(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)

(45) 공고일자 2006년12월01일
(11) 등록번호 10-0652098
(24) 등록일자 2006년11월23일

(21) 출원번호 10-2002-7009870(분할)
(22) 출원일자 2002년07월31일
심사청구일자 2006년01월18일
번역문 제출일자 2002년07월31일
(62) 원출원 특허10-2001-7012032
원출원일자 : 2001년09월21일
(86) 국제출원번호 PCT/JP2001/000346
국제출원일자 2001년01월19일

(65) 공개번호 10-2002-0084904
(43) 공개일자 2002년11월13일
심사청구일자 2002년07월31일
(87) 국제공개번호 WO 2001/54099
국제공개일자 2001년07월26일

(81) 지정국 국내특허 : 오스트레일리아, 브라질, 캐나다, 중국, 대한민국, 멕시코, 뉴질랜드, 미국, 러시아, 싱가포르,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드, 사이프러스, 터어키,

(30) 우선권주장

JP-P-2000-00013322	2000년01월21일	일본(JP)
JP-P-2000-00015551	2000년01월25일	일본(JP)
JP-P-2000-00015858	2000년01월25일	일본(JP)
JP-P-2000-00016029	2000년01월25일	일본(JP)
JP-P-2000-00016213	2000년01월25일	일본(JP)
JP-P-2000-00016251	2000년01월25일	일본(JP)
JP-P-2000-00016292	2000년01월25일	일본(JP)

(73) 특허권자 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

가부시키가이샤 소니 컴퓨터 엔터테인먼트
일본국 도쿄도 107-0062 미나토구 미나미-아오야마 2-6-21

(72) 발명자 아사노, 도모유끼
일본 141-0001 도꾜도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼 가이샤 내

이시바시, 요시히또
일본 141-0001 도꾜도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼 가이샤 내

시라이, 다이조
일본 141-0001 도꾜도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼 가이샤 내

아끼시따, 도루
일본 141-0001 도쿄도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼 가이샤 내

요시모리, 마사하루
일본 107-0052 도쿄도 미나또꾸 아까사까 7쪼메 1반지 1고소 니 컴퓨터 엔터테인먼트 인코포레이티드 내

다나까, 마꼬또
일본 107-0052 도쿄도 미나또꾸 아까사까 7쪼메 1반지 1고소 니 컴퓨터 엔터테인먼트 인코포레이티드 내

(74) 대리인 장수길
구영창

심사관 : 이준석

전체 청구항 수 : 총 14 항

(54) 데이터 인증 처리 시스템

(57) 요약

세이브 데이터의 시큐러티를 확보 가능하게 한 데이터 기록 재생기 및 세이브 데이터 처리 방법을 제공한다. 프로그램에만 고유한 암호 키, 예를 들면 콘텐츠 키, 또는 콘텐츠 키에 기초하여 세이브 데이터 암호화 키를 생성하여 세이브 데이터를 암호화하여 기록 디바이스에 저장하고, 재생 시에는 프로그램 고유의 세이브 데이터 복호화 키에 의해 복호 처리를 실행한다. 또한, 기록 재생기 고유의 키, 또는 사용자 패스워드를 이용하여 세이브 데이터 암호 키, 복호 키를 생성하여 세이브 데이터의 암호화, 복호화를 실행하여 세이브 데이터의 저장, 재생을 실행하는 등, 각종 제한 정보에 기초한 세이브 데이터 암호 키의 생성을 가능하게 하였다.

대표도

도 69

특허청구의 범위

청구항 1.
삭제

청구항 2.
삭제

청구항 3.
삭제

청구항 4.
삭제

청구항 5.

삭제

청구항 6.
삭제

청구항 7.
삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

청구항 18.
삭제

청구항 19.
삭제

청구항 20.
삭제

청구항 21.
삭제

청구항 22.

삭제

청구항 23.
삭제

청구항 24.
삭제

청구항 25.
삭제

청구항 26.
삭제

청구항 27.
삭제

청구항 28.
삭제

청구항 29.
삭제

청구항 30.
삭제

청구항 31.
삭제

청구항 32.
삭제

청구항 33.
삭제

청구항 34.
삭제

청구항 35.
삭제

청구항 36.
삭제

청구항 37.
삭제

청구항 38.
삭제

청구항 39.

삭제

청구항 40.
삭제

청구항 41.
삭제

청구항 42.
삭제

청구항 43.
삭제

청구항 44.
삭제

청구항 45.
삭제

청구항 46.
삭제

청구항 47.
삭제

청구항 48.
삭제

청구항 49.
삭제

청구항 50.
삭제

청구항 51.
삭제

청구항 52.
삭제

청구항 53.
삭제

청구항 54.
삭제

청구항 55.
삭제

청구항 56.

삭제

청구항 57.
삭제

청구항 58.
삭제

청구항 59.
삭제

청구항 60.
삭제

청구항 61.
삭제

청구항 62.
삭제

청구항 63.
삭제

청구항 64.
삭제

청구항 65.
삭제

청구항 66.
삭제

청구항 67.
삭제

청구항 68.
삭제

청구항 69.
삭제

청구항 70.
삭제

청구항 71.

콘텐츠를 재생할 수 있는 데이터 처리 장치에 있어서,

상기 콘텐츠의 세이브 데이터를 기록하도록 동작가능한 기록 디바이스;

상기 세이브 데이터에 대한 암호 처리 및 복호 처리를 실행할 수 있도록 동작가능하며, 상기 암호 처리 및 상기 복호 처리를 실행하기 위한 암호 키를 사용하는 암호 처리부;

상기 세이브 데이터에 대한 프로그램 현지화(program localization) -상기 프로그램 현지화는 데이터 관리 파일 내에서 관리됨- 를 입력하도록 동작할 수 있는 입력부; 및

상기 데이터 관리 파일을 억세스할 수 있으며, 상기 세이브 데이터에 대한 암호 처리 방법 및 복호 처리 방법을 결정하도록 동작할 수 있는 제어부를 포함하며,

상기 암호 처리 방법은 상기 암호 키를 이용할 수 있고, 상기 프로그램 현지화에 따라 결정되며, 상기 암호 처리 방법은 상기 기록 디바이스에 상기 세이브 데이터를 저장하도록 되어 있으며, 상기 복호 처리 방법은 상기 프로그램 현지화에 따라 결정되고 상기 암호 키를 재생하도록 되어 있고,

상기 콘텐츠는 식별자를 포함하고;

상기 프로그램 현지화는 상기 식별자에 따라 상기 세이브 데이터의 이용을 가능하게 하는 프로그램 제한인 것을 특징으로 하는 데이터 처리 장치.

청구항 72.

제71항에 있어서, 상기 데이터 관리 파일은 상기 식별자에 따라 상기 프로그램 제한을 저장하기 위한 테이블로서 구성되고; 만일 상기 프로그램 제한이 상기 프로그램 콘텐츠의 제한을 제공하는 경우, 상기 암호 처리부는 상기 프로그램 콘텐츠의 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 세이브 데이터 암호 키는 상기 프로그램 콘텐츠의 개별 암호 키 또는 개별 정보 중 적어도 하나에 기초하며; 만일 상기 프로그램 제한이 상기 프로그램 콘텐츠의 제한없이 제공하는 경우, 상기 암호 처리부는 시스템 공유 암호 키 및 시스템 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 시스템 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치에 저장되는 것을 특징으로 하는 데이터 처리 장치.

청구항 73.

제72항에 있어서, 상기 개별 암호 키는 콘텐츠 데이터의 헤더부에 저장될 수 있는 콘텐츠 키 K_{con}이고; 상기 시스템 공유 암호 키는 복수의 상이한 데이터 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 장치.

청구항 74.

제71항에 있어서, 식별 정보를 더 포함하며, 상기 프로그램 현지화는 상기 식별 정보에 따라 상기 세이브 데이터를 이용할 수 있게 하는 처리 장치 제한이고; 상기 데이터 관리 파일은 상기 콘텐츠의 식별자와 대응하여 상기 처리 장치 제한을 저장하기 위한 테이블로서 구성되고, 만일 상기 처리 장치 제한이 처리 장치의 제한을 제공하는 경우, 상기 암호 처리부는 상기 처리 장치의 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 세이브 데이터 암호 키는 상기 데이터 처리 장치의 개별 암호 키와 개별 정보 중 적어도 하나에 기초하며, 만일 상기 처리 장치 제한이 상기 처리 장치의 제한 없이 제공하는 경우, 상기 암호 처리부는 시스템 공유 암호 키 및 공유 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 공유 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치 내에 저장되는 것을 특징으로 하는 데이터 처리 장치.

청구항 75.

제74항에 있어서, 상기 개별 암호 키는 상기 데이터 처리 장치에 저장될 수 있는 개별 서명 키 K_{dev}이고; 상기 시스템 공유 암호 키는 복수의 특정 데이터 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 장치.

청구항 76.

제71항에 있어서, 상기 콘텐츠는 식별자를 포함하고; 상기 프로그램 현지화는 사용자의 식별에 따라 상기 세이브 데이터를 이용할 수 있게 하는 사용자 제한이며; 상기 데이터 관리 파일은 상기 식별자에 따라 상기 사용자 제한을 저장하기 위한 테이블로서 구성되고; 만일 상기 사용자 제한이 상기 사용자의 제한을 제공하는 경우, 상기 암호 처리부는 사용자 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 사용자 세이브 데이터 암호 키는 상기 입력부에 의해 수신된 패스워드에 기초하며, 만일 상기 사용자 제한이 상기 사용자의 제한 없이 제공하는 경우, 상기 암호 처리부는 시스템 공유 암호 키 및 공유 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 공유 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치에 저장되는 것을 특징으로 하는 데이터 처리 장치.

청구항 77.

제76항에 있어서, 상기 시스템 공유 암호 키는 복수의 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 장치.

청구항 78.

콘텐츠를 재생할 수 있는 데이터 처리 장치의 데이터 처리 방법에 있어서,

상기 콘텐츠의 세이브 데이터를 기록하는 기록 단계;

상기 세이브 데이터에 대한 암호 처리 및 복호 처리를 실행할 수 있고, 상기 암호 처리 및 상기 복호 처리를 실행하기 위해 암호 키를 사용하는 암호 처리 단계;

상기 세이브 데이터에 대한 프로그램 현지화(program localization) -상기 프로그램 현지화는 데이터 관리 파일 내에서 관리됨- 를 입력하도록 해주는 입력 단계; 및

상기 데이터 관리 파일을 억세스할 수 있으며, 상기 세이브 데이터에 대한 암호 처리 방법 및 복호 처리 방법을 결정하는 제어 단계를 포함하며,

상기 암호 처리 방법은 상기 암호 키를 이용할 수 있고, 상기 프로그램 현지화에 따라 결정되며, 상기 암호 처리 방법은 상기 기록 디바이스에 상기 세이브 데이터를 저장하도록 되어 있으며, 상기 복호 처리 방법은 상기 프로그램 현지화에 따라 결정되고 상기 암호 키를 재생하도록 되어 있고,

상기 콘텐츠는 식별자를 포함하고;

상기 프로그램 현지화는 상기 식별자에 따라 상기 세이브 데이터의 이용을 가능하게 하는 프로그램 제한인 것을 특징으로 하는 데이터 처리 방법.

청구항 79.

제78항에 있어서, 상기 데이터 관리 파일은 상기 식별자에 따라 상기 프로그램 제한을 저장하기 위한 테이블로서 구성되고; 만일 상기 프로그램 제한이 상기 프로그램 콘텐츠의 제한을 제공하는 경우, 상기 암호 처리 단계는 상기 프로그램 콘텐츠의 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 세이브 데이터 암호 키는 상기 프로그램 콘텐츠의 개별 암호 키 또는 개별 정보 중 적어도 하나에 기초하며; 만일 상기 프로그램 제한이 상기 프로그램 콘텐츠의 제한없이 제공하는 경우, 상기 암호 처리 단계는 시스템 공유 암호 키 및 시스템 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 시스템 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치에 저장되는 것을 특징으로 하는 데이터 처리 방법.

청구항 80.

제79항에 있어서, 상기 개별 암호 키는 콘텐츠 데이터의 헤더부에 저장될 수 있는 콘텐츠 키 K_{con}이고; 상기 시스템 공유 암호 키는 복수의 상이한 데이터 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 방법.

청구항 81.

제78항에 있어서, 식별 정보가 상기 데이터 처리 장치 내에 포함되어 있고, 상기 프로그램 현지화는 상기 식별 정보에 따라 상기 세이브 데이터를 이용할 수 있게 하는 처리 장치 제한이고; 상기 데이터 관리 파일은 상기 콘텐츠의 식별자와 대응하여 상기 처리 장치 제한을 저장하기 위한 테이블로서 구성되고, 만일 상기 처리 장치 제한이 처리 장치의 제한을 제공하는 경우, 상기 암호 처리 단계는 상기 처리 장치의 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 세이브 데이터 암호 키는 상기 데이터 처리 장치의 개별 암호 키와 개별 정보 중 적어도 하나에 기초하며, 만일 상기 처리 장치 제한이 상기 처리 장치의 제한 없이 제공하는 경우, 상기 암호 처리 단계는 시스템 공유 암호 키 및 공유 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 공유 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치 내에 저장되는 것을 특징으로 하는 데이터 처리 방법.

청구항 82.

제81항에 있어서, 상기 개별 암호 키는 상기 데이터 처리 장치에 저장될 수 있는 개별 서명 키 K_{dev}이고; 상기 시스템 공유 암호 키는 복수의 특정 데이터 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 방법.

청구항 83.

제78항에 있어서, 상기 콘텐츠는 식별자를 포함하고; 상기 프로그램 현지화는 사용자의 식별에 따라 상기 세이브 데이터를 이용할 수 있게 하는 사용자 제한이며; 상기 데이터 관리 파일은 상기 식별자에 따라 상기 사용자 제한을 저장하기 위한 테이블로서 구성되고; 만일 상기 사용자 제한이 상기 사용자의 제한을 제공하는 경우, 상기 암호 처리 단계는 사용자 세이브 데이터 암호 키를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 복호 처리 방법을 실행하고, 상기 사용자 세이브 데이터 암호 키는 상기 입력 단계에 의해 수신된 패스워드에 기초하며, 만일 상기 사용자 제한이 상기 사용자의 제한 없이 제공하는 경우, 상기 암호 처리 단계는 시스템 공유 암호 키 및 공유 세이브 데이터 암호 키 중 적어도 하나를 이용하여 상기 세이브 데이터에 대해 상기 암호 처리 방법 또는 상기 복호 처리 방법을 실행하고, 상기 공유 세이브 데이터 암호 키는 상기 시스템 공유 암호 키에 기초하고, 상기 시스템 공유 암호 키는 상기 데이터 처리 장치에 저장되는 것을 특징으로 하는 데이터 처리 방법.

청구항 84.

제83항에 있어서, 상기 시스템 공유 암호 키는 복수의 처리 장치에 저장될 수 있는 시스템 서명 키 K_{sys}인 것을 특징으로 하는 데이터 처리 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 데이터 처리 장치 및 데이터 처리 방법에 관한 것으로, 보다 상세하게는 데이터 콘텐츠를 구성하는 데이터의 정당성, 즉 변경의 유무를 검증하는 방법, 장치, 검증치의 부여 방법에 관한 것이다. 또한, 암호 처리에 필요한 개별 키를 각 개별 키에 대응한 마스터 키에 의해 생성함으로써, 시큐러티를 높일 수 있는 장치 및 방법에 관한 것이다. 또한, 본 발명은 데이터 콘텐츠의 부정 이용을 배제하는 구성을 제공하는 것으로, 구체적으로는 부정 재생 기기를 식별하여 콘텐츠의 부정 이용을 배제할 수 있는 장치 및 방법에 관한 것이다. 또한, 본 발명은 데이터 처리 장치에만 이용 가능한 콘텐츠와, 다른 데이터 처리 장치에서도 이용 가능한 콘텐츠를 데이터 처리 장치 고유의 정보 등에 기초하여 용이하게 설정할 수 있는 장치 및 방법에 관한 것이다. 또한, 데이터 콘텐츠를 구성하는 데이터의 정당성, 즉 변경의 유무를 검증하는 방법, 장치, 검증치의 부여 방법에 관한 것이다.

또한, 본 발명은 음성 정보, 화상 정보, 프로그램 데이터 중 적어도 어느 하나를 포함하는 데이터를 암호화 처리하여 각종 헤더 정보와 함께 콘텐츠 이용자에게 제공하고, 콘텐츠 이용자가 재생, 실행 또는 기록 디바이스에 대한 저장 처리 등을 행하는 구성에 있어서 콘텐츠 데이터를 높은 시큐러티 관리 하에서 제공 및 이용할 수 있는 콘텐츠 데이터 구성을 실현하는 데이터 처리 장치, 콘텐츠 데이터 생성 방법 및 데이터 처리 방법에 관한 것이다.

또한, 데이터 콘텐츠가 압축된 음성 데이터 또는 화상 데이터 등인 경우의 재생 처리를 효율적으로 실행하는 구성을 제공하는 것으로, 구체적으로는 콘텐츠 데이터의 구성을 압축 데이터와 신장 처리 프로그램을 조합한 구성으로 하거나, 적용 신장 처리 프로그램을 헤더 정보로서 저장한 압축 데이터 콘텐츠의 헤더 정보에 기초하여 적용 가능한 신장 처리 프로그램을 검색 추출하여 재생 처리를 실행할 수 있는 데이터 처리 장치, 데이터 처리 방법 및 콘텐츠 데이터 생성 방법에 관한 것이다.

본 발명은 DVD, CD 등의 기억 매체 또는 CATV, 인터넷, 위성 통신 등의 유선, 무선 각 통신 수단 등의 경로로 입수 가능한 음성, 화상, 게임, 프로그램 등의 각종 콘텐츠를 사용자가 소유한 기록 재생기에 있어서 재생하고, 전용의 기록 디바이스, 예를 들면 메모리 카드, 하드디스크, CD-R 등에 저장함과 함께, 기록 디바이스에 저장된 콘텐츠를 이용할 때, 콘텐츠 신호 분배측이 희망하는 이용 제한을 붙이는 구성을 실현함과 함께, 이 배포된 콘텐츠를 정규 사용자 이외의 제3자에게 부정 이용되지 않도록 시큐러티를 확보하는 구성 및 방법에 관한 것이다.

최근, 게임 프로그램, 음성 데이터, 화상 데이터, 문서 작성 프로그램 등, 여러가지 소프트웨어 데이터[이하, 이들을 콘텐츠(Content)라 함]가 인터넷 등의 네트워크를 통해, 또는 DVD, CD 등의 유통 가능한 기억 매체를 통해 유통되고 있다. 이들 유통 콘텐츠는 사용자가 소유한 PC(Personal Computer), 게임 기기 등의 기록 재생 기기에 부속하는 기록 디바이스, 예를 들면 메모리 카드, 하드디스크 등에 저장할 수 있으며, 일단 저장된 후에는 저장 매체로부터의 재생에 의해 이용 가능하게 된다.

종래의 비디오 게임 기기, PC 등의 정보 기기에 있어서 사용되는 메모리 카드 장치의 주된 구성 요소는 동작 제어를 위한 제어 수단과, 제어 수단에 접속되어 정보 기기 본체에 설치된 슬롯에 접속하기 위한 커넥터와, 제어 수단에 접속되어 데이터를 기억하기 위한 불휘발성 메모리 등이다. 메모리 카드에 구비된 불휘발성 메모리는 EEPROM, 플래시 메모리 등에 의해 구성된다.

이러한 메모리 카드에 기억된 데이터 또는 프로그램 등의 여러가지 콘텐츠는 재생 기기로서 이용되는 게임 기기, PC 등의 정보 기기 본체로부터의 사용자 지시 또는 접속된 입력 수단을 통한 사용자 지시에 의해 불휘발성 메모리로부터 호출되고, 정보 기기 본체 또는 접속된 디스플레이, 스피커 등을 통해 재생된다.

게임 프로그램, 음악 데이터, 화상 데이터 등, 많은 소프트웨어 콘텐츠는 일반적으로 그 작성자, 판매자에게 반포권 등이 보유되어 있다. 따라서, 이들 콘텐츠 배포에 있어서는 일정한 이용 제한, 즉 정규 사용자에게만, 소프트웨어 사용을 허락하고, 허가가 없는 복제 등이 행해지지 않도록 하는, 즉 시큐러티를 고려한 구성을 하는 것이 일반적으로 되어 있다.

사용자에 대한 이용 제한을 실현하는 하나의 방법이 배포 콘텐츠의 암호화 처리이다. 즉, 예를 들면 인터넷 등을 통해 암호화된 음성 데이터, 화상 데이터, 게임 프로그램 등의 각종 콘텐츠를 배포함과 함께, 정규 사용자라고 확인된 자에 게만, 배포된 암호화 콘텐츠를 복호하는 수단, 즉 복호 키를 부여하는 구성이다.

암호화 데이터는 소정의 수속에 의한 복호화 처리에 의해 이용 가능한 복호 데이터(평문)로 복귀할 수 있다. 이러한 정보의 암호화 처리에 암호화 키를 이용하고, 복호화 처리에 복호화 키를 이용하는 데이터 암호화, 복호화 방법은 종래부터 잘 알려져 있다.

암호화 키와 복호화 키를 이용하는 데이터 암호화·복호화 방법의 형태에는 여러가지 종류가 있지만, 그 하나의 예로서 소위 공통 키 암호화 방식이라 불리는 방식이 있다. 공통 키 암호화 방식은 데이터의 암호화 처리에 이용하는 암호화 키와 데이터의 복호화에 이용하는 복호화 키를 공통의 것으로 하여서, 정규 사용자에게 이들 암호화 처리, 복호화에 이용하는 공통 키를 부여하여 키를 갖지 않은 부정 사용자에 의한 데이터 액세스를 배제하는 것이다. 이 방식의 대표적인 방식으로는 DES (데이터 암호 표준: Date encryption standard)가 있다.

상술한 암호화 처리, 복호화에 이용되는 암호화 키, 복호화 키는 예를 들면 임의의 패스워드 등에 기초하여 해시 함수 등의 일방향성 함수를 적용하여 얻을 수 있다. 일방향성 함수는, 그 출력으로부터 반대로 입력을 구하는 것은 매우 곤란한 함수이다. 예를 들면, 사용자가 결정한 패스워드를 입력으로서 일방향성 함수를 적용하고, 그 출력에 기초하여 암호화 키, 복호화 키를 생성한다. 이와 같이 하여 얻어진 암호화 키, 복호화 키로부터, 반대로 그 오리지널 데이터인 패스워드를 구하는 것은 실질적으로 불가능하게 된다.

또한, 암호화할 때 사용하는 암호화 키에 의한 처리와, 복호할 때 사용하는 복호화 키에 의한 처리를 다른 알고리즘으로 한 방식을, 소위 공개 키 암호화 방식이라 한다. 공개 키 암호화 방식은 불특정 사용자가 사용 가능한 공개 키를 사용하는 방법으로서, 특정 개인에 대한 암호화 문서를 그 특정 개인이 발행한 공개 키를 이용하여 암호화 처리를 행한다. 공개 키에 의해 암호화된 문서는 그 암호화 처리에 사용된 공개 키에 대응하는 비밀 키에 의해서만 복호 처리가 가능하게 된다. 비밀 키는 공개 키를 발행한 개인만이 소유하기 때문에 그 공개 키에 의해 암호화된 문서는 비밀 키를 갖는 개인만이 복호할 수 있다. 공개 키 암호화 방식의 대표적인 것에는 RSA(Rivest-Shamir-Adleman) 암호가 있다.

이러한 암호화 방식을 이용함으로써, 암호화 콘텐츠를 정규 사용자에 대해서만 복호 가능하게 하는 시스템이 가능하게 된다. 이들 암호 방식을 채택한 종래의 콘텐츠 배포 구성에 대하여 도 1을 이용하여 간단히 설명한다.

도 1은 PC(퍼스널 컴퓨터), 게임 기기 등의 재생 수단(10)에 있어서, DVD, CD(30), 인터넷(40) 등의 데이터 제공 수단으로부터 취득한 프로그램, 음성 데이터, 영상 데이터 등[콘텐츠(Content)]을 재생함과 함께, DVD, CD(30), 인터넷(40) 등으로부터 취득한 데이터를 플로피 디스크, 메모리 카드, 하드디스크 등의 기억 수단(20)에 기억 가능하게 한 구성예를 나타내는 것이다.

프로그램, 음성 데이터, 영상 데이터 등의 콘텐츠는 암호화 처리가 이루어지고, 재생 수단(10)을 갖는 사용자에게 제공된다. 정규 사용자는 암호화 데이터와 함께 그 암호화, 복호화 키인 키 데이터를 취득한다.

재생 수단(10)은 CPU(12)를 구비하고, 입력 데이터의 재생 처리를 재생 처리부(14)에서 실행한다. 재생 처리부(14)는 암호화 데이터의 복호 처리를 실행하여 제공된 프로그램의 재생, 음성 데이터, 화상 데이터 등 콘텐츠 재생을 행한다.

정규 사용자는 제공된 프로그램을 다시 사용하기 위해서 기억 수단(20)에 프로그램/데이터 등, 콘텐츠 보존 처리를 행한다. 재생 수단(10)에는 콘텐츠 보존 처리를 실행하기 위한 보존 처리부(13)를 갖는다. 보존 처리부(13)는 기억 수단(20)에 기억된 데이터의 부정 사용을 방지하기 위해서 데이터에 암호화 처리를 실시하여 보존 처리를 실행한다.

콘텐츠를 암호화할 때에는 콘텐츠 암호용 키를 이용한다. 보존 처리부(13)는 콘텐츠 암호용 키를 이용하여 콘텐츠를 암호화하고, 그것을 FD(플로피 디스크), 메모리 카드, 하드디스크 등의 기억 수단(20)의 기억부(21)에 기억한다.

사용자는 기억 수단(20)으로부터 저장 콘텐츠를 추출하여 재생하는 경우에는 기억 수단(20)으로부터 암호화 데이터를 추출하여 재생 수단(10)의 재생 처리부 (14)에 있어서, 콘텐츠 복호용 키, 즉 복호화 키를 이용해서 복호 처리를 실행하여 암호화 데이터로부터 복호 데이터를 취득하여 재생한다.

도 1에 도시한 종래의 구성에에 따르면, 플로피 디스크, 메모리 카드 등의 기억 수단(20)에서는 저장 콘텐츠가 암호화되어 있기 때문에, 외부로부터의 부정 판독은 방지할 수 있다. 그러나, 이 플로피 디스크를 다른 PC, 게임 기기 등의 정보 기기의 재생 수단으로 재생하여 이용하고자 하면, 동일한 콘텐츠 키, 즉 암호화된 콘텐츠를 복호하기 위한 동일한 복호화 키를 갖는 재생 수단이 아니면 재생 불가능하게 된다. 따라서, 복수의 정보 기기에 있어서 이용 가능한 형태를 실현하기 위해서는 사용자에게 제공하는 암호 키를 공통화해 둘 필요가 있다.

그러나, 콘텐츠의 암호 키를 공통화한다는 것은 정규 라이센스를 갖지 않은 사용자에게 암호 처리용 키를 불법 유통시킬 가능성을 높이게 되고, 정규 라이센스를 갖지 않은 사용자에 의한 콘텐츠의 부정 이용을 방지할 수 없게 된다고 하는 결점이 있어, 정규 라이센스를 갖지 않은 PC, 게임 기기 등에서의 부정 이용의 배제가 곤란하게 된다.

또한, 콘텐츠의 암호 키, 복호 키를 공통화한다는 것은 하나의 기기로부터 만일 그 키 정보가 누설된 경우, 피해 범위는 그 키를 이용하고 있는 시스템 전체가 된다.

또한, 상술된 바와 같이 키를 공통화한 환경에서는 예를 들면 임의의 PC 상에서 작성되고, 메모리 카드, 플로피 디스크 등의 기억 수단에 보존된 암호화된 콘텐츠는 다른 플로피 디스크에 용이하게 복제할 수 있고, 오리지널 콘텐츠 데이터가 아닌 복제 플로피 디스크를 이용한 이용 형태가 가능하게 되고, 게임 기기, PC 등의 정보 기기에 있어서 이용 가능한 콘텐츠 데이터가 다수 복제되거나 변경될 가능성이 있었다.

콘텐츠 데이터의 정당성, 즉 데이터가 변경되어 있지 않은 것을 체크하기 위해서 검증용 체크치를 콘텐츠 데이터에 포함시키고, 기록 재생기에 있어서, 검증 대상의 데이터에 기초하여 생성된 체크치와 콘텐츠 데이터에 포함되는 체크치를 대조 처리함으로써, 데이터 검증을 행하는 방법이 종래부터 행해져 왔다.

그러나, 데이터 콘텐츠에 대한 체크치는 데이터 전체에 생성되는 것이 일반적이고, 데이터 전체에 생성된 체크치의 대조 처리를 실행하기 위해서는 체크 대상이 된 데이터 전체에 대한 체크치 생성 처리를 실행할 필요가 있다. 예를 들면, DES-CBC 모드에 있어서 생성되는 메세지 인증 부호(MAC)에 의해 체크치 ICV를 구하는 방법을 행하는 경우, 데이터 전체에 대한 DES-CBC 처리를 실행할 필요가 있다. 이 계산량은 데이터 길이가 길어짐에 따라 증대하게 되어, 처리 효율 측면에서 문제가 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 이러한 종래 기술의 문제점을 해결하는 것으로서, 본 발명의 구성에 있어서는 사전에 기록 디바이스에 복수의 다른 키 세트로서의 키 블록이 저장되어 있다. 기록 재생기는 예를 들면 제품 발송처(국가)별, 또는 제품, 기종, 버전, 어플리케이션별, 인증 처리에 적용해야 할 키 블록, 즉 지정 키 블록이 설정되고, 데이터 전송을 실행하는 두 개의 장치 사이에 있어서, 콘텐츠의 이용 제한을 고려한 장치 간의 인증 처리, 콘텐츠의 저장 처리를 가능하게 한다.

또한, 인증 처리와, 콘텐츠의 이용 처리를 어느 정도 관련시키는지, 즉 인증 처리의 수속을 콘텐츠의 복호 처리, 또는 저장 처리와 어느 정도 밀접 불가분한 수속으로서 실행시키는지에 대해서도 패스워드를 이용한 사용자 인증 등은 가능하지만, 기록 재생기, 또는 기록 디바이스 등 기기에 대한 인증 처리와 콘텐츠 이용 처리를 관련시켜서 콘텐츠의 부정 이용을 배제한 구성은 실현되지 않는다.

예를 들면, 다른 기록 재생기에 있어서, 패스워드 입력 등에 의해 인증 처리를 실행하면, 복수의 다른 기기에 있어서도 콘텐츠가 이용되고, 이러한 콘텐츠의 유용을 방지하기 위해서는 기기 그 자체에 대한 인증 처리와 콘텐츠 이용 처리를 관련시키는 처리가 필요하다.

본 발명은 이러한 문제점을 해결하는 것으로서, 본 발명의 구성에 있어서는 기록 디바이스에 있어서의 인증 처리, 저장 데이터의 암호 처리 등을 소정의 시퀀스에 따라 실행하도록 규정함으로써, 기기의 인증이 실행되지 않은 콘텐츠의 외부 장치로부터의 판독 등, 콘텐츠 이용을 방지하는 데이터 처리 시스템, 기록 디바이스 및 처리 방법을 제공한다.

또한, 종래의 게임 기기, PC 등의 기록 재생기에 있어서의 세이브 데이터 보존 구성은 예를 들면, 기록 재생기에 저장, 또는 외부 부착 가능한 메모리 카드, 플로피 디스크, 게임 카트리지, 또는 하드 디스크 등의 기억 매체에 세이브 데이터를 보존하는 구성을 갖지만, 특히 그 세이브 데이터에 대한 시큐러티 확인 구성을 갖지 않고, 예를 들면 게임 어플리케이션 프로그램에 공통의 사양으로 데이터의 세이브 처리가 행해지는 구성으로 되어 있다.

따라서, 예를 들면, 어느 하나의 기록 재생기 A를 이용하여 세이브된 세이브 데이터가 다른 게임 프로그램에 의해 사용되거나, 기입되거나, 덧씌우기되거나 하는 사태가 발생하고, 세이브 데이터의 시큐러티는 거의 고려되지 않았다.

본 발명의 데이터 기록 재생기는 이와 같은 세이브 데이터의 시큐러티 확보를 실현 가능하게 한 구성을 제공한다. 예를 들면, 임의의 게임 프로그램의 세이브 데이터는 그 게임 프로그램에만 고유한 정보에 기초하여 암호화되어 기록 디바이스에 저장한다. 또는 기록 재생기 고유의 정보에 기초하여 암호화되어 기록 디바이스에 저장한다. 이들 방법에 의해, 세이브 데이터의 방법을 적용함으로써 세이브 데이터의 시큐러티를 확보 가능하게 한 데이터 기록 재생기 및 세이브 데이터 처리 방법을 제공한다.

본 발명의 과제를 해결하기 위한 본 발명의 제1 국면은, 서로 암호 데이터의 전송을 실행하는 기록 재생기와 기록 디바이스를 포함하는 데이터 처리 시스템에 있어서, 상기 기록 디바이스는 기록 재생기와 기록 디바이스 사이에서 전송 가능한 콘텐츠 데이터를 기억하는 데이터 기억부를 구비함과 함께, 기록 재생기와 기록 디바이스 사이의 적어도 인증 처리에 적용 가능한 키 데이터를 저장한 키 블록을 복수 갖고, 상기 복수의 키 블록에 저장된 키 데이터는 각 블록마다 다른 키 데이터를 저장한 구성을 갖고, 상기 기록 재생기는 기록 재생기와 기록 디바이스 사이의 인증 처리에 있어서 상기 기록 디바이스가 갖는 복수의 키 블록으로부터 하나의 키 블록을 지정하고, 지정 키 블록에 저장된 키 데이터에 기초하여 상기 기록 디바이스와의 인증 처리를 실행하는 구성을 갖는 것을 특징으로 하는 데이터 처리 시스템에 있다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록 각각에는 적어도 인증 처리에 적용 가능한 인증 키를 포함하고, 각 키 블록의 인증 키는 서로 다른 키 데이터로 구성되어 있는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 재생기는 인증 처리에 적용해야 할 키 블록을 지정 키 블록으로서 설정한 설정 정보를 기록 재생기내 메모리에 보유하고, 상기 기록 재생기는 기록 재생기와 기록 디바이스 사이의 인증 처리에 있어서 기록 재생기내 메모리에 보유된 설정 정보에 기초하여 상기 기록 디바이스가 갖는 복수의 키 블록으로부터 하나의 키 블록을 지정하여 인증 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 재생기의 지정 키 블록 설정 정보는 기록 재생기의 기종 또는 버전 또는 출하처 등의 소정 제품 단위마다 다르게 설정된 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 재생기는 상기 기록 디바이스와의 인증 처리에 필요한 인증 처리용 키 데이터를 기록 재생기내 메모리에 저장한 구성을 갖고, 상기 기록 재생기내 메모리에 저장된 인증 처리용 키 데이터는 상기 기록 디바이스의 복수의 키 블록의 일부의 키 블록에만 저장된 블록내 키 데이터를 사용한 인증 처리에 있어서만 인증이 성립하고, 다른 키 블록내 키 데이터를 이용한 인증 처리에 있어서는 인증이 성립하지 않은 키 데이터인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 재생기는 기록 디바이스 인증 키용 마스터 키 MK_{ake}를 기록 재생기내 메모리에 저장하고, 상기 기록 디바이스 인증 키용 마스터 키 MK_{ake}에 기초하여 생성되는 인증 키 K_{ake}는 상기 기록 재생기에 설정된 지정 키 블록 내의 키 데이터를 사용한 인증 처리에 있어서만 인증이 성립하고, 다른 키 블록내 키 데이터를 이용한 인증 처리에 있어서는 인증이 성립하지 않은 인증 키인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스는 상기 기록 디바이스내 메모리에 기록 디바이스 식별 정보 ID_{mem}을 보유함과 함께, 상기 복수의 키 블록의 각각에 키 블록마다 다른 인증 키 K_{ake}를 저장한 구성을 갖고, 상기 기록 재생기는 기록 재생기내 메모리에 저장된 기록 디바이스 인증 키용 마스터 키 MK_{ake}에 기초한 상기 기록 디바이스 식별 정보 ID_{mem}의 암호 처리에 의해 인증 키 K_{ake}를 생성하고, 상기 생성된 인증 키 K_{ake}를 이용하여 상기 기록 디바이스의 지정 키 블록과의 인증 처리를 행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스의 키 블록의 각각에는 기록 디바이스의 고유 정보인 기록 디바이스 식별자 정보, 기록 재생기 사이와의 인증 처리에 있어서 사용되는 인증 키 및 난수 생성 키, 또한 상기 데이터 기억부에 대한 저장 데이터의 암호화 처리에 이용되는 보존 키를 포함하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록의 각각에 저장된 상기 보존 키는 각 키 블록마다 다른 키 데이터임과 함께 상기 데이터 기억부의 저장 데이터에 대한 암호 처리에 이용되는 키이고, 상기 기록 디바이스는 기록 디바이스 외부로부터 보존 키로 암호화된 데이터의 이용 요구가 있었던 경우에는 기록 디바이스내에서 보존 키의 키 교환 처리를 실행하여 보존 키와 다른 키에 의한 암호화 데이터를 기록 디바이스 외부로 출력하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스는 암호 처리부를 구비하고, 상기 암호 처리부는 상기 기록 재생기로부터 수신하는 키 블록 지정 정보에 따라 기록 디바이스의 복수의 키 블록의 하나의 키 블록을 선택하고, 상기 선택 키 블록 내의 키 데이터를 이용하여 상기 기록 재생기와의 인증 처리를 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스에 있어서의 암호 처리부는 기록 재생기와 기록 디바이스 사이에서 전송 가능한 콘텐츠 데이터를 기억한 데이터 기억부에 대한 데이터 저장 처리 및 데이터 기억부로부터의 데이터 전송 처리에 있어서 실행하는 암호 처리를 상기 기록 재생기로부터 수신하는 키 블록 지정 정보에 따라 선택한 하나의 키 블록 내의 키 데이터를 이용하여 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 재생기의 지정 가능한 상기 기록 디바이스의 키 블록은 복수이고, 상기 복수의 지정 가능한 키 블록 중의 적어도 하나의 키 블록은 다른 기록 재생기에 있어서도 지정 가능한 공통 지정 가능한 키 블록으로 구성되어 있는 것을 특징으로 한다.

또한, 본 발명의 제2 국면은, 외부 장치와의 사이에서 전송 가능한 콘텐츠 데이터를 기억하는 데이터 기억부를 구비하는 기록 디바이스에 있어서, 기록 디바이스와 상기 외부 장치 사이의 적어도 인증 처리에 적용 가능한 키 데이터를 저장한 키 블록을 복수 갖고, 상기 복수의 키 블록에 저장된 키 데이터는 각 블록마다 다른 키 데이터를 저장한 구성을 갖는 것을 특징으로 하는 기록 디바이스에 있다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록 각각에는 적어도 인증 처리에 적용 가능한 인증 키를 포함하고, 각 키 블록의 인증 키는 서로 다른 키 데이터로 구성되어 있는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스내 메모리에 기록 디바이스 식별 정보 ID_{mem}을 보유함과 함께, 상기 복수의 키 블록의 각각에 키 블록마다 다른 인증 키 K_{ake}를 저장한 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스의 키 블록의 각각에는 기록 디바이스의 고유 정보인 기록 디바이스 식별자 정보, 상기 외부 장치와의 인증 처리에 있어서 사용되는 인증 키 및 난수 생성 키, 또한 상기 데이터 기억부에 대한 저장 데이터의 암호화 처리에 이용되는 보존 키를 포함하는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록의 각각에 저장된 상기 보존 키는 각 키 블록마다 다른 키 데이터임과 함께 상기 데이터 기억부의 저장 데이터에 대한 암호 처리에 이용되는 키이고, 상기 기록 디바이스는 기록 디바이스 외부로부터 보존 키로 암호화된 데이터의 이용 요구가 있었던 경우에는 기록 디바이스내에서 보존 키의 키 교환 처리를 실행하여 보존 키와 다른 키에 의한 암호화 데이터를 기록 디바이스 외부로 출력하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스는 암호 처리부를 구비하고, 상기 암호 처리부는 상기 외부 장치로부터 수신하는 키 블록 지정 정보에 따라 기록 디바이스의 복수의 키 블록의 하나의 키 블록을 선택하고, 상기 선택 키 블록 내의 키 데이터를 이용하여 상기 기록 재생기와의 인증 처리를 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스에 있어서의 암호 처리부는 상기 외부 장치와 기록 디바이스 사이에서 전송 가능한 콘텐츠 데이터를 기억한 데이터 기억부에 대한 데이터 저장 처리 및 데이터 기억부로부터의 데이터 전송 처리에 있어서 실행하는 암호 처리를 상기 외부 장치로부터 수신하는 키 블록 지정 정보에 따라 선택한 하나의 키 블록 내의 키 데이터를 이용하여 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 제3 국면은, 서로 암호 데이터의 전송을 실행하는 기록 재생기와 기록 디바이스를 포함하는 데이터 처리 시스템에 있어서의 데이터 처리 방법에 있어서, 기록 재생기가, 기록 디바이스가 갖는 복수의 키 블록으로부터 하나의 키 블록을 지정하여, 지정 키 블록에 저장된 키 데이터에 기초하여 상기 기록 디바이스와의 인증 처리를 실행하는 것을 특징으로 하는 데이터 처리 방법에 있다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록 각각에는 적어도 인증 처리에 적용 가능한 인증 키를 포함하고, 각 키 블록의 인증 키는 서로 다른 키 데이터로 구성되어 있는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 재생기는 기록 재생기와 기록 디바이스 사이의 인증 처리에 있어서 기록 재생기내 메모리에 보유된 설정 정보에 기초하여 상기 기록 디바이스가 갖는 복수의 키 블록으로부터 하나의 키 블록을 지정하여 인증 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 재생기는 기록 디바이스 인증 키용 마스터 키 MK_{ake}를 기록 재생기내 메모리에 저장하고, 상기 기록 디바이스 인증 키용 마스터 키 MK_{ake}에 기초하여 인증 키 K_{ake}를 생성하고, 생성된 인증 키 K_{ake}를 이용하여 상기 기록 디바이스가 갖는 복수의 키 블록 중의 지정 키 블록 내의 키 데이터를 사용한 인증 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 디바이스는 상기 기록 디바이스내 메모리에 기록 디바이스 식별 정보 ID_{mem}을 보유함과 함께, 상기 복수의 키 블록의 각각에 키 블록마다 다른 인증 키 K_{ake}를 저장한 구성을 갖고, 상기 기록 재생기는 기록 재생기내 메모리에 저장된 기록 디바이스 인증 키용 마스터 키 MK_{ake}에 기초한 상기 기록 디바이스 식별 정보 ID_{mem}의 암호 처리를 실행하여 인증 키 K_{ake}를 생성하고, 생성된 인증 키 K_{ake}를 이용하여 상기 기록 디바이스의 지정 키 블록과의 인증 처리를 행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 디바이스는 상기 기록 재생기로부터 수신하는 키 블록 지정 정보에 따라 기록 디바이스의 복수의 키 블록의 하나의 키 블록을 선택하고, 상기 선택 키 블록 내의 키 데이터를 이용하여 상기 기록 재생기와의 인증 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 디바이스는 기록 재생기와 기록 디바이스 사이에서 전송 가능한 콘텐츠 데이터를 기억한 데이터 기억부에 대한 데이터 저장 처리 및 데이터 기억부로부터의 데이터 전송 처리에 있어서 실행하는 암호 처리를 상기 기록 재생기로부터 수신하는 키 블록 지정 정보에 따라 선택한 하나의 키 블록 내의 키 데이터를 이용하여 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 기록 디바이스의 복수의 키 블록의 각각에는 상기 기록 디바이스 내의 데이터 기억부의 저장 데이터의 암호 처리에 이용되는 보존 키를 포함하고, 기록 디바이스 외부로부터 보존 키로 암호화된 데이터의 이용 요구가 있었던 경우, 기록 디바이스내에서 보존 키의 키 교환 처리를 실행하여 보존 키와 다른 키에 의한 암호화 데이터를 기록 디바이스 외부로 출력하는 것을 특징으로 한다.

또한, 본 발명의 제4 국면은, 서로 암호 데이터의 전송을 실행하는 기록 재생기와 기록 디바이스를 포함하는 데이터 처리 시스템에 있어서의 데이터 처리 방법을 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램을 제공하는 프로그램 제공 매체에 있어서, 상기 컴퓨터 프로그램은 기록 재생기가 기록 디바이스가 갖는 복수의 키 블록으로부터 하나의 키 블록을 지정하여, 지정 키 블록에 저장된 키 데이터에 기초하여 상기 기록 디바이스와의 인증 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 프로그램 제공 매체에 있다.

또한, 본 발명의 제5 국면은, 서로 암호 데이터의 전송을 실행하는 제1 장치와 제2 장치를 포함하는 데이터 처리 시스템에 있어서, 상기 제2 장치는 상기 제1 장치와의 전송 데이터에 관한 암호 처리를 실행하는 암호 처리부를 구비하고, 상기 암호 처리부는 상기 제1 장치로부터 전송되는 커맨드 식별자를 사전에 정해진 설정 시퀀스에 따라 수령하고, 상기 수령 커맨드

식별자에 대응하는 커맨드를 레지스터로부터 추출하여 실행시키는 제어부를 구비하고, 상기 제어부는 상기 제1 장치로부터 전송되는 커맨드 식별자가 상기 설정 시퀀스와 다른 커맨드 식별자인 경우에는 상기 커맨드 식별자에 대응하는 커맨드의 처리를 중지하는 구성을 갖는 것을 특징으로 하는 데이터 처리 시스템에 있다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 제어부가 갖는 상기 제1 장치로부터 수령하는 커맨드 식별자에 관한 설정 시퀀스는 순차, 번호가 인클리먼트되는 커맨드 번호 설정 시퀀스이고, 상기 제어부는 상기 제1 장치로부터의 수령 커맨드 번호의 접수치를 메모리에 저장함과 함께, 상기 제1 장치로부터의 신규 수령 커맨드 번호를 상기 메모리에 저장된 접수가 끝난 커맨드 번호에 기초하여 설정 시퀀스와의 일치를 판정하여, 설정 시퀀스와 다르다고 판정된 경우에는 상기 신규 수령 커맨드 번호에 대응하는 커맨드 처리를 행하지 않고, 상기 메모리에 저장한 커맨드 번호의 리세트를 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 제2 장치는 상기 설정 시퀀스에 따른 커맨드를 저장한 커맨드 레지스터를 구비하고, 상기 커맨드 레지스터에는 상기 제1 장치와 상기 제2 장치와의 인증 처리를 실행하는 인증 처리 커맨드 시퀀스와, 상기 제1 장치와 상기 제2 장치 사이에서의 전송 데이터에 관한 암호 처리를 실행하는 암호 처리 커맨드 시퀀스가 저장되어 있으며, 상기 인증 처리 커맨드 시퀀스에 대응하는 커맨드 식별자는 상기 암호 처리 커맨드 시퀀스에 대응하는 커맨드 식별자보다 이전의 단계에 있어서 실행되도록 시퀀스 설정이 이루어져 있는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 암호 처리 커맨드 시퀀스는 상기 제1 장치로부터 상기 제2 장치에 대하여 전송되고, 상기 제2 장치 내의 기억 수단에 저장되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 및 상기 제2 장치 내의 기억 수단에 저장되고, 상기 제2 장치로부터 상기 제1 장치에 대하여 전송되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 적어도 상기 어느 하나의 커맨드 시퀀스를 포함하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 제어부는 상기 제1 장치와 상기 제2 장치와의 인증 처리에 의해 인증이 성립한 경우에, 인증 완료를 나타내는 인증 플래그를 설정하고, 상기 인증 플래그가 설정되어 있는 동안은 상기 암호 처리 커맨드 시퀀스의 실행을 가능하게 하는 커맨드 관리 제어를 실행하고, 상기 제어부는 상기 인증 처리 커맨드 시퀀스를 새롭게 실행할 때 상기 인증 플래그를 리세트하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 제어부는 상기 암호 키 교환 처리에 있어서 상기 설정 시퀀스 및 커맨드 식별자에 기초하여 커맨드 실행 순서를 관리하고, 상기 제어부는 상기 키 교환 처리에 관한 일련의 커맨드 실행 중에는 상기 제1 장치를 포함하는 외부 장치로부터의 상기 설정 시퀀스와 다른 커맨드 처리를 접수하지 않은 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 제2 장치는 암호화 데이터를 기억하는 데이터 기억부를 갖는 기억 디바이스이고, 상기 제1 장치는 상기 기억 디바이스에 대한 데이터의 저장 처리 및 상기 기억 디바이스에 저장된 데이터를 추출하여 재생, 실행을 행하는 기록 재생기이고, 상기 기록 재생기는 상기 기록 디바이스와의 전송 데이터의 암호 처리를 실행하는 암호 처리부를 포함하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 기록 디바이스는 상기 기록 재생기와 기록 디바이스 사이의 인증 처리에 적용하는 인증 키 및 상기 기록 디바이스 내의 데이터 기억부에 저장하는 데이터의 암호화 키로서의 보존 키를 저장한 키 블록을 갖고, 상기 기록 디바이스의 암호 처리부에서의 상기 제어부는 상기 기록 재생기로부터 상기 설정 시퀀스에 따라 커맨드 식별자를 수령하여 상기 키 블록에 저장한 인증 키를 이용한 인증 처리를 실행하고, 상기 인증 처리 완료 후에 상기 보존 키를 이용한 키 교환 처리를 따른 데이터의 암호 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 시스템의 일실시예에 있어서, 상기 키 블록은 각각 다른 인증 키 및 보존 키를 저장한 복수의 키 블록을 포함하고, 상기 기록 재생기는 상기 복수의 키 블록으로부터 인증 처리 및 데이터의 암호 처리에 사용하는 하나의 키 블록을 지정 키 블록으로서 상기 기록 디바이스에 통지하고, 상기 기록 디바이스는 지정 키 블록에 저장된 인증 키를 이용한 인증 처리, 및 보존 키를 이용한 데이터의 암호 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 제6 국면은, 외부 장치와의 사이에서 전송 가능한 콘텐츠 데이터를 기억하는 데이터 기억부를 갖는 기록 디바이스에 있어서, 상기 기록 디바이스는 외부 장치와의 전송 데이터에 관한 암호 처리를 실행하는 암호 처리부를 구비하고, 상기 암호 처리부는 외부 장치로부터 전송되는 커맨드 식별자를 사전에 정해진 설정 시퀀스에 따라 수령하고, 상기 수

령 커맨드 식별자에 대응하는 커맨드를 레지스터로부터 추출하여 실행시키는 제어부를 구비하고, 상기 제어부는 상기 외부 장치로부터 전송되는 커맨드 식별자가 상기 설정 시퀀스와 다른 커맨드 식별자인 경우에는 상기 커맨드 식별자에 대응하는 커맨드의 처리를 중지하는 구성을 갖는 것을 특징으로 하는 기록 디바이스에 있다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 제어부는 상기 설정 시퀀스로서, 순차, 번호가 인클리먼트되는 커맨드 번호 설정 시퀀스를 구비하고, 상기 제어부는 상기 외부 장치로부터의 수령 커맨드 번호의 접수치를 메모리에 저장함과 함께, 상기 외부 장치로부터의 신규 수령 커맨드 번호를 상기 메모리에 저장된 접수 완료된 커맨드 번호에 기초하여 설정 시퀀스와의 일치를 판정하여, 설정 시퀀스와 다르다고 판정된 경우에는 상기 신규 수령 커맨드 번호에 대응하는 커맨드 처리를 행하지 않고, 상기 메모리에 저장한 커맨드 번호의 리세트를 실행하는 구성을 갖는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스는 상기 설정 시퀀스에 따른 커맨드를 저장한 커맨드 레지스터를 구비하고, 상기 커맨드 레지스터에는 상기 외부 장치와 상기 기록 디바이스와의 인증 처리를 실행하는 인증 처리 커맨드 시퀀스와, 상기 외부 장치와 상기 기록 디바이스 사이에서의 전송 데이터에 관한 암호 처리를 실행하는 암호 처리 커맨드 시퀀스가 저장되어 있으며, 상기 인증 처리 커맨드 시퀀스에 대응하는 커맨드 식별자는 상기 암호 처리 커맨드 시퀀스에 대응하는 커맨드 식별자보다 이전의 단계에 있어서 실행되도록 시퀀스 설정이 이루어져 있는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 암호 처리 커맨드 시퀀스는 상기 외부 장치로부터 상기 기록 디바이스에 대하여 전송되고, 상기 기록 디바이스 내의 기억 수단에 저장되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 및 상기 기록 디바이스 내의 기억 수단에 저장되고, 상기 기록 디바이스로부터 상기 외부 장치에 대하여 전송되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 적어도 상기 어느 하나의 커맨드 시퀀스를 포함하는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 제어부는 상기 외부 장치와 상기 기록 디바이스와의 인증 처리에 의해 인증이 성립한 경우에, 인증 완료를 나타내는 인증 플래그를 설정하고, 상기 인증 플래그가 설정되어 있는 동안은 상기 암호 처리 커맨드 시퀀스의 실행을 가능하게 하는 커맨드 관리 제어를 실행하고, 상기 제어부는 상기 인증 처리 커맨드 시퀀스를 새롭게 실행할 때 상기 인증 플래그를 리세트하는 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 제어부는 상기 암호 키 교환 처리에 있어서 상기 설정 시퀀스 및 커맨드 식별자에 기초하여 커맨드 실행 순서를 관리하고, 상기 제어부는 상기 키 교환 처리에 관한 일련의 커맨드 실행 중에는 상기 외부 장치를 포함하는 외부 장치로부터의 상기 설정 시퀀스와 다른 커맨드 처리를 접수하지 않는 구성인 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 기록 디바이스는 상기 외부 장치와 기록 디바이스 사이의 인증 처리에 적용하는 인증 키 및 상기 기록 디바이스 내의 데이터 기억부에 저장하는 데이터의 암호화 키로서의 보존 키를 저장한 키 블록을 갖고, 상기 기록 디바이스의 암호 처리부에서의 상기 제어부는 상기 외부 장치로부터 상기 설정 시퀀스에 따라 커맨드 식별자를 수령하여 상기 키 블록에 저장한 인증 키를 이용한 인증 처리를 실행하고, 상기 인증 처리 완료 후에 상기 보존 키를 이용한 키 교환 처리를 따른 데이터의 암호 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 기록 디바이스의 일실시예에 있어서, 상기 키 블록은 각각 다른 인증 키 및 보존 키를 저장한 복수의 키 블록을 포함하고, 상기 외부 장치는 상기 복수의 키 블록으로부터 인증 처리 및 데이터의 암호 처리에 사용하는 하나의 키 블록을 지정 키 블록으로서 상기 기록 디바이스에 통지하고, 상기 기록 디바이스는 지정 키 블록에 저장된 인증 키를 이용한 인증 처리 및 보존 키를 이용한 데이터의 암호 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 제7 국면은, 서로 암호 데이터의 전송을 실행하는 제1 장치와 제2 장치를 포함하는 데이터 처리 시스템에 있어서의 데이터 처리 방법에 있어서, 상기 제2 장치는 상기 제1 장치로부터 전송되는 커맨드 식별자를 사전에 정해진 설정 시퀀스에 따라 수령하고, 상기 수령 커맨드 식별자에 대응하는 커맨드를 레지스터로부터 추출하여 실행시키는 커맨드 처리 제어 단계를 실행하고, 상기 커맨드 처리 제어에 있어서 상기 제1 장치로부터 전송되는 커맨드 식별자가 상기 설정 시퀀스와 다른 커맨드 식별자인 경우에는 상기 커맨드 식별자에 대응하는 커맨드의 처리를 중지하는 것을 특징으로 하는 데이터 처리 방법에 있다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 커맨드 처리 제어 단계에 있어서, 상기 제1 장치로부터 수령하는 커맨드 식별자에 관한 설정 시퀀스는 순차, 번호가 인클리먼트되는 커맨드 번호 설정 시퀀스이고, 상기 커맨드 처리 제어 단계는 상기 제1 장치로부터의 수령 커맨드 번호의 접수치를 메모리에 저장하는 단계와, 상기 제1 장치로부터의 신

규 수령 커맨드 번호를 상기 메모리에 저장된 접수가 완료된 커맨드 번호에 기초하여 설정 시퀀스와의 일치를 판정하는 판정 단계와, 상기 판정 단계에 있어서 설정 시퀀스와 다르다고 판정된 경우에는 상기 신규 수령 커맨드 번호에 대응하는 커맨드 처리를 행하지 않고, 상기 메모리에 저장한 커맨드 번호의 리세트를 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 커맨드 처리 제어 단계는 상기 제1 장치와 상기 제2 장치와의 인증 처리를 실행하는 인증 처리 커맨드 시퀀스와, 상기 제1 장치와 상기 제2 장치 사이에서의 전송 데이터에 관한 암호 처리를 실행하는 암호 처리 커맨드 시퀀스를 실행하는 단계이고, 상기 설정 시퀀스는 상기 인증 처리 커맨드 시퀀스를 상기 암호 처리 커맨드 시퀀스에 선행하여 실행하는 시퀀스인 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 암호 처리 커맨드 시퀀스는 상기 제1 장치로부터 상기 제2 장치에 대하여 전송되고, 상기 제2 장치 내의 기억 수단에 저장되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 및 상기 제2 장치 내의 기억 수단에 저장되고, 상기 제2 장치로부터 상기 제1 장치에 대하여 전송되는 암호화 데이터에 대한 암호 키 교환 처리를 포함하는 커맨드 시퀀스, 적어도 상기 어느 하나의 커맨드 시퀀스를 포함하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 제1 장치와 상기 제2 장치와의 인증 처리에 의해 인증이 성립한 경우에 인증이 완료됨을 나타내는 인증 플래그를 설정하는 인증 플래그 설정 단계를 포함하고, 상기 커맨드 처리 제어 단계는 상기 인증 플래그가 설정되어 있는 동안은 상기 암호 처리 커맨드 시퀀스의 실행을 가능하게 하는 커맨드 관리 제어를 실행하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 인증 처리 커맨드 시퀀스를 새롭게 실행할 때 상기 인증 플래그를 리세트하는 것을 특징으로 한다.

또한, 본 발명의 데이터 처리 방법의 일실시예에 있어서, 상기 데이터 처리 방법에 있어서의 상기 커맨드 처리 제어 단계에 있어서, 상기 키 교환 처리에 관한 일련의 커맨드 실행 중에는 상기 설정 시퀀스 및 커맨드 식별자에 기초하여 커맨드 실행 순서를 관리하고, 상기 제1 장치를 포함하는 외부 장치로부터의 상기 설정 시퀀스와 다른 커맨드 처리를 접수하지 않는 것을 특징으로 한다.

또한, 본 발명의 제8 국면은, 서로 암호 데이터의 전송을 실행하는 제1 장치와 제2 장치를 포함하는 데이터 처리 시스템에 있어서의 데이터 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램을 제공하는 프로그램 제공 매체에 있어서, 상기 제1 장치로부터 상기 제2 장치에 전송되는 커맨드 식별자를 사전에 정해진 설정 시퀀스에 따라 수령하고, 상기 수령 커맨드 식별자에 대응하는 커맨드를 레지스터로부터 추출하여 실행시키는 커맨드 처리 제어 단계를 갖고, 상기 커맨드 처리 제어 단계에 있어서 상기 제1 장치로부터 전송되는 커맨드 식별자가 상기 설정 시퀀스와 다른 커맨드 식별자인 경우에는 상기 커맨드 식별자에 대응하는 커맨드의 처리를 중지하는 단계를 포함하는 것을 특징으로 하는 프로그램 제공 매체에 있다.

본 발명의 제9 국면은, 프로그램 콘텐츠를 재생 실행 가능한 데이터 기록 재생기에 있어서, 상기 프로그램 콘텐츠에 관한 세이브 데이터를 기록하는 기록 디바이스와, 상기 기록 디바이스에 대한 저장 세이브 데이터의 암호화 처리 및 상기 기록 디바이스로부터 재생하는 재생 세이브 데이터의 복호화 처리를 실행하는 암호 처리부와, 세이브 데이터의 사용 제한 정보를 입력하는 입력 수단과, 세이브 데이터의 암호화 처리 방법 및 복호화 처리 방법을 결정하는 제어부를 포함하고, 상기 제어부는 상기 입력 수단으로부터의 입력 사용 제한 정보에 따라 상기 기록 디바이스에 대하여 저장하는 세이브 데이터의 암호화 처리 방법을 결정함과 함께, 상기 제어부가 액세스 가능한 기억부 또는 기록 디바이스에 저장한 데이터 관리 파일에 설정된 세이브 데이터 사용 제한 정보에 따라 상기 기록 디바이스로부터 재생하는 세이브 데이터의 복호화 처리 방법을 결정하는 구성을 갖고, 상기 암호 처리부는, 상기 제어부가 결정한 암호화 처리 방법 또는 복호화 처리 방법에 따라 다른 암호 키를 이용하여 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하는 구성을 갖는 것을 특징으로 하는 데이터 기록 재생기에 있다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 콘텐츠 프로그램의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 프로그램 제한이고, 상기 데이터 관리 파일은 콘텐츠 프로그램의 식별자에 대응시켜서 프로그램 제한 정보를 저장한 테이블로 구성되고, 상기 암호화 처리부는 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 프로그램 제한 있음의 입력 또는 설정인 경우, 상기 콘텐츠 프로그램에 고유의 암호 키, 또는 콘텐츠 프로그램에 고유의 암호 키 또는 고유의 정보의 적어도 어느 하나에 기초하여 생성되는 프로그램 고유 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를

실행하고, 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 프로그램 제한 없음의 입력 또는 설정인 경우, 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 콘텐츠 프로그램에 고유의 암호 키는 상기 콘텐츠 프로그램을 포함하는 콘텐츠 데이터의 헤더부에 저장된 콘텐츠 키 K_{con}이고, 상기 시스템 공통의 암호 키는 복수의 다른 데이터 기록 재생기에 공통으로 저장된 시스템 서명 키 K_{sys}인 것을 특징으로 한다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 데이터 기록 재생기의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 기록 재생기 제한으로서, 상기 데이터 관리 파일은 콘텐츠 프로그램의 식별자에 대응시켜서 기록 재생기 제한 정보를 저장한 테이블로 구성되고, 상기 암호 처리부는 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 기록 재생기 제한 있음의 입력 또는 설정인 경우, 상기 데이터 기록 재생기에 고유의 암호 키, 또는 데이터 기록 재생기에 고유의 암호 키 또는 고유의 정보 중 적어도 어느 하나에 기초하여 생성되는 기록 재생기 고유 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하고, 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 프로그램 제한 없음의 입력 또는 설정인 경우, 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 데이터 기록 재생기에 고유의 암호 키는 상기 데이터 기록 재생기에 저장된 상기 데이터 기록 재생기 고유의 서명 키 K_{dev}이고, 상기 시스템 공통의 암호 키는 복수의 데이터 기록 재생기에 공통으로 저장된 시스템 서명 키 K_{sys}인 것을 특징으로 한다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 사용자의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 사용자 제한으로서, 상기 데이터 관리 파일은 콘텐츠 프로그램의 식별자에 대응시켜서 사용자 제한 정보를 저장한 테이블로 구성되고, 상기 암호 처리부는 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 사용자 제한 있음의 입력 또는 설정인 경우, 상기 입력 수단으로부터 입력되는 패스워드, 또는 상기 패스워드에 기초하여 생성되는 사용자 고유 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하고, 상기 입력 수단으로부터의 입력 사용 제한 정보, 또는 상기 데이터 관리 파일의 설정 사용 제한 정보가 사용자 제한 없음의 입력 또는 설정인 경우, 상기 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키에 의해 세이브 데이터의 암호화 처리 또는 복호화 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 데이터 기록 재생기의 일실시예에 있어서, 상기 시스템 공통의 암호 키는 복수의 기록 재생기에 공통으로 저장된 시스템 서명 키 K_{sys}인 것을 특징으로 한다.

또한, 본 발명의 제10 국면은, 프로그램 콘텐츠를 재생 실행 가능한 데이터 기록 재생기에 있어서의 세이브 데이터 처리 방법에 있어서, 입력 수단으로부터의 입력 사용 제한 정보에 따라 기록 디바이스에 대하여 저장하는 세이브 데이터의 암호화 처리 형태를 결정하는 암호화 처리 형태 결정 단계와, 상기 암호화 처리 형태 결정 단계에 있어서 결정된 암호화 처리 형태에 따라 암호화 처리에 적용하는 암호화 키를 선택하는 암호화 키 선택 단계와, 상기 암호화 키 선택 단계에 있어서 선택된 암호화 키를 이용하여 세이브 데이터의 암호화 처리를 실행하는 것을 특징으로 하는 세이브 데이터 처리 방법에 있다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 콘텐츠 프로그램의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 프로그램 제한으로서, 프로그램 제한 있음의 경우에는 상기 암호화 키 선택 단계에 있어서, 상기 콘텐츠 프로그램에 고유의 암호 키, 또는 콘텐츠 프로그램에 고유의 암호 키 또는 고유의 정보 중 적어도 어느 하나에 기초하여 생성되는 프로그램 고유 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하고, 프로그램 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 데이터 기록 재생기의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 기록 재생기 제한으로서, 기록 재생기 제한 있음의

경우에는 상기 암호화 키 선택 단계에 있어서, 상기 데이터 기록 재생기에 고유의 암호 키, 또는 데이터 기록 재생기에 고유의 암호 키 또는 고유의 정보 중 적어도 어느 하나에 기초하여 생성되는 기록 재생기 고유 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하고, 기록 재생기 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 사용자의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 사용자 제한으로서, 사용자 제한 있음의 경우에는 상기 암호화 키 선택 단계에 있어서, 사용자 입력 패스워드, 또는 상기 패스워드에 기초하여 생성되는 사용자 고유 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하고, 기록 재생기 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 암호 키를 암호화 처리에 적용하는 암호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 제11 국면은, 프로그램 콘텐츠를 재생 실행 가능한 데이터 기록 재생기에 있어서의 세이브 데이터 처리 방법에 있어서, 기억 수단 또는 기록 디바이스에 저장된 데이터 관리 파일에 설정된 설정 사용 제한 정보에 따라 기록 디바이스로부터의 재생 세이브 데이터의 복호화 처리 형태를 결정하는 복호화 처리 형태 결정 단계와, 상기 복호화 처리 형태 결정 단계에 있어서 결정된 복호화 처리 형태에 따라 복호화 키를 선택하는 복호화 키 선택 단계와, 상기 복호화 키 선택 단계에 있어서 선택된 복호화 키를 이용하여 세이브 데이터의 복호화 처리를 실행하는 것을 특징으로 하는 세이브 데이터 처리 방법에 있다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 콘텐츠 프로그램의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 프로그램 제한으로서, 프로그램 제한 있음의 경우에는 상기 복호화 키 선택 단계에 있어서, 상기 콘텐츠 프로그램에 고유의 암호 키, 또는 콘텐츠 프로그램에 고유의 암호 키 또는 고유의 정보 중 적어도 어느 하나에 기초하여 생성되는 프로그램 고유 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하고, 프로그램 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 데이터 기록 재생기의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 기록 재생기 제한으로서, 기록 재생기 제한 있음의 경우에는 상기 복호화 키 선택 단계에 있어서, 상기 데이터 기록 재생기에 고유의 암호 키, 또는 데이터 기록 재생기에 고유의 암호 키 또는 고유의 정보 중 적어도 어느 하나에 기초하여 생성되는 기록 재생기 고유 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하고, 기록 재생기 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 세이브 데이터 처리 방법의 일실시예에 있어서, 상기 세이브 데이터의 사용 제한 정보는 사용자의 동일성을 조건으로 하여 세이브 데이터의 이용을 가능하게 하는 사용자 제한으로서, 사용자 제한 있음의 경우에는 상기 복호화 키 선택 단계에 있어서, 사용자 입력 패스워드, 또는 패스워드에 기초하여 생성되는 사용자 고유 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하고, 기록 재생기 제한 없음의 경우에는 상기 데이터 기록 재생기에 저장된 시스템 공통의 암호 키, 또는 시스템 공통의 암호 키에 기초하여 생성되는 공통 세이브 데이터 복호화 키를 복호화 처리에 적용하는 복호화 키로서 선택하는 것을 특징으로 한다.

또한, 본 발명의 제12 국면은, 프로그램 콘텐츠를 재생 실행 가능한 데이터 기록 재생기에 있어서의 세이브 데이터 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램을 제공하는 프로그램 제공 매체에 있어서, 상기 컴퓨터 프로그램은, 입력 수단으로부터의 입력 사용 제한 정보에 따라 기록 디바이스에 대하여 저장하는 세이브 데이터의 암호화 처리 형태를 결정하는 암호화 처리 형태 결정 단계와, 상기 암호화 처리 형태 결정 단계에 있어서 결정된 암호화 처리 형태에 따라 암호화 처리에 적용하는 암호화 키를 선택하는 암호화 키 선택 단계와, 상기 암호화 키 선택 단계에 있어서 선택된 암호화 키를 이용하여 세이브 데이터의 암호화 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 프로그램 제공 매체에 있다.

또한, 본 발명의 제13 국면은, 프로그램 콘텐츠를 재생 실행 가능한 데이터 기록 재생기에 있어서의 세이브 데이터 처리를 컴퓨터 시스템 상에서 실행시키는 컴퓨터 프로그램을 제공하는 프로그램 제공 매체에 있어서, 상기 컴퓨터 프로그램은, 기억 수단 또는 기록 디바이스에 저장된 데이터 관리 파일에 설정된 설정 사용 제한 정보에 따라 기록 디바이스로부터 재생하는 세이브 데이터의 복호화 처리 형태를 결정하는 복호화 처리 형태 결정 단계와, 상기 복호화 처리 형태 결정 단계에 있

어서 결정된 복호화 처리 형태에 따라 복호화 처리에 적용하는 복호화 키를 선택하는 복호화 키 선택 단계와, 상기 복호화 키 선택 단계에 있어서 선택된 복호화 키를 이용하여 세이브 데이터의 복호화 처리를 실행하는 단계를 포함하는 것을 특징으로 하는 프로그램 제공 매체에 있다.

본 발명에 따른 프로그램 제공 매체는 예를 들면 여러가지 프로그램 코드를 실행 가능한 범용 컴퓨터 시스템에 대하여 컴퓨터 프로그램을 컴퓨터가 판독할 수 있는 형식으로 제공하는 매체이다. 매체는 CD나 FD, MO 등의 기억 매체, 또는 네트워크 등의 전송 매체 등, 그 형태는 특별히 한정되지 않는다.

이러한 프로그램 제공 매체는 컴퓨터 시스템 상에서 소정의 컴퓨터 프로그램의 기능을 실현하기 위한 컴퓨터 프로그램과 제공 매체와의 구조 상 또는 기능 상의 협동적 관계를 정의한 것이다. 다시 말하면, 제공 매체를 통해 컴퓨터 프로그램을 컴퓨터 시스템에 인스톨함으로써 컴퓨터 시스템 상에서 협동적 작용이 발휘되고, 본 발명의 다른 측면과 동일한 작용 효과를 얻을 수 있다.

본 발명의 또 다른 목적, 특징이나 이점은 후술하는 본 발명의 실시예나 첨부 도면에 기초한, 보다 상세한 설명에 의해 명확해질 것이다.

이와 같이, 본 발명의 데이터 처리 시스템, 기록 디바이스 데이터 처리 방법에 따르면, 기록 디바이스에 인증 처리에 적용 가능한 키 데이터를 저장한 키 블록을 복수 구성하고, 복수의 키 블록에 저장된 키 데이터를 각 블록마다 다른 키 데이터로서 하고, 기록 재생기와 기록 디바이스 간의 인증 처리를 특정 키 블록을 지정하여 실행하도록 구성했기 때문에, 제품 발송처(국가)별, 또는 제품, 기종, 버전, 어플리케이션별, 인증 처리에 적용해야 할 키 블록을 설정함으로써, 제품, 기종, 버전, 어플리케이션별 콘텐츠 이용 제한을 용이하게 설정할 수 있다.

또한, 본 발명의 데이터 처리 시스템, 기록 디바이스 및 데이터 처리 방법에 따르면, 각 키 블록에 저장된 보존 키가 다른 키에 의해 구성되어 있기 때문에, 다른 키 블록으로 기록 디바이스의 기억부에 저장된 콘텐츠 데이터, 또는 키 데이터 등은 다른 키 블록의 설정이 이루어진 기록 재생기를 이용한 복호 처리가 불가능하기 때문에, 콘텐츠 데이터, 또는 키 데이터의 부정 유통을 방지할 수 있다.

또한, 본 발명의 데이터 처리 시스템, 기록 디바이스 및 데이터 처리 방법에 있어서는, 기록 디바이스에 있어서의 인증 처리 및 저장 데이터의 암호 처리 등의 각종 처리를 실행 커맨드 순을 미리 정한 설정 시퀀스에 따라 실행하도록 구성했다. 즉, 기록 재생기로부터 기록 디바이스에 대하여 커맨드 번호를 송신하고, 기록 디바이스의 제어부가 미리 정한 시퀀스에 따른 커맨드 번호만을 접수하여 실행하는 구성으로 함과 함께, 설정 시퀀스의 인증 처리 커맨드를 암호 처리 커맨드에 선행하여 실행하도록 설정했기 때문에, 인증 처리가 완료된 기록 재생기만이 기록 디바이스에 대한 콘텐츠의 저장, 또는 재생 처리를 실행할 수 있으며, 인증 처리가 완료되지 않은 부정 기기에 의한 콘텐츠 이용을 배제할 수 있다.

또한, 본 발명의 데이터 처리 시스템, 기록 디바이스 및 데이터 처리 방법에 따르면, 인증 처리가 완료되었음을 나타내는 인증 플래그를 설정하고, 인증 플래그가 설정된 기기에 대해서는 암호화 데이터의 저장 처리, 재생 처리를 실행 가능하게 했기 때문에, 저장 처리, 재생 처리를 반복 실행할 경우, 인증 플래그가 설정되어 있을 경우, 반복 인증 처리를 실행할 필요가 없고, 효율적인 데이터 처리가 가능하게 된다.

발명의 구성

이하, 본 발명의 실시예를 설명한다. 설명의 순서는 이하의 항목에 따라 행한다.

(1) 데이터 처리 장치 구성

(2) 콘텐츠 데이터 포맷

(3) 데이터 처리 장치에서 적용 가능한 암호 처리 개요

(4) 기록 재생기의 저장 데이터 구성

(5) 기록 디바이스의 저장 데이터 구성

(6) 기록 재생기, 기록 디바이스 사이에서의 상호 인증 처리

(6-1) 상호 인증 처리의 개요

(6-2) 상호 인증 시의 키 블록의 전환

(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리

(8) 기록 디바이스 저장 정보의 기록 재생기에서의 재생 처리

(9) 상호 인증 후의 키 교환 처리

(10) 복수의 콘텐츠 데이터 포맷과, 각 포맷에 대응하는 다운로드 및 재생 처리

(11) 콘텐츠 프로바이더에 있어서의 체크치(ICV) 생성 처리 형태

(12) 마스터 키에 기초한 암호 처리 키 생성 구성

(13) 암호 처리에 있어서의 암호 강도의 제어

(14) 콘텐츠 데이터에 있어서의 취급 방침 중의 기동 우선 순위에 기초한 프로그램 기동 처리

(15) 콘텐츠 구성 및 재생(신장) 처리

(16) 세이브 데이터의 생성 및 기록 디바이스로의 저장, 재생 처리

(17) 부정 기기의 배제(폐지) 구성

(18) 시큐어 칩 구성 및 제조 방법

(1) 데이터 처리 장치 구성

도 2에 본 발명의 데이터 처리 장치의 일 실시예에 따른 전체 구성 블록도를 나타낸다. 본 발명의 데이터 처리 장치는 기록 재생기(300)와 기록 디바이스(400)를 주요 구성 요소로 한다.

기록 재생기(300)는 예를 들면 퍼스널 컴퓨터(PC: Personal Computer) 또는 게임 기기 등에 의해 구성된다. 기록 재생기(300)는 도 2에 도시한 바와 같이 기록 재생기(300)에 있어서의 암호 처리 시의 기록 디바이스(400)와의 통신 제어를 포함하는 통괄적 제어를 실행하는 제어부(301), 암호 처리 전반을 담당하는 기록 재생기 암호 처리부(302), 기록 재생기에 접속되는 기록 디바이스(400)와 인증 처리를 실행하여 데이터의 기입 및 판독을 행하는 기록 디바이스 컨트롤러(303), DVD 등의 미디어(500)로부터 적어도 데이터의 판독을 행하는 판독부(304), 외부와 데이터의 송수신을 행하는 통신부(305)를 갖는다.

기록 재생기(300)는 제어부(301)의 제어에 의해 기록 디바이스(400)에 대한 콘텐츠 데이터의 다운로드, 기록 디바이스(400)로부터의 콘텐츠 데이터 재생을 실행한다. 기록 디바이스(400)는 기록 재생기(300)에 대하여 바람직하게는 착탈 가능한 기억 매체, 예를 들면 메모리 카드 등이고, EEPROM, 플래시 메모리 등의 불휘발성 메모리, 하드디스크, 전지 있는 RAM 등으로 구성되는 외부 메모리(402)를 갖는다.

기록 재생기(300)는 도 2의 좌단에 도시한 기억 매체, DVD, CD, FD, HDD에 저장된 콘텐츠 데이터를 입력 가능한 인터페이스로서의 판독부(304), 인터넷 등의 네트워크로부터 신호 분배되는 콘텐츠 데이터를 입력 가능한 인터페이스로서의 통신부 (305)를 구비하고, 외부로부터 콘텐츠를 입력한다.

