(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년01월31일
(11) 등록번호 10-1109995
(24) 등록일자 2012년01월18일

(51) Int. Cl.
G11B 20/10 (2006.01) *G06F 12/14* (2006.01)
H04L 9/08 (2006.01)
(21) 출원번호 10-2005-7012571
(22) 출원일자(국제출원일자) 2004년03월11일
심사청구일자 2008년12월16일
(85) 번역문제출일자 2005년07월04일
(65) 공개번호 10-2006-0058047
(43) 공개일자 2006년05월29일
(86) 국제출원번호 PCT/JP2004/003161
(87) 국제공개번호 WO 2004/082203
국제공개일자 2004년09월23일
(30) 우선권주장
JP-P-2003-00065591 2003년03월11일 일본(JP)
JP-P-2003-00158927 2003년06월04일 일본(JP)
(56) 선행기술조사문헌
US05886979 A1*
US06367019 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
파나소닉 주식회사
일본 오오사카후 가도마시 오오아자 가도마 1006 반치
(72) 발명자
나카노 도시히사
일본국 오오사카후 네야가와시 시메노 3-35-15
야마미치 마사미
일본국 군마켄 오타시 오시마쵸 440-23
(뒷면에 계속)
(74) 대리인
김영철

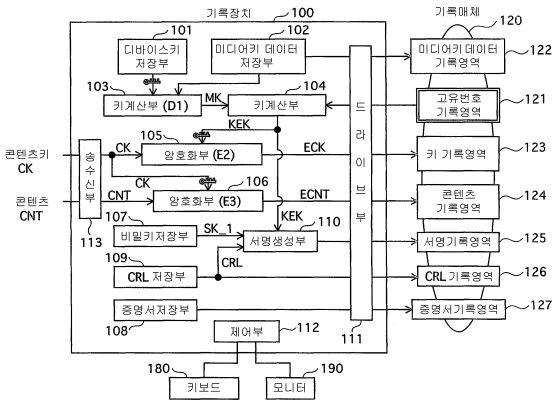
전체 청구항 수 : 총 7 항 심사관 : 안지현

(54) 저작물 보호시스템

(57) 요 약

콘텐츠의 부정 이용을 방지할 수 있는 기록장치 및 재생장치를 제공한다. 기록매체는 재기입 불가영역에 매체 고유번호를 기록하고 있다. 재생장치는 미디어 키 데이터 및 암호화 콘텐츠를 상기 기록매체에 기입한다. 상기 미디어 키 데이터는, 무효화 되어 있지 않은 각 재생장치에 대하여 미디어 키가, 무효화 된 각 재생장치에 대하여 소정의 검지정보가, 각각 당해 재생장치의 디바이스 키를 이용하여 암호화 되어서 생성된 복수의 암호화 미디어 키로 구성된다. 재생장치는, 디바이스 키를 이용하여 암호화 미디어 키를 복호 하여 복호 미디어 키를 생성하고, 복호 미디어 키가 검지정보인가 여부를 판단하여, 검지정보인 경우에, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 금지한다.

대 표 도 - 도2



(72) 발명자

후타 유이치

일본국 오오사카후 오오사카시 미야코지마쿠 다이토쵸 3-7-36

오모리 모토지

일본국 오오사카후 히라카타시 히가시타미야 1-7-30-103

다테바야시 마코토

일본국 효고켄 다카라즈카시 메후 1-16-21

하라다 ? 지

일본국 오오사카후 오오사카시 니시나리쿠 다마데니시 2-20-52

무라세 가오루

일본국 나라켄 나라시 진구 6-4-1-506

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

판독 전용의 재기입 불가영역과 판독 및 기입이 가능한 재기입 가능영역을 구비한 기록매체에 암호화 콘텐츠를 기록하는 기록장치와, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 시도하는 복수의 재생장치로 구성되는 디지털 저작물 보호시스템에서의 기록장치로,

상기 기록장치는,

(i) 무효화되어 있지 않은 복수의 재생장치 중에서 무효화되어 있지 않은 각각의 재생장치에 대하여, (ii) 상기 무효화되어 있지 않은 각각의 재생장치에 할당된 디바이스 키에 기초하여 미디어 키를 암호화함으로써 생성된

복수의 암호화 미디어 키를 포함하는 미디어 키 데이터를 기억하고 있는 기억수단과,

상기 콘텐츠를 상기 기록매체에 기록할 때 상기 미디어 키 데이터가 상기 기록매체에 존재하는가 여부를 확인하는 존재확인수단과,

디지털 데이터인 상기 콘텐츠를 콘텐츠 키에 기초하여 암호화하여 상기 암호화 콘텐츠를 생성하는 콘텐츠 암호화수단과,

상기 존재확인수단이 상기 기록매체에 상기 미디어 키 데이터가 존재하지 않는다는 것을 확인한 때, 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터로부터 취득한 미디어 키에 기초하여 상기 콘텐츠 키를 암호화함으로써 암호화 콘텐츠 키를 생성하는 키 암호화수단과,

상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터를 상기 기록매체의 상기 재기입 가능영역에 기록하는 기입수단을 포함하며,

상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 미디어 키 데이터는 상기 존재확인수단이 상기 미디어 키 데이터가 상기 기록매체에 존재하지 않는다는 것을 확인한 때에 상기 기록매체의 상기 재기입 가능영역에 기록되고,

상기 존재 확인수단은 상기 콘텐츠를 상기 기록매체에 기입할 때, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터, 또는 (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터가 상기 기록매체에 존재하는가 여부를 확인하고,

상기 키 암호화수단은 상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 것도 상기 기록매체에 존재하지 않는다는 것을 확인한 경우, 상기 기억수단에 기억되어 있는 미디어 키 데이터로부터 얻은 상기 미디어 키에 기초하여 상기 콘텐츠 키를 암호화하여 암호화 콘텐츠 키를 생성하며,

상기 기입수단은 상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 것도 상기 기록매체에 존재하지 않는다는 것을 확인한 경우, 상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터를 상기 기록매체의 재기입 가능영역에 기록하고,

상기 기록매체에 기록되어 있는 미디어 키 데이터를 상기 기억수단에 기억되어 있는 미디어 키 데이터와 비교하여, 상기 기록매체에 기록되어 있는 미디어 키 데이터와 상기 기억수단에 기억되어 있는 미디어 키 데이터 중 어느 것이 더 새로운가를 판정하는 비교수단과,

상기 기억수단에 기억되어 있는 상기 미디어 키 데이터를 갱신하는 갱신수단을 더 포함하며,

상기 비교수단은,

상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 하나가 상기 기록매체에 존재한다고 확인한 경우에 상기 비교를 수행하고,

상기 존재 확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 하나가 상기 기록매체에 존재한다고 판정하고, 상기 비교수단이 상기 기록매체에 기록되어 있는 미디어 키 데이터가 더 새로운 것으로 판정한 경우에, 상기 갱신수단은 상기 기록매체로부터 상기 미디어 키 데이터를 판독하여, 상기 기록매체로부터 판독한 미디어 키 데이터로 상기 기억수단에 기억되어 있는 미디어 키 데이터를 갱신하는 것을 특징으로 하는 기록장치.

청구항 47

제 46 항에 있어서,

상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이

터 중 어느 하나가 상기 기록매체에 존재한다고 판정하고, 상기 비교수단이 상기 기록매체에 기록되어 있는 미디어 키 데이터가 더 오래된 것으로 판정한 경우, 상기 키 암호화수단은 상기 기억수단에 기억되어 있는 미디어 키 데이터로부터 얻은 미디어 키에 기초하여 상기 콘텐츠 키를 암호화하여 상기 암호화 콘텐츠 키를 생성하며,

상기 기입수단은 상기 암호화 콘텐츠 키를 상기 기록매체의 재기입 가능영역에 더 기록하는 것을 특징으로 하는 기록장치.

청구항 48

제 47 항에 있어서,

상기 기록매체의 재기입 가능영역으로부터 상기 암호화 콘텐츠 키를 판독하는 판독수단과,

상기 기록매체에 기록되어 있는 미디어 키 데이터로부터 얻은 미디어 키에 기초하여 상기 판독한 암호화 콘텐츠 키를 복호하여 상기 콘텐츠 키를 생성하는 콘텐츠 키 복호수단을 더 포함하고,

상기 키 암호화수단은 상기 기억수단에 기억되어 있는 미디어 키 데이터로부터 얻은 미디어 키에 기초하여 상기 콘텐츠 키 복호수단이 생성한 상기 콘텐츠 키를 더 암호화하여 상기 암호화 콘텐츠 키를 생성하고,

상기 기입수단은 상기 암호화 콘텐츠 키를 상기 기록매체의 재기입 가능영역에 더 기록하는 것을 특징으로 하는 기록장치.

청구항 49

제 46 항에 있어서,

상기 기억수단에 기억되어 있는 미디어 키 데이터는 상기 기억수단에 기억되어 있는 당해 미디어 키 데이터의 세대를 나타내는 제 1 버전 정보를 포함하고,

상기 기록매체에 기록되어 있는 상기 미디어 키 데이터는 상기 기록매체에 기록되어 있는 당해 미디어 키 데이터의 세대를 나타내는 제 2 버전 정보를 포함하며,

상기 비교수단은 상기 제 1 버전 정보와 상기 제 2 버전 정보를 비교함으로써 (i) 상기 기억수단에 기억되어 있는 미디어 키 데이터와 (ii) 상기 기록매체에 기록되어 있는 미디어 키 데이터 중 어느 것이 더 새로운가를 판정하는 것을 특징으로 하는 기록장치.

청구항 50

제 46 항에 있어서,

상기 기억수단에 기억되어 있는 상기 미디어 키 데이터는 상기 기억수단에 기억되어 있는 당해 미디어 키 데이터가 생성된 시각을 나타내는 제 1 시각 정보를 포함하고,

상기 기록매체에 기록되어 있는 미디어 키 데이터는 상기 기록매체에 기록되어 있는 당해 미디어 키 데이터가 생성된 시각을 나타내는 제 2 시각 정보를 포함하며,

상기 비교수단은 상기 제 1 시각 정보와 상기 제 2 시각 정보를 비교함으로써 (i) 상기 기억수단에 기억되어 있는 미디어 키 데이터와 (ii) 상기 기록매체에 기록되어 있는 미디어 키 데이터 중 어느 것이 더 새로운가를 판정하는 것을 특징으로 하는 기록장치.

청구항 51

삭제

청구항 52

삭제

청구항 53

판독 전용의 재기입 불가영역과 판독 및 기입이 가능한 재기입 가능영역을 구비한 기록매체에 암호화 콘텐츠를 기록하는 기록장치와, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 시도하는 복수의 재생장치로 구

성되는 디지털 저작물 보호시스템에서의 기록장치로,

상기 기록장치는,

(i) 무효화되어 있지 않은 복수의 재생장치 중에서 무효화되어 있지 않은 각각의 재생장치에 대하여, (ii) 상기 무효화되어 있지 않은 각각의 재생장치에 할당된 디바이스 키에 기초하여 미디어 키를 암호화함으로써 생성된 복수의 암호화 미디어 키를 포함하는 미디어 키 데이터를 기억하고 있는 기억수단과,

상기 콘텐츠를 상기 기록매체에 기록할 때 상기 미디어 키 데이터가 상기 기록매체에 존재하는가 여부를 확인하는 존재확인수단과,

디지털 데이터인 상기 콘텐츠를 콘텐츠 키에 기초하여 암호화하여 상기 암호화 콘텐츠를 생성하는 콘텐츠 암호화수단과,

상기 존재확인수단이 상기 기록매체에 상기 미디어 키 데이터가 존재하지 않는다는 것을 확인한 때, 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터로부터 취득한 미디어 키에 기초하여 상기 콘텐츠 키를 암호화함으로써 암호화 콘텐츠 키를 생성하는 키 암호화수단과,

상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터를 상기 기록매체의 상기 재기입 가능영역에 기록하는 기입수단을 포함하며,

상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 미디어 키 데이터는 상기 존재확인수단이 상기 미디어 키 데이터가 상기 기록매체에 존재하지 않는다는 것을 확인한 때에 상기 기록매체의 상기 재기입 가능영역에 기록되고,

상기 존재 확인수단은 상기 콘텐츠를 상기 기록매체에 기입할 때, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터, 또는 (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터가 상기 기록매체에 존재하는가 여부를 확인하고,

상기 키 암호화수단은 상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 것도 상기 기록매체에 존재하지 않는다는 것을 확인한 경우, 상기 기억수단에 기억되어 있는 미디어 키 데이터로부터 얻은 상기 미디어 키에 기초하여 상기 콘텐츠 키를 암호화하여 암호화 콘텐츠 키를 생성하며,

상기 기입수단은 상기 존재확인수단이, (i) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 동일한 세대를 갖는 미디어 키 데이터와, (ii) 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터와 다른 세대를 갖는 미디어 키 데이터 중 어느 것도 상기 기록매체에 존재하지 않는다는 것을 확인한 경우, 상기 암호화 콘텐츠, 상기 암호화 콘텐츠 키 및 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터를 상기 기록매체의 재기입 가능영역에 기록하고,

상기 기억수단에 기억되어 있는 미디어 키 데이터는 상기 기억수단에 기억되어 있는 미디어 키 데이터를 식별하는 제 1 데이터 식별자를 더 포함하며,

상기 기입수단은, (i) 상기 제 1 데이터 식별자와 상기 암호화 콘텐츠를 대응시켜서 상기 기록매체의 상기 재기입 가능영역에 기록하고, (ii) 상기 제 1 데이터 식별자를 포함하는 상기 미디어 키 데이터를 상기 기록매체의 재기입 가능영역에 기록하고,

상기 기억수단에 기억되어 있는 미디어 키 데이터를 상기 기록매체에 기록되어 있는 미디어 키 데이터와 비교하여, 상기 기억수단에 기억되어 있는 미디어 키 데이터와 상기 기록매체에 기록되어 있는 미디어 키 데이터 중 어느 것이 더 새로운가를 판정하는 비교수단과,

상기 기억수단에 기억되어 있는 미디어 키 데이터가 더 새로운 것으로 판정된 때에 상기 제 1 데이터 식별자를 상기 기억수단에 기억되어 있는 미디어 키 데이터에 할당하는 할당수단을 더 포함하는 것을 특징으로 하는 기록장치.

청구항 54

제 53 항에 있어서,

상기 기억수단에 기억되어 있는 미디어 키 데이터는 상기 기억수단에 기억되어 있는 당해 미디어 키 데이터가 생성된 시각을 나타내는 제 1 시각 정보를 포함하고,

상기 기록매체에 기록되어 있는 미디어 키 데이터는 상기 기록매체에 기록되어 있는 당해 미디어 키 데이터가 생성된 시각을 나타내는 제 2 시각 정보를 포함하며,

상기 비교수단은 상기 제 1 시각 정보와 상기 제 2 시각 정보를 비교함으로써 (i) 상기 기억수단에 기억되어 있는 미디어 키 데이터와 (ii) 상기 기록매체에 기록되어 있는 미디어 키 데이터 중 어느 것이 더 새로운가를 판정하는 것을 특징으로 하는 기록장치.

청구항 55

삭제

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 디지털 데이터를 대용량의 기록매체에 기록하여 재생하는 기술에 관한 것으로, 특히 부정한 장치(Illegitimate Apparatus)에 의한 콘텐츠의 부정한 기록 및 부정한 재생을 방지하는 기술에 관한 것이다.

배 경 기 술

[0002] 최근, 멀티미디어 관련 기술의 발전 및 대용량 기록매체의 출현 등을 배경으로 하여, 동화상, 음성 등으로 이루어지는 디지털 콘텐츠(이하, 콘텐츠라 한다)를 생성하여 광디스크 등의 대용량 기록매체에 저장하여 배포하거나, 또는 네트워크를 경유하여 배포하는 시스템이 보급해 가고 있다.

[0003] 배포된 콘텐츠는 컴퓨터나 재생장치 등으로 판독되며, 재생 또는 복제의 대상이 된다.

[0004] 일반적으로, 콘텐츠의 저작권을 보호하기 위해, 즉 콘텐츠의 부정 재생이나 부정 복제 등을 방지하기 위해 암호화기술이 사용된다. 구체적으로는, 기록장치는 콘텐츠를 암호화 키를 이용하여 암호화해서 광디스크 등의 기록매체에 기록하여 배포한다. 이에 대해, 그 암호화 키에 대응하는 복호 키를 보유하는 재생장치만이 기록매체로부터 판독된 암호 콘텐츠를 그 복호 키를 이용하여 복호 해서 콘텐츠의 재생 등을 행할 수 있다.

[0005] 또한, 콘텐츠를 암호화하여 기록매체에 기록할 때에는, 재생장치가 보유하는 복호 키를 이용하여, 콘텐츠 그 자체를 암호화하여 기록하는 방법이나, 콘텐츠를 어떤 키로 암호화하여 기록한 다음, 그 키에 대응하는 복호용의 키를 재생장치가 보유하는 복호 키에 대응하는 암호화 키로 암호화하여 기록하는 방법 등이 사용된다.

[0006] 이때, 재생장치가 보유하는 복호 키는 외부에 노출되지 않도록 엄중하게 관리될 필요가 있으나, 부정 사용자(Illegitimate User)에 의한 당해 재생장치 내부의 부정한 해석에 의해, 복호 키가 외부로 유출될 위험성이 있다. 복호 키가 일반 부정 사용자에 의해 유출되어 버리면, 이 부정 사용자는 콘텐츠를 부정으로 이용하는 기록장치, 재생장치를 제조하여 불법으로 판매하거나, 또는 콘텐츠를 부정 이용하기 위한 컴퓨터 프로그램을 작성하여, 인터넷 등에 의해 이와 같은 프로그램을 배포하는 것을 생각할 수 있다.

[0007] 이와 같은 경우, 저작권자는 일단 유출된 복호 키로는 다음부터 제공하는 콘텐츠를 취급하지 않도록 하기를 원한다. 이와 같은 것을 실현하는 기술을 키 무효화 기술이라고 하며, 특허문헌 1에 의해 키 무효화를 실현하는 시스템이 개시되어 있다.

[0008] 종래의 키 무효화 기술에서는, 미리, 기록매체의 재기입 불가영역(Un-rewritable Area)에 장치가 보유하는 키가

무효화 되어 있다는 취지를 나타내는 키 무효화정보를 기록하고 있다. 장치는, 기록매체에 기록되어 있는 키 무효화정보를 이용하여 당해 장치가 보유하는 키가 무효화 되어 있는가 여부를 판단하여, 무효화 된 키를 보유하는 경우에는, 당해 장치는 상기 기록매체를 이용할 수 없도록 하고 있다. 또, 새로운 키의 무효화가 발생하면, 상기 키 무효화정보는 갱신되고, 이 무효화 발생 이후에 제조되는 새로운 기록매체에는 갱신 후의 키 무효화정보가 기록된다. 이렇게 하여 무효화 된 키로는 새로운 기록매체를 이용할 수 없는 체제로 되어 있다.

[0009] 한편, 광디스크 등의 기록매체에 기록되어 있는 콘텐츠의 판독이나 기입은 광디스크 드라이브라고 불리는 퍼스널컴퓨터 주변기기로 행하는 것이 일반적이나, 기기의 호환성을 달성하기 위해, 그 입출력방법은 공개된 정보로 표준화되며, 비밀로는 되지 않는 것이 일반적이다. 이 때문에, 기록매체에 기록되어 있는 콘텐츠는 퍼스널컴퓨터 등에 의해 용이하게 판독할 수 있으며, 또, 판독 데이터를 다른 기록매체에 기입하는 것도 용이하다. 따라서 콘텐츠의 저작권을 보호하는 시스템에 있어서는, 기록매체 상의 데이터를 판독하여 다른 기록매체에 기입하는, 통상의 사용자(User)가 행할 수 있는 행위에 대하여, 그것을 방지하는 유효한 기능을 구비하는 시스템이어야 한다. 기록매체에서 판독한 데이터가 다른 기록매체에 기입되는 것을 방지하는 기술을 미디어 바인드 기술(Media Bind Technique)이라고 하며, 특허문헌 2에 의해 미디어 바인드를 실현하는 메커니즘이 개시되어 있다.

[0010] 종래의 미디어바인드 기술을 이용하여 저작권 보호를 실현하기 위해, 미리, 기록매체의 재기입 불가영역에는 기록매체를 식별하는 식별자가 기록되어 있고, 당해 기록매체에 기록되어 있는 암호화 콘텐츠는 이 매체 식별자에 의거하여 암호화되어 있다, 따라서 암호화 콘텐츠만을 다른 기록매체에 복제해도, 다른 기록매체는 별도의 다른 의 매체 식별자를 기록하고 있어서, 이 별도의 다른 매체 식별자에 의거하여 암호화 콘텐츠를 올바르게 복호 할 수는 없다.

[0011] 그러나 콘텐츠의 부정한 이용의 확대를 방지하기 위해, 다양한 부정방지기술의 실현이 요구되고 있다.

[0012] <특허문헌 1>

[0013] 일본국 특개2002-281013호 공보

[0014] <특허문헌 2>

[0015] 일본국 특허 제3073590호 공보

[0016] <특허문헌 3>

[0017] 일본국 특개평09-160492호 공보

발명의 상세한 설명

[0018] 본 발명은, 상기 요구에 대처하기 위하여, 콘텐츠의 부정 이용을 방지할 수 있는 저작물 보호시스템, 기록장치, 기록방법, 재생장치, 재생방법, 컴퓨터 프로그램 및 기록매체를 제공함을 목적으로 한다.

[0019] 상기 목적을 달성하기 위해 본 발명은, 기록매체에 콘텐츠를 암호화하여 기입하는 기록장치와, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 시도하는 복수의 재생장치로 구성되는 저작물 보호시스템이다.

[0020] 상기 복수의 재생장치 중 어느 1대 이상은 무효화 되어 있다.

[0021] 상기 기록매체는, 판독 전용의 재기입 불가영역과, 판독 및 기입이 가능한 재기입 가능영역을 구비하며, 상기 재기입 불가영역에는 당해 기록매체에 고유한 매체 고유번호가 미리 기록되어 있다.

[0022] 상기 기록장치는, 무효화 되어 있지 않은 각 재생장치에 대하여 미디어 키가, 무효화 된 각 재생장치에 대하여 소정의 검지정보가, 각각 당해 재생장치의 디바이스 키를 이용하여 암호화 되어서 생성된 복수의 암호화 미디어 키로 구성되는 미디어 키 데이터를 기억하고 있는 기억수단과, 상기 기록매체의 상기 재기입 불가영역에서 상기 매체 고유번호를 판독하는 판독수단과, 판독한 상기 매체 고유번호 및 상기 미디어 키에 의거하여 암호화 키를 생성하는 생성수단과, 생성된 상기 암호화 키에 의거하여 디지털 데이터인 콘텐츠를 암호화하여 암호화 콘텐츠를 생성하는 암호화수단과, 상기 기억수단에서 상기 미디어 키 데이터를 판독하는 판독수단과, 판독된 상기 미디어 키 데이터 및 생성된 상기 암호화 콘텐츠를 상기 기록매체의 상기 재기입 가능영역에 기입하는 기입수단을 구비하고 있다.

[0023] 각 재생장치는, 상기 기록매체의 상기 재기입 가능영역에 기입된 미디어 키 데이터에서 당해 재생장치에 대응하는 암호화 미디어 키를 판독하는 판독수단과, 당해 재생장치의 디바이스 키를 이용하여 판독된 상기 암호화 미디어 키를 복호 해서 복호 미디어 키를 생성하는 복호수단과, 생성된 복호 미디어 키가 상기 검지정보인가 여부

를 판단하고, 상기 검지정보인 경우에 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 금지하고, 검지정보가 아닌 경우에 암호화 콘텐츠의 복호를 허가하는 제어수단과, 복호가 허가된 경우에, 상기 기록매체에서 상기 암호화 콘텐츠를 판독하고, 생성된 복호 미디어 키에 의거하여 판독한 상기 암호화 콘텐츠를 복호 하여 복호 콘텐츠를 생성하는 복호수단을 구비한다.

[0024] 이 구성에 의하면, 상기 기록장치는, 무효화 되어 있지 않은 각 재생장치에 대하여 미디어 키가, 무효화 된 각 재생장치에 대하여 소정의 검지정보가, 각각 당해 재생장치의 디바이스 키를 이용하여 암호화 되어서 생성된 복수의 암호화 미디어 키로 구성되는 미디어 키 데이터를 기록매체에 기입하며, 또, 매체 고유번호 및 상기 미디어 키에 의거하여 암호화 키를 생성하며, 생성된 상기 암호화 키에 의거하여 생성된 암호화 콘텐츠를 기록매체에 기입한다. 또 재생장치는, 디바이스 키를 이용하여 암호화 미디어 키를 복호 해서 복호 미디어 키를 생성하고, 생성한 복호 미디어 키가 상기 검지정보인 경우에, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 금지한다.

[0025] 이와 같이 구성되어 있으므로, 무효화 된 재생장치를 배제할 수 있다.

[0026] 여기서, 다른 기록매체(상기 기록매체와는 별개의 제 2 기록매체, 이하 같다)는, 무효가 되어 있지 않은 각 재생장치에 대해서 미디어 키가, 무효화 된 각 재생장치에 대해서 소정의 검지정보가, 각각 당해 재생장치의 디바이스 키를 이용하여 암호화 되어서 생성된 복수의 다른 암호화 미디어 키로 구성되는 다른 미디어 키 데이터를 기억하고 있다. 상기 기록장치는, 상기 다른 기록매체에 기억되어 있는 다른 미디어 키 데이터와, 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터의 신, 구를 비교하는 비교수단과, 상기 다른 미디어 키 쪽이 새롭다고 판단되는 경우에, 상기 다른 기록매체에서 상기 다른 미디어 키 데이터를 판독하고, 판독한 상기 다른 미디어 키 데이터를 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터에 덮어쓰는(Overwrite) 갱신수단을 더 구비하고, 상기 판독수단은, 상기 미디어 키 데이터의 판독에 대신하여, 상기 기억수단에서 상기 다른 미디어 키 데이터를 판독하고, 상기 기입수단은, 상기 미디어 키 데이터의 기입에 대신하여, 판독된 상기 다른 미디어 키 데이터를 상기 기록매체의 상기 재기입 가능영역에 기입한다.

[0027] 이 구성에 의하면, 기록장치는 내부에 기억하고 있는 미디어 키 데이터를 다른 기록매체에서 취득한 다른 암호화 미디어 키로 갱신할 수 있다.

[0028] 여기서, 상기 기억수단은 당해 기록장치 및 상기 복수의 재생장치 중 어느 하나에 할당된 공개 키가 무효화되어 있는 것을 나타내는 무효화 데이터를 더 기억하고 있고, 상기 기록장치는 상기 무효화 데이터에 대하여 디지털 서명을 실시하여 검증정보를 생성하는 서명생성수단을 더 구비하며, 상기 기입수단은 생성한 상기 검증정보를 상기 기록매체의 상기 재기입 가능영역에 더 기입한다. 또, 상기 기록장치는, 당해 기록장치 및 상기 복수의 재생장치 중 어느 하나에 할당된 공개 키가 무효화되어 있는 것을 나타내는 무효화 데이터를 더 기억하고 있고, 상기 무효화 데이터에 대하여 디지털 서명을 실시하여 검증정보를 생성하여, 생성한 상기 검증정보를 상기 기록매체의 상기 재기입 가능영역에 더 기입하며, 상기 판독수단은 상기 기록매체의 상기 재기입 가능영역에 기입된 상기 검증정보를 더 판독하고, 상기 재생장치는, 판독한 상기 검증정보에 의거하여 서명 검증을 실시하여, 검증의 성공 또는 실패를 나타내는 검증 결과를 출력하는 검증수단을 더 구비하며, 상기 제어수단은, 상기 검증 결과가 검증의 실패를 나타내는 경우에 상기 암호화 콘텐츠의 복호를 금지하고, 상기 검증 결과가 검증의 성공을 나타내는 경우에 상기 암호화 콘텐츠의 복호를 허가한다.

[0029] 이 구성에 의하면, 기록장치는 디지털 서명에 의해 생성한 검증정보를 기록매체에 더 기록하므로, 재생장치에서 검증정보를 검증함으로써, 부정한 재생장치를 배제할 수 있다.

[0030] 여기서, 상기 기억수단은 당해 기록장치의 공개키증명서를 더 기억하고 있고, 상기 판독수단은 상기 기억수단에서 상기 공개키 증명서를 더 판독하며, 상기 기입수단은 판독된 상기 공개키 증명서를 상기 기록매체의 상기 재기입 가능영역에 기입한다. 또, 상기 기록장치는, 당해 기록장치의 공개키 증명서를 더 기억하고 있고, 상기 공개키 증명서를 판독하여, 판독한 상기 공개키 증명서를 상기 기록매체의 상기 재기입 가능영역에 기입하며, 상기 재생장치는, 상기 기록장치 및 상기 복수의 재생장치 중 어느 하나에 할당된 공개 키가 무효화되어 있는 것을 나타내는 제 1 무효화 데이터를 기억하고 있는 기억수단과, 상기 기록매체에서 상기 공개키 증명서를 판독하는 증명서 판독수단과, 판독한 공개키 증명서에 포함되는 공개 키가 상기 제 1 무효화 데이터에 의해 무효화되어 있는가 여부를 검증하는 공개키 검증수단을 더 포함하며, 상기 제어수단은, 상기 공개 키가 무효화되어 있는 경우에 상기 암호화 콘텐츠의 복호를 금지하고, 상기 공개 키가 무효화되어 있지 않은 경우에 상기 암호화 콘텐츠의 복호를 허가한다.

[0031] 이 구성에 의하면, 기록장치는 공개키 증명서를 기록매체에 기입하고, 재생장치는, 기록매체에서 공개키 증명서를 판독하여, 공개 키가 무효화되어 있는 경우에 암호화 콘텐츠의 복호를 금지할 수 있다.

[0032] 여기서, 다른 기록매체는 상기 기록장치 및 상기 복수의 재생장치 중 어느 하나에 할당된 공개 키가 무효화되어 있는 것을 나타내는 제 2 무효화 데이터를 기억하고 있고, 상기 재생장치는, 상기 다른 기록매체에 기억되어 있는 상기 제 2 무효화 데이터와 상기 기억수단에 기억되어 있는 상기 제 1 무효화 데이터의 신, 구를 비교하는 비교수단과, 상기 제 2 무효화 데이터 쪽이 새로운 것으로 판단되는 경우에, 상기 다른 기록매체에서 상기 제 2 무효화 데이터를 판독하여, 판독한 상기 제 2 무효화 데이터를 상기 기억수단에 기억되어 있는 상기 제 1 무효화 데이터에 덮어쓰는 갱신수단을 더 포함한다.

[0033] 이 구성에 의하면, 재생장치는 무효화 된 데이터를 최신의 상태로 갱신할 수 있다.

[0034] 여기서, 상기 기억수단은 당해 기록장치를 식별하는 장치 식별자를 더 기억하고 있고, 상기 기록장치는, 상기 기억수단에서 상기 장치 식별자를 판독하고, 판독한 상기 장치 식별자를 상기 콘텐츠에 전자 워터마크(electronic watermark)로 삽입하는 삽입수단을 더 구비하며, 상기 암호화수단은 상기 장치 식별자가 삽입된 콘텐츠를 암호화한다. 또, 상기 재생장치는, 당해 재생장치를 식별하는 장치 식별자를 기억하고 있는 상기 기억수단과, 복호가 허가된 경우에 상기 기억수단에서 상기 장치 식별자를 판독하고, 판독한 상기 장치 식별자를 상기 암호화 콘텐츠에 전자 워터마크로서 삽입하는 삽입수단을 더 구비하며, 상기 장치 식별자가 삽입된 상기 암호화 콘텐츠를 상기 기록매체에 기입한다.

[0035] 기록장치 및 재생장치는, 장치 식별자가 삽입된 콘텐츠를 기록매체에 기입하므로, 상기 콘텐츠가 부정으로 유통한 경우에, 상기 콘텐츠에서 삽입된 장치 식별자를 추출함으로써, 그 콘텐츠를 기록한 기록장치 및 재생장치를 특정할 수 있다.

[0036] 여기서, 상기 기억수단에 기억되어 있는 상기 미디어 키 데이터는 당해 미디어 키 데이터를 식별하는 데이터 식별자를 더 포함하고, 상기 기입수단은, 상기 데이터 식별자와 상기 암호화 콘텐츠를 대응시켜서 상기 기록매체의 상기 재기입 가능영역에 기입하고, 상기 데이터 식별자를 포함하는 상기 미디어 키 데이터를 상기 재기입 가능영역에 기입한다. 또, 상기 기록매체에 기억되어 있는 상기 미디어 키 데이터는 당해 미디어 키 데이터를 식별하는 데이터 식별자를 더 포함하고, 상기 기록장치는, 상기 데이터 식별자와 상기 암호화 콘텐츠를 대응시켜서 상기 기록매체의 상기 재기입 가능영역에 기입하고, 상기 데이터 식별자를 포함하는 상기 미디어 키 데이터를 상기 재기입 가능영역에 기입하며, 상기 재생장치는, 상기 기록매체에 기록되어 있는 상기 암호화 콘텐츠의 지정을 접수하는 지정접수수단과, 지정이 접수된 상기 암호화 콘텐츠에 대응 지워진 상기 데이터 식별자를 상기 기록매체에서 판독하는 판독수단과, 판독한 상기 데이터 식별자를 포함하는 상기 미디어 키 데이터를 상기 기록매체에서 판독하는 판독수단을 더 포함하며, 상기 제어수단은 판독한 상기 미디어 키 데이터에 의거하여 상기 암호화 콘텐츠의 복호의 가부를 판단한다.

