(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6197286号
(P6197286)
(45)発行日　平成29年9月20日(2017.9.20)　(24)登録日　平成29年9月1日(2017.9.1)

(51)Int.Cl.　F I
G06F 3/12 (2006.01)　G06F 3/12 322
G06F 3/12 338
G06F 3/12 365
G06F 3/12 368
G06F 3/12 304

請求項の数 6　(全 20 頁)

(21)出願番号　特願2012-280102(P2012-280102)
(22)出願日　平成24年12月21日(2012.12.21)
(65)公開番号　特開2014-123320(P2014-123320A)
(43)公開日　平成26年7月3日(2014.7.3)
審査請求日　平成27年11月26日(2015.11.26)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　佐藤　淑美
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　三橋　竜太郎

最終頁に続く

(54)【発明の名称】通信装置、情報処理システム及び情報処理システムの制御方法

(57)【特許請求の範囲】
【請求項１】
複数の利用者で共用するゲスト機器に所定の処理を実行させる通信端末であって、
利用者のファイルを管理するデータ管理装置にログインするログイン手段と、
前記ログインしたデータ管理装置から送信される前記利用者のファイルの一覧を表示させ、前記ファイルの一覧から前記利用者によって選択されたファイルの情報を前記データ管理装置に送信するファイル選択手段と、
前記選択されたファイルを前記データ管理装置から取得するための認証情報であって、前記データ管理装置において、前記選択されたファイル及び前記認証情報の有効期限を示す情報と対応付けて管理される認証情報を、前記データ管理装置から受信するパスワード管理手段と、
前記データ管理装置を特定するための情報、及び前記認証情報を含むアクセス情報を作成し、作成した前記アクセス情報を含むＮＦＣデータを生成するＮＦＣデータ生成手段と、
前記ＮＦＣデータを受信すると、受信した前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含むかを判定し、前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含む場合には、前記データ管理装置から前記選択されたファイルを取得し前記所定の処理を実行する前記ゲスト機器に、前記ＮＦＣデータを送信するＮＦＣ通信手段と、
を有する通信端末。
【請求項２】

前記ゲスト機器は、
前記データ管理装置から、前記認証情報に対応する前記選択されたファイルを取得する手段を有する請求項１に記載の通信端末。
【請求項３】
前記データ管理装置は、
前記選択されたファイルを一時ファイルとして記憶する手段と、
前記一時ファイルと、前記一時ファイルに対応する前記認証情報との関係を管理する手段と、を有する請求項１又は２に記載の通信端末。
【請求項４】
前記データ管理装置は、
前記ゲスト機器が、前記データ管理装置からデータを取得した後に、前記認証情報を無効化する手段を有することを特徴とする請求項１乃至３のいずれか一項に記載の通信端末。
【請求項５】
複数の利用者で共用するゲスト機器と、前記ゲスト機器に所定の処理を実行させる通信端末と、利用者のファイルと管理するデータ管理装置と、を含む情報処理システムであって、
前記通信端末は、
利用者のファイルを管理するデータ管理装置にログインするログイン手段と、
前記ログインしたデータ管理装置から送信される前記利用者のファイルの一覧を表示させ、前記ファイルの一覧から前記利用者によって選択されたファイルの情報を前記データ管理装置に送信するファイル選択手段と、
前記選択されたファイルを前記データ管理装置から取得するための認証情報であって、前記データ管理装置において、前記選択されたファイル及び前記認証情報の有効期限を示す情報と対応付けて管理される認証情報を、前記データ管理装置から受信するパスワード管理手段と、
前記データ管理装置を特定するための情報、及び前記認証情報を含むアクセス情報を作成し、作成した前記アクセス情報を含むＮＦＣデータを生成するＮＦＣデータ生成手段と、
前記ＮＦＣデータを受信すると、受信した前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含むかを判定し、前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含む場合には、前記データ管理装置から前記選択されたファイルを取得し前記所定の処理を実行する前記ゲスト機器に、前記ＮＦＣデータを送信するＮＦＣ通信手段と、
を有する情報処理システム。
【請求項６】
複数の利用者で共用するゲスト機器と、前記ゲスト機器に所定の処理を実行させる通信端末と、利用者のファイルと管理するデータ管理装置と、を含む情報処理システムの制御方法であって、
前記通信端末が、
利用者のファイルを管理するデータ管理装置にログインするステップと、
前記ログインしたデータ管理装置から送信される前記利用者のファイルの一覧を表示させるステップと、
前記ファイルの一覧から前記利用者によって選択されたファイルの情報を前記データ管理装置に送信するステップと、
前記選択されたファイルを前記データ管理装置から取得するための認証情報であって、前記データ管理装置において、前記選択されたファイル及び前記認証情報の有効期限を示す情報と対応付けて管理される認証情報を、前記データ管理装置から受信するステップと、
前記データ管理装置を特定するための情報、及び前記認証情報を含むアクセス情報を作成し、作成した前記アクセス情報を含むＮＦＣデータを生成するステップと、

前記ＮＦＣデータを受信すると、受信した前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含むかを判定し、前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含む場合には、前記データ管理装置から前記選択されたファイルを取得し前記所定の処理を実行する前記ゲスト機器に、前記ＮＦＣデータを送信するステップと、

を含むことを特徴とする情報処理システムの制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信装置、情報処理システム及び情報処理システムの制御方法に関する。

【背景技術】

【０００２】

従来、サービスの利用者登録をしたユーザが、ネットワークに接続可能な情報機器を使ってサービスにアクセスし、オンラインストレージ上にファイルを保管することができるオンラインストレージサービスが広く利用されている。オンラインストレージサービスでは、ユーザはユーザ毎に割り当てられた容量に応じて、デスクトップＰＣで編集したファイル等をネットワーク上のサーバに保管することができる。その場合、ユーザはノートＰＣやタブレット端末等から上記サーバに保管されたファイルを外出先で閲覧、編集が可能である。

【０００３】

また、上記サーバに保管されたファイルは、複数のユーザによって共用される情報機器からもアクセスが可能である。例えば、オフィスやコンビニエンスストア等に設置された複合機からロケーションフリーのプリントサービスを利用して印刷することや、会議室に設置されたネットワーク接続可能なプロジェクタから映写すること等も可能である。

【０００４】

しかし、複数のユーザによって共用される情報機器からオンラインストレージ上のファイルにアクセスする際には、利用の都度、ユーザが自分のアカウント情報を手動で入力する必要があった。

【０００５】

特許文献１には、サービスを提供するプロバイダから通知された情報とユーザが設定したアクセス情報を、上記サービスを実行可能な任意のデバイスのタッチパネル等から入力することによって、ユーザのアカウント情報なしで印刷する技術が開示されている。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、引用文献１に開示の技術では、上記プロバイダから通知された情報として、データを印刷するためのＵＲＬ情報、印刷を行うためのワンタイムパスワード、さらには、ユーザが事前に設定したアクセス情報という複数のデータの入力が必要であった。

【０００７】

そのため、ユーザは、サービスを利用する度に、サービスを実行可能な任意のデバイスのタッチパネル等から、上記複数のデータを入力しなければならないという問題点があった。

【０００８】

本発明は、上記問題点を鑑みてなされたものであって、複数のユーザによって共用される情報処理装置から、サービスを提供するサーバのファイルに簡便にアクセスできる通信装置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】

