(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

(43) 国際公開日
2003 年12 月18 日 (18.12.2003)

PCT

(10) 国際公開番号
WO 03/104997 A1

(51) 国際特許分類[7]: G06F 12/14, 17/60, G06K 17/00

(21) 国際出願番号: PCT/JP03/07250

(22) 国際出願日: 2003 年6 月9 日 (09.06.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-169241 2002 年6 月10 日 (10.06.2002) JP
特願2002-169244 2002 年6 月10 日 (10.06.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 Tokyo (JP).

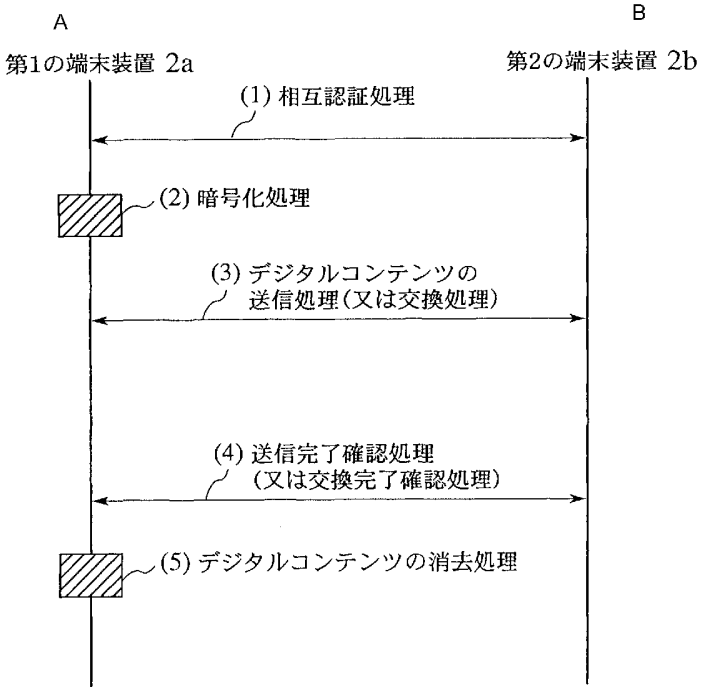
(71) 出願人 および
(72) 発明者: 坂村 健 (SAKAMURA,Ken) [JP/JP]; 〒141-0032 東京都 品川区 大崎4丁目9-2 Tokyo (JP). 越塚 登 (KOSHIZUKA,Noboru) [JP/JP]; 〒180-0013 東京都 武蔵野市 西久保2丁目27-20 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 森 謙作 (MORI,Kensaku) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 石井 一彦 (ISHII,Kazuhiko) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 山王パークタワー 株

[続葉有]

(54) Title: IC CARD, TERMINAL DEVICE, AND DATA COMMUNICATION METHOD

(54) 発明の名称: ＩＣカード、端末装置及びデータ通信方法



A...FIRST TERMINAL DEVICE 2a
B...SECOND TERMINAL DEVICE 2b
(1)...INTERACTIVE AUTHENTICATION
(2)...ENCRYPTION
(3)...DIGITAL CONTENT TRANSMISSION (OR EXCHANGE)
(4)...TRANSMISSION COMPLETION CONFIRMATION (OR EXCHANGE COMPLETION CONFIRMATION)
(5)...DIGITAL CONTENT ERASE

(57) Abstract: A data communication method includes a step of executing a predetermined command when an IC card (1a) has received a predetermined trigger signal, a step of storing the state of the IC card (1a) before transmitting a first digital content, a step of encrypting the first digital content according to key information related to the first digital content, a step of erasing the first digital content from a holder section (18) of the IC card (1a) when a commit instruction to notify that reception of the first digital content encrypted is complete is received from a transmission destination device (1b), and a step of returning to the state of the IC card (1a) when the transmission of the first digital content is interrupted.

[続葉有]

WO 03/104997 A1

式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 青野 博 (AONO,Hiroshi) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 本郷 節之 (HONGO,Sadayuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

(74) 代理人: 三好 秀和 (MIYOSHI,Hidekazu); 〒105-0001 東京都 港区 虎ノ門1丁目2番3号 虎ノ門第一ビル9階 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, GB).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

本発明に係るデータ通信方法は、ＩＣカード１ａが所定のトリガー信号を受信すると所定のコマンドを実行する工程と、第１のデジタルコンテンツの送信前におけるＩＣカード１ａの状態を記憶する工程と、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行う工程と、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置１ｂから受信した場合にＩＣカード１ａのホルダー部１８から第１のデジタルコンテンツを消去する工程と、第１のデジタルコンテンツの送信処理が中断された場合にＩＣカード１ａの状態への復帰処理を行う工程とを有する。

明　細　書

ＩＣカード、端末装置及びデータ通信方法

技術分野

本発明は、電子商取引（ｅコマース）やコンテンツ配信等に利用可能なＩＣカード、当該ＩＣカードを操作するための端末装置、及び、これらを用いたデータ通信方法に関する。

背景技術

従来、ＩＣカード内に電子マネー等のデジタルコンテンツが格納されており、リーダライタ等の操作端末装置（送信元装置）が、ＩＣカードから当該デジタルコンテンツを読み出し、読み出したデジタルコンテンツを送信先装置に対して送信する通信プラットホームが開発されている。

また、ＩＣカード内に第１のデジタルコンテンツが格納されており、リーダライタ等の操作端末装置（送信元装置）が、ＩＣカードから第１のデジタルコンテンツを読み出し、読み出した第１のデジタルコンテンツを送信先装置に対して送信するとともに、送信先装置に格納されている第２のデジタルコンテンツを受信することによって、デジタルコンテンツの交換を行う通信プラットホームが開発されている。

従来の通信プラットホームでは、操作端末装置（送信元装置）が、ＩＣカードからデジタルコンテンツを読み出し、当該操作端末装置に備えられたハードウェアやソフトウェアのコマンドを用いて、当該デジタルコンテンツに対する暗号化処理を行うとともに、当該操作端末装置上で実行されているＯＳのプロトコルに基づいて、当該デジタルコンテンツ

の送信を行っている。

かかるデジタルコンテンツの送信にあっては、当該デジタルコンテンツの安全な送信を担保するために、送信先装置に一時的に当該デジタルコンテンツを複製した後に、当該操作端末装置において当該デジタルコンテンツを消去する方式を採用している。

しかしながら、従来の通信プラットホームでは、ＩＣカード内に格納されているデジタルコンテンツが、操作端末装置（送信元装置）上に読み出された後、当該操作端末装置のコマンドやプロトコル等により処理されるため、当該デジタルコンテンツが当該操作端末装置に読み出された際に、悪意の操作者や悪意の第三者によって当該デジタルコンテンツの内容が、改ざんされたり不正に複製されたりする可能性があった。

また、従来の通信プラットホームでは、複数の操作端末装置間で、デジタルコンテンツの送受信処理を行う場合、当該デジタルコンテンツが送信先の操作端末装置に一時的に複製された後に、送信元の操作端末装置においてデジタルコンテンツを消去する方式を採用している。

そのため、当該デジタルコンテンツの送受信処理中に通信が切断されたときには、送信先の操作端末装置及び送信元の操作端末装置の両方において、当該送受信処理に係るデジタルコンテンツが消失してしまう可能性がある。

また、送信先の操作端末装置及び送信元の操作端末装置の両方において当該デジタルコンテンツが存在する状態で、当該デジタルコンテンツの送受信処理が中断される場合、操作者の意図によらず、当該デジタルコンテンツが送信先の操作端末装置において複製される結果となる。

特に、電子マネー等による電子商取引においては、送信元の操作端末装置と送信先の操作端末装置との間で、デジタルコンテンツが確実に交

換されるか、或いは、通信障害が生じた場合には、当該電子商取引の開始時の状態に、送信元の操作端末装置及び送信先の操作端末装置を完全に復帰させる必要がある。

発明の開示

そこで、本発明は、上記に鑑みてなされたものであり、ＩＣカード間で直接通信を行う通信プラットホーム上で、デジタルコンテンツを送信する際に、送受信者及び悪意の操作者又は第三者によるデジタルコンテンツの複製や紛失を回避することのできるＩＣカード、端末装置及びデータ通信方法を提供することを目的とする。

また、本発明は、ＩＣカードと端末装置と間で直接通信を行う通信プラットホーム上で、デジタルコンテンツを交換する際に、送受信者及び悪意の操作者又は第三者による当該デジタルコンテンツの複製や紛失を回避することのできるＩＣカード、端末装置及びデータ通信方法を提供することを目的とする。

上記目的を達成するために、本発明の第１の特徴は、ＩＣカードであって、第１のデジタルコンテンツを格納するホルダー部と、第１のデジタルコンテンツに対応付けられた鍵情報を含む証明書データを格納する証明書データ格納部と、暗号処理部と、実行処理部とを備え、実行処理部が、所定のトリガー信号を受信すると、所定のコマンドを実行し、実行処理部によって実行された所定のコマンドは、実行処理部に、第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶させ、暗号化処理部に、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行わせ、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット

命令を送信先装置から受信した場合にホルダー部から第１のデジタルコンテンツを消去し、第１のデジタルコンテンツの送信処理が中断された場合に実行処理部に記憶されているＩＣカードの状態への復帰処理を行うことを要旨とする。

本発明の第１の特徴において、実行処理部によって実行された所定のコマンドが、コミット命令を受信した場合に送信先装置に対して第２のデジタルコンテンツの送信要求を送信し、第２のデジタルコンテンツの受信処理が完了した場合にホルダー部から第１のデジタルコンテンツを消去することが好ましい。

また、本発明の第１の特徴において、第１のデジタルコンテンツの送信に先だって、送信先装置から送信先装置の証明書データを取得し、送信先装置の証明書データに基づいて送信先装置の正当性を認証する認証部を具備し、実行処理部が、送信先装置の正当性が認証された場合に所定のコマンドを実行することが好ましい。

また、本発明の第１の特徴において、認証部が、送信先装置との間のセッションを識別するセッションＩＤとセッションモードとに応じて、ホルダー部に格納されている第１のデジタルコンテンツへのアクセスレベルを設定することが好ましい。

また、本発明の第１の特徴において、認証部が、第１のデジタルコンテンツの送信に先だって、証明書データ格納部に格納されている証明書データを送信先装置に対して送信し、送信先装置から証明書データの正当性が認証された旨を通知する認証確認通知を取得し、実行処理部が、認証確認通知が取得された場合に所定のコマンドを実行することが好ましい。

本発明の第２の特徴は、ＩＣカードに格納されている第１のデジタル

コンテンツを送信先装置に送信する端末装置であって、入力された操作信号に基づいて所定のトリガー信号をＩＣカードに対して出力する制御部を具備し、ＩＣカードの実行処理部が、所定のトリガー信号に応じて所定のコマンドを実行し、実行処理部によって実行された前記所定のコマンドが、実行処理部に、第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶させ、ＩＣカードの暗号化処理部に、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行わせ、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置から受信した場合にＩＣカードのホルダー部から第１のデジタルコンテンツを消去し、第１のデジタルコンテンツの送信処理が中断された場合に実行処理部に記憶されているＩＣカードの状態への復帰処理を行うことを要旨とする。

本発明の第２の特徴において、実行処理部によって実行された所定のコマンドが、コミット命令を受信した場合に送信先装置に対して第２のデジタルコンテンツの送信要求を送信し、第２のデジタルコンテンツの受信処理が完了した場合にホルダー部から第１のデジタルコンテンツを消去することが好ましい。

また、本発明の第２の特徴において、ＩＣカードから送信先装置に第１のデジタルコンテンツを送信した後、所定の待機時間を経過するまでの間に送信先装置から応答がない場合、第１のデジタルコンテンツの送信処理が中断された旨をＩＣカードに通知する通信監視部を具備することが好ましい。

また、本発明の第２の特徴において、ＩＣカードと送信先装置との間で確立されているセッションを識別するセッションＩＤとセッションモ

ードとに応じて設定されたアクセスレベルに基づいて、ホルダー部から第１のデジタルコンテンツに関する情報を読み出して表示する表示部を具備することが好ましい。

本発明の第３の特徴は、ＩＣカードに格納されている第１のデジタルコンテンツを送信先装置に送信するデータ通信方法であって、ＩＣカードが、所定のトリガー信号を受信すると、所定のコマンドを実行する工程と、第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶する工程と、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行う工程と、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置から受信した場合にＩＣカードのホルダー部から第１のデジタルコンテンツを消去する工程と、第１のデジタルコンテンツの送信処理が中断された場合に、記憶されているＩＣカードの状態への復帰処理を行う工程とを有することを要旨とする。

また、本発明の第３の特徴において、コミット命令を受信した場合、送信先装置に対して第２のデジタルコンテンツの送信要求を送信する工程と、第２のデジタルコンテンツの受信処理が完了した場合、ホルダー部から第１のデジタルコンテンツを消去する工程とを有することが好ましい。

また、本発明の第３の特徴において、ＩＣカードが装填された端末装置が、入力された操作信号に基づいて、所定のトリガー信号を、ＩＣカードに対して出力する工程を有することが好ましい。

また、本発明の第３の特徴において、第１のデジタルコンテンツの送信に先だって、送信先装置から送信先装置の証明書データを取得する工程と、送信先装置の証明書データに基づいて送信先装置の正当性を認証

する工程と、ＩＣカードが、送信先装置の正当性が認証された場合に所定のコマンドを実行する工程とを有することが好ましい。

また、本発明の第３の特徴において、送信先装置との間のセッションを識別するセッションＩＤとセッションモードとに応じて、ホルダー部に格納されている第１のデジタルコンテンツへのアクセスレベルを設定する工程を有することが好ましい。

また、本発明の第３の特徴において、第１のデジタルコンテンツの送信に先だって、証明書データ格納部に格納されている証明書データを送信先装置に対して送信する工程と、送信先装置から証明書データの正当性が認証された旨を通知する認証確認通知を取得する工程と、ＩＣカードが、認証確認通知が取得された場合に所定のコマンドを実行する工程とを有することが好ましい。

また、本発明の第３の特徴において、ＩＣカードから送信先装置に第１のデジタルコンテンツを送信した後、所定の待機時間を経過するまでの間に送信先装置から応答がない場合、第１のデジタルコンテンツの送信処理が中断された旨をＩＣカードに通知する工程を有することが好ましい。

また、本発明の第３の特徴において、端末装置が、ＩＣカードと送信先装置との間で確立されているセッションを識別するセッションＩＤとセッションモードとに応じて設定されたアクセスレベルに基づいて、ホルダー部から第１のデジタルコンテンツに関する情報を読み出して表示する工程を有することが好ましい。

図面の簡単な説明

図１は、本発明の第１の実施形態に係るデータ通信方法を実現するシ

ステムの全体構成図である。

図２は、本発明の第１の実施形態に係る端末装置及びＩＣカードの内部構造を示す図である。

図３は、本発明の第１の実施形態に係るデータ通信方法の全体動作を示すシーケンス図である。

図４は、本発明の第１の実施形態に係るデータ通信方法の全体動作を示すフローチャートである。

図５は、本発明の第１の実施形態に係るデータ通信方法における相互認証処理を示すフローチャートである。

図６は、本発明の第１の実施形態に係るデータ通信方法における第１のＩＣカード側の送信処理を示すフローチャートである。

図７は、本発明の第１の実施形態に係るデータ通信方法における第２のＩＣカード側の送信処理を示すフローチャートである。

図８は、本発明の第１の実施形態に係るデータ通信方法における交換処理を示すフローチャートである。

図９は、本発明の第１の実施形態に係るデータ通信方法における通信状況の監視処理を示すフローチャートである。

図１０は、本発明の第２の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

図１１は、本発明の第２の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

図１２は、本発明の第２の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

図１３は、本発明の第２の実施形態に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

図１４は、本発明の変更例１に係るデジタルコンテンツ発行システムの概略構成図である。

図１５は、本発明の変更例１に係るデジタルコンテンツ発行システムの概略構成図である。

図１６は、本発明の変更例１に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

図１７は、本発明の変更例２に係るデジタルコンテンツ発行システムの概略構成図である。

図１８は、本発明の変更例２に係るデジタルコンテンツ発行システムの概略構成図である。

図１９は、本発明の変更例３に係るデジタルコンテンツ発行システムの概略構成図である。

図２０は、本発明の変更例３に係るデジタルコンテンツ発行システムの概略構成図である。

図２１は、本発明の変更例３に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

発明を実施するための最良の形態

［第１の実施形態］

本発明の第１の実施形態に係るデータ通信方法、当該データ通信方法に用いて好適なＩＣカード及び端末装置について、図を参照しながら説明する。

図１は、本実施形態に係るデータ通信方法を実現するためのシステムの構成を示す説明図である。

図１に示すように、本実施形態では、機能分散システム上において、

「送信元装置」である第１のＩＣカード１ａに格納されている「第１のデジタルコンテンツ」を、「送信先装置」である第２のＩＣカード１ｂに対して送信し、第２のＩＣカード１ｂに格納されている「第２のデジタルコンテンツ」を、第１のＩＣカード１ａに送信する場合を例に説明する。

