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

特許第6031360号
(P6031360)

(45)発行日　平成28年11月24日(2016.11.24)　(24)登録日　平成28年10月28日(2016.10.28)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04N	7/173	(2011.01)	H04L	9/00	601E
			H04N	7/173	610Z
			H04N	7/173	630

請求項の数 4　(全 23 頁)

(21)出願番号　特願2013-2225(P2013-2225)
(22)出願日　平成25年1月10日(2013.1.10)
(65)公開番号　特開2014-135620(P2014-135620A)
(43)公開日　平成26年7月24日(2014.7.24)
審査請求日　平成27年12月1日(2015.12.1)

特許権者において、実施許諾の用意がある。

(73)特許権者　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　110001807
特許業務法人磯野国際特許商標事務所
(74)代理人　100064414
弁理士　磯野　道造
(74)代理人　100111545
弁理士　多田　悦夫
(72)発明者　西本　友成
東京都世田谷区砧一丁目１０番１１号　日本放送協会放送技術研究所内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】アクセス制御プログラム、送信装置、受信装置および情報漏洩元特定装置

(57)【特許請求の範囲】
【請求項１】
デジタル放送の受信装置に当該受信装置のデバイスごとに組み込まれるコンテンツを限定受信するためのアクセス制御プログラムであって、暗号化されたスクランブル鍵に関連する関連情報を用いて、コンテンツを暗号化した前記スクランブル鍵を復号するために、前記受信装置のコンピュータを、
送信装置から送信された、当該受信装置固有のマスタ鍵により暗号化されたワーク鍵を含んだ前記関連情報である個別情報を前記マスタ鍵で復号し、前記ワーク鍵を取得する個別情報処理手段、
前記送信装置から送信された、前記ワーク鍵により暗号化された前記スクランブル鍵を含んだ前記関連情報である共通情報を前記個別情報処理手段で復号されたワーク鍵で復号し、前記スクランブル鍵を取得する共通情報処理手段、
前記共通情報に前記スクランブル鍵の復号停止を指示する情報が含まれている場合に、前記受信装置の予め定めたデバイスごとに異なるアクセス制御プログラムの遅延パラメータとして、予め当該プログラムに設定された遅延時間を計時し、前記遅延時間経過後、前記共通情報処理手段に前記スクランブル鍵の復号停止を指示する復号停止遅延手段、
として機能させるためのアクセス制御プログラム。
【請求項２】
コンテンツおよび当該コンテンツを暗号化した鍵に関連する関連情報と、当該コンテンツを限定受信するためのアクセス制御プログラムおよび当該アクセス制御プログラムを暗

号化した鍵に関連する関連情報とを、受信装置に送信するデジタル放送の送信装置であって、
第１ワーク鍵を受信装置個別のマスタ鍵で暗号化し、暗号化した第１ワーク鍵を含んだ受信装置個別の第１個別情報を生成する第１個別情報生成手段と、
第１スクランブル鍵を前記第１ワーク鍵で暗号化し、暗号化した第１スクランブル鍵を含んだ受信装置共通の第１共通情報を生成する第１共通情報生成手段と、
前記コンテンツを前記第１スクランブル鍵で暗号化し、暗号化コンテンツを生成するコンテンツスクランブル手段と、
受信装置の予め定めたデバイスごとに、第２ワーク鍵を当該デバイスごとのデバイス鍵で暗号化し、暗号化した第２ワーク鍵を含んだ受信装置のデバイス個別の第２個別情報を生成する第２個別情報生成手段と、
第２スクランブル鍵を前記第２ワーク鍵で暗号化し、暗号化した第２スクランブル鍵を含んだ受信装置共通の第２共通情報を生成する第２共通情報生成手段と、
受信装置のデバイスごとに予め異なる遅延時間を遅延パラメータとして組み込んだ請求項１に記載のアクセス制御プログラムを前記第２スクランブル鍵で暗号化し、暗号化アクセス制御プログラムを生成するプログラムスクランブル手段と、
前記第１個別情報と、前記第１共通情報と、前記暗号化コンテンツと、前記第２個別情報と、前記第２共通情報と、前記暗号化アクセス制御プログラムとを多重化し、放送信号を生成する多重化手段と、
を備えることを特徴とする送信装置。
【請求項３】
コンテンツを暗号化した暗号化コンテンツと、前記コンテンツを暗号化した第１スクランブル鍵を含んだ受信装置共通の第１共通情報と、前記第１スクランブル鍵を暗号化した第１ワーク鍵を含んだ受信装置個別の第１個別情報と、前記コンテンツを限定受信するためのアクセス制御プログラムを暗号化した暗号化アクセス制御プログラムと、前記アクセス制御プログラムを暗号化した第２スクランブル鍵を含んだ受信装置共通の第２共通情報と、前記第２スクランブル鍵を暗号化した第２ワーク鍵を含んだ受信装置のデバイスごとに個別の第２個別情報とを多重化した放送信号を、送信装置から受信するデジタル放送の受信装置であって、
前記多重化された放送信号を分離する分離手段と、
前記第２個別情報を当該受信装置の予め定めたデバイス単位の鍵であるデバイス鍵で復号し、前記第２ワーク鍵を取得する第２個別情報処理手段と、
前記第２共通情報を前記第２個別情報処理手段で復号された第２ワーク鍵で復号し、前記第２スクランブル鍵を取得する第２共通情報処理手段と、
前記暗号化アクセス制御プログラムを前記第２共通情報処理手段で復号された第２スクランブル鍵で復号し、前記アクセス制御プログラムを取得するプログラムデスクランブル手段と、
このプログラムデスクランブル手段で取得されたアクセス制御プログラムを動作させるアクセス制御手段と、を備え、
前記アクセス制御手段は、前記アクセス制御プログラムの動作により、
前記第１個別情報を当該受信装置個別の鍵であるマスタ鍵で復号し、前記第１ワーク鍵を取得する第１個別情報処理手段と、
前記第１共通情報を前記第１個別情報処理手段で復号された第１ワーク鍵で復号し、前記第１スクランブル鍵を取得する第１共通情報処理手段と、
前記第１共通情報に前記第１スクランブル鍵の復号停止を指示する情報が含まれている場合に、予め遅延パラメータとして定めた遅延時間を計時し、前記遅延時間経過後、前記第１共通情報処理手段に前記第１スクランブル鍵の復号停止を指示する復号停止遅延手段として機能することを特徴とする受信装置。
【請求項４】
スクランブル鍵の復号停止を指示されてから実際に復号停止を行うまでの遅延時間が受

信装置のデバイスごとに異なるアクセス制御プログラムを組み込んだ受信装置から複製された複製受信装置が、前記デバイスのうちいずれのデバイスからの情報漏洩により複製されたものかを特定する情報漏洩元特定装置であって、
擬似放送信号を生成して前記複製受信装置に送信する擬似放送信号生成手段と、
前記複製受信装置が前記擬似放送信号を復号した表示信号から、前記複製受信装置のアクセス制御機能の情報漏洩元のデバイスを特定するアクセス制御機能種別判定手段と、を備え、
前記擬似放送信号生成手段は、
ワーク鍵を受信装置個別のマスタ鍵で暗号化し、暗号化したワーク鍵を含んだ受信装置個別の個別情報を生成する個別情報生成手段と、
スクランブル鍵を前記ワーク鍵で暗号化し、暗号化したスクランブル鍵を含んだ受信装置共通の共通情報を生成するとともに、外部から指示されたタイミングで、前記スクランブル鍵による復号の停止を指示する復号停止情報を前記共通情報に付加する共通情報生成手段と、
コンテンツを前記スクランブル鍵で暗号化し、暗号化コンテンツを生成するコンテンツスクランブル手段と、
前記個別情報と、前記共通情報と、前記暗号化コンテンツとを、多重化して擬似放送信号を生成する多重化手段と、を備え、
前記アクセス制御機能種別判定手段は、
前記デバイスを識別する情報であるデバイス識別と、前記復号停止情報を取得して復号を停止するまでの遅延時間とを対応付けて記憶する記憶手段と、
前記複製受信装置の表示信号を解析し、復号の停止を検出する復号停止検出手段と、
前記共通情報生成手段において前記共通情報に前記復号停止情報を付加した時点から、前記復号停止検出手段において復号の停止を検出した時点までの遅延時間を測定する遅延時間測定手段と、
この遅延時間測定手段で測定された遅延時間に対応して前記記憶手段に記憶されているデバイス識別を前記情報漏洩元のデバイスとして判定する種別判定手段と、
を備えることを特徴とする情報漏洩元特定装置。

【発明の詳細な説明】

【技術分野】

【０００１】
本発明は、デジタル放送の限定受信機能に関する秘密情報の漏洩元を特定するためのアクセス制御プログラム、送信装置、受信装置および情報漏洩元特定装置に関する。

【背景技術】

【０００２】
現行のデジタル放送では、契約者の受信装置のみに放送番組（以下、コンテンツという）を限定受信させる機能や、正規の受信装置のみにコンテンツを受信させたり、コピー制限を行ったりすることで著作権保護を行う機能を、アクセス制御方式であるＣＡＳ（Conditional Access System）を用いて実現している。
具体的には、アクセス制御に関する機能（例えば、暗号化されたコンテンツを復号するための鍵の復号等；以下、ＣＡＳ機能という）を、耐タンパモジュールであるＩＣカード（ＣＡＳカード）に実装したり、ＣＡＳプログラムとしてソフトウェア形式で受信装置に実装したりすることで、アクセス制限を行っている。

【０００３】
しかし、このＣＡＳ機能は、受信装置内部に保持する鍵（デバイス鍵等）の流出や、アルゴリズムの解析等によって、セキュリティが破られる可能性がある。すなわち、ＣＡＳ機能の秘密情報が漏洩した場合、その秘密情報を用いて不正な複製受信装置を製造することが可能になる。
このように、ＣＡＳ機能における鍵等の秘密情報が漏洩した場合、有料放送の視聴、コンテンツのコピー等におけるコンテンツを保護するための安全性が確保されず、放送サー

