピーしたいコンテンツデータのコンテンツ番号を含むコンテンツ要求コマンドを、セッション鍵 K_t で暗号化して第1の情報処理装置100の受信装置170へ送る（手順⑤）。

コンテンツ要求コマンドを受信した第1の情報処理装置100の受信装置170は、セッション鍵 K_t で受信したデータを復号し、コンテンツ番号を取得する。そして、第1の情報処理装置100の大容量記憶装置180からコンテンツ番号に応じた被暗号化コンテンツデータ $K_c(\text{Cont})$ と被暗号化コンテンツ鍵 $K_d(K_c)$ を検索して取り出す（手順⑥）。

続いて、第1の情報処理装置100の受信装置170は、コンテンツ鍵復号部23により記憶モジュール152内に保持している配送鍵 K_d で被暗号化コンテンツ鍵 $K_d(K_c)$ からコンテンツ鍵 K_c を復号し（手順⑦）、識別情報付加部24により復号したコンテンツ鍵 K_c に自己の識別情報 ID_1 を付加する（手順⑧）。

続いて、第1の情報処理装置100の受信装置41は、コンテンツ鍵暗号化部42により、自己の識別情報 ID_1 を付加したコンテンツ鍵 $(K_c + ID_1)$ をセッション鍵 K_t を用いて暗号化する（手順⑨）。そして、これらの被暗号化コンテンツ鍵 $K_t(K_c + ID_1)$ 及び被暗号化コンテンツデータ $K_c(\text{Cont})$ を通信部110を介して

第2の情報処理装置200の受信装置270へ送信する(手順⑩)。

第2の情報処理装置200の受信装置270は、第1の情報処理装置100の受信装置170から送信されたセッション鍵 K_t により暗号化された被暗号化コンテンツ鍵 $K_t(K_c + ID1)$ と、コンテンツ鍵 K_c により暗号化された被暗号化コンテンツデータ $K_c(Cont)$ を、通信部210を介して受信する(手順⑪)。第2の情報処理装置200の受信装置270は、コンテンツ鍵復号部52により、セッション鍵生成部54で生成したセッション鍵 K_t を用いて受信した被暗号化コンテンツ鍵 $K_t(K_c + ID1)$ を復号する(手順⑫)。

第2の情報処理装置200の受信装置51は、被暗号化コンテンツ鍵 $K_t(K_c + ID1)$ から識別情報が付加されたコンテンツ鍵 $(K_c + ID1)$ を復号することによって、コンテンツ鍵 K_c と第1の情報処理装置100の識別情報 $ID1$ を得ることができる。第2の情報処理装置200の受信装置51は、コンテンツ復号部34により、このコンテンツ鍵 K_c を用いて被暗号化コンテンツデータ $K_c(Cont)$ からコンテンツデータ $Cont$ を復号する(手順⑬)。そして、伸張部35は、コンテンツ復号部34により復号したコンテンツデータの $ATRA C$ 等の伸張処理を行う(手順⑭)。そして、電子透かし処理部36は、コンテンツ鍵復号部33でコンテンツ鍵 $K_t(K_c + ID1)$ から識別情報が付加されたコンテンツ鍵 $(K_c + ID1)$ を復号することにより得られた第1の情報処理装置100固有の識別情報データ $ID1$ を、コンテンツ復号部34により復号したコンテンツデータ $Cont$ に対して、電子透かし処理により埋め込み、出力端子37を介して出力する(手順⑮)。

また、第2の情報処理装置200の受信装置270は、コンテン

ツ鍵復号部 5 2 により復号されたコンテンツ鍵 K_c を、記憶モジュール 2 5 2 に記憶された第 2 の保存鍵 K_s' を用いてコンテンツ鍵暗号化部 5 5 により暗号化する。そして、第 2 の保存鍵 K_s' により暗号化した被暗号化コンテンツ鍵 $K_s'(K_c)$ を大容量記憶装置 2 8 0 に記憶する（手順⑯）。

以上のような手順で、第 1 の情報処理装置 1 0 0 の大容量受信装置 1 8 0 に記憶されたコンテンツデータを第 2 の情報処理装置 2 0 0 に転送することにより、転送されたコンテンツデータには、コンテンツを買い取った第 1 の情報処理装置 1 0 0 の固有の識別情報 ID_1 が電子透かし処理により埋め込まれる。したがって、例えば、悪意を持ったユーザがコンテンツを複製して販売しようとしても、コンテンツには買い取ったユーザの識別情報が書き込まれ、契約外の違法な複製等をしたユーザの追跡が可能となり、犯罪抑止力が向上する。また、この第 1 の情報処理装置 1 0 0 及び第 2 の情報処理装置 2 0 0 では、その構成が簡易になり、効率よく第 1 の情報処理装置 1 0 0 の識別情報 ID_1 をコンテンツデータに埋め込むことができる。また、特に、第 2 の実施の形態では、第 2 の情報処理装置 2 0 0 の第 2 の保存鍵 K_s' を伝送して第 1 の情報処理装置 1 0 0 に供給する必要がないため、より安全性が高まる。

次に図 1 及び図 2 並びに図 1 4 及び図 1 5 を参照して、本発明の第 3 の実施の形態について説明する。

この第 3 の実施の形態では、図 1 4 に示すように、暗号化されていないコンテンツ（例えば音楽データ、映像データ、書籍等の文書データ、静止画データ等）を保持するコンテンツ・プロバイダ 1 0 は、自己が保持する又は生成したコンテンツ鍵 K_c でコンテンツデ

ータ(Cont)を暗号化し、これをサービス・プロバイダ20に供給する(手順①)。また、コンテンツ・プロバイダ20は、コンテンツ鍵Kcを、鍵管理センタ30に供給する(手順②)。このコンテンツ鍵Kcは、コンテンツ毎に違うものを用いても良いし、同じものでも良い。

鍵管理センタ30は、自己の保持する配送鍵(ユーザの受信装置170毎にすべて異なる鍵にしても良いし、すべて共通でも良い)Kdでこのコンテンツ鍵Kcを暗号化して、ユーザの受信装置170からの要求に応じて、この配送鍵Kdにより暗号化した被暗号化コンテンツ鍵Kd(Kc)をユーザの受信装置170に供給する(手順③)。

ユーザの情報処理装置100の受信装置170は、衛星通信やケーブル通信、インターネット等を介して、サービス・プロバイダー20から、コンテンツ鍵Kcにより暗号化された被暗号化コンテンツデータKc(Cont)を受信する(手順④)。被暗号化コンテンツデータKc(Cont)を受信した受信装置170は、暗号を解くために、鍵管理センタ30に復号用のコンテンツ鍵Kcを要求する(手順⑤)。鍵管理センタ30は、コンテンツ鍵Kcの送信要求があると、配送鍵Kdにより暗号化された被暗号化コンテンツ鍵Kd(Kc)をユーザの情報処理装置100に送信する(手順⑥)。このとき、鍵管理センタ30は、課金処理も同時に行う。この課金処理は、鍵管理センタ30に登録されたユーザの銀行口座から料金を引き落としても良いし、ユーザの受信装置170からクレジットカード番号を送信してもらいこのカード番号に従って課金しても良い。また、情報処理装置100の受信装置170に備え付けられたICカードに蓄

えられているプリペイドから必要な料金を引き落としても良い。

暗号化されたコンテンツ鍵 $K_d(K_c)$ を受信したユーザの情報処理装置 100 の受信装置 170 は、記憶モジュール 152 に保持されている配送鍵 K_d で被暗号化コンテンツ鍵 $K_d(K_c)$ からコンテンツ鍵 K_c を復号し、復号したコンテンツ鍵 K_c を用いて暗号化されたコンテンツを復号することができる。

上記情報処理装置 100 の受信装置 170 は、復号したコンテンツ鍵 K_c を、独自に保持する保存用鍵 K_s で暗号化して大容量記憶装置 180 に保存する（手順⑦）。これは、コンテンツ鍵 K_c を配送するときに使った配送用鍵 K_d が一定期毎に変わる可能性があるためである。また、暗号化しないままコンテンツ鍵 K_c を保存することはコンテンツを暗号化しないで保存することと本質的に変わらず、他人に自由に内容を見られる可能性があるためである。また、ユーザの受信装置 170 は、自己が保持する保存用鍵 K_s でコンテンツ鍵 K_c を暗号化することにより、同一のコンテンツを復号する際に、再度課金されることなく使用することができる。

次に、ユーザの持つ情報処理装置 100 により、保存用鍵 K_s で暗号化した被暗号化コンテンツデータ $K_s(Cont)$ の復号手順と、復号したコンテンツデータを他の機器に転送するための手順について説明する。

この情報処理装置 100 における受信装置 170 の大容量記憶装置 180 には、被暗号化コンテンツデータ $K_c(Cont)$ と、被暗号化コンテンツ鍵 $K_s(K_c)$ が保存されている。また、受信装置 170 の内部に備えられた記憶モジュール 152 には、保存用鍵 K_s とこの受信装置 170 の識別情報（ID）が保存されている。

上記大容量記憶装置 180 内の被暗号化コンテンツデータ Kc(Cont) からコンテンツデータを復号して他の機器に転送する場合、

情報処理装置 100 の受信装置 170 は、まず、大容量記憶装置 180 から被暗号化コンテンツ鍵 Ks(Kc)を読み出し(手順①)、上記記憶モジュール 152 から読み出される保存用鍵 Ks を用いてコンテンツ鍵復号部 113 により上記被暗号化コンテンツ鍵 Ks(Kc)から使用可能なコンテンツ鍵 Ks を復号する(手順②)。次に、上記受信装置 170 は、大容量記憶装置 180 から被暗号化コンテンツデータ Kc(Cont)を読み出し(手順③)、上記コンテンツ鍵 Kc を用いてコンテンツ復号部 114 により上記被暗号化コンテンツデータ Kc(Cont) からコンテンツデータを復号し(手順④)、伸張部 116 により復号したコンテンツデータを ATRAC で伸張して PCM データとして(手順⑤)、伸張したコンテンツデータに対して電子透かし埋込部 115 でこの受信装置 170 の固有の識別情報を埋め込み、出力端子 118 を介して出力する(手順⑥)。

