(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G11B 20/10 (2006.01)

(11) 공개번호 10-2006-0048496
(43) 공개일자 2006년05월18일

(21) 출원번호 10-2005-0054544
(22) 출원일자 2005년06월23일

(30) 우선권주장 JP-P-2004-00185897 2004년06월24일 일본(JP)

(71) 출원인 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 가자미 신이치
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고 소니가부시끼 가이샤내
다카하시 가즈요시
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고 소니가부시끼 가이샤내

(74) 대리인 유미특허법인

심사청구 : 없음

(54) 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법,및 컴퓨터·프로그램

요약

본 발명은 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법, 및 컴퓨터·프로그램 에 관한 것으로서, 데이터 유출을 방지할 수 있는 정보 기록 매체의 기록 데이터 검증 처리 구성을 제공한다. 정보 기록 매체로부터의 재생 데이터에 따른 연산 결과로서 산출된 요약값, 예를 들면 MDC(메시지 다이제스트 코드)를 검증용 재생 데이터로 하여, 비교 대조부에 출력하고, 데이터 비교 대조부에 있어서, 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 결과인 검증용 기록 데이터(MDC)와의 비교 대조를 실행한다. 본 구성에 의해, 비교 대조부로의 출력 데이터를 컨텐츠나 키 정보 등의 실(實)데이터가 아닌 연산 결과 데이터(MDC)로 하는 것이 가능해져, 컨텐츠나 키 정보 등의 실데이터의 유출을 방지할 수 있다.

대표도

도 3

색인어

정보 기록 매체, 검증 장치, 검증 방법, 컴퓨터·프로그램

명세서

도면의 간단한 설명

도 1은 종래의 정보 기록 매체 검증 처리 구성에 대하여 설명하는 도면이다.

도 2는 일반적인 정보 기록 매체의 제조 루트, 데이터 공급 구성에 대하여 설명하는 도면이다.

도 3은 본 발명의 정보 기록 매체 검증 처리 구성에 대하여 설명하는 도면이다.

도 4는 본 발명의 정보 기록 매체 검증 처리 구성에 대하여 설명하는 도면이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은, 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법, 및 컴퓨터 프로그램에 관한 것이다. 또한, 상세하게는, 예를 들면 저작권 보호 대상의 컨텐츠 등을 저장한 정보 기록 매체에 저장된 암호 키 등 유출을 방지해야 할 정보에 대하여, 시큐리티를 높여 확실한 검증을 실현하는 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법, 및 컴퓨터·프로그램에 관한 것이다.

음악 등의 오디오 데이터, 영화 등의 화상 데이터, 게임 프로그램, 각종 어플리케이션 프로그램 등, 다양한 소프트 웨어 데이터(이하, 이들을 컨텐츠(Content라고 함)는, 기록 미디어, 예를 들면, 청색 레이저를 적용한 Blu-ray 디스크, 또는 DVD(Digital Versatile Disc), MD(Mini Disc), CD(Compact Disc)에 디지털 데이터로서 저장할 수 있다. 특히, 청색 레이저를 이용한 Blu-ray 디스크는, 고밀도 기록 가능한 디스크이며 대용량의 영상 컨텐츠 등을 고화질 데이터로서 기록할 수 있다. 이들 다양한 정보 기록 매체(기록 미디어)에 디지털 컨텐츠가 저장되고, 사용자에게 제공된다.

사용자는, 소유하는 PC(Personal Computer), 디스크 플레이어 등의 재생 장치에 있어서 컨텐츠의 재생, 이용을 행한다.

음악 데이터, 화상 데이터 등, 많은 컨텐츠는, 일반적으로 그 작성자 또는 판매자에게 반포권 등이 보유되어 있다. 따라서, 이들 컨텐츠의 배포에 즈음해서는, 일정한 이용 제한, 즉 정규의 사용자에게 대하여만, 컨텐츠의 이용을 허락하고, 허가가 없는 복제 등이 행해지지 않도록 하는 구성을 취하는 것이 일반적으로 되어 있다.

디지털 기록 장치 및 기록 매체에 의하면, 예를 들면 화상이나 음성을 열화시키는 일 없이 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.

DVD, 또는 최근 개발이 진행되고 있는 청색 레이저를 이용한 기록 매체 등의 대용량형 기록 매체는, 1개의 매체에 예를 들면 영화 1개~수개분의 대량의 데이터를 디지털 정보로서 기록할 수 있다. 이와 같이 영상 정보 등을 디지털 정보로서 기록하는 것이 가능해지면 부정 카피를 방지하여 저작권자의 보호를 도모하는 것이 더욱 더 중요한 과제로 되어 있다. 최근에는, 이와 같은 디지털 데이터의 부정한 카피를 방지하기 위해 디지털 기록 장치 및 기록 매체에 위법한 카피를 방지하기 위한 다양한 기술이 실용화되어 있다.

컨텐츠를 저장한 CD, DVD 등의 정보 기록 매체를 제조하는 경우, 컨텐츠 오너, 컨텐츠 편집자, 디스크 제조자, 또한 암호처리에 적용하는 키의 관리, 발행 처리를 행하는 키 관리 센터(KIC: Key Issuing Center) 등의 복수개의 엔티티가, 필요한 정보의 제공을 행하고, 각 엔티티 사이에서 정보를 유통, 검증하면서 정보 기록 매체를 제조한다.

예를 들면 디스크 제조 플랜트로서의 디스크 제조 엔티티는, 컨텐츠 편집자 등으로부터 제공된 데이터의 정당성 검증을 행하여, 디스크에 대한 데이터 기록 처리를 실행한다. 또한, 디스크 제조 엔티티에 있어서는, 디스크에 기록된 데이터가 기록 예정 데이터와 일치하는 것의 확인 처리가 실행된다. 이 처리는, 데이터 기록필 디스크로부터의 재생 데이터와, 기록 예정 데이터와의 대조 처리에 따라 실행된다. 그러나, 이와 같은 데이터 검증을 실행하는 경우, 검증용의 재생 데이터가 유출될 우려가 있다. 이와 같은 데이터 유출이 발생하면, 컨텐츠 권리자의 이익이 손상되게 된다.

도 1을 참조하여, 일반적인 디스크 제조 및 검증 처리에 대하여 설명한다.

도 1에는, 키의 관리, 발행 처리를 행하는 키 관리 센터(KIC: Key Issuing Center)(101), 컨텐츠 편집 처리를 실행하는 스튜디오 등의 컨텐츠 편집 엔티티(102), 디스크 제조 플랜트로서의 정보 기록 매체 제조 엔티티(110)를 나타내고 있다. 정보 기록 매체 제조 엔티티(110)는, 키 관리 센터(101)가 발행하는 암호 키 및 키 생성 정보 등의 암호 키 관련 정보를 수령하고, 또 컨텐츠 편집 엔티티(102)로부터 디스크에 기록하기 위한 편집 컨텐츠, 그 외의 컨텐츠 관련 정보를 수령한다.

정보 기록 매체 제조 엔티티(110)는, 기록 데이터 생성부(Formatter)(111)에 있어서, 키 관리 센터(101)로부터 수령한 암호 키 및 암호 키 관련 정보, 컨텐츠 편집 엔티티(102)로부터 수령한 편집 컨텐츠 등을 소정 포맷으로 정보 기록 매체(Disc)(112)에 기록하는 처리를 실행한다. 그리고, 이 때, 기록 데이터 생성부(111)는, 필요에 따라, 키 관리 센터(101)로부터 수령한 암호 키를 적용한 컨텐츠 등의 암호화 처리를 행하고, 생성된 암호화 데이터를 정보 기록 매체(112)에 기록한다.

