

明 細 書

発明の名称：

情報処理装置、情報処理方法、プログラム及び記録媒体

技術分野

[0001] 本発明は、暗号化された情報を取り扱う情報処理装置、情報処理方法、プログラム及び記録媒体に関する。

背景技術

[0002] 従来からセキュリティを確保するために電子ファイルやフォルダに暗号を付与することは知られている。このような暗号を付与する態様として、送信端末が、所定のパスワードを受信側メールアドレスと関連付けて記憶部に記憶し、電子メールに添付されるファイルを、受信側メールアドレスと関連付けて記憶されている所定のパスワードを用いて復号できるように暗号化し、受信側端末が所定のパスワードを送信側メールアドレスと関連付けて記憶部に記憶し、受信端末が、送信側メールアドレスと関連付けて記憶されている所定のパスワードを用いて、暗号化されたファイルを復号することが提案されている（特許文献1参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開2017-167796号公報

発明の概要

発明が解決しようとする課題

[0004] このような態様では、送信端末及び受信端末の各々に専用のアプリケーションがインストールされている必要がある。

[0005] 本発明は、受信側端末において専用のアプリケーションがインストールされていなくても暗号化された情報を受信側端末で確認できる情報処理装置、情報処理方法、プログラム及び記録媒体を提供する。

課題を解決するための手段

[0006] [概念 1]

本発明による情報処理装置は、
ユーザ端末からの情報を受信する受信部と、
前記ユーザ端末からの情報に基づいてユーザの識別を行うとともに、対象となっているファイルを閲覧できるか否かを判断する識別判断部と、
前記識別判断部によって前記ユーザが前記ファイルを閲覧できると判断された場合に、暗号化されたファイルを復号する復号部と、
を備えてもよい。

[0007] [概念 2]

本発明の概念 1 による情報処理装置において、
前記受信部は、前記ユーザ端末から暗号化された第一ファイルを受信し、
前記復号部は、前記暗号化された第一ファイルを復号し、
前記復号された第一ファイルを、前記ユーザ端末のブラウザで表示可能な形式からなる第二ファイルに変換する変換部が設けられてもよい。

[0008] [概念 3]

本発明の概念 2 による情報処理装置は、
前記ユーザ端末に対して情報を送信する送信部と、
前記第二ファイルを暗号化する暗号化部と、をさらに備え、
前記送信部は、前記暗号化部で暗号化された第二ファイルを前記ユーザ端末に送信してもよい。

[0009] [概念 4]

本発明の概念 3 による情報処理装置は、
前記送信部が前記暗号化された第二ファイルを前記ユーザ端末に送信した後で、前記暗号化された第二ファイルを消去する消去部をさらに備えてもよい。

[0010] [概念 5]

本発明の概念 2 乃至 4 による情報処理装置は、

前記ユーザ端末に対して情報を送信する送信部をさらに備え、
前記受信部は、前記暗号化された第二ファイルの部分的な情報を前記ユーザ端末から受信し、
前記復号部は、前記ユーザ端末から受信する前記暗号化された第二ファイルの部分的な情報を復号し、
前記送信部は、復号された前記第二ファイルの部分的な情報を前記ユーザ端末に送信してもよい。

[0011] [概念 6]

本発明の概念 5 による情報処理装置において、
前記受信部は、前記暗号化された第二ファイルの部分的な情報を n バイト単位（「 n 」は 10, 240 以上の整数である。）で前記ユーザ端末から受信し、
前記復号部は、前記ユーザ端末から受信する前記暗号化された第二ファイルの部分的な情報を n バイト単位で復号し、
前記送信部は、復号された前記第二ファイルの部分的な情報を n バイト単位で前記ユーザ端末に送信してもよい。

[0012] [概念 7]

本発明の概念 2 乃至 6 による情報処理装置は、
前記第一ファイルは所定の拡張子からなるラップファイル内に格納されており、
前記ラップファイルが実行されることで、前記受信部がユーザ端末からの情報を受信してもよい。

[0013] [概念 8]

本発明の概念 1 乃至 7 による情報処理装置は、
前記ユーザ端末に対して情報を送信する送信部をさらに備え、
前記受信部は、前記ユーザ端末から暗号化された第一ファイルを受信し、
前記復号部は、前記暗号化された第一ファイルを復号し、
前記復号された第一ファイルを第二ファイルに変換する変換部が設けられ

、
前記送信部は、前記変換部で変換された第二ファイルを前記ユーザ端末に送信してもよい。

[0014] [概念 9]

本発明の概念 1 乃至 8 による情報処理装置は、
前記ユーザ端末に対して情報を送信する送信部をさらに備え、
前記受信部は、暗号化された第三ファイルの部分的な情報を前記ユーザ端末から受信し、
前記復号部は、前記暗号化された第三ファイルの部分的な情報を復号し、
前記送信部は、復号された前記第三ファイルの部分的な情報を前記ユーザ端末に送信してもよい。

