(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 17/00 (2006.01)
G11B 20/00 (2006.01)

(11) 공개번호 10-2006-0130645
(43) 공개일자 2006년12월19일

(21) 출원번호 10-2006-7015723
(22) 출원일자 2006년08월03일
심사청구일자 없음
번역문 제출일자 2006년08월03일
(86) 국제출원번호 PCT/JP2005/000497
국제출원일자 2005년01월17일
(87) 국제공개번호 WO 2005/076142
국제공개일자 2005년08월18일

(30) 우선권주장 JP-P-2004-00027940 2004년02월04일 일본(JP)

(71) 출원인 소니 가부시키가이샤
일본국 도쿄도 시나가와구 기타시나가와 6쵸메 7반 35고

(72) 발명자 아사노 토모유키
일본국 141-0001 토쿄-토 시나가와-쿠 키타시나가와 6-쵸메 7-35소니 가부시키가이샤 내

(74) 대리인 문경진
김학수

전체 청구항 수 : 총 22 항

(54) 서비스 제공 서버, 정보 처리 장치 및 데이터 처리 방법과컴퓨터·프로그램

(57) 요약

정보 기록 매체에 격납(格納; store, storage)한 컨텐츠에 대응한 서비스의 제공을 정당한(正當; authentic) 정보 기록 매체를 가지는 디바이스에 대해서만 실행하는 것을 가능하게 한 장치, 방법을 제공한다.

정보 기록 매체에 컨텐츠를 격납해서 제공하고, 또 네트워크 접속한 서비스 제공 서버로부터의 서비스 제공 처리를 행하는 구성에 있어서, 서비스 제공 서버가 유저 디바이스로부터 송신(送信)되는 정보 기록 매체 ID를 검증(檢證)하고, 정보 기록 매체 ID마다의 서비스 제공 상황 데이터에 의거해서 서비스 제공 가부(可否)를 판정해서 서비스 제공을 행한다. 서비스 요구를 송신한 정보 처리 장치가 정당한 정보 기록 매체 ID를 정보 기록 매체로부터 판독(讀取; read)한 정보 처리 장치이며, 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용되어 있는 경우에 한해서, 서비스를 제공한다.

대표도

도 17

특허청구의 범위

청구항 1.

정보 처리 장치로부터의 서비스 제공 요구에 따른 서비스 제공 처리를 실행하는 서비스 제공 서버이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신(受信)하는 데이터 수신부와,

정보 기록 매체의 격납(格納; store, storage) 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다(固有値每)의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부와,

상기 데이터 수신부를 거쳐서 수신한 정보 기록 매체 ID의 검증(檢證; verifying) 처리를 실행하고, 정당성(正當性; validity)이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득해서, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정(特定)되는 서비스의 제공 가부(可否)를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리부

를 가지는 것을 특징으로 하는 서비스 제공 서버.

청구항 2.

제1항에 있어서,

상기 데이터 처리부는,

정보 기록 매체 ID의 검증 처리를 정보 기록 매체 ID에 포함되는 서명(署名) 데이터의 검증 처리로서 실행하고, 정보 기록 매체 ID에 포함되는 타이틀 고유값, 또는 정보 기록 매체 ID에 포함되는 데이터에 의거하는 연산을 실행해서 산출한 타이틀 고유값에 따라서, 타이틀 고유값 대응의 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 하는 서비스 제공 서버.

청구항 3.

제1항에 있어서,

상기 서비스 제공 서버는, 부정(不正; unauthorized)한 정보 기록 매체 ID의 리스트인 리보케이션 리스트(revocation list)를 격납한 기억부를 가지고,

상기 데이터 처리부에서의 정보 기록 매체 ID의 검증 처리는,

정보 처리 장치로부터 수신한 정보 기록 매체 ID와, 상기 리보케이션 리스트에 기록된 ID와의 대조확인(照合; comparing) 처리로서 실행하는 것을 특징으로 하는 서비스 제공 서버.

청구항 4.

제1항에 있어서,

상기 정보 기록 매체 ID는,

정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠(秘密鍵; secret key)에 의거해서 생성된 정보 기록 매체마다 다른(異) 서명 데이터를 포함하고,

상기 데이터 처리부는,

상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 하는 서비스 제공 서버.

청구항 5.

제1항에 있어서,

상기 정보 기록 매체 ID는,

제조된 정보 기록 매체의 매수(枚數)(W)에 대응해서 설정되는 소수(素數; prime) p(w)와,

소수 p(w)와, 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고,

상기 데이터 처리부는, 상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 데이터 IDKey(w)로부터 타이틀 고유값을 산출하고, 산출한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 하는 서비스 제공 서버.

청구항 6.

서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 정보 처리 장치이며,

정보 기록 매체의 액세스 처리를 실행하는 기록 매체 인터페이스와,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독(讀取; read)된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신(送信) 처리를 실행하는 데이터 처리부

를 가지는 것을 특징으로 하는 정보 처리 장치.

청구항 7.

제6항에 있어서,

상기 데이터 처리부는,

정보 기록 매체 ID의 검증 처리를, 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하는 구성인 것을 특징으로 하는 정보 처리 장치.

청구항 8.

제6항에 있어서,

상기 데이터 처리부에서의 정보 기록 매체 ID의 검증 처리는,

부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트를 기억부 또는 정보 기록 매체로부터 취득하고, 취득한 리보케이션 리스트에 기록된 ID와, 정보 처리 장치로부터 수신한 정보 기록 매체 ID와의 대조확인 처리로서 실행하는 구성인 것을 특징으로 하는 정보 처리 장치.

청구항 9.

제6항에 있어서,

상기 정보 기록 매체 ID는,

정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고,

상기 데이터 처리부는,

상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행하는 구성인 것을 특징으로 하는 정보 처리 장치.

청구항 10.

제6항에 있어서,

상기 정보 기록 매체 ID는,

제조된 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수 p(w)와,

소수 p(w)와, 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고,

상기 데이터 처리부는,

상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행하는 구성인 것을 특징으로 하는 정보 처리 장치.

청구항 11.

정보 처리 장치로부터의 서비스 제공 요구에 따른 처리를 실행하는 데이터 처리 방법이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신하는 데이터 수신 스텝과,

수신한 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부로부터, 취득한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 취득해서, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정되는 서비스의 제공 가부를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 데이터 처리 방법.

청구항 12.

제11항에 있어서,

상기 데이터 처리 스텝은,

정보 기록 매체 ID의 검증 처리를 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하고, 정보 기록 매체 ID에 포함되는 타이틀 고유값, 또는 정보 기록 매체 ID에 포함되는 데이터에 의거하는 연산을 실행해서 산출한 타이틀 고유값에 따라서, 타이틀 고유값 대응의 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 13.

제11항에 있어서,

상기 데이터 처리 스텝에서의 정보 기록 매체 ID의 검증 처리는,

정보 처리 장치로부터 수신한 정보 기록 매체 ID와, 부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트에 기록된 ID와의 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 14.

제11항에 있어서,

상기 정보 기록 매체 ID는,

정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고,

상기 데이터 처리 스텝은,

상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 15.

제11항에 있어서,

상기 정보 기록 매체 ID는,

제조된 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수 p(w)와,

소수 p(w)와, 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고,

상기 데이터 처리 스텝은,

상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 데이터 IDKey(w)로부터 타이틀 고유값을 산출하고, 산출한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 16.

서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 데이터 처리 방법이며,

기록 매체 인터페이스를 거쳐서 정보 기록 매체의 액세스 처리를 실행하는 정보 기록 매체 액세스 스텝과,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 데이터 처리 방법.

청구항 17.

제16항에 있어서,

상기 데이터 처리 스텝은,

정보 기록 매체 ID의 검증 처리를, 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하는 것을 특징으로 하는 데이터 처리 방법.

청구항 18.

제16항에 있어서,

상기 데이터 처리 스텝에서의 정보 기록 매체 ID의 검증 처리는,

부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트를 기억부 또는 정보 기록 매체로부터 취득하고, 취득한 리보케이션 리스트에 기록된 ID와, 정보 처리 장치로부터 수신한 정보 기록 매체 ID와의 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 19.

제16항에 있어서,

상기 정보 기록 매체 ID는,

정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고,

상기 데이터 처리 스텝은,

상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 20.

제16항에 있어서,

상기 정보 기록 매체 ID는,

제조된 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수 p(w)와,

소수 p(w)와, 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고,

상기 데이터 처리 스텝은,

상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행하는 스텝을 포함하는 것을 특징으로 하는 데이터 처리 방법.

청구항 21.

정보 처리 장치로부터의 서비스 제공 요구에 따른 처리를 실행하는 컴퓨터·프로그램이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신하는 데이터 수신 스텝과,

수신한 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부로부터, 취득한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 취득해서, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정되는 서비스의 제공 가부를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 컴퓨터·프로그램.

청구항 22.

서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 컴퓨터·프로그램이며,

기록 매체 인터페이스를 거쳐서 정보 기록 매체의 액세스 처리를 실행하는 정보 기록 매체 액세스 스텝과,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 컴퓨터·프로그램.

명세서

기술분야

본 발명은 서비스 제공 서버, 정보 처리 장치 및 데이터 처리 방법과 컴퓨터·프로그램에 관한 것이다. 상세하게는, 컨텐츠를 격납(格納; store, storage)한 디스크 등의 정보 기록 매체의 재생 처리를 실행하는 유저 디바이스에 대해서, 컨텐츠에 관한 서비스의 제공을 실현하는 서비스 제공 서버, 정보 처리 장치 및 데이터 처리 방법과 컴퓨터·프로그램에 관한 것이다.

배경기술

음악 등의 오디오 데이터, 영화 등의 화상 데이터, 게임 프로그램, 각종 어플리케이션 프로그램 등, 여러가지 소프트웨어 데이터(이하, 이들을 컨텐츠(Content)라고 부른다)는 기록 미디어, 예를 들면 DVD(Digital Versatile Disc), MD(Mini

Disc), CD(Compact Disc), 혹은 청색 레이저를 이용한 고밀도 기록 가능한 디스크[청색 광디스크(Blu-ray Disc)] 등의 정보 기록 매체에 격납되어 유저에게 제공되고, 유저는 PC(Personal Computer), 디스크 플레이어 등의 유저 디바이스, 즉 재생 장치에서 컨텐츠를 재생하여 이용할 수가 있다.

또, 근년(近年; recent years)에, 디스크 등의 정보 기록 매체에 격납된 컨텐츠에 관련된 여러가지 서비스를, 유저 디바이스와 네트워크 접속한 서버로부터 제공하는 서비스 제공 구성이 이용되고 있다.

예를 들면, 디스크 격납 컨텐츠가 외국어 영화인 경우의 음성에 대한 자막(字幕; subtitle) 데이터나 더빙(吹替; dubbing) 음성 데이터, 혹은 컨텐츠의 속편(續編; sequel)의 디스크의 구입 할인권 등, 여러가지 컨텐츠 관련 서비스가, 네트워크를 거쳐서 접속한 서버로부터 PC 등의 유저 디바이스에 제공된다.

서버로부터 제공하는 서비스의 형체(形體)는 여러가지이고, 유저의 제한을 만드는(마련하는) 일이 없는 서비스 형태(形態)도 있지만, 예를 들면 서비스 관련 컨텐츠를 기록한 디스크 1매에 대해(1매당) 1번까지 등, 일정한(一定; certain) 조건하에서의 서비스 제공 형태도 있다.

디스크에 격납되는 컨텐츠, 즉 음악 데이터, 화상 데이터 등, 많은 컨텐츠는 일반적으로 그 작성자 혹은 판매자에게 반포권(頒布權) 등이 보유(保有)되고, 이들 컨텐츠의 이용에 대해서는 일정한 이용 제한, 즉 정규한 유저 에 대해서만, 컨텐츠의 이용을 허락하고, 허가가 없는 이용이 행해지지 않도록 하는 구성을 취하는 것이 일반적으로 되어 있다.

따라서, 컨텐츠에 관련해서 제공하는 서비스에 대해서도, 일정한 이용 권한의 확인, 예를 들면 정규 디스크의 구입 유저인 것의 확인 처리 등을 조건으로 해서 서비스 제공을 허용한다고 하는 시스템의 구축이 요망되고 있다.

발명의 상세한 설명

[발명의 개시]

[발명이 해결하고자 하는 과제]

본 발명은 상술한 문제점을 감안해서 이루어진 것이며, DVD, CD, 청색 레이저 기록 매체 등의 각종 정보 기록 매체에 컨텐츠를 격납해서 제공하고, 또 네트워크 접속한 서비스 제공 서버로부터의 서비스 제공 처리를 행하는 구성에 있어서, 정당한(正當; authentic) 서비스 이용 권한을 확인(確認; validating)해서, 부정한(不正; unauthorized) 서비스 이용을 배제(排除)하는 것을 가능하게 하는 서비스 제공 서버, 정보 처리 장치 및 데이터 처리 방법과 컴퓨터·프로그램을 제공하는 것을 목적으로 한다.

[과제를 해결하기 위한 수단]

본 발명의 제1 측면(側面; aspect)은,

정보 처리 장치로부터의 서비스 제공 요구에 따른 서비스 제공 처리를 실행하는 서비스 제공 서버이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신(受信)하는 데이터 수신부와,

정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다(固有値每)의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부와,

상기 데이터 수신부를 거쳐서 수신한 정보 기록 매체 ID의 검증(檢證; verifying) 처리를 실행하고, 정당성(正當性; validity)이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하고, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정되는 서비스의 제공 가부(可否)를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리부

를 가지는 것을 특징으로 하는 서비스 제공 서버에 있다.