정보 기록 매체에는, 컨텐츠 및 다양한 암호 키 정보가 기록되게 된다. 정보 기록 매체 제조 엔티티(110)는, 다음에, 데이터 기록필의 정보 기록 매체(112)에 정확한 데이터가 기록되어 있는지 여부의 검증 처리를 실행한다. 이 검증 처리는, 기록필 디스크 모두, 또는 샘플링된 일부의 디스크에 대하여 실행된다.

이 데이터 검증 처리는, 데이터 재생부(Drive)(113)에 있어서 재생된 데이터와, 기록 데이터 생성부(111)의 출력 데이터와의 2개의 데이터를 정보 기록 매체 검증부(Disc Checker)(114)에 입력하고, 입력되는 2개의 데이터를 비교 대조함으로써 행해진다.

이 검증 처리의 실행에 있어서, 기록 데이터 생성부(111)로부터 정보 기록 매체 검증부(114)에 대한 데이터 입력 경로나, 데이터 재생부로부터 정보 기록 매체 검증부(114)에 대한 데이터 입력 경로에는, 비교 대조 처리의 대상 데이터로서, 유출을 방지해야 할 컨텐츠 데이터나 암호 키 정보가 전송되게 된다. 이 데이터 전송로로부터의 데이터 도청 등에 의한 데이터 유출이 발생하면, 컨텐츠 권리자의 이익이 손상되게 된다.

발명이 이루고자 하는 기술적 과제

본 발명은, 이와 같은 상황을 감안하여 이루어진 것이며, 저작권 관리 등 시큐어인 데이터 관리의 요구되는 다양한 컨텐츠가 저장된 정보 기록 매체의 생산에 있어서 실행해야 할 데이터 검증 처리를 시큐어로 확실하게 실행하는 것을 가능하게 하는 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법, 및 컴퓨터·프로그램을 제공하는 것을 목적으로 하는 것이다.

발명의 구성 및 작용

본 발명의 제1 측면은,

정보 기록 매체의 기록 데이터 검증 처리를 실행하는 정보 기록 매체 검증 장치이며,

정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생부와,

상기 데이터 재생부의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성부와,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조부

를 구비한 정보 기록 매체 검증 장치에 있다.

또한, 본 발명의 정보 기록 매체 검증 장치의 일실시예에 있어서, 상기 검증용 재생 데이터 생성부는, 정보 기록 매체로부터의 재생 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며, 상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 장치의 일실시예에 있어서, 상기 데이터 재생부는, 정보 기록 매체에 저장된 암호화 데이터를 상기 검증용 재생 데이터 생성부에 출력하는 구성이며, 상기 검증용 재생 데이터 생성부는, 상기 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며, 상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 포함되는 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 장치의 일실시예에 있어서, 상기 데이터 재생부는, 또한 정보 기록 매체로부터의 재생 데이터에 포함되는 암호화 데이터의 복호 처리를 실행하는 데이터 복호부를 가지고, 상기 데이터 재생부는, 상기 데이터 복호부에 있어서 복호된 비암호화 데이터를 상기 검증용 재생 데이터 생성부에 출력하는 구성이며, 상기 검증용 재생 데이터 생성부는, 상기 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며, 상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터의 원래의 데이터로서의 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 장치의 일실시예에 있어서, 상기 검증용 재생 데이터 생성부는, 데이터 재생부의 재생 데이터에 따른 메시지 다이제스트 코드(MDC)의 산출 처리를 실행하는 구성이며, 상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부의 생성한 메시지 다이제스트 코드(MDC)와 정보 기록 매체에 대한 기록 예정 데이터에 따른 메시지 다이제스트 코드(MDC)와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 장치의 일실시예에 있어서, 상기 데이터 재생부는, 정보 기록 매체로부터 암호화 컨텐츠 및 키 정보를 포함하는 데이터의 재생을 실행하고, 상기 데이터 비교 대조부는, 암호화 컨텐츠 또는 복호 컨텐츠에 따른 연산 결과로서의 검증용 데이터와, 키 정보에 따른 연산 결과로서의 검증용 데이터에 따라 컨텐츠 및 키 정보의 검증 처리를 실행하는 구성인 것을 특징으로 한다.

또한, 본 발명의 제2 측면은, 정보 기록 매체의 기록 데이터 검증 처리를 실행하는 정보 기록 매체 검증 방법이며,

정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생 스텝과, 상기 데이터 재생 스텝에 있어서의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성 스텝과,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조 스텝

을 포함하는 정보 기록 매체 검증 방법에 있다.

또한, 본 발명의 정보 기록 매체 검증 방법의 일실시예에 있어서, 상기 검증용 재생 데이터 생성 스텝은, 정보 기록 매체로부터의 재생 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며, 상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 방법의 일실시예에 있어서, 상기 데이터 재생 스텝은, 정보 기록 매체에 저장된 암호화 데이터를 재생, 출력하는 스텝이며, 상기 검증용 재생 데이터 생성 스텝은, 상기 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며, 상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 포함되는 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 방법의 일실시예에 있어서, 상기 정보 기록 매체 검증 방법은, 또한 정보 기록 매체로부터의 재생 데이터에 포함되는 암호화 데이터의 복호 처리를 실행하고, 비암호화 데이터를 생성하는 데이터 복호 스텝을 포함하고, 상기 검증용 재생 데이터 생성 스텝은, 상기 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며, 상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데

이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터의 원래의 데이터로서의 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 방법의 일실시예에 있어서, 상기 검증용 재생 데이터 생성 스텝은, 데이터 재생부의 재생 데이터에 따른 메시지 다이제스트 코드(MDC)의 산출 처리를 실행하는 스텝이며, 상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 메시지 다이제스트 코드(MDC)와 정보 기록 매체에 대한 기록 예정 데이터에 따른 메시지 다이제스트 코드(MDC)와의 비교 대조 처리를 실행하는 스텝인 것을 특징으로 한다.

또한, 본 발명의 정보 기록 매체 검증 방법의 일실시예에 있어서, 상기 데이터 재생 스텝은, 정보 기록 매체로부터 암호화 컨텐츠 및 키 정보를 포함하는 데이터의 재생을 실행하고, 상기 데이터 비교 대조 스텝은, 암호화 컨텐츠 또는 복호 컨텐츠에 따른 연산 결과로서의 검증용 데이터와, 키 정보에 따른 연산 결과로서의 검증용 데이터에 따라 컨텐츠 및 키 정보의 검증 처리를 실행하는 것을 특징으로 한다.

또한, 본 발명의 제3 측면은,

정보 기록 매체의 기록 데이터 검증 처리를 실행하는 컴퓨터·프로그램이며,

정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생 스텝과,

상기 데이터 재생 스텝에 있어서의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성 스텝과,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조 스텝

을 포함하는 컴퓨터·프로그램에 있다.

그리고, 본 발명의 컴퓨터·프로그램은, 예를 들면, 다양한 프로그램·코드를 실행 가능한 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 제공 가능한 컴퓨터·프로그램이다. 이와 같은 프로그램을 컴퓨터 판독 가능한 형식으로 제공함으로써, 컴퓨터·시스템 상에서 프로그램에 따른 처리가 실현된다.

본 발명의 또다른 목적, 특징이나 이점은, 후술하는 본 발명의 실시예나 첨부하는 도면에 따른 보다 상세한 설명에 따라서 명백해질 것이다. 그리고, 본 명세서에 있어서 시스템이란, 복수개의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 캐비닛 내에 있는 것에는 한정되지 않는다.

