(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년11월21일
(11) 등록번호 10-1313825
(24) 등록일자 2013년09월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 15/00* (2006.01)
G06F 21/00 (2006.01)
(21) 출원번호 10-2007-7017166
(22) 출원일자(국제) 2006년11월22일
심사청구일자 2011년10월11일
(85) 번역문제출일자 2007년07월25일
(65) 공개번호 10-2008-0075059
(43) 공개일자 2008년08월14일
(86) 국제출원번호 PCT/JP2006/323275
(87) 국제공개번호 WO 2007/063753
국제공개일자 2007년06월07일
(30) 우선권주장
JP-P-2005-00344699 2005년11월29일 일본(JP)
(56) 선행기술조사문헌
JP2004532495 A*
JP2005092830 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
소니 주식회사
일본국 도쿄도 미나토쿠 코난 1-7-1
(72) 발명자
다카시마 요시카즈
일본국 도쿄도 미나토쿠 코난 1-7-1 소니 가부시끼 가이샤내
(74) 대리인
유미특허법인

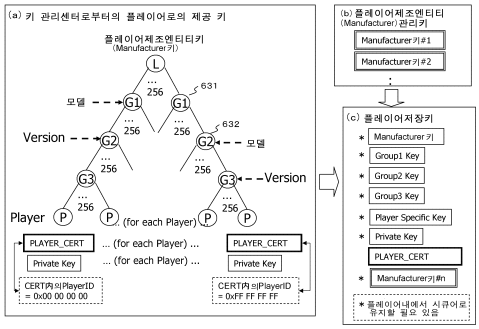
전체 청구항 수 : 총 20 항 심사관 : 이석형

(54) 발명의 명칭 **정보 처리 장치, 정보 기록 매체 제조 장치, 정보 기록매체**

(57) 요 약

본 발명은 다양한 기종, 버전의 장치나 어플리케이션에 대응한 적정한 컨텐츠 코드를 선택한 처리를 실행시키는 구성을 제공한다. 정보 기록 매체에 저장된 컨텐츠 코드를 취득하고, 컨텐츠 코드에 따른 시큐리티 체크, 컨텐츠 데이터의 변환, 플레이어 정보의 컨텐츠에 대한 매립 등의 처리를 실행하는 구성에 있어서, 컨텐츠 코드 중 적어도 일부를 암호화 데이터로서 설정하고, 그 암호 키로서 계층 구성을 가지는 키 트리의 노드에 대응하여 설정된 노드 키를 적용한다. 본 구성에 의해, 노드 키를 적용하여 컨텐츠 코드의 암호화부를 복호 할 수 있는 플레이어를 미리 특정 가능하고, 각 플레이어에 대응하는 적정한 컨텐츠 코드만을 처리시켜, 부정한 컨텐츠 코드의 적용 처리를 방지할 수 있다.

대 표 도 - 도12



특허청구의 범위

청구항 1

정보 처리 장치로서,

정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하고, 상기 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리부와,

계층 구성을 가지는 키 트리에 있어서, 상기 정보 처리 장치에 대응시킨 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리

를 가지고,

상기 데이터 처리부는,

상기 컨텐츠 코드 중 적어도 일부 구성 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하고, 복호의 결과 취득한 컨텐츠 코드에 따른 데이터 처리를 실행하는 구성이며,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 데이터 처리부는, 또한,

복호된 상기 컨텐츠 코드로부터 상기 변환 데이터를 취득하고, 상기 변칙 데이터의 기록 영역을 변환 데이터로 치환하는 처리를 행하는 구성이며,

상기 노드 키는, 상기 정보 처리 장치에 속하는 그룹에 대응하여 설정된 노드 키이며, 상기 데이터 처리부는 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 메모리로부터 자기 장치(自裝置)에 속하는 그룹에 대응하여 설정된 노드 키를 선택하는,

정보 처리 장치.

청구항 2

제1항에 있어서,

상기 데이터 처리부는,

상기 컨텐츠 코드의 복호에 적용하는 키 지정 정보, 및 상기 컨텐츠 코드 중에 설정된 암호화 데이터의 위치를 나타내는 암호화 데이터 위치 지정 정보를 상기 정보 기록 매체의 저장 데이터로부터 취득하고, 취득 정보에 따라 상기 메모리로부터 노드 키를 선택하고, 상기 암호화 데이터 위치 지정 정보에 따라 복호 대상 데이터를 특정하여, 선택 노드 키를 적용한 복호 처리를 실행하는 구성인, 정보 처리 장치.

청구항 3

제1항에 있어서,

상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 상기 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터이며,

상기 데이터 처리부는,

상기 코드 정보 암호화 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하는 처리를 실행하는 구성인, 정보 처리 장치.

청구항 4

제1항에 있어서,

상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 구성이며,

상기 데이터 처리부는,

상기 암호화 키 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하여 고유 암호 키를 취득하고, 상기 코드 정보 암호화 데이터를, 상기 고유 암호 키를 적용하여 복호하는 처리를 실행하는 구성인, 정보 처리 장치.

청구항 5

제1항에 있어서,

상기 컨텐츠 코드는, 상기 정보 처리 장치에 대응하는 시큐리티 체크 코드를 포함하고,

상기 데이터 처리부는,

상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따른 시큐리티 체크 처리를 실행하는 구성인, 정보 처리 장치.

청구항 6

제1항에 있어서,

상기 컨텐츠 코드는, 상기 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고,

상기 데이터 처리부는,

상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라 상기 정보 기록 매체에 저장된 컨텐츠의 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 구성인, 정보 처리 장치.

청구항 7

제1항에 있어서,

상기 컨텐츠 코드는, 상기 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고,

상기 데이터 처리부는,

상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 구성인, 정보 처리 장치.

청구항 8

제1항에 있어서,

상기 데이터 처리부는,

상기 정보 처리 장치의 메모리에 기억된 플레이어 증명서를 취득하여, 상기 플레이어 증명서의 정당성 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로서, 상기 플레이어 증명서의 기록 정보로부터, 상기 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 취득하고, 취득 정보에 따라 처리 대상의 컨텐츠 코드를 선택하는 처리를 실행하는 구성인, 정보 처리 장치.

청구항 9

정보 기록 매체 제조 장치로서,

정보 기록 매체에 기록하는 컨텐츠 데이터를 저장한 컨텐츠 파일을 생성하는 컨텐츠 파일 생성 수단과,

컨텐츠의 이용을 행할 때 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 컨텐츠 코드 파일 생성 수단과,

상기 컨텐츠 파일 생성 수단에서 생성한 컨텐츠 파일, 및 상기 컨텐츠 코드 파일 생성 수단에서 생성한 컨텐츠 코드 파일을 상기 정보 기록 매체에 기록하는 기록 수단을 가지고,

상기 컨텐츠 코드 파일 생성 수단은,

각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성이며,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 노드 키는, 각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션이 속하는 그룹에 대응하여 설정된 노드 키이며, 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 각 정보 처리 장치의 메모리로부터 선택되는 키인,

정보 기록 매체 제조 장치.

청구항 10

제9항에 있어서,

상기 컨텐츠 코드 파일 생성 수단은,

상기 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인, 정보 기록 매체 제조 장치.

청구항 11

제9항에 있어서,

상기 컨텐츠 코드 파일 생성 수단은,

상기 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인, 정보 기록 매체 제조 장치.

청구항 12

제9항에 있어서,

상기 컨텐츠 코드 파일 생성 수단은,

정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인, 정보 기록 매체 제조 장치.

청구항 13

제9항에 있어서,

상기 컨텐츠 코드 파일 생성 수단은,

상기 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인, 정보 기록 매체 제조 장치.

청구항 14

정보 기록 매체로서,

컨텐츠 데이터를 저장한 컨텐츠 파일과

컨텐츠의 이용을 행할 때 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일

을 저장 데이터로서 가지고,

상기 컨텐츠 코드 파일은,

각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 구성이며,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 노드 키는, 각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션이 속하는 그룹에 대응하여 설정된 노드 키이며, 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 각 정보 처리 장치의 메모리로부터 선택되는 키이며,

상기 정보 기록 매체에 저장된 컨텐츠 재생을 실행하는 정보 처리 장치에 있어서, 상기 컨텐츠 코드에 따른 노드 키의 선택 처리와, 선택 노드 키에 의한 컨텐츠 코드의 복호 처리와, 상기 치환용 데이터를 적용한 데이터 치환을 실행시키는 것을 가능하게 한,

정보 기록 매체.

청구항 15

제14항에 있어서,

상기 컨텐츠 코드 파일은,

상기 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인, 정보 기록 매체.

청구항 16

제14항에 있어서,

상기 컨텐츠 코드 파일은,

상기 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인, 정보 기록 매체.

청구항 17

제14항에 있어서,

상기 컨텐츠 코드 파일은,

정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인, 정보 기록 매체.

청구항 18

정보 처리 장치에 있어서, 정보 기록 매체의 기록 데이터를 적용한 데이터 처리를 실행하는 정보 처리 방법으로서,

상기 정보 처리 장치의 데이터 처리부가, 상기 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하는 컨텐츠 코드 취득 스텝과,

상기 데이터 처리부가, 계층 구성을 가지는 키 트리에 있어서, 상기 정보 처리 장치에 대응시킨 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리로부터 노드 키를 선택하는 노드 키 선택 스텝과,

상기 데이터 처리부가, 상기 노드 키 선택 스텝에서 선택한 노드 키를 적용하여, 상기 컨텐츠 코드 중 적어도

일부 구성 데이터를 복호하는 코드 복호 스텝과,

상기 데이터 처리부가, 상기 코드 복호 스텝에서 복호한 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리 스텝을 실행하고,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 데이터 처리 스텝에서는,

상기 데이터 처리부가, 복호된 컨텐츠 코드로부터 상기 변환 데이터를 취득하고, 상기 변칙 데이터의 기록 영역을 변환 데이터로 치환하는 처리를 행하고,

상기 노드 키는, 상기 정보 처리 장치에 속하는 그룹에 대응하여 설정된 노드 키이며,

상기 노드 키 선택 스텝에서는, 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 메모리로부터 자기 장치(自裝置)에 속하는 그룹에 대응하여 설정된 노드 키를 선택하는,

정보 처리 방법.

청구항 19

정보 기록 매체 제조 장치에서의 정보 기록 매체 제조 방법으로서,

상기 정보 기록 매체 제조 장치의 컨텐츠 파일 생성 수단이, 정보 기록 매체에 기록하는 컨텐츠 데이터를 저장한 컨텐츠 파일을 생성하는 컨텐츠 파일 생성 스텝과,

상기 정보 기록 매체 제조 장치의 컨텐츠 파일 생성 수단이, 컨텐츠의 이용을 행할 때 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 컨텐츠 코드 파일 생성 스텝과,

상기 정보 기록 매체 제조 장치의 기록 수단이, 상기 컨텐츠 파일 생성 스텝에서 생성한 컨텐츠 파일, 및 상기 컨텐츠 코드 파일 생성 스텝에서 생성한 컨텐츠 코드 파일을 상기 정보 기록 매체에 기록하는 기록 스텝을 실행하고,

상기 컨텐츠 코드 파일 생성 스텝은,

각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상 중 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝이며,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 노드 키는, 각 정보 처리 장치 또는 각 정보 처리 장치가 실행하는 재생 어플리케이션이 속하는 그룹에 대응하여 설정된 노드 키이며, 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 각 정보 처리 장치의 메모리로부터 선택되는 키인,

정보 기록 매체 제조 방법.

청구항 20

정보 처리 장치에 있어서, 정보 기록 매체의 기록 데이터를 적용한 데이터 처리를 실행시키는 컴퓨터 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체로서,

상기 정보 처리 장치의 데이터 처리부에, 상기 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하는 컨텐츠 코드 취득 스텝과,

상기 데이터 처리부에, 계층 구성을 가지는 키 트리에 있어서, 정보 처리 장치에 대응시킨 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리로부터 노드 키를 선택하는 노드 키 선택 스텝과,

상기 데이터 처리부에, 상기 노드 키 선택 스텝에서 선택한 노드 키를 적용하여, 상기 컨텐츠 코드 중 적어도 일부 구성 데이터를 복호하는 코드 복호 스텝과,

상기 데이터 처리부에, 상기 코드 복호 스텝에서 복호한 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리 스텝을 실행시키고,

상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠에 설정된 정상인 컨텐츠 재생을 방해하는 변칙 데이터에 대한 치환용 데이터인 변환 데이터와, 상기 노드 키의 지정 정보인 키 지정 정보를 포함하고,

상기 데이터 처리 스텝에서는,

상기 데이터 처리부에, 복호된 컨텐츠 코드로부터 상기 변환 데이터를 취득하고, 상기 변칙 데이터의 기록 영역을 변환 데이터로 치환하는 처리를 실행시키고,

상기 노드 키는, 정보 처리 장치에 속하는 그룹에 대응하여 설정된 노드 키이며,

상기 노드 키 선택 스텝에서는, 상기 컨텐츠 코드에 포함되는 키 지정 정보에 따라 상기 메모리로부터 자기 장치(自裝置)에 속하는 그룹에 대응된 노드 키를 선택하게 하는 컴퓨터 프로그램이 기록된,

컴퓨터로 판독 가능한 기록 매체.

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

명 세 서

기 술 분 야

[0001] 본 발명은, 정보 처리 장치, 정보 기록 매체 제조 장치, 정보 기록 매체, 정보 처리 방법, 정보 기록 매체 제조 방법 및 컴퓨터 프로그램에 관한 것이다. 보다 상세하게는, 컨텐츠의 이용 제어 프로그램으로서 컨텐츠와 함께 정보 기록 매체에 기록되는 컨텐츠 코드를 적용한 데이터 처리에 대하여, 각 정보 처리 장치나 재생 어플리케이션 등의 플레이어에 대응한 적정한 컨텐츠 코드를 확실하게 선택하여 실행시키는 구성으로 한 정보 처리 장치, 정보 기록 매체 제조 장치, 정보 기록 매체, 정보 처리 방법, 정보 기록 매체 제조 방법 및 컴퓨터 프로그램에 관한 것이다.

배 경 기 술

[0002] 음악 등의 오디오 데이터, 영화 등의 화상 데이터, 게임 프로그램, 각종 어플리케이션 프로그램 등, 다양한 소프트웨어 데이터(이하, 이들을 컨텐츠(Content)라고 한다)는, 기록 미디어, 예를 들면, 청색 레이저를 적용한 Blu-ray Disc(상표), 또는 DVD(Digital Versatile Disc), MD(Mini Disc), CD(Compact Disc)에 디지털 데이터로서 저장할 수 있다. 특히, 청색 레이저를 이용한 Blu-ray Disc(상표)는, 고밀도 기록 가능한 디스크이며 대용량의 영상 컨텐츠 등을 고화질 데이터로서 기록할 수 있다.

[0003] 이들 다양한 정보 기록 매체(기록 미디어)에 디지털 컨텐츠가 저장되고, 사용자에게 제공된다. 사용자는, 소유하고 있는 PC(Personal Computer), 디스크 플레이어 등의 재생 장치에 있어서 컨텐츠의 재생, 이용을 행한다.

[0004] 음악 데이터, 화상 데이터 등, 많은 컨텐츠는, 일반적으로 그 작성자 또는 판매 사람에게 반포권 등이 보유되어 있다. 따라서, 이들 컨텐츠의 배포에 대하여는, 일정한 이용 제한, 즉 정규인 사용자에 대하여만, 컨텐츠의 이용을 허락하고, 허가가 없는 복제 등이 행해지지 않도록 하는 구성을 취하는 것이 일반적으로 되어 있다.

[0005] 디지털 기록 장치 및 기록 매체에 의하면, 예를 들면, 화상이나 음성을 열화시키지 않고 기록, 재생을 반복하는 것이 가능하며, 부정 카피 컨텐츠의 인터넷을 통한 분배나, 컨텐츠를 CD-R 등에 카피한, 이른바 해적판 디스크의 유통이나, PC 등의 하드 디스크에 저장한 카피 컨텐츠의 이용이 만연하고 있다는 문제가 발생하고 있다.

[0006] DVD, 또는 최근 개발이 진행되어 있는 청색 레이저를 이용한 기록 매체 등의 대용량형 기록 매체는, 1개의 매체에 예를 들면, 영화 1개 ~ 수개 분의 대량의 데이터를 디지털 정보로서 기록할 수 있다. 이와 같이 영상 정보 등을 디지털 정보로서 기록하는 것이 가능하게 되면 부정 카피를 방지하여 저작권자의 보호를 도모하는 것이 더욱더 중요한 과제로 되어 있다. 최근에서는, 이와 같은 디지털 데이터의 부정한 카피를 방지하기 위하여, 디지털 기록 장치 및 기록 매체에 위법한 카피를 방지하기 위한 다양한 기술이 실용화되어 있다.

[0007] 컨텐츠의 부정 카피를 방지하여 저작권자의 보호를 도모하는 1개의 방법으로서 컨텐츠의 암호화 처리가 있다. 그러나, 컨텐츠를 암호화해도, 암호 키의 누출이 발생해버리면, 부정으로 복호된 컨텐츠가 유출되는 문제가 발생한다. 이와 같은 문제를 해결하는 1개의 구성을 개시한 종래 기술로서, 특허 문헌 1인 일본국 특개 제2002-311998호에 기재된 구성이 있다. 특허 문헌 1은, 컨텐츠의 일부를 더미 데이터에 치환하여 기록함으로써, 컨텐츠의 부정 재생을 방지한 구성을 개시하고 있다.

[0008] 컨텐츠를 더미 데이터에 치환하여 컨텐츠의 재생 처리를 행할 때에는, 더미 데이터를 정상적인 컨텐츠 데이터에 재차, 치환하는 처리가 필요해진다. 이 데이터 변환 처리는, 정상 컨텐츠의 외부로의 누출을 발생시키지 않고 행해지는 것이 필요하고, 또 더미 데이터의 배치 위치 등이나 변환 방법 등의 처리 정보에 대해도 누출을 방지하는 것이 바람직하다.

[0009] 이와 같이, 컨텐츠의 재생을 행할 때에는, 컨텐츠의 복호 처리나 데이터 변환 처리 등을 실행하는 것이 필요하고, 또, 컨텐츠를 이용하려고 하는 정보 처리 장치나 재생(플레이어) 프로그램이 정당한 라이센스를 받은 기기나 프로그램인가라는 정당성 확인 처리 등의 시큐리티 체크를 행하는 경우가 있다. 이와 같은 데이터 처리는, 컨텐츠의 이용 제어 프로그램으로서, 컨텐츠와 함께 정보 기록 매체에 기록되는 컨텐츠 코드를 실행함으로써 행해진다. 그리고, 컨텐츠 코드를 이용한 컨텐츠 이용 처리에에 대하여는, 예를 들면, 특허 문헌 1에 기재가 있다.

[0010] 컨텐츠 코드는, 컨텐츠와는 독립된 파일로서 설정하고, 정보 기록 매체에 기록된다. 따라서, 컨텐츠 코드만을

다른 정보 기록 매체에 이동시키는 처리나, 카피하는 처리도 가능해진다. 컨텐츠 코드의 누출이 발생하고, 부정 유통, 부정 이용이 행해지면, 많은 컨텐츠가 부정으로 재생, 이용되는 가능성이 있으므로, 큰 손해를 발생시킬 가능성이 있다.

[0011] 또한, 컨텐츠 재생을 실행하는 장치나, 어플리케이션으로서는, 다양한 메이커의 상이한 장치나 어플리케이션이 적용되는 것이 생각되지만, 컨텐츠 코드를 이용한 시큐리티 체크나 데이터 변환 처리를 실행하는 경우, 다양한 메이커의 상이한 장치나 어플리케이션 등의 플레이어에 대응시킨 적정한 컨텐츠 코드를 선택시켜, 각각의 시퀀스에 따른 시큐리티 체크를 행하고, 또한, 플레이어에 대응하는 고유한 데이터 변환 처리를 행하게 하는 설정으로 하는 것이 바람직하다. 특히 데이터 변환에 있어서는, 플레이어 식별 정보를 컨텐츠 중에 매립하는 처리를 행하는 경우가 있으므로, 플레이어에 대응하는 정확한 컨텐츠 코드의 선택이 행해지지 않은 경우에는, 정확한 플레이어 식별 정보의 매립이 실행되지 않게 되는 문제가 있다.

[0012] [특허 문헌 1] 일본국 특개 2002-311998

[0013] 본 발명은, 이와 같은 상황을 감안하여 이루어진 것이며, 컨텐츠의 이용 제어 프로그램으로서 컨텐츠와 함께 정보 기록 매체에 기록되는 컨텐츠 코드의 엄격한 관리 구성을 실현하고, 컨텐츠 코드를 적용한 데이터 처리에 대하여, 각 정보 처리 장치나 재생 어플리케이션 등의 플레이어에 대응한 적정한 컨텐츠 코드를 확실하게 선택하여 실행시키는 구성으로 한 정보 처리 장치, 정보 기록 매체 제조 장치, 정보 기록 매체, 정보 처리 방법, 정보 기록 매체 제조 방법 및 컴퓨터 프로그램을 제공하는 것을 목적으로 하는 것이다.

발명의 상세한 설명

[0014] 본 발명의 제1 측면은,

[0015] 정보 처리 장치로서,

[0016] 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하고, 상기 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리부와,

[0017] 계층 구성을 가지는 키 트리에 있어서, 정보 처리 장치에 대응한 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리를 가지고,

[0018] 상기 데이터 처리부는,

[0019] 상기 컨텐츠 코드 중 적어도 일부 구성 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하고, 복호의 결과 취득한 컨텐츠 코드에 따른 데이터 처리를 실행하는 구성을 구비한 것을 특징으로 하는 정보 처리 장치에 있다.

[0020] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 데이터 처리부는, 상기 컨텐츠 코드의 복호에 적용하는 키 지정 정보, 및 상기 컨텐츠 코드 중에 설정된 암호화 데이터의 위치를 나타내는 암호화 데이터 위치 지정 정보를 상기 정보 기록 매체의 저장 데이터로부터 취득하고, 상기 취득 정보에 따라 상기 메모리로부터 노드 키를 선택하고, 상기 암호화 데이터 위치 지정 정보에 따라 복호 대상 데이터를 특정하여, 선택 노드 키를 적용한 복호 처리를 실행하는 구성인 것을 특징으로 한다.

[0021] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 상기 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터이며, 상기 데이터 처리부는, 상기 코드 정보 암호화 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하는 처리를 실행하는 구성인 것을 특징으로 한다.

[0022] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 구성이며, 상기 데이터 처리부는, 상기 암호화 키 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하여 고유 암호 키를 취득하고, 상기 코드 정보 암호화 데이터를, 상기 고유 암호 키를 적용하여 복호하는 처리를 실행하는 구성인 것을 특징으로 한다.

[0023] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 처리 장치에 대응하는 시큐리티 체크 코드를 포함하고, 상기 데이터 처리부는, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따른 시큐리티 체크 처리를 실행하는 구성인 것을 특징으로 한다.

[0024] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고, 상기 데이터 처리부는, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라, 상기 정보 기록 매체에 저장된 컨텐츠의 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 구성인 것을 특징으로 한다.

[0025] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고, 상기 데이터 처리부는, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라, 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 구성인 것을 특징으로 한다.

[0026] 또한, 본 발명의 정보 처리 장치의 일 실시예에 있어서, 상기 데이터 처리부는, 정보 처리 장치의 메모리에 기억된 플레이어 증명서를 취득하고, 상기 플레이어 증명서의 정당성 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로서, 상기 플레이어 증명서의 기록 정보로부터, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 취득하고, 상기 취득 정보에 따라 처리 대상의 컨텐츠 코드를 선택하는 처리를 실행하는 구성인 것을 특징으로 한다.

[0027] 또한, 본 발명의 제2 측면은,

[0028] 정보 기록 매체 제조 장치로서,

[0029] 정보 기록 매체에 기록하는 컨텐츠 데이터를 저장한 컨텐츠 파일을 생성하는 컨텐츠 파일 생성 수단과,

[0030] 컨텐츠의 이용에 대하여 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 컨텐츠 코드 파일 생성 수단과,

[0031] 상기 컨텐츠 파일 생성 수단에서 생성한 컨텐츠 파일, 및 상기 컨텐츠 코드 파일 생성 수단에서 생성한 컨텐츠 코드 파일을 정보 기록 매체에 기록하는 기록 수단을 가지고,

[0032] 상기 컨텐츠 코드 파일 생성 수단은,

[0033] 각 정보 처리 장치 또는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인 것을 특징으로 하는 정보 기록 매체 제조 장치에 있다.

[0034] 또한, 본 발명의 정보 기록 매체 제조 장치의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 수단은, 상기 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인 것을 특징으로 한다.

[0035] 또한, 본 발명의 정보 기록 매체 제조 장치의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 수단은, 상기 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인 것을 특징으로 한다.

