(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3815950号
(P3815950)
(45)発行日　平成18年8月30日(2006.8.30)　(24)登録日　平成18年6月16日(2006.6.16)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　H04L 9/00 601D
H04L 9/32 (2006.01)　H04L 9/00 673E

請求項の数 12　(全 28 頁)

(21)出願番号　特願2000-148962(P2000-148962)
(22)出願日　平成12年5月19日(2000.5.19)
(65)公開番号　特開2001-60945(P2001-60945A)
(43)公開日　平成13年3月6日(2001.3.6)
審査請求日　平成14年3月8日(2002.3.8)
審判番号　不服2002-22622(P2002-22622/J1)
審判請求日　平成14年11月21日(2002.11.21)
(31)優先権主張番号　特願平11-167897
(32)優先日　平成11年6月15日(1999.6.15)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　小野　貴敏
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内
(72)発明者　原田　俊治
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】デジタルデータ書込装置、デジタルデータ記録装置、デジタルデータ利用装置

(57)【特許請求の範囲】
【請求項１】
デジタルデータの利用を制限し、かつ更新されることにより価値が変化する情報を含む制限情報と、当該デジタルデータが暗号化された暗号化デジタルデータの復号処理を特定する復号情報とを含む管理情報に、メモリカード毎に固有の値であるカードＩＤにより特定される復号処理を施すことにより復号できるように暗号化された暗号化管理情報、及び、当該暗号化デジタルデータを記録するための半導体メモリと、その制御回路とを備えるインテリジェントなメモリカードであって、
前記半導体メモリは、
前記カードＩＤを保持しているカードＩＤ保持手段と、
前記制限情報として第１制限情報を含み、かつ、前記復号情報として第１復号情報を含む第１管理情報に、前記カードＩＤ保持手段に保持しているカードＩＤに対応する暗号処理が施された第１暗号化管理情報を記録している暗号化管理情報記録手段と、
前記第１復号情報により特定される復号処理により復号できるようにデジタルデータが暗号化された第１暗号化デジタルデータを記録している暗号化デジタルデータ記録手段とを含み、
前記制御回路は、
カードＩＤ保持手段に保持しているカードＩＤを、メモリカード利用装置に送信するカードＩＤ送信手段と、
送信処理の度に異なる第１鍵情報を取得し、受信処理の度に異なる第２鍵情報を取得す

る鍵情報取得手段と、
暗号化管理情報記録手段に記録している第１暗号化管理情報に、鍵情報取得手段により取得された第１鍵情報により特定されるデータ変換を施して、第１変換管理情報を生成するデータ変換手段と、
暗号化デジタルデータ記録手段に記録している第１暗号化デジタルデータに前記データ変換を施すことなくそのまま、データ変換手段により生成された第１変換管理情報と、当該第１暗号化デジタルデータとをセットで、前記メモリカード利用装置に利用に供するために送信するデータ送信手段と、
鍵情報取得手段により取得された第２鍵情報により特定される逆データ変換を施すことにより第２暗号化管理情報に復元できるように、前記メモリカード利用装置においてデータ変換されて生成される第２変換管理情報を、当該メモリカード利用装置から受信する受信手段とを含み、
前記第２暗号化管理情報は、前記制限情報として第２制限情報を含む第２管理情報に前記カードＩＤ保持手段に保持しているカードＩＤに対応する暗号処理が施されたものであり、
前記第２制限情報は、前記メモリカード利用装置により、前記第１制限情報が更新されたものであり、
前記制御回路は、さらに、
受信手段により受信された第２変換管理情報に、前記逆データ変換を施して、第２暗号化管理情報を復元する逆データ変換手段を含み、
前記暗号化管理情報記録手段は、さらに、
逆データ変換手段により復元された第２暗号化管理情報を記録すること
を特徴とするメモリカード。
【請求項２】
前記第２管理情報は、さらに、
前記復号情報として第２復号情報を含み、
前記受信手段は、
前記第２変換管理情報と、前記第２復号情報により特定される復号処理により復号できるように暗号化された第２暗号化デジタルデータとをセットで、前記メモリカード利用装置から受信し、
前記暗号化デジタルデータ記録手段は、
受信手段により受信された第２暗号化デジタルデータを、前記逆データ変換を施すことなくそのまま記録すること
を特徴とする請求項１に記載のメモリカード。
【請求項３】
前記第１復号情報と、前記第２復号情報とは、同一であること
を特徴とする請求項２に記載のメモリカード。
【請求項４】
前記鍵情報取得手段は、
取得する第１鍵情報及び第２鍵情報を、前記メモリカード利用装置と共有し、
前記データ変換手段は、
前記第１鍵情報を共有鍵暗号方式の共有鍵として用いて前記第１暗号化管理情報を暗号化して、前記第１変換管理情報を生成し、
前記逆データ変換手段は、
前記第２鍵情報を共有鍵暗号方式の共有鍵として用いて前記第２変換管理情報を復号して、前記第２暗号化管理情報を復元すること
を特徴とする請求項１に記載のメモリカード。
【請求項５】
前記鍵情報取得手段は、
取得する第１鍵情報及び第２鍵情報を前記メモリカード利用装置と共有するに際し、第

１鍵情報及び第２鍵情報そのものは送受信せずに、第１鍵情報及び第２鍵情報とは異なるデータをやりとりして、やりとりした結果得られた当該メモリカード利用装置と共有するデータに、予め当該メモリカード利用装置と共有する秘密のデータ変換を施して、第１鍵情報及び第２鍵情報を生成すること
を特徴とする請求項４に記載のメモリカード。
【請求項６】
前記鍵情報取得手段は、
取得する第１鍵情報及び第２鍵情報を前記メモリカード利用装置と共有するに際し、第１鍵情報及び第２鍵情報そのものは送受信せずに、当該メモリカード利用装置と共有する時刻に基づくデータに、予め当該メモリカード利用装置と共有する秘密のデータ変換を施して、第１鍵情報及び第２鍵情報を生成すること
を特徴とする請求項４に記載のメモリカード。
【請求項７】
前記半導体メモリは、さらに、
受信処理及び送信処理の度に取得される最新の第１鍵情報又は第２鍵情報を記録する鍵情報記録手段を含み、
前記鍵情報取得手段は、
鍵情報記録手段に記録された最新の第１鍵情報又は第２鍵情報に、予め定めた所定の変換を施して、第１鍵情報又は第２鍵情報を更新すること
を特徴とする請求項４に記載のメモリカード。
【請求項８】
前記鍵情報取得手段は、
鍵情報記録手段に記録された最新の第１鍵情報又は第２鍵情報に、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施して、第１鍵情報又は第２鍵情報を更新すること
を特徴とする請求項７に記載のメモリカード。
【請求項９】
前記データ変換手段は、
前記第１暗号化管理情報と、前記第１鍵情報とを排他的論理和して、前記第１変換管理情報を生成し、
前記逆データ変換手段は、
前記第２変換管理情報と、前記第２鍵情報とを排他的論理和して、前記第２暗号化管理情報を復元すること
を特徴とする請求項４に記載のメモリカード。
【請求項１０】
前記鍵情報取得手段は、
取得する第１鍵情報を、公開鍵暗号方式の公開鍵として取得し、当該公開鍵に対応する秘密鍵を前記メモリカード利用装置が取得し、
前記データ変換手段は、
前記第１鍵情報を公開鍵暗号方式の公開鍵として用いて、前記第１暗号化管理情報を暗号化して、前記変換管理情報を生成し、
前記鍵情報取得手段は、さらに、
取得する第２鍵情報を、公開鍵暗号方式の秘密鍵として取得し、当該秘密鍵に対応する公開鍵を前記メモリカード利用装置が取得し、
前記逆データ変換手段は、
前記第２鍵情報を公開鍵暗号方式の秘密鍵として用いて、前記第２変換管理情報を復号して、前記第２暗号化管理情報を復元すること
を特徴とする請求項１に記載のメモリカード。
【請求項１１】
前記鍵情報取得手段は、

取得する第１鍵情報を、回復型署名方式の秘密鍵として取得し、当該秘密鍵に対応する公開鍵を前記メモリカード利用装置が取得し、
前記データ変換手段は、
前記第１鍵情報を回復型署名方式の秘密鍵として用いて、前記第１暗号化管理情報を暗号化し、
前記鍵情報取得手段は、さらに、
取得する第２鍵情報を、回復型署名方式の公開鍵として取得し、当該公開鍵に対応する秘密鍵を前記メモリカード利用装置が取得し、
前記逆データ変換手段は、
前記第２鍵情報を回復型署名方式の公開鍵として用いて、前記第２変換管理情報を復号すること
を特徴とする請求項１に記載のメモリカード。
【請求項１２】
前記データ変換手段は、
データ変換の度に異なる乱数を生成し、前記第１暗号化管理情報の所定位置に、生成した乱数を付加した後で、前記データ変換を施し、
前記受信手段が受信する第２変換管理情報は、データ変換を施すべき第２暗号化管理情報の所定位置に乱数を付加した後、前記データ変換を施してあり、
前記逆データ変換手段は、
前記第２変換管理情報に、前記逆データ変換を施した後、前記所定位置の乱数を削除して、前記第２暗号化管理情報を復元すること
を特徴とする請求項１に記載のメモリカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、デジタルデータを記録し利用する装置に関し、特に、デジタルデータの不正使用を防止する技術に関する。
【０００２】
【従来の技術】
近年、情報のデジタル化が進んでいる。デジタル化された情報（以下「デジタルコンテンツ」と言う）は時間とともに劣化することがなく、また比較的取り扱い易いので、特に音声情報や画像情報のデジタル化が著しく進んでいる。
【０００３】
【発明が解決しようとする課題】
しかしデジタルコンテンツはコピーしてもオリジナルと全く同じものができるので、著作権のある情報が無断で複製されたり、改ざんされたりといった不正行為が簡易に行なわれてしまうという欠点を持っている。
このような不正行為を防ぐために、例えば記録媒体であるメモリカードにそれぞれユニークな番号（以下「カードＩＤ」と言う）を持たせ、自身のカードＩＤを用いて暗号化されたデジタルコンテンツ（以下「暗号化コンテンツ」と言う）を記録する方法が考えられる。
【０００４】
このようにすると、メモリカードに記録された暗号化コンテンツを他のメモリカードにコピーしたとしても、他のメモリカードはカードＩＤが異なり暗号化コンテンツを復号できないので不正行為が成立しない。
また、暗号化コンテンツに、利用回数や利用条件等の様な利用を制限する制限情報を添付することがある。
【０００５】
ここで暗号化コンテンツと同様に、制限情報もカードＩＤを用いて暗号化して記録しておけば、他のメモリカードにコピーするという不正行為は成立しない。

しかしながら、利用回数のように時間の経過に伴なって情報の価値が変化する情報が制限情報に含まれる場合には、たとえ制限情報をカードＩＤを用いて暗号化したとしても、利用側において、価値が高い時に受け取った制限情報をバックアップして以後の利用の際にこれに置き換えるというような不正行為が成立する。