본 발명의 구성에 의하면, 정보 기록 매체로부터의 데이터 재생을 실행하여 재생 데이터에 따른 연산 처리를 실행하여 생성한 검증용 재생 데이터를 비교 대조부에 출력하고, 데이터 비교 대조부에 있어서, 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성으로 하였으므로, 검증 처리 대상 데이터로서 비교 대조부에 출력되는 데이터를 컨텐츠나 키 정보 등의 실(實)데이터와 다른 연산 결과 데이터로 하는 것이 가능해져, 검증용 데이터가 외부 유출된 경우라도 컨텐츠나 키 정보 등의 실데이터의 유출을 방지할 수 있다.

본 발명의 구성에 의하면, 비교 대조부에 출력되는 검증용 데이터는, 컨텐츠나, 키 정보 자체가 아니고, 이들 데이터에 따른 연산 결과로서 산출된 요약값, 즉 MDC(메시지 다이제스트 코드)이며, 이 MDC 데이터가 외부에 유출된 경우라도 컨텐츠 실체나 키 정보 실체가 유출되지 않고, 시큐리티를 유지해야 할 데이터가 유출될 우려는 없고, 시큐리티의 유지된 환경에서의 데이터 검증이 가능해진다.

이하, 도면을 참조하면서 본 발명의 정보 기록 매체 검증 장치, 및 정보 기록 매체 검증 방법, 및 컴퓨터·프로그램의 상세에 대하여 설명한다.

먼저, 정보 기록 매체의 제조 프로세스 개요에 대하여 설명한다.

그리고, 이하의 실시예에서는, 정보 기록 매체의 일례로서 디스크형 기록 매체를 예로서 설명하지만, 본 발명의 처리를 적용 가능한 정보 기록 매체는, 광, 자기, 반도체, 플래시 메모리 등, 다양한 형체의 정보 기록 매체를 포함하고, 디스크형의 것에 한정되는 것은 아니다.

도 2에 나타낸 바와 같이, 정보 기록 매체에 저장하는 컨텐츠는, 컨텐츠 편집 엔티티(AS: Authoring Studio)(202)에 있어서 편집되고, 그 후, 정보 기록 매체 제조 엔티티(Plant)(300)에 있어서, 사용자에게 제공되는 매체로서의 CD, DVD 등이 대량으로 복제(replicas)되어, 정보 기록 매체(200)가 제조되어 사용자에게 제공된다. 정보 기록 매체(200)는 사용자의 정보 처리 장치(204)에 있어서 재생된다.

이 디스크 제조, 판매, 사용 처리에 있어서 적용하는 암호 키 또는 키 생성 정보 등의 키 관련 정보의 발행, 관리를 실행하는 것이 키 관리 센터(KIC: Key Issuing Center)(201)이다. 키 관리 센터(KIC: Key Issuing Center)(201)은, 컨텐츠 편집 엔티티(AS: Authoring Studio)(202), 및 정보 기록 매체 제조 엔티티(Plant)(300)에 대하여 다양한 관리 정보를 제공하고, 컨텐츠 편집 엔티티(AS: Authoring Studio)(202), 및 정보 기록 매체 제조 엔티티(Plant)(300)은, 키 관리 센터(KIC: Key Issuing Center)(201)로부터 수령한 관리 정보에 따라, 컨텐츠의 편집, 암호화 키의 생성, 컨텐츠의 암호화, 데이터의 저장 처리 등을 행한다.

또, 키 관리 센터(KIC: Key Issuing Center)(201)는, 사용자의 정보 처리 장치에 있어서 정보 기록 매체(200)에 저장된 암호화 컨텐츠의 복호 처리에 적용하는 암호 키(디바이스 키)의 관리, 제공도 행한다.

다음에, 도 3을 참조하여, 본 발명에 따른 정보 기록 매체 검증 처리의 상세에 대하여 설명한다. 도 3에는, 키의 관리, 발행 처리를 행하는 키 관리 센터(201), 컨텐츠 편집 처리를 실행하는 스튜디오 등의 컨텐츠 편집 엔티티(202), 디스크 제조 플랜트로서의 정보 기록 매체 제조 엔티티(300)를 나타내고 있다.

정보 기록 매체 제조 엔티티(300)는, 키 관리 센터(201)가 발행하는 암호 키 및 키 생성 정보 등의 암호 키 관련 정보를 수령하고, 또 컨텐츠 편집 엔티티(202)로부터 디스크에 기록하기 위한 편집 컨텐츠, 그 외의 컨텐츠 관련 정보를 수령한다.

키 관리 센터(201)가 발행하고, 정보 기록 매체 제조 엔티티(300)에 제공하는 키 관련 데이터에는, 예를 들면 이른바 계층형 트리 구조에 따른 정보 분배 방식에 의해, 사용자 디바이스(정보 처리 장치)의 라이센스의 유효성에 따른 키 취득을 가능하게 한 블록 키 정보(RKB: Renewal Key Block), 디스크 대응의 디스크 키(Kd), 그 외의 암호 키, 키 생성 정보가 포함된다. 이들 키 정보를 [CPKeys.DAT] 로 한다.

키 관리 센터(201)는, 키 정보 [CPKeys.DAT] 를 정보 기록 매체 제조 엔티티(300)에 제공할 때, 키 정보 [CPKeys.DAT] 의 정당성, 변조 검증을 행하기 위한 데이터로서 키 정보 [CPKeys.DAT] 에 따라 생성되는 검증값을 부가한다. 이 검증값은, 예를 들면 키 정보 [CPKeys.DAT] 의 구성 데이터에 대하여 일방향성 함수(해시 함수)를 적용하여 구한 메시지 다이제스트 코드(MDC) 등이 적용된다. 일방향성 함수로서는 예를 들면 SHA-1 등의 함수가 적용된다. 이 검증값을 [MDC(CPKeys.DAT]라고 한다.

즉, 키 관리 센터(201)는, 정보 기록 매체 제조 엔티티(300)에 대하여,

(a) 키 정보 [CPKeys.DAT]

(b) 검증값 [MDC(CPKeys.DAT]의 각 데이터를 제공한다.

정보 기록 매체 제조 엔티티(300)에서는, 키 관리 센터(201)로부터 수령한 키 정보 [CPKeys.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 새롭게 검증값: MDC'(CPKeys.DAT)를 산출하고, 산출한 값과, 키 관리 센터(201)로부터 수령한 검증값 [MDC(CPKeys.DAT]을 비교 대조하고, 일치한 경우에는, 키 관리 센터(201)로부터 수령한 키 정보 [CPKeys.DAT] 가 변조되어 있지 않은 정당한 것이라고 판정한다.

또, 컨텐츠 편집 엔티티(202)로부터 디스크에 기록하기 위한 편집 컨텐츠, 그 외의 컨텐츠 관련 정보가 정보 기록 매체 제조 엔티티(300)에 제공된다. 컨텐츠 편집 엔티티(202)로부터 정보 기록 매체 제조 엔티티(300)에 제공되는 데이터에는, 동화상 데이터 등의 컨텐츠, 컨텐츠의 재생 제어 정보 등이 포함된다. 이들 편집 컨텐츠, 그 외의 컨텐츠 관련 정보를 컨텐츠 정보 [Con.DAT] 로 한다.

컨텐츠 편집 엔티티(202)는, 컨텐츠 정보 [Con.DAT] 를 정보 기록 매체 제조 엔티티(300)에 제공할 때, 컨텐츠 정보 [Con.DAT] 의 변조 검증을 행하기 위한 데이터로서, 전술한 바와 마찬가지의 컨텐츠 정보 [Con.DAT] 에 대하여 일방향성 함수(해시 함수)를 적용하여 구한 검증값으로서의 메시지 다이제스트 코드(MDC)를 부가한다. 이 검증값을 [MDC(Con.DAT]로 한다.