上記課題を解決するため、請求項１に係る通信装置は、複数の利用者で共用するゲスト機器に所定の処理を実行させる通信端末であって、利用者のファイルを管理するデータ管理装置にログインするログイン手段と、前記ログインしたデータ管理装置から送信される

前記利用者のファイルの一覧を表示させ、前記ファイルの一覧から前記利用者によって選択されたファイルの情報を前記データ管理装置に送信するファイル選択手段と、前記選択されたファイルを前記データ管理装置から取得するための認証情報であって、前記データ管理装置において、前記選択されたファイル及び前記認証情報の有効期限を示す情報と対応付けて管理される認証情報を、前記データ管理装置から受信するパスワード管理手段と、前記データ管理装置を特定するための情報、及び前記認証情報を含むアクセス情報を作成し、作成した前記アクセス情報を含むＮＦＣデータを生成するＮＦＣデータ生成手段と、前記ＮＦＣデータを受信すると、受信した前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含むかを判定し、前記ＮＦＣデータが予め定められた形式の前記アクセス情報を含む場合には、前記データ管理装置から前記選択されたファイルを取得し前記所定の処理を実行する前記ゲスト機器に、前記ＮＦＣデータを送信するＮＦＣ通信手段と、を有する。

【発明の効果】

【００１０】

本発明の実施の形態によれば、複数のユーザによって共用される情報処理装置から、サービスを提供するサーバのファイルに簡便にアクセスできる通信装置を提供することができる。

【図面の簡単な説明】

【００１１】

【図１】一実施形態に係る情報処理システムの全体構成図である。

【図２】一実施形態に係る情報処理システムのブロック図である。

【図３】一実施形態に係る通信端末の情報処理部の構成を示すブロック図である。

【図４】一実施形態に係るゲスト機器の情報処理部の構成を示すブロック図である。

【図５】一実施形態に係る情報処理システムのシーケンスチャートである。

【図６】一実施形態に係るデータ管理装置のワンタイムパスワード発行処理のフローチャートである。

【図７】一実施形態に係る通信端末のアクセス情報送信処理のフローチャートである。

【図８】一実施形態に係るゲスト機器のアクセス情報受信後の処理のフローチャートである。

【図９】一実施形態に係るデータ管理装置のファイル提供処理のフローチャートである。

【図１０】一実施形態に係るワンタイムパスワードの期限管理処理のフローチャートである。

【図１１】一実施形態に係るNFCデータ生成手段が生成するデータフォーマット一例を示す図である。

【図１２】一実施形態に係るワンタイムパスワードの管理テーブルの一例を示す図である。

【発明を実施するための形態】

【００１２】

以下に、本発明の実施の形態について、添付の図面を参照して説明する。

【００１３】

＜システム構成＞

図１は、本発明の一実施形態に係る情報処理システムの全体構成図である。

【００１４】

情報処理システム１００は、インターネット１０４に共通に接続される、データ管理装置１０１、通信端末１０２、及びゲスト機器１０３で構成される。

【００１５】

データ管理装置１０１は、オンラインストレージサービスを提供するサーバ群で構成される。データ管理装置１０１は、インターネット１０４を介して、通信端末１０２及びゲスト機器１０３を含むクライアント機器にオンラインストレージサービスを提供する。

【００１６】

オンラインストレージサービスは、背景技術でも述べた通り、サービスに登録したユーザが、ネットワークに接続可能な情報端末からアクセスして、オンラインストレージ上にファイルを保管できるサービスである。尚、オンラインストレージサービスは、データ管理装置１０１が提供するネットワークサービスの一例であって、プリントサービスや音楽ダウンロード等の他のサービスであっても良い。

【００１７】

通信端末１０２は、インターネット１０４に接続可能な通信端末であり、好適な例としては、無線ＬＡＮや移動体通信網によりインターネット１０４に接続可能なモバイル通信端末である。通信端末１０２は、ＮＦＣ（Near Field Communication）により、ゲスト機器１０３と近接させることによりデータ通信を開始する。

【００１８】

ゲスト機器１０３は、複数のユーザで共有する、インターネット１０４に接続可能な情報機器であり、ＮＦＣにより通信端末１０２とデータの送受信が可能である。ゲスト機器１０３は、例えば、スキャナ・ファックス・コピー機能を備えた複合機、プリンタ、プロジェクタ等の情報処理装置であり、また、複数のユーザで共有するパーソナルコンピュータ等の情報処理装置であっても良い。

【００１９】

インターネット１０４は、データ管理装置１０１、通信端末１０２、ゲスト機器１０３が共通に接続されるネットワークで、企業内ネットワーク等、インターネット以外のネットワークであっても良い。

【００２０】

図１の構成において、データ管理装置１０１は、ユーザに指定されたファイルに対応する認証情報を生成する。通信端末１０２は、生成された認証情報をデータ管理装置１０１から取得し、データ管理装置１０１のＵＲＬ情報及び上記認証情報を含むアクセス情報を生成し、ＮＦＣで送信可能な構成となっている。ゲスト機器１０３は、ＮＦＣにより予め定められた形式のアクセス情報を受信すると、アクセス情報に基づいてデータ管理装置１０１にアクセスし、認証情報に対応するファイルを取得する。

【００２１】

上記構成により、ユーザは、通信端末１０２をゲスト機器１０３に近接させてＮＦＣ通信を開始することにより、自動的にゲスト機器１０３上にユーザが指定したファイルを取得し、利用できるようになる。

【００２２】

図２は、本発明の一実施形態に係る情報処理システム１００の構成を示すブロック図である。図２を参照して、情報処理システム１００の構成を説明する。

【００２３】

図１で既に説明した通り、情報処理システム１００は、インターネット１０４に共通に接続される、データ管理装置１０１、通信端末１０２、ゲスト機器１０３により構成されている。

【００２４】

<データ管理装置>

図２を参照して、まずデータ管理装置１０１の構成を説明する。

【００２５】

データ管理装置１０１は、認証機能を持つ認証サーバ２４０、オンラインストレージサービスを提供するアプリケーションサーバ２５０、及びユーザが登録したファイルを管理するためのストレージサーバ２６０で構成される。

【００２６】

認証サーバ２４０は、ユーザ情報管理手段２４１、ユーザ情報記憶手段２４２、認証手段２４３、及びネットワーク通信手段２４４で構成され、データ管理装置１０１にアクセスを要求するユーザのアカウント情報の認証を行う。

【００２７】

ユーザ情報管理手段２４１は、サービスに利用登録されているユーザの情報をユーザ情報記憶手段２４２に記憶させ管理する。

【００２８】

認証手段２４３は、ユーザ情報管理手段２４１が管理するユーザの情報に基づいて、データ管理装置１０１にアクセスを要求するユーザがサービスに利用登録されているユーザであるかどうかを認証する。

【００２９】

ネットワーク通信手段２４４は、認証サーバ２４０をインターネット１０４等のネットワークに接続する。

【００３０】

アプリケーションサーバ２５０は、一時ファイル管理手段２５１、一時ファイル記憶手段２５２、ワンタイムパスワード管理手段２５３、ファイル選択手段２５４、ファイル提供手段２５５及びネットワーク通信手段２５６で構成される。アプリケーションサーバ２５０は、オンラインストレージサービスの提供に係る処理を行う。