【０００６】

そこで、本発明はかかる問題点に鑑みてなされたものであり、制限情報をバックアップして以後の利用の際に置き換えるような不正行為が成立しないデジタルデータ書込装置、デジタルデータ記録装置、デジタルデータ利用装置、それらの方法、及び、それらをコンピュータに実行させるプログラムを記録する記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記目的を達成するために、本発明に係るデジタルデータ記録装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ利用装置に利用に供するために送信するデジタルデータ記録装置であって、前記管理情報を記録している管理情報記録手段と、前記デジタルデータを記録しているデジタルデータ記録手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、管理情報記録手段に記録している管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、データ変換手段により生成された変換管理情報とデジタルデータ記録手段に記録しているデジタルデータとをセットで前記デジタルデータ利用装置に送信する送信手段とを備えることを特徴とする。

【０００８】

上記目的を達成するために、本発明に係るデジタルデータ記録装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ書込装置から受信して記録するデジタルデータ記録装置であって、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記管理情報に復元できるように前記デジタルデータ書込装置においてデータ変換された変換管理情報と前記デジタルデータとをセットで当該デジタルデータ書込装置から受信する受信手段と、受信手段により受信された変換管理情報に前記逆データ変換を施して管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された管理情報を記録する管理情報記録手段と、受信手段により受信されたデジタルデータを記録するデジタルデータ記録手段とを備えることを特徴とする。

【０００９】

上記目的を達成するために、本発明に係るデジタルデータ利用装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置から受信して利用するデジタルデータ利用装置であって、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記管理情報に復元できるように前記デジタルデータ記録装置においてデータ変換された変換管理情報と前記デジタルデータとをセットで当該デジタルデータ記録装置から受信する受信手段と、受信手段により受信された変換管理情報に前記逆データ変換を施して管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された管理情報に含まれる情報が示すデジタルデータの利用の制限に従い受信手段により受信されたデジタルデータを利用する利用手段とを備えることを特徴とする。

【００１０】

上記目的を達成するために、本発明に係るデジタルデータ書込装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置に送信して記録させるデジタルデータ書込装置であって、前記管理情報を入手する管理情報入手手段と、前記デジタルデータを入手するデジタルデータ入手手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、管理情報入手手段により入手された管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、データ変換手段により生成された変換管理情報とデジ

タルデータ入手手段により入手されたデジタルデータとをセットで前記デジタルデータ記録装置に送信する送信手段とを備えることを特徴とする。

【００１１】

【発明の実施の形態】

＜概要＞

本実施の形態は、デジタルコンテンツをレコーダからメモリカードへ書込む際には、まずメモリカードからレコーダへカードＩＤを伝送し、レコーダとメモリカードとで共有鍵を持ち合う。続いてレコーダは、制限情報とコンテンツ鍵とを含む管理情報を、受信したカードＩＤを鍵として暗号化して暗号化管理情報とした後、さらに、共有鍵を用いてデータ変換を施して変換管理情報を生成し、また管理情報に含まれるコンテンツ鍵を用いてデジタルコンテンツを暗号化して暗号化コンテンツを生成し、変換管理情報と暗号化コンテンツとをメモリカードへ送信する。ここでメモリカードが、受信した変換管理情報を共有鍵を用いてデータ変換とは逆のデータ変換を施して暗号化管理情報として記録し、受信した暗号化コンテンツをそのまま記録する。

【００１２】

また、デジタルコンテンツをメモリカードからプレーヤへ送信する際には、まずメモリカードからプレーヤへカードＩＤを伝送し、メモリカードとプレーヤとで共有鍵を持ち合う。続いてメモリカードは、記録している暗号化管理情報を共有鍵を用いてデータ変換を施して変換管理情報を生成し、変換管理情報と記録している暗号化コンテンツとをプレーヤへ送信する。ここでプレーヤは、受信した変換管理情報を共有鍵を用いてデータ変換とは逆のデータ変換を施して暗号化管理情報とした後、さらに、受信したカードＩＤを鍵として復号して管理情報を得る。そして、管理情報に含まれる制限情報によるデジタルコンテンツに関する利用等の制限に従いつつ、受信した暗号化コンテンツを管理情報に含まれるコンテンツ鍵を用いて復号してデジタルコンテンツを得る。

【００１３】

このように、制限情報を含む管理情報を、管理情報の送受信の度に異なる共有鍵を用いてデータ変換を施すことで、管理情報をバックアップして以後の利用の際に置き換えるような不正行為ができないようにしている。

＜構成＞

図１は、本実施の形態に係るレコーダ、メモリカード、及び、プレーヤの構成を示す図である。

【００１４】

図１に示すように本実施の形態は、レコーダ１００、メモリカード１２０、及び、プレーヤ１４０からなる。なお、レコーダ１００とプレーヤ１４０とが一体となった構成や、メモリカード１２０から書き込み機能を削除して、各記録部と再生機能とだけからなる再生専用の製品形態も一般的である。

レコーダ１００は、音楽情報等のデジタルコンテンツとその管理情報を他の外部機器等から入手して、不正行為を防ぐために暗号化等を施してメモリカード１２０に送信するものであって、カードＩＤ受信部１０１、セッション鍵共有部１０２、管理情報入手部１０３、管理情報処理部１０４、コンテンツ入手部１０５、コンテンツ暗号化部１０６、及び、暗号化コンテンツ送信部１０７を備える。

【００１５】

カードＩＤ受信部１０１は、メモリカード１２０から送信されるカードＩＤを受信する。ここでは例として８バイトのカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を受信するものとする。

セッション鍵共有部１０２は、メモリカード１２０と乱数等をやり取りし、メモリカード１２０に暗号化コンテンツを記録させるセッション毎に異なるセッション鍵を生成する。ここではメモリカード１２０のセッション鍵共有部１２３でも同様にして同じセッション鍵が生成されるものとする。より具体的には、セッション鍵共有部１０２とセッション鍵共有部１２３とは、互いに８バイトの乱数を発生させてそれぞれ他方に送信し、双方がそ

れぞれ自身で発生した乱数と受信した乱数とにそれぞれ予め決められた秘密の一方向性変換を施してこれらを排他的論理和してセッション鍵を生成することにより、セッション鍵自体を送受信することなく同じセッション鍵を共有する。さらに双方はそれぞれ、受信した乱数に一方向性変換を施して送り返し、自身で発生した乱数に当該一方向性変換を施した値と送り返された値とを比較し、これらが一致する場合にのみ相手の機器が正規のものであると認識する。ここでは例としてセッション鍵共有部１０２が８バイトの乱数Ｘを発生させて送信し、乱数Ｙを受信して一方向性変換を施して“００１１３３７７８８ＣＣＥＥＦＦＨ”を生成して送り返し、発生させた乱数Ｘに一方向性変換を施して“０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０ＦＨ”を生成したとすると、送り返された値と比較して一致した場合に相手の機器が正規のものであると認識した後、これらを排他的論理和したデータ“０Ｆ１Ｅ３Ｃ７８８７Ｃ３Ｅ１Ｆ０Ｈ”に一方向性変換を施してセッション鍵を生成する。

【００１６】

管理情報入手部１０３は、制限情報とコンテンツ鍵とを含む管理情報を入手する。ここで制限情報とは、デジタルコンテンツの利用を制限する情報であり、例えばデジタルコンテンツを利用するたびにデクリメントされる利用回数情報や、利用できる地域や時間等を示す利用条件等である。ここでは例として８バイトのコンテンツ鍵“３３３３３３３３３３３３３３Ｈ”と８バイトの制限情報“０００００００００００００００ＡＨ”とからなる１６バイトの管理情報“３３３３３３３３３３３３３３３０００００００００００００ＡＨ”を入手するものとする。またコンテンツ鍵とは、デジタルコンテンツを暗号化する際に用いる暗号鍵である。

【００１７】

管理情報処理部１０４は、カードＩＤ受信部１０１により受信されたカードＩＤと、セッション鍵共有部１０２により生成されたセッション鍵とを用いて、管理情報入手部１０３により入手された管理情報に暗号化処理とデータ変換を施して送信する。

図２は、管理情報処理部１０４の詳細な構成を示す図である。

【００１８】

図２に示すように管理情報処理部１０４は、暗号化部１０８、データ変換部１０９、及び、送信部１１０を含む。

暗号化部１０８は、カードＩＤ受信部１０１により受信されたカードＩＤを暗号化鍵として用いて、所定のアルゴリズムにより、管理情報入手部１０３により入手された管理情報を暗号化して暗号化管理情報を生成する。ここで所定のアルゴリズムとは、例えばＤＥＳ暗号等の様な暗号化鍵によって特定される暗号処理を指す。

【００１９】

データ変換部１０９は、暗号化部１０８により生成された暗号化管理情報を、セッション鍵共有部１０２により生成されたセッション鍵を用いて所定のデータ変換を施して変換管理情報を生成する。ここで所定のデータ変換とは、セッション鍵によって特定される暗号処理を指し、ＤＥＳ暗号等の様な暗号処理であってもよいが、ここでは排他的論理和を施すこととする。

【００２０】

送信部１１０は、データ変換部１０９により生成された変換管理情報をメモリカード１２０へ送信する。

コンテンツ入手部１０５は、デジタルコンテンツを入手する。

コンテンツ暗号化部１０６は、コンテンツ入手部１０５により入手されたデジタルコンテンツを、管理情報入手部１０３により入手された管理情報に含まれるコンテンツ鍵を用いて、所定のブロック暗号処理を施し、暗号化コンテンツを生成する。ここでは例として、デジタルコンテンツを８バイトづつブロック単位に分割し、それぞれを、コンテンツ鍵“３３３３３３３３３３３３３３３Ｈ”を用いて暗号化を施して暗号化されたコンテンツのブロックを生成し、これらをつないで暗号化コンテンツを生成するものとする。

