(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06K 17/00

(11) 공개번호 10-2004-0092450
(43) 공개일자 2004년11월03일

(21) 출원번호 10-2004-0027667
(22) 출원일자 2004년04월22일

(30) 우선권주장 JP-P-2003-00117822 2003년04월23일 일본(JP)

(71) 출원인 가부시끼가이샤 르네사스 테크놀로지
일본 100-6334 도꾜도 지요다구 마루노우찌 2-쪼메 4-1

(72) 발명자 이마이츠토무
일본국도쿄도치요타쿠마루노우치2쵸메4-1가부시끼가이샤르네사스테크놀로지나이

카네히라아키라
일본국도쿄도치요타쿠마루노우치2쵸메4-1가부시끼가이샤르네사스테크놀로지나이

카타야마쿠니히로
일본국도쿄도치요타쿠마루노우치2쵸메4-1가부시끼가이샤르네사스테크놀로지나이

(74) 대리인 이종일

심사청구 : 없음

(54) 불휘발성 기억장치 및 데이터 처리장치

요약

재생장치나 단말장치내부의 시계의 조작에 의한 기한첨부 데이터의 부정 억세스를 효과적으로 억제한다.

불휘발성 기억장치는, 제어 회로(16)와 불휘발성 기억회로(14)를 갖는다. 불휘발성 기억회로는 이용정보에 대한 억세스 제한을 행하는 제한정보의 저장 영역을 갖는다. 제한정보에는 억세스 기한정보와 억세스 시간정보를 포함한다. 제어 회로는 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 이용정보의 억세스 가부를 판정하고, 시각정보에 근거해서 억세스 시간정보를 갱신하는 억세스 판정 동작을 행한다. 억세스 가부의 판정에 있어서 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 시각정보가 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 한다. 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행한다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명을 적용한 컨텐츠데이터 배신시스템의 블럭도이다.

도 2는 본 발명을 적용한 컨텐츠데이터 배신시스템에 다른 데이터 단말장치가 접속되어 있는 예를 나타내는 설명도이다.

도 3은 단말 일시데이터에 근거해서 갱신되는 카드 일시데이터에 의한 이용 제한의 개요를 예시하는 설명도이다.

도 4는 도 1에 있어서의 이용기한 판정부와 단말내부시계의 구체예를 나타내는 블럭도이다.

도 5는 일시데이터의 포맷을 예시하는 설명도이다.

도 6은 도 2의 메모리카드에 내장된 이용기한 판정부의 구체예를 나타내는 블럭도이다.

도 7은 재생 라이센스의 포맷을 예시하는 설명도이다.

도 8은 시큐어라이센스의 포맷을 예시하는 설명도이다.

도 9는 라이센스의 기입시의 인증(기입 인증)처리 순서를 예시하는 흐름도이다.

도 10은 라이센스의 독출시의 인증(독출 인증)처리 순서를 예시하는 흐름도 이다.

도 11은 이용기한부 컨텐츠의 재생 처리의 일례를 나타내는 흐름도이다.

도 12는 도 11의 이용기한판정처리R21의 상세를 예시하는 흐름도이다.

도 13은 도 11의 카드 일시데이터 갱신 처리R22의 상세를 예시하는 흐름도이다.

도 14는 기한첨부 데이터의 재생 단말장치를 예시하는 블럭도이다.

도 15는 다운로드 단말장치를 예시하는 블럭도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 기억매체에 저장된 동화나 음악등의 컨텐츠데이터등에 대한 재생 기한관리에 관한 것이며, 재생 기한관리의 제어를 적용한 불휘발성 기억장치, 재생 단말장치 및 반포 단말장치에 관계된다.

메모리카드등의 기억매체에 기억된 화상 데이터 및 음악 데이터렌탈될 경우, 미리 설정된 재생 기한내이면 유저는 재생장치를 이용해서 화상 및 음악을 재생할 수 있다. 유저의 재생장치에 있어서 검지된 시각과, 기억매체에 디지털 데이터를 기억할 때에 기입된 재생 기한정보에 근거해서 재생이 관리된다. 유저의 재생장치에 의해 검지되는 현재 시각이 고쳐지면 재생 기한을 경과하고 있는데도 불구하고, 컨텐츠를 재생할 수 있다.

재생장치의 시간 개선에 대한 대책으로서, 예를 들면 일본국 특개2002 —259917호 공보(단락99, 도7)에 기재된 기술이 있다. 즉, 데이터기입장치는 데이터 독취 장치에 의해 데이터를 출력가능한 기한을 설정하고, 기억매체에 데이터와 기한과 기억매체에 관한 데이터 및 기한의 기입일시를 기입한다. 데이터 독취 장치는 기억매체로부터 독취한 기한과 기입일시와 검지한 현재일시에 근거하여 기억매체에 기입된 데이터의 출력의 가부를 판단하고, 데이터의 출력이 가능하면, 기억매체로부터 데이터를 독취해서 출력한다. 데이터를 출력할 수 있는 기한이 경과했을 때에, 데이터 독취 장치의 검지수단에 의해 검지되는 현재일시를 기입일시 이전에 변경하고, 부정으로 데이터의 출력을 행하려고 할 경우를 상정한다. 이 경우, 부정으로 변경된 현재일시가 데이터가 기입된 일시 이전이기 때문에, 판단 수단은 데이터의 출력이 가능하다고 판단하지 않는다. 또한 상기 기입일시는 재생 처리의 종료시에 현재 시각으로 갱신하도록되어 있다.

발명이 이루고자 하는 기술적 과제

상기 일본국 특개2002—259917호 공보(단락99, 도7)의 기술에 따르면 메모리카드 등의 기억매체에 일시데이터를 기록함으로써 단말내부의 시계가 조작되어도 기한첨부 컨텐츠의 부정한 재생을 억제할 수 있지만 충분하지 않은 것이 본 발명자에 의해 발견되었다. 제1로, 기억매체의 현재 시각을 재생종료 시점에서 갱신하는 것 만으로는 불충분할 경우가 상정된다. 예를 들면 컨텐츠 재생종료 직전에 전원이 차단되었을 경우에는 기억매체의 현재 시각이 전혀 갱신되지 않을 우려가 있다. 제2로, 기한첨부 컨텐츠의 부정재생억제기능은 재생장치측이 갖추기 때문에, 재생장치를 바꾸면 여전히 부정 억세스가 가능하게 된다.

본 발명의 목적은, 재생장치나 단말장치내부의 시계의 조작에 의한 기한첨부 데이터의 부정 억세스를 효과적으로 억제하는 기술을 제공하는 것에 있다.

본 발명의 상기 및 그 밖의 목적과 신규인 특징은 본 명세서의 기술 및 첨부 도면으로부터 밝혀질 것이다.

본원에 있어서 개시되는 발명 중 대표적인 것의 개요를 간단히 설명하면 하기와 같다.

《불휘발성 기억장치》

본 발명의 제1의 관점은, 기한첨부 데이터의 부정 억세스 억지 기능을 기억매체로서의 불휘발성 기억장치가 구비하는 관점이다.

〔1〕 본 발명에 관련되는 불휘발성 기억장치는, 제어 회로와 불휘발성 기억회로를 갖는다. 상기 불휘발성 기억회로는 이용정보에 대한 억세스 제한을 행하는 제한정보의 저장 영역을 갖는다. 상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함된다. 상기 제어 회로는, 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행한다. 상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정한다. 상기 제어 회로에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행한다.

상기수단에 의해, 메모리카드 등의 불휘발성 기억장치에 억세스 시간정보와 같은 일시데이터를 갱신해서 기록하기 때문에 갱신마다 억세스 시간정보에 의해 나타나는 시간과 기한정보에 의해 나타나는 시간차이는 좁아져 최후에 억세스 시간정보에 의해 나타나는 시간이 기한정보에 의해 나타나는 시간을 초월한다. 일단 넘으면 이용 불가로 된다. 이미 유저는 단말내의 시계를 이용 제한보다 이전의 일시로 돌려도 재생은 불가하게 된다. 이것에 의해, 재생장치등의 단말내부의 시계가 조작되어도 기한첨부 이용정보의 부정한 재생을 억제하는 것이 가능하게 된다. 억세스 시간정보의 갱신은 억세스 종료 시점뿐만 아니라 억세스 시작시점에서도 행하여지기 때문에, 이용정보의 재생종료 직전에 전원이 차단되어도 적어도 1회의 억세스 시간정보의 갱신은 보증된다. 기한첨부 이용정보의 부정재생억제기능은 불휘발성 기억장치가 구비하기 때문에, 재생장치를 바꾸어도 여전히 부정 억세스 억지 기능을 동작시키는 것은 용이하다.

〔2〕 억세스 판정 동작은 적어도 불휘발성 기억장치로 동작전원을 투입할 때와 동작전원을 차단할 때에 행하도록 해도 좋다.

〔3〕 또한 억세스 판정 동작을 다른 타이밍으로 행해도 좋다. 즉, 이용정보를 복수로 분할해서 억세스를 행할 때 억세스 개시시의 상기 억세스 판정 동작에 있어서 억세스 가능이라고 판정된 후는 분할된 상기 이용정보의 억세스마다 또는 소정의 복수 억세스마다 상기 억세스 판정 동작을 행해도 좋다.

〔4〕 분할된 상기 이용정보의 억세스 단위는 예를 들면 섹터다.

〔5〕 상기 분할된 이용정보의 억세스에 대한 억세스 판정 동작에 있어서, 제2회째이후의 억세스 판정 동작에서는 시각정보가 상기 억세스 기한정보에 의해 나타나는 억세스 기한보다 뒤에 있어도 억세스 가능이라고 판정하도록 해서 좋다. 억세스 판정 동작을 몇회나 행할 때 이용정보의 재생 도중등에서 기한이 도래해서 재생이 중단되는 불편함을 간단히 해소할 수 있다.

〔6〕 상기 불휘발성 기억장치는, 예를 들면 상기 시각정보를 출력가능한 외부장치에 접속되어 사용되는 것이며, 상기 외부장치에 상기 분할된 이용정보를 출력가능하다.

〔7〕 상기 불휘발성 기억회로는 예를 들면 불휘발성 반도체 메모리이며, 외부장치에 접속되는 인터페이스단자를 갖는 소정의 메모리카드 케이싱에 내장되어서 이루어진다.

〔8〕 상기 제한정보는 상기 제어 회로에 의해 암호화되어서 상기 불휘발성 기억회로에 저장된다. 억세스 제한이 행하여지지 않고 있는 영역에 저장되는 경우에 간편하고 적합하다.

〔9〕 상기 제한정보의 암호화에 사용하는 암호열쇠는, 예를 들면 불휘발성 기억장치고유의 속성정보로 하면 좋다.

〔10〕 저작권보호의 관점이 고려될 경우에는, 상기 제어 회로는 상기 이용정보를 복호하기 위한 컨텐츠 열쇠를 포함하는 이용정보 라이센스를 수령하기 때문에 증명정보를 외부에 출력가능한 것이 좋다.

〔11〕 그 증명정보에 대하여 외부로부터 인증되면, 상기 제어 회로는 상기 이용정보 라이센스를 외부로부터 수령할 수 있고, 수령한 라이센스를 상기 불휘발 성 기억회로에 저장하는 것이 좋다.

〔12〕 상기 제어 회로는 상기 컨텐츠 열쇠와 함께 입력되는 시간정보를 상기 억세스 시간정보의 초기값으로서 상기 불휘발성 기억회로에 저장하는 것이 바람직하다. 그러한 시간정보에 대해서는 개선되어 있을 가능성은 대단히 낮다.

〔13〕 시큐어 영역과 같은 억세스 제한 영역에 대해서 고려한다. 상기 불휘발성 기억회로는 억세스 제한 영역과 억세스 비제한 영역을 가질 때, 상기 제한정보는 억세스 제한 영역에 저장하고, 상기 이용정보는 억세스 비제한 영역에 저장하면 좋다.

〔14〕 억세스 제한 영역에 대한 기입 인증에 대해서 고려한다. 상기 제어 회로는 외부로부터의 인증을 받아서 상기 억세스 제한 영역에 대한 기입이 가능해지면 좋다. 억세스 제한 영역에 대한 부정한 기입이 저지된다.

〔15〕 상기 억세스 제한 영역은 예를 들면 상기 이용정보 라이센스 등의 저장 영역이 된다.

〔16〕 억세스 제한 영역에 대한 독출 인증에 대해서 고려한다. 상기 제어 회로는 외부로부터 주어지는 증명정보에 대한 인증을 행해서 상기 억세스 제한 영역에 대한 독출을 가능하게 한다. 억세스 제한 영역에 대한 부정한 독출을 저지할 수 있다.

《재생 단말장치》

본 발명의 제2의 관점은 기한첨부 데이터의 부정 억세스 억지 기능을 재생 단말등의 데이터 처리장치를 구비하는 관점이다.

〔17〕 본 발명에 관한 데이터 처리장치는 재생부와 이용 제한부를 가지고, 이용정보에 대한 억세스 제한을 행하는 제한정보를 고쳐쓰기 가능하게 저장하는 기억매체를 억세스해서 상기 이용정보를 재생가능하다. 상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함된다. 상기 이용 제한부는, 데이터 처리장치에서 생성되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 기억매체상의 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행한다. 상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정한다. 상기 이용 제한부에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행한다.

상기수단에 의해, 메모리카드 등의 기억매체에 억세스 시간정보와 같은 일시데이터를 갱신해서 기록하기 때문에, 갱신마다 억세스 시간정보에 의해 나타나는 시간과 기한정보에 의해 나타나는 시간차이는 좁아지고, 최후에 억세스 시간정보에 의해 나타나는 시간이 기한정보에 의해 나타나는 시간을 초과한다. 일단 넘으면 이용 불가하게 된다. 이미 유저는 단말내의 시계를 이용 제한보다 이전의 일시에 돌려줘도 재생은 불가라고 한다. 이것에 의해, 재생장치등의 단말내부의 시계가 조작되어도 기한첨부 컨텐츠의 부정한 재생을 억제하는 것이 가능하게 된다. 억세스 시간정보의 갱신은 억세스 종료 시점뿐만아니라 억세스 시작시점에서도 행하여지기 때문에, 이용정보의 재생종료 직전에 전원이 차단되어도 적어도 1회의 억세스 시간정보의 갱신은 보증된다.