기록 재생기(300)는 암호 처리부(302)를 구비하고, 판독부(304) 또는 통신부 (305)를 통해 외부로부터 입력되는 콘텐츠 데이터를 기록 디바이스(400)에 다운로드 처리할 때, 또는 콘텐츠 데이터를 기록 디바이스(400)로부터 재생, 실행할 때의 인증 처리, 암호화 처리, 복호화 처리, 또한 데이터 검증 처리 등을 실행한다. 암호 처리부(302)는 암호 처리부(302) 전체

를 제어하는 제어부(306), 암호 처리용 키 등의 정보를 보유하고, 외부로부터 용이하게 데이터를 판독하지 않도록 처리가 실시된 내부 메모리(307), 암호화 처리, 복호화 처리, 인증용 데이터의 생성·검증, 난수의 발생 등을 행하는 암호/복호화부(308)로 구성되어 있다.

제어부(301)는 예를 들면, 기록 재생기(300)에 기록 디바이스(400)가 장착되었을 때 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)에 초기화 명령을 송신하거나 또는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)와 기록 디바이스 암호 처리부(401)의 암호/복호화부(406) 사이에서 행해지는 상호 인증 처리, 체크치 대조 처리, 암호화, 복호화 처리 등, 각종 처리에 있어서의 중개 처리를 행한다. 이들 각 처리에 대해서는 후단에서 상세하게 설명한다.

암호 처리부(302)는 상술한 바와 같이 인증 처리, 암호화 처리, 복호화 처리, 또한 데이터 검증 처리 등을 실행하는 처리부로서, 암호 처리 제어부(306), 내부 메모리(307), 암호/복호화부(308)를 갖는다.

암호 처리 제어부(306)는 기록 재생기(300)에 있어서 실행되는 인증 처리, 암호화/복호화 처리 등의 암호 처리 전반에 관한 제어를 실행하는 제어부로서, 예를 들면, 기록 재생기(300)와 기록 디바이스(400) 사이에서 실행되는 인증 처리 완료시에 있어서의 인증 완료 플래그의 설정, 기록 재생기 암호 처리부(302)의 암호 /복호화부(308)에 있어서 실행되는 각종 처리, 예를 들면 다운로드 또는 재생 콘텐츠 데이터에 관한 체크치 생성 처리의 실행 명령, 각종 키 데이터의 생성 처리의 실행 명령 등, 암호 처리 전반에 관한 제어를 행한다.

내부 메모리(307)는 후단에서 상세하게 설명하지만, 기록 재생기(300)에 있어서 실행되는 상호 인증 처리, 체크치 대조 처리, 암호화, 복호화 처리 등, 각종 처리에 있어서 필요한 키 데이터 또는 식별 데이터 등을 저장한다.

암호/복호화부(308)는 내부 메모리(307)에 저장된 키 데이터 등을 사용하여 외부로부터 입력되는 콘텐츠 데이터를 기록 디바이스(400)에 다운로드 처리할 때 또는 기록 디바이스(400)에 저장된 콘텐츠 데이터를 기록 디바이스(400)로부터 재생, 실행할 때의 인증 처리, 암호화 처리, 복호화 처리, 또한 소정의 체크치나 전자 서명의 생성·검증, 데이터의 검증, 난수의 발생 등의 처리를 실행한다.

여기서, 기록 재생기 암호 처리부(302)의 내부 메모리(307)는 암호 키 등의 중요한 정보를 보유하고 있기 때문에 외부로부터 부정 판독하기 어려운 구조로 해 둘 필요가 있다. 따라서, 암호 처리부(302)는 외부로부터 액세스하기 어려운 구조를 갖는 반도체 칩으로 구성되고, 다층 구조를 구비하며, 그 내부 메모리는 알루미늄층 등의 더미층에 끼워지거나, 최하층에 구성되고, 또한 동작하는 전압 또는 /또한 주파수의 폭이 좁다는 등, 외부로부터 데이터의 부정 판독이 어려운 특성을 갖는 내 탬퍼 메모리로서 구성된다. 이 구성에 대해서는 후단에서 상세히 설명한다.

기록 재생기(300)는 이들 암호 처리 기능 외에 중앙 연산 처리 장치(메인 CPU: Central Processing Unit: 106), RAM(Random Access Memory: 107), ROM(Read Only Memory: 108), AV 처리부(109), 입력 인터페이스(110), PIO(병렬 I/O 인터페이스: 111), SIO(직렬 I/O 인터페이스: 112)를 구비하고 있다.

중앙 연산 처리 장치(메인 CPU: Central Processing Unit: 106), RAM(Random Access Memory: 107), ROM(Read Only Memory: 108)은 기록 재생기(300) 본체의 제어계로서 기능하는 구성부로서, 주로 기록 재생기 암호 처리부(302)로 복호된 데이터의 재생을 실행하는 재생 처리부로서 기능한다. 예를 들면, 중앙 연산 처리 장치(메인 CPU: Central Processing Unit: 106)는 제어부(301)의 제어 하에 기록 디바이스로부터 판독되어 복호된 콘텐츠 데이터를 AV 처리부(109)로 출력하는 등, 콘텐츠의 재생, 실행에 관한 제어를 행한다.

RAM(107)은 CPU(106)에 있어서의 각종 처리용 주기억 메모리로서 사용되고, 메인 CPU(106)에 의한 처리를 위한 작업 영역으로서 사용된다. ROM(108)은 메인 CPU(106)로 기동되는 OS 등을 상승시키기 위한 기본 프로그램 등이 저장된다.

AV 처리부(109)는 구체적으로는 예를 들면 MPEG2 디코더, ATRAC 디코더, MP3 디코더 등의 데이터 압축 신장 처리 기구를 구비하고, 기록 재생기 본체에 부속 또는 접속된 도시하지 않은 디스플레이 또는 스피커 등의 데이터 출력 기기에 대한 데이터 출력을 위한 처리를 실행한다.

입력 인터페이스(110)는 접속된 컨트롤러, 키보드, 마우스 등, 각종 입력 수단으로부터의 입력 데이터를 메인 CPU(106)로 출력한다. 메인 CPU(106)는 예를 들면 실행 중인 게임 프로그램 등에 기초하여 사용자로부터의 컨트롤러로부터의 지시에 따른 처리를 실행한다.

PIO(병렬 I/O 인터페이스: 111), SIO(직렬 I/O 인터페이스: 112)는 메모리 카드, 게임 카트리지 등의 기억 장치, 휴대용 전자 기기 등과의 접속 인터페이스로서 사용된다.

또한, 메인 CPU(106)는 예를 들면 실행 중인 게임 등에 관한 설정 데이터 등을 세이브 데이터로서 기록 디바이스(400)에 기억할 때의 제어도 행한다. 이 처리 시에는 기억 데이터를 제어부(301)로 전송하고, 제어부(301)는 필요에 따라 암호 처리부(302)에 세이브 데이터에 관한 암호 처리를 실행시키고, 암호화 데이터를 기록 디바이스(400)에 저장한다. 이들 암호 처리에 대해서는 후단에서 상세하게 설명한다.

기록 디바이스(400)는 상술한 바와 같이 바람직하게는 기록 재생기(300)에 대하여 착탈 가능한 기억 매체로서, 예를 들면 메모리 카드로 구성된다. 기록 디바이스(400)는 암호 처리부(401), 외부 메모리(402)를 갖는다.

기록 디바이스 암호 처리부(401)는 기록 재생기(300)로부터의 콘텐츠 데이터의 다운로드, 또는 기록 디바이스(400)로부터 기록 재생기(300)로의 콘텐츠 데이터의 재생 처리 시 등에 있어서의 기록 재생기(300)와 기록 디바이스(400) 사이의 상호 인증 처리, 암호화 처리, 복호화 처리, 또한 데이터 검증 처리 등을 실행하는 처리부로서, 기록 재생기(300)의 암호 처리부와 마찬가지로 제어부, 내부 메모리, 암호/복호화부 등을 갖는다. 이들 상세는 도 3에 도시한다. 외부 메모리(402)는 상술한 바와 같이 예를 들면 EEPROM 등의 플래시 메모리로 이루어진 불휘발성 메모리, 하드디스크, 전지가 부착된 RAM 등에 의해 구성되어, 암호화된 콘텐츠 데이터 등을 저장한다.

도 3은 본 발명의 데이터 처리 장치가 데이터 공급을 받는 콘텐츠 제공 수단인 미디어(500), 통신 수단(600)으로부터 입력되는 데이터 구성의 개략을 나타냄 과 함께, 이들 콘텐츠 제공 수단(500, 600)으로부터 콘텐츠를 입력하는 기록 재생기(300)와, 기록 디바이스(400)에 있어서의 암호 처리에 관한 구성을 중심으로 하여, 그 구성을 나타낸 도면이다.

미디어(500)는 예를 들면 광 디스크 미디어, 자기 디스크 미디어, 자기 테이프 미디어, 반도체 미디어 등이다. 통신 수단(600)은 인터넷 통신, 케이블 통신, 위성 통신 등의 데이터 통신 가능한 수단이다.

도 3에 있어서, 기록 재생기(300)는 콘텐츠 제공 수단인 미디어(500), 통신 수단(600)으로부터 입력되는 데이터, 즉 도 3에 도시한 바와 같은 소정의 포맷에 따른 콘텐츠를 검증하고, 검증 후에 콘텐츠를 기록 디바이스(400)에 보존한다.

도 3의 미디어(500), 통신 수단(600) 부분에 도시한 바와 같이 콘텐츠 데이터는 다음과 같은 구성부를 갖는다.

식별 정보: 콘텐츠 데이터의 식별자로서의 식별 정보.

취급 방침: 콘텐츠 데이터의 구성 정보, 예를 들면 콘텐츠 데이터를 구성하는 헤더부 사이즈, 콘텐츠부 사이즈, 포맷 버전, 콘텐츠가 프로그램인지 데이터인지 등을 나타내는 콘텐츠 타입, 또한 콘텐츠가 다운로드한 기기만으로밖에 이용할 수 없는 것인지 다른 기기라도 이용할 수 있는 것인지 등의 이용 제한 정보 등을 포함하는 취급 방침.

블록 정보: 콘텐츠 블록의 수, 블록 사이즈, 암호화 유무를 나타내는 암호화 플래그 등으로 구성되는 블록 정보.

키 데이터: 상술한 블록 정보를 암호화하는 암호화 키 또는 콘텐츠 블록을 암호화하는 콘텐츠 키 등으로 이루어진 키 데이터.

콘텐츠 블록: 실제 재생 대상이 되는 프로그램 데이터, 음악, 화상 데이터 등으로 이루어진 콘텐츠 블록

을 갖는다. 또, 콘텐츠 데이터 상세에 대해서는 후단에서 도 4 이하를 이용하여 더욱 상세하게 설명한다.

콘텐츠 데이터는 콘텐츠 키{여기서는 이를 콘텐츠 키[Content Key(이하, K_{con}으로 함)]라 함}에 의해 암호화되고, 미디어(500), 통신 수단(600)으로부터 기록 재생기(300)에 제공된다. 콘텐츠는 기록 재생기(300)를 통해 기록 디바이스(400)의 외부 메모리에 저장할 수 있다.

예를 들면, 기록 디바이스(400)는 기록 디바이스 내의 내부 메모리(405)에 저장된 기록 디바이스 고유의 키{여기서는 이를 보존 키[Storage Key(이하, K_{str}로 함)]라 함]를 이용하여 콘텐츠 데이터에 포함되는 콘텐츠 및 콘텐츠 데이터의 헤더 정보로서 포함되는 블록 정보, 각종 키 정보, 예를 들면 콘텐츠 키 K_{con} 등을 암호화하여 외부 메모리(402)에 기억한다. 콘

텐츠 데이터의 기록 재생기(300)로부터 기록 디바이스(400)로의 다운로드 처리 또는 기록 재생기(300)에 의한 기록 디바이스 (400) 내에 저장된 콘텐츠 데이터의 재생 처리에 있어서는 기기간의 상호 인증 처리, 콘텐츠 데이터의 암호화, 복호화 처리 등 소정 수속이 필요하게 된다. 이들 처리에 대해서는 후단에서 상세하게 설명한다.

기록 디바이스(400)는 도 3에 도시한 바와 같이 암호 처리부(401), 외부 메모리(402)를 구비하고, 암호 처리부(401)는 제어부(403), 통신부(404), 내부 메모리(405), 암호/복호화부(406), 외부 메모리 제어부(407)를 구비한다.

기록 디바이스(400)는 암호 처리 전반을 담당하여 외부 메모리(402)를 제어함과 함께, 기록 재생기(300)로부터의 커맨드를 해석하고, 처리를 실행하는 기록 디바이스 암호 처리부(401)와, 콘텐츠 등을 보유하는 외부 메모리(402)로 이루어진다.

기록 디바이스 암호 처리부(401)는 기록 디바이스 암호 처리부(401) 전체를 제어하는 제어부(403), 기록 재생기(300)와 데이터의 송수신을 행하는 통신부 (404), 암호 처리용 키 데이터 등의 정보를 보유하고, 외부로부터 용이하게 판독되지 않도록 처리가 실시된 내부 메모리(405), 암호화 처리, 복호화 처리, 인증용 데이터의 생성·검증, 난수의 발생 등을 행하는 암호/복호화부(406), 외부 메모리 (402)의 데이터를 기입 및 판독하는 외부 메모리 제어부(407)를 갖는다.

제어부(403)는 기록 디바이스(400)에 있어서 실행되는 인증 처리, 암호화/복호화 처리 등의 암호 처리 전반에 따른 제어를 실행하는 제어부로서, 예를 들면, 기록 재생기(300)와 기록 디바이스(400) 사이에서 실행되는 인증 처리의 완료 시에 있어서의 인증 완료 플래그의 설정, 암호 처리부(401)의 암호/복호화부(406)에 있어서 실행되는 각종 처리, 예를 들면 다운로드 또는 재생 콘텐츠 데이터에 관한 체크치 생성 처리의 실행 명령, 각종 키 데이터의 생성 처리의 실행 명령 등, 암호 처리 전반에 관한 제어를 행한다.

내부 메모리(405)는 후단에서 상세하게 설명하지만, 복수의 블록을 갖는 메모리로 구성되어 있으며, 기록 디바이스(400)에 있어서 실행되는 상호 인증 처리, 체크치 대조 처리, 암호화, 복호화 처리 등, 각종 처리에 있어서 필요한 키 데이터 또는 식별 데이터 등의 조를 복수 저장한 구성으로 되어 있다.

기록 디바이스 암호 처리부(401)의 내부 메모리(405)는 먼저 설명한 기록 재생기 암호 처리부(302)의 내부 메모리(307)와 마찬가지로 암호 키 등의 중요한 정보를 보유하고 있기 때문에 외부로부터 부정 판독하기 어려운 구조로 해 둘 필요가 있다. 따라서, 기록 디바이스(400)의 암호 처리부(401)는 외부로부터 액세스하기 어려운 구조를 갖은 반도체 칩으로 구성되고, 다층 구조를 구비하며, 그 내부 메모리는 알루미늄층 등의 더미층에 끼워지거나, 최하층에 구성되고, 또한 동작하는 전압 또는/또한 주파수의 폭이 좁다는 등, 외부로부터 데이터의 부정 판독이 어려운 특성으로 한 구성이 된다. 또, 기록 재생기 암호 처리부(302)는 키 등의 비밀의 정보를 외부로 용이하게 누설되지 않도록 구성된 소프트웨어라도 좋다.

암호/복호화부(406)는 기록 재생기(300)로부터의 콘텐츠 데이터의 다운로드 처리, 기록 디바이스(400)의 외부 메모리(402)에 저장된 콘텐츠 데이터의 재생 처리 또는 기록 재생기(300)와 기록 디바이스(400) 사이의 상호 인증 처리 시, 내부 메모리(405)에 저장된 키 데이터 등을 사용하여 데이터의 검증 처리, 암호화 처리, 복호화 처리, 소정의 체크치나 전자 서명의 생성·검증, 난수의 발생 등의 처리 등을 실행한다.

통신부(404)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)에 접속되고, 기록 재생기(300)의 제어부(301) 또는 기록 디바이스(400)의 제어부(403)의 제어에 따라 콘텐츠 데이터의 다운로드 처리, 재생 처리 또는 상호 인증 처리 시의 기록 재생기(300)와 기록 디바이스(400) 사이의 전송 데이터의 통신을 행한다.

(2) 콘텐츠 데이터 포맷

다음으로, 도 4 내지 도 6을 이용하여 본 발명의 시스템에 있어서의 미디어 (500)에 저장되거나, 데이터 통신 수단(600) 상을 유통하는 데이터의 데이터 포맷에 대하여 설명한다.

도 4에 도시한 구성이 콘텐츠 데이터 전체의 포맷을 나타내는 도면이고, 도 5에 도시한 구성이 콘텐츠 데이터의 헤더부의 일부를 구성하는 「취급 방침」의 상세를 나타내는 도면이고, 도 6에 도시한 구성이 콘텐츠 데이터의 헤더부의 일부를 구성하는 「블록 정보」의 상세를 나타내는 도면이다.

또, 여기서는 본 발명의 시스템에 있어서 적용되는 데이터 포맷의 대표적인 일례에 대하여 설명하지만, 본 발명의 시스템에서는 예를 들면 게임 프로그램에 대응한 포맷, 음악 데이터 등의 실시간 처리에 적합한 포맷 등, 다른 복수의 데이터 포맷이 이용 가능하고, 이들 포맷 형태에 대해서는 후단 「(10) 복수의 콘텐츠 데이터 포맷과, 각 포맷에 대응하는 다운로드 및 재생 처리」에서, 더욱 상세하게 진술한다.

도 4에 도시한 데이터 포맷에 있어서, 회색으로 나타내는 부분은 암호화된 데이터이고, 이중 프레임 부분은 변경 체크 데이터이고, 그 밖의 흰 부분은 암호화되어 있지 않은 평문 데이터이다. 암호화부의 암호화 키는 각각의 프레임 좌측에 나타내는 키이다. 도 4에 도시한 예에 있어서는 콘텐츠부의 각 블록(콘텐츠 블록 데이터)에 암호화된 것과 암호화되어 있지 않은 것이 혼재하고 있다. 이들 형태는 콘텐츠 데이터에 따라 다른 것이며, 데이터에 포함되는 모든 콘텐츠 블록 데이터가 암호화되어 있는 구성이이도 좋다.

도 4에 도시한 바와 같이 데이터 포맷은 헤더부와 콘텐츠부로 분리되어 있으며, 헤더부는 식별 정보(Content ID), 취급 방침(Usage Policy), 체크치 A [Integrity Check Value A(이하, ICV_a로 함)], 블록 정보 키[Block Information Table Key (이하, K_{bit}로 함)], 콘텐츠 키 K_{con}, 블록 정보[Block Information Table(이하, BIT로 함)], 체크치 B(ICV_b), 총 체크치(ICV_t)에 의해 구성되어 있으며, 콘텐츠부는 복수의 콘텐츠 블록(예를 들면, 암호화된 콘텐츠와, 암호화되어 있지 않은 콘텐츠)으로 구성되어 있다.

여기서, 식별 정보는 콘텐츠를 식별하기 위한 개별 식별자(Content ID)를 나타내고 있다. 취급 방침은 도 5에 그 상세를 도시한 바와 같이 헤더 부분의 사이즈를 나타내는 헤더 사이즈(Header Length), 콘텐츠 부분의 사이즈를 나타내는 콘텐츠 사이즈(Content Length), 포맷의 버전 정보를 나타내는 포맷 버전(Format Version), 포맷의 종류를 나타내는 포맷 타입(Format Type), 콘텐츠부에 보존되어 있는 콘텐츠가 프로그램인지, 데이터인지 등 콘텐츠의 종류를 나타내는 콘텐츠 타입(Content Type), 콘텐츠 타입이 프로그램인 경우의 기동 우선 순위를 나타내는 기동 우선 순위 정보(Operation Priority), 이 포맷에 따라 다운로드된 콘텐츠가 다운로드한 기기만으로밖에 이용할 수 없는 것인지, 다른 동일한 기기라도 이용할 수 있는 것인지를 나타내는 이용 제한 정보(Localization Fie1d), 이 포맷에 따라 다운로드된 콘텐츠가 다운로드한 기기로부터 다른 동일한 기기에 복제할 수 있는 것인지의 여부를 나타내는 복제 제한 정보(Copy Permission), 이 포맷에 따라 다운로드된 콘텐츠가 다운로드한 기기로부터 다른 동일한 기기로 이동할 수 있는 것인지의 여부를 나타내는 이동 제한 정보(Move Permission), 콘텐츠부내의 콘텐츠 블록을 암호하는 데 사용한 알고리즘을 나타내는 암호 알고리즘(Encryption Algorithm), 콘텐츠부내의 콘텐츠를 암호화하는 데 사용한 알고리즘의 사용 방법을 나타내는 암호화 모드(Encryption Mode), 체크치가 생성 방법을 나타내는 검증 방법(Integrity Check Method)으로 구성되어 있다.

또, 상술한 취급 방침에 기록하는 데이터 항목은 하나의 예로서, 대응하는 콘텐츠 데이터의 형태에 따라 여러가지 취급 방침 정보를 기록할 수 있다. 예를 들면 후단의 「(17) 부정 기기의 배제(폐지) 구성」에서 상세하게 진술하지만, 부정한 기록 재생기의 식별자를 데이터로서 기록하고, 이용 개시 시의 대조에 의해 부정 기기에 의한 콘텐츠 이용을 배제하도록 구성할 수도 있다.

체크치 A, ICV_a는 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치이다. 콘텐츠 데이터 전체가 아닌 부분 데이터의 체크치, 즉 부분 체크치로서 기능한다. 데이터 블록 정보 키 K_{bit}는 블록 정보를 암호화하는 데 이용되고, 콘텐츠 키 K_{con}은 콘텐츠 블록을 암호화하는 데 이용된다. 또, 블록 정보 키 K_{bit} 및 콘텐츠 키 K_{con}은 미디어(500) 상 및 통신 수단(600) 상에서는 후술하는 배송 키[Distribution Key(이하, K_{dis}로 함)]로 암호화되어 있다.

블록 정보의 상세를 도 6에 도시한다. 또, 도 6의 블록 정보는 도 4에서 알 수 있는 바와 같이 전부 블록 정보 키 K_{bit}에 의해 암호화되어 있는 데이터이다. 블록 정보는 도 6에 도시한 바와 같이 콘텐츠 블록의 수를 나타내는 콘텐츠 블록 수(Block Number)와 N개의 콘텐츠 블록 정보로 구성되어 있다. 콘텐츠 블록 정보는 블록 사이즈(Block Length), 암호화되어 있는지의 여부를 나타내는 암호화 플래그 (Encryption Flag), 체크치를 계산할 필요가 있는지의 여부를 나타내는 검증 대상 플래그(ICV Flag), 콘텐츠 체크치(ICV_i)로 구성되어 있다.

콘텐츠 체크치는 각 콘텐츠 블록의 변경을 검증하기 위해 이용되는 체크치이다. 콘텐츠 체크치의 생성 방법의 구체예에 대해서는 후단의 「(10) 복수의 데이터 포맷과, 각 포맷에 대응하는 기록 디바이스로의 다운로드 처리 및 기록 디바이스로부터의 재생 처리」에서 설명한다. 또, 블록 정보를 암호화하고 있는 블록 정보 키 K_{bit}는, 또한 배송 키 K_{dis}에 의해 암호화되어 있다.

도 4의 데이터 포맷 설명을 계속한다. 체크치 B, ICV_b는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경을 검증하기 위한 체크치이다. 콘텐츠 데이터 전체가 아닌 부분 데이터의 체크치, 즉 부분 체크치로서 기능한다. 총 체크치 ICV_t는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 ICV_i(설정되어 있는 경우), 이들 부분 체크치 또는 그 체크 대상이 되는 데이터 전부의 변경을 검증하기 위한 체크치이다.

또, 도 6에 있어서는 블록 사이즈, 암호화 플래그, 검증 대상 플래그를 자유롭게 설정할 수 있도록 하고 있지만, 어느 정도 룰을 정한 구성으로 하여도 좋다. 예를 들면, 암호문 영역과 평문 영역을 고정 사이즈를 반복하거나, 모든 콘텐츠 데이터를 암호화하기도 하고, 블록 정보 BIT를 압축해도 좋다. 또한, 콘텐츠 키 K_{con}을 콘텐츠 블록마다 다르게 하기 위해서, 콘텐츠 키 K_{con}을 헤더 부분이 아니라, 콘텐츠 블록에 포함시켜도 좋다. 콘텐츠 데이터 포맷의 예에 대해서는 「(10) 복수의 콘텐츠 데이터 포맷과, 각 포맷에 대응하는 다운로드 및 재생 처리」에서 더욱 상세하게 설명한다.

(3) 본 발명의 데이터 처리 장치에서 적용 가능한 암호 처리 개요

다음으로, 본 발명의 데이터 처리 장치에서 적용될 수 있는 각종 암호 처리의 형태에 대하여 설명한다. 또, 본 항목 「(3) 본 발명의 데이터 처리 장치에서 적용 가능한 암호 처리의 개요」에 나타내는 암호 처리에 관한 설명은 후단에서 구체적으로 설명하는 본 발명의 데이터 처리 장치에서의 각종 처리, 예를 들면 a. 기록 재생기와 기록 디바이스 사이에서의 인증 처리. b. 콘텐츠의 기록 디바이스에 대한 다운로드 처리. c. 기록 디바이스에 저장한 콘텐츠의 재생 처리 등의 처리에 있어서 실행되는 처리의 기초가 되는 암호 처리의 형태에 대하여, 그 개요를 설명하는 것이다. 기록 재생기(300)와 기록 디바이스(400)에 있어서의 구체적 처리에 대해서는 본 명세서의 항목 (4) 이하에 있어서, 각 처리마다 상세하게 설명한다.

이하, 데이터 처리 장치에서 적용 가능한 암호 처리의 개요에 대하여,

(3-1) 공통 키 암호 방식에 의한 메세지 인증

(3-2) 공개 키 암호 방식에 의한 전자 서명

(3-3) 공개 키 암호 방식에 의한 전자 서명의 검증

(3-4) 공통 키 암호 방식에 의한 상호 인증

(3-5) 공개 키 증명서

(3-6) 공개 키 암호 방식에 의한 상호 인증

(3-7) 타원 곡선 암호를 이용한 암호화 처리

(3-8) 타원 곡선 암호를 이용한 복호화 처리

(3-9) 난수 생성 처리

의 순으로 설명한다.

(3-1) 공통 키 암호 방식에 의한 메세지 인증

우선, 공통 키 암호 방식을 이용한 변경 검출 데이터의 생성 처리에 대하여 설명한다. 변경 검출 데이터는 변경의 검출을 행하고자 하는 데이터에 붙이고, 변경의 체크 및 작성자 인증을 하기 위한 데이터이다.

예를 들면, 도 4에서 설명한 데이터 구조 중의 이중 프레임 부분의 각 체크치 A, B, 총 체크치 및 도 6에 도시한 블록 정보 중의 각 블록에 저장된 콘텐츠 체크치 등이 이 변경 검출 데이터로서 생성된다.

여기서는 전자 서명 데이터의 생성 처리 방법예의 하나로서 공통 키 암호 방식에 있어서의 DES를 이용한 예를 설명한다. 또, 본 발명에 있어서는 DES 이외에도, 동일한 공통 키 암호 방식에 있어서의 처리로서 예를 들면 FEAL(Fast Encipherment Algorithm: NTT), AES(Advanced Encryption Standard: 미국 차기 표준 암호) 등을 이용할 수도 있다.

일반적인 DES를 이용한 전자 서명의 생성 방법을 도 7을 이용하여 설명한다. 우선, 전자 서명을 생성하기에 앞서, 전자 서명의 대상이 되는 메세지를 8바이트 단위로 분할한다(이하, 분할된 메세지를 M1, M2, …, MN으로 함). 그리고, 초기치[Initial Value(이하, IV로 함)]와 M1을 배타적 논리합한다(그 결과를 I1로 함). 다음으로, I1을 DES 암호화부에 넣고, 키(이하, K1로 함)를 이용하여 암호화한다(출력을 E1로 함). 계속하여, E1 및 M2를 배타적 논리합하고, 그 출력 I2를 DES 암호화부에 넣고, 키 K1을 이용하여 암호화한다(출력 E2). 이하, 이를 반복하고, 모든 메세지에 대하여 암호화 처리를 실시한다. 마지막으로 생성된 EN이 전자 서명이 된다. 이 값은 일반적으로는 메세지 인증 부호[MAC(Message Authentication Code)]라 불리고, 메세지의 변경 체크에 이용된다. 또한, 이와 같이 암호문을 연쇄시키는 방식을 CBC (Cipher Block Chaining) 모드라 한다.

또, 도 7과 같은 생성예에 있어서 출력되는 MAC치가 도 4에서 도시한 데이터 구조 중의 이중 프레임 부분의 각 체크치 A, B, 총 체크치 및 도 6에 도시한 블록 정보 중의 각 블록에 저장된 콘텐츠 체크치 ICV_1~ICV_N으로서 사용 가능하다. 이 MAC치의 검증 시에는 검증자가 생성 시와 동일한 방법으로 MAC치를 생성하고, 동일한 값이 얻어진 경우, 검증 성공으로 한다.

또, 도 7에 도시한 예에서는 초기치 IV를 처음 8바이트 메세지 M1에 배타적 논리합하였지만, 초기치 IV=0으로서, 초기치를 배타적 논리합하지 않은 구성으로 할 수도 있다.

도 7에 도시한 MAC치 생성 방법에 대하여, 시큐러티를 더욱 향상시킨 MAC치 생성 방법을 나타내는 처리 구성도를 도 8에 도시한다. 도 8은 도 7의 싱글 DES 대신에 트리플 DES(Triple DES)를 이용하여 MAC치의 생성을 실행하는 예를 나타낸 것이다.

도 8에 도시한 각 트리플 DES(Triple DES) 구성부의 상세 구성예를 도 9에 도시한다. 도 9의 (A), (B)에 도시한 바와 같이 트리플 DES(Triple DES)로서의 구성에는 두 가지의 다른 형태가 있다. 도 9의 (A)는 두 개의 암호 키를 이용한 예를 나타내는 것이며, 키 1에 의한 암호화 처리, 키 2에 의한 복호화 처리, 또한 키 1에 의한 암호화 처리 순으로 처리를 행한다. 키는 K1, K2, K1의 순으로 2 종류 이용한다. 도 9의 (B)는 세 개의 암호 키를 이용한 예를 나타내는 것이며, 키 1에 의한 암호화 처리, 키 2에 의한 암호화 처리, 또한 키 3에 의한 암호화 처리의 순으로 처리를 행하여 3회 모두 암호화 처리를 행한다. 키는 K1, K2, K3의 순으로 3 종류의 키를 이용한다. 이와 같이 복수의 처리를 연속시키는 구성으로 함으로써, 싱글 DES에 비하여 시큐러티 강도를 향상시키고 있다. 그러나, 이 트리플 DES (Triple DES) 구성은 처리 시간이 싱글 DES의 3배 정도 걸린다는 결점을 갖는다.

도 8 및 도 9에서 설명한 트리플 DES 구성을 개량한 MAC치 생성 구성예를 도 10에 도시한다. 도 10에 있어서는 서명 대상이 되는 메세지 열의 처음부터 도중까지의 각 메세지에 대한 암호화 처리는 전부 싱글 DES에 의한 처리로 하고, 마지막 메세지에 대한 암호화 처리만을 도 9의 (A)에 도시한 트리플 DES(Triple DES) 구성으로 한 것이다.

도 10에 도시한 이러한 구성으로 함으로써, 메세지의 MAC치의 생성 처리 시간은 싱글 DES에 의한 MAC치 생성 처리에 필요한 시간과 거의 같은 정도로 단축되고, 또한 시큐러티는 싱글 DES에 의한 MAC치보다 높일 수 있다. 또, 최종 메세지에 대한 트리플 DES 구성은 도 9의 (B)의 구성으로 할 수도 있다.

(3-2) 공개 키 암호 방식에 의한 전자 서명

이상은 암호화 방식으로서 공통 키 암호화 방식을 적용한 경우의 전자 서명 데이터의 생성 방법이지만, 다음으로, 암호화 방식으로서 공개 키 암호 방식을 이용한 전자 서명의 생성 방법을 도 11을 이용하여 설명한다. 도 11에 도시한 처리는 EC-DSA[(Elliptic Curve Digital Signature Algorithm), IEEE P1363/D3]를 이용한 전자 서명 데이터의 생성 처리 플로우이다. 또, 여기서는 공개 키 암호로서 타원 곡선 암호[Elliptic Curve Cryptography(이하, ECC라 함)]를 이용한 예를 설명한다. 또, 본 발명의 데이터 처리 장치에서는 타원 곡선 암호 이외에도, 동일한 공개 키 암호 방식에 있어서의, 예를 들면 RSA 암호[(Rivest, Shamir, Adleman) 등 (ANSI X9. 31)]를 이용할 수도 있다.

도 11의 각 단계에 대하여 설명한다. 단계 S1에 있어서, p를 표수, a, b를 타원 곡선의 계수(타원 곡선: $y^2=x^3+ax+b$), G를 타원 곡선 상의 베이스 포인트, r을 G의 자리수, Ks를 비밀 키(0<Ks<r)로 한다. 단계 S2에 있어서 메세지 M의 해시값을 계산하여, f=Hash(M)로 한다.

여기서, 해시 함수를 이용하여 해시값을 구하는 방법을 설명한다. 해시 함수는 메세지를 입력으로 하고, 이를 소정의 비트 길이의 데이터에 압축하여 해시값으로서 출력하는 함수이다. 해시 함수는 해시값(출력)으로부터 입력을 예측하는 것이 어렵고, 해시 함수에 입력된 데이터의 1비트가 변화했을 때, 해시값의 많은 비트가 변화하고, 또한 동일한 해시값을 갖는 다른 입력 데이터를 찾아내는 것이 곤란한 특징을 갖는다. 해시 함수로서는 MD4, MD5, SHA-1 등이 이용되는 경우도 있고, 도 7 또는 다른 도면에서 설명한 것과 동일한 DES-CBC가 이용되는 경우도 있다. 이 경우, 최종 출력치가 되는 MAC(체크치: ICV에 상당함)가 해시값이 된다.

계속하여, 단계 S3에서 난수 u(0<u<r)를 생성하고, 단계 S4에서 베이스 포인트를 u배한 좌표 V(Xv, Yv)를 계산한다. 또, 타원 곡선 상의 가산, 2배산은 다음과 같이 정의되어 있다.

P=(Xa, Ya), Q=(Xb, Yb), R=(Xc, Yc)=P+Q로 하면

P≠Q일 때, (가산),

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Q일 때(2배산),

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$ … (1)

이들을 이용하여 점 G의 u배를 계산한다[속도는 느리지만, 가장 알기 쉬운 연산 방법으로서 다음과 같이 행한다. G, 2×G, 4×G ‥를 계산하여, u를 2진수 전개하여 1이 설정되는 것에 대응하는 $2^i\times G$(G를 i회 2배산한 값)를 가산함(i는 u의 LSB부터 카운트했을 때의 비트 위치)].

단계 S5에서 c=Xv mod r을 계산하고, 단계 S6에서 이 값이 0이 되는지의 여부를 판정하여, 0이 아니면 단계 S7에서 d=[(f+cKs)/u] mod r을 계산하고, 단계 S8에서 d가 0인지의 여부를 판정하여, d가 0이 아니면 단계 S9에서 c 및 d를 전자 서명 데이터로서 출력한다. 만일, r을 160비트 길이의 길이라고 가정하면, 전자 서명 데이터는 320비트 길이가 된다.

단계 S6에 있어서, c가 0인 경우, 단계 S3으로 되돌아가 새로운 난수를 재생성한다. 마찬가지로, 단계 S8에서 d가 0인 경우도, 단계 S3으로 되돌아가 난수를 재생성한다.

(3-3) 공개 키 암호 방식에 의한 전자 서명의 검증

다음으로, 공개 키 암호 방식을 이용한 전자 서명의 검증 방법을 도 12를 이용하여 설명한다. 단계 S11에서, M을 메세지, p를 표수, a, b를 타원 곡선의 계수 (타원 곡선: $y^2=x^3+ax+b$), G를 타원 곡선 상의 베이스 포인트, r을 G의 자리수, G 및 Ks×G를 공개 키(0<Ks<r)로 한다. 단계 S12에서 전자 서명 데이터 c 및 d가 0< c<r, 0<d<r을 만족하는지 검증한다. 이를 만족한 경우, 단계 S13에서 메세지 M의 해시값을 계산하여 f=Hash(M)로 한다. 다음으로, 단계 S14에서 h=1/d mod r을 계산하고, 단계 S15에서 h1=fh mod r, h2=ch mod r을 계산한다.

단계 S16에 있어서, 이미 계산한 h1 및 h2를 이용하여 점 P=(Xp, Yp)=h1×G+ h2·Ks×G를 계산한다. 전자 서명 검증자는 공개 키 G 및 Ks×G를 알고 있기 때문에, 도 11의 단계 S4와 마찬가지로 타원 곡선 상의 점의 스칼라배의 계산을 할 수 있다. 그리고, 단계 S17에서 점 P가 무한 원점인지의 여부를 판정하여, 무한원점이 아니면 단계 S18로 진행한다(실제로는 무한 원점의 판정은 단계 S16에서 할 수 있다. 즉, P=(X, Y), Q=(X, Y)의 가산을 행하면, λ을 계산할 수 없고, P+ Q가 무한 원점인 것이 판명되어 있음). 단계 S18에서 Xp mod r을 계산하여, 전자 서명 데이터 c와 비교한다. 마지막으로, 이 값이 일치한 경우, 단계 S19로 진행하여 전자 서명이 정확하다고 판정한다.

전자 서명이 정확하다고 판정된 경우, 데이터는 변경되어 있지 않고, 공개 키에 대응한 비밀 키를 보유하는 사람이 전자 서명을 생성한 것을 알 수 있다.

단계 S12에 있어서, 전자 서명 데이터 c 또는 d가 0<c<r, 0<d<r을 만족하지 않은 경우, 단계 S20으로 진행한다. 또한, 단계 S17에 있어서, 점 P가 무한원점인 경우도 단계 S20으로 진행한다. 또한, 단계 S18에 있어서, Xp mod r의 값이 전자 서명 데이터 c와 일치하지 않은 경우에도 단계 S20으로 진행한다.

단계 S20에 있어서, 전자 서명이 정확하지 않다고 판정된 경우, 데이터는 변경되어 있는지, 공개 키에 대응한 비밀 키를 보유하는 사람이 전자 서명을 생성한 것이 아님을 알 수 있다.

(3-4) 공통 키 암호 방식에 의한 상호 인증

다음으로, 공통 키 암호 방식을 이용한 상호 인증 방법을 도 13을 이용하여 설명한다. 도 13에 있어서, 공통 키 암호 방식으로서 DES를 이용하고 있지만, 상술한 바와 같이 동일한 공통 키 암호 방식이면 모두 좋다. 도 13에 있어서, 우선, B가 64비트의 난수 R_b를 생성하여 R_b 및 자신의 ID인 ID(b)를 A로 송신한다. 이를 수신한 A는 새롭게 64비트의 난수 R_a를 생성하여 R_a, R_b, ID(b) 순으로, DES의 CBC 모드로 키 K_{ab}를 이용하여 데이터를 암호화하고, B로 반송한다. 도 7에 도시한 DES의 CBC 모드 처리 구성에 따르면, R_a가 M1, R_b가 M2, ID(b)가 M3에 상당하여, 초기치: IV=0으로 했을 때의 출력 E1, E2, E3이 암호문이 된다.

이를 수신한 B는 수신 데이터를 키 K_{ab}로 복호화한다. 수신 데이터의 복호화 방법은 우선, 암호문 E1을 키 K_{ab}로 복호화하여 난수 R_a를 얻는다. 다음으로, 암호문 E2를 키 K_{ab}로 복호화하고, 그 결과와 E1을 배타적 논리합하여 R_b를 얻는다. 마지막으로, 암호문 E3을 키 K_{ab}로 복호화하고, 그 결과와 E2를 배타적 논리합하여 ID (b)를 얻는다. 이렇게 해서 얻어진 R_a, R_b, ID(b) 중, R_b 및 ID(b)가, B가 송신한 것과 일치하는지 검증한다. 이 검증에 통과한 경우, B는 A를 정당한 것으로서 인증한다.

다음으로, B는 인증 후에 사용하는 세션 키[Session Key(이하, K_{ses}로 함)]를 생성한다(생성 방법은 난수를 이용함). 그리고, R_b, R_a, K_{ses} 순으로, DES의 CBC 모드로 키 K_{ab}를 이용하여 암호화하고, A로 반송한다.

이를 수신한 A는 수신 데이터를 키 K_{ab}로 복호화한다. 수신 데이터의 복호화 방법은 B의 복호화 처리와 동일하므로, 여기서는 상세를 생략한다. 이렇게 해서 얻어진 R_b, R_a, K_{ses} 중, R_b 및 R_a가, A가 송신한 것과 일치하는지 검증한다. 이 검증에 통과한 경우, A는 B를 정당한 것으로서 인증한다. 상호 상대를 인증한 후에는 세션 키 K_{ses}는 인증 후 비밀 통신을 위한 공통 키로서 이용된다.

또, 수신 데이터의 검증 시에 부정, 불일치가 발견된 경우에는 상호 인증이 실패한 것으로서 처리를 중단한다.

(3-5) 공개 키 증명서

다음으로, 공개 키 증명서에 대하여 도 14를 이용하여 설명한다. 공개 키 증명서는 공개 키 암호 방식에 있어서의 인증국(CA: Certificate Authority)이 발행하는 증명서로서, 사용자가 자신의 ID, 공개 키 등을 인증국에 제출함으로써, 인증국측이 인증국의 ID나 유효 기한 등의 정보를 부가하고, 또한 인증국에 의한 서명을 부가하여 작성되는 증명서이다.

도 14에 도시한 공개 키 증명서는 증명서의 버전 번호, 인증국이 증명서 이용자에게 할당하는 증명서의 일련 번호, 전자 서명에 이용한 알고리즘 및 파라미터 인증국의 이름, 증명서의 유효 기한, 증명서 이용자의 이름(사용자 ID), 증명서 이용자의 공개 키 및 전자 서명을 포함한다.

전자 서명은 증명서의 버전 번호, 인증국이 증명서 이용자에게 할당하는 증명서의 일련 번호, 전자 서명에 이용한 알고리즘 및 파라미터, 인증국의 이름, 증명서의 유효 기한, 증명서 이용자의 이름 및 증명서 이용자의 공개 키 전체에 대하여 해시 함수를 적용하여 해시값을 생성하고, 그 해시값에 대하여 인증국의 비밀 키를 이용하여 생성한 데이터이다. 이 전자 서명의 생성에는, 예를 들면 도 11에서 설명한 처리 플로우가 적용된다.

인증국은 도 14에 도시한 공개 키 증명서를 발행함과 함께, 유효 기한이 다 된 공개 키 증명서를 갱신하고, 부정을 행한 이용자의 배척을 행하기 위한 부정자 리스트의 작성, 관리, 배포(이를 폐지: Revocation이라 함)를 행한다. 또한, 필요에 따라 공개 키·비밀 키의 생성도 행한다.

한편, 이 공개 키 증명서를 이용할 때, 이용자는 자신이 보유한 인증국의 공개 키를 이용하고, 해당 공개 키 증명서의 전자 서명을 검증하고, 전자 서명의 검증에 성공한 후에 공개 키 증명서로부터 공개 키를 추출하여 해당 공개 키를 이용한다. 따라서, 공개 키 증명서를 이용하는 모든 이용자는 공통의 인증국의 공개 키를 보유하고 있을 필요가 있다. 또, 전자 서명의 검증 방법에 대해서는 도 12에서 설명하였으므로, 그 상세는 생략한다.

(3-6) 공개 키 암호 방식에 의한 상호 인증

다음으로, 공개 키 암호 방식인 160비트 길이의 타원 곡선 암호를 이용한 상호 인증 방법을 도 15를 이용하여 설명한다. 도 15에 있어서, 공개 키 암호 방식으로서 ECC를 이용하고 있지만, 상술한 바와 같이 동일한 공개 키 암호 방식이면 모두 좋다. 또한, 키 사이즈도 160비트가 아니어도 좋다. 도 15에 있어서, 우선 B가 64비트의 난수 R_b를 생성하여 A로 송신한다. 이를 수신한 A는 새롭게 64비트의 난수 R_a 및 표수 p보다 작은 난수 Ak를 생성한다. 그리고, 베이스 포인트 G를 Ak 배한 점 Av=Ak×G를 구하고, R_a, R_b, Av(X 좌표와 Y 좌표)에 대한 전자 서명 A. Sig를 생성하여 A의 공개 키 증명서와 함께 B로 반송한다. 여기서, R_a 및 R_b는 각각 64비트, Av의 X 좌표와 Y 좌표가 각각 160비트이므로, 합계 448비트에 대한 전자 서명을 생성한다. 전자 서명의 생성 방법은 도 11에서 설명하였으므로, 그 상세는 생략한다. 또한, 공개 키 증명서도 도 14에서 설명하였으므로, 그 상세는 생략한다.

A의 공개 키 증명서, R_a, R_b, Av, 전자 서명 A. Sig를 수신한 B는 A가 송신한 R_b가, B가 생성한 것과 일치하는지 검증한다. 그 결과, 일치한 경우에는 A의 공개 키 증명서 내의 전자 서명을 인증국의 공개 키로 검증하고, A의 공개 키를 추출한다. 공개 키 증명서의 검증에 대해서는 도 14를 이용하여 설명하였으므로, 그 상세는 생략한다. 그리고, 추출한 A의 공개 키를 이용하여 전자 서명 A. Sig를 검증한다. 전자 서명의 검증 방법은 도 12에서 설명하였으므로, 그 상세는 생략한다. 전자 서명의 검증에 성공한 후, B는 A를 정당한 것으로서 인증한다.

다음으로, B는 표수 p보다 작은 난수 Bk를 생성한다. 그리고, 베이스 포인트 G를 Bk배한 점 Bv=Bk×G를 구하고, R_b, R_a, Bv(X 좌표와 Y 좌표)에 대한 전자 서명 B. Sig를 생성하여 B의 공개 키 증명서와 함께 A로 반송한다.

B의 공개 키 증명서, R_b, R_a, Av, 전자 서명 B. Sig를 수신한 A는 B가 송신한 R_a가, A가 생성한 것과 일치하는지 검증한다. 그 결과, 일치한 경우에는 B의 공개 키 증명서 내의 전자 서명을 인증국의 공개 키로 검증하여 B의 공개 키를 추출한다. 그리고, 추출한 B의 공개 키를 이용하여 전자 서명 B. Sig를 검증한다. 전자 서명의 검증에 성공한 후, A는 B를 정당한 것으로서 인증한다.

양자가 인증에 성공한 경우에는 B는 Bk×Av(Bk는 난수이지만, Av는 타원 곡선 상의 점이기 때문에, 타원 곡선 상의 점의 스칼라배 계산이 필요)를 계산하고, A는 Ak×Bv를 계산하여, 이들 점의 X 좌표의 하위 64비트를 세션 키로서 이후의 통신에 사용한다(공통 키 암호를 64비트 키 길이의 공통 키 암호로 한 경우). 물론, Y 좌표로부터 세션 키를 생성해도 좋고, 하위 64비트가 아니어도 좋다. 또, 상호 인증 후의 비밀 통신에 있어서는 송신 데이터는 세션 키로 암호화될 뿐만 아니라, 전자 서명도 첨부되는 경우가 있다.

전자 서명의 검증이나 수신 데이터의 검증 시에 부정, 불일치가 발견된 경우에는 상호 인증이 실패한 것으로서 처리를 중단한다.

(3-7) 타원 곡선 암호를 이용한 암호화 처리

다음으로, 타원 곡선 암호를 이용한 암호화에 대하여, 도 16을 이용하여 설명한다. 단계 S21에 있어서, Mx, My를 메세지, p를 표수, a, b를 타원 곡선의 계수(타원 곡선: $y^2=x^3+ax+b$), G를 타원 곡선 상의 베이스 포인트, r을 G의 자리수, G 및 Ks×G를 공개 키(0<Ks<r)로 한다. 단계 S22에서 난수 u를 0<u<r이 되도록 생성하고, 단계 S23에서 공개 키 Ks×G를 u배한 좌표 V를 계산한다. 또, 타원 곡선 상의 스칼라배는 도 11의 단계 S4에서 설명하였으므로, 상세는 생략한다. 단계 S24에서 V의 X 좌표를 Mx배하여 p로 잉여를 구하여 X0으로 하고, 단계 S25에서 V의 Y 좌표를 My배하여 p로 잉여를 구하여 Y0으로 한다. 또, 메세지 길이가 p의 비트 수보다 적은 경우, My는 난수를 사용하여 복호화부에서 My를 파기하도록 한다. 단계 S26에 있어서, u×G를 계산하고, 단계 S27에서 암호문 u×G, (X0, Y0)를 얻는다.

(3-8) 타원 곡선 암호를 이용한 복호화 처리

다음으로, 타원 곡선 암호를 이용한 복호화에 대하여, 도 17을 이용하여 설명한다. 단계 S31에 있어서, u×G, (X0, Y0)을 암호문 데이터 p를 표수, a, b를 타원 곡선의 계수(타원 곡선: $y^2=x^3+ax+b$), G를 타원 곡선 상의 베이스 포인트, r을 G의 자리수, Ks를 비밀 키(0<Ks<r)로 한다. 단계 S32에 있어서, 암호 데이터 u×G를 비밀 키 Ks배하여, 좌표 V(Xv, Yv)를 구한다. 단계 S33에서는 암호 데이터 중, (X0, Y0)의 X 좌표를 추출하여 X1=X0/Xv mod p를 계산하고, 단계 S34에 있어서는 Y 좌표를 추출하여 Y1=Y0/Yv mod p를 계산한다. 그리고, 단계 S35에서 X1을 Mx로 하고, Y1을 My로 하여 메세지를 추출한다. 이 때, My를 메세지로 하고 있지 않은 경우, Y1은 파기한다.

이와 같이 비밀 키를 Ks, 공개 키를 G, Ks×G로 함으로써, 암호화에 사용하는 키와 복호화에 사용하는 키를 다른 키로 할 수 있다.

또한, 공개 키 암호의 다른 예로서는 RSA 암호가 알려져 있지만, 자세한 설명은 생략한다(PKCS#1 Version 2에 상세가 기술되어 있음).

(3-9) 난수 생성 처리

다음으로, 난수의 생성 방법에 대하여 설명한다. 난수의 생성 방법으로서는 열 잡음을 증폭하고, 그 A/D 출력으로부터 생성하는 진성난수 생성법이나, M계열 등의 선형 회로를 복수 조합하여 생성하는 유사난수 생성법 등이 알려져 있다. 또한, DES 등의 공통 키 암호를 이용하여 생성하는 방법도 알려져 있다. 본 예에서는 DES를 이용한 유사난수 생성 방법에 대하여 설명한다(ANSI X9. 17 베이스).

우선, 시간 등의 데이터로부터 얻어진 64비트(이 이하의 비트 수의 경우, 상위 비트를 0으로 함)의 값을 D, Triple-DES에 사용되는 키 정보를 Kr, 난수 발생용의 원인(Seed)을 S로 한다. 이 때, 난수 R은 다음과 같이 계산된다.

I=Triple-DES(Kr, D) … (2-1)

R=Triple-DES(Kr, S^I) … (2-2)

S=Triple-DES(Kr, R^I) … (2-3) … (2)

여기서, Triple-DES()는 제1 인수를 암호 키 정보로 하여 제2 인수치를 Triple-DES로 암호화하는 함수로 하고, 연산 ^은 64비트 단위의 배타적 논리합, 마지막에 생성된 값 S는 신규 Seed(원인)로서 갱신되는 것으로 한다.

이하, 연속해서 난수를 생성하는 경우에는 (2-2), (2-3)을 반복하는 것으로 한다.

이상, 본 발명의 데이터 처리 장치에서 적용 가능한 암호 처리에 관한 각종 처리 형태에 대하여 설명하였다. 다음으로, 본 발명의 데이터 처리 장치에서 실행되는 구체적인 처리에 대하여 상세히 설명한다.

(4) 기록 재생기의 저장 데이터 구성

도 18은 도 3에 도시한 기록 재생기(300)에서의 기록 재생기 암호 처리부 (302)에 구성된 내부 메모리(307)의 데이터 보유 내용을 설명하는 도면이다.

도 18에 도시한 바와 같이 내부 메모리(307)에는 이하의 키, 데이터가 저장되어 있다.

MK_{ake}: 기록 재생기(300)와 기록 디바이스(400: 도 3 참조) 사이에서 실행되는 상호 인증 처리에 필요한 인증 키 [Authentication and Key Exchange Key(이하, K_{ake}로 함)]를 생성하기 위한 기록 디바이스 인증 키용 마스터 키.

IV_{ake}: 기록 디바이스 인증 키용 초기치.

MK_{dis}: 배송 키 K_{dis}를 생성하기 위한 배송 키용 마스터 키.

IV_{dis}: 배송 키 생성용 초기치.

K_{icva}: 체크치 ICV_a를 생성하기 위한 키인 체크치 A 생성 키.

K_{icvb}: 체크치 ICV_b를 생성하기 위한 키인 체크치 B 생성 키.

K_{icvc}: 각 콘텐츠 블록의 체크치 ICV_i(i=1～N)를 생성하기 위한 키인 콘텐츠 체크치 생성 키.

K_{icvt}: 총 체크치 ICV_t를 생성하기 위한 키인 총 체크치 생성 키.

K_{sys}: 신호 분배 시스템에 공통의 서명 또는 ICV를 붙이기 위해서 사용하는 시스템 서명 키.

K_{dev}: 기록 재생기마다 다르고, 기록 재생기가 서명 또는 ICV를 붙이기 위해서 사용하는 기록 재생기 고유의 기록 재생기 서명 키.

IV_{mem}: 초기치, 상호 인증 처리 등의 시의 암호 처리에 이용되는 초기치. 기록 디바이스와 공통.

이들 키, 데이터가 기록 재생기 암호 처리부(302)에 구성된 내부 메모리 (307)에 저장되어 있다.

(5) 기록 디바이스의 저장 데이터 구성

도 19는 기록 디바이스 상에서의 데이터 보유 상황을 나타내는 도면이다. 도 19에 있어서, 내부 메모리(405)는 복수의 블록(본 예에서는 N 블록)으로 분할되어 있으며, 각각의 블록 중에 이하의 키, 데이터가 저장되어 있다.

ID_{mem}: 기록 디바이스 식별 정보, 기록 디바이스 고유의 식별 정보.

K_{ake}: 인증 키, 기록 재생기(300)와의 상호 인증 시에 이용하는 인증 키.

IV_{mem}: 초기치, 상호 인증 처리 등의 시의 암호 처리에 이용되는 초기치.

K_{str}: 보존 키, 블록 정보 키 다른 콘텐츠 데이터의 암호 키.

K_r: 난수 생성 키.

S: 원인

이들 데이터를 개별 블록에 각각 보유하고 있다. 외부 메모리(402)는 복수(본 예에서는 M개)의 콘텐츠 데이터를 보유하고 있으며, 각각 도 4에서 설명한 데이터를 예를 들면 도 26 또는 도 27과 같이 보유하고 있다. 도 26, 도 27의 구성의 차이에 대해서는 후단에서 설명한다.

(6) 기록 재생기, 기록 디바이스 사이에서의 상호 인증 처리

(6-1) 상호 인증 처리의 개요

도 20은 기록 재생기(300)와 기록 디바이스(400)와의 인증 순서를 나타내는 흐름도이다. 단계 S41에 있어서, 이용자가 기록 디바이스(400)를 기록 재생기 (300)에 삽입한다. 단, 비접촉으로 통신할 수 있는 기록 디바이스를 사용하는 경우에는 삽입할 필요는 없다.

기록 재생기(300)에 기록 디바이스(400)를 세트하면, 도 3에 도시한 기록 재생기(300) 내의 기록 디바이스 검지 수단(도시하지 않음)이 제어부(301)에 기록 디바이스(400)의 장착을 통지한다. 다음으로, 단계 S42에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)에 초기화 명령을 송신한다. 이를 수신한 기록 디바이스(400)는 기록 디바이스 암호 처리부(401)의 제어부(403)에 있어서, 통신부(404)를 통해 명령을 수신하여 인증 완료 플래그가 세트되어 있으면 클리어한다. 즉, 미 인증 상태로 설정한다.

다음으로, 단계 S43에 있어서, 기록 재생기(300)의 제어부(301)는 기록 재생기 암호 처리부(302)에 초기화 명령을 송신한다. 이 때, 기록 디바이스 삽입구 번호도 함께 송신한다. 기록 디바이스 삽입구 번호를 송신함으로써, 기록 재생기 (300)에 복수의 기록 디바이스가 접속된 경우라도 동시에 복수의 기록 디바이스 (400)와의 인증 처리 및 데이터 송수신이 가능하게 된다.

초기화 명령을 수신한 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 재생기 암호 처리부(302)의 제어부(306)에 있어서, 기록 디바이스 삽입구 번호에 대응하는 인증 완료 플래그가 세트되어 있으면 클리어한다. 즉, 미 인증 상태로 설정한다.

다음으로, 단계 S44에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)가 사용하는 키 블록 번호를 지정한다. 또, 키 블록 번호가 상세히 관해서는 후술한다. 단계 S45에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스(400)의 내부 메모리(405)의 지정된 키 블록에 저장된 기록 디바이스 식별 정보 ID_{mem}을 판독한다. 단계 S46에 있어서, 기록 재생기(300)의 제어부(301)는 기록 재생기 암호 처리부(302)에 기록 디바이스 식별 정보 ID_{mem}을 송신하여, 기록 디바이스 식별 정보 ID_{mem}에 기초한 인증 키 K_{ake} 를 생성시킨다. 인증 키 K_{ake}의 생성 방법은 예를 들면 다음과 같다.

$K_{ake}=DES(MK_{ake}, ID_{mem}\hat{}IV_{ake})$ …… (3)

여기서, MK_{ake}는 기록 재생기(300)와 기록 디바이스(400: 도 3 참조) 사이에서 실행되는 상호 인증 처리에 필요한 인증 키 K_{ake}를 생성하기 위한 기록 디바이스 인증 키용 마스터 키로서, 이는 상술한 바와 같이 기록 재생기(300)의 내부 메모리 (307)에 저장되어 있는 키이다. 또한, ID_{mem}은 기록 디바이스(400)에 고유한 기록 디바이스 식별 정보이다. 또한, IV_{ake}는 기록 디바이스 인증 키용 초기치이다. 또한, 상기 식에 있어서, DES()는 제1 인수를 암호 키로 하여 제2 인수치를 DES로 암호화하는 함수이고, 연산 ^은 64 비트 단위의 배타적 논리합을 나타낸다.

예를 들면 도 7, 도 8에 도시한 DES 구성을 적용하는 경우에는 도 7, 8에 도시한 메세지 M을 기록 디바이스 식별 정보: ID_{mem}으로 하고, 키 K1을 디바이스 인증 키용 마스터 키: MK_{ake}로 하고, 초기치 IV를: IV_{ake}로 하여 얻어지는 출력이 인증 키 K_{ake}가 된다.

다음으로, 단계 S47에서 상호 인증 및 세션 키 K_{ses}의 생성 처리를 행한다. 상호 인증은 기록 재생기 암호 처리부(302)의 암호/복호화부(308)와 기록 디바이스 암호 처리부(401)의 암호/복호화부(406) 사이에서 행해지고, 그 중개를 기록 재생기(300)의 제어부(301)가 행하고 있다.

상호 인증 처리는 예를 들면 상술한 도 13에서 설명한 처리에 따라 실행할 수 있다. 도 13에 도시한 구성에 있어서, A, B가 각각 기록 재생기(300)와 기록 디바이스(400)에 대응한다. 우선, 기록 재생기(300)의 기록 재생기 암호 처리부 (302)가 난수 R_b를 생성하고, 난수 R_b 및 자신의 ID인 기록 재생기 식별 정보 ID_{dev}를 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)로 송신한다. 또, 기록 재생기 식별 정보 ID_{dev}는 기록 재생기(300) 내에 구성된 기억부에 기억된 재생기 고유의 식별자이다. 기록 재생기 암호 처리부(302)의 내부 메모리 중에 기록 재생기 식별 정보 ID_{dev}를 기록하는 구성으로 하여도 좋다.

난수 R_b 및 기록 재생기 식별 정보 ID_{dev}를 수신한 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)는 새롭게 64비트의 난수 R_a를 생성하고, R_a, R_b 와 기록 재생기 식별 정보 ID_{dev} 순으로, DES의 CBC 모드로 인증 키 K_{ake}를 이용하여 데이터를 암호화하고, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 반송한다. 예를 들면, 도 7에 도시한 DES의 CBC 모드 처리 구성에 따르면, R_a가 M1, R_b가 M2, ID_{dev}가 M3에 상당하여 초기치: IV=IV_{mem}로 했을 때의 출력 E1, E2, E3이 암호문이 된다.

암호문 E1, E2, E3을 수신한 기록 재생기(300)의 기록 재생기 암호 처리부 (302)는 수신 데이터를 인증 키 K_{ake}로 복호화한다. 수신 데이터의 복호화 방법은 우선, 암호문 E1을 인증 키 K_{ake}로 복호화하고, 그 결과와 IV_{mem}을 배타적 논리합하여 난수 R_a를 얻는다. 다음으로, 암호문 E2를 인증 키 K_{ake}로 복호화하고, 그 결과와 E1을 배타적 논리합하여 R_b를 얻는다. 마지막으로, 암호문 E3을 인증 키 K_{ake}로 복호화하고, 그 결과와 E2를 배타적 논리합하여 기록 재생기 식별 정보 ID_{dev}를 얻는다. 이렇게 해서 얻어진 R_a, R_b, 기록 재생기 식별 정보 ID_{dev} 중, R_b 및 기록 재생기 식별 정보 ID_{dev}가, 기록 재생기(300)가 송신한 것과 일치하는지 검증한다. 이 검증에 통과한 경우, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 디바이스(400)를 정당한 것으로서 인증한다.

다음으로, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 인증 후에 사용하는 세션 키[Session Key(이하, K_{ses}로 함)]를 생성한다(생성 방법은 난수를 이용함). 그리고, R_b, R_a, K_{ses} 순으로, DES의 CBC 모드로 키 K_{ake} , 초기치 IV_{mem}을 이용하여 암호화하고, 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)로 반송한다.

이를 수신한 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)는 수신 데이터를 키 K_{ake}로 복호화한다. 수신 데이터의 복호화 방법은 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 있어서의 복호화 처리와 동일하므로, 여기서는 상세를 생략한다. 이렇게 해서 얻어진 R_b, R_a, K_{ses} 중, R_b 및 R_a가, 기록 디바이스 (400)가 송신한 것과 일치하는지 검증한다. 이 검증에 통과한 경우, 기록 디바이스(400)의 기록 디바이스 암호 처리부(401)는 기록 재생기(300)를 정당한 것으로서 인증한다. 상호 상대를 인증한 후에는, 세션 키 K_{ses}는 인증 후의 비밀 통신을 위한 공통 키로서 이용된다.

또, 수신 데이터의 검증 시에 부정, 불일치가 발견된 경우에는 상호 인증이 실패한 것으로서 처리를 중단한다.

상호 인증에 성공한 경우에는 단계 S48에서 단계 S49로 진행하여, 세션 키 K_{ses}를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 보유함과 함께, 상호 인증이 종료한 것을 나타내는 인증 완료 플래그를 세트한다. 또한, 상호 인증에 실패한 경우에는 단계 S50으로 진행하여, 인증 처리 과정에서 생성된 세션 키 K_{ses}를 파기함과 함께, 인증 완료 플래그를 클리어한다. 또, 이미 클리어되어 있는 경우에는 반드시 클리어 처리는 필요하지 않다.

또, 기록 디바이스(400)가 기록 디바이스 삽입구로부터 제거된 경우에는 기록 재생기(300) 내의 기록 디바이스 검지 수단이 기록 재생기(300)의 제어부(301)에 기록 디바이스(400)가 제거된 것을 통지하고, 이를 받은 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 대하여 기록 디바이스 삽입구 번호에 대응하는 인증 완료 플래그를 클리어하도록 명령하고, 이를 받은 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 디바이스 삽입구 번호에 대응하는 인증 완료 플래그를 클리어한다.

또, 여기서는 상호 인증 처리를 도 13에 도시한 수속에 따라 실행하는 예에 대하여 설명하였지만, 상술한 인증 처리예에 한하지 않고, 예를 들면 먼저 설명한 도 15의 상호 인증 수속에 따른 처리를 실행해도 좋다. 또한, 도 13에 도시한 수속에 있어서, 도 13의 A를 기록 재생기(300)로 하고, B를 기록 디바이스(400)로 하여, B: 기록 디바이스(400)가 A: 기록 재생기

(300)에 최초로 송부하는 ID를 기록 디바이스 중의 키 블록 중의 기록 디바이스 식별 정보로서 상호 인증 처리를 행해도 좋다. 본 발명에 있어서 실행되는 인증 처리 수속은 여러가지 처리가 적용 가능하고, 상술한 인증 처리에 한정되는 것이 아니다.

(6-2) 상호 인증 시의 키 블록의 전환

본 발명의 데이터 처리 장치에서의 상호 인증 처리에 있어서의 하나의 특징은 기록 디바이스(400)측에 복수의 키 블록(ex. N개의 키 블록)을 구성하여, 기록 재생기(300)가 하나의 키 블록을 지정(도 20의 처리 플로우에 있어서의 단계 S44) 하여 인증 처리를 실행하는 점이다. 앞서 도 19에 있어서 설명한 바와 같이 기록 디바이스(400)의 암호 처리부(401)에 구성된 내부 메모리(405)에는 복수의 키 블록이 형성되어 있으며, 각각이 다른 키 데이터 ID 정보 등 각종 데이터를 저장하고 있다. 도 20에서 설명한 기록 재생기(300)와 기록 디바이스(400) 사이에서 실행되는 상호 인증 처리는 도 19의 기록 디바이스(400)의 복수의 키 블록의 하나의 키 블록에 대하여 실행된다.

종래, 기억 매체와 그 재생 기기 사이에서의 상호 인증 처리를 실행하는 구성에서는 상호 인증에 이용하는 키: 인증 키는 공통인 것이 사용되는 것이 일반적이었다. 따라서, 예를 들면 제품 발송처(나라별)별 또는 제품별 인증 키를 변경하고자 하면, 기록 재생기측과, 기록 디바이스측의 인증 처리에 필요한 키 데이터를 쌍방의 기기에 있어서 변경하는 것이 필요하다. 따라서, 예를 들면 새롭게 발매된 기록 재생기에 저장된 인증 처리에 필요한 키 데이터는 먼저 판매된 기록 디바이스에 저장된 인증 처리에 필요한 키 데이터에 대응하지 않고, 새로운 기록 재생기는 오래된 버전의 기록 디바이스로의 액세스를 할 수 없게 되는 사태가 발생한다. 반대로, 새로운 버전의 기록 디바이스와 오래된 버전의 기록 재생기와의 관계에 있어서도 동일한 사태가 발생한다.

본 발명의 데이터 처리 장치에서는 도 19에 도시한 바와 같이 사전에 기록 디바이스(400)에 복수의 다른 키 세트로서의 키 블록이 저장되어 있다. 기록 재생기는 예를 들면 제품 발송처(나라별)별 또는 제품, 기종, 버전, 어플리케이션별로 인증 처리에 적용해야 할 키 블록, 즉 지정 키 블록이 설정된다. 이 설정 정보는 기록 재생기의 메모리부, 예를 들면, 도 3에 있어서의 내부 메모리(307) 또는 기록 재생기(300)가 갖는 그 밖의 기억 소자 내에 저장되고, 인증 처리 시에 도 3의 제어부(301)에 의해 액세스되어 설정 정보에 따른 키 블록 지정이 행해진다.

기록 재생기(300)의 내부 메모리(307)의 기록 디바이스 인증 키용 마스터 키 MK_{ake}는 각각의 지정 키 블록의 설정에 따라 설정된 인증 키용 마스터 키로서, 지정 키 블록에만 대응 가능하게 되어 있으며, 지정 키 블록 이외의 키 블록과의 상호 인증은 성립하지 않은 구성으로 되어 있다.

도 19에서 알 수 있는 바와 같이, 기록 디바이스(400)의 내부 메모리(405)에는 1～N의 N개의 키 블록이 설정되고, 각 키 블록마다 기록 디바이스 식별 정보, 인증 키, 초기치, 보존 키, 난수 생성 키, 원인이 저장되고, 적어도 인증용 기입 데이터가 블록마다 다른 데이터로서 저장되어 있다.

이와 같이 기록 디바이스(400)의 키 블록의 키 데이터 구성은 블록마다 다르다. 따라서, 예를 들면, 어떤 기록 재생 기기 A가 내부 메모리에 저장된 기록 디바이스 인증 키용 마스터 키 MK_{ake}를 이용하여 인증 처리를 행하여 얻는 키 블록은 키 블록 No. 1이고, 또한 다른 사양의 기록 재생기 B가 인증 가능한 키 블록은 다른 키 블록, 예를 들면 키 블록 No. 2와 같이 설정할 수 있다.

후단에서 더욱 상세하게 설명하지만, 콘텐츠를 기록 디바이스(400)의 외부 메모리(402)에 저장할 때, 각 키 블록에 저장된 보존 키 K_{str}를 이용하여 암호화 처리가 이루어져 저장된다. 보다 구체적으로는 콘텐츠 블록을 암호화하는 콘텐츠 키를 보존 키로 암호화 처리한다.

도 19에 도시한 바와 같이 보존 키는 각 블록마다 다른 키로서 구성되어 있다. 따라서, 다른 키 블록을 지정하도록 설정된 두 개의 다른 설정의 기록 재생기 사이에서는 어떤 하나의 기록 디바이스의 메모리에 저장된 콘텐츠를 양자로 공통으로 이용하는 것은 방지된다. 즉, 다른 설정이 이루어진 기록 재생기는 각각의 설정에 합치하는 기록 디바이스에 저장된 콘텐츠만 이용할 수 있다.

또, 각 키 블록에 대하여 공통화 가능한 데이터는 공통화할 수도 있고, 예를 들면 인증용 키 데이터, 보존 키 데이터만을 다르게 구성해도 좋다.

이러한 기록 디바이스에 복수의 다른 키 데이터로 이루어진 키 블록을 구성하는 구체예로서는, 예를 들면 기록 재생기(300)의 기종별(거치형, 휴대형 등)로 지정해야 할 키 블록 번호를 다르게 설정하거나, 어플리케이션마다 지정 키 블록을 다르게 설정하는 예가 있다. 또한, 예를 들면 일본에서 판매하는 기록 재생기에 대해서는 지정 키 블록을 No. 1로 하고, 미국에서 판매하는 기록 재생기는 지정 키 블록을 No. 2로 하도록 지역마다 다른 키 블록 설정을 행하는 구성으로 할 수도 있다. 이러한 구성으로 함으로써, 각각의 다른 판매 지역에서 사용되고, 기록 디바이스에 다른 보존 키로 저장된 콘텐츠는, 가령 메모리 카드와 같은 기록 디바이스가 미국에서 일본, 또는 일본에서 미국으로 전송되어 와도, 다른 키 설정이 이루어진 기록 재생기로 이용할 수 없기 때문에, 메모리에 저장한 콘텐츠의 부정, 불법 유통을 방지할 수 있다. 구체적으로는 다른 보존 키 K_{str}로 암호화되어 있는 콘텐츠 키 K_{con}이 두 나라 사이에서 상호 이용 가능한 상태를 배제할 수 있다.

또한, 도 19에 도시한 기록 디바이스(400)의 내부 메모리(405)의 키 블록 1 ~N까지의 적어도 하나의 키 블록, 예를 들면 No. N의 키 블록을 어느 하나의 기록 재생기(300)에서도 공통으로 이용 가능한 키 블록으로 하여 구성해도 좋다.

예를 들면, 모든 기기에 키 블록 No. N과의 인증 가능한 기록 디바이스 인증 키용 마스터 키 MK_{ake}를 저장함으로써, 기록 재생기(300)의 기종별, 어플리케이션별, 발송 나라별 등과 무관하게 유통 가능한 콘텐츠로 취급할 수 있다. 예를 들면, 키 블록 No. N에 저장된 보존 키로 메모리 카드에 저장된 암호화 콘텐츠는 모든 기기에 있어서 이용 가능한 콘텐츠가 된다. 예를 들면, 음악 데이터 등을 공통으로 이용 가능한 키 블록의 보존 키로 암호화하여 메모리 카드에 기억하고, 이 메모리 카드를 역시 공통의 기록 디바이스 인증 키용 마스터 키 MK_{ake}를 저장한 예를 들면 휴대형 음성 재생 기기 등으로 세트함으로써, 메모리 카드로부터의 데이터의 복호 재생 처리를 가능하게 할 수 있다.

본 발명의 데이터 처리 장치에서의 복수의 키 블록을 갖는 기록 디바이스의 이용 예를 도 21에 도시한다. 기록 재생기(2101)는 일본용 제품의 기록 재생기로서, 기록 디바이스의 키 블록의 No. 1, 4 사이에서의 인증 처리가 성립하는 마스터 키를 갖고 있다. 기록 재생기(2102)는 US용 제품의 기록 재생기로서, 기록 디바이스의 키 블록의 No. 2, 4 사이에서의 인증 처리가 성립하는 마스터 키를 갖고 있다. 기록 재생기(2103)는 EU용 제품의 기록 재생기이고, 기록 디바이스의 키 블록의 No. 3, 4 사이에서의 인증 처리가 성립하는 마스터 키를 갖고 있다.

예를 들면, 기록 재생기(2101)는 기록 디바이스 A, 참조 번호(2104)의 키 블록 1 또는 키 블록 4 사이에서 인증이 성립하고, 각각의 키 블록에 저장된 보존 키를 통한 암호 처리를 실시한 콘텐츠가 외부 메모리에 저장된다. 기록 재생기 (2102)는 기록 디바이스 B, 참조 번호(2105)의 키 블록 2 또는 키 블록 4 사이에서 인증이 성립하고, 각각의 키 블록에 저장된 보존 키를 통한 암호 처리를 실시한 콘텐츠가 외부 메모리에 저장된다. 기록 재생기(2103)는 기록 디바이스 C, 참조 번호(2106)의 키 블록 3 또는 키 블록 4 사이에서 인증이 성립하고, 각각의 키 블록에 저장된 보존 키를 통한 암호 처리를 실시한 콘텐츠가 외부 메모리에 저장된다. 여기서, 기록 디바이스 A, 참조 번호(2104)를 기록 재생기(2102) 또는 기록 재생기(2103)에 장착한 경우, 키 블록 1의 보존 키로 암호 처리가 이루어진 콘텐츠는 기록 재생기(2102), 기록 재생기(2103)와 키 블록 1 사이에서의 인증이 성립하지 않기 때문에 이용 불가능하게 된다. 한편, 키 블록 4의 보존 키로 암호 처리가 이루어진 콘텐츠는 기록 재생기(2102), 기록 재생기(2103)와 키 블록 4 사이에서의 인증이 성립하기 때문에 이용 가능하게 된다.

상술한 바와 같이 본 발명의 데이터 처리 장치에서는 기록 디바이스에 복수의 다른 키 세트로 이루어진 키 블록을 구성하고, 한편 기록 재생 기기에는 특정한 키 블록에 대한 인증 가능한 마스터 키를 저장하는 구성으로 하였기 때문에, 여러가지 이용 형태에 따른 콘텐츠 이용 제한을 설정할 수 있다.

또, 하나의 기록 재생 기기에 있어서 지정 가능한 키 블록을 복수, 예를 들면 1~k로 하고, 다른 기록 재생기에 있어서 지정 가능한 키 블록을 p~q와 같이 복수로 할 수도 있고, 또한 공통으로 이용 가능한 키 블록을 복수 설치하는 구성으로 해도 좋다.

(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리

다음으로, 본 발명의 데이터 처리 장치에서 기록 재생기(300)로부터 기록 디바이스(400)의 외부 메모리에 콘텐츠를 다운로드하는 처리에 대하여 설명한다.

도 22는 기록 재생기(300)로부터 기록 디바이스(400)로 콘텐츠를 다운로드하는 순서를 설명하는 흐름도이다. 또, 도 22에서는 이미 기록 재생기(300)와 기록 디바이스(400) 사이에서 상술한 상호 인증 처리가 완료하고 있는 것으로 한다.

단계 S51에 있어서, 기록 재생기(300)의 제어부(301)는 판독부(304)를 사용하여 콘텐츠를 저장한 미디어(500)로부터 소정의 포맷에 따른 데이터를 판독하거나, 통신부(305)를 사용하여 통신 수단(600)으로부터 소정의 포맷에 따라 데이터를 수신한다. 그리고, 기록 재생기(300)의 제어부(301)는 데이터 내의 헤더(Header) 부분(도 4 참조)을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다.

다음으로, 단계 S52에 있어서, 단계 S51에서 헤더(Header)를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 체크치 A를 계산시킨다. 체크치 A는 도 23에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보(Content ID)와 취급 방침(Usage Policy)을 메세지로 하여 도 7에서 설명한 ICV 계산 방법에 따라 계산된다. 또, 초기치는 IV=0으로서도, 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 체크치 A 생성용 초기치 IVa를 보존해 두고, 그것을 사용해도 좋다. 마지막으로, 체크치 A와 헤더 (Header) 내에 저장된 체크치:ICV_a를 비교하여, 일치한 경우에는 단계 S53으로 진행한다.

앞서 도 4에 있어서 설명한 바와 같이 체크치 A, ICV_a는 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보 (Content ID)와 취급 방침(Usage Policy)을 메세지로 하여 도 7에서 설명한 ICV 계산 방법에 따라 계산되는 체크치 A가 헤더 (Header) 내에 저장된 체크치:ICV_a와 일치한 경우에는 식별 정보, 취급 방침의 변경은 없다고 판단된다.

다음으로, 단계 S53에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 배송 키 K_{dis}의 생성을 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 행하게 한다. 배송 키 K_{dis}의 생성 방법으로서는 예를 들면 다음과 같다.