즉, 컨텐츠 편집 엔티티(202)는, 정보 기록 매체 제조 엔티티(300)에 대하여,

(a) 컨텐츠 정보 [Con.DAT]

(b) 검증값 [MDC(Con.DAT]의 각 데이터를 제공한다.

정보 기록 매체 제조 엔티티(300)에서는, 컨텐츠 편집 엔티티(202)로부터 수령한 컨텐츠 정보 [Con.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 새롭게 검증값: MDC'(Con.DAT)를 산출하고, 산출한 값과 컨텐츠 편집 엔티티(202)로부터 수령한 검증값 [MDC(Con.DAT]를 비교 대조하고, 일치한 경우에는, 컨텐츠 편집 엔티티(202)로부터 수령한 키 정보 [CPKeys.DAT] 가 변조되어 있지 않은 정당한 것이라고 판정한다.

이와 같이, 정보 기록 매체 제조 엔티티(300)에서는, 키 관리 센터(201), 컨텐츠 편집 엔티티(202)로부터 수령한 각각의 정보의 정당성을 검증값에 따라 정당성을 판정한 후, 디스크(330)에 대한 데이터 기록 처리를 행한다.

그리고, 전술한 예에서는, 검증값으로서 메시지 다이제스트 코드만을 적용한 예를 나타냈으나, 또한 예를 들면 공개키 암호 방식에 따른 전자 서명(signature)을 설정하고, 서명 검증에 의한 데이터 검증을 행하는 구성으로 해도 된다.

전술한 검증 처리가 실행되고 정당성의 확인된 데이터가, 도 3에 나타낸 정보 기록 매체 제조 엔티티(300)의 기록 데이터 생성부(Formatter)(310)에 입력되고, 예를 들면 키 관리 센터(201)로부터 제공된 키를 적용한 컨텐츠 암호화, 데이터 포맷 처리 등의 처리가 실행되고, 정보 기록 매체(디스크)(330)에 데이터 기록이 실행된다. 그리고, 정보 기록 매체(디스크)(330)에는, 컨텐츠뿐아니라, 각종의 키 정보, 예를 들어 전술한 암호 키 블록(RKB) 등도 기록된다.

정보 기록 매체 제조 엔티티(300)에서는, 또한 데이터 기록필의 정보 기록 매체(330)에 정확한 데이터가 기록되어 있는지 여부지의 검증 처리를 실행한다. 이 검증 처리는, 기록필 디스크 모두, 또는 샘플링된 일부의 디스크에 대하여 실행된다.

데이터 검증 처리는, 정보 기록 매체 검증부(320)에 있어서 실행된다.

정보 기록 매체 검증부(320)는, 데이터 재생부(321), 검증용 재생 데이터 생성부(322), 데이터 비교 대조부(323), 결과 출력부(324)를 가진다.

데이터 재생부(Drive)(321)는, 데이터를 기록한 정보 기록 매체(330)로부터의 데이터 재생을 실행한다. 이 재생 데이터에는, 검증 대상이 되는 컨텐츠, 키 정보가 포함된다. 재생 데이터로서는 전술한 컨텐츠 정보 [Con.DAT] 에 대응하는 컨텐츠 정보와, 키 정보 [CPKeys.DAT] 에 대응하는 키 정보가 포함되게 된다.

여기서 재생 데이터를

(a) 재생 암호화 컨텐츠 정보 [R－Enc__Con.DAT]

(b) 재생 키 정보 [R－CPKeys.DAT]

의 2개의 데이터로 한다.

(R)은 재생 데이터인 것을 나타내고, (Enc)는 암호화 데이터인 것을 나타낸다. 기록 데이터 생성부(310)는, 컨텐츠를 암호화하여 정보 기록 매체(330)에 기록하고 있고, 데이터 재생부(Drive)(321)가 재생하는 데이터는 암호화 데이터로 된다. 그리고, 검증 대상 데이터는 이 외에도 다수 존재하는 경우가 있지만, 여기서는 간략화하여, 상기 2개의 데이터를 검증 대상 데이터로서 설명한다.

검증용 재생 데이터 생성부(322)는, 데이터 재생부(321)로부터,

(a) 재생 암호화 컨텐츠 정보 [R－Enc__Con.DAT]

(b) 재생 키 정보 [R－CPKeys.DAT]

를 입력하고, 검증용 데이터를 생성한다.

검증용 재생 데이터 생성부(322)는, 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성한다. 구체적으로는, (a) 재생 암호화 컨텐츠 정보 [R－Enc__Con.DAT] 에 대하여는, 재생 암호화 컨텐츠 정보 [R－Enc__Con.DAT] 에 따라 SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(R－Enc__Con.DAT)를 산출하고, 산출한 값을 컨텐츠 검증값으로서 데이터 비교 대조부(323)에 출력한다.

또한, (b) 재생 키 정보 [R－CPKeys.DAT] 에 대해서도, 재생 키 정보 [R－CPKeys.DAT] 에 따라 SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(R－CPKeys.DAT)를 산출하고, 산출한 값을 키 정보 검증값으로서 데이터 비교 대조부(323)에 출력한다.

데이터 비교 대조부(323)는, 검증용 재생 데이터 생성부(322)로부터 입력하는 각 검증값과, 기록 데이터 생성부(310)의 검증용 기록 데이터 생성부(311)로부터의 입력값과의 비교 대조 처리를 실행한다.

기록 데이터 생성부(310)의 검증용 기록 데이터 생성부(311)는, 정보 기록 매체(330)에 대한 기록 예정 정보, 즉,

(a) 기록 암호화 컨텐츠 정보 [Enc__Con.DAT]

(b) 기록 키 정보 [CPKeys.DAT] 에 따라 검증용 데이터를 생성한다.

검증용 기록 데이터 생성부(311)는, (a) 기록 암호화 컨텐츠 정보 [Enc__Con.DAT] 에 대하여는, 기록 암호화 컨텐츠 정보 [Enc__Con.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(Enc__Con.DAT)를 산출하고, 산출한 값을 컨텐츠 검증값으로서 데이터 비교 대조부(323)에 출력한다. 또한, (b) 기록 예정의 키 정보 [CPKeys.DAT] 에 대해서도, 기록 키 정보 [CPKeys.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(CPKeys.DAT)를 산출하고, 산출한 값을 키 정보 검증값으로서 데이터 비교 대조부(323)에 출력한다.

그리고, 전술한 바와 같이, 예를 들면 키 관리 센터(201)은, 정보 기록 매체 제조 엔티티(300)에 대하여,

(a) 키 정보 [CPKeys.DAT]

(b) 검증값 [MDC(CPKeys.DAT]

의 각 데이터를 제공하고 있고, 정보 기록 매체 제조 엔티티(300)가, 검증값 [MDC(CPKeys.DAT]데이터를 유지하고 있는 경우는, 검증용 기록 데이터 생성부(311)는, 검증용 데이터를 새롭게 생성하지 않고, 유지 데이터를 그대로 검증값으로서 데이터 비교 대조부(323)에 출력하는 구성으로 해도 된다.

데이터 비교 대조부(323)는, 검증용 재생 데이터 생성부(322)로부터 입력하는 각 검증값과, 기록 데이터 생성부(310)의 검증용 기록 데이터 생성부(311)로부터의 입력값과의 비교 대조 처리를 실행한다.