또, 본 발명의 서비스 제공 서버의 1실시 형태(實施態樣; embodiment)에 있어서, 상기 데이터 처리부는, 정보 기록 매체 ID의 검증 처리를 정보 기록 매체 ID에 포함되는 서명(署名; signature) 데이터의 검증 처리로서 실행하고, 정보 기록 매체 ID에 포함되는 타이틀 고유값, 또는 정보 기록 매체 ID에 포함되는 데이터에 의거하는 연산을 실행해서 산출한 타이틀 고유값에 따라서, 타이틀 고유값 대응의 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 서비스 제공 서버의 1실시 형태에 있어서, 상기 서비스 제공 서버는, 부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트(revocation list)를 격납한 기억부를 가지고, 상기 데이터 처리부에서의 정보 기록 매체 ID의 검증 처리는, 정보 처리 장치로부터 수신한 정보 기록 매체 ID와, 상기 리보케이션 리스트에 기록된 ID와의 대조확인(照合; comparing) 처리로서 실행하는 것을 특징으로 한다.

또, 본 발명의 서비스 제공 서버의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠(秘密鍵; secret key)에 의거해서 생성된 정보 기록 매체마다 다른(異) 서명 데이터를 포함하고, 상기 데이터 처리부는, 상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠(公開鍵; public key)를 적용한 메시지 생성 및 대조확인 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 서비스 제공 서버의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 제조된 정보 기록 매체의 매수(枚數)(W)에 대응해서 설정되는 소수(素數; prime) p(w)와, 소수 p(w)와 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고, 상기 데이터 처리부는, 상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 데이터 IDKey(w)로부터 타이틀 고유값을 산출하고, 산출한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 제2 측면은,

서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 정보 처리 장치이며,

정보 기록 매체의 액세스 처리를 실행하는 기록 매체 인터페이스와,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독(讀取; read)된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신(送信) 처리를 실행하는 데이터 처리부

를 가지는 것을 특징으로 하는 정보 처리 장치에 있다.

또, 본 발명의 정보 처리 장치의 1실시 형태에 있어서, 상기 데이터 처리부는, 정보 기록 매체 ID의 검증 처리를, 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 정보 처리 장치의 1실시 형태에 있어서, 상기 데이터 처리부에서의 정보 기록 매체 ID의 검증 처리는, 부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트를 기억부 또는 정보 기록 매체로부터 취득하고, 취득한 리보케이션 리스트에 기록된 ID와 정보 처리 장치로부터 수신한 정보 기록 매체 ID와의 대조확인 처리로서 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 정보 처리 장치의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고, 상기 데이터 처리부는, 상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 정보 처리 장치의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 제조된 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수 p(w)와, 소수 p(w)와 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고, 상기 데이터 처리부는, 상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행하는 구성인 것을 특징으로 한다.

또, 본 발명의 제3 측면은, 정보 처리 장치로부터의 서비스 제공 요구에 따른 처리를 실행하는 데이터 처리 방법이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신하는 데이터 수신 스텝과,

수신한 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부로부터, 취득한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 취득하고, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정되는 서비스의 제공 가부를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 데이터 처리 방법에 있다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 데이터 처리 스텝은, 정보 기록 매체 ID의 검증 처리를 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하고, 정보 기록 매체 ID에 포함되는 타이틀 고유값, 또는 정보 기록 매체 ID에 포함되는 데이터에 의거하는 연산을 실행해서 산출한 타이틀 고유값에 따라서, 타이틀 고유값 대응의 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 데이터 처리 스텝에 있어서의 정보 기록 매체 ID의 검증 처리는, 정보 처리 장치로부터 수신한 정보 기록 매체 ID와, 부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트에 기록된 ID와의 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고, 상기 데이터 처리 스텝은, 상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 제조된 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수 p(w)와, 소수 p(w)와 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고, 상기 데이터 처리 스텝은, 상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행함과 동시에, 정보 기록 매체 ID에 포함되는 데이터 IDKey(w)로부터 타이틀 고유값을 산출하고, 산출한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 상기 기억부로부터 취득하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 제4 측면은, 서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 데이터 처리 방법이며,

기록 매체 인터페이스를 거쳐서 정보 기록 매체의 액세스 처리를 실행하는 정보 기록 매체 액세스 스텝과,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 데이터 처리 방법에 있다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 데이터 처리 스텝은, 정보 기록 매체 ID의 검증 처리를, 정보 기록 매체 ID에 포함되는 서명 데이터의 검증 처리로서 실행하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 데이터 처리 스텝에서의 정보 기록 매체 ID의 검증 처리는, 부정한 정보 기록 매체 ID의 리스트인 리보케이션 리스트를 기억부 또는 정보 기록 매체로부터 취득하고, 취득한 리보케이션 리스트에 기록된 ID와, 정보 처리 장치로부터 수신한 정보 기록 매체 ID와의 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값과, 관리 장치의 비밀열쇠에 의거해서 생성된 정보 기록 매체마다 다른 서명 데이터를 포함하고,

상기 데이터 처리 스텝은, 상기 정보 기록 매체 ID의 검증 처리를, 상기 정보 기록 매체 ID에 포함되는 서명 데이터에 대한 상기 관리 장치의 공개 열쇠를 적용한 메시지 생성 및 대조확인 처리로서 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 데이터 처리 방법의 1실시 형태에 있어서, 상기 정보 기록 매체 ID는, 제조된 정보 기록 매체의 매수(w)에 대응해서 설정되는 소수 p(w)와, 소수 p(w)와 타이틀 고유값에 의거하는 연산에 의해서 산출되는 데이터 IDKey(w)를 포함하고, 상기 데이터 처리 스텝은, 상기 정보 기록 매체 ID에 포함되는 데이터가 소수인지 여부를 판정하는 처리를 ID 검증 처리로서 실행하는 스텝을 포함하는 것을 특징으로 한다.

또, 본 발명의 제5 측면은, 정보 처리 장치로부터의 서비스 제공 요구에 따른 처리를 실행하는 컴퓨터·프로그램이며,

정보 처리 장치로부터의 정보 기록 매체 ID 및 서비스 ID를 수반하는 서비스 요구를 수신하는 데이터 수신 스텝과,

수신한 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID에 의거해서 타이틀 고유값을 취득하고, 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 타이틀 고유값 마다의 서비스 관리 데이터로서 상기 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터를 격납한 기억부로부터, 취득한 타이틀 고유값에 대응하는 서비스 제공 상황 데이터를 취득하고, 상기 정보 기록 매체 ID 및 상기 서비스 ID에 의해서 특정되는 서비스의 제공 가부를 판정하고, 제공 가능하다는 판정을 조건으로 한 서비스 제공 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 컴퓨터·프로그램에 있다.

또, 본 발명의 제6 측면은, 서비스 제공 서버에 대한 서비스 제공 요구를 실행하는 컴퓨터·프로그램이며,

기록 매체 인터페이스를 거쳐서 정보 기록 매체의 액세스 처리를 실행하는 정보 기록 매체 액세스 스텝과,

상기 기록 매체 인터페이스를 거쳐서 정보 기록 매체로부터 판독된 정보 기록 매체 ID의 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로 해서, 그 정보 기록 매체 ID의 서비스 제공 서버에 대한 송신 처리를 실행하는 데이터 처리 스텝

을 가지는 것을 특징으로 하는 컴퓨터·프로그램에 있다.

또한, 본 발명의 컴퓨터·프로그램은, 예를 들면 여러가지 프로그램·코드를 실행 가능한 컴퓨터·시스템에 대해서, 컴퓨터 판독가능한(可讀; readable) 형식으로 제공하는 기억 매체, 통신 매체, 예를 들면 CD나 FD, MO 등의 기록 매체, 혹은 네트워크 등의 통신 매체에 의해서 제공 가능한 컴퓨터·프로그램이다. 이와 같은 프로그램을 컴퓨터 판독가능한 형식으로 제공하는 것에 의해, 컴퓨터·시스템 상(上)에서 프로그램에 따른 처리가 실현된다.

본 발명의 또 다른 목적, 특징이나 이점은, 후술하는 본 발명의 실시예나 첨부하는 도면에 의거하는 보다 상세한 설명에 의해서 명확하게 될 것이다. 또한, 본 명세서에서 시스템이라 함은, 복수의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 하우징(筐體; housing, enclosure) 내에 있는 것에는 한정되지 않는다.

[발명의 효과]

본 발명의 구성에 의하면, DVD, CD, 청색 레이저 기록 매체 등의 각종 정보 기록 매체에 컨텐츠를 격납해서 제공하고, 또 네트워크 접속한 서비스 제공 서버로부터의 서비스 제공 처리를 행하는 구성에 있어서, 서비스 제공 서버 측에서, 정보 처리 장치(유저 디바이스)로부터 송신되는 정보 기록 매체 ID를 검증하고, 정보 기록 매체 ID 마다의 서비스 제공 상황 데이

터에 의거하는 서비스 제공을 행하는 구성으로 했으므로, 서비스 요구를 송신한 정보 처리 장치가 정당한 정보 기록 매체 ID를 정보 기록 매체로부터 판독한 정보 처리 장치이며, 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용되고 있는 서비스인 것이 확인된 경우에 한(限)해서, 서비스의 제공이 실행된다.

또, 본 발명의 구성에 의하면, 정보 기록 매체에 격납된 정보 기록 매체 ID는, 관리 장치의 서명 데이터 등의 정당성을 확인 가능한 데이터를 포함하고, 또 타이틀 고유값을 가지거나 혹은 산출 가능한 데이터를 포함하는 구성으로 했으므로, 서비스 제공 서버에서는, 정보 기록 매체 ID에 포함되는 데이터에 의거하는 정당성의 확인이 가능하고, 또 타이틀 고유값을 취득하는 것이 가능해지고, 타이틀 고유값에 대응지어서 설정된 서비스 제공 상황 데이터의 특정을 행하는 것이 가능해진다.

실시예

[발명을 실시하기 위한 최량의 형태]

이하, 도면을 참조하면서 본 발명의 서비스 제공 서버, 정보 처리 장치 및 데이터 처리 방법과 컴퓨터·프로그램의 상세(詳細)에 대해서 설명한다. 또한, 설명은 이하의 항목에 따라서 행한다.

1. 정보 기록 매체의 격납 데이터

2. 컨텐츠 격납 정보 기록 매체의 제공 및 이용 관리 구성

3. 서비스 제공 서버 및 유저 디바이스를 구성하는 정보 처리 장치의 구성

4. 유저 디바이스에서의 처리의 상세

5. 서비스 제공 서버에서의 처리의 상세

[1. 정보 기록 매체의 격납 데이터]

도 1에 정보 기록 매체의 데이터 기록 구성예를 도시한다. 도 1은 CD(Compact Disc), DVD(Digital Versatile Disc), MD(Mini Disc), 청색 광디스크(Blu-ray Disc), 플래시 메모리 등, 각종 정보 기록 매체(100)의 격납 데이터에 대해서 설명하는 도면이다. 도 1에는 디스크 모양(狀)의 매체를 예로서 도시하고 있지만, 본 발명은 디스크 모양의 매체에 한정되지 않고, 플래시 메모리 등의 각종 정보 기록 매체에 있어서 적용 가능하다.

정보 기록 매체(100)에는, 도 1에 도시하는 정보, 즉 디스크 ID(101), 컨텐츠(102), 디스크 ID 리보케이션 리스트(DIRL: Disc ID Revocation List)(103), 암호 열쇠 정보(EKE: Enabling Key Block)(104)가 격납되어 있다.

디스크 ID(101)는 예를 들면 디스크 고유의 식별자(識別子; identifier)이며, 소거(消去; erase)나 개서(書換; rewrite)가 곤란하도록 격납된다. 또한, 본 발명에서, 디스크 ID(101)는 정보 기록 매체(100)에 격납되는 컨텐츠(102)에 대응하는 타이틀 마다 고유의 값(타이틀 고유값)과, 정보 기록 매체(100) 마다 고유의 값(디스크 고유값)과, 그 정당성을 나타내는 정보, 예를 들면 서명 등의 정보(정당성 검증값) 등에 의해 구성된다. 디스크 ID의 상세에 대해서는, 후술(後述)한다.

또한, 이하에 설명하는 실시예에서는, 디스크 모양의 매체를 컨텐츠 격납 정보 기록 매체의 예로서 나타내고 있으므로, 그 식별자를 디스크 ID 로서 설명한다. 플래시 메모리 등의 각종 정보 기록 매체를 컨텐츠 격납 정보 기록 매체로서 이용한 경우에는 디스크 ID에 대응하는 정보 기록 매체 ID가 설정된다.

정보 기록 매체(100)에는 또, 컨텐츠(102)가 격납된다. 컨텐츠는 예를 들면 암호화 컨텐츠로서 격납된다. 암호화 컨텐츠로 한 경우에는, 컨텐츠를 복호(復號; decrypt)하기 위한 열쇠 정보가, 정보 기록 매체(100)에 격납되거나, 혹은 네트워크를 거쳐서 제공된다.

정보 기록 매체(100)에는 또, 디스크 ID 리보케이션 리스트 (DIRL: Disc ID Revocation List)(103)가 격납된다. 디스크 ID 리보케이션 리스트(DIRL: Disc ID Revocation List)(103)는 부정 카피 등이 행해졌다고 인정된 디스크, 예를 들면 시장(市場)에 부정한 카피 컨텐츠를 격납한 CD-R이 발견된 경우에, 그 부정 CD-R에 컨텐츠와 함께 카피된 디스크 ID를 추출

(抽出; extract)해서, 리스트화(化)한 데이터이다. 디스크 ID 리보케이션 리스트(DIRL: Disc ID Revocation List)(103)의 생성, 관리, 디스크 제조자에 대한 리스트 정보의 제공 등은, 특정의 신뢰되는 관리국(管理局)(CA: Central Authority)이 실행한다.