【００２１】

暗号化コンテンツ送信部１０７は、コンテンツ暗号化部１０６により生成された暗号化コ

ンテンツをメモリカード１２０へ送信する。
メモリカード１２０は、暗号化コンテンツと暗号化管理情報とを記録するための大容量の半導体メモリとその制御回路とを備えるインテリジェントな記録装置であって、カードＩＤ保持部１２１、カードＩＤ送信部１２２、セッション鍵共有部１２３、第１管理情報処理部１２４、暗号化管理情報保持部１２５、第２管理情報処理部１２６、暗号化コンテンツ受信部１２７、暗号化コンテンツ保持部１２８、及び、暗号化コンテンツ送信部１２９を備える。
【００２２】
カードＩＤ保持部１２１は、それぞれのカード毎に固有の値であるカードＩＤを保持する。
カードＩＤ送信部１２２は、カードＩＤ保持部１２１に保持されたカードＩＤを、レコーダ１００及びプレーヤ１４０に送信する。ここでは例として８バイトのカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を送信するものとする。
【００２３】
セッション鍵共有部１２３は、レコーダ１００と乱数等をやり取りし、メモリカード１２０に暗号化コンテンツを記録させるセッション毎に異なるセッション鍵を生成し、また、プレーヤ１４０と乱数等をやり取りし、メモリカード１２０に記録された暗号化コンテンツを利用するセッション毎に異なるセッション鍵を生成する。ここではレコーダ１００のセッション鍵共有部１０２、及び、プレーヤ１４０のセッション鍵共有部１４２でも同様にして、セッション鍵共有部１２３と同じセッション鍵が生成されるものとする。より具体的にはレコーダ１００のセッション鍵共有部１０２で説明したものと同様であるので説明を省略する。
【００２４】
第１管理情報処理部１２４は、レコーダ１００から送信される変換管理情報を受信し、セッション鍵共有部１２３によりレコーダ１００のセッション鍵共有部１０２とのやり取りの結果生成されたセッション鍵を用いてデータ変換部１０９におけるデータ変換とは逆のデータ変換を施して暗号化管理情報を生成する。
図３は、第１管理情報処理部１２４の詳細な構成を示す図である。
【００２５】
図３に示すように第１管理情報処理部１２４は、受信部１３０、及び、逆データ変換部１３１を含む。
受信部１３０は、レコーダ１００の送信部１１０より送信された変換管理情報を受信する。
逆データ変換部１３１は、受信部１３０により受信された変換管理情報を、セッション鍵共有部１２３により生成されたセッション鍵を用いて、レコーダ１００のデータ変換部１０９における所定のデータ変換とは逆のデータ変換を施して暗号化管理情報を生成する。例えばレコーダ１００のデータ変換部１０９において、セッション鍵を加算するデータ変換を行うときには第１管理情報処理部１２４はセッション鍵を減算するデータ変換を行う事になる。ここでは所定のデータ変換を排他的論理和を施すこととしたので、逆のデータ変換は排他的論理和を施すこととする。ちなみに、ある値に同じ値で２回、排他的論理和を施すと元の値に戻るので、排他的論理和の逆の変換は同じ排他的論理和である。
【００２６】
暗号化管理情報保持部１２５は、第１管理情報処理部１２４により生成された暗号化管理情報を内部の不揮発性メモリに保持する。
第２管理情報処理部１２６は、暗号化管理情報保持部１２５に保持された暗号化管理情報を、セッション鍵共有部１２３によりプレーヤ１４０のセッション鍵共有部１４２とのやり取りの結果生成されたセッション鍵を用いて所定のデータ変換を施して変換管理情報を生成して、プレーヤ１４０へ送信する。
【００２７】
図４は、第２管理情報処理部１２６の詳細な構成を示す図である。

図４に示すように第２管理情報処理部１２６は、データ変換部１３２、及び、送信部１３３を含む。
データ変換部１３２は、暗号化管理情報保持部１２５に保持された暗号化管理情報を、セッション鍵共有部１２３により生成されたセッション鍵を用いて所定のデータ変換を施して変換管理情報を生成する。ここで所定のデータ変換とは、セッション鍵によって特定される暗号処理を指し、ＤＥＳ暗号等の様な暗号処理であってもよいが、ここでは、データ変換部１０９と同様に排他的論理和を施すこととする。
【００２８】
送信部１３３は、データ変換部１３２により生成された変換管理情報をプレーヤ１４０へ送信する。
暗号化コンテンツ受信部１２７は、レコーダ１００から送信される暗号化コンテンツを受信する。
暗号化コンテンツ保持部１２８は、暗号化コンテンツ受信部１２７により受信された暗号化コンテンツを内部の不揮発性メモリに保持する。
【００２９】
暗号化コンテンツ送信部１２９は、暗号化コンテンツ保持部１２８に保持された暗号化コンテンツをプレーヤ１４０に送信する。
プレーヤ１４０は、音楽情報等のデジタルコンテンツとその管理情報を、暗号化等が施された状態でメモリカード１２０から入手して、再生等の利用を行うものであって、カードＩＤ受信部１４１、セッション鍵共有部１４２、管理情報処理部１４３、管理情報解析部１４４、暗号化コンテンツ受信部１４５、コンテンツ復号部１４６、及び、コンテンツ利用部１４７を備える。
【００３０】
カードＩＤ受信部１４１は、メモリカード１２０から送信されるカードＩＤを受信する。ここでは例として８バイトのカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を受信するものとする。
セッション鍵共有部１４２は、メモリカード１２０と乱数等をやり取りし、メモリカード１２０に記録された暗号化コンテンツを利用するセッション毎に異なるセッション鍵を生成する。ここではメモリカード１２０のセッション鍵共有部１２３でも同様にして、同じセッション鍵が生成されるものとする。より具体的にはレコーダ１００のセッション鍵共有部１０２で説明したものと同様であるので説明を省略する。
【００３１】
管理情報処理部１４３は、メモリカード１２０から送信される変換管理情報を受信し、セッション鍵共有部１４２により生成されたセッション鍵と、カードＩＤ受信部１４１により受信されたカードＩＤとを用いて、データ変換部１３２におけるデータ変換とは逆のデータ変換と復号処理とを施して管理情報を生成する。
【００３２】
図５は、管理情報処理部１４３の詳細な構成を示す図である。
図５に示すように管理情報処理部１４３は、受信部１４８、逆データ変換部１４９、及び、復号部１５０を含む。
受信部１４８は、メモリカード１２０の送信部１３３より送信された変換管理情報を受信する。
【００３３】
逆データ変換部１４９は、受信部１４８により受信された変換管理情報を、セッション鍵共有部１４２により生成されたセッション鍵を用いて、データ変換部１３２における所定のデータ変換とは逆のデータ変換を施して暗号化管理情報を生成する。ここではデータ変換部１３２における所定のデータ変換を排他的論理和を施すこととしたので、逆のデータ変換は排他的論理和を施すこととする。
【００３４】
復号部１５０は、カードＩＤ受信部１４１により受信されたカードＩＤを復号鍵として用

いて、所定のアルゴリズムにより、逆データ変換部１４９により生成された暗号化管理情報を復号して管理情報を生成する。ここで所定のアルゴリズムとは、例えばＤＥＳ暗号等の様な復号鍵によって特定される復号処理を指し、レコーダ１００の暗号化部１０８における暗号処理の逆変換であるものとする。

【００３５】

管理情報解析部１４４は、管理情報処理部１４３により生成された管理情報を解析して、管理情報に含まれるコンテンツ鍵をコンテンツ復号部１４６に渡し、管理情報に含まれる制限情報によるデジタルコンテンツに関する利用等の制限に従う。例えば、利用回数が“１０回”に制限されている場合には、利用する度に利用回数のデータを更新し、利用回数が“１０回”を越えた時には利用禁止としたり、使用期限が“３週間”に制限されている場合には、３週間後に利用禁止とする。

【００３６】

暗号化コンテンツ受信部１４５は、メモリカード１２０から送信される暗号化コンテンツを受信する。

コンテンツ復号部１４６は、暗号化コンテンツ受信部１４５により受信された暗号化コンテンツを、管理情報解析部１４４より渡された管理情報に含まれるコンテンツ鍵を用いて、所定のブロック復号処理を施し、デジタルコンテンツを生成する。ここでは例として、暗号化コンテンツを８バイトづつブロック単位に分割し、それぞれを、コンテンツ鍵“３３３３３３３３３３３３３３３３Ｈ”を用いて復号を施してデジタルコンテンツのブロックを生成し、これらをつないでデジタルコンテンツを生成するものとする。

【００３７】

コンテンツ利用部１４７は、コンテンツ復号部１４６により生成されたデジタルコンテンツを利用して音楽の再生等を行う。

＜動作＞

ここで、本実施の形態に係るレコーダ、及び、メモリカードにおける暗号化コンテンツの記録動作を説明する。

【００３８】

図６は、本実施の形態のレコーダ１００、及び、メモリカード１２０における暗号化コンテンツの記録動作の一例を示す図である。

（１）メモリカード１２０のカードＩＤ送信部１２２が、カードＩＤ保持部１２１に保持されたカードＩＤ（記号“ＣＩＤ”）を、レコーダ１００に送信する。ここでは例として８バイトのカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を送信するものとする（ステップＳ２１）。

（２）レコーダ１００のカードＩＤ受信部１０１が、メモリカード１２０から送信されるカードＩＤ“ＣＩＤ”を受信する（ステップＳ１１）。

（３）レコーダ１００のセッション鍵共有部１０２と、メモリカード１２０のセッション鍵共有部１２３とが乱数等をやり取りし、メモリカード１２０に暗号化コンテンツを記録させるセッション毎に異なるセッション鍵（記号“ＳＫ１”）を共有する。ここでは例として、セッション鍵共有部１０２では８バイトの乱数Ｘを発生させて送信し、乱数Ｙを受信して一方向性変換を施して“００１１３３７７８８ＣＣＥＥＦＦＨ”を生成して送り返し、自身で発生させた乱数Ｘに一方向性変換を施して“０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０ＦＨ”を生成し、送り返された値と比較して一致した場合にメモリカード１２０が正規のものであると認識した後、これらを排他的論理和したデータ“０Ｆ１Ｅ３Ｃ７８８７Ｃ３Ｅ１Ｆ０Ｈ”に一方向性変換を施してセッション鍵を生成し、一方、セッション鍵共有部１２３では８バイトの乱数Ｙを発生させて送信し、乱数Ｘを受信して一方向性変換を施して“０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０ＦＨ”を生成して送り返し、自身で発生させた乱数Ｙに一方向性変換を施して“００１１３３７７８８ＣＣＥＥＦＦＨ”を生成し、送り返された値と比較して一致した場合にレコーダ１００が正規のものであると認識した後、これらを排他的論理和したデータ“０Ｆ１Ｅ３Ｃ７８８７Ｃ３Ｅ１Ｆ０Ｈ”に一方向性変換を施してセッション鍵を生成する（ステップＳ１２、ステップＳ２２）。

（４）レコーダ１００の管理情報入手部１０３が、制限情報とコンテンツ鍵とを含む管理情報（記号“Ｌｉｃ”）を入手する。ここでは例として８バイトのコンテンツ鍵“３３３３３３３３３３３３３３Ｈ”と８バイトの制限情報“０００００００００００００００ＡＨ”とからなる１６バイトの管理情報“３３３３３３３３３３３３３３３０００００００００００００ＡＨ”を入手する（ステップＳ１３）。

（５）レコーダ１００の暗号化部１０８が、カードＩＤ受信部１０１により受信されたカードＩＤ“ＣＩＤ”を暗号化鍵として用いて、所定のアルゴリズム（記号“Ｅ”）により、管理情報入手部１０３により入手された管理情報“Ｌｉｃ”を暗号化して暗号化管理情報（式“Ｅ（ＣＩＤ，Ｌｉｃ）”）を生成する。ここではカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を暗号化鍵として用いて、管理情報“３３３３３３３３３３３３３３３３０００００００００００００００ＡＨ”を暗号化して１６バイトの暗号化管理情報を生成する（ステップＳ１４）。