[0037] 기록장치는, 상기 데이터 식별자와 상기 암호화 콘텐츠를 대응시켜서 상기 기록매체에 기입하고, 상기 데이터 식별자를 포함하는 상기 미디어 키 데이터를 상기 기록매체에 기입하므로, 재생장치에서, 데이터 식별자를 거쳐서 암호화 콘텐츠에 대응하는 미디어 키 데이터를 취득하고, 취득한 미디어 키 데이터에 의거하여 암호화 콘텐츠의 복호의 가부를 판단할 수 있다.

실 시 예

[0058] 1. 제 1 실시 예

[0059] 본 발명에 관한 제 1 실시 예로서의 콘텐츠 공급시스템(10)에 대하여 설명한다.

[0060] 1. 1 콘텐츠 공급시스템(10)의 구성

[0061] 콘텐츠 공급시스템(10)은, 도 1에 도시한 바와 같이, 콘텐츠 서버장치(500), 기록장치(100) 및 재생장치(200a, 200b, 200c, 200d, 200e …)로 구성되어 있다. 기록장치(100) 및 재생장치(200a, 200b, 200c, 200d, 200e …)의 대수의 합계는 n대이다. 기록장치(100)에는 장치 번호 「1」이 할당되어 있고, 재생장치(200a, 200b, 200c, 200d, 200e …)에는 각각 장치번호 「2」, 「3」, 「4」, …「n」이 할당되어 있다. 각 장치는 할당된 각 장치번호에 의해 식별된다.

[0062] 이들 n대의 장치 중, 재생장치 200b 및 재생장치 200c는 부정한 제3자에 의한 부정한 공격을 받았으므로, 본래 비밀로 내장해야 할 키가 유출되어 있고, 이 때문에, 재생장치 200b 및 재생장치 200c는 무효화 되어 있다.

[0063] 음악이나 영화 등의 콘텐츠 공급업자는, 콘텐츠 서버장치(500) 및 기록장치(100)를 가지고 있고, 콘텐츠 서버장치(500)와 기록장치(100)는 전용회선(30)을 경유하여 서로 접속되어 있다.

[0064] 콘텐츠 서버장치(500)는, 콘텐츠 및 상기 콘텐츠를 암호화할 때에 사용되는 콘텐츠 키를 가지고 있고, 기록장치(100)로부터의 요구에 의해 콘텐츠 및 대응하는 콘텐츠 키를 전용회선(30)을 거쳐서 기록장치(100)에 송신한다.

[0065] 기록장치(100)는, 콘텐츠 서버장치(500)로부터 전용회선(30)을 거쳐서 콘텐츠 및 대응하는 콘텐츠 키를 취득하고, 취득한 콘텐츠와 콘텐츠 키를 암호화하여, 암호화 콘텐츠, 암호화 콘텐츠 키 및 기타 관련하는 정보를 기록매체(120)에 기입한다.

[0066] 암호화 콘텐츠, 암호화 콘텐츠 키 및 기타 관련정보가 기록된 기록매체(120)는 판매점에서 판매하며, 이용자는 기록매체(120)를 구입한다.

[0067] 이용자가 갖는 재생장치(200a)는, 기록매체(120)가 장착되면, 기록매체(120)로부터 암호화 콘텐츠, 암호화 콘텐츠 키 및 기타 관련정보를 판독하고, 판독한 기타 관련정보를 이용하여 콘텐츠의 복호의 가부를 판단하여, 복호가 가능하다고 판단되는 경우에, 암호화 콘텐츠 키로부터 복호 콘텐츠 키를 생성하고, 복호 콘텐츠 키를 이용하여 복호 콘텐츠를 생성하며, 생성한 복호 콘텐츠로부터 영화나 음악을 생성하여 출력한다.

[0068] 1. 2 콘텐츠 서버장치(500)

[0069] 콘텐츠 서버장치(500)는, 정보기억부(500), 제어부(502), 입력부(503), 표시부(504) 및 송수신부(505)로 구성되어 있다(미도시).

[0070] 콘텐츠 서버장치(500)는, 구체적으로는, 마이크로프로세서, ROM, RAM, 하드디스크 유닛, 통신유닛, 디스플레이 유닛, 키보드, 마우스 등으로 구성되는 컴퓨터시스템이다. 상기 RAM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 콘텐츠 서버장치(500)의 각 구성요소는 그 기능을 달성한다.

[0071] 송수신부(505)는, 전용회선(30)을 경유하여 기록장치(100)에 접속되어 있고, 기록장치(100)와 제어부(502) 사이에서 송수신을 행한다.

[0072] 정보기억부(501)는, 영상정보 및 음성정보가 고 효율로 압축 부호화 되어서 생성된 콘텐츠와, 콘텐츠를 암호화할 때에 키로서 이용되는 콘텐츠 키의 세트를 복수 개 미리 기억하고 있다.

[0073] 제어부(502)는, 기록장치(100)로부터, 전용회선(30) 및 송수신부(505)를 거쳐서, 어느 하나의 콘텐츠의 취득 요구를 수신한다. 상기 취득요구를 수신하면, 제어부(502)는 정보기억부(501)에서 상기 취득요구에 의해 제시되는 콘텐츠 및 콘텐츠 키를 판독하고, 판독한 콘텐츠 및 콘텐츠 키를 송수신부(505) 및 전용회선(30)을 거쳐서 기록장치(100)에 송신한다.

[0074] 입력부(503)는, 콘텐츠 서버장치(500)의 조작자의 지시를 접수하고, 접수한 지시를 제어부(502)에 출력한다.

[0075] 표시부(504)는 제어부(502)의 제어에 의해 각종 정보를 표시한다.

[0076] 1. 3 기록장치(100)

[0077] 기록장치(100)는, 도 2에 도시한 바와 같이, 디바이스 키 저장부(101), 미디어 키 데이터 저장부(102), 키 계산부 103, 키 계산부 104, 암호화부 105, 암호화부 106, 비밀 키 저장부(107), 증명서 저장부(108), CRL 저장부(109), 서명생성부(110), 드라이브부(111), 제어부(112) 및 송수신부(113)로 구성되어 있다.

[0078] 기록장치(100)는, 구체적으로는, 콘텐츠 서버장치(500)와 마찬가지로, 마이크로프로세서, ROM, RAM, 하드디스크 유닛 등으로 구성되는 컴퓨터시스템이다. 상기 RAM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로프로세서가 상기 프로그램에 따라서 동작함으로써 기록장치(100)는 그 기능을 달성한다.

[0079] (1) 디바이스 키 저장부(101)

[0080] 디바이스 키 저장부(101)는 외부의 장치로부터 액세스가 불가능하도록 디바이스 키 DK_1을 비밀로 기억하고 있다. 디바이스 키 DK_1은 기록장치(100)에 고유한 키이다. 또한, 본 명세서에 있어서, 장치 m이 보유하는 디바이스 키를 DK_1로 표현하고 있다.

[0081] (2) 미디어 키 데이터 저장부(102)

[0082] 미디어 키 데이터 저장부(102)는 미디어 키 데이터 MDATA를 기억하고 있다. 미디어 키 데이터 MDATA는 n개의 세

트를 포함하며, 각 세트는 암호화 미디어 키 및 장치번호로 구성되어 있다. 각 세트에 포함되어 있는 암호화 미디어 키와 장치번호는 대응하고 있다. 여기서 n은, 앞에서 설명한 바와 같이, 기록장치(100) 및 재생장치(200a, 200b, …)의 대수의 합계 값이다.

[0083] n개의 세트 중, 제 1 세트는 제 1 암호화 미디어 키 및 장치번호 「1」로 구성되어 있다. 장치번호 「1」은 기록장치(100)를 식별하는 식별정보이다. 제 1 암호화 미디어 키는 장치번호 「1」에 의해 식별되는 장치, 즉, 기록장치(100)에 할당된 디바이스 키 DK_1을 이용하여, 미디어 키 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0084] ? 제 1 암호화 미디어 키 = E1(DK_1, MK)

[0085] 여기서, 암호화 알고리즘 E1은, 일 예로서, DES(Data Encryption Standard)에 의한 것이다. 또, E(A, B)는, 키 A를 이용하여, 평문 B에 대하여 암호화 알고리즘 E를 실시하여 얻어진 암호문을 나타내고 있다.

[0086] 또, 미디어 키 MK는 기록매체(120)에 고유한 키이다.

[0087] 또, n개의 세트 중, 제 2 세트는 각각 제 2 암호화 미디어 키 및 장치번호 「2」로 구성되어 있다. 여기서, 장치번호 「2」는 재생장치 200a를 식별한다. 또, 제 2 암호화 미디어 키는 장치번호 「2」의 장치, 즉, 재생장치 200a에 할당된 디바이스 키 DK_2를 이용하여, 미디어 키 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0088] ? 제 2 암호화 미디어 키 = E1(DK_2, MK)

[0089] 또, n개의 세트 중, 제 3, 제 4 세트는, 각각 제 3 암호화 미디어 키 및 장치번호 「3」, 제 4 암호화 미디어 키 및 장치번호 「4」로 구성되어 있다. 여기서, 장치번호 「3」 및 「4」는 각각 재생장치 200b, 200c를 식별한다. 또, 제 3, 제 4 암호화 미디어 키는 각각 장치번호 「3」, 「4」에 의해 식별되는 장치, 즉, 재생장치 200b, 200c에 할당된 디바이스 키 DK_3, DK_4를 이용하여, 미디어 키 MK 대신 값「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0090] ? 제 3 암호화 미디어 키 = E1(DK_3, 0)

[0091] ? 제 4 암호화 미디어 키 = E1(DK_4, 0)

[0092] 여기서, 값 「0」은 미디어 키(MK)와는 전혀 관계가 없는 데이터이다.

[0093] 미디어 키 MK 대신 값 「0」을 이용하는 것은 제 3 및 제 4 암호화 미디어 키에 각각 대응하는 재생장치 200b 및 200c가 무효화 되어 있기 때문이며, 재생장치 200b 및 200c가 무효화 되어 있다는 것을 알기 위한 검지정보로 이용된다.

[0094] 무효화 된 장치에 대하여, 무효화 된 장치의 디바이스 키를 이용하여, 미디어 키 MK와는 전혀 관계가 없는 데이터, 즉 값 「0」을 암호화하여 암호화 미디어 키를 생성함으로써, 무효화 된 장치 이외의 모든 장치만이 미디어 키 MK를 공유할 수 있다. 또, 무효화 된 장치를 이 시스템으로부터 배제할 수 있다.

[0095] 여기서는, 값 「0」을 이용하고 있으나, 미디어 키 MK와는 전혀 관계가 없는 다른 데이터로 해도 된다. 예를 들어, 다른 고정 값인 「0xFFFF」, 암호화 미디어 키를 생성하는 시점의 일자나 시각을 나타내는 정보, 당해 무효화 된 장치의 디바이스 키 등이라도 된다.

[0096] 또한, 장치의 무효화 방법은 다른 방법을 이용해도 좋으며, 예를 들어, 특허문헌 1에는 트리구조를 이용한 무효화 방법이 개시되어 있다.

[0097] 또, n개의 세트 중, 제 5, …, 제 n 세트는 각각 제 5 암호화 미디어 키 및 장치번호 「5」, …, 제 n 암호화 미디어 키 및 장치번호 「n」으로 구성되어 있다. 여기서 장치번호 「5」, …, 「n」은 각각 재생장치 200d, 200e, …를 식별한다. 또, 제 5, …, 제 n 암호화 미디어 키는 각각 장치번호 「5」, …, 「n」의 장치, 즉, 재생장치 200d, 200e, …에 할당된 디바이스 키 DK_5, …, DK_n을 이용하여 미디어 키 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0098] ? 제 5 암호화 미디어 키 = E1(DK_5, MK)

[0099] ……

[0100] ? 제 n 암호화 미디어 키 = E1(DK_n, MK)

[0101] ⑶ 키 계산부(103)

[0102] 키 계산부(103)는 기록장치(100)에 할당된 장치번호 「1」을 미리 기억하고 있다.

[0103] 키 계산부(103)는, 미디어 키 데이터 저장부(102)에 기억되어 있는 미디어 키 데이터 MDATA를 구성하는 n개의 세트로부터 미리 기억하고 있는 장치번호 「1」을 포함하는 세트를 탐색하여 판독하고, 판독한 세트에서 장치번호 「1」에 대응하는 암호화 미디어 키 E1(DK_1, MK)을 추출한다.

[0104] 다음으로, 키 계산부 103은, 디바이스 키 저장부(101)에서 디바이스 키 DK_1을 판독하고, 판독한 디바이스 키 DK_1을 이용하여 추출한 암호화 미디어 키 E1(DK_1, MK)에 복호 알고리즘 D1을 실시하여 미디어 키 MK를 생성한다.

[0105] ? 미디어 키 MK = D1(DK_1, (E1(DK_1, MK))

[0106] 여기서, 복호 알고리즘 D1은 암호화 알고리즘 E1을 실시하여 생성된 암호문을 복호 하는 알고리즘이며, 일 예로서, DES에 의한 것이다. 또, D(A, B)는, 키 A를 이용하여, 암호문 B에 대해 복호 알고리즘 D를 실시하여 얻어진 복호 문을 나타내고 있다.

[0107] 다음에, 키 계산부 103은 생성한 미디어 키 MK를 키 계산부 104에 출력한다.

[0108] 또한, 도 2에서, 기록장치(100)의 각 구성부를 나타내는 각 블록은 접속 선에 의해 다른 블록과 접속되어 있다. 단, 일부의 접속 선을 생략하고 있다. 여기서, 각 접속 선은 신호나 정보가 전달되는 경로를 나타내고 있다. 또, 키 계산부 103을 표시하는 블록에 접속되어 있는 복수의 접속 선 중, 접속 선 상에 키 마크가 그려져 있는 것은 키 계산부 103에 키로서의 정보가 전달되는 경로를 나타내고 있다. 그 외의 구성요소를 나타내는 블록에 대해서도 동일하다. 또, 다른 도면에 대해서도 동일하다.

[0109] ⑷ 키 계산부 104

[0110] 키 계산부 104는, 키 계산부 103으로부터 미디어 키 MK를 취득하고, 드라이브부(111)를 거쳐서, 기록매체(120)의 고유번호 기록영역(12)으로부터 고유매체번호 MID를 판독한다,

[0111] 다음에, 키 계산부 104는, 취득한 미디어 키 MK와 판독한 매체고유번호 MID를 그 순서대로 결합하여, 결합 값(MK?MID)를 생성한다. 여기서, 「A?B」는 데이터 A와 데이터 B를 그 순서대로 비트 결합한 것을 나타낸다. 다음에, 키 계산부 104는 생성한 결합 값 (MK?MID)에 해시함수(Hash Function) SHA-1을 실시하여 해시함수 SHA-1(MK?MID)을 얻고, 얻어진 해시함수 H를 키 암호화 키 KEK로 하여, 키 암호화 키 KEK를 암호화부(105) 및 서명 생성부(110)에 출력한다.

[0112] 여기서, SHA-1(A)은, 해시함수 SHA-1을 실시하여 얻어진 해시 값을 키 암호화 키 KEK로 하고 있으나, 이에 한정되는 것은 아니다. 얻어진 해시 값의 일 부분을 키 암호화 키 KEK로 해도 된다.

[0113] 또, 해시함수 SHA-1에 대해서는 공지이므로 설명을 생략한다. 또한, 다른 해시함수를 사용해도 된다.

[0114] ⑸ 암호화부 105

[0115] 암호화부 105는, 콘텐츠 서버장치(500)로부터 송수신부(113)를 거쳐서 콘텐츠 키 CK를 취득하고, 키 계산부 104에서 키 암호화 키 KEK를 취득한다.

[0116] 다음에, 암호화부 105는, 취득한 키 암호화 키 KEK를 이용하여, 취득한 콘텐츠 키 CK에 암호화 알고리즘 E2를 실시하여, 암호화 콘텐츠 키 ECK를 생성한다.

[0117] ? 암호화 콘텐츠 키 ECK = E2(KEK, CK)

[0118] 여기서, 암호화 알고리즘 E2는, 일 예로서 DES이다.

[0119] 다음에, 암호화부 105는, 드라이브부(111)를 거쳐서 기록매체(120) 상에 기록영역(123)을 확보하고, 이어서, 생성한 암호화 콘텐츠 키 ECK를 드라이브부(111)를 거쳐서 기록매체(120)의 키 기록영역(123)에 기입한다.

[0120] ⑹ 암호화부 106

[0121] 암호화부 106은, 콘텐츠 서버장치(500)로부터 송수신부(113)를 거쳐서 콘텐츠 키 CK 및 콘텐츠 CNT를 취득하고, 취득한 콘텐츠 키 CK를 이용하여 취득한 콘텐츠 CNT에 암호화 알고리즘 E3을 실시하여 암호화 콘텐츠 ECNT를 생성한다.

[0122] ? 암호화 콘텐츠 ECNT = E3(CK, CNT)

[0123] 여기서, 암호화 알고리즘 E3은, 일 예로서, DES에 의한 것이다.

[0124] 다음에, 암호화부 106은 드라이브부(111)를 거쳐서 기록매체(120) 상에 콘텐츠 기록영역(124)을 확보하고, 이어서, 생성한 암호와 콘텐츠 ECNT를 드라이브부(111)를 거쳐서 기록매체(120)의 기록영역(124)에 기입한다.

[0125] ⑺ 비밀 키 저장부(107)

[0126] 비밀 키 저장부(107)는 외부장치로부터 액세스할 수 없도록 기록장치(100)의 비밀 키 SK_1을 기억하고 있다. 비밀 키 SK_1은 공개 키 암호방식에 의한 것이다. 여기서, 상기 공개 키 암호방식은, 일 예로서, RSA(Rivest Shamir Adleman) 암호방식이다.

[0127] ⑻ 증명서 저장부(108)

[0128] 증명서 저장부(108)는 공개 키 증명서 PKC를 기억하고 있다. 공개 키 증명서 PKC는, 증명서 식별자 ID_1, 공개 키 PK_1 및 서명데이터 Sig_1을 포함하여 구성된다.

[0129] 증명서 식별자 ID_1은 공개 키 증명서 PKC를 일의(一意)로 식별하는 식별정보이다. 공개 키 PK_1은 비밀 키 저장부(107)에 기억되어 있는 비밀 키 SK_1에 대응하는 공개 키이다. 또, 서명데이터 Sig_1은, 인증국 CA(Certificate Authority)의 비밀 키 SK_CA를 이용하여, 증명서 식별자 ID_1 및 공개 키 PK_1의 결합 값(ID_1?PK_1)에 대하여 디지털 서명 Sig를 실시하여 생성된 것이다.

[0130] ? 서명데이터 Sig_1 = Sig(SK_CA, ID_1?PK_1)

[0131] 여기서, Sig(A, B)는, 키 A를 이용하여, 데이터 B에 대해서, 디지털 서명 Sig를 실시하여 얻어진 서명데이터를 나타내고 있다. 또, 디지털 서명 Sig의 일 예는 해시함수 SHA-1을 사용한 RSA를 이용하는 디지털 서명이다.

[0132] ⑼ CRL저장부(109)

[0133] CRL저장부(109)는 제 1 시점에서의 무효화 된 공개키 증명서를 나타내는 공개 키 증명서 무효화리스트(이하, 무효화리스트 CRL이라 한다)를 기록하고 있다.

[0134] 무효화 리스트 CRL은, 1개 이상의 증명서 식별자와, 서명데이터 SigID와, 판수(版數)를 포함하고 있다.

[0135] 각 증명서 식별자는 무효화 된 공개 키 증명서를 식별하는 식별정보이다.

[0136] 서명데이터 SigID는, 인증국 CA의 비밀 키 SK_CA를 이용하여, 무효화리스트 CRL에 포함되는 모든 증명서 식별자의 결합 값에 대하여(무효화리스트 CRL에 1개의 증명서 식별자가 포함되어 있는 경우에는 상기 1개의 증명서 식별자에 대하여) 디지털 서명 Sig를 실시하여 생성된 것이다.

[0137] ? 서명데이터 SigID = Sig(SK_CA, 모든 증명서 식별자의 결합 값)

[0138] 예를 들어, 증명서 식별자 ID_3 및 ID_4에 의해 식별되는 공개키 증명서가 무효화 되어 있는 경우에는, 무효화리스트 CRL은, 증명서 식별자 ID_3, ID_4, 서명 SigID = Sig(SK_CA,(ID_3?ID_4)) 및 판수를 포함한다.

[0139] 판수는, 무효화 리스트 CRL의 세대를 나타내는 정보이며, 무효화 리스트 CRL이 상기 제 1 시점에서의 것이라는 것을 나타낸다. 판수는 공개키 증명서 무효화리스트의 세대가 새로울수록 큰 값을 취한다.

[0140] ⑽ 서명생성부(110)

[0141] 서명생성부(110)는, 비밀 키 저장부(107)에서 비밀 키 SK_1을 판독하고, CRL저장부(109)에서 무효화 리스트 CRL을 판독하며, 키 계산부 104에서 키 암호화 키 KEK를 취득한다.

[0142] 다음으로, 서명생성부(110)는 취득한 키 암호화 키 KEK와 판독한 무효화 리스트 CRL을 그 순서대로 결합하여 결합 값 (KEK?CRL)을 생성하고, 판독한 비밀 키 SK_1을 이용하여 생성한 결합 값 (KEK?CRL)에 디지털 서명 Sig를 실시하여 서명데이터 SigCRL을 생성한다.

[0143] ? 서명데이터 SigCRL = Sig(SK_1, (KEK?CRL))

[0144] 다음에, 서명생성부(110)는 드라이브부(111)를 거쳐서 기록매체(120) 상에 서명기록영역(125)을 확보하고, 이어서, 생성한 서명데이터 SigCRL을 드라이브부(111)를 거쳐서 기록매체(120)의 서명기록영역(125)에 기입한다.

[0145] ⑾ 제어부(112)

[0146] 제어부(112)는, 송수신부(113)를 거쳐서, 콘텐츠 서버장치(500)에 대하여 콘텐츠의 취득 요구를 송신한다.

[0147] 제어부(112)는, 증명서 저장부(108)로부터 공개 키 증명서 PKC를 판독하고, 드라이브부(111)를 거쳐서, 기록매체(120) 상에 증명서 기록영역(127)을 확보하며, 이어서, 판독한 공개 키 증명서 PKC를 드라이브부(111)를 거쳐서 기록매체(120)의 증명서 기록영역(127)에 기입한다.

[0148] 또, 제어부(112)는, 미디어 키 데이터 저장부(102)에서 미디어 키 데이터 MDATA를 판독하고, 드라이브부(111)를 거쳐서 기록매체(120) 상에 미디어 키 데이터 기록영역(122)을 확보하며, 이어서, 판독한 미디어 키 데이터 MDATA를 드라이브부(111)를 거쳐서 기록매체(120)의 미디어 키 데이터 기록영역(122)에 기입한다.

[0149] 또, 제어부(112)는, CRL 저장부(109)에서 무효화 리스트 CRL을 판독하고, 드라이브부(111)를 거쳐서 기록매체(120) 상에 CRL 기록영역(126)을 확보하며, 이어서, 판독한 무효화 리스트 CRL을 드라이브부(111)를 거쳐서 기록매체(120)의 CRL 기록영역(126)에 기입한다.

[0150] 제어부(112)는, 기록장치(100)의 조작자의 조작 지시에 의해 키보드(180)로부터 지시정보를 수신하며, 지시정보에 따라서 동작한다. 또, 기록장치(100)를 구성하는 다른 구성요소의 동작을 제어한다.

[0151] ⑿ 송수신부(113)

[0152] 송수신부(113)는, 전용회선(300을 경유하여 콘텐츠 서버장치(500)와 접속되어 있으며, 콘텐츠 서버장치(500)와 제어부(112) 사이에서 정보의 송수신을 행한다. 또, 제어부(112)의 제어에 의거, 콘텐츠 서버장치(500)와 암호화부 105 사이에서, 및 콘텐츠 서버장치(500)와 암호화부 106 사이에서 정보의 송수신을 행한다.

[0153] ⒀ 드라이브부(111)

[0154] 드라이브부(111)는, 제어부(112)의 제어에 의거, 기록매체(120)의 고유번호 기록영역(121)에서 매체고유번호 MID를 판독하고, 판독한 매체고유번호 MID를 키 계산부 114에 출력한다.

[0155] 또, 드라이브부(111)는, 제어부(112)의 제어에 의거, 암호화부 105, 암호화부 106, 서명생성부(110)에서 각각 정보를 취득하고, 취득한 정보를 기입하기 위한 각 영역을 기록매체(120) 상에 확보하며, 확보한 영역에 상기 정보를 기입한다.

[0156] 또, 드라이브부(111)는, 제어부(112)로부터 정보를 취득하고, 취득한 정보를 기입하기 위한 각 영역을 기록매체(120) 상에 확보하며, 확보한 영역에 상기 정보를 기입한다.

[0157] ⒁ 키보드(180) 및 모니터(190)

[0158] 키보드(180)는, 기록장치(100)의 조작자의 조작지시를 접수하고, 접수한 조작지시에 대응하는 지시정보를 제어부(112)에 출력한다.

[0159] 모니터(190)는 제어부(112)의 제어에 의해 각종 정보를 표시한다.

[0160] 1. 4 기록매체(120)

[0161] 기록매체(1200)는 광디스크 미디어이며, 도 3에 도시하는 바와 같이, 고유번호 기록영역(121)과, 일반영역(129)으로 구성되어 있다.

[0162] 고유번호 기록영역(121)에는 기록매체(120)를 식별하는 고유의 번호인 매체 고유번호 MID가 미리 기록되어 있다. 고유번호 기록영역(121)은 다른 정보의 기입이나 기록되어 있는 매체 고유번호 MID의 고쳐 쓰기가 불가능한 고쳐 쓰기 불가능영역이다. 매체 고유번호 MID는, 일 예로, 16진수 8자리로 표현되어 있고, 「0x00000006」이다. 또한, 본 명세서에서 「0x」는 이후의 표시가 16진수에 의한 것이라는 것을 가리킨다.

[0163] 일반영역(129)은, 다른 정보의 기입이 가능한 영역이며, 당초, 일반영역(129)에는 어떤 정보도 기입되어 있지 않다.

[0164] 기록장치(100)의 상술한 동작의 종료 후에 있어서, 일반영역(129)에는, 도 3에 도시하는 바와 같이, 미디어 키 데이터 기록영역(122), 키 기록영역(123), 콘텐츠 기록영역(124), 서명 기록영역(125), CRL 기록영역(126) 및 증명서 기록영역(127)이 확보된다.

[0165] 상술한 바와 같이, 제 1 실시 예에서는, 기록장치(100) 및 재생장치(200a, 200b, 200c, 200d, 200e, …)의 대수의 합계가 n대이고, 이들 장치 중, 재생장치 200b 및 재생장치 200c가 무효화 되어 있으며, n대의 장치는 각각 고유의 디바이스 키를 하나만 보유하고 있는 것으로 가정하고 있다. 이와 같은 가정에 의거, 기록매체(120)의 일반영역(129)에 포함되어 있는 각 영역에는 구체 예로서의 각종 데이터가 기록되어 있다.

[0166] <미디어 키 데이터 기록영역(122)>

[0167] 미디어 키 데이터 기록영역(122)에는 미디어 키 데이터 MDATA가 기록되어 있다. 미디어 키 데이터 MDATA는 n개의 세트로 구성되며, 각 세트는 암호화 미디어 키 및 장치번호를 포함한다.

[0168] 장치번호는 장치를 식별하는 식별정보이다.

[0169] 암호화 미디어 키는, 대응하는 장치번호 「m」에 의해 지시되는 장치 m에 할당된 디바이스 키 DK_m을 이용하여, 미디어 키 MK 또는 값 「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다. 여기서, 장치 m이 무효화 되어 있는 경우에는 값 「0」을 이용한다. 또, 장치 m이 무효화 되어 있지 않은 경우에는 미디어 키 MK를 이용한다.

[0170] ? 암호화 미디어 키 = E1(DK_m, MK) 또는

[0171] ? 암호화 미디어 키 = E1(DK_m, 0)

[0172] <키 기록영역(123)>

[0173] 키 기록영역(123)에는 암호화 콘텐츠 키 ECK가 기록되어 있다. 암호화 콘텐츠 키 ECK는, 키 암호화 키 KEK를 이용하여, 콘텐츠 키 CK에 암호화 알고리즘 E2를 실시하여 생성된 것이다.

[0174] ? 암호화 콘텐츠 키 ECK = E2(KEK, CK)

[0175] 여기서, 키 암호화 키 KEK는, 미디어 키 MK와 매체 고유번호 MID를 결합한 값을 입력 값으로 하여, 해시함수의 출력 값을 이용하여 산출되는 키이다.

[0176] ? 키 암호화 키 KEK = SHA-1(MK?MID)

[0177] <콘텐츠 기록영역(124)>

[0178] 콘텐츠 기록영역(124)에는 암호화 콘텐츠 ECNT가 기록되어 있다. 암호화 콘텐츠 ECNT는, 콘텐츠 키 CK를 이용하여, 콘텐츠에 암호화 알고리즘 E3을 실시하여 생성된 것이다.

[0179] ? 암호화 콘텐츠 ECNT = E3(CK, CNT)

[0180] <서명 기록영역(125)>

[0181] 서명 기록영역(125)에는 서명데이터 SigCRL이 기록되어 있다.

[0182] 서명데이터 SigCRL는, 비밀 키 SK_1을 이용하여, 키 암호화 키 KEK와 무효화리스트 CRL와의 결합 값 (KEK?CRL)에 디지털 서명 Sig를 실시하여 생성된 것이다.

[0183] ? 서명데이터 SigCRL = Sig(SL_1, (KEK?CRL))

[0184] <CRL 기록영역(125)>

[0185] CRL 기록영역(125)에는 무효화리스트 CRL이 기록되어 있고, 무효화리스트 CRL에는 무효화하여야 할 증명서의 ID가 기재되어 있다. 무효화리스트 CRL은, 일 예로서, 증명서 식별자 ID_3, ID_4, 서명데이터 SigID 및 판수를 포함하고 있다.

[0186] 증명서 식별자 ID_3, ID_4는 무효화 된 공개키 증명서를 식별하는 식별정보이다.

[0187] 서명데이터 SigID는, 인증국 CA의 비밀 키 SK_CA를 이용하여, 무효화리스트 CRL에 포함되는 모든 증명서 식별자의 결합 값에 대해서(무효화리스트 CRL에 1개의 증명서 식별자가 포함되어 있는 경우에는, 상기 1개의 증명서 식별자에 대하여) 디지털 서명 Sig를 실시하여 생성된 것이다.

[0188] ? 서명데이터 SigID = Sig(SK_CA, 모든 증명서 식별자의 결합 값)

[0189] 인증국 CA에 의한 서명데이터가 포함되어 있는 것은 무효화리스트 CRL의 정당성을 보증하기 위해서이다.

[0190] 판수는 무효화리스트 CRL의 세대를 나타내는 정보이다.

[0191] 또한, CRL의 포맷은 공지의 것이라도 좋고, 또, 어떤 시스템에 특화한 포맷이라도 좋다.

[0192] <증명서 기록영역(127)>

[0193] 증명서 기록영역(127)에는 공개키 증명서 PCK가 기록되어 있다. 공개키 증명서 PCK는, 증명서 식별자 ID_1, 공

개키 PK_1 및 서명데이터 Sig_1을 포함하고 있다.

[0194] 증명서 식별자 ID_1은 공개 키 증명서 PKC를 식별하는 식별정보이다.

[0195] 공개키 PK_1은, 공개키 암호방식에 의한 것이며, 비밀 키 SK_1에 대응하고 있다.

[0196] 서명데이터 Sig_1은, 인증국 CA의 비밀 키 SK_CA를 이용하여, 증명서 식별자 ID_1 및 공개 키 PK_1의 결합 값(ID_1?PK_1)에 대하여 디지털 서명을 실시하여 생성된 것이다.

[0197] ? 서명데이터 Sig_1 = Sig(SK_CA, ID_1?PK_1)

[0198] 또한, 인증국 CA에 의한 서명데이터가 포함되어 있는 것은 공개키 증명서의 정당성을 보증하기 위해서이다.