【００３１】

ファイル選択手段２５４は、サービスに登録されているユーザがストレージサーバに保存しているファイル一覧を作成して通信端末１０２に送信し、通信端末１０２を介してユーザが指定したファイル情報を取得する。

【００３２】

一時ファイル管理手段２５１は、ユーザから指定されたファイルを一時ファイルとして、一時ファイル記憶手段２５２に記憶させ、管理する。

【００３３】

ワンタイムパスワード管理手段２５３は、一時ファイル記憶手段２５２に記憶された一時ファイルに対応するワンタイムパスワードを生成し、管理する。尚、ワンタイムパスワードについては後述する。

【００３４】

ファイル提供手段２５５は、ゲスト機器１０３からのアクセス要求に応じて、ファイルを提供する処理を行う。

【００３５】

ネットワーク通信手段２５６は、アプリケーションサーバ２５０をインターネット１０４等のネットワークに接続する。

【００３６】

ストレージサーバ２６０は、ファイル管理手段２６１、ストレージ手段２６２、及びネットワーク通信手段２６３で構成され、サービスに登録されているユーザが登録したファイルを記憶し、管理する。

【００３７】

ファイル管理手段は、オンラインストレージサービスに登録されているユーザが登録したファイルをストレージ手段２６２に保存して管理する。

【００３８】

ネットワーク通信手段２６３は、ストレージサーバ２６０をインターネット１０４等のネットワークに接続する。

【００３９】

上記構成により、データ管理装置１０１は、ユーザにオンラインストレージサービスを提供する。

【００４０】

＜通信端末＞

次に、図２を参照して、通信端末１０２の構成について説明する。

【００４１】

通信端末１０２は、ＮＦＣ通信部２１１、表示制御部２１２、入力制御部２１３、ネットワーク通信部２１４、情報処理部２１５、及びデータ記憶部２１６を備えている。

【００４２】
ＮＦＣ通信部２１１は、ＮＦＣと呼ばれる非接触ＩＣ等を含む無線通信規格により、他のＮＦＣ対応機器と近接させることにより、非接触でデータ通信を行うものである。通信端末１０２のＮＦＣ通信部２１１をゲスト機器１０３のＮＦＣ通信部２２４の通信範囲内（例えば１０ｃｍ以内等）に位置させることにより、ゲスト機器１０３のＮＦＣ通信部２２４とデータの通信を行う。
【００４３】
表示制御部２１２は、通信端末１０２の表示部に、ログイン画面、ファイル選択画面を表示させる。
【００４４】
入力制御部２１３は、ユーザが通信端末１０２の入力キーやＧＵＩ（Graphical User Interface）を介して入力した情報を処理する。
【００４５】
ネットワーク通信部２１４は、通信端末１０２をインターネット１０４接続させるためのインタフェースである。ネットワーク通信部２１４は、例えば無線ＬＡＮや移動体通信網等を使って、インターネット１０４に接続可能である。尚、ネットワーク通信部２１４は、有線接続等によってインターネット１０４に接続するものであっても良い。
【００４６】
情報処理部２１５は、オンラインストレージサービスを利用するためのプログラムを実行するブロックで、例えばマイコンやＣＰＵ、メモリで実現される。尚、情報処理部２１５の機能構成については後述する。
【００４７】
データ記憶部２１６は、情報処理部２１５の制御にしたがって、処理対象のデータを記憶する。
【００４８】
この構成により、通信端末１０２は、データ管理装置１０１が提供するオンラインストレージサービスを利用することができ、またデータ管理装置１０１から取得したデータをＮＦＣで通信可能となる。
【００４９】
ここで、図３を参照して、通信端末１０２の情報処理部２１５の機能構成について説明する。
【００５０】
情報処理部２１５は、ログイン手段３０１、ファイル選択手段３０２、パスワード管理手段３０３、ＮＦＣデータ生成手段３０４を有する。
【００５１】
また、図２において、表示制御部２１２と入力制御部２１３を別々の構成として説明したが、ＧＵＩによってデータの入出力を行う場合には図３のように入出力制御を合わせて行う入出力制御部３０５としても良い。
【００５２】
ログイン手段３０１は、ユーザにデータ管理装置１０１が提供するオンラインストレージサービスにアクセスするための機能を提供する。ログイン手段３０１は、入出力制御部３０５にオンラインストレージサービスのログイン画面を表示させ、ユーザが入力したアカウント情報を用いてデータ管理装置１０１へのログイン処理を行う。また、通信端末１０２が、ユーザの専用端末である場合には、ログイン手段３０１は、ユーザ情報を記憶しておくことにより、ユーザが利用する度にアカウント情報の入力する手間を省くことができる。
【００５３】
ファイル選択手段３０２は、ログイン後にデータ管理装置１０１から送られてくるファイルの一覧を入出力制御部３０５に表示させ、ユーザに必要なファイルを選択させる。
【００５４】

ユーザがファイルを指定すると、ファイル選択手段３０２は、指定されたファイルの情報をデータ管理装置１０１に送信し、ワンタイムパスワードの発行を要求する。ワンタイムパスワードは、上記指定されたファイルにアクセスするための認証情報であり、データ管理装置１０１によって生成される。

【００５５】

パスワード管理手段３０３は、データ管理装置１０１が生成したワンタイムパスワードを受信し、受信したワンタイムパスワードをデータ記憶部２１６に記憶させて管理する。

【００５６】

ＮＦＣデータ生成手段３０４は、少なくとも、データ管理装置１０１へのアクセス先を特定するための情報及び指定したファイルに対応するワンタイムパスワードを含むアクセス情報を作成する。さらに、ＮＦＣデータ生成手段３０４は、上記アクセス情報を含むＮＦＣで送信可能なデータを生成する。

【００５７】

尚、ＮＦＣデータ生成手段３０４によって生成されたＮＦＣで送信可能なデータのフォーマットは、ゲスト機器１０３がアクセス情報であると認識できるように予め定められた形式であれば、任意で良い。従って、ここでは敢えてアクセス情報の具体的な構成を特定せず、一例を上げて概要のみを説明する。

【００５８】

図１１に、ＮＦＣデータ生成手段３０４が生成するデータフォーマットの一例を示す。

【００５９】

図１１の下の図は、ＮＦＣデータ生成手段３０４が作成するアクセス情報の例である。図１１のサービス種別には、本メッセージがオンラインストレージサービスに係るメッセージであることを示す値を設定する。メッセージタイプには、ゲスト機器１０３の具体的な動作、例えば、印刷、表示、データ取得、データ消去等を示す値を設定する。

【００６０】

ここで、サービス種別、メッセージタイプに設定する値は、システム毎に予め定められた値であって、通信端末１０２のNFCデータ生成手段３０４、及びゲスト機器１０３のデータ判定手段４０１が同じ値を使用する。

