

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(10) 国際公開番号

WO 2010/143299 A1

PCT

(43) 国際公開日
2010年12月16日(16.12.2010)

- (51) 国際特許分類:
G06F 21/24 (2006.01) H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/JP2009/060779
- (22) 国際出願日: 2009年6月12日(12.06.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 株式会社 東芝(KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 磯崎 宏(ISOZAKI Hiroshi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 藤原 吉伸(FUJIWARA Yoshinobu) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 本沢 邦朗(HONSAWA Ku-

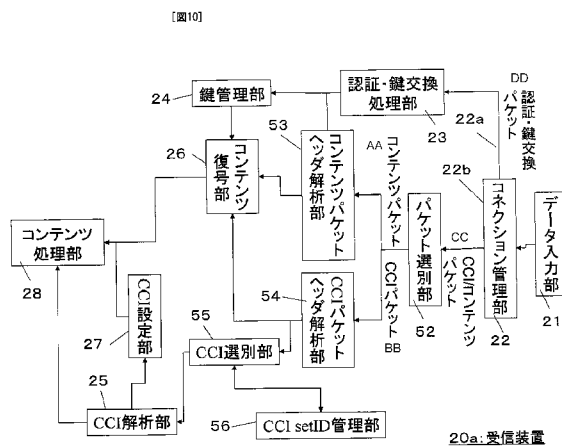
nio) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 加藤 拓(KATO Taku) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP).

- (74) 代理人: 吉武 賢次, 外(YOSHITAKE Kenji et al.); 〒1000005 東京都千代田区丸の内三丁目2番3号 富士ビル323号 協和特許法律事務所 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE

(54) 発明の名称: 情報処理装置



20a: RECEPTION DEVICE
28: CONTENT PROCESSING SECTION
27: CCI SETTING SECTION
25: CCI ANALYSIS SECTION
24: KEY MANAGEMENT SECTION
26: CONTENT DECODING SECTION
55: CCI SORTING SECTION
53: CONTENT PACKET HEADER ANALYSIS SECTION
54: CCI PACKET HEADER ANALYSIS SECTION
56: CCI setID MANAGEMENT SECTION
23: AUTHENTICATION/KEY EXCHANGE PROCESSING SECTION
AA: CONTENT PACKET
BB: CCI PACKET
52: PACKET SORTING SECTION
CC: CCI/CONTENT PACKET
22: CONNECTION MANAGEMENT SECTION
DD: AUTHENTICATION/KEY EXCHANGE PACKET
21: DATA INPUT SECTION

(57) Abstract: The copyright protection and effective use of content can be improved even if new copy control information is added sometime in the future. A transmission device transmits a CCI packet (33) aside from a content packet (39). The CCI packet (33) is capable of including a plurality of CCI groups (36). A unique CCI Set ID is allocated to the CCI packet (33) for each of the CCI groups, and a reception device decodes the content only when the device can interpret a CCI corresponding to a CCI Set ID included in the CCI packet (33). The calculation of a content key for decoding the content data uses the values of CCI group fields, so that, even if the values of the CCI group fields are revised in the middle of communication, the reception device cannot obtain the value of a correct content key, thereby making it possible to improve the copyright protection of the content.

(57) 要約: [課題] 新たなコピー制御情報が将来的に追加された場合であっても、コンテンツの著作権保護とコンテンツの有効活用を図れるようにする。 [解決手段] 送信装置はコンテンツ packets 39 とは別に CCI packets 33 を送信する。CCI packets 33 は複数の CCI 群 36 を含むことが可能である。CCI packets 33 には、CCI 群ごとにユニークな CCI Set ID が割り当てられており、受信装置は CCI packets 33 に含まれる CCI Set ID に対応する CCI を自装置が解釈可能な場合のみコンテンツの復号を行う。コンテンツデータを復号するコンテンツ鍵の計算には、CCI 群フィールドの値を利用するため、CCI 群フィールドの値が通信途中で改変

されたとしても、受信装置は正しいコンテンツ鍵の値を取得することはできず、コンテンツの著作権保護を図ることができる。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF,

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第 21 条(3))
- 補正された請求の範囲 (条約第 19 条(1))

明 細 書

発明の名称： 情報処理装置

技術分野

[0001] 本発明は、著作権保護が必要なコンテンツを受信または送信する情報処理装置に関する。

背景技術

[0002] デジタル情報機器で伝送されるコンテンツは各種のデジタルデータであり、例えばMPEG2やMPEG4などの動画データや音声データ、ストリームデータ、テキストデータ、静止画データなどの各種のデータである。この種のデジタルデータは、本来的に劣化なく複製できることから、コンテンツの著作権について十分に注意を払う必要がある。コンテンツの著作権保護を図りつつ、コンテンツの利便性を高める種々の提案がなされている（例えば、非特許文献1～3参照）。

先行技術文献

非特許文献

[0003] 非特許文献1：DTCP Specification Volume 1 Revision 1.51、<http://www.dtcp.com/data/info%2020071001%20DTCP%20V1%201p51.pdf>

非特許文献2：DTCP Volume 1 Supplement E Mapping DTCP to IP, Revision 1.2、<http://www.dtcp.com/data/info%2020070615%20DTCP%20V1SE%201p2.pdf>

非特許文献3：社団法人 電波産業界 地上デジタルTVジョン放送運用規定
技術資料 ARIB TR-B14

発明の概要

発明が解決しようとする課題

[0004] 上述した非特許文献1～3では、新たなコピー制御情報が将来的に追加される可能性があることを想定しておらず、また、新たなコピー制御情報を解釈できる機器と解釈できない機器が混在した場合のコンテンツ伝送についても考慮していない。

[0005] 本発明は、新たなコピー制御情報が将来的に追加された場合であっても、コンテンツの著作権保護とコンテンツの有効活用を図ることができる情報処理装置を提供するものである。

課題を解決するための手段

[0006] 上記の課題を解決するために、本発明の一態様によれば、通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、

前記通信装置から送信されたパケットが暗号化コンテンツを含むコンテンツパケットか、または少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCIパケットかを判別するパケット選別部と、

前記認証及び鍵交換処理で生成した認証鍵と、前記CCIパケットに含まれるコピー制御情報とに基づいてコンテンツ鍵を生成するコンテンツ鍵生成部と、

前記CCI選別部により選別された前記CCIパケットの後に続いて受信された前記コンテンツパケットに含まれる暗号化コンテンツを、前記コンテンツ鍵に基づいて復号してコンテンツデータを生成するコンテンツ復号部と、

認識可能なコピー制御情報に対応するCCI識別子を管理するCCI識別子管理部と、

前記パケット選別部により前記CCIパケットと判別された場合は、前記CCIパケットに含まれるCCI識別子が前記CCI識別子管理部で管理されているCCI識別子と一致するか否かを判定して、受信処理に用いるべきCCI識別子を選別するCCI選別部と、

前記CCI選別部により選別されたCCI識別子に対応するコピー制御情報を解析するCCI解析部と、

前記CCI解析部による解析結果に基づいて、前記CCIパケットの後に続いて受信された前記コンテンツパケットに対応する前記コンテンツデータの受信処理を行うコンテンツ処理部と、

前記認証及び鍵交換処理を行うための第1の通信コネクション部と、

前記コンテンツ packets 及び前記CCI packets を伝送するための第2の通信コネクション部と、を備えることを特徴とする情報処理装置が提供される。

[0007] また、本発明の一態様によれば、通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、

前記認証及び鍵交換処理に成功した前記通信装置からコンテンツ要求を受けた場合に、対応するコンテンツデータの少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCI packets を生成するCCI packets 化部と、

前記認証及び鍵交換処理で生成した認証鍵と、前記CCI packets に含まれるコピー制御情報とに基づいて、前記コンテンツデータを暗号化するためのコンテンツ鍵を生成するコンテンツ鍵生成部と、

前記認証鍵に対応するラベル情報と、前記コンテンツ鍵を用いて前記コンテンツデータを暗号化した暗号化コンテンツと、を含むコンテンツ packets を生成するコンテンツ packets 生成部と、

前記CCI packets を送信した後に、前記CCI packets に含まれるコピー制御情報が適用される前記コンテンツ packets を送信するデータ出力部と、を備えることを特徴とする情報処理装置が提供される。

発明の効果

[0008] 本発明によれば、新たなコピー制御情報が将来的に追加された場合であっても、コンテンツの著作権保護とコンテンツの有効活用を図ることができる。

図面の簡単な説明

[0009] [図1]送信装置がネットワークに出力するコンテンツ packets 1の構成の一例を表した図。

[図2]コンテンツデータ5のフォーマットの一例を示す図。

[図3]図2のコンテンツデータを送信可能な送信装置10の内部構成の一例を示すブロック図。

[図4]図3の送信装置10に対応する受信装置20の内部構成の一例を示すブ

ロック図。

[図5] コピー制御情報のフォーマットの一例を示す図。

[図6] 本発明の第1の実施形態による送信装置10aがネットワークに出力する際のコンテンツのパケットフォーマットの一例を表した図。

[図7] 第1の実施形態によるコンテンツデータ38のフォーマットを示す図。

[図8] 第1の実施形態による送信装置10aの内部構成を示すブロック図。

[図9] 図8に示したコンテンツパケット39の詳細なフォーマットの一例を示す図。

[図10] 第1の実施形態による受信装置20aの内部構成の一例を示すブロック図。

[図11] 図10の受信装置20aの動作手順の一例を示すフローチャート。

[図12] 図8の送信装置10aと図10の受信装置20aを備えたコンテンツ送受信システムの処理手順を示すシーケンス図。

[図13] 第2の実施形態によるCCIパケット33のフォーマットを示す図。

[図14] 第2の実施形態による受信装置20bの内部構成の一例を示すブロック図。

[図15] 第3の実施形態によるCCIパケット33のフォーマットを示す図。

[図16] 第3の実施形態による受信装置20cの内部構成の一例を示すブロック図。

[図17] 第4の実施形態によるCCIパケット33のフォーマットを示す図。

[図18] 第4の実施形態による送信装置の内部構成を示すブロック図。

[図19] 第4の実施形態による受信装置の内部構成を示すブロック図。

発明を実施するための形態

[0010] 以下、図面を参照しながら、本発明の実施形態について詳細に説明する。

[0011] まず、本発明の具体的な実施形態を説明する前に、本発明の実施形態で達成すべき内容を説明する。

[0012] 本発明の実施形態は、コンテンツの著作権保護とコンテンツの利便性向上の両方を担保するために、以下の(1)～(4)の条件を満たすことを特徴

としている。

[0013] (1) さまざまなコピー制御情報を伝送できる。

非特許文献 1、2 で定義されているように、現状の技術でも世代管理情報だけでなく、個数制限コピー可など様々なコピー制御情報が定義されており、日本のデジタル放送などで運用されている。したがって、それらのさまざまなコピー制御情報を効率よく伝送できる仕組みが必要である。ここで、個数制限コピー可は、日本ではいわゆるダビング 10 のことを指す。

[0014] (2) コピー制御情報を追加で定義できる。

新たなビジネスモデルの出現などによって新しいコピー制御情報を定義する必要がある場合がある。例えば、現状ではコピーの世代管理を表現するのに一世代に限りコピー可というフラグしか定義されていないが、新しいビジネスモデルでは三世代に限りコピー可というフラグを定義することになるかもしれない。そのような新しいコピー制御情報を容易に追加できる必要がある。

[0015] (3) 過去の受信装置や送信装置との互換性がある。

新しいコピー制御情報を追加した場合に、新しいコピー制御情報に対応した送信装置から、以前に製造・出荷した受信装置に対してコンテンツを送信できなければならない。以前に製造・出荷した受信装置が新しいコピー制御情報を解釈できる必要はないが、新しいコピー制御情報の付与されたコンテンツを受信する際、矛盾なく動作できなければならない。

[0016] 非特許文献 1 には世代管理情報を送信装置から受信装置に伝送する機能はあるが、利用期限を伝送する情報は想定していない。例えば受信したコンテンツを蓄積し、ある期限まで再生してよいという時間制限のコピー制御情報を新たに定義したとする。送信装置は、記録してもよいことを示す既存のコピー制御情報である一世代のみコピー可 (Copy One Generation) に、今回新たに定義した Rental Time (Rental Time で示す時間内であれば利用可) という時間制限のコピー制御情報をコンテンツに付与して、Rental Time で示された時間内に限り記録及び再生を許可するという時間制限を付けてコンテンツを送

信したとする。このとき、新しいコピー制御情報であるRental Timeを認識できる受信装置はそのとおり解釈して動作するが、世代管理情報しか認識できない過去に製造・出荷された受信装置は一世代のみコピー可のコンテンツと解釈してしまい、Rental Timeで示された時間を超えてコンテンツを記録、再生してしまう。

[0017] 同様の問題として、従来のコピー制御情報が一世代のみコピー可という世代管理情報しか定義されていないときに、新たなコピー制御情報としてコピーの個数を定義したとする。送信装置は新しいコピー制御情報を解釈し、コンテンツに対して一世代のみコピー可とコピーの個数を示す情報Xを付与し、コピーの個数はXで記された数のみコピー可で、かつ一世代のみコピー可という制限を付けて送信したとする。このとき、新しいコピー制御情報を受信できる受信装置はそのとおり解釈するが、世代管理情報しか認識できない過去に製造・出荷された受信装置は一世代のみコピー可のコンテンツと解釈して無制限の個数のコピーを作成してしまう。

[0018] 上述した二つの例では、過去に製造・出荷された受信装置は送信装置の本来の意図を解釈しているとは言えない。過去に製造・出荷された受信装置がコンテンツを受信した場合、解釈できるコンテンツか、解釈できないコンテンツかを判別する手段を提供する必要がある。なお、将来どのようなコピー制御情報が新たに定義されるか分からないので、上述した問題が起きないような仕組みにしておくことが重要である。

[0019] (4) さまざまなコンテンツフォーマットに対応できる。

現状普及しているデジタルコンテンツでは、記録型DVDや家庭内IPネットワークはMPEG2-PS、デジタル放送はMPEG2-TSと言うように、コンテンツを伝送するための種々のフォーマットが存在し、フォーマットごとにどのようなコピー制御情報をどこに挿入するかを決めなければならない。

[0020] 特に、各国のデジタル放送で用いられているMPEG2-TSに関しては、コンテンツ自体が同じフォーマットであっても、コピー制御情報のビットの割り当て方(ビット長やビットの意味)は異なっており、同じフォーマットであるか

らといって、同じようにコピー制御情報が挿入されているとは限らない。

[0021] 例えば、国AではCopy Neverのビットの割り当てを11b、Copy Freeを00bと定義し、国BではCopy Neverを00b、Copy Freeを11bと定義した場合、受信装置はコピー制御情報が11となっているコンテンツを受信する際、その受信装置がどちらの国のコピー制御情報として判断するかによってCopy Neverと解釈するかCopy Freeと解釈するか、その解釈がまったく異なってしまう。このような誤った解釈が起きないように仕組みを提供する必要がある。

[0022] なお、コピー制御情報(CCI: Copy Control Information)とは、狭義の意味では世代管理情報のみを指す。世代管理情報とは、コピー禁止を示すCopy Neverと、一世代のみコピー可を示すCopy One Generation (COG)と、制限なくコピー可を示すCopy Freeとを含む。

[0023] 以下の説明では、CCIの中に、世代管理情報に加えて、コピーの個数や再生期限情報、画質制限(ICT: Image Constraint Token)、デジタル出力のみ許可(DOT: Digital Only Token)など、さまざまなコンテンツ保護に関連する管理情報を含めるものとする。

[0024] 受信装置は受信したコピー制御情報に応じて蓄積、外部出力、自装置での描画などの制御を行う。また、コピー制御情報(CCI)の他にも、コンテンツ管理情報(CMI: Content Management Information)という用語が用いられる場合もあるが、ここではコンテンツ管理情報とコピー制御情報は同義として使うものとする。

[0025] コンテンツの著作権を保護しつつ、家庭内ネットワークにコンテンツを出力する方式としてDTCP方式やDTCP-IP方式が広く普及している。以下では、これらをまとめてDTCP-IP方式と呼ぶ。

[0026] ところが、現状では、DTCP-IP方式にはCopy One Generation(1世代のみコピー可)などコピーの世代管理情報を表すCCIを通知する機能しかなく、送信装置から受信装置に複雑なCCIを送ることができない。また、コピー制御情報を伝送するためのフィールド(E-EMIフィールド)が定義されているが、固定長であり、挿入可能なCCIの種類も少なく、新たなCCIを追加していくと、いず

れはビット長が足りなくなり、上述した（３）の拡張性の要求を満たせなくなる。

[0027] 拡張性のあるCCIを伝送する方法として、代表的なコピー制御情報はE-EMIフィールドに挿入し、その他のコピー制御情報はコンテンツの中に埋め込み、埋め込むCCIについては拡張性を持たせる手法（DTCP_descriptor）が定義されている。ところが、DTCP_descriptorはMPEG-TSフォーマットのみに適用可能であり、上述した（２）のさまざまなフォーマットに対応できるという要求を満たせない。

[0028] このような問題を解決する手法が図１に示されている。図１は送信装置がネットワークに出力するコンテンツパケット（CCI & コンテンツパケット）１の構成の一例を表した図である。図１のコンテンツパケット１は、ヘッダ２、CCI ３及び暗号化コンテンツ４を含む。

[0029] ヘッダ２のフィールドは、バージョン情報と鍵情報を含む。バージョン情報フィールドは必須ではない。鍵情報フィールドは、時間または送信データ量に応じて更新される鍵情報（N）を含む。暗号化コンテンツフィールドは、コンテンツ鍵（Kc）で暗号化されたコンテンツを含む。

[0030] CCI ３のフィールドは、CCIごとに、CCIの種別を表すIDと、CCIのバイト長と、CCIの値とを含む。図１では、CCIの種別を表すIDのビット長は固定長であることを前提としているが、可変長にして、このIDのビット長を示す不図示のLengthフィールドを新たに定義してもよい。

[0031] 例えば、CCIとして、受信装置で生成可能なコピーの個数を定義する場合、そのCCIに対応するCCI IDは予め送信装置と受信装置で取り決めておいた数字（例えばi）に設定され、CCIの値は許可されるコピー個数に設定される。

[0032] 受信装置はCCIが認識可能か否かをCCI IDで判別し、認識可能なCCI IDで示されるCCIの値だけを解釈してそのCCIの値に従った処理を行う。例えば、コンテンツのコピーを複数個作成する能力がない受信装置は、CCI ID=iとなっているCCIの値フィールドは読み飛ばす。一方、コンテンツのコピーを複数個作成する能力がある受信装置は、CCI ID=iとなっているCCI ３のフィールドを

読み、その値に入っている分だけのコピーを作成する。

[0033] このように、送信装置は、受信装置の機能にかかわらず、コピー制御情報とそのコピー制御情報に対応するIDをコンテンツパッケージ1に付加することで、すべての受信装置に対して同一のコンテンツを送信することができる。

[0034] 送信装置から受信装置に送信されるコンテンツデータ5は、図1のコンテンツパッケージ1の集合体である。図2はコンテンツデータ5のフォーマットの一例を示す図である。図示のように、コンテンツデータ5は、複数のCCI & コンテンツパッケージ1からなり、個々のCCI & コンテンツパッケージ1は、図1と同様にヘッダ2と、CCI 3と、暗号化コンテンツ4とを含んでいる。