〔18〕 억세스 판정 동작은, 적어도 재생부로 기억매체를 장착할 때와 재생부로부터 기억매체를 이탈할 때에 행하도록 해도 좋다.

〔19〕 또 다른 대요로서 억세스 판정동작은 재생부에 기억매체가 장착된 상태로 동작전원이 투입될 때와, 재생부에 기억매체가 장착된 상태로 동작전원이 차단될 때에 행하도록 해도 좋다.

〔20〕 상기 이용 제한부는 기억매체고유의 속성정보를 암호열쇠로서 암호화를 행해서 억세스 시간정보의 갱신을 행한다. 억세스 제한이 행하여지지 않고 있는 영역에 저장되는 경우에 간편하고 적합하다.

〔21〕 상기 기억매체는 예를 들면 고쳐쓰기 가능한 불휘발성 기억장치다.

〔22〕 시큐어 영역과 같은 억세스 제한 영역에 대해서 고려한다. 상기 불휘발성 기억장치는 억세스 제한 영역과 억세스 비제한 영역을 가질 때, 상기 이용 제한 판정부는 억세스 제한 영역에 대하여 제한정보의 억세스를 행하고, 상기 재생부는 억세스 비제한 영역에 대하여 이용정보의 억세스를 행한다.

〔23〕 억세스 제한 영역에 대한 기입 인증에 대해서 고려한다. 상기 이용 제한부는 불휘발성 기억장치로부터 출력되는 증명정보에 대하여 인증을 행한 후에 억세스 제한 영역에 기입이 가능하게 되는 것이 좋다. 억세스 제한 영역에 대한 부정한 기입이 저지된다.

〔24〕 상기 억세스 제한 영역은 상기 이용정보를 복호하기 위한 이용정보 라 이센스의 저장 영역으로 된다.

〔25〕 억세스 제한 영역에 대한 독출 인증에 대해서 고려한다. 상기 이용 제한부는 불휘발성 기억장치에 증명정보를 주어서 인증을 받은 후에 상기 억세스 제한영역에 대한 독출이 가능하게 되는 것이 좋다. 억세스 제한 영역에 대한 부정독출을 저지할 수 있다.

〔26〕 호스트 인터페이스제어부를 가질 때, 저작권보호의 관점이 고려될 경우에는, 해당 호스트 인터페이스제어부는, 상기 이용정보를 복호하기 위한 컨텐츠 열쇠를 포함하는 이용정보 라이센스를 수령하기 위해서 상기 기억매체가 보유하는 증명정보를 호스트장치를 향해서 출력가능한 것이 바람직하다.

〔27〕 그 증명정보에 대하여 호스트 송치로 인증되면, 상기 호스트 인터페이스제어 회로는 상기 이용정보 라이센스를 호스트장치로부터 수령해서 상기 기억매체에 저장가능한 것이 바람직하다.

〔28〕 상기 호스트 인터페이스제어 회로는, 상기 컨텐츠 열쇠와 함께 입력되는 시간정보를 상기제억세스 시간정보의 초기값으로서 상기 기억매체에 저장가능한 것이 바람직하다. 그러한 시간정보에 대해서는 개선되어 있을 가능성은 대단히 낮다.

《다운로드 단말장치》

본 발명의 제3의 관점은, 기한첨부 데이터의 부정 억세스 억지 기능을 다운로드 단말장치등의 데이터 처리장치가 지원하는 관점이다.

〔29〕 본 발명에 관한 데이터 처리장치는 호스트 인터페이스부, 매체 인터페 이스부 및 데이터 처리부를 가지고 매체 인터페이스부에 장착된 기억매체에 소정의 정보를 저장한다.상기 데이터처리부는, 복호열쇠의 수령 요구와 함께 기억매체가 보유하는 증명정보를 호스트 인터페이스부로부터 외부에 출력하고, 이것에 응답해서 호스트 인터페이스부로 돌아가는 정보를 수령하고, 이것에 기초해서 매체 인터페이스부에서 상기 기억매체로 상기 소정의 정보로서, 이용정보를 복호하기 위한 복호열쇠와 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장한다. 상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함된다. 상기 억세스 시간정보의 초기값은 상기 수령한 정보에 포함되는 시간정보이다. 상기 증명정보는 특정한 기억매체인 것을 나타내는 정보다. 상기 특정의 기억매체는 제어 회로와 불휘발성 기억회로를 가지고, 상기 불휘발성 기억회로는 상기 제한정보의 저장 영역을 갖는다. 상기 제어 회로는, 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행한다. 상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타내는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정한다. 상기 제어 회로에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행한다.

《반포 단말장치》

본 발명의 제4의 관점은, 기한첨부 데이터의 부정 억세스 억지 기능을 반포 단말장치등의 데이터 처리장치가 지원하는 관점이다.

〔30〕 본 발명에 관한 데이터 처리장치는 매체 인터페이스부 및 데이터 처리부를 가지고, 매체 인터페이스부에 장착된 기억매체에 소정의 정보를 저장한다. 상기 데이터 처리부는 복호열쇠의 발행 요구에 응답해서 기억매체로부터 증명정보를 취득하고 기억매체를 인증한 후에, 매체 인터페이스부로부터 기억매체에 상기 소정의 정보로서 이용정보를 복호하기 위한 복호열쇠와 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장한다. 상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고, 상기 억세스 시간정보의 초기값은 소정으로 시간정보이다. 상기 증명정보는 특정한 기억매체인 것을 표시하는 정보이다. 특정한 기억매체는 상기 항목 〔29〕의 기억매체와 같다.

발명의 구성 및 작용

도 1에는 컨텐츠데이터 송신시스템가 예시된다. 컨텐츠 서버(1)이 접속하는 네트워크(2)에는 대표적으로 나타나는 이용기한첨부 데이터 단말장치(데이터처리장치) (3)이 접속된다. 이용기한첨부 데이터 단말장치(단순히 데이터 단말장치라고도 칭한다)(3)는 다운로드 재생부(다운로드부 및 재생부)(10), 이용기한 판정부(이용제한부) (11) 및 단말내부시계(12)를 갖는다. 데이터 단말장치(3)에는 기억매체로서 불휘발성 기억장치(단순히 메모리카드라고도 칭한다)(13)이 착탈자재로된다. 메모리카드(13)은 플래시메모리등의 전기적으로 소거 및 기입 가능한 불휘발성 메모리(불휘발성 기억회로)(14)를 구비한다.

데이터 단말장치(3)에 의한 컨텐츠데이터의 다운로드 기능의 개략을 설명한 다. 데이터 단말장치(3)에 메모리카드(13)이 장착되어서, 데이터 단말장치(3)에 컨텐츠데이터의 다운로드가 지시되면, 데이터 단말장치(3)은 컨텐츠 서버(1)로부터 이용기한첨부 컨텐츠데이터(이용정보)와 그것에 대응한 재생 라이센스(이용정보 라이센스)를 다운로드하고 메모리카드에 기입한다. 또한, 서버(1)로부터 다운로드의 일시데이터를 취득하고, 메모리카드(13)에 기입한다. 메모리카드(13)에 기입된 일시데이터가 카드 일시데이터이다. 특별히 제한되지 않지만, 다운로드된 일시데이터는 이용 제한 판정부에서 라이센스 포맷에 조합되어서 시큐어라이센스로서 불휘발성 메모리(14)의 시큐어 영역에 저장된다. 특별히 제한되지 않지만, 이용기한도 시큐어라이센스가 보유한다. 또한, 특별히 제한되지 않지만, 재생 라이센스도 불휘발성 메모리(14)의 시큐어 영역에 저장된다.

데이터 단말장치(3)에 의한 기한첨부 컨텐츠데이터의 재생 기능에 대해서 개략을 설명한다. 데이터 단말장치(3)에 재생이 지시되면 데이터 단말장치(3)은 메모리카드(13)로부터 재생 라이센스를 독출한다. 독출한 재생 라이센스로부터 이용기한을 독출하고, 컨텐츠데이터의 이용기한을 이용기한 판정부(11)에 전달한다. 이용기한부11은, 컨텐츠데이터의 이용기한(억세스 기한정보), 단말내부시계(12)가 나타내는 단말 일시데이터(시각정보), 카드가 보유하는 카드 일시데이터(억세스 시간정보)에 의해 억세스 가부를 판정한다. 즉, 상기 단말 일시데이터에 의해 나타나는 일시가 억세스 기한정보에 의해 나타내는 억세스 기한보다도 뒤이거나 또는 상기 단말 일시데이터에 의해 나타나는 일시가 카드 일시데이터에 의해 나타나는 일시보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정한다. 억세스 가능이면 메모리카드(13)의 컨텐츠데이터를 독출하여 재생한다. 억세스불가이면 재생 라이센스등을 소거한다. 이용기한 판정부(11)은 상기 억세스 가부판정과 함께, 상기 단말 일시데이터에 근거해서 메모리카드(13)내의 카드 일시데이터를 갱신한다.

카드 일시데이터의 갱신은, 상기 억세스 가부판정시에 대표되는 억세스 개시시뿐만아니라, 억세스 종료시에도 행한다. 또한, 예를 들면, 적어도 메모리카도로 동작전원을 투입할 때와 동작전원을 차단할 때에 행하도록 해도 좋다.

도 2에는 컨텐츠데이터 배신시스템에 다른 데이터 단말장치(4)가 접속되어 있는 예가 나타난다. 데이터 단말장치(4)은 다운로드 재생부(다운로드부 및 재생부)(10)과 단말내부시계(12)을 갖는다. 데이터 단말장치(3)에는 기억매체로서 불휘발성 기억장치(단순히 메모리카드라고도 칭한다)(15)가 착탈 자재로 된다. 메모리카드(15)은 이용기한 판정부(이용 제한부)(16)과 불휘발성 메모리(14)을 구비한다.

데이터 단말장치(4)에 의한 컨텐츠데이터의 다운로드 기능의 개략을 설명한다. 데이터 단말장치(4)에 메모리카드(15)이 장착되어서, 데이터 단말장치(4)에 컨텐츠데이터의 다운로드가 지시되면, 데이터 단말장치(4)은 컨텐츠 서버(1)로부터 이용기한첨부 컨텐츠데이터(이용정보)과 그것에 대응한 재생 라이센스(이용정보 라이센스)을 다운로드하고 메모리카드(15)에 기입한다. 또한, 서버(1)로부터 다운로드의 일시데이터를 취득하고 메모리카드(15)에 기입한다. 메모리카드(15)에 기입된 일시데이터가 카드 일시데이터이다. 특별히 제한되지 않지만, 다운로드된 일시데이 터는 이용제한 판정부에서 라이센스 포맷에 조합되어서 시큐어라이센스로서 불휘발성 메모리(14)의 시큐어 영역에 저장된다. 특별히 제한되지 않지만, 재생 라이센스도 불휘발성 메모리(14)의 시큐어 영역에 저장된다.

기한첨부 컨텐츠데이터의 재생 기능에 대해서 개략을 설명한다. 데이터 단말장치(4)에 재생이 지시되면 데이터 단말장치(4)은 이용기한 판정부(16)에 메모리카드(15)의 재생 라이센스를 취득시킨다. 이용기한 판정부(16)은 독출한 재생 라이센스로부터 이용기한을 취출한다. 이용기한 판정부(16)은, 컨텐츠데이터의 이용기한(억세스 기한정보), 단말내부시계(12)이 나타내는 단말 일시데이터(시각정보), 불휘발성 메모리(14)이 보유하는 카드 일시데이터(억세스 시간정보)에 의해 억세스 가부를 판정한다. 즉, 상기 단말 일시데이터에 의해 나타나는 일시가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 상기 단말 일시데이터에 의해 나타나는 일시가 카드 일시데이터에 의해 나타내는 일시보다도 이전인 경우에 억세스 불가로 판정하고, 그 밖의 경우를 억세스 가능이라고 판정한다. 억세스 가능이면 이용기한 판정부(16)은 다운로드 재생부(10)에 메모리카드(13)의 컨텐츠데이터를 독출시켜서 재생 가능하게 한다. 이용기한 판정부(16)은 상기 억세스 가부판정과 함께 상기 단말 일시데이터에 근거해서 메모리카드내의 카드 일시데이터를 갱신한다.

카드 일시데이터의 갱신은, 상기 억세스 가부판정시에 대표되는 억세스 개시시뿐만아니라, 억세스 종료시에도 행한다. 또한, 예를 들면, 적어도 메모리 카도에 관한 동작전원을 투입할 때와 동작전원을 차단할 때에 행하도록 해도 좋다

.

도 3에는 상기 단말 일시데이터에 근거해서 갱신되는 카드 일시데이터에 의한 이용 제한의 개요가 예시된다. 컨텐츠 데이터를 다운로드한 일시(빌린 날)(Ts), 이용기한(반환일)(Te)는 고정이다. 현재라고 되어 있는 시간은 단말 일시데이터가 나타내는 시간Tc이다. 억세스 일시로 되어 있는 것이 카드 일시데이터가 나타내는 시간(Tacs)다. 카드 일시데이터가 갱신되지 않으면 그것이 나타내는 일시는 컨텐츠데이터를 다운로드한 일시(빌린 날)(Ts)로 고정된다. 만일 (a)과 같이, 카드 일시데이터(Tacs)가 갱신되지 않으면 현재일시(Tc)가 빌린 날(Ts)과 이용기한(Te)의 사이의 어디에 있어도 이용 가능해지고, 예를 들면 (b)와 같이 현재일시(Tc)가 이용기한(Te)를 넘으면 이용 불가로 된다. 그러나, 단말시계를 조작해서 현재일시를 빌린 날과 이용기한의 사이로 이동하면, 컨텐츠데이터는 부정으로 이용 가능하게 된다. 이것에 대하여 도 1, 도 2에서는 상기 단말 일시데이터에 근거해서 메모리카드내의 카드 일시데이터를 갱신하기 때문에, (c)와 같이 억세스 일시라고 되어 있는 카드 일시데이터(Tacs)가 나타내는 일시부터 이용기한까지의 시간은 갱신마다 좁혀지며 최후로 이용기한(Te)을 초월한다. 일단 넘으면 이용 불가로 된다. 이미 유저는 단말내의 시계를 이용 제한보다 이전의 일시로 돌려도 재생은 불가로된다. 이것에 의해, 데이터 단말장치내부의 시계가 조작되어도 기한첨부 컨텐츠의 부정한 재생을 충분히 억제하는 것이 가능하게 된다.