図１に示すように、第１のＩＣカード１ａ及び第２のＩＣカード１ｂは、それぞれ、第１のＩＣチップ１１ａ及び第２のＩＣチップ１１ｂを搭載している。具体的には、第１のＩＣチップ１１ａ及び第２のＩＣチップ１１ｂは、プラスチック等で形成された第１のＩＣカード１ａ及び第２のＩＣカード１ｂの基板上に固着された集積回路である。

また、第１のＩＣカード１ａ及び第２のＩＣカード１ｂは、それぞれ第１の端末装置２ａ及び第２の端末装置２ｂに装填されており、各端末装置２ａ及び２ｂからの操作に基づいて、当該端末装置２ａ及び２ｂを介して、第１及び第２のデジタルコンテンツの送受信処理を行う。

図２は、第１のＩＣカード１ａ（又は、第２のＩＣカード１ｂ）及び第１の端末装置２ａ（又は、第２の端末装置２ｂ）の内部構成を示すブロック図である。

第１のＩＣカード１ａの内部構成及び第２のＩＣカード１ｂの構成は基本的に同一であり、第１の端末装置２ａの内部構成及び第２の端末装置２ｂの内部構成も、基本的に同一であるため、以下、第１のＩＣカード１ａ及び第１の端末装置２ａの内部構成について説明する。

図２に示すように、第１のＩＣカード１ａは、第１のＩＣチップ１１ａと第１の端末装置２ａとの間で、例えば、デジタルコンテンツや証明書データやコミット命令（後述）や送信要求（後述）等のデータの送受信処理を行うデータ送受信部１２を備えている。

本実施形態において、第１のＩＣカード１ａは、コンピュータの周辺機器として、リーダライタ等の操作端末装置を通して操作されるものではなく、分散環境におけるノードとして設計されており、ネットワーク上のサービス提供モジュールのチップに対して、対等に「Ｐｅｅｒ-ｔｏ-Ｐｅｅｒ」で通信が可能となっている。

第１のＩＣチップ１１ａは、耐タンパ性を有するＬＳＩであり、演算処理デバイスやメモリ等から構成されており、ＩＣカードの他、例えば、スマートカードやＰＤＡ端末といったハードウェア上に実装されることも可能である。

第１の端末装置２ａには、第１のＩＣカード１ａが、挿抜可能に装填されている。また、第１の端末装置２ａは、第１のＩＣカード１ａとの間で、データの読込処理及び書込処理を行うリードライタ機能を備えており、ＬＡＮ等の通信ネットワークに対する非接触（コンタクトレス）通信の物理層を橋渡しするゲートウェイ（ブリッジ）の役割を果たすものである。

具体的に、第１の端末装置２ａは、例えば、ＰＤＡ端末や携帯電話端末等の形態を採ることができる。

（本実施形態に係るＩＣカード）

本実施形態に係る第１のＩＣカード１ａは、図２に示すように、認証部１３と、暗号処理部１４と、実行処理部１５と、コマンド記憶部１６と、証明書データ格納部１７と、ホルダー部１８とを備えている。

認証部１３は、他のＩＣカード（例えば、第２のＩＣカード１ｂ）との通信を確立する際に、当該他のＩＣカードとの間で相互認証処理を行う演算デバイスである。

具体的には、認証部１３は、第１のデジタルコンテンツの送信に先だ

って、第２のＩＣカード１ｂから当該第２のＩＣカード１ｂの証明書データを取得し、取得した証明書データに含まれる当該第２のＩＣカード１ｂのホルダーＩＤと署名データとに基づいて、当該第２のＩＣカード１ｂの正当性を認証するとともに、当該第２のＩＣカード１ｂに対して当該第１のＩＣカード１ａの証明書データを送信し、当該第２のＩＣカード１ｂから、当該第１のＩＣカード１ａの証明書データの正当性が認証された旨を通知する「認証確認通知」を取得することによって、当該第２のＩＣカード１ｂとの間で相互認証処理を行う。

また、本実施形態において、認証部１３は、第２のＩＣカード１ｂとの間の相互認証処理の際に、当該第２のＩＣカード１ｂとの間で確立されている通信（セッション）を識別する「セッションＩＤ」と、指定された「セッションモード」とを取得し、取得された「セッションＩＤ」と「セッションモード」とに応じて、ホルダー部１８に格納されているデジタルコンテンツへのアクセスレベルを設定する。

本実施形態では、当該セッションモードには、以下に示すように、「（情報）発行者モード」と「所有者モード」の２つのモードがある。これらのセッションモードは、第１のＩＣカード１ａと第２のＩＣカード１ｂとの間の相互認証処理時に指定されるものである。各セッションモードによって、用いられる認証アルゴリズムが異なる。

「（情報）発行者モード」は、アクセス者（例えば、第２のＩＣカード１ｂ）を、当該デジタルコンテンツの発行者として認証するセッションモードである。

「（情報）発行者モード」による認証によって設定されたアクセスレベルを有するアクセス者は、当該情報発行者が作成したデジタルコンテンツには、発行者権限でアクセスでき、それ以外のデジタルコンテンツ

には、その他権限でアクセスすることができる。

「所有者モード」は、アクセス者（例えば、第２のＩＣカード１ｂ）を第１のＩＣカード１ａの所有者として認証するモードである。本実施形態において、「所有者モード」による認証では、パスワード等、人間にとって扱いやすい認証方法が使用される。

「所有者モード」による認証によって設定されたアクセルレベルを有するアクセス者は、所有者権限を持つ。

暗号処理部１４は、第１のＩＣカード１ａ内部において、ホルダー部１８に格納されている第１のデジタルコンテンツについての暗号化処理を行うものである。ホルダー部１８に格納されている第１のデジタルコンテンツは、暗号処理部１４によって暗号化処理が施された後、データ送受信部１２を通じて、第１の端末装置２ａ側に送出される。

実行処理部１５は、外部からの所定のトリガー信号に基づいて、コマンド記憶部１６から所定のコマンドを呼び出し、第１のデジタルコンテンツの暗号化処理や送信処理を実行する演算処理装置である。本実施形態において、所定のトリガー信号は、操作部２４からの操作信号に基づいて、制御部２６によって出力されるものである。

また、実行処理部１５は、認証部１３と連動する形態となっており、認証部１３が、第２のＩＣカード１ｂが正当であると認証するとともに、当該第２のＩＣカード１ｂから認証確認通知を取得して、当該第２のＩＣカード１ｂとの間の相互認証処理が完了された場合に、上述の所定のコマンドを実行する。

コマンド記憶部１６は、所定のコマンドを記憶するメモリ等の記憶装置である。

例えば、所定のコマンドは、暗号処理部１４に対して、ホルダー部１

８に格納されている第１のデジタルコンテンツを暗号化させたり、データ送受信部１２に対して、第２のＩＣカードＩＣ１ｂに第１のデジタルコンテンツを送信させたり、第２のＩＣカードＩＣ１ｂから第２のデジタルコンテンツを受信させたりするためのコマンドである。

証明書データ格納部１７は、ホルダー部１８に格納されている第１のデジタルコンテンツに対応付けられた証明書データ（後述）を格納するメモリ等の記憶装置である。証明書データ格納部１７は、認証部１３による認証処理や暗号処理部１４による暗号化処理の際に、これらの処理に必要なデータである「ホルダーＩＤ」や「鍵情報」や「署名データ」を提供するものである。

ホルダー部１８は、他のＩＣカード（例えば、第２のＩＣカード１ｂ）等との間で情報交換を行うネットワーク上の計算実体であり、第１のデジタルコンテンツを格納する耐タンパ性のメモリ装置である。

データ送受信部１２は、接触式通信或いは非接触式通信によって、暗号化された第１のデジタルコンテンツや、第１のＩＣカード１ａの証明書データや等の各種データを、外部に対して送信する通信デバイスである。

なお、本実施形態におけるデータ送受信部１２は、第１のＩＣカード１ａが第１の端末装置２ａ内に装填された状態において、当該第１の端末装置２ａ側のデータ送受信部２３と接触して、各種データの送受信処理を行うように形成されている。

（本実施形態に係る端末装置）

本実施形態に係る第１の端末装置２ａは、カードリーダや携帯電話端末やＰＤＡ端末等の携帯端末装置、或いはパーソナルコンピュータ等の汎用コンピュータで実現することが可能である。

図２に示すように、第１の端末装置２ａは、通信部２１と、通信監視部２２と、データ送受信部２３と、操作部２４と、表示部２５と、制御部２６とを備えている。

通信部２１は、無線通信等によって、外部（例えば、第２の端末装置２ｂ）との間で各種データの送受信を行う通信デバイスである。

通信監視部２２は、通信部２１による通信状態を監視する装置である。また、通信監視部２２は、最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断されたと判断し、その旨をデータ送受信部２３及び１２を介して、第１のＩＣカード１ａ内の実行処理部１５に送出する。

データ送受信部２３は、第１の端末装置２ａ内に装填された第１のＩＣカード１ａのデータ送受信部１２と接触されるように設けられており、データ送受信部１２との間で各種データの送受信処理を行うものである。

操作部２４は、例えば、第１の端末装置２ａの表面に配置されたボタンやスティックであり、操作者の操作により、種々の操作信号を制御部２６に対して入力する操作デバイスである。

表示部２５は、例えば、第１の端末装置２ａの表面に配置された液晶ディスプレイ等の表示デバイスであり、通信部２１による通信状態や、操作部２４による操作結果を表示する。

特に、本実施形態において、表示部２５は、現在、第１のＩＣカード１ａと他のＩＣカード（例えば、第２のＩＣカード１ｂ）との間で確立されている通信（セッション）を識別する「セッションＩＤ」と、指定された「セッションモード」とに応じて設定されたアクセスレベルに基づいて、当該デジタルコンテンツに関する情報をホルダー部１８から読み出して表示する機能を有する。

制御部２６は、第１の端末装置２ａにおける各部２１乃至２５の動作を制御するＣＰＵである。特に、制御部２６は、操作部２４からの操作信号に基づいて、実行処理部１５に対して、所定のコマンドの実行処理を開始させるトリガー信号を出力する。

（デジタルコンテンツ）

第１のＩＣカード１ａには、第１のデジタルコンテンツを格納する多様なアプリケーションが実装される可能性があるため、第１のデジタルコンテンツとしては、様々なタイプが想定される。

例えば、第１のデジタルコンテンツとして、以下のようなものが考えられる。

・　第１のＩＣカード１ａの所有者が変更することができず、情報発行者だけが変更することができるデジタルコンテンツ（例えば、電子チケットの座席番号）

・　第１のＩＣカード１ａの所有者でさえ見ることができないデジタルコンテンツ（例えば、電子チケットを変更するための鍵情報）

・　第１のＩＣカード１ａの所有者だけが完全に制御できるデジタルコンテンツ（例えば、第１のＩＣカード１ａの所有者の個人情報）

・　何人も読むことができるデジタルコンテンツ

なお、これらの第１のデジタルコンテンツは、発行サーバ等の第三者機関により発行され、証明書データとともに第１のＩＣカード１ａ内に格納される。

（証明書データ）

証明書データには、ホルダー部１８に格納されている第１のデジタルコンテンツを識別する「ホルダーＩＤ」と、証明書データを発行した者が当該証明書データが正当である旨を保証する「署名データ」と、当該

第１のデジタルコンテンツに関連付けられた「公開鍵（鍵情報）」とが含まれている。

「ホルダーＩＤ」は、分散システム（分散環境）全体でユニークに定められた識別子であり、第１のＩＣカード１ａを物理的に識別するだけでなく、分散システム上での経路制御にも利用され、認証通信における相手に対する識別子としても利用される。すなわち、「ホルダーＩＤ」は、ネットワーク上で、ＩＣカードやサービスクライアントの認証、メッセージの経路制御等に用いられる。なお、本実施形態において、「ホルダーＩＤ」は、１６オクテット（１２８ビット）で表現される。

（コマンド）

コマンド記憶部１６に格納されている所定のコマンドは、第１の端末装置２ａ側から受信した所定のトリガー信号に応じて、実行が開始されると、第２の端末装置２ａ側における操作とは独立してアトミックに一連の処理が進行される原子性を有するものである。

当該所定のコマンドによる一連の処理としては、

（１）相互認証処理

（２）暗号化処理

（３）デジタルコンテンツの送信処理又は交換処理

（４）送信完了確認処理又は交換完了確認処理

（５）デジタルコンテンツの消去処理

がある。

ここで、所定のコマンドは、実行処理部１５に対して、デジタルコンテンツの送信処理（又は、交換処理）に先立って、第１のＩＣカード１ａ内における「各部１２乃至１９の状態（ＩＣカードの状態）」を記憶させる。

また、所定のコマンドは、当該第１のデジタルコンテンツの送信処理完了後、データ送受信部１２を介して、第２のＩＣカード１ｂから「受信処理を完了した旨」を通知する「コミット命令」を受信した場合に、ホルダー部１８内に格納されている当該第１のデジタルコンテンツを消去する。

また、所定のコマンドは、第２のＩＣカード１ｂから受信した「コミット命令」に応じて、第２のＩＣカード１ｂに対して第２のデジタルコンテンツの「送信要求」を送信し、当該「送信要求」に応じて第２のＩＣカード１ｂから送信された第２のデジタルコンテンツの受信処理が完了した場合に、その旨を通知する「送信完了要求」を送信すると共に、ホルダー部１８内に格納されている当該第１のデジタルコンテンツを消去するように構成されていても良い。

また、所定のコマンドは、当該第１のデジタルコンテンツの送信処理（又は、デジタルコンテンツの交換処理）の実行中に、通信が中断された場合には、実行処理部１５に記憶されている「各部１２乃至１９の状態（ＩＣカードの状態）」を読み出し、ロールバック処理（復帰処理）によって、第１のＩＣカード１ａ内の各部１２乃至１９を、当該デジタルコンテンツの送信処理（又は、交換処理）開始前の状態（読み出した「各部１２乃至１９の状態（ＩＣカードの状態）」）に復帰させる。

また、所定のコマンドは、第２のＩＣカード１ｂの実行処理部１５に対して、当該デジタルコンテンツの送信処理（又は、交換処理）開始前における第２のＩＣカード１ｂ内の「各部１２乃至１９の状態（ＩＣカードの状態）」を記憶させ、当該デジタルコンテンツの送信処理（又は、交換処理）が中断された場合に、第２のＩＣカード１ｂ内の各部１２乃至１９を、第２のＩＣカード１ｂの実行処理部１５に記憶されている「各

部１２乃至１９の状態（ＩＣカードの状態）」に復帰させる。

（本実施形態に係るデータ通信方法）

図を参照して、本実施形態に係るデータ通信方法について説明する。ここで、図３乃至図９は、本実施形態に係るデータ通信方法の手順を示すフロー図である。なお、本実施形態では、第１のＩＣカード１ａの操作者による操作に基づいて、第１のＩＣカード１ａから第２のＩＣカード１ｂへの第１のデジタルコンテンツの送信処理、及び、第１のＩＣカード１ａと第２のＩＣカード１ｂとの間で行われる第１及び第２のデジタルコンテンツの交換処理の双方に係るデータ通信方法について説明する。

（１）　全体処理

図３を参照して、本実施形態に係るデータ通信方法の全体処理について説明する。

図３に示すように、本実施形態に係るデータ通信方法では、ステップ（１）において、第１の端末装置２ａと第２の端末装置２ｂとの間で、相互認証処理が行われる。ステップ（２）において、相互認証処理及びが完了した後に、デジタルコンテンツについての暗号化処理が行われる。ステップ（３）において、暗号化処理が完了した後に、デジタルコンテンツの送信処理（又は、交換処理）が行われる。ステップ（４）において、第１及び第２の端末装置２ａ、２ｂにおいて、デジタルコンテンツの送信完了確認処理及び交換完了確認処理が行われる。ステップ（５）において、デジタルコンテンツの消去処理が行われる。

このとき、前提として、第１のＩＣカード１ａ内には、既に第１のデジタルコンテンツが格納されているものとする。

すなわち、図４に示すように、第１のデジタルコンテンツの情報発行

者が、ステップＳ１０１において、第１のデジタルコンテンツ及び証明書データを発行する。

第１のＩＣカード１ａから第２のＩＣカード１ｂへの第１のデジタルコンテンツの送信処理の場合、ステップＳ１０２において、第１のデジタルコンテンツの情報発行者が、当該第１のデジタルコンテンツ及び当該証明書データを、それぞれ第１のＩＣカード１ａ内のホルダー部１８及び証明書データ格納部１７に格納する。