K_{dis}=DES(MK_{dis}, Content ID^IV_{dis}) (4)

여기서, MK_{dis}는 배송 키 K_{dis}를 생성하기 위한 배송 키용 마스터 키로서, 이는 상술한 바와 같이 기록 재생기(300)의 내부 메모리에 저장되어 있는 키이다. 또한, Content ID는 콘텐츠 데이터의 헤더부의 식별 정보이고, 또한 IV_{dis}는 배송 키용 초기치이다. 또한, 상기 식에 있어서, DES()는 제1 인수를 암호 키로 하여 제2 인수치를 암호화하는 함수이고, 연산 ^은 64비트 단위의 배타적 논리합을 나타낸다.

단계 S54에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)를 사용하여 단계 S53에서 생성한 배송 키 K_{dis}를 이용하여 판독부(304)를 통해 수신한 미디어(500) 또는 통신부(305)를 통해 통신 수단(600)으로부터 수신한 데이터의 헤더부에 저장된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}(도 4 참조)의 복호화 처리를 행한다. 도 4에 도시된 바와 같이 이들 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}은 DVD, CD 등의 미디어 또는 인터넷 등의 통신로 상에서는 배송 키 K_{dis}에 의해 사전에 암호화 처리가 실시되어 있다.

또한, 단계 S55에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)를 사용하여 단계 S54에서 복호화한 블록 정보 키 K_{bit}로 블록 정보(BIT)를 복호화한다. 도 4에 도시된 바와 같이 블록 정보(BIT)는 DVD, CD 등의 미디어 또는 인터넷 등의 통신로 상에서는 블록 정보 키 K_{bit}에 의해 사전에 암호화 처리가 실시되어 있다.

또한, 단계 S56에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)를 8바이트 단위로 분할하여, 이들 모두를 배타적 논리합한다(가산, 감산 등, 어느 연산이라도 좋음). 다음으로, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 체크치 B(ICV_b)를 계산시킨다. 체크치 B는 도 24에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 조금전에 계산한 배타적 논리합 값을 DES로 암호화하여 생성한다. 마지막으로, 체크치 B와 Header 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S57로 진행한다.

앞서 도 4에 있어서 설명한 바와 같이 체크치 B, ICV_b는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보(BIT)의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)를 8바이트 단위로 분할하여 배타적 논리합하여 얻어지는 값을 DES로 암호화하여 생성한 체크치 B가 헤더(Header) 내에 저장된 체크치:ICV_b와 일치한 경우에는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경은 없다고 판단된다.

단계 S57에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 중간 체크치의 계산을 시킨다. 중간 체크치는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 총 체크치 생성 키 K_{icvt}를 키로 하고, 검증한 헤더 (Header) 내의 체크치 A, 체크치 B, 보유해 둔 모든 콘텐츠 체크치를 메세지로 하여 도 7에서 설명한 ICV 계산 방법에 따라 계산한다. 또, 초기치 IV=0으로 해도, 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 총 체크치 생성용 초기치 IVt를 보존해 두고, 그것을 사용해도 좋다. 또한, 생성된 중간 체크치는 필요에 따라 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 보유해 둔다.

이 중간 체크치는 체크치 A, 체크치 B, 모든 콘텐츠 체크치를 메세지로 하여 생성되는 것으로서, 이들 각 체크치의 검증 대상으로 되어 있는 데이터에 대한 검증을 중간 체크치의 대조 처리에 의해 행해도 좋다. 그러나, 본 실시예에서는 시스템 전체의 공유 데이터로서의 비변경성 검증 처리와, 다운로드 처리 후에 각 기록 재생 기기(300)만이 점유하는 점유 데이터로서 식별하기 위한 검증 처리를 구별하여 실행 가능하게 하기 위해서, 중간 체크치로부터 또한 복수의 다른 체크치, 즉 총 체크치 ICV_t와, 기록 재생기 고유 체크치 ICV_{dev}를 각각, 중간 체크치에 기초하여 생성 가능하게 하고 있다. 이들 체크치에 대해서는 후단에서 설명한다.

기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부 (302)의 암호/복호화부(308)에 총 체크치 ICV_t의 계산을 시킨다. 총 체크치 ICV_t는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 시스템 서명 키 K_{sys}를 키로 하고, 중간 체크치를 DES로 암호화하여 생성한다. 마지막으로, 생성된 총 체크치 ICV_t와 단계 S51에서 보존해 둔 Header 내의 ICV_t를 비교하여, 일치한 경우에는 단계 S58로 진행한다. 시스템 서명 키 K_{sys}는 복수의 기록 재생기, 즉 어떤 일정한 데이터의 기록 재생 처리를 실행하는 시스템 집합 전체에 있어서 공통되는 서명 키이다.

앞서 도 4에 있어서 설명한 바와 같이 총 체크치 ICV_t는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 모든 변경을 검증하기 위한 체크치이다. 따라서, 상술한 처리에 의해 생성된 총 체크치가 헤더(Header) 내에 저장된 체크치:ICV_t와 일치한 경우에는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치의 모든 변경은 없다고 판단된다.

다음으로, 단계 S58에 있어서, 기록 재생기(300)의 제어부(301)는 블록 정보 (BIT) 내의 콘텐츠 블록 정보를 추출하여, 콘텐츠 블록이 검증 대상으로 되어 있는지의 여부를 조사한다. 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 헤더 중의 블록 정보 중에 콘텐츠 체크치가 저장되어 있다.

콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 해당하는 콘텐츠 블록을 기록 재생기(300)의 판독부(304)를 사용하여 미디어(500)로부터 판독하거나, 기록 재생기(300)의 통신부(305)를 사용하여 통신 수단(600)으로부터 수신하여, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다. 이를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부 (308)에 콘텐츠 중간치를 계산시킨다.

콘텐츠 중간치는 단계 S54에서 복호화한 콘텐츠 키 K_{con}로 입력된 콘텐츠 블록을 DES의 CBC 모드로 복호화하고, 그 결과를 8바이트마다 구획하여 전부 배타적 논리합(가산, 감산 등, 어느 연산이라도 좋다)하여 생성한다.

다음으로, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 콘텐츠 체크치의 계산을 시킨다. 콘텐츠 체크치는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 콘텐츠 체크치 생성 키 K_{icvc}를 키로 하고, 콘텐츠 중간치를 DES로 암호화하여 생성한다. 그리고, 기록 재생기 암호 처리부(302)의 제어부(306)는 해당 콘텐츠 체크치와, 단계 S51에서 기록 재생기(300)의 제어부(301)로부터 수신한 콘텐츠 블록 내의 ICV를 비교하여, 그 결과를 기록 재생기(300)의 제어부(301)에 건네 준다. 이를 수신한 기록 재생기(300)의 제어부(301)

는 검증에 성공한 경우, 다음 검증 대상 콘텐츠 블록을 추출하여 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 검증시키고, 모든 콘텐츠 블록을 검증할 때까지 동일한 검증 처리를 반복한다. 또, Header 생성측과 맞춰 두면, IV=0으로 해도, 기록 재생기 암호 처리부(302)의 내부 메모리 (307)에 콘텐츠 체크치 생성용 초기치 IVc를 보존해 두고, 그것을 사용해도 좋다. 또한, 체크한 모든 콘텐츠 체크치는 기록 재생기(300)의 기록 재생기 암호 처리부 (302)에 보유해 둔다. 또한, 기록 재생기(300)의 기록 재생기 암호 처리부 (302)는 검증 대상의 콘텐츠 블록의 검증 순서를 감시하여, 순서가 틀렸거나, 동일한 콘텐츠 블록을 2회 이상 검증된 경우에는 인증에 실패한 것으로 한다. 그리고, 모든 검증이 성공한 경우에는 단계 S59로 진행한다.

다음으로, 단계 S59에 있어서, 기록 재생기(300)의 기록 재생기 암호 처리부 (302)는 단계 S54에서 복호화해 둔 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화시킨다. 기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기(300)의 기록 재생기 암호 처리부 (302)로부터 판독하고, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러 (303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S60에 있어서, 기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 디바이스(400)는 수신된 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화시키고, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시킨다. 마지막으로, 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러 (303)를 통해 기록 디바이스(400)로부터 보존 키 K_{str}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 판독한다. 그리고, 이들 키를 배송 키 K_{dis}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}으로 치환한다.

단계 S61에 있어서, 기록 재생기(300)의 제어부(301)는 데이터의 헤더부의 취급 방침(Usage Policy)으로부터 이용 제한 정보를 추출하여, 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는지(이 경우, 이용 제한 정보가 1로 설정), 다른 동일한 기록 재생기(300)라도 이용할 수 있는지(이 경우, 이용 제한 정보가 0으로 설정)를 판정한다. 판정 결과, 이용 제한 정보가 1인 경우에는 단계 S62로 진행한다.

단계 S62에 있어서, 기록 재생기(300)의 제어부(301)는 기록 재생기 고유의 체크치를 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 계산시킨다. 기록 재생기 고유의 체크치는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 기록 재생기 서명 키 K_{dev}를 키로 하고, 단계 S58에서 보유해 둔 중간 체크치를 DES로 암호화하여 생성한다. 계산된 기록 재생기 고유의 체크치 ICV_{dev}는 총 체크치 ICV_t 대신에 덧씌우기된다.

앞서 설명한 바와 같이 시스템 서명 키 K_{sys}는 신호 분배 시스템에 공통의 서명 또는 ICV를 붙이기 위해서 사용하는 시스템 서명 키이고, 또한 기록 재생기 서명 키 K_{dev}는 기록 재생기마다 다르고, 기록 재생기가 서명 또는 ICV를 붙이기 위해서 사용하는 기록 재생기 서명 키이다. 즉, 시스템 서명 키 K_{sys}에 의해 서명된 데이터는 동일한 시스템 서명 키를 갖는 시스템(기록 재생기)에 의해 체크가 성공, 즉 총 체크치 ICV_t가 일치하게 되기 때문에 공통으로 이용 가능하게 되지만, 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 경우에는 기록 재생기 서명 키는 그 기록 재생기에 고유의 키이기 때문에 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 데이터, 즉 서명 후, 기록 디바이스에 저장된 데이터는 다른 기록 재생기에 그 기록 디바이스를 장착하여 재생하고자 한 경우, 기록 재생기 고유의 체크치 ICV_{dev}가 불일치가 되어 에러가 되기 때문에, 재생할 수 없게 된다.

따라서, 본 발명의 데이터 처리 장치에서는 이용 제한 정보의 설정에 의해 시스템에 공통으로 사용할 수 있는 콘텐츠, 기록 재생기 고유하게 이용할 수 있는 콘텐츠를 자유롭게 설정할 수 있다.

단계 S63에 있어서, 기록 재생기(300)의 제어부(301)는 콘텐츠를 기록 디바이스(400)의 외부 메모리(402)에 보존한다.

도 26은 이용 제한 정보가 0인 경우에 있어서의 기록 디바이스 내의 콘텐츠 상황을 나타내는 도면이다. 도 27은 이용 제한 정보가 1인 경우에 있어서의 기록 디바이스 내의 콘텐츠 상황을 나타내는 도면이다. 도 26이 도 4와 다른 점은 콘텐츠 블

록 정보 키 K_{bit}와 콘텐츠 키 K_{con}이 배송 키 K_{dis}로 암호화되어 있거나, 보존 키 K_{str}로 암호화되어 있다는 점이다. 또한, 도 27이 도 26과 다른 점은 중간 체크치로부터 계산되는 체크치가 도 26에는 시스템 서명 키 K_{sys}로 암호화되어 있는 데 반해, 도 27에서는 기록 재생기 고유의 기록 재생기 서명 키 K_{dev}로 암호화되어 있는 것이다.

또, 도 22의 처리 플로우에 있어서, 단계 S52에서 체크치 A의 검증에 실패한 경우, 단계 S56에서 체크치 B의 검증에 실패한 경우, 단계 S57에서 총 체크치 ICV_t의 검증에 실패한 경우, 단계 S58에서 각 콘텐츠 블록의 콘텐츠 체크치의 검증에 실패한 경우에는 단계 S64로 진행하고, 소정의 에러 표시를 행한다.

또한, 단계 S61에서 이용 제한 정보가 0인 경우에는 단계 S62를 스킵하여 단계 S63으로 진행한다.

(8) 기록 디바이스 저장 정보의 기록 재생기에서의 재생 처리

다음으로, 기록 디바이스(400)의 외부 메모리(402)에 저장된 콘텐츠 정보의 기록 재생기(300)에서의 재생 처리에 대하여 설명한다.

도 28은 기록 재생기(300)가 기록 디바이스(400)로부터 콘텐츠를 판독하여, 콘텐츠를 이용하는 순서를 설명하는 흐름도이다. 또, 도 28에 있어서도, 이미 기록 재생기(300)와 기록 디바이스(400) 사이에서 상호 인증이 완료하고 있는 것으로 한다.

단계 S71에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스 컨트롤러(303)를 사용하여 기록 디바이스(400)의 외부 메모리(402)로부터 콘텐츠를 판독한다. 그리고, 기록 재생기(300)의 제어부(301)는 데이터 내의 헤더(Header) 부분을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다. 단계 S72는 「(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리」에서 설명한 단계 S52와 동일한 처리이고, 헤더(Header)를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)가 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 체크치 A를 계산시키는 처리이다. 체크치 A는 먼저 설명한 도 23에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보(Content ID)와 취급 방침(Usage Policy)을 메세지로 하여, 도 7에서 설명한 것과 동일한 ICV 계산 방법에 따라 계산된다.

앞서 설명한 바와 같이 체크치 A, ICV_a는 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보(Content ID)와 취급 방침(Usage Policy)을 메세지로 하여 도 7에서 설명한 ICV 계산 방법에 따라 계산되는 체크치 A가 헤더(Header) 내에 저장된 체크치:ICV_a와 일치한 경우에는 기록 디바이스(400)에 저장된 식별 정보, 취급 방침의 변경은 없다고 판단된다.

다음으로, 단계 S73에 있어서, 기록 재생기(300)의 제어부(301)는 판독한 헤더(Header) 부분으로부터 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 추출하고, 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다. 기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 디바이스(400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 복호화 처리시키고, 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 재 암호화시킨다. 그리고, 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로부터 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 판독한다.

다음으로, 단계 S74에 있어서, 기록 재생기(300)의 제어부(301)는 수신한 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다.

세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화시킨다. 그리고, 복호화한 블록 정보 키 K_{bit}로 단계 S71에서 수신해 둔 블록 정보를 복호화시킨다.

또, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 복호화한 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보 BIT를 단계 S71에서 수신해 둔 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보 BIT로 치환해 보유해 둔다. 또한, 기록 재생기(300)의 제어부(301)는 복호화된 블록 정보 BIT를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독해 둔다.

단계 S75는 「(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리」에 서 설명한 단계 S56과 동일한 처리이다. 기록 재생기 암호 처리부(302)의 제어부 (306)가 기록 디바이스(400)로부터 판독한 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)를 8바이트 단위로 분할하여, 이들 모두를 배타적 논리합한다. 다음으로, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부 (302)의 암호/복호화부(308)에 체크치 B(ICV_b)를 계산시킨다. 앞서 설명한 도 24에 도시한 바와 같이 체크치 B는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하여, 조금전에 계산한 배타적 논리합 값을 DES로 암호화하여 생성한다. 마지막으로, 체크치 B와 Header 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S76으로 진행한다.

앞서 설명한 바와 같이 체크치 B, ICV_b는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} , 블록 정보의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 기록 디바이스(400)로부터 판독한 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보 (BIT)를 8바이트 단위로 분할하여 배타적 논리합하여 얻어지는 값을 DES로 암호화하여 생성한 체크치 B가 기록 디바이스(400)로부터 판독한 데이터 중 헤더 (Header) 내에 저장된 체크치:ICV_b와 일치한 경우에는 기록 디바이스(400)에 저장된 데이터의 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경은 없다고 판단된다.

단계 S76에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 중간 체크치의 계산을 시킨다. 앞서 설명한 도 25에 도시한 바와 같이 중간 체크치는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 총 체크치 생성 키 K_{icvt}를 키로 하고, 검증한 헤더(Header) 내의 체크치 A, 체크치 B, 보유해 둔 모든 콘텐츠 체크치를 메세지로 하여, 도 7 또는 그 밖의 도면에서 설명한 ICV 계산 방법에 따라 계산한다. 또, 초기치는 IV=0으로 해도, 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 총 체크치 생성용 초기치에 IVt를 보존해 두고, 그것을 사용해도 좋다. 또한, 생성된 중간 체크치는 필요에 따라 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 보유해 둔다.

다음으로, 단계 S77에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스(400)의 외부 메모리(402)로부터 판독한 데이터의 헤더부에 포함되는 취급 방침(Usage Policy)으로부터 이용 제한 정보를 추출하여, 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는지(이용 제한 정보가 1), 다른 동일한 기록 재생기(300)라도 이용할 수 있는지(이용 제한 정보가 0)를 판정한다. 판정 결과, 이용 제한 정보가 1, 즉 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는 이용 제한이 설정되어 있는 경우에는 단계 S80으로 진행하고, 이용 제한 정보가 0, 즉 다른 동일한 기록 재생기(300)라도 이용할 수 있는 설정인 경우에는 단계 S78로 진행한다. 또, 단계 S77의 처리는 암호 처리부(302)가 행해도 좋다.

단계 S78에 있어서는 「(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리」에서 설명한 단계 S58과 동일한 총 체크치 ICV_t의 계산이 실행된다. 즉, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 총 체크치 ICV_t의 계산을 시킨다. 앞서 설명한 도 25에 도시한 바와 같이 총 체크치 ICV_t는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 시스템 서명 키 K_{sys}를 키로 하고, 중간 체크치를 DES로 암호화하여 생성한다.

다음으로, 단계 S79로 진행하여, 단계 S78에서 생성한 총 체크치 ICV_t와 단계 S71에서 보존해 둔 헤더(Header) 내의 ICV_t를 비교하여, 일치한 경우에는 단계 S82로 진행한다.

앞서 설명한 바와 같이 총 체크치 ICV_t는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 전부의 변경을 검증하기 위한 체크치이다. 따라서, 상술한 처리에 의해 생성된 총 체크치가 헤더(Header) 내에 저장된 체크치:ICV_t와 일치한 경우에는 기록 디바이스(400)에 저장된 데이터에 있어서, ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 전부의 변경은 없다고 판단된다.

단계 S77에서의 판정에 있어서, 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는 설정인 경우, 즉 설정 정보가 1인 경우에는 단계 S80으로 진행한다.

단계 S80에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 기록 재생기 고유의 체크치 ICV_{dev}의 계산을 시킨다. 앞서 설명한 도 25에 도시한 바와 같이 기록 재생기 고유의 체크치 ICV_{dev}는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 기록 재생기 고유의 기록 재생기 서명 키 K_{dev}를 키로 하고, 중간 체크치를 DES로 암호화하여 생성한다. 단계 S81에 있어서, 단계 S80에서 계산한 기록 재생기 고유의 체크치 ICV_{dev}와 단계 S71에서 보존해 둔 Header 내의 ICV_{dev}를 비교하여, 일치한 경우에는 단계 S82로 진행한다.

이와 같이 시스템 서명 키 K_{sys}에 의해 서명된 데이터는 동일한 시스템 서명 키를 갖는 시스템(기록 재생기)에 의해 체크가 성공, 즉 총 체크치 ICV_t가 일치하므로 공통으로 이용 가능하게 되고, 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 경우에는 기록 재생기 서명 키는 그 기록 재생기에 고유의 키이기 때문에 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 데이터, 즉 서명 후, 기록 디바이스에 저장된 데이터는 다른 기록 재생기에 그 기록 디바이스를 장착하여 재생하고자 한 경우, 기록 재생기 고유의 체크치 ICV_{dev}가 불일치가 되어 에러가 되기 때문에, 재생할 수 없다. 따라서, 이용 제한 정보의 설정에 의해 시스템에 공통으로 사용할 수 있는 콘텐츠, 기록 재생기 고유하게 이용할 수 있는 콘텐츠를 자유하게 설정할 수 있다.

단계 S82에 있어서, 기록 재생기(300)의 제어부(301)는 단계 S74에서 판독해 둔 블록 정보 BIT 내의 콘텐츠 블록 정보를 추출하여, 콘텐츠 블록이 암호화 대상으로 되어 있는지의 여부를 조사한다. 암호화 대상으로 되어 있는 경우에는 해당하는 콘텐츠 블록을 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)의 외부 메모리(402)로부터 판독하여, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다. 이를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 콘텐츠를 복호화시킴과 함께 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 다음의 단계 S83에 있어서 콘텐츠 체크치를 검증시킨다.

단계 S83은 「(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리」에 서 설명한 단계 S58과 동일한 처리이다. 기록 재생기(300)의 제어부(301)는 블록 정보(BIT) 내의 콘텐츠 블록 정보를 추출하여, 콘텐츠 블록이 검증 대상으로 되어 있는지의 여부를 콘텐츠 체크치의 저장 상황으로부터 판정하여, 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 해당하는 콘텐츠 블록을 기록 디바이스(400)의 외부 메모리(402)로부터 수신하여, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다. 이를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 콘텐츠 중간치를 계산시킨다.

콘텐츠 중간치는 단계 S74에서 복호화한 콘텐츠 키 K_{con}로 입력된 콘텐츠 블록을 DES의 CBC 모드로 복호화하고, 그 결과를 8바이트로 구획하여 전부 배타적 논리합하여 생성한다.

다음으로, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 콘텐츠 체크치의 계산을 시킨다. 콘텐츠 체크치는 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 콘텐츠 체크치 생성 키 K_{icvc}를 키로 하고, 콘텐츠 중간치를 DES로 암호화하여 생성한다. 그리고, 기록 재생기 암호 처리부(302)의 제어부(306)는 해당 콘텐츠 체크치와, 단계 S71에서 기록 재생기(300)의 제어부(301)로부터 수신한 콘텐츠 블록 내의 ICV를 비교하여, 그 결과를 기록 재생기(300)의 제어부(301)에 건네 준다. 이를 수신한 기록 재생기(300)의 제어부(301)는 검증에 성공한 경우, 다음 검증 대상 콘텐츠 블록을 추출하여 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 검증시켜서, 모든 콘텐츠 블록을 검증할 때까지 동일한 검증 처리를 반복한다. 또, 초기치는 IV=0으로 해도, 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 콘텐츠 체크치 생성용 초기치 IVc를 보존해 두고, 그것을 사용해도 좋다. 또한, 체크한 모든 콘텐츠 체크치는 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 보유해 둔다. 또한, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 검증 대상의 콘텐츠 블록의 검증 순서를 감시하여, 순서가 틀렸거나, 동일한 콘텐츠 블록이 2회 이상 검증된 경우에는 인증에 실패한 것으로 한다.

기록 재생기(300)의 제어부(301)는 해당 콘텐츠 체크치의 비교 결과(검증 대상으로 되어 있지 않은 경우, 비교 결과는 전부 성공으로 함)를 수신하여, 검증에 성공한 경우에는 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 복호화된 콘텐츠를 추출한다. 그리고, 다음 복호화 대상 콘텐츠 블록을 추출하여 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 복호화시키고, 모든 콘텐츠 블록을 복호화할 때까지 반복한다.

또, 단계 S83에 있어서, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 콘텐츠 체크치의 검증 처리에 있어서 불일치가 된 경우에는 검증 실패로서 그 시점에서 처리를 중지하고, 남는 콘텐츠의 복호화는 행하지 않는다. 또한, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 복호화 대상의 콘텐츠 블록의 복호화 순서를 감시하여, 순서가 틀렸거나, 동일한 콘텐츠 블록이 2회 이상 복호화된 경우에는 복호화에 실패한 것으로 한다.

또, 단계 S72에서 체크치 A의 검증에 실패한 경우, 단계 S75에서 체크치 B의 검증에 실패한 경우, 단계 S79에서 총 체크치 ICV_t의 검증에 실패한 경우, 단계 S81에서 기록 재생기 고유의 체크치 ICV_{dev}의 검증에 실패한 경우, 단계 S83에서 각 콘텐츠 블록의 콘텐츠 체크치의 검증에 실패한 경우에는, 단계 S84로 진행하여 소정의 에러 표시를 행한다.

이상 설명한 바와 같이, 콘텐츠를 다운로드하거나, 이용하거나 할 때 중요한 데이터나 콘텐츠를 암호화해 두어 은폐화하거나, 변경 검증을 할 수 있을 뿐만 아니라, 블록 정보 BIT를 복호화하기 위한 블록 정보 키 K_{bit}, 콘텐츠를 복호화하기 위한 콘텐츠 키 K_{con}이 기록 디바이스 고유의 보존 키 K_{str}로 보존되어 있기 때문에, 단순하게 기록 미디어 상의 데이터를 다른 기록 미디어에 복제했다고 해도, 콘텐츠를 정확하게 복호화할 수 없게 할 수 있다. 보다 구체적으로는 예를 들면 도 28의 단계 S74에 있어서, 기록 디바이스마다 다른 보존 키 K_{str}로 암호화된 데이터를 복호화하기 위해서, 다른 기록 디바이스에서는 데이터를 정확하게 복호화할 수 없는 구성을 갖기 때문이다.

(9) 상호 인증 후의 키 교환 처리

본 발명의 데이터 처리 장치에서의 특징의 하나로, 상술한 기록 재생기(300)와 기록 디바이스(400) 사이에서 실행되는 상호 인증 처리의 후에 있어서만, 기록 디바이스의 이용을 가능하게 하고, 또한 그 이용 형태를 제한한 점이 있다.

예를 들면, 부정 복제 등에 의해 콘텐츠를 저장한 메모리 카드 등의 기록 디바이스를 생성하고, 이를 기록 재생기로 세트하여 이용되는 것을 배제하기 위해서, 기록 재생기(300)와, 기록 디바이스(400) 사이에서의 상호 인증 처리를 실행하고, 또한 인증 OK가 된 것을 조건으로 하여, 콘텐츠(암호화된)의 기록 재생기(300) 및 기록 디바이스(400) 사이에서의 전송을 가능하게 하고 있다.

상기한 제한적 처리를 실현하기 위해서, 본 발명의 데이터 처리 장치에서는 기록 디바이스(400)의 암호 처리부(401)에서의 처리는 전부, 사전에 설정된 커맨드 열에 기초하여 실행되는 구성으로 되어 있다. 즉, 기록 디바이스는 커맨드 번호에 기초한 커맨드를 순차 레지스터로부터 추출하여 실행하는 커맨드 처리 구성을 갖는다. 이 기록 디바이스에서의 커맨드 처리 구성을 도 29에 도시한다.

도 29에 도시한 바와 같이 기록 재생기 암호 처리부(302)를 갖는 기록 재생기(300)와 기록 디바이스 암호 처리부(401)를 갖는 기록 디바이스(400) 사이에서는 기록 재생기(300)의 제어부(301)의 제어 하에 기록 디바이스 컨트롤러(303)로부터 기록 디바이스(400)의 통신부(수신 레지스터를 포함함: 404)에 대하여 커맨드 번호 (No.)가 출력된다.

기록 디바이스(400)는 암호 처리부(401) 내의 제어부(403)에 커맨드 번호 관리부(2901)를 갖는다. 커맨드 번호 관리부(2901)는 커맨드 레지스터(2902)를 보유하고 있으며, 기록 재생기(300)로부터 출력되는 커맨드 번호에 대응하는 커맨드 열을 저장하고 있다. 커맨드 열은 도 29의 우측에 도시한 바와 같이 커맨드 번호 0부터 y까지 순차, 커맨드 번호에 대하여 실행 커맨드가 대응되어 있다. 커맨드 번호 관리부(2901)는 기록 재생기(300)로부터 출력되는 커맨드 번호를 감시하고, 대응하는 커맨드를 커맨드 레지스터(2902)로부터 추출하여 실행한다.

커맨드 레지스터(2902)에 저장된 커맨드 시퀀스는 도 29의 우측에 도시한 바와 같이 인증 처리 시퀀스에 관한 커맨드 열이 선행하는 커맨드 번호 0～k에 대응되어 있다. 또한, 인증 처리 시퀀스에 관한 커맨드 열의 후의 커맨드 번호 p～s에 복호, 키 교환, 암호 처리 커맨드 시퀀스 1, 또한 후속하는 커맨드 번호 u～y에 복호, 키 교환, 암호 처리 커맨드 시퀀스 2가 대응되어 있다.

앞서, 도 20의 인증 처리 플로우에 있어서 설명한 바와 같이 기록 디바이스 (400)가 기록 재생기(300)에 장착되면, 기록 재생기(300)의 제어부(301)는 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)에 초기화 명령을 송신한다. 이를 수신한 기록 디바이스(400)는 기록 디바이스 암호 처리부(401)의 제어부(403)에 있어서, 통신부(404)를 통해 명령을 수신하여, 인증 플래그(2903)를 클리어한다. 즉, 미 인증 상태로 설정한다. 또는 기록 재생기(300)로부터 기록 디바이스(400)에 전원이 공급된 경우에는 파워 온 시에 미 승인 상태로서 세트를 행하는 방식이라도 좋다.

다음으로, 기록 재생기(300)의 제어부(301)는 기록 재생기 암호 처리부(302)에 초기화 명령을 송신한다. 이 때, 기록 디바이스 삽입구 번호도 함께 송신한다. 기록 디바이스 삽입구 번호를 송신함으로써, 기록 재생기(300)에 복수의 기록 디바이스가 접속된 경우에서도 동시에 복수의 기록 디바이스(400)와의 인증 처리 및 데이터 송수신이 가능하게 된다.

초기화 명령을 수신한 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 재생기 암호 처리부(302)의 제어부에서 기록 디바이스 삽입구 번호에 대응하는 인증 플래그(2904)를 클리어한다. 즉, 미 인증 상태로 설정한다.

이들 초기화 처리가 완료하면, 기록 재생기(300)의 제어부(301)는 기록 디바이스 컨트롤러(303)를 통해 커맨드 번호 0부터 순차 커맨드 번호를 올림차순으로 출력한다. 기록 디바이스(400)의 커맨드 번호 관리부(2901)는 기록 재생기(300)로부터 입력되는 커맨드 번호를 감시하고, 0부터 순차 입력되는 것을 확인하여 대응하는 커맨드를 커맨드 레지스터(2902)로부터 추출하여 인증 처리 등, 각종 처리를 실행한다. 입력되는 커맨드 번호가 규정 순서가 아닌 경우에는 에러로 하여, 커맨드 번호 접수치를 초기 상태, 즉 실행 가능 커맨드 번호=0으로 리세트한다.

도 29에 도시한 바와 같이 커맨드 레지스터(2902)에 저장된 커맨드 시퀀스는 인증 처리를 선행하여 처리하도록 커맨드 번호가 부여되어 있으며, 그 후의 처리에 복호, 키 교환, 암호화 처리의 처리 시퀀스가 저장되어 있다.

복호, 키 교환, 암호화 처리의 처리 시퀀스의 구체예를 도 30, 31을 이용하여 설명한다.

도 30은 앞서 도 22에 있어서 설명한 기록 재생기(300)로부터 기록 디바이스 (400)로의 콘텐츠의 다운로드 처리에 있어서 실행되는 처리의 일부를 구성하는 것이다. 구체적으로는 도 22에 있어서의 단계 S59～S60 사이에서 실행된다.

도 30에 있어서, 단계 S3001은 기록 재생기로부터 세션 키 K_{ses}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 기록 디바이스가 수신하는 처리로서, 그 후, 상술한 도 29에 도시한 커맨드 열 p～s가 개시된다. 커맨드 열 p～s는 인증 처리 커맨드 0～k가 완료하고, 도 29에 도시한 인증 플래그(2903, 2904)에 인증 완료한 플래그가 세트된 후 개시된다. 이는 커맨드 번호 관리부(2901)가 커맨드 번호를 0부터 올림 차순으로만 접수함으로써 보증된다.

단계 S3002는 기록 디바이스가 기록 재생기로부터 수신한 세션 키 K_{ses}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 레지스터에 저장하는 처리이다.

단계 S3003은 세션 키 K_{ses}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 레지스터로부터 추출하여 세션 키 K_{ses}로 복호하는 처리를 실행하는 단계이다.

단계 S3004는 세션 키 K_{ses}로 복호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 보존 키 K_{str}로 암호화하는 처리를 실행하는 단계이다.

상기한 처리 단계 3002～3004는 앞의 도 29에서 설명한 커맨드 레지스터 중의 커맨드 번호 p～s에 포함되는 처리이다. 이들 처리는 기록 디바이스(400)의 커맨드 번호 관리부(2901)에 있어서 기록 재생기(300)로부터 수신하는 커맨드 번호 p～s에 따라 기록 디바이스 암호 처리부(401)가 순차 실행한다.

다음의 단계 S3005는 보존 키 K_{str}로 암호화한 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 기록 디바이스의 외부 메모리에 저장하는 단계이다. 이 단계에 있어서는 기록 디바이스 암호 처리부(401)로부터 기록 재생기(300)가 보존 키 K_{str}로 암호화한 데이터를 판독하고, 그 후에 기록 디바이스(400)의 외부 메모리(402)에 저장해도 좋다.

상술한 단계 S3002~S3004는 연속 실행되는 인터럽트 불가능한 실행 시퀀스로서, 예를 들면, 단계 S3003의 복호 처리 종료 시점에서, 기록 재생기(300)로부터의 데이터 판독 명령이 있었다고 해도, 그 판독 커맨드는 커맨드 레지스터(2902)의 커맨드 번호 p~s에 설정된 올림차순의 커맨드 번호와는 다르기 때문에, 커맨드 번호 관리부(2901)는 판독 실행을 접수하지 않는다. 따라서, 기록 디바이스(400)에 있어서의 키 교환 시에 발생하는 복호 데이터를 외부, 예를 들면 기록 재생기(300)로부터 판독하는 것은 불가능하게 되고, 키 데이터 콘텐츠의 부정 판독을 방지할 수 있다.

도 31은 먼저 도 28에 있어서 설명한 기록 디바이스(400)로부터 콘텐츠를 판독하여 기록 재생기(300)에 있어서 재생하는 콘텐츠 재생 처리에 있어서 실행되는 처리의 일부를 구성하는 것이다. 구체적으로는 도 28에 있어서의 단계 S73에 있어서 실행되는 처리이다.

도 31에 있어서, 단계 S3101은 기록 디바이스(400)의 외부 메모리(402)로부터 보존 키 K_{str}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})의 판독을 실행하는 단계이다.

단계 S3102는 기록 디바이스의 메모리로부터 판독한 보존 키 K_{str}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 레지스터에 저장하는 단계이다. 이 단계에 있어서는 기록 디바이스(400)의 외부 메모리(402)로부터 기록 재생기(300)가 보존 키 K_{str}로 암호화한 데이터를 판독하고, 그 후에 기록 디바이스(400)의 레지스터에 저장해도 좋다.

단계 S3103은 보존 키 K_{str}로 암호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 레지스터로부터 추출하여 보존 키 K_{str}로 복호 처리하는 단계이다.

단계 S3104는 보존 키 K_{str}로 복호화된 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 세션 키 K_{ses}로 암호화 처리하는 단계이다.

상기한 처리 단계 3102~3104는 앞의 도 29에서 설명한 커맨드 레지스터 중의 커맨드 번호 u~y에 포함되는 처리이다. 이들 처리는 기록 디바이스의 커맨드 번호 관리부(2901)에 있어서 기록 재생기(300)로부터 수신하는 커맨드 번호 u~y에 따라 기록 디바이스 암호 처리부(406)가 순차 실행한다.

다음의 단계 S3105는 세션 키 K_{ses}로 암호화한 데이터(ex. 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con})를 기록 디바이스로부터 기록 재생기로 송신하는 처리이다.

상술한 단계 S3102~S3104는 연속 실행되는 인터럽트 불가능한 실행 시퀀스로서, 예를 들면, 단계 S3103의 복호 처리 종료 시점에서, 기록 재생기(300)로부터의 데이터 판독 명령이 있었다고 해도, 그 판독 커맨드는 커맨드 레지스터(2902)의 커맨드 번호 u~y에 설정된 올림차순의 커맨드 번호와는 다르기 때문에, 커맨드 번호 관리부(2901)는 판독 실행을 접수하지 않는다. 따라서, 기록 디바이스(400)에 있어서의 키 교환 시에 발생하는 복호 데이터를 외부, 예를 들면 기록 재생기(300)로부터 판독하는 것은 불가능하게 되고, 키 데이터 또는 콘텐츠의 부정 판독을 방지할 수 있다.

또, 도 30, 31에 도시한 처리에서는 키 교환에 의해 복호, 암호화되는 대상이 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}인 예를 나타내었지만, 이들 도 29에 도시한 커맨드 레지스터(2902)에 저장된 커맨드 시퀀스에는 콘텐츠 자체의 키 교환을 수반하는 복호, 암호화 처리를 포함시켜도 좋고, 키 교환에 의해 복호, 암호화되는 대상은 상술한 예에 한정되는 것이 아니다.

이상, 본 발명의 데이터 처리 장치에서의 상호 인증 후의 키 교환 처리에 대하여 설명하였다. 이와 같이 본 발명의 데이터 처리 장치에서의 키 교환 처리는 기록 재생기와 기록 디바이스 사이에서의 인증 처리가 종료한 후에 있어서만 실행 가능하게 되고, 키 교환 처리에 있어서의 복호 데이터의 외부로부터의 액세스가 방지 가능한 구성으로 되어 있기 때문에 콘텐츠, 키 데이터의 고도의 시큐러티가 확보된다.

(10) 복수의 콘텐츠 데이터 포맷과, 각 포맷에 대응하는 다운로드 및 재생 처리

상술한 실시예에서는 예를 들면 도 3에 도시한 미디어(500) 또는 통신 수단 (600)에 있어서의 데이터 포맷이 도 4에 도시한 하나의 종류인 경우에 대하여 설명하였다. 그러나, 미디어(500) 또는 통신 수단(600)에 있어서의 데이터 포맷은 상술한

도 4에 도시한 포맷에 한하지 않고, 콘텐츠가 음악인 경우, 화상 데이터인 경우, 게임 등의 프로그램인 경우 등, 콘텐츠에 따른 데이터 포맷을 채택하는 것이 바람직하다. 이하, 복수의 다른 데이터 데이터 포맷과, 각 포맷에 대응한 기록 디바이스로의 다운로드 처리 및 기록 디바이스로부터의 재생 처리에 대하여 설명한다.

도 32～35에 4개의 다른 데이터 포맷을 나타낸다. 각 도의 좌측에는 도 3에 도시한 미디어(500) 또는 통신 수단(600) 상에 있어서의 데이터 포맷을 나타내고, 또한 각 도의 우측에는 기록 디바이스(400)의 외부 메모리(402)에 저장되는 경우의 데이터 포맷을 나타내고 있다. 먼저, 도 32～35에 도시한 데이터 포맷의 개략을 설명하고, 그 후, 각 포맷에 있어서의 각 데이터의 내용 및 각 포맷에 있어서의 데이터의 차이에 대하여 설명한다.

도 32는 포맷 타입 0으로서, 상술한 설명 중에서 예로서 나타낸 타입과 공통의 것이다. 포맷 타입 0의 특징은 데이터 전체를 임의의 크기의 N개의 데이터 블록, 즉 블록 1～블록 N으로 분할하고, 각 블록에 대하여 임의로 암호화하고, 암호화 블록과 비 암호화 블록, 즉 평문 블록을 혼재시켜서 데이터를 구성할 수 있다는 점이다. 블록의 암호화는 콘텐츠 키 K_{con}에 의해 실행되어 있으며, 콘텐츠 키 K_{con}은 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다. 블록 정보 키 K_{bit}에 대해서도 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다. 이들 키 교환은 상술한 「(9) 상호 인증 후의 키 교환 처리」에서 설명한 처리에 따라 실행된다.

도 33은 포맷 타입 1로서, 포맷 타입 1은 포맷 타입 0과 마찬가지로 데이터 전체를 N개의 데이터 블록, 즉 블록 1～블록 N으로 분할하고 있지만, N개의 각 블록의 크기를 동일한 크기로 한 점에서 상술한 포맷 타입 0과 다르다. 콘텐츠 키 K_{con}에 의한 블록의 암호화 처리 형태는 상술한 포맷 타입 0과 동일하다. 또한, 미디어 상에서 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화되는 콘텐츠 키 K_{con} 및 블록 정보 키 K_{bit} 구성도 상술한 포맷 타입 0과 동일하다. 포맷 타입 1은 포맷 타입 0과 달리, 고정적인 블록 구성으로 함으로써, 블록별 데이터 길이 등의 구성 데이터가 간략화되므로, 포맷 타입 0에 비하여 블록 정보의 메모리 사이즈를 줄일 수 있다.

도 33의 구성예에서는 각 블록을 암호화 파트와 비 암호화(평문) 파트의 1조에 의해 구성하고 있다. 이와 같이 블록의 길이, 구성이 규칙적이면, 복호 처리 등의 시에 각 블록 길이, 블록 구성을 확인할 필요가 없기 때문에 효율적인 복호, 암호 처리가 가능하게 된다. 또, 포맷 1에 있어서는 각 블록을 구성하는 파트, 즉 암호화 파트, 비 암호화(평문) 파트는 각 파트마다 체크 대상으로서 정의 가능한 구성으로 되어 있으며, 체크 필요 파트를 포함하는 블록인 경우에는 그 블록에 관하여 콘텐츠 체크치 ICV_i가 정의된다.

도 34는 포맷 타입 2로서, 포맷 타입 2의 특징은 동일한 크기의 N개의 데이터 블록, 즉 블록 1～블록 N으로 분할되고, 각 블록에 대하여 각각 개별 블록 키 K_{blc}으로 암호화되어 있는 것이다. 각 블록 키 K_{blc}의 암호화는 콘텐츠 키 K_{con}에 의해 실행되어 있으며, 콘텐츠 키 K_{con}은 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다. 블록 정보 키 K_{bit}에 대해서도 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다.

도 35는 포맷 타입 3으로서, 포맷 타입 3의 특징은 포맷 타입 2와 마찬가지로 동일한 크기의 N개의 데이터 블록, 즉 블록 1～블록 N으로 분할되고, 각 블록에 대하여, 각각 개별 블록 키 K_{blc}으로 암호화되어 있는 것, 또한 콘텐츠 키를 이용하지 않고 각 블록 키 K_{blc}의 암호화는 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스 상에서는 보존 키 K_{str}에 의해 암호화되어 있다는 점이다. 콘텐츠 키 K_{con}은 미디어 상, 디바이스 상, 어디에도 존재하지 않는다. 블록 정보 키 K_{bit}는 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다.

다음으로, 상기 포맷 타입 0～3의 데이터의 내용에 대하여 설명한다. 앞서 설명한 바와 같이 데이터는 크게 헤더부와 콘텐츠부로 분류되며, 헤더부에는 콘텐츠 식별자, 취급 방침, 체크치 A, B, 총 체크치, 블록 정보 키, 콘텐츠 키, 블록 정보가 포함된다.

취급 방침에는 콘텐츠의 데이터 길이, 헤더 길이, 포맷 타입(이하, 설명하는 포맷 0～3), 예를 들면 프로그램인지, 데이터인지 등의 콘텐츠 타입, 상술한 콘텐츠의 기록 디바이스로의 다운로드, 재생의 항목에서 설명한 바와 같이 콘텐츠가 기록 재생기 고유하게 이용 가능한지의 여부를 결정하는 플래그인 로컬리제이션 플래그, 또한 콘텐츠 복사, 이동 처리에 관한 허가 플래그, 또한 콘텐츠 암호화 알고리즘, 모드 등, 콘텐츠에 관한 각종 이용 제한 정보 및 처리 정보를 저장한다.

체크치 A:ICV_a는 식별 정보, 취급 방침에 대한 체크치로서, 예를 들면 상술한 도 23에서 설명한 방법에 의해 생성된다.

블록 정보 키 K_{bit}는 블록 정보를 암호화하기 위한 키로서, 앞서 설명한 바와 같이 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다.

콘텐츠 키 K_{con}은 콘텐츠의 암호화에 이용하는 키로서, 포맷 타입 0, 1에서는 블록 정보 키 K_{bit}와 마찬가지로 미디어 상에서는 배송 키 K_{dis}에 의해 암호화되고, 기록 디바이스에 있어서의 보존 시에는 기록 디바이스의 내부 메모리에 저장된 보존 키 K_{str}에 의해 암호화된다. 또, 포맷 타입 2에서는 콘텐츠 키 K_{con}은 콘텐츠 각 블록에 구성되는 블록 키 K_{blc}의 암호화에도 이용된다. 또한, 포맷 타입 3에 있어서는 콘텐츠 키 K_{con}은 존재하지 않는다.

블록 정보는 각각의 블록 정보를 기술하는 테이블로서, 블록의 크기, 암호화되어 있는지의 여부에 대한 플래그, 즉 각 블록이 체크 대상(ICV)으로 되어 있는지의 여부를 나타내는 정보가 저장된다. 블록이 체크 대상으로 되어 있는 경우에는 블록의 체크치 ICV_i(블록 i의 체크치)가 테이블 중에 정의되어 저장된다. 블록 정보는 블록 정보 암호 키 K_{bit}에 의해 암호화된다.

또, 블록의 체크치, 즉 콘텐츠 체크치 ICV_i는 블록이 암호화되어 있는 경우, 평문(복호문) 전체를 8바이트 단위로 배타 논리합한 값을 기록 재생기(300)의 내부 메모리(307)에 저장된 콘텐츠 체크치 생성 키 K_{icvc}로 암호화한 값으로서 생성된다. 또한, 블록이 암호화되어 있지 않은 경우에는 블록 데이터(평문)의 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다. 도 36에 콘텐츠 블록의 체크치 ICV_i를 생성하는 구성예를 나타낸다. 메세지 M의 각각이 복호문 데이터 또는 평문 데이터의 각 8바이트를 구성한다.

또, 포맷 타입 1에 있어서는 블록 내의 파트 중 적어도 하나가 체크치 ICV_i의 대상 데이터, 즉 체크 필요 파트인 경우에는 그 블록에 관하여 콘텐츠 체크치 ICV_i가 정의된다. 블록 i에서의 파트 j의 체크치 P-ICV_{ij}는 파트 j가 암호화되어 있는 경우, 평문(복호문) 전체를 8바이트 단위로 배타 논리합한 값을 콘텐츠 체크치 생성 키 K_{icvc}로 암호화한 값으로서 생성된다. 또한, 파트 j가 암호화되어 있지 않은 경우, 파트의 블록의 데이터(평문)의 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다.

또한, 하나의 블록 i 내에 체크 대상임을 나타내는 [ICV 플래그=subject of ICV]인 파트, 즉 체크 필요 파트가 하나만 존재하는 경우에는 상술한 방법에서 생성한 체크치 P-ICV_{ij}를 그대로 블록의 체크치 ICV_i로 하고, 또한 하나의 블록 i 내에 체크 대상임을 나타내는 [ICV 플래그=subject of ICV]인 파트가 복수 존재하는 경우에는 복수의 파트 체크치 P-ICV_{ij}를 파트 번호 순으로 연결한 데이터를 대상으로 하여 8바이트 단위로 도 37에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다. 도 37에 콘텐츠 블록의 콘텐츠 체크치 ICV_i를 생성하는 구성예를 나타낸다.

또, 포맷 타입 2, 3에 있어서는 블록의 체크치 ICV_i는 정의되지 않는다.

체크치 B:ICV_b는 블록 정보 키, 콘텐츠 키, 블록 정보 전체에 대한 체크치로서, 예를 들면, 상술한 도 24에서 설명한 방법에 의해 생성된다.

총 체크치 ICV_t는 상술한 체크치 A:ICV_a, 체크치 B:ICV_b, 또한 콘텐츠의 체크 대상으로 되어 있는 각 블록에 포함되는 체크치 ICV_i 전체에 대한 체크치로서, 상술한 도 25에서 설명한 바와 같이 체크치 A:ICV_a 등의 각 체크치로부터 생성되는 중간 체크치에 시스템 서명 키 K_{sys}를 적용하여 암호화 처리를 실행함으로써 생성된다.

또, 포맷 타입 2, 3에 있어서는 총 체크치 ICV_t는 상술한 체크치 A:ICV_a, 체크치 B:ICV_b에 콘텐츠 데이터, 즉 블록 1의 블록 키로부터 최종 블록까지의 콘텐츠 데이터 전체를 연결한 데이터로부터 생성되는 중간 체크치에 시스템 서명 키 K_{sys}를 적용하여 암호화 처리를 실행함으로써 생성된다. 도 38에 포맷 타입 2, 3에 있어서의 총 체크치 ICV_t를 생성하는 구성예를 나타낸다.

고유 체크치 ICV_{dev}는 상술한 로컬리제이션 플래그가 1로 세트되어 있는 경우, 즉, 콘텐츠가 기록 재생기 고유하게 이용 가능한 것을 나타내고 있는 경우에 총 체크치 ICV_t로 치환되는 체크치로서, 포맷 타입 0, 1인 경우에는 상술한 체크치 A:ICV_a, 체크치 B:ICV_b, 또한 콘텐츠의 체크 대상으로 되어 있는 각 블록에 포함되는 체크치 ICV_i 전체에 대한 체크치로서 생성된다. 구체적으로는 상술한 도 25 또는 도 38에서 설명한 바와 같이 체크치 A:ICV_a 등의 각 체크치로부터 생성되는 중간 체크치에 기록 재생기 서명 키 K_{dev}를 적용하여 암호화 처리를 실행함으로써 생성된다.

다음으로, 포맷 타입 0～3 각각에 있어서의 기록 재생기(300)로부터 기록 디바이스(400)에 대한 콘텐츠의 다운로드 처리 및 기록 재생기(300)에 있어서의 기록 디바이스(400)로부터의 재생 처리에 대하여 도 39～44의 플로우를 이용하여 설명한다.

우선, 포맷 타입 0, 1에 있어서의 콘텐츠의 다운로드 처리에 대하여 도 39를 이용하여 설명한다.

도 39에 도시한 처리는 예를 들면 도 3에 도시한 기록 재생기(300)에 기록 디바이스(400)를 장착함으로써 개시된다. 단계 S101은 기록 재생기와 기록 디바이스 사이에서의 인증 처리 단계로서, 앞서 설명한 도 20의 인증 처리 플로우에 따라 실행된다.

단계 S101의 인증 처리가 종료하여 인증 플래그가 세트되면, 기록 재생기 (300)는 단계 S102에 있어서, 예를 들면 콘텐츠 데이터를 저장한 미디어(500)로부터 판독부(304)를 통해 소정의 포맷에 따른 데이터를 판독하거나, 통신부(305)를 사용하여 통신 수단(600)으로부터 소정의 포맷에 따라 데이터를 수신하여, 기록 재생기(300)의 제어부(301)가 데이터 내의 헤더(Header) 부분을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다.

다음으로, 단계 S103에 있어서, 암호 처리부(302)의 제어부(306)가 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 체크치 A를 계산시킨다. 체크치 A는 도 23에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보(Content ID)와 취급 방침(Usage Policy)을 메세지로 하여, 도 7을 이용하여 설명한 ICV 계산 방법에 따라 계산된다. 다음으로, 단계 S104에 있어서, 체크치 A와 헤더(Header) 내에 저장된 체크치:ICV_a를 비교하여, 일치한 경우에는 단계 S105로 진행한다.

앞서 설명한 바와 같이 체크치 A, ICV_a는 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보(Content ID)와 취급 방침(Usage Policy)을 메세지로 하여, 예를 들면 ICV 계산 방법에 따라 계산되는 체크치 A가 헤더(Header) 내에 저장된 체크치:ICV_a와 일치한 경우에는 식별 정보, 취급 방침의 변경은 없다고 판단된다.

다음으로, 단계 S105에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 배송 키 K_{dis}의 추출 또는 생성을 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 행하게 한다. 배송 키 K_{dis}의 생성 방법은 먼저 설명한 도 22의 단계 S53과 마찬가지로 예를 들면 배송 키용 마스터 키 MK_{dis}를 이용하여 행해진다.

다음으로, 단계 S106에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)가 기록 재생기 암호 처리부(302)의 암호/복호화부(308)를 사용하여 생성한 배송 키 K_{dis}를 이용하고, 판독부(304)를 통해 수신한 미디어(500) 또는 통신부 (305)를 통해 통신 수단(600)으로부터 수신한 데이터의 헤더부에 저장된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}의 복호화 처리를 행한다.

또한, 단계 S107에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 있어서, 복호화한 블록 정보 키 K_{bit}로 블록 정보를 복호화한다.

또한, 단계 S108에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)로부터 체크치 B($ICV_{b'}$)를 생성한다. 체크치 B는 도 24에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하여, 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)로 이루어진 배타적 논리합 값을 DES로 암호화하여 생성한다. 다음으로, 단계 S109에 있어서, 체크치 B와 헤더(Header) 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S110으로 진행한다.

앞서 설명한 바와 같이 체크치 B, ICV_b는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} , 블록 정보의 변경을 검증하기 위한 체크치이다. 기록 재생기 암호 처리부 (302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)를 8바이트 단위로 분할하여 배타적 논리합하여 얻어지는 값을 DES로 암호화하여 생성한 체크치 B가 헤더 (Header) 내에 저장된 체크치:ICV_b와 일치한 경우에는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경은 없다고 판단된다.

단계 S110에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 중간 체크치의 계산을 시킨다. 중간 체크치는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 총 체크치 생성 키 K_{icvt}를 키로 하고, 검증한 Header 내의 체크치 A, 체크치 B, 보유해 둔 모든 콘텐츠 체크치를 메세지로 하여, 도 7 또는 그 밖의 도면에서 설명한 ICV 계산 방법에 따라 계산한다. 또, 생성된 중간 체크치는 필요에 따라 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 보유해 둔다.

다음으로, 단계 S111에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 총 체크치 $ICV_{t'}$의 계산을 시킨다. 총 체크치 $ICV_{t'}$는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 시스템 서명 키 K_{sys}를 키로 하고, 중간 체크치를 DES로 암호화하여 생성한다. 다음으로, 단계 S112에 있어서, 생성된 총 체크치 $ICV_{t'}$와 헤더(Header) 내의 ICV_t를 비교하여, 일치한 경우에는 단계 S113으로 진행한다.

앞서 도 4에 있어서 설명한 바와 같이 총 체크치 ICV_t는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 모든 변경을 검증하기 위한 체크치이다. 따라서, 상술한 처리에 의해 생성된 총 체크치가 헤더(Header) 내에 저장된 체크치:ICV_t와 일치한 경우에는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 모든 변경은 없다고 판단된다.

다음으로, 단계 S113에 있어서, 기록 재생기(300)의 제어부(301)는 블록 정보(BIT) 내의 콘텐츠 블록 정보를 추출하고, 콘텐츠 블록이 검증 대상으로 되어 있는지의 여부를 조사한다. 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 헤더 중의 블록 정보 중에 콘텐츠 체크치가 저장되어 있다.

콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 단계 S114에 있어서, 해당하는 콘텐츠 블록을 기록 재생기(300)의 판독부(304)를 사용하여 미디어(500)로부터 판독하거나, 기록 재생기(300)의 통신부(305)를 사용하여 통신 수단(600)으로부터 수신하여, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다. 이를 수신한 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 콘텐츠 체크치 $ICV_{i'}$를 계산시킨다.

콘텐츠 체크치 $ICV_{i'}$는 앞서 설명한 바와 같이 블록이 암호화되어 있는 경우, 콘텐츠 키 K_{con}로 입력된 콘텐츠 블록을 DES의 CBC 모드로 복호화하고, 그 결과를 전부 8바이트 단위로 배타적 논리합하여 생성한 콘텐츠 중간치를 기록 재생기

(300)의 내부 메모리(307)에 저장된 콘텐츠 체크치 생성 키 K_{icvc}로 암호화하여 생성한다. 또한, 블록이 암호화되어 있지 않은 경우에는 데이터(평문) 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다.

다음으로, 단계 S115에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 해당 콘텐츠 체크치와, 단계 S102에서 기록 재생기(300)의 제어부(301)로부터 수신한 콘텐츠 블록 내의 ICV를 비교하여, 그 결과를 기록 재생기(300)의 제어부(301)에 건네 준다. 이를 수신한 기록 재생기(300)의 제어부(301)는 검증에 성공한 경우, 다음 검증 대상 콘텐츠 블록을 추출하여 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 검증시키고, 모든 콘텐츠 블록을 검증할 때까지 동일한 검증 처리를 반복한다(단계 S116).

또, 단계 S104, 단계 S109, 단계 S112, 단계 S115 중 어느 하나에 있어서, 체크치의 일치가 얻어지지 않은 경우에는 에러로서 다운로드 처리는 종료한다.

다음으로, 단계 S117에 있어서, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 단계 S106에서 복호화한 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화시킨다. 기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기(300)의 기록 재생기 암호 처리부 (302)로부터 판독하여, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러 (303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S118에 있어서, 기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 디바이스(400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화시키고, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시키고, 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로부터 보존 키 K_{str}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con} 을 판독한다. 즉, 배송 키 K_{dis}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con} 의 키의 재기입을 행한다.

다음으로, 단계 S119에 있어서, 기록 재생기(300)의 제어부(301)는 데이터의 헤더부의 취급 방침(Usage Po1icy)으로부터 이용 제한 정보를 추출하고, 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는지의 여부를 판정한다. 이 판정은 로컬리제이션 플래그(이용 제한 정보)=1로 설정되어 있는 경우에는 다운로드한 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있고, 로컬리제이션(이용 제한 정보)=0으로 설정되어 있는 경우에는 다운로드한 콘텐츠가 다른 동일한 기록 재생기(300)라도 이용할 수 있는 것을 나타낸다. 판정의 결과, 로컬리제이션 (이용 제한 정보)=1인 경우에는 단계 S120으로 진행한다.

단계 S120에 있어서, 기록 재생기(300)의 제어부(301)는 기록 재생기 고유의 체크치를 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 계산시킨다. 기록 재생기 고유의 체크치는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 기록 재생기에 고유의 기록 재생기 서명 키 K_{dev}를 키로 하고, 단계 S110에서 생성된 중간 체크치를 DES로 암호화하여 생성한다. 계산된 기록 재생기 고유의 체크치 ICV_{dev}는 총 체크치 ICV_t 대신에 덧씌우기된다.

앞서 설명한 바와 같이, 시스템 서명 키 K_{sys}는 신호 분배 시스템에 공통의 서명 또는 ICV를 붙이기 위해서 사용하는 시스템 서명 키이고, 또한 기록 재생기 서명 키 K_{dev}는 기록 재생기마다 다르고, 기록 재생기가 서명 또는 ICV를 붙이기 위해서 사용하는 기록 재생기 서명 키이다. 즉, 시스템 서명 키 K_{sys}에 의해 서명된 데이터는 동일한 시스템 서명 키를 갖는 시스템(기록 재생기)에 의해 체크가 성공, 즉 총 체크치 ICV_t가 일치하게 되므로 공통으로 이용 가능하게 되지만, 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 경우에는 기록 재생기 서명 키는 그 기록 재생기 고유의 키이므로, 기록 재생기 서명 키 K_{dev}를 이용하여 서명된 데이터, 즉 서명 후, 기록 디바이스에 저장된 데이터는 다른 기록 재생기에 그 기록 디바이스를 장치하여 재생하고자 한 경우, 기록 재생기 고유의 체크치 ICV_{dev}가 불일치가 되어 에러가 되기 때문에, 재생할 수 없게 된다. 본 발명의 데이터 처리 장치에서는 이용 제한 정보의 설정에 의해 시스템에 공통으로 사용할 수 있는 콘텐츠, 기록 재생기 고유하게 이용할 수 있는 콘텐츠를 가능하게 설정할 수 있는 것이다.

다음으로, 단계 S121에 있어서, 기록 재생기(300)의 제어부(301)는 기록 재생기 암호 처리부(302)에 저장 데이터 포맷의 형성을 실행시킨다. 앞서 설명한 바와 같이, 포맷 타입은 0~3까지 각 타입이 있으며, 헤더 중의 취급 방침(도 5 참조) 중에 설정되고, 설정 타입에 따라 앞서 설명한 도 32~35의 우측의 저장 포맷에 따라 데이터를 형성한다. 도 39에 도시한 플로우는 포맷 0, 1 중 어느 하나이므로, 도 32, 33 중 어느 하나의 포맷으로 형성된다.

단계 S121에 있어서 저장 데이터 포맷의 형성이 종료하면, 단계 122에 있어서, 기록 재생기(300)의 제어부(301)는 콘텐츠를 기록 디바이스(400)의 외부 메모리(402)에 보존한다.

이상이 포맷 타입 0, 1에 있어서의 콘텐츠 데이터의 다운로드 처리의 형태이다.

다음으로, 포맷 타입 2에 있어서의 콘텐츠 데이터의 다운로드 처리에 대하여 도 40을 이용하여 설명한다. 상기한 포맷 타입 0, 1의 다운로드 처리와 다른 점을 중심으로 설명한다.

단계 S101~S109는 상기한 포맷 타입 0, 1의 다운로드 처리와 동일하므로 설명은 생략한다.

포맷 타입 2는 앞서 설명한 바와 같이 콘텐츠 체크치 ICV_i가 정의되어 있지 않기 때문에 블록 정보 중에는 콘텐츠 체크치 ICV_i를 갖지 않는다. 포맷 타입 2에 있어서의 중간 체크치는 도 38에 도시한 바와 같이 체크치 A, 체크치 B와, 제1 블록의 선두 데이터(블록1의 블록 키)로부터 최종 블록까지의 콘텐츠 데이터 전체를 연결한 데이터에 기초하여 생성되는 중간 체크치에 시스템 서명 키 K_{sys}를 적용하여 암호화 처리를 실행함으로써 생성된다.

따라서, 포맷 타입 2의 다운로드 처리에 있어서는 단계 S151에 있어서 콘텐츠 데이터를 판독하고, 단계 S152에 있어서, 체크치 A, 체크치 B와 판독한 콘텐츠 데이터에 기초하여 중간 체크치의 생성을 실행한다. 또, 콘텐츠 데이터는 암호화되어 있는 경우라도, 복호 처리를 행하지 않는다.

포맷 타입 2에서는 상술한 포맷 타입 0, 1에서의 처리와 같이 블록 데이터의 복호, 콘텐츠 체크치의 조회 처리를 행하지 않기 때문에 신속한 처리가 가능하게 된다.

단계 S111 이하의 처리는 포맷 타입 O, 1에 있어서의 처리와 동일하므로 설명을 생략한다.

이상이 포맷 타입 2에 있어서의 콘텐츠 데이터의 다운로드 처리의 형태이다. 상술한 바와 같이 포맷 타입 2의 다운로드 처리는 포맷 타입 0, 1에서의 처리와 같이 블록 데이터의 복호, 콘텐츠 체크치의 조회 처리를 행하지 않기 때문에 신속한 처리가 가능하게 되고, 음악 데이터 등 실시간 처리가 요구되는 데이터 처리에 적합한 포맷이다.

다음으로, 포맷 타입 3에 있어서의 콘텐츠 데이터의 다운로드 처리에 대하여 도 41을 이용하여 설명한다. 상기한 포맷 타입 0, 1, 2의 다운로드 처리와 다른 점을 중심으로 설명한다.

단계 S101~S105는 상기한 포맷 타입 0, 1, 2의 다운로드 처리와 동일하므로 설명은 생략한다.

포맷 타입 3은 기본적으로 포맷 타입 2에서의 처리와 공통되는 부분이 많지만, 포맷 타입 3은 콘텐츠 키를 갖고 있지 않으며, 또한 블록 키 K_{blc}이 기록 디바이스에 있어서는 보존 키 K_{str}로 암호화되어 저장되는 점이 포맷 타입 2와 다르다.

포맷 타입 3의 다운로드 처리에 있어서의 포맷 타입 2와 서로 다른 점을 중심으로 하여 설명한다. 포맷 타입 3에서는 단계 S105의 다음 단계인 단계 S161에 있어서, 블록 정보 키의 복호를 행한다. 기록 재생기 암호 처리부(302)의 제어부 (306)가 기록 재생기 암호 처리부(302)의 암호/복호화부(308)를 사용하여, 단계 S105에서 생성된 배송 키 K_{dis}를 이용하여 판독부(304)를 통해 수신한 미디어(500) 또는 통신부(305)를 통해 통신 수단(600)으로부터 수신한 데이터의 헤더부에 저장된 블록 정보 키 K_{bit}의 복호화 처리를 행한다. 포맷 타입 3에서는 데이터 중에 콘텐츠 키 K_{con}이 존재하지 않기 때문에, 콘텐츠 키 K_{con}의 복호화 처리는 실행되지 않는다.

다음의 단계 S107에서는 단계 S161에서 복호한 블록 정보 키 K_{bit}를 이용하여 블록 정보의 복호가 실행되고, 또한 단계 S162에 있어서, 기록 재생기 암호 처리부 (302)의 제어부(306)는 블록 정보 키 K_{bit} 및 블록 정보(BIT)로부터 체크치 B

($ICV_{b'}$)를 생성한다. 체크치 B는 기록 재생기 암호 처리부(302)의 내부 메모리 (307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 블록 정보 키 K_{bit} 및 블록 정보(BIT)로 이루어진 배타적 논리합 값을 DES로 암호화하여 생성한다. 다음으로, 단계 S109에 있어서, 체크치 B와 헤더(Header) 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S151로 진행한다.

포맷 타입 3에서는 체크치 B, ICV_b는 블록 정보 키 K_{bit}, 블록 정보의 변경을 검증하기 위한 체크치로서 기능한다. 생성된 체크치 B가 헤더(Header) 내에 저장된 체크치:ICV_b와 일치한 경우에는 블록 정보 키 K_{bit}, 블록 정보의 변경은 없다고 판단된다.

단계 S151～S112는 포맷 타입 2의 처리와 동일하므로 설명을 생략한다.

단계 S163에서는 단계 S151에서 판독한 콘텐츠 데이터에 포함되는 블록 키 K_{blc}를 단계 S105에서 생성된 배송 키 K_{dis}에 의해 복호한다.

다음으로, 단계 S164에서는 기록 재생기(300)의 기록 재생기 암호 처리부 (302)가 단계 S161에서 복호화한 블록 정보 키 K_{bit}와, 단계 S163에서 복호한 블록 키 K_{blc}을 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화시킨다. 기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}와 블록 키 K_{blc}을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독하고, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S165에 있어서, 기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}와 블록 키 K_{blc}을 수신한 기록 디바이스(400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화시키고, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시키고, 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통하고, 기록 디바이스(400)로부터 보존 키 K_{str}로 재 암호화된 블록 정보 키 K_{bit}와 블록 키 K_{blc} 을 판독한다. 즉, 당초, 배송 키 K_{dis}로 암호화된 블록 정보 키 K_{bit}와 블록 키 K_{blc} 을 보존 키 K_{str}로 재 암호화된 블록 정보 키 K_{bit}와 블록 키 K_{blc}으로 치환을 행한다.

이하의 단계 S119～S122는 상술한 포맷 타입 0, 1, 2와 동일하므로 설명을 생략한다.

이상이 포맷 타입 3에 있어서의 콘텐츠 데이터의 다운로드 처리의 형태이다. 상술한 바와 같이 포맷 타입 3의 다운로드 처리는 포맷 타입 2와 마찬가지로 블록 데이터의 복호, 콘텐츠 체크치의 조회 처리를 행하지 않기 때문에 신속한 처리가 가능하게 되고, 음악 데이터 등 실시간 처리가 요구되는 데이터 처리에 적합한 포맷이다. 또한, 블록 키 K_{blc}에 의해 암호화 콘텐츠를 보호하는 범위가 국소화되어 있기 때문에 포맷 타입 2에 비하여, 보다 시큐러티가 고도하게 된다.

다음으로, 포맷 타입 0～3 각각에 있어서의 기록 재생기(300)에 있어서의 기록 디바이스(400)로부터의 재생 처리에 대하여 도 42～45의 플로우를 이용하여 설명한다.

우선, 포맷 타입 0에 있어서의 콘텐츠의 재생 처리에 대하여 도 42를 이용하여 설명한다.

단계 S201은 기록 재생기와 기록 디바이스 사이에서의 인증 처리 단계로서, 앞서 설명한 도 20의 인증 처리 플로우에 따라 실행된다.

단계 S201의 인증 처리가 종료하여 인증 플래그가 세트되면, 기록 재생기 (300)는 단계 S202에 있어서, 기록 디바이스(400)로부터 소정의 포맷에 따른 데이터의 헤더를 판독하여, 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신한다.

다음으로, 단계 S203에 있어서, 암호 처리부(302)의 제어부(306)가 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 체크치 A를 계산시킨다. 체크치 A는 먼저 설명한 도 23에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모

리(307)에 보존되어 있는 체크치 A 생성 키 K_{icva}를 키로 하고, 식별 정보 (Content ID)와 취급 방침(Usage Policy)을 메세지로 하여 계산된다. 다음으로, 단계 S204에 있어서, 계산된 체크치 A와 헤더(Header) 내에 저장된 체크치:ICV_a를 비교하여, 일치한 경우에는 단계 S205로 진행한다.

체크치 A, ICV_a는 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치이다. 계산된 체크치 A가 헤더(Header) 내에 저장된 체크치: ICV_a와 일치한 경우에는 기록 디바이스(400)에 저장된 식별 정보, 취급 방침의 변경은 없다고 판단된다.

다음으로, 단계 S205에 있어서, 기록 재생기(300)의 제어부(301)는 판독한 헤더로부터 기록 디바이스 고유의 보존 키 K_{str}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 추출하여, 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 디바이스(400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 복호화 처리시키고, 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 재 암호화시킨다. 이 처리는 상술한 「(9) 상호 인증 후의 키 교환 처리」에서 상세하게 진술한 바와 같다.

단계 S206에서는 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로부터 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한다.

다음으로, 단계 S207에 있어서, 기록 재생기(300)의 제어부(301)는 수신한 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신하고, 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 수신한 기록 재생기(300)의 기록 재생기 암호 처리부 (302)는 기록 재생기 암호 처리부 (302)의 암호/복호화부(308)에 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}와 콘텐츠 키 K_{con}을 상호 인증 시에 공유해 둔 세션 키 K_{ses} 로 복호화시킨다.

또한, 단계 S208에 있어서, 복호화된 블록 정보 키 K_{bit}로 단계 S202에서 판독해 둔 블록 정보를 복호화한다. 또, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 복호화한 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보 BIT를 단계 S202에서 판독한 헤더에 포함되는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보 BIT로 치환하여 보유해 둔다. 또한, 기록 재생기(300)의 제어부(301)는 복호화된 블록 정보 BIT를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독해 둔다.

또한, 단계 S209에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)로부터 체크치 B($ICV_{b'}$)를 생성한다. 체크치 B는 도 24에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con} 및 블록 정보(BIT)로 이루어진 배타적 논리합 값을 DES로 암호화하여 생성한다. 다음으로, 단계 S210에 있어서, 체크치 B와 헤더(Header) 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S211로 진행한다.

체크치 B, ICV_b는 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경을 검증하기 위한 체크치로서, 생성된 체크치 B가 헤더(Header) 내에 저장된 체크치:ICV_b와 일치한 경우에는 기록 디바이스(400)에 보존된 데이터 중의 블록 정보 키 K_{bit} 콘텐츠 키 K_{con}, 블록 정보의 변경은 없다고 판단된다.

단계 S211에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 중간 체크치의 계산을 시킨다. 중간 체크치는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 총 체크치 생성 키 K_{icvt}를 키로 하고, 검증한 Header 내의 체크치 A, 체크치 B, 블록 정보 중의 모든 콘텐츠 체크치를 메세지로 하여, 도 7 또는 그 밖의 도면에서 설명한 ICV 계산 방법에 따라 계산한다. 또, 생성된 중간 체크치는 필요에 따라 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 보유해 둔다.

다음으로, 단계 S212에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스(400)의 외부 메모리(402)로부터 판독한 데이터의 헤더부에 포함되는 취급 방침(Usage Policy)으로부터 이용 제한 정보를 추출하여, 재생 예정인 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는지(이용 제한 정보가 1), 다른 동일한 기록 재생기(300)라도 이용할 수 있는지(이용 제한 정보가 0)를 판정한다. 판정 결과, 이용 제한 정보가 1, 즉 재생 콘텐츠가 해당 기록 재생기(300)만으로 이용할 수 있는 이용 제한이 설정되어 있는 경우에는 단계 S213으로 진행하고, 이용 제한 정보가 0, 즉 다른 동일한 기록 재생기(300)라도 이용할 수 있는 설정인 경우에는 단계 S215로 진행한다. 또, 단계 S212의 처리는 암호 처리부(302)가 행해도 좋다.

단계 S213에서는 기록 재생기(300)의 제어부(301)는 기록 재생기 고유의 체크치 $ICV_{dev'}$를 기록 재생기(300)의 기록 재생기 암호 처리부(302)에 계산시킨다. 기록 재생기 고유의 체크치 $ICV_{dev'}$는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 기록 재생기 서명 키 K_{dev}를 키로 하고, 단계 S211에서 보유해 둔 중간 체크치를 DES로 암호화하여 생성한다.

다음으로, 단계 S214에 있어서, 단계 S213에서 계산한 기록 재생기 고유의 체크치 $ICV_{dev'}$와 단계 S202에서 판독한 헤더 내의 ICV_{dev}를 비교하여, 일치한 경우에는 단계 S217로 진행한다.

한편, 단계 S215에서는 기록 재생기 암호 처리부(302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 총 체크치 ICV_t의 계산을 시킨다. 총 체크치 $ICV_{t'}$는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 시스템 서명 키 K_{sys}를 키로 하고, 중간 체크치를 DES로 암호화하여 생성한다. 다음으로, 단계 S216에 있어서, 생성한 총 체크치 $ICV_{t'}$와 헤더(Header) 내의 ICV_t를 비교하여, 일치한 경우에는 단계 S217로 진행한다.

총 체크치 ICV_t 및 기록 재생기 고유의 체크치 ICV_{dev}는 ICV_a, ICV_b , 각 콘텐츠 블록의 체크치 전부의 변경을 검증하기 위한 체크치이다. 따라서, 상술한 처리에 의해 생성된 체크치가 헤더(Header) 내에 저장된 체크치:ICV_t 또는 ICV_{dev}와 일치한 경우에는 기록 디바이스(400)에 저장된 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 전부의 변경은 없다고 판단된다.

다음으로, 단계 S217에 있어서, 기록 재생기(300)의 제어부(301)는 기록 디바이스(400)로부터 블록 데이터를 판독한다. 또한, 단계 S218에 있어서 암호화되어 있는지의 여부를 판정하여, 암호화되어 있는 경우에는 기록 재생기(300)의 암호 처리부(302)에 있어서 블록 데이터의 복호를 행한다. 암호화되어 있지 않은 경우에는 단계 S219를 스킵하여 단계 S220으로 진행한다.

다음으로, 단계 S220에 있어서, 기록 재생기(300)의 제어부(301)는 블록 정보(BIT) 내의 콘텐츠 블록 정보에 기초하여 콘텐츠 블록이 검증 대상으로 되어 있는지의 여부를 조사한다. 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 헤더 중의 블록 정보 중에 콘텐츠 체크치가 저장되어 있다. 콘텐츠 블록이 검증 대상으로 되어 있는 경우에는 단계 S221에 있어서, 해당하는 콘텐츠 블록의 콘텐츠 체크치 $ICV_{i'}$를 계산시킨다. 콘텐츠 블록이 검증 대상으로 되어 있지 않은 경우에는 단계 S221과 S222를 스킵하여 단계 S223으로 진행한다.

콘텐츠 체크치 $ICV_{i'}$는 먼저 도 36에서 설명한 바와 같이 블록이 암호화되어 있는 경우, 콘텐츠 키 K_{con}로 입력된 콘텐츠 블록을 DES의 CBC 모드로 복호화하고, 그 결과를 전부 8바이트 단위로 배타적 논리합하여 생성한 콘텐츠 중간치를 기록 재생기(300)의 내부 메모리(307)에 저장된 콘텐츠 체크치 생성 키 K_{icvc}로 암호화하여 생성한다. 또한, 블록이 암호화되어 있지 않은 경우에는 데이터(평문) 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다.

단계 S222에 있어서는 기록 재생기 암호 처리부(302)의 제어부(306)는 생성된 콘텐츠 체크치 $ICV_{i'}$와, 단계 S202에서 기록 디바이스(400)로부터 수신한 헤더부에 저장된 콘텐츠 체크치 ICV_i를 비교하여, 그 결과를 기록 재생기(300)의 제어부(301)에 건네 준다. 이를 수신한 기록 재생기(300)의 제어부(301)는 검증에 성공하고 있는 경우, 단계 S223에 있어서, 기

록 재생기 시스템 RAM 상에 실행(재생)용 콘텐츠 평문 데이터를 저장한다. 기록 재생기(300)의 제어부(301)는 또한 다음의 검증 대상 콘텐츠 블록을 추출하여 기록 재생기(300)의 기록 재생기 암호 처리부 (302)에 검증시키고, 모든 콘텐츠 블록을 검증할 때까지 동일한 검증 처리, RAM 저장 처리를 반복한다(단계 S224).

또, 단계 S204, 단계 S210, 단계 S214, 단계 S216, 단계 S222 중 어느 하나에 있어서, 체크치의 일치가 얻어지지 않은 경우에는 에러로서 재생 처리는 종료한다.

단계 S224에 있어서 모든 블록 판독으로 판정되면, 단계 S225로 진행하여 콘텐츠(프로그램, 데이터)의 실행, 재생이 개시된다.

이상이 포맷 타입 0에 있어서의 콘텐츠 데이터의 재생 처리의 형태이다.

다음으로, 포맷 타입 1에 있어서의 콘텐츠 데이터의 재생 처리에 대하여 도 43을 이용하여 설명한다. 상기한 포맷 타입 0의 재생 처리와 다른 점을 중심으로 설명한다.

단계 S201～단계 S217까지의 처리는 상기한 포맷 타입 0의 재생 처리와 동일하므로 설명은 생략한다.

포맷 타입 1에서는 단계 S231에 있어서, 암호화 파트의 복호가 실행되어, 파트 ICV가 생성된다. 또한, 단계 S232에 있어서, 블록 $ICV_{i'}$이 생성된다. 앞서 설명한 바와 같이 포맷 타입 1에 있어서는 블록 내의 파트 중 적어도 하나가 체크치 ICV_i의 대상 데이터인 경우에는 그 블록에 관하여 콘텐츠 체크치 ICV_i가 정의된다. 블록 i에서의 파트 j의 체크치 $P\text{-}ICV_{ij}$는 파트 j가 암호화되어 있는 경우, 평문(복호문) 전체를 8바이트 단위로 배타 논리합한 값을 콘텐츠 체크치 생성 키 K_{icvc}로 암호화한 값으로서 생성된다. 또한, 파트 j가 암호화되어 있지 않은 경우에는 데이터(평문) 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다.

