(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7133589号
(P7133589)

(45)発行日　令和4年9月8日(2022.9.8)

(24)登録日　令和4年8月31日(2022.8.31)

(51)国際特許分類

Ｇ０６Ｆ　21/62　(2013.01)	Ｇ０６Ｆ	21/62	３０９
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０６Ｆ	21/44	
Ｇ０６Ｑ　30/00　(2012.01)	Ｇ０６Ｑ	30/00	３４０

ＦＩ

請求項の数　4　（全10頁）

(21)出願番号　特願2020-133318(P2020-133318)
(22)出願日　令和2年8月5日(2020.8.5)
(65)公開番号　特開2021-166028(P2021-166028A)
(43)公開日　令和3年10月14日(2021.10.14)
審査請求日　令和3年11月10日(2021.11.10)
早期審査対象出願

(73)特許権者　515253821
ＳＢＩＮＦＴ株式会社
東京都港区六本木一丁目６番１号
(74)代理人　100114258
弁理士　福地 武雄
(74)代理人　100125391
弁理士　白川 洋一
(72)発明者　金 東日
東京都港区六本木四丁目２番４５号高會堂ビル２階 株式会社スマートアプリ内
(72)発明者　高 長徳
東京都港区六本木四丁目２番４５号高會堂ビル２階 株式会社スマートアプリ内
審査官　中里 裕正

最終頁に続く

(54)【発明の名称】　ＮＦＴアクセス制限システムおよびＮＦＴアクセス制限プログラム

(57)【特許請求の範囲】

【請求項１】

ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限システムであって、

アクセス制限を解除するための秘密鍵を用いて、ＮＦＴに記録されているデータにアクセス制限を設定し、前記アクセス制限が設定された制限付きＮＦＴ記録データをブロックチェーンに書き込むデータサーバと、

前記アクセス制限を解除するための秘密鍵を保持するアプリケーションサーバと、を備え、

前記アプリケーションサーバは、前記ブロックチェーンからアクセス制限が設定された制限付きＮＦＴ記録データを取得したクライアント装置によるリクエストに基づいて、アクセス制限を解除するための秘密鍵と前記リクエストとを対応付け、

前記データサーバは、前記秘密鍵および前記リクエストに基づいて、前記クライアント装置に対する認証を実行し、認証が得られた場合は、前記クライアント装置へＮＦＴの実データの閲覧を可能とすることを特徴とするＮＦＴアクセス制限システム。

【請求項２】

前記データサーバは、

前記秘密鍵を動的に生成する秘密鍵生成部と、

ＮＦＴの実データを記録するデータ記録部と、を備え、

前記アプリケーションサーバは、

前記動的に生成された秘密鍵を保持する秘密鍵保持部を備えることを特徴とする請求項１記載のＮＦＴアクセス制限システム。
【請求項３】
ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限プログラムであって、
アクセス制限を解除するための秘密鍵を用いて、ＮＦＴに記録されているデータにアクセス制限を設定する処理と、
前記アクセス制限が設定された制限付きＮＦＴ記録データをブロックチェーンに書き込む処理と、
前記アクセス制限を解除するための秘密鍵を保持する処理と、
前記ブロックチェーンからアクセス制限が設定された制限付きＮＦＴ記録データを取得したクライアント装置によるリクエストを取得する処理と、
前記リクエストに基づいて、アクセス制限を解除するための秘密鍵と前記リクエストとを対応付ける処理と、
前記秘密鍵および前記リクエストに基づいて、前記クライアント装置に対する認証を実行する処理と、
前記認証が得られた場合は、前記クライアント装置へＮＦＴの実データの閲覧を可能とする処理と、の一連処理をコンピュータに実行させることを特徴とするＮＦＴアクセス制限プログラム。
【請求項４】
前記秘密鍵を動的に生成する処理と、
ＮＦＴの実データを記録する処理と、
前記動的に生成された秘密鍵を保持する処理と、をさらに含むことを特徴とする請求項３記載のＮＦＴアクセス制限プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限システムおよびＮＦＴアクセス制限プログラムに関する。
【背景技術】
【０００２】
ブロックチェーンとは、分散型ネットワークを構成する複数のコンピュータに暗号技術適用して、データを同期して記録する技術である。一定の期間内に生成されたデータを、ブロックごとにまとめ、コンピュータ間で相互に検証して正しい記録をチェーン（鎖）のように連結させて蓄積する。このようなブロックチェーンにおいては、一部のコンピュータでデータが改竄されたとしても、他のコンピュータとの間で、多数決によって正しいデータが選択されるため、データの改竄や不正な取引を防止することができる。
【０００３】
次に、ＮＦＴとは、「Ｎｏｎ－Ｆａｎｇｉｂｌｅ－Ｔｏｋｅｎ」の頭文字であり、Ｅｔｈｅｒｅｕｍ（登録商標）の規格であるＥＲＣ７２１に基づいて発行される唯一無二の価値を持ったトークンのことである。すなわち、代替不可能な固有のデータを持つことができるトークンであり、ブロックチェーン上に保存される。
【０００４】
特許文献１には、ブロックチェーンに登録したデータへのアクセスを制限する技術が開示されている。この技術において、パブリックブロックチェーンに登録された情報へのアクセスを制限するアクセス制限システムは、複数のユーザグループそれぞれに設けられたプライベートブロックチェーンと、データを暗号化して、パブリックブロックチェーンに登録するデータ登録部と、暗号化に利用した鍵を、データの閲覧を許可するユーザグループに設けられたプライベートブロックチェーンに登録する鍵登録部と、を備え、ブロック