[0015] [概念 10]

本発明の概念 9 による情報処理装置は、
前記第三ファイルは前記ユーザ端末のブラウザで表示可能な形式からなってもよい。

[0016] [概念 11]

本発明の概念 1 乃至 10 による情報処理装置は、
前記ユーザ端末に対して情報を送信する送信部と、
ファイルを暗号化する暗号化部と、をさらに備え、
前記受信部は第四ファイルをユーザ端末から受信し、
前記ユーザ端末からの情報に基づき前記識別判断部によって前記ユーザがファイルを暗号化できると判断された場合に、前記暗号化部は前記第四ファイルを暗号化し、
前記送信部は、暗号化された前記第四ファイルを前記ユーザ端末に送信してもよい。

[0017] [概念 12]

本発明による情報処理方法は、
識別判断部によって、ユーザ端末からの情報に基づいてユーザの識別を行

うとともに、対象となっているファイルを閲覧できるか否かを判断することと、

前記識別判断部によって前記ファイルを閲覧できると判断された場合に、復号部によって暗号化されたファイルを復号することと、
を備えてもよい。

[0018] [概念 1 3]

本発明によるプログラムは、
情報処理装置にインストールするプログラムであって、
前記プログラムをインストールされた情報処理装置は、
識別判断部によって、ユーザ端末からの情報に基づいてユーザの識別を行うとともに、対象となっているファイルを閲覧できるか否かを判断することと、

前記識別判断部によって前記ファイルを閲覧できると判断された場合に、復号部によって暗号化されたファイルを復号することと、
を実行可能となってもよい。

[0019] [概念 1 4]

本発明による記録媒体は、
情報処理装置にインストールするプログラムを記録した記録媒体であって、
、
前記プログラムをインストールされた情報処理装置は、
識別判断部によって、ユーザ端末からの情報に基づいてユーザの識別を行うとともに、対象となっているファイルを閲覧できるか否かを判断することと、

前記識別判断部によって前記ファイルを閲覧できると判断された場合に、復号部によって暗号化されたファイルを復号することと、
を実行可能となってもよい。

発明の効果

[0020] 本発明において、ユーザ端末からの情報に基づいてユーザの識別を行うと

ともに、対象となっているファイルを閲覧できるか否かを判断し、ファイルを閲覧できると判断された場合に暗号化されたファイルを復号する態様を採用した場合には、ファイルを復号するアプリケーションがインストールされていないユーザ端末でも、情報処理装置にアクセスすることでファイルを復号することができる。

図面の簡単な説明

[0021] [図1]図1は、本発明の第1の実施の形態による情報処理システムの構成図である。

[図2]図2は、本発明の第1の実施の形態による情報処理システムによるデータの流れを示した図である。

[図3]図3は、図2に続く、本発明の第1の実施の形態による情報処理システムによるデータの流れを示した図である。

[図4]図4は、図3に続く、本発明の第1の実施の形態による情報処理システムによるデータの流れを示した図である。

[図5]図5は、本発明の第1の実施の形態による情報処理システムのうち、情報処理装置の構成をブロックで示した図である。

[図6]図6は、本発明の第2の実施の形態による情報処理システムによるデータの流れを示した図である。

[図7]図7は、本発明の第3の実施の形態による情報処理システムによるデータの流れを示した図である。

[図8]図8は、本発明の第4の実施の形態による情報処理システムによるデータの流れを示した図である。

[図9]は、図8に続く、本発明の第4の実施の形態による情報処理システムによるデータの流れを示した図である。

発明を実施するための形態

[0022] 第1の実施の形態

《構成》

以下、本発明に係る情報処理装置、情報処理システム、プログラム、記録

媒体及び情報処理方法の実施の形態について、図面を参照して説明する。本実施の形態において「又は」と「もしくは」は「及び」と「並びに」の意味も含んでいる。つまり、例えば、本実施の形態において「A又はB」とは、「A、B並びにA及びB」のいずれかを意味している。

[0023] 本実施の形態の情報処理装置100は、例えばユーザプログラム等のプログラムをインストールすることで生成される。このプログラムは電子メールで配信されてもよいし、所定のURLにアクセスしたうえでログインすることで入手できてよいし、記録媒体に記録されてもよい。本実施の形態によるプログラムは以下に示す情報処理装置100を生成するために利用され、本実施の形態による記録媒体は当該プログラムを記録するために利用される。また、本実施の形態の情報処理方法は上記プログラムがインストールされた情報処理装置100によって実施される。情報処理装置100は、情報処理装置100にインストールされたアプリケーションを実行することによって、本実施の形態の情報処理方法を実行してもよい。