또한, 하나의 블록 i 내에 체크 대상인 것을 나타내는 [ICV 플래그=subject of ICV]인 파트가 하나만 존재하는 경우에는 상술한 방법에서 생성한 체크치 $P\text{-}ICV_{ij}$를 그대로 블록의 체크치 ICV_i로 하고, 또한 하나의 블록 i 내에 체크 대상임을 나타내는 [ICV 플래그=subject of ICV]인 파트가 복수 존재하는 경우에는 복수의 파트 체크치 $P\text{-}ICV_i$, j를 파트 번호 순으로 연결한 데이터를 대상으로 하여 데이터(평문) 전체를 8바이트 단위로 도 36에 도시한 변경 체크치 생성 함수(DES-CBC-MAC, 콘텐츠 체크치 생성 키 K_{icvc}를 키로 함)에 입력하여 얻은 값으로서 생성된다. 이는 앞서 도 37에서 설명한 바와 같다.

포맷 타입 1에서는 상술한 순서로 생성된 콘텐츠 체크치의 비교 처리가 단계 S222에서 실행된다. 이하의 단계 S223 이하의 처리는 포맷 타입 0과 동일하므로 설명은 생략한다.

다음으로, 포맷 타입 2에 있어서의 콘텐츠 데이터의 재생 처리에 대하여 도 44를 이용하여 설명한다. 상기한 포맷 타입 0, 1의 재생 처리와 다른 점을 중심으로 설명한다.

단계 S201～S210은 상기한 포맷 타입 0, 1의 재생 처리와 동일하므로 설명은 생략한다.

포맷 타입 2에 있어서는 포맷 타입 0, 1에 있어서 실행된 단계 S211～S216의 처리가 실행되지 않는다. 또한, 포맷 타입 2에 있어서는 콘텐츠 체크치를 갖지 않기 때문에, 포맷 타입 0, 1에 있어서 실행된 단계 S222의 콘텐츠 체크치의 검증도 실행되지 않는다.

포맷 타입 2의 데이터 재생 처리에 있어서는 단계 S210의 체크치 B의 검증 단계 후, 단계 S217로 진행하여 기록 재생기(300)의 제어부(301)의 제어에 의해 블록 데이터가 판독된다. 또한, 단계 S241에 있어서, 기록 재생기(300)의 암호 처리부(306)에 의한 블록 데이터에 포함되는 블록 키 K_{blc}의 복호 처리가 실행된다. 기록 디바이스(400)에 저장된 블록 키 K_{blc}은 도 34에서 도시한 바와 같이 콘텐츠 키 K_{con}로 암호화되어 있으며, 앞의 단계 S207에 있어서 복호한 콘텐츠 키 K_{con}을 이용하여 블록 키 K_{blc}의 복호를 행한다.

다음으로, 단계 S242에 있어서, 단계 S241에서 복호된 블록 키 K_{blc}을 이용하여 블록 데이터의 복호 처리가 실행된다. 또한, 단계 S243에 있어서, 콘텐츠(프로그램, 데이터)의 실행, 재생 처리가 실행된다. 단계 S217～단계 S243의 처리가 모든 블록에 대하여 반복 실행된다. 단계 S244에 있어서 모든 블록 판독이라고 판정되면 재생 처리는 종료한다.

이와 같이 포맷 타입 2의 처리는 총 체크치 등의 체크치 검증 처리를 생략하고 있으며, 고속의 복호 처리 실행에 적합한 구성으로서, 음악 데이터 등 실시간 처리가 요구되는 데이터 처리에 적합한 포맷이다.

다음으로, 포맷 타입 3에 있어서의 콘텐츠 데이터의 재생 처리에 대하여 도 45를 이용하여 설명한다. 상기한 포맷 타입 0, 1, 2의 재생 처리와 다른 점을 중심으로 설명한다.

포맷 타입 3은 기본적으로 포맷 타입 2에 있어서의 처리와 공통되는 부분이 많지만, 포맷 타입 3은 도 35에 있어서 설명한 바와 같이 콘텐츠 키를 갖고 있지 않으며, 또한 블록 키 K_{blc}이 기록 디바이스에 있어서는 보존 키 K_{str}로 암호화되어 저장되는 점이 포맷 타입 2와 다르다.

단계 S201～S210에 있어서, 단계 S251, 단계 S252, 단계 S253, 단계 S254의 처리는 상술한 포맷 타입 0, 1, 2에 있어서의 대응 처리와 달리 콘텐츠 키를 포함하지 않은 처리로서 구성되어 있다.

단계 S251에 있어서, 기록 재생기(300)의 제어부(301)는 판독한 헤더로부터 기록 디바이스 고유의 보존 키 K_{str}로 암호화된 블록 정보 키 K_{bit}를 추출하여, 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

기록 재생기(300)로부터 송신된 블록 정보 키 K_{bit}를 수신한 기록 디바이스 (400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 복호화 처리시키고, 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 재 암호화시킨다. 이 처리는 상술한 「(9) 상호 인증 후의 키 교환 처리」에서 상세하게 진술한 바와 같다.

단계 S252에서는 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로부터 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}를 수신한다.

다음으로, 단계 S253에 있어서, 기록 재생기(300)의 제어부(301)는 수신한 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로 송신하고, 세션 키 K_{ses}로 재 암호화된 블록 정보 키 K_{bit}를 수신한 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 기록 재생기 암호 처리부 (302)의 암호/복호화부(308)에 세션 키 K_{ses}로 암호화된 블록 정보 키 K_{bit}를 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화시킨다.

또한, 단계 S208에 있어서, 복호화된 블록 정보 키 K_{bit}로 단계 S202에서 판독해 둔 블록 정보를 복호화한다. 또, 기록 재생기(300)의 기록 재생기 암호 처리부(302)는 복호화한 블록 정보 키 K_{bit} 및 블록 정보 BIT를 단계 S202에서 판독한 헤더에 포함되는 블록 정보 키 K_{bit} 및 블록 정보 BIT로 치환하여 보유해 둔다. 또한, 기록 재생기(300)의 제어부(301)는 복호화된 블록 정보 BIT를 기록 재생기 (300)의 기록 재생기 암호 처리부(302)로부터 판독해 둔다.

또한, 단계 S254에 있어서, 기록 재생기 암호 처리부(302)의 제어부(306)는 블록 정보 키 K_{bit} 및 블록 정보(BIT)로부터 체크치 B($ICV_{b'}$)를 생성한다. 체크치 B는 도 24에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 체크치 B 생성 키 K_{icvb}를 키로 하고, 블록 정보 키 K_{bit} 및 블록 정보 (BIT)로 이루어진 배타적 논리합 값을 DES로 암호화하여 생성한다. 다음으로, 단계 S210에 있어서, 체크치 B와 헤더(Header) 내의 ICV_b를 비교하여, 일치한 경우에는 단계 S211로 진행한다.

포맷 타입 3에서는 또한, 블록 키가 기록 디바이스에서의 저장 시에 보존 키에 의해 암호화되기 때문에, 기록 디바이스(400)에 있어서의 보존 키로의 복호 처리 및 세션 키로의 암호화 처리, 또한 기록 재생기(300)에서의 세션 키로의 복호 처리가 필요하게 된다. 이들 일련의 처리가 단계 S255, 단계 S256에서 나타낸 처리 단계이다.

단계 S255에서는 기록 재생기(300)의 제어부(301)는 단계 S217에서 판독한 블록으로부터 기록 디바이스 고유의 보존 키 K_{str}로 암호화된 블록 키 K_{blc}을 추출하여, 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

기록 재생기(300)로부터 송신된 블록 키 K_{blc}을 수신한 기록 디바이스(400)는 수신한 데이터를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 복호화 처리시키고, 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 재 암호화시킨다. 이 처리는 상술한 「(9) 상호 인증 후의 키 교환 처리」에서 상세하게 진술한 바와 같다.

단계 S256에서는 기록 재생기(300)의 제어부(301)는 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로부터 세션 키 K_{ses}로 재 암호화된 블록 키 K_{blc}을 수신한다.

다음으로, 단계 S257에 있어서, 기록 재생기(300)의 암호 처리부(306)에 의한 블록 키 K_{blc}의 세션 키 K_{ses}를 이용한 복호 처리가 실행된다.

다음으로, 단계 S242에 있어서, 단계 S257에서 복호된 블록 키 K_{blc}를 이용하여 블록 데이터의 복호 처리가 실행된다. 또한, 단계 S243에 있어서, 콘텐츠(프로그램, 데이터)의 실행, 재생 처리가 실행된다. 단계 S217～단계 S243의 처리가 모든 블록에 대하여 반복 실행된다. 단계 S244에 있어서 모든 블록 판독이라고 판정되면 재생 처리는 종료한다.

이상의 처리가 포맷 타입 3에 있어서의 콘텐츠의 재생 처리이다.

총 체크치의 검증 처리가 생략된 점에서 포맷 타입 2와 유사하지만, 블록 키의 키 교환 처리를 포함하는 점에서 포맷 타입 2에 비하여, 시큐러티 레벨이 더욱 높은 처리 구성으로 되어 있다.

(11) 콘텐츠 프로바이더에 있어서의 체크치(ICV) 생성 처리 형태

상술한 실시예 중에서, 각종 체크치 ICV에 대한 검증 처리가 콘텐츠의 다운로드 또는 재생 처리 등의 단계에서 실행되는 것을 설명하였다. 여기서는 이들 각 체크치(ICV) 생성 처리, 검증 처리의 형태에 대하여 설명한다.

우선, 실시예에서 설명한 각 체크치에 대하여 간단히 정리하면, 본 발명의 데이터 처리 장치에서 이용되는 체크치 ICV에는 다음과 같다.

체크치 A, ICV_a: 콘텐츠 데이터 중의 식별 정보, 취급 방침의 변경을 검증하기 위한 체크치.

체크치 B, ICV_b: 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보의 변경을 검증하기 위한 체크치.

콘텐츠 체크치 ICV_i: 콘텐츠의 각 콘텐츠 블록의 변경을 검증하기 위한 체크치.

총 체크치 ICV_t: 체크치 ICV_a, 체크치 ICV_b, 각 콘텐츠 블록의 체크치 전부의 변경을 검증하기 위한 체크치이다.

재생기 고유 체크치 ICV_{dev}: 로컬리제이션 플래그가 1로 세트되어 있는 경우, 즉, 콘텐츠가 기록 재생기 고유하게 이용 가능한 것을 나타내고 있는 경우에 총 체크치 ICV_t로 치환되는 체크치로서, 상술한 체크치 A:ICV_a, 체크치 B:ICV_b, 또한 콘텐츠의 체크 대상으로 되어 있는 각 블록에 포함되는 체크치 ICV_i 전체에 대한 체크치로서 생성된다.

포맷에 따라서는 ICV_t, ICV_{dev}가 체크하는 대상에 포함되는 것은 각 콘텐츠 블록의 체크치가 아니라, 콘텐츠 그 자체가 되는 경우도 있다.

이상의 각 체크치가 본 발명의 데이터 처리 장치에서 이용된다. 상기 각 체크치 중, 체크치 A, 체크치 B, 총 체크치, 콘텐츠 체크치는 예를 들면 도 32～35 및 도 6에 도시된 바와 같이 콘텐츠 데이터를 제공하는 콘텐츠 프로바이더 또는 콘텐츠 관

리자에 의해 각각의 검증 대상 데이터에 기초하여 ICV 치가 생성되어, 콘텐츠와 같이 데이터 중에 저장되어 기록 재생기(300)의 이용자에게 제공된다. 기록 재생기의 이용자, 즉 콘텐츠 이용자는 이 콘텐츠를 기록 디바이스에 다운로드할 때 또는 재생할 때 각각의 검증 대상 데이터에 기초하여 검증용 ICV를 생성하여, 저장 완료한 ICV와의 비교를 행한다. 또한, 재생기 고유 체크치 ICV_{dev}는 콘텐츠가 기록 재생기 고유하게 이용 가능한 것을 나타내고 있는 경우에 총 체크치 ICV_t로 치환되어 기록 디바이스에 저장되는 것이다.

체크치의 생성 처리는 상술한 실시예 중에서는 주로 DES-CBC에 의한 생성 처리 구성을 설명하였다. 그러나, ICV의 생성 처리 형태에는 상술한 방법에 한하지 않고 여러가지 생성 처리 형태, 또한 여러가지 검증 처리 형태가 있다. 특히, 콘텐츠 제공자 또는 관리자와, 콘텐츠 이용자와의 관계에 있어서는 이하에 설명하는 각종 ICV 생성 및 검증 처리 구성이 가능하다.

도 46~도 48에 체크치 ICV의 생성자에 있어서의 생성 처리와, 검증자에 의한 검증 처리를 설명하는 도면을 나타낸다.

도 46은 상술한 실시예 중에서 설명한 DES-CBC에 의한 ICV의 생성 처리를 예를 들면 콘텐츠 제공자 또는 관리자인 ICV 생성자가 행하고, 생성된 ICV를 콘텐츠와 같이 기록 재생기 이용자, 즉 검증자에게 제공하는 구성이다. 이 경우, 기록 재생기 이용자, 즉 검증자가 검증 처리 시에 필요한 키는 예를 들면 도 18에 도시한 내부 메모리(307)에 저장된 각 체크치 생성 키이다. 콘텐츠 이용자인 검증자(기록 재생기 이용자)는 내부 메모리(307)에 저장된 체크치 생성 키를 사용하고, 검증 대상의 데이터에 DES-CBC를 적용하여 체크치를 생성하여 저장 체크치와 비교 처리를 실행한다. 이 경우, 각 체크치 생성 키는 ICV의 생성자와, 검증자가 비밀로 공유하는 키로서 구성된다.

도 47은 콘텐츠 제공자 또는 관리자인 ICV의 생성자가 공개 키 암호계의 디지털 서명에 의해 ICV를 생성하고, 생성된 ICV를 콘텐츠와 함께 콘텐츠 이용자, 즉 검증자에게 제공한다. 콘텐츠 이용자, 즉 검증자는 ICV 생성자의 공개 키를 보존하고, 이 공개 키를 이용하여 ICV의 검증 처리를 실행하는 구성이다. 이 경우, 콘텐츠 이용자(기록 재생기 이용자), 즉 검증자가 갖는 ICV 생성자의 공개 키는 비밀로 할 필요가 없고, 관리는 용이하게 된다. ICV의 생성, 관리가 하나의 엔티티에 있어서 실행되는 경우 등, ICV의 생성, 관리가 높은 시큐러티 관리 레벨로 행해지고 있는 경우에 적합한 형태이다.

도 48은 콘텐츠 제공자 또는 관리자인 ICV의 생성자가 공개 키 암호계의 디지털 서명에 의해 ICV를 생성하고, 생성된 ICV를 콘텐츠와 함께 콘텐츠 이용자, 즉 검증자에게 제공하고, 또한 검증자가 검증에 이용하는 공개 키를 공개 키 증명서(예를 들면, 도 14 참조)에 저장하여 콘텐츠 데이터와 함께 기록 재생기 이용자, 즉 검증자에게 제공한다. ICV의 생성자가 복수 존재하는 경우에는 각 생성자는 공개 키의 정당성을 증명하는 데이터(공개 키 증명서)를 키 관리 센터에 작성해 받는다.

ICV의 검증자인 콘텐츠 이용자는 키 관리 센터의 공개 키를 갖고, 검증자는 공개 키 증명서의 검증을 키 관리 센터의 공개 키에 의해 실행하여 정당성이 확인되면, 그 공개 키 증명서에 저장된 ICV의 생성자의 공개 키를 추출한다. 또한, 추출한 ICV의 생성자의 공개 키를 이용하여 ICV의 검증을 실행한다.

이 방법은 ICV의 생성자가 복수 있으며, 이들 관리를 실행하는 센터에 의한 관리의 실행 시스템이 확립하고 있는 경우에 유효한 형태이다.

(12) 마스터 키에 기초한 암호 처리 키 생성 구성

다음으로, 본 발명의 데이터 처리 시스템에 있어서의 특징적인 구성의 하나인 마스터 키에 기초한 각종 암호 처리용 키의 생성 구성에 대하여 설명한다.

먼저 도 18을 이용하여 설명한 바와 같이 본 발명의 데이터 처리 장치에서의 기록 재생기(300)의 내부 메모리에는 여러가지 마스터 키가 저장되고, 이들 각 마스터 키를 이용하여 예를 들면 인증 키 K_{ake}를 생성(수 3 참조) 하거나 또는 배송 키 K_{dis}를 생성(수 4 참조)하는 구성으로 되어 있다.

종래, 1:1의 엔티티간, 즉 콘텐츠 프로바이더와 콘텐츠 이용자간, 또는 상술한 본 발명의 데이터 처리 장치에서의 기록 재생기(300)와 기록 미디어(400) 사이에서 암호 통신, 상호 인증, MAC 생성, 검증 등을 행할 때는 각 엔티티에 공통인 비밀 정보, 예를 들면 키 정보를 보유시키고 있었다. 또한, 1:다(多)의 관계, 예를 들면 하나의 콘텐츠 프로바이더에 대한 다수의 콘텐츠 이용자 또는 하나의 기록 재생기에 대한 다수의 기록 미디어 등의 관계에 있어서는 모든 엔티티, 즉 다수의 콘텐츠

이용자 또는 다수의 기록 미디어에 있어서 공유시킨 비밀 정보, 예를 들면 키 정보를 저장 보유시키는 구성으로 하거나, 하나의 콘텐츠 프로바이더가 다수의 콘텐츠 이용자 각각의 비밀 정보(ex. 키)를 개별로 관리하고, 이를 각 콘텐츠 이용자에 따라 구분하여 사용하고 있었다.

그러나, 상기한 바와 같은 1:다의 이용 관계가 있는 경우, 전부가 공유하는 비밀 정보(ex. 키)를 소유한 구성에 있어서는 1개소의 비밀 누설이 발생하면 동일한 비밀 정보(ex. 키)를 이용하고 있는 사람 전부에게 영향을 주게 되는 결점이 있다. 또한, 하나의 관리자, 예를 들면 콘텐츠 프로바이더가 다수의 콘텐츠 이용자 각각의 비밀 정보(ex. 키)를 개별로 관리하고, 이를 각 콘텐츠 이용자에 따라 구분하여 사용하는 구성으로 하면, 모든 이용자를 식별하고, 또한 그 식별 데이터에 고유의 비밀 정보(ex. 키)를 대응시킨 리스트가 필요하게 되고, 이용자 증대에 따른 리스트의 보수 관리의 부담이 증가한다고 하는 결점이 있다.

본 발명의 데이터 처리 장치에서는 이러한 엔티티 사이에서의 비밀 정보의 공유에 있어서의 종래의 문제점을 마스터 키의 보유 및 마스터 키로부터 각종 개별 키를 생성하는 구성에 의해 해결하였다. 이하, 이 구성에 대하여 설명한다.

본 발명의 데이터 처리 장치에서는 기록 디바이스나 콘텐츠를 저장한 미디어 또는 기록 재생기 사이에서의 각종 암호 처리, 인증 처리 등에 있어서 다른 개별 키가 필요하게 되는 경우, 그 개별 키를 디바이스나 미디어가 고유하게 갖는 식별자 데이터(ID) 등의 개별 정보와 기록 재생기(300) 내에서 사전에 결정된 개별 키 생성 방식을 이용하여 생성한다. 이 구성에 의해 만일, 생성된 개별 키가 특정된 경우라도 마스터 키의 누설을 방지하면, 시스템 전체에 대한 피해를 방지할 수 있다. 또한, 마스터 키에 의해 키를 생성하는 구성에 대응시켜 리스트의 관리도 불필요하게 된다.

구체적인 구성예에 대하여 도면을 이용하여 설명한다. 우선, 도 49에 각종 키를 기록 재생기(300)가 갖는 각종 마스터 키를 이용하여 생성하는 구성을 설명하는 도면을 나타낸다. 도 49의 미디어(500), 통신 수단(600)으로부터는 이미 설명한 실시예와 마찬가지로 콘텐츠가 입력된다. 콘텐츠는 콘텐츠 키 K_{con}에 의해 암호화되고, 또한 콘텐츠 키 K_{con}은 배송 키 K_{dis}에 의해 암호화되어 있다.

예를 들면, 기록 재생기(300)가 미디어(500), 통신 수단(600)으로부터 콘텐츠를 추출하여, 기록 디바이스(400)에 다운로드하고자 하는 경우, 앞의 도 22, 도 39～41에 있어서 설명한 바와 같이 기록 재생기(300)는 콘텐츠 키를 암호화하고 있는 배송 키 K_{dis}를 취득할 필요가 있다. 이 K_{dis}를 미디어(500), 통신 수단(600)으로부터 직접 취득하거나, 사전에 기록 재생기(300)가 취득하여 기록 재생기(300) 내의 메모리에 저장해 둘 수도 있지만, 이러한 키의 다수의 사용자에 대한 배포 구성은 앞에서도 설명한 바와 같이 시스템 전체에 영향을 줄 누설 가능성이 있다.

본 발명의 데이터 처리 시스템에서는 이 배송 키 K_{dis}를 도 49의 하부에 도시한 바와 같이 기록 재생기(300)의 메모리에 저장된 배송 키용 마스터 키 MK_{dis}와, 콘텐츠 ID에 기초한 처리, 즉 K_{dis}=DES(MK_{dis}, 콘텐츠 ID)를 적용하여 배송 키 K_{dis} 를 생성하는 구성으로 하고 있다. 본 구성에 따르면, 미디어(500), 통신 수단(600)으로부터 콘텐츠를 공급하는 콘텐츠 프로바이더와 그 콘텐츠 이용자인 기록 재생기 (300) 사이에서의 콘텐츠 배포 구성에 있어서, 콘텐츠 프로바이더가 다수 존재한 경우에서도, 각각의 배송 키 K_{dis}를 미디어, 통신 매체 등을 통해 유통시킬 필요도 없고, 또한 각 기록 재생기(300)에 저장할 필요도 없고, 시큐러티를 고도로 유지할 수 있다.

다음으로, 인증 키 K_{ake}의 생성에 대하여 설명한다. 앞서 설명한 도 22, 도 39～41의 기록 재생기(300)로부터 기록 미디어(400)에 대한 다운로드 처리 또는 도 28, 도 42～45에서 설명한 기록 미디어(400)에 저장된 콘텐츠를 기록 재생기(300)에 있어서 실행, 재생하는 경우, 기록 재생기(300)와 기록 미디어(400) 사이에서의 상호 인증 처리(도 20 참조)가 필요하게 된다.

도 20에서 설명한 바와 같이 이 인증 처리에 있어서 기록 재생기(300)는 인증 키 K_{ake}가 필요하게 된다. 기록 재생기(300)는 인증 키를 예를 들면 기록 미디어 (400)로부터 직접 취득하거나, 사전에 기록 재생기(300)가 취득하여 기록 재생기 (300) 내의 메모리에 저장해 둘 수도 있지만, 상술한 배송 키의 구성과 마찬가지로 이러한 키의 다수 사용자에 대한 배포 구성은 시스템 전체에 영향을 줄 누설 가능성이 있다.

본 발명의 데이터 처리 시스템에서는 이 인증 키 K_{ake}를 도 49의 하부에 도시한 바와 같이 기록 재생기(300)의 메모리에 저장된 인증 키용 마스터 키 MK_{ake}와, 기록 디바이스 식별 ID:ID_{mem}에 기초한 처리, 즉 K_{ake}=DES(MK_{ake}, ID_{mem})에 의해 인증 키 K_{ake}를 구하는 구성으로 하고 있다.

또한, 도 22, 도 39~41의 기록 재생기(300)로부터 기록 미디어(400)에 대한 다운로드 처리 또는 도 28, 도 42~45에서 설명한 기록 미디어(400)에 저장된 콘텐츠를 기록 재생기(300)에 있어서 실행, 재생하는 경우, 기록 재생기 고유하게 이용 가능한 콘텐츠인 경우의 기록 재생기 고유 체크치 ICV_{dev}의 생성 처리에 필요한 기록 재생기 서명 키 K_{dev}에 대해서도 상술한 배송 키, 인증 키와 동일한 구성으로 할 수 있다. 상술한 실시예 중에서는 기록 재생기 서명 키 K_{dev}는 내부 메모리에 저장하는 구성으로 하고 있었지만, 기록 재생기 서명 키용 마스터 키 MK_{dev}를 메모리에 저장하고, 기록 재생기 서명 키 K_{dev}는 내부 메모리에 저장하지 않고, 필요에 따라 도 49의 하부에 도시한 바와 같이 기록 재생기 식별자:ID_{dev}와 기록 재생기 서명 키용 마스터 키 MK_{dev}에 기초하여 K_{dev}=DES(MK_{dev}, ID_{dev})에 의해 기록 재생기 서명 키 K_{dev}를 구하는 구성으로 함으로써, 기록 재생기 서명 키 K_{dev}를 기기 개별로 갖게 할 필요가 없게 된다고 하는 이점을 들 수 있다.

이와 같이 본 발명의 데이터 처리 장치에서는 프로바이더와 기록 재생기 또는 기록 재생기와 기록 디바이스 사이와 같은 두 개의 엔티티 사이에서의 암호 정보 처리에 관한 수속에 필요한 키 등의 정보를 마스터 키와 각 ID로부터 순차적으로 생성하는 구성으로 하였기 때문에, 키 정보가 각 엔티티로부터 누설한 경우라도, 개별 키에 의한 피해 범위는 보다 한정되고, 또한 상술한 바와 같은 개별 엔티티별로 키 리스트의 관리도 불필요하게 된다.

본 구성에 관한 복수의 처리예에 대하여 플로우를 나타내어 설명한다. 도 50은 콘텐츠 제작 또는 관리자에 있어서의 마스터 키를 이용한 콘텐츠 등의 암호화 처리와, 사용자 디바이스, 예를 들면 상술한 실시예에 있어서의 기록 재생기(300)에 있어서의 마스터 키를 이용한 암호화 데이터의 복호 처리예이다.

콘텐츠 제작 또는 관리자에 있어서의 단계 S501은 콘텐츠에 대한 식별자(콘텐츠 ID)를 부여하는 단계이다. 단계 S502는 콘텐츠 제작 또는 관리자가 갖는 마스터 키와 콘텐츠 ID에 기초하여 콘텐츠 등을 암호화하는 키를 생성하는 단계이다. 이는 예를 들면, 배송 키 K_{dis}를 생성하는 공정으로 하면, 상술한 K_{dis}=DES(MK_{dis} , 콘텐츠 ID)에 의해 배송 키 K_{dis}를 생성한다. 다음으로, 단계 S503은 콘텐츠의 일부 또는 전부를 키(예를 들면, 배송 키 K_{dis})에 의해 암호화하는 단계이다. 콘텐츠 제작자는 이러한 단계를 거쳐 암호화 처리를 행한 콘텐츠를 DVD 등의 미디어, 통신 수단 등을 통해 신호 분배한다.

한편, 예를 들면 기록 재생기(300) 등의 사용자 디바이스측에서는 단계 S504에 있어서, 미디어, 통신 수단 등을 통해 수령한 콘텐츠 데이터 중에서 콘텐츠 ID를 판독한다. 다음으로, 단계 S505에 있어서, 판독한 콘텐츠 ID와 소유한 마스터 키에 기초하여 암호화 콘텐츠의 복호에 적용하는 키를 생성한다. 이 생성 처리는 배송 키 K_{dis}를 얻는 것인 경우에는 예를 들면 배송 키 K_{dis}=DES(MK_{dis}, 콘텐츠 ID)가 된다. 단계 S506에서 이 키를 이용하여 콘텐츠를 복호하고, 단계 S507에서 복호 콘텐츠의 이용, 즉 재생 또는 프로그램을 실행한다.

이 예에 있어서는 도 50 하단에 도시한 바와 같이 콘텐츠 제작 또는 관리자와, 사용자 디바이스의 쌍방이 마스터 키(예를 들면, 배송 키 생성용 마스터 키 MK_{dis})를 구비하고, 콘텐츠의 암호화, 복호에 필요한 배송 키를 순차적으로 각각이 소유한 마스터 키와 각 ID(콘텐츠 ID)에 기초하여 생성한다.

이 시스템에서는 만일 배송 키가 제3자에게 누설된 경우, 그 콘텐츠의 복호가 제3자에 있어서 가능하게 되나, 콘텐츠 ID가 다른 그 밖의 콘텐츠의 복호는 방지할 수 있기 때문에, 하나의 콘텐츠 키의 누설이 시스템 전체에 미치는 영향을 최소한으로 할 수 있다고 하는 효과가 있다. 또한, 사용자 디바이스측, 즉 기록 재생기에 있어서, 콘텐츠별 키의 대응 리스트를 보유할 필요가 없다고 하는 효과도 있다.

다음으로, 도 51을 이용하여 콘텐츠 제작 또는 관리자가 복수의 마스터 키를 소유하여, 콘텐츠의 신호 분배 대상에 따른 처리를 실행하는 예에 대하여 설명한다.

콘텐츠 제작 또는 관리자에 있어서의 단계 S511은 콘텐츠에 대한 식별자(콘텐츠 ID)를 부여하는 단계이다. 단계 S512는 콘텐츠 제작 또는 관리자가 갖는 복수의 마스터 키(예를 들면, 복수의 배송 키 생성용 마스터 키 MK_{dis})로부터 하나의 마스터 키를 선택하는 단계이다. 이 선택 처리는 도 52를 이용하여 설명하지만, 콘텐츠의 이용자의 나라별, 기종별 또는 기종의 버전별 등에 대응하여 사전에 적용하는 마스터 키를 설정해 두고, 그 설정에 따라 실행하는 것이다.

다음으로, 단계 S513에서는 단계 S512에서 선택한 마스터 키와, 단계 S511에서 결정한 콘텐츠 ID에 기초하여 암호화용 키를 생성한다. 이는 예를 들면, 배송 키 K_{disi}를 생성하는 공정으로 하면, K_{disi}=DES(MK_{disi}, 콘텐츠 ID)에 의해 생성한다. 다음으로, 단계 S514는 콘텐츠의 일부 또는 전부를 키(예를 들면, 배송 키 K_{disi})에 의해 암호화하는 단계이다. 콘텐츠 제작자는 단계 S515에 있어서, 콘텐츠 ID와, 사용한 마스터 키 식별 정보와, 암호화 콘텐츠를 하나의 배포 단위로서 암호화 처리를 행한 콘텐츠를 DVD 등의 미디어, 통신 수단 등을 통해 신호 분배한다.

한편, 예를 들면 기록 재생기(300) 등의 사용자 디바이스측에서는 단계 S516에 있어서, DVD 등의 미디어, 통신 수단 등을 통해 신호 분배된 콘텐츠 데이터 중 마스터 키 식별 정보에 대응하는 마스터 키를 자신이 소유하는가의 여부에 대하여 판정한다. 콘텐츠 데이터 중 마스터 키 식별 정보에 대응하는 마스터 키를 갖지 않은 경우, 그 배포 콘텐츠는 그 사용자 디바이스에 있어서는 이용할 수 없는 것이며, 처리는 종료한다.

신호 분배된 콘텐츠 데이터 중 마스터 키 식별 정보에 대응하는 마스터 키를 자신이 소유한 경우에는 단계 S517에 있어서, 미디어, 통신 수단 등을 통해 수령한 콘텐츠 데이터 중에서 콘텐츠 ID를 판독한다. 다음으로, 단계 S518에 있어서, 판독한 콘텐츠 ID와 소유한 마스터 키에 기초하여 암호화 콘텐츠의 복호에 적용하는 키를 생성한다. 이 생성 처리는 배송 키 K_{disi}를 얻는 것인 경우에는 예를 들면 배송 키 K_{disi}=DES(MK_{disi}, 콘텐츠 ID)가 된다. 단계 S519에서, 이 키를 이용하여 콘텐츠를 복호하고, 단계 S520에서 복호 콘텐츠의 이용, 즉 재생 또는 프로그램을 실행한다.

이 예에 있어서는 도 51 하단에 도시한 바와 같이 콘텐츠 제작 또는 관리자는 복수의 마스터 키, 예를 들면 복수의 배송 키 생성용 마스터 키 MK_{dis1}～$_n$으로 이루어진 마스터 키 세트를 갖는다. 한편, 사용자 디바이스에는 하나의 마스터 키, 예를 들면 하나의 배송 키 생성용 마스터 키 MK_{disi}를 구비하고, 콘텐츠 제작 또는 관리자가 MK_{disi}를 이용하여 암호화 처리하고 있는 경우만, 사용자 디바이스는 그 콘텐츠를 복호하여 이용할 수 있다.

도 51의 플로우에 도시한 형태의 구체예로서, 나라마다 다른 마스터 키를 적용한 예를 도 52에 도시한다. 콘텐츠 프로바이더는 마스터 키 MK1～n을 구비하고, MK1은 일본용 사용자 디바이스에 신호 분배하는 콘텐츠의 암호화 처리를 실행하는 키 생성에 이용한다. 예를 들면, 콘텐츠 ID와 MK1로부터 암호화 키 K1을 생성하여 K1에 의해 콘텐츠를 암호화한다. 또한, MK2는 US용 사용자 디바이스에 신호 분배하는 콘텐츠의 암호화 처리를 실행하는 키 생성에 이용하고, MK3은 EU(유럽)용 사용자 디바이스에 신호 분배하는 콘텐츠의 암호화 처리를 실행하는 키 생성에 이용하도록 설정하고 있다.

한편, 일본용 사용자 디바이스, 구체적으로는 일본에서 판매되는 PC 또는 게임 기기 등의 기록 재생기에는 마스터 키 MK1이 그 내부 메모리에 저장되고, US용 사용자 디바이스에는 마스터 키 MK2가 그 내부 메모리에 저장되고, EU용 사용자 디바이스에는 마스터 키 MK3이 그 내부 메모리에 저장되어 있다.

이러한 구성에 있어서, 콘텐츠 프로바이더는 콘텐츠를 이용 가능한 사용자 디바이스에 따라 마스터 키 MK1～n부터, 마스터 키를 선택적으로 사용하여 사용자 디바이스에 신호 분배하는 콘텐츠의 암호화 처리를 실행한다. 예를 들면, 콘텐츠를 일본용 사용자 디바이스만 이용 가능하게 하기 위해서는 마스터 키 MK1을 이용하여 생성된 키 K1에 의해 콘텐츠를 암호화한다. 이 암호화 콘텐츠는 일본용 사용자 디바이스에 저장된 마스터 키 MK1을 이용하여 복호 가능, 즉 복호 키를 생성할 수 있지만, 다른 US 또는 EU용 사용자 디바이스에 저장된 마스터 키 MK2, MK3으로부터는 키 K1을 얻을 수 없기 때문에 암호화 콘텐츠의 복호는 불가능하게 된다.

이와 같이 콘텐츠 프로바이더가 복수의 마스터 키를 선택적으로 사용함으로써, 여러가지 콘텐츠의 이용 제한을 설정할 수 있다. 도 52에서는 사용자 디바이스의 나라별로 마스터 키를 구별하는 예를 나타내었지만, 상술한 바와 같이 사용자 디바이스의 기종에 따라 또는 버전에 따라 마스터 키를 전환하는 등, 여러가지 이용 형태가 가능하다.

다음으로, 도 53에 미디어 고유의 식별자, 즉 미디어 ID와 마스터 키를 조합한 처리예를 나타낸다. 여기서, 미디어는 예를 들면 DVD, CD 등의 콘텐츠를 저장한 미디어이다. 미디어 ID는 하나 하나의 미디어마다 고유로 해도 좋고, 예를 들면, 영화 등의 콘텐츠 타이틀마다 고유로 해도 좋고, 미디어의 제조 로트마다 고유로 해도 좋다. 이와 같이 미디어 ID의 할당 방법으로서는 여러가지 방법을 이용할 수 있다.

미디어 제작 또는 관리자에 있어서의 단계 S521은 미디어에 대한 식별자(미디어 ID)를 결정하는 단계이다. 단계 S522는 미디어 제작 또는 관리자가 갖는 마스터 키와 미디어 ID에 기초하여 미디어 내의 저장 콘텐츠 등을 암호화하는 키를 생성하는 단계이다. 이는 예를 들면, 배송 키 K_{dis}를 생성하는 공정으로 하면, 상술한 K_{dis}=DES(MK_{dis}, 미디어 ID)에 의해 배송 키 K_{dis}를 생성한다. 다음으로, 단계 S523은 미디어 저장 콘텐츠의 일부 또는 전부를 키(예를 들면, 배송 키 K_{dis})에 의해 암호화하는 단계이다. 미디어 제작자는 이러한 단계를 거쳐 암호화 처리를 행한 콘텐츠 저장 미디어를 공급한다.

한편, 예를 들면 기록 재생기(300) 등의 사용자 디바이스측에서는 단계 S524에 있어서, 공급된 미디어로부터 미디어 ID를 판독한다. 다음으로, 단계 S525에 있어서, 판독한 미디어 ID와 소유한 마스터 키에 기초하여 암호화 콘텐츠의 복호에 적용하는 키를 생성한다. 이 생성 처리는 배송 키 K_{dis}를 얻는 것인 경우에는 예를 들면 배송 키 K_{dis}=DES(MK_{dis}, 미디어 ID)가 된다. 단계 S526에서, 이 키를 이용하여 콘텐츠를 복호하고, 단계 S527에서 복호 콘텐츠의 이용, 즉 재생 또는 프로그램을 실행한다.

본 예에 있어서는 도 53 하단에 도시한 바와 같이 미디어 제작 또는 관리자와, 사용자 디바이스의 쌍방이 마스터 키(예를 들면, 배송 키 생성용 마스터 키 MK_{dis})를 구비하고, 콘텐츠의 암호화, 복호에 필요한 배송 키를 순차적으로 각각이 소유한 마스터 키와 각 ID(미디어 ID)에 기초하여 생성한다.

이 시스템에서는 만일 미디어 키가 제3자에게 누설된 경우, 그 미디어 내의 콘텐츠의 복호가 제3자에 있어서 가능하게 되나, 미디어 ID가 다른 그 밖의 미디어에 저장된 콘텐츠의 복호는 방지할 수 있기 때문에, 하나의 미디어 키의 누설이 시스템 전체에 미치는 영향을 최소한으로 할 수 있는 효과가 있다. 또한, 사용자 디바이스측, 즉 기록 재생기에 있어서 미디어별 키의 대응 리스트를 보유할 필요가 없다고 하는 효과도 있다. 또한, 하나의 미디어 키로 암호화되는 콘텐츠 사이즈는 그 미디어 내에 저장 가능한 용량에 제한되기 때문에, 암호문 공격을 위해 필요한 정보량에 도달할 가능성은 적고, 암호 해독의 가능성을 저감시킬 수 있다.

다음으로, 도 54에 기록 재생기 고유의 식별자, 즉 기록 재생기 ID와 마스터 키를 조합한 처리예를 나타낸다.

기록 재생기 이용자에 있어서의 단계 S531은 기록 재생기의 예를 들면 내부 메모리에 저장된 마스터 키와 기록 재생기 ID에 기초하여 콘텐츠 등을 암호화하는 키를 생성하는 단계이다. 이는 예를 들면, 콘텐츠 키 K_{con}을 생성하는 공정으로 하면, K_{con}=DES(MK_{con}, 기록 재생기 ID)에 의해 콘텐츠 키 K_{con}을 생성한다. 다음으로, 단계 S532는 저장하는 콘텐츠의 일부 또는 전부를 키(예를 들면, 배송 키 K_{con})에 의해 암호화하는 단계이다. 단계 S533은 암호화 콘텐츠를 예를 들면 하드디스크 등의 기록 디바이스에 저장한다.

한편, 기록 재생기를 관리하는 시스템 관리자측에서는 콘텐츠를 저장한 기록 재생기 이용자로부터 저장 데이터의 복구를 의뢰되면, 단계 S534에 있어서, 기록 재생기로부터 기록 재생기 ID를 판독한다. 다음으로, 단계 S535에 있어서, 판독한 기록 재생기 ID와 소유한 마스터 키에 기초하여 암호화 콘텐츠의 복호에 적용하는 키를 생성한다. 이 생성 처리는 콘텐츠 키 K_{con}을 얻는 것인 경우에는 예를 들면 콘텐츠 키 K_{con}=DES(MK_{con}, 기록 재생기 ID)가 된다. 단계 S536에서, 이 키를 이용하여 콘텐츠를 복호한다.

이 예에 있어서는 도 54 하단에 도시한 바와 같이 기록 재생기 이용자와, 시스템 관리자의 쌍방이 마스터 키(예를 들면, 콘텐츠 키 생성용 마스터 키 MK_{con})를 구비하고, 콘텐츠의 암호화, 복호에 필요한 배송 키를 순차적으로 각각이 소유한 마스터 키와 각 ID(기록 재생기 ID)에 기초하여 생성한다.

이 시스템에서는 만일 콘텐츠 키가 제3자에게 누설된 경우, 그 콘텐츠의 복호가 제3자에 있어서 가능하게 되나, 기록 재생기 ID가 다른 그 밖의 기록 재생기용에 암호화된 콘텐츠의 복호는 방지할 수 있기 때문에, 하나의 콘텐츠 키의 누설이 시스템 전체에 미치는 영향을 최소한으로 할 수 있다고 하는 효과가 있다. 또한, 시스템 관리측, 사용자 디바이스측 양자에 있어서, 콘텐츠별 키의 대응 리스트를 보유할 필요가 없다고 하는 효과도 있다.

도 55는 슬레이브 디바이스, 예를 들면 메모리 카드 등의 기록 디바이스와, 호스트 디바이스, 예를 들면 기록 재생기 사이에서의 상호 인증 처리에 이용하는 인증 키를 마스터 키에 기초하여 생성하는 구성이다. 앞서 설명한 인증 처리(도 20 참조)에서는 슬레이브 디바이스의 내부 메모리에 인증 키를 사전에 저장한 구성으로 하고 있지만, 이를 도 55에 도시한 바와 같이 인증 처리 시에 마스터 키에 기초하여 생성하는 구성으로 할 수 있다.

예를 들면, 기록 디바이스인 슬레이브 디바이스는 인증 처리 개시 전의 초기화 처리로서, 단계 S541에 있어서, 기록 디바이스인 슬레이브 디바이스의 내부 메모리에 저장한 마스터 키와 슬레이브 디바이스 ID에 기초하여 상호 인증 처리에 이용하는 인증 키 K_{ake}를 생성한다. 이는 예를 들면, K_{ake}=DES(MK_{ake}, 슬레이브 디바이스 ID)에 의해 생성한다. 다음으로, 단계 S542에 있어서, 생성된 인증 키를 메모리에 저장한다.

한편, 예를 들면 기록 재생기 등의 호스트 디바이스측에서는 단계 S543에 있어서, 장착된 기록 디바이스, 즉 슬레이브 디바이스로부터 통신 수단을 통해 슬레이브 디바이스 ID를 판독한다. 다음으로, 단계 S544에 있어서, 판독된 슬레이브 디바이스 ID와 소유한 인증 키 생성용 마스터 키에 기초하여 상호 인증 처리에 적용하는 인증 키를 생성한다. 이 생성 처리는 예를 들면 인증 키 K_{ake}=DES(MK_{ake}, 슬레이브 디바이스 ID)가 된다. 단계 S545에서, 이 인증 키를 이용하여 인증 처리를 실행한다.

이 예에 있어서는 도 55 하단에 도시한 바와 같이 슬레이브 디바이스와, 마스터 디바이스의 쌍방이 마스터 키, 즉 인증 키 생성용 마스터 키 MK_{ake}를 구비하고, 상호 인증 처리에 필요한 인증 키를 순차적으로 각각이 소유한 마스터 키와 슬레이브 디바이스 ID에 기초하여 생성한다.

이 시스템에서는 만일 인증 키가 제3자에게 누설된 경우, 그 인증 키는 그 슬레이브 디바이스에만 유효하기 때문에, 다른 슬레이브 디바이스와의 관계에 있어서는 인증이 성립하지 않게 되며, 키 누설에 의해 발생하는 영향을 최소한으로 할 수 있다고 하는 효과가 있다.

이와 같이 본 발명의 데이터 처리 장치에서는 콘텐츠 프로바이더와 기록 재생기 또는 기록 재생기와 기록 디바이스 사이와 같은 두 개의 엔티티 사이에서의 암호 정보 처리에 관한 수속에 필요한 키 등의 정보를 마스터 키와 각 ID로부터 순차적으로 생성하는 구성으로 하였다. 따라서, 키 정보가 각 엔티티로부터 누설된 경우라도, 개별 키에 의한 피해 범위는 보다 한정되고, 또한 상술한 바와 같은 개별 엔티티별 키 리스트의 관리도 불필요하게 된다.

(13) 암호 처리에 있어서의 암호 강도의 제어

상술한 실시예에 있어서, 기록 재생기(300)와 기록 디바이스(400) 사이에서의 암호 처리는 설명을 이해하기 쉽게 하기 위해서, 주로, 앞서 도 7을 이용하여 설명한 싱글 DES 구성에 의한 암호 처리를 이용한 예에 대하여 설명하였다. 그러나, 본 발명의 데이터 처리 장치에서 적용되는 암호화 처리 방식은 상술한 싱글 DES 방식에 한정되는 것이 아니라, 필요한 시큐러티 상태에 따른 암호화 방식을 채택할 수 있다.

예를 들면, 앞서 설명한 도 8～도 10의 구성과 같은 트리플 DES 방식을 적용해도 좋다. 예를 들면, 도 3에 도시한 기록 재생기(300)의 암호 처리부(302)와, 기록 디바이스(400)의 암호 처리부(401)의 쌍방에 있어서, 트리플 DES 방식을 실행 가능한 구성으로 하고, 도 8～도 10에서 설명한 트리플 DES 방식에 의한 암호 처리에 대응하는 처리를 실행하는 구성이 가능하다.

그러나, 콘텐츠 제공자는 콘텐츠에 따라 처리 속도를 우선하여 콘텐츠 키 K_{con}을 싱글 DES 방식에 의한 64비트 키 구성으로 하는 경우도 있으며, 또한 시큐러티를 우선하여 콘텐츠 키 K_{con}을 트리플 DES 방식에 의한 128비트 또는 192비트 키 구성으로 하는 경우도 있다. 따라서, 기록 재생기(300)의 암호 처리부(302)와, 기록 디바이스(400)의 암호 처리부(401)의 구성을 트리플 DES 방식, 싱글 DES 방식 어느 한쪽의 방식에만 대응 가능한 구성으로 하는 것은 바람직하지 못하다. 따라서, 기록 재생기(300)의 암호 처리부(302)와, 기록 디바이스(400)의 암호 처리부 (401)는 싱글 DES, 트리플 DES 어느 하나의 방식에도 대응 가능하게 하는 구성이 바람직하다.

그러나, 기록 재생기(300)의 암호 처리부(302)와, 기록 디바이스(400)의 암호 처리부(401)의 암호 처리 구성을 싱글 DES 방식, 트리플 DES 방식의 쌍방을 실행 가능한 구성으로 하기 위해서는 각각의 다른 회로, 논리를 구성해야 한다. 예를 들

면, 기록 디바이스(400)에 있어서 트리플 DES에 대응하는 처리를 실행하기 위해서는 앞의 도 29에 도시한 커맨드 레지스터에 트리플 DES의 명령 세트를 새롭게 저장할 필요가 있다. 이는 기록 디바이스(400)에 구성하는 처리부의 복잡화를 초래하게 된다.

그래서, 본 발명의 데이터 처리 장치는 기록 디바이스(400)측의 암호 처리부 (401)가 갖는 논리를 싱글 DES 구성으로서, 또한 트리플 DES 암호화 처리에 대응한 처리가 실행 가능하고, 트리플 DES 방식에 의한 암호화 데이터(키, 콘텐츠 등)를 기록 디바이스의 외부 메모리(402)에 저장하는 것을 가능하게 한 구성을 제안한다.

예를 들면, 도 32에 도시한 데이터 포맷 타입 0의 예에 있어서, 기록 재생기 (300)로부터 기록 디바이스(400)에 대하여 콘텐츠 데이터의 다운로드를 실행할 때, 앞서 설명한 포맷 타입 0의 다운로드의 플로우를 나타내는 도 39의 단계 S101에서 인증 처리를 실행하고, 여기서 세션 키 K_{ses}를 생성한다. 또한, 단계 S117에 있어서, 기록 재생기(300)측의 암호 처리부(302)에 있어서 세션 키 K_{ses}에 의한 콘텐츠 키 K_{con}의 암호화 처리가 실행되고, 이 암호화 키가 기록 디바이스(400)에 통신 수단을 통해 전송되고, 단계 S118에 있어서, 이 암호화 키를 수신한 기록 디바이스 (400)의 암호 처리부(403)가 세션 키 K_{ses}에 의한 콘텐츠 키 K_{con}의 복호 처리를 실행하고, 또한 보존 키 K_{str}에 의한 콘텐츠 키 K_{con}의 암호화 처리를 실행하여, 이를 기록 재생기(300)의 암호 처리부(302)로 송신하고, 그 후 기록 재생기(300)가 데이터 포맷을 형성(단계 S121)하여 포맷화된 데이터를 기록 디바이스(400)로 송신하고, 기록 디바이스(400)가 수신한 데이터를 외부 메모리(402)에 저장하는 처리를 행하고 있다.

상기 처리에 있어서 단계 S117, S118 사이에서 실행되는 기록 디바이스(400)의 암호 처리부(401)에서의 암호 처리를 싱글 DES 또는 트리플 DES 어느 하나의 방식을 선택적으로 실행 가능한 구성으로 하면, 콘텐츠 제공 업자가 트리플 DES에 따른 콘텐츠 키 K_{con}을 이용한 콘텐츠 데이터를 제공하는 경우도, 또한 싱글 DES에 따른 콘텐츠 키 K_{con}을 이용한 콘텐츠 데이터를 제공하는 경우도, 어느 경우에도 대응할 수 있다.

도 56에 본 발명의 데이터 처리 장치에서의 기록 재생기(300)의 암호 처리부 (302)와, 기록 디바이스(400)의 암호 처리부(401)의 쌍방을 이용하여 트리플 DES 방식에 따른 암호 처리 방법을 실행하는 구성을 설명하는 플로우를 나타낸다. 도 56에서는 일례로서 기록 재생기(300)로부터 콘텐츠 데이터를 기록 디바이스(400)에 다운로드할 때 실행되는 보존 키 K_{str}를 이용한 콘텐츠 키 K_{con}의 암호화 처리예로서, 콘텐츠 키 K_{con}이 트리플 DES 방식에 의한 키인 경우의 예를 나타내고 있다. 또, 여기서는 콘텐츠 키 K_{con}을 대표하여 그 처리예를 나타내지만, 다른 키 또는 콘텐츠 등, 그 밖의 데이터에 대해서도 동일한 처리가 가능하다.

트리플 DES 방식에 있어서는 앞의 도 8～10에 있어서 설명한 바와 같이 싱글 DES에서는 64비트 키, 트리플 DES 방식에 의한 경우에는 128비트 또는 192비트 키 구성으로서, 두 개 또는 세 개의 키가 이용되는 처리이다. 이들 세 개의 콘텐츠 키를 각각 K_{con1}, K_{con2}, (K_{con3})으로 한다. K_{con3}은 이용되지 않은 경우도 있기 때문에, 괄호로 나타내고 있다.

도 56의 처리에 대하여 설명한다. 단계 S301은 기록 재생기(300)와, 기록 디바이스(400) 사이에서의 상호 인증 처리 단계이다. 상호 인증 처리 단계는 앞서 설명한 도 20의 처리에 의해 실행된다. 또, 인증 처리 시, 세션 키 K_{ses}가 생성된다.

단계 S301의 인증 처리가 종료하면, 단계 S302에 있어서, 각 체크치, 체크치 A, 체크치 B, 콘텐츠 체크치, 총 체크치, 각 ICV의 대조 처리가 실행된다.

이들 체크치(ICV) 대조 처리가 종료하여 데이터 변경이 없다고 판정하면, 단계 S303으로 진행하고, 기록 재생기(300)에 있어서, 기록 재생기 암호 처리부 (302)의 제어부(306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)를 사용하여, 먼저 추출한 또는 생성한 배송 키 K_{dis}를 이용하여 수신한 미디어(500) 또는 통신부(305)를 통해 통신 수단(600)으로부터 수신한 데이터의 헤더부에 저장된 콘텐츠 키 K_{con}의 복호화 처리를 행한다. 이 경우의 콘텐츠 키는 트리플 DES 방식에 의한 키이고, 콘텐츠 키 K_{con1}, K_{con2}, (K_{con3})이다.

다음으로, 단계 S304에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 있어서, 단계 S303에서 복호화한 콘텐츠 키 K_{con1}, K_{con2}, (K_{con3}) 중 콘텐츠 키 K_{con1} 만을 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화한다.

기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 콘텐츠 키 K_{con1}을 포함하는 데이터를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독하고, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S305에 있어서, 기록 재생기(300)로부터 송신된 콘텐츠 키 K_{con1}을 수신한 기록 디바이스(400)는 수신한 콘텐츠 키 K_{con1}을 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화한다. 또한, 단계 S306에 있어서, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시키고, 통신부(404)를 통해 기록 재생기(300)로 송신한다.

다음으로, 단계 S307에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 있어서, 단계 S303에서 복호화한 콘텐츠 키 K_{con1}, K_{con2}, (K_{con3}) 중 콘텐츠 키 K_{con2} 만을 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화한다.

기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 콘텐츠 키 K_{con2}를 포함하는 데이터를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독하고, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S308에 있어서, 기록 재생기(300)로부터 송신된 콘텐츠 키 K_{con2}를 수신한 기록 디바이스(400)는 수신한 콘텐츠 키 K_{con2}를 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화한다. 또한, 단계 S309에 있어서, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시키고, 통신부(404)를 통해 기록 재생기(300)로 송신한다.

다음으로, 단계 S310에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 있어서, 단계 S303에서 복호화한 콘텐츠 키 K_{con1}, K_{con2}, (K_{con3})의 중의 콘텐츠 키 K_{con3} 만을 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 암호화한다.

기록 재생기(300)의 제어부(301)는 세션 키 K_{ses}로 암호화된 콘텐츠 키 K_{con3}을 포함하는 데이터를 기록 재생기(300)의 기록 재생기 암호 처리부(302)로부터 판독하고, 이들 데이터를 기록 재생기(300)의 기록 디바이스 컨트롤러(303)를 통해 기록 디바이스(400)로 송신한다.

다음으로, 단계 S311에 있어서, 기록 재생기(300)로부터 송신된 콘텐츠 키 K_{con3}을 수신한 기록 디바이스(400)는 수신된 콘텐츠 키 K_{con3}을 기록 디바이스 암호 처리부(401)의 암호/복호화부(406)에 상호 인증 시에 공유해 둔 세션 키 K_{ses}로 복호화한다. 또한, 단계 S312에 있어서, 기록 디바이스 암호 처리부(401)의 내부 메모리(405)에 보존되어 있는 기록 디바이스 고유의 보존 키 K_{str}로 재 암호화시키고, 통신부(404)를 통해 기록 재생기(300)로 송신한다.

다음으로, 단계 S313에 있어서, 기록 재생기의 암호 처리부는 도 32~35에서 설명한 각종 데이터 포맷을 형성하고, 기록 디바이스(400)로 송신한다.

마지막으로 단계 S314에 있어서, 기록 디바이스(400)는 포맷 형성이 종료한 수신 데이터를 외부 메모리(402)에 저장한다. 이 포맷 데이터에는 보존 키 K_{str}로 암호화된 콘텐츠 키 K_{con1}, K_{con2}, (K_{con3})을 포함하고 있다.

이러한 처리를 실행함으로써, 기록 디바이스(400)에 저장하는 콘텐츠 키를 트리플 DES 방식의 암호 방식에 의한 키로서 저장할 수 있다. 또, 콘텐츠 키가 K_{con1}, K_{con2}의 두 개의 키인 경우에는 단계 S310~S312의 처리는 생략된다.

이와 같이 기록 디바이스(400)는 동일한 형태의 처리, 즉 단계 S305, S306의 처리 단계를 수회, 그 대상을 변경하는 것만으로 반복 실행함으로써, 트리플 DES가 적용된 키를 메모리에 저장할 수 있다. 콘텐츠 키 K_{con}이 싱글 DES의 적용 키인 경우에는 단계 S305, S306을 실행하고, 단계 S313의 포맷화 처리를 실행하여 메모리에 저장하면 좋다. 이러한 구성은 단

계 S305, S306의 처리를 실행하는 커맨드를 앞서 설명한 도 29의 커맨드 레지스터에 저장하고, 이 처리를 콘텐츠 키의 형태, 즉 트리플 DES 방식인지, 싱글 DES 방식인지에 따라 적절하게 1회～3회 실행하는 구성으로 하면 좋다. 따라서, 기록 디바이스(400)의 처리 논리 중에 트리플 DES의 처리 방식을 포함시키지 않고 트리플 DES 방식, 싱글 DES 방식의 쌍방 처리가 가능하게 된다. 또, 암호화 방식에 대해서는 콘텐츠 데이터의 헤더부 내의 취급 방침에 기록하고, 이를 참조함으로써 판정할 수 있다.

(14) 콘텐츠 데이터에 있어서의 취급 방침 중의 기동 우선 순위에 기초한 프로그램 기동 처리

앞서 설명한 도 4～6의 콘텐츠 데이터 구성에서 알 수 있는 바와 같이, 본 발명의 데이터 처리 장치에서 이용되는 콘텐츠 데이터의 헤더부에 저장된 취급 방침에는 콘텐츠 타입, 기동 우선 순위 정보가 포함된다. 본 발명의 데이터 처리 장치에서의 기록 재생기(300)는 기록 디바이스(400) 또는 DVD, CD, 하드디스크, 게다가 게임 카트리지 등의 각종 기록 매체에 기록된 액세스 가능한 콘텐츠 데이터가 복수 존재하는 경우, 이들 콘텐츠의 기동 순위를 기동 우선 순위 정보에 따라 결정한다.

기록 재생기(300)는 각 기록 디바이스 DVD 장치, CD 드라이브 장치, 하드 디스크 드라이브 장치 등 각종 기록 디바이스와의 인증 처리를 실행 후, 콘텐츠 데이터 중의 우선 순위 정보에 따라 가장 우선 순위가 높은 콘텐츠 데이터 중의 프로그램을 우선하여 실행한다. 이하, 「콘텐츠 데이터에 있어서의 취급 방침 중의 기동 우선 순위에 기초한 프로그램 기동 처리」에 대하여 설명한다.

상술한 본 발명의 데이터 처리 장치 실시예의 설명에 있어서는 기록 재생기 (300)가 하나의 기록 디바이스(400)로부터 콘텐츠 데이터를 재생, 실행하는 경우의 처리를 중심으로 하여 설명하였다. 그러나, 일반적으로 기록 재생기(300)는 도 2에 도시한 바와 같이 기록 디바이스(400) 외에 판독부(304)를 통해 DVD, CD, 하드디스크, 또한 PIO(111), SIO(112)를 통해 접속되는 메모리 카드, 게임 카트리지 등, 각종 기록 매체를 액세스 가능한 구성을 갖는다. 또, 도 2에서는 도면의 복잡화를 피하기 위해서 판독부(304)를 하나만 기재하고 있지만, 기록 재생기(300)는 다른 기억 매체, 예를 들면 DVD, CD, 플로피 디스크, 하드디스크를 병렬로 장착 가능하다.

기록 재생기(300)는 복수의 기억 매체를 액세스 가능하고, 각각의 기억 매체에는 각각 콘텐츠 데이터가 저장되어 있다. 예를 들면, CD 등 외부의 콘텐츠 프로바이더가 공급하는 콘텐츠 데이터는 상술한 도 4의 데이터 구성으로 미디어에 저장되고, 이들 미디어 또는 통신 수단을 통해 다운로드한 경우에는 도 26, 도 27의 콘텐츠 데이터 구성으로 메모리 카드 등의 각 기억 매체에 저장되어 있다. 또한, 구체적으로는 콘텐츠 데이터의 포맷 타입에 따라 도 32～35에 도시한 바와 같이 미디어 상, 기록 디바이스 상에서 각각 다른 포맷으로 저장된다. 그러나, 어느 경우에도 콘텐츠 데이터의 헤더 중의 취급 방침에는 콘텐츠 타입, 기동 우선 순위 정보가 포함된다.

이들, 복수의 콘텐츠 데이터에 대한 액세스가 가능한 경우의 기록 재생기의 콘텐츠 기동 처리를 플로우에 따라 설명한다.

도 57은 기동 가능 콘텐츠가 복수 있는 경우의 처리예(1)를 나타내는 처리 플로우이다. 단계 S611은 기록 재생기(300)가 액세스 가능한 기록 디바이스의 인증 처리를 실행하는 단계이다. 액세스 가능한 기록 디바이스에는 메모리 카드, DVD 장치, CD 드라이브, 하드디스크 장치, 또한 예를 들면 PIO(111), SIO(112)를 통해 접속되는 게임 카트리지 등이 포함된다. 인증 처리는 도 2에 도시한 제어부 (301)의 제어 하에 각 기록 디바이스에 대하여 예를 들면 먼저 도 20에서 설명한 순서에 따라 실행된다.

다음으로, 단계 S612에 있어서, 인증에 성공한 기록 디바이스 내의 메모리에 저장된 콘텐츠 데이터로부터 기동 가능한 프로그램을 검출한다. 이는 구체적으로는 콘텐츠 데이터의 취급 방침에 포함되는 콘텐츠 타입이 프로그램인 것을 추출하는 처리로서 실행된다.

다음으로, 단계 S613에 있어서, 단계 S612에서 추출된 기동 가능한 프로그램에 있어서의 기동 우선 순위를 판정한다. 이는 구체적으로는 단계 S612에 있어서 선택된 복수의 기동 가능한 콘텐츠 데이터의 헤더 중의 취급 정보에 포함되는 우선 정보를 비교하여 가장 높은 우선 순위를 선택하는 처리이다.

다음으로, 단계 S614에서 선택된 프로그램을 기동한다. 또, 복수의 기동 가능한 프로그램에 있어서 설정된 우선 순위가 동일한 경우에는 기록 디바이스 사이에서 디폴트의 우선 순위를 설정하여, 최우선되는 디바이스에 저장된 콘텐츠 프로그램을 실행한다.

도 58에는 복수의 기록 디바이스에 식별자를 설정하고, 각 식별자가 첨부된 기록 디바이스에 대하여 순차, 인증 처리, 콘텐츠 프로그램 검색을 실행하는 처리 형태, 즉 기동 가능 콘텐츠가 복수 있는 경우의 처리예(2)를 나타내었다.

단계 S621에서는 기록 재생기(300)에 장착된 기록 디바이스(i)의 인증 처리(도 20 참조)를 실행하는 단계이다. 복수(n개)의 기록 디바이스에는 순차 1～n의 식별자가 부여되어 있다.

단계 S622에서는 단계 S621에서의 인증이 성공하였는지의 여부를 판정하여, 인증이 성공한 경우에는 단계 S623으로 진행하고, 그 기록 디바이스(i)의 기록 매체 중에서 기동 가능 프로그램을 검색한다. 인증이 성공하지 않은 경우에는 단계 S627로 진행하고, 새로운 콘텐츠 검색 가능한 기록 디바이스의 유무를 판정하여, 기록 디바이스가 없는 경우에는 처리를 종료하고, 기록 디바이스가 존재하는 경우에는 단계 S628로 진행하여 기록 디바이스 식별자 i를 갱신하고, 단계 S621 이후의 인증 처리 단계를 반복한다.

단계 S623에 있어서의 처리는 기록 디바이스(i)에 저장된 콘텐츠 데이터로부터 기동 가능한 프로그램을 검출하는 처리이다. 이는 구체적으로는 콘텐츠 데이터의 취급 방침에 포함되는 콘텐츠 타입이 프로그램인 것을 추출하는 처리로서 실행된다.

단계 S624에서는 콘텐츠 타입이 프로그램인 것이 추출되었는지의 여부를 판정하여, 추출된 경우에는 단계 S625에 있어서, 추출 프로그램 중 가장 우선 순위가 높은 것을 선택하고, 단계 S626에 있어서 선택 프로그램을 실행한다.

단계 S624에 있어서, 콘텐츠 타입이 프로그램인 것이 추출되지 않았다고 판정된 경우에는 단계 S627로 진행하여 새로운 콘텐츠 검색인 기록 디바이스의 유무를 판정하여, 기록 디바이스가 없는 경우에는 처리를 종료하고, 기록 디바이스가 존재하는 경우에는 단계 S628로 진행하여 기록 디바이스 식별자 i를 갱신하고, 단계 S621 이후의 인증 처리 단계를 반복한다.

도 59는 기동 가능 콘텐츠가 복수 있는 경우의 처리예(3)를 나타내는 처리 플로우이다. 단계 S651은 기록 재생기(300)가 액세스 가능한 기록 디바이스의 인증 처리를 실행하는 단계이다. 액세스 가능한 DVD 장치, CD 드라이브, 하드디스크 장치, 메모리 카드, 게임 카트리지 등의 인증 처리를 실행한다. 인증 처리는 도 2에서 도시한 제어부(301)의 제어 하에 각 기록 디바이스에 대하여 예를 들면 먼저 도 20에서 설명한 순서에 따라 실행된다.

다음으로, 단계 S652에 있어서, 인증에 성공한 기록 디바이스 내의 메모리에 저장된 콘텐츠 데이터로부터 기동 가능한 프로그램을 검출한다. 이는 구체적으로는 콘텐츠 데이터의 취급 방침에 포함되는 콘텐츠 타입이 프로그램인 것을 추출하는 처리로서 실행된다.

다음으로, 단계 S653에 있어서, 단계 S652에서 추출된 기동 가능한 프로그램의 명칭 등의 정보를 표시 수단에 표시한다. 또, 표시 수단은 도 2에서는 도시되어 있지 않지만, AV 출력 데이터로서 출력된 데이터가 도시하지 않은 표시 수단에 출력되는 구성으로 되어 있다. 또, 각 콘텐츠 데이터의 프로그램명 등의 사용자 제공 정보는 콘텐츠 데이터의 식별 정보 중에 저장되어 있으며, 도 2에 도시한 메인 CPU(106)의 제어 하에 제어부(301)를 통해 인증 완료한 각 콘텐츠 데이터의 프로그램 명칭 등, 프로그램 정보를 출력 수단에 출력한다.

다음으로, 단계 S654에서는 도 2에 도시한 입력 인터페이스, 컨트롤러, 마우스, 키보드 등의 입력 수단으로부터의 사용자에 의한 프로그램 선택 입력을 입력 인터페이스(110)를 통해 메인 CPU(106)가 수령하고, 선택 입력에 따라 단계 S655에 있어서 사용자 선택 프로그램을 실행한다.

이와 같이 본 발명의 데이터 처리 장치에서는 콘텐츠 데이터 중의 헤더 내의 취급 정보에 프로그램 기동 우선 순위 정보를 저장하여, 기록 재생기(300)가 이 우선 순위에 따라 프로그램을 기동하거나, 표시 수단에 기동 프로그램 정보를 표시하여 사용자에 의해 선택하는 구성으로 하였기 때문에 사용자가 프로그램을 검색할 필요가 없고, 기동에 필요한 시간 및 사용자의 노동력을 생략할 수 있다. 또, 기동 가능한 프로그램은 전부 기록 디바이스의 인증 처리 후에 기동 또는 기동 가능 프로그램인 것의 표시가 이루어지기 때문에 프로그램을 선택하고 나서 정당성 확인을 행하는 등의 처리의 번잡성이 해소된다.

(15) 콘텐츠 구성 및 재생(신장) 처리

본 발명의 데이터 처리 장치에서는 상술한 바와 같이 기록 재생기(300)는 미디어(500) 또는 통신 수단(600)으로부터 콘텐츠를 다운로드 또는 기록 디바이스 (400)로부터 재생 처리를 행한다. 상기한 설명은 콘텐츠의 다운로드 또는 재생 처리에 따른 암호화 데이터의 처리를 중심으로 하여 설명하였다.

도 3의 기록 재생기(300)에 있어서의 제어부(301)는 콘텐츠 데이터를 제공하는 DVD 등의 디바이스(500), 통신 수단(600), 기록 디바이스로부터의 콘텐츠 데이터의 다운로드 처리 또는 재생 처리에 따른 인증 처리, 암호화, 복호화 처리 전반을 제어한다.

이들 처리 결과로서 얻어진 재생 가능한 콘텐츠는 예를 들면 음성 데이터, 화상 데이터 등이다. 복호 데이터는 제어부(301)로부터 도 2에 도시한 메인 CPU 의 제어 하에 놓이고, 음성 데이터, 화상 데이터 등에 따라 AV 출력부로 출력된다. 그러나, 콘텐츠가 예를 들면 음성 데이터이고 MP3 압축이 이루어져 있으면, 도 2에 도시한 AV 출력부의 MP3 디코더에 의해 음성 데이터의 복호 처리가 실행되어 출력된다. 또한, 콘텐츠 데이터가 화상 데이터이고 MPEG2 압축 화상이면, AV 처리부의 MPEG2 디코더에 의해 신장 처리가 실행되어 출력된다. 이와 같이 콘텐츠 데이터에 포함된 데이터는 압축(부호화) 처리가 이루어져 있는 경우도 있고, 또한 압축 처리가 실시되고 있지 않은 데이터도 있어, 콘텐츠에 따른 처리를 실시하여 출력한다.

그러나, 압축 처리, 신장 처리 프로그램에는 여러가지 종류가 있으며, 콘텐츠 프로바이더로부터 압축 데이터를 제공받아도 대응하는 신장 처리 실행 프로그램이 없는 경우에는 이를 재생할 수 없다고 하는 사태가 발생한다.

그래서, 본 발명의 데이터 처리 장치는 데이터 콘텐츠 중에 압축 데이터와 그 복호(신장) 처리 프로그램을 더불어 저장하는 구성 또는 압축 데이터와 복호(신장) 처리 프로그램과의 링크 정보를 콘텐츠 데이터의 헤더 정보로서 저장하는 구성을 개시한다.

도 2에 도시한 데이터 처리 전체 도면으로부터 본 구성에 관한 요소 및 관련 요소를 간단하게 정리한 도면을 도 60에 도시한다. 기록 재생기(300)는 예를 들면 DVD, CD 등의 디바이스(500) 또는 통신 수단(600) 또는 콘텐츠를 저장한 메모리 카드 등의 기록 디바이스(400)로부터 여러가지 콘텐츠의 제공을 받는다. 이들 콘텐츠는 음성 데이터, 정지 화상, 동화상 데이터, 프로그램 데이터 등이고, 또한 암호화 처리가 실시되어 있는 것, 실시되어 있지 않은 것, 또한 압축 처리가 이루어져 있는 것, 이루어져 있지 않은 것 등, 여러가지 데이터가 포함된다.

수령 콘텐츠가 암호화되어 있는 경우에는 이미 상술한 항목 중에서 설명한 바와 같은 방법에 의해 제어부(301)의 제어 및 암호 처리부(302)의 암호 처리에 의해 복호 처리가 실행된다. 복호된 데이터는 메인 CPU(106)의 제어 하에서, AV 처리부(109)로 전송되어 AV 처리부(109)의 메모리(3090)에 저장된 후, 콘텐츠 해석부 (3091)에 있어서 콘텐츠 구성의 해석이 실행된다. 예를 들면, 콘텐츠 중에 데이터 신장 프로그램이 저장되어 있으면, 프로그램 기억부(3093)에 프로그램을 저장하고, 음성 데이터, 화상 데이터 등의 데이터가 포함되어 있으면 이들을 데이터 기억부 (3092)에 기억한다. 신장 처리부(3094)에서는 프로그램 기억부에 기억된 예를 들면 MP3 등의 신장 처리 프로그램을 이용하여 데이터 기억부(3092)에 기억된 압축 데이터의 신장 처리를 실행하여, 스피커(3001), 모니터(3002)로 출력된다.

다음으로, AV 처리부(109)가 제어부(301)를 통해 수령하는 데이터의 구성 및 처리의 몇 개의 예에 대하여 설명한다. 또, 여기서는 콘텐츠의 예로서 음성 데이터를 나타내고, 또한 압축 프로그램의 예로서 MP3을 적용한 것을 대표하여 설명하지만, 본 구성은 음성 데이터뿐만 아니라, 화상 데이터에도 적용할 수 있는 것이고, 또한 압축 신장 처리 프로그램에 대해서도 MP3뿐만 아니라, MPEG2, 4 등 각종 프로그램을 적용할 수 있다.

도 61에 콘텐츠 구성예를 나타낸다. 도 61은 MP3에 의해 압축된 음악 데이터(6102), MP3 복호(신장) 처리 프로그램(6101)을 더불어 하나의 콘텐츠로서 구성한 예이다. 이들 콘텐츠는 1콘텐츠로서 미디어(500) 또는 기록 디바이스(400)에 저장되거나, 통신 수단(600)으로부터 신호 분배된다. 기록 재생기(300)는 이들 콘텐츠가 먼저 설명한 바와 같이 암호화되어 있는 것이면, 암호 처리부(303)에 의해 복호 처리를 실행한 후, 처리부(109)로 전송된다.

AV 처리부(109)의 콘텐츠 해석부(3091)에서는 수취한 콘텐츠를 해석하고, 음성 데이터 신장 프로그램(MP3 디코더)부와, 압축 음성 데이터부로 이루어진 콘텐츠로부터 음성 데이터 신장 프로그램(MP3 디코더)부를 추출하여 프로그램 기억부(3093)에 프로그램을 기억하고, 압축 음성 데이터를 데이터 기억부(3092)에 기억한다. 또, 콘텐츠 해석부(3091)는 콘텐츠와는 별도로 수령한 콘텐츠명, 콘텐츠 구성 정보 등의 정보를 수령하거나 또는 콘텐츠 내에 포함되는 데이터명 등의 식별 데이터, 데이터 길이, 데이터 구성 등을 나타내는 데이터에 기초하여 콘텐츠 해석을 실행해도 좋다. 다음으로, 압축 신장 처리부(3094)는 프로그램 기억부(3093)에 기억된 음성 데이터 신장 프로그램(MP3 디코더)에 따라 데이터 기억부(3092)에 기억된 MP3 압축 음성 데이터의 신장 처리를 실행하고, AV 처리부(109)는 신장한 음성 데이터를 스피커(3001)로 출력한다.

도 62에 도 61의 콘텐츠 구성을 갖는 데이터의 재생 처리의 일례를 나타내는 플로우를 나타낸다. 단계 S671은 AV 처리부(109)의 메모리(3090)에 저장된 데이터명, 예를 들면 음악 데이터의 콘텐츠이면 곡명 등의 정보를 콘텐츠와는 별도로 수령한 정보 또는 콘텐츠 내의 데이터로부터 추출하여 모니터(3002)에 표시한다. 단계 S672는 사용자의 선택을 스위치, 키보드 등의 각종 입력 수단으로부터 입력 인터페이스(110)를 통해 수령하고, CPU(106)의 제어 하에 사용자 입력 데이터에 기초한 재생 처리 명령을 AV 처리부(109)로 출력한다. AV 처리부(109)는 단계 S673에 있어서 사용자 선택에 의한 데이터의 추출, 신장 처리를 실행한다.

다음으로, 도 63에 하나의 콘텐츠에는 압축 음성 데이터 또는 신장 처리 프로그램 중 어느 한쪽이 포함되고, 또한 각 콘텐츠의 헤더 정보로서 콘텐츠의 내용을 나타내는 콘텐츠 정보가 포함되는 구성예를 나타낸다.

도 63에 도시한 바와 같이 콘텐츠가 프로그램(6202)인 경우에는 헤더 정보 (6201)로서 프로그램인 것 및 프로그램 종류가 MP3 신장 프로그램인 것을 나타내는 콘텐츠 식별 정보가 포함된다. 한편, 음성 데이터(6204)를 콘텐츠로서 포함하는 경우에는 헤더(6203)의 콘텐츠 정보에는 MP3 압축 데이터인 정보가 포함된다. 이 헤더 정보는 예를 들면, 상술한 도 4에 도시한 콘텐츠 데이터 구성의 취급 방침(도 5 참조) 중에 포함되는 데이터로부터 재생에 필요한 정보만을 선택하여 AV 처리부 (109)로 전송하는 콘텐츠에 부가하여 구성할 수 있다. 구체적으로는 도 5에 도시한 「취급 방침」 중의 각 구성 데이터에 암호 처리부(302)에 있어서 필요한 취급 방침 데이터와, AV 처리부(109)에 있어서의 재생 처리 시에 필요한 데이터와의 식별치를 부가하고, 이들 식별치가 AV 처리부(109)에 있어서 필요한 것을 나타내는 것만을 추출하여 헤더 정보로 할 수 있다.

도 63에 도시한 각 콘텐츠를 수령한 AV 처리부(109)의 콘텐츠 해석부(3091)는 헤더 정보에 따라 프로그램인 경우에는 프로그램 콘텐츠를 프로그램 기억부 (3093)에 기억하고, 데이터인 경우에는 데이터 콘텐츠를 데이터 기억부(3092)에 기억한다. 그 후, 압축 신장 처리부(3094)는 데이터 기억부로부터 데이터를 추출하고, 프로그램 기억부(3093)에 기억한 MP3 프로그램에 따라 신장 처리를 실행하여 출력한다. 또, 프로그램 기억부(3093)에 이미 동일 프로그램이 저장되어 있는 경우에는 프로그램 저장 처리는 생략해도 좋다.

도 64에 도 63의 콘텐츠 구성을 갖는 데이터의 재생 처리의 일례를 나타내는 플로우를 나타낸다. 단계 S675는 AV 처리부(109)의 메모리(3090)에 저장된 데이터명, 예를 들면 음악 데이터의 콘텐츠이면 곡명 등의 정보를 콘텐츠와는 별도로 수령한 정보 또는 콘텐츠 내의 헤더로부터 추출하여 모니터(3002)에 표시한다. 단계 S676은 사용자의 선택을 스위치, 키보드 등의 각종 입력 수단으로부터 입력 인터페이스(110)를 통해 수령한다.