ビスそのものの運用継続が困難になってしまう。
【０００４】
そこで、この問題を解決するために、ＩＣカードに実装するアクセス制御に関する機能を、ＣＡＳプログラムとして受信装置に蓄積し、ＣＡＳ機能の秘密情報が漏洩した場合、放送波や通信を介してＣＡＳ機能を更新する手法が開示されている（特許文献１，２参照）。
【０００５】
例えば、特許文献１に開示された手法では、送信装置は、暗号化したＣＡＳプログラムを、コンテンツ権利保護関連の共通情報であるＥＣＭ－ＲＭＰ（ＥＣＭ：Entitlement Control Message、ＲＭＰ：Rights Management and Protection）で受信装置に伝送する。また、送信装置は、暗号化したＣＡＳプログラムを復号するための鍵を、コンテンツ権利保護関連の個別情報であるＥＭＭ－ＲＭＰ（ＥＭＭ：Entitlement Management Message）で受信装置に伝送する。
一方、受信装置は、ＥＭＭ－ＲＭＰで配信される鍵によって、ＥＣＭ－ＲＭＰで配信される暗号化されたＣＡＳプログラムをダウンロードし復号することで、ＣＡＳプログラムの蓄積、更新を行う。
【０００６】
また、特許文献２に開示された手法では、送信装置は、スクランブル鍵で暗号化したＣＡＳプログラムをデータカルーセルで伝送し、スクランブル鍵を伝送路保護鍵で暗号化し、ＥＣＭ－ＲＭＰで受信装置に伝送する。また、送信装置は、暗号化した伝送路保護鍵を、ＥＭＭ－ＲＭＰで受信装置に伝送する。
一方、受信装置は、ＥＭＭ－ＲＭＰで配信される伝送路保護鍵によって、ＥＣＭ－ＲＭＰで配信される暗号化されたスクランブル鍵を復号する。そして、受信装置は、データカルーセルで伝送されるＣＡＳプログラムをスクランブル鍵で復号することで、ＣＡＳプログラムの蓄積、更新を行う。
これによって、特許文献１，２に記載された手法では、受信装置におけるＣＡＳ機能を更新させることができる。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２００９－２６７６０５号公報
【特許文献２】特開２０１２－２３５４７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
前記したように特許文献１，２に記載された従来の手法は、受信装置からＣＡＳ機能の秘密情報が漏洩し、不正な複製受信装置が製造された場合であっても、ＣＡＳ機能を更新することで、不正な複製受信装置においてコンテンツの利用を停止させることができる。
【０００９】
しかし、従来の手法は、秘密情報の漏洩元を特定せずに、デジタル放送を受信可能な受信装置に対して、一斉に、ＣＡＳ機能を更新することになる。そのため、先に不正に複製受信装置を製造した製造元が、再度、同じ受信装置から不正に取得した秘密情報により、新たなＣＡＳ機能を複製した複製受信装置を製造する可能性がある。
すなわち、従来の手法では、不正な複製受信装置の製造とＣＡＳ機能の更新とが、繰り返されることになり、コンテンツの保護が適正に行われないという問題がある。
【００１０】
また、不正な複製受信装置が、正規の受信装置のＣＡＳ機能を完全に複製したものである場合、正規の受信装置と変わらずにＣＡＳ機能が更新されていくことになる。
すなわち、従来の手法では、単に、ＣＡＳ機能を更新することだけでは、コンテンツの保護が適正に行われない可能性があるという問題がある。

【００１１】
本発明は、このような問題に鑑みてなされたものであり、秘密情報が漏洩し不正に複製された受信装置を、デバイス（デバイス鍵）単位で特定することが可能なアクセス制御プログラム、送信装置、受信装置および情報漏洩元特定装置を提供することを課題とする。
【課題を解決するための手段】
【００１２】
前記課題を解決するため、請求項１に記載のアクセス制御プログラムは、デジタル放送の受信装置に当該受信装置のデバイスごとに組み込まれるコンテンツを限定受信するためのアクセス制御プログラムであって、暗号化されたスクランブル鍵に関連する関連情報を用いて、コンテンツを暗号化した前記スクランブル鍵を復号するために、前記受信装置のコンピュータを、個別情報処理手段、共通情報処理手段、復号停止遅延手段、として機能させることを特徴とする。
【００１３】
かかる構成において、アクセス制御プログラムは、個別情報処理手段によって、送信装置から送信された、当該受信装置固有のマスタ鍵により暗号化された鍵の関連情報である個別情報をマスタ鍵で復号し、個別情報に含まれているワーク鍵を取得する。
また、アクセス制御プログラムは、共通情報処理手段によって、送信装置から送信された、ワーク鍵により暗号化された鍵の関連情報である共通情報を個別情報処理手段で復号されたワーク鍵で復号し、共通情報に含まれているスクランブル鍵を取得する。
このスクランブル鍵によって、受信装置は、スクランブル（暗号化）されたコンテンツをデスクランブル（復号）することができる。
【００１４】
そして、アクセス制御プログラムは、復号停止遅延手段によって、共通情報にスクランブル鍵の復号停止を指示する情報が含まれている場合に、受信装置の予め定めたデバイスごとに異なるアクセス制御プログラムの遅延パラメータとして、予め当該プログラムに設定された遅延時間を計時し、その遅延時間経過後、共通情報処理手段にスクランブル鍵の復号停止を指示する。
ここで、受信装置のデバイスとは、受信装置のメーカ、機種、製造のロット等の予め定めた単位をいう。
【００１５】
これによって、当該アクセス制御プログラムが組み込まれて動作する受信装置において、共通情報でスクランブル鍵の復号停止が指示された場合、当該プログラムに設定された受信装置のデバイスごとに異なる遅延時間を経過した後に、スクランブル鍵の復号が停止され、その結果、コンテンツの復号が停止されることになる。
このように、デバイスごとに復号停止までの遅延時間が異なるアクセス制御プログラムを受信装置に組み込んでおくことで、情報漏洩によって、受信装置からアクセス制御機能が複製されて複製受信装置が生成された場合、共通情報に復号停止を指示する情報を含ませることで、デバイスごとに遅延時間が異なり、漏洩元となった受信装置のデバイスを特定することができる。
【００１６】
また、請求項２に記載の送信装置は、コンテンツおよび当該コンテンツを暗号化した鍵に関連する関連情報と、当該コンテンツを限定受信するためのアクセス制御プログラムおよび当該アクセス制御プログラムを暗号化した鍵に関連する関連情報とを、受信装置に送信するデジタル放送の送信装置であって、第１個別情報生成手段と、第１共通情報生成手段と、コンテンツスクランブル手段と、第２個別情報生成手段と、第２共通情報生成手段と、プログラムスクランブル手段と、多重化手段と、を備える構成とした。
【００１７】
かかる構成において、送信装置は、第１個別情報生成手段によって、第１ワーク鍵を受信装置個別のマスタ鍵で暗号化し、暗号化した第１ワーク鍵を含んだ受信装置個別の第１個別情報を生成する。そして、送信装置は、第１共通情報生成手段によって、第１スクラ

ンブル鍵を第１ワーク鍵で暗号化し、暗号化した第１スクランブル鍵を含んだ受信装置共通の第１共通情報を生成する。そして、送信装置は、コンテンツスクランブル手段によって、コンテンツを第１スクランブル鍵で暗号化し、暗号化コンテンツを生成する。

【００１８】

また、送信装置は、第２個別情報生成手段によって、受信装置の予め定めたデバイスごとに、第２ワーク鍵を当該デバイスごとのデバイス鍵で暗号化し、暗号化した第２ワーク鍵を含んだ受信装置のデバイス個別の第２個別情報を生成する。そして、送信装置は、第２共通情報生成手段によって、第２スクランブル鍵を第２ワーク鍵で暗号化し、暗号化した第２スクランブル鍵を含んだ受信装置共通の第２共通情報を生成する。

そして、送信装置は、プログラムスクランブル手段によって、受信装置のデバイスごとに予め異なる遅延時間を遅延パラメータとして組み込んだアクセス制御プログラムを第２スクランブル鍵で暗号化し、暗号化アクセス制御プログラムを生成する。

【００１９】

そして、送信装置は、多重化手段によって、第１個別情報と、第１共通情報と、暗号化コンテンツと、第２個別情報と、第２共通情報と、暗号化アクセス制御プログラムとを多重化し、放送信号を生成する。

これによって、送信装置は、受信装置のデバイスごとに、復号停止を指示してから復号停止までの遅延時間が異なるアクセス制御機能を有するアクセス制御プログラムを、受信装置に組み込むことができる。

【００２０】

また、請求項３に記載の受信装置は、コンテンツを暗号化した暗号化コンテンツと、前記コンテンツを暗号化した第１スクランブル鍵を含んだ受信装置共通の第１共通情報と、前記第１スクランブル鍵を暗号化した第１ワーク鍵を含んだ受信装置個別の第１個別情報と、前記コンテンツを限定受信するためのアクセス制御プログラムを暗号化した暗号化アクセス制御プログラムと、前記アクセス制御プログラムを暗号化した第２スクランブル鍵を含んだ受信装置共通の第２共通情報と、前記第２スクランブル鍵を暗号化した第２ワーク鍵を含んだ受信装置のデバイスごとに個別の第２個別情報とを多重化した放送信号を、送信装置から受信するデジタル放送の受信装置であって、分離手段と、第２個別情報処理手段と、第２共通情報処理手段と、プログラムデスクランブル手段と、アクセス制御手段と、を備え、アクセス制御手段は、プログラムデスクランブル手段で取得したアクセス制御プログラムの動作により、第１個別情報処理手段と、第１共通情報処理手段と、復号停止遅延手段として機能する構成とした。

【００２１】

かかる構成において、受信装置は、分離手段によって、多重化された放送信号を分離する。

そして、受信装置は、第２個別情報処理手段によって、分離手段で分離された第２個別情報を当該受信装置の予め定めたデバイス単位の鍵であるデバイス鍵で復号し、第２ワーク鍵を取得する。また、受信装置は、第２共通情報処理手段によって、分離手段で分離された第２共通情報を第２個別情報処理手段で復号された第２ワーク鍵で復号し、第２スクランブル鍵を取得する。

【００２２】

そして、受信装置は、プログラムデスクランブル手段によって、分離手段で分離された暗号化アクセス制御プログラムを第２共通情報処理手段で復号された第２スクランブル鍵で復号し、アクセス制御プログラムを取得する。そして、受信装置は、アクセス制御手段によって、アクセス制御プログラムを動作させる。