[0024] 本実施の形態の情報処理装置100は一台の装置から構成されてもよいが、複数の装置から構成されてもよい。情報処理装置100が複数の装置から構成される場合には、情報処理装置100を構成する装置は異なる部屋又は異なる場所に設置されてもよく、情報処理装置100の一部と情報処理装置100の残部が遠隔地に配置されてもよい。本実施の形態では「情報処理装置」及び「情報処理システム」という文言を用いて説明するが、確実に2つ以上の装置に分かれている場合には「情報処理システム」という文言を用い、単独の装置から構成されることもあるし、複数の装置から構成されることもある場合には「情報処理装置」という文言を用いる。

[0025] 情報処理装置100は例えばサーバであり、本実施の形態では、一例として、情報処理装置100がサーバである態様を用いて以下説明する。

[0026] 本実施の形態の情報処理装置100は、複数のユーザ端末200と通信可能になっている。情報処理装置100及び複数のユーザ端末200から情報処理システムが構成されている。ユーザ端末200は例えばパソコン、タブ

レット、スマートフォン等である。図5に示すように、情報処理装置100は、ユーザ端末200からの情報を受信する装置受信部（受信部）60と、ユーザ端末200に対して情報を送信する装置送信部（送信部）70と、ユーザ端末200からの情報に基づいてユーザの識別を行うとともに、対象となっているファイルを閲覧できるか否かを判断する識別判断部10と、識別判断部10によって対象となっているファイルを閲覧できると判断された場合に、暗号化されたファイルを復号する復号部30と、様々な情報を記憶する装置記憶部90と、を有してもよい。

[0027] 識別判断部10によるユーザ認証は、ワンタイムパスワード認証、SAML認証、AD認証、メールアドレスによる認証であってもよいし、これらを組み合わせた認証であってもよい。このようにしてユーザ認証が行われることで、当該ユーザ認証に紐づけられたユーザ権限が確認されるようにしてもよい。なお、ファイルの内容によっては、ユーザの識別は行うもののパスワード等を要求せず、ユーザ認証を行わないようにしてもよい。また、ファイルが開いたかどうかだけを確認できるようにしてもよい。このような態様を採用した場合には、ファイルの開いた回数、日時、頻度等に関するファイル取り扱い情報を情報処理装置100で取得して装置記憶部90で記憶してもよい。この場合には、これらの情報を用いてユーザの当該ファイルに対する関心度を調査することができ、当該情報をマーケティング活動に利用することもできる。

[0028] ユーザ端末200は、ユーザ端末200のIE（Internet Explore（登録商標））等のブラウザを通じて情報処理装置100と通信接続されてもよい。例えば、ユーザ端末200がhtmlファイル等の所定の拡張子からなるラップファイル105（図2参照）を実行すると、拡張子html等が関連付けられているブラウザのようなアプリケーションが起動されて、ユーザ端末200が情報処理装置100と通信接続される。所定の拡張子はユーザ端末200が認識できる拡張子であればよく、htmlは単なる一例である。

[0029] 前述したようにユーザ端末200が情報処理装置100と通信接続される

と、情報処理装置１００の識別判断部１０では、ユーザ認証が行われ、かつ例えばhtmlファイル等からなるラップファイル１０５に対するユーザ権限の確認が行われる。このラップファイル１０５には後述する第一ファイル１１０等のファイルが格納されてもよい（埋め込まれてもよい）。ユーザ認証及びユーザ権限に関する情報はラップファイル１０５を作成する作成者が指定してもよい。なお、このようにラップファイル１０５に第一ファイル１１０等のファイルを格納することで、ラップファイル１０５に付けられた拡張子に基づいてユーザ端末２００がファイルを認識できる。このため、例えばラップファイル１０５としてhtmlファイル等を採用した場合には、htmlファイル等の形式としてユーザ端末２００がファイルを認識でき、情報処理装置１００へのアクセスを容易に行うことができるようになる。

[0030] 情報処理装置１００の識別判断部１０で、当該ユーザのユーザ権限で当該ラップファイル１０５内の情報を閲覧できると確認されると、ユーザ端末２００でラップファイル１０５から暗号化された第一ファイル１１０が取り出される等して、ラップファイル１０５でラップされる前の状態に戻ってもよい。なお、このようなラップは、第一ファイル１１０を暗号化したユーザによって行われる。そして、ラップファイル１０５を電子メールによって受信したりUSBメモリ等を介して受け取ったりしたユーザがラップファイル１０５を実行することで、前述したようなユーザ認証やユーザ権限の確認を情報処理装置１００に依頼することになる。