즉, 컨텐츠에 대하여는, 검증용 재생 데이터 생성부(322)로부터 입력하는 검증값: MDC(R－Enc__Con.DAT)와, 검증용 기록 데이터 생성부(311)로부터의 입력하는 검증값: MDC(Enc__Con.DAT)과의 비교 대조 처리를 실행하고, 일치하면, 기록 데이터와 재생 데이터가 일치하고, 정당한 데이터 기록이 이루어진 것으로 판정하고, 판정 결과를 결과 출력부(324)에 출력한다.

또한, 키 정보에 대하여는, 검증용 재생 데이터 생성부(322)로부터 입력하는 검증값: MDC(R－CPKeys.DAT)와 검증용 기록 데이터 생성부(311)로부터의 입력하는 검증값: MDC(CPKeys.DAT)과의 비교 대조 처리를 실행하고, 일치하면, 기록 데이터와 재생 데이터가 일치하고, 정당한 데이터 기록이 이루어진 것으로 판정하고, 판정 결과를 결과 출력부(324)에 출력한다.

본 구성에서는, 기록 데이터 생성부(310)의 검증용 기록 데이터 생성부(311)로부터 정보 기록 매체 검증부(320)로의 데이터 전송로 상을 전송하는 데이터가, 컨텐츠나, 키 정보 자체가 아니고, 이들 데이터에 따라 산출된 요약값, 즉 MDC(메시지 다이제스트 코드)이며, 이 MDC 데이터가 외부에 유출된 경우라도 컨텐츠 실체나 키 정보 실체가 유출되지 않고, 시큐리티를 유지해야 할 데이터가 유출될 우려는 없다. 또, 데이터 재생부(321)로부터 데이터 비교 대조부(323)에 이르는 경로도, 외부로부터 액세스할 수 없는 닫혀진 구성으로 함으로써 데이터 유출이 방지되어 시큐리티가 유지된 환경에서의 데이터 검증이 가능해진다.

그리고, 도면에 나타낸 구성에서는, 데이터 재생부(321), 검증용 재생 데이터 생성부(322), 데이터 비교 대조부(323), 결과 출력부(324)의 3요소를 모아서 1개의 정보 기록 매체 검증부(320)로 한 장치를 나타내고 있지만, 검증용 재생 데이터 생성부로부터의 출력 데이터는, MDC 등의 데이터이며 외부 유출에 문제가 없는 데이터이므로, 데이터 재생부(321)과 검증용 재생 데이터 생성부(322) 사이를 외부로부터의 액세스를 금지한 구성으로 하면 충분하고, 검증용 재생 데이터 생성부(322), 데이터 비교 대조부(323), 결과 출력부(324) 사이는, 검증용 기록 데이터 생성부(311)와 데이터 비교 대조부(323)와의 접속 구성과 마찬가지의 일반적인 데이터 전송 경로에 의해 접속하는 구성으로 해도 된다.

그리고, 정보 기록 매체 검증부(320)에 있어서의 데이터 재생부(321)이 데이터 재생 처리만아니라, 데이터 복호 처리를 실행 가능한 구성으로 하고, 데이터 재생부로부터의 복호 데이터에 따른 검사 데이터를 대조 처리 데이터로서 설정하는 구성으로 해도 된다. 도 4를 참조하여, 데이터 재생부가 복호 처리를 실행하는 기능을 가지는 경우의 처리에 대하여 설명한다.

도 4에 있어서, 정보 기록 매체 제조 엔티티의 기록 데이터 생성부(Formatter)(410)는, 예를 들면 키 관리 센터로부터 제공된 키를 적용한 컨텐츠 암호화, 데이터 포맷 처리 등의 처리를 실행하고, 정보 기록 매체(디스크)(430)에 대한 데이터 기록 처리를 실행한다. 정보 기록 매체(디스크)(430)에는, 컨텐츠 이외에, 각종의 키 정보, 예를 들어 전술한 암호 키 블록(RKB) 등의 기록이 행해진다.

데이터 검증 처리는, 정보 기록 매체 검증부(420)에 있어서 실행된다. 정보 기록 매체 검증부(420)는, 데이터 재생부(421), 검증용 재생 데이터 생성부(423), 데이터 비교 대조부(424), 결과 출력부(425)를 가진다.

데이터 재생부(Drive)(421)는, 재생 암호화 데이터의 복호 처리를 실행하는 데이터 복호부(422)를 내장하고 있다. 데이터 재생부(Drive)(421)는, 데이터를 기록한 정보 기록 매체(330)로부터의 데이터 재생을 실행하고, 또한 데이터 복호부(422)에 있어서 재생 암호화 데이터의 복호 처리를 실행한다.

복호 결과로서의 비암호화 데이터를 검증용 재생 데이터 생성부(423)에 출력한다.

그리고, 출력 데이터에는, 검증 대상이 되는 컨텐츠, 키 정보가 포함된다.

예를 들면 컨텐츠 정보와, 키 정보가 포함된다.

데이터 재생부(421)로부터의 출력 데이터를

(a) 재생 컨텐츠 정보 [R－Con.DAT]

(b) 재생 키 정보 [R－CPKeys.DAT]

의 2개의 데이터로 한다.

(R)은 재생 데이터인 것을 나타낸다.

검증용 재생 데이터 생성부(423)는, 데이터 재생부(421)로부터,

(a) 재생 컨텐츠 정보 [R－Con.DAT]

(b) 재생 키 정보 [R－CPKeys.DAT] 를 입력하고, 검증용 데이터를 생성한다.

검증용 재생 데이터 생성부(422)는, 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성한다. 구체적으로는, (a) 재생 컨텐츠 정보 [R__Con.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(R－Con.DAT)를 산출하고, 산출한 값을 컨텐츠 검증값으로서 데이터 비교 대조부(424)에 출력한다. 또한, (b) 재생 키 정보 [R－CPKeys.DAT] 에 대해서도, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(R－CPKeys.DAT)를 산출하고, 산출한 값을 키 정보 검증값으로서 데이터 비교 대조부(424)에 출력한다.

데이터 비교 대조부(424)는, 검증용 재생 데이터 생성부(423)로부터 입력하는 각 검증값과, 기록 데이터 생성부(410)의 검증용 기록 데이터 생성부(411)로부터의 입력값과의 비교 대조 처리를 실행한다.

기록 데이터 생성부(410)는, 정보 기록 매체(430)에 대하여는, 암호화 컨텐츠 [Enc__Con.DAT] 의 기록을 실행하지만, 검증용 기록 데이터 생성부(411)는, 암호화 이전의 비암호화 컨텐츠 정보에 따라 검증용 데이터를 생성한다.

검증용 기록 데이터 생성부(411)는, 컨텐츠 정보 [Con.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(Con.DAT)를 산출하고, 산출한 값을 컨텐츠 검증값으로서 데이터 비교 대조부(424)에 출력한다. 또한, 기록 예정의 키 정보 [CPKeys.DAT] 에 따라, SHA-1 등의 일방향성 함수를 적용하여 검증값: MDC(CPKeys.DAT)를 산출하고, 산출한 값을 키 정보 검증값으로서 데이터 비교 대조부(424)에 출력한다.

그리고, 전술한 바와 같이, 키 관리 센터나 컨텐츠 편집 엔티티는, 정보 기록 매체 제조 엔티티에 대하여 제공하는 데이터에 대한 검증값(MDC)을 데이터에 병행하여 제공하고 있고, 검증용 기록 데이터 생성부(311)는, 검증용 데이터를 새롭게 생성하지 않고, 유지 데이터를 그대로 검증값으로서 데이터 비교 대조부(424)에 출력하는 구성으로 해도 된다.

데이터 비교 대조부(424)는, 검증용 재생 데이터 생성부(423)로부터 입력하는 각 검증값과, 기록 데이터 생성부(410)의 검증용 기록 데이터 생성부(411)로부터의 입력값과의 비교 대조 처리를 실행한다.