[0035] 暗号化コンテンツ4は、送信装置と受信装置であらかじめ共有されたコンテンツ鍵(Kc)を使って暗号化したものである。このコンテンツ鍵(Kc)を計算する際に、CCIの値を用いてもよい。これにより、CCIが通信途中で不正に改変された場合には、暗号化コンテンツ4の復号が不可能になる。

[0036] 図3は図2のコンテンツデータを送信可能な送信装置10の内部構成の一例を示すブロック図である。図3の送信装置10は、コンテンツ供給部11と、認証・鍵交換処理部12と、鍵管理部13と、CCI判定部14と、CCI挿入部15と、コンテンツパッケージ化部16と、コンテンツ暗号部17と、接続管理部18と、データ出力部19とを有する。

[0037] コンテンツ供給部11は、暗号化していない平文のコンテンツを供給する。平文のコンテンツとは、デジタル放送TVで受信可能なデジタル放送コンテンツや、HDD等のデジタル録画機器で記録されたコンテンツなどである。

[0038] 認証・鍵交換処理部12は、受信装置と認証・鍵交換処理を行う。認証・鍵交換処理部12は、各受信装置との間で認証・鍵交換処理を行い、認証・鍵交換処理が成功すると、コンテンツの暗号化に利用する共通鍵Kxを不図示の乱数生成器にて生成する。そして、認証・鍵交換処理に成功した受信装置との間で鍵交換を行った共有鍵を利用して、共通鍵Kxを暗号化して暗号化鍵データを生成し、それを受信装置に送信する。

- [0039] なお、受信装置が複数の送信装置 10 から共通鍵Kxを受信することを考慮し、暗号化コンテンツを受信した場合にどの送信装置 10 の共通鍵で暗号化されたコンテンツであったかを識別できるように、送信装置 10 は共通鍵Kxの識別子として共通鍵ラベルを暗号化された共通鍵Kxに付加して送信してもよい。この共通鍵ラベル自体は秘密の情報ではないため、暗号化せずに共通鍵Kxに付加して平文で送信してもよい。
- [0040] 上述した共通鍵Kxを共有鍵で暗号あるいは復号するための暗号アルゴリズムとしては、AES (Advanced Encryption Standard) などの公知の手法を用いてもよく、特にその手法は限定されない。
- [0041] ここで、認証・鍵交換処理部 12 が行う認証・鍵交換処理とは、送信装置 10 や受信装置が所定のライセンス機関から正しくライセンスを受けた装置であることを相互に認証し、正当な装置であると確認できた場合に共有鍵を生成する処理のことを指す。認証の方法として、ISO/IEC 9798-3やISO/IEC 9798-2のような公知の手法を用いてもよく、特にその手法は限定されない。
- [0042] 鍵管理部 13 は、共通鍵Kx、CCI及び鍵情報に基づいてコンテンツ鍵(Kc)を計算し、それを管理する処理を行う。鍵情報とは、データ量もしくは時間で更新する値であり、コンテンツ鍵を時変鍵にするために用いられる。鍵情報の初期値は不図示の乱数生成部によって生成した乱数とし、更新のたびに1ずつ増加（または減少）させるルールを採用してもよいし、更新のたびに乱数を生成して値を設定してもよい。
- [0043] 鍵情報自体は秘密にすべき情報ではないため、コンテンツパケットのヘッダの一部として平文で送信してよい。コンテンツ鍵(Kc)は、暗号化前の平文コンテンツのCCIの更新時、すなわちCCIパケットの中のいずれかのCCIの値が変化してコンテンツ鍵Kcの再計算が必要になったとき、または鍵情報の値が変化したときに更新される。
- [0044] CCI判定部 14 はコンテンツ供給部 11 から供給される平文コンテンツのCCIの値を判定し、コンテンツ鍵Kcの更新タイミングを鍵管理部 13 に通知したり、CCI挿入部 15 にCCIの値を通知したりする処理を行う。

- [0045] CCI挿入部 15はCCI判定部 14から通知されたCCIの値をCCIの種別を表すID（以下、CCI ID）で表現される形式に変換し、図 1に示したCCIフィールドの中のCCIの値を設定する。CCI IDは、ライセンス機関等が予め規格として一意に定義するものであり、例えば、コピー世代管理情報であるCopy Never（コピー禁止）に対して特定の値からなるCCI IDを割り当てる。
- [0046] CCI挿入部 15はその定義に従ってCCI判定部 14にて判定した値をCCI IDとLength、それにCCIの値に変換する処理を行う。もちろんこの変換処理はCopy Neverに限らず、コンテンツ供給部 11から供給されるコンテンツが持つさまざまなCCIに対して行う。
- [0047] コンテンツパケット化部 16は暗号化コンテンツを所定のフォーマットに整形する処理を行う。コンテンツ暗号部 17はコンテンツパケットのコンテンツデータ部分に暗号処理を施す処理を行う。
- [0048] コネクション管理部 18は認証・鍵交換処理用のコネクションと、CCIとコンテンツデータを伝送するパケット用のコネクションを管理する処理を行う。認証・鍵交換処理用のコネクションと、CCIパケット及びコンテンツデータを伝送するパケット用のコネクションは異なるコネクション（例えばTCPコネクション）を用いる。
- [0049] データ出力部 19はIP(Internet Protocol)層またはそれ以下の層の物理層の処理を行う。
- [0050] 図 4は図 3の送信装置 10に対応する受信装置 20の内部構成の一例を示すブロック図である。図 4に示すように、受信装置 20は、データ入力部 21と、コネクション管理部 22と、認証・鍵交換処理部 23と、鍵管理部 24と、CCI解析部 25と、コンテンツ復号部 26と、CCI設定部 27と、コンテンツ処理部 28とを有する。
- [0051] データ入力部 21は、ネットワーク経由で送信装置 10から送信されるコンテンツデータを入力するIP(Internet Protocol)層またはそれ以下の層の物理層の処理を行う。
- [0052] コネクション管理部 22は、認証・鍵交換処理用のコネクションと、CCIパ

ケット及びコンテンツデータを伝送するパケット用のコネクションを管理する処理を行う。認証・鍵交換処理用のコネクションと、CCIパケット及びコンテンツデータを伝送するパケット用のコネクションは異なるコネクション(例えばTCPコネクション)を用いる。

[0053] 認証・鍵交換処理部23は送信装置10と認証・鍵交換処理を行う。認証・鍵交換処理部23は、認証・鍵交換処理が成功すると送信装置10と共有鍵を共有し、その共有鍵を使って暗号化された共通鍵Kxを受信し、共有鍵を使って共通鍵Kxを復号する。

[0054] 鍵管理部24は、認証・鍵交換処理部23の処理が成功すると、認証・鍵交換処理部23から共通鍵Kxを受信して保持する。なお、認証・鍵交換処理にて共通鍵Kxとともに共通鍵ラベル情報が付加される場合は共通鍵Kxと共通鍵ラベルを対にして保持してもよい。

[0055] CCI解析部25は図2に示すフォーマットのコンテンツデータを読み込んでコンテンツデータのどの部分までがCCIフィールドであるかを解析し、かつそのCCIフィールドにどのようなCCI IDが含まれており、そのCCI IDで示されたCCIがどのような値であるかを解析してCCI設定部27に通知する。

[0056] コンテンツ復号部26はCCI解析部25で得たCCIの値と、鍵管理部24が保持する共通鍵Kxの値とに基づいて、コンテンツ鍵Kcを計算し、コンテンツ鍵Kcを使ってコンテンツを復号し、平文のコンテンツをコンテンツ処理部28に受け渡す。

[0057] CCI設定部27は、CCI解析部25が解析した結果に基づいて、コンテンツ処理部28に対して適切なコピー制御を行わせる。

[0058] コンテンツ処理部28は、CCI設定部27の指示に従ってコンテンツを処理する。例えば、CCI設定部27がCopy Never(コピー禁止)を設定した場合、受信装置20が仮にコンテンツを記録する機能を備えていて受信したコンテンツを蓄積記録している最中だったとしても、コンテンツを蓄積蓄積する処理を中断する。

[0059] 図1に示すコンテンツパケットの構成だと、各CCIが完全に独立して動作す

る場合には問題ないが、CCIが相互に依存している場合には問題がある。例えば、コンテンツの再生許可期限を表すRental Timeを含むCCIと、コピーの世代管理情報を含むCCIとが存在する場合を考えてみる。Rental Timeの具体的な値は24時間といった相対値(24時間以内であれば再生を許可する)や、2010年1月1日13:00といった絶対値(2010年1月1日の13:00までは再生を許可する)で表現される。このRental Timeと世代管理情報を組み合わせることによって、一世代に限りコピーを許可するが、再生期限は24時間に限定するといった制限(Copy One Generation + Rental Time)や、コピーは無制限に行ってもよいが再生期限は24時間に限定するといった制限(EPN + Rental Time)などを表現することができる。

[0060] ここで、便宜上、世代管理情報を表すCCIのCCI IDをM、Rental TimeをあらわすCCIのCCI IDをNと定義しておく。送信装置10は一世代に限りコピーを許可するが、再生期限は24時間に限定するコンテンツに付与するコピー制御情報は図5に示すようなフォーマットになる。すなわち、世代管理情報を表すCCI 31の中のCCI ID=MのフィールドにCopy One Generation、Rental Timeを表すCCI 32の中のCCI ID = Nのフィールドに24時間(24 Hours)という値が挿入される。

[0061] 受信装置20に世代管理情報とRental Timeの両方を解釈する能力がある場合は、それぞれのCCI IDとCCIの値を確認することで、当該装置にのみコピーの記録が許可され、再生期限は24時間ということが正しく伝わる。しかしながら、世代管理情報しか解釈できない受信装置20は、Rental TimeのCCIを読み飛ばして世代管理情報記録のみを解釈してしまう。世代管理情報には一世代限りコピー可となっているため、当該機器にコピーするが、再生期限はない。このように、図1や図5で示したフォーマットでは、送信装置10が意図したCCIが受信装置20に正しく伝達されない場合がある。

[0062] そこで、以下に詳述する本発明の実施形態は、送信装置がコンテンツを送信可能な受信装置20のすべてが必ずしもCCIを正しく解釈できるとは限らないという前提に立って、送信装置10が上述した(1)～(4)の条件を満

たすことができ、受信装置 20 もそれに対応した動作を行うことができることを特徴とする。

[0063] (第 1 の実施形態)

図 6 は本発明の第 1 の実施形態による送信装置 10a がネットワークに出力する際のコンテンツのパケットフォーマットの一例を表した図であり、CCI をパケット化した CCI パケット 33 のフォーマットを示している。図 1 との違いは、CCI ごとに CCI ID を付与するのではなく、1 つ以上の CCI の組み合わせで識別子 (CCI Set ID) を付与する点にある。

[0064] 例えば、CCI Set ID(0) は、2 ビットで世代管理情報を示す CCI (CCI #1) と、1 ビットでアナログ出力時の画質制限 (Image Constraint Token) を示す CCI (CCI #2) と、1 ビットでアナログ出力を禁止すること (Digital Only Token) を示す CCI (CCI #3) とを組合わせた CCI の識別子である。

[0065] また、CCI Set ID(1) は、4 ビットで世代管理情報を示す CCI (CCI #x) と、1 ビットで個数制限コピー可を示す CCI (CCI #y) と、4 ビットでコピーの個数を示す CCI (CCI #z) とを組合わせた CCI の識別子である。

[0066] このように、CCI Set ID とは、その中に含まれる CCI の組み合わせ (以下では CCI 群と呼ぶ) を区別する識別子 (CCI 群識別子) である。このように、CCI 群識別子は、CCI パケット 33 に含まれる個々の CCI 群を識別する情報である。ある CCI Set ID と別の CCI Set ID は、包含関係にある場合と、一部重複する場合と、まったく重複しない場合と、同じ CCI を含むが CCI の値が異なる場合とのいずれかである。包含関係にあるとは、例えば、CCI Set ID=X は CCI Set ID=Y に含まれる CCI を含み、それに加えて別の CCI も含む場合である。一部重複する場合とは、CCI Set ID=X と CCI Set ID=Y は同一の CCI を含むが、それぞれ別の CCI も含む場合である。

[0067] CCI Set ID に対応する CCI 群は、コンテンツデータが MPEG-TS のように多重化されたストリームで構成されている場合、それぞれのストリームに対してどのような CCI を設定するかを指定できるようになっていてもよい。

[0068] CCI Set ID は、各 CCI 群に含まれる CCI の種類だけでなく、CCI のフォーマッ

トやCCIのビットアサインに応じて同じCCI Set IDの値が使われることがないよう、一意（ユニーク）でなければならない。

[0069] 例えば、同一のCCI群のフォーマットとなっているが、アナログ出力時の画質制限(ON/OFFで表現する)がONであることをあるCCI群では1と定義し、別のCCI群では0と定義し、それ以外はまったく同じ二つのフォーマット(形式、長さ、ビットアサイン)のCCI群があったとき、似ているからといって同じ識別子CCI Set ID=Zを割り当ててはいけない。

[0070] 送信装置10aがアナログ出力時の画質制限をONとしているコンテンツを送信するとき、CCI Set IDをZという値で送信する。受信装置20は1のときONと解釈するように実装すると問題ないが、0をONとして受信装置20を実装すると、そのコンテンツを受信した受信装置20はアナログ出力時の画質制限を行わなくてもよいと解釈してしまうので、予めCCI Set IDを特定の値Zに設定する必要がある。運用としては、デバイス間での認証・鍵交換のために用いる秘密鍵の配布元であるライセンス組織が各CCI群でユニークとなるようにCCI Set IDを割り振ればよい。

[0071] 図6に示すように、CCIパケット33は、バージョン情報を示すVersion34のフィールドと、CCI群フィールドの長さを示すLength35のフィールドと、1つ以上のCCI群からなるCCI群36のフィールドとを含む。なお、VersionフィールドとLengthフィールドはCCIパケット33のヘッダ37を構成するが、このヘッダは必須ではない。各CCI群フィールドの中に定義されているLengthフィールドは各CCI群フィールドの長さを示す。1つのCCI群の中には、一つ以上のCCIが含まれている。

[0072] 図7は第1の実施形態によるコンテンツデータ38のフォーマットを示す図である。図7では、コンテンツデータがCCIとは別にパケット化されている点が図1や非特許文献1、非特許文献2とは異なる。具体的には、コンテンツデータは、CCIパケット33の後に、そのCCIパケット33のCCIが適用される1つ以上のコンテンツパケット39が続くフォーマットになっている。CCIパケット33は図6のフォーマットのCCIを含んでおり、コンテンツパケット

３９はヘッダ４０と暗号化コンテンツ４１を含んでいる。

[0073] 図７に示した例では、右端に記されたCCIパケット３３に含まれるCCIは右から３つのコンテンツパケット３９に適用される。左から二番目のCCIパケット３３に含まれるCCIは一番左のコンテンツパケット３９に適用される。

[0074] なお、図７の例では、CCIパケット３３が途中で切り替わる例を示したが、コンテンツのCCIが変化しなければCCIパケット３３をコンテンツ伝送の最初に一つだけ伝送し、その後はCCIパケット３３を伝送しなくてもよい。また、CCIが変化しなくても、個々のコンテンツパケット３９に対応づけてCCIパケット３３を挿入してもよい。

[0075] 非特許文献１や非特許文献２に示す公知技術では、暗号化コンテンツを復号する前に受信装置２０が知りうるCCIは世代管理情報などに限定されており、その他のCCIは暗号化前のコンテンツ(平文のコンテンツ)に埋め込まれていたため、受信装置２０はコンテンツを復号してみないとすべてのCCIの値を知ることができなかった。

[0076] また、コンテンツのフォーマットによっては、CCIなどの付属データを挿入するビット幅が固定長であるため、拡張性がなく、追加で新たなCCIを定義することができなかった。

[0077] これに対して、第１の実施形態では、世代管理情報を含むさまざまな種類のCCIを暗号化コンテンツの中に埋め込むのではなく、暗号化コンテンツとは別のCCIパケット３３を設ける。これにより、受信装置２０は、コンテンツの復号をする前にそのコンテンツにどのようなCCIの組合せが付与されているかを把握でき、かつコンテンツのフォーマットに依存せずにCCIパケット３３を拡張できる。したがって、新たなCCIの定義を容易に行うことができる。なお、コンテンツの暗号化に用いる鍵の計算方法については後述する。

[0078] 図８は第１の実施形態による送信装置１０aの内部構成を示すブロック図である。図８に示すように、送信装置１０aは、コンテンツ供給部１１と、認証・鍵交換処理部１２と、鍵管理部１３と、CCI判定部１４と、CCI挿入部１５と、CCIパケット化部５１と、コンテンツパケット化部１６と、コンテン

ツ暗号部 17 と、コネクション管理部 18 と、データ出力部 19 とを有する。コンテンツパッケージ化部 16 とコンテンツ暗号部 17 がコンテンツパッケージ生成部に対応する。

[0079] 図 3 の送信装置 10a と異なる点は、CCI パケット 33 を生成する CCI パッケージ化部 51 を新たに備えている点である。図 3 では送信装置 10a はコンテンツパッケージ 39 の中に CCI を挿入していた。これに対し、第 1 の実施形態による送信装置 10a は CCI を別パケットとして送信するため、CCI を所定のフォーマットにパッケージ化した CCI パケット 33 を生成する処理を行う CCI パッケージ化部 51 を備えている。なお、CCI パケット 33 をコンテンツパッケージ 39 とは別個に設けることにしたため、コンテンツパッケージ化部 16 は図 3 と異なり、CCI を挿入する処理を行わない。

[0080] CCI 挿入部 15 は、CCI 判定部 14 から通知されたコンテンツに付随する CCI の値を各 CCI Set ID で表現される図 6 の形式に変換し、CCI の値と CCI Set ID からなる CCI 群を含む CCI パケット 33 を生成する。

[0081] 例えば、同じコピー世代管理情報である Copy Never (コピー禁止) を表現するのに、ある CCI Set ID に対応する CCI は 2 ビットの値で表現するかもしれないし、別の CCI Set ID に対応する CCI は 4 ビットの値で表現するかもしれない。このように、各 CCI ID が Copy Never という値を表現するのに、どのような形式のどのような値に設定すればよいかを考慮に入れてビット数の変換処理を行う。もちろんこの変換処理は Copy Never に限らず、コンテンツ供給部 11 から供給されるコンテンツが持つさまざまな CCI に対して行う。

[0082] また、図 3 に示した送信装置 10a は、コピー世代管理情報を表す CCI が CCI パケット 33 の中で一つだったのに対し、図 8 の処理ではコピー世代管理情報を表す CCI が複数の CCI 群で定義される可能性がある。例えばコピー世代管理情報が CCI Set ID(0) と CCI Set ID(1) の両方で定義されるかもしれない。送信装置が CCI Set ID(0) と CCI Set ID(1) の CCI パケットを送信する場合、CCI Set ID(0) と CCI Set ID(1) の両方に CCI 解析部 25 で取得したコピー世代管理情報を挿入する。なお、ライセンス団体が CCI Set ID を複数定義している