また、第１のＩＣカード１ａと第２のＩＣカード１ｂとの間で行われる第１及び第２のデジタルコンテンツの交換処理の場合、ステップＳ１０２において、第１及び第２のデジタルコンテンツの情報発行者は、当該第１及び第２のデジタルコンテンツ及び当該証明書データを、それぞれ、第１のＩＣカード１ａ及び第２のＩＣカード１ｂ内のホルダー部１８及び証明書データ格納部１７に格納する。

ここで、証明書データには、当該証明書データの格納先である第１のＩＣカード１ａ又は第２のＩＣカード１ｂを識別する「ホルダーＩＤ」と、ホルダー部１８に格納されている第１又は第２のデジタルコンテンツに対応付けられた「公開鍵（鍵情報）」と、当該情報発行者によって当該第１又は第２のデジタルコンテンツが正当である旨を証明するための「署名データ」とが含まれている。

ステップＳ１０３において、第１の端末装置２ａの操作者が、当該デジタルコンテンツの送信処理（又は、交換処理）を行うための操作を開始する。具体的には、第１の端末装置２ａの操作者が、第１の端末装置２ａの操作部２４において、デジタルコンテンツの送信処理（又は、交換処理）を開始するための操作を行い、この操作に応じて、制御部２６は、データ送受信部２３及び１２を通じて、第１のＩＣカード１ａに所

定のトリガー信号を出力する。

第１のＩＣカード１ａの実行処理部１５は、当該所定のトリガー信号に応じて、コマンド記憶部１６から所定のコマンドを読み出して、読み出した所定のコマンドを実行する。

その結果、ステップＳ１０４において、認証部１３が、第２のＩＣカード１ｂとの間の相互認証処理を行い、ステップＳ１０５において、第１のＩＣカード１ａの暗号処理部１４が、第１のデジタルコンテンツの暗号化処理を行い、ステップＳ１０６において、第１の端末装置２ａの通信部２１が、第２のＩＣカード１ｂとの間で第１のデジタルコンテンツの送信処理（又は、第１及び第２のデジタルコンテンツの交換処理）を開始する。

当該デジタルコンテンツの送信処理（又は、交換処理）の間、通信監視部２２は、ステップＳ１０７において、第１のＩＣカード１ａと第２のＩＣカード１ｂとの間の通信状態を監視しており、ステップＳ１０８において、当該デジタルコンテンツの送信処理（又は、交換処理）が中断されないか否かについて判断する。

当該デジタルコンテンツの送信処理（又は、交換処理）が中断されなかった場合、すなわち、当該デジタルコンテンツの送信処理（又は、交換処理）が正常に完了した場合、ステップＳ１０９において、送信完了確認処理（又は、交換完了確認処理）が行われ、第１のＩＣカード１ａ（及び、第２のＩＣカード１ｂ）のホルダー部１８内の第１のデジタルコンテンツの消去処理が行われる。

一方、当該デジタルコンテンツの送信処理（又は、交換処理）が中断された場合、すなわち、当該デジタルコンテンツの送信処理（又は、交換処理）が正常に完了しなかった場合は、ステップＳ１１０において、

復帰処理が行われる。

（２） 相互認証処理

以下、図５を参照して、上述のステップＳ１０４における相互認証処理について詳細に説明する。図５は、本実施形態に係るデータ通信方法における相互認証処理の動作を示すフロー図である。

図５に示すように、第１の端末装置２ａにおいて、相互認証処理が開始されると、ステップＳ２０１において、第１のＩＣカード１ａの認証部１３が、証明書データ格納部１７に格納されている証明書データを、第１の端末装置２ａの通信部２１を介して、第２の端末装置２ｂ内の第２のＩＣカード１ｂに送信する。

ステップＳ２０２において、第２のＩＣカード１ｂの認証部１３は、受信した証明書データに含まれる「署名データ」と「ホルダーＩＤ」とに基づいて、第１のＩＣカード１ａの正当性についての認証処理を行う。

第１のＩＣカード１ａの正当性が確認された場合には、ステップＳ２０３において、第２のＩＣカード１ｂの認証部１３は、その旨を示す「認証確認通知」を、第１のＩＣカード１ａに対して送信する。一方、第１のＩＣカード１ａの正当性が否認された場合には、当該相互認証処理は中断される。

ステップＳ２０４において、第１のＩＣカード１ａの認証部１３が、第２のＩＣカード１ｂから送信された「認証確認通知」を受信した場合、第２のＩＣカード１ｂにおける認証処理は、終了する。

このような第２のＩＣカード１ｂにおける認証処理と並行して、第１のＩＣカード１ａにおいても同様な認証処理が実行される。

すなわち、ステップＳ２０５において、第１のＩＣカード１ａの認証部１３は、第２のＩＣカード１ｂから証明書データを取得する。ステッ

プＳ２０６において、第１のＩＣカード１ａの認証部１３は、取得した証明書データに含まれる「署名データ」と「ホルダーＩＤ」とに基づいて、第２のＩＣカード１ｂの正当性についての認証処理を行う。

第１のＩＣカード１ａ及び第２のＩＣカード１ｂの認証部１３は、ステップＳ２０７において、当該セッションでのみ有効な「セッションＩＤ」を設定するとともに、セッションモードを相互に取得しあう。

ステップＳ２０８において、第１のＩＣカード１ａの認証部１３は、取得したセッションモードと、第２のＩＣカード１ｂのカードＩＤ（ホルダーＩＤ）とに基づいて、当該デジタルコンテンツに対するアクセスレベルを設定する。

設定されたアクセスレベルに応じて、ホルダー部１８内のデジタルコンテンツのセキュリティーレベルが決定されると共に、操作者に開示するデジタルコンテンツの内容が制限される。ここで、開示を制限されていないデジタルコンテンツは、ホルダー部１８から読み出されることが可能であり、表示部２５に表示される。また、表示されるデジタルコンテンツとしては、デジタルコンテンツのファイル名や、デジタルコンテンツの種類（電子マネーやクーポン・チケット等）等が考えられる。

上述のように、相互認証処理が完了した後、第１のＩＣカード１ａの実行処理部１５は、コマンド記憶部１６に記憶されている所定のコマンドを呼び出し、デジタルコンテンツの送信処理（又は、交換処理）を実行する。

（３-１）　送信処理

以下、図６及び図７を参照して、上述のステップＳ１０６における送信処理について詳細に説明する。図６は、本実施形態に係るデータ通信方法における第１のＩＣカード１ａ側の送信処理の動作を示すフロー図

であり、図７は、本実施形態に係るデータ通信方法における第２のＩＣカード１ａｂの送信処理の動作を示すフロー図である。

図６に示すように、第１のデジタルコンテンツの送信処理が開始されると、ステップＳ４０１において、第１のＩＣカード１ａの実行処理部１５が、第１のデジタルコンテンツの送信処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）を記憶する。ステップＳ４０２において、第１のＩＣカード１ａのデータ送受信部１２が、暗号化されている第１のデジタルコンテンツを、第２のＩＣカード１ｂに対して送信する。

ステップＳ４０３において、第２のＩＣカード１ｂのデータ送受信部１２が、当該第１のデジタルコンテンツの受信処理を完了すると、ステップＳ４０４において、第２のＩＣカード１ｂの実行処理部１５は、当該第１のデジタルコンテンツの受信処理が正常に完了した旨を通知する「コミット命令」を、第１のＩＣカード１ａに対して送信する。

ステップＳ４０５において、第１のＩＣカード１ａのデータ送受信部１２が、当該コミット命令を受信すると、ステップＳ４０６において、第１のＩＣカード１ａの実行処理部１５は、ホルダー部１８から第１のデジタルコンテンツを消去する。

一方、ステップＳ４０５において、第１のＩＣカード１ａのデータ送受信部１２が、当該コミット命令を受信しない場合、ステップＳ４０７において、第１のＩＣカード１ａの実行処理部１５は、第１のデジタルコンテンツの消去処理を行わず、各部１２乃至１９を、記憶している送信処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。

図７に示すように、第１のデジタルコンテンツの送信処理が開始されると、ステップＳ３０１において、第２のＩＣカード１ｂの実行処理部

１５が、送信処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）を記憶する。その後、第２のＩＣカード１ｂにおいて、当該第１のデジタルコンテンツの受信処理が開始されると、第２のＩＣカード１ｂは、受信した第１のデジタルコンテンツの蓄積を行う。

ステップＳ３０２において、当該第１のデジタルコンテンツの送信処理が中断されることなく終了した場合は、第２のＩＣカード１ｂは、受信した第１のデジタルコンテンツを保存して、当該送信処理は終了する。

一方、ステップＳ３０２において、当該第１のデジタルコンテンツの送信処理の中断が生じた場合には、ステップＳ３０３において、第２のＩＣカード１ｂの実行処理部１５は、各部１２乃至１９を、記憶している送信処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。このとき、受信されていた第１のデジタルコンテンツは消去される。

（３-２）　交換処理

以下、図８を参照して、上述のステップＳ１０６における交換処理について詳細に説明する。図８は、本実施形態に係るデータ通信方法における交換処理の動作を示すフロー図である。

図８に示すように、交換処理が開始されると、ステップＳ６０１及びＳ６０２において、第１のＩＣカード１ａ及び第２のＩＣカード１ｂの実行処理部１５が、交換処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）を記憶する。

ステップＳ６０３において、第１のＩＣカード１ａのデータ送受信部１２が、第１の端末装置２ａの通信部２１を介して、第２のＩＣカード１ｂに対して、暗号化された第１のデジタルコンテンツの送信を行う。

ステップＳ６０４において、第２のＩＣカード１ｂのデータ送受信部

１２が、当該第１のデジタルコンテンツの受信処理を完了すると、ステップＳ６０５において、第２のＩＣカード１ｂの実行処理部１５が、当該第１のデジタルコンテンツの受信処理が正常に完了した旨を通知する「コミット命令」を、第１のＩＣカード１ａに対して送信する。

ステップＳ６０６において、第１のＩＣカード１ａのデータ送受信部１２が、当該コミット命令を受信すると、第１のＩＣカード１ａの実行処理部１５は、第２のＩＣカード１ｂに対して、第２のデジタルコンテンツの「送信要求」を送信する。ステップＳ３０７において、第２のＩＣカード１ｂのデータ送受信部１２が、当該送信要求を受けて、第１のＩＣカード１ａに対して、第２のデジタルコンテンツの送信を行う。

第１のＩＣカード１ａのデータ送受信部１２が、当該第２のデジタルコンテンツの受信処理を完了すると、ステップＳ６０８において、その旨を示す「コミット命令」を、第２のＩＣカード１ｂに対して送信する。

ステップＳ６０９において、第２のＩＣカード１ｂのデータ送受信部１２が、当該コミット命令を受信した場合、すなわち、当該デジタルコンテンツの交換処理が中断されることなく正常に終了した場合、ステップＳ６１０において、第１のＩＣカード１ａ及び第２のＩＣカード１ｂの実行処理部１５が、ホルダー部１８から第１のデジタルコンテンツを消去する。

一方、ステップＳ６０６において、第１のＩＣカード１ａの実行処理部１５は、上述のコミット命令を受信しなかった場合、ステップＳ６１１において、第２のＩＣカード１ｂに対して送信処理を完了している第１のデジタルコンテンツを消去することなく、各部１２乃至１９を、記憶している交換処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。

かかる場合、第２のＩＣカード１ｂの実行処理部１５は、第１のＩＣカード１ａから送られてきて一時的に保持している第１のデジタルコンテンツを消去すると共に、各部１２乃至１９を、記憶している交換処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。

また、ステップＳ６０９において、第２のＩＣカード１ａの実行処理部１５が、上述のコミット命令を受信しなかった場合、ステップＳ６１１において、第１のＩＣカード１ａの実行処理部１５は、第２のＩＣカード１ｂから送られてきて一時的に保持している第２のデジタルコンテンツを消去する。また、第１のＩＣカード１ａの実行処理部１５は、第２のＩＣカード１ｂに対して送信処理を完了している第１のデジタルコンテンツを消去することなく、各部１２乃至１９を、記憶している交換処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。

かかる場合、第２のＩＣカード１ａの実行処理部１５は、第１のＩＣカード１ａに対して送信を完了している第２のデジタルコンテンツを消去することなく、各部１２乃至１９を、記憶している交換処理開始時の各部１２乃至１９の状態（ＩＣカードの状態）に復帰させる。また、第２のＩＣカード１ａの実行処理部１５は、第１のＩＣカード１ａから送られてきて一時的に保持している第１のデジタルコンテンツを消去する

（４）　監視処理

以下、図９を参照して、上述のステップＳ１０７における通信状態の監視処理について詳細に説明する。図９は、本実施形態に係るデータ通信方法における監視処理の動作を示すフロー図である。

図９に示すように、第１のＩＣカード１ａのデータ送受信部１２が、暗号化された第１のデジタルコンテンツを、第２のＩＣカード１ｂに対

して送信する。ステップＳ５０１において、第１のＩＣカード１ａの実行処理部１５が、デジタルコンテンツの送信時刻を計測し、最後にデジタルコンテンツを送信した時点を記憶する。

第１のＩＣカード１ａの実行処理部１５が、ステップＳ５０２において、最後にデジタルコンテンツを送信した時点からの経過時間を測定し、ステップＳ５０３及びＳ５０４において、所定長の待機時間が経過する間に、第２のＩＣカード１ｂから何らかの応答があるか否かを判断を行う。

ステップＳ５０４において、第２のＩＣカード１ｂからの応答があった場合は、第１のＩＣカード１ａの実行処理部１５は、ステップＳ５０２において、継続して経過時間の測定を行う。

一方、ステップＳ５０４において、第２のＩＣカード１ｂからの応答が無かったと判断された場合には、第１のＩＣカード１ａの実行処理部１５は、ステップＳ５０５において、監視処理についての中断処理を行う。この中断処理としては、上述した復帰処理（例えば、図４に示すステップＳ１１０）が考えられる。

［第２の実施形態］

（基本構成）

次いで、本発明の第２の実施形態について説明する。本実施形態では、本発明の第１の実施形態に係るデータ通信方法を、電子チケットや電子クーポンの配布等の電子商取引に応用することを特徴とする。

すなわち、本実施形態に係るデータ通信方法では、図１０に示すように、上述の第１の実施形態に係る第１のＩＣカード１ａが、電子チケット等のデジタルコンテンツを発行するコンテンツ発行サーバ１１に装填されて用いられる。

また、本実施形態に係るデータ通信方法では、コンテンツ発行サーバ１１により発行されたデジタルコンテンツは、当該コンテンツ発行サーバ１１から第２のＩＣカード１ｂに送信され、当該第２のＩＣカード１ｂは、当該コンテンツ発行サーバ１１から送信されたデジタルコンテンツの代金として電子マネーを支払う。

図１０乃至図１２は、第２の実施形態に係るデータ通信方法を採用したデジタルコンテンツ発行システムの構成を模式的に示す説明図である。

図１０に示すように、デジタルコンテンツ発行システムは、第２のＩＣカード１ｂに対してデジタルコンテンツを発行するコンテンツ発行サーバ１１と、当該デジタルコンテンツの発行に用いられる「ｃｒｅａｔｅコマンド（所定のコマンド）」及び「ｃｒｅａｔｅ権（生成権）」を生成して管理するコマンド生成サーバ３とを備える。

ここで、デジタルコンテンツの発行は、コンテンツ発行サーバ１１において生成されたデジタルコンテンツと、第２のＩＣカード１ｂに格納されている電子マネーとを交換することによって行われる。

詳述すると、デジタルコンテンツの発行は、コンテンツ発行サーバ１１内に装填された第１のＩＣカード１ａ内に一時的に格納されているデジタルコンテンツ（電子チケット等）が、第２のＩＣカード１ｂに転送され、第２のＩＣカード１ｂ内に一時的に格納されているデジタルコンテンツ（電子マネー）が、コンテンツ発行サーバ１１に転送されることによって行われる。

この際、コマンド生成サーバ３から取得したｃｒｅａｔｅコマンドが実行されることによって、コンテンツ発行サーバ１１と第２のＩＣカード１ｂとの間のデジタルコンテンツの交換が行われる。ｃｒｅａｔｅコマンドを実行するには、コマンド生成サーバ３で発行されたｃｒｅａｔ

ｅ権が必要となる。

コンテンツ発行サーバ１１は、一時的にデジタルコンテンツを格納する第１のＩＣカード１ａが装填されるインターフェイスを備えており、ｃｒｅａｔｅコマンドを実行することによって、デジタルコンテンツを、第２のＩＣカード１ｂ内に転送するサービスを行うサーバである。

ｃｒｅａｔｅコマンドは、図１１に示すように、コンテンツ発行サーバ１１からコマンド生成サーバ３に対して「登録要求」が送信された場合に、コマンド生成サーバ３によって登録が認められたコンテンツ発行サーバ１１に対して発行される実行プログラムである。