（６）レコーダ１００のデータ変換部１０９が、暗号化部１０８により生成された暗号化管理情報“Ｅ（ＣＩＤ，Ｌｉｃ）”を、セッション鍵共有部１０２により生成されたセッション鍵“ＳＫ１”を用いて所定のデータ変換（ここでは排他的論理和、記号“ＸＯＲ”）を施して変換管理情報（式“ＸＯＲ（ＳＫ１，Ｅ（ＣＩＤ，Ｌｉｃ））”）を生成する。ここでは、１６バイトの暗号化管理情報と、８バイトのセッション鍵を２つ連結した１６バイトのデータとを排他的論理和して１６バイトの変換管理情報を生成する（ステップＳ１５）。

（７）レコーダ１００の送信部１１０が、データ変換部１０９により生成された変換管理情報“ＸＯＲ（ＳＫ１，Ｅ（ＣＩＤ，Ｌｉｃ））”をメモリカード１２０へ送信する（ステップＳ１６）。

（８）メモリカード１２０の受信部１３０が、レコーダ１００の送信部１１０より送信された変換管理情報“ＸＯＲ（ＳＫ１，Ｅ（ＣＩＤ，Ｌｉｃ））”を受信する（ステップＳ２３）。

（９）メモリカード１２０の逆データ変換部１３１が、受信部１３０により受信された変換管理情報“ＸＯＲ（ＳＫ１，Ｅ（ＣＩＤ，Ｌｉｃ））”を、セッション鍵共有部１２３により生成されたセッション鍵“ＳＫ１”を用いて、レコーダ１００のデータ変換部１０９における所定のデータ変換とは逆のデータ変換を施して暗号化管理情報“Ｅ（ＣＩＤ，Ｌｉｃ）”を生成する。ここでは１６バイトの変換管理情報と、８バイトのセッション鍵を２つ連結した１６バイトのデータとを排他的論理和して１６バイトの暗号化管理情報を生成する（ステップＳ２４）。

（１０）メモリカード１２０の暗号化管理情報保持部１２５が、第１管理情報処理部１２４により生成された暗号化管理情報“Ｅ（ＣＩＤ，Ｌｉｃ）”を内部の不揮発性メモリに保持する（ステップＳ２５）。

（１１）レコーダ１００のコンテンツ入手部１０５が、デジタルコンテンツ（記号“Ｃｏｎ”）を入手する。ここでは、１Ｍバイトのデジタルコンテンツを入手するものとする（ステップＳ１７）。

（１２）レコーダ１００のコンテンツ暗号化部１０６が、コンテンツ入手部１０５により入手されたデジタルコンテンツ“Ｃｏｎ”を、管理情報入手部１０３により入手された管理情報に含まれるコンテンツ鍵（記号“ＣＫ”）を用いて、所定のブロック暗号処理（記号“Ｅ”）を施し、暗号化コンテンツ（式“Ｅ（ＣＫ，Ｃｏｎ）”）を生成する。ここでは、デジタルコンテンツを８バイトづつブロック単位に分割し、それぞれを、コンテンツ鍵“３３３３３３３３３３３３３３３３Ｈ”を用いて暗号化を施して暗号化されたコンテンツのブロックを生成し、これらをつないで１Ｍバイトの暗号化コンテンツを生成するものとする（ステップＳ１８）。

（１３）レコーダ１００の暗号化コンテンツ送信部１０７が、コンテンツ暗号化部１０６により生成された暗号化コンテンツ“Ｅ（ＣＫ，Ｃｏｎ）”をメモリカード１２０へ送信する（ステップＳ１９）。

（１４）メモリカード１２０の暗号化コンテンツ受信部１２７が、レコーダ１００から送

信される暗号化コンテンツ“Ｅ（ＣＫ，Ｃｏｎ）”を受信する（ステップＳ２６）。
（１５）メモリカード１２０の暗号化コンテンツ保持部１２８が、暗号化コンテンツ受信部１２７により受信された暗号化コンテンツ“Ｅ（ＣＫ，Ｃｏｎ）”を内部の不揮発性メモリに保持する（ステップＳ２７）。
【００３９】
ここで、本実施の形態に係るメモリカード、及び、プレーヤにおける暗号化コンテンツの利用動作を説明する。
図７は、本実施の形態のメモリカード１２０、及び、プレーヤ１４０における暗号化コンテンツの利用動作の一例を示す図である。
（１）メモリカード１２０のカードＩＤ送信部１２２が、カードＩＤ保持部１２１に保持されたカードＩＤ“ＣＩＤ”を、プレーヤ１４０に送信する。ここでは例として８バイトのカードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を送信するものとする（ステップＳ３１）。
（２）プレーヤ１４０のカードＩＤ受信部１４１が、メモリカード１２０から送信されるカードＩＤ“ＣＩＤ”を受信する（ステップＳ４１）。
（３）メモリカード１２０のセッション鍵共有部１２３と、プレーヤ１４０のセッション鍵共有部１４２とが乱数等をやり取りし、メモリカード１２０に記録された暗号化コンテンツを利用するセッション毎に異なるセッション鍵“ＳＫ２”を共有する。ここでは例として、セッション鍵共有部１２３では８バイトの乱数Ｎを発生させて送信し、乱数Ｍを受信して一方向性変換を施して“１１２２４４８８７７ＢＢＤＤＥＥＨ”を生成して送り返し、自身で発生させた乱数Ｎに一方向性変換を施して“Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｈ”を生成し、送り返された値と比較して一致した場合にプレーヤ１４０が正規のものであると認識した後、これらを排他的論理和したデータ“Ｅ１Ｄ２Ｂ４７８８７４Ｂ２Ｄ１ＥＨ”に一方向性変換を施してセッション鍵を生成し、一方、セッション鍵共有部１４２では８バイトの乱数Ｍを発生させて送信し、乱数Ｎを受信して一方向性変換を施して“Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｆ０Ｈ”を生成して送り返し、自身で発生させた乱数Ｍに一方向性変換を施して“１１２２４４８８７７ＢＢＤＤＥＥＨ”を生成し、送り返された値と比較して一致した場合にメモリカード１２０が正規のものであると認識した後、これらを排他的論理和したデータ“Ｅ１Ｄ２Ｂ４７８８７４Ｂ２Ｄ１ＥＨ”に一方向性変換を施してセッション鍵を生成する（ステップＳ３２、ステップＳ４２）。
（４）メモリカード１２０のデータ変換部１３２が、暗号化管理情報保持部１２５に保持された暗号化管理情報（式“Ｅ（ＣＩＤ，Ｌｉｃ）”）を、セッション鍵共有部１２３により生成されたセッション鍵“ＳＫ２”を用いて所定のデータ変換（ここでは排他的論理和、記号“ＸＯＲ”）を施して変換管理情報（式“ＸＯＲ（ＳＫ２，Ｅ（ＣＩＤ，Ｌｉｃ））”）を生成する。ここでは、１６バイトの暗号化管理情報と、８バイトのセッション鍵を２つ連結した１６バイトのデータとを排他的論理和して１６バイトの変換管理情報を生成する（ステップＳ３３）。
（５）メモリカード１２０の送信部１３３が、データ変換部１３２により生成された変換管理情報“ＸＯＲ（ＳＫ２，Ｅ（ＣＩＤ，Ｌｉｃ））”をプレーヤ１４０へ送信する（ステップＳ３４）。
（６）プレーヤ１４０の受信部１４８が、メモリカード１２０の送信部１３３より送信された変換管理情報“ＸＯＲ（ＳＫ２，Ｅ（ＣＩＤ，Ｌｉｃ））”
を受信する（ステップＳ４３）。
（７）プレーヤ１４０の逆データ変換部１４９が、受信部１４８により受信された変換管理情報“ＸＯＲ（ＳＫ２，Ｅ（ＣＩＤ，Ｌｉｃ））”を、セッション鍵共有部１４２により生成されたセッション鍵“ＳＫ２”を用いて、データ変換部１３２における所定のデータ変換とは逆のデータ変換（ここでは排他的論理和、記号“ＸＯＲ”）を施して暗号化管理情報“Ｅ（ＣＩＤ，Ｌｉｃ）”を生成する。ここでは、１６バイトの変換管理情報と、８バイトのセッション鍵を２つ連結した１６バイトのデータとを排他的論理和して１６バイトの暗号化管理情報を生成する（ステップＳ４４）。

（８）プレーヤ１４０の復号部１５０が、カードＩＤ受信部１４１により受信されたカードＩＤ“ＣＩＤ”を復号鍵として用いて、所定のアルゴリズムにより、逆データ変換部１４９により生成された暗号化管理情報“Ｅ（ＣＩＤ，Ｌｉｃ）”を復号して管理情報“Ｌｉｃ”を生成する。ここでは、カードＩＤ“０１２３４５６７８９ＡＢＣＤＥＦＨ”を復号鍵として用いて、１６バイトの暗号化管理情報を復号して１６バイトの管理情報“３３３３３３３３３３３３３３３０００００００００００００００ＡＨ”を生成する（ステップＳ４５）。

（９）プレーヤ１４０の管理情報解析部１４４が、管理情報処理部１４３により生成された管理情報“Ｌｉｃ”を解析して、管理情報に含まれるコンテンツ鍵（記号“ＣＫ”）をコンテンツ復号部１４６に渡し、管理情報に含まれる制限情報によるデジタルコンテンツに関する利用等の制限に従う。ここでは、１６バイトの管理情報“３３３３３３３３３３３３３３３０００００００００００００００ＡＨ”に含まれる８バイトのコンテンツ鍵“３３３３３３３３３３３３３３３３Ｈ”をコンテンツ復号部１４６に渡し、８バイトの制限情報“０００００００００００００００ＡＨ”による利用等の制限に従う（ステップＳ４６）。

（１０）メモリカード１２０の暗号化コンテンツ送信部１２９が、暗号化コンテンツ保持部１２８に保持された暗号化コンテンツ（記号“Ｅ（ＣＫ，Ｃｏｎ）”）をプレーヤ１４０に送信する（ステップＳ３５）。

（１１）プレーヤ１４０の暗号化コンテンツ受信部１４５が、メモリカード１２０から送信される暗号化コンテンツ“Ｅ（ＣＫ，Ｃｏｎ）”を受信する（ステップＳ４７）。

（１２）プレーヤ１４０のコンテンツ復号部１４６が、暗号化コンテンツ受信部１４５により受信された暗号化コンテンツ“Ｅ（ＣＫ，Ｃｏｎ）”を、管理情報解析部１４４より渡された管理情報に含まれるコンテンツ鍵“ＣＫ”を用いて、所定のブロック復号処理を施し、デジタルコンテンツ“Ｃｏｎ”を生成する。ここでは、暗号化コンテンツを８バイトづつブロック単位に分割し、それぞれを、コンテンツ鍵“３３３３３３３３３３３３３３３３Ｈ”を用いて復号を施してデジタルコンテンツのブロックを生成し、これらをつないで１Ｍバイトのデジタルコンテンツを生成するものとする（ステップＳ４８）。

