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

特許第4989293号
(P4989293)

(45)発行日　平成24年8月1日(2012.8.1)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	21/22	116
G09C 5/00	(2006.01)	G09C	5/00	
G09C 1/00	(2006.01)	G09C	1/00	640D
H04N 7/16	(2011.01)	H04N	7/16	Z

請求項の数 18　(全 52 頁)

(21)出願番号　特願2007-118387 (P2007-118387)
(22)出願日　平成19年4月27日 (2007.4.27)
(65)公開番号　特開2007-317175 (P2007-317175A)
(43)公開日　平成19年12月6日 (2007.12.6)
審査請求日　平成22年3月4日 (2010.3.4)
(31)優先権主張番号　特願2006-123619 (P2006-123619)
(32)優先日　平成18年4月27日 (2006.4.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(73)特許権者　504137912
国立大学法人　東京大学
東京都文京区本郷七丁目３番１号
(74)代理人　100090446
弁理士　中島　司朗
(74)代理人　100072442
弁理士　松村　修治
(74)代理人　100125597
弁理士　小林　国人
(72)発明者　野仲　真佐男
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】コンテンツ配信システム

(57)【特許請求の範囲】
【請求項１】
コンテンツを受信装置へ送信する送信装置であって、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段と
を備えることを特徴とする送信装置。
【請求項２】
前記コンテンツは、動画及び／又は音声から構成されるマルチメディアデータであり、
前記埋込手段は、前記追跡情報に対して、電子透かし技術を用いて、前記ハッシュ値及び前記証拠情報を埋め込む
ことを特徴とする請求項１に記載の送信装置。

【請求項３】
前記送信装置は、さらに、
前記追跡情報を秘匿通信処理するために用いる複数個のコンテンツ鍵データを生成するコンテンツ鍵生成手段を備え、
前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データのそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項４】
前記送信装置は、さらに、
前記追跡情報を暗号処理するために用いる複数個のコンテンツ鍵データと、前記複数個のコンテンツ鍵データのそれぞれを識別する複数個のコンテンツ鍵データ識別子とを生成するコンテンツ鍵生成手段を備え、
前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データ識別子のそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項５】
前記送信装置は、さらに、
当該送信装置に対応付けられている公開鍵データと秘密鍵データとを保持しており、
前記複数個の候補情報のそれぞれは、前記公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項６】
前記送信装置は、さらに、
前記追跡情報を秘匿通信処理するために用いる複数個の乱数データを生成する乱数生成手段を備え、
前記複数個の候補情報のそれぞれは、前記乱数データのそれぞれに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項７】
前記送信装置は、さらに、
当該送信装置に対応付けられている複数個の公開鍵データ及び秘密鍵データを保持しており、
前記複数個の候補情報のそれぞれは、前記複数個の公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項８】
前記送信装置は、さらに、
当該送信装置に対応付けられている複数個の公開鍵データ、秘密鍵データ、及び公開鍵識別子を保持しており、
前記複数個の候補情報のそれぞれは、前記複数個の公開鍵識別子に基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項９】
前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の公開鍵データに基づき生成される
ことを特徴とする請求項２に記載の送信装置。
【請求項１０】
前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の秘密鍵データに基づき生成された電子署名データを含む
ことを特徴とする請求項２に記載の送信装置。
【請求項１１】
送信装置からコンテンツを受信する受信装置であって、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、

選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段と
を備えることを特徴とする受信装置。
【請求項１２】
送信装置から受信装置へコンテンツを転送するコンテンツ配信システムであって、
前記送信装置は、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段とを備え、
前記受信装置は、
前記複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、
選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段とを備える
ことを特徴とするコンテンツ配信システム。
【請求項１３】
複製手段、候補情報取得手段、証拠情報取得手段、ハッシュ生成手段、埋込手段および送信手段を備え、コンテンツを受信装置へ送信する送信装置で用いられるコンテンツ送信方法であって、
前記送信装置の前記複製手段が、１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製ステップと、
前記送信装置の前記候補情報取得手段が、複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得ステップと、
前記送信装置の前記証拠情報取得手段が、前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得ステップと、
前記送信装置の前記ハッシュ生成手段が、前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成ステップと、
前記送信装置の前記埋込手段が、各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込ステップと、
前記送信装置の前記送信手段が、ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信ステップと
を含むことを特徴とするコンテンツ送信方法。
【請求項１４】
複製手段、候補情報取得手段、証拠情報取得手段、ハッシュ生成手段、埋込手段および送信手段を備え、コンテンツを受信装置へ送信する送信装置で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記コンピュータプログラムは、

前記送信装置の前記複製手段に、１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製ステップを実行させ、
前記送信装置の前記候補情報取得手段に、複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得ステップを実行させ、
前記送信装置の前記証拠情報取得手段に、前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得ステップを実行させ、
前記送信装置の前記ハッシュ生成手段に、前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成ステップを実行させ、
前記送信装置の前記埋込手段に、各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込ステップを実行させ、
前記送信装置の前記送信手段に、ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信ステップを実行させる
ことを特徴とする記録媒体。

【請求項１５】
コンテンツを受信装置へ送信する送信装置で用いられる集積回路であって、
１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、
複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、
前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報取得手段と、
前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、
各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、
ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段と
を備えることを特徴とする集積回路。

【請求項１６】
選択手段、生成手段、送信手段および取得手段を備え、送信装置からコンテンツを受信する受信装置で用いられるコンテンツ受信方法であって、
前記受信装置の前記選択手段が、１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択ステップと、
前記受信装置の前記生成手段が、選択した前記候補情報に基づき、証拠情報を生成する生成ステップと、
前記受信装置の前記送信手段が、前記証拠情報を前記送信装置へ送信する送信ステップと、
前記受信装置の前記取得手段が、前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得ステップと
を含むことを特徴とするコンテンツ受信方法。

【請求項１７】
選択手段、生成手段、送信手段および取得手段を備え、送信装置からコンテンツを受信する受信装置で用いられるコンピュータプログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記コンピュータプログラムは、
前記受信装置の前記選択手段に、１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択ステップを実行させ、

前記受信装置の前記生成手段に、選択した前記候補情報に基づき、証拠情報を生成する生成ステップを実行させ、
前記受信装置の前記送信手段に、前記証拠情報を前記送信装置へ送信する送信ステップを実行させ、
前記受信装置の前記取得手段に、前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得ステップを実行させる
ことを特徴とする記録媒体。
【請求項１８】
送信装置からコンテンツを受信する受信装置で用いられる集積回路であって、
１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、
選択した前記候補情報に基づき、証拠情報を生成する生成手段と、
前記証拠情報を前記送信装置へ送信する送信手段と、
前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段と
を備えることを特徴とする集積回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、映画や音楽などの著作物であるデジタルデータ（以下、「コンテンツ」という。）を送受信する技術に関し、特に、コンテンツを不正にコピーする著作権侵害行為を防止し、更に、不正にコピーされたコンテンツが流出した場合には、流出したコンテンツから、不正を行った装置を特定する技術に関する。
【背景技術】
【０００２】
コンテンツの個人利用が盛んになるにつれて、コンテンツが不正にコピーされ生成された、所謂、「海賊版コンテンツ」が出回るようになってきた。
特許文献１は、サーバからクライアントへコンテンツを配信するモデルにおいて、不正コピーされたコンテンツから、不正コピーを行ったクライアントを特定する技術を開示している。
【０００３】
具体的には、サーバがコンテンツ内のあるシーンを複数個にコピーし、それぞれのシーンに異なる電子透かし（ウォーターマーク）を埋め込む。続いて、サーバは、異なる電子透かしを埋め込んだシーンのそれぞれを、複数個の異なる暗号鍵で暗号化した後、コンテンツをクライアントに配信する。クライアントは、複数の鍵の何れかを保持しており、指定された鍵を用いて、指定された部分を復号することにより、コンテンツを再生することができる。
【０００４】
そして、不正コピーにより作成された海賊版コンテンツが出回った場合には、海賊版コンテンツに埋め込まれている電子透かしを抽出することにより、不正コピーを行ったクライアントを特定することが可能となる。
【特許文献１】米国特許第６２８５７７４号
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、本来であればコンテンツホルダから信用されるべきサーバ側が不正を行うことも想定され、サーバ側の不正を防止したいというコンテンツホルダの要求がある。
また近年では、家庭内において、ユーザが保持する複数個の端末装置をネットワーク接続し、端末装置間においてコンテンツを送受信することが行われてきている。この様な場合、各端末装置は、サーバ側（送信側）にも、クライアント側（受信側）にもなり得るため、コンテンツの受信側だけでなく、送信側の不正を防止する仕組みも必要となってきた

。
【０００６】
ここで、上記の特許文献１に記載の技術では、コンテンツの受信側の不正を防止することは可能であるが、送信側の不正を防止することはできないという問題が存在する。
本発明は、上記の要求、及び上記の問題点に鑑みてなされたものであって、コンテンツを送信する送信装置が、コンテンツを受信する受信装置に成りすまして不正を行うことを防止するコンテンツ配信システムを提供することを目的とする。
【０００７】
ここで、「送信装置が受信装置に成りすまして不正を行う」とは、どのようなことを言うのか説明する。
コンテンツホルダからコンテンツを取得した送信装置は、コンテンツを正規の流通経路で流通させることを期待されており、コンテンツを不正コピーすることにより海賊版コンテンツを作成し、流出させた場合、それは、コンテンツホルダに容易に不正を特定されることから、通常、送信装置がそのような不正を行うことは考えにくい。しかしながら、送信装置は、後の検証により、不正コピーを作成したのが受信装置であると判断される情報を埋め込んだ海賊版コンテンツを流出させることが可能である。
【０００８】
また、ユーザが保持する複数個の端末装置間においてコンテンツを送受信する場合には、送信側の端末装置が、後の検証により、受信側の端末装置が不正を行ったと判断される情報を埋め込んだ海賊版コンテンツを作成することが可能である。なお、この場合は特に、コンテンツがエンドユーザの端末装置間で送受信されるため、不正が行われる可能性が高くなる。
【０００９】
上記のような場合を「送信装置が受信装置に成りすまして不正を行う」と言う。
【課題を解決するための手段】
【００１０】
上記の目的を達成するために、本発明は、コンテンツを受信装置へ送信する送信装置であって、１個のコンテンツからその全部又は一部を抽出して追跡情報を生成し、生成した追跡情報を複数個複製する複製手段と、複数個の追跡情報のそれぞれに対応した複数個の候補情報を取得する候補情報取得手段と、前記複数個の候補情報のうちから受信装置により選択された１個の候補情報に依存して生成された証拠情報を取得する証拠情報手段と、前記複数個の候補情報のそれぞれに基づいて、複数個のハッシュ値を生成するハッシュ生成手段と、各追跡情報に、当該追跡情報に対応する候補情報に基づいて生成された前記ハッシュ値を埋め込み、各追跡情報に、前記証拠情報を埋め込む埋込手段と、ハッシュ値と証拠情報とが埋め込まれた各追跡情報を送信する送信手段とを備えることを特徴とする。
【００１１】
また、本発明は、送信装置からコンテンツを受信する受信装置であって、１個のコンテンツの全部又は一部が複製されて生成された複数個の追跡情報のそれぞれに対応する複数個の候補情報のうちから、１個の候補情報を選択する選択手段と、選択した前記候補情報に基づき、証拠情報を生成する生成手段と、前記証拠情報を前記送信装置へ送信する送信手段と、前記送信装置から、選択した前記候補情報に対応する追跡情報を取得する取得手段とを備えることを特徴とする。
【発明の効果】
【００１２】
上記の構成によると、送信装置は、受信装置から受信した証拠情報からは、受信装置により選択された候補情報が何れであるのかを特定することは出来ない。従って、送信装置は、受信装置が何れの追跡情報を取得するのかを知ることが出来ない。
そのため、送信装置は、受信装置が取得した１個のコンテンツを特定し、受信装置が取得した１個のコンテンツに含まれる電子透かしと同一の電子透かしを埋め込んだコンテンツのみを不正にコピーして、流出させ、その他の電子透かしを埋め込んだコンテンツは流

出させないことは非常に困難である。そのため、送信装置は、受信装置に成りすまして、海賊版コンテンツを流出させることは現実的には不可能となる。

【００１３】

ここで、前記コンテンツは、動画及び／又は音声から構成されるマルチメディアデータであり、前記埋込手段は、前記追跡情報に対して、電子透かし技術を用いて、前記ハッシュ値及び前記証拠情報を埋め込むように構成してもよい。

この構成によると、送信装置は、埋め込んだ証拠情報をユーザに知覚されることなく、コンテンツを受信装置へ送信することができる。

【００１４】

ここで、前記送信装置は、さらに、前記追跡情報を秘匿通信処理するために用いる複数個のコンテンツ鍵データを生成するコンテンツ鍵生成手段を備え、前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データのそれぞれに基づき生成されるように構成してもよい。

この構成によると、送信装置は、前記候補情報を前記受信装置へ送信することにより、前記受信装置との間で、前記秘匿通信処理に用いるコンテンツ鍵データを共有することができる。そして、送信装置は、前記受信装置が何れのコンテンツ鍵データに基づき生成された候補情報を選択したのかを知ることができない。

【００１５】

ここで、前記送信装置は、さらに、前記追跡情報を暗号処理するために用いる複数個のコンテンツ鍵データと、前記複数個のコンテンツ鍵データのそれぞれ識別する複数個のコンテンツ鍵データ識別子とを生成するコンテンツ鍵生成手段を備え、前記複数個の候補情報のそれぞれは、前記コンテンツ鍵データ識別子のそれぞれに基づき生成されるように構成してもよい。

【００１６】

この構成によると、コンテンツ鍵データそのものを候補情報とする場合と比較して、送信装置と受信装置とにおける候補情報送受信処理の安全性が高まる。そして、送信装置は、前記受信装置が何れのコンテンツ鍵データ識別子に基づき生成された候補情報を選択したのかを知ることができない。

ここで、前記送信装置は、さらに、当該送信装置に対応付けられている公開鍵データと秘密鍵データとを保持しており、前記複数個の候補情報のそれぞれは、前記公開鍵データに基づき生成されるように構成してもよい。

【００１７】

この構成によると、候補情報は、公開鍵データに基づき生成されるので、送信装置と受信装置とにおける候補情報送受信処理の安全性が高まる。

ここで、前記送信装置は、さらに、前記追跡情報を秘匿通信処理するために用いる複数個の乱数データを生成する乱数生成手段を備え、前記複数個の候補情報のそれぞれは、前記乱数データのそれぞれに基づき生成されるように構成してもよい。

【００１８】

この構成によると、送信装置は、予め公開鍵データを保持したり、外部から公開鍵データを取得したりすることなく、候補情報を生成することができる。また、送信装置は、前記受信装置が何れの乱数データに基づき生成された候補情報を選択したのか知ることができない。

ここで、前記送信装置は、さらに、当該送信装置に対応付けられている複数個の公開鍵データ及び秘密鍵データを保持しており、前記複数個の候補情報のそれぞれは、前記複数個の公開鍵データに基づき生成されるように構成してもよい。

【００１９】

この構成によると、候補情報は、公開鍵データに基づき生成されるので、送信装置と受信装置とにおける候補情報送受信処理の安全性が高まる。そして、送信装置は、前記受信装置が何れの公開鍵データに基づき生成された候補情報を選択したのか知ることができない。

ここで、前記送信装置は、さらに、当該送信装置に対応付けられている複数個の公開鍵データ、秘密鍵データ、及び公開鍵識別子を保持しており、前記複数個の候補情報のそれぞれは、前記複数個の公開鍵識別子に基づき生成されるように構成してもよい。

【００２０】

この構成によると、候補情報が公開鍵データに基づき生成される場合と比較し、送信装置と受信装置とにおける候補情報送受信処理の安全性が高まる。また、送信装置は、前記受信装置が何れの公開鍵識別子に基づき生成された候補情報を選択したのか知ることができない。

ここで、前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の公開鍵データに基づき生成されるように構成してもよい。

【００２１】

この構成によると、送信装置は、受信装置の秘密鍵データを知り得ないので、取得した証拠情報から、受信装置が何れの候補情報を選択したのかを知ることができない。従って、送信装置は、受信装置が取得した１個のコンテンツを特定し、受信装置が取得した１個のコンテンツに含まれる電子透かしと同一の電子透かしを埋め込んだコンテンツのみを不正にコピーして、流出させ、その他の電子透かしを埋め込んだコンテンツは流出させないことは非常に困難である。そのため、送信装置は、受信装置に成りすまして、海賊版コンテンツを流出させることは現実的には不可能となる。

【００２２】

ここで、前記証拠情報は、前記受信装置に対応付けられている公開鍵暗号の秘密鍵データに基づき生成された電子署名データを含むように構成してもよい。

この構成によると、送信装置は、電子署名データを検証することにより、受信装置が正当な証拠情報を送信してきたのか否かを判定することができる。受信装置が正当な証拠情報を送信してこない場合には、送信装置は、受信装置へのコンテンツの送受信処理を中止し、コンテンツの著作権を保護することができる。

【発明を実施するための最良の形態】

【００２３】

≪第１の実施形態≫

本発明の第１の実施形態として、コンテンツ配信システム１について、図面を参照して説明する。

＜概要＞

ここでは、コンテンツ配信システム１の概要について説明する。

【００２４】

図１は、コンテンツ配信システム１の構成を示すシステム構成図である。

同図に示すように、コンテンツ配信システム１は、送信装置１０、受信装置２０、コンテンツ流出元特定装置３０、記録媒体４０、及び放送局装置５０から構成される。ここで、送信装置１０と受信装置２０とは、ケーブル６０を介して接続されている。

放送局装置５０は、具体的には、地上デジタル放送を放送する放送局に設置された装置であって、映像データ及び音声データが多重化され、圧縮符号化されたコンテンツを、デジタル放送波に乗せて放送する。

【００２５】

送信装置１０は、具体的には、地上デジタル放送を受信するデジタルテレビ受像機であって、放送局装置５０から放送されたコンテンツを受信する。送信装置１０は、受信したコンテンツを映像データと音声データとに変換し、ディスプレイ等に出力する。

受信装置２０は、具体的には、コンテンツを録画することが可能なＤＶＤレコーダであり、ケーブル６０を介して、送信装置１０からコンテンツを受け取り、受け取ったコンテンツをＤＶＤ－ＲＡＭ等に記録する。

【００２６】

ケーブル６０は、送信装置１０と受信装置２０との間で、各種データを送受信する通信路であり、例えばイーサネット（登録商標）（Ｅｔｈｅｒｎｅｔ（登録商標））ケーブル

、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ケーブル、ＩＥＥＥ１３９４ケーブル等である。

記録媒体４０は、具体的には、ＤＶＤ－ＲＡＭであって、不正コピーにより作成された、所謂、海賊版コンテンツを格納しているものとする。

【００２７】

コンテンツ流出元特定装置３０は、システムの管理者が保有する装置であって、記録媒体４０に格納されている海賊版コンテンツから、不正を行った装置を特定する。

コンテンツ配信システム１では、送信装置１０から受信装置２０へのコンテンツ転送時に、先ず、送信装置１０は、複数個のコンテンツ鍵を生成し、生成した複数個のコンテンツ鍵を受信装置２０へ送信する。受信装置２０は、複数個のコンテンツ鍵のうち１つを選択して受け取り、残りは受け取ることが出来ないようにする。ここで、送信装置１０は、受信装置２０がどのコンテンツ鍵を選択したか知ることは出来ない。

【００２８】

その後、送信装置１０は、コンテンツを複数個に複製し、それぞれを異なるコンテンツ鍵で暗号化する。送信装置１０は、暗号化の前に、各コンテンツに対して、受信装置２０が選択したコンテンツ鍵を示す証拠情報と、そのコンテンツを暗号化するのに用いるコンテンツ鍵を示す値とを電子透かし（ウォーターマーク）として埋め込む。そして、送信装置１０は、電子透かしの埋め込まれた複数個の暗号化コンテンツを受信装置２０へ送信する。

【００２９】

受信装置２０は、複数個の暗号化コンテンツを受信すると、事前に選択したコンテンツ鍵を用いて、複数個の暗号化コンテンツの内の一つを復号する。

一方、海賊版コンテンツが流出した場合に、コンテンツ流出元特定装置３０は、海賊版コンテンツが記録されている記録媒体４０から、コンテンツデータを取得し、そのコンテンツデータに含まれる電子透かしを抽出する。コンテンツ流出元特定装置３０は、抽出した証拠情報と使用されたコンテンツ鍵を示す値とを取得し、それらを調査することにより、海賊版コンテンツの流出元が送信装置１０であるか、受信装置２０であるかを判断する。

＜構成＞

ここでは、各装置の構成について、詳細に説明する。

【００３０】

１．送信装置１０

図２は、送信装置１０の構成を示すブロック図である。同図に示すように、送信装置１０は、コンテンツ鍵生成部１０１、コンテンツ鍵識別子生成部１０２、コンテンツ鍵保持部１０３、公開鍵保持部１０４、第一送信制御部１０５、第二送信制御部１０６、証拠取得部１０７、証拠保持部１０８、第一コンテンツデータ保持部１０９、コンテンツ複製部１１０、装置識別子埋込部１１１、ハッシュ埋込部１１２、証拠埋込部１１３、装置識別子保持部１１４、転送先装置識別子取得部１１５、暗号処理部１１６、入力部１１７、送受信部１１８、及び、第三送信制御部１１９から構成される。

【００３１】

送信装置１０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどを備えるコンピュータシステムである。送信装置１０は、マイクロプロセッサが、ＲＯＭ、ＲＡＭ、又はハードディスクに記録されているコンピュータプログラムに従い動作することにより、その機能を達成する。

なお、送信装置１０を構成する各ブロックは、ハードウェアにより構成されてもよいし、またソフトウェアにより構成されてもよい。

【００３２】

以下では、送信装置１０を構成する各ブロックについて説明する。

（１）コンテンツ鍵生成部１０１

コンテンツ鍵生成部１０１は、転送先装置識別子取得部１１５からコンテンツ鍵生成要

求ＲＥＱ１が入力されると、ｎ個（ｎは予め与えられる２以上の整数）の１２８ビットのコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを生成する。コンテンツ鍵の生成方法の一例として、コンテンツ鍵生成部１０１は、乱数生成器を用いてランダムに乱数を生成する方法などがある。