[0199] 또, 공개키 증명서의 포맷은 공지의 것이라도 좋고, 또 어떤 시스템에 특화한 포맷이라도 좋다.

[0200] 1. 5 재생장치(200)

[0201] 재생장치(200a, 200b, 200c, …)는 동일한 구성을 가지고 있으므로, 여기서는 재생장치(200)로 하여 설명한다.

[0202] 재생장치(200)는, 도 4에 도시한 바와 같이, 디바이스 키 저장부(201), 키 계산부 202, 키 계산부 203, 복호부 204, 복호부 205, CA공개키 저장부(206), 증명서 검증부(207), CRL저장부(208), CRL검증부(209), CRL비교갱신부(210), 증명서 판정부(211), 서명 검증부(212), 스위치(213), 재생부(214), 제어부(215), 입력부(216), 표시부(217) 및 드라이브부(218)로 구성되어 있다.

[0203] 재생장치(200)는, 구체적으로는, 콘텐츠 서버장치(500)와 마찬가지로, 마이크로프로세서, ROM, RAM, 하드디스크 유닛 등으로 구성되는 컴퓨터이다. 상기 RAM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써, 재생장치(200)는 그 기능을 달성한다.

[0204] ⑴ 디바이스 키 저장부(201)

[0205] 디바이스 키 저장부(201)는, 외부의 장치로부터 액세스할 수 없도록, 디바이스 키 DK_x를 비밀로 기억하고 있다. 디바이스 키 DK_x는 재생장치(200)에 고유한 키이다.

[0206] 또한, 디바이스 키 저장부(201)가 기억하고 있는 디바이스 키 DK_x는 재생장치(200a, 200b, 200c, 200d, 200e, …)에 따라 다르다. 재생장치(200a, 200b, 200c, 200d, 200e, …)의 각 디바이스 키 저장부(201)는 각각 디바이스 키 DK_2, DK_3, DK_4, DK_5, DK_6, …을 기억하고 있다.

[0207] ⑵ 키 계산부 202

[0208] 키 계산부 202는 재생장치(200)에 할당된 장치번호 「x」를 미리 기억하고 있다. 또한, 키 계산부 202가 기억하고 있는 장치번호 「x」는 재생장치(200a, 200b, 200c, 200d, 200e, …)에 따라 다르다. 재생장치(200a, 200b, 200c, 200d, 200e, …)의 키 계산부 202는 각각 장치번호 「2」, 「3」, 「4」, 「5」, 「6」을 기억하고 있다.

[0209] 키 계산부 202는, 기록매체(120)의 미디어 키 데이터 기록영역(122)에서, 드라이브부(218)를 거쳐서, 미디어 키 데이터 MDATA를 구성하는 n개의 세트를 순서대로 판독하고, 판독한 세트 중에서 기억하고 있는 장치번호 「x」를 포함하는 세트를 탐색한다. 장치번호 「x」를 포함하는 세트를 발견하면, 발견한 세트에서 장치번호 「x」에 대응하는 암호화 미디어 키 E1(DK_x, y)을 추출한다. 여기서, 재생장치(200)가 재생장치 200b 또는 재생장치 200c인 경우에는 y는 값 「0」이다. 또, 재생장치(200)가 재생장치 200b 또는 재생장치 200c를 제외한 다른 재생장치인 경우에는 y는 미디어 키 MK이다.

[0210] 다음에, 키 계산부 202는, 디바이스 키 저장부(201)에서 디바이스 키 DK_x를 판독하고, 판독한 디바이스 키 DK_x를 이용하여, 추출한 암호화 미디어 키 E1(DK_x, y)에 복호 알고리즘 D1을 실시하여 복호 미디어 키 y를 생성한다.

[0211] ? 복호 미디어 키 y = D1(DK_x, (E 1(DK_x, y))

[0212] 여기서, 복호 미디어 키 y는 미디어 키 MK 및 값 「0」 중 어느 하나이다.

[0213] 다음에, 키 계산부 202는 생성한 복호 미디어 키 y를 키 계산부 203에 출력한다.

[0214] ⑶ 키 계산부 203

[0215] 키 계산부 203은 키 계산부 102와 동일하게 동작한다.

[0216] 키 계산부 203은, 키 계산부 202로부터 복호 미디어 키 y를 취득하고, 드라이브부(218)를 거쳐서, 기록매체(120)의 고유번호 기록영역(121)에서 매체 고유번호 MID를 판독한다.

[0217] 다음에, 키 계산부 203은 취득한 복호 미디어 키 y와 판독한 매체 고유번호 MID를, 그 순서대로 결합하여, 결합 값 (y?MID)를 생성한다. 다음에, 키 계산부 203은, 생성한 결합 값 (y?MID)에 해시함수 SHA-1을 실시하여, 해시 값 H` = SHA-1 (y?MID)를 얻고, 얻어진 해시 값 H`를 키 복호 키 KDK로 하여, 키 복호 키 KDK를 복호부(204) 및 서명 검증부(212)에 출력한다.

[0218] 또한, 상술한 바와 같이, 키 계산부 104가 얻어진 해시함수의 일부분을 키 암호화 키 KEK로 하는 경우에는, 키 계산부 203도 얻어진 해시함수 값의 상기 일부분과 동일한 부분을 키 복호 키 KDK로 한다.

[0219] ⑷ 복호부 204

[0220] 복호부 204는, 기록매체(120)의 키 기록영역(123)에서, 드라이브부(218)를 거쳐서, 암호화 콘텐츠 키 ECK를 판독하고, 키 계산부 203에서 키 복호 키 KDK를 취득한다.

[0221] 다음에, 복호부 204는, 취득한 키 복호 키 KDK를 이용하여, 판독한 암호화 콘텐츠 키 ECK에 복호 알고리즘 D2를 실시하여 복호 콘텐츠 키 DCK를 생성한다.

[0222] ? 복호 콘텐츠 키 DCK = D2(KDK, ECK)

[0223] 여기서, 복호 알고리즘 D2는 암호화 알고리즘 E2를 실시하여 생성된 암호문을 복호 하는 알고리즘이며, 일예로, EDS에 의하는 것이 있다.

[0224] 다음에, 복호부 204는 생성한 복호 콘텐츠 키 DCK를 복호부(205)에 출력한다.

[0225] ⑸ 복호부 205

[0226] 복호부 205는, 기록매체(120)의 콘텐츠 기록영역(124)에서, 드라이브부(218)를 거쳐서, 암호화 콘텐츠 ECNT를 판독하고, 복호부 204에서 복호 콘텐츠 키 DCK를 취득한다.

[0227] 다음으로, 복호부 205는, 취득한 복호 콘텐츠 키 DCK를 이용하여, 판독한 암호화 콘텐츠 ECNT에 복호 알고리즘 D3을 실시하여 복호 콘텐츠 DCNT를 생성한다.

[0228] ? 복호 콘텐츠 DCNT = D3(DCK, ECNT)

[0229] 여기서, 복호 알고리즘 D3은 암호화 알고리즘 E3을 실시하여 생성된 암호문을 복호 하는 알고리즘이며, 일예로, DES에 의하는 것이 있다.

[0230] 다음에, 복호부 205는 생성한 복호 콘텐츠 DCNT를 스위치(213)에 출력한다.

[0231] ⑹ CA 공개키 저장부(206)

[0232] CA 공개키 저장부(206)는 인증국 CA의 공개 키 PK_CA를 미리 기억하고 있다.

[0233] ⑺ 증명서 검증부(207)

[0234] 증명서 검증부(207)는, CA 공개키 저장부(206)에서 공개 키 PK_CA를 판독하고, 기록매체(120)의 증명서 기록영역(127)에서, 드라이브부(218)를 거쳐서, 공개키 증명서 PKC를 판독한다.

[0235] 다음에, 증명서 검증부(207)는, 판독한 공개키 증명서 PKC에서, 증명서 식별자 ID_1, 공개 키 PK_1 및 서명데이터 Sig_1을 추출하고, 추출한 증명서 식별자 ID_1 및 공개 키 PK_1을 그 순서대로 결합하여 결합 값 (ID_1?PK_1)을 생성한다.

[0236] 이어서, 증명서 검증부(207)는, 판독한 공개 키 PK_CA를 이용하여, 추출한 서명데이터 Sig_1 및 생성한 결합 값 (ID_1?PK_1)에 서명검증 알고리즘 Vrfy를 실시하여, 검증결과 RSL2를 얻는다. 검증결과 RSL2는 검증 성공 및 검증 실패 중 어느 하나를 나타내는 정보이다.

[0237] 여기서, 서명검증 알고리즘 Vrfy는 디지털 서명 Sig_1에 의해 생성된 서명데이터를 검증하는 알고리즘이다.

[0238] 다음에, 증명서 검증부(207)는 검증결과 RSL2를 스위치(213)에 출력한다.

[0239] ⑻ CRL저장부(208)

[0240] CRL저장부(208)는 제 2 시점에서의 무효화 된 공개키 증명서를 나타내는 공개키 증명서 무효화 리스트(이하, 축

적 무효화 리스트 CRL_ST라 한다)를 기록하고 있다.

[0241] 축적 무효화 리스트 CRL_ST는, 제 1 시점에서의 무효화 된 공개키 증명서를 나타내는 리스트인 무효화 리스트 CRL과 마찬가지로, 1개 이상의 증명서 식별자와, 서명데이터 SigID와, 판수를 포함하고 있다.

[0242] 증명서 식별자 및 서명데이터 SigID에 대해서는 앞에서 설명한 것과 같다.

[0243] 판수는, 축적 무효화 리스트 CRL_ST의 세대를 나타내는 정보이며, 축적 무효화 리스트 CRL_ST가 상기 제 2 시점에서의 것이라는 것을 나타낸다. 판수는 공개키 증명서 무효화 리스트의 세대가 새로울수록 큰 값을 취한다.

[0244] ⑼ CRL검증부(209)

[0245] CRL검증부(209)는, CA공개키 저장부(206)에서 공개키 PK_CA를 판독하고, 기록매체(120)의 CRL 기록영역(126)에서, 드라이브부(218)를 거쳐서, 무효화리스트 CRL을 판독한다.

[0246] 다음에, CRL검증부(209)는 판독한 무효화리스트 CRL에서 1개 이상의 증명서 식별자와 서명데이터 SigID를 추출한다. 여기서, 복수의 증명서 식별자가 추출된 경우에는 이들을 무효화리스트 CRL 내에 배치되어 있는 순서로 결합하여 결합 값을 생성한다. 또, 1개의 증명서 식별자만이 추출된 경우에는 추출된 1개의 증명서 식별자를 상기 결합 값으로 한다.

[0247] 다음에, CRL검증부(209)는, 판독한 공개 키 PK_CA를 이용하여, 추출한 서명데이터 Sig_ID와 생성한 상기 결합 값에 서명검증 알고리즘 Vrfy를 실시하여 검증결과 RSL3를 얻는다. 검증결과 RSL3은 검증 성공 및 검증 실패 중 어느 하나이다.

[0248] 얻어진 검증결과 RSL3가 검증 성공을 나타내는 경우에는, CRL검증부(209)는 판독한 무효화리스트 CRL을 서명검증부(212) 및 CRL 비교갱신부(210)에 출력한다.

[0249] ⑽ CRL비교갱신부(210)

[0250] CRL비교갱신부(210)는 CRL 검증부(209)에서 무효화리스트 CRL을 취득한다.

[0251] 무효화리스트 CRL을 취득한 경우에, CRL비교갱신부(210)는, 취득한 무효화리스트 CRL에서 판수를 추출하고, CRL 저장부(208)에서 축적 무효화리스트 CRL_ST를 판독하여, 판독한 축적 무효화리스트 CRL_ST에서 판수를 추출한다. 다음에, 무효화리스트 CRL에서 추출한 판수가 축적 무효화리스트 CRL_ST에서 추출한 판수보다 큰가 여부를 판단한다.

[0252] 무효화리스트 CRL에서 추출한 판수가 축적 무효화리스트 CRL_ST에서 추출한 판수보다 크다고 판단한 경우에는, CRL 비교갱신부(210)는, 무효화리스트 CRL의 세대는 축적 무효화리스트 CRL_ST의 세대보다 새로운 것으로 간주하여, 무효화리스트 CRL을 축적 무효화리스트 CRL_ST로 하여, CRL저장부(208)에 다시 기입한다.

[0253] 무효화리스트 CRL에서 추출한 판수가 축적 무효화리스트 CRL_ST에서 추출한 판수보다 작거나 같다고 판단한 경우에, 무효화리스트 CRL의 세대는 축적 무효화리스트CRL_ST의 세대보다 오래되었거나 또는 같은 것으로 간주하여, 상기 재 기입을 하지 않는다.

[0254] ⑾ 증명서 판정부(211)

[0255] 증명서 판정부(211)는 CRL 저장부(208)에서 축적 무효화리스트 CRL_ST를 판독한다. 여기서, CRL저장부(208)에 기억되어 있는 축적 무효화리스트 CRL_ST는 CRL 비교갱신부(210)에 의해 최신의 것으로 갱신되어 있다. 또, 증명서 판정부(211)는, 기록매체(120)의 증명서 기록영역(127)에서, 드라이브부(218)를 거쳐서, 공개키 증명서 PKC를 판독한다.

[0256] 다음에, 증명서 판정부(211)는, 판독한 공개키 증명서 PKC에서 증명서 식별자 ID_1을 추출하고, 추출한 증명서 식별자 ID_1이 축적 무효화리스트 CRL_ST에 포함되어 있는가 여부를 판단한다. 다음에, 판단결과 JDG를 스위치(213)에 출력한다. 여기서, 판단결과 JDG는 증명서 식별자 ID_1이 축적 무효화리스트 CRL_ST에 포함되어 있는가 여부를 나타내는 정보이다.

[0257] ⑿ 서명검증부(212)

[0258] 서명검증부(212)는 키 계산부 203에서 키 복호 키 KDK를 취득한다. 또, 기록매체(120)의 서명기록영역(125)에서, 드라이브부(218)를 거쳐서, 서명데이터 SigCRL을 판독하고, 기록매체(120)의 증명서기록영역(127)에서, 드라이브부(218)를 거쳐서, 공개키 증명서 PKC를 판독한다. 또, CRL검증부(209)에서 무효화리

스트 CRL을 취득한다.

[0259] 다음에, 서명검증부(212)는, 판독한 공개키 증명서 PKC에서 공개 키 PK_1을 추출하고, 취득한 키 복호 키 KDK와 취득한 무효화리스트 CRL을 결합하여 결합 값 (KDK?CRL)을 생성하며, 추출한 공개 키 PK_1을 이용하여 판독한 서명데이터 SigCRL 및 생성한 결합 값 (KDK?CRL)에 서명검증 알고리즘 Vrfy를 실시하여 검증결과 RSL1을 얻는다. 검증결과 RSL1은 검증 성공 및 검증 실패 중 어느 하나의 정보를 나타내는 정보이다.

[0260] 다음에, 서명검증부(212)는 검증결과 RSL1을 스위치(213)에 출력한다.

[0261] ⑬ 스위치(213)

[0262] 스위치(213)는 복호부(205)에서 복호 콘텐츠 DCNT를 취득한다. 또, 증명서 판정부(211)로부터 판단결과 JDG를 취득하고, 증명서 검증부(207)로부터 검증결과 RSL2를 취득하며, 서명 검증부(212)로부터 검증결과 RSL1을 취득한다.

[0263] 취득한 검증결과 RSL1이 검증 성공을 나타내고, 또한 취득한 검증결과 RSL2가 검증 성공을 나타내며, 또한 취득한 판단결과 JDG가 증명서 식별자 ID_1이 축적 무효화리스트 CRL_ST에 포함되어 있지 않다는 것을 나타내는 경우에 한해, 스위치(213)는 취득한 복호 콘텐츠 DCNT를 재생부(214)로 출력한다.

[0264] 취득한 검증결과 RSL1이 검증 실패를 나타내거나, 또는 취득한 검증결과 RSL2가 검증 실패를 나타내거나, 또는 취득한 판단결과 JDG가 증명서 식별자 ID_1이 축적 무효화리스트 CRL_ST에 포함되어 있다는 것을 나타내는 경우에, 스위치(213)는 취득한 복호 콘텐츠 DCNT를 재생부(214)로 출력하지 않는다.

[0265] ⑭ 재생부(214)

[0266] 재생부(214)는, 스위치(213)에서 복호 콘텐츠 DCNT를 취득하고, 취득한 복호콘텐츠 DCNT로부터 영상정보 및 음성정보를 생성하고, 생성한 영상정보 및 음성정보를 아날로그의 영상신호 및 음성신호로 변환하여, 아날로그의 영상신호 및 음성신호를 모니터(290)에 출력한다.

[0267] ⑮ 제어부(215), 입력부(216), 표시부(217), 드라이브부(218), 모니터(290) 및 리모컨(280)

[0268] 제어부(215)는 재생장치(200)를 구성하는 각 구성요소를 제어한다.

[0269] 리모컨(280)은, 각종 버튼을 구비하며, 조작자의 상기 버튼의 조작에 따른 조작지시정보를 생성하고, 생성한 조작지시정보를 적외선에 실어서 출력한다.

[0270] 입력부(216)는, 리모컨(280)에서 조작지시정보가 실린 적외선을 취득하고, 취득한 적외선에서 조작자 지시정보를 추출하며, 추출한 조작자 지시정보를 제어부(215)에 출력한다.

[0271] 표시부(217)는 제어부(215)의 제어에 의해 각종 정보를 표시한다.

[0272] 드라이브부(218)는 기록매체(120)로부터의 정보의 판독을 행한다.

[0273] 모니터(290)는, CRT 및 스피커를 구비하며, 재생부(214)로부터 아날로그의 영상신호 및 음성신호를 수신하여, 영상신호에 의거 영상을 표시하고, 음성신호에 의거 음성을 출력한다.

[0274] 1. 6 콘텐츠 공급시스템(10)의 동작

[0275] 콘텐츠 공급시스템(10)의 동작에 대해서, 특히, 기록장치(100)에 의한 기록매체(120)에 대한 데이터의 기입동작, 및 재생장치(200)에 의한 기록매체(120)에 기록되어 있는 데이터의 재생동작에 대하여 설명한다.

[0276] ⑴ 기록장치(100)에 의한 기입동작

[0277] 기록장치(100)에 의한 기록매체(120)에 대한 기입동작에 대하여, 도 5에 도시한 플로우챠트를 이용하여 설명한다.

[0278] 키 계산부 103은, 디바이스 키 저장부(101) 및 미디어 키 데이터 저장부(102)에서, 각각 디바이스 키 DK_1 및 미디어 키 데이터 MDATA를 판독하고(스텝 S301), 이어서, 판독한 디바이스 키 DK_1 및 미디어 키 데이터 MDATA를 이용하여 미디어 키 MK를 생성한다(스텝 S302).

[0279] 다음에, 키 계산부 104는, 기록매체(120)의 고유번호 기록영역(121)에서 매체 고유번호 MID를 판독하고(스텝 S303), 생성된 미디어 키 MK와 판독한 매체 고유번호 MID를 이용하여 키 암호화 키 KEK를 산출한다(스텝 S304).

[0280] 다음에, 암호화부 105는, 산출된 키 암호화 키 KEK를 이용해서, 콘텐츠 서버장치(500)에서 취득한 콘텐츠 키 CK

를 암호화하여 암호화 콘텐츠 키 ECK를 생성한다(스텝 S305).

[0281] 다음에, 암호화부 106은, 콘텐츠 서버장치(500)에서 취득한 콘텐츠 CNT를 암호화하여 암호화 콘텐츠 ECNT를 생성한다(스텝 S306).

[0282] 다음에, 서명생성부(110)는, 비밀키저장부(107)에서 비밀 키 SK_1을 판독하고(스텝 S307), 판독한 비밀 키 SK_1을 이용하여, 키 암호화 키 KEK 및 무효화리스트 CRL에 대한 서명 SigCRL을 생성한다(스텝 S308).

[0283] 다음에, 기록장치(100)는, 미디어 키 데이터 MDATA, 암호화 콘텐츠 키 ECK, 암호화 콘텐츠 ECNT, 서명데이터 SigCRL, 무효화리스트 CRL 및 공개키 증명서 PKC를, 드라이브부(111)를 거쳐서, 기록매체(120)에 기록한다(스텝 S309).

[0284] ⑵ 재생장치(200)에 의한 재생동작

[0285] 재생장치(200)에 의한 기록매체(120)에 기록되어 있는 데이터의 재생동작에 대하여, 도 6 내지 도 7에 도시한 플로우챠트를 이용하여 설명한다.

[0286] 재생장치(200)는, 기록매체(120)에서, 미디어 키 데이터 MDATA, 매체 고유번호 MID, 암호화 콘텐츠 키 ECK, 암호화 콘텐츠 ECNT, 서명데이터 SigCRL, 무효화리스트 CRL 및 공개키 증명서 PKC를 판독한다(스텝 S401).

[0287] 다음에, 키 계산부 202는, 디바이스 키 저장부(201)에서 디바이스 키 DK_x를 판독하고(스텝 S402), 판독한 미디어 키 데이터 MDATA 및 디바이스 키 DK_x를 이용하여 복호 미디어 키 y를 얻는다(스텝 403).

[0288] 다음에, 키 계산부 203은, 판독한 매체 고유번호 MID 및 얻어진 복호 키 y로부터 키 복호 키 KDK를 산출한다(스텝 S404).

[0289] 다음에, 복호부 204는, 산출된 키 복호 키 KDK를 이용하여, 판독된 암호화 콘텐츠 키 ECK를 복호 하여 복호 콘텐츠 키 DCK를 얻는다(스텝 S405).

[0290] 다음에, 복호부 205는, 판독한 암호화 콘텐츠 ECNT를, 얻어진 복호 콘텐츠 키 DCK를 이용하여 복호 하여, 복호 콘텐츠 DCNT를 얻는다(스텝 S406).

[0291] 다음에, 증명서 검증부(207)는, CA공개키 저장부에서 인증국 CA의 공개 키 PK_CA를 판독하고(스텝 S407), 판독한 인증국 CA의 공개 키 PK_CA를 이용하여, 판독한 공개키 증명서 PKC의 정당성을 검증한다(스텝 S408).

[0292] 공개키 증명서 PKC의 정당성의 검증에 실패한 경우에는(스텝 S409), 스텝 S422로 제어를 옮긴다. 공개키 증명서 PKC의 정당성의 검증에 성공한 경우에는(스텝 S409), CRL 검증부(209)는, 인증국 CA의 공개 키 PK_CA를 이용하여 판독한 무효화리스트 CRL의 정당성을 검증한다(스텝 S410).

[0293] 무효화리스트 CRL의 정당성 검증에 실패한 경우에는(스텝 S411), 스텝 S422로 제어를 옮긴다. 무효화리스트 CRL의 정당성 검증에 성공한 경우에는(스텝 S411), CRL 비교갱신부(210)는, CRL 저장부(208)에서 축적 무효화리스트 CRL_ST를 판독하고(스텝 S412), 기록매체(120)에서 판독한 무효화리스트 CRL과 CRL 저장부(208)에서 판독한 축적 무효화리스트 CRL_ST의 신, 구를 비교한다(스텝 S413).

[0294] CRL 비교갱신부(210)는, 상기 비교의 결과, 무효화리스트 CRL 쪽이 축적 무효화리스트 CRL_ST보다 새롭다고 판단되는 경우에(스텝 S414), 새운 것으로 판단한 무효화리스트 CRL을 축적 무효화리스트 CRL_ST로 하여 CRL 저장부(208)에 덮어쓰기를 한다(스텝 S415). 무효화리스트 CRL 쪽이 축적 무효화리스트 CRL_ST보다 오래된 것으로 판단되는 경우(스텝 S414), 스텝 S416으로 제어를 옮긴다.

[0295] 다음에, 증명서 판정부(211)는, CRL 저장부(208)에서 축적 무효화리스트 CRL_ST를 판독하고(스텝 S416), 판독한 공개키 증명서 PKC에서 추출한 증명서 식별자 ID_1이 축적 무효화리스트 CRL_ST에 포함되어 있는가 여부를 판단함으로써, 판독한 축적 무효화리스트 CRL_ST에 공개키 증명서 PKC가 등록되어 있는가 여부를 판정한다(스텝 S417).

[0296] 등록되어 있다고 판정된 경우(스텝 S418), 스텝 S422로 제어를 옮긴다. 등록되어 있지 않다고 판정된 경우(스텝 S418), 서명검증부(212)는, 키 복호 키 KDK, 공개키 증명서 PKC 및 무효화리스트 CRL을 이용하여 서명데이터 SigCRL의 정당성을 검증한다(스텝 S419).

[0297] 서명데이터 SigCRL의 정당성의 검증에 실패한 경우(스텝 S420), 스위치(213)는 개방되며, 콘텐츠는 재생되지 않고(스텝 S422), 재생장치(200)의 동작이 종료한다.

[0298] 한편, 서명데이터 SigCRL의 정당성의 검증에 성공한 경우(스텝 S420), 스위치(213)가 폐쇄되며, 복호 콘텐츠 DCNT를 재생부(214)에 출력하고, 재생부(214)는 복호 콘텐츠 DCNT를 재생하며(스텝 S421), 재생장치(200)의 동작이 종료한다.

[0299] 1. 7 기타 변형 예

[0300] (1) 제 1 실시 예에서는, 기록매체를 거쳐서 무효화리스트 CRL을 전파하는 구조의 실현을 위해, 기록장치가 무효화리스트 CRL을 서명대상으로 하여 서명데이터 SigCRL을 생성하고, 생성한 서명데이터 SigCRL을 기록매체에 기입하도록 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0301] 예를 들어, 기록장치는, 무효화리스트 CRL의 해시 값을 산출하고, 그 해시 값에 대하여 서명데이터를 생산하는 것으로 해도 된다.

[0302] ? 서명데이터 = Sig(SK_1, HASH(CRL))

[0303] 여기서, HASH(A)는 데이터 A에 대하여 해시함수 HASH를 실시하여 얻어진 해시 값이다.

[0304] 또, 기록장치는, 무효화리스트 CRL의 해시 값을 산출하여, 그 해시 값과 미디어 키 MK를 XOR(배타적 논리합) 연산하고, 그 연산결과에 대하여 서명데이터를 생성하는 것으로 해도 된다.

[0305] ? 서명데이터 = Sig(SK_1, (HASH(CRL))XOR(MK))

[0306] 이와 같이, 기록장치는, 무효화리스트 CRL 및 각종 키 데이터에 대하여 서명데이터를 생성하며, 생성한 서명데이터를 기록매체에 기입함으로써, 기록매체 상의 무효화리스트 CRL의 개찬(改竄, Falsification)이나 삭제를 방지할 수 있다.

[0307] 또, 이들의 경우에, 재생장치는 각각 대응하는 데이터를 이용하여 서명 검증을 행한다.

[0308] (2) 제 1 실시 예에서는, 외부에서 취득하는 무효화리스트 CRL 및 내부에 기억하고 있는 무효화리스트 CRL의 신, 구를 비교할 때에 버전 번호를 비교하는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0309] 예를 들어, 무효화리스트 CRL이 갱신됨에 따라서 무효화되는 장치의 수가 단조로 증가한다고 가정할 수 있으며, 무효화 되는 장치의 대수의 비교에 의해, 무효화 대수가 많은 쪽을 새롭다고 판단해도 된다.

[0310] 이상과 같이, CRL로부터 신, 구 비교를 할 수 있는 정보를 얻을 수 있는 구성이면 어떤 구성이라도 좋다.

[0311] (3) 별도의 다른 기록매체를 통해서, 미디어 키 데이터의 최신판이, 기록장치에 대해서, 전파되는 구성이라도 좋다.

[0312] 상기 별도의 다른의 기록매체에는 최신판의 미디어 키 데이터가 기록되어 있다.

[0313] 기록장치는 내부에 미리 미디어 키 데이터를 보유하고 있다. 미디어 키 데이터가 기록되어 있는 상기 별도의 다른 기록매체가 장착되면, 기록장치는, 자신이 보유하고 있는 미디어 키 데이터와 기록매체에 기록되어 있는 미디어 키 데이터와의 신, 구를 비교하여, 자신이 보유하는 미디어 키 데이터보다도 기록매체에 기록되어 있는 미디어 키 데이터 쪽이 새로우면, 자신이 보유하고 있는 미디어 키 데이터 대신 기록매체에 기록되어 있는 미디어 키 데이터를 내부에 기입한다.

[0314] 여기서, 각 미디어 키 데이터에는 그 세대를 나타내는 버전 번호가 부여되어 있고, 기록장치는 각 버전 번호를 이용하여 각 미디어 키 데이터의 신, 구를 비교한다.

[0315] 또, 미디어 키 데이터에서 산출되는 미디어 키의 일부는 버전 번호이며, 나머지 부분은 난수를 이용하여 생성되는 것으로 해도 된다. 기록장치는, 각 미디어 키 데이터에서 미디어 키의 일부인 버전 번호를 추출하고, 추출한 각 버전 번호를 이용하여 각 미디어 키 데이터의 신, 구를 비교한다.

[0316] 또, 미디어 키 데이터에 있어서 무효화 되어 있는 장치의 대수, 즉, 미디어 키 MK에 대신하여 값 「0」이 암호화의 대상으로 되어 있는 암호화 미디어 키의 수는, 미디어 키 데이터의 갱신에 따라서 단조로 증가한다고 가정하고, 기록장치는 미디어 키 데이터에 포함되어 있는 무효화 되어 있는 장치의 대수를 이용하여 각 미디어 키 데이터의 신, 구를 비교하는 것으로 해도 좋다.

[0317] 이상과 같이, 미디어 키 데이터의 신, 구를 정확하게 비교할 수 있는 구성이라면 어떤 구성이라도 좋다.

[0318] 또, 각 미디어 키 데이터에는 개찬 방지를 위한 인증국 CA의 서명이 부여되어 있는 것으로 해도 된다. 기록장치

는 서명을 검증함으로써 미디어 키 데이터의 정당성을 확인한다.

[0319] (4) 미디어 키 데이터 및 암호화 콘텐츠 등이 미리 기록되어 있는 기록매체에 대하여, 별도의 다른 암호화 콘텐츠를 추가하여 기입하는 경우에, 기록장치는, 자신이 보유하는 미디어 키 데이터에 의거하여, 또는 상기 기록매체에 기록되어 있는 미디어 키 데이터에 의거하여, 외부(예를 들어, 콘텐츠 서버장치)에서 취득한 콘텐츠를 암호화하여 별도의 다른 암호화 콘텐츠를 생성하고, 생성한 별도의 다른 암호화 콘텐츠를 상기 기록매체에 기록하는 것으로 해도 된다.

[0320] 이 경우, 상기 기록매체 상에는, 복수의 미디어 키 데이터, 복수의 공개키 증명서, 복수의 무효화리스트 CRL이 존재하는 경우가 있다.

[0321] (5) 제 1 실시 예에서는, 키 암호화 키 KEK에 대하여, 디지털 서명을 실시하여 서명데이터를 생성하는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0322] 예를 들어, 콘텐츠 CNT 전체의 해시 값에 대하여 디지털 서명을 실시하여 서명데이터를 생성해도 된다.

[0323] ? 서명데이터 = Sig(SK_1, HASH(CNT))

[0324] 즉, 서명은 콘텐츠를 기록한 기록장치의 정당성의 확인이 목적이므로, 서명의 대상이 되는 데이터는, 콘텐츠에 관련하는 정보나 암호화 시에 사용하는 키에 관련되는 정보라면 어떤 정보라도 좋다.

[0325] (6) 제 1 실시 예에서는, 기록장치(100)는, 도 2에 도시한 바와 같이, 디바이스 키 저장부(101), 미디어 키 데이터 저장부(102), 키 계산부 103, 키 계산부 104, 암호화부 105, 암호화부 106, 비밀키 저장부(107), 증명서 저장부(108), CRL 저장부(109), 서명생성부(110), 드라이브부(111), 제어부(112) 및 송수신부(113)로 구성되는 일체의 장치로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0326] 예를 들어, 디바이스 키 저장부(101), 미디어 키 데이터 저장부(102), 키 계산부 103, 키 계산부 104, 암호화부 105, 암호화부 106, 비밀키 저장부(107), 증명서 저장부(108), CRL 저장부(109), 서명생성부(110), 드라이브부(111), 제어부(112)의 일부가 일체로 된 드라이브장치로 구성되고, 제어부(112)의 다른 일부 및 송수신부(113)가 일체로 된 처리장치로 구성되어 있는 것으로 해도 된다. 이 구성에서는, 기록매체에 대한 데이터의 판독/기입 및 암호처리를 행하는 드라이브장치와, 그 외의 처리를 행하는 처리장치로 분리하고 있다.

[0327] 또, 디바이스 키 저장부(101), 미디어 키 데이터 저장부(102), 비밀키 저장부(107), 증명서 저장부(108) 및 CRL 저장부(109)는 외부의 기억장치의 기억영역 상에 기억하고 있는 것으로 해도 된다. 여기서, 상기 외부 기억장치의 일 예는, 휴대형의 시큐어 메모리카드(Portable Secure Memory Card)이다.