また、このコンテンツデータを他の装置に転送する場合には、上記受信装置 170 は、コンテンツ暗号化部 117 により同一のコンテンツ鍵 Kc でコンテンツデータを暗号化し、暗号化した被暗号化コンテンツデータ Kc(Cont) を出力端子 119 を介して出力する(手順⑦)。

このように、この受信装置 170 から外部装置に転送されるコンテンツデータには、コンテンツを買い取ったユーザの情報処理装置 100 において受信装置 170 固有の識別情報が電子透かし処理により埋め込まれる。したがって、例えば、悪意を持ったユーザがコンテンツを複製して販売しようとしても、コンテンツには買い取っ

たユーザの識別情報が書き込まれるため、ユーザの追跡が可能となり、犯罪抑止力が向上する。

請 求 の 範 囲

1. 被暗号化コンテンツ (Content) 信号を受信する受信手段と、
上記受信手段で受信した被暗号化コンテンツ信号を記憶する記憶手段と、

ユーザ指示情報として、上記記憶手段に記憶された上記被暗号化コンテンツ信号を復号する指示が与えられたときに、上記記憶手段に記憶された上記被暗号化コンテンツ信号を復号する復号手段と、

上記復号手段により復号されたコンテンツ信号に識別情報を付加する識別情報付加手段と

を備えること特徴とするコンテンツ信号受信装置。

2. 上記識別情報は、当該コンテンツ信号受信装置固有の識別情報であることを特徴とする請求の範囲第1項記載のコンテンツ信号受信装置。

3. 上記識別情報は、電子透かしとして上記コンテンツ信号に埋め込まれることを特徴とする請求の範囲第1項記載のコンテンツ信号受信装置。

4. 上記被暗号化コンテンツ信号は、コンテンツ鍵によって暗号化されており、

上記受信手段は、上記コンテンツ鍵を受信し、

上記復号手段は、上記受信手段で受信したコンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第1項記載のコンテンツ信号受信装置。

5. 上記コンテンツ鍵は、配送鍵によって暗号化されており、

上記受信手段は、上記配送鍵によって暗号化されている上記コンテンツ鍵を受信し、

上記復号手段は、上記配送鍵によって暗号化されているコンテンツ鍵を復号し、復号したコンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第4項記載のコンテンツ信号受信装置。

6. 上記配送鍵は、定期的に更新されることを特徴とする請求の範囲第4項記載のコンテンツ信号受信装置。

7. 外部装置から被暗号化コンテンツ信号及び識別情報を受信する受信手段と、

上記被暗号化コンテンツ信号を復号する復号手段と、

上記復号手段により復号されたコンテンツ信号に識別情報を付加する識別情報付加手段と

を備えること特徴とするコンテンツ信号受信装置。

8. 上記識別情報は、上記外部装置固有の識別情報であることを特徴とする請求の範囲第7項記載のコンテンツ信号受信装置。

9. 上記識別情報は、電子透かしとして上記コンテンツ信号に埋め込まれることを特徴とする請求の範囲第7項記載のコンテンツ信号受信装置。

10. コンテンツ鍵を用いて、被暗号化コンテンツ信号を復号する復号手段と、

上記復号手段により上記コンテンツ鍵を復号するごとにログ情報を生成するログ情報生成手段と、

上記ログ情報を記憶する記憶手段と、

所定のタイミングで上記ログ情報を送信する送信手段と

を備えることを特徴とするコンテンツ処理装置。

11. 被暗号化コンテンツ信号を復号するためのコンテンツ鍵を受信する受信手段を備え、

上記復号手段は、上記受信手段により受信したコンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

12. 上記受信手段は、上記被暗号化コンテンツ信号を受信することを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

13. 上記送信手段は、一定期間毎に上記ログ情報を送信することを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

14. 上記受信手段が受信する上記コンテンツ鍵は、所定期間毎に更新される配送鍵で暗号化されており、

上記送信手段は、上記配送鍵を所定回数復号したときに、上記ログ情報を送信することを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

15. 上記受信手段が受信する上記コンテンツ鍵は、所定期間毎に更新される配送鍵で暗号化されており、

上記送信手段は、上記配送鍵が更新されたときに、上記ログ情報を送信することを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

16. 上記所定期間は、一定の期間であることを特徴とする請求の範囲第15項記載のコンテンツ処理装置。

17. 上記コンテンツ鍵は、各種類のコンテンツ信号毎に設けられており、

上記復号手段によって復号された各コンテンツ鍵を保存鍵で暗号

化する暗号化手段と、

上記暗号化手段によって暗号化されたコンテンツ鍵を記憶する記憶手段を

さらに備えることを特徴とする請求の範囲第10項記載のコンテンツ処理装置。

18. 被暗号化コンテンツ信号を復号するためのコンテンツ鍵を所定期間毎に更新される配送鍵で暗号化して得た被暗号化コンテンツ鍵を受信する受信手段と、

上記コンテンツ鍵によって上記被暗号化コンテンツ信号を復号する復号手段と、

上記被暗号化コンテンツ信号の使用に関する課金情報を生成する課金情報生成手段と、

上記課金情報を記憶する記憶手段と、

上記配送鍵が更新されたときに、上記課金情報を送信する送信手段と

を備えること特徴とするコンテンツ処理装置。

19. 被暗号化コンテンツ信号を復号するための鍵であり、所定期間毎に更新される配送鍵を受信する受信手段と、

上記配送鍵に基づいて、上記被暗号化コンテンツ信号を復号する復号手段と、

上記被暗号化コンテンツ信号の使用に関する課金情報を生成する課金情報生成手段と、

上記課金情報を記憶する記憶手段と、

上記配送鍵が更新されたときに、上記課金情報を送信する送信手段と

を備えること特徴とするコンテンツ処理装置。

20. 上記被暗号化コンテンツ信号はコンテンツ鍵を用いて暗号化されており、

上記受信手段は、上記配送鍵を用いて暗号化されている上記コンテンツ鍵を受信し、

上記復号手段は、上記配送鍵を用いて暗号化されているコンテンツ鍵を復号し、復号したコンテンツ鍵を用いて上記被暗号化コンテンツ信号を復号する

ことを特徴とする請求の範囲第19項記載のコンテンツ処理装置。

21. コンテンツ信号を復号するためのコンテンツ鍵が暗号化されてなる被暗号化コンテンツ鍵を復号する復号手段と、

上記コンテンツ鍵を復号する毎にログ情報を生成するログ情報生成手段と、

上記コンテンツ鍵を保存鍵で暗号化する暗号化手段と、

上記復号手段、上記ログ情報生成手段及び上記暗号化手段を内蔵する1チップモジュールとからなる暗号処理装置。

22. 上記復号手段によって復号された上記コンテンツ鍵に、識別情報を付加し、上記暗号化手段に出力する識別情報付加手段を

さらに備えることを特徴とする請求の範囲第21項記載の暗号処理装置。

23. 上記識別情報は、電子透かしとして上記コンテンツ鍵に埋め込まれることを特徴とする請求の範囲第22項記載の暗号処理装置。

24. 被暗号化コンテンツ信号を記憶する記憶手段と、識別情報を記憶する記憶手段と、上記被暗号化コンテンツ信号及び上記識別

情報を送信する送信手段とを備える第 1 のコンテンツ処理装置と、

上記被暗号化コンテンツ信号及び上記識別情報を受信する受信手段と、上記被暗号化コンテンツ信号を復号する復号手段と、上記復号手段によって復号されたコンテンツ信号に上記識別情報を付加する識別情報付加手段とを備える第 2 のコンテンツ処理装置と

を備えるコンテンツ処理システム。

25. コンテンツ鍵によって被暗号化コンテンツ信号を復号する復号手段と、上記復号手段によって上記コンテンツ鍵を復号する毎にログ情報を生成するログ情報生成手段と、上記ログ情報を記憶する記憶手段と、所定のタイミングで上記ログ情報を送信する送信手段とを備えるコンテンツ処理装置と、

上記ログ情報を受信する受信手段と、上記ログ情報に基づいて課金処理を行う課金手段とを備える課金処理装置と

からなるコンテンツ処理システム。

26. 被暗号化コンテンツ (Content) 信号を受信し、

受信した被暗号化コンテンツ信号を記憶し、

ユーザ指示情報として、記憶した上記被暗号化コンテンツ信号を復号する指示が与えられたときに、記憶した上記被暗号化コンテンツ信号を復号し、

復号したコンテンツ信号に識別情報を付加するステップからなることを特徴とするコンテンツ信号受信方法。

27. 上記識別情報は、コンテンツ信号受信装置固有の識別情報であることを特徴とする請求の範囲第 26 項記載のコンテンツ信号受信方法。

28. 上記識別情報は、電子透かしとして上記コンテンツ信号に

埋め込まれることを特徴とする請求の範囲第 26 項記載のコンテンツ信号受信方法。

29. 上記被暗号化コンテンツ信号は、コンテンツ鍵によって暗号化されており、

受信した上記コンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第 26 項記載のコンテンツ信号受信方法。

30. 上記コンテンツ鍵は、配送鍵によって暗号化されており、

上記配送鍵によって暗号化されている上記コンテンツ鍵を受信し、

上記配送鍵によって暗号化されているコンテンツ鍵を復号し、復号したコンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第 29 項記載のコンテンツ信号受信方法。