そして、受信装置は、第１個別情報処理手段によって、分離手段で分離された第１個別情報を当該受信装置個別の鍵であるマスタ鍵で復号し、第１ワーク鍵を取得する。また、受信装置は、第１共通情報処理手段によって、分離手段で分離された第１共通情報を第１個別情報処理手段で復号された第１ワーク鍵で復号し、第１スクランブル鍵を取得する。

【００２３】

そして、受信装置は、復号停止遅延手段によって、第１共通情報に第１スクランブル鍵の復号停止を指示する情報が含まれている場合に、予め遅延パラメータとして定めた遅延時間を計時し、その遅延時間経過後、第１共通情報処理手段に第１スクランブル鍵の復号停止を指示する。

これによって、受信装置は、コンテンツを復号するスクランブル鍵の復号停止が指示された場合に、予めデバイスごとに定めた遅延時間経過後、復号を停止するアクセス制御機能が組み込まれることになる。

【００２４】

また、請求項４に記載の情報漏洩元特定装置は、スクランブル鍵の復号停止を指示されてから実際に復号停止を行うまでの遅延時間が受信装置のデバイスごとに異なるアクセス制御プログラムを組み込んだ受信装置から複製された複製受信装置が、前記デバイスのうちいずれのデバイスからの情報漏洩により複製されたものかを特定する情報漏洩元特定装置であって、擬似放送信号生成手段と、アクセス制御機能種別判定手段と、を備え、擬似放送信号生成手段が、個別情報生成手段と、共通情報生成手段と、コンテンツスクランブル手段と、多重化手段と、を備え、アクセス制御機能種別判定手段が、記憶手段と、復号停止検出手段と、遅延時間測定手段と、種別判定手段と、を備える構成とした。

【００２５】

かかる構成において、情報漏洩元特定装置は、個別情報生成手段によって、ワーク鍵を受信装置個別のマスタ鍵で暗号化し、暗号化したワーク鍵を含んだ受信装置個別の個別情報を生成する。また、情報漏洩元特定装置は、共通情報生成手段によって、スクランブル鍵をワーク鍵で暗号化し、暗号化したスクランブル鍵を含んだ受信装置共通の共通情報を生成するとともに、外部から指示されたタイミングで、スクランブル鍵による復号の停止を指示する復号停止情報を共通情報に付加する。

また、情報漏洩元特定装置は、コンテンツスクランブル手段によって、コンテンツをスクランブル鍵で暗号化し、暗号化コンテンツを生成する。

そして、情報漏洩元特定装置は、多重化手段によって、個別情報と、共通情報と、暗号化コンテンツとを、多重化して擬似放送信号を生成する。

これによって、情報漏洩元特定装置は、暗号化コンテンツと当該暗号化コンテンツを復号するための鍵関連情報とを含んだ擬似放送信号を生成するとともに、当該擬似放送信号を介して、複製受信装置にコンテンツの復号停止を指示することができる。

【００２６】

一方、情報漏洩元特定装置は、復号停止検出手段によって、複製受信装置の表示信号を解析し、復号の停止を検出する。そして、情報漏洩元特定装置は、遅延時間測定手段によって、共通情報生成手段において共通情報に復号停止情報を付加した時点から、復号停止検出手段において復号の停止を検出した時点までの遅延時間を測定する。

そして、情報漏洩元特定装置は、種別判定手段によって、遅延時間測定手段で測定された遅延時間に対応して予め記憶手段に記憶されているデバイス識別を情報漏洩元のデバイスとして判定する。

このように、復号停止までの遅延時間は、受信装置のデバイスごとに異なるため、情報漏洩元特定装置は、その遅延時間を測定することで、どのデバイスの情報が漏洩して複製受信装置が生成されたのかを特定することができる。

【発明の効果】

【００２７】

本発明は、以下に示す優れた効果を奏するものである。

請求項１に記載の発明によれば、スクランブル鍵の復号停止までの遅延時間として、受信装置のデバイスごとに予め異なる時間が設定されているため、スクランブル鍵の復号を停止させる旨が指示された場合に、受信装置のデバイスごとで異なるアクセス制御を実現することができる。これによって、受信装置の情報漏洩に伴いアクセス制御機能が複製された場合であっても、復号停止までの遅延時間の相違によって、漏洩元のデバイスを特定することができる。

【００２８】
請求項２，３に記載の発明によれば、受信装置のデバイス単位でスクランブル鍵の復号停止までの遅延時間が異なるアクセス制御プログラムを、デバイス単位で受信装置に組み込むことができる。これによって、受信装置の情報漏洩に伴いアクセス制御機能が複製された場合であっても、漏洩元のデバイスを特定することができる。
【００２９】
請求項４に記載の発明によれば、受信装置のアクセス制御機能を複製した複製受信装置に対して、コンテンツ（スクランブル鍵）の復号を停止させることができ、さらに、その停止までの遅延時間を計時することで、遅延時間に対応するデバイスを特定することができる。
【図面の簡単な説明】
【００３０】
【図１】本発明の概要を説明するための説明図であって、（ａ）はデバイス鍵ごとに異なるアクセス制御プログラム（ＣＡＳプログラム）を配信する様子を説明するための図、（ｂ）は不正に複製された受信装置から情報漏洩元を特定する仕組みを説明するための図である。
【図２】本発明の実施形態に係る送信装置の構成を示す構成図である。
【図３】本発明の実施形態に係るアクセス制御プログラムの機能ブロックを示す構成図である。
【図４】復号停止情報を含んだ共通情報のデータフォーマットの一例を示す図である。
【図５】本発明の実施形態に係る受信装置の構成を示す構成図である。
【図６】本発明の実施形態に係る送信装置のアクセス制御プログラム（ＣＡＳプログラム）を送信する動作を示すフローチャートである。
【図７】本発明の実施形態に係る送信装置のコンテンツを送信する動作を示すフローチャートである。
【図８】本発明の実施形態に係る受信装置のアクセス制御プログラム（ＣＡＳプログラム）を受信する動作を示すフローチャートである。
【図９】本発明の実施形態に係る受信装置のコンテンツを受信する動作を示すフローチャートである。
【図１０】本発明の実施形態に係るアクセス制御プログラムのアクセス制御機能（ＣＡＳ機能）の動作を示すフローチャートである。
【図１１】本発明の実施形態に係る情報漏洩元特定装置の構成を示す構成図である。
【発明を実施するための形態】
【００３１】
以下、本発明の実施形態について図面を参照して説明する。
［本発明の概要］
最初に、図１を参照して、本発明の概要について説明する。
本発明は、アクセス制御に関する機能（以下、ＣＡＳ機能という）を実行させるアクセス制御プログラム（以下、ＣＡＳプログラムという）を、受信装置のデバイスごとに異なるプログラムで作成しておき、不正に複製された複製受信装置が発見された際に、当該複製受信装置が、どのデバイスから複製されたものかを検出することを特徴とする。
すなわち、本発明では、図１（ａ）に示すように、送信装置１が、受信装置２のデバイスごと（例えば、受信装置のメーカごと）に異なるＣＡＳ機能を有するＣＡＳプログラム（ＣＡＳ－Ｐ Ａ，ＣＡＳ－Ｐ Ｂ，ＣＡＳ－Ｐ Ｃ，…）を、デバイス（デバイス鍵）単位で暗号化して、受信装置２（２_{1}，２_{2}，２_{3}，…）に送信する。
【００３２】
一方、受信装置２は、受信装置メーカ等のデバイス単位で予め付与されているデバイス鍵を備え、そのデバイス（デバイス鍵）単位で、自身宛のＣＡＳプログラムを復号する。
これによって、受信装置２では、それぞれのデバイス単位で異なるＣＡＳ機能（ＣＡＳ機能Ａ，ＣＡＳ機能Ｂ，ＣＡＳ機能Ｃ，…）が機能することになる。

ここで、ＣＡＳプログラムは、一般的なＣＡＳ機能に加え、放送信号によってコンテンツの復号を停止する機能を有する。また、ＣＡＳプログラムは、受信装置２のデバイス（デバイス鍵）ごとに異なる機能として、コンテンツの復号停止を指示されてから、実際に復号を停止するまでの時間が異なるものとする。

これによって、受信装置２は、コンテンツの復号停止が指示された場合に、デバイスごとのＣＡＳ機能によって異なる時間で、コンテンツの復号が停止されることになる。

【００３３】

ここで、不正に複製された複製受信装置２Ｂが発見された場合、本発明では、図１（ｂ）に示すように、情報漏洩元特定装置３によって、どのＣＡＳ機能を有する受信装置２から秘密情報が漏洩して複製受信装置２Ｂが複製されたのかを検出する。

すなわち、情報漏洩元特定装置３は、コンテンツの復号停止を放送ストリーム（放送信号）として擬似的に生成し、復号停止を指示した後、複製受信装置２Ｂが実際に復号を停止するまで（すなわち、映像音声断まで）の時間を測定する。

この復号停止指示後から実際に復号を停止するまでの時間は、ＣＡＳ機能（デバイス）ごとに異なるため、情報漏洩元特定装置３は、どのＣＡＳ機能を有する受信装置２から秘密情報が漏洩したのかを特定することができる。

以下、本発明の実施形態に係る送信装置１、受信装置２および情報漏洩元特定装置３について詳細に説明する。

【００３４】

［送信装置の構成］

まず、図２を参照（適宜図１参照）して、送信装置１の構成について説明する。

送信装置１は、放送波を介して、コンテンツ（放送番組）を受信装置２に送信するものである。なお、この送信装置１は、放送波を介して、コンテンツへのアクセス制御に関する機能を有するＣＡＳプログラムを送信し、更新する機能を有する。

【００３５】

ここでは、送信装置１は、記憶手段１０と、コンテンツスクランブル手段１１と、第１共通情報生成手段１２と、第１個別情報生成手段１３と、プログラムスクランブル手段１４と、第２共通情報生成手段１５と、第２個別情報生成手段１６と、多重化手段１７と、を備える。

【００３６】

記憶手段１０は、コンテンツやＣＡＳプログラムをスクランブル／デスクランブルするための鍵、それに関連する関連情報を生成するための鍵、および、受信装置２に配信するＣＡＳプログラムＰを記憶するものである。例えば、この記憶手段１０は、ハードディスク等の記憶媒体で構成される。