[0328] 또, 제 1 실시 예에서는, 재생장치(200)는, 도 4에 도시한 바와 같이, 디바이스 키 저장부(201), 키 계산부 202, 키 계산부 203, 복호부 204, 복호부 205, CA공개키 저장부(206), 증명서 검증부(207), CRL저장부(208), CRL검증부(209), CRL비교갱신부(210), 증명서 판정부(211), 서명 검증부(212), 스위치(213), 재생부(214), 제어부(215), 입력부(216), 표시부(217) 및 드라이브부(218)로 구성되는 일체의 장치로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0329] 디바이스 키 저장부(201), 키 계산부 202, 키 계산부 203, 복호부 204, 복호부 205, CA공개키 저장부(206), 증명서 검증부(207), CRL저장부(208), CRL검증부(209), CRL비교갱신부(210), 증명서 판정부(211), 서명 검증부(212), 스위치(213) 및 드라이브부(218)로 구성되어 일체로 된 드라이브장치로 구성되고, 재생부(214), 제어부(215), 입력부(216), 표시부(217)로 구성되어 일체로 된 처리장치로 구성되는 것으로 해도 된다. 이 구성에서는, 기록매체에 대한 데이터의 판독/기입 및 암호처리를 행하는 드라이브장치와, 그 외의 처리를 행하는 처리장치로 분리하고 있다.

[0330] 또, 디바이스 키 저장부(201), CA공개키 저장부(206) 및 CRL저장부(208)는 외부의 기억장치의 기억영역 상에 구성되어 있는 것으로 해도 된다. 여기서, 상기 외부의 기억장치의 일 예는 휴대형의 시큐어 메모리카드(Portable Secure Memory Card)이다.

[0331] 이상과 같이, 기억장치 및 재생장치는, 각각 일체의 장치가 아니라, 데이터 판독/기입 및 처리장치가 별개의 구성이라도 좋다. 이 경우, 데이터 판독/기입장치에서 암호처리를 행해도 좋고, 처리장치에서 암호처리를 행해도 좋다.

[0332] (7) 제 1실시 예에서는, 미디어 키 데이터 MDATA, 암호화 콘텐츠 키 ECK, 암호화 콘텐츠 ECNT, 서명데이터 SigCRL, 무효화리스트 CRL 및 공개키 증명서 PKC를 모두 동일한 기록매체에 기록하는 것으로 하고 있으나, 본

발명은 이에 한정되는 것은 아니다.

[0333] 예를 들어, 기록장치(100)는, 서명데이터 SigCRL, 무효화리스트 CRL 및 공개키 증명서 PKC 등의 데이터의 일부를, 기록매체 120과는 별도의 다른 기록매체에 기록하고, 기록매체 120 및 이 별도의 다른 기록매체가 배포되는 것으로 해도 된다.

[0334] 또, 기록장치(100)는 인터넷을 대표로 하는 네트워크에 접속되어 있고, 이들 데이터의 일부를 네트워크를 거쳐서 배포하는 것으로 해도 된다. 재생장치(200)도, 네트워크에 접속되어 있고, 기록장치(100)로부터 네트워크를 거쳐서 이들 데이터의 일부를 취득한다.

[0335] 이상과 같이, 미디어 키 데이터 MDATA, 암호화 콘텐츠 키 ECK, 암호화 콘텐츠 ECNT, 서명데이터 SigCRL, 무효화리스트 CRL 및 공개키 증명서 PKC가 1개 이상의 기록매체에 기록되어 배포되거나, 또는 1개 이상의 기록매체에 기록되고 또한 네트워크를 거쳐서 배포되어도 된다.

[0336] (8) 제 1 실시 예에서는, 디바이스 키에 의거하여 콘텐츠를 암호화하고, 또 암호화 콘텐츠를 복호하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0337] 예를 들어, 기록장치 및 재생장치가 이용조건을 취득하고 있고, 이 이용조건에 의거하여 기록 및 재생을 제어하는 구성이라도 된다. 여기서, 이용조건이란, 콘텐츠에 부수하는 관리정보이며, 예를 들어, 콘텐츠의 기록 및 재생을 허가하는 일자, 시간 또는 횟수이다.

[0338] (9) 제 1 실시 예에서는, 재생장치가 CRL 저장부에서 무효화리스트 CRL을 판독하여 신, 구 비교를 행하고, 새로운 무효화리스트 CRL을 CRL 저장부에 저장하며, 공개키 증명서의 등록 유무의 확인시에 재차 무효화리스트 CRL을 판독하는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0339] 예를 들어, 재생장치는, 무효화리스트 CRL의 신, 구 비교를 행하지 않고, 또, 새로운 것으로 판단한 무효화리스트 CRL을 CRL 저장부에 저장하지도 않으며, 공개키 증명서의 무효화리스트 CRL에서의 등록의 유무를 판정한 후에, 기록매체(120)로부터 판독한 무효화리스트 CRL을 CRL 저장부에 저장하는 것으로 해도 된다.

[0340] 또, 서명검증, CRL검증, 공개키 증명서의 판정의 순서도 제 1 실시 예에 기재된 것에 한정되지 않으며, 재생장치는, 다양한 순서에 의해, 서명검증, CRL검증, 공개키 증명서의 판정을 행하여 콘텐츠의 재생을 제어하는 것으로 해도 된다.

[0341] (10) 기록장치 및 재생장치가 전자 워터마크(Electronic Watermark)를 생성하여 삽입하는 전자 워터마크 처리부를 구비하는 구성으로 해도 된다.

[0342] 예를 들어, 기록장치가 그 장치를 특정하는 장치 ID를 기억하고 있고, 콘텐츠를 기록매체에 기록할 때에, 콘텐츠에 대하여, 그 장치 ID를 전자 워터마크로 삽입해도 된다.

[0343] 이때, 장치 ID가 전자 워터마크로 삽입된 콘텐츠가 부정 유출된 경우에, 콘텐츠에서 삽입된 장치 ID를 추출함으로써, 그 콘텐츠를 기록한 기록장치를 특정할 수 있다.

[0344] 또, 마찬가지로, 재생장치가 재생시에, 자신의 장치 ID를 전자 워터마크로 하여 기록매체 상의 콘텐츠에 삽입하는 구성이라도 된다. 이때, 장치 ID가 삽입된 콘텐츠가 부정 유출된 경우에, 콘텐츠에서 삽입된 장치 ID를 추출함으로써, 그 콘텐츠를 재생한 재생장치를 특정할 수 있다.

[0345] (11) 콘텐츠 공급시스템은, 유출된 디바이스 키를 가진 부정장치가 발견된 경우에, 내부에 저장되어 있는 디바이스 키를 특정할 수 있는 디바이스 키 발견장치를 포함하는 것으로 해도 된다. 이 부정장치는 재생장치(200)와 동일한 구성을 가지고 있다.

[0346] 디바이스 키 발견장치는, 도 8에 도시한 바와 같이, n매의 기록매체 MD1, MD2, MD3, …, MDn을 생성한다. 또한, 도 8에서는 미디어 키 데이터 이외의 다른 데이터에 대해서는 도시를 생략하고 있다.

[0347] 기록매체 MD1, MD2, MD3, …, MDn은 이하의 점을 제외하고, 제 3에 기재한 기록매체 120과 동일한 내용의 데이터를 기록하고 있다.

[0348] (a) 기록매체 MD1, MD2, MD3, …, MDn에 기록되어 있는 무효화리스트 CRL에 등록되어 있는 무효화 된 공개키 증명서는 없다. 즉, 무효화리스트 CRL은 공개키 증명서의 식별자를 포함하고 있지 않다.

[0349] (b) 기록매체 MD1, MD2, MD3, …, MDn에 기록되어 있는 각 미디어 키 데이터는 기록매체 120에 기록되어 있는 미디어 키 데이터와는 다른 것이다. 기록매체 MD1, MD2, MD3, …, MDn에 기록되어 있는 각 미디어 키 데이터의 일

예를 도 8에 도시한다.

[0350] (b-1) 기록매체 MD1에 기록되어 있는 미디어 키 데이터는 n개의 세트로 구성된다. 각 세트는 암호화 미디어 키와 장치번호를 포함한다. 장치번호에 대해서는 제 1 실시 예에서 설명한 것과 같다.

[0351] 제 1 암호화 미디어 키는, 디바이스 키 DK_1을 이용하여, 미디어 키 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0352] 제 2, 제 3, …, 제 n 암호화 미디어 키는, 디바이스 키 DK_2, DK_3, …, DK-n을 이용하여, 값 「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0353] (b-2) 기록매체 MD2에 기록되어 있는 미디어 키 데이터는 n개의 세트로 구성된다. 각 세트는 암호화 미디어 키와 장치번호를 포함한다. 장치번호에 대해서는 제 1 실시 예에서 설명한 것과 같다.

[0354] 제 1 미디어 암호화 키는, 디바이스 키 DK_1을 이용하여, 값 「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0355] 제 2 암호화 미디어 키는, 디바이스 키 DK_2를 이용하여, 미디어 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0356] 제 3, …, 제 n의 암호화 미디어 키는, 각각 디바이스 키 DK_3, …, 제 DK_n을 이용하여, 값 「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0357] (b-3) 기록매체 MD3, …, MDn에 대해서도 상기와 동일하다. 정수 $i(1 \leq i \leq n)$에 대하여, 기록매체 MDi에 기록되어 있는 미디어 키 데이터는 n 개의 세트로 구성된다. 각 세트는 암호화 미디어 키와 장치번호를 포함한다. 장치번호에 대해서는 제 1 실시 예에서 설명한 것과 같다.

[0358] 제 1 암호화 미디어 키는, 디바이스 키 MD-i를 이용하여, 값 「0」에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0359] 그 외의 암호화 미디어 키는, 대응하는 디바이스 키를 이용하여, 미디어 키 MK에 암호화 알고리즘 E1을 실시하여 생성된 것이다.

[0360] 다음에, 조작자는, 기록매체 MD1, MD2, MD3, …, MDn을 1매씩 순서대로 부정장치에 장착하여, 콘텐츠의 재생을 부정장치에 지시한다.

[0361] 이렇게 하여, n 매의 기록매체가 부정장치에 의해 시도된다.

[0362] 부정장치에 의해 콘텐츠가 정상적으로 재생된 경우에, 장착된 기록매체에 의해 부정장치가 내장했을 디바이스 키를 특정할 수 있다.

[0363] 예를 들어, 기록매체 MD1이 장착된 경우에, 부정장치에 의해 콘텐츠가 정상적으로 재생되었다면, 부정장치가 내장하는 디바이스 키는 DK_1이다.

[0364] 일반화하면, 기록매체 MDi가 장착된 경우에, 부정장치에 의해 콘텐츠가 정상적으로 재생된 것이라면, 부정장치가 내장하는 디바이스 키는 DK_i이다.

[0365] 부정장치는, 재생장치(200)와 동일한 구성을 가지고 있고, 도 6-7에 도시한 것과 같이 동작하므로, 기록매체 MD1, MD2, MD3, …, MDn 중 어느 1매가 장착된 경우에 한해 콘텐츠를 정상적으로 재생한다.

[0366] ⑿ 제 1 실시 예에서는, 서명생성 알고리즘으로 서명대상 데이터에 그 서명을 부여하는 부록형 서명을 이용하고 있으나, 본 발명은 이에 한정되는 것은 아니다.

[0367] 예를 들어, 메시지 부록형 서명이 아니라, 메시지 회복형 서명을 사용하는 것으로 해도 된다. 또한, 메시지 회복형 서명에 대해서는 특허문헌 3에 개시되어 있다.

[0368] 메시지회복형 서명에서는, 서명자가, 생성하는 서명에 비밀정보를 삽입할 수 있고, 검증자가, 서명검증 후에 그 비밀정보를 얻을 수 있다. 이 특징을 이용하여, 기록장치는, 비밀정보와 키 데이터(예를 들어, 콘텐츠 키)에 XOR연산(배타적 논리합)을 실시하고, 연산결과에 대하여 메시지회복형 서명을 실시하여 서명데이터를 생성한다. 이때, 재생장치는, 서명 검증을 하고, 검증이 성공한 경우에, 상기 연산결과를 얻으며, 내장하고 있는 비밀정보와 연산결과에 대하여 XOR연산을 실시하여 키 데이터(예를 들어, 콘텐츠 키)를 얻는다.

[0369] 또한, 비밀정보와 키 데이터 사이의 연산은 XOR 연산으로 한정할 필요는 없으며, 가산연산이나, 양 데이터를 결합한 데이터를 입력 값으로 하여, 해시함수의 출력 값을 이용하는 구성이라도 좋다.

[0370] 또, 비밀정보가 작용하게 하는 정보는 콘텐츠 키일 필요는 없으며, 키 암호화 키 등의 다른 키라도 좋다.

[0371] 이상과 같이, 서명 검증을 하여서 얻을 수 있는 비밀정보를 획득하지 않는 한은, 콘텐츠의 재생이 이루어지지 않는 구성이라면 어떤 구성이라도 좋다. 이와 같이, 메시지회복형 서명을 이용함으로써, 콘텐츠의 재생에는 서명 검증이 필수가 된다.

[0372] ⑬ 제 1 실시 예에서는, 콘텐츠 키 및 콘텐츠는 기록장치의 외부에서 얻는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0373] 예를 들어, 콘텐츠 기록장치 내부에 미리 콘텐츠 키 및 콘텐츠를 대응시켜서 저장하고 있는 것으로 해도 된다. 또, 콘텐츠 키를 이용할 때마다 기록장치 내부에서 생성해도 된다.

[0374] ⑭ 제 1 실시 예에서는, 각종 검증, 및 판정결과에 의해 제어되는 스위치(213)를 복호부 205와 재생부(214)의 사이에 구비하여, 재생부(214)에 대하여, 복호 콘텐츠의 출력 여부를 제어하는 것으로 하고 있으나, 본 발명은 이에 한정되는 것은 아니다.

[0375] 예를 들어, 스위치(213)를 복호부 204와 복호부 205 사이에 구비하여, 복호부 205에 대하여, 복호 콘텐츠 키의 출력을 행하는가의 여부를 제어하는 것으로 해도 된다.

[0376] 또, 스위치(213)를 키 계산부(203)와 복호부 204 사이에 구비하여, 복호부 204에 대하여, 키 복호 키 KDK의 출력을 행하는가의 여부를 제어하는 것으로 해도 된다.

[0377] 이와 같이, 각 검증의 결과에 의거하여 최종적인 콘텐츠의 재생을 제어할 수 있는 구성이라면 어떤 구성이라도 좋다. 또한, 스위치(213)는 물리적인 스위치일 필요는 없으며, 재생 제어를 행할 수 있는 구성이라면 소프트웨어에 의한 구성이라도 된다.

[0378] 또, 키 계산부(202)는, 생성한 복호 미디어 키 y가 검지 정보인 값 「0」인가 여부를 판단하여, 복호 미디어 키 y가 값 「0」이라고 판단하는 경우에, 스위치(213)에 대하여, 복호 콘텐츠 DCNT를 재생부(214)로 출력하지 않도록 지시하는 것으로 해도 된다.

[0379] 또, 키 계산부(202)는, 복호 미디어 키 y가 값 「0」이라고 판단하는 경우에, 키 계산부(203), 복호부 204, 복호부 205의 전부 또는 어느 하나에 대하여, 복호 키의 생성, 복호 콘텐츠 키의 생성, 복호 콘텐츠의 생성을 행하지 않도록 지시하는 것으로 해도 된다.

[0380] 또, 키 계산부(202)는, 복호 미디어 키 y가 값 「0」이라고 판단하는 경우에, 제어부(215)에 대하여, 복호 미디어 키 y가 값 「0」이라는 취지의 메시지를 통지하고, 제어부(215)는, 상기 메시지를 취득하면, 재생장치(200)를 구성하는 다른 구성요소에 대하여, 암호화 콘텐츠의 복호 및 재생을 중지하도록 지시하는 것으로 해도 된다.

[0381] ⑮ 제 1 실시 예에서는, 미디어 키, 암호화 키 및 콘텐츠 키의 3 계층으로 암호화 시스템을 채용하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0382] 예를 들어, 콘텐츠 키를 생략하고, 키 암호화 키로 직접 콘텐츠를 암호화하는 구성으로 해도 된다. 혹은, 새로운 키를 도입하여 그 계층을 1 계층 증가시키는 구성으로 해도 된다.

[0383] (16) 기록장치 또는 재생장치는, 인터넷으로 대표되는 네트워크를 거쳐서, 미디어 키 데이터 및 무효화리스트 CRL의 최신판을 취득하여, 내장하는 데이터를 갱신하는 구성으로 해도 된다.

[0384] (17) 제 1 실시 예에서는, 기록장치가 무효화 리스트 CRL을 기록매체에 기록하는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0385] 예를 들어, 재생장치는 무효화리스트 CRL을 네트워크를 거쳐서 취득하는 것으로 하고, 기록장치는 CRL을 기록매체에 기록하지 않는 구성이라도 된다.

[0386] (18) 제 1 실시 예에서는, 기록장치가, 기록매체에 기록하는 콘텐츠 또는 콘텐츠에 관련하는 정보에 대하여 서명데이터를 생성하고, 생성한 서명데이터를 기록매체에 기록하는 것으로 하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0387] 예를 들어, 기록장치는 서명 생성을 하지 않는 것으로 해도 된다. 이때, 기록장치는, 자신이 보유하는 미디어

키 데이터 및 매체 고유번호에 의거하여 콘텐츠를 암호화하여, 암호화에 사용한 미디어 키 데이터와 암호화된 콘텐츠를 기록매체에 기록하는 것으로 해도 된다. 이때, 재생장치는, 기록매체로부터 미디어 키 데이터, 매체 고유번호, 및 암호화 콘텐츠를 판독하고, 미디어 키 데이터 및 매체 고유번호에 의거하여 콘텐츠를 복호 한다.

[0388] (19) 제 1 실시 예에서는, 기록장치는, 미디어 키 및 매체 고유번호로부터 키 암호화 키를 생성함으로써 미디어 바인드를 실현하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0389] 예를 들어, 기록장치는, 미디어 키 및 매체 고유번호에 의거하여 인증자를 생성하고, 생성한 인증자를 기록매체에 기록함으로써 미디어 바인드를 실현하는 것으로 해도 된다. 이때, 재생장치는, 동일하게, 미디어 키 및 매체 고유번호로부터 인증자를 생성하고, 기록매체에 기록된 인증자와 생성한 인증자가 일치하는가 여부를 판정하여 콘텐츠의 재생을 제어한다.

[0390] 상기 인증자의 생성방법은, 일 예로서, 다음과 같다.

[0391] 미디어 키, 매체 고유번호 및 암호화 콘텐츠 키를 결합한 값에 해시함수를 실시하여, 얻어진 해시 값, 또는 해시 값의 특정한 일부를 인증자로 한다.

[0392] (20) 제 1 실시 예에서는, 1매의 기록매체는 1개의 콘텐츠 공급시스템에만 대응하고 있으나, 본 발명은 이 구성에 한정되는 것은 아니다.

[0393] 복수의 콘텐츠 공급시스템이 존재하며, 예를 들어, 하나의 콘텐츠 공급시스템은 영화 콘텐츠를 공급하는 시스템이고, 다른 콘텐츠 공급시스템은 컴퓨터 소프트웨어를 공급하는 시스템이다. 이와 같이, 공급되는 콘텐츠의 종류에 따라 다른 콘텐츠 공급시스템이 사용된다.

[0394] 또, 예를 들어, 하나의 콘텐츠 공급시스템은 영화공급업자 A에 의해 영화 콘텐츠를 공급하는 시스템이다. 다른 콘텐츠 공급시스템은 영화공급업자 B에 의해 영화 콘텐츠를 공급하는 시스템이다. 또 다른 콘텐츠 공급시스템은 영화공급업자 C에 의해 영화 콘텐츠를 공급하는 시스템이다. 이와 같이, 다른 콘텐츠 공급시스템이 사용되는 경우도 있다.

[0395] 여기서는, 1매의 기록매체가 다른 복수의 콘텐츠 공급시스템에서 사용되는 방법에 대하여 설명한다.

[0396] 도 9에 상기 기록매체에 기록되는 데이터의 일 예를 도시한다.

[0397] 기록매체(700)에는, 재기입 불가영역(710)과, 재기입 가능영역(720)이 존재하며, 재기입 불가영역(710)에는 제 1 콘텐츠 공급시스템용의 키 무효화 데이터 기록영역(711)과 고유번호 기록영역(712)이 존재한다. 또, 재기입 가능영역(720)에는, 제 2 콘텐츠 공급시스템용의 키 무효화 데이터 기록영역(721)과, 제 1 암호화 콘텐츠 기록영역(722)과, 제 2 암호화 콘텐츠 키 기록영역(723)과, 그 외의 암호화 콘텐츠 기록영역(미 도시)이 존재한다.

[0398] 여기서, 제 2 콘텐츠 공급시스템용의 키 무효화 데이터 기록영역(721)은 제 1 실시 예에서의 미디어 키 데이터 기록영역(122)에 상당한다. 또한, 제 1 암호화 콘텐츠 기록영역(722)에는 제 1 콘텐츠 공급시스템용의 키 무효화 데이터에 의거하여 암호화 된 데이터가 기록되고, 마찬가지로, 제 2 암호화 콘텐츠 키 기록영역(723)에는 제 2 콘텐츠 공급시스템용의 키 무효화 데이터에 의거하여 암호화된 데이터가 기록된다.

[0399] 이와 같이, 하나의 기록매체가 복수의 콘텐츠 공급시스템을 서포트 하는 경우, 매체 고유번호는 시스템별로 복수 존재할 필요는 없으며, 기록매체에 유일한 것이라도 좋고, 각 콘텐츠 공급시스템이 동일한 매체 고유번호, 혹은 그 일부분을 공통으로 사용하는 구성이라도 좋다.

[0400] 여기서, 매체 고유번호의 일부분을 사용한다는 것은, 예를 들어 128비트의 매체 고유번호가 존재하는 경우에, 상위 32비트는 사용하지 않고, 하위 96비트를 매체 고유번호로 하여 사용하거나, 매체 고유번호의 상위 32비트를 올(All) 0으로 치환해서, 128비트의 매체 고유번호로 하여 사용하거나 하는 것을 의미한다.

[0401] 이상과 같이, 기록매체에 미리 기록되어 있는 매체 고유번호를 복수의 콘텐츠 공급시스템에서 공통으로 사용함으로써, 이미 시판되어 이용되고 있는 매체 고유번호만을 기록한 기록매체에 있어서도 저작물의 저작권을 보호할 수 있는 시스템의 실현이 가능해진다. 또, 시스템별로 매체 고유번호를 기록할 필요가 없으므로, 재기입 불가영역의 용량 삭감도 가능하게 된다.

[0402] 이상과 같이, 본 발명은 적어도 제 1 및 제 2 콘텐츠 공급시스템에 대하여 저작물 보호의 방안을 제공하는 저작물 보호시스템이다.

[0403] 기록매체는, 판독 전용의 재기입 불가영역과, 판독 및 기입이 가능한 재기입 가능영역을 구비하며, 상기 재기입

불가영역에는, 당해 기록매체의 고유한 매체 고유번호와, 제 1 콘텐츠 공급시스템용의 무효화 데이터가 미리 기록되어 있다.

[0404] 제 1 콘텐츠 공급시스템은, 상기 기록매체에 콘텐츠를 암호화하여 기입하는 기록장치와, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 시도하는 복수의 재생장치로 구성되어 있다. 상기 복수의 재생장치 중 어느 1대 이상은 무효화 되어 있다. 상기 기록매체의 상기 재기입 불가영역에 기록되어 있는 상기 키 무효화 데이터는 상기 무효화 된 재생장치의 키를 나타내고 있다.

[0405] 상기 기록장치는, 상기 재기입 불가영역에 기록되어 있는 상기 무효화 데이터를 이용하여, 콘텐츠를 암호화하는 암호화부와, 생성한 암호화 콘텐츠를 상기 기록매체의 상기 재기입 가능영역에 기입하는 기입부를 구비한다.

[0406] 상기 재생장치는, 상기 기록매체의 상기 재기입 불가영역에 기록되어 있는 상기 키 무효화 데이터와, 상기 기록매체에 기록되어 있는 상기 암호화 콘텐츠를 판독하는 판독부와, 판독한 상기 키 무효화 데이터를 이용하여 상기 암호화 콘텐츠의 복호의 허가 여부를 판단하는 판단부와, 복호가 허가되지 않는 경우에 상기 암호화 콘텐츠의 복호를 금지하고, 복호가 허가되는 경우에 상기 암호화 콘텐츠를 복호 하여 복호 콘텐츠를 생성하는 복호부를 구비한다.

[0407] 또, 제 2 콘텐츠 공급시스템은, 상기 기록매체에 콘텐츠를 암호화하여 기입하는 기록장치와, 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 시도하는 복수의 재생장치로 구성되어 있다. 상기 복수의 재생장치 중 어느 1대 이상은 무효화 되어 있다.

[0408] 상기 기록장치는, 무효화 되어 있지 않은 각 재생장치에 대한 미디어 키와, 무효화 된 각 재생장치에 대한 소정의 검지 정보가, 각각 당해 재생장치의 디바이스 키를 이용하여 암호화되어 생성된 복수의 암호화 미디어 키로 구성되는 미디어 키 데이터를 기억하고 있는 기억부와, 상기 기록매체의 상기 재기입 불가영역에서 상기 매체 고유번호를 판독하는 판독부와, 판독한 상기 매체 고유번호 및 상기 미디어 키에 의거하여 암호화 키를 생성하는 생성부와, 생성된 상기 암호화 키에 의거하여 디지털 데이터인 콘텐츠를 암호화하여 암호화 콘텐츠를 생성하는 암호화부와, 상기 기억부에서 상기 미디어 키 데이터를 판독하는 판독부와, 판독된 상기 미디어 키 데이터 및 생성된 상기 암호화 콘텐츠를 상기 기록매체의 상기 재기입 가능영역에 기입하는 기입부를 구비한다.

[0409] 각 재생장치는, 상기 기록매체의 상기 재기입 불가영역에 기입된 미디어 키 데이터에서 당해 재생장치에 대응하는 암호화 미디어 키를 판독하는 판독부와, 당해 재생장치의 디바이스 키를 이용하여 판독된 상기 미디어 암호화 키를 복호 하여 미디어 키를 생성하는 복호부와, 생성된 복호 미디어 키가 상기 검지 정보인가 여부를 판단하여, 상기 검지 정보인 경우에 상기 기록매체에 기록되어 있는 암호화 콘텐츠의 복호를 금지하고, 상기 검지 정보가 아닌 경우에 암호화된 콘텐츠의 복호를 허가하는 제어부와, 복호가 허가된 경우에, 상기 기록매체에서 상기 암호화 콘텐츠를 판독하고, 생성된 복호 미디어 키에 의거하여 판독한 상기 암호화콘텐츠를 복호 하여 복호 콘텐츠를 생성하는 복호부를 구비한다.

[0410] 1. 8 요약

[0411] 이상 설명한 바와 같이, 본 발명은, 콘텐츠를 암호화하여 기록하는 기록장치와, 암호화 콘텐츠를 기록하는 기록매체와, 상기 기록매체에서 암호화 콘텐츠를 판독하여 복호 하는 재생장치로 이루어지는 저작권 보호시스템이다.

[0412] 상기 기록장치는, 특정 장치가 보유하는 키를 무효화하기 위한 무효화 데이터를 보유하고, 상기 무효화 데이터에 의거하여 상기 콘텐츠를 암호화하여, 상기 기록매체에 상기 무효화 데이터 및 상기 암호화 콘텐츠를 기록하며, 또한, 상기 콘텐츠 혹은 상기 콘텐츠의 암호화에 관련하는 데이터에 대하여 서명을 생성하고, 상기 생성한 서명을 상기 기록매체에 기록한다.

[0413] 상기 기록매체는, 사용자에 의해 재기입할 수 없는 영역에, 상기 기록매체를 일의(一意)로 식별하는 식별번호를 기록하고, 또한, 상기 무효화 데이터, 상기 암호화 콘텐츠, 및 상기 서명을 기록한다.

[0414] 상기 재생장치는, 상기 기록매체에서, 상기 무효화 데이터, 상기 암호화 콘텐츠, 및 상기 서명을 판독하고, 상기 무효화 데이터에 의거하여 상기 콘텐츠를 복호 하며, 상기 서명의 정당성을 검증한 결과에 의거하여 상기 복호 한 콘텐츠의 재생을 제어하는 것으로 해도 된다.

[0415] 여기서, 상기 저작권 보호시스템에 있어서, 상기 기록매체는 상기 무효화 데이터 및 상기 암호화 콘텐츠를 기록하고, 상기 서명은 상기 기록매체와는 다른 매체, 혹은 통신매체를 거쳐서 배포되는 것으로 해도 된다.

[0416] 여기서, 상기 저작권 보호시스템에 있어서, 상기 기록장치는 2개 이상의 장치의 조합으로 처리를 행하며, 상기 장치별로 처리를 분담하는 것으로 해도 된다.

[0417] 여기서, 상기 저작권 보호시스템에 있어서, 상기 재생장치는 2개 이상의 장치의 조합으로 처리를 행하며, 상기 장치별로 처리를 분담하는 것으로 해도 된다.

[0418] 여기서, 상기 저작권 보호시스템에 있어서, 상기 기록장치는 콘텐츠의 이용조건에 의거하여 콘텐츠를 기록하는 것으로 해도 된다.

[0419] 여기서, 상기 저작권 보호시스템에 있어서, 상기 재생장치는 콘텐츠의 이용조건에 의거하여 콘텐츠를 기록하는 것으로 해도 된다.

[0420] 여기서, 상기 저작권 보호시스템에 있어서, 상기 기록장치는, 상기 기록장치를 일의로 식별하는 장치 특정번호를 보유하고, 콘텐츠의 기록시에 상기 장치 특정번호를 전자 워터마크로 하여 상기 콘텐츠에 삽입해도 된다.

[0421] 여기서, 상기 저작권 보호시스템에 있어서, 상기 재생장치는, 상기 재생장치를 일의로 식별하는 장치 특정번호를 보유하고, 콘텐츠의 기록시에 상기 장치 특정번호를 전자 워터마크로 하여 상기 콘텐츠에 삽입해도 된다.

[0422] 여기서, 상기 저작권 보호시스템에 있어서, 부정장치가 발견된 때에, 상기 부정장치가 보유하는 키의 종류를 판정하는 키 발견장치를 포함하는 것으로 해도 된다.

[0423] 또, 본 발명은 콘텐츠를 암호화하여 기록하는 기록장치이다. 상기 기록장치는, 특정 장치가 보유하는 키를 무효화하기 위한 무효화 데이터를 보유하며, 상기 무효화 데이터에 의거하여 상기 암호화 콘텐츠를 암호화하고, 기록매체에 상기 무효화 데이터 및 상기 암호화 콘텐츠를 기록하며, 또한, 상기 콘텐츠 혹은 상기 콘텐츠의 암호화에 관련하는 데이터에 대하여 서명을 생성하고, 상기 생성한 서명을 상기 기록매체에 기록한다.

[0424] 여기서, 상기 기록장치는, 상기 무효화 데이터에 부가하여, 상기 기록매체를 일의로 식별하는 식별번호에 의거하여 상기 콘텐츠를 암호화하는 것으로 해도 된다.

[0425] 여기서, 상기 기록장치는, 공개 키의 무효화 리스트를 서명 대상으로 하여 서명의 생성을 행하는 것으로 해도 된다.

[0426] 여기서, 상기 기록장치는, 상기 콘텐츠 키를 기록하는 기록매체에 무효화 데이터가 존재하는 경우에, 상기 기록장치가 보유하는 무효화 데이터와 상기 기록매체에 존재하는 무효화 데이터의 신, 구를 비교하여, 새로운 무효화 데이터를 보유하는 것으로 해도 된다.

[0427] 여기서, 상기 기록장치는, 상기 무효화 데이터의 신, 구의 비교를 무효화 데이터의 사이즈의 비교에 의해 행하여, 사이즈가 큰 무효화 데이터를 새로운 것으로 판단하는 것으로 해도 된다.

[0428] 여기서, 상기 기록장치는, 상기 무효화 데이터의 신, 구의 비교를 무효화하고 있는 키의 수의 비교에 의해 행하여, 무효화하고 있는 키의 수가 많은 무효화 데이터를 새로운 것으로 판단하는 것으로 해도 된다.

[0429] 여기서, 상기 기록장치는, 상기 무효화 데이터의 신, 구의 비교를 무효화 데이터의 생성일, 혹은 버전 번호의 비교에 의해 행하며, 상기 생성일, 혹은 상기 버전 번호는 개찬으로부터 보호되고 있는 것으로 해도 된다.