【００３３】

コンテンツ鍵生成部１０１は、生成したｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを、コンテンツ鍵識別子生成部１０２へ出力する。

（２）コンテンツ鍵識別子生成部１０２

コンテンツ鍵識別子生成部１０２は、コンテンツ鍵生成部１０１からｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎが入力されると、各コンテンツ鍵を識別するコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎを生成する。ここでは具体例として、コンテンツ鍵識別子生成部１０２は、１から数字をインクリメントさせて、ｎ個のコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎを生成する。従って、ＣＫＩＤ＿１は１、ＣＫＩＤ＿２は２、…、ＣＫＩＤ＿ｎはｎとなる。

【００３４】

コンテンツ鍵識別子生成部１０２は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎと、ｎ個のコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎとをそれぞれ対応付けて、コンテンツ鍵保持部１０３へ格納する。

その後、コンテンツ鍵識別子生成部１０２は、第一送信制御部１０５へ、第一送信制御開始要求ＲＥＱ２を出力する。

【００３５】

（３）コンテンツ鍵保持部１０３

コンテンツ鍵保持部１０３は、図３に示すように、コンテンツ鍵識別子とコンテンツ鍵とを対応付けた、ｎ個の組｛（ＣＫＩＤ＿１、ＣＫ＿１）、（ＣＫＩＤ＿２、ＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＣＫ＿ｎ）｝を保持している。

（４）公開鍵保持部１０４

公開鍵保持部１０４は、図４に示すように、送信装置公開鍵情報ＰＫ１と送信装置秘密鍵情報ＳＫ１とを保持している。

【００３６】

送信装置公開鍵情報ＰＫ１は、公開鍵暗号アルゴリズムＲＳＡ（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ）の公開鍵である第一公開鍵ｎ１及びｅ１から構成され、送信装置秘密鍵情報ＳＫ１は、ＲＳＡの秘密鍵である第一秘密鍵ｄ１により構成される。これらの鍵情報は、システム管理者によって計算され、送信装置製造時に公開鍵保持部１０４に格納されたものとする。以下では、これらの鍵情報の生成方法について説明する。

【００３７】

（ａ）第一公開鍵ｎ１及びｅ１の生成方法

まず、システム管理者は、５１２ビットの二つの素数ｐ１、ｑ１をランダムに生成する。そして、ｐ１とｑ１を乗算した値ｐ１×ｑ１を計算し、その１０２４ビットの値をｎ１とする。次に、システム管理者は、Ｌ１＝ＬＣＭ（ｐ１－１、ｑ１－１）を計算する。ＬＣＭ（ｘ、ｙ）は、ｘとｙの最小公倍数とする。その後、Ｌ１と互いに素となる値ｅ１を生成する。ｅ１は例えば１１である。このようにして生成されたｎ１及びｅ１を、第一公開鍵とする。

【００３８】

（ｂ）第一秘密鍵ｄ１の生成方法

システム管理者は、ｅ１×ｄ１＝１（ｍｏｄ　Ｌ１）を満たすｄ１を計算する。ここで、（ｍｏｄ　Ｌ１）は、Ｌ１で割った余りを表している。ｄ１は、拡張ユークリッド互除法を利用することにより計算することが出来る。拡張ユークリッド互除法については公知であるため、説明は省略する。このようにして生成されたｄ１を、第一秘密鍵とする。

【００３９】

（５）第一送信制御部１０５

第一送信制御部１０５は、コンテンツ鍵識別子生成部１０２から第一送信制御開始要求ＲＥＱ２が入力されると、先ず、コンテンツ鍵保持部１０３からｎ組のコンテンツ鍵識別子とコンテンツ鍵と｛（ＣＫＩＤ＿１、ＣＫ＿１）、（ＣＫＩＤ＿２、ＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＣＫ＿ｎ）｝を取得する。

【００４０】

次に、第一送信制御部１０５は、暗号処理部１１６へ、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎと、ＲＳＡ暗号化処理要求ＲＳＡＥとを出力する。そして、第一送信制御部１０５は、暗号処理部１１６からｎ個の暗号化されたデータである第一暗号化コンテンツ鍵を受け取る。以下では、コンテンツ鍵ＣＫ＿ｉ（ｉ＝１、２、…、ｎ）に対応するＲＳＡ暗号文を、ＥＣＫ＿ｉとする。

【００４１】

続いて、第一送信制御部１０５は、コンテンツ鍵識別子と第一暗号化コンテンツ鍵とを対応付け、送受信部１１８を介して、図８に示すように、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝を、受信装置２０へ送信する。

（６）第二送信制御部１０６

第二送信制御部１０６は、送受信部１１８を介して、受信装置２０から１個の第二暗号化コンテンツ鍵Ｅ２ＣＫを受信すると、暗号処理部１１１６へ第二暗号化コンテンツ鍵Ｅ２ＣＫとＲＳＡ復号処理要求ＲＳＡＤを出力する。そして、第二送信制御部１０６は、暗号処理部１１６から、第二暗号化コンテンツ鍵Ｅ２ＣＫが復号されたデータである第三暗号化コンテンツ鍵Ｅ３ＣＫを受け取る。

【００４２】

次に、第二送信制御部１０６は、第三暗号化コンテンツ鍵Ｅ３ＣＫを、証拠取得部１０７へ出力すると共に、送受信部１１８を介して、受信装置２０へ送信する。

続いて、第二送信制御部１０６は、第三送信制御部１１９に対して、コンテンツ転送要求ＲＥＱ３を出力する。

（７）証拠取得部１０７

証拠取得部１０７は、第二送信制御部１０６から第三暗号化コンテンツ鍵Ｅ３ＣＫを受け取ると、受け取った第三暗号化コンテンツ鍵Ｅ３ＣＫを、証拠情報ＥＶとして、証拠保持部１０８へ格納する。

【００４３】

（８）証拠保持部１０８

証拠保持部１０８は、図５に示すように、証拠情報ＥＶを保持している。証拠情報ＥＶは、先に述べたように、第三暗号化コンテンツ鍵Ｅ３ＣＫと同一のデータである。

（９）第一コンテンツデータ保持部１０９

第一コンテンツデータ保持部１０９は、図６に示すように、第一コンテンツデータＣＮＴ１を保持している。第一コンテンツデータＣＮＴ１は、送信装置１０で利用可能な形式のコンテンツデータであるとする。

【００４４】

（１０）コンテンツ複製部１１０

コンテンツ複製部１１０は、第三送信制御部１１９から第一コンテンツデータＣＮＴ１が入力されると、第一コンテンツデータＣＮＴ１を複製することにより、第一コンテンツデータＣＮＴ１と同一内容のデータであるｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを生成する。コンテンツ複製部１１０は、生成したｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する。

【００４５】

（１１）装置識別子埋込部１１１

装置識別子埋込部１１１は、第三送信制御部１１９から、ｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎが入力されると、以下の手順で電子透か

しの埋め込みを行う。
先ず、装置識別子埋込部１１１は、装置識別子保持部１１４から転送元装置識別子ＩＤ＿１、及び転送先装置識別子ＩＤ＿２を取得する。
【００４６】
転送元装置識別子ＩＤ＿１は、コンテンツデータの転送元である送信装置１０を識別する情報であり、転送先装置識別子ＩＤ＿２は、コンテンツデータの転送先となる受信装置２０を識別する情報である。ここで、転送元装置識別子ＩＤ＿１、及び転送先装置識別子ＩＤ＿２は、それぞれ、送信装置１０、及び受信装置２０の製造時に与えられた情報であってもよい。
【００４７】
次に、装置識別子埋込部１１１は、ｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎのそれぞれに対して、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＩＤ＿２とを、電子透かし（ウォーターマーク）として埋め込み、ｎ個の装置識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎを生成する。
【００４８】
その後、装置識別子埋込部１１１は、生成したｎ個の装置識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する。
ここで、電子透かしとは、静止画や動画、音声データ等に対して、人間が知覚出来ない程度に透かし情報を埋め込む技術であり、加工や改変によって透かし情報が消えないという特徴を持つ。なお、電子透かしを埋め込む技術は、既に公知であるため、説明は省略する。
【００４９】
（１２）ハッシュ埋込部１１２
ハッシュ埋込部１１２は、第三送信制御部１１９から、転送元装置識別子ＩＤ＿１及び転送先装置識別子ＩＤ＿２が埋め込まれたｎ個の装置識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎが入力されると、以下の手順で電子透かしの埋め込みを行う。
【００５０】
先ず、ハッシュ埋込部１１２は、コンテンツ鍵保持部１０３からｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを取得する。
次に、ハッシュ埋込部１１２は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎと、ハッシュ値計算要求ＨＡＳＨとを暗号処理部１１６へ出力する。その後、ハッシュ埋込部１１２は、暗号処理部１１６から、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのそれぞれに対するハッシュ値であるコンテンツ鍵ハッシュＨＣＫ＿１、ＨＣＫ＿２、…、ＨＣＫ＿ｎを取得する。
【００５１】
そして、ハッシュ埋込部１１２は、ｎ個の装置識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎのそれぞれに、異なるｎ個のコンテンツ鍵ハッシュＨＣＫ＿１、ＨＣＫ＿２、…、ＨＣＫ＿ｎを、電子透かしとして埋め込み、ｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎを生成する。
【００５２】
具体的には、ハッシュ埋込部１１２は、ＤＣＮＴ１＿１に対して、ＨＣＫ＿１を埋め込みＨＣＮＴ１＿１を生成し、ＤＣＮＴ１＿２に対して、ＨＣＫ＿２を埋め込みＨＣＮＴ１＿２を生成し、…、ＤＣＮＴ１＿ｎに対して、ＨＣＫ＿ｎを埋め込み、ＨＣＮＴ１＿ｎを生成する。
その後、ハッシュ埋込部１１２は、生成したｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する

。
【００５３】
（１３）証拠埋込部１１３
証拠埋込部１１３は、第三送信制御部１１９から、ｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎが入力されると、以下の手順で電子透かしの埋め込みを行う。
先ず、証拠埋込部１１３は、証拠保持部１０８から証拠情報ＥＶを取得する。そして、ｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎのそれぞれに、証拠情報ＥＶを電子透かしとして埋め込み、ｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎを生成する。
【００５４】
その後、証拠埋込部１１３は、生成したｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する。
（１４）装置識別子保持部１１４
装置識別子保持部１１４は、図７に示すように、転送元装置識別子ＩＤ＿１と転送先装置識別子ＩＤ＿２とを保持している。
【００５５】
先に述べたように、転送元装置識別子ＩＤ＿１は、送信装置１０を特定する識別子であり、送信装置１０の製造時に予め与えられた不変の値である。転送先装置識別子ＩＤ＿２は、コンテンツデータの転送先となる端末装置を特定する識別子であり、コンテンツデータを転送する端末装置が変わる毎に変更される値である。しかしながら、本実施形態では、コンテンツデータの転送先は受信装置２０のみを想定しているので、転送先装置識別子ＩＤ＿２も、ＩＤ＿１と同様に不変の値となる。
【００５６】
（１５）転送先装置識別子取得部１１５
転送先装置識別子取得部１１５は、入力部１１７から転送先装置識別子要求情報が入力された場合、送受信部１１８を介して、転送先装置識別子取得依頼情報ＲＥＱ５を受信装置２０へ送信する。そして、転送先装置識別子取得部１１５は、送受信部１１８を介して、装置識別子ＩＤ＿２を受信すると、受信したＩＤ＿２を、転送先装置識別子として、装置識別子保持部１１４へ格納する。
【００５７】
続いて、転送先装置識別子取得部１１５は、コンテンツ鍵生成部１０１に対して、コンテンツ鍵生成要求ＲＥＱ１を出力する。
（１６）暗号処理部１１６
暗号処理部１１６は、以下の暗号処理を行う。
（ａ）第一送信制御部１０５からＲＳＡ暗号化処理要求ＲＳＡＥが入力された場合
暗号処理部１１６は、以下の手順でｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを暗号化し、暗号文を生成する。
【００５８】
先ず、暗号処理部１１６は、公開鍵保持部１０４から、送信装置公開鍵情報ＰＫ１に含まれる第一公開鍵ｎ１及びｅ１を取得する。
次に、暗号処理部１１６は、第一公開鍵ｎ１及びｅ１を用いて、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…ＣＫ＿ｎのそれぞれに対してＲＳＡ暗号化処理を行う。
ＲＳＡ暗号化処理は、具体的には、元のメッセージＭに対して、Ｍ＾ｅ１（ｍｏｄ　ｎ１）を計算することにより行われる。“＾”は、べき乗を表しており、即ち、ｘ＾ｙは、ｘをｙ乗した値である。ここで、コンテンツ鍵ＣＫ＿ｉを元のメッセージとした場合、その暗号文は、ＣＫ＿ｉ＾ｅ１（ｍｏｄ　ｎ１）となる。以下では、ＣＫ＿ｉ＾ｅ１（ｍｏｄ　ｎ１）を、ＥＣＫ＿ｉと表す。
【００５９】
暗号処理部１１６は、ｎ個のコンテンツ鍵に対応する暗号文ＥＣＫ＿１、ＥＣＫ＿２、

…、ＥＣＫ＿ｎを、第一送信制御部１０５へ出力する。
（ｂ）第二送信制御部１０６からＲＳＡ復号処理要求ＲＳＡＤが入力された場合
暗号処理部１１６は、以下の手順で第二暗号化コンテンツ鍵Ｅ２ＣＫを復号し、復号文を生成する。
【００６０】
先ず、暗号処理部１１６は、公開鍵保持部１０４から、送信装置公開鍵情報ＰＫ１に含まれる第一公開鍵ｎ１と、送信装置秘密鍵情報ＳＫ１に含まれる第一秘密鍵ｄ１とを取得する。
次に、暗号処理部１１６は、第一公開鍵ｎ１と、第一秘密鍵ｄ１とを用いて、第二暗号化コンテンツ鍵Ｅ２ＣＫに対してＲＳＡ復号処理を行う。
【００６１】
ＲＳＡ復号化処理は、具体的には、暗号文メッセージＣに対して、Ｃ＾ｄ１（ｍｏｄ　ｎ１）を計算することにより行われる。ここで、第二暗号化コンテンツ鍵Ｅ２ＣＫを暗号文とした場合、その復号文は、Ｅ２ＣＫ＾ｄ１（ｍｏｄ　ｎ１）となる。以下では、Ｅ２ＣＫ＾ｄ（ｍｏｄ　ｎ１）を、Ｅ３ＣＫと表す。
暗号処理部１１６は、第二暗号化コンテンツ鍵Ｅ２ＣＫに対応する復号文Ｅ３ＣＫを、第二送信制御部１０６へ出力する。
【００６２】
（ｃ）ハッシュ埋込部１１２から、ハッシュ値計算要求ＨＡＳＨが入力された場合
暗号処理部１１６は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのそれぞれに対するハッシュ値であるコンテンツ鍵ハッシュＨＣＫ＿１、ＨＣＫ＿２、…、ＨＣＫ＿ｎを計算する。ハッシュ値は、ハッシュ関数にデータを入力した際の出力値である。暗号処理部１１６は、ハッシュ関数アルゴリズムとして、例えば、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ－１）を用いるものとする。
【００６３】
暗号処理部１１６は、ｎ個のコンテンツ鍵ハッシュＨＣＫ＿１、ＨＣＫ＿２、…、ＨＣＫ＿ｎを、ハッシュ埋込部１１２へ出力する。
（ｄ）第三送信制御部１１９からコンテンツ暗号化要求ＡＥＳＥが入力された場合
暗号処理部１１６は、以下の手順で、ｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎの暗号化処理を行う。
【００６４】
先ず、暗号処理部１１６は、コンテンツ鍵保持部１０３からｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを取得する。
続いて、暗号処理部１１６は、ｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎのそれぞれに対して、それぞれ異なるｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを暗号鍵として用い、暗号化処理を行う。
【００６５】
具体的には、暗号処理部１１６は、証拠埋込コンテンツデータＶＣＮＴ１＿１を、コンテンツ鍵ＣＫ＿１を暗号鍵として用いて暗号化し、暗号化第一コンテンツデータＥＣＮＴ１＿１を生成する。ｉ＝２、３、…、ｎにつても同様にして、暗号処理部１１６は、暗号化第一コンテンツデータＥＣＮＴ１＿２、ＥＣＮＴ１＿３、…、ＥＣＮＴ１＿ｎを生成する。暗号処理部１１６がここで用いる暗号化アルゴリズムは、共通鍵ブロック暗号であるＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）アルゴリズムとする。
【００６６】
暗号処理部１１６は、生成したｎ個の暗号化第一コンテンツデータＥＣＮＴ１＿１、ＥＣＮＴ１＿２、…、ＥＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する。
（１７）入力部１１７
入力部１１７は、例えば、ボタン等で実現され、ユーザからボタン等が操作されることにより、受信装置２０へのコンテンツデータの転送要求である転送依頼情報を受け付ける

。入力部１１７は、転送依頼情報を受け付けると、転送先装置識別子取得部１１５へ、転送先装置識別子要求情報ＲＥＱ４を出力する。

【００６７】

（１８）送受信部１１８

送受信部１１８は、ケーブル６０を介して、受信装置２０の送受信部２１１と接続されており、第一送信制御部１０５、第二送信制御部１０６、及び第三送信制御部１１９からの要求に従い、受信装置２０へデータを送信する。

また、送受信部１１８は、受信装置２０から送信されたデータを受信する。

【００６８】

（１９）第三送信制御部１１９

第三送信制御部１１９は、第二送信制御部１０６からコンテンツ転送要求ＲＥＱが入力されると、先ず、第一コンテンツデータ保持部１０９から第一コンテンツデータＣＮＴ１を取得する。次に、第三送信制御部１１９は、第一コンテンツデータＣＮＴ１をコンテンツ複製部１１０へ出力し、コンテンツ複製部１１０から、ｎ個に複製された第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを取得する。

【００６９】

続いて、第三送信制御部１１９は、ｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを、装置識別子埋込部１１１へ出力し、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＴＩＤ＿２とが電子透かしとして埋め込まれたｎ個の識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎを取得する。

続いて、第三送信制御部１１９は、ｎ個の識別子埋込コンテンツデータＤＣＮＴ１＿１、ＤＣＮＴ１＿２、…、ＤＣＮＴ１＿ｎを、ハッシュ埋込部１１２へ出力し、コンテンツ鍵ハッシュＨＣＫ＿１、ＨＣＫ＿２、…、ＨＣＫ＿ｎの電子透かしが追加して埋め込まれた、ｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎを取得する。

【００７０】

続いて、第三送信制御部１１９は、ｎ個のハッシュ埋込コンテンツデータＨＣＮＴ１＿１、ＨＣＮＴ１＿２、…、ＨＣＮＴ１＿ｎを、証拠埋込部１１３へ出力し、証拠情報ＥＶの電子透かしが追加で埋め込まれた、ｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎを取得する。

その後、第三送信制御部１１９は、コンテンツ暗号化要求ＡＥＳＥとｎ個の証拠埋込コンテンツデータＶＣＮＴ１＿１、ＶＣＮＴ１＿２、…、ＶＣＮＴ１＿ｎとを暗号処理部１１６へ出力し、暗号処理部１１６から、暗号化された証拠埋込コンテンツデータであるｎ個の暗号化第一コンテンツデータＥＣＮＴ１＿１、ＥＣＮＴ１＿２、…、ＥＣＮＴ１＿ｎを取得する。

【００７１】

そして、第三送信制御部１１９は、図９に示すように、暗号化第一コンテンツデータと暗号化に用いたコンテンツ鍵の識別子とを対応付けた（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）から成るｎ組を、送受信部１１８を介して、受信装置２０へ送信する。

２．受信装置２０

図１０は、受信装置２０の構成を示すブロック図である。同図に示すように、受信装置２０は、公開鍵保持部２０１、復号コンテンツ鍵保持部２０２、第一受信制御部２０３、第二受信制御部２０４、選択情報保持部２０５、コンテンツ鍵選択部２０６、暗号化コンテンツ選択部２０７、第二コンテンツデータ保持部２０８、装置識別子出力部２０９、装置識別子保持部２１０、送受信部２１１、暗号処理部２１２、及び第三受信制御部２１３から構成される。

【００７２】

受信装置２０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどを備えるコンピュータシステムである。受信装置２０は、マイクロプロセッ

サが、ＲＯＭ、ＲＡＭ、又はハードディスクに記録されているコンピュータプログラムに従い動作することにより、その機能を達成する。

なお、受信装置２０を構成する各ブロックは、ハードウェアにより構成されてもよいし、またソフトウェアにより構成されてもよい。

【００７３】

以下では、受信装置２０を構成する各ブロックについて説明する。

（１）公開鍵保持部２０１

公開鍵保持部２０１は、図１１に示すように、受信装置公開鍵情報ＰＫ２と受信装置秘密鍵情報ＳＫ２とを保持している。

受信装置公開鍵情報ＰＫ２は、ＲＳＡの公開鍵である第二公開鍵ｎ２及びｅ２から構成され、受信装置秘密鍵情報ＳＫ２は、ＲＳＡの秘密鍵である第二秘密鍵ｄ２から構成される。

【００７４】

これらの鍵情報は、システム管理者によって計算され、受信装置２０の製造時に公開鍵保持部２０１に格納されたものである。第二公開鍵ｎ２及びｅ２と、第二秘密鍵ｄ２との生成方法については、送信装置１０の第一公開鍵ｎ１及びｅ１の生成方法、並びに、第一秘密鍵ｄ１の生成方法と同様であるが、ここで注意する点は、第二公開鍵及び第二秘密鍵の生成においては、第一公開鍵及び第一秘密鍵の生成に用いた素数ｐ１及びｑ１とは異なる素数ｐ２及びｑ２を選択する点である。