즉, 컨텐츠에 대하여는, 검증용 재생 데이터 생성부(423)로부터 입력하는 검증값: MDC(R－Con.DAT)와, 검증용 기록 데이터 생성부(411)로부터의 입력하는 검증값: MDC(Con.DAT)와의 비교 대조 처리를 실행하고, 일치하면, 기록 데이터와 재생 데이터가 일치하고, 정당한 데이터 기록이 이루어진 것으로 판정하고, 판정 결과를 결과 출력부(425)에 출력한다.

또한, 키 정보에 대하여는, 검증용 재생 데이터 생성부(423)로부터 입력하는 검증값: MDC(R－CPKeys.DAT)와 검증용 기록 데이터 생성부(411)로부터의 입력하는 검증값: MDC(CPKeys.DAT)와의 비교 대조 처리를 실행하고, 일치하면, 기록 데이터와 재생 데이터가 일치하고, 정당한 데이터 기록이 이루어진 것으로 판정하고, 판정 결과를 결과 출력부(425)에 출력한다.

본 구성에 있어서도, 기록 데이터 생성부(410)의 검증용 기록 데이터 생성부(411)로부터 정보 기록 매체 검증부(420)로의 데이터 전송로 상을 전송하는 데이터가, 컨텐츠나, 키 정보 자체가 아니고, 이들 데이터에 따라 산출된 요약값, 즉 MDC(메시지 다이제스트 코드)이며, 이 MDC 데이터가 외부에 유출된 경우라도 컨텐츠 실체나 키 정보 실체가 유출되지 않고, 시큐리티를 유지해야 할 데이터가 유출될 우려는 없다. 또, 데이터 재생부(421)로부터 데이터 비교 대조부(424)에 이르는 경로도, 외부로부터 액세스할 수 없는 닫혀진 구성으로 함으로써 데이터 유출이 방지되어 시큐리티의 유지된 환경에서의 데이터 검증이 가능해진다.

그리고, 본 예에 있어서도 도면에 나타낸 구성에서는, 데이터 재생부(421), 검증용 재생 데이터 생성부(423), 데이터 비교 대조부(424), 결과 출력부(425)의 요소를 모아서 1개의 정보 기록 매체 검증부(420)로 한 장치를 나타내고 있지만, 검증용 재생 데이터 생성부(423)로부터의 출력 데이터는, MDC 등의 데이터여 외부 유출에 문제가 없는 데이터이므로, 데이터 재생부(421)와 검증용 재생 데이터 생성부(423) 사이를 외부로부터의 액세스를 금지한 구성으로 하면 충분하고, 검증용 재생 데이터 생성부(423), 데이터 비교 대조부(424), 결과 출력부(425) 간은, 검증용 기록 데이터 생성부(411)와 데이터 비교 대조부(424)와의 접속 구성과 마찬가지의 일반적인 데이터 전송 경로에 의해 접속하는 구성으로 해도 된다.

이상, 특정한 실시예를 참조하면서, 본 발명에 대하여 상세히 설명하였다. 그러나, 본 발명의 요지를 벗어나지 않는 범위에서 당업자가 상기 실시예의 수정이나 변경을 해낼 수 있는 것은 자명하다. 즉, 예시라는 형태로 본 발명을 개시한 것이며, 한정적으로 해석해서는 안된다. 본 발명의 요지를 판단하기 위해서는, 서두에 기재한 특허 청구의 범위의 란을 참작해야 한다.

그리고, 명세서 중에 있어서 설명한 일련의 처리는 하드웨어, 또는 소프트 웨어, 또는 양자의 복합 구성에 의해 실행할 수 있다.

소프트 웨어에 의한 처리를 실행하는 경우는, 처리 시켄스를 기록한 프로그램을, 전용의 하드웨어에 내장된 컴퓨터 내의 메모리에 인스톨하여 실행시키든가, 또는 각종 처리가 실행 가능한 범용 컴퓨터에 프로그램을 인스톨하여 실행시키는 것이 가능하다.

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 리무버블 기록 매체에, 일시 목표 또는 영속적으로 저장(기록)해 둘 수가 있다. 이와 같은 리무버블 기록 매체는, 이른바 팩키지 소프트웨어로서 제공할 수 있다.

그리고, 프로그램은, 전술한 바와 같은 리무버블 기록 매체로부터 컴퓨터에 인스톨하는 것 외에, 다운로드 사이트로부터, 컴퓨터에 무선 전송한, LAN(Local Area Network), 인터넷이라는 네트워크를 통하여, 컴퓨터에 유선으로 전송하고, 컴퓨터에서는, 그와 같이 하여 전송되어 오는 프로그램을 수신하고, 내장하는 하드 디스크 등의 기록 매체에 인스톨할 수 있다.

그리고, 명세서에 기재된 각종의 처리는, 기재에 따라 시계열로 실행되는 것만아니라, 처리를 실행하는 장치의 처리 능력 또는 필요에 따라 병렬적으로 또는 개별적으로 실행되어도 된다.

또, 본 명세서에 있어서 시스템이란, 복수개의 장치의 논리적 집합 구성이며, 각 구성의 장치가 동일 캐비닛 내에 있는 것에는 한정되지 않는다.

발명의 효과

이상, 설명한 바와 같이, 본 발명의 구성에 의하면, 정보 기록 매체로부터의 데이터 재생을 실행하고 재생 데이터에 따른 연산 처리를 실행하여 생성한 검증용 재생 데이터를 비교 대조부에 출력하고, 데이터 비교 대조부에 있어서, 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성으로 하였으므로, 검증 처리 대상 데이터로서 비교 대조부에 출력되는 데이터를 컨텐츠나 키 정보 등의 실데이터와 다른 연산 결과 데이터로 하는 것이 가능해져, 검증용 데이터가 외부 유출된 경우라도 컨텐츠나 키 정보 등의 실데이터의 유출을 방지할 수 있다.

본 발명의 구성에 의하면, 비교 대조부에 출력되는 검증용 데이터는, 컨텐츠나, 키 정보 자체가 아니고, 이들 데이터에 따른 연산 결과로서 산출된 요약값, 즉 MDC(메시지 다이제스트 코드)이며, 이 MDC 데이터가 외부에 유출된 경우라도 컨텐츠 실체나 키 정보 실체가 유출되지 않아, 시큐리티를 유지해야 할 데이터가 유출될 우려는 없고, 시큐리티가 유지된 환경에서의 데이터 검증이 가능해진다.

(57) 청구의 범위

청구항 1.

정보 기록 매체의 기록 데이터 검증 처리를 실행하는 정보 기록 매체 검증 장치로서, 상기 정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생부와,

상기 데이터 재생부의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성부와,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조부

를 구비한 정보 기록 매체 검증 장치.

청구항 2.

제1항에 있어서,

상기 검증용 재생 데이터 생성부는, 상기 정보 기록 매체로부터의 재생 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며,

상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 상기 정보 기록 매체에 대한 기록 예정 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 하는 정보 기록 매체 검증 장치.

청구항 3.

제1항에 있어서,

상기 데이터 재생부는, 정보 기록 매체에 저장된 암호화 데이터를 상기 검증용 재생 데이터 생성부에 출력하는 구성이며,

상기 검증용 재생 데이터 생성부는, 상기 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며,

상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 상기 정보 기록 매체에 대한 기록 예정 데이터에 포함되는 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 하는 정보 기록 매체 검증 장치.

청구항 4.