[0031] ラップファイル１０５から暗号化された第一ファイル１１０が取り出されると、ユーザ端末２００から暗号化された第一ファイル１１０が送信され（アップロードされ）、情報処理装置１００の装置受信部６０がユーザ端末２００から当該第一ファイル１１０を受信してもよい。このように装置受信部６０が第一ファイル１１０を受信すると、情報処理装置１００の復号部３０が暗号化された第一ファイル１１０を復号して復号第一ファイル１１０aを作成してもよい（図３参照）。

[0032] 図５に示すように、情報処理装置１００は、復号第一ファイル１１０aを

、ユーザ端末200のブラウザで表示可能な形式からなる第二ファイル120（図3参照）に変換する変換部50と、第二ファイル120を暗号化して、暗号化された第二ファイル120a（以下「暗号化第二ファイル120a」ともいう。）を作成する暗号化部40を有してもよい。変換部50は、復号されたワード（登録商標）やエクセル（登録商標）等からなる復号第一ファイル110aを例えばPDF（登録商標）ファイルや画像ファイル等の第二ファイル120に変換してもよい。暗号化部40は、このようなPDFファイルや画像ファイル等からなる第二ファイル120を暗号化してもよい。なお、PDFファイルや画像ファイル等のユーザ端末200のブラウザで表示可能な形式に変換できる拡張子としては、例えば、PDFファイル、xlsファイル、xlsxファイル、xlsmファイル、docファイル、docxファイル、docmファイル、pptファイル、pptxファイル、pptmファイル、jpegファイル、jpgファイル、pngファイル、gifファイル、bmpファイル、txtファイル等を挙げることができる。なお、第二ファイルのファイル形式はブラウザで表示可能な形式からなっていればよく、PDF等は一例に過ぎない。

[0033] 装置送信部70は、暗号化第二ファイル120aをユーザ端末200に送信してもよい。この際、装置送信部70はユーザ端末200のブラウザに対して暗号化第二ファイル120aを送信してもよい。暗号化第二ファイル120aを受信したユーザ端末200は、ブラウザの一時保存領域に暗号化第二ファイル120aを保存してもよい。

[0034] 情報処理装置100は、装置送信部70が暗号化第二ファイル120aをユーザ端末200に送信した後で、暗号化第二ファイル120aを消去する消去部55を有してもよい。この消去部55は暗号化第二ファイル120aだけではなく第一ファイル110、復号第一ファイル110a、第二ファイル120等の暗号化第二ファイル120aに関連したファイルも消去してもよい。また、第一ファイル110を復号して復号第一ファイル110aを生成する際に第一ファイル110が復号第一ファイル110aに代わってしまい（この結果、第一ファイル110は存在しなくなり）、復号第一ファイル

110aから第二ファイルを生成する際に復号第一ファイル110aが第二ファイルに代わってしまい（この結果、復号第一ファイル110aは存在しなくなり）、第二ファイルを暗号化して暗号化第二ファイル120aを生成する際に第二ファイルが暗号化第二ファイル120aに変わってしまう（この結果、第二ファイルが存在しなくなる）態様を採用することもできる。

[0035] 暗号化第二ファイル120aの閲覧を希望するユーザ端末200からの情報に基づき、装置受信部60は、暗号化第二ファイル120aの部分的な情報をユーザ端末200から受信してもよい（図4参照）。復号部30は、このようにユーザ端末200から受信する暗号化第二ファイル120aの部分的な情報を復号してもよい。装置送信部70は、復号された第二ファイル120の部分的な情報120bをユーザ端末200に送信（返信）してもよい。この際、装置受信部60で受信された第二ファイル120の部分的な情報120bは、装置記憶部90で記憶されることなく、復号部30で復号されて、そのままユーザ端末200に送信されるようにしてもよい。この態様を採用した場合には、復号された第二ファイル120の部分的な情報120bが情報処理装置100に残ることを未然に防止できる。仮に復号された第二ファイル120の部分的な情報120bが情報処理装置100に残る態様を採用した場合には、消去部55によって復号された第二ファイル120の部分的な情報120bを消去するようにしてもよい。

[0036] ユーザ端末200は、nバイト単位（「n」は10, 240以上の整数である。）で暗号化第二ファイル120aの情報を情報処理装置100に送信し（ポストし）、復号部30は送信された暗号化第二ファイル120aのnバイト単位の情報を復号してもよい。なお、発明者らによれば、暗号化第二ファイル120aの情報を部分的に送信して復号する場合において、10, 240バイト以上であればページ描画平均時間が収束して安定した状態となることを確認できたことから、10, 240バイト以上の単位で送信、受信及び復号することは有益である。なお、発明者らが確認したとことによると、ページ描画平均時間を収束させる観点からすると51, 200バイト以上