場合、送信装置 10a は自身で解釈できるすべての CCI Set ID の CCI 群を生成して CCI パケット 33 に挿入してもよいし、CCI Set ID を選択してその選択した CCI Set ID に対応する CCI 群のみを CCI パケット 33 に挿入してもよい。

[0083] 図 9 は図 8 に示したコンテンツパケット 39 の詳細なフォーマットの一例を示す図である。本実施形態のコンテンツパケット 39 は、ヘッダ 40 のフィールドと暗号化コンテンツ 41 のフィールドを有する。ヘッダ 40 のフィールドは、さらに細かく、鍵ラベル 42 のフィールドと、鍵情報 43 のフィールドと、Length 44 のフィールドとを有する。

[0084] 鍵ラベル 42 のフィールドには、どの送信装置 10a の鍵で暗号化されたコンテンツであるのかを受信装置 20 が把握できるようにするために、共通鍵 K_x ごとに割り振られたユニークなラベル情報が格納される。鍵情報 43 のフィールドには、送信装置 10a がデータ量もしくは時間に応じて更新する鍵情報が格納される。後述するように、鍵情報は、コンテンツ鍵 (K_c) の計算に用いられる場合がある。Length フィールドには、暗号化コンテンツの長さが格納される。

[0085] 暗号化コンテンツ 44 のフィールドには、暗号化前は平文コンテンツデータが格納される。なお、暗号アルゴリズムによっては、平文コンテンツデータにパディング情報(例えば値 0)を付加してもよい。

[0086] コンテンツ鍵 (K_c) は、CCI パケット 33 で定義された CCI の値と共通鍵 K_x を用いて計算される。具体的には、例えば以下の (1) 式により計算される。ここで、CCI の値とは、図 6 に示した少なくとも CCI 群フィールドの値を含むものとする。

$$\text{コンテンツ鍵}(K_c) = f(\text{CCI}, K_x) \quad \cdots (1)$$

[0087] コンテンツ鍵が所定の条件で更新されるように、以下の (2) 式のように計算式に鍵情報 (N) を含めてもよい。

$$\text{コンテンツ鍵}(K_c) = g(\text{CCI}, K_x, N) \quad \cdots (2)$$

[0088] また、以下の (3) 式で示すように、パラメータをハッシュ関数(関数 h)などを用いて所定のビット長に圧縮してもよい。

$$\text{コンテンツ鍵}(K_c) = i(h(\text{CCI}, K_x), N) \cdots (3)$$

- [0089] 上記(1)～(3)式の関数 f , g , i は、右辺括弧内のパラメータを使って計算される暗号化アルゴリズムである。アルゴリズムとしてはAESなどの既存の暗号アルゴリズムを用いてもよい。
- [0090] 送信装置10aは、コンテンツを伝送している間にコンテンツ供給部11から供給されるコンテンツに付随するCCIの値が変化すれば、CCIパケット化部51はその更新されたCCIの値を使ってCCIパケット33を再度生成する。さらにそのCCIパケット33以降に送られるコンテンツパケット39に含まれるコンテンツは、その更新されたCCIパケット33のCCIの値を使って再計算したコンテンツ鍵(K_c)を使って暗号化する。
- [0091] 上述した(2)または(3)式のコンテンツ鍵(K_c)を用いる場合は、送信装置10aは、データ量もしくは時間に応じて鍵情報が更新された場合も、コンテンツ鍵(K_c)の再計算を行って、CCIパケット33と暗号化パケットの作成を行う。
- [0092] 送信装置10aが同一のコネクション(HTTPの場合はTCPコネクション、RT Pの場合はセッション)においてCCIパケット33を挿入するタイミングは、
(a) コンテンツデータの伝送に先立ち1回だけ挿入、(b) コンテンツのCCIが変更される時に挿入、(c) 定期的に挿入のいずれか、あるいはこれらの組合せのいずれでもよい。
- [0093] 図9では、鍵情報をコンテンツパケット39に挿入する例を示した。鍵情報をコンテンツパケット39に含めることにより、CCIの切り替えと鍵情報の切り替えを独立に行うことができる。例えば、鍵情報は時間またはデータ量に応じて定期的に更新されるが、これは定期的にコンテンツ鍵(K_c)を更新することを意味している。一般に、データを暗号化する際に用いる鍵は同一のものを使い続けるよりも変更した方が暗号化データから暗号化鍵を推測する攻撃に対する耐性は強い。CCIパケット33の挿入タイミングを上記(a)とした場合でも、コンテンツパケット39内の鍵情報を更新することによって、コンテンツ鍵(K_c)を更新することができる。

- [0094] なお、鍵情報をコンテンツパッケージ 39 に含める以外にも、CCI パッケージ 33 のみに含める方法、CCI パッケージ 33 とコンテンツパッケージ 39 の両方に同じ値を含める手法、CCI パッケージ 33 とコンテンツパッケージ 39 に異なる値の鍵情報を挿入する手法があり、これらを採用してもよい。
- [0095] CCI パッケージ 33 のみに含める手法では、鍵情報または CCI のいずれかが変化した場合に CCI パッケージ 33 を挿入する。CCI パッケージ 33 とコンテンツパッケージ 39 に異なる値の鍵情報を挿入する手法では、両方の鍵情報をコンテンツ鍵 (Kc) の計算に含める場合と、どちらか更新された方の値を使う場合とがある。また、鍵情報をコンテンツパッケージ 39 に定義し、CCI パッケージ 33 の CCI 群フィールドのハッシュ値を計算し、そのハッシュ値をコンテンツパッケージ 39 の鍵情報フィールドの一部 (例えば上位 X ビット) として使い、残りのフィールド (例えば下位 Y ビット) は乱数で生成して、1 ずつ増えるように更新してもよい。この場合、 $X + Y$ が鍵情報の全ビット長となる。
- [0096] 図 8 の送信装置 10a は、上述した処理以外は、図 3 の送信装置 10a と同様の処理を行うため、詳しい説明を省略する。
- [0097] 次に受信装置 20a について説明する。図 10 は第 1 の実施形態による受信装置 20a の内部構成の一例を示すブロック図である。図 10 に示すように、受信装置 20a は、データ入力部 21 と、コネクション管理部 22 と、認証・鍵交換処理部 23 と、鍵管理部 24 と、パケット選別部 52 と、コンテンツパッケージヘッダ解析部 53 と、コンテンツ復号部 26 と、CCI パッケージヘッダ解析部 54 と、CCI 選別部 55 と、CCI Set ID 管理部 56 と、CCI 解析部 25 と、CCI 設定部 27 と、コンテンツ処理部 28 とを有する。
- [0098] 図 4 の受信装置 20a と異なる点はパケット選別部 52 と、CCI パッケージヘッダ解析部 54 と、CCI Set ID 管理部 56 (CCI 識別子管理部) と、CCI 選別部 55 と、CCI 解析部 25 とを備えている点である。また、コンテンツ復号部 26 の処理も異なる。
- [0099] パケット選別部 52 は、受信したデータが図 7 に示すコンテンツパッケージ 39 か CCI パッケージ 33 かを判別し、コンテンツパッケージヘッダ解析部 53 と

CCIパケットヘッダ解析部54にデータを振り分ける処理を行う。なお、コンテンツパケット39かCCIパケット33かを区別する方法としては、コンテンツパケット39とCCIパケット33のヘッダに両者を区別する識別子を設ければよい。

- [0100] 非特許文献2に記載の送信装置10aが送信するコンテンツパケット39では、暗号アルゴリズムを識別する情報が定義されているが、第1の実施形態による送信装置10aが送信するコンテンツパケット39を非特許文献2に記載の受信装置20aが受信してもそのパケットを無視するかコネクションを切断するようにするために、暗号モードや暗号アルゴリズムを識別する情報を非特許文献2で定義されていない値に設定すればよい。これにより、非特許文献2に記載の受信装置20aはパケットの中身を知ることができなくなる。
- [0101] CCIパケットヘッダ解析部54は、図6に示したCCIパケット33のうち、CCI群フィールドにどのようなCCI Set IDが含まれているのかを解析する処理を行う。前述のようにコンテンツ鍵(Kc)の計算にはCCIパケット33に含まれるCCIの情報をを用いる。
- [0102] 図2に示したコンテンツデータとは異なり、本実施形態のCCIはコンテンツパケット39とは別のCCIパケット33の中に含まれている。CCIパケットヘッダ解析部54はCCIパケット33に含まれるCCIの値をコンテンツ復号部26に伝達する。
- [0103] 図2に示したコンテンツデータでは、CCIは図2に示すCCI & コンテンツパケット39で伝送されるため、パケット単位でコンテンツ鍵(Kc)を計算することが可能であった。ところが、本実施形態では、コンテンツパケット39が複数回連続して受信される場合もあるため、コンテンツパケット39は必ずしもCCIパケット33の直後に送られてくるとは限らない。
- [0104] コンテンツ鍵(Kc)はCCIと鍵情報の両方を使って計算される。すなわち、CCIまたは鍵情報のどちらかが更新された場合にコンテンツ鍵(Kc)の再計算を行う。コンテンツ復号部26は再計算されたコンテンツ鍵(Kc)を使ってコンテ

ンツを復号する。別の言い方をすると、図2に示したCCI&コンテンツパッケージ39を受信する受信装置20aは、共通鍵KxとCCI&コンテンツパッケージ39だけでコンテンツ鍵(Kc)を計算できたが、第1の実施形態ではコンテンツパッケージ39にはCCIが含まれないため、コンテンツ復号部26は次のCCIパッケージ33を受信するまでCCIの値を保存しておく必要がある。この点は図4に示した受信装置20aとは異なる。CCIパッケージ33に含まれるCCIの値が変化していた場合には、コンテンツ復号部26はそれ以降に受信したコンテンツパッケージ39を復号する際、更新されたコンテンツ鍵(Kc)の値を使って復号する。

[0105] さて、送信装置10aは鍵情報を(a)CCIパッケージ33のみに含める方法、(b)コンテンツパッケージ39のみに含める方法、(c)CCIパッケージ33とコンテンツパッケージ39に同じ値を含める方法、(d)CCIパッケージ33とコンテンツパッケージ39に異なる値を含める方法がある。

[0106] (a)の場合、コンテンツ復号部26はCCIパッケージ33に含まれる鍵情報を使ってコンテンツ鍵(Kc)を計算する。

[0107] (b)の場合、コンテンツ復号部26はコンテンツパッケージ39に含まれる鍵情報を使ってコンテンツ鍵(Kc)を計算する。

[0108] (c)の場合、CCIパッケージ33とコンテンツパッケージ39のいずれかに含まれる鍵情報を使ってコンテンツ鍵(Kc)を計算するが、CCIパッケージ33に含まれる鍵情報とコンテンツパッケージ39に含める鍵情報が一致するか比較処理を行い、一致するときのみコンテンツの復号を行うようにしてもよい。

[0109] (d)の場合、両方の鍵情報を使ってコンテンツ鍵(Kc)を計算する方法と、どちらか更新された方の値を使う場合とがある。

[0110] なお、CCIパッケージ33のハッシュ値が鍵情報の一部として挿入されている場合には、CCIパッケージ33に含まれるCCIを使ってハッシュ値を計算し、そのハッシュ値と鍵情報の一部が一致するか否かの比較処理を行い、一致する場合のみコンテンツを復号する。一致しない場合にはコンテンツの復号を中止する。

[0111] 図8のCCI Set ID管理部56は受信装置20aが解釈可能なCCIに対応するCCI Setの値を管理する。CCI選別部55はCCIパケットヘッダ解析部54で解析されたCCI Set IDと、CCI Set ID管理部56に格納されている値を比較し、CCIコンテンツに含まれているCCI群を選別する処理を行う。CCI選別部55は、受信装置20aが複数のCCI Set IDを解釈可能であれば、CCIパケット33に含まれるCCI Set IDのうちどのCCI Set IDを選択するか、すなわちどのCCI群を採用するのか決定する。この決定の手法としては、採用するCCI群の優先順位を予め指定しておく手法、どのCCI群を採用するかその時の受信装置20aの状態に応じて決定する手法、送信装置10aとネットワークを介してネゴシエーションを行う手法などがある。受信装置20aの状態に応じて決定する手法とは、例えば受信装置20aのコンテンツ処理部28が蓄積、外部出力、内部レンダリングなどの複数の処理を備えている場合に、そのうちの選択された処理に対応してCCI群を選択する手法である。また、コンテンツ処理部28が異なる複数の記録形式でコンテンツを蓄積可能な場合も、選択する記録形式に応じたCCI群を選択する。

[0112] 例えば、受信装置20aがCCI群Aを使って保護して記録する方式と、CCI群Bを使って保護して記録する方式を備えていた場合に、その時の記録方式に応じてCCI群AとCCI群Bのどちらを採用するのか決定するときに使う。なお、CCIパケット33に自装置が解釈可能なCCI Set IDが含まれていない場合はコンテンツデータの受信を中断する。

[0113] CCI解析部25はCCI選別部55で選別されたCCI SetにどのようなCCIが含まれるのかを解析してCCI設定部27に通知する。

[0114] 図11は図10の受信装置20aの動作手順の一例を示すフローチャートである。受信装置20aはまず送信装置10aに認証・鍵交換要求を送信し（ステップS1）、送信装置10aと認証・鍵交換処理を行う。その後、認証・鍵交換処理に成功したか否かを判別し（ステップS2）、認証・鍵交換処理が失敗すれば、エラー処理を行い（ステップS3）、以降の処理は行わない。

- [0115] 認証・鍵交換処理が成功すれば、送信装置 10a から送信された暗号化された共通鍵Kxを受信し（ステップS4）、鍵交換処理で共有した鍵を用いて共通鍵Kxを復号する。次に、受信装置 20a が認識可能なCCI Set IDを送信装置 10a に通知し（ステップS5）、その後、送信装置 10a に対してコンテンツ要求を送信する（ステップS6）。
- [0116] このコンテンツ要求に応じて送信装置 10a が送信するコンテンツデータは図7のようなフォーマットであり、CCIパケット33とコンテンツパケット39を含んでいる。このようなコンテンツデータを受信すると（ステップS7）、CCIパケット33に認識可能なCCI Set IDが含まれているかどうか確認する（ステップS8）。もし含まれていなければ、コンテンツの受信を中断し（ステップS9）、ステップS3のエラー処理を行う。含まれていれば、共通鍵KxとCCI選別部55で選別されたCCIパケット33中のCCIを用いて、上述した（1）～（3）式のいずれかに基づいてコンテンツ鍵(Kc)を計算し、そのコンテンツ鍵(Kc)を用いて暗号化コンテンツを復号する（ステップS10）。
- [0117] 図12は図8の送信装置 10a と図10の受信装置 20a を備えたコンテンツ送受信システムの処理手順を示すシーケンス図である。本実施形態では、送信装置 10a と受信装置 20a との間に2つのコネクションが設けられている。一つは認証・鍵交換処理を行うためのもの（第1の通信コネクション部22a）であり、もう一つはコンテンツパケット39とCCIパケット33を伝送するためのもの（第2の通信コネクション部22b）である。
- [0118] 図12は送信装置 10a が二つの受信装置 20a にコンテンツを送信する例を示している。この場合、合計4つのコネクションA～Dが設けられる。まず受信装置Aが送信装置 10a と認証・鍵交換を行う（ステップS11）。認証・鍵交換が成功すると（ステップS12）、受信装置 20a はコンテンツ要求を送信し（ステップS13）、その応答として送信装置 10a はCCIパケット33とコンテンツパケット39を送信する（ステップS14）。このときのCCIパケット33に含まれるCCI Set IDは受信装置 20a が解釈可能

なCCI Set IDのいずれか(この場合、CCI Set ID=a)もしくは送信装置10aが解釈可能なCCI Set IDすべての値となる。もちろん異常シーケンスとして送信装置10aは受信装置20aが解釈できないCCI Set IDをCCIパケット33に含めて送信してもよいが、その場合、受信装置20aはコンテンツの受信を中断する。

[0119] 図12では省略しているが、受信装置20aはコンテンツ要求の送信に先立ち、どのCCI Set IDなら解釈できるかを送信装置10aに通知する。この通知手段としては認証・鍵交換用のコネクションを使って認証・鍵交換時に通知する手法、認証・鍵交換用のコネクションを使ってコンテンツ要求に先立ち通知する手法、コンテンツ伝送用のコネクションを使ってコンテンツ要求にCCI Set IDを含める手法がある。

[0120] 受信装置20aが送信装置10aに対して解釈可能なCCI Set IDを通知する代わりに、送信装置10aから受信装置20aに対してどのCCI Set IDが解釈可能か問い合わせてもよい。受信装置20aが解釈可能なCCI Set IDを送信装置10aに通知する際にCCI Set IDは共通鍵Kxや共有鍵などを使って暗号化することにより保護して伝送してもよいし、平文で送信してもよい。平文で送信した場合、通信途中で不正に改変されたとしても受信装置20aはそのCCI Set IDが解釈できないか、その改変されたCCI Set IDに応じてコンテンツのCCIを解釈するため、送信装置10aの意図と異なるようにCCIが受信装置20aに伝わるわけではない。したがって、そのような通信経路上でのCCI Set IDの改変は受信装置20aにとってはサービス妨害になったとしても、コンテンツの著作権が不正に操作されるわけではないため、上述した(1)～(4)の目的が阻害されるわけではない。

[0121] 送信装置10aがコンテンツ要求の受信に先立ち、事前にCCI Set IDの通知を受ける利点として、送信装置10aの実装を容易にすることができる点が考えられる。例えば、送信装置10aが複数の受信装置20aに対してコンテンツを送信する場合を考える。送信装置10aは各受信装置20aがどのようなCCI Set IDを解釈できるか、その組み合わせの総和を集計しておく

。受信装置 20a は非同期に送信装置 10a に対してコンテンツ要求を送信するが、送信装置 10a はコンテンツ受信要求を受信すると、集計しておいた CCI Set ID をすべて含めて CCI パケット 33 を送信する。

[0122] このように、送信装置 10a は、コンテンツ受信要求を受信する際、そのコンテンツ受信要求がどの受信装置 20a から送られてきたのかを判断する必要がないため、送信装置 10a の処理を簡易化することができる。

[0123] 上述したステップ S 11 ~ S 14 と同様に、受信装置 B も、送信装置 10a と認証・鍵交換処理を行い（ステップ S 15）、認証・鍵交換処理に成功すれば（ステップ S 16）、コンテンツ要求を送信装置 10a に対して送信し（ステップ S 17）、送信装置 10a から送信されたコンテンツを受信する（ステップ S 18）。このとき、送信装置 10a はコンテンツ送信を受信装置 A と受信装置 B に対して別々のコネクションで配信する。送信装置 10a は、CCI パケット 33 に含める CCI Set に関して、（a）受信装置 A に対しては CCI Set ID=a, 受信装置 B に対しては CCI Set ID=b として送信する手法、（b）受信装置 A、B とも CCI Set ID=a, b の両方を含めた CCI パケット 33 を送信する手法、（c）受信装置 20a がどの CCI Set ID を解釈可能かに限らず、送信装置 10a は CCI パケット 33 化が可能なすべての CCI Set ID を含めた CCI パケット 33 を送信する手法、のいずれかの手法を用いることができる。（c）の場合、CCI 群によっては無効にすべき情報が含まれる場合がある。たとえば、再生許可期限指定されたコンテンツを伝送する場合、CCI パケット化の可能なすべての CCI 群に再生許可期限を示す情報が含まれていればよいが、そうでない CCI 群が存在する可能性もある。そのような場合に対応するため、送信装置 10a は特定の CCI 群は無効である事を示す情報を CCI パケット 33 に含めて送信してもよい。この情報は CCI 群ごとに付けてもよいし、その CCI パケット 33 の中でどの CCI 群が無効か（あるいは有効か）を示す CCI 群のリスト情報を CCI パケットの先頭に付与してもよい。なお、ここではコンテンツ伝送プロトコルとして HTTP が用いられることを想定しているが、RTP を用いて伝送する場合も同様の手法で送信すればよい。