スクランブル鍵Ｋｓ１、ワーク鍵Ｋｗ１およびマスタ鍵Ｋｍは、コンテンツＣを限定受信するための鍵およびそれに関連する関連情報を生成するための鍵である。

【００３７】

具体的には、スクランブル鍵Ｋｓ１は、コンテンツＣをスクランブルする鍵である。このスクランブル鍵Ｋｓ１は、数秒に１回程度更新され、ここでは、適宜外部から新たなスクランブル鍵Ｋｓ１が入力されることで更新されるものとする。

このスクランブル鍵Ｋｓ１は、コンテンツＣをスクランブルする際に、コンテンツスクランブル手段１１で用いられる。

【００３８】

ワーク鍵Ｋｗ１は、スクランブル鍵Ｋｓ１を暗号化する鍵である。このワーク鍵Ｋｗ１は、スクランブル鍵Ｋｓ１に比べ、更新時間が長く、例えば、１ヶ月程度で更新される。ここでは、適宜外部から新たなワーク鍵Ｋｗ１が入力されることで更新されるものとする。このワーク鍵Ｋｗ１は、受信装置２に共通の鍵関連情報としてスクランブル鍵Ｋｓ１を設定する第１共通情報を暗号化する鍵であって、第１共通情報生成手段１２で用いられる。

【００３９】

マスタ鍵Ｋｍは、ワーク鍵Ｋｗ１を暗号化する鍵である。このマスタ鍵Ｋｍは、受信装置２ごとに異なる予め個々の受信装置２に付与されている固定の鍵である。
このマスタ鍵Ｋｍは、受信装置２ごとに個別の鍵関連情報としてワーク鍵Ｋｗ１を設定する第１個別情報を暗号化する鍵であって、第１個別情報生成手段１３で用いられる。
【００４０】
スクランブル鍵Ｋｓ２、ワーク鍵Ｋｗ２およびデバイス鍵Ｋｄは、ＣＡＳプログラムＰを暗号伝送するための鍵およびそれに関連する関連情報を生成するための鍵である。
具体的には、スクランブル鍵Ｋｓ２は、ＣＡＳプログラムＰをスクランブルする鍵である。このスクランブル鍵Ｋｓ２は、数秒に１回程度更新され、ここでは、適宜外部から新たなスクランブル鍵Ｋｓ２が入力されることで更新されるものとする。
【００４１】
ワーク鍵Ｋｗ２は、スクランブル鍵Ｋｓ２を暗号化する鍵である。このワーク鍵Ｋｗ２は、スクランブル鍵Ｋｓ２に比べ、更新時間が長く、例えば、１ヶ月程度で更新される。ここでは、適宜外部から新たなワーク鍵Ｋｗ２が入力されることで更新されるものとする。このワーク鍵Ｋｗ２は、受信装置２のデバイスごと（例えば、受信装置のメーカごと）に共通の鍵関連情報としてスクランブル鍵Ｋｓ２を設定する第２共通情報を暗号化する鍵であって、第２共通情報生成手段１５で用いられる。なお、デバイスは、予め固有の識別子（デバイス識別）で区別されるものとする。
【００４２】
デバイス鍵Ｋｄは、ワーク鍵Ｋｗ２を暗号化する鍵である。このデバイス鍵Ｋｄは、受信装置２のデバイスごとに異なる鍵であって、デバイス単位で予め受信装置２に付与されている固定の鍵である。このデバイス単位とは、受信装置２を認証するための予め定めた単位であって、例えば、受信装置のメーカごと、機種ごと、ロットごと等である。ここでは、デバイス鍵Ｋｄは、デバイス識別に対応付けて記憶手段１０に記憶しておく。
このデバイス鍵Ｋｄは、受信装置２のデバイスごとに個別の鍵関連情報としてワーク鍵Ｋｗ２を設定する第２個別情報を暗号化する鍵であって、第２個別情報生成手段１６で用いられる。
【００４３】
ＣＡＳプログラムＰは、受信装置２において、ＣＡＳ機能を動作させるためのプログラムである。具体的には、ＣＡＳプログラムＰは、送信装置１から送信されるスクランブル鍵Ｋｓ１の関連情報（第１共通情報、第１個別情報）に基づいて、放送ストリーム（放送信号）からスクランブル鍵Ｋｓ１を抽出する。このＣＡＳプログラムＰは、受信装置２のデバイス（デバイス識別〔デバイス鍵〕）単位で実装されるプログラムであって、予めデバイス識別に対応付けて記憶手段１０に記憶しておく。
【００４４】
ここでは、ＣＡＳプログラムＰは、放送信号を介して、コンテンツＣに対応するスクランブル鍵Ｋｓ１の抽出を停止させる旨の指示（復号停止情報）を通知された段階で、デバイス単位のＣＡＳプログラムＰで異なる予め定めた時間経過後に、スクランブル鍵Ｋｓ１の抽出を停止する機能を有する。
なお、ＣＡＳプログラムＰは、ＯＳ（Operating System）上で動作するソフトウェアとして構成してもよいし、ＦＰＧＡ（Field Programmable Gate Array）等のプログラマブルデバイス上で動作する回路情報で構成してもよい。
このＣＡＳプログラムＰの詳細な機能ブロックについては、後で図３を参照して説明することとする。
【００４５】
コンテンツスクランブル手段１１は、入力されたコンテンツ（映像、音声、データ等）Ｃをスクランブル鍵Ｋｓ１でスクランブル（暗号化）するものである。
このスクランブル鍵Ｋｓ１による暗号化は、一般的な共通鍵暗号アルゴリズムを用いればよく、例えば、ＭＵＬＴＩ２暗号により暗号化する。コンテンツスクランブル手段１１は、スクランブルしたコンテンツ（暗号化コンテンツＳＣ）を、多重化手段１７に出力す

る。

【００４６】

第１共通情報生成手段１２は、コンテンツスクランブル手段１１で用いるスクランブル鍵Ｋｓ１をワーク鍵Ｋｗ１で暗号化し、暗号化したスクランブル鍵Ｋｓ１を含んだ共通情報（第１共通情報）を生成するものである。このワーク鍵Ｋｗ１による暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。

ここで、第１共通情報は、すべての受信装置２に共通の情報である。この第１共通情報は、社団法人電波産業会（ＡＲＩＢ）のＳＴＤ－Ｂ２５の限定受信方式（ＣＡＳ方式）で規定されているＥＣＭ（Entitlement Control Message）構造を有するメッセージとして生成することができる。ここでは、第１共通情報生成手段１２は、ＥＣＭとして生成した第１共通情報（ＥＣＭ－ＣＡＳ）を、多重化手段１７に出力する。

【００４７】

第１個別情報生成手段１３は、第１共通情報生成手段１２で用いるワーク鍵Ｋｗ１をマスタ鍵Ｋｍ１で暗号化し、暗号化したワーク鍵Ｋｗ１を含んだ個別情報（第１個別情報）を生成するものである。このマスタ鍵Ｋｍ１による暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。

ここで、第１個別情報は、受信装置２ごとに個別の情報である。この第１個別情報は、ＡＲＩＢ　ＳＴＤ－Ｂ２５の限定受信方式（ＣＡＳ方式）で規定されているＥＭＭ（Entitlement Management Message）構造を有するメッセージとして生成することができる。ここでは、第１個別情報生成手段１３は、ＥＭＭとして生成した第１個別情報（ＥＭＭ－ＣＡＳ）を、多重化手段１７に出力する。

【００４８】

プログラムスクランブル手段１４は、ＣＡＳプログラムＰをスクランブル鍵Ｋｓ２でスクランブル（暗号化）するものである。このスクランブル鍵Ｋｓ２による暗号化は、一般的な共通鍵暗号アルゴリズムを用いればよい。また、プログラムスクランブル手段１４は、ＣＡＳプログラムＰをスクランブルした暗号化プログラムＳＰを生成する際に、ＣＡＳプログラムＰを識別するための識別子を付加しておくこととする。

また、プログラムスクランブル手段１４は、受信装置２のデバイス単位で異なるＣＡＳプログラムＰを順次記憶手段１０から読み出してスクランブルすることとする。

このプログラムスクランブル手段１４は、スクランブルしたプログラム（暗号化プログラムＳＰ）を、多重化手段１７に出力する。

なお、プログラムスクランブル手段１４は、予め定めたブロック単位でＣＡＳプログラムＰをスクランブルし、データカルーセルの形式で多重化手段１７に出力することとしてもよい。

【００４９】

第２共通情報生成手段１５は、プログラムスクランブル手段１４で用いるスクランブル鍵Ｋｓ２をワーク鍵Ｋｗ２で暗号化し、暗号化したスクランブル鍵Ｋｓ２を含んだ共通情報（第２共通情報）を生成するものである。このワーク鍵Ｋｗ２による暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。

ここで、第２共通情報は、すべての受信装置２に共通の情報である。この第２共通情報は、ＡＲＩＢ　ＳＴＤ－Ｂ２５のコンテンツ保護方式（ＲＭＰ方式）で規定されているＥＣＭ構造を有するメッセージとして生成することができる。ここでは、第２共通情報生成手段１５は、ＥＣＭとして生成した第２共通情報（ＥＣＭ－ＲＭＰ）を、多重化手段１７に出力する。

【００５０】

第２個別情報生成手段１６は、第２共通情報生成手段１５で用いるワーク鍵Ｋｗ２をデバイス鍵Ｋｄで暗号化し、暗号化したワーク鍵Ｋｗ２を含んだ個別情報（第２個別情報）を生成するものである。このデバイス鍵Ｋｄによる暗号化には、一般的な共通鍵暗号アルゴリズムを用いればよい。

ここで、第２個別情報は、受信装置２のデバイス（受信装置２のメーカ等）ごとに個別

の情報である。この第２個別情報は、ＡＲＩＢ　ＳＴＤ－Ｂ２５のコンテンツ保護方式（ＲＭＰ方式）で規定されているＥＭＭ構造を有するメッセージとして生成することができる。なお、第２個別情報生成手段１６は、プログラムスクランブル手段１４がスクランブルするＣＡＳプログラムＰと同じデバイス識別に対応するデバイス鍵Ｋｄでワーク鍵Ｋｗ２を暗号化する。