であることがより有益であった。

- [0037] ユーザ端末200は、暗号化第二ファイル120aの情報を閲覧するサイズ分だけ情報処理装置100に送信してもよい。閲覧するサイズとは、例えばユーザ端末200の表示画面に示されるサイズであってもよいし、同一ページの情報であってもよい。閲覧するサイズがユーザ端末200の表示画面に示されるサイズである場合には、画面がスクロールされる度に、ユーザ端末200が暗号化第二ファイル120aの部分的な情報を情報処理装置100に送信し、復号部30がユーザ端末200から受信する暗号化第二ファイル120aの部分的な情報を復号し、装置送信部70が復号された暗号化第二ファイル120aの部分的な情報をユーザ端末200に送信するようにしてもよい。閲覧するサイズが1ページ分の情報である場合には、ページが変わる度に、ユーザ端末200が暗号化第二ファイル120aの部分的な情報を情報処理装置100に送信し、復号部30がユーザ端末200から受信する暗号化第二ファイル120aの部分的な情報を復号し、装置送信部70が復号された暗号化第二ファイル120aの部分的な情報をユーザ端末200に送信するようにしてもよい。
- [0038] なお、ファイルをラップファイル105内に格納する場合には、専用のアプリケーションを用いられることになる。専用のアプリケーションは、専用のアプリケーションを立ち上げるためのアイコンを右クリック（ダブルクリック）したり、専用のアプリケーションにドラッグアンドドロップしたりするようにしてもよい。
- [0039] ラップファイル105内に格納するファイルは既に暗号化されているものを用いてもよいし、暗号化されていないものを用いてもよい。ファイルを暗号化してラップファイル105内に格納する際、ブラウザを通じて変換できる権限を所定のユーザに付与するように選択してもよい。この際の拡張子としては、例えば「.html」が用いられてもよい。既に暗号化されているファイルを用いる場合には、暗号化されているファイルと、当該ファイルを暗号化して格納するラップファイル105とは別ファイルとして取り扱われてもよ

い。この場合には、暗号化されているファイルの作成者と、当該ファイルを暗号化して格納するラップファイル１０５の作成者とが異なる者となることもある。なお、所定の権限が設定されている場合にだけ、既に暗号化されているファイルをラップファイル１０５内に格納する形式に変換できるようになってもよい。

[0040] 第一ファイル１１０等のファイルを暗号化してラップファイル１０５に格納するとき、コピーアンドペーストを禁止したり、印刷権限の有無を設定したり、印刷したときに透かしを入れるようにしてもよい。また第一ファイル１１０等のファイルを暗号化してラップファイル１０５に格納するとき、どのような認証方式を採用するかを選択できるようにしてもよい。なお、ファイルを暗号化してラップファイル１０５に格納するときにキャプチャを禁止するように制御するようにしてもよく、この場合においてユーザ端末２００に専用アプリケーションがインストールされているときには、ユーザ端末２００のキャプチャ機能を制御し、キャプチャを取得できないようにすることもできる。

[0041] ラップファイル１０５の形式としては様々なものを用いることができ、前述したhtmlファイルの他、exeファイル、pdfファイル、gifファイル、jpegファイル、bmpファイル、pngファイル等を用いることができる。

[0042] 《方法》

本実施の形態の情報処理方法では、前述した「構成」についてのあらゆる態様を利用することができるが、以下では、情報処理方法の一例を説明する。なお、「方法」で述べるあらゆる構成は、本実施の形態の構成として利用することができる。

[0043] ユーザ端末２００がhtmlファイル等からなるラップファイル１０５（図２参照）を実行すると、拡張子html等が関連付けられているブラウザのようなアプリケーションが起動されて、ユーザ端末２００が情報処理装置１００と通信接続される。このようにしてユーザ端末２００が情報処理装置１００と通信接続されると、情報処理装置１００の識別判断部１０では、ユーザ端末

２００からの情報に基づいてユーザの識別が行われ、対象となっているラップファイル１０５内の情報（本実施の形態では第一ファイル１１０）を閲覧できるか否かが判断される。

[0044] 識別判断部１０によってラップファイル１０５内の情報を閲覧できると判断されると、ラップファイル１０５内の暗号化された第一ファイル１１０がラップファイル１０５内から取り出される。

[0045] 次に、ユーザ端末２００から暗号化された第一ファイル１１０が送信され（アップロードされ）、情報処理装置１００の装置受信部６０がユーザ端末２００から当該第一ファイル１１０を受信する。

[0046] 次に、情報処理装置１００の復号部３０が暗号化された第一ファイル１１０を復号して復号第一ファイル１１０aを作成する（図３参照）。

[0047] 次に、情報処理装置１００の変換部５０が、復号された第一ファイル１１０がユーザ端末２００のブラウザで表示可能な形式からなる第二ファイル１２０に変換する。