카드 일시데이터의 갱신은, 억세스 종료 시점뿐만 아니라 억세스 시작시점에서도 행하여지기 때문에, 이용정보의 재생종료 직전에 전원이 차단되어도 적어도 1회의 억세스 시간정보의 갱신은 보증된다. 도 2와 같이, 기한첨부 이용정보의 부정 재생억제기능은 불휘발성 기억장치가 구비하므로, 재생장치를 바꾸어도 여전히 부정 억세스 억지 기능을 작용시키는 것은 용이하다.

도 4에는 상기 이용기한 판정부(11)와 단말내부시계(12)의 구체적인 예가 나타난다. 20에서 나타나는 회로 블럭은, 적어도 상기 이용기한 판정부(11)와 단말내부시계(12)를 실현하는 마이크로 컴퓨터라고 한다. 도4에는 마이크로 컴퓨터(20)의 내부를 기능 블럭에 의해 나타내고 있다. 마이크로 컴퓨터(20)는 일시데이터 취득 작성부(21), 암호화부(22), 라이센스 작성부(23), 시큐어 영역 억세스부(24), 일시데이터 취득부(25), 복호부(26), 이용 제한 판정부(26),및 단말내 시계회로(27)를 갖는다.

불휘발성 메모리(14)은 시큐어 영역(억세스 제한 영역)(14A)와 비시큐어 영역(억세스 비제한 영역)(14B)을 갖는다. 시큐어 영역(14A)에 대한 기입 억세스는 메모리카드(13)내의 증명정보에 대하여 메모리카드 외부 예를 들면 단말장치(20)이나 서버(1)에 의한 인증을 받아서 가능하게 된다. 외부로부터 시큐어 영역(14A)에 대한 독출은 외부로부터 주어지는 증명정보에 대하여 인증을 얻는 것을 조건으로 허가된다. 도시는 생략하지만, 메모리카드(13)은 불휘발성 메모리(14)의 억세스 제어와 외부와의 인터페이스제어를 행하는 카드 컨트롤러를 가지고 있다. 시큐어 영역 억세스부(24)은 그 카드 컨트롤러를 통해서 인터페이스된다.

이 예에서는, 카드 일시데이터 암호화부(22)에서 암호화한 후, 이것을 라이센스 작성부(23)에서 시큐어라이센스에 메워넣고, 시큐어 영역 억세스부(24)의 제어로 불휘발성 메모리(14)의 시큐어 영역(14A)에 기록하게 되어 있다.

상기 일시데이터 취득 작성부(21)는 서버(1)가 컨텐츠데이터나 라이센스를 다운로드했을 때 서버(1)로부터 일시데이터(다운로드 일시데이터)을 취득하는 회로다. 취득한 일시데이터의 포맷은 도5에 예시되는 것 같이, 16바이트의 데이터로 구성된다.

상기 암호화부(22)은 서버로부터 취득한 상기 일시데이터를 암호화한다. 암호화 방식은, 특별히 제한되지 않지만, 컨텐츠의 암호화 복호처리에서 이용되고 있는 것과 같은 AES(Advanced Encryption Standard)방식을 이용한다. 일시데이터를 암호화하는 열쇠는 메모리카드 고유의 속성정보, 예를 들면, 카드의 시리얼번호등을 이용한다.

상기 라이센스 작성부(23)은, 취득해서 암호화한 일시데이터를 예를 들면 라이센스 포멧중의 컨텐츠 열쇠의 부분에 메워넣어서 시큐어라이센스를 작성한다.

상기 시큐어 영역 억세스부(24)은 일시데이터가 포함되어 있는 시큐어라이센스를 불휘발성 메모리의 시큐어 영역(14A)에 기입한다. 시큐어 영역(14A)에 관한 기입에는 상기 기입 인증이 필요하다. 상기 일시데이터 취득부(25)은 암호화된 일시데이터가 포함되는 라이센스를 시큐어 영역에서 독출하고, 암호화된 일시데이터를 취출한다. 시큐어 영역(14A)의 독출에는 상기 독출 인증이 필요해 진다.

복호부(26)는 시큐어라이센스로부터 취출한 암호화된 일시데이터를 AES에서 복호한다. 복호하는 열쇠는 암호부(22)에서 이용한 열쇠와 같은 것을 사용한다.

상기 이용 제한 판정부(27)는 상술한 바와 같이, 이용기한이 끊어져 있지 않은지를 판정함과 동시에, 단말내의 시계가 유저에 의해 조작되고 있지 않는지를 판 정한다. 그 판정 내용은 도1을 참조해서 이미 설명했다. 조작되어 있다고 판정하면, 카드내의 라이센스를 모두 소거한다. 단말내 시계회로(28)는 단말내의 시계로부터 연월일시간을 취득한다.

도 4의 각기능블럭는, 특별히 도시하지는 않았지만, 중앙처리장치, 부동 소수점연산 유닛, 그것들의 처리 프로그램을 보유하는 ROM(리드 · 온리 · 메모리), 중앙처리장치의 워크 영역 등에 이용되는 RAM(랜덤 · 억세스 · 메모리), 리얼 타임클럭회로, 타이머 및 입출력 회로등에 의해 구성된다.

도 4의 회로의 동작을 설명한다. 최초로 서버(1)과 통신했을 때나 컨텐츠, 라이센스를 다운로드했을 때의 동작을 설명한다.

서버(1)과 접속했을 때, 서버(1)로부터 일시데이터를 일시데이터 취득 · 작성부(21)에서 취득한다. 취득한 일시데이터는 라이센스 포맷중의 컨텐츠열쇠 영역에 조합가능하게 하기 위해서, 일시데이터는 예를 들면 도 5에 예시하는 16바이트의 데이터 구성이 된다. 일시가 2002년10달10일(목) 15시 30분45초00일 때, 이 일시데이터를 16진(進)으로 표시하면, '07D2 000A 000A 0004 000F 001E 002D 0000 h'가 된다.

암호화부(22)에서, 일시데이터 취득 · 작성부(21)에서 작성한 16바이트의 일시데이터을 AES방식으로 암호 한다. 암호화하는 열쇠는 카드 고유의 시리얼번호를 사용한다.

라이센스 작성부(23)에서, 암호화한 일시데이터를 라이센스내의 컨텐츠 열쇠의 부분에 메워넣고, 하나의 라이센스를 작성한다. 작성된 라이센스는, 시큐어 영 역 억세스부(24)에 의해 메모리카드의 시큐어 영역에 기입된다. 시큐어 영역이 128개의 라이센스를 기록할 수 있을 경우에는, 최후의 128번째에 일시데이터를 포함하는 라이센스를 기입한다. 시큐어 영역(14A)에 대한 기입은 상기 기입 인증을 받아서 가능하게 된다.

다음으로 이용 제한 판정 처리의 동작에 대해서 설명한다. 시큐어 영역 억세스부(24)에서, 시큐어 영역(14A)로부터 암호화되어 있는 일시데이터가 포함되어 있는 시큐어라이센스를 독출한다. 시큐어 영역에 대한 리드 억세스는 상기 독출 인증을 받아서 가능하게 된다. 일시데이터 독출부(25)에서, 독출한 라이센스로부터 암호화되어 있는 일시데이터 16바이트를 취출한다. 복호화부(26)에서, 16바이트의 일시데이터를 AES방식으로 복호한다. 복화화하는 열쇠는 암호화했을 때와 같은 카드 고유의 시리얼번호를 사용한다. 이어서, 단말내 시계취득부(28)에서 단말내의 일시를 취득한다. 이용 제한 판정부(27)에서, 이용기한, 단말의 일시데이터, 카드의 일시데이터를 이용해서 기한이 다 되어 있지 않은지 부정한 조작이 행하여지고 있지 않는지를 판정한다.

다음으로 일시데이터의 갱신 처리 동작에 대해서 설명한다. 카드내에는 전원이 없기 때문에, 카드 스스로는 일시데이터를 갱신할 수는 없다. 따라서, 상기에서 설명한 것 같이 서버와의 접속시나 컨텐츠의 재생, 표시시(이용제한판정 처리일 때)에 일시데이터를 갱신한다. 그러나, 서버와 접속을 하지 않을 경우나 컨텐츠의 재생 표시를 행하지 않을 경우에는 장시간 갱신되지 않을 경우가 있다. 일시데이터를 갱신하는 타이밍은, 상술의 억세스 개시시와 종료시의 이외에, 메모리카드가 데이 터 단말에 삽입되었을 때와 이탈되었을 때, 또는 메모리카드가 데이터 단말에 장착되어 있는 상태로 데이터 단말의 전원온이 지시되었을 때와 전원오프가 지시되었을 때 등이어서 좋다. 데이터 단말의 전원을 오프로 할 때에는, 마이크로 컴퓨터 내부의 타이머로 측정한 시간을 카드에 기록되어 있는 일시데이터에 가산하는 것에 의해 갱신하면 좋다.

도 6에는 상기 메모리카드(15)에 내장된 상기 이용기한 판정부(16)의 구체예가 나타난다. 상기 이용기한 판정부(16)은 마이크로 컴퓨터(30)에 의해 구성된다. 도6에서는 마이크로 컴퓨터(30)는 외부 인터페이스 컨트롤러(31) 및 메모리 컨트롤러(32)와 함께 카드 컨트롤러를 구성한다. 도6에는 마이크로 컴퓨터(30)을 그 일부의 기능인 이용기한 판정부(16)을 구성하는 기능 블럭에 의해 도시하고 있다. 마이크로 컴퓨터(30)에 의해 실현되는 도시된 기능 블럭은, 암호화부(33), 라이센스 작성부(34), 일시데이터 취득부(35), 복호부(36), 이용기한취출부(37) 및 이용 제한 판정부(38)이다.

외부 인터페이스 컨트롤러(31)은 마이크로 컴퓨터(30)의 지시에 따라서 소정의 메모리카도인터페이스 사양에 준거한 외부 인터페이스제어를 행한다. 메모리 컨트롤러(32)은 마이크로 컴퓨터(30)의 지시에 따라서 불휘발성 메모리(14)에 대한 소거, 기입 및 독출의 억세스 제어를 행한다.

특별히 도시하지는 않았지만, 마이크로 컴퓨터(30)는 중앙처리장치, 부동 소수점연산 유닛, 그것들의 처리 프로그램을 보유하는 ROM(리드 · 온리 · 메모리), 중앙처리장치의 워크 영역등에 이용되는 RAM(랜덤 · 억세스 · 메모리), 리얼타임클럭 회로, 타이머 및 입출력 회로등에 의해 구성된다. 마이크로 컴퓨터(30)는 상기 이용기한 판정부(16)을 실현함과 동시에, 그 동작 프로그램을 따라서 인증을 위한 연산 처리나 불휘발성 메모리(14)을 억세스하기 위한 어드레스연산 처리 등을 행하는 기능을 갖는다.

불휘발성 메모리(14)은 시큐어 영역(억세스 제한 영역)(14A)와 비시큐어영역(억세스 비제한 영역)(14B)을 갖는다. 시큐어 영역(14A)에 대한 기입 억세스는 메모리카드(15)내의 증명정보에 대하여 메모리카드 외부 예를 들면 단말장치(20)이나 서버(1)에 의한 인증을 받아서 가능하게 된다. 외부로부터 시큐어 영역(14A)에 대한 독출은 외부로부터 주어지는 증명정보에 대하여 인증을 얻는 것을 조건에 허가된다. 메모리카드(15)내의 상기 증명정보는, 그 메모리카

드(15)가 도 2 및 도 6에서 설명한 이용기한판정 기능등을 구비한 메모리카드이며, 그 밖의 메모리카드와 구별가능한 정보를 포함하고 있다.

이 예에서는, 카드 일시데이터 암호화부(33)에서 암호화한 후, 이것을 라이센스 작성부(34)에서 시큐어라이센스에 메워넣고, 메모리 컨트롤러(32)을 통해서 불휘발성 메모리(14)의 시큐어 영역(14A)에 기록하게 되어 있다. 특별히 제한되지 않지만, 컨텐츠의 이용기한도 시큐어라이센스가 보유한다.

도 2의 다운로드 재생부(10)가 컨텐츠데이터나 라이센스를 서버로부터 다운로드했을 때 서버(1)로부터 일시데이터(다운로드 일시데이터)가 취득된다. 일시데이터는 컨텐츠 라이센스에 부수된다. 취득한 일시데이터의 포맷은 도 5에 예시되는 것 같이, 16바이트의 데이터로 구성된다.

상기 암호화부(33)는 서버로부터 취득한 상기 일시데이터를 수취하고 암호화한다. 암호화 방식은, 특별히 제한되지 않지만, 컨텐츠의 암호화 복호처리에서 이용하고 있는 것과 같은 AES(Advanced Encryption Standard)방식을 이용한다. 일시데이터를 암호화하는 열쇠는 메모리카드 고유의 속성정보, 예를 들면, 카드의 시리얼번호 등을 이용한다.

상기 라이센스 작성부(34)은, 취득해서 암호화한 일시데이터를 예를 들면 라이센스 포맷중의 컨텐츠 열쇠의 부분에 메워넣어서 시큐어라이센스를 작성한다.

작성된 시큐어라이센스는 메모리 컨트롤러(32)을 통해서 불휘발성메모리의 시큐어 영역(14A)에 기입된다. 시큐어 영역(14A)에 관한 기입에는 상기 기입 인증이 필요해진다. 상기 일시데이터 취득부(36)은 암호화된 일시데이터가 포함되는 시큐어라이센스가 시큐어 영역(14A)로부터 독출되었을 때, 그것로부터 암호화된 일시데이터를 추출한다. 이용기한취출부(37)은 시큐어라이센스가 시큐어 영역(14A)로부터 독출되었을 때, 그것로부터 이용기한 데이터를 추출한다. 시큐어 영역(14A)의 독출에는 상기 독출 인증이 필요하다.

복호부(36)은 시큐어라이센스로부터 취출한 암호화된 일시데이터를 AES에서 복호한다. 복호하는 열쇠는 암호부(33)에서 이용한 열쇠와 같은 것을 사용한다.