[0036] 또한, 본 발명의 정보 기록 매체 제조 장치의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 수단은, 정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인 것을 특징으로 한다.

[0037] 또한, 본 발명의 정보 기록 매체 제조 장치의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 수단은, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성인 것을 특징으로 한다.

[0038] 또한, 본 발명의 제3 측면은,

[0039] 정보 기록 매체로서,

[0040] 컨텐츠 데이터를 저장한 컨텐츠 파일과

[0041] 컨텐츠의 이용에 대하여 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일

[0042] 을 저장 데이터로서 가지고,

[0043] 상기 컨텐츠 코드 파일은,

[0044] 각 정보 처리 장치 또는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 포함하는 것을 특징으로 하는 정보 기록 매체에 있다.

[0045] 또한, 본 발명의 정보 기록 매체의 일 실시예에 있어서, 상기 컨텐츠 코드 파일은, 상기 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인 것을 특징으로 한다.

[0046] 또한, 본 발명의 정보 기록 매체의 일 실시예에 있어서, 상기 컨텐츠 코드 파일은, 상기 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인 것을 특징으로 한다.

[0047] 또한, 본 발명의 정보 기록 매체의 일 실시예에 있어서, 상기 컨텐츠 코드 파일은, 정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인 것을 특징으로 한다.

[0048] 또한, 본 발명의 정보 기록 매체의 일 실시예에 있어서, 상기 컨텐츠 코드 파일은, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일인 것을 특징으로 한다.

[0049] 또한, 본 발명의 제4 측면은,

[0050] 정보 처리 장치에 있어서, 정보 기록 매체의 기록 데이터를 적용한 데이터 처리를 실행하는 정보 처리 방법으로서,

[0051] 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하는 컨텐츠 코드 취득 스텝과,

[0052] 계층 구성을 가지는 키 트리에 있어서, 정보 처리 장치에 대응시킨 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리로부터 노드 키를 선택하는 노드 키 선택 스텝과,

[0053] 상기 노드 키 선택 스텝에서 선택한 노드 키를 적용하여, 상기 컨텐츠 코드 중 적어도 일부 구성 데이터를 복호하는 코드 복호 스텝과,

[0054] 상기 코드 복호 스텝에서 복호한 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리 스텝

[0055] 을 구비한 것을 특징으로 하는 정보 처리 방법에 있다.

[0056] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 노드 키 선택 스텝은, 상기 컨텐츠 코드의 복호에 적용하는 키 지정 정보를 상기 정보 기록 매체의 저장 데이터로부터 취득하고, 상기 취득 정보에 따라 상기 메모리로부터 노드 키를 선택하는 스텝이며, 상기 코드 복호 스텝은, 상기 컨텐츠 코드 중에 설정된 암호화 데이터의 위치를 나타내는 암호화 데이터 위치 지정 정보를 상기 정보 기록 매체의 저장 데이터로부터 취득하고, 상기 취득 정보에 따라 복호 대상 데이터를 특정하여, 선택 노드 키를 적용한 복호 처리를 실행하는 스텝인 것을 특징으로 한다.

[0057] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 상기 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터이며, 상기 코드 복호 스텝은, 상기 코드 정보 암호화 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하는 처리를 실행하는 스텝인 것을 특징으로 한다.

[0058] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 컨텐츠 코드는 적어도 일부 구성 데이터를, 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한

암호화 키 데이터를 포함하는 구성이며, 상기 코드 복호 스텝은, 상기 암호화 키 데이터를, 상기 메모리로부터 취득한 노드 키를 적용하여 복호하여 고유 암호 키를 취득하고, 상기 코드 정보 암호화 데이터를, 상기 고유 암호 키를 적용하여 복호하는 처리를 실행하는 스텝인 것을 특징으로 한다.

[0059] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 처리 장치에 대응하는 시큐리티 체크 코드를 포함하고, 상기 데이터 처리 스텝은, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따른 시큐리티 체크 처리를 실행하는 스텝인 것을 특징으로 한다.

[0060] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고, 상기 데이터 처리 스텝은, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라, 상기 정보 기록 매체에 저장된 컨텐츠의 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 스텝인 것을 특징으로 한다.

[0061] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 컨텐츠 코드는, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하고, 상기 데이터 처리 스텝은, 상기 노드 키를 적용하여 복호한 컨텐츠 코드에 따라, 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성을 실행하는 스텝인 것을 특징으로 한다.

[0062] 또한, 본 발명의 정보 처리 방법의 일 실시예에 있어서, 상기 정보 처리 방법은, 또한 정보 처리 장치의 메모리에 기억된 플레이어 증명서를 취득하고, 상기 플레이어 증명서의 정당성 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로서, 상기 플레이어 증명서의 기록 정보로부터, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 취득하고, 상기 취득 정보에 따라 처리 대상의 컨텐츠 코드를 선택하는 처리를 실행하는 스텝을 포함하는 것을 특징으로 한다.

[0063] 또한, 본 발명의 제5 측면은,

[0064] 정보 기록 매체 제조 장치에서의 정보 기록 매체 제조 방법으로서,

[0065] 정보 기록 매체에 기록하는 컨텐츠 데이터를 저장한 컨텐츠 파일을 생성하는 컨텐츠 파일 생성 스텝과,

[0066] 컨텐츠의 이용에 대하여 실행해야 할 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 컨텐츠 코드 파일 생성 스텝과,

[0067] 상기 컨텐츠 파일 생성 스텝에서 생성한 컨텐츠 파일, 및 상기 컨텐츠 코드 파일 생성 스텝에서 생성한 컨텐츠 코드 파일을 정보 기록 매체에 기록하는 기록 스텝을 포함하고,

[0068] 상기 컨텐츠 코드 파일 생성 스텝은,

[0069] 각 정보 처리 장치 또는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝인 것을 특징으로 하는 정보 기록 매체 제조 방법에 있다.

[0070] 또한, 본 발명의 정보 기록 매체 제조 방법의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 스텝은, 상기 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝인 것을 특징으로 한다.

[0071] 또한, 본 발명의 정보 기록 매체 제조 방법의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 스텝은, 상기 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키로 암호화한 코드 정보 암호화 데이터와, 상기 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝인 것을 특징으로 한다.

[0072] 또한, 본 발명의 정보 기록 매체 제조 방법의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 스텝은, 정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝인 것을 특징으로 한다.

[0073] 또한, 본 발명의 정보 기록 매체 제조 방법의 일 실시예에 있어서, 상기 컨텐츠 코드 파일 생성 스텝은, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는

식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 스텝인 것을 특징으로 한다.

[0074] 또한, 본 발명의 제6 측면은,

[0075] 정보 처리 장치에 있어서, 정보 기록 매체의 기록 데이터를 적용한 데이터 처리를 실행시키는 컴퓨터 프로그램으로서,

[0076] 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하는 컨텐츠 코드 취득 스텝과,

[0077] 계층 구성을 가지는 키 트리에 있어서, 정보 처리 장치에 대응한 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 저장한 메모리로부터 노드 키를 선택하는 노드 키 선택 스텝과,

[0078] 상기 노드 키 선택 스텝에서 선택한 노드 키를 적용하여, 상기 컨텐츠 코드 중 적어도 일부 구성 데이터를 복호하는 코드 복호 스텝과,

[0079] 상기 코드 복호 스텝에서 복호한 컨텐츠 코드에 따른 데이터 처리를 실행하는 데이터 처리 스텝

[0080] 을 실행시키는 것을 특징으로 하는 컴퓨터 프로그램에 있다.

[0081] 그리고, 본 발명의 컴퓨터 프로그램은, 예를 들면, 다양한 프로그램 코드를 실행할 수 있는 컴퓨터 시스템에 대하여, 컴퓨터 판독 가능한 형식으로 제공하는 기억 매체, 통신 매체, 예를 들면, CD나 FD, MO 등의 기록 매체, 또는 네트워크 등의 통신 매체에 의해 제공할 수 있는 컴퓨터 프로그램이다. 이와 같은 프로그램을 컴퓨터 판독 가능한 형식으로 제공함으로써, 컴퓨터 시스템상에서 프로그램에 따른 처리가 실현된다.

[0082] 본 발명의 또 다른 목적, 특징이나 이점은, 후술하는 본 발명의 실시예나 첨부하는 도면에 따른 더욱 상세한 설명에 의해 명백해 질 것이다. 그리고, 본 명세서에 있어서 시스템은, 복수개의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 하우징 내에 있는 것에 한정되지 않는다.

실 시 예

[0104] 이하, 도면을 참조하면서 본 발명의 정보 처리 장치, 정보 기록 매체 제조 장치, 정보 기록 매체, 정보 처리 방법, 정보 기록 매체 제조 방법 및 컴퓨터 프로그램의 상세에 대하여 설명한다. 그리고, 설명은, 이하의 기재 항목에 따라 행한다.

[0105] 1. 정보 기록 매체의 저장 데이터와, 드라이브 및 호스트에 있어서의 처리의 개요

[0106] 2. 컨텐츠 관리 유닛(CPS 유닛)에 대하여

[0107] 3. 변형 데이터를 포함하는 컨텐츠의 데이터 구성 및 데이터 변환 처리의 개요

[0108] 4. 컨텐츠 재생 처리

[0109] 5. 시큐리티 체크 코드를 적용한 처리

[0110] 6. 정보 처리 장치에 대한 암호 키 배포 구성과 컨텐츠 코드의 암호화 및 이용 처리 구성

[0111] 7. 정보 처리 장치의 구성

[0112] 8. 정보 기록 매체 제조 장치 및 정보 기록 매체

[0113] [1. 정보 기록 매체의 저장 데이터와, 드라이브 및 호스트에 있어서의 처리의 개요]

[0114] 먼저, 정보 기록 매체의 저장 데이터와, 드라이브 및 호스트에 있어서의 처리의 개요에 대하여 설명한다. 도 1에, 컨텐츠가 저장된 정보 기록 매체(100), 드라이브(120) 및 호스트(140)의 구성을 나타낸다. 호스트(140)는, 예를 들면, PC 등의 정보 처리 장치로 실행되는 데이터 재생(또는 기록) 어플리케이션이며, 소정의 데이터 처리 시퀀스에 따라 PC 등의 정보 처리 장치의 하드웨어를 이용한 처리를 행한다.

[0115] 정보 기록 매체(100)는, 예를 들면, Blu-ray Disc(상표), DVD 등의 정보 기록 매체이며, 정당한 컨텐츠 저작권, 또는 반포권을 가지는 이른바 컨텐츠 권리자의 허가 하에 디스크 제조 공장에서 제조된 정당한 컨텐츠를 저장한 정보 기록 매체(ROM 디스크 등), 또는 데이터 기록 가능한 정보 기록 매체(RE 디스크 등)이다. 그리

고, 이하의 실시예에서는, 정보 기록 매체의 예로서 디스크형의 매체를 예로서 설명하지만, 본 발명은 다양한 태양의 정보 기록 매체를 사용한 구성에서 적용가능하다.

[0116] 도 1에 나타낸 바와 같이, 정보 기록 매체(100)에는, 암호화 처리 및 일부 데이터의 치환 처리가 행해진 암호화 컨텐츠(101)와, 브로드캐스트 암호화 방식의 한 종류로서 알려진 트리 구조의 키 분배 방식에 따라 생성되는 암호 키 블록으로서의 MKB(Media Key Block)(102), 컨텐츠 복호 처리에 적용하는 타이틀 키를 암호화한 데이터(Encrypted CPS Unit Key) 등으로 구성되는 타이틀 키 파일(103), 컨텐츠의 카피·재생 제어 정보로서의 CCI(Copy Control Information) 등을 포함하는 사용 허락 정보(104), 암호화 컨텐츠(101)의 이용에 대하여 실행되는 데이터 처리 프로그램을 포함하는 컨텐츠 코드(105)가 저장된다.

[0117] 컨텐츠 코드(105)에는, 컨텐츠 중의 소정 영역의 치환 데이터에 대응하는 변환 데이터를 등록한 변환 테이블(Fix-up Table)(106)이 포함되고, 또한 컨텐츠 재생을 실행하는 플레이어(재생 장치)의 정당성 등을 검증하기 위한 프로그램 등에 의해 구성되는 시큐리티 체크 코드(107)가 포함된다.

[0118] 컨텐츠의 재생을 실행하는 정보 처리 장치는, 먼저, 컨텐츠 코드(105)에 포함되는 시큐리티 체크 코드(107)에 따라, 플레이어(재생 장치)의 정당성 등의 검증 처리를 실행하고, 검증 처리 후, 컨텐츠 코드(105)에 포함되는 데이터 변환 처리 프로그램에 따라 컨텐츠 코드(105)에 포함되는 변환 테이블(Fix-up Table)(106)에 기록된 변환 데이터를 인출하여, 컨텐츠의 구성 데이터의 치환 처리를 행한다.

[0119] 그리고, 변환 테이블(Fix-up Table)(106)이나, 시큐리티 체크 코드(107)에는, 다양한 재생 장치나 재생 어플리케이션 종류 등에 따른 처리, 즉 시큐리티 체크 처리나 변환 처리를 실행 가능하게 하기 위하여, 다양한 종류의 코드가 포함된다. 예를 들면, A사제의 플레이어에 대응하는 시큐리티 체크 코드, 변환 테이블, B사제의 플레이어에 대응하는 시큐리티 체크 코드, 변환 테이블 등이다. 컨텐츠를 이용하려고 하는 플레이어는, 이들 시큐리티 체크 코드나 변환 테이블로부터, 자기의 플레이어에 대응하는 시큐리티 체크 코드나 변환 테이블을 선택하여 처리를 실행하게 된다.

[0120] 이와 같이, 컨텐츠 코드(105)에는, 변환 데이터를 적용한 변환 처리 프로그램 외에, 스타트 업 처리나, 시큐리티 체크 처리 등의 다양한 처리를 실행하기 위한 정보나 프로그램이 포함된다. 컨텐츠 코드의 상세한 것에 대하여는, 후단에서 상세하게 설명한다. 그리고, 도면에 나타낸 정보 기록 매체의 저장 데이터 예는 일례이며, 저장 데이터는, 디스크의 종류 등에 따라 다소 상이하다. 이하, 이들 각종 정보의 개요에 대하여 설명한다.

[0121] (1) 암호화 컨텐츠(101)

[0122] 정보 기록 매체(100)에는, 다양한 컨텐츠가 저장된다. 예를 들면, 고정밀 동화상 데이터인 HD(High Definition) 무비 컨텐츠 등의 동영상 컨텐츠의 AV(Audio Visual)스트림이나 특정한 규격으로 규정된 형식의 게임 프로그램, 화상 파일, 음성 데이터, 텍스트 데이터 등을 포함하는 컨텐츠이다. 이들 컨텐츠는, 특정한 AV 포맷 규격 데이터이며, 특정한 AV 데이터 포맷에 따라 저장된다. 구체적으로는, 예를 들면, Blu-ray Disc(상표) ROM 규격 데이터로서, Blu-ray Disc(상표) ROM 규격 포맷에 따라 저장된다.

[0123] 또한, 예를 들면, 서비스 데이터로서의 게임 프로그램이나, 화상 파일, 음성 데이터, 텍스트 데이터 등이 저장되는 경우도 있다. 이들 컨텐츠는, 특정한 AV 데이터 포맷에 따르지 않는 데이터 포맷을 가지는 데이터로서 저장되는 경우도 있다.

[0124] 컨텐츠의 종류로서는, 음악 데이터, 동영상, 정지화상 등의 화상 데이터, 게임 프로그램, WEB 컨텐츠 등, 다양한 컨텐츠가 포함되고, 이들 컨텐츠에는, 정보 기록 매체(100)로부터의 데이터만에 의해 이용 가능한 컨텐츠 정보와, 정보 기록 매체(100)로부터의 데이터와, 네트워크 접속된 서버로부터 제공되는 데이터를 병행하여 이용 가능하게 되는 컨텐츠 정보 등, 다양한 태양의 정보가 포함된다. 정보 기록 매체에 저장되는 컨텐츠는, 구분 컨텐츠마다의 상이한 이용 제어를 실현하므로, 구분 컨텐츠마다 상이한 키(CPS 유닛 키 또는 유닛 키(또는 타이틀 키라고 하는 경우도 있다))가 할당되고 암호화되어 저장된다. 1개의 유닛 키를 할당하는 단위를 컨텐츠 관리 유닛(CPS 유닛)이라고 한다. 또한, 컨텐츠는, 구성 데이터의 일부가, 정확한 컨텐츠 데이터와 상이한 데이터에 의해 치환되어 변칙 데이터로서 설정되고, 복호 처리 만으로는 정확한 컨텐츠 재생이 실행되지 않고, 재생을 행하는 경우에는, 변칙 데이터를 변환 테이블에 등록된 데이터로 치환하는 처리가 필요하다. 이들 처리는 후단에서 상세하게 설명한다.

[0125] (2) MKB

[0126] MKB(매체 키 블록, Media Key Block)(102)는, 브로드캐스트 암호화 방식의 한 종류로서 알려진 트리 구조의 키

분배 방식에 따라 생성되는 암호 키 블록이다. MKB(102)는 유효한 라이센스를 가지는 사용자의 정보 처리 장치에 저장된 디바이스 키 [Kd] 에 따른 처리(복호)에 의해서만, 컨텐츠의 복호에 필요한 키인 미디어 키 [Km] 의 취득을 가능하게 하는 키 정보 블록이다. 이것은 이른바 계층형 트리 구조에 따른 정보 분배 방식을 적용한 것이며, 사용자 디바이스(정보 처리 장치)가 유효한 라이센스를 가지는 경우에만, 미디어 키 [Km] 의 취득을 가능하게 하고, 무효화(배제 처리)된 사용자 디바이스에 있어서는, 미디어 키 [Km] 의 취득이 불가능하게 된다.

[0127] 라이센스 엔티티(Entity)로서의 관리 센터는 MKB에 저장하는 키 정보의 암호화에 사용하는 디바이스 키의 변경에 의해, 특정한 사용자 디바이스에 저장된 디바이스 키에서는 복호할 수 없는, 즉 컨텐츠 복호에 필요한 미디어 키를 취득할 수 없는 구성을 가지는 MKB를 생성할 수 있다. 따라서, 임의 타이밍에서 부정 디바이스를 배제(revoke)하여, 유효한 라이센스를 가지는 디바이스에 대해서만 복호 가능한 암호화 컨텐츠를 제공하는 것이 가능해진다. 컨텐츠의 복호 처리에 대하여는 후술한다.

[0128] (3) 타이틀 키 파일

[0129] 전술한 바와 같이 각 컨텐츠 또는 복수개 컨텐츠의 집합은, 컨텐츠의 이용 관리를 위하여, 각각, 개별의 암호키(타이틀 키(CPS 유닛 키))를 적용한 암호화가 행해져 정보 기록 매체(100)에 저장된다. 즉, 컨텐츠를 구성하는 AV(Audio Visual)스트림, 음악 데이터, 동영상, 정지화상 등의 화상 데이터, 게임 프로그램, WEB 컨텐츠 등은, 컨텐츠 이용의 관리 단위로서의 유닛으로 구분되어, 구분된 유닛마다 상이한 타이틀 키를 생성하여, 복호 처리를 행하는 것이 필요하다. 이 타이틀 키를 생성하기 위한 정보가 타이틀 키 데이터이며, 예를 들면, 미디어 키 등에 의해 생성된 키로 암호화 타이틀 키를 복호함으로써 타이틀 키를 얻는다. 타이틀 키 데이터를 적용한 소정의 암호 키 생성 시퀀스에 따라, 각 유닛에 대응하는 타이틀 키가 생성되고, 컨텐츠의 복호가 실행된다.

[0130] (4) 사용 허락 정보

[0131] 사용 허락 정보에는, 예를 들면, 카피·재생 제어 정보(CCI)가 포함된다. 즉, 정보 기록 매체(100)에 저장된 암호화 컨텐츠(101)에 대응하는 이용 제어를 위한 카피 제한 정보나, 재생 제한 정보이다. 이 카피·재생 제어 정보(CCI)는, 컨텐츠 관리 유닛으로서 설정되는 CPS 유닛 개별의 정보로서 설정되는 경우나, 복수개의 CPS 유닛에 대응하여 설정되는 경우 등, 다양한 설정이 가능하다.

[0132] (5) 컨텐츠 코드

[0133] 컨텐츠 코드(105)는, 컨텐츠 중의 소정 영역의 치환 데이터에 대응하는 변환 데이터를 등록한 변환 테이블(Fix-up Table)(106)과, 컨텐츠 재생을 실행하는 플레이어(재생 장치)의 정당성 등을 검증하는 프로그램인 시큐리티 체크 코드(107)가 포함된다.

[0134] 전술한 바와 같이, 변환 테이블이나 시큐리티 체크 코드에는, 다양한 재생 장치로서의 플레이어의 종류에 따른 처리를 가능하게 하기 위하여, 다양한 종류의 코드가 포함된다. 컨텐츠를 이용하려고 하는 플레이어는, 자기의 플레이어에 대응하는 시큐리티 체크 코드나 변환 테이블을 선택하여 시큐리티 체크 처리와 데이터 변환 처리를 실행한다.

[0135] 컨텐츠 재생을 실행하는 재생 장치의 재생 어플리케이션로서의 호스트는, 데이터 변환 처리를 실행하는 버추얼 머신(VM)을 설정하고, 버추얼 머신(VM)에 있어서, 정보 기록 매체(100)로부터 판독한 컨텐츠 코드에 따라 시큐리티 체크 처리 및 데이터 변환 처리를 실행하여, 변환 테이블(Fix-up Table)(106)의 등록 엔트리를 적용하여, 컨텐츠의 일부 구성 데이터의 데이터 변환 처리를 실행한다.

[0136] 정보 기록 매체(100)에 저장된 암호화 컨텐츠(101)는, 소정의 암호화가 행해져 있는 동시에, 컨텐츠 구성 데이터의 일부가, 정확한 데이터와는 상이한 변칙 데이터(broken data)에 의해 구성되어 있다. 컨텐츠 재생을 행할 때는, 이 변칙 데이터를 정확한 컨텐츠 데이터인 변환 데이터로 치환하는 데이터 재기록 처리가 필요하다. 이 변환 데이터를 등록한 테이블이 변환 테이블(Fix-up Table)(106)이다. 변칙 데이터는 컨텐츠 중에 산재해 다수 설정되고, 컨텐츠 재생에 대해서는, 이들 복수개의 변칙 데이터를 변환 테이블에 등록된 변환 데이터로 치환(재기록)하는 처리가 필요하다. 이 변환 데이터를 적용함으로써, 예를 들면, 암호 키가 누출되어 컨텐츠의 복호가 부정으로 행해진 경우라도, 컨텐츠의 복호만으로는, 치환 데이터의 존재에 의해 정확한 컨텐츠의 재생이 불가능하게 되고, 부정한 컨텐츠 이용을 방지할 수 있다.

[0137] 그리고, 변환 테이블(106)에는, 통상의 변환 데이터뿐 아니라, 컨텐츠 재생 장치 또는 컨텐츠 재생 어플리케이션을 식별할 수 있게 한 식별 정보의 구성 비트를 해석 가능하게 하는 데이터를 포함하는 변환 데이터(Forensic Mark)가 포함된다. 구체적으로는, 예를 들면, 플레이어(호스트 어플리케이션을 실행하는 장치)의 식별 데이터

로서의 플레이어 ID 또는 플레이어 ID에 따라 생성된 식별 정보가 기록된 식별 마크를 포함하는 변환 데이터(Forensic Mark)가 포함된다. 식별 마크를 포함하는 변환 데이터는, 컨텐츠의 재생에 영향을 주지 않은 레벨로, 정확한 컨텐츠 데이터의 비트값을 약간 변경한 데이터이다.

[0138] 그리고, 컨텐츠 코드(105)에는, 전술한 변환 테이블(106)을 적용한 데이터 변환 처리 프로그램 외에, 스타트 업 처리나, 시큐리티 체크 처리 등의 다양한 처리를 실행하기 위한 정보나 프로그램이 포함된다. 컨텐츠 코드의 상세한 것에 대하여는, 후단에서 상세하게 설명한다.

[0139] 다음에, 호스트(140)와 드라이브(120)의 구성, 처리의 개요에 대하여, 도 1을 참조하여 설명한다. 정보 기록 매체(100)에 저장된 컨텐츠의 재생 처리는, 드라이브(120)를 통하여 호스트(140)에 데이터가 전송되어 실행된다.

[0140] 호스트(140)에는, 재생(플레이어) 어플리케이션(150)과 시큐어 VM(160)이 설정된다. 재생(플레이어) 어플리케이션(150)은, 컨텐츠 재생 처리부이며, 컨텐츠 재생 처리에 있어서 실행되는 드라이브와의 인증 처리, 컨텐츠 복호, 디코드 처리 등의 처리를 실행한다.