디스크 ID 리보케이션 리스트(DIRL: Disc ID Revocation List)의 데이터 구성에 대해서, 도 2를 참조해서 설명한다. 디스크 ID 리보케이션 리스트(DIRL: Disc ID Revocation List)(150)는 도 2에 도시하는 바와 같이, 리스트(DIRL: Disc ID Revocation List)가 작성된 시기(時期)에 따라 단조 증가(單調增加; monotonously increase)하는 버전 번호(151)와, 배제해야 할 디스크의 디스크 ID를 나열(羅列)한 리보크 디스크(revoked disc) ID 리스트(152)와, 버전 번호(151)와 리보크 디스크 ID 리스트(152)에 대한 개찬(改竄; tampering) 검증값(153)으로서의 인증자(認證子; authenticator)가 포함된다. 개찬 검증값(153) 은 대상(對象)으로 되는 데이터, 이 경우에는 버전 번호(151)와 리보크 디스크 ID 리스트(152)가 개찬되어 있는지 여부를 판별하기 위해서 적용하는 데이터이며, 공개 열쇠 암호 기술(暗號技術; encryption technique)을 이용한 디지털 서명이나, 공통열쇠 암호 기술을 이용한 메시지 인증 코드(MAC: Message Authentication Code)가 적용된다.

개찬 검증값(153)으로서 공개 열쇠 암호 기술을 이용한 디지털 서명을 이용할 때에는, 신뢰할 수 있는 기관, 예를 들면 상술한 관리국(CA: Central Authority)의 서명 검증 열쇠(공개 열쇠)를 재생기(再生機; playback machine)가 취득하고, 관리국(CA: Central Authority)의 서명 생성 열쇠(비밀 열쇠)를 이용해서 만들어진 서명을 각 재생기가 취득한 서명 검증 열쇠(공개 열쇠)에 의해서 검증함으로써, 버전 번호(151)와 리보크 디스크 ID 리스트(152)가 개찬되어 있는지 여부를 판별한다.

개찬 검증값(153)으로서 메시지 인증 코드(MAC: Message Authentication Code)를 이용했을 때의 MAC 생성, 검증 처리에 대해서, 도 3을 참조해서 설명한다. 메시지 인증 코드(MAC: Message Authentication Code)는 데이터의 개찬 검증용의 데이터로서 생성되는 것이며, MAC 생성 처리, 검증 처리 형태(態樣; mode)에는 여러가지 형태가 가능하지만, 1예로서 DES 암호 처리 구성을 이용한 MAC값 생성예를 도 3에 도시한다.

도 3에 도시하는 바와 같이, 대상으로 되는 메시지, 이 경우에는, 도 2에 도시하는 버전 번호(151)와 리보크 디스크 ID 리스트(152)를 8바이트 단위로 분할하고, (이하, 분할된 메시지를 M1, M2, … , MN이라고 한다), 우선, 초기값(Initial Value(이하, IV라고 한다))과 M1을 배타적 논리합(排他的論理和; XOR)한다(그 결과를 I1이라고 한다). 다음에, I1을 DES 암호화부에 입력(入; input)하고, 열쇠(이하, K1이라고 한다)를 이용해서 암호화한다(출력을 E1이라고 한다). 계속해서, E1 및 M2를 배타적 논리합하고, 그 출력 I2를 DES 암호화부에 입력하고, 열쇠 K1을 이용해서 암호화한다(출력 E2). 이하, 이것을 되풀이(繰返)하고, 모든 메시지에 대해서 암호화 처리를 행한다. 최후(最後)에 출력(出; output)되어 온 EN이 메시지 인증 부호(MAC (Message Authentication Code))로 된다.

MAC값은 그 생성원(生成元; generator) 데이터가 변경되면, 다른 값으로 되고, 검증 대상의 데이터(메시지)에 의거해서 생성한 MAC와, 기록되어 있는 MAC와의 비교를 행하고, 일치하고 있으면, 검증 대상의 데이터(메시지)는 변경, 개찬이 이루어져 있지 않는 것이 증명된다.

도 1로 되돌아가서, 정보 기록 매체(100)의 격납 데이터에 대한 설명을 계속한다. 정보 기록 매체(100)에는 또, 암호 열쇠 정보(EKB : Enabling Key Block)(104)가 격납되어 있다.

암호 열쇠 정보 (EKB)를 이용한 비밀 정보 제공 구성에 대해서, 도면을 참조해서 설명한다. 도 4의 최하단에 나타내는 넘버(number) 0～15가, 예를 들면 컨텐츠 이용을 행하는 정보 처리 장치로서의 유저 디바이스이다. 즉, 도 4에 도시하는 계층형 나무 구조(階層型木構造; hierarchical tree structure)의 각 잎(리프: leaf)이 각각의 디바이스에 상당한다.

각 디바이스 0～15는 제조시 혹은 출하시(出荷時), 혹은 그 후에 있어서, 계층형 트리(나무) 구조에서의 자신(自分; its own)의 리프로부터 루트(root)에 이를 때까지의 노드에 할당된 열쇠(노드 키 및 각 리프의 리프 키로 이루어지는 키 세트(디바이스 키(DNK: Device Node Key))를 메모리에 격납한다. 도 4의 최하단에 나타내는 K0000～K1111이 각 디바이스 0～15에 각각 할당된 리프 키이며, 최상단의 KR(루트 키)로부터, 최하단에서 2번째의 마디(節)(노드)에 기재된 키: KR～K111을 노드 키로 한다.

도 4에 도시하는 나무 구조에서, 예를 들면 디바이스 0은 리프 키 K0000과, 노드 키 : K000, K00, K0, KR을 디바이스 키로서 소유(所有)한다. 디바이스 5는 K0101, K010, K01, K0, KR을 소유한다. 디바이스 15는 K1111, K111, K11, K1, KR을 소유한다. 또한, 도 4의 트리에는 디바이스가 0～15의 16개만 기재되고, 트리 구조도 4단(段) 구성의 균형이 잡힌 좌우 대칭 구성으로서 도시하고 있지만, 더 많은 디바이스가 트리 중에 구성되고, 또 트리의 각 부에서 다른(異) 단수 구성을 가지는 것이 가능하다.

또, 도 4의 트리 구조에 포함되는 각 디바이스에는 여러가지 기록 매체, 예를 들면 디바이스 매립형(埋入型; embeded) 혹은 디바이스에 착탈 자유롭게(着脫自在; releasable) 구성된 DVD, CD, MD, 플래시 메모리 등을 사용하는 여러가지 타입의 디바이스가 포함되어 있다. 또, 여러가지 어플리케이션 서비스가 공존(共存; coexist) 가능하다. 이와 같은 다른 디바이스, 다른 어플리케이션의 공존 구성 상에 도 4에 도시하는 컨텐츠 혹은 열쇠 배포 구성인 계층형 트리 구조가 적용된다.

이들 여러가지 디바이스, 어플리케이션이 공존하는 시스템에서, 예를 들면 도 4의 점선으로 둘러싼 부분, 즉 디바이스 0, 1, 2, 3을 하나의 그룹으로서 설정한다. 예를 들면, 이 점선으로 둘러싼 그룹 내에 포함되는 디바이스만이 정보 기록 매체에 격납한 암호화 컨텐츠의 정당한 이용권, 즉 라이센스(licenses)를 보유한다. 이 경우, 디바이스 0, 1, 2, 3만이 컨텐츠 복호에 적용하는 열쇠의 취득을 가능하게 한 EKB를 설정해서, 암호화 컨텐츠를 격납한 정보 기록 매체에 격납하게 된다.

도 4로부터 명확한 바와 같이, 하나의 그룹에 포함되는 세개의 디바이스 0, 1, 2, 3은 각각의 디바이스에 격납한 디바이스 키(DNK : Device Node Key)로서 공통의 키 K00, K0, KR을 보유하고 있다.

이 때, 디바이스 0, 1, 2만이 컨텐츠의 복호에 적용하는 컨텐츠 키 (Kcon)를 취득 가능하게 한 EKB의 구성은, 예를 들면 도 5에 도시하는 구성으로 된다. 즉, EKB는

인덱스 암호화 키

000 Enc(K000, Kcon)

0010 Enc(K0010, Kcon)으로서 설정된다.

또한, Enc(Kx, Ky)는 데이터 Ky를 열쇠 Kx로 암호화한 암호화 데이터를 의미한다. 이 때, 디바이스 0, 1은 자기(自己)가 보유하는 디바이스 키 [K000]을 이용해서 인덱스 [000]의 암호화 데이터의 복호가 가능하고, 또 디바이스 2는 디바이스 키 [K0010]을 이용해서 상기 EKB 중의 인덱스 [0010]의 암호화 데이터의 복호가 가능하며, 각각의 암호화 데이터의 복호 처리에 의해 컨텐츠 키(Kcon)를 취득할 수가 있다. 그 밖의 디바이스는 디바이스 키 [K000], [K0010]의 어느것도 보유하고 있지 않으며, 도 5에 도시하는 구성을 가지는 EKB를 수령(受領; receive)해도 EKB의 복호에 의한 컨텐츠 키의 취득을 할 수 없다.

이와 같이, EKB는 라이센스를 보유하는 디바이스에 따른 구성 데이터로 함으로써, 임의의 선택된 디바이스에서만 처리 가능하게 해서 컨텐츠 열쇠 등의 비밀 정보를 특정의 디바이스에만 제공 가능하게 한 열쇠 정보 블록으로서 구성된다. 열쇠 정보(EKB) 발행 센터(104)는 컨텐츠의 이용을 허용하는 디바이스에서만 처리 가능한 EKB를 생성하여 정보 기록 매체 제조 엔티티(entity)(103)에 제공한다. 정보 기록 매체 제조 엔티티(103)는 이 EKB를 암호화 컨텐츠와 함께 정보 기록 매체(100)에 격납해서 유저에게 제공한다.

[2. 컨텐츠 격납 정보 기록 매체의 제공 및 이용 관리 구성]

도 6은 상술한 각종 데이터를 격납한 정보 기록 매체(200)의 제공 및 이용 관리 구성을 설명하는 도면이다.

도 6에 도시하는 바와 같이, 컨텐츠 제공 및 관리 구성에서는, 관리국 (CA:Central Authority)이 사용하는 관리 장치(201)와, 컨텐츠 프로바이더(content provider)가 사용하는 컨텐츠 제공 장치(203)와, 디스크 제조자(製造者)가 사용하는 디스크 제조 장치(202)와, 유저가 사용하는 컨텐츠 재생 처리를 행하는 정보 처리 장치(유저 디바이스)(400)와, 정보 처리 장치(유저 디바이스)(400)에 대해서 정보 기록 매체(200)에 격납된 컨텐츠에 대응하는 서비스, 예를 들면 자막 정보의 제공 처리 등을 실행하는 서비스 제공 서버(300)가 존재한다.

관리 장치(201)가, 전술한 디스크 ID와 디스크 ID 리보케이션 리스트 (DIRL)를 생성해서 디스크 제조 장치(202)에 제공한다. 또, 컨텐츠 제공 장치(203)가, 암호화 컨텐츠와 유효화 열쇠 블록(EKB)을 디스크 제조 장치(202)에 제공한다.

디스크 제조 장치(202)는 관리 장치(201)로부터 받은 디스크 ID 및 디스크 ID 리보케이션 리스트(DIRL)와, 컨텐츠 제공 장치(203)로부터 받은 암호화 컨텐츠 데이터와 유효화 열쇠 블록(EKB)을 기록한 정보 기록 매체(200)를 제조한다.

유저는 정보 기록 매체(200)를 예를 들면 구입하고, 정보 처리 장치(유저 디바이스)(400)에 세트한다. 정보 처리 장치(유저 디바이스)(400)는 정보 기록 매체(200)에 기록된 디스크 ID가 정당하다고 검증하고, 해당(當該) 디스크 ID가 리보케이션 리스트(DIRL) 내에 존재하지 않는 것을 확인하고, 스스로(自)의 디바이스 노드 열쇠 데이터(DNK)에 의거해서 유효화 열쇠 블록(EKB)으로부터 적절한 컨텐츠 열쇠 데이터를 취득하고, 암호화 컨텐츠 데이터를 복호하여, 재생할 수가 있다.

또, 정보 처리 장치(유저 디바이스)(400)는 정보 기록 매체(200)에 기록된 디스크 ID와, 서비스 식별자로서의 서비스 ID를 서비스 제공 서버(300)에 송신하고, 서비스 제공 서버(300)에서, 디스크 ID의 정당성이 검증되며, 또 서비스의 제공 가부를 서비스 제공 서버(300)가 가지는 서비스 제공 상황 데이터에 의거해서 판정하고, 디스크 ID가 정당하고, 서비스 제공 상황 데이터에 의거해서 서비스 제공 가능하다고 판정한 경우에, 정보 처리 장치(유저 디바이스)(400)에 대한 서비스 제공 처리를 실행한다.

[3. 서비스 제공 서버 및 유저 디바이스를 구성하는 정보 처리 장치의 구성]

다음에, 서비스 제공 서버 및 유저 디바이스를 구성하는 정보 처리 장치의 구성에 대해서 설명한다.

도 7은 도 6에 도시하는 서비스 제공 서버의 구성도이다. 도 7에 도시하는 바와 같이, 서비스 제공 서버(300)는 예를 들면 CPU 등에 의해서 구성되는 컨트롤러(302), 각종 연산 처리를 실행하는 연산 유닛(303), 데이터 입력 장치나 데이터 출력 장치에 대한 데이터 입출력, 및 네트워크를 거치는 데이터 입출력용 인터페이스로서의 입출력 인터페이스(I/F)(304), 시큐어 메모리(secure memory)(305), 메인 메모리(306)를 가진다. 이들은 버스(301)를 거쳐서 접속되어 있다.

메인 메모리(306)는 연산 유닛(303) 및 컨트롤러(302)에서의 처리에 이용되는 여러 가지 데이터 중, 시큐러티 레벨(security level)이 낮은 데이터를 기억한다. 시큐어 메모리(305)는 연산 유닛(303) 및 컨트롤러(302)의 처리에 이용되는 여러 가지 데이터 중, 시큐러티 레벨이 높은 데이터를 기억한다. 시큐어 메모리(305)는 예를 들면 도 6에 도시하는 관리 장치(201)로부터 수령하는 디스크 ID 등을 기억한다.

입출력 인터페이스(304)는 예를 들면 도시하지 않은 조작 수단 혹은 네트워크 등에 접속되고, 도 6에 도시하는 관리 장치(201)나, 컨텐츠 제공 장치(203)로부터의 여러가지 데이터의 수령을 행하고, 또 서비스 제공을 받는 정보 처리 장치(유저 디바이스)(400)와의 통신을 실행해서 서비스를 제공한다.