다음으로, 단계 S677에서는 사용자 선택에 대응하는 데이터의 재생용 프로그램(예를 들면, MP3)을 검색한다. 프로그램 검색 대상은 기록 재생기(300)의 액세스 가능한 범위를 최대 검색 범위로 하는 것이 바람직하고, 예를 들면 도 60에 도시한 각 미디어(500), 통신 수단(600), 기록 디바이스(400) 등도 검색 범위로 한다.

AV 처리부(109)에 건네 받는 콘텐츠는 데이터부만이고, 프로그램 콘텐츠는 기록 재생기(300) 내의 다른 기록 매체에 저장되는 경우도 있고, DVD, CD 등의 미디어를 통해 콘텐츠 제공 업자로부터 제공되는 경우도 있다. 따라서, 검색 대상을 기록 재생기(300)의 액세스 저장 범위를 검색 범위로 한다. 검색 결과로서 재생 프로그램이 발견되면, CPU(106)의 제어 하에 사용자 입력 데이터에 기초한 재생 처리 명령을 AV 처리부(109)로 출력한다. AV 처리부(109)는 단계 S679에 있어서 사용자 선택에 의한 데이터의 추출, 신장 처리를 실행한다. 또한, 다른 실시예로서, 프로그램 검색을 단계 S675보다 전에 행하고, 단계 S675에 있어서는 프로그램이 검출된 데이터만을 표시하도록 하여도 좋다.

다음으로, 도 65에 하나의 콘텐츠에 압축 음성 데이터(6303), 신장 처리 프로그램(6302)이 포함되고, 또한 콘텐츠의 헤더 정보(6301)로서 콘텐츠의 재생 우선 순위 정보가 포함되는 구성예를 나타낸다. 이는 앞의 도 61의 콘텐츠 구성에 헤더 정보로서 재생 우선 순위 정보를 부가한 예이다. 이는 상술한 「(14) 콘텐츠 데이터에 있어서의 취급 방침 중의 기동 우선 순위에 기초한 프로그램 기동 처리」와 마찬가지로 AV 처리부(109)가 수령한 콘텐츠 사이에서 설정된 재생 우선 순위에 기초하여 재생 순서를 결정하는 것이다.

도 66에 도 65의 콘텐츠 구성을 갖는 데이터의 재생 처리의 일례를 나타내는 플로우를 나타낸다. 단계 S681은 AV 처리부(109)의 메모리(3090)에 저장된 데이터, 즉 재생 대상 데이터의 데이터 정보를 검색 리스트로 설정한다. 검색 리스트는 AV 처리부(109) 내의 메모리의 일부 영역을 사용하여 설정한다. 다음으로, 단계 S682에 있어서, AV 처리부(109)의 콘텐츠 해석부(3091)에 있어서 검색 리스트로부터 우선 순위가 높은 데이터를 선택하고, 단계 S683에 있어서, 선택된 데이터의 재생 처리를 실행한다.

다음으로, 도 67에 하나의 콘텐츠에 헤더 정보와 프로그램 데이터(6402) 또는 헤더 정보(6403)와, 압축 데이터(6404) 중 어느 조합으로 이루어진 예에 있어서, 데이터 콘텐츠의 헤더(6403)에만, 재생 우선 순위 정보가 부가되어 있는 구성예를 나타낸다.

도 68에 도 67의 콘텐츠 구성을 갖는 데이터의 재생 처리의 일례를 나타내는 플로우를 나타낸다. 단계 S691은 AV 처리부(109)의 메모리(3090)에 저장된 데이터, 즉 재생 대상 데이터의 데이터 정보를 검색 리스트로 설정한다. 검색 리스트는 AV 처리부(109) 내의 메모리의 일부 영역을 사용하여 설정한다. 다음으로, 단계 S692에 있어서, AV 처리부(109)의 콘텐츠 해석부(3091)에 있어서 검색 리스트로부터 우선 순위가 높은 데이터를 선택한다.

다음으로, 단계 S693에서는 선택된 데이터에 대응하는 데이터 재생용 프로그램(예를 들면, MP3)을 검색한다. 프로그램 검색 대상은 앞의 도 64의 플로우에 있어서의 처리와 마찬가지로 기록 재생기(300)의 액세스 저장 범위를 최대 검색 범위로 하는 것이 바람직하고, 예를 들면 도 60에 도시한 각 미디어(500), 통신 수단 (600), 기록 디바이스(400) 등도 검색 범위로 한다.

검색 결과로서 재생 프로그램이 발견되면(단계 S694에서 Yes), 단계 S695에 있어서, 선택된 데이터를 검색 결과 얻어진 프로그램을 이용하여 신장 재생 처리를 실행한다.

한편, 검색 결과로서 프로그램이 검출되지 않은 경우(단계 S694에서 Yes)는 단계 S696으로 진행하고, 단계 S691에서 설정한 검색 리스트 중에 포함되는 다른 데이터에 있어서, 동일한 프로그램을 이용한 재생 처리가 필요한 것을 삭제한다. 이는 새롭게 그 데이터에 대한 재생 프로그램 검색을 실행해도 검출되지 않은 것이 분명하기 때문이다. 또한, 단계 S697에 있어서 검색 리스트가 비어있는 가를 판정하여, 그렇지 않은 경우에는 단계 S692로 되돌아가고, 또한 다음의 우선 순위가 높은 데이터를 추출하여 프로그램 검색 처리를 실행한다.

이와 같이 본 구성에 따르면, 압축 처리된 콘텐츠는 그 복호(신장) 프로그램과 함께 구성되거나, 콘텐츠가 압축된 데이터만 또는 신장 처리 프로그램만인 경우에는 각각의 콘텐츠에 콘텐츠가 어떠한 압축 데이터인지 또는 어떠한 처리를 실행하는지를 나타내는 헤더 정보를 갖고 있기 때문에 콘텐츠를 수령한 처리부(예를 들면, AV 처리부)는 압축 데이터에 부속하는 신장 처리 프로그램을 이용하여 신장 재생 처리를 실행하거나 또는 신장 처리 프로그램을 압축 데이터의 헤더 정보에 기초하여 검색해서, 검색 결과 얻어진 프로그램에 따라 신장 재생 처리를 실행하기 때문에 사용자에 의한 데이터의 신장 프로그램의 선택, 검색 등의 처리가 불필요하게 되고, 사용자 부담이 경감되어 효율적인 데이터 재생이 가능하게 된다. 또한, 헤더에 재생 우선 순위 정보를 갖은 구성에 따르면, 재생 순서를 자동 설정하는 구성이 가능하게 되고, 사용자에 의한 재생 순서 설정의 조작을 생략할 수 있다.

또, 상술한 실시예에서는 압축 음성 데이터 콘텐츠 및 음성 압축 데이터의 신장 처리 프로그램으로서의 MP3을 예로서 설명하였지만, 압축 데이터를 포함하는 콘텐츠, 압축 화상 데이터의 신장 처리 프로그램을 갖는 콘텐츠라도 본 구성은 마찬가지로 적용 가능하고, 동일한 효과를 발휘하는 것이다.

(16) 세이브 데이터의 생성 및 기록 디바이스로의 저장, 재생 처리

본 발명의 데이터 처리 장치는 예를 들면 기록 재생기(300)에 있어서 실행되는 콘텐츠가 게임 프로그램 등인 경우 등, 게임 프로그램을 도중에 중단하여, 소정 시간 후, 새롭게 재개하고자 하는 경우에는 그 중단 시점의 게임 상태 등을 세이브, 즉 기록 디바이스에 저장하고, 이를 재개 시에 판독하여 게임을 속행할 수 있는 구성을 갖는다.

종래의 게임 기기, 퍼스널 컴퓨터 등의 기록 재생기에 있어서의 세이브 데이터 보존 구성은 예를 들면 기록 재생기에 내장 또는 외부 부착 가능한 메모리 카드, 플로피 디스크, 게임 카트리지 또는 하드디스크 등의 기억 매체에 세이브 데이터를 보존하는 구성을 갖지만, 특히 그 세이브 데이터에 대한 시큐러티 확보 구성을 갖고 있지 않으며, 예를 들면 게임 어플리케이션 프로그램에 공통 사양으로 데이터의 세이브 처리가 행해지는 구성으로 되어 있다.

따라서, 예를 들면 어떤 하나의 기록 재생기 A를 이용하여 세이브된 세이브 데이터가 다른 게임 프로그램에 의해 사용되거나, 재기입되거나 하는 사태가 발생하고, 종래 세이브 데이터의 시큐러티는 거의 고려되어 있지 않은 것이 실상이다.

본 발명의 데이터 처리 장치는 이러한 세이브 데이터의 시큐러티 확보를 실현할 수 있는 구성을 제공한다. 예를 들면, 어떤 게임 프로그램의 세이브 데이터는 그 게임 프로그램만이 사용 가능한 정보에 기초하여 암호화해서 기록 디바이스에 저장

한다. 또는, 기록 재생기 고유의 정보에 기초하여 암호화해서 기록 디바이스에 저장한다. 이들 방법에 의해 세이브 데이터의 이용을 특정한 기기, 특정한 프로그램에만 제한할 수 있어서, 세이브 데이터의 시큐러티가 확보된다. 이하, 본 발명의 데이터 처리 장치에서의 「세이브 데이터의 생성 및 기록 디바이스로의 저장, 재생 처리」에 대하여 설명한다.

도 69에 본 발명의 데이터 처리 장치에서의 세이브 데이터 저장 처리에 대하여 설명하는 블록도를 나타낸다. DVD, CD 등의 미디어(500) 또는 통신 수단(600)으로부터 콘텐츠가 기록 재생기(300)에 제공된다. 제공되는 콘텐츠는 앞에서 설명한 바와 같이 콘텐츠 고유의 키인 콘텐츠 키 K_{con}에 의해 암호화되어 있으며, 기록 재생기(300)는 상술한 「(7) 기록 재생기로부터 기록 디바이스로의 다운로드 처리」에서 설명(도 22 참조)한 처리에 따라 콘텐츠 키를 취득하여, 암호화 콘텐츠를 복호한 후, 기록 디바이스(400)에 저장한다. 여기서는 기록 재생기(300)가 콘텐츠 프로그램을 미디어, 통신 수단으로부터 복호하여 재생, 실행을 행하고, 실행 후, 얻어지는 세이브 데이터를 외부 부착 또는 내장의 메모리 카드, 하드디스크 등의 각종 기록 디바이스(400A, 400B, 400C) 중 어느 하나에 저장하고, 재생하는 처리 또는 콘텐츠를 기록 디바이스(400A)에 다운로드한 후, 기록 디바이스(400A)로부터 콘텐츠를 재생, 실행하여 그 세이브 데이터를 외부 부착 또는 내장의 메모리 카드, 하드디스크 등의 각종 기록 디바이스(400A, 400B, 400C) 중 어느 하나에 저장하는 처리 기록 디바이스(400)에 저장하고, 재생하는 처리에 대하여 설명한다.

기록 재생기(300)에는 앞서 설명한 바와 같이 기록 재생기 식별자 ID_{dev}, 시스템에 공통의 서명 키인 시스템 서명 키 K_{sys}, 개개의 기록 재생기에 고유의 서명 키인 기록 재생기 서명 키 K_{dev}, 또한 각종 개별 키를 생성하는 마스터 키를 갖는다. 마스터 키에 대해서는 「(12) 마스터 키에 기초한 암호 처리 키 생성 구성」에서 상세하게 설명한 바와 같이 예를 들면, 배송 키 K_{dis} 또는 인증 키 K_{ake} 등을 생성하는 키이다. 여기서는 특히 마스터 키의 종류를 한정하지 않고 기록 재생기 (300)가 갖는 마스터 키 전반을 대표하는 것으로서 MKx로서 나타낸다. 도 69의 하단에는 세이브 데이터의 암호 키 K_{sav}의 예를 나타내었다. 세이브 데이터 암호 키 K_{sav}는 세이브 데이터를 각종 기록 디바이스(400A～C)에 저장하는 경우의 암호화 처리, 그리고 각종 기록 디바이스(400A～C)로부터 재생할 때의 복호 처리에 이용되는 암호 키이다. 도 70 이하를 이용하여 세이브 데이터의 저장 처리 및 재생 처리의 예를 설명한다.

도 70은 콘텐츠 고유키, 시스템 공통 키 중 어느 하나를 이용하여 세이브 데이터를 기록 디바이스(400A～C) 어느 하나에 저장하는 처리의 플로우 도면이다. 또, 각 플로우에 있어서의 처리는 기록 재생기(300)가 실행하는 처리이고, 각 플로우로 세이브 데이터를 저장하는 기록 디바이스는 내장, 외부 부착 기록 디바이스 (400A～C) 중 어느 하나이면 좋고, 어느 하나에 한정된 것은 아니다.

단계 S701은 콘텐츠 식별자, 예를 들면 게임 ID를 기록 재생기(300)가 판독하는 처리이다. 이는 앞서 설명한 도 4, 26, 27, 32～35에 도시한 콘텐츠 데이터 중의 식별 정보에 포함되는 데이터로서, 세이브 데이터의 저장 처리 명령을 도 2에 도시한 입력 인터페이스(110)를 통해 수령한 메인 CPU(106)가 콘텐츠 식별자의 판독을 제어부(301)에 지시한다.

제어부(301)는 실행 프로그램이 DVD, CD-ROM 등, 판독부(304)를 통해 실행되고 있는 콘텐츠인 경우에는 판독부(304)를 통해 콘텐츠 데이터 중의 헤더에 포함되는 식별 정보를 추출하고, 실행 프로그램이 기록 디바이스(400)에 저장된 콘텐츠인 경우에는 기록 디바이스 컨트롤러(303)를 통해 식별 정보를 추출한다. 또, 기록 재생기(300)가 콘텐츠 프로그램을 실행 중, 이미 기록 재생기 중인 RAM, 그 밖의 액세스 가능한 기록 매체에 콘텐츠 식별자가 저장 종료된 경우에는 새로운 판독 처리를 실행하지 않고, 판독 종료된 데이터에 포함되는 식별 정보를 이용해도 좋다.

다음으로, 단계 S702는 프로그램의 사용 제한을 행하는지의 여부에 의해 처리를 변경하는 단계이다. 프로그램 사용 제한은, 보존하는 세이브 데이터를 그 프로그램에만 고유하게 이용 가능한 제한을 붙이는지의 여부를 설정하는 제한 정보로서, 프로그램에만 고유하게 이용 가능한 경우에는 「프로그램 사용 제한 있음」으로 하고, 프로그램에 이용을 구속받지 않은 세이브 데이터로 하는 경우를 「프로그램 사용 제한 없음」으로 한다. 이는 사용자가 임의로 설정할 수 있도록 해도 좋고, 콘텐츠 제작자가 설정하여 이 정보를 콘텐츠 프로그램 중에 저장해 두어도 좋고, 설정된 제한 정보는 도 69의 기록 디바이스(400A～C)에 데이터 관리 파일로서 저장된다.

데이터 관리 파일의 예를 도 71에 도시한다. 데이터 관리 파일은 항목으로서 데이터 번호, 콘텐츠 식별자, 기록 재생기 식별자, 프로그램 사용 제한을 포함하는 테이블로서 생성된다. 콘텐츠 식별자는 세이브 데이터를 저장하는 대상이 된 콘텐츠 프로그램의 식별 데이터이다. 기록 재생기 식별자는 세이브 데이터를 저장한 기록 재생기의 식별자, 예를 들면 도 69에 도시한 [ID_{dev}]이다. 프로그램 사용 제한은 상술한 바와 같이 보존하는 세이브 데이터를 그 프로그램에만 고유하게 이용 가

능한 경우, 「한다」의 설정으로 하고, 대응 프로그램에 제한되지 않은 이용을 가능한 경우 「하지 않는다」의 설정이 된다. 프로그램 사용 제한은 콘텐츠 프로그램을 이용하는 사용자가 임의로 설정할 수 있도록 해도 좋고, 콘텐츠 제작자가 설정하여 이 정보를 콘텐츠 프로그램 중에 저장해 두어도 좋다.

도 70으로 되돌아가 플로우의 설명을 계속한다. 단계 S702에 있어서, 프로그램 사용 제한에 대하여 「한다」의 설정이 되어 있는 경우에는 단계 S703으로 진행한다. 단계 S703에서는 콘텐츠 데이터로부터 콘텐츠 고유의 키, 예를 들면 앞서 설명한 콘텐츠 키 K_{con}을 판독하여 콘텐츠 고유 키를 세이브 데이터 암호 키 K_{sav}로 하거나 콘텐츠 고유 키에 기초하여 세이브 데이터 암호 키 K_{sav}를 생성한다.

한편, 단계 S702에 있어서, 프로그램 사용 제한에 대하여 「하지 않는다」의 설정이 되어 있는 경우에는 단계 S707로 진행한다. 단계 S707에서는 기록 재생기 (300) 내에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 기록 재생기 (300)의 내부 메모리(307)로부터 판독하여, 시스템 서명 키 K_{sys}를 세이브 데이터 암호 키 K_{sav}로 하거나 시스템 서명 키에 기초하여 세이브 데이터 암호 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로서 사용해도 좋다.

다음으로, 단계 S704에 있어서, 단계 S703 또는 단계 S707에서 선택 또는 생성된 세이브 데이터 암호화 키 K_{sav}를 이용하여 세이브 데이터의 암호화 처리를 실행한다. 암호화 처리는 도 2에 있어서의 암호 처리부(302)가 예를 들면 상술한 DES 알고리즘을 적용하여 실행한다.

단계 S704에 있어서 암호화 처리된 세이브 데이터는 단계 S705에 있어서 기록 디바이스에 저장된다. 세이브 데이터를 저장 가능한 기록 디바이스가 도 69에 도시한 바와 같이 복수 있는 경우에는 사용자가 기록 디바이스(400A～C) 중 어느 하나를 세이브 데이터 저장처로서 사전에 선택한다. 또한, 단계 S706에 있어서 앞서 도 71을 이용하여 설명한 데이터 관리 파일에 먼저 단계 S702에서 설정한 프로그램 사용 제한 정보의 기입, 즉 프로그램 사용 제한 「한다」 또는 「하지 않는다」의 기입을 실행한다.

이상으로, 세이브 데이터의 저장 처리가 종료한다. 단계 S702에 있어서 Yes, 즉 「프로그램 사용 제한한다」의 선택이 이루어지고, 단계 S703에 있어서 콘텐츠 고유 키에 기초하여 생성된 세이브 데이터 암호화 키 K_{sav}에 의해 암호화 처리된 세이브 데이터는 콘텐츠 고유 키 정보를 갖지 않은 콘텐츠 프로그램에 의한 복호 처리가 불가능하게 되고, 세이브 데이터는 동일한 콘텐츠 키 정보를 갖는 콘텐츠 프로그램만이 이용할 수 있게 된다. 단, 여기서는 세이브 데이터 암호화 키 K_{sav}는 기록 재생기 고유의 정보에 기인하여 생성된 것이 아니므로, 예를 들면 메모리 카드 등의 착탈 가능한 기록 디바이스에 저장된 세이브 데이터는 다른 기록 재생기에 있어서도 대응하는 콘텐츠 프로그램과 함께 사용하는 한 재생 가능하게 된다.

또한, 단계 S702에 있어서 No, 즉 「프로그램 사용 제한하지 않는다」의 선택이 이루어지고, 단계 S707에 있어서 시스템 공통 키에 기초한 세이브 데이터 암호화 키 K_{sav}에 의해 암호화 처리된 세이브 데이터는 콘텐츠 식별자가 다른 프로그램을 이용한 경우라도, 또한 기록 재생기가 다른 경우라도 재생하여 이용할 수 있다.

도 72는 도 70의 세이브 데이터 저장 처리에 의해 저장된 세이브 데이터를 재생하는 처리를 나타낸 플로우이다.

단계 S711은 콘텐츠 식별자, 예를 들면 게임 ID를 기록 재생기(300)가 판독하는 처리이다. 이는 앞서 설명한 도 70의 세이브 데이터 저장 처리의 단계 S701과 동일한 처리이고, 콘텐츠 데이터 중의 식별 정보에 포함되는 데이터를 판독하는 처리이다.

다음으로, 단계 S712에서는 도 69에 도시한 기록 디바이스(400A～C)로부터 도 71을 이용하여 설명한 데이터 관리 파일을 판독하고, 단계 S711에 있어서 판독한 콘텐츠 식별자 및 대응하여 설정된 사용 프로그램 제한 정보를 추출한다. 데이터 관리 파일에 설정된 프로그램 사용 제한이 「한다」인 경우에는 단계 S714로 진행하고, 「하지 않는다」인 경우에는 단계 S717로 진행한다.

단계 S714에서는 콘텐츠 데이터로부터 콘텐츠 고유의 키, 예를 들면 앞서 설명한 콘텐츠 키 K_{con}을 판독하여 콘텐츠 고유 키를 세이브 데이터 복호화 키 K_{sav}로 하거나 콘텐츠 고유 키에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 이 복

호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 어떤 콘텐츠 고유 키에 기초하여 암호화된 데이터는 동일한 콘텐츠 고유 키에 기초하여 생성된 복호 키에 의해 복호 가능한 것이 되는 복호화 키 생성 알고리즘이 적용된다.

한편, 단계 S712에 있어서, 데이터 관리 파일의 설정이 프로그램 사용 제한에 대하여 「하지 않는다」의 설정인 경우에는 단계 S717에 있어서, 기록 재생기 (300) 내에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 기록 재생기 (300)의 내부 메모리(307)로부터 판독하여, 시스템 서명 키 K_{sys}를 세이브 데이터 복호화 키 K_{sav}로 하거나 시스템 서명 키에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로서 사용해도 좋다.

다음으로, 단계 S715에 있어서, 단계 S714 또는 단계 S717에서 선택 또는 생성된 세이브 데이터 복호화 키 K_{sav}를 이용하여 세이브 데이터의 복호화 처리를 실행하고, 단계 S716에 있어서, 복호된 세이브 데이터를 기록 재생기(300)에 있어서 재생, 실행한다.

이상으로, 세이브 데이터의 재생 처리가 종료한다. 상술된 바와 같이 데이터 관리 파일에 「프로그램 사용 제한한다」의 설정이 이루어져 있는 경우에는 콘텐츠 고유 키에 기초하여 세이브 데이터 복호화 키가 생성되고, 「프로그램 사용 제한하지 않음」의 설정이 있는 경우에는 시스템 공통 키에 기초하여 세이브 데이터 복호화 키가 생성된다. 「프로그램 사용 제한한다」의 설정이 되어 있는 경우, 사용하고 있는 콘텐츠의 콘텐츠 식별자가 동일한 것이 아니면 세이브 데이터의 복호 처리가 가능한 복호화 키를 얻을 수 없는 것이 되어, 세이브 데이터의 시큐러티를 높일 수 있다.

도 73, 도 74는 콘텐츠 식별자를 이용하여 세이브 데이터의 암호화 키, 복호화 키를 생성하는 세이브 데이터 저장 처리 플로우(도 73), 세이브 데이터 재생 처리 플로우(도 74)이다.

도 73에 있어서, 단계 S721～S722는 도 70의 단계 S701 ～S702와 동일한 처리이고, 설명을 생략한다.

도 73의 세이브 데이터 저장 처리 플로우는 단계 S722에 있어서 「프로그램 사용 제한한다」의 설정을 행한 경우, 단계 S723에 있어서 콘텐츠 데이터로부터 콘텐츠 식별자, 즉 콘텐츠 ID를 판독하여 콘텐츠 ID를 세이브 데이터 암호화 키 K_{sav}로 하거나, 콘텐츠 ID에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 예를 들면, 기록 재생기(300)의 암호 처리부(307)는 콘텐츠 데이터로부터 판독한 콘텐츠 ID에 기록 재생기(300)의 내부 메모리에 저장된 마스터 키 MKx를 적용하여, 예를 들면 DES(MKx, 콘텐츠 ID)에 의해 세이브 데이터 암호화 키 K_{sav}를 얻을 수 있다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로서 사용해도 좋다.

한편, 단계 S722에 있어서, 프로그램 사용 제한에 대하여 「하지 않는다」의 설정으로 한 경우에는 단계 S727에 있어서, 기록 재생기(300) 내에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 기록 재생기(300)의 내부 메모리(307)로부터 판독하여, 시스템 서명 키 K_{sys}를 세이브 데이터 암호화 키 K_{sav}로 하거나 시스템 서명 키에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로서 사용해도 좋다.

단계 S724 이하의 처리는 상술한 도 70의 처리 플로우에 있어서의 단계 S704 이하의 처리와 동일하므로, 설명을 생략한다.

또한, 도 74는 도 73의 세이브 데이터 저장 처리 플로우로 기록 디바이스에 저장된 세이브 데이터를 재생, 실행하는 처리 플로우이고, 단계 S731～S733은 상술한 도 72의 대응 처리와 동일하고, 단계 S734만이 다르다. 단계 S734에 있어서는 콘텐츠 데이터로부터 콘텐츠 식별자, 즉 콘텐츠 ID를 판독하여 콘텐츠 ID를 세이브 데이터 복호화 키 K_{sav}로 하거나, 콘텐츠 ID에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 복호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 어떤 콘텐츠 식별자에 기초하여 암호화된 데이터는 동일한 콘텐츠 식별자에 기초하여 생성된 복호 키에 의해 복호 가능한 것이 되는 복호화 키 생성 알고리즘이 적용된다.

이하의 처리, 단계 S735, S736, S737은 도 72의 대응 처리와 동일하므로, 설명을 생략한다. 도 73, 도 74의 세이브 데이터 저장 및 재생 처리에 따르면, 프로그램 사용 제한하는 설정을 행한 경우, 콘텐츠 ID를 사용하여 세이브 데이터 암호화 키, 복호화 키를 생성하는 구성으로 하였기 때문에 앞의 콘텐츠 고유 키를 사용한 세이브 데이터 저장, 재생 처리와 마찬가지로 대응하는 콘텐츠 프로그램이 정합하는 경우 이외는 세이브 데이터를 이용할 수 없는 구성이 되어, 세이브 데이터 시큐러티를 높인 보존이 가능하게 된다.

도 75, 도 77은 기록 재생기 고유 키를 이용하여 세이브 데이터의 암호화 키, 복호화 키를 생성하는 세이브 데이터 저장 처리 플로우(도 75), 세이브 데이터 재생 처리 플로우(도 77)이다.

도 75에 있어서, 단계 S741은 도 70의 단계 S701과 동일한 처리이므로, 설명을 생략한다. 단계 S742는 기록 재생기의 제한 여부를 설정하는 단계이다. 기록 재생기 제한은 세이브 데이터를 이용 가능한 기록 재생기를 한정하는 경우, 즉 세이브 데이터를 생성하여 저장한 기록 재생기에만 이용 가능한 경우를 「한다」로 설정하고, 다른 기록 재생기라도 이용 가능한 경우를 「하지 않는다」의 설정으로 하는 것이다. 단계 S742에 있어서 「기록 재생기 제한한다」의 설정을 하면, 단계 S743으로 진행하고, 「하지 않는다」의 설정을 하면 단계 S747로 진행한다.

데이터 관리 파일의 예를 도 76에 도시한다. 데이터 관리 파일은 항목으로서 데이터 번호, 콘텐츠 식별자, 기록 재생기 식별자, 기록 재생기 제한을 포함하는 테이블로서 생성된다. 콘텐츠 식별자는 세이브 데이터를 저장하는 대상이 된 콘텐츠 프로그램의 식별 데이터이다. 기록 재생기 식별자는 세이브 데이터를 저장한 기록 재생기의 식별자, 예를 들면 도 69에 도시한 [ID_{dev}]이다. 기록 재생기 제한은 세이브 데이터를 이용 가능한 기록 재생기를 한정하는 경우, 즉 세이브 데이터를 생성하여 저장한 기록 재생기에만 이용 가능한 경우를 「한다」고 설정하고, 다른 기록 재생기라도 이용 가능한 경우를 「하지 않는다」의 설정으로 하는 것이다. 기록 재생기 제한 정보는 콘텐츠 프로그램을 이용하는 사용자가 임의로 설정할 수 있도록 해도 좋고, 콘텐츠 제작자가 설정하여 이 정보를 콘텐츠 프로그램 중에 저장해 두어도 좋다.

도 75의 세이브 데이터 저장 처리 플로우에 있어서는 단계 S742에 있어서 「기록 재생기 제한한다」의 설정을 행한 경우, 단계 S743에 있어서 기록 재생기 (300)로부터 기록 재생기 고유 키, 예를 들면 기록 재생기 서명 키 K_{dev}를 기록 재생기 (300)의 내부 메모리(307)로부터 판독하여 기록 재생기 서명 키 K_{dev}를 세이브 데이터 암호화 키 K_{sav}로 하거나, 기록 재생기 서명 키 K_{dev}에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

한편, 단계 S742에 있어서, 기록 재생기 제한에 대하여 「하지 않는다」의 설정으로 한 경우에는 단계 S747에 있어서, 기록 재생기(300) 내에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 기록 재생기(300)의 내부 메모리(307)로부터 판독하여, 시스템 서명 키 K_{sys}를 세이브 데이터 암호화 키 K_{sav}로 하거나, 시스템 서명 키에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

단계 S744, S745의 처리는 상술한 도 70의 처리 플로우에 있어서의 대응 처리와 동일하므로, 설명을 생략한다.

단계 S746에서는 데이터 관리 파일(도 76 참조)에 콘텐츠 식별자, 기록 재생기 식별자, 그리고 단계 742에서 사용자가 설정한 기록 재생기 제한 정보 「한다/하지 않는다」를 기입한다.

또한, 도 77은 도 75의 세이브 데이터 저장 처리 플로우로 기록 디바이스에 저장된 세이브 데이터를 재생, 실행하는 처리 플로우이고, 단계 S751은 상술한 도 72의 대응 처리와 마찬가지로 콘텐츠 식별자를 판독한다. 다음으로, 단계 S752에 있어서는 기록 재생기(300) 내의 메모리에 저장된 기록 재생기 식별자(ID_{dev})를 판독한다.

단계 S753에서는 데이터 관리 파일(도 76 참조)로부터 콘텐츠 식별자, 기록 재생기 식별자, 설정 완료된 기록 재생기 제한 정보 「한다/하지 않는다」의 각 정보를 판독한다. 데이터 관리 파일 중의 콘텐츠 식별자가 일치하는 엔트리에 있어서, 기록 재생기 제한 정보가 「한다」로 설정되어 있는 경우, 테이블 엔트리의 기록 재생기 식별자가 단계 S752에서 판독된 기록 재생기 식별자와 다른 경우에는 처리를 종료한다.

다음으로, 단계 S754에서 데이터 관리 파일의 설정이 「기록 재생기 제한한다」인 경우에는 단계 S755로 진행하고, 「하지 않는다」인 경우에는 단계 S758로 진행한다.

단계 S755에 있어서는 기록 재생기(300)로부터 기록 재생기 고유 키, 예를 들면 기록 재생기 서명 키 K_{dev}를 기록 재생기(300)의 내부 메모리(307)로부터 판독하여 기록 재생기 서명 키 K_{dev}를 세이브 데이터 복호화 키 K_{sav}로 하거나 기록 재생기 서명 키 K_{dev}에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 복호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 어떤 기록 재생기 고유 키에 기초하여 암호화된 데이터는 동일한 기록 재생기 고유 키에 기초하여 생성된 복호 키에 의해 복호 가능한 것이 되는 복호화 키 생성 알고리즘이 적용된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

한편 단계 S758에 있어서는 기록 재생기(300) 내에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 기록 재생기(300)의 내부 메모리(307)로부터 판독하여 시스템 서명 키 K_{sys}를 세이브 데이터 복호화 키 K_{sav}로 하거나, 시스템 서명 키에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기 (300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다. 이하의 단계 S756, S757은 상술한 세이브 데이터 재생 처리 플로우의 대응 단계와 동일한 처리이다.

도 75, 도 77에 도시한 세이브 데이터 저장, 재생 처리 플로우에 따르면, 「기록 재생기 제한한다」의 선택이 이루어진 세이브 데이터는 기록 재생기 고유 키에 의해 암호화, 복호화 처리가 실행되기 때문에, 동일한 기록 재생기 고유키를 갖는 기록 재생기, 즉 동일한 기록 재생기에 의해서만 복호하여 이용할 수 있다.

다음으로, 도 78, 도 79에 기록 재생기 식별자를 이용하여 세이브 데이터의 암호화, 복호화 키를 생성하여 저장, 재생하는 처리 플로우를 나타낸다.

도 78은 기록 재생기 식별자를 이용하여 세이브 데이터의 암호화를 행하여 기록 디바이스에 저장한다. 단계 S761～S763은 앞의 도 75와 동일한 처리이다. 단계 S764에서는 기록 재생기로부터 판독한 기록 재생기 식별자(ID_{dev})를 이용하여 세이브 데이터의 암호화 키 K_{sav}를 생성한다. ID_{dev}를 세이브 데이터 암호화 키 K_{sav}로서 적용하거나, 또는 기록 재생기(300)의 내부 메모리에 저장된 마스터 키 MKx를 적용하여, DES(MKx, ID_{dev})에 의해 세이브 데이터 암호화 키 K_{sav}를 얻는 등, ID_{dev}에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기 (300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

이하의 처리 단계 S765～S768은 상술한 도 75의 대응 처리와 동일하므로, 설명을 생략한다.

도 79는 도 78의 처리에 의해 기록 디바이스에 저장된 세이브 데이터를 재생, 실행하는 처리 플로우이다. 단계 S771～S774는 상술한 도 77의 대응 처리와 동일하다.

단계 S775에서는 기록 재생기로부터 판독한 기록 재생기 식별자(ID_{dev})를 이용하여 세이브 데이터의 복호화 키 K_{sav}를 생성한다. ID_{dev}를 세이브 데이터 복호화 키 K_{sav}로서 적용하거나, 기록 재생기(300)의 내부 메모리에 저장된 마스터 키 MKx를 적용하여, DES(MKx, ID_{dev})에 의해 세이브 데이터 복호화 키 K_{sav}를 얻는 등, ID_{dev}에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 복호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 어떤 기록 재생기 식별자에 기초하여 암호화된 데이터는 동일한 기록 재생기 식별자에 기초하여 생성된 복호 키에 의해 복호 가능한 것이 되는 복호화 키 생성 알고리즘이 적용된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

이하의 처리 단계 S776～S778은 상술한 도 76의 대응 단계의 처리와 동일하다.

도 78, 도 79에 도시한 세이브 데이터 저장, 재생 처리 플로우에 따르면, 「기록 재생기 제한한다」의 선택이 이루어진 세이브 데이터는 기록 재생기 식별자에 의해 암호화, 복호화 처리가 실행되기 때문에, 동일한 기록 재생기 식별자를 갖는 기록 재생기, 즉 동일한 기록 재생기에 의해서만 복호하여 이용할 수 있다.

다음으로, 도 80~82를 이용하여 상술한 프로그램 사용 제한 및 기록 재생기 사용 제한을 더불어 실행하는 세이브 데이터 저장, 재생 처리에 대하여 설명한다.

도 80은 세이브 데이터 저장 처리 플로우이다. 단계 S781에 있어서, 콘텐츠 식별자를 콘텐츠 데이터로부터 판독하고, 단계 S782에 있어서, 프로그램 사용 제한 판정을 행하고, 단계 S783에 있어서 기록 재생기 제한 판정을 행한다.

「프로그램 사용 제한있음」이고, 「기록 재생기 제한있음」인 경우에는 단계 S785에 있어서, 콘텐츠 고유 키(ex. K_{con})와, 기록 재생기 고유 키(K_{dev})의 쌍방에 기초하여 세이브 데이터 암호화 키 K_{sav}가 생성된다. 이는 예를 들면 K_{sav}=(K_{con} XOR K_{dev}) 또는 기록 재생기(300)의 내부 메모리에 저장된 마스터 키 MKx를 적용하여 K_{sav} =DES(MKx, K_{con} XOR K_{dev}) 등에 의해 얻을 수 있다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

「프로그램 사용 제한있음」이고, 「기록 재생기 제한없음」인 경우에는 단계 S786에 있어서, 콘텐츠 고유 키(ex. K_{con})를 세이브 데이터 암호화 키 K_{sav}로 하거나, 콘텐츠 고유 키(ex. K_{con})에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다.

「프로그램 사용 제한없음」이고, 「기록 재생기 제한있음」인 경우에는 단계 S787에 있어서, 기록 재생기 고유 키(K_{dev})를 세이브 데이터 암호화 키 K_{sav}로 하거나, 기록 재생기 고유 키(K_{dev})에 기초하여 세이브 데이터 암호화 키 K_{sav}가 생성된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

또한, 「프로그램 사용 제한없음」이고, 「기록 재생기 제한없음」인 경우에는 단계 S787에 있어서, 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 세이브 데이터 암호화 키 K_{sav}로 하거나, 시스템 서명 키 K_{sys}에 기초하여 세이브 데이터 암호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

단계 S789에서는 단계 S785~S788 중 어느 하나로 생성된 세이브 데이터 암호화 키 K_{sav}에 의해 세이브 데이터가 암호화되어, 기록 디바이스에 저장된다.

또한, 단계 S790에서는 단계 S782, S783에 있어서 설정한 제한 정보가 데이터 관리 파일에 저장된다. 데이터 관리 파일은 예를 들면 도 81에 도시한 구성이 되어, 항목으로서 데이터 번호, 콘텐츠 식별자, 기록 재생기 식별자, 프로그램 사용 제한, 기록 재생기 제한을 포함한다.

도 82는 도 80의 처리에 의해 기록 디바이스에 저장된 세이브 데이터를 재생, 실행하는 처리 플로우이다. 단계 S791에서는 실행 프로그램의 콘텐츠 식별자, 기록 재생기 식별자를 판독하고, 단계 S792에 있어서, 도 81에 도시한 데이터 관리 파일로부터 콘텐츠 식별자, 기록 재생기 식별자, 프로그램 사용 제한, 기록 재생기 제한 정보를 판독한다. 이 경우, 프로그램 사용 제한이 「한다」로 콘텐츠 식별자가 불일치인 경우 또는 기록 재생기 제한 정보가 「한다」로 기록 재생기 식별자가 불일치인 경우에는 처리를 종료한다.

다음으로, 단계 S793, S794, S795에서는 데이터 관리 파일의 기록 데이터에 따라 복호 키 생성 처리를 단계 S796~S799의 네가지 형태 중 어느 하나로 설정한다.

「프로그램 사용 제한있음」이고, 「기록 재생기 제한있음」인 경우에는 단계 S796에 있어서, 콘텐츠 고유 키(ex. K_{con})와 기록 재생기 고유 키(K_{dev})의 쌍방에 기초하여 세이브 데이터 복호화 키 K_{sav}가 생성된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다. 「프로그램 사용 제한있음」이고, 「기록 재생기 제한없음」인 경우에는 단계 S797에 있어서, 콘텐츠 고유 키(ex. K_{con})를 세이

브 데이터 복호화 키 K_{sav}로 하거나, 콘텐츠 고유 키(ex. K_{con})에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

「프로그램 사용 제한없음」이고, 「기록 재생기 제한있음」인 경우에는 단계 S798에 있어서, 기록 재생기 고유 키(K_{dev})를 세이브 데이터 복호화 키 K_{sav}로 하거나, 기록 재생기 고유 키(K_{dev})에 기초하여 세이브 데이터 복호화 키 K_{sav}가 생성된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다. 또한, 「프로그램 사용 제한없음」이고, 「기록 재생기 제한없음」인 경우에는 단계 S799에 있어서, 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 세이브 데이터 복호화 키 K_{sav}로 하거나, 시스템 서명 키 K_{sys}에 기초하여 세이브 데이터 복호화 키 K_{sav}를 생성한다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

이들 복호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 동일한 콘텐츠 고유 키, 기록 재생기 고유 키에 기초하여 암호화된 데이터는 동일한 콘텐츠 고유 키, 기록 재생기 고유 키에 기초하여 생성된 복호 키에 의해 복호 가능한 것이 되는 복호화 키 생성 알고리즘이 적용된다.

단계 S800에서는 상술한 단계 S796~S799 중 어느 하나에 있어서 생성된 세이브 데이터 복호화 키를 이용하여 복호 처리가 실행되고, 복호 세이브 데이터가 기록 재생기(300)에 있어서 재생, 실행된다.

도 80, 82에 있어서 나타낸 세이브 데이터 저장, 재생 처리 플로우에 따르면, 「프로그램 사용 제한한다」의 선택이 이루어진 세이브 데이터는 콘텐츠 고유 키에 의해 암호화, 복호화 처리가 실행되기 때문에, 동일한 콘텐츠 고유 키를 갖는 콘텐츠 데이터를 사용하는 경우만 복호하여 이용할 수 있다. 또, 「기록 재생기 제한한다」의 선택이 이루어진 세이브 데이터는 기록 재생기 식별자에 의해 암호화, 복호화 처리가 실행되기 때문에, 동일한 기록 재생기 식별자를 갖는 기록 재생기, 즉 동일한 기록 재생기에 의해서만 복호하여 이용할 수 있다. 따라서, 콘텐츠, 기록 재생기 양자에 의해 이용 제한을 설정할 수 있고, 세이브 데이터의 시큐러티를 더욱 높일 수 있다.

또, 도 80, 82에 있어서는 콘텐츠 고유 키, 기록 재생기 고유키를 이용한 세이브 데이터 암호화 키, 복호화 키의 생성 구성을 나타내었지만, 콘텐츠 고유키 대신에 콘텐츠 식별자, 또한 기록 재생기 고유 키 대신에 기록 재생기 식별자를 이용하여 이들 식별자에 기초하여 세이브 데이터 암호화 키, 복호화 키의 생성을 실행하는 구성으로 해도 좋다.

다음으로, 도 83~85를 이용하여 사용자가 입력한 패스워드에 기초하여 세이브 데이터의 암호화 키, 복호화 키를 생성하는 구성에 대하여 설명한다.

도 83은 사용자가 입력한 패스워드에 기초하여 세이브 데이터의 암호화 키를 생성하여 기록 디바이스에 저장하는 처리 플로우이다.

단계 S821은 콘텐츠 데이터로부터 콘텐츠 식별자를 판독하는 처리로서, 상술한 각 처리와 동일하다. 단계 S822는 사용자에 의한 프로그램 사용 제한의 설정 여부를 결정하는 단계이다. 본 구성에 있어서 설정되는 데이터 관리 파일은 예를 들면 도 84에 도시한 구성을 갖는다.

도 84에 도시한 바와 같이 데이터는 데이터 번호, 콘텐츠 식별자, 기록 재생기 식별자, 또한 사용자에 의한 프로그램 사용 제한 정보가 포함된다. 「사용자에 의한 프로그램 사용 제한 정보」는 프로그램을 사용하는 사용자 제한 여부를 설정하는 항목이다.

도 83에 있어서의 처리 플로우에 있어서의 단계 S822에 있어서 사용 제한하는 설정이 이루어지면, 단계 S823에 있어서 사용자 패스워드의 입력이 이루어진다. 이 입력은 도 2에 도시한 예를 들면 키보드 등의 입력 수단으로부터 입력된다.

입력된 패스워드는 메인 CPU(106), 제어부(301)의 제어 하에 암호 처리부 (302)로 출력되고, 단계 S824에 있어서의 처리, 즉 입력 사용자 패스워드에 기초한 세이브 데이터 암호화 키 K_{sav}가 생성된다. 세이브 데이터 암호화 키 K_{sav} 생성 처

리로서는 예를 들면 패스워드 자체를 암호화 키 K_{sav}로 해도 좋거나, 기록 재생기의 마스터 키 MKx를 이용하여 세이브 데이터 암호화 키 K_{sav}=DES(MKx, 패스워드)에 의해 생성해도 좋다. 또한, 패스워드를 입력으로서 일방향성 함수를 적용하여 그 출력에 기초하여 암호화 키를 생성해도 좋다.

단계 S822에 있어서의 사용자 제한이 No라고 되어 있는 경우에는 단계 S828에 있어서, 기록 재생기(300)의 시스템 공통 키에 기초하여 세이브 데이터 암호화 키가 생성된다.

또한, 단계 S825에서 단계 S824 또는 단계 S828에서 생성된 세이브 데이터 암호화 키 K_{sav}를 이용하여 세이브 데이터의 암호화 처리가 이루어지고, 단계 S826에 있어서 암호화 처리가 이루어진 세이브 데이터가 기록 디바이스에 저장된다.

또한, 단계 S827에 있어서, 도 84의 데이터 관리 파일에 단계 S822에서 설정한 사용자에 의한 프로그램 사용 제한 정보가 콘텐츠 식별자와 기록 재생기 식별자에 대응되어 기입된다.

도 85는 도 83의 처리에 의해 저장된 세이브 데이터의 재생 처리 플로우를 나타낸 도면이다. 단계 S831에 있어서, 콘텐츠 데이터로부터 콘텐츠 식별자를 판독하고, 단계 S832에 있어서 도 84에 도시한 데이터 관리 파일로부터 콘텐츠 식별자, 사용자에 의한 프로그램 사용 제한 정보를 판독한다.

단계 S833에 있어서, 데이터 관리 파일 중의 데이터에 기초한 판정을 실행하여, 「사용자에 의한 프로그램 사용 제한한다」가 설정되어 있는 경우에는 단계 S834에 있어서, 패스워드 입력을 구하고, 단계 S835에 있어서, 입력 패스워드에 기초한 복호화 키를 생성한다. 이 복호화 키 생성 처리는 암호화 키 생성 처리에 대응하는 처리 알고리즘이 적용되고, 어떤 패스워드에 기초하여 암호화된 데이터는 동일한 패스워드에 기초하여 생성된 복호 키에 의해 복호 가능하게 되는 복호화 키 생성 알고리즘에 설정된다.

단계 S833의 판정이 사용자에 의한 프로그램 사용 제한 없음인 경우에는 단계 S837에 있어서 기록 재생기(300)의 내부 메모리에 저장된 시스템 공통 키, 예를 들면 시스템 서명 키 K_{sys}를 이용하여 세이브 데이터 복호 키 K_{sav}가 생성된다. 또는 별도로, 기록 재생기(300)의 내부 메모리(307) 내에 보존해 둔 다른 키는 다른 암호 키를 세이브 데이터 암호 키 K_{sav}로 사용해도 좋다.

단계 S836에서는 단계 S835, 단계 S837 중 어느 하나에 있어서 생성된 복호화 키 K_{sav}를 이용하여 기록 디바이스에 저장된 세이브 데이터의 복호가 실행되고, 단계 S836에 있어서 기록 재생기에서 세이브 데이터의 재생, 실행이 이루어진다.

도 83, 도 85에 있어서 도시한 세이브 데이터 저장, 재생 처리 플로우에 따르면, 「사용자에 의한 프로그램 사용 제한한다」의 선택이 이루어진 세이브 데이터는 사용자 입력 패스워드에 기초한 키에 의해 암호화, 복호화 처리가 실행되기 때문에, 동일한 패스워드를 입력한 경우만 복호하여 이용할 수 있으며, 세이브 데이터의 시큐러티를 높일 수 있다.

이상, 몇 개의 세이브 데이터의 저장 처리, 재생 처리 형태에 대하여 설명하였지만, 상술한 처리를 융합한 처리, 예를 들면 패스워드와, 기록 재생기 식별자, 콘텐츠 식별자 등을 임의로 조합하여 사용해서 세이브 데이터 암호화 키, 복호화 키를 생성하는 형태도 가능하다.

(17) 부정 기기의 배제(폐지) 구성

이미 설명한 바와 같이 본 발명의 데이터 처리 장치에서는 미디어(500: 도 3 참조), 통신 수단(600)으로부터 제공된 여러 가지 콘텐츠 데이터를 기록 재생기 (300)에 있어서, 인증, 암호화 처리 등을 실행하고, 기록 디바이스에 저장하는 구성에 의해 제공 콘텐츠의 시큐러티를 높임과 함께, 또한 정당한 이용자만이 이용 할 수 있는 구성을 갖는다.

상술한 설명에서 알 수 있는 바와 같이 입력 콘텐츠는 기록 재생기(300)의 암호 처리부(302)에 구성되는 내부 메모리(307)에 저장된 여러가지 서명 키, 마스터 키, 체크치 생성 키(도 18 참조)를 이용하여 인증 처리, 암호화 처리, 복호화 처리가 이루어진다. 이 키 정보를 저장하는 내부 메모리(307)는 앞서 설명한 바와 같이 기본적으로 외부로부터 액세스하기 어려운 구조를 갖은 반도체 칩으로 구성되고, 다층 구조를 구비하며, 그 내부의 메모리는 알루미늄층 등의 더미층에 끼워지거나, 최하층에 구성되고, 또한 동작하는 전압 또는/또한 주파수의 폭이 좁다는 등, 외부로부터 부정하게 데이터의 판독

이 어려운 특성으로 한 구성이 되는 것이 바람직하지만, 만일 내부 메모리가 부정한 판독이 실행되어, 이들 키 데이터 등이 유출하여, 정규 라이센스가 되어 있지 않은 기록 재생기에 복사된 경우, 복사된 키 정보에 의해 부정한 콘텐츠 이용이 이루어질 가능성이 있다.

여기서는 이들 부정 복사에 의한 키의 복제에 의한 콘텐츠의 부정 이용을 방지하는 구성에 대하여 설명한다.

도 86에 본 구성 「(17) 부정 기기의 배제 구성」을 설명하는 블록도를 나타낸다. 기록 재생기(300)는 상술한 도 2, 3에 도시한 기록 재생기와 동일하고, 내부 메모리를 구비하고, 앞서 설명한(도 18) 각종 키 데이터, 또한 기록 재생기 식별자를 갖고 있다. 또, 여기서는 제3자에 의해 복제되어 있는 기록 재생기 식별자, 키 데이터 등은 도 3에 도시한 내부 메모리(307)에 저장된다고는 한하지 않고, 도 86에 도시한 기록 재생기(300)의 키 데이터 등은 암호 처리부(302: 도 2, 3 참조)에 의해 액세스 가능한 메모리부에 통합 또는 분산 저장되어 있는 구성으로 한다.

부정 기기의 배제 구성을 실현하기 위해서, 콘텐츠 데이터의 헤더부가 부정한 기록 재생기 식별자 리스트를 기억한 구성으로 하였다. 도 86에 도시한 바와 같이 콘텐츠 데이터에는 부정한 기록 재생기 식별자(ID_{dev}) 리스트로서의 폐지(Revocation) 리스트를 보유하고 있다. 또한, 폐지 리스트의 변경 체크용 리스트 체크치 ICV_{rev}를 설치하고 있다. 부정한 기록 재생기 식별자(ID_{dev}) 리스트는 콘텐츠 제공자 또는 관리자가 예를 들면 부정 복사의 유통 상태 등으로부터 판명된 부정한 기록 재생기의 식별자 ID_{dev}를 리스트화한 것이다. 이 폐지 리스트는 예를 들면 배송 키 K_{dis}에 의해 암호화되어 저장해도 좋다. 기록 재생기에 의한 복호 처리에 대해서는 예를 들면 앞의 도 22의 콘텐츠 다운로드 처리의 형태와 동일하다.

또, 여기서는 이해를 쉽게 하기 위해서, 폐지 리스트를 단독 데이터로서 도 86의 콘텐츠 데이터 중에 나타내고 있지만, 예를 들면 앞서 설명한 콘텐츠 데이터의 헤더부의 구성 요소인 취급 방침(예를 들면, 도 32~35 참조) 중에 폐지 리스트를 포함시켜도 좋다. 이 경우에는 앞서 설명한 체크치 ICV_a에 의해 폐지 리스트를 포함하는 취급 방침 데이터의 변경 체크가 이루어진다. 폐지 리스트가 취급 방침 중에 포함되는 경우에는 체크치 A:ICV_a의 체크에 의해 대체되고, 기록 재생기 내의 체크치 A 생성 키 K_{icva}가 이용되고, 체크치 생성 키 $K_{icv-rev}$를 저장할 필요는 없다.

폐지 리스트를 단독의 데이터로서 콘텐츠 데이터 중에 포함시키는 경우에는 폐지 리스트의 변경 체크용 리스트 체크치 ICV_{rev}에 의한 폐지 리스트의 체크를 실행함과 함께, 리스트 체크치 ICV_{rev}와 콘텐츠 데이터 중의 다른 부분 체크치로부터 중간 체크치를 생성하여 중간 체크치의 검증 처리를 행하는 구성으로 한다.

폐지 리스트의 변경 체크용 리스트 체크치 ICV_{rev}에 의한 폐지 리스트의 체크 방법은 상술한 도 23, 도 24 등에서 설명한 ICV_a, ICV_b 등의 체크치 생성 처리와 동일한 방법으로 실행 가능하다. 즉, 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존한 체크치 생성 키 $K_{icv-rev}$를 키로 하고, 콘텐츠 데이터 중에 포함되는 폐지 리스트를 메세지로서 도 23, 도 24 등에서 설명한 ICV 계산 방법에 따라 계산된다. 계산된 체크치 ICV-rev'와 헤더(Header) 내에 저장된 체크치: ICV-rev를 비교하여, 일치한 경우에는 변경이 없다고 판정한다.

리스트 체크치 ICV_{rev}를 포함하는 중간 체크치는 예를 들면, 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 총 체크치 생성 키 K_{icvt}를 키로 하여, 검증한 Header 내의 체크치 A, 체크치 B, 리스트 체크치 ICV_{rev}, 또한 포맷에 따라 콘텐츠 체크치를 가한 메세지 열에 도 7 또는 그 밖의 도면에서 설명한 ICV 계산 방법을 적용하여 생성한다.

이들 폐지 리스트, 리스트 체크치는 DVD, CD 등의 미디어(500), 통신 수단 (600)을 통해 또는 메모리 카드 등의 기록 디바이스(400)를 통해 기록 재생기(300)에 제공된다. 여기서 기록 재생기(300)는 정당한 키 데이터를 보유하는 기록 재생기인 경우와, 부정하게 복제된 식별자 ID를 갖는 경우가 있다.

이러한 구성에 있어서의 부정한 기록 재생기의 배제 처리의 처리 플로우를 도 87 및 도 88에 도시한다. 도 87은 DVD, CD 등의 미디어(500) 또는 통신 수단 (600)으로부터 콘텐츠가 제공되는 경우의 부정 기록 재생기 배제(폐지) 처리 플로우이고, 도 88은 메모리 카드 등의 기록 디바이스(400)로부터 콘텐츠가 제공되는 경우의 부정 기록 재생기 배제(폐지) 처리 플로우이다.

우선, 도 87의 처리 플로우에 대하여 설명한다. 단계 901은 미디어를 장착하여, 콘텐츠의 제공, 즉 재생 처리 또는 다운로드의 요구를 행하는 단계이다. 도 87에 도시한 처리는 예를 들면 기록 재생기에 DVD 등의 미디어를 장착하여 다운로드 처리 등을 실행하기 전의 단계으로서 실행된다. 다운로드 처리에 대해서는 도 22를 이용하여 앞서 설명한 바와 같고, 도 22의 처리 플로우의 실행의 전 단계로서 또는 도 22의 처리 플로우 중에 삽입되는 처리로서 도 87의 처리가 실행된다.

기록 재생기(300)가 네트워크 등의 통신 수단을 통해 콘텐츠 제공을 받는 경우에는 단계 S911에 있어서 콘텐츠 신호 분배 서비스측과의 통신 세션을 확립하고, 그 후, 단계 S902로 진행한다.

단계 S902에서는 콘텐츠 데이터의 헤더부로부터 폐지 리스트(도 86 참조)를 취득한다. 이 리스트 취득 처리는 콘텐츠가 미디어 내에 있는 경우에는 도 3에 도시한 제어부(301)가 판독부(304)를 통해 미디어로부터 판독하고, 콘텐츠가 통신 수단으로부터인 경우에는 도 3에 도시한 제어부(301)가 통신부(305)를 통해 콘텐츠 신호 분배측으로부터 수신한다.

다음으로, 단계 S903에 있어서, 제어부(301)는 암호 처리부(302)에 미디어 (500) 또는 통신 수단(600)으로부터 취득한 폐지 리스트를 암호 처리부(302)에 건네주고, 체크치 생성 처리를 실행시킨다. 기록 재생기(300)는 내부에 폐지 체크치 생성 키 $K_{icv-rev}$를 구비하고, 수령한 폐지 리스트를 메세지로서 폐지 체크치 생성 키 $K_{icv-rev}$를 적용하고, 예를 들면 도 23, 도 24 등에서 설명한 ICV 계산 방법에 따라 체크치 $ICV_{-rev'}$를 계산하고, 계산 결과와 콘텐츠 데이터의 헤더(Header) 내에 저장된 체크치:ICV_{-rev}를 비교하여, 일치한 경우에는 변경이 없다(단계 S904에서 Yes)고 판정한다. 일치하지 않은 경우에는 변경되어 있다고 판정되고, 단계 S909로 진행하여 처리 에러로서 처리를 종료한다.

다음으로, 단계 S905에 있어서, 기록 재생기 암호 처리부(302)의 제어부 (306)는 기록 재생기 암호 처리부(302)의 암호/복호화부(308)에 총 체크치 $ICV_{t'}$의 계산을 시킨다. 총 체크치 $ICV_{t'}$는 도 25에 도시한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307)에 보존되어 있는 시스템 서명 키 K_{sys}를 키로 하여, 중간 체크치를 DES로 암호화하여 생성한다. 또, 각 부분 체크치, 예를 들면 ICV_a, ICV_b 등의 검증 처리는 도 87에 도시한 처리 플로우 중에서는 생략되어 있지만, 앞서 설명한 도 39~도 45의 처리 플로우와 동일한 각 데이터 포맷에 따른 부분 체크치의 검증이 행해진다.

다음으로, 단계 S906에 있어서, 생성된 총 체크치 $ICV_{t'}$와 헤더(Header) 내의 ICV_t를 비교하여, 일치한 경우(단계 S906에서 Yes)에는 단계 S907로 진행한다. 일치하지 않은 경우에는 변경되어 있다고 판정되고, 단계 S909로 진행하여 처리 에러로서 처리를 종료한다.

앞서 설명한 바와 같이 총 체크치 ICV_t는 ICV_a, ICV_b, 또한 데이터 포맷에 따라 각 콘텐츠 블록의 체크치 등, 콘텐츠 데이터에 포함되는 부분 체크치 전체를 체크하는 것이지만, 여기서는 이들 부분 체크치에 또한, 폐지 리스트의 변경 체크용의 리스트 체크치 ICV_{rev}를 부분 체크치로서 덧붙여, 이들 모든 변경을 검증한다. 상술한 처리에 의해 생성된 총 체크치가 헤더(Header) 내에 저장된 체크치:ICV_t와 일치한 경우에는 ICV_a, ICV_b, 각 콘텐츠 블록의 체크치 및 리스트 체크치 ICV_{rev} 전부의 변경은 없다고 판단된다.

또한, 단계 S907에서는 변경 없음으로 판정된 폐지 리스트와, 자신의 기록 재생기(300)에 저장된 기록 재생기 식별자(ID_{dev})의 비교가 이루어진다.

콘텐츠 데이터로부터 판독된 부정한 기록 재생기 식별자 ID_{dev}의 리스트에 자신의 기록 재생기의 식별자 ID_{dev}가 포함되어 있는 경우에는 그 기록 재생기(300)는 부정하게 복제된 키 데이터를 갖고 있다고 판정되어, 단계 S909로 진행하고, 이후의 수속은 중지된다. 예를 들면 도 22의 콘텐츠 다운로드 처리의 수속을 실행 불가능으로 한다.

단계 S907에 있어서, 부정한 기록 재생기 식별자 ID_{dev}의 리스트에 자신의 기록 재생기의 식별자 ID_{dev}가 포함되어 있지 않다고 판정된 경우에는 그 기록 재생기 (300)는 정당한 키 데이터를 갖고 있다고 판정되어, 단계 S908로 진행하고, 이후의 수속, 예를 들면, 프로그램 실행 처리 또는 도 22 등의 콘텐츠 다운로드 처리 등이 실행 가능하게 된다.

도 88은 메모리 카드 등의 기록 디바이스(400)에 저장한 콘텐츠 데이터를 재생하는 경우의 처리를 나타낸다. 앞서 설명한 바와 같이 메모리 카드 등의 기록 디바이스(400)와 기록 재생기(300)는 도 20에서 설명한 상호 인증 처리(단계 S921)가 실행된다. 단계 S922에 있어서, 상호 인증 OK인 경우에만, 단계 S923 이후의 처리로 진행하고, 상호 인증에 실패한 경우에는 단계 S930의 에러가 되어, 이후의 처리는 실행되지 않는다.

단계 S923에서는 콘텐츠 데이터의 헤더부로부터 폐지 리스트(도 86 참조)를 취득한다. 이후의 단계 S924～S930의 처리는 앞의 도 87에 있어서의 대응 처리와 동일한 처리이다. 즉, 리스트 체크치에 의한 리스트의 검증(S924, S925), 총 체크치에 의한 검증(S926, S927), 리스트의 엔트리와 자신의 기록 재생기 식별자 ID_{dev}와의 비교(S928)를 실행하여, 콘텐츠 데이터로부터 판독된 부정한 기록 재생기 식별자 ID_{dev}의 리스트에 자기의 기록 재생기의 식별자 ID_{dev}가 포함되어 있는 경우, 그 기록 재생기(300)는 부정하게 복제된 키 데이터를 갖고 있다고 판정되어, 단계 S930으로 진행하고, 이후의 수속은 중지된다. 예를 들면, 도 28에 도시한 콘텐츠의 재생 처리를 실행 불가능으로 한다. 한편, 부정한 기록 재생기 식별자 ID_{dev}의 리스트에 자신의 기록 재생기의 식별자 ID_{dev}가 포함되어 있지 않다고 판정된 경우에는 그 기록 재생기(300)는 정당한 키 데이터를 갖고 있다고 판정되고, 단계 S929로 진행하여, 이후의 수속이 실행 가능하게 된다.

이와 같이 본 발명의 데이터 처리 장치에서는 콘텐츠 제공자 또는 관리자가 제공하는 콘텐츠에 더불어 부정한 기록 재생기를 식별하는 데이터, 즉 부정한 기록 재생기 식별자 ID_{dev}를 리스트화한 폐지 리스트를 콘텐츠 데이터의 헤더부의 구성 데이터로서 포함시켜서 기록 재생기 이용자에게 제공하고, 기록 재생기 이용자는 기록 재생기에 의한 콘텐츠의 이용에 앞서, 자신의 기록 재생기의 메모리에 저장된 기록 재생기 식별자 ID_{dev}와, 리스트 식별자와의 대조를 실행하여 일치하는 데이터가 존재한 경우에는 이후의 처리를 실행시키지 않는 구성으로 하였기 때문에 키 데이터를 복제하여 메모리에 저장한 부정한 기록 재생기에 의한 콘텐츠 이용을 배제할 수 있다.

(18) 시큐어 칩 구성 및 제조 방법

앞서 설명한 바와 같이 기록 재생기 암호 처리부(302)의 내부 메모리(307) 또는 기록 디바이스(400)의 내부 메모리(405)는 암호 키 등의 중요한 정보를 보유하고 있기 때문에 외부로부터 부정하게 판독하기 어려운 구조로 해 둘 필요가 있다. 따라서, 기록 재생기 암호 처리부(302), 기록 디바이스 암호 처리부(401)는 예를 들면 외부로부터 액세스하기 어려운 구조를 갖은 반도체 칩으로 구성되고, 다층 구조를 구비하며, 그 내부의 메모리는 알루미늄층 등의 더미층에 끼워지거나, 최하층에 구성되고, 또한 동작하는 전압 또는/또한 주파수의 폭이 좁다는 등, 외부로부터 부정하게 데이터의 판독이 어려운 특성을 갖는 내탬퍼 메모리로서 구성된다.

그러나, 상술한 설명에서 알 수 있는 바와 같이 예를 들면 기록 재생기 암호 처리부(302)의 내부 메모리(307)에는 기록 재생기 서명 키 K_{dev} 등의 기록 재생기마다 다른 데이터를 기입할 필요가 있다. 또한, 칩 내의 불휘발성 기억 영역, 예를 들면 플래시 메모리, FeRAM 등에 칩마다의 개별 정보, 예를 들면 식별 정보(ID)나 암호 키 정보를 기입한 후, 예를 들면 제품 출하 후에 있어서의 데이터의 재기입, 판독을 곤란하게 하는 것이 필요하게 된다.

종래의 기입 데이터의 판독, 재기입 처리를 곤란하게 하기 위한 방법에는 예를 들면 데이터 기입의 커맨드 프로토콜을 비밀로 한다. 또는 칩 상의 데이터 기입 커맨드를 접수하는 신호선과, 제품화한 후에 이용되는 통신용 신호선을 분리하여 구성하고, 기판 상의 칩에 직접 신호를 보내지 않는 한, 데이터 기입 커맨드가 유효하게 되지 않도록 하는 등의 방법이 있다.

그러나, 이러한 종래 방법을 채택해도 기억 소자의 전문 지식을 갖는 것에 있어서는 회로를 구동시키는 설비와 기술이 있으면, 칩의 데이터 기입 영역에 대한 신호 출력이 가능하고, 또한 가령 데이터 기입의 커맨드 프로토콜이 비밀이었다고 해도, 프로토콜의 해석 가능성은 항상 존재한다.

이러한 비밀 데이터의 개변 가능성을 보유한 암호 처리 데이터의 저장 소자를 유통시키는 것은 암호 처리 시스템 전체를 위협하는 결과가 된다. 또한, 데이터의 판독을 방지하기 위해서, 데이터 판독 커맨드 자체를 실장하지 않은 구성으로 할 수도 있지만, 그 경우, 정규 데이터 기입을 실행한 경우라도, 메모리에 대한 데이터 기입이 실제로 행해졌는지의 여부를 확인하거나, 기입된 데이터가 정확하게 기입되어 있는지의 여부를 판정하는 것이 불가능하게 되고, 불량 데이터 기입이 행해진 칩이 공급될 가능성이 발생한다.

이들 종래 기술에 감안하여, 여기서는, 예를 들면 플래시 메모리, FeRAM 등의 불휘발성 메모리에 정확한 데이터 기입을 가능하게 함과 함께, 데이터의 판독을 곤란하게 하는 시큐어 칩 구성 및 시큐어 칩 제조 방법을 제공한다.

도 89에 예를 들면, 상술한 기록 재생기 암호 처리부(302) 또는 기록 디바이스(400)의 암호 처리부(401)에 적용 가능한 시큐러티 칩 구성을 나타낸다. 도 89의 (A)는 칩의 제조 과정, 즉 데이터의 기입 과정에서의 시큐러티 칩 구성을 나타내고, 도 89의 (B)는 데이터를 기입한 시큐러티 칩을 탑재한 제품의 구성예, 예를 들면 기록 재생기(300), 기록 디바이스(400) 예를 나타낸다.

제조 과정에 있는 시큐러티 칩은 처리부(8001)에 모드 지정용 신호선(8003) 및 각종 커맨드 신호선(8004)이 접속되고, 처리부(8001)는 모드 지정용 신호선 (8003)으로 설정된 모드로서, 예를 들면 데이터 기입 모드 또는 데이터 판독 모드에 따라 불휘발성 메모리인 기억부(8002)로의 데이터 기입 처리 또는 기억부(8002)로부터의 데이터 판독 처리를 실행한다.

한편, 도 89의 (B)의 시큐러티 칩 탑재 제품에 있어서는 시큐러티 칩과 외부 접속 인터페이스, 주변 기기, 다른 소자 등이 범용 신호선으로 접속되지만, 모드 신호선(8003)은 비 접속 상태가 된다. 구체적인 처리는 예를 들면 모드 신호선 (8003)을 접지 접속하는 Vcc로 끌어 올리거나 신호선을 컷트하거나 절연체 수지로 봉인하거나 한다. 이러한 처리에 의해 제품 출하 후는 시큐러티 칩의 모드 신호선에 대한 액세스가 곤란하게 되고, 외부로부터 칩의 데이터를 판독하거나 기입을 행하거나 하는 것이 곤란성을 높일 수 있다.

또한, 본 구성의 시큐러티 칩(8000)은 데이터의 기억부(8002)에 대한 기입 처리 및 기억부(8002)에 기입된 데이터의 판독 처리를 곤란하게 하는 구성을 갖고, 가령 제3자가 모드 신호선(8003)의 액세스에 성공한 경우라도 부정 데이터의 기입, 판독을 방지할 수 있다. 도 90에 본 구성을 갖는 시큐러티 칩에서의 데이터 기입 또는 판독 처리 플로우를 나타낸다.

단계 S951은 모드 신호선(8003)을 데이터 기입 모드 또는 데이터 판독 모드로 설정하는 단계이다.

단계 S952는 칩으로부터 인증용 정보를 추출하는 단계이다. 본 구성의 시큐러티 칩에는 예를 들면 와이어(Wire), 마스크 ROM 구성에 의해 사전에 패스워드, 암호 기술에 있어서의 인증 처리용 키 정보 등, 인증 처리에 필요한 정보가 저장된다. 단계 S952는 이 인증 정보를 판독하여 인증 처리를 실행한다. 예를 들면 정규 데이터 기입 지그, 데이터 판독 장치를 범용 신호선에 접속하여 인증 처리를 실행한 경우에는 인증 OK(단계 S953에 있어서 Yes)의 결과가 얻어지지만, 부정한 데이터 기입 지그, 데이터 판독 장치를 범용 신호선에 접속하여 인증 처리를 실행한 경우에는 인증에 실패(단계 S953에 있어서 No)하여, 그 시점에서 처리가 중지된다. 인증 처리는 예를 들면, 앞서 설명한 도 13의 상호 인증 처리 수속에 따라 실행 가능하다. 도 89에 도시한 처리부(8001)는 이들 인증 처리를 실행 가능한 구성을 갖는다. 이는 예를 들면, 앞서 설명한 도 29에 도시한 기록 디바이스(400)의 암호 처리부(401)의 제어부(403)에 삽입된 커맨드 레지스터와 동일한 구성에 의해 실현 가능하다. 예를 들면 도 89의 칩의 처리부는 도 29에 도시한 기록 디바이스 (400)의 암호 처리부(401)의 제어부(403)에 삽입된 커맨드 레지스터와 동일한 구성을 갖고, 각종 커맨드 신호선(8004)에 접속된 기기로부터 소정의 커맨드 No가 입력되면, 대응하는 처리를 실행하여, 인증 처리 시퀀스를 실행할 수 있다.

처리부(8001)는 인증 처리에 있어서 인증이 이루어진 경우에만, 데이터의 기입 커맨드 또는 데이터의 판독 커맨드를 접수하여 데이터의 기입 처리(단계 S955) 또는 데이터의 판독 처리(단계 S956)를 실행한다.

이와 같이 본 구성의 시큐러티 칩에서는 데이터의 기입 시, 판독 시에 인증 처리를 실행하는 구성으로 하였기 때문에 정당한 권리를 갖지 않은 제3자에 의한 시큐러티 칩의 기억부로부터 데이터의 판독 또는 기억부로의 데이터 기입을 방지할 수 있다.

다음으로, 시큐러티가 더욱 높은 소자 구성으로 한 실시예를 도 91에 도시한다. 본 예에서는 시큐러티 칩의 기억부(8200)가 두 개의 영역으로 분리되어, 한쪽은 데이터의 기입 및 판독이 가능한 판독 기입 병용 영역(RW: Read Write 영역: 8201)이고, 다른 쪽은 데이터 기입만 가능한 기입 전용 영역(WO: Write Only 영역: 8202)이다.

이 구성에 있어서, 기입 전용 영역(WO: Write Only 영역: 8202)에는 암호 키 데이터, 식별자 데이터 등의 시큐러티 요청이 높은 데이터를 기입하고, 한편 시큐러티도가 그다지 높지 않은, 예를 들면 체크용 데이터 등을 판독 기입 병용 영역(RW: Read Write 영역: 8201)에 기입한다.

처리부(8001)는 판독 기입 병용 영역(RW: Read Write 영역: 8201)으로부터의 데이터 판독 처리는 상술한 도 90에서 설명한 인증 처리를 따른 데이터 판독 처리를 실행한다. 그러나, 데이터 기입 처리는 도 92의 플로우에 따라 실행한다.

도 92의 단계 S961은 모드 신호선(8003)을 기입 모드에 설정하는 단계로서, 단계 S962에서는 앞의 도 90에서 설명한 것과 동일한 인증 처리를 실행한다. 인증 처리로 인증이 이루어지면, 단계 S963으로 진행하여, 커맨드 신호선(8004)을 통해 기입 전용(WO) 영역(8202)에 시큐러티가 높은 키 데이터 등의 정보의 기입, 판독 기입 병용 영역(RW: Read Write 영역: 8201)에 시큐러티도가 그다지 높지 않은, 예를 들면 체크용 데이터 기입하는 커맨드를 처리부(8001)에 대하여 출력한다.

단계 S964에서는 커맨드를 수령한 처리부(8001)가 커맨드에 따른 데이터 기입 처리를 각각 기입 전용(WO) 영역(8202), 판독 기입 병용 영역(RW: Read Write 영역: 8201)에 대하여 실행한다.

또한, 기입 전용(WO) 영역(8202)에 기입된 데이터의 검증 처리 플로우를 도 93에 도시한다.

도 93의 단계 S971은 처리부(8001)에 있어서, 기입 전용(WO) 영역(8202)에 기입된 데이터에 기초한 암호 처리를 실행시킨다. 이들 실행 구성은 앞의 인증 처리 실행 구성과 마찬가지로 커맨드 레지스터에 저장된 암호 처리 시퀀스를 순차 실행하는 구성에 의해 실현된다. 또한, 처리부(8001)에 있어서 실행되는 암호 처리 알고리즘은 특별히 한정되는 것이 아니라, 예를 들면 먼저 설명한 DES 알고리즘을 실행하는 구성으로 할 수 있다.

다음으로, 단계 S972에서, 시큐러티 칩에 접속된 검증 장치가 처리부(8001)로부터 암호 처리 결과를 수신한다. 다음으로, 단계 S973에 있어서, 먼저 기억부에 기입 처리를 행한 정규 기입 데이터에 대하여 처리부(8001)에 있어서 실행된 알고리즘과 동일한 암호화 처리를 적용하여 얻은 결과와, 처리부(8001)로부터의 암호화 결과를 비교한다.

비교한 결과가 동일하면, 기입 전용(WO) 영역(8202)에 기입된 데이터는 올바른 것이 검증된다.

본 구성에서는 인증 처리가 파괴되어 판독 커맨드가 만일 실행 가능하게 되어도, 데이터의 판독 가능 영역은 판독 기입 병용 영역(RW: Read Write 영역: 8201)에 한정되고, 기입 전용(WO) 영역(8202)에 기입된 데이터의 판독은 불가능하여 시큐러티가 더욱 높은 구성이 된다. 또한, 완전히 판독을 불가능하게 한 칩과 달리, 판독 기입 병용 영역(RW: Read Write 영역: 8201)이 구성되어 있기 때문에 메모리 액세스의 정당성 체크가 가능하다.

이상, 특정한 실시예를 참조하여 본 발명에 대하여 상세하게 설명하였다. 그러나, 본 발명의 요지를 일탈하지 않은 범위에서 당업자가 그 실시예의 수정이나 대용을 할 수 있는 것은 자명하다. 즉, 예시라는 형태로 본 발명을 개시한 것이며, 한정적으로 해석되어서는 안된다. 또한, 상기한 실시예에서는 콘텐츠의 기록, 재생을 가능한 기록 재생기를 예로 하여 설명하였지만, 데이터 기록만, 데이터 재생만 가능한 장치에서도 본 발명의 구성은 적용 가능한 것이며, 본 발명은 퍼스널 컴퓨터 게임 기기, 그 밖의 각종 데이터 처리 장치 일반에 있어서 실시 가능한 것이다. 본 발명의 요지를 판단하기 위해서는 첫머리에 기재한 특허 청구의 범위를 참작해야 한다.

발명의 효과

상술한 바와 같이 본 발명의 데이터 기록 재생기 및 세이브 데이터 처리 방법은 프로그램에만 고유한 암호 키, 예를 들면 콘텐츠 키를 이용하거나, 콘텐츠 키를 기초하여 생성된 세이브 데이터 암호 키를 이용하여 세이브 데이터를 암호화하여 기록 디바이스에 저장 가능한 구성으로 하고, 또한 기록 재생기 고유의 키, 예를 들면 기록 재생기 서명 키를 이용하여 세이브 데이터 암호 키를 생성하여 세이브 데이터를 암호화하여 기록 디바이스에 저장하는 구성으로 하였기 때문에, 프로그램의 동일성, 또는 기록 재생기의 동일성 등이 확보된 경우에만 세이브 데이터를 이용할 수 있으며, 제3자에 의한 세이브 데이터의 부정 이용, 변경 등을 방지할 수 있다.

또한, 본 발명의 데이터 기록 재생기 및 세이브 데이터 처리 방법에 의하면, 사용자의 고유 정보, 예를 들면 입력 패스워드에 기초하여 세이브 데이터의 암호 키를 생성하여 사용자 고유의 세이브 데이터 암호 키에 의한 세이브 데이터 저장을 가능하게 하였다. 또한, 이러한 각종 이용 제한, 즉 프로그램 동일성, 기록 재생기의 동일성, 사용자의 동일성을 임의 조합하여 세이브 데이터의 이용 제한을 붙여서 기록 디바이스에 저장할 수 있으며, 시큐러티가 높은 세이브 데이터의 저장, 재생 처리가 가능하게 된다.

도면의 간단한 설명

도 1은 종래의 데이터 처리 시스템의 구성을 나타내는 도면.

도 2는 본 발명이 적용되는 데이터 처리 장치의 구성을 나타내는 도면.

도 3은 본 발명이 적용되는 데이터 처리 장치의 구성을 나타내는 도면.

도 4는 미디어 상, 통신로 상에서의 콘텐츠 데이터의 데이터 포맷을 나타내는 도면.

도 5는 콘텐츠 데이터 중의 헤더에 포함되는 취급 방침을 나타내는 도면.

도 6은 콘텐츠 데이터 중의 헤더에 포함되는 블록 정보를 나타내는 도면.

도 7은 DES를 이용한 전자 서명 생성 방법을 나타내는 도면.

도 8은 트리플 DES를 이용한 전자 서명 생성 방법을 나타내는 도면.

도 9는 트리플 DES 형태를 설명하는 도면.

도 10은 일부에 트리플 DES를 이용한 전자 서명 생성 방법을 나타내는 도면.