（１３）プレーヤ１４０のコンテンツ利用部１４７が、コンテンツ復号部１４６により生成されたデジタルコンテンツ“Ｃｏｎ”を利用して音楽の再生等を行う（ステップＳ４９）。

【００４０】

以上のように、本実施の形態では、制限情報を含む管理情報を、セッション毎に異なるセッション鍵で排他的論理和を施して送受信するので、管理情報をバックアップして以後の利用の際に置き換えても、以後の利用の際にはセッション鍵が異なるため、バックアップした管理情報は役に立たない。

なお、本実施の形態では、管理情報をデータ変換する具体的方法として、処理が簡易であり、且つ、処理速度が高速であるビット毎の排他的論理和を用いたが、セッション鍵によって特定される暗号処理であれば何であってもよい。さらに、管理情報の特定の位置に（例えば先頭に）乱数を付加してもよい。この方式を使うことにより、生成する乱数度がさらに増し、データ変換による送受信情報の隠蔽性がさらに強固になる。

【００４１】

また、セッション鍵を記録しておき、前の処理の際に使用して記録しておいたセッション鍵に基づいて、新たなセッション鍵を生成する連鎖暗号方式、及び、連鎖復号方式であってもよい。例えば記録しておいたセッション鍵から新たなセッション鍵を生成する方法としては、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換等が考えられる。

【００４２】

また本実施の形態ではセッション鍵は共通鍵暗号方式による共通鍵としたが、送信側のセッション鍵を公開鍵暗号方式による公開鍵とし、受信側のセッション鍵を当該公開鍵に対応する秘密鍵としてもよい。また、送信側のセッション鍵を回復型署名方式の秘密鍵とし

、受信側のセッション鍵を当該秘密鍵に対応する公開鍵としてもよい。
【００４３】
また本実施の形態では、セッション鍵を共有する処理において、乱数をやり取りする方法をとったが、システム全体に共通する値を基にしてセッション鍵をそれぞれ独自に生成する方法であってもよい。例えばシステム全体に共通する値としては、時刻データ等が考えられる。
また本実施の形態では、暗号化コンテンツと暗号化管理情報とを記録するための媒体として、大容量の半導体メモリとその制御回路とを備えるメモリカードを用いたが、ハードディスク、フロッピーディスク、ＤＶＤ－ＲＡＭ、ＣＤ－Ｒなどのあらゆる読み書き可能な記録媒体とその制御装置との組合せを用いてもよい。なお、メモリカード以外の記録媒体を用いる場合には、記録媒体毎に固有の値である他の情報をカードＩＤの代わりとする。
【００４４】
また、コンピュータに本実施の形態のような動作を実行させることができるプログラムが、コンピュータ読み取り可能な記録媒体に記録され、この記録媒体が流通し、取り引きの対象となりうる。
ここでコンピュータ読み取り可能な記録媒体とは、例えば、フロッピーディスク、ＣＤ、ＭＯ、ＤＶＤ、メモリカード等の着脱可能な記録媒体、及び、ハードディスク、半導体メモリ等の固定記録媒体等であり、特に限定されるものではない。
【００４５】
【発明の効果】
本発明に係るデジタルデータ記録装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ利用装置に利用に供するために送信するデジタルデータ記録装置であって、前記管理情報を記録している管理情報記録手段と、前記デジタルデータを記録しているデジタルデータ記録手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、管理情報記録手段に記録している管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、データ変換手段により生成された変換管理情報とデジタルデータ記録手段に記録しているデジタルデータとをセットで前記デジタルデータ利用装置に送信する送信手段とを備えることを特徴とする。
【００４６】
これによって、記録している管理情報に、送信処理の度に異なる鍵情報により特定されるデータ変換を施して送信することができる。
従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。
【００４７】
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ利用装置と共有し、前記データ変換手段は、前記鍵情報を共有鍵暗号方式の共有鍵として用いて前記管理情報を暗号化して前記変換管理情報を生成することを特徴とすることもできる。
これによって、デジタルデータ利用装置と鍵情報を共有することができ、共有鍵暗号方式による暗号通信を行うことができる。
【００４８】
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ利用装置と共有するに際、鍵情報そのものは送受信せずに鍵情報とは異なるデータをやりとりして、やりとりした結果得られた当該デジタルデータ利用装置と共有するデータに予め当該デジタルデータ利用装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。
【００４９】
これによって、鍵情報そのものを送受信せずに鍵情報を共有することができるので、変換

管理情報と鍵情報とをバックアップして以後の利用の際に置き換えるような不正行為が成立しない。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ利用装置と共有するに際し鍵情報そのものは送受信せずに当該デジタルデータ利用装置と共有する時刻に基づくデータに予め当該デジタルデータ利用装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。
【００５０】
これによって、鍵情報を時刻に基づくデータから生成することができるので、送信処理の度に確実に異なる鍵情報が生成される。
また、デジタルデータ記録装置において、前記デジタルデータ記録装置は、さらに、送信処理の度に取得される最新の鍵情報を記録する鍵情報記録手段を備え、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に予め定めた所定の変換を施して鍵情報を更新することを特徴とすることもできる。
【００５１】
これによって、前の鍵情報から新しい鍵情報を生成することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施して鍵情報を更新することを特徴とすることもできる。
【００５２】
これによって、前の鍵情報にインクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施すだけで新しい鍵情報を生成することができるので、処理が簡単になる。
また、デジタルデータ記録装置において、前記データ変換手段は、前記管理情報と前記鍵情報とを排他的論理和して前記変換管理情報を生成することを特徴とすることもできる。
【００５３】
これによって、排他的論理和によりデータ変換を施すことができ、逆変換が同じデータ変換になるので、処理が簡単になる。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を公開鍵暗号方式の公開鍵として取得し当該公開鍵に対応する秘密鍵を前記デジタルデータ利用装置が取得し、前記データ変換手段は、前記鍵情報を公開鍵暗号方式の公開鍵として用いて前記管理情報を暗号化して前記変換管理情報を生成することを特徴とすることもできる。
【００５４】
これによって、デジタルデータ記録装置では公開鍵を、デジタルデータ利用装置では秘密鍵を取得することができ、公開鍵暗号方式による暗号通信を行うことができる。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を回復型署名方式の秘密鍵として取得し当該秘密鍵に対応する公開鍵を前記デジタルデータ利用装置が取得し、前記データ変換手段は、前記鍵情報を回復型署名方式の秘密鍵として用いて前記管理情報を暗号化することを特徴とすることもできる。
【００５５】
これによって、デジタルデータ記録装置では秘密鍵を、デジタルデータ利用装置では公開鍵を取得することができ、回復型署名方式による暗号通信を行うことができる。
また、デジタルデータ記録装置において、前記データ変換手段は、データ変換の度に異なる乱数を生成し前記管理情報の所定位置に生成した乱数を付加した後で前記データ変換を施すことを特徴とすることもできる。
【００５６】
これによって、管理情報の所定位置に乱数を付加することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。

本発明に係るデジタルデータ記録装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ書込装置から受信して記録するデジタルデータ記録装置であって、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記管理情報に復元できるように前記デジタルデータ書込装置においてデータ変換された変換管理情報と前記デジタルデータとをセットで当該デジタルデータ書込装置から受信する受信手段と、受信手段により受信された変換管理情報に前記逆データ変換を施して管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された管理情報を記録する管理情報記録手段と、受信手段により受信されたデジタルデータを記録するデジタルデータ記録手段とを備えることを特徴とする。

【００５７】

これによって、変換管理情報を受信して、受信処理の度に異なる鍵情報により特定される逆データ変換を施して管理情報を生成して記録することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００５８】

また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ書込装置と共有し、前記逆データ変換手段は、前記鍵情報を共有鍵暗号方式の共有鍵として用いて前記変換管理情報を復号して前記管理情報を復元することを特徴とすることもできる。

これによって、デジタルデータ書込装置と鍵情報を共有することができ、共有鍵暗号方式による暗号通信を行うことができる。

【００５９】

また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ書込装置と共有するに際し鍵情報そのものは送受信せずに鍵情報とは異なるデータをやりとりして、やりとりした結果得られた当該デジタルデータ書込装置と共有するデータに予め当該デジタルデータ書込装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。

【００６０】

これによって、鍵情報そのものを送受信せずに鍵情報を共有することができるので、変換管理情報と鍵情報とをバックアップして以後の利用の際に置き換えるような不正行為が成立しない。

また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ書込装置と共有するに際し鍵情報そのものは送受信せずに当該デジタルデータ書込装置と共有する時刻に基づくデータに予め当該デジタルデータ書込装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。

【００６１】

これによって、鍵情報を時刻に基づくデータから生成することができるので、送信処理の度に確実に異なる鍵情報が生成される。

また、デジタルデータ記録装置において、前記デジタルデータ記録装置は、さらに、受信処理の度に取得される最新の鍵情報を記録する鍵情報記録手段を備え、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に予め定めた所定の変換を施して鍵情報を更新することを特徴とすることもできる。

【００６２】

これによって、前の鍵情報から新しい鍵情報を生成することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。

また、デジタルデータ記録装置において、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施して、鍵情報を更新することを特徴

とすることもできる。
【００６３】
これによって、前の鍵情報にインクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施すだけで新しい鍵情報を生成することができるので、処理が簡単になる。
また、デジタルデータ記録装置において、前記逆データ変換手段は、前記変換管理情報と前記鍵情報とを排他的論理和して前記管理情報を復元することを特徴とすることもできる。
【００６４】
これによって、排他的論理和によりデータ変換を施すことができ、逆変換が同じデータ変換になるので、処理が簡単になる。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を公開鍵暗号方式の秘密鍵として取得し当該秘密鍵に対応する公開鍵を前記デジタルデータ書込装置が取得し、前記逆データ変換手段は、前記鍵情報を公開鍵暗号方式の秘密鍵として用いて前記変換管理情報を復号して前記管理情報を復元することを特徴とすることもできる。
【００６５】
これによって、デジタルデータ書込装置では公開鍵を、デジタルデータ記録装置では秘密鍵を取得することができ、公開鍵暗号方式による暗号通信を行うことができる。
また、デジタルデータ記録装置において、前記鍵情報取得手段は、取得する鍵情報を回復型署名方式の公開鍵として取得し当該公開鍵に対応する秘密鍵を前記デジタルデータ書込装置が取得し、前記逆データ変換手段は、前記鍵情報を回復型署名方式の公開鍵として用いて前記変換管理情報を復号することを特徴とすることもできる。
【００６６】
これによって、デジタルデータ書込装置では秘密鍵を、デジタルデータ記録装置では公開鍵を取得することができ、回復型署名方式による暗号通信を行うことができる。
また、デジタルデータ記録装置において、前記受信手段が受信する変換管理情報はデータ変換を施すべき管理情報の所定位置に乱数を付加した後前記データ変換を施してあり、前記逆データ変換手段は、前記変換管理情報に前記逆データ変換を施した後前記所定位置の乱数を削除して管理情報を復元することを特徴とすることもできる。
【００６７】
これによって、管理情報の所定位置に乱数を付加することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。
本発明に係るデジタルデータ利用装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置から受信して利用するデジタルデータ利用装置であって、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記管理情報に復元できるように前記デジタルデータ記録装置においてデータ変換された変換管理情報と前記デジタルデータとをセットで当該デジタルデータ記録装置から受信する受信手段と、受信手段により受信された変換管理情報に前記逆データ変換を施して管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された管理情報に含まれる情報が示すデジタルデータの利用の制限に従い受信手段により受信されたデジタルデータを利用する利用手段とを備えることを特徴とする。
【００６８】
これによって、変換管理情報を受信して、受信処理の度に異なる鍵情報により特定される逆データ変換を施して管理情報を生成して利用することができる。
従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。
【００６９】