연산 유닛(303)은 컨트롤러(302)로부터의 제어에 의거해서, 서명 데이터의 검증용 데이터의 생성 등, 각종 연산을 실행한다. 컨트롤러(302)는 예를 들면 유저 디바이스에 대한 서비스 제공을 허용해도 좋은지 여부의 확인 처리 프로그램, 서비스 제공 프로그램 등의 각종 프로그램을 실행한다.

서비스 제공 서버(300)는 입출력 인터페이스(I/F)(304)를 거쳐서, 관리 장치(201) 또는 컨텐츠 제공 장치(203) 또는 그 밖의 장치로부터 디스크 ID 리보케이션 리스트를 정기적으로, 또는 이벤트(event)마다 수신하고, 항상 최신판(最新版)을 시큐어 메모리(305)에 격납한다.

또, 입출력 인터페이스(I/F)(304)를 거쳐서, 컨텐츠 제공 장치(203) 또는 그 밖의 장치로부터, 타이틀 마다의 타이틀 고유값과, 제공하는 서비스를 식별하는 서비스 식별 정보를 수신하고, 타이틀 마다의 서비스 제공 상황 정보를 관리한 서비스 제공 상황 데이터 베이스를 시큐어 메모리(305)에 격납한다.

타이틀이라 함은, 정보 처리 장치(유저 디바이스)(400)가 장착(裝着; attach)한 정보 기록 매체(200)에 격납한 컨텐츠에 대응하는 타이틀이다.

서비스 제공 상황 데이터 베이스의 데이터 구성예를 도 8에 도시한다. 서비스 제공 상황 데이터 베이스에는, 도 8에 도시하는 바와 같이, 서비스 제공 서버(300)가 제공하는 서비스 대응의 컨텐츠의 타이틀 식별 정보, 타이틀 고유값마다 설정되어 있고, 그 타이틀의 컨텐츠를 격납한 디스크의 각 디스크 ID에 대한 각 서비스의 제공 상황이 격납된다.

예를 들면, 도 8에 도시하는 서비스 제공 상황 데이터는

타이틀 식별 정보: aaaa

타이틀 고유값: bbbb

에 대한 서비스 제공 상황 데이터이며, 이 타이틀 대응의 컨텐츠에 대응하는 서비스 1과 서비스 2에 대해서, 디스크 ID1과 디스크 ID2의 각각의 디스크에 의거하는 서비스 제공 요구에 대해서 지금까지 몇번 서비스를 제공했는지를 기록하고 있다.

또한, 도 8에 도시하는 서비스 제공 상황 데이터에서,

서비스1은 디스크 ID 하나에 대해(1개당) 1회(回)까지 제공가능한 서비스

서비스2는 디스크 ID 하나에 대해 5회까지, 제공 가능한 서비스

라고 규정된 서비스이다.

서비스 제공 서버(300)는 도 8에 도시하는 서비스 제공 상황 데이터를, 예를 들면 시큐어 메모리(305)에 격납해서 보존유지(保持; hold, keep)하고, 정보 처리 장치(유저 디바이스)(400)로부터의 디스크 ID를 수반하는 서비스 제공 요구에 따라서, 서비스 제공 요구 디바이스가, 정당한 디스크 ID에 의거하는 서비스 요구인지의 확인을 실행하고, 또 도 8에 도시하는 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용 상한(上限)에 도달(達; reach)해 있지 않은 경우에 한해서, 서비스의 제공을 행한다.

서비스 제공 서버(300)는 정보 처리 장치(유저 디바이스)(400)로부터의 디스크 ID를 수반하는 서비스 제공 요구를 수신하면, 정보 처리 장치(유저 디바이스)(400)로부터 송신되는 디스크 ID의 정당성의 확인, 서비스 제공 서버(300)가 보유하는 리보케이션 리스트에서 정보 처리 장치(유저 디바이스)(400)로부터 송신되는 디스크 ID가 리보크되어 있지 않은 것의 확인을 행한다.

또, 정당성이 확인된 디스크 ID에 의거하는 타이틀 고유값의 확인 또는 취출, 디스크 고유값의 취출 등의 처리를 실행한다. 서비스 제공 서버(300)는 취득한 타이틀 고유값에 의거해서, 도 8에 도시하는 서비스 제공 상황 데이터를 격납한 데이터베이스로부터, 대응 타이틀에 대한 서비스 제공 상황 데이터를 특정하고, 그 데이터에 의거해서, 서비스를 제공해도 좋은지를 체크한다. 즉, 도 8에 도시하는 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용 상한에 도달해 있지 않은 경우에 한해서, 서비스의 제공을 행한다.

또한, 도 8에 도시하는 서비스 제공 상황 데이터의 구성예에서는, 디스크 ID 마다 서비스 제공 상황의 데이터를 격납하는 예를 나타내고 있지만, 디스크 ID 대신에, 개개의(個個; individual) 디스크를 식별하기 위한 디스크 고유값을 사용하는 구성으로 해도 좋다.

또한, 서비스 제공 서버(300)가 정보 처리 장치(유저 디바이스)(400)에 대해서, 서비스의 제공을 실행한 경우에는, 도 8에 도시하는 서비스 제공 상황 데이터를 갱신하는 처리를 실행한다.

다음에, 도 9를 참조해서, 정보 처리 장치(유저 디바이스)(400)의 구성에 대해서 설명한다.

도 9에 도시하는 바와 같이, 정보 처리 장치(유저 디바이스)(400)는 예를 들면 입출력 인터페이스(402), MPEG(Moving Picture Experts Group) 등의 각종 부호화(符號化; coded) 데이터의 생성 및 복호(復號; decoding)를 실행하는 코덱(codec)(403), A/D, D/A 컨버터(405)를 구비한 입출력 인터페이스(404), 암호 처리부(406), ROM(Read Only Memory)(407), 컨트롤러(408), 메모리(409) 및, 정보 기록 매체(200)에 액세스하기 위한 기록 매체 인터페이스(410)를 가지고, 이들이 버스(401)에 의해서 상호(相互) 접속되어 있다.

입출력 인터페이스(402)는 네트워크 등, 외부로부터 공급되는 디지털 신호를 수신하고, 버스(401) 상에 출력함과 동시에, 버스(401) 상의 디지털 신호를 수신하여, 외부로 출력한다.

코덱(403)은 버스(401)를 거쳐서 공급되는 예를 들면 MPEG 부호화된 데이터를 디코드하여, 입출력 인터페이스(404)에 출력함과 동시에, 입출력 인터페이스(404)로부터 공급되는 디지털 신호를 인코드(encode)해서 버스(401) 상으로 출력한다.

입출력 인터페이스(404)는 A/D, D/A 컨버터(405)를 내장(內藏; incorporate)하고 있다. 입출력 인터페이스(404)는 외부로부터 공급되는 아날로그 신호를 수신하고, A/D, D/A 컨버터(405)로 A/D(Analog Digital) 변환함으로써, 디지털 신호로서 코덱(403)에 출력함과 동시에, 코덱(403)으로부터의 디지털 신호를 A/D, D/A 컨버터(405)로 D/A(Digital Analog) 변환함으로써, 아날로그 신호로서, 외부에 출력한다.

암호 처리부(406)는 예를 들면 1칩(one-chip)의 LSI로 구성되고, 버스(401)를 거쳐서 공급되는 예를 들면 컨텐츠 등의 디지털 신호를 암호화 또는 복호하고, 버스(401) 상에 출력하는 구성을 가진다. 또한, 암호 처리부(406)는 1칩 LSI에 한정되지 않고, 각종 소프트웨어 또는 하드웨어를 조합(組合; combine)한 구성에 의해서 실현하는 것도 가능하다.

ROM(407)은 예를 들면 유저 디바이스로서의 정보 처리 장치 마다 고유의, 혹은 복수의 정보 처리 장치(유저 디바이스)의 그룹 마다 고유의 디바이스 열쇠 데이터인 리프 열쇠 데이터와, 복수의 재생 장치, 혹은 복수의 그룹에 공유의(共有; shared) 디바이스 열쇠 데이터인 노드 열쇠 데이터를 기억하고 있다. 이들은 전술한 암호 열쇠 정보로서의 유효화 열쇠 블록(EKB)의 복호 처리에 적용된다.

컨트롤러(408)는 예를 들면 메모리(409)에 기억된 프로그램을 실행하는 CPU 등에 의해서 구성된다. 컨트롤러(408)는 정보 처리 장치(유저 디바이스)(400)의 처리를 통괄해서 제어한다. 즉, 정보 처리 장치(유저 디바이스)(400)의 기능(처리)은 컨트롤러(408)가 실행하는 프로그램에 의해서 규정된다.

메모리(409)는 상술한 디스크 ID 리보케이션 리스트(DIRL)를 정보 기록 매체(200)로부터 판독해서 시큐어한(안전한) 상태로 격납한다. 예를 들면 정보 처리 장치(유저 디바이스)(400)에 설정된 ID에 의거하는 암호화를 행해서 메모리에 격납하는 등에 의해 내(耐)탬퍼성(性)(tamper-resistant)을 보존유지한 데이터로서 격납하는 것이 바람직하다. 이와 같이, 디스크 ID 리보케이션 리스트(DIRL)는 외부로부터 지워지거나, 내용이 개찬되거나, 옛날(古; old) 버전의 리스트로 교체(入替; replace)되는 것을 용이하게 실행되지 않도록 격납한다. 기록 매체 인터페이스(410)는 정보 기록 매체(200)에 액세스하기 위해서 이용된다.

[4. 유저 디바이스에서의 처리의 상세]

다음에, 유저 디바이스로서의 정보 처리 장치(400)가, 서비스 제공 서버(300)로부터 서비스를 수령할 때의 처리의 상세에 대해서 설명한다.

도 10은 도 9에 도시하는 정보 처리 장치(유저 디바이스)(400)가 정보 기록 매체를 장착하고, 서비스 제공 서버로부터의 서비스를 수령할 때에 실행하는 시퀀스(sequence)를 설명하는 플로차트이다.

스텝 S101에서, 정보 처리 장치(유저 디바이스)(400)는 소정의 액세스 위치에 정보 기록 매체(200)가 세트되면, 기록 매체 인터페이스(410)를 거쳐서, 정보 기록 매체(200)로부터 디스크 ID를 판독출력(讀出; read)하고, 이것을 메모리(409)에 격납한다.

스텝 S102에서, 정보 처리 장치(유저 디바이스)(400)의 컨트롤러(408)는 메모리(409)에 격납한 디스크 ID를 판독출력해서 그의 개찬 유무 및 정당성을 검증한다. 해당 검증 처리에 대해서는, 나중(後)에 상세하게 설명한다.

스텝 S103에서, 컨트롤러(408)는 스텝 S102에서 상기 디스크 ID가 정당하다고 판정하면 스텝 S105의 처리로 진행하고, 그렇지 않은 경우에는 스텝 S104로 진행하고, 스텝 S104에서, 컨트롤러(408)는 정보 기록 매체(200)에 기록되어 있는 암호화 컨텐츠의 복호 및 재생을 정지(금지)한다.

디스크 ID가 정당하다고 판정한 경우에는, 스텝 S105에서, 컨트롤러(408)는 기록 매체 인터페이스(410)를 거쳐서, 정보 기록 매체(200)로부터 디스크 ID 리보케이션 리스트(DIRL)를 판독출력한다. 그리고, 컨트롤러(408) 는 해당 판독한 리보케이션 리스트의 개찬 검증값으로서 공개 열쇠 암호 기술을 이용한 디지털 서명이 이루어져 있는 경우에는, 서명 검증 열쇠(공개 열쇠)에 의해서 검증한다. 또, 개찬 검증값으로서 메시지 인증 코드(MAC)가 부여되어 있는 경우에는, 앞서 도 3을 참조해서 설명한 MAC 검증 처리가 실행된다.

컨트롤러(408)는 디스크 ID 리보케이션 리스트 (DIRL)에 개찬이 없다고 판정된 것을 조건으로, 해당 디스크 ID 리보케이션 리스트(DIRL)의 버전과, 메모리(409)에 이미 격납되어 있는 디스크 ID 리보케이션 리스트(DIRL)와의 버전 비교를 실행한다.

컨트롤러(408)는 판독출력한 디스크 ID 리보케이션 리스트(DIRL)의 버전이 메모리(409)에 이미 격납되어 있는 디스크 ID 리보케이션 리스트 (DIRL)보다 새로운 경우에는, 판독출력한 디스크 ID 리보케이션 리스트(DIRL)에 의해서, 메모리(409) 내의 리보케이션 리스트(DIRL)를 갱신(更新; update)한다.

스텝 S106에서, 컨트롤러(408)는 스텝 S101에서 판독출력한 디스크 ID가 리보케이션 리스트(DIRL) 내에 존재하는지 여부를 판단하고, 존재한다고 판단하면 스텝 S107로 진행하고, 그렇지 않은 경우에는 스텝 S108로 진행한다. 스텝 S107에서는, 컨트롤러(408)는 정보 기록 매체(200)에 기록되어 있는 암호화 컨텐츠의 복호 및 재생을 정지(금지)한다.

디스크 ID가 리보케이션 리스트 내에 존재하지 않은 경우에는, 스텝 S108로 진행하고, 컨트롤러(408)는 스텝 S101에서 판독출력한 디스크 ID를 서비스 제공 서버에 송신한다. 또, 스텝 S109에서, 서비스 제공 서버로부터의 서비스를 수령한다. 또한, 서비스 제공 서버는 스텝 S108에서, 정보 처리 장치(유저 디바이스)(400)로부터 수령한 디스크 ID의 검증을 실행해서, 정당성이 확인된 경우에만, 서비스의 제공 처리를 실행하게 된다.

이하, 스텝 S102에서 실행하는 디스크 ID의 검증 처리에 대해서 설명한다.