[0048] 次に、情報処理装置１００の暗号化部４０が、第二ファイル１２０を暗号化して暗号化第二ファイル１２０aを作成する。

[0049] 次に、暗号化第二ファイル１２０aが、第一ファイル１１０を情報処理装置１００に送信したユーザ端末２００に装置送信部７０を介して送信（返信）される。この際、装置送信部７０はユーザ端末２００のブラウザに対して第二ファイル１２０を送信してもよい。

[0050] このようにして暗号化第二ファイル１２０aがユーザ端末２００に送信されると、消去部５５が第一ファイル１１０、復号第一ファイル１１０a、第二ファイル１２０及び暗号化第二ファイル１２０aを消去する。

[0051] 暗号化第二ファイル１２０aをユーザが閲覧する際には、装置受信部６０が暗号化第二ファイル１２０aの部分的な情報をユーザ端末２００から受信する（図４参照）。そして、復号部３０がユーザ端末２００から受信する暗号化された第二ファイル１２０の部分的な情報１２０bを復号し、装置送信部７０が復号された第二ファイル１２０の部分的な情報１２０bをユーザ端

末２００に送信する。この結果として、第二ファイル１２０の部分的な情報１２０ｂがユーザによって確認できるようになる。

[0052] 《作用・効果》

次に、上述した構成又は方法によって得られる作用・効果であって、未だ説明していないものを中心に説明する。なお、「作用・効果」で述べるあらゆる構成は、本実施の形態の構成として利用することができる。

[0053] 本実施の形態において、ユーザ認証とユーザ権限を確認し、ユーザ認証及びユーザ権限に基づいて暗号化されたファイルを復号する態様を採用した場合には、ファイルを復号するアプリケーションがインストールされていないユーザ端末２００でも、情報処理装置１００にアクセスすることでファイルを復号することができる。

[0054] ユーザ端末２００から受信した暗号化された第一ファイル１１０を復号して復号第一ファイル１１０ａを作成し、復号第一ファイル１１０ａを第二ファイル１２０に変換する態様を採用した場合には、第一ファイル１１０のファイル形式に係わらず、第二ファイル１２０という所定のファイル形式に変更できる。例えば、ワードやエクセル等ではブラウザで表示させることはできないが、第二ファイル１２０としてPDFや画像の形式にすることでブラウザによって表示させることができるようになる。

[0055] 第二ファイル１２０を暗号化して、暗号化した第二ファイル１２０をユーザ端末２００に送信する態様を採用する場合には、ユーザ端末２００に戻った第二ファイル１２０に関して一定の制御をかけることができる点で有益である。仮に第二ファイル１２０が暗号化されていない場合には、ユーザ端末２００で自由に操作することができるようになるが、本態様を採用することで、このような事態が発生することを防止できる。

[0056] 装置送信部７０が暗号化された第二ファイル１２０をユーザ端末２００に送信した後で、情報処理装置１００の装置記憶部９０内から第二ファイル１２０を消去する態様を採用した場合には、例えばサーバである情報処理装置１００に情報が残ることも防止できる。このため、より高いセキュリティを

実現できる点で有益である。

[0057] ユーザが暗号化第二ファイル 120a を閲覧する際に、装置受信部 60 が暗号化された第二ファイル 120 の部分的な情報 120b をユーザ端末 200 から受信し、復号部 30 がユーザ端末 200 から受信する暗号化された第二ファイル 120 の部分的な情報 120b を復号し、装置送信部 70 が復号された第二ファイル 120 の部分的な情報 120b をユーザ端末 200 に送信する態様を採用した場合には、ユーザ装置では第二ファイル 120 の部分的な情報 120b が表示されるだけであることから、第二ファイル 120 内の情報を高いセキュリティで管理できる。なお、ユーザ端末 200 に戻される部分的に復号された情報は例えばブラウザを通じて表示され、画面から表示されなくなったりページが変わったりしたタイミングで、情報処理装置 100 からの指示によってブラウザのキャッシュが消されるようにしてもよい。

[0058] 復号部 30 がユーザ端末 200 から受信する暗号化された第二ファイル 120 の情報を閲覧するサイズ分だけ復号する態様を採用した場合には、閲覧するのに必要な非常に限られた範囲のみで復号することから高いセキュリティを実現できる。

[0059] 装置受信部 60 が暗号化された第二ファイル 120 の部分的な情報 120b を n バイト単位（「 n 」は 10, 240 以上の整数である。）でユーザ端末 200 から受信し、復号部 30 がユーザ端末 200 から受信する暗号化された第二ファイル 120 の部分的な情報 120b を n バイト単位で復号し、装置送信部 70 が復号された第二ファイル 120 の部分的な情報 120b を n バイト単位でユーザ端末 200 に送信する態様を採用した場合には、前述したように、ページ描画平均時間を収束させることができ、安定した状態で復号した情報を画面表示させることができる。