[0430] 여기서, 상기 기록장치는, 상기 콘텐츠를 기록하는 기록매체에 무효화 데이터 및 암호화 콘텐츠가 존재하고, 또한, 상기 기록장치가 보유하는 무효화 데이터가 상기 기록매체에 기록되어 있는 무효화 데이터와 비교하여 새로운 경우에, 상기기록매체에 기록되어 있는 상기 암호화 콘텐츠를, 마찬가지로, 상기기록매체에 기록된 무효화 데이터에 의거하여 일단 복호 해서, 상기 기록장치가 보유하는 무효화 데이터에 의거하여 재 암호화하는 것으로 해도 된다.

[0431] 여기서, 상기 기록장치는, 상기 기록장치 내부에서 비밀정보를 생성하여, 상기 비밀정보와 상기 무효화 데이터에 의거하여 상기 콘텐츠를 암호화하고, 상기 비밀정보를 서명에 삽입하는 정보로 하여 서명을 생성해도 된다.

[0432] 또, 본 발명은 기록매체로부터 암호화 콘텐츠를 판독하여 복호 하는 재생장치이다. 상기 재생장치는, 상기 기록매체로부터 무효화 데이터, 상기 암호화 콘텐츠, 및 서명을 판독하고, 상기 무효화 데이터에 의거하여 상기 콘텐츠를 복호 하며, 상기 서명의 정당성을 검증한 결과에 의거하여 상기 복호 한 콘텐츠의 재생을 제어한다.

[0433] 여기서, 상기 재생장치는, 상기 무효화 데이터에 부가하여, 상기 기록매체를 일의로 식별하는 식별번호에 의거하여 상기 암호화 콘텐츠를 복호 하는 것으로 해도 된다.

[0434] 여기서, 상기 재생장치는, 공개 키의 무효화 리스트를 보유하여, 상기 무효화리스트를 사용하여, 상기 서명의 정당성의 검증에 사용하는 공개 키가 상기 무효화리스트에 등록되어 있는가 여부를 판단하고, 상기 판단한 결과에 의거하여 상기 복호 한 콘텐츠의 재생을 제어하는 것으로 해도 된다.

[0435] 여기서, 상기 재생장치는, 상기 기록매체에 상기 무효화리스트가 존재하는 경우에, 상기 재생장치가 보유하는 무효화 리스트와, 상기 기록매체에 존재하는 무효화 데이터의 신, 구를 비교하여, 새로운 무효화 리스트를 보유하는 것으로 해도 된다.

[0436] 여기서, 상기 재생장치는, 상기 무효화 리스트의 신, 구의 비교를 무효화 리스트의 사이즈의 비교에 의해 행하여, 사이즈가 큰 무효화 리스트를 새로운 것으로 판단하는 것으로 해도 된다.

[0437] 여기서, 상기 재생장치는, 상기 무효화 리스트의 신, 구의 비교를 무효화하고 있는 공개 키의 수의 비교에 의해 행하여, 무효화하고 있는 공개 키의 수가 많은 무효화 리스트를 새로운 것으로 판단하는 것으로 해도 된다.

[0438] 여기서, 상기 재생장치는, 상기 서명의 정당성의 검증을 행함으로써 비밀정보를 획득하고, 상기 획득한 비밀정보 및 무효화 데이터에 의거하여 상기 암호화 콘텐츠를 복호 하는 것으로 해도 된다.

[0439] 또, 본 발명은 암호화 콘텐츠를 기록하는 기록매체이다. 상기 기록매체는, 사용자에 의해 재기입 가능한 영역에 상기 기록매체를 일의로 식별하는 식별번호를 기록하고, 또한, 무효화 데이터, 암호화 콘텐츠, 및 서명을 기록하고 있다.

[0440] 여기서, 상기 기록매체는, 상기 무효화 데이터, 및 식별번호에 의거하여 암호화된 콘텐츠를 기록하고 있는 것으로 해도 된다.

[0441] 여기서, 상기 기록매체는, 상기 서명의 생성에 사용한 비밀 키에 대응하는 공개 키를 기록하고 있는 것으로 해도 된다.

[0442] 여기서, 상기 기록매체는, 2개 이상의 기록장치에 의해 기록된 경우에, 2개 이상의 무효화 데이터, 및 2개 이상의 공개 키를 기록하고 있는 것으로 해도 된다.

[0443] 이상 설명한 바와 같이, 제 1 실시 예에 있어서는, 기록장치가, 미디어 키 데이터로부터 산출되는 미디어 키에 의거하여 콘텐츠를 암호화하고, 또한, 기록장치 자신의 공개키 증명서 및 생성한 서명을 합하여 기록매체에 기록함으로써, 기록매체의 재기입 불가영역에 키 무효화정보가 기록되어 있지 않은 기록매체라도 키 무효화 및 미디어 바인드를 실현하여, 부정장치를 사용한 콘텐츠의 기록 또는 재생에 의한 저작물 침해의 방지를 실현할 수 있다.

[0444] 구체적으로는, 정규 기록장치 및 부정한 재생장치가 존재하는 경우, 정규 기록장치는 부정한 재생장치의 무효화를 나타내는 미디어 키 데이터에 의거하여 콘텐츠를 암호화해서 기록매체에 기록한다. 그 기록매체를 삽입한 부정한 재생장치는 기록되어 있는 미디어 키 데이터로부터는 미디어 키를 복호 할 수 없으므로, 부정한 재생장치에 의한 콘텐츠의 재생을 방지할 수 있다.

[0445] 또, 부정한 기록장치 및 정규 재생장치가 존재하는 경우, 부정한 기록장치는 자신이 무효화되어 있는 낡은(무효화 된) 미디어 키 데이터에 의거하여 콘텐츠를 암호화하여 기록매체에 기록한다. 이때, 기록장치 자신의 공개키 증명서 및 생성한 서명데이터도 기록한다. 그 기록매체를 삽입한 정규 재생장치는 기록되어 있는 미디어 키 데이터로부터 미디어 키를 복호 할 수 없다. 그러나 콘텐츠의 재생 전에 공개키 증명서가 무효화리스트 CRL에 등록되어 있는가 여부를 판단하므로, 무효화리스트 CRL에 등록되어 있는 부정한 기록장치에 의해 기록된 콘텐츠라면 그 재생을 정지시킬 수 있다.

[0446] 2. 제 2 실시 예

[0447] 본 발명에 관한 다른 실시 예로서의 콘텐츠 공급시스템(20)에 대하여 설명한다.

[0448] 2. 1 콘텐츠 공급시스템(20)의 구성

[0449] 콘텐츠 공급시스템 20은, 콘텐츠 공급시스템 10과 유사한 구성을 가지고 있다. 도 10에 도시한 바와 같이, 배신국장치(1400), 콘텐츠 서버장치(1500), 기록장치(1100) 및 재생장치(1200a, 1200b, 1200c, 1200d, 1200e, …)로 구성되어 있다.

[0450] 제 1 실시 예와 마찬가지로 재생장치 중 일부는 무효화되어 있다.

[0451] 2. 2 배신국장치(1400)

[0452] 배신국장치(1400)는, 정보기억부(1401), 제어부(1402), 입력부(1403), 표시부(1404) 및 송수신부(1405)로 구성되어 있다(미 도시).

[0453] 배신국장치(1400)는, 구체적으로는, 제 1 실시 예의 콘텐츠 서버장치(500)와 마찬가지로, 마이크로 프로세서, ROM, RAM, 하드디스크 유닛, 통신유닛, 디스플레이유닛, 키보드, 마우스 등으로 구성되는 컴퓨터시스템이다. 상기 RAM 또는 상기 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 배신국장치(1400)의 각 구성요소는 그 기능을 달성한다.

[0454] 송수신부(1405)는, 인터넷(40)을 거쳐서, 기록장치(1100)와 접속되어 있고, 기록장치(1100)와 제어부(1402) 사이에서 정보의 송수신을 행한다.

[0455] 정보기억부(1401)는 키 무효화 데이터 RDATA와 버전 번호 VR을 대응시켜서 미리 기억하고 있다.

[0456] 키 무효화 데이터 RDATA는 제 1 실시 예의 미디어 키 데이터 MDATA와 동일하다. 여기서는 상세한 설명을 생략한다.

[0457] 버전 번호 VR은 당해 버전 번호 VR에 대응하는 키 무효화 데이터 RDATA의 세대를 나타내는 정보이다.

[0458] 제어부(1402)는, 기록장치(1100)에서, 인터넷(40) 및 송수신부(1405)를 거쳐서, 키 무효화 데이터 RDATA의 취득 요구를 수신하고, 상기 취득 요구를 수신하면, 제어부(1401)는, 정보기억부(1401)에서 키 무효화 데이터 RDATA와 버전 번호 VR을 판독하고, 판독한 키 무효화 데이터 RDATA와 버전 번호 VR을 송수신부(1405) 및 인터넷(40)을 거쳐서 기록장치(1100)에 송신한다.

[0459] 입력부(1403)는, 배신국장치(1400)의 조작자의 지시를 접수하고, 접수한 지시를 제어부(1402)에 출력한다.

[0460] 표시부(1404)는 제어부(1402)의 제어에 의해 각종 정보를 표시한다.

[0461] 2. 3 콘텐츠 서버장치(1500)

[0462] 콘텐츠 서버장치(1500)는 제 1 실시 예의 콘텐츠 서버장치(500)와 동일한 구성을 가지고 있다. 여기서는 설명을 생략한다.

[0463] 2. 4 기록장치(1100)

[0464] 기록장치(1100)는, 도 11에 도시한 바와 같이, 디바이스 키 저장부(1101), 무효화 데이터 저장부(1102), 키 계산부(1103), 암호화부 1105, 암호화부 1106, 인증자 생성부(1104), 할당부(1107), 비교부(1108), 제어부(1109), 드라이브부(1110) 및 송수신부(1111)로 구성되어 있다.

[0465] ⑴ 디바이스 키 저장부(1101)

[0466] 디바이스 키 저장부(1101)는, 외부의 장치에서 액세스할 수 없도록, 디바이스 키 DK_1을 비밀로 기억하고 있다. 디바이스 키 DK_1은 기록장치(1100)에 고유한 키이다.

[0467] ⑵ 무효화 데이터 저장부(1102)

[0468] 무효화 데이터 저장부(1102)는 배신국장치(1400)에서 취득한 키 무효화 데이터 RDATA와 버전 번호 VR을 기록하기 위한 영역을 가지고 있다.

[0469] ⑶ 키 계산부(1103)

[0470] 키 계산부(1103)는 제 1 실시 예의 키 계산부(102)와 동일한 구성을 가지고 있다.

[0471] 키 계산부(1103)는, 무효화 데이터 저장부(1102)에서 키 무효화 데이터 RDATA를 판독하고, 디바이스 키 저장부(1101)에서 디바이스 키 DK_1을 판독한다. 다음으로, 키 계산부 103과 마찬가지로, 판독한 디바이스 키 DK_1을 이용하여, 판독한 무효화 데이터 RDATA에 복호 알고리즘 D1을 실시하여 미디어 키 MK를 생성하고, 생성한 미디어 키 MK를 인증자 생성부(1104) 및 암호화부 1105에 출력한다.

[0472] ⑷ 암호화부 1105

[0473] 암호화부 1105는, 콘텐츠 서버장치(1500)에서, 송수신부(1111)를 거쳐서, 콘텐츠 키 CK를 취득하고, 키 계산부(1103)에서 미디어 키 MK를 취득한다.

[0474] 다음에, 암호화부 1105는 취득한 미디어 키 MK를 이용하여, 취득한 콘텐츠 키 CK에 암호화 알고리즘 E2를 실시하여, 암호화 콘텐츠 키 ECK를 생성한다.

[0475] ? 암호화 콘텐츠 키 ECK = E2(MK, CK)

[0476] 다음에, 암호화부 1105는, 드라이브부(1110)를 거쳐서, 기록매체(1300) 상의 암호화 콘텐츠 파일(1320) 내에 키 기록부(1323)를 확보하고, 이어서, 생성한 암호화 콘텐츠 키 ECK를, 드라이브부(1110)를 거쳐서, 키 기록부(1323)에 기입한다.

[0477] 또, 암호화부 1105는 생성한 암호화 콘텐츠 키 ECK를 인증자 생성부(1104)에 출력한다.

[0478] (5) 암호화부 1106

[0479] 암호화부 1106은, 콘텐츠 서버장치(1500)에서, 송수신부(1111)를 거쳐서, 콘텐츠 키 CK 및 콘텐츠 CNT를 취득하고, 취득한 콘텐츠 키 CK를 이용하여 취득한 콘텐츠 CNT에 암호화 알고리즘 E3을 실시하여 암호화 콘텐츠 ECNT를 생성한다.

[0480] ? 암호화 콘텐츠 ECNT = E3(CK, CNT)

[0481] 다음에, 암호화부 1106은, 드라이브부(1110)를 거쳐서, 기록매체(1300) 상의 암호화 콘텐츠 파일(1320) 내에 콘텐츠 기록부(1324)를 확보하고, 이어서, 생성한 암호화 콘텐츠 ECNT를, 드라이브부(1110)를 거쳐서, 콘텐츠 기록영역(1324)에 기입한다.

[0482] (6) 인증자 생성부(1104)

[0483] 인증자 생성부(1104)는, 키 계산부(1103)에서 미디어 키 MK를 취득하고, 암호화부 1105에서 암호화 콘텐츠 키 ECK를 취득하며, 기록매체(1300)의 고유번호 기록영역(1301)에서 매체 고유번호 MID를 판독한다.

[0484] 다음에, 인증자 생성부(1104)는, 취득한 미디어 키 MK와, 판독한 매체 고유번호 MID와, 취득한 암호화 콘텐츠 키 ECK를 그 순서대로 결합하여 결합 데이터를 생성하고, 생성한 결합 데이터에 일 방향성 함수 F를 실시하여 인증자 MAC(Message Authentication Code)를 생성한다.

[0485] ? MAC = F(MK?ECK?MID)

[0486] 여기서, F(A)는 데이터 A에 대하여 일 방향성 함수 F를 실시하여 얻어진 값을 나타내고 있다. 또, 일 방향성 함수 F의 일 예는 해시함수 SHA-1이다.

[0487] 다음에, 인증자 생성부(1104)는, 드라이브부(1110)를 거쳐서, 기록매체(1300) 상의 암호화 파일(1320) 내에 인증자 기록부(1322)를 확보하고, 생성한 인증자 MAC를, 드라이브부(1110)를 거쳐서, 인증자 기록부(1322)에 기입한다.

[0488] 이와 같이 하여 생성된 인증자 MAC는 재생장치(1200)에서 콘텐츠의 정당성을 판정할 때에 이용된다.

[0489] (7) 할당부(1107)

[0490] 할당부(1107)는, 기록매체(1300)에 기록하는 키 무효화 데이터 RDATA에 대해서, 기록매체(1300)에서 그 키 무효화 데이터 RDATA를 일의로 식별하는 키 무효화 데이터 식별자 RID를 생성한다. 이어서, 드라이브부(1110)를 거쳐서, 기록매체(1300) 상의 암호화 콘텐츠 파일(1320) 내에 식별자 기록부(1321)를 확보하고, 생성한 키 무효화 데이터 식별자 RID를, 드라이브부(1110)를 거쳐서, 식별자 기록부(1321)에 기입한다.

[0491] 또한, 할당부(1107)에 의한 키 무효화 데이터 식별자 RID의 구체적인 할당방법은 후술한다.

[0492] (8) 비교부(1108)

[0493] 비교부(1108)는, 제어부(1109)의 지시에 의해, 드라이브부(1110)를 거쳐서, 기록매체(1300)에 키 무효화 데이터 파일이 존재하는가 여부를 확인한다. 다음에, 드라이브부(1110)에서 키 무효화 데이터 파일이 존재하는가 여부를 나타내는 존부(存否) 정보를 취득한다.

[0494] 취득한 존부정보가 기록매체(1300)에 키 무효화 데이터 파일이 존재하지 않는 것을 나타내는 경우에는, 비교부(1108)는, 할당부(1107)에 대하여 키 무효화 데이터 식별자 RID의 생성을 지시하고, 또, 드라이브부(1110)에 대하여, 무효화 데이터 저장부(1102)에 기록되어 있는 키 무효화 데이터 RDATA와, 그 버전 번호 VR과, 할당부(1107)에 의해 생성된 키 무효화 데이터 식별자 RID로 구성되는 키 무효화 데이터 파일을 기록매체(1300)에 기

입하도록 지시한다.

[0495] 상기 존부정보가, 기록매체(1300)에 키 무효화 데이터 파일이 존재하는 것을 나타내는 경우에는, 비교부(1108)는, 드라이브부(1110)를 거쳐서, 기록매체(1300) 상의 각 키 무효화 데이터 파일에서 키 무효화 데이터 RDATA에 포함되어 있는 버전 번호 VF를 판독한다. 이 경우에, 1개 이상의 버전 번호 VF가 판독된다. 또, 무효화 데이터 저장부(1102)에서 키 무효화 데이터 RDATA에 대응하는 버전 번호 VR을 판독한다.

[0496] 다음에, 비교부(1108)는, 판독한 버전 번호 VR과 동일한 내용의 버전 번호가 판독한 1개 이상의 버전 번호 VF 중에 존재하는가 여부를 판단하여, 존재하지 않는다고 판단하는 경우에, 상기와 마찬가지로, 할당부(1107)에 대하여 키 무효화 데이터 식별자 RID의 생성을 지시하고, 또, 드라이브부(1110)에 대하여, 무효화 데이터 저장부(1102)에 기록되어 있는 키 무효화 데이터 RDATA와, 그 버전 번호 VR과, 할당부(1107)에 의해 생성된 키 무효화 데이터 식별자 RID로 구성되는 키 무효화 데이터 파일을 기록매체(1300)에 기입하도록 지시한다.

[0497] 존재한다고 판단하는 경우에, 비교부(1108)는 판독한 버전 번호 VR과 동일한 내용의 버전 번호가 존재하는 것을 나타내는 정보를 제어부(1109)에 출력한다.

[0498] ⑼ 제어부(1109)

[0499] 제어부(1109)는, 송수신부(1111) 및 인터넷(40)을 거쳐서, 배신국장치(1400)에 대하여 키 무효화 데이터 RDATA의 취득 요구를 송신한다. 또, 제어부(1109)는, 송수신부(1111)를 거쳐서, 콘텐츠 서버장치(1500)에 대하여 콘텐츠의 취득 요구를 송신한다.

[0500] 제어부(1109)는, 비교부(1108)에 대하여, 기록매체(1300)에 키 무효화 데이터 파일이 존재하는가 여부를 확인하도록 지시한다.

[0501] 비교부(1108)로부터 버전 번호 VR과 동일한 내용의 버전 번호가 존재하는 것을 나타내는 정보를 취득한 경우에는, 드라이브부(1110)에 대하여, 기록매체(1300) 상에서 버전 번호 VR과 동일한 내용의 버전번호를 포함하는 키 무효화 데이터 파일에서 키 무효화 데이터 식별자 RID를 판독하도록 지시하여, 드라이브부(1110)에서 키 무효화 데이터 식별자 RID를 취득한다.

[0502] 다음에, 제어부(1109)는, 키 계산부(1103)에 대하여, 디바이스 키 DK_1과 키 무효화 데이터 RDATA를 판독하여 미디어 키 MK를 생성하도록 지시하고, 암호화부 1105에 대하여, 콘텐츠 키 CK를 암호화하도록 지시하며, 인증자 생성부(1104)에 대하여, 매체 고유번호 MID를 판독하여 인증자 MAC를 생성하도록 지시하고, 암호화부 1106에 대하여, 콘텐츠 CNT를 암호화하도록 지시하며, 이어서, 드라이브부(1110)에 대하여, 기록매체(1300) 상에 암호화 콘텐츠 파일을 확보하도록 지시하고, 인증자 생성부(1104), 암호화부 1105 및 암호화부 1106에 대하여, 각각 생성된 인증자 MAC와, 생성된 암호화 콘텐츠 키 ECK와, 생성된 암호화 콘텐츠 ECNT를 기록매체(1300) 상의 암호화 콘텐츠 파일 내에 기입하도록 지시한다. 또, 드라이브부(1110)에 대하여, 기록매체(1300) 상의 암호화 콘텐츠 파일 내에 식별자 기록부(1303)를 확보하도록 지시하며, 할당부(1107)에 의해 생성된, 또는 드라이브부(1110)에서 취득한 키 무효화 데이터 식별자 RID를 식별자 기록부(1303)에 기입하도록 지시한다.

[0503] ⑽ 송수신부(1111)

[0504] 송수신부(1111)는 인터넷(40)을 거쳐서 배신국장치(1400)와 접속되어 있다. 또, 전용회선(30)을 거쳐서 콘텐츠 서버장치(1500)와 접속되어 있다.

[0505] 송수신부(1111)는, 배신국장치(1400)에서, 인터넷(40)을 거쳐서, 키 무효화 데이터 RDATA와 버전 번호 VR을 수신한다. 키 무효화 데이터 RDATA와 버전 번호 VR을 수신하면, 수신한 키 무효화 데이터 RDATA 및 버전 번호 VR을 대응시켜서 무효화 데이터 저장부(1102)에 기입한다.

[0506] 또, 송수신부(1111)는, 전용회선(30)을 거쳐서, 콘텐츠 서버장치(1500)에서 콘텐츠 키 CK 및 콘텐츠 CNT를 암호화부 1106에 출력하고, 수신한 콘텐츠 키 CK를 암호화부 1105에 출력한다.

[0507] ⑾ 드라이브부(1110)

[0508] 드라이브부(1110)는, 기록장치(1100)를 구성하는 각 구성요소의 지시에 의해 기록매체(1300)에서 정보를 판독하고, 판독한 정보를 당해 구성요소에 출력한다.

[0509] 또, 드라이브부(1110)는, 기록장치(1100)를 구성하는 각 구성요소의 지시에 의해 기록매체(1300)에 각 영역을 확보하고, 또, 각 구성요소로부터 정보를 취득하여 확보한 영역에 취득한 상기 정보를 기입한다.

[0510] ⑿ 키보드(1180) 및 모니터(1190)

[0511] 키보드(1180)는, 기록장치(1100)의 조작자의 조작지시를 접수하고, 접수한 조작지시에 대응하는 지시정보를 제어부(1109)에 출력한다.

[0512] 모니터(1190)는 제어부(1109)의 제어에 의해 각종 정보를 표시한다.

[0513] 2. 5 기록매체(1300)

[0514] 기록매체 1300은 기록매체 120과 마찬가지로 광디스크 미디어이며, 도 12에 도시한 바와 같이, 재기입 불가영역(1308)과 재기입 가능영역(1309)으로 구성되어 있다.

[0515] 재기입 불가영역(1308)은, 도 12에 도시한 바와 같이, 고유번호 기록영역(1301)을 가지고 있다. 기록매체(1300)의 제조시에, 고유번호 기록영역(1301)에는 기록매체(1300)에 고유한 매체고유번호 MID가 기록되어 있다. 이 때, 재기입 가능영역(1308)에는 아무것도 기록되어 있지 않다. 이 도면에서는, 매체 고유번호 MID는 16진수 8자리로 표현되어 있고, 구체적으로는 「5」이다.

[0516] 그 후, 상술한 바와 같이, 기록장치(1100)에 의해 기록매체(1300) 상에 정보가 기입되면, 재기입 가능영역(1309)에는 기록장치(1100)에 의해 기록영역 1305와 기록영역 1306이 확보되고, 기록영역 1305에는 1개 이상의 키 무효화 데이터 파일이 기록되고, 기록영역 1306에는 1개 이상의 암호화 콘텐츠 파일이 기록된다.

[0517] 일 예로서, 도 12에 도시한 바와 같이, 기록영역 1305에는 키 무효화 데이터 파일(1310)이 기록되며, 기록영역 1306에는 암호화 콘텐츠 파일(1320)이 기록된다. 또한, 도 12에 도시하는 기록매체(1300)에는, 일 예로서, 1개의 키 무효화 파일과 1개의 암호화 콘텐츠 파일이 기록되어 있으나, 1개 이상의 키 무효화 파일과 1개 이상의 암호화 콘텐츠 파일이 기록매체 상에 기록되는 경우도 있다.

[0518] 키 무효화 데이터 파일(1310)은, 도 12에 도시한 바와 같이, 판수 기록부(1311), 식별자 기록부(1312) 및 데이터 기록부(1313)로 구성되어 있다.

[0519] 판수 기록부(1311)에는 키 무효화 데이터 RDATA의 세대를 나타내는 버전 번호가 기록되어 있고, 식별자 기록부(1312)에는 기록장치(1100)의 할당부(1107)에 의해 할당된 키 무효화 데이터 식별자 RID가 기록되어 있으며, 데이터 기록부(1313)에는 키 무효화 데이터 RDATA가 기록되어 있다.

[0520] 여기서, 버전 번호, 키 무효화 데이터 식별자 RID 및 키 무효화 데이터 RDATA에 대해서는 상술한 바와 같다.

[0521] 도 12에서, 버전 번호는 16진수 4자리로 표현되어 있고, 구체적으로는, 「3」이다. 제 2 실시 예에서는 배신국 장치(1400)에서 키 무효화 데이터의 버전번호가 할당된다.

[0522] 도 12에서, 키 무효화 데이터 식별자는 16진수 4자리로 표현되어 있고, 키 무효화 데이터 식별자 RID는, 구체적으로는 「1」이다.

[0523] 또, 암호화 콘텐츠 파일(1320)은,도 12에 도시한 바와 같이, 식별자 기록부(1321), 인증자 기록부(1322), 키 기록부(1323) 및 콘텐츠 기록부(1324)로 구성되어 있다. 또, 암호화 콘텐츠 파일(1320)에는 당해 파일에 포함되어 있는 암호화 콘텐츠를 식별하는 콘텐츠 번호가 부가되어 있다(미 도시).

[0524] 식별자 기록부(1321)에는 키 무효화 데이터 식별자 RID가 기록되어 있다. 키 무효화 데이터 식별자 RID는, 콘텐츠 암호화에서 사용되는 키 무효화 데이터에 대하여, 기록장치(1100)의 할당부(1107)에 의해 할당된 것이다.

[0525] 인증자 기록부(1322)에는 인증자 MAC가 기록되어 있다. 인증자 MAC는 기록장치(1100)의 인증자 생성부(1104)에 의해 생성된 것이다.

[0526] 키 기록부(1323)에는 기록장치(1100)의 암호화부 1105에 의해 생성된 암호화 콘텐츠 키 ECK가 기록되어 있다.

[0527] 콘텐츠 기록부(1324)에는 기록장치(1100)의 암호화부 1106에 의해 생성된 암호화 콘텐츠 ECNT가 기록되어 있다.

[0528] 2. 6 재생장치(1200)

[0529] 재생장치(1200a, 1200b, 1200c, …)는 동일한 구성을 가지고 있으므로 여기서는 재생장치(1200)로 하여 설명한다.

[0530] 재생장치(1200)는, 도 13에 도시한 바와 같이, 디바이스 키 저장부(1201), 키 계산부(1202), 인증자 생성부(1203), 복호부 1204, 복호부 1205, 비교부(1206), 지정접수부(1207), 취득부(1208), 검색부(1209), 스위치

(1211), 드라이브부(1213), 재생부(1214), 제어부(1215), 입력부(1216) 및 표시부(1217)로 구성되어 있다.

[0531] 재생장치 1200은, 구체적으로는, 재생장치 200과 마찬가지로, 마이크로 프로세서, ROM, RAM, 하드디스크 유닛 등으로 구성되는 컴퓨터 시스템이다. 상기 RAM 또는 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써 재생장치(1200)는 그 기능을 달성한다.

[0532] (1) 지정접수부(1207)

[0533] 지정접수부(1207)는, 이용자로부터, 리모컨(1280) 및 입력부(1216)를 거쳐서 재생해야 할 콘텐츠의 지정을 접수하고, 지정을 접수한 콘텐츠를 식별하는 콘텐츠 번호를 취득부(1208) 및 인증자 생성부(1203)에 출력한다.

[0534] (2) 취득부(1208)

[0535] 취득부(1208)는, 지정접수부(1208)에서 콘텐츠 번호를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300)의 기록영역(1305)에서 취득한 콘텐츠 번호가 부가된 암호화 콘텐츠 파일(1320)을 검색하고, 검색한 암호화콘텐츠 파일(1320)의 식별자 기록부(1321)에서 키 무효화 데이터 식별자 RID를 판독한다. 다음에, 판독한 키 무효화 데이터 식별자 RID를 검색부(1209)에 출력한다.

[0536] (3) 검색부(1209)

[0537] 검색부(1209)는 취득부(1208)에서 키 무효화 데이터 식별자 RID를 취득한다. 키 무효화 데이터 식별자 RID를 취득하면, 드라이브부(1213)를 거쳐서, 기록매체(1300)의 기록영역(1305)에 기록된 1개 이상의 키 무효화 데이터 파일에서 취득한 키 무효화 데이터 식별자 RID와 동일한 내용의 키 무효화 데이터 식별자를 식별자 기록부에 포함하는 키 무효화 데이터 파일을 검색하고, 검색한 키 무효화 데이터 파일의 데이터 기록부로부터 키 무효화 데이터 RDATA를 판독한다.

[0538] 다음에, 검색부(1209)는 판독한 키 무효화 데이터 RDATA를 키 계산부(1202)에 출력한다.

[0539] (4) 디바이스 키 저장부(1201)

[0540] 디바이스 키 저장부 1201은, 디바이스 키 저장부 201과 마찬가지로, 외부의 장치에서 액세스할 수 없도록, 디바이스 키 DK_x를 비밀로 기억하고 있다. 디바이스 키 DK_x는 재생장치(1200)에 고유한 키이다.

[0541] (5) 키 계산부(1202)

[0542] 키 계산부(1202)는, 검색부(1209)에서 키 무효화 데이터 RDATA를 취득하고, 디바이스 키 저장부(1201)에서 디바이스 키 DK_x를 판독한다.

[0543] 다음에, 키 계산부 1202는, 키 계산부 202와 동일한 방법으로, 판독한 디바이스 키 DK_x를 이용하여, 취득한 키 무효화 데이터 RDATA에 복호 알고리즘 D1 실시하여, 복호 미디어 키 y를 생성한다.

[0544] 여기서, 복호 미디어 키 y는 미디어 키 MK 및 값 「0」 중 어느 하나이다.

[0545] 다음에, 키 계산부(1202)는 생성한 복호 미디어 키 y를 인증자 생성부(1203) 및 스위치(1211)에 출력한다.

[0546] (6) 인증자 생성부(1203)

[0547] 인증자 생성부(1203)는, 키 계산부(1202)에서 복호 미디어 키 y를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300)의 고유번호 기록영역(1301)에서 기록매체 고유번호(MID)를 판독한다. 또, 지정접수부(1207)에서 콘텐츠 번호를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300) 상에서 취득한 상기 콘텐츠 번호가 부가된 암호화 콘텐츠 파일(1320)을 특정하고, 특정된 암호화 콘텐츠 파일(1320)의 키 기록부(1323)에서 암호화 콘텐츠 키 ECK를 판독한다.

[0548] 다음에, 취득한 복호 미디어 키 y와, 판독한 암호화 콘텐츠 키 ECK와, 판독한 매체 고유번호 MID를 그 순서대로 결합하여 결합 데이터를 생성하고, 생성한 결합 데이터에 일 방향성 함수 F를 실시하여 복호 인증자 DMAC를 생성한다.

[0549] ? DMAC = F(y?ECK?MID)

[0550] 다음에, 인증자 생성부(1203)는 생성한 복호 인증자 DMAC를 비교부(1206)에 출력한다.

[0551] (7) 비교부(1206)

[0552] 비교부(1206)는 인증자 생성부(1203)에서 복호 인증자 DMAC를 취득한다. 또, 비교부(1206)는, 지정접수부(120

7)에서 콘텐츠 번호를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300) 상에서 취득한 상기 콘텐츠 번호가 부가된 암호화 콘텐츠 파일(1320)을 특정하며, 특정된 암호화 콘텐츠 파일(1320)의 인증자 기록부(1322)에 기록되어 있는 인증자 MAC를 판독한다.

[0553] 다음에, 비교부(1206)는 취득한 복호 인증자 DMAC와 판독한 인증자 MAC가 일치하는가 여부를 판독한다. 일치한다고 판단하는 경우에, 스위치(1211)에 폐쇄 지시를 출력하고, 일치하지 않는다고 판단하는 경우에 스위치(1211)에 개방 지시를 출력한다.

[0554] ⑻ 스위치(1211)

[0555] 스위치(1211)는 비교부(1206)로부터의 지시에 의해 개폐가 제어된다. 스위치(1211)는, 비교부(1206)로부터 폐쇄 지시를 취득한 경우에 폐쇄되고, 개방 지시를 취득한 경우에 개방된다.

[0556] 또, 스위치(1211)는 키 계산부(1202)에서 복호 미디어 키 y를 취득한다. 폐쇄 지시를 취득한 경우에는 복호 미디어 키 y는 외부로 출력하지 않는다.