チェーンに登録したデータへのアクセスを制限する。
【０００５】
　また、特許文献２には、ＵＴＸＯ（unspent transaction output）基盤プロトコルを使用して、ブロックチェーン基盤で文書を管理するための技術が開示されている。この技術では、スマートコントラクト（smart contract）を利用することによって、文書の発給、閲覧、破棄などのために必要な権限（permission)が厳格に管理され、権限のない者が任意で文書の内容を作成、その内容を閲覧するか破棄する行為を行なうことができなくなる。
【先行技術文献】
【特許文献】
【０００６】
【文献】特開２０１９－１７４９９５号公報
特表２０２０－５１７２００号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
　上述したように、ＮＦＴは、代替不可能な固有のデータを持つことができるトークンであることから、これにアクセス制限を加える必要が生じる場合がある。しかし、従来は、ＮＦＴにアクセス制限を加えるための具体的な手法については、十分に議論されていなかった。
【０００８】
　本発明は、このような事情に鑑みてなされたものであり、ブロックチェーン上に保存され、固有の価値として発行されるトークンであるＮＦＴについて、アクセス制限を加えることによって、ＮＦＴに対してセキュアな制御を行なうことができるＮＦＴアクセス制限システムおよびＮＦＴアクセス制限プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００９】
　（１）上記の目的を達成するために、本発明は、以下のような手段を講じた。すなわち、本発明のＮＦＴアクセス制限システムは、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限システムであって、アクセス制限を解除するための秘密鍵を用いて、ＮＦＴに記録されているデータにアクセス制限を設定し、前記アクセス制限が設定された制限付きＮＦＴ記録データをブロックチェーンに書き込むデータサーバと、前記アクセス制限を解除するための秘密鍵を保持するアプリケーションサーバと、を備えることを特徴とする。
【００１０】
　（２）また、本発明のＮＦＴアクセス制限システムは、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限システムであって、前記ブロックチェーンからアクセス制限が設定された制限付きＮＦＴ記録データを取得したクライアント装置によるリクエストに基づいて、アクセス制限を解除するための秘密鍵と前記リクエストとを対応付けるアプリケーションサーバと、前記秘密鍵および前記リクエストに基づいて認証を実行し、認証が得られた場合は、前記クライアント装置へＮＦＴの実データの閲覧を可能とするデータサーバと、を備えることを特徴とする。
【００１１】
　（３）また、本発明のＮＦＴアクセス制限システムにおいて、前記データサーバは、前記秘密鍵を動的に生成する秘密鍵生成部と、ＮＦＴの実データを記録するデータ記録部と、を備え、前記アプリケーションサーバは、前記動的に生成された秘密鍵を保持する秘密鍵保持部を備えることを特徴とする。
【００１２】
　（４）また、本発明のＮＦＴアクセス制限プログラムは、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限プログ