상기 이용 제한 판정부(27)은, 상술한 바와 같이, 이용기한이 다 되어 있지 않은지를 판정함과 동시에, 데이터 단말(4)내의 시계(12)가 유저에 의해 조작되고 있지 않은지를 판정한다. 그 판정 내용은 도2을 참조해서 이미 설명했다. 조작되고 있다고 판정하면, 시큐어 영역(14A)내의 라이센스를 모두 소거한다.

도 6의 회로의 동작을 설명한다. 최초로, 서버(1)과 통신했을 때나 컨텐츠, 라이센스를 다운로드했을 때의 동작을 설명한다.

데이터 단말장치(4)가 서버(1)에 접속했을 때, 서버(1)로부터의 일시데이터를 외부 인터페이스 컨트롤러(31)을 통해서 입력한다. 아울러 재생 기한일 데이터도 입력한다. 재생 기한일은 예를 들면 재생 라이센스에 포함되는 것을 이용한다. 입력한 일시데이터는 도5에 예시하는 16바이트의 데이터 구성으로 된다. 일시데이터는 암호화부(33)에 의해 예를 들면 AES방식으로 암호 된다. 암호화하는 열쇠는 카드 고유의 시리얼번호를 사용한다.

라이센스 작성부(34)에서, 암호화한 일시데이터를 라이센스내의 컨텐츠 열쇠의 부분에 메워넣고, 시큐어라이센스를 작성한다. 작성된 라이센스는, 메모리 컨트롤러(32)을 통해서 메모리카드(14)의 시큐어 영역(14A)에 기입된다. 시큐어 영역이 128개의 라이센스를 기록할 수 있을 경우에는, 최후의 128번째에 상기 시큐어라이센스를 기입한다. 시큐어 영역(14A)에 대한 기입은 상기 기입 인증을 받아서 가능해 진다.

다음으로 이용 제한 판정 처리의 동작에 대해서 설명한다. 메모리 컨트롤러(32)을 통해서 시큐어 영역(14A)로부터 시큐어라이센스가 독출된다. 시큐어 영역에 대한 리드 억세스는 상기 독출 인증을 받아서 가능하게 된다. 일시데이터 취출부(35)에서, 독출한 라이센스로부터 암호화되어 있는 일시데이터16바이트를 취출한다. 이용기한취출부(37)에서는 이용기한을 취출한다. 복호부(36)에서, 16바이트의 일시데이터를 AES방식으로 복호한다. 복호하는 열쇠는 암호화했을 때와 같 은 카드 고유의 시리얼번호를 사용한다. 이어서, 단말내의 일시를 취득한다. 이용 제한 판정부(38)에서 이용기한, 단말의 일시데이터, 카드의 일시데이터를 이용해서 기한이 다 되어 있는 것인지, 부정한 조작이 행하여지지 않고 있는 것인지를 판정한다.

다음으로 일시데이터의 갱신 처리 동작에 대해서 설명한다. 카드내에는 전원이 없기 때문에, 카드 스스로는 일시데이터를 갱신할 수는 없다. 따라서, 상기에서 설명한 것 같이 서버와의 접속시나 컨텐츠의 재생, 표시시(이용 제한 판정 처리시)에 일시데이터를 갱신한다. 그러나, 서버와 접속을 하지 않을 경우나 컨텐츠의 재생 표시를 행하지 않을 경우에는 장시간 갱신되지 않을 경우가 있다. 일시데이터를 갱신하는 타이밍은 상술의 억세스 개시시와 종료시의 이외에, 메모리카드가 데이터 단말에 삽입되었을 때와 이탈되었을 때, 또는 메모리카드가 데이터 단말에 장착되어 있는 상태로 데이터 단말의 전원온이 지시되었을 때와, 전원오프가 지시되었을 때등이어도 좋다. 데이터 단말의 전원을 으포로

할 때에는, 마이크로 컴퓨터 내부의 타이머로 측정한 시간을 카드에 기록되어 있는 일시데이터에 가산하는 것에 의해 갱신하면 좋다.

갱신 처리를 또 다른 타이밍으로 행해도 좋다. 즉, 메모리카드가 화일 메모리 방식에 의한 섹터 단위로 분할해서 데이터 억세스를 행할 경우, 억세스 개시시의 상기 억세스 판정 동작에 있어서 억세스 가능이라고 판정된 후는, 후속 섹터의 억세스마다 또는 소정의 복수 억세스마다 상기 억세스 판정 동작을 행해도 좋다. 이와 같이 섹터 단위로 분할된 데이터의 억세스에 대한 억세스 판정 동작에 있어서, 제2회째 이후의 억세스 판정 동작에서는, 시각정보가 상기 억세스 기한정보에 의해 나타나는 억세스 기한보다 뒤에 있어도 억세스 가능이라고 판정하도록 해서 좋다. 억세스 판정 동작을 몇회나 행할 때, 이용정보의 재생 도중등에서 기한이 도래해서 재생이 중단되는 문제점을 간단히 해소할 수 있다.

도 7에는 재생 라이센스의 포맷이 예시되어 있고, 도 8에는 시큐어 라이센스의 포맷이 예시된다. 컨텐츠ID는 컨텐츠마다 유니크에 할당되는 식별자이다. 트랜잭션ID는 트랜잭션마다 유니크한 식별자이다. 트랜잭션ID에는 재생 가능횟수(라이센스를 독출시키는 횟수), 이동 가능횟수(라이센스를 이동할 수 있는 횟수) 및 세이프 레벨(보호 강도)의 식별자를 포함한다. 미디어 억세스 조건은 미디어 내부에서 강제가능한 억세스 조건이다. 컨텐츠 열쇠는 컨텐츠를 암호화할 때에 이용한 열쇠이며, 컨텐츠를 복호할 때에 이용한다. 디코더 억세스 조건은 재생용 디코더의 내부에서 강제가능한 억세스 조건을 나타낸다. 디코더 억세스 조건에는 재생 사이즈(1개의 라이센스로 재생가능한 컨텐츠 사이즈)과 이용기한(이용가능한 기한)를 포함한다. 확장 미디어 억세스 조건은 증명서인증, PIN인증을 행할 것이 아닌가를 나타내는 플래그로 된다. 재생 라이센스는 컨텐츠 열쇠를 가지고 있지만, 시큐어라이센스는, 그 재생 라이센스의 컨텐츠 열쇠를 카드 일시데이터에 바꿔 넣어서 구성된다.

증명서인증 예를 들면 시큐어 영역의 기입 인증을 받기 위한 증명정보, 그리고 PIN(Personal Identification Number)에 의한 개인인증을 행하기 위한 PIN은 불휘발성 메모리(14)에 저장되어 있다.

도 9에는 라이센스의 기입시의 인증(기입 인증)처리 순서가 예시된다. 우선, 증명인증을 행할 것인지 아닌지가 판정되고(S1), 행할 경우에는 메모리카드로부터 인증 정보와 공개 암호열쇠를 갖는 증명서(미디어클래스 증명서)를 독출하고(S2), 이것을 서버에 송신한다(S3). 서버는 그 증명서를 검증하고(S4), 그것에 의해서 인증되면, 메모리카드의 시큐어 영역에 대한 재생 라이센스 및 시큐어라이센스의 기입이 허용된다(S5). 상기 미디어클래스 증명서는, 예를 들면 상기 이용기한판정 기능등을 구비한 메모리카드(15)를, 해당 기능을 갖추고 있지 않은 다른 메모리카드와 구별할 수 있는 증명정보를 가지고 있다.

도 10에는 라이센스의 독출시의 인증(독출 인증)처리 순서가 예시된다. 우선, 증명인증을 행할 것인지 아닌지가 판정되고(S11), 행할 경우에는 데이터 단말로 메모리카드에 인증 정보와 공개 암호열쇠를 갖는 증명서(디코더클래스 증명서)을 송신한다(S12). 메모리카드는 그 증명서를 검증하고(S3), 그것에 의해서 인증되면, 메모리카드의 시큐어 영역으로부터 재생 라이센스 및 시큐어라이센스의 독출이 허용된다(S14). 처리(S11)의 판별로 증명인증을 행하지 않을 경우에는, PIN인증을 행할지의 판별을 행하고(S15), 행할 경우에는 데이터 단말장치로부터 PIN을 메모리카드에 송신하고(S16), 메모리카드내에서 PIN의 검증을 행한다. PIN이 정당하면 라이센스의 독출을 행한다(S14). PIN이 부당할 경우, PIN인증을 행하지 않을 경우, 증명인증을 얻을 수 없을 경우에는 그대로 처리를 종료한다.

도 11에는 이용기한부 컨텐츠의 재생 처리 플로우의 일례가 나타난다. 재생 라이센스를 이용해서 이용기한부 컨텐츠의 재생을 행할 경우, 우선 이용기한판정처 리R21을 행하고, 재생가능하면 카드 일시데이터 갱신 처리(R22)를 행하고, 이용기한부 컨텐츠의 재생종료를 판정하고(S23), 종료가 아니면 소정의 인터벌마다 카드 일시데이터 갱신 처리(R22)를 반복한다. 재생종료를 판별하면, 최후에 카드 일시 갱신 처리(R22)을 행해서 종료한다.

도 12에는 이용기한판정처리R21의 상세한 일례가 나타난다. 데이터 단말장치의 일시정보를 취득하고, 단말 일시데이터를 작성한다(S31). 이어서, 필요한 증명인증 또는 PIN인증을 행하고 메모리카드로부터, 카드 일시데이터를 취득하고(S32), 라이센스로부터 이용기한을 취득한다(S33). 이용 제한과 카드 일시데이터를 비교하고(S34), 이용기한≤카드 일시데이터의 경우에는 기한 마감이라고 판정해서 처리를 종료한다. 이용기한>카드 일시데이터의 경우에는 단말 일시데이터와 카드 일시데이터를 비교한다(S35). 단말 일시데이터≤카드 일시데이터의 경우에는 단말 일시데이터가 부정이라고 판정하고, 메모리카드가 보유하는 모든 라이센스의 소거를 행한다(S36). 단말 일시데이터>카드 일시데이터의 경우에는 카드의 일시데이터를 단말의 일시데이터에 갱신한다(S37).

도 13에는 카드 일시데이터 갱신 처리R22의 상세한 일례가 나타난다. 데이터 단말장치의 일시정보를 취득하고, 단말 일시데이터를 작성한다(S41). 이어서, 필요한 증명인증 또는 PIN인증을 행하고 메모리카드로부터 카드 일시데이터를 취득한다 (S42). 단말 일시데이터와 카드 일시데이터를 비교한다(S43). 단말 일시데이터≤카드 일시데이터의 경우에는 단말 일시데이터가 부정이라고 판정하고, 메모리카드가 보유하는 모든 라이센스의 소거를 행한다(S44). 단말 일시데이터>카드 일시데이터 의 경우에는 카드의 일시데이터를 단말의 일시데이터에 갱신한다(S45). 도 13의 처리는 도 12에 대하여 라이센스로부터 이용기한을 취득하지 않고, 이용기한≤카드 일시데이터의 경우에 기한 마감이라고 판정해서 처리를 종료하는 것을 행하지 않는다. 따라서, 이용기한부 컨텐츠의 재생 도중등에서 재생 기한이 도래해서 재

생이 중단되는 문제점을 해소할 수 있다.

도 14에는 기한첨부 데이터의 재생 단말장치(40)가 나타난다. 같은 도에 나타나는 재생 단말장치(40)은 재생부(41)을 가지고, 도 2의 단말장치(4)에 대하여 컨텐츠데이터와 라이센스의 다운로드 기능이 생략된 재생전용기으로서 구성된다. 도 11내지 도 13에 나타나는 컨텐츠 재생 처리를 행할 수 있다.

도 15에는 다운로드 단말장치(45)가 나타난다. 같은 도에 나타나는 다운로드 단말장치(45)는 도 2에서 설명한 단말장치(4)에 있어서의 다운로드 재생부(10)에 대하여 컨텐츠데이터의 재생 기능이 생략된 컨텐츠데이터와 라이센스의 다운로드 전용 단말장치로 된다. 다운로드 전용 단말장치(45)은 호스트 인터페이스부(46), 메모리카드인터페이스부(47) 및 데이터 처리부(48)을 가지고, 메모리카드인터페이스부(47)에 장착된 메모리카드(15)에 컨텐츠를 복호하기 위한 컨텐츠 라이센스, 컨텐츠에 대한 억세스 제한을 행하는 재생 기한 데이터 및 카드 일시데이터를 초기적으로 저장한다. 상기 데이터 처리부(48)는 상기 컨텐츠 라이센스의 수령 요구와 함께 메모리카드(15)가 보유하는 증명정보를 호스트 인터페이스부(46)로부터 외부에 출력하고, 이것에 응답해서 예를 들면 서버(1)로부터 호스트 인터페이스부(46)에 돌아가는 정보를 수령해서 메모리카드인터페이스부(47)로부터 상기 메모리카드(15) 에 저장한다. 상기 수령하는 정보는, 컨텐츠의 복호에 이용되는 컨텐츠 열쇠, 컨텐츠에 대한 억세스 제한을 행하는 재생 기한 데이터 및 카드 일시데이터를 포함한다. 상기 증명정보는 이용기한판정 기능을 갖는 메모리카드(15)인 것을 나타내는 정보이다. 이 다운로드 단말장치를 이용해서 메모리카드에 컨텐츠 및 그 재생 라이센스를 반포 또는 판매하는 것에 의해, 대상이 되는 기억매체가 상기 이용기한판정 기능을 갖는 메모리카드(15)에 한정되기 때문에, 기한첨부 컨텐츠데이터에 대한 부정 억세스의 억지를 지원할 수 있다.

도 15의 구성은 네트워크에 접속하는 단말장치로서의 구성에 한정되지 않는다. 특별히 도시하지 않았지만, 다운로드 단말장치(45) 그것 자체가 컨텐츠 서버여도 좋고, 견해를 바꾸면 스텐드어론의 반포 단말장치가 된다.

이상 본 발명자에 의해 된 발명을 실시 형태에 근거해서 구체적으로 설명했지만, 본 발명은 그것에 한정되는 것이 아니고 그 요지를 일탈하지 않는 범위에 있어서 갖가지 변경가능한 것은 말할 필요도 없다.