31. 上記配送鍵は、定期的に更新されることを特徴とする請求の範囲第 29 項記載のコンテンツ信号受信方法。

32. 外部から被暗号化コンテンツ信号及び識別情報を受信し、

上記被暗号化コンテンツ信号を復号し、

復号した上記コンテンツ信号に識別情報を付加するステップからなることを特徴とするコンテンツ信号受信方法。

33. 上記識別情報は、上記外部装置固有の識別情報であることを特徴とする請求の範囲第 32 項記載のコンテンツ信号受信方法。

34. 上記識別情報は、電子透かしとして上記コンテンツ信号に埋め込まれることを特徴とする請求の範囲第 32 項記載のコンテンツ信号受信方法。

35. コンテンツ鍵を用いて、被暗号化コンテンツ信号を復号

し、

上記コンテンツ鍵を復号するごとにログ情報を生成し、

上記ログ情報を記憶し、

所定のタイミングで上記ログ情報を送信するステップからなることを特徴とするコンテンツ処理方法。

36. 被暗号化コンテンツ信号を復号するためのコンテンツ鍵を受信し、

受信した上記コンテンツ鍵を用いて、上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

37. 上記被暗号化コンテンツ信号を受信することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

38. 一定期間毎に上記ログ情報を送信することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

39. 受信する上記コンテンツ鍵は、所定期間毎に更新される配送鍵で暗号化されており、

上記配送鍵を所定回数復号したときに、上記ログ情報を送信することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

40. 受信する上記コンテンツ鍵は、所定期間毎に更新される配送鍵で暗号化されており、

上記配送鍵が更新されたときに、上記ログ情報を送信することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

41. 上記所定期間は、一定の期間であることを特徴とする請求の範囲第40項記載のコンテンツ処理方法。

42. 上記コンテンツ鍵は、各種類のコンテンツ信号毎に設けら

れており、

復号された各コンテンツ鍵を保存鍵で暗号化し、

暗号化されたコンテンツ鍵を記憶することを特徴とする請求の範囲第35項記載のコンテンツ処理方法。

43. 被暗号化コンテンツ信号を復号するためのコンテンツ鍵を所定期間毎に更新される配送鍵で暗号化して得た被暗号化コンテンツ鍵を受信し、

上記コンテンツ鍵によって上記被暗号化コンテンツ信号を復号し、

上記被暗号化コンテンツ信号の使用に関する課金情報を生成し、

上記課金情報を記憶し、

上記配送鍵が更新されたときに、上記課金情報を送信するステップからなること特徴とするコンテンツ処理方法。

44. 被暗号化コンテンツ信号を復号するための鍵であり、所定期間毎に更新される配送鍵を受信し、

上記配送鍵に基づいて、上記被暗号化コンテンツ信号を復号し、

上記被暗号化コンテンツ信号の使用に関する課金情報を生成し、

上記課金情報を記憶し、

上記配送鍵が更新されたときに、上記課金情報を送信するステップからなること特徴とするコンテンツ処理方法。

45. 上記被暗号化コンテンツ信号はコンテンツ鍵を用いて暗号化されており、

上記配送鍵を用いて暗号化されている上記コンテンツ鍵を受信し、

上記配送鍵を用いて暗号化されているコンテンツ鍵を復号し、復号したコンテンツ鍵を用いて上記被暗号化コンテンツ信号を復号することを特徴とする請求の範囲第44項記載のコンテンツ処理方法。