【００６１】

また、URL情報のエリアには、オンラインストレージサービスへのアクセス先を特定するための情報を設定し、そのデータ長をURLデータ長に設定する。

【００６２】

さらに、ワンタイムパスワードのエリアには、データ管理装置１０１から提供されたワンタイムパスワードを設定し、そのデータ長をPWデータ長に設定する。

【００６３】

このアクセス情報を、NFC通信で送信する際には、NFC通信で定められたメッセージフォーマットでカプセル化して送信すれば良い。

【００６４】

例えば、図１１を参照して、上の図をNFC通信部２１１とNFC通信部２２４との間でデータを送信する場合のフォーマットであるとする。ヘッダ（Header）部分には、ペイロード（PAYLOAD）のデータ長が含まれ、任意のサイズのデータを送信可能である。

【００６５】

ここで、通信端末１０２が上記アクセス情報をゲスト機器１０３に送信する場合には、ヘッダ部分に上記アクセス情報のデータ長を設定し、ペイロード部分に上記アクセス情報を設定して送信すれば良い。

【００６６】

尚、図１１の構成は、あくまでもＮＦＣデータ生成手段３０４が生成するデータの一例であって、本発明の範囲を限定するものではない。

例えば、図１１のように既存のNFCメッセージでカプセル化を行うのではなく、新たなNFCメッセージを定義しても良いことは言うまでもない。

【００６７】
また、本実施の形態では、データ管理装置１０１へアクセスするためのＵＲＬ情報は、通信端末１０２が本サービスに登録した際に取得して保持している情報を使用する。但し、変形例として、ワンタイムパスワード発行時に、データ管理装置１０１から通知を受けるようにしても良いことは言うまでもない。
【００６８】
また、ゲスト機器１０３が対応する複数のオンラインストレージサーバのＵＲＬ情報を有している場合には、URL情報の代わりにオンラインストレージサーバの名前や、対応する管理番号等、アクセス先を特定できるだけの情報を通知するだけでも良い。
【００６９】
尚、通信端末１０２は、上記情報処理部２１５の機能を有する専用端末である必要はない。即ち、スマートフォン等の一般的な携帯端末に、オンラインストレージサービスに対応したアプリケーションをダウンロードすることによって、上記機能を実現しても良い。
【００７０】
＜ゲスト機器＞
図２に戻って、ゲスト機器１０３の構成について説明する。
【００７１】
ゲスト機器１０３は、ネットワーク通信部２２１、出力制御部２２２、入力制御部２２３、ＮＦＣ通信部２２４、情報処理部２２５、データ記憶部２２６を備えている。
【００７２】
ネットワーク通信部２２１は、ゲスト機器１０３をインターネット１０４に接続するためのインタフェースである。
【００７３】
出力制御部２２２は、データ管理装置１０１から取得したファイル等を出力する制御を行う。具体的には、ゲスト機器１０３がプリンタであれば、取得したファイルを印刷し、プロジェクタであれば取得したファイルを投影する制御を行う。
【００７４】
入力制御部２２３は、ユーザがゲスト機器１０３の入力キーやＧＵＩ等を介して入力した情報を処理する。
【００７５】
プリンタ等の機器の操作部は、独自形状で操作手順も機種毎に異なるため、入力に手間がかかることが多い。このようなゲスト機器１０３からの入力を行うことなく、ゲスト機器１０３を利用する手段を提供することも、本発明の目的の一つである。
【００７６】
ＮＦＣ通信部２２４は、通信端末１０２がゲスト機器１０３のＮＦＣ通信部２２４の通信範囲内に位置した場合に、通信端末１０２のＮＦＣ通信部２１１とＮＦＣ通信を確立し、通信端末１０２から送信されたアクセス情報を含むデータを受信する。
【００７７】
情報処理部２２５は、データ管理装置１０１が提供するオンラインストレージサービスを利用するためのプログラムを実行するブロックで、例えばマイコンやＣＰＵ、メモリ等で実現される。尚、情報処理部２１５の機能的な構成については、後述する。
【００７８】
データ記憶部２２６は、情報処理部２２５の制御にしたがって、データを記憶する。
【００７９】
上記構成より、ゲスト機器１０３は、ＮＦＣから受信したデータに応じて、データ管理装置１０１が提供するオンラインストレージサービスを利用することができる。
【００８０】
ここで、図４を参照して、ゲスト機器１０３の情報処理部２２５の機能構成について説明する。
【００８１】

情報処理部２２５は、データ判定手段４０１、パスワード管理手段４０２、アクセス制御手段４０３、データ取得手段４０４を有している。

【００８２】

データ判定手段４０１は、ＮＦＣ通信部２２４がデータを受信すると、受信したデータが予め定められた形式のアクセス情報を含むかどうかを判定する。受信したデータが正しいアクセス情報を有していれば、そのアクセス情報は、データ管理装置１０１へアクセスするために必要な情報と、ユーザが指定したファイルへのワンタイムパスワードを有している。

【００８３】

パスワード管理手段４０２は、ＮＦＣ通信部２２４から受信したデータが予め定められた形式のアクセス情報である場合、そのアクセス情報をデータ記憶部２２６に記憶させ管理する。

【００８４】

アクセス制御手段４０３は、データ記憶部２２６に記憶されたアクセス情報に基づいて、データ管理装置１０１にアクセスを行う。より具体的には、アクセス情報に含まれるＵＲＬに、認証情報であるワンタイムパスワードを用いてアクセスを要求する。

【００８５】

データ取得手段４０４は、データ管理装置１０１からアクセス許可を受信すると、データ管理装置１０１からワンタイムパスワードに対応するデータを取得し、取得したデータをデータ記憶部２２６に記憶させる。

【００８６】

尚、ゲスト機器１０３についても、オンラインストレージサービスに対応する上記情報処理部２２５に示す機能を有している必要があるが、通信端末１０２と同様に必ずしも専用端末である必要はない。即ち、オンラインサービスに対応するアプリケーションをインストールすることによって、情報処理部２２５の機能を実現できるものであっても良い。

【００８７】

＜動作の説明＞

続いて、本発明の一実施形態に係る情報処理システムの動作を説明する。

【００８８】

図５は、情報処理システム１００における、ファイル取得手順の一例を示すシーケンスチャートである。

【００８９】

ユーザは、通信端末１０２からデータ管理装置１０１が提供するオンラインストレージサービスにインターネット１０４を介して接続し、登録済のアカウント情報でログインを要求する（処理１、２）。

【００９０】

データ管理装置１０１は、ユーザからのログイン要求を受け取ると、アカウント情報の認証を行い、アカウント情報がサービスに利用登録されたユーザのものである場合には、ユーザのログインを許可する（処理３）。

【００９１】

ユーザのログインが許可されると、データ管理装置１０１は、ユーザが登録しているファイルの一覧を通信端末１０２に送信する（処理４）。

【００９２】

ユーザは、通信端末１０２に表示されたファイルの一覧の中から、利用するファイルを選択する（処理５）。

【００９３】

通信端末１０２は、データ管理装置１０１に対して、ユーザから指定されたファイルの情報を通知し、指定されたファイルにアクセスするためのワンタイムパスワードの発行を要求する（処理６）。

【００９４】

データ管理装置１０１は、指定されたファイルを一時ファイル記憶手段２５２に一時ファイルとして記憶し、記憶された一時ファイルにアクセスするためのワンタイムパスワードを生成して記憶する（処理７）。