[0557] ⑼ 복호부 1204

[0558] 복호부 1204는 스위치(1211)에서 복호 미디어 키 y를 취득한다. 또, 지정접수부(1207)에서 콘텐츠 번호를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300) 상에서 취득한 상기 콘텐츠 번호가 부가된 암호화 콘텐츠파일(1320)을 특정하고, 특정된 암호화 콘텐츠 파일(1320)의 키 기록부(1323)에 기록되어 있는 암호화 콘텐츠 키 ECK를 판독하여, 취득한 복호 미디어 키 y를 이용하여, 판독한 암호화 콘텐츠 키 ECK에 복호 알고리즘 D2를 실시하여 복호 콘텐츠 키 DCK를 생성하며, 생성한 복호 콘텐츠 키 DCK를 복호부 1205에 출력한다.

[0559] ⑽ 복호부 1205

[0560] 복호부 1205는 복호부 1204로부터 복호 콘텐츠 키 DCK를 취득한다. 또, 지정접수부(1207)에서 콘텐츠 번호를 취득하고, 드라이브부(1213)를 거쳐서, 기록매체(1300) 상에서 취득한 상기 콘텐츠 번호가 부가된 암호화 콘텐츠 파일(1320)을 특정하며, 특정된 암호화 콘텐츠파일(1320)의 콘텐츠 기록부(1324)에 기록되어 있는 암호화 콘텐츠 ECNT를 판독하고, 취득한 복호 콘텐츠 키 DCK를 이용하여 판독한 암호화 콘텐츠 ECNT에 복호 알고리즘 D3을 실시해서 복호 콘텐츠 DCNT를 생성하며, 생성한 복호 콘텐츠 DCNT를 재생부(1214)에 출력한다.

[0561] ⑾ 재생부(1214)

[0562] 재생부(1214)는 복호부 1205로부터 복호 콘텐츠 DCNT를 취득하고, 취득한 복호 콘텐츠 DCNT로부터 영상정보 및 음성정보를 생성하며, 생성한 영상정보 및 음성정보를 아날로그 영상신호 및 음성신호로 변환하여, 아날로그 영상신호 및 음성신호를 모니터(1290)에 출력한다.

[0563] ⑿ 제어부(1215), 입력부(1216), 표시부(1217), 드라이브부(1213), 모니터(1290) 및 리모컨(1280)

[0564] 제어부(1215)는 재생장치(1200)를 구성하는 각 구성요소의 동작을 제어한다.

[0565] 리모컨(1280)은, 각종 버튼을 구비하며, 조작자의 상기 버튼의 조작에 따른 조작지시정보를 생성하고, 생성한 조작지시정보를 적외선에 실어서 출력한다.

[0566] 입력부(1216)는, 리모컨(1280)으로부터 조작지시정보가 실린 적외선을 수신하고, 수신한 적외선에서 조작지시정보를 추출하며, 추출한 조작지시정보를 제어부(1215) 또는 지정접수부(1207)에 출력한다.

[0567] 표시부(1217)는 제어부(1215)의 제어에 의해 각종 정보를 표시한다.

[0568] 드라이브부(1213)는 기록매체(1300)로부터의 정보의 판독을 행한다.

[0569] 모니터(1290)는, CRT 및 스피커를 구비하며, 재생부(1214)로부터 아날로그의 영상신호 및 음성신호를 수신하여, 영상신호에 의거 영상을 표시하고 음성신호에 의거 음성을 출력한다.

[0570] 2. 7 기록매체에 기록되는 데이터의 구조와 관련 처리

[0571] ⑴ 버전 번호

[0572] 도 12에서, 버전 번호는 16진수 4자리로 표현되어 있고, 구체적으로는, 「3」이다. 제 2 실시 예에서는 배신국 장치(1400)로부터 키 무효화 데이터의 버전 번호가 할당된다.

[0573] 구체적으로는, 최초에 발행된 키 무효화 데이터에는 버전 번호로서 「1」이 할당되고, 그 후 발행되는 키 무효

화 데이터는 버전 번호가 「2」, 「3」, … 과 같이 할당된다.

[0574] 키 무효화가 발생한 경우 새로운 키 무효화 데이터가 발행되며, 그때에 새로운 버전 번호가 부여된다. 또한, 새로운 키 무효화 데이터의 발행은 키 무효화가 발생한 경우 만에 한정되는 것은 아니다. 예를 들어, 보안의 관점에서 미리 정해진 일정 기간마다 새로운 키 무효화 데이터의 발행을 해도 된다.

[0575] ⑵ 키 무효화 데이터 식별자

[0576] 도 12에서, 식별자 기록부(1312)에 기록되어 있는 키 무효화 데이터 식별자는 16진수 4자리로 표현되어 있고, 키 무효화 데이터 식별자 RID는 「1」이다.

[0577] 여기서, 키 무효화 데이터 식별자 RID는 기록매체별로 각각 기록되는 키 무효화 데이터를 일의적으로 식별하기 위한 정보이다. 따라서 기록매체별로 독립된 체계에 의해 키 무효화 데이터 식별자를 할당할 수 있다.

[0578] 기록장치(1100)의 할당부(1107)에 의한 키 무효화 데이터 식별자 RID의 구체적인 할당방법으로는, 할당부(1107)는 이미 기록매체에 기록되어 있는 키 무효화 데이터에 할당된 키 무효화 데이터 식별자와는 다른 값을 할당한다.

[0579] 예를 들어, 도 14에 도시하는 바와 같이, 기록매체 1300a에 이미 키 무효화 데이터 파일 1과 키 무효화 데이터 파일 2가 기록되어 있고, 각각의 키 무효화 데이터 식별자는 「1」 및 「2」라고 하자.

[0580] 이때, 이 기록매체에 새로운 키 무효화 데이터 파일 3을 기록할 때, 할당부(1107)는 키 무효화 데이터 식별자 RID로 「1」 및 「2」 이외의 값인, 예를 들어 「3」을 할당한다.

[0581] ⑶ 디바이스 키와 미디어 키

[0582] 도 12에서, 데이터 기록부(1313)에는, n개의 디바이스 키 DK_i(i = 1, 2, 3, …, n)를 이용하여, 미디어 키 MK를 각각 암호화함으로써 얻어지는 암호화 미디어 키 E(DK_i, MK)가 기록되어 있다.

[0583] 또, 도 12에서, 장치 n이 보유하는 디바이스 키를 DK_n으로 표현하고 있다. 이 도면의 예에서는 장치 3 및 장치 4가 무효화되어 있으므로, 각각이 보유하는 DK_3 및 DK_4에서는 미디어 키 MK와는 전혀 관계가 없는 데이터 「0」이 암호화되어 기록되어 있다.

[0584] 키 무효화 데이터를 이와 같이 생성함으로써, 예를 들어, 디바이스 키 DK_1을 보유하는 장치 1은 키 무효화 데이터의 E(DK_1, MK)를 디바이스 키 DK_1로 복호 함으로써 미디어 키 MK를 얻을 수 있으나, 디바이스 키 DK_3을 보유하는 장치 3은 키 무효화 데이터 E(DK_3, 0)를 디바이스 키 DK_3으로 복호 하였다고 해도 미디어 키 MK를 얻을 수 없다.

[0585] 이와 같이, 도 12의 예에서는, 장치 3 및 장치 4 이외의 모든 장치만이 올바른 미디어 키 MK를 공유할 수 있고, 장치 3 및 장치 4는 올바른 미디어 키 MK를 얻을 수 없다. 이렇게 하여, 무효화 된 장치 3 및 장치 4를 시스템에서 배제할 수 있다.

[0586] 또한, 장치의 무효화방법은 다른 방법을 이용해도 되며, 예를 들어, 특허문헌 1에는 트리구조를 이용한 무효화 방법이 개시되어 있다.

[0587] ⑷ 암호화 콘텐츠 파일

[0588] 도 12에서, 암호화 콘텐츠 파일(1320)은, 식별자 기록부(1321), 인증자 기록부(1322), 키 기록부(1323) 및 콘텐츠 기록부(1324)로 이루어진다.

[0589] 이 도면에서, 식별자 기록부(1321)에 기록되어 있는 키 무효화 데이터 식별자는 16진수 4자리로 표현되어 있고, 키 무효화 데이터 식별자 RID는 구체적으로는 「1」이다.

[0590] 키 무효화 데이터 식별자 RID는, 이하에서 설명하는 바와 같이, 재생장치(1200)에서 재생하고자 하는 암호화 콘텐츠를 복호 하기 위해 사용하는 키 무효화 데이터 파일(310)을 기록매체(1300)로부터 취득하기 위해 사용된다.

[0591] 즉, 재생장치(1200)에서 기록매체(1300)에 기록된 암호화 콘텐츠를 복호 재생할 때, 재생하고자 하는 암호화 콘텐츠 파일(1320)의 식별자 기록부(1321)에 기록되어 있는 키 무효화 데이터 식별자 RID와 동일한 키 무효화 데이터 ID를 식별자 기록부(1312)에 포함하는 키 무효화 데이터 파일(310)을 기록매체(1300)에서 취득한다.

[0592] 여기서, 도 15를 이용하여 보다 구체적으로 설명한다. 도 15에 도시하는 바와 같이, 기록매체 1300b에는, 키 무효화 데이터 파일 1, 키 무효화 데이터 파일 2, 암호화 콘텐츠 파일 A, 암호화 콘텐츠 파일 B, 암호화 콘텐츠

파일 C가 기록되어 있다.

[0593] 이 도면에 도시하는 바와 같이, 키 무효화 데이터 파일 1 및 키 무효화 데이터 파일 2의 키 무효화 데이터 식별자는 각각 「1」 및 「2」이다. 또, 암호화 콘텐츠 파일 A, 암호화 콘텐츠 파일 B 및 암호화 콘텐츠 파일 C의 키 무효화 데이터 식별자는 각각 「1」, 「1」 및 「2」이다.

[0594] 이것은, 기록장치(1100)에서, 암호화 콘텐츠 파일 A를 생성할 때 키 무효화 데이터 파일 1의 키 무효화 데이터를 사용하고, 암호화 콘텐츠 파일 B를 생성할 때 키 무효화 데이터 파일 1의 키 무효화 데이터를 사용하며, 암호화 콘텐츠 파일 C를 생성할 때 키 무효화 데이터 파일 2의 키 무효화 데이터를 사용하였다는 것을 나타내고 있다.

[0595] 이때, 재생장치(1200)는, 예를 들어, 도 15에 도시하는 기록매체 1300b에서의 암호화 콘텐츠 파일 B를 복호 하여 재생하는 경우에는, 암호화 콘텐츠 파일 B의 키 무효화 데이터 식별자는 「1」이므로, 키 무효화 데이터 식별자가 「1」인 키 무효화 데이터 파일 1을 취득하고, 취득한 키 무효화 데이터 파일 1에 포함되어 있는 키 무효화 데이터를 사용하여, 암호화 콘텐츠 파일 B에 저장되어 있는 암호화 콘텐츠를 복호 한다.

[0596] 2. 8 콘텐츠 공급시스템(20)의 동작

[0597] 콘텐츠 공급시스템(20)의 동작에 대해서, 특히, 기록장치(1100)에 의한 기록매체(1300)로의 데이터의 기입동작 및 재생장치(1200)에 의한 기록매체(1300)에 기록되어 있는 데이터의 재생동작에 대하여 설명한다.

[0598] ⑴ 기록장치(1100)에 의한 기입동작

[0599] 기록장치(1100)에 의한 기록매체(1300)로의 데이터의 기입동작에 대하여 도 16 내지 도 18의 플로우챠트를 이용하여 설명한다.

[0600] 기록장치(1100)의 송수신부(1111)는, 배신국장치(1400)로부터 인터넷(40)을 거쳐서 키 무효화 데이터 RDATA 및 버전번호 VR을 수신하고, 수신한 키 무효화 데이터 RDATA 및 버전번호 VR을 대응시켜서 무효화데이터 저장부(1102)에 저장한다(스텝 S1501).

[0601] 또한, 스텝 S1501에서의 키 무효화 데이터 RDAT 및 버전 번호 VR의 수신은 배신국장치(1400)에 의해 새로운 키 무효화 데이터 RDATA가 발행된 때에 행해진다. 키 무효화 데이터 RDATA에는, 상술한 바와 같이, 그 발행순서를 나타내는 버전 번호 VR이 부가되어 있다. 기록장치(1100)는 이 버전번호 VR에 의거하여 수신한 키 무효화 데이터 RDATA가 새로운 것인가 여부를 확인한다.

[0602] 예를 들어, 기록장치(1100)의 무효화 데이터 저장부(1102)가 버전번호 「1」이 부가된 키 무효화 데이터를 보유하고 있는 경우, 배신국장치(1400)로부터 버전 번호 「2」가 부가된 키 무효화 데이터를 수신했다고 상정한 때, 기록장치(1100)의 제어부(1109)는 수신한 키 무효화 데이터에 부가된 버전번호 「2」와 무효화 데이터 저장부에 보유되어 있는 버전 번호 「1」을 비교한다. 수신한 키 무효화 데이터에 부가된 버전 번호 「2」가 더 새로운 것이므로, 제어부(1109)는, 수신한 키 무효화 데이터는 새로운 것으로 하여, 수신한 키 무효화 데이터와 버전번호 「2」를 무효화 데이터 저장부(1102)에 저장하도록 송수신부(1111)에 지시를 한다. 여기서, 버전 번호는 그 값이 클수록 새로운 것을 나타내고 있는 것으로 한다.

[0603] 또한, 여기서는 키 무효화 데이터의 신, 구의 비교에 버전 번호를 이용하는 경우에 대하여 설명을 하였으나, 이 방법에 한정되는 것은 아니다. 예를 들어, 버전 번호 대신, 키 무효화 데이터에는 그 발행일시가 부가되어 있고, 키 무효화 데이터의 발행일시를 이용하여 키 무효화 데이터의 신, 구를 비교하는 구성으로 해도 된다. 또, 여기서는, 배신국장치(1400)로부터 키 무효화 데이터를 입수하는 것으로 하였으나, 키 무효화 데이터의 취득방법은 이 구성에 한정되는 것은 아니다. 예를 들어, 키 무효화 데이터와 버전 번호가 기록된 기록매체가 배포되고, 기록장치(1100)는 이 기록매체에서 키 무효화 데이터와 버전 번호를 판독하는 것으로 해도 된다.

[0604] 다음에, 기록장치(1100)의 비교부(1108)는, 드라이브부(1110)를 거쳐서, 기록매체(1300)의 기록영역(1305)에 키 무효화 데이터 파일이 존재하는가 여부를 확인한다. 키 무효화 데이터 파일이 존재하지 않는다고 확인된 경우에는(스텝 S1502) 후술하는 스텝 S1505a로 진행한다.

[0605] 키 무효화 데이터 파일(310)이 존재하는 것으로 확인된 경우에는(스텝 S1502), 비교부(1108)는 존재하는 모든 키 무효화 데이터 파일의 관수 기록부에 기록되어 있는 버전 번호에 대하여 스텝 S1501에서 입수한 키 무효화 데이터에 부가된 버전 번호와 동일 내용의 것이 존재하는가 여부를 확인한다(스텝 S1503).

[0606] 스텝 S1503에서 상기 조건을 만족하는 버전 번호가 존재하지 않는 경우에는(스텝 S1504) 후술하는 스텝 S1505a

로 진행한다.

[0607] 스텝 S1504에서 상기 조건을 만족하는 버전 번호가 존재하는 경우에는(스텝 S1504), 제어부(1109)는 드라이브부(1110)를 거쳐서 상기 조건을 만족하는 버전 번호를 포함하는 키 무효화 데이터 파일(1310)의 식별자 기록부(1312)로부터 키 무효화 데이터 식별자 RID를 판독한다(스텝 S1505).

[0608] 키 계산부(1103)는, 디바이스 키 저장부(101)에서 디바이스 키를 판독하고, 무효화 데이터 저장부(1102)에서 키 무효화 데이터를 판독하며(스텝 S1506), 판독한 키 무효화 데이터를 판독한 디바이스 키로 복호함으로써 미디어 키 MK를 산출한다(스텝 S1507).

[0609] 다음에, 암호화부 1105는, 산출된 미디어 키를 이용하여, 콘텐츠 서버장치(1500)에서 수신한 콘텐츠 키 CK를 암호화하여 암호화 콘텐츠 키 ECK를 생성한다(스텝 S1508).

[0610] 인증자 생성부(1104)는, 기록매체(1300)의 고유번호 기록영역(1301)에서 매체 고유번호 MID를 판독하고(스텝 S1509), 키 계산부(1103)에 의해 산출된 미디어 키 MK와, 암호화부 1105에 의해 생성된 암호화 콘텐츠 키 ECK와, 판독된 매체 고유번호 MID를 결합한 값을 해시함수의 입력 값으로 한 때의 출력 값으로 하여 인증자 MAC를 생성한다(스텝 S1510). 또한, 여기서 사용하는 해시함수는 공지의 기술로 실현할 수 있다. 예를 들어, 해시함수로서 SHA-1을 사용하는 것으로 해도 된다. 또한, SHA-1에 한정되는 것은 아니다.

[0611] 다음에, 암호화부(1106)는 콘텐츠 서버장치(1500)에서 수신한 콘텐츠 키 CK를 이용하여 동일하게 수신한 콘텐츠 CNT를 암호화한다(스텝 S1511).

[0612] 기록장치(1100)는, 스텝 S1505에서 취득한, 또는 스텝 S1505a에서 할당된 키 무효화 데이터 식별자 RID와, 스텝 S1510에서 생성한 인증자 MAC와, 스텝 S1508에서 생성한 암호화 콘텐츠 키와, 스텝 S1511에서 생성한 암호화 콘텐츠를 포함하는 암호화 콘텐츠 파일을 기록매체(1300)의 기록영역(1305)에 기록하고(스텝 S1512), 처리를 종료한다.

[0613] 또, 기록매체(1300)에 키 무효화 데이터 파일(1310)이 존재하지 않는 것으로 확인된 경우(스텝 S1502), 및 스텝 S1503에서 조건을 만족하는 버전 번호가 존재하지 않는 경우에는(스텝 S1504), 할당부(1107)는, 스텝 S1501에서 입수한 키 무효화 데이터에 대하여, 기록매체(1300)의 기록영역(1305)에 기록되어 있는 모든 키 무효화 데이터 파일에 이미 할당된 키 무효화 데이터 식별자 RID와는 다른 값을 키 무효화 데이터 식별자로서 할당한다(스텝 S1505a).

[0614] 예를 들어, 기록매체(1300)에 키 무효화 데이터 파일이 전혀 존재하지 않는 경우에는, 할당부(1107)는 임의의 값, 예를 들어 「1」을 할당한다. 또, 도 14에 도시하는 예와 같이, 기록매체 1300a에 키 무효화 데이터 식별자 RID가 「1」 및 「2」인 키 무효화 데이터 파일 1 및 2가 존재하는 경우에는, 할당부(1107)는 「1」 및 「2」와는 다른 값인, 예를 들어 「3」을 할당한다.

[0615] 다음에, 기록장치(1100)의 드라이브부(1110)는, 스텝 S1501에서 입수한 키 무효화 데이터와, 그 키 무효화 데이터의 버전 번호와, 스텝 S1505a에서 할당된 키 무효화 데이터 식별자를 갖는 키 무효화 데이터 파일을 기록매체(1300)의 키 무효화 데이터 파일(1302)에 기록한다(스텝 S1505b). 이때, 키 무효화 데이터, 버전 번호 및 키 무효화 데이터 식별자 RID를 각각 키 무효화 데이터 파일(310)의 데이터 기록부(1313), 판수 기록부(1311) 및 식별자 기록부(1312)에 기록한다. 이어서, 스텝 S1506으로 제어를 옮기며, 이후, 전술한 스텝 S1506에서 스텝 S1512까지가 실행된다.

[0616] ⑵ 재생장치(1200)에 의한 재생동작

[0617] 재생장치(1200)에 의한 기록매체(1300)에 기록되어 있는 데이터의 재생동작에 대하여도 19 내지 도 20의 플로우 챠트를 이용하여 설명한다.

[0618] 재생장치(1200)의 지정 접수부(1207)는 재생하여야 할 콘텐츠의 지정을 접수한다(스텝 S1601).

[0619] 취득부(1208)는 기록매체(1300)의 기록영역(1305)으로부터 스텝 S1601에서 지정된 콘텐츠에 대응하는 암호화 콘텐츠 파일을 검색한다(스텝 S1602).

[0620] 또한, 지정접수부(1207)에서의 재생하여야 할 콘텐츠의 지정방법 및 지정된 콘텐츠에 대응하는 암호화 콘텐츠 파일을 검색하는 방법으로는, 예를 들어, 재생장치(1200)는, 기록매체(1300)의 기록영역(1305)에 기록되어 있는 모든 암호화 콘텐츠 파일의 속성을 나타내는 정보(예를 들어, 암호화 콘텐츠의 파일 명, 콘텐츠의 타이틀 명, 콘텐츠의 기록일시, 콘텐츠의 요약정보, 콘텐츠의 섬네일 화상(thumbnail image), 콘텐츠를 가리키는 아이콘

등)의 일람을 재생장치(1200)의 표시부(1217)에 표시하여, 이용자에게 그 일람 중에서 재생하고자 하는 콘텐츠를 선택하도록 함으로써, 재생하여야 할 콘텐츠의 지정을 접수한다. 또, 재생장치(1200)는, 지정된 콘텐츠의 속성정보로부터 지정된 콘텐츠가 저장된 암호화 콘텐츠 파일의 파일 명을 알아서, 기록매체(1300)의 기록영역(1305)에서 해당하는 파일 명의 암호화 콘텐츠를 찾는다.

[0621] 또한, 암호화 콘텐츠 파일을 찾는 방법으로는 상술한 방법에 한정되는 것은 아니며, 다른 방법을 이용해도 된다.

[0622] 취득부(1208)는 스텝 S1602에서 찾아낸 암호화 콘텐츠 파일(1320)의 식별자 기록부(1321)에서 무효화 데이터 식별자를 판독한다(스텝 S1603).

[0623] 검색부(1209)는, 기록매체(1300)의 기록영역(1305)에서, 스텝 S1603에서 판독한 키 무효화 데이터 식별자 RID와 같은 값이 식별자 기록부(1312)에 기록되어 있는 키 무효화 데이터 파일(310)을 찾는다(스텝 S1604). 다음에, 검색부(1209)는 스텝 S1604에서 찾아낸 키 무효화 데이터 파일(1310)을 취득한다(스텝 S1605).

[0624] 키 계산부(1202)는, 디바이스 키 저장부(1201)에서 디바이스 키를 판독하고, 검색부(1209)에서 키 무효화 데이터를 취득한다(스텝 S1606).

[0625] 키 계산부(1202)는 스텝 S1606에서 취득한 키 무효화 데이터를 디바이스 키를 이용하여 복호 함으로써 복호 미디어 키 y를 산출한다(스텝 S1607).

[0626] 인증자 생성부(1203)는, 기록매체(1300)의 고유번호 기록영역(1301)에서 매체 고유번호 MID를 판독하고(스텝 S1608), 스텝 S1602에서 찾아낸 암호화 콘텐츠 파일(1302)의 키 기록부(1323)에서 암호화 콘텐츠 키 ECK를 판독하며(스텝 S1609), 스텝 S1607에서 취득한 복호 미디어 키 y와, 스텝 S1609에서 판독한 암호화 콘텐츠 키 ECK와, 스텝 S1608에서 취득한 매체고유번호 MID를 결합한 값을 해시함수의 입력 값으로 한 때의 출력 값으로 하여 복호인증자 DMAC를 생성한다(스텝 S1610). 여기서 사용하는 해시함수는 기록장치(1100)에서 사용한 것과 동일한 해시함수 SHA-1이다.

[0627] 비교부(1206)는, 스텝 S1602에서 찾아낸 암호화 콘텐츠 파일(1320)의 인증자 기록부(322)에서 인증자 MAC를 판독하고(스텝 S1611), 스텝 S1610에서 산출된 복호 인증자 DMAC와 스텝 S1611에서 판독한 인증자 MAC가 일치하는가 여부를 확인한다(스텝 S1612).

[0628] 복호인증자 DMAC와 인증자 MAC가 일치하지 않으면(스텝 S1613) 재생동작은 종료한다.

[0629] 복호인증자 DMAC와 인증자 MAC가 일치하면(스텝 S1613), 복호부 1204는, 암호화 콘텐츠 키를 스텝 S1607에서 산출한 복호 미디어 키 y로 복호 하여, 복호 콘텐츠 키 DCK를 취득한다(스텝 S1614).

[0630] 복호부 1205는, 스텝 S1602에서 찾아낸 암호화 콘텐츠파일(1320)의 콘텐츠 기록부(1324)에서 암호화 콘텐츠를 판독하고(스텝 S1615), 스텝 S1615에서 판독한 암호화 콘텐츠를 스텝 S1614에서 복호 한 복호 콘텐츠 키 DCK를 이용하여 복호 하여 복호 콘텐츠로 하며, 재생부(1214)는 복호 콘텐츠를 재생한다(스텝 S1616).

[0631] 2. 9 기타 변형 예

[0632] 이하에 제시하는 것과 같이 구성해도 된다.

[0633] (1) 제 2 실시 예에서는, 키 무효화 데이터의 세대를 나타내는 버전 번호 및 키 무효화 데이터를 식별하는 키 무효화 데이터 식별자를 각각 키 무효화 데이터 파일에서의 판수 기록부 및 식별자 기록부에 기록하는 것으로 하였으나, 이 방법에 한정되지는 않는다.

[0634] 예를 들어, 키 무효화 데이터 파일을 식별하는 파일 명의 일부에, 키 무효화 데이터의 버전 번호와 키 무효화 데이터 식별자의 양자, 또는 적어도 하나를 포함하는 구성으로 해도 된다. 구체적으로는, 키 무효화 데이터 파일의 파일 명을 "KRD_n_m"으로 해도 된다. 여기서, n은 버전 번호이고, m은 키 무효화 데이터 식별자이다. 이 경우, 예를 들어, "KRD_0001_0002"라고 하는 파일 명에 의해 식별되는 키 무효화 데이터 파일의 버전 번호는 「1」이고 키 무효화 데이터 식별자 RID는 「2」이다.

[0635] 이와 같이, 파일 명에 버전 번호나 키 무효화 데이터 식별자의 양자 또는 적어도 하나를 포함함으로써, 재생장치는, 파일 명을 보면 키 무효화 데이터 파일의 버전 번호나 키 무효화 데이터 식별자 RID를 알 수 있어서, 재생장치에서의 파일 검색 시의 처리가 경감될 수 있다고 하는 이점이 있다.

[0636] (2) 제 2 실시 예에서는, 키 무효화 데이터 식별자를 암호화 콘텐츠 파일에서의 식별자 기록부에 기록하는 것으

로 하였으나, 이 방법에 한정되는 것은 아니다.

[0637] 예를 들어, 암호화 콘텐츠 파일을 식별하는 파일 명의 일부에 키 무효화 데이터 식별자를 포함하는 구성으로 해도 된다. 구체적으로는, 암호화 콘텐츠를 식 별하는 파일 명을 ECNT_m으로 해도 된다. 여기서 m은 키 무효화 데이터 식별자이다. 예를 들어, ECNT_0002라고 하는 파일 명의 암호화 콘텐츠 파일의 키 무효화 데이터 식별자 RID는 「2」이다.

[0638] 이와 같이 파일 명에 키 무효화 데이터 식별자를 포함함으로써, 재생장치에서 파일 명을 보면 키 무효화 데이터 식별자를 알 수 있고, 재생장치에서의 키 무호화 데이터 식별자의 취득 시의 처리가 경감될 수 있다는 이점이 있다.

[0639] (3) 제 2 실시 예에서는, 키 무효화 데이터를 키 무효화 데이터 식별자와 관련시키기 위해, 또 암호화 콘텐츠를 상기 키 무효화 데이터 식별자 RID와 관련시키기 위해, 키 무효화 데이터 파일(1310)에 판수 기록부(1311)와 식별자 기록부(1312)를 설치하여, 각각 버전 번호와 키 무효화 데이터 식별자를 기록하고, 암호화 콘텐츠 파일(1320)에 식별자 기록부(1321)를 설치하여, 키 무효화 데이터 식별자를 기록하는 구성으로 하고 있으나, 이 구성에 한정되는 것은 아니다.

[0640] 예를 들어, 상기 기록장치는, 기록매체(1300) 상에, 1개 이상의 키 무효화 데이터 파일과, 1개 이상의 암호화 콘텐츠 파일과, 1개의 키 무효화 데이터 관리파일을 기록하는 것으로 해도 된다. 이 키 무효화 데이터 관리파일에는, 키 무효화 데이터 파일별로, 그 키 무효화 데이터의 버전 번호와, 키 무효화 데이터 식별자와, 기록매체 상에서 당해 키 무효화 데이터 파일을 일의로 특정하기 위한 정보(예를 들어, 키 무효화 데이터 파일이 기록되어 있는 디렉터리 명이나 파일 명 등)와, 당해 키 무효화 데이터 파일을 이용하여 암호화한 암호화 콘텐츠 파일을 기록매체 상에서 일의로 특정하기 위한 정보(예를 들어, 암호화 콘텐츠 파일이 기록되어 있는 디렉터리 명이나 파일 명 등)가 포함된다. 재생장치는 이 키 무효화 데이터 관리파일에 기록되어 있는 상기 정보에 의거하여 재생이 지정된 암호화 콘텐츠에 관련하는 키 무효화 데이터 파일을 취득한다.

[0641] 또, 본 실시 예의 구성과 키 무효화 데이터 관리파일을 설치하는 구성을 조합시킨 구성으로 해도 된다.

[0642] (4) 제 2 실시 예에서는, 키 무효화 데이터의 버전 번호와 키 무효화 데이터 양방이 존재하는 구성으로 하였으나, 이 구성에 한정되지는 않으며, 키 무효화 데이터 식별자만이 존재하는 구성이라도 좋다.

[0643] (5) 제 2 실시 예에서는, 키 무효화 기술로서, 기록매체의 재기입 가능영역에 기록하는 키 무효화 데이터를, 무효화 되어 있지 않은 장치가 보유하는 디바이스 키를 이용하여 미디어 키를 암호화한 것과, 무효화 된 장치기 보유하는 디바이스 키를 이용하여 미디어 키와는 관계가 없는 값(예를 들어 「0」)을 암호화한 것으로 하고, 기록매체의 재기입 가능영역에 기록하는 암호화 콘텐츠를 상기 미디어 키에 의거하여 암호화한 것으로 하는 경우에 대하여 설명하였으나, 이 구성에 한정되는 것은 아니다.

[0644] 예를 들어, 기록매체의 재기입 가능영역에 기록하는 키 무효화 데이터와 암호화 콘텐츠로서, 무효화 되어 있지 않은 장치에 있어서는 키 무효화 데이터에 의거하여 암호화 콘텐츠를 복호 재생할 수 있고, 무효화 된 장치에 있어서는 키 무효화 데이터에 의거하여 암호화 콘텐츠를 복호 재생할 수 없다고 하는 조전을 만족하는 것이라면 어떤 구성이라도 좋다.

[0645] (6) 제 2 실시 예에서는, 미디어 바인드기술로, 기록장치(1100)에서 매체 고유번호 MID를 이용해서 인증자 MAC를 생성하고, 재생장치(1200)에서 인증자 MAC의 비교를 행하는 것으로 하고 있으나, 이 구성에 한정되는 것은 아니다.

[0646] 예를 들어, 기록장치(1100)에서 매체 고유번호 MID를 이용하여 콘텐츠를 암호화하여 기록매체에 기록하고, 재생장치(1200)에서 매체 고유번호 MID를 이용하여 암호화된 콘텐츠를 복호 하는 구성으로 해도 된다.

[0647] (7) 제 2 실시 예에서는, 키 무효화 데이터 식별자를 할당할 때, 기록장치(1100)에 이미 기록되어 있는 키 무효화 데이터에 할당되어 있지 않은 값을 키 무효화 ID로서 할당하는 구성으로 하고 있으나, 이 구성에 한정되는 것은 아니다.

[0648] 예를 들어, 기록장치(1100)는, 이미 할당된 키 무효화 데이터 식별자를 매체 고유번호 MID와 함께 기억해 두고, 기록장치(1100)에 기억하고 있는 상기 정보에 의거하여 키 무효화 데이터 식별자를 할당하는 구성으로 해도 된다.