[0124] 上述した（b）または（c）のように一つのCCIパケット33の中に複数のCCI群を含める利点は、CCIパケット33やコンテンツパケット39をマルチキャストで伝送できることである。一般に、マルチキャスト伝送を行う場合は複数の受信装置20aに対して同一のパケットを送信する必要がある。（b）または（c）の手法を用いることで、複数の受信装置20aに対して同一のCCIパケット33やコンテンツパケット39を伝送でき、通信帯域を抑制できる。

[0125] なお、既存のパケットフォーマットしか解釈できない既存の受信装置20aが、図6に示すCCIパケット33や図9に示すコンテンツパケット39を受信しても問題ないようにCCIパケット33やコンテンツパケット39のヘッダの中に、既存のパケットフォーマットと区別する情報を挿入してもよい。例えば、非特許文献2に示すとおり、既存のパケットのヘッダにはコンテンツを暗号化するための暗号アルゴリズムを区別する情報が含まれている（C_Aフィールド）。現状では利用可能な暗号アルゴリズムとしてAESのみ定義されている。図6に示すCCIパケット33や図9に示すコンテンツパケット39のヘッダのフォーマットを既存のパケットのヘッダのフォーマットと同一にしておき、暗号アルゴリズムを区別するフィールドをAES以外の暗号を使っているようにビットをセットすれば、既存の受信装置20aはAESしか実装していないため、受信装置20aがCCIパケット33やコンテンツパケット39を受信したとしても、それらのパケットを無視して破棄する動作が期待できる。この他に、既存のパケットフォーマットと、CCIパケット33やコンテンツパケット39と区別できるように、既存のパケットのヘッダ部に定義されている暗号モードを区別する情報（E-EMIフィールド）の値を現在定義されていない値に設定したり、既存のパケットのヘッダ部に定義されている予約領域を利用して区別してもよい。

[0126] 以下、上述した第1の実施形態の構成上の特徴と効果をまとめて説明する。第1の実施形態による送信装置10aはコンテンツパケット39とは別にCCIパケット33を送信する。CCIパケット33は複数のCCI群を含むことが可

能である。また、CCI群はLengthフィールドを定義することにより可変長であるため、任意の長さのCCIを複数挿入することができる。

[0127] CCIパケット33が複数のCCI群を含むことができるということは、新たなCCIを定義する必要が生じた場合に、そのCCIに対して未使用のCCI Set IDを割り当てることで、容易にCCIの追加に対応できることを示しており、将来的な拡張性に優れている。

[0128] 本実施形態のCCIパケット33には、CCI群ごとにユニークなCCI Set IDが割り当てられており、受信装置20aはCCIパケット33に含まれるCCI Set IDに対応するCCIを自装置が解釈可能な場合のみコンテンツの復号を行う。過去に製造・販売された受信装置20aは新たに定義されたCCI Set IDは解釈せず読み飛ばし、自装置が認識可能なCCI群のみ解釈することになるため、送信装置10aの意図と反して受信装置20aがCCIを解釈するような不具合は生じない。しかも、新しいCCI群が定義されたCCIパケット33であってもコンテンツ鍵(Kc)の計算は古いものと同一の方式であるため、古いCCI群しか解釈できない受信装置20aであってもコンテンツを復号することができる。

[0129] CCIパケット33はコンテンツパケット39と別パケットで送信されるため、コンテンツパケット39のフォーマットには依存せずにCCIを送信できる。また、新たに定義されたCCIをCCIパケット33に含める場合にも、コンテンツパケット39には影響を与えずに済む。

[0130] また、コンテンツデータを復号するコンテンツ鍵(Kc)の計算には、CCI群フィールドの値を利用するため、CCI群フィールドの値が通信途中で改変されたとしても、受信装置20aは正しいコンテンツ鍵(Kc)の値を取得することはできず、結果として改変されたCCI群フィールドの値としてコンテンツを解釈することはなく、コンテンツの著作権保護を図ることができる。

[0131] また、送信装置10aは受信装置20aごとにその受信装置20aがどのようなCCI Set IDを解釈できるかを区別せずに、同一のコンテンツを送信することができる。このため、送信装置10a内部での送信処理が容易になる。

[0132] (第2の実施形態)

第1の実施形態では各CCI群間での関連性がないフォーマットを定義した。第2の実施形態は、CCI群の中に、どの受信装置20aであっても解釈可能な必須CCI群を定義するものである。

[0133] 図13は第2の実施形態によるCCIパケット33のフォーマットを示す図である。図13に示すように、CCIパケット33のCCI群は、どの受信装置20aでも解釈可能な必須CCI群45と、図6に示すフォーマットの任意CCI群46とを有する。

[0134] このように必須CCI群45を定義することにより、送信装置10aと受信装置20aとの間で認識可能なCCI Set IDの組み合わせが一致しなかったとしても、必須CCIの部分については送信装置10aと受信装置20aの双方とも解釈可能であるため、最低限の相互接続を確保することができる。

[0135] なお、任意CCI群46は、(a) 必須CCI群45で定義されていないCCIのみを定義する手法、(b) 必須CCI群45で定義されているCCIと同じものも含むが、任意のフォーマットで定義するCCIを優先する手法などがある。

[0136] (b) の場合、例えば必須CCI群45には世代管理情報のみ定義されており、任意CCI群46の中のCCIフォーマットXには世代管理情報とレンタル時間に関するCCI "Rental Time" が定義される等が考えられる。このとき、送信装置10aが1世代に限りRental Timeで指定された時間までコピー可というコンテンツを送信する場合を考える。必須CCIとしてCopy One Generation、フォーマットXのCCIにはCopy One Generation/Rental Time=Nとしてしまうと、前述のように必須CCIしか解釈できない受信装置20aは時間に制限なく受信できるという問題がある。

[0137] しかしながら、必須CCI群45でCopy NeverのCCIを定義し、任意CCI群46の中のCCIフォーマットXのCCIをCopy One Generation/Rental Time=Nと定義しておけば、必須CCIしか解釈できない受信装置20aはコピーの記録は禁止され、CCIフォーマットXを解釈できる受信装置20aは1世代に限りRental Timeで指定された時間までコピー可としてコンテンツを受信する。

[0138] 本実施形態の場合、必須CCI群45しか解釈できない受信装置20aの利便性は低下してしまうが、無制限のコピーを禁止するという著作権者(送信装置10a)の意図を正しく受信装置20aに伝達することが保証される。これは、CCI Set IDのフォーマットを定義したことから実現できたことであり、図1で示すCCIのフォーマットでは実現できない。

[0139] 図14は第2の実施形態による受信装置20bの内部構成の一例を示すブロック図である。第1の実施形態における受信装置20bの内部構成との違いは必須CCI解析部57を備えている点である。

[0140] 任意CCI群46において、必須CCI群45で定義されていないCCIのみを定義する場合、必須CCI解析部57は必須CCI部分にどのようなCCIが含まれるかを解析し、その結果をCCI解析部25に通知する。一方、任意CCI群46で定義するCCIについてはCCI選別部55で選別する。CCI解析部25は、必須CCI解析部57の解析結果とCCI選別部55の選別結果に基づいて、コンテンツの受信処理に用いるCCIを決定する。

[0141] 任意CCI群46で定義するCCIが、必須CCI群45で定義されているCCIと同じものも含む場合に、任意CCI群46で定義するCCIを優先させることが可能である。この場合、CCI選別部55は受信したコンテンツに自装置が解釈可能なCCI Set IDが含まれているかどうか判断し、含まれている場合は解釈可能なCCIフォーマットで定義されたCCIを採用するようCCI解析部25に通知する。一方、含まれていない場合は、必須CCI解析部57が解析した必須CCI部分のCCIを採用するようCCI解析部25に通知する。

[0142] このように、第2の実施形態では、どの受信装置20bでも解釈可能な必須CCI群45をCCIパケット33の中を含めるため、どの受信装置20bでも必要最低限の受信処理を行うことができ、コンテンツの著作権保護を損なわない範囲で、コンテンツの有効活用を図れる。

[0143] (第3の実施形態)

第2の実施形態では、最低限の相互接続性を確保するために、CCIパケット33内に必須CCI群45を定義した。以下に説明する第3の実施形態では、CC

1パケット33のフォーマットは第1の実施形態と同じにするものの、自装置だけのレンダリング（再生処理）は許可することで、最低限の相互接続を保証するものである。

[0144] 図15は第3の実施形態によるCCIパケット33のフォーマットを示す図である。図15では、CCIパケット33にRendering Only47のフィールドを新たに定義している。Rendering Only47のフィールドは、ONの場合には自装置内部でのモニター出力が許可され、OFFの場合には出力が禁止されることを送信装置10aに通知するフィールドである。

[0145] このRendering Only47のフィールドは、図15に示すように、CCIパケット33のヘッダフィールドに設けられる。

[0146] 第3の実施形態による受信装置20cは、CCIパケット33に自装置で認識可能なCCI Set IDが含まれていない場合、Rendering Only47のフィールドをチェックする。Rendering Only47のフィールドはONの場合には自装置内部でのモニター出力が許可され、OFFの場合には出力が禁止される。CCIパケット33に自装置で認識可能なCCI Set IDが含まれている場合には、Rendering Only47のフィールドを無視して、その認識可能なCCI Set IDが示すCCI群のCCIに従って動作する。

[0147] 例えば、レンタル時間のような時間管理が必要なCCIの一つとして、蓄積は無制限に行ってもよいがX日以降でないと再生は禁止するといった封切り前のコンテンツを伝送する場合、時間管理のCCIを解釈可能な受信装置20cは蓄積したり再生したりできるが、時間管理ができない受信装置20cは、蓄積はもちろん再生も禁止されなければならない。この場合、送信装置10aはRendering Only47のフィールドをOFFとして送信することで、時間管理のCCIを定義したCCI Set IDが解釈できる受信装置20cのみ、封切り前のコンテンツを蓄積及び再生することを許可し、それ以外の受信装置20cには蓄積も再生もできないようにする制限を実現できる。

[0148] 図16は第3の実施形態による受信装置20cの内部構成の一例を示すブロック図である。図16の受信装置20cは、コンテンツ処理部28の内部

に、蓄積部 28 a、外部出力部 28 b、内部レンダリング部 28 c を設けている。この他、受信装置 20 c は CCI 破棄部 58 を有する。

[0149] 蓄積部 28 a はハードディスクなどにコンテンツを蓄積する処理を行う。外部出力部 28 b はアナログ端子や HDMI などのデジタル端子にコンテンツを出力する処理を行う。内部レンダリング部 28 c は自装置に備え付けの不図示の表示装置にコンテンツを再生出力する処理を行う。

[0150] CCI 選別部 55 にて受信したコンテンツに付随する CCI パケット 33 に CCI Set ID 管理部 56 で管理する CCI Set ID が含まれていない場合、CCI 解析部 25 は Rendering Only 47 のフィールドをチェックし、Rendering Only 47 のフィールドが ON になっている場合は自装置に設けた表示装置への再生出力を許可する CCI を内部レンダリング部 28 c に設定する。

[0151] もちろん、ハードディスクなどの蓄積機能を持たない装置や外部出力端子を備えていない機器も考えられるため、蓄積部 28 a、外部出力部 28 b、内部レンダリング部 28 c のすべてを備えている必要はない。

[0152] このように、第 3 の実施形態では、CCI パケット 33 のヘッダフィールドに Rendering Only 47 のフィールドを設けるため、受信装置 20 c が CCI パケット 33 を正しく解釈できない場合には、CCI 破棄部 58 で CCI パケット 33 の内容を破棄して、Rendering Only 47 のフィールドの値によって受信装置 20 c の動作を制御できる。したがって、CCI パケット 33 を正しく解釈できない受信装置 20 c が送信装置 10 a の意図に反したコンテンツ受信処理を行うおそれがなくなり、コンテンツの著作権保護が図れる。

[0153] なお、第 1 及び第 2 の実施形態では、受信装置 20 c 内のコンテンツ処理部 28 の内部処理を細分化していないが、図 16 に示す蓄積部 28 a、外部出力部 28 b 及び内部レンダリング部 28 c の少なくとも一つを備えていることが考えられる。

[0154] (第 4 の実施形態)

第 1 の実施形態では、送信装置が送信する CCI パケットに CCI 群を識別する情報 (CCI Set ID) を定義し、受信装置は CCI Set ID により自装置が解釈可能

なCCI群と一致するCCI群のみ取得する手法を示した。第4の実施形態では、特定の受信装置に解釈させるべき特定のCCI群を送信装置が指定することを実現するものである。

[0155] 図17は第4の実施形態によるCCIパケット33のフォーマットを示す図である。図17では、CCI群の中に受信装置のデバイスIDのリスト(Device IDs、装置識別情報)を記述したデバイスIDフィールド61が含まれている点が図6とは異なる。デバイスIDのリストは、そのデバイスIDが示すCCI群を利用することができるデバイスのリストを示す情報である。なお、図17ではDevice IDフィールドを各CCI群フィールドの中に定義したが、CCIパケットの先頭に、どのCCI群フィールドはどのDevice IDが利用可能かを示すマッピング情報を定義してもよい。

[0156] 図18は第4の実施形態による送信装置10bの内部構成を示すブロック図である。デバイスID管理部62を備えている点と、CCI挿入部にデバイスIDを挿入する点が図8と異なる。各受信装置にはそれぞれの機器を識別するためにユニークなID(Device ID)が割り振られている。このデバイスIDは複数の受信装置で重複した値とならないようライセンス機関等が発行するものとする。

[0157] CCI挿入部はどの受信装置にどのようなCCIでコンテンツの受信処理を行わせるか指示するために受信装置のデバイスIDを挿入する処理を行う。たとえば、受信装置Aに対してCCI Set ID(0)で示すCCIにてコンテンツの受信処理を行わせ、受信装置Bに対してCCI Set ID(1)で示すCCIにてコンテンツの受信処理を行わせる場合、送信装置10bはCCI Set ID(0)のDevice IDsフィールドには受信装置AのデバイスIDを挿入し、CCI Set ID(1)のDevice IDsフィールドには受信装置BのデバイスIDを挿入する。

[0158] なお、Device IDsフィールドは複数のデバイスIDを格納してもよい。その場合、いくつのデバイスIDがDevice IDsフィールドに含まれているかを示すために不図示のLengthフィールドを定義してもよい。なお、Device IDsフィールドに特殊な値(たとえばオール0の値)を挿入したり、Device IDsフィール

ドを空にしたりすることで、すべての受信装置に対してCCI群を利用してもよいことを示してもよい。

[0159] 図19は第4の実施形態による受信装置20dの内部構成を示すブロック図である。認証・鍵交換処理部にデバイスID管理部63を備えている点と、CCI選別部にデバイスID判定部（装置識別情報判定部）64を備えている点が図10と異なる。デバイスID管理部63はライセンス機関等から与えられたデバイスIDを格納する処理部である。デバイスID判定部64は、受信したCCIパケットに含まれるCCI群のうち、Device IDsフィールドを確認して自装置が利用可能なCCI群を選別する処理を行う。

[0160] 本実施形態において、CCI Set IDは同じでDevice IDsが異なるCCIパケットを設けてもよい。たとえば、CCI Set ID(0)には世代管理情報とコピー許可回数の二つのCCIが含まれているとする。受信装置A、BともCCI Set ID(0)が解釈可能とする。受信装置Aに対しては世代管理情報をCopy One Generationかつコピー許可回数を3とし、受信装置Bに対しては世代管理情報をCopy One Generationかつコピー許可回数を5とするコンテンツを送信する場合を考える。送信装置10bは一つ目のCCI群はCCI Set ID(0)、受信装置AのデバイスID、Copy One Generation, 3とし、もう一つのCCI群はCCI Set ID(0)、受信装置BのデバイスID、Copy One Generation, 5というようなCCIパケットを送信する。受信装置A、BはCCIパケットのCCI Set IDとDevice IDsフィールドから、自装置が解釈してよいCCI群を抽出し、そのCCI群で示されるCCIに従ってコピー制御を行う。

[0161] このように、第4の実施形態では、CCIパケット33にDevice IDsフィールドを定義し、どのCCI群をどの受信装置に解釈させてもよいか送信装置10bが指定することができる。これにより、送信装置10bは受信装置20dからコンテンツ受信要求を受信した際、そのコンテンツ受信要求がどの受信装置からのものであるか識別する必要なく、どの受信装置に対しても同様のCCIパケット33を送信することができるため、送信装置10bの内部構成を簡易化することができる。また個々の受信装置20dは自装置で解釈すべきCCI

群をCCIパケット内のデバイスIDで特定できるため、マルチキャスト伝送が可能となり、通信帯域を節約することができる。

[0162] 上述した実施形態で説明した送信装置10a、10bおよび受信装置20a～20dの少なくとも一部は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、送信装置10aおよび受信装置20a～20dの少なくとも一部の機能を実現するプログラムをフレキシブルディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

[0163] また、送信装置10a、10bおよび受信装置20a～20dの少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

[0164] 上記の記載に基づいて、当業者であれば、本発明の追加の効果や種々の変形を想到できるかもしれない。したがって、本発明の態様は、上述した個々の実施形態には限定されない。特許請求の範囲に規定された内容およびその均等物から導き出される本発明の概念的な思想と趣旨を逸脱しない範囲で種々の追加、変更および部分的削除が可能である。

符号の説明

- [0165] 10、10a、10b 送信装置
16 コンテンツパケット化部
17 コンテンツ暗号部
20、20a、20b、20c、20d 受信装置
25 CCI解析部
27 CCI設定部
28 コンテンツ処理部

- 3 3 CCI パケット
- 3 9 コンテンツパケット
- 5 2 パケット選別部
- 5 3 コンテンツパケットヘッダ解析部
- 5 4 CCI パケットヘッダ解析部
- 5 5 CCI 選別部
- 5 6 CCI Set ID 管理部
- 5 7 必須 CCI 解析部
- 6 2, 6 3 デバイス ID 管理部
- 6 4 デバイス ID 判定部