[0141] 시큐어 VM(160)은, 컨텐츠 코드(105)를 적용한 처리를 실행한다. 컨텐츠 코드(105)에는, 변환 테이블(106), 시큐리티 체크 코드(107)가 포함되고, 시큐어 VM(160)은, 자기의 플레이어에 대응하는 시큐리티 체크 코드(107)를 선택하여, 시큐리티 체크 처리를 실행하고, 또한 변환 테이블(106)을 이용한 컨텐츠의 일부 데이터의 치환 처리를 실행한다. 그리고, 시큐어 VM(160)은, 호스트(140) 내에 버추얼 머신으로서 설정된다. 버추얼 머신(VM)은 중간 언어를 직접 해석하여 실행하는 가상 컴퓨터이며, 플랫폼에 의존하지 않는 중간 언어에서의 명령 코드 정보를 정보 기록 매체(100)로부터 판독하여 해석을 실행한다.

[0142] 시큐어 VM(160)은, 정보 기록 매체(100)에 기록된 암호화 컨텐츠(101)의 이용에 적용하는 프로그램 또는 적용 정보를 포함하는 컨텐츠 코드(105)를 취득하여, 취득한 컨텐츠 코드(105)에 따라 데이터 처리를 실행하는 데이터 처리부로서 기능한다.

[0143] 시큐어 VM(160)은, 시큐어 VM이 액세스 가능한 메모리인 메모리 b(161)로부터 플레이어 정보를 취득하고, 플레이어 정보에 대응하는 컨텐츠 코드를 정보 기록 매체로부터 선택하여 실행한다. 그리고, 컨텐츠 코드의 일부는, 암호화 데이터로서 설정되어 있고, 이 암호화 데이터를 복호하기 위한 암호 키(노드 키)가 메모리 b(161)에 저장되어 있다. 시큐어 VM(160)은, 메모리 b(161)로부터 선택한 키를 적용하여 컨텐츠 코드의 복호 처리를 실행한다.

[0144] 메모리 b(161)에는, 계층 구성을 가지는 키 트리에 있어서, 정보 처리 장치에 대응시킨 최하층 노드로서의 리프로부터 정점 노드에 이르는 루트 상의 각 노드에 대응하여 설정된 노드 키를 포함하는 암호 키 세트가 저장되어 있다. 시큐어 VM(160)은, 컨텐츠 코드에 대응하는 키 지정 정보에 따라 메모리 b(161)로부터 노드 키를 선택하여 선택한 키를 적용하여 컨텐츠 코드의 복호 처리를 실행한다. 그리고, 메모리 b(161)에 저장되는 암호 키 세트의 상세, 및 시큐어 VM(160)을 실행하는 처리의 상세한 것에 대하여는 후단에서 설명한다.

[0145] 재생(플레이어) 어플리케이션(150)과 시큐어 VM(160)사이의 정보 전달, 또는 처리 요구는, 재생(플레이어) 어플리케이션(150)으로부터 시큐어 VM(160)에 대한 중간개입(INTRP)과 시큐어 VM(160)로부터 재생(플레이어) 어플리케이션(150)에 대한 응답(Call)처리의 시퀀스에 의해 실행된다. 어플리케이션(150)으로부터 시큐어 VM(160)에 대한 중간개입(INTRP)과 시큐어 VM(160)로부터 재생(플레이어) 어플리케이션(150)에 대한 응답(Call)처리의 시퀀스에 의해 행해진다.

[0146] 호스트(140)가 실행하는 주된 처리에 대하여 설명한다. 컨텐츠의 이용에 앞서, 드라이브(120)와 호스트(140) 사이에서는 상호 인증 처리가 실행되고, 이 인증 처리의 성립에 의해 양쪽의 정당성이 확인된 후, 드라이브로부터 호스트에게 암호화 컨텐츠가 전송되고, 호스트 측에서 컨텐츠의 복호 처리가 행해져, 전술한 변환 테이블에 의한 데이터 변환 처리가 실행되어 컨텐츠 재생이 행해진다.

[0147] 드라이브(120)의 데이터 처리부(121)는, 컨텐츠 이용에 대하여 실행되는 호스트와의 인증 처리, 또한 정보 기록 매체로부터의 데이터를 판독하고, 호스트로 데이터 전송 처리 등을 실행한다.

[0148] 호스트(140)의 재생(플레이나) 어플리케이션(150)은, 예를 들면, PC 등의 정보 처리 장치에서 실행되는 데이터 재생(또는 기록) 어플리케이션이며, 소정의 데이터 처리 시퀀스에 따라 PC 등의 정보 처리 장치의 하드웨어를 이용한 처리를 행한다.

[0149] 호스트(140)는, 드라이브(120)와의 상호 인증 처리나, 데이터 전송 제어 등을 실행하는 데이터 처리부(151), 암

호화 컨텐츠의 복호 처리를 실행하는 복호 처리부(153), 전술한 변환 테이블(105)의 등록 데이터에 따른 데이터 변환 처리를 실행하는 데이터 변환 처리부(154), 디코드(예를 들면, MPEG 디코드)처리를 실행하는 디코드 처리부(155)를 가진다.

[0150] 복호 처리부(153)에서는, 메모리 a(156)에 저장된 각종 정보, 및 정보 기록 매체(100)로부터의 판독 데이터를 적용하여, 컨텐츠의 복호에 적용하는 키를 생성하고, 암호화 컨텐츠(101)의 복호 처리를 실행한다. 데이터 변환 처리부(154)는, 정보 기록 매체(100)로부터 취득되는 데이터 변환 처리 프로그램에 따라, 정보 기록 매체(100)로부터 취득되는 변환 테이블에 등록된 변환 데이터를 적용하여 컨텐츠의 구성 데이터의 치환 처리(재기록)를 실행한다. 디코드 처리부(155)는, 디코드(예를 들면, MPEG 디코드) 처리를 실행한다.

[0151] 정보 처리 장치(150)의 메모리 a(156)에는, 디바이스 키(Kd)나, 상호 인증 처리에 적용하는 키 정보나 복호에 적용하는 키 정보 등이 저장된다. 그리고, 컨텐츠의 복호 처리의 상세한 것에 대하여는 후술한다. 디바이스 키(Kd)는, 먼저 설명한 MKB의 처리에 적용하는 키이다. MKB는 유효한 라이센스를 가지는 사용자의 정보 처리 장치에 저장된 디바이스 키 [Kd] 에 따른 처리(복호)에 의해서만, 컨텐츠의 복호에 필요한 키인 미디어 키 [Km] 의 취득을 가능하게 하는 키 정보 블록이며, 암호화 컨텐츠의 복호에 대하여, 정보 처리 장치(150)는, 메모리 a(156)에 저장된 디바이스 키(Kd)를 적용하여 MKB의 처리를 실행하게 된다. 그리고, 컨텐츠의 복호 처리의 상세한 것에 대하여는 후술한다.

[0152] [2. 컨텐츠 관리 유닛(CPS 유닛)에 대하여]

[0153] 전술한 바와 같이, 정보 기록 매체에 저장되는 컨텐츠는, 유닛마다의 상이한 이용 제어를 실현하므로 유닛마다 상이한 키가 할당되고 암호화 처리가 행해져 저장된다. 즉, 컨텐츠는 컨텐츠 관리 유닛(CPS 유닛)으로 구분되어, 개별의 암호화 처리가 행해지고, 개별의 이용 관리가 행해진다.

[0154] 컨텐츠 이용에 대해서는, 먼저, 각 유닛에 할당된 CPS 유닛 키(타이틀 키 라고도 한다)를 취득하는 것이 필요하고, 또한 그 외의 필요한 키, 키 생성 정보 등을 적용하여 미리 정해진 복호 처리 시퀀스에 따른 데이터 처리를 실행하여 재생을 행한다. 컨텐츠 관리 유닛(CPS 유닛)의 설정 태양에 대하여, 도 2를 참조하여 설명한다.

[0155] 도 2에 나타낸 바와 같이, 컨텐츠는, (A) 인덱스(210), (B) 무비 오브젝트(220), (C) 플레이 리스트(230), (D) 클립(240)의 계층 구성을 가진다. 재생 어플리케이션에 의해 액세스되는 타이틀 등의 인덱스를 지정하면, 예를 들면, 타이틀에 관련된 재생 프로그램이 지정되어, 지정된 재생 프로그램의 프로그램 정보에 따라 컨텐츠의 재생 순서 등을 규정하고 플레이 리스트가 선택된다.

[0156] 플레이 리스트에는, 재생 대상 데이터 정보로서의 플레이 아이템이 포함된다. 플레이 리스트에 포함되는 플레이 아이템에 의해 규정되는 재생 구간으로서의 클립 정보에 의해, 컨텐츠 실(實)데이터로서의 AV 스트림 또는 커맨드가 선택적으로 판독되어, AV 스트림의 재생, 커맨드의 실행 처리가 행해진다. 그리고, 플레이 리스트, 플레이 아이템은 다수 존재하고, 각각에 식별 정보로서의 플레이 리스트 ID, 플레이 아이템 ID가 대응하고 있다.

[0157] 도 2에는, 2개의 CPS 유닛을 나타내고 있다. 이들은, 정보 기록 매체에 저장된 컨텐츠의 일부를 구성하고 있다. CPS 유닛 1(271), CPS 유닛 2(272)의 각각은, 인덱스로서의 타이틀과 재생 프로그램 파일로서의 무비 오브젝트와 플레이 리스트와 컨텐츠 실데이터로서의 AV 스트림 파일을 포함하는 클립을 포함하는 유닛으로서 설정된 CPS 유닛이다.

[0158] 컨텐츠 관리 유닛 1(CPS 유닛 1)(271)에는, 타이틀 1(211)과 타이틀 2(212), 재생 프로그램(221, 222), 플레이 리스트(231, 232), 클립(241, 242)이 포함되고, 이들 2개의 클립(241, 242)에 포함되는 컨텐츠의 실데이터인 AV 스트림 데이터 파일(261, 262)이, 적어도 암호화 대상 데이터이며, 원칙적으로 컨텐츠 관리 유닛 1(CPS 유닛 1)(271)에 대응시켜 설정되는 암호 키인 타이틀 키(Kt1)(CPS 유닛 키 라고도 한다)를 적용하여 암호화된 데이터로서 설정된다.

[0159] 컨텐츠 관리 유닛 2(CPS 유닛 2)(272)에는, 인덱스로서 어플리케이션 1(213), 재생 프로그램(224), 플레이 리스트(233), 클립(243)이 포함되고, 클립(243)에 포함되는 컨텐츠의 실데이터인 AV 스트림 데이터 파일(263)이 컨텐츠 관리 유닛 2(CPS 유닛 2)(272)에 대응시켜 설정되는 암호 키인 타이틀 키(Kt2)를 적용하여 암호화된다.

[0160] 예를 들면, 사용자가 컨텐츠 관리 유닛 1(271)에 대응하는 어플리케이션 파일 또는 컨텐츠 재생 처리를 실행하기 위해서는, 컨텐츠 관리 유닛 1(CPS 유닛 1)(271)에 대응시켜 설정된 암호 키로서의 타이틀 키(Kt1)를 취득

하여 복호 처리를 실행하는 것이 필요하다. 컨텐츠 관리 유닛 2(272)에 대응하는 어플리케이션 파일 또는 컨텐츠 재생 처리를 실행하기 위해서는, 컨텐츠 관리 유닛 2(CPS 유닛 2)(272)에 대응시켜 설정된 암호 키로서의 타이틀 키(Kt2)를 취득하여 복호 처리를 실행하는 것이 필요하다.

[0161] CPS 유닛의 설정 구성, 및 타이틀 키의 대응예를 도 3에 나타낸다. 도 3에는, 정보 기록 매체에 저장되는 암호화 컨텐츠의 이용 관리 단위로서의 CPS 유닛 설정 단위와 각 CPS 유닛에 적용하는 타이틀 키(CPS 유닛 키)의 대응을 나타내고 있다. 그리고, 미리 후발 데이터용의 CPS 유닛 및 타이틀 키를 저장하고 설정하여 두는 일도 가능하다. 예를 들면, 데이터부(281)가 후발 데이터용의 엔트리이다.

[0162] CPS 유닛 설정 단위는, 컨텐츠의 타이틀, 어플리케이션, 데이터 그룹 등, 여러 가지이고, CPS 유닛 관리 테이블에는, 각각의 CPS 유닛에 대응하는 식별자로서의 CPS 유닛 ID가 설정된다.

[0163] 도 3에 있어서, 예를 들면, 타이틀 1은 CPS 유닛 1이며, CPS 유닛 1에 속하는 암호화 컨텐츠의 복호에 대해서는, 타이틀 키 Kt1을 생성하고, 생성한 타이틀 키 Kt1에 따른 복호 처리를 행하는 것이 필요로 된다.

[0164] 이와 같이, 정보 기록 매체(100)에 저장되는 컨텐츠는, 유닛마다의 상이한 이용 제어를 실현하므로 유닛마다 상이한 키가 할당되고 암호화 처리가 행해져 저장된다. 각 컨텐츠 관리 유닛(CPS 유닛)에 대한 개별의 이용 관리를 위하여, 각 컨텐츠 관리 유닛(CPS 유닛)에 대한 사용 허락 정보(UR: Usage Rule)가 설정되어 있다. 사용 허락 정보는, 전술한 바와 같이, 컨텐츠에 대한 예를 들면, 카피·재생 제어 정보(CCI)를 포함하는 정보이며, 각 컨텐츠 관리 유닛(CPS 유닛)에 포함되는 암호화 컨텐츠의 카피 제한 정보나, 재생 제한 정보이다.

[0165] 그리고, 타이틀 키의 생성에는, 정보 기록 매체에 저장된 다양한 정보를 적용한 데이터 처리가 필요하다. 이들 처리의 구체예에 대하여는 후단에서 상세하게 설명한다.

[0166] [3. 변형 데이터를 포함하는 컨텐츠의 데이터 구성 및 데이터 변환 처리의 개요]

[0167] 다음에, 변형 데이터를 포함하는 컨텐츠의 구성 및 데이터 변환 처리의 개요에 대하여 설명한다. 정보 기록 매체(100)에 포함되는 암호화 컨텐츠(101)는, 전술한 바와 같이, 구성 데이터의 일부가, 정확한 컨텐츠 데이터와는 상이한 데이터에 의해 치환된 변칙 데이터로서 설정되고, 복호 처리 만으로는 정확한 컨텐츠 재생이 실행되지 않게 되어, 재생을 행하는 경우에는, 변칙 데이터를 변환 테이블에 등록된 변환 데이터로 치환하는 처리가 필요하다.

[0168] 도 4를 참조하여, 정보 기록 매체에 저장되는 컨텐츠의 구성 및 재생 처리의 개요에 대하여 설명한다. 정보 기록 매체(100)에는 예를 들면, 영화 등의 AV(Audio Visual)컨텐츠가 저장된다. 이들 컨텐츠는 암호화가 행해지고, 소정의 라이센스를 가지는 재생 장치에 있어서만 취득 가능한 암호 키를 적용한 처리에 의해 복호한 뒤, 컨텐츠 재생이 가능해진다. 구체적인 컨텐츠 재생 처리에 대하여는 후단에서 설명한다. 정보 기록 매체(100)에 저장되는 컨텐츠는, 암호화뿐 아니라, 컨텐츠의 구성 데이터가 변형 데이터에 의해 치환된 구성을 가진다.

[0169] 도 4에는, 정보 기록 매체(100)에 저장되는 기록 컨텐츠(291)의 구성예를 나타내고 있다. 기록 컨텐츠(291)는 변형이 되어 있지 않은 정상적인 컨텐츠 데이터(292)와, 변형이 가하여져 파괴된 컨텐츠인 변칙 데이터(293)에 의해 구성된다. 변칙 데이터(293)는, 본래의 컨텐츠에 대하여 데이터 처리에 의해 파괴가 행해진 데이터이다. 따라서, 이 변칙 데이터를 포함하는 컨텐츠(291)를 적용하여 정상적인 컨텐츠 재생은 실행할 수 없다.

[0170] 컨텐츠 재생을 행하기 위해서는, 기록 컨텐츠(291)에 포함되는 변칙 데이터(293)를 정상적인 컨텐츠 데이터로 치환하는 처리를 행하고 재생 컨텐츠(296)를 생성하는 것이 필요하다. 각 변칙 데이터 영역에 대응하는 정상적인 컨텐츠 데이터로서의 변환용의 데이터(변환 데이터)는, 정보 기록 매체(100)에 기록된 컨텐츠 코드(105) 내의 변환 테이블(FUT(Fix-Up Table))(106)(도 1 참조)에 등록된 변환 엔트리(295)로부터 변환 데이터를 취득하여, 변칙 데이터 영역의 데이터를 치환하는 처리를 실행하여, 재생 컨텐츠(296)를 생성하여 재생을 실행한다.

[0171] 그리고, 재생 컨텐츠(296)의 생성을 행할 때에는, 변칙 데이터(293)를 정상적인 컨텐츠 데이터로서의 변환 데이터(297)로 치환하는 처리뿐 아니라, 기록 컨텐츠(291)의 일부 영역을, 컨텐츠 재생 장치 또는 컨텐츠 재생 어플리케이션을 식별 할 수 있는 식별 정보(예를 들면, 플레이어 ID)의 구성 비트를 해석 가능하게 한 데이터(Forensic Mark)를 포함하는 식별자 설정 변환 데이터(298)에 의해 치환하는 처리를 행한다. 예를 들면, 부정으로 카피된 컨텐츠가 유출된 경우, 유출 컨텐츠 중의 식별자 설정 변환 데이터(298)의 해석에 의해, 부정 컨텐

츠의 유출원을 특정하는 것이 가능해진다.

[0172] 그리고, 변환 데이터를 포함하는 변환 테이블의 구성 데이터로서의 변환 엔트리는, 컨텐츠의 구성 데이터 내의 특정 패킷에 분산되어 중복 기록하는 구성으로 해도 된다. 즉, 변환 데이터는, 도 1에 나타낸 변환 테이블(106)에 저장되는 동시에, 암호화 컨텐츠(101)에도 분산 기록되고, 중복되어 기록된다. 컨텐츠 재생을 실행하는 정보 처리 장치는, 변환 테이블(106)에 저장된 변환 데이터를 취득하여 데이터 치환을 실행할 것인지, 또는 컨텐츠에 분산 기록된 변환 엔트리를 취득하여 데이터 치환을 실행할 것인지 중 어느 하나의 처리를 행한다.

[0173] [4. 컨텐츠 재생 처리]

[0174] 다음에, 도 5를 참조하여, 호스트가 실행하는 컨텐츠 재생 처리에 대하여 설명한다. 도 5에는, 좌측으로부터 암호화 컨텐츠가 저장된 정보 기록 매체(330), 정보 기록 매체(330)를 세트하고, 데이터의 판독을 실행하는 드라이브(340), 드라이브와 데이터 통신 가능하게 접속되고, 정보 기록 매체(330)에 저장된 컨텐츠를 드라이브(340)를 통하여 취득하여 재생 처리를 실행하는 재생 어플리케이션을 실행하는 호스트(345)를 나타내고 있다.

[0175] 그리고, 도 5에 나타낸 호스트(345)는, 컨텐츠의 복호, 디코드, 데이터 변환 처리 등을 실행하는 재생(플레이어) 어플리케이션 블록(350)과, 정보 기록 매체에 기록된 컨텐츠 코드에 포함되는 시큐리티 체크 코드에 따른 시큐리티 체크 처리 및 변환 테이블에 따른 변환 처리에 적용하는 파라미터 산출 처리 등을 실행하는 시큐어 VM(360)을 가지는 시큐어 VM(360) 블록을 구분하여 나타내고 있다.

[0176] 정보 기록 매체(330)는, MKB(Media Key Block)(331), 타이틀 키 파일(332), 암호화 컨텐츠(333), 컨텐츠 코드(334)를 기록 데이터로서 포함한다. 암호화 컨텐츠(333)는, 먼저, 도 4를 참조하여 설명한 바와 같이, 일부를 변환 테이블로부터 취득하는 데이터로 치환할 필요가 있는 컨텐츠이다.

[0177] 컨텐츠 코드(334)에는, 컨텐츠 재생을 실행하는 플레이어(재생 장치)의 정당성 등을 검증하기 위한 프로그램 등에 의해 구성되는 시큐리티 체크 코드(335)와, 컨텐츠 중의 소정 영역의 치환 데이터에 대응하는 변환 데이터를 등록한 변환 테이블(Fix-up Table)(336)이 포함된다. 호스트(345)는, MKB의 처리에 적용하는 디바이스 키(351)를 유지하고 있다.

[0178] 도 5에 나타낸 호스트(345)가 드라이브(340)를 통하여 정보 기록 매체(330)의 저장 컨텐츠를 취득하여 재생하는 처리 시퀀스에 대하여 설명한다. 먼저, 정보 기록 매체(330)의 저장 컨텐츠의 판독에 앞서, 호스트(345)와 드라이브(340)는, 스텝 S101에 있어서, 상호 인증을 실행한다. 이 상호 인증은, 호스트 및 드라이브가 각각 정당한 기기 또는 어플리케이션 소프트 인가를 확인하는 처리이다. 이 상호 인증 처리 시퀀스로서는, 다양한 처리가 적용가능하다. 상호 인증 처리에 의해, 드라이브(340)와 호스트(345)는 공통의 비밀키로서의 세션 키(Ks)를 공유한다.

[0179] 스텝 S101에 있어서, 호스트와 드라이브 사이의 상호 인증이 실행되고, 세션 키(Ks)를 공유한 후, 호스트(345)의 재생(플레이어) 어플리케이션(350)은, 스텝 S102에 있어서, 정보 기록 매체(330)에 기록된 MKB(331)를, 드라이브를 통하여 취득하여, 메모리에 저장된 디바이스 키(351)를 적용한 MKB(331)의 처리를 실행하여, MKB로부터 미디어 키(Km)를 취득한다.

[0180] 전술한 바와 같이, MKB(Media Key Block)(331)는, 브로드캐스트 암호화 방식의 한 종류로서 알려진 트리 구조의 키 분배 방식에 따라 생성되는 암호 키 블록이며, 유효한 라이센스를 가지는 장치에 저장된 디바이스 키(Kd)에 따른 처리(복호)에 의해서만, 컨텐츠의 복호에 필요한 키인 미디어 키(Km)의 취득을 가능하게 하는 키 정보 블록이다.

[0181] 다음에, 스텝 S103에 있어서, 스텝 S102에 있어서의 MKB 처리로 취득한 미디어 키(Km)를 적용하여, 정보 기록 매체(330)로부터 판독한 타이틀 키 파일(332)의 복호를 실행하여, 타이틀 키(Kt)를 취득한다. 정보 기록 매체(330)에 저장되는 타이틀 키 파일(332)은 미디어 키에 의해 암호화된 데이터를 포함하는 파일이며, 미디어 키를 적용한 처리에 의해 컨텐츠 복호에 적용하는 타이틀 키(Kt)를 취득할 수 있다. 그리고, 스텝 S103의 복호 처리는, 예를 들면, AES 암호 알고리즘이 적용된다.

[0182] 다음에, 호스트(345)의 재생(플레이어) 어플리케이션(350)은, 드라이브(340)를 통하여 정보 기록 매체(330)에 저장된 암호화 컨텐츠(333)를 판독하여, 트랙 버퍼(352)에 판독 컨텐츠를 저장하고, 이 버퍼 저장 컨텐츠에 대하여, 스텝 S104에 있어서, 타이틀 키(Kt)를 적용한 복호 처리를 실행하고, 복호 컨텐츠를 취득한다.

[0183] 복호 컨텐츠는, 평문 TS(Plain TS) 버퍼(353)에 저장한다. 평문 TS는 복호된 평문 트랜스포트 스트림을 의미한다. 여기서, 평문 TS 버퍼(353)에 저장되는 복호 컨텐츠는, 전술한 변칙 데이터를 포함하는 컨텐츠이며, 이대로는 재생하지 못하고, 소정의 데이터 변환(재기록에 의한 데이터 치환)을 행할 필요가 있다.

[0184] 스텝 S105에 있어서, 시큐어 VM(361)은, 데이터 변환에 필요한 파라미터 등을 컨텐츠 코드(334)로부터 생성하는 처리를 실행한다. 그 후, 스텝 S106에 있어서, 리얼타임 이벤트 핸들러(356)의 제어에 의해, 테이블 복원 & 데이터 변환 처리가 실행된다. 리얼타임 이벤트 핸들러(356)의 제어에 의해, 재생(플레이어) 어플리케이션(350)은, 컨텐츠의 구성 데이터로서의 세그먼트의 전환에 따라 파라미터 산출 요구를 시큐어 VM(361)에 중간개입(INTRP)으로서 출력하고, 시큐어 VM(361)으로부터 파라미터를, 차례로 수령하고, 변환 테이블 블록의 복호 또는 연산을 실행하여 평문 변환 테이블 블록을 취득하고, 취득한 변환 테이블 블록에 포함되는 변환 엔트리를 취득한다.