【００７５】

（２）復号コンテンツ鍵保持部２０２

復号コンテンツ鍵保持部２０２は、図１２に示すように、復号コンテンツ鍵ＤＣＫを保持している。

（３）第一受信制御部２０３

第一受信制御部２０３は、送受信部２１１を介して、送信装置１０から図８に示したｎ組のコンテンツ鍵識別子、及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝を受信すると、受信したｎ組のコンテンツ鍵識別子、及び第一暗号化コンテンツ鍵を、コンテンツ鍵選択部２０６へ出力する。その後、第一受信制御部２０３は、コンテンツ鍵選択部２０６から、１組の選択コンテンツ鍵識別子ＳＣＫＩＤ、及び選択第一暗号化コンテンツ鍵ＳＥＣＫを受け取る。

【００７６】

第一受信制御部２０３は、選択コンテンツ鍵識別子ＳＣＫＩＤを、選択情報保持部２０５に格納し、選択第一暗号化コンテンツ鍵ＳＥＣＫとＲＳＡ暗号化処理要求ＲＳＡＥとを、暗号処理部２１２へ出力する。その後、第一受信制御部２０３は、暗号処理部２１２から、暗号化されたデータである第二暗号化コンテンツ鍵Ｅ２ＣＫを受け取る。

第一受信制御部２０３は、送受信部２１１を介して、第二暗号化コンテンツ鍵Ｅ２ＣＫを、送信装置１０へ送信する。

【００７７】

（４）第二受信制御部２０４

第二受信制御部２０４は、送受信部２１１を介して、送信装置１０から１個の第三暗号化コンテンツ鍵Ｅ３ＣＫを受信すると、暗号処理部２１２へ第三暗号化コンテンツ鍵Ｅ３ＣＫとＲＳＡ復号処理要求ＲＳＡＤとを出力する。その後、第二受信制御部２０４は、暗号処理部２１２から復号化されたデータである復号コンテンツ鍵ＤＣＫを受け取る。続いて、第二受信制御部２０４は、復号コンテンツ鍵ＤＣＫを、復号コンテンツ鍵保持部２０２へ格納する。

【００７８】

（５）選択情報保持部２０５

選択情報保持部２０５は、図１３に示すように、選択コンテンツ鍵識別子ＳＣＫＩＤを保持している。

（６）コンテンツ鍵選択部２０６

コンテンツ鍵選択部２０６は、第一受信制御部２０３からｎ組のコンテンツ鍵識別子、及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝が入力されると、ｎ組の中から１組のコンテンツ鍵識別子、及び第一暗号化コンテンツ鍵を選択する。ここで、ｎ組の中から一組を選択する方法は、例えば、ｎ以下の乱数を生成し、生成された乱数をもとに１組を選択してもよい。

【００７９】

以下では、選択されたコンテンツ識別子を、選択コンテンツ鍵識別子ＳＣＫＩＤ＿ｓ（ｓ＝１、２、…、ｎの何れか）とし、選択された第一暗号化コンテンツ鍵を、選択第一暗号化コンテンツ鍵ＳＥＣＫ＿ｓ（ｓ＝１、２、…、ｎの何れか）とする。

コンテンツ鍵選択部２０６は、選択コンテンツ鍵識別子ＳＣＫＩＤと選択第一暗号化コンテンツ鍵ＳＥＣＫとを、第一受信制御部２０３へ出力する。

【００８０】

（７）暗号化コンテンツ選択部２０７

暗号化コンテンツ選択部２０７は、第三受信制御部２１３からｎ組のコンテンツ鍵識別子、及び暗号化第一コンテンツデータ（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）が入力されると、先ず、選択情報保持部２０５から選択コンテンツ鍵識別子ＳＣＫＩＤを取得する。

【００８１】

続いて、暗号化コンテンツ選択部２０７は、ｎ個のコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎの中から、選択コンテンツ鍵識別子ＳＣＫＩＤの値と一致するものを抽出する。以下では、選択コンテンツ鍵識別子ＳＣＫＩＤの値と一致するコンテンツ鍵識別子により識別される暗号化第一コンテンツデータを、ＳＥＣＮＴ１とする。

【００８２】

その後、暗号化コンテンツ選択部２０７は、選択コンテンツ鍵識別子ＳＣＫＩＤと暗号化第一コンテンツデータＳＥＣＮＴ１とを、第三受信制御部２１３へ出力する。

（８）第二コンテンツデータ保持部２０８

第二コンテンツデータ保持部２０８は、図１４に示すように、第二コンテンツデータＣＮＴ２を保持している。同図に示すように、第二コンテンツデータＣＮＴ２には、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ，及びコンテンツ鍵ハッシュＨＣＫが電子透かしとして埋め込まれている。

【００８３】

（９）装置識別子出力部２０９

装置識別子出力部２０９は、送受信部２１１を介して、送信装置１０から転送先装置識別子取得依頼情報ＲＥＱ５を受信すると、装置識別子保持部２１０から装置識別子ＩＤ＿２を取得する。装置識別子出力部２０９は、取得した装置識別子ＩＤ＿２を、送受信部２１１を介して、送信装置１０へ送信する。

【００８４】

（１０）装置識別子保持部２１０

装置識別子保持部２１０は、図１５に示すように、装置識別子ＩＤ＿２を保持している。装置識別子ＩＤ＿２は、受信装置２０を識別する情報であり、受信装置２０の製造時に予め与えられ、装置識別子保持部２１０に格納された不変の値である。

（１１）送受信部２１１

送受信部２１１は、送信装置１０の送受信部１１８とケーブル６０を介して接続されており、第一受信制御部２０３、及び第二受信制御部２０４からの要求に従い、送信装置１０へデータを送信する。

【００８５】

また、送受信部２１１は、送信装置１０から送信されたデータを受信する。

（１２）暗号処理部２１２
暗号処理部２１２は、以下の暗号処理を行う。
（ａ）第一受信制御部２０３からＲＳＡ暗号化処理要求ＲＳＡＥを入力された場合
暗号処理部２１２は、以下の手順で選択第一暗号化コンテンツ鍵ＳＥＣＫを暗号化し、暗号文を生成する。
【００８６】
先ず、暗号処理部２１２は、公開鍵保持部２０１から、受信装置公開鍵情報ＰＫ２に含まれる第二公開鍵ｎ２及びｅ２を取得する。
次に、暗号処理部２１２は、第二公開鍵ｎ２及びｅ２を用い、選択第一暗号化コンテンツ鍵ＳＥＣＫに対してＲＳＡ暗号化処理を行う。ここで、選択第一暗号化コンテンツ鍵ＳＥＣＫを元のメッセージとした場合、その暗号文は、ＳＥＣＫ＾ｅ２（ｍｏｄ　ｎ２）となる。選択第一暗号化コンテンツ鍵ＳＥＣＫの暗号文ＳＥＣＫ＾ｅ２（ｍｏｄ　ｎ２）を、第二暗号化コンテンツ鍵Ｅ２ＣＫとする。なお、ＲＳＡ暗号化処理は、送信装置１０の説明で述べたため、ここでは詳細な説明は省略する。
【００８７】
続いて、暗号処理部２１２は、第二暗号化コンテンツ鍵Ｅ２ＣＫを第二受信制御部２０４へ出力する。
（ｂ）第二受信制御部２０４からＲＳＡ復号処理要求ＲＳＡＤを入力された場合
暗号処理部２１２は、以下の手順で、第三暗号化コンテンツ鍵Ｅ３ＣＫを復号し、復号文を生成する。
【００８８】
先ず、暗号処理部２１２は、公開鍵保持部２０１から、受信装置公開鍵情報ＰＫ２に含まれる第二公開鍵ｎ２と受信装置秘密鍵情報ＳＫ２に含まれる第二秘密鍵ｄ２とを取得する。
次に、暗号処理部２１２は、第二公開鍵ｎ２と第二秘密鍵ｄ２とを用い、第三暗号化コンテンツ鍵Ｅ３ＣＫに対してＲＳＡ復号処理を行う。第三暗号化コンテンツ鍵Ｅ３ＣＫの復号文を、復号コンテンツ鍵ＤＣＫとする。なお、ＲＳＡ復号処理は、送信装置１０の説明で述べたため、ここでは詳細な説明は省略する。
【００８９】
続いて、暗号処理部２１２は、復号コンテンツ鍵ＤＣＫを、第二受信制御部２０４へ出力する。
（ｃ）第三受信制御部２１３からコンテンツ復号化要求ＡＥＳＤを入力された場合
暗号処理部２１２は、受け取った復号コンテンツ鍵ＤＣＫを用い、暗号化第一コンテンツデータＳＥＣＮＴ１の復号処理を行う。ここで、暗号処理部２１２は、復号アルゴリズムとして、送信装置１０において暗号化第一コンテンツデータの生成に用いた暗号化アルゴリズムであるＡＥＳを用いる。
【００９０】
その後、暗号処理部２１２は、復号された暗号化第一コンテンツデータＳＥＣＮＴ１である復号コンテンツＤＣＮＴを第三受信制御部２１３へ出力する。
（１３）第三受信制御部２１３
第三受信制御部２１３は、送受信部２１１を介して、送信装置１０から、ｎ個のコンテンツ鍵識別子と、暗号化第一コンテンツデータとの組（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）を受信する。
【００９１】
第三受信制御部２１３は、先ず、ｎ個のコンテンツ鍵識別子と暗号化第一コンテンツデータとの組（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）を、暗号化コンテンツ選択部２０７へ出力し、暗号化コンテンツ選択部２０７から、１組のコンテンツ鍵識別子ＳＣＫＩＤと、暗号化第一コンテンツデータＳＥＣＮＴ１とを取得する。

【００９２】
次に、第三受信制御部２１３は、復号コンテンツ鍵保持部２０２から復号コンテンツ鍵ＤＣＫを取得する。
続いて、第三受信制御部２１３は、暗号処理部２１２へコンテンツ復号化要求ＡＥＳＤと暗号化第一コンテンツデータＳＥＣＮＴ１と復号コンテンツ鍵識別子ＤＣＫとを出力し、暗号処理部２１２から、復号されたコンテンツデータである復号化コンテンツデータＤＣＮＴを取得する。
【００９３】
その後、第三受信制御部２１３は、復号化コンテンツデータＤＣＮＴを、第二コンテンツデータＣＮＴ２として、第二コンテンツデータ保持部２０８へ格納する。
３．コンテンツ流出元特定装置３０
図１６は、コンテンツ流出元特定装置３０の構成を示すブロック図である。同図に示すように、コンテンツ流出元特定装置３０は、透かし情報抽出部３０１、証拠検証部３０２、流出元判定部３０３、流出元出力部３０４、コンテンツデータ入力部３０５、追跡コンテンツデータ保持部３０６、暗号処理部３０７、及び暗号鍵保持部３０８から構成される。
【００９４】
コンテンツ流出元特定装置３０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット等を備えるコンピュータシステムである。コンテンツ流出元特定装置３０は、マイクロプロセッサが、ＲＯＭ、ＲＡＭ又はハードディスクに記憶されているコンピュータプログラムに従い動作することにより、その機能を達成する。
なお、コンテンツ流出元特定装置３０を構成する各ブロックは、ハードウェアにより構成されてもよいし、またソフトウェアにより構成されてもよい。
【００９５】
以下では、コンテンツ流出元特定装置３０を構成する各ブロックについて説明する。
（１）透かし情報抽出部３０１
透かし情報抽出部３０１は、コンテンツデータ入力部３０５から、透かし情報抽出要求が入力された場合、追跡コンテンツデータ保持部３０６から、追跡コンテンツデータＴＣＮＴを取得する。
【００９６】
透かし情報抽出部３０１は、取得した追跡コンテンツデータＴＣＮＴに埋め込まれている電子透かしの抽出を行う。なお、電子透かしを抽出する技術は、すでに公知技術であり、広く知られているため、ここでは説明は省略する。
透かし情報抽出部３０１は、追跡コンテンツデータＴＣＮＴから、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫを抽出し、抽出した各情報を、証拠検証部３０２へ出力する。
【００９７】
（２）証拠検証部３０２
証拠検証部３０２は、透かし情報抽出部３０１から転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫが入力されると、証拠情報ＥＶのＲＳＡ復号処理をするために、暗号処理部３０７へ転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びＲＳＡ復号処理要求ＲＳＡＤを出力する。
【００９８】
証拠検証部３０２は、暗号処理部３０７から、復号されたデータである復号化証拠情報ＤＥＶを受け取る。続いて、証拠検証部３０２は、復号化証拠情報ＤＥＶのハッシュ値を計算するために、ハッシュ値計算要求ＨＡＳＨと復号化証拠情報ＤＥＶとを、暗号処理部３０７へ出力する。その後、証拠検証部３０２は、暗号処理部３０７から、復号化証拠情報のハッシュ値である復号化証拠情報ハッシュＨＤＥＶを取得する。
【００９９】
証拠検証部３０２は、復号化証拠情報ハッシュＨＤＥＶの値と、コンテンツ鍵ハッシュ

ＨＣＫの値とが等しい否か、比較する。
復号化証拠情報ハッシュＨＤＥＶの値と、とコンテンツ鍵ハッシュＨＣＫの値とが等しい場合、証拠検証部３０２は、証拠正当フラグＦＬＡＧを「１」に設定し、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠正当フラグＦＬＡＧを、流出元判定部３０３へ出力する。
【０１００】
一方、復号化証拠情報ハッシュＨＤＥＶの値と、コンテンツ鍵ハッシュＨＣＫの値とが異なる場合、証拠検証部３０２は、証拠正当フラグＦＬＡＧを「０」に設定し、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、及び証拠正当フラグＦＬＡＧを、流出元判定部３０３へ出力する。
（３）流出元判定部３０３
流出元判定部３０３は、証拠検証部３０２から、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、及び証拠正当フラグＦＬＡＧを受け取る。
【０１０１】
受け取った証拠正当フラグが１に設定されている場合、流出元判定部３０３は、転送先装置識別子ＩＤ＿２を、流出元装置識別子として、流出元出力部３０４へ出力する。
一方、受け取った証拠正当フラグが０に設定されている場合、流出元判定部３０３は、転送元装置識別子ＩＤ＿１を、流出元装置識別子として、流出元出力部３０４へ出力する。
【０１０２】
（４）流出元出力部３０４
流出元出力部３０４は、ディスプレイを備えており、ディスプレイに出力するための画面情報の生成等を行う。
流出元出力部３０４は、流出元判定部３０３から流出元装置識別子を受け取ると、受け取った流出元装置識別子を表示するための画面情報を生成し、生成した画面情報を、ディスプレイに出力する。
【０１０３】
（５）コンテンツデータ入力部３０５
コンテンツデータ入力部３０５は、具体的には、ＤＶＤドライブユニットであって、ＤＶＤ－ＲＡＭである記録媒体４０からコンテンツデータを読み出す。コンテンツデータ入力部は、読み出したコンテンツデータを、追跡コンテンツデータＴＣＮＴとして、追跡コンテンツデータ保持部３０６に格納する。
【０１０４】
その後、コンテンツデータ入力部３０５は、透かし情報抽出部３０１へ、透かし情報抽出要求を出力する。
ここで、記録媒体４０は、不正コピーにより作成された海賊版コンテンツが記録されている記録媒体である。
（６）追跡コンテンツデータ保持部３０６
追跡コンテンツデータ保持部３０６は、図１７に示すように、追跡コンテンツデータＴＣＮＴを保持している。同図に示すように、追跡コンテンツデータには、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫが、電子透かしとして埋め込まれている。
【０１０５】
（７）暗号処理部３０７
暗号処理部３０７は、以下の暗号処理を行う。
（ａ）証拠検証部３０２からＲＳＡ復号処理要求ＲＳＡＤを入力された場合
暗号処理部３０７は、以下の手順で、証拠情報ＥＶを復号し、復号文を生成する。
先ず、暗号処理部３０７は、暗号鍵保持部３０８を検索し、証拠検証部３０２から受け取った転送先装置識別子ＩＤ＿２と等しい装置識別子に対応付けられている鍵情報ＳＫ＿２を取得する。そして、鍵情報ＳＫ＿２に含まれる公開鍵ｎ２と、秘密鍵ｄ２とを用いて

、証拠情報ＥＶに対し、ＲＳＡ復号処理を行う。
【０１０６】
ＲＳＡ復号処理では、暗号文Ｃ、公開鍵ｎｊ、秘密鍵ｄｊとした場合、その復号文は、Ｃ＾ｄｊ（ｍｏｄ　ｎｊ）となる。従って、暗号処理部３０７は、証拠情報ＥＶの復号文として、ＥＶ＾ｄ２（ｍｏｄ　ｎ２）を得る。
暗号処理部３０７は、証拠情報ＥＶの復号文ＥＶ＾ｄ２（ｍｏｄ　ｎ２）を、復号化証拠情報ＤＥＶとして、証拠検証部３０２へ出力する。
【０１０７】
（ｂ）証拠検証部３０２ら、ハッシュ値計算要求ＨＡＳＨを入力された場合
暗号処理部３０７は、復号化証拠情報ＤＥＶに対するハッシュ値である復号化証拠情報ハッシュＨＤＥＶを計算する。
既に説明したように、ハッシュ値は、ハッシュ関数にデータを入力した際の出力値であり、暗号処理部３０７は、ハッシュ関数アルゴリズムとして、送信装置１０の暗号処理部１１６と同一のアルゴリズムを用いるものとする。
【０１０８】
（８）暗号鍵保持部３０８
暗号鍵保持部３０８は、図１８に示すように、複数個の装置識別子と鍵情報とを対応付けて保持している。
各装置識別子に対応付けら得ている鍵情報は、公開鍵及び秘密鍵を含み、各装置識別子により識別される装置が保持する公開鍵及び秘密鍵と共通である。
＜動作＞
１．システム全体の動作
図１９は、コンテンツ配信システム１全体の動作を示すフローチャートである。
【０１０９】
先ず、コンテンツ配信システム１は、送信装置１０と受信装置２０との間において、コンテンツ送受信処理鍵を行う（ステップＳ１０１）。
海賊版コンテンツが流出した場合には、コンテンツ配信システム１は、コンテンツ流出元特定処理を行う（ステップＳ１０２）。
２．コンテンツ送受信処理の動作
図２０から図２２は、コンテンツ送受信処理の動作を示すフローチャートである、なお、ここに示す動作は、図１９のステップＳ１０１の詳細である。
【０１１０】
送信装置１０の入力部１１７は、ユーザからコンテンツの転送依頼情報を受け付けると（ステップＳ２０１）、転送先装置識別子取得部１１５へ、転送先装置識別子要求情報ＲＥＱ４を出力する（ステップＳ２０２）。
転送先装置識別子取得部１１５は、転送先装置識別子要求情報を受け付けると、送受信部１１８を介して、受信装置２０へ、転送先装置識別子取得依頼情報ＲＥＱ５を送信し、受信装置２０の送受信部２１１は、転送先装置識別子取得依頼情報ＲＥＱ５を受信する（ステップＳ２０３）。
【０１１１】
受信装置２０の装置識別子出力部２０９は、送受信部２１１を介して、送信装置１０から、転送先装置識別子取得依頼情報ＲＥＱ５を受信すると、装置識別子保持部２１０から、装置識別子ＩＤ＿２を取得する（ステップＳ２０４）。
装置識別子出力部２０９は、装置識別子ＩＤ＿２を、転送先装置識別子として、送受信部２１１を介して、送信装置１０へ送信し、送信装置１０の送受信部１１８は、転送先装置識別子ＩＤ＿２を受信する（ステップＳ２０５）。
【０１１２】
転送先装置識別子取得部１１５は、送受信部１１８を介して、転送先装置識別子ＩＤ＿２を受信すると、装置識別子保持部１１４へ格納する（ステップＳ２０６）。その後、転送先装置識別子取得部１１５は、コンテンツ鍵生成部１０１に対して、コンテンツ鍵生成

要求ＲＥＱ１を出力する。
コンテンツ鍵生成部１０１は、転送先装置識別子取得部１１５から、コンテンツ鍵生成要求ＲＥＱ１を受け付けると、ｎ個（ｎは予め与えられる２以上の整数）の１２８ビットのコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを生成する（ステップＳ２０７）。そして、コンテンツ鍵生成部１０１は、生成したｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを、コンテンツ鍵識別子生成部１０２へ出力する。

【０１１３】

コンテンツ鍵識別子生成部１０２は、コンテンツ鍵生成部１０１からｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎが入力されると、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのそれぞれを識別するコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎを生成する（ステップＳ２０８）。
コンテンツ鍵識別子生成部１０２は、入力されたｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎと、生成したｎ個のコンテンツ鍵識別子ＣＫＩＤ＿１、ＣＫＩＤ＿２、…、ＣＫＩＤ＿ｎとを、それぞれ対応付けて、コンテンツ鍵保持部１０３へ格納する（ステップＳ２０９）。その後、コンテンツ鍵識別子生成部１０２は、第一送信制御部１０５へ、第一送信制御開始要求ＲＥＱ２を出力する。

【０１１４】

第一送信制御部１０５は、コンテンツ鍵識別子生成部１０２から第一送信制御開始要求ＲＥＱ２が入力されると、先ず、コンテンツ鍵保持部１０３からｎ組のコンテンツ鍵識別子とコンテンツ鍵｛（ＣＫＩＤ＿１、ＣＫ＿１）、（ＣＫＩＤ＿２、ＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＣＫ＿ｎ）｝を取得する。
その後、第一送信制御部１０５は、暗号処理部１１６へ、ｎ個のコンテンツ鍵とＲＳＡ暗号化処理要求ＲＳＡＥとを出力する。

【０１１５】

暗号処理部１１６は、まず、公開鍵保持部１０４から、送信装置公開鍵情報ＰＫ１に含まれる第一公開鍵ｎ１及びｅ１を取得する。次に、暗号処理部１１６は、第一公開鍵ｎ１及びｅ１を用いて、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのそれぞれに対して、ＲＳＡ暗号化処理を行う（ステップＳ２１０）。ここでは、コンテンツ鍵ＣＫ＿ｉの暗号文をＥＣＫ＿ｉとすると、具体的には、ＥＣＫ＿ｉ＝ＣＫ＿ｉ＾ｅ１（ｍｏｄｎ１）となる。暗号処理部１１６は、ｎ個のコンテンツ鍵に対応する暗号文ＥＣＫ＿１、ＥＣＫ＿２、…、ＥＣＫ＿ｎを、第一送信制御部１０５へ出力する。