제1항에 있어서,

상기 데이터 재생부는, 정보 기록 매체로부터의 재생 데이터에 포함되는 암호화 데이터의 복호 처리를 실행하는 데이터 복호부를 추가로 구비하고,

상기 데이터 재생부는, 상기 데이터 복호부에 있어서 복호된 비암호화 데이터를 상기 검증용 재생 데이터 생성부에 출력하는 구성이며,

상기 검증용 재생 데이터 생성부는, 상기 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 상기 데이터 비교 대조부에 출력하는 구성이며,

상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터의 원래의 데이터로서의 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 하는 정보 기록 매체 검증 장치.

청구항 5.

제1항에 있어서,

상기 검증용 재생 데이터 생성부는, 데이터 재생부의 재생 데이터에 따른 메시지 다이제스트 코드(MDC)의 산출 처리를 실행하는 구성이며,

상기 데이터 비교 대조부는, 상기 검증용 재생 데이터 생성부가 생성한 메시지 다이제스트 코드(MDC)와 정보 기록 매체에 대한 기록 예정 데이터에 따른 메시지 다이제스트 코드(MDC)와의 비교 대조 처리를 실행하는 구성인 것을 특징으로 하는 정보 기록 매체 검증 장치.

청구항 6.

제1항에 있어서,

상기 데이터 재생부는, 상기 정보 기록 매체로부터 암호화 컨텐츠 및 키 정보를 포함하는 데이터의 재생을 실행하고,

상기 데이터 비교 대조부는, 암호화 컨텐츠 또는 복호 컨텐츠에 따른 연산 결과로서의 검증용 데이터와, 키 정보에 따른 연산 결과로서의 검증용 데이터에 따라 컨텐츠 및 키 정보의 검증 처리를 실행하는 구성인 것을 특징으로 하는 정보 기록 매체 검증 장치.

청구항 7.

정보 기록 매체의 기록 데이터 검증 처리를 실행하는 정보 기록 매체 검증 방법으로서,

상기 정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생 스텝과,

상기 데이터 재생 스텝에 있어서의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성 스텝과,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조 스텝

을 포함하는 정보 기록 매체 검증 방법.

청구항 8.

제7항에 있어서,

상기 검증용 재생 데이터 생성 스텝은, 정보 기록 매체로부터의 재생 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며,

상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 하는 정보 기록 매체 검증 방법.

청구항 9.

제7항에 있어서,

상기 데이터 재생 스텝은, 정보 기록 매체에 저장된 암호화 데이터를 재생, 출력하는 스텝이며,

상기 검증용 재생 데이터 생성 스텝은, 상기 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며,

상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 포함되는 암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 하는 정보 기록 매체 검증 방법.

청구항 10.

제7항에 있어서,

상기 정보 기록 매체 검증 방법은, 정보 기록 매체로부터의 재생 데이터에 포함되는 암호화 데이터의 복호 처리를 실행하고, 비암호화 데이터를 생성하는 데이터 복호 스텝을 추가로 포함하고,

상기 검증용 재생 데이터 생성 스텝은, 상기 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리를 실행하고, 상기 연산 결과를 검증용 재생 데이터로서 출력하는 스텝이며,

상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터의 원래의 데이터로서의 비암호화 데이터에 대한 일방향성 함수를 적용한 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 것을 특징으로 하는 정보 기록 매체 검증 방법.

청구항 11.

제7항에 있어서,

상기 검증용 재생 데이터 생성 스텝은, 데이터 재생부의 재생 데이터에 따른 메시지 다이제스트 코드(MDC)의 산출 처리를 실행하는 스텝이며,

상기 데이터 비교 대조 스텝은, 상기 검증용 재생 데이터 생성 스텝에 있어서 생성한 메시지 다이제스트 코드(MDC)와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 메시지 다이제스트 코드(MDC)와의 비교 대조 처리를 실행하는 스텝인 것을 특징으로 하는 정보 기록 매체 검증 방법.

청구항 12.

제7항에 있어서,

상기 데이터 재생 스텝은, 정보 기록 매체로부터 암호화 컨텐츠 및 키 정보를 포함하는 데이터의 재생을 실행하고,

상기 데이터 비교 대조 스텝은, 암호화 컨텐츠 또는 복호 컨텐츠에 따른 연산 결과로서의 검증용 데이터와, 키 정보에 따른 연산 결과로서의 검증용 데이터에 따라 컨텐츠 및 키 정보의 검증 처리를 실행하는 것을 특징으로 하는 정보 기록 매체 검증 방법.

청구항 13.

정보 기록 매체의 기록 데이터 검증 처리를 실행하는 컴퓨터·프로그램으로서,

정보 기록 매체로부터의 데이터 재생을 실행하는 데이터 재생 스텝과,

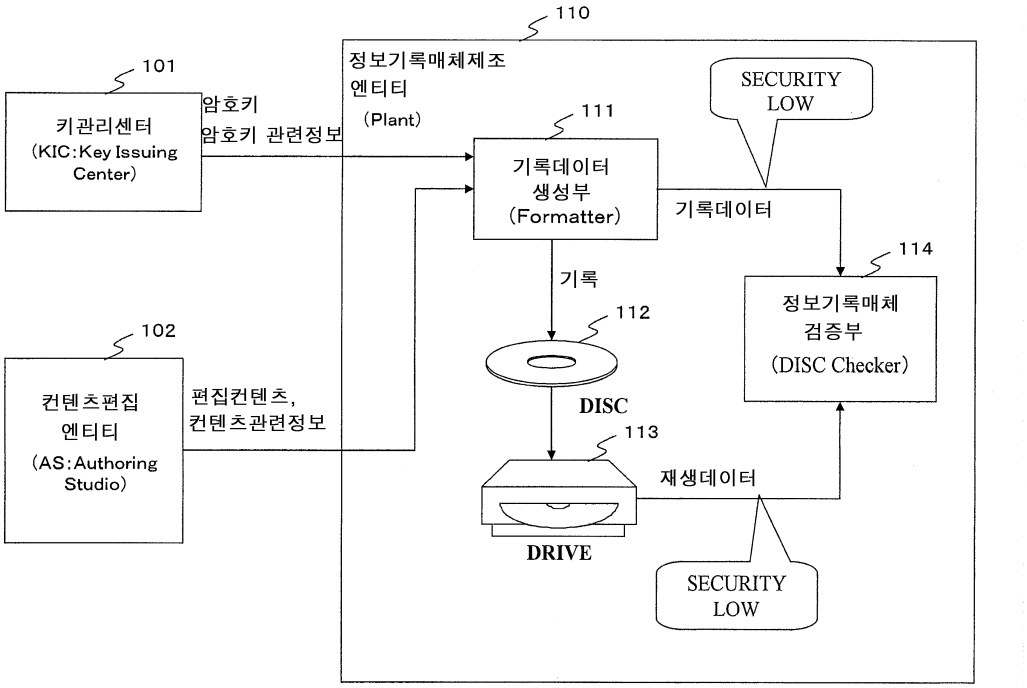
상기 데이터 재생 스텝에 있어서의 재생 데이터에 따른 연산 처리를 실행하고, 검증용 재생 데이터를 생성하는 검증용 재생 데이터 생성 스텝과,

상기 검증용 재생 데이터와, 정보 기록 매체에 대한 기록 예정 데이터에 따른 연산 처리 결과인 검증용 기록 데이터와의 비교 대조 처리를 실행하는 데이터 비교 대조 스텝