1/15

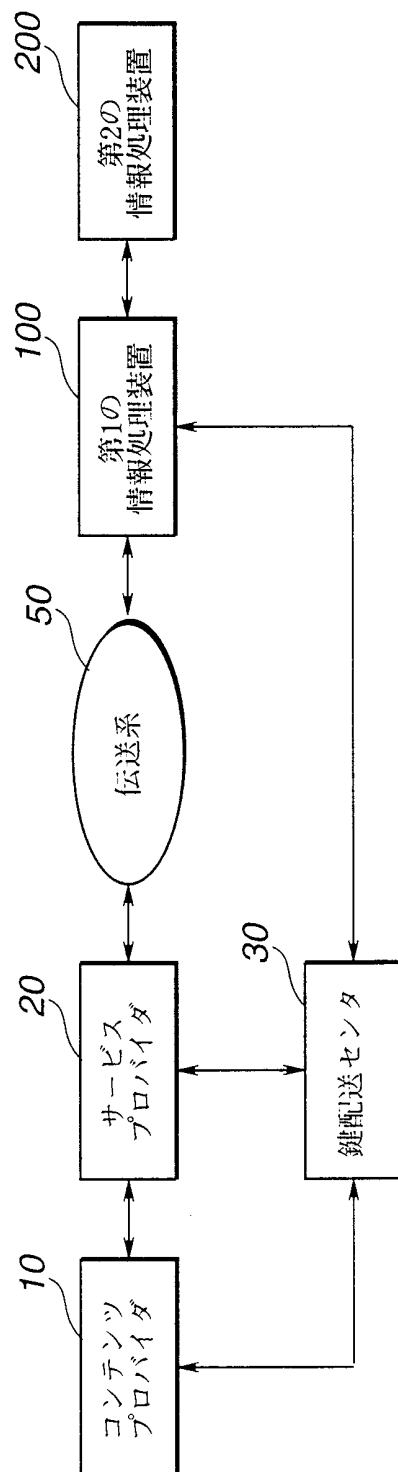


FIG.1

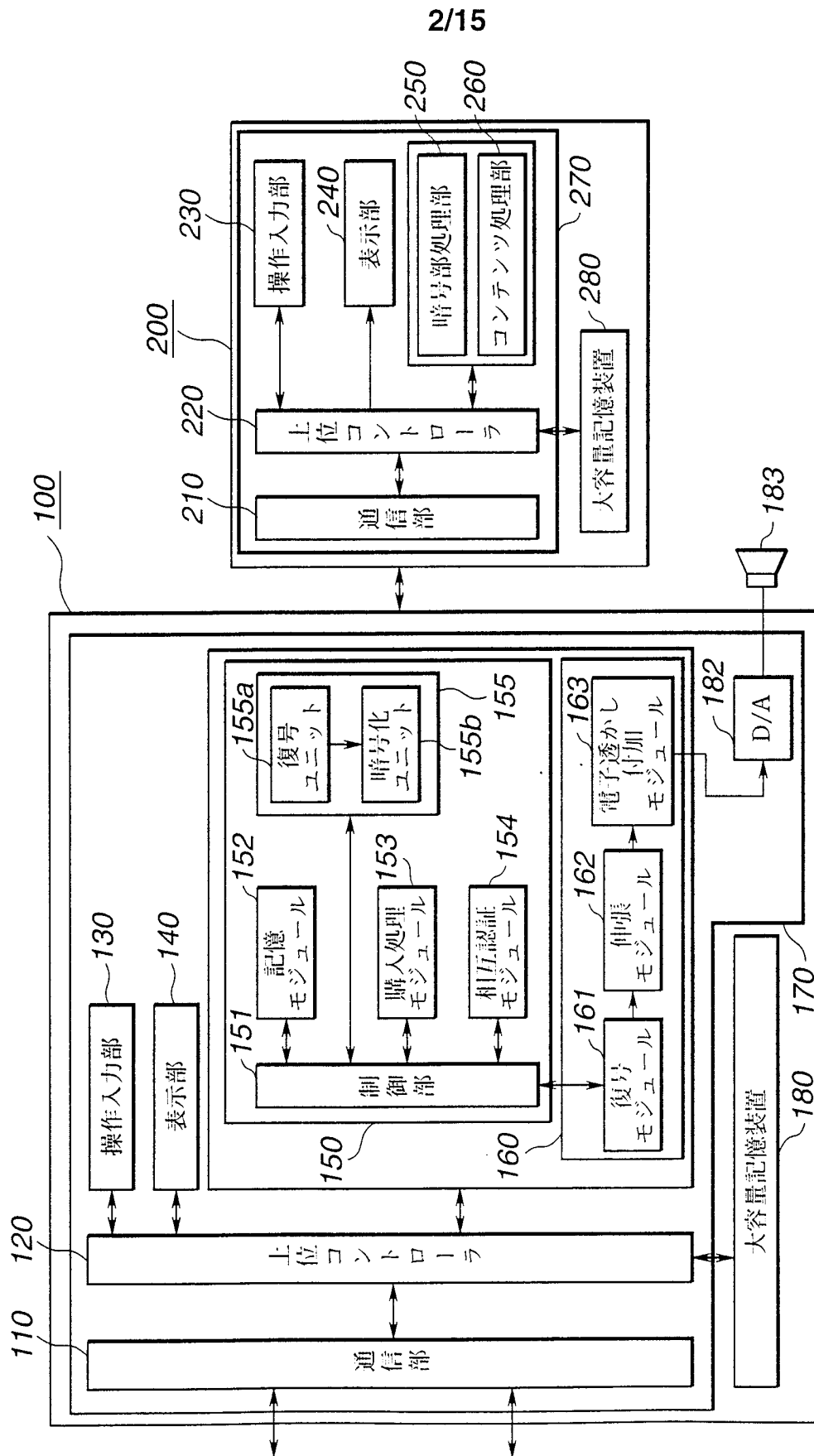


FIG.2

3/15

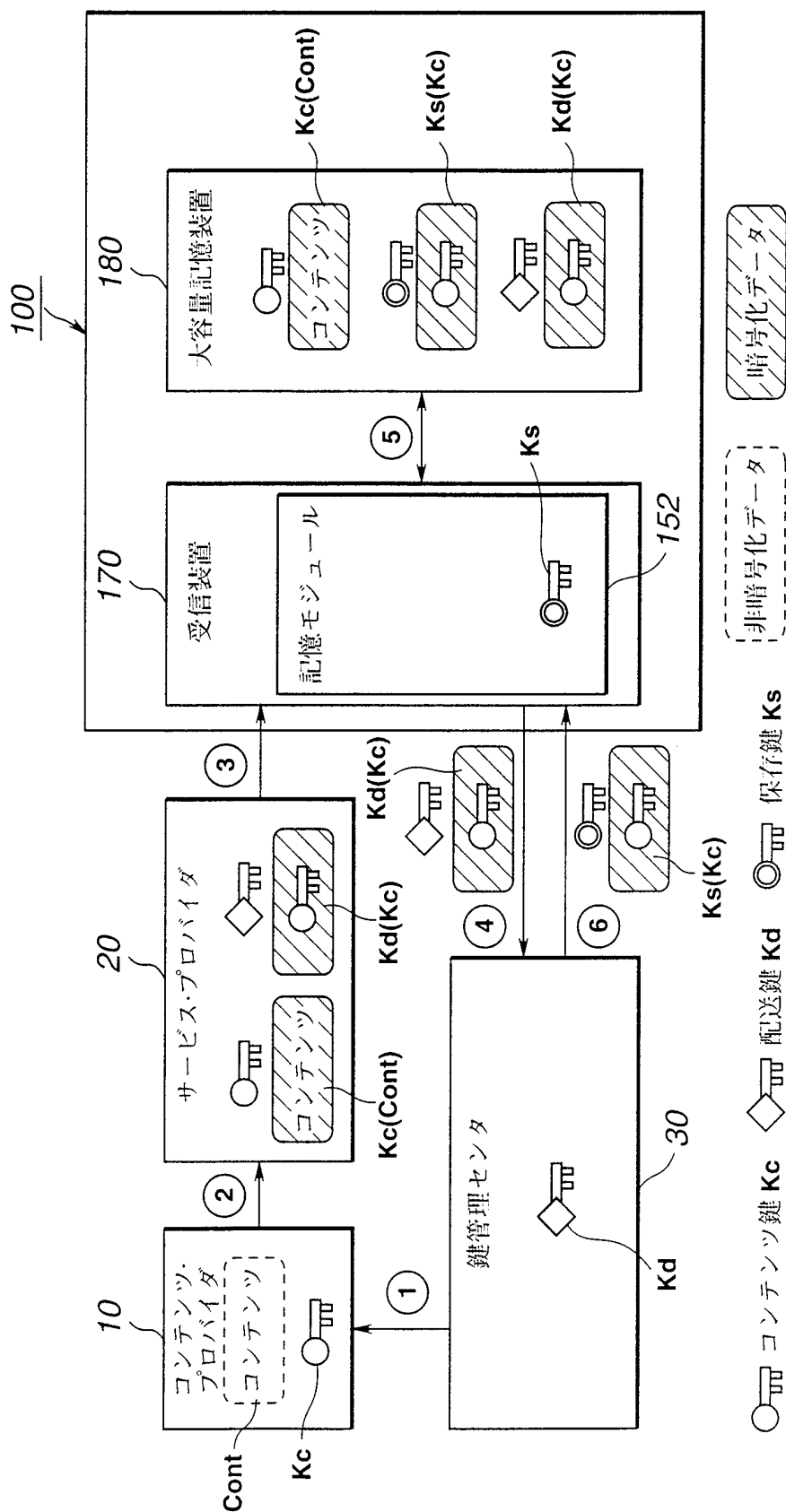


FIG.3