[0649] 2. 10. 요약

[0650] 이상의 설명으로부터 명확한 바와 같이, 본 발명에 관한 기록장치는, 특정장치가 보유하는 키를 무효화하기 위한 키 무효화 데이터를 저장하는 키 무효화 데이터 저장수단과, 상기 키 무효화 데이터에 의거하여 상기 콘텐츠를 암호화하는 콘텐츠 암호화수단과, 상기 키 무효화 데이터에 대하여, 상기 기록매체에서 상기 키 무효화 데이터를 일의로 식별하기 위한 키 무효화 데이터 식별정보를 할당하는 키 무효화 데이터 식별정보 할당수단과, 상기 기록매체에 상기 키 무효화 데이터를 상기 키 무효화 데이터 식별정보와 관련 지워서 기록하는 키 무효화 데이터 기록수단과, 상기 암호화 콘텐츠를 상기 키 무효화 데이터 식별정보와 관련 지워서 기록하는 암호화 콘텐츠 기록수단을 구비한다.

[0651] 또, 본 발명의 기록장치에서의 상기 키 무효화 데이터 식별정보 할당수단은 상기 기록매체에 기록되어 있는 키 무효화 데이터에 이미 할당된 키 무효화 데이터 식별정보와는 다른 값을 키 무효화 데이터 식별정보로 할당한다.

[0652] 또, 본 발명의 기록장치에서의 상기 키 무효화 데이터 식별정보 할당수단은, 상기 기록매체에 기록되어 있는 키 무효화 데이터와 상기 키 무효화 데이터 저장수단에 저장되어 있는 키 무효화 데이터의 신, 구를 비교하여, 상기 키 무효화 데이터 저장수단에 저장되어 있는 키 무효화 데이터가 새로운 경우에만 키 무효화 데이터 식별정보의 할당을 행하는 것을 특징으로 한다.

[0653] 또, 본 발명의 기록장치에서의 상기 키 무효화 데이터 식별정보 할당수단은, 상기 기록매체에 기록되어 있는 키 무효화 데이터와, 상기 키 무효화 데이터 저장수단에 저장되어 있는 키 무효화 데이터의 신, 구를 비교하여, 각 키 무효화 데이터가 생성된 일시에 관련한 정보, 혹은 각 키 무효화 데이터가 생성된 순서에 관련되는 정보에 의거하여 할당을 행한다.

[0654] 또, 본 발명에 관한 재생장치는, 상기 기록매체에서, 암호화 콘텐츠와, 상기 암호화 콘텐츠와 관련지어서 기록된 키 무효화 데이터 식별정보를 판독하는 암호화 콘텐츠 판독수단과, 상기 기록매체에서, 상기 암호화 콘텐츠 판독수단에 의해 판독한 키 무효화 데이터 식별정보와 동일한 키 무효화 데이터 식별정보가 관련지어져서 기록되어 있는 키 무효화 데이터를 판독하는 키 무효화 데이터 판독수단과, 상기 키 무효화 데이터 판독수단에 의해 판독한 키 무효화 데이터에 의거하여 암호화 콘텐츠 판독수단에서 판독한 상기 암호화 콘텐츠를 복호 하는 콘텐츠 복호수단을 구비한다.

[0655] 또, 본 발명에서의 기록매체는, 키 무효화 데이터를, 상기 기록매체에서 이 키 무효화 데이터를 일의로 식별하기 위한 키 무효화 데이터 식별정보와 관련 지워서 기록하는 키 무효화 데이터 저장수단과, 상기 키 무효화 데이터에 의거하여 암호화된 암호화 콘텐츠를 상기 무효화 데이터 식별정보와 관련 지워서 기록하는 암호화 콘텐츠 저장수단을 구비한다.

[0656] 또, 본 발명에서의 기록매체는 키 무효화 데이터의 신, 구를 나타내는 정보를 키 무효화 데이터와 관련 지워서 기록한다.

[0657] 또, 본 발명의 저작권 보호시스템은, 기록장치와, 기록매체와, 재생장치로 이루어지며, 상기 기록장치는, 특정장치가 보유하는 키를 무효화하기 위한 키 무효화 데이터를 저장하는 키 무효화 데이터 저장수단과, 상기 키 무효화 데이터에 의거하여 상기 콘텐츠를 암호화하는 콘텐츠 암호화수단과, 상기 키 무효화 데이터에 대하여, 상기 기록매체에서 상기 키 무효화 데이터를 일의로 식별하기 위한 키 무효화 데이터 식별정보를 할당하는 키 무효화 데이터 식별정보 할당수단과, 상기 기록매체에 상기 키 무효화 데이터를 상기 키 무효화 데이터 식별정보와 관련 지워서 기록하는 키 무효화 데이터 기록수단과, 상기 암호화 콘텐츠를 상기 키 무효화 데이터 식별정보와 관련 지워서 기록하는 암호화 콘텐츠 기록수단을 구비하고, 상기 기록매체는, 상기 키 무효화 데이터를 상기 키 무효화 데이터 식별정보와 관련 지워서 기록하는 키 무효화 데이터 저장수단과, 상기 암호화 콘텐츠를 상기 무효화 데이터 식별정보와 관련 지워서 기록하는 암호화 콘텐츠 저장수단을 구비하며, 상기 재생장치는, 상기 기록매체에서, 암호화 콘텐츠와, 상기 암호화 콘텐츠와 관련지어서 기록된 키 무효화 데이터 식별정보를 판독하는 암호화 콘텐츠 판독수단과, 상기 암호화 콘텐츠 판독수단에 의해 판독한 키 무효화 데이터 식별정보와 동일한 키 무효화 데이터 식별정보가 관련지어져서 기록되어 있는 키 무효화 데이터를 판독하는 키 무효화 데이터 판독수단과, 상기 키 무효화 데이터 판독수단에 의해 판독한 키 무효화 데이터에 의거하여 암호화 콘텐츠 판독수단에서 판독한 상기 암호화 콘텐츠를 복호 하는 콘텐츠 복호수단을 구비한다.

[0658] 이와 같이, 제 2 실시 예에 관한 기록장치, 기록매체, 재생장치, 및 저작권 보호시스템에 있어서는, 기록매체에 기록하는 키 무효화 데이터에 대하여, 기록매체에서 그 키 무효화 데이터를 일의로 식별하기 위한 키 무효화 데이터 ID를 할당하고, 이 키 무효화 데이터 ID를 기록매체에 기록하는 키 무효화 데이터와 관련지어서 키 무효화

데이터 파일로 하여 기록함과 동시에, 이 키 무효화 데이터 ID를 키 무효화 데이터를 사용하여 암호화한 콘텐츠와 관련지어서, 암호화 콘텐츠 파일로 하여 기록함으로써, 재생장치에서 당해 암호화 콘텐츠를 복호 재생하는 경우에, 기록매체에 복수의 암호화 콘텐츠 파일과 복수의 키 무효화 데이터 파일이 기록되어 있는 경우에도, 당해 암호화 콘텐츠 파일에 포함되는 키 무효화 데이터 ID와 동일한 키 무효화 데이터 ID를 포함하는 키 무효화 데이터 파일을 검색 취득할 수 있고, 암호화 콘텐츠 파일을 취득한 키 무효화 데이터 파일을 이용하여 복호 재생할 수 있게 된다.

[0659] 3. 기타 변형 예

[0660] 또한, 본 발명을 상기 각 실시 예에 의하여 설명하였으나, 본 발명은 상기 실시 예에 한정되는 것은 물론 아니다. 이하와 같은 경우도 본 발명에 포함된다.

[0661] (1) 각 실시 예에서 콘텐츠는 영상데이터와 음성데이터가 고 효율로 압축 부호화된 데이터로 하고 있으나, 이에 한정되는 것은 아니다. 예를 들어, 콘텐츠는, 소설, 정지화상, 음성 등이 디지털화된 컴퓨터 데이터로 해도 된다.

[0662] 또, 예를 들어, 콘텐츠는 컴퓨터를 구성하는 마이크로 프로세서의 동작을 제어하는 복수의 명령으로 구성되는 컴퓨터 프로그램이라도 된다. 또, 표 계산 소프트웨어에 의해 생성되는 표 데이터라도 좋고, 데이터베이스 소프트웨어에 의해 생성되는 데이터베이스로 해도 된다.

[0663] (2) 상기 각 장치는, 구체적으로는, 마이크로 프로세서, ROM, RAM, 하드디스크 유닛, 디스플레이 유닛, 키보드, 마우스 등으로 구성되는 컴퓨터시스템이다. 상기 RAM 도는 하드디스크 유닛에는 컴퓨터 프로그램이 기억되어 있다. 상기 마이크로 프로세서가 상기 컴퓨터 프로그램에 따라서 동작함으로써, 각 장치는 그 기능을 달성한다.

[0664] (3) 본 발명은 상기에 제시한 방법이라도 된다. 또, 이들 방법을 컴퓨터에 의해 실현하는 컴퓨터 프로그램이라도 되고, 상기 컴퓨터 프로그램으로 이루어지는 디지털 신호라도 좋다.

[0665] 또, 본 발명은 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 컴퓨터 판독 가능한 기록매체, 예를 들어, 플렉시블 디스크, 하드디스크, CD-ROM, MO, DVD, DVD-ROM, DVD-RAM, BD(Blu-ray Disc), 반도체 메모리 등에 기억한 것이라도 된다. 또, 이들 기록매체에 기록되어 있는 상기 컴퓨터 프로그램 또는 상기 디지털 신호라도 된다.

[0666] 또, 본 발명은, 상기 컴퓨터 프로그램 또는 상기 디지털 신호를 전기통신회선, 무선 또는 유선통신회선, 인터넷을 대표로 하는 네트워크, 데이터방송 등을 경유하여 전송하는 것이라도 된다.

[0667] 또, 본 발명은, 마이크로 프로세서와 메모리를 구비한 컴퓨터 시스템으로서, 상기 메모리는 상기 컴퓨터 프로그램을 기억하고 있고, 상기 마이크로 프로세서는 상기 컴퓨터 프로그램에 따라서 동작하는 것으로 해도 된다.

[0668] 또, 상기 프로그램 또는 상기 디지털 신호를 상기 기록매체에 기록하여 이송하는 것에 의해, 또는 상기 프로그램 또는 상기 디지털 신호를 상기 네트워크 등을 경유하여 이송함으로써, 독립한 다른 컴퓨터 시스템에 의해 실시하는 것으로 해도 된다.

[0669] (4) 상기 각 실시 예 및 상기 각 변형 예를 각각 조합시키는 것으로 해도 된다.

산업상 이용 가능성

[0670] 본 발명을 구성하는 각 장치 및 기록매체는, 콘텐츠를 제작하고 배급하는 콘텐츠 배급산업에서, 경영적으로, 또 계속적 및 반복적으로 사용할 수 있다. 또, 본 발명을 구성하는 각 장치 및 기록매체는 전기기기 제조산업에서, 경영적으로, 또 계속적 및 반복적으로 제조하거나 판매할 수 있다.

도면의 간단한 설명

[0038] 도 1은 콘텐츠 공급시스템(10)의 구성을 나타내는 구성도이다.

[0039] 도 2는 기록장치(100)의 구성을 나타내는 블록도이다.

[0040] 도 3은 기록매체(120)에 기록되어 있는 데이터의 구조를 나타내는 데이터 구조도이다.

[0041] 도 4는 재생장치(200)의 구성을 나타내는 블록도이다.

[0042] 도 5는 기록장치(100)에 의한 기록매체(120)에 데이터의 기입 동작을 나타내는 플로우차트이다.

[0043] 도 6은 재생장치(200)에 의한 기록매체(120)에 기록되어 있는 데이터의 재생동작을 나타내는 플로우차트이다.

도 7에 계속.

[0044] 도 7은 재생장치(200)에 의한 기록매체(120)에 기록되어 있는 데이터의 재생동작을 나타내는 플로우차트이다. 도 6에서 계속.

[0045] 도 8은 제 1 실시 예의 변형 예에서 n매의 기록매체에 기록되어 있는 데이터 구조를 나타내는 데이터 구조도이다.

[0046] 도 9는 제 1 실시 예의 변형 예에서 기록매체에 기록되어 있는 데이터 구조를 나타내는 데이터 구조도이다.

[0047] 도 10은 콘텐츠 공급시스템(20)의 구성을 나타내는 구성도이다.

[0048] 도 11은 기록장치(1100)의 구성을 나타내는 블록도이다.

[0049] 도 12는 기록매체(1300)에 기록되어 있는 데이터의 구조를 나타내는 데이터 구조도이다.

[0050] 도 13은 재생장치(1200)의 구성을 나타내는 블록도이다.

[0051] 도 14는 기록매체(1300a)에 기록되어 있는 데이터의 구조를 나타내는 데이터 구조도이다.

[0052] 도 15는 기록매체(1300b)에 기록되어 있는 데이터의 구조를 나타내는 데이터 구조도이다.

[0053] 도 16은 기록장치(1100)에 의한 기록매체(1300)에 데이터의 기입 동작을 나타내는 플로우차트이다. 도 17에 계속.

[0054] 도 17은 기록장치(1100)에 의한 기록매체(1300)에 데이터의 기입 동작을 나타내는 플로우차트이다. 도 18에 계속.

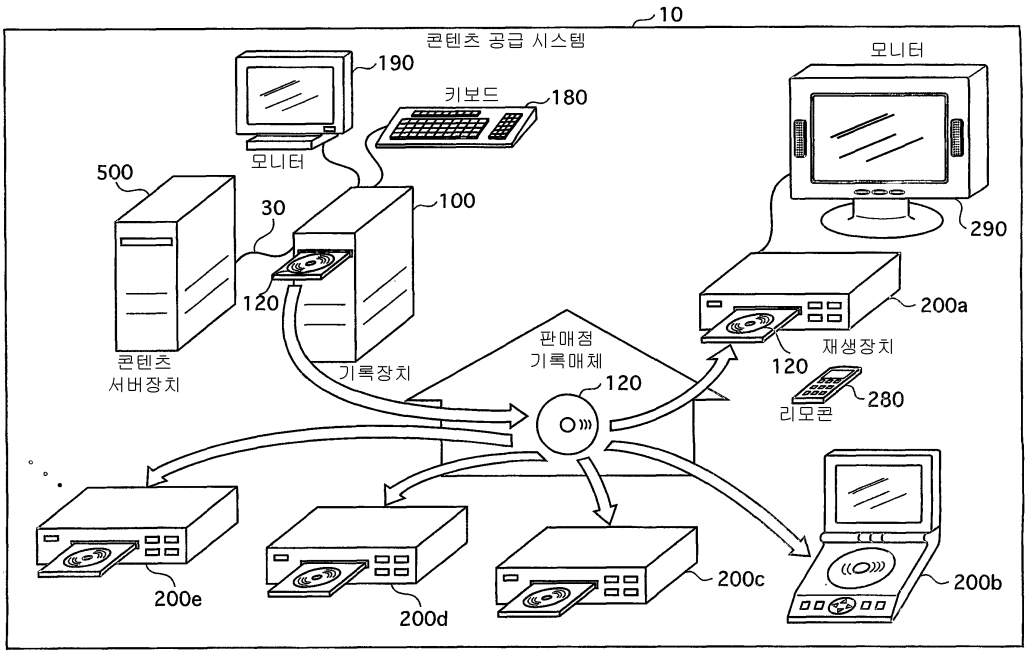
[0055] 도 18은 기록장치(1100)에 의한 기록매체(1300)에 데이터의 기입 동작을 나타내는 플로우차트이다. 도 17에서 계속.

[0056] 도 19는 재생장치(1200)에 의한 기록매체(1300)에 기록되어 있는 데이터의 재생 동작을 나타내는 플로우차트이다. 도 20에 계속.

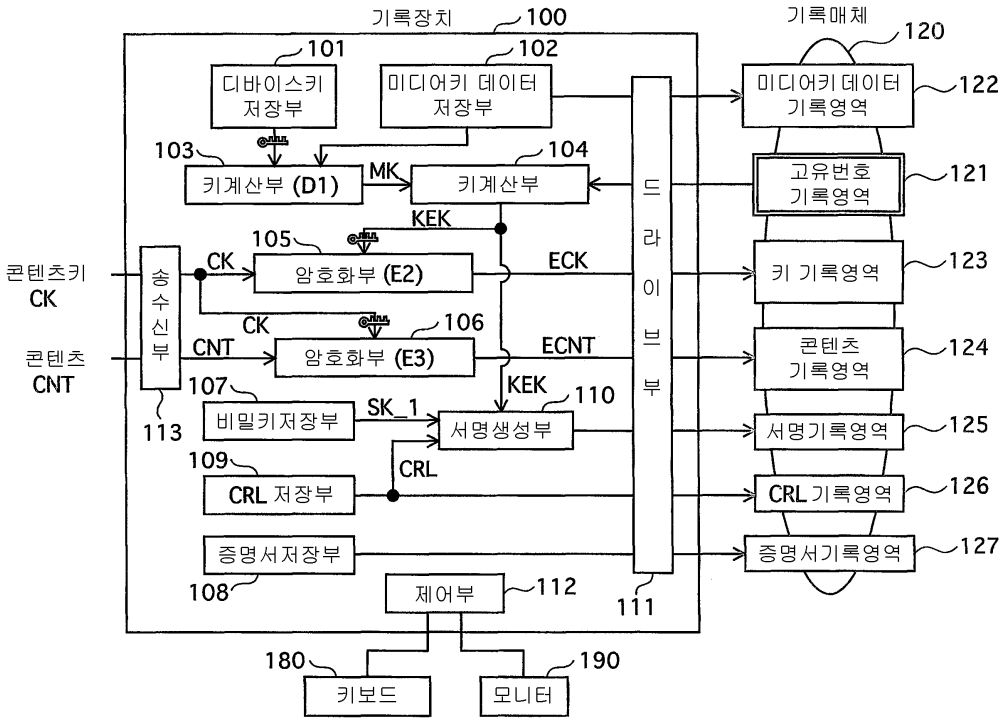
[0057] 도 20은 재생장치(1200)에 의한 기록매체(1300)에 기록되어 있는 데이터의 재생 동작을 나타내는 플로우차트이다. 도 19에서 계속.

도면

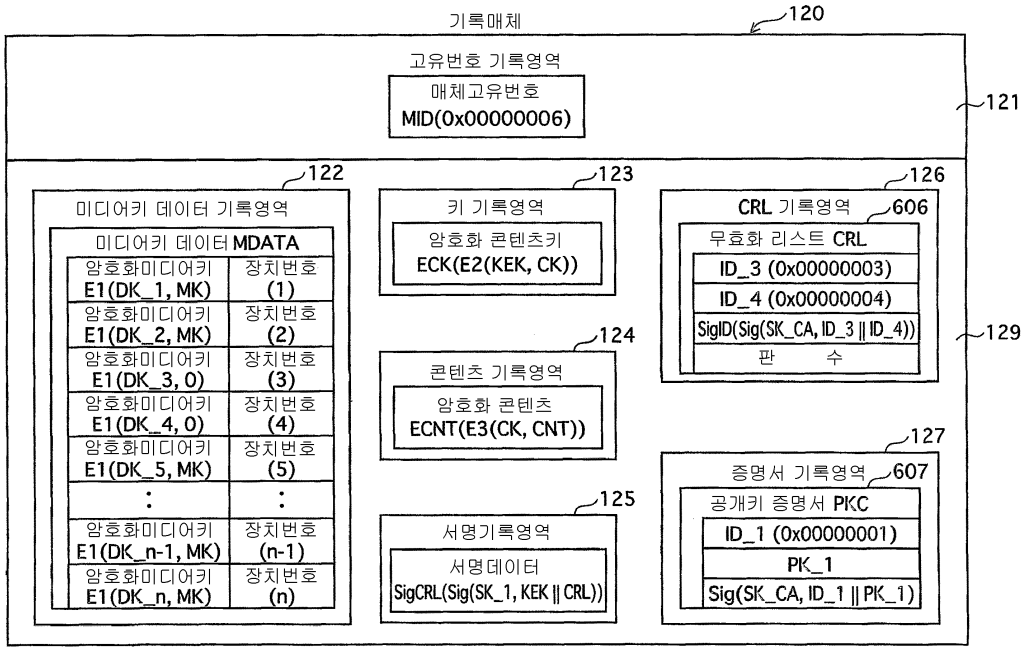
도면1



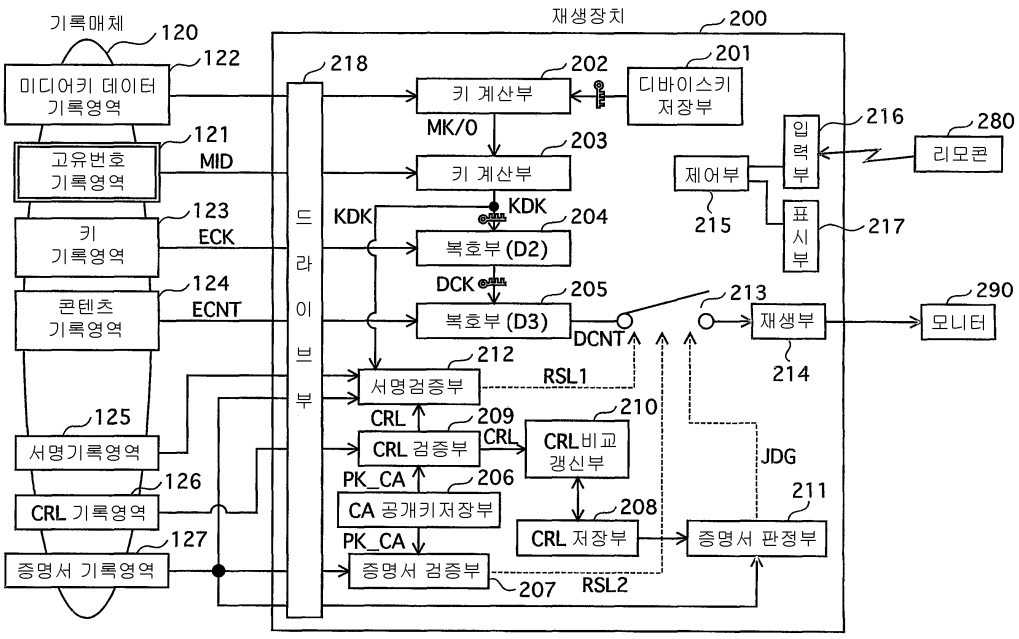
도면2


기록장치
100
기록매체
120
101
디바이스키 저장부
102
미디어키 데이터 저장부
미디어키 데이터 기록영역
122
103
키계산부 (D1)
MK
104
키계산부
고유번호 기록영역
121
KEK
105
콘텐츠키 CK
송수신부
CK
암호화부 (E2)
ECK
키 기록영역
123
CK
106
콘텐츠 CNT
CNT
암호화부 (E3)
ECNT
콘텐츠 기록영역
124
KEK
107
110
113
비밀키저장부
SK_1
서명생성부
서명기록영역
125
109
CRL
CRL 저장부
CRL 기록영역
126
증명서저장부
증명서기록영역
127
108
제어부
112
111
드라이브부
180
190
키보드
모니터

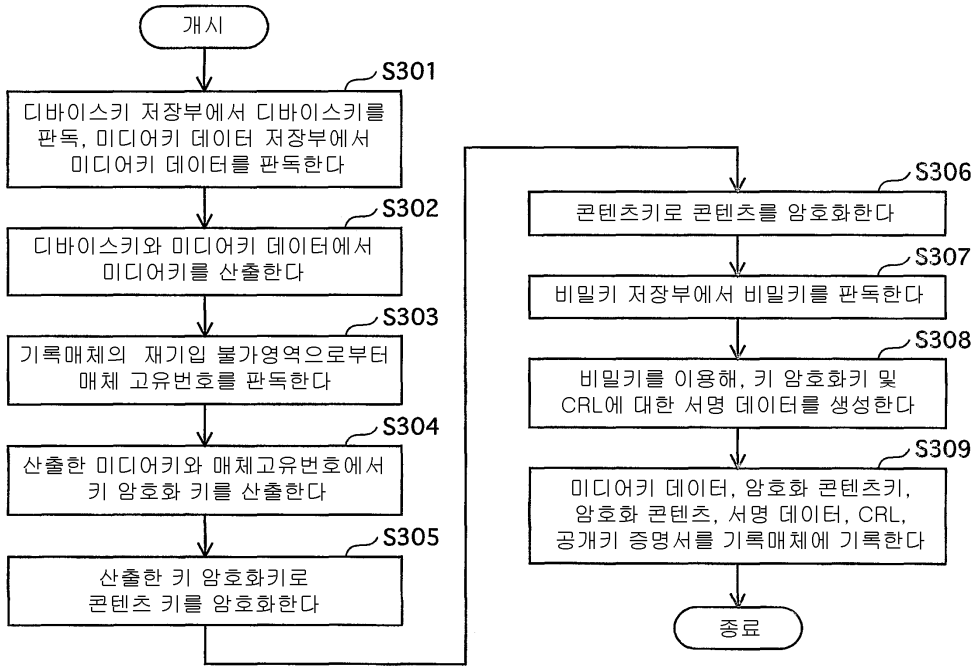
도면3


기록매체
120
고유번호 기록영역
매체고유번호
MID(0x00000006)
121
122
미디어키 데이터 기록영역
미디어키 데이터 MDATA
암호화미디어키 E1(DK_1, MK) 장치번호 (1)
암호화미디어키 E1(DK_2, MK) 장치번호 (2)
암호화미디어키 E1(DK_3, 0) 장치번호 (3)
암호화미디어키 E1(DK_4, 0) 장치번호 (4)
암호화미디어키 E1(DK_5, MK) 장치번호 (5)
암호화미디어키 E1(DK_n-1, MK) 장치번호 (n-1)
암호화미디어키 E1(DK_n, MK) 장치번호 (n)
123
키 기록영역
암호화 콘텐츠키
ECK(E2(KEK, CK))
124
콘텐츠 기록영역
암호화 콘텐츠
ECNT(E3(CK, CNT))
125
서명기록영역
서명데이터
SigCRL(Sig(SK_1, KEK || CRL))
126
CRL 기록영역
606
무효화 리스트 CRL
ID_3 (0x00000003)
ID_4 (0x00000004)
SigID(Sig(SK_CA, ID_3 || ID_4))
판 수
129
127
증명서 기록영역
607
공개키 증명서 PKC
ID_1 (0x00000001)
PK_1
Sig(SK_CA, ID_1 || PK_1)

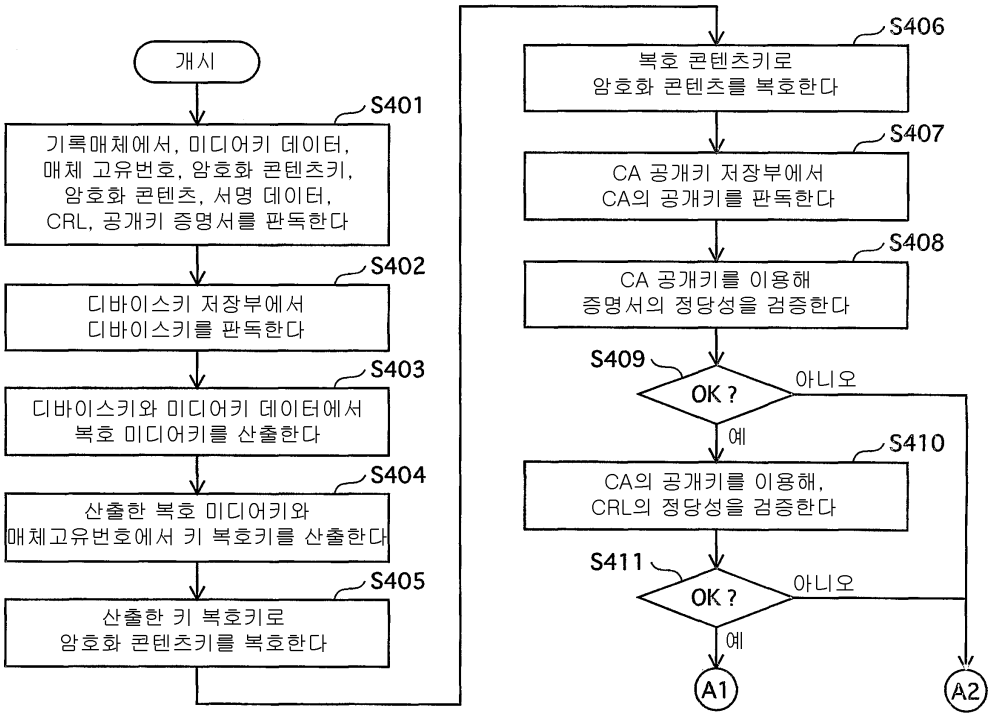
도면4


기록매체
120
재생장치
200
122
미디어키 데이터 기록영역
218
202
키 계산부
201
디바이스키 저장부
121
고유번호 기록영역
MID
MK/0
203
키 계산부
216
입력부
280
리모콘
123
키 기록영역
ECK
KDK
KDK
204
복호부 (D2)
제어부
215
표시부
217
124
콘텐츠 기록영역
ECNT
DCK
205
복호부 (D3)
213
재생부
290
모니터
DCNT
214
212
서명검증부
RSL1
125
서명기록영역
CRL
209
CRL 검증부
CRL
210
CRL비교 갱신부
JDG
126
CRL 기록영역
PK_CA
206
CA 공개키저장부
211
208
CRL 저장부
증명서 판정부
127
증명서 기록영역
PK_CA
증명서 검증부
207
RSL2
드라이브부

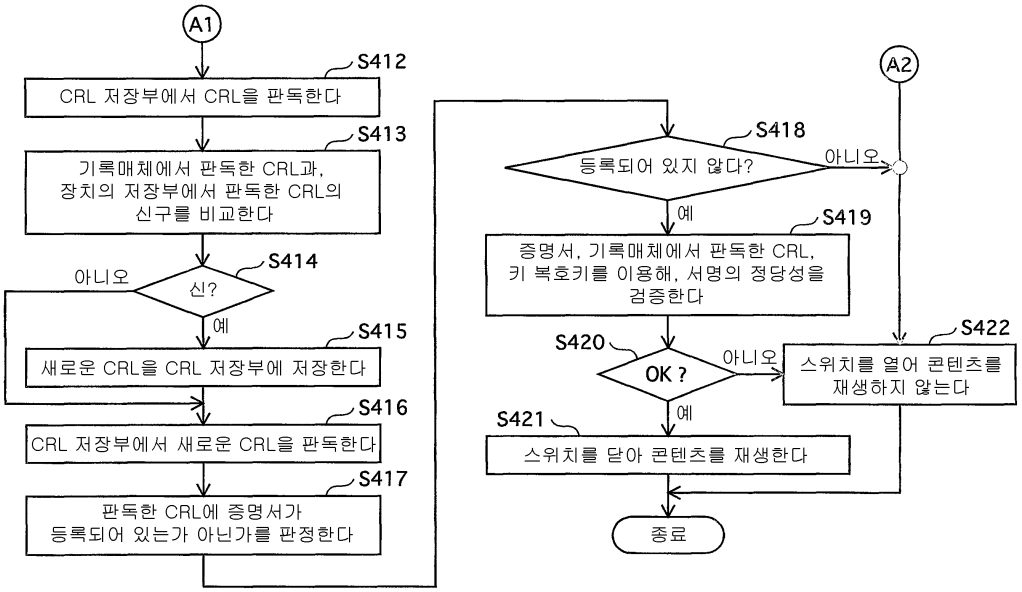
도면5


개시
S301
디바이스키 저장부에서 디바이스키를 판독, 미디어키 데이터 저장부에서 미디어키 데이터를 판독한다
S302
디바이스키와 미디어키 데이터에서 미디어키를 산출한다
S303
기록매체의 재기입 불가영역으로부터 매체 고유번호를 판독한다
S304
산출한 미디어키와 매체고유번호에서 키 암호화 키를 산출한다
S305
산출한 키 암호화키로 콘텐츠 키를 암호화한다
S306
콘텐츠키로 콘텐츠를 암호화한다
S307
비밀키 저장부에서 비밀키를 판독한다
S308
비밀키를 이용해, 키 암호화키 및 CRL에 대한 서명 데이터를 생성한다
S309
미디어키 데이터, 암호화 콘텐츠키, 암호화 콘텐츠, 서명 데이터, CRL, 공개키 증명서를 기록매체에 기록한다
종료

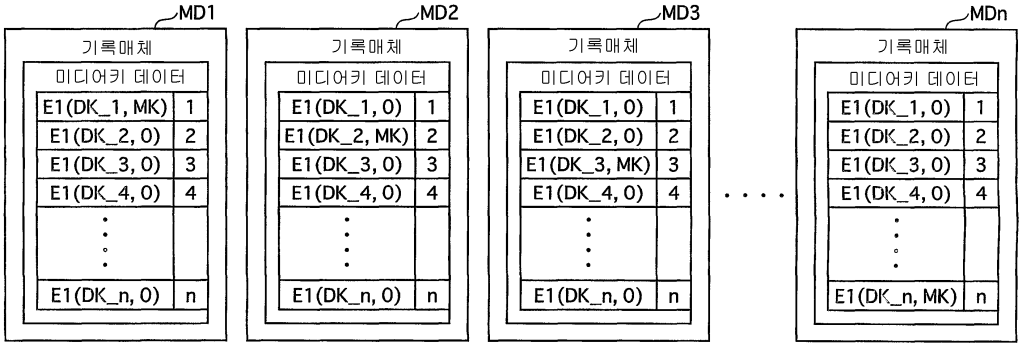
도면6


개시
S401
기록매체에서, 미디어키 데이터, 매체 고유번호, 암호화 콘텐츠키, 암호화 콘텐츠, 서명 데이터, CRL, 공개키 증명서를 판독한다
S402
디바이스키 저장부에서 디바이스키를 판독한다
S403
디바이스키와 미디어키 데이터에서 복호 미디어키를 산출한다
S404
산출한 복호 미디어키와 매체고유번호에서 키 복호키를 산출한다
S405
산출한 키 복호키로 암호화 콘텐츠키를 복호한다
S406
복호 콘텐츠키로 암호화 콘텐츠를 복호한다
S407
CA 공개키 저장부에서 CA의 공개키를 판독한다
S408
CA 공개키를 이용해 증명서의 정당성을 검증한다
S409
OK ?
아니오
예
S410
CA의 공개키를 이용해, CRL의 정당성을 검증한다
S411
OK ?
아니오
예
A1
A2