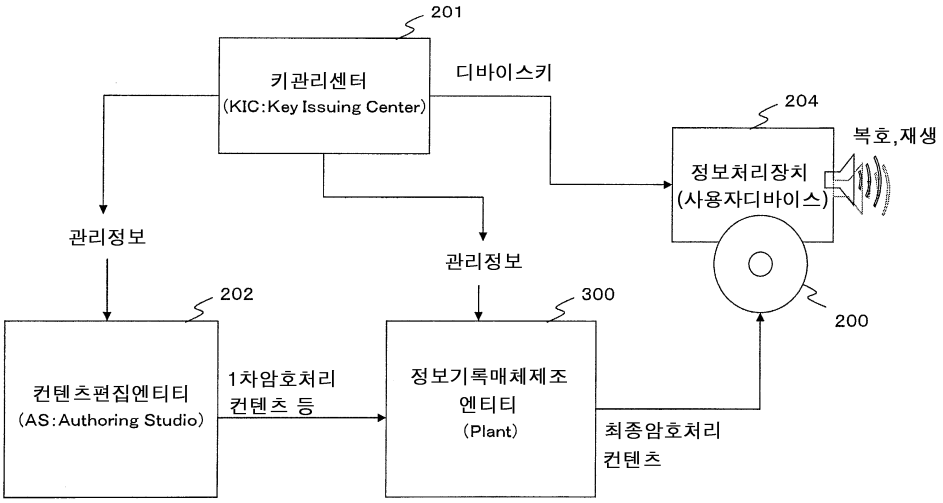
을 포함하는 컴퓨터·프로그램.

도면

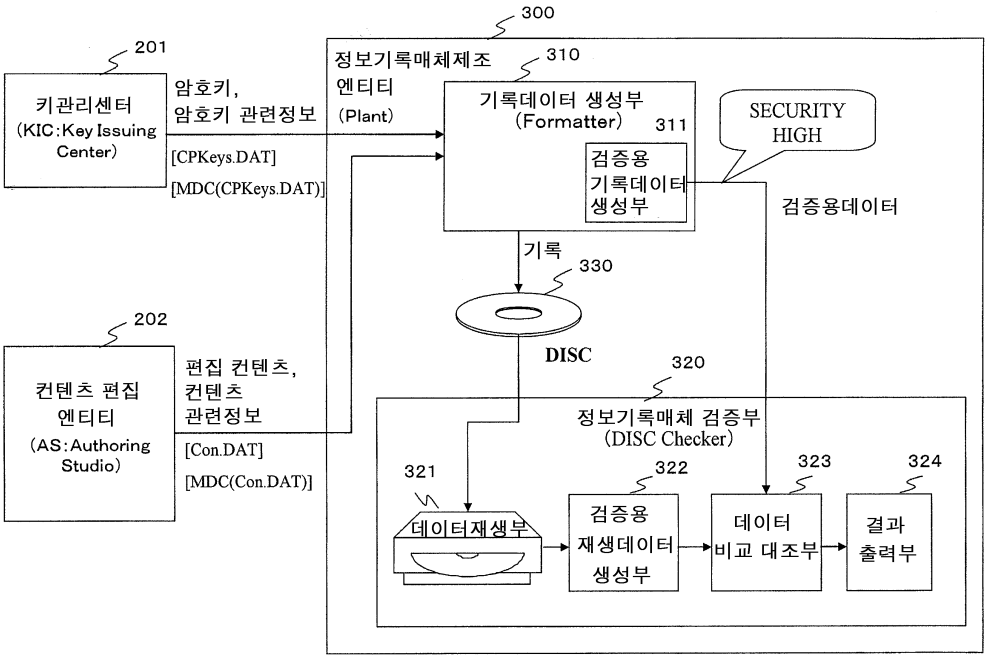
도면1



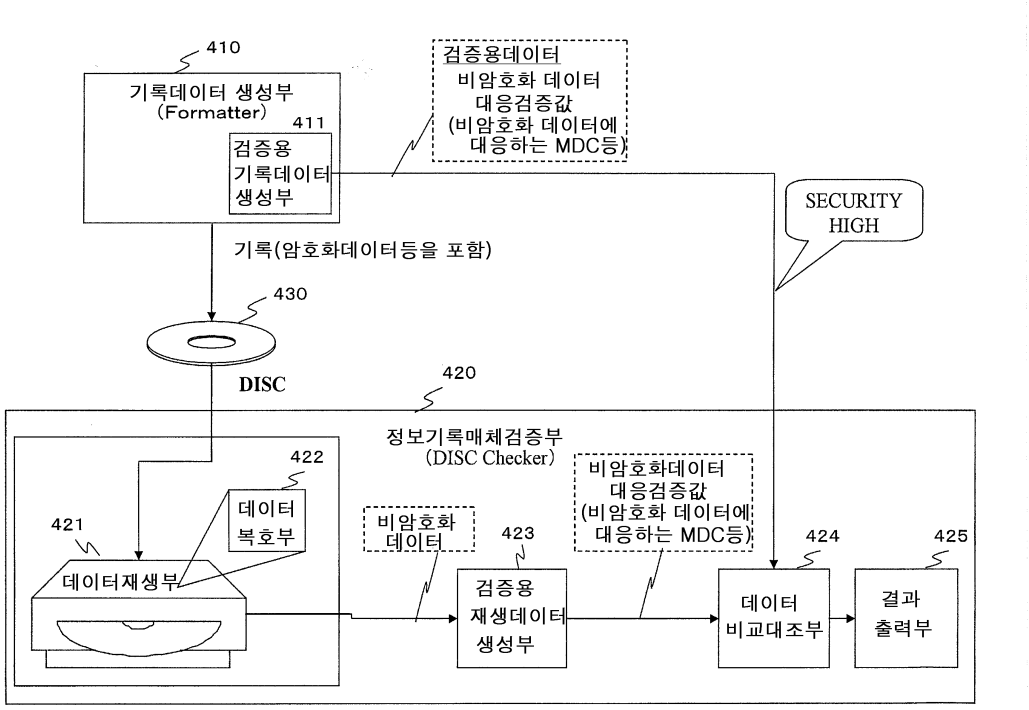
도면2


201
키관리센터
(KIC:Key Issuing Center)
디바이스키
204
복호,재생
정보처리장치
(사용자디바이스)
관리정보
관리정보
202
300
200
컨텐츠편집엔티티
(AS:Authoring Studio)
1차암호처리
컨텐츠 등
정보기록매체제조
엔티티
(Plant)
최종암호처리
컨텐츠

도면3


300
201
정보기록매체제조
엔티티
(Plant)
310
키관리센터
(KIC:Key Issuing
Center)
암호키,
암호키 관련정보
[CPKeys.DAT]
[MDC(CPKeys.DAT)]
기록데이터 생성부
(Formatter)
311
SECURITY
HIGH
검증용
기록데이터
생성부
검증용데이터
기록
330
DISC
202
320
컨텐츠 편집
엔티티
(AS:Authoring
Studio)
편집 컨텐츠,
컨텐츠
관련정보
[Con.DAT]
[MDC(Con.DAT)]
정보기록매체 검증부
(DISC Checker)
321
322
323
324
데이터재생부
검증용
재생데이터
생성부
데이터
비교 대조부
결과
출력부

도면4


410
기록데이터 생성부
(Formatter)
411
검증용
기록데이터
생성부
검증용데이터
비암호화 데이터
대응검증값
(비암호화 데이터에
대응하는 MDC등)
SECURITY
HIGH
기록(암호화데이터등을 포함)
430
DISC
420
정보기록매체검증부
(DISC Checker)
422
데이터
복호부
421
데이터재생부
비암호화
데이터
423
검증용
재생데이터
생성부
비암호화데이터
대응검증값
(비암호화 데이터에
대응하는 MDC등)
424
데이터
비교대조부
425
결과
출력부