また、デジタルデータ利用装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有し、前記逆データ変換手段は、前記鍵情報を共有鍵暗号方式の共有鍵として用いて前記変換管理情報を復号して前記管理情報を復元することを特徴とすることもできる。
これによって、デジタルデータ記録装置と鍵情報を共有することができ、共有鍵暗号方式による暗号通信を行うことができる。
【００７０】
また、デジタルデータ利用装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有するに際し鍵情報そのものは送受信せずに鍵情報とは異なるデータをやりとりして、やりとりした結果得られた当該デジタルデータ記録装置と共有するデータに予め当該デジタルデータ記録装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。
【００７１】
これによって、鍵情報そのものを送受信せずに鍵情報を共有することができるので、変換管理情報と鍵情報とをバックアップして以後の利用の際に置き換えるような不正行為が成立しない。
また、デジタルデータ利用装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有するに際し鍵情報そのものは送受信せずに当該デジタルデータ記録装置と共有する時刻に基づくデータに予め当該デジタルデータ記録装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。
【００７２】
これによって、鍵情報を時刻に基づくデータから生成することができるので、送信処理の度に確実に異なる鍵情報が生成される。
また、デジタルデータ利用装置において、前記デジタルデータ利用装置は、さらに、受信処理の度に取得される最新の鍵情報を記録する鍵情報記録手段を備え、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に予め定めた所定の変換を施して鍵情報を更新することを特徴とすることもできる。
【００７３】
これによって、前の鍵情報から新しい鍵情報を生成することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。
また、デジタルデータ利用装置において、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施して鍵情報を更新することを特徴とすることもできる。
【００７４】
これによって、前の鍵情報にインクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施すだけで新しい鍵情報を生成することができるので、処理が簡単になる。
また、デジタルデータ利用装置において、前記逆データ変換手段は、前記変換管理情報と前記鍵情報とを排他的論理和して前記管理情報を復元することを特徴とすることもできる。
【００７５】
これによって、排他的論理和によりデータ変換を施すことができ、逆変換が同じデータ変換になるので、処理が簡単になる。
また、デジタルデータ利用装置において、前記鍵情報取得手段は、取得する鍵情報を公開鍵暗号方式の秘密鍵として取得し当該秘密鍵に対応する公開鍵を前記デジタルデータ記録装置が取得し、前記逆データ変換手段は、前記鍵情報を公開鍵暗号方式の秘密鍵として用いて前記変換管理情報を復号して前記管理情報を復元することを特徴とすることもできる。
【００７６】

これによって、デジタルデータ記録装置では公開鍵を、デジタルデータ利用装置では秘密鍵を取得することができ、公開鍵暗号方式による暗号通信を行うことができる。
また、デジタルデータ利用装置において、前記鍵情報取得手段は、取得する鍵情報を回復型署名方式の公開鍵として取得し当該公開鍵に対応する秘密鍵を前記デジタルデータ書込装置が取得し、前記逆データ変換手段は、前記鍵情報を回復型署名方式の公開鍵として用いて前記変換管理情報を復号することを特徴とすることもできる。

【００７７】

これによって、デジタルデータ記録装置では秘密鍵を、デジタルデータ利用装置では公開鍵を取得することができ、回復型署名方式による暗号通信を行うことができる。
また、デジタルデータ利用装置において、前記受信手段が受信する変換管理情報はデータ変換を施すべき管理情報の所定位置に乱数を付加した後前記データ変換を施してあり、前記逆データ変換手段は、前記変換管理情報に前記逆データ変換を施した後前記所定位置の乱数を削除して管理情報を復元することを特徴とすることもできる。

【００７８】

これによって、管理情報の所定位置に乱数を付加することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。
本発明に係るデジタルデータ書込装置は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置に送信して記録させるデジタルデータ書込装置であって、前記管理情報を入手する管理情報入手手段と、前記デジタルデータを入手するデジタルデータ入手手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、管理情報入手手段により入手された管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、データ変換手段により生成された変換管理情報とデジタルデータ入手手段により入手されたデジタルデータとをセットで前記デジタルデータ記録装置に送信する送信手段とを備えることを特徴とする。

【００７９】

これによって、入手した管理情報に、送信処理の度に異なる鍵情報により特定されるデータ変換を施して送信することができる。
従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００８０】

また、デジタルデータ書込装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有し、前記データ変換手段は、前記鍵情報を共有鍵暗号方式の共有鍵として用いて前記管理情報を暗号化して前記変換管理情報を生成することを特徴とすることもできる。
これによって、デジタルデータ記録装置と鍵情報を共有することができ、共有鍵暗号方式による暗号通信を行うことができる。

【００８１】

また、デジタルデータ書込装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有するに際し鍵情報そのものは送受信せずに鍵情報とは異なるデータをやりとりして、やりとりした結果得られた当該デジタルデータ記録装置と共有するデータに予め当該デジタルデータ記録装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。

【００８２】

これによって、鍵情報そのものを送受信せずに鍵情報を共有することができるので、変換管理情報と鍵情報とをバックアップして以後の利用の際に置き換えるような不正行為が成立しない。
また、デジタルデータ書込装置において、前記鍵情報取得手段は、取得する鍵情報を前記デジタルデータ記録装置と共有するに際し鍵情報そのものは送受信せずに当該デジタルデ

ータ記録装置と共有する時刻に基づくデータに予め当該デジタルデータ記録装置と共有する秘密のデータ変換を施して鍵情報を生成することを特徴とすることもできる。

【００８３】

これによって、鍵情報を時刻に基づくデータから生成することができるので、送信処理の度に確実に異なる鍵情報が生成される。

また、デジタルデータ書込装置において、前記デジタルデータ書込装置は、さらに、送信処理の度に取得される最新の鍵情報を記録する鍵情報記録手段を備え、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に予め定めた所定の変換を施して鍵情報を更新することを特徴とすることもできる。

【００８４】

これによって、前の鍵情報から新しい鍵情報を生成することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。

また、デジタルデータ書込装置において、前記鍵情報取得手段は、鍵情報記録手段に記録された最新の鍵情報に、インクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施して鍵情報を更新することを特徴とすることもできる。

【００８５】

これによって、前の鍵情報にインクリメント、デクリメント、予め定めた値との四則演算、及び、予め決められた秘密の一方向性変換の何れかを施すだけで新しい鍵情報を生成することができるので、処理が簡単になる。

また、デジタルデータ書込装置において、前記データ変換手段は、前記管理情報と前記鍵情報とを排他的論理和して前記変換管理情報を生成することを特徴とすることもできる。

【００８６】

これによって、排他的論理和によりデータ変換を施すことができ、逆変換が同じデータ変換になるので、処理が簡単になる。

また、デジタルデータ書込装置において、前記鍵情報取得手段は、取得する鍵情報を公開鍵暗号方式の公開鍵として取得し当該公開鍵に対応する秘密鍵を前記デジタルデータ記録装置が取得し、前記データ変換手段は、前記鍵情報を公開鍵暗号方式の公開鍵として用いて前記管理情報を暗号化して前記変換管理情報を生成することを特徴とすることもできる。

【００８７】

これによって、デジタルデータ書込装置では公開鍵を、デジタルデータ記録装置では秘密鍵を取得することができ、公開鍵暗号方式による暗号通信を行うことができる。

また、デジタルデータ書込装置において、前記鍵情報取得手段は、取得する鍵情報を回復型署名方式の秘密鍵として取得し当該秘密鍵に対応する公開鍵を前記デジタルデータ記録装置が取得し、前記データ変換手段は、前記鍵情報を回復型署名方式の秘密鍵として用いて前記管理情報を暗号化することを特徴とすることもできる。

【００８８】

これによって、デジタルデータ書込装置では秘密鍵を、デジタルデータ記録装置では公開鍵を取得することができ、回復型署名方式による暗号通信を行うことができる。

また、デジタルデータ書込装置において、前記データ変換手段は、データ変換の度に異なる乱数を生成し前記管理情報の所定位置に生成した乱数を付加した後で前記データ変換を施すことを特徴とすることもできる。

【００８９】

これによって、管理情報の所定位置に乱数を付加することができるので、データ変換による送受信情報の隠蔽性がさらに強固になる。

本発明に係る暗号化デジタルデータ記録装置は、デジタルデータの利用を制限する情報と当該デジタルデータが暗号化された暗号化デジタルデータを復号するための復号処理を特定する情報とを含む管理情報が暗号化デジタルデータ記録装置毎に固有の値である装置ＩＤにより特定される復号処理を施すことにより復号できるように暗号化された暗号化管理

情報及び当該暗号化デジタルデータを暗号化デジタルデータ利用装置に利用に供するために送信する暗号化デジタルデータ記録装置であって、前記装置ＩＤを保持している装置ＩＤ保持手段と、装置ＩＤ保持手段に保持している装置ＩＤを前記暗号化デジタルデータ利用装置に送信する装置ＩＤ送信手段と、前記暗号化管理情報を記録している暗号化管理情報記録手段と、前記暗号化デジタルデータを記録している暗号化デジタルデータ記録手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、暗号化管理情報記録手段に記録している暗号化管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、データ変換手段により生成された変換管理情報と暗号化デジタルデータ記録手段に記録している暗号化デジタルデータとをセットで前記暗号化デジタルデータ利用装置に送信するデータ送信手段とを備えることを特徴とする。

【００９０】

これによって、装置ＩＤを用いて復号できるように暗号化された管理情報に、送信処理の度に異なる鍵情報により特定されるデータ変換を施して送信することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００９１】

また、記録している変換管理情報、及び、暗号化デジタルデータを不正に、別の暗号化デジタルデータ記録装置にコピーしても、暗号化デジタルデータ記録装置毎に装置ＩＤが異なり復号できないので役にたたず、この様な不正行為も成立しない。