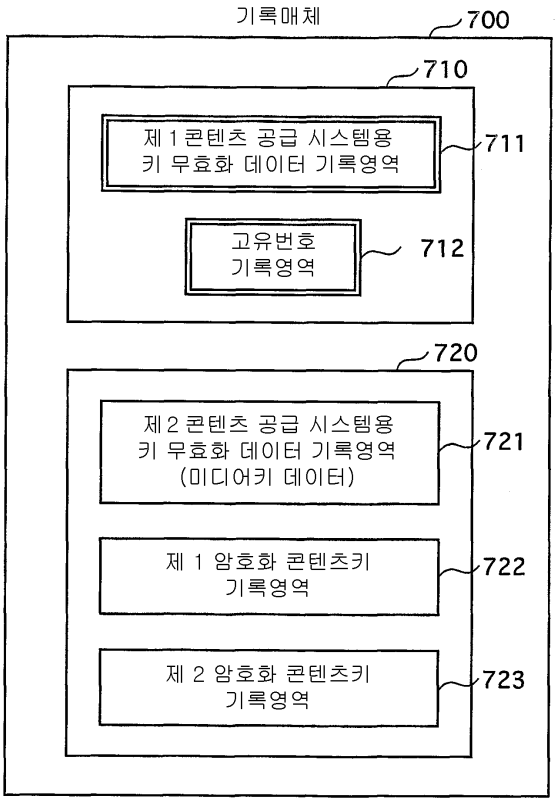
도면7


A1
S412
CRL 저장부에서 CRL을 판독한다
S413
기록매체에서 판독한 CRL과, 장치의 저장부에서 판독한 CRL의 신구를 비교한다
S414
아니오
신?
예
S415
새로운 CRL을 CRL 저장부에 저장한다
S416
CRL 저장부에서 새로운 CRL을 판독한다
S417
판독한 CRL에 증명서가 등록되어 있는가 아닌가를 판정한다
A2
S418
등록되어 있지 않다?
아니오
예
S419
증명서, 기록매체에서 판독한 CRL, 키 복호키를 이용해, 서명의 정당성을 검증한다
S420
OK ?
아니오
예
S421
스위치를 닫아 콘텐츠를 재생한다
S422
스위치를 열어 콘텐츠를 재생하지 않는다
종료

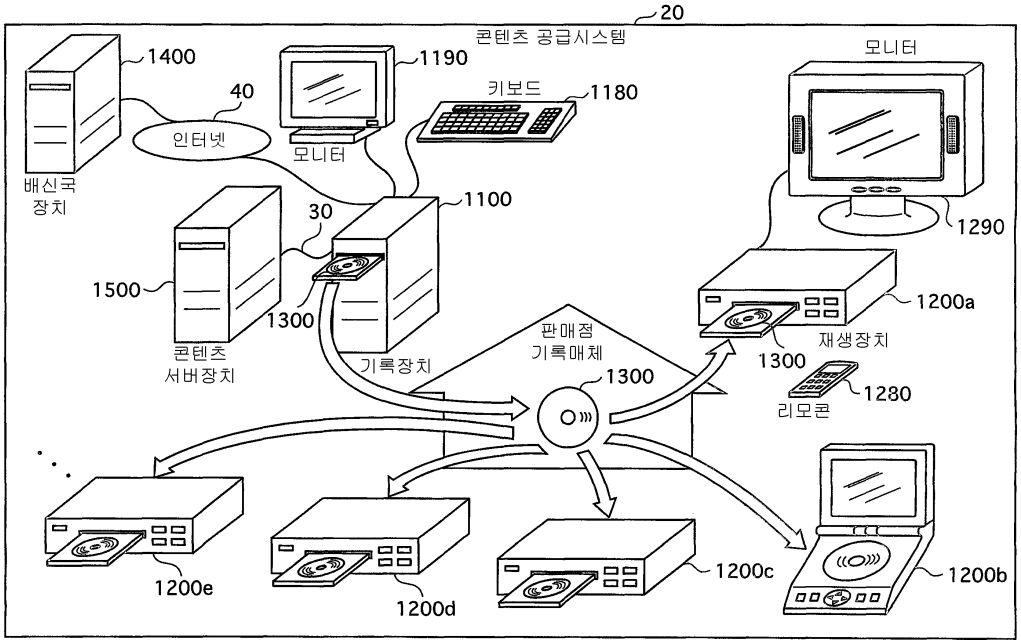
도면8


MD1
기록매체
미디어키 데이터
E1(DK_1, MK) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD2
기록매체
미디어키 데이터
E1(DK_1, 0) 1
E1(DK_2, MK) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD3
기록매체
미디어키 데이터
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, MK) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MDn
기록매체
미디어키 데이터
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, MK) n

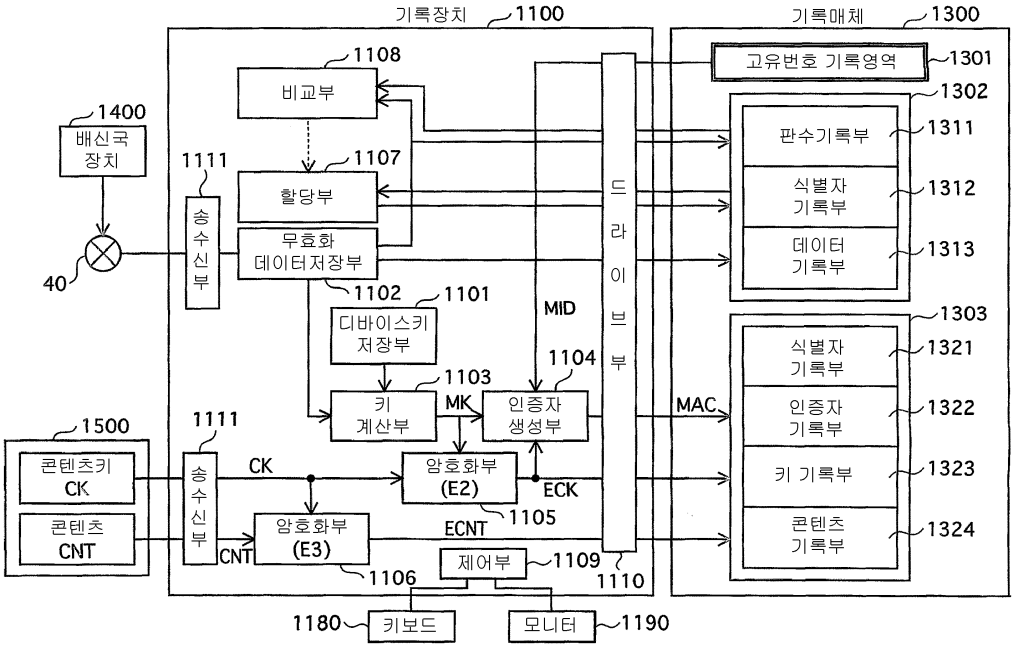
도면9


기록매체
700
710
제 1 콘텐츠 공급 시스템용
키 무효화 데이터 기록영역
711
고유번호
기록영역
712
720
제 2 콘텐츠 공급 시스템용
키 무효화 데이터 기록영역
(미디어키 데이터)
721
제 1 암호화 콘텐츠키
기록영역
722
제 2 암호화 콘텐츠키
기록영역
723

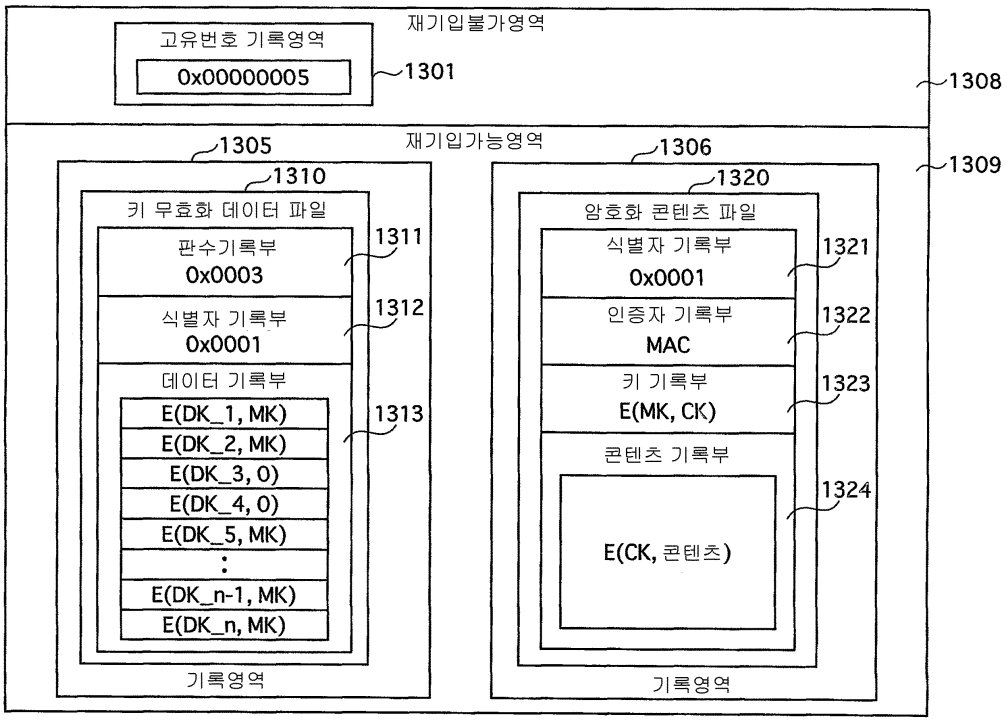
도면10


20
콘텐츠 공급시스템
1400
배신국 장치
40
인터넷
1190
모니터
키보드
1180
모니터
1290
1100
30
1500
콘텐츠 서버장치
1300
기록장치
판매점 기록매체
1300
1200a
재생장치
1300
1280
리모콘
1200e
1200d
1200c
1200b

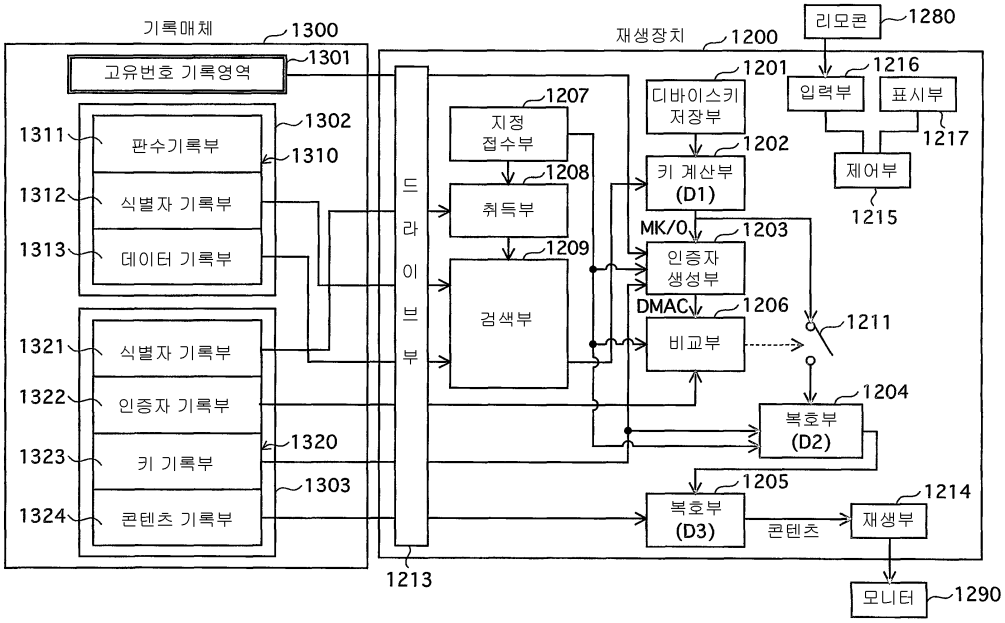
도면11


기록장치
1100
기록매체
1300
1108
비교부
고유번호 기록영역
1301
1302
1400
배신국 장치
1111
1107
할당부
판수기록부
1311
식별자 기록부
1312
데이터 기록부
1313
송수신부
무효화 데이터저장부
40
1102
1101
디바이스키 저장부
MID
1303
식별자 기록부
1321
1104
1103
키 계산부
MK
인증자 생성부
MAC
인증자 기록부
1322
1500
1111
콘텐츠키 CK
송수신부
CK
암호화부 (E2)
ECK
키 기록부
1323
콘텐츠 CNT
암호화부 (E3)
ECNT
1105
콘텐츠 기록부
1324
CNT
제어부
1109
1106
1110
1180
키보드
모니터
1190

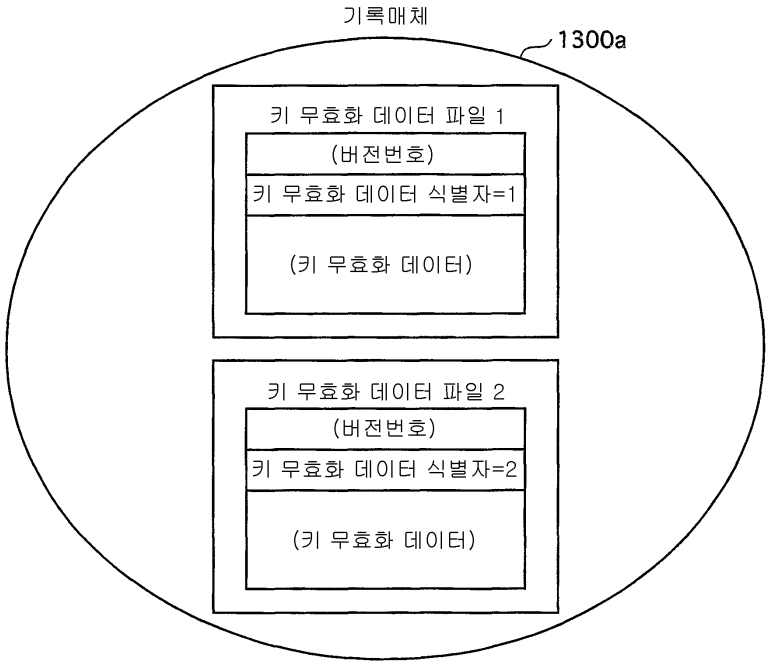
도면12


재기입불가영역
고유번호 기록영역
0x00000005
1301
1308
재기입가능영역
1305
1306
1309
1310
키 무효화 데이터 파일
판수기록부
0x0003
1311
식별자 기록부
0x0001
1312
데이터 기록부
E(DK_1, MK)
E(DK_2, MK)
E(DK_3, 0)
E(DK_4, 0)
E(DK_5, MK)
E(DK_n-1, MK)
E(DK_n, MK)
1313
기록영역
1320
암호화 콘텐츠 파일
식별자 기록부
0x0001
1321
인증자 기록부
MAC
1322
키 기록부
E(MK, CK)
1323
콘텐츠 기록부
E(CK, 콘텐츠)
1324
기록영역

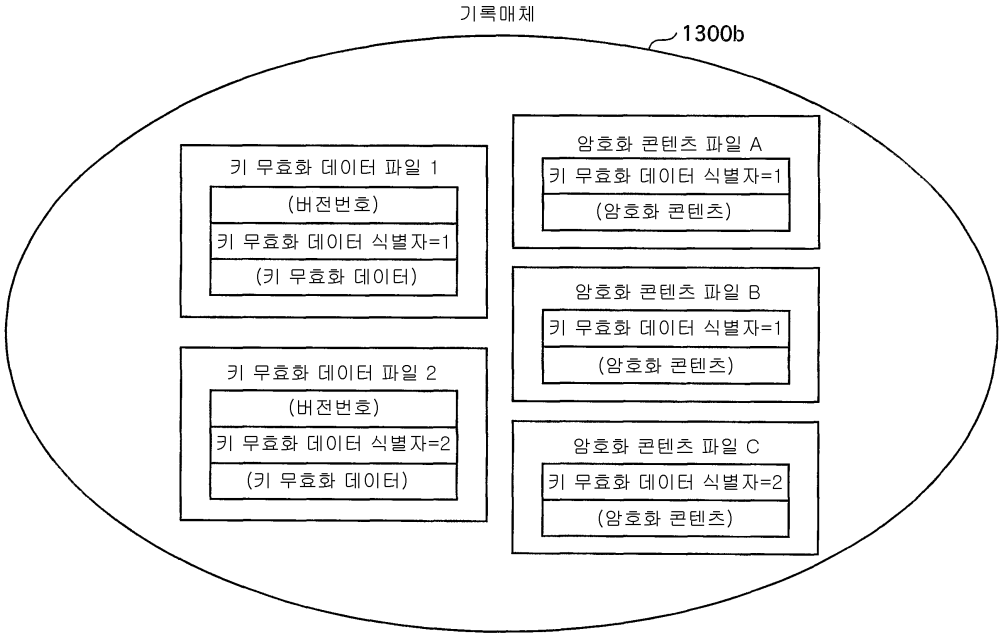
도면13


기록매체
1300
고유번호 기록영역
1301
판수기록부
1302
1310
식별자 기록부
데이터 기록부
1311
1312
1313
식별자 기록부
인증자 기록부
키 기록부
콘텐츠 기록부
1320
1303
1321
1322
1323
1324
1213
드라이브부
재생장치
1200
리모콘
1280
1201
디바이스키 저장부
1202
키 계산부 (D1)
1203
인증자 생성부
1206
비교부
1204
복호부 (D2)
1205
복호부 (D3)
1207
지정 접수부
1208
취득부
1209
검색부
MK/0
DMAC
1211
1216
입력부
표시부
1217
제어부
1215
1214
재생부
콘텐츠
모니터
1290

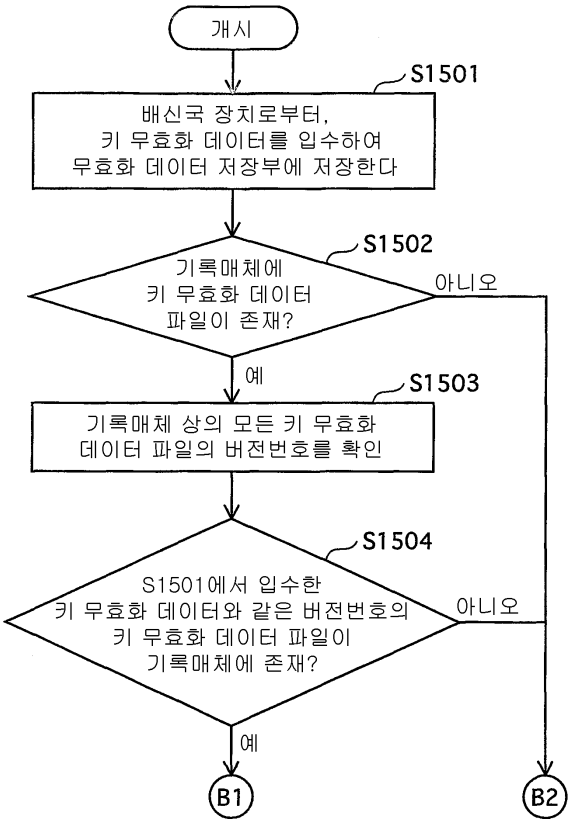
도면14


기록매체
1300a
키 무효화 데이터 파일 1
(버전번호)
키 무효화 데이터 식별자=1
(키 무효화 데이터)
키 무효화 데이터 파일 2
(버전번호)
키 무효화 데이터 식별자=2
(키 무효화 데이터)

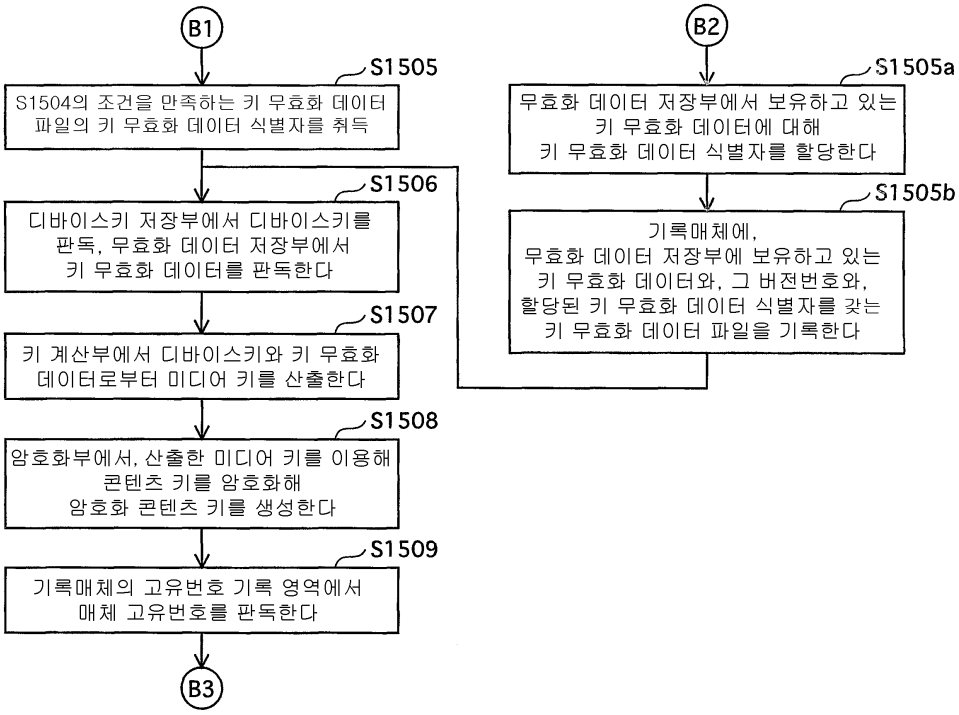
도면15


기록매체
1300b
키 무효화 데이터 파일 1
(버전번호)
키 무효화 데이터 식별자=1
(키 무효화 데이터)
키 무효화 데이터 파일 2
(버전번호)
키 무효화 데이터 식별자=2
(키 무효화 데이터)
암호화 콘텐츠 파일 A
키 무효화 데이터 식별자=1
(암호화 콘텐츠)
암호화 콘텐츠 파일 B
키 무효화 데이터 식별자=1
(암호화 콘텐츠)
암호화 콘텐츠 파일 C
키 무효화 데이터 식별자=2
(암호화 콘텐츠)

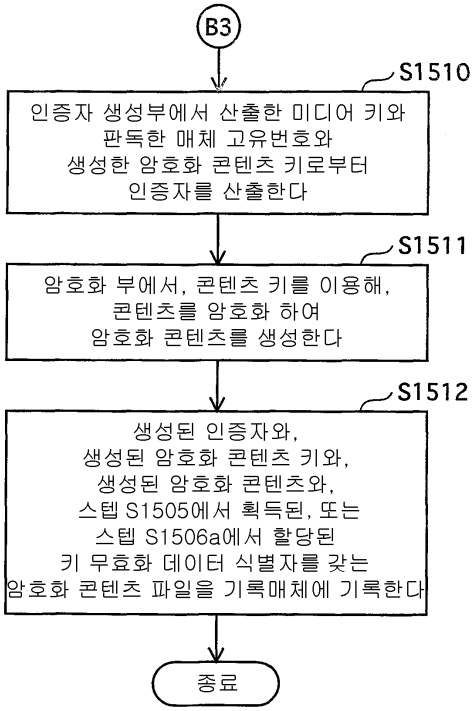
도면16


개시
S1501
배신국 장치로부터,
키 무효화 데이터를 입수하여
무효화 데이터 저장부에 저장한다
S1502
기록매체에
키 무효화 데이터
파일이 존재?
아니오
예
S1503
기록매체 상의 모든 키 무효화
데이터 파일의 버전번호를 확인
S1504
S1501에서 입수한
키 무효화 데이터와 같은 버전번호의
키 무효화 데이터 파일이
기록매체에 존재?
아니오
예
B1
B2

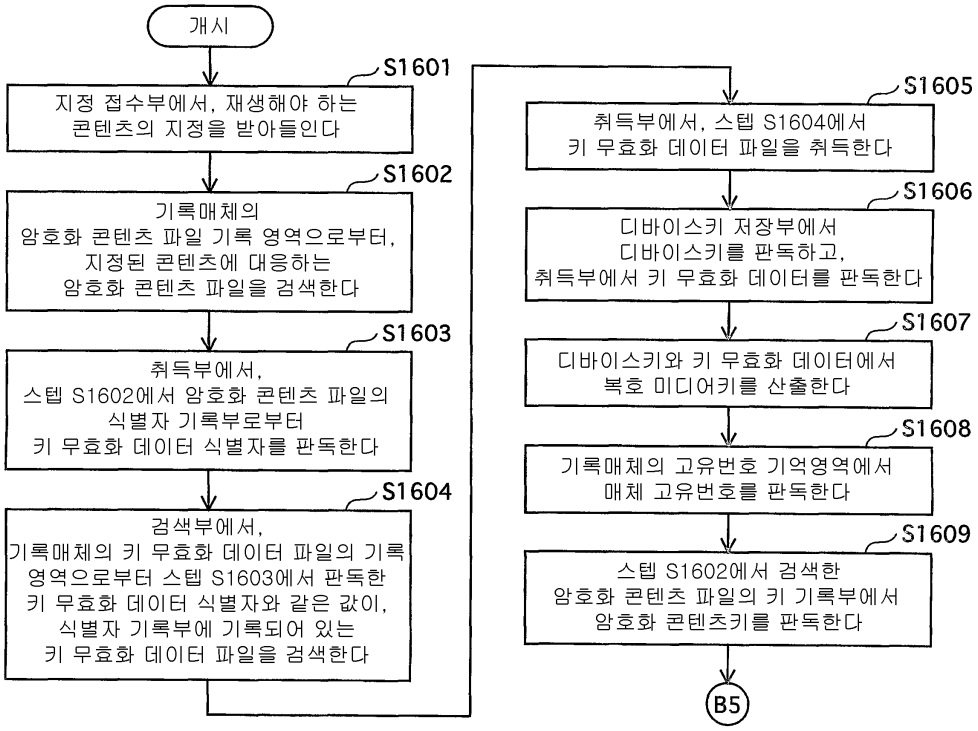
도면17


B1
S1505
S1504의 조건을 만족하는 키 무효화 데이터 파일의 키 무효화 데이터 식별자를 취득
S1506
디바이스키 저장부에서 디바이스키를 판독, 무효화 데이터 저장부에서 키 무효화 데이터를 판독한다
S1507
키 계산부에서 디바이스키와 키 무효화 데이터로부터 미디어 키를 산출한다
S1508
암호화부에서, 산출한 미디어 키를 이용해 콘텐츠 키를 암호화해 암호화 콘텐츠 키를 생성한다
S1509
기록매체의 고유번호 기록 영역에서 매체 고유번호를 판독한다
B3
B2
S1505a
무효화 데이터 저장부에서 보유하고 있는 키 무효화 데이터에 대해 키 무효화 데이터 식별자를 할당한다
S1505b
기록매체에, 무효화 데이터 저장부에 보유하고 있는 키 무효화 데이터와, 그 버전번호와, 할당된 키 무효화 데이터 식별자를 갖는 키 무효화 데이터 파일을 기록한다

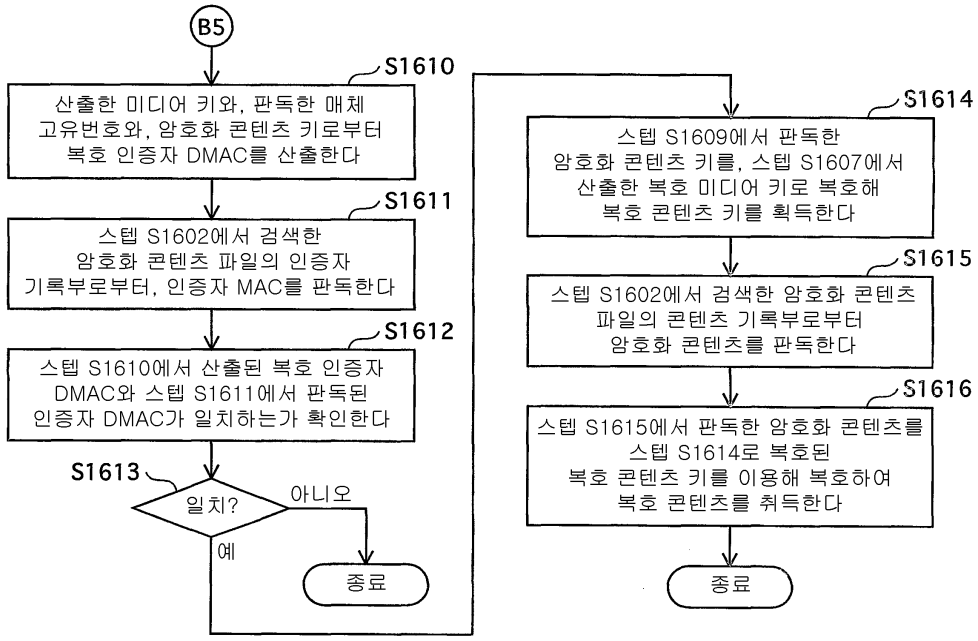
도면18


B3
S1510
인증자 생성부에서 산출한 미디어 키와 판독한 매체 고유번호와 생성한 암호화 콘텐츠 키로부터 인증자를 산출한다
S1511
암호화 부에서, 콘텐츠 키를 이용해, 콘텐츠를 암호화 하여 암호화 콘텐츠를 생성한다
S1512
생성된 인증자와, 생성된 암호화 콘텐츠 키와, 생성된 암호화 콘텐츠와, 스텝 S1505에서 획득된, 또는 스텝 S1506a에서 할당된 키 무효화 데이터 식별자를 갖는 암호화 콘텐츠 파일을 기록매체에 기록한다
종료

도면19


개시
S1601
지정 접수부에서, 재생해야 하는 콘텐츠의 지정을 받아들인다
S1602
기록매체의 암호화 콘텐츠 파일 기록 영역으로부터, 지정된 콘텐츠에 대응하는 암호화 콘텐츠 파일을 검색한다
S1603
취득부에서, 스텝 S1602에서 암호화 콘텐츠 파일의 식별자 기록부로부터 키 무효화 데이터 식별자를 판독한다
S1604
검색부에서, 기록매체의 키 무효화 데이터 파일의 기록 영역으로부터 스텝 S1603에서 판독한 키 무효화 데이터 식별자와 같은 값이, 식별자 기록부에 기록되어 있는 키 무효화 데이터 파일을 검색한다
S1605
취득부에서, 스텝 S1604에서 키 무효화 데이터 파일을 취득한다
S1606
디바이스키 저장부에서 디바이스키를 판독하고, 취득부에서 키 무효화 데이터를 판독한다
S1607
디바이스키와 키 무효화 데이터에서 복호 미디어키를 산출한다
S1608
기록매체의 고유번호 기억영역에서 매체 고유번호를 판독한다
S1609
스텝 S1602에서 검색한 암호화 콘텐츠 파일의 키 기록부에서 암호화 콘텐츠키를 판독한다
B5

도면20


B5
S1610
산출한 미디어 키와, 판독한 매체 고유번호와, 암호화 콘텐츠 키로부터 복호 인증자 DMAC를 산출한다
S1611
스텝 S1602에서 검색한 암호화 콘텐츠 파일의 인증자 기록부로부터, 인증자 MAC를 판독한다
S1612
스텝 S1610에서 산출된 복호 인증자 DMAC와 스텝 S1611에서 판독된 인증자 DMAC가 일치하는가 확인한다
S1613
일치?
아니오
예
종료
S1614
스텝 S1609에서 판독한 암호화 콘텐츠 키를, 스텝 S1607에서 산출한 복호 미디어 키로 복호해 복호 콘텐츠 키를 획득한다
S1615
스텝 S1602에서 검색한 암호화 콘텐츠 파일의 콘텐츠 기록부로부터 암호화 콘텐츠를 판독한다
S1616
스텝 S1615에서 판독한 암호화 콘텐츠를 스텝 S1614로 복호된 복호 콘텐츠 키를 이용해 복호하여 복호 콘텐츠를 취득한다
종료