ここでは、第２個別情報生成手段１６は、ＥＭＭとして生成した第２個別情報（ＥＭＭ－ＲＭＰ）を、多重化手段１７に出力する。

【００５１】

多重化手段１７は、コンテンツスクランブル手段１１が生成した暗号化コンテンツＳＣと、第１共通情報生成手段１２が生成した第１共通情報（ＥＣＭ－ＣＡＳ）と、第１個別情報生成手段１３が生成した第１個別情報（ＥＭＭ－ＣＡＳ）と、プログラムスクランブル手段１４が生成した暗号化プログラムＳＰと、第２共通情報生成手段１５が生成した第２共通情報（ＥＣＭ－ＲＭＰ）と、第２個別情報生成手段１６が生成した第２個別情報（ＥＭＭ－ＲＭＰ）とを、それぞれ入力された段階で多重化して、多重化信号を生成するものである。

【００５２】

ここでは、多重化手段１７は、入力された各情報を、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓで定義されるＴＳ（トランスポートストリーム）の形式（ＭＰＥＧ－２　ＴＳ）に多重化するものとする。

なお、ここでは図示を省略するが、多重化手段１７は、これらの情報以外にも、番組配列情報であるＰＳＩ（Program Specific Information）／ＳＩ（Service Information）の情報テーブル等を適宜多重化することはいうまでもない。また、送信装置１は、ＣＡＳプログラムＰを指定して動作させたい場合、ＰＳＩ／ＳＩにプログラム指定情報として、プログラムスクランブル手段１４で暗号化プログラムＳＰに付加して受信装置２に送信したＣＡＳプログラムＰの識別子を付加すればよい。

【００５３】

このように送信装置１を構成することで、送信装置１は、コンテンツＣの復号停止が指示されてから実際に復号を停止するまでの時間が、受信装置２のデバイス単位で異なる時間となるように、受信装置２のデバイス単位でＣＡＳプログラムＰを更新させることができる。

【００５４】

〔ＣＡＳプログラムの構成〕

次に、図３を参照（適宜図２参照）して、送信装置１が配信するＣＡＳプログラム（アクセス制御プログラム）の構成について説明する。

図３の機能ブロックとして示すように、ＣＡＳプログラムＰは、受信装置２のコンピュータを、第１個別情報処理手段２１、第１共通情報処理手段２２、復号停止遅延手段２３、として機能させるためのプログラムである。

【００５５】

第１個別情報処理手段（個別情報処理手段）２１は、放送ストリームに多重化されている第１個別情報（ＥＭＭ－ＣＡＳ）とマスタ鍵Ｋｍとを入力し、第１個別情報をマスタ鍵Ｋｍで復号し、ワーク鍵Ｋｗ１を取得するものである。この第１個別情報処理手段２１は、復号したワーク鍵Ｋｗ１を、第１共通情報処理手段２２に出力する。

【００５６】

第１共通情報処理手段（共通情報処理手段）２２は、放送ストリームに多重化されている第１共通情報（ＥＣＭ－ＣＡＳ）と第１個別情報処理手段２１で復号されたワーク鍵Ｋｗ１とを入力し、第１共通情報をワーク鍵Ｋｗ１で復号し、スクランブル鍵Ｋｓ１を取得するものである。この第１共通情報処理手段２２は、復号したスクランブル鍵Ｋｓ１をＣＡＳプログラムＰの出力結果として出力する。

ただし、第１共通情報処理手段２２は、第１共通情報に復号停止情報が含まれている場合、復号停止情報を検出した旨の通知（復号停止検出通知）を復号停止遅延手段２３に出

力する。そして、第１共通情報処理手段２２は、復号停止遅延手段２３から、復号停止指示を入力した以降は、スクランブル鍵Ｋｓ１の出力を停止する。

【００５７】

ここで、第１共通情報（ＥＣＭ－ＣＡＳ）は、図４に示すように、ＥＣＭ構造を有している。なお、図４中、本発明と直接関係のない情報は省略している。

図４に示すように、ＥＣＭセクションヘッダに続く、ＥＣＭ本体の固定部にスクランブル鍵が暗号化されて格納される。ここでは、適宜更新されるスクランブル鍵のうち、現在と次のスクランブル鍵を２つ（Ｏｄｄ／Ｅｖｅｎ）示している。

また、図４に示すように、ＥＣＭ本体の可変部に必要に応じて復号停止情報が格納される。この可変部に復号停止情報が設定されている場合に、第１共通情報処理手段２２は、復号停止遅延手段２３に復号停止検出通知を出力する。

この復号停止情報は、例えば、当該情報が復号停止情報であることを示す予め定めた固有の識別子である。

【００５８】

復号停止遅延手段２３は、第１共通情報処理手段２２から、復号停止検出通知を入力した段階で、遅延パラメータとして予め設定されている遅延時間経過後に、復号停止指示を出力するものである。この復号停止遅延手段２３は、図示を省略したタイマ（計時手段）によって遅延時間を計時する。なお、遅延パラメータ（遅延時間）は、予めＣＡＳプログラムＰ内部に埋め込まれている、受信装置２に付与されているデバイス鍵ごとに異なる時間である。

これによって、ＣＡＳプログラムＰは、受信装置２に配信された後に、第１共通情報で復号停止情報が通知された場合、内部に埋め込まれている遅延時間経過後、スクランブル鍵Ｋｓ１の出力を停止する。

【００５９】

［受信装置の構成］

次に、図５を参照（適宜図１参照）して、受信装置２の構成について説明する。

受信装置２は、放送波を介して、コンテンツ（放送番組）を送信装置１から受信するものである。なお、この受信装置２は、放送波を介して、コンテンツへのアクセス制御に関する機能を有するＣＡＳプログラムを受信し、更新する機能を有する。

【００６０】

ここでは、受信装置２は、第１個別情報処理手段２１、第１共通情報処理手段２２および復号停止遅延手段２３を備えたアクセス制御手段２０と、分離手段２４と、記憶手段２５と、第２個別情報処理手段２６と、第２共通情報処理手段２７と、プログラムデスクランブル手段２８と、コンテンツデスクランブル手段２９と、を備える。

【００６１】

アクセス制御手段２０は、送信装置１から送信されたコンテンツへのアクセスを制御するものである。このアクセス制御手段２０は、送信装置１から送信されるＣＡＳプログラムＰを受信装置２内の不揮発性メモリにロードして、プログラムを実行することで、ＣＡＳ機能を実現する。

すなわち、アクセス制御手段２０は、図３で説明したＣＡＳプログラムＰと同様に、第１個別情報処理手段２１と、第１共通情報処理手段２２と、復号停止遅延手段２３と、を備えることになる。この個々の構成は、図３で説明したＣＡＳプログラムＰと同じものであるため、説明を省略する。

【００６２】

なお、第１個別情報処理手段２１に入力される第１個別情報（ＥＭＭ－ＣＡＳ）は、分離手段２４によって放送ストリームから分離された情報である。また、第１個別情報処理手段２１に入力されるマスタ鍵Ｋｍは、記憶手段２５に予め記憶されている受信装置２に固有の鍵である。

また、第１共通情報処理手段２２に入力される第１共通情報（ＥＣＭ－ＣＡＳ）は、分離手段２４によって放送ストリームから分離された情報である。また、第１共通情報処理

手段２２が出力するスクランブル鍵Ｋｓ１は、コンテンツデスクランブル手段２９に出力される。

【００６３】

分離手段２４は、送信装置１から送信された放送ストリーム（多重化信号；ＭＰＥＧ－２　ＴＳ）を分離するものである。この分離手段２４は、ＭＰＥＧ－２　ＴＳから、暗号化コンテンツＳＣと、限定受信用の関連情報を含んだ第１個別情報（ＥＭＭ－ＣＡＳ）および第１共通情報（ＥＣＭ－ＣＡＳ）と、ＣＡＳプログラムの暗号伝送用の関連情報を含んだ第２個別情報（ＥＭＭ－ＲＭＰ）および第２共通情報（ＥＣＭ－ＲＭＰ）と、暗号化ＣＡＳプログラムＳＰと、を分離する。

【００６４】

記憶手段２５は、限定受信用の関連情報やＣＡＳプログラムの暗号伝送用の関連情報を復号するための鍵を記憶するものである。例えば、この記憶手段２５は、半導体メモリ等の記憶媒体で構成される。

ここでは、記憶手段２５は、限定受信用の関連情報を復号するための鍵であるマスタ鍵Ｋｍと、ＣＡＳプログラムの暗号伝送用の関連情報を復号するための鍵であって、固有の識別子（デバイス識別）で特定されるデバイス鍵Ｋｄとを、予め記憶している。

なお、マスタ鍵Ｋｍは、受信装置２ごとに異なる予め個々の受信装置２に付与されている固定の鍵である。また、デバイス鍵Ｋｄは、受信装置２のデバイスごとに異なる鍵であって、デバイス（デバイス識別）単位で予め受信装置２に付与されている固定の鍵である。

【００６５】

第２個別情報処理手段２６は、分離手段２４で分離された第２個別情報（ＥＭＭ－ＲＭＰ）を、記憶手段２５に予め記憶されているデバイス鍵Ｋｄで復号し、ワーク鍵Ｋｗ２を取得するものである。この第２個別情報処理手段２６は、復号したワーク鍵Ｋｗ２を、第２共通情報処理手段２７に出力する。

【００６６】

第２共通情報処理手段２７は、分離手段２４で分離された第２共通情報（ＥＣＭ－ＲＭＰ）を、第２個別情報処理手段２６で復号されたワーク鍵Ｋｗ２で復号し、スクランブル鍵Ｋｓ２を取得するものである。この第２共通情報処理手段２７は、復号したスクランブル鍵Ｋｓ２を、プログラムデスクランブル手段２８に出力する。

【００６７】

プログラムデスクランブル手段２８は、分離手段２４で分離抽出された暗号化ＣＡＳプログラムＳＰを、第２共通情報処理手段２７で復号されたスクランブル鍵Ｋｓ２でデスクランブル（復号）するものである。

このプログラムデスクランブル手段２８は、デスクランブルしたＣＡＳプログラムＰを、受信装置２内の図示を省略した不揮発性メモリにロードして、動作させる。

【００６８】

なお、より具体的には、プログラムデスクランブル手段２８が、ＣＡＳプログラムＰを記憶手段２５に記憶した後、アクセス制御手段２０が、ＰＳＩ／ＳＩにより、ＣＡＳプログラムＰの識別子を含んだプログラム指定情報を通知された段階で、不揮発性メモリにロードし、実行させる。

【００６９】

コンテンツデスクランブル手段２９は、分離手段２４で分離抽出された暗号化コンテンツＳＣを、アクセス制御手段２０（ＣＡＳプログラムＰ）の第１共通情報処理手段２２から出力されるスクランブル鍵Ｋｓ１でデスクランブル（復号）するものである。