請求の範囲

- [請求項1] 通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、
- 前記通信装置から送信されたパケットが暗号化コンテンツを含むコンテンツパケットか、または少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCIパケットかを判別するパケット選別部と、
- 前記認証及び鍵交換処理で生成した認証鍵と、前記CCIパケットに含まれるコピー制御情報とに基づいてコンテンツ鍵を生成するコンテンツ鍵生成部と、
- 前記CCIパケットの後に続いて受信された前記コンテンツパケットに含まれる暗号化コンテンツを、前記コンテンツ鍵に基づいて復号してコンテンツデータを生成するコンテンツ復号部と、
- 認識可能なコピー制御情報に対応するCCI識別子を管理するCCI識別子管理部と、
- 前記パケット選別部により前記CCIパケットと判別された場合は、前記CCIパケットに含まれるCCI識別子が前記CCI識別子管理部で管理されているCCI識別子と一致するか否かを判定して、受信処理に用いるべきCCI識別子を選別するCCI選別部と、
- 前記CCI選別部により選別されたCCI識別子に対応するコピー制御情報を解析するCCI解析部と、
- 前記CCI解析部による解析結果に基づいて、前記CCIパケットの後に続いて受信された前記コンテンツパケットに対応する前記コンテンツデータの受信処理を行うコンテンツ処理部と、
- 前記認証及び鍵交換処理を行うための第1の通信コネクション部と、
- 前記コンテンツパケット及び前記CCIパケットを伝送するための第2の通信コネクション部と、を備えることを特徴とする情報処理装置

。

[請求項2] 前記コンテンツ鍵生成部は、前記認証鍵と、前記CCI解析部で解析されたコピー制御情報と、前記通信装置が所定の条件で随時更新する鍵情報と、を用いて前記コンテンツ鍵を生成することを特徴とする請求項1に記載の情報処理装置。

[請求項3] 前記コンテンツ鍵生成部は、前記認証鍵及び前記コピー制御情報に対応するハッシュ値と、前記通信装置が所定の条件で随時更新する鍵情報とを用いて前記コンテンツ鍵を生成することを特徴とする請求項1に記載の情報処理装置。

[請求項4] 前記通信装置のすべての通信相手が認識可能なコピー制御情報およびそれに対応するCCI識別子が前記CCIパケットに含まれる場合に、その内容を解析する必須CCI解析部を備え、

前記コンテンツ処理部は、前記CCIパケットに含まれるコピー制御情報に対応する識別子のいずれもが前記CCI識別子管理部で管理されている識別子と一致しないと検出された場合には、前記必須CCI解析部による解析結果に基づいて、前記コンテンツデータの受信処理を行うことを特徴とする請求項1乃至3のいずれかに記載の情報処理装置。

[請求項5] 前記コンテンツ処理部は、前記CCIパケットに含まれるコピー制御情報に対応する識別子のいずれもが前記CCI識別子管理部で管理されている識別子と一致しないと検出され、かつ前記CCIパケットに含まれる前記CCI群とは別個に、特定のコピー制御情報が前記CCIパケットに含まれている場合には、前記特定のコピー制御情報に基づいて、前記コンテンツデータの受信処理を行うことを特徴とする請求項1乃至3のいずれかに記載の情報処理装置。

[請求項6] 前記コンテンツ処理部が行う前記コンテンツデータの受信処理は、前記コンテンツデータの蓄積、外部出力および自装置内での再生の少なくとも一つであることを特徴とする請求項1乃至5のいずれかに記

載の情報処理装置。

[請求項7]

前記CCIパケットは、個々のCCI群ごとに、対応するCCI群に基づいてコンテンツ受信処理を行う装置を指定する装置種別情報を含んでおり、

前記CCIパケットに含まれるCCI群のうち、前記装置識別情報が自装置の装置識別情報と一致するCCI群が存在するか否かを判定する装置識別情報判定部を備え、

前記CCI選別部は、前記CCIパケットに含まれるCCI識別子が前記CCI識別子管理部で管理されているCCI識別子と一致するか否かの判定結果と、前記装置識別情報判定部の判定結果とに基づいて、受信処理に用いるべきCCI群を選別することを特徴とする請求項1～6のいずれかに記載の情報処理装置。

[請求項8]

通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、

前記認証及び鍵交換処理に成功した前記通信装置からコンテンツ要求を受けた場合に、対応するコンテンツデータの少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCIパケットを生成するCCIパケット化部と、

前記認証及び鍵交換処理で生成した認証鍵と、前記CCIパケットに含まれるコピー制御情報とに基づいて、前記コンテンツデータを暗号化するためのコンテンツ鍵を生成するコンテンツ鍵生成部と、

前記認証鍵に対応するラベル情報と、前記コンテンツ鍵を用いて前記コンテンツデータを暗号化した暗号化コンテンツと、を含むコンテンツパケットを生成するコンテンツパケット生成部と、

前記CCIパケットを送信した後に、前記CCIパケットに含まれるコピー制御情報が適用される前記コンテンツパケットを送信するデータ出力部と、を備えることを特徴とする情報処理装置。

[請求項9]

前記コンテンツ鍵生成部は、前記認証鍵と、前記暗号化コンテンツ

に対応するコピー制御情報と、前記通信装置が所定の条件で随時更新する鍵情報と、を用いて前記コンテンツ鍵を生成し、

前記コンテンツパケット生成部は、前記ラベル情報と、前記鍵情報と、前記暗号化コンテンツのビット長とを含む前記コンテンツパケットを生成することを特徴とする請求項 8 に記載の情報処理装置。

[請求項10]

前記CCIパケット化部は、すべての前記通信装置が認識可能なコピー制御情報およびそのCCI識別子を含む必須CCI群を有する前記CCIパケットを生成することを特徴とする請求項 8 または 9 に記載の情報処理装置。

補正された請求の範囲
[2010年5月24日 (24.05.2010) 国際事務局受理]

- [請求項1] 通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、
- 前記通信装置から送信されたパケットが暗号化コンテンツを含むコンテンツパケットか、または少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCIパケットかを判別するパケット選別部と、
- 前記認証及び鍵交換処理で生成した認証鍵と、前記CCIパケットに含まれるコピー制御情報とに基づいてコンテンツ鍵を生成するコンテンツ鍵生成部と、
- 前記CCIパケットの後に続いて受信された前記コンテンツパケットに含まれる暗号化コンテンツを、前記コンテンツ鍵に基づいて復号してコンテンツデータを生成するコンテンツ復号部と、
- 認識可能なコピー制御情報に対応するCCI識別子を管理するCCI識別子管理部と、
- 前記パケット選別部により前記CCIパケットと判別された場合は、前記CCIパケットに含まれるCCI識別子が前記CCI識別子管理部で管理されているCCI識別子と一致するか否かを判定して、受信処理に用いるべきCCI識別子を選別するCCI選別部と、
- 前記CCI選別部により選別されたCCI識別子に対応するコピー制御情報を解析するCCI解析部と、
- 前記CCI解析部による解析結果に基づいて、前記CCIパケットの後に続いて受信された前記コンテンツパケットに対応する前記コンテンツデータの受信処理を行うコンテンツ処理部と、
- 前記認証及び鍵交換処理を行うための第1の通信コネクション部と、
- 前記コンテンツパケット及び前記CCIパケットを伝送するための第2の通信コネクション部と、を備えることを特徴とする情報処理装置

。

[請求項2] 前記コンテンツ鍵生成部は、前記認証鍵と、前記CCI解析部で解析されたコピー制御情報と、前記通信装置が所定の条件で随時更新する鍵情報と、を用いて前記コンテンツ鍵を生成することを特徴とする請求項1に記載の情報処理装置。

[請求項3] 前記コンテンツ鍵生成部は、前記認証鍵及び前記コピー制御情報に対応するハッシュ値と、前記通信装置が所定の条件で随時更新する鍵情報とを用いて前記コンテンツ鍵を生成することを特徴とする請求項1に記載の情報処理装置。

[請求項4] (補正後) 前記通信装置のすべての通信相手が認識可能なコピー制御情報およびそれに対応するCCI識別子が前記CCIパケットに含まれる場合に、その内容を解析する必須CCI解析部を備え、

前記コンテンツ処理部は、前記CCIパケットに含まれるコピー制御情報に対応する識別子のいずれもが前記CCI識別子管理部で管理されている識別子と一致しないと検出された場合には、前記必須CCI解析部による解析結果に基づいて、前記コンテンツデータの受信処理を行うことを特徴とする請求項1に記載の情報処理装置。

[請求項5] (補正後) 前記コンテンツ処理部は、前記CCIパケットに含まれるコピー制御情報に対応する識別子のいずれもが前記CCI識別子管理部で管理されている識別子と一致しないと検出され、かつ前記CCIパケットに含まれる前記CCI群とは別個に、特定のコピー制御情報が前記CCIパケットに含まれている場合には、前記特定のコピー制御情報に基づいて、前記コンテンツデータの受信処理を行うことを特徴とする請求項1に記載の情報処理装置。

[請求項6] (補正後) 前記コンテンツ処理部が行う前記コンテンツデータの受信処理は、前記コンテンツデータの蓄積、外部出力および自装置内での再生の少なくとも一つであることを特徴とする請求項1に記載の情報処理装置。

[請求項7] (補正後) 前記CCIパケットは、個々のCCI群ごとに、対応するCCI群に基づいてコンテンツ受信処理を行う装置を指定する装置種別情報を含んでおり、

前記CCIパケットに含まれるCCI群のうち、前記装置識別情報が自装置の装置識別情報と一致するCCI群が存在するか否かを判定する装置識別情報判定部を備え、

前記CCI選別部は、前記CCIパケットに含まれるCCI識別子が前記CCI識別子管理部で管理されているCCI識別子と一致するか否かの判定結果と、前記装置識別情報判定部の判定結果とに基づいて、受信処理に用いるべきCCI群を選別することを特徴とする請求項1に記載の情報処理装置。

[請求項8] 通信装置との間で認証及び鍵交換処理を行う認証及び鍵交換処理部と、

前記認証及び鍵交換処理に成功した前記通信装置からコンテンツ要求を受けた場合に、対応するコンテンツデータの少なくとも一つのコピー制御情報及びCCI群識別子の組合せからなるCCI群を少なくとも一つ含むCCIパケットを生成するCCIパケット化部と、

前記認証及び鍵交換処理で生成した認証鍵と、前記CCIパケットに含まれるコピー制御情報とに基づいて、前記コンテンツデータを暗号化するためのコンテンツ鍵を生成するコンテンツ鍵生成部と、

前記認証鍵に対応するラベル情報と、前記コンテンツ鍵を用いて前記コンテンツデータを暗号化した暗号化コンテンツと、を含むコンテンツパケットを生成するコンテンツパケット生成部と、

前記CCIパケットを送信した後に、前記CCIパケットに含まれるコピー制御情報が適用される前記コンテンツパケットを送信するデータ出力部と、を備えることを特徴とする情報処理装置。

[請求項9] 前記コンテンツ鍵生成部は、前記認証鍵と、前記暗号化コンテンツに対応するコピー制御情報と、前記通信装置が所定の条件で随時更新

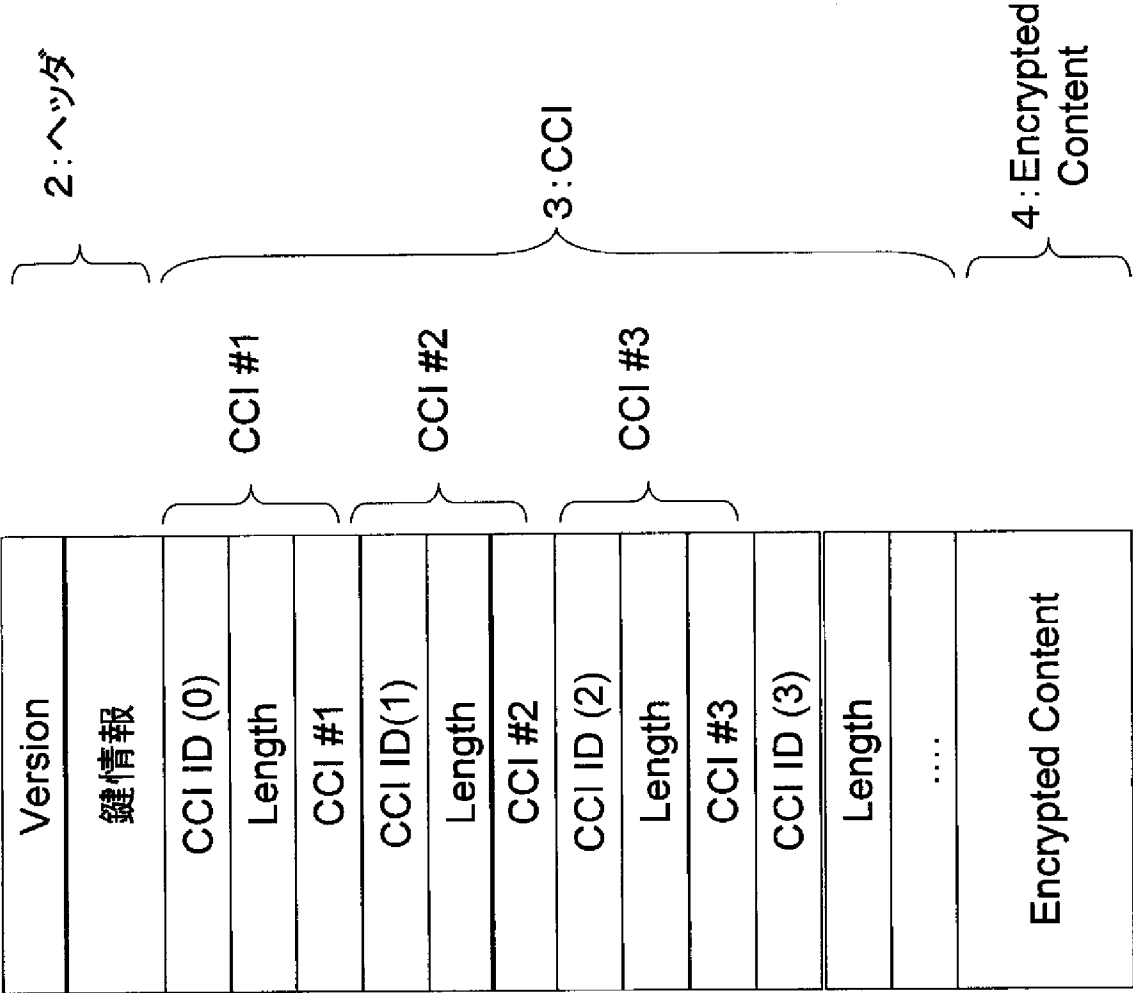
する鍵情報と、を用いて前記コンテンツ鍵を生成し、

前記コンテンツパケット生成部は、前記ラベル情報と、前記鍵情報と、前記暗号化コンテンツのビット長とを含む前記コンテンツパケットを生成することを特徴とする請求項 8 に記載の情報処理装置。

[請求項10]

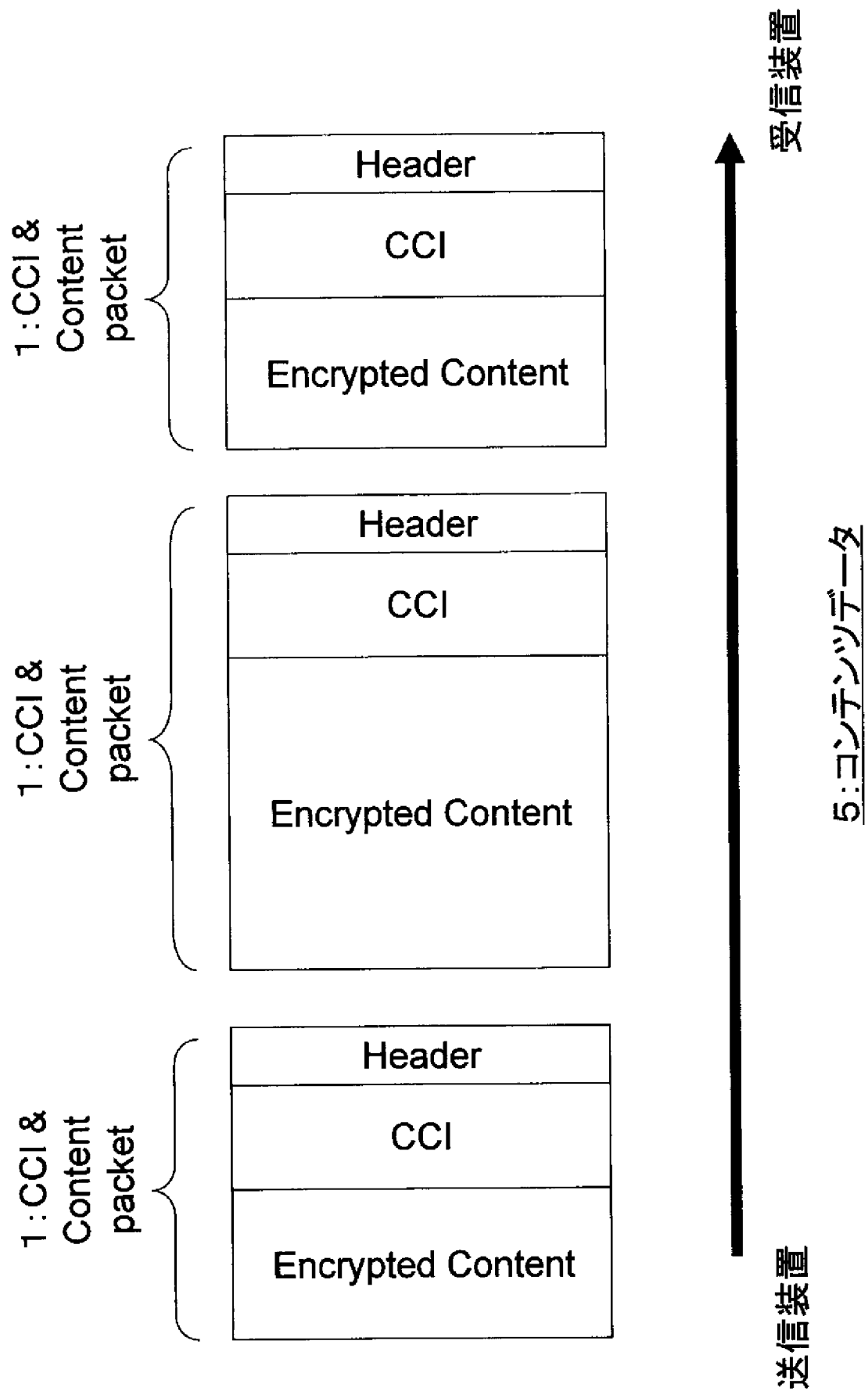
(補正後) 前記CCIパケット化部は、すべての前記通信装置が認識可能なコピー制御情報およびそのCCI識別子を含む必須CCI群を有する前記CCIパケットを生成することを特徴とする請求項 8 に記載の情報処理装置。

[図1]