ラムであって、アクセス制限を解除するための秘密鍵を用いて、ＮＦＴに記録されているデータにアクセス制限を設定する処理と、前記アクセス制限が設定された制限付きＮＦＴ記録データをブロックチェーンに書き込む処理と、前記アクセス制限を解除するための秘密鍵を保持する処理と、の一連処理をコンピュータに実行させることを特徴とする。

【００１３】

（５）また、本発明のＮＦＴアクセス制限プログラムは、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限プログラムであって、前記ブロックチェーンからアクセス制限が設定された制限付きＮＦＴ記録データを取得したクライアント装置によるリクエストを取得する処理と、前記リクエストに基づいて、アクセス制限を解除するための秘密鍵と前記リクエストとを対応付ける処理と、前記秘密鍵および前記リクエストに基づいて認証を実行する処理と、前記認証が得られた場合は、前記クライアント装置へＮＦＴの実データの閲覧を可能とする処理と、の一連処理をコンピュータに実行させることを特徴とする。

【００１４】

（６）また、本発明のＮＦＴアクセス制限プログラムは、前記秘密鍵を動的に生成する処理と、ＮＦＴの実データを記録する処理と、前記動的に生成された秘密鍵を保持する処理と、をさらに含むことを特徴とする。

【発明の効果】

【００１５】

本発明によれば、ＮＦＴに対してセキュアな制御を行なうことが可能となる。

【図面の簡単な説明】

【００１６】

【図１】本発明の実施形態に係るＮＦＴアクセス制限システムの概略構成を示す図である。

【図２Ａ】データサーバがＮＦＴを発行する様子を示す図である。

【図２Ｂ】データサーバがＮＦＴを発行する動作を示すシーケンスチャートである。

【図３】クライアントＡがＮＦＴを取得する様子を示す図である。

【図４Ａ】クライアントＢがデータサーバからＮＦＴの実データを取得する様子を示す図である。

【図４Ｂ】クライアントＢがデータサーバからＮＦＴの実データを取得する動作を示すシーケンスチャートである。

【発明を実施するための形態】

【００１７】

本発明者らは、ブロックチェーン上に保存されるＮＦＴに着目し、「NFT JSON」などのように、ＮＦＴに記録されるデータを暗号化することによって、ＮＦＴの全部または一部にアクセス制限を加えることができることを見出し、本発明に至った。

【００１８】

すなわち、本発明のＮＦＴアクセス制限システムは、ブロックチェーンに記録されるＮＦＴ（Non-Fungible Token）にアクセス制限を設定するＮＦＴアクセス制限システムであって、アクセス制限を解除するための秘密鍵を用いて、ＮＦＴに記録されているデータにアクセス制限を設定し、前記アクセス制限が設定された制限付きＮＦＴ記録データをブロックチェーンに書き込むデータサーバと、前記アクセス制限を解除するための秘密鍵を保持するアプリケーションサーバと、を備えることを特徴とする。また、前記ブロックチェーンからアクセス制限が設定された制限付きＮＦＴ記録データを取得したクライアント装置によるリクエストに基づいて、アクセス制限を解除するための秘密鍵と前記リクエストとを対応付けるアプリケーションサーバと、前記秘密鍵および前記リクエストに基づいて認証を実行し、認証が得られた場合は、前記クライアント装置へＮＦＴの実データの閲覧を可能とするデータサーバと、を備えることを特徴とする。