[0185] 변환 엔트리에는, 변환 데이터, 즉,

[0186] (a) 변환 데이터

[0187] (b) 식별자 설정 변환 데이터(Forensic Mark)

[0188] 와, 이들 변환 데이터의 컨텐츠에서의 기록 위치 지정 정보가 기록되어 있고, 재생(플레이어) 어플리케이션(350)은, 스텝 S106에 있어서, 지정 위치에 기록하는 데이터 변환 처리를 컨텐츠 재생 처리 또는 외부 출력 처리에 병행한 리얼 타임 처리로서 실행한다.

[0189] 시큐어 VM(361)은, 예를 들면, 컨텐츠의 구성 데이터로서의 세그먼트마다 적용하는 상이한 파라미터를, 컨텐츠 코드에 따라 생성하여 출력한다. 예를 들면, 파라미터(SP1, SP2, SP3・・・)가 소정의 컨텐츠 부분 데이터 단위인 세그먼트에 대응하는 변환 엔트리와의 배타 논리합(XOR) 연산 파라미터인 경우, 스텝 S303에 있어서의 테이블 복원 처리로서는,

[0190] [변환 엔트리 1](XOR) [SP1] ,

[0191] [변환 엔트리 2](XOR) [SP2] ,

[0192] [변환 엔트리 3](XOR) [SP3] ,

[0193] : :

[0194] 이들 배타 논리합 연산 처리를 실행하여, 변환 테이블 블록 데이터에 포함되는 변환 엔트리를 취득한다. 그리고, 상기 식에 있어서, [A] (XOR) [B] 는, A와 B의 배타 논리합 연산을 의미하는 것으로 한다.

[0195] 이와 같이, 정보 기록 매체에 기록된 컨텐츠(333)에 포함되는 변환 엔트리는, 파라미터(SP1, SP2, SP3・・・)와 배타 논리합 연산되어 저장되어 있다. 이 파라미터는, 시큐어 VM(361)에 의해 순서대로, 취득되고 출력된다.

[0196] 스텝 S106의 테이블 복원 & 데이터 변환 처리에 있어서는, 파라미터(SP1, SP2, SP3・・・)를 적용한 연산 또는 암호 처리에 의해, 취득한 복원된 변환 엔트리로부터 변환 데이터를 취득하여, 컨텐츠에 포함되는 변칙 데이터를 정당한 컨텐츠 구성 데이터인 변환 데이터로 치환하고, 또한 식별자 설정 변환 데이터를 컨텐츠의 일부 데이터와 교체하는 데이터 재기록 처리를 실행하고, 평문 TS 버퍼(353)의 저장 데이터를 변환 처리된 데이터로 변경한다. 이 데이터 변환 처리의 개요에 대하여, 도 6을 참조하여 설명한다.

[0197] 정보 기록 매체에 저장된 암호화 컨텐츠(333)가, 일단, 호스트 측의 트랙 버퍼(352)에 저장된다. 도 6 중 (1)은 트랙 버퍼 저장 데이터(401)를 나타낸다. 호스트 측의 복호 처리에 의해, 트랙 버퍼 저장 데이터(401)로서의 암호화 컨텐츠의 복호가 실행되어, 복호 결과 데이터가 평문 TS 버퍼(353)에 저장된다. 도 6 중 (2)는 복호 결과 데이터(402)를 나타낸 것이다.

[0198] 복호 결과 데이터(402)에는, 정상적인 컨텐츠 구성 데이터가 아닌, 변칙 데이터(403)가 포함된다. 호스트의 데이터 변환 처리부는, 이 변칙 데이터(403)를, 정확한 컨텐츠 구성 데이터로서의 변환 데이터(404)로 치환하는 처리를 실행한다. 이 치환 처리는, 예를 들면, 평문 TS 버퍼(353)에 기록된 데이터에 대한 일부 데이터의 재기록 처리로서 실행된다.

[0199] 또한, 호스트가 실행하는 데이터 변환 처리는, 변칙 데이터를 정상적인 컨텐츠 데이터인 변환 데이터로 치환하는 처리뿐만 아니라, 도 6에 나타낸 바와 같이, 식별자 설정 변환 데이터(405)에 의해, 복호 결과 데이터(402)의 일부 구성 데이터를 치환하는 처리를 실행한다.

[0200] 식별자는, 전술한 바와 같이 컨텐츠 재생 장치 또는 컨텐츠 재생 어플리케이션을 식별할 수 있게 한 식별 정보의 구성 비트를 해석 가능하게 한 데이터이다. 구체적으로는 예를 들면, 호스트 어플리케이션을 실행하는 플레이어로서의 정보 처리 장치의 식별 정보(플레이어 ID)의 구성 데이터 또는, 플레이어 ID에 따라 생성되는 식별 마크이다. 식별자 설정 변환 데이터는, 먼저 설명한 바와 같이 컨텐츠의 재생에 영향을 주지 않은 레벨로, 정확한 컨텐츠 데이터의 비트값을 약간 변경한 데이터이다.

[0201] 식별자 설정 변환 데이터(405)는, 컨텐츠 중에 다수 설정되고, 이들 복수개의 식별자 설정 변환 데이터(405)를 집적해 해석함으로써, 예를 들면, 플레이어 ID가 판별된다. 식별자 설정 변환 데이터(405)는, 컨텐츠로서 통상 재생 가능한 레벨로 정상 컨텐츠 데이터의 구성 비트를 변경한 데이터이며, MPEG 비트 스트림 해석에 의해 비트(식별 마크 구성 비트)판별이 가능한 데이터이다.

[0202] 정보 기록 매체에 저장되는 변환 테이블에는, 도 6에 나타낸 변환 데이터(404), 식별자 설정 변환 데이터(405)가 다수 등록되어 있고, 또한 이들 기록 위치 정보에 대해도 등록되어 있다. 이 변환 테이블 저장 정보에 따른 데이터 변환 처리를 실행함으로써, 평문 TS 버퍼(353)에 저장된 데이터는, 도 6 중 (3)에 나타낸 변환 처리된 데이터(406)로 치환되게 된다.

[0203] 그 후, 변환된 TS(트랜스포트 스트림)는, 네트워크 등을 통하여 외부로 출력되고, 외부의 재생기기에서 재생된다. 또는, 스텝 S107에 있어서, 디멀티플렉서에 의한 처리에 의해, 트랜스포트 스트림(TS)으로부터 엔리멘트리 스트림(ES)으로의 변환이 실행되고, 또한 디코드 처리(스텝 S108)가 행해진 후, 디스플레이 스피커를 통하여 재생된다.

[0204] [5. 시큐리티 체크 코드를 적용한 처리]

[0205] 전술한 컨텐츠 재생 처리의 개시 전에, 시큐어 VM(361)은, 컨텐츠 코드(334) 중의 시큐리티 체크 코드(335)를 적용한 시큐리티 체크를 실행한다. 그리고, 시큐어 VM(361)은, 또한 필요에 따라 컨텐츠 재생 처리의 실행 기간에 있어서도 시큐리티 체크 코드(335)를 적용한 시큐리티 체크를 실행한다.

[0206] 시큐어 VM(361)은, 이벤트 핸들러(354)의 제어 하에, 컨텐츠 코드(334)에 포함되는 시큐리티 체크 코드(335)에 따라 플레이어(재생 장치)의 정당성 등의 검증 처리를 실행한다. 그리고, 전술한 바와 같이, 변환 테이블(Fix-up Table)(336)이나 시큐리티 체크 코드(335)는, 재생 장치로서의 플레이어의 종류에 따른 처리를 실행 가능하게 하기 위하여, 다양한 종류의 코드를 포함하는 설정으로 된다.

[0207] 시큐어 VM(361)은, 플레이어 정보(355)로서 재생 장치의 기억부에 저장된 플레이어 증명서(Player Certificate)나, 플레이어 구성, 예를 들면, 재생 장치가 가지는 포트에 관한 정보 등의 플레이어 구성 정보 등을 취득하여, 컨텐츠 코드(334) 중에 포함되는 시큐리티 체크 코드(335)로부터, 자기의 플레이어에 대응하는 시큐리티 체크 코드를 선택하여, 시큐리티 체크 처리를 실행한다. 즉, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보 또는 속성 정보 중 적어도 어느 하나를 플레이어 정보로서 취득하고, 이와 같은 플레이어 정보에 대응하는 시큐리티 체크 코드를 선택하여, 선택 코드에 따른 시큐리티 체크 처리를 실행한다.

[0208] 이와 같이, 정보 기록 매체에 저장되는 컨텐츠를 이용하는 경우에는, 시큐어 VM(361)에 있어서 시큐리티 체크가 실행된다. 시큐어 VM(361)에서의 시큐리티 체크에 있어서 컨텐츠의 이용이 허용된 정당한 기기인 것이 증명되고, 또한, 부정한 컨텐츠의 외부 출력 등이 행해지지 않은 것을 기기 구성 정보 등에 따라서, 검증한 후, 컨텐츠의 재생이 행해지게 된다.

[0209] 이와 같은 시큐리티 체크는, 재생 장치의 구성, 재생 어플리케이션의 종류 등에 따라 상이한 처리가 요구되는 경우가 있고, 그러므로, 시큐리티 체크 코드는, 다양한 기기나 어플리케이션에 대응한 코드의 세트로서 컨텐츠 코드 중에 기록되어 있다.

[0210] 정보 기록 매체에서의 컨텐츠 코드의 기록 태양에 대하여, 도면을 참조하여 설명한다. 도 7은, 정보 기록 매체에 저장되는 데이터 전체의 디렉토리 구성을 나타낸 도면이다. 정보 기록 매체의 저장 데이터는, 크게 2개의 데이터로 구분된다. 하나는, 컨텐츠 관리 데이터, CPS 유닛 키, 컨텐츠 이용 제어 정보(CCI), 컨텐츠 등을 포함하는 컨텐츠 관련 데이터를 설정한 BDMV 디렉토리와, 시큐리티 체크 코드, 변환 테이블 등을 포함하는 컨텐츠 코드를 설정한 BDSVM 디렉토리를 가진다.

[0211] 이들 각 디렉토리의 상세예에 대하여, 도 8, 도 9를 참조하여 설명한다. 먼저, 도 2를 참조하여 설명한 계층 구조를 가지는 컨텐츠를 정보 기록 매체에 저장하는 경우, 다양한 데이터, 또는 컨텐츠 코드 등의 프로그램 등

은, 개별의 파일로서 기록되고, 예를 들면, 도 8에 나타낸 디렉토리 설정에 따라 정보 기록 매체에 저장된다.

[0212] (A) 도 2에 있어서의 인덱스(210)는 도 8에 나타낸 디렉토리 중의 index.bdmv 파일

[0213] (B) 도 2에 있어서의 무비 오브젝트(220)는 도 8에 나타낸 디렉토리 중의 MovieObject.bdmv 파일

[0214] (C) 도 2에 있어서의 플레이 리스트(230)는 도 8에 나타낸 디렉토리 중의 PLAYLIST 디렉토리 하의 파일,

[0215] (D) 도 2에 있어서의 클립(240)은 도 8에 나타낸 디렉토리 중의 CLIPINF 디렉토리 하의 파일과 STREAM 디렉토리 하의 파일에서 같은 파일 번호 가지는 것의 쌍에 대응한다.

[0216] (E) 그 외에, 음성 데이터나 폰트 데이터를 저장한 AUXDATA 파일, 메타 데이터를 저장한 META 파일, BD-J오브젝트를 저장한 BDOJ 파일 등이 정보 기록 매체에 저장된다.

[0217] 정보 기록 매체에 저장되는 컨텐츠는, 전술한 바와 같이, 컨텐츠의 구성 데이터의 일부가, 정확한 컨텐츠 데이터와는 상이한 데이터에 의해 치환된 변칙 데이터로서 설정되고, 복호 처리 만으로는 정확한 컨텐츠 재생이 실행되지 않아, 재생을 행하는 경우에는, 변칙 데이터를 변환 테이블에 등록된 데이터(변환 데이터)로 치환하는 처리가 필요하다. 이 치환 처리에는, 정보 기록 매체에 저장된 컨텐츠 코드를 적용하여, 변환 테이블(Fix-up Table)의 등록 데이터에 의한 데이터 변환 처리를 실행한다.

[0218] 이 변환 테이블, 및 시큐리티 체크 코드를 포함하는 컨텐츠 코드에 대해서도, 개별의 파일로서 정보 기록 매체에 저장된다. 컨텐츠 코드를 설정한 디렉토리 구성을 도 9에 나타낸다. 도 9는, 예를 들면, 도 8의 디렉토리 구조를 가지는 AV 컨텐츠에 대하여 작성되는 컨텐츠 코드의 디렉토리 구성이다.

[0219] 컨텐츠 코드는, 전술한 바와 같이 시큐리티 체크 코드와 변환 테이블을 포함한다. 정보 기록 매체에 저장되는 컨텐츠 코드는, 도 9에 나타낸 바와 같이, BDSVM 디렉토리에 설정된 복수개의 개별 파일 [nnnnn.svm] 에 저장된다. 또한, BACKUP 디렉토리에 카피 데이터로서의 백업 데이터가 설정된다.

[0220] 이들 컨텐츠 코드의 각각의 파일은, 예를 들면,

[0221] (a) 전(全) 컨텐츠 및 전(全) 플레이어(장치 또는 재생 어플리) 공통의 컨텐츠 코드

[0222] (b) 컨텐츠 고유의 컨텐츠 코드

[0223] (c) 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드

[0224] (d) 컨텐츠 & 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드

[0225] 등의 각 카테고리로 분류된다.

[0226] 상기의 (a) ~ (d)의 카테고리 분류로 함으로써, 컨텐츠 코드는, 각각 독립된 데이터 파일로서 설정 가능하며, 이들 컨텐츠 코드 파일은, 재이용 가능하다. 즉, 상이한 컨텐츠나 상이한 플레이어(장치 또는 재생 어플리케이션)에 대해도 공통으로 이용 가능한 경우가 있다. 이와 같은 컨텐츠 코드의 재이용 구성에 대하여, 도 10을 참조하여 설명한다.

[0227] 도 10에 있어서, 예를 들면, 컨텐츠 코드 파일(601~604)은, 각 컨텐츠 코드 제작 엔티티 또는 제공 엔티티가 유지하는 컨텐츠 코드 파일이며, 각각,

[0228] 컨텐츠, 플레이어 공통 컨텐츠 코드 파일 [00000.svm] (601),

[0229] 플레이어 고유 컨텐츠 코드 파일 [00001.svm] [00002.svm] (602),

[0230] 컨텐츠 고유 컨텐츠 코드 파일 [00003.svm] (603),

[0231] 컨텐츠, 플레이어 고유 컨텐츠 코드 파일 [00004.svm] (604),

[0232] 이들 컨텐츠 코드 파일을 나타내고 있다.

[0233] 이들 컨텐츠 코드 파일(601~604)에는, 각 컨텐츠 코드 제작 엔티티 또는 제공 엔티티에 의한 전자 서명이 부여되어, 각 엔티티에서 보관된다.

[0234] 새로운 컨텐츠를 기록한 정보 기록 매체를 제작하는 경우, 각 엔티티는, 이미 다른 컨텐츠 기록 정보 기록 매체에 있어서 이용한 이들 컨텐츠 코드 파일(601~604)을 재이용할 수 있다.

[0235] 그리고, 컨텐츠 코드는 변조를 방지하기 위하여, 각 컨텐츠 코드 파일은, 관리 센터에 제공되고, 관리

센터에서, 전자 서명을 설정하여, 정보 기록 매체(610)에 저장한다. 정보 기록 매체(610)에 기록되는 컨텐츠 코드에는, 관리 센터(KIC)에 의한 전자 서명, 및 관리 센터가 설정한 고유 ID가 부여된다. 정보 기록 매체(610)에 기록되는 컨텐츠 코드(620)에는, 도면에 나타낸 바와 같이 시큐리티 체크 코드(621), 및 변환 테이블(622)이 포함된다. 구체적인 디렉토리 구성은, 디렉토리 구성(630)에 나타낸 바와 같이, 각 엔티티가 생성한 컨텐츠 코드가 개별적으로 설정된 구성으로 된다.

[0236] 이와 같이, 컨텐츠 코드는, 다양한 컨텐츠에 대응하여 재이용 가능하며, 각 컨텐츠에 따라 변경이 필요한 컨텐츠 코드와 재이용 가능한 컨텐츠 코드를, 적당히 조합시켜, 정보 기록 매체에 기록 되게 된다.

[0237] 또한, 도 9에 나타낸 바와 같이, 각 컨텐츠 코드 파일은, 다음과 같은 분류에 의해 설정하는 구성으로 하는 것도 가능하다.

[0238] 컨텐츠 코드 파일 [00000.svm] : 플레이어 정보의 판별에 적용하는 코드

[0239] 컨텐츠 코드 파일 [00001.svm] , [00002.svm] : 플레이어 정보에 따라 선택되는 코드(예를 들면, 00001.svm는 플레이어 A용의 코드, 00002.svm는 플레이어 B용의 코드 등)

[0240] 컨텐츠 코드 파일 [00003.svm] : 플레이어 정보에 의하지 않는 처리(예를 들면, 컨텐츠 발매시보다 후에 발매되는 기기에 대하여는, 00003.svm에 기재된 디폴트의 코드를 실행한다)

[0241] 이와 같이, 정보 기록 매체에는, 다양한 종류로 구분된 상이한 컨텐츠 코드가 저장되고, 컨텐츠 코드를 이용한 시큐리티 체크를 실행하는 플레이어(재생 장치)는, 자기의 플레이어에 대응하는 시큐리티 체크 코드를 선택하여 시큐리티 체크를 실행한다.

[0242] 도 5에 나타낸 시큐어 VM(361)은, 자체 장치에 대응한 시큐리티 체크 코드를 선택하여 시큐리티 체크 처리를 실행한다. 이 경우, 시큐어 VM(361)은, 플레이어 정보(355)를 입력하여, 시큐리티 체크 코드에 의한 시큐리티 체크 처리를 행하게 된다.

[0243] 플레이어 정보(355)에는, 예를 들면, 재생 장치의 메모리에 저장된 플레이어 증명서(Player Certificate)나, 예를 들면, 재생 장치가 가지는 포트에 관한 정보 등의 플레이어의 구성 정보 등이 포함된다. 그리고, 이들 정보에는, 시큐어 VM(361)이 직접 메모리로부터 취득하는 것이 가능한 정보와, 재생 어플리케이션에 의해 취득 가능한 정보나, 또는 OS(Operating System)에 의해 취득 가능한 정보 등, 다양한 종류의 정보가 포함된다.

[0244] 시큐어 VM에 의해 실행되는 시큐리티 체크 처리의 하나는, 장치가 정당한 플레이어 증명서(Player Certificate)를 가지고 있는 것의 확인이다. 플레이어 증명서는, 컨텐츠의 이용 권한을 증명하는 증명서이며, 컨텐츠의 관리를 실행하는 관리 엔티티가 발행한다.

[0245] 플레이어 증명서의 데이터 구성예를 도 11에 나타낸다. 플레이어 증명서는, 도 11에 나타낸 바와 같이,

[0246] * 플레이어 증명서 사이즈,

[0247] * 증명서 버전,

[0248] * 플레이어 제조자 식별자,

[0249] * 시리얼 번호,

[0250] * 서명 일시,

[0251] * 디바이스(플레이어) 속성 정보,

[0252] * 플레이어 공개키,

[0253] * 전자 서명,

[0254] 이들 데이터를 가진다. 이들 데이터 외에도, 예를 들면, 플레이어 모델명이나, 플레이어 모델의 버전 정보 등을 포함하는 구성으로 해도 된다.

[0255] 시큐어 VM(361)은, 정보 기록 매체로부터 판독한 시큐리티 체크 코드에 따라, 상기 플레이어 증명서의 검증 처리를 실행하고, 정당성을 확인한 후, 그 후의 시큐리티 체크에 필요한 정보를 이 증명서로부터 취득할 수 있다. 구체적인 처리로서는, 먼저, 시큐어 VM(361)은, 플레이어 증명서의 서명 검증 처리를 실행한다. 예를 들면, 플레이어 증명서의 서명 실행 엔티티인 관리 센터의 공개키를 적용한 서명 검증을 실행한다. 관리 센터의 공개키

는, 미리 취득하여 장치의 메모리에 유지된 것을 적용해도 되고, 정보 기록 매체로부터 취득 또는 네트워크를 통하여 취득해도 된다.

[0256] 서명 검증에 의해, 플레이어 증명서의 정당성이 확인되지 않은 경우에는, 그 후의 데이터 변환을 수반하는 컨텐츠 재생으로의 이행이 정지된다. 플레이어 증명서의 정당성이 확인된 경우에는, 또한 플레이어에 대응하는 시큐리티 체크가 실행된다. 제조 메이커 등의 기본적인 플레이어 정보는, 플레이어 증명서로부터 취득할 수 있다.

[0257] 즉 시큐어 VM(361)은, 플레이어 증명서의 정당성 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로서, 상기 플레이어 증명서의 기록 정보로부터, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보 또는 속성 정보, 즉 장치나 어플리케이션의 메이커, 종류, 버전, 시리얼 번호 등을 취득하는 처리를 실행한다. 이들 취득 정보에 따라 취득 정보에 대응하는 시큐리티 체크 코드를 선택하여, 선택 코드에 따른 시큐리티 체크 처리를 실행한다. 그리고, 시큐리티 체크 처리에 필요한 장치 구성 정보 등의 플레이어 정보는, 예를 들면, 재생 어플리케이션이나 시큐어 VM의 정보 취득 처리에 의해 취득된다.

[0258] [6. 정보 처리 장치에 대한 암호 키 배포 구성과 컨텐츠 코드의 암호화 및 이용 처리 구성]

[0259] 먼저 설명한 바와 같이, 시큐어 VM(361)은, 정보 기록 매체에 기록된 컨텐츠 코드에 포함되는 시큐리티 체크 코드에 따른 시큐리티 체크 처리 및 변환 테이블에 따른 변환 처리에 적용하는 파라미터 산출 처리 등을 실행한다. 이 처리에 대하여, 시큐어 VM(361)은, 플레이어 증명서의 정당성 검증 처리를 실행하고, 정당성이 확인된 것을 조건으로서, 상기 플레이어 증명서의 기록 정보로부터, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션을 판별하고, 판별 정보에 대응하는 시큐리티 체크 코드를 선택하여, 선택 코드에 따른 시큐리티 체크 처리를 실행하고, 전술한 변환 테이블(Fix up Table)을 적용한 데이터 변환 처리에 있어서, 컨텐츠의 변환을 행할 때 필요한 파라미터 산출을 실행한다.

[0260] 변환 테이블에 따라 실행되는 데이터의 치환은, 먼저 설명한 바와 같이,

[0261] (a) 변환 데이터

[0262] (b) 식별자 설정 변환 데이터(Forensic Mark)

[0263] 이들 데이터를 적용한 변환이 실행된다.

[0264] 시큐리티 체크 코드에 의한 시큐리티 체크나, 변환 테이블에 따라 실행되는 데이터 변환 처리는, 정확한 플레이어 정보에 따라 선택된 컨텐츠 코드에 따라 실행되는 처리이다. 그러나, 부정한 재생 장치가, 플레이어 증명서를 다른 장치로부터 카피하는 등, 부정한 플레이어 정보를 사용한 처리가 행해질 가능성이 있다. 플레이어 증명서의 검증 만에 의해, 정보 처리 장치나 재생 어플리케이션에 대응하는 플레이어 종류를 판정하고, 플레이어에 대응하는 컨텐츠 코드에 따른 시큐리티 체크 처리나 데이터 변환 처리를 행하면, 본래 필요한 시큐리티 체크를 벗어난 컨텐츠 이용이 행해지는 경우가 있으므로, 또, 본래 컨텐츠에 매립해야하는 식별자 설정 변환 데이터(Forensic Mark)가 정확한 것과는 다른 플레이어 정보를 포함하는 데이터로 되어 버릴 경우가 발생할 수 있다. 이와 같은 부정한 플레이어 정보가 매립된 컨텐츠를 추적해도, 부정 플레이어를 밝혀낼 수 없다는 문제가 발생한다.

[0265] 또, 예를 들면, 극히 엄격한 시큐리티 체크가 요구되는 PC 등의 정보 처리 장치가, 단순한 시큐리티 체크만으로 컨텐츠 이용이 허용되는 재생 전용 기기의 플레이어 증명서를 카피하여 PC에 저장하고, PC에 있어서, 재생 전용 기기의 플레이어 증명서를 적용하여 플레이어 판별을 실행시켜, 단순한 시큐리티 체크만을 실행하여 컨텐츠를 이용해버리는 사태도 발생할 가능성이 있다.