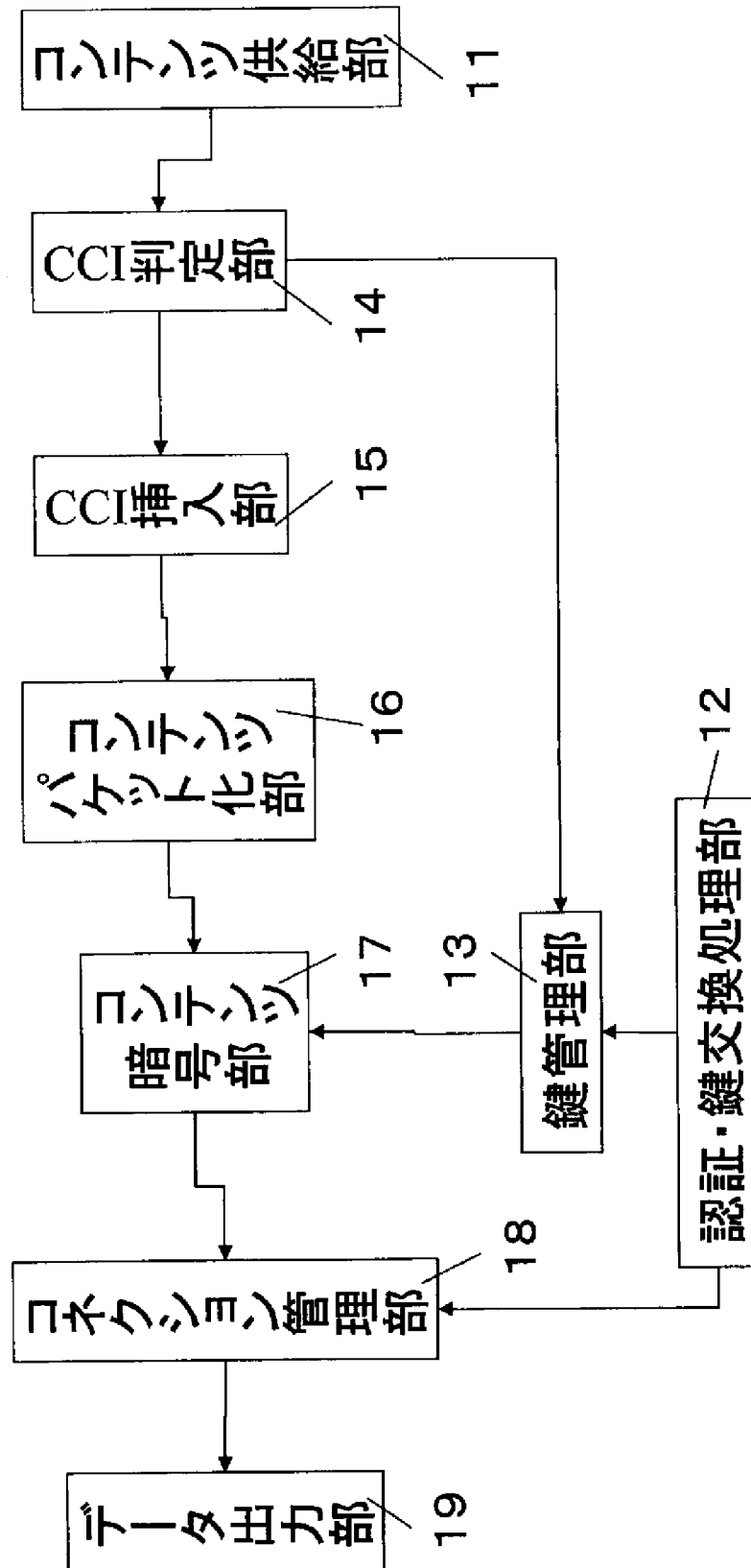


1: CCI & コンテンツパッケージ

[図2]

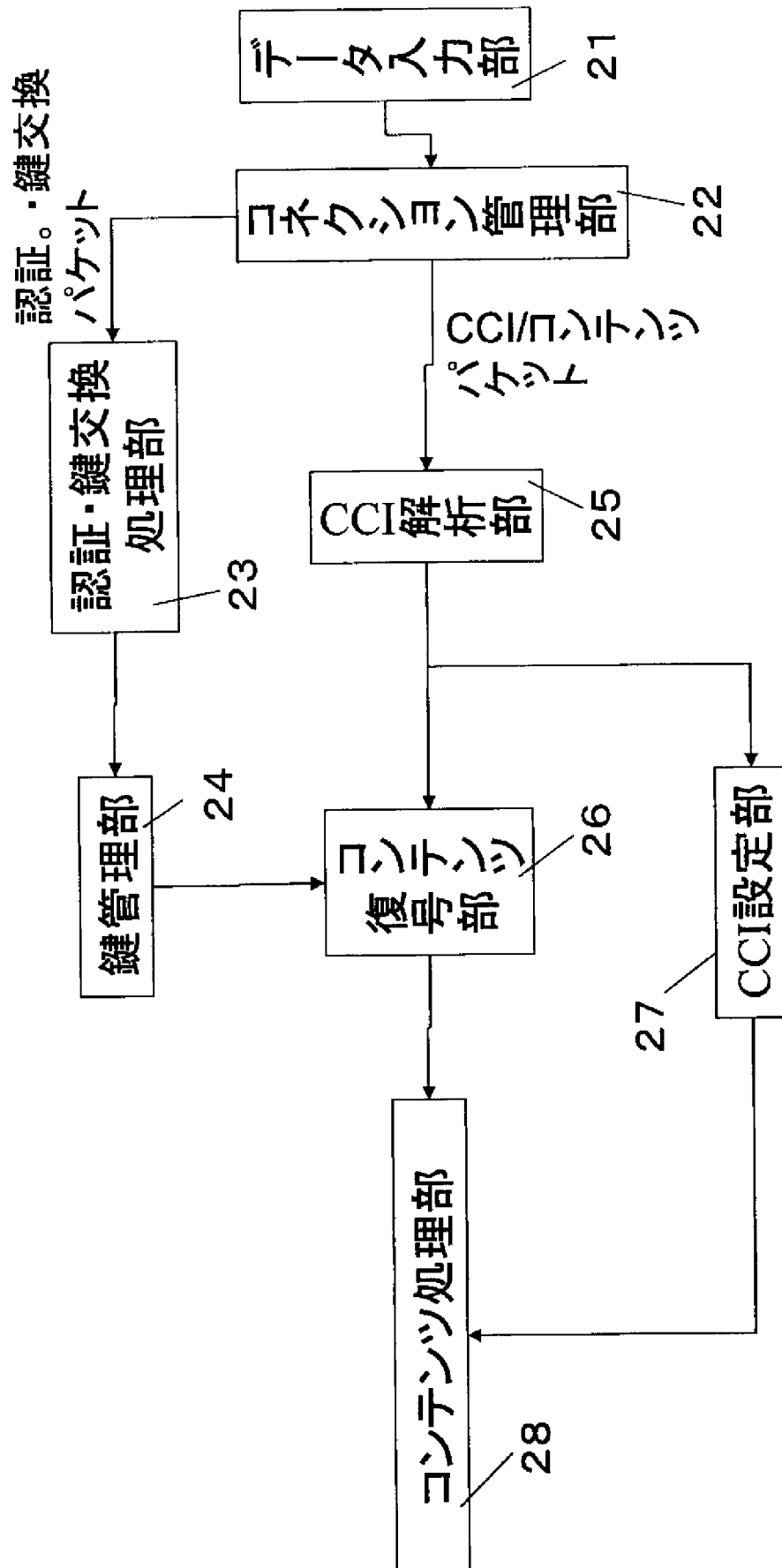


[図3]

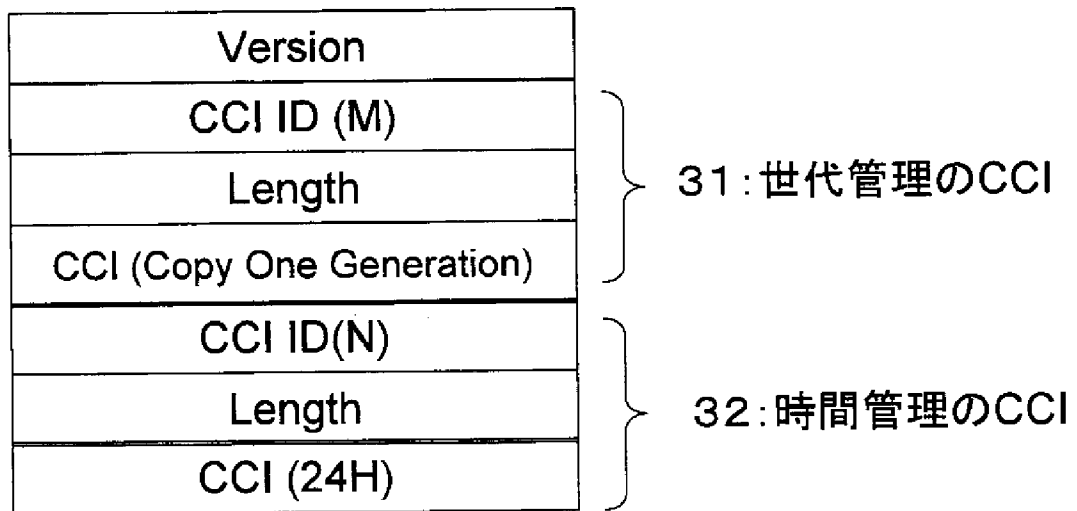


10: 送信装置

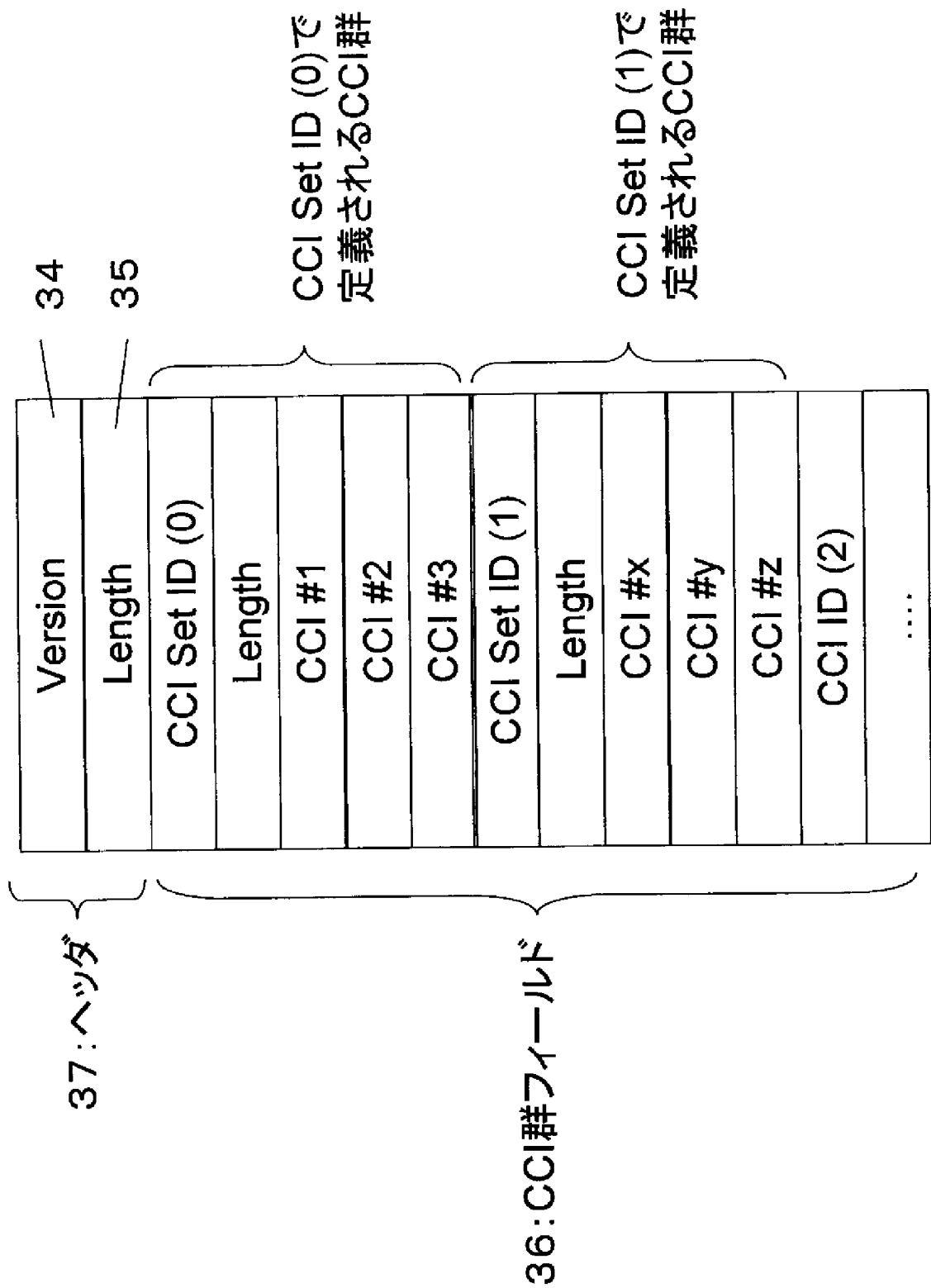
[図4]



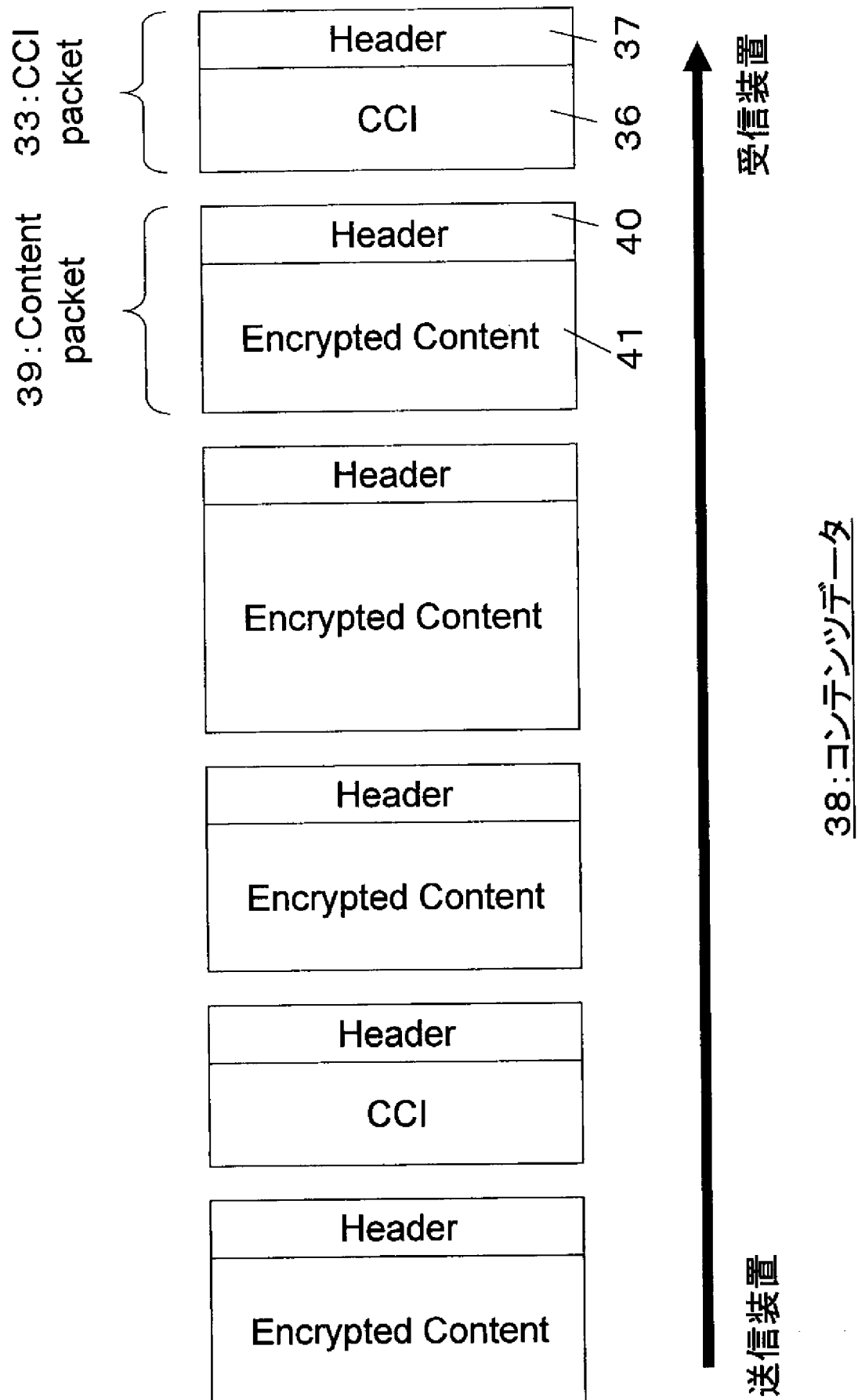
[図5]



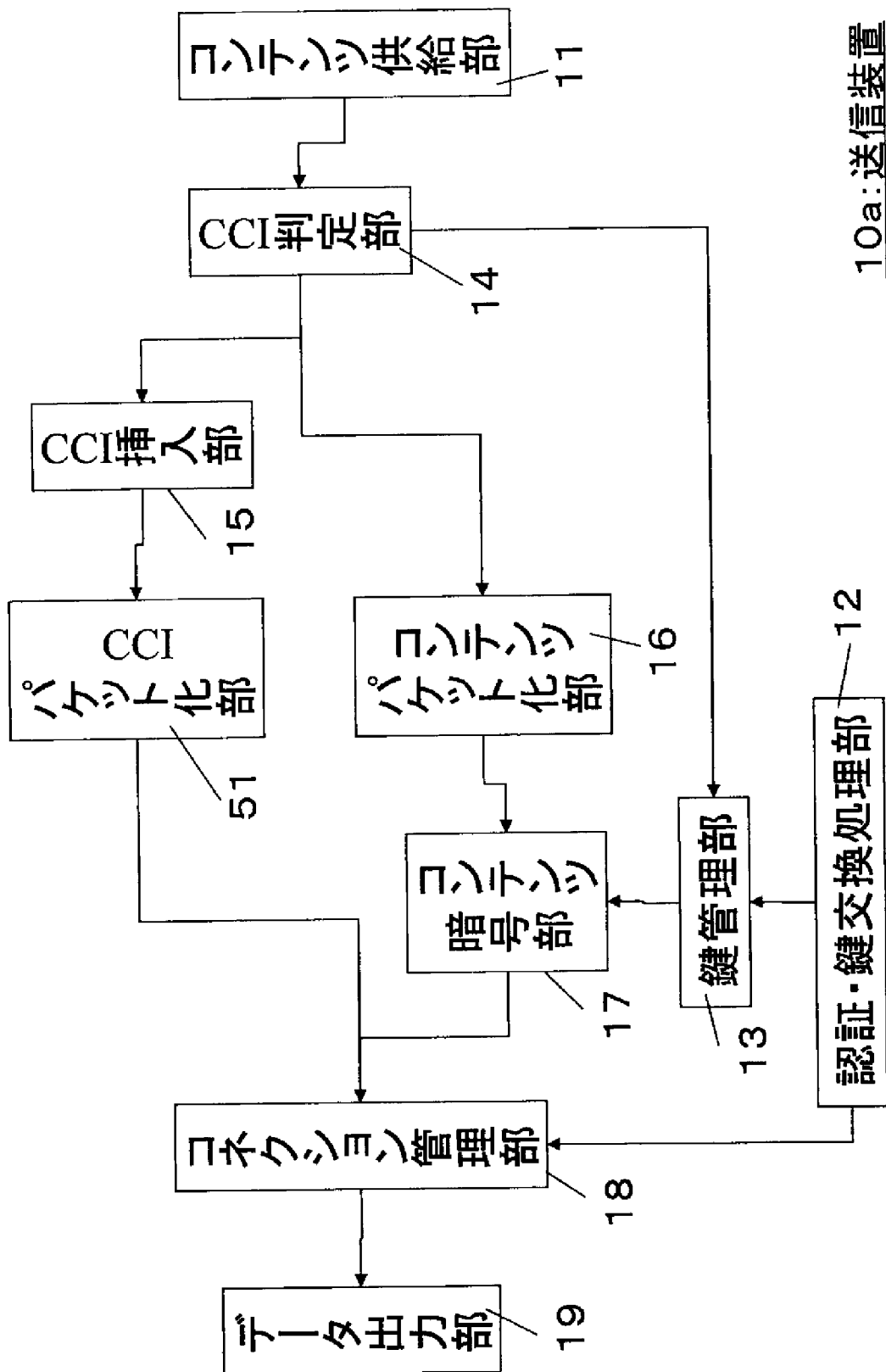
[図6]