本発明に係る暗号化デジタルデータ記録装置は、デジタルデータの利用を制限する情報と当該デジタルデータが暗号化された暗号化デジタルデータを復号するための復号処理を特定する情報とを含む管理情報が暗号化デジタルデータ記録装置毎に固有の値である装置ＩＤにより特定される復号処理を施すことにより復号できるように暗号化された暗号化管理情報及び当該暗号化デジタルデータを暗号化デジタルデータ書込装置から受信して記録する暗号化デジタルデータ記録装置であって、前記装置ＩＤを保持している装置ＩＤ保持手段と、装置ＩＤ保持手段に保持している装置ＩＤを前記暗号化デジタルデータ書込装置に送信する装置ＩＤ送信手段と、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記暗号化管理情報に復元できるように前記暗号化デジタルデータ書込装置においてデータ変換されて生成される変換管理情報と前記暗号化デジタルデータとをセットで当該暗号化デジタルデータ書込装置から受信する受信手段と、受信手段により受信された変換管理情報に前記逆データ変換を施して暗号化管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された暗号化管理情報を記録する暗号化管理情報記録手段と、受信手段により受信された暗号化デジタルデータを記録する暗号化デジタルデータ記録手段とを備えることを特徴とする。

【００９２】

これによって、変換管理情報を受信して、受信処理の度に異なる鍵情報により特定される逆データ変換を施して、装置ＩＤを用いて復号できるように暗号化された管理情報を生成して記録することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００９３】

また、記録している変換管理情報、及び、暗号化デジタルデータを、不正に別の暗号化デジタルデータ記録装置にコピーしても、暗号化デジタルデータ記録装置毎に装置ＩＤが異なり復号できないので役にたたず、この様な不正行為も成立しない。

本発明に係る暗号化デジタルデータ利用装置は、デジタルデータの利用を制限する制限情報と当該デジタルデータが暗号化された暗号化デジタルデータを復号するための復号処理

を特定する復号情報とを含む管理情報が暗号化デジタルデータ記録装置毎に固有の値である装置ＩＤにより特定される復号処理を施すことにより復号できるように暗号化された暗号化管理情報及び当該暗号化デジタルデータを暗号化デジタルデータ記録装置から受信して利用する暗号化デジタルデータ利用装置であって、前記装置ＩＤを前記暗号化デジタルデータ記録装置から受信する装置ＩＤ受信手段と、受信処理の度に異なる鍵情報を取得する鍵情報取得手段と、鍵情報取得手段により取得された鍵情報により特定される逆データ変換を施すことにより前記暗号化管理情報に復元できるようにデータ変換された変換管理情報と前記暗号化デジタルデータとをセットで前記暗号化デジタルデータ記録装置から受信するデータ受信手段と、データ受信手段により受信された変換管理情報に前記逆データ変換を施して暗号化管理情報を復元する逆データ変換手段と、逆データ変換手段により復元された暗号化管理情報を装置ＩＤ受信手段により受信された装置ＩＤにより特定される復号処理を施して管理情報を生成する管理情報復号手段と、データ受信手段により受信された暗号化デジタルデータに管理情報復号手段により生成された管理情報に含まれる復号情報により特定される復号処理を施してデジタルデータを生成するデジタルデータ復号手段と、管理情報復号手段により生成された管理情報に含まれる制限情報が示すデジタルデータの利用の制限に従いデジタルデータ復号手段により生成されたデジタルデータを利用する利用手段とを備えることを特徴とする。

【００９４】

これによって、変換管理情報を受信して、受信処理の度に異なる鍵情報により特定される逆データ変換を施して暗号化管理情報を生成し、さらに、装置ＩＤにより特定される復号処理を施して管理情報を生成して利用することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００９５】

また、暗号化デジタルデータ記録装置に記録された変換管理情報、及び、暗号化デジタルデータを不正に、別の暗号化デジタルデータ記録装置にコピーしても、暗号化デジタルデータ記録装置毎に装置ＩＤが異なり復号できないので役にたたず、この様な不正行為も成立しない。

本発明に係る暗号化デジタルデータ書込装置は、デジタルデータの利用を制限する制限情報と当該デジタルデータが暗号化された暗号化デジタルデータを復号するための復号処理を特定する復号情報とを含む管理情報を暗号化デジタルデータ記録装置毎に固有の値である装置ＩＤが特定する復号処理により復号できるように暗号化して暗号化管理情報を生成し当該デジタルデータを当該復号情報が特定する復号処理により復号できるように暗号化して暗号化デジタルデータを生成し当該暗号化管理情報及び当該暗号化デジタルデータを暗号化デジタルデータ記録装置に送信して記録させる暗号化デジタルデータ書込装置であって、前記装置ＩＤを前記暗号化デジタルデータ記録装置から受信する装置ＩＤ受信手段と、前記管理情報を入手する管理情報入手手段と、前記デジタルデータを入手するデジタルデータ入手手段と、送信処理の度に異なる鍵情報を取得する鍵情報取得手段と、管理情報入手手段により入手された管理情報を装置ＩＤ受信手段により受信された装置ＩＤにより特定される復号処理を施すことにより復号できるように暗号化して暗号化管理情報を生成する管理情報暗号化手段と、管理情報暗号化手段により生成された暗号化管理情報に鍵情報取得手段により取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換手段と、デジタルデータ入手手段により入手されたデジタルデータを管理情報入手手段により入手された管理情報に含まれる復号情報により特定される復号処理により復号できるように暗号化して暗号化デジタルデータを生成するデジタルデータ暗号化手段と、データ変換手段により生成された変換管理情報とデジタルデータ暗号化手段により生成された暗号化デジタルデータとをセットで前記暗号化デジタルデータ記録装置に送信する送信手段とを備えることを特徴とする。

【００９６】

これによって、管理情報を、装置ＩＤにより特定される復号処理を施すことにより復号できるように暗号化し、さらに、送信処理の度に異なる鍵情報により特定されるデータ変換を施して送信することができる。
従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００９７】

また、暗号化デジタルデータ記録装置に記録された変換管理情報、及び、暗号化デジタルデータを不正に、別の暗号化デジタルデータ記録装置にコピーしても、暗号化デジタルデータ記録装置毎に装置ＩＤが異なり復号できないので役にたたず、この様な不正行為も成立しない。
本発明に係るデジタルデータ利用方法は、デジタルデータ記録装置が記録するデジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ利用装置において利用するデジタルデータ利用方法であって、当該デジタルデータの利用の度に前記デジタルデータ記録装置においてデータ変換を特定する変換鍵情報を生成し同時に前記デジタルデータ利用装置において当該データ変換の逆変換である逆データ変換を特定する逆変換鍵情報を生成する鍵情報生成ステップと、前記デジタルデータ記録装置において記録している管理情報に鍵情報生成ステップにより生成された変換鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換ステップと、前記デジタルデータ記録装置においてデータ変換ステップにより生成された変換管理情報を前記デジタルデータ利用装置に送信する変換管理情報送信ステップと、前記デジタルデータ利用装置において変換管理情報送信ステップにより送信された変換管理情報を前記デジタルデータ記録装置から受信する変換管理情報受信ステップと、前記デジタルデータ利用装置において変換管理情報受信ステップにより受信された変換管理情報に鍵情報生成ステップにより生成された逆変換鍵情報により特定される逆データ変換を施して管理情報を復元する逆データ変換ステップと、前記デジタルデータ記録装置において記録しているデジタルデータを前記デジタルデータ利用装置に送信するデジタルデータ送信ステップと、前記デジタルデータ利用装置においてデジタルデータ送信ステップにより送信されたデジタルデータを前記デジタルデータ記録装置から受信するデジタルデータ受信ステップと、前記デジタルデータ利用装置において逆データ変換ステップにより復元された管理情報に含まれる情報が示すデジタルデータの利用の制限に従いデジタルデータ受信ステップにより受信されたデジタルデータを利用するデジタルデータ利用ステップとを備えることを特徴とする。

【００９８】

これによって、記録装置が管理情報に送信処理の度に異なる変換鍵情報により特定されるデータ変換を施して送信し、利用装置がこれを受信して、受信処理の度に異なる逆変換鍵情報により特定される逆データ変換を施して管理情報を生成して利用することができる。
従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【００９９】

本発明に係るデジタルデータ書込方法は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ書込装置からデジタルデータ記録装置に送信して記録するデジタルデータ書込方法であって、当該デジタルデータの記録の度に前記デジタルデータ書込装置においてデータ変換を特定する変換鍵情報を生成し同時に前記デジタルデータ記録装置において当該データ変換の逆変換である逆データ変換を特定する逆変換鍵情報を生成する鍵情報生成ステップと、前記デジタルデータ書込装置において前記管理情報を入手する管理情報入手ステップと、前記デジタルデータ書込装置において管理情報入手ステップにより入手された管理情報に鍵情報生成ステップにより生成された変換鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換ステップと、前記デジタルデータ書込装置においてデータ変換ステップにより生成された変換管

理情報を前記デジタルデータ記録装置に送信する変換管理情報送信ステップと、前記デジタルデータ記録装置において変換管理情報送信ステップにより送信された変換管理情報を前記デジタルデータ書込装置から受信する変換管理情報受信ステップと、前記デジタルデータ記録装置において変換管理情報受信ステップにより受信された変換管理情報に鍵情報生成ステップにより生成された逆変換鍵情報により特定される逆データ変換を施して管理情報を復元する逆データ変換ステップと、前記デジタルデータ記録装置において逆データ変換ステップにより復元された管理情報を記録する管理情報記録ステップと、前記デジタルデータ書込装置において前記デジタルデータを入手するデジタルデータ入手ステップと、前記デジタルデータ書込装置においてデジタルデータ入手ステップにより入手されたデジタルデータを前記デジタルデータ記録装置に送信するデジタルデータ送信ステップと、前記デジタルデータ記録装置においてデジタルデータ送信ステップにより送信されたデジタルデータを前記デジタルデータ書込装置から受信するデジタルデータ受信ステップと、前記デジタルデータ記録装置においてデジタルデータ受信ステップにより受信されたデジタルデータを記録するデジタルデータ記録ステップとを備えることを特徴とする。

【０１００】

これによって、書込装置が送信処理の度に異なる変換鍵情報により特定されるデータ変換を施して送信し、記録情報がこれを受信して、受信処理の度に異なる逆変換鍵情報により特定される逆データ変換を施して管理情報を生成して記録することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【０１０１】

本発明に係るデジタルデータ利用プログラムを記録したコンピュータ読み取り可能な記録媒体は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置から受信して利用するデジタルデータ利用プログラムを記録したコンピュータ読み取り可能な記録媒体であって、コンピュータに、受信処理の度に異なる鍵情報を取得する鍵情報取得ステップと、鍵情報取得ステップにより取得された鍵情報により特定される逆データ変換を施すことにより前記管理情報に復元できるように前記デジタルデータ記録装置においてデータ変換された変換管理情報と前記デジタルデータとをセットで当該デジタルデータ記録装置から受信する受信ステップと、受信ステップにより受信された変換管理情報に前記逆データ変換を施して管理情報を復元する逆データ変換ステップと、逆データ変換ステップにより復元された管理情報に含まれる情報が示すデジタルデータの利用の制限に従い受信ステップにより受信されたデジタルデータを利用するデジタルデータ利用ステップとを実行させることを特徴とする。

【０１０２】

これによって、変換管理情報を受信して、受信処理の度に異なる鍵情報により特定される逆データ変換を施して管理情報を生成して利用することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【０１０３】