도 11은 전자 서명 생성에 있어서의 처리 플로우를 나타내는 도면.

도 12는 전자 서명 검증에 있어서의 처리 플로우를 나타내는 도면.

도 13은 대칭 키 암호 기술을 이용한 상호 인증 처리의 처리 시퀀스를 설명하는 도면.

도 14는 공개 키 증명서를 설명하는 도면.

도 15는 비 대칭 키 암호 기술을 이용한 상호 인증 처리의 처리 시퀀스를 설명하는 도면.

도 16은 타원 곡선 암호를 이용한 암호화 처리의 처리 플로우를 나타내는 도면.

도 17은 타원 곡선 암호를 이용한 복호화 처리의 처리 플로우를 나타내는 도면.

도 18은 기록 재생기 상의 데이터 보유 상황을 나타내는 도면.

도 19는 기록 디바이스 상의 데이터 보유 상황을 나타내는 도면.

도 20은 기록 재생기와 기록 디바이스와의 상호 인증 처리 플로우를 나타내는 도면.

도 21은 기록 재생기의 마스터 키와 기록 디바이스의 대응 키 블록과의 관계를 나타내는 도면.

도 22는 콘텐츠의 다운로드 처리에 있어서의 처리 플로우를 나타내는 도면.

도 23은 체크치 A:ICV_a의 생성 방법을 설명하는 도면.

도 24는 체크치 B:ICV_b의 생성 방법을 설명하는 도면.

도 25는 총 체크치, 기록 재생기 고유 체크치의 생성 방법을 설명하는 도면.

도 26은 기록 디바이스에 보존된 콘텐츠 데이터의 포맷(이용 제한 정보=0)을 나타내는 도면.

도 27은 기록 디바이스에 보존된 콘텐츠 데이터의 포맷(이용 제한 정보=1)을 나타내는 도면.

도 28은 콘텐츠의 재생 처리에 있어서의 처리 플로우를 나타내는 도면.

도 29는 기록 디바이스에 있어서의 커맨드 실행 방법에 대하여 설명하는 도면.

도 30은 기록 디바이스에 있어서의 콘텐츠 저장 처리에 있어서의 커맨드 실행 방법에 대하여 설명하는 도면.

도 31은 기록 디바이스에 있어서의 콘텐츠 재생 처리에 있어서의 커맨드 실행 방법에 대하여 설명하는 도면.

도 32는 콘텐츠 데이터 포맷의 포맷 타입 0의 구성을 설명하는 도면.

도 33은 콘텐츠 데이터 포맷의 포맷 타입 1의 구성을 설명하는 도면.

도 34는 콘텐츠 데이터 포맷의 포맷 타입 2의 구성을 설명하는 도면.

도 35는 콘텐츠 데이터 포맷의 포맷 타입 3의 구성을 설명하는 도면.

도 36은 포맷 타입 0에 있어서의 콘텐츠 체크치 ICV_i의 생성 처리 방법을 설명하는 도면.

도 37은 포맷 타입 1에 있어서의 콘텐츠 체크치 ICV_i의 생성 처리 방법을 설명하는 도면.

도 38은 포맷 타입 2, 3에 있어서의 총 체크치, 기록 재생기 고유 체크치의 생성 처리 방법을 설명하는 도면.

도 39는 포맷 타입 0, 1에 있어서의 콘텐츠 다운로드 처리의 처리 플로우를 나타내는 도면.

도 40은 포맷 타입 2에 있어서의 콘텐츠 다운로드 처리의 처리 플로우를 나타내는 도면.

도 41은 포맷 타입 3에 있어서의 콘텐츠 다운로드 처리의 처리 플로우를 나타내는 도면.

도 42는 포맷 타입 0에 있어서의 콘텐츠 재생 처리의 처리 플로우를 나타내는 도면.

도 43은 포맷 타입 1에 있어서의 콘텐츠 재생 처리의 처리 플로우를 나타내는 도면.

도 44는 포맷 타입 2에 있어서의 콘텐츠 재생 처리의 처리 플로우를 나타내는 도면.

도 45는 포맷 타입 3에 있어서의 콘텐츠 재생 처리의 처리 플로우를 나타내는 도면.

도 46은 콘텐츠 생성자와 콘텐츠 검증자에 있어서의 체크치의 생성, 검증 방법을 설명하는 도면(1).

도 47은 콘텐츠 생성자와 콘텐츠 검증자에 있어서의 체크치의 생성, 검증 방법을 설명하는 도면(2).

도 48은 콘텐츠 생성자와 콘텐츠 검증자에 있어서의 체크치의 생성, 검증 방법을 설명하는 도면(3).

도 49는 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 설명하는 도면.

도 50은 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 콘텐츠 프로바이더와 사용자에 있어서의 처리예를 나타내는 도면(예 1).

도 51은 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 콘텐츠 프로바이더와 사용자에 있어서의 처리예를 나타내는 도면(예 2).

도 52는 마스터 키의 구분 사용에 의해 이용 제한을 실행하는 구성에 대하여 설명하는 도면.

도 53은 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 콘텐츠 프로바이더와 사용자에 있어서의 처리예를 나타내는 도면(예 3).

도 54는 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 콘텐츠 프로바이더와 사용자에 있어서의 처리예를 나타내는 도면(예 4).

도 55는 마스터 키를 이용하여 각종 키를 개별 생성하는 방법에 대하여 콘텐츠 프로바이더와 사용자에 있어서의 처리예를 나타내는 도면(예 5).

도 56은 트리플 DES를 적용한 암호 키를 싱글 DES 알고리즘을 이용하여 저장하는 처리 플로우를 나타내는 도면.

도 57은 우선 순위에 기초한 콘텐츠 재생 처리 플로우(예 1)를 나타내는 도면.

도 58은 우선 순위에 기초한 콘텐츠 재생 처리 플로우(예 2)를 나타내는 도면.

도 59는 우선 순위에 기초한 콘텐츠 재생 처리 플로우(예 3)를 나타내는 도면.

도 60은 콘텐츠 재생 처리에 있어서의 압축 데이터의 복호(신장) 처리를 실행하는 구성에 대하여 설명하는 도면.

도 61은 콘텐츠의 구성예(예 1)를 나타내는 도면.

도 62는 콘텐츠의 구성예 1에 있어서의 재생 처리 플로우를 나타내는 도면.

도 63은 콘텐츠의 구성예(예 2)를 나타내는 도면.

도 64는 콘텐츠의 구성예 2에 있어서의 재생 처리 플로우를 나타내는 도면.

도 65는 콘텐츠의 구성예(예 3)를 나타내는 도면.

도 66은 콘텐츠의 구성예 3에 있어서의 재생 처리 플로우를 나타내는 도면.

도 67은 콘텐츠의 구성예(예 4)를 나타내는 도면.

도 68은 콘텐츠의 구성예 4에 있어서의 재생 처리 플로우를 나타내는 도면.

도 69는 세이브 데이터의 생성, 저장 처리에 대하여 설명하는 도면.

도 70은 세이브 데이터의 저장 처리예(예 1)에 관한 처리 플로우를 나타내는 도면.

도 71은 세이브 데이터의 저장, 재생 처리에 있어서 사용되는 데이터 관리 파일 구성(예 1)을 나타내는 도면.

도 72는 세이브 데이터의 재생 처리예(예 1)에 관한 처리 플로우를 나타내는 도면.

도 73은 세이브 데이터의 저장 처리예(예 2)에 관한 처리 플로우를 나타내는 도면.

도 74는 세이브 데이터의 재생 처리예(예 2)에 관한 처리 플로우를 나타내는 도면.

도 75는 세이브 데이터의 저장 처리예(예 3)에 관한 처리 플로우를 나타내는 도면.

도 76은 세이브 데이터의 저장, 재생 처리에 있어서 사용되는 데이터 관리 파일 구성(예 2)을 나타내는 도면.

도 77은 세이브 데이터의 재생 처리예(예 3)에 관한 처리 플로우를 나타내는 도면.

도 78은 세이브 데이터의 저장 처리예(예 4)에 관한 처리 플로우를 나타내는 도면.

도 79는 세이브 데이터의 재생 처리예(예 4)에 관한 처리 플로우를 나타내는 도면.

도 80은 세이브 데이터의 저장 처리예(예 5)에 관한 처리 플로우를 나타내는 도면.

도 81은 세이브 데이터의 저장, 재생 처리에 있어서 사용되는 데이터 관리 파일 구성(예 3)을 나타내는 도면.

도 82는 세이브 데이터의 재생 처리예(예 5)에 관한 처리 플로우를 나타내는 도면.

도 83은 세이브 데이터의 저장 처리예(예 6)에 관한 처리 플로우를 나타내는 도면.

도 84는 세이브 데이터의 저장, 재생 처리에 있어서 사용되는 데이터 관리 파일 구성(예 4)을 나타내는 도면.

도 85는 세이브 데이터의 재생 처리예(예 6)에 관한 처리 플로우를 나타내는 도면.

도 86은 콘텐츠 부정 이용자 배제(폐지) 구성을 설명하는 도면.

도 87은 콘텐츠 부정 이용자 배제(폐지)의 처리 플로우(예 1)를 나타내는 도면.

도 88은 콘텐츠 부정 이용자 배제(폐지)의 처리 플로우(예 2)를 나타내는 도면.

도 89는 시큐러티 칩의 구성(예 1)을 설명하는 도면.

도 90은 시큐러티 칩의 제조 방법에 있어서의 처리 플로우를 나타내는 도면.

도 91은 시큐러티 칩의 구성(예 2)을 설명하는 도면.

도 92는 시큐러티 칩(예 2)에 있어서의 데이터 기입 처리에 있어서의 처리 플로우를 나타내는 도면.

도 93은 시큐러티 칩(예 2)에 있어서의 기입 데이터 체크 처리에 있어서의 처리 플로우를 나타내는 도면.

<도면의 주요 부분에 대한 부호의 설명>

300 : 기록 재생기

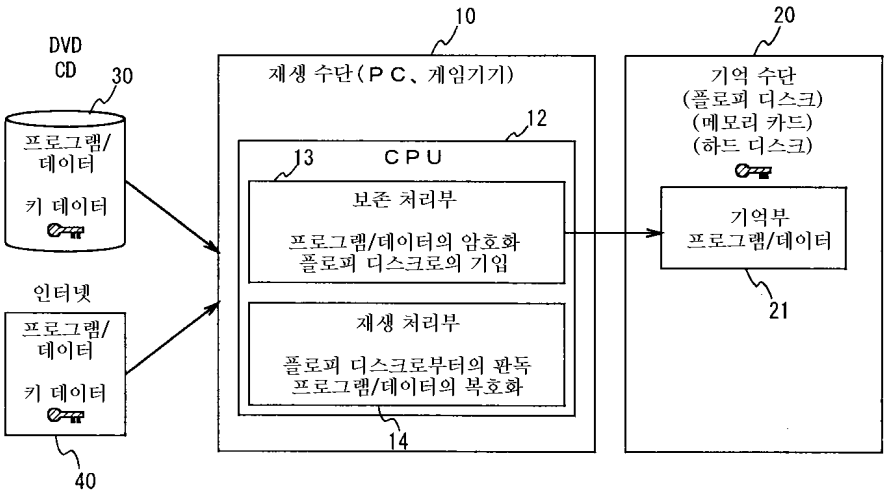
400 : 기록 디바이스

500 : 미디어

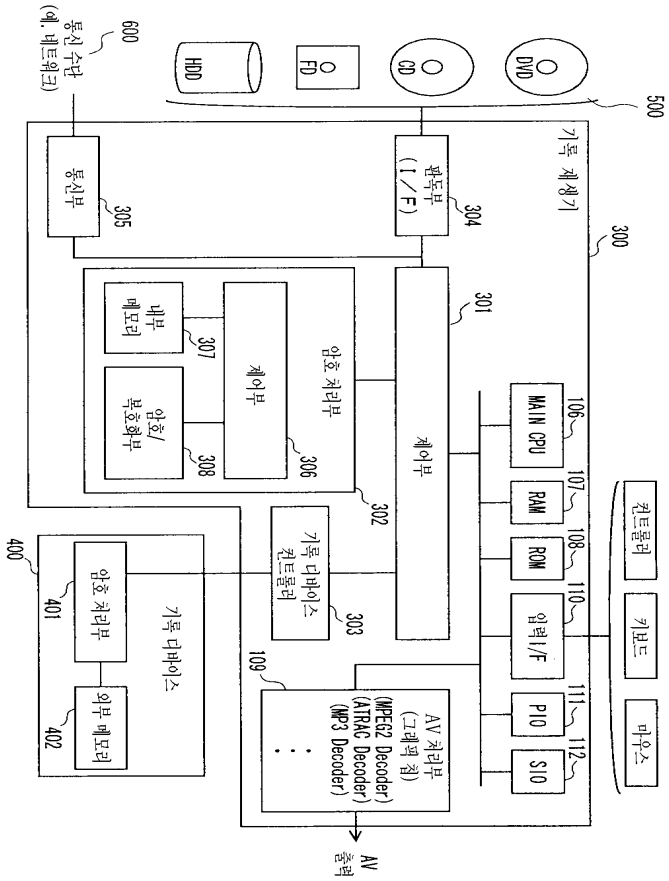
600 : 통신 수단

도면

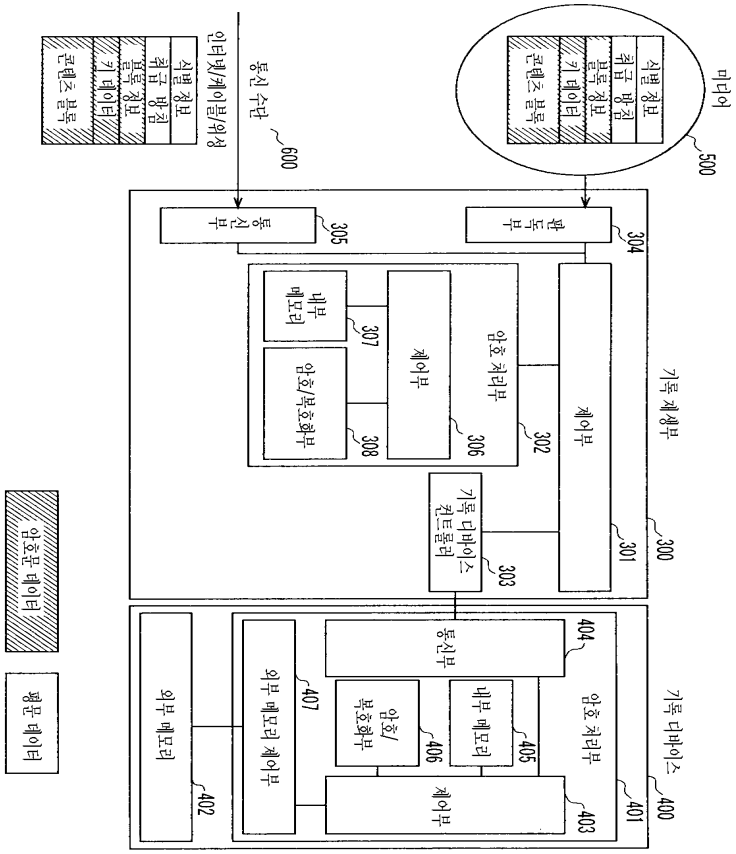
도면1


DVD
CD
30
프로그램/
데이터
키 데이터
인터넷
프로그램/
데이터
키 데이터
40
10
재생 수단(PC、게임기기)
12
13
CPU
보존 처리부
프로그램/데이터의 암호화
플로피 디스크로의 기입
재생 처리부
플로피 디스크로부터의 판독
프로그램/데이터의 복호화
14
20
기억 수단
(플로피 디스크)
(메모리 카드)
(하드 디스크)
기억부
프로그램/데이터
21

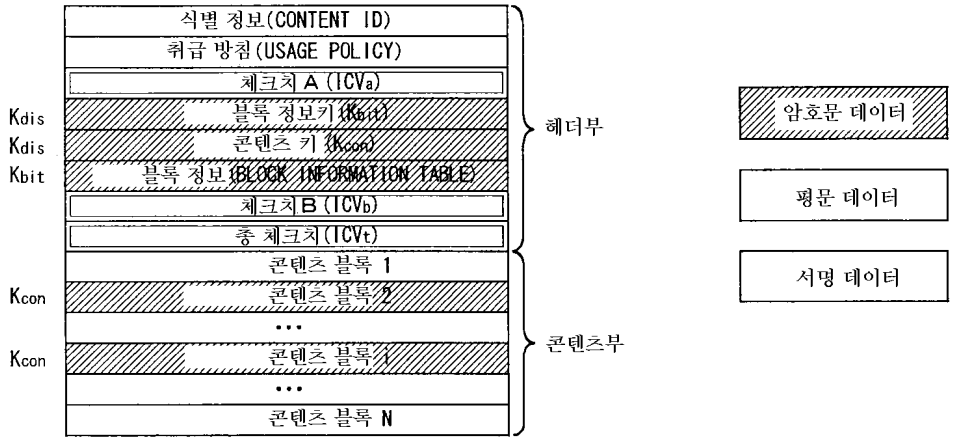
도면2


600
통신 수단
(예. 네트워크)
HDD
FD
CD
DVD
500
기록 재생기
300
통신부
305
판독부
(I/F)
304
301
내부
메모리
307
암호 처리부
제어부
306
암호/
복호화부
308
제어부
302
MAIN CPU
106
RAM
107
ROM
108
입력I/F
110
PIO
111
SIO
112
컨트롤러
키보드
마우스
400
암호 처리부
401
기록 디바이스
컨트롤러
303
기록 디바이스
외부 메모리
402
109
AV 처리부
(그래픽 칩)
(MPEG2 Decoder)
(ATRAC Decoder)
(MP3 Decoder)
AV
출력

도면3



도면4



미디어 상 및 통신로 상의 데이터 포맷

도면5

헤더 사이즈(Header Length)
콘텐츠 사이즈(Content Length)
포맷 버전(Format Version)
포맷 타입(Format Type)
콘텐츠 타입(Content Type)
기동 우선 순위 정보(Operation Priority)
이용 제한 정보(Localization Field)
복제 제한 정보(Copy Permission)
이동 제한 정보(Move Permission)
암호 알고리즘(Encryption Algorithm)
암호화 모드(Encryption Mode)
검증 방법(Integrity Check Method)

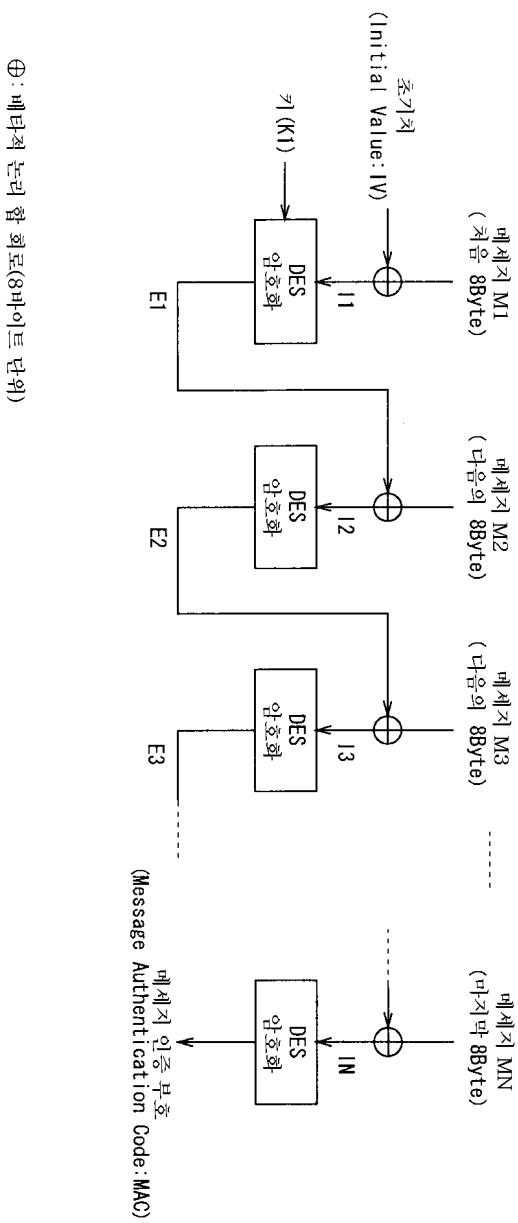
취급 방침

도면6

Kbit		
		콘텐츠 블록수(Block Number)
블록 1		블록 사이즈(Block Length)
		암호화 플러그(Encryption Flag)
		검증 대상 플러그(ICV Flag)
		콘텐츠 체크치(ICV1)
		. . . .
블록 N		블록 사이즈(Block Length)
		암호화 플러그(Encryption Flag)
		검증 대상 플러그(ICV Flag)
		콘텐츠 체크치(ICVN)

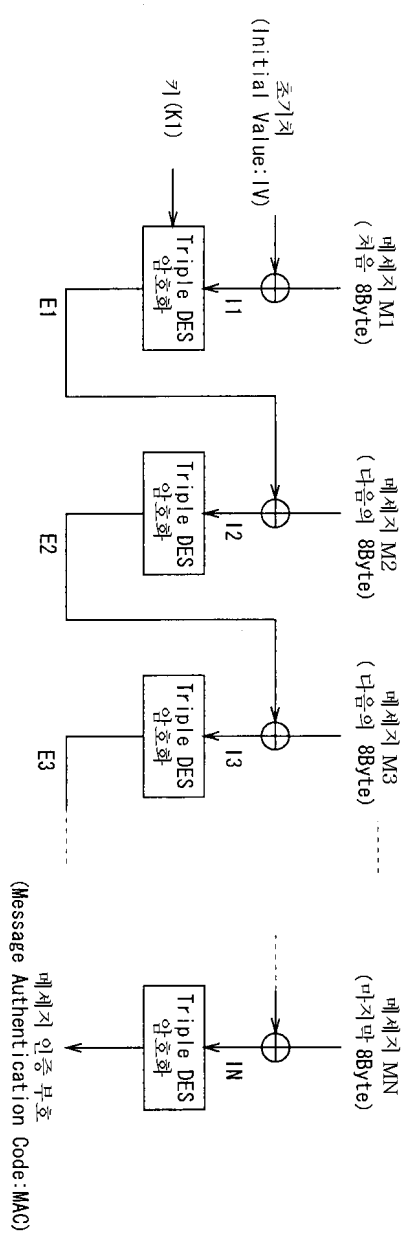
블록 정보

도면7

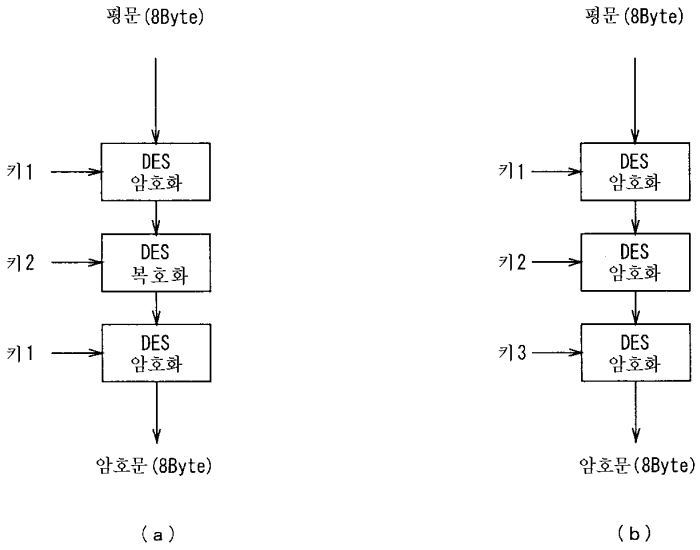


⊕ : 베타적 논리 합 회로(8바이트 단위)

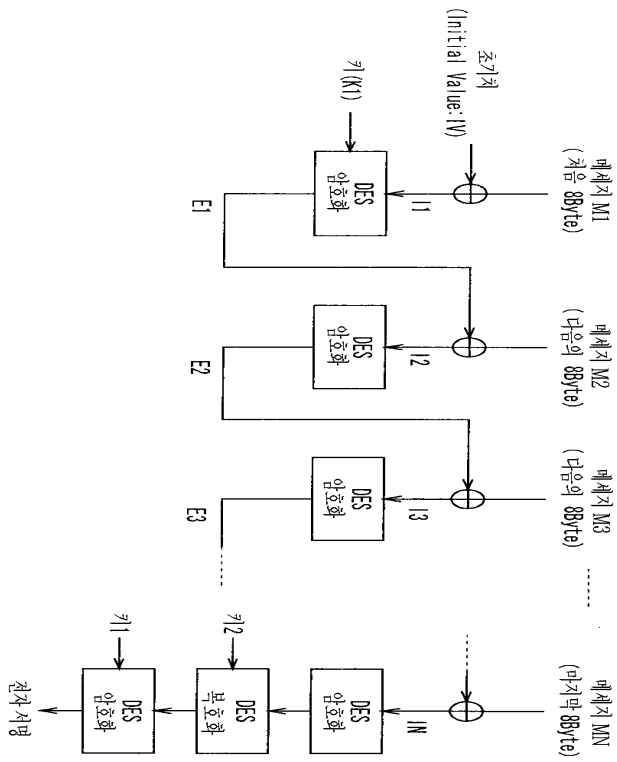
도면8


메세지 M1
(처음 8Byte)
초기치
(Initial Value:IV)
키(K1)
Triple DES
암호화
I1
E1
메세지 M2
(다음의 8Byte)
I2
E2
메세지 M3
(다음의 8Byte)
I3
E3
메세지 MN
(마지막 8Byte)
IN
메세지 인증 부호
(Message Authentication Code:MAC)

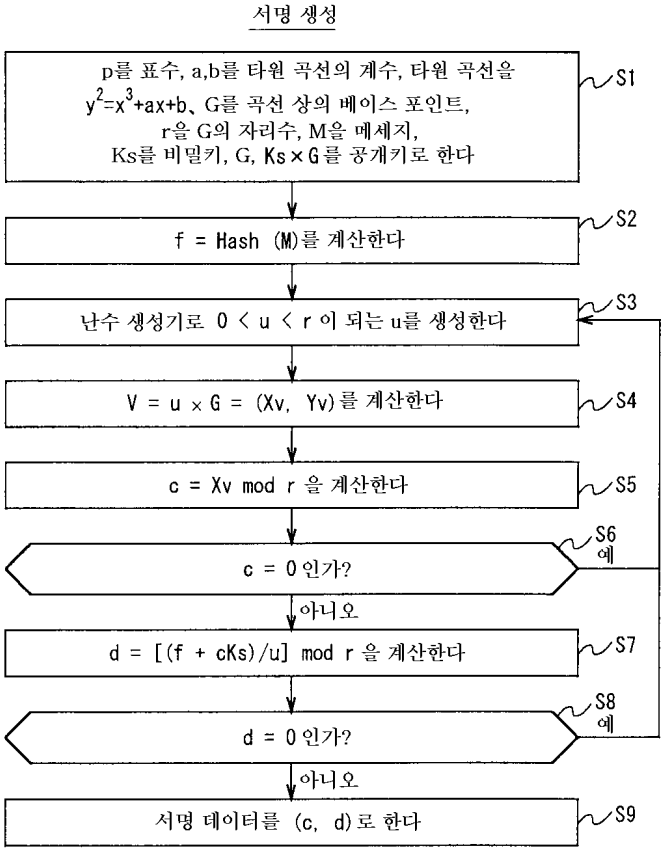
도면9


평문(8Byte)
키1
DES 암호화
키2
DES 복호화
키1
DES 암호화
암호문(8Byte)
(a)
평문(8Byte)
키1
DES 암호화
키2
DES 암호화
키3
DES 암호화
암호문(8Byte)
(b)

도면10

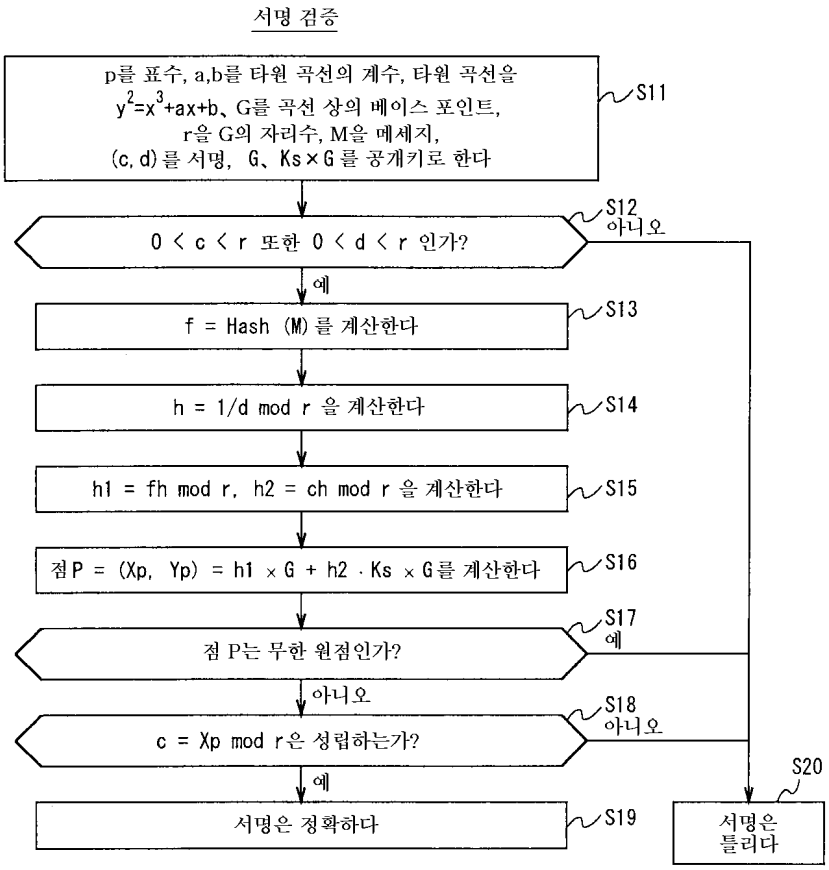

초기치 (Initial Value:IV)
키(K1)
DES 암호화
I1
메세지 M1 (처음 8Byte)
E1
DES 암호화
I2
메세지 M2 (다음의 8Byte)
E2
DES 암호화
I3
메세지 M3 (다음의 8Byte)
E3
키1
DES 암호화
키2
DES 복호화
DES 암호화
IN
메세지 MN (마지막 8Byte)
전자서명

도면11



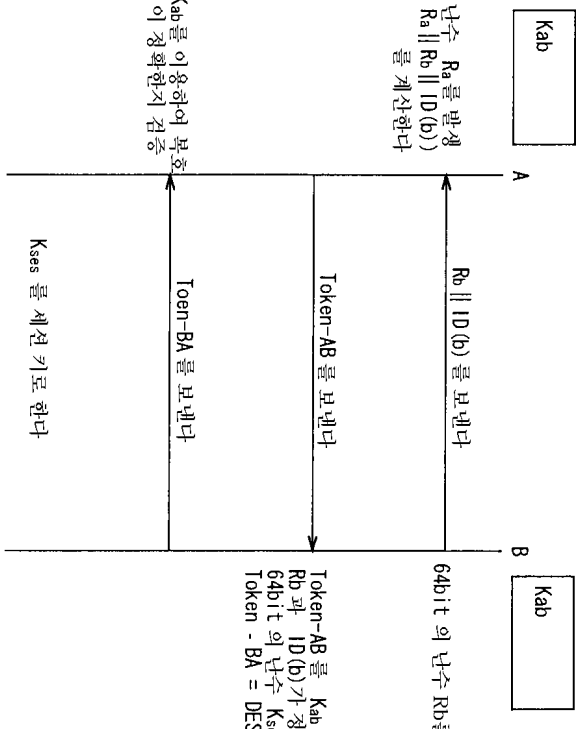
서명 생성(IEEE P1363/D3)

도면12



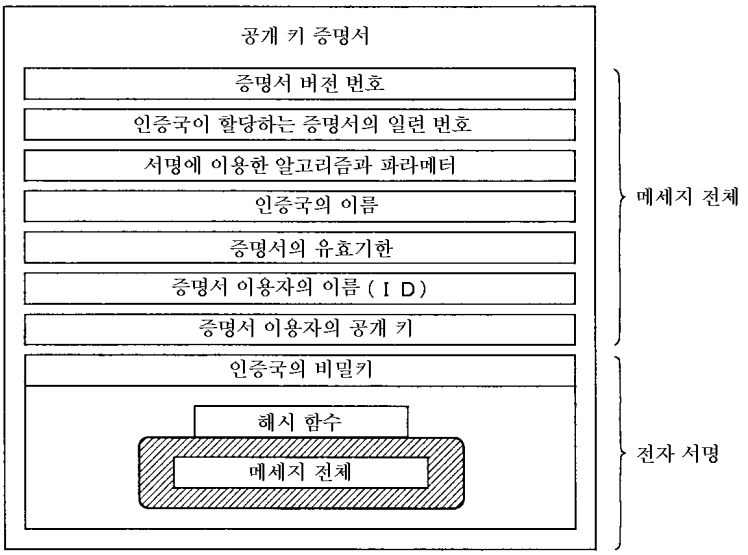
서명 검증(IEEE P1363/D3)

도면13



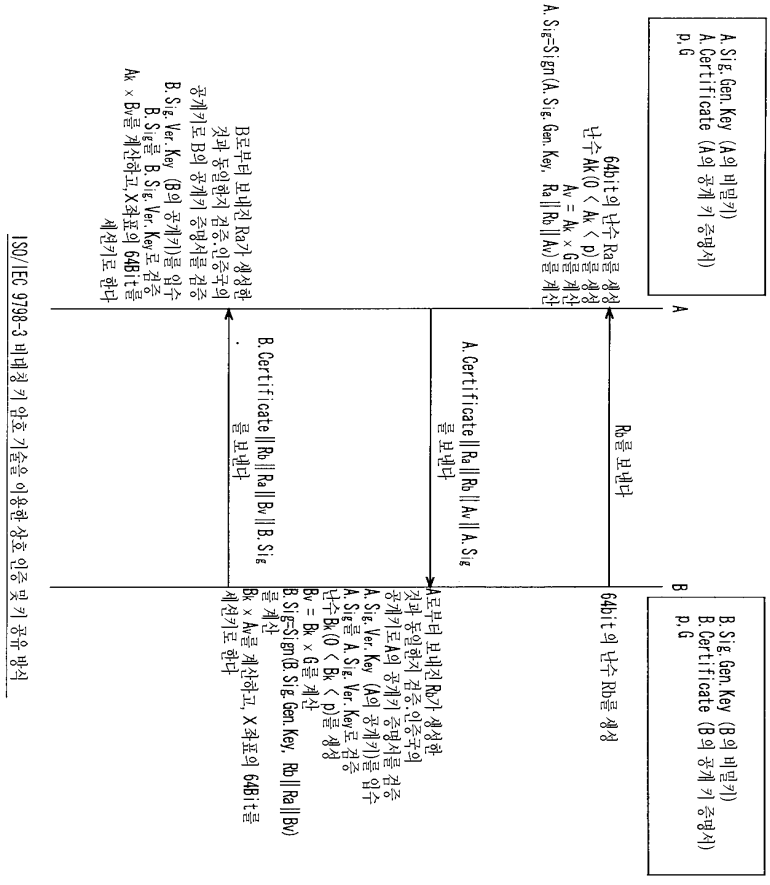
ISO/IEC 9798-2 대칭 키 암호키 기술을 이용한 상호 인증 및 키 공유 방식

도면14



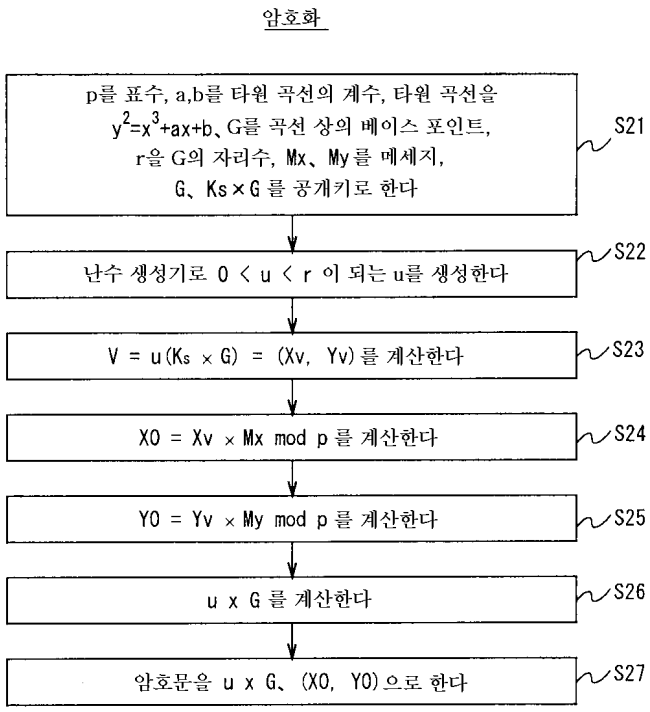
공개 키 증명서

도면15



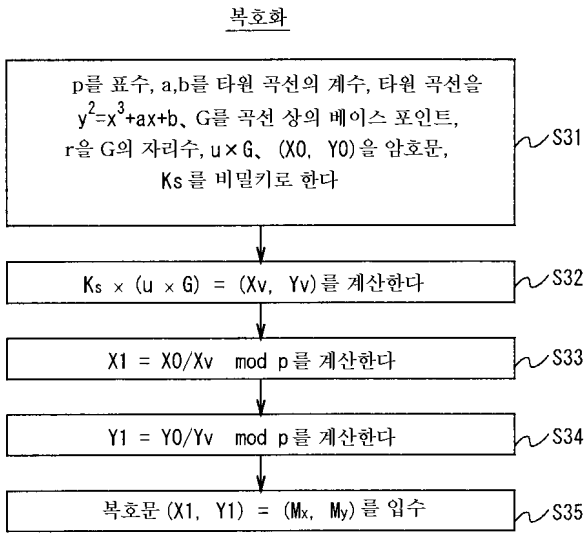
ISO/IEC 9798-3 비대칭 키 암호 기술을 이용한 상호 인증 및 키 공유 방식

도면16



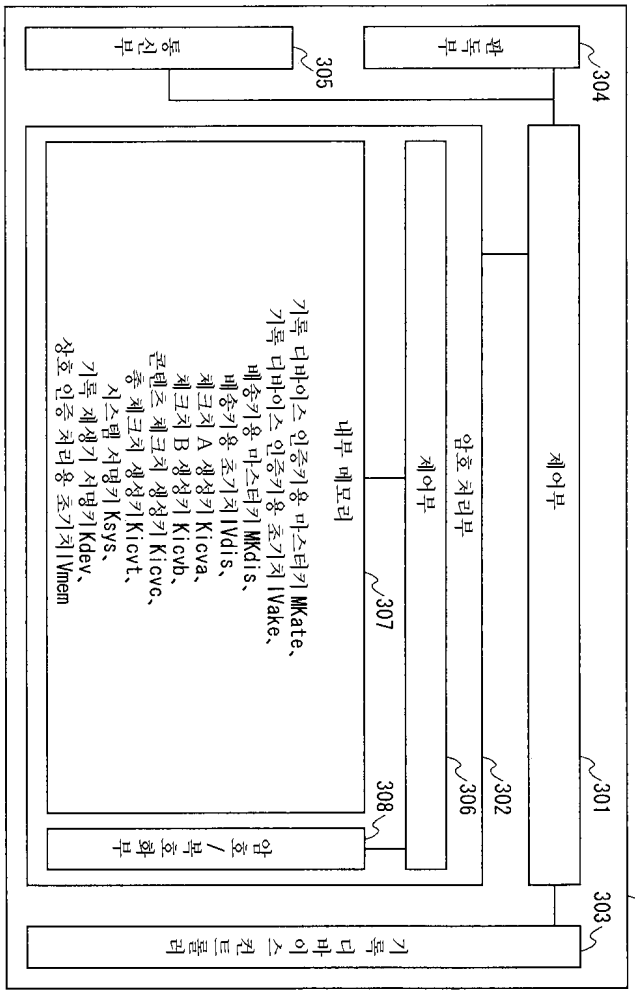
타원 곡선 암호를 이용한 암호화(Menezens-Vanstone)

도면17



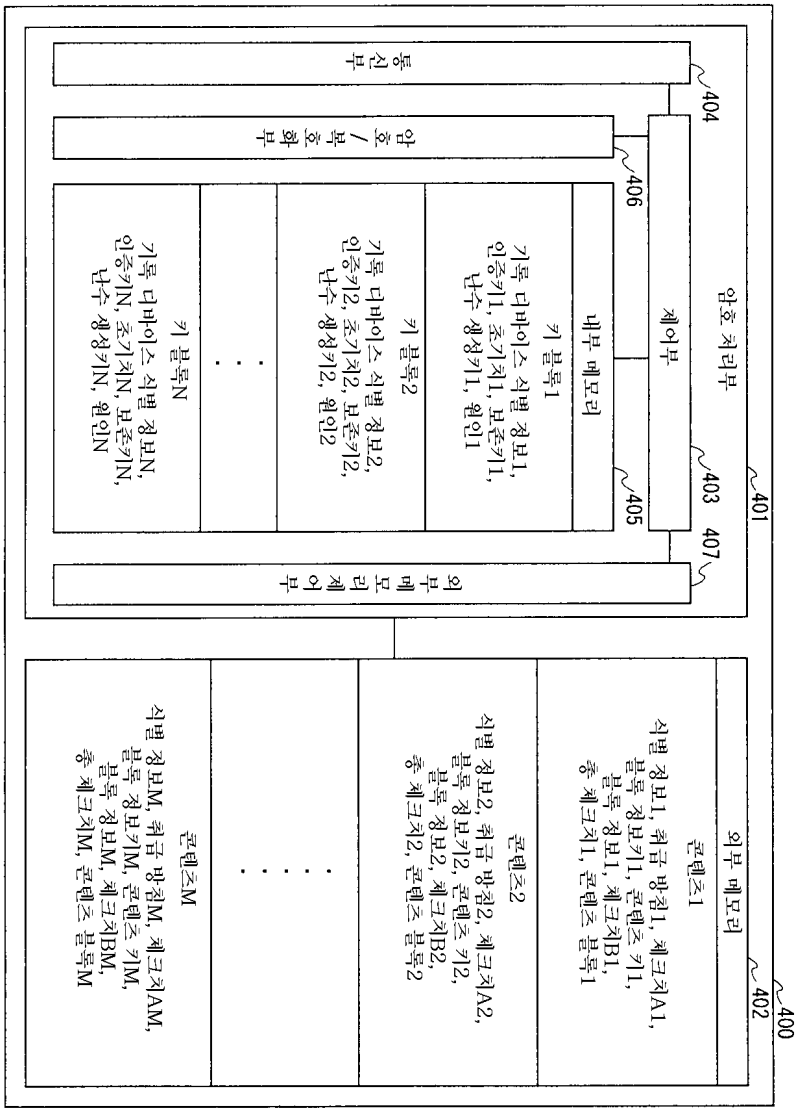
타원 곡선 암호를 이용한 복호화(Menezes-Vanstone)

도면18

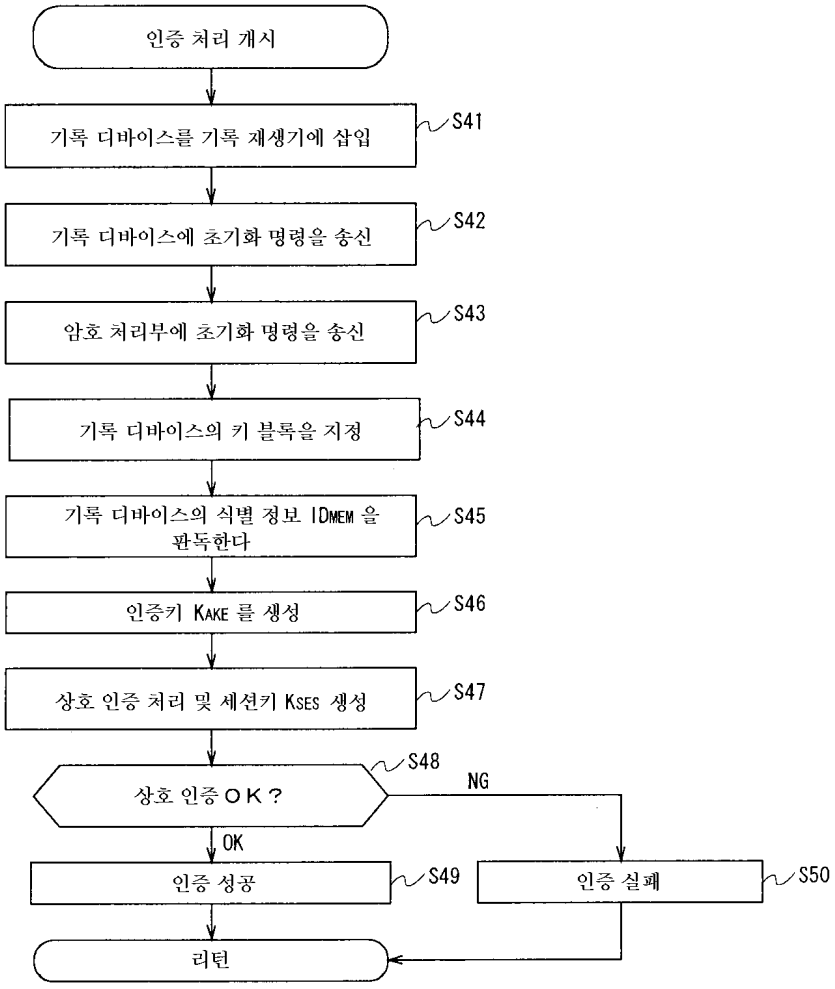


기록 제생기 상의 데이터 보유 상황

도면19

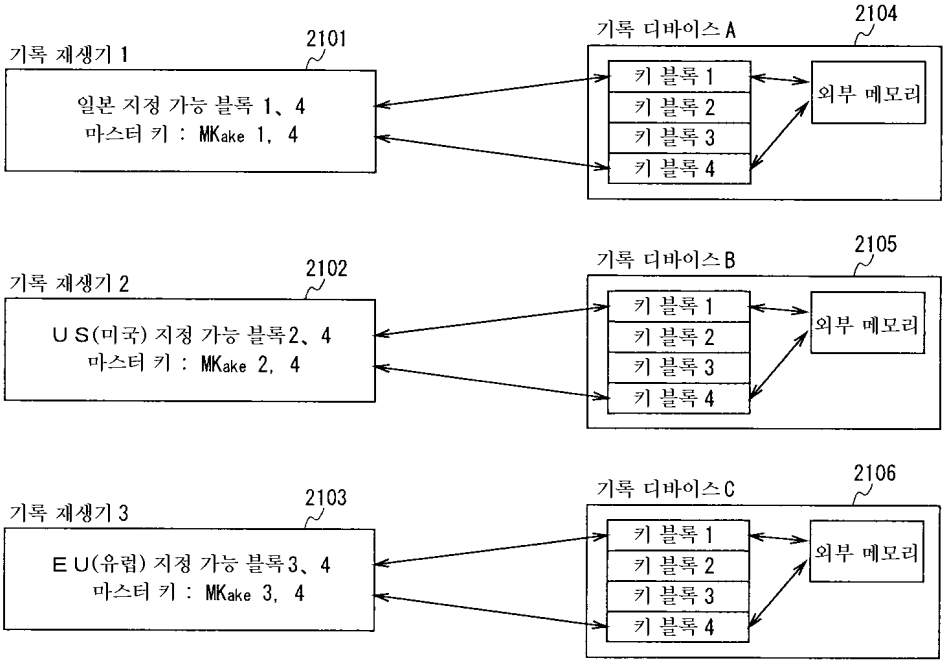

400
401
402
403
404
405
406
407
암호 처리부
외부 메모리
제어부
내부 메모리
외부 메모리 제어부
암호/복호화부
통신부
콘텐츠1
식별 정보1, 취급 방침1, 체크치A1,
블록 정보키1, 콘텐츠 키1,
블록 정보1, 체크치B1,
총 체크치1, 콘텐츠 블록1
콘텐츠2
식별 정보2, 취급 방침2, 체크치A2,
블록 정보키2, 콘텐츠 키2,
블록 정보2, 체크치B2,
총 체크치2, 콘텐츠 블록2
콘텐츠M
식별 정보M, 취급 방침M, 체크치AM,
블록 정보키M, 콘텐츠 키M,
블록 정보M, 체크치BM,
총 체크치M, 콘텐츠 블록M
키 블록1
기록 디바이스 식별 정보1,
인증키1, 초기치1, 보존키1,
난수 생성키1, 원인1
키 블록2
기록 디바이스 식별 정보2,
인증키2, 초기치2, 보존키2,
난수 생성키2, 원인2
키 블록N
기록 디바이스 식별 정보N,
인증키N, 초기치N, 보존키N,
난수 생성키N, 원인N
기록 디바이스 상의 데이터 보유 상황

도면20

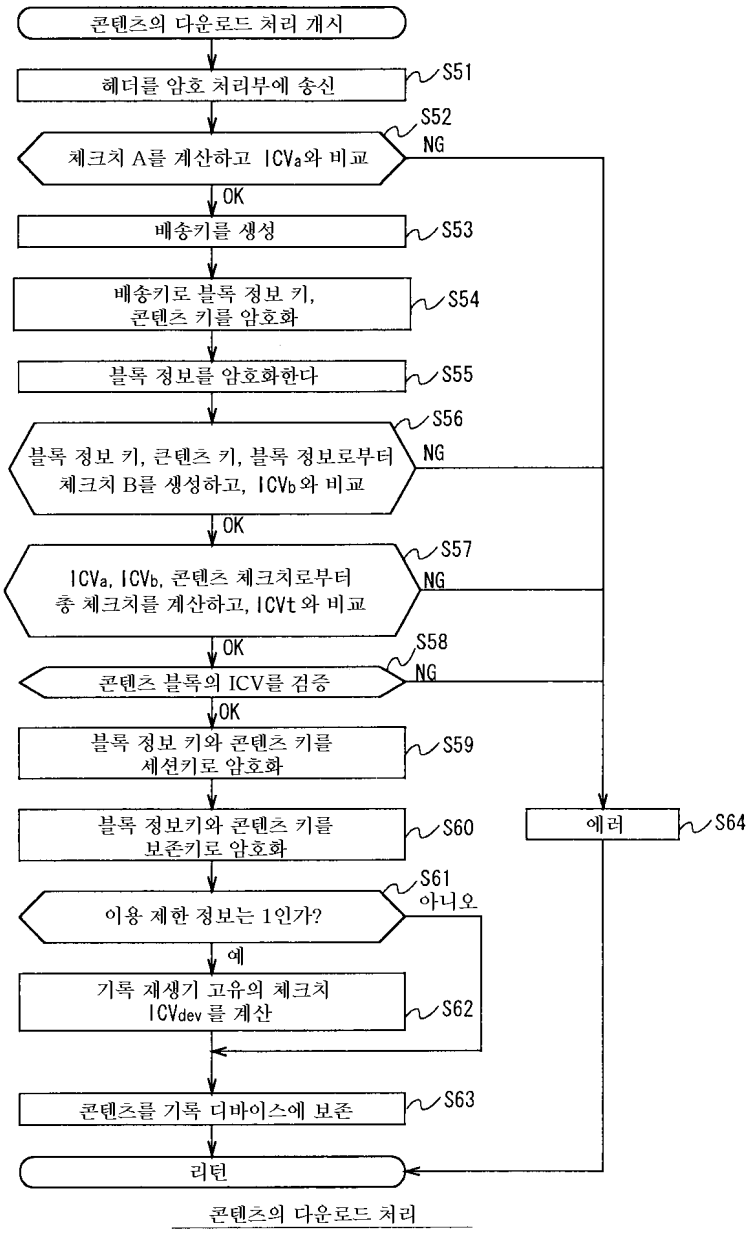


기록 재생기와 기록 디바이스의 상호 인증

도면21

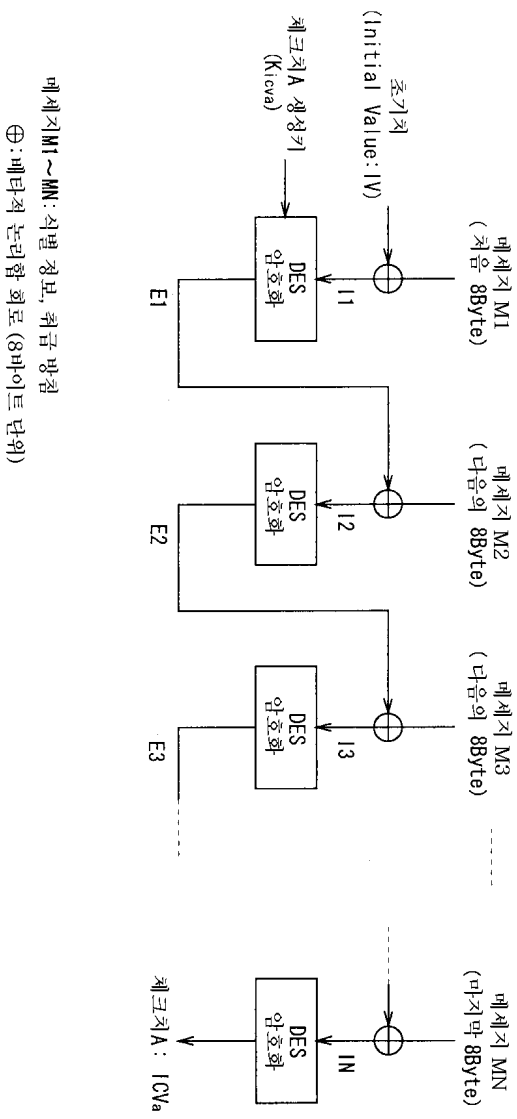

기록 재생기 1
2101
일본 지정 가능 블록 1、4
마스터 키 : MKake 1, 4
기록 디바이스 A
2104
키 블록 1
키 블록 2
키 블록 3
키 블록 4
외부 메모리
기록 재생기 2
2102
U S(미국) 지정 가능 블록2、4
마스터 키 : MKake 2, 4
기록 디바이스 B
2105
키 블록 1
키 블록 2
키 블록 3
키 블록 4
외부 메모리
기록 재생기 3
2103
E U(유럽) 지정 가능 블록3、4
마스터 키 : MKake 3, 4
기록 디바이스 C
2106
키 블록 1
키 블록 2
키 블록 3
키 블록 4
외부 메모리

도면22



콘텐츠의 다운로드 처리

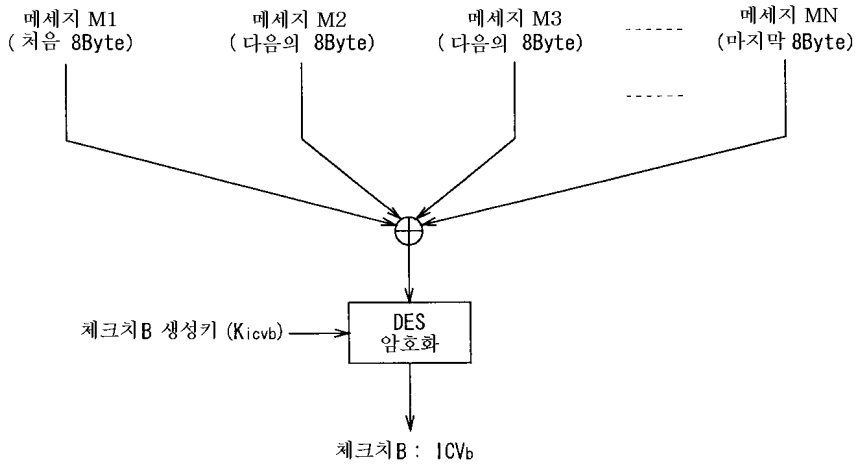
도면23



메세지M1~MN: 식별 정보, 취급 방침

⊕:베타적 논리합 회로 (8바이트 단위)

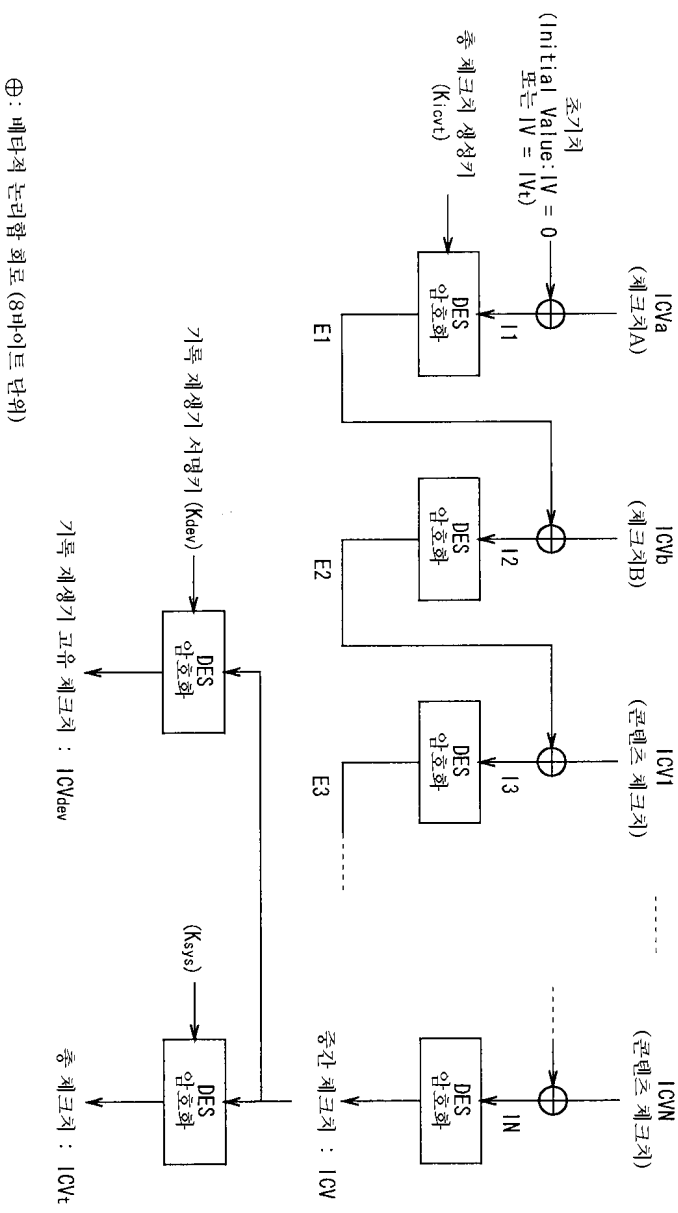
도면24



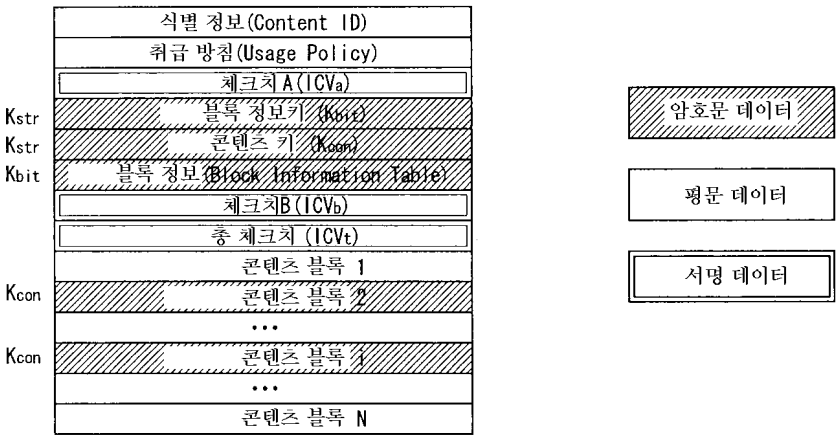
메세지M1～MN : 블록 정보 키 K_{bit}, 콘텐츠 키 K_{con}, 블록 정보

⊕ : 배타적 논리합 회로 (8바이트 단위)

도면25

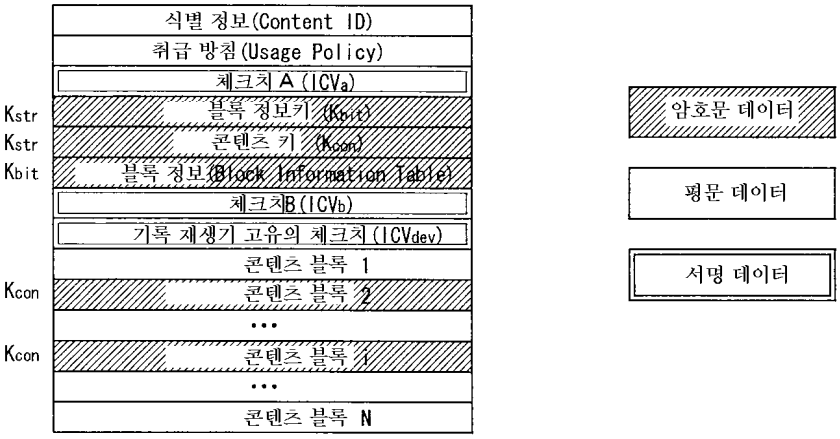

초기치
(Initial Value: IV = 0
또는 IV = IVt)
ICVa
(체크치A)
I1
DES
암호화
E1
ICVb
(체크치B)
I2
DES
암호화
E2
ICV1
(콘텐츠 체크치)
I3
DES
암호화
E3
ICVN
(콘텐츠 체크치)
IN
DES
암호화
중간 체크치 : ICV
총 체크치 생성키
(Kicvt)
기록 체생기 서명키 (Kdev)
DES
암호화
기록 체생기 고유 체크치 : ICVdev
(Ksys)
DES
암호화
총 체크치 : ICVt
⊕: 배타적 논리합 회로 (8바이트 단위)

도면26



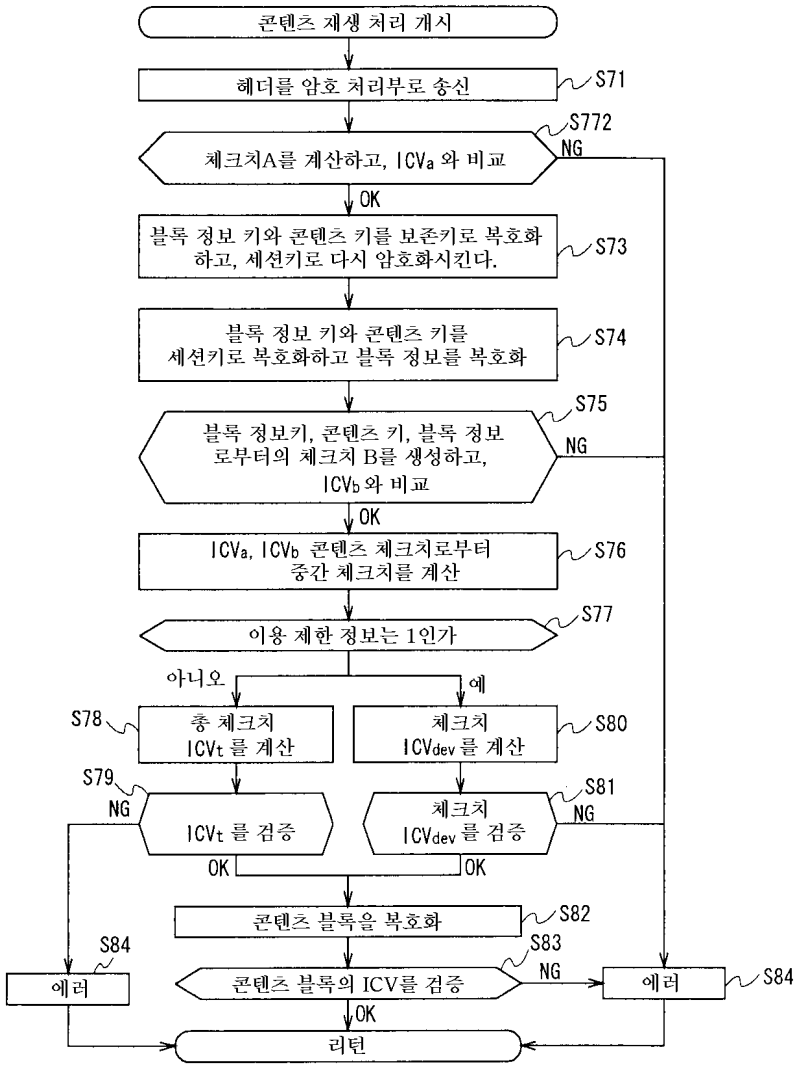
기록 디바이스에 보존된 콘텐츠
(기록 제한 정보 = 0)

도면27



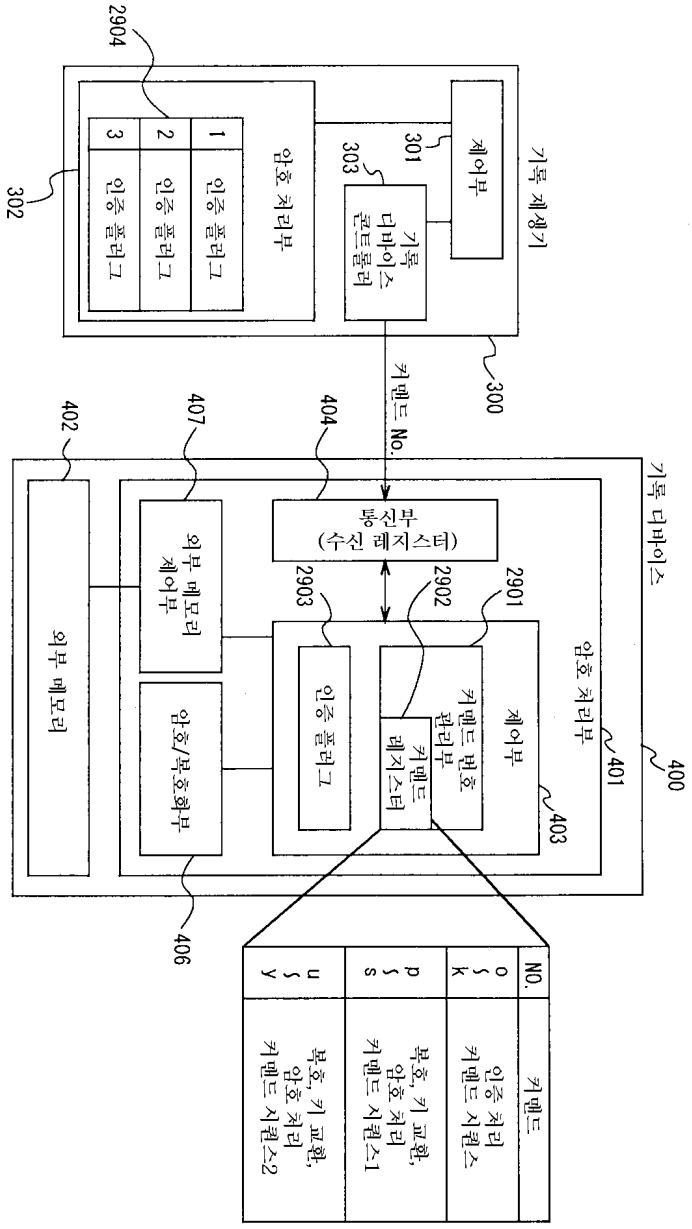
기록 디바이스에 보존된 콘텐츠
(기록 제한 정보 = 1)

도면28

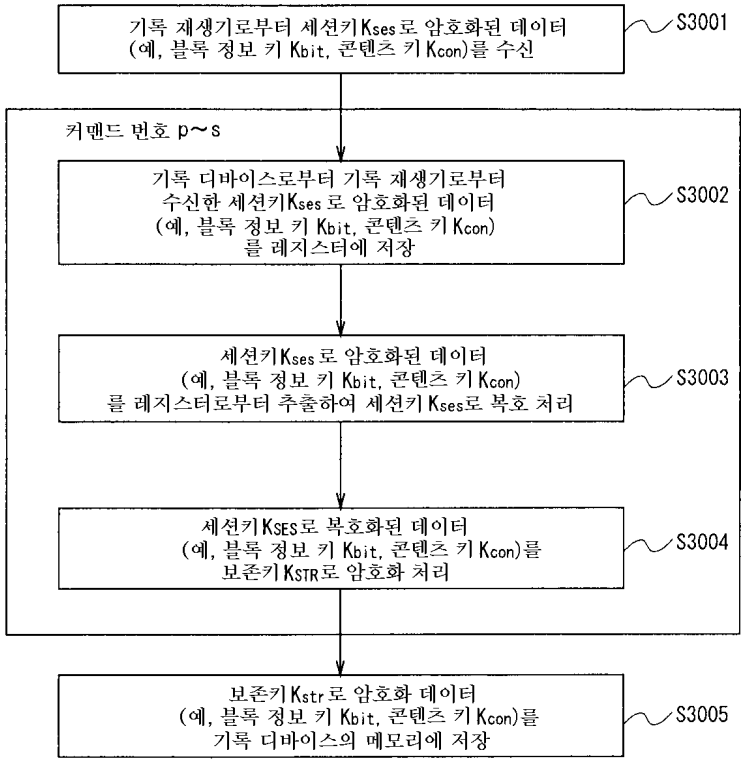


콘텐츠 재생 처리

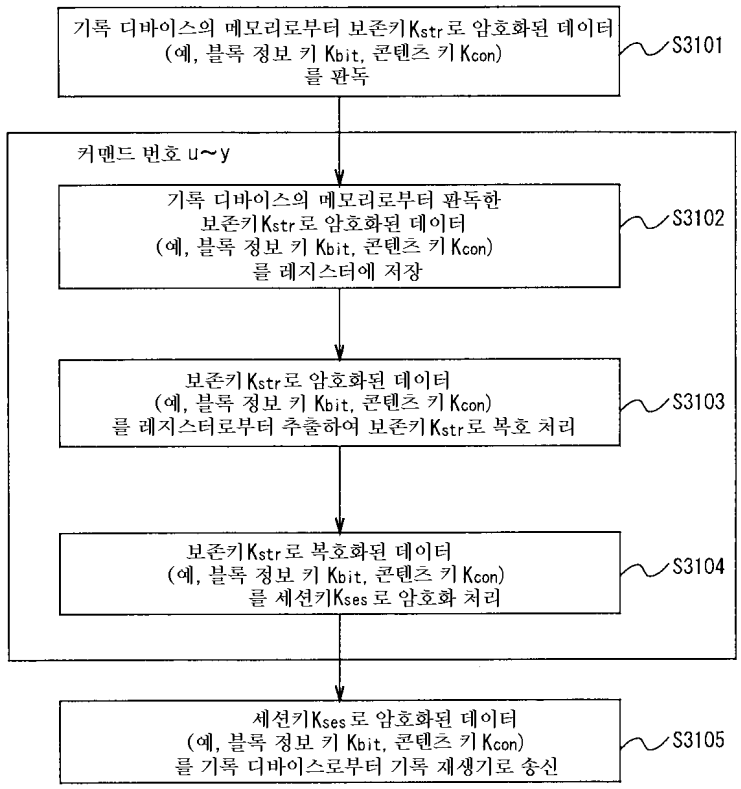
도면29


기록 재생기
제어부
301
303
기록 디바이스 콘트롤러
암호 처리부
2904
1 인증 플러그
2 인증 플러그
3 인증 플러그
302
300
커맨드 No.
기록 디바이스
402
407
404
외부 메모리
외부 메모리 제어부
통신부 (수신 레지스터)
2903
2902
2901
인증 플러그
커맨드 번호 관리부
커맨드 레지스터
제어부
403
암호 처리부
401
400
암호/복호화부
406
NO.
커맨드
0 ~ k
인증 처리 커맨드 시퀀스
p ~ s
복호, 키 교환, 암호 처리 커맨드 시퀀스1
u ~ y
복호, 키 교환, 암호 처리 커맨드 시퀀스2

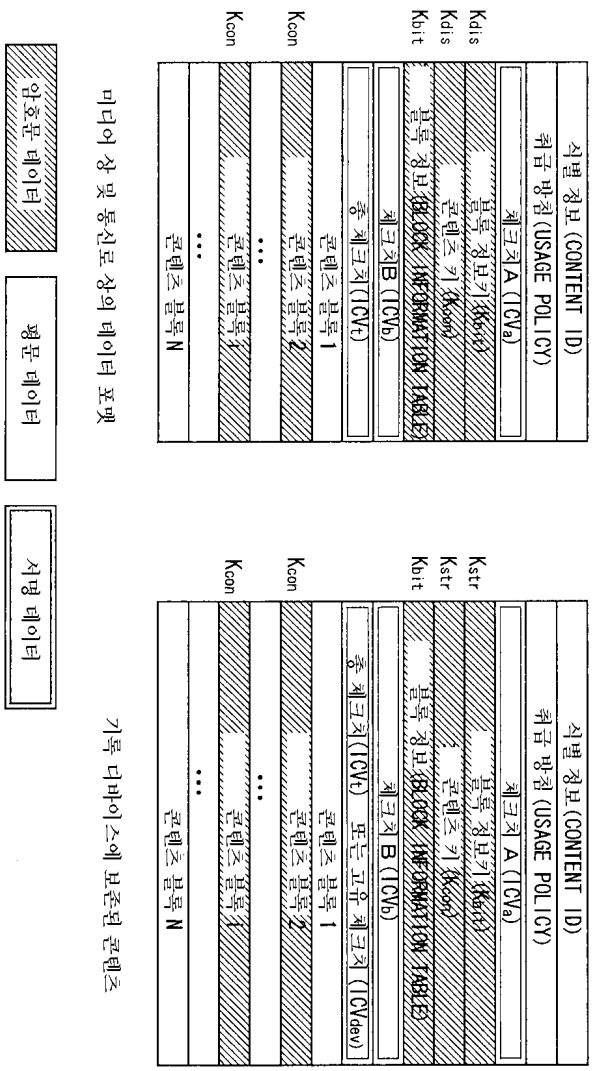
도면30


기록 재생기로부터 세션키 Kses로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)를 수신
S3001
커맨드 번호 p~s
기록 디바이스로부터 기록 재생기로부터
수신한 세션키 Kses로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 레지스터에 저장
S3002
세션키 Kses로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 레지스터로부터 추출하여 세션키 Kses로 복호 처리
S3003
세션키 KSES로 복호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)를
보존키 KSTR로 암호화 처리
S3004
보존키 Kstr로 암호화 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)를
기록 디바이스의 메모리에 저장
S3005

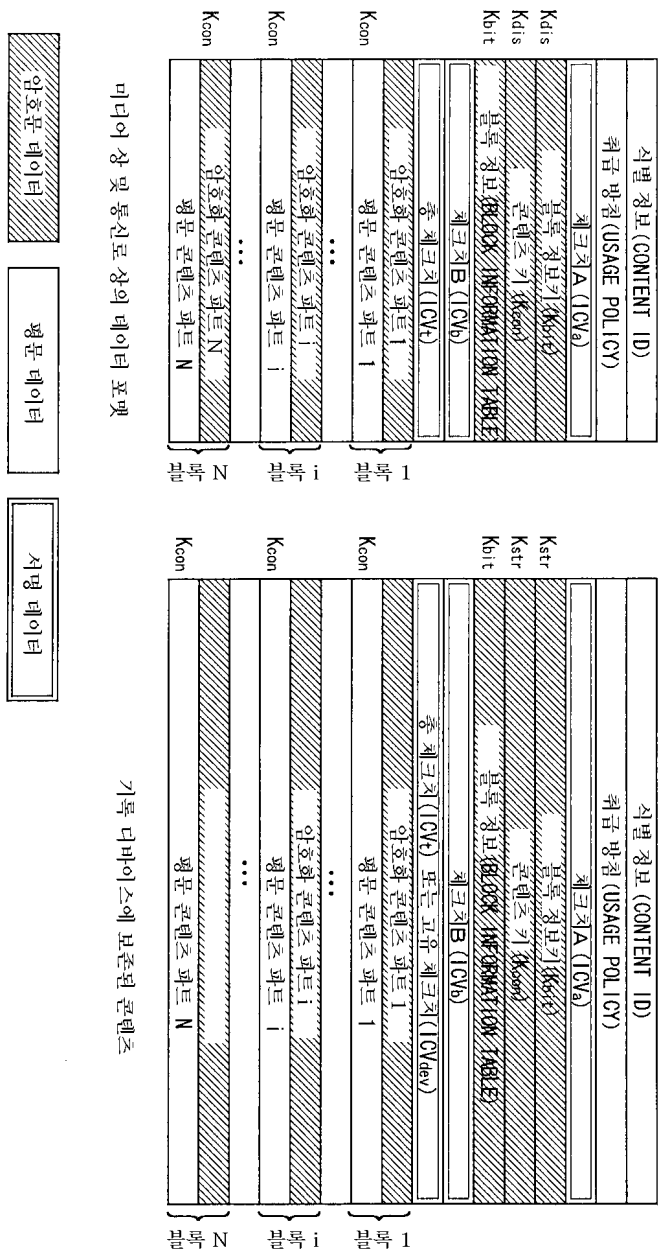
도면31


기록 디바이스의 메모리로부터 보존키 Kstr로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 판독
S3101
커맨드 번호 u~y
기록 디바이스의 메모리로부터 판독한
보존키 Kstr로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 레지스터에 저장
S3102
보존키 Kstr로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 레지스터로부터 추출하여 보존키 Kstr로 복호 처리
S3103
보존키 Kstr로 복호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 세션키 Kses로 암호화 처리
S3104
세션키 Kses로 암호화된 데이터
(예, 블록 정보 키 Kbit, 콘텐츠 키 Kcon)
를 기록 디바이스로부터 기록 재생기로 송신
S3105