예를 들면, 지금까지 설명한 다운로드 기능을 갖는 데이터 단말은 컨텐츠 및 컨텐츠 라이센스의 쌍방을 다운로드해서 반포하는 기능을 갖는 것으로서 설명했지만, 본 발명은 그것에 한정되지 않고 컨텐츠 라이센스만의 다운로드 또는 반포여도 좋다. 또한, 재생 기능을 갖는 데이터 단말장치에 있어서, 컨텐츠는 라이센스와 같은 메모리카드에 저장되어 있지 않아도 좋은 경우가 있다. 그 경우, 컨텐츠데이터는 CD-ROM이나 DVD-RAM등의 리무버 디스크드라이브를 이용해서 억세스하도록 해도 좋다. 또는 하드디스크불드라이브로부터 억세스하도록 해도 좋다.

또, 상기 설명에서는, 일시데이터를 암호화해서 라이센스에 메워넣어서 시큐어 영역에 기록하는 예를 나타냈지만, 암호화를 생략해도 좋다. 일시데이터를 암호화하지 않고 라이센스에 메워넣기 위해서 처리량이 적어서 된다. 또한, 일시데이터를 암호화해서 비시큐어 영역에 기록해도 좋다. 시큐어 영역을 가지지 않는 기억매체에도 사용할 수 있다. 또한, 일시데이터를 암호화하지 않고 또한 비시큐어 영역에 기록해도 좋다. 시큐어 영역을 가지지 않는 기억매체에도 사용할 수 있고, 게다가 AES의 암호/복호처리를 할 필요가 없기 때문에 최소의 구성으로 실현할 수 있다. 그러나, 유저에 의해 일시데이터가 조작될 가능성이 큰 것에 주의를 필요로 한다.

발명의 효과

본원에 있어서 개시되는 발명의 동안 대표적인 것에 의해 얻을 수 있는 효과를 간단히 설명하면 하기 대로다.

즉, 메모리카드 등의 불휘발성 기억장치에 억세스 시간정보와 같은 일시데이터를 갱신해서 기록하고, 게다가 억세스 시간정보의 갱신은 억세스 종료 시점뿐만아니라 복수시점에서 행하기 때문에, 이용정보의 재생종료 직전에 전원이 차단되어도 적어도 1회의 억세스 시간정보의 갱신은 보증된다. 기한첨부 이용정보의 부정재생억제기능을 불휘발성 기억장치가 구비함으로써 재생장치를 바꿔도 여전히 부정 억세스 억지 기능을 작용시키는 것이 용이하다.

(57) 청구의 범위

청구항 1.

제어 회로와 불휘발성 기억회로를 가지고,

상기 불휘발성 기억회로는 이용정보에 대한 억세스 제한을 행하는 제한정보의 저장 영역을 가지고,

상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 제어 회로는, 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱신하는 억세스판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고,

상기 제어 회로에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 2.
제어 회로와 불휘발성 기억회로를 가지고,

상기 불휘발성 기억회로는 이용정보에 대한 억세스 제한을 행하는 제한정보의 저장영역을 가지고,

상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 제어 회로는, 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타내는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고,

상기 제어 회로에 의한 억세스 판정 동작을 적어도 불휘발성 기억장치에 동작전원을 투입할 때와 동작전원을 차단할 때에 행하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 3.
청구항 1또는 2에 있어서,

상기 불휘발성 기억회로는 상기 이용정보의 저장 영역을 가지고, 상기 불휘발성 기억장치는 상기 이용정보를 복수로 분할해서 억세스를 행하고,

억세스 개시시의 상기 억세스 판정 동작에 있어서 억세스 가능이라고 판정된 후, 분할된 상기 이용정보의 억세스마다 또는 소정의 복수 억세스마다 상기 억세스 판정 동작을 행하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 4.
청구항 3에 있어서,

분할된 상기 이용정보의 억세스 단위는 섹터인 것을 특징으로 하는 불휘발성 기억장치.

청구항 5.
청구항 3에 있어서,

상기 분할된 이용정보의 억세스에 대한 억세스 판정동작에 있어서, 제2회째이후의 억세스 판정 동작에서는, 시각정보가 상기 억세스 기한정보에 의해 나타내는 억세스 기한보다 뒤에 있어도 억세스 가능이라고 판정하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 6.
청구항 3에 있어서,

상기 불휘발성 기억장치는 상기 시각정보가 출력가능한 외부장치에 접속되어 사용되는 것이며, 상기 외부장치에 상기 분할된 이용정보를 출력가능한 것을 특징으로 하는 불휘발성 기억장치.

청구항 7.
청구항 3에 있어서,

상기 불휘발성 기억회로는 불휘발성 반도체 메모리이며, 외부장치에 접속되는 인터페이스단자를 갖는 소정의 메모리 카드 케이싱에 내장되어서 이루어지는 것을 특징으로 하는 불휘발성 기억장치.

청구항 8.
청구항 1또는 2에 있어서,

상기 제한정보는 상기 제어 회로에 의해 암호화되어서 상기 불휘발성기억회 로에 저장되는 것을 특징으로 하는 불휘발성 기억장치.

청구항 9.
청구항 8에 있어서,

상기 제한정보의 암호화에 사용하는 암호열쇠는 불휘발성 기억장치고유의 속성정보인 것을 특징으로 하는 불휘발성 기억장치.

청구항 10.
청구항 1또는 2에 있어서,

상기 제어 회로는 상기 이용정보를 복호하기 위한 컨텐츠 열쇠를 포함하는 이용정보 라이센스를 수령하기 위해서 증명정보를 외부에 출력가능한 것을 특징으로 하는 불휘발성 기억장치.

청구항 11.
청구항 10에 있어서,

상기 제어 회로는, 상기 이용정보 라이센스를 외부로부터 수령해서 상기 불휘발성 기억회로에 저장하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 12.
청구항 11에 있어서,

상기 제어 회로는 상기 컨텐츠 열쇠와 함께 입력되는 시간정보를 상기 억세스 시간정보의 초기값으로서 상기 불휘발성 기억회로에 저장하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 13.
청구항 1또는 2에 있어서,

상기 불휘발성 기억회로는 억세스 제한 영역과 억세스 비제한 영역을 가지고,

상기 제한정보는 억세스 제한 영역에 저장되고,

상기 이용정보는 억세스 비제한 영역에 저장되는 것을 특징으로 하는 불휘발성 기억장치.

청구항 14.
청구항 13에 있어서,

상기 제어 회로는 외부로부터의 인증을 받아서 상기 억세스 제한영역에 대한 기입이 가능하게 되는 것을 특징으로 하는 불휘발성 기억장치.

청구항 15.
청구항 14에 있어서,

상기 억세스 제한 영역은 상기 이용정보 라이센스의 저장 영역으로 되는 것을 특징으로 하는 불휘발성 기억장치.

청구항 16.
청구항 13또는 14에 있어서,

상기 제어 회로는 외부로부터 주어지는 증명정보에 대한 인증을 행하고 상기 억세스 제한 영역에 대한 독출을 가능하게 하는 것을 특징으로 하는 불휘발성 기억장치.

청구항 17.
재생부와 이용 제한부를 가지고, 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장하여 고쳐쓰기 가능한 기억매체를 억세스해서 상기 이용정보를 재생가능한 데이터 처리장치이며,

상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 이용 제한부는 데이터 처리장치에서 생성되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 기억매체상의 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고,

상기 이용 제한부에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 18.
재생부와 이용 제한부를 가지고, 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장하는 고쳐쓰기 가능한 기억매체를 억세스해서 상기 이용정보를 재생이용가능한 데이터 처리장치이며,

상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 이용 제한부는 데이터 처리장치에서 생성되는 시각정보와 상기 제한정 보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 기억매체상의 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타내는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고,

상기 이용 제한부에 의한 억세스 판정 동작을 적어도 재생부에 기억매체를 장착할 때와 재생부에서 기억매체를 이탈할 때에 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 19.
청구항 18에 있어서,

상기 이용 제한부는, 재생부에 기억매체가 장착된 상태로 동작전원이 투입될 때와, 재생부에 기억매체가 장착된 상태로 동작전원이 차단될 때에 상기 억세스 판정 동작을 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 20.
청구항 17내지 19의 어느 1항에 있어서,

상기 이용 제한부는 기억매체고유의 속성정보를 암호열쇠로 하는 암호화를 행하고 억세스 시간정보의 갱신을 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 21.
청구항 17내지 19의 어느 1항에 있어서,

상기 기억매체는 고쳐쓰기 가능한 불휘발성 기억장치인 것을 특징으로 하는 데이터 처리장치.

청구항 22.
청구항 21에 있어서,

상기 불휘발성 기억장치는 억세스 제한 영역과 억세스 비제한 영역을 가지고,

상기 이용 제한 판정부는 억세스 제한 영역에 대하여 제한정보의 억세스를 행하고,

상기 재생부는 억세스 비제한 영역에 대하여 이용정보의 억세스를 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 23.
청구항 22에 있어서,

상기 이용 제한부는 불휘발성 기억장치로부터 주어지는 증명정보에 대하여 인증을 행한 후에 상기 억세스 제한 영역에 기입이 가능하게 되는 것을 특징으로 하는 데이터 처리장치.

청구항 24.
청구항 23에 있어서,

상기 억세스 제한 영역은 상기 이용정보를 복호하기 위한 이용정보 라이센스의 저장 영역이 되는 것을 특징으로 하는 데이터 처리장치.

청구항 25.
청구항 24에 있어서,

상기 이용 제한부는 불휘발성 기억장치에 증명정보를 주어서 인증을 받은 후에 상기 억세스 제한 영역에 대한 독출이 가능하게 되는 것을 특징으로 하는 데이터 처리장치.

청구항 26.
청구항 17내지 19의 어느 1항에 있어서,

호스트 인터페이스제어부를 가지고, 해당 호스트 인터페이스제어부는 상기 이용정보를 복호하기 위한 컨텐츠 열쇠를 포함하는 이용정보 라이센스를 수령하기 위해서 상기 기억매체가 보유하는 증명정보를 호스트장치를 향해서 출력가능한 것을 특징으로 하는 데이터 처리장치.

청구항 27.
청구항 26에 있어서,

상기 호스트 인터페이스제어 회로는 상기 이용정보 라이센스를 호스트장치로부터 수령해서 상기 기억매체에 저장가능한 것을 특징으로 하는 데이터 처리장치.

청구항 28.
청구항 27에 있어서,

상기 호스트 인터페이스제어 회로는 상기 컨텐츠 열쇠와 함께 입력되는 시간정보를 상기제 억세스 시간정보의 초기값으로서 상기 기억매체에 저장가능한 것을 특징으로 하는 데이터 처리장치.

청구항 29.
호스트 인터페이스부, 매체 인터페이스부 및 데이터 처리부를 가지고, 매체 인터페이스부에 장착된 기억매체에 소정의 정보를 저장하는 데이터 처리장치이며,

상기 데이터 처리부는, 복호열쇠의 수령 요구와 함께 기억매체가 보유하는 증명정보를 호스트 인터페이스부로부터 외부에 출력하고, 이것에 응답해서 호스트 인터페이스부에 돌아가는 정보를 수령하고, 이것에 기초하여 매체 인터페이스부에서 상기 기억매체에, 상기 소정의 정보로서 이용정보를 복호하기 위한 복호열쇠와 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장하고,

상기 제한 정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 억세스 시간정보의 초기값은 상기 수령한 정보에 포함되는 시간정보이며,

상기 증명정보는 특정한 기억매체인 것을 나타내는 정보이며,

상기 특정의 기억매체는, 제어 회로와 불휘발성 기억회로를 가지고,

상기 불휘발성 기억회로는 상기 제한정보의 저장 영역을 가지고,

상기 제어 회로는 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱 신 하는 억세스 판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타내는 억세스 기한보다도 뒤이거나 또는 상기 시각정보가 상기 억세스 시간정보에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고, 상기 제어 회로에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행하는 것을 특징으로 하는 데이터 처리장치.

청구항 30.

매체 인터페이스부 및 데이터 처리부를 가지고, 매체 인터페이스부에 장착된 기억매체에 소정의 정보를 저장하는 데이터 처리장치이며,

상기 데이터 처리부는 복호열쇠의 발행 요구에 응답해서 기억매체로부터 증명정보를 취득하고, 기억매체를 인증한 후에, 매체 인터페이스부로부터 기억매체에 상기 소정의 정보로서 이용정보를 복호하기 위한 복호열쇠와 이용정보에 대한 억세스 제한을 행하는 제한정보를 저장하고,

상기 제한정보에는 억세스 기한정보와 억세스 시간정보가 포함되고,

상기 억세스 시간정보의 초기값은 소정에 시간정보이며,

상기 증명정보는 특정한 기억매체인 것을 나타내는 정보이며,

상기 특정의 기억매체는 제어 회로와 불휘발성 기억회로를 가지고,

상기 불휘발성 기억회로는 상기 제한정보의 저장 영역을 가지고,

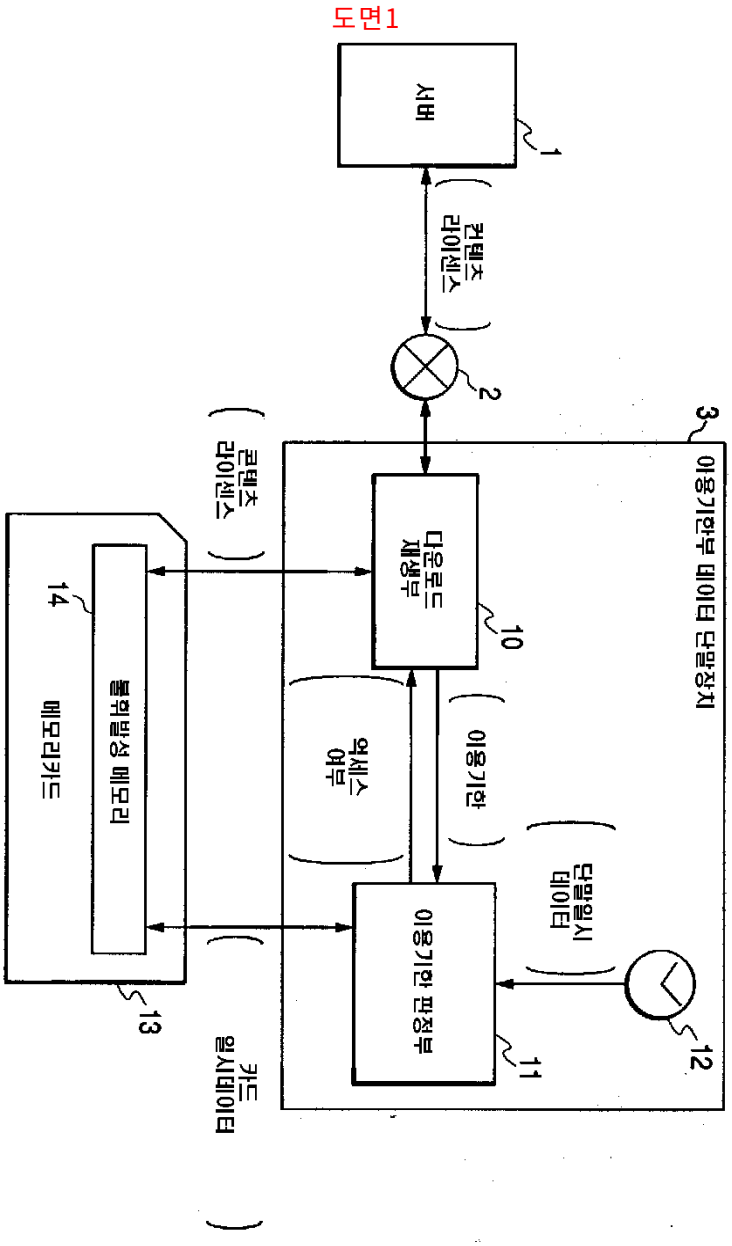
상기 제어 회로는, 외부로부터 공급되는 시각정보와 상기 제한정보에 기초해서 상기 이용정보의 억세스 가부를 판정하고, 상기 시각정보에 근거해서 상기 억세스 시간정보를 갱신하는 억세스 판정 동작을 행하고,