【００９５】

その後、データ管理装置１０１は、ワンタイムパスワードを通信端末１０２に送信する（処理８）。

【００９６】

通信端末１０２は、ワンタイムパスワードを受信すると、ワンタイムパスワードとデータ管理装置１０１のＵＲＬ情報を含むアクセス情報を予め定められた形式で作成し、ＮＦＣで送信可能なデータを作成する（処理９）。

【００９７】

その後、ユーザが、通信端末１０２をゲスト機器１０３のＮＦＣ通信部２２４に近接させると（処理１０）、通信端末１０２とゲスト機器１０３との間でＮＦＣ通信が確立される。この時、通信端末１０２からゲスト機器１０３に、ワンタイムパスワードとデータ管理装置１０１のＵＲＬ情報を含むアクセス情報が予め定められたフォーマットで送信される（処理１１）。

【００９８】

通信端末１０２は、ゲスト機器１０３へのアクセス情報の送信が完了すると、送信したワンタイムパスワードを破棄する（処理１２）。

【００９９】

ゲスト機器１０３は、ＮＦＣ通信によりデータを受信すると、受信したデータが予め定められた形式の正しいアクセス情報であるかどうかを判定する（処理１３）。

【０１００】

ゲスト機器１０３は、ＮＦＣ通信から受信したデータがアクセス情報であると判定されると、受信したアクセス情報に基づいて、データ管理装置１０１にワンタイムパスワードを用いてアクセス要求を行う（処理１４）。

【０１０１】

データ管理装置１０１は、アクセス要求に含まれるワンタイムパスワードに対応するファイルが一時ファイル記憶手段２５２にあるかどうかを検索し（処理１５）、対応するファイルが見つかった場合には、ゲスト機器１０３にアクセス許可を通知する（処理１６）。

【０１０２】

アクセス許可を受信したゲスト機器１０３は、データ管理装置１０１に指定されたファイルの取得を要求し（処理１７）、指定されたファイルを取得する（処理１８）。

【０１０３】

ゲスト機器１０３は、指定されたファイルを取得し保存（処理１９）した後で、データ管理装置１０１にファイル取得の完了を通知し（処理２０）、ワンタイムパスワードを破棄する（処理２１）。

【０１０４】

データ管理装置１０１は、ゲスト機器１０３からファイル取得の完了の通知を受けると、ワンタイムパスワードを無効化する（処理２２）。

【０１０５】

ゲスト機器１０３は、指定されたファイルを、自動的に、またはユーザ操作に応じて、印刷、表示等、出力を行う（処理２３）。

【０１０６】

ゲスト機器は、指定されたファイルを出力した後、必要に応じて削除する（処理２４）。

【０１０７】

以上、図５のシーケンスによれば、ユーザは、通信端末１０２からファイルを指定し他後、ゲスト機器１０３のＮＦＣ部に通信端末１０２を近接させるだけで、指定したファイ

ルにアクセスするために必要な情報をゲスト機器１０３に入力できる。
【０１０８】
そのため、ユーザは操作部からアカウント情報や、ワンタイムパスワード等を直接入力することなく、指定されたファイルをゲスト機器１０３から出力することができる。また、指定されたファイルを出力した後に、指定されたファイルやワンタイムパスワードが削除されるので、不正なユーザからの利用を防ぐことができる。
【０１０９】
次に、図２及び図６を参照して、データ管理装置１０１のワンタイムパスワード発行処理の手順について、さらに詳しく説明する。
【０１１０】
データ管理装置１０１が通信端末１０２からログイン要求を受信すると（Ｓ６０１）、ユーザ情報管理手段２４１は、ユーザ情報記憶手段２４２に記憶されているオンラインストレージサービスのユーザ情報に基づいて、ログイン要求の認証を行う（Ｓ６０２）。
【０１１１】
ユーザ情報管理手段２４１が、ログインユーザがサービスに登録済みのユーザであると判断した場合、ファイル選択手段２５４は、ストレージサーバ２６０にユーザが保存しているファイルの一覧を作成し、通信端末１０２に送信する（Ｓ６０３）。
【０１１２】
一方、ユーザ情報管理手段２４１が、ログインユーザがサービスに登録されているユーザではないと判断した場合には、ログイン失敗として処理を終了する（Ｓ６０４）。
【０１１３】
ファイル選択手段２５４がファイルの一覧を通信端末１０２に送信した後、通信端末１０２から、ファイルを指定し、ワンタイムパスワードの発行を要求するメッセージを受信（Ｓ６０５）する。
【０１１４】
ここで、一時ファイル管理手段２５１は、ストレージサーバ２６０に記憶されているユーザのデータの中から、指定されたファイルを取得し、一時ファイル記憶手段２５２に記憶させる（Ｓ６０６）。
【０１１５】
次に、ワンタイムパスワード管理手段２５３は、一時ファイル記憶手段２５２に保存されたファイルにアクセスするためのワンタイムパスワードを生成し、生成されたワンタイムパスワードを通信端末１０２に通知する（Ｓ６０７）。
【０１１６】
ここで、ワンタイムパスワード管理手段２５３は、一時ファイル記憶手段２５２に保存されたファイルのファイル名、保存場所、発行日時、またワンタイムパスワードの満了日時等との対応関係を、例えば図１２のようなテーブル形式で管理しても良い。
【０１１７】
尚、図１２のワンタイムパスワード部分のサイズは、システムに応じて必要な長さに設定する。
【０１１８】
本実施の形態では、ワンタイムパスワードをＮＦＣ通信で送信するため、ワンタイムパスワードを手で入力するときのようにワンタイムパスワードの長さを短く制限する必要がないので、ワンタイムパスワードの長さを十分に長く設定することができる。
【０１１９】
従って、ワンタイムパスワード管理手段２５３は、管理するファイルの数が増大した場合でも、ファイル毎にユニークなワンタイムパスワードを発行可能であり、ワンタイムパスワードのみで、ファイルの特定、管理が可能となる。
【０１２０】
ワンタイムパスワード管理手段２５３は、ワンタイムパスワードが、対応する一時ファイルと１対１に対応するように、ユニークな値のワンタイムパスワードを生成する。例え

ば、ワンタイムパスワードを生成した日時、ファイル名等に基づいてワンタイムパスワードを作成しても良い。また、日時、ファイル名に乱数を合わせて使用しても良い。

【０１２１】

本実施の形態では、ワンタイムパスワード管理手段２５３によって正当な手続きで生成されたワンタイムパスワードは、対応するファイルが一時ファイル記憶手段２５２に保存されている。従って、ワンタイムパスワードに該当するファイルが一時ファイル記憶手段２５２に無い場合には、不正なワンタイムパスワードと判断できる。

【０１２２】

以上より、本実施の形態に係るワンタイムパスワードは、一時ファイル記憶手段２５２上の対応するファイルを特定する情報であると共に、ワンタイムパスワードの正当性を確認する認証情報でもある。