【０１１６】

第一送信制御部１０５は、暗号処理部１１６から、ｎ個の暗号化されたデータである第一暗号化コンテンツ鍵を受け取ると、送受信部１１８を介して、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝を、受信装置２０へ送信し、受信装置２０の送受信部２１１は、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵を受信する（ステップＳ２１１）。

【０１１７】

受信装置２０の第一受信制御部２０３は、送受信部２１１を介して、送信装置１０から、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝を受信すると、先ず、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵を、コンテンツ鍵選択部２０６へ出力する。

【０１１８】

コンテンツ鍵選択部２０６は、ｎ組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵｛（ＣＫＩＤ＿１、ＥＣＫ＿１）、（ＣＫＩＤ＿２、ＥＣＫ＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＫ＿ｎ）｝の中から、１組のコンテンツ鍵識別子及び第一暗号化コンテンツ鍵を選択する（ステップＳ２２１）。
第一受信制御部２０３は、コンテンツ鍵選択部２０６から、選択コンテンツ鍵識別子Ｓ

ＣＫＩＤと選択第一暗号化コンテンツ鍵ＳＥＣＫとを受け取る。そして、受け取った選択コンテンツ鍵識別子ＳＣＫＩＤを、選択情報保持部２０５に格納する（ステップＳ２２２）。その後、第一受信制御部２０３は、選択第一暗号化コンテンツ鍵ＳＥＣＫと、ＲＳＡ暗号化処理要求ＲＳＡＥとを、暗号処理部２１２へ出力する。

【０１１９】

暗号処理部２１２は、公開鍵保持部２０１から、受信装置公開鍵情報ＰＫ２に含まれる公開鍵ｎ２及びｅ２を取得する。続いて、暗号処理部２１２は、第二公開鍵ｎ２及びｅ２を用いて、選択第一暗号化コンテンツ鍵ＳＥＣＫに対してＲＳＡ暗号化処理を行い、第二暗号化コンテンツ鍵Ｅ２ＣＫを生成する（ステップＳ２２３）。第二暗号化コンテンツ鍵は、具体的には、Ｅ２ＣＫ＝ＣＫ＿ｓ＾（ｅ１×ｅ２）（ｍｏｄ　ｎ２）となる。ここで、ｓ＝１、２、…、ｎの何れかである。

【０１２０】

第一受信制御部２０３は、暗号処理部２１２から第二暗号化コンテンツ鍵Ｅ２ＣＫを受け取ると、送受信部２１１を介して、第二暗号化コンテンツ鍵Ｅ２ＣＫを送信装置１０へ送信し、送信装置１０は、第二暗号化コンテンツ鍵Ｅ２ＣＫを受信する（ステップＳ２２４）。

送信装置１０の第二送信制御部１０６は、送受信部１１８を介して、受信装置２０から１個の第二暗号化コンテンツ鍵Ｅ２ＣＫを受信すると、暗号処理部１１６へ、第二暗号化コンテンツ鍵Ｅ２ＣＫと、ＲＳＡ復号処理要求ＲＳＡＤを出力する。

【０１２１】

暗号処理部１１６は、公開鍵保持部１０４から、第一公開鍵ｎ１と第一秘密鍵ｄ１とを取得する。次に、暗号処理部１１６は、第一公開鍵ｎ１と第一秘密鍵ｄ１とを用いて、第二暗号化コンテンツ鍵Ｅ２ＣＫに対してＲＳＡ復号化処理を行う（ステップＳ２２５）。ここでは、第二暗号化コンテンツ鍵Ｅ２ＣＫの復号文を、第三暗号化コンテンツ鍵Ｅ３ＣＫとする。第三暗号化コンテンツ鍵は、具体的には、Ｅ３ＣＫ＝ＣＫ＿ｓ＾（ｅ１×ｅ２×ｄ１）（ｍｏｄ　ｎ１）＝ＣＫ＿ｓ＾ｅ２（ｍｏｄ　ｎ１）となる。暗号処理部１１６は、第三暗号化コンテンツ鍵Ｅ３ＣＫを、第二送信制御部１０６へ出力する。

【０１２２】

第二送信制御部１０６は、暗号処理部１１６から、第二暗号化コンテンツ鍵Ｅ２ＣＫが復号化されたデータである第三暗号化コンテンツ鍵Ｅ３ＣＫを受け取ると、受け取った第三暗号化コンテンツ鍵Ｅ３ＣＫを、証拠取得部１０７へ出力する。

証拠取得部１０７は、第二送信制御部１０６から、証拠情報ＥＶとして、第三暗号化コンテンツ鍵Ｅ３ＣＫを取得し（ステップＳ２２６）、証拠情報ＥＶを、証拠保持部１０８へ格納する（ステップＳ２２７）。

【０１２３】

続いて、第二送信制御部１０６は、送受信部１１８を介して、第三暗号化コンテンツ鍵Ｅ３ＣＫを、受信装置２０へ送信し、受信装置２０の送受信部２１１は、第三暗号化コンテンツ鍵Ｅ３ＣＫを受信する（ステップＳ２２８）。また一方で、第二送信制御部１０６は、第三送信制御部１１９に対して、コンテンツ転送要求ＲＥＱ３を出力する。

受信装置２０の第二受信制御部２０４は、送受信部２１１を介して、送信装置１０から、１個の第三暗号化コンテンツ鍵Ｅ３ＣＫを受信すると、暗号処理部２１２へ、第三暗号化コンテンツ鍵Ｅ３ＣＫとＲＳＡ復号処理要求ＲＳＡＤとを出力する。

【０１２４】

暗号処理部２１２は、公開鍵保持部２０１から、第二公開鍵ｎ２と第二秘密鍵ｄ２とを取得する。次に、暗号処理部２１２は、第二公開鍵ｎ２と第二秘密鍵ｄ２とを用いて、第三暗号化コンテンツ鍵Ｅ３ＣＫに対してＲＳＡ復号化処理を行い、復号コンテンツ鍵ＤＣＫを生成する（ステップＳ２２９）。ここで、復号コンテンツ鍵ＤＣＫは、具体的にはＤＣＫ＝ＣＫ＿ｓ＾（ｅ２×ｄ２）（ｍｏｄ　ｎ２）＝ＣＫ＿ｓ（ｍｏｄ　ｎ２）となる。暗号処理部２１２は、生成した復号コンテンツ鍵ＤＣＫを、第二受信制御部２０４へ出力する。

【０１２５】
第二受信制御部２０４は、暗号処理部２１２から復号コンテンツ鍵ＤＣＫを受け取ると、受け取った復号コンテンツ鍵ＤＣＫを、復号コンテンツ鍵保持部２０２へ格納する（ステップＳ２３０）。
第三送信制御部１１９は、第二送信制御部１０６からコンテンツ転送要求ＲＥＱが入力されると、先ず、第一コンテンツデータ保持部１０９から第一コンテンツデータＣＮＴ１を取得する。次に、第三送信制御部１１９は、第一コンテンツデータＣＮＴ１をコンテンツ複製部１１０へ出力する。
【０１２６】
コンテンツ複製部１１０は、第三送信制御部１１９から第一コンテンツデータＣＮＴ１が入力されると、第一コンテンツデータＣＮＴ１を複製し、全く同じデータであるｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを生成する（ステップＳ２４１）。コンテンツ複製部１１０は、生成したｎ個の第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを、第三送信制御部１１９へ出力する。
【０１２７】
第三送信制御部１１９は、ｎ個に複製された第一コンテンツデータＣＮＴ１＿１、ＣＮＴ１＿２、…、ＣＮＴ１＿ｎを取得すると、第三送信制御部１１９、装置識別子埋込部１１１、ハッシュ透かし埋込部１１２、証拠埋込部１１３、及び暗号処理部１１６は、ｉ＝１からｎについて、ステップＳ２４２からステップＳ２４８までを繰り返す（ステップＳ２４２）。
【０１２８】
先ず、第一コンテンツデータＣＮＴ１＿ｉに対して、装置識別子埋込部１１１は、転送元装置識別子ＩＤ＿１を、電子透かしとして埋め込み（ステップＳ２４３）、続いて、転送先装置識別子ＩＤ＿２を、電子透かしとして埋め込む（ステップＳ２４４）。
続いて、ハッシュ埋込部１１２は、ＩＤ＿１及びＩＤ＿２が埋め込まれた第一暗号化コンテンツデータＤＣＮＴ＿ｉに対して、コンテンツ鍵ハッシュＨＣＫ＿ｉを電子透かしとして埋め込み、ハッシュ埋込コンテンツデータＨＣＫ＿ｉを生成する（ステップＳ２４５）。
【０１２９】
次に、証拠埋込部１１３は、ハッシュ埋込コンテンツデータＨＣＫ＿ｉに対して、証拠情報ＥＶを電子透かしとして埋め込み、証拠埋込コンテンツデータＶＣＮＴ１＿ｉを生成する（ステップＳ２４６）。
最後に、暗号処理部１１６は、証拠埋込コンテンツデータＶＣＮＴ１＿ｉを、コンテンツ鍵ＣＫ＿ｉを暗号鍵として用いて暗号化し、暗号化第一コンテンツデータＥＣＮＴ１＿ｉを生成する（ステップＳ２４７）。
【０１３０】
第三送信制御部１１９は、暗号処理部１１６から、ｎ個の暗号化第一コンテンツデータを受け取ると、送受信部１１８を介して、暗号化第一コンテンツデータと、暗号化に用いたコンテンツ鍵の識別子であるコンテンツ鍵識別子との組である（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）を、受信装置２０へ送信し、受信装置２０の送受信部２１１は、ｎ組の暗号化第一コンテンツデータとコンテンツ識別子とを受信する（ステップＳ２４９）。
【０１３１】
受信装置２０の第三受信制御部２１３は、送受信部２１１を介して、ｎ組の暗号化第一コンテンツデータとコンテンツ鍵識別子（ＣＫＩＤ＿１、ＥＣＮＴ１＿１）、（ＣＫＩＤ＿２、ＥＣＮＴ１＿２）、…、（ＣＫＩＤ＿ｎ、ＥＣＮＴ１＿ｎ）を受信すると、ｎ組の暗号化第一コンテンツデータとコンテンツ鍵識別子とを、暗号化コンテンツ選択部２０７へ出力する。
【０１３２】
暗号化コンテンツ選択部２０７は、選択情報保持部２０５から取得した選択コンテンツ

鍵識別子ＳＣＫＩＤと一致するコンテンツ鍵識別子を選択し（ステップＳ２５０）、選択コンテンツ鍵識別子ＳＣＫＩＤと、対応する暗号化第一コンテンツデータＳＥＣＮＴ１とを、第三受信制御部２１３へ出力する。

第三受信制御部２１３は、１組のコンテンツ鍵識別子ＳＣＫＩＤと暗号化第一コンテンツデータＳＥＣＮＴ１とを取得すると、復号コンテンツ鍵保持部２０２から、復号コンテンツ鍵ＤＣＫを取得する（ステップＳ２５１）。

【０１３３】

第三受信制御部２１３は、暗号処理部２１２へ、コンテンツ復号化要求ＡＥＳＤと、暗号化第一コンテンツデータＳＥＣＮＴ１と、復号コンテンツ鍵識別子ＤＣＫとを出力する。

暗号処理部２１２は、復号コンテンツ鍵ＤＣＫを復号鍵として用い、暗号化第一コンテンツデータＳＥＣＮＴ１を復号して、復号コンテンツデータＤＣＮＴを生成する（ステップＳ２５２）。暗号処理部２１２は、復号コンテンツデータＤＣＮＴを、第三受信制御部２１３へ出力する。

【０１３４】

第三受信制御部２１３は、暗号処理部２１２から復号化コンテンツデータＤＣＮＴを取得すると、復号化コンテンツデータＤＣＮＴを、第二コンテンツデータＣＮＴ２として、第二コンテンツデータ保持部２０８へ格納する（ステップＳ２５３）。

３．コンテンツ流出元特定処理の動作

図２３及び図２４は、コンテンツ流出元特定処理の動作を示すフローチャートである。なお、ここに示す動作は、図１９のステップＳ１０２の詳細である。

【０１３５】

コンテンツデータ入力部３０５は、記録媒体４０からコンテンツデータを読み出し（ステップＳ３０１）、読み出したコンテンツデータを、追跡コンテンツデータＴＣＮＴとして、追跡コンテンツデータ保持部３０６に格納する（ステップＳ３０２）。そして、コンテンツデータ入力部３０５は、透かし情報抽出部３０１へ透かし情報抽出要求を出力する。

【０１３６】

透かし情報抽出部３０１は、コンテンツデータ入力部３０５から、透かし情報抽出要求が入力されると、追跡コンテンツデータ保持部３０６から、追跡コンテンツデータＴＣＮＴを取得する。

そして、透かし情報抽出部３０１は、追跡コンテンツデータＴＣＮＴに埋め込まれている電子透かしの抽出を行い、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫを取得する（ステップＳ３０３）。透かし情報抽出部３０１は、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫを、証拠検証部３０２へ出力する。

【０１３７】

証拠検証部３０２は、透かし情報抽出部３０１から、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫが入力されると、暗号処理部３０７へ、転送先装置識別子ＩＤ＿２、証拠情報ＥＶ、及びＲＳＡ復号処理要求ＲＳＡＤを出力する。

暗号処理部３０７は、暗号鍵保持部３０８から、転送先装置識別子ＩＤ＿２に対応する鍵情報ＳＫ＿２（ｎ２、ｄ２）を取得し（ステップＳ３０４）、証拠情報ＥＶを復号する（ステップＳ３０５）。証拠検証部３０２は、暗号処理部３０７から、証拠情報ＥＶを復号した結果である復号化証拠情報ＤＥＶを取得する（ステップＳ３０６）。

【０１３８】

次に、証拠検証部３０２は、暗号処理部３０７へ、ハッシュ値計算要求ＨＡＳＨと復号化証拠情報ＤＥＶとを出力する。

暗号処理部３０７は、復号化証拠情報ＤＥＶのハッシュ値を算出し（ステップＳ３０７）、算出された復号化証拠情報ハッシュ値ＨＤＥＶを、証拠検証部３０２へ出力する。

そして、証拠検証部３０２は、復号化証拠情報ハッシュ値ＨＤＥＶとコンテンツ鍵ハッシュＨＣＫとの値が等しいか否か比較する（ステップＳ３０８）。

【０１３９】

復号化証拠情報ハッシュ値ＨＤＥＶとコンテンツ鍵ハッシュＨＣＫ値とが異なる場合（ステップＳ３０８でＮＯ）、証拠検証部３０２は、証拠正当フラグＦＬＡＧに「０」を設定する（ステップＳ３０９）。

復号化証拠情報ハッシュ値ＨＤＥＶとコンテンツ鍵ハッシュＨＣＫ値とが等しい場合（ステップＳ３０８でＹＥＳ）、証拠検証部３０２は、証拠正当フラグＦＬＡＧに「１」を設定する（ステップＳ３１０）。

【０１４０】

その後、証拠検証部３０２は、転送元装置識別子ＩＤ＿１、転送先装置識別子ＩＤ＿２、及び証拠正当フラグＦＬＡＧを、流出元判定部３０３へ出力する。

流出元判定部３０３は、証拠検証部３０２から、ＩＤ＿１、ＩＤ＿２、及び証拠正当フラグの値を取得する（ステップＳ３１１）。

流出元判定部３０３は、証拠正当フラグの値を判断する（ステップＳ３１２）。

【０１４１】

証拠正当フラグの値が０の場合（ステップＳ３１２で「０」）、流出元判定部３０３は、転送元装置識別子ＩＤ＿１を、流出元装置識別子として流出元出力部３０４へ出力する（ステップＳ３１３）。

証拠正当フラグの値が１の場合（ステップＳ３１２で「１」）、流出元判定部３０３は、転送先装置識別子ＩＤ＿２を、流出元装置識別子として流出元出力部３０４へ出力する（ステップＳ３１４）。

【０１４２】

流出元出力部３０４は、流出元判定部３０３から流出元装置識別子を受け取ると、受け取った流出元装置識別子を、ディスプレイに表示する（ステップＳ３１５）。

＜第１の実施形態の効果＞

ここでは、第１の実施形態の効果について述べる。

（ａ）先ず、第１の実施形態においては、受信装置２０は、送信装置１０が生成した複数個のコンテンツ鍵のうち、何れを取得したのか送信装置１０に知られることなく、１個のコンテンツ鍵を取得することが可能となる。その理由を以下に示す。

【０１４３】

送信装置１０は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのそれぞれを、ＲＳＡアルゴリズムを用いて、送信装置１０の暗号鍵ｅ１で暗号化する。これにより、ｎ個の暗号化第一コンテンツ鍵は、それぞれ、ＣＫ＿１＾ｅ１（ｍｏｄ　ｎ１）、ＣＫ＿２＾ｅ１（ｍｏｄ　ｎ１）、…、ＣＫ＿ｎ＾ｅ１（ｍｏｄ　ｎ１）となる。そして、ｎ個の第一暗号化コンテンツ鍵は、受信装置２０へ送付される。

【０１４４】

受信装置２０は、ｎ個の第一暗号化コンテンツ鍵から１個の第一暗号化コンテンツ鍵ＣＫ＿ｓ＾ｅ１（ｍｏｄ　ｎ１）（ｓ＝１、２、…、ｎの何れか）を選択し、ＲＳＡアルゴリズムを用いて、受信装置２０の暗号化鍵ｅ２で暗号化する。これにより、第二暗号化コンテンツ鍵は、ＣＫ＿ｓ＾（ｅ１×ｅ２）（ｍｏｄ　ｎ２）となる。そして、第二暗号化コンテンツ鍵をＣＫ＿ｓ＾（ｅ１×ｅ２）（ｍｏｄ　ｎ２）、送信装置１０へ送付する。

【０１４５】

送信装置１０は、受信装置２０の公開鍵を保持していないため、受け取った第二暗号化コンテンツ鍵を復号することが出来ず、受信装置２０が、どの第一暗号化コンテンツ鍵を選択したのか判断することが出来ない。これが、送信装置１０は、受信装置２０の取得するコンテンツデータを特定出来ない根拠である。

そして、送信装置１０は、第二暗号化コンテンツ鍵ＣＫ＿ｓ＾（ｅ１×ｅ２）（ｍｏｄ　ｎ２）を、送信装置１０の復号鍵ｄ１で復号する。

【０１４６】

これにより、第三暗号化コンテンツ鍵は、
ＣＫ＿ｓ＾（ｅ１×ｅ２×ｄ１）（ｍｏｄ　ｎ１）となる。
ここで、ｎ１は、二つの素数ｐ１、ｑ１の積ｐ１×ｑ１であり、ｅ１とｄ１は、条件式ｅ１×ｄ１＝１（ｍｏｄ　Ｌ）を満たすように生成されている。なお、Ｌは、ｐ１－１とｑ１－１との最小公倍数である。

【０１４７】

従って、第三暗号化コンテンツ鍵は、
ＣＫ＿ｓ＾（ｅ１×ｅ２×ｄ１）＝ＣＫ＿ｓ＾（１×ｅ２）（ｍｏｄ　ｎ１）＝ＣＫ＿ｓ＾ｅ２（ｍｏｄ　ｎ１）となる。
そして、送信装置１０は、第三暗号化コンテンツ鍵ＣＫ＿ｓ＾ｅ２（ｍｏｄ　ｎ１）を受信装置２０へ送付する。

【０１４８】

受信装置２０は、受け取った第三暗号化コンテンツ鍵ＣＫ＿ｓ＾ｅ２（ｍｏｄ　ｎ１）を、受信装置２０の復号鍵ｄ２で復号する。
これにより、復号コンテンツ鍵ＤＣＫは、
ＣＫ＿ｓ＾（ｅ２×ｄ２）（ｍｏｄ　ｎ２）となる。
ここで、先程と同様に、ｎ２は、二つの素数ｐ２、ｑ２の積ｐ２×ｑ２であり、ｅ２とｄ２は、条件式ｅ２×ｄ２＝１（ｍｏｄ　Ｌ）を満たすように生成されている。なお、Ｌは、ｐ２－１とｑ２－１との最小公倍数である。

【０１４９】

従って、復号コンテンツ鍵ＤＣＫは、
ＤＣＫ＝ＣＫ＿ｓ＾（ｅ２×ｄ２）＝ＣＫ＿ｓ＾１＝ＣＫ＿ｓ（ｍｏｄ　ｎ２）となる。
以上のことから、受信装置２０は、送信装置１０に知られることなく、送信装置１０が生成したコンテンツ鍵ＣＫ＿ｓを取得することが出来る。

【０１５０】

（ｂ）続いて、第１の実施形態においては、海賊版コンテンツから、流出元装置を特定することが出来る。その理由を以下に示す。
ここでは先ず、仮に、コンテンツの転送元である送信装置１０が不正端末である場合を考える。この場合、送信装置１０は、コンテンツの転送先である受信装置２０が受け取った電子透かし入りのコンテンツデータを特定して、そのコンテンツデータを海賊版コンテンツとして外部に流出することが出来れば、受信装置２０へ罪を擦り付けることが可能となる。

【０１５１】

しかし、上述したように、送信装置１０は、受信装置２０がどのコンテンツ鍵を選択して、どの電子透かし入りのコンテンツデータを取得したのか、知ることが出来ない。これにより、送信装置１０は、受信装置２０が取得した電子透かし入りのコンテンツを特定することが出来ない。
また、第１の実施形態では、コンテンツデータに含まれる電子透かしを抽出することにより、受信装置２０が受け取ったコンテンツデータであるか否かを判断することが出来る。

【０１５２】

これらにより、送信装置１０は、複数個に複製し、それぞれに異なる電子透かしを埋め込んだコンテンツデータのうち、何れかを適当に選択して外部に流出したとしても、そのコンテンツデータが、受信装置２０が受け取っていないコンテンツデータである確率が高いため、不正を行ったと判断される。
次に、仮に、コンテンツの転送先である受信装置２０が不正端末である場合を考える。第１の実施形態においては、受信装置２０は、自機が取得したことを示す証拠が電子透かしとして埋め込まれているコンテンツデータしか入手することが出来ない。