상기 억세스 가부의 판정에 있어서 상기 시각정보가 억세스 기한정보에 의해 나타나는 억세스 기한보다도 뒤지거나 또는 상기 시각정보가 상기 억세스 시간정보 에 의해 나타나는 억세스 시간보다도 이전인 경우에 억세스불가라고 판정하고, 그 밖의 경우를 억세스 가능이라고 판정하고,

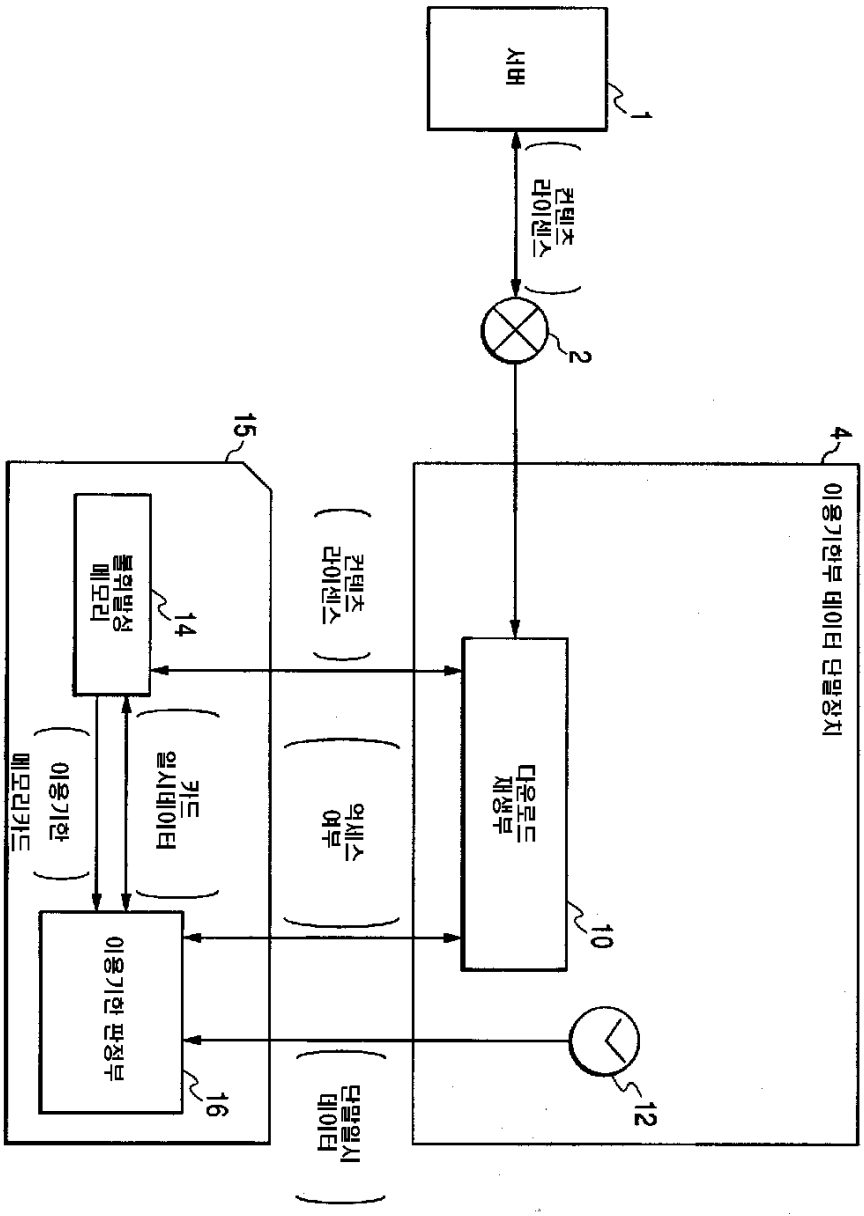
상기 제어 회로에 의한 억세스 판정 동작을 적어도 상기 이용정보에 대한 억세스 개시시와 억세스 종료시에 행하는 것을 특징으로 하는 데이터 처리장치.

도면

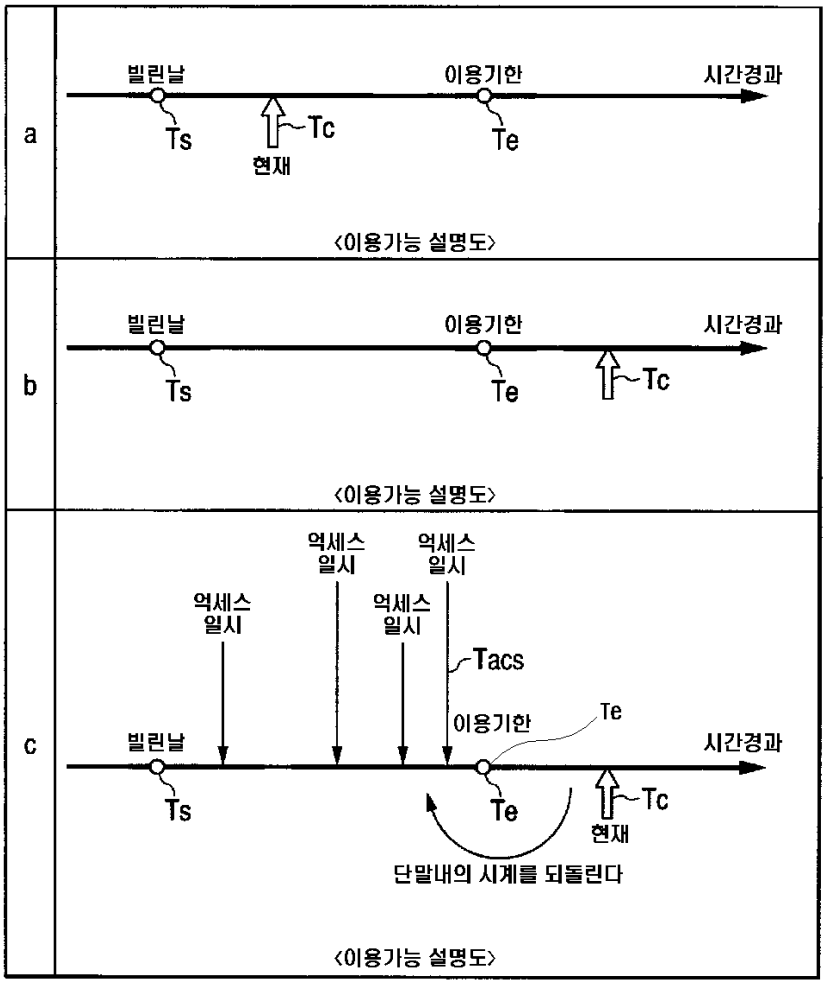
도면1


서버
1
컬렉조 라이센스
2
3
이용기한부 데이터 다운장치
다운로드 제어부
10
이용기한
엑세스 여부
이용기한 판정부
11
단말기시 데이터
12
콜렉조 라이센스
14
메모리카드
플래쉬 메모리
13
카드 일시데이터

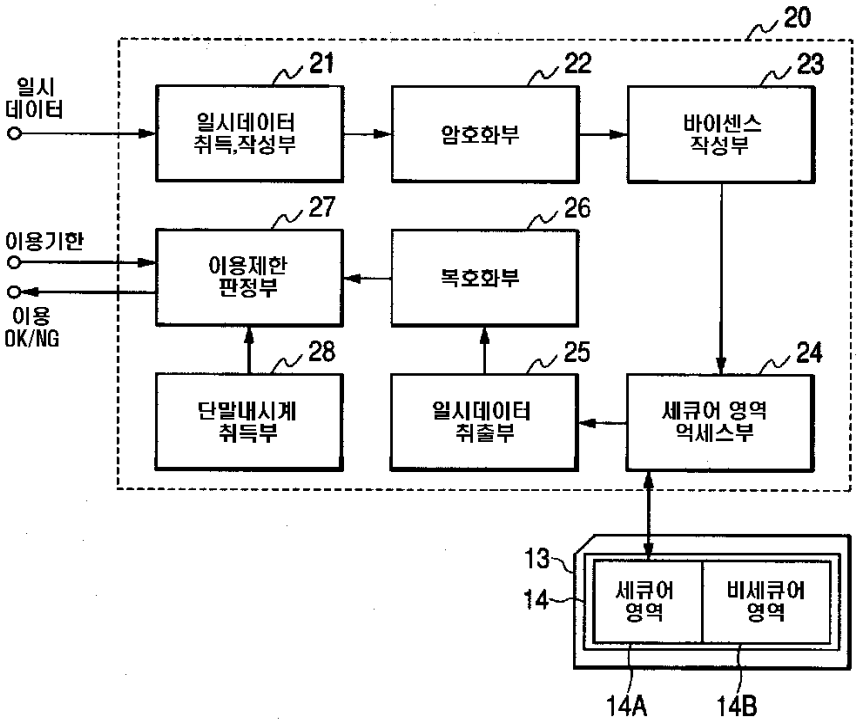
도면2


서버
1
컨텍스 라이센스
2
이용기한부 데이터 단말장치
4
다운로드 재생부
10
12
컨텍스 라이센스
억세스
다운로드 시 데이터
메모리카드
15
플래쉬 메모리
14
이용기한
키 데이터
이용기한 표현부
16

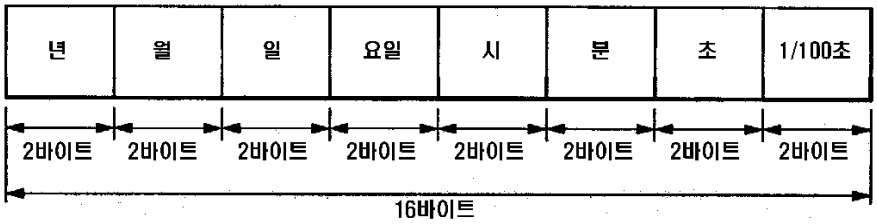
도면3


a
빌린날
이용기한
시간경과
Ts
Tc
현재
Te
〈이용가능 설명도〉
b
빌린날
이용기한
시간경과
Ts
Te
Tc
〈이용가능 설명도〉
c
억세스 일시
억세스 일시
억세스 일시
억세스 일시
Tacs
빌린날
이용기한
Te
시간경과
Ts
Te
Tc
현재
단말내의 시계를 되돌린다
〈이용가능 설명도〉

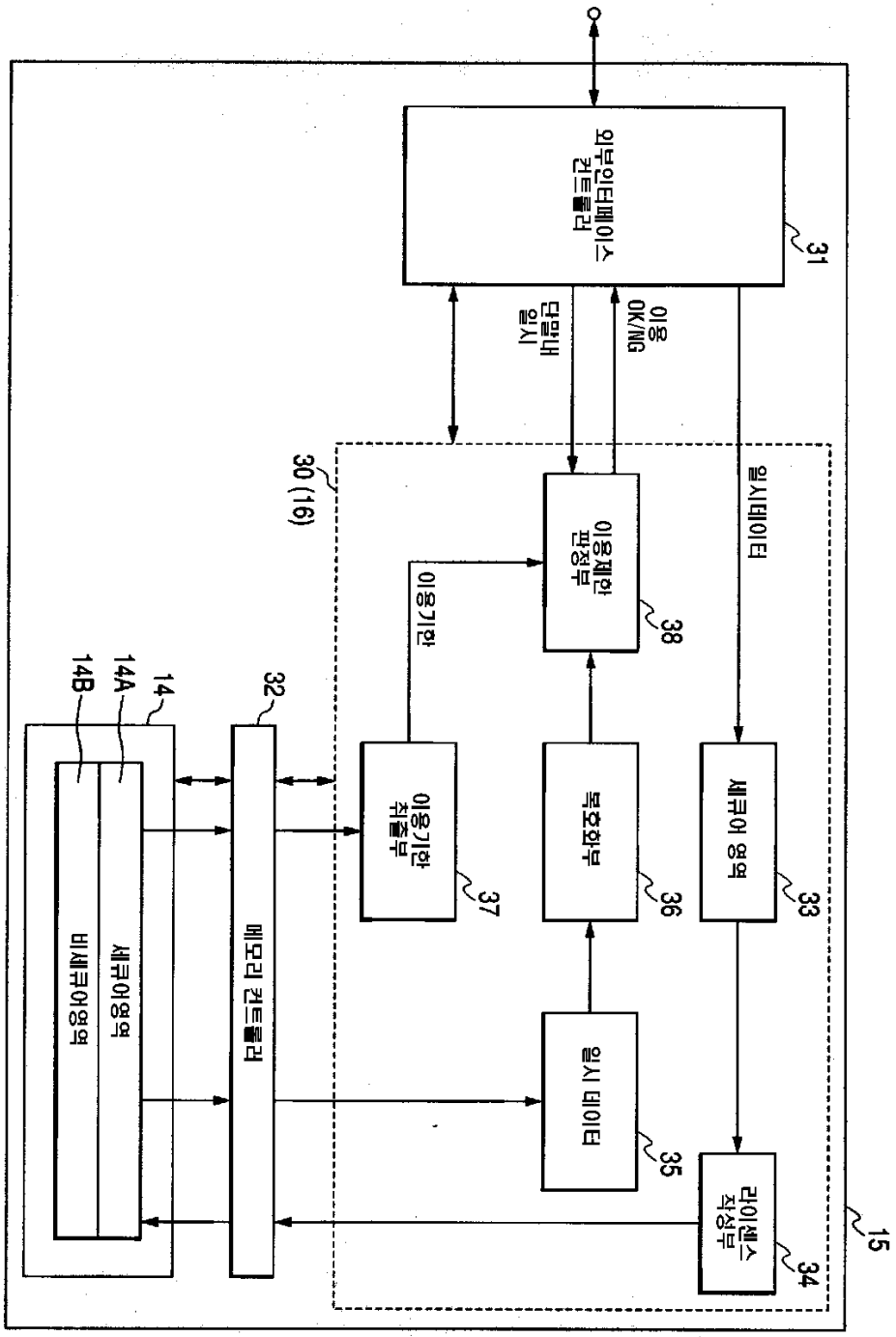
도면4


20
21
22
23
일시 데이터
일시데이터 취득,작성부
암호화부
바이센스 작성부
27
26
이용기한
이용제한 판정부
복호화부
이용 OK/NG
28
25
24
단말내시계 취득부
일시데이터 취출부
세큐어 영역 억세스부
13
14
세큐어 영역
비세큐어 영역
14A
14B