また、図１２に示すように、ｃｒｅａｔｅコマンドは、第１のＩＣカード１ａによって実行される度に、コマンド生成サーバ３に対して「認証要求」を送信し、当該ｃｒｅａｔｅコマンドに対応するｃｒｅａｔｅ権が存在するか否かについて、すなわち、当該ｃｒｅａｔｅ権が発行されているか否かについて照合（認証）する。

当該ｃｒｅａｔｅコマンドは、当該ｃｒｅａｔｅコマンドに対応するｃｒｅａｔｅ権が発行されている場合にのみ動作し、当該ｃｒｅａｔｅ権が発行されていない場合には、動作を拒否する。

なお、本実施形態では、図１２に示すように、コンテンツ発行サーバ１１は、コマンド生成サーバ３における認証結果について、コマンド生成サーバ３から送信される「ａｃｋ（ｏｋ/ｒｅｊｅｃｔ）」によって確認することができる。

すなわち、コンテンツ発行サーバ１１は、ｃｒｅａｔｅコマンドを実行することにより、コマンド生成サーバ３に対して、コマンド生成要求（上述の認証要求）を送信し、当該コマンド生成要求に対してコマンド生成サーバ３からａｃｋ（ｏｋ）を取得した場合に、デジタルコンテン

ツを生成することができる。

また、コンテンツ発行サーバ１１は、デジタルコンテンツの生成に先立って、コマンド生成サーバ３に対して登録処理を行い、ｃｒｅａｔｅコマンドを取得する必要がある。かかる登録処理によって、コマンド生成サーバ３は、当該ｃｒｅａｔｅコマンドに対するｃｒｅａｔｅ権を発行する。この発行されたｃｒｅａｔｅ権は、登録サーバデータベース３１において管理される。

また、コンテンツ発行サーバ１１は、デジタルコンテンツを生成する際、コマンド生成サーバ３との間で認証処理を行い、ｃｒｅａｔｅ権を取得する必要がある。かかる認証処理において、コンテンツ発行サーバ１１は、コマンド生成サーバ３に対して、コンテンツ生成要求（認証要求）と、個人情報（サーバ情報）と、当該コンテンツ発行サーバ１１自身の署名データとを送信する。

また、コマンド生成サーバ３は、ｃｒｅａｔｅコマンドを生成（発行）して、コンテンツ発行サーバ１１に対して送信するとともに、発行されたｃｒｅａｔｅコマンドに対応するｃｒｅａｔｅ権を発行して管理するものである。かかるｃｒｅａｔｅ権の管理には、登録サーバデータベース３１に格納された登録サーバリスト３１ａが用いられる。

コマンド生成サーバ３は、コンテンツ発行サーバ１１から「登録要求」と「個人情報（サーバ情報）」と「署名データ」とを受信した場合、受信した「個人情報（サーバ情報）」に基づいて当該コンテンツ発行サーバ１１の正当性を検証し、当該コンテンツ発行サーバ１１がデジタルコンテンツを生成する資格があると判断した場合は、登録サーバリスト３１ａに、当該コンテンツ発行サーバ１１に係る「個人情報（サーバ情報）」を登録し、ｃｒｅａｔｅコマンドを発行して当該コンテンツ発行サーバ

１１へ送信する。

また、コマンド生成サーバ３は、コンテンツ発行サーバ１１から、コンテンツ生成要求（認証要求）を受信した場合、当該コンテンツ生成要求に応じて、登録サーバリスト３１ａの照合（認証）を行い、認証結果が肯定的であるコンテンツ発行サーバのみにａｃｋ（ｏｋ）を返す。

（動作）

本実施形態に係るデータ通信方法（デジタルコンテンツの発行方法）について説明する。図１３は、本実施形態に係るデジタルコンテンツの発行方法を示すシーケンス図である。

図１３に示すように、ステップＳ１１０１において、コンテンツ発行サーバ１１が、コマンド生成サーバ３に対して、「登録要求」と共に、「個人情報（サーバ情報）」及び「署名データ」を送信する。

ステップＳ１１０２において、コマンド生成サーバ３は、受信した「個人情報（サーバ情報）」に基づいて、当該コンテンツ発行サーバ１１の正当性を検証し、当該コンテンツ発行サーバ１１がデジタルコンテンツを生成する資格があると判断した場合は、登録サーバリスト３１ａに、当該コンテンツ発行サーバ１１に係る「個人情報（サーバ情報）」を登録し、ステップＳ１１０３において、ｃｒｅａｔｅコマンドを当該コンテンツ発行サーバ１１へ送信する。

ステップＳ１１０４において、コンテンツ発行サーバ１１内に装填されている第１のＩＣカード１ａが、ｃｒｅａｔｅコマンドを実行すると、ステップＳ１１０５において、当該ｃｒｅａｔｅコマンドは、コマンド生成サーバ３に対して、「コンテンツ生成要求（認証要求）」と「個人情報（サーバ情報）」と「当該コンテンツ発行サーバ１１自身の署名データ」とを送信する。

ステップＳ１１０６において、コマンド生成サーバ３は、当該ｃｒｅａｔｅコマンドに対するｃｒｅａｔｅ権が存在するか否かについて、登録サーバリスト３１ａにおいて照合する。

ステップＳ１１０７において、コマンド生成サーバ３は、当該認証結果を「ａｃｋ（ｏｋ/ｒｅｊｅｃｔ）」として、コンテンツ発行サーバ１１に送信する。

コマンド生成サーバ３から送信されたａｃｋの内容が「ｏｋ」である場合、ステップＳ１１０８において、コンテンツ発行サーバ１１は、デジタルコンテンツ（例えば、電子チケット等）を生成する。

一方、コマンド生成サーバ３から送信されたａｃｋの内容が「ｒｅｊｅｃｔ」である場合、ステップＳ１１０９において、コンテンツ発行サーバ１１は、デジタルコンテンツ（例えば、電子チケット等）の生成を行わず、ｃｒｅａｔｅコマンド実行エラー処理を行う。

（変更例１）

なお、上述した第２の実施形態に対して、以下のような変更を採用することができる。図１４及び図１５は、変更例１に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本変更例では、ｃｒｅａｔｅコマンドとともに、ｃｒｅａｔｅ権自体が、コンテンツ発行サーバ１１に対して発行される。

図１４及び図１５に示すように、本変更例に係るデジタルコンテンツ発行システムは、第１のＩＣカード１ａに対してデジタルコンテンツの発行を行うコンテンツ発行サーバ１１と、デジタルコンテンツの発行に用いられるｃｒｅａｔｅコマンド及びｃｒｅａｔｅ権を生成して管理するコマンド生成サーバ３’とを備える。

本変更例に係るコマンド生成サーバ３’は、ｃｒｅａｔｅコマンドと

ｃｒｅａｔｅ権とを対応付けて管理する発行権管理部３２を有する。

コンテンツ発行サーバ１１は、コマンド生成サーバ３’から受信したｃｒｅａｔｅコマンド及びｃｒｅａｔｅ権を、第１のＩＣカード１ａ内に格納する。

ｃｒｅａｔｅコマンドは、第１のＩＣカード１ａによって実行される度に、第１のＩＣカード１ａ内において、当該ｃｒｅａｔｅコマンドに対応付けられて格納されているｃｒｅａｔｅ権が存在するか否かについて確認し、当該ｃｒｅａｔｅ権が存在する場合には、デジタルコンテンツを発行し、当該ｃｒｅａｔｅ権が存在しない場合には、ｃｒｅａｔｅコマンド実行エラー処理を行う。

本変更例に係るデータ通信方法（デジタルコンテンツの発行方法）について説明する。図１６は、本変更例に係るデジタルコンテンツの発行方法を示すシーケンス図である。

ステップＳ１２０１において、コンテンツ発行サーバ１１は、コマンド生成サーバ３’に対して、「ｃｒｅａｔｅ権生成要求」と「個人情報（サーバ情報）」とを送信する。

ステップＳ１２０２において、コマンド生成サーバ３’は、「ｃｒｅａｔｅ権生成要求」の受信に応じて、受信した「個人情報」を検証して、当該コンテンツ発行サーバ１１にデジタルコンテンツを生成する資格があるか否かを検証し、デジタルコンテンツを生成する資格があると判断した場合には、ステップＳ１２０３において、コンテンツ発行サーバ１１に対して、ｃｒｅａｔｅ権及びｃｒｅａｔｅコマンドを送信する。

ステップＳ１２０４において、コマンド生成サーバ３’から送信されたｃｒｅａｔｅ権及びｃｒｅａｔｅコマンドは、コンテンツ発行サーバ１１内の第１のＩＣカード１ａ内に直接格納される。

ステップＳ１２０５において、コンテンツ発行サーバ１１が、デジタルコンテンツを発行する場合は、ｃｒｅａｔｅコマンドを実行する。

ステップＳ１２０６において、ｃｒｅａｔｅコマンドは、第１のＩＣカード１ａ内のｃｒｅａｔｅ権が存在するか否かを確認する。

第１のＩＣカード１ａ内にｃｒｅａｔｅ権が存在すれば、コンテンツ発行サーバ１１が、ステップＳ１２０７において、ｃｒｅａｔｅコマンドを用いて、デジタルコンテンツを発行し、第１のＩＣカード１ａ内にｃｒｅａｔｅ権が存在しない場合には、コンテンツ発行サーバ１１が、ステップＳ１２０８において、ｃｒｅａｔｅコマンド実行エラー処理を行う。

（変更例２）

図１７及び図１８を参照して、第２の実施形態の変更例２について説明する。図１７及び図１８は、本変更例に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本変更例では、コンテンツ発行サーバ１１の正当性の検証は、ソフトウェアによって行われるのではなく、物理的に行われる。

図１７及び図１８に示すように、本変更例に係るデジタルコンテンツ発行システムは、第１のＩＣカード１ａに対してデジタルコンテンツの発行を行うコンテンツ発行サーバ１１を具備している。

ここで、コンテンツ発行サーバ１１には、最初からｃｒｅａｔｅコマンドが焼き込まれているＩＣカード（ＩＣチップ）４が接続（装填）されており、当該コンテンツ発行サーバ１１は、デジタルコンテンツを発行する際には、当該ＩＣカード４にアクセスすることによって、ｃｒｅａｔｅコマンドを呼び出して実行する。

ＩＣカード４には、ｃｒｅａｔｅコマンドが物理的に固定されており、

外部からの変更ができないようになっている。デジタルコンテンツ発行システムを変更する場合には、物理的に当該ＩＣチップ４を変更することで、コンテンツ発行サーバ１１を変更する。

（変更例３）

次いで、図１９乃至図２１を参照して、第２の実施形態の変更例３について説明する。図１９及び図２０は、本変更例に係るデジタルコンテンツ発行システムの構成を示すブロック図である。

図１９及び図２０に示すように、本変更例に係るデジタルコンテンツ発行システムは、第１のＩＣカード１ａに対してデジタルコンテンツの発行を行うコンテンツ発行サーバ１１と、デジタルコンテンツの発行に用いられるｃｒｅａｔｅコマンドを生成するコマンド生成サーバ３”とを備える。

本変更例に係るコマンド生成サーバ３”は、正当性が認証されたコンテンツ発行サーバ１１（又は、第１のＩＣカード１ａ）のＩＤを用いて、ｃｒｅａｔｅコマンドを暗号化して、当該コンテンツ発行サーバ１１に対して送信する機能を有する。

図２１を参照して、本変更例に係るデータ通信方法（デジタルコンテンツの発行方法）について説明する。図２１は、本変更例に係るデジタルコンテンツの発行方法を示すシーケンス図である。

図２１に示すように、ステップＳ１３－１において、コンテンツ発行サーバ１１は、コマンド生成サーバ３”に対して、「ｃｒｅａｔｅコマンド生成要求」と共に、「個人情報（コンテンツ発行サーバ１１又は第１のＩＣカード１ａのＩＤを含む）」を送信する。

コマンド生成サーバ３”は、ステップＳ１３０２において、「ｃｒｅａｔｅコマンド生成要求」に応じて、受信した「個人情報」に基づいて、

当該コンテンツ発行サーバ１１の正当性について認証を行った後、当該コンテンツ発行サーバ１１にデジタルコンテンツを生成する資格があると判断した場合には、ステップＳ１３０３において、コンテンツ発行サーバ１１（又は、第１のＩＣカード１ａ）のＩＤを用いて、ｃｒｅａｔｅコマンドを暗号化する。

ステップＳ１３０４において、コマンド生成サーバ３”は、暗号化されたｃｒｅａｔｅコマンドを、コンテンツ発行サーバ１１に対して送信する。

コンテンツ発行サーバ１１は、この暗号化されたｃｒｅａｔｅコマンドを受け取り、第１のＩＣカード１ａ内に直接格納する。第１のＩＣカード１ａは、当該コンテンツ発行サーバ１１に係る個人情報から、当該コンテンツ発行サーバ１１のＩＤを抽出する。

ステップＳ１３０５において、第１のＩＣカード１ａは、抽出したコンテンツ発行サーバ１１のＩＤ（又は、第１のＩＣカード１ａのＩＤ）を用いて、格納しているｃｒｅａｔｅコマンドの復号を行う。

ステップＳ１３０６において、第１のＩＣカード１ａは、復号されたcreateコマンドを実行し、デジタルコンテンツを発行する。この結果、正当性が認証されたコンテンツ発行サーバ１１のみに、ｃｒｅａｔｅコマンドを発行することが可能となる。

産業上の利用可能性

以上説明したように、本発明によれば、外部の端末装置やサーバのコマンドを用いることなく、ＩＣカード内部に備えられたアトミックなコマンドを用いて、デジタルコンテンツの暗号化処理や送信処理や交換処理を行うことから、外部の端末装置やサーバ側からの不正な操作による

影響を回避することができ、外部の端末装置やサーバのセキュリティー環境によらず、安全なデジタルコンテンツの送信処理（又は、交換処理）を行うことができる。

この結果、ＩＣカード間で直接通信を行う通信プラットホーム上で、デジタルコンテンツを送信（又は、交換）する際に、送受信者及び悪意のある第三者による複製や紛失を回避することができる。

請 求 の 範 囲

1． 第１のデジタルコンテンツを格納するホルダー部と、

前記第１のデジタルコンテンツに対応付けられた鍵情報を含む証明書データを格納する証明書データ格納部と、

暗号処理部と、

実行処理部とを備え、

前記実行処理部は、所定のトリガー信号を受信すると、所定のコマンドを実行し、

前記実行処理部によって実行された前記所定のコマンドは、

前記実行処理部に、前記第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶させ、

前記暗号化処理部に、前記第１のデジタルコンテンツに対応付けられた前記鍵情報に基づいて、該第１のデジタルコンテンツの暗号化処理を行わせ、

暗号化された前記第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置から受信した場合、前記ホルダー部から前記第１のデジタルコンテンツを消去し、

前記第１のデジタルコンテンツの送信処理が中断された場合、前記実行処理部に記憶されている前記ＩＣカードの状態への復帰処理を行うことを特徴とするＩＣカード。

2． 前記実行処理部によって実行された前記所定のコマンドは、

前記コミット命令を受信した場合、前記送信先装置に対して第２のデジタルコンテンツの送信要求を送信し、

前記第２のデジタルコンテンツの受信処理が完了した場合、前記ホル

ダー部から前記第１のデジタルコンテンツを消去することを特徴とする請求項１に記載のＩＣカード。

３．　前記第１のデジタルコンテンツの送信に先だって、前記送信先装置から該送信先装置の証明書データを取得し、該証明書データに基づいて該送信先装置の正当性を認証する認証部を具備し、

前記実行処理部は、前記送信先装置の正当性が認証された場合に、前記所定のコマンドを実行することを特徴とする請求項１に記載のＩＣカード。

４．　前記認証部は、前記送信先装置との間のセッションを識別するセッションＩＤとセッションモードとに応じて、前記ホルダー部に格納されている前記第１のデジタルコンテンツへのアクセスレベルを設定することを特徴とする請求項３に記載のＩＣカード。

５．　前記認証部は、前記第１のデジタルコンテンツの送信に先だって、前記証明書データ格納部に格納されている前記証明書データを前記送信先装置に対して送信し、前記送信先装置から該証明書データの正当性が認証された旨を通知する認証確認通知を取得し、

前記実行処理部は、前記認証確認通知が取得された場合に、前記所定のコマンドを実行することを特徴とする請求項３に記載のＩＣカード。

６．　ＩＣカードに格納されている第１のデジタルコンテンツを送信先装置に送信する端末装置であって、

入力された操作信号に基づいて、所定のトリガー信号を、前記ＩＣカードに対して出力する制御部を具備し、

前記ＩＣカードの実行処理部は、前記所定のトリガー信号に応じて、所定のコマンドを実行し、

前記実行処理部によって実行された前記所定のコマンドは、

前記実行処理部に、前記第１のデジタルコンテンツの送信前における前記ＩＣカードの状態を記憶させ、

前記ＩＣカードの暗号化処理部に、前記第１のデジタルコンテンツに対応付けられた鍵情報に基づいて、該第１のデジタルコンテンツの暗号化処理を行わせ、

暗号化された前記第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を前記送信先装置から受信した場合、前記ＩＣカードのホルダー部から前記第１のデジタルコンテンツを消去し、