【００１９】

これにより、本発明者らは、ＮＦＴに対してセキュアな制御を行なうことを可能とした。以下、本発明の実施形態について、図面を参照しながら具体的に説明する。

【００２０】
図１は、本発明の実施形態に係るＮＦＴアクセス制限システムの概略構成を示す図である。ブロックチェーン１００は、分散型ネットワークを構成する複数のコンピュータで構成され、暗号技術を適用し、データを同期して記録する。ＮＦＴ１０２は、「Ｎｏｎ－Ｆａｎｇｉｂｌｅ－Ｔｏｋｅｎ」であり、Ｅｔｈｅｒｅｕｍ（登録商標）の規格であるＥＲＣ７２１に基づいて発行される唯一無二の価値を持ったトークンである。図１に示すように、ＮＦＴ１０２は、ブロックチェーン上に保存される。
【００２１】
インターネット２００には、アプリケーションサーバ２０２およびデータサーバ２０６が接続されている。アプリケーションサーバ２０２は、ＮＦＴに記録するデータ（ＮＦＴ記録データ）に対してアクセス制限を設定し、または解除するための秘密鍵を保持する秘密鍵保持部２０４を備えている。この秘密鍵は、オープンソースである。暗号化を解除する機能を有する「アプリケーション」の形式を採り、この「アプリケーション」を保有するクライアント装置（ＰＣ、スマートフォン、タブレット等の通信機能を有する電子機器）のみにＮＦＴの実データを閲覧可能とすることができる。また、アプリケーションサーバ２０２は、アクセス権を有していて、秘密鍵を取得可能なクライアント装置に対して、データサーバ２０６からＮＦＴの実データを取得するためのツールとなるアプリケーションを、前記クライアント装置へ提供しても良い。なお、「実データ」とは、例えば、著作権で保護されている特定の人の画像、映像または文書などの情報である。
【００２２】
また、「ログイン情報」の形式を採り、この「ログイン情報」に基づいてアクセスしたクライアント装置のみにＮＦＴの実データを閲覧可能とすることができる。さらに、「時刻設定」の形式で、特定の時刻または時間帯にアクセスしたクライアント装置のみにＮＦＴの実データを閲覧可能としたり、「他のアプリケーションのアカウントの形式」で、アクセスしたクライアント装置のみにＮＦＴの実データを閲覧可能としたりすることができる。
【００２３】
データサーバ２０６は、ＮＦＴの実データを記録するデータ記録部２０８および動的に秘密鍵を生成する秘密鍵生成部２１０を備えている。データサーバ２０６は、クライアント装置からＮＦＴデータを登録する旨のリクエストを受けると、データ記録部２０８にＮＦＴの実データを記録すると共に、秘密鍵を動的に生成する。秘密鍵を動的に生成する方法については、本発明では、特に限定されず、例えば、ＸＯＲ（Exclusive OR）処理とビットの位置転換により暗号化する「秘密鍵暗号方式（ＤＥＳ方式）」や、その他の暗号化方式を採ることが可能である。そして、生成した秘密鍵を用いて、ＮＦＴ記録データの全部または一部に対してアクセス制限を加えて、ブロックチェーン１００に書き込む。
【００２４】
以上の説明では、便宜上、アプリケーションサーバ２０２とデータサーバ２０６を分離しているが、本発明は、これに限定されるわけではなく、アプリケーションサーバ２０２およびデータサーバ２０６が一体となっている態様を採っても良い。このため、以下の説明では、単に「サーバ」という場合は、アプリケーションサーバ２０２およびデータサーバ２０６の両方を意味するものとする。また、本明細書では、ＮＦＴに記録され、アクセス制限されたデータを、「制限付きＮＦＴ記録データ」と呼称すると共に、ＮＦＴに記録され、アクセス制限されていないデータを、「制限無しＮＦＴ記録データ」と呼称する。
【００２５】
クライアントＡは、インターネットに２００を介して、ブロックチェーン１００に接続可能であり、ＮＦＴ記録データを取得することが可能である。ただし、制限付きＮＦＴ記録データを閲覧することはできない。一方、クライアントＢは、インターネットに２００を介して、ブロックチェーン１００に接続可能であり、ＮＦＴ記録データを取得することが可能である。そして、制限付きＮＦＴ記録データを取得すると、アプリケーションサーバ２０２の秘密鍵に基づいて、制限付きＮＦＴ記録データのアクセス制限を解除して、制

限無しＮＦＴ記録データを生成し、制限無しＮＦＴ記録データに基づいて、データサーバ２０６からＮＦＴの実データを取得し、閲覧可能となる。

【００２６】

図２Ａは、データサーバがＮＦＴを発行する様子を示す図であり、図２Ｂは、データサーバがＮＦＴを発行する動作を示すシーケンスチャートである。クライアントＸ５００が、本実施形態に係るＮＦＴアクセス制限システムにログインし（ステップＳ１０１）、ＮＦＴデータを提供すると（ステップＳ１０２）、データサーバ２０６は、秘密鍵を動的に生成し、生成した秘密鍵に基づいて、ＮＦＴ記録データを暗号化し、「制限付きＮＦＴ記録データ２１０（例えば、公開ＵＲＬ）」を生成する（ステップＳ１０３）。データサーバ２０６は、「制限付きＮＦＴ記録データ２１０（例えば、公開ＵＲＬ）」を、クライアントＸ５００に発行する（ステップＳ１０４）。図２Ａでは、制限付きＮＦＴ記録データ２１０として、「Name」、「Description」、「URL」を含む「NFT JSON２１０」を例示しているが、これは一例であって、本発明は、これに限定されるわけではない。