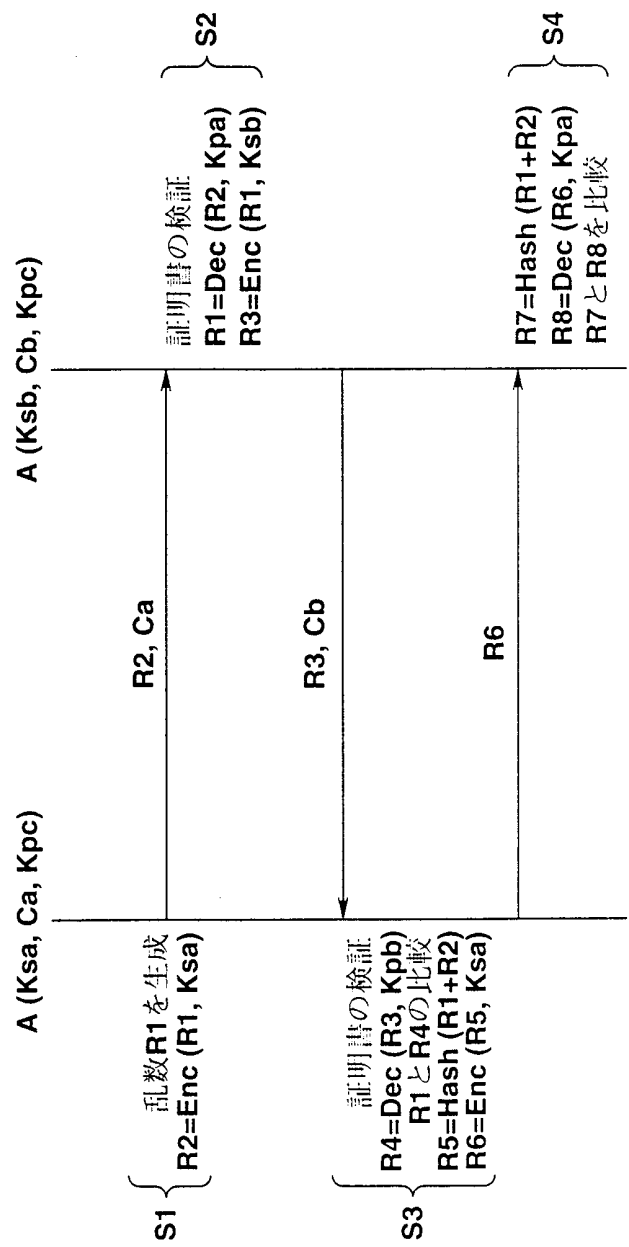


FIG.4

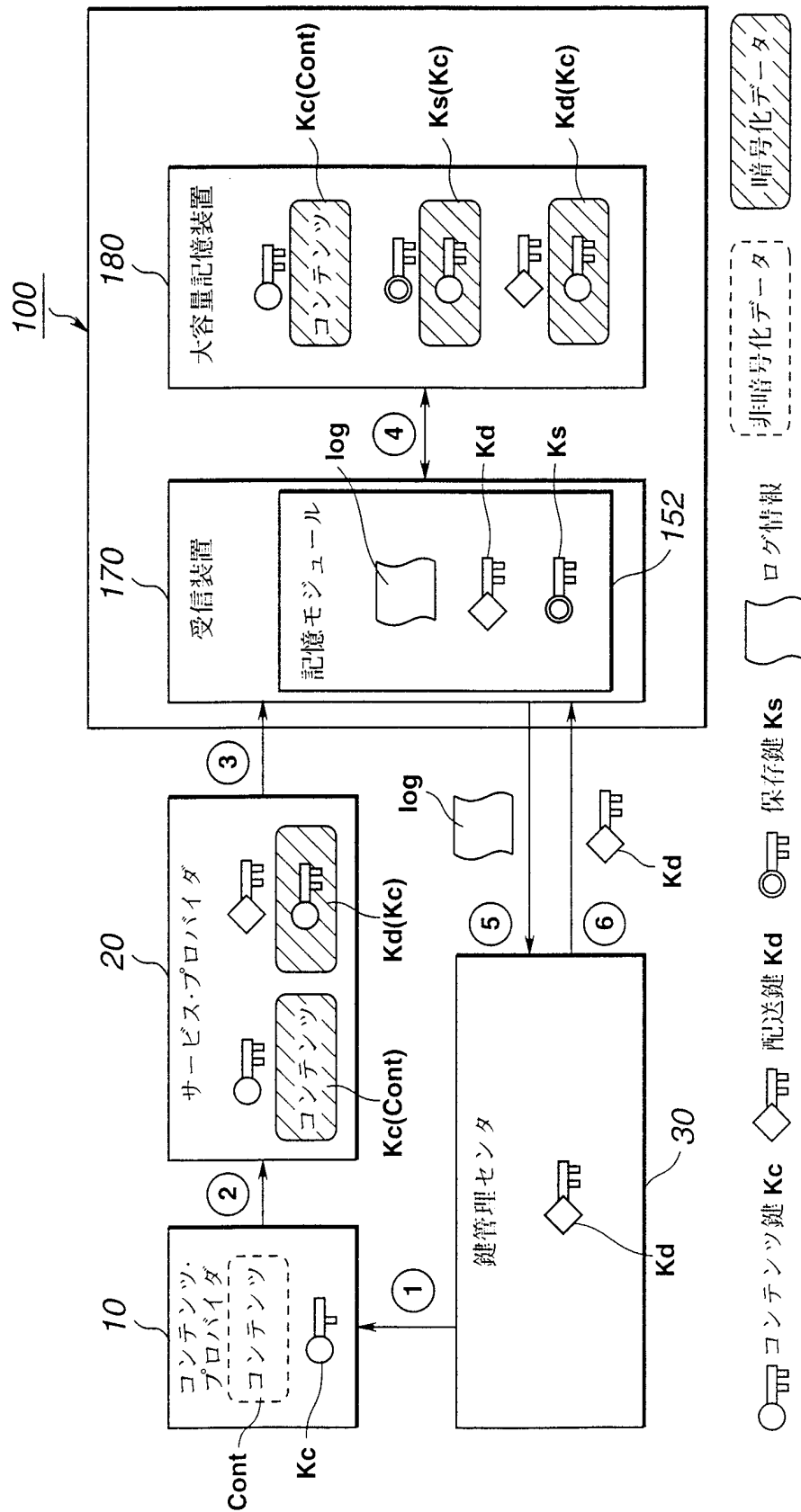


FIG.5

6/15

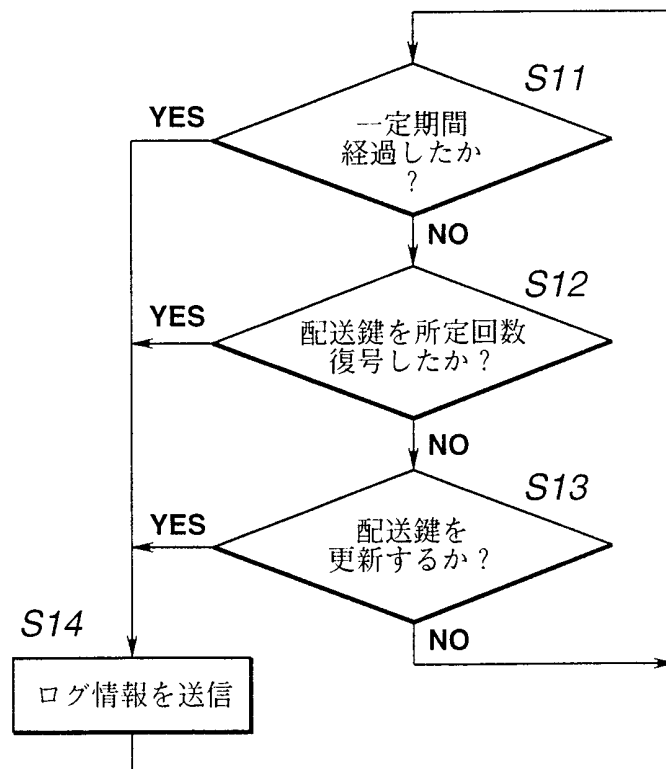


FIG.6

7/15

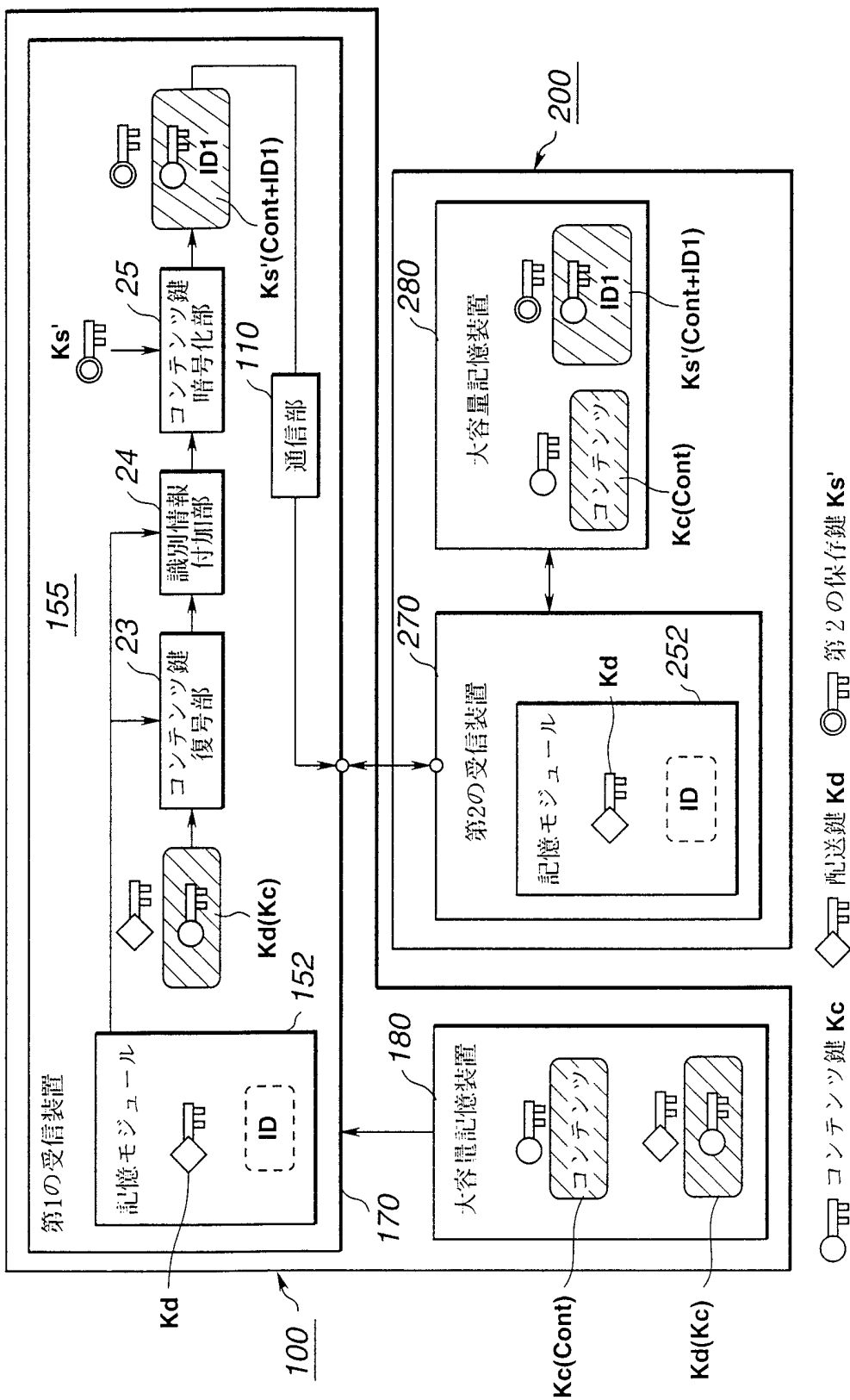