このコンテンツデスクランブル手段２９は、デスクランブルしたコンテンツＣを外部に出力する。これによって、外部に接続された表示装置（不図示）によって、コンテンツが再生されることになる。

【００７０】

このように受信装置２を構成することで、受信装置２は、デバイス単位で配信されたＣ

ＡＳプログラムＰによって、コンテンツＣの復号停止が指示されてから実際に復号を停止するまでの時間を、受信装置２のデバイス単位で異なる時間となるように制御することできる。

【００７１】

［送信装置および受信装置の動作］

次に、図６～図１０を参照して、送信装置１および受信装置２の動作について説明する。

【００７２】

〔送信装置の動作：ＣＡＳプログラム送信〕

最初に、図６を参照（構成については適宜図２参照）して、送信装置１のＣＡＳプログラム送信動作について説明する。

まず、送信装置１は、第２個別情報生成手段１６によって、スクランブルするＣＡＳプログラムＰと同じデバイス（デバイス識別）に対応するデバイス鍵Ｋｄで、ワーク鍵Ｋｗ２を暗号化し、暗号化したワーク鍵Ｋｗ２を含んだ個別情報（第２個別情報）を生成する（ステップＳ１）。

そして、送信装置１は、第２共通情報生成手段１５によって、ＣＡＳプログラムＰをスクランブルするスクランブル鍵Ｋｓ２を、ワーク鍵Ｋｗ２で暗号化し、暗号化したスクランブル鍵Ｋｓ２を含んだ共通情報（第２共通情報）を生成する（ステップＳ２）。

【００７３】

さらに、送信装置１は、プログラムスクランブル手段１４によって、デバイス単位のＣＡＳプログラムＰを記憶手段１０から読み出し、スクランブル鍵Ｋｓ２でスクランブルする（ステップＳ３）。

そして、送信装置１は、多重化手段１７によって、ステップＳ１で生成された第２個別情報（ＥＭＭ－ＲＭＰ）と、ステップＳ２で生成された第２共通情報（ＥＣＭ－ＲＭＰ）と、ステップＳ３でスクランブルされた暗号化プログラムＳＰとを多重化して、多重化信号（放送ストリーム）を生成する（ステップＳ４）。

【００７４】

なお、ここでは、ＣＡＳプログラム送信動作を一連の動作として説明したが、第２個別情報や第２共通情報は、ワーク鍵Ｋｗ２やスクランブル鍵Ｋｓ２が更新されるタイミングで生成され、多重化手段１７によって多重化される。

送信装置１は、以上の動作をデバイス単位のＣＡＳプログラムＰごとに行う。これによって、送信装置１は、受信装置２に対してデバイス単位で異なるＣＡＳプログラムＰを送信することができる。

【００７５】

〔送信装置の動作：コンテンツ送信〕

次に、図７を参照（構成については適宜図２参照）して、送信装置１のコンテンツ送信動作について説明する。

まず、送信装置１は、第１個別情報生成手段１３によって、受信装置２ごとのマスタ鍵Ｋｍで、ワーク鍵Ｋｗ１を暗号化し、暗号化したワーク鍵Ｋｗ１を含んだ個別情報（第１個別情報）を生成する（ステップＳ１１）。

そして、送信装置１は、第１共通情報生成手段１２によって、コンテンツＣをスクランブルするスクランブル鍵Ｋｓ１を、ワーク鍵Ｋｗ１で暗号化し、暗号化したスクランブル鍵Ｋｓ１を含んだ共通情報（第１共通情報）を生成する（ステップＳ１２）。

【００７６】

さらに、送信装置１は、コンテンツスクランブル手段１１によって、コンテンツＣを、スクランブル鍵Ｋｓ１でスクランブルする（ステップＳ１３）。

そして、送信装置１は、多重化手段１７によって、ステップＳ１１で生成された第１個別情報（ＥＭＭ－ＣＡＳ）と、ステップＳ１２で生成された第１共通情報（ＥＣＭ－ＣＡＳ）と、ステップＳ１３でスクランブルされた暗号化コンテンツＳＣとを多重化して、多重化信号（放送ストリーム）を生成する（ステップＳ１４）。

なお、ここでは、コンテンツ送信動作を一連の動作として説明したが、第１個別情報や第１共通情報は、ワーク鍵Ｋｗ１やスクランブル鍵Ｋｓ１が更新されるタイミングで生成され、多重化手段１７によって多重化される。

【００７７】

以上、送信装置１の動作について説明したが、図６におけるＣＡＳプログラム送信動作や、図７におけるコンテンツ送信動作において、多重化手段１７が、多重化信号を生成する動作（ステップＳ４，Ｓ１４）は、それぞれ個別に動作するものではない。すなわち、多重化手段１７は、多重化対象となる情報が生成されたタイミングで、逐次それぞれの情報が多重化される。

【００７８】

〔受信装置の動作：ＣＡＳプログラム受信〕

次に、図８を参照（構成については適宜図５参照）して、受信装置２のＣＡＳプログラム受信動作について説明する。

まず、受信装置２は、分離手段２４によって、送信装置１から送信された放送ストリーム（放送信号；多重化信号）に多重化されている情報を分離する（ステップＳ２１）。

そして、受信装置２は、ステップＳ２１で分離された情報に第２個別情報（ＥＭＭ－ＲＭＰ）が含まれている場合、第２個別情報処理手段２６によって、第２個別情報を記憶手段２５に予め記憶されているデバイス鍵Ｋｄで復号し、ワーク鍵Ｋｗ２を取得する（ステップＳ２１）。

【００７９】

また、受信装置２は、ステップＳ２１で分離された情報に第２共通情報（ＥＣＭ－ＲＭＰ）が含まれている場合、第２共通情報処理手段２７によって、第２共通情報をステップＳ２１で復号されたワーク鍵Ｋｗ２で復号し、スクランブル鍵Ｋｓ２取得する（ステップＳ２２）。

【００８０】

そして、受信装置２は、ステップＳ２１で分離された情報に暗号化ＣＡＳプログラムＳＰが含まれている場合、プログラムデスクランブル手段２８によって、暗号化ＣＡＳプログラムＳＰを、ステップＳ２２で復号されたスクランブル鍵Ｋｓ２でデスクランブルする（ステップＳ２３）。

以上の動作によって、受信装置２内に、デバイスごとに異なるＣＡＳプログラムＰがロードされることになる。

【００８１】

〔受信装置の動作：コンテンツ受信〕

次に、図９を参照（構成については適宜図５参照）して、受信装置２のコンテンツ受信動作について説明する。

まず、受信装置２は、分離手段２４によって、送信装置１から送信された放送ストリーム（放送信号；多重化信号）に多重化されている情報を分離する（ステップＳ３１）。

そして、受信装置２は、アクセス制御手段（ＣＡＳプログラム）２０によって、コンテンツに対するアクセス制御（ＣＡＳ機能動作）を行う（ステップＳ３２）。

【００８２】

ここで、図１０を参照して、アクセス制御手段２０におけるステップＳ３２の動作について詳細に説明する。

図１０に示すように、受信装置２は、図９のステップＳ３１で分離された情報に第１個別情報（ＥＭＭ－ＣＡＳ）が含まれている場合、アクセス制御手段２０の第１個別情報処理手段２１によって、第１個別情報を記憶手段２５に予め記憶されているマスタ鍵Ｋｍで復号し、ワーク鍵Ｋｗ１を取得する（ステップＳ３２１）。

【００８３】

また、受信装置２は、図９のステップＳ３１で分離された情報に第１共通情報（ＥＣＭ－ＣＡＳ）が含まれている場合、アクセス制御手段２０の第１共通情報処理手段２２によって、第１共通情報をステップＳ３２１で復号されたワーク鍵Ｋｗ１で復号し、スクラン

ブル鍵Ｋｓ１を取得する（ステップＳ３２２）。
ここで、第１共通情報に復号停止情報が含まれている場合（ステップＳ３２３でＹｅｓ）、第１共通情報処理手段２２が復号停止遅延手段２３にその旨（復号停止検出通知）を通知する。そして、受信装置２は、復号停止遅延手段２３によって、復号停止までの時間の計時を開始して（ステップＳ３２４）、ステップＳ３２５に動作を進める。
一方、第１共通情報に復号停止情報が含まれていない場合（ステップＳ３２３でＮｏ）、受信装置２は、ステップＳ３２５に動作を進める。
【００８４】
そして、受信装置２は、復号停止遅延手段２３によって、計時時間が予め定められている遅延パラメータの時間（遅延時間）を経過した場合（ステップＳ３２５でＹｅｓ）、第１共通情報処理手段２２に復号停止指示を通知することで、第１共通情報処理手段２２がスクランブル鍵Ｋｓ１の出力を停止する（ステップＳ３２６）。
一方、まだ、計時時間が遅延パラメータの時間（遅延時間）を経過していない場合（ステップＳ３２５でＮｏ）、第１共通情報処理手段２２はスクランブル鍵Ｋｓ１を出力する（ステップＳ３２７）。
これによって、アクセス制御手段２０（ＣＡＳプログラムＰ）は、復号停止情報を受信後、デバイスごとに予め定めた遅延時間経過後、スクランブル鍵Ｋｓ１の出力を停止する。
図９に戻って、受信装置２のコンテンツ受信動作について説明する。
【００８５】
図１０で説明した動作によって、ステップＳ３２では、アクセス制御手段２０（ＣＡＳプログラムＰ）からスクランブル鍵Ｋｓ１が出力されるか否かが制御される。
そして、アクセス制御手段２０（ＣＡＳプログラムＰ）からスクランブル鍵Ｋｓ１が出力される場合（ステップＳ３３でＹｅｓ）、受信装置２は、コンテンツデスクランブル手段２９によって、分離手段２４で分離された暗号化コンテンツＳＣを、スクランブル鍵Ｋｓ１でデスクランブルする（ステップＳ３４）。
【００８６】
一方、アクセス制御手段２０（ＣＡＳプログラムＰ）からスクランブル鍵Ｋｓ１が出力されない場合（ステップＳ３３でＮｏ）、受信装置２は、コンテンツデスクランブル手段２９におけるデスクランブルを行わない。
これによって、受信装置２は、放送ストリーム（放送信号）で、復号停止が指示された場合、ＣＡＳプログラムＰに埋め込まれている遅延パラメータの時間（遅延時間）経過後、コンテンツの復号を停止する。
【００８７】
［情報漏洩元特定装置］
次に、図１１を参照して、情報漏洩元特定装置３について説明する。
情報漏洩元特定装置３は、受信装置２からＣＡＳ機能の秘密情報（鍵情報、アルゴリズム等）を不正に取得して複製した複製受信装置２Ｂが、どのＣＡＳ機能（どのデバイス）を複製したものかを特定するものである。
ここでは、情報漏洩元特定装置３は、擬似放送信号生成手段３１と、ＣＡＳ機能種別判定手段３２と、を備える。
【００８８】
擬似放送信号生成手段３１は、送信装置１（図２参照）の機能のうちで、コンテンツと、コンテンツをスクランブルする鍵およびその関連情報とを、放送ストリーム（擬似放送ストリーム〔擬似放送信号〕）として生成する機能を模擬するものである。さらに、擬似放送信号生成手段３１は、放送ストリームに、コンテンツのデスクランブルを停止する復号停止情報を付加する機能を有している。
【００８９】
ここでは、擬似放送信号生成手段３１は、コンテンツスクランブル手段３１０と、共通情報生成手段３１１と、個別情報生成手段３１２と、多重化手段３１３と、を備える。