前記第１のデジタルコンテンツの送信処理が中断された場合、前記実行処理部に記憶されている前記ＩＣカードの状態への復帰処理を行うことを特徴とする端末装置。

７．　前記実行処理部によって実行された前記所定のコマンドは、

前記コミット命令を受信した場合、前記送信先装置に対して第２のデジタルコンテンツの送信要求を送信し、

前記第２のデジタルコンテンツの受信処理が完了した場合、前記ホルダー部から前記第１のデジタルコンテンツを消去することを特徴とする請求項６に記載の端末装置。

８．　前記ＩＣカードから前記送信先装置に前記第１のデジタルコンテンツを送信した後、所定の待機時間を経過するまでの間に、該送信先装置から応答がない場合、前記第１のデジタルコンテンツの送信処理が中断された旨を前記ＩＣカードに通知する通信監視部を具備することを特徴とする請求項６に記載の端末装置。

９．　前記ＩＣカードと前記送信先装置との間で確立されているセッションを識別するセッションＩＤとセッションモードとに応じて設定されたアクセスレベルに基づいて、前記ホルダー部から前記第１のデジタル

コンテンツに関する情報を読み出して表示する表示部を具備することを特徴とする請求項６に記載の端末装置。

１０．　ＩＣカードに格納されている第１のデジタルコンテンツを送信先装置に送信するデータ通信方法であって、

前記ＩＣカードが、所定のトリガー信号を受信すると、所定のコマンドを実行する工程と、

前記第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶する工程と、

前記第１のデジタルコンテンツに対応付けられた鍵情報に基づいて、該第１のデジタルコンテンツの暗号化処理を行う工程と、

暗号化された前記第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を前記送信先装置から受信した場合、前記ＩＣカードのホルダー部から前記第１のデジタルコンテンツを消去する工程と、

前記第１のデジタルコンテンツの送信処理が中断された場合、記憶されている前記ＩＣカードの状態への復帰処理を行う工程とを有することを特徴とするデータ通信方法。

１１．　前記コミット命令を受信した場合、前記送信先装置に対して第２のデジタルコンテンツの送信要求を送信する工程と、

前記第２のデジタルコンテンツの受信処理が完了した場合、前記ホルダー部から前記第１のデジタルコンテンツを消去する工程とを有することを特徴とする請求項１０に記載のデータ通信方法。

１２．　前記ＩＣカードが装填された端末装置が、入力された操作信号に基づいて、前記所定のトリガー信号を、前記ＩＣカードに対して出力する工程を有することを特徴とする請求項１０に記載のデータ通信方法。

FIG.1

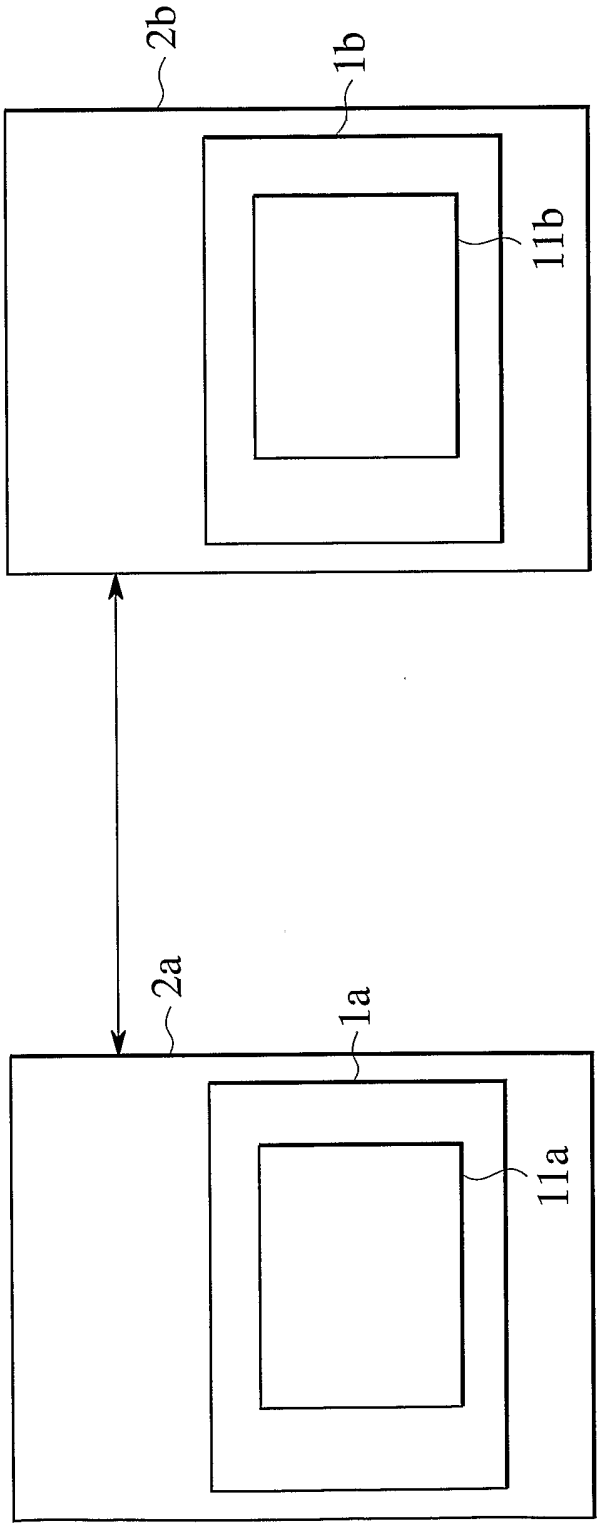


FIG.2

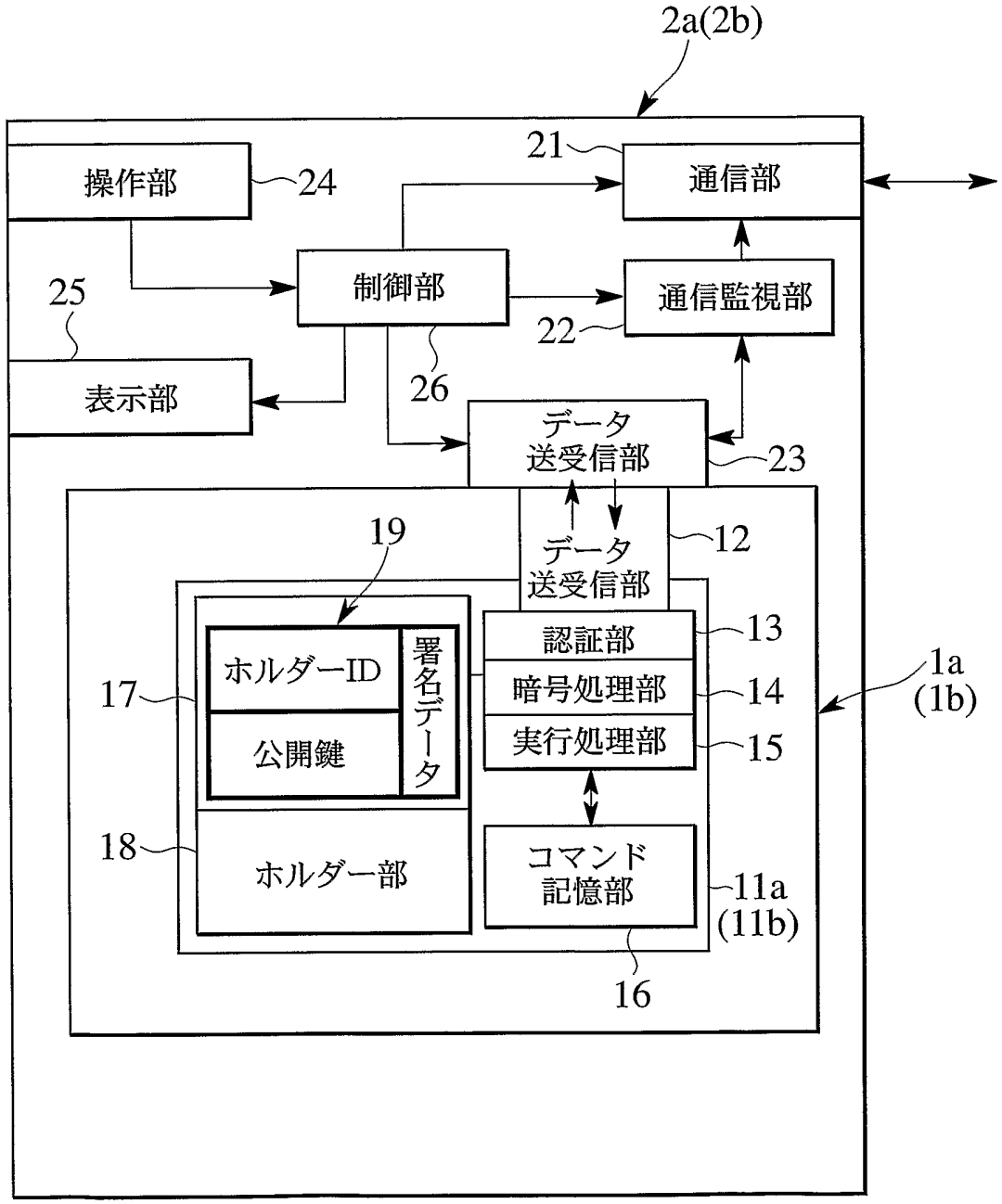

2a(2b)
操作部
24
21
通信部
制御部
通信監視部
25
22
表示部
26
データ
送受信部
23
19
データ
送受信部
12
ホルダーID
署名データ
公開鍵
認証部
13
暗号処理部
14
実行処理部
15
17
1a
(1b)
18
ホルダー部
コマンド
記憶部
11a
(11b)
16

FIG.3

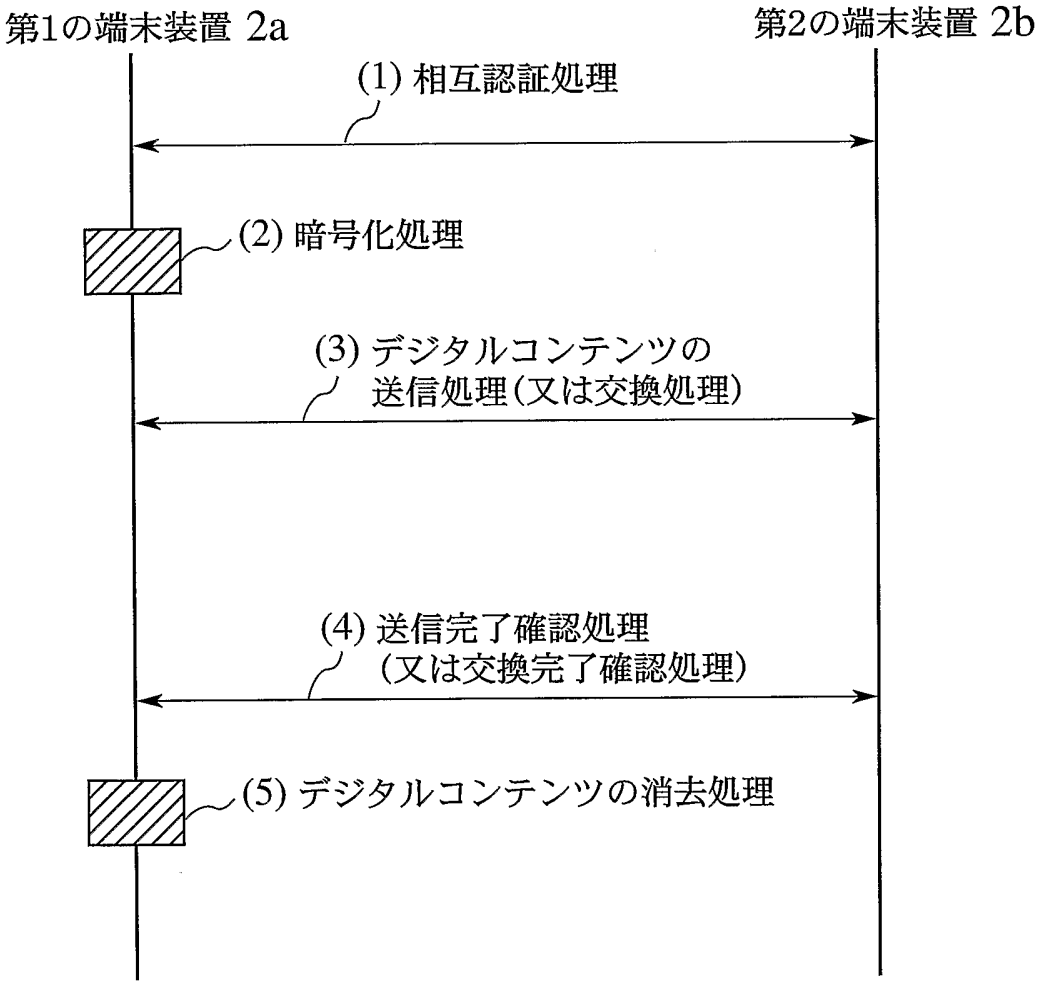

第1の端末装置 2a
第2の端末装置 2b
(1) 相互認証処理
(2) 暗号化処理
(3) デジタルコンテンツの
送信処理(又は交換処理)
(4) 送信完了確認処理
(又は交換完了確認処理)
(5) デジタルコンテンツの消去処理

FIG.4

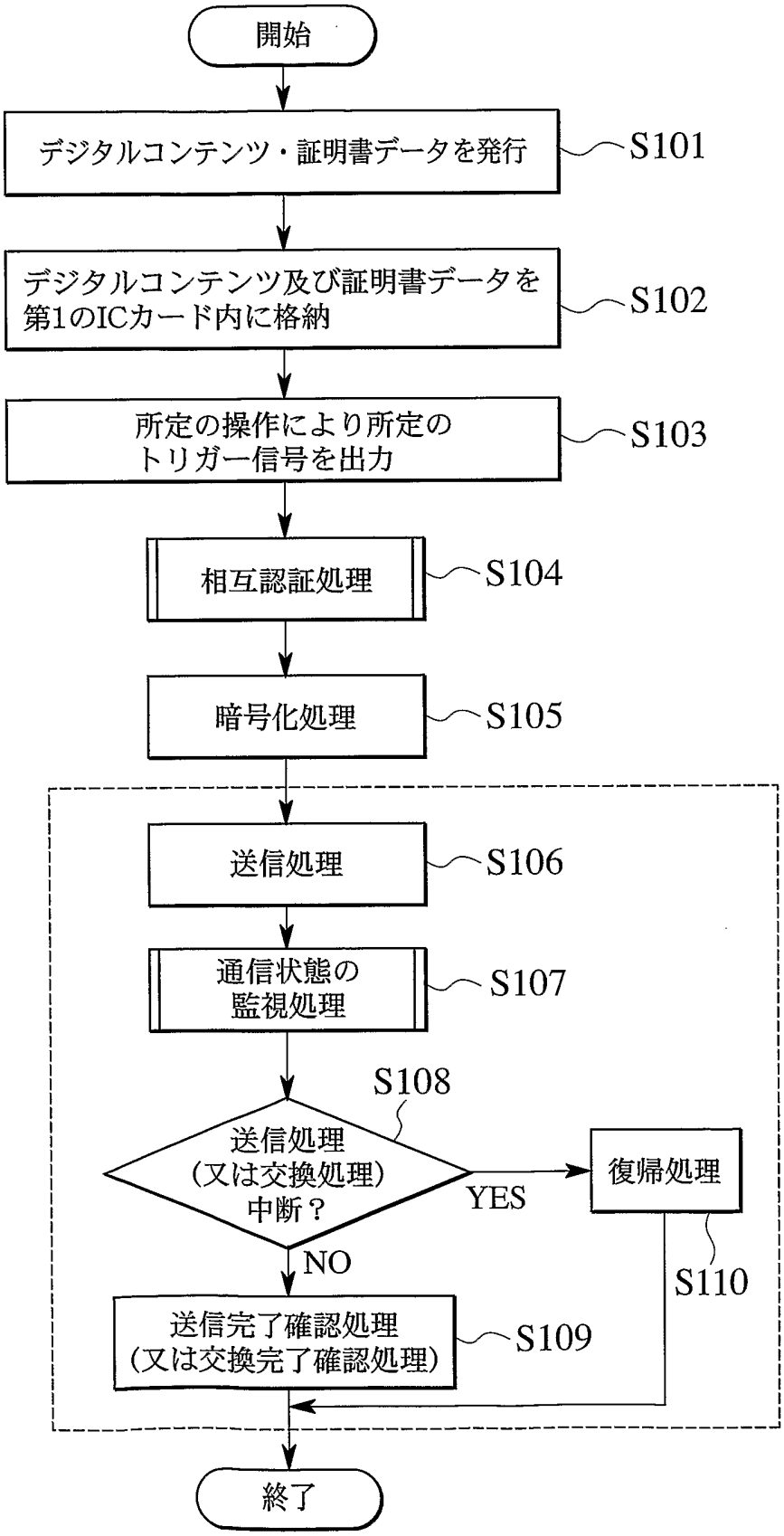

開始
デジタルコンテンツ・証明書データを発行
S101
デジタルコンテンツ及び証明書データを第1のICカード内に格納
S102
所定の操作により所定のトリガー信号を出力
S103
相互認証処理
S104
暗号化処理
S105
送信処理
S106
通信状態の監視処理
S107
S108
送信処理(又は交換処理)中断？
YES
復帰処理
S110
NO
送信完了確認処理(又は交換完了確認処理)
S109
終了