정보 기록 매체에 격납되는 디스크 ID는 위조 곤란성(僞造困難性; counterfeit-resistant)이 높은 식별 정보로서 설정된다. 디스크 ID의 구성예를 도 11에 도시한다.

도 11에는, 정보 기록 매체 식별자로서의 정보 기록 매체 ID(디스크 ID)와, 정보 기록 매체에 격납한 컨텐츠의 타이틀에 대해서 설정되는 고유값인 타이틀 고유값과, 정보 기록 매체의 고유값으로서 설정되는 디스크 고유값과의 대응예로서 6종류의 디스크 ID 설정예를 도시하고 있다. 또한, 디스크 ID, 디스크 고유값은 어느것이나(both) 관리 장치(201)가 생성한다. 타이틀 고유값: M은 정보 기록 매체에 격납한 컨텐츠를 구성하는 일부 정보를 적용해도 좋고, 혹은 관리 장치(201), 컨텐츠 제공 장치(203)가 생성하는 구성으로 해도 좋다. 타이틀 고유값: S는 관리 장치(201)가 타이틀 고유값: M에 의거해서 생성한다.

도 11에 도시하는 각 기호(記號)의 의미는, 이하와 같다.

M: 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 고유값

w:w=1, 2, … W이며, W는 제조하는 정보 기록 매체의 매수(枚數)

Sig(w): 관리 장치의 비밀 열쇠(예를 들면, 공개 열쇠 암호 방식에 의거해서 설정된 비밀 열쇠)에 의거하는 서명 데이터, 제조하는 정보 기록 매체의 매수(W)에 따라서 생성되고, 각 정보 기록 매체마다 다른 서명 데이터로 된다. Sig(w)는 각 디스크의 서명이 Sig(1), Sig(2)…Sig(W)로서 설정되는 것을 의미하고 있다

p(w): 제조하는 정보 기록 매체의 매수(W)에 대응해서 설정되는 소수(素數), 제조하는 정보 기록 매체의 매수(W)에 따라서 생성되는 각 정보 기록 매체마다 다른 소수 데이터로 된다.

S: 정보 기록 매체의 격납 컨텐츠의 타이틀에 대응하는 고유값이며, $S=K^{T}\mathrm{mod}M$, 다만 T는 하기 식에 의해서 산출되는 값

[수학식 1]

$$T = \prod_{w=1}^{W} p_w$$

IDKey(w):$IDKey(w)=K^{T/P(w)}\mathrm{mod}M$

다만, K는 각 타이틀에 대해서 설정되는 값이며, $K \in Z^{*}_{M}$(K는 순회군(巡回群; cyclic group) Z^{*}_{M}의 생성원, 또한 $X \in Z^{*}_{M}$은 X가 1~X-1의 정수(整數; integer) x 중에서 x를 법(法; modulo)으로 해서 역원(逆元; inverse element)을 가지는 집합 요소인 것을 나타낸다)를 만족시키는 값이다.

e(w): $e(w) \in Z^*_M$을 만족시키는 디스크 제조 매수(W)에 대응하는 수(數)의 다른 값

다만, e(w)와 λ(M)은 서로 소(素; disjoint), 즉 e(w)와 λ(M)의 최대공약수(最大公約數)가 1이다. 또한, λ(M)은 소수(q1-1)과 (q2-1)의 최소 공배수(最小公倍數)이다. q1, q2는 RSA 암호에 적용하는데 필요로 되는 정도로 큰 소수이다.

I(w):$I(w)=S^{d(w)} \bmod M$

다만, d(w)는 λ(M)을 법으로 했을 때의 e(w)의 역수(逆數; inverse)이다.

∑w: 데이터 S와, 데이터 e(w)의 연결 데이터인 메시지 M(w)를 관리 장치(CA))(201)의 비밀 열쇠로 암호화한 데이터

이하, 도 11에 도시하는 여섯개의 다른 디스크 ID의 설정예에 대응한 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스를 설명한다.

설정예 1에서의 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스에 대해서, 도 12를 참조해서 설명한다.

설정예 1은

디스크 ID=M, Sig(w)

타이틀 고유값=M

디스크 고유값=Sig(w)

로 한 설정예이다.

정보 처리 장치(유저 디바이스)(400)의 컨트롤러(408)는 스텝 S201에서, 디스크 ID(w) 내의 서명 데이터 SIG(w)를 취출한다. 또한, 디스크 ID는 디스크 제조 매수를 W로 했을 때, w=1, 2…W에 의해서 나타내어지는 개개의 디스크(w)에 따라서 다른 값으로 되므로, 디스크 ID(w)로서 표기(標記)한다.

스텝 S202에서, 컨트롤러(408)는 메모리(409)로부터 판독출력한 관리 장치(201)(관리국(CA))의 공개 열쇠 및 공개된 파라미터를 토대로, 스텝 S201에서 판독출력한 서명 데이터 SIG(w)로부터 메시지 M(w)′를 생성한다. 메시지의 표기도 디스크 ID(w)의 표기와 마찬가지이며, 디스크마다 다른 메시지가 대응지어져 있는 것을 M(w)로 나타내고 있다.

스텝 S203에서, 컨트롤러(408)는 디스크 ID(w) 내에 포함되는 메시지 M(w)와, 스텝 S202에서 생성한 메시지 M(w)′를 비교한다.

스텝 S204에서, 컨트롤러(408)는 스텝 S203의 비교 처리에서 일치하고 있다고 판정하면 스텝 S205로 진행하고, 그렇지 않은 경우에는 스텝 S206으로 진행한다.

스텝 S205에서, 컨트롤러(408)는 스텝 S201에서 취출한 디스크 I D(w)가 정당하다고 판정한다. 스텝 S206에서는, 컨트롤러(408)는 스텝 S201에서 취출한 디스크 ID(w)가 부정하다고 판정한다.

설정예 2는

디스크 ID=S, Sig(w)

타이틀 고유값=S

디스크 고유값=Sig(w)

로 한 설정예이다.

이 설정예 2는 설정예 1에서의 타이틀 고유값 M을 S로 치환(置換)했을 뿐이며, 설정예 1에서의 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스와 마찬가지 시퀀스이며, 스텝 S202에서 서명 데이터로부터 생성하는 데이터가 메시지 S′(w)로 되고, 스텝 S203에서의 비교 데이터가 디스크 ID에 포함되는 데이터 S(w)로 되는 점이 다를 뿐이다.

다음에, 설정예 3에서의 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스에 대해서, 도 13을 참조하여 설명한다.

설정예 3은

디스크 ID=p(w), IDKey(w)

타이틀 고유값=S

디스크 고유값=p(w) 또는 IDKey(w)

로 한 설정예이다.

스텝 S301에서, 정보 처리 장치(유저 디바이스)(400)의 컨트롤러(408)는 정보 기록 매체(200)로부터 판독출력한 디스크 ID(w) 내의 데이터 p(w)를 취출한다.

스텝 S302에서, 컨트롤러(408)는 스텝 S302에서 취출한 데이터 p(w)가 소수인지 여부를 판단한다. 컨트롤러(408)는 데이터 p(w)가 소수라고 판단하면 스텝 S303으로 진행하고, 그렇지 않은 경우에는 스텝 S304로 진행한다.

스텝 S303에서, 컨트롤러(408)는 스텝 S301에서 취출한 디스크 ID(w)가 정당하다고 판정한다. 스텝 S304에서는, 컨트롤러(408)는 스텝 S301에서 취출한 디스크 ID(w)가 부정하다고 판정한다.

다음에, 설정예 4에서의 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스에 대해서, 도 14를 참조하여 설명한다.

설정예 4는

디스크 ID=e(w), I(w)

타이틀 고유값=S

디스크 고유값=e(w) 또는 I(w)

로 한 설정예이다.

스텝 S401에서, 정보 처리 장치(유저 디바이스)(400)는 소정의 액세스 위치에 정보 기록 매체(200)가 세트되면, 기록 매체 인터페이스(410)를 거쳐서, 정보 기록 매체(200)로부터 디스크 ID를 판독출력하고, 이것을 메모리(409)에 격납한다.

스텝 S402에서, 정보 처리 장치(유저 디바이스)(400)의 컨트롤러(408) 는 메모리(409)에 기록한 디스크 ID 내의 데이터 e(w)와 I(w)를 이용해서, $I(w)^{e(w)}$modM을 산출하고, 그 결과를 데이터 S′로 한다. 즉,

$S'=I(w)^{e(w)}$modM

으로 한다.

스텝 S403에서, 컨트롤러(408)는 기록 매체 인터페이스(410)를 거쳐서, 정보 기록 매체(200)로부터 디스크 ID 리보케이션 리스트(DIRL)를 판독출력한다. 컨트롤러(408)는 판독출력한 디스크 ID 리보케이션 리스트(DIRL)의 개찬 검증값으로서 공개 열쇠 암호 기술을 이용한 디지털 서명이 이루어져 있는 경우에는, 서명 검증 열쇠(공개 열쇠)에 의해서 검증한다. 또, 개찬 검증값으로서 메시지 인증 코드(MAC)가 부여되어 있는 경우에는, 앞서 도 3을 참조해서 설명한 MAC 검증 처리가 실행된다.

컨트롤러(408)는 디스크 ID 리보케이션 리스트(DIRL)에 개찬이 없다고 판정된 것을 조건으로, 해당 디스크 ID 리보케이션 리스트(DIRL)의 버전과, 메모리(409)에 이미 격납되어 있는 디스크 ID 리보케이션 리스트(DIRL)와의 버전 비교를 실행한다. 컨트롤러(408)는 해당 판독출력한 디스크 ID 리보케이션 리스트(DIRL)의 버전이 메모리(409)에 이미 격납되어 있는 디스크 ID 리보케이션 리스트(DIRL)보다 새로운 경우에는, 판독출력한 디스크 ID 리보케이션 리스트(DIRL)에 의해서, 메모리(409) 내의 리보케이션 리스트(DIRL)를 갱신한다.

스텝 S404에서, 컨트롤러(408)는 스텝 S401에서 판독출력한 디스크 ID가 리보케이션 리스트 내에 존재하는지 여부를 판단하고, 존재한다고 판단하면 스텝 S405로 진행하고, 그렇지 않은 경우에는 스텝 S406으로 진행한다.

스텝 S405에서는, 컨트롤러(408)는 정보 기록 매체(200)에 기록되어 있는 컨텐츠의 재생을 정지(금지)한다. 스텝 S406에서는, 컨트롤러(408)는 스텝 S401에서 판독출력한 디스크 ID를 서비스 제공 서버에 송신한다. 또, 스텝 S407에서, 서비스 제공 서버로부터의 서비스를 수령한다. 또한, 서비스 제공 서버는 스텝 S406에서, 정보 처리 장치(유저 디바이스)(400)로부터 수령한 디스크 ID의 검증을 실행해서, 정당성이 확인된 경우에만, 서비스의 제공 처리를 실행하게 된다.

다음에, 설정예 5에서의 정보 처리 장치(유저 디바이스)(400)에서의 디스크 ID의 검증 처리 시퀀스에 대해서, 도 15를 참조하여 설명한다.

설정예 5는

디스크 ID=∑w

타이틀 고유값=S

디스크 고유값=e(w)

로 한 설정예이다.

스텝 S501에서, 정보 처리 장치(유저 디바이스)(400)의 컨트롤러(408)는 정보 기록 매체(200)로부터 판독출력한 디스크 ID(w)를, 관리 장치(201)(관리국(CA))의 공개 열쇠 데이터를 토대로 복호해서 메시지 M(w)를 생성한다. 메시지 M(w)는 전술한 바와 같이, 데이터 S와 데이터 e(w)가 연결된 데이터이다.

스텝 S502에서, 정보 처리 장치(유저 디바이스)(400)는 관리 장치(201)에 의해서 공개된 사이즈 |S| 및 사이즈 |e(w)| 및, 데이터 S와 데이터 e(w)와의 조합 패턴을 토대로, 스텝 S501에서 복호된 메시지 M(w)로부터, 데이터 S를 취출한다.

정보 처리 장치(유저 디바이스)(400)는 상술한 도 15에 도시하는 처리에 계속해서, 도 10에 도시하는 스텝 S105~S109의 처리를 행한다. 이 경우에, 정보 처리 장치(유저 디바이스)(400)는 도 10에 도시하는 스텝 S105, S106에서의 리보케이션 리스트와의 디스크 ID 대조확인 처리에서, 디스크 ID로서 스텝 S501에서 정보 기록 매체(200)로부터 판독출력한 디스크 ID(w)를 이용한다.

정보 처리 장치(유저 디바이스)(400)는 스텝 S502에서 취출한 데이터 S를 컨텐츠 열쇠 데이터로서 이용해서, 컨텐츠 데이터를 복호한다. 따라서, 상기 스텝 S501, S502의 처리를 거쳐(經; via) 적절한 데이터 S를 취득할 수 없는 경우에는, 컨텐츠 데이터를 적절히 복호할 수가 없다.

설정예 6은

디스크 ID=p(w), IDKey(w)

타이틀 고유값=S

디스크 고유값=p(w)

로 한 설정예이며, 이것은 설정예 3과 디스크 ID의 구성이 마찬가지이므로, 앞서 도 13을 참조해서 설명한 처리와 마찬가지의 디스크 ID 검증 처리가 실행되게 된다.

[5. 서비스 제공 서버에서의 처리의 상세]

다음에, 서비스 제공 서버(300)가 정보 처리 장치(유저 디바이스)(400)로부터의 서비스 제공 요구를 수신했을 때의 처리에 대해서 설명한다.

도 16에 도시하는 바와 같이, 서비스 제공 서버(300)는 정보 처리 장치(유저 디바이스)(400)로부터, 디스크 ID를 수신한다. 이 디스크 ID는 정보 기록 매체(200)를 장착하고, 정보 기록 매체(200)로부터의 디스크 ID의 판독 처리를 실행한 정보 처리 장치(유저 디바이스)(400)에서 검증 처리에 의해서 정당성을 검증한 디스크 ID이다.