【０１５３】

従って、受信装置２０は、取得した電子透かし入りのコンテンツを外部に流出したとしても、それは、受信装置２０が取得したコンテンツデータであると判断され、不正を行ったと判断される。

（ｃ）以上のことから、第１の実施形態では、コンテンツの転送元である送信装置１０が不正端末である場合であっても、コンテンツの転送先である受信装置２０が不正端末である場合であっても、コンテンツの流出元を特定することが出来る。

≪第２の実施形態≫

本発明の第２の実施形態について説明する。

＜概要＞

第１の実施形態では、ＲＳＡ暗号を用いて、コンテンツの流出元を特定することができるコンテンツ送受信処理を実現していたが、第２の実施形態では、ＲＳＡ暗号に限定されず、ＥｌＧａｍａｌ暗号や楕円曲線暗号など、任意の公開鍵暗号アルゴリズムを用いて、コンテンツの流出元を特定することができるコンテンツ送受信処理を実現することが可能となる。

＜構成＞

第２の実施形態は、図１に示したコンテンツ配信システム１と同様のシステム構成を有する。即ち、第２の実施形態は、放送局装置、送信装置、受信装置、コンテンツ流出元特定装置、及び記録媒体から構成される。各装置の内部構成は、第１の実施形態における送信装置１０、受信装置２０、コンテンツ流出元特定装置３０と同様である。

【０１５４】

第２の実施形態では、送信装置は、任意の公開鍵暗号アルゴリズムの公開鍵ＰＫ１及び秘密鍵ＳＫ１を保持しており、受信装置は、送信装置と同じ公開鍵暗号アルゴリズムの公開鍵ＰＫ２及び秘密鍵ＳＫ２を保持しているものとする。また、コンテンツ流出元端末装置は、送信装置の公開鍵ＰＫ１及び秘密鍵ＳＫ１、並びに、受信装置の公開鍵ＰＫ２及び秘密鍵ＳＫ２を保持しているものとする。

＜動作＞

ここでは、図２５から図２８に示すフローチャートを用いて、第２の実施形態の動作について説明する。

【０１５５】

１．システム全体の動作

第２の実施形態の全体の動作は、図１９に示した第１の実施形態の動作と同様であるため、説明を省略する。

２．コンテンツ送受信処理の動作

第２の実施形態におけるコンテンツ送受信処理の動作は、その一部が、第１の実施形態と同様である。具体的には、第２の実施形態は、ステップ２０１からステップＳ２０６まで、及び、ステップＳ２４１からステップＳ２５３まで、第１の実施形態と同様の処理を行う。

【０１５６】

第２の実施形態は、送信装置及び受信装置によるコンテンツ鍵の送受信処理が、第１の実施形態とは異なるので、以下では、図２５及び図２６に示すフローチャートを用いて、第１実施形態と異なる部分について説明する。

先ず、送信装置は、１２８ビットのｎ個の乱数ｒ１、ｒ２、…、ｒｎを生成する（ステップＳ４０１）。

【０１５７】

送信装置は、生成したｎ個の乱数ｒ１、ｒ２、…、ｒｎと、送信装置の公開鍵ＰＫ１とを受信装置へ送信し、受信装置は、ｎ個の乱数ｒ１、ｒ２、…、ｒｎと、送信装置の公開鍵ＰＫ１とを受信する（ステップＳ４０２）。

受信装置は、受信したｎ個の乱数のうち、１つをランダムに選択する（ステップＳ４０２）。ここでは、選択した乱数をｒｓ（ｓ＝１、２、…、ｎの何れか）とする。

【０１５８】

次に、受信装置は、１２８ビットの復号コンテンツ鍵ＤＣＫを生成し（ステップＳ４０４）、生成した復号コンテンツ鍵ＤＣＫを、ステップＳ４０２で受信した送信装置の公開鍵ＰＫ１を暗号鍵として用い、暗号化する（ステップＳ４０５）。ここでは、復号コンテンツ鍵ＤＣＫの暗号文を、Ｃ１＝Ｅｎｃ（ＰＫ１、ＤＣＫ）とする。ここでＥｎｃ（Ｋ、Ｍ）は、暗号鍵Ｋを用い、平文Ｍを暗号化した際の暗号文とする。

【０１５９】

続いて、受信装置は、Ｃ１に、ステップＳ４０３で選択した乱数ｒｓを足し合わせ、Ｃ２＝Ｅｎｃ（ＰＫ１，ＤＣＫ）＋ｒｓを生成する（ステップＳ４０６）。

次に、受信装置は、１２８ビットの乱数Ｐを生成し（ステップＳ４０７）、復号コンテンツ鍵ＤＣＫ、乱数ｒｓ、及び乱数Ｐを連結する（ステップＳ４０８）。ここでは、連結した値を、ＤＣＫ‖ｒｓ‖Ｐと表す。

【０１６０】

そして、受信装置は、自機の公開鍵ＰＫ２を暗号鍵として用い、ＤＣＫ‖ｒｓ‖Ｐを暗号化し、Ｅ＝Ｅｎｃ（ＰＫ２、ＤＣＫ‖ｒｓ‖Ｐ）を生成する（ステップＳ４０９）。

その後、受信装置は、自機の秘密鍵ＳＫ２を署名生成鍵として用い、暗号文Ｃ２と暗号文Ｅとを連結した値であるＣ２‖Ｅに対し、デジタル署名Ｓ＝Ｇｅｎ（ＳＫ２、Ｃ２‖Ｅ）を生成する（ステップＳ４１０）。ここで、Ｇｅｎ（Ｋ，Ｍ）は、署名生成鍵Ｋを用いて、メッセージＭに対して生成されたデジタル署名であるとする。デジタル署名を作成する技術については、既に公知であるので説明は省略する。

【０１６１】

受信装置は、Ｃ２、Ｅ、Ｓ、及び公開鍵ＰＫ２を、送信装置へ送信し、送信装置は、Ｃ２、Ｅ、Ｓ、及び公開鍵ＰＫ２を受信する（ステップＳ４１１）。

送信装置は、受信装置の公開鍵ＰＫ２を署名検証鍵として用い、デジタル署名Ｓが、Ｃ２‖Ｅに対する正規の署名であるか否かを検証する（ステップＳ４１２）。

検証の結果、デジタル署名Ｓが、受信装置が発行した正しいデジタル署名でないと判断された場合（ステップＳ４１３でＮＯ）、送信装置は、受信装置へのコンテンツ転送処理を終了する。

【０１６２】

検証の結果、デジタル署名Ｓが、受信装置が発行した正しいデジタル署名であると判断された場合（ステップＳ４１３でＹＥＳ）、送信装置は、値Ｃ、値Ｅ、及びデジタル署名Ｓを、証拠情報ＥＶとして、証拠情報保持部へ格納する（ステップＳ４１４）。即ち、第２の実施形態では、証拠情報ＥＶの値が、第１の実施形態とは異なる。

次に、送信装置は、値Ｃ２をｎ個に複製し、それらをＣ２＿１、Ｃ２＿２、…、Ｃ２＿ｎとする（ステップＳ４１５）。

【０１６３】

続いて、送信装置は、ｉ＝１、２、…、ｎについて、ステップＳ４１６からステップＳ４１９までを繰り返す。

先ず、送信装置は、Ｃ２＿ｉから、ステップＳ４０１で生成した乱数ｒｉの値を減算し、Ｃ３＿ｉ＝Ｃ２＿ｉ－ｒｉを生成する（ステップＳ４１７）。次に、送信装置は、Ｃ３＿ｉを自機の秘密鍵ＳＫ１を復号鍵として用い復号し、ＣＫ＿ｉ＝Ｄｅｃ（ＳＫｉ、Ｃ３＿ｉ）を生成する（ステップＳ４１８）。ここで、Ｄｅｃ（Ｋ、Ｃ）は、復号化鍵Ｋを用い、暗号文Ｃを復号した際の復号文とする。

【０１６４】

そして、送信装置は、ｎ個の値ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎをコンテンツ鍵として、コンテンツ鍵保持部へ格納する（ステップＳ４２０）。

以上により、第２の実施形態における送信装置と受信装置とによるコンテンツ鍵の送受信処理を終了し、以後は、第１の実施形態のステップＳ２４１へ続く。

３．コンテンツ流出元特定処理の動作

第２の実施形態におけるコンテンツ流出元特定処理の動作は、その一部が、第１の実施形態と同様である。具体的には、第２の実施形態は、ステップ３０１からステップＳ３０

２まで、及び、ステップＳ３１１からステップＳ３１５まで、第１の実施形態と同様の処理を行う。

【０１６５】

以下では、図２７及び図２８に示すフローチャートを用いて、第１の実施形態と異なる部分について説明する。

先ず、証拠検証部は、透かし情報抽出部から転送元装置識別子ＩＤ＿１、転送先装置識別子ＴＩＤ＿２、証拠情報ＥＶ、及びコンテンツ鍵ハッシュＨＣＫが入力されると、証拠情報ＥＶに含まれる値Ｃと値Ｅとデジタル署名Ｓを取得する（ステップＳ５０１）。

【０１６６】

次に、証拠検証部は、暗号鍵保持部から、転送先装置識別子ＩＤ＿２に対応する公開鍵ＰＫ２を取得する（ステップＳ５０２）。そして、証拠検証部は、ＰＫ２を用いて、デジタル署名Ｓが、値Ｃ‖Ｅの正規の署名であるか否かを検証する（ステップＳ５０３）。

検証の結果、デジタル署名Ｓが、正しいデジタル署名でないと判断された場合（ステップＳ５０４でＮＯ）、証拠検証部は、証拠正当フラグＦＬＡＧに「０」を設定し（ステップ５０５）、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＩＤ＿２と、証拠正当フラグＦＬＡＧとを、流出元判定部へ出力する。

【０１６７】

検証の結果、デジタル署名Ｓが、正しいデジタル署名であると判断された場合（ステップＳ５０４でＹＥＳ）、証拠検証部は、値Ｅを復号するために、暗号処理部へ転送先装置識別子ＩＤ＿２と、証拠情報ＥＶに含まれる値Ｅと、復号処理要求を出力する。暗号処理部は、受信装置の秘密鍵ＳＫ２を用いて、値Ｅを復号し、ＤＣＫ‖ｒｓ‖Ｐを取得する（ステップＳ５０６）。

【０１６８】

次に、暗号処理部は、送信装置の公開鍵ＰＫ１を用いてＤＣＫを暗号化し、その値に、ｒｓを足し合わせ、Ｅｎｃ（ＰＫ１、ＤＣＫ）＋ｒｓを生成する（ステップＳ５０７）。暗号処理部は、生成したＥｎｃ（ＰＫ１、ＤＣＫ）＋ｒｓを、証拠検証部へ出力する。

証拠検証部は、暗号処理部からＥｎｃ（ＰＫ１、ＤＣＫ）＋ｒｓを受け取ると、　その値と値Ｃ２とが一致するか否か確認する。

【０１６９】

Ｅｎｃ（ＰＫ１、ＤＣＫ）＋ｒｓの値と値Ｃ２とが一致しない場合（ステップＳ５０８でＮＯ）、証拠検証部は、証拠正当フラグＦＬＡＧに「１」を設定し（ステップ５０９）、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＩＤ＿２と、証拠正当フラグＦＬＡＧとを、流出元判定部へ出力する。

一方、Ｅｎｃ（ＰＫ１、ＤＣＫ）＋ｒｓの値と値Ｃ２とが一致する場合（ステップＳ５０８でＹＥＳ）、証拠検証部は、ＤＣＫのハッシュ値を計算するために、ハッシュ値計算要求ＨＡＳＨとＤＣＫとを、暗号処理部へ出力する。

【０１７０】

暗号処理部は、ＤＣＫのハッシュ値である証拠情報ハッシュ値ＨＫを算出し（ステップＳ５１０）、算出した証拠情報ハッシュ値ＨＫを、証拠検証部へ出力する。

そして、証拠検証部は、証拠情報ハッシュ値ＨＫとコンテンツ鍵ハッシュＨＣＫが等しい否か比較する。

証拠情報ハッシュ値ＨＫとコンテンツ鍵ハッシュＨＣＫが異なる場合（ステップＳ５１１でＮＯ）、証拠検証部は、証拠正当フラグＦＬＡＧに「０」を設定し（ステップＳ５１２）、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＩＤ＿２と、証拠正当フラグＦＬＡＧとを、流出元判定部へ出力する。

【０１７１】

証拠情報ハッシュ値ＨＫとコンテンツ鍵ハッシュＨＣＫが等しい場合（ステップＳ５１１でＹＥＳ）、証拠検証部は、証拠正当フラグＦＬＡＧに「１」を設定し（ステップＳ５１３）、転送元装置識別子ＩＤ＿１と、転送先装置識別子ＩＤ＿２と、証拠正当フラグＦＬＡＧとを、流出元判定部へ出力する。

以後、第１の実施形態のステップＳ３１１へ続く。
＜第２の実施形態の効果＞
ここでは、第２の実施形態の効果について述べる。
【０１７２】
（ａ）第２の実施形態においては、送信装置は、受信装置が取得するコンテンツを特定することが出来ない。その理由を以下に示す。
先ず、送信装置は、ｎ個の乱数ｒ１、ｒ２、…、ｒｎと、自機の公開鍵ＰＫ１とを受信装置へ送信する。
受信装置は、自機において、復号コンテンツ鍵ＤＣＫを生成する。そして、送信装置の公開鍵ＰＫ１を用いて、復号コンテンツ鍵ＤＣＫを暗号化し、暗号化した値をＣ１＝Ｅｎｃ（ＰＫ１、ＤＣＫ）とする。その後、受信装置は、ｎ個の乱数ｒ１、ｒ２、…、ｒｎのうち一つの乱数ｒｓ（ｓ＝１、２、…、ｎの何れか）を選択し、選択した乱数ｒｓの値を、Ｃ１に足し合わせる。足し合わせた値をＣ２＝Ｃ１＋ｒｓとする。
【０１７３】
そして、受信装置は、値Ｃ２と受信装置の公開鍵ＰＫ２とを、送信装置へ送信する。ここでは、値Ｅとデジタル署名Ｓとについては述べない。
送信装置は、値Ｃ２と受信装置の公開鍵ＰＫ２とを受け取るが、復号コンテンツ鍵ＤＣＫの値を知らないため、受け取った値Ｃ２から、受信装置がどの乱数を選択したのか判断することが出来ない。
【０１７４】
そこで、送信装置は、受信装置がどの乱数を選択した場合であっても、１個のコンテンツを利用できるように、全ての乱数ｒ１、ｒ２、…、ｒｎを用いて、値Ｃ２から各乱数を減算する。その結果を、Ｃ３＿１＝Ｃ２＿１－ｒ１、Ｃ３＿２＝Ｃ２＿２－ｒ２、…、Ｃ３＿ｎ＝Ｃ２＿ｎ－ｒｎとする。これにより、値Ｃ３の内の何れか一つは、受信装置が選択した乱数ｒｓの値と一致する。
【０１７５】
その後、送信装置は、自機の秘密鍵ＳＫ１を用いて、値Ｃ３＿１、Ｃ３＿２、…、Ｃ３＿ｎを復号し、ＣＫ＿１＝Ｄｅｃ（ＳＫ１、Ｃ３＿１）、ＣＫ＿２＝Ｄｅｃ（ＳＫ１、Ｃ３＿２）、…、ＣＫ＿ｎ＝Ｄｅｃ（ＳＫ１、Ｃ３＿ｎ）を生成する。
これにより、ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎの内、何れか一つは受信装置が生成した復号コンテンツ鍵ＤＣＫの値と一致するが、送信装置は、どれが復号コンテンツ鍵ＤＣＫと一致するのかを判断することは出来ない。
【０１７６】
そして、送信装置は、コンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを用いて、異なる透かしを埋め込んだｎ個のコンテンツデータを暗号化し、ｎ個の暗号化コンテンツデータを生成する。
受信装置は、送信装置からｎ個の暗号化コンテンツデータを受信すると、復号コンテンツ鍵ＤＣＫを用い、何れのコンテンツデータを取得したのか送信装置に知られることなく、１個のコンテンツデータを取得することが出来る。
【０１７７】
（ｂ）第２の実施形態においては、海賊版コンテンツから、流出元装置を特定することが出来る。その理由を以下に示す。
基本的には、第１の実施形態と同様であるが、第２の実施形態では、第１の実施形態と異なり、証拠情報ＥＶに受信装置のデジタル署名Ｓが含まれている。
デジタル署名Ｓを含める理由は、受信装置が、値Ｃ２及び値Ｅを偽造する不正行為を防止するためである。
【０１７８】
より具体的に説明すると、受信装置は、真の復号コンテンツ鍵ＤＣＫではない値を、ＰＫ２を用いて暗号化し、値Ｃ２及び値Ｅを生成したとする。受信装置がこのような不正行為を行った上で、海賊版コンテンツを作成した場合、コンテンツ流出元特定装置は、海賊

版コンテンツの流出元を、送信装置であると誤判定してしまう。
そこで、第２の実施形態では、このような受信装置の不正行為を想定した上で、Ｃ２‖Ｅに対して、デジタル署名Ｓを付加することにより、コンテンツ流出元特定装置が、海賊版コンテンツの流出元を正しく判定することが出来るようになる。
【０１７９】
（ｃ）以上のことから、第２の実施形態では、第１の実施形態と同様に、コンテンツの転送元である送信装置が不正端末である場合であっても、コンテンツの転送先である受信装置が不正端末である場合であっても、コンテンツの流出元を特定することが出来る。
≪第３の実施形態≫
本発明の第３の実施形態について説明する。
＜概要＞
第１の実施形態では、ＲＳＡ暗号を用いて、コンテンツの流出元を特定することができるコンテンツ送受信処理を実現していた。
【０１８０】
第２の実施形態では、ＲＳＡ暗号に限定されず、ＥｌＧａｍａｌ暗号や楕円曲線暗号など、任意の公開鍵暗号アルゴリズムで、第１の実施形態と同様のシステムを実現することが可能となった。ここで、第２の実施形態では、送信装置が、乱数を生成しなければならなかったが、第３の実施形態では、送信装置が、乱数を生成する必要がないシステムを開示する。
＜構成＞
第３の実施形態は、図１に示したコンテンツ配信システム１と同様のシステム構成を有する。即ち、第３の実施形態は、放送局装置、送信装置、受信装置、コンテンツ流出元特定装置、及び記録媒体から構成される。各装置の内部構成は、第１の実施形態における送信装置１０、受信装置２０、コンテンツ流出元特定装置３０と同様である。
【０１８１】
第３の実施形態では、送信装置は、ｎ個の公開鍵ＰＫ１＿１、ＰＫ１＿２、…、ＰＫ１＿ｎ、と、各公開鍵に対応するｎ個の秘密鍵ＳＫ１＿１、ＳＫ１＿２、…、ＳＫ１＿ｎとを、インデックス情報ＩＤ＿ｓに対応付けて保持しているものとする。また、受信装置は、公開鍵ＰＫ２と秘密鍵ＳＫ２とを保持しているものとする。
ここで、送信装置と受信装置とが用いる公開鍵暗号アルゴリズムは、ＲＳＡ暗号、ＥｌＧａｍａｌ暗号、楕円曲線暗号など、任意のアルゴリズムでよい。
＜動作＞
第３の実施形態の全体の動作は、図１９に示した第１の実施形態の動作と同様であるため、説明を省略する。
【０１８２】
また、第３の実施形態におけるコンテンツ流出元特定処理の動作は、図２７及び図２８に示した第２の実施形態の動作と同様であるため、説明を省略する。
第３の実施形態におけるコンテンツ送受信処理の動作は、その一部が、第１の実施形態と同様である。具体的には、第３の実施形態は、ステップ２０１からステップＳ２０６まで、及び、ステップＳ２４１からステップＳ２５３まで、第１の実施形態と同様の処理を行う。
【０１８３】
第３の実施形態は、送信装置及び受信装置によるコンテンツ鍵の送受信処理が、第１の実施形態とは異なるので、以下では、図２９及び図３０に示すフローチャートを用いて、第１実施形態と異なる部分について説明する。
送信装置は、自機が保持するｎ個の公開鍵ＰＫ１＿１、ＰＫ１＿２、…、ＰＫ１＿ｎを読み出し（ステップＳ６０１）、読み出したｎ個の公開鍵を、受信装置へ送信し、受信装置は、ｎ個の公開鍵を受信する（ステップＳ６０２）。
【０１８４】
受信装置は、受信したｎ個の公開鍵のうち、１つをランダムに選択する。ここでは、選

択した公開鍵をＰＫ１＿ｓ（ｓ＝１、２、…、ｎの何れか）とする（ステップＳ６０３）。

次に、受信装置は、１２８ビットの復号コンテンツ鍵ＤＣＫを生成する（ステップＳ６０４）。そして、受信装置は、復号コンテンツ鍵ＤＣＫを、ステップＳ６０３で選択した送信装置の公開鍵ＰＫ１＿ｓを用いて暗号化し、Ｃ１＝Ｅｎｃ（ＰＫ１＿ｓ、ＤＣＫ）を生成する（ステップＳ６０５）。

【０１８５】

次に、受信装置は、１２８ビットの乱数Ｐを生成し（ステップＳ６０６）、復号コンテンツ鍵ＤＣＫと、ステップＳ６０３で選択した公開鍵のインデックス情報ＩＤ＿ｓと、乱数Ｐとを連結し、ＤＣＫ‖ＩＤ＿ｓ‖Ｐを生成する（ステップＳ６０７）。

そして、受信装置は、自機の公開鍵ＰＫ２を用いて、ＤＣＫ‖ＩＤ＿ｓ‖Ｐを暗号化し、Ｅ＝Ｅｎｃ（ＰＫ２、ＤＣＫ‖ＩＤ＿ｓ‖Ｐ）を生成する（ステップＳ６０８）。

【０１８６】

次に、受信装置は、自機の秘密鍵ＳＫ２を署名生成鍵として用いて、値Ｃ１と値Ｅに対するデジタル署名Ｓ＝Ｇｅｎ（ＳＫ２、Ｃ１‖Ｅ）を作成する（ステップＳ６０９）。

受信装置は、値Ｃ１、値Ｅ、デジタル署名Ｓ、及び公開鍵ＰＫ２を送信装置へ送信し、送信装置は、値Ｃ１、値Ｅ、デジタル署名Ｓ、及び公開鍵ＰＫ２を受信する（ステップＳ６１０）。