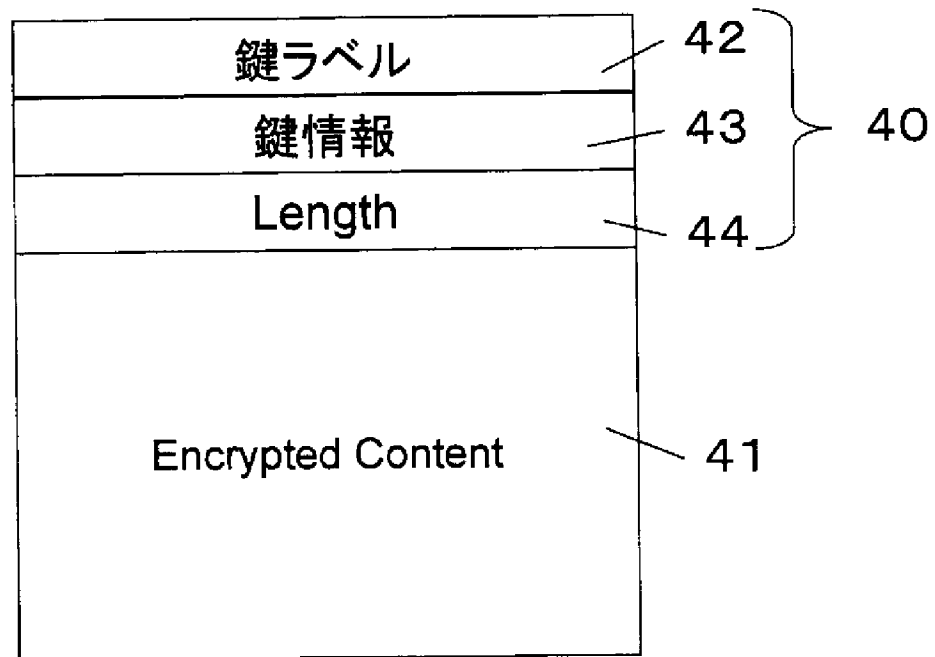
[図7]



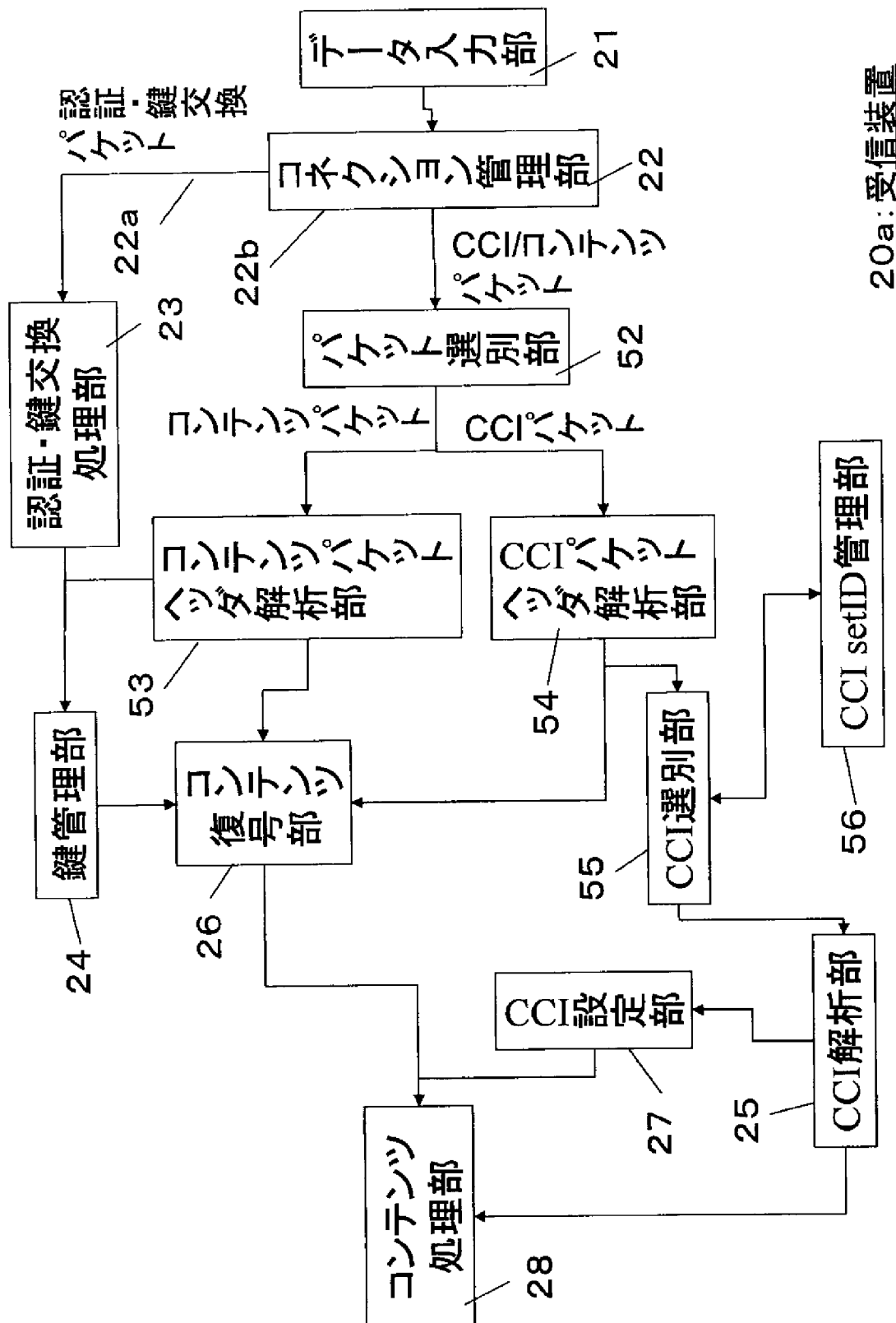
[図8]



[図9]

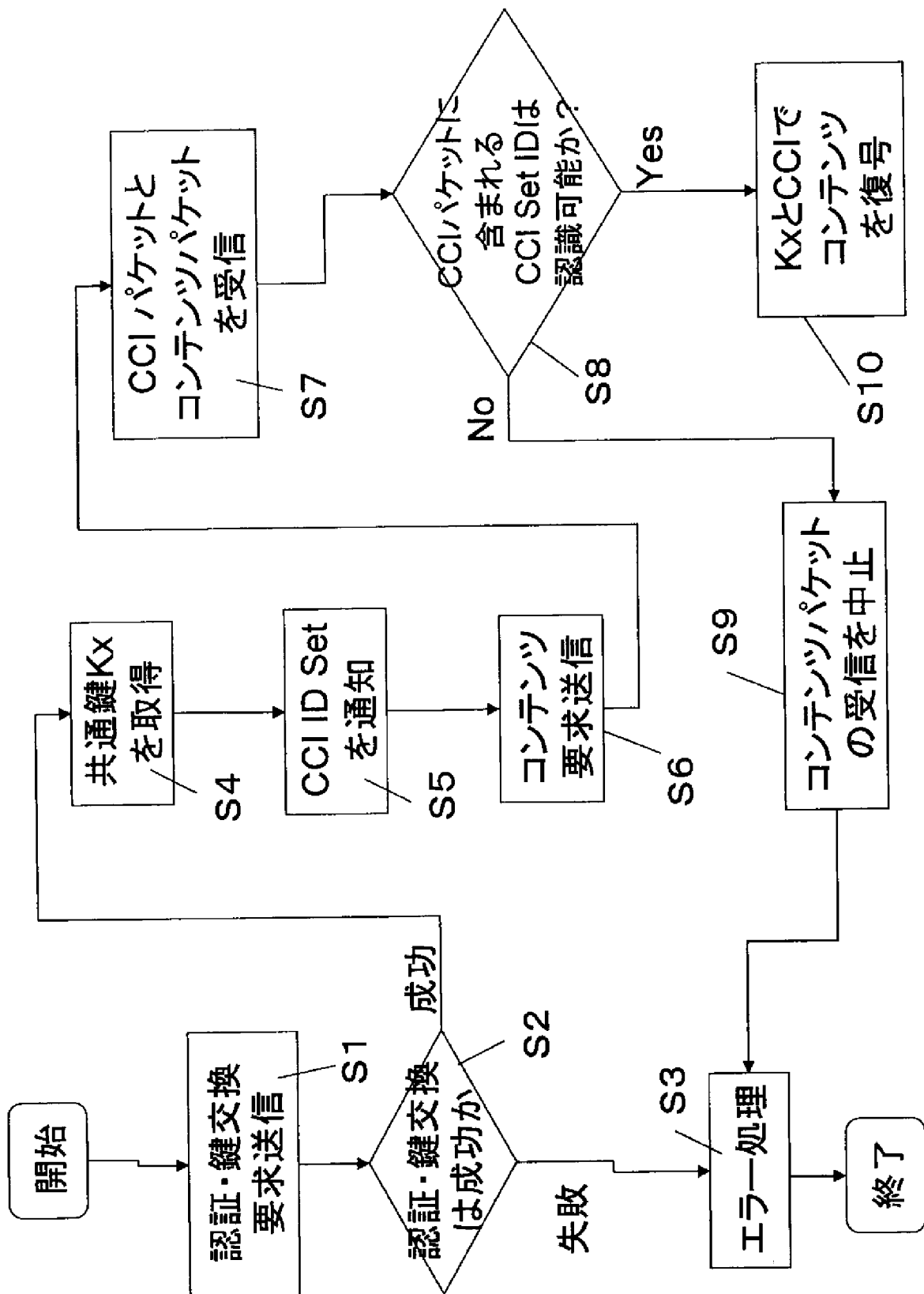
39:コンテンツパッケージ

[図10]

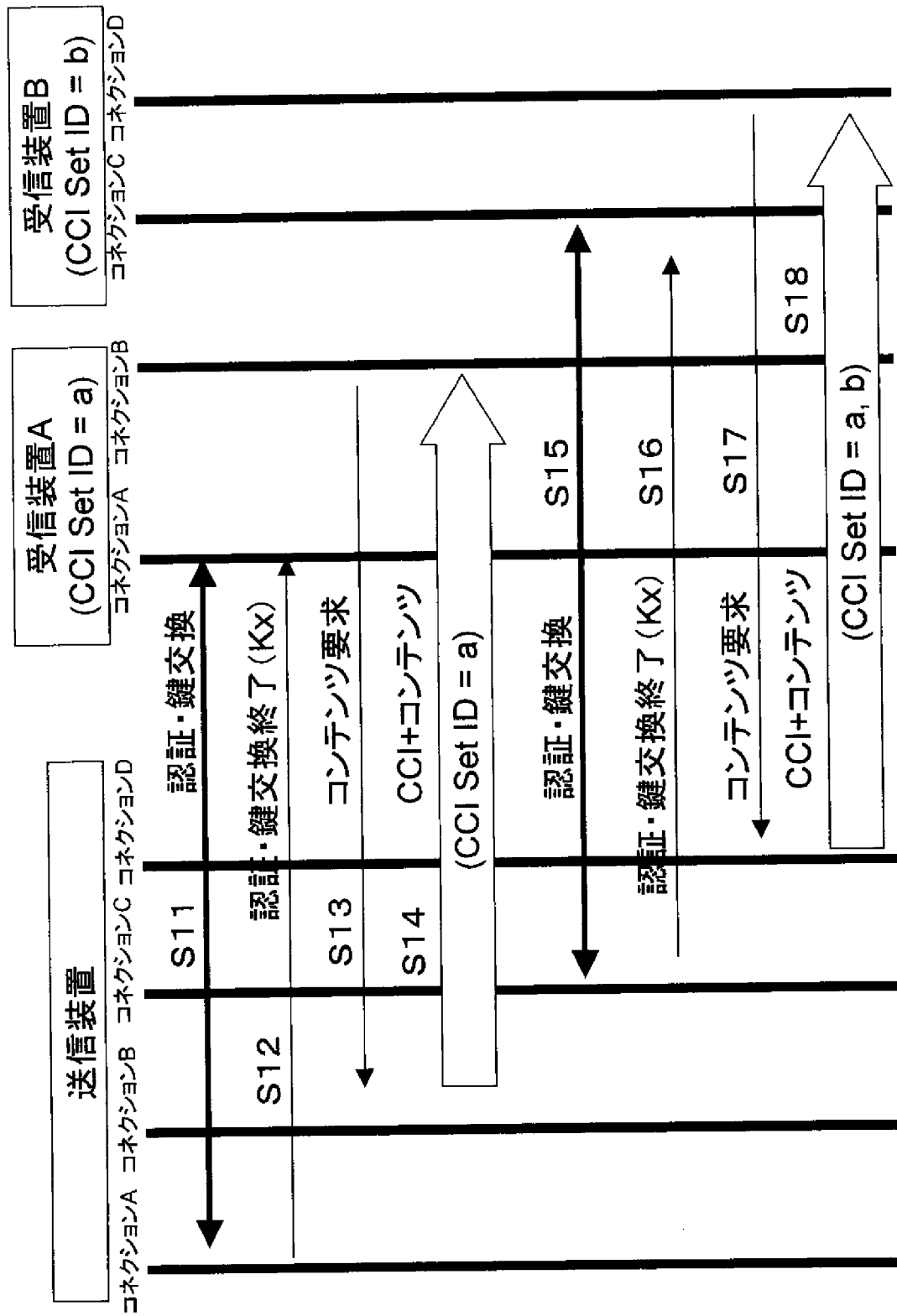


20a: 受信装置

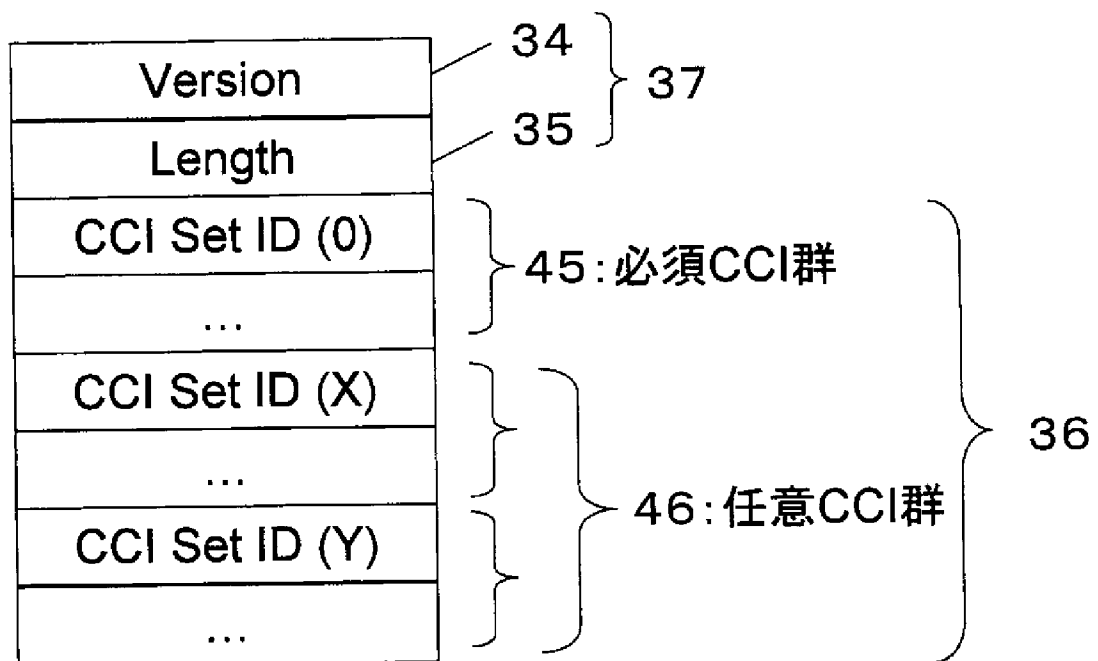
[図11]



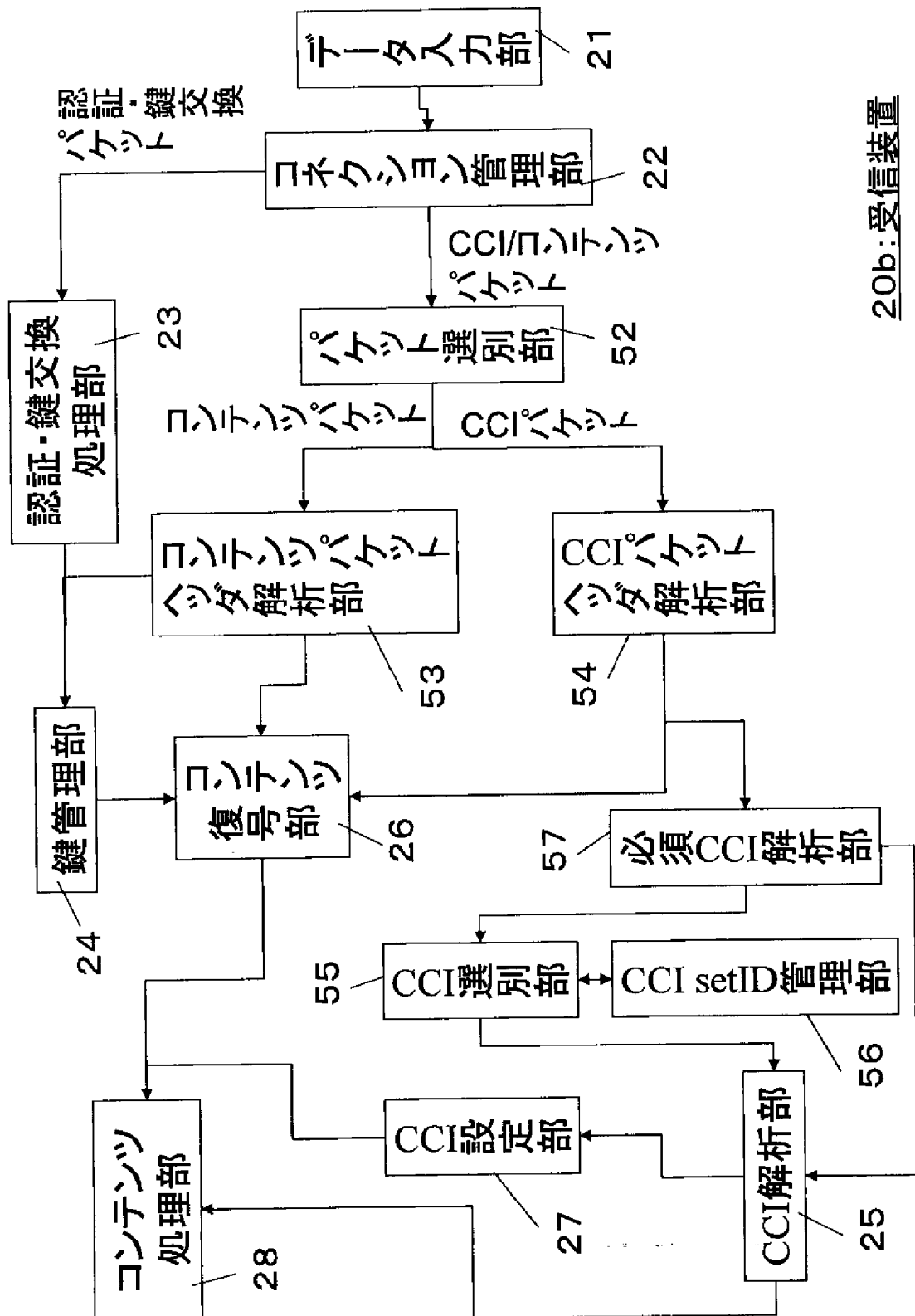
[図12]