本発明に係るデジタルデータ書込プログラムを記録したコンピュータ読み取り可能な記録媒体は、デジタルデータの利用を制限する情報を含む管理情報及び当該デジタルデータをデジタルデータ記録装置に送信して記録させるデジタルデータ書込プログラムを記録したコンピュータ読み取り可能な記録媒体であって、コンピュータに、前記管理情報を入手する管理情報入手ステップと、前記デジタルデータを入手するデジタルデータ入手ステップと、送信処理の度に異なる鍵情報を取得する鍵情報取得ステップと、管理情報入手ステップにより入手された管理情報に鍵情報取得ステップにより取得された鍵情報により特定されるデータ変換を施して変換管理情報を生成するデータ変換ステップと、データ変換ステップにより生成された変換管理情報とデジタルデータ入手ステップにより入手されたデジ

タルデータとをセットで前記デジタルデータ記録装置に送信する送信ステップとを実行させることを特徴とする。

【０１０４】

これによって、入手した管理情報に、送信処理の度に異なる鍵情報により特定されるデータ変換を施して送信することができる。

従って、不正に変換管理情報をバックアップして以後の利用の際に置き換えても、バックアップしたときと置き換えたときとで鍵情報が異なり、置き換えた変換管理情報は正常に逆データ変換できないので役にたたず、不正行為が成立しない。

【図面の簡単な説明】

【図１】本実施の形態に係るレコーダ、メモリカード、及び、プレーヤの構成を示す図である。

【図２】管理情報処理部１０４の詳細な構成を示す図である。

【図３】第１管理情報処理部１２４の詳細な構成を示す図である。

【図４】第２管理情報処理部１２６の詳細な構成を示す図である。

【図５】管理情報処理部１４３の詳細な構成を示す図である。

【図６】本実施の形態のレコーダ１００、及び、メモリカード１２０における暗号化コンテンツの記録動作の一例を示す図である。

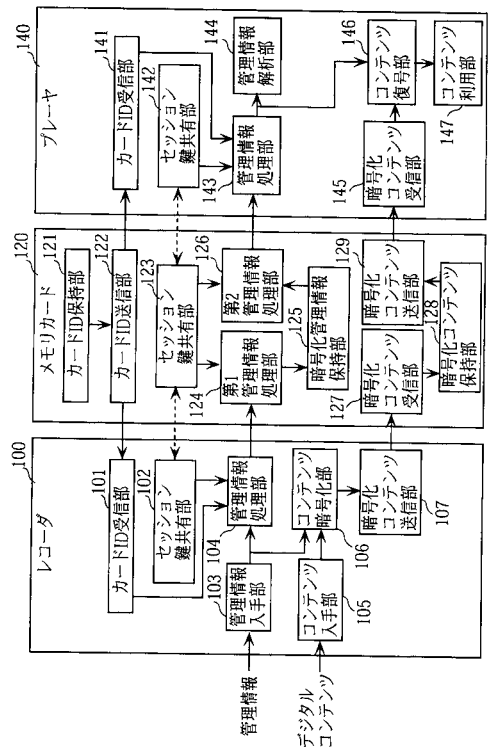
【図７】本実施の形態のメモリカード１２０、及び、プレーヤ１４０における暗号化コンテンツの利用動作の一例を示す図である。

【符号の説明】

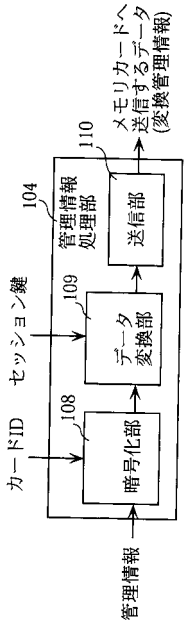
１００　レコーダ
１０１　カードＩＤ受信部
１０２　セッション鍵共有部
１０３　管理情報入手部
１０４　管理情報処理部
１０５　コンテンツ入手部
１０６　コンテンツ暗号化部
１０７　暗号化コンテンツ送信部
１０８　暗号化部
１０９　データ変換部
１１０　送信部
１２０　メモリカード
１２１　カードＩＤ保持部
１２２　カードＩＤ送信部
１２３　セッション鍵共有部
１２４　第１管理情報処理部
１２５　暗号化管理情報保持部
１２６　第２管理情報処理部
１２７　暗号化コンテンツ受信部
１２８　暗号化コンテンツ保持部
１２９　暗号化コンテンツ送信部
１３０　受信部
１３１　逆データ変換部
１３２　データ変換部
１３３　送信部
１４０　プレーヤ
１４１　カードＩＤ受信部
１４２　セッション鍵共有部
１４３　管理情報処理部
１４４　管理情報解析部

１４５　　暗号化コンテンツ受信部
１４６　　コンテンツ復号部
１４７　　コンテンツ利用部
１４８　　受信部
１４９　　逆データ変換部
１５０　　復号部

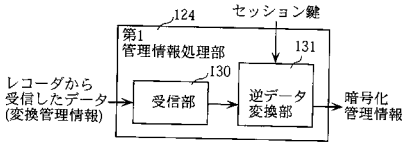
【図１】



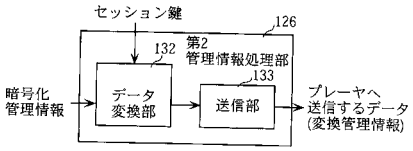
【図２】



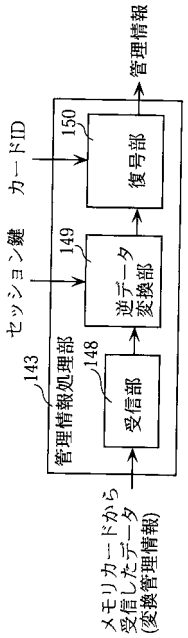
【図３】


124
セッション鍵
第1
管理情報処理部
131
130
レコーダから
受信したデータ
(変換管理情報)
受信部
逆データ
変換部
暗号化
管理情報

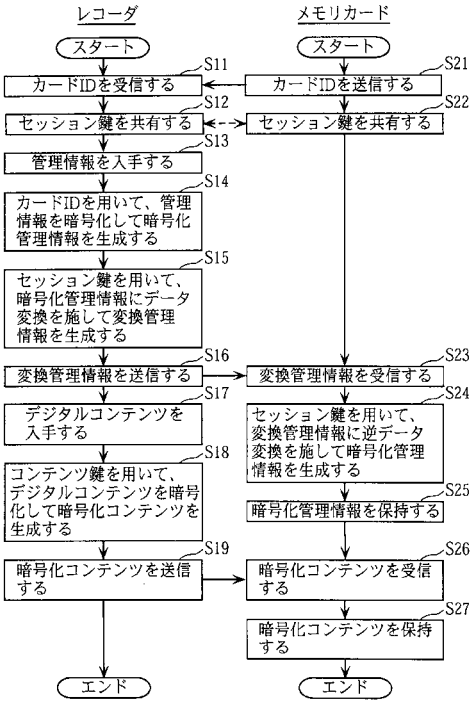
【図４】


セッション鍵
126
第2
管理情報処理部
132
133
暗号化
管理情報
データ
変換部
送信部
プレーヤへ
送信するデータ
(変換管理情報)

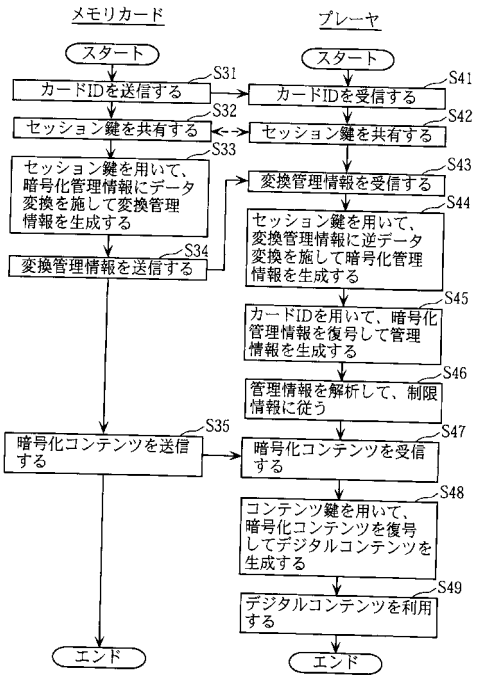
【図５】


管理情報
カードID
150
復号部
セッション鍵
149
逆データ
変換部
143
管理情報処理部
148
受信部
メモリカードから
受信したデータ
(変換管理情報)

【図６】


レコーダ
メモリカード
スタート
スタート
S11
カードIDを受信する
S21
カードIDを送信する
S12
セッション鍵を共有する
S22
セッション鍵を共有する
S13
管理情報を入手する
S14
カードIDを用いて、管理情報を暗号化して暗号化管理情報を生成する
S15
セッション鍵を用いて、暗号化管理情報にデータ変換を施して変換管理情報を生成する
S16
変換管理情報を送信する
S23
変換管理情報を受信する
S17
デジタルコンテンツを入手する
S24
セッション鍵を用いて、変換管理情報に逆データ変換を施して暗号化管理情報を生成する
S18
コンテンツ鍵を用いて、デジタルコンテンツを暗号化して暗号化コンテンツを生成する
S25
暗号化管理情報を保持する
S19
暗号化コンテンツを送信する
S26
暗号化コンテンツを受信する
S27
暗号化コンテンツを保持する
エンド
エンド

【図７】


メモリカード
プレーヤ
スタート
スタート
S31
カードIDを送信する
S41
カードIDを受信する
S32
セッション鍵を共有する
S42
セッション鍵を共有する
S33
セッション鍵を用いて、暗号化管理情報にデータ変換を施して変換管理情報を生成する
S43
変換管理情報を受信する
S34
変換管理情報を送信する
S44
セッション鍵を用いて、変換管理情報に逆データ変換を施して暗号化管理情報を生成する
S45
カードIDを用いて、暗号化管理情報を復号して管理情報を生成する
S46
管理情報を解析して、制限情報に従う
S35
暗号化コンテンツを送信する
S47
暗号化コンテンツを受信する
S48
コンテンツ鍵を用いて、暗号化コンテンツを復号してデジタルコンテンツを生成する
S49
デジタルコンテンツを利用する
エンド
エンド

フロントページの続き

合議体
審判長　井関　守三
審判官　成瀬　博之
審判官　冨吉　伸弥

(56)参考文献　特開平９－２０５４２４（ＪＰ，Ａ）
特開平７－２８４０５（ＪＰ，Ａ）
“小型メモリ・カードで音楽著作権を守る”，日経エレクトロニクス，日本，日経ＢＰ社，１９９９年　3月２２日，Ｎｏ．７３９，ｐ．４９－５３
一松　信，“データ保護と暗号化の研究”，日本，日本経済新聞社，１９８３年　7月２９日，１版１刷，ｐ．５９－６５
岡本栄司，“暗号理論入門”，日本，共立出版株式会社，１９９３年2月２５日，初版１刷，ｐ．１１３

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00