【０１８７】

送信装置は、受信装置の公開鍵ＰＫ２を署名検証鍵として用い、デジタル署名Ｓが、Ｃ１‖Ｅに対する正規の署名であるか否かを検証する（ステップＳ６１１）。

検証の結果、デジタル署名Ｓは、受信装置が発行した正しいデジタル署名でないと判断された場合（ステップＳ６１２でＮＯ）、送信装置は、受信装置へのコンテンツ転送処理を終了する。

【０１８８】

検証の結果、デジタル署名Ｓは、受信装置が発行した正しいデジタル署名であると判断された場合（ステップＳ６１２でＹＥＳ）、送信装置は、値Ｃ１、値Ｅ、及びデジタル署名Ｓを、証拠情報ＥＶとして、証拠情報保持部へ格納する（ステップＳ６１３）。即ち、第３の実施形態では、証拠情報ＥＶの値が、第１の実施形態と異なる。

次に、送信装置は、値Ｃ１を複製し、Ｃ１＿１、Ｃ１＿２、…、Ｃ１＿ｎを生成する（ステップＳ６１４）。続いて、送信装置は、ｉ＝１、２、…、ｎについて、ステップＳ６１５からステップＳ６１７までを繰り返す。

【０１８９】

先ず、送信装置は、Ｃ１＿ｉを、自機の秘密鍵ＳＫ１＿ｉを用いて復号し、ＣＫ＿ｉ＝Ｄｅｃ（ＳＫ１＿ｉ、Ｃ１＿ｉ）を生成する（ステップＳ６１６）。

送信装置は、生成したｎ個の値ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを、コンテンツ鍵として、コンテンツ鍵保持部へ格納する（ステップＳ６１８）。

以上により、第３の実施形態における送信装置と受信装置によるコンテンツ鍵の送受信処理を終了し、以後は、第１の実施形態のステップＳ２４１へ続く。

＜第３の実施形態の効果＞

ここでは、第３の実施形態の効果について述べる。

【０１９０】

（ａ）第３の実施形態においては、送信装置は、受信装置が取得するコンテンツを特定することが出来ない。その理由を以下に示す。

送信装置は、ｎ個の公開鍵ＰＫ１＿１、ＰＫ１＿２、…、ＰＫ１＿ｎを受信装置へ送信する。一方、受信装置は、自機において、復号コンテンツ鍵ＤＣＫを生成する。そして、受信装置は、送信装置のｎ個の公開鍵のうち、一つの公開鍵ＰＫ１＿ｓ（ｓ＝１、２、…、ｎの何れか）を用いて、復号コンテンツ鍵ＤＣＫを暗号化する。ここで、暗号化した値をＣ１＝Ｅｎｃ（ＰＫ１＿ｓ、ＤＣＫ）とする。そして、受信装置は、値Ｃ１と、自機の公開鍵ＰＫ２とを、送信装置へ送信する。なお、受信装置は、Ｃ１及びＰＫ２に加えて、

値Ｅとデジタル署名Ｓとを送信装置へ送信するが、ここでは、それらについては述べない。

【０１９１】

送信装置は、受信装置から値Ｃ１と公開鍵ＰＫ２とを受信する。ここで送信装置は、受信装置が生成した復号コンテンツ鍵ＤＣＫの値を知らないため、値Ｃ１から、受信装置がｎ個の公開鍵のうちの、何れの公開鍵を選択したのか、判断することが出来ない。

そこで、送信装置は、受信装置が、ｎ個の公開鍵ＰＫ１＿１、ＰＫ１＿２、…、ＰＫ１＿ｎの内、どの公開鍵を選択した場合であっても、１個のコンテンツを利用できるように、全ての秘密鍵ＳＫ１＿１、ＳＫ１＿２、…、ＳＫ１＿ｎを用いて、値Ｃ１を復号し、ＣＫ＿１＝Ｄｅｃ（ＳＫ１＿１、Ｃ１）、ＣＫ＿２＝Ｄｅｃ（ＳＫ１＿２、Ｃ１）、…、ＣＫ＿ｎ＝Ｄｅｃ（ＳＫ１＿ｎ、Ｃ１）を生成する。

【０１９２】

これにより、送信装置が生成したＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのうち、何れか一つは、受信装置が生成した復号コンテンツ鍵ＤＣＫと一致する。

そして、送信装置は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを用いて、異なる透かしを埋め込んだｎ個のコンテンツデータをそれぞれ暗号化して、ｎ個の暗号化コンテンツデータを生成する。

【０１９３】

受信装置は、送信装置からｎ個の暗号化コンテンツデータを受信すると、復号コンテンツ鍵ＤＣＫを用い、何れのコンテンツデータを取得したのか送信装置に知られることなく、１個のコンテンツデータを取得することが出来る。

（ｂ）第３の実施形態においては、第２の実施形態と同様に、証拠情報ＥＶに受信装置のデジタル署名Ｓが含まれているため、第２の実施形態の効果で説明したように、コンテンツ流出元特定装置が、海賊版コンテンツの流出元を正しく判定することが出来る。

【０１９４】

（ｃ）以上のことから、第３の実施形態では、第１の実施形態及び第２の実施形態と同様に、コンテンツの転送元である送信装置が不正端末である場合であっても、コンテンツの転送先である受信装置が不正端末である場合であっても、コンテンツの流出元を特定することが出来る。

≪第４の実施形態≫

本発明の第４の実施形態について説明する。

＜概要＞

第４の実施形態では、第１の実施形態、第２の実施形態、及び第３の実施形態のそれぞれで説明した、送信装置と受信装置とにおけるコンテンツ鍵の送受信処理とは異なる方法を用いて、コンテンツ鍵を送受信する。

＜構成＞

第４の実施形態は、図１に示したコンテンツ配信システム１と同様のシステム構成を有する。即ち、第３の実施形態は、放送局装置、送信装置、受信装置、コンテンツ流出元特定装置、及び記録媒体から構成される。各装置の内部構成は、第１の実施形態における送信装置１０、受信装置２０、コンテンツ流出元特定装置３０と同様である。

【０１９５】

第４の実施形態では、受信装置は、公開鍵ＰＫ２と秘密鍵ＳＫ２とを保持してものとする。第４の実施形態で用いる公開鍵暗号アルゴリズムは、ＲＳＡ暗号、ＥｌＧａｍａｌ暗号、楕円曲線暗号など、任意のアルゴリズムでよい。

＜動作＞

第４の実施形態の全体の動作は、図１９に示した第１の実施形態の動作と同様であるため、説明を省略する。

【０１９６】

また、第４の実施形態におけるコンテンツ流出元特定処理の動作は、図２７及び図２８に示した第２の実施形態の動作と同様であるため、説明を省略する。

第４の実施形態におけるコンテンツ送受信処理の動作は、その一部が、第１の実施形態と同様である。具体的には、第４の実施形態は、ステップ２０１からステップＳ２０６まで、及び、ステップＳ２４１からステップＳ２５３まで、第１の実施形態と同様の処理を行う。第４の実施形態は、送信装置及び受信装置によるコンテンツ鍵の送受信処理が、第１の実施形態とは異なるので、以下では、図３１及び図３３に示すフローチャートを用いて、第１実施形態と異なる部分について説明する。

【０１９７】

送信装置は、１０２４ビットの素数ｐをランダムに生成する（ステップＳ７０１）。また、送信装置は、２以上ｐ－１以下の２つの異なる数ｇ、ｈをランダムに生成する（ステップＳ７０２）。

次に、送信装置は、１６０ビット以上１０２４ビット以下の数ｘ１をランダムに生成する（ステップＳ７０３）。そして、送信装置は、ｍｏｄ　ｐにおいてｇをｘ１乗した値であるＣ１＝ｇ＾ｘ１（ｍｏｄ　ｐ）を算出する（ステップＳ７０４）。

【０１９８】

その後、送信装置は、ｎ個の数ｒ＿１、ｒ＿２、…、ｒ＿ｎを生成する（ステップＳ７０５）。ここで生成するｎ個の数は、１２８ビット程度の乱数であってもよいし、単純に、１からｎまでの数であってもよい。

そして、送信装置は、値ｐ、値ｇ、値ｈ、値Ｃ１、及びｎ個の数ｒ＿１、ｒ＿２、…、ｒ＿ｎを受信装置へ送信し、受信装置は、値ｐ、値ｇ、値ｈ、値Ｃ１、及びｎ個の数ｒ＿１、ｒ＿２、…、ｒ＿ｎを受信する（ステップＳ７０６）。

【０１９９】

受信装置は、１６０ビット以上１０２４ビット以下の数ｘ２をランダムに生成する（ステップＳ７０７）。そして、受信装置は、ｍｏｄ　ｐにおいてＣ１をｘ２乗した値Ｃ１＾ｘ２（ｍｏｄ　ｐ）を計算し、この値を復号コンテンツ鍵ＤＣＫとして格納する（ステップＳ７０８）。なお、この値は、１０２４ビットとなる。受信装置は、１０２４ビットの復号コンテンツ鍵ＤＣＫを、ハッシュ関数を用いて１２８ビットに圧縮する（ステップＳ７０９）。

【０２００】

次に、受信装置は、ステップＳ７０６で受信したｎ個の値ｒ＿１、ｒ＿２、…、ｒ＿ｎのうち、１つをランダムに選択し、選択した値をｒ＿ｓ（ｓ＝１、２、…、ｎの何れか）とする（ステップＳ７１０）。

次に、受信装置は、ｍｏｄ　ｐにおいてｇをｘ２乗した値ｇ＾ｘ２（ｍｏｄ　ｐ）を算出し（ステップＳ７１１）、ｍｏｄ　ｐにおいてｈをｒ＿ｓ乗した値ｈ＾ｒ＿ｓ（ｍｏｄ　ｐ）を算出する（ステップＳ７１２）。

【０２０１】

続いて、受信装置は、ステップＳ７１１、及びステップＳ７１２で算出された二つの値をｍｏｄ　ｐで乗算し、その値をＣ２＝（ｇ＾ｘ２）×（ｈ＾ｒ＿ｓ）とする（ステップＳ７１３）。

次に、受信装置は、１２８ビットの乱数Ｐを生成し（ステップＳ７１４）、復号コンテンツ鍵ＤＣＫ、乱数ｒ＿ｓ、及び乱数Ｐを連結し、ＤＣＫ‖ｒ＿ｓ‖Ｐを生成する（ステップＳ７１５）。

【０２０２】

その後、受信装置は、自機の公開鍵ＰＫ２を用いて、ＤＣＫ‖ｒｓ‖Ｐを暗号化し、Ｅ＝Ｅｎｃ（ＰＫ２、ＤＣＫ‖ｒ＿ｓ‖Ｐ）を生成する（ステップＳ７１６）。

また、受信装置は、自機の秘密鍵ＳＫ２を署名生成鍵として用い、値Ｃ２‖Ｅに対するデジタル署名Ｓ＝Ｇｅｎ（ＳＫ２、Ｃ‖Ｅ）を作成する（ステップＳ７１７）。

受信装置は、値Ｃ２、値Ｅ、デジタル署名Ｓ、及び公開鍵ＰＫ２を送信装置へ送信し、送信装置は、値Ｃ２、値Ｅ、デジタル署名Ｓ、及び公開鍵ＰＫ２を受信する（ステップＳ７１８）。

【０２０３】

送信装置は、受信装置の公開鍵ＰＫ２を署名検証鍵として用い、デジタル署名Ｓが、Ｃ２‖Ｅに対する正規の署名であるか否かを検証する（ステップＳ７１９）。
検証の結果、デジタル署名Ｓは、受信装置が発行した正しいデジタル署名でないと判断された場合（ステップＳ７２０でＮＯ）、送信装置は、受信装置へのコンテンツ転送処理を終了する。

【０２０４】

検証の結果、デジタル署名Ｓは、受信装置が発行した正しいデジタル署名であると判断された場合（ステップＳ７２０でＹＥＳ）、送信装置は、値Ｃ２、値Ｅ、及びデジタル署名Ｓを、証拠情報ＥＶとして、証拠情報保持部へ格納する（ステップＳ７２１）。即ち、第４の実施形態では、証拠情報ＥＶの値が、第１の実施形態と異なる。
続いて、送信装置は、値Ｃ２をｎ個に複製し、Ｃ２＿１、Ｃ２＿２、…、Ｃ２＿ｎを生成し（ステップＳ７２２）、ｉ＝１、２、…、ｎについて、ステップＳ７２３からステップＳ７２７までを繰り返す。

【０２０５】

先ず、送信装置は、ステップＳ７０５で生成した値ｒ＿ｉから、ｈ＾ｒ＿ｉ（ｍｏｄ　ｐ）を算出する（ステップＳ７２４）。
次に、送信装置は、Ｃ２＿ｉを、値ｈ＾ｒ＿ｉ（ｍｏｄ　ｐ）除算して、Ｃ２＿ｉ÷ｈ＾ｒ＿ｉ（ｍｏｄ　ｐ）を算出する（ステップＳ７２５）。そして、送信装置は、ステップＳ７２４で算出した値を、ｍｏｄ　ｐでｘ１乗し、ＣＫ＿ｉ＝（Ｃ２＿ｉ÷ｈ＾ｒ＿ｉ）＾ｘ１（ｍｏｄ　ｐ）を算出する（ステップＳ７２６）。

【０２０６】

送信装置は、算出されたｎ個の値ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを、コンテンツ鍵として、コンテンツ鍵保持部へ格納する（ステップＳ７２８）。
以上により、第４の実施形態における送信装置と受信装置によるコンテンツ鍵の送受信処理を終了し、以後は、第１の実施形態のステップＳ２４１へ続く。

＜第４の実施形態の効果＞

ここでは、第４の実施形態の効果について述べる。

【０２０７】

（ａ）第４の実施形態においては、送信装置は、受信装置が取得するコンテンツを特定することが出来ない。その理由を以下に示す。
第４の実施形態における送信装置と受信装置とは、基本的に、ＤＨ（Ｄｉｆｆｉｅ　Ｈｅｌｌｍａｎ）鍵共有法と同じ原理を用いて、コンテンツ鍵を送受信する。
ここで、第４の実施形態に特徴的な点は、送信装置が、値ｇ、値ｈ、及びｎ個の値ｒ＿１、ｒ＿２、…、ｒ＿ｎを受信装置へ送信する点である。

【０２０８】

そして、受信装置は、ｎ個の値の中から一つの値ｒ＿ｓを選択し、Ｃ２＝（ｇ＾ｘ２）×（ｈ＾ｒ＿ｓ）を算出し、この値を送信装置へ送信する。
ここで、送信装置は、受信装置が生成したｘ２の値を知ることができないため、Ｃ２の値から、受信装置がｎ個の値ｒ＿１、ｒ＿２、…、ｒ＿ｎの内、どの値を選択したのか判別することが出来ない。

【０２０９】

そこで、送信装置は、受信装置が、ｒ＿１、ｒ＿２、…、ｒ＿ｎの内、どの値を選択した場合であっても、１個のコンテンツを利用できるように、全ての値ｒ＿１、ｒ＿２、…、ｒ＿ｎを用いて、値Ｃ２を、ｈ＾ｒ＿１、ｈ＾ｒ＿２、…、ｈ＾ｒ＿ｎで除算する。
これにより、受信装置が選択したｒ＿ｓと一致した場合にのみ、Ｃ２÷ｈ＾ｒ＿１、Ｃ２÷ｈ＾ｒ＿２、…、Ｃ２÷ｈ＾ｒ＿ｎの結果が、ｇ＾ｘ２（ｍｏｄ　ｐ）と等しくなる。

【０２１０】

そして、送信装置は、Ｃ２÷ｈ＾ｒ＿１、Ｃ２÷ｈ＾ｒ＿２、…、Ｃ２÷ｈ＾ｒ＿ｎを、全てｍｏｄ　ｐ上でｘ１乗し、その値を、ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎとすると

、何れかの値が、ｇ＾（ｘ１×ｘ２）（ｍｏｄ　ｐ）となる。
　これにより、送信装置が生成したＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎのうち、何れか一つは、受信装置が生成した復号コンテンツ鍵ＤＣＫと一致する。
【０２１１】
　そして、送信装置は、ｎ個のコンテンツ鍵ＣＫ＿１、ＣＫ＿２、…、ＣＫ＿ｎを用いて、異なる透かしを埋め込んだｎ個のコンテンツデータをそれぞれ暗号化して、ｎ個の暗号化コンテンツデータを生成する。
　受信装置は、送信装置からｎ個の暗号化コンテンツデータを受信すると、復号コンテンツ鍵ＤＣＫを用い、何れのコンテンツデータを取得したのか送信装置に知られることなく、１個のコンテンツデータを取得することが出来る。
【０２１２】
　（ｂ）第４の実施形態においては、第２の実施形態と同様に、証拠情報ＥＶに受信装置のデジタル署名Ｓが含まれているため、第２の実施形態の効果で説明したように、コンテンツ流出元特定装置が、海賊版コンテンツの流出元を正しく判定することが出来る。
　（ｃ）以上のことから、第４の実施形態では、第１の実施形態、第２の実施形態、及び第３の実施形態と同様に、コンテンツの転送元である送信装置が不正端末である場合であっても、コンテンツの転送先である受信装置が不正端末である場合であっても、コンテンツの流出元を特定することが出来る。
≪その他の変形例≫
　なお、本発明を上記の実施形態に基づき説明してきたが、本発明は、上記の実施形態に限定されないのは勿論であり、以下のような場合も、本発明に含まれる。
【０２１３】
　（１）上記実施の形態では、送信装置と受信装置とにおけるコンテンツ送受信処理について、４つの実施形態を用いて説明したが、送信装置と受信装置とにおけるコンテンツ送受信処理は、４つの実施形態に限定されないのは勿論である。
　本発明は、送信装置と受信装置とにおいて、送信装置から受信装置へ送られるｎ個のコンテンツ鍵のうち、受信装置が１個のコンテンツ鍵のみを取得でき、更に、送信装置が、受信装置が取得したコンテンツ鍵が何れのコンテンツ鍵であるのかを特定できない方法を用いてコンテンツ鍵を送受信する仕組みを有していればよい。
【０２１４】
　（２）上記の実施形態において、送信装置は、コンテンツの全体をｎ個に複製する構成を有するが、本発明においてこの構成は必須ではない。送信装置は、コンテンツを部分コンテンツに分割し、分割した１個の部分コンテンツについてのみ、ｎ個に複製するように構成してもよい。そして、複製された複数個の部分コンテンツに、送信先装置識別子、送信元装置識別子、証拠情報、及びコンテンツ鍵ハッシュを電子透かしとして埋め込み、異なる電子透かしが埋め込まれたそれぞれの部分コンテンツを、異なるコンテンツ鍵で暗号化するように構成してもよい。ここで、複製されていない部分コンテンツに関しては、共通する一つの鍵で暗号化して、送付するようにしてもよい。この構成により、送信装置から受信装置へ送信するデータ量を削減しつつ、上記の実施形態と同様の効果を得ることができる。
【０２１５】
　また、送信装置から受信装置へ送信するデータ量を削減しつつ、受信装置の選択可能なコンテンツの数を増加させるために、本発明は、上記の実施形態におけるコンテンツ鍵送受信処理を、送信装置と受信装置とにおいて複数回繰り返して行うように構成してもよい。例えば、送信装置が複製するコンテンツの数、及び生成するコンテンツ鍵の数がｎ＝４であった場合、受信装置が選択可能なコンテンツの数は４個である。この処理に加え、送信装置と受信装置とにおけるコンテンツ鍵送受信処理を、例えば３回繰り返して行うことにより、受信装置が選択可能なコンテンツの数は、６４個に増加する。
【０２１６】
　（３）上記の実施形態では、１台の送信装置と１台の受信装置との間でコンテンツを送

受信する構成を有しているが、本発明は、このようなピアツーピアのコンテンツ送受信に限定されず、１台のサーバ装置から、複数台のクライアント装置へ、コンテンツを送受信する構成であってもよい。

（４）上記の実施形態では、コンテンツの具体例として、映像データ及び音声データが多重化された動画像データを用いているが、本発明におけるコンテンツは、様々なデジタルデータを含む概念である。

【０２１７】

本発明におけるコンテンツは、例えば、動画、静止画、写真、音楽、ゲーム、コンピュータプログラム、電子地図、電子カルテ、Ｗｏｒｄ、ＰｏｗｅｒＰｏｉｎｔ、ＰＤＦ（Ｐｏｒｔａｂｌｅ Ｄｏｃｕｍｅｎｔ Ｆｏｒｍａｔ）等で作成された文書及び画像、テキストデータ等でもあってもよい。なお、テキストデータに電子透かしを埋め込む技術は、既に公知となっている。

【０２１８】

まは、本発明におけるコンテンツは、送信装置が外部の放送局装置から取得するコンテンツに限定されず、送信装置が予め保持していてもよい。即ち、本発明におけるコンテンツは、個人が所有する写真や映像などのプライベートコンテンツも含む概念である。

また、本発明がサーバークライアントシステムで構成される場合には、本発明におけるコンテンツは、掲示板、ＳＮＳ（Ｓｏｃｉａｌ Ｎｅｔｗｏｒｋｉｎｇ Ｓｅｒｖｉｃｅ）等であってもよい。

【０２１９】

（５）上記の実施形態では、送信装置と受信装置とは、ケーブルという通信路を用いてコンテンツを送受信しているが、本発明において、コンテンツが通信路を介して送受信される構成は必須ではない。コンテンツは、通信路を用いずに、ＤＶＤ－ＲＡＭや、ＳＤカード等の記録媒体を用いて送受信される構成でもよい。

また、上記の実施形態では、送信装置及び受信装置の具体例として、据置型の機器を用いているが、本発明において、送信装置及び受信装置は、据置型の機器に限定されず、例えば、持ち運びが可能なポータブル機器でもよいし、コンピュータ上のソフトウェアでもよい。