서비스 제공 서버(300)는 정보 처리 장치(유저 디바이스)(400)로부터 서비스 제공 요구에 아울러(併) 디스크 ID를 수신하면, 디스크 ID의 정당성을 검증해서, 정당성이 확인된 것을 조건으로 해서, 서비스를 제공한다.

또한, 정보 처리 장치(유저 디바이스)(400)로부터 서비스 제공 요구에 아울러 디스크 ID와 함께 서비스 식별자로서의 서비스 ID도 서비스 제공 서버(300)에 송신한다.

서비스 제공 서버(300)는 도 7에 도시하는 입출력 인터페이스(I/F)(304)를 거쳐서, 관리 장치(201) 또는 컨텐츠 제공 장치(203) 또는 그 밖의 장치로부터 디스크 ID 리보케이션 리스트를 정기적으로, 또는 이벤트 마다 수신하고, 항상 최신판을 시큐어 메모리(305)에 격납하는 처리를 실행하고, 또 입출력 인터페이스(I/F)(304)를 거쳐서, 컨텐츠 제공 장치(203) 또는 그 밖의 장치로부터, 타이틀 마다의 타이틀 고유값과, 제공하는 서비스를 식별하는 서비스 식별 정보를 수신하고, 먼저 도 8을 참조해서 설명한 타이틀마다의 서비스 제공 상황 정보를 관리한 서비스 제공 상황 데이터 베이스를 시큐어 메모리(305)에 격납하고 있다.

서비스 제공 서버(300)는 도 8에 도시하는 서비스 제공 상황 데이터를, 예를 들면 시큐어 메모리(305)에 격납해서 보존유지하고, 정보 처리 장치(유저 디바이스)(400)로부터의 디스크 ID를 수반하는 서비스 제공 요구에 따라서, 서비스 제공 요구 디바이스가, 정당한 디스크 ID에 의거하는 서비스 요구인지의 확인을 실행하고, 또 도 8에 도시하는 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용 상한에 도달해 있지 않은 경우에 한해서, 서비스의 제공을 행한다.

도 17을 참조해서, 서비스 제공 서버(300)가, 정보 처리 장치(유저 디바이스)(400)로부터의 서비스 제공 요구를 수신했을 때의 처리 시퀀스에 대해서 설명한다.

스텝 S701에서, 서비스 제공 서버(300)는 도 7에 도시하는 입출력 인터페이스(I/F)(304)를 거쳐서, 정보 처리 장치(유저 디바이스)(400)로부터의 서비스 제공 요구를 수신한다. 이 정보 처리 장치(유저 디바이스)(400)로부터의 서비스 제공 요구에는 정보 처리 장치(유저 디바이스)(400)가, 정보 기록 매체(200)로부터 취득한 디스크 ID와, 요구 서비스의 식별자(서비스 식별자)가 포함된다. 디스크 ID는 앞서 도 11을 참조해서 설명한 설정예 1～6의 어느것인가(any)의 디스크 ID이다.

스텝 S702에서, 서비스 제공 서버(300)는 수신한 디스크 ID의 검증 처리를 실행한다. 이 검증 처리는 정보 처리 장치(유저 디바이스)(400)에서 실행하는 검증 처리와 마찬가지의 검증 시퀀스, 즉 도 12～도 15를 참조해서 설명한 디스크 ID의 설정예 1～6에 따른 검증 시퀀스를 실행한다.

스텝 S703에서, 디스크 ID의 검증 처리에 의해서 디스크 ID의 정당성이 확인되면, 스텝 S705로 진행하고, 디스크 ID가 부정하다고 판정되면, 스텝 S704로 진행해서 서비스의 제공 처리를 중지한다. 또한, 이 중지 처리시에, 정보 처리 장치(유저 디바이스)(400)에 대한 서비스 제공 처리의 중지 메시지를 송신하는 처리를 행하는 구성으로 해도 좋다.

디스크 ID의 정당성이 확인되어 스텝 S705로 진행한 경우에는, 시큐어 메모리(305)(도 7 참조)에 격납된 디스크 ID 리보케이션 리스트(DIRL)를 판독출력한다.

스텝 S706에서, 정당성 확인이 끝난(確認濟; validated), 수신 디스크 ID가 리보케이션 리스트에 기록되어 있지 않은지를 판정한다.

수신 디스크 ID가 리보케이션 리스트에 기록되어 있는 경우에는, 부정 ID라고 판정하고, 스텝 S711로 진행해서, 서비스의 제공 처리를 중지한다. 또한, 이 중지 처리시에, 정보 처리 장치(유저 디바이스)(400)에 대한 서비스 제공 처리의 중지 메시지를 송신하는 처리를 행하는 구성으로 해도 좋다.

수신 디스크 ID가 리보케이션 리스트에 기록되어 있지 않은 경우에는, 스텝 S707에서, 디스크 ID에 의거해서 타이틀 고유값을 산출한다. 디스크 ID는 앞서 도 11을 참조해서 설명한 타이틀 고유값 M 또는 S를 포함하는 데이터, 혹은 타이틀 고유값 M 또는 S를 산출 가능한 데이터로서 구성되어 있으며, 서비스 제공 서버(300)는 수신한 디스크 ID에 포함되는 타이틀 고유값 M 또는 S를 취득, 혹은 연산 유닛(303)의 연산 처리에 의해, 수신한 디스크 ID로부터 타이틀 고유값 M 또는 S를 산출한다. 이 타이틀 고유값 M 또는 S의 취득, 산출 처리는 앞서 도 11을 참조해서 설명한 설정예 1～6에 따라서 다른 처리로서 실행되게 된다.

스텝 S707에서는 또, 디스크 ID로부터 취득한 타이틀 고유값 M 또는 S에 의거해서, 타이틀 대응의 서비스 제공 상황 데이터를 데이터 베이스로부터 취득한다. 즉, 도 8을 참조해서 설명한 서비스 제공 상황 데이터이며, 각 디스크 ID에 대응하는 각 서비스의 제공 상황을 설정한 데이터이다.

스텝 S707에서, 서비스 제공 상황 데이터 중에서, 정보 처리 장치(유저 디바이스)(400)로부터 수신한 디스크 ID와 서비스 식별자에 대응하는 데이터를 추출하고, 제공 가능한 서비스인지 여부를 체크한다.

도 8에 도시하는 서비스 제공 상황 데이터를 예로 해서 설명하면, 예를 들면 정보 처리 장치(유저 디바이스)(400)로부터 수신한 디스크 ID가 (DiscID1)이고, 서비스 식별자가 (서비스 1)인 경우, 서비스 1은 상한 1회이며, 서비스 제공 상황은 [미제공(未提供; unprovided)]이므로, 제공 가능하다고 판단된다.

스텝 S708에서, 서비스 제공 상황 데이터에 의거해서 서비스 제공 가능으로 판정하면, 스텝 S709로 진행하고, 스텝 S708에서, 서비스 제공 상황 데이터에 의거해서 서비스 제공 불가능으로 판정하면, 스텝 S711로 진행한다.

스텝 S711에서는, 서비스의 제공 처리를 중지한다. 또한, 이 중지 처리시에, 정보 처리 장치(유저 디바이스)(400)에 대한 서비스 제공 처리의 중지 메시지를 송신하는 처리를 행하는 구성으로 해도 좋다.

서비스 제공 상황 데이터에 의거해서 서비스 제공 가능으로 판정한 경우에는, 스텝 S709에서, 데이터 베이스의 갱신을 행한다.

도 8에 도시하는 서비스 제공 상황 데이터를 예로 해서 설명하면, 예를 들면 정보 처리 장치(유저 디바이스)(400)로부터 수신한 디스크 ID가 (DiscID1)이고, 서비스 식별자가 (서비스 1)인 경우, 서비스 제공 상황은 [미제공]을 [1회 제공필(提供畢; provided; 제공을 마친 상태)]로 변경한다.

스텝 S710에서는, 서비스 제공 서버(300)는 서비스 제공 요구를 송신해 온 정보 처리 장치(유저 디바이스)(400)에 대한 서비스 제공 처리를 실행한다.

예를 들면, 디스크 격납 컨텐츠가 외국어 영화인 경우의 음성에 대한 자막 데이터나 더빙 음성 데이터, 혹은 컨텐츠의 속편의 디스크의 구입 할인권 등, 여러가지 컨텐츠 관련 서비스가, 네트워크를 거쳐서 서비스 제공 서버(300)로부터 정보 처리 장치(유저 디바이스)(400)에 제공된다.

또한, 정보 처리 장치(유저 디바이스)(400)와 서비스 제공 서버(300) 사이의 통신은 암호 기술을 이용한 상호 인증, 및 세션 키(session key)의 공유를 행해서 안전한 통신로를 작성하고, 그 위(上)에서 통신을 행하는 것이 바람직하다.

또, 상술한 예에서는, 서비스 제공 요구를 수령할 때마다 스텝 S705, S706에서 디스크 ID 리보케이션 리스트(DIRL)를 체크하도록 되어 있지만, 미리 예를 들면 정기적(定期的)으로 디스크 ID 리보케이션 리스트(DIRL)를 체크하고, 그곳에 리스트된 디스크 ID에 대해서는 데이터 베이스를 갱신해서 그 이상(以上)의 서비스 제공을 행하지 않도록 해 두는 구성으로 해도 좋다. 이와 같은 구성으로 한 경우에는, 서비스 제공 요구를 수령했을 때의 디스크 ID 리보케이션 리스트(DIRL)의 체크를 생략할 수 있어, 서비스를 제공하기 위한 시간을 짧게 할 수도 있다.

또, 상술한 실시예에서는 디스크 ID는 디스크 1매마다 다른 것으로서 설명해 왔지만, 디스크 ID를 예를 들면 10매, 100매, 1000매라고 하는 그룹 단위로 공통으로 하고, 디스크 ID 하나에 대해서 제공하는 서비스의 회수(回數)를 그룹의 매수를 고려(考慮)해서 결정해도 좋다.

이상, 특정의 실시예를 참조하면서, 본 발명에 대해서 상세하게 풀이(詳解)해 왔다. 그렇지만, 본 발명의 요지를 일탈(逸脫)하지 않는 범위에서 당업자(當業者)가 그 실시예의 수정이나 대용(代用)을 할 수 있는 것은 자명(自明)하다. 즉, 예시라는 형태(形態)로 본 발명을 개시해 온 것이며, 한정적으로 해석되어서는 안 된다. 본 발명의 요지를 판단하기 위해서는, 아래에 기재한 특허청구범위의 란(欄)을 참작해야만 한다.

또한, 명세서 중에서 설명한 일련(一連)의 처리는 하드웨어 또는 소프트웨어, 혹은 양자(兩者)의 복합 구성에 의해서 실행하는 것이 가능하다. 소프트웨어에 의한 처리를 실행하는 경우에는, 처리 시퀀스를 기록한 프로그램을, 전용(專用)의 하드웨어에 실장(組入; incorporate)된 컴퓨터 내의 메모리에 인스톨(install)해서 실행시키거나, 혹은 각종 처리가 실행 가능한 범용 컴퓨터에 프로그램을 인스톨해서 실행시키는 것이 가능하다.

예를 들면, 프로그램은 기록 매체로서의 하드디스크나 ROM(Read Only Memory)에 미리 기록해 둘 수가 있다. 혹은, 프로그램은 플렉시블 디스크, CD-ROM(Compact Disc Read Only Memory), MO(Magneto Optical) 디스크, DVD(Digital Versatile Disc), 자기(磁氣) 디스크, 반도체 메모리 등의 리무버블(removable) 기록 매체에, 일시적(一時的) 혹은 영속적(永續的)으로 격납(기록)해 둘 수가 있다. 이와 같은 리무버블 기록 매체는 이른바 패키지 소프트웨어로서 제공할 수가 있다.

또한, 프로그램은 상술한 바와 같은 리무버블 기록 매체로부터 컴퓨터에 인스톨하는 것 이외에도, 다운로드 사이트로부터, 컴퓨터에 무선 전송(無線轉送)하거나 LAN(Local Area Network), 인터넷이라고 하는 네트워크를 거쳐서, 컴퓨터에 유선(有線)으로 전송하고, 컴퓨터에서는 그와 같이 해서 전송되어 오는 프로그램을 수신하고, 내장하는 하드디스크 등의 기록 매체에 인스톨할 수가 있다.

또한, 명세서에 기재된 각종 처리는 기재(記載)에 따라서 시계열로(時系列; time-sequentially) 실행될 뿐만 아니라, 처리를 실행하는 장치의 처리 능력 혹은 필요에 따라서 병렬적으로 혹은 개별로(個別; individually) 실행되어도 좋다. 또, 본 명세서에서 시스템이라 함은, 복수의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 하우징 내에 있는 것에는 한정되지 않는다.

산업상 이용 가능성

이상 설명한 바와 같이, 본 발명의 구성에 의하면, DVD, CD, 청색 레이저 기록 매체 등의 각종 정보 기록 매체에 컨텐츠를 격납해서 제공하고, 또 네트워크 접속한 서비스 제공 서버로부터의 서비스 제공 처리를 행하는 구성에 있어서, 서비스 제공 서버 측에서, 정보 처리 장치(유저 디바이스)로부터 송신되는 정보 기록 매체 ID를 검증하고, 정보 기록 매체 ID 마다의 서비스 제공 상황 데이터에 의거하는 서비스 제공을 행하는 구성으로 했으므로, 서비스 요구를 송신한 정보 처리 장치가 정당한 정보 기록 매체 ID를 정보 기록 매체로부터 판독한 정보 처리 장치이며, 서비스 제공 상황 데이터에 의거해서 서비스 제공이 허용되고 있는 서비스인 것이 확인된 경우에 한해서, 서비스의 제공이 실행된다. 본 발명의 구성은 컨텐츠에 대응하는 여러가지 서비스 정보, 예를 들면 디스크 격납 컨텐츠가 영화 컨텐츠인 경우의 자막 데이터, 더빙 음성 데이터 등의 컨텐츠에 부수하는 정보를 서버로부터 제공하는 시스템 등에 있어서, 서비스 제공처(提供先; receiver)를 엄격하게 심사(審査)해서, 정당한 권한을 확인한 다음(확인하고 나서) 컨텐츠에 대응하는 여러가지 서비스 정보를 제공하는 것이 가능해진다.