[図13]

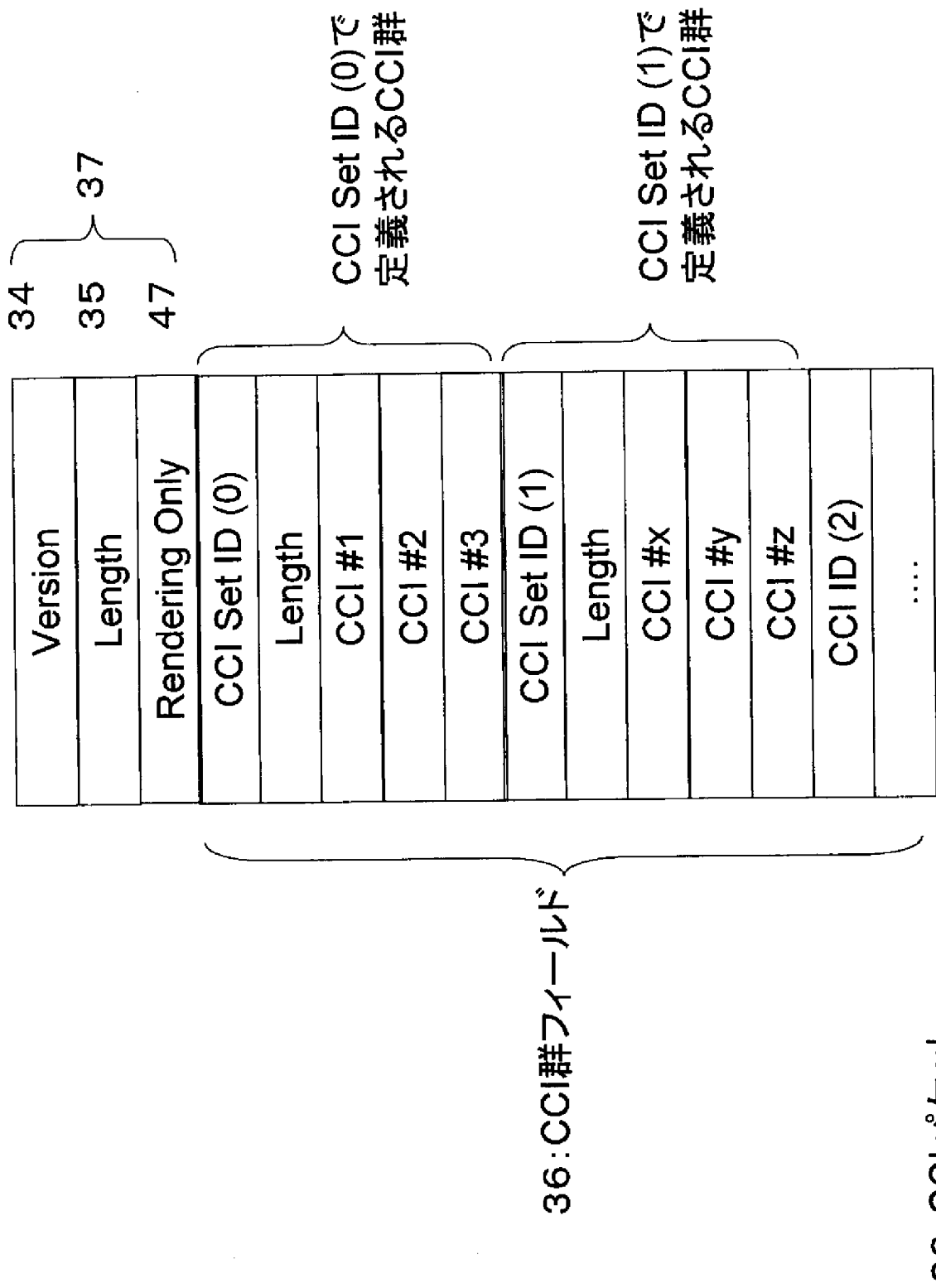
33: CCIパケット

[図14]

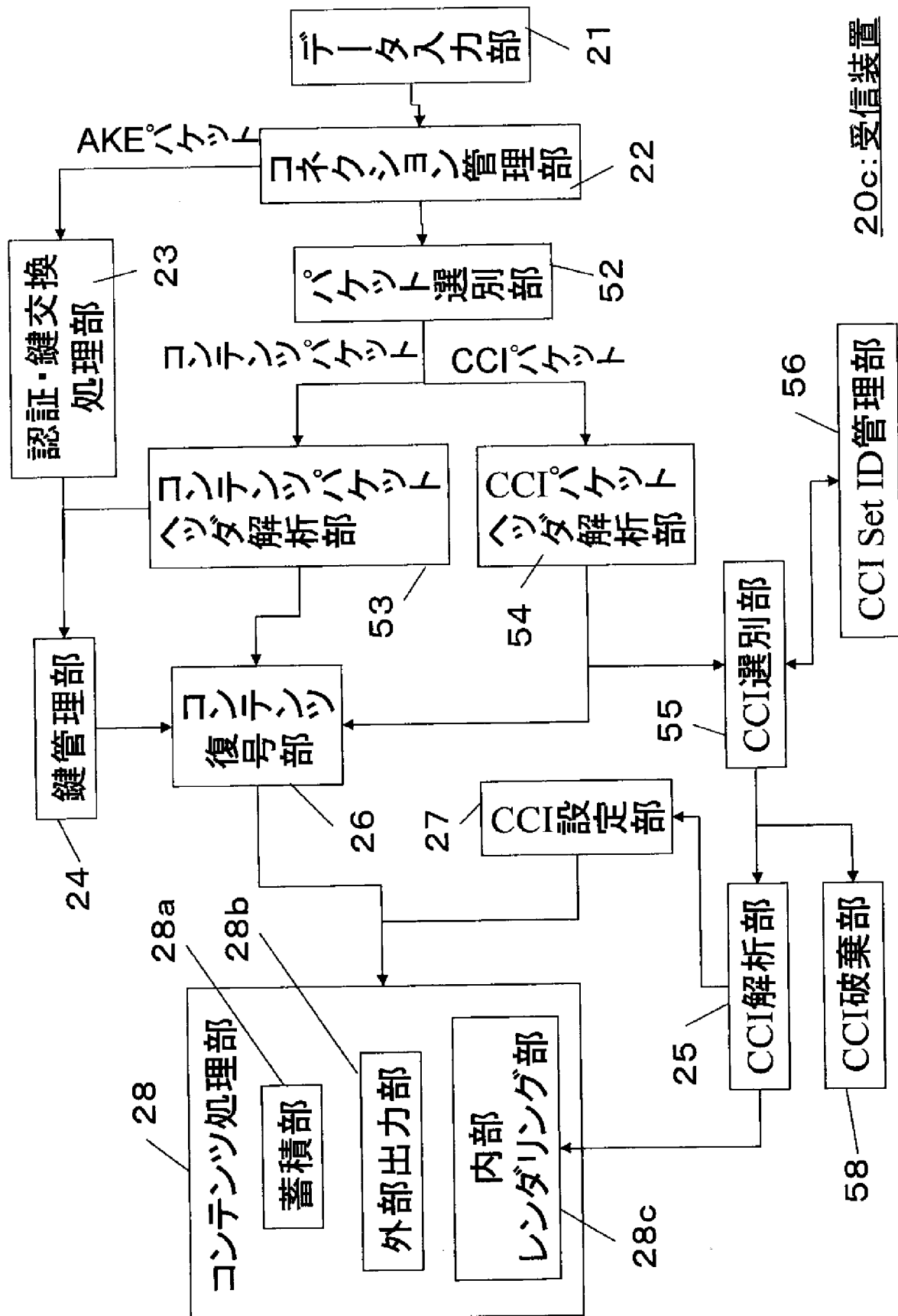


20b: 受信装置

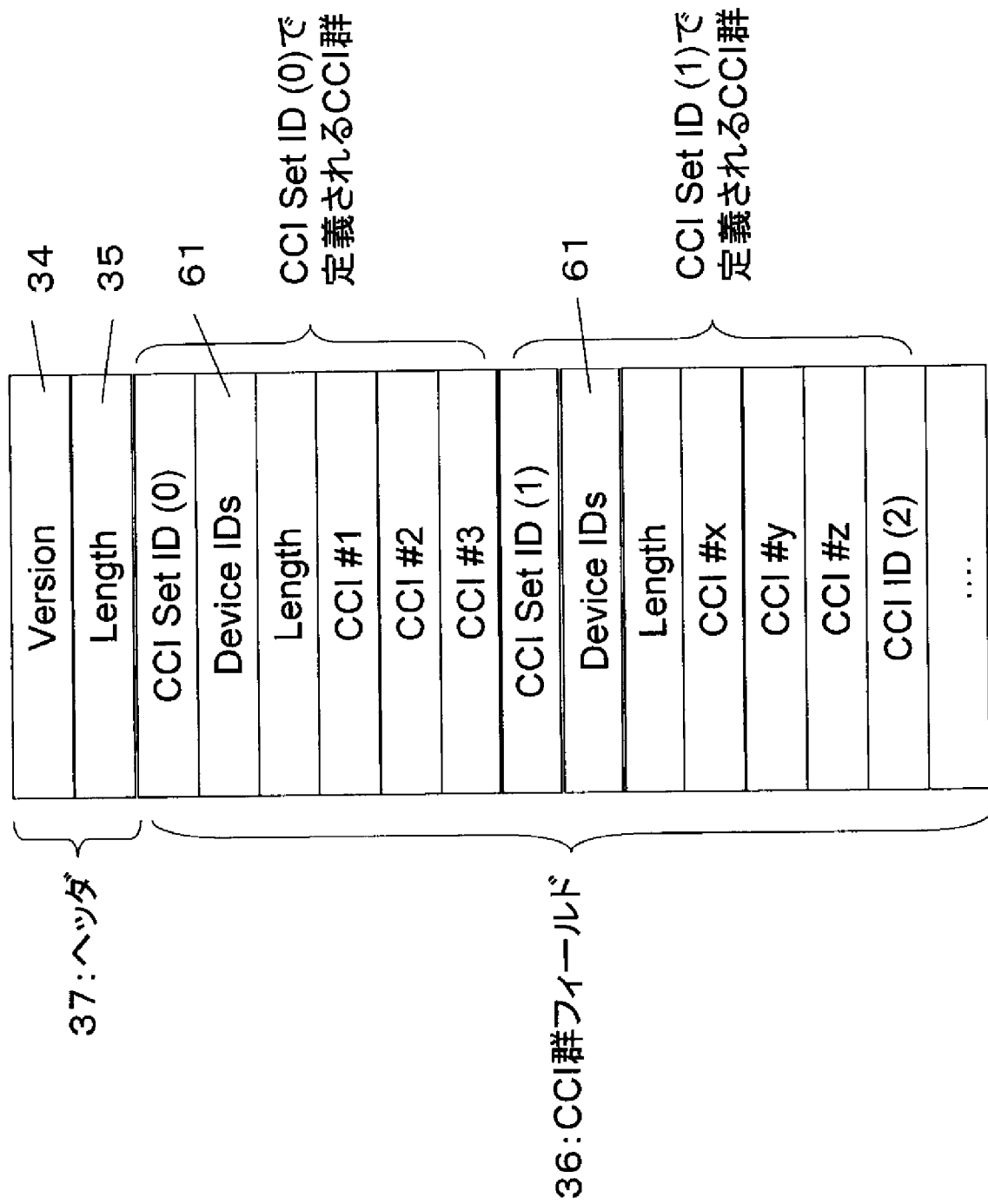
[図15]



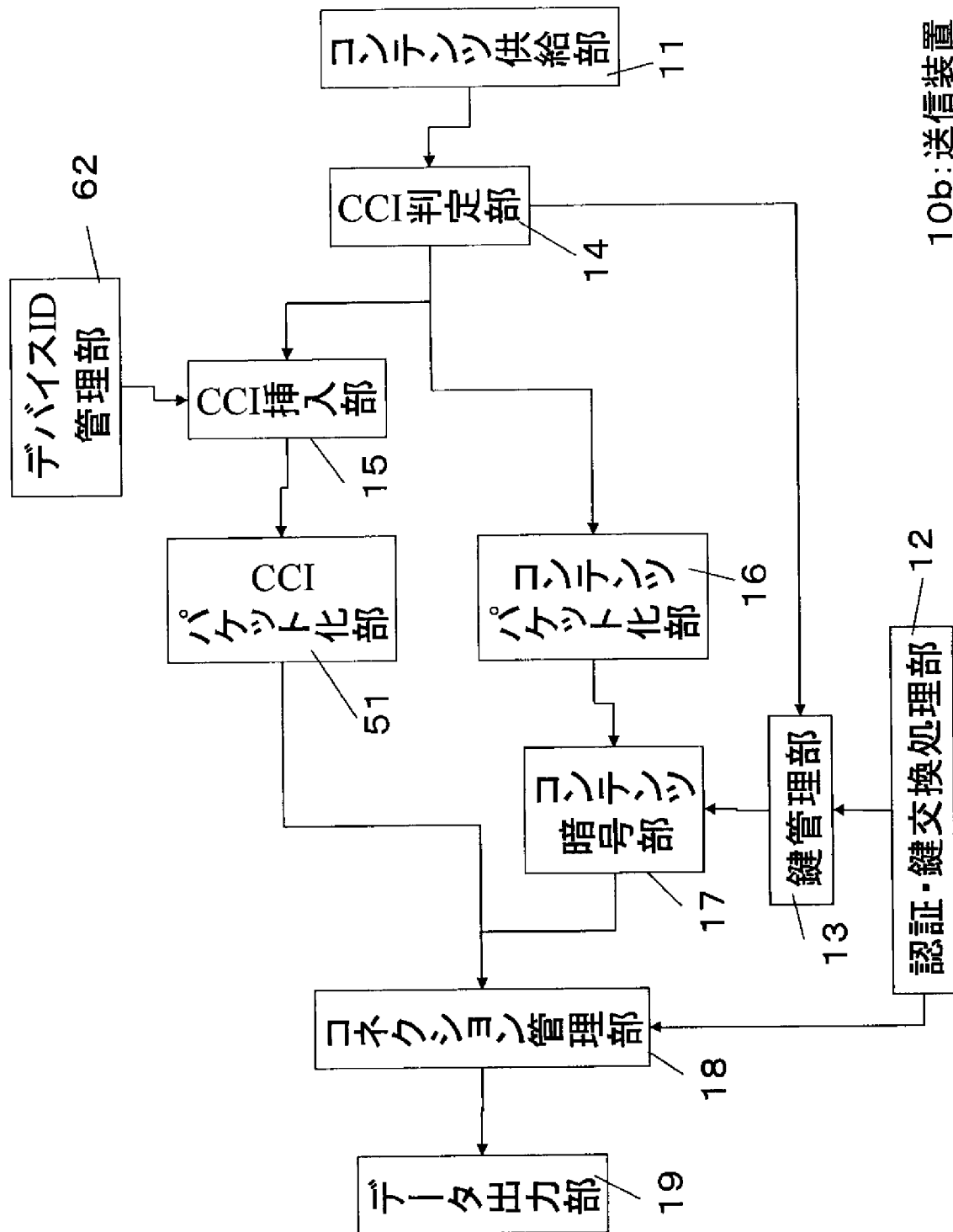
[図16]



[図17]



[図18]



10b: 送信装置

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/060779

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24 (2006.01) i, H04L9/08 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24, H04L9/08

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2010

Kokai Jitsuyo Shinan Koho 1971-2010 Toroku Jitsuyo Shinan Koho 1994-2010

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-323707 A (Hitachi, Ltd.), 30 November 2006 (30.11.2006), entire text; all drawings & US 2006/0265735 A1 & CN 1866825 A	1-10
A	JP 2005-275828 A (Hitachi, Ltd.), 06 October 2005 (06.10.2005), entire text; all drawings & US 2005/0228858 A1 & EP 1580954 A2 & KR 10-2005-0095512 A & CN 1674509 A	1-10
A	JP 2004-104470 A (Sony Corp.), 02 April 2004 (02.04.2004), entire text; all drawings & US 2004/0098252 A1 & GB 2393319 A & KR 10-2004-0023527 A & CN 1495770 A	1-10

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
02 February, 2010 (02.02.10)Date of mailing of the international search report
16 February, 2010 (16.02.10)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/060779

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-7494 A (Matsushita Electric Industrial Co., Ltd.), 08 January 2004 (08.01.2004), entire text; all drawings & US 2003/0231334 A1 & EP 1490871 A & WO 2003/081586 A1 & BR 308705 A & PL 372464 A & CN 1643594 A	1-10
A	JP 2003-345661 A (NEC Corp.), 05 December 2003 (05.12.2003), entire text; all drawings (Family: none)	1-10

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G06F21/24(2006.01)i, H04L9/08(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. G06F21/24, H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2006-323707 A (株式会社日立製作所) 2006. 11. 30, 全文、全図 & US 2006/0265735 A1 & CN 1866825 A	1-10
A	JP 2005-275828 A (株式会社日立製作所) 2005. 10. 06, 全文、全図 & US 2005/0228858 A1 & EP 1580954 A2 & KR 10-2005-0095512 A & CN 1674509 A	1-10
A	JP 2004-104470 A (ソニー株式会社) 2004. 04. 02, 全文、全図 & US 2004/0098252 A1 & GB 2393319 A & KR 10-2004-0023527 A	1-10

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

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

0 2 . 0 2 . 2 0 1 0

国際調査報告の発送日

1 6 . 0 2 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官 (権限のある職員)

鳥居 稔

5 S

4 0 5 6

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
	& CN 1495770 A	
A	JP 2004-7494 A (松下電器産業株式会社) 2004. 01. 08, 全文、全図 & US 2003/0231334 A1 & EP 1490871 A & WO 2003/081586 A1 & BR 308705 A & PL 372464 A & CN 1643594 A	1-10
A	JP 2003-345661 A (日本電気株式会社) 2003. 12. 05, 全文、全図 (ファミリーなし)	1-10