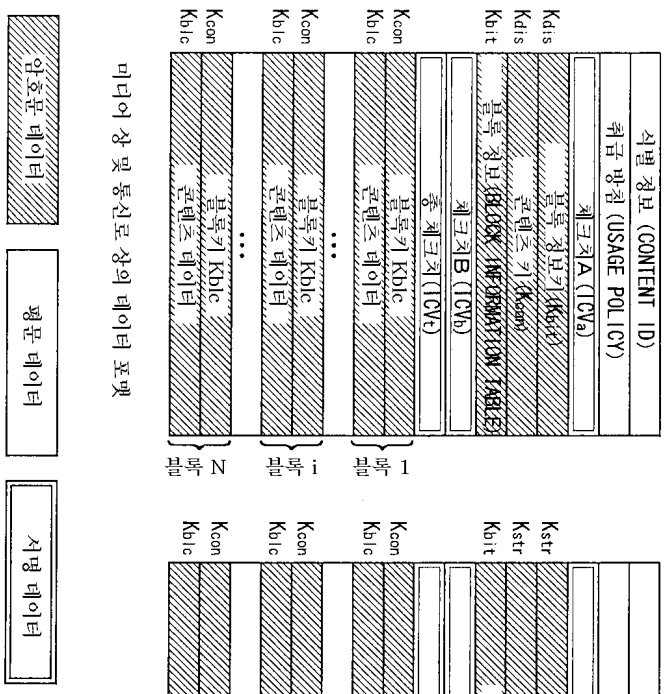
도면32


포맷 타입 0
식별 정보 (CONTENT ID)
취급 방침 (USAGE POLICY)
체크치A (ICVa)
블록 정보키 (Kstr)
콘텐츠 키 (Kcon)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
Kdis
Kdis
Kbit
총 체크치(ICVt)
콘텐츠 블록 1
콘텐츠 블록 2
콘텐츠 블록 N
Kcon
Kcon
Kcon
식별 정보(CONTENT ID)
취급 방침 (USAGE POLICY)
체크치 A (ICVa)
블록 정보키 (Kstr)
콘텐츠 키 (Kcon)
블록 정보 (BLOCK INFORMATION TABLE)
체크치 B (ICVb)
Kstr
Kstr
Kbit
총 체크치(ICVt) 또는 고유 체크치 (ICVdev)
콘텐츠 블록 1
콘텐츠 블록 2
콘텐츠 블록 N
Kcon
Kcon
Kcon
미디어 상 및 통신로 상의 데이터 포맷
기록 디바이스에 보존된 콘텐츠
암호문 데이터
평문 데이터
서명 데이터

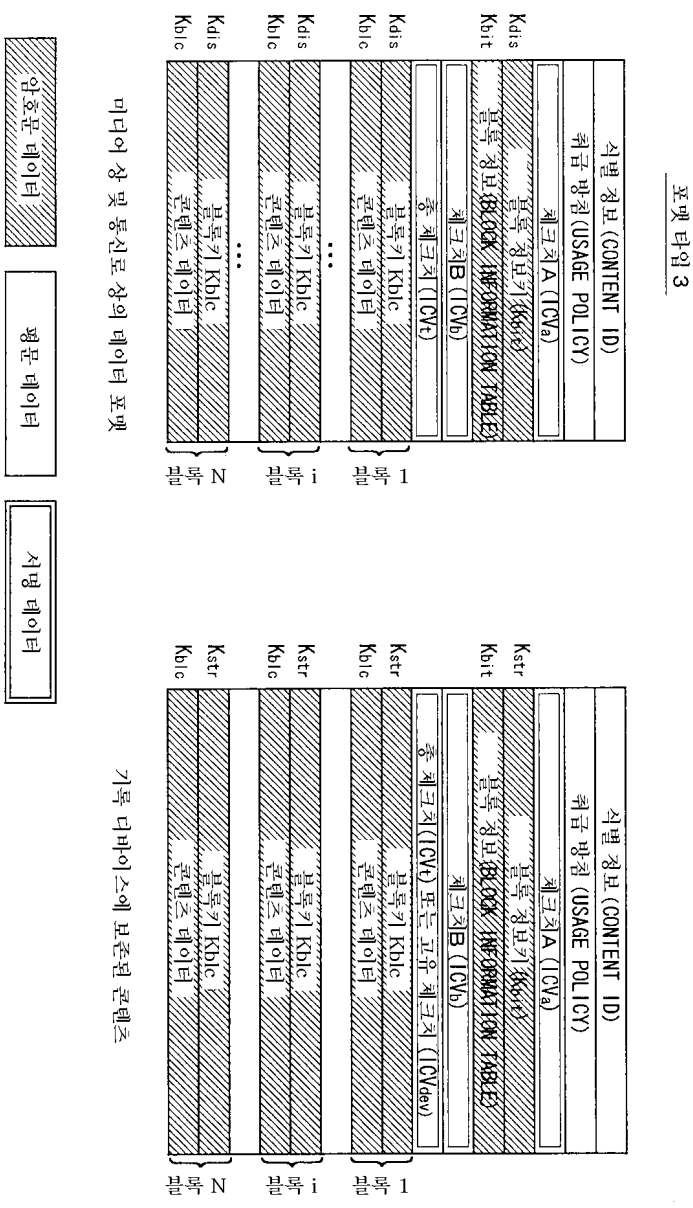
도면33


포맷 타입 1
식별 정보 (CONTENT ID)
권리 방침 (USAGE POLICY)
체크치A (ICVa)
부분 정보키 (Kstr)
콘텐츠키 (Kcon)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
총 체크치 (ICVt)
암호화 콘텐츠 파트 1
평문 콘텐츠 파트 1
암호화 콘텐츠 파트 i
평문 콘텐츠 파트 i
암호화 콘텐츠 파트 N
평문 콘텐츠 파트 N
Kdis
Kdis
Kbit
Kcon
Kcon
Kcon
블록 N
블록 i
블록 1
미디어 상 및 통신로 상의 데이터 포맷
식별 정보 (CONTENT ID)
권리 방침 (USAGE POLICY)
체크치A (ICVa)
부분 정보키 (Kstr)
콘텐츠키 (Kcon)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
총 체크치 (ICVt) 또는 고유 체크치 (ICVdev)
암호화 콘텐츠 파트 1
평문 콘텐츠 파트 1
암호화 콘텐츠 파트 i
평문 콘텐츠 파트 i
평문 콘텐츠 파트 N
Kstr
Kstr
Kbit
Kcon
Kcon
Kcon
블록 N
블록 i
블록 1
기록 디바이스에 보존된 콘텐츠
암호문 데이터
평문 데이터
서명 데이터

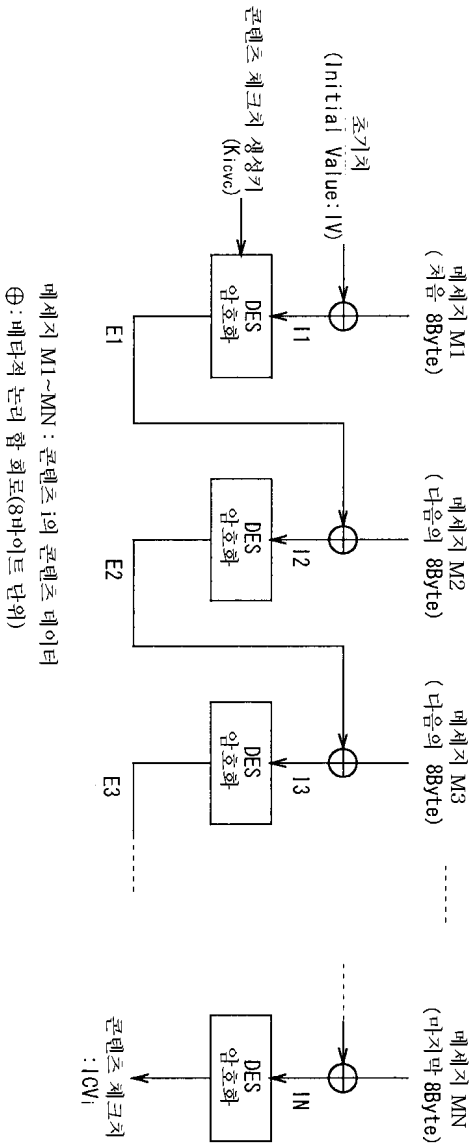
도면34


포맷 타입 2
식별 정보 (CONTENT ID)
취급 방침 (USAGE POLICY)
체크치A (ICVa)
블록 정보키 (Kblk)
콘텐츠 키 (Kcon)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
총 체크치 (ICVt)
블록키 Kblc
콘텐츠 데이터
블록 1
블록 i
블록 N
미디어 상 및 통신로 상의 데이터 포맷
기록 디바이스에 보존된 콘텐츠
암호문 데이터
평문 데이터
서명 데이터

도면35

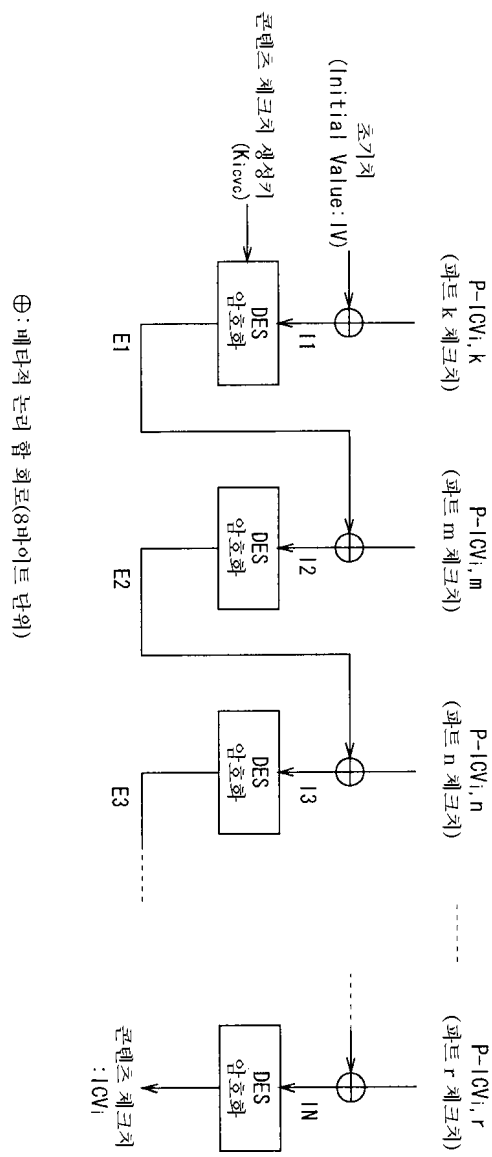

포맷 타입 3
식별 정보 (CONTENT ID)
권급 방침 (USAGE POLICY)
체크치A (ICVa)
블록 정보키 (Kbiv)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
Kdis
Kbit
Kdis
Kblc
블록키 Kblc
콘텐츠 데이터
총 체크치 (ICVt)
Kdis
Kblc
블록키 Kblc
콘텐츠 데이터
...
Kdis
Kblc
블록키 Kblc
콘텐츠 데이터
Kdis
Kblc
블록키 Kblc
콘텐츠 데이터
블록 N
블록 i
블록 1
미디어 상 및 통신로 상의 데이터 포맷
식별 정보 (CONTENT ID)
권급 방침 (USAGE POLICY)
체크치A (ICVa)
블록 정보키 (Kbiv)
블록 정보 (BLOCK INFORMATION TABLE)
체크치B (ICVb)
Kstr
Kbit
Kstr
Kblc
블록키 Kblc
콘텐츠 데이터
총 체크치 (ICVt) 또는 고유 체크치 (ICVdev)
Kstr
Kblc
블록키 Kblc
콘텐츠 데이터
...
Kstr
Kblc
블록키 Kblc
콘텐츠 데이터
Kstr
Kblc
블록키 Kblc
콘텐츠 데이터
블록 N
블록 i
블록 1
기록 디바이스에 보존된 콘텐츠
암호문 데이터
평문 데이터
서명 데이터

도면36

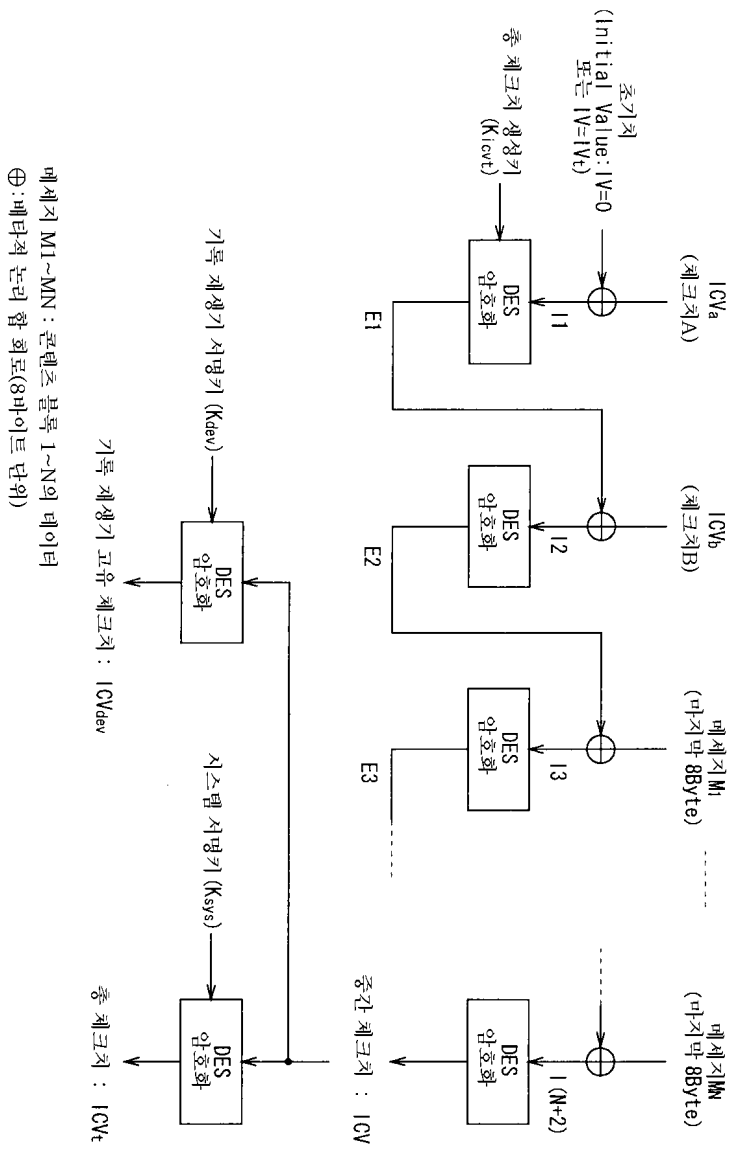


메세지 M1~MN : 콘텐츠 i의 콘텐츠 데이터
⊕ : 배타적 논리 합 회로(8바이트 단위)

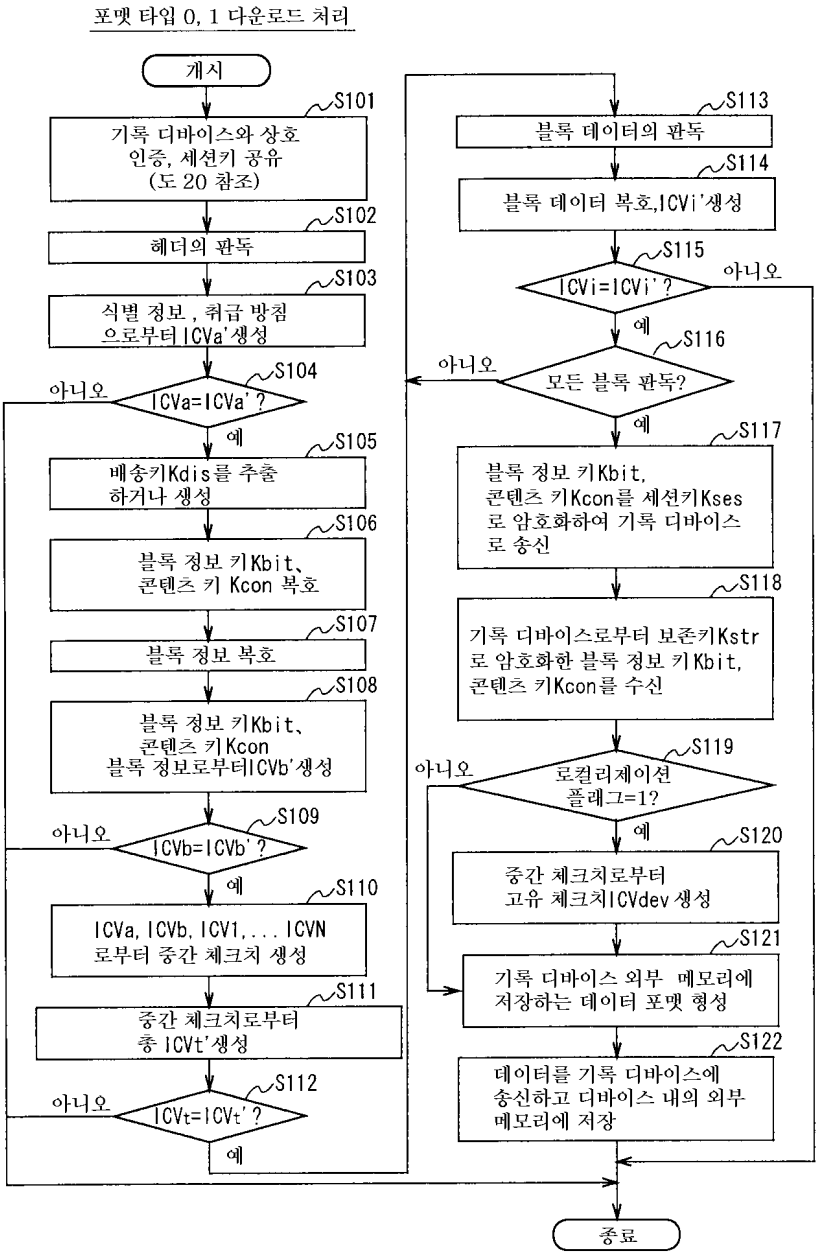
도면37


초기치
(Initial Value:IV)
콘텐츠 체크치 생성키
(Kicvc)
P-ICVi,k
(파트 k 체크치)
P-ICVi,m
(파트 m 체크치)
P-ICVi,n
(파트 n 체크치)
P-ICVi,r
(파트 r 체크치)
DES
암호화
I1
I2
I3
IN
E1
E2
E3
콘텐츠 체크치
:ICVi
⊕ : 배타적 논리 합 회로(8바이트 단위)

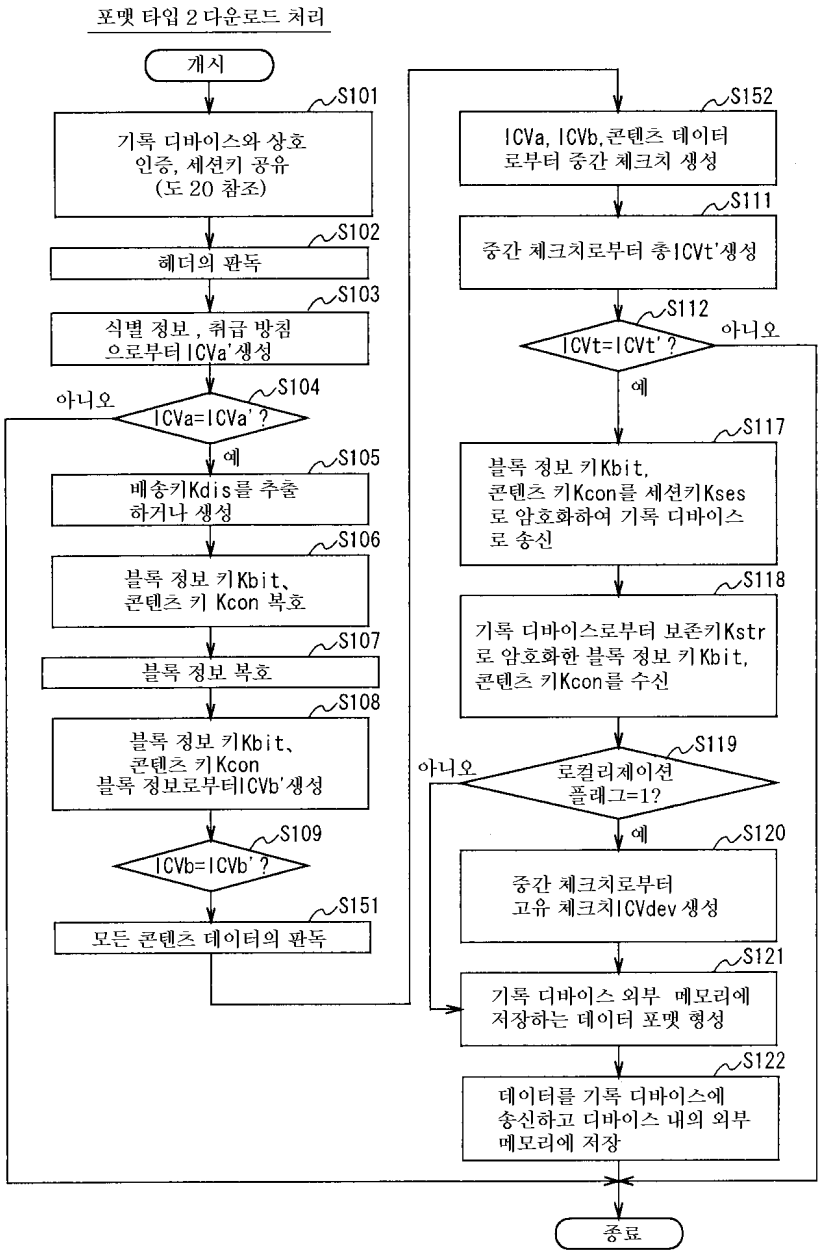
도면38


ICVa
(체크치A)
초기치
(Initial Value:IV=0
또는 IV=IVt)
중 체크치 생성키
(Kicvt)
DES
암호화
I1
E1
ICVb
(체크치B)
DES
암호화
I2
E2
메세지 M1
(마지막 8Byte)
DES
암호화
I3
E3
메세지 MN
(마지막 8Byte)
DES
암호화
I (N+2)
중간 체크치 : ICV
기록 재생기 서명키 (Kdev)
DES
암호화
기록 재생기 고유 체크치 : ICVdev
시스템 서명키 (Ksys)
DES
암호화
중 체크치 : ICVt
메세지 M1~MN : 콘텐츠 블록 1~N의 데이터
⊕ : 배타적 논리 합 회로(8바이트 단위)

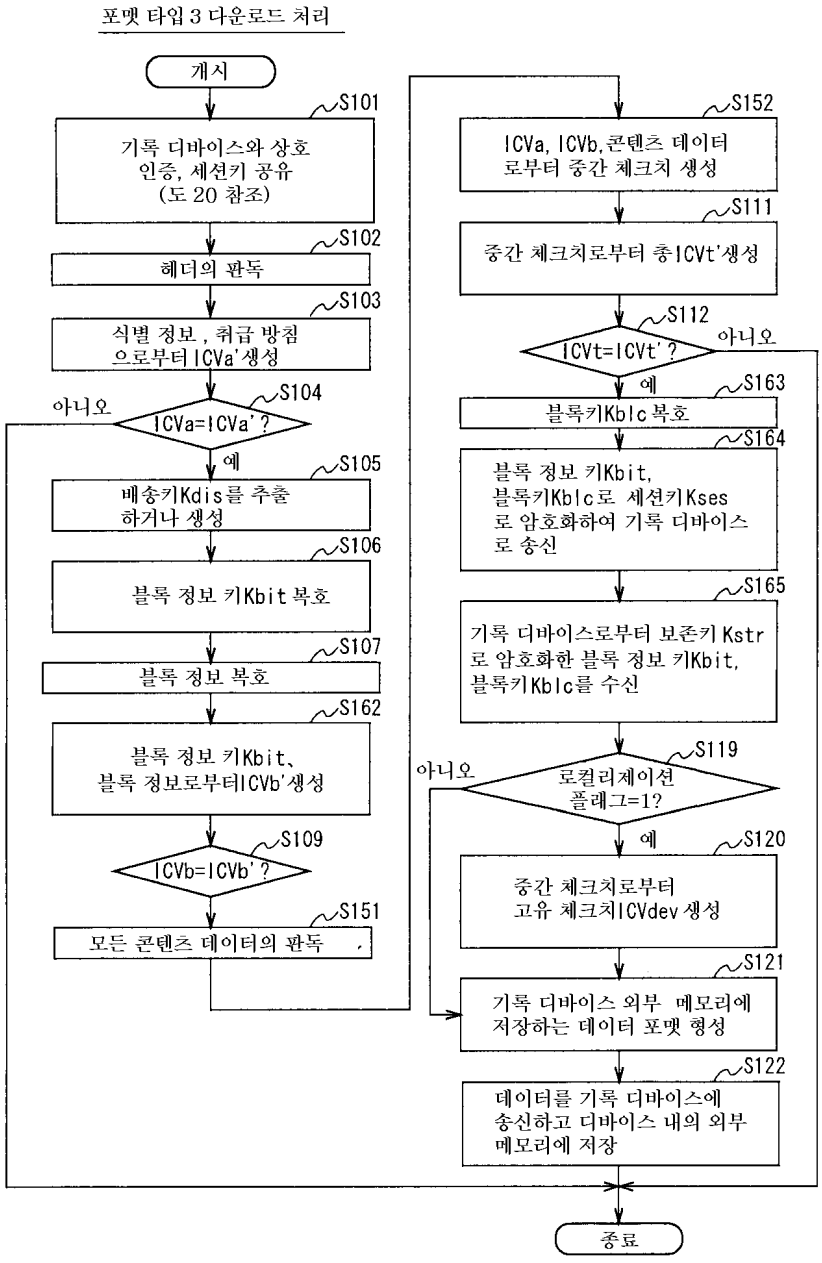
도면39


포맷 타입 0, 1 다운로드 처리
개시
S101
기록 디바이스와 상호 인증, 세션키 공유 (도 20 참조)
S102
헤더의 판독
S103
식별 정보, 취급 방침으로부터 ICVa'생성
S104
ICVa=ICVa'?
아니오
예
S105
배송키Kdis를 추출하거나 생성
S106
블록 정보 키Kbit, 콘텐츠 키 Kcon 복호
S107
블록 정보 복호
S108
블록 정보 키Kbit, 콘텐츠 키Kcon 블록 정보로부터ICVb'생성
S109
ICVb=ICVb'?
아니오
예
S110
ICVa, ICVb, ICV1, . . . ICVN 로부터 중간 체크치 생성
S111
중간 체크치로부터 총 ICVt'생성
S112
ICVt=ICVt'?
아니오
예
S113
블록 데이터의 판독
S114
블록 데이터 복호,ICVi'생성
S115
ICVi=ICVi'?
아니오
예
S116
모든 블록 판독?
아니오
예
S117
블록 정보 키Kbit, 콘텐츠 키Kcon를 세션키Kses로 암호화하여 기록 디바이스로 송신
S118
기록 디바이스로부터 보존키Kstr로 암호화한 블록 정보 키Kbit, 콘텐츠 키Kcon를 수신
S119
로컬리제이션 플래그=1?
아니오
예
S120
중간 체크치로부터 고유 체크치ICVdev 생성
S121
기록 디바이스 외부 메모리에 저장하는 데이터 포맷 형성
S122
데이터를 기록 디바이스에 송신하고 디바이스 내의 외부 메모리에 저장
종료

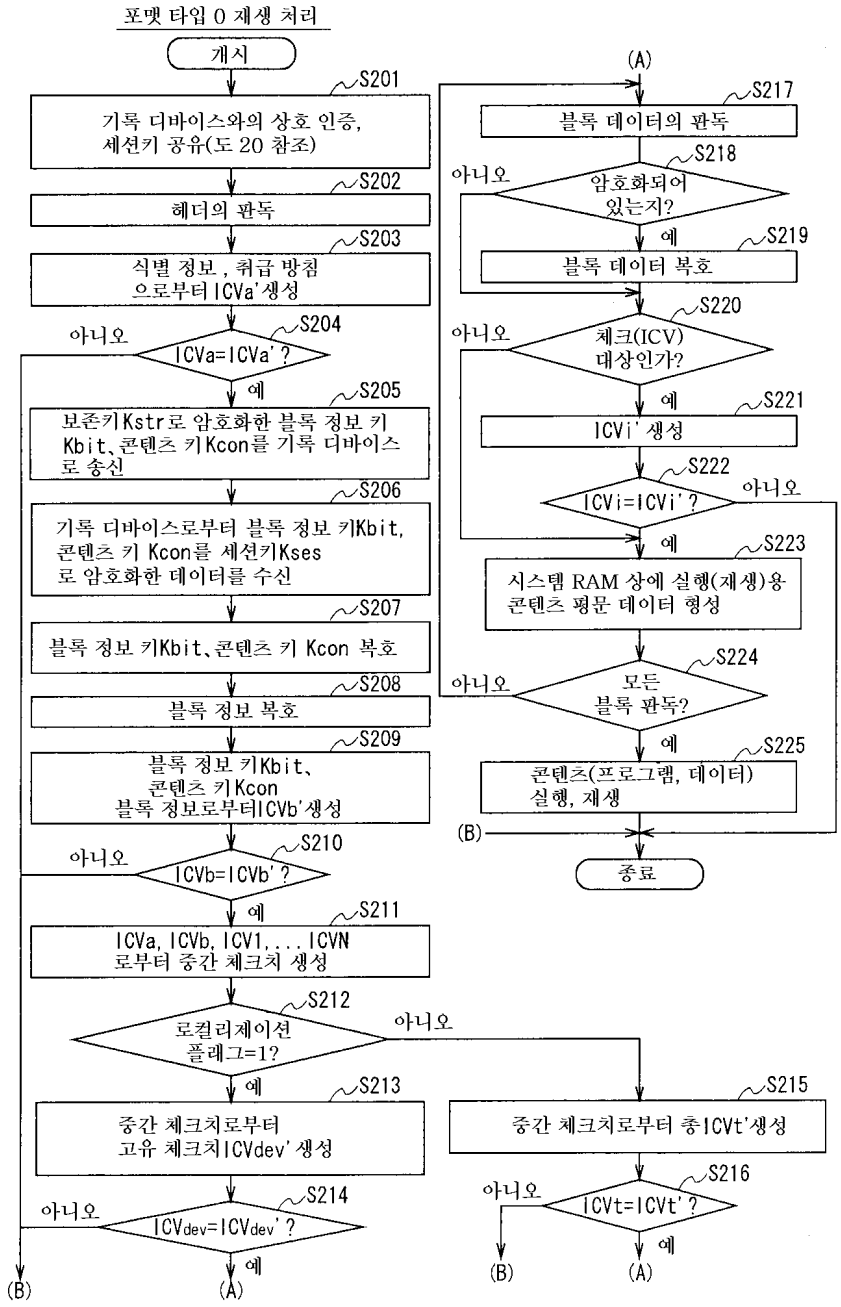
도면40


포맷 타입 2 다운로드 처리
개시
S101
기록 디바이스와 상호 인증, 세션키 공유 (도 20 참조)
S102
헤더의 판독
S103
식별 정보 , 취급 방침으로부터 ICVa'생성
S104
ICVa=ICVa' ?
아니오
예
S105
배송키Kdis를 추출하거나 생성
S106
블록 정보 키Kbit、콘텐츠 키 Kcon 복호
S107
블록 정보 복호
S108
블록 정보 키Kbit、콘텐츠 키Kcon 블록 정보로부터ICVb'생성
S109
ICVb=ICVb' ?
S151
모든 콘텐츠 데이터의 판독
S152
ICVa, ICVb,콘텐츠 데이터로부터 중간 체크치 생성
S111
중간 체크치로부터 총ICVt'생성
S112
ICVt=ICVt' ?
아니오
예
S117
블록 정보 키Kbit, 콘텐츠 키Kcon를 세션키Kses로 암호화하여 기록 디바이스로 송신
S118
기록 디바이스로부터 보존키Kstr로 암호화한 블록 정보 키Kbit, 콘텐츠 키Kcon를 수신
S119
로컬리제이션 플래그=1?
아니오
예
S120
중간 체크치로부터 고유 체크치ICVdev 생성
S121
기록 디바이스 외부 메모리에 저장하는 데이터 포맷 형성
S122
데이터를 기록 디바이스에 송신하고 디바이스 내의 외부 메모리에 저장
종료

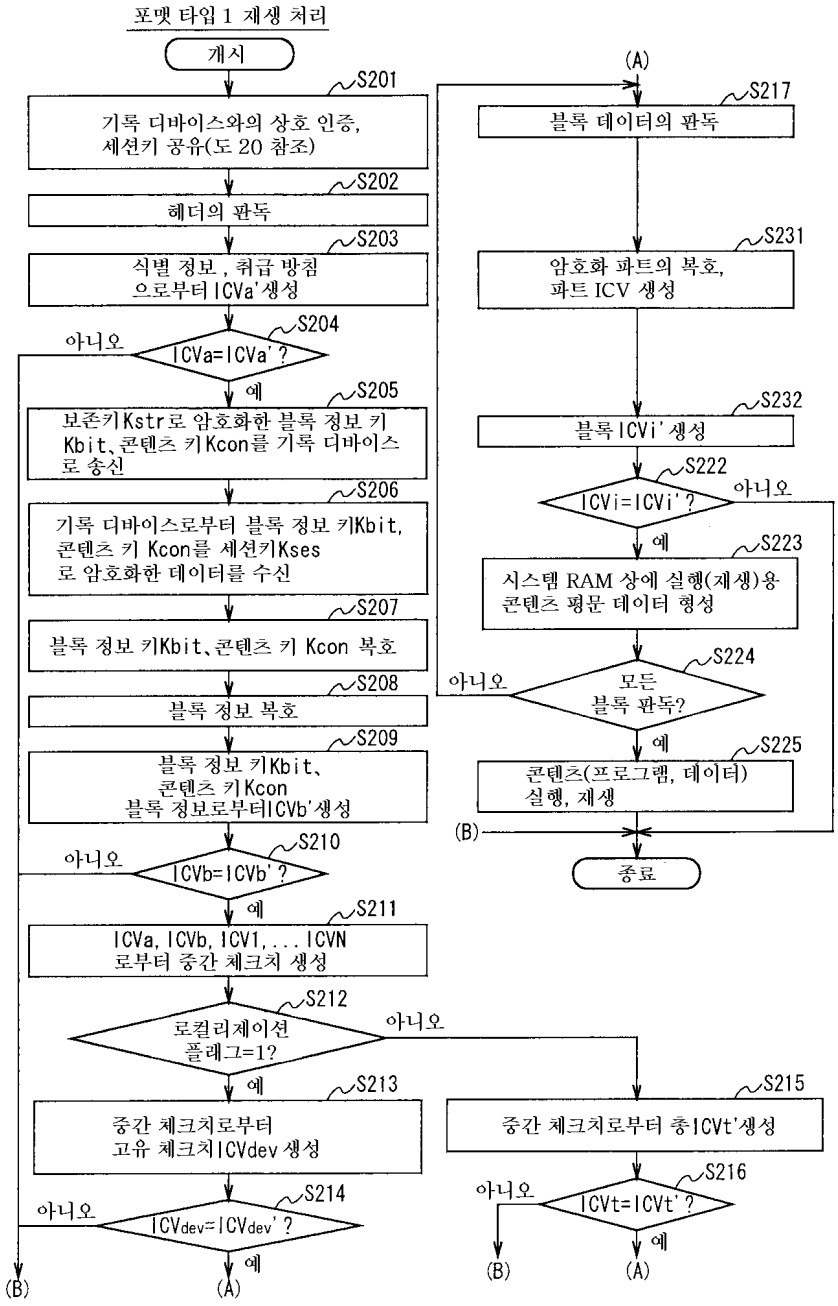
도면41


포맷 타입 3 다운로드 처리
개시
S101
기록 디바이스와 상호 인증, 세션키 공유 (도 20 참조)
S102
헤더의 판독
S103
식별 정보, 취급 방침으로부터 ICVa'생성
S104
아니오
ICVa=ICVa'?
예
S105
배송키Kdis를 추출하거나 생성
S106
블록 정보 키Kbit 복호
S107
블록 정보 복호
S162
블록 정보 키Kbit, 블록 정보로부터ICVb'생성
S109
ICVb=ICVb'?
S151
모든 콘텐츠 데이터의 판독
S152
ICVa, ICVb,콘텐츠 데이터로부터 중간 체크치 생성
S111
중간 체크치로부터 총ICVt'생성
S112
ICVt=ICVt'?
아니오
예
S163
블록키Kblc 복호
S164
블록 정보 키Kbit, 블록키Kblc로 세션키Kses로 암호화하여 기록 디바이스로 송신
S165
기록 디바이스로부터 보존키 Kstr로 암호화한 블록 정보 키Kbit, 블록키Kblc를 수신
S119
아니오
로컬리제이션 플래그=1?
예
S120
중간 체크치로부터 고유 체크치ICVdev 생성
S121
기록 디바이스 외부 메모리에 저장하는 데이터 포맷 형성
S122
데이터를 기록 디바이스에 송신하고 디바이스 내의 외부 메모리에 저장
종료

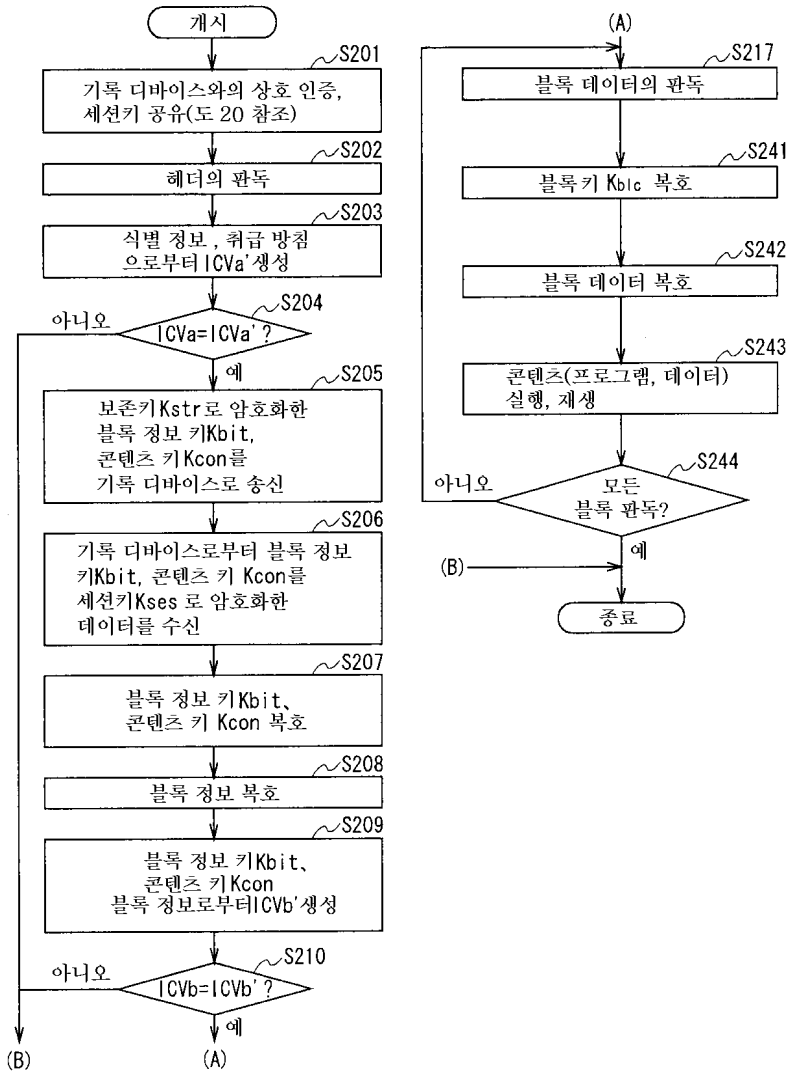
도면42


포맷 타입 0 재생 처리
개시
S201
기록 디바이스와의 상호 인증,
세션키 공유(도 20 참조)
S202
헤더의 판독
S203
식별 정보, 취급 방침
으로부터 ICVa'생성
S204
아니오
ICVa=ICVa'?
예
S205
보존키Kstr로 암호화한 블록 정보 키
Kbit, 콘텐츠 키Kcon를 기록 디바이스
로 송신
S206
기록 디바이스로부터 블록 정보 키Kbit,
콘텐츠 키 Kcon를 세션키Kses
로 암호화한 데이터를 수신
S207
블록 정보 키Kbit, 콘텐츠 키 Kcon 복호
S208
블록 정보 복호
S209
블록 정보 키Kbit,
콘텐츠 키Kcon
블록 정보로부터ICVb'생성
S210
아니오
ICVb=ICVb'?
예
S211
ICVa, ICVb, ICV1, . . . ICVN
로부터 중간 체크치 생성
S212
로컬리제이션
플래그=1?
아니오
예
S213
중간 체크치로부터
고유 체크치ICVdev'생성
S214
아니오
ICVdev=ICVdev'?
예
(B)
(A)
S215
중간 체크치로부터 총ICVt'생성
S216
아니오
ICVt=ICVt'?
예
(B)
(A)
(A)
S217
블록 데이터의 판독
S218
아니오
암호화되어
있는지?
예
S219
블록 데이터 복호
S220
아니오
체크(ICV)
대상인가?
예
S221
ICVi' 생성
S222
ICVi=ICVi'?
아니오
예
S223
시스템 RAM 상에 실행(재생)용
콘텐츠 평문 데이터 형성
S224
아니오
모든
블록 판독?
예
S225
콘텐츠(프로그램, 데이터)
실행, 재생
(B)
종료

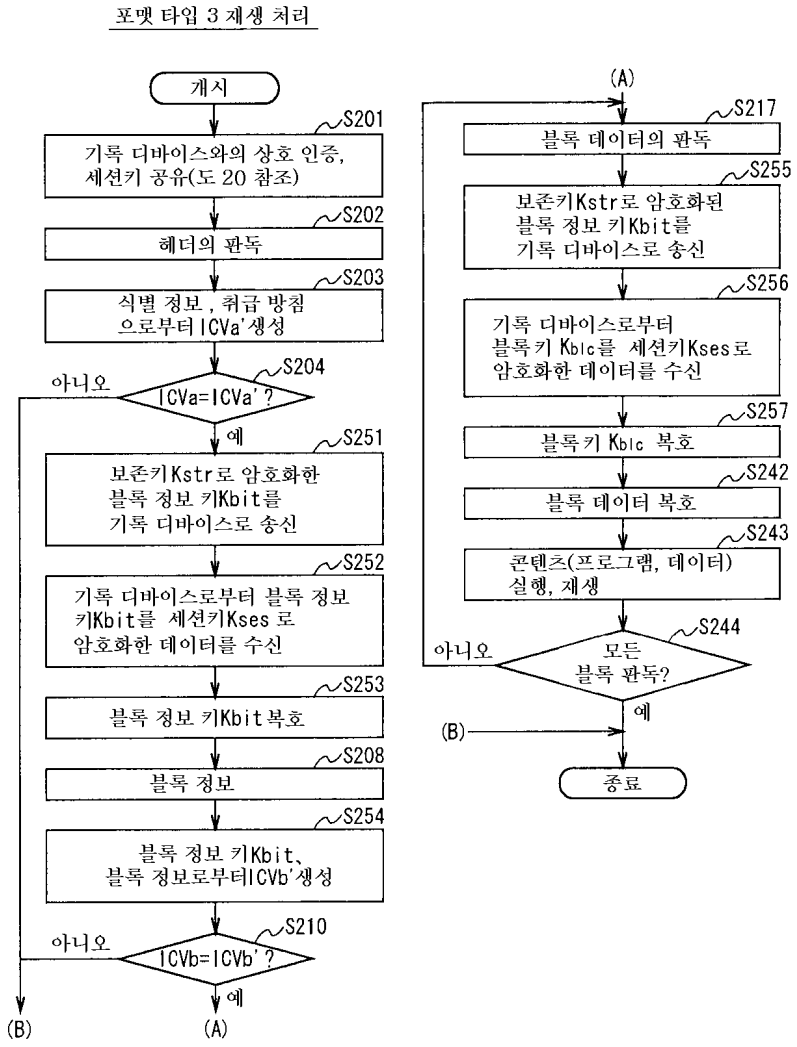
도면43


포맷 타입 1 재생 처리
개시
S201
기록 디바이스와의 상호 인증,
세션키 공유(도 20 참조)
S202
헤더의 판독
S203
식별 정보 , 취급 방침
으로부터 ICVa'생성
S204
아니오
ICVa=ICVa' ?
예
S205
보존키Kstr로 암호화한 블록 정보 키
Kbit、콘텐츠 키Kcon를 기록 디바이스
로 송신
S206
기록 디바이스로부터 블록 정보 키Kbit,
콘텐츠 키 Kcon를 세션키Kses
로 암호화한 데이터를 수신
S207
블록 정보 키Kbit、콘텐츠 키 Kcon 복호
S208
블록 정보 복호
S209
블록 정보 키Kbit、
콘텐츠 키Kcon
블록 정보로부터ICVb'생성
S210
아니오
ICVb=ICVb' ?
예
S211
ICVa, ICVb, ICV1, . . . ICVN
로부터 중간 체크치 생성
S212
로컬리제이션
플래그=1?
아니오
예
S213
중간 체크치로부터
고유 체크치ICVdev 생성
S214
아니오
ICVdev=ICVdev' ?
예
(B)
(A)
(A)
S217
블록 데이터의 판독
S231
암호화 파트의 복호,
파트 ICV 생성
S232
블록ICVi' 생성
S222
ICVi=ICVi' ?
아니오
예
S223
시스템 RAM 상에 실행(재생)용
콘텐츠 평문 데이터 형성
S224
아니오
모든
블록 판독?
예
S225
콘텐츠(프로그램, 데이터)
실행, 재생
(B)
종료
S215
중간 체크치로부터 총ICVt'생성
S216
아니오
ICVt=ICVt' ?
예
(B)
(A)

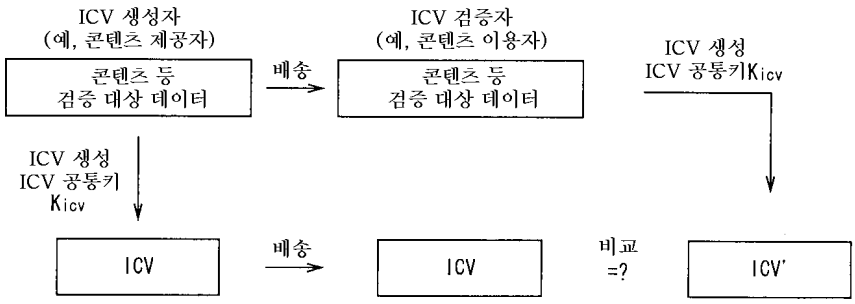
도면44


개시
S201
기록 디바이스와의 상호 인증,
세션키 공유(도 20 참조)
S202
헤더의 판독
S203
식별 정보, 취급 방침
으로부터 ICVa'생성
S204
아니오
ICVa=ICVa'?
예
S205
보존키 Kstr로 암호화한
블록 정보 키Kbit,
콘텐츠 키Kcon를
기록 디바이스로 송신
S206
기록 디바이스로부터 블록 정보
키Kbit, 콘텐츠 키 Kcon를
세션키Kses 로 암호화한
데이터를 수신
S207
블록 정보 키Kbit、
콘텐츠 키 Kcon 복호
S208
블록 정보 복호
S209
블록 정보 키Kbit、
콘텐츠 키Kcon
블록 정보로부터ICVb'생성
S210
아니오
ICVb=ICVb'?
예
(B)
(A)
(A)
S217
블록 데이터의 판독
S241
블록키 Kblc 복호
S242
블록 데이터 복호
S243
콘텐츠(프로그램, 데이터)
실행, 재생
S244
아니오
모든
블록 판독?
(B)
예
종료

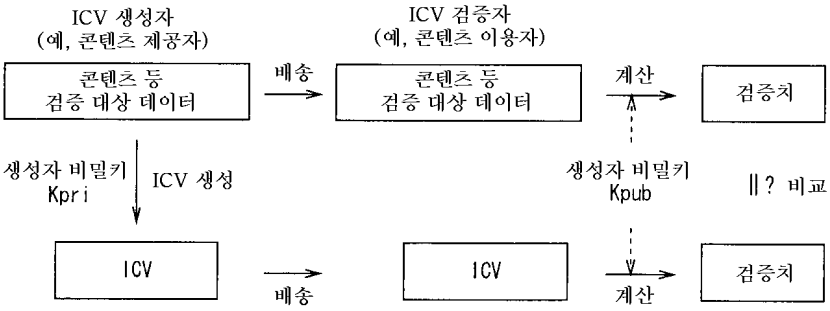
도면45


포맷 타입 3 재생 처리
개시
S201
기록 디바이스와의 상호 인증,
세션키 공유(도 20 참조)
S202
헤더의 판독
S203
식별 정보, 취급 방침
으로부터 ICVa'생성
S204
아니오
ICVa=ICVa'?
예
S251
보존키Kstr로 암호화한
블록 정보 키Kbit를
기록 디바이스로 송신
S252
기록 디바이스로부터 블록 정보
키Kbit를 세션키Kses로
암호화한 데이터를 수신
S253
블록 정보 키Kbit복호
S208
블록 정보
S254
블록 정보 키Kbit,
블록 정보로부터ICVb'생성
S210
아니오
ICVb=ICVb'?
예
(B)
(A)
(A)
S217
블록 데이터의 판독
S255
보존키Kstr로 암호화된
블록 정보 키Kbit를
기록 디바이스로 송신
S256
기록 디바이스로부터
블록키 Kblc를 세션키Kses로
암호화한 데이터를 수신
S257
블록키 Kblc 복호
S242
블록 데이터 복호
S243
콘텐츠(프로그램, 데이터)
실행, 재생
S244
아니오
모든
블록 판독?
예
(B)
종료

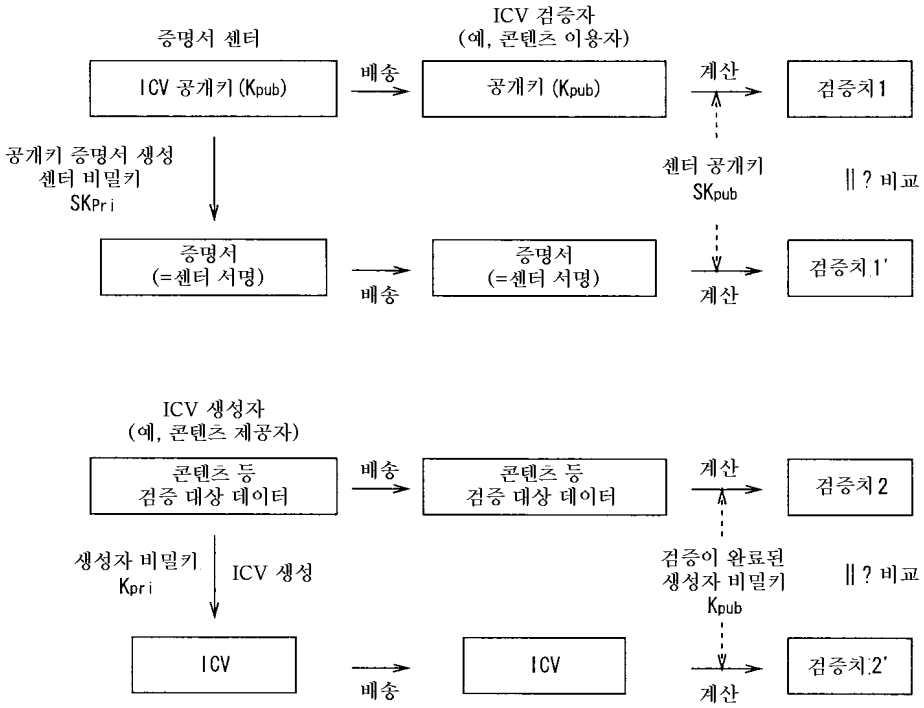
도면46


ICV 생성자
(예, 콘텐츠 제공자)
콘텐츠 등
검증 대상 데이터
배송
ICV 검증자
(예, 콘텐츠 이용자)
콘텐츠 등
검증 대상 데이터
ICV 생성
ICV 공통키Kicv
ICV 생성
ICV 공통키
Kicv
ICV
배송
ICV
비교
=?
ICV'

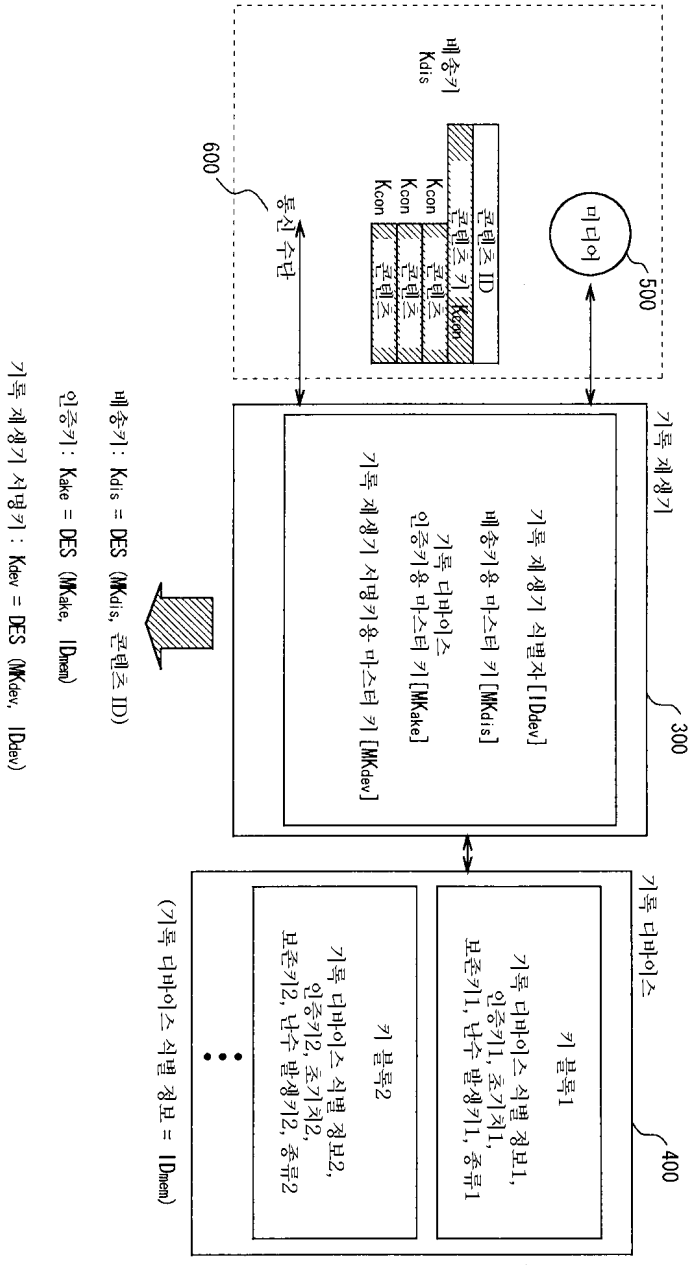
도면47


ICV 생성자
(예, 콘텐츠 제공자)
콘텐츠 등
검증 대상 데이터
배송
ICV 검증자
(예, 콘텐츠 이용자)
콘텐츠 등
검증 대상 데이터
계산
검증치
생성자 비밀키
Kpri
ICV 생성
생성자 비밀키
Kpub
‖ ? 비교
ICV
배송
ICV
계산
검증치

도면48


증명서 센터
ICV 공개키 (Kpub)
배송
ICV 검증자
(예, 콘텐츠 이용자)
공개키 (Kpub)
계산
검증치1
공개키 증명서 생성
센터 비밀키
SKPri
센터 공개키
SKpub
‖ ? 비교
증명서
(=센터 서명)
배송
증명서
(=센터 서명)
계산
검증치1'
ICV 생성자
(예, 콘텐츠 제공자)
콘텐츠 등
검증 대상 데이터
배송
콘텐츠 등
검증 대상 데이터
계산
검증치2
생성자 비밀키
Kpri
ICV 생성
검증이 완료된
생성자 비밀키
Kpub
‖ ? 비교
ICV
배송
ICV
계산
검증치2'

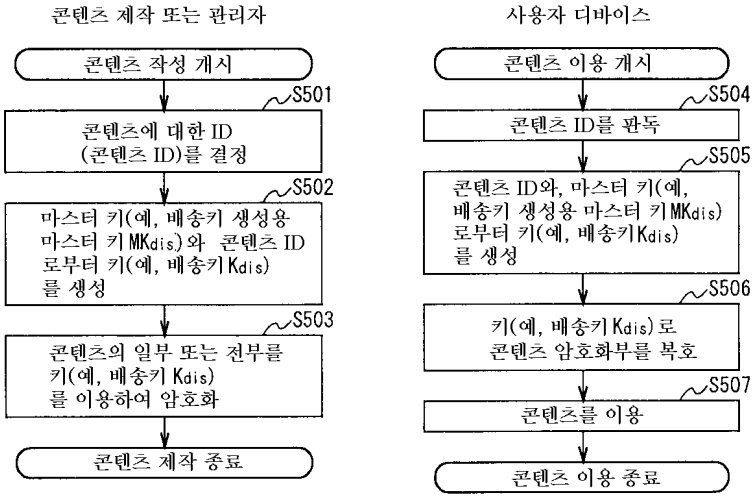
도면49


미디어
500
콘텐츠 ID
콘텐츠 키 Kcon
콘텐츠
Kcon
콘텐츠
Kcon
콘텐츠
배송키
Kdis
600
통신 수단
기록 재생기
300
기록 재생기 식별자 [IDdev]
배송키용 마스터 키 [MKdis]
기록 디바이스
인증키용 마스터 키 [MKake]
기록 재생기 서명키용 마스터 키 [MKdev]
기록 디바이스
400
키 블록1
기록 디바이스 식별 정보1,
인증키1, 초기치1,
보존키1, 난수 발생기1, 종류1
키 블록2
기록 디바이스 식별 정보2,
인증키2, 초기치2,
보존키2, 난수 발생기2, 종류2
(기록 디바이스 식별 정보 = IDmem)
배송키: Kdis = DES (MKdis, 콘텐츠 ID)
인증키: Kake = DES (MKake, IDmem)
기록 재생기 서명키 : Kdev = DES (MKdev, IDdev)

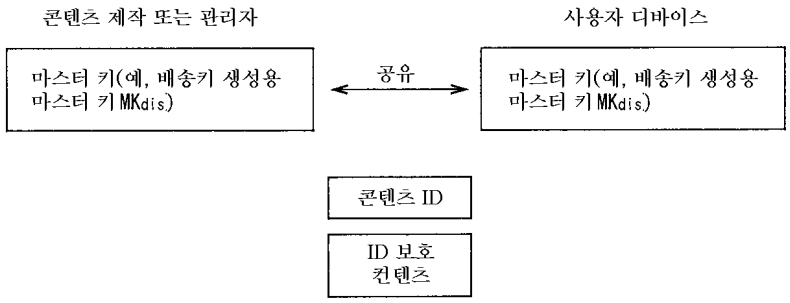
도면50

마스터 키로부터 개별키를 생성하는 방법(1)

[기본 플로우]



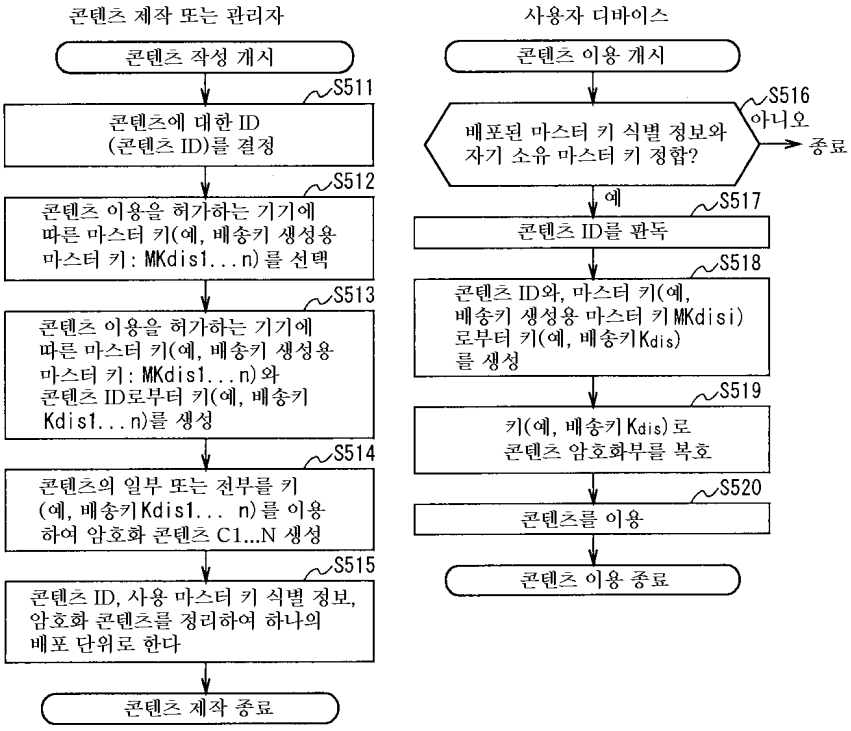
[키 소유 구성]



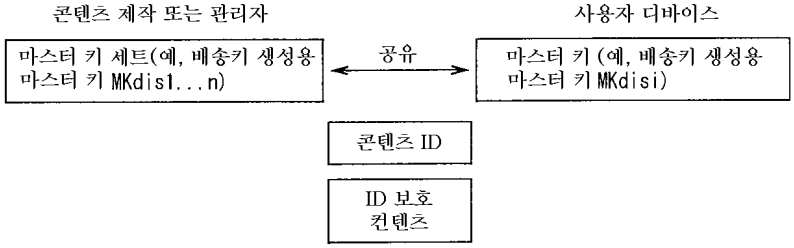
도면51

마스터 키로부터 개별키를 생성하는 방법(2)

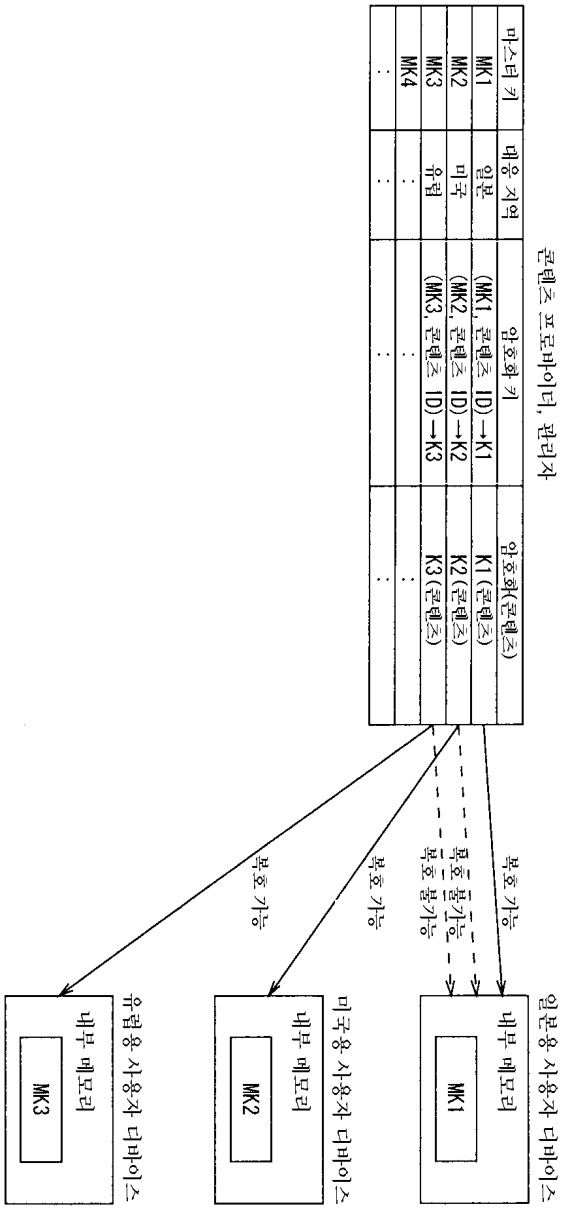
[기본 플로우]



[키 소유 구성]



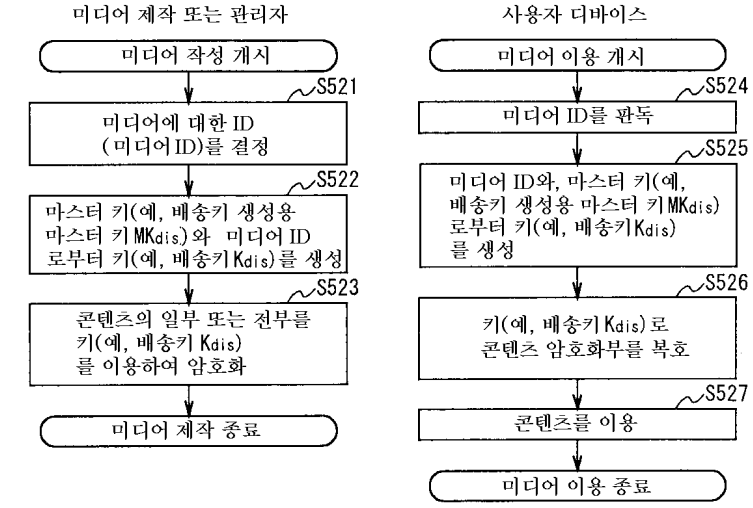
도면52


콘텐츠 프로바이더, 관리자
마스터 키
대응 지역
암호화 키
암호화(콘텐츠)
MK1
일본
(MK1, 콘텐츠 ID)→K1
K1 (콘텐츠)
MK2
미국
(MK2, 콘텐츠 ID)→K2
K2 (콘텐츠)
MK3
유럽
(MK3, 콘텐츠 ID)→K3
K3 (콘텐츠)
MK4
복호 가능
복호 불가능
복호 가능
복호 가능
일본용 사용자 디바이스
내부 메모리
MK1
미국용 사용자 디바이스
내부 메모리
MK2
유럽용 사용자 디바이스
내부 메모리
MK3

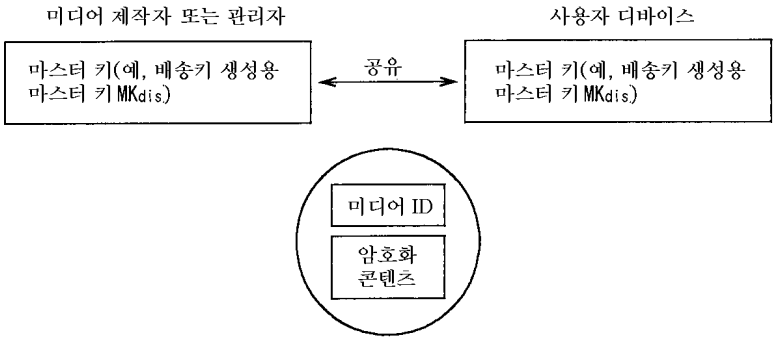
도면53

마스터 키로부터 개별키를 생성하는 방법(3)

[기본 플로우]



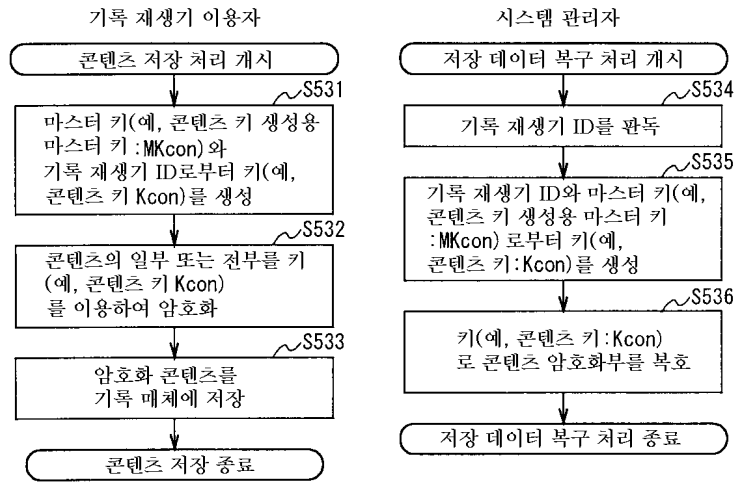
[키 소유 구성]



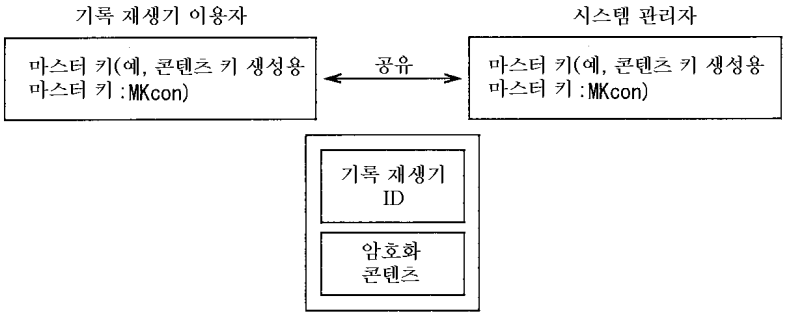
도면54

마스터 키로부터 개별키를 생성하는 방법(4)

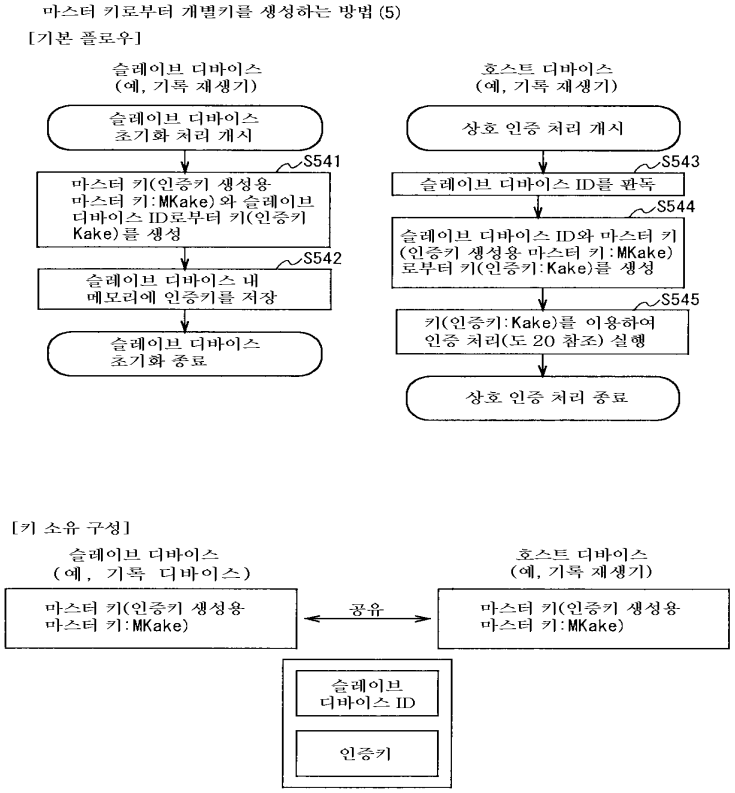
[기본 플로우]



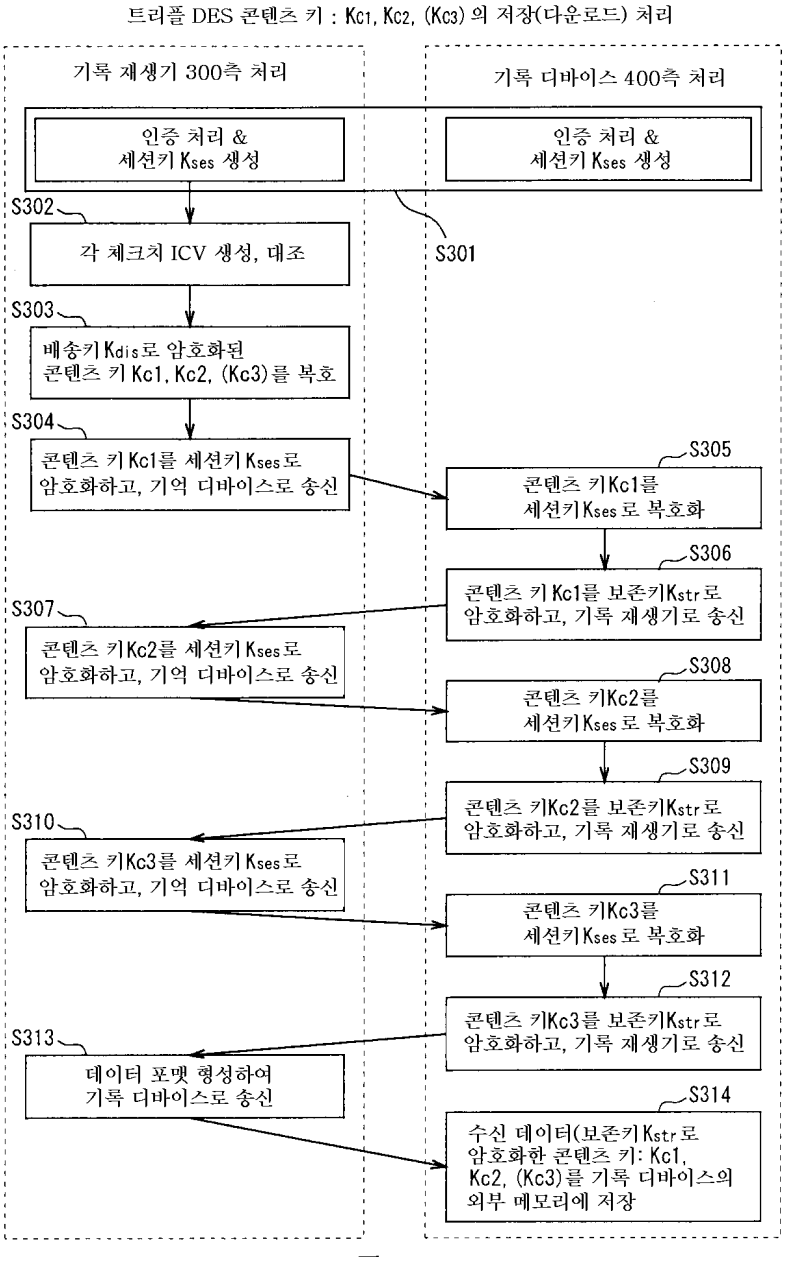
[키 소유 구성]



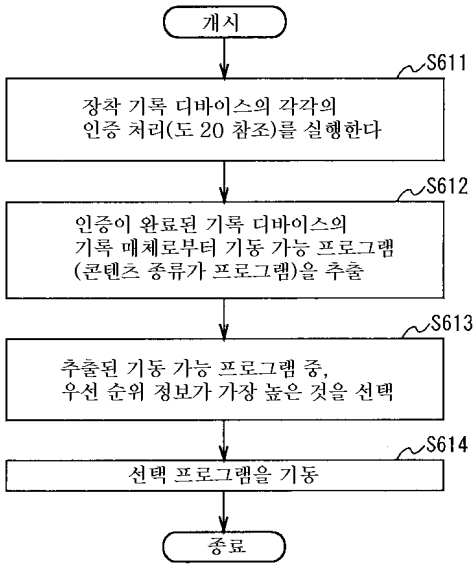
도면55


마스터 키로부터 개별키를 생성하는 방법 (5)
[기본 플로우]
슬레이브 디바이스
(예, 기록 재생기)
슬레이브 디바이스
초기화 처리 개시
S541
마스터 키(인증키 생성용
마스터 키:MKake)와 슬레이브
디바이스 ID로부터 키(인증키
Kake)를 생성
S542
슬레이브 디바이스 내
메모리에 인증키를 저장
슬레이브 디바이스
초기화 종료
호스트 디바이스
(예, 기록 재생기)
상호 인증 처리 개시
S543
슬레이브 디바이스 ID를 판독
S544
슬레이브 디바이스 ID와 마스터 키
(인증키 생성용 마스터 키:MKake)
로부터 키(인증키:Kake)를 생성
S545
키(인증키:Kake)를 이용하여
인증 처리(도 20 참조) 실행
상호 인증 처리 종료
[키 소유 구성]
슬레이브 디바이스
(예, 기록 디바이스)
마스터 키(인증키 생성용
마스터 키:MKake)
공유
호스트 디바이스
(예, 기록 재생기)
마스터 키(인증키 생성용
마스터 키:MKake)
슬레이브
디바이스 ID
인증키

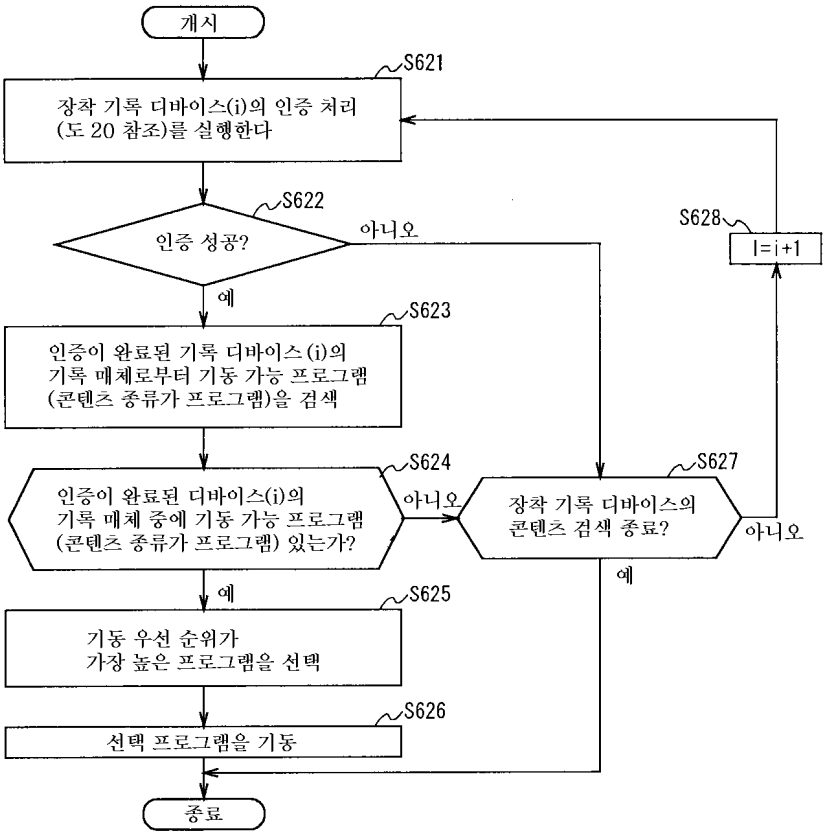
도면56


트리플 DES 콘텐츠 키 : Kc1, Kc2, (Kc3) 의 저장(다운로드) 처리
기록 재생기 300측 처리
기록 디바이스 400측 처리
인증 처리 & 세션키 Kses 생성
인증 처리 & 세션키 Kses 생성
S301
S302
각 체크치 ICV 생성, 대조
S303
배송키 Kdis로 암호화된 콘텐츠 키 Kc1, Kc2, (Kc3)를 복호
S304
콘텐츠 키 Kc1를 세션키 Kses로 암호화하고, 기억 디바이스로 송신
S305
콘텐츠 키 Kc1를 세션키 Kses로 복호화
S306
콘텐츠 키 Kc1를 보존키 Kstr로 암호화하고, 기록 재생기로 송신
S307
콘텐츠 키 Kc2를 세션키 Kses로 암호화하고, 기억 디바이스로 송신
S308
콘텐츠 키 Kc2를 세션키 Kses로 복호화
S309
콘텐츠 키 Kc2를 보존키 Kstr로 암호화하고, 기록 재생기로 송신
S310
콘텐츠 키 Kc3를 세션키 Kses로 암호화하고, 기억 디바이스로 송신
S311
콘텐츠 키 Kc3를 세션키 Kses로 복호화
S312
콘텐츠 키 Kc3를 보존키 Kstr로 암호화하고, 기록 재생기로 송신
S313
데이터 포맷 형성하여 기록 디바이스로 송신
S314
수신 데이터(보존키 Kstr로 암호화한 콘텐츠 키: Kc1, Kc2, (Kc3)를 기록 디바이스의 외부 메모리에 저장