[0060] 第 2 の実施の形態

次に、本発明の第 2 の実施の形態について、主に図 6 を用いて説明する。

[0061] 本実施の形態では、装置受信部 60 がユーザ端末 200 から暗号化された

第一ファイル 110 を受信し（図 2 参照）、復号部 30 が暗号化された第一ファイル 110 を復号して復号第一ファイル 110 a を作成し（図 6 参照）、変換部 50 が復号された第一ファイル 110 を第二ファイル 120 に変換し、装置送信部 70 が変換部 50 で変換された第二ファイル 120 をユーザ端末 200 に送信する態様となっている。本実施の形態では、第 1 の実施の形態で説明したあらゆる態様を本実施の形態で採用することができる。第 1 の実施の形態と同一の物については同じ符号を付して説明する。

[0062] 本実施の形態によれば、第 1 の実施の形態と比較して制御態様が簡便な点で有益である。他方、本実施の形態と比較すると、第 1 の実施の形態では、第二ファイル 120 が暗号化されてユーザ端末 200 に戻される点及び第二ファイル 120 の情報が部分的に復号される点でセキュリティが高くなっていることが有益である。

[0063] なお、本実施の形態でも消去部 55 が、ユーザ端末 200 に送信された第二ファイル 120 と、第二ファイル 120 に関連する第一ファイル 110 及び復号第一ファイル 110 a を消去してもよい。

[0064] 第 3 の実施の形態

次に、本発明の第 3 の実施の形態について、主に図 7 を用いて説明する。

[0065] 第 1 の実施の形態及び第 2 の実施の形態では、ユーザ端末 200 から情報処理装置 100 に暗号化された第一ファイル 110 が送信される態様となっていた。本実施の形態では、ユーザ端末 200 から情報処理装置 100 に対して第一ファイル 110 等のファイルそのものは送信されない。本実施の形態では、装置受信部 60 が暗号化された第三ファイル 130 の部分的な情報をユーザ端末 200 から受信する態様となっている（図 7 参照）。この第三ファイル 130 は、ユーザ端末 200 のブラウザで表示可能な形式からなっている。第三ファイル 130 の部分的な情報を情報処理装置 100 が受信すると、復号部 30 が当該部分的な情報を復号し、復号された第三ファイル 130 の部分的な情報 130 b はユーザ端末 200 に送信されることになる。本実施の形態では、第 1 の実施の形態及び第 2 の実施の形態で説明したあら

ゆる態様を本実施の形態で採用することができる。第1の実施の形態及び第2の実施の形態と同一の物については同じ符号を付して説明する。

[0066] 本実施の形態では、ファイルがユーザ端末200から情報処理装置100に送信されない点で、処理が簡易なものとなり、またセキュリティを高めることもできる。

[0067] 第1の実施の形態で説明したのと同様に、ユーザ端末200は、nバイト単位（「n」は10, 240以上の整数である。）で暗号化された第三ファイル130の情報を情報処理装置100に送信し（ポストし）、復号部30は送信された暗号化された第三ファイル130のnバイト単位の情報を復号してもよい。

[0068] ユーザ端末200は、暗号化された第三ファイル130の情報を閲覧するサイズ分だけ情報処理装置100に送信してもよい。閲覧するサイズとは、例えばユーザ端末200の表示画面に示されるサイズであってもよいし、同一ページの情報であってもよい。閲覧するサイズがユーザ端末200の表示画面に示されるサイズである場合には、画面がスクロールされる度に、ユーザ端末200が暗号化された第三ファイル130の部分的な情報を情報処理装置100に送信し、復号部30がユーザ端末200から受信する暗号化された第三ファイル130の部分的な情報を復号し、装置送信部70が復号された第三ファイル130の部分的な情報130bをユーザ端末200に送信するようにしてもよい。閲覧するサイズが1ページ分の情報である場合には、ページが変わる度に、ユーザ端末200が暗号化された第三ファイル130の部分的な情報を情報処理装置100に送信し、復号部30がユーザ端末200から受信する暗号化された第三ファイル130の部分的な情報を復号し、装置送信部70が復号された第三ファイル130の部分的な情報130bをユーザ端末200に送信するようにしてもよい。

[0069] また、装置受信部60で受信された第三ファイル130の部分的な情報は、装置記憶部90で記憶されることなく、復号部30で復号されて、そのままユーザ端末200に送信されるようにしてもよい。