[0266] 이와 같이, 정보 처리 장치가 정확한 플레이어 정보를 제공하지 않는 경우에는, 컨텐츠의 이용이 부정으로 행해지고, 또한 부정 추적도 곤란하게 된다. 즉, 잘못된 플레이어 정보를 제시하면, 정확한 시큐리티 체크가 실행되지 않고, 또한 변환 테이블에 따른 정확한 데이터 변환이 행해지지 않아, 컨텐츠에 대한 플레이어 정보의 매립도 정확하게 행해지지 않는 가능성이 있다. 이하에서는, 이와 같은 부정 행위를 방지하는 구성에 대하여 설명한다.

[0267] 즉, 장치 측에 있어서 부정한 플레이어 정보를 제시하는 경우에도, 각 플레이어에 따른 정확한 컨텐츠 코드를 선택시켜, 컨텐츠를 이용하는 정보 처리 장치나 재생 어플리케이션에 대응하는 정규의 시큐리티 체크 처리를 실

행시키고, 또한 전술한 변환 테이블을 적용한 데이터 변환 처리에 있어서도 정확한 플레이어 정보의 매립을 실행시키는 구성에 대하여 설명한다.

[0268] 플레이어에 대응하는 정확한 컨텐츠 코드를 선택하고 실행시키기 위하여, 본 처리예에서는, 컨텐츠 재생을 실행하는 다수의 정보 처리 장치의 각각에 대하여, 특정한 룰에 따른 고유의 암호 키 세트를 배포하고, 또한 정보 기록 매체에 기록하여 시큐어 VM에 의해 실행되는 컨텐츠 코드 중 적어도 일부를, 정보 처리 장치에 배포한 암호 키를 적용한 암호화 데이터로 한다. 이하, 암호 키 배포 구성 및 처리예에 대하여 설명한다.

[0269] 먼저, 암호 키 배포 구성에 대하여 도 12 이하를 참조하여 설명한다. 키 관리 센터는, 각 플레이어, 즉 컨텐츠 재생을 실행하는 재생 어플리케이션을 실행하는 정보 처리 장치에 대하여, 소정의 암호 키 세트를 배포한다. 그리고, 암호 키 세트의 배포 대상은, 재생 어플리케이션, 또는 재생 어플리케이션을 실행하는 정보 처리 장치, 어느 것에도 설정 가능하다. 단, 키 관리 센터는, 암호 키 세트의 배포처에 대해서의 등록 정보를 유지한다. 예를 들면, 각 재생 어플리케이션의 고유 식별자, 또는 정보 처리 장치의 고유 식별자와 배포 암호 키 세트를 대응시킨 등록 테이블을 유지하고 관리한다.

[0270] 도 12 중 (a)는, 키 관리 센터가 각 플레이어에 배부하는 키 세트를 설명하는 도면이다. 그리고, 이하의 설명에 있어서, 「플레이어」는, 재생 어플리케이션, 또는 재생 어플리케이션을 실행하는 정보 처리 장치 어느 것도 포함하는 개념이며, 키 관리 센터가 배부하는 암호 키 세트의 배포 대상이다.

[0271] 키 관리 센터는, 도 12 중 (a)에 나타낸 바와 같이, 정보 처리 장치 또는 재생 어플리케이션인 플레이어의 제조를 행하는 플레이어 제조 엔티티에 대응하여 설정되는 키 [플레이어 제조 엔티티 키(Manufacture 키]를 정점으로 하는 키 트리를 설정하고, 1개의 정점 또는 분기점(노드)으로부터 n개(도면의 예에서는 n=(256))의 하위 키를 설정한다. 예를 들면, 키 트리의 정점에 있는 플레이어 제조 엔티티 키의 바로 아래의 (2)단째의 키는, 예를 들면, 플레이어 제조 엔티티가 제조 판매하는 플레이어의 모델마다 G1-1 ~ G1-256까지, 256개의 상이한 그룹 키 G1이 설정된다.

[0272] 또한, (3)단째의 키는, 또한 각 G1레이어의 모델로부터 파생한, 예를 들면, 후계 기기로서의 G2모델에 대하여, G2-1 ~ G2-256*256의 키, 즉 256^2개의 상이한 그룹 키 G2가 설정된다. 이하, (3)단째에서는, 각 모델에 대한 버전마다 256^3의 상이한 그룹 키 G3가, (4)단째에서는, 256^4개의 상이한 그룹 키 G4로 계속되고, 최하층의 노드(리프)는, 각 플레이어 1대마다 할당되고, 각 플레이어에 대응하는 플레이어 고유 키 [Player Specific Key] 가 설정된다.

[0273] 각 플레이어는, 자체 플레이어에 대응하는 최하층의 하나의 노드(리프)로부터 계층 구성의 정점 노드에 이르는 루트에 있는 각 노드에 대응하는 키를 보유한다. 예를 들면, 그룹 키 G1(631)은, 도면에 나타낸 계층 구성 중, 최하층의 리프에 대응하는 플레이어 중, 우측 절반의 리프에 대응하는 플레이어에는 배부되지만, 좌측 절반의 리프에 대응하는 플레이어에는 배부되지 않는다. 또, 그룹 키 G2(632)는, 도면에 나타낸 계층 구성 중, 최하층의 리프에 대응하는 플레이어 중, 우측 1/4의 리프에 대응하는 플레이어에는 배부되지만, 그 이외의 좌측 3/4의 리프에 대응하는 플레이어에는 배부되지 않는다. 이와 같이, 각 플레이어에 대하여 배부되는 암호 키 세트는 상이한 설정으로 된다. 구체적인 플레이어의 저장 키 설정에 대하여는, 도 12 중 (c)를 참조하여 후단에서 설명한다. 그리고, 각 플레이어는 플레이어 비밀키 [Private Key] 와 플레이어에 대응하는 공개키를 저장한 공개키 증명서 [Player__Cert] 도 할당된다.

[0274] 그리고, 도 12 중 (a)에 나타낸 계층 구성 중의 정점 노드 ~ 리프에 설정되는 키를 계층 키 또는 노드 키라고 한다. 그리고, 각 계층에 대응하는 모델이나 버전의 설정예는 일례이며, 모델이나 버전에 한정되지 않고, 예를 들면, 라이센시, 플랫폼, 모델, 버전 등으로부터 다층의 구분에 의한 계층 설정도 가능하고, 또한 판매 지역에서 그룹을 나누거나, 제조 일시에 그룹 분류를 하는 등의 설정도 가능하다. 이와 같이, 각 계층의 설정은, 다양한 설정이 가능하다.

[0275] 플레이어에 대응의 공개키를 저장한 공개키 증명서 [Player__Cert] 에는, 플레이어 식별자 [PlayerID] 가 저장된다. 플레이어 식별자는 각 플레이어별로 상이한 식별자이며, 예를 들면 0x00 00 00 00 ~ 0xFF FF FF FF의 각 값이, 각 플레이어에 대응하는 플레이어 ID로서 설정된다.

[0276] 도 12 중 (b)는, 플레이어 제조 엔티티가 관리하는 키이며, 이들은, 플레이어 제조 엔티티가 제조하는 플레이어마다 설정하는 등, 플레이어 제조 엔티티에서 결정한 룰에 따라 생성되는 키이다. 플레이어 제조 엔티티는, 각 키와 그 키의 대응하는 플레이어, 모델이나 버전을 대응시킨 관리 정보를 유지한다.

[0277] 도 12 중 (c)는, 플레이어가 유지하는 키 세트를 나타내고 있다. 먼저 설명한 바와 같이, 각 플레이어는, 자체 플레이어에 대응하는 최하층의 하나의 노드(리프)로부터 계층 구성의 정점 노드에 이르는 루트에 있는 각 노드에 대응하는 키를 보유한다. 도 12 중 (c)에 나타낸 키 세트 중, 플레이어 제조 엔티티 키(Manufacture 키) ~ 플레이어 고유 키(Player Specific Key), 또한 플레이어 비밀키(Private Key) 및 플레이어 공개키 증명서(PLAYER_CERT)는 키 관리 센터로부터 배포되는 키 데이터이다. 또한, 플레이어는, 플레이어 제조 엔티티가 관리하는 플레이어 제조 엔티티 키(Manufacture 키#n)를 유지한다. 그리고, 이들 각 키 정보는, 플레이어로서의 정보 처리 장치의 제조 단계에서 정보 처리 장치의 메모리에 기억 저장된다. 또는, 네트워크를 통하여 취득하는 구성으로 해도 된다.

[0278] 그리고, 도 12 중 (c)에 나타낸 플레이어가 유지하는 키 세트 중, [*] 표시를 부여한 키, 즉 키 관리 센터가 배부하는 플레이어 제조 엔티티 키(Manufacture 키) ~ 플레이어 고유 키(Player Specific Key), 및 플레이어 비밀키(Private Key)와 플레이어 제조 엔티티가 배부하는 플레이어 제조 엔티티 키(Manufacture 키#n)는, 플레이어가 시큐어로 유지할 필요가 있는 키이며, 누출을 방지하는 것이 필요하다. 공개키 증명서에 대하여는, 특히 비밀로 유지할 필요는 없다.

[0279] 각 플레이어에 대하여 배부되는 암호 키 세트는, 먼저 설명한 바와 같이, 계층 구성의 플레이어에 대응하는 리프로부터 정점 노드에 이르는 각 노드의 그룹 키, 플레이어 고유 키이며, 상이한 설정으로 된다. 구체적인 플레이어의 저장 키 설정에 대하여는, 도 12 중 (c)를 참조하여 후단에서 설명한다. 그리고, 각 플레이어는 플레이어 비밀키 [Private Key] 와 플레이어에 대응하는 공개키를 저장한 공개키 증명서 [Player_Cert] 도 할당된다.

[0280] 다음에, 도 13을 참조하여 정보 기록 매체에 저장하는 컨텐츠 코드의 암호화 처리 태양에 대하여 설명한다. 먼저, 도 10을 참조하여 설명한 바와 같이, 컨텐츠 코드는, 이하의 4개의 카테고리로 분류 가능하다.

[0281] (a) 전(全) 컨텐츠 및 전(全) 플레이어(장치 또는 재생 어플리) 공통으로 이용되는 컨텐츠 코드

[0282] (b) 컨텐츠 고유의 컨텐츠 코드

[0283] (c) 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드

[0284] (d) 컨텐츠 & 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드

[0285] 이들 각각의 컨텐츠 코드는, 먼저 도 9를 참조하여 설명한 바와 같이, 개별의 파일, 또는 집적되어 1개의 파일로서 정보 기록 매체에 저장된다. 이들 각 카테고리의 컨텐츠 코드는, 각각 코드의 제작을 행하는 엔티티가 상이한 경우가 있다. 예를 들면, (b) 컨텐츠 고유 데이터에 대응하는 컨텐츠 코드는, 컨텐츠의 제작자인 스튜디오 등이 설정한다. 또, (c) 플레이어(장치 또는 재생 어플리) 고유 데이터에 대하여는, 플레이어로서의 재생 장치나, 재생 어플리케이션을 제작하는 엔티티가 생성하는 경우가 많다.

[0286] 이와 같이, 상이한 엔티티에 의해 생성되는 컨텐츠 코드가, 정보 기록 매체에 기록되기까지의 시퀀스에 대하여, 도 13을 참조하여 설명한다. 도 13에는, 전술한 4개의 카테고리에 대응하는 컨텐츠 코드의 구성 데이터가 정보 기록 매체에 대하여 기록되는 과정을 나타내고 있다. 즉,

[0287] (a) 전(全) 컨텐츠 및 전(全) 플레이어(장치 또는 재생 어플리) 공통으로 이용되는 컨텐츠 코드: 예를 들면, 스타트 업 루틴, 공통 루틴(외부 기록으로의 액세스 등), 플레이어 식별 루틴용의 코드 등이 포함된다.

[0288] (b) 컨텐츠 고유의 컨텐츠 코드: 예를 들면, 변환 테이블(Fix Up Table) 정보, 타이틀 초기화(Fix Up Table 생성 처리를 포함함) 처리 코드 등이 포함된다.

[0289] (c) 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드: 예를 들면, 런 네이티브(Run Native) 실행 부분, 네이티브 코드(Native Code), 플레이어 고유의 체크 루틴에 적용하는 코드 등이 포함된다.

[0290] (d) 컨텐츠 & 플레이어(장치 또는 재생 어플리) 고유의 컨텐츠 코드: 예를 들면, 디스커버리 램(Discovery RAM) 실행 부분, 디스커버리 램(Discovery RAM)용 비교 데이터 등의 코드가 포함된다.

[0291] 이들 4개의 상이한 카테고리의 컨텐츠 코드이다.

[0292] 이들 컨텐츠 코드는, 각각 상이한 엔티티, 즉 컨텐츠의 제작, 편집을 행하는 스튜디오, 오서링(authoring) 회사, 또한, 플레이어(장치 또는 재생 어플리)의 제조 메이커 등, 상이한 엔티티에 의해 제작되는 경우가 있다.

[0293] 이들 각 컨텐츠 코드 구성 부품 생성 엔티티는, 스텝 S201에 있어서, 먼저 도 12를 참조하여 설명한 라이센시/

플랫폼/모델/버전/ 등에 고유한 키, 즉 먼저 도 12를 참조하여 설명한 노드 키(그룹 키 [Gn] 나 플레이어 고유 키)를 사용하여 컨텐츠 코드의 일부를 암호화하는 전제로 컨텐츠 코드를 준비한다.

[0294] 또한, 각 컨텐츠 코드 구성 부품 생성 엔티티는, 각 컨텐츠 코드의 암호화 구성 정보를 가지는 컨텐츠 코드 암호 구성 정보(642)를 생성하여, 생성한 컨텐츠 코드와 함께, 키 관리 센터에 송부한다. 컨텐츠 코드 암호 구성 정보(642)는, 도면에 나타낸 바와 같이, 컨텐츠 코드 식별 정보로서의 컨텐츠 코드 번호와, 암호화 구간 정보와, 암호화 구간에 적용하는 키 지정 정보와의 대응 데이터에 의해 구성된다.

[0295] 키 관리 센터에서는, 각 컨텐츠 코드 구성 부품 생성 엔티티로부터 수령한 컨텐츠 코드에 대하여, 컨텐츠 코드 암호 구성 정보(642)에 따른 암호화를 실행한다. 즉, 키 관리 센터는, 도 12 중 (a)를 참조하여 설명한 계층 구성의 키 정보로 이루어지는 발행완료의 키 데이터 베이스로부터, 컨텐츠 코드 암호 구성 정보(642)에서 지정된 키를 취득하고, 컨텐츠 코드 암호 구성 정보(642)에서 지정된 컨텐츠 코드의 지정 부분을 암호화한다.

[0296] 이와 같이 하여, 도 13에 나타낸 암호화된 컨텐츠 코드(641)가 생성되고, 이 암호화된 컨텐츠 코드(641)가 정보 기록 매체 제조 엔티티인 디스크 공장에 송부되어 디스크에 기록된다. 그리고, 컨텐츠 코드 암호 구성 정보(642)에 대해서도, 디스크 공장에 송부되어 디스크에 기록된다. 그리고, 컨텐츠 코드 암호 구성 정보(642)는, 컨텐츠 코드의 구성 데이터에 포함되어 정보 기록 매체에 기록되거나, 또는 고유의 독립 파일로서 정보 기록 매체에 기록되는 설정으로 한다.

[0297] 암호화된 컨텐츠 코드(641)로서, 도 13에는 4개의 컨텐츠 코드 파일 [00000.svm] ~ [00003.svm] 을 나타내고 있다. 이들 컨텐츠 코드는, 각각 부분적으로 암호화된 암호화 데이터를 포함한다. 이들 암호화에 적용한 암호 키는, 예를 들면, 도 12 중 (a)를 참조하여 설명한 그룹 키 [Gn]이며, 컨텐츠 코드 암호 구성 정보(642)에 따라 선택된 키를 적용하여 암호화가 되어 있다.

[0298] 예를 들면, 컨텐츠 코드 파일 00000.svm가, 도 12 중 (a)에 나타낸 그룹 키 G1(631)을 적용하여 암호화되어 있다고 하면, 이 암호화 데이터를 복호 할 수 있는 것은, 그룹 키 G1(631)을 유지하고 있는 플레이어만이 되고, 도 12에 나타낸 계층 구성의 최하층의 리프에 대응하는 플레이어 중, 우측 절반의 리프에 대응하는 플레이어만이 컨텐츠 코드 00000.svm의 암호화부 데이터를 이용할 수 있다. 좌측 절반의 리프에 대응하는 플레이어는, 그룹 키 G1(631)을 유지하고 있지 않으므로, 컨텐츠 코드 00000.svm의 암호화부 데이터를 이용할 수 없다.

[0299] 마찬가지로, 예를 들면, 컨텐츠 코드 파일 00001.svm가, 도 12 중 (a)에 나타낸 그룹 키 G2(632)를 적용하여 암호화되어 있다고 하면, 이 암호화 데이터를 복호 할 수 있는 것은, 그룹 키 G2(632)를 유지하고 있는 플레이어만이 되고, 도 12에 나타낸 계층 구성의 최하층의 리프에 대응하는 플레이어 중, 우측의 1/4의 리프에 대응하는 플레이어만이 컨텐츠 코드 00001.svm의 암호화부 데이터를 이용할 수 있다.

[0300] 이와 같이, 컨텐츠 코드를, 그룹 키 [Gn] 또는 플레이어 고유 키를 적용하여 암호화함으로써, 컨텐츠 코드를 복호하여 이용 가능한 플레이어를 한정하는 것이 가능해진다. 컨텐츠 코드에는, 전술한 바와 같이 시큐리티 체크용의 시큐리티 체크 코드나, 컨텐츠의 데이터 변환에 적용하는 변환 테이블이 포함되어 있고, 시큐리티 체크 처리나, 데이터 변환 처리를, 특정한 플레이어에 대해서만 실행 가능한 설정으로 할 수 있다.

[0301] 따라서, 플레이어 증명서를 다른 플레이어로부터 카피하는 등의 처리에 의해, 부정한 플레이어 증명서를 적용한 플레이어 정보 제시 처리를 행한 경우, 그 플레이어 정보에 대응하는 플레이어 고유의 컨텐츠 코드를 취득하여 처리를 실행할려고 해도, 그 컨텐츠 코드는, 플레이어에 저장된 암호 키 세트에 포함되는 그룹 키에 의해 복호하는 것이 불가능하게 되고, 부정한 플레이어 증명서에 의해 식별된 플레이어 정보에 대응하는 플레이어 고유의 컨텐츠 코드가 부정으로 적용되는 것이 방지된다.

[0302] 다음에, 도 14를 참조하여 컨텐츠 코드의 상이한 생성 방법에 대하여 설명한다. 각 컨텐츠 코드 구성 부품 생성 엔티티는, 스텝 S211에 있어서, 컨텐츠 코드 제작시에, 난수(亂數) 등을 적용하여 생성한 오리지날 암호 키를 사용하여 컨텐츠 코드의 일부를 암호화한다. 그 후, 컨텐츠 코드의 암호화에 사용한 오리지날 암호 키를, 먼저 도 12를 참조하여 설명한 노드 키(그룹 키 [Gn] 나 플레이어 고유 키), 즉 라이센시/플랫폼/모델/버전/ 등에 고유한 키를 사용하여 암호화하도록 키 관리 센터에 의뢰한다.

[0303] 각 컨텐츠 코드 구성 부품 생성 엔티티는, 오리지날 암호 키를 적용하여 암호화한 컨텐츠 코드와 오리지날 암호 키, 또한 각 컨텐츠 코드의 암호화 구성 정보를 가지는 컨텐츠 코드 암호 구성 정보(642)를 키 관리 센터에 송부한다. 컨텐츠 코드 암호 구성 정보(642)는, 도면에 나타낸 바와 같이, 컨텐츠 코드 식별 정보로서의 컨텐츠 코드 번호와, 암호화 구간 정보와, 암호화 구간에 적용하는 키의 지정 정보와의 대응 데이터에 의해 구성된다.

[0304] 키 관리 센터에서는, 각 컨텐츠 코드 구성 부품 생성 엔티티로부터 수령한 오리지날 암호 키에 대하여, 컨텐츠 코드 암호 구성 정보(642)에 따른 암호화를 실행한다. 즉, 키 관리 센터는, 도 12 중 (a)를 참조하여 설명한 계층 구성의 키 정보로 이루어지는 발행완료의 키 데이터 베이스로부터, 컨텐츠 코드 암호 구성 정보(642)에서 지정된 키를 취득하고, 각 컨텐츠 코드 구성 부품 생성 엔티티로부터 수령한 오리지날 암호 키를 암호화하여 컨텐츠 코드에 저장한다.

[0305] 도 14에 나타낸 예에서는, 컨텐츠 코드 파일 [00000.svm] 에 설정된 암호화 키 데이터(643)가, 오리지날 암호 키를 암호화한 데이터의 저장 영역이다. 즉, 각 컨텐츠 코드 구성 부품 생성 엔티티로부터 수령한 복수개의 오리지날 암호 키에 대하여, 각각 컨텐츠 코드 암호 구성 정보(642)에 따라 선택된 암호 키, 즉 도 12 중 (a)를 참조하여 설명한 계층 구성 중 중 어느 하나의 그룹 키 [Gn] 를 적용하여 각 오리지날 암호 키를 암호화한다.

[0306] 컨텐츠 코드 파일 [00000.svm] ~ [00003.svm] 에 설정된 암호화 데이터는, 각 컨텐츠 코드 구성 부품 생성 엔티티가, 각각 생성한 오리지날 암호 키에 의해 암호화된 데이터이다.

[0307] 예를 들면, 컨텐츠 코드 파일 [00000.svm]에 설정된 암호화 키 데이터(643)의 최후미에는, 컨텐츠 코드 파일(0003)에 포함되는 암호화 데이터의 암호화에 적용한 오리지날 암호 키(K03)를 그룹 키 [Gn] 로 암호화한 암호화 데이터가 저장된다.

[0308] 예를 들면, 오리지날 암호 키(K03)가, 도 12 중 (a)에 나타낸 그룹 키 G1(631)을 적용하여 암호화되어 있다고 하면, 이 암호화 키를 복호하여 오리지날 암호 키(K03)를 취득할 수 있는 것은, 그룹 키 G1(631)을 유지하고 있는 플레이어만이 되어, 도 12에 나타낸 계층 구성의 최하층의 리프에 대응하는 플레이어 중, 우측 절반의 리프에 대응하는 플레이어만이 된다.

[0309] 이 결과, 오리지날 암호 키(K03)를 취득하고, 컨텐츠 코드 [00003.svm]의 암호화부 데이터를 이용할 수 있는 것은, 도 12에 나타낸 계층 구성의 최하층의 리프에 대응하는 플레이어 중, 우측 절반의 리프에 대응하는 플레이어만이 된다. 좌측 절반의 리프에 대응하는 플레이어는, 그룹 키 G1(631)을 유지하고 있지 않으므로, 오리지날 암호 키(K03)를 취득할 수 없고, 컨텐츠 코드 [00003.svm]의 암호화부 데이터를 이용할 수 없다. 본 처리예에서는, 키 관리 센터에서의 암호화 처리가 오리지날 암호 키의 암호화만이며, 신속한 처리가 가능해진다. 또한, 각 컨텐츠 코드 구성 부품 생성 엔티티로부터 키 관리 센터에 송부되는 컨텐츠 코드가 이미 오리지날 암호 키에 의해 암호화되어 있으므로, 정보 누출의 가능성도 저감시킬 수 있다.

[0310] 다음에, 도 15를 참조하여, 플레이어에 있어서의 컨텐츠 코드의 처리에 대하여 설명한다. 컨텐츠 재생을 실행하는 정보 처리 장치의 데이터 처리로서의 시큐어 VM는, 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하고, 상기 컨텐츠 코드에 따른 데이터 처리를 실행한다. 이 컨텐츠 코드 중 적어도 일부는, 도 13, 도 14를 참조하여 설명한 바와 같이 노드 키를 적용하여 암호화되어 있다.

[0311] 시큐어 VM는, 컨텐츠 코드의 복호에 적용하는 키 지정 정보, 및 컨텐츠 코드 중에 설정된 암호화 데이터의 위치를 나타내는 암호화 데이터 위치 지정 정보를 정보 기록 매체의 저장 데이터로부터 취득하고, 상기 취득 정보에 따라 메모리로부터 노드 키를 선택하고, 암호화 데이터 위치 지정 정보에 따라 복호 대상 데이터를 특정하여, 선택 노드 키를 적용한 복호 처리를 실행한다.

[0312] 도 15는, 도 14의 설정을 가지는 컨텐츠 코드의 플레이어 측의 처리를 설명하는 도면이며, 먼저, 도를 참조하여 설명한 플레이어 저장 키(650)를 적용한 시큐어 VM(652)에 의한 처리를 설명하는 도면이다. 정보 기록 매체에 저장된 컨텐츠 코드는, 시큐어 VM(652)에 의해 판독되어 처리가 행해진다. 시큐어 VM(652)은, 시큐어 VM용 메모리(651)에 정보 기록 매체로부터 판독한 컨텐츠 코드를 저장하여 처리를 실행한다.