FIG.7

8/15

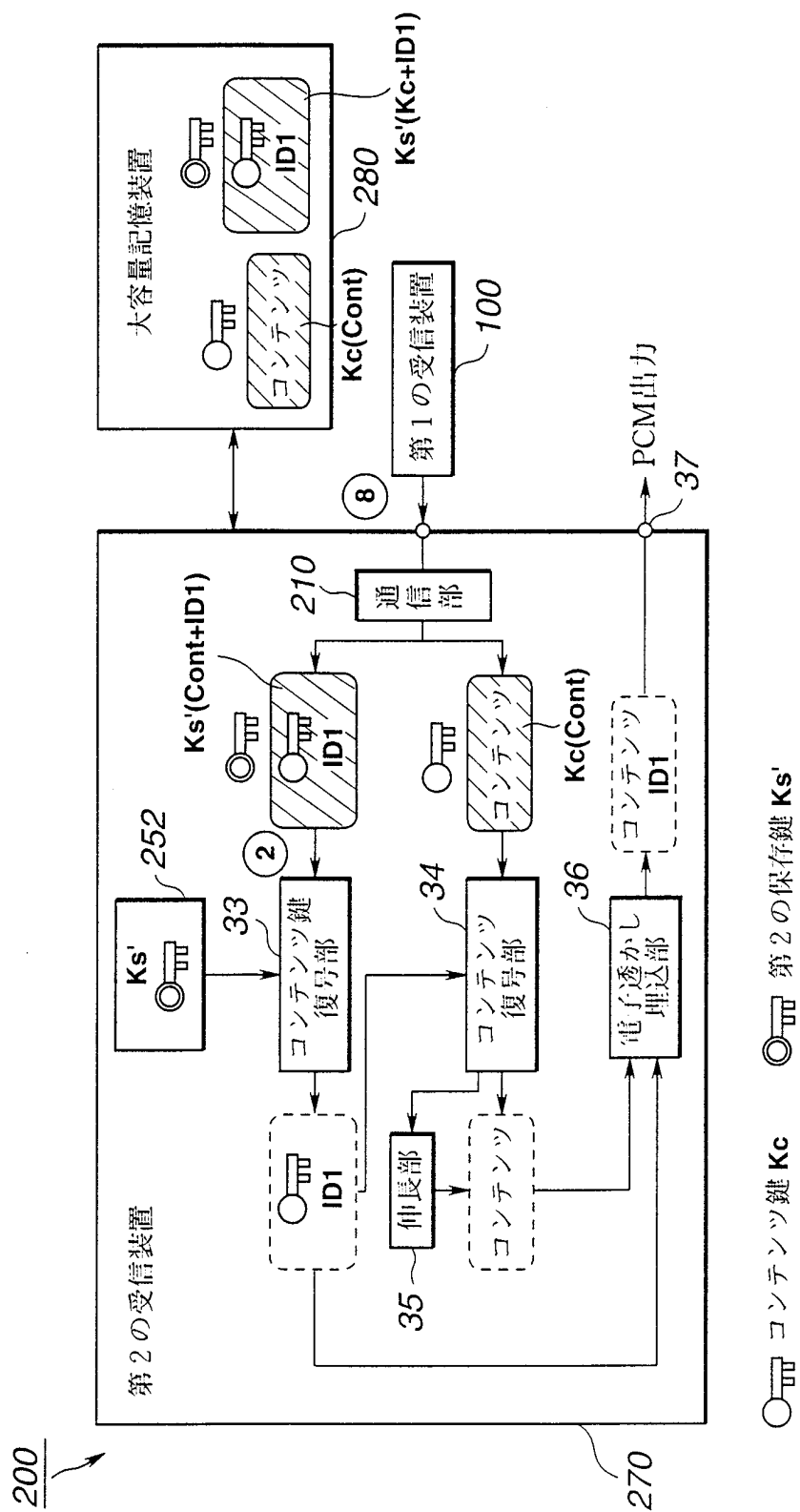


FIG.8

9/15

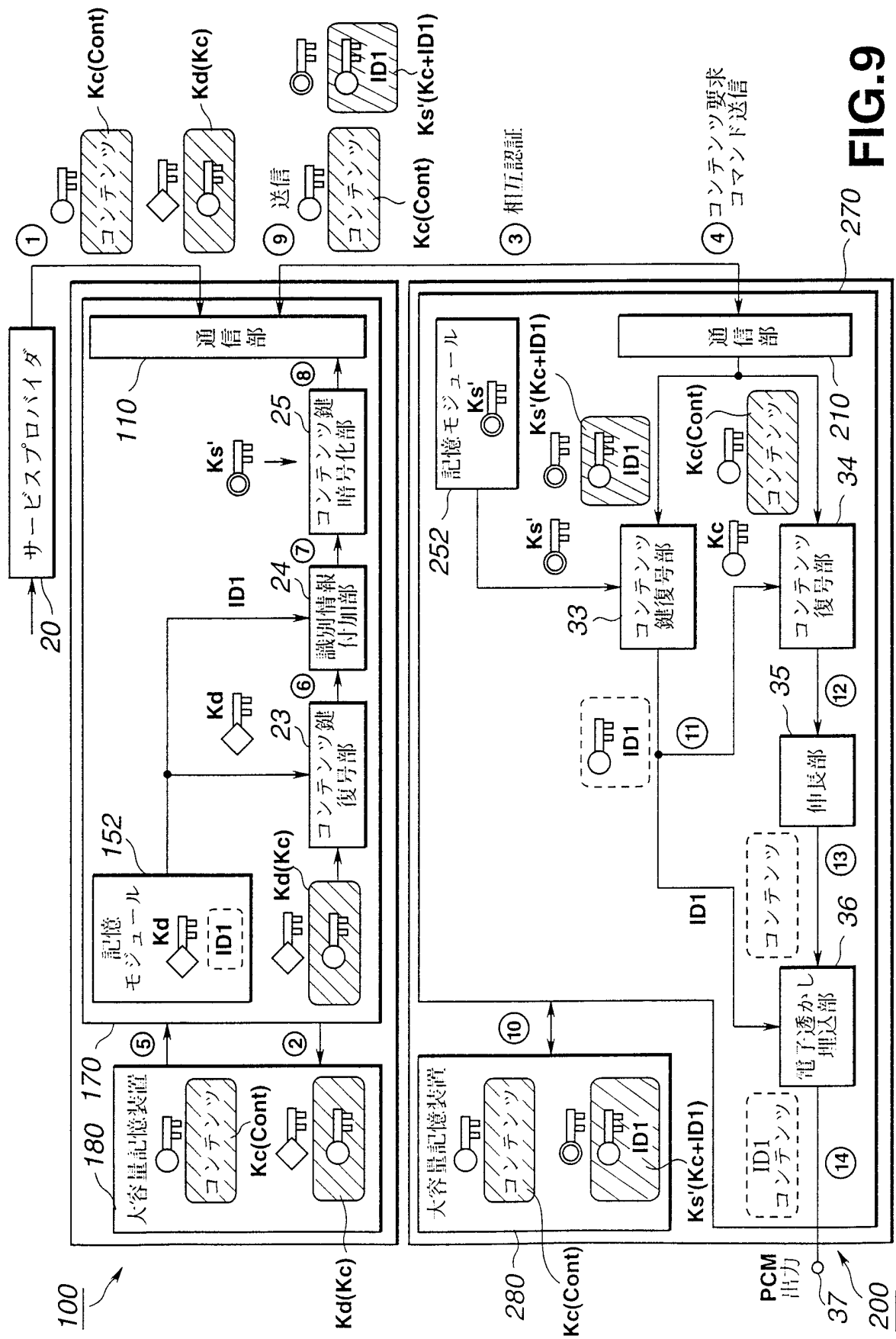
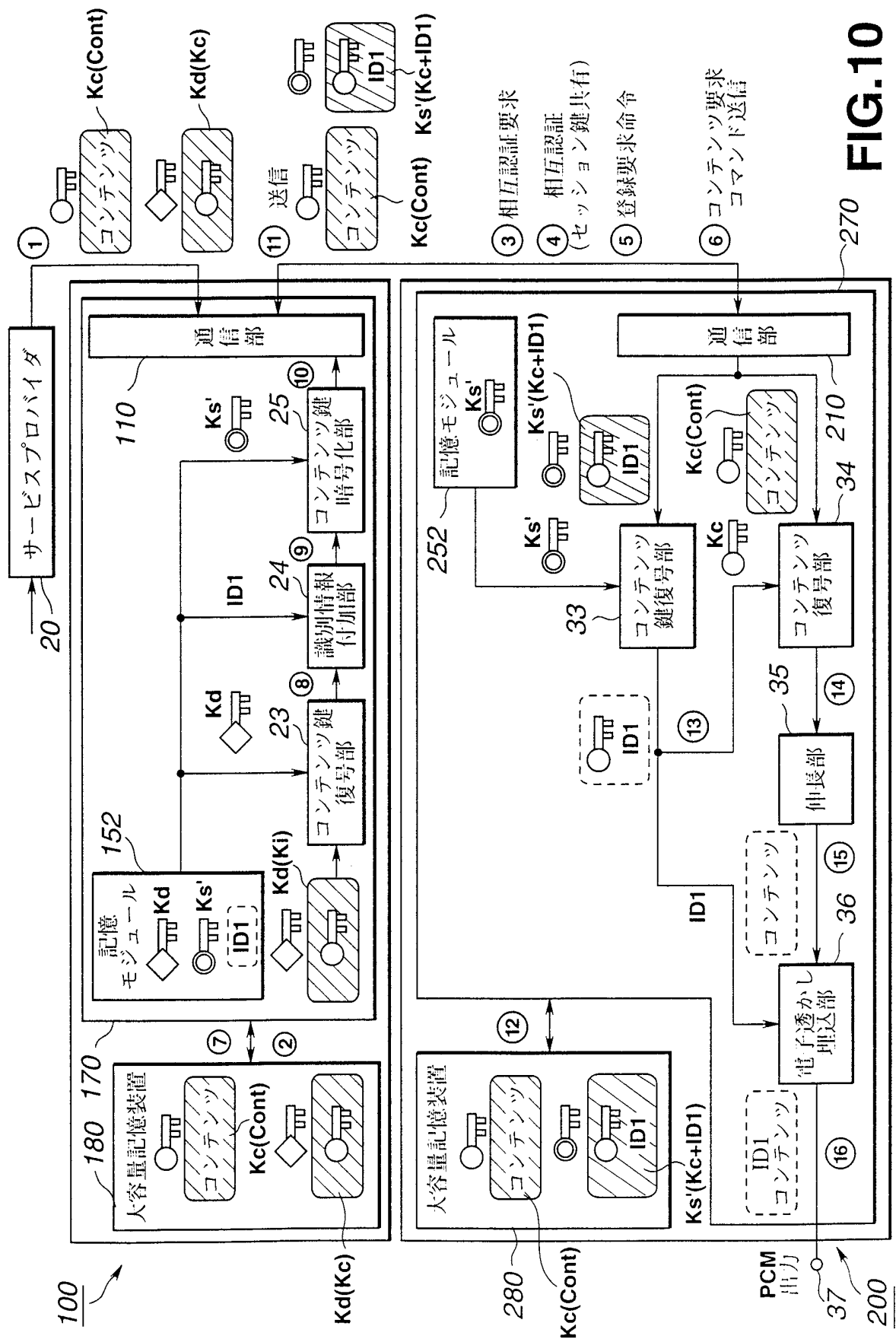