또, 본 발명의 구성에 의하면, 정보 기록 매체에 격납된 정보 기록 매체 ID는 관리 장치의 서명 데이터 등의 정당성이 확인 가능한 데이터를 포함하고, 또 타이틀 고유값을 가지거나 혹은 산출 가능한 데이터를 포함하는 구성으로 했으므로, 서비스 제공 서버에 있어서는, 정보 기록 매체 ID에 포함되는 데이터에 의거하는 정당성의 확인이 가능하고, 또 타이틀 고유값을 취득하는 것이 가능해지고, 타이틀 고유값에 대응지어서 설정된 서비스 제공 상황 데이터의 특정을 행하는 것이 가능해진다. 따라서, 서비스 제공처를 엄격하게 심사해서, 정당한 권한을 확인한 다음 컨텐츠에 대응하는 여러가지 서비스 정보를 제공하는 것이 가능해진다.

도면의 간단한 설명

도 1은 정보 기록 매체의 격납 데이터를 설명하는 도면,

도 2는 리보케이션 리스트의 구성에 대해서 설명하는 도면,

도 3은 메시지 인증 코드(MAC: Message Authentication Code)를 이용했을 때의 MAC 생성, 검증 처리에 대해서 설명하는 도면,

도 4는 각종 키, 데이터의 암호화 처리, 배포 처리에 적용되는 계층형나무 구조를 설명하는 도면,

도 5는 컨텐츠 열쇠의 유효화 키 블록(EKB)을 사용한 배포예와 복호 처리예를 도시하는 도면,

도 6은 정보 기록 매체의 제조, 관리 처리 구성에 대해서 설명하는 도면,

도 7은 서비스 제공 서버의 구성예에 대해서 설명하는 도면,

도 8은 서비스 제공 서버가 보유하는 서비스 제공 상황 데이터를 도시하는 도면,

도 9는 정보 처리 장치(유저 디바이스)의 구성예에 대해서 설명하는 도면,

도 10은 디스크 ID의 설정예에 대해서 설명하는 도면,

도 11은 정보 처리 장치(유저 디바이스)가 실행하는 처리를 설명하는 플로차트,

도 12는 정보 처리 장치(유저 디바이스)가 실행하는 디스크 ID 검증 시퀀스를 설명하는 플로차트,

도 13은 정보 처리 장치(유저 디바이스)가 실행하는 디스크 ID 검증 시퀀스를 설명하는 플로차트,

도 14는 정보 처리 장치(유저 디바이스)가 실행하는 디스크 ID 검증시퀀스를 설명하는 플로차트,

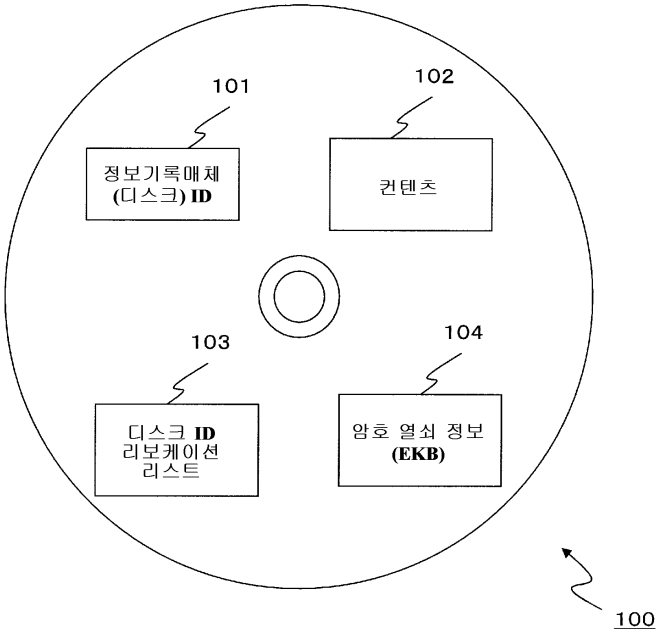
도 15는 정보 처리 장치(유저 디바이스)가 실행하는 디스크 ID 검증 시퀀스를 설명하는 플로차트,

도 16은 정보 처리 장치(유저 디바이스)가 서비스 제공 서버로부터 서비스를 수령하는 처리에 대해서 설명하는 도면,

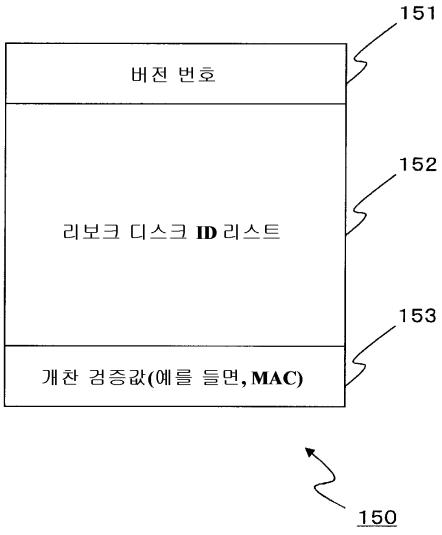
도 17은 서비스 제공 서버가 실행하는 처리를 설명하는 플로차트.

도면

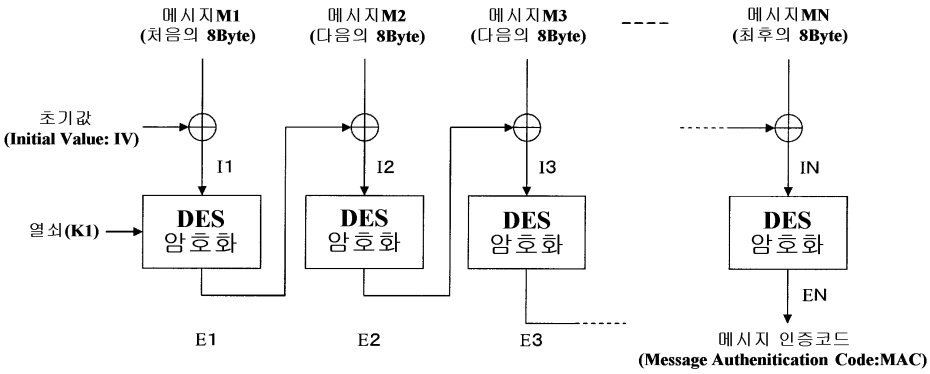
도면1


101
정보기록매체
(디스크) ID
102
컨텐츠
103
디스크 ID
리보케이션
리스트
104
암호 열쇠 정보
(EKB)
100

도면2

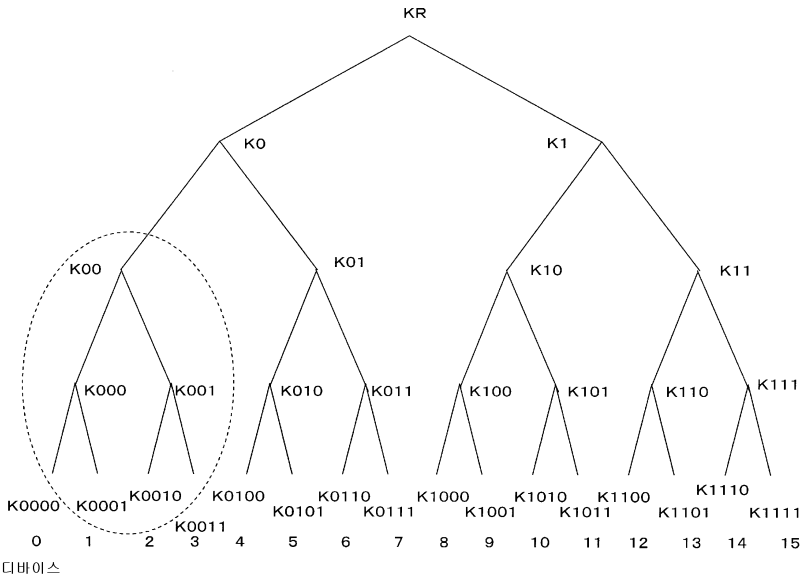

151
버전 번호
152
리보크 디스크 ID 리스트
153
개찬 검증값(예를 들면, MAC)
150

도면3

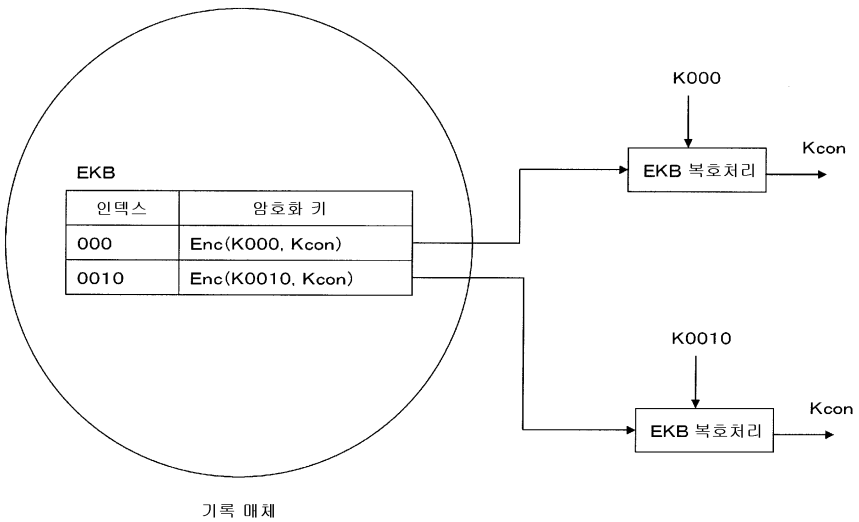


⊕ : 배타적 논리합 처리(8바이트 단위)