[0313] 그리고, 플레이어 저장 키(650)에는, 먼저 도 12를 참조하여 설명한 키, 즉 키 관리 센터가 배부하는 플레이어 제조 엔티티 키(Manufacture 키) ~ 플레이어 비밀키(Private Key)와 공개키 증명서, 및 플레이어 제조 엔티티가 배부하는 플레이어 제조 엔티티 키(Manufacture 키#n)를 나타내고 있다.

[0314] 시큐어 VM(652)은, 먼저, 스텝 S251에 있어서, 시큐어 VM용 메모리(651)에 저장된 메모리 저장 데이터(661)로부터, 처리 대상의 컨텐츠 코드에 설정된 암호화 키 데이터 [X] (662)를 취득하고, 이 컨텐츠 코드에 포함되는 기록 데이터 또는 다른 데이터 파일로부터 취득한 키 지정 정보에 따라 암호화 키 데이터 [X] (662)의 복호 처리에 적용하는 키를 플레이어 저장 키(650)로부터 선택한다. 키 지정 정보는, 먼저, 도 13, 도 14를 참조하여 설명한 컨텐츠 코드 암호 구성 정보(642)에 따라 정보 기록 매체에 기록되는 정보이다.

[0315] 본 처리예에서는, 키 지정 정보는, 키 ID=4, 즉 플레이어 고유 키(Player Specific Key)를 지정하는 정보라고

한다. 시큐어 VM(652)은, 키 지정 정보 [키 ID=4]에 따라, 플레이어 저장 키(650)로부터 플레이어 고유 키(Player Specific Key)를 선택하고, 암호화 키 데이터 [X] (662)의 복호 처리를 실행한다.

[0316] 이 복호 처리에 의해, 컨텐츠 코드의 일부를 암호화한 오리지날 암호 키 [K] 가 취득된다. 시큐어 VM(652)은, 스텝 S252에 있어서, 취득한 오리지날 암호 키 [K] 를 적용하여, 컨텐츠 코드의 암호화부에 대응하는 입력 데이터(663)를 복호하고, 복호 결과를 출력 데이터(664)로서 시큐어 VM용 메모리(651)에 저장한다. 이 처리에 의해, 플레이어는, 예를 들면, 플레이어 고유의 컨텐츠 코드의 이용이 가능해진다.

[0317] 그리고, 이와 같은 시큐어 VM(652)에 있어서의 처리는, 예를 들면, 컨텐츠 재생 처리를 실행하는 재생(플레이어) 어플리케이션으로부터 시큐어 VM에 대한 중간개입(INTRP)과 시큐어 VM로부터 재생(플레이어) 어플리케이션에 대한 응답(Call)처리의 시퀀스에 의해 실행된다. 컨텐츠 코드의 복호 처리는, 예를 들면, 하기의 함수의 호출에 의해 실행된다.

[0318] CALL AES(출력처 어드레스, 입력 데이터 어드레스, AES 처리 블록 수, 키 어드레스, 키 ID)

[0319] 상기 함수는, 키 어드레스로 지정되는 128bit의 값(도 15중의 암호화 키 데이터 [X] (662))을, 키 ID(도 15에서는 ID=4)로 지정된 플레이어가 가지는 비밀키로 복호하는 처리를 실행하고, 복호 결과를 복호 키로 하여, 입력 데이터 어드레스로부터 AES 처리 블록 수*16바이트 분의 데이터를 복호하고, 출력처 어드레스에 복호 후의 데이터를 출력하는 처리를 실행시키는 함수이다.

[0320] 또한, 도 16을 참조하여, 플레이어에 있어서의 컨텐츠 코드의 상이한 처리예에 대하여 설명한다. 도 16은, 플레이어 저장 키(650) 중의 플레이어 비밀키 [Private Key] 를 적용한 서명 처리를 설명하는 도면이다.

[0321] 시큐어 VM(652)은, 시큐어 VM용 메모리(651)에 저장한 메모리 저장 데이터(671)의 입력 데이터(672)에 대하여, 스텝 S272에 있어서, 예를 들면, SHA1 등의 해시 함수를 적용하여 해시값을 산출한다. 그리고, 이 해시값 산출 전 스텝으로서 스텝 S271에 있어서 플레이어 정보나 미디어 정보를 가산해도 된다. 다음에, 스텝 S273에 있어서, 플레이어 저장 키(650)로부터 플레이어 비밀키 [Private Key] 를 취득하여, 해시값에 대한 전자 서명, 예를 들면, EC-DSA 알고리즘에 따른 전자 서명을 행하고, 서명을 포함하는 데이터를 출력 데이터(673)로서 시큐어 VM용 메모리(651)에 저장한다. 그 후, 컨텐츠 코드의 실행을 행할 때, 출력 데이터(673)를 취득하여 서명 검증 처리를 실행함으로써, 플레이어의 정당성을 검증하는 것이 가능해진다.

[0322] 그리고, 이 서명 설정 처리는, 시큐어 VM(652)에 의한, 예를 들면, 하기의 함수의 호출에 의해 실행된다.

[0323] CALL PrivateKey(출력처 어드레스, 입력 데이터 어드레스, 서명 대상 데이터 길이, Option 지정, 키 ID)

[0324] 상기 함수는, 입력 데이터 어드레스로부터 서명 대상 데이터 길이 분의 데이터를 인출하고, 옵션(Option) 지정되는 Media/Player 정보를 바이트 열에 추가한 것을 SHA1함수로 해시값으로 변환하여, 변환 결과에 플레이어가 가지는 비밀키로 서명하여 출력처 어드레스에 기록하는 처리를 실행시키는 함수이다.

[0325] 이상, 설명한 바와 같이, 먼저, 도 12 중 (a)를 참조하여 설명한 계층 구성상의 각 노드에 설정된 노드 키 세트를 정보 기록 매체에 배부하고, 노드 키를 선택 적용한 암호화 처리를 실행한 컨텐츠 코드를 생성하여 정보 기록 매체에 저장함으로써, 특정한 선택된 플레이어 만에 의해 처리 가능한 컨텐츠 코드를 제공하는 것이 가능해진다.

[0326] 플레이어에 대한 키의 배포 구성은 먼저, 도 12를 참조하여 설명한 구성뿐 아니라, 다양한 설정이 가능하다. 이들 예에 대하여, 도 17, 도 18을 참조하여 설명한다. 도 17에 나타낸 예는, 계층 구성에 대하여는 먼저, 도 12 중 (a)를 참조하여 설명한 구성과 동일한 구성이며, 각 플레이어는, 자체 플레이어에 대응하는 최하층의 하나의 노드(리프)로부터 계층 구성의 정점 노드에 이르는 루트에 있는 각 노드에 대응하는 키를 보유한다. 즉, 도 17 중 (b)에 나타낸 바와 같이, 플레이어 제조 엔티티 키(Manufacture 키) ~ 플레이어 고유 키(Player Specific Key), 또한 플레이어 비밀키(Private Key) 및 플레이어 공개키 증명서(PLAYER_CERT)가 키 관리 센터로부터 배포된다.

[0327] 도 17에 나타낸 예에서는, 또한 키 관리 센터는, 모델 키 [Model 키#n] , 버전 키 [Version#n] 를 설정하고, 이들 각 키로부터 플레이어에 대응하는 모델, 버전에 대응하는 키를 선택하여 플레이어에 제공한다.

[0328] 도 18에 나타낸 예도, 계층 구성에 대하여는 먼저, 도 12 중 (a)를 참조하여 설명한 구성과 동일한 구성이며, 각 플레이어는, 자체 플레이어에 대응하는 최하층의 하나의 노드(리프)로부터 계층 구성의 정점 노드에 이르는 루트에 있는 각 노드에 대응하는 키를 보유한다. 즉, 도 17 중 (b)에 나타낸 바와 같이, 플레이어 제조 엔티티

키(Manufacture 키) ~ 플레이어 고유 키(Player Specific Key), 또한 플레이어 비밀키(Private Key) 및 플레이어 공개키 증명서(PLAYER_CERT)가 키 관리 센터로부터 배포된다.

[0329] 도 18에 나타낸 예에서는, 또한 키 관리 센터는, 시스템 키 [A] 로서 모델 고유값 [Model고유값#An] , 버전 고유값 [Version고유값#An] 을 설정하고, 이들 각 고유값으로부터 플레이어에 대응하는 모델, 버전에 대응하는 고유값을 선택하여 플레이어에 제공한다.

[0330] 시스템 키는 복수개 정의 가능하며, 예를 들면, 재생 전용 기기로서의 CE기나, PC 등 크게 상이한 시스템 사이에서 분류하는 것이 가능하다. 모델 고유값 [Model고유값#An] , 버전 고유값 [Version고유값#An] 은 시스템 키로 암호화된 상태로 플레이어가 유지하고, 시스템 키로 복호함으로써 모델이나 버전 고유의 키로 하여 사용할 수 있는 설정으로 한다. 이와 같이 설정함으로써, 예를 들면, 모델(플랫폼)로서 시큐어한 시스템이면, 버전에 관계없이 모델 전체에 대하여 동일한 컨텐츠 코드를 적용할 수도 있다. 한편, 모델 중 1개의 버전이 취약한 경우에는, 상기 모델이 있는 버전에만 컨텐츠 코드를 적용할 수 있다.

[0331] 도 17, 도 18의 어느 것에 있어서도, 계층 구성 내의 노드 키를 적용한 처리 구성에 대하여는, 먼저, 도 12 ~ 도 16을 참조하여 설명한 처리와 동일한 처리가 가능하며, 특정한 플레이어를 선택하여, 선택된 플레이어에서만 이용 가능한 컨텐츠 코드를 설정하여 정보 기록 매체에 저장하여 제공하는 것이 가능해지고, 부정한 플레이어 정보를 제시해 부정으로 컨텐츠 코드를 적용한 부정 처리를 방지하는 것이 가능해진다.

[0332] 다음에, 도 19에 나타낸 플로차트를 참조하여, 컨텐츠 코드 중의 시큐리티 체크 코드를 적용한 시큐리티 체크 처리 및 변환 테이블을 적용한 변환 처리에 따른 컨텐츠 재생 시퀀스에 대하여 설명한다.

[0333] 먼저, 스텝 S301에 있어서, 시큐어 VM는 정보 기록 매체로부터 컨텐츠 코드를 취득하고, 컨텐츠 코드에 플레이어 정보의 취득 요구가 포함되어 있는지 여부를 판정한다. 이것은, 예를 들면, 도 9에 나타낸 디렉토리 설정의 경우, 플레이어 정보의 판별에 적용하는 코드를 저장한 컨텐츠 코드 파일 [00000.svm] 을 읽어내 판정한다.

[0334] 컨텐츠 코드에 플레이어 정보의 취득 요구가 포함되어 있지 않은 경우에는, 스텝 S306으로 진행한다. 컨텐츠 코드에 플레이어 정보의 취득 요구가 포함되어 있는 경우에는, 스텝 S302으로 진행하고, 컨텐츠 코드에 따라 시큐리티 체크에 필요한 플레이어 정보를 취득한다. 이들 정보에는, 예를 들면, 도 11을 참조하여 설명한 플레이어 증명서 등이 포함된다.

[0335] 다음에, 스텝 S303에 있어서, 플레이어에 대응하는 컨텐츠 코드를 취득하고, 스텝 S304에 있어서, 컨텐츠 코드에 포함되는 암호화 데이터의 복호 키를 취득하고, 복호를 실행한다. 이 처리 태양으로서는 여러 가지이고, 예를 들면, 도 13을 참조하여 설명한 컨텐츠 코드의 설정에서는, 시큐어 VM는, 정보 처리 장치 내의 메모리에 저장된 암호 키 세트로부터 지정 노드 키(그룹 키 등)를 취득하여, 컨텐츠 코드의 암호화 데이터의 복호를 실행한다. 도 14에 나타낸 컨텐츠 코드의 설정의 경우에는, 먼저, 도 15를 참조하여 설명한 바와 같이, 정보 처리 장치 내의 메모리에 저장된 암호 키 세트로부터 지정 노드 키(그룹 키 등)를 취득하여, 컨텐츠 코드에 포함되는 오리지날 암호 키의 암호화 데이터를 복호하여 오리지날 암호 키를 취득한 후, 취득한 오리지날 암호 키를 적용하여 컨텐츠 코드에 포함되는 암호화 데이터의 복호를 실행한다. 그리고, 키 지정 정보나, 암호화 데이터의 위치 정보는, 컨텐츠 코드 또는 그 외의 데이터 파일로부터 취득된다.

[0336] 스텝 S305에 있어서, 컨텐츠 코드의 복호에 성공했는지 여부를 판정하고, 실패한 경우에는, 처리를 중지하여 종료한다. 이 경우에는, 컨텐츠 코드에 대응하는 플레이어 대응의 정확한 키 적용이 행해지지 않은 것을 의미하고, 이 경우에는 컨텐츠 코드를 이용한 처리, 예를 들면, 시큐리티 체크 처리, 또는 변환 테이블에 따른 컨텐츠의 데이터 변환 처리는 실행되지 않고, 결과로서 컨텐츠의 이용이 금지된다.

[0337] 스텝 S305에 있어서, 컨텐츠 코드의 복호에 성공했다고 판정되면, 스텝 S306으로 진행하고 컨텐츠 코드를 이용한 처리가 실행된다. 즉, 시큐리티 체크 처리, 또는 변환 테이블에 따른 컨텐츠의 데이터 변환 처리가 실행되고, 컨텐츠의 이용이 행해진다.

[0338] 그리고, 처리 대상의 컨텐츠 코드에 의해, 시큐어 VM이 실행하는 처리는 상이하다. 예를 들면, 컨텐츠 코드가 시큐리티 체크 코드인 경우에는, 컨텐츠 코드에 따른 시큐리티 체크 처리를 실행하고, 컨텐츠 코드가, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드인 경우에는, 컨텐츠 코드에 따라 정보 기록 매체에 저장된 컨텐츠의 데이터 변환 처리에 적용하는 데이터 생성을 실행한다. 또한, 컨텐츠 코드가, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드인 경우

에는, 컨텐츠 코드에 따라 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성을 실행한다.

[0339] [7. 정보 처리 장치의 구성]

[0340] 다음에, 도 20을 참조하여, 전술한 재생(플레이어) 어플리케이션 및 시큐어 VM을 적용한 데이터 처리를 실행하는 정보 처리 장치의 하드웨어 구성예에 대하여 설명한다. 정보 처리 장치(800)는, OS나 컨텐츠 재생 또는 기록 어플리케이션 프로그램, 상호 인증 처리, 컨텐츠 재생에 따른 다양한 처리, 예를 들면, 전술한 시큐리티 체크 코드에 따른 시큐리티 체크 처리, 변환 테이블을 적용한 데이터 변환 처리 등을 포함하는 각종 프로그램에 따른 데이터 처리를 실행하는 CPU(809), 프로그램, 파라미터 등의 기억 영역으로서의 ROM(808), 메모리(810), 디지털 신호를 입출력하는 입출력 I/F(802), 아날로그 신호를 입출력하고, A/D, D/A컨버터(805)를 가지는 입출력 I/F(804), MPEG 데이터의 인코드, 디코드 처리를 실행하는 MPEG 코덱(803), TS(Transport Stream)·PS(Program Stream) 처리를 실행하는 TS·PS처리 수단(806), 상호 인증, 암호화 컨텐츠의 복호 처리 등 각종의 암호 처리를 실행하는 암호 처리 수단(807), 하드 디스크 등의 기록 매체(812), 기록 매체(812)의 구동, 데이터 기록 재생 신호의 입출력을 행하는 드라이브(811)를 가지고, 버스(801)에 각 블록이 접속되어 있다.

[0341] 정보 처리 장치(호스트)(800)는, 예를 들면, ATAPI-BUS 등의 접속 버스에 의해 드라이브와 접속되어 있다. 변환 테이블, 컨텐츠 등을 디지털 신호용 입출력 I/F(802)를 통하여 입출력한다. 암호화 처리, 복호 처리는, 암호화 처리 수단(807)에 의해, 예를 들면, AES 알고리즘 등을 적용하여 실행된다.

[0342] 그리고, 컨텐츠 재생 또는 기록 처리를 실행하는 프로그램은 예를 들면, ROM (808)내에 보관되어 있고, 프로그램의 실행 처리 중에는 필요에 따라 파라미터, 데이터의 보관, 공작물 영역으로서 메모리(810)를 사용한다.

[0343] ROM(808) 또는 기록 매체(812)에는, 예를 들면, 전술한 플레이어 증명서, 또한 플레이어 증명서의 서명 검증 등에 적용하는 관리 센터의 공개키, 또한 드라이브와의 인증 처리 등에서 적용하는 호스트 대응 비밀키, 호스트에 대응하는 공개키 증명서, 또한 공개키 증명서의 무효화 리스트로서의 리보케이션 리스트 등이 저장된다.

[0344] 컨텐츠 재생 또는 컨텐츠의 외부 출력을 행할 때는, 정보 기록 매체로부터 취득한 데이터 변환 처리 프로그램을 적용하여, 암호화 컨텐츠의 복호와 변환 테이블의 복원, 변환 테이블의 저장 데이터에 따른 변환 데이터의 기록 처리 등, 먼저 설명한 처리 시퀀스에 따른 처리를 실행한다.

[0345] [8. 정보 기록 매체 제조 장치 및 정보 기록 매체]

[0346] 다음에, 정보 기록 매체 제조 장치 및 정보 기록 매체에 대하여 설명한다. 즉, 전술한 컨텐츠 재생 처리에 있어서 적용되는 정보 기록 매체의 제조 장치, 정보 기록 매체의 제조 방법, 및 정보 기록 매체에 대하여 설명한다.

[0347] 정보 기록 매체 제조 장치는, 예를 들면, 먼저, 도 1을 참조하여 설명한 기록 데이터를 저장한 정보 기록 매체(100)를 제조하는 장치이다. 정보 기록 매체(100)에는, 시큐리티 체크 코드나 변환 테이블을 포함하는 컨텐츠 코드가 저장된다. 컨텐츠 코드는, 도 13, 도 14를 참조하여 설명한 바와 같이, 일부에 다양한 노드 키 또는 난수 등에 의해 생성된 오리지날 암호 키를 적용하여 암호화된 데이터를 포함하는 컨텐츠 코드이다.

[0348] 정보 기록 매체 제조 장치는, 도 21에 나타낸 바와 같이, 정보 기록 매체에 기록하는 컨텐츠 데이터를 저장한 컨텐츠 파일을 생성하는 컨텐츠 파일 생성 수단(901)과, 컨텐츠의 이용을 행할 때 실행해야 할 시큐리티 체크 처리용 프로그램을 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 컨텐츠 코드 파일 생성 수단(902)과, 컨텐츠 파일 생성 수단(901)에서 생성한 컨텐츠 파일, 및 컨텐츠 코드 파일 생성 수단(902)에서 생성한 컨텐츠 코드 파일을 정보 기록 매체(910)에 기록하는 기록 수단(903)을 가진다.

[0349] 컨텐츠 코드 파일 생성 수단(902)은, 먼저, 도 9를 참조하여 설명한 바와 같이, 정보 처리 장치 또는 컨텐츠 이용 어플리케이션의 종류에 대응하는 복수개의 컨텐츠 코드 파일의 생성 처리를 실행하는 구성이다. 컨텐츠 코드 파일에 저장되는 컨텐츠 코드는, 먼저, 도 13, 도 14를 참조하여 설명한 바와 같이, 일부에 다양한 노드 키 또는 난수 등에 의해 생성된 오리지날 암호 키를 적용하여 암호화된 데이터를 포함하는 컨텐츠 코드이다.

[0350] 컨텐츠 코드 파일 생성 수단(902)은, 각 정보 처리 장치 또는 재생 어플리케이션을 최하층 노드인 리프에 대응시킨 계층 구성을 가지는 키 트리 상의 어느 하나의 노드에 대응하는 노드 키를 적용하여 암호화한 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성한다. 구체적인 컨텐츠 코드의 암호화 태양으로

서는, 먼저, 도 13, 도 14를 참조하여 설명한 태양이 있다. 즉, 컨텐츠 코드 파일 생성 수단(902)은, 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하거나, 또는 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키(오리지날 암호 키)로 암호화한 코드 정보 암호화 데이터와, 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성한다.

[0351] 그리고, 컨텐츠 코드 파일 생성 수단(902)은, 정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성하는 구성이며, 또, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 생성한다.

[0352] 이와 같은, 정보 기록 매체 제조 장치에 의해 생성된 정보 기록 매체(910)에는, 도 1 및 기타를 참조하여 설명한 각종의 데이터가 기록된다. 구체적으로는, 적어도 컨텐츠 데이터를 저장한 컨텐츠 파일과 컨텐츠의 이용을 행할 때 실행해야 할 시큐리티 체크 처리용 프로그램, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일을 포함하는 구성으로 된다.

[0353] 정보 기록 매체(910)에 기록되는 컨텐츠 코드 파일은, 컨텐츠 코드의 구성 데이터를 암호화한 암호화 데이터를 포함한다. 구체적인 컨텐츠 코드의 암호화 태양으로서는, 먼저, 도 13, 도 14를 참조하여 설명한 태양이 있다. 즉, 컨텐츠 코드의 구성 데이터를, 노드 키를 직접 적용하여 암호화한 코드 정보 암호화 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일이나, 컨텐츠 코드의 구성 데이터를 노드 키와는 상이한 고유 암호 키(오리지날 암호 키)로 암호화한 코드 정보 암호화 데이터와, 고유 암호 키를 노드 키로 암호화한 암호화 키 데이터를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일 등이 저장된다.

[0354] 그리고, 정보 기록 매체(910)에 기록되는 컨텐츠 코드 파일은, 정보 처리 장치에 대응하는 시큐리티 체크 코드, 및 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 데이터 변환 처리에 적용하는 데이터 생성 처리 코드 중 적어도 어느 하나의 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일이며, 또한, 정보 기록 매체에 저장된 컨텐츠의 구성 데이터의 일부에 정보 처리 장치 또는 컨텐츠 이용 어플리케이션에 대응하는 식별 정보를 매립하는 데이터 변환 처리에 적용하는 데이터 생성 처리 코드를 포함하는 컨텐츠 코드를 저장한 컨텐츠 코드 파일이 포함된다.

[0355] 이상, 특정한 실시예를 참조하면서, 본 발명에 대하여 상세하게 설명하였다. 그러나, 본 발명의 요지를 벗어나지 않는 범위에서 당업자가 상기 실시예의 수정이나 대용을 해낼 수 있는 것은 자명하다. 즉, 예시의 형태로 본 발명을 개시한 것이며, 한정적으로 해석해서는 안 된다. 본 발명의 요지를 판단하기 위해서는, 특허 청구의 범위를 참작해야한다.

[0356] 그리고, 명세서 중에 있어서 설명한 일련의 처리는 하드웨어, 또는 소프트 웨어, 또는 양자의 복합 구성에 의해 실행할 수 있다. 소프트 웨어에 의한 처리를 실행하는 경우에는, 처리 시퀀스를 기록한 프로그램을, 전용의 하드웨어에 내장된 컴퓨터 내의 메모리에 인스톨 하여 실행시키거나, 또는 각종 처리를 실행할 수 있는 범용 컴퓨터에 프로그램을 인스톨 하여 실행시키는 것이 가능하다.

[0357] 예를 들면, 프로그램은 기록 매체로서의 하드 디스크나 ROM(Read Only Memory)에 미리 기록하여 둘 수가 있다. 또는, 프로그램은 플렉시블 디스크, CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)디스크, DVD(Digital Versatile Disc), 자기 디스크, 반도체 메모리 등의 분리성(removable) 기록 매체에, 일시적 또는 영속적으로 저장(기록)해 둘 수가 있다. 이와 같은 분리성 기록 매체는, 이른바 패키지 소프트웨어로서 제공할 수 있다.

[0358] 그리고, 프로그램은, 전술한 바와 같은 분리성 기록 매체로부터 컴퓨터에 인스톨하는 것 외에, 다운로드 사이트로부터, 컴퓨터에 무선 전송하거나, LAN(Local Area Network), 인터넷과 같은 네트워크를 통하여, 컴퓨터에 유선으로 전송하고, 컴퓨터에서는, 그와 같이 전송되어 오는 프로그램을 수신하고, 내장된 하드 디스크 등의 기록 매체에 인스톨 할 수 있다.

[0359] 그리고, 명세서에 기재된 각종의 처리는, 기재에 따라 시계열로 실행될 뿐 아니라, 처리를 실행하는 장치의 처리 능력 또는 필요에 따라 병렬적으로 또는 개별적으로 실행되어도 된다. 또, 본 명세서에 있어서 시스템은,

복수개의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 하우징 내에 있는 것에는 한정되지 않는다.