【００２７】

クライアントＸ５００は、データサーバ２０６から取得した「制限付きＮＦＴ記録データ（例えば、公開ＵＲＬ）」をブロックチェーン１００に提供し、ＮＦＴ発行リクエストを行なう（ステップＳ１０５）。ブロックチェーン１００は、リクエストのあった「制限付きＮＦＴ記録データ」を、ＮＦＴ１０２として書き込み、クライアントＸ５００に対して、ＮＦＴ発行済み情報を提供する（ステップＳ１０６）。

【００２８】

ステップＳ１０３におけるデータ暗号化処理では、データサーバ２０６は、ＮＦＴ記録データの全部または一部に対してアクセス制限を加える。例えば、データサーバ２０６が、秘密鍵によってアクセス制限した「制限付きNFT JSON URLと制限付きImage URL」を発行する。そして、「制限付きNFT JSON URLと制限付きImage URL」をブロックチェーン上に書き込むようにしても良い。

【００２９】

図３は、クライアントＡがＮＦＴを取得する様子を示す図である。クライアントＡ３００は、インターネットに２００を介して、ブロックチェーン１００からＮＦＴ記録データを取得することができる。このＮＦＴ記録データが、「制限付きＮＦＴ記録データ３０２」である場合、クライアントＡ３００は、秘密鍵を入手することができないため、ＮＦＴ記録データのすべてを閲覧することはできない。図３では、クライアントＡ３００が取得したＮＦＴ記録データは、制限付きＮＦＴ記録データ３０２であり、「Name」、「Description」については閲覧可能であるが、「URL」にアクセス制限が加えられているため、クライアントＡ３００が、ＮＦＴ記録データのＵＲＬに基づいて、データサーバ２０６へアクセスしようとしても、エラーメッセージのみが返ってきて、ＮＦＴの実データを閲覧することはできない。

【００３０】

図４Ａは、クライアントＢがデータサーバからＮＦＴの実データを取得する様子を示す図であり、図４Ｂは、クライアントＢがデータサーバからＮＦＴの実データを取得する動作を示すシーケンスチャートである。クライアントＢ４００が、本実施形態に係るＮＦＴアクセス制限システムにログインし（ステップＳ２０１）、ブロックチェーン１００に対して、ＮＦＴリクエストを行なうと（ステップＳ２０２）、ブロックチェーン１００は、クライアントＢ４００に対して、ＮＦＴ（制限付きＮＦＴ記録データ）１０２を提供する（ステップＳ２０３）。クライアントＢ４００が、アプリケーションサーバ２０２に制限解除リクエストを行なうと（ステップＳ２０４）、アプリケーションサーバ２０２は、リクエストに基づいて、アクセス制限を解除するための秘密鍵とリクエストとを対応付け、データサーバ２０６は、秘密鍵およびリクエストに基づいて認証を実行する。認証が得られた場合は、データ復号化を実行し（ステップＳ２０５）、「制限無しＮＦＴ記録データ」を得る。

【００３１】

ここで、上述したように、秘密鍵の形式については、「アプリケーション」の形式、「ログイン情報」の形式、「時刻設定」の形式、または「他のアプリケーションのアカウントの形式」を採ることができる。また、ステップＳ２０４におけるクライアントＢ４００からの制限解除リクエストに基づいて、アプリケーションサーバ２０２が秘密鍵（鍵データそのもの）をクライアントＢ４００へ提供し、クライアントＢ４００が秘密鍵を用いて復号化するようにしても良い。クライアントＢ４００が制限付きＮＦＴ記録データを、秘密鍵を用いて符号化し、「制限無しＮＦＴ記録データ４０２」を得て、この「制限無しＮＦＴ記録データ」に基づいて、ＮＦＴの実データをデータサーバ２０６にリクエストしても良い。