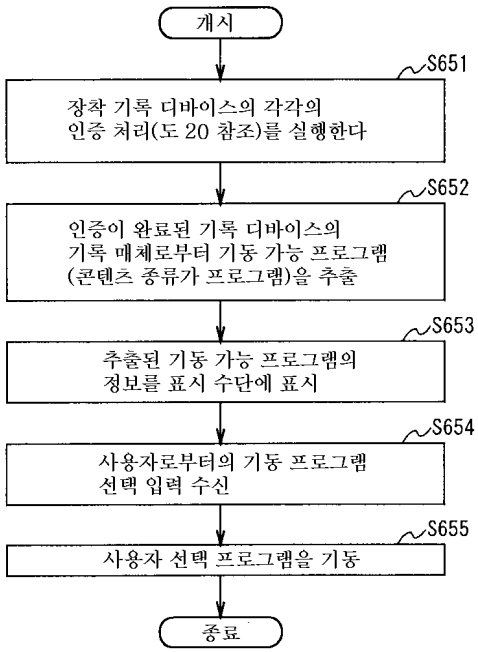
도면57


개시
S611
장착 기록 디바이스의 각각의
인증 처리(도 20 참조)를 실행한다
S612
인증이 완료된 기록 디바이스의
기록 매체로부터 기동 가능 프로그램
(콘텐츠 종류가 프로그램)을 추출
S613
추출된 기동 가능 프로그램 중,
우선 순위 정보가 가장 높은 것을 선택
S614
선택 프로그램을 기동
종료

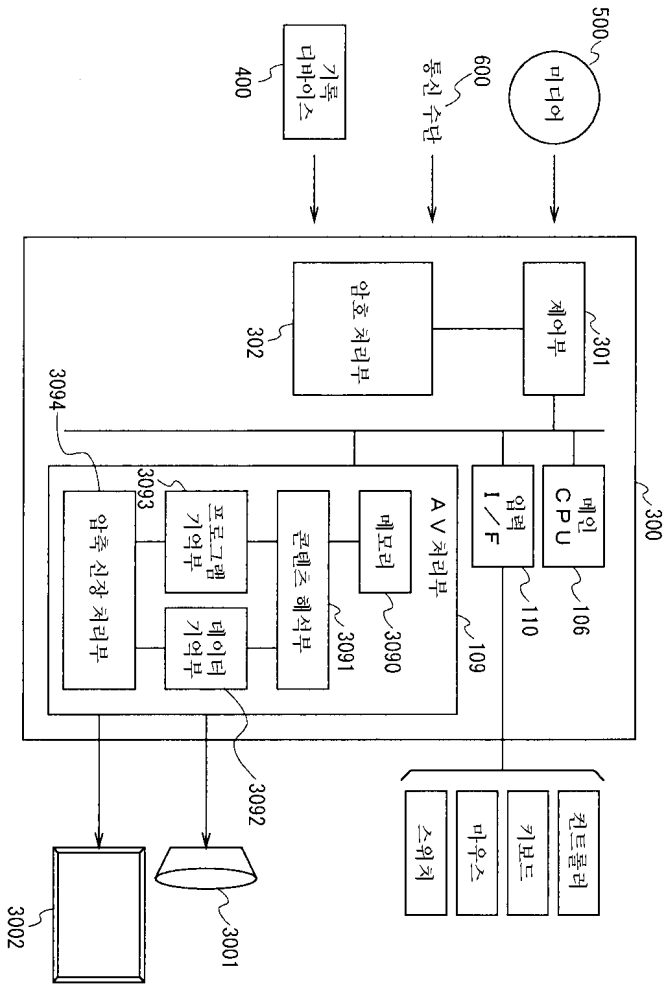
도면58


개시
S621
장착 기록 디바이스(i)의 인증 처리
(도 20 참조)를 실행한다
S622
인증 성공?
아니오
예
S623
인증이 완료된 기록 디바이스(i)의
기록 매체로부터 기동 가능 프로그램
(콘텐츠 종류가 프로그램)을 검색
S624
인증이 완료된 디바이스(i)의
기록 매체 중에 기동 가능 프로그램
(콘텐츠 종류가 프로그램) 있는가?
아니오
예
S625
기동 우선 순위가
가장 높은 프로그램을 선택
S626
선택 프로그램을 기동
종료
S627
장착 기록 디바이스의
콘텐츠 검색 종료?
아니오
예
S628
I=i+1

도면59

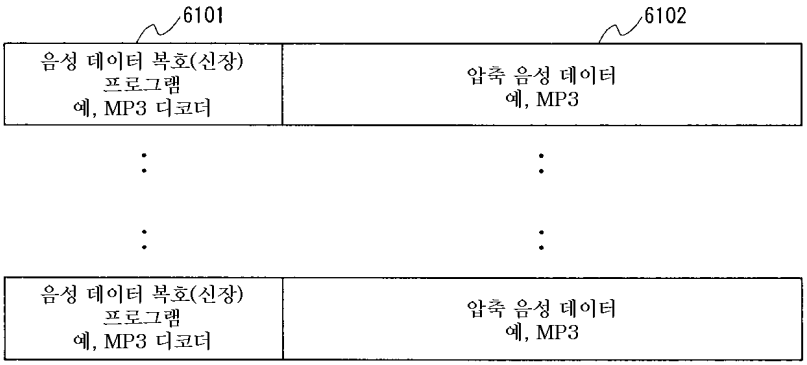

개시
S651
장착 기록 디바이스의 각각의
인증 처리(도 20 참조)를 실행한다
S652
인증이 완료된 기록 디바이스의
기록 매체로부터 기동 가능 프로그램
(콘텐츠 종류가 프로그램)을 추출
S653
추출된 기동 가능 프로그램의
정보를 표시 수단에 표시
S654
사용자로부터의 기동 프로그램
선택 입력 수신
S655
사용자 선택 프로그램을 기동
종료

도면60

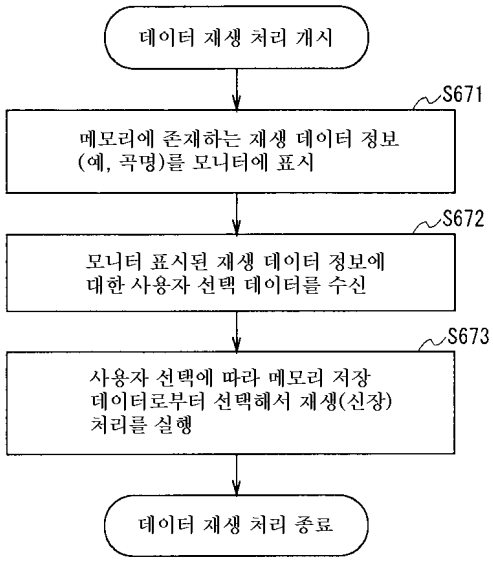

500
미디어
600
통신 수단
400
기록
디바이스
암호 처리부
302
제어부
301
3094
300
3093
압축 신장 처리부
프로그램
기억부
데이터
기억부
콘텐츠 해석부
3091
메모리
3090
AV 처리부
109
입력
I/F
110
메인
CPU
106
3092
스위치
마우스
키보드
컨트롤러
3002
3001

도면61

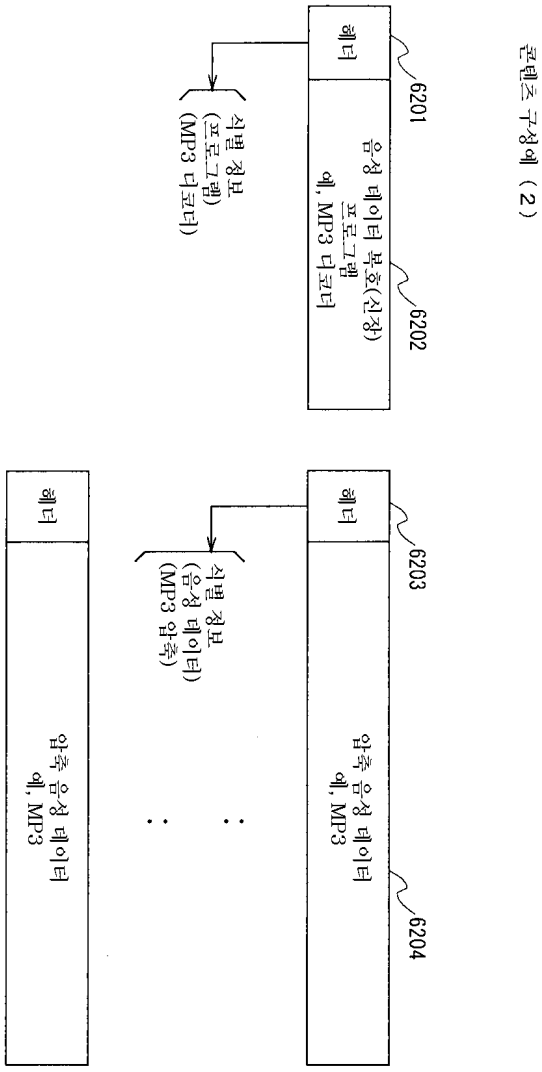
콘텐츠 구성예 (1)



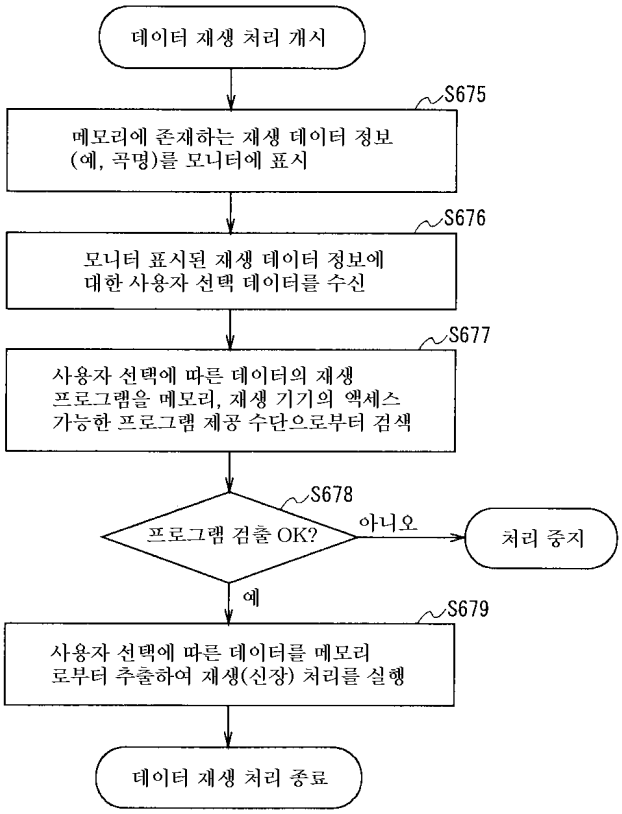
도면62



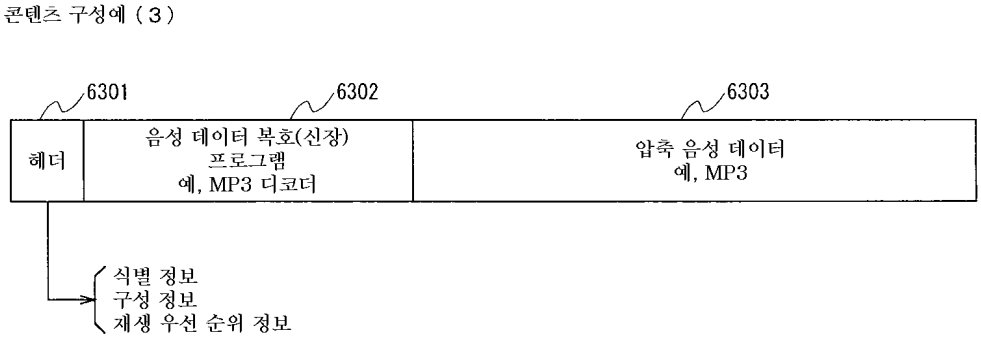
도면63


콘텐츠 구성예 (2)
헤더
6201
음성 데이터 복호(신장) 프로그램
예, MP3 디코더
6202
식별 정보
(프로그램)
(MP3 디코더)
헤더
6203
압축 음성 데이터
예, MP3
6204
식별 정보
(음성 데이터)
(MP3 압축)
헤더
압축 음성 데이터
예, MP3

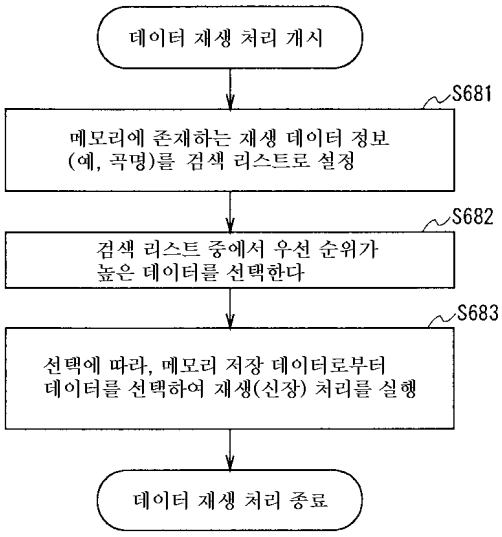
도면64


데이터 재생 처리 개시
S675
메모리에 존재하는 재생 데이터 정보
(예, 곡명)를 모니터에 표시
S676
모니터 표시된 재생 데이터 정보에
대한 사용자 선택 데이터를 수신
S677
사용자 선택에 따른 데이터의 재생
프로그램을 메모리, 재생 기기의 액세스
가능한 프로그램 제공 수단으로부터 검색
S678
프로그램 검출 OK?
아니오
처리 중지
예
S679
사용자 선택에 따른 데이터를 메모리
로부터 추출하여 재생(신장) 처리를 실행
데이터 재생 처리 종료

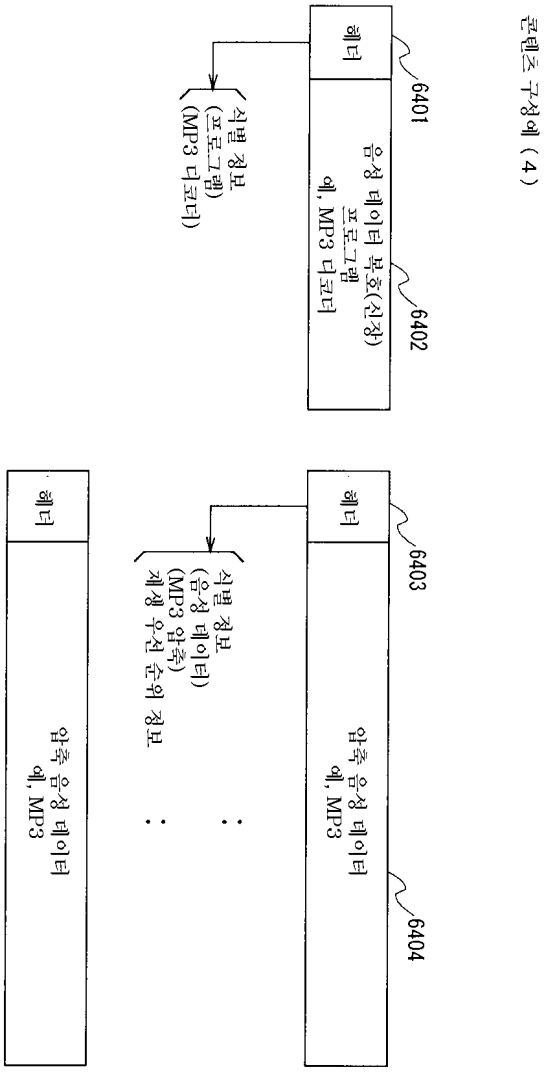
도면65


콘텐츠 구성예 (3)
6301
6302
6303
헤더
음성 데이터 복호(신장)
프로그램
예, MP3 디코더
압축 음성 데이터
예, MP3
식별 정보
구성 정보
재생 우선 순위 정보

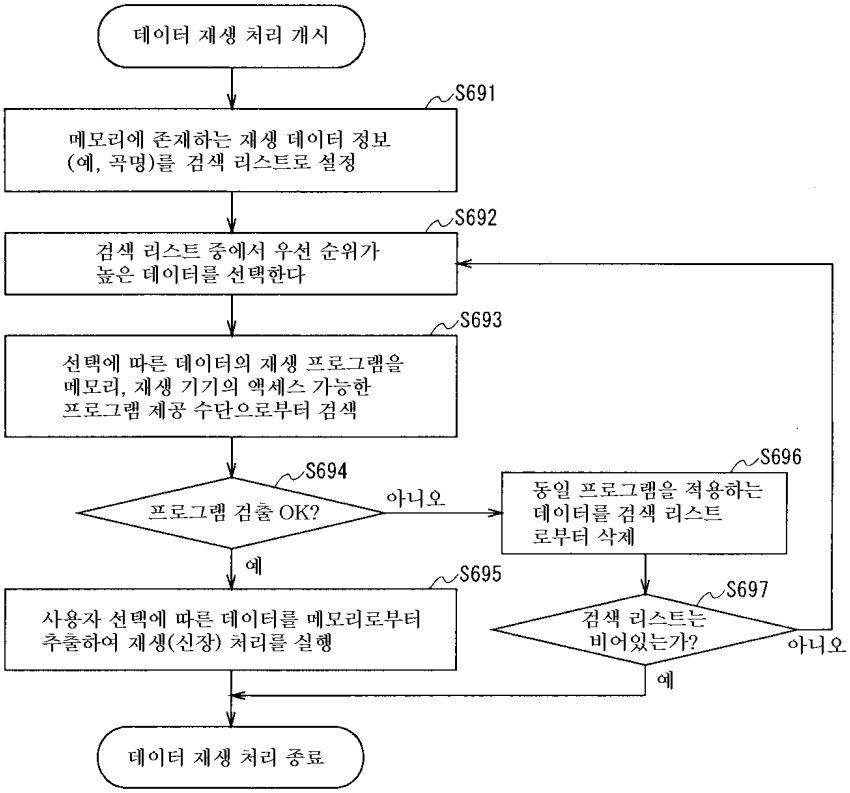
도면66


데이터 재생 처리 개시
S681
메모리에 존재하는 재생 데이터 정보
(예, 곡명)를 검색 리스트로 설정
S682
검색 리스트 중에서 우선 순위가
높은 데이터를 선택한다
S683
선택에 따라, 메모리 저장 데이터로부터
데이터를 선택하여 재생(신장) 처리를 실행
데이터 재생 처리 종료

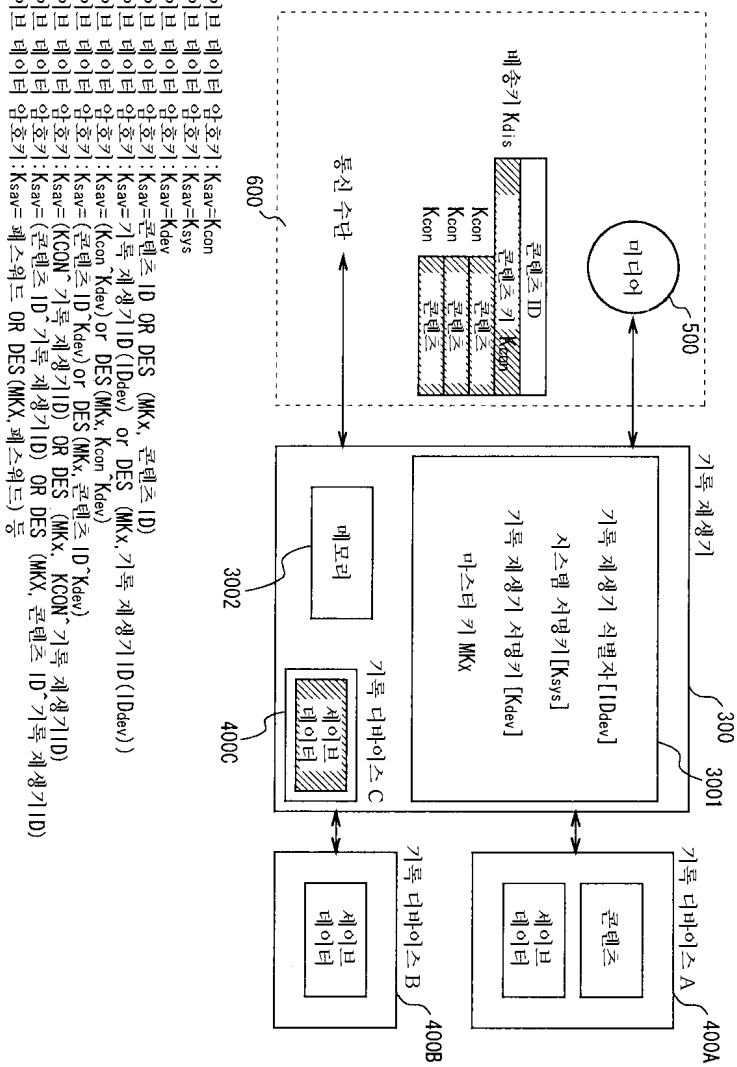
도면67


콘텐츠 구성예 (4)
헤더
6401
음성 데이터 복호(신장)
프로그램
예, MP3 디코더
6402
식별 정보
(프로그램)
(MP3 디코더)
헤더
6403
압축 음성 데이터
예, MP3
6404
식별 정보
(음성 데이터)
(MP3 압축)
재생 우선 순위 정보
헤더
압축 음성 데이터
예, MP3

도면68


데이터 재생 처리 개시
S691
메모리에 존재하는 재생 데이터 정보
(예, 곡명)를 검색 리스트로 설정
S692
검색 리스트 중에서 우선 순위가
높은 데이터를 선택한다
S693
선택에 따른 데이터의 재생 프로그램을
메모리, 재생 기기의 액세스 가능한
프로그램 제공 수단으로부터 검색
S694
프로그램 검출 OK?
아니오
S696
동일 프로그램을 적용하는
데이터를 검색 리스트
로부터 삭제
예
S695
사용자 선택에 따른 데이터를 메모리로부터
추출하여 재생(신장) 처리를 실행
S697
검색 리스트는
비어있는가?
아니오
예
데이터 재생 처리 종료

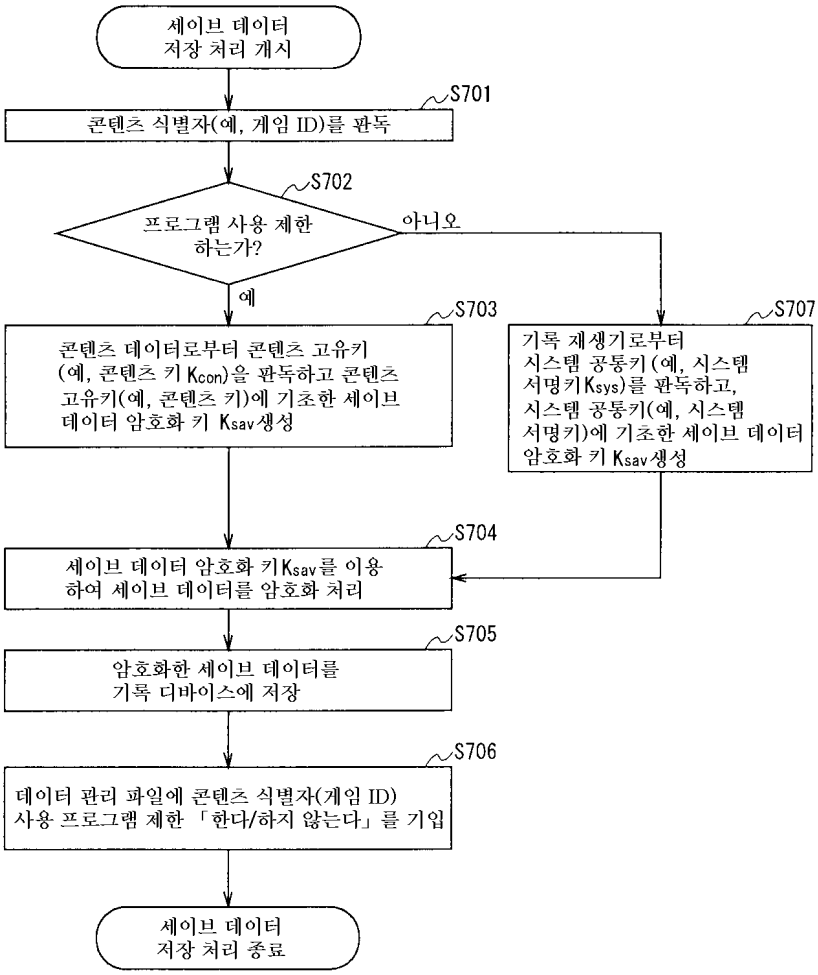
도면69



세이브 데이터 암호키 : Ksav=Kcon
세이브 데이터 암호키 : Ksav=Ksys
세이브 데이터 암호키 : Ksav=Kdev
세이브 데이터 암호키 : Ksav=콘텐츠 ID OR DES (MKx, 콘텐츠 ID)
세이브 데이터 암호키 : Ksav=기록 재생기 ID (IDdev) or DES (MKx,기록 재생기 ID (IDdev))
세이브 데이터 암호키 : Ksav= (Kcon ^Kdev) or DES (MKx, Kcon ^Kdev)
세이브 데이터 암호키 : Ksav= (콘텐츠 ID^Kdev)or DES (MKx,콘텐츠 ID^Kdev)
세이브 데이터 암호키 : Ksav= (KCON^기록 재생기ID) OR DES (MKx, KCON^기록 재생기ID)
세이브 데이터 암호키 : Ksav= (콘텐츠 ID^기록 재생기ID) OR DES (MKX, 콘텐츠 ID^기록 재생기ID)
세이브 데이터 암호키 : Ksav= 패스워드 OR DES (MKX,패스워드) 등

도면70

(1) 콘텐츠 고유키, or 시스템 공통키를 사용한 세이브 데이터 저장 처리예



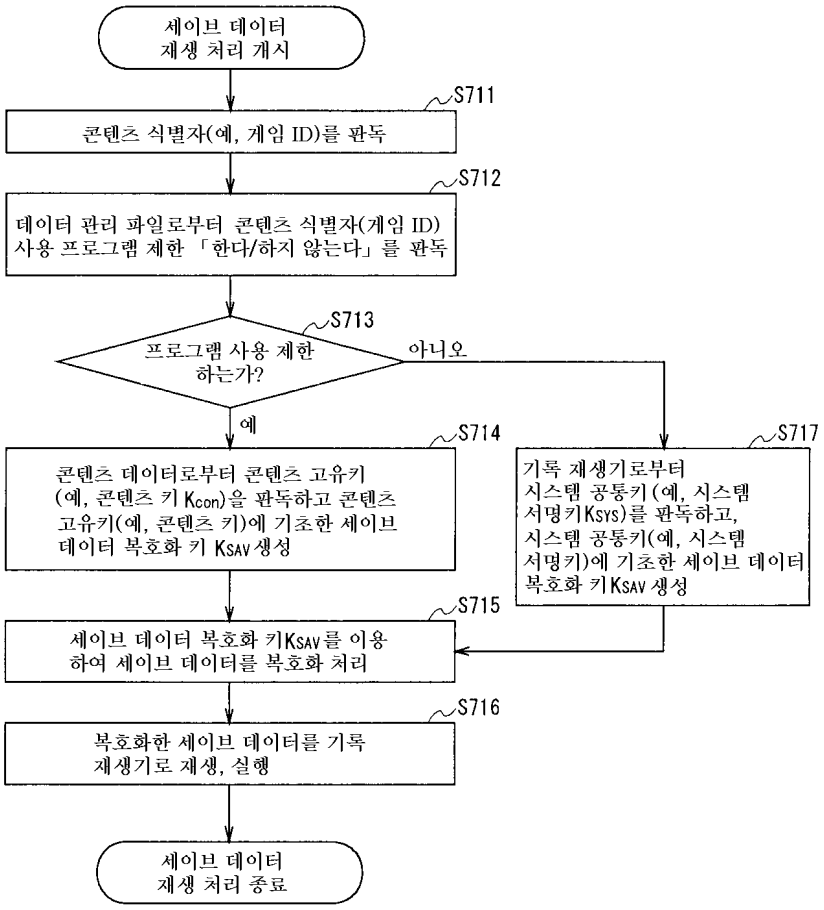
도면71

데이터 관리 파일(1)

데이터 번호	콘텐츠 식별자 (게임 ID)	기록 재생기 식별자 (IDdev)	프로그램 사용 제한
1	12345678...	56789012...	한다
2	ABCDEF12...	09876543...	한다
3	12245678...	58834762...	하지 않는다
:	:	:	:

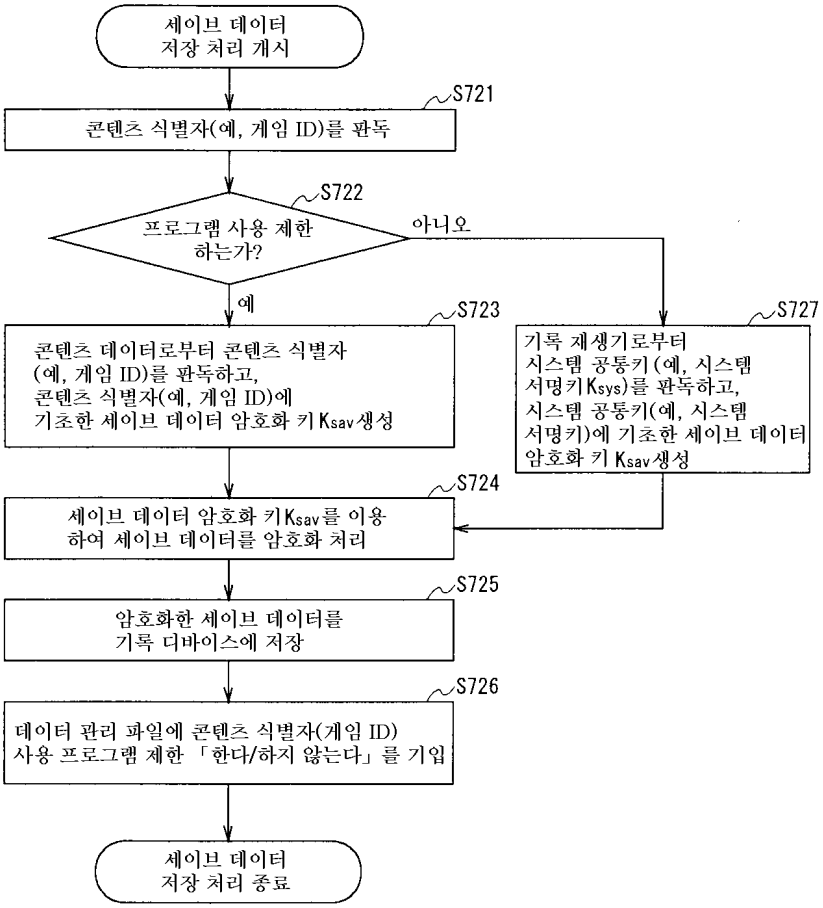
도면72

(2) 콘텐츠 고유키, or 시스템 공통키를 사용한 세이브 데이터 재생 처리예



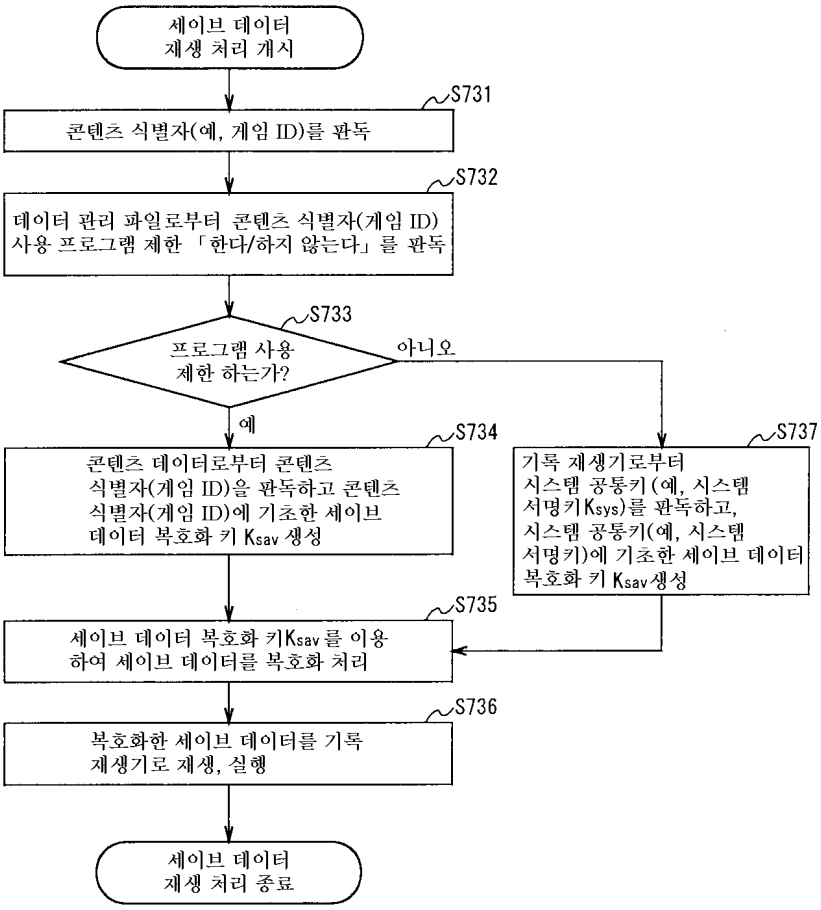
도면73

(3) 콘텐츠 ID or 시스템 공통키를 사용한 세이브 데이터 저장 처리에



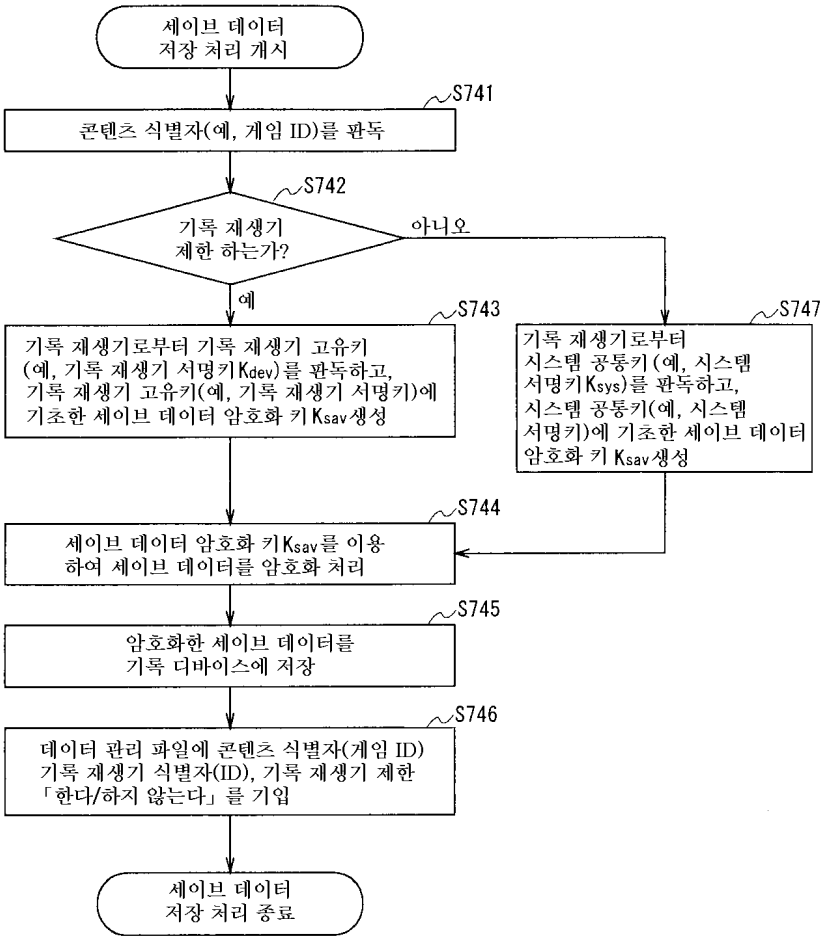
도면74

(4) 콘텐츠 ID or 시스템 공통키를 사용한 세이브 데이터 재생 처리예



도면75

(5)기록 재생기 고유키, or 시스템 공통키를 사용한 세이브 데이터 저장 처리예



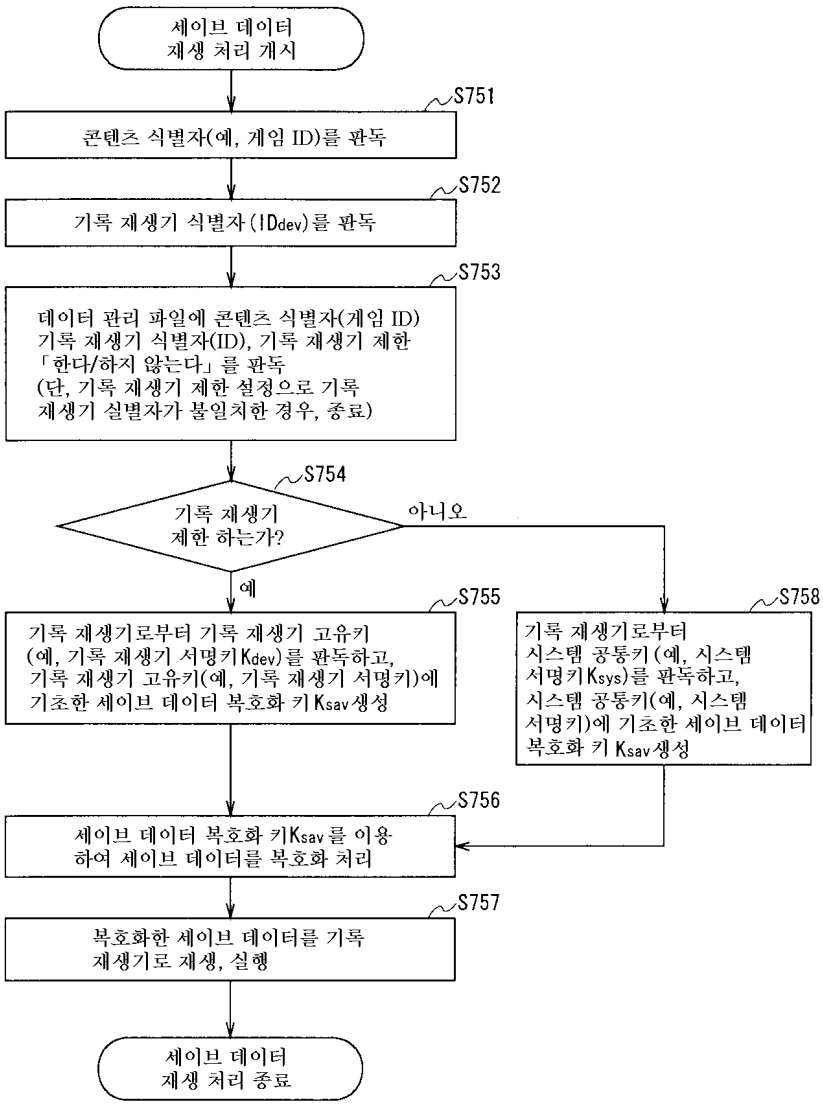
도면76

데이터 관리 파일(2)

데이터 번호	콘텐츠 식별자 (게임 ID)	기록 재생기 식별자 (IDdev)	기록 재생기 제한
1	12345678...	56789012...	하지 않는다
2	ABCDEF12...	09876543...	한다
3	12245678...	58834762...	한다
:	:	:	:

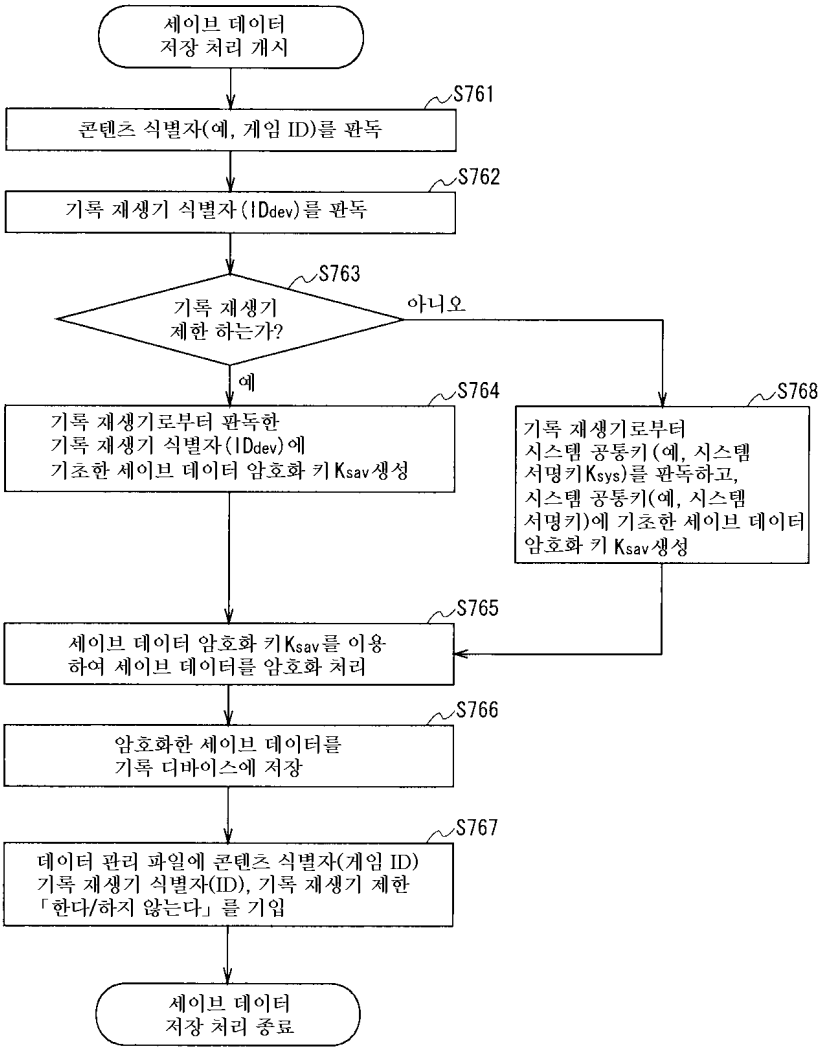
도면77

(6) 기록 재생기 고유키, or 시스템 공통키를 사용한 세이브 데이터 재생 처리예



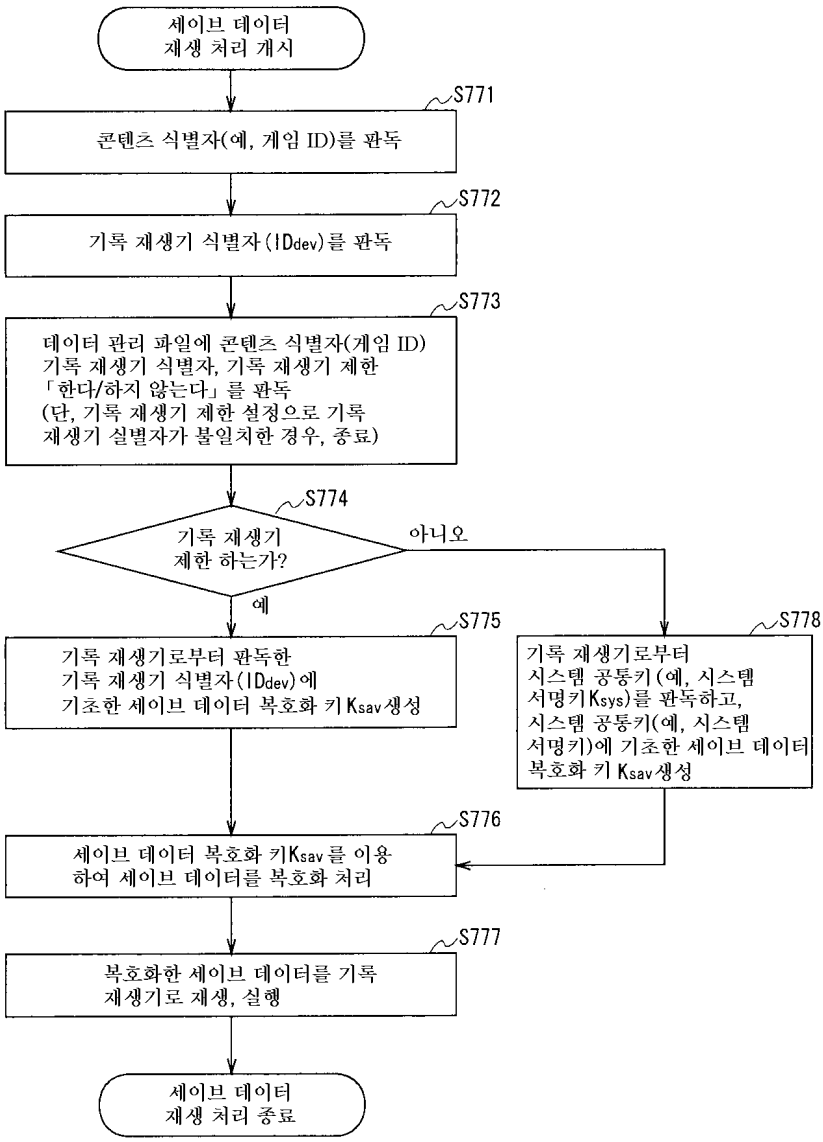
도면78

(7) 기록 재생기 식별자 or 시스템 공통키를 사용한 세이브 데이터 저장 처리예

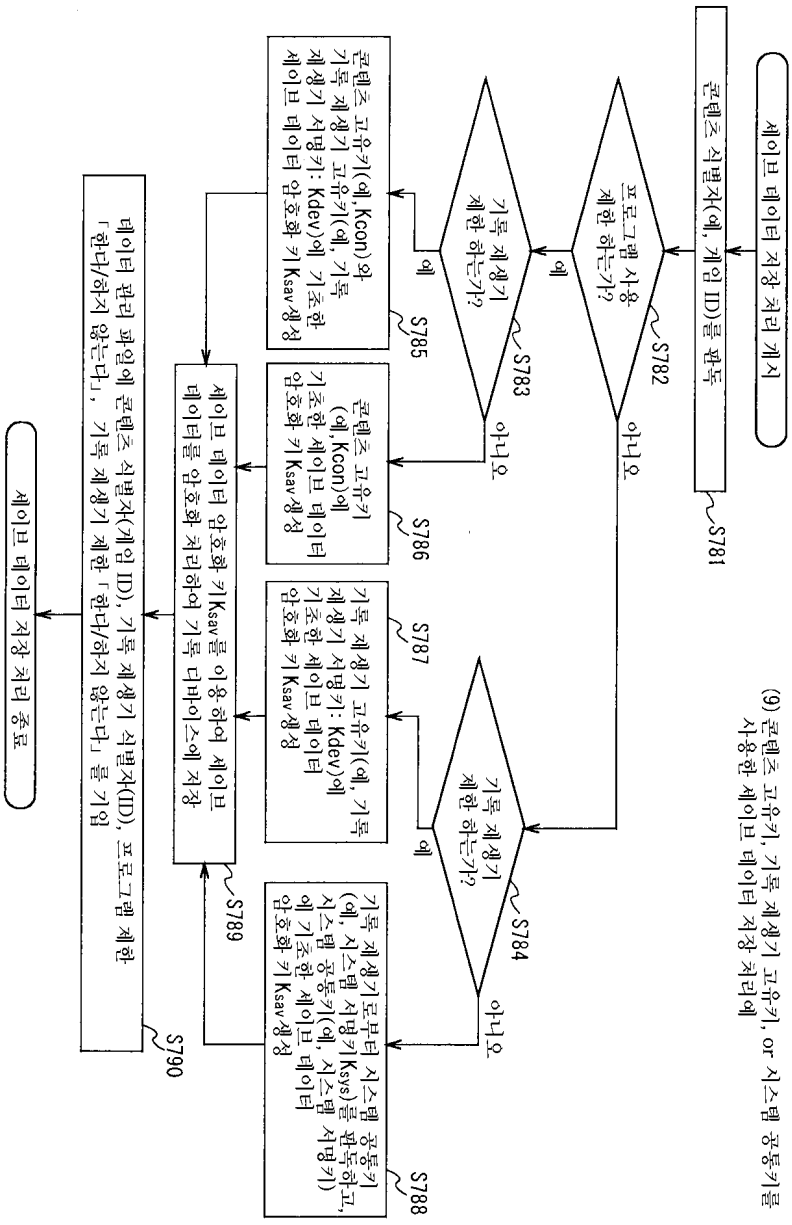


도면79

(8)기록 재생기 식별자, or 시스템 공통키를 사용한 세이브 데이터 재생 처리예



도면80

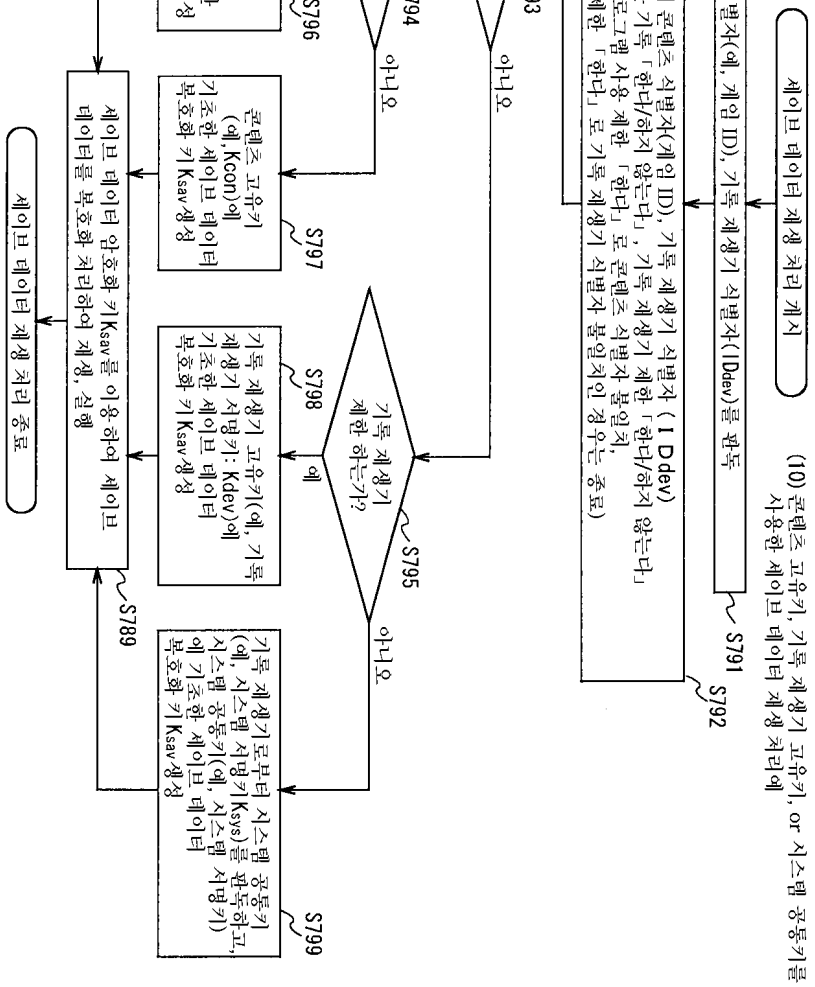


도면81

데이터 관리 파일(3)

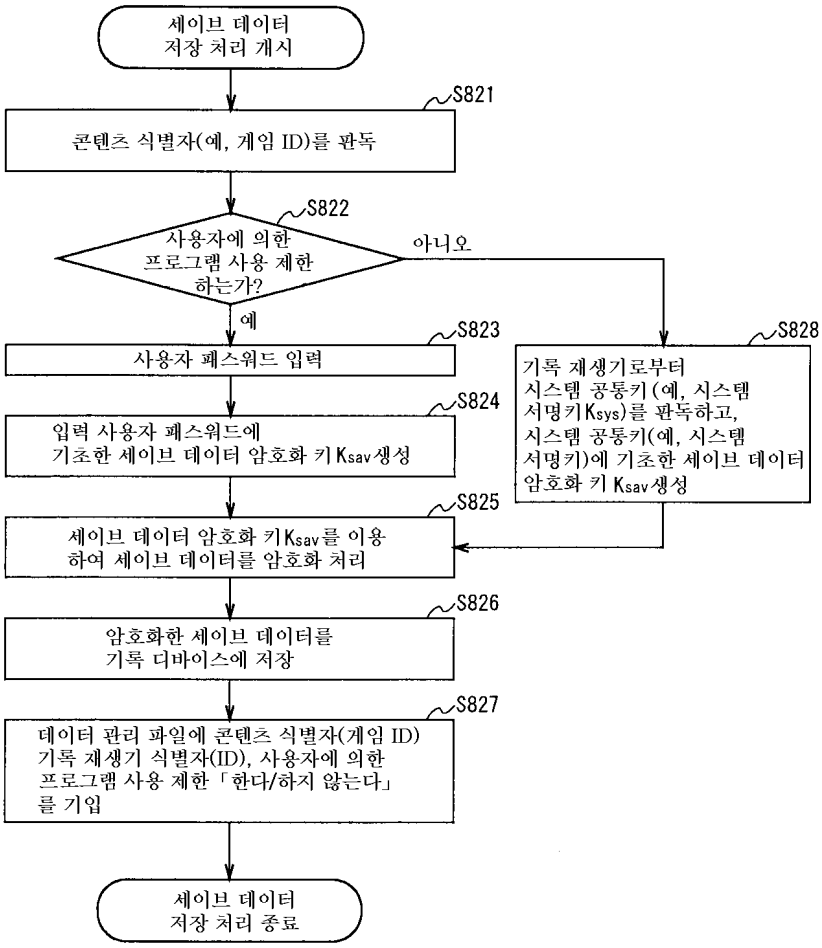
데이터 번호	콘텐츠 식별자 (게임 ID)	기록 재생기 식별자 (IDdev)	프로그램 사용 제한	기록 재생기 제한
1	12345678...	56789012...	한다	하지 않는다
2	ABCDEF12...	09876543...	한다	한다
3	12245678...	58834762...	하지 않는다	한다
:	:	:	:	:

도면82


세이브 데이터 재생 처리 개시
콘텐츠 식별자(예, 게임 ID), 기록 재생기 식별자(IDdev)를 판독
S791
데이터 관리 파일에 콘텐츠 식별자(게임 ID), 기록 재생기 식별자 (I D dev)
프로그램 사용 제한 기록 「한다/하지 않는다」, 기록 재생기 제한 「한다/하지 않는다」
를 판독한다.(단 프로그램 사용 제한 「한다」 로 콘텐츠 식별자 불일치,
또는 기록 재생기 제한 「한다」 로 기록 재생기 식별자 불일치인 경우는 종료)
S792
프로그램 사용 제한 하는가?
S793
예
아니오
기록 재생기 제한 하는가?
S794
예
아니오
기록 재생기 제한 하는가?
S795
예
아니오
콘텐츠 고유키(예,Kcon)와 기록 재생기 고유키(예, 기록 재생기 식별키: Kdev)에 기초한 세이브 데이터 복호화 키 Ksav생성
S796
콘텐츠 고유키 (예,Kcon)에 기초한 세이브 데이터 복호화 키 Ksav생성
S797
기록 재생기 고유키(예, 기록 재생기 식별키: Kdev)에 기초한 세이브 데이터 복호화 키 Ksav생성
S798
기록 재생기로부터 시스템 공통키(예, 시스템 서명키 Ksys)를 판독하고, 시스템 공통키(예, 시스템 서명키)에 기초한 세이브 데이터 복호화 키 Ksav생성
S799
세이브 데이터 암호화 키 Ksav를 이용하여 세이브 데이터를 복호화 처리하여 재생, 실행
S789
세이브 데이터 재생 처리 종료
(10) 콘텐츠 고유키, 기록 재생기 고유키, or 시스템 공통키를 사용한 세이브 데이터 재생 처리에

도면83

(11) 사용자 패스워드, 또는 시스템 공통키를 사용한 세이브 데이터 저장 처리예



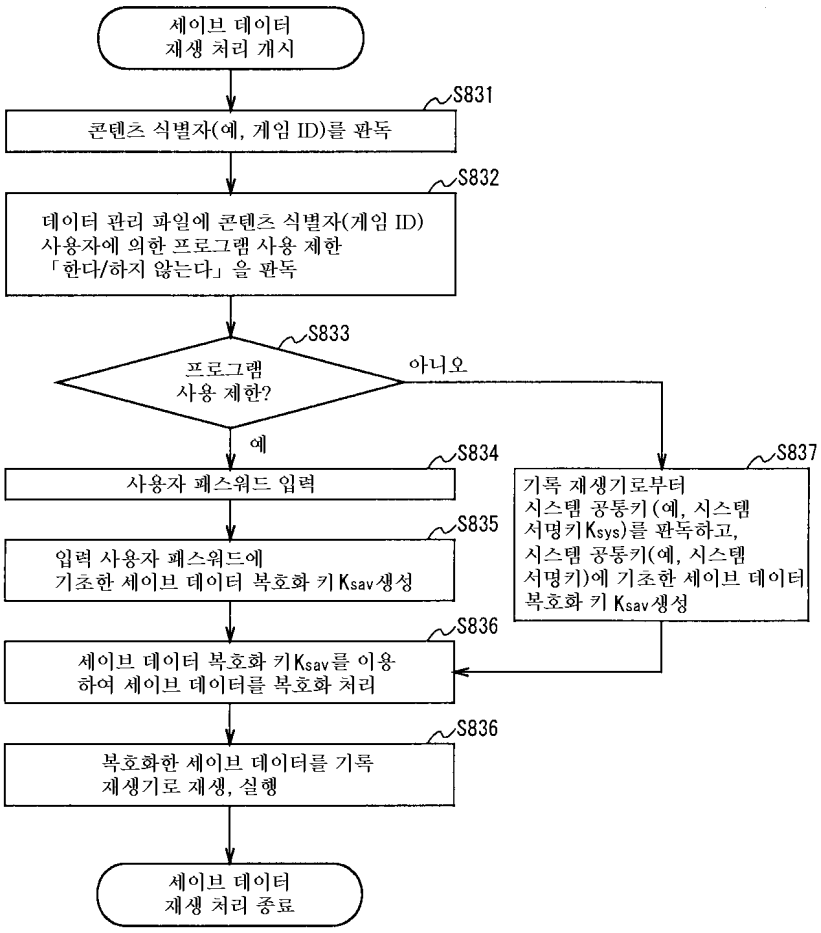
도면84

데이터 관리 파일(4)

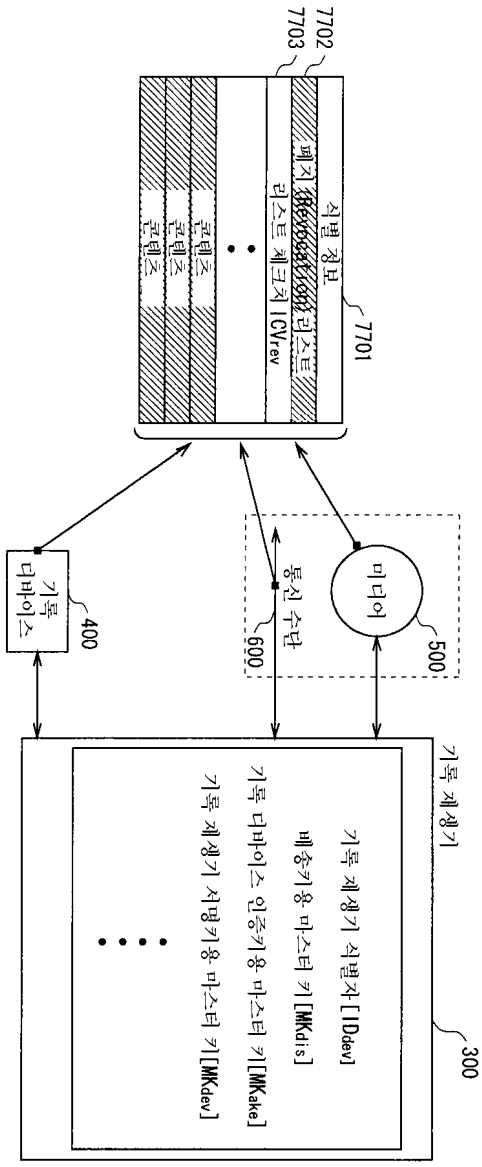
데이터 번호	콘텐츠 식별자 (게임 ID)	기록 재생기 식별자 (IDdev)	사용자에 의한 프로그램 사용 제한
1	12345678...	56789012...	한다
2	ABCDEF12...	09876543...	한다
3	12245678...	58834762...	하지 않는다
:	:	:	:

도면85

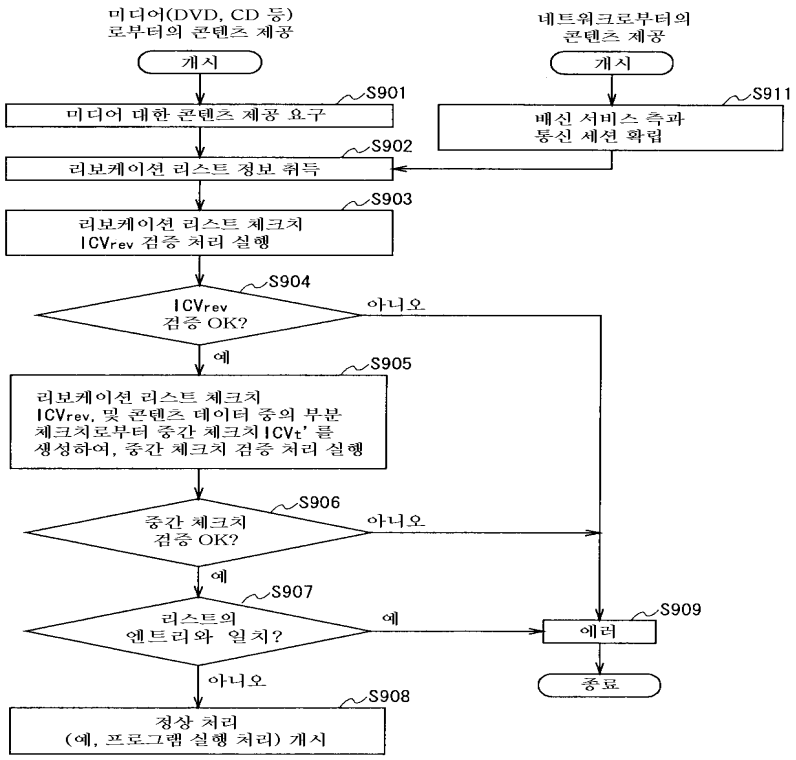
(12) 사용자 패스워드, 또는 시스템 공통키를 사용한 세이브 데이터 재생 처리예



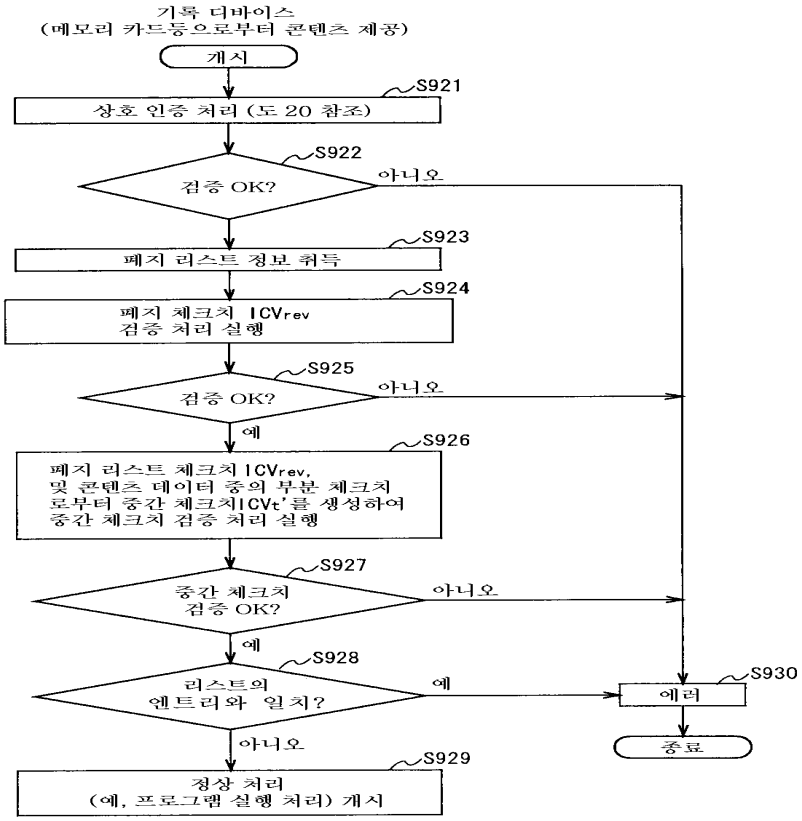
도면86


7702
7703
식별 정보
리스트 체크치 [CVrev]
콘텐츠
콘텐츠
콘텐츠
7701
기록 디바이스
400
통신 수단
600
미디어
500
기록 재생기
기록 재생기 식별자 [IDdev]
배송키용 마스터 키 [MKdis]
기록 디바이스 인증키용 마스터 키 [MKake]
기록 재생기 서명키용 마스터 키 [MKdev]
300

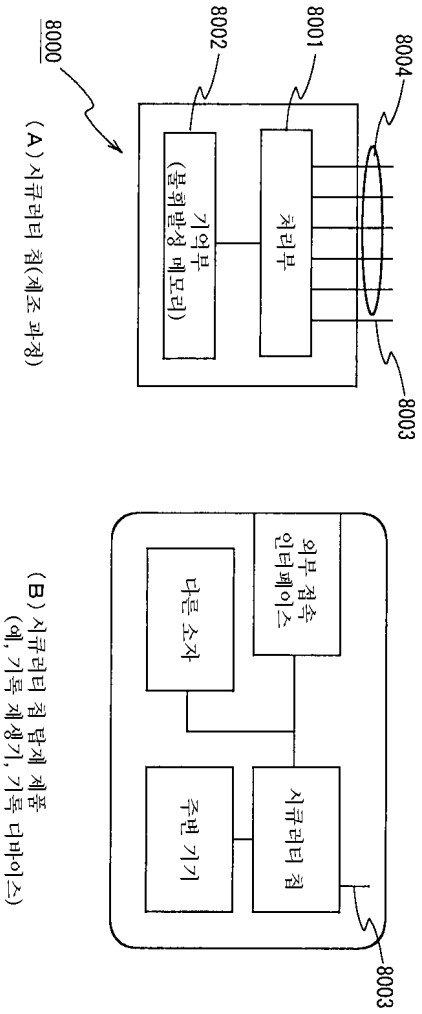
도면87


미디어(DVD, CD 등)
로부터의 콘텐츠 제공
개시
S901
미디어 대한 콘텐츠 제공 요구
S902
리보케이션 리스트 정보 취득
S903
리보케이션 리스트 체크치
ICVrev 검증 처리 실행
S904
ICVrev
검증 OK?
아니오
예
S905
리보케이션 리스트 체크치
ICVrev, 및 콘텐츠 데이터 중의 부분
체크치로부터 중간 체크치 ICVt' 를
생성하여, 중간 체크치 검증 처리 실행
S906
중간 체크치
검증 OK?
아니오
예
S907
리스트의
엔트리와 일치?
예
아니오
S908
정상 처리
(에, 프로그램 실행 처리) 개시
네트워크로부터의
콘텐츠 제공
개시
S911
배신 서비스 측과
통신 세션 확립
S909
에러
종료

도면88


기록 디바이스
(메모리 카드등으로부터 콘텐츠 제공)
개시
S921
상호 인증 처리 (도 20 참조)
S922
검증 OK?
아니오
S923
페지 리스트 정보 취득
S924
페지 체크치 ICVrev
검증 처리 실행
S925
검증 OK?
아니오
예
S926
페지 리스트 체크치 ICVrev,
및 콘텐츠 데이터 중의 부분 체크치
로부터 중간 체크치 ICVt' 를 생성하여
중간 체크치 검증 처리 실행
S927
중간 체크치
검증 OK?
아니오
예
S928
리스트의
엔트리와 일치?
예
아니오
S929
정상 처리
(에, 프로그램 실행 처리) 개시
S930
에러
종료

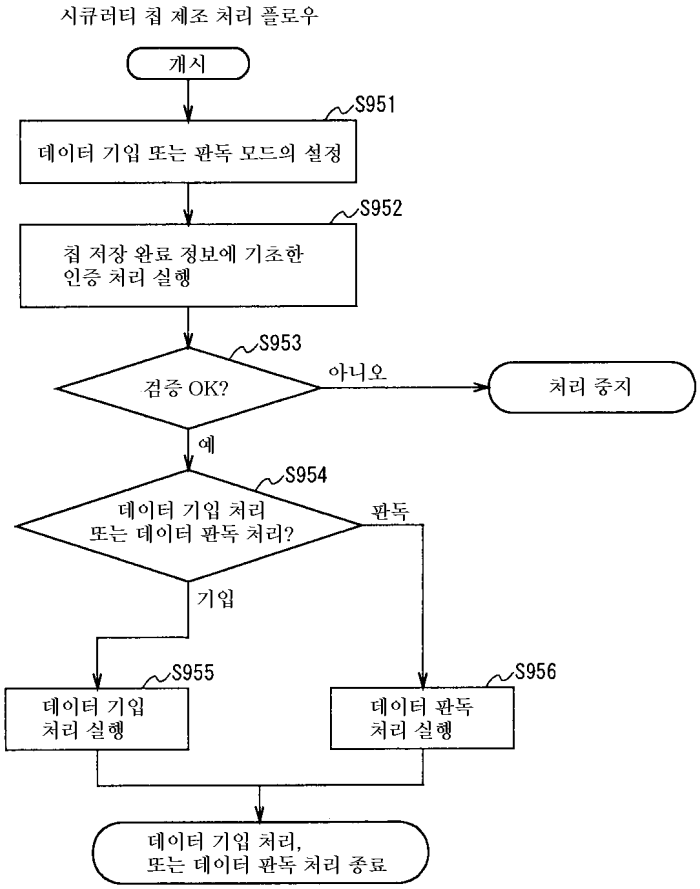
도면89



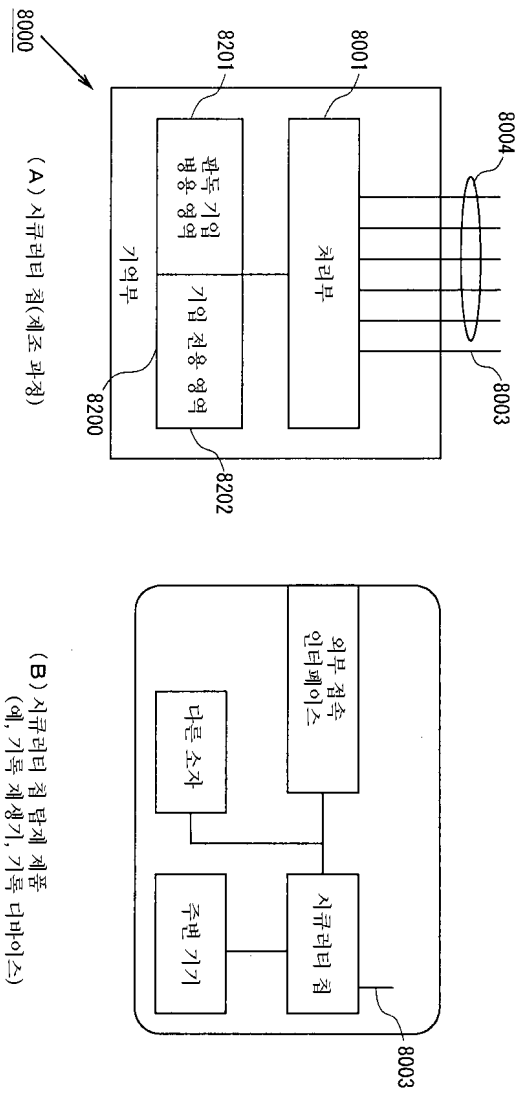
(A) 시큐러티 칩(제조 과정)

(B) 시큐러티 칩 탑재 제품
(예, 기록 재생기, 기록 디바이스)

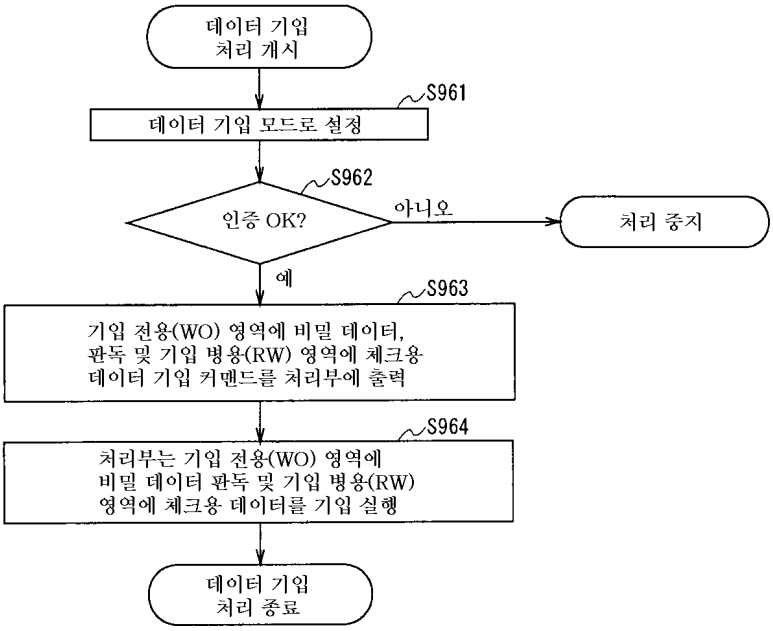
도면90


시큐러티 칩 제조 처리 플로우
개시
S951
데이터 기입 또는 판독 모드의 설정
S952
칩 저장 완료 정보에 기초한
인증 처리 실행
S953
검증 OK?
아니오
처리 중지
예
S954
데이터 기입 처리
또는 데이터 판독 처리?
판독
기입
S955
데이터 기입
처리 실행
S956
데이터 판독
처리 실행
데이터 기입 처리,
또는 데이터 판독 처리 종료

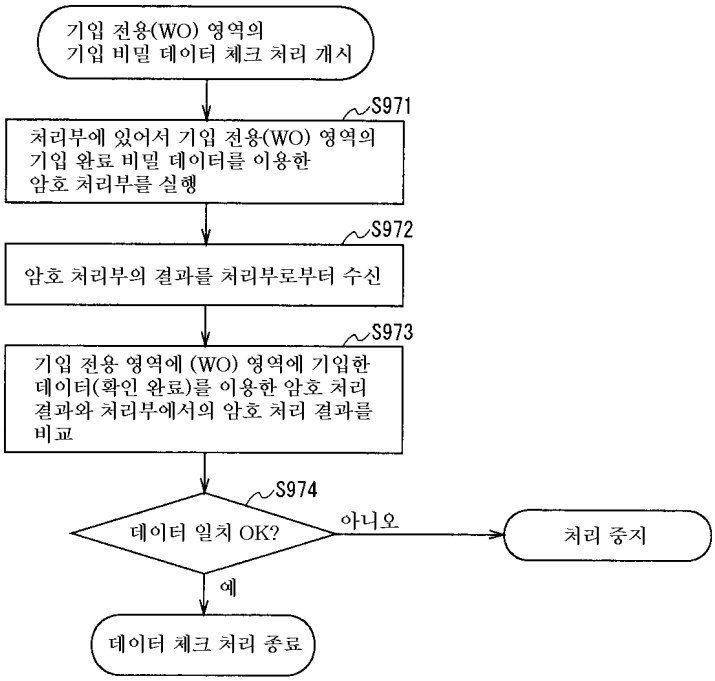
도면91


8000
8201
8001
8004
8003
8200
8202
독점 기입 영역
기입 전용 영역
기억부
처리부
(A) 시큐러티 칩(제조 과정)
외부 접속 인터페이스
다른 소자
주변 기기
시큐러티 칩
8003
(B) 시큐러티 칩 탑재 제품
(예, 기록 재생기, 기록 디바이스)

도면92


데이터 기입
처리 개시
S961
데이터 기입 모드로 설정
S962
인증 OK?
아니오
처리 중지
예
S963
기입 전용(WO) 영역에 비밀 데이터,
판독 및 기입 병용(RW) 영역에 체크용
데이터 기입 커맨드를 처리부에 출력
S964
처리부는 기입 전용(WO) 영역에
비밀 데이터 판독 및 기입 병용(RW)
영역에 체크용 데이터를 기입 실행
데이터 기입
처리 종료

도면93


기입 전용(WO) 영역의
기입 비밀 데이터 체크 처리 개시
S971
처리부에 있어서 기입 전용(WO) 영역의
기입 완료 비밀 데이터를 이용한
암호 처리부를 실행
S972
암호 처리부의 결과를 처리부로부터 수신
S973
기입 전용 영역에 (WO) 영역에 기입한
데이터(확인 완료)를 이용한 암호 처리
결과와 처리부에서의 암호 처리 결과를
비교
S974
데이터 일치 OK?
아니오
처리 중지
예
데이터 체크 처리 종료