산업상 이용 가능성

[0360] 이상, 설명한 바와 같이, 본 발명의 일 실시예의 구성에 의하면, 정보 기록 매체에 기록된 데이터 처리 프로그램을 포함하는 컨텐츠 코드를 취득하고, 컨텐츠 코드에 따른 시큐리티 체크 처리나 컨텐츠의 구성 데이터의 변환 처리, 플레이어 정보의 컨텐츠에 대한 매립 처리 등의 데이터 처리를 실행하는 구성에 있어서, 컨텐츠 코드 중 적어도 일부를 암호화 데이터로서 설정하고, 그 암호 키로서, 계층 구성을 가지는 키 트리의 노드에 대응하여 설정된 노드 키를 적용하는 구성으로 하였다. 노드 키를 적용하여 컨텐츠 코드의 암호화부를 복호 할 수 있는 플레이어는 미리 특정하는 것이 가능하며, 각 플레이어에 대응하는 적정한 컨텐츠 코드만을 처리시키는 것이 가능해지고, 부정한 컨텐츠 코드의 적용 처리를 방지하는 구성이 실현된다.

도면의 간단한 설명

[0083] 도 1은 정보 기록 매체의 저장 데이터 및 드라이브 장치, 정보 처리 장치의 구성 및 처리에 대하여 설명하는 도면이다.

[0084] 도 2는 정보 기록 매체의 저장 컨텐츠에 대하여 설정하는 컨텐츠 관리 유닛의 설정예에 대하여 설명하는 도면이다.

[0085] 도 3은 정보 기록 매체의 저장 컨텐츠에 대하여 설정하는 컨텐츠 관리 유닛과 유닛 키와의 대응에 대하여 설명하는 도면이다.

[0086] 도 4는 정보 기록 매체에 기록되는 컨텐츠와, 컨텐츠 재생에 있어서 필요한 데이터 변환 처리에 대하여 설명하는 도면이다.

[0087] 도 5는 컨텐츠 재생 처리의 처리예에 대하여 설명하는 도면이다.

[0088] 도 6은 컨텐츠 재생시에 실행하는 데이터 변환 처리에 대하여 설명하는 도면이다.

[0089] 도 7은 정보 기록 매체에 기록되는 데이터의 디렉토리 구성을 나타낸 도면이다.

[0090] 도 8은 정보 기록 매체에 기록되는 컨텐츠, 관리 데이터 등의 디렉토리 구성을 나타낸 도면이다.

[0091] 도 9는 정보 기록 매체에 기록되는 컨텐츠 코드의 디렉토리 구성을 나타낸 도면이다.

[0092] 도 10은 정보 기록 매체에 기록되는 컨텐츠 코드의 생성, 기록 프로세스의 상세에 대하여 설명하는 도면이다.

[0093] 도 11은 플레이어 증명서의 데이터 구성예에 대하여 설명하는 도면이다.

[0094] 도 12는 플레이어에 대하여 배포되는 암호 키의 설정예에 대하여 설명하는 도면이다.

[0095] 도 13은 정보 기록 매체에 저장하는 컨텐츠 코드의 생성 처리, 암호화 처리 구성에 대하여 설명하는 도면이다.

[0096] 도 14는 정보 기록 매체에 저장하는 컨텐츠 코드의 생성 처리, 암호화 처리 구성에 대하여 설명하는 도면이다.

[0097] 도 15는 정보 처리 장치에서의 컨텐츠 코드의 이용 처리 시퀀스에 대하여 설명하는 도면이다.

[0098] 도 16은 정보 처리 장치에서의 컨텐츠 코드의 이용 처리 시퀀스에 대하여 설명하는 도면이다.

[0099] 도 17은 플레이어에 대하여 배포되는 암호 키의 설정예에 대하여 설명하는 도면이다.

[0100] 도 18은 플레이어에 대하여 배포되는 암호 키의 설정예에 대하여 설명하는 도면이다.

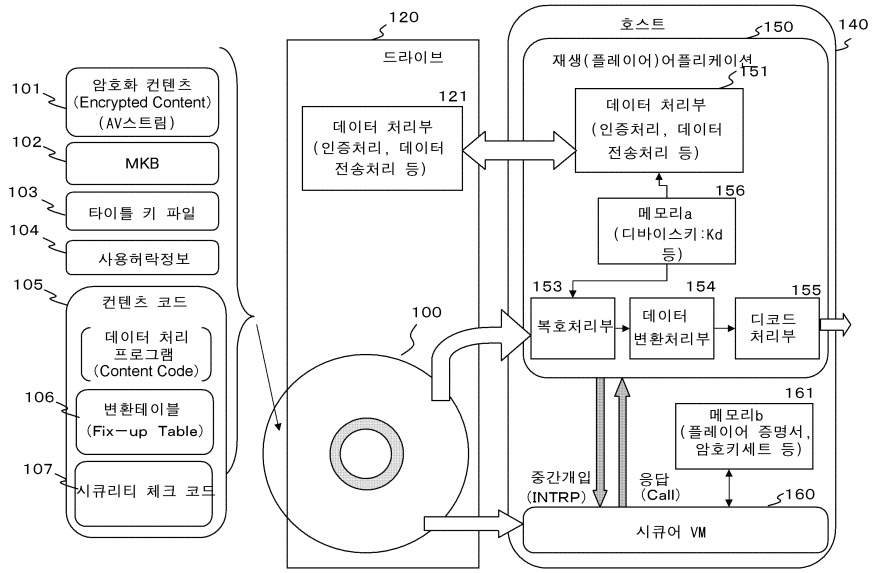
[0101] 도 19는 정보 처리 장치에서의 컨텐츠 재생에 따른 처리의 실행 시퀀스에 대하여 설명하는 플로차트를 나타낸 도면이다.

[0102] 도 20은 정보 처리 장치의 하드웨어 구성예에 대하여 설명하는 도면이다.

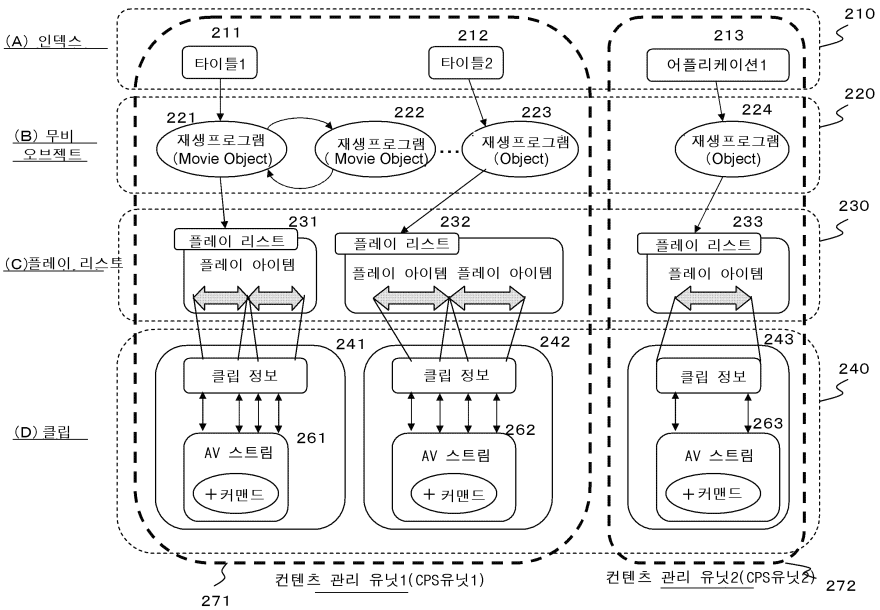
[0103] 도 21은 정보 기록 매체 제조 장치의 구성에 대하여 설명하는 블록도이다.

도면

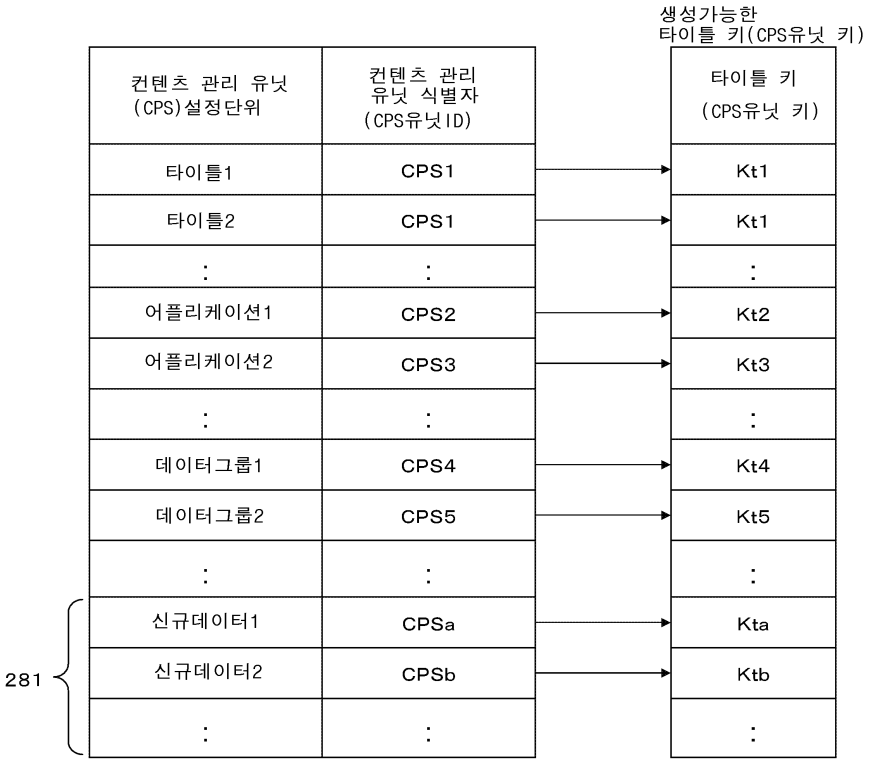
도면1


120
드라이브
121
데이터 처리부
(인증처리, 데이터 전송처리 등)
100
호스트
140
150
재생(플레이어)어플리케이션
151
데이터 처리부
(인증처리, 데이터 전송처리 등)
156
메모리a
(디바이스키:Kd 등)
153
154
155
복호처리부
데이터 변환처리부
디코드 처리부
161
메모리b
(플레이어 증명서, 암호키세트 등)
중간개입
(INTRP)
응답
(Call)
160
시큐어 VM
101
암호화 컨텐츠
(Encrypted Content)
(AV스트림)
102
MKB
103
타이틀 키 파일
104
사용허락정보
105
컨텐츠 코드
데이터 처리 프로그램
(Content Code)
106
변환테이블
(Fix-up Table)
107
시큐리티 체크 코드

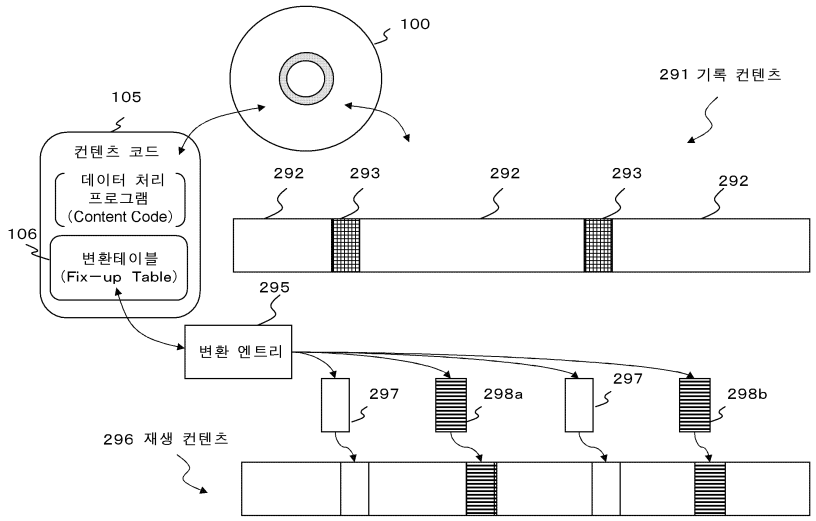
도면2


(A) 인덱스
(B) 무비 오브젝트
(C)플레이 리스트
(D) 클립
210
211
타이틀1
212
타이틀2
213
어플리케이션1
220
221
재생프로그램
(Movie Object)
222
재생프로그램
(Movie Object)
223
재생프로그램
(Object)
224
재생프로그램
(Object)
230
231
플레이 리스트
플레이 아이템
232
플레이 리스트
플레이 아이템 플레이 아이템
233
플레이 리스트
플레이 아이템
240
241
클립 정보
242
클립 정보
243
클립 정보
261
AV 스트림
+커맨드
262
AV 스트림
+커맨드
263
AV 스트림
+커맨드
271
컨텐츠 관리 유닛1(CPS유닛1)
272
컨텐츠 관리 유닛2(CPS유닛2)

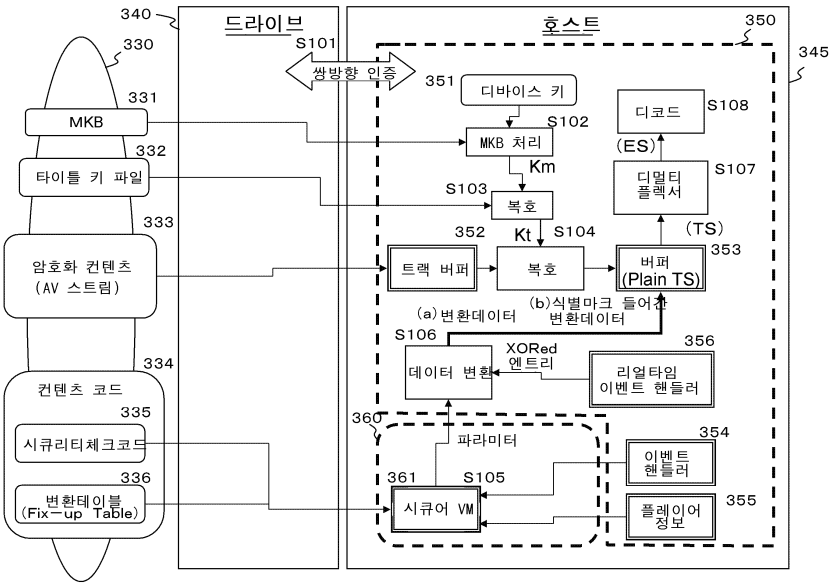
도면3


생성가능한
타이틀 키(CPS유닛 키)
컨텐츠 관리 유닛
(CPS)설정단위
컨텐츠 관리
유닛 식별자
(CPS유닛ID)
타이틀 키
(CPS유닛 키)
타이틀1
CPS1
Kt1
타이틀2
CPS1
Kt1
어플리케이션1
CPS2
Kt2
어플리케이션2
CPS3
Kt3
데이터그룹1
CPS4
Kt4
데이터그룹2
CPS5
Kt5
신규데이터1
CPSa
Kta
신규데이터2
CPSb
Ktb
281

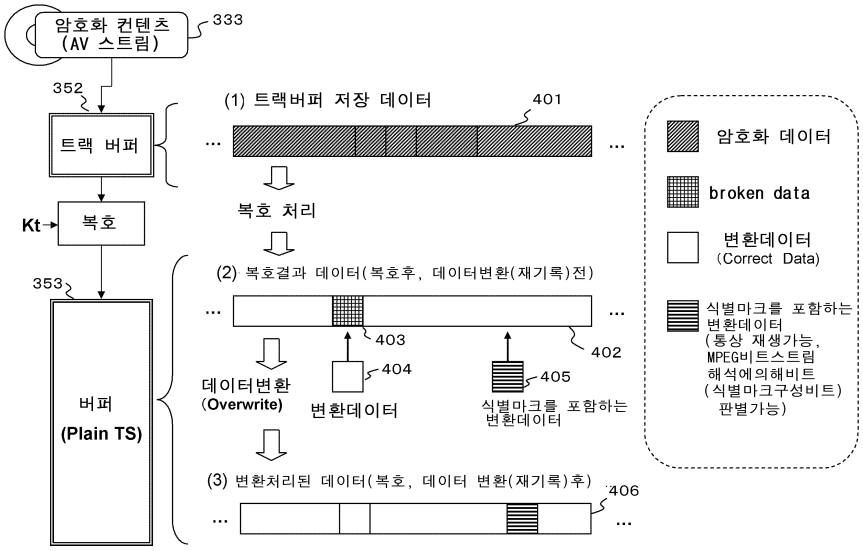
도면4


100
105
컨텐츠 코드
데이터 처리
프로그램
(Content Code)
106
변환테이블
(Fix-up Table)
291 기록 컨텐츠
292
293
292
293
292
295
변환 엔트리
297
298a
297
298b
296 재생 컨텐츠

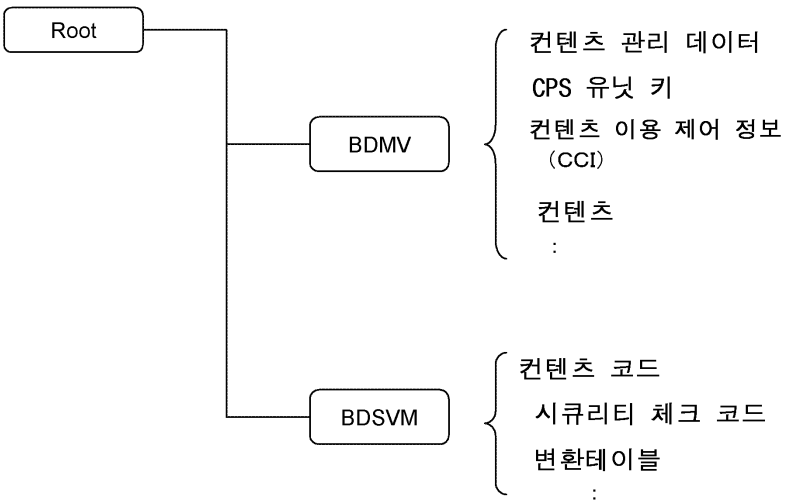
도면5


340
드라이브
호스트
350
345
330
S101
쌍방향 인증
351
디바이스 키
331
MKB
S102
MKB 처리
디코드
S108
(ES)
332
타이틀 키 파일
Km
디멀티
플렉서
S107
S103
복호
333
352
Kt
S104
(TS)
암호화 컨텐츠
(AV 스트림)
트랙 버퍼
복호
버퍼
(Plain TS)
353
(a)변환데이터
(b)식별마크 들어간
변환데이터
S106
356
334
XORed
엔트리
데이터 변환
리얼타임
이벤트 핸들러
컨텐츠 코드
360
335
파라미터
354
시큐리티체크코드
이벤트
핸들러
361
S105
336
시큐어 VM
355
변환테이블
(Fix-up Table)
플레이어
정보

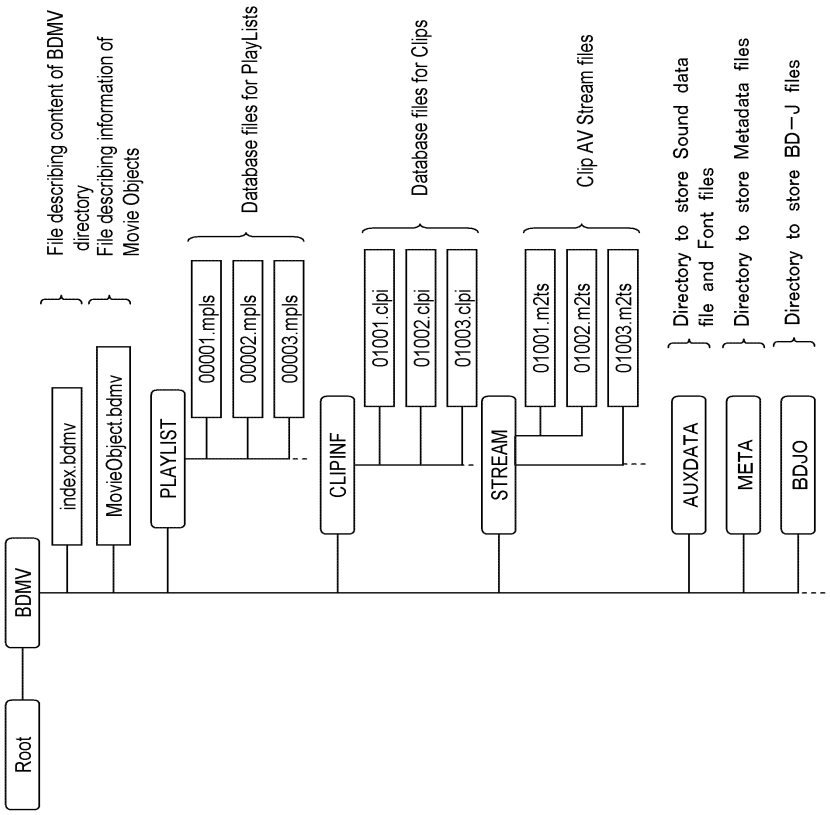
도면6


암호화 컨텐츠
(AV 스트림)
333
352
(1) 트랙버퍼 저장 데이터
401
트랙 버퍼
복호 처리
Kt
복호
(2) 복호결과 데이터(복호후, 데이터변환(재기록)전)
353
403
402
404
405
데이터변환
(Overwrite)
변환데이터
식별마크를 포함하는
변환데이터
버퍼
(Plain TS)
(3) 변환처리된 데이터(복호, 데이터 변환(재기록)후)
406
암호화 데이터
broken data
변환데이터
(Correct Data)
식별마크를 포함하는
변환데이터
(통상 재생가능,
MPEG비트스트림
해석에의해비트
(식별마크구성비트)
판별가능)

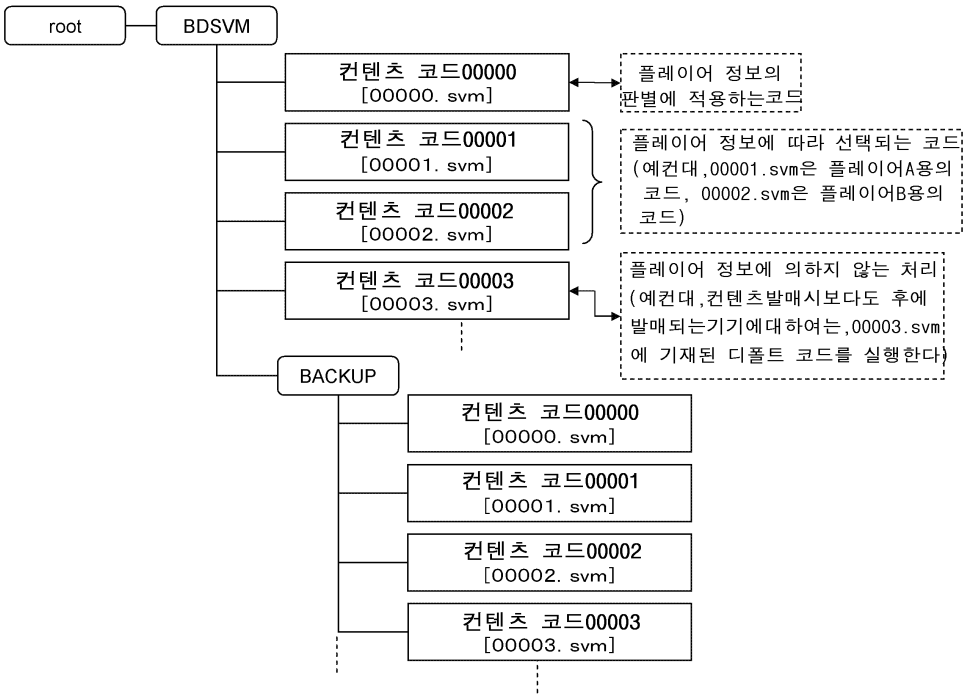
도면7


Root
BDMV
BDSVM
컨텐츠 관리 데이터
CPS 유닛 키
컨텐츠 이용 제어 정보
(CCI)
컨텐츠
:
컨텐츠 코드
시큐리티 체크 코드
변환테이블
:

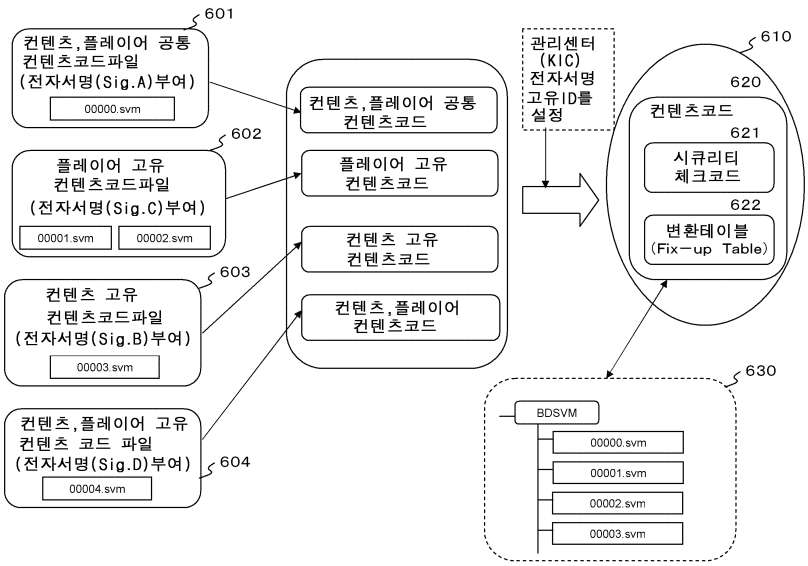
도면8


Root
BDMV
index.bdmv
MovieObject.bdmv
PLAYLIST
CLIPINF
STREAM
AUXDATA
META
BDJO
00001.mpls
00002.mpls
00003.mpls
01001.clpi
01002.clpi
01003.clpi
01001.m2ts
01002.m2ts
01003.m2ts
File describing content of BDMV directory
File describing information of Movie Objects
Database files for PlayLists
Database files for Clips
Clip AV Stream files
Directory to store Sound data file and Font files
Directory to store Metadata files
Directory to store BD-J files