【０１２３】

次に、図３及び図７を参照して、通信端末１０２のＮＦＣ通信によるデータ送信処理の手順について説明する。

【０１２４】

ユーザは、通信端末１０２を指定のファイルを出力したいゲスト機器１０３のＮＦＣ通信部２２４に近接させる（かざす）ことによって、ＮＦＣ通信を開始させる（Ｓ７０１）。

【０１２５】

これにより、通信端末１０２のＮＦＣ通信部２１１は、ゲスト機器１０３のＮＦＣ通信部２２４と自動的にＮＦＣ通信を確立する（Ｓ７０２）。

【０１２６】

このとき、通信端末１０２のＮＦＣデータ生成手段３０４によって生成された、予め定められた形式のアクセス情報は、ゲスト機器１０３に送信される（Ｓ７０３）。

【０１２７】

通信端末１０２のパスワード管理手段３０３は、アクセス情報がゲスト機器１０３に正しく送信されたことを（Ｓ７０４）を確認した後、必要に応じて、記憶しているワンタイムパスワードを破棄（削除）する（Ｓ７０５）。

【０１２８】

次に、図４及び図８を参照して、通信端末１０２からアクセス情報を受信した後のゲスト機器１０３のファイル取得動作の処理について説明する。

【０１２９】

通信端末１０２のＮＦＣ通信部２２４からデータを受信すると、ゲスト機器１０３のデータ判定手段４０１は、受信データが予め定められた形式のアクセス情報を含むかどうかを判定する（Ｓ８０１、Ｓ８０２）。

【０１３０】

データ判定手段４０１が、受信したデータが正しいアクセス情報ではないと判定した場合には、処理を終了する。

【０１３１】

一方、データ判定手段４０１が、受信したデータが正しいアクセス情報であると判定した場合、パスワード管理手段４０２は、アクセス情報をデータ記憶部２２６に記憶させる（Ｓ８０３）。

【０１３２】

次に、アクセス制御手段４０３は、データ記憶部２２６に記憶されたアクセス情報を用いて、データ管理装置１０１にアクセスを要求する（Ｓ８０４）。

【０１３３】

Ｓ８０５において、アクセスに失敗した場合、例えば、データ管理装置から該当するファイルが無い旨の通知を受けた場合には、アクセス制御手段は、エラーを表示して処理を終了させる（Ｓ８０７）。

【０１３４】

一方、Ｓ８０５においてアクセスに成功すると、データ取得手段４０４はデータ管理装置１０１から指定されたファイルをダウンロードし（Ｓ８０６）、取得したファイルをデータ記憶部２２６に保存する（Ｓ８０８）。

【０１３５】

取得したファイルを保存した後、データ取得手段４０４は、データ管理装置１０１にデータの取得完了を通知する（Ｓ８０９）。

【０１３６】

その後、アクセス制御手段４０３は、データの取得・保存が完了したファイルに対応するアクセス情報をデータ記憶部２２６から削除する（Ｓ８１０）。

【０１３７】

次に、図２及び図９を参照して、データ管理装置１０１側のファイル提供動作の処理について説明する。

【０１３８】

ファイル提供手段２５５が　アクセス要求を受信（Ｓ９０１）すると、ワンタイムパスワード管理手段２５３は、アクセス要求に含まれるワンタイムパスワードに対応するファイルが一時ファイル記憶手段２５２に記憶されているかどうか検索する（Ｓ９０３）。

【０１３９】

ワンタイムパスワードに対応するファイルが見つかった場合には、ファイル提供手段２５５は、一時ファイル記憶手段２５２に記憶された、ワンタイムパスワードに対応するファイルへのアクセスをゲスト機器１０３に許可する（Ｓ９０４）。

【０１４０】

また、ワンタイムパスワードに対応するファイルが見つからなかった場合には、ファイル提供手段２５５は、該当するファイルが無い旨をゲスト機器１０３に通知する（Ｓ９０５）。

【０１４１】

ゲスト機器１０３がワンタイムパスワードに対応するファイルを取得（Ｓ９０６）した後、ファイル提供手段２５５がファイル取得完了の通知を受信すると（Ｓ９０７）、ワンタイムパスワード管理手段２５３は、ワンタイムパスワードを無効化する（Ｓ９０８）。

【０１４２】

その後、一時ファイル管理手段２５１は、無効化されたワンタイムパスワードに対応するファイルを、一時ファイル記憶手段２５２から削除する（Ｓ９０９）。

【０１４３】

次に、図１０と図１２を参照して、データ管理装置１０１のワンタイムパスワードの期限管理に関する処理ついて説明する。

【０１４４】

これは、発行されたワンタイムパスワードが使用されなかった場合に、一時ファイル記憶手段２５２に記憶された上記ワンタイムパスワードに対応するファイルが溜まってしまうことに対応する処理である。

【０１４５】

ワンタイムパスワード管理手段２５３は、定期的にワンタイムパスワードの有効期限を確認する（Ｓ１００１）。

【０１４６】

ワンタイムパスワード管理手段２５３は、ワンタイムパスワードを生成すると、図１２に示すワンタイムパスワード管理テーブルで、ワンタイムパスワードと一時ファイルとの関係を管理すると共に、ワンタイムパスワードの満了日時も管理する。

【０１４７】

ワンタイムパスワード管理手段２５３は、満了日時を過ぎたワンタイムパスワードを期限切れと判断し、無効化または削除する（Ｓ１００２）。

【０１４８】

一時ファイル管理手段２５１は、無効化または削除されたワンタイムパスワードに対応

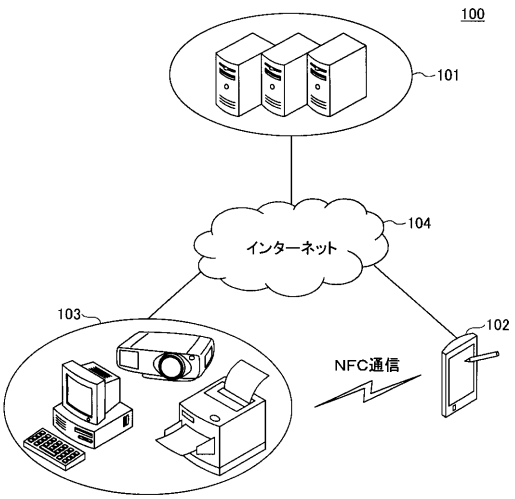
するファイルを、一時ファイル記憶手段２５２から削除する（Ｓ１００３）。
【０１４９】
上記処理により、一時ファイル記憶手段２５２に不要なデータが蓄積されていくことを防止できる。
【０１５０】
以上、本実施の形態によれば、ゲスト機器１０３は、ＮＦＣ通信により予め定められた形式のアクセス情報を受信すると、自動的にデータ管理装置１０１にアクセスするので、ゲスト機器１０３の操作部を操作することなく、簡便に所望のファイルにアクセスできる。従って、通信端末１０２をゲスト機器１０３のＮＦＣ部にかざすだけで、自動的にゲスト機器１０３から所望のファイルを印刷する、または表示する出力機器を実現可能である。
【０１５１】
また、データ管理装置１０１は、ユーザが指定したファイルを一時ファイル記憶手段２５２に一時ファイルとして保存し、対応するワンタイムパスワードと関連付けて管理するため、ワンタイムパスワードに対応する指定されたファイルを短時間で提供できる。
【０１５２】
また、ユーザが指定したファイルに対応するワンタイムパスワードをＮＦＣ通信で受信するため、手入力の時よりも十分に長く設定できる。このため、データ管理装置１０１は、ワンタイムパスワードだけで、ユーザが指定したファイルを特定可能となり、また同時に十分なセキュリティが確保できる。
【０１５３】
なお、本実施の形態は本発明の範囲を限定するものではない。
【０１５４】
例えば、通信端末１０２で行っているデータ管理装置１０１のＵＲＬ情報とワンタイムパスワードを含むアクセス情報を生成する手段を、データ管理装置１０１で行って、通信端末１０２に通知する構成としても良い。
【０１５５】
また、データ管理装置１０１を３つのサーバとして説明したが、１つ以上の任意の数のサーバで実現しても良い。
【０１５６】
また、ワンタイムパスワードを１回のみ利用可能なものとして説明したが、２回以上の回数制限を持つ回数制限付のパスワードとしても良い。さらに、ワンタイムパスワードに回数制限を設けず、期限内であれば何回でも利用可能な期限付パスワードとしても良い。
【０１５７】
また、データ管理装置１０１が提供するサービスを、ユーザファイルを保存可能なオンラインストレージサービスとして説明したが、音楽、映像、ゲーム等を提供するコンテンツサービスとしても良い。
【０１５８】
なお、本実施の形態で説明したシステム構成は一例であり、用途や目的に応じて様々なシステム構成があることは言うまでもない。
【符号の説明】
【０１５９】
１００　情報処理システム
１０１　データ管理装置
１０２　通信端末
１０３　ゲスト機器
２１１　ＮＦＣ通信部
２１２　表示制御部
２１３　入力制御部
２１４　ネットワーク通信部