【０２２０】

（６）上記の実施形態では、コンテンツが複数の著作権保護システムに跨って流通する構成を有する。

具体的には、日本地上デジタル放送を放送する放送局装置は、放送向けの著作権保護規格であるＢ－ＣＡＳ（ＢＳ－Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）方式で保護された形でコンテンツを送信し、正規のテレビ受像機である送信装置は、Ｂ－ＣＡＳ方式で保護されたコンテンツを解除し、ディスプレイに表示する。

【０２２１】

送信装置は、コンテンツを受信装置へ送信する場合、Ｂ－ＣＡＳ方式で保護されたコンテンツを解除し、ＩＥＥＥ１３９４の著作権保護規格であるＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）形式で再度保護する。その後、送信装置は、ＩＥＥＥ１３９４規格ケーブル（ケーブル６０）用いて、コンテンツを受信装置へ送信する。

【０２２２】

コンテンツを受信した受信装置は、受信したコンテンツをＤＶＤ－ＲＡＭメディアに記録する場合には、ＤＴＣＰ形式で保護されたコンテンツを解除し、ＤＶＤ－ＲＡＭ上の著作権保護規格であるＣＰＲＭ（Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ｆｏｒ Ｒｅｃｏｒｄａｂｌｅ Ｍｅｄｉａ）形式で再度保護する。その後、受信装置は、コンテンツをＤＶＤ－ＲＡＭメディアに記録する。

【０２２３】

ここで、Ｂ－ＣＡＳ形式、ＤＴＣＰ形式、及びＣＰＲＭ形式は、それぞれ運営団体が異なる著作権保護規格である。従って、このようなシステムにいて不正コピーされたコンテ

ンツが発見された場合には、先ず、どのコンテンツ保護規格が不正なユーザに解析されたのか把握しなければならない。

上記の実施形態では、海賊版コンテンツを作成した装置を特定することが出来るように、コンテンツに受信装置の装置識別子、及び送信装置の装置識別子を電子透かしとして埋め込む構成を有しているが、本発明は、不正なユーザにより解析されたコンテンツ保護規格を特定するために、装置識別子に代えて、受信装置が属するシステムを識別する情報である受信装置システム識別子、及び、送信装置が属するシステムを識別する情報である送信装置システム識別子をコンテンツに埋め込むように構成してもよい。ここで、システム識別子は、予め１個のシステムに１個の識別子が割り当てられているものとする。例えば、テレビ受像機システムに対しては「０１」が割り当てられ、ＤＶＤレコーダシステムに対しては「０２」が割り当てられており、送信装置は、ｎ個の第一コンテンツデータに、送信装置システム識別子０１と、受信装置システム識別子０２とを電子透かしとして埋め込む。

【０２２４】

（７）また、本発明は、上記の実施形態のようにコンテンツが複数の著作権保護システムに跨って流通する構成に限定されないのは、勿論である。

本発明は、送信装置と受信装置とが同一の著作権保護システムを用いて、コンテンツを送受信する場合も含まれる。

（８）上記の実施形態では、受信装置と送信装置という２つの端末装置間でコンテンツを転送するシステムを用いて、本発明を説明していたが、本発明は、これに限るものではない。例えば、端末装置が３台以上（例えば、端末装置Ａ、端末装置Ｂ、端末装置Ｃ）存在し、端末装置Ａから端末装置Ｂへコンテンツが転送され、その後、同じコンテンツが端末装置Ｂから端末装置Ｃへ転送されてもよい。

【０２２５】

（９）また、本発明における電子透かし埋込処理は、以下に示す方法を用いてもよい。

放送媒体、記録媒体などの各メディアシステムが、それぞれに異なる電子透かし埋め込みパラメータを保持しており、各メディアシステムに所属する装置が、電子透かし埋め込みパラメータを用いて、電子透かしを埋め込むように構成してもよい。そして、各メディアシステムが保持するパラメータは、他のメディアシステムには秘密にするように構成してもよい。ここで、前記パラメータは、例えば、コンテンツのどの部分に電子透かしを埋め込むのかを示す情報、どの周波数体に埋め込むのかを示す情報、どういうアルゴリズムで埋め込むのかを示す情報などである。

【０２２６】

これにより、海賊版コンテンツが流出した場合には、海賊版コンテンツに埋め込まれている電子透かしが、どのメディアシステムに属する装置が埋め込んだのかを特定出来るようになる。

（１０）本発明における電子透かし埋込処理は、非対称電子透かしアルゴリズムを用いても良い。

【０２２７】

ここで、非対象電子透かしとは、ある秘密情報を知らなければ、電子透かしを埋め込むことは出来ないが、その秘密情報に対応する公開情報を知っている全ての者が、埋め込まれた電子透かしを抽出することが出来るアルゴリズムである。

非対称電子透かしを用いると、海賊版コンテンツが流出した場合には、海賊版コンテンツに埋め込まれている電子透かしが、どのメディアシステムにより埋め込まれたのかを判断することにより、流出元を特定することができる。

【０２２８】

（１１）本発明において、コンテンツに埋め込む電子透かし（ウォーターマーク）は、上記の実施形態に記載したデータに限定されない。

例えば、実施形態で埋め込むと記載したデータとＩＤとを予め対応付けておき、コンテンツにＩＤを埋め込むように構成してもよい。即ち、コンテンツに埋め込む電子透かしは

、コンテンツ漏洩時に、コンテンツ流出特定装置において追跡できる形になっていればよい。

【０２２９】

（１２）また、本発明において、コンテンツに埋め込む電子透かしは、上記の実施形態に記載したデータそのものでなく、その一部分であってもよい。

例えば、実施形態に記載したデータの下位１０ビットを埋め込むように構成してもよい。この場合、異なるデータから、同じ電子透かしが埋め込まれる可能性があるため、１回の流出元特定処理で、海賊版コンテンツの流出元を特定することは出来なくなる可能性がある。しかし、流出元特定処理を複数回繰り返すことにより、絞り込んでいくことが可能であり、最終的には流出元装置を一意に特定することは可能である。このように構成することのメリットは、（ａ）ある第三者が、そのコンテンツの電子透かしを抽出しても、データ全体を把握することはできないので、プライバシを保護することができる点。（ｂ）電子透かし技術に制限（例えば、数十ビット程度しか埋め込めない）がある場合であっても、上記の実施形態と同様の効果が実現できる点である。

【０２３０】

（１３）また、本発明において、コンテンツに埋め込む電子透かしは、サーバや装置の公開鍵（もしくは共通鍵暗号系の共有鍵）で暗号化して埋め込むようにしてもよい。このように構成することにより、ある第三者が、そのコンテンツの電子透かしを抽出した場合であっても、当該第三者は、電子透かしから、埋め込んだ元データを把握することは出来ず、受信装置が選択した情報を判断することが出来ない。これにより、より安全なコンテンツ流通を実現することが可能となる。更に、公開鍵暗号方式として、乱数を用いる確率暗号（例えばＥｌＧａｍａｌ暗号）を使えば、同じメッセージであっても毎回異なる暗号文が出力されるので、より高い安全性を実現することができる。

【０２３１】

（１４）また、本発明においては、コンテンツに埋め込む電子透かしとして、送信装置及び／又は受信装置を識別する情報（著作権保護方式ＩＤや端末ＩＤ）を含めても良い。また、コンテンツのヘッダ部やフッタ部に、それらの情報を追加するようにしてもよい。これにより、コンテンツ流出元装置における流出元装置の追跡がより容易になる。

（１５）また、本発明は、受信装置が、さらに別の受信装置へコンテンツを送信するシステムであってもよい。

【０２３２】

この場合、同じコンテンツに、複数の電子透かしを埋め込むことにより、上記の実施形態と同様に海賊版コンテンツの流出元装置を追跡できるようになる。

更に、この場合、下記のような工夫を加えてもよい。

（ａ）コンテンツに、世代数やコピー数などを加えるようにしてもよい。

（ｂ）送信装置は、電子透かしが埋め込まれていない部分を判断し、そこに電子透かしを埋め込むようにしてもよい。

【０２３３】

（ｃ）送信装置と受信装置とに関する情報（例えば、端末ＩＤなど）から、例えば、一方向性関数を用いて一意に求まる場所に電子透かしを埋め込んでもよい。

（ｄ）コンテンツの先頭（Ａ）から順番に、電子透かしを埋め込んでもよい。

（ｅ）各受信装置は、それぞれ異なる電子透かし埋め込み手法を用いてもよい。もしくは、各受信装置は、異なる電子透かし埋め込みパラメータ（周波数帯域とか）を用いてもよい。

【０２３４】

（ｆ）上記の（ａ）から（ｅ）を組み合わせでもよい。例えば、同一のコンテンツ保護方式内は、コンテンツの先頭から順番に（Ａ、Ｂ、Ｃ、…）電子透かしを埋め込み、異なるコンテンツ保護方式間は、異なる電子透かし埋め込み方式を用いてもよい。

（１６）本発明は、受信装置へコンテンツを送信する送信装置であって、複数個のコンテンツ鍵に第一演算を施して生成された複数個の第一演算化コンテンツ鍵を、前記受信装

置へ送信する候補鍵送信手段と、前記受信装置により選択された１個の第一演算化コンテンツ鍵に、第二演算を施して生成された第二演算化コンテンツ鍵を、前記受信装置から取得する選択鍵取得手段と、前記第二演算化コンテンツ鍵に、前記第一演算の逆変換である第三演算を施して、証拠情報を生成する証拠情報生成手段と、同一内容の複数個のコンテンツのそれぞれに、前記証拠情報と当該コンテンツに対応するコンテンツ鍵のハッシュ値とを電子透かしとして埋め込む証拠埋込手段と、前記証拠情報と前記ハッシュ値とが埋め込まれた複数個のコンテンツのそれぞれを、対応するコンテンツ鍵を用いて暗号化し、複数個の暗号化コンテンツを生成する暗号化手段と、前記証拠情報及び前記複数個の暗号化コンテンツを、前記受信装置へ送信するコンテンツ送信手段とを備えることを特徴とする。

【０２３５】

また、本発明は、受信装置へコンテンツを送信する送信装置であって、複数個の候補情報を、前記受信装置へ送信する候補情報送信手段と、前記受信装置により選択された１の候補情報と、前記受信装置により生成された復号コンテンツ鍵とに、第一演算が施されて生成された選択情報を、前記受信装置から取得する選択情報取得手段と、前記選択情報を複数個に複製する複製手段と、前記複数個の選択情報に、前記第一演算の逆変換である第二演算を施すことにより、複数個のコンテンツ鍵を生成するコンテンツ鍵生成手段と、同一内容の複数個のコンテンツのそれぞれに、前記選択情報と当該コンテンツに対応するコンテンツ鍵のハッシュ値とを電子透かしとして埋め込む証拠埋込手段と、前記選択情報と前記ハッシュ値とが埋め込まれた複数個のコンテンツのそれぞれを、対応するコンテンツ鍵を用いて暗号化し、暗号化コンテンツを生成する暗号化手段と、前記複数個の暗号化コンテンツを、前記受信装置へ送信するコンテンツ送信手段とを備えることを特徴とする。

【０２３６】

また、本発明は、送信装置からコンテンツを取得する受信装置であって、前記送信装置から、複数個のコンテンツ鍵が暗号化されて生成された複数個の暗号化コンテンツ鍵を受信する候補鍵受信手段と、前記複数個の暗号化コンテンツ鍵から１個を選択する鍵選択手段と、選択された前記暗号化コンテンツ鍵に、第一演算を施すことにより、第一演算化コンテンツ鍵を生成する選択鍵変換手段と、前記第一演算化コンテンツ鍵を、前記送信装置へ送信する選択鍵送信手段と、前記送信装置から、前記第一演算化コンテンツ鍵に、第二演算を施して生成された第二演算化コンテンツ鍵を受信するコンテンツ鍵受信手段と、前記第二演算化コンテンツ鍵に、前記第一演算の逆変換である第三演算を施すことにより、復号コンテンツ鍵を取得する復号コンテンツ鍵取得手段と、前記送信装置から、前記複数個のコンテンツ鍵に基づき暗号化された複数個の暗号化コンテンツを受信するコンテンツ受信手段と、前記復号コンテンツ鍵に基づき、前記複数個の暗号化コンテンツの内の１個を取得する復号手段とを備えることを特徴とする。

【０２３７】

また、本発明は、送信装置からコンテンツを取得する受信装置であって、前記送信装置から、複数個の候補情報を受信する候補情報受信手段と、前記複数個の候補情報から、１の候補情報を選択する選択手段と、１の復号コンテンツ鍵を生成する復号コンテンツ鍵生成手段と、前記選択手段により選択された１の候補情報及び前記復号コンテンツ鍵に、第一演算を施すことにより、選択情報を生成する選択情報生成手段と、前記選択情報を、前記送信装置に送信する選択情報送信手段と、前記送信装置から、前記複数個の候補情報及び前記選択情報に、前記第一演算の逆変換である第二演算を施すことにより生成された複数個のコンテンツ鍵に基づき暗号化された複数個の暗号化コンテンツを受信するコンテンツ受信手段と、前記複数個の暗号化コンテンツの内の１個を、前記復号コンテンツ鍵に基づき復号し、１個のコンテンツを取得する復号手段とを備えることを特徴とする。

【０２３８】

（１７）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【０２３９】

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

【０２４０】

また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１８）本発明の各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ Ｓｃａｌｅ Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路で実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）やＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

【０２４１】

更には、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用などが可能性として有り得る。

（１９）本発明の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【０２４２】

（２０）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０２４３】

本発明は、映画や音楽などの著作物であるデジタルデータを配信する産業において、著作権侵害行為を防止する技術として特に有用である。

【図面の簡単な説明】

【０２４４】

【図１】コンテンツ配信システム１の構成を示すシステム構成図である。

【図２】送信装置１０の構成を示すブロック図である。

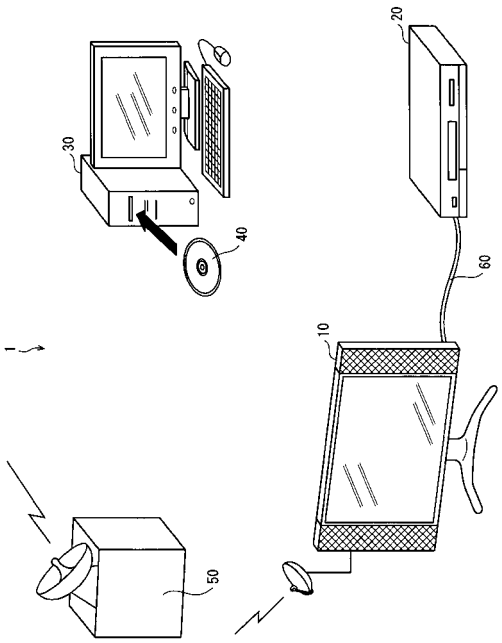
【図３】コンテンツ鍵保持部１０３が保持している情報を示す図である。

【図４】公開鍵保持部１０４が保持している情報を示す図である。

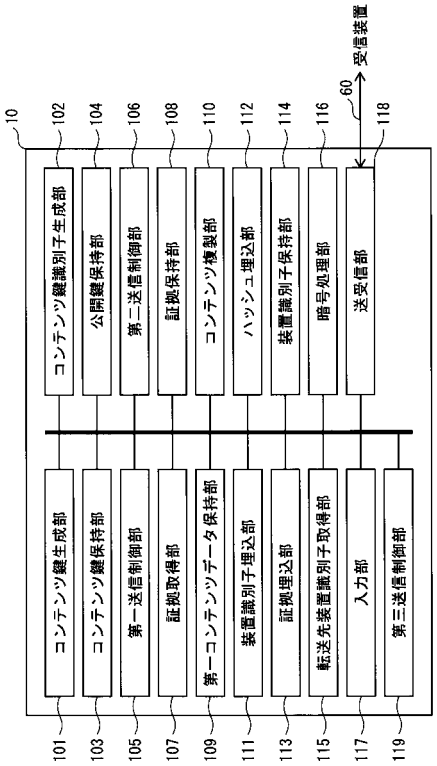
【図５】証拠保持部１０８が保持している情報を示す図である。
【図６】第一コンテンツデータ保持部１０９が保持している情報を示す図である。
【図７】装置識別子保持部１１４が保持している情報を示す図である。
【図８】送信装置１０から受信装置２０へ送信される暗号化コンテンツ鍵を示す図である。
【図９】送信装置１０から受信装置２０へ送信される暗号化第一コンテンツを示す図である。
【図１０】受信装置２０の構成を示すブロック図である。
【図１１】公開鍵保持部２０１が保持している情報を示す図である。
【図１２】復号コンテンツ鍵保持部２０２が保持している情報を示す図である。
【図１３】選択情報保持部２０５が保持している情報を示す図である。
【図１４】第二コンテンツデータ保持部２０８が保持している情報を示す図である。
【図１５】装置識別子保持部２１０が保持している情報を示す図である。
【図１６】コンテンツ流出元特定装置３０の構成を示すブロック図である。
【図１７】追跡コンテンツデータ保持部３０６が保持している情報を示す図である。
【図１８】暗号鍵保持部３０８が保持している情報を示す図である。
【図１９】コンテンツ配信システム１の動作を示すフローチャートである。
【図２０】第１の実施形態におけるコンテンツ送受信処理の動作を示すフローチャートであり、図２１へ続く。
【図２１】第１の実施形態におけるコンテンツ送受信処理の動作を示すフローチャートであり、図２２へ続く。
【図２２】第１の実施形態におけるコンテンツ送受信処理の動作を示すフローチャートである。
【図２３】第１の実施形態におけるコンテンツ流出元特定処理の動作を示すフローチャートであり、図２４へ続く。
【図２４】第１の実施形態におけるコンテンツ流出元特定処理の動作を示すフローチャートである。
【図２５】第２の実施形態におけるコンテンツ送受信処理の動作の一部を示すフローチャートであり、図２６へ続く。
【図２６】第２の実施形態におけるコンテンツ送受信処理の動作の一部を示すフローチャートである。
【図２７】第２の実施形態におけるコンテンツ流出元特定処理の動作の一部を示すフローチャートであり、図２８へ続く。
【図２８】第２の実施形態におけるコンテンツ流出元特定処理の動作の一部を示すフローチャートである。
【図２９】第３の実施形態におけるコンテンツ送受信処理の動作の一部を示すフローチャートであり、図３０へ続く。
【図３０】第３の実施形態におけるコンテンツ送受信処理の動作の一部を示すフローチャートである。
【図３１】第４の実施形態におけるコンテンツ送受信処理の一部を示すフローチャートであり、図３２へ続く。
【図３２】第４の実施形態におけるコンテンツ送受信処理の一部を示すフローチャートであり、図３３へ続く。
【図３３】第４の実施形態におけるコンテンツ送受信処理の一部を示すフローチャートである。
【符号の説明】
【０２４５】
１　コンテンツ配信システム
１０　送信装置
２０　受信装置

３０　コンテンツ流出元特定装置
４０　記録媒体
５０　放送局装置
６０　ケーブル
１０１　コンテンツ鍵生成部
１０２　コンテンツ鍵識別子生成部
１０３　コンテンツ鍵保持部
１０４　公開鍵保持部
１０５　第一送信制御部
１０６　第二送信制御部
１０７　証拠取得部
１０８　証拠保持部
１０９　第一コンテンツデータ保持部
１１０　コンテンツ複製部
１１１　装置識別子埋込部
１１２　ハッシュ埋込部
１１３　証拠埋込部
１１４　装置識別子保持部
１１５　転送先装置識別子取得部
１１６　暗号処理部
１１７　入力部
１１８　送受信部
１１９　第三送信制御部
２０１　公開鍵保持部
２０２　復号コンテンツ鍵保持部
２０３　第一受信制御部
２０４　第二受信制御部
２０５　選択情報保持部
２０６　コンテンツ鍵選択部
２０７　暗号化コンテンツ選択部
２０８　第二コンテンツデータ保持部
２０９　装置識別子出力部
２１０　装置識別子保持部
２１１　送受信部
２１２　暗号処理部
２１３　第三受信制御部
３０１　情報抽出部
３０２　証拠検証部
３０３　流出元判定部
３０４　流出元出力部
３０５　コンテンツデータ入力部
３０６　追跡コンテンツデータ保持部
３０７　暗号処理部
３０８　暗号鍵保持部