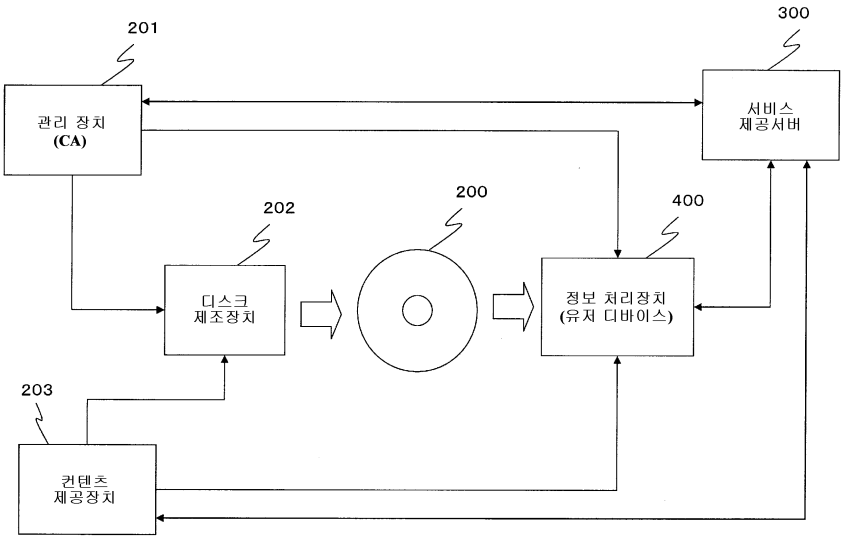
도면4



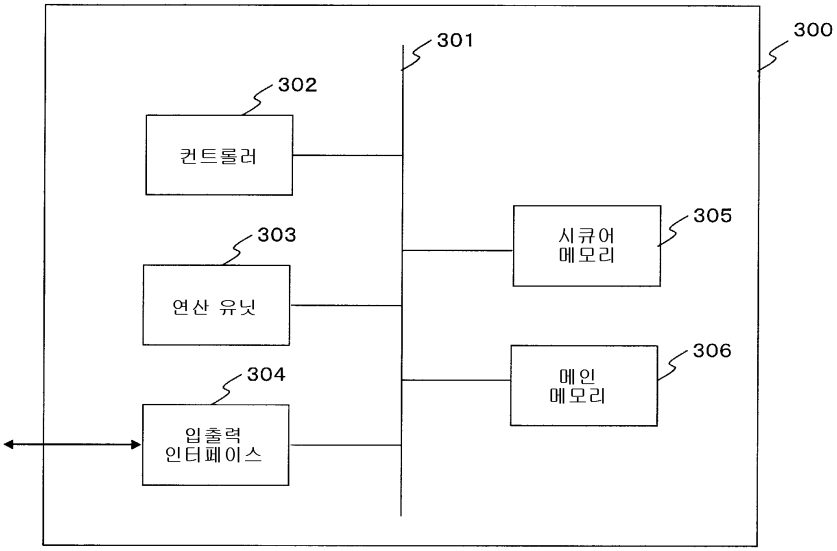
도면5



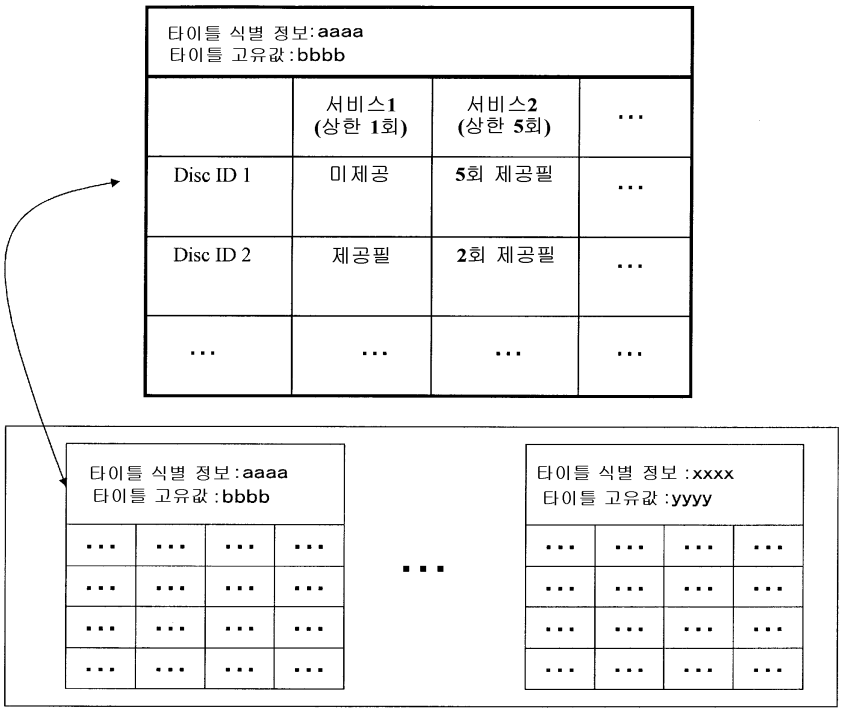
도면6


201
관리 장치
(CA)
300
서비스
제공서버
202
디스크
제조장치
200
400
정보 처리장치
(유저 디바이스)
203
컨텐츠
제공장치

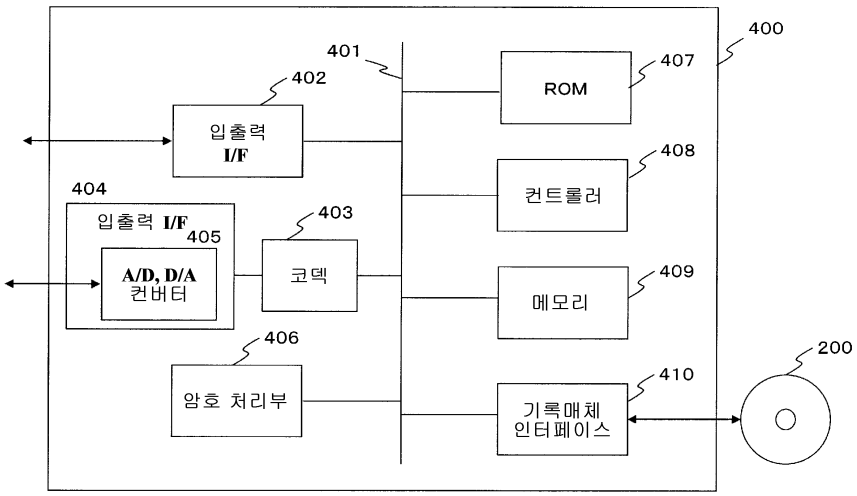
도면7


300
301
302
컨트롤러
303
연산 유닛
304
입출력
인터페이스
305
시큐어
메모리
306
메인
메모리

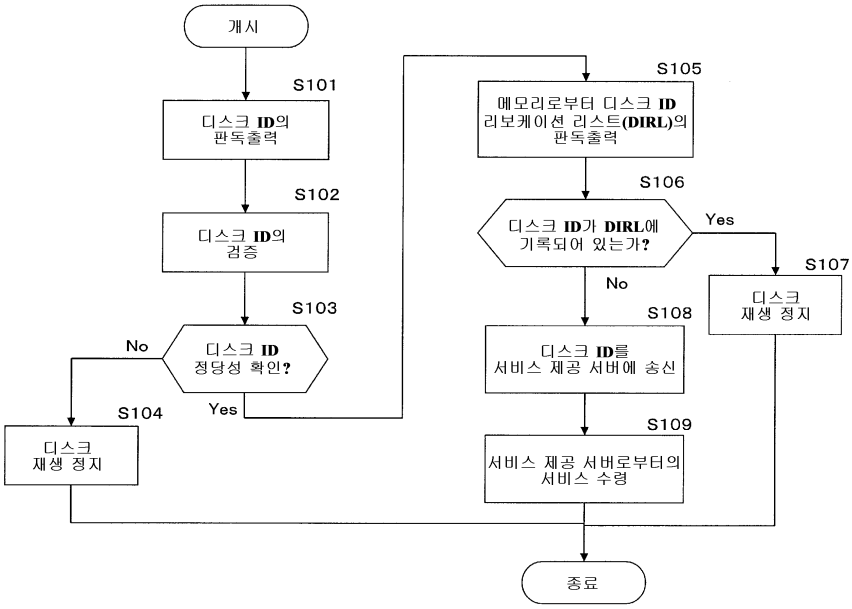
도면8


타이틀 식별 정보:aaaa
타이틀 고유값:bbbb
서비스1 (상한 1회)
서비스2 (상한 5회)
Disc ID 1
미제공
5회 제공필
Disc ID 2
제공필
2회 제공필
타이틀 식별 정보:aaaa
타이틀 고유값:bbbb
타이틀 식별 정보:xxxx
타이틀 고유값:yyyy

도면9


400
401
402
입출력 I/F
ROM
407
408
컨트롤러
404
입출력 I/F
405
A/D, D/A 컨버터
403
코덱
409
메모리
406
암호 처리부
410
기록매체 인터페이스
200

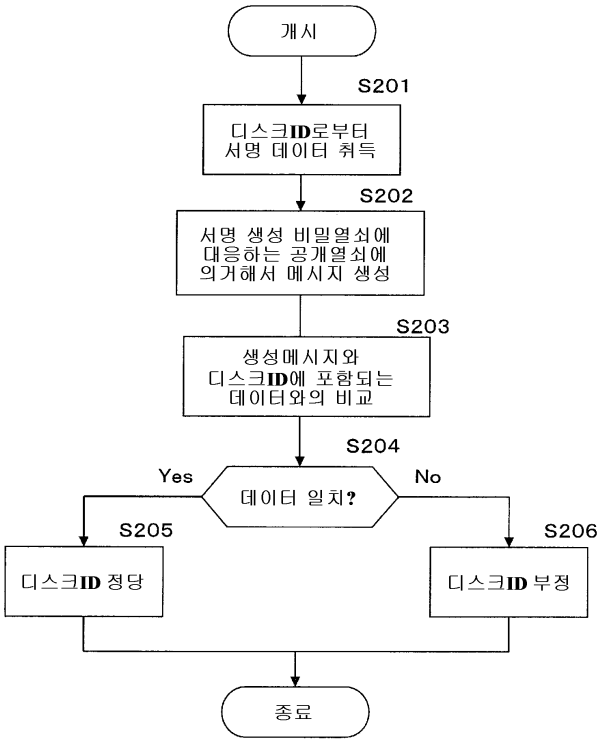
도면10



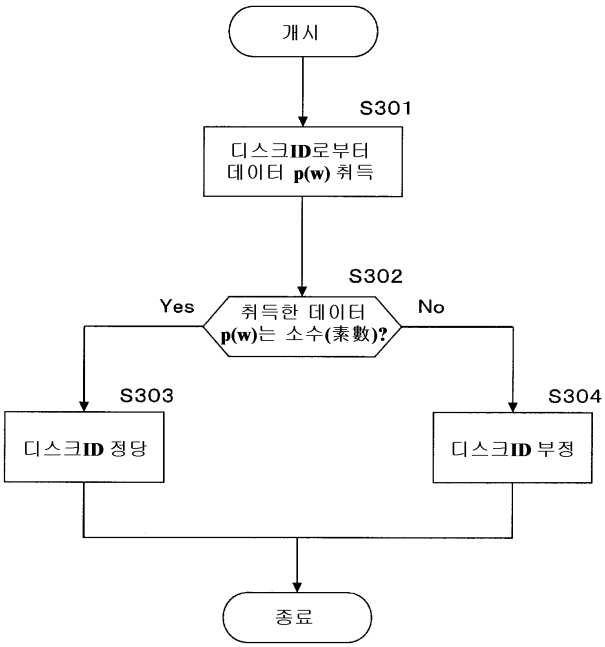
도면11

	디스크ID	타이틀 고유값	디스크 고유값
디스크 ID 설정예1	M, Sig(w)	M	Sig(w)
디스크 ID 설정예2	S, Sig(w)	S	Sig(w)
디스크 ID 설정예3	p(w), IDKey(w)	S	p(w) 또는, IDKey(w)
디스크 ID 설정예4	e(w), I(w)	S	e(w) 또는, I(w)
디스크 ID 설정예5	Σw	S	e(w)
디스크 ID 설정예6	p(w), IDKey(w)	S	p(w)

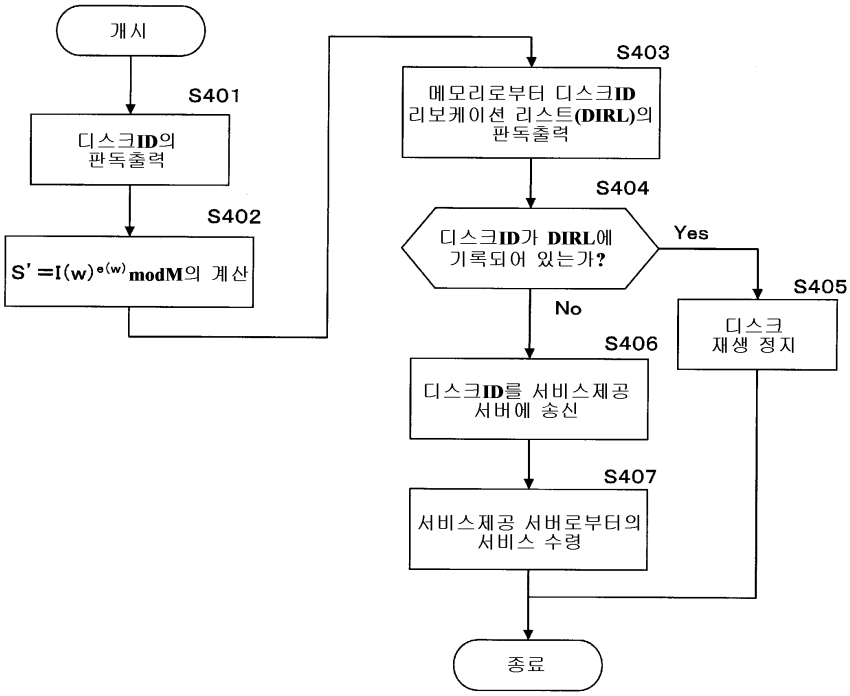
도면12


개시
S201
디스크ID로부터
서명 데이터 취득
S202
서명 생성 비밀열쇠에
대응하는 공개열쇠에
의거해서 메시지 생성
S203
생성메시지와
디스크ID에 포함되는
데이터와의 비교
S204
Yes
데이터 일치?
No
S205
디스크ID 정당
S206
디스크ID 부정
종료

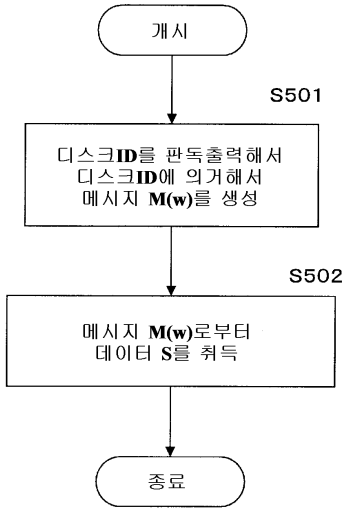
도면13


개시
S301
디스크ID로부터
데이터 p(w) 취득
S302
Yes
취득한 데이터
p(w)는 소수(素數)?
No
S303
디스크ID 정당
S304
디스크ID 부정
종료

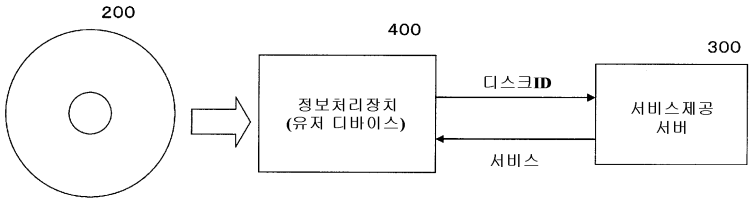
도면14



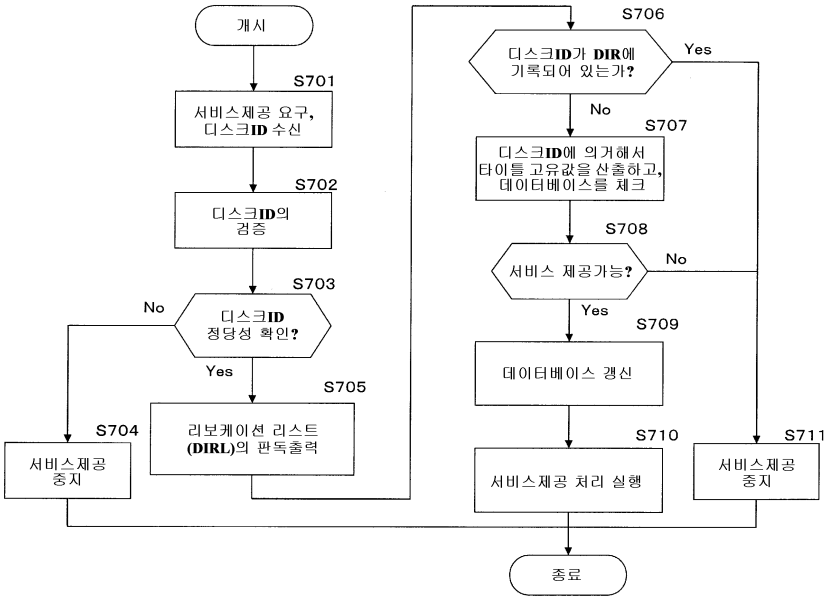
도면15



도면16



도면17


개시
S701
서비스제공 요구,
디스크ID 수신
S702
디스크ID의
검증
S703
디스크ID
정당성 확인?
No
Yes
S704
서비스제공
중지
S705
리보케이션 리스트
(DIRL)의 판독출력
S706
디스크ID가 DIR에
기록되어 있는가?
Yes
No
S707
디스크ID에 의거해서
타이틀 고유값을 산출하고,
데이터베이스를 체크
S708
서비스 제공가능?
No
Yes
S709
데이터베이스 갱신
S710
서비스제공 처리 실행
S711
서비스제공
중지
종료