FIG. 9

10/15



11/15

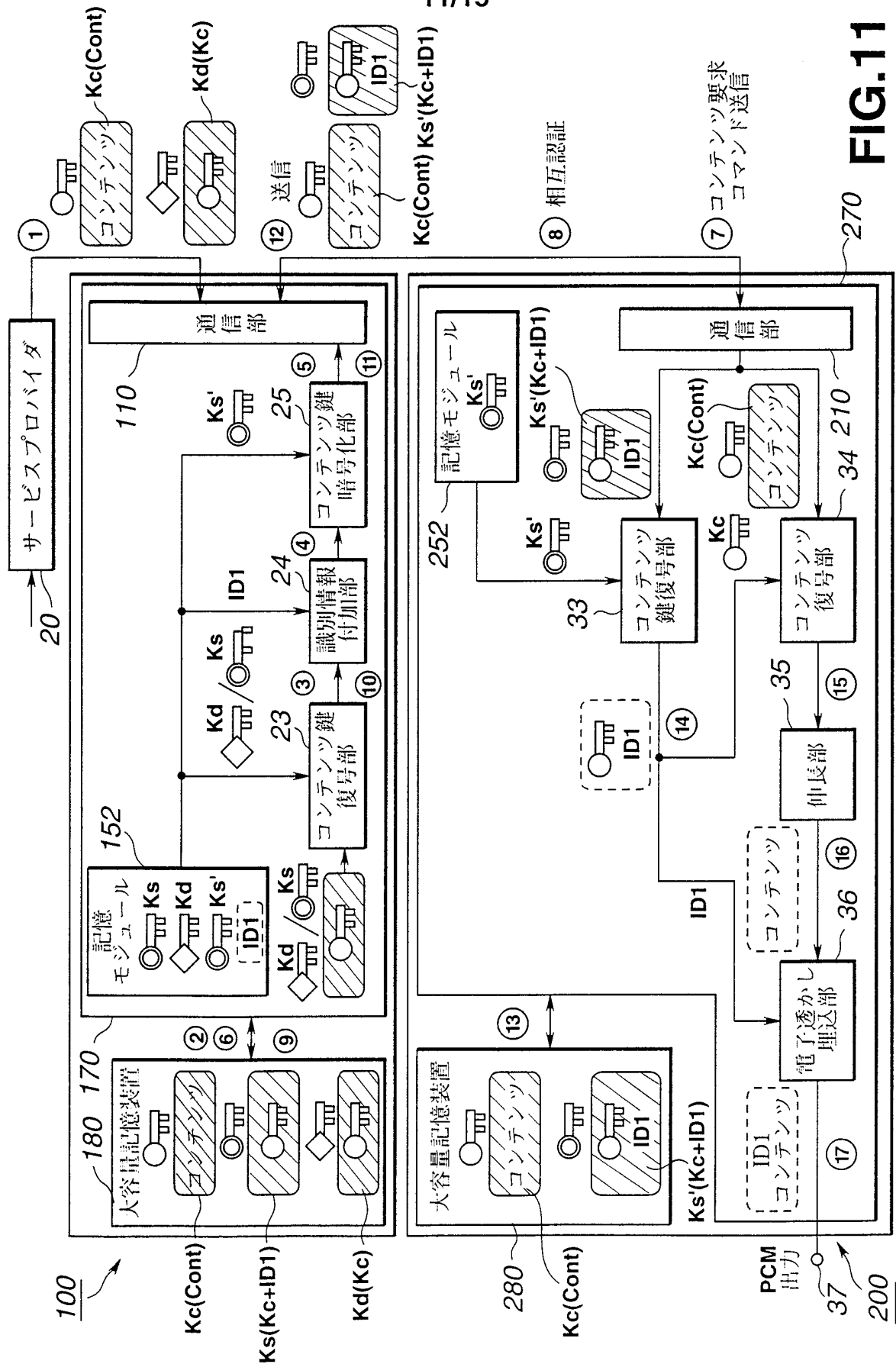
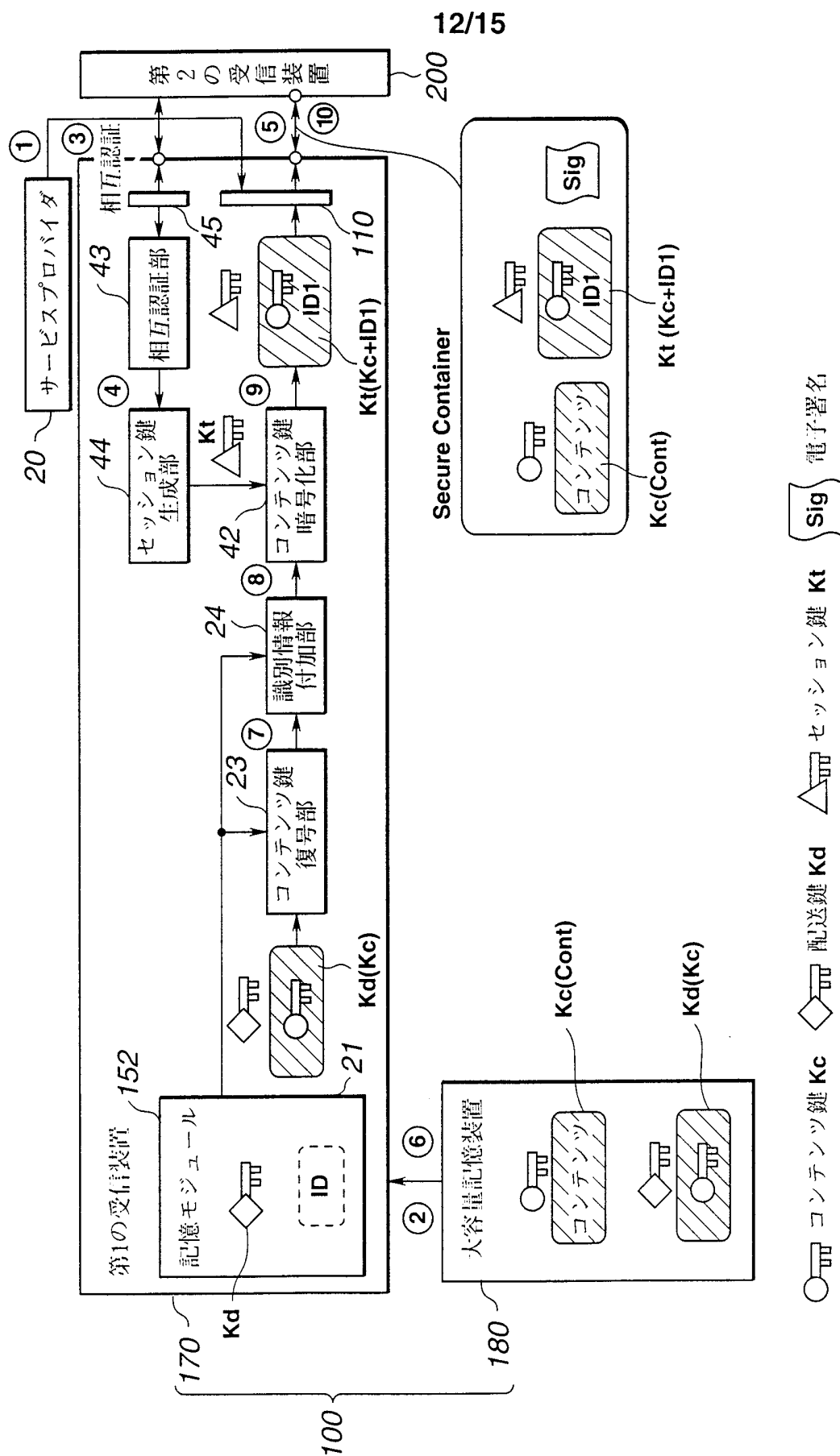