【００３２】

図４Ｂにおいて、データ復号化がされると（ステップＳ２０５）、データサーバ２０６は、「制限無しＮＦＴ記録データ」に基づいて、ＮＦＴの実データをクライアントＢ４００へ提供する（ステップＳ２０６）。これにより、クライアントＢ４００では、制限無しＮＦＴ記録データ４０２に対応する実データを表示したり、再生したりすることが可能となる（ステップＳ２０７）。これらの動作は、例えば、クライアントＢ４００が、「制限付きNFT JSONと制限付きImage URL」を取得すると共に、アプリケーションサーバ２０２から秘密鍵を取得し、「制限付きNFT JSONと制限付きImage URL」を解除して得られた「制限無しNFT JSONと制限無しImage URL」に基づいて、データサーバ２０６から所望のデータを取得するように構成することも可能である。

【００３３】

以上説明したように、本実施形態によれば、ＮＦＴの全部または一部に閲覧制限を設定し、セキュリティを高めることが可能となる。

【００３４】

以上、本発明の実施形態について説明したが、本発明は、上述した実施形態に限るものではない。また、前述した実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、実施形態に記載されたものに限定されるものではない。本実施形態に係るアクセス制限システムは、コンピュータプログラムを実行することによって実現される。コンピュータプログラムによって実現される場合には、このコンピュータプログラムが、コンピュータにインストールされ、実行される。また、このプログラムは、ＤＶＤ－ＲＯＭのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。さらに、これらのプログラムは、ダウンロードされることなくネットワークを介したＷｅｂサービスとして、ユーザのコンピュータに提供されても良い。

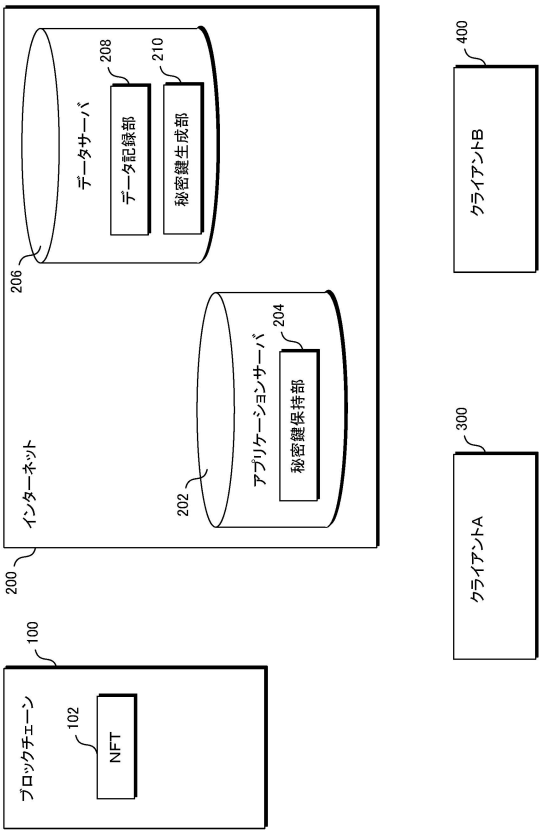
【符号の説明】

【００３５】

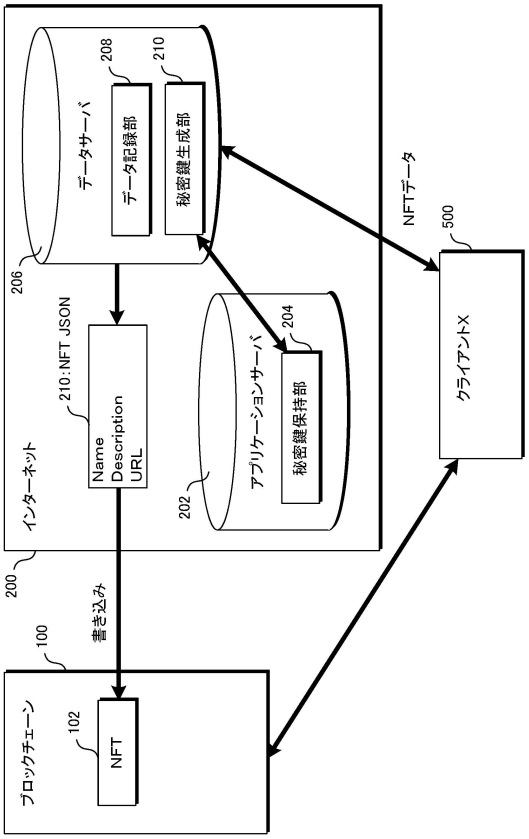
１００…ブロックチェーン
１０２…制限付きＮＦＴ記録データ
２００…インターネット
２０２…アプリケーションサーバ
２０４…秘密鍵保持部
２０６…データサーバ
２０８…データ記録部
２１０…秘密鍵生成部
２１０…ＮＦＴ　ＪＳＯＮ（制限付きＮＦＴ記録データ）
３００…クライアントＡ
３０２…制限付きＮＦＴ記録データ
４００…クライアントＢ
４０２…制限無しＮＦＴ記録データ
５００…クライアントＸ