FIG.5

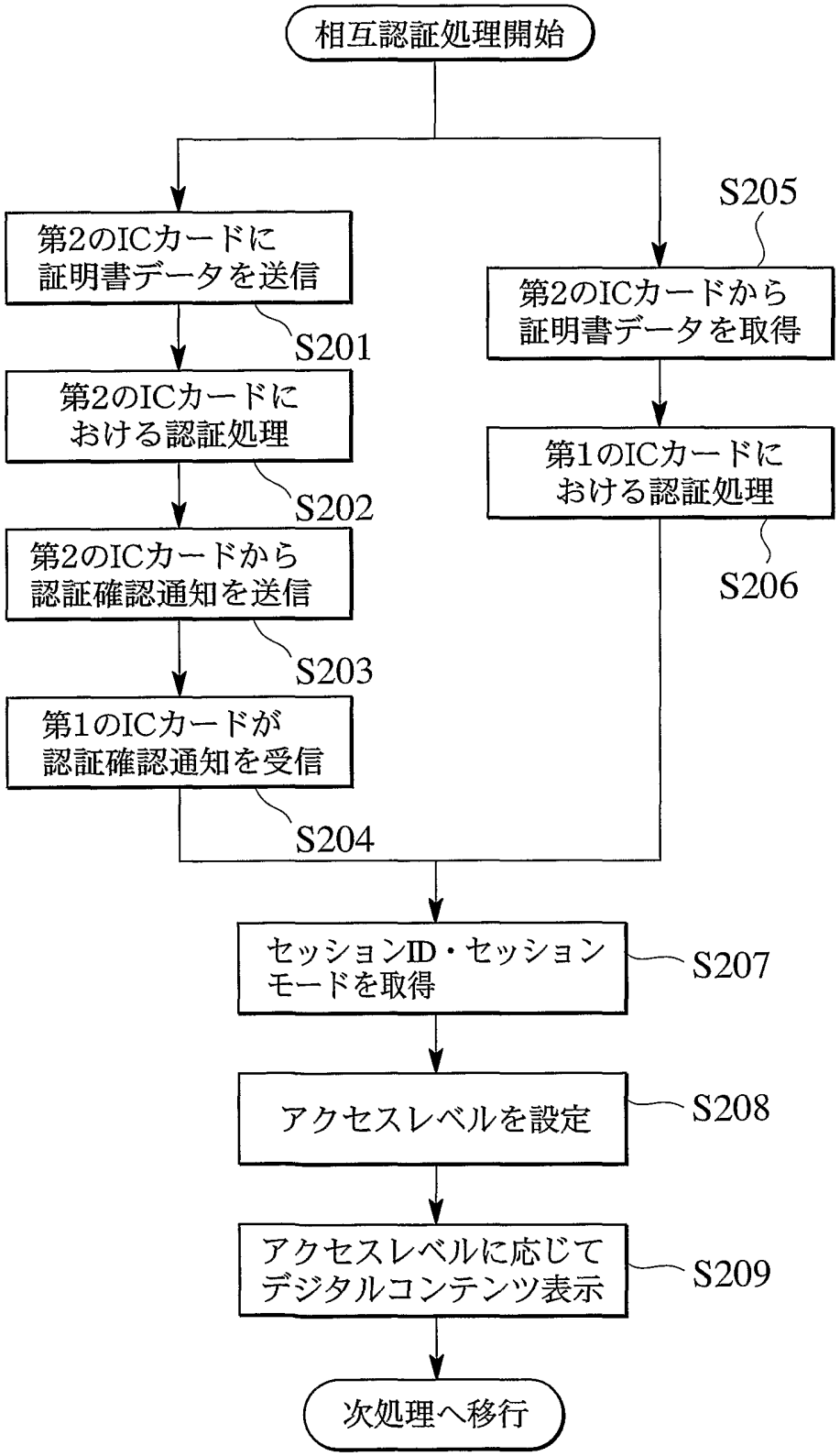

相互認証処理開始
第2のICカードに
証明書データを送信
S201
第2のICカードに
おける認証処理
S202
第2のICカードから
認証確認通知を送信
S203
第1のICカードが
認証確認通知を受信
S204
S205
第2のICカードから
証明書データを取得
第1のICカードに
おける認証処理
S206
セッションID・セッション
モードを取得
S207
アクセスレベルを設定
S208
アクセスレベルに応じて
デジタルコンテンツ表示
S209
次処理へ移行

FIG.6

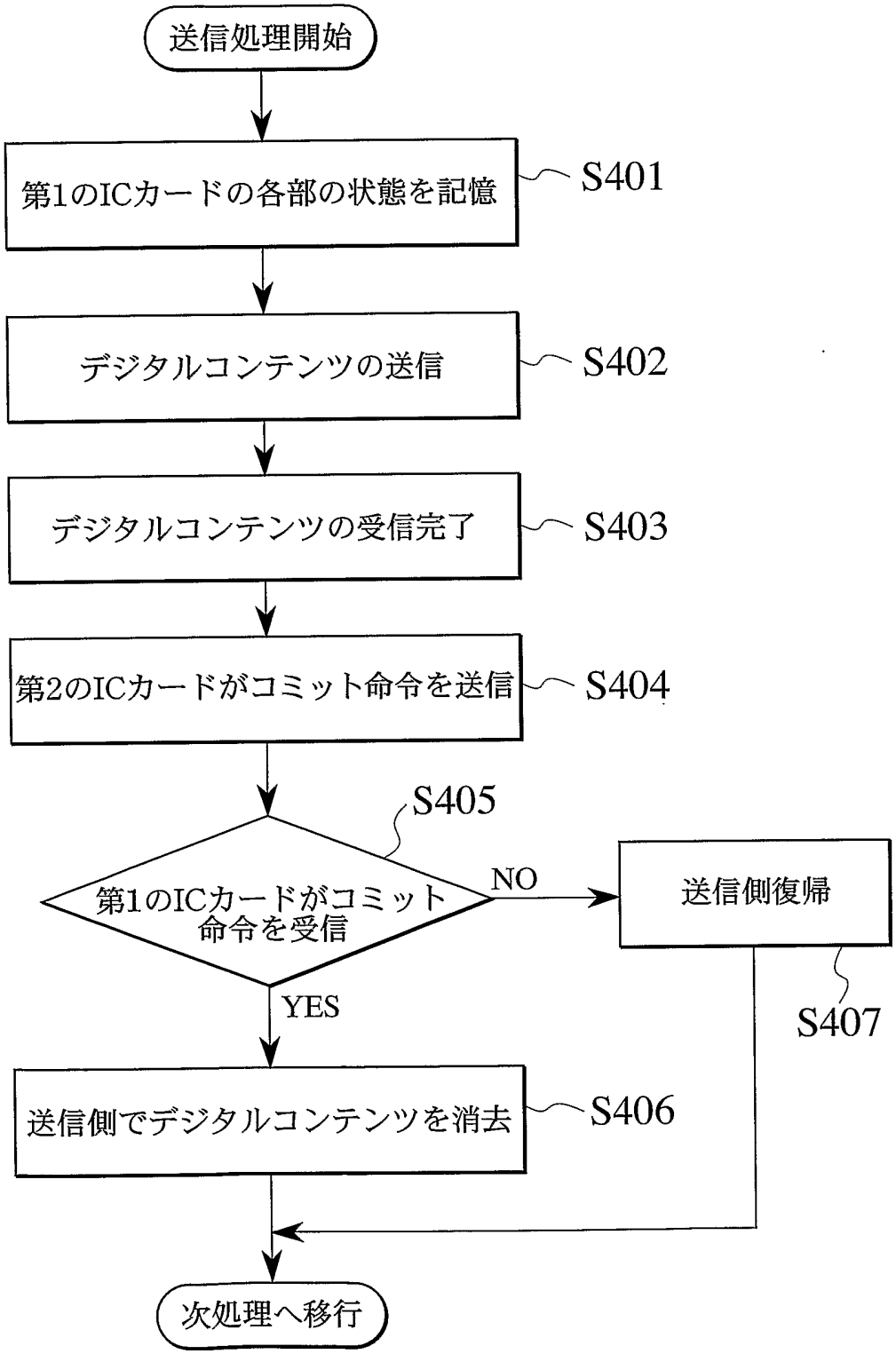

送信処理開始
第1のICカードの各部の状態を記憶
S401
デジタルコンテンツの送信
S402
デジタルコンテンツの受信完了
S403
第2のICカードがコミット命令を送信
S404
S405
第1のICカードがコミット命令を受信
NO
送信側復帰
S407
YES
送信側でデジタルコンテンツを消去
S406
次処理へ移行

FIG.7

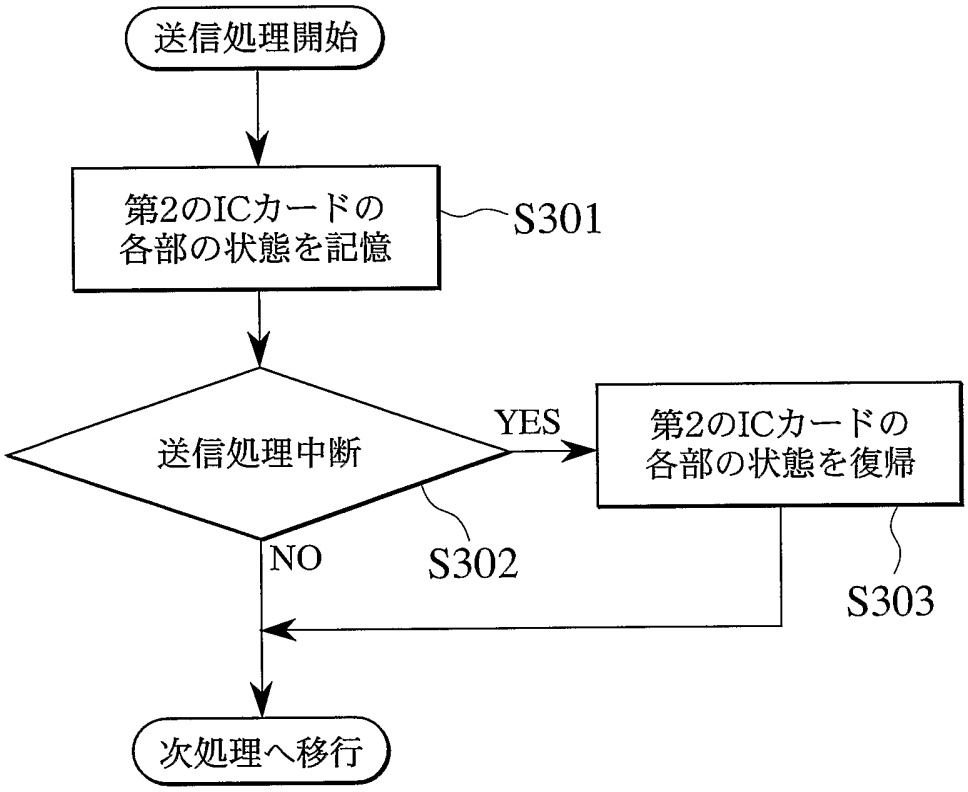

送信処理開始
第2のICカードの
各部の状態を記憶
S301
送信処理中断
YES
第2のICカードの
各部の状態を復帰
NO
S302
S303
次処理へ移行

FIG.8

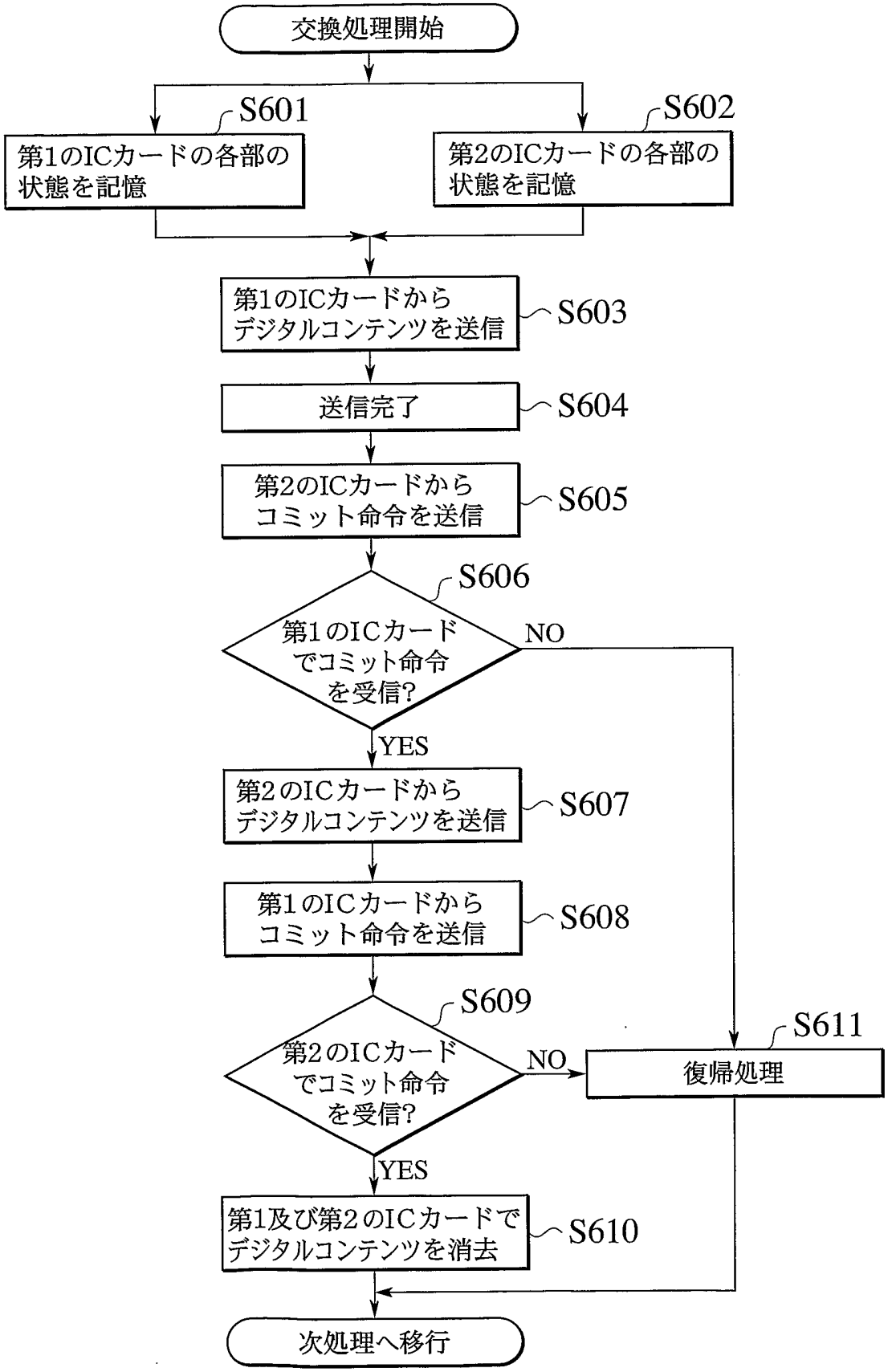

交換処理開始
S601
第1のICカードの各部の状態を記憶
S602
第2のICカードの各部の状態を記憶
第1のICカードからデジタルコンテンツを送信
S603
送信完了
S604
第2のICカードからコミット命令を送信
S605
S606
第1のICカードでコミット命令を受信?
NO
YES
第2のICカードからデジタルコンテンツを送信
S607
第1のICカードからコミット命令を送信
S608
S609
第2のICカードでコミット命令を受信?
NO
S611
復帰処理
YES
第1及び第2のICカードでデジタルコンテンツを消去
S610
次処理へ移行