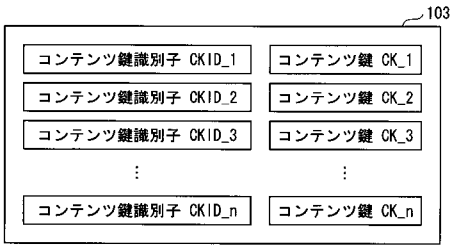
【図１】



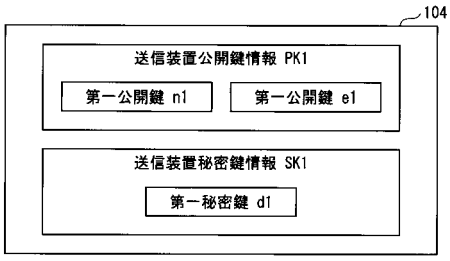
【図２】



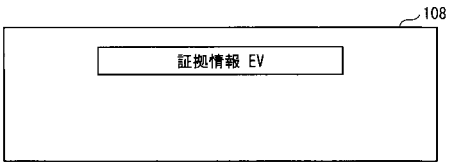
【図３】



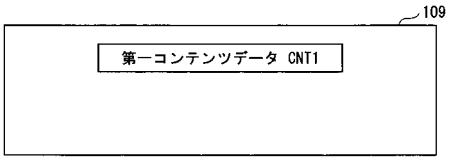
【図４】



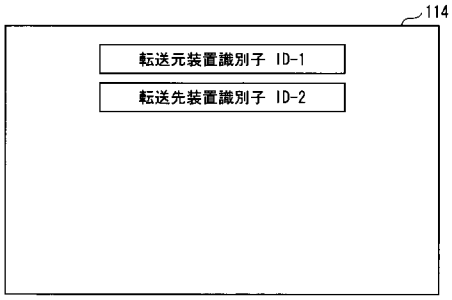
【図５】



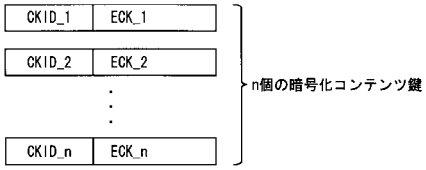
【図６】



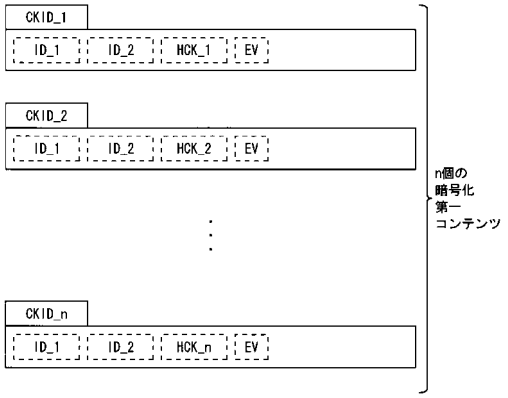
【図７】



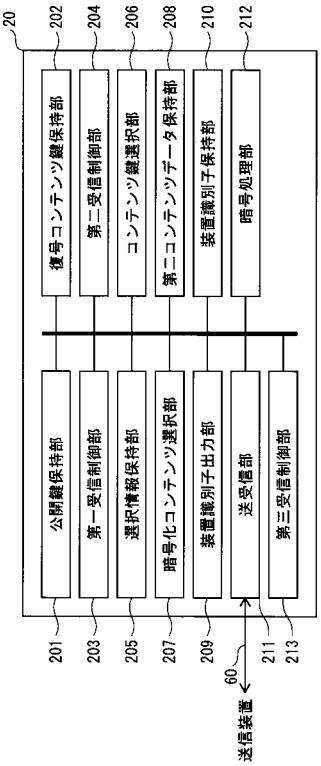
【図８】



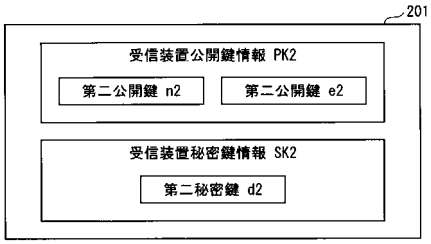
【図９】



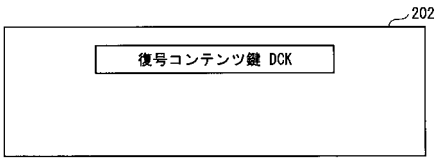
【図１０】



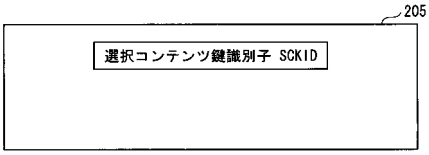
【図１１】



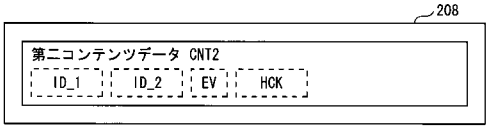
【図１２】



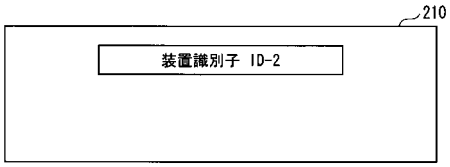
【図１３】



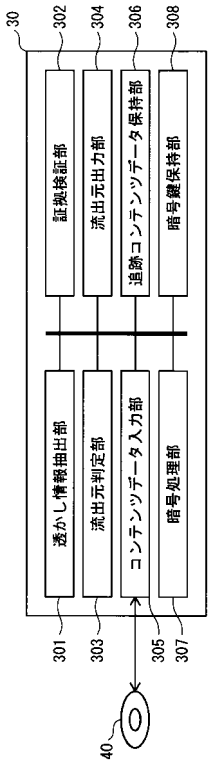
【図１４】



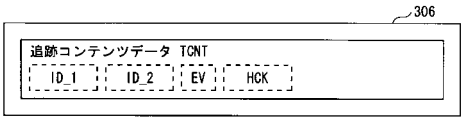
【図１５】



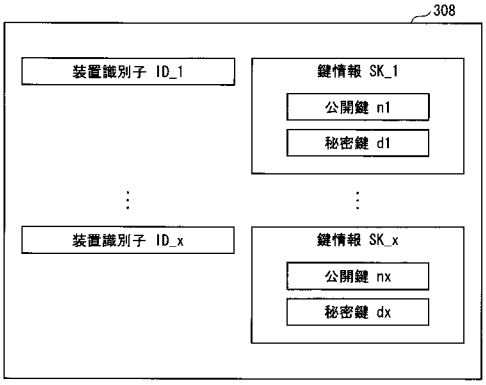
【図１６】



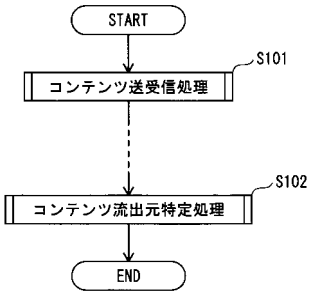
【図１７】



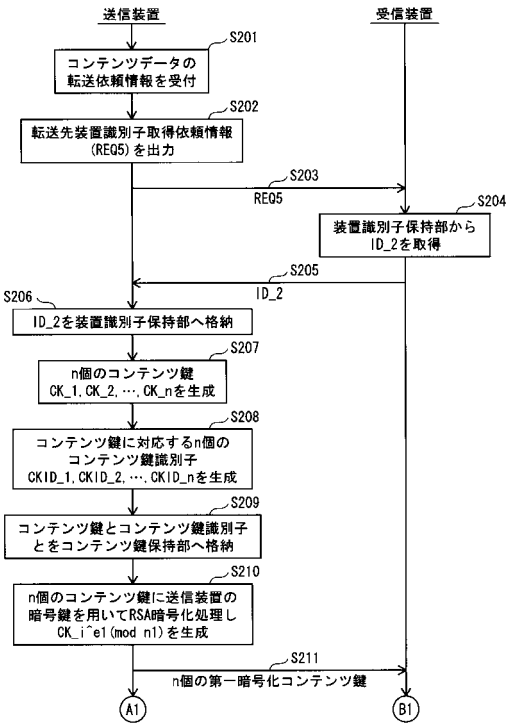
【図１８】



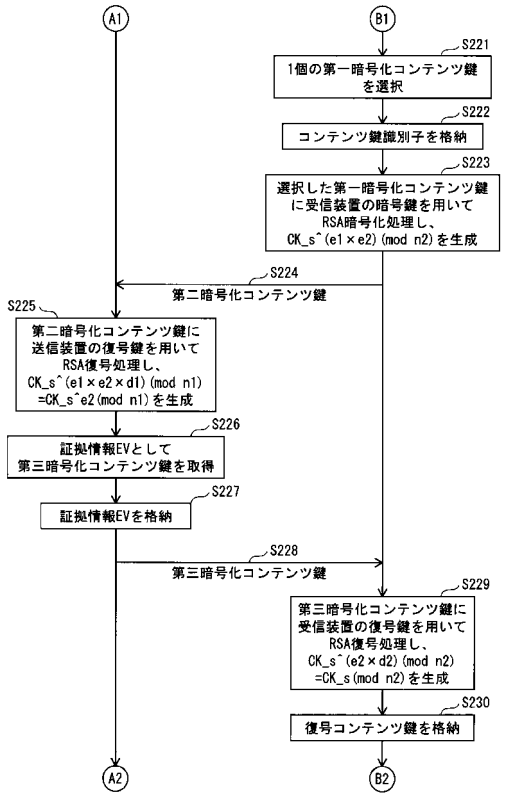
【図１９】



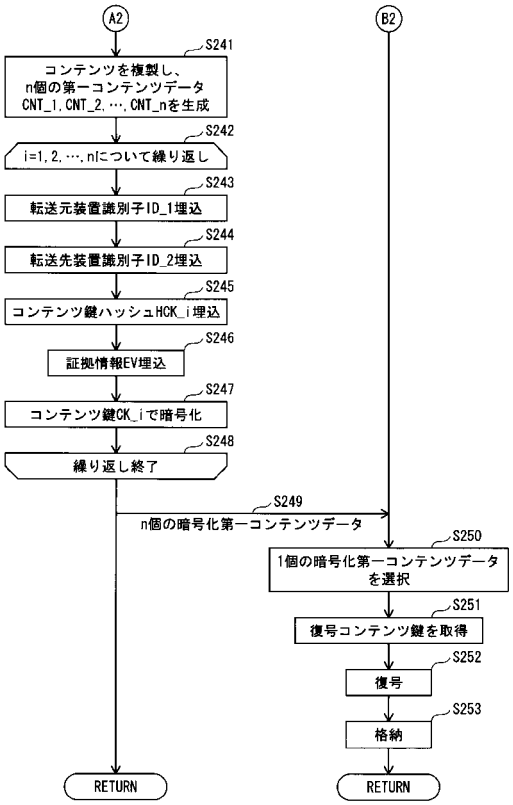
【図２０】



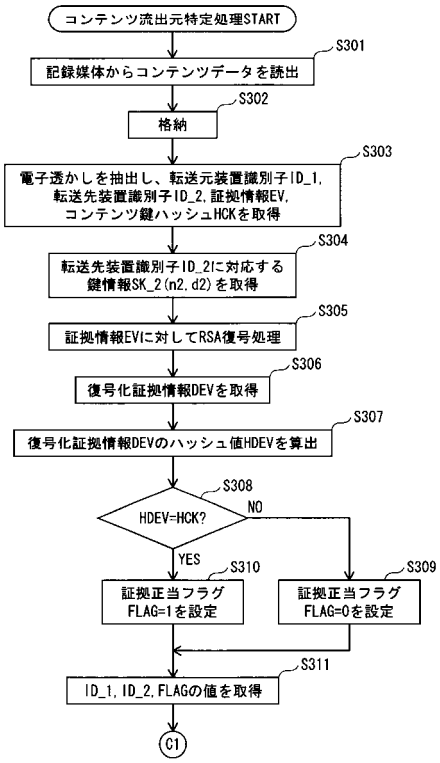
【図２１】



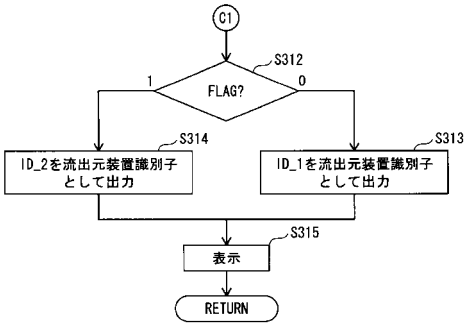
【図２２】



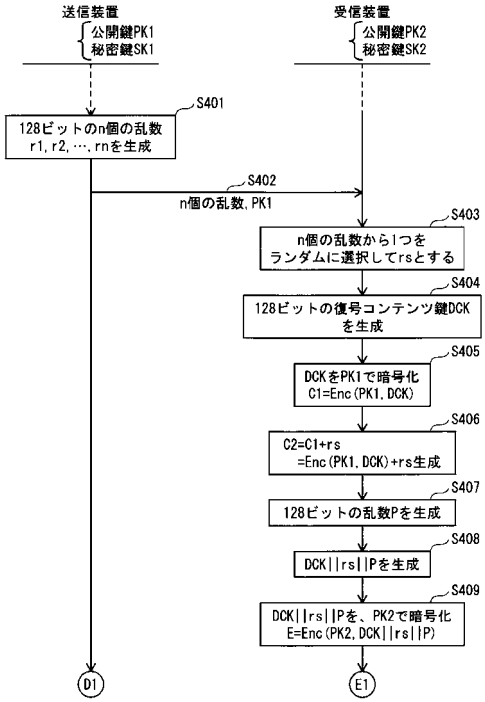
【図２３】



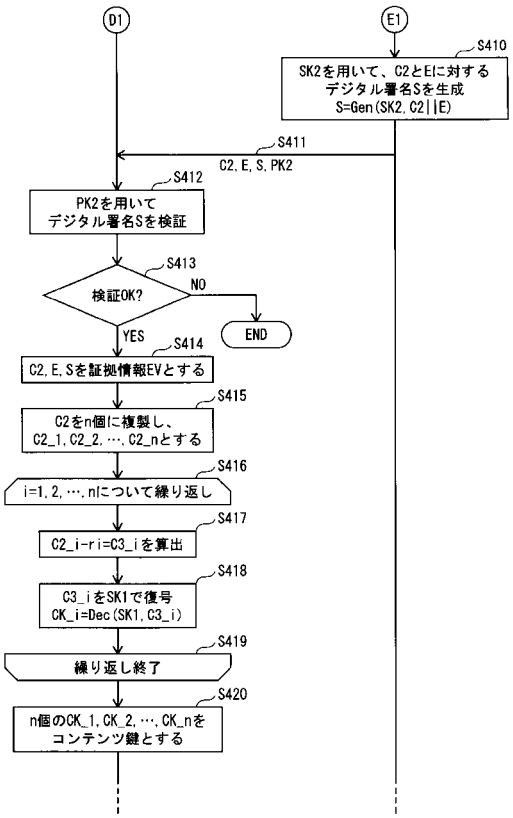
【図２４】



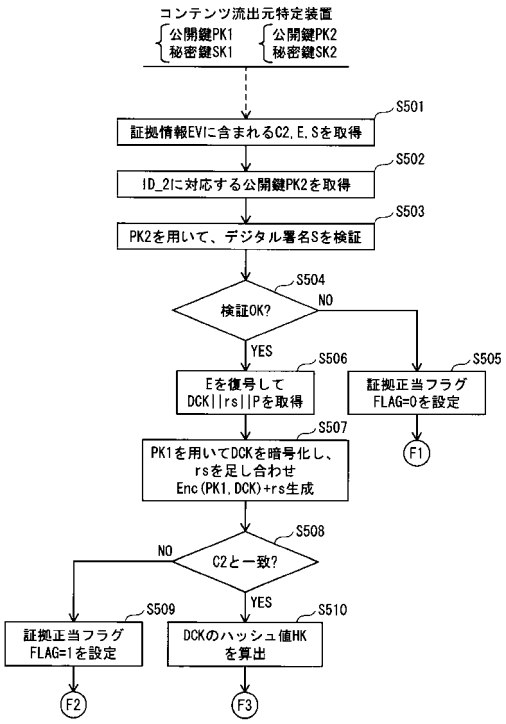
【図２５】



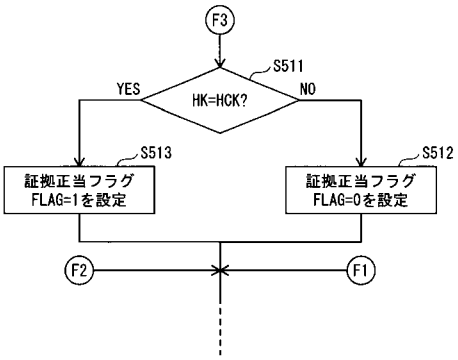
【図２６】



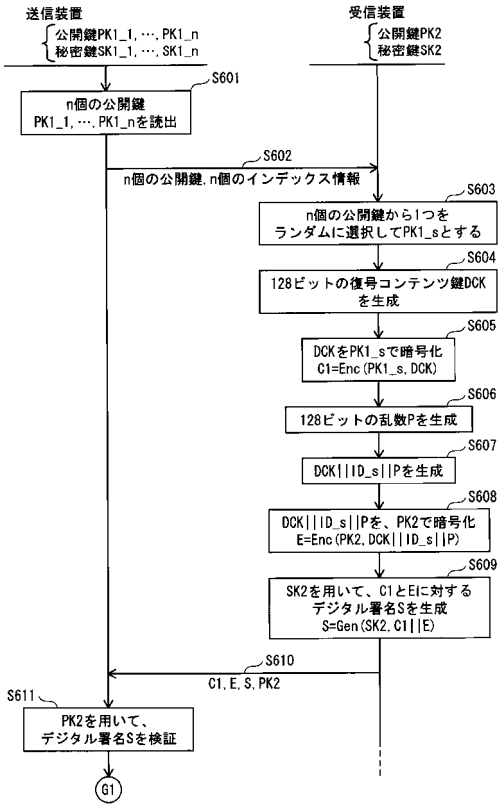
【図２７】



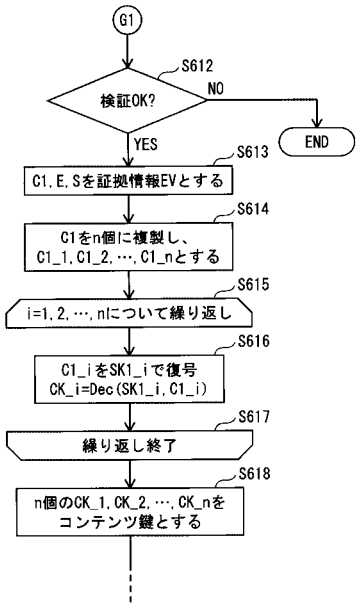
【図２８】



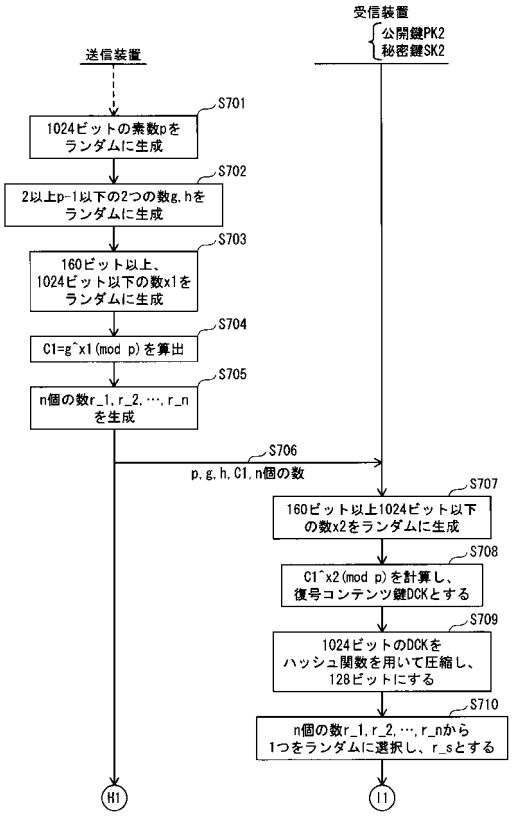
【図２９】



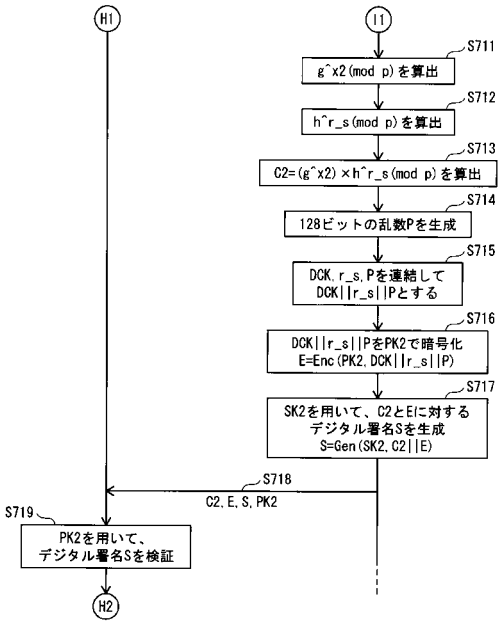
【図３０】



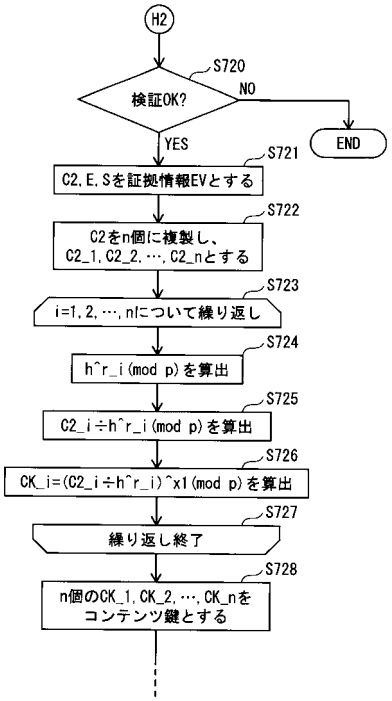
【図３１】



【図３２】


H1
I1
S711
g^x2(mod p)を算出
S712
h^r_s(mod p)を算出
S713
C2=(g^x2)×h^r_s(mod p)を算出
S714
128ビットの乱数Pを生成
S715
DCK, r_s, Pを連結して
DCK||r_s||Pとする
S716
DCK||r_s||PをPK2で暗号化
E=Enc(PK2, DCK||r_s||P)
S717
SK2を用いて、C2とEに対する
デジタル署名Sを生成
S=Gen(SK2, C2||E)
S718
C2, E, S, PK2
S719
PK2を用いて、
デジタル署名Sを検証
H2

【図３３】


H2
S720
検証OK?
NO
END
YES
S721
C2, E, Sを証拠情報EVとする
S722
C2をn個に複製し、
C2_1, C2_2, …, C2_nとする
S723
i=1, 2, …, nについて繰り返し
S724
h^r_i(mod p)を算出
S725
C2_i÷h^r_i(mod p)を算出
S726
CK_i=(C2_i÷h^r_i)^x1(mod p)を算出
S727
繰り返し終了
S728
n個のCK_1, CK_2, …, CK_nを
コンテンツ鍵とする

フロントページの続き

(72)発明者　中野　稔久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　布田　裕一
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　古原　和邦
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内
(72)発明者　野島　良
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内
(72)発明者　今井　秀樹
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内

審査官　和田　財太

(56)参考文献　特開２００４－３１８４４８（ＪＰ，Ａ）
特開２００３－３４８０８１（ＪＰ，Ａ）
特開平１１－０６６０１０（ＪＰ，Ａ）
渡邊裕治（外3名），Ｏｂｌｉｖｉｏｕｓ　Ｐｏｌｙｎｏｍｉａｌ　Ｅｖａｌｕａｔｉｏｎを用いた非対称不正者追跡法，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０００年　9月22日，Ｖｏｌ．１００，Ｎｏ．３２４，ｐ．１５５－ｐ．１６２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２－２１／２４
Ｇ０９Ｃ　１／００
Ｇ０９Ｃ　５／００
Ｈ０４Ｎ　７／１６