【図面】

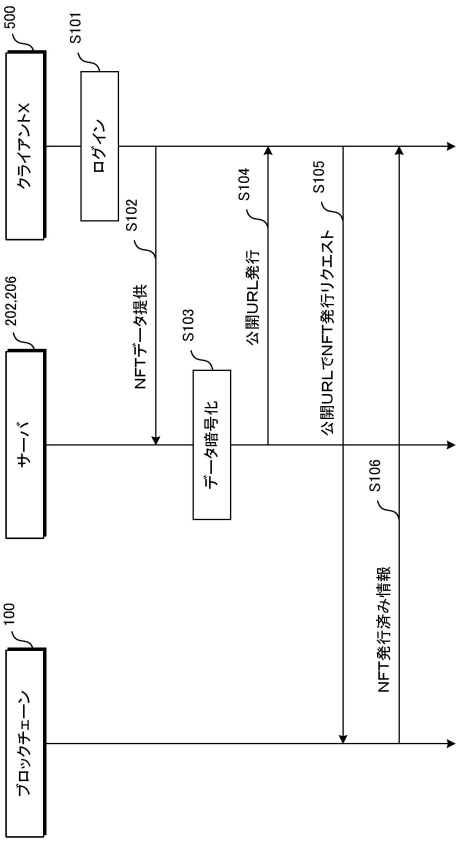
【図１】



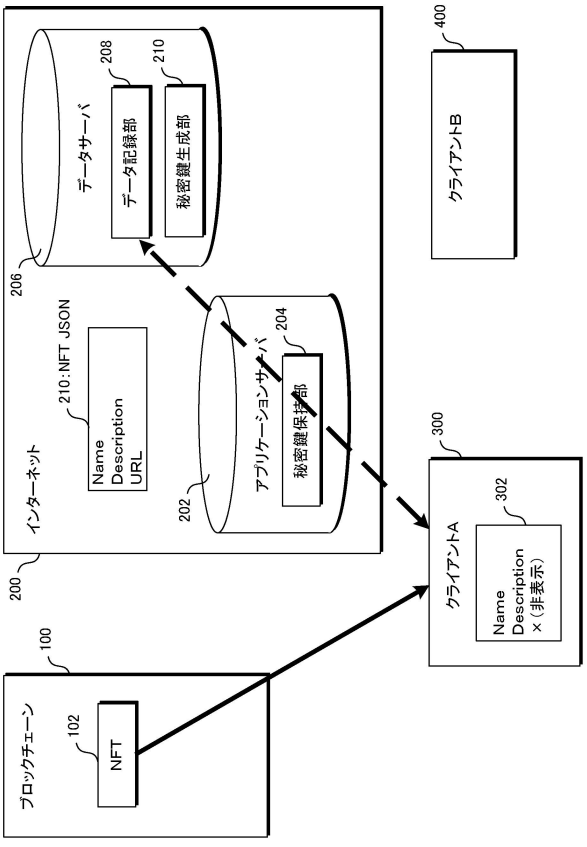
【図２Ａ】



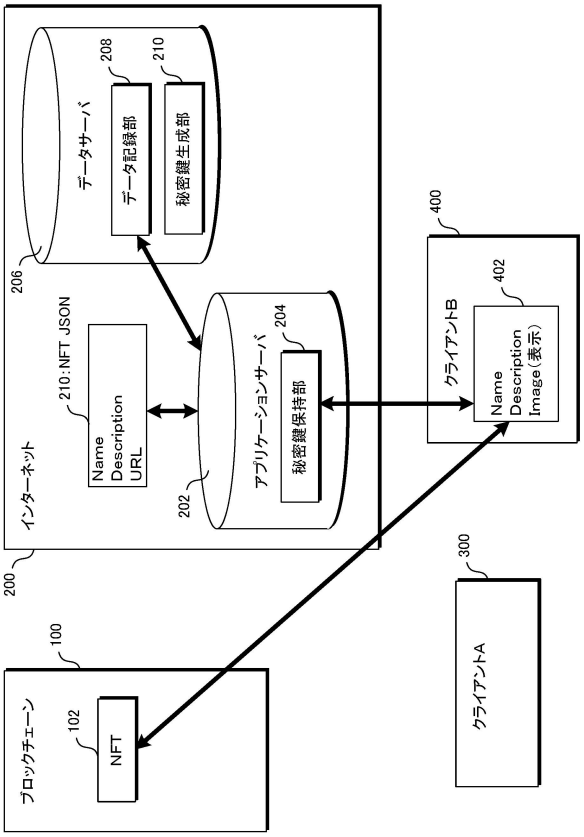
【図２Ｂ】



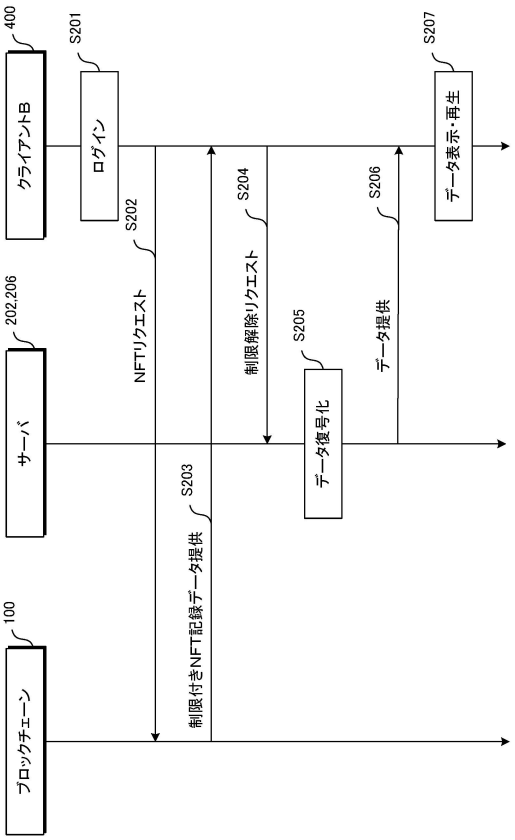
【図３】



【図４Ａ】


インターネット
200
データサーバ
206
208
データ記録部
210
秘密鍵生成部
210:NFT JSON
Name
Description
URL
アプリケーションサーバ
202
204
秘密鍵保持部
ブロックチェーン
100
102
NFT
クライアントA
300
クライアントB
400
402
Name
Description
Image(表示)

【図４Ｂ】


クライアントB
400
ログイン
S201
NFTリクエスト
S202
制限付きNFT記録データ提供
S203
制限解除リクエスト
S204
データ復号化
S205
データ提供
S206
データ表示・再生
S207
サーバ
202,206
ブロックチェーン
100

フロントページの続き

(56)参考文献 特開２０２０－８６６３４（ＪＰ，Ａ）
特開２０１９－１７４９９５（ＪＰ，Ａ）
特開２０１１－１７２０９９（ＪＰ，Ａ）
米国特許出願公開第２０２０／０１８６３３８（ＵＳ，Ａ１）
米国特許出願公開第２０１９／０３６６４７５（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０３０６９８２（ＵＳ，Ａ１）
MINACORI, V.，Using NFTs to build a CryptoGift market，[online]，2018年11月25日，URL:https://vittominacori.medium.com/using-nfts-to-build-a-cryptogift-market-c0663e851301
MINE, A.，ERC721とは？NFT（代替不可能で唯一無二なトークン）を作る標準，[onleine]，2018年10月22日，URL:https://gaiax-blockchain.com/erc721

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ２１／４４