FIG.9

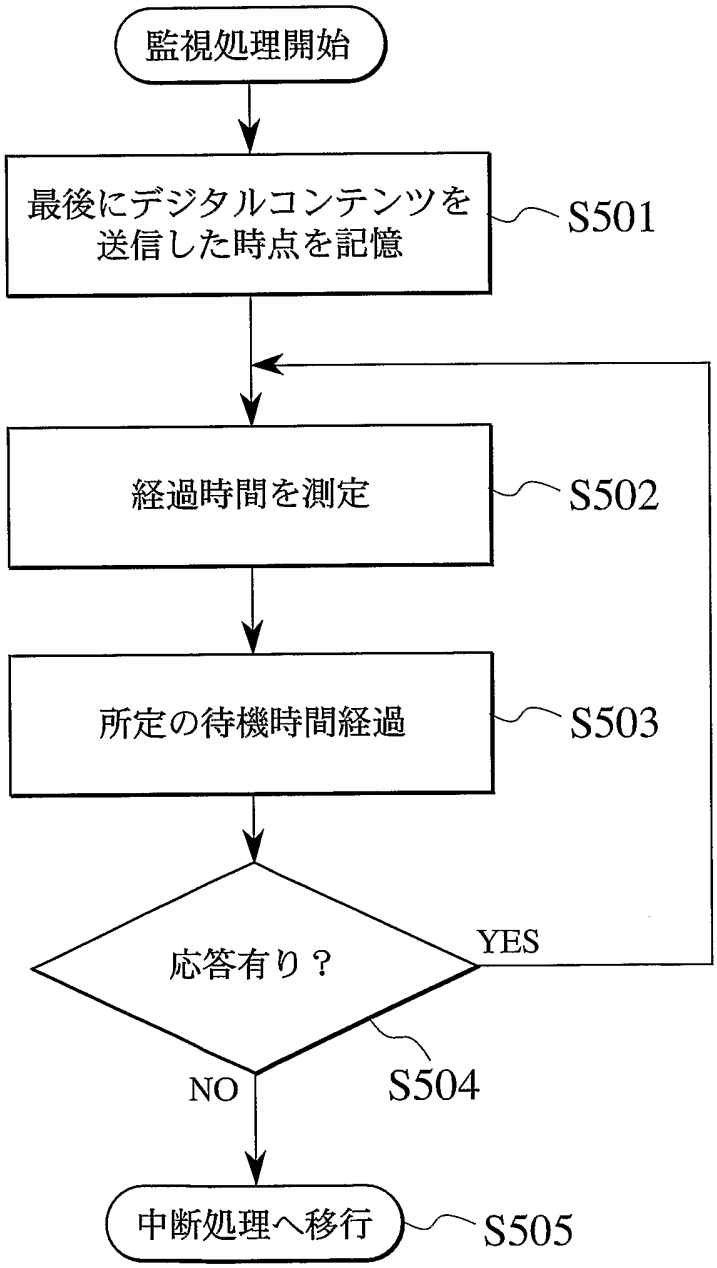

監視処理開始
最後にデジタルコンテンツを送信した時点を記憶
S501
経過時間を測定
S502
所定の待機時間経過
S503
応答有り？
YES
NO
S504
中断処理へ移行
S505

FIG.10

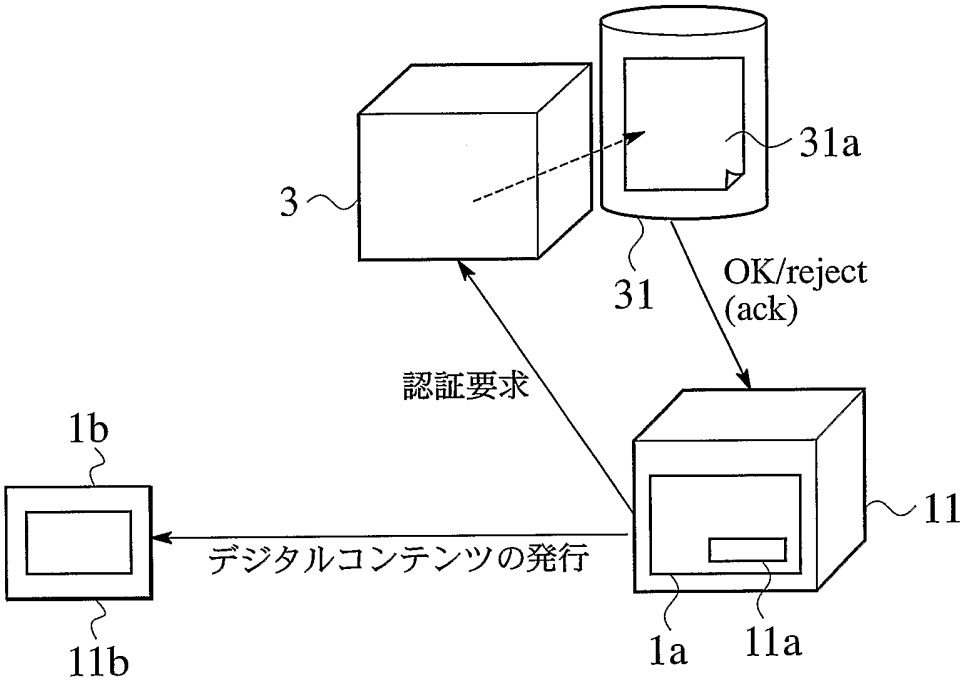

3
31a
31
OK/reject
(ack)
認証要求
1b
11
デジタルコンテンツの発行
11b
1a
11a

FIG.11

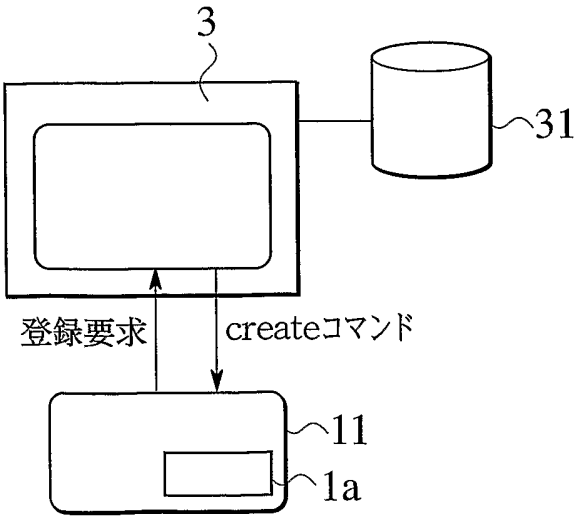

3
31
登録要求
createコマンド
11
1a

FIG.12

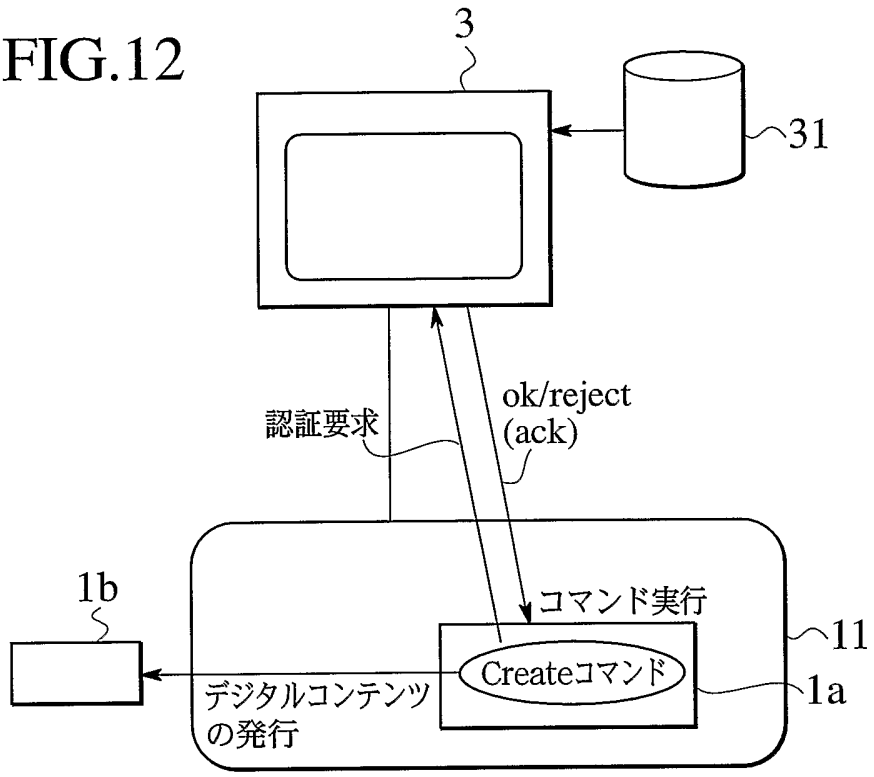

3
31
認証要求
ok/reject
(ack)
1b
コマンド実行
11
Createコマンド
1a
デジタルコンテンツ
の発行

FIG.13

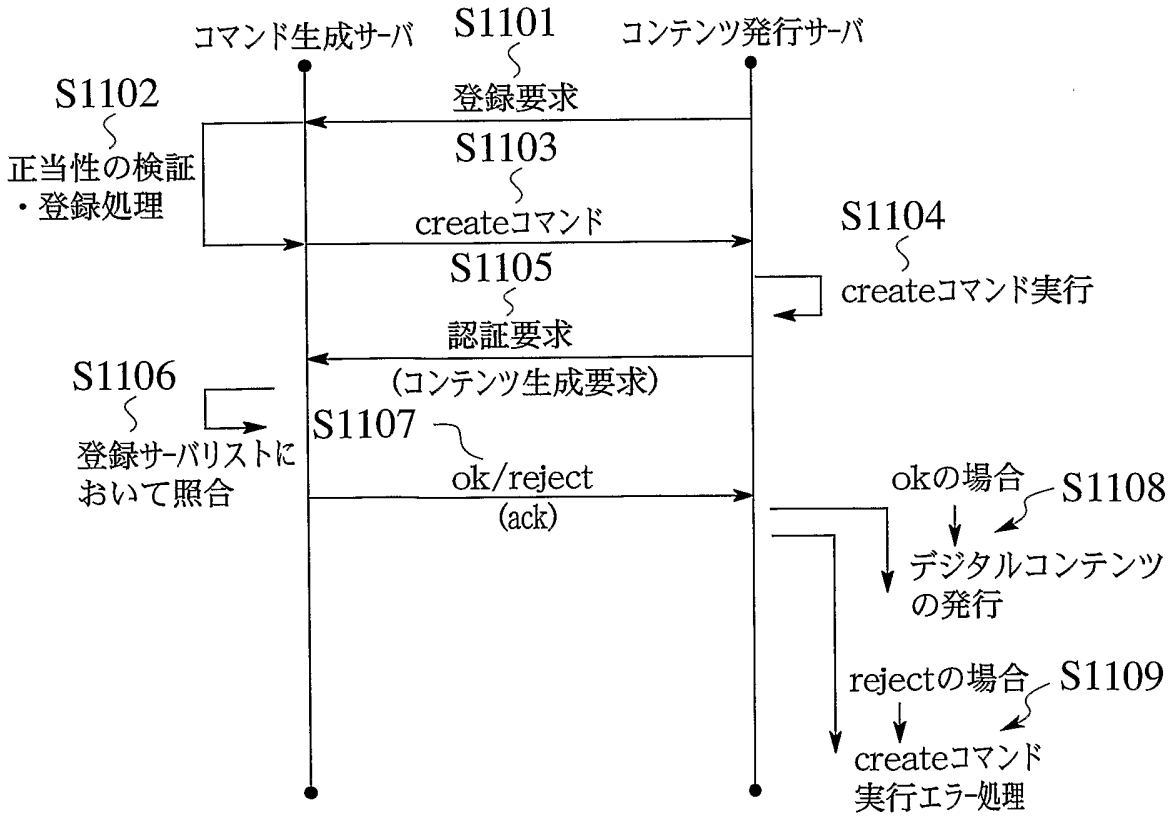

コマンド生成サーバ
S1101
コンテンツ発行サーバ
S1102
登録要求
正当性の検証
・登録処理
S1103
createコマンド
S1104
createコマンド実行
S1105
認証要求
(コンテンツ生成要求)
S1106
S1107
登録サーバリストに
おいて照合
ok/reject
(ack)
okの場合
S1108
デジタルコンテンツ
の発行
rejectの場合
S1109
createコマンド
実行エラー処理

FIG.14

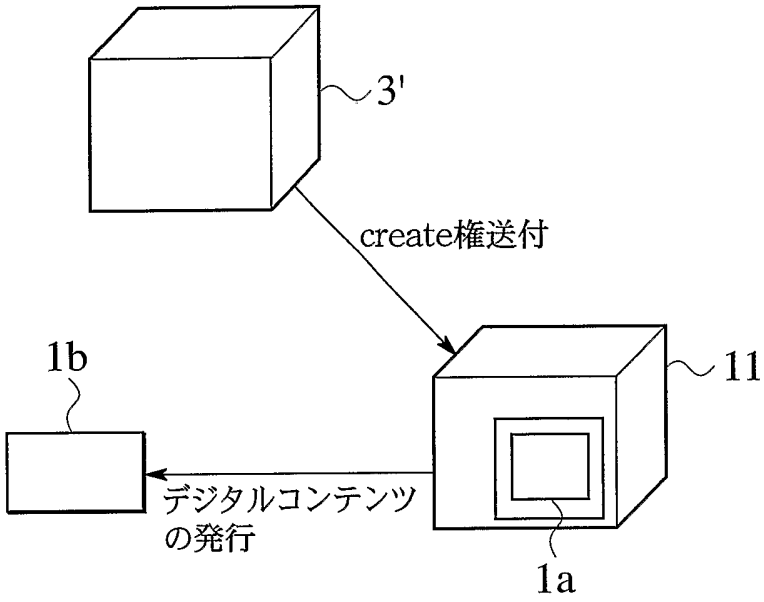

3'
create権送付
1b
11
デジタルコンテンツ
の発行
1a

FIG.15

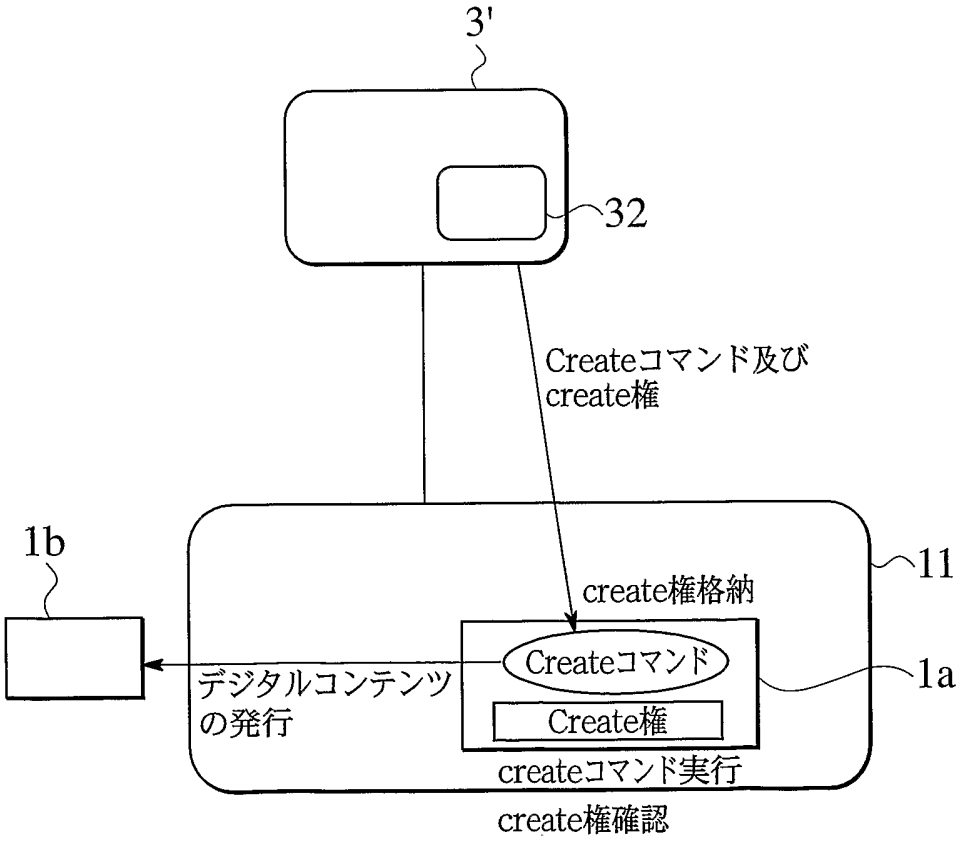

3'
32
Createコマンド及び
create権
1b
11
create権格納
Createコマンド
デジタルコンテンツ
の発行
1a
Create権
createコマンド実行
create権確認