なお、コンテンツスクランブル手段３１０、個別情報生成手段３１２および多重化手段３１３は、図２で説明した送信装置１のコンテンツスクランブル手段１１、第１個別情報生成手段１３および多重化手段１７とそれぞれ同じものであるため、説明は省略する。ただし、多重化手段３１３で多重化された擬似放送ストリーム（擬似放送信号）の出力先は、複製受信装置２Ｂとなる。

【００９０】

共通情報生成手段３１１は、コンテンツスクランブル手段３１０で用いるスクランブル鍵Ｋｓ１をワーク鍵Ｋｗ１で暗号化し、暗号化したスクランブル鍵Ｋｓ１を含んだ共通情報を生成するものであって、図２で説明した第１共通情報生成手段１２と同じ機能を有する。

さらに、共通情報生成手段３１１は、外部から復号停止情報が入力された場合に、共通情報に復号停止情報を付加する機能を有する。すなわち、共通情報生成手段３１１は、復号停止情報が入力されたとき、図４で説明したように、ＥＣＭ構造を有するメッセージとして共通情報を生成し、その可変部に復号停止情報を付加する。

また、共通情報生成手段３１１は、復号停止情報を付加した共通情報を生成し、多重化手段３１３に出力したタイミングで、ＣＡＳ機能種別判定手段３２に、復号停止情報付き共通情報を複製受信装置２Ｂに送信した旨を通知する。

【００９１】

なお、擬似放送信号生成手段３１に入力するスクランブル鍵Ｋｓ１やワーク鍵Ｋｗ１は、特に更新する必要はなく、固定の鍵を用いればよい。

また、擬似放送信号生成手段３１に入力するマスタ鍵Ｋｍは、正規の受信装置２に予め付与しているマスタ鍵Ｋｍを、順次入力することとする。なお、マスタ鍵Ｋｍを切り替えるタイミングは、予めＣＡＳプログラムＰに埋め込まれている遅延パラメータ（遅延時間）の最大遅延時間よりも長い時間間隔とする。

【００９２】

ＣＡＳ機能種別判定手段（アクセス制御機能種別判定手段）３２は、複製受信装置２Ｂの表示信号（映像音声信号）を解析し、復号停止を指示してから実際に復号が停止されるまでの時間に基づいて、複製受信装置２ＢのＣＡＳ機能、すなわち、どのデバイスのＣＡＳ機能が複製されたかを特定するものである。

ここでは、ＣＡＳ機能種別判定手段３２は、記憶手段３２０と、復号停止検出手段３２１と、遅延時間測定手段３２２と、種別判定手段３２３と、を備える。

【００９３】

記憶手段３２０は、正規の受信装置２のＣＡＳプログラムＰに予め組み込まれている遅延パラメータである遅延時間Ｄと、受信装置２のデバイスを識別するためのデバイス識別Ｋとを予め対応付けて記憶するものである。例えば、この記憶手段２５は、ハードディスク等の記憶媒体で構成される。

【００９４】

復号停止検出手段３２１は、複製受信装置２Ｂの表示信号（映像音声信号）が断絶したか否かを判定することで、復号が停止されたことを検出するものである。

この表示信号が断絶したか否かの判定は、表示信号をビデオキャプチャして画像解析することで行うことができる。例えば、復号停止検出手段３２１は、表示信号を予め定めたフレーム間隔でビデオキャプチャし、予め定めた時間、そのキャプチャした画像が変化しなかった場合に表示信号が断絶したと判定する。また、例えば、復号停止検出手段３２１は、キャプチャしたフレーム画像の画素値を解析し、フレーム画像全体が暗転（ブラックアウト）したときに表示信号が断絶したと判定する。

この復号停止検出手段３２１は、復号が停止されたことを検出した場合、その旨を遅延時間測定手段３２２に通知する。

【００９５】

なお、ここでは、複製受信装置２Ｂとして、ＰＣ（パーソナルコンピュータ）等のように表示装置が分離した構成の装置を想定し、復号停止検出手段３２１が、複製受信装置２

Ｂから直接出力される表示信号を入力することとした。しかし、複製受信装置２Ｂが、テレビ受像機のように表示装置を含んで構成されている場合、図示を省略したカメラ等の撮像装置によって、複製受信装置２Ｂの表示画面を再撮し、復号停止検出手段３２１は、その撮像装置から表示信号を入力すればよい。

【００９６】

遅延時間測定手段３２２は、復号停止情報が付加された共通情報が生成されてから、複製受信装置２Ｂにおいてコンテンツのデスクランブル（復号）が停止されるまでの遅延時間を測定するものである。

ここでは、遅延時間測定手段３２２は、共通情報生成手段３１１から復号停止情報付き共通情報を送信した旨を通知されたときに時間の計時を開始し、復号停止検出手段３２１から復号停止を検出した旨を通知されるまでの時間を遅延時間として測定する。

この遅延時間測定手段３２２は、測定した遅延時間を種別判定手段３２３に出力する。

【００９７】

種別判定手段３２３は、遅延時間測定手段３２２で測定された遅延時間に基づいて、複製受信装置２Ｂが動作しているＣＡＳ機能の種別を特定するものである。

ここでは、種別判定手段３２３は、遅延時間測定手段３２２で測定された遅延時間に対応して、記憶手段３２０に記憶されているデバイス種別Ｋを読み出して、判定結果として外部に出力する。なお、種別判定手段３２３は、遅延時間測定手段３２２で測定された実測値である遅延時間と、記憶手段３２０に記憶されている遅延時間Ｄとが、予め定めた誤差の範囲で一致するか否かで、対応するデバイス種別Ｋを読み出すこととする。

【００９８】

このように、情報漏洩元特定装置３を構成することで、情報漏洩元特定装置３は、複製受信装置２Ｂに対して、共通情報（ＥＣＭ－ＣＡＳ）で復号停止を指示し、実際に復号が停止されるまでの遅延時間によって、複製受信装置２Ｂがどのデバイスの秘密情報の漏洩によりＣＡＳ機能が複製されたのかを特定することができる。

なお、情報漏洩元特定装置３は、この構成に限定されるものではない。

例えば、擬似放送信号生成手段３１と、ＣＡＳ機能種別判定手段３２とを、それぞれ別の装置（擬似放送信号生成装置、ＣＡＳ機能種別判定装置）として構成してもよい。

【００９９】

以上、本発明に係る秘密情報が漏洩し不正に複製された受信装置を、デバイス（デバイス鍵）単位で特定することが可能なアクセス制御プログラム、送信装置、受信装置および情報漏洩元特定装置について説明した。

このように情報漏洩元のデバイスを特定することができることで、例えば、正規の受信装置（情報漏洩されていないデバイスの受信装置）についてのみ、新たな機能を付加したアクセス制御プログラムを更新すること等の運用を行うことができる。

このように、本発明は、不正に複製した受信装置のデバイスを特定することができるため、不正な受信装置の複製に対する抑止力としての効果も奏する。

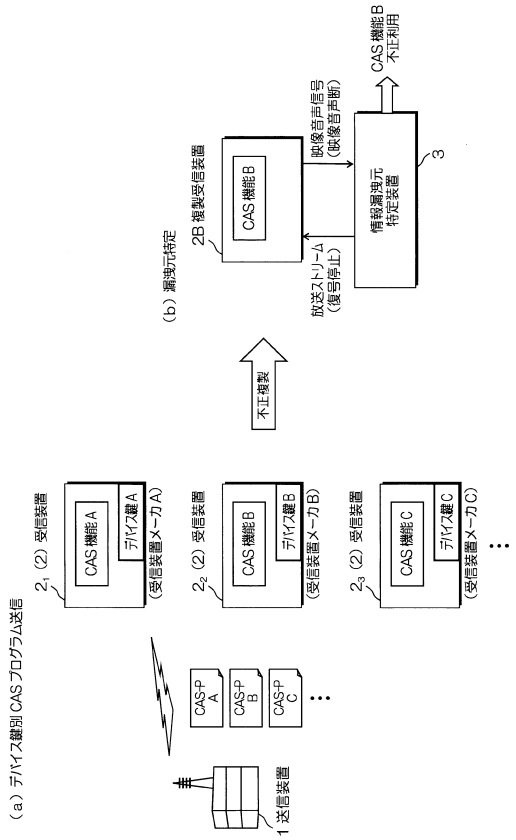
【符号の説明】

【０１００】

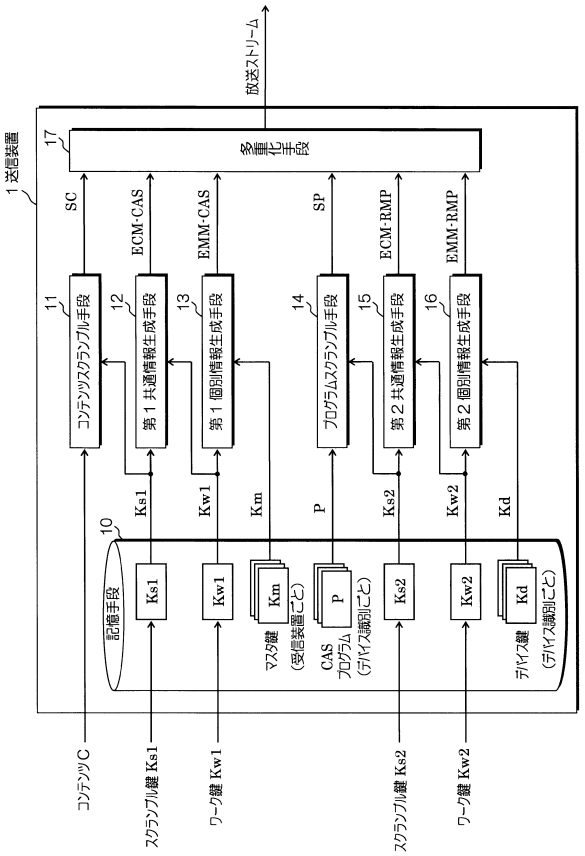
１　送信装置
１０　記憶手段
１１　コンテンツスクランブル手段
１２　第１共通情報生成手段
１３　第１個別情報生成手段
１４　プログラムスクランブル手段
１５　第２共通情報生成手段
１６　第２個別情報生成手段
１７　多重化手段
２　受信装置
２０　アクセス制御手段（アクセス制御プログラム〔ＣＡＳプログラム〕）