[0070] 但し、本実施の形態において第三ファイル１３０がユーザ端末２００のブラウザで表示可能な形式（例えばPDF形式）からなる態様を採用する場合には、柔軟な運用を取る際に支障が出ることがある。例えば、ユーザの権限を変えて、ラップファイル１０５を受信した第一ユーザにラップファイル１０５に格納されたファイルの情報を変更できる権限を設定したとしても、ラップファイル１０５内にはブラウザで表示可能な形式からなる例えばPDFのような第三ファイル１３０が格納されており、ワードファイルやエクセルファイルのような元データがラップファイル１０５内には格納されていない。このため、第一ユーザはラップファイル１０５に格納されたファイルの情報を変更できる権限を有していても、元データを有していないことから、加工が困難になる。この点、例えば第１の実施の形態では、ワードファイルやエクセルファイルのような元データからなる第一ファイル１１０がラップファイル１０５内には格納されていることから、ユーザの権限を変えて、ラップファイル１０５を受信した第一ユーザにラップファイル１０５に格納されたファイルの情報を変更できる権限を設定した場合には、当該第一ユーザは元データを用いてデータの加工を行うことができる点で有益である。

[0071] なお、第三ファイル１３０を暗号化してラップファイル１０５内に格納する場合には、前述したように専用のアプリケーションを用いられることになる。

[0072] 第４の実施の形態

次に、本発明の第４の実施の形態について、主に図８及び図９を用いて説明する。

[0073] 上記各実施の形態では、ラップファイル１０５に格納されたファイルを受信したユーザの立場から説明を行っていた。本実施の形態では、ファイルをラップファイル１０５に格納して送信するユーザの立場で説明する。本実施の形態では、識別判断部１０でユーザ認証が正常に行われた場合、つまりユーザ端末２００からの情報に基づいて識別判断部１０によって当該ユーザがファイルを暗号化できると判断された場合に、暗号化部４０が第四ファイル

140等のファイルを暗号化できるようになっている。第四ファイル140等のファイルが暗号化されると、装置送信部70は暗号化された第四ファイル140a（以下「暗号化第四ファイル140a」ともいう。）をユーザ端末200に送信する（図9参照）。本実施の形態では、上記各実施の形態で説明したあらゆる態様を本実施の形態で採用することができる。上記各実施の形態と同一の物については同じ符号を付して説明する。

[0074] 一例としては、ユーザ端末200からの情報に基づいて情報処理装置100の識別判断部10でユーザ認証が行われ、当該ユーザがファイルを暗号化することができる権限があることを識別判断部10が確認できれば、ユーザ端末200から第四ファイル140が情報処理装置100に対してアップロードされて、情報処理装置100の装置受信部60が第四ファイル140を受信する（図8参照）。

[0075] このように装置受信部60が第四ファイル140を受信すると、情報処理装置100の暗号化部40が第一ファイル110を暗号化して暗号化第四ファイル140aを作成する（図9参照）。

[0076] このように暗号化第四ファイル140aが作成されると、情報処理装置100の装置送信部70からユーザ端末200のブラウザに対して暗号化第四ファイル140aが送信される。そして、この暗号化第四ファイル140aはユーザ端末200の記憶部等で記憶できるようになる。

[0077] 本態様によれば、専用のアプリケーションがインストールされていなくても、サーバ等の情報処理装置100によって第四ファイル140のようなファイルを暗号化することができる。

[0078] 本実施の形態では、消去部55が第四ファイル140及び暗号化第四ファイル140aを消去してもよい。

[0079] なお、本実施の形態を採用する場合には、第1の実施の形態乃至第3の実施の形態のように受信側のユーザ端末200からの処理態様が採用されてもよいし、逆に第1の実施の形態乃至第3の実施の形態のように受信側のユーザ端末200からの処理態様は採用されなくてもよい。

[0080] 上述した各実施の形態の記載及び図面の開示は、特許請求の範囲に記載された発明を説明するための一例に過ぎず、上述した実施の形態の記載又は図面の開示によって特許請求の範囲に記載された発明が限定されることはない。

[0081] 上記各実施の形態の識別判断部 10、復号部 30、暗号化部 40、変換部 50、消去部 55 等を含む各構成要素は、ＩＣチップ、ＬＳＩ等の集積回路等に形成された論理回路（ハードウェア）や専用回路によって実現してもよいし、ＣＰＵ、メモリ等を用いてソフトウェアによって実現してもよい。また、各構成要素は、１又は複数の集積回路により実現されてよく、複数の構成要素が１つの集積回路によって実現されてもよい。

符号の説明

[0082]	10	識別判断部
	30	復号部
	40	暗号化部
	50	変換部
	55	消去部
	60	装置受信部（受信部）
	70	装置送信部（送信部）
	100	情報処理装置
	110	第一ファイル
	120	第二ファイル
	130	第三ファイル
	140	第四ファイル
	200	ユーザ端末