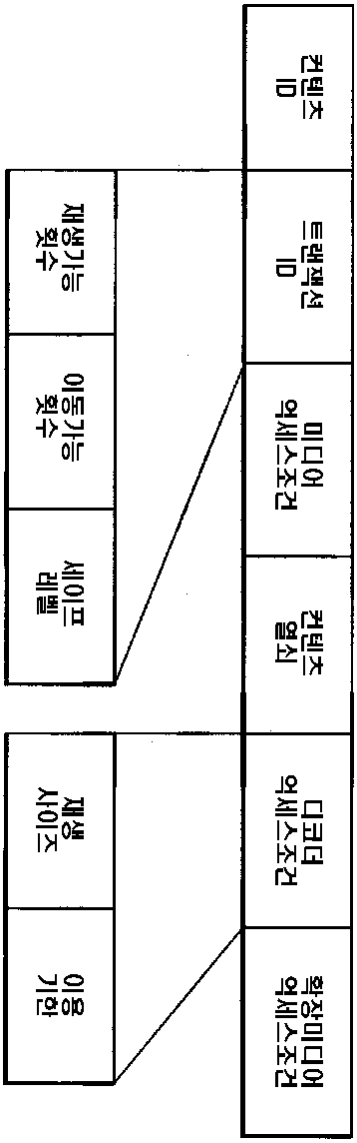
도면5


년
월
일
요일
시
분
초
1/100초
2바이트
2바이트
2바이트
2바이트
2바이트
2바이트
2바이트
2바이트
16바이트

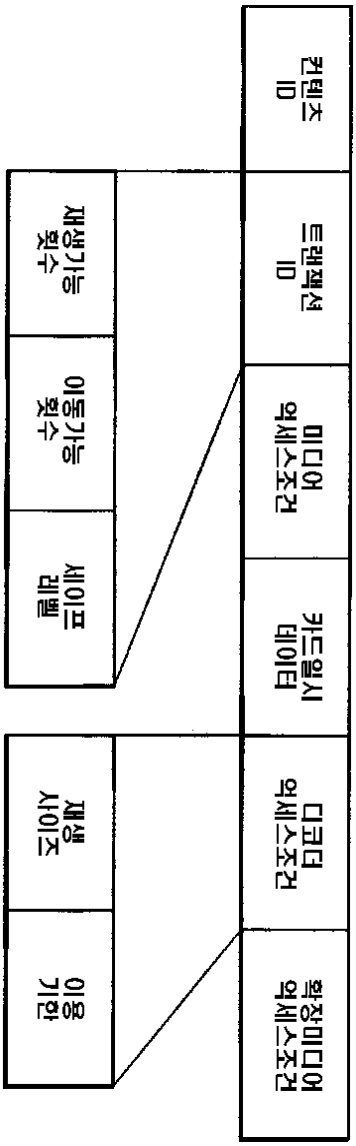
도면6


외부인터페이스 컨트롤러
31
이용 OK/NG
업데이트 요청
일시데이터
30 (16)
이용제한 관리부
38
이용기한
32
14
14B
14A
이용기한 처리부
37
복호화부
36
세큐어 영역
33
메모리 컨트롤러
비세큐어영역
세큐어영역
일시 데이터
35
라이센스 처리부
34
15

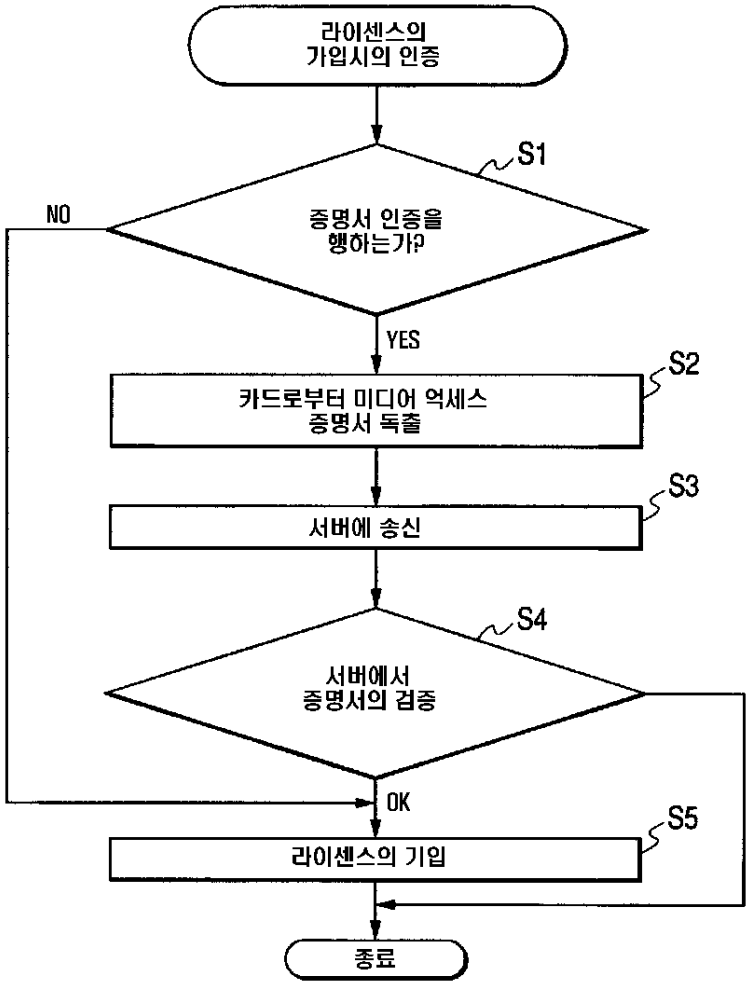
도면7


컨텐츠 ID
트랜잭션 ID
미디어 억세스조건
컨텐츠 열쇠
디코더 억세스조건
확장미디어 억세스조건
재생기능 횟수
이동가능 횟수
세이프 레벨
재생 사이즈
이용 기한

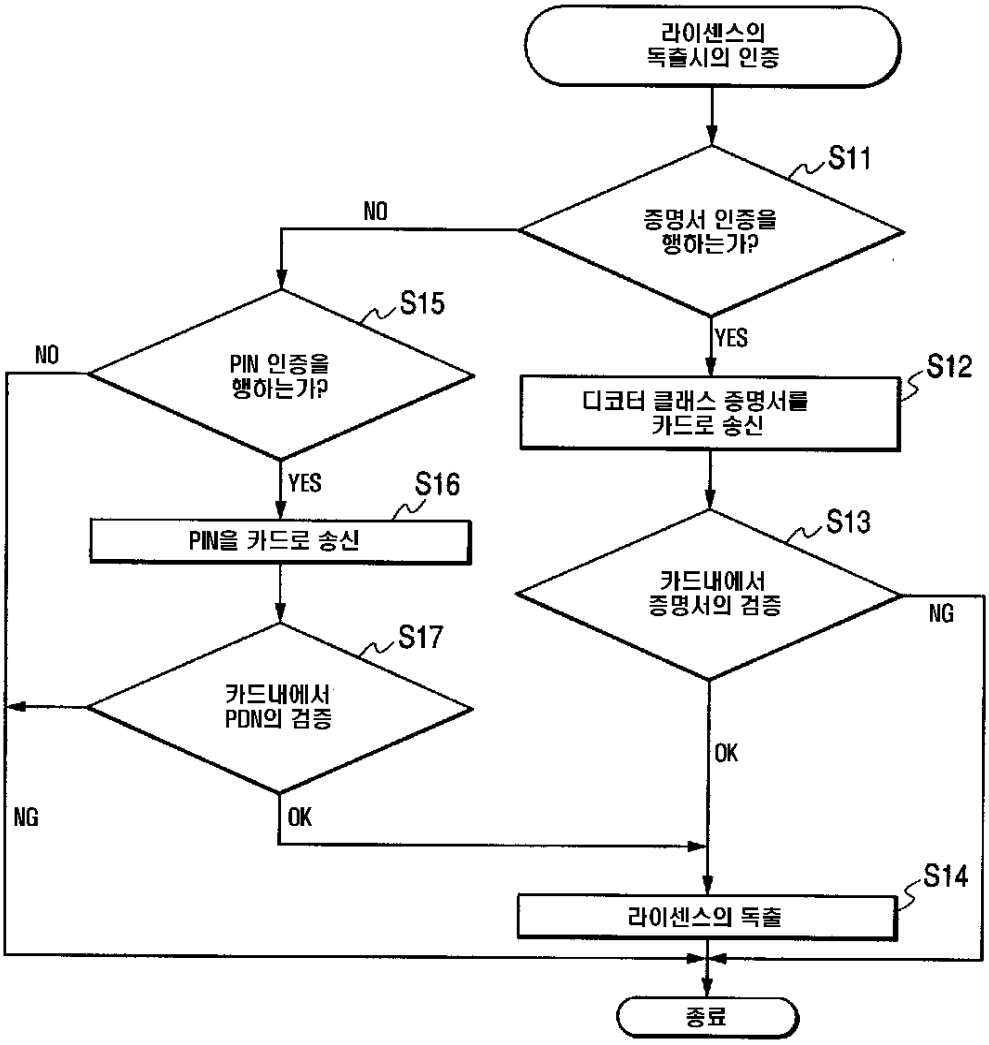
도면8


컨텐츠 ID
트랙젝션 ID
미디어 액세스조건
카드일시 데이터
디코더 액세스조건
확장미디어 액세스조건
재생가능 횟수
이동가능 횟수
세이프 레벨
재생 사이즈
이용 기한

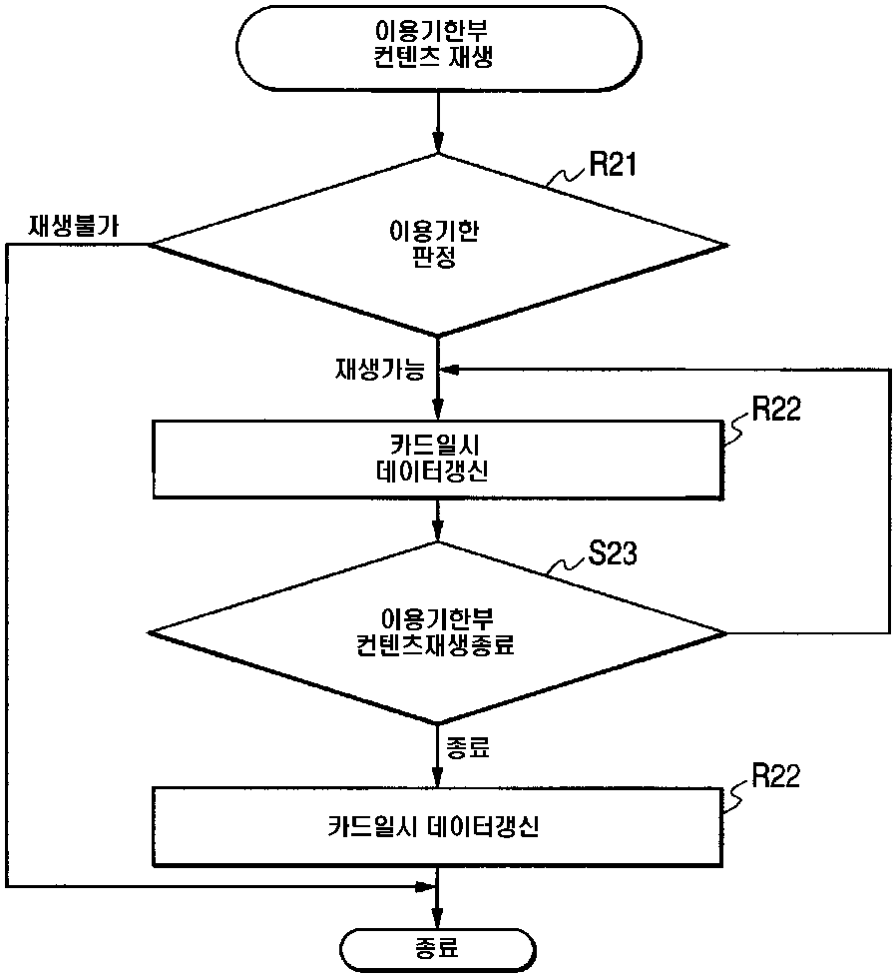
도면9


라이센스의
가입시의 인증
S1
증명서 인증을
행하는가?
NO
YES
S2
카드로부터 미디어 억세스
증명서 독출
S3
서버에 송신
S4
서버에서
증명서의 검증
OK
S5
라이센스의 기입
종료