２１５　情報処理部
２１６　データ記憶部
２２１　ネットワーク通信部
２２２　出力制御部
２２３　入力制御部
２２４　ＮＦＣ通信部
２２５　情報処理部
２２６　データ記憶部
２４０　認証サーバ
２４１　ユーザ情報管理手段
２４２　ユーザ情報記憶手段
２４３　認証手段
２４４　ネットワーク通信手段
２５０　アプリケーションサーバ
２５１　一時ファイル管理手段
２５２　一時ファイル記憶手段
２５３　ワンタイムパスワード管理手段
２５４　ファイル選択手段
２５５　ファイル提供手段
２５６　ネットワーク通信手段
２６０　ストレージサーバ
２６１　ファイル管理手段
２６２　ストレージ手段
２６３　ネットワーク通信手段
３０１　ログイン手段
３０２　ファイル選択手段
３０３　パスワード管理手段
３０４　ＮＦＣデータ生成手段
４０１　データ判定手段
４０２　パスワード管理手段
４０３　アクセス制御手段
４０４　データ取得手段

【先行技術文献】
【特許文献】
【０１６０】
【特許文献１】特開２００６－１６４１５８号公報

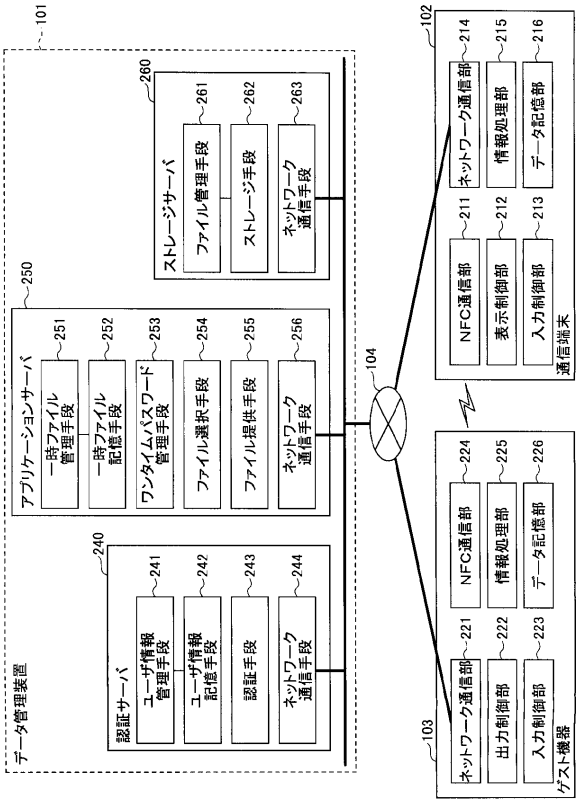
【図１】

一実施形態に係る情報処理システムの全体構成図



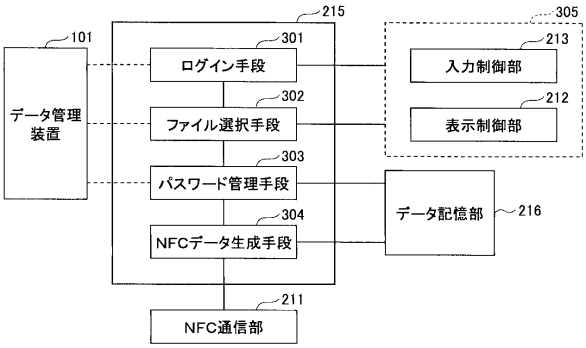
【図２】

一実施形態に係る情報処理システムのブロック図



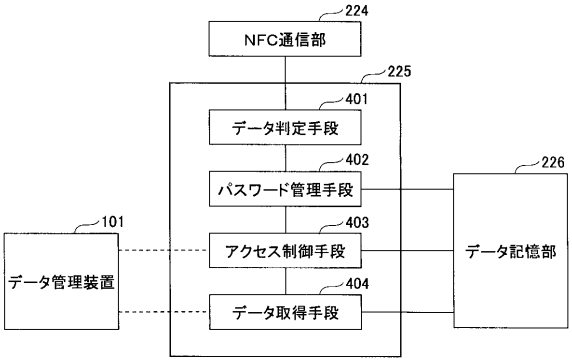
【図３】

一実施形態に係る通信端末の情報処理部の構成を示すブロック図



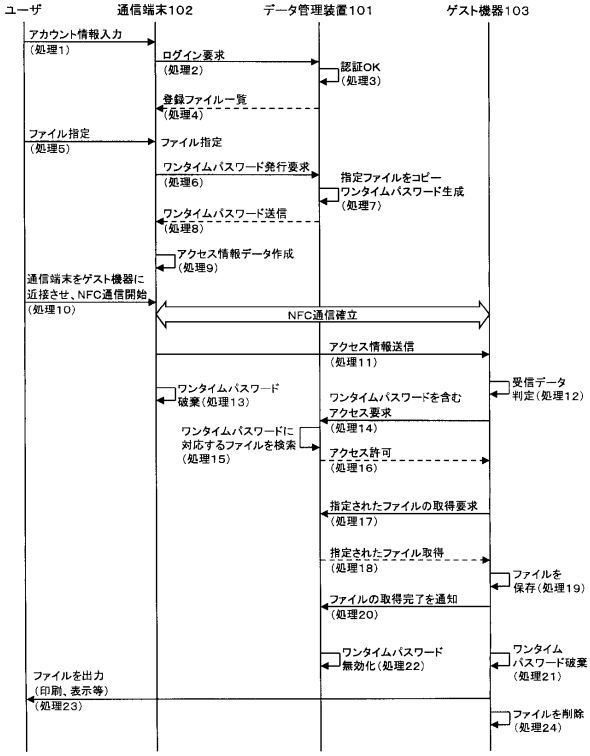
【図４】

一実施形態に係るゲスト機器の情報処理部の構成を示すブロック図



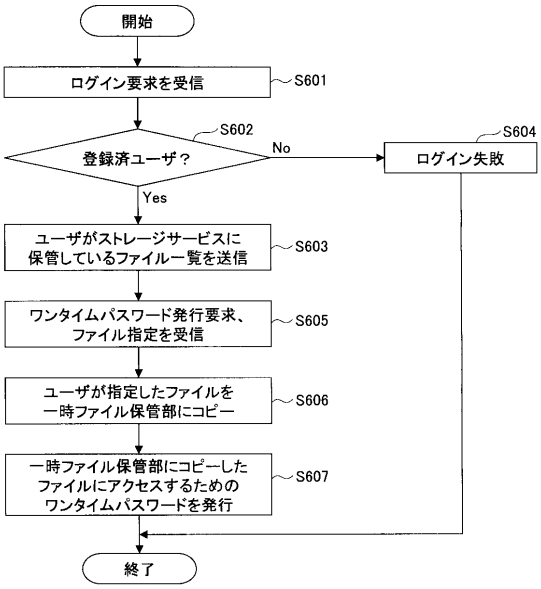
【図５】

一実施形態に係る情報処理システムのシーケンスチャート