FIG.11



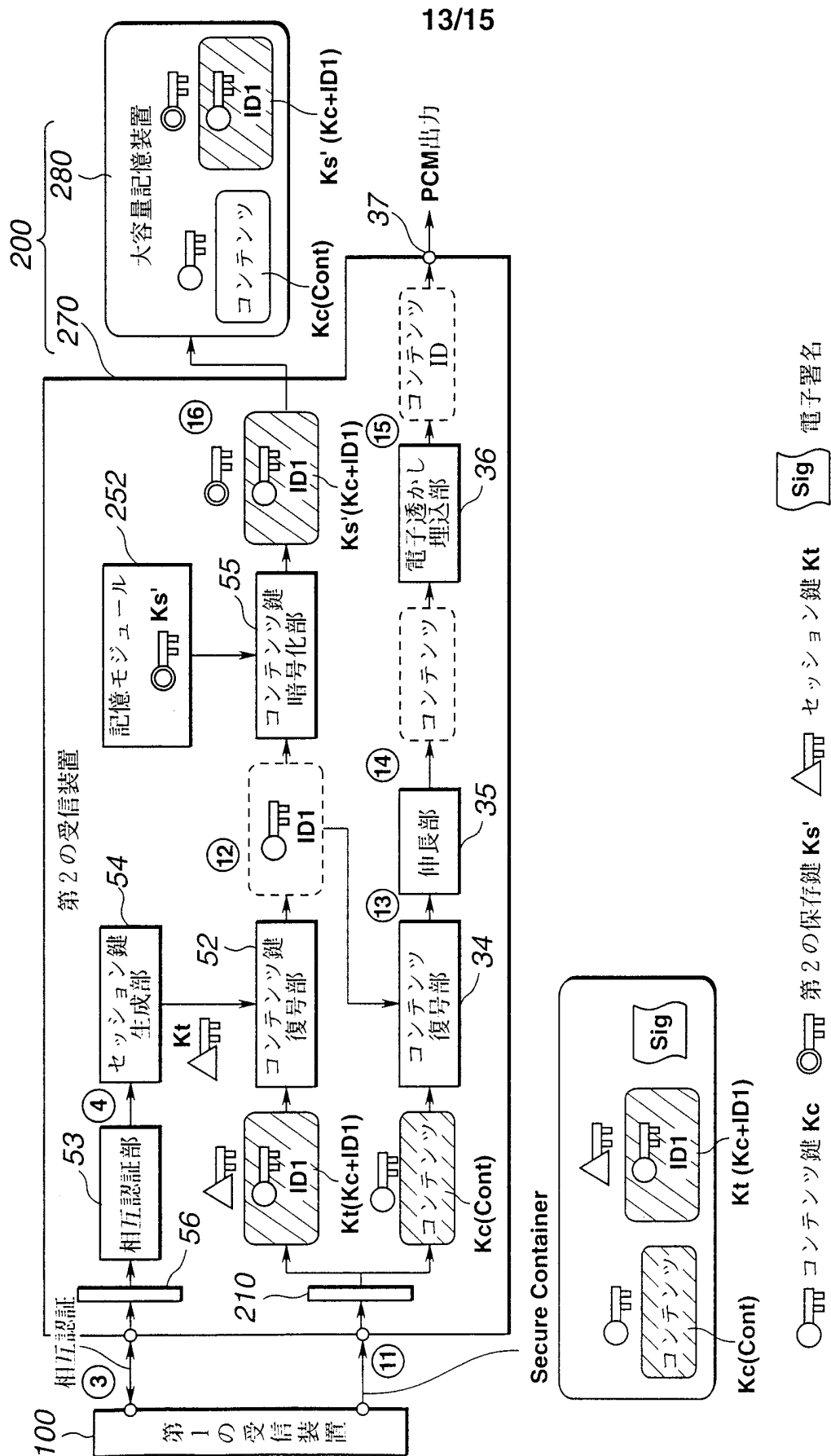


FIG. 13

14/15

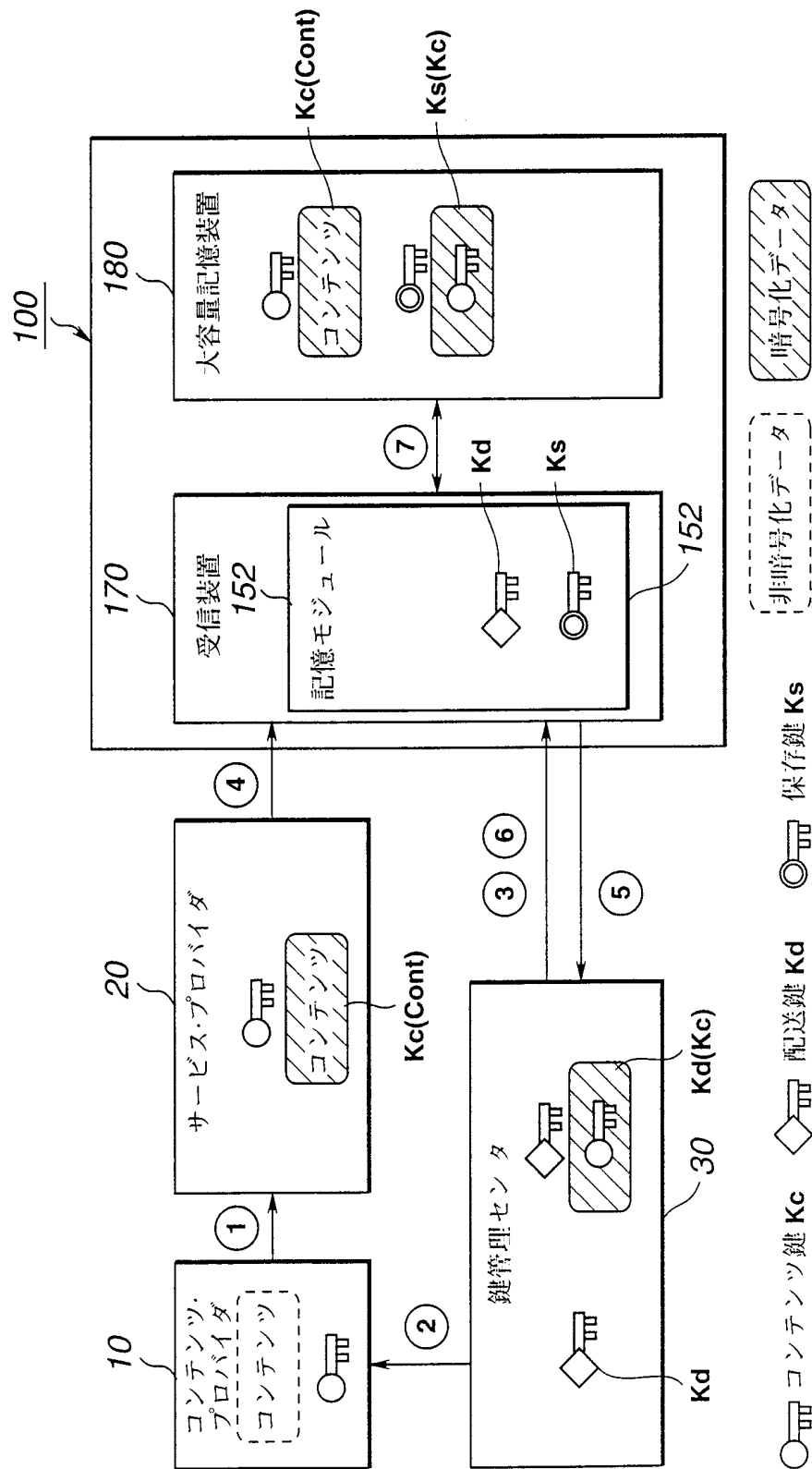


FIG.14

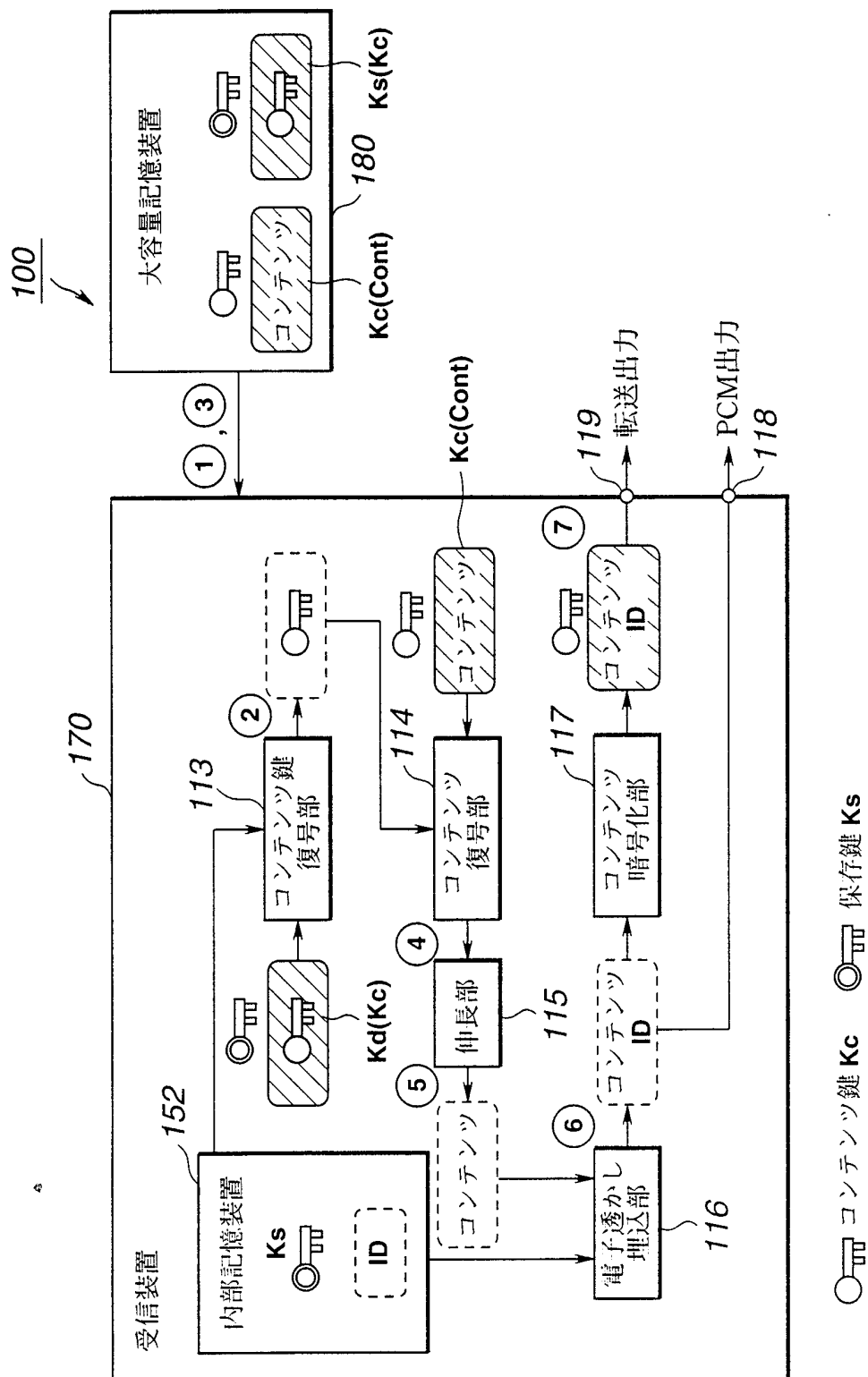


FIG. 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/04132

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁶ H04L9/32, G09C1/00, G09C5/00, G06F17/60

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)

Int.Cl⁶ H04L9/00, G09C1/00-5/00, G06F12/00-17/00, G06T1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 10-191036, A (Monolith Co., Ltd.), 21 July, 1998 (21. 07. 98)	1-3, 7-9, 24, 26-28, 32-34
Y	& WO, 98/20672, A2 & EP, 938807, A1 & AU, 5430898, A1	4-6, 29-31
Y	Harumitsu Nakajima, Kazuya Miyazaki, Tetsuo Nakakawaji, "Secure digital contents haifu system-DIGITEX-no kaihatsu", Denshi Jouhou Tsuushin Gakkai 1998 Nen Sougou Taikai Kouen Rombunshuu, SD-3-7, (06. 03. 98)	4-6, 29-31
Y	Shin'ichi Ikeno, Kenji Oyama, "Gendai angou riron", 3rd edition, IEICE, (20. 05. 89), p.268	6, 31
A	JP, 10-133955, A (Matsushita Electric Industrial Co., Ltd.), 22 May, 1998 (22. 05. 98) & EP, 840194, A2 & AU, 2839497, A1 & CN, 1182916, A	1-45

☐ 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 document 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 another 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
18 October, 1999 (18. 10. 99)

Date of mailing of the international search report
2 November, 1999 (02. 11. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/J P 99/04132

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁶

H 04 L 9/32, G 09 C 1/00, G 09 C 5/00, G 06 F 17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁶

H 04 L 9/00, G 09 C 1/00-5/00, G 06 F 12/00-17/00, G 06 T 1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 10-191036, A (株式会社モノリス) 21. 7月. 1998 (21. 07. 98)	1-3, 7-9, 24, 26-28, 32-34
Y	& WO, 98/20672, A2 & EP, 938807, A1 & AU, 5430898, A1	4-6, 29-31
Y	中嶋春光, 宮崎一哉, 中川路哲男, “セキュアデジタルコンテンツ 配布システム-DIGITEX-の開発” 電子情報通信学会1998年総 合大会講演論文集, SD-3-7, (06. 03. 98)	4-6, 29-31
Y	池野信一, 小山謙二「現代暗号理論」第3版, 電子情報通信学会, (20. 05. 89), p. 268	6, 31

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

18. 10. 99

国際調査報告の発送日

02.11.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政



5W

9570

電話番号 03-3581-1101 内線 3576

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 10-133955, A (松下電器産業株式会社) , 22. 5月. 1998 (22. 05. 98) & EP, 840194, A2 & AU, 2839497, A1 & CN, 1182916, A	1-45