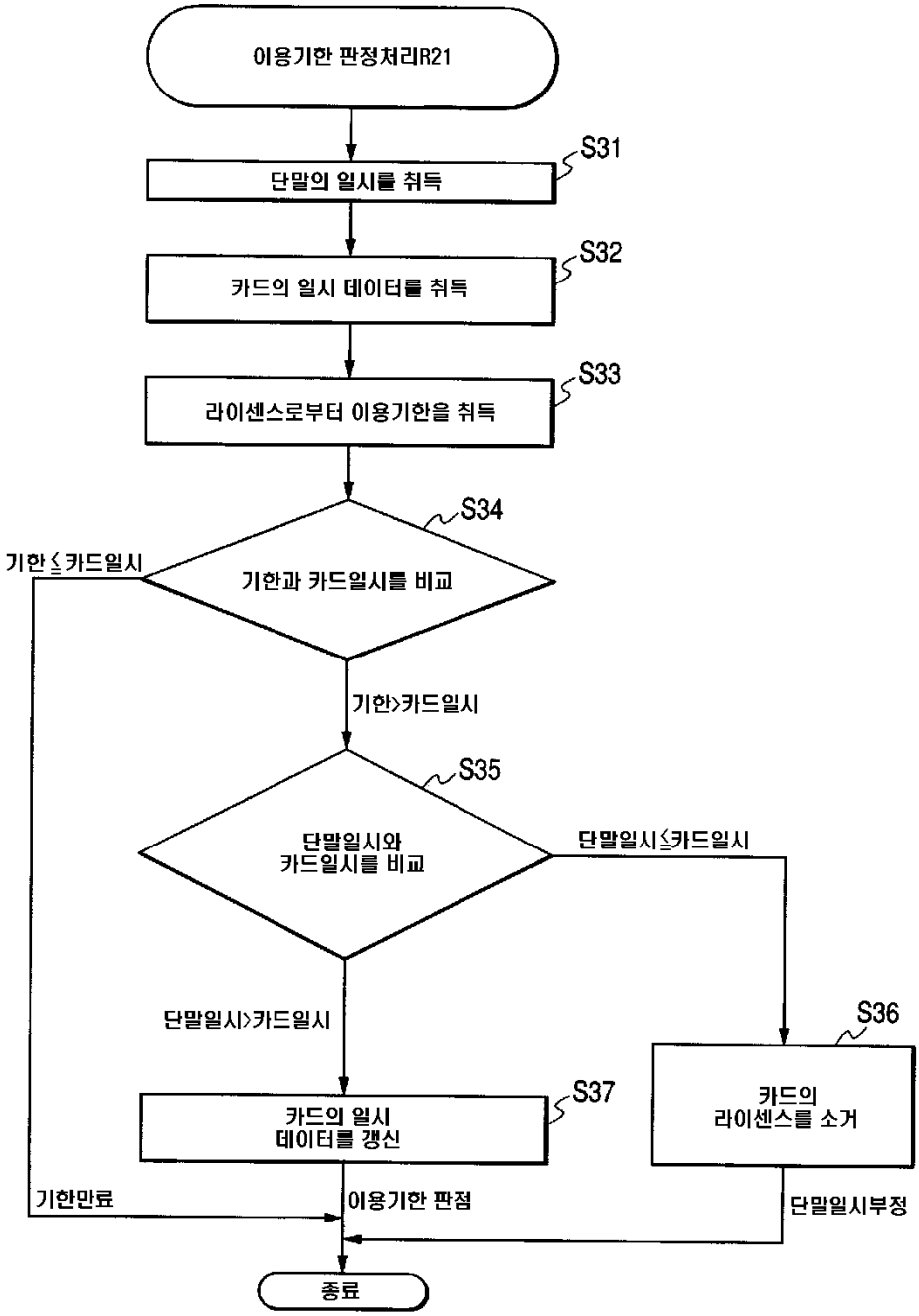
도면10


라이센스의
독출시의 인증
S11
증명서 인증을
행하는가?
NO
YES
S15
PIN 인증을
행하는가?
NO
YES
S16
PIN을 카드로 송신
S17
카드내에서
PDN의 검증
NG
OK
S12
디코터 클래스 증명서를
카드로 송신
S13
카드내에서
증명서의 검증
NG
OK
S14
라이센스의 독출
종료

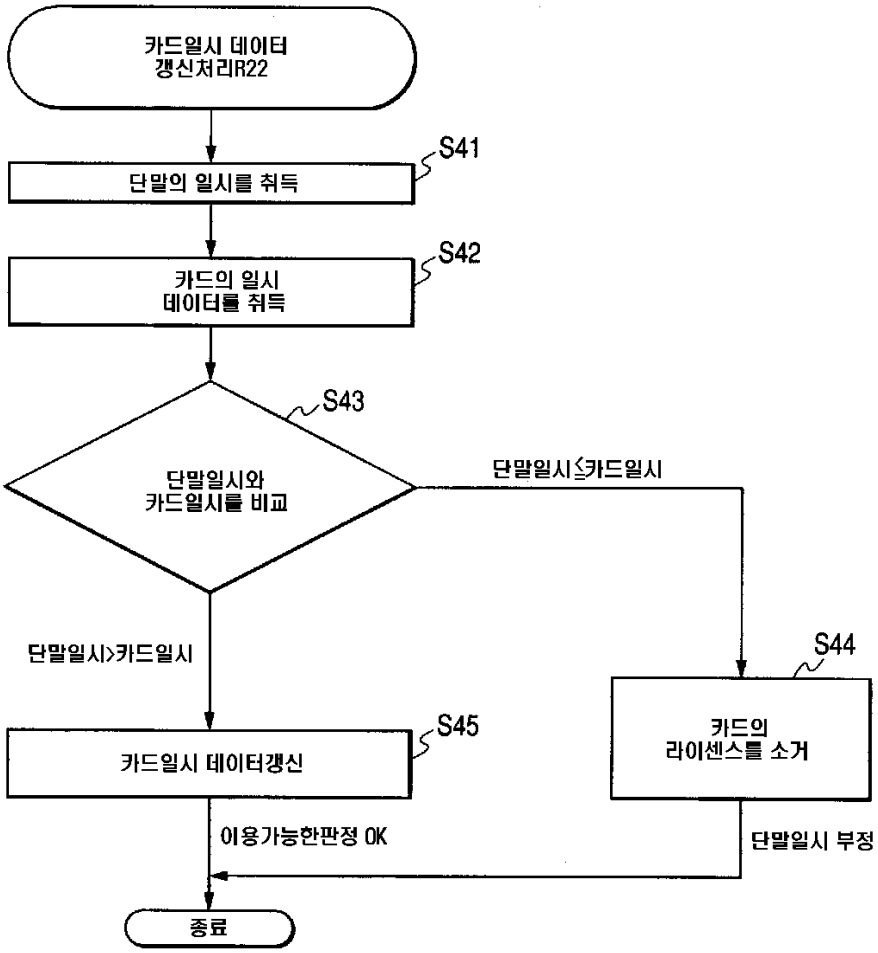
도면11


이용기한부
컨텐츠 재생
R21
재생불가
이용기한
판정
재생가능
R22
카드일시
데이터갱신
S23
이용기한부
컨텐츠재생종료
종료
R22
카드일시 데이터갱신
종료

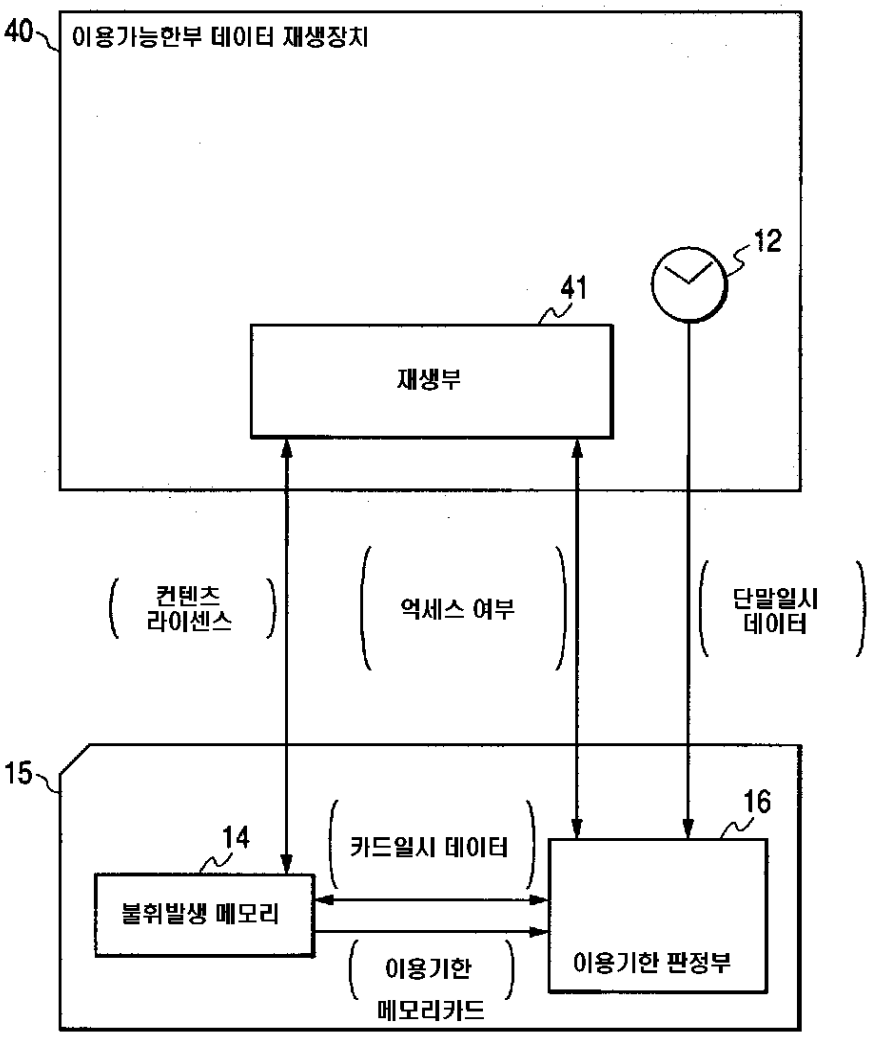
도면12


이용기한 판정처리R21
S31
단말의 일시를 취득
S32
카드의 일시 데이터를 취득
S33
라이센스로부터 이용기한을 취득
S34
기한과 카드일시를 비교
기한≦카드일시
기한>카드일시
S35
단말일시와
카드일시를 비교
단말일시≦카드일시
단말일시>카드일시
S36
카드의
라이센스를 소거
S37
카드의 일시
데이터를 갱신
기한만료
이용기한 판정
단말일시부정
종료

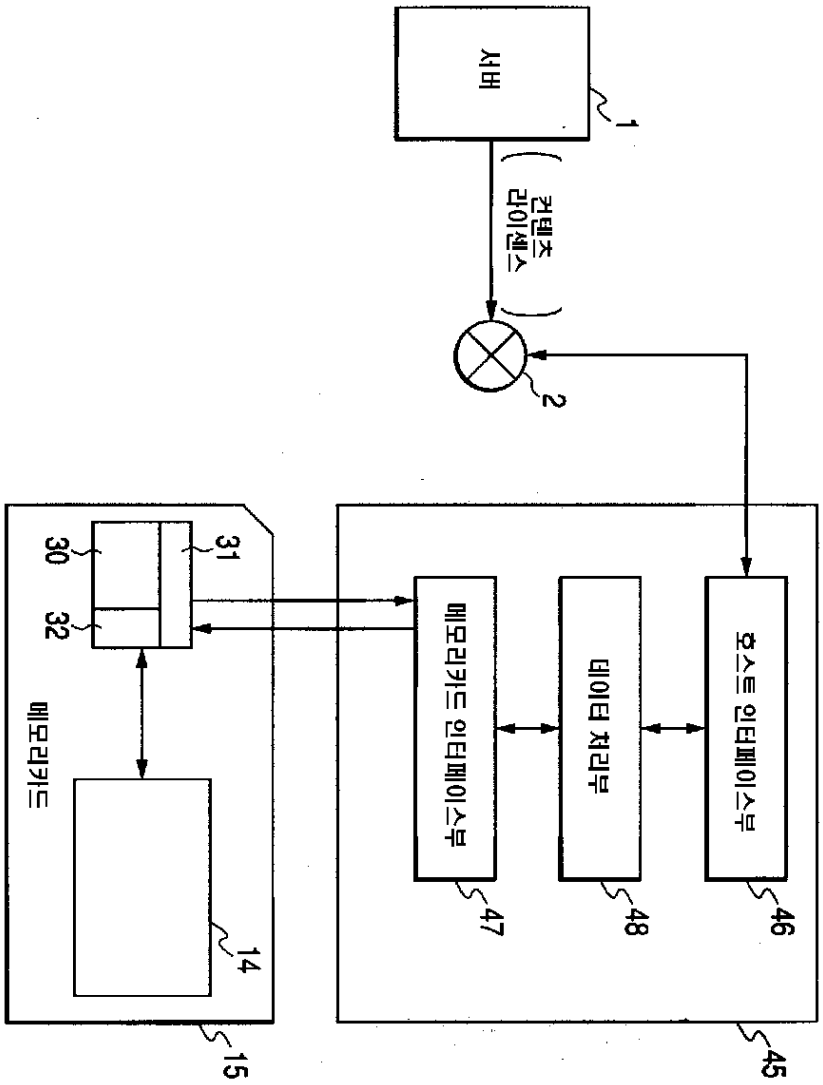
도면13


카드일시 데이터
갱신처리R22
S41
단말의 일시를 취득
S42
카드의 일시
데이터를 취득
S43
단말일시와
카드일시를 비교
단말일시≦카드일시
단말일시>카드일시
S44
카드의
라이센스를 소거
S45
카드일시 데이터갱신
이용가능한판정 OK
단말일시 부정
종료

도면14


40
이용가능한부 데이터 재생장치
12
41
재생부
컨텐츠
라이센스
억세스 여부
단말일시
데이터
15
16
14
카드일시 데이터
불휘발생 메모리
이용기한 판정부
이용기한
메모리카드

도면15


서버
1
컨텐츠
라이센스
2
30
31
32
메모리카드
14
15
메모리카드 인터페이스부
47
데이터 처리부
48
호스트 인터페이스부
46
45