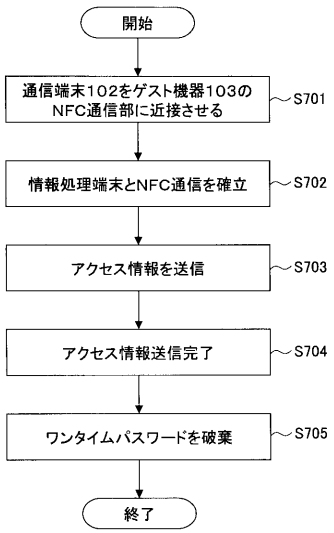
【図６】

一実施形態に係るデータ管理装置のワンタイムパスワード発行処理のフローチャート



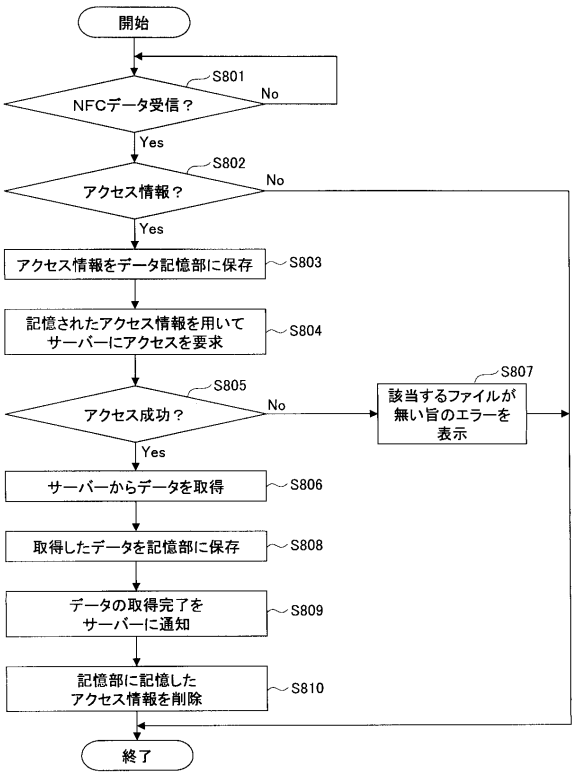
【図７】

一実施形態に係る通信端末のアクセス情報送信処理のフローチャート



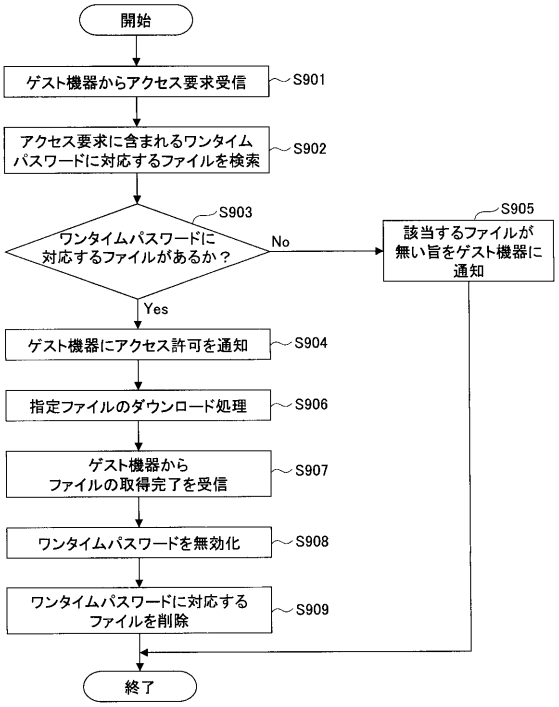
【図８】

一実施形態に係るゲスト機器のアクセス情報受信後の処理のフローチャート



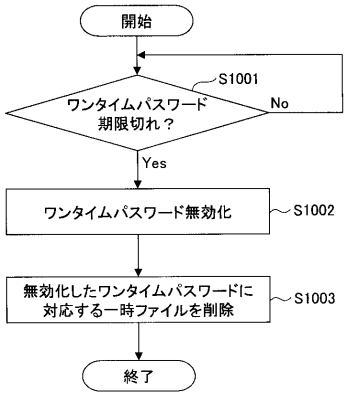
【図９】

一実施形態に係るデータ管理装置のファイル提供処理のフローチャート



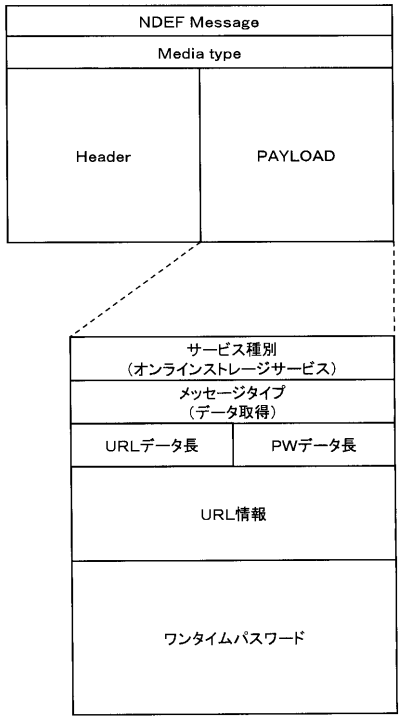
【図１０】

一実施形態に係るワンタイムパスワードの期限管理処理のフローチャート



【図１１】

一実施形態に係るNFCデータ生成手段が生成する
データフォーマット一例を示す図



【図１２】

一実施形態に係るワンタイムパスワードの管理テーブルの一例を示す図

発行日時	満了日時	ファイル名	ディレクトリ	ワンタイムパスワード
yyyymmdd hhmm	YYYYMMDD HHMM	xxxxxxx.doc	¥¥temp_drive¥yymmdd¥	xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

フロントページの続き

(56)参考文献 特開２０１２－０６４０３０（ＪＰ，Ａ）
特開２００６－１６４１５７（ＪＰ，Ａ）
特開２０１２－１９００７４（ＪＰ，Ａ）
国際公開第２０１０／０７３７３２（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　３／０９－３／１２