２１　第１個別情報処理手段（個別情報処理手段）
２２　第１共通情報処理手段（共通情報処理手段）
２３　復号停止遅延手段
２４　分離手段
２５　記憶手段
２６　第２個別情報処理手段
２７　第２共通情報処理手段
２８　プログラムデスクランブル手段
２９　コンテンツデスクランブル手段
２Ｂ　複製受信装置
３　情報漏洩元特定装置
３１　擬似放送信号生成手段
３１０　コンテンツスクランブル手段
３１１　共通情報生成手段
３１２　個別情報生成手段
３１３　多重化手段
３２　ＣＡＳ機能種別判定手段（アクセス制御機能種別判定手段）
３２０　記憶手段
３２１　復号停止検出手段
３２２　遅延時間測定手段
３２３　種別判定手段

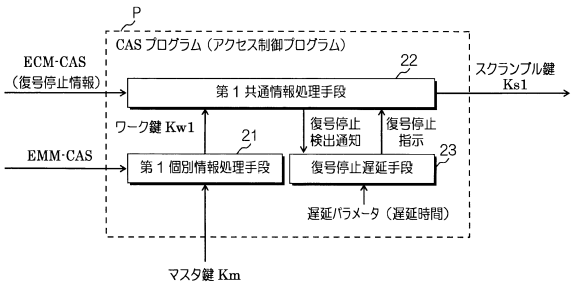
【図１】



【図２】



【図３】

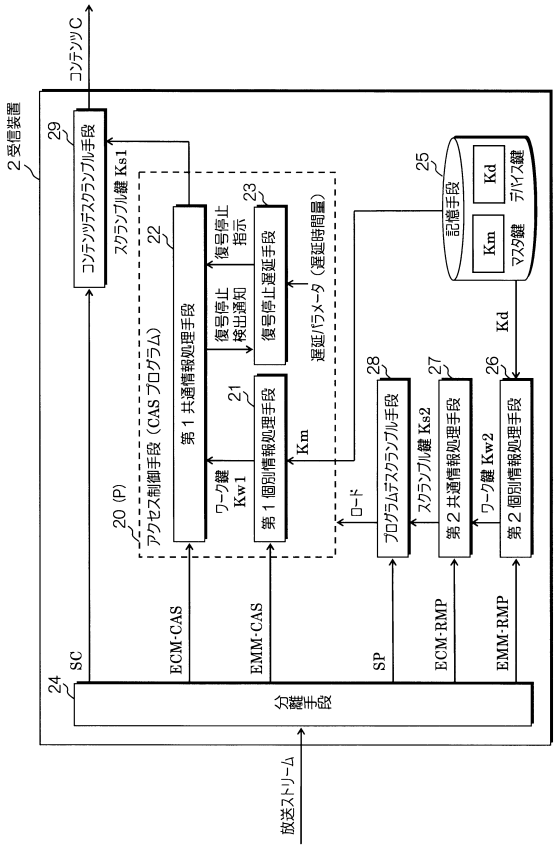


【図４】

第１共通情報（ECM-CAS）

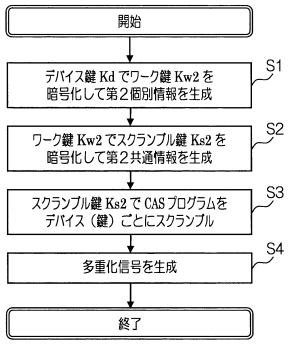
説明				備考（バイト数）
ECMセクション	ECMセクションヘッダ			８バイト
	ECM本体	固定部	:	:
			スクランブル鍵（Odd）	８バイト
			スクランブル鍵（Even）	８バイト
			:	:
		可変部	復号停止情報	１バイト
	CRC誤り検出			４バイト

【図５】



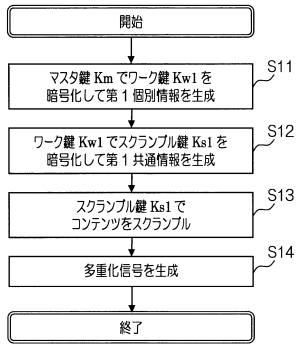
【図６】

CASプログラム送信



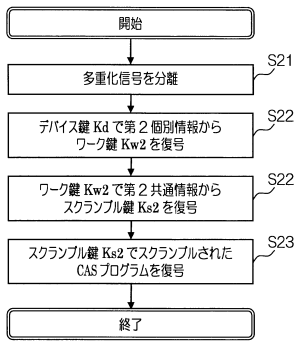
【図７】

コンテンツ送信



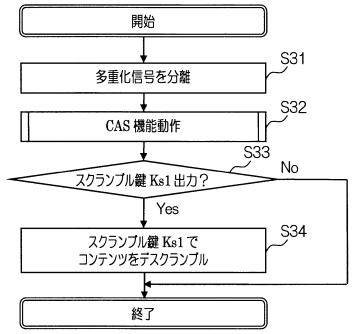
【図８】

CASプログラム受信

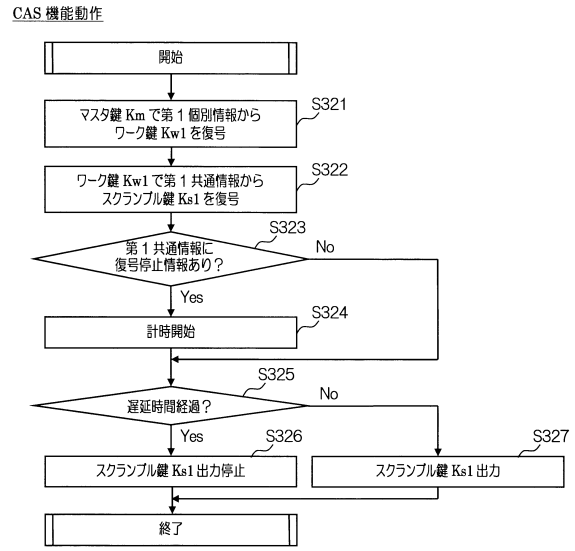


【図９】

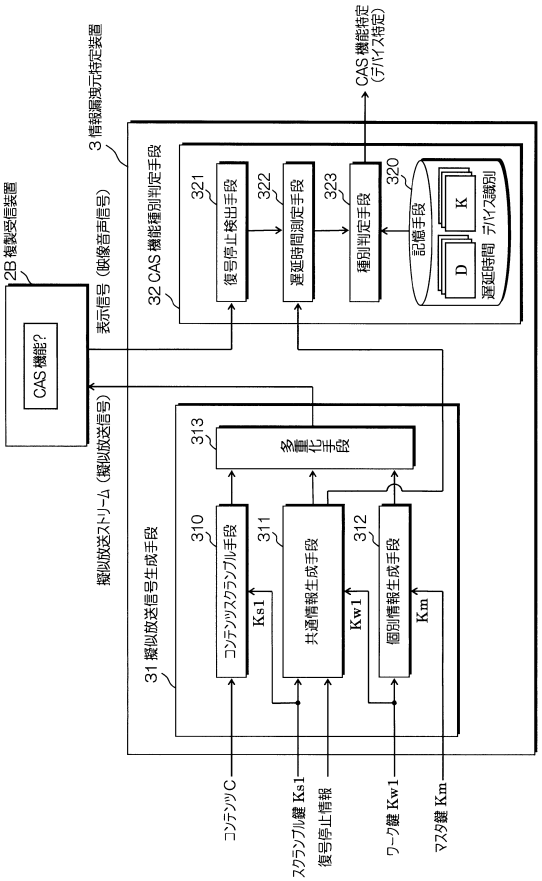
コンテンツ受信



【図１０】


CAS 機能動作
開始
マスタ鍵 Km で第１個別情報から
ワーク鍵 Kw1 を復号
S321
ワーク鍵 Kw1 で第１共通情報から
スクランブル鍵 Ks1 を復号
S322
第１共通情報に
復号停止情報あり？
S323
No
Yes
計時開始
S324
遅延時間経過？
S325
No
Yes
スクランブル鍵 Ks1 出力停止
S326
スクランブル鍵 Ks1 出力
S327
終了

【図１１】


CAS 機能特定
(デバイス特定)
3 情報漏洩元特定装置
2B 複製受信装置
CAS 機能?
表示信号（映像音声信号）
擬似放送ストリーム（擬似放送信号）
32 CAS 機能種別判定手段
321
復号停止検出手段
322
遅延時間測定手段
323
種別判定手段
320
記憶手段
K
D
デバイス識別
遅延時間
31 擬似放送信号生成手段
313
多重化手段
310
コンテンツスクランブル手段
311
共通情報生成手段
312
個別情報生成手段
Ks1
Kw1
Km
コンテンツC
スクランブル鍵 Ks1
復号停止情報
ワーク鍵 Kw1
マスタ鍵 Km

フロントページの続き

(56)参考文献 特開２００９－２６７６０５（ＪＰ，Ａ）
特開２０１２－０２３５４７（ＪＰ，Ａ）
特開２００４－２２１８００（ＪＰ，Ａ）
特開２００４－２４８２３２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｎ　　７／１７３