도면9


root
BDSVM
컨텐츠 코드00000
[00000. svm]
컨텐츠 코드00001
[00001. svm]
컨텐츠 코드00002
[00002. svm]
컨텐츠 코드00003
[00003. svm]
플레이어 정보의 판별에 적용하는코드
플레이어 정보에 따라 선택되는 코드 (예컨대,00001.svm은 플레이어A용의 코드, 00002.svm은 플레이어B용의 코드)
플레이어 정보에 의하지 않는 처리 (예컨대,컨텐츠발매시보다도 후에 발매되는기기에대하여는,00003.svm에 기재된 디폴트 코드를 실행한다)
BACKUP
컨텐츠 코드00000
[00000. svm]
컨텐츠 코드00001
[00001. svm]
컨텐츠 코드00002
[00002. svm]
컨텐츠 코드00003
[00003. svm]

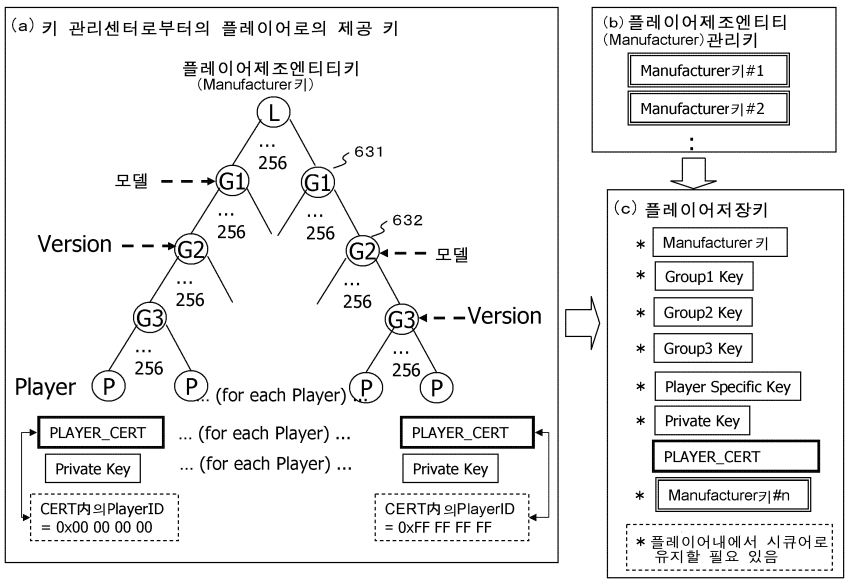
도면10


601
컨텐츠,플레이어 공통 컨텐츠코드파일 (전자서명(Sig.A)부여)
00000.svm
602
플레이어 고유 컨텐츠코드파일 (전자서명(Sig.C)부여)
00001.svm
00002.svm
603
컨텐츠 고유 컨텐츠코드파일 (전자서명(Sig.B)부여)
00003.svm
컨텐츠,플레이어 고유 컨텐츠 코드 파일 (전자서명(Sig.D)부여)
00004.svm
604
컨텐츠,플레이어 공통 컨텐츠코드
플레이어 고유 컨텐츠코드
컨텐츠 고유 컨텐츠코드
컨텐츠,플레이어 컨텐츠코드
관리센터 (KIC) 전자서명 고유ID를 설정
610
620
컨텐츠코드
621
시큐리티 체크코드
622
변환테이블 (Fix-up Table)
630
BDSVM
00000.svm
00001.svm
00002.svm
00003.svm

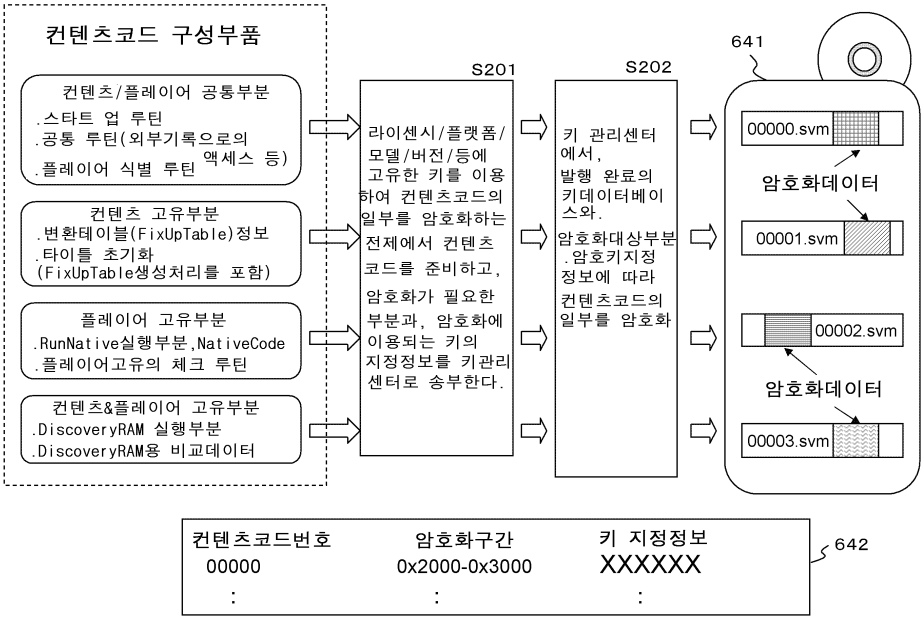
도면11

필 드
플레이어증명서사이즈(PlayerCertificateSize)
증명서 버전 (CertificateVersion)
플레이어제조자식별자(ManufacturerID)
시리얼번호
서명일시
디바이스(플레이어)속성정보
플레이어공개키(PlayerPublicKey)
전자서명(Signature)

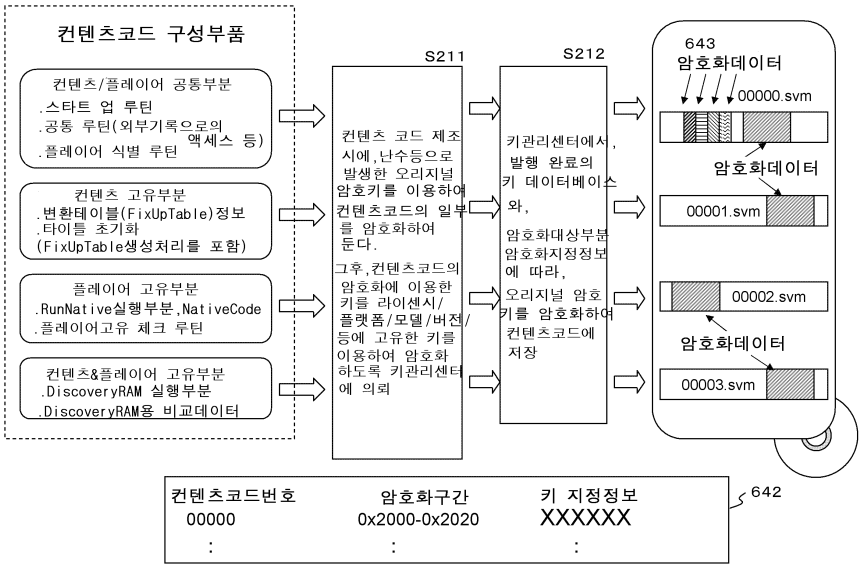
도면12



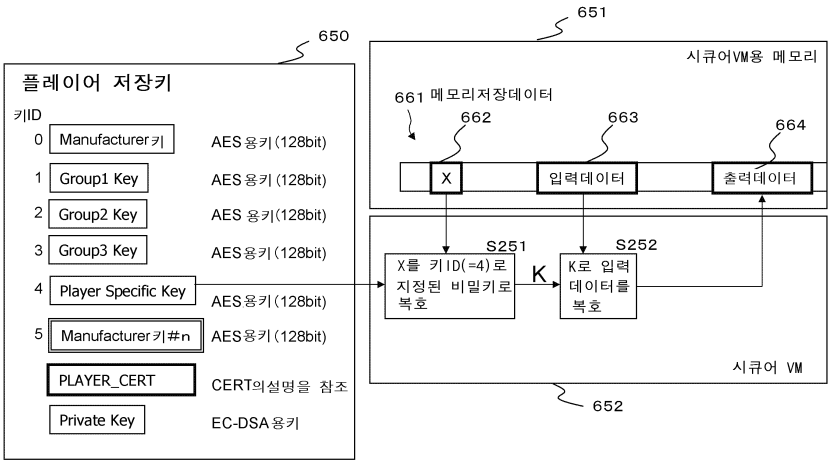
도면13


컨텐츠코드 구성부품
컨텐츠/플레이어 공통부분
.스타트 업 루틴
.공통 루틴(외부기록으로의 액세스 등)
.플레이어 식별 루틴
컨텐츠 고유부분
.변환테이블(FixUpTable)정보
.타이틀 초기화
(FixUpTable생성처리를 포함)
플레이어 고유부분
.RunNative실행부분,NativeCode
.플레이어고유의 체크 루틴
컨텐츠&플레이어 고유부분
.DiscoveryRAM 실행부분
.DiscoveryRAM용 비교데이터
S201
라이센시/플랫폼/모델/버전/등에 고유한 키를 이용하여 컨텐츠코드의 일부를 암호화하는 전제에서 컨텐츠 코드를 준비하고, 암호화가 필요한 부분과, 암호화에 이용되는 키의 지정정보를 키관리센터로 송부한다.
S202
키 관리센터에서, 발행 완료의 키데이터베이스와.
암호화대상부분 .암호키지정정보에 따라 컨텐츠코드의 일부를 암호화
641
00000.svm
암호화데이터
00001.svm
00002.svm
암호화데이터
00003.svm
컨텐츠코드번호
암호화구간
키 지정정보
00000
0x2000-0x3000
XXXXXX
642

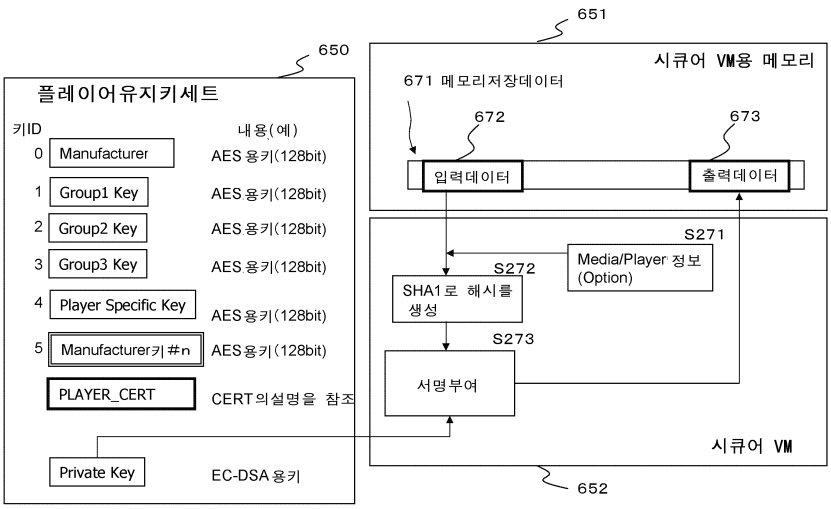
도면14


컨텐츠코드 구성부품
컨텐츠/플레이어 공통부분
.스타트 업 루틴
.공통 루틴(외부기록으로의 액세스 등)
.플레이어 식별 루틴
컨텐츠 고유부분
.변환테이블(FixUpTable)정보
.타이틀 초기화
(FixUpTable생성처리를 포함)
플레이어 고유부분
.RunNative실행부분,NativeCode
.플레이어고유 체크 루틴
컨텐츠&플레이어 고유부분
.DiscoveryRAM 실행부분
.DiscoveryRAM용 비교데이터
S211
컨텐츠 코드 제조시에,난수등으로 발생한 오리지널 암호키를 이용하여 컨텐츠코드의 일부를 암호화하여 둔다.
그후,컨텐츠코드의 암호화에 이용한 키를 라이센시/플랫폼/모델/버전/등에 고유한 키를 이용하여 암호화하도록 키관리센터에 의뢰
S212
키관리센터에서, 발행 완료의 키 데이터베이스와,
암호화대상부분 암호화지정정보에 따라, 오리지널 암호키를 암호화하여 컨텐츠코드에 저장
643
암호화데이터
00000.svm
암호화데이터
00001.svm
00002.svm
암호화데이터
00003.svm
컨텐츠코드번호
암호화구간
키 지정정보
00000
0x2000-0x2020
XXXXXX
642

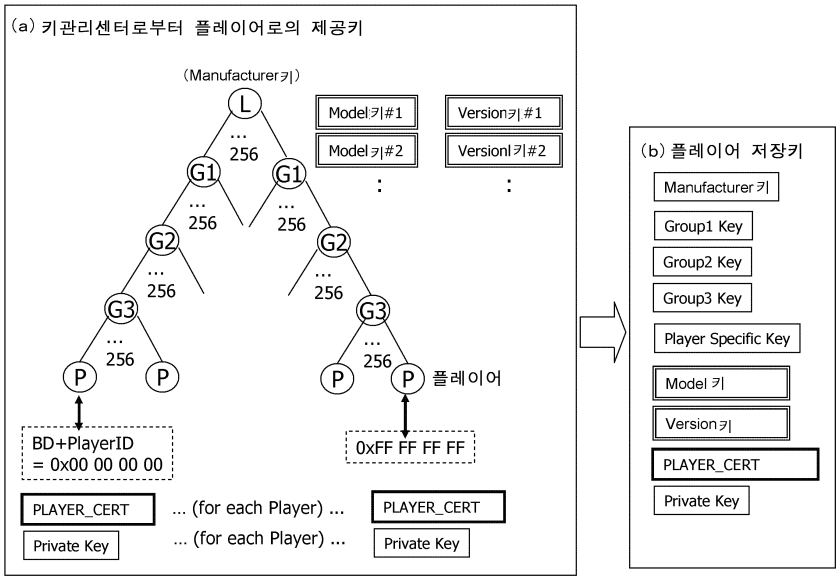
도면15


650
플레이어 저장키
키ID
0 Manufacturer키 AES 용키(128bit)
1 Group1 Key AES 용키(128bit)
2 Group2 Key AES 용키(128bit)
3 Group3 Key AES 용키(128bit)
4 Player Specific Key AES 용키(128bit)
5 Manufacturer키#n AES 용키(128bit)
PLAYER_CERT CERT의 설명을 참조
Private Key EC-DSA 용키
651
시큐어VM용 메모리
661 메모리저장데이터
662
663
664
X
입력데이터
출력데이터
S251
X를 키ID(=4)로 지정된 비밀키로 복호
K
S252
K로 입력 데이터를 복호
시큐어 VM
652

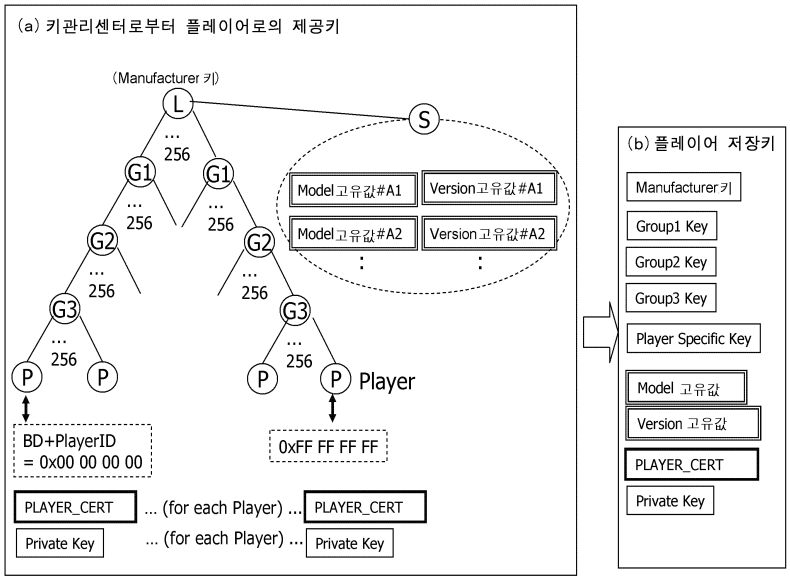
도면16


650
플레이어유지키세트
키ID
내용(예)
0 Manufacturer AES 용키(128bit)
1 Group1 Key AES 용키(128bit)
2 Group2 Key AES 용키(128bit)
3 Group3 Key AES 용키(128bit)
4 Player Specific Key AES 용키(128bit)
5 Manufacturer키#n AES 용키(128bit)
PLAYER_CERT CERT의 설명을 참조
Private Key EC-DSA 용키
651
시큐어 VM용 메모리
671 메모리저장데이터
672
673
입력데이터
출력데이터
S271
Media/Player 정보 (Option)
S272
SHA1로 해시를 생성
S273
서명부여
시큐어 VM
652

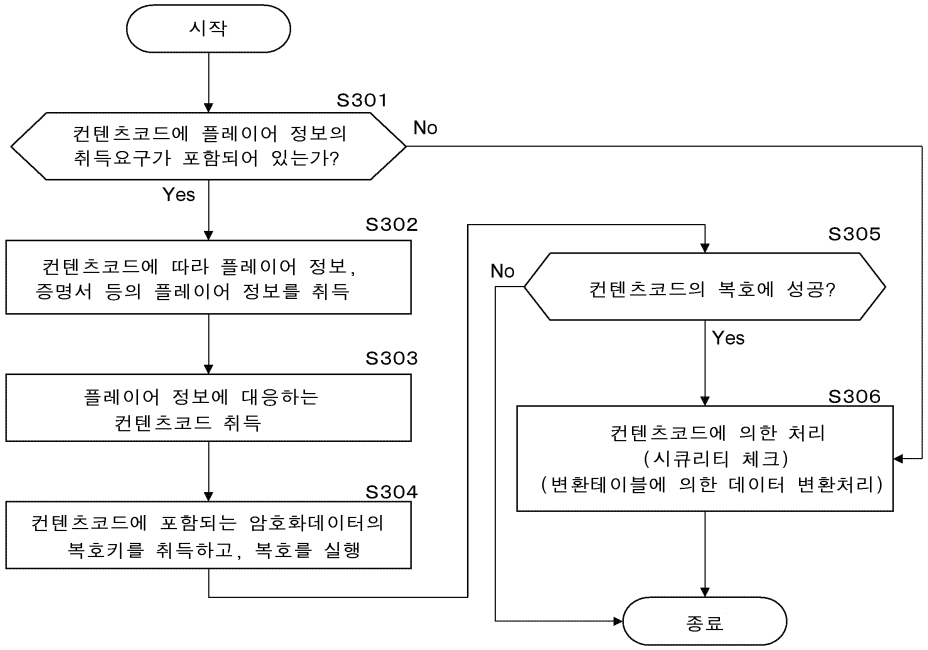
도면17


(a) 키관리센터로부터 플레이어로의 제공키
(Manufacturer키)
L
256
Model키#1
Model키#2
Version키#1
Version키#2
G1
G2
G3
P
플레이어
BD+PlayerID
= 0x00 00 00 00
0xFF FF FF FF
PLAYER_CERT
Private Key
... (for each Player) ...
(b) 플레이어 저장키
Manufacturer키
Group1 Key
Group2 Key
Group3 Key
Player Specific Key
Model 키
Version키
PLAYER_CERT
Private Key

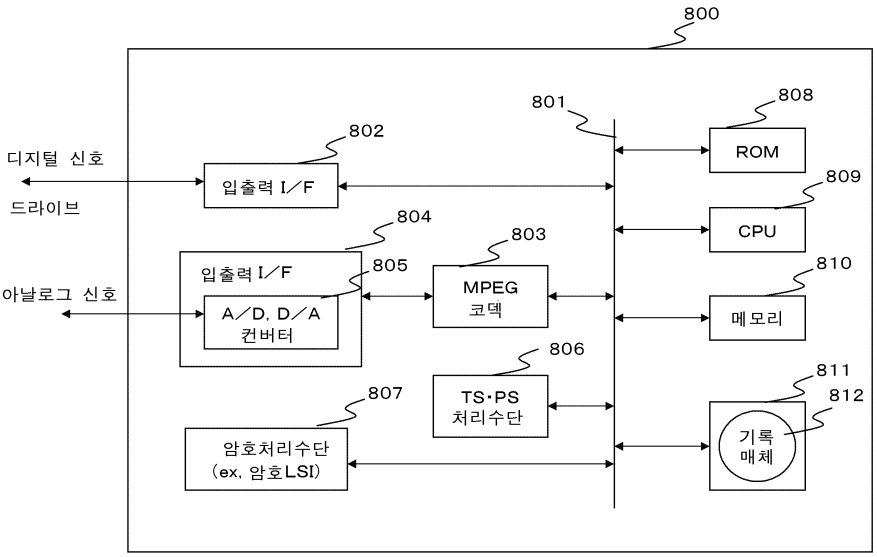
도면18


(a) 키관리센터로부터 플레이어로의 제공키
(Manufacturer키)
L
S
256
G1
G2
G3
P
Player
Model고유값#A1
Version고유값#A1
Model고유값#A2
Version고유값#A2
BD+PlayerID
= 0x00 00 00 00
0xFF FF FF FF
PLAYER_CERT
Private Key
... (for each Player) ...
(b) 플레이어 저장키
Manufacturer키
Group1 Key
Group2 Key
Group3 Key
Player Specific Key
Model 고유값
Version 고유값
PLAYER_CERT
Private Key

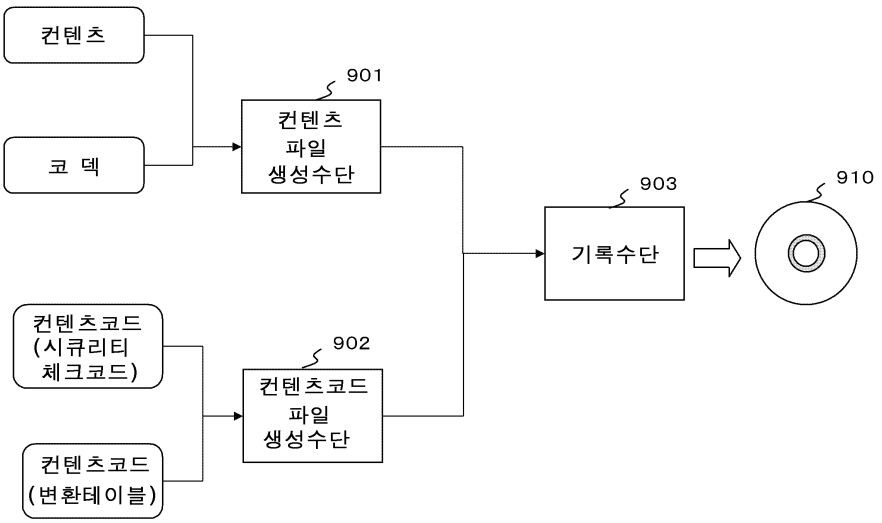
도면19


시작
S301
컨텐츠코드에 플레이어 정보의 취득요구가 포함되어 있는가?
No
Yes
S302
컨텐츠코드에 따라 플레이어 정보, 증명서 등의 플레이어 정보를 취득
S303
플레이어 정보에 대응하는 컨텐츠코드 취득
S304
컨텐츠코드에 포함되는 암호화데이터의 복호키를 취득하고, 복호를 실행
S305
No
컨텐츠코드의 복호에 성공?
Yes
S306
컨텐츠코드에 의한 처리 (시큐리티 체크) (변환테이블에 의한 데이터 변환처리)
종료

도면20


800
801
808
ROM
802
디지털 신호
입출력 I/F
드라이브
809
CPU
804
803
입출력 I/F
805
MPEG 코덱
810
아날로그 신호
A/D, D/A 컨버터
메모리
806
811
TS·PS 처리수단
807
812
암호처리수단 (ex, 암호LSI)
기록 매체

도면21


컨텐츠
코 덱
901
컨텐츠
파일
생성수단
903
기록수단
910
컨텐츠코드
(시큐리티
체크코드)
902
컨텐츠코드
파일
생성수단
컨텐츠코드
(변환테이블)