FIG.16

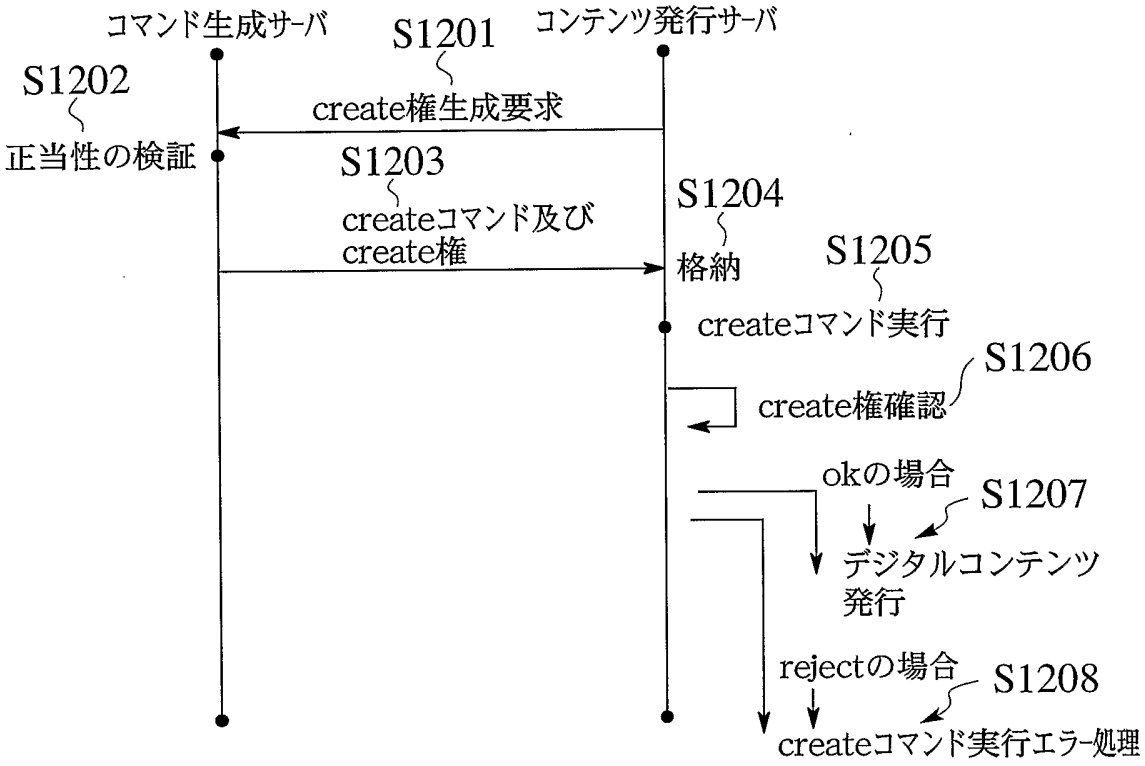

コマンド生成サーバ
S1201
コンテンツ発行サーバ
S1202
create権生成要求
正当性の検証
S1203
S1204
createコマンド及び
create権
格納
S1205
createコマンド実行
S1206
create権確認
okの場合
S1207
デジタルコンテンツ
発行
rejectの場合
S1208
createコマンド実行エラー処理

FIG.17

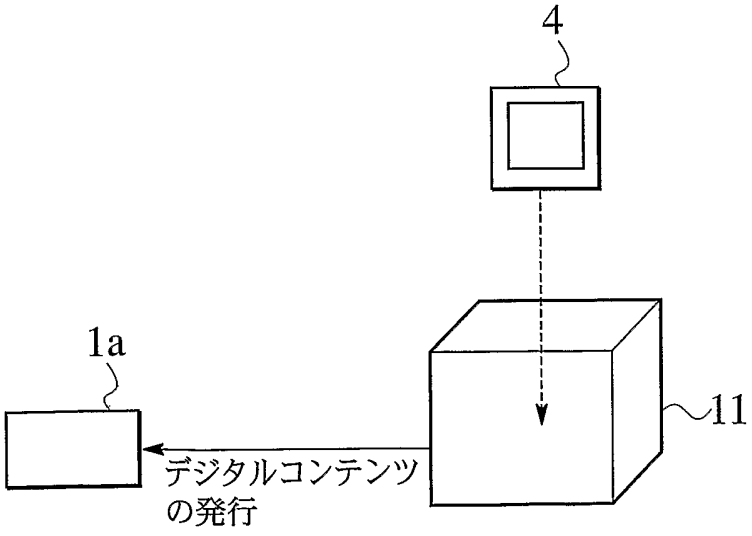

4
1a
11
デジタルコンテンツ
の発行

FIG.18

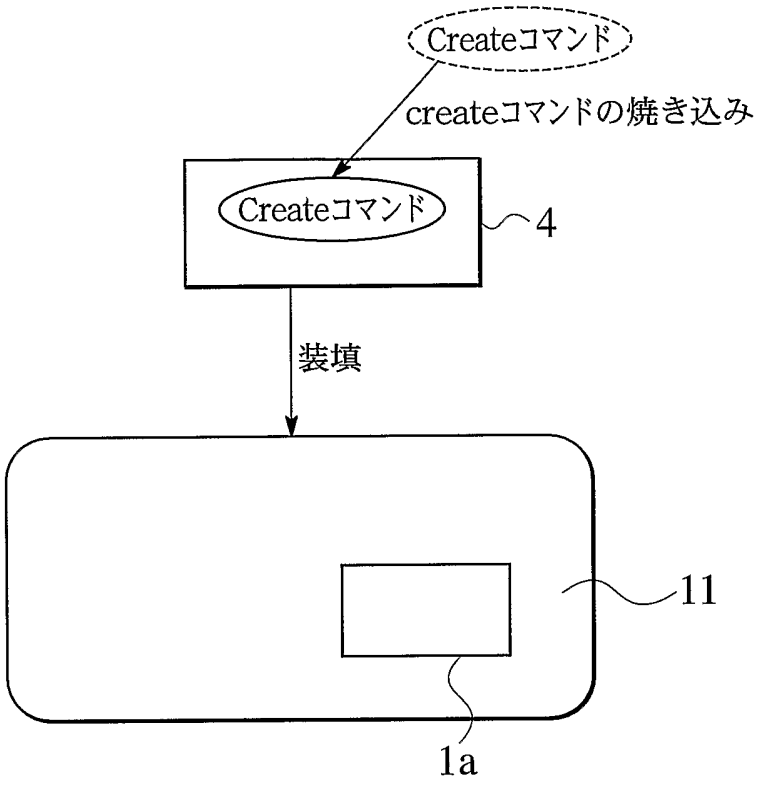

Createコマンド
createコマンドの焼き込み
Createコマンド
4
装填
11
1a

FIG.19

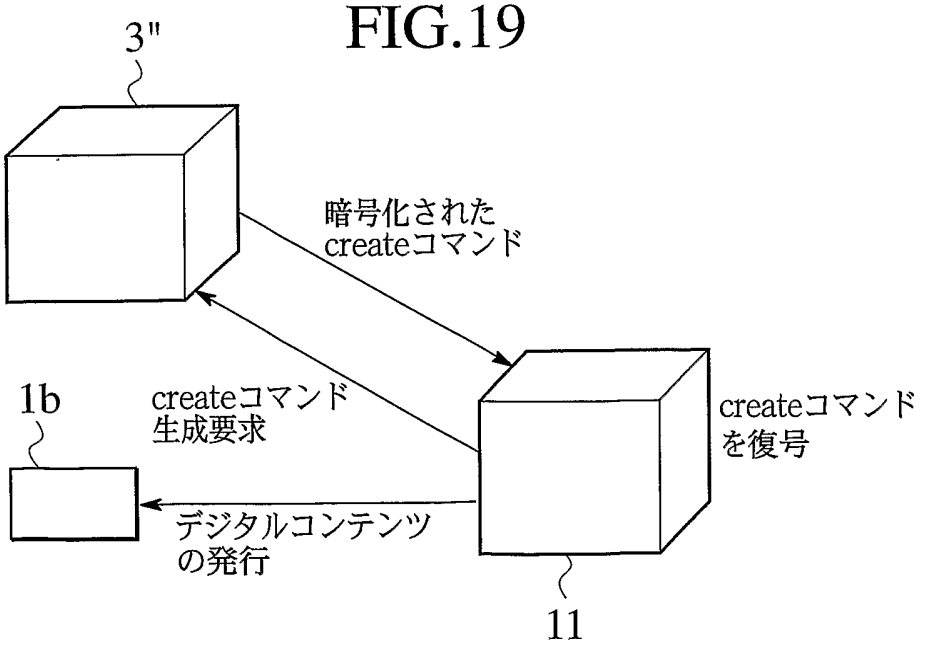

3"
暗号化された
createコマンド
1b
createコマンド
生成要求
createコマンド
を復号
デジタルコンテンツ
の発行
11

FIG.20

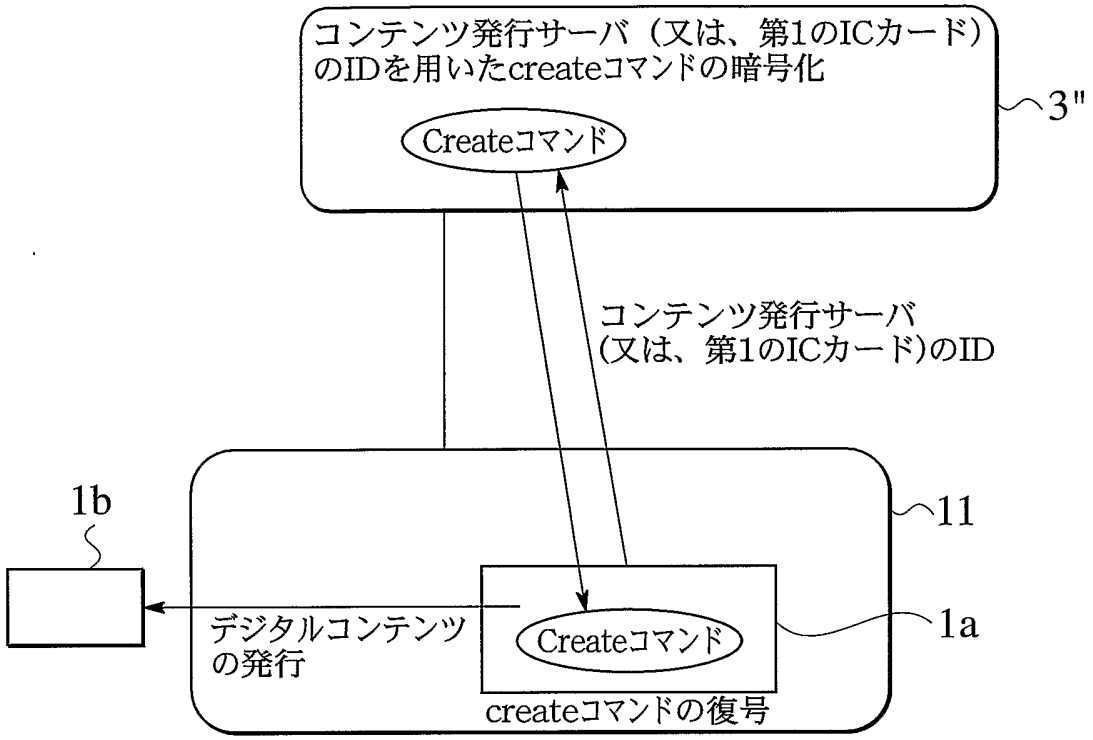
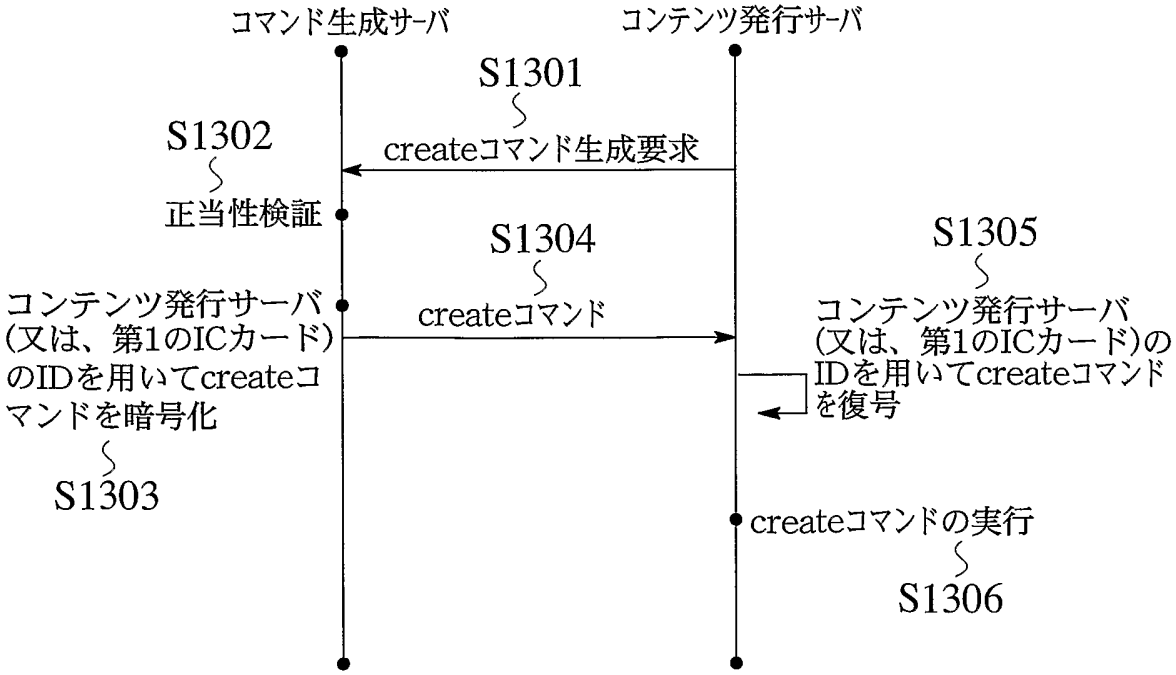

コンテンツ発行サーバ（又は、第1のICカード）のIDを用いたcreateコマンドの暗号化
Createコマンド
3"
コンテンツ発行サーバ(又は、第1のICカード)のID
1b
11
デジタルコンテンツの発行
Createコマンド
1a
createコマンドの復号

FIG.21


コマンド生成サーバ
コンテンツ発行サーバ
S1301
createコマンド生成要求
S1302
正当性検証
S1304
createコマンド
S1305
コンテンツ発行サーバ(又は、第1のICカード)のIDを用いてcreateコマンドを暗号化
S1303
コンテンツ発行サーバ(又は、第1のICカード)のIDを用いてcreateコマンドを復号
createコマンドの実行
S1306

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/07250

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F17/60, G06K17/00, G06K19/10, G06F15/00, G09C1/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F17/60, G06K17/00, G06K19/10, G06F15/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2001-84177 A (Matsushita Electric Industrial Co., Ltd.), 30 March, 2001 (30.03.01), All pages; all drawings (Family: none)	1,3-6,8-10,12 2,7,11
Y A	JP 2002-101087 A (Hitachi, Ltd.), 05 April, 2002 (05.04.02), All pages; all drawings & US 2002/34306 A1	1,3-6,8-10,12 2,7,11
Y	JP 2001-333371 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), All pages; all drawings & WO 01/89210 A1	1,3-6,8-10,12

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
29 August, 2003 (29.08.03)	09 September, 2003 (09.09.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/07250

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2001-243707 A (Sony Corp.), 07 September, 2001 (07.09.01), All pages; all drawings (Family: none)	1,3-6,8-10, 12 2,7,11
A	"TRONWARE VOL.73", Personal Media Corp., 10 February, 2002 (10.02.02), Vol.13, No.1, whole No. 73, pages 48 to 56	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０７２５０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl[7]　G06F12/14, G06F17/60, G06K17/00,
G06K19/10, G06F15/00, G09C1/00

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl[7]　G06F12/14, G06F17/60, G06K17/00,
G06K19/10, G06F15/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926 - 1996
日本国公開実用新案公報　1971 - 2003
日本国登録実用新案公報　1994 - 2003
日本国実用新案登録公報　1996 - 2003

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2001-84177 A (松下電器産業株式会社) 2001.03.30, 全頁, 全図 (ファミリーなし)	1,3-6, 8-10,12
A		2,7,11
Y	JP 2002-101087 A (株式会社日立製作所) 2002.04.05, 全頁, 全図 & US 2002/34306 A1	1,3-6, 8-10,12
A		2,7,11

☒ 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　29.08.03

国際調査報告の発送日　09.09.03

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　奥村　元宏　５Ｎ　３０４４

電話番号　０３－３５８１－１１０１　内線　３５８５

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／０７２５０

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-333371 A (松下電器産業株式会社) 2001.11.30, 全頁, 全図 & WO 01/89210 A1	1,3-6, 8-10,12
A		2,7,11
Y	JP 2001-243707 A (ソニー株式会社) 2001.09.07, 全頁, 全図 (ファミリーなし)	1,3-6, 8-10,12
A		2,7,11
A	"TRONWARE VOL.73", パーソナルメディア株式会社, 2002.02.10, 第13巻, 第1号, 通巻73号, pp.48-56	1-12